StorageGRID 11.6 문서

StorageGRID

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/storagegrid-116/index.html on April 10, 2024. Always check docs.netapp.com for the latest.

목차

StorageGRID 11.6 문서 . . . 1
릴리스 정보 . . . 2
시작하십시오 . . . 3
- 그리드 프라이머 . . . 3
- 네트워킹 지침 . . . 70

어플라이언스 하드웨어를 설치하고 유지 관리합니다 . . . 100
- SG100 및 SG1000 서비스 어플라이언스 . . . 100
- SG6000 스토리지 어플라이언스 . . . 209
- SG5700 스토리지 어플라이언스 . . . 388
- SG5600 스토리지 어플라이언스 . . . 519

소프트웨어 설치 및 업그레이드 . . . 636
- StorageGRID 소프트웨어를 업그레이드합니다 . . . 636
- Red Hat Enterprise Linux 또는 CentOS를 설치합니다 . . . 669
- Ubuntu 또는 Debian을 설치합니다 . . . 730
- VMware를 설치합니다 . . . 792

시스템 관리를 수행합니다 . . . 839
- StorageGRID 관리 . . . 839
- ILM을 사용하여 개체를 관리합니다 . . . 1129
- 시스템 강화 . . . 1286
- FabricPool를 구성합니다 . . . 1294

StorageGRID를 사용합니다 . . . 1313
- 테넌트 계정을 사용합니다 . . . 1313
- S3을 사용합니다 . . . 1413
- Swift를 사용합니다 . . . 1535

StorageGRID 모니터링 및 유지 관리 . . . 1565
- 모니터링하고 문제를 해결합니다 . . . 1565
- 그리드를 확장합니다 . . . 1897
- 복구 및 유지 관리 . . . 1948
- 감사 로그를 검토합니다 . . . 2186

사용자 환경에서 StorageGRID를 활성화하는 방법 . . . 2269
기타 버전의 NetApp StorageGRID 설명서 . . . 2270
법적 고지 . . . 2271
- 저작권 . . . 2271
- 상표 . . . 2271
- 특허 . . . 2271
- 개인 정보 보호 정책 . . . 2271
- 오픈 소스 . . . 2271

StorageGRID 11.6 문서

릴리스 정보

새로운 기능, 제거되거나 사용되지 않는 기능, 해결된 문제 및 알려진 문제에 대한 릴리스 관련 정보를 얻습니다.

NetApp Support 사이트 에 로그인합니다 "PDF 파일을 보거나 다운로드합니다" StorageGRID 11.6 릴리스 정보 포함.

시작하십시오

그리드 프라이머

그리드 프라이머: 개요

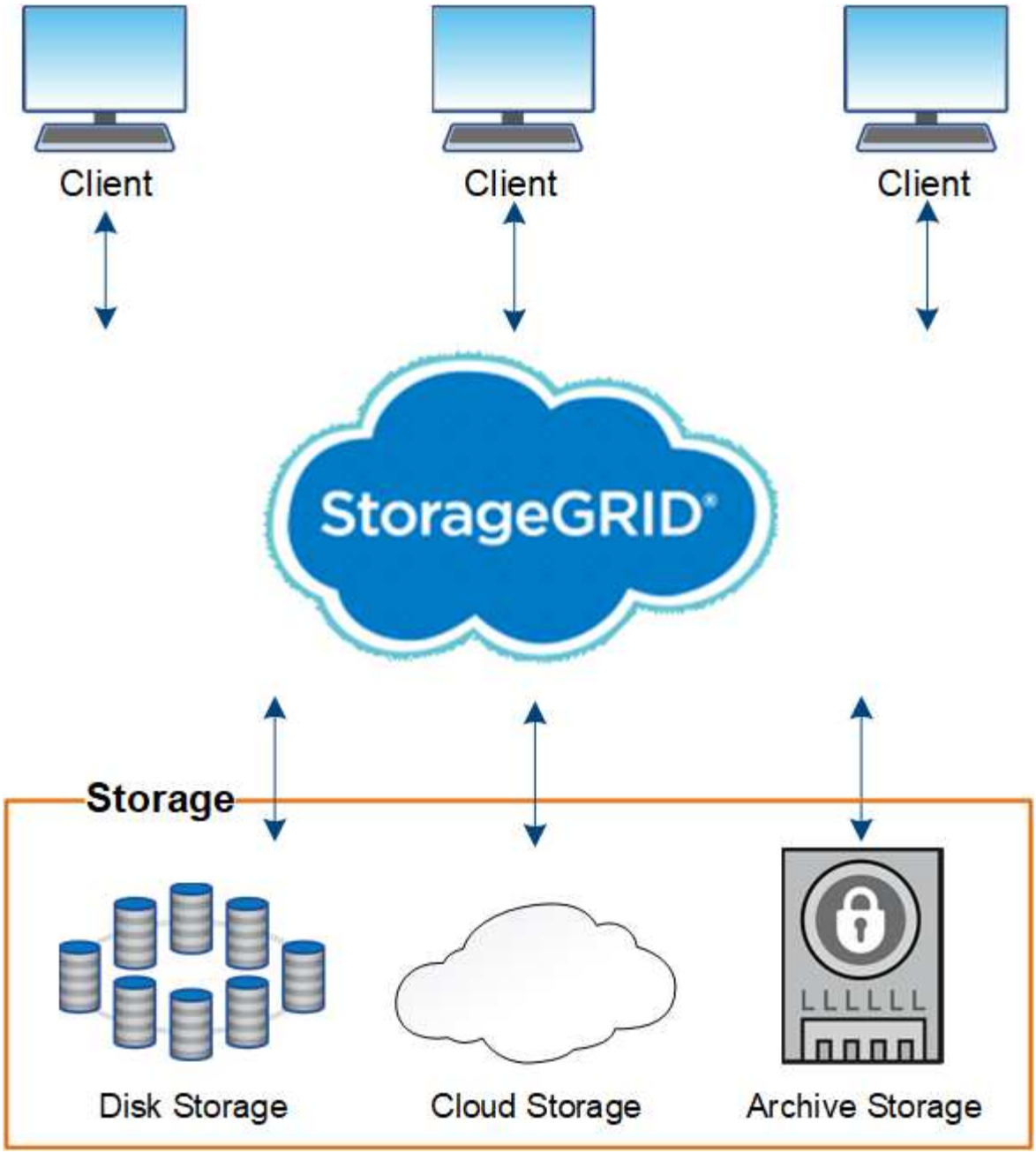
이 소개를 사용하여 StorageGRID 시스템에 대한 개요를 살펴보고 StorageGRID 아키텍처와 네트워킹 토폴로지, 데이터 관리 기능 및 사용자 인터페이스에 대해 알아보십시오.

StorageGRID란 무엇입니까**?**

NetApp ® StorageGRID ® 는 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.

StorageGRID는 비정형 데이터를 대규모로 저장할 수 있는 안전하고 내구성 있는 스토리지를 제공합니다. 메타데이터 중심의 통합 라이프사이클 관리 정책은 라이프사이클 전반에서 데이터 위치를 최적화합니다. 콘텐츠가 적절한 위치에 적시에 적절한 스토리지 계층에 배치되어 비용을 절감합니다.

StorageGRID는 지리적으로 분산된 이중화, 이기종 노드로 구성되며, 기존 및 차세대 클라이언트 애플리케이션과 모두 통합할 수 있습니다.



StorageGRID 시스템의 장점은 다음과 같습니다.

- 비정형 데이터를 위해 지리적으로 분산된 데이터 저장소를 대규모로 확장 및 사용하기 쉽습니다.
- 표준 오브젝트 스토리지 프로토콜:
  - Amazon Web Services S3(Simple Storage Service)
  - OpenStack Swift
- 하이브리드 클라우드 지원: 정책 기반 ILM(정보 라이프사이클 관리)은 AWS(Amazon Web Services) 및 Microsoft Azure를 비롯한 퍼블릭 클라우드에 오브젝트를 저장합니다. StorageGRID 플랫폼 서비스를 사용하면 퍼블릭 클라우드에 저장된 개체를 콘텐츠 복제, 이벤트 알림 및 메타데이터에서 검색할 수 있습니다.
- 내구성과 가용성을 보장하는 유연한 데이터 보호 복제 및 계층적 삭제 코딩을 사용하여 데이터를 보호할 수 있습니다. 사용되지 않는 데이터와 사용 중인 데이터를 검증하여 장기간 보존에 대한 무결성을 보장합니다.
- 동적 데이터 라이프사이클 관리: 스토리지 비용 관리를 지원합니다. 개체 수준에서 데이터 라이프사이클을 관리하는

ILM 규칙을 만들고 데이터 지역성, 내구성, 성능, 비용 및 보존 시간을 사용자 지정할 수 있습니다. 테이프는 통합 아카이브 계층으로 사용할 수 있습니다.

- StorageGRID 리소스 전체에서 데이터 로드를 최적화하기 위한 통합 로드 밸런싱으로 데이터 스토리지 및 일부 관리 기능의 고가용성 제공
- 여러 스토리지 테넌트 계정을 지원하여 시스템에 저장된 객체를 다른 엔터티로 분리할 수 있습니다.
- 포괄적인 알림 시스템, 그래픽 대시보드, 모든 노드 및 사이트에 대한 자세한 상태 등을 비롯하여 StorageGRID 시스템의 상태를 모니터링하는 다양한 툴이 제공됩니다.
- 소프트웨어 또는 하드웨어 기반 구축 지원 다음 중 한 가지 방법으로 StorageGRID를 구축할 수 있습니다.
  - VMware에서 실행 중인 가상 시스템
  - Linux 호스트의 컨테이너 엔진
  - StorageGRID 엔지니어링 어플라이언스:
    - 스토리지 어플라이언스는 오브젝트 스토리지를 제공합니다.
    - 서비스 어플라이언스는 그리드 관리 및 로드 밸런싱 서비스를 제공합니다.
- 다음 규정에 따른 스토리지 요구사항 준수:
  - 17 CFR § 240.17a-4(f)의 증권거래위원회(SEC)로 교환 회원, 중개인 또는 딜러를 규제합니다.
  - SEC Rule 17a-4(f)의 형식 및 미디어 요구 사항을 방어하는 금융 산업 규제 기관(FINRA) 규칙 4511(c).
  - CFTC(Commodity Futures Trading Commission): 17 CFR § 1.31(c) - (d) 규제로 상품 선물거래를 규제합니다.
- 무중단 업그레이드 및 유지보수 운영: 업그레이드, 확장, 서비스 해제 및 유지보수 절차 중에도 내용에 대한 액세스 유지
- 통합 ID 관리. 사용자 인증을 위해 Active Directory, OpenLDAP 또는 Oracle Directory Service와 통합됩니다. SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용하여 StorageGRID와 AD FS(Active Directory Federation Services) 간에 인증 및 권한 부여 데이터를 교환하는 SSO(Single Sign-On)를 지원합니다.

StorageGRID 하이브리드 클라우드

정책 기반의 데이터 관리를 구현하여 클라우드 스토리지 풀에 오브젝트를 저장하고 StorageGRID 플랫폼 서비스를 활용하여 NetApp FabricPool를 통해 StorageGRID로 데이터를 이동하는 하이브리드 클라우드 구성에서 StorageGRID를 사용할 수 있습니다.

클라우드 스토리지 풀

클라우드 스토리지 풀을 사용하면 StorageGRID 시스템 외부에 오브젝트를 저장할 수 있습니다. 예를 들어, 자주 액세스하지 않는 오브젝트를 Amazon S3 Glacier, S3 Glacier Deep Archive 또는 Microsoft Azure Blob 스토리지의 아카이브 액세스 계층과 같은 저비용 클라우드 스토리지로 이동할 수 있습니다. 또는 스토리지 볼륨 또는 스토리지 노드 장애로 인해 손실된 데이터를 복구하는 데 사용할 수 있는 StorageGRID 개체의 클라우드 백업을 유지 관리할 수도 있습니다.

> FabricPool에서 클라우드 스토리지 풀 타겟의 객체를 검색하는 지연 시간이 추가되었기 때문에 클라우드 스토리지 풀을 사용할 수 없습니다.

S3 플랫폼 서비스

S3 플랫폼 서비스를 사용하면 원격 서비스를 오브젝트 복제, 이벤트 알림 또는 검색 통합을 위한 엔드포인트로 사용할 수 있습니다. 플랫폼 서비스는 그리드의 ILM 규칙과 독립적으로 작동하며 개별 S3 버킷에 대해 활성화됩니다. 지원되는 서비스는 다음과 같습니다.

- CloudMirror 복제 서비스는 지정된 오브젝트를 Amazon S3 또는 두 번째 StorageGRID 시스템에 있는 타겟 S3 버킷에 자동으로 미러링합니다.
- 이벤트 알림 서비스는 지정된 작업에 대한 메시지를 SNS(Simple Notification Service) 이벤트 수신을 지원하는 외부 끝점으로 보냅니다.
- 검색 통합 서비스는 외부 Elasticsearch 서비스에 개체 메타데이터를 전송하여 타사 도구를 사용하여 메타데이터를 검색, 시각화 및 분석할 수 있도록 합니다.

예를 들어, CloudMirror 복제를 사용하여 특정 고객 레코드를 Amazon S3에 미러링한 다음 AWS 서비스를 활용하여 데이터에 대한 분석을 수행할 수 있습니다.

StorageGRID를 이용한 ONTAP 데이터 계층화

FabricPool를 사용하여 데이터를 StorageGRID로 계층화하여 ONTAP 스토리지 비용을 절감할 수 있습니다. FabricPool는 사내 또는 사외에서 데이터를 저비용 오브젝트 스토리지 계층으로 자동 계층화하는 NetApp Data Fabric 기술입니다.

수동 계층화 솔루션과 달리 FabricPool는 데이터 계층화를 자동화하여 스토리지 비용을 줄임으로써 총 소유 비용을 절감합니다. StorageGRID를 비롯한 퍼블릭 클라우드와 프라이빗 클라우드로 계층화하여 클라우드 경제성의 이점을 제공합니다.

관련 정보

- StorageGRID 관리
- 테넌트 계정을 사용합니다
- ILM을 사용하여 개체를 관리합니다
- FabricPool용 StorageGRID를 구성합니다

StorageGRID 아키텍처 및 네트워크 토폴로지

StorageGRID 시스템은 하나 이상의 데이터 센터 사이트에 있는 여러 유형의 그리드 노드로 구성됩니다.

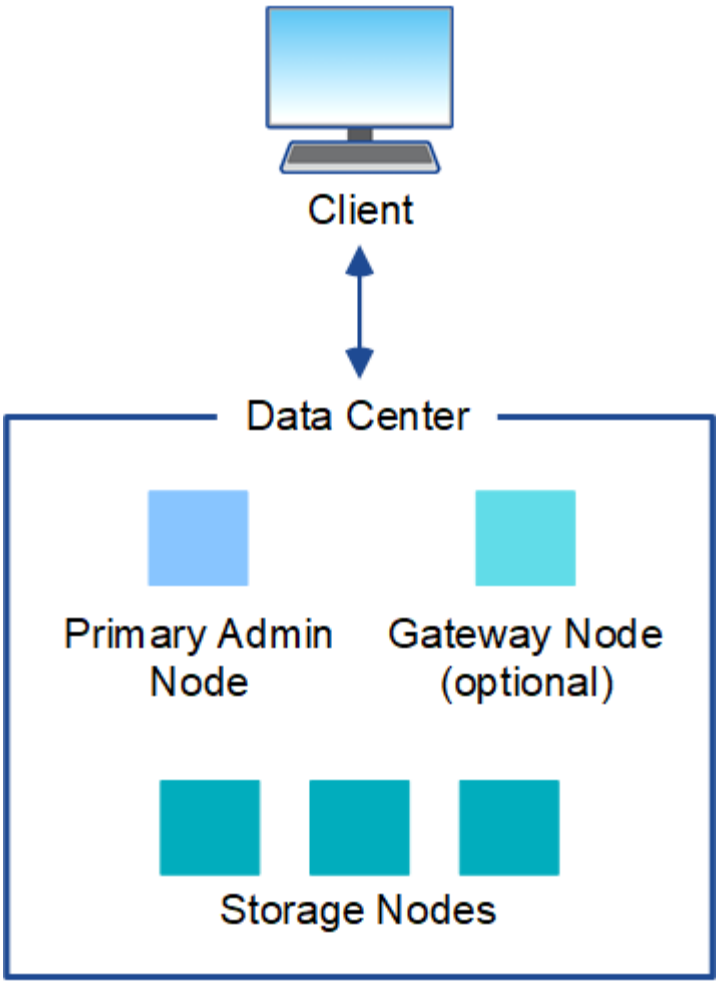
StorageGRID 네트워크 토폴로지, 요구 사항 및 그리드 통신에 대한 자세한 내용은 를 참조하십시오 네트워킹 지침.

구축 토폴로지

StorageGRID 시스템은 단일 데이터 센터 사이트 또는 여러 데이터 센터 사이트에 구축할 수 있습니다.

단일 사이트

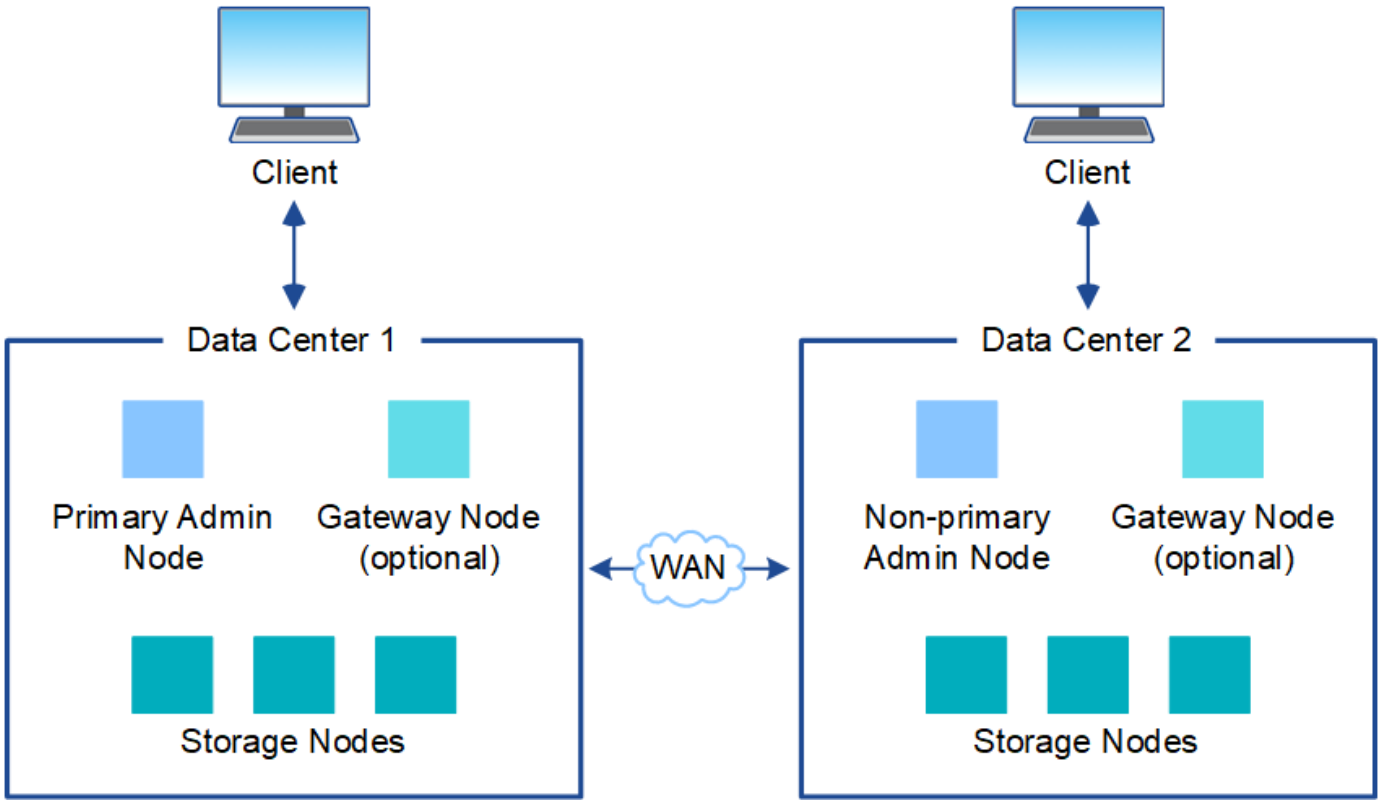
단일 사이트를 통한 배포에서는 StorageGRID 시스템의 인프라 및 운영이 중앙 집중화됩니다.



여러 사이트

사이트가 여러 개인 배포에서는 각 사이트에 다양한 유형과 개수의 StorageGRID 리소스를 설치할 수 있습니다. 예를 들어, 한 데이터 센터에 다른 데이터 센터보다 더 많은 스토리지가 필요할 수 있습니다.

지진에 장애가 있거나 홍수 범람장과 같이 서로 다른 장애 도메인에 있는 서로 다른 지역에 여러 사이트가 있는 경우가 많습니다. 데이터를 다른 사이트에 자동으로 배포하면 데이터 공유 및 재해 복구가 가능합니다.



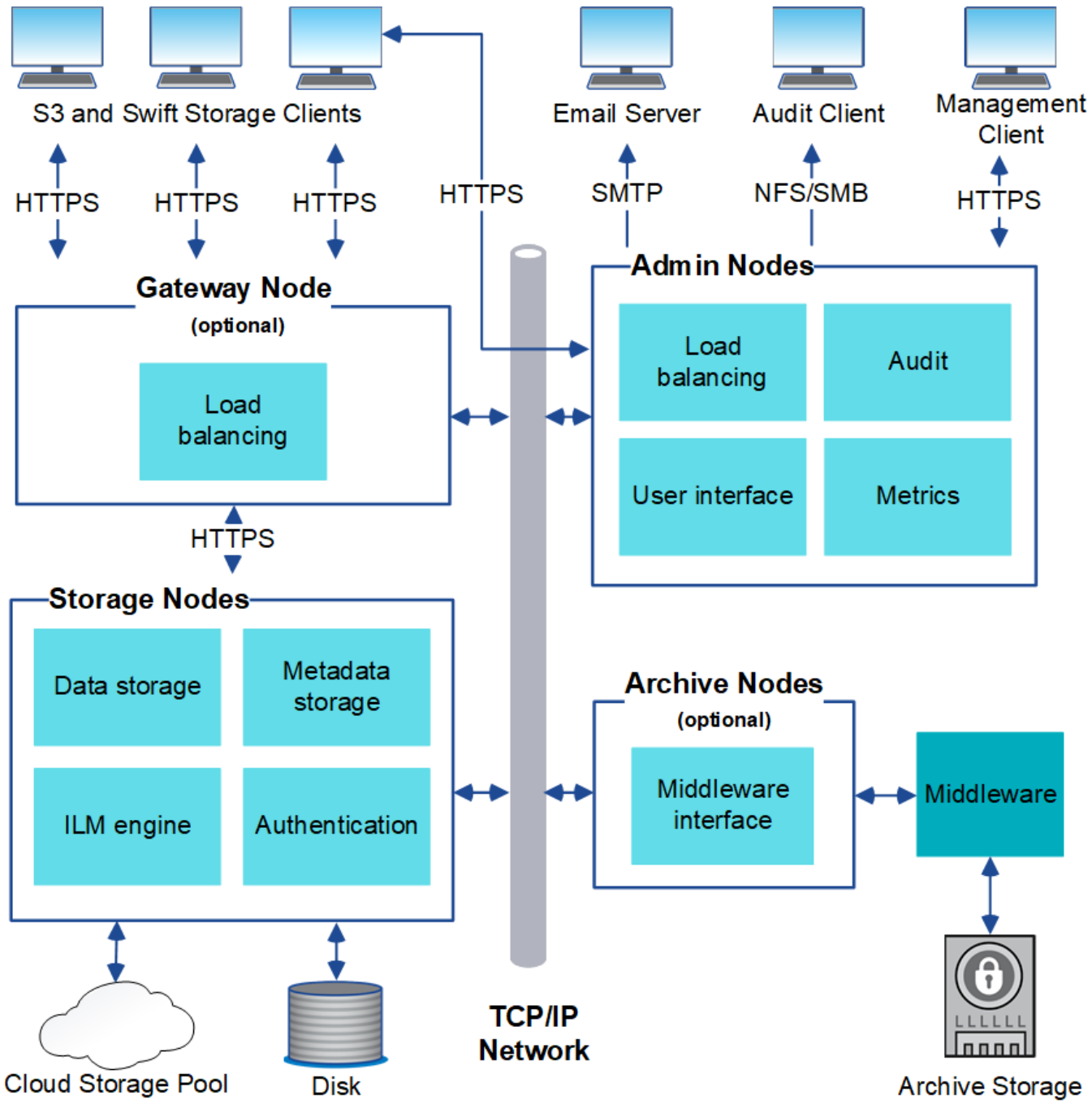
또한 단일 데이터 센터 내에 여러 개의 논리적 사이트가 존재하여 분산된 복제 및 삭제 코딩을 통해 가용성과 복원력을 높일 수 있습니다.

그리드 노드 이중화

단일 사이트 또는 다중 사이트 배포에서는 이중화를 위해 선택적으로 여러 관리 노드 또는 게이트웨이 노드를 포함할 수 있습니다. 예를 들어, 단일 사이트나 여러 사이트에 둘 이상의 관리 노드를 설치할 수 있습니다. 그러나 각 StorageGRID 시스템에는 하나의 기본 관리 노드만 있을 수 있습니다.

시스템 아키텍처

이 다이어그램은 StorageGRID 시스템 내에서 그리드 노드를 배열하는 방법을 보여 줍니다.



S3 및 Swift 클라이언트는 StorageGRID에 오브젝트를 저장하고 검색합니다. 다른 클라이언트는 e-메일 알림을 보내고, StorageGRID 관리 인터페이스에 액세스하고, 선택적으로 감사 공유에 액세스하는 데 사용됩니다.

S3 및 Swift 클라이언트는 게이트웨이 노드 또는 관리 노드에 연결하여 스토리지 노드에 대한 로드 밸런싱 인터페이스를 사용할 수 있습니다. 또는 S3 및 Swift 클라이언트가 HTTPS를 사용하여 스토리지 노드에 직접 연결할 수 있습니다.

오브젝트는 소프트웨어 또는 하드웨어 기반 스토리지 노드의 StorageGRID 내부, 테이프 등의 외부 아카이브 미디어 또는 외부 S3 버킷 또는 Azure Blob 스토리지 컨테이너로 구성된 클라우드 스토리지 풀에 저장할 수 있습니다.

그리드 노드 및 서비스

StorageGRID 시스템의 기본 구성 요소는 그리드 노드입니다. 노드에는 그리드 노드에 일련의 기능을 제공하는 소프트웨어 모듈인 서비스가 포함됩니다.

StorageGRID 시스템은 네 가지 유형의 그리드 노드를 사용합니다.

- * 관리 노드 * 는 시스템 구성, 모니터링 및 로깅과 같은 관리 서비스를 제공합니다. Grid Manager에 로그인하면 관리 노드에 연결됩니다. 각 그리드에는 1개의 기본 관리 노드가 있어야 하며 이중화를 위해 추가적인 비 기본 관리 노드가 있을 수 있습니다. 모든 관리 노드에 연결할 수 있으며 각 관리 노드에는 StorageGRID 시스템의 유사한 보기가 표시됩니다. 그러나 기본 관리 노드를 사용하여 유지 관리 절차를 수행해야 합니다.

  관리 노드를 사용하여 S3 및 Swift 클라이언트 트래픽의 로드 밸런싱을 수행할 수도 있습니다.

- * 스토리지 노드 * 는 오브젝트 데이터와 메타데이터를 관리하고 저장합니다. 각 StorageGRID 시스템에는 3개 이상의 스토리지 노드가 있어야 합니다. 여러 사이트가 있는 경우 StorageGRID 시스템 내의 각 사이트에도 3개의 스토리지 노드가 있어야 합니다.
- * 게이트웨이 노드(선택 사항) * 클라이언트 응용 프로그램이 StorageGRID에 연결하는 데 사용할 수 있는 로드 밸런싱 인터페이스를 제공합니다. 로드 밸런서는 클라이언트를 최적의 스토리지 노드로 원활하게 전달하여 노드 장애나 전체 사이트에 대한 투명성이 확보되도록 합니다. 로드 밸런싱에 게이트웨이 노드와 관리 노드 조합을 사용하거나 타사 HTTP 로드 밸런서를 구현할 수 있습니다.
- * 아카이브 노드(선택 사항) * 는 오브젝트 데이터를 테이프에 아카이빙할 수 있는 인터페이스를 제공합니다.

자세한 내용은 을 참조하십시오 StorageGRID 관리.

소프트웨어 기반 노드

소프트웨어 기반 그리드 노드는 다음과 같은 방법으로 구축할 수 있습니다.

- VMware vSphere에서 VM(가상 머신)으로 사용됩니다
- Linux 호스트의 컨테이너 엔진 내 지원되는 운영 체제는 다음과 같습니다.
  - Red Hat Enterprise Linux
  - CentOS
  - 우분투
  - 데비안

자세한 내용은 다음을 참조하십시오.

- VMware를 설치합니다
- Red Hat Enterprise Linux 또는 CentOS를 설치합니다
- Ubuntu 또는 Debian을 설치합니다

를 사용합니다 "NetApp 상호 운용성 매트릭스 툴" 를 클릭하여 지원되는 버전 목록을 가져옵니다.

StorageGRID 어플라이언스 노드

StorageGRID 하드웨어 어플라이언스는 StorageGRID 시스템에서 사용하도록 특별히 설계되었습니다. 일부 어플라이언스는 스토리지 노드로 사용할 수 있습니다. 다른 어플라이언스를 관리 노드 또는 게이트웨이 노드로 사용할 수 있습니다. 어플라이언스 노드를 소프트웨어 기반 노드와 결합하거나, 외부 하이퍼바이저, 스토리지 또는 컴퓨팅 하드웨어에 종속되지 않는 완전히 엔지니어링된 모든 어플라이언스 그리드를 구축할 수 있습니다.

다음과 같은 네 가지 유형의 StorageGRID 어플라이언스를 사용할 수 있습니다.

- SG100 및 SG1000 서비스 어플라이언스 * 는 각각 기본 관리 노드, 비기본 관리 노드 또는 게이트웨이 노드로 작동할 수 있는 1랙 유닛(1U) 서버입니다. 두 어플라이언스 모두 게이트웨이 노드와 관리 노드(운영 및 비운영)로 동시에 작동할 수 있습니다.
- SG6000 스토리지 어플라이언스 * 는 스토리지 노드로 작동하며 1U SG6000-CN 컴퓨팅 컨트롤러를 2U 또는 4U 스토리지 컨트롤러 쉘프와 결합합니다. SG6000은 다음 세 가지 모델로 제공됩니다.
  - * SGF6024 *: SG6000-CN 컴퓨팅 컨트롤러를 24개의 SSD(Solid State Drive) 및 이중 스토리지 컨트롤러가 포함된 2U 스토리지 컨트롤러 쉘프와 결합합니다.
  - * SG6060 및 SG6060X *: SG6000-CN 컴퓨팅 컨트롤러를 58개의 NL-SAS 드라이브, 2개의 SSD 및 중복 스토리지 컨트롤러가 포함된 4U 엔클로저와 결합합니다. SG6060 및 SG6060X는 각각 60-드라이브 확장 쉘프를 1개 또는 2개 지원하므로 오브젝트 스토리지 전용 드라이브를 최대 178개까지 제공할 수 있습니다.
- SG5700 스토리지 어플라이언스 * 는 스토리지 노드로 작동하는 통합 스토리지 및 컴퓨팅 플랫폼입니다. SG5700은 4가지 모델로 제공됩니다.
  - * SG5712 및 SG5712X *: 12개의 NL-SAS 드라이브와 통합 스토리지 및 컴퓨팅 컨트롤러가 포함된 2U 엔클로저
  - * SG5760 및 SG5760X *: 4U 엔클로저로, NL-SAS 드라이브 60개, 통합 스토리지 및 컴퓨팅 컨트롤러 포함.
- SG5600 스토리지 어플라이언스 * 는 스토리지 노드로 작동하는 통합 스토리지 및 컴퓨팅 플랫폼입니다. SG5600은 다음 두 가지 모델로 사용할 수 있습니다.
  - * SG5612 *: 12개의 NL-SAS 드라이브와 통합 스토리지 및 컴퓨팅 컨트롤러를 포함하는 2U 엔클로저
  - * SG5660 *: 60개의 NL-SAS 드라이브와 통합 스토리지 및 컴퓨팅 컨트롤러를 포함하는 4U 엔클로저

자세한 내용은 다음을 참조하십시오.

- "NetApp Hardware Universe를 참조하십시오"
- SG100 및 SG1000 서비스 어플라이언스
- SG6000 스토리지 어플라이언스
- SG5700 스토리지 어플라이언스
- SG5600 스토리지 어플라이언스

관리 노드에 대한 기본 서비스

다음 표에서는 관리 노드의 기본 서비스를 보여 줍니다. 그러나 이 테이블에는 모든 노드 서비스가 나열되지는 않습니다.

서비스	키 기능
AMS(감사 관리 시스템)	시스템 활동을 추적합니다.
구성 관리 노드(CMN)	시스템 전체 구성을 관리합니다. 기본 관리자 노드만.
관리 애플리케이션 프로그램 인터페이스(관리 API)	Grid Management API 및 Tenant Management API의 요청을 처리합니다.
고가용성	관리 노드 및 게이트웨이 노드 그룹의 고가용성 가상 IP 주소를 관리합니다. • 참고: * 이 서비스는 게이트웨이 노드에서도 찾을 수 있습니다.

서비스	키 기능
로드 밸런서	클라이언트에서 스토리지 노드로 S3 및 Swift 트래픽의 로드 밸런싱을 제공합니다. • 참고: * 이 서비스는 게이트웨이 노드에서도 찾을 수 있습니다.
네트워크 관리 시스템(NMS)	그리드 관리자를 위한 기능을 제공합니다.
프로메테우스	메트릭을 수집 및 저장합니다.
서버 상태 모니터(SSM)	운영 체제 및 기본 하드웨어를 모니터링합니다.

스토리지 노드의 기본 서비스

다음 표에는 스토리지 노드의 기본 서비스가 나와 있지만 이 표에는 모든 노드 서비스가 나와 있지 않습니다.

ADC 서비스 및 RSM 서비스와 같은 일부 서비스는 일반적으로 각 사이트의 세 스토리지 노드에만 존재합니다.

서비스	키 기능
계정(acct)	테넌트 계정을 관리합니다.
관리 도메인 컨트롤러(ADC)	토폴로지 및 그리드 전체의 구성 유지
Cassandra 를 클릭합니다	오브젝트 메타데이터를 저장하고 보호합니다.
Cassandra Refaper(Cassandra 성형기)	오브젝트 메타데이터를 자동으로 복구합니다.
청크	삭제 코딩 데이터 및 패리티 조각을 관리합니다.
Data Mover(DMV)	데이터를 클라우드 스토리지 풀로 이동합니다.
DDS(분산 데이터 저장소)	오브젝트 메타데이터 스토리지를 모니터링합니다.
ID(idnt)	LDAP 및 Active Directory에서 사용자 ID를 페더레이션합니다.
LDR(Local Distribution Router)	오브젝트 스토리지 프로토콜 요청을 처리하고 디스크의 오브젝트 데이터를 관리합니다.
복제된 상태 시스템(RSM)	S3 플랫폼 서비스 요청이 해당 엔드포인트로 전송되도록 합니다.
서버 상태 모니터(SSM)	운영 체제 및 기본 하드웨어를 모니터링합니다.

게이트웨이 노드에 대한 기본 서비스

다음 표에서는 게이트웨이 노드의 기본 서비스를 보여 줍니다. 그러나 이 테이블에는 모든 노드 서비스가 나열되지는 않습니다.

서비스	키 기능
연결 로드 밸런서(CLB)	클라이언트에서 스토리지 노드로 S3 및 Swift 트래픽의 계층 3 및 4 로드 밸런싱을 제공합니다. 레거시 로드 밸런싱 메커니즘 • 참고: * CLB 서비스는 더 이상 사용되지 않습니다.
고가용성	관리 노드 및 게이트웨이 노드 그룹의 고가용성 가상 IP 주소를 관리합니다. • 참고: * 이 서비스는 관리 노드에서도 찾을 수 있습니다.
로드 밸런서	클라이언트에서 스토리지 노드로 S3 및 Swift 트래픽의 계층 7 로드 밸런싱을 제공합니다. 이것은 권장되는 로드 밸런싱 메커니즘입니다. • 참고: * 이 서비스는 관리 노드에서도 찾을 수 있습니다.
서버 상태 모니터(SSM)	운영 체제 및 기본 하드웨어를 모니터링합니다.

아카이브 노드에 대한 기본 서비스

다음 표에는 아카이브 노드의 기본 서비스가 나와 있지만 이 표에는 모든 노드 서비스가 나열되어 있지 않습니다.

서비스	키 기능
아카이브(ARC)	TSM(Tivoli Storage Manager) 외부 테이프 스토리지 시스템과 통신합니다.
서버 상태 모니터(SSM)	운영 체제 및 기본 하드웨어를 모니터링합니다.

StorageGRID 서비스

다음은 StorageGRID 서비스의 전체 목록입니다.

- * 계정 서비스 전달자*

  로드 밸런서 서비스가 원격 호스트에서 계정 서비스를 쿼리하도록 하는 인터페이스를 제공하고 로드 밸런서 끝점 구성 변경 사항을 로드 밸런서 서비스에 알려 줍니다. 로드 밸런서 서비스는 관리 노드 및 게이트웨이 노드에 있습니다.

- * ADC 서비스(관리 도메인 컨트롤러) *

  LDR 및 CMN 서비스의 토폴로지 정보 유지, 인증 서비스 제공 및 쿼리에 응답 ADC 서비스는 사이트에 설치된 처음 세 개의 스토리지 노드 각각에 제공됩니다.

- * AMS 서비스(감사 관리 시스템) *

감사된 모든 시스템 이벤트 및 트랜잭션을 모니터링하고 텍스트 로그 파일에 기록합니다. AMS 서비스가 관리 노드에 있습니다.

- * ARC 서비스(보관) *

  TSM 미들웨어를 통해 S3 인터페이스 또는 테이프를 통해 클라우드와 같은 외부 아카이브 스토리지에 대한 연결을 구성하는 관리 인터페이스를 제공합니다. ARC 서비스는 아카이브 노드에 있습니다.

- * Cassandra Refaper 서비스 *

  오브젝트 메타데이터를 자동으로 복구합니다. Cassandra Refaper 서비스는 모든 스토리지 노드에 있습니다.

- * 청크 서비스 *

  삭제 코딩 데이터 및 패리티 조각을 관리합니다. 스토리지 노드에 청크 서비스가 있습니다.

- * CLB 서비스(연결 로드 밸런서) *

  HTTP를 통해 연결하는 클라이언트 응용 프로그램에 대한 게이트웨이를 StorageGRID에 제공하는 더 이상 사용되지 않는 서비스입니다. CLB 서비스가 게이트웨이 노드에 있습니다. CLB 서비스는 더 이상 사용되지 않으며 향후 StorageGRID 릴리스에서 제거됩니다.

- * CMN 서비스(구성 관리 노드) *

  시스템 전체 구성 및 그리드 작업 관리 각 그리드에는 기본 관리 노드에 있는 하나의 CMN 서비스가 있습니다.

- * DDS 서비스(분산 데이터 저장소) *

  Cassandra 데이터베이스와 연결되어 개체 메타데이터를 관리합니다. DDS 서비스는 스토리지 노드에 있습니다.

- * DMV 서비스(Data Mover) *

  데이터를 클라우드 엔드포인트로 이동합니다. DMV 서비스가 스토리지 노드에 있습니다.

- * 동적 IP 서비스 *

  그리드를 모니터링하여 동적 IP 변경 사항을 모니터링하고 로컬 구성을 업데이트합니다. 동적 IP(dynip) 서비스가 모든 노드에 존재합니다.

- * Grafana 서비스 *

  Grid Manager에서 메트릭 시각화에 사용됩니다. Grafana 서비스가 관리 노드에 존재합니다.

- * 고가용성 서비스 *

  High Availability Groups 페이지에 구성된 노드의 고가용성 가상 IP를 관리합니다. 고가용성 서비스는 관리 노드 및 게이트웨이 노드에 있습니다. 이 서비스는 Keeepalived 서비스라고도 합니다.

- * ID(idnt) 서비스 *

  LDAP 및 Active Directory에서 사용자 ID를 페더레이션합니다. ID 서비스(idnt)는 각 사이트의 세 스토리지 노드에 있습니다.

- * 람다 중재인 서비스 *

  S3 Select SelectObjectContent 요청을 관리합니다.

- * 로드 밸런서 서비스 *

  클라이언트에서 스토리지 노드로 S3 및 Swift 트래픽의 로드 밸런싱을 제공합니다. 부하 분산 서비스는 부하 분산 엔드포인트 구성 페이지를 통해 구성할 수 있습니다. 로드 밸런서 서비스는 관리 노드 및 게이트웨이 노드에 있습니다. 이 서비스는 nginx-GW 서비스라고도 합니다.

- * LDR 서비스(Local Distribution Router) *

  그리드 내의 컨텐츠 저장 및 전송을 관리합니다. LDR 서비스가 스토리지 노드에 있습니다.

- * MISCd 정보 서비스 제어 데몬 서비스 *

  다른 노드의 서비스를 쿼리 및 관리하고 다른 노드에서 실행 중인 서비스 상태를 쿼리하는 것과 같은 노드의 환경 구성을 관리하기 위한 인터페이스를 제공합니다. MISCd 서비스가 모든 노드에 있습니다.

- * nginx 서비스 *

  HTTPS API를 통해 다른 노드의 서비스와 통신할 수 있도록 다양한 그리드 서비스(예: Prometheus 및 Dynamic IP)를 위한 인증 및 보안 통신 메커니즘 역할을 합니다. nginx 서비스는 모든 노드에 있습니다.

- * nginx-GW 서비스 *

  로드 밸런서 서비스에 전원을 공급합니다. Nginx-GW 서비스는 관리 노드 및 게이트웨이 노드에 있습니다.

- * NMS 서비스(네트워크 관리 시스템) *

  Grid Manager를 통해 표시되는 모니터링, 보고 및 구성 옵션을 강화합니다. NMS 서비스가 관리 노드에 있습니다.

- * 지속성 서비스 *

  재부팅 시 유지되어야 하는 루트 디스크의 파일을 관리합니다. Persistence 서비스는 모든 노드에 있습니다.

- * Prometheus 서비스 *

  모든 노드의 서비스에서 시계열 메트릭을 수집합니다. Prometheus 서비스는 관리 노드에 있습니다.

- RSM 서비스(복제된 상태 기계 서비스) *

  플랫폼 서비스 요청이 각 엔드포인트로 전송되도록 합니다. RSM 서비스는 ADC 서비스를 사용하는 스토리지 노드에 있습니다.

- * SSM 서비스(서버 상태 모니터) *

  하드웨어 조건을 모니터링하고 NMS 서비스에 보고합니다. SSM 서비스의 인스턴스는 모든 그리드 노드에 존재합니다.

- * 추적 수집기 서비스 *

  기술 지원 부서에서 사용할 정보를 수집하기 위해 추적 수집을 수행합니다. 추적 수집기 서비스는 오픈 소스 Jaeger

소프트웨어를 사용하며 관리 노드에 있습니다.

오브젝트 관리

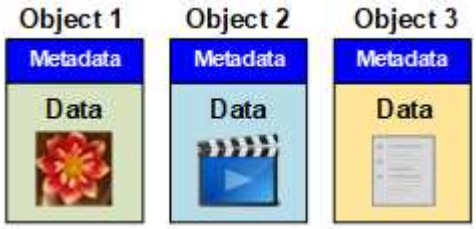
StorageGRID의 데이터 관리 방법

StorageGRID 시스템으로 작업을 시작할 때 StorageGRID 시스템에서 데이터를 관리하는 방법을 이해하는 것이 좋습니다.

개체의 정의

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.



오브젝트 데이터

오브젝트 데이터는 사진, 동영상 또는 의료 기록 등의 무엇이든 될 수 있습니다.

오브젝트 메타데이터

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(UUID), 개체 이름, S3 버킷 또는 Swift 컨테이너의 이름, 테넌트 계정 이름 또는 ID, 개체의 논리적 크기, 개체를 처음 만든 날짜 및 시간을 포함한 시스템 메타데이터 및 객체가 마지막으로 수정된 날짜 및 시간입니다.
- 각 오브젝트 복사본 또는 삭제 코딩 조각의 현재 스토리지 위치입니다.
- 오브젝트와 연결된 모든 사용자 메타데이터

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.

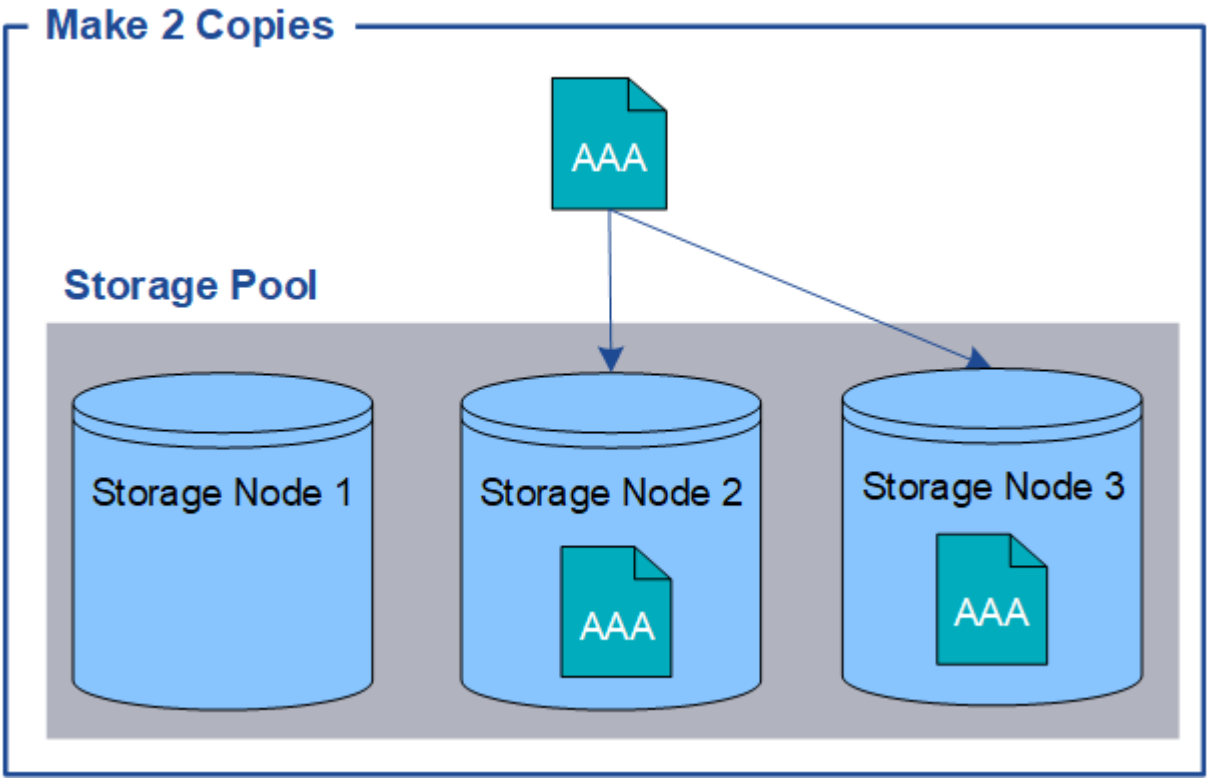
오브젝트 데이터의 보호 방법

StorageGRID 시스템은 오브젝트 데이터의 손실로부터 보호하기 위한 복제 및 삭제 코딩의 두 가지 메커니즘을 제공합니다.

복제

StorageGRID가 복제된 복사본을 만들도록 구성된 ILM(정보 수명 주기 관리) 규칙에 개체를 일치하면 시스템에서 정확한 오브젝트 데이터 복사본을 생성하고 스토리지 노드, 아카이브 노드 또는 클라우드 스토리지 풀에 저장합니다. ILM 규칙에 따라 생성된 복사본 수, 복사본이 저장되는 위치 및 시스템에 의해 복사본 보관되는 시간이 결정됩니다. 예를 들어, 스토리지 노드의 손실로 인해 복제본이 손실되어도 StorageGRID 시스템의 다른 위치에 복제본을 생성할 경우 객체를 계속 사용할 수 있습니다.

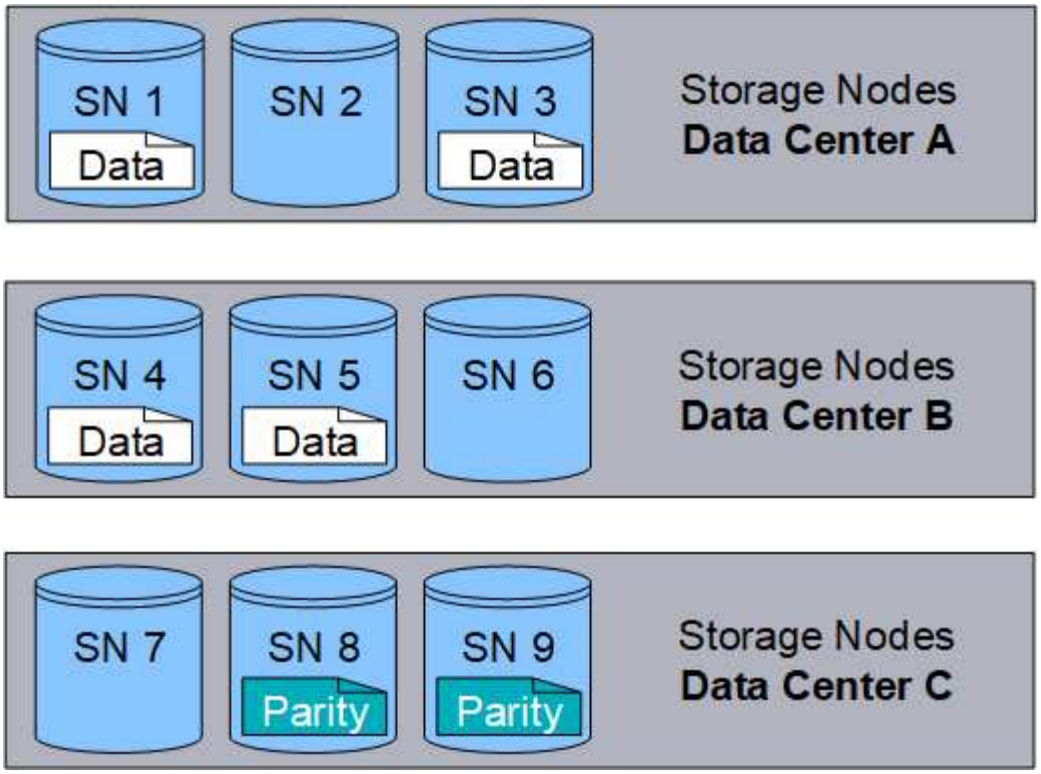
다음 예에서는 복제본 2개 만들기 규칙에 따라 각 객체의 복제된 복제본 2개가 스토리지 노드 3개가 포함된 스토리지 풀에 배치되도록 지정합니다.



삭제 코딩

StorageGRID가 오브젝트를 삭제 코딩 복사본을 만들도록 구성된 ILM 규칙과 일치시키는 경우 오브젝트 데이터를 데이터 조각으로 슬라이스하고, 추가 패리티 조각을 계산하고, 각 조각을 다른 스토리지 노드에 저장합니다. 개체에 액세스하면 저장된 조각을 사용하여 다시 조립됩니다. 데이터 또는 패리티 조각이 손상되거나 손실될 경우 삭제 코딩 알고리즘이 나머지 데이터 및 패리티 조각의 일부를 사용하여 해당 조각을 다시 생성할 수 있습니다. ILM 규칙 및 삭제 코딩 프로필은 사용된 삭제 코딩 스키마를 결정합니다.

다음 예제에서는 오브젝트의 데이터에서 삭제 코딩을 사용하는 방법을 보여 줍니다. 이 예제에서 ILM 규칙은 4+2 삭제 코딩 체계를 사용합니다. 각 개체는 4개의 동일한 데이터 조각으로 분할되며 두 개의 패리티 조각은 개체 데이터에서 계산됩니다. 6개의 각 조각은 3개의 데이터 센터 전반에 걸쳐 서로 다른 스토리지 노드에 저장되어 노드 장애 또는 사이트 손실에 대한 데이터 보호 기능을 제공합니다.



관련 정보

- ILM을 사용하여 개체를 관리합니다
- 정보 수명 주기 관리를 사용합니다

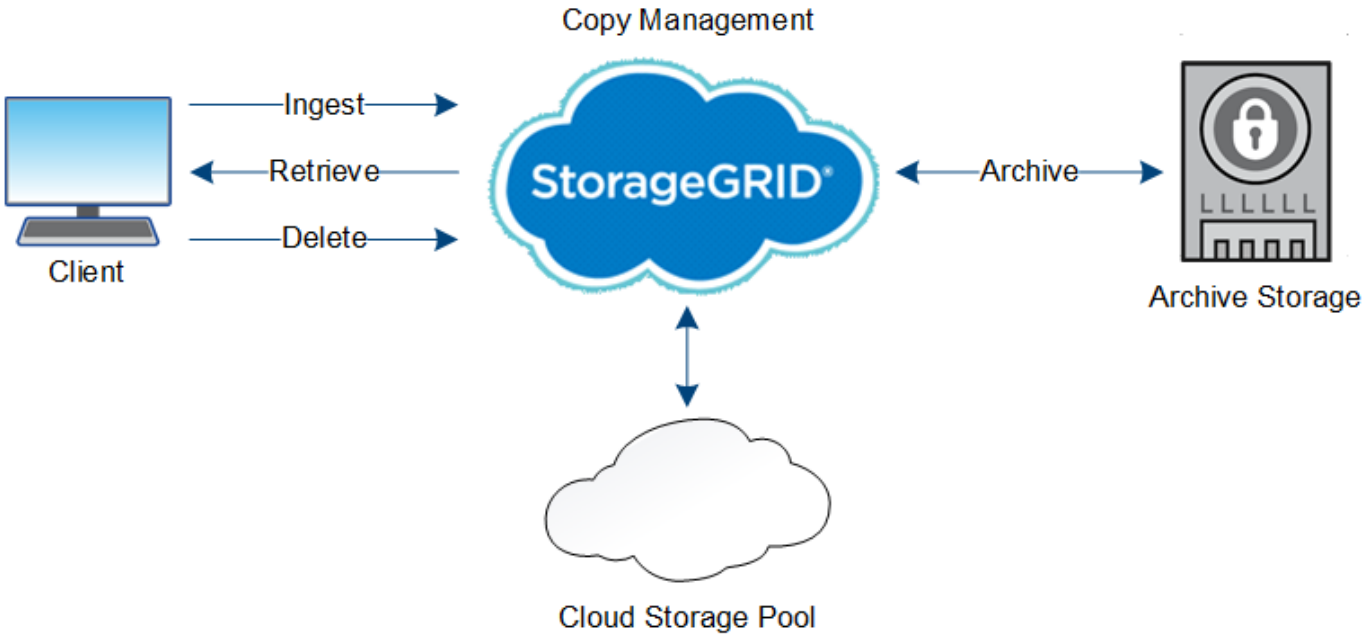
오브젝트 라이프사이클

개체의 수명입니다

개체의 수명은 다양한 단계로 구성됩니다. 각 단계는 객체와 함께 발생하는 작업을 나타냅니다.

오브젝트의 수명에는 수집, 복사본 관리, 검색 및 삭제 작업이 포함됩니다.

- * Ingest *: HTTP를 통해 개체를 StorageGRID 시스템에 저장하는 S3 또는 Swift 클라이언트 응용 프로그램의 프로세스입니다. 이 단계에서 StorageGRID 시스템이 객체를 관리하기 시작합니다.
- * 복사본 관리 *: 활성 ILM 정책의 ILM 규칙에 따라 StorageGRID에서 복제되고 삭제 코딩 복사본을 관리하는 프로세스입니다. 복사 관리 단계에서 StorageGRID는 스토리지 노드, 클라우드 스토리지 풀 또는 아카이브 노드에서 지정된 수의 오브젝트 복사본 및 유형을 생성하고 유지함으로써 오브젝트 데이터 손실을 방지합니다.
- * 검색 *: StorageGRID 시스템에 저장된 개체에 액세스하는 클라이언트 응용 프로그램의 프로세스입니다. 클라이언트는 스토리지 노드, 클라우드 스토리지 풀 또는 아카이브 노드에서 검색된 객체를 읽습니다.
- * 삭제 *: 모눈에서 모든 개체 복사본을 제거하는 프로세스입니다. StorageGRID 시스템에 삭제 요청을 보낸 클라이언트 응용 프로그램의 결과나 개체의 수명이 만료될 때 StorageGRID가 수행하는 자동 프로세스의 결과로 개체를 삭제할 수 있습니다.



관련 정보

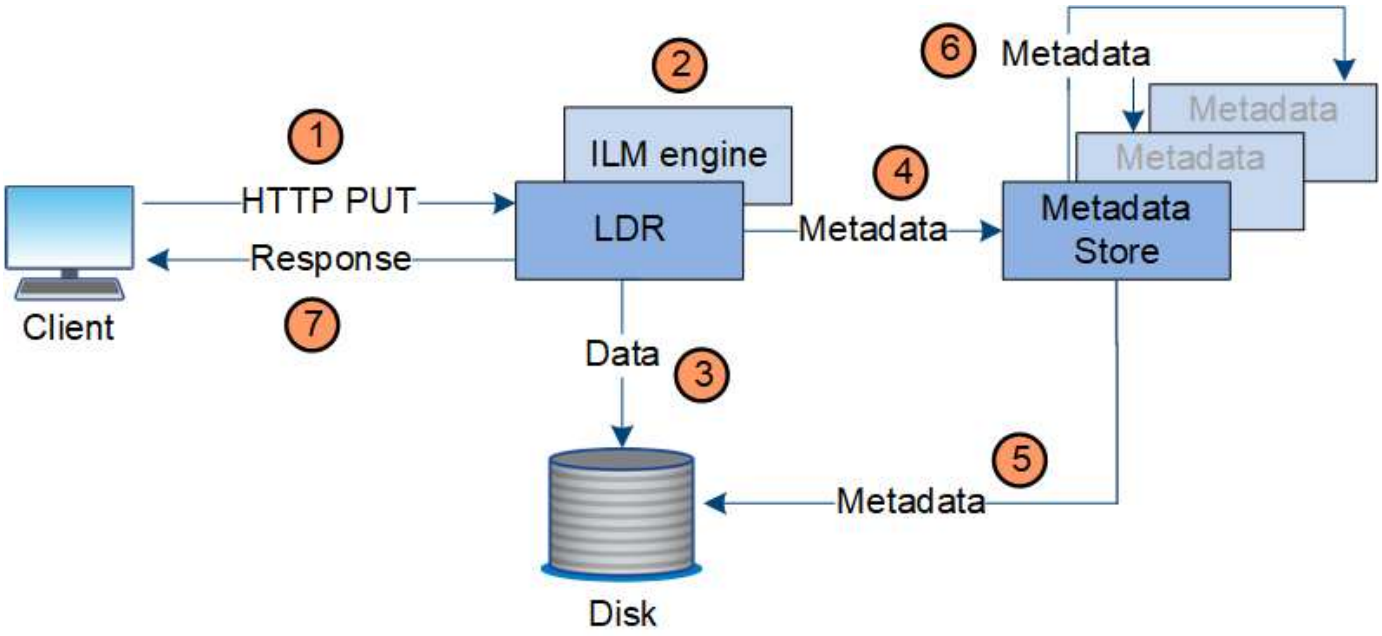
- ILM을 사용하여 개체를 관리합니다
- 정보 수명 주기 관리를 사용합니다

수집 데이터 흐름

수집 또는 저장 작업은 클라이언트와 StorageGRID 시스템 간에 정의된 데이터 흐름으로 구성됩니다.

데이터 흐름

클라이언트가 StorageGRID 시스템에 개체를 요청하면 스토리지 노드의 LDR 서비스가 요청을 처리하고 메타데이터 및 데이터를 디스크에 저장합니다.



1. 클라이언트 응용 프로그램은 개체를 만들어 HTTP PUT 요청을 통해 StorageGRID 시스템으로 보냅니다.
2. 객체는 시스템의 ILM 정책에 따라 평가됩니다.
3. LDR 서비스는 오브젝트 데이터를 복제된 복사본 또는 삭제 코딩 복사본으로 저장합니다. (이 다이어그램은 복제된 복사본을 디스크에 저장하는 간단한 버전을 보여 줍니다.)
4. LDR 서비스는 개체 메타데이터를 메타데이터 저장소로 보냅니다.
5. 메타데이터 저장소는 객체 메타데이터를 디스크에 저장합니다.
6. 메타데이터 저장소가 객체 메타데이터의 복제본을 다른 스토리지 노드로 전파합니다. 이러한 사본은 디스크에도 저장됩니다.
7. LDR 서비스는 개체가 수집되었음을 확인할 수 있도록 클라이언트에 대한 HTTP 200 OK 응답을 반환합니다.

복사 관리

개체 데이터는 활성 ILM 정책 및 해당 ILM 규칙에 의해 관리됩니다. ILM 규칙은 복제 또는 삭제 코딩 복사본을 만들어 오브젝트 데이터의 손실로부터 보호합니다.

오브젝트 복사본의 다양한 유형 또는 위치는 오브젝트의 수명 동안 서로 다른 시간에 필요할 수 있습니다. ILM 규칙은 주기적으로 평가하여 개체가 필요에 따라 배치되도록 합니다.

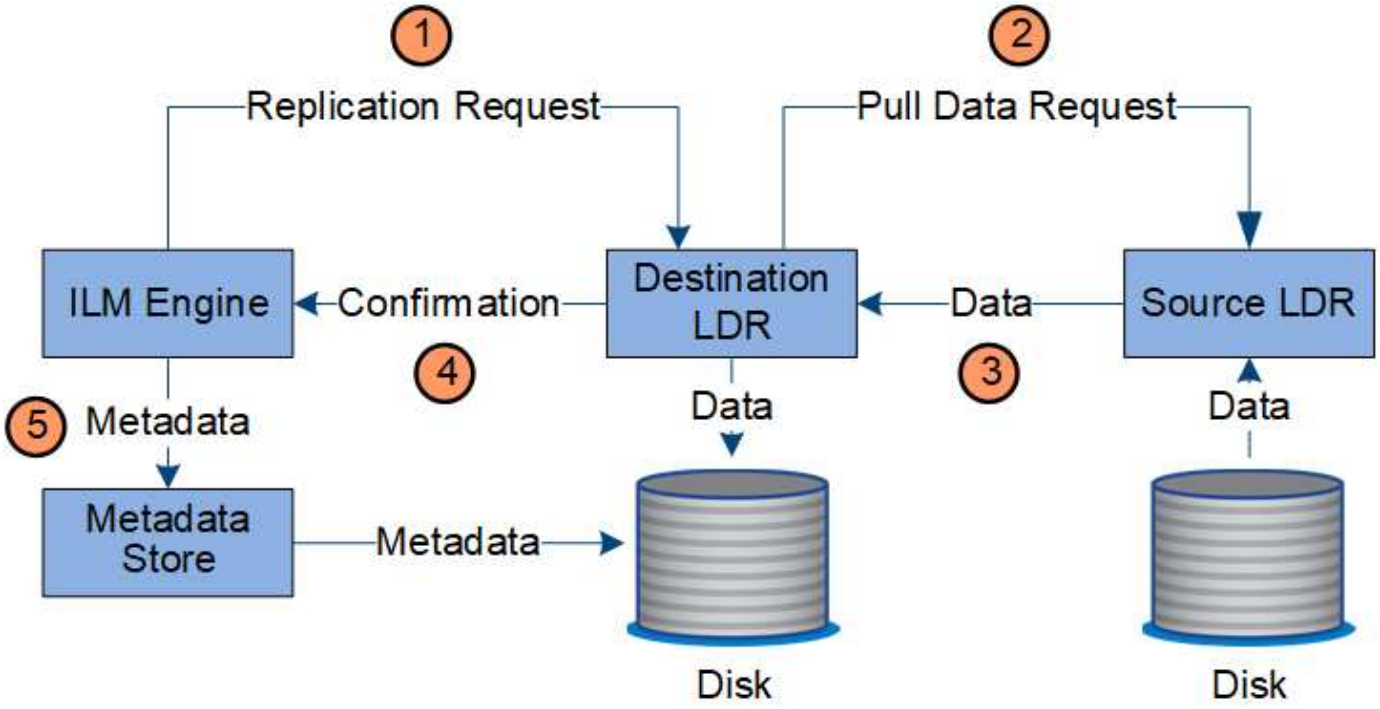
개체 데이터는 LDR 서비스에서 관리합니다.

컨텐츠 보호**:** 복제

ILM 규칙의 콘텐츠 배치 지침에 따라 오브젝트 데이터의 복제된 복사본이 필요한 경우 복사본은 구성된 스토리지 풀을 구성하는 스토리지 노드에 의해 만들어지면 디스크에 저장됩니다.

데이터 흐름

LDR 서비스의 ILM 엔진은 복제를 제어하고 올바른 위치에 올바른 복제본 수를 올바른 시간 동안 저장합니다.



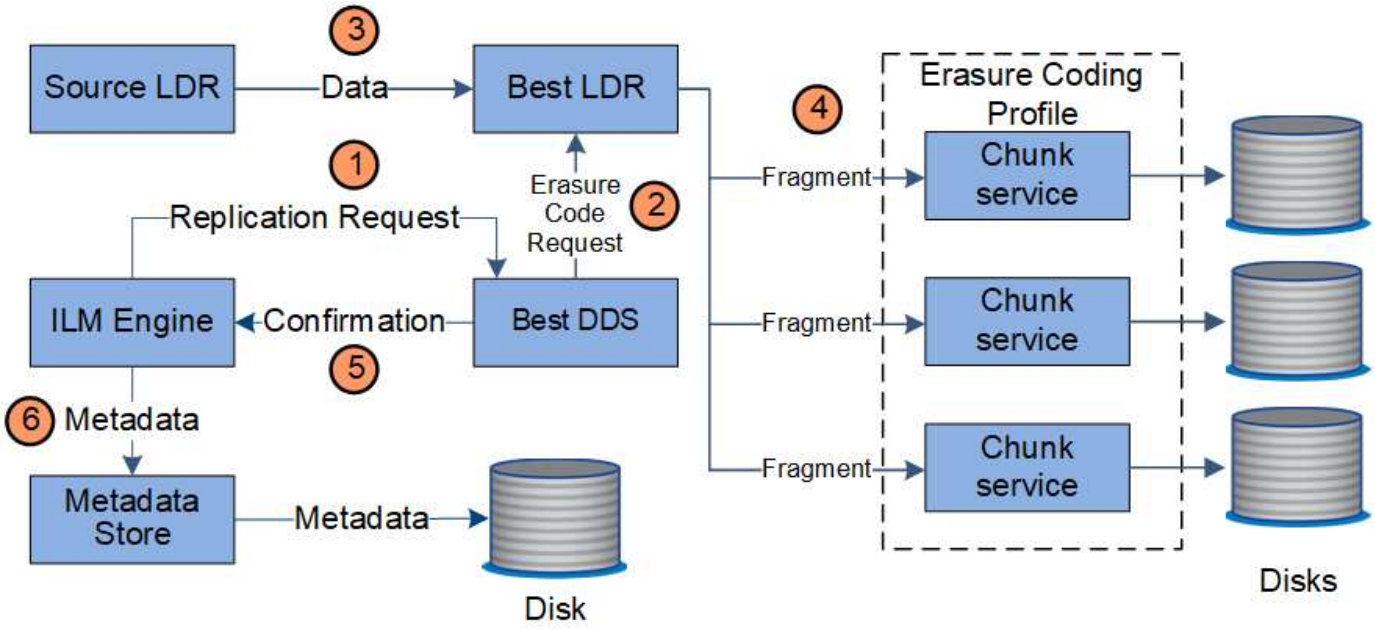
1. ILM 엔진은 ADC 서비스를 쿼리하여 ILM 규칙에 지정된 스토리지 풀 내에서 최상의 대상 LDR 서비스를 결정합니다. 그런 다음 LDR 서비스에 복제를 시작하는 명령을 보냅니다.
2. 대상 LDR 서비스는 ADC 서비스에 최상의 소스 위치를 쿼리합니다. 그런 다음 복제 요청을 소스 LDR 서비스로 보냅니다.
3. 소스 LDR 서비스는 대상 LDR 서비스에 복사본을 보냅니다.
4. 대상 LDR 서비스는 ILM 엔진에 개체 데이터가 저장되었음을 알립니다.
5. ILM 엔진은 메타데이터 저장소를 개체 위치 메타데이터로 업데이트합니다.

콘텐츠 보호: 삭제 코딩

ILM 규칙에 오브젝트 데이터의 삭제 코딩 복사본을 만드는 지침이 포함된 경우 해당 삭제 코딩 스키마를 통해 오브젝트 데이터를 데이터 및 패리티 조각으로 나누어 삭제 코딩 프로필에 구성된 스토리지 노드에 분산합니다.

데이터 흐름

LDR 서비스의 구성 요소인 ILM 엔진은 삭제 코딩을 제어하고 삭제 코딩 프로필이 오브젝트 데이터에 적용되도록 합니다.



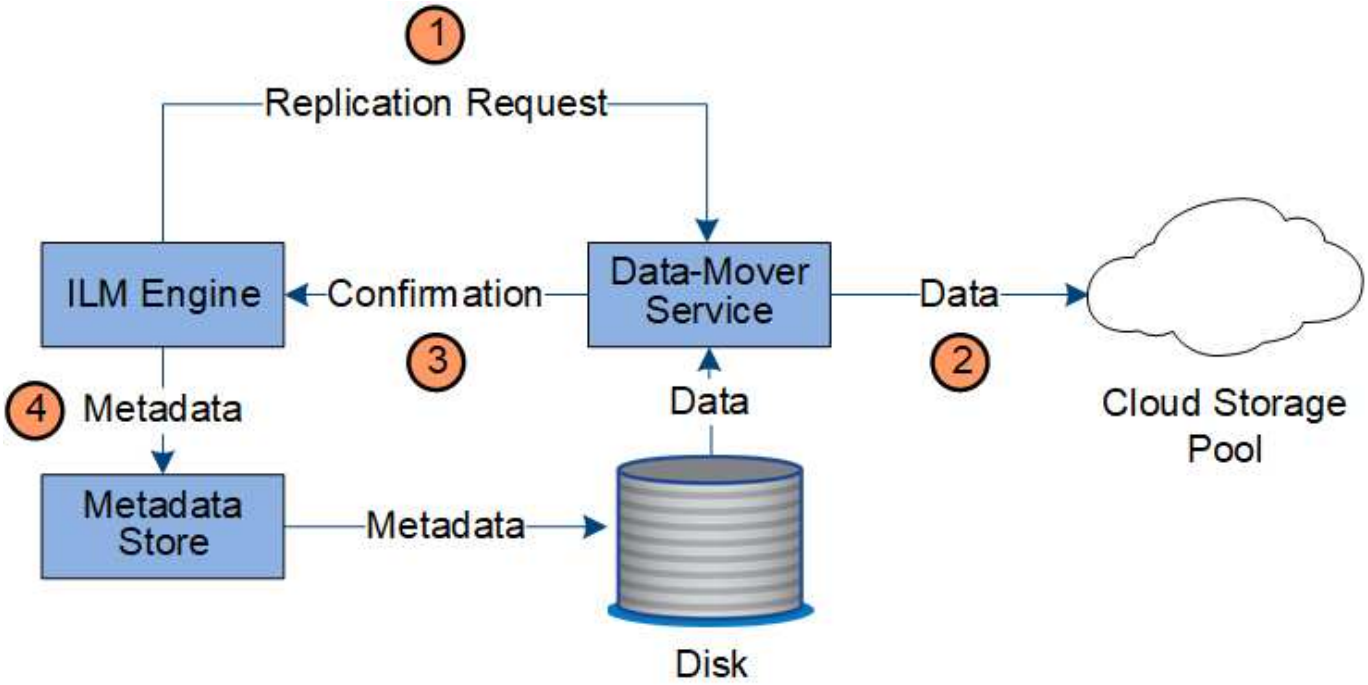
1. ILM 엔진은 ADC 서비스에 쿼리하여 삭제 코딩 작업을 가장 잘 수행할 수 있는 DDS 서비스를 결정합니다. ILM 엔진이 결정되면 해당 서비스에 "시작" 요청을 보냅니다.
2. DDS 서비스는 LDR에 오브젝트 데이터를 삭제 코딩하도록 지시합니다.
3. 소스 LDR 서비스는 삭제 코딩을 위해 선택된 LDR 서비스에 복사본을 보냅니다.
4. 적절한 수의 패리티 및 데이터 조각으로 분할된 LDR 서비스는 이러한 조각을 삭제 코딩 프로필의 스토리지 풀을 구성하는 스토리지 노드(청크 서비스)에 분산합니다.
5. LDR 서비스는 ILM 엔진에 개체 데이터가 성공적으로 배포되었는지 확인하여 이를 알립니다.
6. ILM 엔진은 메타데이터 저장소를 개체 위치 메타데이터로 업데이트합니다.

콘텐츠 보호: 클라우드 스토리지 풀

ILM 규칙의 콘텐츠 배치 명령에 따라 오브젝트 데이터의 복제된 복사본이 Cloud Storage Pool에 저장되어야 하는 경우 오브젝트 데이터는 Cloud Storage Pool에 지정된 외부 S3 버킷 또는 Azure Blob 스토리지 컨테이너에 복제됩니다.

데이터 흐름

LDR 서비스의 구성 요소인 ILM 엔진 및 Data Mover 서비스는 클라우드 스토리지 풀에 대한 객체 이동을 제어합니다.

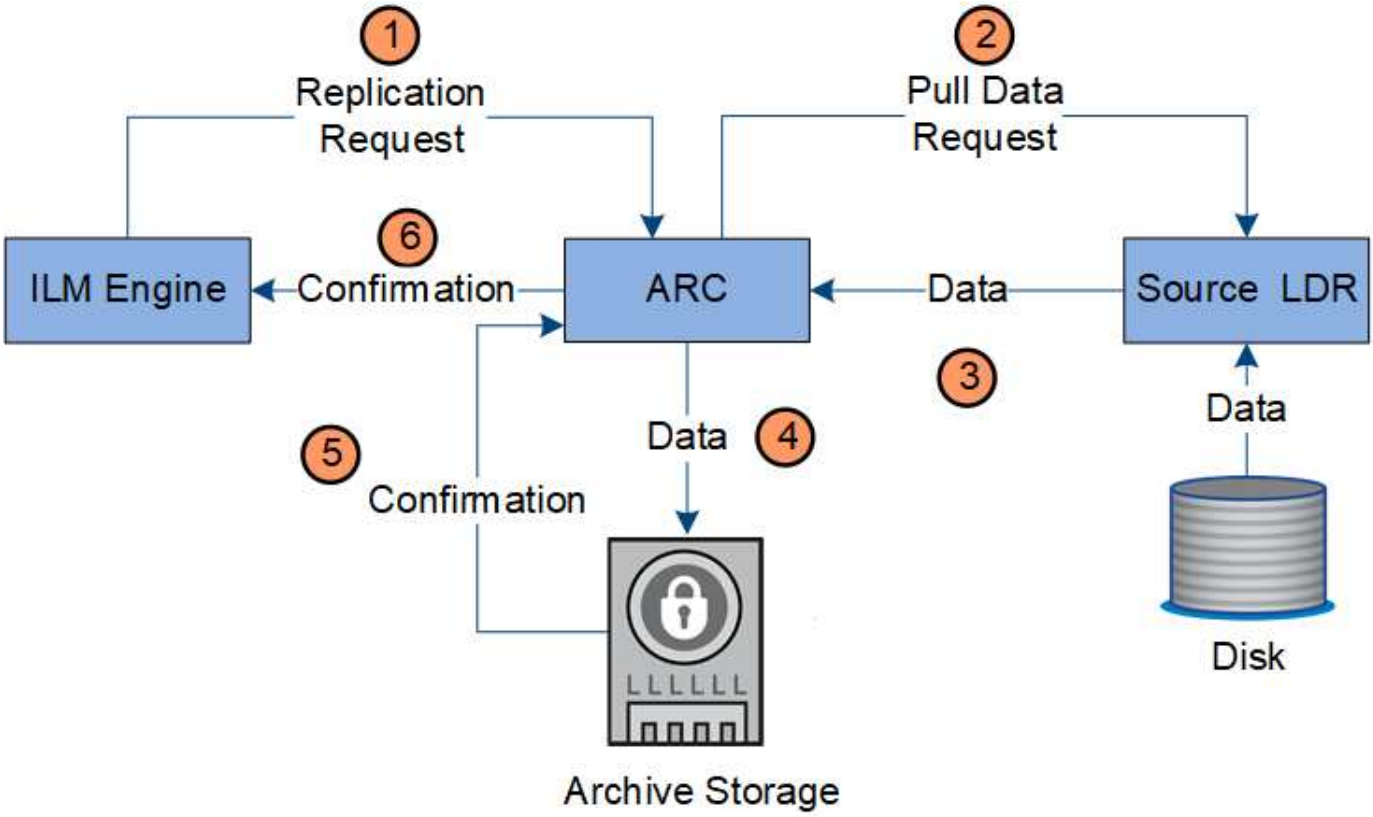


1. ILM 엔진은 Data Mover 서비스를 선택하여 Cloud Storage Pool에 복제합니다.
2. Data Mover 서비스는 객체 데이터를 클라우드 스토리지 풀로 보냅니다.
3. Data Mover 서비스는 ILM 엔진에 개체 데이터가 저장되었음을 알립니다.
4. ILM 엔진은 메타데이터 저장소를 개체 위치 메타데이터로 업데이트합니다.

콘텐츠 보호: 아카이브

아카이브 작업은 StorageGRID 시스템과 클라이언트 간에 정의된 데이터 흐름으로 구성됩니다.

ILM 정책에 따라 오브젝트 데이터 복사본을 보관해야 할 경우 LDR 서비스의 구성 요소인 ILM 엔진이 요청을 아카이브 노드로 전송한 다음, 아카이브 스토리지 시스템으로 오브젝트 데이터 복사본을 보냅니다.



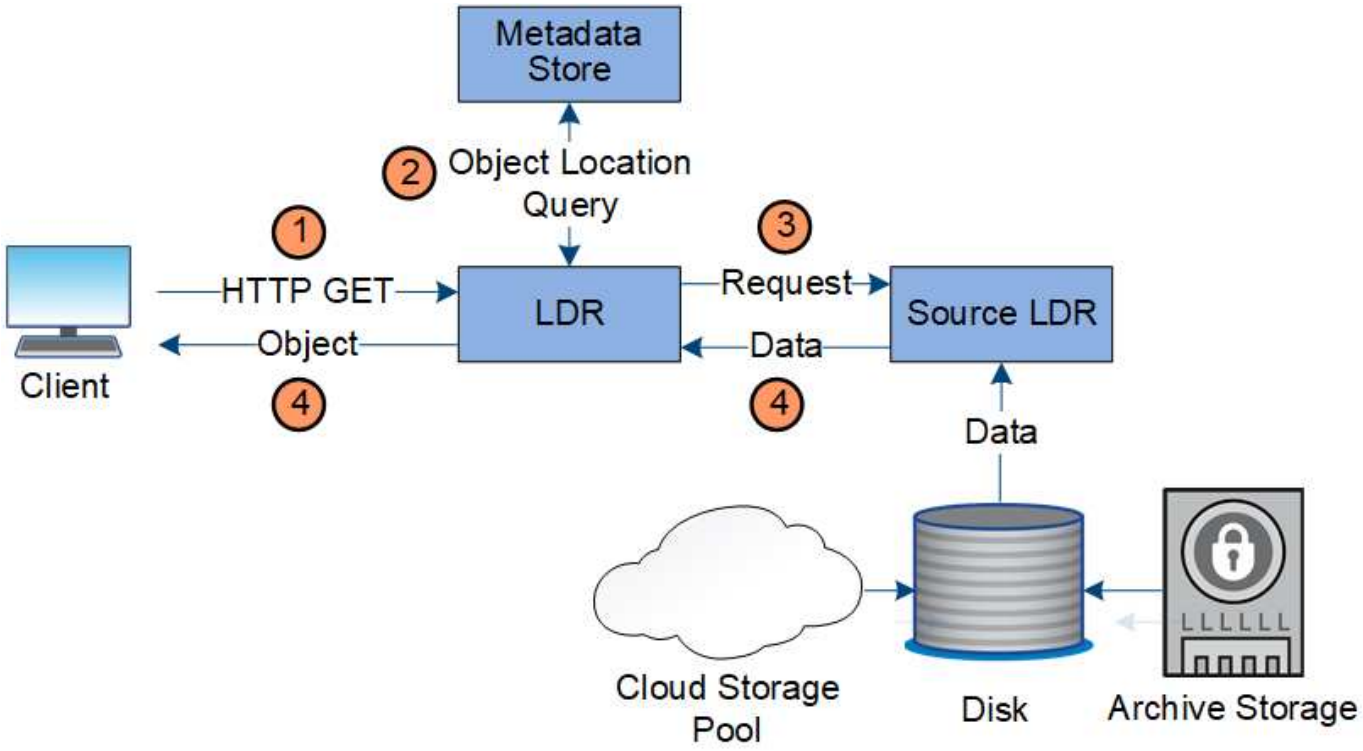
1. ILM 엔진은 ARC 서비스에 아카이브 미디어에 사본을 저장하도록 요청을 보냅니다.
2. ARC 서비스는 최상의 소스 위치에 대한 ADC 서비스를 쿼리하고 소스 LDR 서비스에 요청을 보냅니다.
3. ARC 서비스는 LDR 서비스에서 개체 데이터를 검색합니다.
4. ARC 서비스는 개체 데이터를 보관 매체 대상으로 전송합니다.
5. 아카이브 미디어는 ARC 서비스에 개체 데이터가 저장되었음을 알립니다.
6. ARC 서비스는 ILM 엔진에 개체 데이터가 저장되었음을 알립니다.

데이터 흐름을 검색합니다

검색 작업은 StorageGRID 시스템과 클라이언트 간에 정의된 데이터 흐름으로 구성됩니다. 시스템에서는 특성을 사용하여 스토리지 노드나 필요한 경우 클라우드 스토리지 풀 또는 아카이브 노드에서 객체 검색을 추적합니다.

스토리지 노드의 LDR 서비스는 메타데이터 저장소에서 오브젝트 데이터의 위치를 쿼리하고 소스 LDR 서비스에서 이를 검색합니다. 우선, 검색은 스토리지 노드에서 이루어집니다. 스토리지 노드에서 객체를 사용할 수 없는 경우 검색 요청은 클라우드 스토리지 풀 또는 아카이브 노드로 전달됩니다.

> AWS Glacier 스토리지 또는 Azure Archive 계층에 있는 개체 복사본만 있는 경우 클라이언트 애플리케이션은 S3 POST Object 복원 요청을 발행하여 검색할 수 있는 복사본을 클라우드 스토리지 풀에 복원해야 합니다.



1. LDR 서비스는 클라이언트 응용 프로그램에서 검색 요청을 받습니다.
2. LDR 서비스는 개체 데이터 위치 및 메타데이터에 대한 메타데이터 저장소를 쿼리합니다.
3. LDR 서비스는 검색 요청을 원본 LDR 서비스로 전달합니다.
4. 소스 LDR 서비스는 쿼리된 LDR 서비스의 개체 데이터를 반환하고 시스템은 개체를 클라이언트 응용 프로그램으로 반환합니다.

데이터 흐름을 삭제합니다

클라이언트가 삭제 작업을 수행하거나 개체의 수명이 만료되면 StorageGRID 시스템에서 모든 개체 복사본이 제거되어 자동 제거가 트리거됩니다. 개체 삭제에 대해 정의된 데이터 흐름이 있습니다.

삭제 계층

StorageGRID 개체가 보존되거나 삭제되는 시기를 제어하는 여러 가지 방법을 제공합니다. 객체는 클라이언트 요청에 의해 또는 자동으로 삭제될 수 있습니다. StorageGRID는 항상 S3 오브젝트 잠금 설정의 우선 순위를 클라이언트 삭제 요청보다 우선적으로 지정합니다. 이 요청은 S3 버킷 수명 주기 및 ILM 배치 지침보다 우선적으로 적용됩니다.

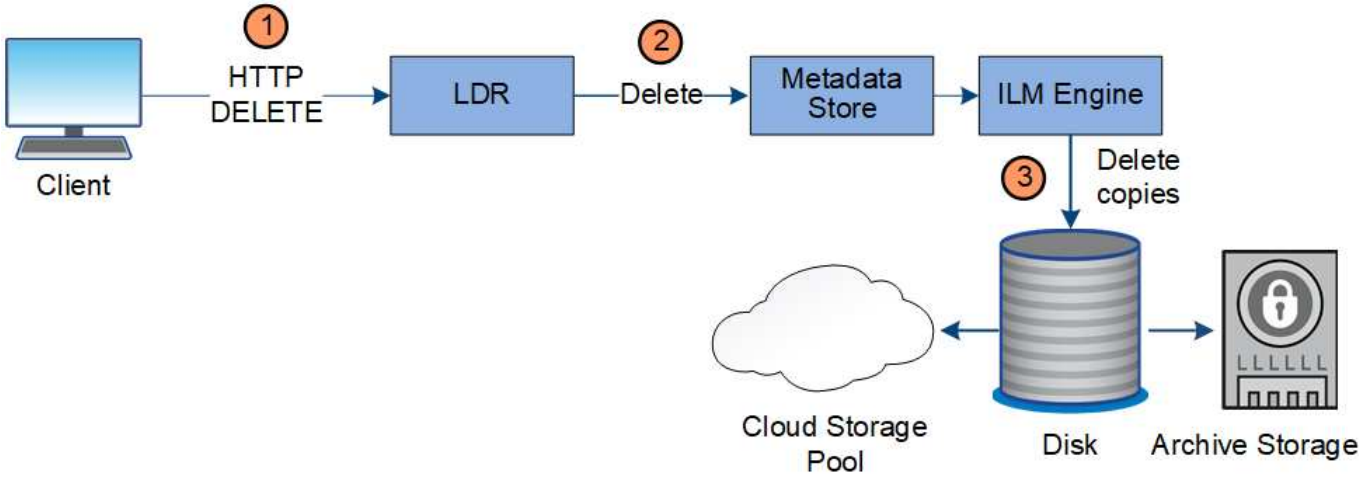
- * S3 오브젝트 잠금 *: 그리드에 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 S3 클라이언트는 S3 오브젝트 잠금이 활성화된 버킷을 생성한 다음 S3 REST API를 사용하여 해당 버킷에 추가된 각 오브젝트 버전에 대한 보관 기한 및 법적 보류 설정을 지정할 수 있습니다.
  - 법적 증거 자료 보관 중인 개체 버전은 어떤 방법으로도 삭제할 수 없습니다.
  - 개체 버전의 보존 기한 에 도달하기 전에 어떤 방법으로도 해당 버전을 삭제할 수 없습니다.
  - S3 오브젝트 잠금이 활성화된 버킷의 오브젝트는 ILM ""영구""에 의해 유지됩니다. 그러나 보존 기한에 도달한 후에는 클라이언트 요청 또는 버킷 라이프사이클의 만료에 의해 오브젝트 버전을 삭제할 수 있습니다.
  - S3 클라이언트가 버킷에 기본 보존 종료 날짜를 적용할 경우 각 오브젝트에 대해 보존 종료 날짜를 지정할

필요가 없습니다.

- * 클라이언트 삭제 요청 *: S3 또는 Swift 클라이언트가 삭제 오브젝트 요청을 실행할 수 있습니다. 클라이언트가 개체를 삭제하면 개체의 모든 복사본이 StorageGRID 시스템에서 제거됩니다.
- * S3 버킷 수명 주기 *: S3 클라이언트는 만료 작업을 지정하는 버킷에 수명 주기 구성을 추가할 수 있습니다. 버킷 라이프사이클이 있는 경우, 클라이언트가 먼저 오브젝트를 삭제하지 않는 한, StorageGRID은 만료 작업에 지정된 날짜 또는 일 수가 충족될 때 오브젝트의 모든 복사본을 자동으로 삭제합니다.
- * ILM 배치 지침 *: 버킷에 S3 오브젝트 잠금이 활성화되어 있지 않고 버킷 라이프사이클이 없다고 가정할 때, StorageGRID은 ILM 규칙의 마지막 기간이 끝나고 해당 오브젝트에 대해 지정된 추가 배치가 없을 때 오브젝트를 자동으로 삭제합니다.

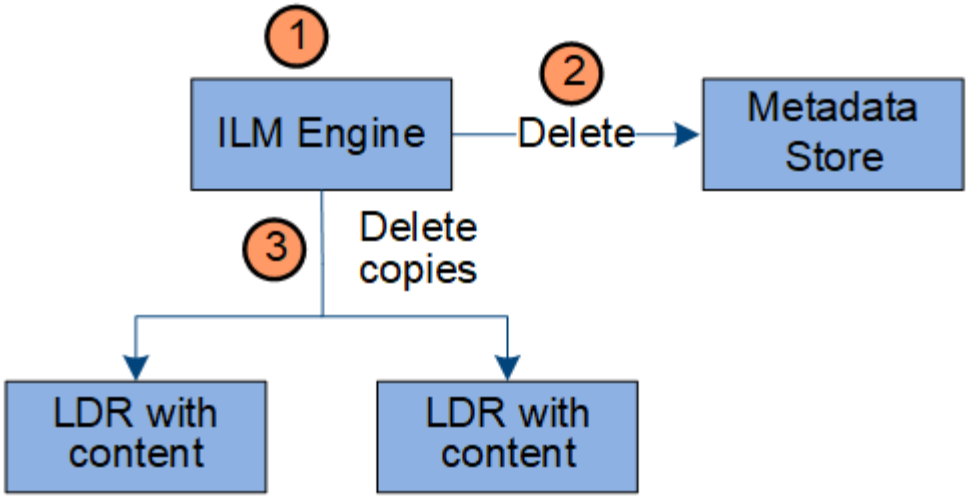
> S3 버킷 라이프사이클의 만료 작업은 항상 ILM 설정을 재정의합니다. 따라서 개체를 배치하기 위한 ILM 명령이 만료된 후에도 개체가 그리드에 유지될 수 있습니다.

클라이언트 삭제에 대한 데이터 흐름



1. LDR 서비스는 클라이언트 응용 프로그램에서 삭제 요청을 받습니다.
2. LDR 서비스는 개체가 클라이언트 요청에 대해 삭제된 것으로 표시되도록 메타데이터 저장소를 업데이트하고 ILM 엔진에 개체 데이터의 모든 복사본을 제거하도록 지시합니다.
3. 객체가 시스템에서 제거됩니다. 메타데이터 저장소가 업데이트되어 개체 메타데이터를 제거합니다.

ILM의 데이터 흐름은 삭제됩니다



1. ILM 엔진이 개체를 삭제해야 한다고 결정합니다.
2. ILM 엔진이 메타데이터 저장소에 알립니다. 메타데이터 저장소는 객체가 클라이언트 요청에 대해 삭제된 것으로 표시되도록 객체 메타데이터를 업데이트합니다.
3. ILM 엔진은 개체의 모든 복사본을 제거합니다. 메타데이터 저장소가 업데이트되어 개체 메타데이터를 제거합니다.

StorageGRID 사용 방법

Grid Manager를 살펴봅니다

그리드 관리자는 StorageGRID 시스템을 구성, 관리 및 모니터링할 수 있는 브라우저 기반 그래픽 인터페이스입니다.

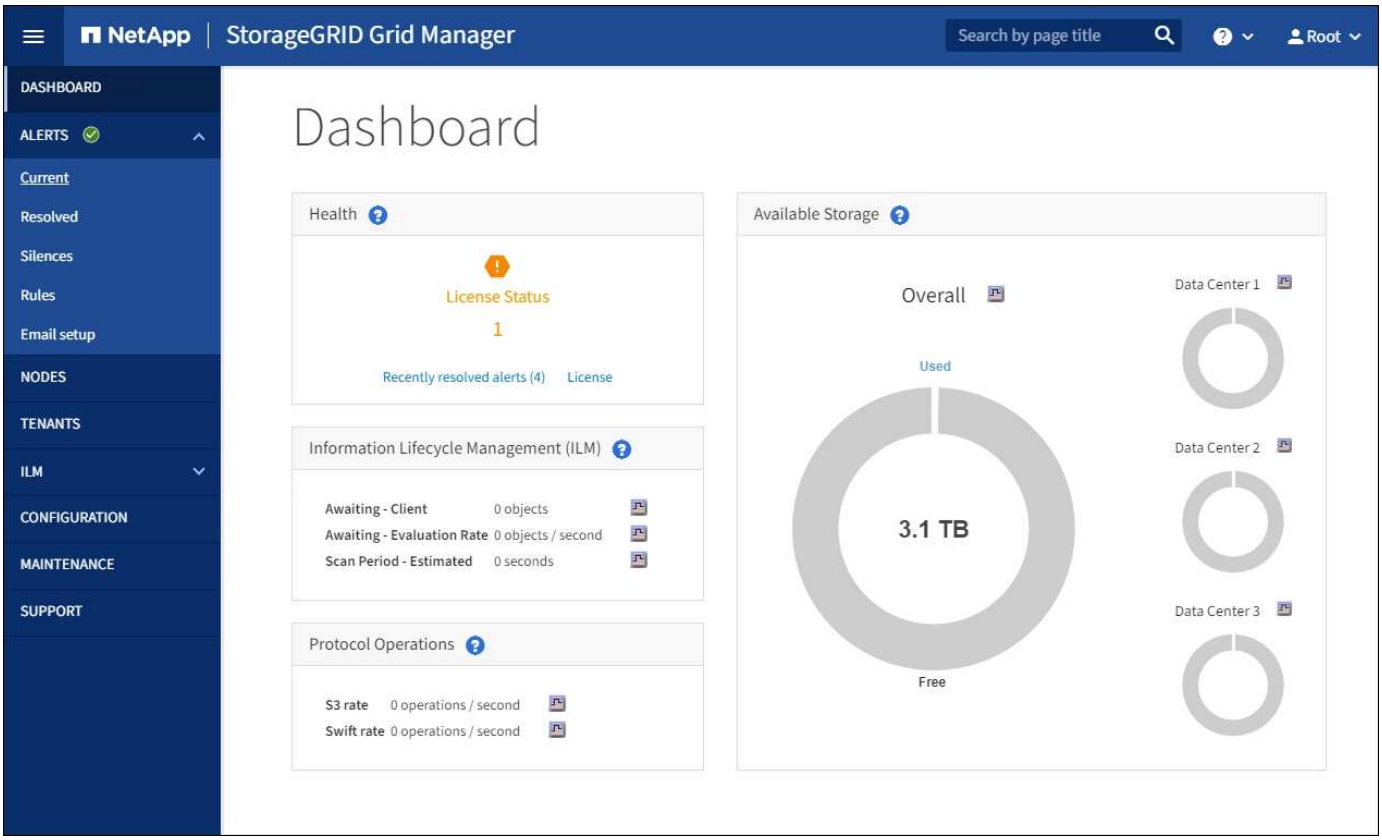
Grid Manager에 로그인하면 관리 노드에 연결됩니다. 각 StorageGRID 시스템에는 1개의 기본 관리 노드와 1차 관리자가 아닌 노드 수가 포함되어 있습니다. 모든 관리 노드에 연결할 수 있으며 각 관리 노드에는 StorageGRID 시스템의 유사한 보기가 표시됩니다.

를 사용하여 그리드 관리자에 액세스할 수 있습니다 지원되는 웹 브라우저.

Grid Manager 대시보드

그리드 관리자에 처음 로그인할 때 대시보드를 사용하여 시스템 활동을 한 눈에 모니터링할 수 있습니다.

대시보드에는 시스템 상태, 스토리지 사용, ILM 프로세스 및 S3 및 Swift 작업에 대한 요약 정보가 포함되어 있습니다.



각 패널의 정보에 대한 설명을 보려면 도움말 아이콘을 클릭하십시오 해당 패널용.

자세한 정보

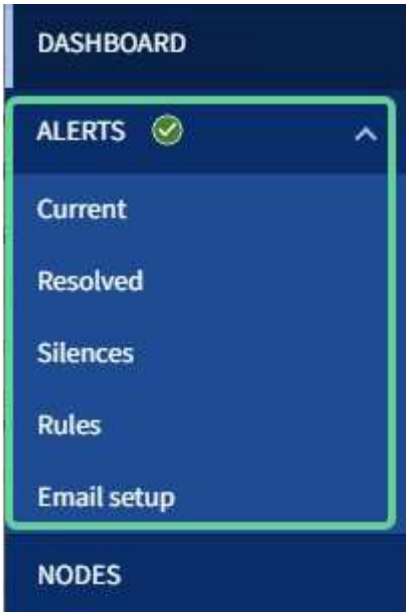
- 모니터링하고 문제를 해결합니다

검색 필드

머리글 표시줄의 * 검색 * 필드를 사용하면 그리드 관리자 내의 특정 페이지로 빠르게 이동할 수 있습니다. 예를 들어, KMS(키 관리 서버) 페이지에 액세스하기 위해 * km * 를 입력할 수 있습니다. * 검색 * 을 사용하여 Grid Manager의 측면 표시줄 및 구성, 유지 관리 및 지원 메뉴에서 항목을 찾을 수 있습니다.

알림 메뉴

경고 메뉴는 StorageGRID 작동 중에 발생할 수 있는 문제를 감지, 평가 및 해결하는 사용하기 쉬운 인터페이스를 제공합니다.



경고 메뉴에서 다음을 수행할 수 있습니다.

- 현재 경고를 검토합니다
- 해결된 경고를 검토합니다
- 알림 알림을 표시하지 않도록 설정을 구성합니다
- 알림을 트리거하는 조건에 대한 경고 규칙을 정의합니다
- 경고 알림을 위한 e-메일 서버를 구성합니다

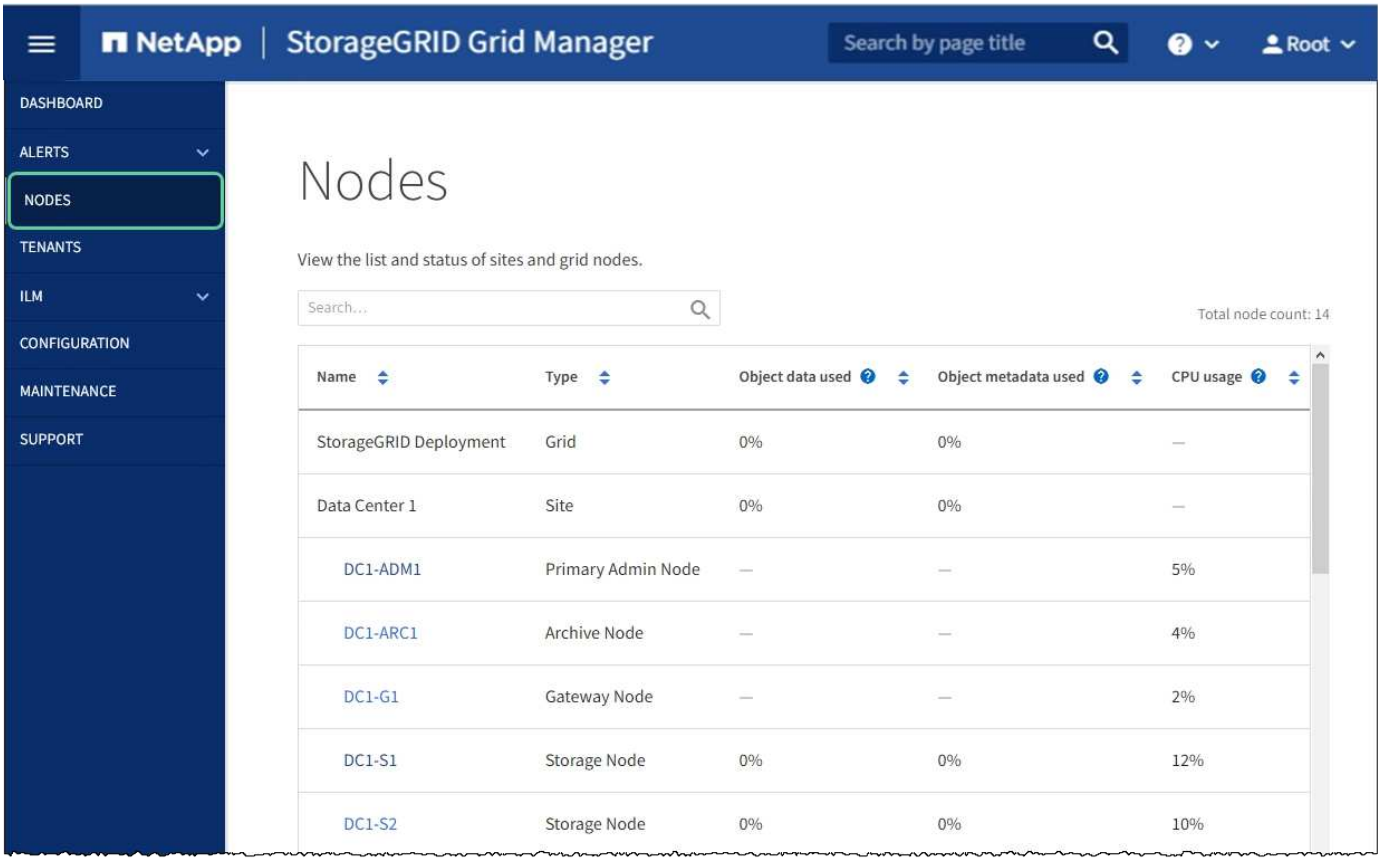
자세한 정보

- 경고를 모니터링하고 관리합니다
- 모니터링하고 문제를 해결합니다

노드 페이지

노드 페이지에는 전체 그리드, 그리드의 각 사이트 및 사이트의 각 노드에 대한 정보가 표시됩니다.

노드 홈 페이지에는 전체 그리드에 대한 결합된 메트릭이 표시됩니다. 특정 사이트 또는 노드에 대한 정보를 보려면 사이트 또는 노드를 선택합니다.



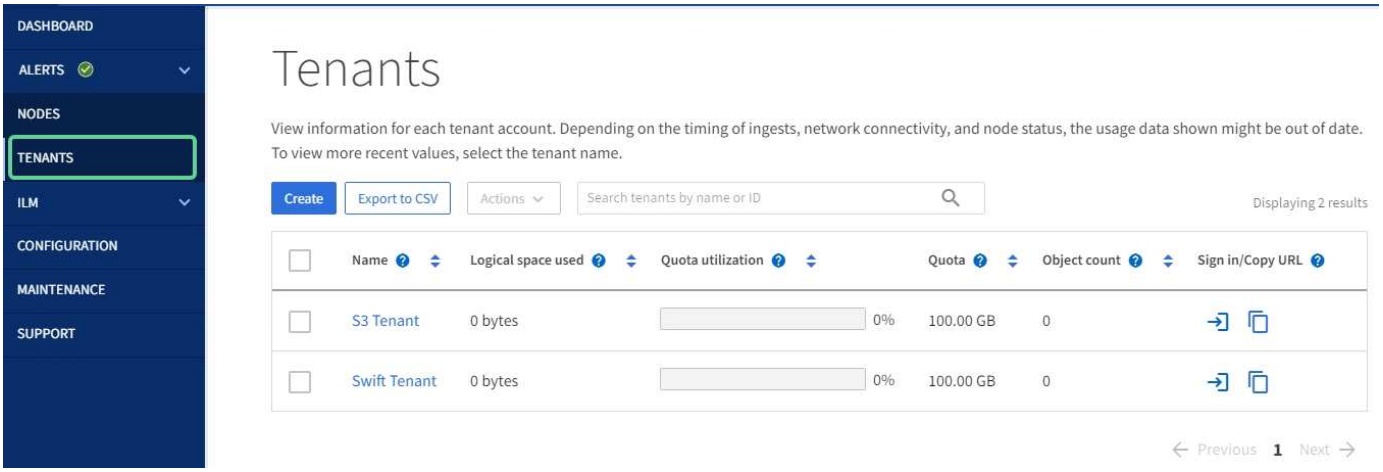
자세한 정보

- 노드 페이지를 봅니다
- 모니터링하고 문제를 해결합니다

Tenants 페이지

Tenants 페이지에서는 StorageGRID 시스템의 스토리지 테넌트 계정을 만들고 모니터링할 수 있습니다. 객체를 저장 및 검색할 수 있는 사람과 객체를 사용할 수 있는 기능을 지정하려면 하나 이상의 테넌트 계정을 생성해야 합니다.

또한 테넌트 페이지에는 사용된 스토리지 양과 객체 수를 비롯한 각 테넌트의 사용 세부 정보도 제공됩니다. 테넌트를 생성할 때 할당량을 설정하면 해당 할당량이 얼마나 사용되었는지 확인할 수 있습니다.



자세한 정보

- 테넌트 및 클라이언트 연결을 관리합니다
- StorageGRID 관리
- 테넌트 계정을 사용합니다

ILM 메뉴

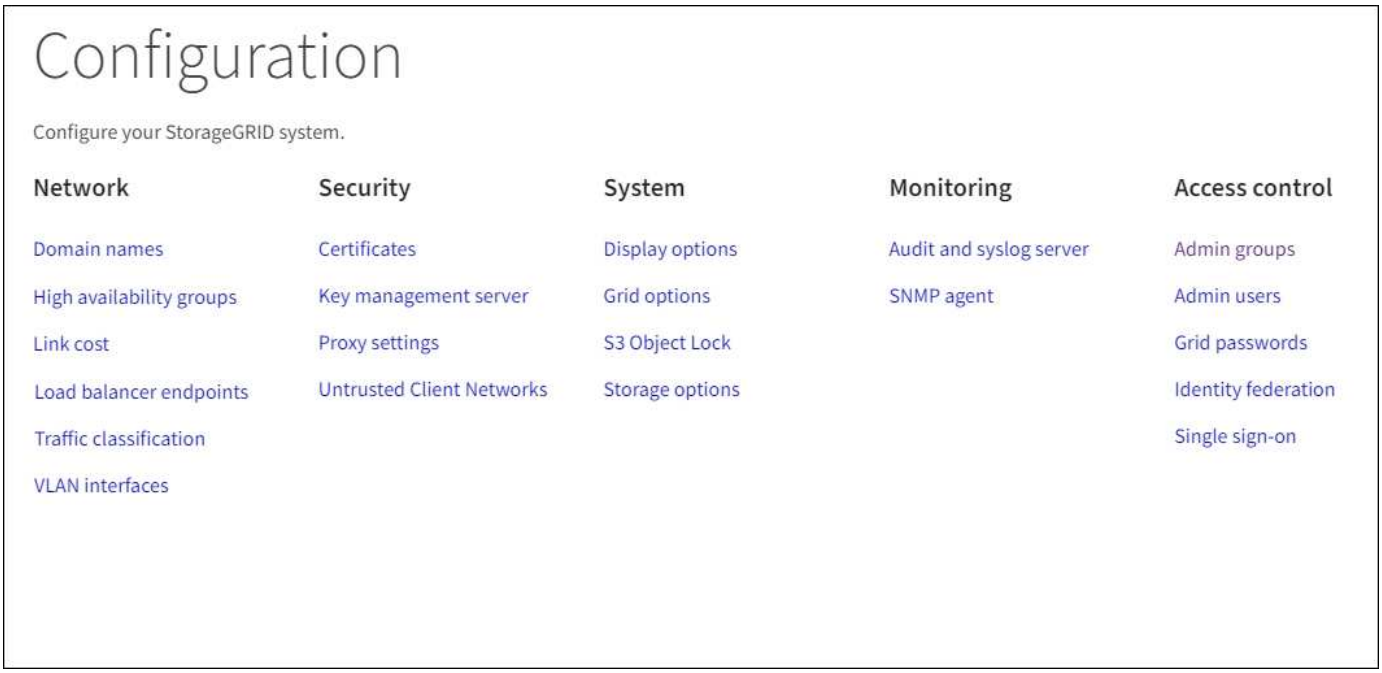
ILM 메뉴를 사용하여 데이터 내구성 및 가용성에 대한 정보 수명 주기 관리(ILM) 규칙 및 정책을 구성할 수 있습니다. 개체 식별자를 입력하여 해당 개체의 메타데이터를 볼 수도 있습니다.

자세한 정보

- 정보 수명 주기 관리를 사용합니다
- ILM을 사용하여 개체를 관리합니다

구성 메뉴

구성 메뉴를 사용하여 네트워크 설정, 보안 설정, 시스템 설정, 모니터링 옵션 및 액세스 제어 옵션을 지정할 수 있습니다.

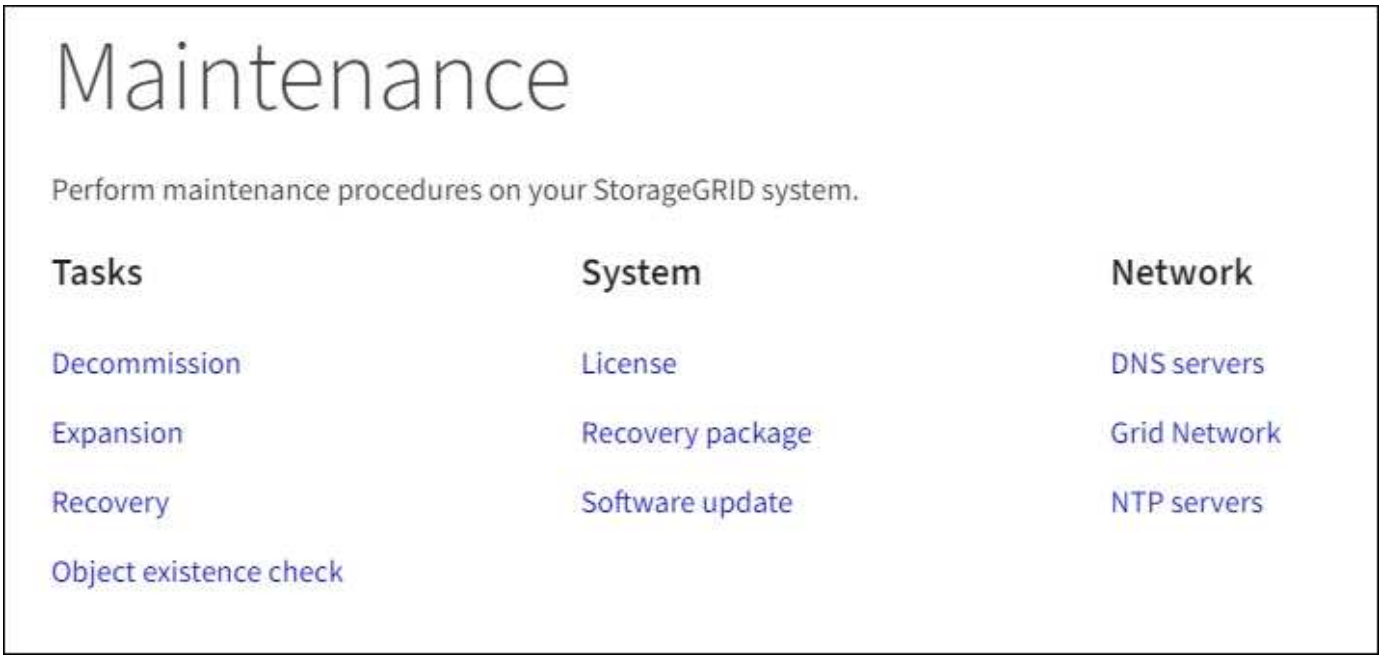


자세한 정보

- 네트워크 설정을 구성합니다
- 테넌트 및 클라이언트 연결을 관리합니다
- 감사 메시지를 검토합니다
- StorageGRID 액세스를 제어합니다
- StorageGRID 관리
- 모니터링하고 문제를 해결합니다
- 감사 로그를 검토합니다

유지 관리 메뉴

유지 관리 메뉴를 사용하면 유지 관리 작업, 시스템 유지 관리 및 네트워크 유지 관리를 수행할 수 있습니다.



작업

유지보수 태스크는 다음과 같습니다.

- 사용되지 않는 그리드 노드 및 사이트를 제거하는 운영 중단
- 새 그리드 노드와 사이트를 추가하기 위한 확장 작업.
- 장애가 발생한 노드를 교체하고 데이터를 복원하는 복구 작업
- 개체 존재 여부를 점검하여 개체 데이터의 존재 여부를 확인합니다(정확성은 아님).

시스템

수행할 수 있는 시스템 유지보수 작업은 다음과 같습니다.

- 현재 StorageGRID 라이센스에 대한 세부 정보 검토 또는 새 라이센스 업로드
- 복구 패키지 생성.
- 선택한 어플라이언스에서 SANtricity OS 소프트웨어에 대한 소프트웨어 업그레이드, 핫픽스 및 업데이트를 포함한 StorageGRID 소프트웨어 업데이트 수행

네트워크

수행할 수 있는 네트워크 유지 보수 작업은 다음과 같습니다.

- DNS 서버에 대한 정보 편집
- 그리드 네트워크에서 사용되는 서브넷을 구성합니다.
- NTP 서버에 대한 정보 편집

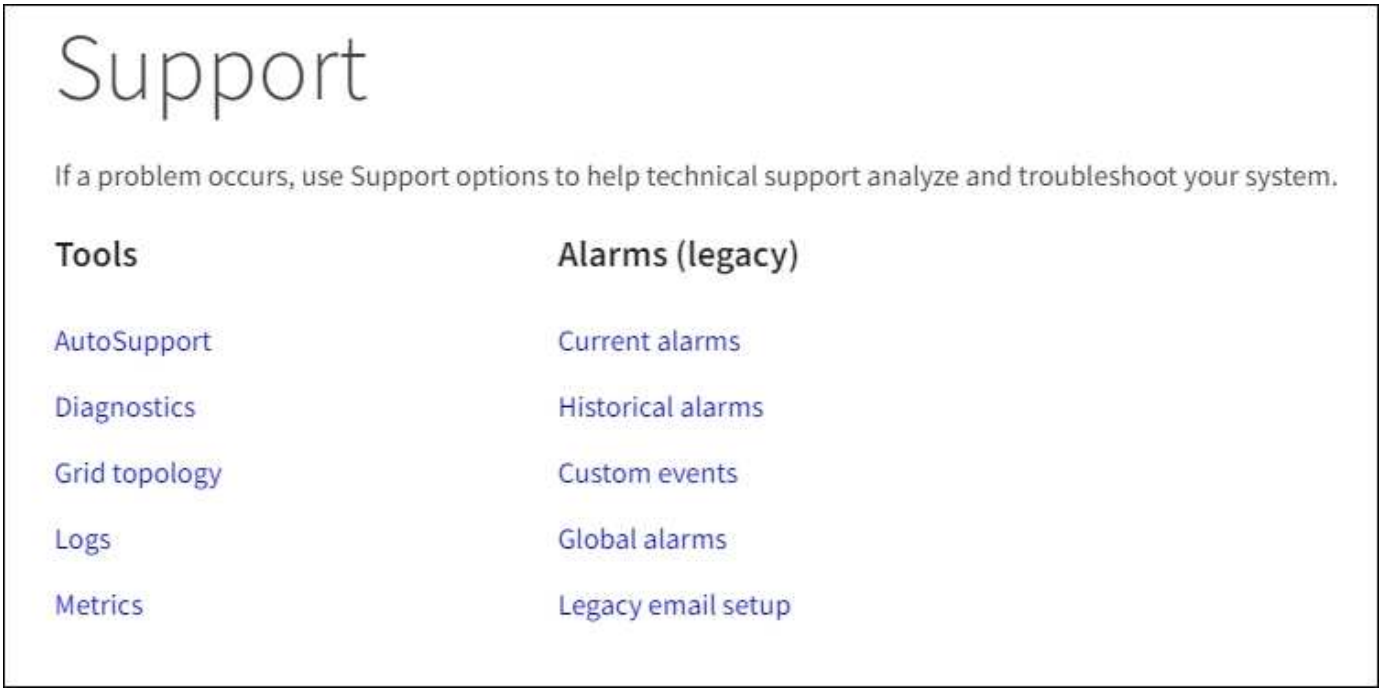
자세한 정보

- 유지 관리를 수행합니다

- 복구 패키지를 다운로드합니다
- 그리드를 확장합니다
- 소프트웨어 업그레이드
- 복구 및 유지 관리
- SG6000 스토리지 어플라이언스
- SG5700 스토리지 어플라이언스
- SG5600 스토리지 어플라이언스

지원 메뉴

지원 메뉴는 기술 지원 부서에서 시스템을 분석하고 문제를 해결하는 데 도움이 되는 옵션을 제공합니다. Support(지원) 메뉴에는 Tools(도구) 및 Alarms(알람)(레거시)의 두 가지 부분이 있습니다.



도구

지원 메뉴의 도구 섹션에서 다음을 수행할 수 있습니다.

- AutoSupport를 활성화합니다.
- 그리드의 현재 상태에 대해 일련의 진단 점검을 수행합니다.
- 그리드 토폴로지 트리에 액세스하여 그리드 노드, 서비스 및 속성에 대한 자세한 정보를 볼 수 있습니다.
- 로그 파일 및 시스템 데이터를 검색합니다.
- 자세한 메트릭 및 차트를 검토하십시오.

> 메트릭* 옵션에서 사용할 수 있는 도구는 기술 지원 부서에서 사용하도록 설계되었습니다. 이러한 도구 내의 일부 기능 및 메뉴 항목은 의도적으로 작동하지 않습니다.

알람(레거시)

지원 메뉴의 알람(레거시) 섹션에서 현재 알람, 과거 알람 및 전체 알람을 검토하고 사용자 지정 이벤트를 설정하며 레거시 알람 및 AutoSupport에 대한 이메일 알림을 설정할 수 있습니다.

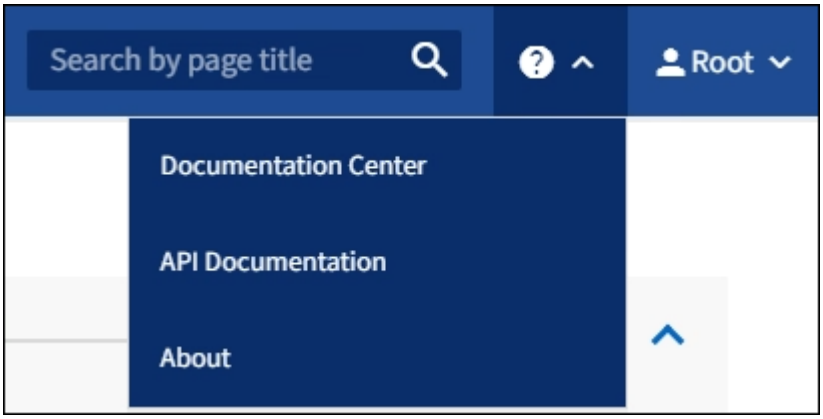
> 기존 알람 시스템은 계속 지원되지만, 알림 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

자세한 정보

- StorageGRID 아키텍처 및 네트워크 토폴로지
- StorageGRID 속성
- StorageGRID 지원 옵션을 사용합니다
- StorageGRID 관리
- 모니터링하고 문제를 해결합니다

도움말 메뉴

Help(도움말) 옵션을 사용하면 현재 릴리스 및 API 설명서에 대한 StorageGRID 설명서 센터에 액세스할 수 있습니다. 현재 설치되어 있는 StorageGRID 버전을 확인할 수도 있습니다.



자세한 정보

- StorageGRID 관리

테넌트 관리자를 탐색합니다

테넌트 관리자는 테넌트 사용자가 액세스하여 스토리지 계정을 구성, 관리 및 모니터링하는 브라우저 기반 그래픽 인터페이스입니다.

테넌트 사용자가 테넌트 관리자에 로그인하면 해당 사용자는 관리 노드에 연결됩니다.

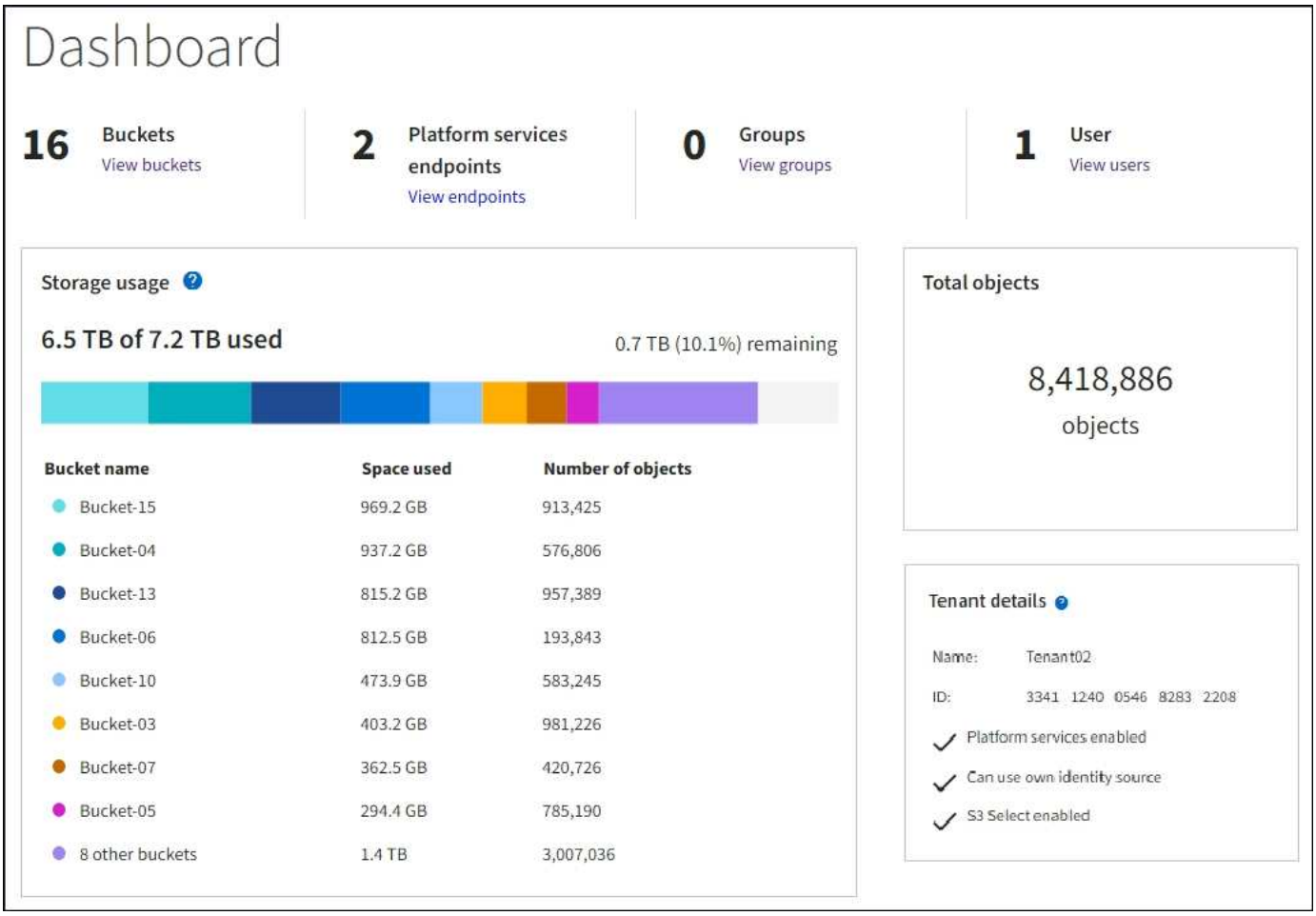
테넌트 관리자 대시보드

그리드 관리자가 그리드 관리자 또는 그리드 관리 API를 사용하여 테넌트 계정을 생성한 후 테넌트 사용자는 테넌트 관리자에 로그인할 수 있습니다.

테넌트 관리자 대시보드를 사용하면 테넌트 사용자가 스토리지 사용량을 한 눈에 모니터링할 수 있습니다. 스토리지 사용 패널에는 테넌트를 위한 가장 큰 버킷(S3) 또는 컨테이너(Swift)의 목록이 포함되어 있습니다. 사용된 공간 값은 버킷이나 컨테이너에 있는 오브젝트 데이터의 총 양입니다. 막대 차트는 이러한 버킷 또는 컨테이너의 상대적 크기를

나타냅니다.

막대 차트 위에 표시된 값은 테넌트의 모든 버킷 또는 컨테이너에 사용되는 공간의 합계입니다. 계정을 생성할 때 테넌트에 사용할 수 있는 최대 GB, 테라바이트 또는 페타바이트 수를 지정한 경우 사용된 할당량과 남은 용량 또한 표시됩니다.



스토리지 메뉴(**S3** 테넌트만 해당)

스토리지 메뉴는 S3 테넌트 계정에만 제공됩니다. 이 메뉴를 통해 S3 사용자는 액세스 키를 관리하고, 버킷을 생성 및 삭제하고, 플랫폼 서비스 엔드포인트를 관리할 수 있습니다.

내 액세스 키

S3 테넌트 사용자는 다음과 같이 액세스 키를 관리할 수 있습니다.

- 자신의 S3 자격 증명 관리 권한이 있는 사용자는 자신의 S3 액세스 키를 생성하거나 제거할 수 있습니다.
- 루트 액세스 권한이 있는 사용자는 S3 루트 계정, 자신의 계정 및 다른 모든 사용자의 액세스 키를 관리할 수 있습니다. 루트 액세스 키는 또한 버킷 정책에 의해 명시적으로 비활성화되지 않는 한 테넌트의 버킷 및 오브젝트에 대한 전체 액세스를 제공합니다.

> 다른 사용자의 액세스 키 관리는 Access Management(액세스 관리) 메뉴에서 수행됩니다.

버킷

적절한 권한이 있는 S3 테넌트 사용자는 버킷과 관련된 다음 작업을 수행할 수 있습니다.

- 버킷을 생성합니다
- 새 버킷에 대해 S3 오브젝트 잠금 활성화(StorageGRID 시스템에 대해 S3 오브젝트 잠금이 활성화된 것으로 가정)
- 정합성 보장 레벨 설정을 업데이트합니다
- 기본 보존 설정을 적용합니다
- CORS(Cross-Origin Resource Sharing) 구성
- 테넌트에 속한 버킷에 대한 마지막 액세스 시간 업데이트 설정을 활성화 및 비활성화합니다
- 빈 버킷을 삭제합니다
- 를 사용하여 버킷의 오브젝트를 관리합니다 Experimental S3 Console을 선택합니다

그리드 관리자가 테넌트 계정에 대한 플랫폼 서비스 사용을 활성화한 경우 적절한 권한이 있는 S3 테넌트 사용자도 다음 작업을 수행할 수 있습니다.

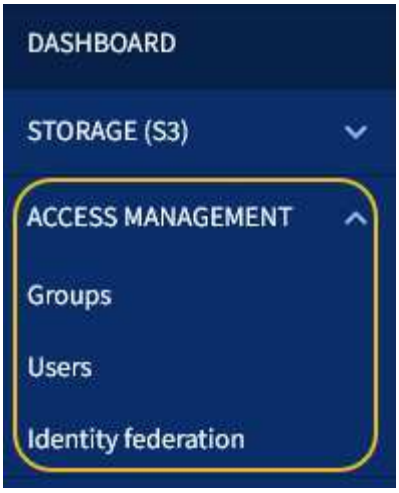
- AWS SNS(Simple Notification Service ™)를 지원하는 대상 서비스로 전송할 수 있는 S3 이벤트 알림을 구성합니다.
- 테넌트가 외부 S3 버킷에 오브젝트를 자동으로 복제할 수 있도록 CloudMirror 복제를 구성합니다.
- 객체를 생성, 삭제 또는 해당 메타데이터 또는 태그가 업데이트될 때마다 대상 검색 인덱스에 객체 메타데이터를 전송하는 검색 통합을 구성합니다.

플랫폼 서비스 엔드포인트

그리드 관리자가 테넌트 계정에 대한 플랫폼 서비스 사용을 활성화한 경우 엔드포인트 관리 권한이 있는 S3 테넌트 사용자는 각 플랫폼 서비스에 대한 대상 끝점을 구성할 수 있습니다.

Access Management(관리) 메뉴

액세스 관리 메뉴를 사용하면 StorageGRID 테넌트가 통합 ID 소스에서 사용자 그룹을 가져오고 관리 권한을 할당할 수 있습니다. 전체 StorageGRID 시스템에 SSO(Single Sign-On)가 적용되지 않는 한 테넌트는 로컬 테넌트 그룹 및 사용자를 관리할 수도 있습니다.



관련 정보

- Grid Manager를 살펴봅니다
- 테넌트 계정을 사용합니다

StorageGRID 액세스를 제어합니다

그룹 및 사용자를 만들거나 가져오고 각 그룹에 권한을 할당하여 StorageGRID에 액세스할 수 있는 사용자와 사용자가 수행할 수 있는 작업을 제어할 수 있습니다. 선택적으로 SSO(Single Sign-On)를 활성화하고, 클라이언트 인증서를 생성하고, 그리드 암호를 변경할 수 있습니다.

그리드 관리자에 대한 액세스를 제어합니다

ID 페더레이션 서비스에서 그룹과 사용자를 가져오거나 로컬 그룹 및 로컬 사용자를 설정하여 Grid Manager 및 Grid Management API에 액세스할 수 있는 사용자를 결정합니다.

ID 페더레이션을 사용하면 그룹 및 사용자를 더 빠르게 설정할 수 있으며, 사용자는 익숙한 자격 증명을 사용하여 StorageGRID에 로그인할 수 있습니다. Active Directory, OpenLDAP 또는 Oracle Directory Server를 사용하는 경우 ID 페더레이션을 구성할 수 있습니다.

> 다른 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의하십시오.

각 그룹에 서로 다른 권한을 할당하여 각 사용자가 수행할 수 있는 작업을 결정합니다. 예를 들어 한 그룹의 사용자가 ILM 규칙 및 다른 그룹의 사용자를 관리하여 유지 관리 작업을 수행할 수 있도록 할 수 있습니다. 시스템에 액세스하려면 사용자가 하나 이상의 그룹에 속해 있어야 합니다.

선택적으로 그룹을 읽기 전용으로 구성할 수 있습니다. 읽기 전용 그룹의 사용자는 설정과 기능만 볼 수 있습니다. 그리드 관리자 또는 그리드 관리 API에서 어떠한 변경이나 작업도 수행할 수 없습니다.

SSO(Single Sign-On)를 활성화합니다

StorageGRID 시스템은 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용하여 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.

SSO가 활성화되어 있고 사용자가 StorageGRID에 로그인하면 조직의 SSO 페이지로 리디렉션되어 자격 증명을

검증합니다. 사용자가 하나의 관리 노드에서 로그아웃하면 모든 관리 노드에서 자동으로 로그아웃됩니다.

그리드 암호를 변경합니다

프로비저닝 암호는 많은 설치 및 유지 관리 절차와 StorageGRID 복구 패키지 다운로드에 필요합니다. 또한 StorageGRID 시스템에 대한 그리드 토폴로지 정보와 암호화 키의 백업을 다운로드하려면 암호문도 필요합니다. 필요에 따라 이 암호를 변경할 수 있습니다.

관련 정보

- StorageGRID 관리
- 테넌트 계정을 사용합니다

테넌트 및 클라이언트 연결을 관리합니다

그리드 관리자는 S3 및 Swift 클라이언트가 오브젝트를 저장 및 검색하는 데 사용하는 테넌트 계정을 만들고 관리하며 클라이언트가 StorageGRID 시스템에 연결하는 방법을 제어하는 구성 옵션을 관리합니다.

테넌트 계정

테넌트 계정을 사용하면 StorageGRID 시스템을 사용하여 객체를 저장 및 검색할 수 있는 사용자 및 사용 가능한 기능을 지정할 수 있습니다. 테넌트 계정을 사용하면 S3 REST API 또는 Swift REST API를 지원하는 클라이언트 애플리케이션이 StorageGRID에 오브젝트를 저장하고 검색할 수 있습니다. 각 테넌트 계정은 S3 클라이언트 프로토콜 또는 Swift 클라이언트 프로토콜을 사용합니다.

StorageGRID 시스템에 객체를 저장하는 데 사용할 각 클라이언트 프로토콜에 대해 하나 이상의 테넌트 계정을 생성해야 합니다. 필요에 따라 시스템에 저장된 객체를 다른 엔터티로 분리하려는 경우 추가 테넌트 계정을 생성할 수 있습니다. 각 테넌트 계정에는 자체 통합 또는 로컬 그룹 및 사용자와 자체 버킷(Swift용 컨테이너) 및 객체가 있습니다.

Grid Manager 또는 Grid Management API를 사용하여 테넌트 계정을 생성할 수 있습니다. 테넌트 계정을 생성할 때 다음 정보를 지정합니다.

- 테넌트의 표시 이름(테넌트의 계정 ID가 자동으로 할당되며 변경할 수 없음)
- 테넌트 계정에서 S3 또는 Swift를 사용할지 여부를 나타냅니다.
- S3 테넌트 계정의 경우: 테넌트 계정이 플랫폼 서비스를 사용하도록 허용되는지 여부 플랫폼 서비스를 사용할 수 있는 경우 그리드 사용을 지원하도록 구성해야 합니다.
- 필요한 경우 테넌트 계정의 스토리지 할당량 — 테넌트의 객체에 사용할 수 있는 최대 GB, 테라바이트 또는 PB입니다. 테넌트의 스토리지 할당량은 물리적 크기(디스크 크기)가 아닌 논리적 양(오브젝트 크기)을 나타냅니다.
- StorageGRID 시스템에 대해 ID 페더레이션이 설정된 경우 테넌트 계정을 구성할 수 있는 루트 액세스 권한이 있는 통합 그룹입니다.
- StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하지 않는 경우 테넌트 계정이 자체 ID 소스를 사용할지 또는 그리드의 ID 소스를 공유할지 여부 및 테넌트의 로컬 루트 사용자의 초기 암호를 공유할지 여부

S3 테넌트 계정이 규정 요구 사항을 준수해야 하는 경우 그리드 관리자는 StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정을 활성화할 수 있습니다. 시스템에 S3 오브젝트 잠금이 설정되어 있으면 모든 S3 테넌트 계정에서 S3 오브젝트 잠금이 설정된 버킷을 생성한 다음 해당 버킷의 오브젝트 버전에 대한 보존 및 법적 보류 설정을 지정할 수 있습니다.

테넌트 계정이 생성된 후 테넌트 사용자는 테넌트 관리자에 로그인할 수 있습니다.

StorageGRID 노드에 대한 클라이언트 접속

테넌트 사용자가 S3 또는 Swift 클라이언트를 사용하여 StorageGRID에 데이터를 저장하고 검색하기 전에 이러한 클라이언트가 StorageGRID 노드에 어떻게 연결할지 결정해야 합니다.

클라이언트 응용 프로그램은 다음 중 하나를 연결하여 개체를 저장하거나 검색할 수 있습니다.

- 관리 노드 또는 게이트웨이 노드의 부하 분산 서비스 이것은 권장되는 연결입니다.
- 게이트웨이 노드의 CLB 서비스.

> CLB 서비스는 더 이상 사용되지 않습니다.

- 외부 로드 밸런서가 있거나 없는 스토리지 노드

클라이언트가 로드 밸런서 서비스를 사용할 수 있도록 StorageGRID를 구성할 때 다음 단계를 수행합니다.

1. 필요에 따라 고가용성(HA) 그룹을 구성합니다. HA 그룹을 생성하면 여러 관리 노드 및 게이트웨이 노드의 인터페이스가 액티브 백업 구성에 배치됩니다. HA 그룹의 가상 IP 주소를 사용하여 클라이언트 연결이 이루어집니다.
2. 로드 밸런서 서비스의 끝점을 구성합니다. 관리 노드 또는 게이트웨이 노드의 부하 분산 서비스는 들어오는 네트워크 연결을 클라이언트 애플리케이션에서 스토리지 노드로 분산합니다. 로드 밸런서 끝점을 만들 때 끝점에서 HTTP 또는 HTTPS 연결을 허용하는지 여부, 끝점을 사용할 클라이언트 유형(S3 또는 Swift) 및 HTTPS 연결에 사용할 인증서(해당하는 경우)를 포트 번호로 지정합니다.
3. 노드의 클라이언트 네트워크에 대한 모든 연결이 로드 밸런서 끝점에서 발생하도록 노드의 클라이언트 네트워크를 신뢰할 수 없도록 지정합니다(선택 사항).

관련 정보

- StorageGRID 관리
- 테넌트 계정을 사용합니다
- S3을 사용합니다
- Swift를 사용합니다
- 테넌트 관리자를 탐색합니다
- 네트워크 설정을 구성합니다

네트워크 설정을 구성합니다

그리드 관리자에서 다양한 네트워크 설정을 구성하여 StorageGRID 시스템의 작동을 미세 조정할 수 있습니다.

도메인 이름

S3 가상 호스팅 스타일 요청을 지원하려는 경우 S3 클라이언트가 연결하는 끝점 도메인 이름 목록을 구성해야 합니다. 예를 들어 3.example.com, 3.example.co.uk, 3-east.example.com 등이 있습니다.

구성된 서버 인증서는 끝점 도메인 이름과 일치해야 합니다.

고가용성 그룹

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

HA 그룹을 생성할 때 하나 이상의 노드에 대한 네트워크 인터페이스를 선택합니다. 각 HA 그룹은 선택한 노드의 공유 서비스에 대한 액세스를 제공합니다.

- 게이트웨이 노드의 인터페이스를 포함하는 HA 그룹, 관리 노드 또는 둘 다 S3 및 Swift 클라이언트에 고가용성 데이터 연결을 제공합니다.
- 관리 노드의 인터페이스를 포함하는 HA 그룹은 Grid Manager 및 테넌트 관리자에 대한 고가용성 연결만 제공합니다.

인터페이스는 그리드 네트워크(eth0), 클라이언트 네트워크(eth2) 또는 VLAN 네트워크에 속할 수 있습니다.

각 HA 그룹에 최대 10개의 가상 IP(VIP) 주소를 할당할 수 있습니다. 하나의 인터페이스를 기본 인터페이스로 지정하고 다른 인터페이스의 우선 순위를 지정합니다. Primary 인터페이스는 장애가 발생하지 않는 한 Active 인터페이스입니다. 활성 인터페이스에 장애가 발생하면 VIP 주소가 우선 순위에 따라 첫 번째 백업 인터페이스로 이동합니다. 이 인터페이스에 장애가 발생하면 VIP 주소가 다음 백업 인터페이스로 이동합니다.

비용 연결

링크 비용을 조정하여 사이트 간 지연 시간을 반영할 수 있습니다. 두 개 이상의 데이터 센터 사이트가 존재하는 경우 링크 비용은 요청된 서비스를 제공해야 하는 데이터 센터 사이트의 우선 순위를 지정합니다.

부하 분산 장치 엔드포인트

로드 밸런서를 사용하여 S3 및 Swift 클라이언트에서 수집 및 검색 워크로드를 처리할 수 있습니다. 로드 밸런싱은 여러 스토리지 노드에 워크로드와 연결을 분산하여 속도와 연결 용량을 극대화합니다.

관리 노드 및 게이트웨이 노드에 포함된 StorageGRID 로드 밸런서 서비스를 사용하려면 하나 이상의 로드 밸런서 끝점을 구성해야 합니다. 각 엔드포인트는 S3 및 스토리지 노드에 대한 Swift 요청에 대한 게이트웨이 노드 또는 관리 노드 포트를 정의합니다.

트래픽 분류

트래픽 분류 정책을 생성하여 특정 버킷, 테넌트, 클라이언트 서브넷 또는 로드 밸런서 엔드포인트와 관련된 트래픽을 포함하여 다양한 유형의 네트워크 트래픽을 식별하고 처리할 수 있습니다. 이러한 정책은 트래픽 제한 및 모니터링을 지원할 수 있습니다.

VLAN 인터페이스

VLAN(Virtual LAN) 인터페이스를 생성하여 트래픽을 격리하고 파티셔닝하여 보안, 유연성 및 성능을 확보할 수 있습니다. 각 VLAN 인터페이스는 관리 노드 및 게이트웨이 노드에서 하나 이상의 상위 인터페이스와 연결됩니다. HA 그룹 및 로드 밸런서 끝점에서 VLAN 인터페이스를 사용하여 클라이언트 또는 관리 트래픽을 애플리케이션 또는 테넌트별로 분리할 수 있습니다.

예를 들어 네트워크에서 FabricPool 트래픽에는 VLAN 100을 사용하고 아카이브 애플리케이션에는 VLAN 200을 사용할 수 있습니다.

관련 정보

- StorageGRID 관리

- 테넌트 및 클라이언트 연결을 관리합니다

보안 설정을 구성합니다

그리드 관리자에서 다양한 보안 설정을 구성하여 StorageGRID 시스템을 보호할 수 있습니다.

인증서

StorageGRID는 두 가지 유형의 보안 인증서를 사용합니다.

- HTTPS 연결을 사용할 때는 서버 인증서가 필요합니다. 서버 인증서는 클라이언트와 서버 간의 보안 연결을 설정하고, 클라이언트에 대한 서버 ID를 인증하고, 데이터에 대한 보안 통신 경로를 제공하는 데 사용됩니다. 서버와 클라이언트마다 인증서의 복사본이 있습니다.
- 클라이언트 인증서는 서버에 대한 클라이언트 또는 사용자 ID를 인증하여 암호만 사용하는 것보다 더 안전한 인증을 제공합니다. 클라이언트 인증서는 데이터를 암호화하지 않습니다.

구성 * > * 보안 * > * 인증서 * 페이지에서 모든 StorageGRID 인증서를 볼 수 있습니다.

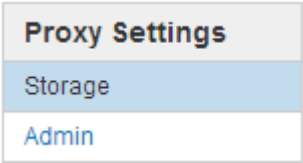
키 관리 서버

하나 이상의 외부 키 관리 서버(KMS)를 구성하여 StorageGRID 서비스 및 스토리지 어플라이언스에 암호화 키를 제공할 수 있습니다. 각 KMS 또는 KMS 클러스터는 KMIP(Key Management Interoperability Protocol)를 사용하여 관련 StorageGRID 사이트의 어플라이언스 노드에 암호화 키를 제공합니다. 키 관리 서버를 사용하면 어플라이언스가 데이터 센터에서 제거되더라도 StorageGRID 데이터를 보호할 수 있습니다. 어플라이언스 볼륨이 암호화된 후에는 노드에서 KMS와 통신할 수 없는 한 어플라이언스의 데이터에 액세스할 수 없습니다.

> 암호화 키 관리를 사용하려면 어플라이언스를 그리드에 추가하기 전에 설치 중에 각 어플라이언스에 대해 * 노드 암호화 * 설정을 활성화해야 합니다.

프록시 설정

S3 플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 스토리지 노드와 외부 S3 엔드포인트 간에 투명하지 않은 프록시 서버를 구성할 수 있습니다. HTTPS 또는 HTTP를 사용하여 AutoSupport 메시지를 보내는 경우 관리자 노드와 기술 지원 간에 투명하지 않은 프록시 서버를 구성할 수 있습니다.



신뢰할 수 없는 클라이언트 네트워크

클라이언트 네트워크를 사용하는 경우 각 노드의 클라이언트 네트워크를 신뢰할 수 없도록 지정하여 악의적인 공격으로부터 StorageGRID를 보호할 수 있습니다. 노드의 클라이언트 네트워크를 신뢰할 수 없는 경우 노드는 로드 밸런서 끝점으로 명시적으로 구성된 포트의 인바운드 연결만 허용합니다.

예를 들어, 게이트웨이 노드가 HTTPS S3 요청을 제외한 클라이언트 네트워크의 모든 인바운드 트래픽을 거부하도록 할 수 있습니다. 또는 클라이언트 네트워크의 해당 스토리지 노드에 대한 인바운드 연결을 방지하면서 스토리지 노드에서 아웃바운드 S3 플랫폼 서비스 트래픽을 활성화할 수 있습니다.

관련 정보

- StorageGRID 관리
- 테넌트 및 클라이언트 연결을 관리합니다

시스템 설정을 구성합니다

그리드 관리자에서 다양한 시스템 설정을 구성하여 StorageGRID 시스템의 작동을 미세 조정할 수 있습니다.

표시 옵션

표시 옵션을 사용하면 사용자 세션의 제한 시간을 지정하고 레거시 알람 및 이벤트 트리거 AutoSupport 메시지에 대한 이메일 알림을 표시하지 않을 수 있습니다.

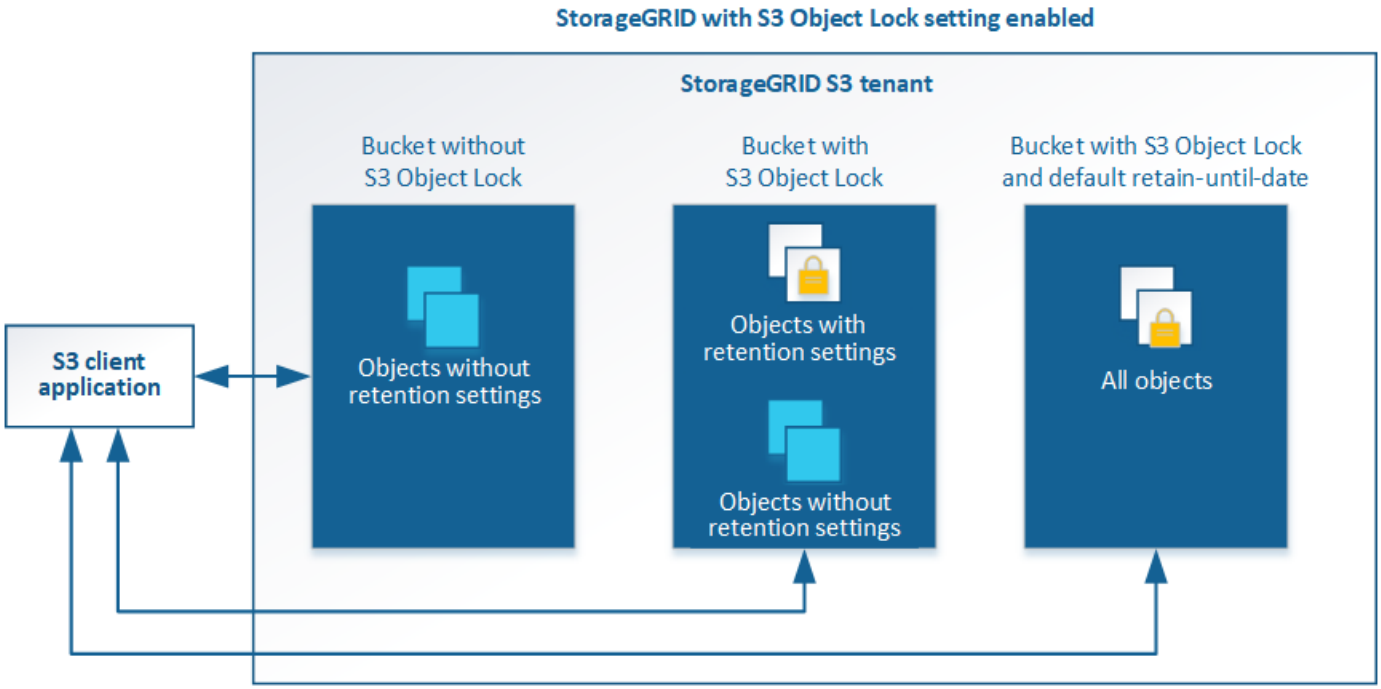
그리드 옵션

그리드 옵션을 사용하여 저장된 오브젝트 압축, 저장된 오브젝트 암호화를 포함하여 StorageGRID 시스템에 저장된 모든 오브젝트에 대한 설정을 구성할 수 있습니다. 및 저장된 객체 해싱입니다.

이 옵션을 사용하여 S3 및 Swift 클라이언트 작업에 대한 글로벌 설정을 지정할 수도 있습니다.

S3 오브젝트 잠금

StorageGRID S3 오브젝트 잠금 기능은 Amazon S3(Amazon Simple Storage Service)의 S3 오브젝트 잠금과 동등한 오브젝트 보호 솔루션입니다. StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정을 활성화하면 S3 테넌트 계정에서 S3 오브젝트 잠금이 설정된 버킷을 생성할 수 있습니다. 그런 다음 테넌트는 S3 클라이언트 애플리케이션을 사용하여 해당 버킷의 오브젝트에 대한 보존 설정(종료 날짜, 법적 보류 또는 둘 다 유지)을 선택적으로 지정할 수 있습니다. 또한 S3 오브젝트 잠금이 활성화된 각 버킷에는 선택적으로 기본 보존 모드 및 보존 기간이 있을 수 있으며, 이 기간은 객체가 고유한 보존 설정 없이 버킷에 추가되는 경우에 적용됩니다.



스토리지 옵션

스토리지 옵션을 사용하면 객체 분할을 제어하고 스토리지 볼륨 워터마크 설정을 재정의하여 스토리지 노드의 사용 가능한 스토리지 공간을 관리할 수 있습니다.

정보 수명 주기 관리를 사용합니다

ILM(정보 수명 주기 관리)을 사용하여 StorageGRID 시스템의 모든 개체에 대한 배치, 기간 및 데이터 보호를 제어할 수 있습니다. ILM 규칙은 StorageGRID이 시간에 따라 개체를 저장하는 방법을 결정합니다. 하나 이상의 ILM 규칙을 구성한 다음 ILM 정책에 추가합니다.

ILM 규칙 정의:

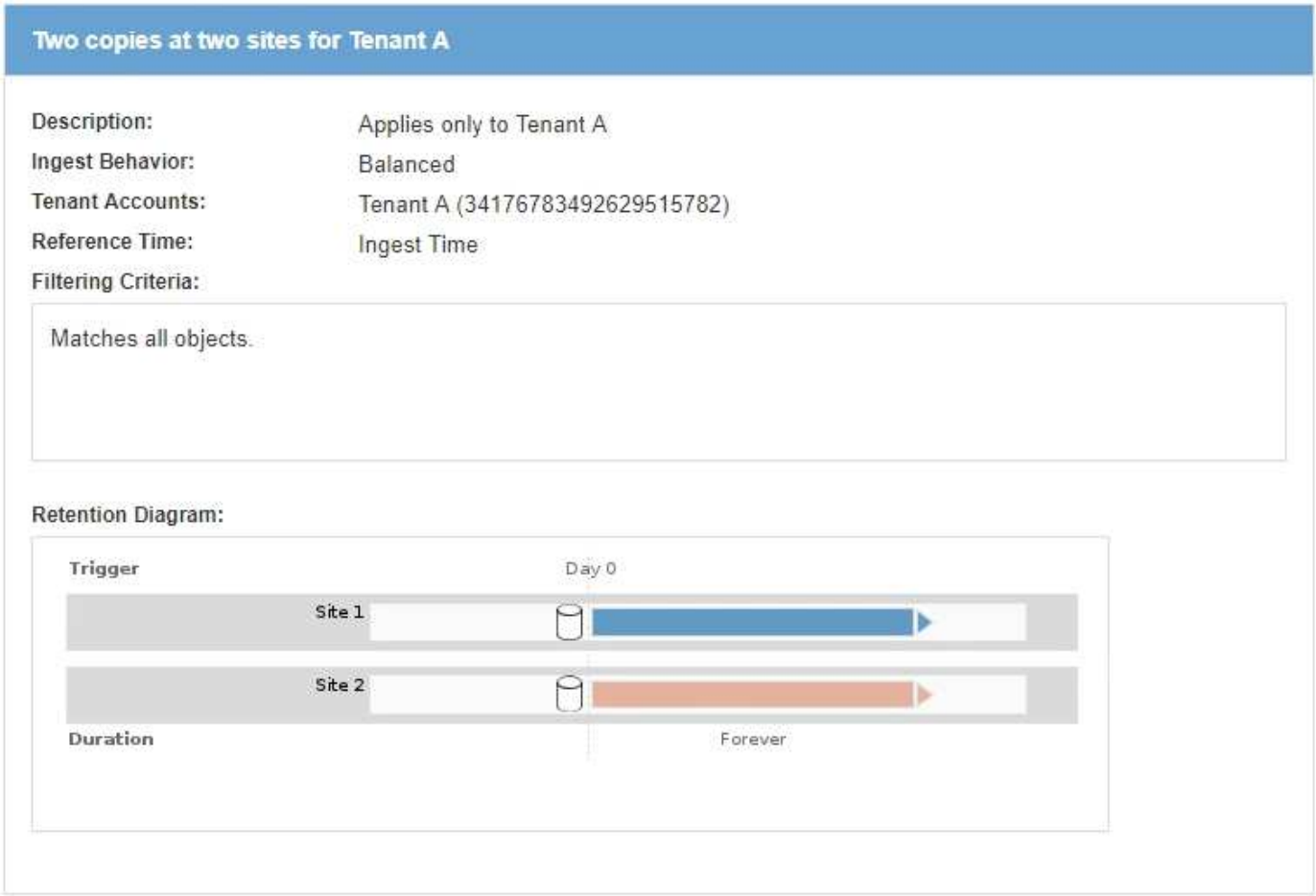
- 어떤 오브젝트를 저장해야 하는지. 규칙은 모든 개체에 적용할 수 있으며, 규칙을 적용할 개체를 식별하는 필터를 지정할 수도 있습니다. 예를 들어, 규칙은 특정 테넌트 계정, 특정 S3 버킷 또는 Swift 컨테이너 또는 특정 메타데이터 값과 연결된 오브젝트에만 적용할 수 있습니다.
- 스토리지 유형 및 위치입니다. 오브젝트는 스토리지 노드, 클라우드 스토리지 풀 또는 아카이브 노드에 저장할 수 있습니다.
- 생성된 오브젝트 복사본의 유형입니다. 복사본을 복제하거나 삭제 코딩할 수 있습니다.
- 복제된 복사본의 경우 생성된 복사본 수입니다.
- 삭제 코딩 복사본의 경우 삭제 코딩 방법을 사용합니다.
- 시간이 지나면서 개체의 스토리지 위치 및 복사본 유형이 변경됩니다.
- 오브젝트를 그리드에 수집하면서 오브젝트 데이터를 보호하는 방법(동기식 배치 또는 이중 커밋)

개체 메타데이터는 ILM 규칙에 의해 관리되지 않습니다. 대신 오브젝트 메타데이터는 메타데이터 저장소라고 하는 Cassandra 데이터베이스에 저장됩니다. 데이터가 손실되지 않도록 보호하기 위해 각 사이트에 오브젝트 메타데이터의 복사본 3개가 자동으로 유지됩니다. 복제본은 모든 스토리지 노드에 균등하게 분산됩니다.

ILM 규칙 예

이 ILM 규칙 예는 테넌트 A에 속하는 객체에 적용됩니다 즉, 이러한 객체의 복제본을 두 개 생성하고 각 복제본을 다른 사이트에 저장합니다. 두 개의 사본은 영구 보관되어 있습니다. 즉, StorageGRID는 이를 자동으로 삭제하지 않습니다. 대신, StorageGRID는 이러한 객체가 클라이언트 삭제 요청에 의해 삭제되거나 버킷 수명 주기가 만료될 때까지 해당 객체를 유지합니다.

이 규칙은 수집 동작에 균형 옵션을 사용합니다. 테넌트 A가 개체를 StorageGRID에 저장하는 즉시 두 사이트 배치 명령이 적용됩니다. 단, 두 필요한 복제본을 모두 즉시 생성할 수 없습니다. 예를 들어 테넌트 A가 객체를 저장할 때 사이트 2에 연결할 수 없는 경우 StorageGRID는 사이트 1의 스토리지 노드에 두 개의 중간 복제본을 만듭니다. 사이트 2를 사용할 수 있게 되면 StorageGRID는 해당 사이트에서 필요한 복사본을 만듭니다.



ILM 정책이 개체를 평가하는 방법

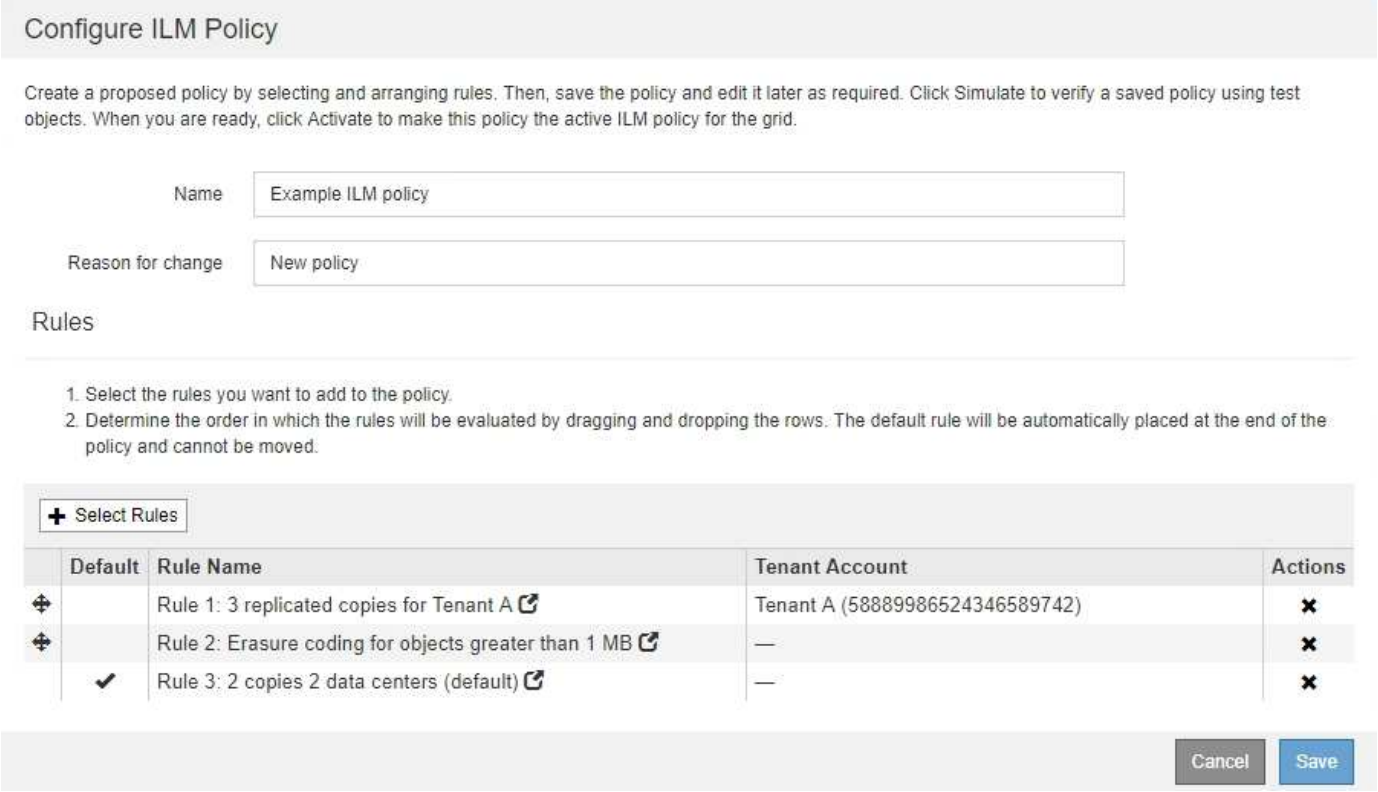
StorageGRID 시스템에 대한 활성 ILM 정책은 모든 개체의 배치, 기간 및 데이터 보호를 제어합니다.

클라이언트가 개체를 StorageGRID에 저장하면 활성 정책에서 정렬된 ILM 규칙 집합에 대해 다음과 같이 개체가 평가됩니다.

1. 정책의 첫 번째 규칙에 대한 필터가 개체와 일치하면 해당 규칙의 수집 동작에 따라 개체가 수집되고 해당 규칙의 배치 지침에 따라 저장됩니다.
2. 첫 번째 규칙의 필터가 개체와 일치하지 않으면 일치하는 항목이 될 때까지 해당 개체가 정책의 다음 각 규칙에 대해 평가됩니다.
3. 개체와 일치하는 규칙이 없으면 정책의 기본 규칙에 대한 수집 동작 및 배치 지침이 적용됩니다. 기본 규칙은 정책의 마지막 규칙이며 필터를 사용할 수 없습니다. 모든 테넌트, 모든 버킷 및 모든 오브젝트 버전에 적용되어야 합니다.

ILM 정책의 예

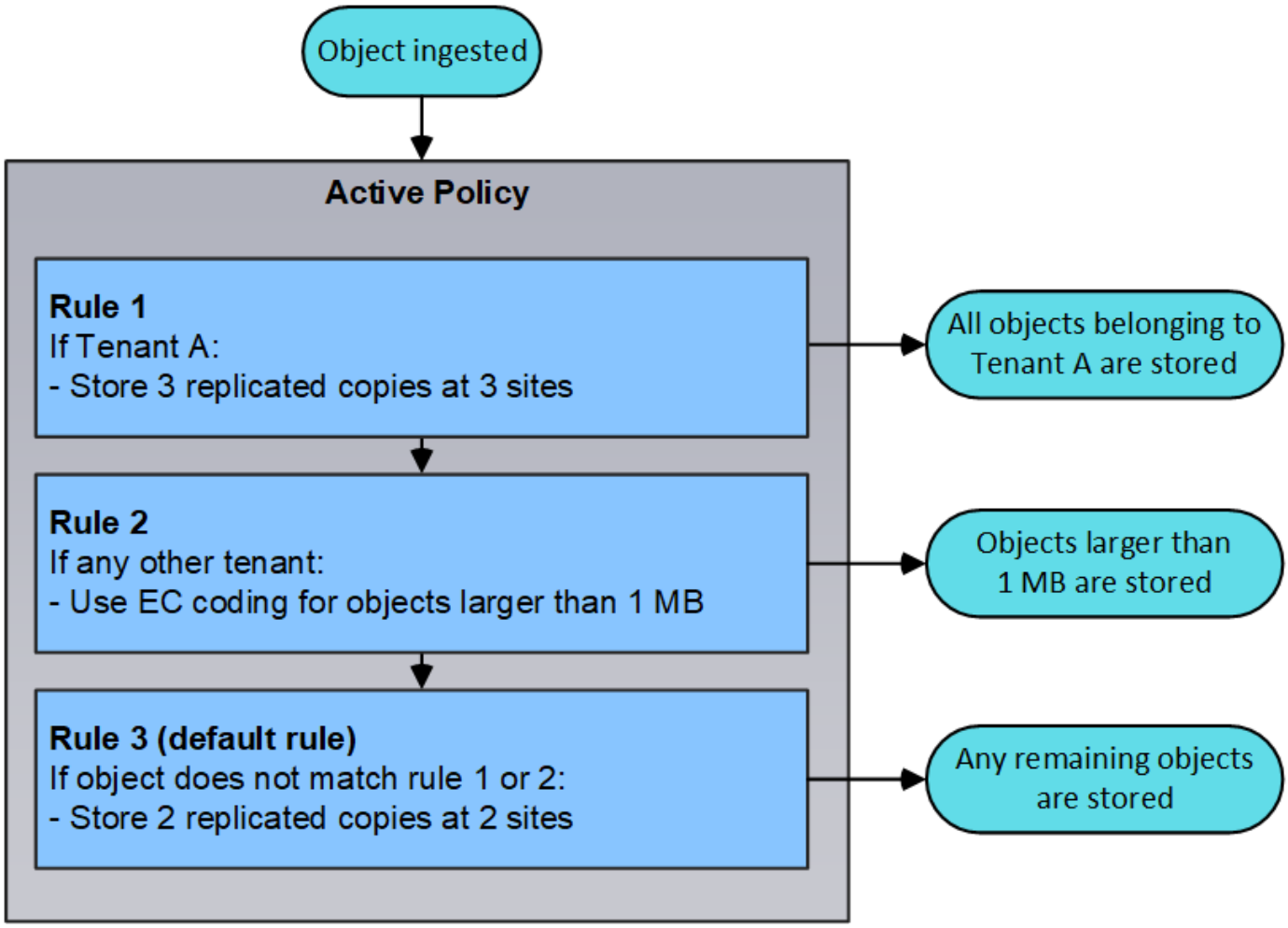
이 ILM 정책은 세 가지 ILM 규칙을 사용합니다.



이 예제에서 규칙 1은 테넌트 A에 속하는 모든 객체를 일치시킵니다 이러한 오브젝트는 3개의 사이트에 3개의 복제된 복사본으로 저장됩니다. 다른 테넌트에 속한 개체는 규칙 1에 의해 일치하지 않으므로 규칙 2에 대해 평가됩니다.

규칙 2는 다른 테넌트의 모든 객체를 일치하지만 1MB 이상인 경우에만 일치합니다. 이러한 큰 오브젝트는 3개의 사이트에서 6+3 삭제 코딩을 사용하여 저장됩니다. 규칙 2가 1MB 이하의 객체와 일치하지 않으므로 규칙 3에 대해 이러한 객체가 평가됩니다.

규칙 3은 정책의 마지막 기본 규칙이며 필터를 사용하지 않습니다. 규칙 3은 규칙 1 또는 규칙 2(1MB 이하의 테넌트 A에 속하지 않는 객체)에 의해 일치하지 않는 모든 객체의 복제된 복제본을 두 개 만듭니다.

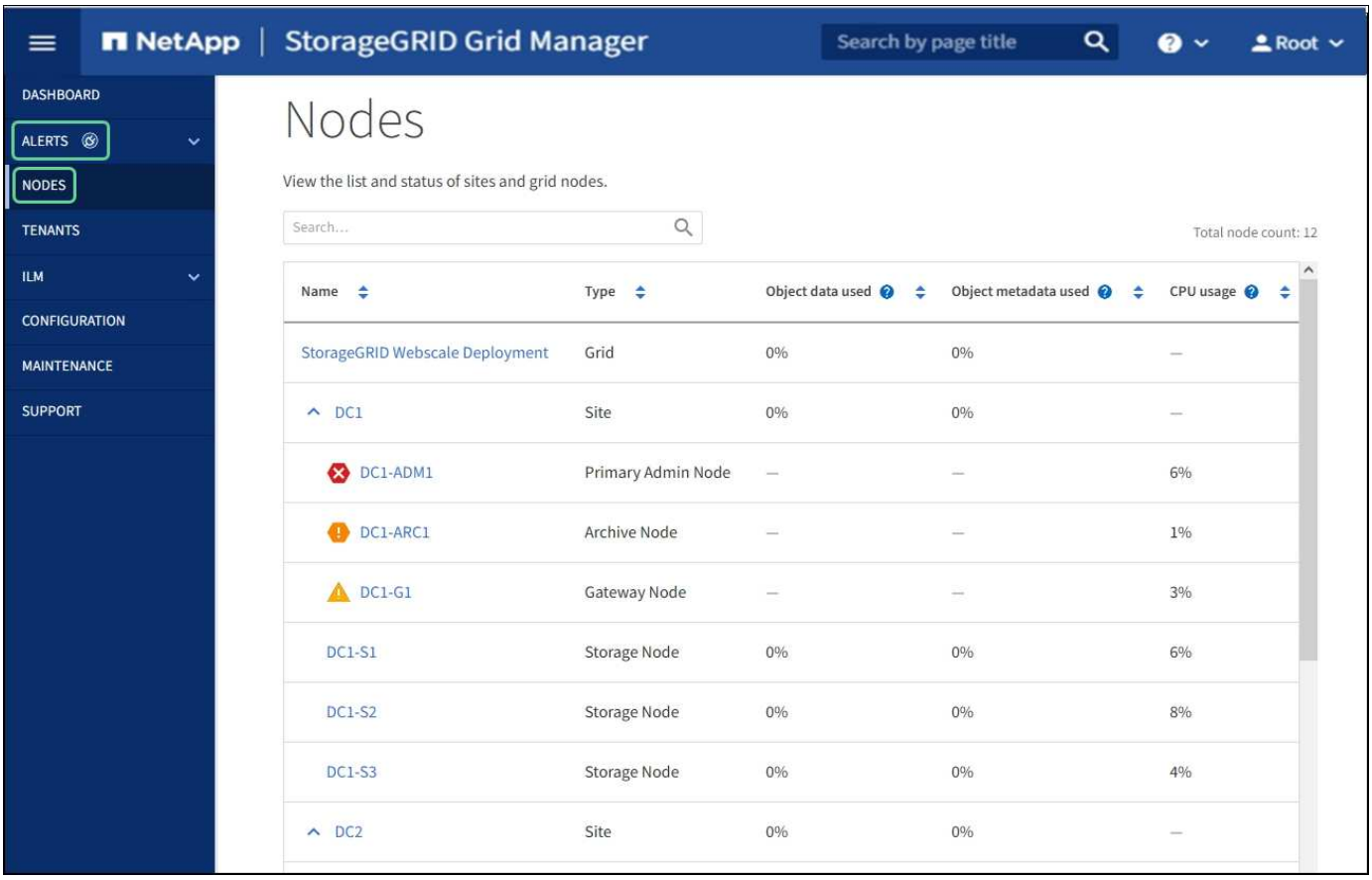


- 관련 정보 *
- ILM을 사용하여 개체를 관리합니다

작업을 모니터링합니다

노드 페이지를 봅니다

대시보드에서 제공하는 것보다 StorageGRID 시스템에 대한 자세한 정보가 필요한 경우 노드 페이지를 사용하여 전체 그리드, 그리드의 각 사이트 및 사이트의 각 노드에 대한 메트릭을 볼 수 있습니다.



노드 테이블에는 StorageGRID 시스템의 모든 사이트 및 노드가 나열됩니다. 각 노드에 대한 요약 정보가 표시됩니다. 노드에 활성 경고가 있는 경우 노드 이름 옆에 아이콘이 표시됩니다. 노드가 연결되어 있고 활성 경고가 없는 경우 아이콘이 표시되지 않습니다.

연결 상태 아이콘

- * 연결되지 않음 - 알 수 없음 * : 알 수 없는 이유로 노드가 그리드에 연결되어 있지 않습니다. 예를 들어, 노드 간 네트워크 연결이 끊어지거나 전원이 꺼졌습니다. 노드 * 와 통신할 수 없음 알림도 트리거될 수 있습니다. 다른 알림도 활성 상태일 수 있습니다. 이 상황은 즉각적인 주의가 필요합니다.

  관리되는 종료 작업 중에 노드가 알 수 없음으로 나타날 수 있습니다. 이러한 경우 알 수 없음 상태를 무시할 수 있습니다.

- * 연결되지 않음 - 관리 중단 * : 노드가 예상 이유로 그리드에 연결되어 있지 않습니다. 예를 들어, 노드의 노드 또는 서비스가 정상적으로 종료되었거나 노드가 재부팅 중이거나 소프트웨어가 업그레이드 중입니다. 하나 이상의 경고가 활성 상태일 수도 있습니다.

노드가 그리드에서 분리되면 기본 경고가 있을 수 있지만 ""연결되지 않음" 아이콘만 나타납니다. 노드의 활성 알림을 보려면 노드를 선택합니다.

경고 아이콘

노드에 대한 활성 경고가 있는 경우 노드 이름 옆에 다음 아이콘 중 하나가 표시됩니다.

- * 심각 * : StorageGRID 노드나 서비스의 정상적인 작동을 중지해 온 비정상적인 조건이 존재합니다. 기본

문제를 즉시 해결해야 합니다. 문제가 해결되지 않으면 서비스가 중단되거나 데이터가 손실될 수 있습니다.

- * 주 * : 현재 작업에 영향을 미치거나 위험 경고에 대한 임계값에 근접한 비정상적인 상태가 존재합니다. StorageGRID 노드나 서비스의 정상 작동을 비정상적인 상태로 중지하지 않도록 주요 경고를 조사하고 모든 기본 문제를 해결해야 합니다.
- * 보조 * : 시스템이 정상적으로 작동하지만 시스템이 계속 작동할 경우 시스템 기능에 영향을 줄 수 있는 비정상적인 상태가 존재합니다. 보다 심각한 문제를 초래하지 않도록 자체적으로 명확하지 않은 사소한 경고를 모니터링하고 해결해야 합니다.

시스템, 사이트 또는 노드에 대한 세부 정보입니다

사용 가능한 정보를 보려면 다음과 같이 그리드, 사이트 또는 노드의 이름을 선택합니다.

- 전체 StorageGRID 시스템에 대한 통계 요약을 보려면 그리드 이름을 선택합니다. (스크린샷은 StorageGRID 배포라는 시스템을 보여 줍니다.)
- 특정 데이터 센터 사이트를 선택하면 해당 사이트의 모든 노드에 대한 통계 요약을 볼 수 있습니다.
- 특정 노드를 선택하여 해당 노드에 대한 세부 정보를 봅니다.

노드 페이지의 탭입니다

노드 페이지 맨 위의 탭은 왼쪽의 트리에서 선택한 항목을 기반으로 합니다.

탭 이름	설명	에 포함
개요	• 각 노드에 대한 기본 정보를 제공합니다. • 노드에 영향을 주는 활성 경고를 표시합니다.	모든 노드
하드웨어	• 각 노드의 CPU 사용률 및 메모리 사용량을 표시합니다 • 어플라이언스 노드의 경우 에 추가 하드웨어 정보가 나와 있습니다.	모든 노드
네트워크	네트워크 인터페이스를 통해 수신 및 전송된 네트워크 트래픽을 보여 주는 그래프를 표시합니다. 단일 노드의 보기에는 노드에 대한 추가 정보가 표시됩니다.	모든 노드, 각 사이트 및 전체 그리드
스토리지	• 각 노드의 디스크 디바이스 및 볼륨에 대한 자세한 내용은 에 나와 있습니다. • 스토리지 노드, 각 사이트 및 전체 그리드에는 시간에 따라 사용된 오브젝트 데이터 스토리지 및 메타데이터 스토리지를 보여 주는 그래프가 포함됩니다.	모든 노드, 각 사이트 및 전체 그리드
오브젝트	• S3, Swift 수집 및 검색 속도에 대한 정보를 제공합니다. • 스토리지 노드의 경우 메타데이터 저장소 쿼리 및 백그라운드 확인에 대한 개체 수와 정보를 제공합니다.	스토리지 노드, 각 사이트 및 전체 그리드

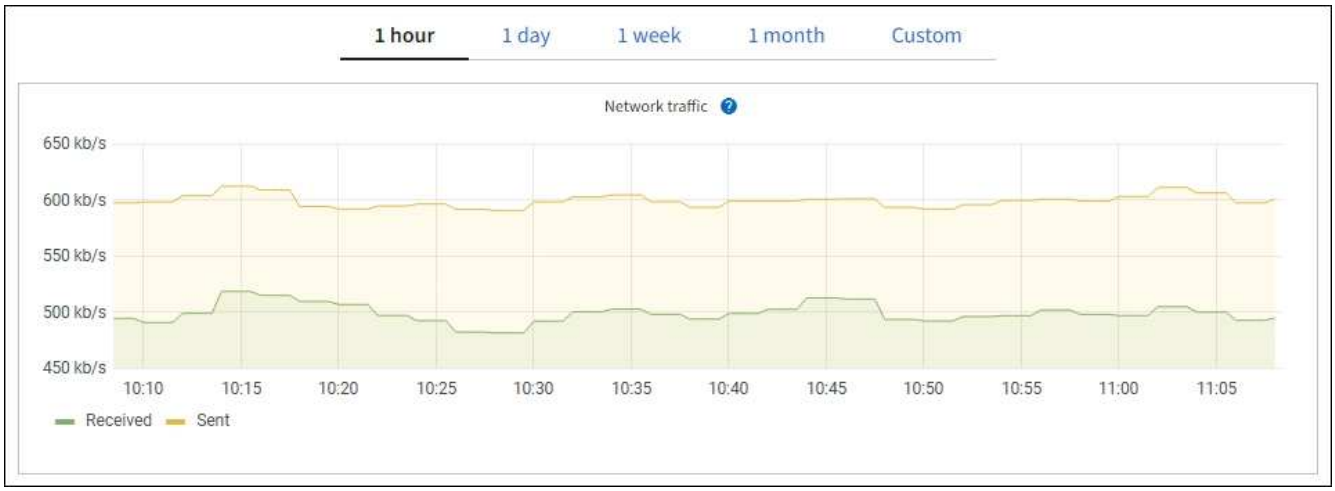
탭 이름	설명	에 포함
ILM을 참조하십시오	ILM(정보 수명 주기 관리) 작업에 대한 정보를 제공합니다. • 스토리지 노드의 경우, 삭제 코딩 개체에 대한 ILM 평가 및 백그라운드 검증에 대한 세부 정보를 제공합니다. • 각 사이트 및 전체 그리드에 대해 시간의 경과에 따른 ILM 대기열 그래프를 표시합니다. • 전체 그리드에서 는 모든 개체에 대한 전체 ILM 스캔을 완료하는 데 필요한 예상 시간을 제공합니다.	스토리지 노드, 각 사이트 및 전체 그리드
로드 밸런서	부하 분산 서비스와 관련된 성능 및 진단 그래프를 포함합니다. • 각 사이트에 대해 해당 사이트의 모든 노드에 대한 통계를 집계한 요약을 제공합니다. • 전체 그리드에서 는 모든 사이트에 대한 통계를 집계한 요약을 제공합니다.	관리 노드 및 게이트웨이 노드, 각 사이트 및 전체 그리드
플랫폼 서비스	사이트의 S3 플랫폼 서비스 작업에 대한 정보를 제공합니다.	있습니다
SANtricity 시스템 관리자	SANtricity 시스템 관리자에 대한 액세스를 제공합니다. SANtricity 시스템 관리자는 스토리지 컨트롤러에 대한 하드웨어 진단 및 환경 정보와 드라이브 관련 문제를 검토할 수 있습니다.	스토리지 어플라이언스 노드 • 참고 *: 스토리지 어플라이언스의 컨트롤러 펌웨어가 8.70(11.70) 이전인 경우 SANtricity 시스템 관리자 탭이 나타나지 않습니다.

Prometheus 측정 지표

관리 노드의 Prometheus 서비스는 모든 노드의 서비스에서 시계열 메트릭을 수집합니다.

Prometheus에서 수집한 메트릭은 Grid Manager의 여러 위치에서 사용됩니다.

- * 노드 페이지 *: 노드 페이지에서 사용할 수 있는 탭의 그래프와 차트 Grafana 시각화 도구를 사용하여 Prometheus에서 수집한 시계열 메트릭을 표시합니다. Grafana는 시계열 데이터를 그래프 및 차트 형식으로 표시하며, Prometheus는 백엔드 데이터 소스로 사용됩니다.



- * 알림 *: Prometheus 메트릭을 사용하는 알림 규칙 조건이 true로 평가되면 특정 심각도 수준에서 경고가 트리거됩니다.
- * 그리드 관리 API *: 사용자 지정 경고 규칙이나 외부 자동화 도구에서 Prometheus 메트릭을 사용하여 StorageGRID 시스템을 모니터링할 수 있습니다. Grid Management API에서 Prometheus 메트릭의 전체 목록을 확인할 수 있습니다. (Grid Manager 상단에서 도움말 아이콘을 선택하고 * API Documentation * > * metrics * 를 선택합니다.) 1,000개 이상의 메트릭을 사용할 수 있지만 가장 중요한 StorageGRID 작업을 모니터링하는 데 상대적으로 적은 수의 메트릭만 필요합니다.

> 이름에 _private_이 포함된 메트릭은 내부 전용이며 StorageGRID 릴리스 간에 예고 없이 변경될 수 있습니다.

- 지원 * > * 도구 * > * 진단 * 페이지 및 * 지원 * > * 도구 * > * 메트릭 * 페이지: 이 페이지는 주로 기술 지원 부서에서 사용하기 위한 것으로 Prometheus 메트릭의 값을 사용하는 다양한 도구와 차트를 제공합니다.

> 메트릭 페이지의 일부 기능 및 메뉴 항목은 의도적으로 작동하지 않으며 변경될 수 있습니다.

StorageGRID 속성

속성 StorageGRID 시스템의 여러 기능에 대한 값 및 상태를 보고합니다. 특성 값은 각 그리드 노드, 각 사이트 및 전체 그리드에 대해 사용할 수 있습니다.

StorageGRID 속성은 그리드 관리자의 여러 위치에서 사용됩니다.

- * 노드 페이지 *: 노드 페이지에 표시되는 대부분의 값은 StorageGRID 속성입니다. (Prometheus 메트릭도 노드 페이지에도 표시됩니다.)
- * 알람 *: 속성이 정의된 임계값에 도달하면 StorageGRID 알람(레거시 시스템)이 특정 심각도 수준에서 트리거됩니다.
- * 그리드 토폴로지 트리 **:** 속성 값은 그리드 토폴로지 트리**(** 지원 * > * 도구 * > * 그리드 토폴로지 *)에 표시됩니다.
- * 이벤트 *: 시스템 이벤트는 네트워크 오류와 같은 오류를 포함하여 특정 특성에 노드에 대한 오류 또는 오류 조건이 기록될 때 발생합니다.

속성 값

속성은 최선의 노력을 바탕으로 보고되며 대략 정확합니다. 서비스 충돌 또는 그리드 노드 장애 및 재생성과 같은 일부

상황에서는 특성 업데이트가 손실될 수 있습니다.

또한 전파 지연으로 인해 속성 보고가 느려질 수 있습니다. 대부분의 속성에 대해 업데이트된 값은 고정된 간격으로 StorageGRID 시스템으로 전송됩니다. 시스템에서 업데이트가 표시되기까지 몇 분이 걸릴 수 있으며, 둘 이상의 특성이 동시에 변경되는 경우 약간 다른 시간에 보고할 수 있습니다.

관련 정보

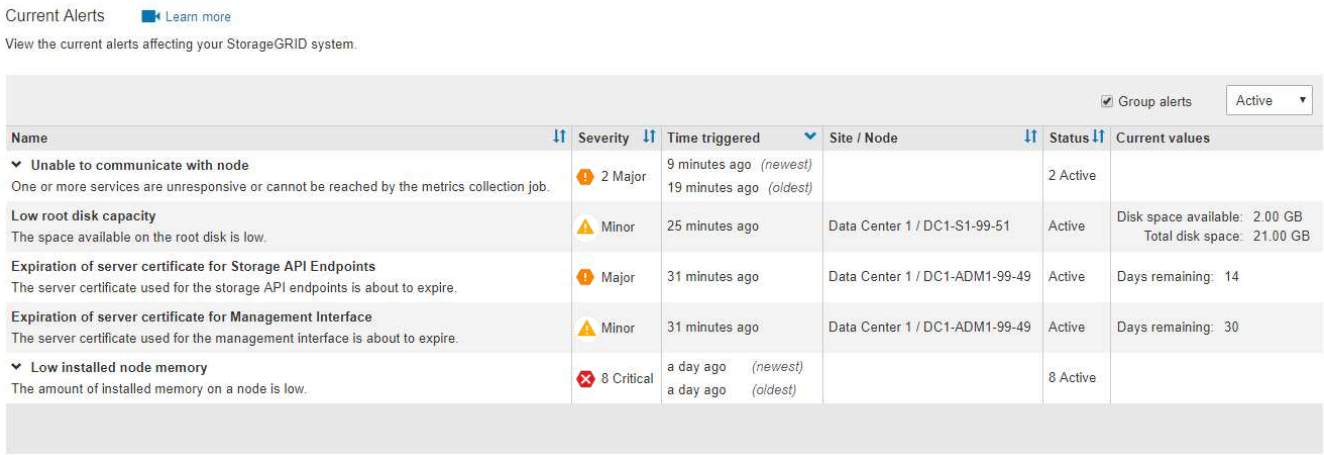
- 모니터링하고 문제를 해결합니다
- 경고를 모니터링하고 관리합니다
- StorageGRID 지원 옵션을 사용합니다

경고를 모니터링하고 관리합니다

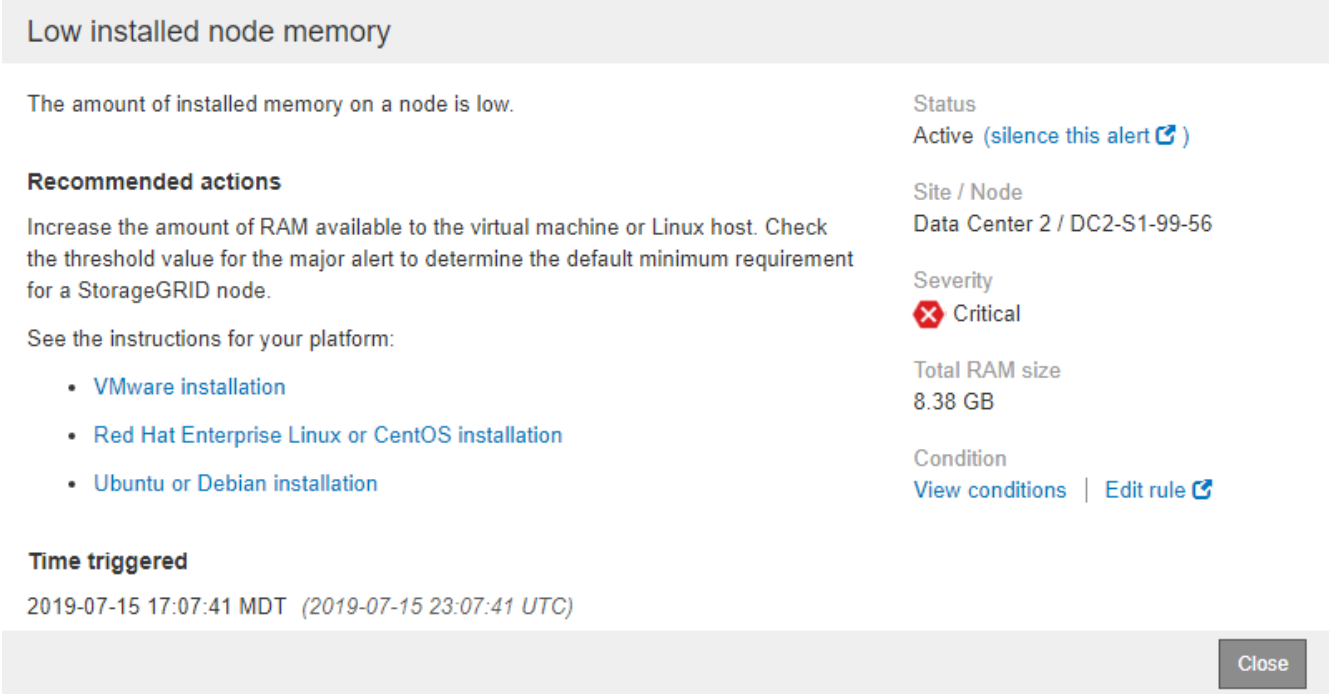
이 경고 시스템은 StorageGRID 작동 중에 발생할 수 있는 문제를 감지, 평가 및 해결하기 위한 사용이 간편한 인터페이스를 제공합니다.

경고 시스템은 StorageGRID 시스템에서 발생할 수 있는 문제를 모니터링하는 기본 도구로 설계되었습니다.

- 알림 시스템은 시스템에서 실행 가능한 문제에 초점을 맞춥니다. 경고는 안전하게 무시할 수 있는 이벤트가 아니라 즉각적인 주의가 필요한 이벤트에 대해 트리거됩니다.
- Current Alerts 및 Resolved Alerts 페이지에서는 현재 및 과거 문제를 볼 수 있는 사용자 친화적인 인터페이스를 제공합니다. 개별 알림 및 알림 그룹을 기준으로 목록을 정렬할 수 있습니다. 예를 들어 모든 알림을 노드/사이트별로 정렬하여 특정 노드에 영향을 미치는 알림을 확인할 수 있습니다. 또는 특정 알림의 가장 최근 인스턴스를 찾기 위해 트리거된 시간을 기준으로 그룹의 알림을 정렬할 수 있습니다.
- 동일한 유형의 여러 알림이 하나의 이메일로 그룹화되어 알림 수가 줄어듭니다. 또한 동일한 유형의 여러 알림이 현재 경고 및 해결된 경고 페이지에 그룹으로 표시됩니다. 알림 그룹을 확장하고 축소하여 개별 알림을 표시하거나 숨길 수 있습니다. 예를 들어, 여러 노드에서 * 노드 * 경고와 통신할 수 없음 알림을 보고하는 경우 하나의 이메일만 전송되고 해당 알림은 현재 알림 페이지에 하나의 그룹으로 표시됩니다.



- 알림은 직관적인 이름과 설명을 사용하여 문제의 원인을 보다 빠르게 파악할 수 있도록 도와줍니다. 알림 알림에는 영향을 받는 노드 및 사이트에 대한 세부 정보, 알림 심각도, 알림 규칙이 트리거된 시간, 경고와 관련된 메트릭의 현재 값이 포함됩니다.
- 경고 이메일 알림 및 현재 경고 및 해결된 경고 페이지의 경고 목록은 경고 해결을 위한 권장 조치를 제공합니다. 이러한 권장 조치에는 보다 자세한 문제 해결 절차를 쉽게 찾아 액세스할 수 있도록 StorageGRID 문서에 대한 직접 링크가 포함되어 있는 경우가 많습니다.



> 기존 경보 시스템은 더 이상 사용되지 않습니다. 레거시 알람 시스템의 사용자 인터페이스 및 API는 향후 릴리즈에서 제거될 예정입니다. 경고 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

알림을 관리합니다

모든 StorageGRID 사용자는 경고를 볼 수 있습니다. 루트 액세스 또는 알림 관리 권한이 있는 경우 다음과 같이 알림을 관리할 수도 있습니다.

- 하나 이상의 심각도 수준에서 알림에 대한 알림을 일시적으로 억제해야 하는 경우 지정된 기간 동안 특정 알림 규칙을 쉽게 해제할 수 있습니다. 전체 그리드, 단일 사이트 또는 단일 노드에 대한 경고 규칙을 해제할 수 있습니다.
- 필요에 따라 기본 경고 규칙을 편집할 수 있습니다. 경고 규칙을 완전히 비활성화하거나 트리거 조건 및 기간을 변경할 수 있습니다.
- 사용자 정의 경고 규칙을 생성하여 자신의 상황과 관련된 특정 조건을 타겟팅하고 자신만의 권장 조치를 제공할 수 있습니다. 사용자 지정 알림의 조건을 정의하려면 Grid Management API의 Metrics 섹션에서 사용할 수 있는 Prometheus 메트릭을 사용하여 표현식을 생성합니다.

  예를 들어, 이 식을 사용하면 노드에 설치된 RAM의 양이 24,000,000,000,000바이트(24GB) 미만인 경우 경고가 트리거됩니다.

  ```
  node_memory_MemTotal < 24000000000
  ```

관련 정보

모니터링하고 문제를 해결합니다

SNMP 모니터링을 사용합니다

SNMP(Simple Network Management Protocol)를 사용하여 StorageGRID를 모니터링하려는

경우 그리드 관리자를 사용하여 SNMP 에이전트를 구성할 수 있습니다.

각 StorageGRID 노드는 MIB(Management Information Base)를 제공하는 SNMP 에이전트 또는 데몬을 실행합니다. StorageGRID MIB에는 알림 및 알람에 대한 테이블 및 알림 정의가 포함되어 있습니다. 각 StorageGRID 노드는 MIB-II 객체의 하위 세트도 지원합니다.

처음에는 모든 노드에서 SNMP가 사용되지 않습니다. SNMP 에이전트를 구성할 때 모든 StorageGRID 노드는 동일한 구성을 받습니다.

StorageGRID SNMP 에이전트는 세 가지 버전의 SNMP 프로토콜을 모두 지원합니다. 에이전트는 쿼리에 대한 읽기 전용 MIB 액세스를 제공하며 관리 시스템에 두 가지 유형의 이벤트 기반 알림을 보낼 수 있습니다.

- * 트랩 * 은 관리 시스템에서 확인이 필요하지 않은 SNMP 에이전트가 보낸 알림입니다. 트랩은 알림이 트리거되는 등 StorageGRID 내에 발생한 사항을 관리 시스템에 알리는 역할을 합니다. 트랩은 SNMP의 세 가지 버전에서 모두 지원됩니다.
- * 알림 * 은 트랩과 유사하지만 관리 시스템에서 확인을 요구합니다. SNMP 에이전트가 일정 시간 내에 승인을 받지 못하면 승인을 받거나 최대 재시도 값에 도달할 때까지 알림을 다시 보냅니다. SNMPv2c 및 SNMPv3에서 알림이 지원됩니다.

다음과 같은 경우 트랩 및 알림 알림이 전송됩니다.

- 기본 또는 사용자 지정 알림은 모든 심각도 수준에서 트리거됩니다. 경고에 대한 SNMP 알림을 표시하지 않으려면 경고에 대한 무음을 구성해야 합니다. 경고 알림은 선호하는 송신자가 되도록 구성된 관리 노드에서 보냅니다.
- 특정 알람(기존 시스템)은 지정된 심각도 수준 이상에서 트리거됩니다.

> 모든 알람 또는 알람 심각도에 대해 SNMP 알림이 전송되지 않습니다.

- 관련 정보 *
- 모니터링하고 문제를 해결합니다

감사 메시지를 검토합니다

감사 메시지를 통해 StorageGRID 시스템의 세부 작업을 보다 잘 이해할 수 있습니다. 감사 로그를 사용하여 문제를 해결하고 성능을 평가할 수 있습니다.

정상적인 시스템 작동 중에 모든 StorageGRID 서비스는 다음과 같이 감사 메시지를 생성합니다.

- 시스템 감사 메시지는 감사 시스템 자체, 그리드 노드 상태, 시스템 전체 작업 및 서비스 백업 작업과 관련되어 있습니다.
- 오브젝트 스토리지 감사 메시지는 오브젝트 스토리지 및 검색, 그리드 노드에서 그리드 노드 전송, 확인을 포함하여 StorageGRID 내의 오브젝트 스토리지 및 관리와 관련되어 있습니다.
- S3 또는 Swift 클라이언트 애플리케이션이 오브젝트 생성, 수정 또는 검색을 요청할 때 클라이언트 읽기 및 쓰기 감사 메시지가 기록됩니다.
- 관리 감사 메시지는 관리 API에 사용자 요청을 기록합니다.

각 관리 노드는 감사 메시지를 텍스트 파일에 저장합니다. 감사 공유에는 활성 파일(audit.log)과 이전 일로부터의 압축된 감사 로그가 포함됩니다. 또한 그리드의 각 노드는 제한된 양의 감사 메시지를 로컬 로그 파일(localaudit.log)에 저장합니다.

감사 로그에 쉽게 액세스할 수 있도록 NFS 및 CIFS에 대한 감사 공유에 대한 클라이언트 액세스를 구성할 수 있습니다(CIFS는 더 이상 사용되지 않음). 관리자 노드의 명령줄에서 직접 감사 로그 파일에 액세스할 수도 있습니다.

선택적으로 관리자 노드 및 로컬 노드에 저장된 감사 정보를 외부 syslog 서버로 보낼 수 있습니다. 외부 syslog 서버를 사용하면 감사 정보를 보다 쉽게 관리하고 네트워크 트래픽을 줄일 수 있습니다. 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다 를 참조하십시오.

감사 로그 파일, 감사 메시지 형식, 감사 메시지 유형 및 감사 메시지 분석에 사용할 수 있는 도구에 대한 자세한 내용은 을 참조하십시오 감사 메시지에 대한 지침. 감사 클라이언트 액세스를 구성하는 방법에 대한 자세한 내용은 을 참조하십시오 감사 클라이언트 액세스를 구성합니다.

관련 정보

- 감사 로그를 검토합니다
- StorageGRID 관리

유지 관리를 수행합니다

StorageGRID 시스템을 최신 상태로 유지하고 효율적으로 작동하도록 하기 위해 다양한 유지보수 절차를 수행합니다. Grid Manager는 유지보수 작업 수행 프로세스를 용이하게 하는 도구와 옵션을 제공합니다.

소프트웨어 업데이트

Grid Manager의 소프트웨어 업데이트 페이지에서 세 가지 유형의 소프트웨어 업데이트를 수행할 수 있습니다.

- StorageGRID 소프트웨어 업그레이드
- StorageGRID 핫픽스
- SANtricity OS 업그레이드

StorageGRID 소프트웨어 업그레이드

새로운 StorageGRID 기능 릴리스를 사용할 수 있는 경우 소프트웨어 업그레이드 페이지에서 필요한 파일을 업로드하고 StorageGRID 시스템을 업그레이드하는 과정을 안내합니다. 기본 관리 노드에서 모든 데이터 센터 사이트의 모든 그리드 노드를 업그레이드해야 합니다.

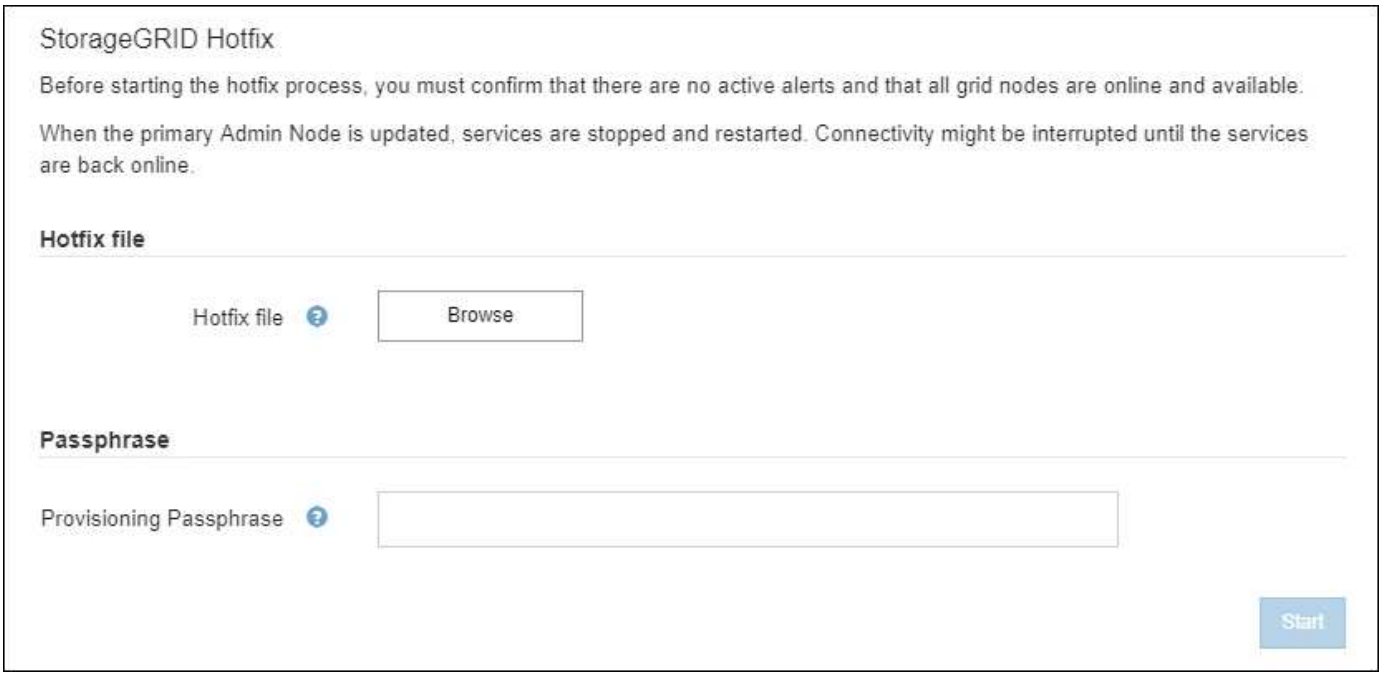
StorageGRID 소프트웨어를 업그레이드하는 동안 클라이언트 애플리케이션에서 오브젝트 데이터를 계속 수집하고 검색할 수 있습니다.

핫픽스

기능 릴리즈 간에 소프트웨어 문제가 탐지 및 해결되면 StorageGRID 시스템에 핫픽스를 적용해야 할 수 있습니다.

StorageGRID 핫픽스에는 기능 또는 패치 릴리스 외부에서 사용할 수 있는 소프트웨어 변경 사항이 포함되어 있습니다. 동일한 변경 사항이 향후 릴리스에 포함됩니다.

아래 표시된 StorageGRID 핫픽스 페이지에서 핫픽스 파일을 업로드할 수 있습니다.



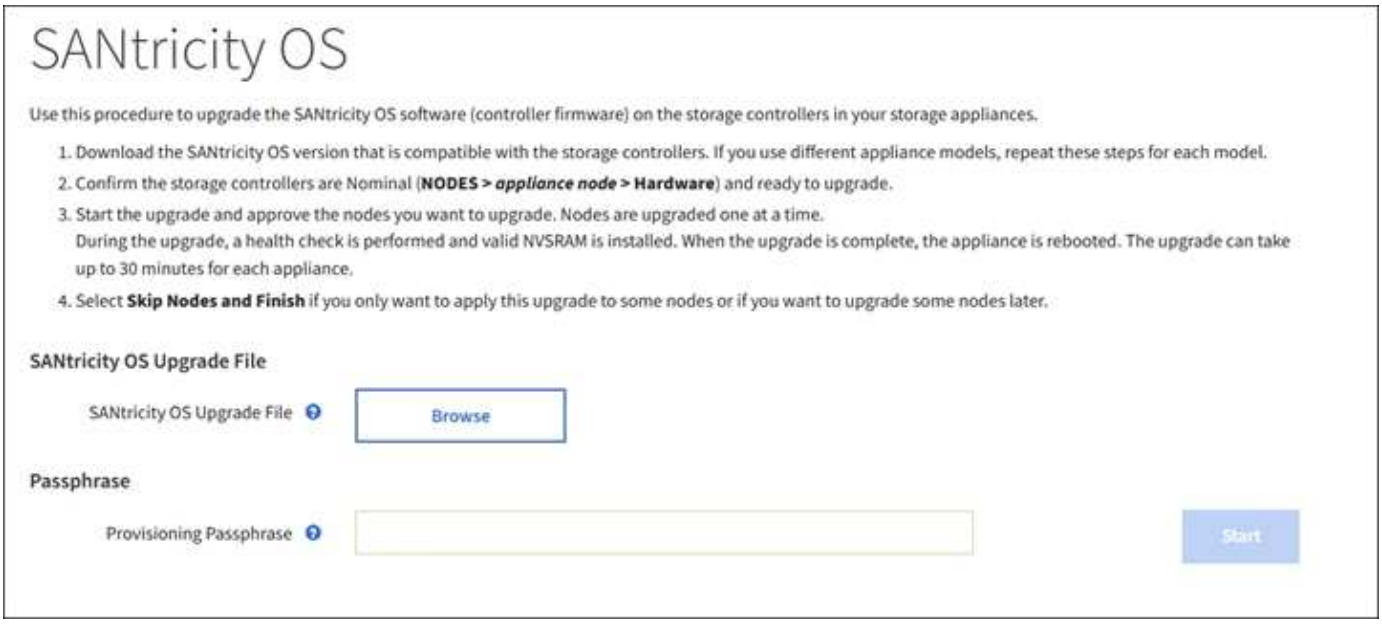
핫픽스가 먼저 기본 관리자 노드에 적용됩니다. 그런 다음 StorageGRID 시스템의 모든 노드에서 동일한 소프트웨어 버전이 실행될 때까지 다른 그리드 노드에 대한 핫픽스 응용 프로그램을 승인해야 합니다. 개별 그리드 노드, 그리드 노드 그룹 또는 모든 그리드 노드를 승인하도록 선택하여 승인 순서를 사용자 지정할 수 있습니다.

> 모든 그리드 노드는 새 핫픽스 버전으로 업데이트되지만 핫픽스의 실제 변경 사항은 특정 노드 유형의 특정 서비스에만 영향을 줄 수 있습니다. 예를 들어 핫픽스는 스토리지 노드의 LDR 서비스에만 영향을 줄 수 있습니다.

SANtricity OS 업그레이드

컨트롤러가 최적의 상태로 작동하지 않으면 스토리지 어플라이언스의 스토리지 컨트롤러에서 SANtricity OS 소프트웨어를 업그레이드해야 할 수 있습니다. SANtricity OS 파일을 StorageGRID 시스템의 기본 관리 노드에 업로드하고 그리드 관리자에서 업그레이드를 적용할 수 있습니다.

아래 표시된 SANtricity 페이지에서 SANtricity OS 업그레이드 파일을 업로드할 수 있습니다.

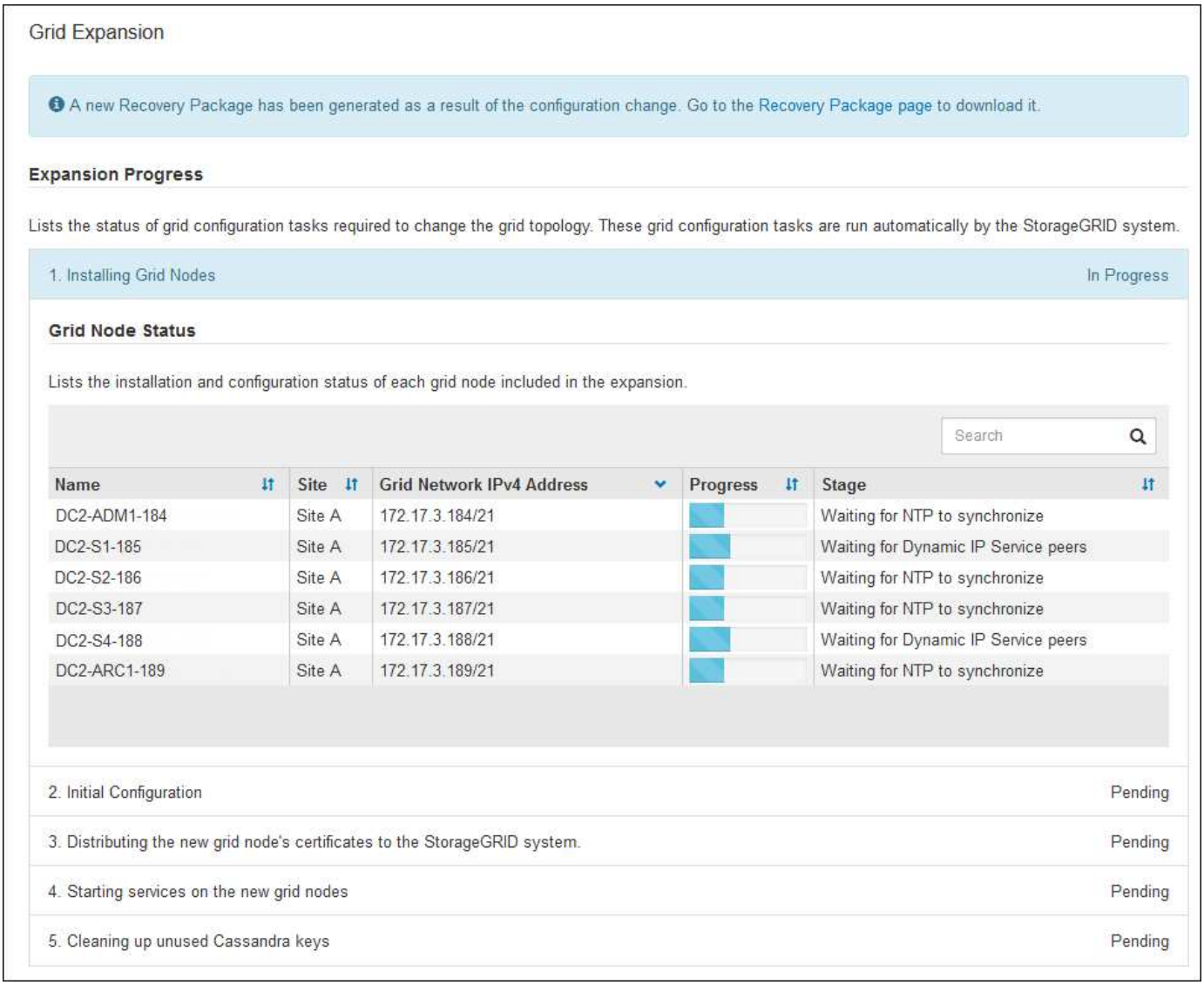


파일을 업로드한 후 개별 스토리지 노드 또는 모든 노드의 업그레이드를 승인할 수 있습니다. 노드를 선별적으로 승인하는 기능을 사용하면 업그레이드를 더 쉽게 예약할 수 있습니다. 업그레이드를 위해 노드를 승인한 후, 시스템은 상태 점검을 수행하고 해당 노드에 해당하는 업그레이드를 설치합니다.

확장 절차

스토리지 노드에 스토리지 볼륨을 추가하거나, 기존 사이트에 새 그리드 노드를 추가하거나, 새 데이터 센터 사이트를 추가하여 StorageGRID 시스템을 확장할 수 있습니다. SG6060 또는 SG6060X 스토리지 어플라이언스를 사용하는 스토리지 노드가 있는 경우 하나 또는 두 개의 확장 쉘프를 추가하여 노드의 스토리지 용량을 두 배 또는 세 배로 늘릴 수 있습니다.

현재 시스템의 운영을 중단하지 않고도 확장을 수행할 수 있습니다. 노드 또는 사이트를 추가할 때는 먼저 새 노드를 배포한 다음 그리드 확장 페이지에서 확장 절차를 수행합니다.

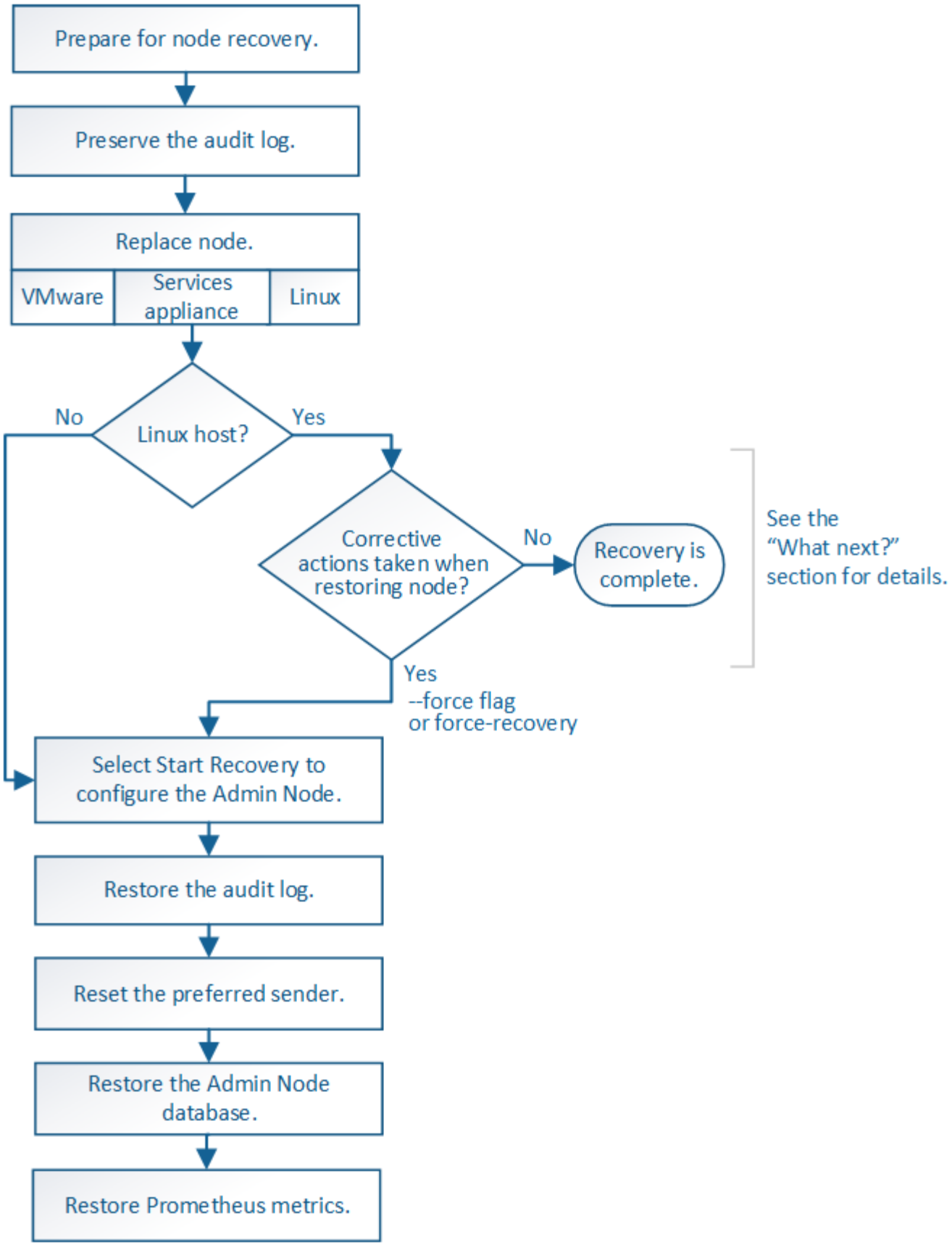


노드 복구 절차

하드웨어, 가상화, 운영 체제 또는 소프트웨어 장애로 인해 노드가 작동 불능 또는 불안정해질 경우 그리드 노드에 장애가 발생할 수 있습니다.

그리드 노드를 복구하는 단계는 그리드 노드가 호스팅되는 플랫폼과 그리드 노드의 유형에 따라 다릅니다. 각 유형의 그리드 노드에는 정확히 따라야 하는 특정 복구 절차가 있습니다. 일반적으로 장애가 발생한 그리드 노드의 데이터를 가능한 한 보존하고, 장애가 발생한 노드를 복구 또는 교체하고, 복구 페이지를 사용하여 교체 노드를 구성하고, 노드의 데이터를 복구하려고 합니다.

예를 들어 이 순서도는 관리자 노드에 장애가 발생한 경우 복구 절차를 보여 줍니다.



해체 절차

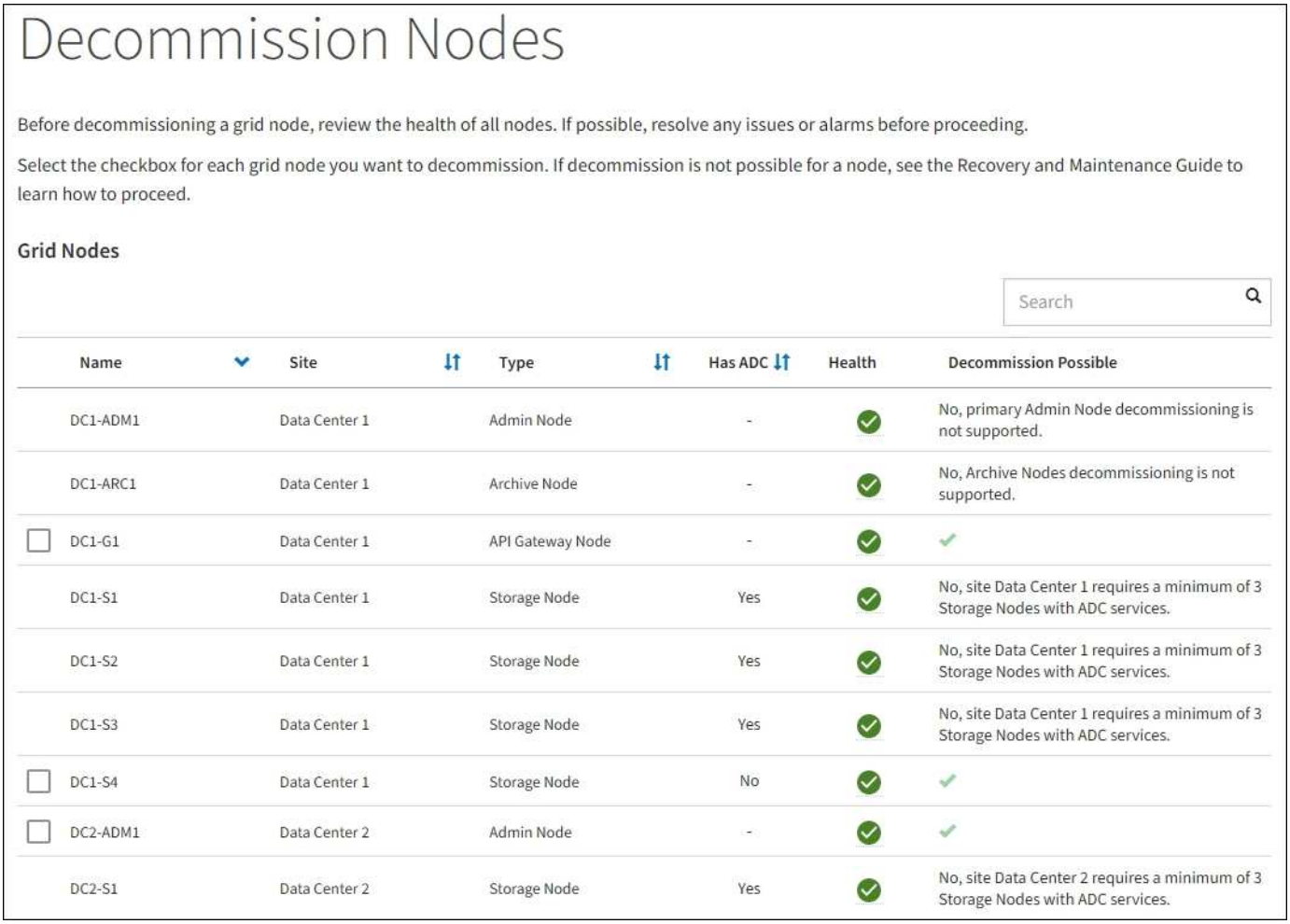
StorageGRID 시스템에서 그리드 노드 또는 전체 데이터 센터 사이트를 영구적으로 제거할 수 있습니다.

예를 들어 다음과 같은 경우 하나 이상의 그리드 노드를 해제할 수 있습니다.

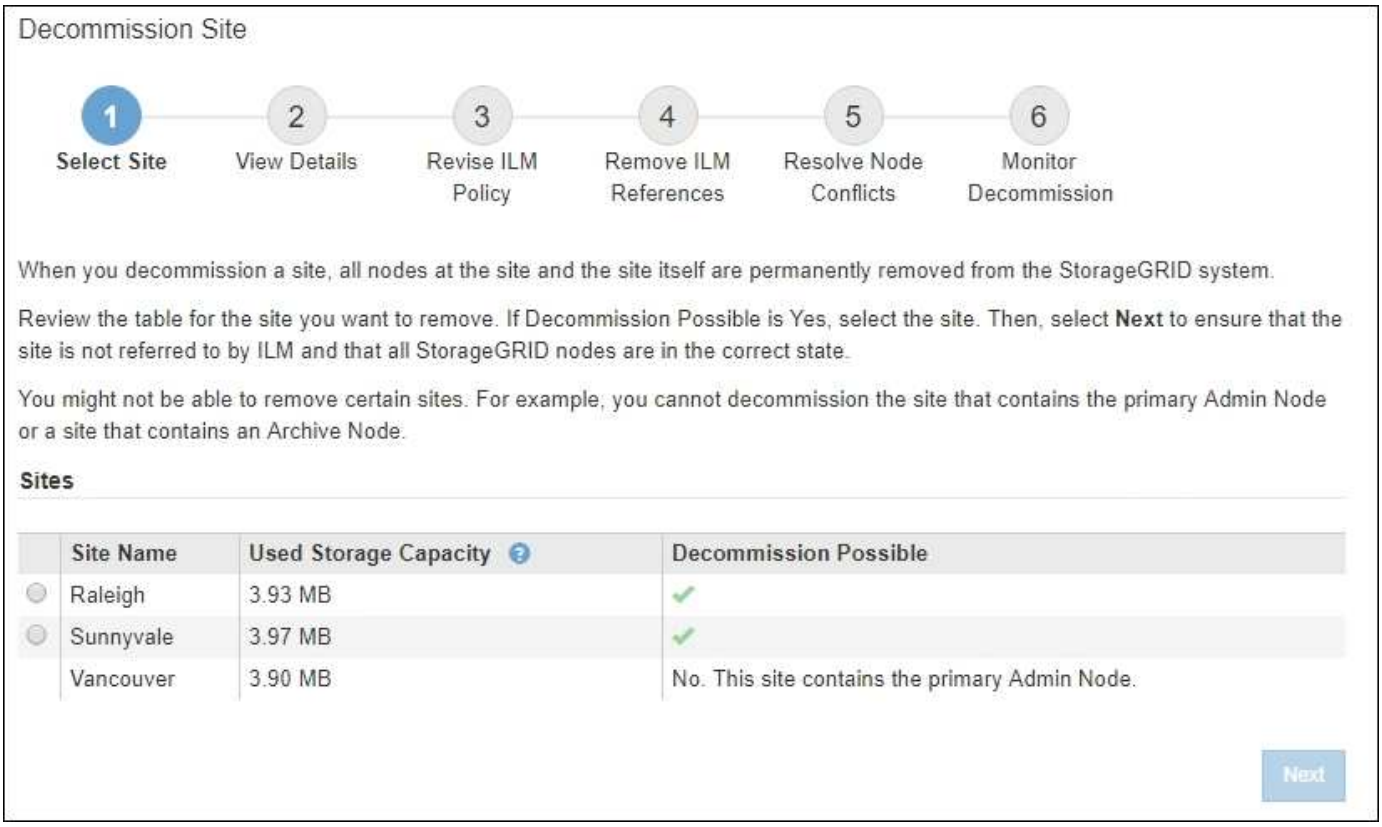
- 시스템에 더 큰 스토리지 노드를 추가했으며 객체를 보존하면서 하나 이상의 더 작은 스토리지 노드를 제거하려는 경우
- 필요한 총 스토리지 용량이 줄어듭니다.
- 더 이상 게이트웨이 노드 또는 비 기본 관리 노드가 필요하지 않습니다.
- 그리드에는 복구하거나 다시 온라인으로 전환할 수 없는 연결 해제된 노드가 포함되어 있습니다.

Grid Manager에서 Decommission Nodes 페이지를 사용하여 다음과 같은 유형의 그리드 노드를 제거할 수 있습니다.

- 특정 요구 사항을 지원할 수 있는 충분한 노드가 사이트에 남아 있지 않는 한 스토리지 노드
- 게이트웨이 노드
- 운영 관리자 노드가 아닌 노드



Grid Manager의 서비스 해제 사이트 페이지를 사용하여 사이트를 제거할 수 있습니다. 연결된 사이트 파기는 운영 사이트를 제거하고 데이터를 보존합니다. 연결이 끊긴 사이트 서비스 해제는 장애가 발생한 사이트를 제거하지만 데이터를 보존하지는 않습니다. 사이트 해제 마법사는 사이트 선택, 사이트 세부 정보 보기, ILM 정책 수정, ILM 규칙에서 사이트 참조 제거 및 노드 충돌 해결 프로세스를 안내합니다.



네트워크 유지보수 절차

수행해야 할 네트워크 유지 관리 절차 중 일부는 다음과 같습니다.

- 그리드 네트워크에서 서브넷을 업데이트합니다
- IP 변경 도구를 사용하여 그리드 배포 중에 처음 설정된 네트워킹 구성을 변경합니다
- DNS(Domain Name System) 서버 추가, 제거 또는 업데이트
- 그리드 노드 간에 데이터가 정확하게 동기화되도록 NTP(네트워크 시간 프로토콜) 서버를 추가, 제거 또는 업데이트합니다
- 나머지 그리드에서 격리되었을 수 있는 노드에 대한 네트워크 연결을 복원합니다

호스트 레벨 및 미들웨어 절차

일부 유지 관리 절차는 Linux 또는 VMware에 배포되거나 StorageGRID 솔루션의 다른 구성 요소에 적용되는 StorageGRID 노드에만 적용됩니다. 예를 들어 그리드 노드를 다른 Linux 호스트로 마이그레이션하거나 TSM(Tivoli Storage Manager)에 연결된 아카이브 노드에서 유지 관리를 수행할 수 있습니다.

어플라이언스 노드 클론 복제

어플라이언스 노드 클론 복제를 사용하면 그리드에 있는 기존 어플라이언스 노드를 동일한 논리적 StorageGRID 사이트에 포함된 새로운 설계나 향상된 기능의 어플라이언스로 쉽게 교체할 수 있습니다. 이 프로세스는 모든 데이터를 새 어플라이언스에 전송하여 이전 어플라이언스 노드를 교체하고 이전 어플라이언스를 설치 전 상태로 둡니다. 클론 복제는 수행이 용이한 하드웨어 업그레이드 프로세스를 제공하며 어플라이언스 교체를 위한 대체 방법을 제공합니다.

그리드 노드 절차

특정 그리드 노드에서 특정 절차를 수행해야 할 수 있습니다. 예를 들어 그리드 노드를 재부팅하거나 특정 그리드 노드

서비스를 수동으로 중지하고 다시 시작해야 할 수 있습니다. 일부 그리드 노드 절차는 그리드 관리자에서 수행할 수 있으며, 그리드 노드에 로그인하여 노드의 명령줄을 사용해야 하는 경우도 있습니다.

관련 정보

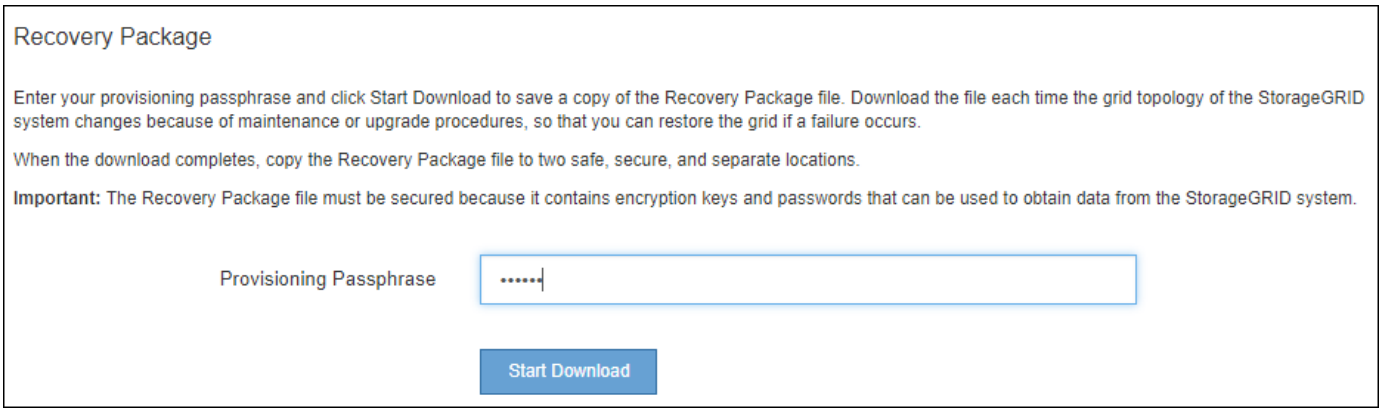
- StorageGRID 관리
- 소프트웨어 업그레이드
- 그리드를 확장합니다
- 복구 및 유지 관리

복구 패키지를 다운로드합니다

복구 패키지는 다운로드 가능한 .zip 파일로, StorageGRID 시스템을 설치, 확장, 업그레이드 및 유지 관리하는 데 필요한 배포 관련 파일 및 소프트웨어를 포함합니다.

또한 복구 패키지 파일에는 서버 호스트 이름 및 IP 주소를 포함한 시스템 관련 구성 및 통합 정보와 시스템 유지 관리, 업그레이드 및 확장 시 필요한 기밀 암호가 포함되어 있습니다. 기본 관리 노드의 장애로부터 복구하려면 복구 패키지가 필요합니다.

StorageGRID 시스템을 설치할 때 복구 패키지 파일을 다운로드하고 이 파일의 내용에 성공적으로 액세스할 수 있는지 확인해야 합니다. 또한 유지 관리 또는 업그레이드 절차로 인해 StorageGRID 시스템의 그리드 토폴로지가 변경될 때마다 파일을 다운로드해야 합니다.



복구 패키지 파일을 다운로드하고 콘텐츠를 추출할 수 있는지 확인한 후 복구 패키지 파일을 두 개의 안전하고 별도의 위치에 복사합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

관련 정보

- 소프트웨어 업그레이드
- 그리드를 확장합니다
- 복구 및 유지 관리

StorageGRID 지원 옵션을 사용합니다

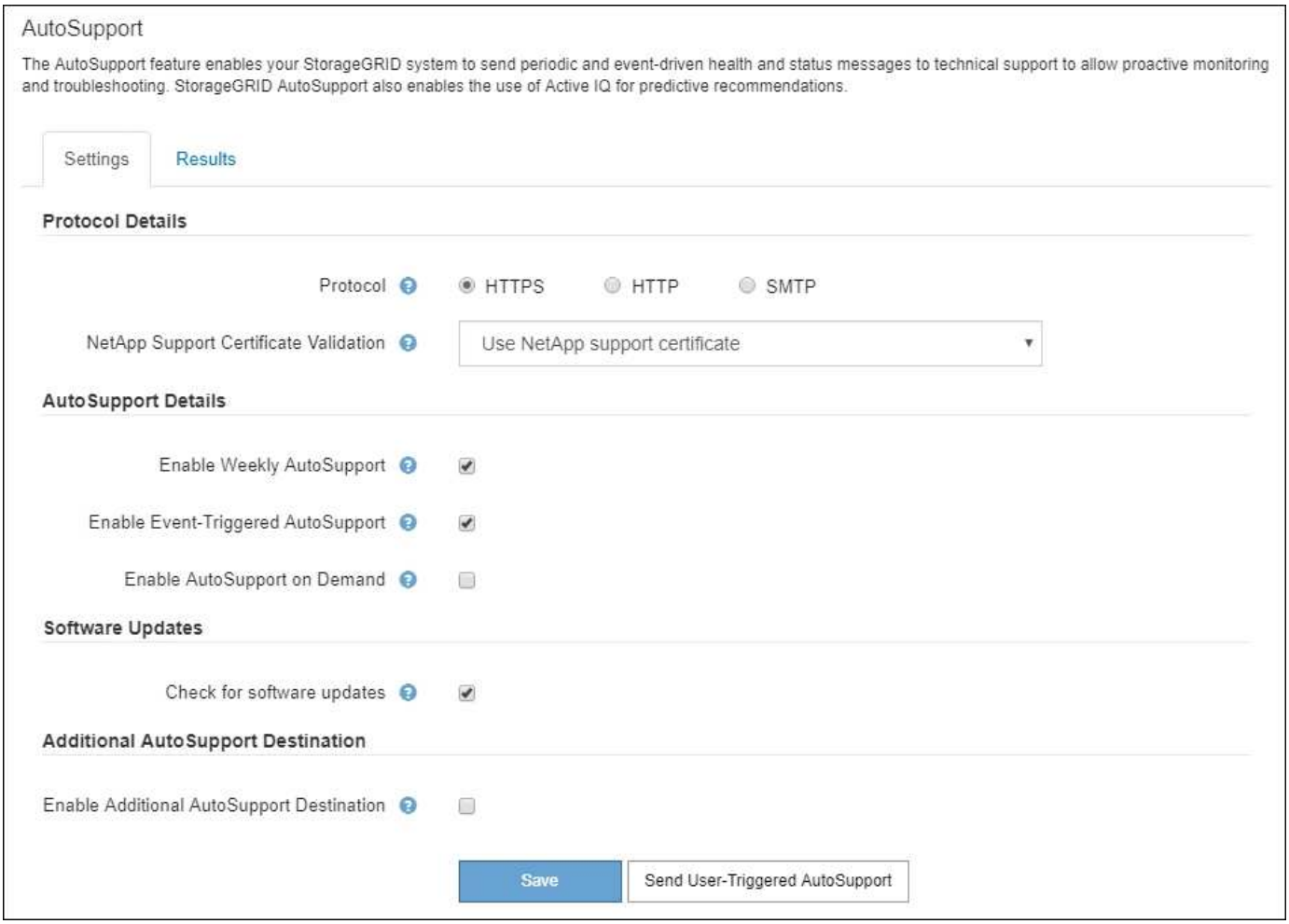
그리드 관리자는 StorageGRID 시스템에 문제가 발생한 경우 기술 지원 부서에 문의할 수 있는

옵션을 제공합니다.

AutoSupport를 구성합니다

AutoSupport 기능을 사용하면 StorageGRID 시스템에서 상태 및 상태 메시지를 기술 지원 부서에 보낼 수 있습니다. AutoSupport를 사용하면 문제를 빠르게 확인하고 해결할 수 있습니다. 기술 지원 부서에서는 시스템의 스토리지 요구 사항을 모니터링하여 새 노드나 사이트를 추가해야 하는지 여부를 결정할 수 있습니다. 선택적으로 AutoSupport 메시지를 하나의 추가 대상으로 보내도록 구성할 수 있습니다.

그리드 관리자(* 지원 * > * 도구 * > * AutoSupport)를 사용하여 **AutoSupport**를 구성합니다**. AutoSupport** 페이지에는 * 설정 * 및 * 결과 * 라는 두 개의 탭이 있습니다.



AutoSupport 메시지에 포함된 정보입니다

AutoSupport 메시지에는 다음과 같은 정보가 포함됩니다.

- StorageGRID 소프트웨어 버전입니다
- 운영 체제 버전입니다
- 시스템 레벨 및 위치 레벨 속성 정보
- 최근 알림 및 알람(기존 시스템)
- 내역 데이터를 포함하여 모든 그리드 작업의 현재 상태입니다

- 관리 노드 데이터베이스 사용
- 손실되거나 누락된 개체 수입니다
- 그리드 구성 설정
- NMS 요소
- 활성 ILM 정책
- 프로비저닝된 그리드 사양 파일
- 진단 메트릭

StorageGRID를 처음 설치할 때 AutoSupport 기능 및 개별 AutoSupport 옵션을 활성화하거나 나중에 활성화할 수 있습니다. AutoSupport가 활성화되어 있지 않으면 그리드 관리자 대시보드에 메시지가 나타납니다. 이 메시지에는 AutoSupport 구성 페이지에 대한 링크가 포함되어 있습니다.

메시지를 닫으면 AutoSupport가 비활성화된 경우에도 브라우저 캐시가 지워질 때까지 메시지가 다시 표시되지 않습니다.

Active IQ를 사용합니다

Active IQ는 NetApp 설치 기반에서 예측 분석 및 커뮤니티 지혜를 활용하는 클라우드 기반 디지털 자문업체입니다. 지속적인 위험 평가, 예측 경고, 규범적 지침 및 자동화된 작업을 통해 문제가 발생하기 전에 이를 방지함으로써 시스템 상태를 개선하고 시스템 가용성을 높일 수 있습니다.

NetApp Support 사이트에서 Active IQ 대시보드 및 기능을 사용하려면 AutoSupport를 사용하도록 설정해야 합니다.

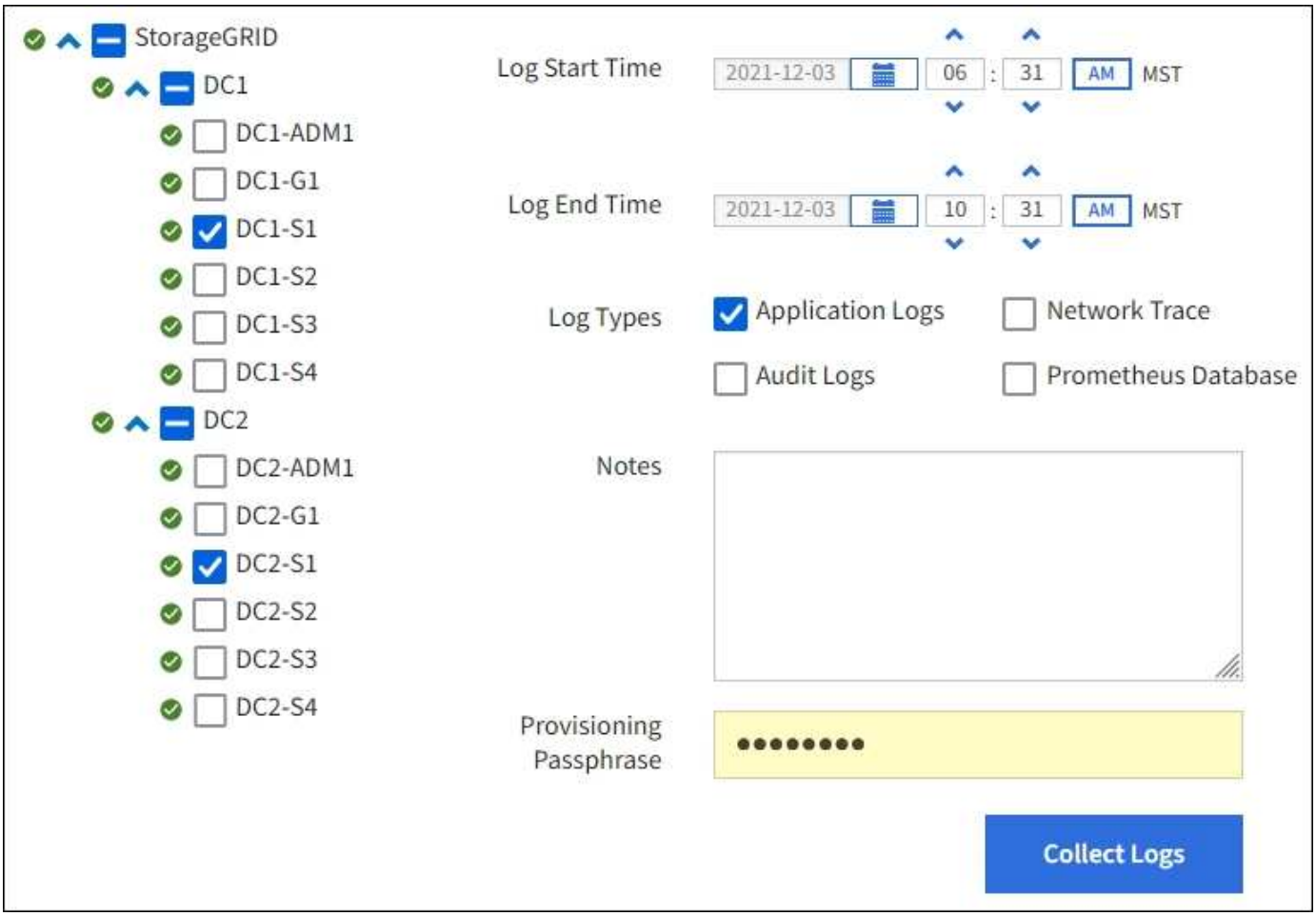
"Active IQ 디지털 자문 문서"

StorageGRID 로그를 수집합니다

문제 해결을 위해 로그 파일을 수집하여 기술 지원 부서에 전달해야 할 수 있습니다.

StorageGRID는 로그 파일을 사용하여 이벤트, 진단 메시지 및 오류 상태를 캡처합니다. bycast.log 파일은 모든 그리드 노드에 대해 유지 관리되며 주요 문제 해결 파일입니다. 또한 StorageGRID는 개별 StorageGRID 서비스에 대한 로그 파일, 배포 및 유지 관리 작업과 관련된 로그 파일, 타사 애플리케이션과 관련된 로그 파일을 생성합니다.

적절한 권한이 있고 StorageGRID 시스템의 프로비저닝 암호를 알고 있는 사용자는 그리드 관리자의 로그 페이지를 사용하여 로그 파일, 시스템 데이터 및 구성 데이터를 수집할 수 있습니다. 로그를 수집할 때 노드를 선택하고 기간을 지정합니다. 데이터는 로컬 컴퓨터로 다운로드할 수 있는 .tar.gz 파일로 수집 및 보관됩니다. 이 파일 안에는 각 그리드 노드에 대해 하나의 로그 파일 아카이브가 있습니다.



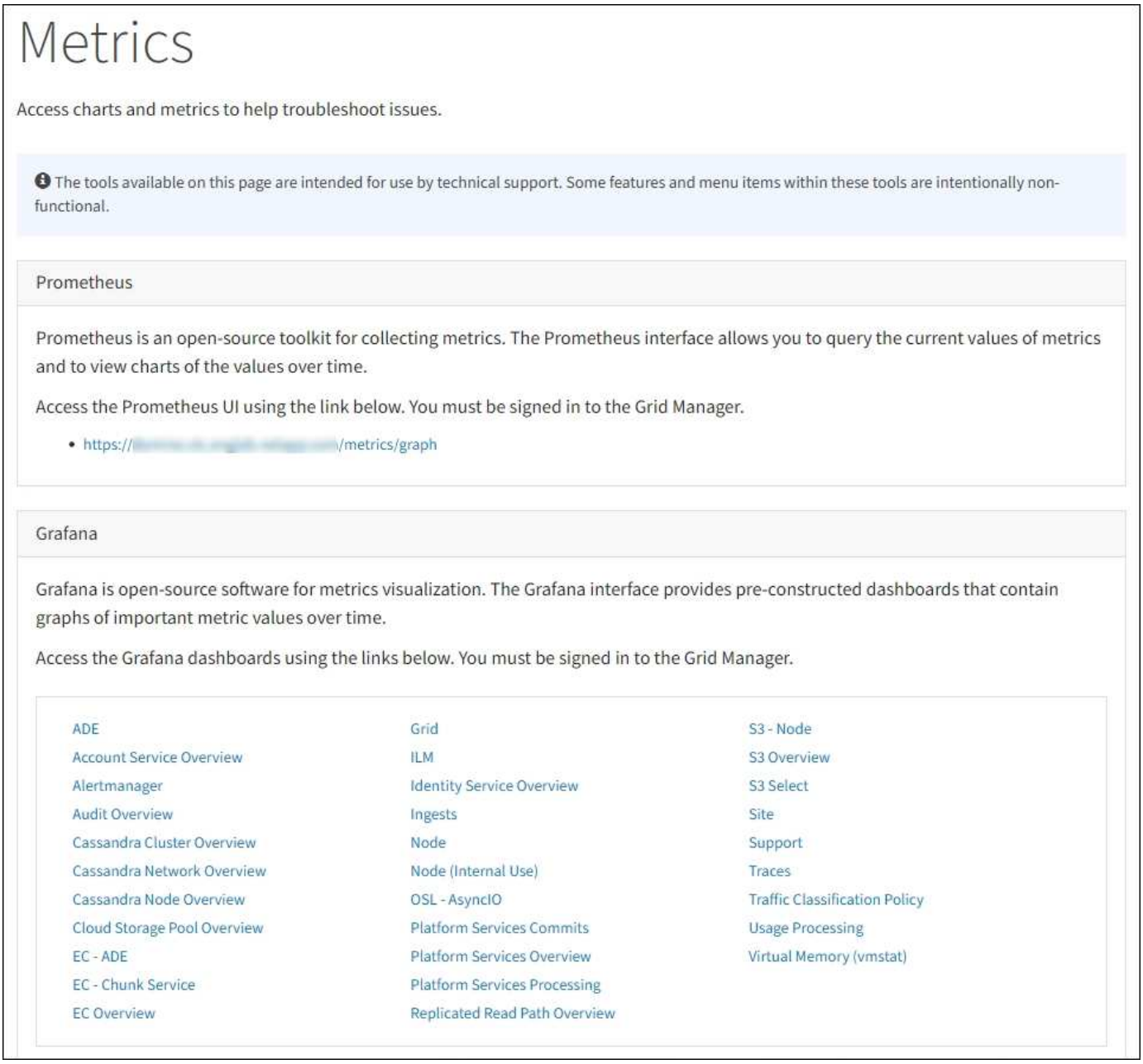
메트릭을 사용하고 진단 유틸리티를 실행합니다

문제를 해결할 때 기술 지원 팀과 협력하여 StorageGRID 시스템에 대한 자세한 메트릭 및 차트를 검토할 수 있습니다. 사전 구성된 진단 쿼리를 실행하여 StorageGRID 시스템의 주요 값을 사전에 평가할 수도 있습니다.

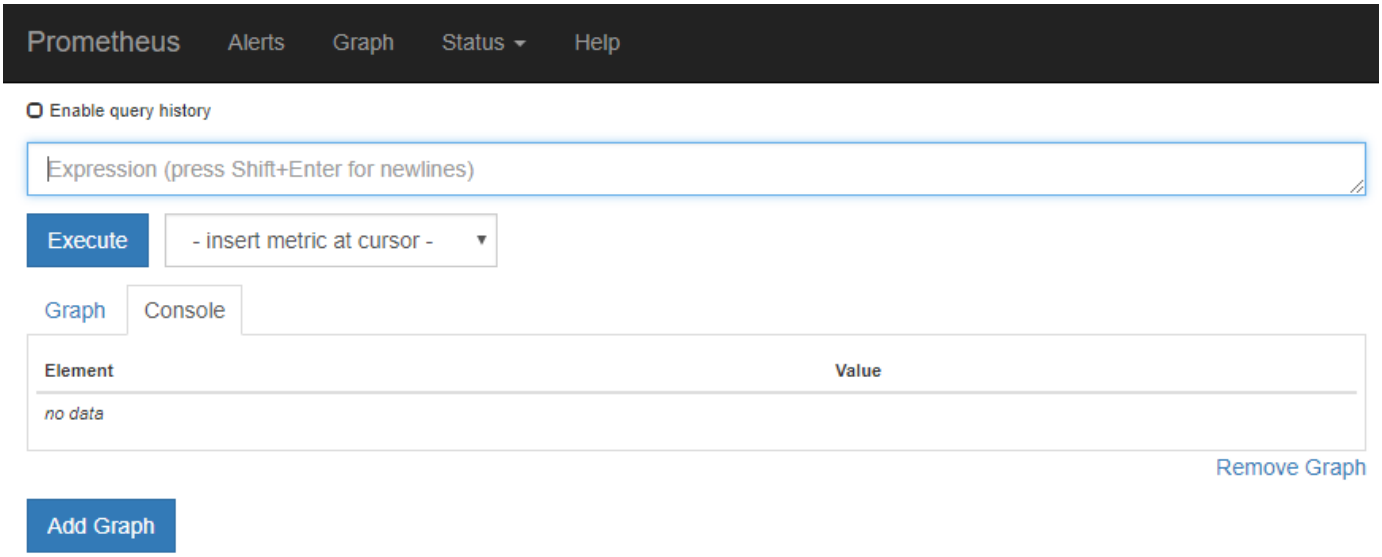
메트릭 페이지

메트릭 페이지에서는 Prometheus 및 Grafana 사용자 인터페이스에 액세스할 수 있습니다. Prometheus는 메트릭 수집을 위한 오픈 소스 소프트웨어입니다. Grafana는 메트릭 시각화를 위한 오픈 소스 소프트웨어입니다.

> 메트릭 페이지에서 사용할 수 있는 도구는 기술 지원 부서에서 사용하기 위한 것입니다. 이러한 도구 내의 일부 기능 및 메뉴 항목은 의도적으로 작동하지 않으며 변경될 수 있습니다.

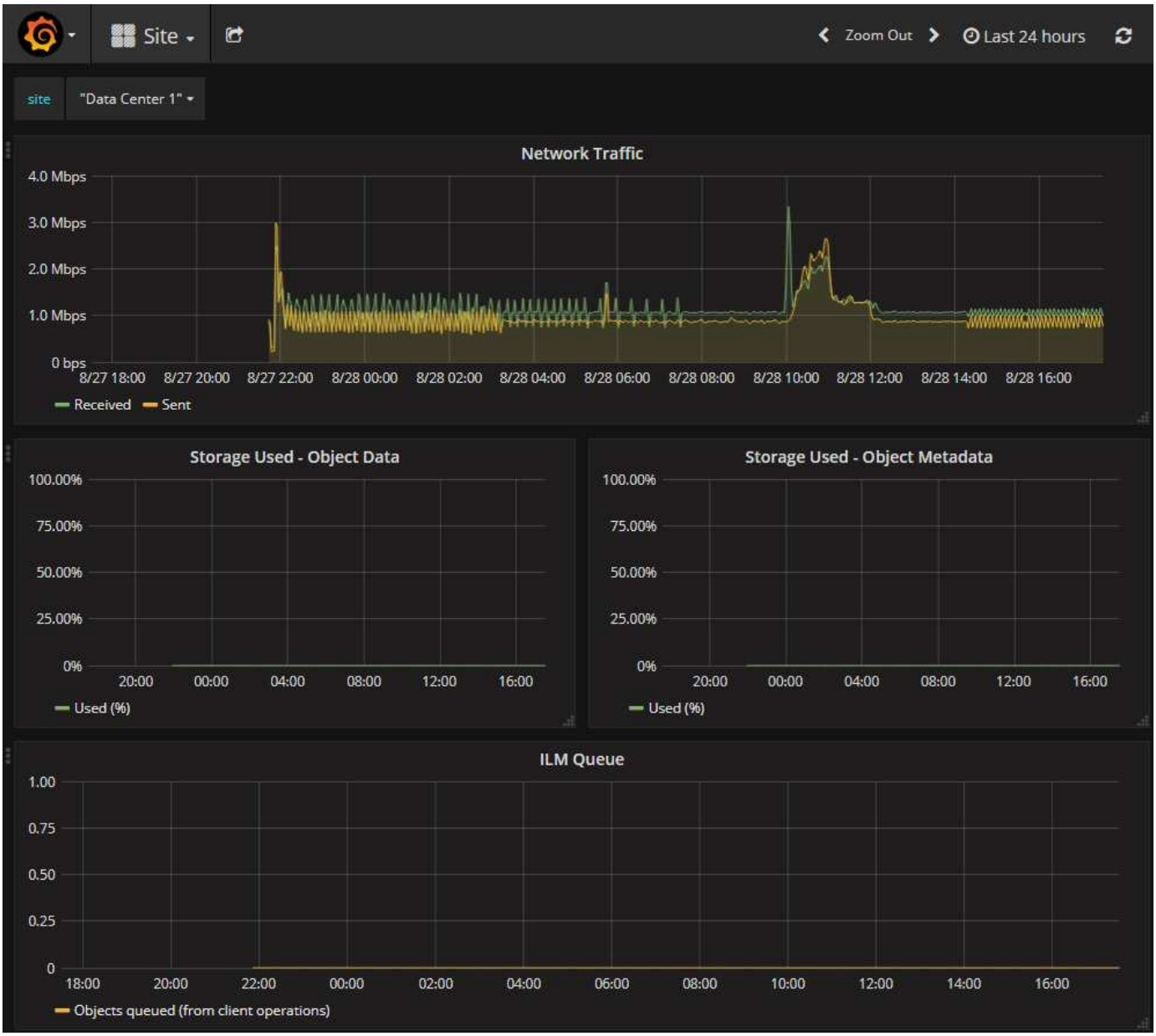


메트릭 페이지의 Prometheus 섹션에 있는 링크를 사용하면 StorageGRID 메트릭의 현재 값을 쿼리하고 시간에 따른 값의 그래프를 볼 수 있습니다.



> 이름에 _private_이 포함된 메트릭은 내부 전용이며 StorageGRID 릴리스 간에 예고 없이 변경될 수 있습니다.

메트릭 페이지의 Grafana 섹션에 있는 링크를 사용하여 시간에 따른 StorageGRID 메트릭 그래프가 포함된 사전 구성된 대시보드에 액세스할 수 있습니다.



진단 페이지를 참조하십시오

Diagnostics(진단) 페이지는 그리드의 현재 상태에 대해 사전 구성된 진단 검사 집합을 수행합니다. 이 예에서 모든 진단 유틸리티는 정상 상태입니다.

Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. A diagnostic check can have one of three statuses:

- **Normal**: All values are within the normal range.
- **Attention**: One or more of the values are outside of the normal range.
- **Caution**: One or more of the values are significantly outside of the normal range.

Diagnostic statuses are independent of current alerts and might not indicate operational issues with the grid. For example, a diagnostic check might show Caution status even if no alert has been triggered.

Run Diagnostics

- Cassandra blocked task queue too large
- Cassandra commit log latency
- Cassandra commit log queue depth
- Cassandra compaction queue too large

특정 진단을 클릭하면 진단 및 현재 결과에 대한 세부 정보를 볼 수 있습니다.

이 예에서는 StorageGRID 시스템의 모든 노드에 대한 현재 CPU 활용률이 표시됩니다. 모든 노드 값이 주의 및 주의 임계값 미만이므로 진단의 전체 상태는 정상입니다.

CPU utilization

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the **Node** Grafana dashboard.

Status Normal

Prometheus query

```
sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))
```

View in Prometheus

Thresholds
Attention >= 75%
Caution >= 95%

Status	Instance	CPU Utilization
	DC1-ADM1	2.598%
	DC1-ARC1	0.937%
	DC1-G1	2.119%
	DC1-S1	8.708%
	DC1-S2	8.142%
	DC1-S3	9.669%
	DC2-ADM1	2.515%
	DC2-ARC1	1.152%
	DC2-S1	8.204%
	DC2-S2	5.000%
	DC2-S3	10.469%

관련 정보

- StorageGRID 관리
- 네트워크 설정을 구성합니다

네트워킹 지침

네트워킹 지침: 개요

이 지침을 사용하여 StorageGRID 아키텍처 및 네트워킹 토폴로지에 대해 알아보고 네트워크 구성 및 프로비저닝에 대한 요구사항을 알아봅니다.

참조하십시오

다음 지침은 StorageGRID 노드를 배포 및 구성하기 전에 StorageGRID 네트워킹 인프라를 만드는 데 사용할 수 있는 정보를 제공합니다. 이러한 지침을 사용하여 그리드의 모든 노드 간에 그리고 그리드와 외부 클라이언트 및 서비스 간에 통신이 이루어질 수 있도록 하십시오.

외부 클라이언트 및 외부 서비스는 다음과 같은 기능을 수행하기 위해 StorageGRID 네트워크에 연결해야 합니다.

- 오브젝트 데이터 저장 및 검색
- 이메일 알림을 수신합니다
- StorageGRID 관리 인터페이스 액세스(그리드 관리자 및 테넌트 관리자)
- 감사 공유 액세스(선택 사항)
- 다음과 같은 서비스 제공:
  - NTP(Network Time Protocol)
  - DNS(Domain Name System)
  - KMS(Key Management Server)

StorageGRID 네트워킹은 이러한 기능 및 기타 기능에 대한 트래픽을 처리할 수 있도록 적절히 구성되어야 합니다.

시작하기 전에

StorageGRID 시스템에 대한 네트워킹을 구성하려면 이더넷 스위칭, TCP/IP 네트워킹, 서브넷, 네트워크 라우팅 및 방화벽에 대한 높은 수준의 경험이 필요합니다.

네트워킹을 구성하기 전에 에 설명된 대로 StorageGRID 아키텍처를 숙지하십시오 그리드 프라이머.

사용할 StorageGRID 네트워크 및 해당 네트워크의 구성 방법을 결정한 후에는 해당 지침에 따라 StorageGRID 노드를 설치 및 구성할 수 있습니다.

소프트웨어 기반 노드 설치

- Red Hat Enterprise Linux 또는 CentOS를 설치합니다
- Ubuntu 또는 Debian을 설치합니다
- VMware를 설치합니다

어플라이언스 노드를 설치합니다

- SG100 및 SG1000 서비스 어플라이언스
- SG6000 스토리지 어플라이언스
- SG5700 스토리지 어플라이언스
- SG5600 스토리지 어플라이언스

StorageGRID 소프트웨어를 구성하고 관리합니다

- StorageGRID 관리
- 릴리스 정보

StorageGRID 네트워크 유형입니다

StorageGRID 시스템의 GRID 노드는 PROCESS_GRID TRAFFIC_, *ADMIN TRAFFIC* 및 _CLIENT TRAFFIC_입니다. 이러한 세 가지 유형의 트래픽을 관리하고 제어 및 보안을 제공하도록 네트워킹을 적절히 구성해야 합니다.

트래픽 유형

트래픽 유형	설명	네트워크 유형입니다
그리드 트래픽	그리드의 모든 노드 사이를 이동하는 내부 StorageGRID 트래픽입니다. 모든 그리드 노드는 이 네트워크를 통해 다른 모든 그리드 노드와 통신할 수 있어야 합니다.	그리드 네트워크(필수)
관리 트래픽	시스템 관리 및 유지 보수에 사용되는 트래픽입니다.	관리 네트워크(선택 사항), VLAN 네트워크(옵션)
클라이언트 트래픽	S3 및 Swift 클라이언트의 모든 오브젝트 스토리지 요청을 포함하여 외부 클라이언트 애플리케이션과 그리드 간에 이동하는 트래픽입니다.	클라이언트 네트워크(선택 사항), VLAN 네트워크(옵션)

다음과 같은 방법으로 네트워킹을 구성할 수 있습니다.

- 그리드 네트워크만
- 그리드 및 관리 네트워크
- 그리드 및 클라이언트 네트워크
- 그리드, 관리 및 클라이언트 네트워크

그리드 네트워크는 필수이며 모든 그리드 트래픽을 관리할 수 있습니다. 설치 시 관리 및 클라이언트 네트워크를 포함시키거나 나중에 추가하여 요구 사항의 변화에 대응할 수 있습니다. 관리 네트워크 및 클라이언트 네트워크는 선택 사항이지만 이러한 네트워크를 사용하여 관리 트래픽과 클라이언트 트래픽을 처리할 때 그리드 네트워크를 격리하고 보호할 수 있습니다.

내부 포트는 그리드 네트워크를 통해서만 액세스할 수 있습니다. 외부 포트는 모든 네트워크 유형에서 액세스할 수 있습니다. 이러한 유연성은 StorageGRID 배포를 설계하고 스위치와 방화벽에서 외부 IP 및 포트 필터링을 설정하기 위한 여러 옵션을 제공합니다. 을 참조하십시오 내부 그리드 노드 통신 및 외부 통신.

네트워크 인터페이스

StorageGRID 노드는 다음 특정 인터페이스를 사용하여 각 네트워크에 연결됩니다.

네트워크	인터페이스 이름입니다
그리드 네트워크(필수)	eth0
관리 네트워크(선택 사항)	eth1
클라이언트 네트워크(옵션)	eth2

가상 또는 물리적 포트를 노드 네트워크 인터페이스에 매핑하는 방법에 대한 자세한 내용은 설치 지침을 참조하십시오.

소프트웨어 기반 노드

- Red Hat Enterprise Linux 또는 CentOS를 설치합니다
- Ubuntu 또는 Debian을 설치합니다
- VMware를 설치합니다

어플라이언스 노드

- SG100 및 SG1000 서비스 어플라이언스
- SG6000 스토리지 어플라이언스
- SG5700 스토리지 어플라이언스
- SG5600 스토리지 어플라이언스

각 노드에 대한 네트워크 정보입니다

노드에서 설정하는 각 네트워크에 대해 다음을 구성해야 합니다.

- IP 주소입니다
- 서브넷 마스크
- 게이트웨이 IP 주소입니다

각 그리드 노드에 있는 세 개의 네트워크 각각에 대해 하나의 IP 주소/마스크/게이트웨이 조합만 구성할 수 있습니다. 네트워크에 대한 게이트웨이를 구성하지 않으려면 IP 주소를 게이트웨이 주소로 사용해야 합니다.

고가용성 그룹

고가용성(HA) 그룹은 가상 IP(VIP) 주소를 그리드 또는 클라이언트 네트워크 인터페이스에 추가하는 기능을 제공합니다. 자세한 내용은 을 참조하십시오 고가용성 그룹을 관리합니다.

그리드 네트워크

그리드 네트워크가 필요합니다. 모든 내부 StorageGRID 트래픽에 사용됩니다. 그리드 네트워크는 모든 사이트와 서브넷에서 그리드의 모든 노드 간에 연결을 제공합니다. 그리드 네트워크의 모든 노드는 다른 모든 노드와 통신할 수 있어야 합니다. 그리드 네트워크는 여러 서브넷으로 구성될 수 있습니다. NTP와 같은 중요한 그리드 서비스가 포함된 네트워크를 그리드 서브넷으로 추가할 수도 있습니다.

> StorageGRID는 노드 간 NAT(네트워크 주소 변환)를 지원하지 않습니다.

그리드 네트워크는 관리 네트워크 및 클라이언트 네트워크가 구성된 경우에도 모든 관리 트래픽과 모든 클라이언트 트래픽에 사용할 수 있습니다. 노드에 클라이언트 네트워크가 구성되어 있지 않은 경우 그리드 네트워크 게이트웨이는 노드 기본 게이트웨이입니다.

> 그리드 네트워크를 구성할 때는 네트워크가 인터넷에 있는 클라이언트와 같이 신뢰할 수 없는 클라이언트로부터 보호되는지 확인해야 합니다.

Grid Network 게이트웨이에 대한 다음 요구 사항과 세부 정보를 확인합니다.

- 그리드 서브넷이 여러 개인 경우 그리드 네트워크 게이트웨이를 구성해야 합니다.
- 그리드 네트워크 게이트웨이는 그리드 구성이 완료될 때까지 노드 기본 게이트웨이입니다.
- 정적 라우트는 글로벌 그리드 네트워크 서브넷 목록에 구성된 모든 서브넷에 대한 모든 노드에 대해 자동으로 생성됩니다.
- 클라이언트 네트워크가 추가되면 그리드 구성이 완료되면 기본 게이트웨이가 그리드 네트워크 게이트웨이에서 클라이언트 네트워크 게이트웨이로 전환됩니다.

관리자 네트워크

관리 네트워크는 선택 사항입니다. 구성 시 시스템 관리 및 유지 보수 트래픽에 사용할 수 있습니다. 관리 네트워크는 일반적으로 전용 네트워크이며 노드 간에 라우팅할 필요가 없습니다.

관리자 네트워크가 활성화되어야 하는 그리드 노드를 선택할 수 있습니다.

관리 네트워크를 사용하면 관리 및 유지 관리 트래픽이 그리드 네트워크를 통해 이동할 필요가 없습니다. 관리 네트워크의 일반적인 용도는 다음과 같습니다.

- Grid Manager 및 Tenant Manager 사용자 인터페이스에 액세스합니다.
- NTP 서버, DNS 서버, 외부 키 관리 서버(KMS) 및 LDAP(Lightweight Directory Access Protocol) 서버와 같은 중요한 서비스에 대한 액세스
- 관리 노드의 감사 로그에 대한 액세스.
- 유지 관리 및 지원을 위한 SSH(Secure Shell Protocol) 액세스

관리 네트워크는 내부 그리드 트래픽에 사용되지 않습니다. 관리 네트워크 게이트웨이가 제공되며 관리 네트워크가 여러 외부 서브넷과 통신할 수 있습니다. 그러나 관리자 네트워크 게이트웨이는 노드 기본 게이트웨이로 사용되지 않습니다.

관리 네트워크 게이트웨이에 대한 다음 요구 사항과 세부 정보를 확인합니다.

- 관리자 네트워크 서브넷 외부에서 연결하거나 여러 관리 네트워크 서브넷이 구성된 경우 관리 네트워크 게이트웨이가 필요합니다.
- 정적 라우트는 노드의 Admin Network Subnet List에 설정된 각 서브넷에 대해 생성된다.

클라이언트 네트워크

클라이언트 네트워크는 선택 사항입니다. 이 애플리케이션은 S3, Swift와 같은 클라이언트 애플리케이션에 그리드 서비스에 대한 액세스를 제공하는 데 사용됩니다. 외부 리소스(예: 클라우드 스토리지 풀 또는 StorageGRID CloudMirror 복제 서비스)에서 StorageGRID 데이터에 액세스할 수 있도록 하려는 경우 외부 리소스에서도 클라이언트

네트워크를 사용할 수 있습니다. 그리드 노드는 클라이언트 네트워크 게이트웨이를 통해 연결할 수 있는 모든 서브넷과 통신할 수 있습니다.

클라이언트 네트워크가 활성화되어야 하는 그리드 노드를 선택할 수 있습니다. 모든 노드가 동일한 클라이언트 네트워크에 있을 필요는 없으며 노드는 클라이언트 네트워크를 통해 서로 통신하지 않습니다. 그리드 설치가 완료될 때까지 클라이언트 네트워크가 작동하지 않습니다.

보안을 강화하기 위해 노드의 클라이언트 네트워크 인터페이스를 신뢰할 수 없도록 지정하여 클라이언트 네트워크가 허용되는 연결 중에서 더 엄격하게 제한되도록 할 수 있습니다. 노드의 클라이언트 네트워크 인터페이스를 신뢰할 수 없는 경우 인터페이스는 CloudMirror 복제에 사용되는 것과 같은 아웃바운드 연결을 허용하지만 로드 밸런서 끝점으로 명시적으로 구성된 포트의 인바운드 연결만 허용합니다. 을 참조하십시오 신뢰할 수 없는 클라이언트 네트워크를 관리합니다 및 로드 밸런서 엔드포인트를 구성합니다.

클라이언트 네트워크를 사용하는 경우 클라이언트 트래픽이 그리드 네트워크를 통해 이동할 필요가 없습니다. 그리드 네트워크 트래픽은 라우팅이 불가능한 보안 네트워크로 분리될 수 있습니다. 다음 노드 유형은 대개 클라이언트 네트워크로 구성됩니다.

- 게이트웨이 노드: 이러한 노드는 StorageGRID 로드 밸런서 서비스에 대한 액세스 및 그리드에 대한 S3 및 Swift 클라이언트 액세스를 제공하기 때문입니다.
- 스토리지 노드: 이러한 노드가 S3, Swift 프로토콜 및 Cloud Storage Pool, CloudMirror 복제 서비스에 대한 액세스를 제공하기 때문입니다.
- 관리 노드: 테넌트 사용자가 관리자 네트워크를 사용하지 않고도 테넌트 관리자에 연결할 수 있도록 합니다.

클라이언트 네트워크 게이트웨이에 대해 다음을 확인합니다.

- 클라이언트 네트워크가 구성된 경우 클라이언트 네트워크 게이트웨이가 필요합니다.
- 그리드 구성이 완료되면 클라이언트 네트워크 게이트웨이가 그리드 노드의 기본 경로가 됩니다.

VLAN 네트워크 옵션

필요에 따라 클라이언트 트래픽 및 일부 유형의 관리 트래픽에 가상 LAN(VLAN) 네트워크를 사용할 수도 있습니다. 그러나 그리드 트래픽은 VLAN 인터페이스를 사용할 수 없습니다. 노드 간 내부 StorageGRID 트래픽은 항상 eth0에서 그리드 네트워크를 사용해야 합니다.

VLAN 사용을 지원하려면 노드에서 하나 이상의 인터페이스를 스위치에서 트렁크 인터페이스로 구성해야 합니다. 그리드 네트워크 인터페이스(eth0) 또는 클라이언트 네트워크 인터페이스(eth2)를 트렁크로 구성하거나 노드에 대한 추가 트렁크 인터페이스를 구성할 수 있습니다.

eth0이 트렁크로 구성된 경우 Grid Network 트래픽은 스위치에 구성된 대로 트렁크 기본 인터페이스를 통해 흐릅니다. 마찬가지로 eth2가 트렁크로 구성되어 있고 클라이언트 네트워크도 같은 노드에 구성되어 있는 경우 클라이언트 네트워크는 스위치에 구성된 트렁크 포트의 기본 VLAN을 사용합니다.

SSH, Grid Manager 또는 Tenant Manager 트래픽에 사용되는 것과 같은 인바운드 관리 트래픽만 VLAN 네트워크를 통해 지원됩니다. NTP, DNS, LDAP, KMS 및 클라우드 스토리지 풀에 사용되는 아웃바운드 트래픽은 VLAN 네트워크를 통해 지원되지 않습니다.

> VLAN 인터페이스는 관리 노드 및 게이트웨이 노드에만 추가할 수 있습니다. 스토리지 노드 또는 아카이브 노드에 대한 클라이언트 또는 관리자 액세스에는 VLAN 인터페이스를 사용할 수 없습니다.

을 참조하십시오 VLAN 인터페이스를 구성합니다 을 참조하십시오.

VLAN 인터페이스는 HA 그룹에서만 사용되며 활성 노드에 VIP 주소가 할당됩니다. 을 참조하십시오 고가용성 그룹을 관리합니다 을 참조하십시오.

관련 정보

- 네트워킹 요구 사항

네트워크 토폴로지 예

그리드 네트워크 토폴로지

가장 간단한 네트워크 토폴로지는 그리드 네트워크만 구성하여 만듭니다.

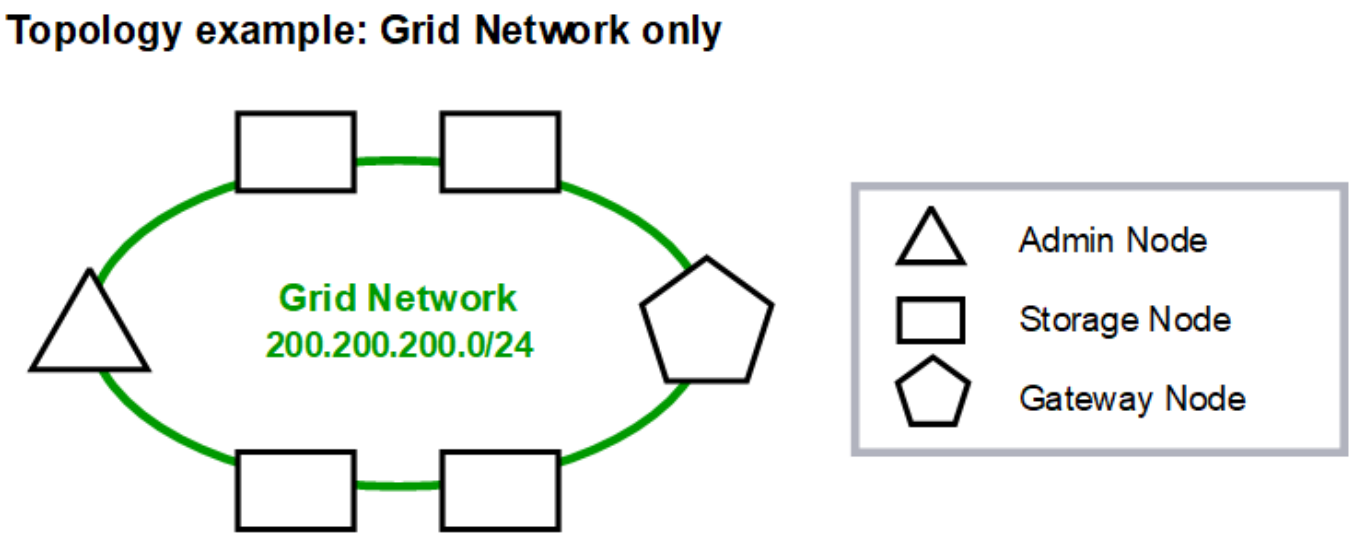
그리드 네트워크를 구성할 때 각 그리드 노드에 대한 eth0 인터페이스에 대한 호스트 IP 주소, 서브넷 마스크 및 게이트웨이 IP 주소를 설정합니다.

구성 중에 모든 그리드 네트워크 서브넷을 그리드 네트워크 서브넷 목록(GNSL)에 추가해야 합니다. 이 목록에는 모든 사이트에 대한 모든 서브넷이 포함되며 NTP, DNS 또는 LDAP와 같은 중요한 서비스에 대한 액세스를 제공하는 외부 서브넷도 포함될 수 있습니다.

설치 시 Grid Network 인터페이스는 GNSL에 있는 모든 서브넷에 대한 정적 라우트를 적용하고, 구성된 경우 노드의 기본 라우트를 Grid Network 게이트웨이로 설정합니다. 클라이언트 네트워크가 없고 그리드 네트워크 게이트웨이가 노드의 기본 경로인 경우에는 GNSL이 필요하지 않습니다. 그리드의 다른 모든 노드에 대한 호스트 라우트도 생성됩니다.

이 예에서 모든 트래픽은 S3 및 Swift 클라이언트 요청과 관련된 트래픽, 관리 및 유지보수 기능을 포함하여 동일한 네트워크를 공유합니다.

> 이 토폴로지는 외부에서 사용할 수 없거나 개념 증명 또는 테스트 배포가 불가능한 단일 사이트 배포나 타사 로드 밸런서가 클라이언트 액세스 경계 역할을 하는 경우에 적합합니다. 가능한 경우 그리드 네트워크는 내부 트래픽에만 사용해야 합니다. 관리 네트워크와 클라이언트 네트워크 모두 내부 서비스에 대한 외부 트래픽을 차단하는 추가 방화벽 제한이 있습니다. 외부 클라이언트 트래픽에 그리드 네트워크 사용이 지원되지만, 이러한 사용은 보호 계층의 수를 줄입니다.



		Provisioned
GNSL → 200.200.200.0/24		
	Grid Network	
Nodes	**IP/mask**	**Gateway**
Admin	200.200.200.32/24	200.200.200.1
Storage	200.200.200.33/24	200.200.200.1
Storage	200.200.200.34/24	200.200.200.1
Storage	200.200.200.35/24	200.200.200.1
Storage	200.200.200.36/24	200.200.200.1
Gateway	200.200.200.37/24	200.200.200.1

System Generated

Nodes	**Routes**			**Type**	**From**
All	0.0.0.0/0	→	200.200.200.1	Default	Grid Network gateway
	200.200.200.0/24	→	eth0	Link	Interface IP/mask

관리 네트워크 토폴로지

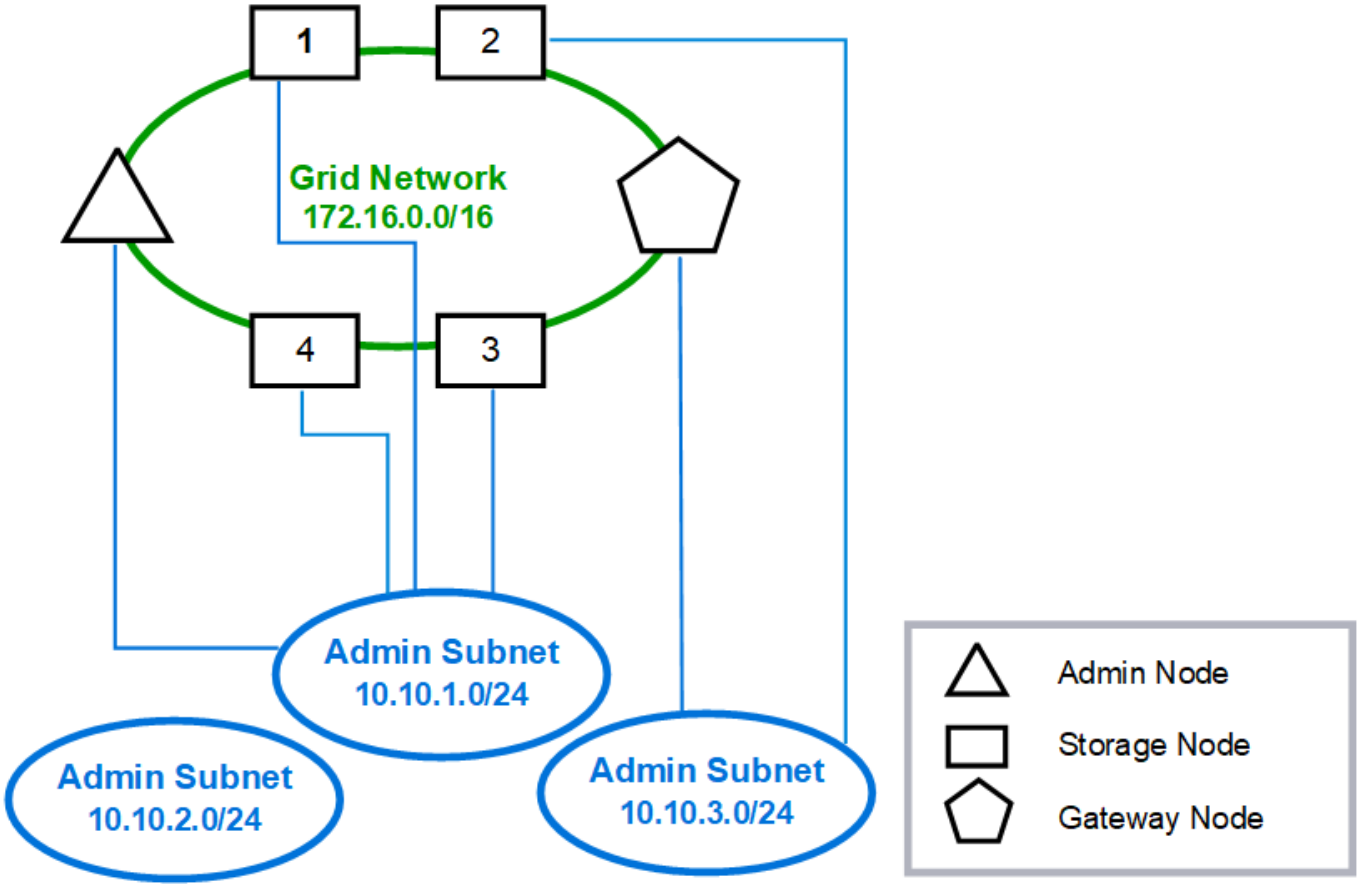
관리 네트워크 보유는 선택 사항입니다. 관리 네트워크 및 그리드 네트워크를 사용할 수 있는 한 가지 방법은 각 노드에 대해 라우팅 가능한 그리드 네트워크 및 경계 관리자 네트워크를 구성하는 것입니다.

관리 네트워크를 구성할 때 각 그리드 노드에 대한 eth1 인터페이스에 대한 호스트 IP 주소, 서브넷 마스크 및 게이트웨이 IP 주소를 설정합니다.

관리자 네트워크는 각 노드에 고유할 수 있으며 여러 서브넷으로 구성될 수 있습니다. 각 노드는 AESL(Admin External Subnet List)으로 구성할 수 있다. AESL은 각 노드에 대해 관리자 네트워크를 통해 연결할 수 있는 서브넷을 나열합니다. 또한 AESL은 NTP, DNS, KMS 및 LDAP와 같이 관리 네트워크를 통해 액세스할 모든 서비스의 서브넷을 포함해야 합니다. 정적 라우트는 AESL의 각 서브넷에 적용됩니다.

이 예에서 그리드 네트워크는 S3 및 Swift 클라이언트 요청 및 오브젝트 관리와 관련된 트래픽에 사용됩니다. 관리 네트워크는 관리 기능에 사용됩니다.

Topology example: Grid and Admin Networks



Provisioned

GNSL → 172.16.0.0/16
AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

	Grid Network		Admin Network	
Nodes	**IP/mask**	**Gateway**	**IP/mask**	**Gateway**
Admin	172.16.200.32/24	172.16.200.1	10.10.1.10/24	10.10.1.1
Storage 1	172.16.200.33/24	172.16.200.1	10.10.1.11/24	10.10.1.1
Storage 2	172.16.200.34/24	172.16.200.1	10.10.3.65/24	10.10.3.1
Storage 3	172.16.200.35/24	172.16.200.1	10.10.1.12/24	10.10.1.1
Storage 4	172.16.200.36/24	172.16.200.1	10.10.1.13/24	10.10.1.1
Gateway	172.16.200.37/24	172.16.200.1	10.10.3.66/24	10.10.3.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	172.16.200.1	Default	Grid Network gateway
Admin, Storage 1, 3, and 4	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	eth1	Link	Interface IP/mask
	10.10.2.0/24	→	10.10.1.1	Static	AESL
	10.10.3.0/24	→	10.10.1.1	Static	AESL
Storage 2, Gateway	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	10.10.3.1	Static	AESL
	10.10.2.0/24	→	10.10.3.1	Static	AESL
	10.10.3.0/24	→	eth1	Link	Interface IP/mask

클라이언트 네트워크 토폴로지

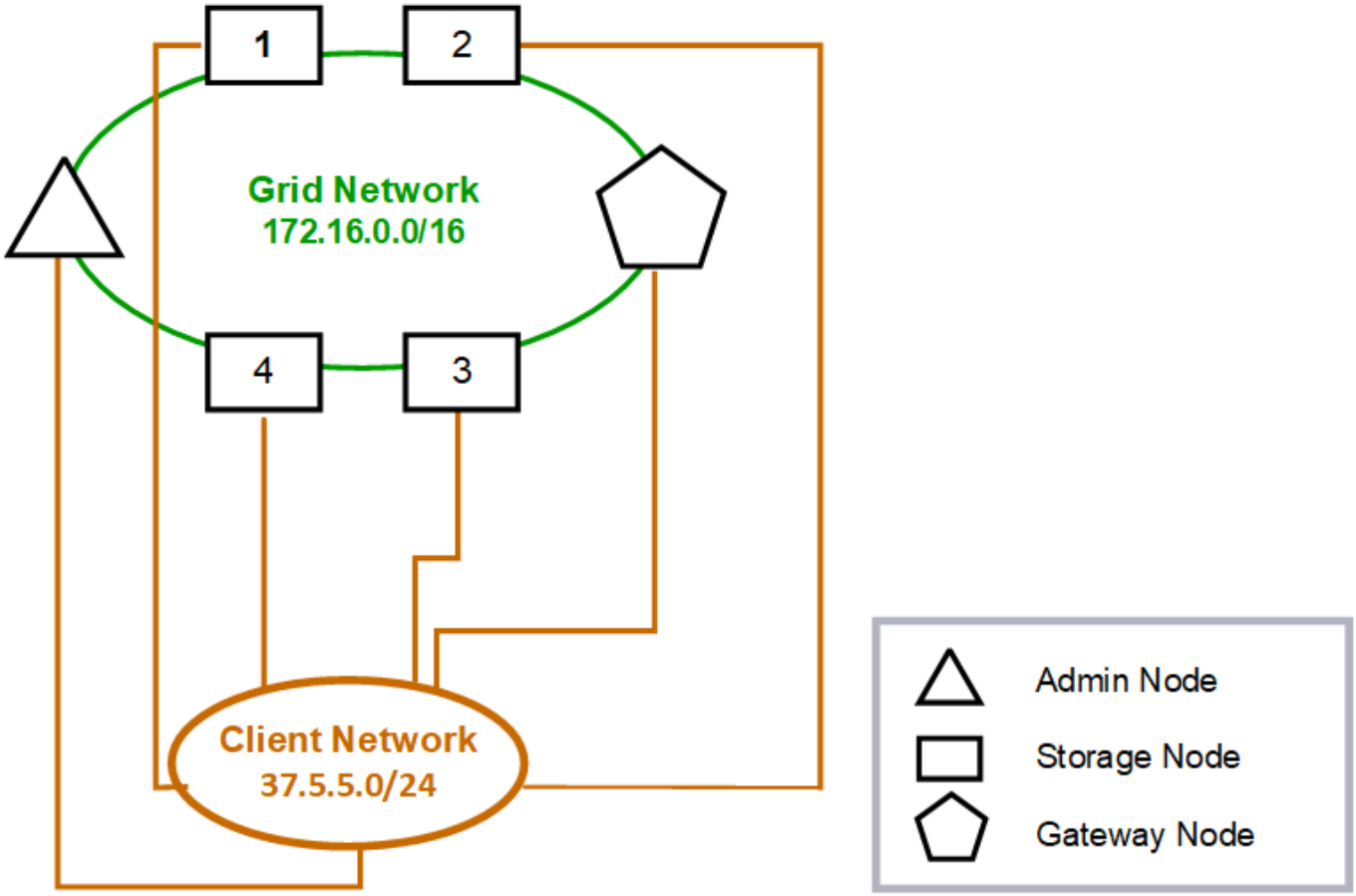
클라이언트 네트워크 보유는 선택 사항입니다. 클라이언트 네트워크를 사용하면 클라이언트 네트워크 트래픽(예: S3 및 Swift)을 그리드 내부 트래픽과 분리할 수 있으므로 그리드 네트워킹의 보안을 강화할 수 있습니다. 관리 네트워크가 구성되지 않은 경우 클라이언트 또는 그리드 네트워크에서 관리 트래픽을 처리할 수 있습니다.

클라이언트 네트워크를 구성할 때 구성된 노드의 eth2 인터페이스에 대한 호스트 IP 주소, 서브넷 마스크 및 게이트웨이 IP 주소를 설정합니다. 각 노드의 클라이언트 네트워크는 다른 노드의 클라이언트 네트워크와 독립할 수 있습니다.

설치 중에 노드에 대한 클라이언트 네트워크를 구성하는 경우 설치가 완료되면 노드의 기본 게이트웨이가 그리드 네트워크 게이트웨이에서 클라이언트 네트워크 게이트웨이로 전환됩니다. 나중에 클라이언트 네트워크를 추가하면 노드의 기본 게이트웨이가 같은 방식으로 전환됩니다.

이 예에서 클라이언트 네트워크는 S3 및 Swift 클라이언트 요청 및 관리 기능에 사용되고 그리드 네트워크는 내부 오브젝트 관리 작업 전용입니다.

Topology example: Grid and Client Networks



Provisioned

GNSL → 172.16.0.0/16			
	Grid Network	Client Network	
Nodes	IP/mask	IP/mask	Gateway
Admin	172.16.200.32/24	37.5.5.10/24	37.5.5.1
Storage	172.16.200.33/24	37.5.5.11/24	37.5.5.1
Storage	172.16.200.34/24	37.5.5.12/24	37.5.5.1
Storage	172.16.200.35/24	37.5.5.13/24	37.5.5.1
Storage	172.16.200.36/24	37.5.5.14/24	37.5.5.1
Gateway	172.16.200.37/24	37.5.5.15/24	37.5.5.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	37.5.5.1	Default	Client Network gateway
	172.16.0.0/16	→	eth0	Link	Interface IP/mask
	37.5.5.0/24	→	eth2	Link	Interface IP/mask

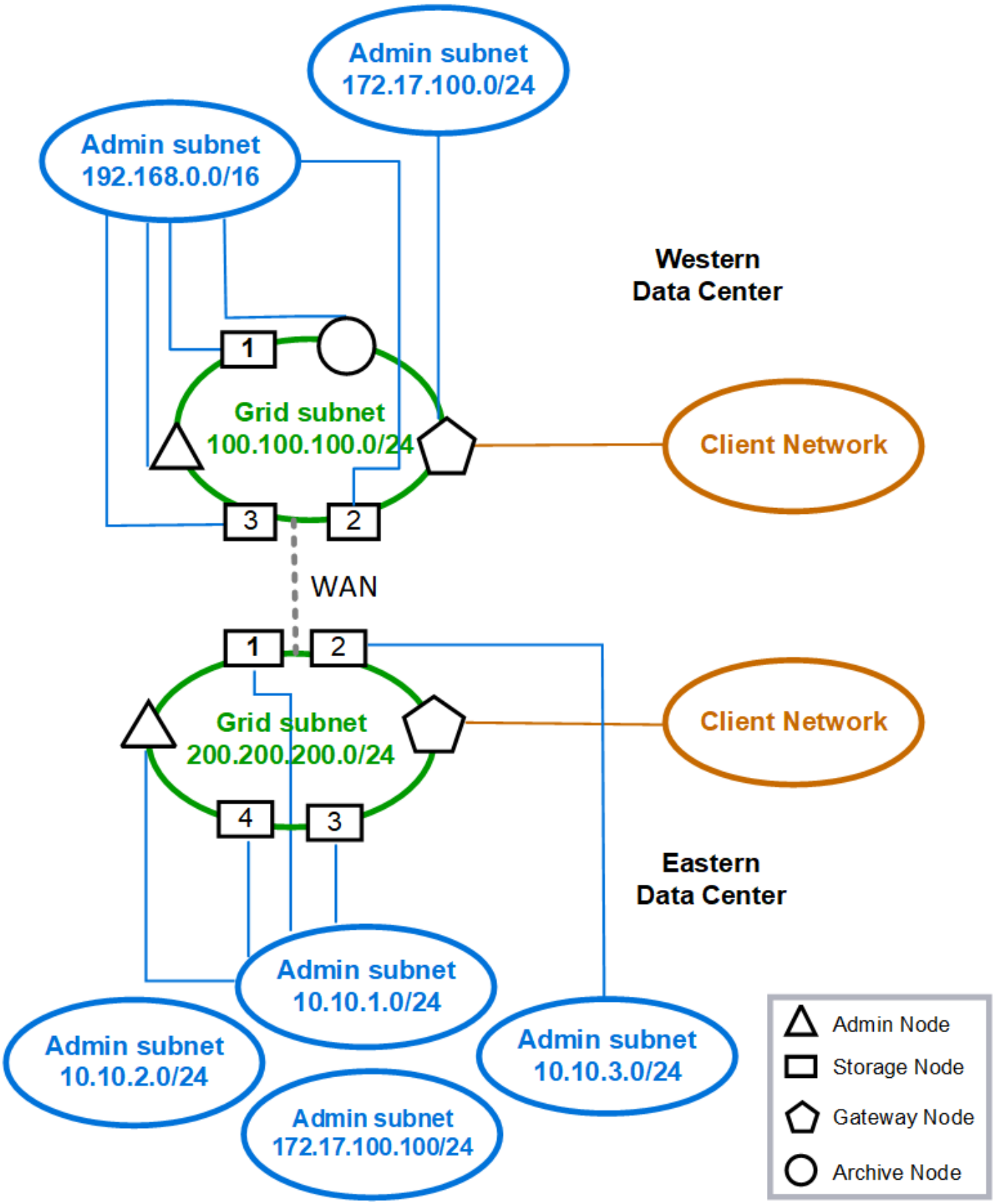
3개의 네트워크를 모두 위한 토폴로지

세 개의 네트워크를 모두 전용 그리드 네트워크, 경계 사이트 특정 관리 네트워크 및 개방형 클라이언트 네트워크로 구성된 네트워크 토폴로지로 구성할 수 있습니다. 로드 밸런서 끝점과 신뢰할 수 없는 클라이언트 네트워크를 사용하면 필요한 경우 추가 보안을 제공할 수 있습니다.

이 예에서

- 그리드 네트워크는 내부 오브젝트 관리 작업과 관련된 네트워크 트래픽에 사용됩니다.
- 관리 네트워크는 관리 기능과 관련된 트래픽에 사용됩니다.
- 클라이언트 네트워크는 S3 및 Swift 클라이언트 요청과 관련된 트래픽에 사용됩니다.

Topology example: Grid, Admin, and Client Networks



네트워킹 요구 사항

현재 네트워킹 인프라 및 구성이 계획된 StorageGRID 네트워크 설계를 지원할 수 있는지 확인해야 합니다.

일반 네트워킹 요구 사항

모든 StorageGRID 배포에서 다음 연결을 지원할 수 있어야 합니다.

이러한 연결은 네트워크 토폴로지 예에 표시된 대로 그리드, 관리자 또는 클라이언트 네트워크 또는 이러한 네트워크의 조합을 통해 발생할 수 있습니다.

- * 관리 연결 * : 일반적으로 SSH를 통해 관리자로부터 노드로 인바운드 연결. 그리드 관리자, 테넌트 관리자 및 StorageGRID 어플라이언스 설치 프로그램에 대한 웹 브라우저 액세스
- * NTP 서버 연결 * : 인바운드 UDP 응답을 수신하는 아웃바운드 UDP 연결입니다.

  1차 관리자 노드에서 하나 이상의 NTP 서버에 연결할 수 있어야 합니다.

- * DNS 서버 연결 * : 인바운드 UDP 응답을 수신하는 아웃바운드 UDP 연결입니다.
- * LDAP/Active Directory 서버 연결 *: 스토리지 노드의 ID 서비스에서 아웃바운드 TCP 연결.
- **AutoSupport**: 관리자 노드에서 의 upport.netapp.com` 또는 고객 구성 프록시로 아웃바운드 TCP 연결.
- * 외부 키 관리 서버 *: 노드 암호화가 활성화된 각 어플라이언스 노드에서 아웃바운드 TCP 연결.
- S3 및 Swift 클라이언트의 인바운드 TCP 연결.
- CloudMirror 복제 또는 클라우드 스토리지 풀과 같은 StorageGRID 플랫폼 서비스의 아웃바운드 요청

StorageGRID가 기본 라우팅 규칙을 사용하여 프로비저닝된 NTP 또는 DNS 서버와 연결할 수 없는 경우 DNS 및 NTP 서버의 IP 주소가 지정된 경우 모든 네트워크(그리드, 관리자 및 클라이언트)에서 자동으로 연결을 시도합니다. 네트워크에서 NTP 또는 DNS 서버에 연결할 수 있는 경우 StorageGRID는 자동으로 추가 라우팅 규칙을 만들어 향후 모든 연결 시도에 네트워크가 사용되도록 합니다.

> 자동으로 검색된 호스트 라우트를 사용할 수 있지만 일반적으로 자동 검색이 실패할 경우 연결을 보장하기 위해 DNS 및 NTP 라우트를 수동으로 구성해야 합니다.

배포 중에 선택적 관리 및 클라이언트 네트워크를 구성할 준비가 되지 않은 경우 구성 단계에서 그리드 노드를 승인할 때 이러한 네트워크를 구성할 수 있습니다. 또한 IP 변경 도구를 사용하여 설치 후 이러한 네트워크를 구성할 수 있습니다(참조) IP 주소를 구성합니다)를 클릭합니다.

VLAN 인터페이스를 통해 S3 및 Swift 클라이언트 연결과 SSH, Grid Manager 및 테넌트 관리자 관리 연결만 지원됩니다. NTP, DNS, LDAP, AutoSupport 및 KMS 서버와 같은 아웃바운드 연결 클라이언트, 관리자 또는 그리드 네트워크 인터페이스를 직접 이동해야 합니다. 인터페이스가 VLAN 인터페이스를 지원하도록 트렁크로 구성된 경우 이 트래픽은 스위치에서 구성된 대로 인터페이스의 네이티브 VLAN을 통해 흐릅니다.

여러 사이트를 위한 **WAN(Wide Area Network**

여러 사이트로 StorageGRID 시스템을 구성할 경우 클라이언트 트래픽을 고려하기 전에 사이트 간 WAN 연결에 각 방향의 최소 대역폭이 25Mbit/초 이상이어야 합니다. 사이트, 노드 또는 사이트 확장, 노드 복구 및 기타 운영 또는 구성 간 데이터 복제 또는 삭제 코딩에 추가 대역폭이 필요합니다.

관리 노드 및 게이트웨이 노드에 대한 연결

관리자 노드는 항상 인터넷에 있는 것과 같이 신뢰할 수 없는 클라이언트로부터 보호되어야 합니다. 신뢰할 수 없는 클라이언트가 그리드 네트워크, 관리 네트워크 또는 클라이언트 네트워크의 관리 노드에 액세스할 수 있는지 확인해야 합니다.

고가용성 그룹에 추가하려는 관리 노드 및 게이트웨이 노드는 정적 IP 주소로 구성해야 합니다. 자세한 내용은 을 참조하십시오 고가용성 그룹을 관리합니다.

NAT(Network Address Translation) 사용

그리드 네트워크에서 그리드 노드 간 또는 StorageGRID 사이트 간에 NAT(네트워크 주소 변환)를 사용하지 마십시오. Grid Network에 전용 IPv4 주소를 사용하는 경우, 이러한 주소는 모든 사이트의 모든 그리드 노드에서 직접 라우팅할 수 있어야 합니다. 그러나 필요한 경우 게이트웨이 노드에 대한 공용 IP 주소를 제공하는 등의 NAT를 외부 클라이언트와 그리드 노드 간에 사용할 수 있습니다. NAT를 사용하여 공용 네트워크 세그먼트를 연결하는 것은 그리드의 모든 노드에 투명하고 터널링 응용 프로그램을 사용하는 경우에만 지원됩니다. 즉, 그리드 노드는 공용 IP 주소를 알 필요가 없습니다.

네트워크 특정 요구 사항

각 StorageGRID 네트워크 유형에 대한 요구 사항을 따릅니다.

네트워크 게이트웨이 및 라우터

- 설정된 경우 해당 네트워크의 게이트웨이는 특정 네트워크의 서브넷 내에 있어야 합니다.
- 정적 주소 지정을 사용하여 인터페이스를 구성하는 경우 0.0.0.0이 아닌 게이트웨이 주소를 지정해야 합니다.
- 게이트웨이가 없는 경우 가장 좋은 방법은 게이트웨이 주소를 네트워크 인터페이스의 IP 주소로 설정하는 것입니다.

서브넷

> 각 네트워크는 노드의 다른 네트워크와 겹치지 않는 자체 서브넷에 연결되어야 합니다.

배포 중에는 Grid Manager에서 다음과 같은 제한 사항이 적용됩니다. 사전 배포 네트워크 계획을 지원하기 위해 여기에 제공됩니다.

- 네트워크 IP 주소에 대한 서브넷 마스크는 255.255.255.254 또는 255.255.255.255(/31 또는 /32 CIDR 표기법)일 수 없습니다.
- 네트워크 인터페이스 IP 주소 및 서브넷 마스크(CIDR)에 의해 정의된 서브넷은 동일한 노드에 구성된 다른 인터페이스의 서브넷과 겹칠 수 없습니다.
- 각 노드의 그리드 네트워크 서브넷은 GNSL에 포함되어야 합니다.
- 관리 네트워크 서브넷은 그리드 네트워크 서브넷, 클라이언트 네트워크 서브넷 또는 GNSL의 모든 서브넷과 겹칠 수 없습니다.
- AESL에 있는 서브넷은 GNSL에 있는 서브넷과 겹칠 수 없습니다.
- 클라이언트 네트워크 서브넷은 그리드 네트워크 서브넷, 관리 네트워크 서브넷, GNSL의 모든 서브넷 또는 AESL의 모든 서브넷과 겹칠 수 없습니다.

그리드 네트워크

- 배포 시 각 그리드 노드는 그리드 네트워크에 연결되어 있어야 하며 노드를 배포할 때 지정한 네트워킹 구성을 사용하여 기본 관리 노드와 통신할 수 있어야 합니다.
- 정상적인 그리드 작업 중에 각 그리드 노드는 그리드 네트워크를 통해 다른 모든 그리드 노드와 통신할 수 있어야 합니다.

> 그리드 네트워크는 각 노드 간에 직접 라우팅할 수 있어야 합니다. 노드 간 NAT(Network Address Translation)는 지원되지 않습니다.

- 그리드 네트워크가 여러 개의 서브넷으로 구성된 경우 그리드 네트워크 서브넷 목록(GNSL)에 추가합니다. 정적 라우트는 GNSL의 각 서브넷에 대한 모든 노드에 생성됩니다.
- 그리드 네트워크 인터페이스가 VLAN 인터페이스를 지원하도록 트렁크로 구성된 경우 트렁크 기본 VLAN은 그리드 네트워크 트래픽에 사용되는 VLAN이어야 합니다. 모든 그리드 노드는 트렁크 기본 VLAN을 통해 액세스할 수 있어야 합니다.

관리자 네트워크

관리 네트워크는 선택 사항입니다. 관리 네트워크를 구성하려는 경우 다음 요구 사항 및 지침을 따르십시오.

관리 네트워크의 일반적인 사용에는 관리 연결, AutoSupport, KMS 및 NTP, DNS 및 LDAP와 같은 중요한 서버에 대한 연결(이러한 연결이 그리드 네트워크 또는 클라이언트 네트워크를 통해 제공되지 않는 경우)이 포함됩니다.

> 원하는 네트워크 서비스 및 클라이언트에 연결할 수 있는 경우 관리 네트워크 및 AESL은 각 노드에 고유할 수 있습니다.

> 외부 서브넷에서 인바운드 연결을 활성화하려면 관리자 네트워크에서 하나 이상의 서브넷을 정의해야 합니다. 정적 라우트는 AESL의 각 서브넷에 대해 자동으로 생성됩니다.

클라이언트 네트워크

클라이언트 네트워크는 선택 사항입니다. 클라이언트 네트워크를 구성하려는 경우 다음 고려 사항에 유의하십시오.

- 클라이언트 네트워크는 S3 및 Swift 클라이언트의 트래픽을 지원하도록 설계되었습니다. 구성된 경우 클라이언트 네트워크 게이트웨이는 노드의 기본 게이트웨이가 됩니다.
- 클라이언트 네트워크를 사용하는 경우 명시적으로 구성된 로드 밸런서 끝점에서만 인바운드 클라이언트 트래픽을 허용하여 악의적인 공격으로부터 StorageGRID를 보호할 수 있습니다. 을 참조하십시오 로드 밸런서 엔드포인트를 구성합니다.
- 클라이언트 네트워크 인터페이스가 VLAN 인터페이스를 지원하도록 트렁크로 구성된 경우 클라이언트 네트워크 인터페이스(eth2)를 구성해야 하는지 여부를 고려하십시오. 구성된 경우 클라이언트 네트워크 트래픽은 스위치에 구성된 트렁크 기본 VLAN을 통해 흐릅니다.

배포별 네트워킹 고려 사항

Linux 배포

효율성, 안정성 및 보안을 위해 StorageGRID 시스템은 Linux에서 컨테이너 엔진의 모음으로 실행됩니다. StorageGRID 시스템에는 컨테이너 엔진 관련 네트워크 구성이 필요하지 않습니다.

컨테이너 네트워크 인터페이스에 VLAN 또는 가상 이더넷(veth) 쌍과 같은 비결합 장치를 사용합니다. 이 디바이스를 노드 구성 파일의 네트워크 인터페이스로 지정합니다.

> 연결 또는 브리지 장치를 컨테이너 네트워크 인터페이스로 직접 사용하지 마십시오. 이렇게 하면 컨테이너 네임스페이스에서 결합 및 브리지 장치와 함께 macvlan을 사용하는 커널 문제로 인해 노드 시작이 방지될 수 있습니다.

의 설치 지침을 참조하십시오 Red Hat Enterprise Linux 또는 CentOS 또는 Ubuntu 또는 Debian 적합합니다.

컨테이너 엔진 구축을 위한 호스트 네트워크 구성

컨테이너 엔진 플랫폼에서 StorageGRID 배포를 시작하기 전에 각 노드에서 사용할 네트워크(그리드, 관리자, 클라이언트)를 결정합니다. 각 노드의 네트워크 인터페이스가 올바른 가상 또는 물리적 호스트 인터페이스에 구성되어 있고 각 네트워크에 충분한 대역폭이 있는지 확인해야 합니다.

물리적 호스트

물리적 호스트를 사용하여 그리드 노드를 지원하는 경우:

- 모든 호스트가 각 노드 인터페이스에 대해 동일한 호스트 인터페이스를 사용해야 합니다. 이 전략은 호스트 구성을 간소화하고 향후 노드 마이그레이션을 지원합니다.
- 물리적 호스트 자체의 IP 주소를 가져옵니다.

> 호스트의 물리적 인터페이스는 호스트 자체와 호스트에서 실행 중인 하나 이상의 노드에서 사용할 수 있습니다. 이 인터페이스를 사용하여 호스트에 할당된 모든 IP 주소는 고유해야 합니다. 호스트와 노드는 IP 주소를 공유할 수 없습니다.

- 호스트에 필요한 포트를 엽니다.
- StorageGRID에서 VLAN 인터페이스를 사용하려면 호스트에 원하는 VLAN에 대한 액세스를 제공하는 하나 이상의 트렁크 인터페이스가 있어야 합니다. 이러한 인터페이스는 eth0, eth2 또는 추가 인터페이스로 노드 컨테이너에 전달될 수 있습니다. 트렁크 또는 액세스 인터페이스를 추가하려면 다음을 참조하십시오.
  - * RHEL 또는 CentOS(노드 설치 전) *: 노드 구성 파일을 생성합니다
  - * Ubuntu 또는 Debian(노드 설치 전) *: 노드 구성 파일을 생성합니다
  - * RHEL, CentOS, Ubuntu 또는 Debian(노드 설치 후) *: Linux: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다

최소 대역폭 권장 사항

다음 표에는 각 유형의 StorageGRID 노드 및 각 네트워크 유형에 대한 최소 대역폭 권장 사항이 나와 있습니다. 해당 호스트에서 실행하려는 StorageGRID 노드의 총 수와 유형에 대한 총 최소 대역폭 요구 사항을 충족할 수 있도록 충분한 네트워크 대역폭을 사용하여 각 물리적 호스트 또는 가상 호스트를 프로비저닝해야 합니다.

노드 유형입니다	네트워크 유형입니다		
	그리드	관리자	클라이언트
관리자	10Gbps	1Gbps	1Gbps

노드 유형입니다	네트워크 유형입니다		
게이트웨이	10Gbps	1Gbps	10Gbps
스토리지	10Gbps	1Gbps	10Gbps
아카이브	10Gbps	1Gbps	10Gbps

> 이 테이블에는 공유 스토리지에 액세스하는 데 필요한 SAN 대역폭이 포함되지 않습니다. 이더넷(iSCSI 또는 FCoE)을 통해 액세스되는 공유 스토리지를 사용하는 경우 충분한 SAN 대역폭을 제공하기 위해 각 호스트에 별도의 물리적 인터페이스를 프로비저닝해야 합니다. 병목 현상을 방지하기 위해 특정 호스트의 SAN 대역폭은 해당 호스트에서 실행 중인 모든 스토리지 노드의 집계 스토리지 노드 네트워크 대역폭과 거의 일치해야 합니다.

이 표를 사용하여 해당 호스트에서 실행하려는 StorageGRID 노드의 수와 유형에 따라 각 호스트에 프로비저닝할 최소 네트워크 인터페이스 수를 결정합니다.

예를 들어 단일 호스트에서 하나의 관리 노드, 하나의 게이트웨이 노드 및 하나의 스토리지 노드를 실행하려면 다음을 수행합니다.

- 관리 노드에서 그리드 및 관리 네트워크 연결(10 + 1 = 11Gbps 필요)
- 게이트웨이 노드에서 그리드 및 클라이언트 네트워크 연결(10 + 10 = 20Gbps 필요)
- 스토리지 노드에서 그리드 네트워크 연결(10Gbps 필요)

이 시나리오에서는 최소 11 + 20 + 10 = 41Gbps의 네트워크 대역폭을 제공해야 합니다. 이 인터페이스는 2개의 40Gbps 인터페이스 또는 5개의 10Gbps 인터페이스를 통해 충족될 수 있으며, 잠재적으로 트렁크로 집계된 다음 그리드, 관리 및 클라이언트 서브넷을 포함하는 물리적 데이터 센터에 로컬로 전달하는 3개 이상의 VLAN에서 공유할 수 있습니다.

StorageGRID 구축을 준비하기 위해 StorageGRID 클러스터의 호스트에서 물리적 리소스와 네트워크 리소스를 구성하는 몇 가지 권장 방법은 다음을 참조하십시오.

- 호스트 네트워크 구성(Red Hat Enterprise Linux 또는 CentOS)
- 호스트 네트워크 구성(Ubuntu 또는 Debian)

플랫폼 서비스 및 클라우드 스토리지 풀을 위한 네트워킹 및 포트

StorageGRID 플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하려는 경우 대상 엔드포인트에 연결할 수 있도록 그리드 네트워킹 및 방화벽을 구성해야 합니다.

플랫폼 서비스를 위한 네트워킹

에 설명된 대로 테넌트를 위한 플랫폼 서비스 관리 및 플랫폼 서비스란 무엇입니까, 플랫폼 서비스에는 검색 통합, 이벤트 알림 및 CloudMirror 복제를 제공하는 외부 서비스가 포함됩니다.

플랫폼 서비스를 사용하려면 StorageGRID ADC 서비스를 외부 서비스 끝점에 호스팅하는 스토리지 노드로부터 액세스해야 합니다. 액세스 제공 예는 다음과 같습니다.

- ADC 서비스가 있는 스토리지 노드에서 대상 끝점으로 라우팅하는 AESL 항목을 사용하여 고유한 관리 네트워크를

구성합니다.

- 클라이언트 네트워크에서 제공하는 기본 경로를 사용합니다. 기본 루트를 사용하는 경우 를 사용할 수 있습니다 신뢰할 수 없는 클라이언트 네트워크 기능입니다 인바운드 연결을 제한합니다.

클라우드 스토리지 풀을 위한 네트워킹

또한 클라우드 스토리지 풀에서는 Amazon S3 Glacier 또는 Microsoft Azure Blob 스토리지와 같이 사용되는 외부 서비스에서 제공하는 엔드포인트로 스토리지 노드에서 액세스할 수 있어야 합니다. 자세한 내용은 을 참조하십시오 클라우드 스토리지 풀은 무엇입니까.

플랫폼 서비스 및 클라우드 스토리지 풀을 위한 포트입니다

기본적으로 플랫폼 서비스 및 클라우드 스토리지 풀 통신에는 다음 포트가 사용됩니다.

- * 80 *: http로 시작하는 끝점 URI입니다
- * 443 *: 끝점 URI의 경우 "https"로 시작합니다

끝점을 만들거나 편집할 때 다른 포트를 지정할 수 있습니다. 을 참조하십시오 네트워크 포트 참조.

투명하지 않은 프록시 서버를 사용하는 경우에도 필요합니다 스토리지 프록시 설정을 구성합니다 인터넷의 끝점과 같은 외부 끝점으로 메시지를 보낼 수 있도록 합니다.

VLAN 및 플랫폼 서비스와 클라우드 스토리지 풀

플랫폼 서비스 또는 클라우드 스토리지 풀에 VLAN 네트워크를 사용할 수 없습니다. 대상 엔드포인트는 그리드, 관리자 또는 클라이언트 네트워크를 통해 연결할 수 있어야 합니다.

어플라이언스 노드

StorageGRID 어플라이언스의 네트워크 포트를 구성하여 처리량, 이중화 및 페일오버 요구사항을 충족하는 포트 결합 모드를 사용할 수 있습니다.

StorageGRID 어플라이언스의 10/25-GbE 포트는 그리드 네트워크 및 클라이언트 네트워크에 연결하기 위해 고정 또는 애그리게이트 결합 모드로 구성할 수 있습니다.

1GbE 관리 네트워크 포트는 독립 또는 Active-Backup 모드로 구성하여 관리 네트워크에 연결할 수 있습니다.

본 제품의 설치 및 유지보수 지침에서 포트 결합 모드에 대한 정보를 참조하십시오.

- SG100 및 SG1000 서비스 어플라이언스
- SG6000 스토리지 어플라이언스
- SG5700 스토리지 어플라이언스
- SG5600 스토리지 어플라이언스

네트워크 설치 및 프로비저닝

노드 배포 및 그리드 구성 중에 그리드 네트워크와 선택적 관리 및 클라이언트 네트워크가 어떻게 사용되는지 이해해야 합니다.

노드의 초기 구축

노드를 처음 배포할 때는 노드를 그리드 네트워크에 연결하고 기본 관리 노드에 대한 액세스 권한이 있는지 확인해야 합니다. 그리드 네트워크가 격리된 경우 그리드 네트워크 외부에서 구성 및 설치 액세스를 위해 기본 관리 노드에서 관리 네트워크를 구성할 수 있습니다.

게이트웨이가 구성된 그리드 네트워크는 구축 중에 노드의 기본 게이트웨이가 됩니다. 기본 게이트웨이를 사용하면 그리드를 구성하기 전에 별도의 서브넷의 그리드 노드가 운영 관리자 노드와 통신할 수 있습니다.

필요한 경우 NTP 서버가 포함되어 있거나 그리드 관리자 또는 API에 대한 액세스가 필요한 서브넷을 그리드 서브넷으로 구성할 수도 있습니다.

운영 관리 노드를 사용한 자동 노드 등록

노드가 배포된 후 그리드 네트워크를 사용하여 기본 관리 노드에 등록됩니다. 그런 다음 그리드 관리자, 'configure-StorageGrid.py' Python 스크립트 또는 설치 API를 사용하여 그리드를 구성하고 등록된 노드를 승인할 수 있습니다. 그리드 구성 중에 여러 그리드 서브넷을 구성할 수 있습니다. 그리드 네트워크 게이트웨이를 통해 이러한 서브넷에 대한 정적 라우트는 그리드 구성을 완료하면 각 노드에 생성됩니다.

관리 네트워크 또는 클라이언트 네트워크 비활성화

관리 네트워크 또는 클라이언트 네트워크를 사용하지 않도록 설정하려면 노드 승인 프로세스 중에 구성을 제거하거나 설치가 완료된 후 IP 변경 도구를 사용할 수 있습니다(참조) IP 주소를 구성합니다)를 클릭합니다.

설치 후 지침

그리드 노드 배포 및 구성을 완료한 후 DHCP 주소 지정 및 네트워크 구성 변경에 대한 다음 지침을 따르십시오.

- DHCP를 사용하여 IP 주소를 할당한 경우 사용 중인 네트워크의 각 IP 주소에 대해 DHCP 예약을 구성합니다.

  배포 단계에서는 DHCP만 설정할 수 있습니다. 구성 중에는 DHCP를 설정할 수 없습니다.

  > IP 주소가 변경되면 노드가 재부팅되므로 DHCP 주소 변경이 동시에 여러 노드에 영향을 미칠 경우 작동이 중단될 수 있습니다.

- 그리드 노드의 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 변경하려면 IP 변경 절차를 사용해야 합니다. 을 참조하십시오 IP 주소를 구성합니다.
- 라우팅 및 게이트웨이 변경을 비롯한 네트워킹 구성을 변경하면 기본 관리 노드 및 다른 그리드 노드에 대한 클라이언트 연결이 손실될 수 있습니다. 적용된 네트워킹 변경 사항에 따라 이러한 연결을 다시 설정해야 할 수 있습니다.

네트워크 포트 참조

네트워크 인프라스트럭처가 그리드 내의 노드 간, 외부 클라이언트 및 서비스 간에 내부 및 외부 통신을 제공할 수 있는지 확인해야 합니다. 내부 및 외부 방화벽, 스위칭 시스템, 라우팅 시스템 전반에 액세스해야 할 수 있습니다.

에 제공된 세부 정보를 사용합니다 내부 그리드 노드 통신 및 외부 통신 필요한 각 포트를 구성하는 방법을 결정합니다.

내부 그리드 노드 통신

StorageGRID 내부 방화벽은 포트 22, 80, 123 및 443을 제외한 그리드 네트워크의 특정 포트에 대한 들어오는 연결만 허용합니다(외부 통신에 대한 정보 참조). 로드 밸런서 끝점에 의해 정의된 포트에서도 연결이 허용됩니다.

> 그리드 노드 간 ICMP(Internet Control Message Protocol) 트래픽을 사용하는 것이 좋습니다. ICMP 트래픽을 허용하면 그리드 노드에 도달할 수 없을 때 장애 조치 성능을 향상시킬 수 있습니다.

StorageGRID는 표에 나열된 ICMP 및 포트 외에도 VRRP(가상 라우터 이중화 프로토콜)를 사용합니다. VRRP는 IP 프로토콜 번호 112를 사용하는 인터넷 프로토콜입니다. StorageGRID는 유니캐스트 모드에서만 VRRP를 사용합니다. VRRP는 경우에만 필요합니다 고가용성 그룹 구성됩니다.

Linux 기반 노드에 대한 지침

엔터프라이즈 네트워킹 정책이 이러한 포트에 대한 액세스를 제한하는 경우 배포 구성 매개 변수를 사용하여 배포 시 포트를 다시 매핑할 수 있습니다. 포트 재매핑 및 배포 구성 매개 변수에 대한 자세한 내용은 다음을 참조하십시오.

- Red Hat Enterprise Linux 또는 CentOS를 설치합니다
- Ubuntu 또는 Debian을 설치합니다

VMware 기반 노드에 대한 지침입니다

VMware 네트워킹 외부의 방화벽 제한을 정의해야 하는 경우에만 다음 포트를 구성합니다.

엔터프라이즈 네트워킹 정책이 이러한 포트에 대한 액세스를 제한하는 경우 VMware vSphere Web Client를 사용하여 노드를 구축하거나 그리드 노드 구축을 자동화할 때 구성 파일 설정을 사용하여 포트를 재매핑할 수 있습니다. 포트 재매핑 및 배포 구성 매개 변수에 대한 자세한 내용은 을 참조하십시오VMware를 설치합니다.

어플라이언스 노드에 대한 지침

엔터프라이즈 네트워킹 정책에서 이러한 포트에 대한 액세스를 제한하는 경우 StorageGRID 어플라이언스 설치 프로그램을 사용하여 포트를 재매핑할 수 있습니다. 어플라이언스의 포트 재매핑에 대한 자세한 내용은 다음을 참조하십시오.

- SG100 및 SG1000 서비스 어플라이언스
- SG6000 스토리지 어플라이언스
- SG5700 스토리지 어플라이언스
- SG5600 스토리지 어플라이언스

StorageGRID 내부 포트

포트	TCP 또는 UDP입니다	보낸 사람	를 선택합니다	세부 정보

22	TCP	기본 관리자 노드	모든 노드	유지 관리 절차의 경우 기본 관리 노드는 포트 22에서 SSH를 사용하여 다른 모든 노드와 통신할 수 있어야 합니다. 다른 노드의 SSH 트래픽을 허용하는 것은 선택 사항입니다.
80	TCP	어플라이언스	기본 관리자 노드	StorageGRID 어플라이언스에서 운영 관리자 노드와 통신하여 설치를 시작하는 데 사용됩니다.
123을 선택합니다	UDP입니다	모든 노드	모든 노드	네트워크 시간 프로토콜 서비스. 모든 노드는 NTP를 사용하여 다른 모든 노드와 시간을 동기화합니다.
443	TCP	모든 노드	기본 관리자 노드	설치 및 기타 유지 보수 절차 중에 기본 관리 노드에 상태를 전달하는 데 사용됩니다.
1139	TCP	스토리지 노드	스토리지 노드	스토리지 노드 간 내부 트래픽
1501	TCP	모든 노드	ADC가 있는 스토리지 노드	보고, 감사 및 구성 내부 트래픽.
1502)를 참조하십시오	TCP	모든 노드	스토리지 노드	S3 및 Swift 관련 내부 트래픽
1504	TCP	모든 노드	관리자 노드	NMS 서비스 보고 및 구성 내부 트래픽
1505	TCP	모든 노드	관리자 노드	AMS 서비스 내부 트래픽
1506	TCP	모든 노드	모든 노드	서버 상태 내부 트래픽.

1507	TCP	모든 노드	게이트웨이 노드	로드 밸런서 내부 트래픽
1508	TCP	모든 노드	기본 관리자 노드	구성 관리 내부 트래픽
1509	TCP	모든 노드	아카이브 노드	아카이브 노드 내부 트래픽
1511)을 참조하십시오	TCP	모든 노드	스토리지 노드	메타데이터 내부 트래픽.
5353)을 참조하십시오	UDP입니다	모든 노드	모든 노드	설치, 확장 및 복구 중에 전체 그리드 IP 변경 및 운영 관리자 노드 검색에 선택적으로 사용됩니다.
7001)을 참조하십시오	TCP	스토리지 노드	스토리지 노드	Cassandra TLS 노드 간 클러스터 통신.
7443	TCP	모든 노드	관리자 노드	유지보수 절차 및 오류 보고를 위한 내부 트래픽.
8443	TCP	기본 관리자 노드	어플라이언스 노드	유지보수 모드 절차와 관련된 내부 트래픽입니다.
9042	TCP	스토리지 노드	스토리지 노드	Cassandra 클라이언트 포트:
9999	TCP	모든 노드	모든 노드	여러 서비스의 내부 트래픽. 유지 보수 절차, 메트릭 및 네트워킹 업데이트를 포함합니다.
10226	TCP	스토리지 노드	기본 관리자 노드	StorageGRID 어플라이언스에서 E-Series SANtricity 시스템 관리자의 AutoSupport 메시지를 운영 관리 노드로 전달하는 데 사용됩니다.

11139	TCP	아카이브/스토리지 노드	아카이브/스토리지 노드	스토리지 노드와 아카이브 노드 간의 내부 트래픽입니다.
18000입니다	TCP	관리/스토리지 노드	ADC가 있는 스토리지 노드	계정 서비스 내부 트래픽.
18001	TCP	관리/스토리지 노드	ADC가 있는 스토리지 노드	ID 페더레이션 내부 트래픽.
18002	TCP	관리/스토리지 노드	스토리지 노드	객체 프로토콜과 관련된 내부 API 트래픽입니다.
18003	TCP	관리/스토리지 노드	ADC가 있는 스토리지 노드	플랫폼 서비스 내부 트래픽
18017	TCP	관리/스토리지 노드	스토리지 노드	Data Mover Service Cloud Storage Pool의 내부 트래픽입니다.
18019	TCP	스토리지 노드	스토리지 노드	삭제 코딩을 위한 청크 서비스 내부 트래픽입니다.
18082	TCP	관리/스토리지 노드	스토리지 노드	S3 관련 내부 트래픽.
18083	TCP	모든 노드	스토리지 노드	스위프트 관련 내부 트래픽.
18200	TCP	관리/스토리지 노드	스토리지 노드	클라이언트 요청에 대한 추가 통계입니다.
19000입니다	TCP	관리/스토리지 노드	ADC가 있는 스토리지 노드	Keystone 서비스 내부 트래픽

- 관련 정보 *

외부 통신

외부 통신

클라이언트는 콘텐츠를 수집하고 검색하기 위해 그리드 노드와 통신해야 합니다. 사용되는 포트는 선택한 오브젝트 스토리지 프로토콜에 따라 다릅니다. 이러한 포트는 클라이언트에서 액세스할 수 있어야 합니다.

포트에 대한 액세스가 제한되어 있습니다

엔터프라이즈 네트워킹 정책에서 포트에 대한 액세스를 제한하는 경우 를 사용할 수 있습니다 부하 분산 장치 엔드포인트 사용자 정의 포트에 대한 액세스를 허용합니다. 그런 다음 를 사용할 수 있습니다 신뢰할 수 없는 클라이언트 네트워크 로드 밸런서 엔드포인트 포트에만 액세스를 허용합니다.

포트 재매핑

SMTP, DNS, SSH 또는 DHCP와 같은 시스템 및 프로토콜을 사용하려면 노드를 배포할 때 포트를 재매핑해야 합니다. 하지만 로드 밸런서 끝점을 다시 매핑하면 안 됩니다. 포트 재매핑에 대한 자세한 내용은 해당 플랫폼의 설치 지침을 참조하십시오.

소프트웨어 기반 노드

- Red Hat Enterprise Linux 또는 CentOS를 설치합니다
- Ubuntu 또는 Debian을 설치합니다
- VMware를 설치합니다

어플라이언스 노드

- SG100 및 SG1000 서비스 어플라이언스
- SG6000 스토리지 어플라이언스
- SG5700 스토리지 어플라이언스
- SG5600 스토리지 어플라이언스

외부 통신에 사용되는 포트

다음 표는 노드로의 트래픽에 사용되는 포트를 보여줍니다.

> 이 목록에는 로 구성할 수 있는 포트가 포함되어 있지 않습니다 부하 분산 장치 엔드포인트 또는 에 사용됩니다 "Syslog 서버".

포트	**TCP** 또는 **UDP**입니다	프로토콜	보낸 사람	를 선택합니다	세부 정보
22	TCP	SSH를 클릭합니다	서비스 노트북	모든 노드	콘솔 단계를 사용하는 절차를 수행하려면 SSH 또는 콘솔 액세스가 필요합니다. 선택적으로 22가 아닌 2022번 포트를 사용할 수 있습니다.
25	TCP	SMTP	관리자 노드	이메일 서버	알림 및 이메일 기반 AutoSupport에 사용됩니다. 이메일 서버 페이지를 사용하여 기본 포트 설정 25를 재정의할 수 있습니다.
53	TCP/UDP	DNS	모든 노드	DNS 서버	도메인 이름 시스템에 사용됩니다.

포트	**TCP** 또는 **UDP**입니다	프로토콜	보낸 사람	를 선택합니다	세부 정보
67	UDP입니다	DHCP를 선택합니다	모든 노드	DHCP 서비스	DHCP 기반 네트워크 구성을 지원하는 데 선택적으로 사용됩니다. dhclient 서비스는 정적으로 구성된 그리드에 대해 실행되지 않습니다.
68	UDP입니다	DHCP를 선택합니다	DHCP 서비스	모든 노드	DHCP 기반 네트워크 구성을 지원하는 데 선택적으로 사용됩니다. dhclient 서비스는 고정 IP 주소를 사용하는 그리드에 대해서는 실행되지 않습니다.
80	TCP	HTTP	브라우저	관리자 노드	포트 80은 관리 노드 사용자 인터페이스를 위해 포트 443으로 리디렉션합니다.
80	TCP	HTTP	브라우저	어플라이언스	포트 80이 StorageGRID 어플라이언스 설치 프로그램의 포트 8443으로 리디렉션됩니다.
80	TCP	HTTP	ADC가 있는 스토리지 노드	설치하고	AWS 또는 HTTP를 사용하는 기타 외부 서비스에 전송된 플랫폼 서비스 메시지에 사용됩니다. 테넌트는 엔드포인트를 생성할 때 기본 HTTP 포트 설정 80을 재정의할 수 있습니다.
80	TCP	HTTP	스토리지 노드	설치하고	Cloud Storage Pools 요청이 HTTP를 사용하는 AWS 타겟으로 전송됩니다. 그리드 관리자는 클라우드 스토리지 풀을 구성할 때 기본 HTTP 포트 설정을 80으로 재정의할 수 있습니다.
111	TCP/UDP	rpcbind	NFS 클라이언트	관리자 노드	NFS 기반 감사 내보내기(portmap)에서 사용됩니다. • 참고: * 이 포트는 NFS 기반 감사 내보내기가 활성화된 경우에만 필요합니다.

포트	**TCP** 또는 **UDP**입니다	프로토콜	보낸 사람	를 선택합니다	세부 정보
123을 선택합니다	UDP입니다	NTP	기본 NTP 노드입니다	외부 NTP	네트워크 시간 프로토콜 서비스. 또한 주 NTP 소스로 선택된 노드는 외부 NTP 시간 소스와 클록 시간을 동기화합니다.
137	UDP입니다	NetBIOS입니다	SMB 클라이언트	관리자 노드	NetBIOS 지원이 필요한 클라이언트에 대해 SMB 기반 감사 내보내기에서 사용됩니다. • 참고: * 이 포트는 SMB 기반 감사 내보내기가 활성화된 경우에만 필요합니다.
138	UDP입니다	NetBIOS입니다	SMB 클라이언트	관리자 노드	NetBIOS 지원이 필요한 클라이언트에 대해 SMB 기반 감사 내보내기에서 사용됩니다. • 참고: * 이 포트는 SMB 기반 감사 내보내기가 활성화된 경우에만 필요합니다.
139	TCP	중소기업	SMB 클라이언트	관리자 노드	NetBIOS 지원이 필요한 클라이언트에 대해 SMB 기반 감사 내보내기에서 사용됩니다. • 참고: * 이 포트는 SMB 기반 감사 내보내기가 활성화된 경우에만 필요합니다.

포트	**TCP** 또는 **UDP**입니다	프로토콜	보낸 사람	를 선택합니다	세부 정보
161	TCP/UDP	SNMP를 선택합니다	SNMP 클라이언트	모든 노드	SNMP 폴링에 사용됩니다. 모든 노드는 기본 정보를 제공하고, 관리 노드는 경고 및 경보 데이터도 제공합니다. 구성 시 기본적으로 UDP 포트 161이 사용됩니다. • 참고: * 이 포트는 필요한 경우에만 필요하며 SNMP가 구성된 경우에만 노드 방화벽에서 열립니다. SNMP를 사용하려는 경우 대체 포트를 구성할 수 있습니다. • 참고: * StorageGRID와 함께 SNMP를 사용하는 방법에 대한 자세한 내용은 NetApp 어카운트 담당자에게 문의하십시오.
162	TCP/UDP	SNMP 알림	모든 노드	통지 대상	아웃바운드 SNMP 알림 및 트랩은 기본적으로 UDP 포트 162로 설정됩니다. • 참고: * 이 포트는 SNMP가 활성화되고 알림 대상이 구성된 경우에만 필요합니다. SNMP를 사용하려는 경우 대체 포트를 구성할 수 있습니다. • 참고: * StorageGRID와 함께 SNMP를 사용하는 방법에 대한 자세한 내용은 NetApp 어카운트 담당자에게 문의하십시오.
389	TCP/UDP	LDAP를 지원합니다	ADC가 있는 스토리지 노드	Active Directory/LDAP를 선택합니다	ID 페더레이션을 위해 Active Directory 또는 LDAP 서버에 연결하는 데 사용됩니다.
443	TCP	HTTPS	브라우저	관리자 노드	그리드 관리자 및 테넌트 관리자에 액세스하기 위해 웹 브라우저 및 관리 API 클라이언트에서 사용됩니다.

포트	**TCP** 또는 **UDP**입니다	프로토콜	보낸 사람	를 선택합니다	세부 정보
443	TCP	HTTPS	관리자 노드	Active Directory를 클릭합니다	SSO(Single Sign-On)가 활성화된 경우 Active Directory에 연결하는 관리 노드에서 사용됩니다.
443	TCP	HTTPS	아카이브 노드	Amazon S3	아카이브 노드에서 Amazon S3에 액세스하는 데 사용됩니다.
443	TCP	HTTPS	ADC가 있는 스토리지 노드	설치하고	AWS로 전송된 플랫폼 서비스 메시지 또는 HTTPS를 사용하는 기타 외부 서비스에 사용됩니다. 테넌트는 엔드포인트를 생성할 때 기본 HTTP 포트 설정 443을 재정의할 수 있습니다.
443	TCP	HTTPS	스토리지 노드	설치하고	Cloud Storage Pools 요청이 HTTPS를 사용하는 AWS 타겟으로 전송됩니다. 그리드 관리자는 클라우드 스토리지 풀을 구성할 때 기본 HTTPS 포트 설정 443을 재정의할 수 있습니다.
445	TCP	중소기업	SMB 클라이언트	관리자 노드	SMB 기반 감사 내보내기에 사용됩니다. • 참고: * 이 포트는 SMB 기반 감사 내보내기가 활성화된 경우에만 필요합니다.
903	TCP	NFS 를 참조하십시오	NFS 클라이언트	관리자 노드	NFS 기반 감사 내보내기('RPC.mountd')에서 사용됩니다. • 참고: * 이 포트는 NFS 기반 감사 내보내기가 활성화된 경우에만 필요합니다.
2022	TCP	SSH를 클릭합니다	서비스 노트북	모든 노드	콘솔 단계를 사용하는 절차를 수행하려면 SSH 또는 콘솔 액세스가 필요합니다. 선택적으로 2022 대신 포트 22를 사용할 수 있습니다.

포트	**TCP** 또는 **UDP**입니다	프로토콜	보낸 사람	를 선택합니다	세부 정보
2049	TCP	NFS 를 참조하십시오	NFS 클라이언트	관리자 노드	NFS 기반 감사 내보내기(NFS)에서 사용됩니다. • 참고: * 이 포트는 NFS 기반 감사 내보내기가 활성화된 경우에만 필요합니다.
5696	TCP	KMIP	어플라이언스	킬로미터	KMIP(Key Management Interoperability Protocol) 노드 암호화를 위해 구성된 어플라이언스에서 KMS(Key Management Server)로의 외부 트래픽(StorageGRID 어플라이언스 설치 프로그램의 KMS 구성 페이지에 다른 포트가 지정되지 않은 경우)
8022	TCP	SSH를 클릭합니다	서비스 노트북	모든 노드	포트 8022의 SSH는 지원 및 문제 해결을 위해 어플라이언스 및 가상 노드 플랫폼에서 기본 운영 체제에 대한 액세스 권한을 부여합니다. 이 포트는 Linux 기반(베어 메탈) 노드에 사용되지 않으며 그리드 노드 간에 또는 정상 운영 중에 액세스할 필요가 없습니다.
8082	TCP	HTTPS	S3 클라이언트	게이트웨이 노드	게이트웨이 노드(HTTPS)에서 더 이상 사용되지 않는 CLB 서비스에 대한 S3 클라이언트 트래픽.
8083	TCP	HTTPS	SWIFT 클라이언트	게이트웨이 노드	게이트웨이 노드(HTTPS)에서 더 이상 사용되지 않는 CLB 서비스로 스위프트 클라이언트 트래픽을 전송합니다.
8084	TCP	HTTP	S3 클라이언트	게이트웨이 노드	게이트웨이 노드(HTTP)에서 더 이상 사용되지 않는 CLB 서비스에 대한 S3 클라이언트 트래픽.
8085	TCP	HTTP	SWIFT 클라이언트	게이트웨이 노드	HTTP(Gateway Nodes)에서 더 이상 사용되지 않는 CLB 서비스로 스위프트 클라이언트 트래픽을 전송합니다.

포트	**TCP** 또는 **UDP**입니다	프로토콜	보낸 사람	를 선택합니다	세부 정보
8443	TCP	HTTPS	브라우저	관리자 노드	선택 사항. 웹 브라우저 및 관리 API 클라이언트에서 Grid Manager에 액세스하는 데 사용됩니다. Grid Manager와 Tenant Manager 통신을 구분하는 데 사용할 수 있습니다.
9022	TCP	SSH를 클릭합니다	서비스 노트북	어플라이언스	지원 및 문제 해결을 위해 사전 구성 모드에서 StorageGRID 어플라이언스에 대한 액세스 권한을 부여합니다. 이 포트는 그리드 노드 간 또는 정상 작업 중에 액세스할 필요가 없습니다.
9091	TCP	HTTPS	외부 Grafana 서비스	관리자 노드	외부 Grafana 서비스에서 StorageGRID Prometheus 서비스에 안전하게 액세스하는 데 사용됩니다. • 참고: * 이 포트는 인증서 기반 Prometheus 액세스가 활성화된 경우에만 필요합니다.
9443	TCP	HTTPS	브라우저	관리자 노드	선택 사항. 테넌트 관리자를 액세스하기 위해 웹 브라우저 및 관리 API 클라이언트에서 사용됩니다. Grid Manager와 Tenant Manager 통신을 구분하는 데 사용할 수 있습니다.
18082	TCP	HTTPS	S3 클라이언트	스토리지 노드	S3 클라이언트 트래픽이 스토리지 노드(HTTPS)로 직접 전송됩니다.
18083	TCP	HTTPS	SWIFT 클라이언트	스토리지 노드	Swift 클라이언트 트래픽이 스토리지 노드(HTTPS)로 직접 전송됩니다.
18084	TCP	HTTP	S3 클라이언트	스토리지 노드	S3 클라이언트 트래픽이 스토리지 노드(HTTP)로 직접 연결됩니다.
18085	TCP	HTTP	SWIFT 클라이언트	스토리지 노드	Swift 클라이언트 트래픽이 스토리지 노드(HTTP)로 직접 연결됩니다.

어플라이언스 하드웨어를 설치하고 유지 관리합니다

SG100 및 SG1000 서비스 어플라이언스

SG100 및 SG1000 어플라이언스: 개요

StorageGRID SG100 서비스 어플라이언스 및 SG1000 서비스 어플라이언스는 게이트웨이 노드 및 관리자 노드로 작동하여 StorageGRID 시스템에서 고가용성 로드 밸런싱 서비스를 제공할 수 있습니다. 두 어플라이언스 모두 게이트웨이 노드와 관리 노드(운영 또는 비운영)로 동시에 작동할 수 있습니다.

어플라이언스 기능

두 서비스 어플라이언스 모델 모두 다음과 같은 기능을 제공합니다.

- StorageGRID 시스템의 게이트웨이 노드 또는 관리자 노드 기능
- 노드 배포 및 구성을 간소화하는 StorageGRID 어플라이언스 설치 프로그램
- 를 구축하면 기존 관리 노드나 로컬 드라이브로 다운로드한 소프트웨어에서 StorageGRID 소프트웨어에 액세스할 수 있습니다. 배포 프로세스를 더욱 단순화하기 위해 제조 과정에서 최신 버전의 소프트웨어가 어플라이언스에 사전 로드됩니다.
- 일부 어플라이언스 하드웨어를 모니터링하고 진단하기 위한 베이스보드 관리 컨트롤러(BMC).
- 그리드 네트워크, 관리자 네트워크 및 클라이언트 네트워크를 포함한 세 가지 StorageGRID 네트워크에 모두 연결할 수 있는 기능:
  - SG100은 그리드 네트워크 및 클라이언트 네트워크에 대한 10GbE 또는 25GbE 연결을 최대 4개까지 지원합니다.
  - SG1000은 그리드 네트워크 및 클라이언트 네트워크에 대한 10, 25, 40 또는 100 GbE 연결을 최대 4개까지 지원합니다.

SG100 및 SG1000 다이어그램

이 그림은 베젤이 분리된 SG100과 SG1000의 전면을 보여줍니다.

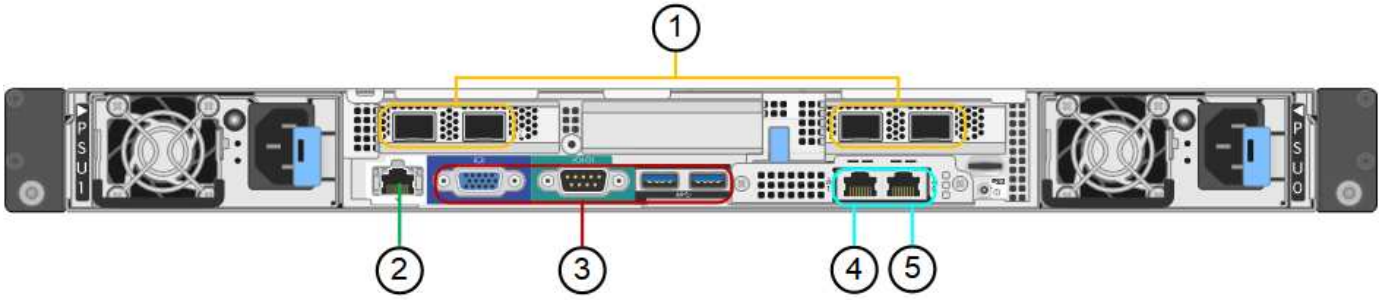
> 전면에서 두 어플라이언스는 베젤에 있는 제품 이름을 제외하고 동일합니다.

주황색 윤곽선으로 표시된 2개의 SSD(Solid State Drive)는 StorageGRID 운영 체제를 저장하는 데 사용되며 이중화를 위해 RAID1을 사용하여 미러링됩니다. SG100 또는 SG1000 서비스 어플라이언스가 관리 노드로 구성된 경우 이러한 드라이브는 감사 로그, 메트릭 및 데이터베이스 테이블을 저장하는 데 사용됩니다.

나머지 드라이브 슬롯은 비어 있습니다.

SG100 후면에 있는 커넥터

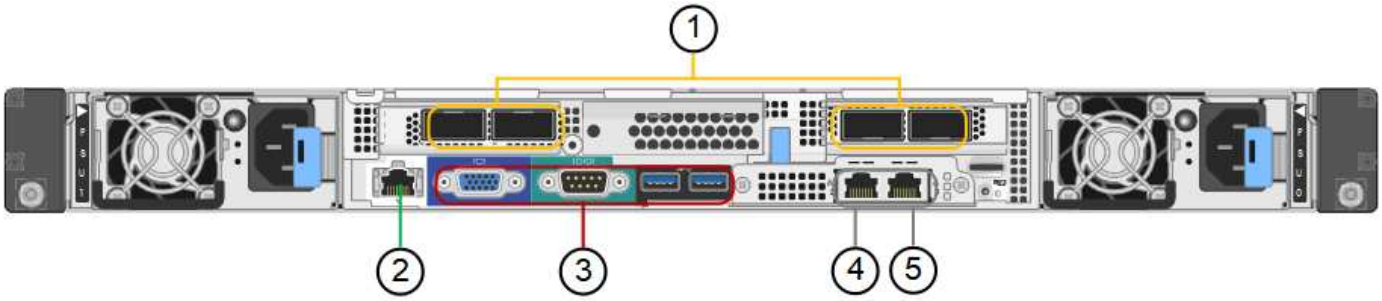
이 그림은 SG100 후면에 있는 커넥터를 보여줍니다.



	포트	유형	사용
1	네트워크 포트 1-4	케이블 또는 SFP 트랜시버 유형(SFP28 및 SFP+ 모듈 지원), 스위치 속도 및 구성된 링크 속도를 기반으로 한 10/25-GbE	그리드 네트워크 및 StorageGRID용 클라이언트 네트워크에 연결합니다.
2	BMC 관리 포트	1GbE(RJ-45)	어플라이언스 베이스보드 관리 컨트롤러에 연결합니다.
3	진단 및 지원 포트	• VGA • 직렬, 115200 8-N-1 • USB	기술 지원용으로 예약되어 있습니다.
4	관리 네트워크 포트 1	1GbE(RJ-45)	StorageGRID용 관리 네트워크에 어플라이언스를 연결합니다.
5	관리 네트워크 포트 2	1GbE(RJ-45)	옵션: • StorageGRID용 관리 네트워크에 대한 중복 연결을 위해 관리 포트 1과 연결합니다. • 연결이 끊어진 상태로 임시 로컬 액세스(IP 169.254.0.1)에 대해 사용 가능한 상태로 둡니다. • 설치하는 동안 DHCP 할당 IP 주소를 사용할 수 없는 경우 IP 구성에 포트 2를 사용합니다.

SG1000 후면의 커넥터

이 그림은 SG1000 후면의 커넥터를 보여줍니다.



	포트	유형	사용
1	네트워크 포트 1-4	케이블 또는 트랜시버 유형, 스위치 속도 및 구성된 링크 속도를 기반으로 하는 10/25/40/100GbE QSFP28 및 QSFP+(40/100GbE)는 기본적으로 지원되며 QSA(별도 판매)와 함께 SFP28/SFP+ 트랜시버를 사용하여 10/25GbE 속도를 사용할 수 있습니다.	그리드 네트워크 및 StorageGRID용 클라이언트 네트워크에 연결합니다.
2	BMC 관리 포트	1GbE(RJ-45)	어플라이언스 베이스보드 관리 컨트롤러에 연결합니다.
3	진단 및 지원 포트	• VGA • 직렬, 115200 8-N-1 • USB	기술 지원용으로 예약되어 있습니다.
4	관리 네트워크 포트 1	1GbE(RJ-45)	StorageGRID용 관리 네트워크에 어플라이언스를 연결합니다.

	포트	유형	사용
5	관리 네트워크 포트 2	1GbE(RJ-45)	옵션: • StorageGRID용 관리 네트워크에 대한 중복 연결을 위해 관리 포트 1과 연결합니다. • 연결이 끊어진 상태로 임시 로컬 액세스(IP 169.254.0.1)에 대해 사용 가능한 상태로 둡니다. • 설치하는 동안 DHCP 할당 IP 주소를 사용할 수 없는 경우 IP 구성에 포트 2를 사용합니다.

SG100 및 SG1000 응용 프로그램

게이트웨이 서비스를 제공하는 다양한 방법과 일부 그리드 관리 서비스의 이중화를 위해 StorageGRID 서비스 어플라이언스를 구성할 수 있습니다.

어플라이언스는 다음과 같은 방법으로 배포할 수 있습니다.

- 새 그리드 또는 기존 그리드를 게이트웨이 노드로 추가합니다
- 새 그리드에 기본 또는 비 기본 관리 노드로 추가하거나 기존 그리드에 비 기본 관리 노드로 추가합니다
- 게이트웨이 노드 및 관리 노드(기본 또는 비기본)로 동시에 작동합니다

이 어플라이언스를 사용하면 고가용성(HA) 그룹과 S3 또는 Swift 데이터 경로 연결을 위한 지능형 로드 밸런싱을 손쉽게 사용할 수 있습니다.

다음 예에서는 제품의 기능을 극대화하는 방법을 설명합니다.

- 2개의 SG100 또는 2개의 SG1000 어플라이언스를 사용하여 게이트웨이 노드로 구성하여 게이트웨이 서비스를 제공하십시오.

  > SG100 및 SG1000 서비스 어플라이언스를 같은 사이트에 배포하지 마십시오. 성능을 예측할 수 없습니다.

- 일부 그리드 관리 서비스의 이중화를 제공하려면 SG100 또는 SG1000 어플라이언스 2개를 사용하십시오. 각 어플라이언스를 관리자 노드로 구성하여 이 작업을 수행합니다.
- 2개의 SG100 또는 2개의 SG1000 어플라이언스를 사용하여 하나 이상의 가상 IP 주소를 통해 액세스되는 고가용성 로드 밸런싱 및 트래픽 셰이핑 서비스를 제공합니다. 이 작업을 수행하려면 관리 노드 또는 게이트웨이 노드의 조합으로 어플라이언스를 구성하고 두 노드를 동일한 HA 그룹에 추가합니다.

동일한 HA 그룹에서 관리 노드와 게이트웨이 노드를 사용하는 경우 CLB(연결 로드 밸런서) 포트와 관리 노드 전용 포트는 페일오버되지 않습니다. HA 그룹 구성에 대한 지침은 StorageGRID 관리 지침을 참조하십시오.

CLB 서비스는 더 이상 사용되지 않습니다.

SG100과 SG1000 서비스 어플라이언스를 StorageGRID 스토리지 어플라이언스와 함께 사용하면 외부 하이퍼바이저 또는 컴퓨팅 하드웨어에 종속되지 않고 어플라이언스 전용 그리드를 구축할 수 있습니다.

관련 정보

StorageGRID 관리

설치 및 구축 개요

StorageGRID를 처음 구축할 때 하나 이상의 StorageGRID 서비스 어플라이언스를 설치하거나 나중에 확장의 일부로 서비스 어플라이언스 노드를 추가할 수 있습니다.

필요한 것

StorageGRID 시스템에서 필요한 버전의 StorageGRID 소프트웨어를 사용하고 있습니다.

어플라이언스	필수 **StorageGRID** 버전입니다
SG100	11.4 이상(최신 핫픽스 권장)
SG1000	11.3 이상(최신 핫픽스 권장)

설치 및 구축 작업

그리드에 StorageGRID 어플라이언스 준비 및 추가에는 4가지 기본 단계가 있습니다.

1. 설치 준비 중:
   - 설치 사이트 준비 중
   - 박스 포장 풀기 및 내용물 확인
   - 추가 장비 및 도구 확보
   - 네트워크 구성을 확인하는 중입니다
   - 선택 사항: 모든 어플라이언스 데이터를 암호화하려는 경우 외부 키 관리 서버(KMS) 구성 StorageGRID 관리 지침에 있는 외부 키 관리에 대한 자세한 내용을 참조하십시오.
2. 하드웨어 설치:
   - 하드웨어를 등록하는 중입니다
   - 캐비닛 또는 랙에 제품 설치
   - 어플라이언스 케이블 연결
   - 전원 코드 연결 및 전원 공급

- 부팅 상태 코드 보기

3. 하드웨어 구성:
   - StorageGRID 어플라이언스 설치 프로그램에 액세스하고 StorageGRID 네트워크에 연결하는 데 필요한 링크 및 네트워크 IP 설정을 구성합니다
   - 어플라이언스의 베이스보드 관리 컨트롤러(BMC) 인터페이스에 액세스합니다.
   - 선택 사항: 외부 KMS를 사용하여 어플라이언스 데이터를 암호화하려는 경우 노드 암호화 사용
4. 어플라이언스 게이트웨이 또는 관리 노드 배포

   어플라이언스 하드웨어를 설치 및 구성한 후 어플라이언스를 게이트웨이 노드 및 StorageGRID 시스템에 관리 노드로 배포할 수 있습니다. SG100과 SG1000 어플라이언스는 모두 게이트웨이 노드 및 관리 노드(운영 노드 및 비운영 노드)로 동시에 작동할 수 있습니다.

작업	지침
새 StorageGRID 시스템에 어플라이언스 게이트웨이 또는 관리자 노드 배포	서비스 어플라이언스 노드를 배포합니다
기존 StorageGRID 시스템에 어플라이언스 게이트웨이 또는 관리자 노드 추가	StorageGRID 시스템을 확장합니다
노드 복구 작업의 일부로 어플라이언스 게이트웨이 또는 관리 노드 배포	StorageGRID 시스템 복구 및 유지 관리

관련 정보

그리드를 확장합니다

그리드 복구 및 유지 관리

StorageGRID 관리

설치 준비(SG100 및 SG1000)

StorageGRID 어플라이언스 설치를 준비하는 과정에서 사이트 준비 및 필요한 모든 하드웨어, 케이블 및 도구 확보 작업이 수반됩니다. 또한 IP 주소와 네트워크 정보도 수집해야 합니다.

관련 정보

웹 브라우저 요구 사항

사이트 준비(SG100 및 SG1000)

제품을 설치하기 전에 StorageGRID 어플라이언스의 사양을 충족하는 사이트와 캐비닛 또는 랙이 맞는지 확인해야 합니다.

단계

1. 사이트가 온도, 습도, 고도 범위, 공기 흐름, 열 손실 요구 사항을 충족하는지 확인합니다. 배선, 전원 및 접지. 자세한 내용은 NetApp Hardware Universe를 참조하십시오.

2. 현재 위치에서 AC 전원의 전압이 올바른지 확인합니다(120 - 240V AC 범위).
3. 이 크기의 선반에 맞게 19인치(48.3-cm) 캐비닛 또는 랙을 준비합니다(케이블 제외).

높이	너비	깊이	최대 중량
1.70in. (4.32cm)	17.32in. (44.0cm)	32.0in. (81.3cm)	39lb. (17.7kg)

4. 제품을 설치할 위치를 결정합니다.

관련 정보

"NetApp Hardware Universe를 참조하십시오"

"NetApp 상호 운용성 매트릭스 툴"

박스 포장 풀기**(SG100** 및 **SG1000)**

StorageGRID 제품을 설치하기 전에 모든 상자의 포장을 풀고 내용물을 포장 명세서에 있는 품목과 비교합니다.

어플라이언스 하드웨어

- SG100 또는 SG1000 *

- * 지침이 포함된 레일 키트 *

전원 코드

StorageGRID 제품 배송에는 다음 전원 코드가 포함됩니다.

- * 해당 국가용 전원 코드 2개 *

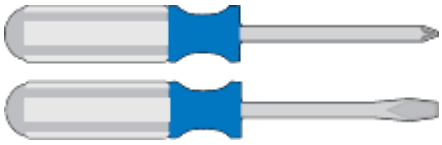
캐비닛에는 제품과 함께 제공된 전원 코드 대신 사용하는 특수 전원 코드가 있을 수 있습니다.

추가 장비 및 도구 확보**(SG100** 및 **SG1000)**

StorageGRID 제품을 설치하기 전에 필요한 추가 장비와 도구가 모두 있는지 확인하십시오.

하드웨어를 설치하고 구성하려면 다음 추가 장비가 필요합니다.

- * 스크류드라이버 *

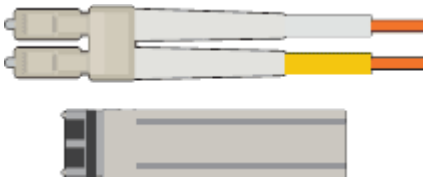


필립스 번호 2 드라이버

중형 일자 드라이버

- * ESD 손목 스트랩 *

- * 광 케이블 및 트랜시버 *



  - 케이블
    - Twinax/구리(1-4개)

      또는

    - 파이버/광(1-4개)
  - 링크 속도를 기반으로 하는 이러한 트랜시버/어댑터 중 1-4개(혼합 속도는 지원되지 않음)
    - SG100:

링크 속도**(GbE)**	필수 장비
10	SFP+ 트랜시버

링크 속도(**GbE**)	필수 장비
25	SFP28 트랜시버

- SG1000:

링크 속도(**GbE**)	필수 장비
10	QSFP-SFP 어댑터(QSA) 및 SFP+ 트랜시버
25	QSFP-SFP 어댑터(QSA) 및 SFP28 트랜시버
40	QSFP+ 트랜시버
100	QFSP28 트랜시버

- RJ-45(Cat5/Cat5e/Cat6/CAT6A) 이더넷 케이블 *

- * 서비스 노트북 *

지원되는 웹 브라우저

1GbE(RJ-45) 포트

> 일부 포트는 10/100 이더넷 속도를 지원하지 않을 수 있습니다.

- * 옵션 도구 *

Phillips 헤드 비트를 이용한 파워 드릴

플래시

어플라이언스 네트워크 연결 검토**(SG100** 및 **SG1000)**

StorageGRID 어플라이언스를 설치하기 전에 어플라이언스에 연결할 수 있는 네트워크를 이해해야 합니다.

StorageGRID 어플라이언스를 StorageGRID 시스템에 노드로 구축할 경우 다음 네트워크에 연결할 수 있습니다.

- * StorageGRID * 용 그리드 네트워크: 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용됩니다. 그리드에서 모든 사이트 및 서브넷의 모든 노드 간에 연결을 제공합니다. 그리드 네트워크가 필요합니다.
- StorageGRID*용 관리자 네트워크: 관리자 네트워크는 시스템 관리 및 유지 보수에 사용되는 폐쇄된 네트워크입니다. 관리 네트워크는 일반적으로 사설 네트워크이며 사이트 간에 라우팅할 필요가 없습니다. 관리 네트워크는 선택 사항입니다.
- * StorageGRID용 클라이언트 네트워크: * 클라이언트 네트워크는 S3 및 Swift를 포함한 클라이언트 애플리케이션에 대한 액세스를 제공하는 데 사용되는 개방형 네트워크입니다. 클라이언트 네트워크는 그리드에 대한 클라이언트 프로토콜 액세스를 제공하므로 그리드 네트워크를 격리하고 보호할 수 있습니다. 이 네트워크를 통해 어플라이언스가 열려 있는 포트만 사용하여 액세스할 수 있도록 클라이언트 네트워크를 구성할 수 있습니다. 클라이언트 네트워크는 선택 사항입니다.
- 서비스 어플라이언스용 * BMC 관리 네트워크 * (선택 사항): 이 네트워크는 SG100 및 SG1000의 베이스보드 관리 컨트롤러에 대한 액세스를 제공합니다. 이 네트워크를 사용하면 어플라이언스에서 하드웨어 구성요소를 모니터링하고 관리할 수 있습니다. 이 관리 네트워크는 StorageGRID용 관리 네트워크와 같을 수도 있고 독립 관리 네트워크일 수도 있습니다.

  선택적 BMC 관리 네트워크가 연결되지 않은 경우 일부 지원 및 유지 관리 절차를 수행하기가 더 어려워집니다. 지원 목적으로 필요한 경우를 제외하고 BMC 관리 네트워크를 연결하지 않은 상태로 둘 수 있습니다.

관련 정보

설치 정보 수집(SG100 및 SG1000)

케이블 어플라이언스 SG100 및 SG1000

네트워킹 지침

그리드 프라이머

SG100 및 **SG1000** 어플라이언스의 포트 결합 모드입니다

SG100 및 SG1000 어플라이언스에 대한 네트워크 링크를 구성할 때 그리드 네트워크 및 선택적 클라이언트 네트워크에 연결하는 포트와 선택적 관리 네트워크에 연결하는 1GbE 관리 포트에 포트 결합을 사용할 수 있습니다. 포트 본딩을 사용하면 StorageGRID 네트워크와 어플라이언스 간에 중복 경로를 제공하여 데이터를 보호할 수 있습니다.

네트워크 연결 모드

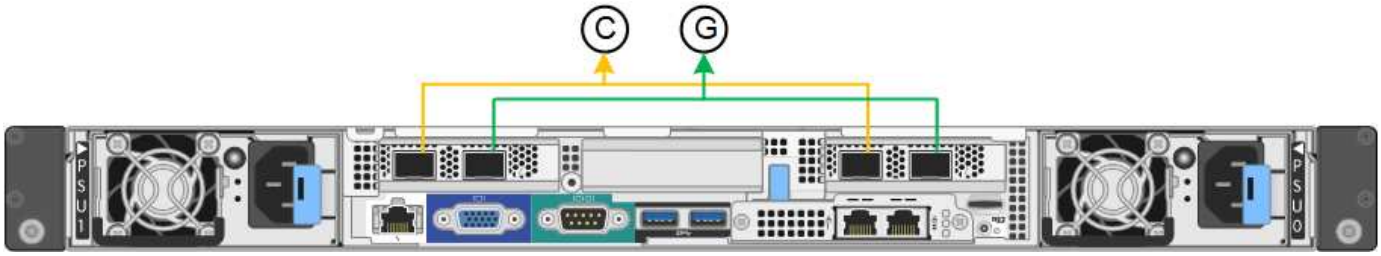
서비스 어플라이언스의 네트워킹 포트는 그리드 네트워크 및 클라이언트 네트워크 연결을 위한

고정 포트 결합 모드 또는 집계 포트 결합 모드를 지원합니다.

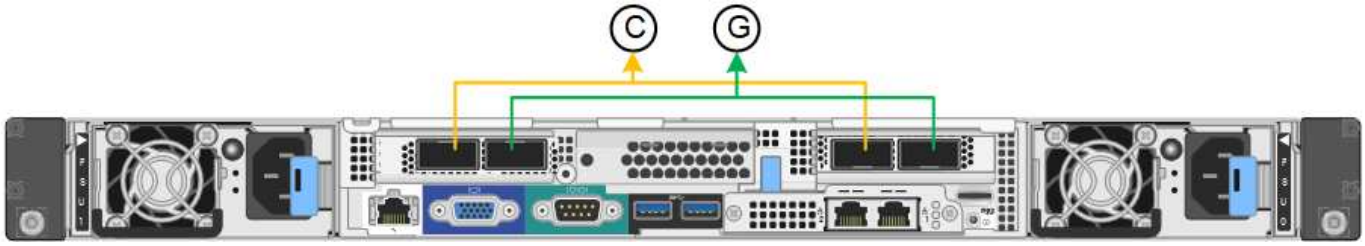
고정 포트 결합 모드

고정 포트 결합 모드는 네트워킹 포트의 기본 구성입니다.

- SG100 고정 포트 결합 모드 *



- SG1000 고정 포트 결합 모드 *



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
c	이 네트워크를 사용하는 경우 포트 1과 3이 클라이언트 네트워크에 대해 함께 연결됩니다.
g	포트 2와 4는 그리드 네트워크를 위해 서로 연결되어 있습니다.

고정 포트 결합 모드를 사용할 때 포트는 액티브-백업 모드 또는 링크 통합 제어 프로토콜 모드(802.3ad)를 사용하여 본드 결합할 수 있습니다.

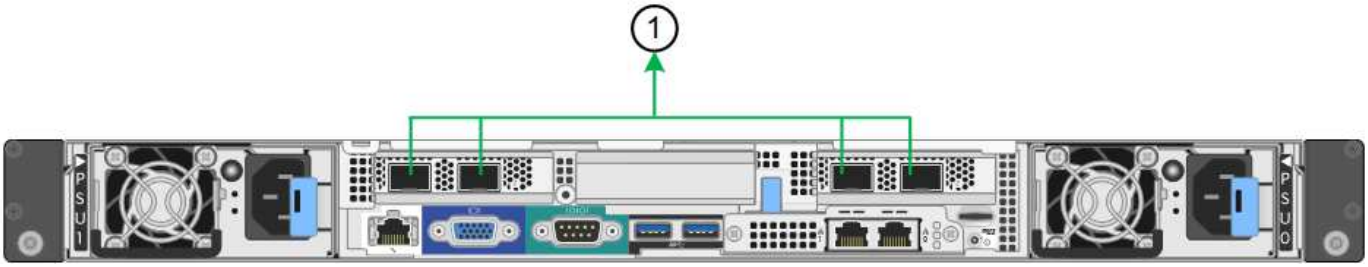
- 액티브-백업 모드(기본값)에서는 한 번에 하나의 포트만 활성화됩니다. 활성 포트에 장애가 발생하면 백업 포트가 자동으로 페일오버 연결을 제공합니다. 포트 4는 포트 2(그리드 네트워크)에 대한 백업 경로를 제공하고 포트 3은 포트 1(클라이언트 네트워크)에 대한 백업 경로를 제공합니다.
- LACP 모드에서 각 포트 쌍은 서비스 어플라이언스와 네트워크 간에 논리 채널을 형성하여 처리량을 높여줍니다. 한 포트에 장애가 발생해도 다른 포트는 계속 채널을 제공합니다. 처리량은 감소하지만 연결성은 영향을 받지 않습니다.

> 중복 연결이 필요하지 않은 경우 각 네트워크에 대해 하나의 포트만 사용할 수 있습니다. 그러나 StorageGRID가 설치된 후 그리드 관리자에서 * 서비스 어플라이언스 링크 다운 * 경고가 트리거되어 케이블이 분리되었음을 나타낼 수 있습니다. 이 경고 규칙을 안전하게 비활성화할 수 있습니다.

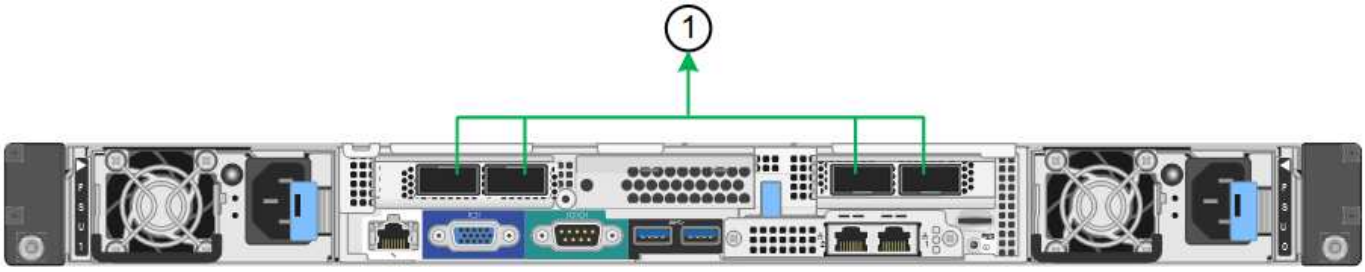
애그리게이트 포트 결합 모드

애그리게이트 포트 결합 모드는 각 StorageGRID 네트워크의 처리량을 크게 증가시키고 추가 페일오버 경로를 제공합니다.

- SG100 애그리게이트 포트 결합 모드 *



- SG1000 집계 포트 결합 모드 *



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
1	연결된 모든 포트는 단일 LACP 결합으로 그룹화되므로 모든 포트를 그리드 네트워크 및 클라이언트 네트워크 트래픽에 사용할 수 있습니다.

애그리게이트 포트 결합 모드를 사용하려는 경우:

- LACP 네트워크 결합 모드를 사용해야 합니다.
- 각 네트워크에 대해 고유한 VLAN 태그를 지정해야 합니다. 이 VLAN 태그는 네트워크 트래픽이 올바른 네트워크로 라우팅되도록 각 네트워크 패킷에 추가됩니다.
- VLAN 및 LACP를 지원할 수 있는 스위치에 포트를 연결해야 합니다. LACP 결합에 여러 스위치가 사용되는 경우 스위치는 MLAG(Multi-Chassis Link Aggregation Group) 또는 이와 동등한 스위치를 지원해야 합니다.
- VLAN, LACP, MLAG 또는 이와 동등한 기능을 사용하도록 스위치를 구성하는 방법을 이해해야 합니다.

포트 4개를 모두 사용하지 않으려면 포트 1개, 2개 또는 3개를 사용할 수 있습니다. 두 개 이상의 포트를 사용하면 포트 중 하나에 장애가 발생하더라도 일부 네트워크 연결이 계속 유지될 가능성을 극대화할 수 있습니다.

> 포트 수를 4개 이하로 선택하면 어플라이언스 노드가 설치된 후 그리드 관리자에서 * 서비스 어플라이언스 연결 해제 * 경고가 트리거되어 케이블이 분리되었음을 나타냅니다. 트리거된 경고에 대해 이 경고 규칙을 안전하게 비활성화할 수 있습니다. Grid Manager에서 * alerts * > * rules * 를 선택하고 규칙을 선택한 다음 * Edit rule * 을 클릭합니다. 그런 다음 * 사용 * 확인란의 선택을 취소합니다.

관리 포트의 네트워크 연결 모드입니다

서비스 어플라이언스에 있는 2개의 1GbE 관리 포트의 경우 독립 네트워크 연결 모드 또는 Active-Backup 네트워크 연결 모드를 선택하여 옵션 관리 네트워크에 연결할 수 있습니다.

SG100 네트워크 관리 포트 *

SG1000 네트워크 관리 포트 *

독립 모드에서는 왼쪽에 있는 관리 포트만 관리 네트워크에 연결됩니다. 이 모드는 중복 경로를 제공하지 않습니다. 오른쪽의 관리 포트가 연결되어 있지 않으며 임시 로컬 연결에 사용할 수 있습니다(IP 주소 169.254.0.1 사용).

Active-Backup 모드에서는 두 관리 포트가 모두 관리 네트워크에 연결됩니다. 한 번에 하나의 포트만 활성화됩니다. 활성 포트에 장애가 발생하면 백업 포트가 자동으로 페일오버 연결을 제공합니다. 이러한 두 개의 물리적 포트를 하나의 논리 관리 포트에 연결하면 관리 네트워크에 대한 중복 경로가 제공됩니다.

> 1GbE 관리 포트가 Active-Backup 모드로 구성되어 있을 때 서비스 어플라이언스에 임시로 로컬 연결해야 하는 경우, 두 관리 포트에서 케이블을 분리하고 오른쪽의 관리 포트에 임시 케이블을 연결한 다음 IP 주소 169.254.0.1을 사용하여 어플라이언스에 액세스합니다.

속성 표시기	네트워크 연결 모드
A	Active-Backup 모드. 두 관리 포트는 모두 관리 네트워크에 연결된 하나의 논리 관리 포트에 연결됩니다.
나는	독립 모드. 왼쪽의 포트는 관리 네트워크에 연결되어 있습니다. 오른쪽의 포트는 임시 로컬 연결(IP 주소 169.254.0.1)에 사용할 수 있습니다.

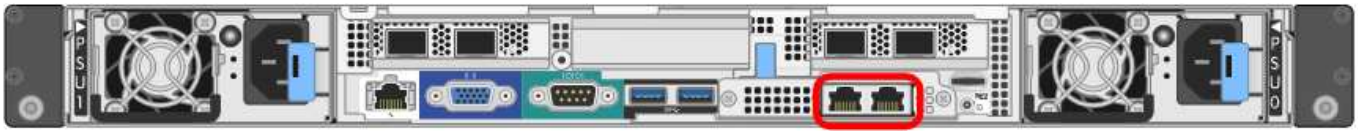
설치 정보 수집**(SG100** 및 **SG1000)**

StorageGRID 어플라이언스를 설치 및 구성할 때 이더넷 스위치 포트, IP 주소, 포트 및 네트워크 연결 모드에 대한 정보를 결정하고 수집해야 합니다. 어플라이언스에 연결하는 각 네트워크에 필요한 정보를 기록합니다. 이러한 값은 하드웨어를 설치하고 구성하는 데 필요합니다.

관리 및 유지보수 포트

StorageGRID용 관리 네트워크는 시스템 관리 및 유지 보수에 사용되는 선택적 네트워크입니다. 어플라이언스는 어플라이언스에서 다음 1GbE 관리 포트를 사용하여 관리 네트워크에 연결됩니다.

SG100 RJ-45 포트 *



SG1000 RJ-45 포트 *

- 관리 및 유지보수 연결 *

정보가 필요합니다	귀사의 가치
관리자 네트워크가 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요 • 예(기본값)
네트워크 연결 모드	다음 중 하나를 선택하십시오. • 독립(기본값) • Active - 백업
다이어그램에서 원으로 표시된 왼쪽 포트의 스위치 포트(독립 네트워크 연결 모드의 기본 활성 포트)	
다이어그램에서 원으로 표시된 오른쪽 포트의 스위치 포트(Active-Backup 네트워크 연결 모드만 해당)	

정보가 필요합니다	귀사의 가치
관리자 네트워크 포트의 MAC 주소입니다 • 참고: * 어플라이언스 전면의 MAC 주소 레이블에는 BMC 관리 포트의 MAC 주소가 나열됩니다. 관리 네트워크 포트의 MAC 주소를 확인하려면 레이블의 16진수에 * 2 * 를 추가해야 합니다. 예를 들어 레이블의 MAC 주소가 * 09 * 로 끝나는 경우 관리 포트의 MAC 주소는 * 0B * 로 끝납니다. 레이블의 MAC 주소가 * (*y*) FF * 로 끝나는 경우 관리 포트의 MAC 주소는 * (*y*+1) 01 * 로 끝납니다. Windows에서 계산기를 열고, Programmer 모드로 설정하고, Hex를 선택하고, MAC 주소를 입력한 다음, * + 2 = * 를 입력하여 이 계산을 쉽게 수행할 수 있습니다.	
전원을 켠 후 사용할 수 있는 경우, Admin Network 포트에 대해 DHCP가 할당한 IP 주소입니다 • 참고: * MAC 주소를 사용하여 할당된 IP를 조회하여 DHCP 할당 IP 주소를 확인할 수 있습니다.	• IPv4 주소(CIDR): • 게이트웨이:
관리 네트워크의 어플라이언스 노드에 사용할 고정 IP 주소입니다 • 참고: * 네트워크에 게이트웨이가 없는 경우 게이트웨이에 대해 동일한 정적 IPv4 주소를 지정합니다.	• IPv4 주소(CIDR): • 게이트웨이:
관리 네트워크 서브넷(CIDR)	

네트워킹 포트

어플라이언스에 있는 4개의 네트워킹 포트는 StorageGRID 그리드 네트워크 및 선택적 클라이언트 네트워크에 연결됩니다.

- 네트워킹 연결 *

정보가 필요합니다	귀사의 가치
링크 속도	SG100의 경우 다음 중 하나를 선택합니다. • 자동(기본값) • 10GbE • 25GbE SG1000의 경우 다음 중 하나를 선택합니다. • 자동(기본값) • 10GbE • 25GbE • 40GbE • 100GbE • 참고: * SG1000, 10 및 25-GbE 속도의 경우 QSA 어댑터를 사용해야 합니다.
포트 결합 모드	다음 중 하나를 선택하십시오. • 고정(기본값) • 집계
포트 1용 스위치 포트(고정 모드용 클라이언트 네트워크)	
포트 2용 스위치 포트(고정 모드용 그리드 네트워크)	
포트 3용 스위치 포트(고정 모드용 클라이언트 네트워크)	
포트 4용 스위치 포트(고정 모드용 그리드 네트워크)	

그리드 네트워크 포트

StorageGRID용 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용되는 필수 네트워크입니다. 이 어플라이언스는 네트워크 포트 4개를 사용하여 그리드 네트워크에 연결됩니다.

- 그리드 네트워크 연결 *

정보가 필요합니다	귀사의 가치
네트워크 연결 모드	다음 중 하나를 선택하십시오. • Active-Backup(기본값) • LACP(802.3ad)

정보가 필요합니다	귀사의 가치
VLAN 태그 지정이 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요(기본값) • 예
VLAN 태그(VLAN 태그 지정이 활성화된 경우)	0에서 4095 사이의 값을 입력합니다.
전원을 켠 후 사용할 수 있는 경우 그리드 네트워크에 대해 DHCP 할당 IP 주소입니다	• IPv4 주소(CIDR): • 게이트웨이:
그리드 네트워크에서 어플라이언스 노드에 사용할 고정 IP 주소입니다 • 참고: * 네트워크에 게이트웨이가 없는 경우 게이트웨이에 대해 동일한 정적 IPv4 주소를 지정합니다.	• IPv4 주소(CIDR): • 게이트웨이:
그리드 네트워크 서브넷(CIDR)	
MTU(Maximum Transmission Unit) 설정(선택 사항) 1500의 기본값을 사용하거나 MTU를 9000과 같은 점보 프레임에 적합한 값으로 설정할 수 있습니다.	

클라이언트 네트워크 포트

StorageGRID용 클라이언트 네트워크는 일반적으로 그리드에 대한 클라이언트 프로토콜 액세스를 제공하는 데 사용되는 선택적 네트워크입니다. 어플라이언스는 네트워크 포트 4개를 사용하여 클라이언트 네트워크에 연결됩니다.

- 클라이언트 네트워크 연결 *

정보가 필요합니다	귀사의 가치
클라이언트 네트워크가 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요(기본값) • 예
네트워크 연결 모드	다음 중 하나를 선택하십시오. • Active-Backup(기본값) • LACP(802.3ad)

정보가 필요합니다	귀사의 가치
VLAN 태그 지정이 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요(기본값) • 예
VLAN 태그(VLAN 태그 지정이 활성화된 경우)	0에서 4095 사이의 값을 입력합니다.
전원을 켠 후 사용할 수 있는 경우 클라이언트 네트워크에 대해 DHCP 할당 IP 주소입니다	• IPv4 주소(CIDR): • 게이트웨이:
클라이언트 네트워크의 어플라이언스 노드에 사용할 고정 IP 주소입니다 • 참고: * 클라이언트 네트워크가 활성화된 경우 어플라이언스의 기본 경로는 여기에 지정된 게이트웨이를 사용합니다.	• IPv4 주소(CIDR): • 게이트웨이:

BMC 관리 네트워크 포트

다이어그램에 표시된 1GbE 관리 포트를 사용하여 서비스 어플라이언스의 BMC 인터페이스에 액세스할 수 있습니다. 이 포트는 IPMI(Intelligent Platform Management Interface) 표준을 사용하여 이더넷을 통한 컨트롤러 하드웨어의 원격 관리를 지원합니다.

- SG100 BMC 관리 포트 *

- SG1000 BMC 관리 포트 *

- BMC 관리 네트워크 연결 *

정보가 필요합니다	귀사의 가치
BMC 관리 포트에 연결할 이더넷 스위치 포트 (다이어그램에서 원으로 표시됨)	
전원을 켠 후 사용할 수 있는 경우 BMC 관리 네트워크에 대해 DHCP 할당 IP 주소입니다	• IPv4 주소(CIDR): • 게이트웨이:

정보가 필요합니다	귀사의 가치
BMC 관리 포트에 사용할 고정 IP 주소입니다	• IPv4 주소(CIDR): • 게이트웨이:

관련 정보

SG100 및 SG1000 어플라이언스 개요

케이블 어플라이언스 SG100 및 SG1000

StorageGRID IP 주소를 구성합니다

하드웨어 설치(SG100 및 SG1000)

하드웨어 등록

어플라이언스 하드웨어를 등록하면 지원 혜택이 제공됩니다.

단계

1. 어플라이언스의 섀시 일련 번호를 찾습니다.

   포장 명세서, 확인 이메일 또는 제품의 포장을 푼 후 제품에서 번호를 확인할 수 있습니다.

2. NetApp Support 사이트 로 이동합니다 "mysupport.netapp.com".
3. 하드웨어를 등록해야 하는지 여부를 확인합니다.

귀하의 경우...	다음 단계를 따르십시오...
더 많은 워크로드 추가)	a. 사용자 이름과 암호를 사용하여 로그인합니다. b. 제품 * > * 내 제품 * 을 선택합니다. c. 새 일련 번호가 나열되는지 확인합니다. d. 그렇지 않은 경우 새 NetApp 고객에 대한 지침을 따르십시오.
신규 NetApp 고객	a. 지금 등록 * 을 클릭하고 계정을 만듭니다. b. 제품 * > * 제품 등록 * 을 선택합니다. c. 제품 일련 번호 및 요청된 세부 정보를 입력합니다. 등록이 승인되면 필요한 소프트웨어를 다운로드할 수 있습니다. 승인 프로세스는 최대 24시간이 걸릴 수 있습니다.

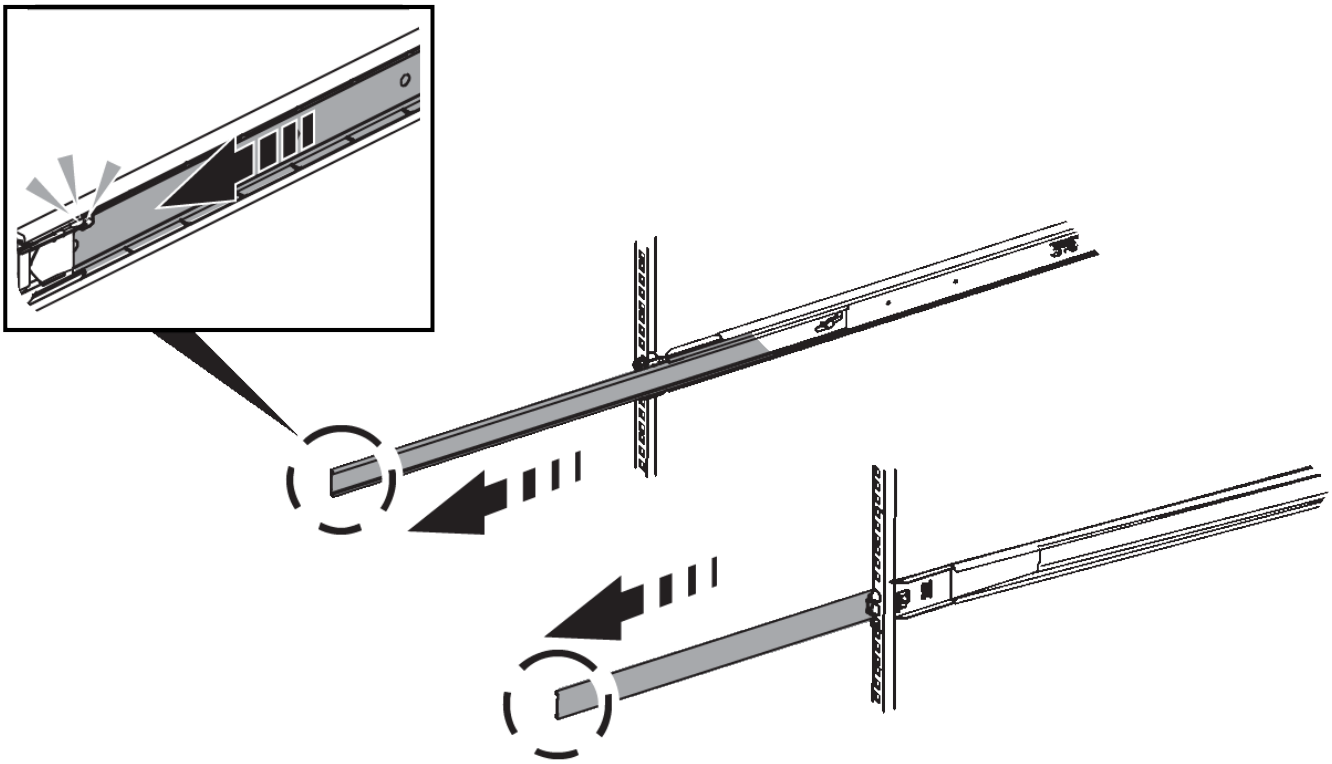
캐비닛이나 랙에 제품 레일 세트를 설치한 다음 제품을 레일에 밀어 넣으십시오.

필요한 것

- 상자에 포함된 안전 고지 문서를 검토하고 하드웨어 이동 및 설치에 대한 예방 조치를 이해했습니다.
- 레일 키트와 함께 제공된 지침이 있습니다.

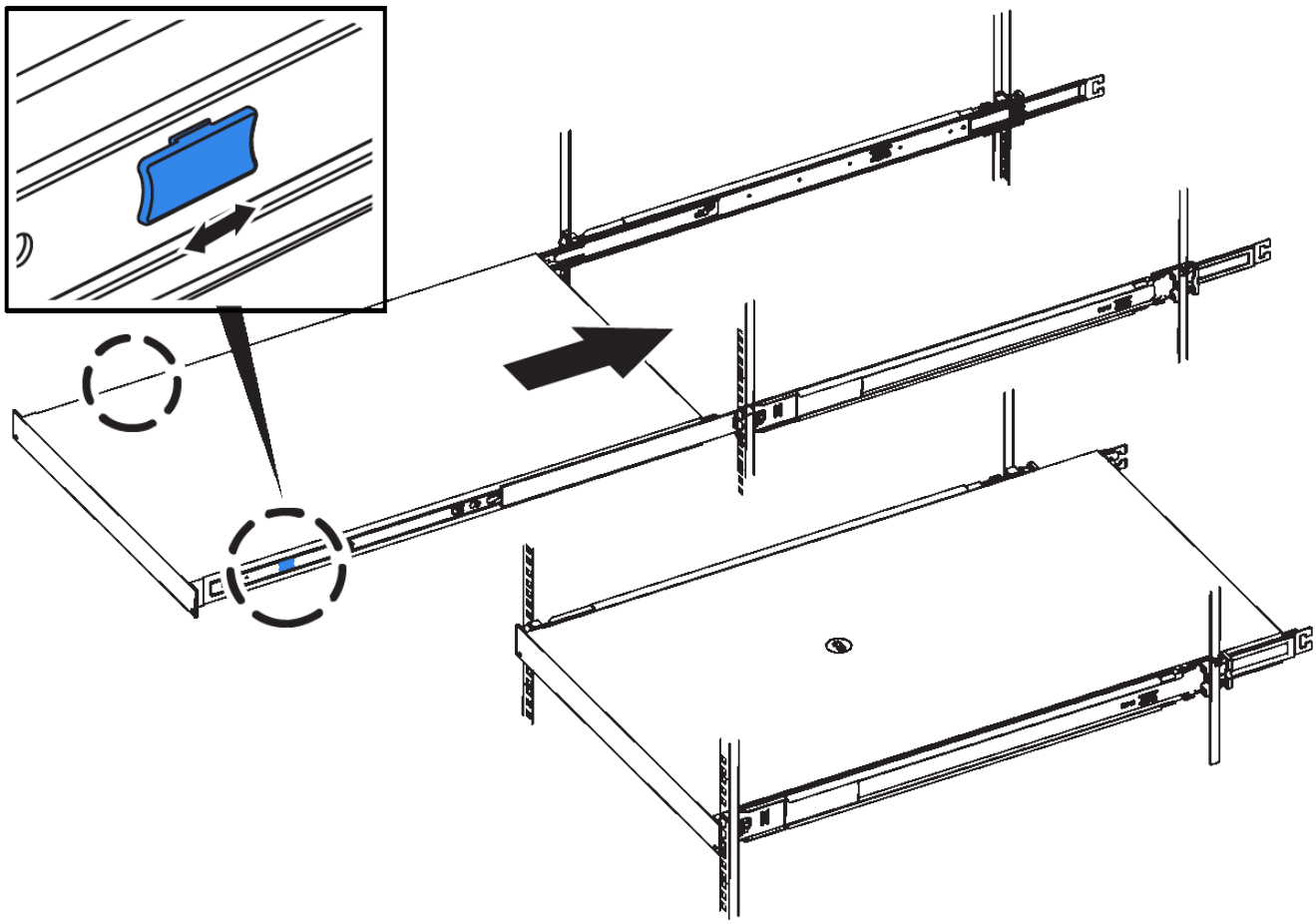
단계

1. 레일 키트의 지침에 따라 캐비닛이나 랙에 레일을 설치합니다.
2. 캐비닛이나 랙에 설치된 두 개의 레일에서 딸깍 소리가 날 때까지 레일의 이동식 부품을 확장합니다.



3. 제품을 레일에 삽입합니다.
4. 제품을 캐비닛 또는 랙에 밀어 넣습니다.

   제품을 더 이상 움직일 수 없는 경우 섀시 양쪽에 있는 파란색 래치를 당겨 제품을 완전히 밀어 넣으십시오.



제품의 전원을 켠 후에 전면 베젤을 연결하지 마십시오.

케이블 어플라이언스 **SG100** 및 **SG1000**

어플라이언스의 관리 포트를 서비스 랩톱에 연결하고 어플라이언스의 네트워크 포트를 그리드 네트워크 및 StorageGRID용 클라이언트 네트워크(옵션)에 연결해야 합니다.

필요한 것

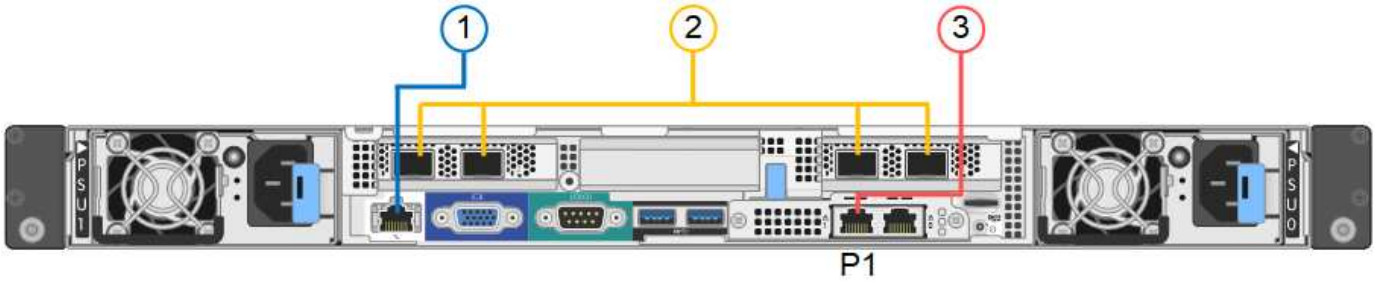
- 관리 포트를 연결하기 위한 RJ-45 이더넷 케이블이 있습니다.
- 네트워크 포트에 대한 다음 옵션 중 하나가 있습니다. 이러한 품목은 제품과 함께 제공되지 않습니다.
  - 4개의 네트워크 포트를 연결하기 위한 TwinAx 케이블 1-4개.
  - SG100의 경우 포트에 광 케이블을 사용하려는 경우 SFP+ 또는 SFP28 트랜시버를 1~4개 사용하십시오.
  - SG1000의 경우 포트에 광 케이블을 사용하려는 경우 QSFP+ 또는 QSFP28 트랜시버를 1~4개 사용하십시오.

* 레이저 방사선에 노출될 위험 * - SFP 또는 QSFP 트랜시버를 분해하거나 제거하지 마십시오. 레이저 방사선에 노출될 수 있습니다.

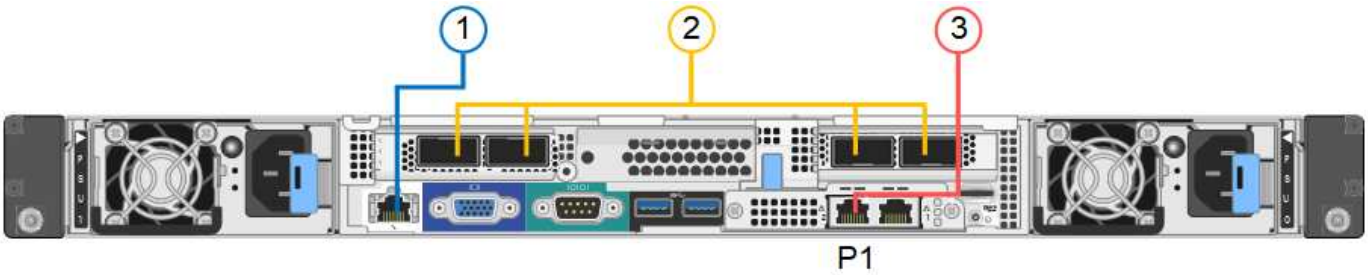
이 작업에 대해

다음 그림은 어플라이언스 후면에 있는 포트를 보여줍니다.

SG100 포트 연결 *



SG1000 포트 연결 *



	포트	포트의 유형입니다	기능
1	어플라이언스의 BMC 관리 포트	1GbE(RJ-45)	BMC 인터페이스에 액세스하는 네트워크에 연결합니다.
2	어플라이언스에 네트워크 포트 4개가 있습니다	• SG100:10/25-GbE의 경우 • SG1000: 10/25/40/100GbE의 경우	그리드 네트워크 및 StorageGRID용 클라이언트 네트워크에 연결합니다.
3	어플라이언스의 관리 네트워크 포트(그림에서 P1 레이블)	1GbE(RJ-45) • 중요: * 이 포트는 1000 BaseT/full에서만 작동하며 10메가비트 또는 100메가비트 속도를 지원하지 않습니다.	StorageGRID용 관리 네트워크에 어플라이언스를 연결합니다.

	포트	포트의 유형입니다	기능
	어플라이언스에서 가장 오른쪽에 있는 RJ-45 포트	1GbE(RJ-45) • 중요: * 이 포트는 1000 BaseT/full에서만 작동하며 10메가비트 또는 100메가비트 속도를 지원하지 않습니다.	• 관리 네트워크에 대한 중복 연결을 원할 경우 관리 포트 1에 연결할 수 있습니다. • 연결을 끊은 상태로 두고 임시 로컬 액세스(IP 169.254.0.1)에 사용할 수 있습니다. • 설치하는 동안 DHCP 할당 IP 주소를 사용할 수 없는 경우 어플라이언스를 서비스 랩톱에 연결하는 데 사용할 수 있습니다.

단계

1. 이더넷 케이블을 사용하여 어플라이언스의 BMC 관리 포트를 관리 네트워크에 연결합니다.

   이 연결은 선택 사항이지만 지원을 원활하게 하는 것이 좋습니다.

2. TwinAx 케이블이나 광 케이블과 트랜시버를 사용하여 어플라이언스의 네트워크 포트를 해당 네트워크 스위치에 연결합니다.

   네트워크 포트 4개는 동일한 링크 속도를 사용해야 합니다. 하드웨어 및 링크 속도에 따라 필요한 장비는 다음 표를 참조하십시오.

SG100 링크 속도**(GbE)**	필수 장비
10	SFP+ 트랜시버
25	SFP28 트랜시버
SG1000 링크 속도(GbE)	필수 장비
10	QSA 및 SFP+ 트랜시버
25	QSA 및 SFP28 트랜시버
40	QSFP+ 트랜시버
100	QFSP28 트랜시버

   - 고정 포트 결합 모드(기본값)를 사용하려는 경우 표 에 나와 있는 대로 포트를 StorageGRID 그리드 및 클라이언트 네트워크에 연결합니다.

포트	연결 대상...
포트 1	클라이언트 네트워크(옵션)

포트	연결 대상...
포트 2	그리드 네트워크
포트 3	클라이언트 네트워크(옵션)
포트 4	그리드 네트워크

- Aggregate 포트 결합 모드를 사용하려는 경우 하나 이상의 네트워크 포트를 하나 이상의 스위치에 연결합니다. 단일 장애 지점이 발생하지 않도록 4개 포트 중 2개 이상을 연결해야 합니다. 단일 LACP 결합에 둘 이상의 스위치를 사용하는 경우 스위치는 MLAG 또는 동급 스위치를 지원해야 합니다.

3. StorageGRID용 관리 네트워크를 사용하려는 경우 이더넷 케이블을 사용하여 어플라이언스의 관리 네트워크 포트를 관리 네트워크에 연결합니다.

전원 코드를 연결하고 전원을 공급합니다**(SG100** 및 **SG1000).**

네트워크 케이블을 연결한 후 어플라이언스에 전원을 공급할 준비가 되었습니다.

단계

1. 전원 코드를 제품에 있는 두 개의 전원 공급 장치에 각각 연결합니다.
2. 이 두 개의 전원 코드를 캐비닛이나 랙에 있는 두 개의 서로 다른 PDU(Power Distribution Unit)에 연결합니다.
3. 제품 앞면에 있는 전원 단추가 현재 파란색으로 켜져 있지 않으면 버튼을 눌러 제품의 전원을 켭니다.

   전원을 켜는 동안 전원 단추를 다시 누르지 마십시오.

4. 오류가 발생하면 문제를 해결하십시오.
5. 분리한 경우 전면 베젤을 제품에 장착합니다.

관련 정보

SG100 및 SG1000 어플라이언스의 상태 표시기를 봅니다

SG100 및 **SG1000** 어플라이언스의 상태 표시기를 봅니다

이 제품에는 어플라이언스 컨트롤러 및 2개의 SSD의 상태를 확인하는 데 도움이 되는 표시등이 포함되어 있습니다.

제품 표시등 및 버튼

	디스플레이	상태
1	전원 단추	• 파란색: 제품의 전원이 켜져 있습니다. • 꺼짐: 제품의 전원이 꺼져 있습니다.
2	재설정 버튼	이 단추를 사용하여 컨트롤러를 하드 리셋합니다.
3	식별 버튼	이 단추는 깜박임, 켜짐(켜짐) 또는 꺼짐 으로 설정할 수 있습니다. • 파란색, 깜박임: 캐비닛이나 랙에 있는 제품을 나타냅니다. • 파란색, 켜짐: 캐비닛이나 랙에 있는 제품을 나타냅니다. • 꺼짐: 캐비닛이나 랙에서 제품을 육안으로 확인할 수 없습니다.
4	알람 LED	• 황색, 켜짐: 오류가 발생했습니다. • 참고: * 부팅 및 오류 코드를 보려면 BMC 인터페이스에 액세스해야 합니다. • 꺼짐: 오류가 없습니다.

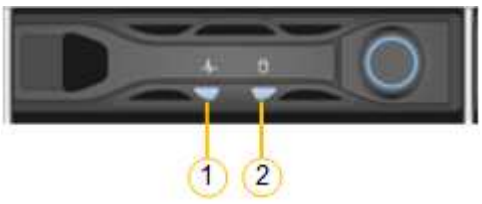
일반 부팅 코드

부팅하거나 제품을 하드 리셋한 후 다음과 같은 현상이 발생합니다.

1. BMC(베이스보드 관리 컨트롤러)는 발생한 오류를 포함하여 부팅 순서의 코드를 기록합니다.
2. 전원 단추가 켜집니다.
3. 부팅 중에 오류가 발생하면 알람 LED가 켜집니다.

   부팅 및 오류 코드를 보려면 BMC 인터페이스에 액세스해야 합니다.

SSD 표시등



LED	디스플레이	상태
1	드라이브 상태/장애	• 파란색(계속 켜짐): 드라이브가 온라인 상태입니다 • 주황색(깜박임): 드라이브 오류가 발생했습니다 • 꺼짐: 슬롯이 비어 있습니다
2	드라이브가 활성 상태입니다	파란색(깜박임): 드라이브에 액세스하는 중입니다

관련 정보

하드웨어 설치 문제 해결(SG100 및 SG1000)

BMC 인터페이스 구성(SG100 및 SG1000)

StorageGRID 접속 구성(SG100 및 SG1000)

StorageGRID 시스템에서 서비스 어플라이언스를 노드로 배포하려면 먼저 어플라이언스와 사용할 네트워크 간의 연결을 구성해야 합니다. 서비스 어플라이언스에 사전 설치된 StorageGRID 어플라이언스 설치 프로그램으로 이동하여 네트워킹을 구성할 수 있습니다.

StorageGRID 어플라이언스 설치 프로그램에 액세스합니다

어플라이언스와 세 StorageGRID 네트워크(그리드 네트워크, 관리자 네트워크(옵션) 및 클라이언트 네트워크(선택 사항) 간의 연결을 구성하려면 StorageGRID 어플라이언스 설치 프로그램에 액세스해야 합니다.

필요한 것

- StorageGRID 관리자 네트워크에 연결할 수 있는 관리 클라이언트를 사용하고 있습니다.
- 클라이언트에 가 있습니다 지원되는 웹 브라우저.
- 서비스 어플라이언스는 사용하려는 모든 StorageGRID 네트워크에 연결되어 있습니다.
- 이러한 네트워크에서 서비스 어플라이언스의 IP 주소, 게이트웨이 및 서브넷을 알고 있습니다.
- 사용할 네트워크 스위치를 구성했습니다.

이 작업에 대해

처음에 StorageGRID 어플라이언스 설치 프로그램에 액세스하려면 서비스 어플라이언스의 관리 네트워크 포트에 대해 DHCP 할당 IP 주소를 사용하거나(관리 네트워크에 연결되어 있다고 가정) 서비스 랩톱을 서비스 어플라이언스에 직접 연결할 수 있습니다.

단계

1. 가능하면 서비스 어플라이언스의 관리 네트워크 포트에 대한 DHCP 주소를 사용하여 StorageGRID 어플라이언스 설치 프로그램에 액세스합니다.

    - SG100 관리 네트워크 포트 *

SG1000 관리자 네트워크 포트 *

a. 서비스 어플라이언스의 전면에서 MAC 주소 레이블을 찾아 관리 네트워크 포트의 MAC 주소를 확인합니다.

   MAC 주소 레이블에는 BMC 관리 포트의 MAC 주소가 나열됩니다.

관리 네트워크 포트의 MAC 주소를 확인하려면 레이블의 16진수에 * 2 * 를 추가해야 합니다. 예를 들어 레이블의 MAC 주소가 * 09 * 로 끝나는 경우 관리 포트의 MAC 주소는 * 0B * 로 끝납니다. 레이블의 MAC 주소가 * (*y*) FF * 로 끝나는 경우 관리 포트의 MAC 주소는 * (*y*+1) 01 * 로 끝납니다. Windows에서 계산기를 열고, Programmer 모드로 설정하고, Hex를 선택하고, MAC 주소를 입력한 다음, * + 2 = * 를 입력하여 이 계산을 쉽게 수행할 수 있습니다.

a. 네트워크 관리자에게 MAC 주소를 제공하여 관리자가 관리 네트워크에서 어플라이언스의 DHCP 주소를 찾을 수 있도록 합니다.

b. 클라이언트에서 StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. + `https://services-appliance_IP:8443*`

   '*services-appliance_ip*'의 경우 DHCP address를 사용한다.

c. 보안 경고 메시지가 나타나면 브라우저의 설치 마법사를 사용하여 인증서를 보고 설치합니다.

   다음에 이 URL에 액세스할 때 알림이 나타나지 않습니다.

StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다. 이 페이지에 처음 액세스할 때 표시되는 정보와 메시지는 어플라이언스가 현재 StorageGRID 네트워크에 연결되어 있는 방식에 따라 다릅니다. 오류 메시지가 나타날 수 있으며, 이 메시지는 이후 단계에서 해결될 것입니다.

2. 또는 DHCP를 사용하여 IP 주소를 얻을 수 없는 경우 링크 로컬 연결을 사용하여 StorageGRID 어플라이언스 설치 프로그램에 액세스합니다.

   a. 서비스 랩톱을 이더넷 케이블을 사용하여 서비스 어플라이언스의 맨 오른쪽 RJ-45 포트에 직접 연결합니다.

      - SG100 링크 로컬 연결 *

      SG1000 링크 로컬 연결 *

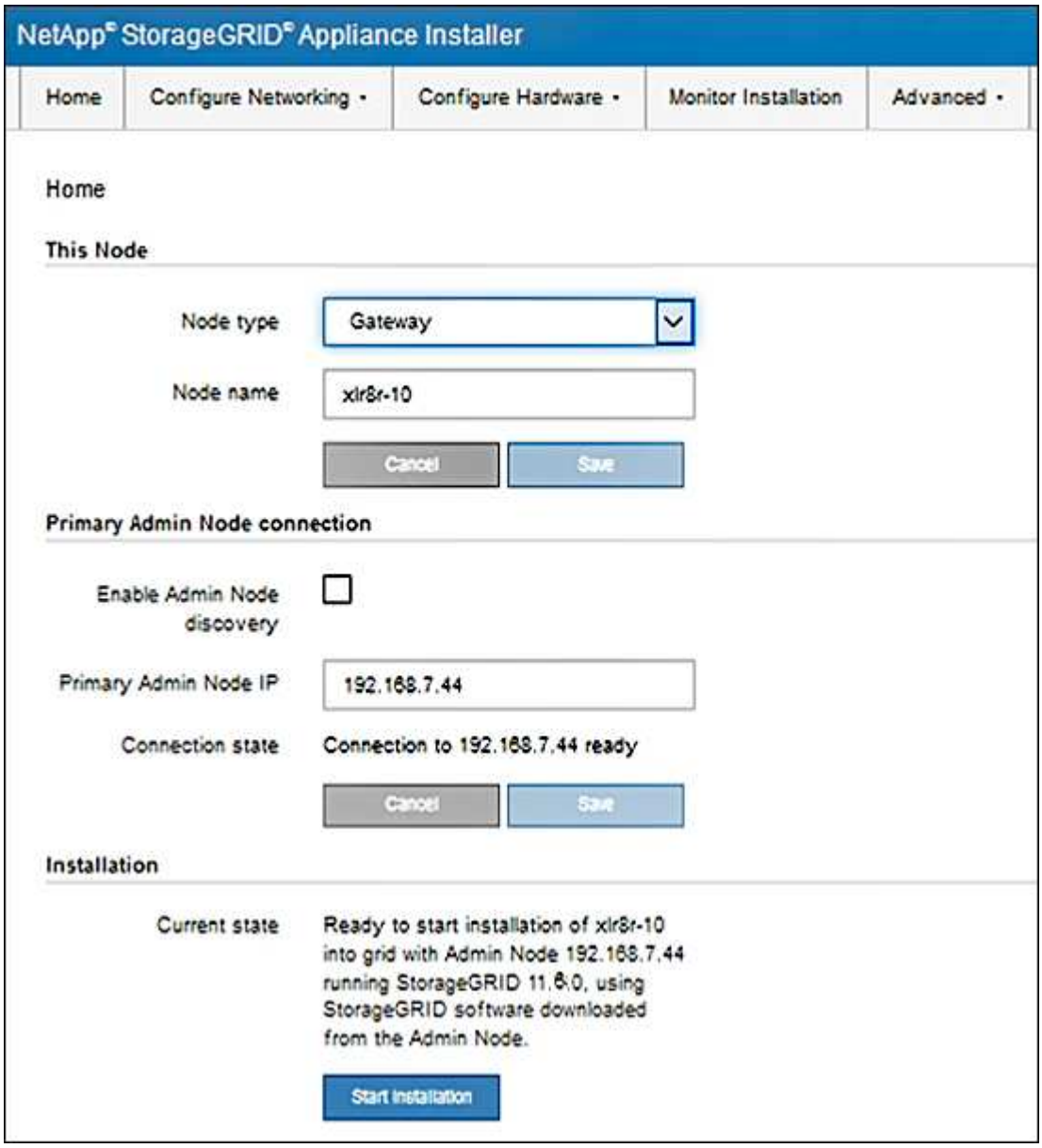
b. 웹 브라우저를 엽니다.

c. StorageGRID 어플라이언스 설치 프로그램에 대한 이 URL을 입력합니다: + `*https://169.254.0.1:8443*`

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다. 이 페이지에 처음 액세스할 때 표시되는 정보와 메시지는 어플라이언스가 현재 StorageGRID 네트워크에 연결되어 있는 방식에 따라 다릅니다. 오류 메시지가 나타날 수 있으며, 이 메시지는 이후 단계에서 해결될 것입니다.

   ⓘ 링크 로컬 연결을 통해 홈 페이지에 액세스할 수 없는 경우 서비스 랩톱 IP 주소를 "169.254.0.2"로 구성한 후 다시 시도하십시오.

3. 홈 페이지에 표시되는 메시지를 검토하고 필요에 따라 링크 구성 및 IP 구성을 구성합니다.



StorageGRID 어플라이언스 설치 프로그램 버전을 확인하고 업그레이드합니다

어플라이언스의 StorageGRID 어플라이언스 설치 프로그램 버전은 StorageGRID 시스템에

설치된 소프트웨어 버전과 일치해야 모든 StorageGRID 기능이 지원됩니다.

필요한 것

StorageGRID 어플라이언스 설치 프로그램에 액세스했습니다.

이 작업에 대해

StorageGRID 어플라이언스는 StorageGRID 어플라이언스 설치 프로그램이 사전 설치된 상태로 제공됩니다. 최근에 업그레이드된 StorageGRID 시스템에 어플라이언스를 추가하는 경우 어플라이언스를 새 노드로 설치하기 전에 StorageGRID 어플라이언스 설치 프로그램을 수동으로 업그레이드해야 할 수 있습니다.

새 StorageGRID 버전으로 업그레이드하면 StorageGRID 어플라이언스 설치 프로그램이 자동으로 업그레이드됩니다. 설치된 어플라이언스 노드에서 StorageGRID 어플라이언스 설치 프로그램을 업그레이드할 필요가 없습니다. 이 절차는 이전 버전의 StorageGRID 어플라이언스 설치 프로그램이 포함된 어플라이언스를 설치하는 경우에만 필요합니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 펌웨어 업그레이드 * 를 선택합니다.
2. 현재 펌웨어 버전을 StorageGRID 시스템에 설치된 소프트웨어 버전과 비교합니다. (그리드 관리자 상단에서 도움말 아이콘을 선택하고 * 정보 * 를 선택합니다.)

   두 버전의 두 번째 숫자가 일치해야 합니다. 예를 들어, StorageGRID 시스템에서 버전 11. * 6 *.*x*._y_를 실행하는 경우 StorageGRID 어플라이언스 설치 프로그램 버전은 3. * 6 *._z_이어야 합니다.

3. 어플라이언스에 StorageGRID 어플라이언스 설치 프로그램의 하위 수준 버전이 있는 경우 로 이동합니다 "NetApp 다운로드: StorageGRID 어플라이언스".

   NetApp 계정의 사용자 이름과 암호를 사용하여 로그인합니다.

4. StorageGRID Appliances*용 * 지원 파일의 적절한 버전과 해당 체크섬 파일을 다운로드하십시오.

   StorageGRID 어플라이언스 파일의 지원 파일은 모든 StorageGRID 어플라이언스 모델의 현재 및 이전 펌웨어 버전을 포함하는 '.zip' 아카이브로, 각 컨트롤러 유형의 하위 디렉토리에 있습니다.

   StorageGRID 어플라이언스 파일용 지원 파일을 다운로드한 후 '.zip' 아카이브의 압축을 풀고 StorageGRID 어플라이언스 설치 프로그램 설치에 대한 중요 정보는 README 파일을 참조하십시오.

5. StorageGRID 어플라이언스 설치 프로그램의 펌웨어 업그레이드 페이지에 있는 지침에 따라 다음 단계를 수행합니다.
   a. 컨트롤러 유형 및 체크섬 파일에 적합한 지원 파일(펌웨어 이미지)을 업로드합니다.
   b. 비활성 파티션을 업그레이드합니다.
   c. 재부팅하고 파티션을 바꿉니다.
   d. 두 번째(비활성) 파티션을 업그레이드합니다.

관련 정보

StorageGRID 어플라이언스 설치 프로그램에 액세스합니다

네트워크 링크 구성**(SG100** 및 **SG1000)**

어플라이언스를 그리드 네트워크, 클라이언트 네트워크 및 관리 네트워크에 연결하는 데

사용되는 포트에 대한 네트워크 링크를 구성할 수 있습니다. 링크 속도와 포트 및 네트워크 연결 모드를 설정할 수 있습니다.

필요한 것

- 케이블 유형 및 링크 속도에 필요한 추가 장비를 확보했습니다.
- 선택한 속도를 지원하는 스위치에 네트워크 포트를 연결했습니다.

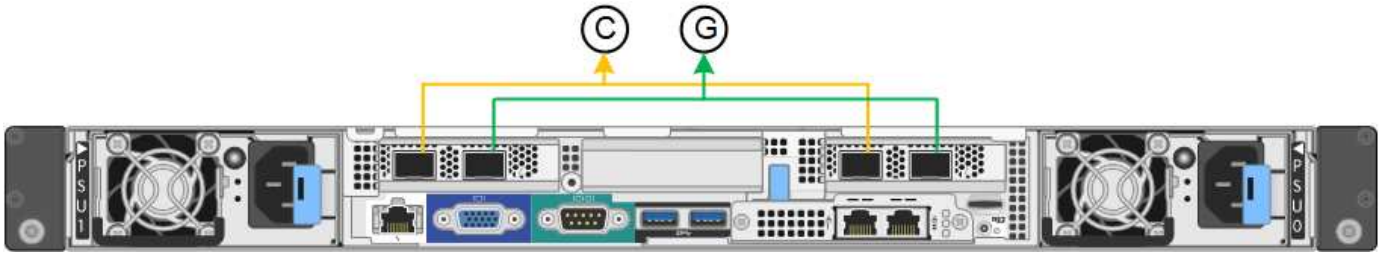
Aggregate 포트 결합 모드, LACP 네트워크 결합 모드 또는 VLAN 태그 지정을 사용하려면 다음을 수행합니다.

- 어플라이언스의 네트워크 포트를 VLAN 및 LACP를 지원할 수 있는 스위치에 연결했습니다.
- LACP 결합에 여러 스위치가 사용되는 경우 스위치는 MLAG(Multi-Chassis Link Aggregation Group) 또는 이와 동등한 스위치를 지원합니다.
- VLAN, LACP, MLAG 또는 이와 동등한 기능을 사용하도록 스위치를 구성하는 방법을 이해합니다.
- 각 네트워크에 사용할 고유 VLAN 태그를 알고 있습니다. 이 VLAN 태그는 네트워크 트래픽이 올바른 네트워크로 라우팅되도록 각 네트워크 패킷에 추가됩니다.

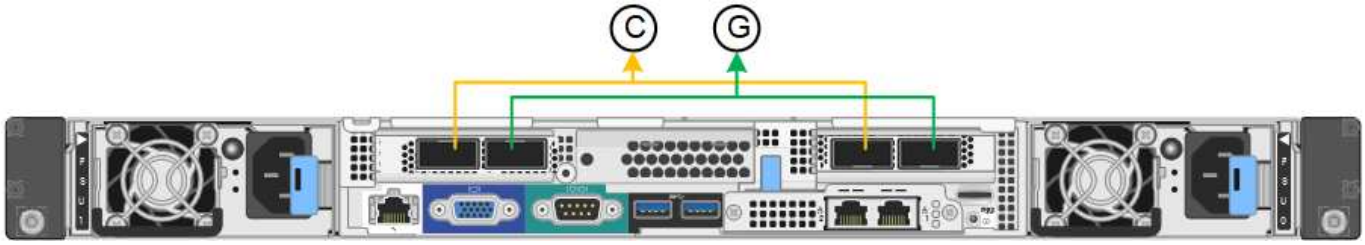
이 작업에 대해

이 그림은 4개의 네트워크 포트가 고정 포트 결합 모드(기본 구성)에서 어떻게 결합되는지 보여줍니다.

- SG100 고정 포트 결합 모드 *



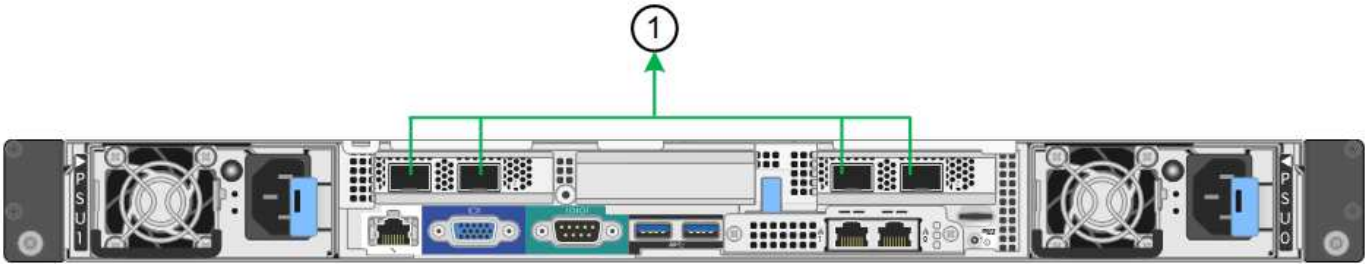
- SG1000 고정 포트 결합 모드 *



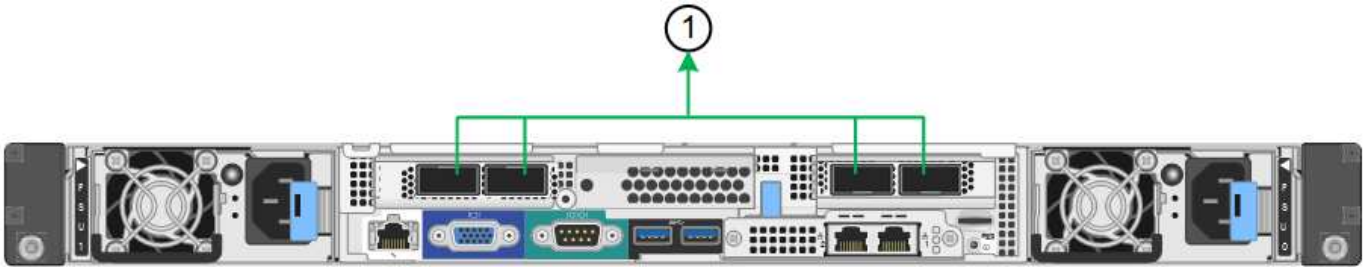
속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
c	이 네트워크를 사용하는 경우 포트 1과 3이 클라이언트 네트워크에 대해 함께 연결됩니다.
g	포트 2와 4는 그리드 네트워크를 위해 서로 연결되어 있습니다.

이 그림은 4개의 네트워크 포트가 애그리게이트 포트 결합 모드에서 결합되는 방식을 보여줍니다.

- SG100 애그리게이트 포트 결합 모드 *



- SG1000 집계 포트 결합 모드 *



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
1	4개 포트 모두 단일 LACP 결합으로 그룹화되므로 모든 포트를 그리드 네트워크 및 클라이언트 네트워크 트래픽에 사용할 수 있습니다.

이 표에는 4개의 네트워크 포트를 구성하는 옵션이 요약되어 있습니다. 기본 설정은 굵게 표시됩니다. 기본이 아닌 설정을 사용하려면 구성 연결 페이지에서 설정을 구성하기만 하면 됩니다.

> LACP 전송 해시 정책은 기본적으로 layer2 + 3 모드로 설정됩니다. 필요한 경우 Grid Management API를 사용하여 layer3+4 모드로 변경할 수 있습니다.

- * 고정(기본값) 포트 결합 모드 *

네트워크 연결 모드	클라이언트 네트워크 비활성화 (기본값)	클라이언트 네트워크가 활성화되었습니다
Active-Backup(기본값)	• 포트 2와 4는 그리드 네트워크에 액티브-백업 결합을 사용합니다. • 포트 1과 3은 사용되지 않습니다. • VLAN 태그는 선택 사항입니다.	• 포트 2와 4는 그리드 네트워크에 액티브-백업 결합을 사용합니다. • 포트 1과 3은 클라이언트 네트워크에 대해 액티브-백업 연결을 사용합니다. • VLAN 태그는 두 네트워크에 대해 모두 지정할 수 있습니다.

네트워크 연결 모드	클라이언트 네트워크 비활성화 (기본값)	클라이언트 네트워크가 활성화되었습니다
LACP(802.3ad)	• 포트 2와 4는 그리드 네트워크에 LACP 결합을 사용합니다. • 포트 1과 3은 사용되지 않습니다. • VLAN 태그는 선택 사항입니다.	• 포트 2와 4는 그리드 네트워크에 LACP 결합을 사용합니다. • 포트 1과 3은 클라이언트 네트워크에 LACP 결합을 사용합니다. • VLAN 태그는 두 네트워크에 대해 모두 지정할 수 있습니다.

- * 집계 포트 결합 모드 *

네트워크 연결 모드	클라이언트 네트워크 비활성화 (기본값)	클라이언트 네트워크가 활성화되었습니다
LACP(802.3ad)만 해당	• 포트 1-4는 그리드 네트워크에 단일 LACP 결합을 사용합니다. • 단일 VLAN 태그는 그리드 네트워크 패킷을 식별합니다.	• 포트 1-4는 그리드 네트워크 및 클라이언트 네트워크에 단일 LACP 결합을 사용합니다. • 두 개의 VLAN 태그를 통해 그리드 네트워크 패킷을 클라이언트 네트워크 패킷과 분리할 수 있습니다.

자세한 내용은 서비스 어플라이언스의 GbE 포트 연결에 대한 문서를 참조하십시오.

이 그림은 SG100의 1GbE 관리 포트 2개가 관리 네트워크의 Active-Backup 네트워크 연결 모드에서 어떻게 연결되어 있는지 보여 줍니다.

이 그림은 어플라이언스에 있는 2개의 1GbE 관리 포트가 관리 네트워크의 Active-Backup 네트워크 연결 모드에서 어떻게 연결되어 있는지 보여 줍니다.

- SG100 관리 네트워크 포트가 연결됨 *

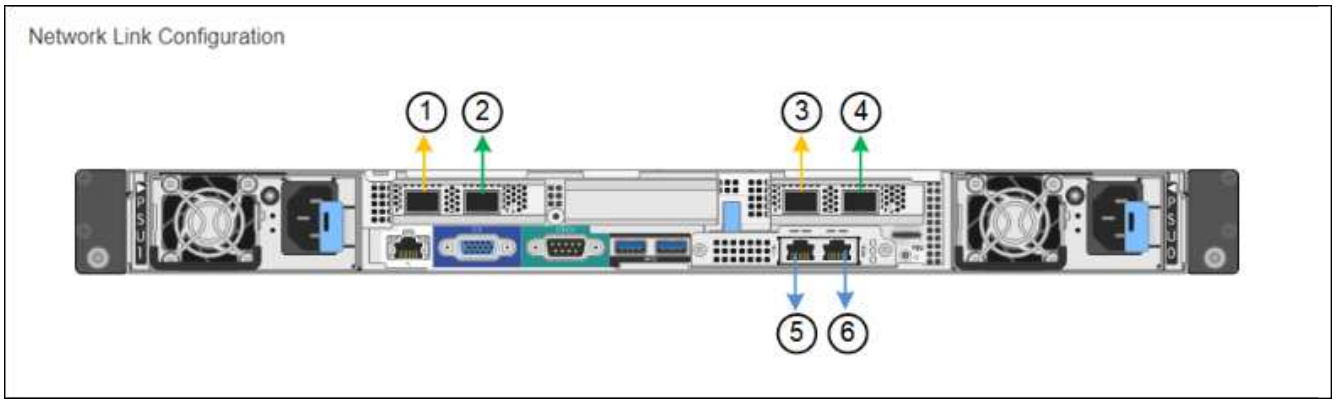
- SG1000 관리자 네트워크 포트가 연결됨 *

단계

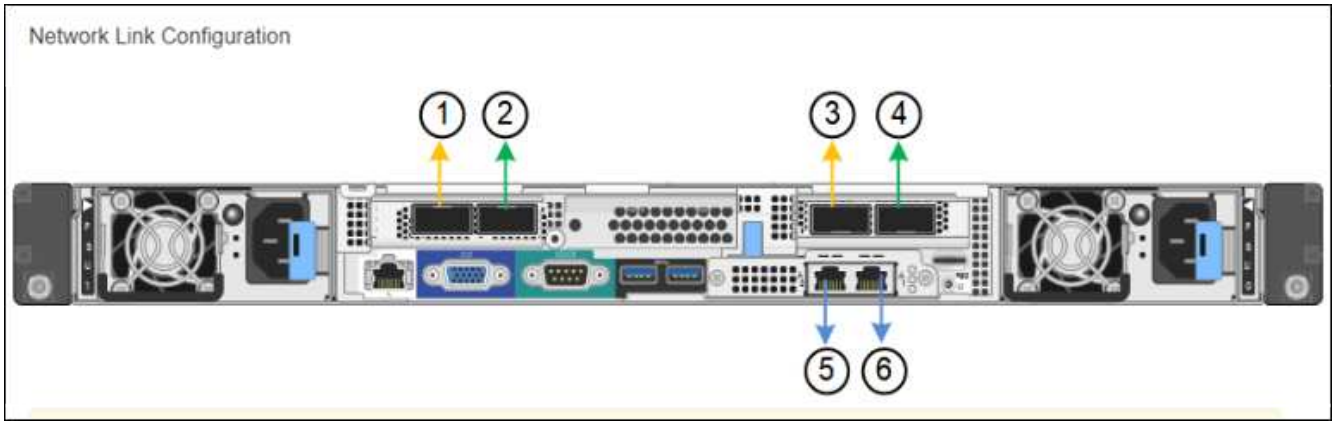
1. StorageGRID 어플라이언스 설치 프로그램의 메뉴 모음에서 * 네트워킹 구성 * > * 링크 구성 * 을 클릭합니다.

   네트워크 링크 구성 페이지에는 네트워크 및 관리 포트 번호가 지정된 어플라이언스 다이어그램이 표시됩니다.

   SG100 포트 *



   SG1000 포트 *



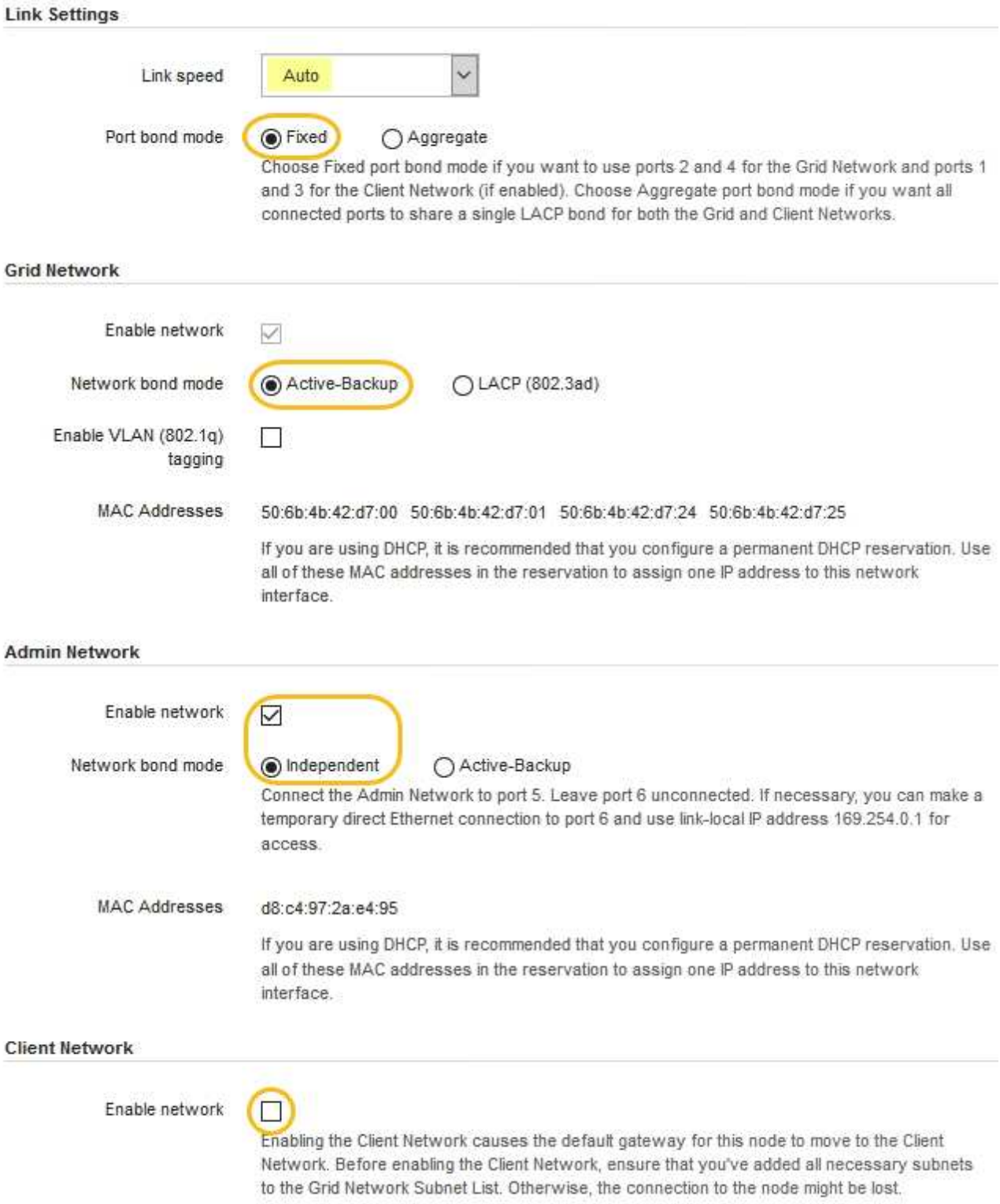
   링크 상태 테이블에는 번호가 매겨진 포트의 링크 상태 및 속도가 나열됩니다(SG1000은 표시됨).

Link Status

Link	State	Speed (Gbps)
1	Up	100
2	Down	N/A
3	Down	N/A
4	Down	N/A
5	Up	1
6	Up	1

이 페이지에 처음 액세스하는 경우:

- * 링크 속도 * 가 * 자동 * 으로 설정되어 있습니다.
- * 포트 결합 모드 * 가 * 고정 * 으로 설정됩니다.
- * 네트워크 연결 모드 * 는 그리드 네트워크에 대해 * Active-Backup * 으로 설정됩니다.
- Admin Network*가 활성화되고 네트워크 연결 모드가 * Independent * 로 설정됩니다.
- 클라이언트 네트워크 * 가 비활성화됩니다.



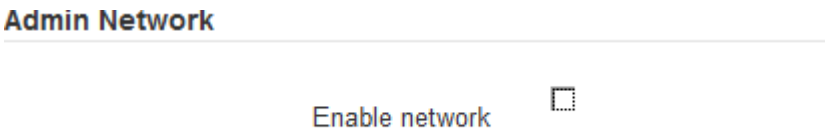
2. 링크 속도 * 드롭다운 목록에서 네트워크 포트의 링크 속도를 선택합니다.

   그리드 네트워크 및 클라이언트 네트워크에 대해 사용 중인 네트워크 스위치도 이 속도를 지원하고 구성해야 합니다. 구성된 링크 속도에 적절한 어댑터 또는 트랜시버를 사용해야 합니다. 이 옵션은 링크 파트너와 링크 속도 및 FEC(Forward Error Correction) 모드를 모두 협상하기 때문에 가능하면 자동 링크 속도를 사용하십시오.

3. 사용하려는 StorageGRID 네트워크를 활성화 또는 비활성화합니다.

그리드 네트워크가 필요합니다. 이 네트워크를 비활성화할 수 없습니다.

a. 어플라이언스가 관리 네트워크에 연결되어 있지 않은 경우 관리 네트워크의 * 네트워크 활성화 * 확인란을 선택 취소합니다.



b. 어플라이언스가 클라이언트 네트워크에 연결되어 있는 경우 클라이언트 네트워크의 * 네트워크 활성화 * 확인란을 선택합니다.

이제 데이터 NIC 포트의 클라이언트 네트워크 설정이 표시됩니다.

4. 표를 참조하여 포트 결합 모드 및 네트워크 연결 모드를 구성합니다.

이 예제는 다음을 보여 줍니다.

- 그리드 및 클라이언트 네트워크에 대해 * 집계 * 및 * LACP * 선택. 각 네트워크에 대해 고유한 VLAN 태그를 지정해야 합니다. 0에서 4095 사이의 값을 선택할 수 있습니다.
- 관리자 네트워크에 대해 * Active-Backup * 이 선택되었습니다.

Link Settings

Link speed: Auto

Port bond mode: ○ Fixed ◉ Aggregate

Choose Fixed port bond mode if you want to use ports 2 and 4 for the Grid Network and ports 1 and 3 for the Client Network (if enabled). Choose Aggregate port bond mode if you want all connected ports to share a single LACP bond for both the Grid and Client Networks.

Grid Network

Enable network: ☑

Network bond mode: ○ Active-Backup ◉ LACP (802.3ad)

If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.

Enable VLAN (802.1q) tagging: ☑

VLAN (802.1q) tag: 328

MAC Addresses: 50:6b:4b:42:d7:00 50:6b:4b:42:d7:01 50:6b:4b:42:d7:24 50:6b:4b:42:d7:25

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

Admin Network

Enable network: ☑

Network bond mode: ○ Independent ◉ Active-Backup

Connect the Admin Network to ports 5 and 6. If necessary, you can make a temporary direct Ethernet connection by disconnecting ports 5 and 6, then connecting to port 6 and using link-local IP address 169.254.0.1 for access.

MAC Addresses: d8:c4:97:2a:e4:95

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

Client Network

Enable network: ☑

Network bond mode: ○ Active-Backup ◉ LACP (802.3ad)

If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.

Enable VLAN (802.1q) tagging: ☑

VLAN (802.1q) tag: 332

MAC Addresses: 50:6b:4b:42:d7:00 50:6b:4b:42:d7:01 50:6b:4b:42:d7:24 50:6b:4b:42:d7:25

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

5. 선택 사항에 만족하면 * 저장 * 을 클릭합니다.

> 연결된 네트워크 또는 링크를 변경한 경우 연결이 끊어질 수 있습니다. 1분 내에 다시 연결되지 않으면 어플라이언스에 할당된 다른 IP 주소 중 하나를 사용하여 StorageGRID 어플라이언스 설치 프로그램의 URL을 다시 입력합니다. + " * https://*services_appliance_IP*:8443*`

관련 정보

추가 장비 및 도구 확보(SG100 및 SG1000)

StorageGRID IP 주소를 구성합니다

StorageGRID 어플라이언스 설치 프로그램을 사용하여 StorageGRID 그리드, 관리자 및 클라이언트 네트워크에서 서비스 어플라이언스에 사용되는 IP 주소 및 라우팅 정보를 구성합니다.

이 작업에 대해

연결된 각 네트워크에서 어플라이언스에 대해 고정 IP를 할당하거나 DHCP 서버의 주소에 대해 영구 임대를 할당해야 합니다.

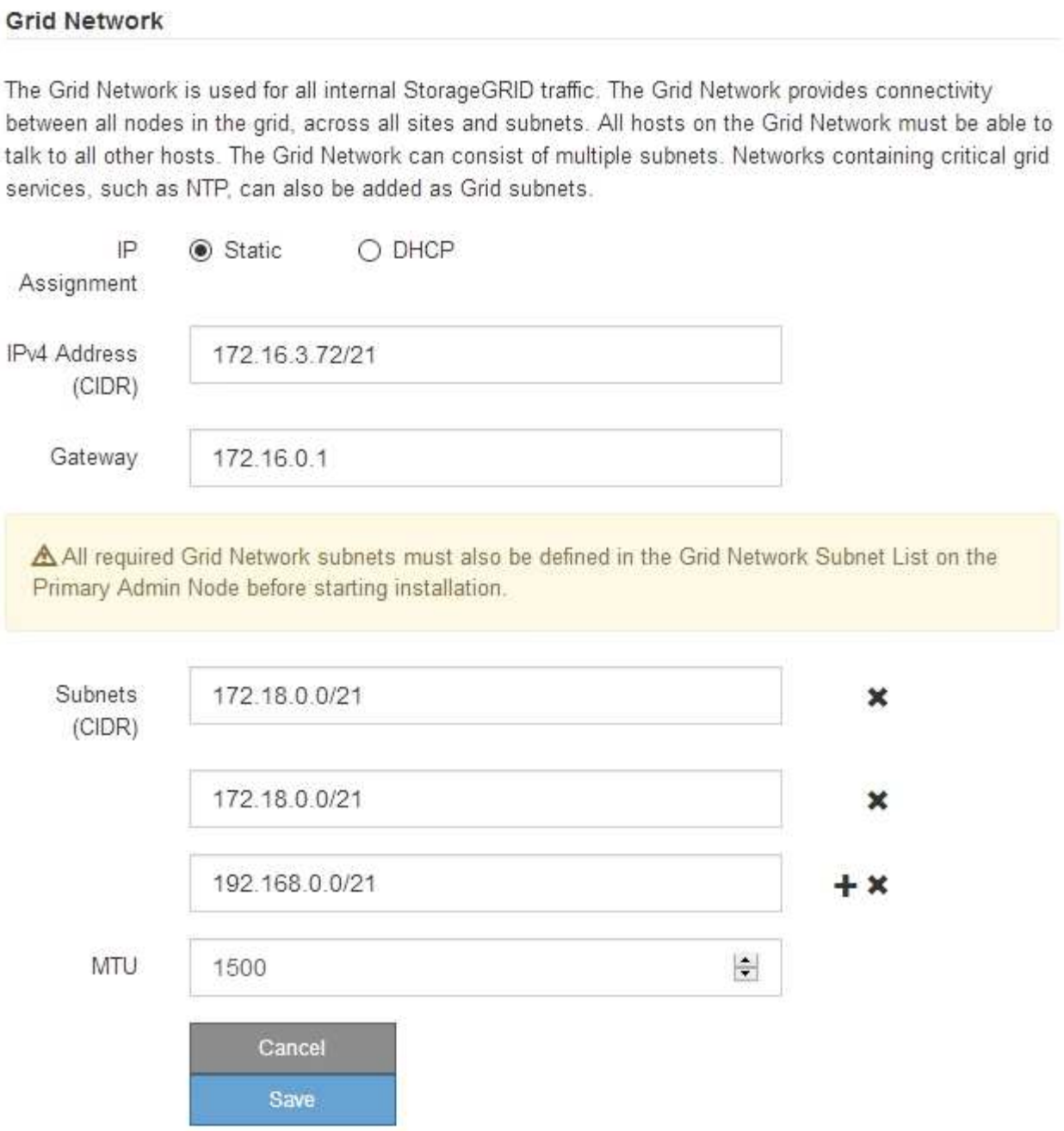
링크 구성을 변경하려면 서비스 어플라이언스의 링크 구성 변경 지침을 참조하십시오.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * IP 구성 * 을 선택합니다.

   IP 구성 페이지가 나타납니다.

2. 그리드 네트워크를 구성하려면 페이지의 * 그리드 네트워크 * 섹션에서 * 정적 * 또는 * DHCP * 를 선택합니다.



3. Static * (정적 *)을 선택한 경우 다음 단계에 따라 Grid Network(그리드 네트워크)를 구성합니다.
   a. CIDR 표기법을 사용하여 정적 IPv4 주소를 입력합니다.
   b. 게이트웨이를 입력합니다.

      네트워크에 게이트웨이가 없는 경우 동일한 정적 IPv4 주소를 다시 입력합니다.

   c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

      > ⓘ 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

> 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

d. 저장 * 을 클릭합니다.

   IP 주소를 변경하면 게이트웨이와 서브넷 목록도 변경될 수 있습니다.

   StorageGRID 어플라이언스 설치 프로그램에 대한 연결이 끊어진 경우 방금 할당한 새 고정 IP 주소를 사용하여 URL을 다시 입력합니다. 예: + `https://services_appliance_IP:8443*

e. 그리드 네트워크 서브넷 목록이 올바른지 확인합니다.

   그리드 서브넷이 있는 경우 그리드 네트워크 게이트웨이가 필요합니다. 지정된 모든 그리드 서브넷은 이 게이트웨이를 통해 연결할 수 있어야 합니다. 이러한 그리드 네트워크 서브넷은 StorageGRID 설치를 시작할 때 기본 관리 노드의 그리드 네트워크 서브넷 목록에도 정의되어 있어야 합니다.

   > 기본 라우트는 나열되지 않습니다. 클라이언트 네트워크가 활성화되지 않은 경우 기본 라우트는 그리드 네트워크 게이트웨이를 사용합니다.

   - 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
   - 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

f. 저장 * 을 클릭합니다.

4. DHCP * 를 선택한 경우 다음 단계에 따라 그리드 네트워크를 구성합니다.

a. DHCP * 라디오 버튼을 선택한 후 * 저장 * 을 클릭합니다.

   IPv4 주소 *, * 게이트웨이 * 및 * 서브넷 * 필드가 자동으로 채워집니다. DHCP 서버가 MTU 값을 할당하도록 설정된 경우 * MTU * 필드가 해당 값으로 채워지고 필드는 읽기 전용이 됩니다.

   웹 브라우저가 자동으로 StorageGRID 어플라이언스 설치 프로그램의 새 IP 주소로 리디렉션됩니다.

b. 그리드 네트워크 서브넷 목록이 올바른지 확인합니다.

   그리드 서브넷이 있는 경우 그리드 네트워크 게이트웨이가 필요합니다. 지정된 모든 그리드 서브넷은 이 게이트웨이를 통해 연결할 수 있어야 합니다. 이러한 그리드 네트워크 서브넷은 StorageGRID 설치를 시작할 때 기본 관리 노드의 그리드 네트워크 서브넷 목록에도 정의되어 있어야 합니다.

   > 기본 라우트는 나열되지 않습니다. 클라이언트 네트워크가 활성화되지 않은 경우 기본 라우트는 그리드 네트워크 게이트웨이를 사용합니다.

   - 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
   - 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

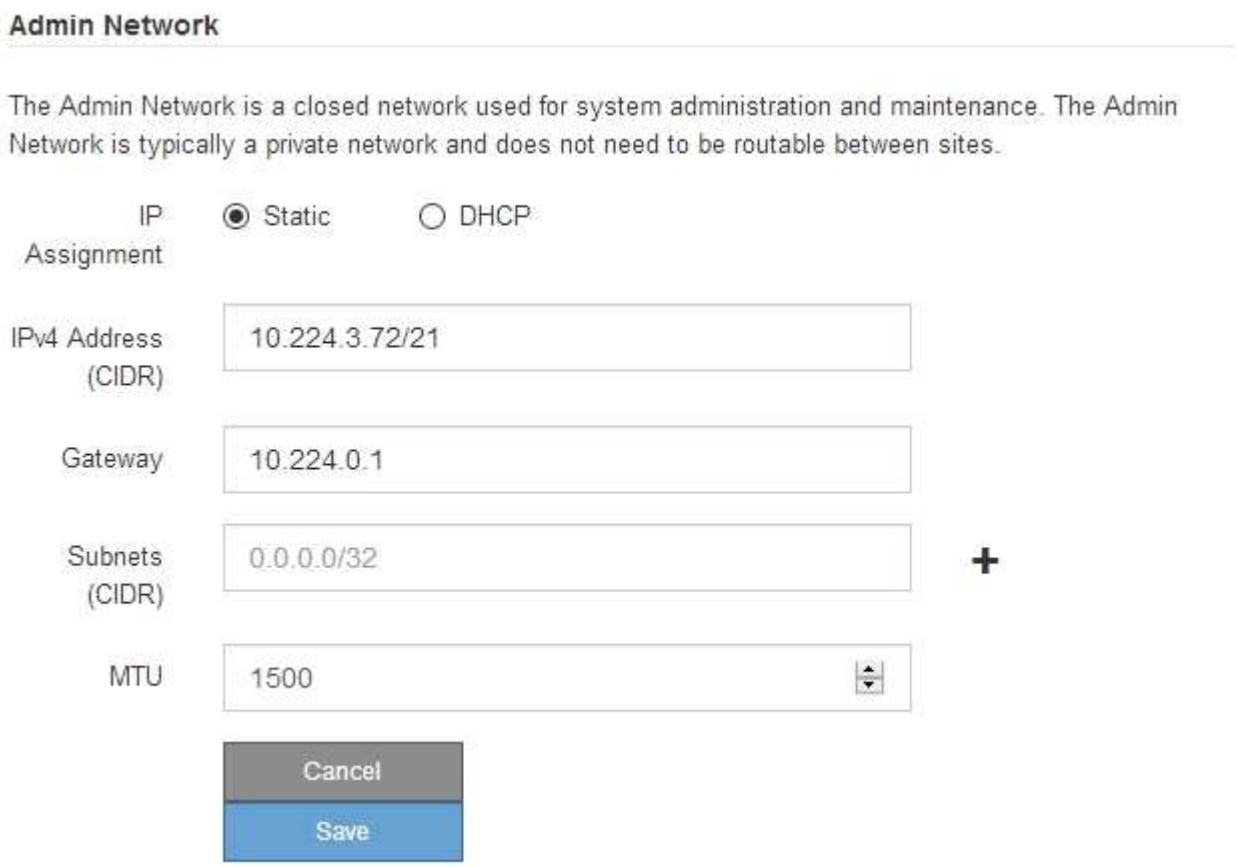
> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

> 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

a. 저장 * 을 클릭합니다.

5. 관리 네트워크를 구성하려면 페이지의 관리 네트워크 섹션에서 * 정적 * 또는 * DHCP * 를 선택합니다.

> 관리 네트워크를 구성하려면 링크 구성 페이지에서 관리 네트워크를 활성화해야 합니다.



6. 정적 * 을 선택한 경우 다음 단계에 따라 관리 네트워크를 구성합니다.

   a. 어플라이언스의 관리 포트 1에 대한 CIDR 표기법을 사용하여 정적 IPv4 주소를 입력합니다.

      관리 포트 1은 어플라이언스의 오른쪽 끝에 있는 2개의 1GbE RJ45 포트 왼쪽에 있습니다.

   b. 게이트웨이를 입력합니다.

      네트워크에 게이트웨이가 없는 경우 동일한 정적 IPv4 주소를 다시 입력합니다.

   c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면

기본값 1500을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

d. 저장 * 을 클릭합니다.

IP 주소를 변경하면 게이트웨이와 서브넷 목록도 변경될 수 있습니다.

StorageGRID 어플라이언스 설치 프로그램에 대한 연결이 끊어진 경우 방금 할당한 새 고정 IP 주소를 사용하여 URL을 다시 입력합니다. 예: + `https://services_appliance:8443*

e. 관리자 네트워크 서브넷 목록이 올바른지 확인합니다.

입력한 게이트웨이를 사용하여 모든 서브넷에 연결할 수 있는지 확인해야 합니다.

> 관리자 네트워크 게이트웨이를 사용하도록 기본 경로를 설정할 수 없습니다.

- 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
- 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

f. 저장 * 을 클릭합니다.

7. DHCP * 를 선택한 경우 다음 단계에 따라 관리 네트워크를 구성합니다.

a. DHCP * 라디오 버튼을 선택한 후 * 저장 * 을 클릭합니다.

IPv4 주소 *, * 게이트웨이 * 및 * 서브넷 * 필드가 자동으로 채워집니다. DHCP 서버가 MTU 값을 할당하도록 설정된 경우 * MTU * 필드가 해당 값으로 채워지고 필드는 읽기 전용이 됩니다.

웹 브라우저가 자동으로 StorageGRID 어플라이언스 설치 프로그램의 새 IP 주소로 리디렉션됩니다.

b. 관리자 네트워크 서브넷 목록이 올바른지 확인합니다.

입력한 게이트웨이를 사용하여 모든 서브넷에 연결할 수 있는지 확인해야 합니다.

> 관리자 네트워크 게이트웨이를 사용하도록 기본 경로를 설정할 수 없습니다.

- 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
- 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

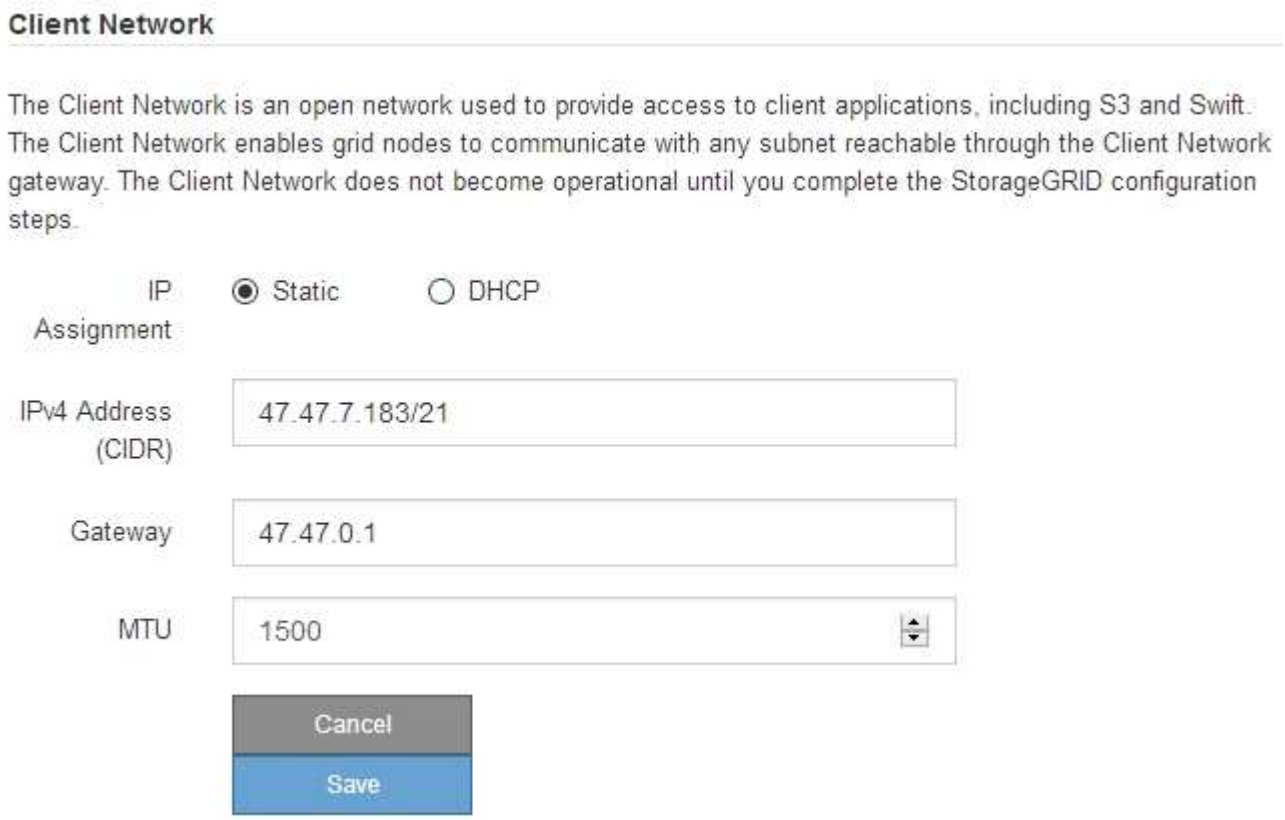
c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

d. 저장 * 을 클릭합니다.

8. 클라이언트 네트워크를 구성하려면 페이지의 * 클라이언트 네트워크 * 섹션에서 * 정적 * 또는 * DHCP * 를 선택합니다.

클라이언트 네트워크를 구성하려면 링크 구성 페이지에서 클라이언트 네트워크를 활성화해야 합니다.



9. 정적 * 을 선택한 경우 다음 단계에 따라 클라이언트 네트워크를 구성합니다.
   a. CIDR 표기법을 사용하여 정적 IPv4 주소를 입력합니다.
   b. 저장 * 을 클릭합니다.
   c. 클라이언트 네트워크 게이트웨이의 IP 주소가 올바른지 확인합니다.

      클라이언트 네트워크가 활성화된 경우 기본 경로가 표시됩니다. 기본 라우트는 클라이언트 네트워크 게이트웨이를 사용하며 클라이언트 네트워크가 활성화된 동안에는 다른 인터페이스로 이동할 수 없습니다.

   d. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

      네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

   e. 저장 * 을 클릭합니다.
10. DHCP * 를 선택한 경우 다음 단계에 따라 클라이언트 네트워크를 구성합니다.
   a. DHCP * 라디오 버튼을 선택한 후 * 저장 * 을 클릭합니다.

      IPv4 주소 * 및 * 게이트웨이 * 필드가 자동으로 채워집니다. DHCP 서버가 MTU 값을 할당하도록 설정된 경우

* MTU * 필드가 해당 값으로 채워지고 필드는 읽기 전용이 됩니다.

웹 브라우저가 자동으로 StorageGRID 어플라이언스 설치 프로그램의 새 IP 주소로 리디렉션됩니다.

a. 게이트웨이가 올바른지 확인합니다.

> 클라이언트 네트워크가 활성화된 경우 기본 경로가 표시됩니다. 기본 라우트는 클라이언트 네트워크 게이트웨이를 사용하며 클라이언트 네트워크가 활성화된 동안에는 다른 인터페이스로 이동할 수 없습니다.

b. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

관련 정보

서비스 어플라이언스의 링크 구성을 변경합니다

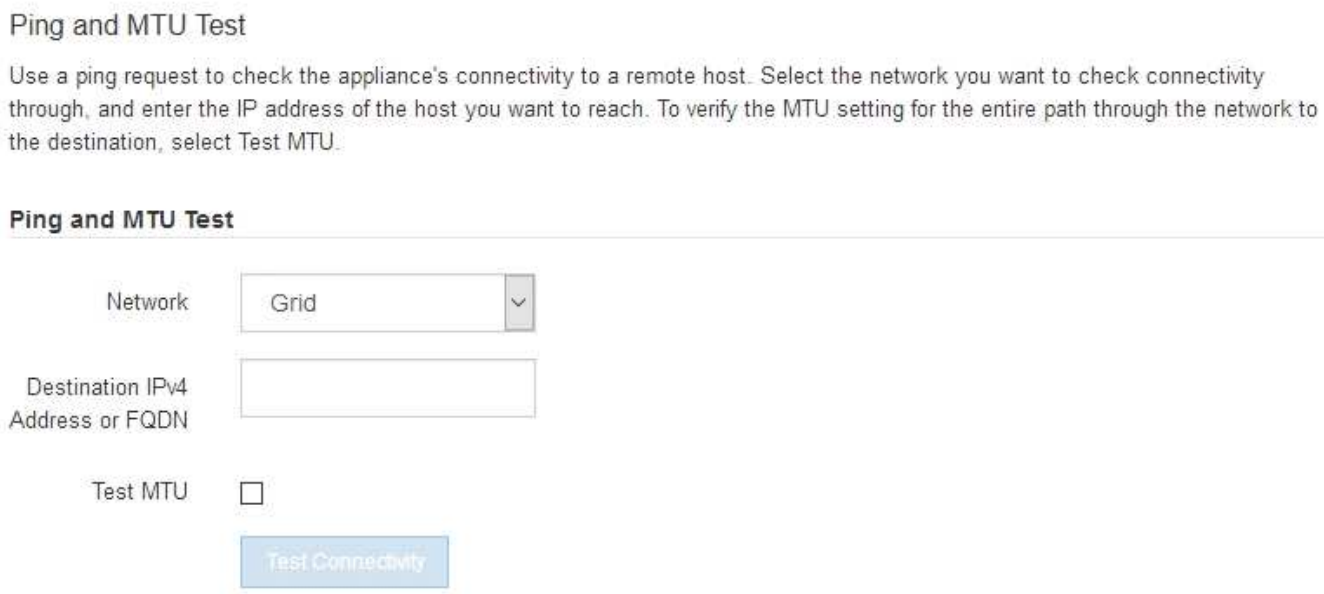
네트워크 연결을 확인합니다

어플라이언스에서 사용 중인 StorageGRID 네트워크에 액세스할 수 있는지 확인해야 합니다. 네트워크 게이트웨이를 통한 라우팅의 유효성을 검사하려면 StorageGRID 어플라이언스 설치 프로그램과 다른 서브넷의 IP 주소 간의 연결을 테스트해야 합니다. MTU 설정을 확인할 수도 있습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램의 메뉴 모음에서 * 네트워킹 구성 * > * Ping 및 MTU 테스트 * 를 클릭합니다.

   Ping 및 MTU 테스트 페이지가 나타납니다.



2. 네트워크 * 드롭다운 상자에서 테스트할 네트워크(그리드, 관리자 또는 클라이언트)를 선택합니다.
3. 해당 네트워크의 호스트에 대한 IPv4 주소 또는 FQDN(정규화된 도메인 이름)을 입력합니다.

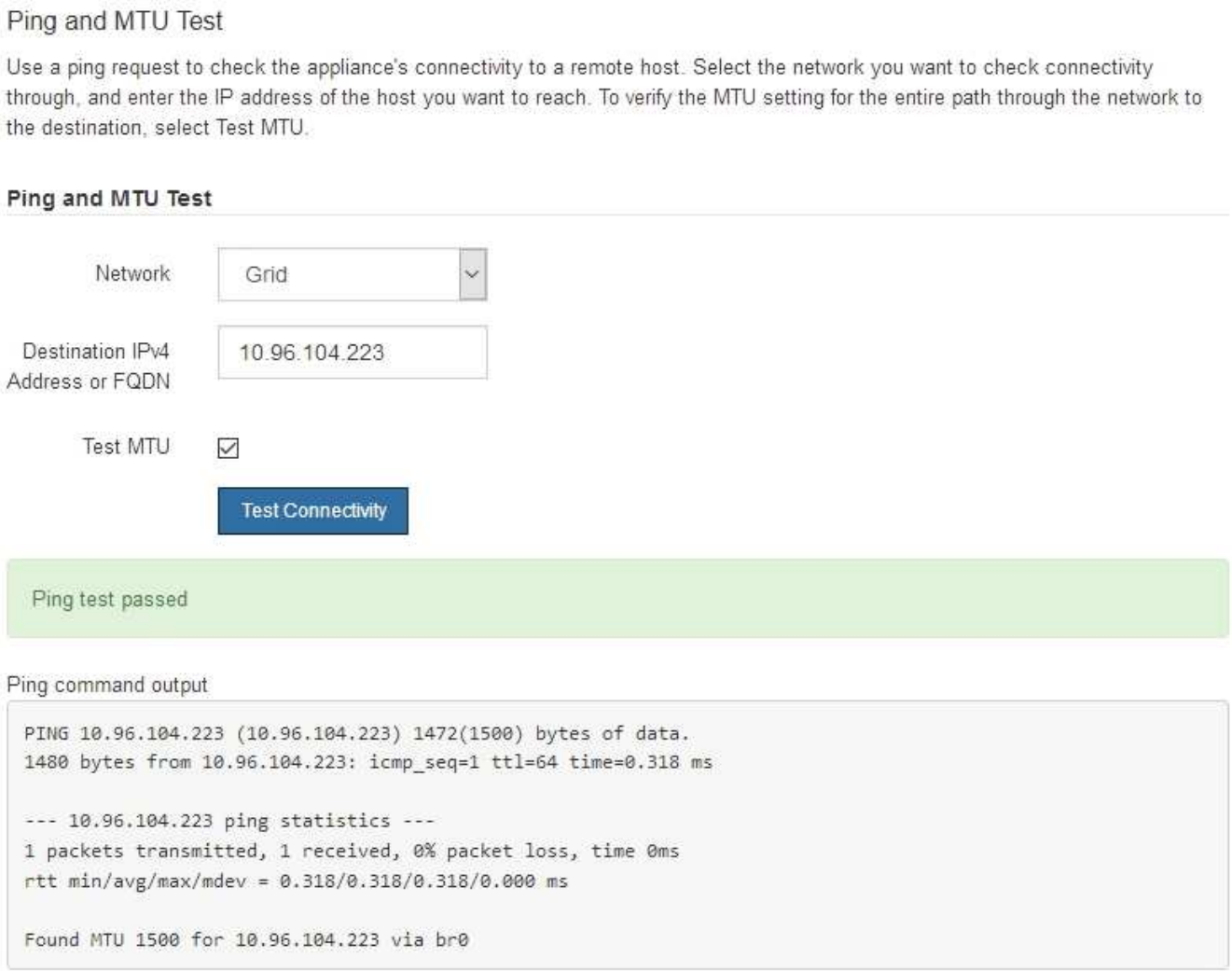
   예를 들어 네트워크 또는 기본 관리 노드의 게이트웨이를 Ping할 수 있습니다.

4. 선택적으로 * Test MTU * 확인란을 선택하여 네트워크를 통해 대상으로 가는 전체 경로에 대한 MTU 설정을 확인합니다.

   예를 들어, 어플라이언스 노드와 다른 사이트의 노드 간 경로를 테스트할 수 있습니다.

5. 연결 테스트 * 를 클릭합니다.

   네트워크 연결이 유효한 경우 ping 명령 출력이 나열된 "Ping test Passed" 메시지가 나타납니다.



관련 정보

네트워크 링크 구성(SG100 및 SG1000)

MTU 설정을 변경합니다

포트 수준 네트워크 연결을 확인합니다

StorageGRID 어플라이언스 설치 프로그램과 다른 노드 간의 액세스가 방화벽에 의해 방해 받지 않도록 하려면 StorageGRID 어플라이언스 설치 관리자가 지정된 IP 주소 또는 주소 범위의 특정 TCP 포트 또는 포트 집합에 연결할 수 있는지 확인합니다.

이 작업에 대해

StorageGRID 어플라이언스 설치 프로그램에 제공된 포트 목록을 사용하여 어플라이언스와 그리드 네트워크의 다른 노드 간의 연결을 테스트할 수 있습니다.

또한 외부 NFS 또는 DNS 서버에 사용되는 것과 같은 UDP 포트와 Admin 및 Client Networks에서 연결을 테스트할 수 있습니다. 이러한 포트 목록은 StorageGRID 네트워킹 지침의 포트 참조를 참조하십시오.

> 포트 연결 테이블에 나열된 그리드 네트워크 포트는 StorageGRID 버전 11.6.0에만 유효합니다. 각 노드 유형에 맞는 포트를 확인하려면 사용 중인 StorageGRID 버전에 대한 네트워킹 지침을 항상 참조해야 합니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * 포트 연결 테스트(nmap) * 를 클릭합니다.

   포트 연결 테스트 페이지가 나타납니다.

   포트 연결 표에는 그리드 네트워크에서 TCP 연결이 필요한 노드 유형이 나와 있습니다. 각 노드 유형에 대해 표에는 어플라이언스에 액세스할 수 있어야 하는 그리드 네트워크 포트가 나열되어 있습니다.

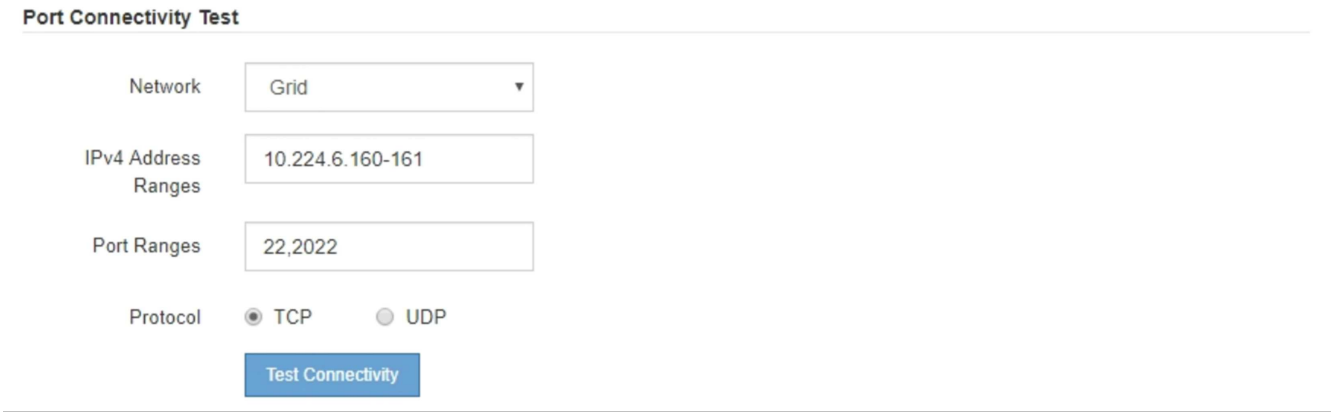
   표에 나열된 어플라이언스 포트와 그리드 네트워크의 다른 노드 간의 연결을 테스트할 수 있습니다.

2. Network * (네트워크 **)** 드롭다운에서 *** Grid * (**그리드 ***), * Admin * (** 관리자 *) 또는 * Client * (클라이언트 *)와 같이 테스트할 네트워크를 선택합니다.
3. 해당 네트워크의 호스트에 대한 IPv4 주소 범위를 지정합니다.

   예를 들어 네트워크 또는 기본 관리 노드의 게이트웨이를 조사할 수 있습니다.

   예제에 표시된 대로 하이픈을 사용하여 범위를 지정합니다.

4. TCP 포트 번호, 쉼표로 구분된 포트 목록 또는 포트 범위를 입력합니다.



5. 연결 테스트 * 를 클릭합니다.

- 선택한 포트 수준 네트워크 연결이 유효하면 ""포트 연결 테스트 통과"" 메시지가 녹색 배너에 나타납니다. nmap 명령 출력은 배너 아래에 나열되어 있습니다.

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- 원격 호스트에 대한 포트 수준 네트워크 연결이 이루어졌지만 호스트가 선택한 포트 중 하나 이상의 포트에서 수신 대기 중이 아니면 ""포트 연결 테스트 실패" 메시지가 노란색 배너에 나타납니다. nmap 명령 출력은 배너 아래에 나열되어 있습니다.

  호스트가 청취하지 않는 모든 원격 포트는 ""닫힘"" 상태입니다. 예를 들어 연결하려는 노드가 사전 설치된 상태이고 StorageGRID NMS 서비스가 아직 실행되지 않은 경우 이 노란색 배너가 나타날 수 있습니다.

Port connectivity test failed
Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
1504/tcp closed evb-elm
1505/tcp open   funkproxy
1506/tcp open   utcd
1508/tcp open   diagmond
7443/tcp open   oracleas-https
9999/tcp open   abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- 하나 이상의 선택한 포트에 대해 포트 수준 네트워크 연결을 설정할 수 없는 경우 빨간색 배너에 ""포트 연결 테스트 실패" 메시지가 나타납니다. nmap 명령 출력은 배너 아래에 나열되어 있습니다.

  빨간색 배너는 원격 호스트의 포트에 대한 TCP 연결 시도가 이루어졌지만 보낸 사람에게 반환된 것이 없음을 나타냅니다. 응답이 반환되지 않으면 포트에 "필터링된" 상태가 있으며 방화벽에 의해 차단될 수 있습니다.

  ⓘ 폐쇄된 항만 목록에 있다.

Port connectivity test failed
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT     STATE    SERVICE
22/tcp   open     ssh
79/tcp   filtered finger
80/tcp   open     http
443/tcp  open     https
1504/tcp closed   evb-elm
1505/tcp open     funkproxy
1506/tcp open     utcd
1508/tcp open     diagmond
7443/tcp open     oracleas-https
9999/tcp open     abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

관련 정보

네트워킹 지침

BMC 인터페이스 구성(SG100 및 SG1000)

서비스 어플라이언스의 BMC(베이스보드 관리 컨트롤러)에 대한 사용자 인터페이스는 하드웨어에 대한 상태 정보를 제공하고 서비스 어플라이언스에 대한 SNMP 설정 및 기타 옵션을 구성할 수 있도록 합니다.

BMC 인터페이스의 루트 암호를 변경합니다

보안을 위해 BMC 루트 사용자의 암호를 변경해야 합니다.

필요한 것

관리 클라이언트에서 을 사용하고 있습니다 지원되는 웹 브라우저.

이 작업에 대해

어플라이언스를 처음 설치할 때 BMC는 루트 사용자('root/calvin')의 기본 암호를 사용합니다. 시스템을 보호하려면 루트 사용자의 암호를 변경해야 합니다.

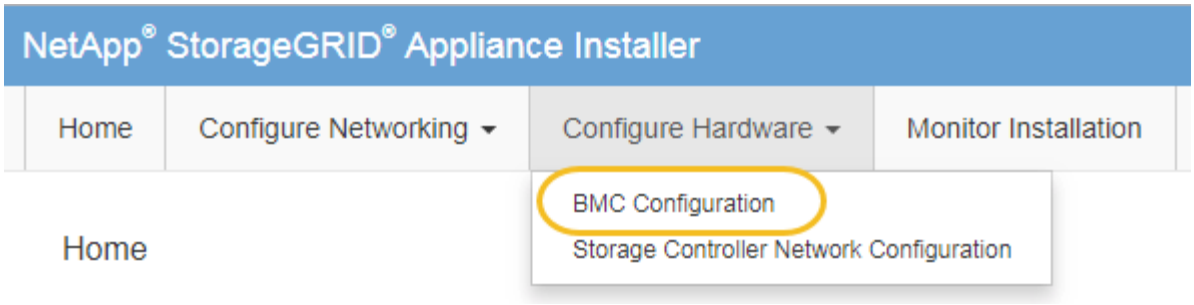
단계

1. 클라이언트에서 StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. + `https://services_appliance_IP:8443*`

   'ervices_appliance_ip'의 경우, 모든 StorageGRID 네트워크에서 어플라이언스의 IP 주소를 사용하십시오.

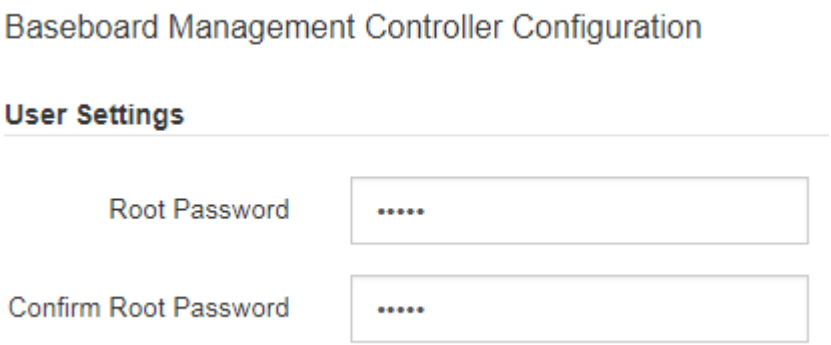
   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 하드웨어 구성 * > * BMC 구성 * 을 선택합니다.



베이스보드 관리 컨트롤러 구성 페이지가 나타납니다.

3. 제공된 두 필드에 루트 계정에 대한 새 암호를 입력합니다.



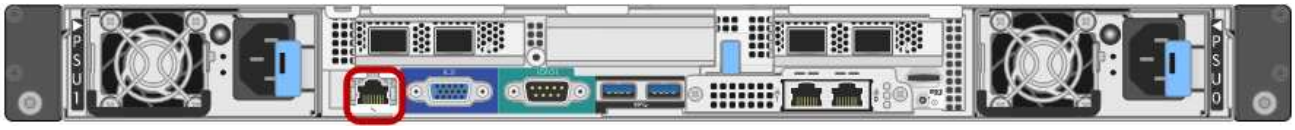
4. 저장 * 을 클릭합니다.

BMC 관리 포트의 **IP** 주소를 설정합니다

BMC 인터페이스에 액세스하려면 먼저 서비스 어플라이언스에서 BMC 관리 포트의 IP 주소를 구성해야 합니다.

필요한 것

- 관리 클라이언트에서 을 사용하고 있습니다 지원되는 웹 브라우저.
- StorageGRID 네트워크에 연결할 수 있는 관리 클라이언트를 사용 중입니다.
- BMC 관리 포트가 사용하려는 관리 네트워크에 연결되어 있습니다.
- SG100 BMC 관리 포트 *



- SG1000 BMC 관리 포트 *

이 작업에 대해

지원을 위해 BMC 관리 포트를 사용하면 낮은 수준의 하드웨어 액세스가 가능합니다. 이 포트는 안전하고 신뢰할 수 있는 내부 관리 네트워크에만 연결해야 합니다. 이러한 네트워크를 사용할 수 없는 경우 기술 지원 부서에서 BMC 연결을 요청하지 않는 한 BMC 포트는 연결되지 않거나 차단된 상태로 둡니다.

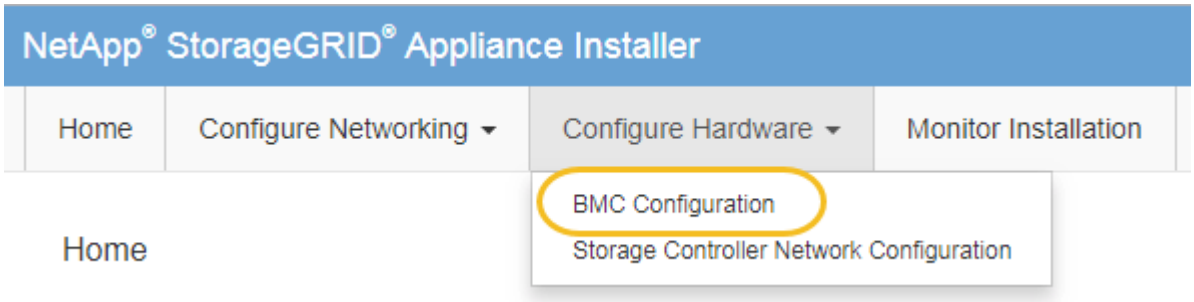
단계

1. 클라이언트에서 StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. + `https://services_appliance_IP:8443*`

   '*services_appliance_ip*'의 경우 StorageGRID 네트워크에서 어플라이언스의 IP 주소를 사용합니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 하드웨어 구성 * > * BMC 구성 * 을 선택합니다.

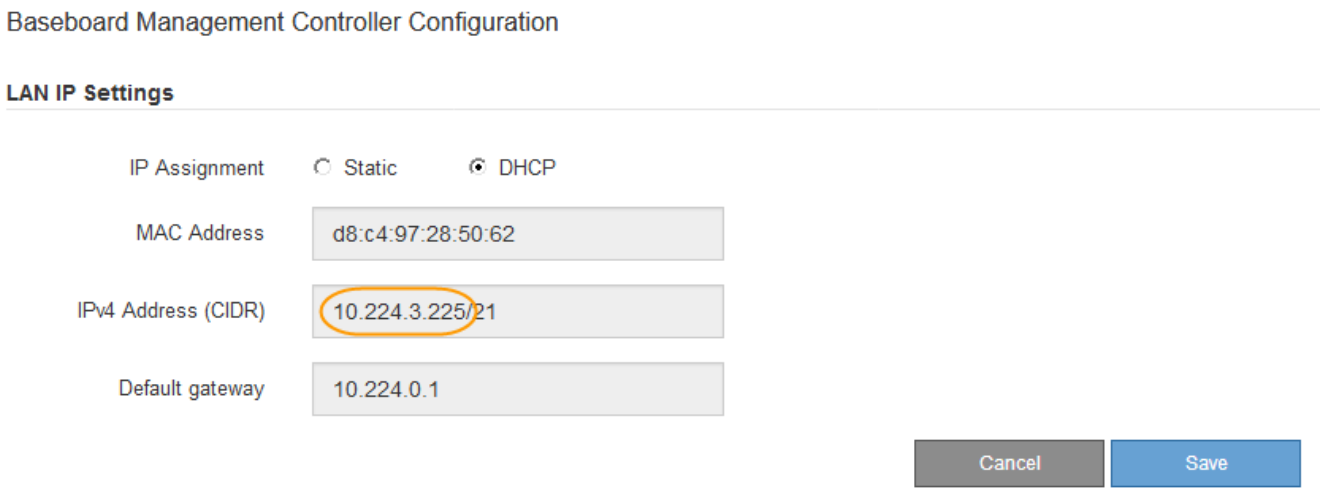


   베이스보드 관리 컨트롤러 구성 페이지가 나타납니다.

3. 자동으로 표시되는 IPv4 주소를 기록해 둡니다.

   DHCP는 이 포트에 IP 주소를 할당하는 기본 방법입니다.

   DHCP 값이 나타나려면 몇 분 정도 걸릴 수 있습니다.



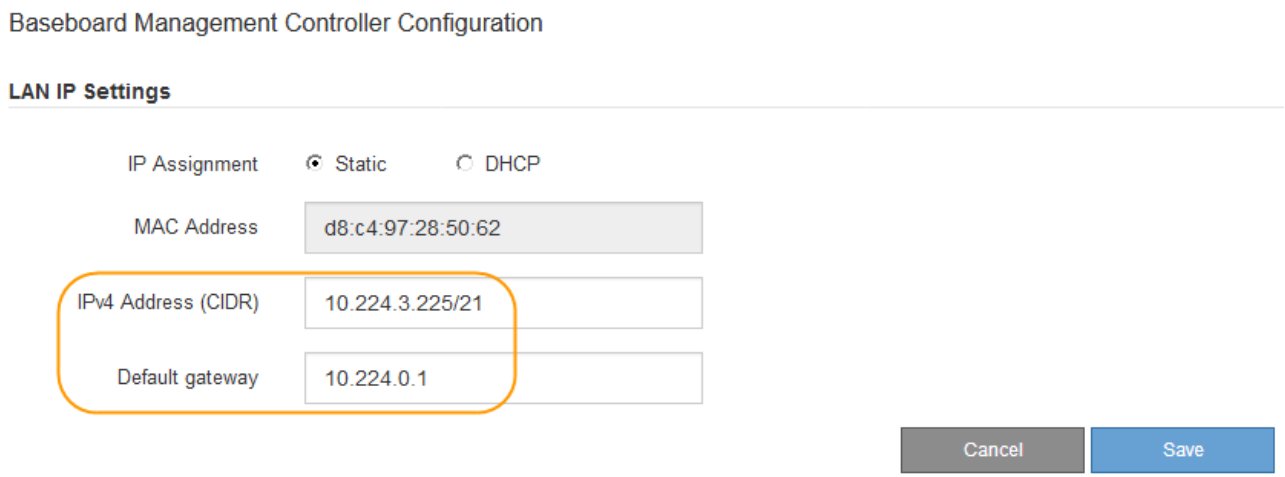
4. 필요에 따라 BMC 관리 포트에 대한 정적 IP 주소를 설정합니다.

BMC 관리 포트에 고정 IP를 할당하거나 DHCP 서버의 주소에 영구 임대를 할당해야 합니다.

a. Static * 을 선택합니다.

b. CIDR 표기법을 사용하여 IPv4 주소를 입력합니다.

c. 기본 게이트웨이를 입력합니다.



d. 저장 * 을 클릭합니다.

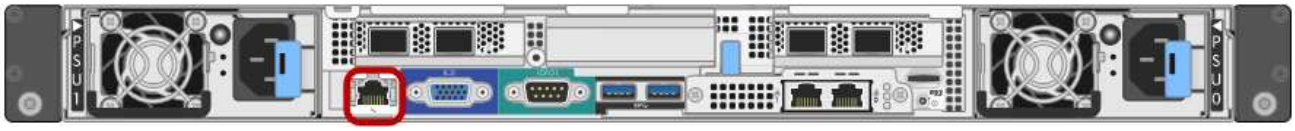
변경 사항을 적용하는 데 몇 분 정도 걸릴 수 있습니다.

BMC 인터페이스에 액세스합니다

BMC 관리 포트의 DHCP 또는 고정 IP 주소를 사용하여 서비스 어플라이언스에서 BMC 인터페이스에 액세스할 수 있습니다.

필요한 것

- 관리 클라이언트에서 을 사용하고 있습니다 지원되는 웹 브라우저.
- 서비스 어플라이언스의 BMC 관리 포트는 사용하려는 관리 네트워크에 연결되어 있습니다.
- SG100 BMC 관리 포트 *



- SG1000 BMC 관리 포트 *

단계

1. BMC 인터페이스의 URL을 입력합니다: + `https://BMC_Port_IP*`

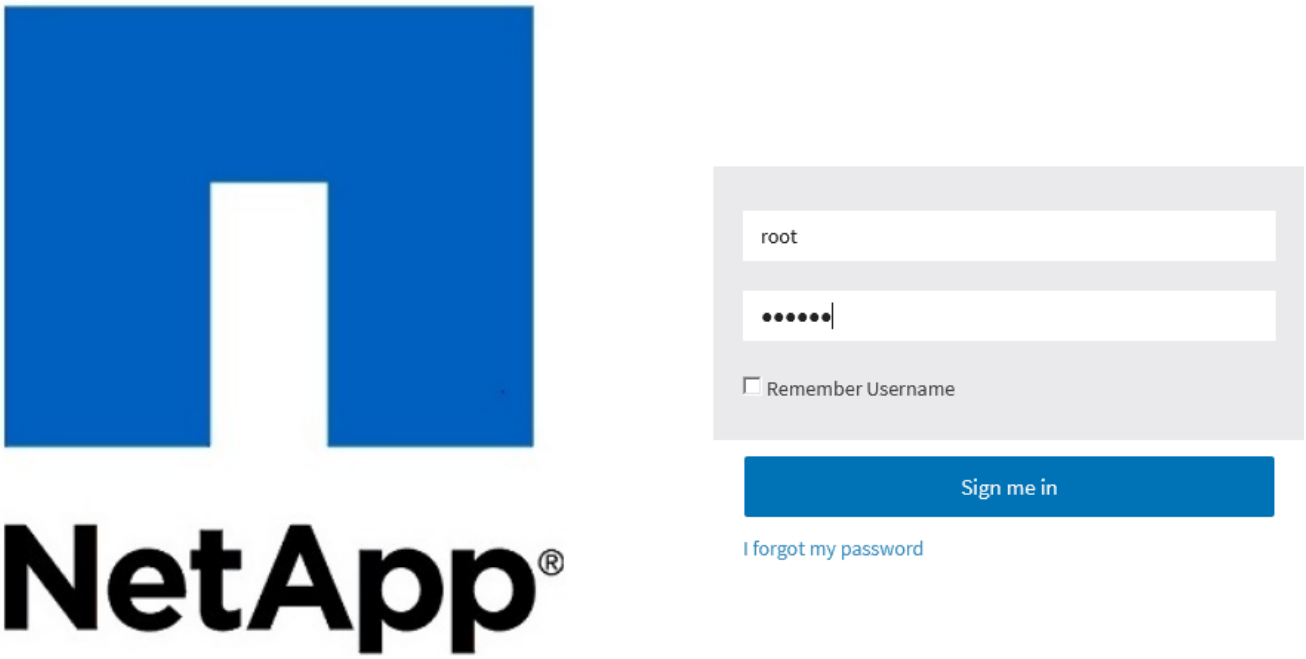
'*BMC_Port_IP*'의 경우 BMC 관리 포트에 대해 DHCP 또는 고정 IP 주소를 사용합니다.

BMC 로그인 페이지가 나타납니다.

> 아직 BMC_Port_IP를 구성하지 않은 경우 의 지침을 따르십시오 BMC 인터페이스 구성(SG100/SG1000). 하드웨어 문제로 인해 해당 절차를 수행할 수 없고 아직 BMC IP 주소를 구성하지 않은 경우 BMC에 계속 액세스할 수 있습니다. 기본적으로 BMC는 DHCP를 사용하여 IP 주소를 얻습니다. BMC 네트워크에서 DHCP가 활성화된 경우 네트워크 관리자는 BMC MAC에 할당된 IP 주소를 제공할 수 있습니다. 이 주소는 SG6000-CN 컨트롤러 전면에 있는 레이블에 인쇄되어 있습니다. BMC 네트워크에서 DHCP가 활성화되어 있지 않으면 몇 분 후에 BMC가 응답하지 않고 기본 정적 IP인 192.168.0.120을 할당합니다. 랩톱을 BMC 포트에 직접 연결하고 네트워크 설정을 변경하여 랩톱에 192.168.0.200/24 등의 IP를 할당하여 192.168.0.120'으로 찾아야 할 수도 있습니다.

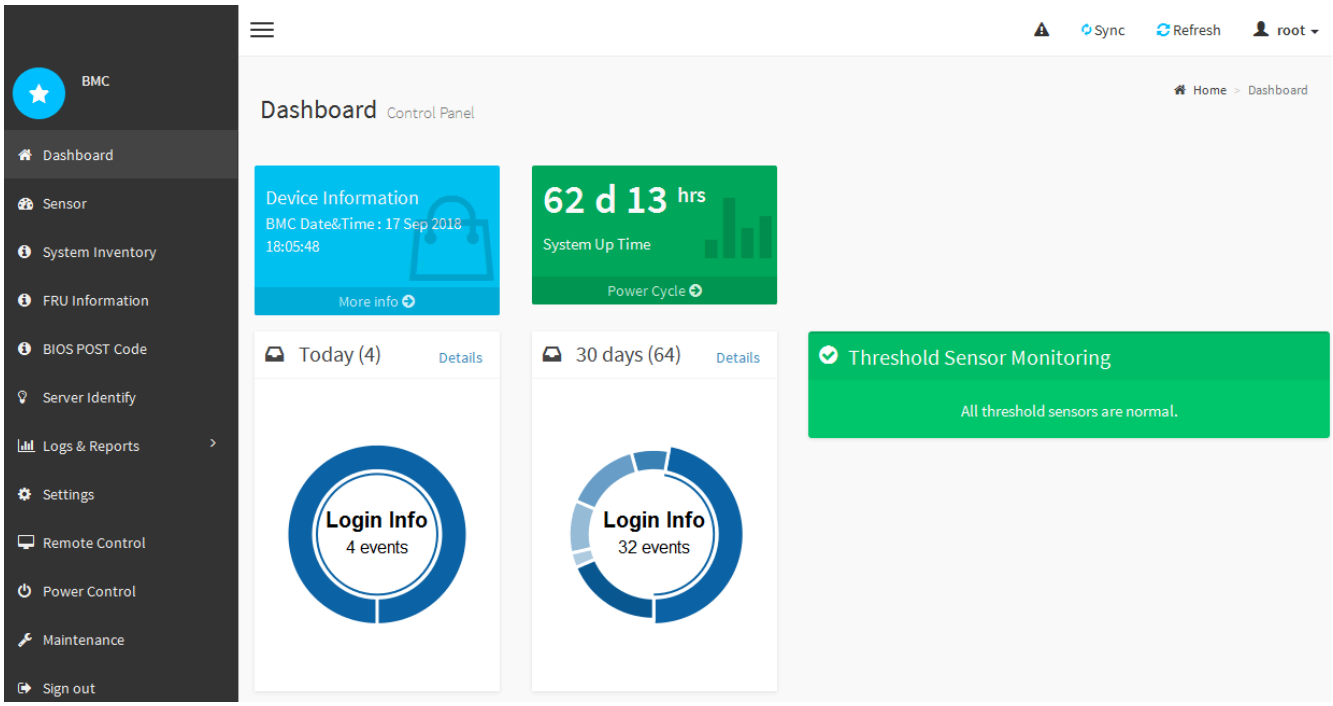
2. 기본 루트 암호를 변경할 때 설정한 암호를 사용하여 루트 사용자 이름과 암호를 입력합니다: + " * root * "

   '**password* *'



3. 로그인 * 을 클릭합니다

   BMC 대시보드가 나타납니다.



4. 선택적으로 * 설정 * > * 사용자 관리 * 를 선택하고 "사용 안 함" 사용자를 클릭하여 추가 사용자를 생성합니다.

> 사용자가 처음 로그인할 때 보안을 강화하기 위해 암호를 변경하라는 메시지가 표시될 수 있습니다.

관련 정보

BMC 인터페이스의 루트 암호를 변경합니다

서비스 어플라이언스에 대한 **SNMP** 설정을 구성합니다

하드웨어에 대한 SNMP 구성에 익숙한 경우 BMC 인터페이스를 사용하여 서비스 어플라이언스에 대한 SNMP 설정을 구성할 수 있습니다. 보안 커뮤니티 문자열을 제공하고, SNMP 트랩을 활성화하고, 최대 5개의 SNMP 대상을 지정할 수 있습니다.

필요한 것

- BMC 대시보드에 액세스하는 방법을 알고 있습니다.
- SNMPv1-v2c 장비에 대한 SNMP 설정을 구성한 경험이 있습니다.

> 이 절차에서 만든 BMC 설정은 어플라이언스에 장애가 발생하여 교체해야 하는 경우 유지되지 않을 수 있습니다. 하드웨어 교체 후 필요한 경우 쉽게 다시 적용할 수 있도록 적용한 모든 설정에 대한 기록이 있어야 합니다.

단계

1. BMC 대시보드에서 * 설정 * > * SNMP 설정 * 을 선택합니다.
2. SNMP 설정 페이지에서 * SNMP V1/V2 * 활성화 를 선택한 다음 읽기 전용 커뮤니티 문자열과 읽기/쓰기 커뮤니티 문자열을 제공합니다.

   읽기 전용 커뮤니티 문자열은 사용자 ID 또는 암호와 같습니다. 침입자가 네트워크 설정에 대한 정보를 얻지 못하게 하려면 이 값을 변경해야 합니다. 읽기-쓰기 커뮤니티 문자열은 인증되지 않은 변경으로부터 장치를 보호합니다.

3. 필요에 따라 * 트랩 사용 * 을 선택하고 필요한 정보를 입력합니다.

> IP 주소를 사용하여 각 SNMP 트랩의 대상 IP를 입력합니다. 정규화된 도메인 이름은 지원되지 않습니다.

서비스 어플라이언스가 비정상 상태일 때 SNMP 콘솔에 즉시 알림을 보내도록 하려면 트랩을 활성화합니다. 트랩은 링크 상승/하강 상태, 특정 임계값을 초과하는 온도 또는 높은 트래픽을 나타낼 수 있습니다.

4. 필요에 따라 * 테스트 트랩 전송 * 을 클릭하여 설정을 테스트합니다.
5. 설정이 올바르면 * 저장 * 을 클릭합니다.

알림에 대한 이메일 알림을 설정합니다

경고가 발생할 때 e-메일 알림을 보내려면 BMC 인터페이스를 사용하여 SMTP 설정, 사용자, LAN 대상, 경고 정책 및 이벤트 필터를 구성해야 합니다.

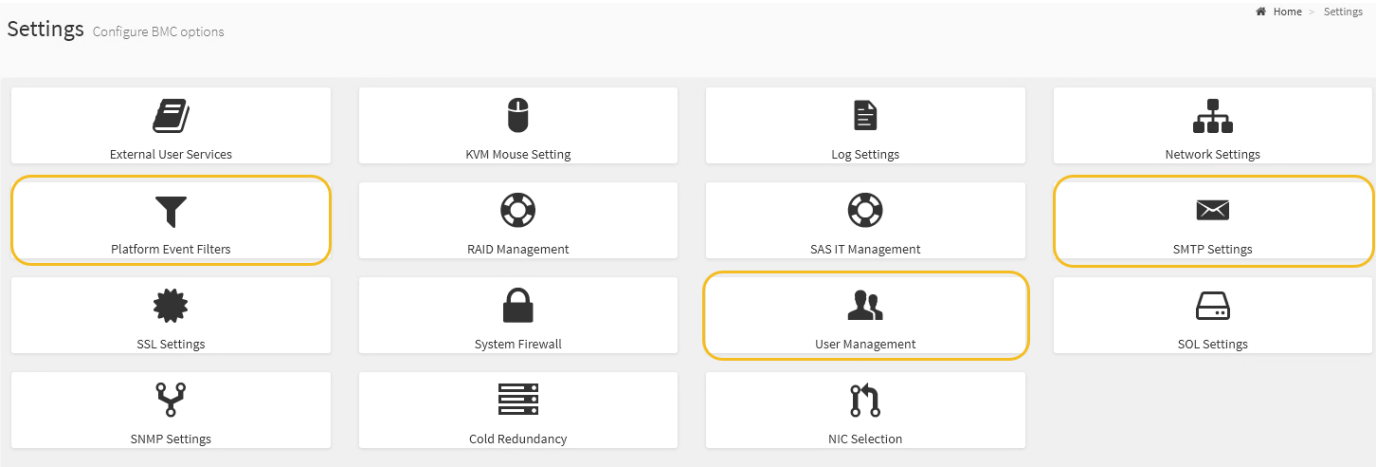
> 이 절차에서 만든 BMC 설정은 어플라이언스에 장애가 발생하여 교체해야 하는 경우 유지되지 않을 수 있습니다. 하드웨어 교체 후 필요한 경우 쉽게 다시 적용할 수 있도록 적용한 모든 설정에 대한 기록이 있어야 합니다.

필요한 것

BMC 대시보드에 액세스하는 방법을 알고 있습니다.

이 작업에 대해

BMC 인터페이스에서 설정 페이지의 * SMTP 설정 *, * 사용자 관리 * 및 * 플랫폼 이벤트 필터 * 옵션을 사용하여 이메일 알림을 구성합니다.



단계

1. SMTP 설정을 구성합니다.
   a. 설정 * > * SMTP 설정 * 을 선택합니다.
   b. 보낸 사람 e-메일 ID의 경우 유효한 e-메일 주소를 입력합니다.

      이 전자 메일 주소는 BMC가 전자 메일을 보낼 때 보내는 사람 주소로 제공됩니다.

2. 알림을 받도록 사용자를 설정합니다.
   a. BMC 대시보드에서 * 설정 * > * 사용자 관리 * 를 선택합니다.
   b. 알림 알림을 수신할 사용자를 한 명 이상 추가하십시오.

      사용자에 대해 구성한 전자 메일 주소는 BMC가 경고 알림을 보내는 주소입니다. 예를 들어 ""notification-user""와 같은 일반 사용자를 추가하고 기술 지원 팀 이메일 배포 목록의 이메일 주소를 사용할 수 있습니다.

3. 경고를 위한 LAN 대상을 구성합니다.
   a. 설정 * > * 플랫폼 이벤트 필터 * > * LAN 대상 * 을 선택합니다.
   b. LAN 대상을 하나 이상 구성합니다.
      - 대상 유형으로 * 이메일 * 을 선택합니다.
      - BMC Username 에서 이전에 추가한 사용자 이름을 선택합니다.
      - 여러 사용자를 추가했으며 모든 사용자가 알림 이메일을 받도록 하려면 각 사용자에 대해 LAN 대상을 추가해야 합니다.
   c. 테스트 알림을 보냅니다.
4. BMC가 경고를 보내는 시기와 위치를 정의할 수 있도록 경고 정책을 구성합니다.
   a. 설정 * > * 플랫폼 이벤트 필터 * > * 경고 정책 * 을 선택합니다.
   b. 각 LAN 대상에 대해 하나 이상의 경고 정책을 구성합니다.
      - 정책 그룹 번호 로 * 1 * 을 선택합니다.
      - 정책 작업의 경우 * 항상 이 대상으로 알림 전송 * 을 선택합니다.
      - LAN 채널의 경우 * 1 * 을 선택합니다.
      - 대상 선택기에서 정책의 LAN 대상을 선택합니다.
5. 다양한 이벤트 유형에 대한 경고를 적절한 사용자에게 보내도록 이벤트 필터를 구성합니다.
   a. 설정 * > * 플랫폼 이벤트 필터 * > * 이벤트 필터 * 를 선택합니다.
   b. 경고 정책 그룹 번호 에 * 1 * 을 입력합니다.
   c. 경고 정책 그룹에 알림을 보낼 모든 이벤트에 대한 필터를 만듭니다.
      - 전원 동작, 특정 센서 이벤트 또는 모든 이벤트에 대한 이벤트 필터를 만들 수 있습니다.
      - 모니터링할 이벤트를 잘 모르는 경우 센서 유형에 대해 * All Sensors * 를 선택하고 이벤트 옵션에 대해 * All Events * 를 선택합니다. 원치 않는 알림을 받으면 나중에 선택 사항을 변경할 수 있습니다.

선택 사항: 노드 암호화를 활성화합니다

노드 암호화를 사용하는 경우 어플라이언스의 디스크는 물리적 손실 또는 사이트 제거로부터 보안 키 관리 서버(KMS) 암호화로 보호할 수 있습니다. 어플라이언스 설치 중에 노드 암호화를 선택하고 활성화해야 하며 KMS 암호화 프로세스가 시작되면 노드 암호화를 선택 취소할 수 없습니다.

필요한 것

StorageGRID 관리 지침에 따라 KMS에 대한 정보를 검토합니다.

이 작업에 대해

노드 암호화가 활성화된 어플라이언스는 StorageGRID 사이트에 대해 구성된 외부 키 관리 서버(KMS)에 연결됩니다. 각 KMS(또는 KMS 클러스터)는 사이트의 모든 어플라이언스 노드에 대한 암호화 키를 관리합니다. 이러한 키는 노드 암호화가 활성화된 어플라이언스에서 각 디스크의 데이터를 암호화하고 해독합니다.

KMS는 제품을 StorageGRID에 설치하기 전이나 설치한 후에 그리드 관리자에서 설정할 수 있습니다. 자세한 내용은 StorageGRID 관리 지침의 KMS 및 어플라이언스 구성에 대한 정보를 참조하십시오.

- KMS가 어플라이언스를 설치하기 전에 설정된 경우 어플라이언스에서 노드 암호화를 사용하도록 설정하고 KMS가 구성된 StorageGRID 사이트에 추가하면 KMS 제어 암호화가 시작됩니다.
- KMS가 어플라이언스를 설치하기 전에 설정되지 않은 경우 KMS가 구성되고 어플라이언스 노드가 포함된 사이트에 대해 사용 가능한 즉시 노드 암호화가 활성화된 각 어플라이언스에 대해 KMS 제어 암호화가 수행됩니다.

> 노드 암호화가 활성화된 어플라이언스에서 KMS에 연결하기 전에 존재하는 데이터는 안전하지 않은 임시 키로 암호화됩니다. KMS에서 제공하는 값으로 키를 설정할 때까지 제품은 제거 또는 도난으로부터 보호되지 않습니다.

디스크 암호를 해독하는 데 필요한 KMS 키가 없으면 어플라이언스의 데이터를 검색할 수 없으며 효과적으로 손실됩니다. 이 경우 암호 해독 키를 KMS에서 검색할 수 없습니다. KMS 구성을 지우거나, KMS 키가 만료되거나, KMS에 대한 연결이 끊어지거나, KMS 키가 설치된 StorageGRID 시스템에서 어플라이언스를 제거하면 이 키에 액세스할 수 없습니다.

단계

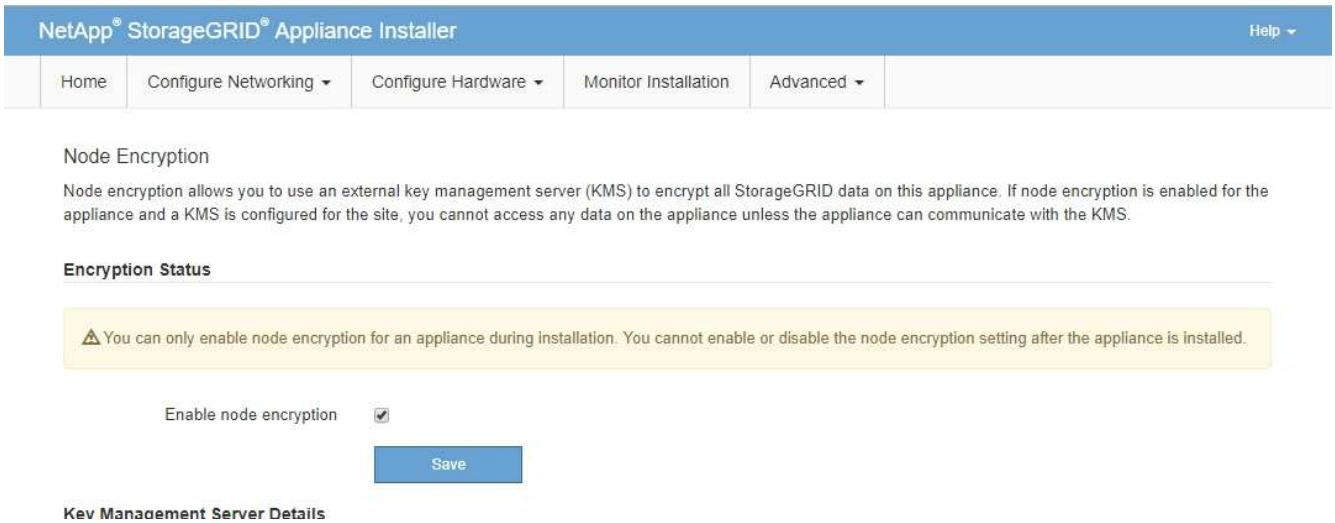
1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

   > KMS 키로 어플라이언스를 암호화한 후에는 동일한 KMS 키를 사용하지 않으면 어플라이언스 디스크를 해독할 수 없습니다.

2. 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.



3. 노드 암호화 사용 * 을 선택합니다.

   어플라이언스를 설치하기 전에 데이터 손실 위험 없이 * 노드 암호화 활성화 * 를 선택 취소할 수 있습니다. 설치가 시작되면 어플라이언스 노드가 StorageGRID 시스템의 KMS 암호화 키에 액세스하여 디스크 암호화를 시작합니다. 어플라이언스를 설치한 후에는 노드 암호화를 비활성화할 수 없습니다.

   > KMS가 있는 StorageGRID 사이트에 노드 암호화가 활성화된 어플라이언스를 추가한 후에는 해당 노드에 대해 KMS 암호화 사용을 중지할 수 없습니다.

4. 저장 * 을 선택합니다.
5. 어플라이언스를 StorageGRID 시스템에 노드로 구축하십시오.

   킬로미터 제어 암호화는 어플라이언스가 StorageGRID 사이트에 구성된 KMS 키에 액세스할 때 시작됩니다. KMS 암호화 프로세스 중에 설치 프로그램이 진행률 메시지를 표시합니다. 이 과정은 어플라이언스에 있는 디스크 볼륨 수에 따라 몇 분 정도 걸릴 수 있습니다.

   > 어플라이언스는 처음에 각 디스크 볼륨에 할당된 임의의 비 KMS 암호화 키로 구성됩니다. 이 디스크는 노드 암호화가 활성화된 어플라이언스가 StorageGRID 사이트에 구성된 KMS 키에 액세스할 때까지 안전하지 않은 임시 암호화 키를 사용하여 암호화됩니다.

작업을 마친 후

어플라이언스 노드가 유지보수 모드일 때 노드 암호화 상태, KMS 세부 정보 및 사용 중인 인증서를 볼 수 있습니다.

관련 정보

StorageGRID 관리

유지보수 모드에서 노드 암호화 모니터링(SG100 및 SG1000)

서비스 어플라이언스 노드를 배포합니다

서비스 어플라이언스를 기본 관리 노드, 비기본 관리 노드 또는 게이트웨이 노드로 배포할 수 있습니다. SG100과 SG1000 어플라이언스는 모두 게이트웨이 노드 및 관리 노드(운영 또는 비운영)로 동시에 작동할 수 있습니다.

서비스 어플라이언스를 기본 관리 노드로 배포합니다

서비스 어플라이언스를 기본 관리 노드로 배포할 때 어플라이언스에 포함된 StorageGRID 어플라이언스 설치 프로그램을 사용하여 StorageGRID 소프트웨어를 설치하거나 설치할 소프트웨어 버전을 업로드합니다. 다른 어플라이언스 노드 유형을 설치하기 전에 기본 관리 노드를 설치하고 구성해야 합니다. 기본 관리 노드는 그리드 네트워크와 선택적 관리 네트워크 및 클라이언트 네트워크(둘 중 하나 또는 둘 다 구성된 경우)에 연결할 수 있습니다.

필요한 것

- 이 제품은 랙 또는 캐비닛에 설치되었고 네트워크에 연결되어 있으며 전원이 켜져 있습니다.
- StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스에 대해 네트워크 링크, IP 주소 및 포트 재매핑(필요한 경우)이 구성되었습니다.

> 포트를 다시 매핑한 경우 동일한 포트를 사용하여 로드 밸런서 끝점을 구성할 수 없습니다. 다시 매핑된 포트를 사용하여 끝점을 만들 수 있지만 이러한 끝점은 로드 밸런서 서비스가 아닌 원래 CLB 포트 및 서비스에 다시 매핑됩니다. 의 단계를 따릅니다 포트 재맵을 제거합니다.

을 참조하십시오 로드 밸런싱 작동 방식 - CLB 서비스(더 이상 사용되지 않음) CLB 서비스에 대한 자세한 내용은 를 참조하십시오.

> CLB 서비스는 더 이상 사용되지 않습니다.

- 에 서비스 랩톱이 있습니다 지원되는 웹 브라우저.
- 어플라이언스에 할당된 IP 주소 중 하나를 알고 있습니다. 연결된 모든 StorageGRID 네트워크에 대해 IP 주소를 사용할 수 있습니다.

이 작업에 대해

어플라이언스 기본 관리 노드에 StorageGRID를 설치하려면 다음을 따르십시오.

- StorageGRID 어플라이언스 설치 프로그램을 사용하여 StorageGRID 소프트웨어를 설치합니다. 다른 버전의 소프트웨어를 설치하려면 먼저 StorageGRID 어플라이언스 설치 프로그램을 사용하여 업로드해야 합니다.
- 소프트웨어가 설치될 때까지 기다립니다.
- 소프트웨어가 설치되면 어플라이언스가 자동으로 재부팅됩니다.

단계

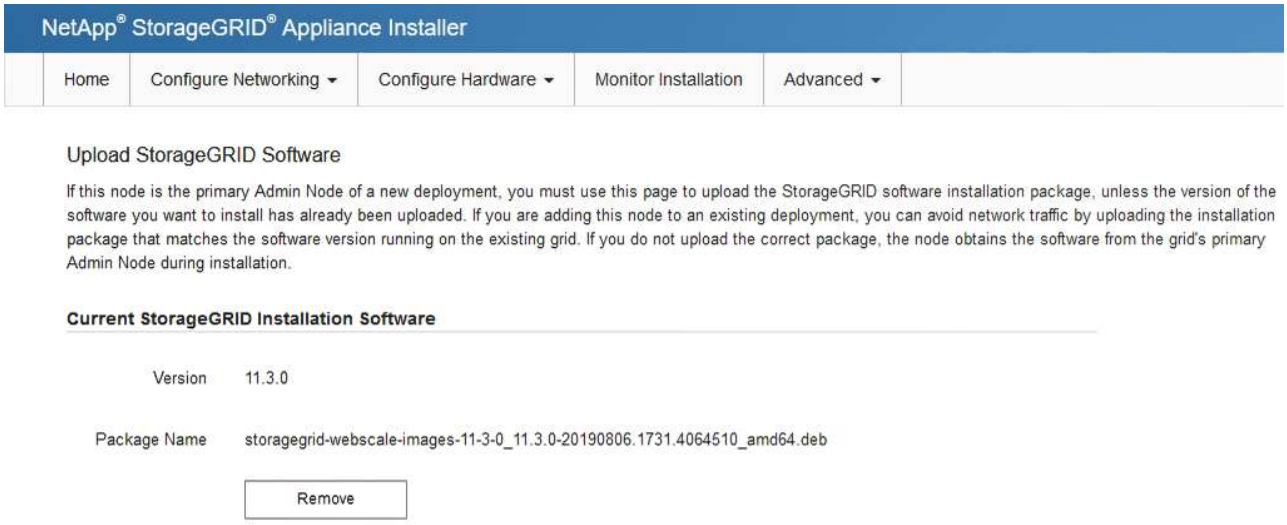
1. 브라우저를 열고 어플라이언스의 IP 주소를 입력합니다. (+) * https://*services_appliance_IP*:8443*`

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

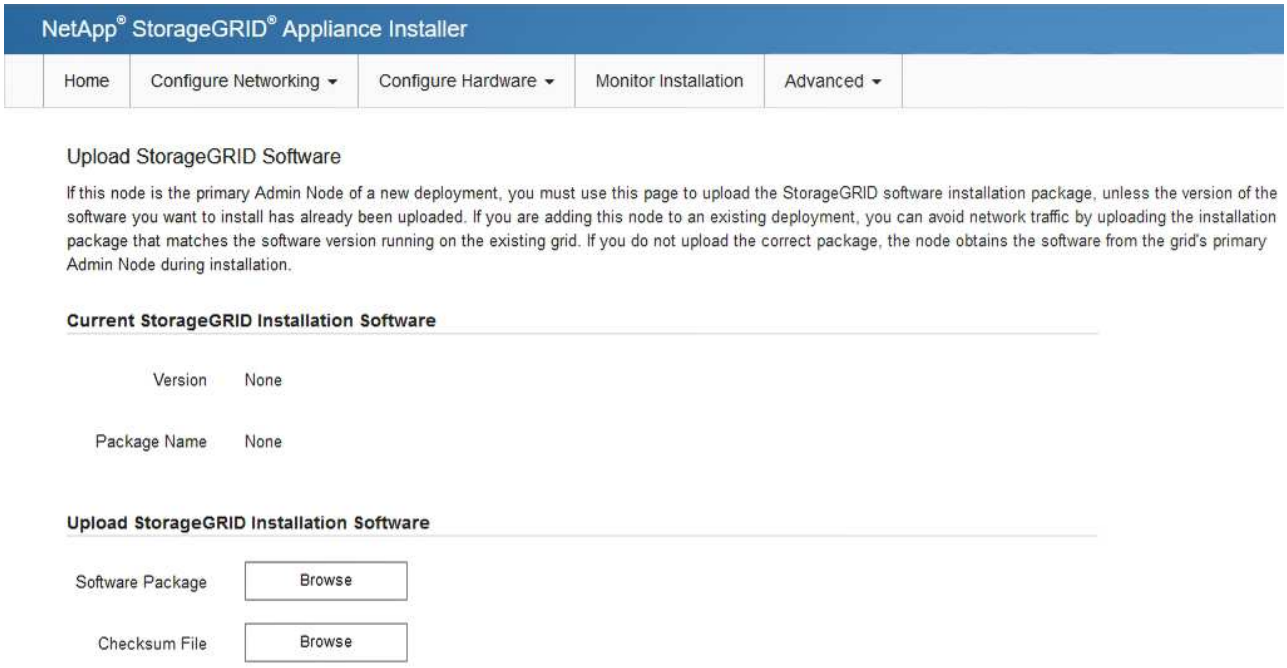
2. 이 노드 * 섹션에서 * 기본 관리자 * 를 선택합니다.
3. 노드 이름 * 필드에 이 어플라이언스 노드에 사용할 이름을 입력하고 * 저장 * 을 클릭합니다.

   노드 이름은 StorageGRID 시스템의 이 어플라이언스 노드에 할당됩니다. 그리드 관리자의 그리드 노드 페이지에 표시됩니다.

4. 필요에 따라 다른 버전의 StorageGRID 소프트웨어를 설치하려면 다음 단계를 수행하십시오.
   a. 설치 아카이브를 다운로드합니다.https://mysupport.netapp.com/site/products/all/details/storagegrid-appliance/downloads-tab["NetApp 다운로드: StorageGRID 어플라이언스"^].
   b. 아카이브를 추출합니다.
   c. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * StorageGRID 소프트웨어 업로드 * 를 선택합니다.
   d. 현재 소프트웨어 패키지를 제거하려면 * 제거 * 를 클릭합니다.



e. 다운로드하고 압축을 푼 소프트웨어 패키지를 * 찾아보기 * 를 클릭한 다음 * 찾아보기 * 를 클릭하여 체크섬 파일을 찾습니다.

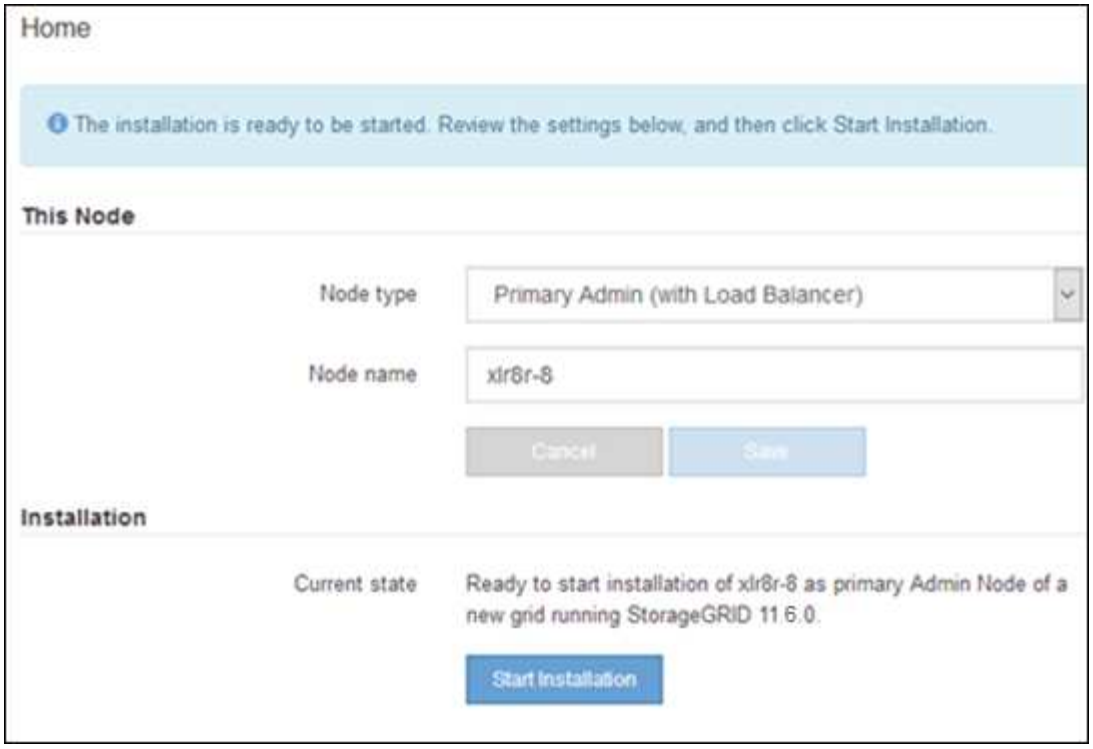


f. 홈 페이지로 돌아가려면 * 홈 * 을 선택합니다.

5. 현재 상태가 ""소프트웨어 버전 x.y로 기본 관리자 노드 이름 설치를 시작할 준비가 되었습니다""이고 * 설치 시작 * 버튼이 활성화되어 있는지 확인합니다.

> 노드 클론 생성 타겟으로 관리 노드 어플라이언스를 구축하는 경우 여기에서 구축 프로세스를 중지하고 에 따라 노드 클론 생성 절차를 계속하십시오 복구 및 유지 관리 지침.

6. StorageGRID 어플라이언스 설치 관리자 홈 페이지에서 * 설치 시작 * 을 클릭합니다.



현재 상태가 ""설치 진행 중""으로 변경되고 모니터 설치 페이지가 표시됩니다.

> 모니터 설치 페이지에 수동으로 액세스해야 하는 경우 메뉴 모음에서 * 모니터 설치 * 를 클릭합니다.

서비스 어플라이언스를 게이트웨이 또는 비기본 관리 노드로 배포합니다

서비스 어플라이언스를 게이트웨이 노드 또는 비 기본 관리 노드로 배포하는 경우 어플라이언스에 포함된 StorageGRID 어플라이언스 설치 프로그램을 사용합니다.

필요한 것

- 이 제품은 랙 또는 캐비닛에 설치되었고 네트워크에 연결되어 있으며 전원이 켜져 있습니다.
- StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스에 대해 네트워크 링크, IP 주소 및 포트 재매핑(필요한 경우)이 구성되었습니다.

> 포트를 다시 매핑한 경우 동일한 포트를 사용하여 로드 밸런서 끝점을 구성할 수 없습니다. 다시 매핑된 포트를 사용하여 끝점을 만들 수 있지만 이러한 끝점은 로드 밸런서 서비스가 아닌 원래 CLB 포트 및 서비스에 다시 매핑됩니다. 의 단계를 따릅니다 포트 재맵을 제거합니다.

> CLB 서비스는 더 이상 사용되지 않습니다.

- StorageGRID 시스템의 기본 관리 노드가 배포되었습니다.
- StorageGRID 어플라이언스 설치 프로그램의 IP 구성 페이지에 나열된 모든 그리드 네트워크 서브넷은 기본 관리 노드의 그리드 네트워크 서브넷 목록에 정의되어 있습니다.
- 에 서비스 랩톱이 있습니다 지원되는 웹 브라우저.
- 어플라이언스에 할당된 IP 주소를 알고 있습니다. 연결된 모든 StorageGRID 네트워크에 대해 IP 주소를 사용할 수 있습니다.

이 작업에 대해

서비스 어플라이언스 노드에 StorageGRID를 설치하려면 다음을 따르십시오.

- 기본 관리 노드의 IP 주소와 어플라이언스 노드의 이름을 지정하거나 확인합니다.
- 설치를 시작하고 소프트웨어가 설치될 때까지 기다립니다.

  어플라이언스 게이트웨이 노드 설치 작업을 중간에 중단하면 설치가 일시 중지됩니다. 설치를 다시 시작하려면 그리드 관리자에 로그인하고 모든 그리드 노드를 승인하고 StorageGRID 설치 프로세스를 완료합니다. 비 기본 관리자 노드 설치는 사용자의 승인이 필요하지 않습니다.

> SG100 및 SG1000 서비스 어플라이언스를 같은 사이트에 배포하지 마십시오. 성능을 예측할 수 없습니다.

> 한 번에 여러 어플라이언스 노드를 구축해야 하는 경우 'configure-sGA.py' 어플라이언스 설치 스크립트를 사용하여 설치 프로세스를 자동화할 수 있습니다. Appliance Installer를 사용하여 구성 정보가 포함된 JSON 파일을 업로드할 수도 있습니다. 을 참조하십시오 어플라이언스 설치 및 구성 자동화(SG100 및 SG1000) 설치 자동화에 대한 자세한 내용은 를 참조하십시오.

단계

1. 브라우저를 열고 어플라이언스의 IP 주소를 입력합니다.

   (* https://*Controller_IP*:8443*`)

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 기본 관리 노드 연결 섹션에서 기본 관리 노드의 IP 주소를 지정해야 하는지 여부를 확인합니다.

   이전에 이 데이터 센터에 다른 노드를 설치한 경우 StorageGRID 어플라이언스 설치 관리자는 기본 관리 노드 또는 admin_IP가 구성된 다른 그리드 노드가 동일한 서브넷에 있다고 가정하여 이 IP 주소를 자동으로 검색할 수 있습니다.

3. 이 IP 주소가 표시되지 않거나 변경해야 하는 경우 주소를 지정합니다.

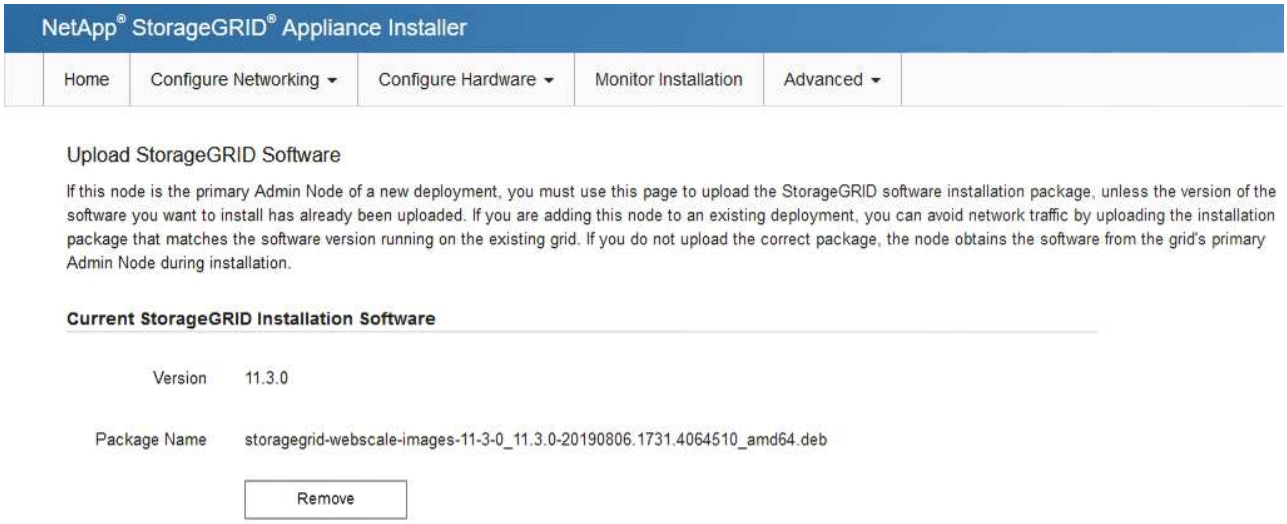
옵션을 선택합니다	설명
수동 IP 입력	a. 관리자 노드 검색 사용 * 확인란의 선택을 취소합니다. b. IP 주소를 수동으로 입력합니다. c. 저장 * 을 클릭합니다. d. 새 IP 주소가 준비될 때까지 연결 상태를 기다립니다.

옵션을 선택합니다	설명
연결된 모든 운영 관리 노드의 자동 검색	a. 관리자 노드 검색 사용 * 확인란을 선택합니다. b. 검색된 IP 주소 목록이 표시될 때까지 기다립니다. c. 이 어플라이언스 스토리지 노드를 구축할 그리드의 기본 관리 노드를 선택합니다. d. 저장 * 을 클릭합니다. e. 새 IP 주소가 준비될 때까지 연결 상태를 기다립니다.

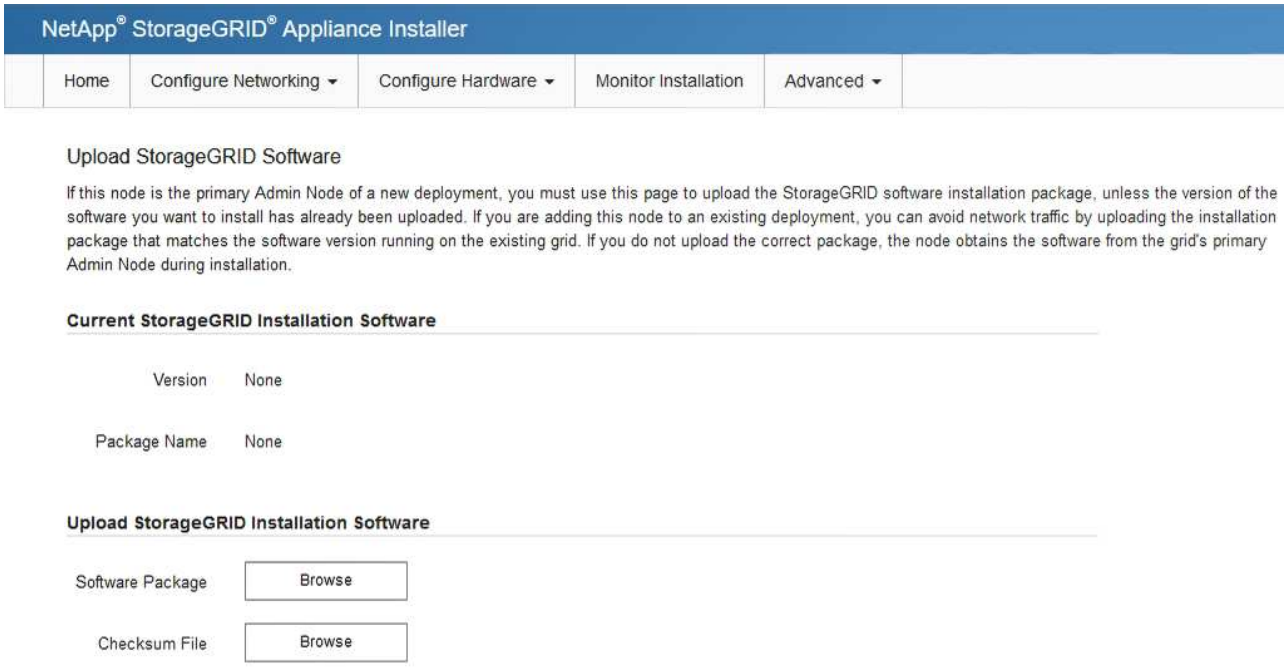
4. 노드 이름 * 필드에 이 어플라이언스 노드에 사용할 이름을 입력하고 * 저장 * 을 클릭합니다.

   노드 이름은 StorageGRID 시스템의 이 어플라이언스 노드에 할당됩니다. 그리드 관리자의 노드 페이지(개요 탭)에 표시됩니다. 필요한 경우 노드를 승인할 때 이름을 변경할 수 있습니다.

5. 필요에 따라 다른 버전의 StorageGRID 소프트웨어를 설치하려면 다음 단계를 수행하십시오.
   a. 설치 아카이브를 다운로드합니다.https://mysupport.netapp.com/site/products/all/details/storagegrid-appliance/downloads-tab["NetApp 다운로드: StorageGRID 어플라이언스"^].
   b. 아카이브를 추출합니다.
   c. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * StorageGRID 소프트웨어 업로드 * 를 선택합니다.
   d. 현재 소프트웨어 패키지를 제거하려면 * 제거 * 를 클릭합니다.



   e. 다운로드하고 압축을 푼 소프트웨어 패키지를 * 찾아보기 * 를 클릭한 다음 * 찾아보기 * 를 클릭하여 체크섬 파일을 찾습니다.

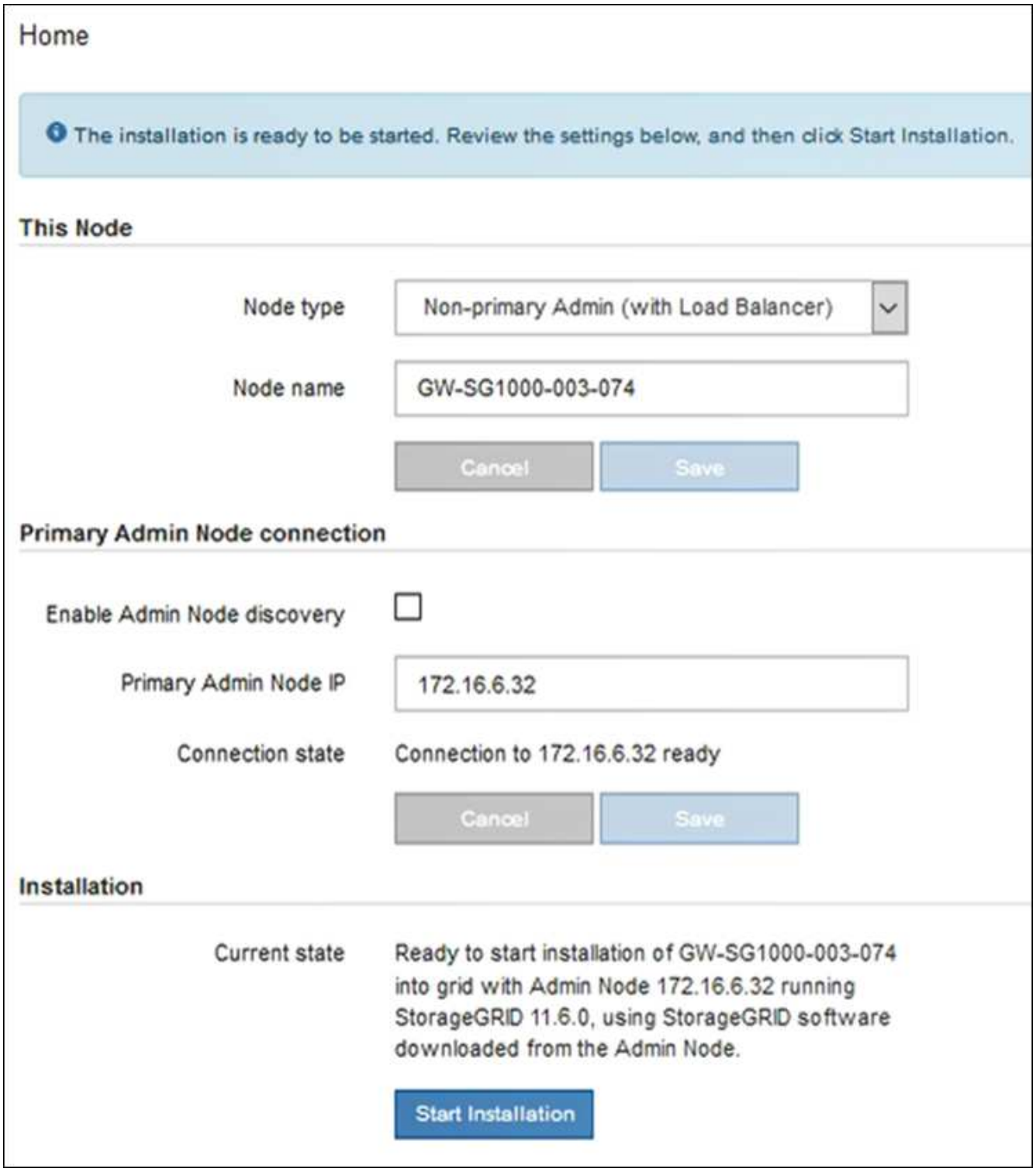


f. 홈 페이지로 돌아가려면 * 홈 * 을 선택합니다.

6. 설치 섹션에서 현재 상태가 기본 관리 노드 '*admin_ip*'을(를) 사용하는 그리드에 '*node name*'의 설치를 시작할 준비가 되었으며 * 설치 시작 * 버튼이 활성화되어 있는지 확인합니다.

   설치 시작 * 버튼이 활성화되지 않은 경우 네트워크 구성 또는 포트 설정을 변경해야 할 수 있습니다. 자세한 내용은 제품의 설치 및 유지보수 지침을 참조하십시오.

7. StorageGRID 어플라이언스 설치 관리자 홈 페이지에서 * 설치 시작 * 을 클릭합니다.



현재 상태가 ""설치 진행 중""으로 변경되고 모니터 설치 페이지가 표시됩니다.

> 모니터 설치 페이지에 수동으로 액세스해야 하는 경우 메뉴 모음에서 * 모니터 설치 * 를 클릭합니다.

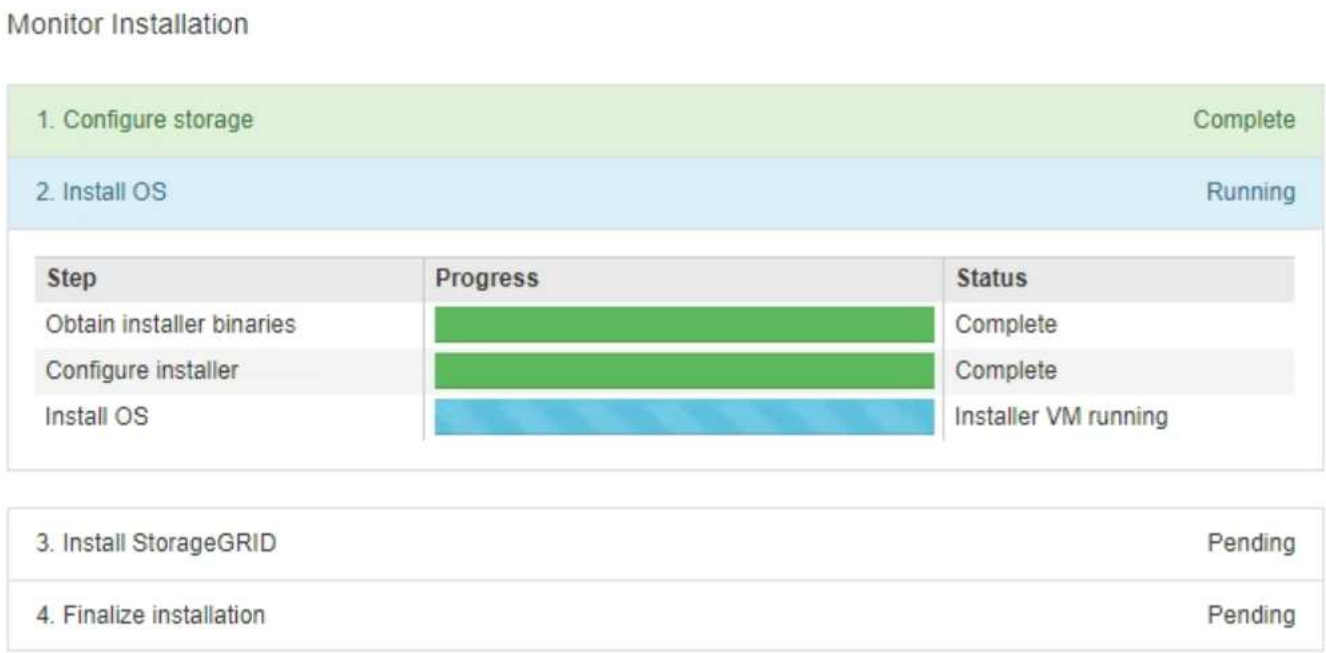
8. 그리드에 어플라이언스 노드가 여러 개 포함된 경우 각 어플라이언스에 대해 이전 단계를 반복합니다.

StorageGRID 어플라이언스 설치 프로그램은 설치가 완료될 때까지 상태를 제공합니다. 소프트웨어 설치가 완료되면 어플라이언스가 재부팅됩니다.

단계

1. 설치 진행률을 모니터링하려면 메뉴 표시줄에서 * 모니터 설치 * 를 클릭합니다.

   Monitor Installation(모니터 설치) 페이지에 설치 진행률이 표시됩니다.

   파란색 상태 표시줄은 현재 진행 중인 작업을 나타냅니다. 녹색 상태 표시줄은 성공적으로 완료된 작업을 나타냅니다.

   > 설치 프로그램은 이전 설치에서 완료된 작업이 다시 실행되지 않도록 합니다. 설치를 다시 실행할 경우 다시 실행할 필요가 없는 작업은 녹색 상태 표시줄과 "중단" 상태로 표시됩니다.

2. 처음 두 설치 단계의 진행 상황을 검토합니다.
   - * 1. 스토리지 구성 *

     이 단계에서 설치 프로그램은 어플라이언스의 드라이브에서 기존 구성을 지우고 호스트 설정을 구성합니다.

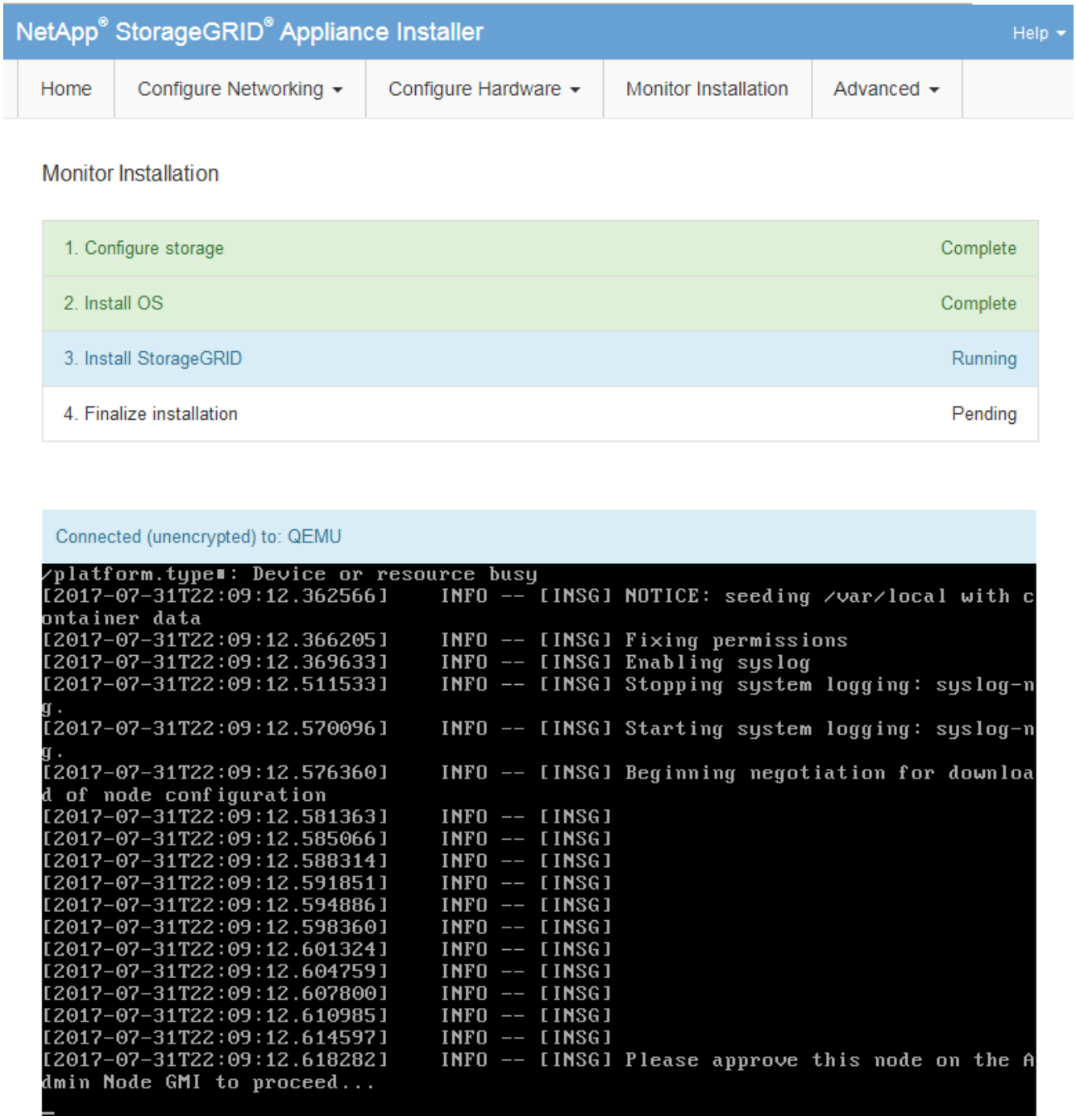
   - * 2. OS * 를 설치합니다

     이 단계에서 설치 프로그램은 StorageGRID의 기본 운영 체제 이미지를 어플라이언스에 복사합니다.

3. 다음 프로세스 중 하나가 발생할 때까지 설치 진행 상태를 계속 모니터링합니다.
   - 기본 관리 노드를 제외한 모든 어플라이언스 노드에 대해 StorageGRID 설치 단계가 일시 중지되고 그리드 관리자를 사용하여 관리 노드에서 이 노드를 승인하라는 메시지가 포함된 콘솔에 나타납니다. 다음 단계로 이동합니다.

- 어플라이언스 운영 관리자 노드 설치의 경우 노드를 승인할 필요가 없습니다. 어플라이언스가 재부팅됩니다. 다음 단계를 건너뛸 수 있습니다.

> 어플라이언스 기본 관리 노드를 설치하는 동안 다섯 번째 단계가 나타납니다(4단계를 보여주는 스크린샷 예 참조). 5단계가 10분 이상 진행 중인 경우 웹 페이지를 수동으로 새로 고칩니다.



4. 기본 관리 노드의 그리드 관리자로 이동하여 보류 중인 그리드 노드를 승인하고 StorageGRID 설치 프로세스를 완료합니다.

   Grid Manager에서 * Install * 을 클릭하면 단계 3이 완료되고 단계 4, * 설치 완료 * 가 시작됩니다. 4단계가 완료되면 어플라이언스가 재부팅됩니다.

어플라이언스 설치 및 구성 자동화(**SG100** 및 **SG1000**)

어플라이언스의 설치 및 구성과 전체 StorageGRID 시스템의 구성을 자동화할 수 있습니다.

이 작업에 대해

설치 및 구성 자동화는 여러 StorageGRID 인스턴스 또는 하나의 크고 복잡한 StorageGRID 인스턴스를 구축하는 데 유용할 수 있습니다.

설치 및 구성을 자동화하려면 다음 옵션 중 하나 이상을 사용하십시오.

- 어플라이언스의 구성 설정을 지정하는 JSON 파일을 생성합니다. StorageGRID 어플라이언스 설치 프로그램을 사용하여 JSON 파일을 업로드합니다.

  동일한 파일을 사용하여 여러 어플라이언스를 구성할 수 있습니다.

- StorageGRID ``configure-sGA.py'' Python 스크립트를 사용하여 어플라이언스 구성을 자동화합니다.
- 추가 Python 스크립트를 사용하여 전체 StorageGRID 시스템의 다른 구성 요소("그리드")를 구성합니다.

  StorageGRID 자동화 Python 스크립트를 직접 사용하거나 직접 개발한 그리드 구축 및 구성 도구에서 StorageGRID 설치 REST API를 사용하는 방법의 예로 사용할 수 있습니다. 의 지침을 참조하십시오 StorageGRID 설치 파일 다운로드 및 추출.

StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스 구성을 자동화합니다

구성 정보가 포함된 JSON 파일을 사용하여 어플라이언스 구성을 자동화할 수 있습니다. StorageGRID 어플라이언스 설치 프로그램을 사용하여 파일을 업로드합니다.

필요한 것

- 어플라이언스는 StorageGRID 11.5 이상과 호환되는 최신 펌웨어에 있어야 합니다.
- 를 사용하여 구성하는 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램에 연결되어 있어야 합니다 지원되는 웹 브라우저.

이 작업에 대해

다음과 같은 어플라이언스 구성 작업을 자동화할 수 있습니다.

- Grid Network, Admin Network 및 Client Network IP 주소입니다
- BMC 인터페이스
- 네트워크 링크
  - 포트 결합 모드
  - 네트워크 연결 모드
  - 링크 속도

업로드된 JSON 파일을 사용하여 어플라이언스를 구성하는 것이 StorageGRID 어플라이언스 설치 프로그램에서 여러 페이지를 사용하여 수동으로 구성하는 것보다 더 효율적인 경우가 많습니다. 특히 여러 노드를 구성해야 하는 경우 더욱 그렇습니다. 각 노드에 대해 한 번에 하나씩 구성 파일을 적용해야 합니다.

> 어플라이언스의 설치와 구성을 모두 자동화하려는 숙련된 사용자는 configure-sga.py 스크립트를 사용합니다.

단계

1. 다음 중 하나를 사용하여 JSON 파일을 생성합니다.
   - 를 클릭합니다 "ConfigBuilder 응용 프로그램".
   - 를 클릭합니다 configure-sga.py 어플라이언스 구성 스크립트. StorageGRID 어플라이언스 설치 프로그램(* 도움말** 어플라이언스 구성 스크립트*)에서 스크립트를 다운로드할 수 있습니다.

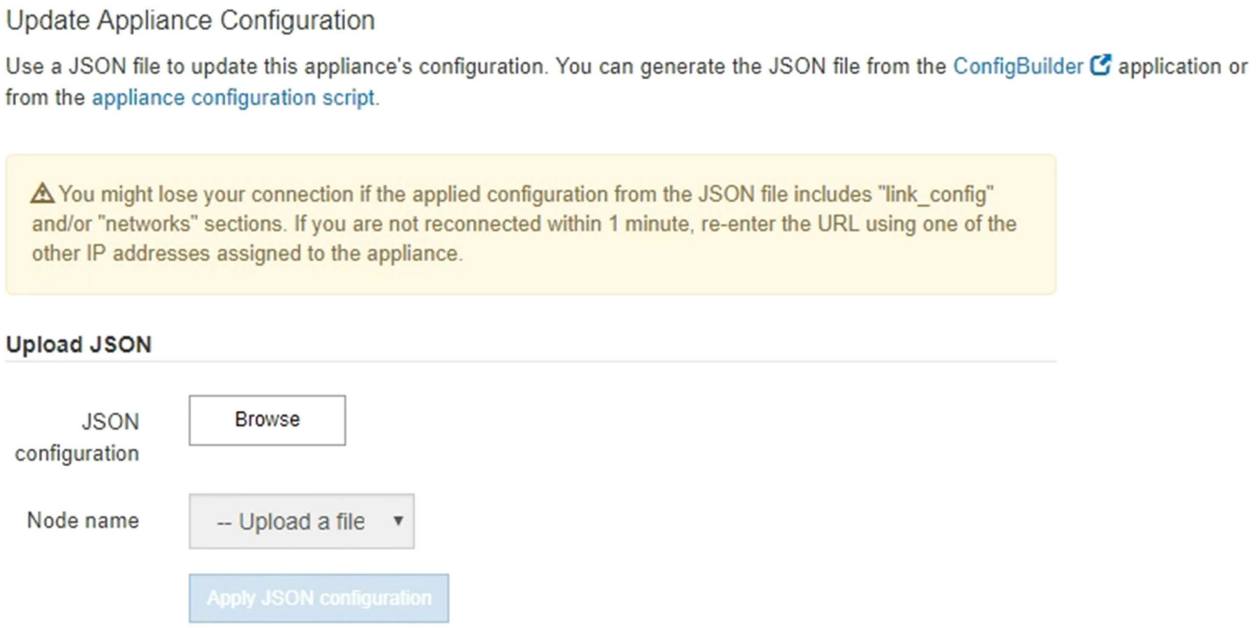
     JSON 파일의 노드 이름은 다음 요구사항을 충족해야 합니다.

     - 1자 이상 32자 이하의 유효한 호스트 이름이어야 합니다
     - 문자, 숫자 및 하이픈을 사용할 수 있습니다
     - 하이픈으로 시작하거나 끝날 수 없습니다
     - 숫자만 포함할 수 없습니다

     > JSON 파일의 노드 이름(최상위 이름)이 고유한지 확인하십시오. 그렇지 않으면 JSON 파일을 사용하여 둘 이상의 노드를 구성할 수 없습니다.

2. Advanced * > * Update Appliance Configuration * 을 선택합니다.

   어플라이언스 구성 업데이트 페이지가 나타납니다.

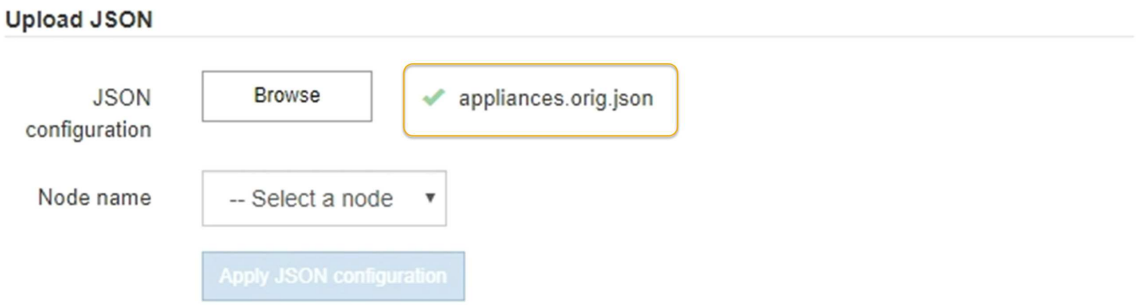


3. 업로드할 구성이 있는 JSON 파일을 선택합니다.
   a. 찾아보기 * 를 선택합니다.
   b. 파일을 찾아 선택합니다.

c. 열기 * 를 선택합니다.

파일이 업로드되고 검증됩니다. 유효성 검사 프로세스가 완료되면 녹색 확인 표시 옆에 파일 이름이 표시됩니다.

> JSON 파일의 구성에 "link_config", "networks" 또는 둘 다에 대한 섹션이 포함된 경우 어플라이언스에 대한 연결이 끊어질 수 있습니다. 1분 이내에 다시 연결되지 않으면 어플라이언스에 할당된 다른 IP 주소 중 하나를 사용하여 어플라이언스 URL을 다시 입력하십시오.

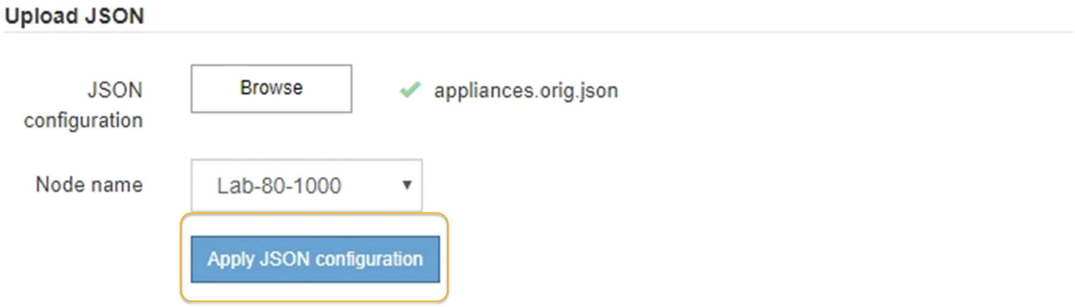


노드 이름 * 드롭다운은 JSON 파일에 정의된 최상위 노드 이름으로 채워집니다.

> 파일이 유효하지 않으면 파일 이름이 빨간색으로 표시되고 오류 메시지가 노란색 배너에 표시됩니다. 잘못된 파일이 어플라이언스에 적용되지 않습니다. ConfigBuilder를 사용하여 올바른 JSON 파일이 있는지 확인할 수 있습니다.

4. 노드 이름 * 드롭다운 목록에서 노드를 선택합니다.

   JSON 설정 적용 * 버튼이 활성화됩니다.



5. JSON 구성 적용 * 을 선택합니다.

   선택한 노드에 구성이 적용됩니다.

configure-sga.py 스크립트를 사용하여 어플라이언스 노드의 설치 및 구성을 자동화합니다

'configure-sGA.py' 스크립트를 사용하면 기본 관리 노드의 설치 및 구성을 포함하여 StorageGRID 어플라이언스 노드에 대한 많은 설치 및 구성 작업을 자동화할 수 있습니다. 이

스크립트는 구성할 어플라이언스가 많은 경우 유용할 수 있습니다. 또한 스크립트를 사용하여 어플라이언스 구성 정보가 포함된 JSON 파일을 생성할 수도 있습니다.

필요한 것

- 이 어플라이언스는 랙에 설치되어 있고 네트워크에 연결되어 있으며 전원이 켜져 있습니다.
- 네트워크 링크 및 IP 주소는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 기본 관리 노드에 대해 구성되었습니다.
- 기본 관리 노드를 설치하는 경우 해당 IP 주소를 알 수 있습니다.
- 다른 노드를 설치 및 구성하는 경우 기본 관리 노드가 배포되었으며 해당 IP 주소를 알고 있는 것입니다.
- 기본 관리 노드 이외의 모든 노드의 경우 StorageGRID 어플라이언스 설치 프로그램의 IP 구성 페이지에 나열된 모든 그리드 네트워크 서브넷이 기본 관리 노드의 그리드 네트워크 서브넷 목록에 정의되어 있습니다.
- 'configure-sGA.py' 파일을 다운로드했습니다. 이 파일은 설치 아카이브에 포함되어 있거나 StorageGRID 어플라이언스 설치 프로그램에서 * 도움말 * > * 어플라이언스 설치 스크립트 * 를 클릭하여 액세스할 수 있습니다.

> 이 절차는 명령줄 인터페이스를 사용하는 일부 경험이 있는 고급 사용자를 위한 것입니다. 또는 을(를) 사용할 수 있습니다 StorageGRID 어플라이언스 설치 프로그램을 사용하여 구성을 자동화합니다.

단계

1. Python 스크립트를 실행하기 위해 사용 중인 Linux 시스템에 로그인합니다.
2. 스크립트 구문에 대한 일반적인 도움말과 사용 가능한 매개 변수 목록을 보려면 다음을 입력합니다.

   ```
   configure-sga.py --help
   ```

   'configure-sGA.py' 스크립트는 5개의 하위 명령을 사용합니다.

   - BMC 구성 및 어플라이언스의 현재 구성이 포함된 JSON 파일을 생성하는 등 고급 StorageGRID 어플라이언스 상호 작용을 위한 '고급' 기능입니다
   - RAID 모드, 노드 이름 및 네트워킹 매개 변수를 구성하기 위한 'configure'
   - StorageGRID 설치 시작을 위한 '설치'입니다
   - StorageGRID 설치 모니터링을 위한 모니터
   - 어플라이언스를 재부팅하기 위한 재부팅

     하위 명령(advanced, configure, install, monitor, reboot) 인수 뒤에 '--help' 옵션을 입력하면 해당 하위 명령 내에서 사용할 수 있는 옵션에 대한 자세한 내용을 제공하는 다른 도움말 텍스트가 표시됩니다. + "configure-sga.py_subcommand_—help

3. 어플라이언스 노드의 현재 구성을 확인하려면 다음과 같이 입력합니다. 여기서 "*SGA-INSTALL-IP*"는 어플라이언스 노드의 IP 주소 중 하나입니다. + "configure-sga.py configure_sGA-install-ip_

   이 결과는 기본 관리 노드의 IP 주소와 관리, 그리드 및 클라이언트 네트워크에 대한 정보를 포함하여 어플라이언스에 대한 현재 IP 정보를 표시합니다.

   ```
   Connecting to +https://10.224.2.30:8443+ (Checking version and
   ```

```
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200

  StorageGRID Appliance
    Name:        LAB-SGA-2-30
    Node type:   storage

  StorageGRID primary Admin Node
    IP:        172.16.1.170
    State:     unknown
    Message:   Initializing...
    Version:   Unknown

  Network Link Configuration
    Link Status
          Link      State      Speed (Gbps)
          ----      -----      -----
          1         Up         10
          2         Up         10
          3         Up         10
          4         Up         10
          5         Up         1
          6         Down       N/A

    Link Settings
        Port bond mode:      FIXED
        Link speed:          10GBE

        Grid Network:        ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

        Admin Network:       ENABLED
            Bonding mode:    no-bond
            MAC Addresses:   00:80:e5:29:70:f4
```

```
        Client Network:      ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

  Grid Network
    CIDR:      172.16.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:8A
    Gateway:   172.16.0.1
    Subnets:   172.17.0.0/21
               172.18.0.0/21
               192.168.0.0/21
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

#################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#################################################################
```

4. 현재 설정의 값을 변경해야 하는 경우 '설정' 하위 명령을 사용하여 값을 업데이트합니다. 예를 들어, 어플라이언스가 기본 관리 노드에 연결하기 위해 사용하는 IP 주소를 ' 172.16.2.99 '로 변경하려면 + ' configure-sga.py configure - -admin -ip 172.16.2.99_sga -install -ip_'를 입력합니다
5. 어플라이언스 구성을 JSON 파일로 백업하려면 고급 및 'backup-file' 하위 명령을 사용하십시오. 예를 들어, IP 주소 '*SGA-INSTALL-IP*'를 사용하는 어플라이언스 구성을 어플라이언스-SG1000.json'이라는 파일에 백업하려면 + "configure-sga.py advanced—backup-file appliance-SG1000.json_sga-install-ip_"를 입력합니다

   구성 정보가 포함된 JSON 파일은 에서 스크립트를 실행한 디렉토리에 작성됩니다.

   > 생성된 JSON 파일의 최상위 노드 이름이 어플라이언스 이름과 일치하는지 확인하십시오. 숙련된 사용자이고 StorageGRID API에 대한 철저한 이해가 없는 경우 이 파일을 변경하지 마십시오.

6. 어플라이언스 구성이 만족스러우면 "install" 및 "monitor" 하위 명령을 사용하여 어플라이언스를 설치합니다. + "configure-sga.py install—monitor_sga-install-ip_"
7. 어플라이언스를 재부팅하려면 + "configure-sga.py reboot_sga-install-ip_"를 입력합니다

StorageGRID 구성 자동화

그리드 노드를 구축한 후 StorageGRID 시스템 구성을 자동화할 수 있습니다.

필요한 것

- 설치 아카이브에서 다음 파일의 위치를 알고 있습니다.

파일 이름	설명
configure-storagegrid.py	구성을 자동화하는 데 사용되는 Python 스크립트입니다
configure -StorageGrid.sample.json	스크립트와 함께 사용할 샘플 구성 파일
configure -StorageGrid.blank.json을 지정합니다	스크립트에 사용할 빈 구성 파일입니다

- "configure-StorageGrid.json" 구성 파일을 만들었습니다. 이 파일을 만들려면 샘플 구성 파일('configure-StorageGrid.sample.json') 또는 빈 구성 파일('configure-StorageGrid.blank.json')을 수정할 수 있습니다.

이 작업에 대해

configure-StorageGrid.py Python 스크립트와 configure-StorageGrid.json 구성 파일을 사용하여 StorageGRID 시스템 구성을 자동화할 수 있습니다.

> 를 사용하여 시스템을 구성할 수도 있습니다 그리드 관리자 또는 을 누릅니다 설치 API.

단계

1. Python 스크립트를 실행하기 위해 사용 중인 Linux 시스템에 로그인합니다.
2. 설치 아카이브를 추출한 디렉토리로 변경합니다.

   예: + 'cd StorageGRID-Webscale -*version/platform*

   여기서, 'platform'은 'dEBS', 'rpms', 'vSphere'입니다.

3. Python 스크립트를 실행하고 생성한 구성 파일을 사용합니다.

   예를 들면 다음과 같습니다.

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

작업을 마친 후

복구 패키지 '.zip' 파일은 구성 프로세스 중에 생성되며 설치 및 구성 프로세스를 실행 중인 디렉토리에 다운로드됩니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 백업해야 합니다. 예를 들어, 안전한 백업 네트워크 위치 및 안전한 클라우드 저장소 위치에 복사합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

임의 암호를 생성해야 한다고 지정한 경우 "passwords.txt" 파일을 추출하고 StorageGRID 시스템에 액세스하는 데 필요한 암호를 찾아야 합니다.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

확인 메시지가 표시되면 StorageGRID 시스템이 설치 및 구성됩니다.

```
StorageGRID has been configured and installed.
```

REST API 설치 개요

StorageGRID는 설치 작업을 수행하기 위한 두 가지 REST API, 즉 StorageGRID 설치 API와 StorageGRID 어플라이언스 설치 관리자 API를 제공합니다.

두 API 모두 Swagger 오픈 소스 API 플랫폼을 사용하여 API 문서를 제공합니다. swagger를 사용하면 개발자와 개발자가 아닌 사용자가 API가 매개 변수 및 옵션에 어떻게 응답하는지 보여주는 사용자 인터페이스에서 API와 상호 작용할 수 있습니다. 이 문서에서는 표준 웹 기술 및 JSON(JavaScript Object Notation) 데이터 형식에 대해 잘 알고 있다고 가정합니다.

> API Docs 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

각 REST API 명령에는 API의 URL, HTTP 작업, 필수 또는 선택적 URL 매개 변수, 그리고 예상되는 API 응답이 포함됩니다.

StorageGRID 설치 API

StorageGRID 설치 API는 StorageGRID 시스템을 처음 구성할 때와 기본 관리자 노드 복구를 수행해야 하는 경우에만 사용할 수 있습니다. 설치 API는 Grid Manager에서 HTTPS를 통해 액세스할 수 있습니다.

API 설명서에 액세스하려면 기본 관리 노드의 설치 웹 페이지로 이동하여 메뉴 모음에서 * 도움말 * > * API 설명서 * 를 선택합니다.

StorageGRID 설치 API에는 다음 섹션이 포함되어 있습니다.

- * config * — 제품 릴리스 및 API 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 API의 주요 버전을 나열할 수 있습니다.
- * 그리드 * — 그리드 레벨 구성 작업. 그리드 세부 정보, 그리드 네트워크 서브넷, 그리드 암호, NTP 및 DNS 서버 IP 주소를 포함한 그리드 설정을 얻고 업데이트할 수 있습니다.

- * 노드 * — 노드 레벨 구성 작업 그리드 노드 목록을 검색하고, 그리드 노드를 삭제하고, 그리드 노드를 구성하고, 그리드 노드를 보고, 그리드 노드의 구성을 재설정할 수 있습니다.
- * 프로비저닝 * — 프로비저닝 작업. 프로비저닝 작업을 시작하고 프로비저닝 작업의 상태를 볼 수 있습니다.
- * 복구 * — 기본 관리 노드 복구 작업 정보를 재설정하고, 복구 패키지를 업로드하고, 복구를 시작하고, 복구 작업의 상태를 볼 수 있습니다.
- * recovery-package * — 복구 패키지를 다운로드하기 위한 작업.
- * 사이트 * — 사이트 수준 구성 작업 사이트를 만들고, 보고, 삭제하고, 수정할 수 있습니다.

StorageGRID 어플라이언스 설치 관리자 **API**입니다

StorageGRID 어플라이언스 설치 프로그램 API는 HTTPS를 통해 '*Controller_IP*:8443'에서 액세스할 수 있습니다.

API 설명서에 액세스하려면 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램으로 이동하여 메뉴 모음에서 * 도움말 * > * API Docs * 를 선택합니다.

StorageGRID 어플라이언스 설치 관리자 API에는 다음 섹션이 포함되어 있습니다.

- * 클론 * — 노드 클로닝을 구성하고 제어하는 작업.
- * 암호화 * — 암호화를 관리하고 암호화 상태를 확인하는 작업.
- * 하드웨어 구성 * — 연결된 하드웨어에서 시스템 설정을 구성하는 작업.
- * 설치 * — 어플라이언스 설치 시작 및 설치 상태 모니터링을 위한 작업.
- * 네트워킹 * — StorageGRID 어플라이언스 및 어플라이언스 포트 설정에 대한 그리드, 관리자 및 클라이언트 네트워크 구성과 관련된 작업.
- * setup * — 시스템에 대한 정보를 얻고 기본 관리 노드 IP를 업데이트하는 요청을 포함하여 초기 어플라이언스 설치 설정에 도움이 되는 작업.
- * 지원 * — 컨트롤러 재부팅 및 로그 가져오기에 대한 운영
- * 업그레이드 * — 어플라이언스 펌웨어 업그레이드와 관련된 작업.
- * 업로그램 * — StorageGRID 설치 파일을 업로드하는 작업.

하드웨어 설치 문제 해결(**SG100** 및 **SG1000**)

설치 중에 문제가 발생하는 경우 하드웨어 설정 및 연결 문제와 관련된 문제 해결 정보를 검토하는 것이 도움이 될 수 있습니다.

어플라이언스의 부팅 코드를 봅니다

장치에 전원을 공급하면 BMC가 일련의 부팅 코드를 기록합니다. BMC 관리 포트에 연결된 그래픽 콘솔에서 이러한 코드를 볼 수 있습니다.

필요한 것

- BMC 대시보드에 액세스하는 방법을 알고 있습니다.
- SOL(Serial-over-LAN)을 사용하려는 경우 IPMI SOL 콘솔 애플리케이션을 사용하는 경험이 있습니다.

단계

1. 어플라이언스 컨트롤러의 부팅 코드를 보려면 다음 방법 중 하나를 선택하고 필요한 장비를 수집합니다.

방법	필수 장비
VGA 콘솔	• VGA 지원 모니터 • VGA 케이블
KVM	• RJ-45 케이블
직렬 포트	• DB-9 직렬 케이블 • 가상 직렬 터미널
솔	• 가상 직렬 터미널

2. VGA 콘솔을 사용하는 경우 다음 단계를 수행하십시오.
   a. VGA 지원 모니터를 제품 뒷면의 VGA 포트에 연결합니다.
   b. 모니터에 표시된 코드를 봅니다.
3. BMC KVM을 사용하는 경우 다음 단계를 수행하십시오.
   a. BMC 관리 포트에 연결하고 BMC 웹 인터페이스에 로그인합니다.
   b. 리모컨 * 을 선택합니다.
   c. KVM을 실행합니다.
   d. 가상 모니터에서 코드를 봅니다.
4. 직렬 포트 및 터미널을 사용하는 경우 다음 단계를 수행하십시오.
   a. 어플라이언스 뒷면의 DB-9 직렬 포트에 연결합니다.
   b. '115200 8-N-1' 설정을 사용합니다.
   c. 직렬 터미널에 인쇄된 코드를 봅니다.
5. SOL을 사용하는 경우 다음 단계를 수행하십시오.
   a. BMC IP 주소 및 로그인 자격 증명을 사용하여 IPMI SOL에 연결합니다.

      BMC 루트 계정 암호를 변경하지 않은 경우 공장 출하시 기본값은 "calvin"일 수 있습니다.

      'ipmitool-i lanplus-H_BMC_Port_IP_-U root-P_Password_SOL activate

   b. 가상 시리얼 터미널에서 코드를 봅니다.
6. 표를 사용하여 제품의 코드를 찾습니다.

코드	를 나타냅니다
안녕	마스터 부트 스크립트가 시작되었습니다.

코드	를 나타냅니다
HP	시스템에서 네트워크 인터페이스 카드(NIC) 펌웨어를 업데이트해야 하는지 확인합니다.
RB	펌웨어 업데이트를 적용한 후 시스템이 재부팅되고 있습니다.
FP	하드웨어 하위 시스템 펌웨어 업데이트 검사가 완료되었습니다. 컨트롤러 간 통신 서비스가 시작됩니다.
HC	시스템에서 기존 StorageGRID 설치 데이터를 확인하고 있습니다.
호	StorageGRID 어플라이언스가 실행 중입니다.
HA	StorageGRID가 실행 중입니다.

관련 정보

BMC 인터페이스에 액세스합니다

어플라이언스에 대한 오류 코드를 봅니다

어플라이언스를 부팅할 때 하드웨어 오류가 발생하면 BMC가 오류 코드를 기록합니다. 필요한 경우 BMC 인터페이스를 사용하여 이러한 오류 코드를 확인한 다음 기술 지원 팀과 협력하여 문제를 해결할 수 있습니다.

필요한 것

- BMC 대시보드에 액세스하는 방법을 알고 있습니다.

단계

1. BMC 대시보드에서 * BIOS POST 코드 * 를 선택합니다.
2. 현재 코드 및 이전 코드에 대해 표시된 정보를 검토합니다.

   다음 오류 코드 중 하나가 표시되면 기술 지원 부서의 도움을 받고 문제를 해결하십시오.

코드	를 나타냅니다
0x0E	마이크로코드를 찾을 수 없습니다
0x0F	마이크로코드가 로드되지 않았습니다
0x50	메모리 초기화 오류. 잘못된 메모리 유형 또는 호환되지 않는 메모리 속도입니다.

코드	를 나타냅니다
0x51	메모리 초기화 오류. SPD 판독에 실패했습니다.
0x52	메모리 초기화 오류. 잘못된 메모리 크기 또는 메모리 모듈이 일치하지 않습니다.
0x53	메모리 초기화 오류. 사용 가능한 메모리가 없습니다.
0x54	지정되지 않은 메모리 초기화 오류입니다
0x55	메모리가 설치되지 않았습니다
0x56	잘못된 CPU 유형 또는 속도입니다
0x57	CPU가 일치하지 않습니다
0x58	CPU 자체 테스트에 실패했거나 CPU 캐시 오류가 발생했을 수 있습니다
0x59	CPU 마이크로 코드를 찾을 수 없거나 마이크로 코드를 업데이트하지 못했습니다
0x5A	내부 CPU 오류입니다
0x5B	PPI 재설정을 사용할 수 없습니다
0x5C	PEI 단계 BMC 자체 테스트에 실패했습니다
0xD0	CPU 초기화 오류
0xD1	노스 브리지 초기화 오류
0xD2	South bridge 초기화 오류
3	일부 아키텍처 프로토콜은 사용할 수 없습니다
0xD4	PCI 리소스 할당 오류입니다. 리소스 부족.
0xD5	레거시 옵션 ROM에 대한 공간이 없습니다
0xD6	콘솔 출력 장치를 찾을 수 없습니다

코드	를 나타냅니다
0xD7	콘솔 입력 장치를 찾을 수 없습니다
0xD8	잘못된 암호입니다
0xD9	부팅 옵션 로드 중 오류 발생(LoadImage가 오류를 반환함)
0xDA	부팅 옵션 실패(StartImage가 오류를 반환함)
0xDB입니다	플래시를 업데이트하지 못했습니다
0xDC	재설정 프로토콜을 사용할 수 없습니다
0xDD	DXE 단계 BMC 자체 테스트 실패
0xE8	MRC:ERR_NO_MEMORY
0xE9	MRC:ERR_LT_LOCK
0xEA	MRC:ERR_DDR_INIT
0xEB	MRC:ERR_MEM_TEST
0xEC	MRC:ERR_VENDOR_VENDOR_VENCE
0XED	MRC:ERR_DIMM_COMPAT
0xEE	MRC:ERR_MRC_compatibility
0xEF	MRC:ERR_MRC_struct
0xF0	MRC:ERR_SET_VDD
0xF1	MRC:ERR_IOT_MEM_BUFFER
0xF2	MRC:ERR_RC_INTERNAL입니다
0xF3	MRC:ERR_INVALID_REG_ACCESS
0xF4	MRC:ERR_SET_MC_Freq
0xF5	MRC:ERR_READ_MC_Freq

코드	를 나타냅니다
0x70	MRC:ERR_DIMM_CHANNEL
0x74	MRC:ERR_BIST_CHECK
0xF6	MRC:ERR_SMBus를 선택합니다
0xF7	MRC:ERR_PCU
0xF8	MRC:ERR_NGN
0xF9	MRC:ERR_interLeave_failure

하드웨어 설치가 중단된 것 같습니다**(SG100** 및 **SG1000).**

하드웨어 장애 또는 케이블 연결 오류로 인해 어플라이언스가 부팅 프로세스를 완료하지 못하는 경우 StorageGRID 어플라이언스 설치 프로그램을 사용할 수 없습니다.

단계

1. 어플라이언스의 LED와 BMC에 표시되는 부팅 및 오류 코드를 검토합니다.
2. 문제 해결에 도움이 필요한 경우 기술 지원 부서에 문의하십시오.

관련 정보

어플라이언스의 부팅 코드를 봅니다

어플라이언스에 대한 오류 코드를 봅니다

연결 문제 해결**(SG100** 및 **SG1000)**

StorageGRID 어플라이언스 설치 중에 연결 문제가 발생하면 나열된 수정 조치 단계를 수행해야 합니다.

어플라이언스에 연결할 수 없습니다

서비스 어플라이언스에 연결할 수 없는 경우 네트워크 문제가 있거나 하드웨어 설치가 성공적으로 완료되지 않았을 수 있습니다.

단계

1. 어플라이언스의 IP 주소를 사용하여 + " * ping_services_appliance_ip_ * "를 사용하여 어플라이언스에 ping을 시도해 보십시오
2. Ping에서 응답이 없는 경우 올바른 IP 주소를 사용하고 있는지 확인합니다.

   그리드 네트워크, 관리 네트워크 또는 클라이언트 네트워크에서 어플라이언스의 IP 주소를 사용할 수 있습니다.

3. IP 주소가 올바른 경우 어플라이언스 케이블 연결, QSFP 또는 SFP 트랜시버 및 네트워크 설정을 확인하십시오.

4. 어플라이언스에 물리적으로 액세스할 수 있는 경우 영구 링크 로컬 IP "169.254.0.1"에 직접 연결하여 컨트롤러 네트워킹 구성을 확인하고 필요한 경우 업데이트할 수 있습니다. 자세한 지침은 의 2단계를 참조하십시오 StorageGRID 어플라이언스 설치 프로그램에 액세스합니다.

   그래도 문제가 해결되지 않으면 기술 지원 부서에 문의하십시오.

5. Ping에 성공하면 웹 브라우저를 엽니다.
6. StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. +
   `https://appliances_controller_IP:8443*`

   홈 페이지가 나타납니다.

StorageGRID 어플라이언스 설치 프로그램이 실행 중인 동안 서비스 어플라이언스를 재부팅합니다

StorageGRID 어플라이언스 설치 프로그램이 실행되는 동안 서비스 어플라이언스를 재부팅해야 할 수 있습니다. 예를 들어, 설치에 실패하면 서비스 어플라이언스를 재부팅해야 할 수 있습니다.

이 작업에 대해

이 절차는 서비스 어플라이언스가 StorageGRID 어플라이언스 설치 프로그램을 실행하는 경우에만 적용됩니다. 설치가 완료되면 StorageGRID 어플라이언스 설치 프로그램을 더 이상 사용할 수 없기 때문에 이 단계가 더 이상 작동하지 않습니다.

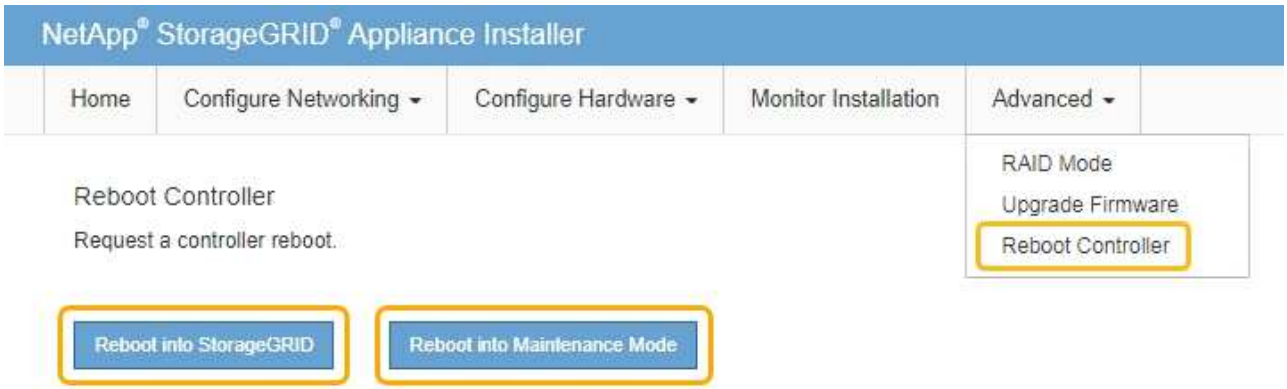
단계

1. StorageGRID 어플라이언스 설치 프로그램의 메뉴 모음에서 * 고급 * > * 컨트롤러 재부팅 * 을 클릭합니다.

   컨트롤러 재부팅 페이지가 나타납니다.

2. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 클릭한 후 다음 옵션 중 하나를 선택합니다.

   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



서비스 어플라이언스가 재부팅됩니다.

제품을 유지보수하십시오

제품에 대한 유지보수 절차를 수행해야 할 수 있습니다. 이 섹션의 절차에서는 어플라이언스가 이미 게이트웨이 노드 또는 StorageGRID 시스템의 관리 노드로 구축되었다고 가정합니다.

제품을 유지보수 모드로 전환합니다

특정 유지보수 절차를 수행하기 전에 제품을 유지보수 모드로 전환해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

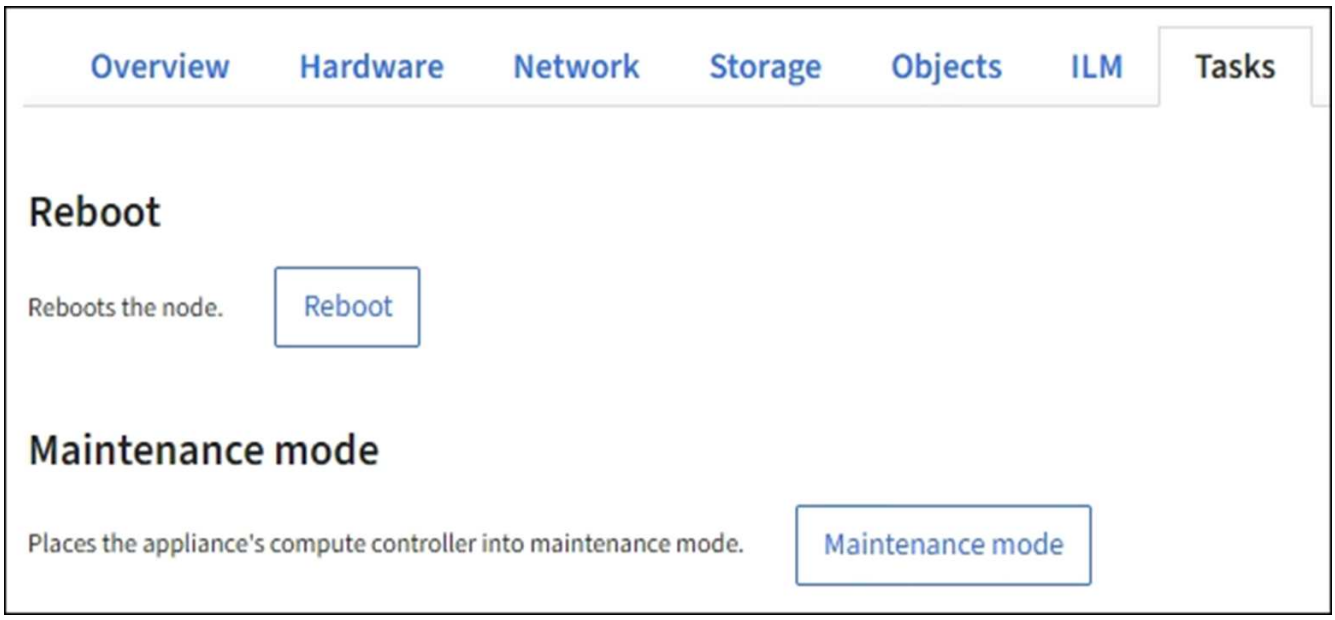
이 작업에 대해

StorageGRID 어플라이언스를 유지보수 모드로 전환하면 원격 액세스가 불가능한 경우가 드물게 있습니다.

> 유지보수 모드에서 StorageGRID 어플라이언스에 대한 admin 계정 암호 및 SSH 호스트 키는 어플라이언스가 서비스 중일 때와 동일하게 유지됩니다.

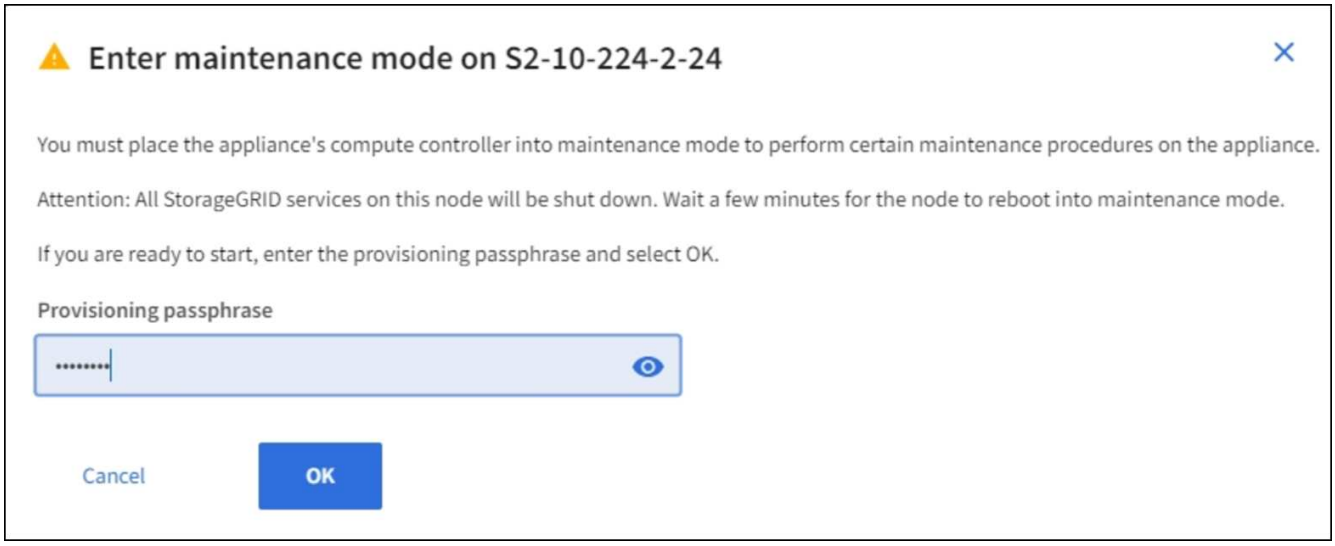
단계

1. Grid Manager에서 * nodes * 를 선택합니다.
2. 노드 페이지의 트리 뷰에서 어플라이언스 스토리지 노드를 선택합니다.
3. 작업 * 탭을 선택합니다.



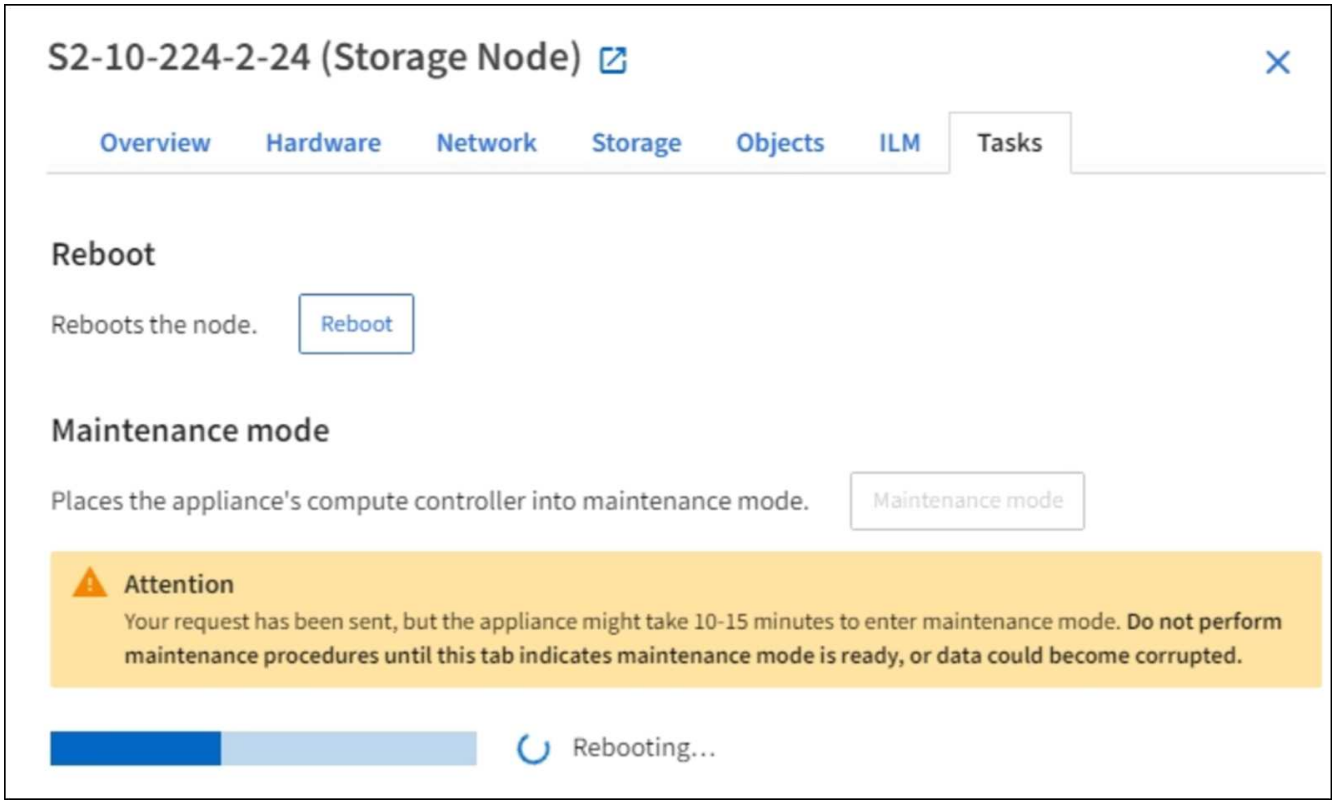
4. 유지보수 모드 * 를 선택합니다.

   확인 대화 상자가 나타납니다.

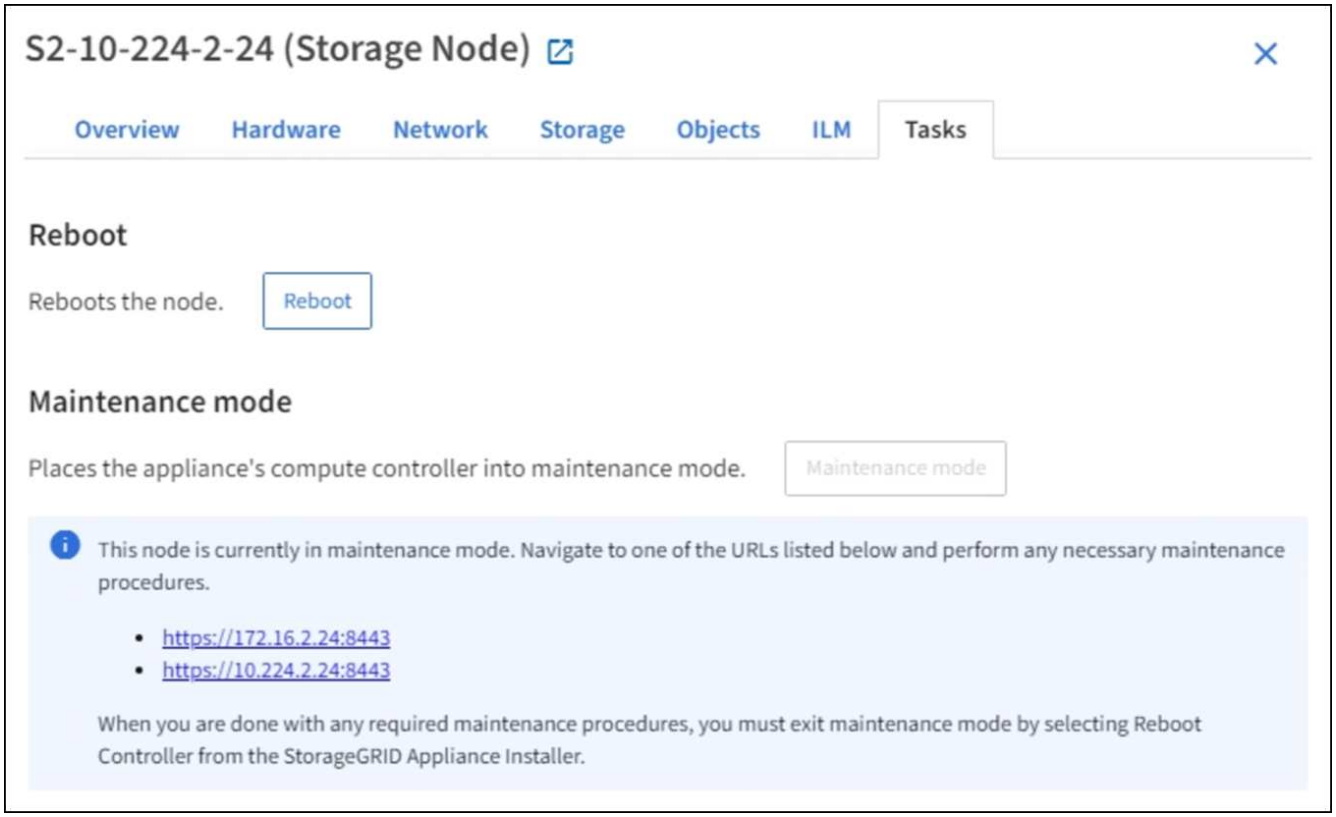


5. 프로비저닝 암호를 입력하고 * OK * 를 선택합니다.

   진행 표시줄과 "전송 요청", "StorageGRID 중지", "재부팅 중"과 같은 일련의 메시지는 어플라이언스가 유지보수 모드로 들어가기 위한 단계를 완료하고 있음을 나타냅니다.



   어플라이언스가 유지보수 모드일 때 확인 메시지에 StorageGRID 어플라이언스 설치 프로그램에 액세스하는 데 사용할 수 있는 URL이 나열됩니다.



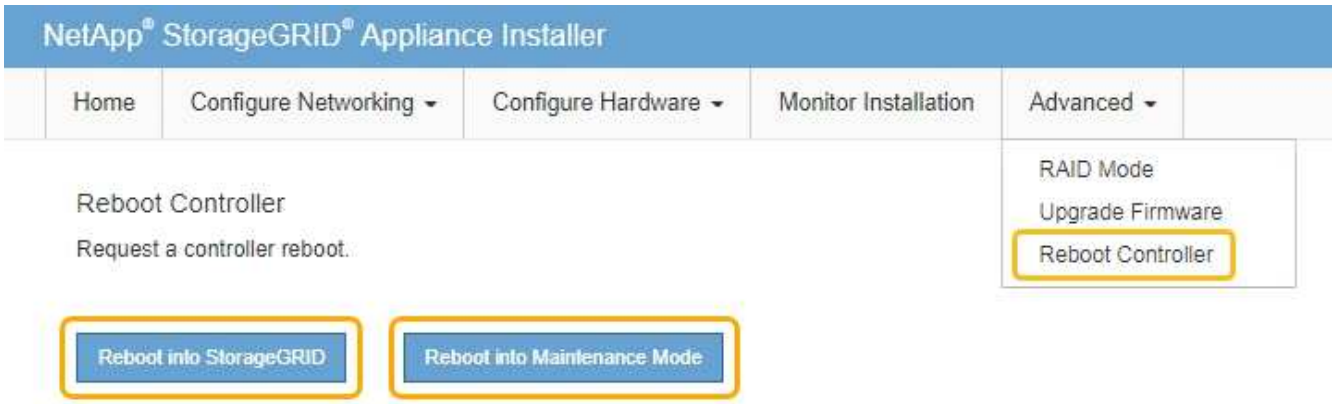
6. StorageGRID 어플라이언스 설치 프로그램에 액세스하려면 표시된 URL 중 하나를 찾습니다.

   가능한 경우 어플라이언스의 관리 네트워크 포트의 IP 주소가 포함된 URL을 사용하십시오.

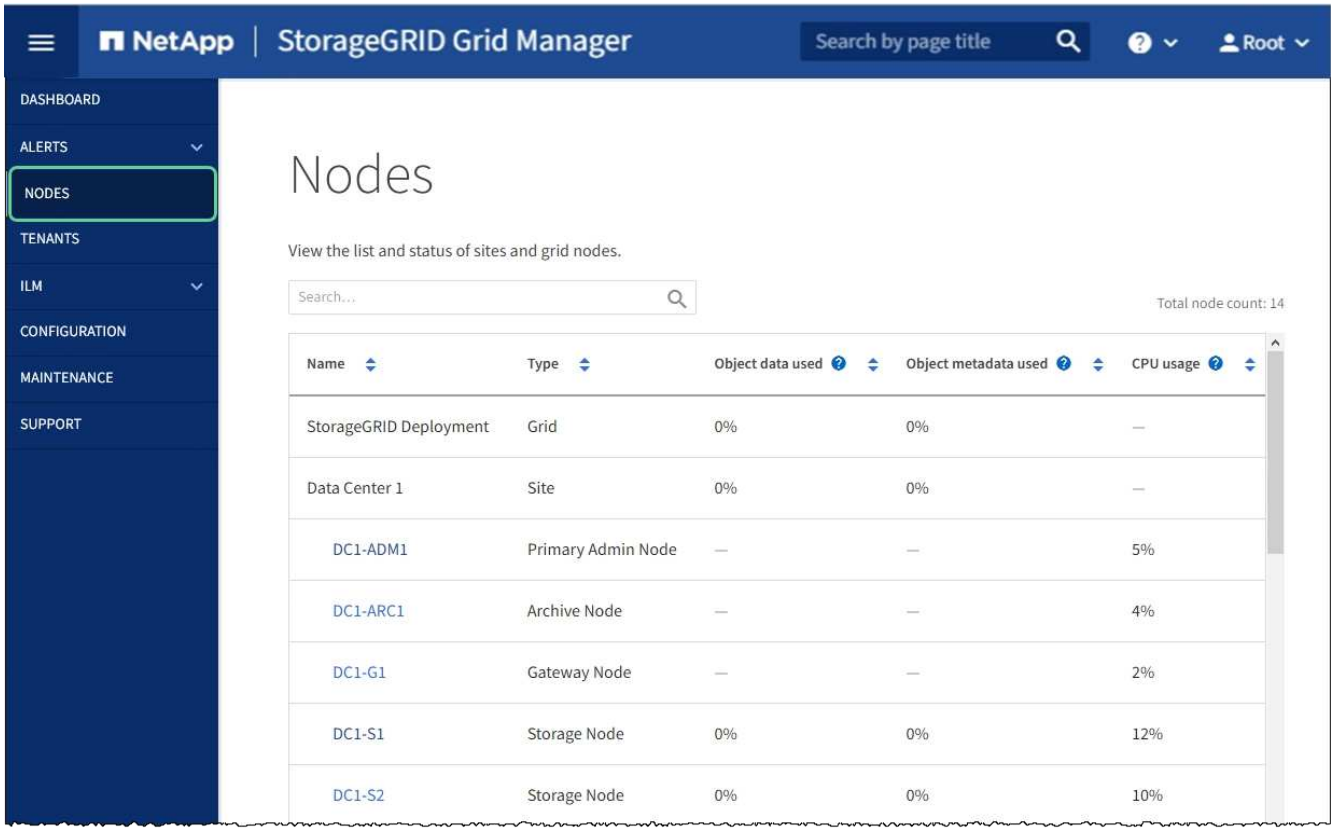
   > 어플라이언스의 관리 포트에 직접 연결되어 있는 경우, 'https://169.254.0.1:8443` 을 사용하여 StorageGRID 어플라이언스 설치 프로그램 페이지에 액세스하십시오.

7. StorageGRID 어플라이언스 설치 프로그램에서 어플라이언스가 유지보수 모드인지 확인합니다.

8. 필요한 유지보수 작업을 수행합니다.
9. 유지보수 작업을 완료한 후 유지보수 모드를 종료하고 정상 노드 운영을 재개합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * StorageGRID * 으로 재부팅 * 을 선택합니다.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



컨트롤러 식별 **LED**를 켜고 끕니다

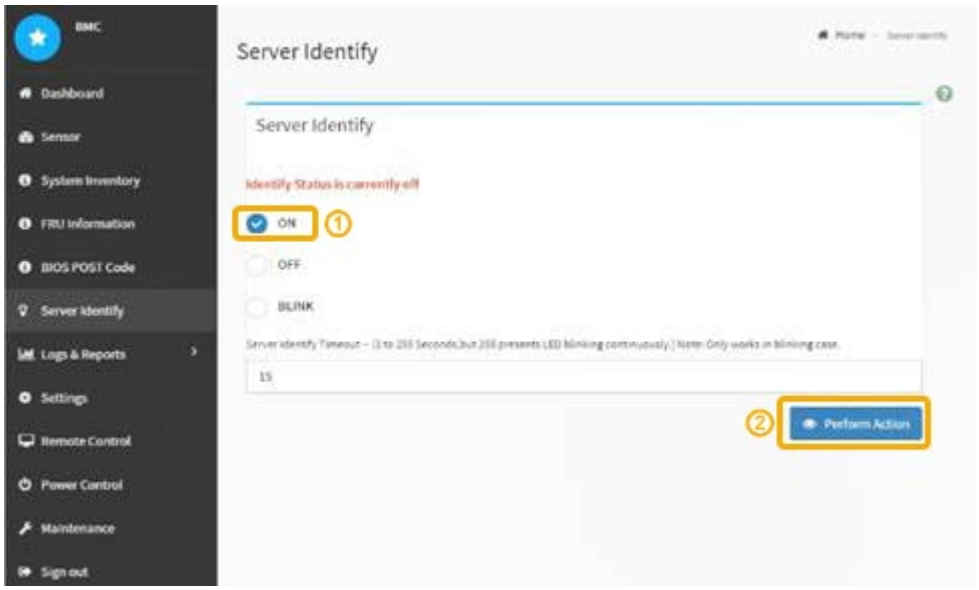
컨트롤러 앞면과 뒷면의 청색 식별 LED를 켜면 데이터 센터에서 제품을 쉽게 찾을 수 있습니다.

필요한 것

식별하려는 컨트롤러의 BMC IP 주소가 있어야 합니다.

단계

1. 컨트롤러 BMC 인터페이스에 액세스합니다.
2. 서버 식별 * 을 선택합니다.
3. On * 을 선택한 다음 * Perform Action * 을 선택합니다.



결과

파란색은 컨트롤러 전면(그림 참조)과 후면에 있는 LED 표시등을 나타냅니다.

베젤이 컨트롤러에 설치되어 있는 경우 전면 식별 LED를 확인하기 어려울 수 있습니다.

작업을 마친 후

컨트롤러 식별 LED를 끄려면:

- 컨트롤러 전면 패널의 식별 LED 스위치를 누릅니다.
- 컨트롤러 BMC 인터페이스에서 * 서버 식별 * 을 선택하고 * 꺼짐 * 을 선택한 다음 * 작업 수행 * 을 선택합니다.

파란색은 컨트롤러 전면과 후면에 있는 LED를 식별합니다.

관련 정보

데이터 센터에서 컨트롤러를 찾습니다

BMC 인터페이스에 액세스합니다

데이터 센터에서 컨트롤러를 찾습니다

하드웨어 유지보수 또는 업그레이드를 수행할 수 있는 컨트롤러를 찾습니다.

필요한 것

- 유지보수가 필요한 컨트롤러를 확인했습니다.
- (선택 사항) 데이터 센터에서 컨트롤러를 찾으려면 파란색 식별 LED를 켭니다.

단계

1. 데이터 센터에서 유지보수가 필요한 컨트롤러를 찾습니다.
   - 컨트롤러 전면 또는 후면에 있는 파란색 식별 LED가 켜져 있는지 확인합니다.

     전면 식별 LED는 컨트롤러 전면 베젤 뒤에 있으며 베젤이 설치되었는지 확인하기 어려울 수 있습니다.

   - 각 컨트롤러 전면에 부착된 태그에 일치하는 부품 번호가 있는지 확인합니다.
2. 컨트롤러 전면 베젤이 설치된 경우 전면 패널 컨트롤 및 표시등에 액세스하려면 전면 베젤을 분리합니다.
3. 선택 사항: 컨트롤러를 찾는 데 사용한 경우 청색 식별 LED를 끕니다.

- 컨트롤러 전면 패널의 식별 LED 스위치를 누릅니다.
- 컨트롤러 BMC 인터페이스를 사용합니다.

서비스 어플라이언스를 종료합니다

서비스 어플라이언스를 종료하여 하드웨어 유지 관리를 수행합니다.

필요한 것

- 데이터 센터에 유지보수가 필요한 서비스 어플라이언스를 물리적으로 배치했습니다.

  데이터 센터에서 컨트롤러 찾기

- 제품이 다 되었습니다 유지보수 모드로 전환됩니다.

이 작업에 대해

서비스 중단을 방지하기 위해 일반적으로 서비스 중단이 필요한 경우 예정된 유지보수 윈도우 중에 서비스 어플라이언스를 종료합니다.

단계

1. 제품을 유지보수 모드로 전환한 후 다음을 수행하십시오.

   > 아래 지정된 명령을 입력하여 어플라이언스 종료를 제어해야 합니다. 전원 스위치를 사용하여 어플라이언스를 종료하면 데이터가 손실됩니다.

   a. PuTTY 또는 다른 ssh 클라이언트를 사용하여 그리드 노드에 로그인합니다.
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

   b. 서비스 어플라이언스를 종료합니다. + " * shutdown -h now * "

      이 명령을 완료하는 데 최대 10분이 걸릴 수 있습니다.

2. 다음 방법 중 하나를 사용하여 제품의 전원이 꺼져 있는지 확인하십시오.
   - 제품 앞면에 있는 전원 LED를 살펴보고 전원이 꺼져 있는지 확인합니다.
   - BMC 인터페이스의 전원 제어 페이지를 확인하여 어플라이언스가 꺼져 있는지 확인합니다.

서비스 어플라이언스를 교체하십시오

제품이 최적의 상태로 작동하지 않거나 고장 난 경우 교체해야 할 수 있습니다.

필요한 것

- 교체 중인 제품과 동일한 부품 번호를 가진 교체용 제품이 있습니다.

- 제품에 연결된 각 케이블을 식별할 수 있는 라벨이 있습니다.
- 있습니다 제품을 물리적으로 위치했습니다.
- 제품이 다 되었습니다 유지보수 모드로 전환되었습니다.

이 작업에 대해

어플라이언스를 교체하는 동안에는 StorageGRID 노드에 액세스할 수 없습니다. 제품이 충분히 작동하는 경우 이 절차를 시작할 때 제어된 종료를 수행할 수 있습니다.

> StorageGRID 소프트웨어를 설치하기 전에 어플라이언스를 교체하는 경우 이 절차를 완료한 후 StorageGRID 어플라이언스 설치 프로그램에 즉시 액세스하지 못할 수 있습니다. 어플라이언스와 동일한 서브넷에 있는 다른 호스트에서 StorageGRID 어플라이언스 설치 프로그램에 액세스할 수 있지만 다른 서브넷에 있는 호스트에서는 액세스할 수 없습니다. 이 상태는 15분 이내에(원래 어플라이언스의 ARP 캐시 항목이 시간 초과될 때) 저절로 해결되거나 로컬 라우터 또는 게이트웨이에서 수동으로 이전 ARP 캐시 항목을 삭제하여 즉시 상태를 지울 수 있습니다.

단계

1. 제품이 유지보수 모드로 전환되면 제품을 종료하십시오.
   a. 그리드 노드에 로그인합니다.
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

   b. 제품을 종료한다: + ` * shutdown -h now * '
2. 다음 두 가지 방법 중 하나를 사용하여 제품의 전원이 꺼져 있는지 확인하십시오.
   - 제품 전면에 있는 전원 표시등 LED가 꺼져 있습니다.
   - BMC 인터페이스의 전원 제어 페이지에는 어플라이언스가 꺼져 있음을 나타냅니다.
3. 어플라이언스에 연결된 StorageGRID 네트워크가 DHCP 서버를 사용하는 경우 DNS/네트워크 및 IP 주소 설정을 업데이트합니다.
   a. 어플라이언스 전면에서 MAC 주소 레이블을 찾아 관리 네트워크 포트의 MAC 주소를 확인합니다.

      > MAC 주소 레이블에는 BMC 관리 포트의 MAC 주소가 나열됩니다.

      관리 네트워크 포트의 MAC 주소를 확인하려면 레이블의 16진수에 * 2 * 를 추가해야 합니다. 예를 들어 레이블의 MAC 주소가 * 09 * 로 끝나는 경우 관리 포트의 MAC 주소는 * 0B * 로 끝납니다. 레이블의 MAC 주소가 * (*y*) FF * 로 끝나는 경우 관리 포트의 MAC 주소는 * (*y*+1) 01 * 로 끝납니다. Windows에서 계산기를 열고, Programmer 모드로 설정하고, Hex를 선택하고, MAC 주소를 입력한 다음, * + 2 = * 를 입력하여 이 계산을 쉽게 수행할 수 있습니다.

   b. 제거한 어플라이언스의 DNS/네트워크 및 IP 주소를 대체 어플라이언스의 MAC 주소와 연관시킬 것을 네트워크 관리자에게 요청하십시오.

> 교체 어플라이언스에 전원을 공급하려면 먼저 원래 어플라이언스의 모든 IP 주소가 업데이트되었는지 확인해야 합니다. 그렇지 않으면 장치가 부팅될 때 새 DHCP IP 주소를 받게 되며 StorageGRID에 다시 연결할 수 없게 됩니다. 이 단계는 어플라이언스에 연결된 모든 StorageGRID 네트워크에 적용됩니다.

> 원래 어플라이언스가 고정 IP 주소를 사용하는 경우 새 어플라이언스는 제거된 어플라이언스의 IP 주소를 자동으로 채택합니다.

4. 다음 방법으로 제품을 분리하고 교체하십시오.
   a. 케이블에 레이블을 지정한 다음 케이블과 모든 네트워크 트랜시버를 분리합니다.

      > 성능 저하를 방지하려면 케이블을 비틀거나 접거나 끼거나 밟지 마십시오.

   b. 캐비닛 또는 랙에서 고장난 어플라이언스를 제거합니다.
   c. 장애가 발생한 어플라이언스에서 2개의 전원 공급 장치, 8개의 냉각 팬 및 2개의 SSD를 교체 어플라이언스로 전송합니다.

      이러한 구성 요소 교체에 대한 지침을 따릅니다.

   d. 캐비닛 또는 랙에 교체용 어플라이언스를 설치합니다.
   e. 케이블 및 광학 트랜시버를 교체합니다.
   f. 제품의 전원을 켜고 어플라이언스 LED 및 부팅 코드를 모니터링합니다.

      BMC 인터페이스를 사용하여 부팅 상태를 모니터링합니다.

5. 어플라이언스 노드가 그리드 관리자에 표시되고 경고가 나타나지 않는지 확인합니다.

관련 정보

캐비닛 또는 랙에 어플라이언스 설치(SG100 및 SG1000)

SG100 및 SG1000 어플라이언스의 상태 표시기를 봅니다

어플라이언스의 부팅 코드를 봅니다

서비스 어플라이언스에서 하나 또는 두 개의 전원 공급 장치를 교체합니다

서비스 어플라이언스에는 이중화를 위한 2개의 전원 공급 장치가 있습니다. 전원 공급 장치 중 하나에 장애가 발생하면 가능한 한 빨리 교체해야 컴퓨팅 컨트롤러에 중복 전원이 공급되는지 확인할 수 있습니다. 컨트롤러에서 작동하는 두 전원 공급 장치의 모델 및 와트는 동일해야 합니다.

필요한 것

- 있습니다 컨트롤러를 물리적으로 위치했습니다 전원 공급 장치를 교체해야 합니다.
- 하나의 전원 공급 장치만 교체하는 경우:
  - 교체 전원 공급 장치의 포장을 풀고 교체할 전원 공급 장치와 동일한 모델 및 와트인지 확인했습니다.

- 다른 전원 공급 장치가 설치되어 실행 중인지 확인했습니다.

- 두 전원 공급 장치를 동시에 교체하는 경우:
  - 교체 전원 공급 장치의 포장을 풀고 동일한 모델 및 와트인지 확인했습니다.

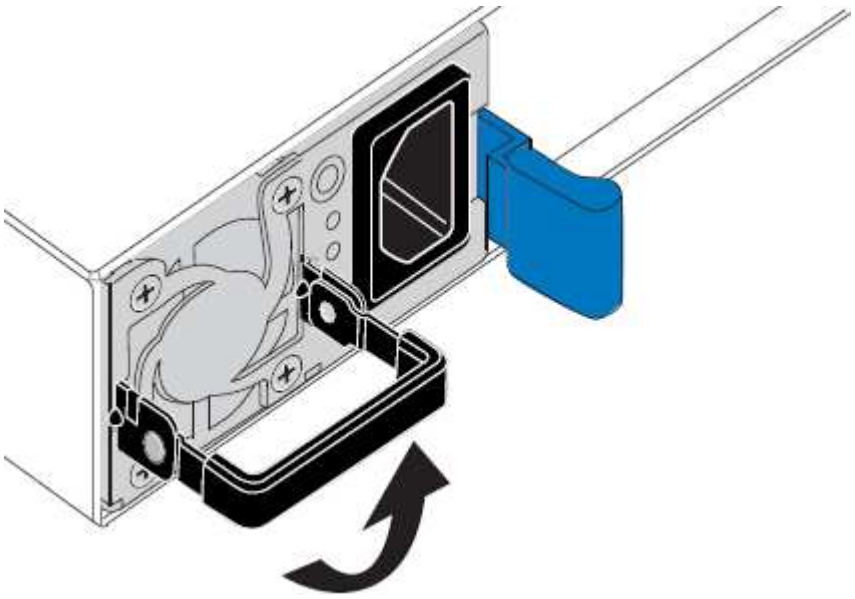
이 작업에 대해

아래 그림은 SG100의 전원 공급 장치 2개를 보여 주며, SG100은 제품 뒷면에서 액세스할 수 있습니다.

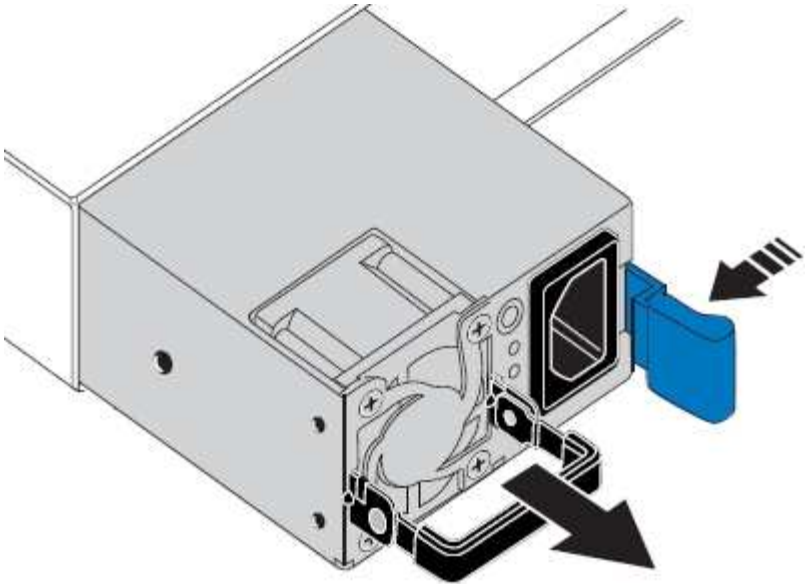
SG1000의 전원 공급 장치는 동일합니다.

단계

1. 하나의 전원 공급 장치만 교체하는 경우 제품을 종료할 필요가 없습니다. 로 이동합니다 전원 코드를 뽑습니다 단계. 두 전원 공급 장치를 동시에 교체하는 경우 전원 코드를 뽑기 전에 다음을 수행하십시오.
   a. 유지 관리 모드로 제품을 두십시오.
   b. 제품을 종료하십시오.
2. 교체할 각 전원 공급 장치에서 전원 코드를 뽑습니다.
3. 교체할 첫 번째 공급 장치의 캠 핸들을 들어 올립니다.



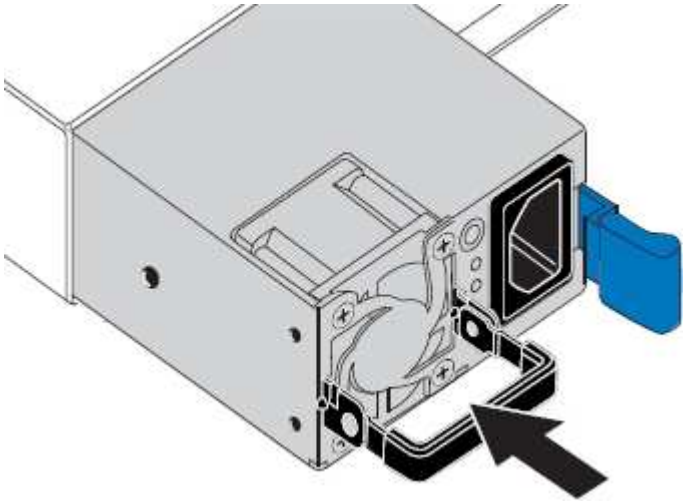
4. 파란색 래치를 누르고 전원 공급 장치를 당겨 빼냅니다.



5. 오른쪽에 있는 파란색 걸쇠를 사용하여 교체 전원 공급 장치를 섀시에 밀어 넣습니다.

   두 전원 공급 장치 모두 모델 및 와트가 동일해야 합니다.

   교체 장치를 밀어 넣을 때 파란색 걸쇠가 오른쪽에 있는지 확인합니다.



6. 캠 핸들을 아래로 눌러 교체용 전원 공급 장치를 고정합니다.
7. 두 전원 공급 장치를 모두 교체하는 경우 2-6단계를 반복하여 두 번째 전원 공급 장치를 교체합니다.
8. 전원 코드를 교체한 장치에 연결하고 전원을 공급합니다.
9. 어플라이언스를 유지보수 모드로 설정한 경우 유지보수 모드를 종료하십시오. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * StorageGRID * 으로 재부팅 * 을 선택합니다.

서비스 어플라이언스에서 팬을 교체합니다

서비스 어플라이언스에는 8개의 냉각 팬이 있습니다. 팬 중 하나에 장애가 발생할 경우 제품이 제대로 식었는지 확인하려면 가능한 한 빨리 교체해야 합니다.

필요한 것

- 교체용 팬의 포장을 풀었습니다.
- 있습니다 제품을 물리적으로 위치했습니다.
- 다른 팬이 설치되어 실행 중인지 확인했습니다.
- 있습니다 제품을 유지보수 모드로 전환하였습니다.

이 작업에 대해

팬을 교체하는 동안에는 어플라이언스 노드에 액세스할 수 없습니다.

사진은 서비스 어플라이언스에 대한 팬을 보여줍니다. 제품에서 상단 덮개를 분리한 후 냉각 팬에 액세스할 수 있습니다.

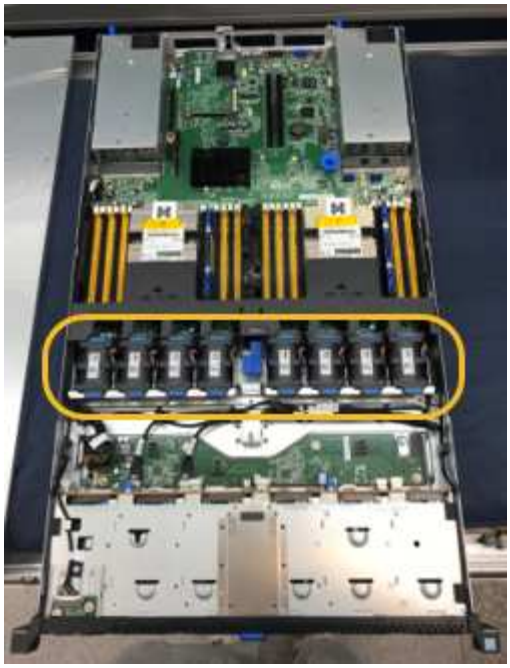
> 두 개의 전원 공급 장치 각각에는 팬도 포함되어 있습니다. 이러한 팬은 이 절차에 포함되어 있지 않습니다.

단계

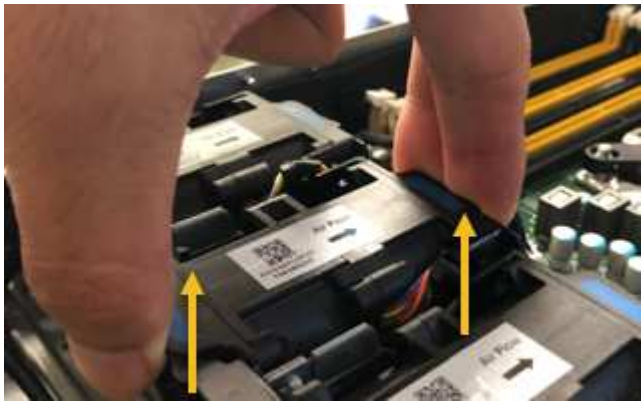
1. 제품이 유지보수 모드로 전환되면 제품을 종료하십시오.
   a. 그리드 노드에 로그인합니다.
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

   b. 서비스 어플라이언스를 종료합니다. + " * shutdown -h now * "
2. 다음 두 가지 방법 중 하나를 사용하여 서비스 어플라이언스의 전원이 꺼져 있는지 확인합니다.
   - 제품 전면에 있는 전원 표시등 LED가 꺼져 있습니다.
   - BMC 인터페이스의 전원 제어 페이지에는 어플라이언스가 꺼져 있음을 나타냅니다.
3. 제품을 랙에서 꺼냅니다.
4. 상단 덮개의 래치를 들어 올리고 제품에서 덮개를 분리합니다.
5. 결함이 있는 팬을 찾습니다.

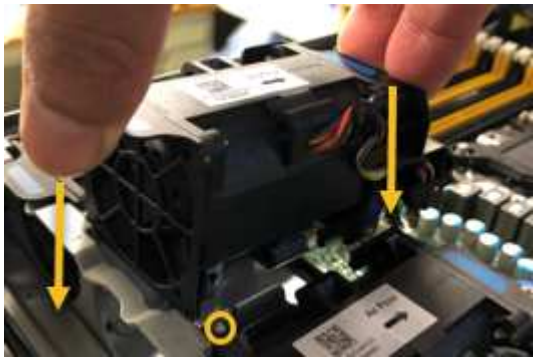


6. 결함이 있는 팬을 들어 올려 섀시에서 분리합니다.

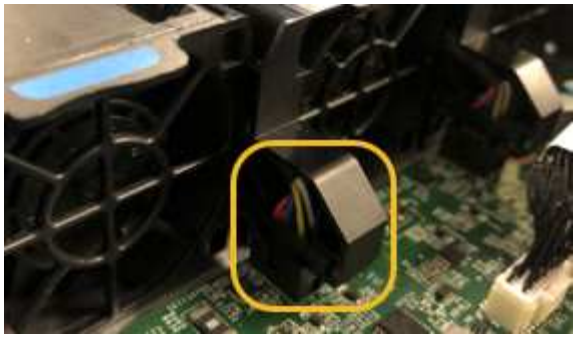


7. 교체용 팬을 섀시의 열려 있는 슬롯에 밀어 넣습니다.

   가이드 핀을 사용하여 팬 가장자리를 일렬로 맞추십시오. 사진에서 핀이 원으로 표시되어 있습니다.



8. 팬 커넥터를 회로 보드에 단단히 누릅니다.



9. 상단 덮개를 다시 제품에 끼우고 래치를 눌러 덮개를 제자리에 고정합니다.
10. 제품의 전원을 켜고 컨트롤러 LED 및 부팅 코드를 모니터링합니다.

    BMC 인터페이스를 사용하여 부팅 상태를 모니터링합니다.

11. 어플라이언스 노드가 그리드 관리자에 표시되고 경고가 나타나지 않는지 확인합니다.

서비스 어플라이언스에서 드라이브를 교체합니다

서비스 어플라이언스의 SSD에는 StorageGRID 운영 체제가 포함되어 있습니다. 또한 어플라이언스가 관리 노드로 구성된 경우 SSD에는 감사 로그, 메트릭 및 데이터베이스 테이블도 포함됩니다. 드라이브는 이중화를 위해 RAID1을 사용하여 미러링됩니다. 드라이브 중 하나에 장애가 발생할 경우 중복성을 보장하기 위해 가능한 한 빨리 드라이브를 교체해야 합니다.

필요한 것

- 있습니다 제품을 물리적으로 위치했습니다.
- 왼쪽 LED가 주황색으로 깜박이는지 확인하여 장애가 발생한 드라이브를 확인했습니다.

> 작동 중인 드라이브를 제거하면 어플라이언스 노드를 내립니다. 상태 표시등을 보는 방법에 대한 정보를 참조하여 오류를 확인하십시오.

- 교체 드라이브를 받았습니다.
- 적절한 ESD 보호 조치를 받았습니다.

단계

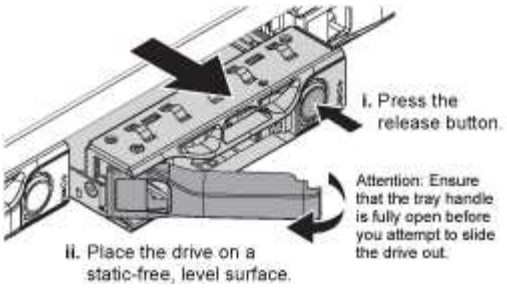
1. 드라이브의 왼쪽 LED가 주황색으로 깜박이는지 확인합니다.

   또한 그리드 관리자를 사용하여 SSD의 상태를 모니터링할 수도 있습니다. 노드 * 를 선택합니다. 그런 다음 "* 어플라이언스 노드*">* 하드웨어*를 선택합니다. 드라이브에 오류가 발생한 경우 스토리지 RAID 모드 필드에 오류가 발생한 드라이브에 대한 메시지가 표시됩니다.

2. ESD 밴드의 스트랩 끝을 손목 둘레에 감고 클립 끝을 금속 바닥에 단단히 고정하여 정전기 방전을 방지하십시오.
3. 교체용 드라이브의 포장을 풀고 제품 근처의 정전기가 없는 평평한 표면에 놓습니다.

   포장재를 모두 보관하십시오.

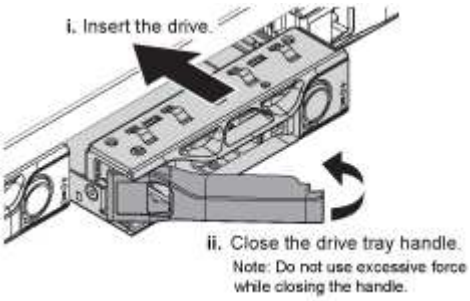
4. 오류가 발생한 드라이브의 분리 단추를 누릅니다.



드라이브 스프링의 핸들이 부분적으로 열리고 드라이브가 슬롯에서 풀리게 됩니다.

5. 핸들을 열고 드라이브를 밀어 빼낸 다음 정전기가 없는 평평한 표면에 놓습니다.
6. 드라이브 슬롯에 삽입하기 전에 교체 드라이브의 분리 단추를 누릅니다.

   래치 스프링이 열립니다.



7. 슬롯에 교체 드라이브를 삽입한 다음 드라이브 핸들을 닫습니다.

   > 핸들을 닫는 동안 과도한 힘을 가하지 마십시오.

   드라이브가 완전히 삽입되면 딸깍 소리가 납니다.

   드라이브는 작동 중인 드라이브에서 미러링된 데이터로 자동으로 재구축됩니다. 그리드 관리자를 사용하여 재생성 상태를 확인할 수 있습니다. 노드 * 를 선택합니다. 그런 다음 "* 어플라이언스 노드*">* 하드웨어*를 선택합니다. 스토리지 RAID 모드 필드에는 드라이브가 완전히 재구축될 때까지 "재구축 중" 메시지가 표시됩니다.

8. 드라이브 교체에 대해서는 기술 지원 부서에 문의하십시오.

   기술 지원 부서에서는 장애가 발생한 드라이브의 반품 지침을 제공합니다.

서비스 어플라이언스의 링크 구성을 변경합니다

서비스 어플라이언스의 이더넷 링크 구성을 변경할 수 있습니다. 포트 연결 모드, 네트워크 연결 모드 및 링크 속도를 변경할 수 있습니다.

필요한 것

- 있습니다 제품을 유지보수 모드로 전환하였습니다.

> StorageGRID 어플라이언스를 유지보수 모드로 전환하면 원격 액세스가 불가능한 경우가 드물게 있습니다.

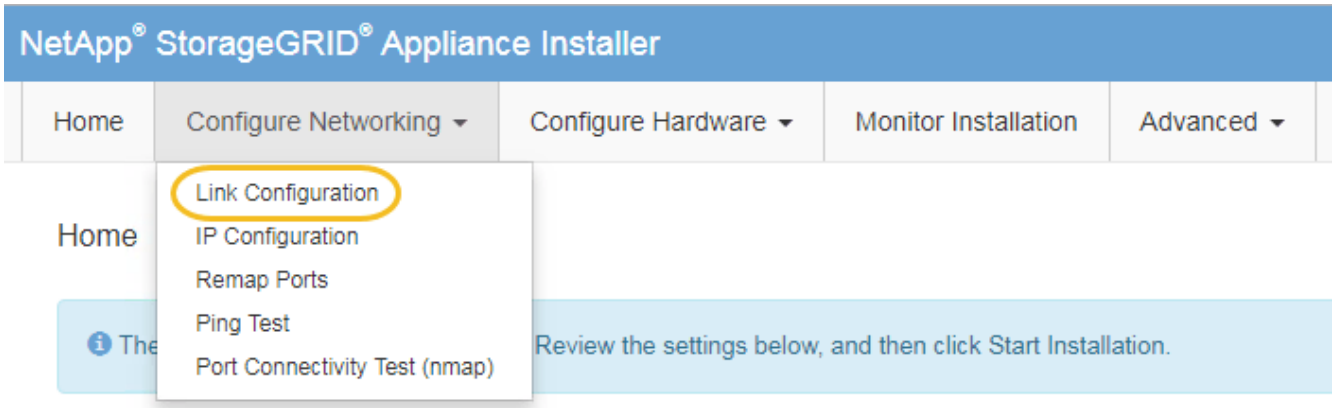
이 작업에 대해

서비스 어플라이언스의 이더넷 링크 구성을 변경하는 옵션은 다음과 같습니다.

- 포트 결합 모드 * 를 고정에서 집계로, 또는 Aggregate에서 고정으로 변경
- Active-Backup에서 LACP로 또는 LACP에서 Active-Backup으로 * 네트워크 결합 모드 * 변경
- VLAN 태그 지정 활성화 또는 비활성화 또는 VLAN 태그 값 변경
- 링크 속도 변경

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * 링크 구성 * 을 선택합니다.



2. 링크 구성을 원하는 대로 변경합니다.

   옵션에 대한 자세한 내용은 을 참조하십시오 네트워크 링크를 구성합니다.

3. 선택 사항에 만족하면 * 저장 * 을 클릭합니다.

   > 연결된 네트워크 또는 링크를 변경한 경우 연결이 끊어질 수 있습니다. 1분 내에 다시 연결되지 않으면 어플라이언스에 할당된 다른 IP 주소 중 하나를 사용하여 StorageGRID 어플라이언스 설치 프로그램의 URL을 다시 입력합니다. + " * https://*services_appliance_IP*:8443*`

4. 어플라이언스에 필요한 IP 주소를 변경합니다.

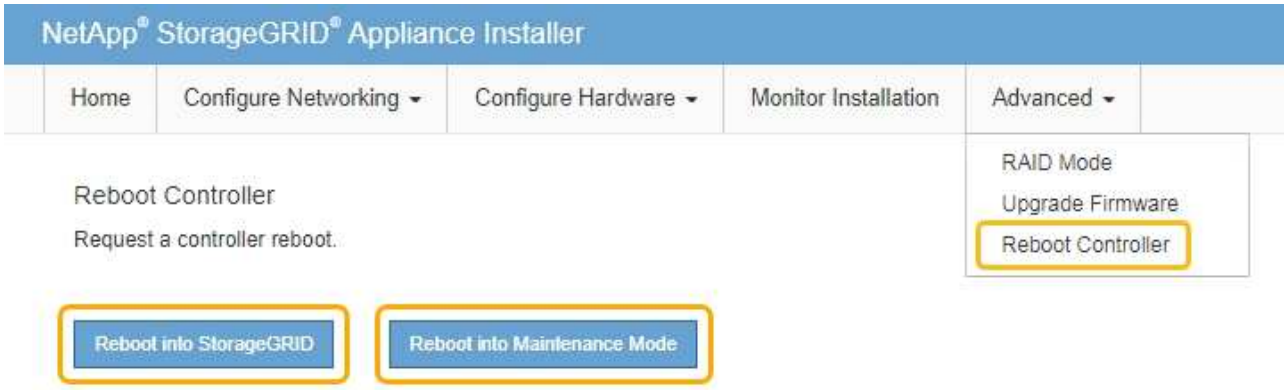
   VLAN 설정을 변경한 경우 어플라이언스의 서브넷이 변경되었을 수 있습니다. 어플라이언스의 IP 주소를 변경해야 하는 경우 를 참조하십시오 StorageGRID IP 주소를 구성합니다.

5. 메뉴에서 * 네트워킹 구성 * > * Ping 테스트 * 를 선택합니다.
6. Ping 테스트 도구를 사용하여 어플라이언스를 구성할 때 변경한 링크 구성의 영향을 받을 수 있는 네트워크의 IP 주소에 대한 연결을 확인합니다.

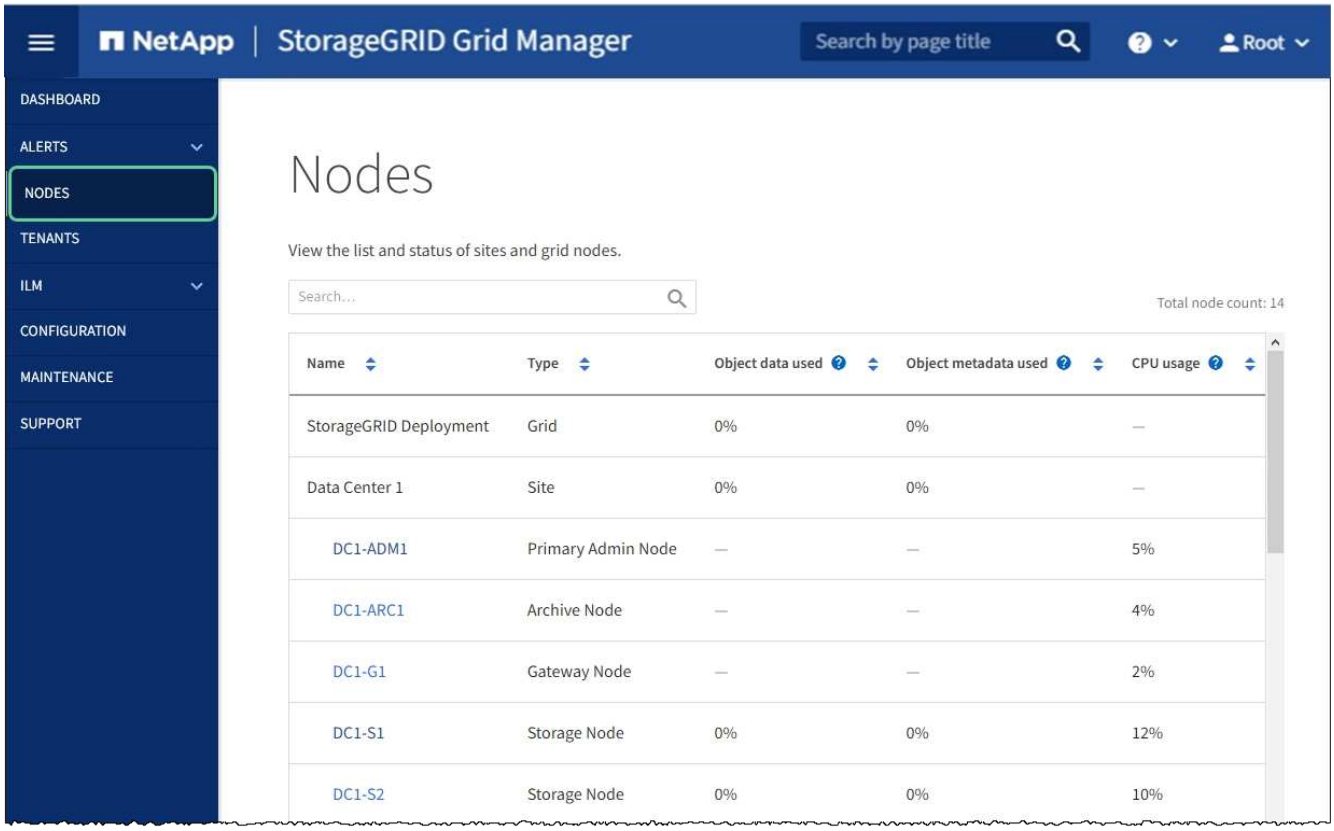
   수행할 다른 모든 테스트와 함께 기본 관리 노드의 그리드 네트워크 IP 주소 및 하나 이상의 다른 노드의 그리드 네트워크 IP 주소를 Ping할 수 있는지 확인합니다. 필요한 경우 네트워크 링크 구성 지침으로 돌아가서 문제를 해결하십시오.

7. 링크 구성 변경 사항이 작동한다고 만족하면 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.

- 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
- 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



MTU 설정을 변경합니다

어플라이언스 노드에 대한 IP 주소를 구성할 때 할당한 MTU 설정을 변경할 수 있습니다.

> 이 작업에 대해
>
> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

> 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

어플라이언스 노드를 재부팅하지 않고 MTU 설정을 변경하려면 IP 변경 도구를 사용합니다.

초기 설치 중에 StorageGRID 어플라이언스 설치 프로그램에서 클라이언트 또는 관리자 네트워크가 구성되지 않은 경우 유지보수 모드를 사용하여 MTU 설정을 변경합니다.

IP 변경 도구를 사용하여 MTU 설정을 변경합니다

필요한 것

- Change IP 툴을 사용할 수 있는 "passwords.txt" 파일이 있습니다.

단계

IP 변경 도구에 액세스하여 에 설명된 대로 MTU 설정을 업데이트합니다 노드 네트워크 구성을 변경합니다.

유지보수 모드를 사용하여 MTU 설정을 변경합니다

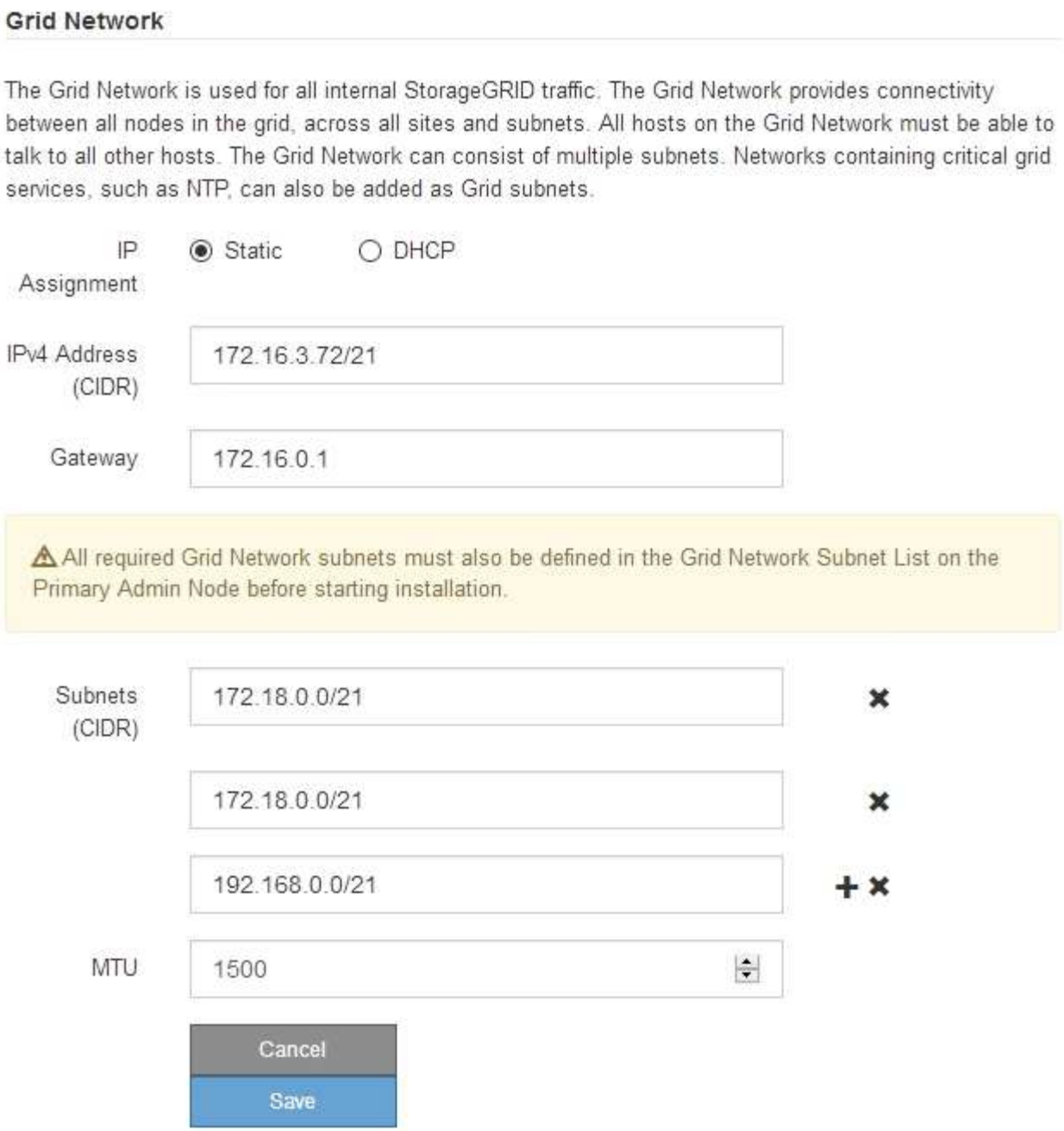
Change IP(IP 변경) 도구를 사용하여 이러한 설정에 액세스할 수 없는 경우 유지보수 모드를 사용하여 MTU 설정을 변경합니다.

필요한 것

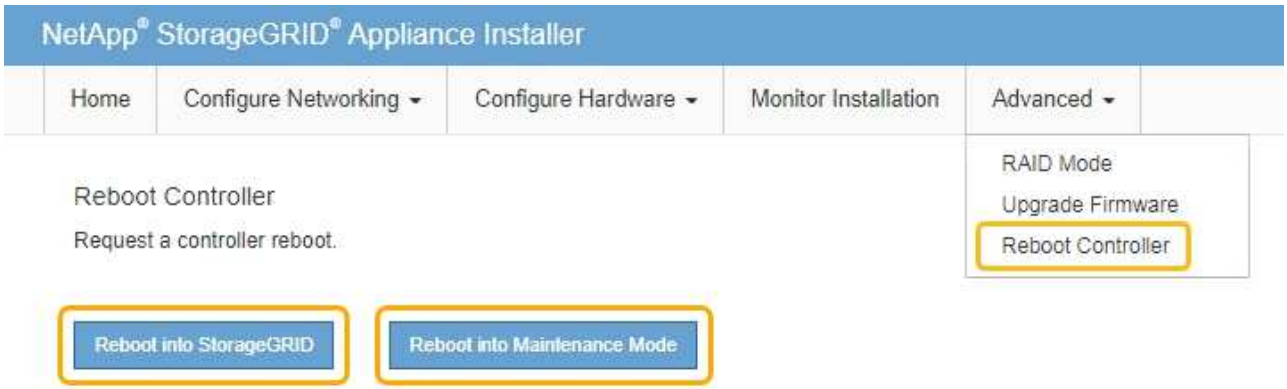
- 있습니다 제품을 유지보수 모드로 전환하였습니다.

단계

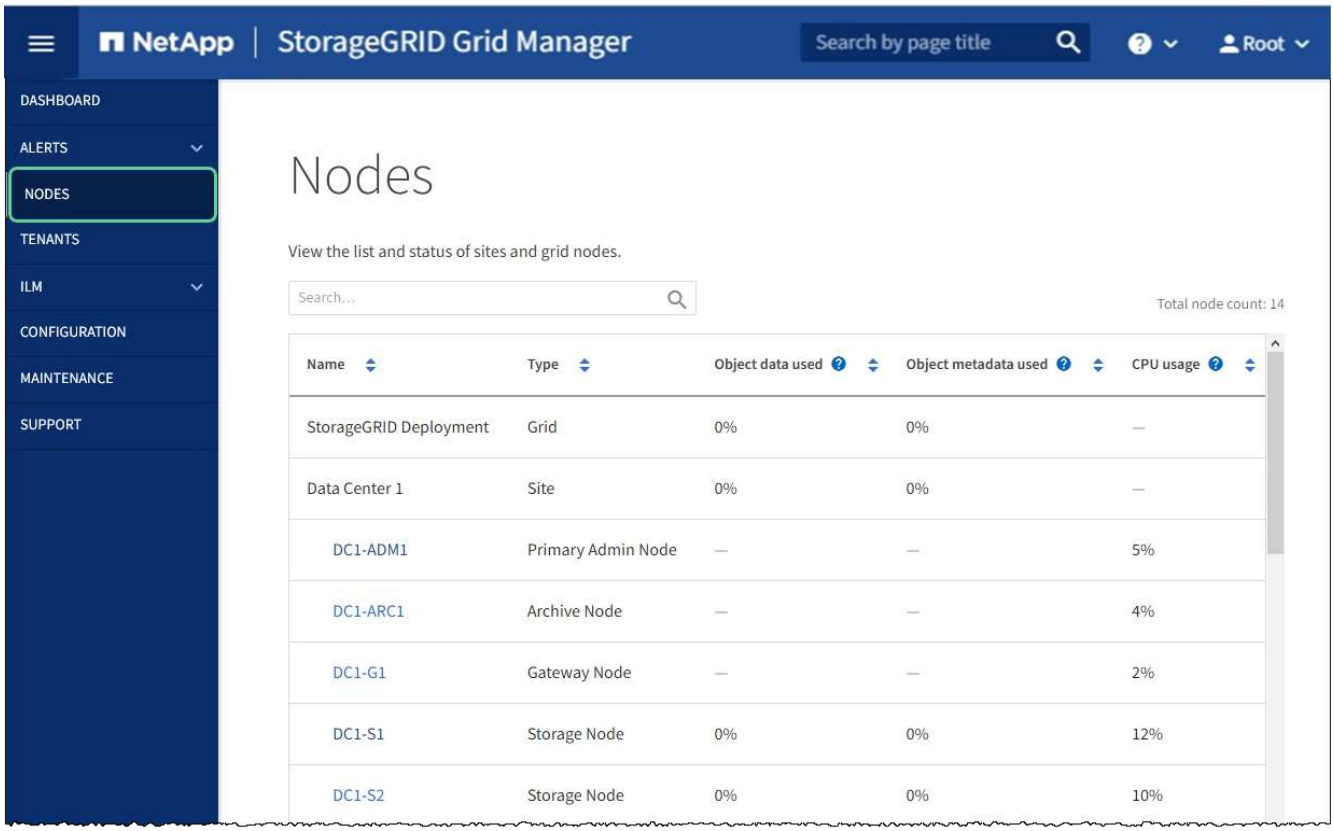
1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * IP 구성 * 을 선택합니다.
2. 그리드 네트워크, 관리자 네트워크 및 클라이언트 네트워크에 대한 MTU 설정을 원하는 대로 변경합니다.



3. 설정이 만족스러우면 * 저장 * 을 선택합니다.
4. 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.
   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

StorageGRID 관리

DNS 서버 구성을 확인합니다

이 어플라이언스 노드에서 현재 사용 중인 DNS(Domain Name System) 서버를 확인하고 일시적으로 변경할 수 있습니다.

필요한 것

- 있습니다 제품을 유지보수 모드로 전환하였습니다.

이 작업에 대해

KMS의 호스트 이름이 IP 주소 대신 도메인 이름으로 지정되었기 때문에 암호화된 어플라이언스가 KMS(키 관리 서버) 또는 KMS 클러스터에 연결할 수 없는 경우 DNS 서버 설정을 변경해야 할 수 있습니다. 어플라이언스에 대한 DNS 설정에 대한 모든 변경 사항은 일시적이며 유지 관리 모드를 종료할 때 손실됩니다. 이러한 변경 사항을 영구적으로 적용하려면 Grid Manager(* 유지 관리 * > * 네트워크 * > * DNS 서버 *)에서 DNS 서버를 지정합니다.

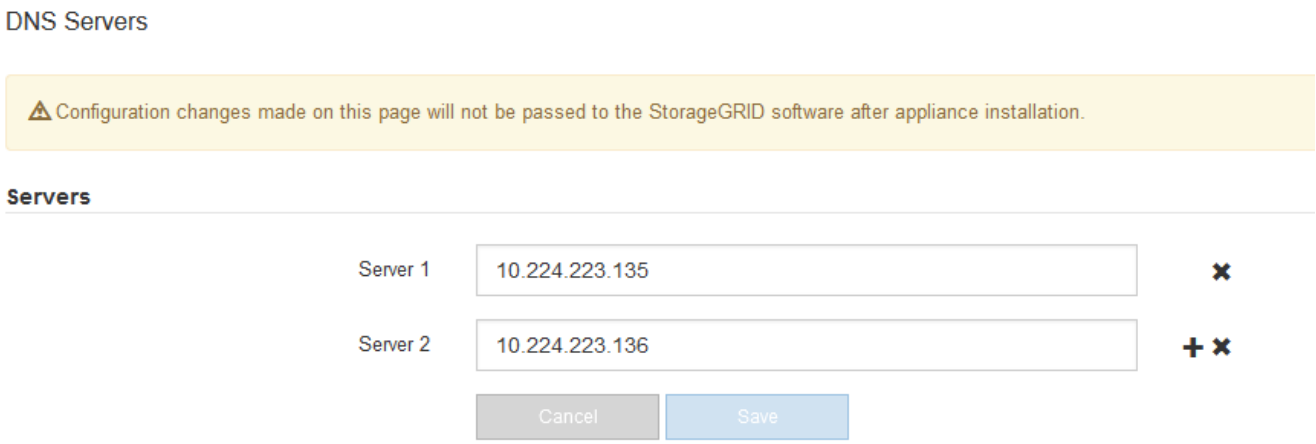
- KMS 서버가 호스트 이름에 대해 IP 주소 대신 정규화된 도메인 이름을 사용하여 정의된 노드 암호화 어플라이언스인 경우에만 DNS 구성을 일시적으로 변경해야 합니다.
- 노드 암호화 어플라이언스가 도메인 이름을 사용하여 KMS에 연결되는 경우 그리드에 정의된 DNS 서버 중 하나에 연결해야 합니다. 그런 다음 이러한 DNS 서버 중 하나가 도메인 이름을 IP 주소로 변환합니다.
- 노드가 그리드의 DNS 서버에 연결할 수 없거나 노드 암호화 어플라이언스 노드가 오프라인일 때 그리드 전체 DNS 설정을 변경한 경우 노드가 KMS에 연결할 수 없습니다. DNS 문제가 해결될 때까지 어플라이언스에 있는 암호화된 데이터를 해독할 수 없습니다.

KMS 연결을 방해하는 DNS 문제를 해결하려면 StorageGRID 어플라이언스 설치 프로그램에서 하나 이상의 DNS 서버의 IP 주소를 지정하십시오. 이러한 임시 DNS 설정을 사용하면 어플라이언스가 KMS에 연결하고 노드의 데이터를 해독할 수 있습니다.

예를 들어, 암호화된 노드가 오프라인 상태일 때 그리드의 DNS 서버가 변경되면 노드가 다시 온라인 상태가 될 때 KMS에 도달할 수 없습니다. KMS는 이전 DNS 값을 계속 사용하고 있기 때문입니다. StorageGRID 어플라이언스 설치 프로그램에 새 DNS 서버 IP 주소를 입력하면 임시 KMS 연결을 통해 노드 데이터를 해독할 수 있습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * DNS 구성 * 을 선택합니다.
2. 지정된 DNS 서버가 올바른지 확인합니다.



3. 필요한 경우 DNS 서버를 변경합니다.

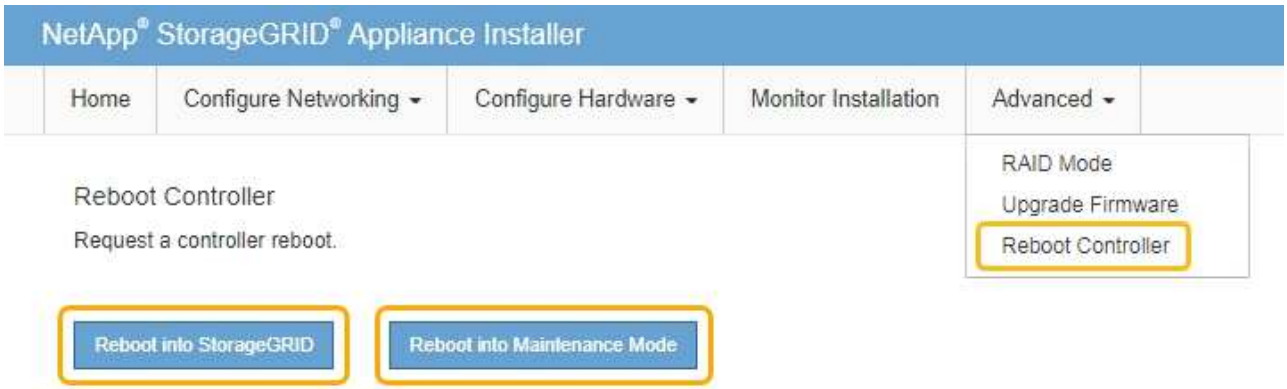
> DNS 설정에 대한 변경 사항은 일시적이며 유지 관리 모드를 종료할 때 손실됩니다.

4. 임시 DNS 설정이 만족스러우면 * Save * 를 선택합니다.

노드는 이 페이지에 지정된 DNS 서버 설정을 사용하여 KMS에 다시 연결하여 노드의 데이터를 해독할 수 있도록 합니다.

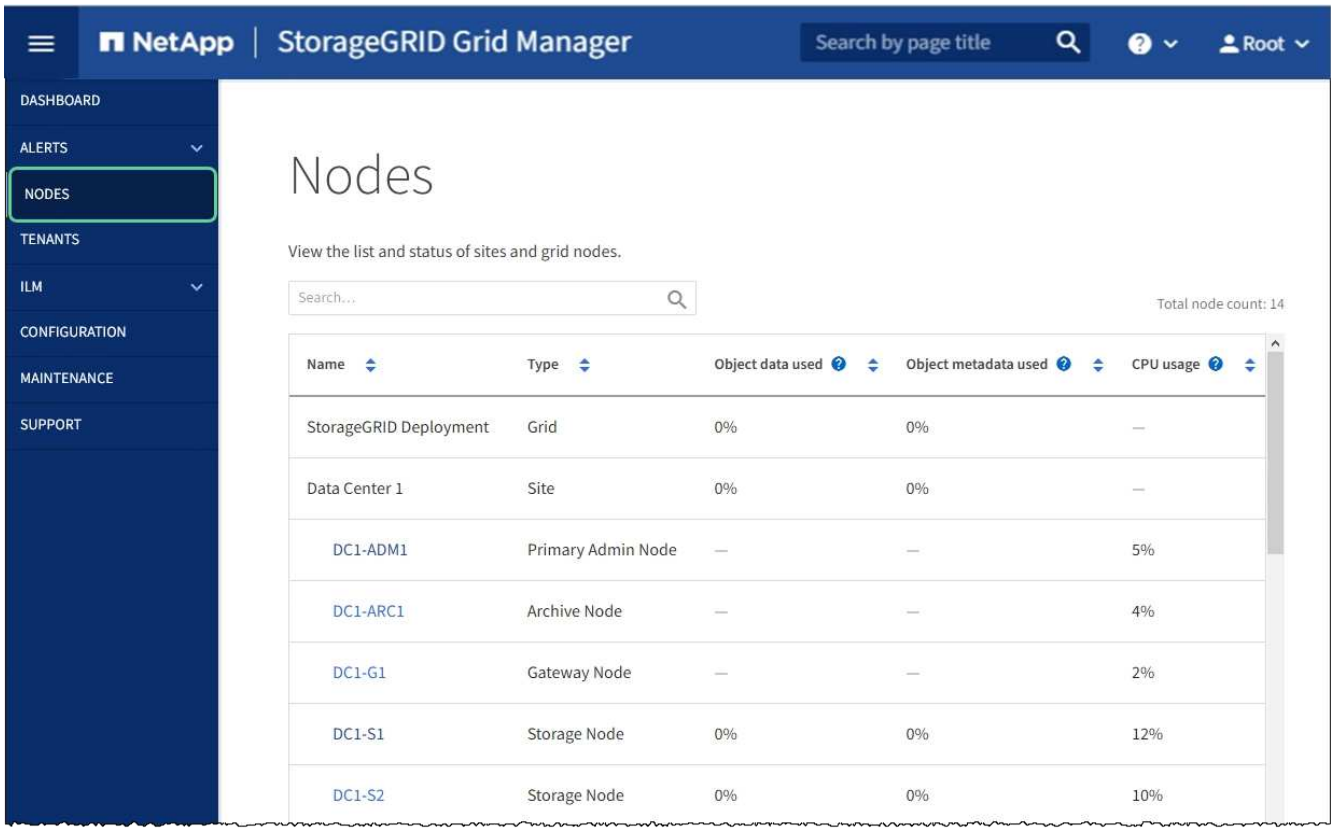
5. 노드 데이터가 해독된 후 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.

   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



> 노드가 재부팅되고 그리드에 다시 연결되면 Grid Manager에 나열된 시스템 전체 DNS 서버가 사용됩니다. 그리드를 다시 연결한 후 어플라이언스는 어플라이언스가 유지보수 모드일 때 StorageGRID 어플라이언스 설치 프로그램에 지정된 임시 DNS 서버를 더 이상 사용하지 않습니다.

어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



유지보수 모드에서 노드 암호화 모니터링**(SG100** 및 **SG1000)**

설치 중에 어플라이언스에 대한 노드 암호화를 활성화한 경우 노드 암호화 상태 및 키 관리 서버(KMS) 세부 정보를 포함하여 각 어플라이언스 노드의 노드 암호화 상태를 모니터링할 수 있습니다.

필요한 것

- 설치 중에 어플라이언스에 대한 노드 암호화를 활성화했습니다. 어플라이언스를 설치한 후에는 노드 암호화를 활성화할 수 없습니다.
- 있습니다 제품을 유지보수 모드로 전환하였습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption ☑

Save

Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate >

Client certificate >

Clear KMS Key

Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

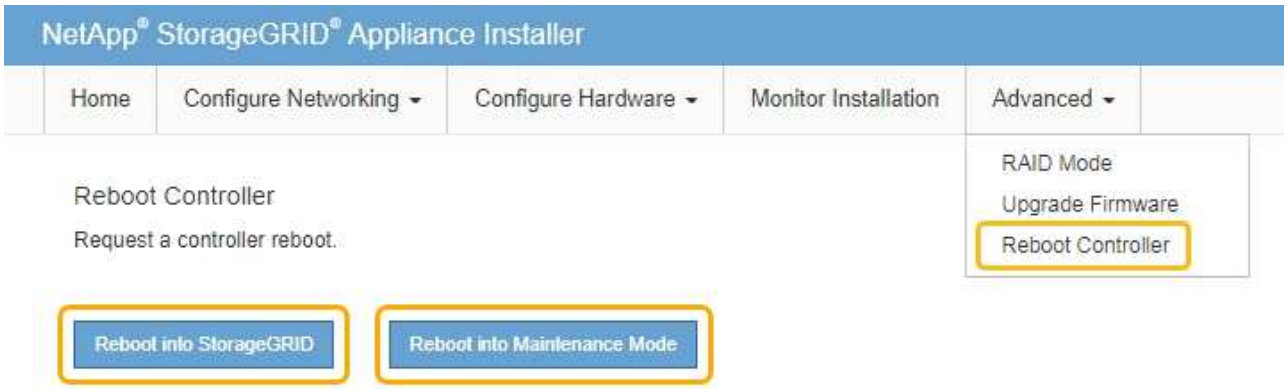
Clear KMS Key and Delete Data

노드 암호화 페이지에는 다음 세 가지 섹션이 있습니다.

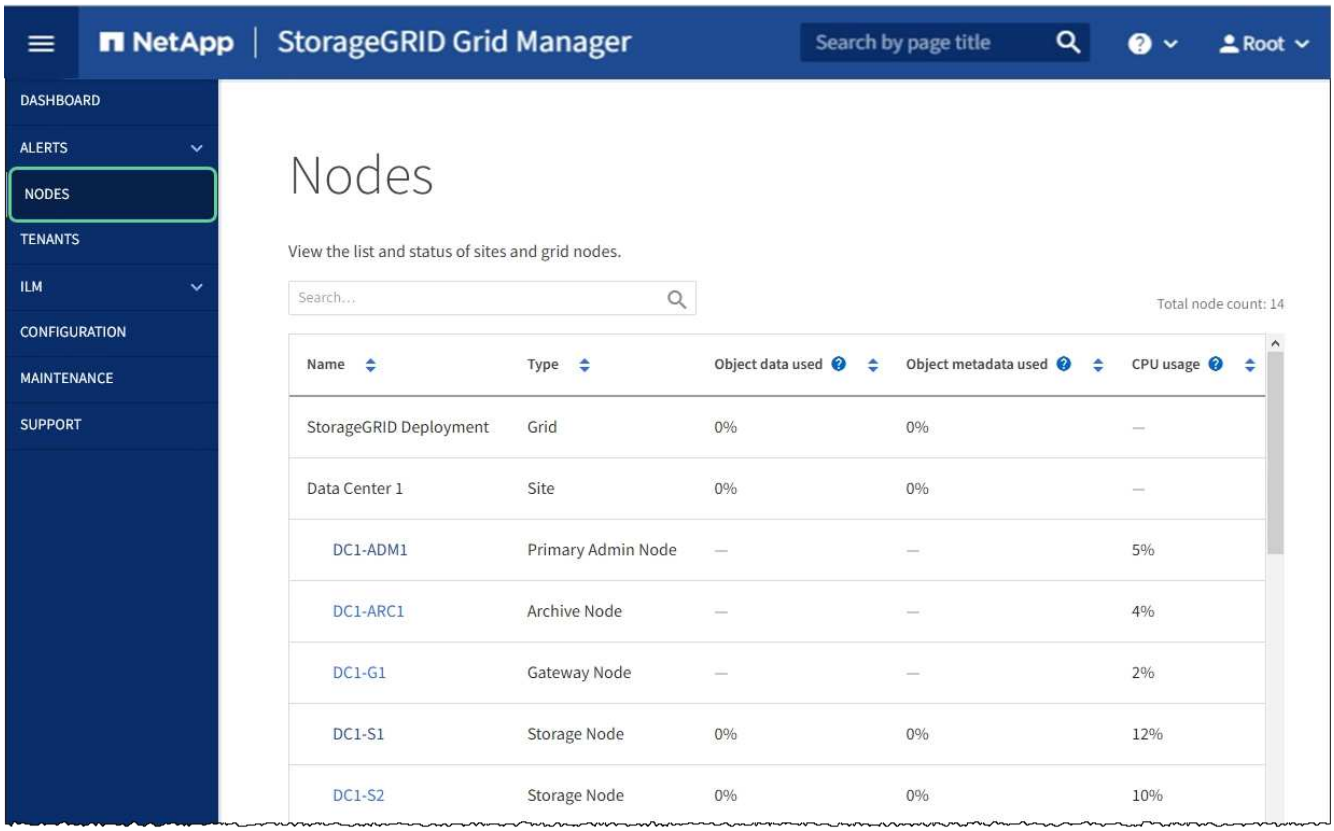
- 암호화 상태 는 어플라이언스에 대해 노드 암호화가 활성화되었는지 여부를 표시합니다.
- 키 관리 서버 세부 정보 는 어플라이언스를 암호화하는 데 사용되는 KMS에 대한 정보를 보여 줍니다. 서버 및 클라이언트 인증서 섹션을 확장하여 인증서 세부 정보 및 상태를 볼 수 있습니다.
  - 만료된 인증서 갱신과 같은 인증서 자체의 문제를 해결하려면 을 참조하십시오 KMS 구성 지침.
  - KMS 호스트에 연결할 때 예기치 않은 문제가 발생하는 경우, 를 확인하십시오 DNS(Domain Name System) 서버가 올바릅니다 그리고 그것입니다 어플라이언스 네트워킹이 올바르게 구성되었습니다.
  - 인증서 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.
- KMS 키 지우기(Clear KMS Key)는 어플라이언스에 대한 노드 암호화를 해제하고, StorageGRID 사이트에 구성된 키 관리 서버와 어플라이언스를 제거하고, 어플라이언스에서 모든 데이터를 삭제합니다. 반드시 해야 합니다 KMS 키를 지웁니다 다른 StorageGRID 시스템에 제품을 설치하기 전에

KMS 구성을 지우면 어플라이언스에서 데이터가 삭제되어 영구적으로 액세스할 수 없게 됩니다. 이 데이터는 복구할 수 없습니다.

2. 노드 암호화 상태 확인을 마쳤으면 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.
   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

StorageGRID 관리

키 관리 서버 구성을 지웁니다

KMS(키 관리 서버) 구성을 지우면 어플라이언스에서 노드 암호화가 비활성화됩니다. KMS 구성을 삭제한 후에는 어플라이언스의 데이터가 영구적으로 삭제되며 더 이상 액세스할 수 없습니다. 이 데이터는 복구할 수 없습니다.

필요한 것

어플라이언스의 데이터를 보존해야 하는 경우 KMS 구성을 지우기 전에 노드 서비스 해제 절차를 수행하거나 노드를 복제해야 합니다.

> KMS를 삭제하면 제품의 데이터가 영구적으로 삭제되고 더 이상 액세스할 수 없게 됩니다. 이 데이터는 복구할 수 없습니다.

노드 서비스 해제 포함된 데이터를 그리드의 다른 노드로 이동하려면 다음을 사용합니다.

이 작업에 대해

어플라이언스 KMS 구성을 지우면 노드 암호화가 비활성화되므로 어플라이언스 노드와 StorageGRID 사이트의 KMS 구성 간의 연결이 제거됩니다. 그러면 어플라이언스의 데이터가 삭제되고 어플라이언스가 사전 설치 상태로 유지됩니다. 이 프로세스는 되돌릴 수 없습니다.

KMS 구성을 지워야 합니다.

- KMS를 사용하지 않거나 다른 KMS를 사용하는 다른 StorageGRID 시스템에 제품을 설치하기 전에

> 동일한 KMS 키를 사용하는 StorageGRID 시스템에 어플라이언스 노드를 재설치하려는 경우 KMS 구성을 지우지 마십시오.

- KMS 구성이 손실되고 KMS 키를 복구할 수 없는 노드를 복구 및 재설치할 수 있습니다.
- 이전에 현장에서 사용 중이던 제품을 반환하기 전에
- 노드 암호화가 설정된 어플라이언스를 서비스 해제 후

> KMS를 제거하기 전에 어플라이언스의 전원을 해제하여 StorageGRID 시스템의 다른 노드로 데이터를 이동합니다. KMS를 폐기하기 전에 제거하면 데이터가 손실되고 어플라이언스가 작동하지 않을 수 있습니다.

단계

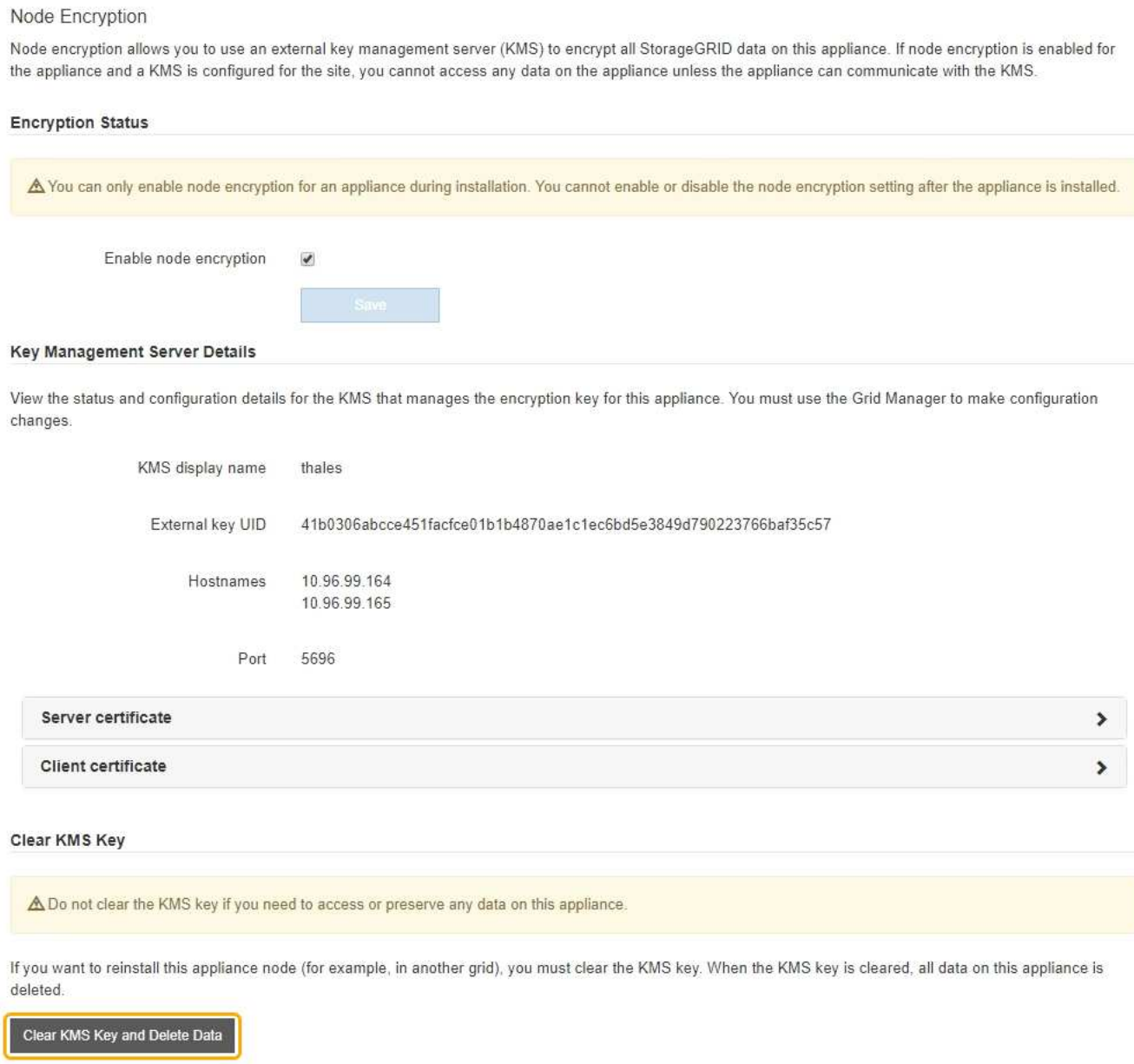
1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다.

   (* https://*Controller_IP*:8443*`)

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

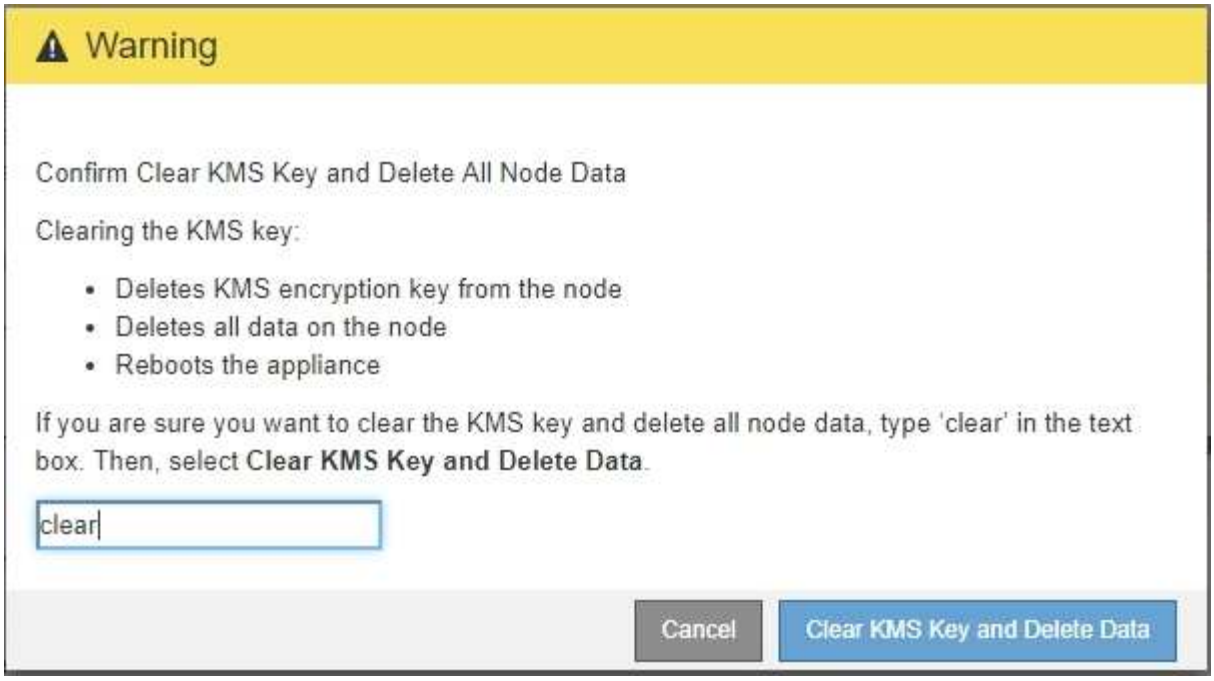
   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.



> KMS 구성이 삭제된 경우 어플라이언스의 데이터가 영구적으로 삭제됩니다. 이 데이터는 복구할 수 없습니다.

3. 창 아래쪽에서 * KMS 키 삭제 및 데이터 삭제 * 를 선택합니다.
4. KMS 구성을 지우려면 + " * clear * "+를 입력하고 * KMS 키 삭제 및 데이터 삭제 * 를 선택합니다.



KMS 암호화 키 및 모든 데이터가 노드에서 삭제되고 어플라이언스가 재부팅됩니다. 이 작업은 최대 20분이 소요될 수 있습니다.

5. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

6. 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.
7. 노드 암호화가 비활성화되었으며 * 키 관리 서버 세부 정보 * 및 * KMS 키 지우기 및 데이터 삭제 * 컨트롤의 키 및 인증서 정보가 창에서 제거되었는지 확인합니다.

   그리드에 다시 설치할 때까지 어플라이언스에서 노드 암호화를 다시 활성화할 수 없습니다.

작업을 마친 후

어플라이언스가 재부팅되고 KMS가 삭제되었으며 사전 설치 상태의 제품이 검증된 경우 StorageGRID 시스템에서 어플라이언스를 물리적으로 제거할 수 있습니다. 를 참조하십시오 어플라이언스 재설치 준비 지침.

관련 정보

StorageGRID 관리

SG6000 스토리지 어플라이언스

SG6000 어플라이언스: 개요

StorageGRID SG6000 어플라이언스는 StorageGRID 시스템의 스토리지 노드로 작동하는 통합 스토리지 및 컴퓨팅 플랫폼입니다. 이러한 어플라이언스는 어플라이언스 스토리지 노드와

가상(소프트웨어 기반) 스토리지 노드를 결합하는 하이브리드 그리드 환경에서 사용할 수 있습니다.

SG6000 어플라이언스는 다음과 같은 기능을 제공합니다.

- 다음 세 가지 모델로 제공됩니다.
  - 60개의 드라이브를 포함하는 SG6060은 확장 쉘프를 지원하고 E2800A 컨트롤러를 사용합니다.
  - 60개의 드라이브를 포함하는 SG6060X는 확장 쉘프를 지원하고 E2800B 컨트롤러를 사용합니다.

    SG6060 및 SG6060X는 스토리지 컨트롤러의 상호 연결 포트 위치를 제외하고 동일한 사양과 기능을 가집니다.

  - 24개의 SSD(Solid State Drive)를 제공하는 SGF6024
- StorageGRID 스토리지 노드의 스토리지 및 컴퓨팅 요소 통합
- 스토리지 노드 구축 및 구성을 단순화하기 위해 StorageGRID 어플라이언스 설치 프로그램을 포함합니다.
- 스토리지 컨트롤러 및 드라이브를 관리 및 모니터링하기 위한 SANtricity 시스템 관리자를 포함합니다.
- 컴퓨팅 컨트롤러의 하드웨어를 모니터링하고 진단하기 위한 BMC(베이스보드 관리 컨트롤러)를 포함합니다.
- StorageGRID 그리드 네트워크 및 클라이언트 네트워크에 대한 10GbE 또는 25GbE 연결을 최대 4개까지 지원합니다.
- FIPS(Federal Information Processing Standard) 드라이브 지원 이러한 드라이브를 SANtricity 시스템 관리자의 드라이브 보안 기능과 함께 사용하면 데이터에 대한 무단 액세스가 방지됩니다.

SG6060 및 **SG6060X** 어플라이언스

StorageGRID SG6060 및 SG6060X 어플라이언스에는 각각 스토리지 컨트롤러 2개와 드라이브 60개가 포함된 컴퓨팅 컨트롤러 및 스토리지 컨트롤러 쉘프가 포함되어 있습니다. 필요에 따라 두 어플라이언스 모두에 60-드라이브 확장 쉘프를 추가할 수 있습니다. 스토리지 컨트롤러의 상호 연결 포트 위치를 제외하고 SG6060과 SG6060X 사이에는 사양이나 기능 차이가 없습니다.

SG6060 및 **SG6060X** 구성 요소

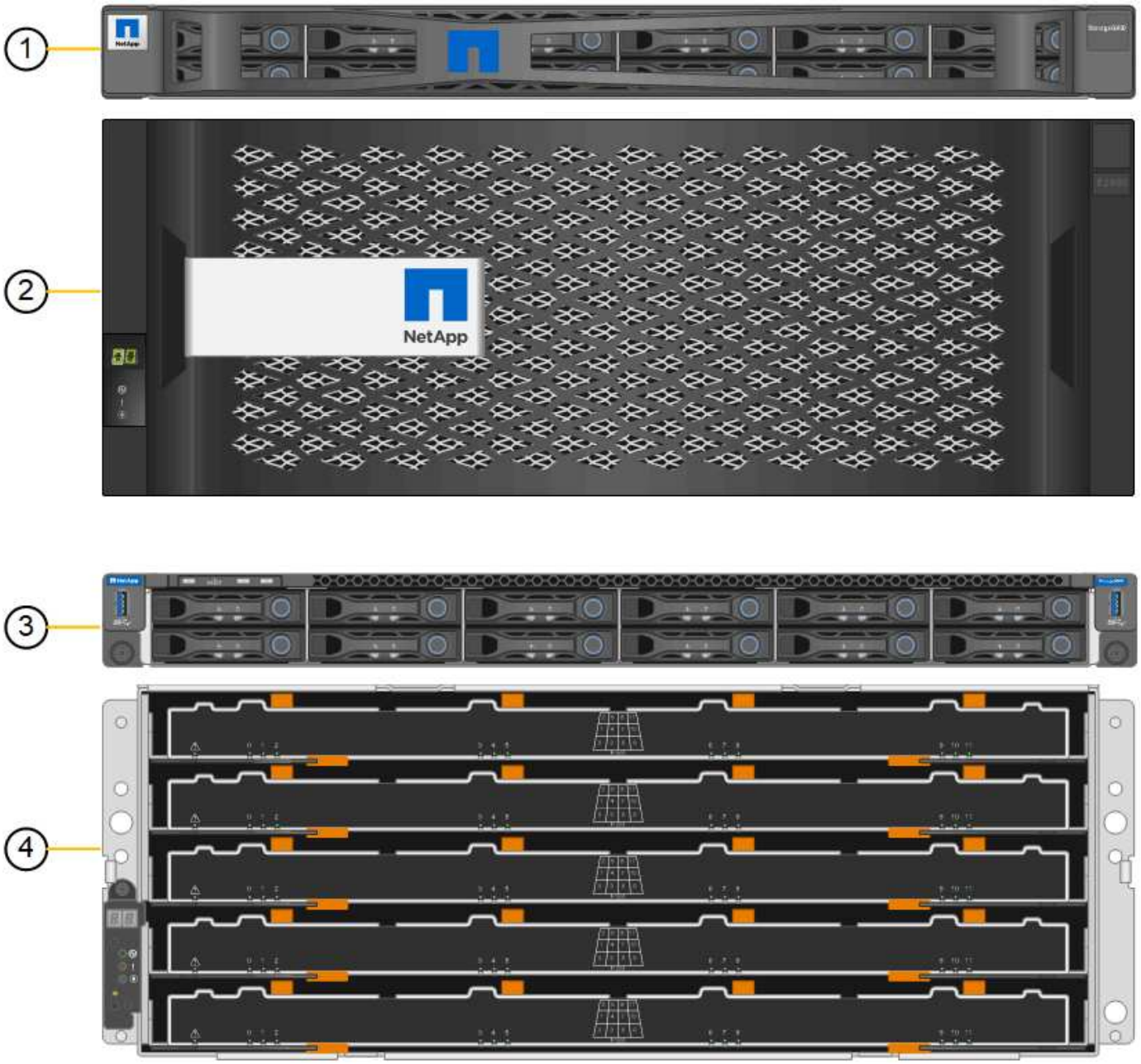
SG6060 및 SG660X 어플라이언스에는 다음 구성 요소가 포함되어 있습니다.

구성 요소	설명
컴퓨팅 컨트롤러	SG6000-CN 컨트롤러, 다음을 포함하는 1랙 유닛(1U) 서버: • 40개 코어(80개 스레드) • 192GB RAM • 최대 4 × 25Gbps 통합 이더넷 대역폭 • 4 × 16Gbps FC(Fibre Channel) 상호 연결 • 하드웨어 관리를 단순화하는 베이스보드 관리 컨트롤러(BMC) • 중복 전원 공급 장치
스토리지 컨트롤러 쉘프	E-Series E2860 컨트롤러 쉘프(스토리지 어레이), 4U 쉘프: • 스토리지 컨트롤러 페일오버 지원을 제공하는 2개의 E2800 시리즈 컨트롤러(이중 구성 ◦ SG6060에는 E2800A 스토리지 컨트롤러가 포함되어 있습니다 ◦ SG6060X에는 E2800B 스토리지 컨트롤러가 포함되어 있습니다 • 60개의 3.5인치 드라이브(SSD 2개, NL-SAS 드라이브 58개)를 보관할 수 있는 5개의 드로어 드라이브 쉘프 • 중복 전원 공급 장치 및 팬
선택 사항: 스토리지 확장 쉘프 • 참고: * 확장 셸프는 초기 배포 중에 설치하거나 나중에 추가할 수 있습니다.	E-Series DE460C 엔클로저, 4U 쉘프: • 입출력 모듈(IOM) 2개 • 각각 12개의 NL-SAS 드라이브가 장착된 5개의 드로어, 총 60개의 드라이브 • 중복 전원 공급 장치 및 팬 각 SG6060 및 SG6060X 어플라이언스는 총 180개의 드라이브에 대해 하나 또는 두 개의 확장 셸프를 가질 수 있습니다.

SG6060 및 **6060X** 다이어그램

SG6060 및 SG6060X의 앞면은 동일합니다. 다음 그림은 1U 컴퓨팅 컨트롤러와 5개의 드라이브 드로어에서 2개의 스토리지 컨트롤러와 60개의 드라이브를 포함하는 4U 쉘프를 포함하는 SG6060의 앞면을 보여줍니다.

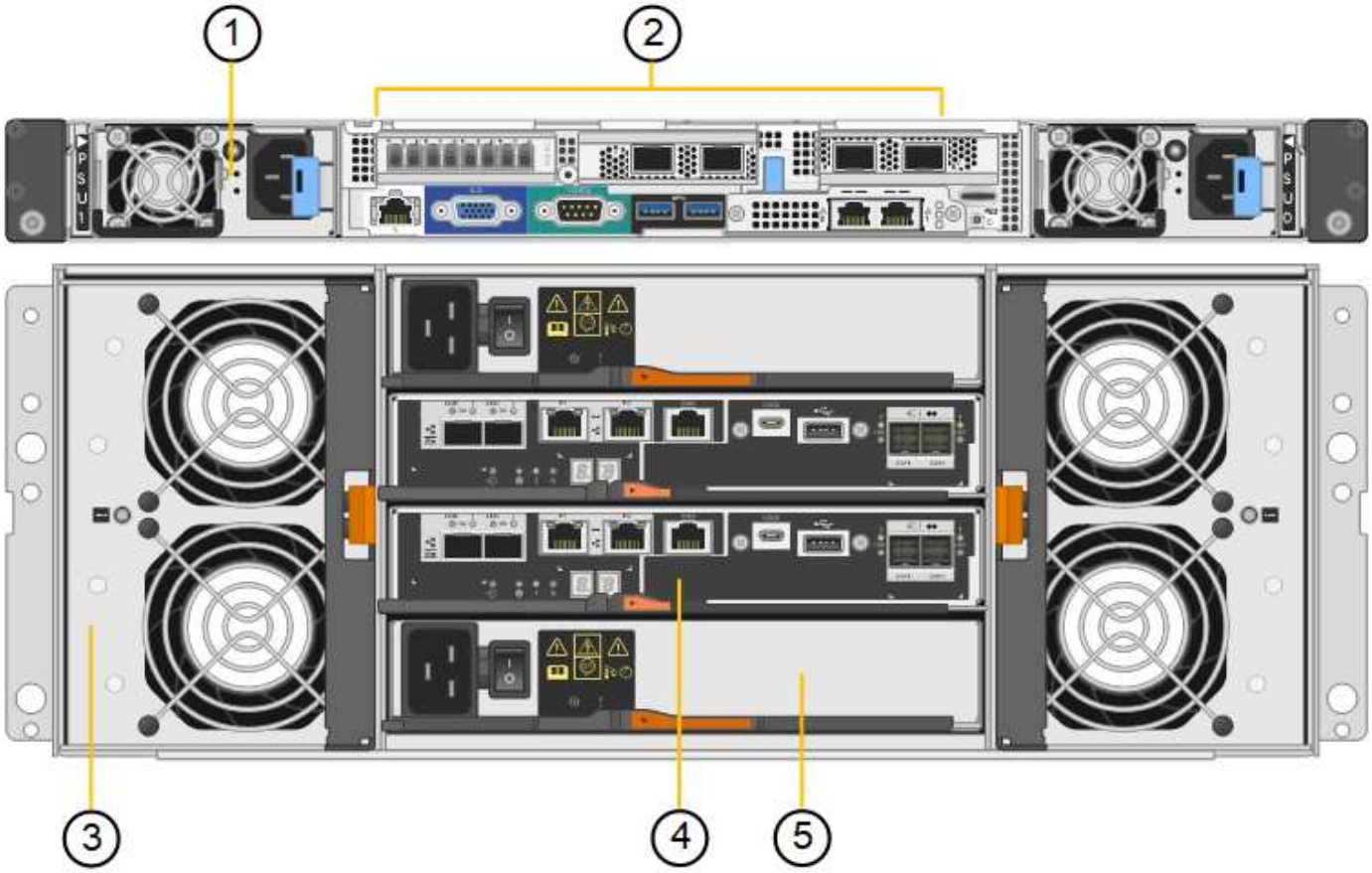
- SG6060 전면 모습 *



속성 표시기	설명
1	전면 베젤이 있는 SG6000-CN 컴퓨팅 컨트롤러
2	E2860 컨트롤러 쉘프 및 전면 베젤(옵션 확장 쉘프가 동일한 것으로 표시됨)
3	전면 베젤이 분리된 SG6000-CN 컴퓨팅 컨트롤러
4	E2860 컨트롤러 쉘프 및 전면 베젤 분리(옵션 확장 쉘프가 동일한 것으로 표시됨)

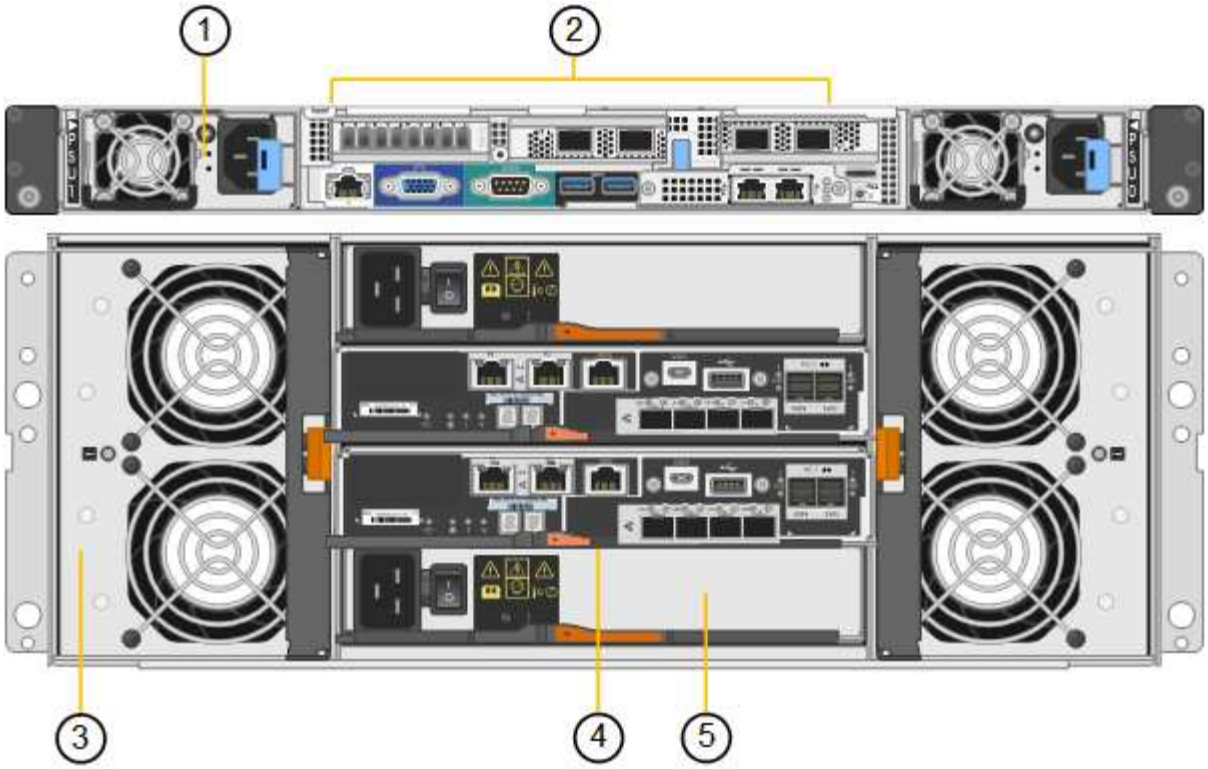
다음 그림은 컴퓨팅 및 스토리지 컨트롤러, 팬 및 전원 공급 장치를 포함하여 SG6060 및 SG6060X의 후면을 보여줍니다.

- SG6060 후면 *



속성 표시기	설명
1	SG6000-CN 컴퓨팅 컨트롤러용 전원 공급 장치(1/2)
2	SG6000-CN 컴퓨팅 컨트롤러용 커넥터
3	E2860 컨트롤러 쉘프용 팬(1/2
4	E-Series E2800A 스토리지 컨트롤러(1/2) 및 커넥터
5	E2860 컨트롤러 쉘프용 전원 공급 장치(1/2

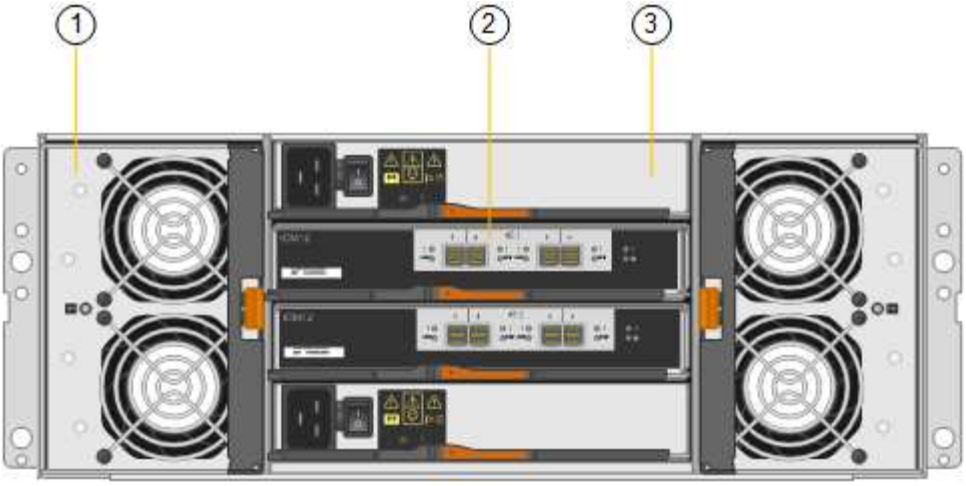
- SG6060X 후면 *



속성 표시기	설명
1	SG6000-CN 컴퓨팅 컨트롤러용 전원 공급 장치(1/2)
2	SG6000-CN 컴퓨팅 컨트롤러용 커넥터
3	E2860 컨트롤러 쉘프용 팬(1/2
4	E-Series E2800B 스토리지 컨트롤러(1/2) 및 커넥터
5	E2860 컨트롤러 쉘프용 전원 공급 장치(1/2

- SG6060 및 SG6060X 확장 쉘프 *

이 그림은 입/출력 모듈(IOM), 팬 및 전원 공급 장치를 포함하여 SG6060 및 SG6060X용 확장 셸프(옵션)의 후면을 보여줍니다. 각 SG6060 및 SG6060X는 1개 또는 2개의 확장 셸프와 함께 설치할 수 있습니다. 확장 셸프는 초기 설치에 포함되거나 나중에 추가할 수 있습니다.



속성 표시기	설명
1	확장 셸프용 팬(1/2
2	확장 쉘프의 IOM(1/2)
3	확장 셸프용 전원 공급 장치(1/2

SGF6024 개요

StorageGRID SGF6024에는 24개의 솔리드 스테이트 드라이브가 포함된 컴퓨팅 컨트롤러와 스토리지 컨트롤러 쉘프가 포함되어 있습니다.

SGF6024 구성 요소

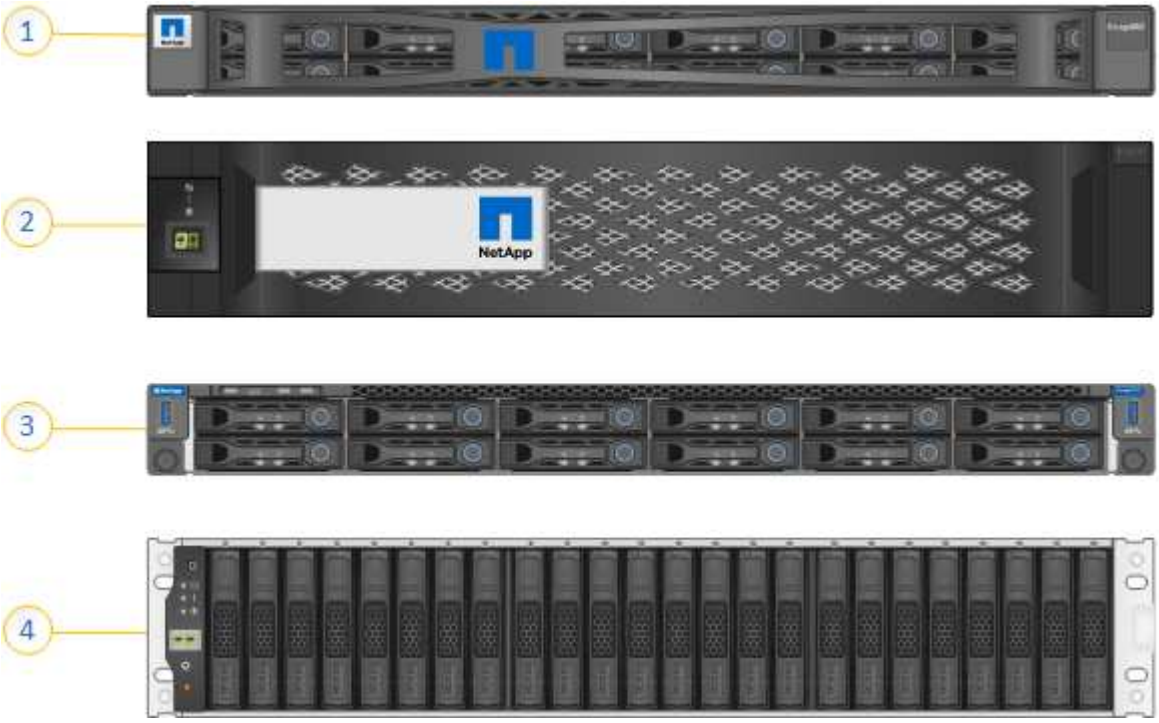
SGF6024 어플라이언스에는 다음 구성 요소가 포함되어 있습니다.

구성 요소	설명
컴퓨팅 컨트롤러	SG6000-CN 컨트롤러, 다음을 포함하는 1랙 유닛(1U) 서버: • 40개 코어(80개 스레드) • 192GB RAM • 최대 4 × 25Gbps 통합 이더넷 대역폭 • 4 × 16Gbps FC(Fibre Channel) 상호 연결 • 하드웨어 관리를 단순화하는 베이스보드 관리 컨트롤러(BMC) • 중복 전원 공급 장치

구성 요소	설명
플래시 어레이(컨트롤러 쉘프)	E-Series EF570 플래시 어레이(컨트롤러 쉘프라고도 함), 2U 쉘프: • 스토리지 컨트롤러 페일오버 지원을 위한 2개의 E-Series EF570 컨트롤러(이중 구성 • 24개의 솔리드 스테이트 드라이브(SSD 또는 플래시 드라이브라고도 함) • 중복 전원 공급 장치 및 팬

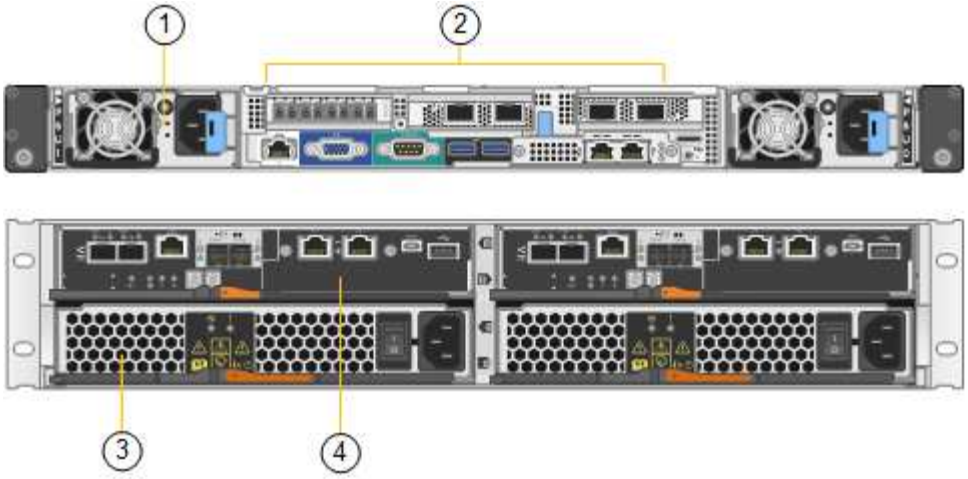
SGF6024 다이어그램

이 그림은 1U 컴퓨팅 컨트롤러와 2개의 스토리지 컨트롤러와 24개의 플래시 드라이브가 포함된 2U 엔클로저가 포함된 SGF6024의 전면을 보여줍니다.



속성 표시기	설명
1	전면 베젤이 있는 SG6000-CN 컴퓨팅 컨트롤러
2	EF570 플래시 어레이(전면 베젤 포함
3	전면 베젤이 분리된 SG6000-CN 컴퓨팅 컨트롤러
4	전면 베젤이 제거된 EF570 플래시 어레이

이 그림은 컴퓨팅 및 스토리지 컨트롤러, 팬 및 전원 공급 장치를 포함하여 SGF6024의 뒷면을 보여줍니다.



속성 표시기	설명
1	SG6000-CN 컴퓨팅 컨트롤러용 전원 공급 장치(1/2)
2	SG6000-CN 컴퓨팅 컨트롤러용 커넥터
3	EF570 플래시 어레이를 위한 전원 공급 장치(전체 2개 중 1개
4	E-Series EF570 스토리지 컨트롤러(1/2) 및 커넥터

SG6000 어플라이언스의 컨트롤러

StorageGRID SG6000 어플라이언스의 각 모델에는 모델에 따라 1U 엔클로저의 SG6000-CN 컴퓨팅 컨트롤러와 2U 또는 4U 엔클로저의 이중 E-Series 스토리지 컨트롤러가 포함됩니다. 각 컨트롤러 유형에 대한 자세한 내용은 다이어그램을 참조하십시오.

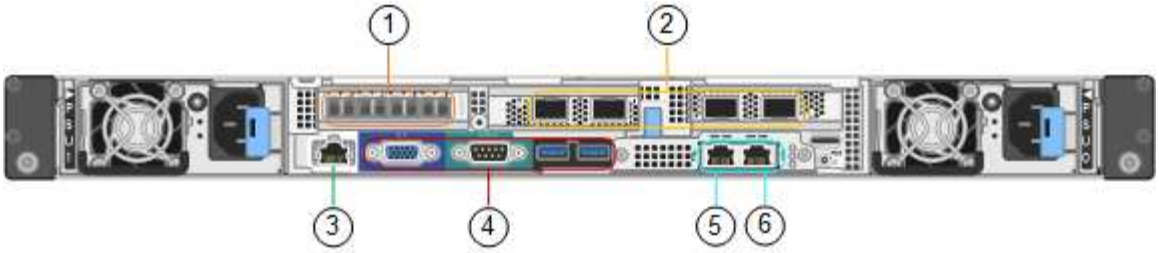
모든 어플라이언스**: SG6000-CN** 컴퓨팅 컨트롤러

- 어플라이언스에 대한 컴퓨팅 리소스를 제공합니다.
- StorageGRID 어플라이언스 설치 프로그램을 포함합니다.

> StorageGRID 소프트웨어는 어플라이언스에 사전 설치되어 있지 않습니다. 이 소프트웨어는 어플라이언스를 배포할 때 관리 노드에서 검색됩니다.

- 는 그리드 네트워크, 관리자 네트워크 및 클라이언트 네트워크를 포함하여 세 개의 StorageGRID 네트워크에 모두 연결할 수 있습니다.
- E-Series 스토리지 컨트롤러에 연결하고 이니시에이터로 작동합니다.

이 그림은 SG6000-CN의 후면에 있는 커넥터를 보여줍니다.



	포트	유형	사용
1	상호 연결 포트 1-4	광 미디어를 내장한 16Gb/s FC(Fibre Channel	SG6000-CN 컨트롤러를 E2800 컨트롤러에 연결합니다(각 E2800에 2개 연결).
2	네트워크 포트 1-4	케이블 또는 SFP 트랜시버 유형, 스위치 속도 및 구성된 링크 속도를 기반으로 한 10GbE 또는 25GbE	그리드 네트워크 및 StorageGRID용 클라이언트 네트워크에 연결합니다.
3	BMC 관리 포트	1GbE(RJ-45)	SG6000-CN 베이스보드 관리 컨트롤러에 연결합니다.
4	진단 및 지원 포트	• VGA • 직렬, 115200 8-N-1 • USB	기술 지원용으로 예약되어 있습니다.
5	관리 네트워크 포트 1	1GbE(RJ-45)	StorageGRID용 관리 네트워크에 SG6000-CN을 연결합니다.
6	관리 네트워크 포트 2	1GbE(RJ-45)	옵션: • StorageGRID용 관리 네트워크에 대한 중복 연결을 위해 관리 포트 1과 연결합니다. • 유선을 해제하고 임시 로컬 액세스(IP 169.254.0.1)를 위해 사용 가능한 상태로 둡니다. • 설치하는 동안 DHCP 할당 IP 주소를 사용할 수 없는 경우 IP 구성에 포트 2를 사용합니다.

SG6060 및 **SG6060X:E2800** 시리즈 스토리지 컨트롤러

- 페일오버 지원을 위한 2개의 컨트롤러
- 드라이브의 데이터 스토리지를 관리합니다.
- 이중 구성에서 표준 E-Series 컨트롤러로 작동합니다.
- SANtricity OS 소프트웨어(컨트롤러 펌웨어)를 포함합니다.
- 스토리지 하드웨어를 모니터링하고 경고, AutoSupport 기능 및 드라이브 보안 기능을 관리하기 위한 SANtricity 시스템 관리자를 포함합니다.
- SG6000-CN 컨트롤러에 연결하고 스토리지에 대한 액세스를 제공합니다.

SG6060 및 SG6060X는 E2800 시리즈 스토리지 컨트롤러를 사용합니다.

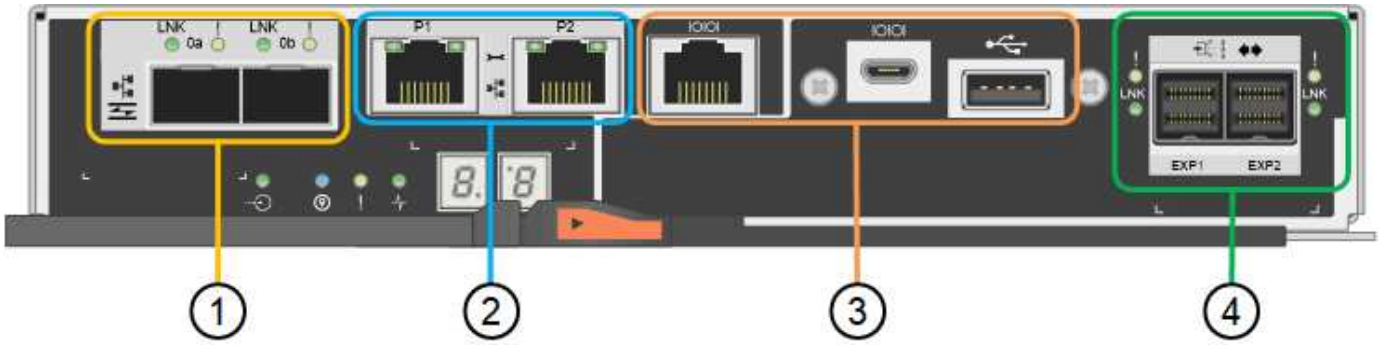
어플라이언스	컨트롤러
SG6060	E2800A 스토리지 컨트롤러 2개
SG6060X	E2800B 스토리지 컨트롤러 2개

E2800A에는 HIC가 없으며 E2800B에는 4포트 HIC가 있습니다. E2800A 및 E2800B 스토리지 컨트롤러는 상호 연결 포트의 위치를 제외하고 사양 및 기능에서 동일합니다.

E2800A 및 E2800B를 동일한 어플라이언스에서 사용하지 마십시오.

다음 그림은 각 E2800 시리즈 컨트롤러 후면의 커넥터를 보여줍니다.

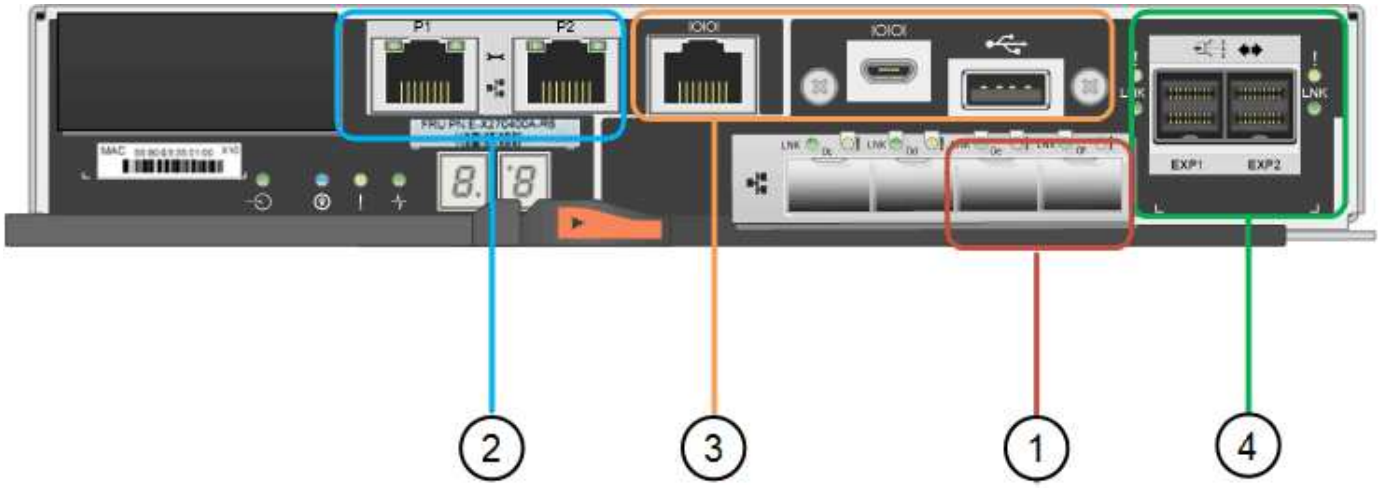
- E2800A 스토리지 컨트롤러 *



	포트	유형	사용
1	상호 연결 포트 1 및 2	16Gb/s FC 광 SFPa	E2800A 각 컨트롤러를 SG6000-CN 컨트롤러에 연결합니다. SG6000-CN 컨트롤러에 대한 4개의 연결이 있습니다(각 E2800A에서 2개).

	포트	유형	사용
2	관리 포트 1 및 2	1Gb(RJ-45) 이더넷	• 포트 1 옵션: ◦ 관리 네트워크에 연결하여 SANtricity 시스템 관리자에 대한 직접 TCP/IP 액세스를 활성화합니다 ◦ 스위치 포트 및 IP 주소를 저장하려면 유선 연결을 해제하십시오. 그리드 관리자 또는 스토리지 그리드 어플라이언스 설치 관리자 UI를 사용하여 SANtricity System Manager에 액세스합니다. • 참고 *: 정확한 로그 타임스탬프를 위한 NTP 동기화와 같은 일부 선택적 SANtricity 기능은 포트 1을 유선으로 남겨 두도록 선택한 경우 사용할 수 없습니다. • 참고 *: 포트 1을 유선으로 연결하지 않은 상태로 두면 StorageGRID 11.5 이상 및 SANtricity 11.70 이상이 필요합니다. • 포트 2는 기술 지원용으로 예약되어 있습니다.
3	진단 및 지원 포트	• RJ-45 직렬 포트 • 마이크로 USB 직렬 포트 • USB 포트	기술 지원용으로 예약되어 있습니다.
4	드라이브 확장 포트 1 및 2	12Gb/s SAS	확장 쉘프에 있는 IOM의 드라이브 확장 포트에 포트를 연결합니다.

• E2800B 스토리지 컨트롤러 *



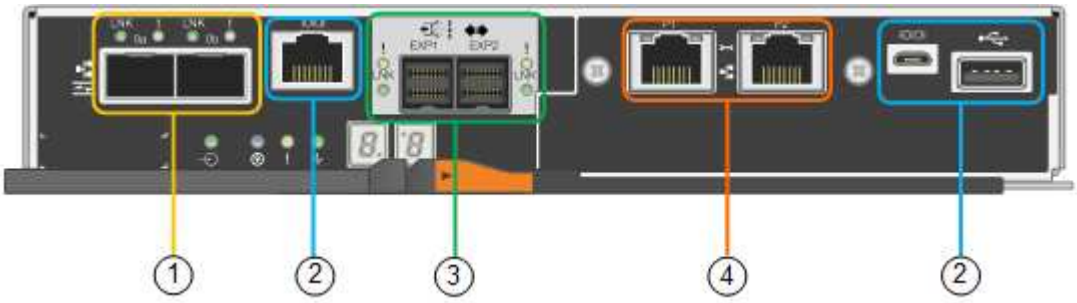
	포트	유형	사용
1	상호 연결 포트 1 및 2	16Gb/s FC 광 SFPa	E2800B 각 컨트롤러를 SG6000-CN 컨트롤러에 연결합니다. SG6000-CN 컨트롤러에 대한 4개의 연결이 있습니다(각 E2800B에서 2개).

	포트	유형	사용
2	관리 포트 1 및 2	1Gb(RJ-45) 이더넷	• 포트 1 옵션: ◦ 관리 네트워크에 연결하여 SANtricity 시스템 관리자에 대한 직접 TCP/IP 액세스를 활성화합니다 ◦ 스위치 포트 및 IP 주소를 저장하려면 유선 연결을 해제하십시오. 그리드 관리자 또는 스토리지 그리드 어플라이언스 설치 관리자 UI를 사용하여 SANtricity System Manager에 액세스합니다. • 참고 *: 정확한 로그 타임스탬프를 위한 NTP 동기화와 같은 일부 선택적 SANtricity 기능은 포트 1을 유선으로 남겨 두도록 선택한 경우 사용할 수 없습니다. • 참고 *: 포트 1을 유선으로 연결하지 않은 상태로 두면 StorageGRID 11.5 이상 및 SANtricity 11.70 이상이 필요합니다. • 포트 2는 기술 지원용으로 예약되어 있습니다.
3	진단 및 지원 포트	• RJ-45 직렬 포트 • 마이크로 USB 직렬 포트 • USB 포트	기술 지원용으로 예약되어 있습니다.
4	드라이브 확장 포트 1 및 2	12Gb/s SAS	확장 쉘프에 있는 IOM의 드라이브 확장 포트에 포트를 연결합니다.

SGF6024: EF570 스토리지 컨트롤러

- 페일오버 지원을 위한 2개의 컨트롤러
- 드라이브의 데이터 스토리지를 관리합니다.
- 이중 구성에서 표준 E-Series 컨트롤러로 작동합니다.
- SANtricity OS 소프트웨어(컨트롤러 펌웨어)를 포함합니다.
- 스토리지 하드웨어를 모니터링하고 경고, AutoSupport 기능 및 드라이브 보안 기능을 관리하기 위한 SANtricity 시스템 관리자를 포함합니다.
- SG6000-CN 컨트롤러에 연결하고 플래시 스토리지에 대한 액세스를 제공합니다.

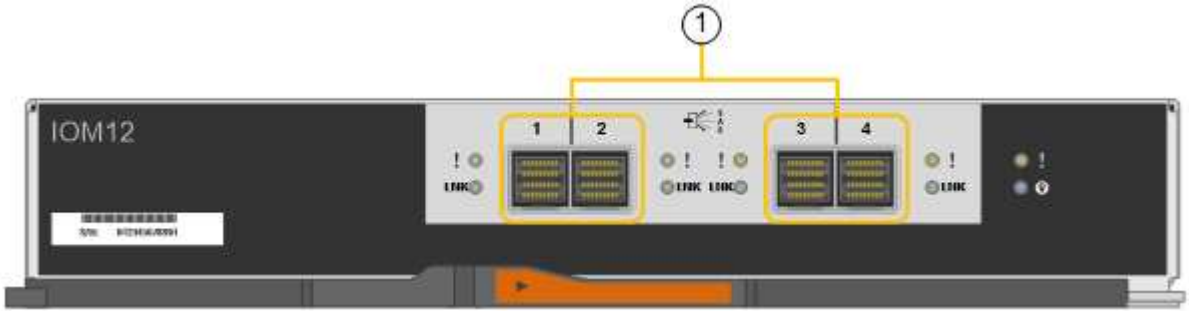
이 그림은 각 EF570 컨트롤러의 뒷면에 있는 커넥터를 보여줍니다.



	포트	유형	사용
1	상호 연결 포트 1 및 2	16Gb/s FC 광 SFPa	각 EF570 컨트롤러를 SG6000-CN 컨트롤러에 연결합니다. SG6000-CN 컨트롤러에 대한 4개의 연결이 있습니다(각 EF570에서 2개).
2	진단 및 지원 포트	• RJ-45 직렬 포트 • 마이크로 USB 직렬 포트 • USB 포트	기술 지원용으로 예약되어 있습니다.
3	드라이브 확장 포트	12Gb/s SAS	사용 안 합니다. SGF6024 어플라이언스는 확장 드라이브 쉘프를 지원하지 않습니다.
4	관리 포트 1 및 2	1Gb(RJ-45) 이더넷	• 포트 1은 브라우저에서 SANtricity 시스템 관리자에 액세스하는 네트워크에 연결합니다. • 포트 2는 기술 지원용으로 예약되어 있습니다.

SG6060 및 SG6060X: 확장 셸프 옵션용 입출력 모듈

확장 쉘프에는 스토리지 컨트롤러 또는 다른 확장 쉘프에 연결하는 2개의 I/O 모듈(IOM)이 포함되어 있습니다.



	포트	유형	사용
1	드라이브 확장 포트 1-4	12Gb/s SAS	각 포트를 스토리지 컨트롤러 또는 추가 확장 쉘프(있는 경우)에 연결합니다.

설치 및 구축 개요

StorageGRID를 처음 구축할 때 하나 이상의 StorageGRID 스토리지 어플라이언스를 설치하거나 나중에 확장을 위해 어플라이언스 스토리지 노드를 추가할 수 있습니다. 복구 작업의 일부로 어플라이언스 스토리지 노드를 설치해야 할 수도 있습니다.

필요한 것

StorageGRID 시스템에서 필요한 버전의 StorageGRID 소프트웨어를 사용하고 있습니다.

어플라이언스	필수 **StorageGRID** 버전입니다
확장 셸프 없이 SG6060 및 SG6060X	11.1.1 이상
확장 선반이 있는 SG6060 및 SG6060X(1개 또는 2개)	11.3 이상 • 참고: * 초기 배포 후에 확장 셸프를 추가하는 경우 버전 11.4 이상을 사용해야 합니다.
SGF6024	11.3 이상

설치 및 구축 작업

StorageGRID 스토리지 어플라이언스를 StorageGRID 시스템에 추가하는 작업은 다음과 같은 네 가지 주요 단계로 이루어집니다.

1. 설치 준비:
    - 설치 사이트 준비 중

- 박스 포장 풀기 및 내용물 확인
- 추가 장비 및 도구 확보
- IP 주소 및 네트워크 정보를 수집하는 중입니다
- 선택 사항: 모든 어플라이언스 데이터를 암호화하려는 경우 외부 키 관리 서버(KMS) 구성 StorageGRID 관리 지침에 있는 외부 키 관리에 대한 자세한 내용을 참조하십시오.

2. 하드웨어 설치:
   - 하드웨어를 등록하는 중입니다
   - 캐비닛 또는 랙에 제품 설치
   - 드라이브 설치
   - 확장 셸프 옵션 설치(모델 SG6060 및 SG6060X 전용, 최대 2개의 확장 셸프)
   - 어플라이언스 케이블 연결
   - 전원 코드 연결 및 전원 공급
   - 부팅 상태 코드 보기
3. 하드웨어 구성:
   - SANtricity 시스템 관리자에 액세스하여 SANtricity 시스템 관리자 설정을 구성합니다
   - StorageGRID 어플라이언스 설치 프로그램에 액세스하여 스토리지 컨트롤러의 관리 포트 1에 대한 정적 IP 주소를 설정하고 StorageGRID 네트워크에 연결하는 데 필요한 링크 및 네트워크 IP 설정을 구성합니다
   - SG6000-CN 컨트롤러의 베이스보드 관리 컨트롤러(BMC) 인터페이스에 액세스합니다
   - 선택 사항: 외부 KMS를 사용하여 어플라이언스 데이터를 암호화하려는 경우 노드 암호화 사용
   - 선택 사항: RAID 모드 변경
4. 어플라이언스를 스토리지 노드로 구축:

작업	지침
새로운 StorageGRID 시스템에 어플라이언스 스토리지 노드 구축	어플라이언스 스토리지 노드 구축
기존 StorageGRID 시스템에 어플라이언스 스토리지 노드 추가	StorageGRID 시스템 확장을 위한 지침
스토리지 노드 복구 작업의 일부로 어플라이언스 스토리지 노드 구축	복구 및 유지 관리 지침

관련 정보

설치 준비(SG6000)

하드웨어 설치(SG6000)

하드웨어 구성(SG6000)

그리드를 확장합니다

설치 준비(SG6000)

StorageGRID 어플라이언스 설치를 준비하는 과정에서 사이트 준비 및 필요한 모든 하드웨어, 케이블 및 도구 확보 작업이 수반됩니다. 또한 IP 주소와 네트워크 정보도 수집해야 합니다.

관련 정보

웹 브라우저 요구 사항

사이트 준비(SG6000)

제품을 설치하기 전에 StorageGRID 어플라이언스의 사양을 충족하는 사이트와 캐비닛 또는 랙이 맞는지 확인해야 합니다.

단계

1. 사이트가 온도, 습도, 고도 범위, 공기 흐름, 열 손실 요구 사항을 충족하는지 확인합니다. 배선, 전원 및 접지. 자세한 내용은 NetApp Hardware Universe를 참조하십시오.
2. 해당 지역에서 SGF6024용 SG6060 또는 120V AC 전원에 대해 240V AC 전원을 공급하는지 확인하십시오.
3. 이 크기의 선반에 맞게 19인치(48.3-cm) 캐비닛 또는 랙을 준비합니다(케이블 제외).

쉘프 유형	높이	너비	깊이	최대 중량
• E2860 컨트롤러 쉘프 * SG6060용	6.87in. (17.46cm)	17.66in. (44.86cm)	38.25in. (97.16cm)	250lb. (113kg)
• SG6060용 선택적 확장 쉘프 * (1개 또는 2개)	6.87in. (17.46cm)	17.66in. (44.86cm)	38.25in. (97.16cm)	250lb. (113kg)
SGF6024용 * EF570 컨트롤러 쉘프	3.35인치 (8.50cm)	17.66in. (44.86cm)	19.00인치 (48.26cm)	51.74lb. (23.47kg)
각 어플라이언스에 * SG6000-CN 컨트롤러 *	1.70in. (4.32cm)	17.32in. (44.0cm)	32.0in. (81.3cm)	39lb. (17.7kg)

4. 제품을 설치할 위치를 결정합니다.

> E2860 컨트롤러 쉘프 또는 선택적 확장 쉘프를 설치할 경우 장비가 넘어가지 않도록 랙 또는 캐비닛 맨 아래에 하드웨어를 설치하십시오. 가장 무거운 장비가 캐비닛 또는 랙의 하단에 있는지 확인하려면 E2860 컨트롤러 쉘프 및 확장 쉘프 위에 SG6000-CN 컨트롤러를 설치합니다.

설치를 시작하기 전에 제품과 함께 제공된 0.5m 광 케이블 또는 제공된 케이블이 계획된 레이아웃에 충분한지 확인하십시오.

관련 정보

"NetApp Hardware Universe를 참조하십시오"

"NetApp 상호 운용성 매트릭스 툴"

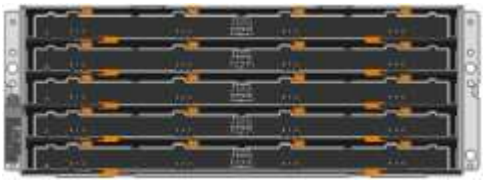
박스 포장 풀기**(SG6000)**

StorageGRID 제품을 설치하기 전에 모든 상자의 포장을 풀고 내용물을 포장 명세서에 있는 품목과 비교합니다.

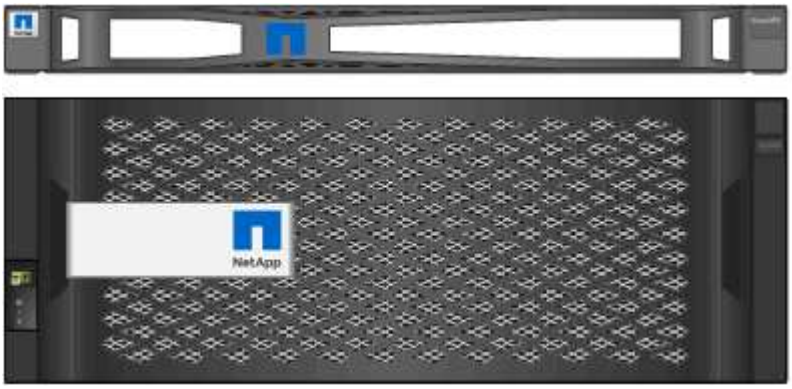
SG6060 및 **SG6060X**

- * SG6000-CN 컨트롤러 *

- * E2860 컨트롤러 쉘프, 드라이브 설치 안 됨 *

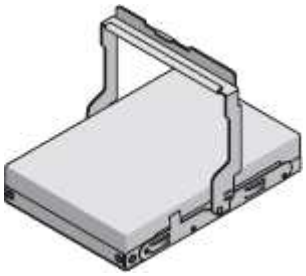


- * 전면 베젤 2개 *

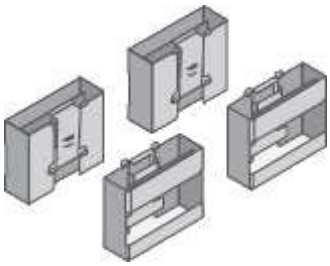


- * 지침이 포함된 레일 키트 2개 *

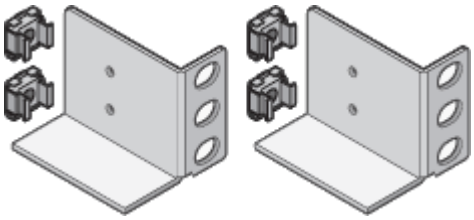
- 60개 드라이브(SSD 2개 및 NL-SAS 58개) *



- * 4개의 핸들 *



- * 사각 구멍 랙 설치용 후면 브래킷 및 케이지 너트 *

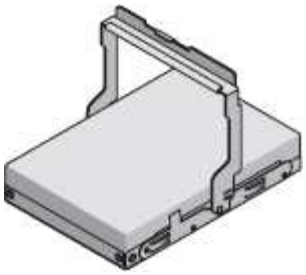


SG6060 및 **SG6060X** 확장 셸프

- * 드라이브가 설치되지 않은 확장 쉘프 *

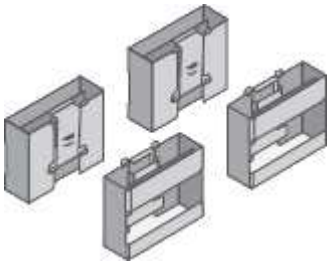
- * 전면 베젤 *

- * 60개의 NL-SAS 드라이브 *

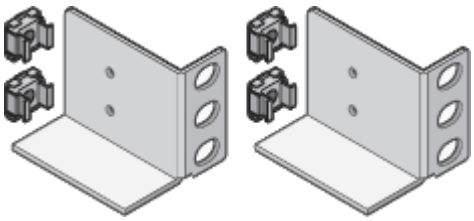


- * 지침이 포함된 레일 키트 1개 *

- * 4개의 핸들 *



- * 사각 구멍 랙 설치용 후면 브래킷 및 케이지 너트 *



SGF6024

- * SG6000-CN 컨트롤러 *

- * EF570 플래시 어레이(24개 SSD(Solid State) 드라이브 설치됨 *

- * 전면 베젤 2개 *

- * 지침이 포함된 레일 키트 2개 *

- * 선반 엔드캡 *

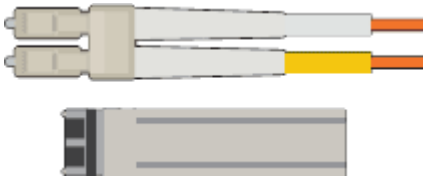
케이블 및 커넥터

StorageGRID 어플라이언스에는 다음과 같은 케이블 및 커넥터가 포함되어 있습니다.

- * 해당 국가용 전원 코드 4개 *

캐비닛에는 제품과 함께 제공된 전원 코드 대신 사용하는 특수 전원 코드가 있을 수 있습니다.

- * 광 케이블 및 SFP 트랜시버 *



FC 상호 연결 포트를 위한 광 케이블 4개

16Gb/s FC를 지원하는 SFP+ 트랜시버 4개

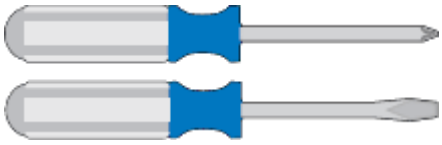
- * 선택 사항: 각 SG6060 또는 SG6060X 확장 셸프 연결용 SAS 케이블 2개 *

추가 장비 및 도구 확보**(SG6000)**

StorageGRID 제품을 설치하기 전에 필요한 추가 장비와 도구가 모두 있는지 확인하십시오.

하드웨어를 설치하고 구성하려면 다음 추가 장비가 필요합니다.

- * 스크류드라이버 *

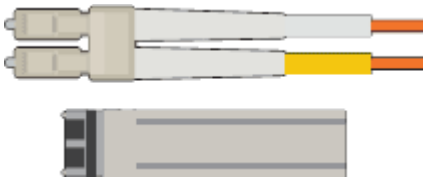


  필립스 번호 2 드라이버

  중형 일자 드라이버

- * ESD 손목 스트랩 *

- * 광 케이블 및 SFP 트랜시버 *



  다음 옵션 중 하나가 필요합니다.

  - SG6000-CN 컨트롤러에서 사용하려는 10/25-GbE 포트용 TwinAx 케이블 또는 광 케이블 1-4개
  - 광 케이블 및 10GbE 링크 속도를 사용할 경우 10/25-GbE 포트용 SFP+ 트랜시버 1-4개
  - 광 케이블과 25-GbE 링크 속도를 사용할 경우 10/25-GbE 포트용 SFP28 트랜시버 1~4개

- RJ-45(Cat5/Cat5e/Cat6) 이더넷 케이블 *

- * 서비스 노트북 *

지원되는 웹 브라우저

1GbE(RJ-45) 포트

- * 옵션 도구 *

Phillips 헤드 비트를 이용한 파워 드릴

플래시

60-드라이브 쉘프용 기계식 리프트

어플라이언스 네트워크 연결 검토**(SG6000)**

StorageGRID 어플라이언스를 설치하기 전에 어플라이언스에 연결할 수 있는 네트워크를 이해해야 합니다.

StorageGRID 어플라이언스를 StorageGRID 시스템에 스토리지 노드로 구축할 경우 다음 네트워크에 연결할 수 있습니다.

- * StorageGRID * 용 그리드 네트워크: 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용됩니다. 그리드에서 모든 사이트 및 서브넷의 모든 노드 간에 연결을 제공합니다. 그리드 네트워크가 필요합니다.
- StorageGRID*용 관리자 네트워크: 관리자 네트워크는 시스템 관리 및 유지 보수에 사용되는 폐쇄된 네트워크입니다. 관리 네트워크는 일반적으로 사설 네트워크이며 사이트 간에 라우팅할 필요가 없습니다. 관리 네트워크는 선택 사항입니다.
- * StorageGRID용 클라이언트 네트워크: * 클라이언트 네트워크는 S3 및 Swift를 포함한 클라이언트 애플리케이션에 대한 액세스를 제공하는 데 사용되는 개방형 네트워크입니다. 클라이언트 네트워크는 그리드에 대한 클라이언트 프로토콜 액세스를 제공하므로 그리드 네트워크를 격리하고 보호할 수 있습니다. 클라이언트 네트워크는 선택 사항입니다.
- * SANtricity 시스템 관리자용 관리 네트워크 * (선택 사항): 이 네트워크는 스토리지 컨트롤러의 SANtricity 시스템 관리자에 대한 액세스를 제공하므로 스토리지 컨트롤러 쉘프의 하드웨어 구성 요소를 모니터링하고 관리할 수

있습니다. 이 관리 네트워크는 StorageGRID용 관리 네트워크와 같을 수도 있고 독립 관리 네트워크일 수도 있습니다.

옵션 SANtricity System Manager 네트워크가 연결되지 않은 경우 일부 SANtricity 기능을 사용하지 못할 수 있습니다.

- * SG6000-CN 컨트롤러용 BMC 관리 네트워크 * (선택 사항): 이 네트워크는 SG6000-CN의 베이스보드 관리 컨트롤러에 대한 액세스를 제공하여 SG6000-CN 컨트롤러의 하드웨어 구성요소를 모니터링하고 관리할 수 있도록 합니다. 이 관리 네트워크는 StorageGRID용 관리 네트워크와 같을 수도 있고 독립 관리 네트워크일 수도 있습니다.

  선택적 BMC 관리 네트워크가 연결되지 않은 경우 일부 지원 및 유지 관리 절차를 수행하기가 더 어려워집니다. 지원 목적으로 필요한 경우를 제외하고 BMC 관리 네트워크를 연결하지 않은 상태로 둘 수 있습니다.

StorageGRID 네트워크에 대한 자세한 내용은 _Grid Primer_를 참조하십시오.

관련 정보

설치 정보 수집(SG6000)

케이블 어플라이언스(SG6000)

SG6000-CN 컨트롤러의 포트 결합 모드

네트워크 지침

SG6000-CN 컨트롤러의 포트 결합 모드

SG6000-CN에 대한 네트워크 링크를 구성할 때 Grid Network 및 선택적 Client Network에 연결되는 10/25-GbE 포트와 선택적 Admin Network에 연결되는 1GbE 관리 포트에 포트 결합을 사용할 수 있습니다. 포트 본딩을 사용하면 StorageGRID 네트워크와 어플라이언스 간에 중복 경로를 제공하여 데이터를 보호할 수 있습니다.

관련 정보

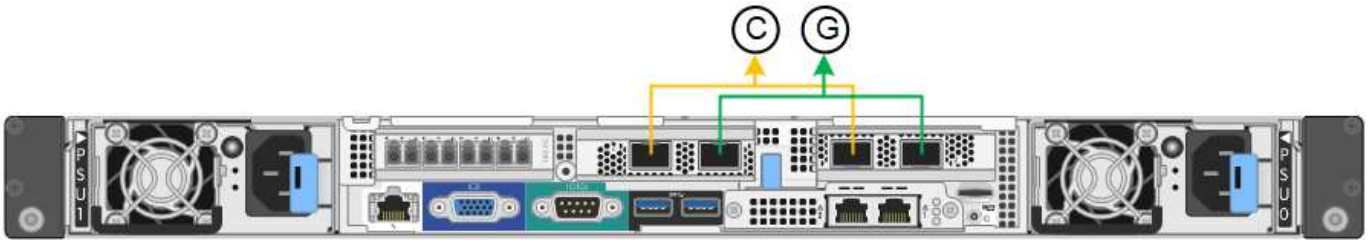
네트워크 링크 구성(SG6000)

10/25-GbE 포트의 네트워크 연결 모드

SG6000-CN 컨트롤러의 10/25-GbE 네트워킹 포트는 그리드 네트워크 및 클라이언트 네트워크 연결을 위한 고정 포트 결합 모드 또는 집계 포트 결합 모드를 지원합니다.

고정 포트 결합 모드

고정 모드는 10/25-GbE 네트워킹 포트의 기본 구성입니다.



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
c	이 네트워크를 사용하는 경우 포트 1과 3이 클라이언트 네트워크에 대해 함께 연결됩니다.
g	포트 2와 4는 그리드 네트워크를 위해 서로 연결되어 있습니다.

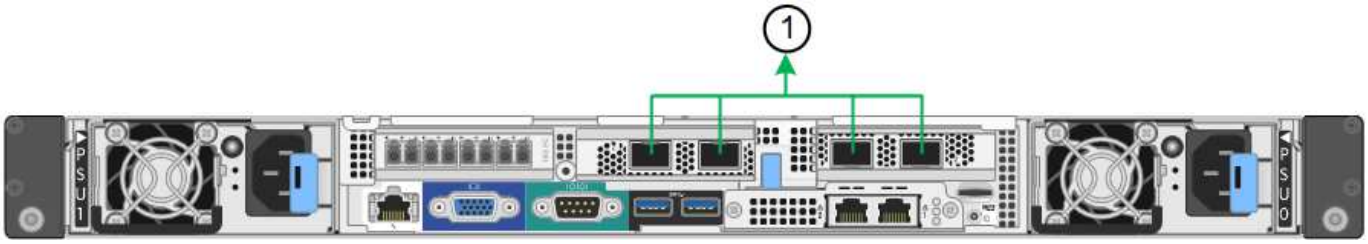
고정 포트 결합 모드를 사용할 때 포트는 액티브-백업 모드 또는 링크 통합 제어 프로토콜 모드(802.3ad)를 사용하여 본드 결합할 수 있습니다.

- 액티브-백업 모드(기본값)에서는 한 번에 하나의 포트만 활성화됩니다. 활성 포트에 장애가 발생하면 백업 포트가 자동으로 페일오버 연결을 제공합니다. 포트 4는 포트 2(그리드 네트워크)에 대한 백업 경로를 제공하고 포트 3은 포트 1(클라이언트 네트워크)에 대한 백업 경로를 제공합니다.
- LACP 모드에서 각 포트 쌍은 컨트롤러와 네트워크 간에 논리 채널을 형성하므로 더 높은 처리량을 허용합니다. 한 포트에 장애가 발생해도 다른 포트는 계속 채널을 제공합니다. 처리량은 감소하지만 연결성은 영향을 받지 않습니다.

> 중복 연결이 필요하지 않은 경우 각 네트워크에 대해 하나의 포트만 사용할 수 있습니다. 그러나 StorageGRID가 설치된 후 그리드 관리자에서 경고가 트리거되어 링크가 다운되었음을 나타냅니다. 이 포트는 의도적으로 분리되어 있으므로 이 알림을 안전하게 비활성화할 수 있습니다. Grid Manager에서 * Alert * > * Rules * 를 선택하고 규칙을 선택한 다음 * Edit rule * 을 클릭합니다. 그런 다음 * 사용 * 확인란의 선택을 취소합니다.

애그리게이트 포트 결합 모드

애그리게이트 포트 결합 모드는 각 StorageGRID 네트워크의 성능을 크게 높이고 추가 페일오버 경로를 제공합니다.



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
1	연결된 모든 포트는 단일 LACP 결합으로 그룹화되므로 모든 포트를 그리드 네트워크 및 클라이언트 네트워크 트래픽에 사용할 수 있습니다.

애그리게이트 포트 결합 모드를 사용하려는 경우:

- LACP 네트워크 결합 모드를 사용해야 합니다.
- 각 네트워크에 대해 고유한 VLAN 태그를 지정해야 합니다. 이 VLAN 태그는 네트워크 트래픽이 올바른 네트워크로 라우팅되도록 각 네트워크 패킷에 추가됩니다.
- VLAN 및 LACP를 지원할 수 있는 스위치에 포트를 연결해야 합니다. LACP 결합에 여러 스위치가 사용되는 경우 스위치는 MLAG(Multi-Chassis Link Aggregation Group) 또는 이와 동등한 스위치를 지원해야 합니다.

- VLAN, LACP, MLAG 또는 이와 동등한 기능을 사용하도록 스위치를 구성하는 방법을 이해해야 합니다.

4개의 10GbE 포트 모두를 사용하지 않으려면 1개, 2개 또는 3개의 포트를 사용할 수 있습니다. 둘 이상의 포트를 사용하면 10/25-GbE 포트 중 하나에 장애가 발생하더라도 일부 네트워크 연결이 계속 유지될 가능성을 극대화할 수 있습니다.

> 포트 수를 4개 이하로 선택하면 어플라이언스 노드가 설치된 후 그리드 관리자에서 * 서비스 어플라이언스 연결 해제 * 경고가 트리거되어 케이블이 분리되었음을 나타냅니다. 트리거된 경고에 대해 이 경고 규칙을 안전하게 비활성화할 수 있습니다. Grid Manager에서 * alerts * > * rules * 를 선택하고 규칙을 선택한 다음 * Edit rule * 을 클릭합니다. 그런 다음 * 사용 * 확인란의 선택을 취소합니다.

1GbE 관리 포트의 네트워크 연결 모드

SG6000-CN 컨트롤러의 1GbE 관리 포트 2개의 경우 독립 네트워크 연결 모드 또는 Active-Backup 네트워크 연결 모드를 선택하여 선택적 관리 네트워크에 연결할 수 있습니다.

독립 모드에서는 왼쪽에 있는 관리 포트만 관리 네트워크에 연결됩니다. 이 모드는 중복 경로를 제공하지 않습니다. 오른쪽의 관리 포트가 연결되어 있지 않으며 임시 로컬 연결에 사용할 수 있습니다(IP 주소 169.254.0.1 사용).

Active-Backup 모드에서는 두 관리 포트가 모두 관리 네트워크에 연결됩니다. 한 번에 하나의 포트만 활성화됩니다. 활성 포트에 장애가 발생하면 백업 포트가 자동으로 페일오버 연결을 제공합니다. 이러한 두 개의 물리적 포트를 하나의 논리 관리 포트에 연결하면 관리 네트워크에 대한 중복 경로가 제공됩니다.

> 1GbE 관리 포트가 Active-Backup 모드로 구성되어 있을 때 SG6000-CN 컨트롤러에 일시적으로 로컬 연결이 필요한 경우 두 관리 포트에서 케이블을 분리하고 오른쪽의 관리 포트에 임시 케이블을 연결한 다음 IP 주소 169.254.0.1을 사용하여 어플라이언스에 액세스합니다.

속성 표시기	네트워크 연결 모드
A	두 관리 포트는 모두 관리 네트워크에 연결된 하나의 논리 관리 포트에 연결됩니다.
나는	왼쪽의 포트는 관리 네트워크에 연결되어 있습니다. 오른쪽의 포트는 임시 로컬 연결(IP 주소 169.254.0.1)에 사용할 수 있습니다.

설치 정보 수집**(SG6000)**

StorageGRID 어플라이언스를 설치 및 구성할 때 이더넷 스위치 포트, IP 주소, 포트 및 네트워크 연결 모드에 대한 정보를 결정하고 수집해야 합니다.

이 작업에 대해

다음 표를 사용하여 어플라이언스에 연결하는 각 네트워크에 필요한 정보를 기록할 수 있습니다. 이러한 값은 하드웨어를 설치하고 구성하는 데 필요합니다.

스토리지 컨트롤러의 **SANtricity System Manager**에 연결하는 데 필요한 정보입니다

어플라이언스(E2800 시리즈 컨트롤러 또는 EF570 컨트롤러)의 두 스토리지 컨트롤러를 SANtricity 시스템 관리자에 사용할 관리 네트워크에 연결해야 합니다. 컨트롤러는 각 어플라이언스에 다음과 같이 있습니다.

- SG6060 및 SG6060X: 컨트롤러 A가 상단에 있고 컨트롤러 B가 하단에 있습니다.
- SGF6024: 컨트롤러 A는 왼쪽에 있고 컨트롤러 B는 오른쪽에 있습니다.

정보가 필요합니다	컨트롤러 **A**의 가치	컨트롤러 **B**의 값입니다
관리 포트 1에 연결할 이더넷 스위치 포트(E2800A 컨트롤러의 경우 P1, E2800B 컨트롤러의 경우 0a 레이블)		
관리 포트 1의 MAC 주소(E2800A 컨트롤러의 포트 P1 및 E2800B 컨트롤러의 0a 근처에 있는 레이블에 인쇄되어 있음)		
전원을 켠 후 사용할 수 있는 경우 관리 포트 1에 대해 DHCP 할당 IP 주소입니다 • 참고: * 스토리지 컨트롤러에 연결할 네트워크에 DHCP 서버가 포함된 경우 네트워크 관리자는 MAC 주소를 사용하여 DHCP 서버에서 할당한 IP 주소를 확인할 수 있습니다.		
관리 네트워크에서 어플라이언스에 사용할 고정 IP 주소입니다	IPv4의 경우: • IPv4 주소: • 서브넷 마스크: • 게이트웨이: IPv6의 경우: • IPv6 주소: • 라우팅 가능한 IP 주소: • 스토리지 컨트롤러 라우터 IP 주소:	IPv4의 경우: • IPv4 주소: • 서브넷 마스크: • 게이트웨이: IPv6의 경우: • IPv6 주소: • 라우팅 가능한 IP 주소: • 스토리지 컨트롤러 라우터 IP 주소:

정보가 필요합니다	컨트롤러 **A**의 가치	컨트롤러 **B**의 값입니다
IP 주소 형식입니다	다음 중 하나를 선택하십시오. • IPv4 • IPv6	다음 중 하나를 선택하십시오. • IPv4 • IPv6
속도 및 이중 모드 • 참고: * SANtricity 시스템 관리자 관리 네트워크의 이더넷 스위치가 자동 교섭으로 설정되어 있는지 확인해야 합니다.	반드시: • 자동 협상(기본값)	반드시: • 자동 협상(기본값)

SG6000-CN 컨트롤러를 관리 네트워크에 연결하는 데 필요한 정보입니다

StorageGRID용 관리 네트워크는 시스템 관리 및 유지 보수에 사용되는 선택적 네트워크입니다. 어플라이언스는 SG6000-CN 컨트롤러의 다음 1GbE 관리 포트를 사용하여 관리 네트워크에 연결됩니다.

정보가 필요합니다	귀사의 가치
관리자 네트워크가 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요 • 예(기본값)
네트워크 연결 모드	다음 중 하나를 선택하십시오. • 독립(기본값) • Active - 백업
다이어그램의 빨간색 원에 있는 왼쪽 포트의 스위치 포트(독립 네트워크 연결 모드의 기본 활성 포트)	
다이어그램의 빨간색 원에 있는 오른쪽 포트의 스위치 포트(액티브-백업 네트워크 연결 모드만 해당)	

정보가 필요합니다	귀사의 가치
관리자 네트워크 포트의 MAC 주소입니다 • 참고: * SG6000-CN 컨트롤러 전면에 있는 MAC 주소 레이블에는 BMC 관리 포트의 MAC 주소가 나열됩니다. 관리 네트워크 포트의 MAC 주소를 확인하려면 레이블의 16진수에 * 2 * 를 추가해야 합니다. 예를 들어 레이블의 MAC 주소가 * 09 * 로 끝나는 경우 관리 포트의 MAC 주소는 * 0B * 로 끝납니다. 레이블의 MAC 주소가 * (*y*) FF * 로 끝나는 경우 관리 포트의 MAC 주소는 * (*y*+1) 01 * 로 끝납니다. Windows에서 계산기를 열고, Programmer 모드로 설정하고, Hex를 선택하고, MAC 주소를 입력한 다음, * + 2 = * 를 입력하여 이 계산을 쉽게 수행할 수 있습니다.	
전원을 켠 후 사용할 수 있는 경우, Admin Network 포트에 대해 DHCP가 할당한 IP 주소입니다 • 참고: * MAC 주소를 사용하여 할당된 IP를 조회하여 DHCP 할당 IP 주소를 확인할 수 있습니다.	• IPv4 주소(CIDR): • 게이트웨이:
관리 네트워크의 어플라이언스 스토리지 노드에 사용할 고정 IP 주소입니다 • 참고: * 네트워크에 게이트웨이가 없는 경우 게이트웨이에 대해 동일한 정적 IPv4 주소를 지정합니다.	• IPv4 주소(CIDR): • 게이트웨이:
관리 네트워크 서브넷(CIDR)	

SG6000-CN 컨트롤러에서 **10/25-GbE** 포트를 연결하고 구성하는 데 필요한 정보입니다

SG6000-CN 컨트롤러의 10/25-GbE 포트 4개는 StorageGRID 그리드 네트워크 및 선택적 클라이언트 네트워크에 연결됩니다.

정보가 필요합니다	귀사의 가치
링크 속도	다음 중 하나를 선택하십시오. • 자동(기본값) • 10GbE • 25GbE

정보가 필요합니다	귀사의 가치
포트 결합 모드	다음 중 하나를 선택하십시오. • 고정(기본값) • 집계
포트 1용 스위치 포트(고정 모드용 클라이언트 네트워크)	
포트 2용 스위치 포트(고정 모드용 그리드 네트워크)	
포트 3용 스위치 포트(고정 모드용 클라이언트 네트워크)	
포트 4용 스위치 포트(고정 모드용 그리드 네트워크)	

SG6000-CN 컨트롤러를 그리드 네트워크에 연결하는 데 필요한 정보

StorageGRID용 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용되는 필수 네트워크입니다. 어플라이언스는 SG6000-CN 컨트롤러의 10/25-GbE 포트를 사용하여 그리드 네트워크에 연결됩니다.

정보가 필요합니다	귀사의 가치
네트워크 연결 모드	다음 중 하나를 선택하십시오. • Active-Backup(기본값) • LACP(802.3ad)
VLAN 태그 지정이 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요(기본값) • 예
VLAN 태그(VLAN 태그 지정이 활성화된 경우)	0에서 4095 사이의 값을 입력합니다.
전원을 켠 후 사용할 수 있는 경우 그리드 네트워크에 대해 DHCP 할당 IP 주소입니다	• IPv4 주소(CIDR): • 게이트웨이:
그리드 네트워크에서 어플라이언스 스토리지 노드에 사용할 고정 IP 주소입니다 • 참고: * 네트워크에 게이트웨이가 없는 경우 게이트웨이에 대해 동일한 정적 IPv4 주소를 지정합니다.	• IPv4 주소(CIDR): • 게이트웨이:
그리드 네트워크 서브넷(CIDR)	

SG6000-CN 컨트롤러를 클라이언트 네트워크에 연결하는 데 필요한 정보입니다

StorageGRID용 클라이언트 네트워크는 일반적으로 그리드에 대한 클라이언트 프로토콜 액세스를 제공하는 데 사용되는 선택적 네트워크입니다. 어플라이언스는 SG6000-CN 컨트롤러의 10/25-GbE 포트를 사용하여 클라이언트 네트워크에 연결됩니다.

정보가 필요합니다	귀사의 가치
클라이언트 네트워크가 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요(기본값) • 예
네트워크 연결 모드	다음 중 하나를 선택하십시오. • Active-Backup(기본값) • LACP(802.3ad)
VLAN 태그 지정이 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요(기본값) • 예
VLAN 태그(VLAN 태그 지정이 활성화된 경우)	0에서 4095 사이의 값을 입력합니다.
전원을 켠 후 사용할 수 있는 경우 클라이언트 네트워크에 대해 DHCP 할당 IP 주소입니다	• IPv4 주소(CIDR): • 게이트웨이:
클라이언트 네트워크의 어플라이언스 스토리지 노드에 사용할 고정 IP 주소입니다 • 참고: * 클라이언트 네트워크가 활성화된 경우 컨트롤러의 기본 라우트는 여기에 지정된 게이트웨이를 사용합니다.	• IPv4 주소(CIDR): • 게이트웨이:

SG6000-CN 컨트롤러를 **BMC** 관리 네트워크에 연결하는 데 필요한 정보입니다

다음 1GbE 관리 포트를 사용하여 SG6000-CN 컨트롤러의 BMC 인터페이스에 액세스할 수 있습니다. 이 포트는 IPMI(Intelligent Platform Management Interface) 표준을 사용하여 이더넷을 통한 컨트롤러 하드웨어의 원격 관리를 지원합니다.

정보가 필요합니다	귀사의 가치
BMC 관리 포트에 연결할 이더넷 스위치 포트 (다이어그램에서 원으로 표시됨)	
전원을 켠 후 사용할 수 있는 경우 BMC 관리 네트워크에 대해 DHCP 할당 IP 주소입니다	• IPv4 주소(CIDR): • 게이트웨이:
BMC 관리 포트에 사용할 고정 IP 주소입니다	• IPv4 주소(CIDR): • 게이트웨이:

관련 정보

SG6000 어플라이언스의 컨트롤러

어플라이언스 네트워크 연결 검토(SG6000)

SG6000-CN 컨트롤러의 포트 결합 모드

케이블 어플라이언스(SG6000)

StorageGRID IP 주소를 구성합니다

하드웨어 설치(SG6000)

하드웨어 설치에는 SG6000-CN 컨트롤러 및 스토리지 컨트롤러 쉘프를 캐비닛 또는 랙에 설치하고, 케이블을 연결하고, 전원을 적용해야 합니다.

하드웨어 등록

어플라이언스 하드웨어를 등록하면 지원 혜택이 제공됩니다.

단계

1. 스토리지 컨트롤러 쉘프의 섀시 일련 번호를 찾습니다.

   포장 명세서, 확인 이메일 또는 제품의 포장을 푼 후 제품에서 번호를 확인할 수 있습니다.

   > 스토리지 어플라이언스에는 여러 개의 일련 번호가 있습니다. 스토리지 컨트롤러 쉘프의 일련 번호는 어플라이언스에 대한 서비스 또는 지원을 호출할 때 등록하고 사용해야 하는 일련 번호입니다.

2. NetApp Support 사이트 로 이동합니다 "mysupport.netapp.com".
3. 하드웨어를 등록해야 하는지 여부를 확인합니다.

귀하의 경우...	다음 단계를 따르십시오...
더 많은 워크로드 추가)	a. 사용자 이름과 암호를 사용하여 로그인합니다. b. 제품 * > * 내 제품 * 을 선택합니다. c. 새 일련 번호가 나열되는지 확인합니다. d. 그렇지 않은 경우 새 NetApp 고객에 대한 지침을 따르십시오.
신규 NetApp 고객	a. 지금 등록 * 을 클릭하고 계정을 만듭니다. b. 제품 * > * 제품 등록 * 을 선택합니다. c. 제품 일련 번호 및 요청된 세부 정보를 입력합니다. 등록이 승인되면 필요한 소프트웨어를 다운로드할 수 있습니다. 승인 프로세스는 최대 24시간이 걸릴 수 있습니다.

SG6060 및 **SG6060X:** 캐비닛 또는 랙에 **60** 드라이브 쉘프를 설치합니다

E2860 컨트롤러 쉘프에 대한 레일 세트를 캐비닛 또는 랙에 설치한 다음 컨트롤러 쉘프를 레일 위로 밀어 추가해야 합니다. 60-드라이브 확장 쉘프를 설치하는 경우, 같은 절차가 적용됩니다.

필요한 것

- 상자에 포함된 안전 고지 문서를 검토하고 하드웨어 이동 및 설치에 대한 예방 조치를 이해했습니다.
- 레일 키트와 함께 제공된 지침이 있습니다.

각 60-드라이브 쉘프의 중량은 드라이브를 설치하지 않고 약 60kg(132lb)입니다. 선반을 안전하게 이동하려면 4명 또는 기계화된 리프트가 필요합니다.

하드웨어 손상을 방지하려면 드라이브가 설치된 경우 쉘프를 이동하지 마십시오. 쉘프를 이동하기 전에 모든 드라이브를 제거해야 합니다.

E2860 컨트롤러 쉘프 또는 선택적 확장 쉘프를 설치할 경우 장비가 넘어가지 않도록 랙 또는 캐비닛 맨 아래에 하드웨어를 설치하십시오. 가장 무거운 장비가 캐비닛 또는 랙의 하단에 있는지 확인하려면 E2860 컨트롤러 쉘프 및 확장 쉘프 위에 SG6000-CN 컨트롤러를 설치합니다.

설치를 시작하기 전에 제품과 함께 제공된 0.5m 광 케이블 또는 제공된 케이블이 계획된 레이아웃에 충분한지 확인하십시오.

단계

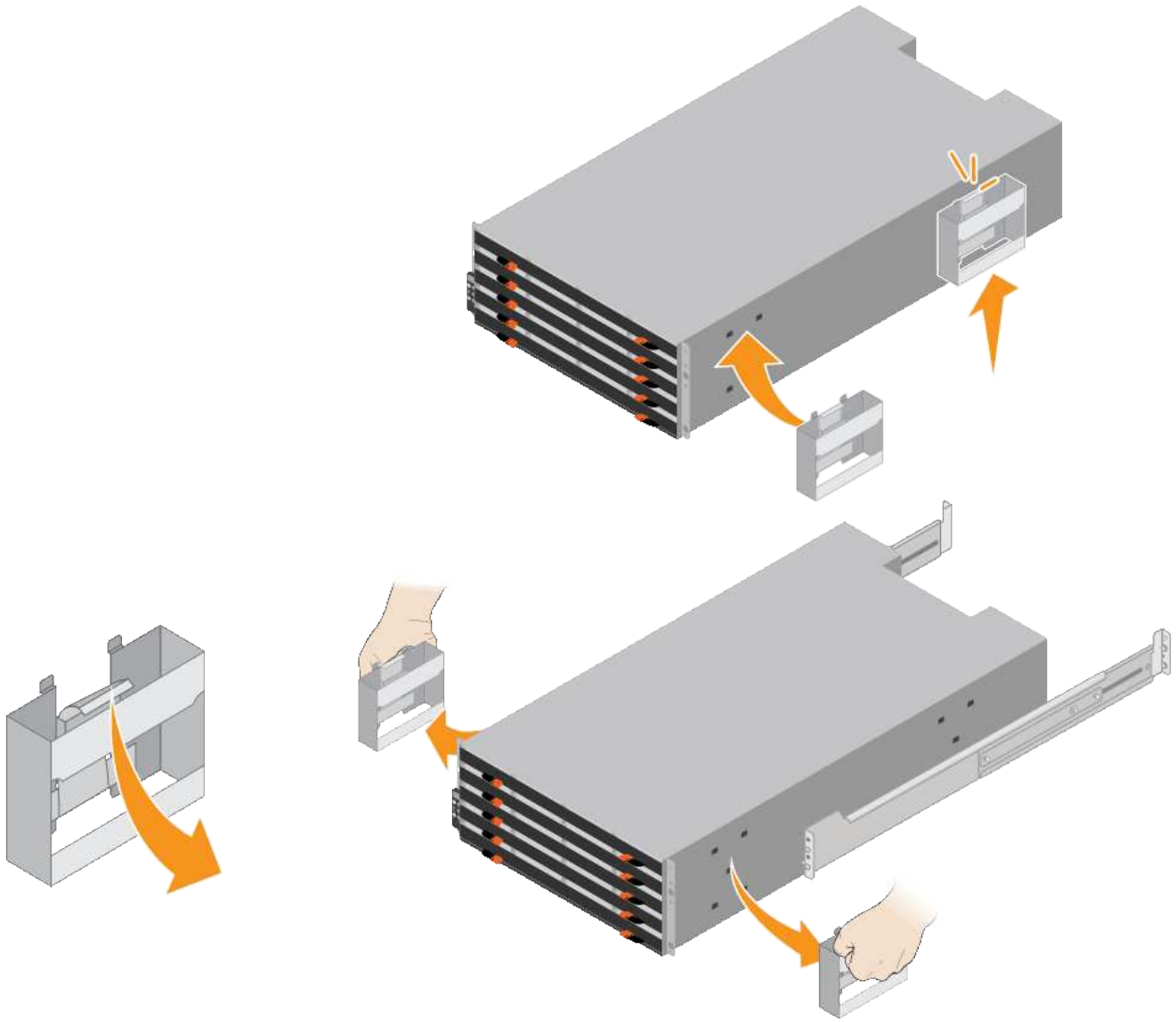
1. 레일 키트의 지침에 따라 캐비닛이나 랙에 레일을 설치합니다.

   사각 구멍 캐비닛의 경우, 먼저 제공된 케이지 너트를 설치하여 선반의 전면과 후면을 나사로 고정해야 합니다.

2. 제품의 외부 포장 박스를 분리하십시오. 그런 다음 안쪽 상자의 플랩을 아래로 접습니다.

3. 제품을 손으로 들어올리는 경우 4개의 손잡이를 섀시 측면에 부착하십시오.

   딸깍 소리가 나면서 제자리에 고정될 때까지 각 손잡이를 위로 밉니다.



4. 선반 후면(커넥터가 있는 끝)을 레일에 놓습니다.
5. 하단에서 쉘프를 지지한 다음 캐비닛에 밀어 넣습니다. 핸들을 사용하는 경우, 엄지 래치를 사용하여 쉘프를 밀어 넣을 때 한 번에 하나의 핸들을 분리합니다.

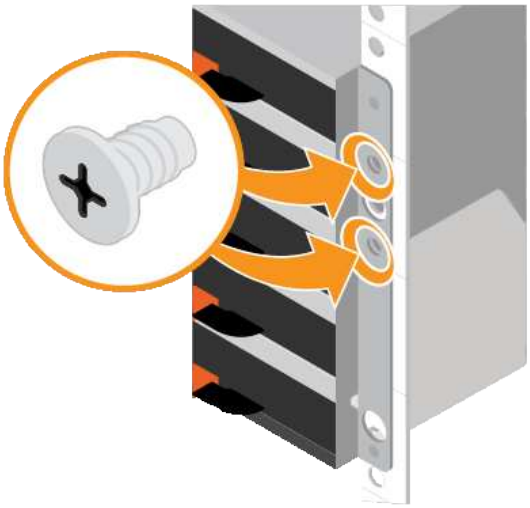
   핸들을 분리하려면 분리 래치를 뒤로 당기고 아래로 누른 다음 쉘프를 당겨 빼냅니다.

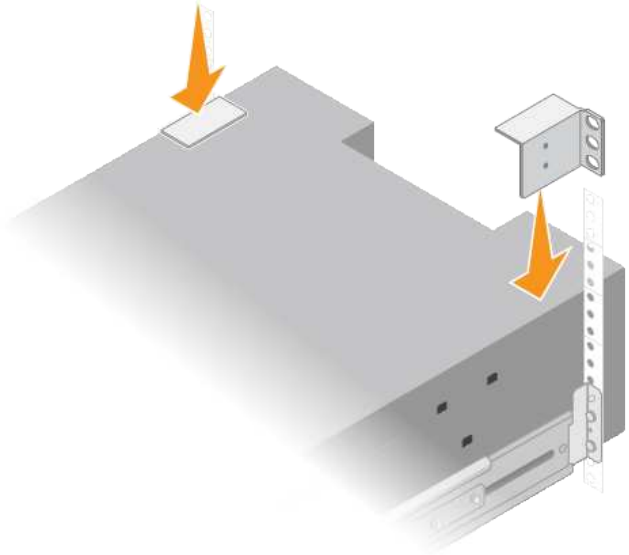
6. 선반을 캐비닛 전면에 고정합니다.

   양쪽의 선반 상단에서 첫 번째 및 세 번째 구멍에 나사를 삽입합니다.

7. 캐비닛 후면에 쉘프를 고정합니다.

   선반 상단 후면 섹션의 양쪽에 후면 브래킷 2개를 놓습니다. 각 브래킷의 첫 번째 및 세 번째 구멍에 나사를 삽입합니다.





8. 모든 확장 쉘프에 대해 이 단계를 반복합니다.

SG6060 및 **SG6060X:** 드라이브를 설치합니다

60-드라이브 쉘프를 캐비닛 또는 랙에 설치한 후에는 60개 드라이브를 모두 쉘프에 설치해야 합니다. E2860 컨트롤러 쉘프에 장착되는 2개의 SSD 드라이브가 포함되어 있으므로 컨트롤러 쉘프의 상단 서랍에 설치해야 합니다. 각 옵션 확장 쉘프에는 HDD 드라이브 60개 및 SSD 드라이브가 없습니다.

필요한 것

E2860 컨트롤러 쉘프 또는 옵션 확장 쉘프(1개 또는 2개)를 캐비닛 또는 랙에 설치했습니다.

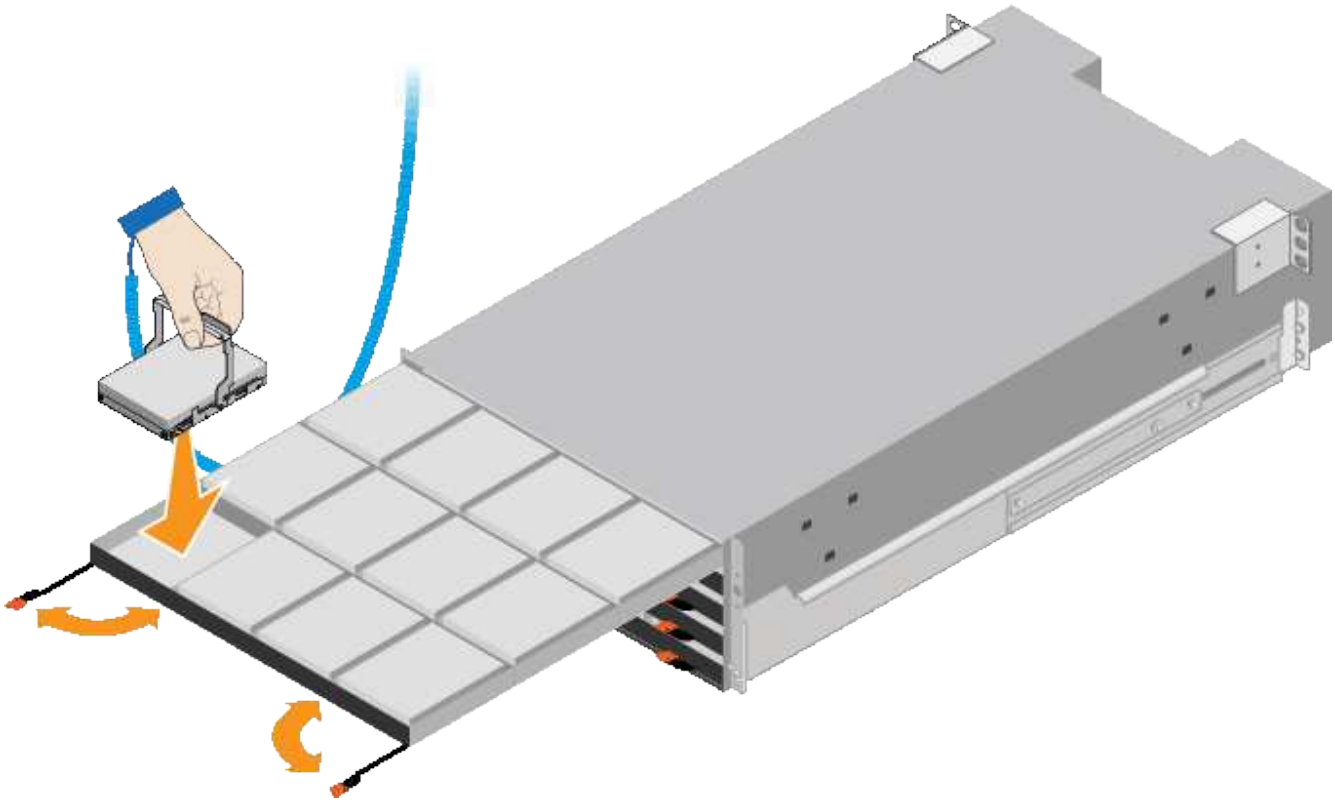
> 하드웨어 손상을 방지하려면 드라이브가 설치된 경우 쉘프를 이동하지 마십시오. 쉘프를 이동하기 전에 모든 드라이브를 제거해야 합니다.

단계

1. ESD 밴드의 스트랩 끝을 손목 둘레에 감고 클립 끝을 금속 바닥에 단단히 고정하여 정전기 방전을 방지하십시오.
2. 포장에서 드라이브를 꺼냅니다.
3. 상단 드라이브 드로어의 레버를 분리하고 레버를 사용하여 드로어를 밀어 꺼냅니다.
4. SSD 드라이브 2개를 찾습니다.

> 확장 쉘프에서는 SSD 드라이브를 사용하지 않습니다.

5. 각 구동 핸들을 수직 위치로 올립니다.
6. 슬롯 0 및 1에 SSD 드라이브 2개를 설치합니다(드로어의 왼쪽에 있는 처음 두 슬롯).
7. 각 드라이브를 해당 슬롯에 조심스럽게 넣고 딸깍 소리가 나면서 제자리에 고정될 때까지 들어 올린 드라이브 핸들을 내립니다.



8. 상단 드로어에 HDD 드라이브 10개를 설치합니다.
9. 중앙을 밀고 양쪽 레버를 부드럽게 닫아 드로어를 다시 밀어 넣습니다.

> 바인딩이 느껴지면 서랍을 미는 작업을 중단합니다. 드로어 전면의 분리 레버를 사용하여 드로어를 뒤로 밉니다. 그런 다음 서랍을 슬롯에 조심스럽게 다시 넣습니다.

10. 이 단계를 반복하여 HDD 드라이브를 다른 4개의 드로어에 설치합니다.

> 올바르게 작동하려면 60개의 드라이브를 모두 설치해야 합니다.

11. 전면 베젤을 쉘프에 연결합니다.
12. 확장 쉘프가 있는 경우, 다음 단계를 반복하여 각 확장 쉘프의 각 서랍에 12개의 HDD 드라이브를 설치합니다.
13. 캐비닛 또는 랙에 SG6000-CN을 설치하는 지침을 따르십시오.

SGF6024: 캐비닛 또는 랙에 **24** 드라이브 쉘프를 설치합니다

캐비닛 또는 랙에 EF570 컨트롤러 셸프용 레일 세트를 설치한 다음 레일을 따라 어레이를 밀어 올려야 합니다.

필요한 것

- 상자에 포함된 안전 고지 문서를 검토하고 하드웨어 이동 및 설치에 대한 예방 조치를 이해했습니다.
- 레일 키트와 함께 제공된 지침이 있습니다.

단계

1. 레일 키트의 지침에 따라 캐비닛이나 랙에 레일을 설치합니다.

사각 구멍 캐비닛의 경우, 먼저 제공된 케이지 너트를 설치하여 선반의 전면과 후면을 나사로 고정해야 합니다.

2. 제품의 외부 포장 박스를 분리하십시오. 그런 다음 안쪽 상자의 플랩을 아래로 접습니다.
3. 선반 후면(커넥터가 있는 끝)을 레일에 놓습니다.

> 완전히 장착된 선반의 중량은 약 24kg(52lb)입니다. 인클로저를 안전하게 옮기려면 두 사람이 필요합니다.

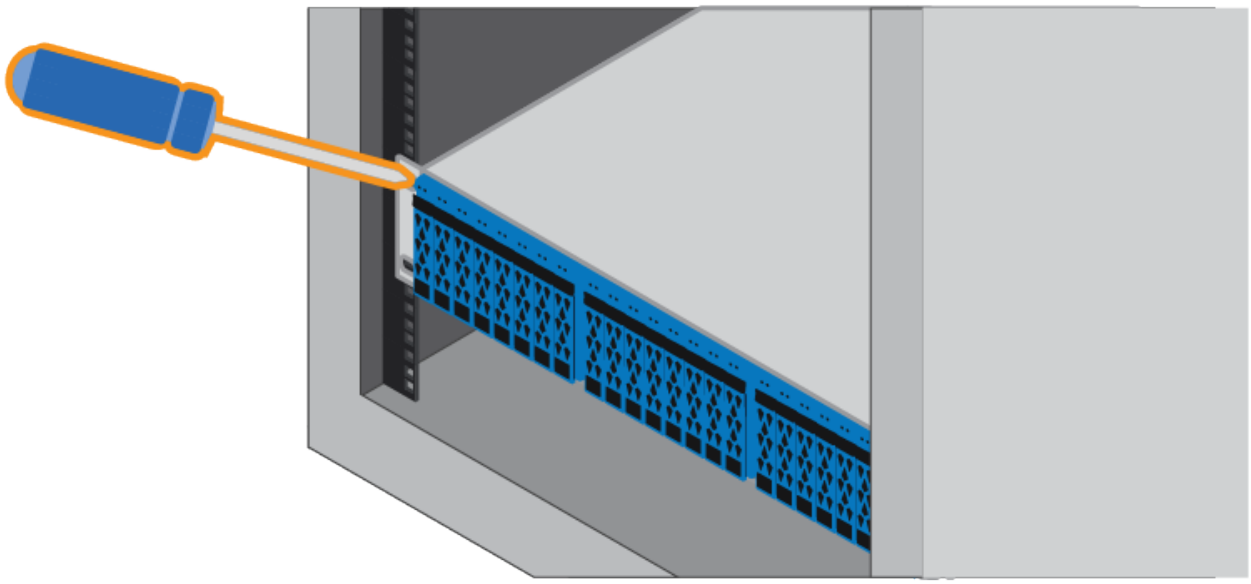
4. 엔클로저를 조심스럽게 레일 위로 끝까지 밀어 넣습니다.

> 엔클로저가 레일에 완전히 장착되도록 레일을 조정해야 할 수 있습니다.

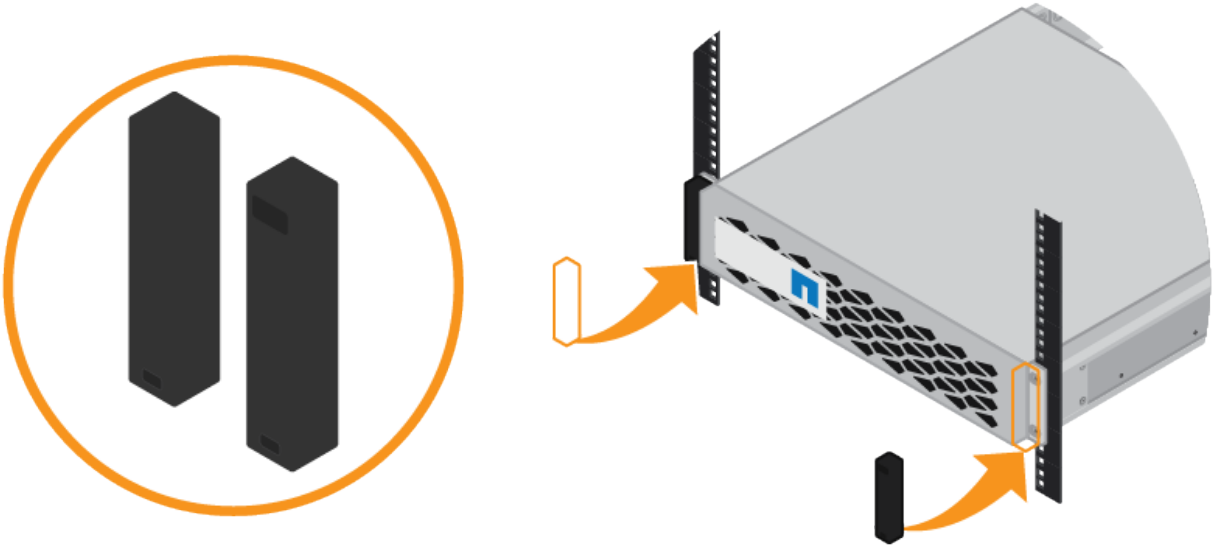
> 엔클로저 설치를 완료한 후에는 레일에 추가 장비를 놓지 마십시오. 레일은 추가 중량을 지지하도록 설계되지 않았습니다.

> 해당하는 경우, 인클로저를 랙 포스트에 고정하기 위해 선반 엔드 캡 또는 시스템 베젤을 분리해야 할 수 있습니다. 그럴 경우, 작업을 마친 후 엔드 캡이나 베젤을 교체해야 합니다.

5. 장착 브래킷(인클로저 전면 양쪽에 사전 설치), 랙 또는 시스템 캐비닛의 구멍 및 레일 전면의 구멍을 통해 M5 나사 2개를 삽입하여 캐비닛이나 랙 및 레일의 전면에 엔클로저를 고정합니다.



6. 엔클로저 및 레일 키트 브래킷의 브래킷을 통해 M5 나사 2개를 삽입하여 엔클로저를 레일 후면에 고정합니다.
7. 해당하는 경우 쉘프 엔드 캡 또는 시스템 베젤을 교체합니다.



SG6000-CN: 캐비닛 또는 랙에 설치합니다

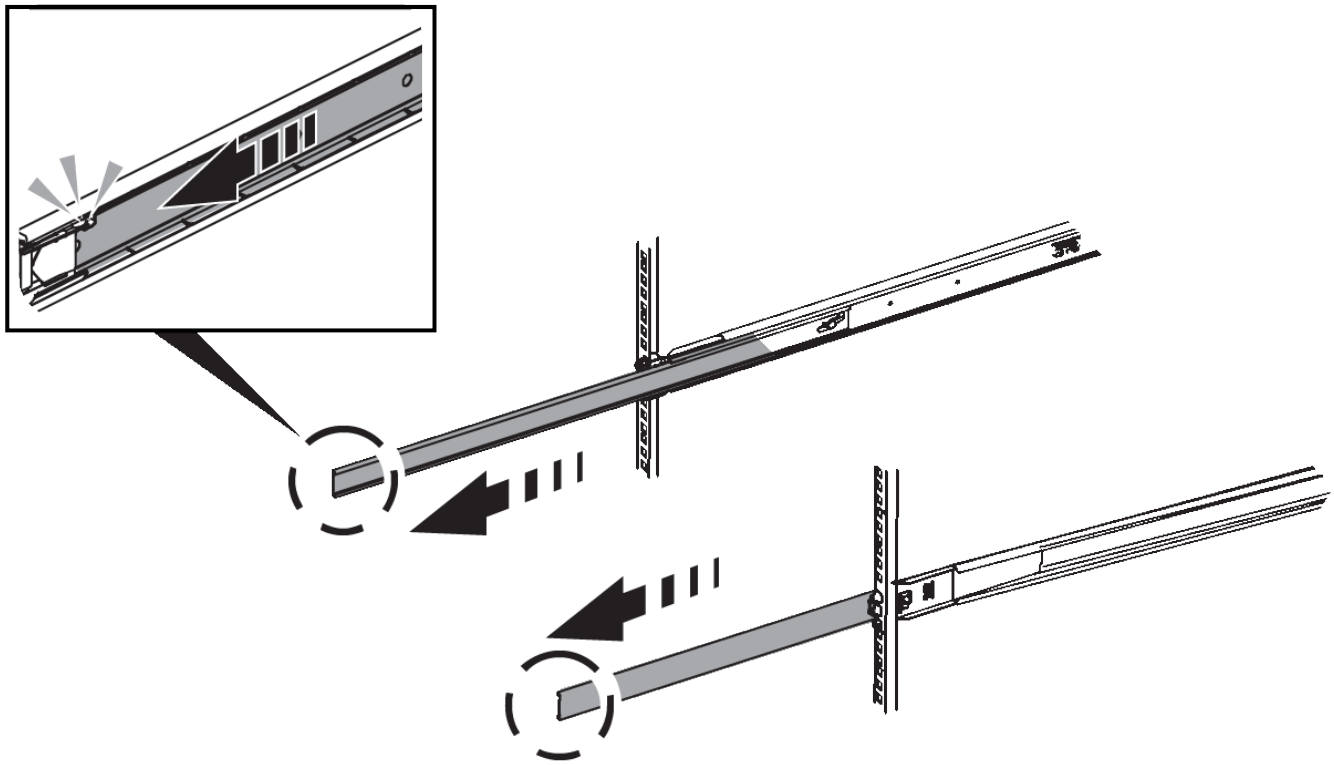
캐비닛 또는 랙에 SG6000-CN 컨트롤러용 레일 세트를 설치한 다음 레일을 따라 컨트롤러를 밀어넣습니다.

필요한 것

- 상자에 포함된 안전 고지 문서를 검토하고 하드웨어 이동 및 설치에 대한 예방 조치를 이해했습니다.
- 레일 키트와 함께 제공된 지침이 있습니다.
- E2860 컨트롤러 쉘프 및 드라이브 또는 EF570 컨트롤러 쉘프를 설치했습니다.

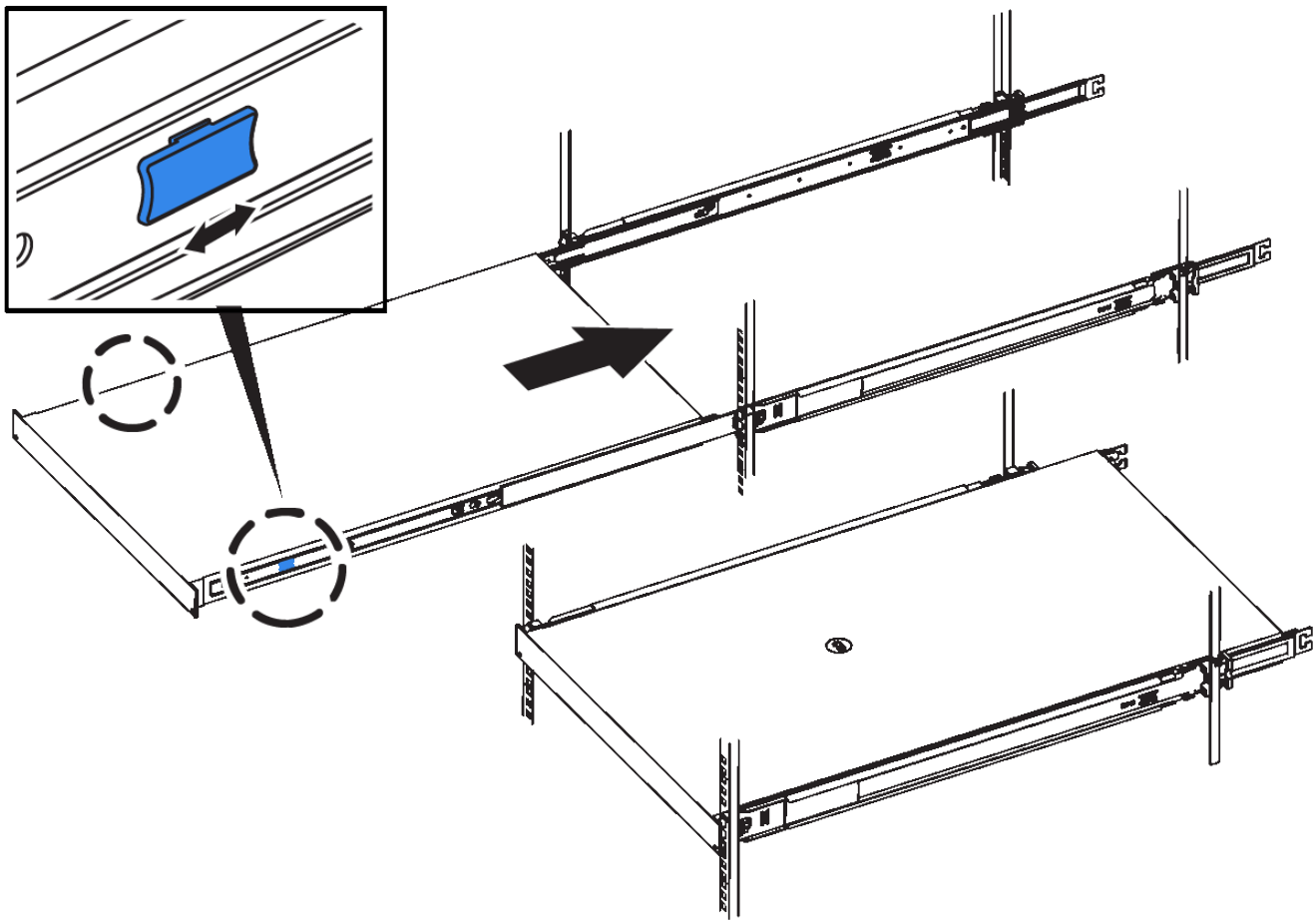
단계

1. 레일 키트의 지침에 따라 캐비닛이나 랙에 레일을 설치합니다.
2. 캐비닛이나 랙에 설치된 두 개의 레일에서 딸깍 소리가 날 때까지 레일의 이동식 부품을 확장합니다.



3. SG6000-CN 컨트롤러를 레일에 삽입합니다.
4. 캐비닛이나 랙에 컨트롤러를 밀어 넣습니다.

   컨트롤러를 더 이상 이동할 수 없는 경우 섀시 양쪽에 있는 파란색 래치를 당겨 컨트롤러를 완전히 밀어 넣습니다.



컨트롤러의 전원을 켜기 전에는 전면 베젤을 연결하지 마십시오.

5. 컨트롤러 전면 패널의 조임 나사를 조여 컨트롤러를 랙에 고정합니다.

케이블 어플라이언스**(SG6000)**

스토리지 컨트롤러를 SG6000-CN 컨트롤러에 연결하고, 세 컨트롤러 모두의 관리 포트를 연결하고, SG6000-CN 컨트롤러의 네트워크 포트를 StorageGRID용 그리드 네트워크 및 선택적 클라이언트 네트워크에 연결해야 합니다.

필요한 것

- 스토리지 컨트롤러 2개를 SG6000-CN 컨트롤러에 연결하기 위해 어플라이언스와 함께 제공된 광 케이블 4개가 있습니다.
- 관리 포트를 연결하기 위한 RJ-45 이더넷 케이블(최소 4개)이 있습니다.
- 네트워크 포트에 대한 다음 옵션 중 하나가 있습니다. 이러한 품목은 제품과 함께 제공되지 않습니다.
  - 4개의 네트워크 포트를 연결하기 위한 TwinAx 케이블 1-4개.

◦ 포트에 광 케이블을 사용하려는 경우 SFP+ 또는 SFP28 트랜시버 1~4개

> * 레이저 방사선에 노출될 위험 * — SFP 트랜시버를 분해하거나 제거하지 마십시오. 레이저 방사선에 노출될 수 있습니다.

이 작업에 대해

이 섹션에서는 다음 장비의 케이블 연결에 대한 지침을 제공합니다.

- SG6060 및 SG6060X
- SGF6024

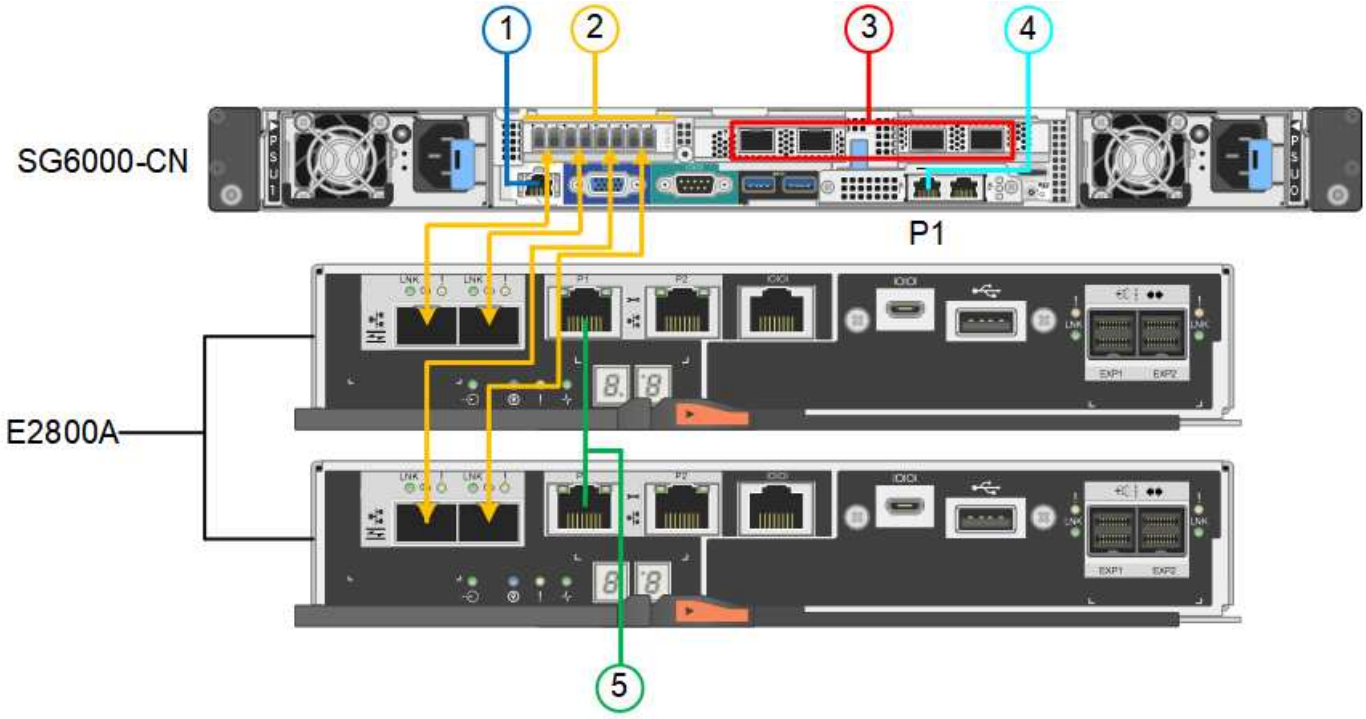
SG6060 또는 **SG6060X**에 케이블을 연결합니다

다음 그림은 SG6060 및 SG6060X 어플라이언스의 컨트롤러 3개와 SG6000-CN 컴퓨팅 컨트롤러가 상단에, E2800 스토리지 컨트롤러 2개가 아래쪽에 있는 모습입니다.

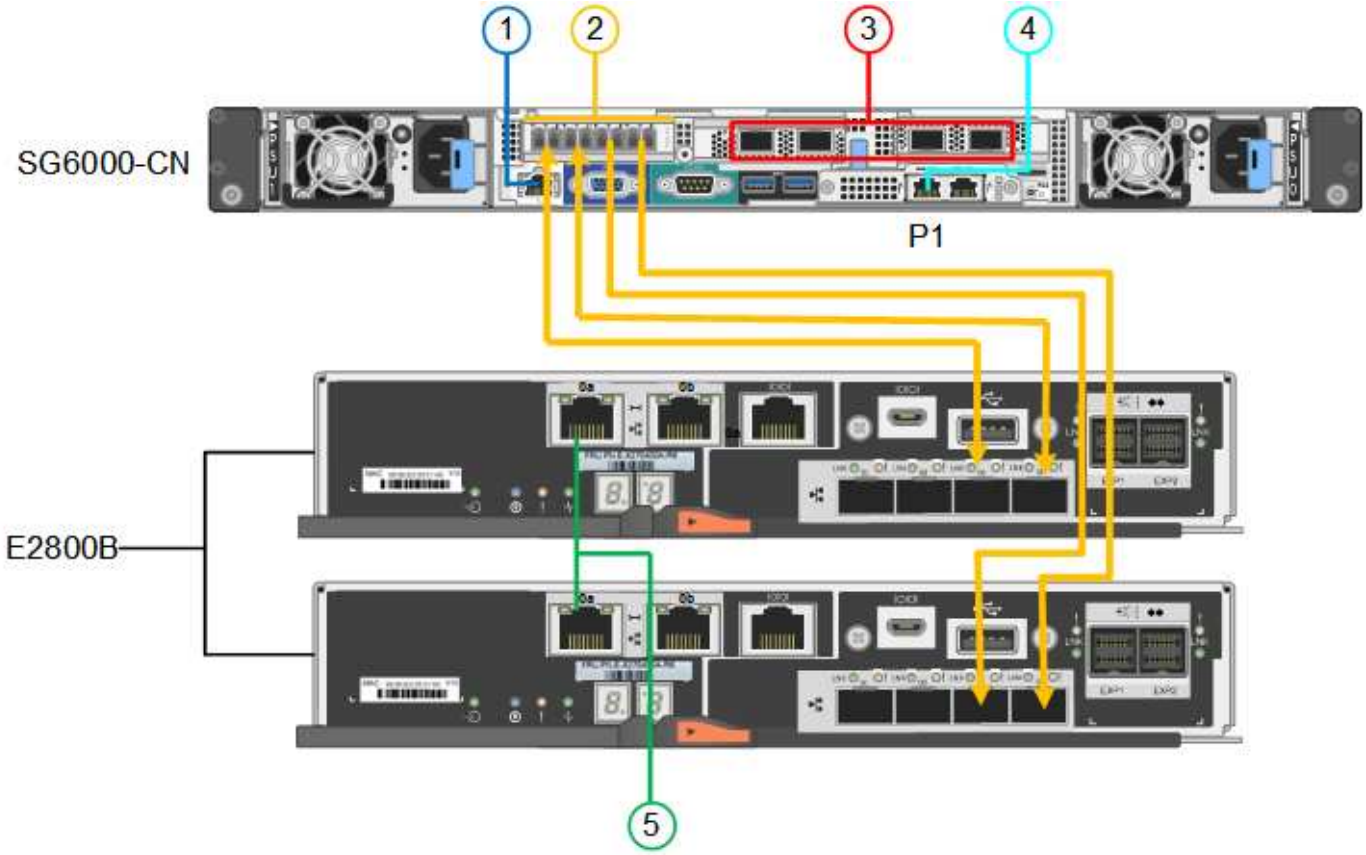
> SG6060에는 E2800A 컨트롤러가 있고 SG6060X에는 E2800B 컨트롤러가 있습니다. E2800 컨트롤러의 두 버전은 상호 연결 포트의 위치를 제외하고 동일한 사양과 기능을 제공합니다.

> E2800A 및 E2800B 컨트롤러를 동일한 어플라이언스에서 사용하지 마십시오.

- SG6060에서 E2800A 연결 *

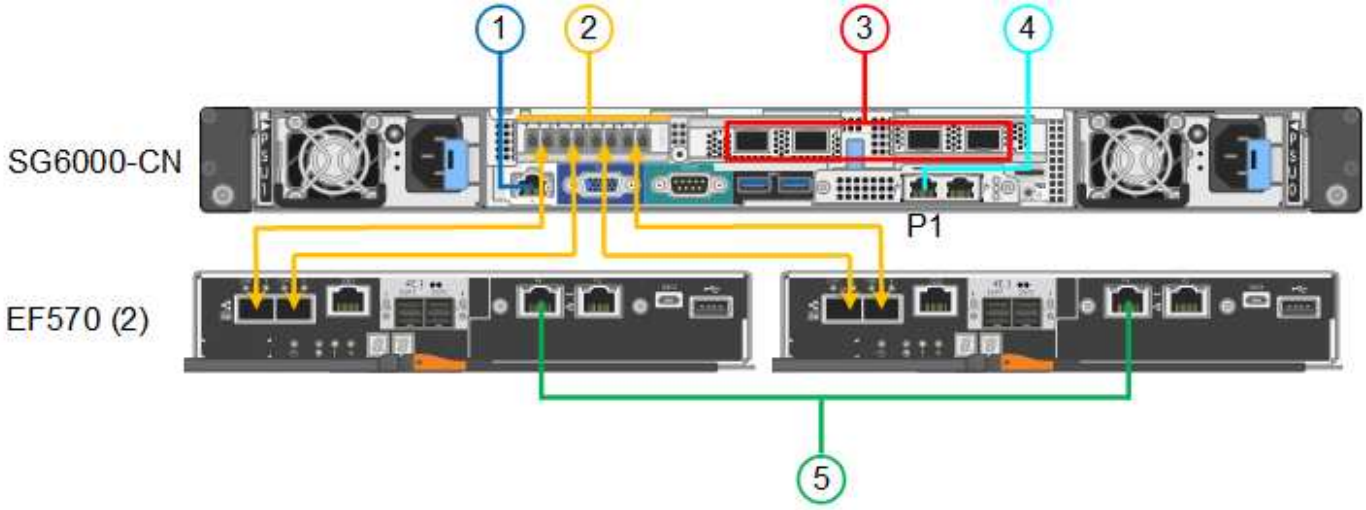


- SG6060X에서 E2800B 연결 *



SGF6024에 케이블을 연결합니다

다음 그림은 SGF6024 어플라이언스에 있는 3개의 컨트롤러와 SG6000-CN 컴퓨팅 컨트롤러가 상단에 있고 두 개의 EF570 스토리지 컨트롤러가 컴퓨팅 컨트롤러 아래에 나란히 표시되어 있습니다.



	포트	포트의 유형입니다	기능
1	SG6000-CN 컨트롤러의 BMC 관리 포트	1GbE(RJ-45)	BMC 인터페이스에 액세스하는 네트워크에 연결합니다.

	포트	포트의 유형입니다	기능
2	FC 연결 포트: • SG6000-CN 컨트롤러에서 4 • 각 스토리지 컨트롤러에 2개씩	16Gb/s FC 광 SFP+	각 스토리지 컨트롤러를 SG6000-CN 컨트롤러에 연결합니다.
3	SG6000-CN 컨트롤러의 네트워크 포트 4개	10/25GbE	그리드 네트워크 및 StorageGRID용 클라이언트 네트워크에 연결합니다.
4	SG6000-CN 컨트롤러의 관리 네트워크 포트 (그림에서 P1 레이블)	1GbE(RJ-45) • 중요: * 이 포트는 1000 BaseT/full에서만 작동하며 10메가비트 또는 100메가비트 속도를 지원하지 않습니다.	SG6000-CN 컨트롤러를 StorageGRID용 관리 네트워크에 연결합니다.
	SG6000-CN 컨트롤러의 가장 오른쪽 RJ-45 포트	1GbE(RJ-45) • 중요: * 이 포트는 1000 BaseT/full에서만 작동하며 10메가비트 또는 100메가비트 속도를 지원하지 않습니다.	• 관리 네트워크에 대한 중복 연결을 원할 경우 관리 포트 1에 연결할 수 있습니다. • 유선을 해제하고 임시 로컬 액세스(IP 169.254.0.1)에 사용할 수 있습니다. • 설치 중에 DHCP 할당 IP 주소를 사용할 수 없는 경우 SG6000-CN 컨트롤러를 서비스 랩톱에 연결하는 데 사용할 수 있습니다.
5	각 스토리지 컨트롤러의 관리 포트 1	1GbE(RJ-45)	SANtricity 시스템 관리자에 액세스하는 네트워크에 연결합니다.
	각 스토리지 컨트롤러의 관리 포트 2	1GbE(RJ-45)	기술 지원용으로 예약되어 있습니다.

단계

1. 이더넷 케이블을 사용하여 SG6000-CN 컨트롤러의 BMC 관리 포트를 관리 네트워크에 연결합니다.

   이 연결은 선택 사항이지만 지원을 원활하게 하는 것이 좋습니다.

2. 스토리지 컨트롤러의 4개의 광 케이블과 4개의 SFP+ 트랜시버를 사용하여 각 스토리지 컨트롤러의 FC 포트 2개를 SG6000-CN 컨트롤러의 FC 포트에 연결합니다.
3. TwinAx 케이블 또는 광 케이블과 SFP+ 또는 SFP28 트랜시버를 사용하여 SG6000-CN 컨트롤러의 네트워크 포트를 해당 네트워크 스위치에 연결합니다.

> 네트워크 포트 4개는 동일한 링크 속도를 사용해야 합니다. 10GbE 링크 속도를 사용하려는 경우 SFP+ 트랜시버를 설치합니다. 25GbE 링크 속도를 사용하려는 경우 SFP28 트랜시버를 설치합니다.

- 고정 포트 결합 모드(기본값)를 사용하려는 경우 표 에 나와 있는 대로 포트를 StorageGRID 그리드 및 클라이언트 네트워크에 연결합니다.

포트	연결 대상...
포트 1	클라이언트 네트워크(옵션)
포트 2	그리드 네트워크
포트 3	클라이언트 네트워크(옵션)
포트 4	그리드 네트워크

- Aggregate 포트 결합 모드를 사용하려는 경우 하나 이상의 네트워크 포트를 하나 이상의 스위치에 연결합니다. 단일 장애 지점이 발생하지 않도록 4개 포트 중 2개 이상을 연결해야 합니다. 단일 LACP 결합에 둘 이상의 스위치를 사용하는 경우 스위치는 MLAG 또는 동급 스위치를 지원해야 합니다.

4. StorageGRID용 관리 네트워크를 사용하려는 경우 이더넷 케이블을 사용하여 SG6000-CN 컨트롤러의 관리 네트워크 포트를 관리 네트워크에 연결합니다.
5. SANtricity 시스템 관리자용 관리 네트워크를 사용하려면 이더넷 케이블을 사용하여 각 스토리지 컨트롤러(왼쪽의 RJ-45 포트)의 관리 포트 1(E2800A의 P1, E2800B의 0a)을 SANtricity 시스템 관리자의 관리 네트워크에 연결합니다.

   스토리지 컨트롤러(오른쪽의 RJ-45 포트)에서 관리 포트 2(E2800A의 P2 및 E2800B의 0b)를 사용하지 마십시오. 이 포트는 기술 지원을 위해 예약되어 있습니다.

관련 정보

SG6000-CN 컨트롤러의 포트 결합 모드

캐비닛 또는 랙에 SG6000-CN 컨트롤러를 다시 설치합니다

SG6060 및 **SG6060X:** 확장 셸프 케이블 연결(옵션

확장 쉘프를 사용하는 경우 E2860 컨트롤러 쉘프에 연결해야 합니다. 각 SG6060 또는 SG6060X 어플라이언스에 대해 최대 2개의 확장 셸프를 가질 수 있습니다.

필요한 것

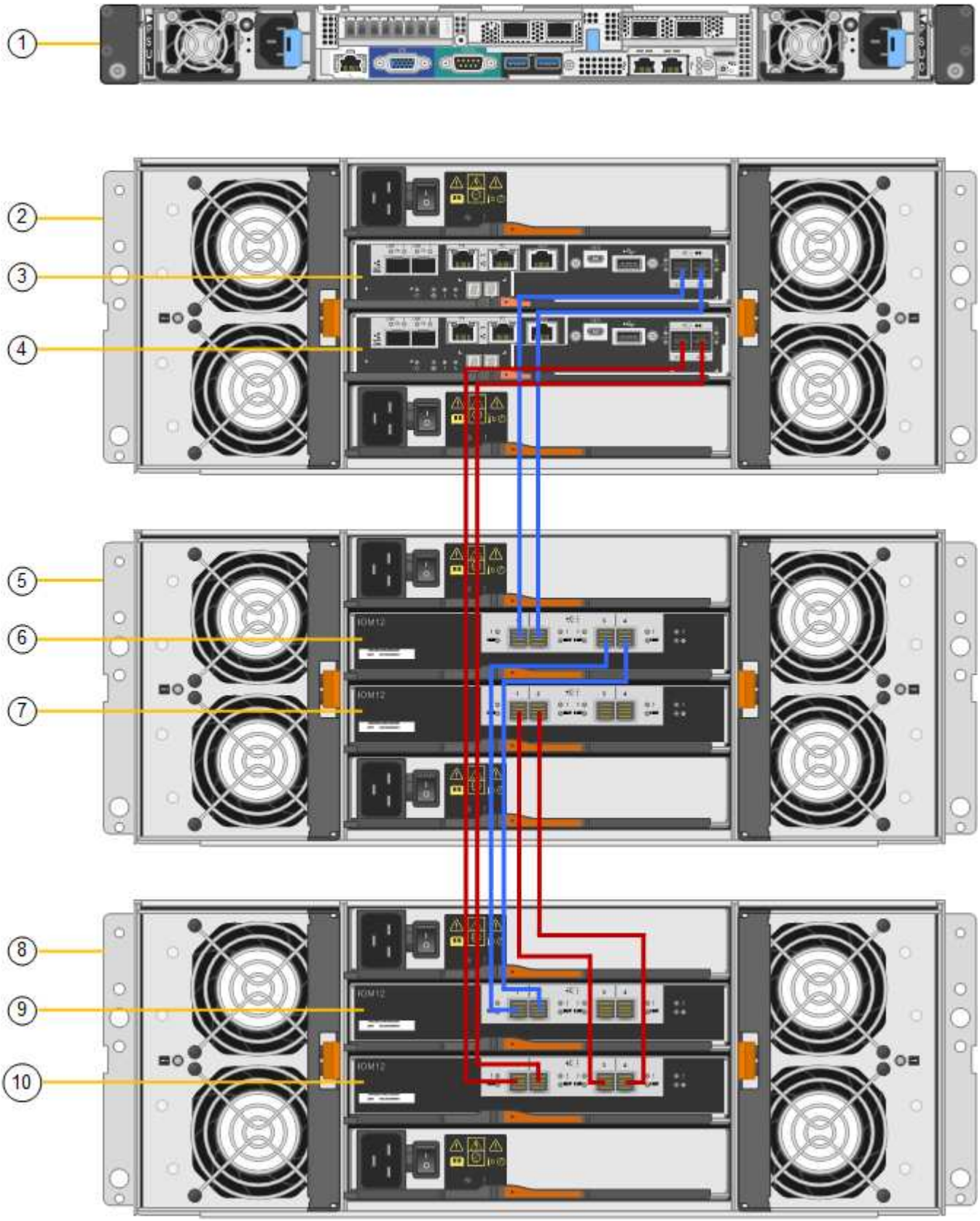
- 각 확장 쉘프와 함께 2개의 SAS 케이블이 제공됩니다.
- E2860 컨트롤러 쉘프가 포함된 캐비닛 또는 랙에 확장 쉘프를 설치했습니다.

  SG6060 및 SG6060X: 캐비닛 또는 랙에 60 드라이브 쉘프를 설치합니다

단계

다이어그램에 표시된 대로 각 확장 쉘프를 E2860 컨트롤러 쉘프에 연결합니다.

이 도면에서는 SG6060의 두 확장 셸프(SG6060X의 확장 케이블 연결은 동일함)에 대한 케이블 연결을 보여 줍니다. 확장 쉘프가 하나인 경우 IOM A를 컨트롤러 A에 연결하고 IOM B를 컨트롤러 B에 연결합니다



속성 표시기	설명
1	SG6000-CN
2	E2860 컨트롤러 쉘프
3	컨트롤러 A
4	컨트롤러 B
5	확장 쉘프 1
6	확장 쉘프 1의 경우 IOM A
7	확장 쉘프 1의 IOM B
8	확장 쉘프 2
9	확장 쉘프 2의 경우 IOM A
10	확장 쉘프 2의 IOM B

전원 코드 연결 및 전원 공급**(SG6000)**

네트워크 케이블을 연결한 후 SG6000-CN 컨트롤러 및 스토리지 컨트롤러 2개 또는 확장 셸프(옵션)에 전원을 공급할 준비가 되었습니다.

단계

1. 스토리지 컨트롤러 쉘프의 두 컨트롤러가 모두 꺼져 있는지 확인합니다.

   * 감전 위험 * — 전원 코드를 연결하기 전에 두 스토리지 컨트롤러 각각에 대한 전원 스위치가 꺼져 있는지 확인하십시오.

2. 확장 쉘프가 있는 경우, IOM 전원 스위치가 모두 꺼져 있는지 확인합니다.

   * 감전 위험 * — 전원 코드를 연결하기 전에 각 확장 셸프에 대한 2개의 전원 스위치가 꺼져 있는지 확인하십시오.

3. SG6000-CN 컨트롤러의 2개의 전원 공급 장치 각각에 전원 코드를 연결합니다.
4. 이 두 개의 전원 코드를 캐비닛이나 랙에 있는 두 개의 서로 다른 PDU(Power Distribution Unit)에 연결합니다.
5. 스토리지 컨트롤러 쉘프에 있는 2개의 전원 공급 장치 각각에 전원 코드를 연결합니다.
6. 확장 선반이 있는 경우 각 확장 선반의 2개의 전원 공급 장치 각각에 전원 코드를 연결합니다.
7. 각 스토리지 쉘프(확장 쉘프 옵션 포함)의 전원 코드 2개를 캐비닛 또는 랙에 있는 서로 다른 PDU 2개에 연결합니다.

8. SG6000-CN 컨트롤러 앞면에 있는 전원 단추가 현재 파란색으로 켜져 있지 않으면 단추를 눌러 컨트롤러 전원을 켭니다.

   전원을 켜는 동안 전원 단추를 다시 누르지 마십시오.

9. 스토리지 컨트롤러 쉘프 뒷면에 있는 2개의 전원 스위치를 켭니다. 확장 쉘프가 있는 경우, 각 쉘프에 대해 2개의 전원 스위치를 켜십시오.
   - 전원을 켜는 동안 전원 스위치를 끄지 마십시오.
   - 스토리지 컨트롤러 쉘프와 옵션 확장 쉘프 의 팬은 처음 시작할 때 매우 클 수 있습니다. 시동 중 큰 소음이 정상입니다.
10. 구성 요소가 부팅된 후 상태를 확인합니다.
    - 각 스토리지 컨트롤러 후면에 있는 7개 세그먼트 디스플레이를 확인합니다. 자세한 내용은 부팅 상태 코드 보기에 대한 문서를 참조하십시오.
    - SG6000-CN 컨트롤러 앞면의 전원 단추가 켜져 있는지 확인합니다.
11. 오류가 발생하면 문제를 해결하십시오.
12. 전면 베젤을 분리한 경우 SG6000-CN 컨트롤러에 연결합니다.

관련 정보

SG6000 스토리지 컨트롤러의 부팅 상태 코드를 봅니다

SG6000-CN 컨트롤러의 상태 표시등 및 단추를 봅니다

캐비닛 또는 랙에 SG6000-CN 컨트롤러를 다시 설치합니다

SG6000-CN 컨트롤러의 상태 표시등 및 단추를 봅니다

SG6000-CN 컨트롤러에는 다음 표시등 및 단추를 포함하여 컨트롤러의 상태를 확인하는 데 도움이 되는 표시등이 포함되어 있습니다.

	디스플레이	설명
1	전원 단추	• 파란색: 컨트롤러의 전원이 켜져 있습니다. • 꺼짐: 컨트롤러의 전원이 꺼져 있습니다.
2	재설정 버튼	_표시기 없음 _ 이 단추를 사용하여 컨트롤러를 하드 리셋합니다.

	디스플레이	설명
3	식별 버튼	• 파란색 깜박임 또는 켜짐: 캐비닛이나 랙의 컨트롤러를 식별합니다. • Off(끄기): 캐비닛이나 랙에서 컨트롤러를 시각적으로 확인할 수 없습니다. 이 단추는 깜박임, 켜짐(켜짐) 또는 꺼짐 으로 설정할 수 있습니다.
4	알람 LED	• 황색: 오류가 발생했습니다. • 참고: * 부팅 및 오류 코드를 보려면 BMC 인터페이스에 액세스해야 합니다. • 꺼짐: 오류가 없습니다.

일반 부팅 코드

부팅 중 또는 SG6000-CN 컨트롤러의 하드 리셋 후, 다음과 같은 현상이 발생합니다.

1. BMC(베이스보드 관리 컨트롤러)는 발생한 오류를 포함하여 부팅 순서의 코드를 기록합니다.
2. 전원 단추가 켜집니다.
3. 부팅 중에 오류가 발생하면 알람 LED가 켜집니다.

   부팅 및 오류 코드를 보려면 BMC 인터페이스에 액세스해야 합니다.

관련 정보

하드웨어 설치 문제 해결(SG6000)

BMC 인터페이스(SG6000) 구성

SG6000-CN 컨트롤러의 전원을 켜고 작동을 확인합니다

SG6000 스토리지 컨트롤러의 부팅 상태 코드를 봅니다

각 스토리지 컨트롤러에는 컨트롤러 전원이 켜질 때 상태 코드를 제공하는 7개의 세그먼트 디스플레이가 있습니다. 상태 코드는 E2800 컨트롤러와 EF570 컨트롤러에서 동일합니다.

이 작업에 대해

이러한 코드에 대한 설명은 스토리지 컨트롤러 유형에 대한 E-Series 시스템 모니터링 정보를 참조하십시오.

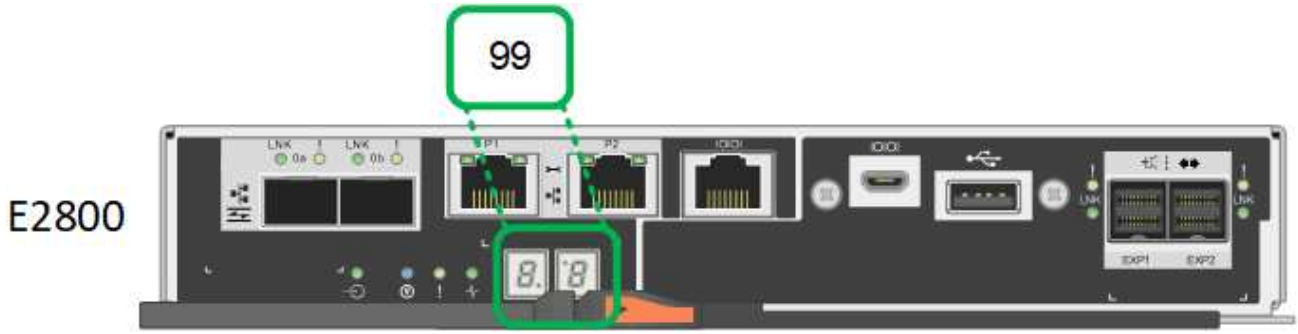
단계

1. 부팅 중에 각 스토리지 컨트롤러의 7개 세그먼트 디스플레이에 표시된 코드를 확인하여 진행 상황을 모니터링합니다.

   각 스토리지 컨트롤러의 7개 세그먼트 디스플레이에는 컨트롤러가 시작 프로세스를 수행하고 있음을 나타내는 반복 시퀀스 * OS *, * SD *, ' **blank* * 가 표시됩니다.

2. 컨트롤러가 부팅된 후 각 스토리지 컨트롤러에 99가 표시되는지 확인합니다. 이 값은 E-Series 컨트롤러 쉘프의 기본 ID입니다.

   이 예의 E2800 컨트롤러에 표시된 대로 이 값이 두 스토리지 컨트롤러 모두에 표시되는지 확인합니다.



3. 한 컨트롤러 또는 두 컨트롤러 모두에 다른 값이 표시되는 경우 를 참조하십시오 하드웨어 설치 문제 해결(SG6000) 설치 단계를 올바르게 완료했는지 확인합니다. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

관련 정보

"E5700 및 E2800 시스템 모니터링 가이드"

"NetApp 지원"

SG6000-CN 컨트롤러의 전원을 켜고 작동을 확인합니다

하드웨어 구성(SG6000)

어플라이언스에 전원을 적용한 후 StorageGRID에서 사용할 네트워크 연결을 구성해야 합니다. 컨트롤러 쉘프의 스토리지 컨트롤러 및 기타 하드웨어를 모니터링하는 데 사용할 소프트웨어인 SANtricity 시스템 관리자를 구성해야 합니다. 또한 SG6000-CN 컨트롤러의 BMC 인터페이스에 액세스할 수 있는지 확인해야 합니다.

StorageGRID 연결 구성(SG6000)

StorageGRID 시스템에서 StorageGRID 어플라이언스를 스토리지 노드로 구축하려면 먼저 어플라이언스와 사용할 네트워크 간의 연결을 구성해야 합니다. SG6000-CN 컨트롤러(컴퓨팅 컨트롤러)에 사전 설치된 StorageGRID 어플라이언스 설치 프로그램으로 이동하여 네트워킹을 구성할 수 있습니다.

StorageGRID 어플라이언스 설치 프로그램에 액세스합니다

설치 프로그램 버전을 확인하고 그리드 네트워크, 관리자 네트워크(옵션) 및 클라이언트 네트워크(옵션)의 세 StorageGRID 네트워크와 어플라이언스 및 네트워크 사이의 연결을 구성하려면 StorageGRID 어플라이언스 설치 프로그램에 액세스해야 합니다.

필요한 것

- StorageGRID 관리 네트워크에 연결할 수 있는 관리 클라이언트를 사용 중이거나 서비스 랩톱을 사용 중입니다.
- 클라이언트 또는 서비스 랩톱에 지원되는 웹 브라우저가 있습니다.

- SG6000-CN 컨트롤러는 사용하려는 모든 StorageGRID 네트워크에 연결되어 있습니다.
- 이러한 네트워크에서 SG6000-CN 컨트롤러의 IP 주소, 게이트웨이 및 서브넷을 알고 있습니다.
- 사용할 네트워크 스위치를 구성했습니다.

이 작업에 대해

StorageGRID 어플라이언스 설치 프로그램에 처음 액세스하려면 SG6000-CN 컨트롤러의 관리 네트워크 포트에 대해 DHCP 할당 IP 주소를 사용하거나(컨트롤러가 관리 네트워크에 연결되어 있다고 가정) 서비스 랩톱을 SG6000-CN 컨트롤러에 직접 연결할 수 있습니다.

단계

1. 가능하면 SG6000-CN 컨트롤러의 관리 네트워크 포트에 대한 DHCP 주소를 사용하여 StorageGRID 어플라이언스 설치 프로그램에 액세스합니다.

   a. SG6000-CN 컨트롤러 전면에서 MAC 주소 레이블을 찾아 관리 네트워크 포트의 MAC 주소를 확인합니다.

      MAC 주소 레이블에는 BMC 관리 포트의 MAC 주소가 나열됩니다.

      관리 네트워크 포트의 MAC 주소를 확인하려면 레이블의 16진수에 * 2 * 를 추가해야 합니다. 예를 들어 레이블의 MAC 주소가 * 09 * 로 끝나는 경우 관리 포트의 MAC 주소는 * 0B * 로 끝납니다. 레이블의 MAC 주소가 * (*y*) FF * 로 끝나는 경우 관리 포트의 MAC 주소는 * (*y*+1) 01 * 로 끝납니다. Windows에서 계산기를 열고, Programmer 모드로 설정하고, Hex를 선택하고, MAC 주소를 입력한 다음, * + 2 = * 를 입력하여 이 계산을 쉽게 수행할 수 있습니다.

   b. 네트워크 관리자에게 MAC 주소를 제공하여 관리자가 관리 네트워크에서 어플라이언스의 DHCP 주소를 찾을 수 있도록 합니다.

   c. 클라이언트에서 StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. + `https://Appliance_Controller_IP:8443*`

      '*SG6000-CN_Controller_IP*'의 경우 DHCP address를 사용한다.

   d. 보안 경고 메시지가 나타나면 브라우저의 설치 마법사를 사용하여 인증서를 보고 설치합니다.

      다음에 이 URL에 액세스할 때 알림이 나타나지 않습니다.

      StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다. 이 페이지에 처음 액세스할 때 표시되는 정보와 메시지는 어플라이언스가 현재 StorageGRID 네트워크에 연결되어 있는 방식에 따라 다릅니다. 오류 메시지가 나타날 수 있으며, 이 메시지는 이후 단계에서 해결될 것입니다.

NetApp® StorageGRID® Appliance Installer

Home | Configure Networking | Configure Hardware | Monitor Installation | Advanced

Home

The installation is ready to be started. Review the settings below, and then click Start Installation.

This Node

Node type: Storage

Node name: MM-2-108-SGA-lab25

Cancel Save

Primary Admin Node connection

Enable Admin Node discovery: ☐

Primary Admin Node IP: 172.16.1.178

Connection state: Connection to 172.16.1.178 ready

Cancel Save

Installation

Current state: Ready to start installation of MM-2-108-SGA-lab25 into grid with Admin Node 172.16.1.178 running StorageGRID 11.2.0, using StorageGRID software downloaded from the Admin Node.

Start Installation

2. DHCP를 사용하여 IP 주소를 얻을 수 없는 경우 링크 로컬 연결을 사용할 수 있습니다.

   a. 이더넷 케이블을 사용하여 SG6000-CN 컨트롤러의 맨 오른쪽 RJ-45 포트에 서비스 랩톱을 직접 연결합니다.

   b. 서비스 랩톱에서 웹 브라우저를 엽니다.

c. StorageGRID 어플라이언스 설치 프로그램에 대한 이 URL을 입력합니다: + `*https://169.254.0.1:8443*`

StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다. 이 페이지에 처음 액세스할 때 표시되는 정보 및 메시지는 어플라이언스가 현재 연결되어 있는 방식에 따라 다릅니다.

> 링크 로컬 연결을 통해 홈 페이지에 액세스할 수 없는 경우 서비스 랩톱 IP 주소를 "169.254.0.2"로 구성한 후 다시 시도하십시오.

작업을 마친 후

StorageGRID 어플라이언스 설치 프로그램에 액세스한 후:

- 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램 버전이 StorageGRID 시스템에 설치된 소프트웨어 버전과 일치하는지 확인합니다. 필요한 경우 StorageGRID 어플라이언스 설치 프로그램을 업그레이드합니다.

  StorageGRID 어플라이언스 설치 프로그램 버전을 확인하고 업그레이드합니다

- StorageGRID 어플라이언스 설치 관리자 홈 페이지에 표시되는 메시지를 검토하고 필요에 따라 링크 구성 및 IP 구성을 구성합니다.

관련 정보

웹 브라우저 요구 사항

StorageGRID 어플라이언스 설치 프로그램 버전을 확인하고 업그레이드합니다

어플라이언스의 StorageGRID 어플라이언스 설치 프로그램 버전은 StorageGRID 시스템에 설치된 소프트웨어 버전과 일치해야 모든 StorageGRID 기능이 지원됩니다.

필요한 것

StorageGRID 어플라이언스 설치 프로그램에 액세스했습니다.

이 작업에 대해

StorageGRID 어플라이언스는 StorageGRID 어플라이언스 설치 프로그램이 사전 설치된 상태로 제공됩니다. 최근에 업그레이드된 StorageGRID 시스템에 어플라이언스를 추가하는 경우 어플라이언스를 새 노드로 설치하기 전에 StorageGRID 어플라이언스 설치 프로그램을 수동으로 업그레이드해야 할 수 있습니다.

새 StorageGRID 버전으로 업그레이드하면 StorageGRID 어플라이언스 설치 프로그램이 자동으로 업그레이드됩니다. 설치된 어플라이언스 노드에서 StorageGRID 어플라이언스 설치 프로그램을 업그레이드할 필요가 없습니다. 이 절차는 이전 버전의 StorageGRID 어플라이언스 설치 프로그램이 포함된 어플라이언스를 설치하는 경우에만 필요합니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 펌웨어 업그레이드 * 를 선택합니다.
2. 현재 펌웨어 버전을 StorageGRID 시스템에 설치된 소프트웨어 버전과 비교합니다. (그리드 관리자 상단에서 도움말 아이콘을 선택하고 * 정보 * 를 선택합니다.)

   두 버전의 두 번째 숫자가 일치해야 합니다. 예를 들어, StorageGRID 시스템에서 버전 11. * 6 *.*x*._y_를 실행하는 경우 StorageGRID 어플라이언스 설치 프로그램 버전은 3. * 6 *._z_이어야 합니다.

3. 어플라이언스에 StorageGRID 어플라이언스 설치 프로그램의 하위 수준 버전이 있는 경우 로 이동합니다 "NetApp

다운로드: StorageGRID 어플라이언스".

NetApp 계정의 사용자 이름과 암호를 사용하여 로그인합니다.

4. StorageGRID Appliances*용 * 지원 파일의 적절한 버전과 해당 체크섬 파일을 다운로드하십시오.

   StorageGRID 어플라이언스 파일의 지원 파일은 모든 StorageGRID 어플라이언스 모델의 현재 및 이전 펌웨어 버전을 포함하는 '.zip' 아카이브로, 각 컨트롤러 유형의 하위 디렉토리에 있습니다.

   StorageGRID 어플라이언스 파일용 지원 파일을 다운로드한 후 '.zip' 아카이브의 압축을 풀고 StorageGRID 어플라이언스 설치 프로그램 설치에 대한 중요 정보는 README 파일을 참조하십시오.

5. 의 펌웨어 업그레이드 페이지에 있는 지침을 따릅니다 StorageGRID 어플라이언스 설치 프로그램 다음 단계를 수행하려면:

   a. 컨트롤러 유형 및 체크섬 파일에 적합한 지원 파일(펌웨어 이미지)을 업로드합니다.

   b. 비활성 파티션을 업그레이드합니다.

   c. 재부팅하고 파티션을 바꿉니다.

   d. 두 번째(비활성) 파티션을 업그레이드합니다.

네트워크 링크 구성**(SG6000** 시리즈**)**

어플라이언스를 그리드 네트워크, 클라이언트 네트워크 및 관리 네트워크에 연결하는 데 사용되는 포트에 대한 네트워크 링크를 구성할 수 있습니다. 링크 속도와 포트 및 네트워크 연결 모드를 설정할 수 있습니다.

필요한 것

어플라이언스 노드를 클론 생성하는 경우 소스 어플라이언스 노드에서 사용하는 모든 링크에 대해 타겟 어플라이언스에 대한 네트워크 링크를 구성합니다.

25GbE 링크 속도를 사용하려는 경우:

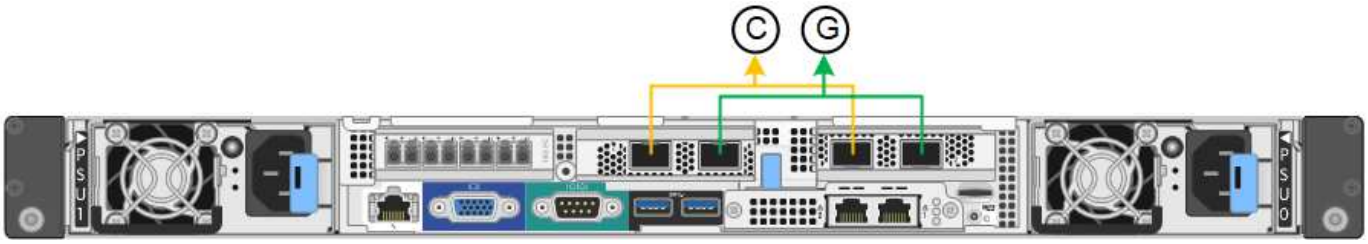
- SFP28 TwinAx 케이블을 사용 중이거나 사용할 네트워크 포트에 SFP28 트랜시버를 설치했습니다.
- 이러한 기능을 지원할 수 있는 스위치에 네트워크 포트를 연결했습니다.
- 이 고속 스위치를 사용하도록 스위치를 구성하는 방법을 이해할 수 있습니다.

Aggregate 포트 결합 모드, LACP 네트워크 결합 모드 또는 VLAN 태그 지정을 사용하려면 다음을 수행합니다.

- 어플라이언스의 네트워크 포트를 VLAN 및 LACP를 지원할 수 있는 스위치에 연결했습니다.
- LACP 결합에 여러 스위치가 사용되는 경우 스위치는 MLAG(Multi-Chassis Link Aggregation Group) 또는 이와 동등한 스위치를 지원합니다.
- VLAN, LACP, MLAG 또는 이와 동등한 기능을 사용하도록 스위치를 구성하는 방법을 이해합니다.
- 각 네트워크에 사용할 고유 VLAN 태그를 알고 있습니다. 이 VLAN 태그는 네트워크 트래픽이 올바른 네트워크로 라우팅되도록 각 네트워크 패킷에 추가됩니다.

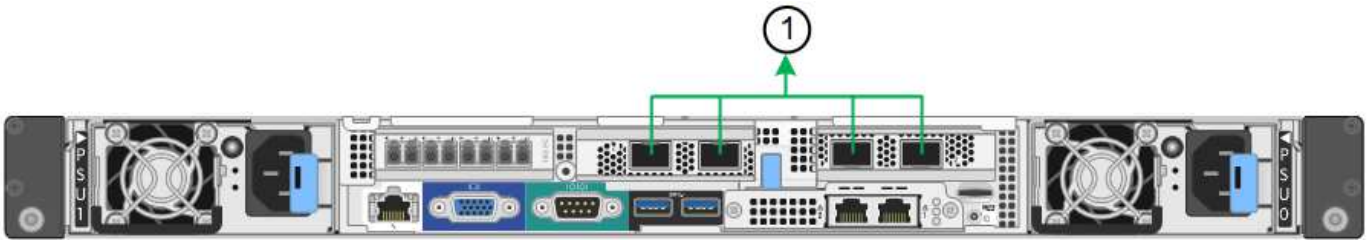
이 작업에 대해

이 그림은 4개의 네트워크 포트가 고정 포트 결합 모드(기본 구성)에서 어떻게 결합되는지 보여줍니다.



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
c	이 네트워크를 사용하는 경우 포트 1과 3이 클라이언트 네트워크에 대해 함께 연결됩니다.
g	포트 2와 4는 그리드 네트워크를 위해 서로 연결되어 있습니다.

이 그림은 4개의 네트워크 포트가 애그리게이트 포트 결합 모드에서 결합되는 방식을 보여줍니다.



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
1	4개 포트 모두 단일 LACP 결합으로 그룹화되므로 모든 포트를 그리드 네트워크 및 클라이언트 네트워크 트래픽에 사용할 수 있습니다.

이 표에는 4개의 네트워크 포트를 구성하는 옵션이 요약되어 있습니다. 기본 설정은 굵게 표시됩니다. 기본이 아닌 설정을 사용하려면 구성 연결 페이지에서 설정을 구성하기만 하면 됩니다.

- * 고정(기본값) 포트 결합 모드 *

네트워크 연결 모드	클라이언트 네트워크 비활성화(기본값)	클라이언트 네트워크가 활성화되었습니다
Active-Backup(기본값)	• 포트 2와 4는 그리드 네트워크에 액티브-백업 결합을 사용합니다. • 포트 1과 3은 사용되지 않습니다. • VLAN 태그는 선택 사항입니다.	• 포트 2와 4는 그리드 네트워크에 액티브-백업 결합을 사용합니다. • 포트 1과 3은 클라이언트 네트워크에 대해 액티브-백업 연결을 사용합니다. • VLAN 태그는 두 네트워크에 대해 모두 지정할 수 있습니다.

네트워크 연결 모드	클라이언트 네트워크 비활성화(기본값)	클라이언트 네트워크가 활성화되었습니다
LACP(802.3ad)	• 포트 2와 4는 그리드 네트워크에 LACP 결합을 사용합니다. • 포트 1과 3은 사용되지 않습니다. • VLAN 태그는 선택 사항입니다.	• 포트 2와 4는 그리드 네트워크에 LACP 결합을 사용합니다. • 포트 1과 3은 클라이언트 네트워크에 LACP 결합을 사용합니다. • VLAN 태그는 두 네트워크에 대해 모두 지정할 수 있습니다.

- * 집계 포트 결합 모드 *

네트워크 연결 모드	클라이언트 네트워크 비활성화(기본값)	클라이언트 네트워크가 활성화되었습니다
LACP(802.3ad)만 해당	• 포트 1-4는 그리드 네트워크에 단일 LACP 결합을 사용합니다. • 단일 VLAN 태그는 그리드 네트워크 패킷을 식별합니다.	• 포트 1-4는 그리드 네트워크 및 클라이언트 네트워크에 단일 LACP 결합을 사용합니다. • 두 개의 VLAN 태그를 통해 그리드 네트워크 패킷을 클라이언트 네트워크 패킷과 분리할 수 있습니다.

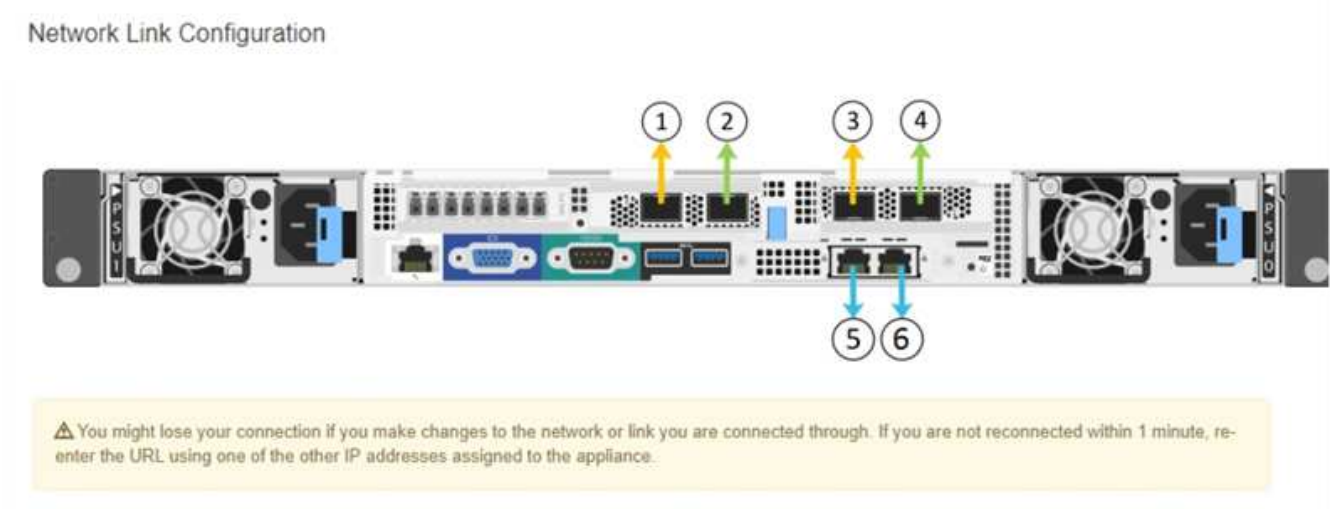
을 참조하십시오 SG6000-CN 컨트롤러의 포트 결합 모드 포트 연결 및 네트워크 연결 모드에 대한 자세한 내용은 를 참조하십시오.

이 그림은 SG6000-CN 컨트롤러의 2개의 1GbE 관리 포트가 관리 네트워크의 Active-Backup 네트워크 연결 모드에서 어떻게 연결되는지를 보여 줍니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * 링크 구성 * 을 클릭합니다.

   네트워크 링크 구성 페이지에는 네트워크 및 관리 포트 번호가 지정된 어플라이언스 다이어그램이 표시됩니다.



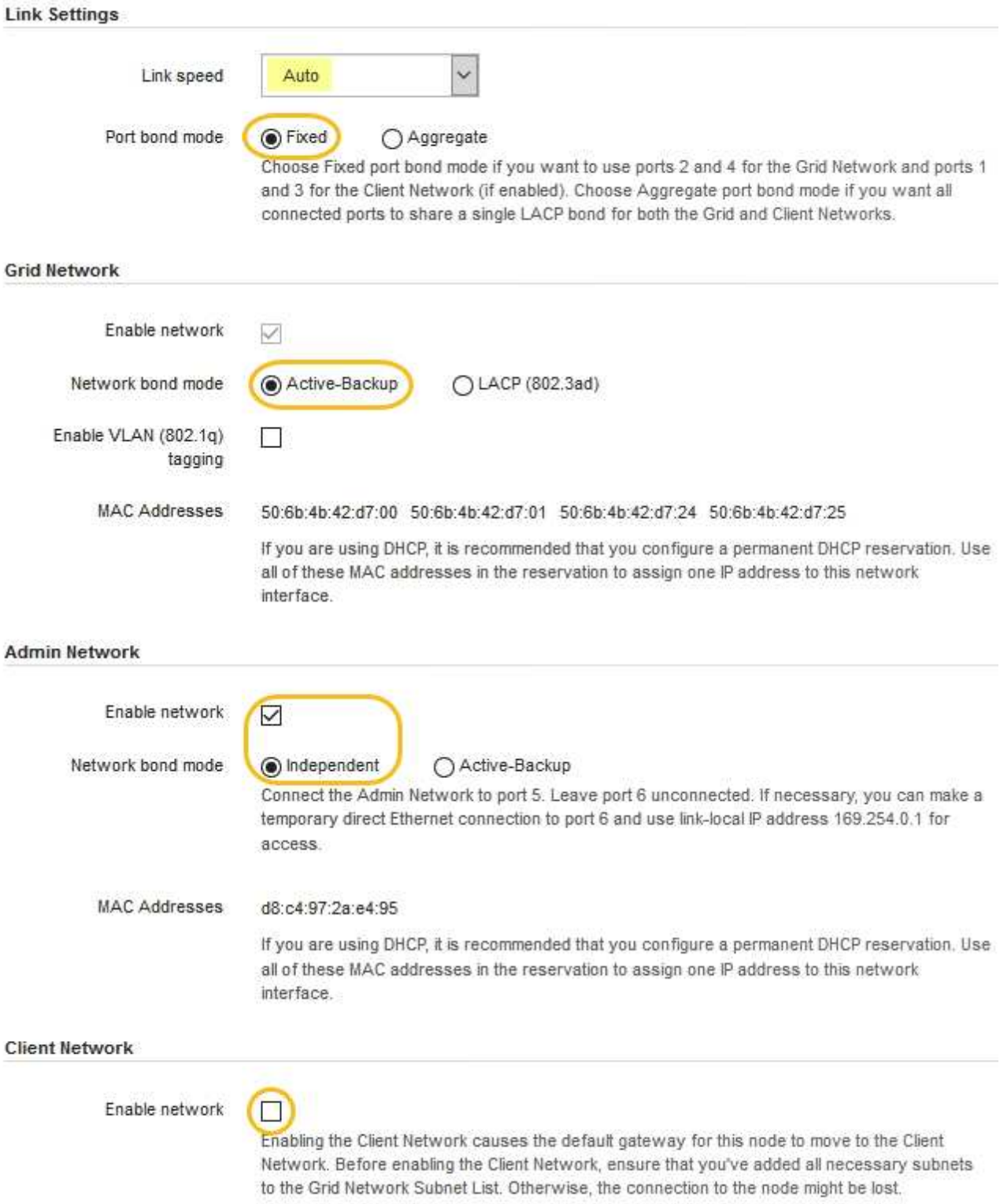
링크 상태 테이블에는 번호가 매겨진 포트의 링크 상태(위/아래) 및 속도(1/10/25/40/100Gbps)가 나열됩니다.

Link Status

Link	State	Speed (Gbps)
1	Up	100
2	Up	100
3	Down	N/A
4	Down	N/A
5	Up	1
6	Up	1

이 페이지에 처음 액세스하는 경우:

- * 링크 속도 * 가 * 자동 * 으로 설정되어 있습니다.
- * 포트 결합 모드 * 가 * 고정 * 으로 설정됩니다.
- * 네트워크 연결 모드 * 는 그리드 네트워크에 대해 * Active-Backup * 으로 설정됩니다.
- Admin Network*가 활성화되고 네트워크 연결 모드가 * Independent * 로 설정됩니다.
- 클라이언트 네트워크 * 가 비활성화됩니다.



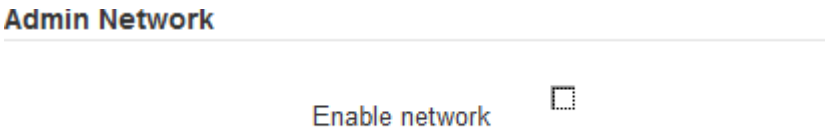
2. 네트워크 포트에 대해 25GbE 링크 속도를 사용하려는 경우 링크 속도 드롭다운 목록에서 * 자동 * 을 선택합니다.

   그리드 네트워크 및 클라이언트 네트워크에 대해 사용 중인 네트워크 스위치도 이 속도를 지원하고 구성해야 합니다. SFP28 TwinAx 케이블 또는 광 케이블과 SFP28 트랜시버를 사용해야 합니다.

3. 사용하려는 StorageGRID 네트워크를 활성화 또는 비활성화합니다.

   그리드 네트워크가 필요합니다. 이 네트워크를 비활성화할 수 없습니다.

a. 어플라이언스가 관리 네트워크에 연결되어 있지 않은 경우 관리 네트워크의 * 네트워크 활성화 * 확인란을 선택 취소합니다.



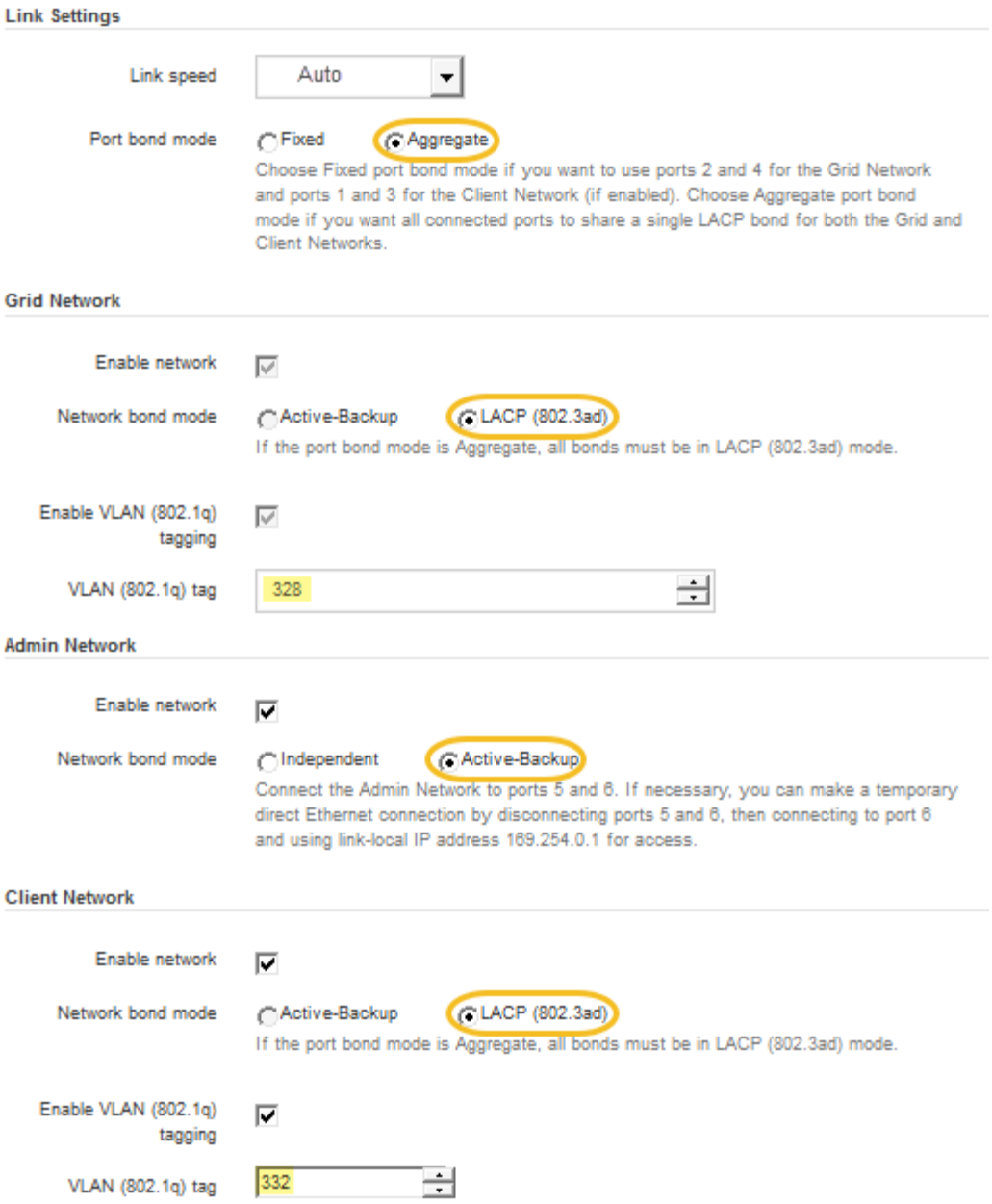
b. 어플라이언스가 클라이언트 네트워크에 연결되어 있는 경우 클라이언트 네트워크의 * 네트워크 활성화 * 확인란을 선택합니다.

이제 네트워크 포트에 대한 클라이언트 네트워크 설정이 표시됩니다.

4. 표를 참조하여 포트 결합 모드 및 네트워크 연결 모드를 구성합니다.

이 예제는 다음을 보여 줍니다.

- 그리드 및 클라이언트 네트워크에 대해 * 집계 * 및 * LACP * 선택. 각 네트워크에 대해 고유한 VLAN 태그를 지정해야 합니다. 0에서 4095 사이의 값을 선택할 수 있습니다.
- 관리자 네트워크에 대해 * Active-Backup * 이 선택되었습니다.



5. 선택 사항에 만족하면 * 저장 * 을 클릭합니다.

> 연결된 네트워크 또는 링크를 변경한 경우 연결이 끊어질 수 있습니다. 1분 내에 다시 연결되지 않으면 다른 하나를 사용하여 StorageGRID 어플라이언스 설치 프로그램의 URL을 다시 입력합니다 IP 주소 어플라이언스에 할당됨: ' * https://*SG6000-CN_Controller_IP*:8443*`

StorageGRID IP 주소를 구성합니다

StorageGRID 어플라이언스 설치 프로그램을 사용하여 StorageGRID 그리드, 관리자 및 클라이언트 네트워크의 어플라이언스 스토리지 노드에 사용되는 IP 주소 및 라우팅 정보를 구성합니다.

이 작업에 대해

연결된 각 네트워크에서 어플라이언스에 대해 고정 IP를 할당하거나 DHCP 서버의 주소에 대해 영구 임대를 할당해야

합니다.

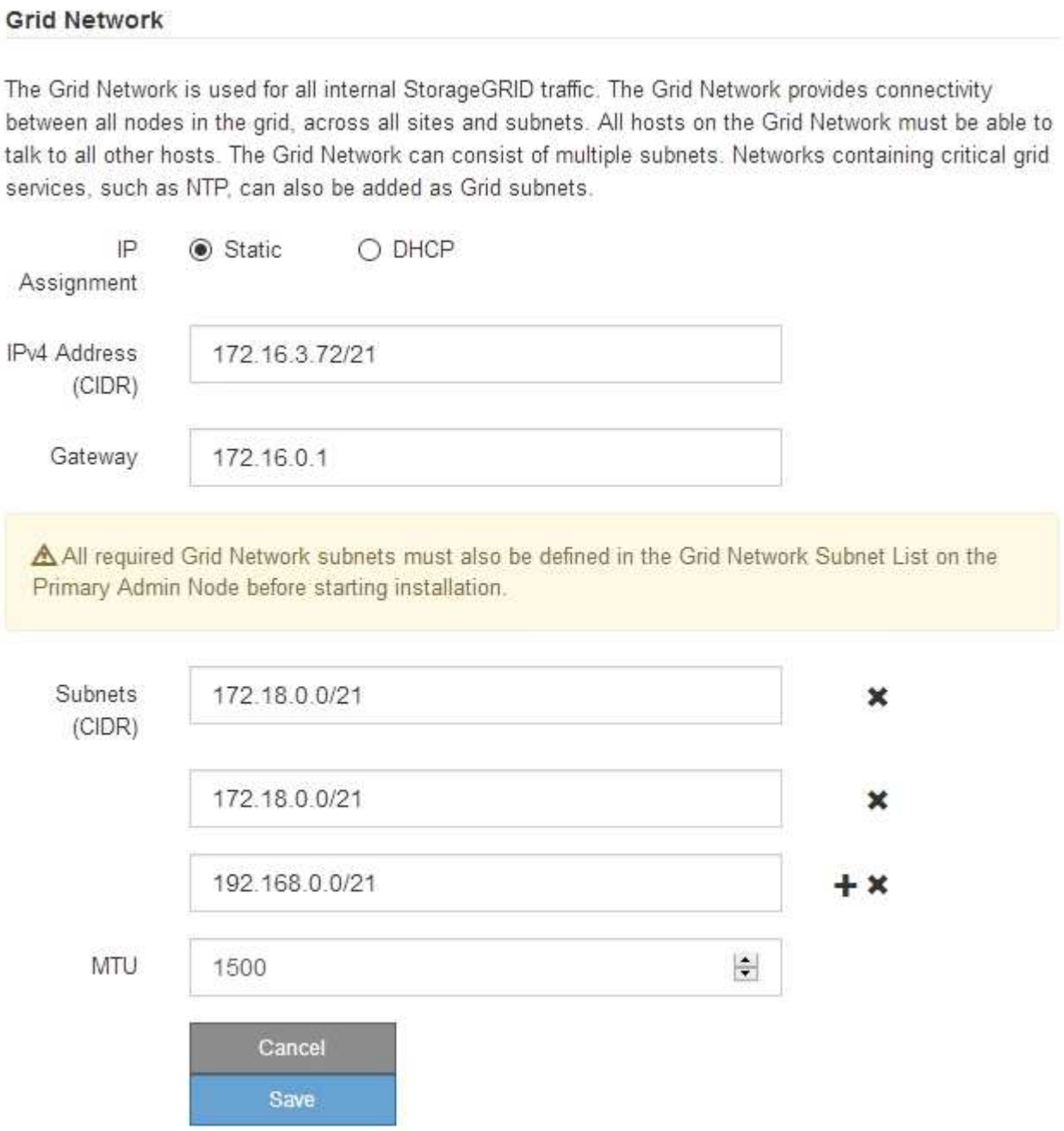
링크 구성을 변경하려면 를 참조하십시오 SG6000-CN 컨트롤러의 링크 구성 변경 지침.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * IP 구성 * 을 선택합니다.

   IP 구성 페이지가 나타납니다.

2. 그리드 네트워크를 구성하려면 페이지의 * 그리드 네트워크 * 섹션에서 * 정적 * 또는 * DHCP * 를 선택합니다.



3. Static * (정적 *)을 선택한 경우 다음 단계에 따라 Grid Network(그리드 네트워크)를 구성합니다.
   a. CIDR 표기법을 사용하여 정적 IPv4 주소를 입력합니다.

b. 게이트웨이를 입력합니다.

네트워크에 게이트웨이가 없는 경우 동일한 정적 IPv4 주소를 다시 입력합니다.

c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

> 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

d. 저장 * 을 클릭합니다.

IP 주소를 변경하면 게이트웨이와 서브넷 목록도 변경될 수 있습니다.

StorageGRID 어플라이언스 설치 프로그램에 대한 연결이 끊어진 경우 방금 할당한 새 고정 IP 주소를 사용하여 URL을 다시 입력합니다. 예: + `https://*services_appliance_IP*:8443*

e. 그리드 네트워크 서브넷 목록이 올바른지 확인합니다.

그리드 서브넷이 있는 경우 그리드 네트워크 게이트웨이가 필요합니다. 지정된 모든 그리드 서브넷은 이 게이트웨이를 통해 연결할 수 있어야 합니다. 이러한 그리드 네트워크 서브넷은 StorageGRID 설치를 시작할 때 기본 관리 노드의 그리드 네트워크 서브넷 목록에도 정의되어 있어야 합니다.

> 기본 라우트는 나열되지 않습니다. 클라이언트 네트워크가 활성화되지 않은 경우 기본 라우트는 그리드 네트워크 게이트웨이를 사용합니다.

- 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
- 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

f. 저장 * 을 클릭합니다.

4. DHCP * 를 선택한 경우 다음 단계에 따라 그리드 네트워크를 구성합니다.

a. DHCP * 라디오 버튼을 선택한 후 * 저장 * 을 클릭합니다.

IPv4 주소 *, * 게이트웨이 * 및 * 서브넷 * 필드가 자동으로 채워집니다. DHCP 서버가 MTU 값을 할당하도록 설정된 경우 * MTU * 필드가 해당 값으로 채워지고 필드는 읽기 전용이 됩니다.

웹 브라우저가 자동으로 StorageGRID 어플라이언스 설치 프로그램의 새 IP 주소로 리디렉션됩니다.

b. 그리드 네트워크 서브넷 목록이 올바른지 확인합니다.

그리드 서브넷이 있는 경우 그리드 네트워크 게이트웨이가 필요합니다. 지정된 모든 그리드 서브넷은 이 게이트웨이를 통해 연결할 수 있어야 합니다. 이러한 그리드 네트워크 서브넷은 StorageGRID 설치를 시작할 때 기본 관리 노드의 그리드 네트워크 서브넷 목록에도 정의되어 있어야 합니다.

> 기본 라우트는 나열되지 않습니다. 클라이언트 네트워크가 활성화되지 않은 경우 기본 라우트는 그리드 네트워크 게이트웨이를 사용합니다.

- 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
- 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

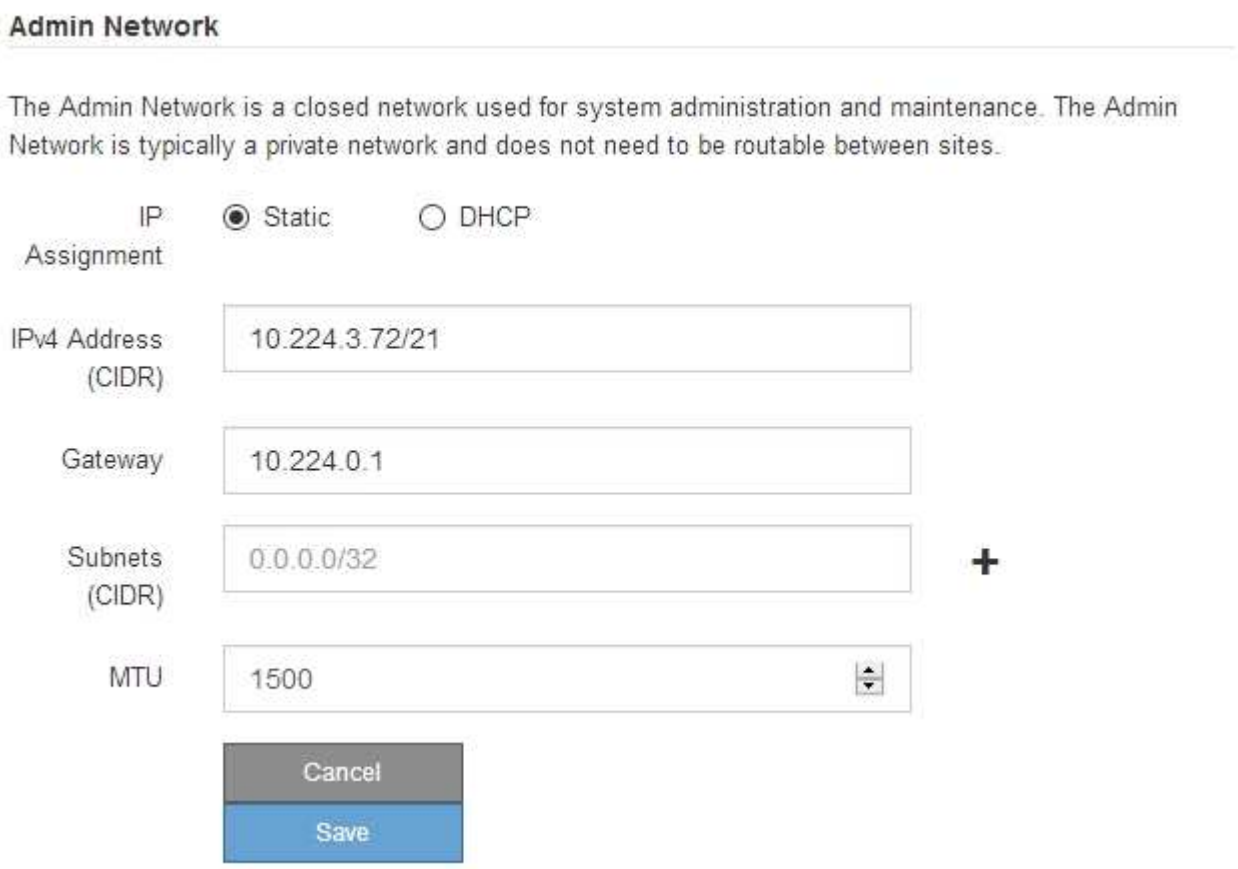
> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

> 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

a. 저장 * 을 클릭합니다.

5. 관리 네트워크를 구성하려면 페이지의 * 관리 네트워크 * 섹션에서 * 정적 * 또는 * DHCP * 를 선택합니다.

> 관리 네트워크를 구성하려면 링크 구성 페이지에서 관리 네트워크를 활성화해야 합니다.



6. 정적 * 을 선택한 경우 다음 단계에 따라 관리 네트워크를 구성합니다.

a. 어플라이언스의 관리 포트 1에 대한 CIDR 표기법을 사용하여 정적 IPv4 주소를 입력합니다.

   관리 포트 1은 어플라이언스의 오른쪽 끝에 있는 2개의 1GbE RJ45 포트 왼쪽에 있습니다.

b. 게이트웨이를 입력합니다.

   네트워크에 게이트웨이가 없는 경우 동일한 정적 IPv4 주소를 다시 입력합니다.

c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

   > 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

d. 저장 * 을 클릭합니다.

   IP 주소를 변경하면 게이트웨이와 서브넷 목록도 변경될 수 있습니다.

   StorageGRID 어플라이언스 설치 프로그램에 대한 연결이 끊어진 경우 방금 할당한 새 고정 IP 주소를 사용하여 URL을 다시 입력합니다. 예: + `https://services_appliance:8443*

e. 관리자 네트워크 서브넷 목록이 올바른지 확인합니다.

   입력한 게이트웨이를 사용하여 모든 서브넷에 연결할 수 있는지 확인해야 합니다.

   > 관리자 네트워크 게이트웨이를 사용하도록 기본 경로를 설정할 수 없습니다.

   - 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
   - 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

f. 저장 * 을 클릭합니다.

7. DHCP * 를 선택한 경우 다음 단계에 따라 관리 네트워크를 구성합니다.

   a. DHCP * 라디오 버튼을 선택한 후 * 저장 * 을 클릭합니다.

      IPv4 주소 *, * 게이트웨이 * 및 * 서브넷 * 필드가 자동으로 채워집니다. DHCP 서버가 MTU 값을 할당하도록 설정된 경우 * MTU * 필드가 해당 값으로 채워지고 필드는 읽기 전용이 됩니다.

      웹 브라우저가 자동으로 StorageGRID 어플라이언스 설치 프로그램의 새 IP 주소로 리디렉션됩니다.

   b. 관리자 네트워크 서브넷 목록이 올바른지 확인합니다.

      입력한 게이트웨이를 사용하여 모든 서브넷에 연결할 수 있는지 확인해야 합니다.

      > 관리자 네트워크 게이트웨이를 사용하도록 기본 경로를 설정할 수 없습니다.

      - 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
      - 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

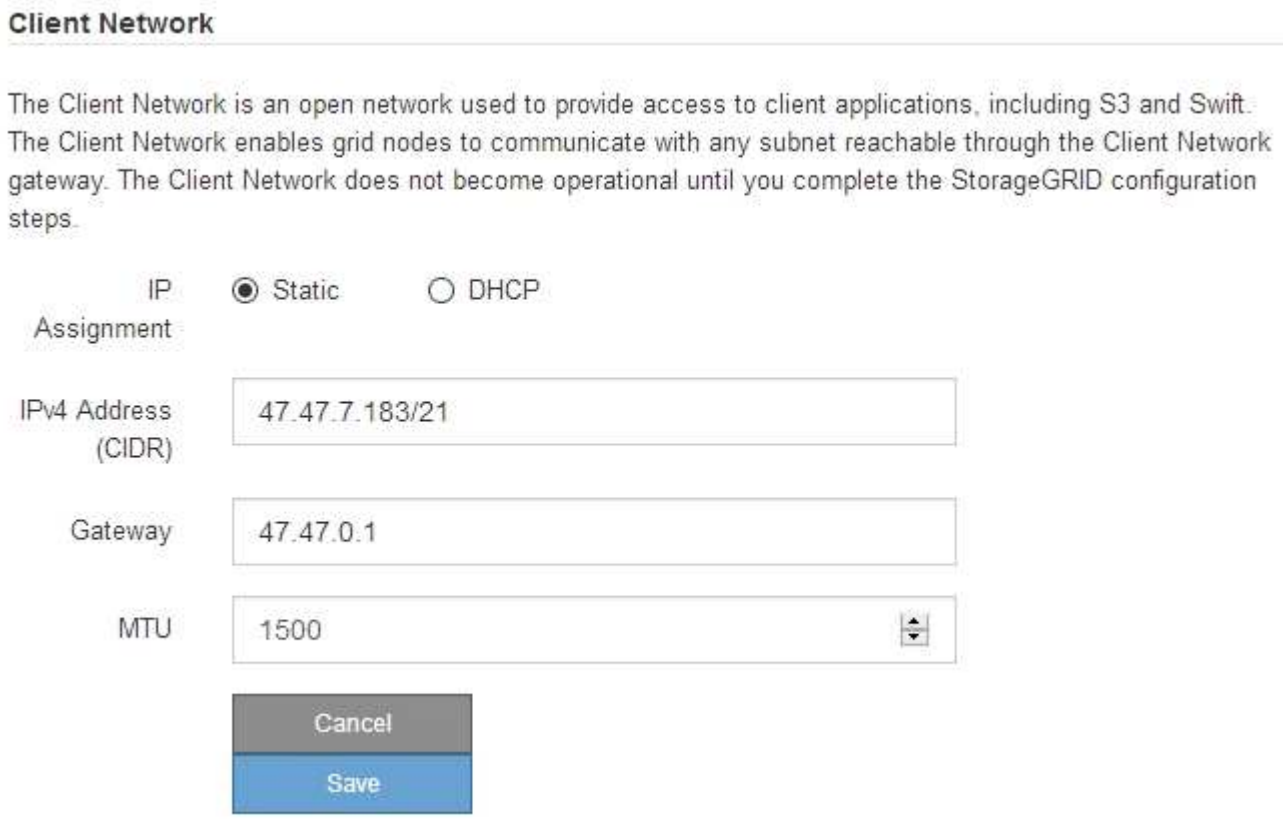
   c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

d. 저장 * 을 클릭합니다.

8. 클라이언트 네트워크를 구성하려면 페이지의 * 클라이언트 네트워크 * 섹션에서 * 정적 * 또는 * DHCP * 를 선택합니다.

> 클라이언트 네트워크를 구성하려면 링크 구성 페이지에서 클라이언트 네트워크를 활성화해야 합니다.



9. 정적 * 을 선택한 경우 다음 단계에 따라 클라이언트 네트워크를 구성합니다.

   a. CIDR 표기법을 사용하여 정적 IPv4 주소를 입력합니다.

   b. 저장 * 을 클릭합니다.

   c. 클라이언트 네트워크 게이트웨이의 IP 주소가 올바른지 확인합니다.

> 클라이언트 네트워크가 활성화된 경우 기본 경로가 표시됩니다. 기본 라우트는 클라이언트 네트워크 게이트웨이를 사용하며 클라이언트 네트워크가 활성화된 동안에는 다른 인터페이스로 이동할 수 없습니다.

   d. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

e. 저장 * 을 클릭합니다.

10. DHCP * 를 선택한 경우 다음 단계에 따라 클라이언트 네트워크를 구성합니다.

    a. DHCP * 라디오 버튼을 선택한 후 * 저장 * 을 클릭합니다.

       IPv4 주소 * 및 * 게이트웨이 * 필드가 자동으로 채워집니다. DHCP 서버가 MTU 값을 할당하도록 설정된 경우 * MTU * 필드가 해당 값으로 채워지고 필드는 읽기 전용이 됩니다.

웹 브라우저가 자동으로 StorageGRID 어플라이언스 설치 프로그램의 새 IP 주소로 리디렉션됩니다.

a. 게이트웨이가 올바른지 확인합니다.

> 클라이언트 네트워크가 활성화된 경우 기본 경로가 표시됩니다. 기본 라우트는 클라이언트 네트워크 게이트웨이를 사용하며 클라이언트 네트워크가 활성화된 동안에는 다른 인터페이스로 이동할 수 없습니다.

b. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

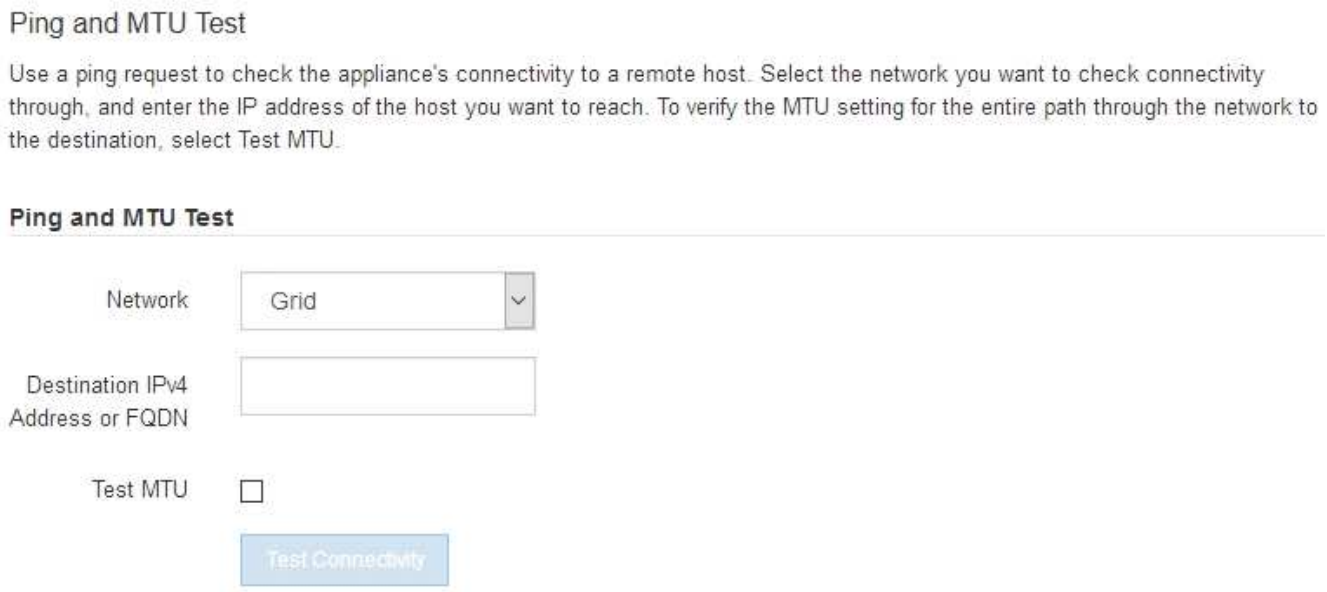
네트워크 연결을 확인합니다

어플라이언스에서 사용 중인 StorageGRID 네트워크에 액세스할 수 있는지 확인해야 합니다. 네트워크 게이트웨이를 통한 라우팅의 유효성을 검사하려면 StorageGRID 어플라이언스 설치 프로그램과 다른 서브넷의 IP 주소 간의 연결을 테스트해야 합니다. MTU 설정을 확인할 수도 있습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램의 메뉴 모음에서 * 네트워킹 구성 * > * Ping 및 MTU 테스트 * 를 클릭합니다.

   Ping 및 MTU 테스트 페이지가 나타납니다.



2. 네트워크 * 드롭다운 상자에서 테스트할 네트워크(그리드, 관리자 또는 클라이언트)를 선택합니다.
3. 해당 네트워크의 호스트에 대한 IPv4 주소 또는 FQDN(정규화된 도메인 이름)을 입력합니다.

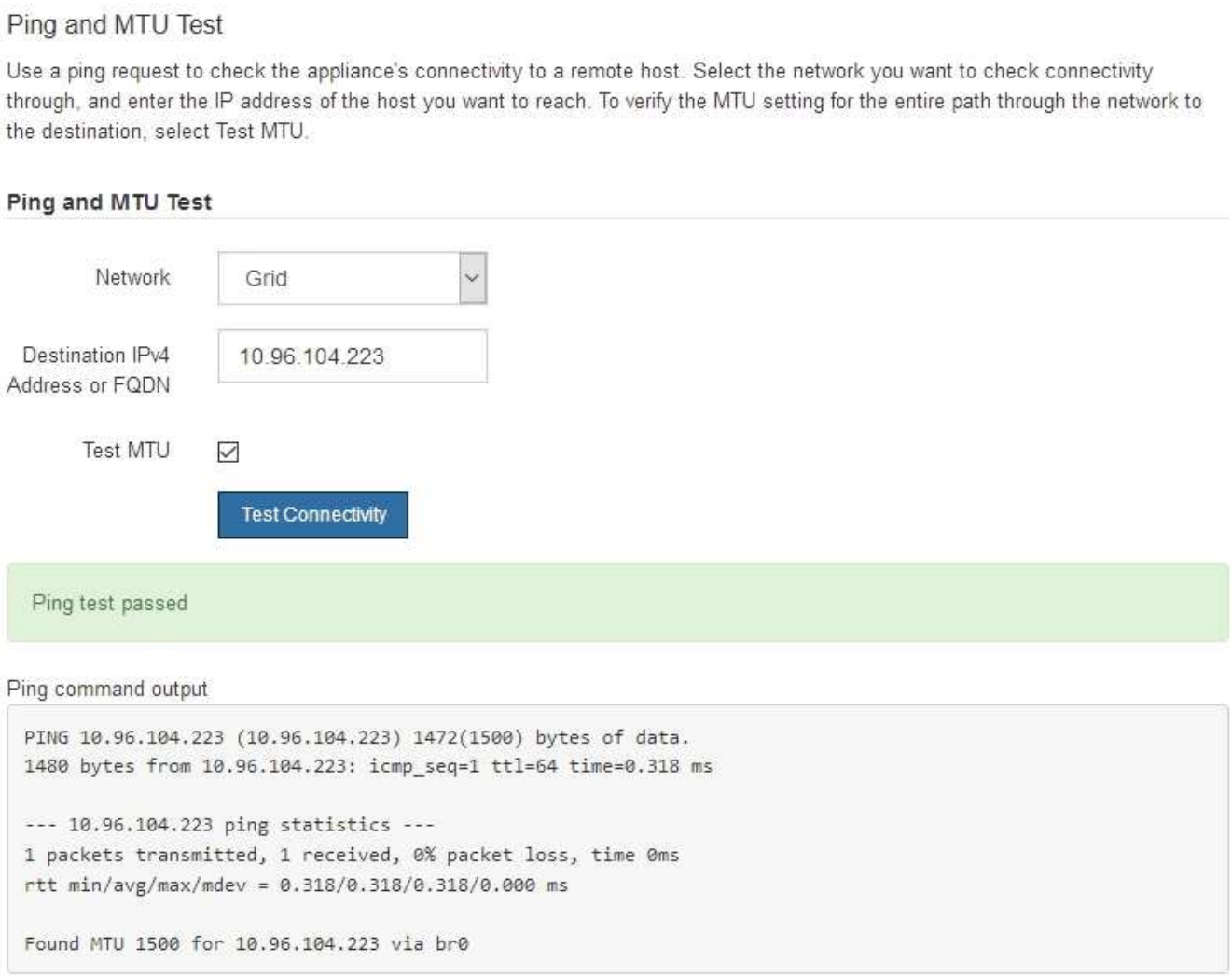
   예를 들어 네트워크 또는 기본 관리 노드의 게이트웨이를 Ping할 수 있습니다.

4. 선택적으로 * Test MTU * 확인란을 선택하여 네트워크를 통해 대상으로 가는 전체 경로에 대한 MTU 설정을 확인합니다.

   예를 들어, 어플라이언스 노드와 다른 사이트의 노드 간 경로를 테스트할 수 있습니다.

5. 연결 테스트 * 를 클릭합니다.

   네트워크 연결이 유효한 경우 ping 명령 출력이 나열된 "Ping test Passed" 메시지가 나타납니다.



관련 정보

네트워크 링크 구성(SG6000)

MTU 설정을 변경합니다

포트 수준 네트워크 연결을 확인합니다

StorageGRID 어플라이언스 설치 프로그램과 다른 노드 간의 액세스가 방화벽에 의해 방해 받지 않도록 하려면 StorageGRID 어플라이언스 설치 관리자가 지정된 IP 주소 또는 주소 범위의 특정 TCP 포트 또는 포트 집합에 연결할 수 있는지 확인합니다.

이 작업에 대해

StorageGRID 어플라이언스 설치 프로그램에 제공된 포트 목록을 사용하여 어플라이언스와 그리드 네트워크의 다른 노드 간의 연결을 테스트할 수 있습니다.

또한 외부 NFS 또는 DNS 서버에 사용되는 것과 같은 UDP 포트와 Admin 및 Client Networks에서 연결을 테스트할 수 있습니다. 이러한 포트 목록은 StorageGRID 네트워킹 지침의 포트 참조를 참조하십시오.

> 포트 연결 테이블에 나열된 그리드 네트워크 포트는 StorageGRID 버전 11.6.0에만 유효합니다. 각 노드 유형에 맞는 포트를 확인하려면 사용 중인 StorageGRID 버전에 대한 네트워킹 지침을 항상 참조해야 합니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * 포트 연결 테스트(nmap) * 를 클릭합니다.

   포트 연결 테스트 페이지가 나타납니다.

   포트 연결 표에는 그리드 네트워크에서 TCP 연결이 필요한 노드 유형이 나와 있습니다. 각 노드 유형에 대해 표에는 어플라이언스에 액세스할 수 있어야 하는 그리드 네트워크 포트가 나열되어 있습니다.

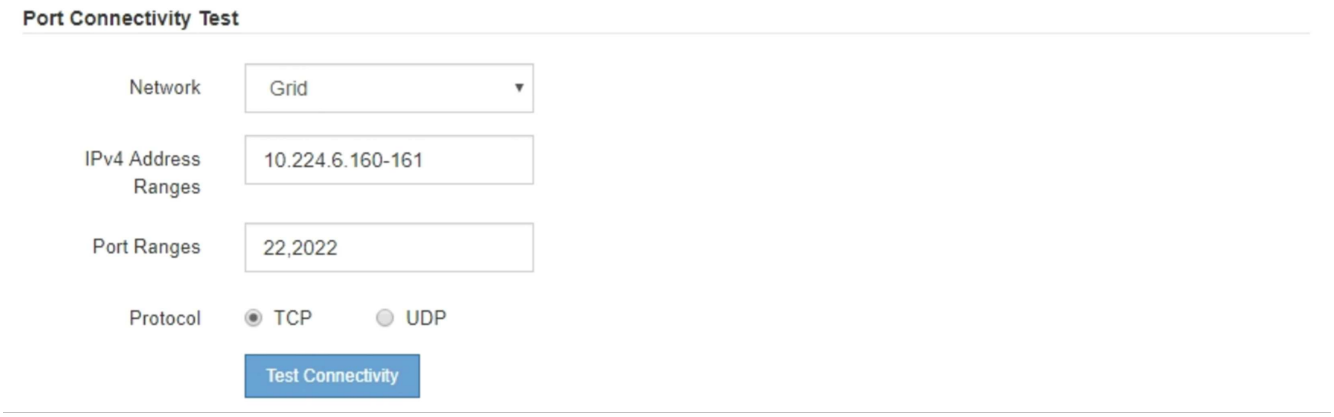
   표에 나열된 어플라이언스 포트와 그리드 네트워크의 다른 노드 간의 연결을 테스트할 수 있습니다.

2. Network * (네트워크 **)** 드롭다운에서 *** Grid * (**그리드 ***), * Admin * (** 관리자 *) 또는 * Client * (클라이언트 *)와 같이 테스트할 네트워크를 선택합니다.
3. 해당 네트워크의 호스트에 대한 IPv4 주소 범위를 지정합니다.

   예를 들어 네트워크 또는 기본 관리 노드의 게이트웨이를 조사할 수 있습니다.

   예제에 표시된 대로 하이픈을 사용하여 범위를 지정합니다.

4. TCP 포트 번호, 쉼표로 구분된 포트 목록 또는 포트 범위를 입력합니다.



5. 연결 테스트 * 를 클릭합니다.

   - 선택한 포트 수준 네트워크 연결이 유효하면 ""포트 연결 테스트 통과"" 메시지가 녹색 배너에 나타납니다. nmap 명령 출력은 배너 아래에 나열되어 있습니다.

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- 원격 호스트에 대한 포트 수준 네트워크 연결이 이루어졌지만 호스트가 선택한 포트 중 하나 이상의 포트에서 수신 대기 중이 아니면 ""포트 연결 테스트 실패" 메시지가 노란색 배너에 나타납니다. nmap 명령 출력은 배너 아래에 나열되어 있습니다.

  호스트가 청취하지 않는 모든 원격 포트는 ""닫힘"" 상태입니다. 예를 들어 연결하려는 노드가 사전 설치된 상태이고 StorageGRID NMS 서비스가 아직 실행되지 않은 경우 이 노란색 배너가 나타날 수 있습니다.

Port connectivity test failed
Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
1504/tcp closed evb-elm
1505/tcp open   funkproxy
1506/tcp open   utcd
1508/tcp open   diagmond
7443/tcp open   oracleas-https
9999/tcp open   abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- 하나 이상의 선택한 포트에 대해 포트 수준 네트워크 연결을 설정할 수 없는 경우 빨간색 배너에 ""포트 연결 테스트 실패" 메시지가 나타납니다. nmap 명령 출력은 배너 아래에 나열되어 있습니다.

  빨간색 배너는 원격 호스트의 포트에 대한 TCP 연결 시도가 이루어졌지만 보낸 사람에게 반환된 것이 없음을 나타냅니다. 응답이 반환되지 않으면 포트에 "필터링된" 상태가 있으며 방화벽에 의해 차단될 수 있습니다.

  ⓘ 폐쇄된 항만 목록에 있다.

Port connectivity test failed
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT     STATE    SERVICE
22/tcp   open     ssh
79/tcp   filtered finger
80/tcp   open     http
443/tcp  open     https
1504/tcp closed   evb-elm
1505/tcp open     funkproxy
1506/tcp open     utcd
1508/tcp open     diagmond
7443/tcp open     oracleas-https
9999/tcp open     abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

관련 정보

네트워킹 지침

SG6000(SANtricity System Manager) 액세스 및 구성

SANtricity 시스템 관리자를 사용하여 스토리지 컨트롤러 쉘프에 있는 스토리지 컨트롤러, 스토리지 디스크 및 기타 하드웨어 구성 요소의 상태를 모니터링할 수 있습니다. 또한 관리 포트를 사용하지 않고 어플라이언스에서 AutoSupport 메시지를 보낼 수 있도록 E-Series AutoSupport에 대한 프록시를 구성할 수도 있습니다.

SANtricity 시스템 관리자를 설정하고 액세스합니다

스토리지 컨트롤러의 하드웨어를 모니터링하거나 E-Series AutoSupport를 구성하려면 스토리지 컨트롤러의 SANtricity System Manager에 액세스해야 할 수 있습니다.

필요한 것

- 을(를) 사용하고 있습니다 지원되는 웹 브라우저.
- 그리드 관리자를 통해 SANtricity 시스템 관리자에 액세스하려면 StorageGRID가 설치되어 있어야 하며 스토리지 어플라이언스 관리자 권한이나 루트 액세스 권한이 있어야 합니다.
- StorageGRID 어플라이언스 설치 프로그램을 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 시스템 관리자 사용자 이름과 암호가 있어야 합니다.
- 웹 브라우저를 통해 SANtricity System Manager에 직접 액세스하려면 SANtricity System Manager 관리자의 사용자 이름과 암호가 있어야 합니다.

> 그리드 관리자 또는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 펌웨어 8.70(11.70) 이상이 있어야 합니다. StorageGRID 어플라이언스 설치 프로그램을 사용하여 * 도움말 * > * 정보 * 를 선택하여 펌웨어 버전을 확인할 수 있습니다.

> 그리드 관리자 또는 어플라이언스 설치 프로그램에서 SANtricity 시스템 관리자에 액세스하는 것은 일반적으로 하드웨어를 모니터링하고 E-Series AutoSupport를 구성하는 데만 사용됩니다. 펌웨어 업그레이드와 같은 SANtricity System Manager 내의 많은 기능과 작업은 StorageGRID 어플라이언스 모니터링에는 적용되지 않습니다. 문제를 방지하려면 항상 어플라이언스에 대한 하드웨어 설치 및 유지 관리 지침을 따르십시오.

이 작업에 대해

설치 및 구성 프로세스 단계에 따라 SANtricity System Manager에 액세스하는 방법에는 세 가지가 있습니다.

- 어플라이언스가 아직 StorageGRID 시스템에 노드로 배포되지 않은 경우 StorageGRID 어플라이언스 설치 프로그램의 고급 탭을 사용해야 합니다.

  > 노드가 배포되면 StorageGRID 어플라이언스 설치 프로그램을 사용하여 SANtricity 시스템 관리자에 액세스할 수 없습니다.

- 어플라이언스가 StorageGRID 시스템에서 노드로 구축된 경우 그리드 관리자의 노드 페이지에서 SANtricity 시스템 관리자 탭을 사용합니다.
- StorageGRID 어플라이언스 설치 관리자 또는 그리드 관리자를 사용할 수 없는 경우 관리 포트에 연결된 웹 브라우저를 사용하여 SANtricity 시스템 관리자에 직접 액세스할 수 있습니다.

이 절차에는 SANtricity 시스템 관리자에 대한 초기 액세스 단계가 포함되어 있습니다. SANtricity 시스템 관리자를 이미 설정한 경우 로 이동합니다 하드웨어 경고 단계를 구성합니다.

> 그리드 관리자 또는 StorageGRID 어플라이언스 설치 프로그램을 사용하면 어플라이언스의 관리 포트를 구성하거나 연결하지 않고도 SANtricity 시스템 관리자에 액세스할 수 있습니다.

SANtricity 시스템 관리자를 사용하여 다음을 모니터링할 수 있습니다.

- 스토리지 어레이 레벨 성능, I/O 지연 시간, CPU 활용률, 처리량 등의 성능 데이터
- 하드웨어 구성 요소 상태입니다
- 진단 데이터 보기를 포함한 지원 기능

SANtricity 시스템 관리자를 사용하여 다음 설정을 구성할 수 있습니다.

- 스토리지 컨트롤러 쉘프에 있는 구성 요소에 대한 e-메일 경고, SNMP 경고 또는 syslog 알림을 제공합니다
- 스토리지 컨트롤러 쉘프의 구성요소에 대한 E-Series AutoSupport 설정입니다.

  E-Series AutoSupport에 대한 자세한 내용은 를 참조하십시오 "NetApp E-Series 시스템 문서 사이트".

- 드라이브 보안 키 - 보안 드라이브 잠금을 해제하는 데 필요(드라이브 보안 기능이 활성화된 경우 이 단계 필요)
- SANtricity 시스템 관리자에 액세스하기 위한 관리자 암호입니다

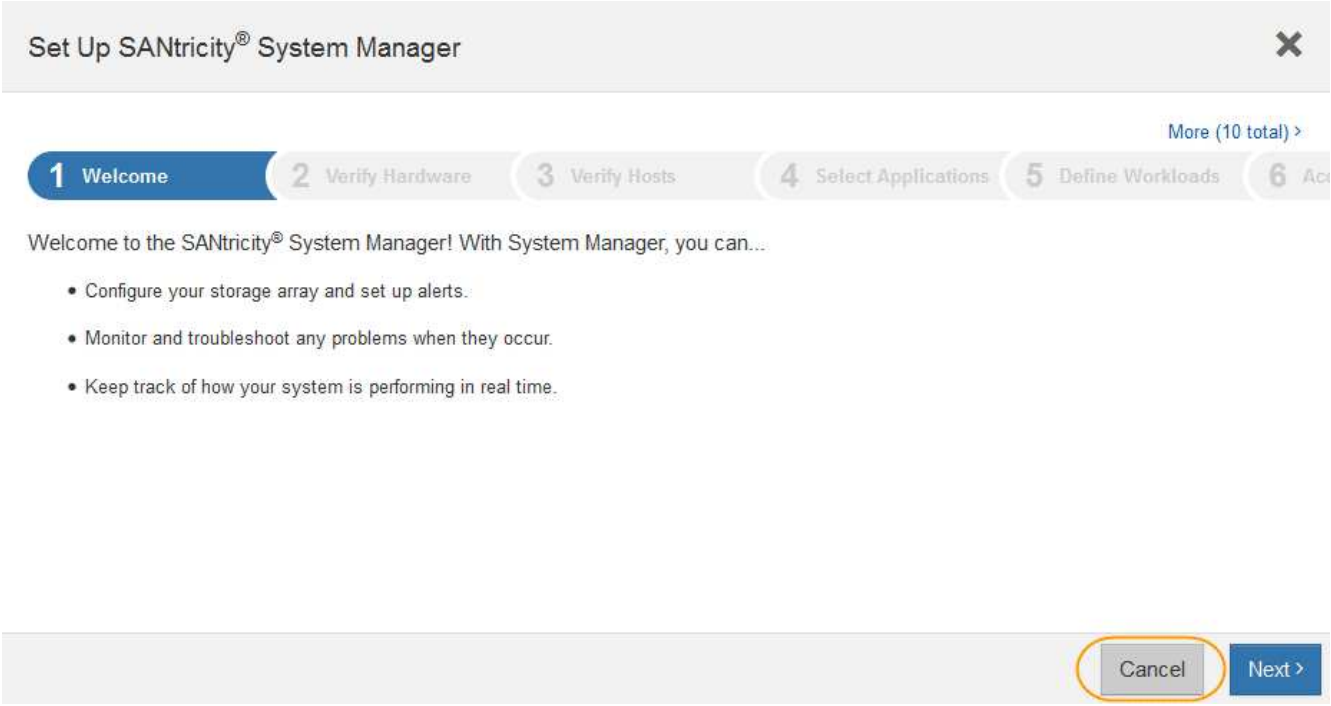
단계

1. StorageGRID 어플라이언스 설치 프로그램을 사용하여 * 고급 * > * SANtricity 시스템 관리자 * 를 선택합니다

> StorageGRID 어플라이언스 설치 프로그램을 사용할 수 없거나 로그인 페이지가 나타나지 않으면 를 사용해야 합니다 스토리지 컨트롤러의 IP 주소입니다. 스토리지 컨트롤러 IP로 이동하여 SANtricity System Manager에 액세스합니다.

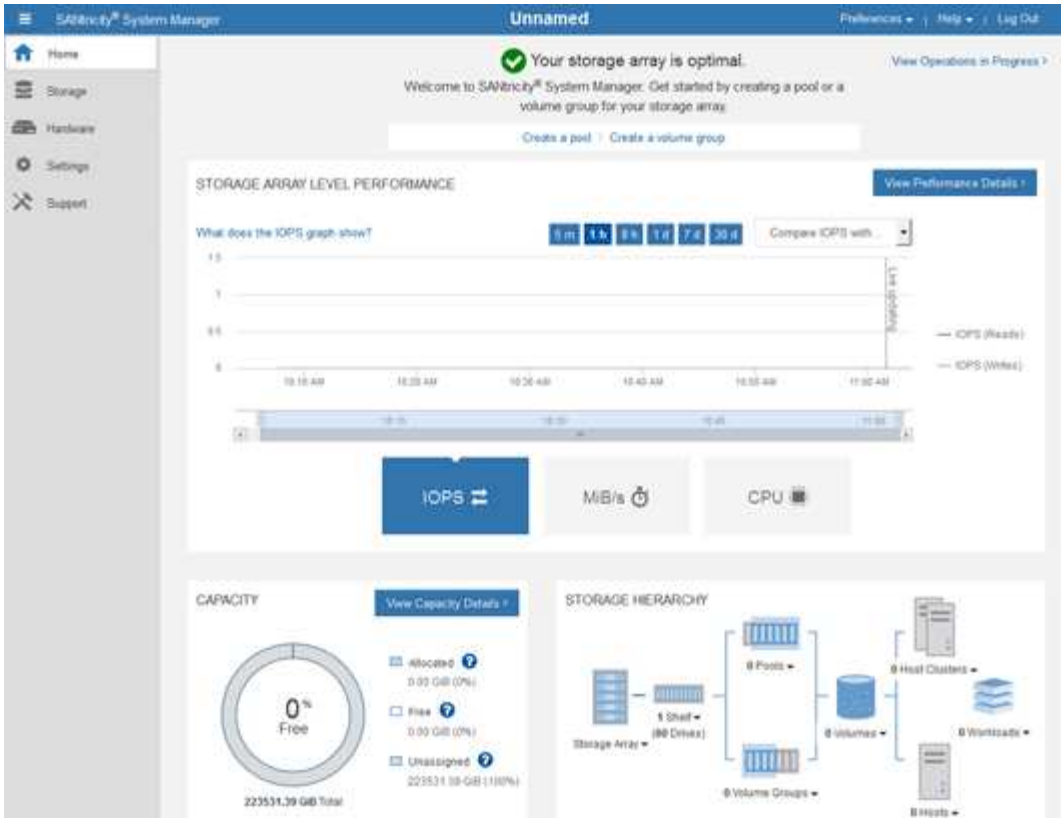
2. 관리자 암호를 설정하거나 입력합니다.

   SANtricity 시스템 관리자는 모든 사용자가 공유하는 단일 관리자 암호를 사용합니다.



3. 마법사를 닫으려면 * 취소 * 를 선택하십시오.

> StorageGRID 어플라이언스에 대한 설정 마법사를 완료하지 마십시오.



4. 하드웨어 경고를 구성합니다.
   a. SANtricity 시스템 관리자의 온라인 도움말을 보려면 * 도움말 * 을 선택하십시오.
   b. 온라인 도움말의 * 설정 * > * 알림 * 섹션을 사용하여 알림에 대해 알아보십시오.
   c. ""방법" 지침에 따라 e-메일 경고, SNMP 경고 또는 syslog 알림을 설정합니다.
5. 스토리지 컨트롤러 쉘프의 구성요소에 대한 AutoSupport를 관리합니다.
   a. SANtricity 시스템 관리자의 온라인 도움말을 보려면 * 도움말 * 을 선택하십시오.
   b. 온라인 도움말의 * 지원 * > * 지원 센터 * 섹션을 사용하여 AutoSupport 기능에 대해 알아보십시오.
   c. AutoSupport를 관리하려면 ""방법" 지침을 따르십시오.

      관리 포트를 사용하지 않고 E-Series AutoSupport 메시지를 보내기 위해 StorageGRID 프록시를 구성하는 방법에 대한 자세한 내용은 로 이동하십시오 스토리지 프록시 설정 구성 지침.
6. 어플라이언스에 대해 드라이브 보안 기능이 활성화된 경우 보안 키를 생성하고 관리합니다.
   a. SANtricity 시스템 관리자의 온라인 도움말을 보려면 * 도움말 * 을 선택하십시오.
   b. 드라이브 보안에 대해 알아보려면 온라인 도움말의 * 설정 * > * 시스템 * > * 보안 키 관리 * 섹션을 사용하십시오.
   c. ""방법" 지침에 따라 보안 키를 만들고 관리합니다.
7. 필요에 따라 관리자 암호를 변경합니다.
   a. SANtricity 시스템 관리자의 온라인 도움말을 보려면 * 도움말 * 을 선택하십시오.
   b. 온라인 도움말의 * Home * > * 스토리지 배열 관리 * 섹션을 사용하여 관리자 암호에 대해 알아보십시오.
   c. ""방법" 지침에 따라 암호를 변경하십시오.

SANtricity 시스템 관리자를 사용하여 스토리지 컨트롤러 쉘프의 개별 하드웨어 구성요소를 모니터링 및 관리하고 하드웨어 진단 및 환경 정보(예: 구성요소 온도)와 드라이브 관련 문제를 검토할 수 있습니다.

필요한 것

- 을(를) 사용하고 있습니다 지원되는 웹 브라우저.
- 그리드 관리자를 통해 SANtricity 시스템 관리자에 액세스하려면 스토리지 어플라이언스 관리자 권한이나 루트 액세스 권한이 있어야 합니다.
- StorageGRID 어플라이언스 설치 프로그램을 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 시스템 관리자 사용자 이름과 암호가 있어야 합니다.
- 웹 브라우저를 통해 SANtricity System Manager에 직접 액세스하려면 SANtricity System Manager 관리자의 사용자 이름과 암호가 있어야 합니다.

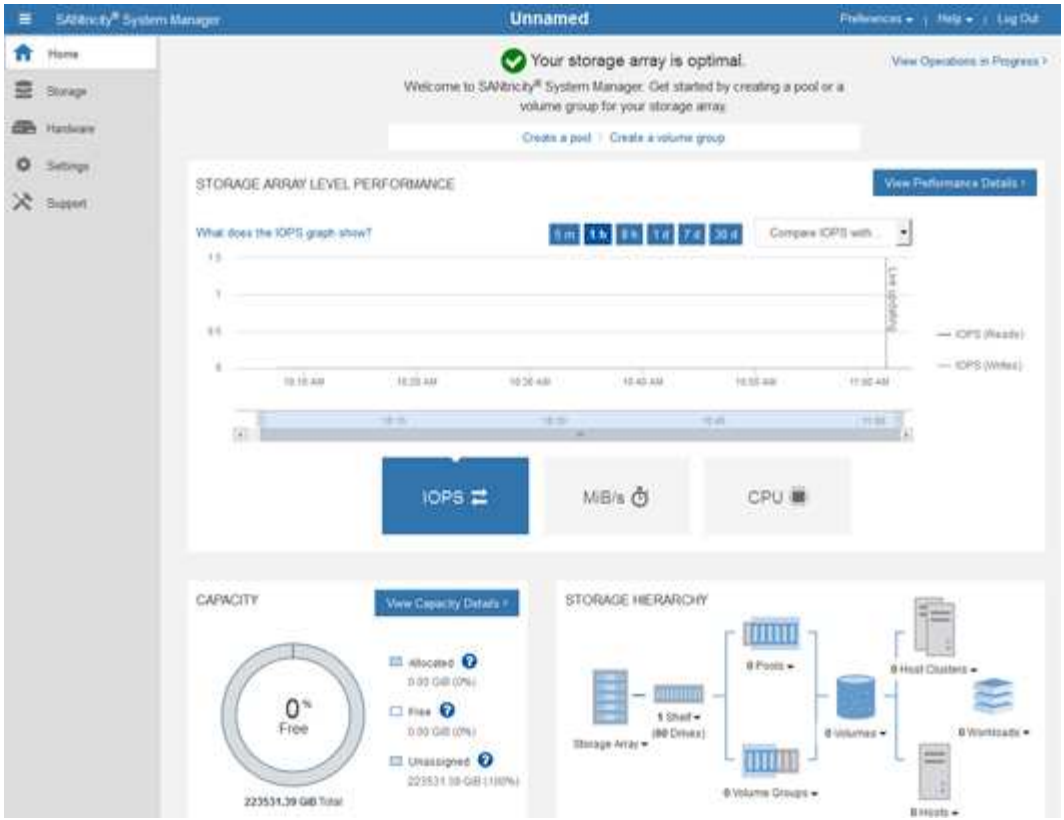
> 그리드 관리자 또는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 펌웨어 8.70(11.70) 이상이 있어야 합니다.

> 그리드 관리자 또는 어플라이언스 설치 프로그램에서 SANtricity 시스템 관리자에 액세스하는 것은 일반적으로 하드웨어를 모니터링하고 E-Series AutoSupport를 구성하는 데만 사용됩니다. 펌웨어 업그레이드와 같은 SANtricity System Manager 내의 많은 기능과 작업은 StorageGRID 어플라이언스 모니터링에는 적용되지 않습니다. 문제를 방지하려면 항상 어플라이언스에 대한 하드웨어 설치 및 유지 관리 지침을 따르십시오.

단계

1. SANtricity 시스템 관리자에 액세스합니다.
2. 필요한 경우 관리자 사용자 이름과 암호를 입력합니다.
3. 설정 마법사를 닫고 SANtricity 시스템 관리자 홈 페이지를 표시하려면 * 취소 * 를 클릭합니다.

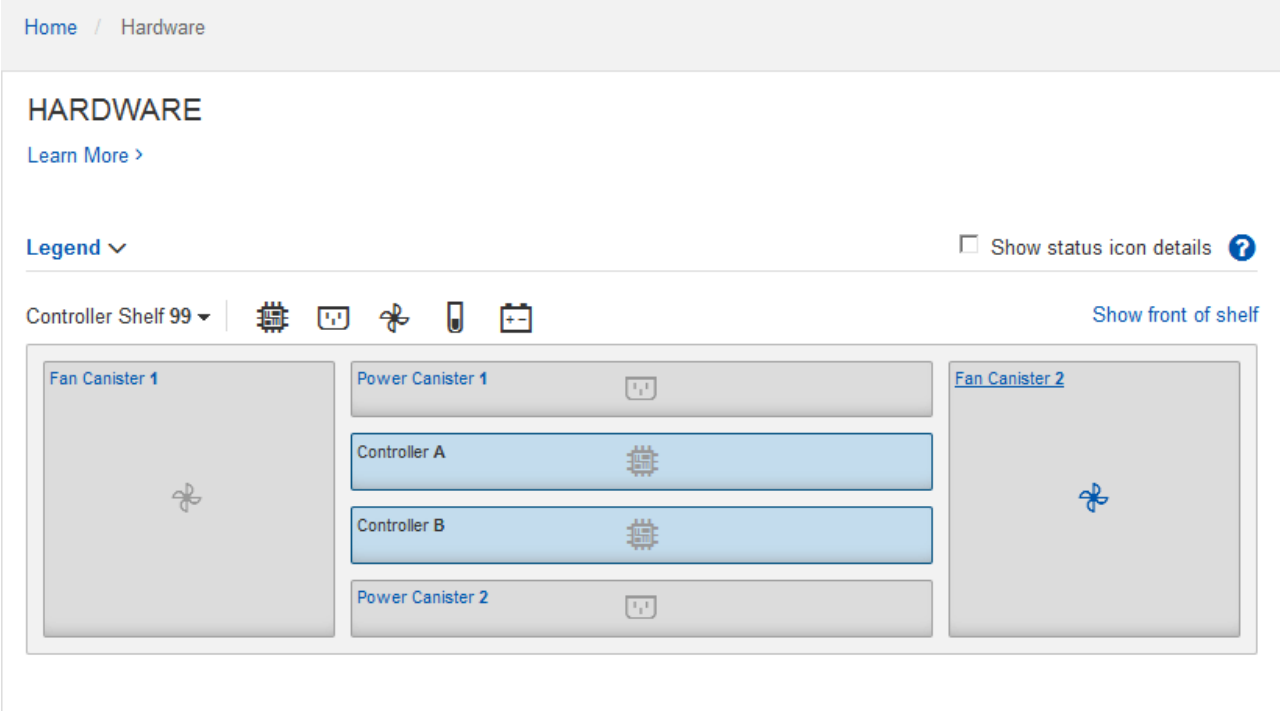
   SANtricity 시스템 관리자 홈 페이지가 나타납니다. SANtricity 시스템 관리자에서 컨트롤러 쉘프는 스토리지 어레이라고 합니다.



4. 어플라이언스 하드웨어에 대해 표시된 정보를 검토하고 모든 하드웨어 구성 요소의 상태가 Optimal(최적)인지 확인합니다.

   a. 하드웨어 * 탭을 클릭합니다.

   b. Show back of shelf * 를 클릭합니다.



쉘프 후면에서 각 스토리지 컨트롤러의 배터리, 2개의 전원 캐니스터, 2개의 팬 캐니스터 및 확장 쉘프(있는 경우)를

모두 볼 수 있습니다. 부품 온도를 볼 수도 있습니다.

a. 각 스토리지 컨트롤러의 설정을 보려면 컨트롤러를 선택하고 컨텍스트 메뉴에서 * 설정 보기 * 를 선택합니다.

b. 쉘프 뒷면에 있는 다른 구성 요소의 설정을 보려면 보려는 구성 요소를 선택합니다.

c. Show front of shelf * 를 클릭하고 보려는 부품을 선택합니다.

   쉘프 전면에서 스토리지 컨트롤러 쉘프 또는 확장 쉘프(있는 경우)에 대한 드라이브 및 드라이브 드로어를 볼 수 있습니다.

구성 요소의 상태에 주의가 필요한 경우 Recovery Guru의 단계에 따라 문제를 해결하거나 기술 지원 부서에 문의하십시오.

StorageGRID 어플라이언스 설치 프로그램을 사용하여 스토리지 컨트롤러의 **IP** 주소를 설정합니다

각 스토리지 컨트롤러의 관리 포트 1은 어플라이언스를 SANtricity 시스템 관리자의 관리 네트워크에 연결합니다. StorageGRID 어플라이언스 설치 프로그램에서 SANtricity 시스템 관리자에 액세스할 수 없는 경우 각 스토리지 컨트롤러의 고정 IP 주소를 설정하여 컨트롤러 쉘프에 있는 하드웨어 및 컨트롤러 펌웨어에 대한 관리 연결이 끊어지지 않도록 해야 합니다.

필요한 것

- StorageGRID 관리 네트워크에 연결할 수 있는 관리 클라이언트를 사용 중이거나 서비스 랩톱을 사용 중입니다.
- 클라이언트 또는 서비스 랩톱에 지원되는 웹 브라우저가 있습니다.

이 작업에 대해

DHCP 할당 주소는 언제든지 변경할 수 있습니다. 고정 IP 주소를 컨트롤러에 할당하여 일관성 있는 접근성을 보장합니다.

> StorageGRID 어플라이언스 설치 프로그램(* 고급*>* SANtricity 시스템 관리자*) 또는 그리드 관리자(* 노드*>* SANtricity 시스템 관리자*)에서 SANtricity 시스템 관리자에 액세스할 수 없는 경우에만 이 절차를 따르십시오.

단계

1. 클라이언트에서 StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. +
   `https://Appliance_Controller_IP:8443*`

   '*Appliance_Controller_IP*'의 경우 StorageGRID 네트워크에서 어플라이언스의 IP 주소를 사용합니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 하드웨어 구성 * > * 스토리지 컨트롤러 네트워크 구성 * 을 선택합니다.

   스토리지 컨트롤러 네트워크 구성 페이지가 나타납니다.

3. 네트워크 구성에 따라 IPv4, IPv6 또는 둘 다에 대해 * Enabled * 를 선택합니다.
4. 자동으로 표시되는 IPv4 주소를 기록해 둡니다.

   DHCP는 스토리지 컨트롤러 관리 포트에 IP 주소를 할당하는 기본 방법입니다.

DHCP 값이 나타나려면 몇 분 정도 걸릴 수 있습니다.

5. 필요에 따라 스토리지 컨트롤러 관리 포트에 대한 정적 IP 주소를 설정합니다.

   관리 포트에 고정 IP를 할당하거나 DHCP 서버의 주소에 영구 임대를 할당해야 합니다.

   a. Static * 을 선택합니다.
   b. CIDR 표기법을 사용하여 IPv4 주소를 입력합니다.
   c. 기본 게이트웨이를 입력합니다.

   d. 저장 * 을 클릭합니다.

      변경 사항을 적용하는 데 몇 분 정도 걸릴 수 있습니다.

   SANtricity System Manager에 연결할 때 새 고정 IP 주소를 URL: + `https://Storage_Controller_IP*` 사용합니다

BMC 인터페이스**(SG6000)** 구성

SG6000-CN 컨트롤러의 BMC(베이스보드 관리 컨트롤러)에 대한 사용자 인터페이스는 하드웨어에 대한 상태 정보를 제공하며 SG6000-CN 컨트롤러에 대한 SNMP 설정 및 기타 옵션을 구성할 수 있습니다.

BMC 인터페이스의 루트 암호를 변경합니다

보안을 위해 BMC 루트 사용자의 암호를 변경해야 합니다.

필요한 것

- 관리 클라이언트에서 을 사용하고 있습니다 지원되는 웹 브라우저.

이 작업에 대해

어플라이언스를 처음 설치할 때 BMC는 루트 사용자('root/calvin')의 기본 암호를 사용합니다. 시스템을 보호하려면 루트 사용자의 암호를 변경해야 합니다.

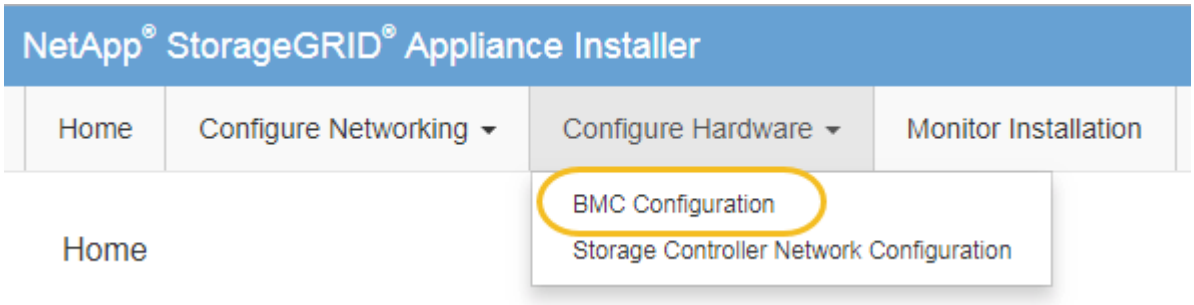
단계

1. 클라이언트에서 StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. + `https://Appliance_Controller_IP:8443*`

   '*Appliance_Controller_IP*'의 경우 StorageGRID 네트워크에서 어플라이언스의 IP 주소를 사용합니다.

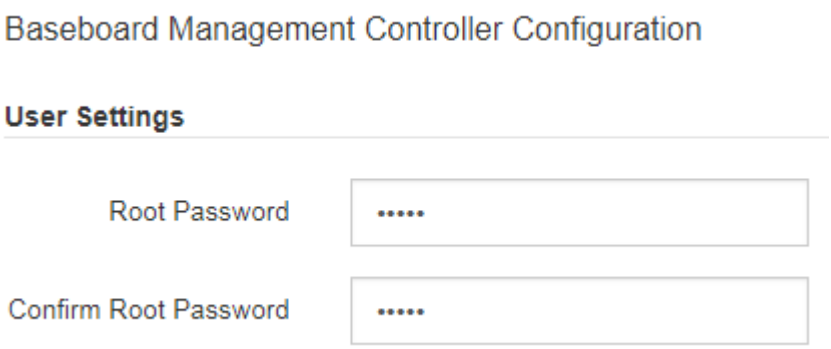
   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 하드웨어 구성 * > * BMC 구성 * 을 선택합니다.



   베이스보드 관리 컨트롤러 구성 페이지가 나타납니다.

3. 제공된 두 필드에 루트 계정에 대한 새 암호를 입력합니다.



4. 저장 * 을 클릭합니다.

BMC 관리 포트의 **IP** 주소를 설정합니다

BMC 인터페이스에 액세스하려면 SG6000-CN 컨트롤러의 BMC 관리 포트에 대한 IP 주소를 구성해야 합니다.

필요한 것

- 관리 클라이언트에서 을 사용하고 있습니다 지원되는 웹 브라우저.
- StorageGRID 네트워크에 연결할 수 있는 관리 클라이언트를 사용 중입니다.
- BMC 관리 포트가 사용하려는 관리 네트워크에 연결되어 있습니다.

이 작업에 대해

지원을 위해 BMC 관리 포트를 사용하면 낮은 수준의 하드웨어 액세스가 가능합니다.

> 이 포트는 안전하고 신뢰할 수 있는 내부 관리 네트워크에만 연결해야 합니다. 이러한 네트워크를 사용할 수 없는 경우 기술 지원 부서에서 BMC 연결을 요청하지 않는 한 BMC 포트는 연결되지 않거나 차단된 상태로 둡니다.

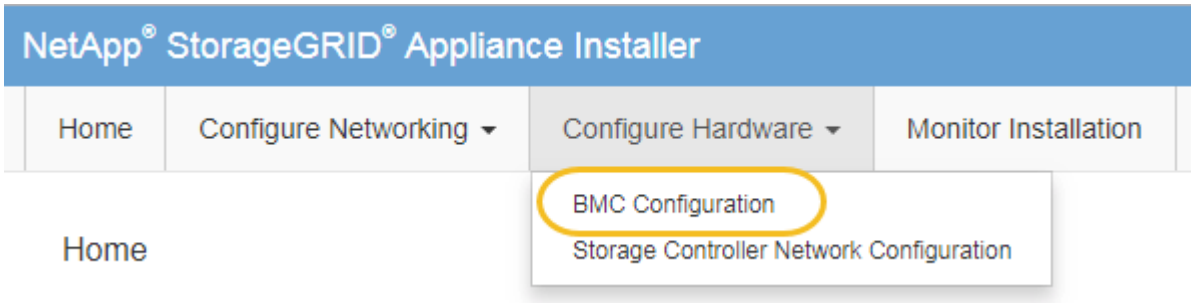
단계

1. 클라이언트에서 StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. + `https://SG6000-CN_Controller_IP:8443*`

   'G6000-CN_Controller_IP'의 경우, 모든 StorageGRID 네트워크에서 어플라이언스의 IP 주소를 사용한다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 하드웨어 구성 * > * BMC 구성 * 을 선택합니다.

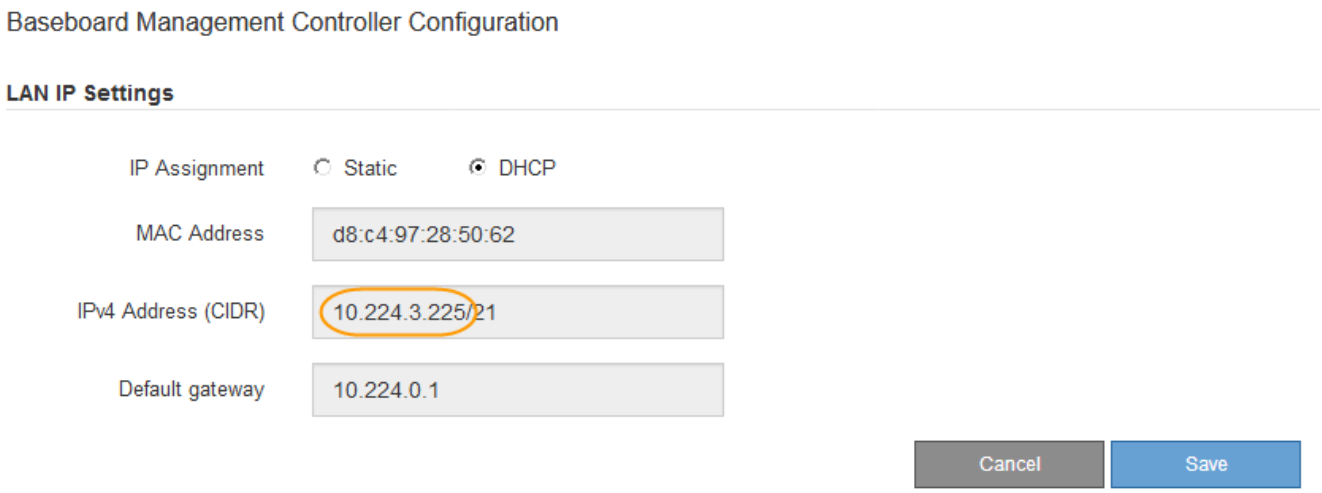


   베이스보드 관리 컨트롤러 구성 페이지가 나타납니다.

3. 자동으로 표시되는 IPv4 주소를 기록해 둡니다.

   DHCP는 이 포트에 IP 주소를 할당하는 기본 방법입니다.

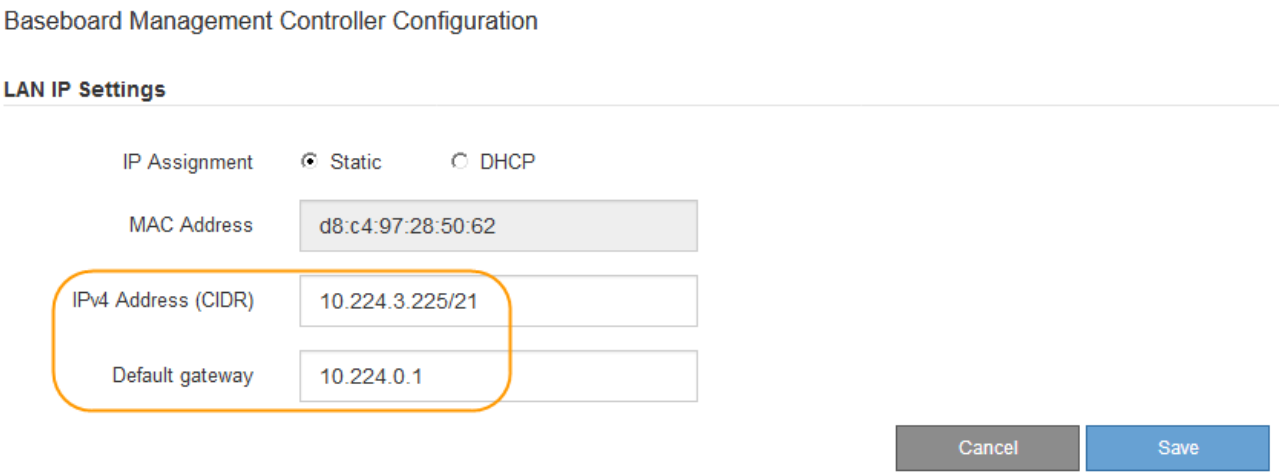
   > DHCP 값이 나타나려면 몇 분 정도 걸릴 수 있습니다.



4. 필요에 따라 BMC 관리 포트에 대한 정적 IP 주소를 설정합니다.

   BMC 관리 포트에 고정 IP를 할당하거나 DHCP 서버의 주소에 영구 임대를 할당해야 합니다.

   a. Static * 을 선택합니다.
   b. CIDR 표기법을 사용하여 IPv4 주소를 입력합니다.
   c. 기본 게이트웨이를 입력합니다.



   d. 저장 * 을 클릭합니다.

      변경 사항을 적용하는 데 몇 분 정도 걸릴 수 있습니다.

BMC 인터페이스에 액세스합니다

BMC 관리 포트의 DHCP 또는 고정 IP 주소를 사용하여 SG6000-CN 컨트롤러의 BMC 인터페이스에 액세스할 수 있습니다.

필요한 것

- SG6000-CN 컨트롤러의 BMC 관리 포트가 사용하려는 관리 네트워크에 연결되어 있습니다.

- 관리 클라이언트에서 을 사용하고 있습니다 지원되는 웹 브라우저.

단계

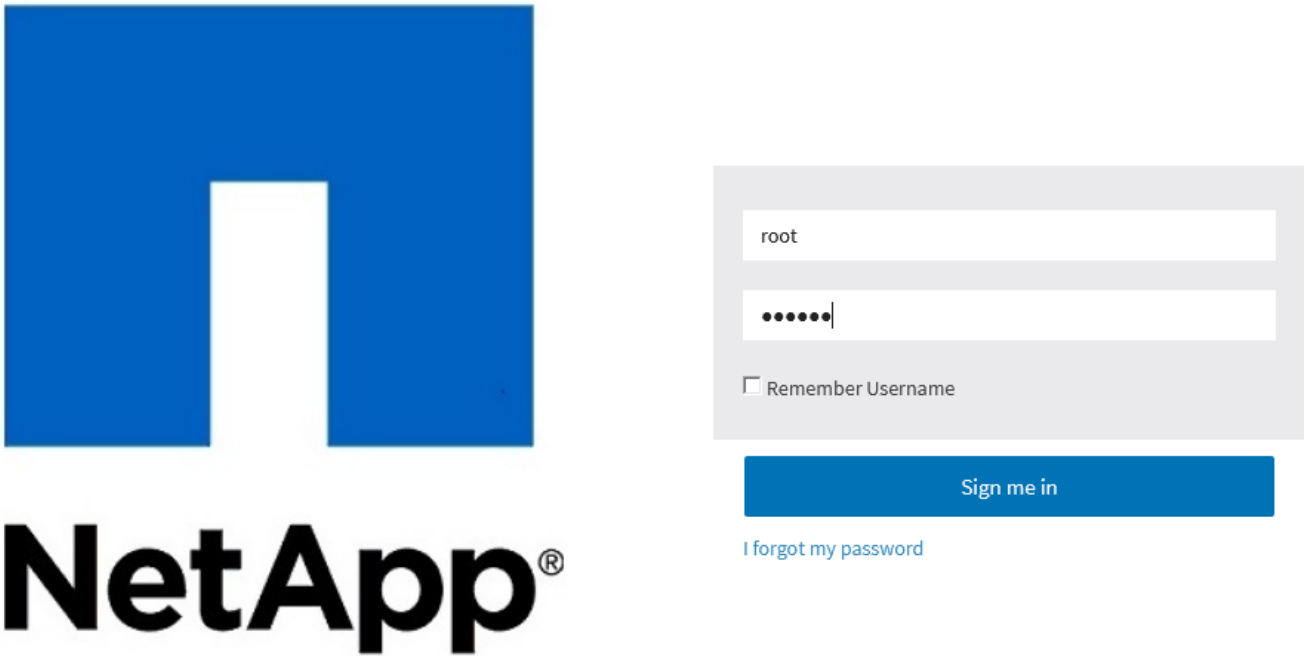
1. BMC 인터페이스의 URL을 입력합니다: + `https://*BMC_Port_IP*`

   '*BMC_Port_IP*'의 경우 BMC 관리 포트에 대해 DHCP 또는 고정 IP 주소를 사용합니다.

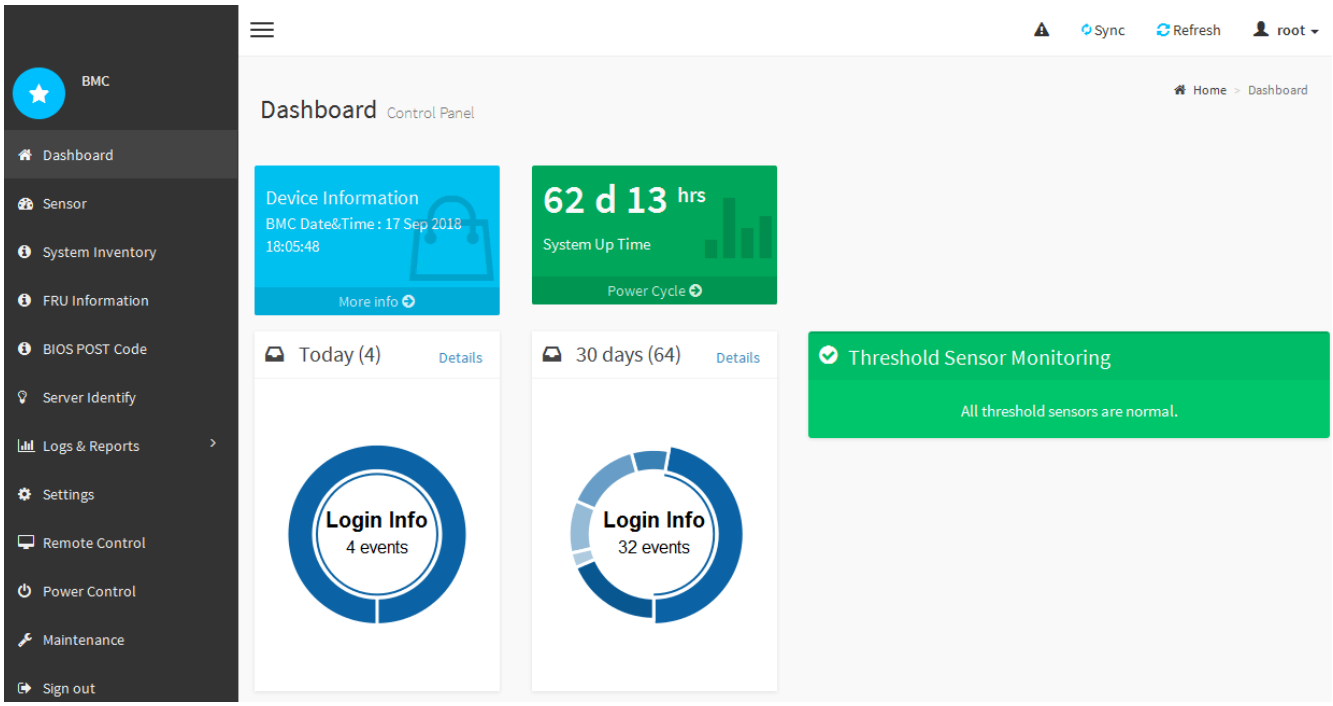
   BMC 로그인 페이지가 나타납니다.

   > 아직 BMC_Port_IP를 구성하지 않은 경우 의 지침을 따르십시오 BMC 인터페이스(SG6000) 구성. 하드웨어 문제로 인해 해당 절차를 수행할 수 없고 아직 BMC IP 주소를 구성하지 않은 경우 BMC에 계속 액세스할 수 있습니다. 기본적으로 BMC는 DHCP를 사용하여 IP 주소를 얻습니다. BMC 네트워크에서 DHCP가 활성화된 경우 네트워크 관리자는 BMC MAC에 할당된 IP 주소를 제공할 수 있습니다. 이 주소는 SG6000-CN 컨트롤러 전면에 있는 레이블에 인쇄되어 있습니다. BMC 네트워크에서 DHCP가 활성화되어 있지 않으면 몇 분 후에 BMC가 응답하지 않고 기본 정적 IP인 192.168.0.120을 할당합니다. 랩톱을 BMC 포트에 직접 연결하고 네트워크 설정을 변경하여 랩톱에 192.168.0.200/24 등의 IP를 할당하여 192.168.0.120'으로 찾아야 할 수도 있습니다.

2. 사용자가 설정한 암호를 사용하여 루트 사용자 이름과 암호를 입력합니다 기본 루트 암호를 변경했습니다:



3. 로그인 * 을 선택합니다.



4. 선택적으로 * 설정 * > * 사용자 관리 * 를 선택하고 "사용 안 함" 사용자를 클릭하여 추가 사용자를 생성합니다.

> 사용자가 처음 로그인할 때 보안을 강화하기 위해 암호를 변경하라는 메시지가 표시될 수 있습니다.

SG6000-CN 컨트롤러에 대한 **SNMP** 설정을 구성합니다

하드웨어에 대한 SNMP 구성에 익숙한 경우 BMC 인터페이스를 사용하여 SG6000-CN 컨트롤러에 대한 SNMP 설정을 구성할 수 있습니다. 보안 커뮤니티 문자열을 제공하고, SNMP 트랩을 활성화하고, 최대 5개의 SNMP 대상을 지정할 수 있습니다.

필요한 것

- BMC 대시보드에 액세스하는 방법을 알고 있습니다.
- SNMPv1-v2c 장비에 대한 SNMP 설정을 구성한 경험이 있습니다.

> SG6000-CN이 실패하고 교체해야 하는 경우 이 절차에 의해 수행된 BMC 설정은 보존되지 않을 수 있습니다. 하드웨어 교체 후 필요한 경우 쉽게 다시 적용할 수 있도록 적용한 모든 설정에 대한 기록이 있어야 합니다.

단계

1. BMC 대시보드에서 * 설정 * > * SNMP 설정 * 을 선택합니다.
2. SNMP 설정 페이지에서 * SNMP V1/V2 * 활성화 를 선택한 다음 읽기 전용 커뮤니티 문자열과 읽기/쓰기 커뮤니티 문자열을 제공합니다.

   읽기 전용 커뮤니티 문자열은 사용자 ID 또는 암호와 같습니다. 침입자가 네트워크 설정에 대한 정보를 얻지 못하게 하려면 이 값을 변경해야 합니다. 읽기-쓰기 커뮤니티 문자열은 인증되지 않은 변경으로부터 장치를 보호합니다.

3. 필요에 따라 * 트랩 사용 * 을 선택하고 필요한 정보를 입력합니다.

> IP 주소를 사용하여 각 SNMP 트랩의 대상 IP를 입력합니다. 정규화된 도메인 이름은 지원되지 않습니다.

SG6000-CN 컨트롤러가 비정상적인 상태에 있을 때 SNMP 콘솔에 즉시 알림을 보내도록 하려면 TRAP를 활성화하십시오. 트랩은 다양한 구성 요소의 하드웨어 장애 또는 온도 임계값을 초과했음을 나타낼 수 있습니다.

4. 필요에 따라 * 테스트 트랩 전송 * 을 클릭하여 설정을 테스트합니다.
5. 설정이 올바르면 * 저장 * 을 클릭합니다.

알림에 대한 이메일 알림을 설정합니다

경고가 발생할 때 e-메일 알림을 보내려면 BMC 인터페이스를 사용하여 SMTP 설정, 사용자, LAN 대상, 경고 정책 및 이벤트 필터를 구성해야 합니다.

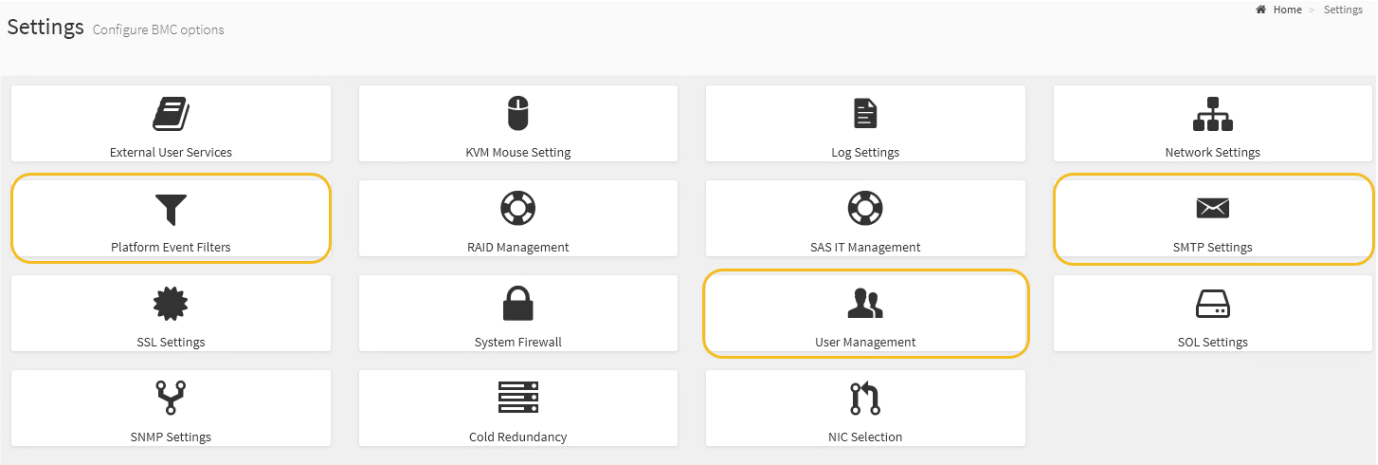
> SG6000-CN이 실패하고 교체해야 하는 경우 이 절차에 의해 수행된 BMC 설정은 보존되지 않을 수 있습니다. 하드웨어 교체 후 필요한 경우 쉽게 다시 적용할 수 있도록 적용한 모든 설정에 대한 기록이 있어야 합니다.

필요한 것

BMC 대시보드에 액세스하는 방법을 알고 있습니다.

이 작업에 대해

BMC 인터페이스에서 설정 페이지의 * SMTP 설정 *, * 사용자 관리 * 및 * 플랫폼 이벤트 필터 * 옵션을 사용하여 이메일 알림을 구성합니다.



단계

1. SMTP 설정을 구성합니다.
   a. 설정 * > * SMTP 설정 * 을 선택합니다.
   b. 보낸 사람 e-메일 ID의 경우 유효한 e-메일 주소를 입력합니다.

      이 전자 메일 주소는 BMC가 전자 메일을 보낼 때 보내는 사람 주소로 제공됩니다.
2. 알림을 받도록 사용자를 설정합니다.
   a. BMC 대시보드에서 * 설정 * > * 사용자 관리 * 를 선택합니다.

b. 알림 알림을 수신할 사용자를 한 명 이상 추가하십시오.

사용자에 대해 구성한 전자 메일 주소는 BMC가 경고 알림을 보내는 주소입니다. 예를 들어 ""notification-user""와 같은 일반 사용자를 추가하고 기술 지원 팀 이메일 배포 목록의 이메일 주소를 사용할 수 있습니다.

3. 경고를 위한 LAN 대상을 구성합니다.
   a. 설정 * > * 플랫폼 이벤트 필터 * > * LAN 대상 * 을 선택합니다.
   b. LAN 대상을 하나 이상 구성합니다.
      - 대상 유형으로 * 이메일 * 을 선택합니다.
      - BMC Username 에서 이전에 추가한 사용자 이름을 선택합니다.
      - 여러 사용자를 추가했으며 모든 사용자가 알림 이메일을 받도록 하려면 각 사용자에 대해 LAN 대상을 추가해야 합니다.
   c. 테스트 알림을 보냅니다.
4. BMC가 경고를 보내는 시기와 위치를 정의할 수 있도록 경고 정책을 구성합니다.
   a. 설정 * > * 플랫폼 이벤트 필터 * > * 경고 정책 * 을 선택합니다.
   b. 각 LAN 대상에 대해 하나 이상의 경고 정책을 구성합니다.
      - 정책 그룹 번호 로 * 1 * 을 선택합니다.
      - 정책 작업의 경우 * 항상 이 대상으로 알림 전송 * 을 선택합니다.
      - LAN 채널의 경우 * 1 * 을 선택합니다.
      - 대상 선택기에서 정책의 LAN 대상을 선택합니다.
5. 다양한 이벤트 유형에 대한 경고를 적절한 사용자에게 보내도록 이벤트 필터를 구성합니다.
   a. 설정 * > * 플랫폼 이벤트 필터 * > * 이벤트 필터 * 를 선택합니다.
   b. 경고 정책 그룹 번호 에 * 1 * 을 입력합니다.
   c. 경고 정책 그룹에 알림을 보낼 모든 이벤트에 대한 필터를 만듭니다.
      - 전원 동작, 특정 센서 이벤트 또는 모든 이벤트에 대한 이벤트 필터를 만들 수 있습니다.
      - 모니터링할 이벤트를 잘 모르는 경우 센서 유형에 대해 * All Sensors * 를 선택하고 이벤트 옵션에 대해 * All Events * 를 선택합니다. 원치 않는 알림을 받으면 나중에 선택 사항을 변경할 수 있습니다.

선택 사항**:** 노드 암호화를 활성화합니다

노드 암호화를 사용하는 경우 어플라이언스의 디스크는 물리적 손실 또는 사이트 제거로부터 보안 키 관리 서버(KMS) 암호화로 보호할 수 있습니다. 어플라이언스 설치 중에 노드 암호화를 선택하고 활성화해야 하며 KMS 암호화 프로세스가 시작되면 노드 암호화를 선택 취소할 수 없습니다.

필요한 것

StorageGRID 관리 지침에 따라 KMS에 대한 정보를 검토합니다.

이 작업에 대해

노드 암호화가 활성화된 어플라이언스는 StorageGRID 사이트에 대해 구성된 외부 키 관리 서버(KMS)에 연결됩니다. 각 KMS(또는 KMS 클러스터)는 사이트의 모든 어플라이언스 노드에 대한 암호화 키를 관리합니다. 이러한 키는 노드

암호화가 활성화된 어플라이언스에서 각 디스크의 데이터를 암호화하고 해독합니다.

KMS는 제품을 StorageGRID에 설치하기 전이나 설치한 후에 그리드 관리자에서 설정할 수 있습니다. 자세한 내용은 StorageGRID 관리 지침의 KMS 및 어플라이언스 구성에 대한 정보를 참조하십시오.

- KMS가 어플라이언스를 설치하기 전에 설정된 경우 어플라이언스에서 노드 암호화를 사용하도록 설정하고 KMS가 구성된 StorageGRID 사이트에 추가하면 KMS 제어 암호화가 시작됩니다.
- KMS가 어플라이언스를 설치하기 전에 설정되지 않은 경우 KMS가 구성되고 어플라이언스 노드가 포함된 사이트에 대해 사용 가능한 즉시 노드 암호화가 활성화된 각 어플라이언스에 대해 KMS 제어 암호화가 수행됩니다.

> 노드 암호화가 활성화된 어플라이언스에서 KMS에 연결하기 전에 존재하는 데이터는 안전하지 않은 임시 키로 암호화됩니다. KMS에서 제공하는 값으로 키를 설정할 때까지 제품은 제거 또는 도난으로부터 보호되지 않습니다.

디스크 암호를 해독하는 데 필요한 KMS 키가 없으면 어플라이언스의 데이터를 검색할 수 없으며 효과적으로 손실됩니다. 이 경우 암호 해독 키를 KMS에서 검색할 수 없습니다. KMS 구성을 지우거나, KMS 키가 만료되거나, KMS에 대한 연결이 끊어지거나, KMS 키가 설치된 StorageGRID 시스템에서 어플라이언스를 제거하면 이 키에 액세스할 수 없습니다.

단계

1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다.

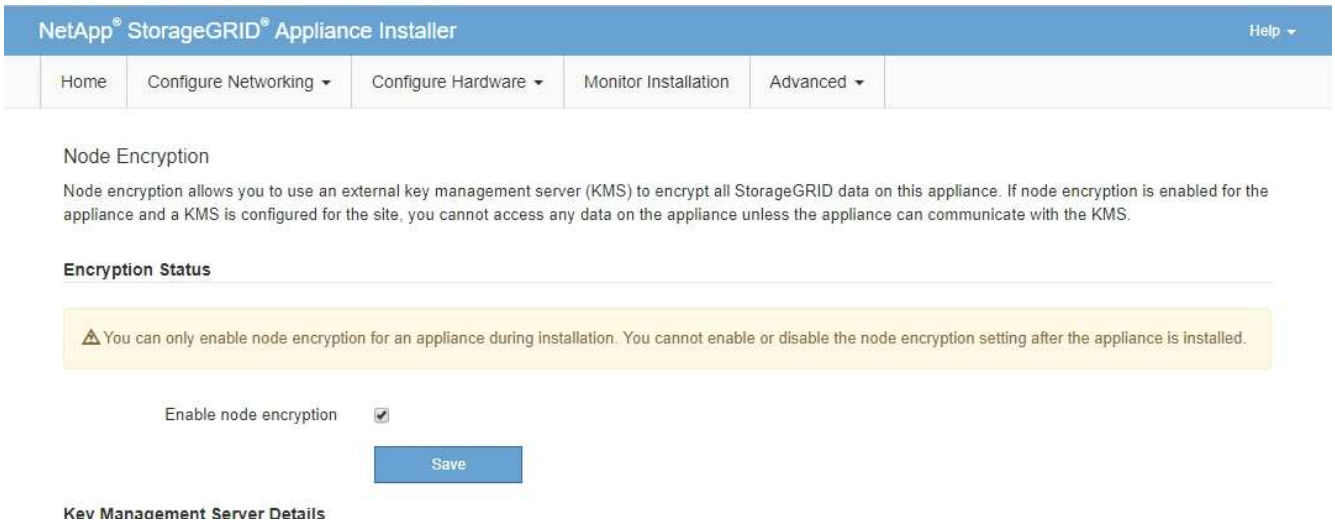
   (* https://*Controller_IP*:8443*`)

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

   > KMS 키로 어플라이언스를 암호화한 후에는 동일한 KMS 키를 사용하지 않으면 어플라이언스 디스크를 해독할 수 없습니다.

2. 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.



3. 노드 암호화 사용 * 을 선택합니다.

어플라이언스를 설치하기 전에 데이터 손실 위험 없이 * 노드 암호화 활성화 * 를 선택 취소할 수 있습니다. 설치가 시작되면 어플라이언스 노드가 StorageGRID 시스템의 KMS 암호화 키에 액세스하여 디스크 암호화를 시작합니다. 어플라이언스를 설치한 후에는 노드 암호화를 비활성화할 수 없습니다.

> KMS가 있는 StorageGRID 사이트에 노드 암호화가 활성화된 어플라이언스를 추가한 후에는 해당 노드에 대해 KMS 암호화 사용을 중지할 수 없습니다.

4. 저장 * 을 선택합니다.
5. 어플라이언스를 StorageGRID 시스템에 노드로 구축하십시오.

   킬로미터 제어 암호화는 어플라이언스가 StorageGRID 사이트에 구성된 KMS 키에 액세스할 때 시작됩니다. KMS 암호화 프로세스 중에 설치 프로그램이 진행률 메시지를 표시합니다. 이 과정은 어플라이언스에 있는 디스크 볼륨 수에 따라 몇 분 정도 걸릴 수 있습니다.

   > 어플라이언스는 처음에 각 디스크 볼륨에 할당된 임의의 비 KMS 암호화 키로 구성됩니다. 이 디스크는 노드 암호화가 활성화된 어플라이언스가 StorageGRID 사이트에 구성된 KMS 키에 액세스할 때까지 안전하지 않은 임시 암호화 키를 사용하여 암호화됩니다.

작업을 마친 후

어플라이언스 노드가 유지보수 모드일 때 노드 암호화 상태, KMS 세부 정보 및 사용 중인 인증서를 볼 수 있습니다.

관련 정보

StorageGRID 관리

유지보수 모드(SG6000)에서 노드 암호화 모니터링

선택 사항**: RAID** 모드 변경**(SG6000**만 해당**)**

스토리지 및 복구 요구 사항을 수용하기 위해 어플라이언스에서 다른 RAID 모드로 변경할 수 있습니다. 어플라이언스 스토리지 노드를 구축하기 전에만 모드를 변경할 수 있습니다.

필요한 것

- StorageGRID에 연결할 수 있는 모든 클라이언트를 사용 중입니다.
- 클라이언트에 가 있습니다 지원되는 웹 브라우저.

이 작업에 대해

어플라이언스를 스토리지 노드로 구축하기 전에 다음 볼륨 구성 옵션 중 하나를 선택할 수 있습니다.

- * DDP *: 이 모드는 데이터 드라이브 8개마다 2개의 패리티 드라이브를 사용합니다. 모든 어플라이언스에 대한 기본 권장 모드입니다. RAID6와 비교하여 DDP는 시스템 성능을 향상하고, 드라이브 장애 후 리빌드 시간을 줄이고, 관리를 간소화합니다.

  > DDP는 2개의 SSD로 인해 SG6060 어플라이언스에서 드로어 손실 보호를 제공하지 않습니다. SG6060에 추가된 확장 쉘프에서는 서랍 손실 보호를 효과적으로 수행합니다.

- * DDP16 *: 이 모드는 데이터 드라이브 16개마다 2개의 패리티 드라이브를 사용하므로 DDP에 비해 스토리지 효율성이 높습니다. RAID6와 비교했을 때 DDP16은 시스템 성능이 향상되고 드라이브 장애 후 리빌드 시간이 줄어들며 관리가 용이하며 스토리지 효율성이 비슷합니다. DDP16 모드를 사용하려면 구성에 최소 20개의

드라이브가 있어야 합니다. DDP16은 드로어 손실 방지 기능을 제공하지 않습니다.

- * RAID6 *: 이 모드는 16개 이상의 데이터 드라이브마다 2개의 패리티 드라이브를 사용합니다. RAID 6 모드를 사용하려면 구성에 최소 20개의 드라이브가 포함되어 있어야 합니다. RAID6는 DDP와 비교할 때 어플라이언스의 스토리지 효율성을 높일 수 있지만 대부분의 StorageGRID 환경에서는 권장되지 않습니다.

> 볼륨이 이미 구성되었거나 StorageGRID가 이전에 설치된 경우 RAID 모드를 변경하면 볼륨이 제거되고 교체됩니다. 해당 볼륨의 모든 데이터가 손실됩니다.

단계

1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다.

   (* https://*Controller_IP*:8443*`)

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 고급 * > * RAID 모드 * 를 선택합니다.
3. RAID 모드 구성 * 페이지의 모드 드롭다운 목록에서 원하는 RAID 모드를 선택합니다.
4. 저장 * 을 클릭합니다.

관련 정보

"NetApp E-Series 시스템 문서 사이트"

옵션: 어플라이언스인 네트워크 포트를 재활용합니다

어플라이언스 스토리지 노드의 내부 포트를 다른 외부 포트에 다시 매핑해야 할 수 있습니다. 예를 들어, 방화벽 문제로 인해 포트를 다시 매핑해야 할 수 있습니다.

필요한 것

- 이전에 StorageGRID 어플라이언스 설치 프로그램에 액세스했습니다.
- 로드 밸런서 엔드포인트를 구성하지 않았거나 구성하지 않을 계획입니다.

> 포트를 재매핑하는 경우 동일한 포트를 사용하여 로드 밸런서 끝점을 구성할 수 없습니다. 로드 밸런서 끝점을 구성하고 이미 포트를 다시 매핑하려면 의 단계를 따릅니다 포트 재맵을 제거합니다.

단계

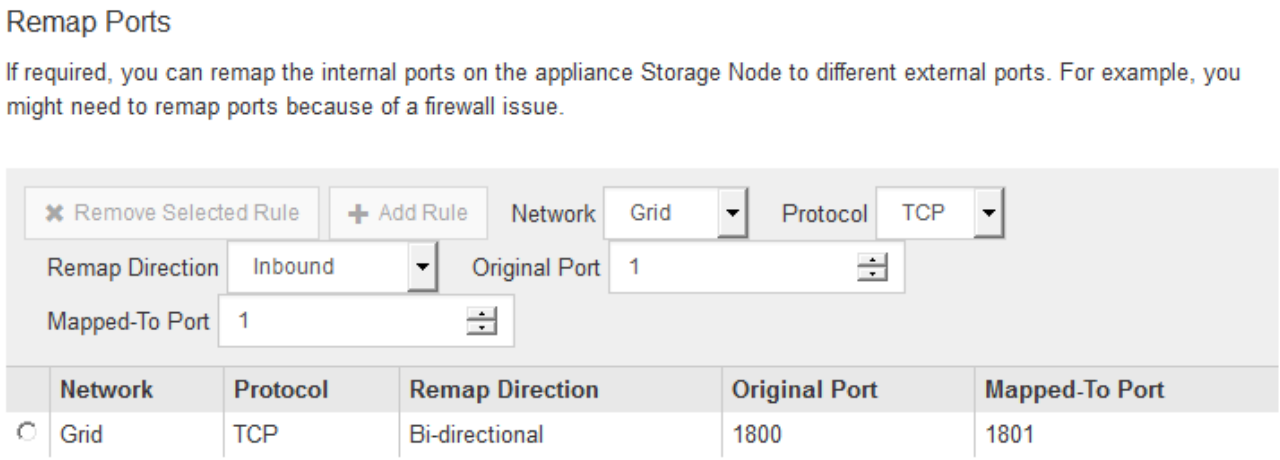
1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * 재매핑 포트 * 를 클릭합니다.

   Remap Port(재매핑 포트) 페이지가 나타납니다.

2. 네트워크 * 드롭다운 상자에서 그리드, 관리자 또는 클라이언트 중 다시 매핑할 포트의 네트워크를 선택합니다.
3. 프로토콜 * 드롭다운 상자에서 IP 프로토콜(TCP 또는 UDP)을 선택합니다.
4. Remap Direction * (재매핑 방향 *) 드롭다운 상자에서 이 포트에 대해 재매핑할 트래픽 방향(Inbound, Outbound 또는 Bi-directional)을 선택합니다.

5. 원래 포트 * 의 경우 재매핑할 포트 번호를 입력합니다.
6. Mapped-to Port*의 경우 대신 사용할 포트 번호를 입력합니다.
7. 규칙 추가 * 를 클릭합니다.

   새 포트 매핑이 테이블에 추가되고 다시 매핑이 즉시 적용됩니다.



8. 포트 매핑을 제거하려면 제거할 규칙의 라디오 버튼을 선택하고 * 선택한 규칙 제거 * 를 클릭합니다.

어플라이언스 스토리지 노드 구축

스토리지 어플라이언스를 설치 및 구성한 후 StorageGRID 시스템에서 스토리지 노드로 구축할 수 있습니다. 어플라이언스를 스토리지 노드로 배포할 때는 어플라이언스에 포함된 StorageGRID 어플라이언스 설치 프로그램을 사용합니다.

필요한 것

- 어플라이언스 노드를 클론 생성하는 경우 복구 및 유지 보수 프로세스를 계속 수행합니다.

  복구 및 유지 관리

- 이 제품은 랙 또는 캐비닛에 설치되었고 네트워크에 연결되어 있으며 전원이 켜져 있습니다.
- StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스에 대해 네트워크 링크, IP 주소 및 포트 재매핑(필요한 경우)이 구성되었습니다.
- 어플라이언스의 컴퓨팅 컨트롤러에 할당된 IP 주소 중 하나를 알고 있습니다. 연결된 모든 StorageGRID 네트워크에 대해 IP 주소를 사용할 수 있습니다.
- StorageGRID 시스템의 기본 관리 노드가 배포되었습니다.
- StorageGRID 어플라이언스 설치 프로그램의 IP 구성 페이지에 나열된 모든 그리드 네트워크 서브넷은 기본 관리 노드의 그리드 네트워크 서브넷 목록에 정의되어 있습니다.
- 지원되는 웹 브라우저가 있는 서비스 랩톱이 있습니다.

이 작업에 대해

각 스토리지 어플라이언스는 단일 스토리지 노드로 작동합니다. 모든 어플라이언스는 그리드 네트워크, 관리 네트워크 및 클라이언트 네트워크에 연결할 수 있습니다

어플라이언스 스토리지 노드를 StorageGRID 시스템에 배포하려면 StorageGRID 어플라이언스 설치 프로그램에 액세스하여 다음 단계를 수행합니다.

- 운영 관리 노드의 IP 주소와 스토리지 노드의 이름을 지정하거나 확인합니다.
- 구축을 시작하고 볼륨이 구성되고 소프트웨어가 설치될 때까지 기다립니다.
- 어플라이언스 설치 작업이 중간에 일시 중지되면 그리드 관리자에 로그인하고 모든 그리드 노드를 승인하고 StorageGRID 설치 및 배포 프로세스를 완료하여 설치를 다시 시작합니다.

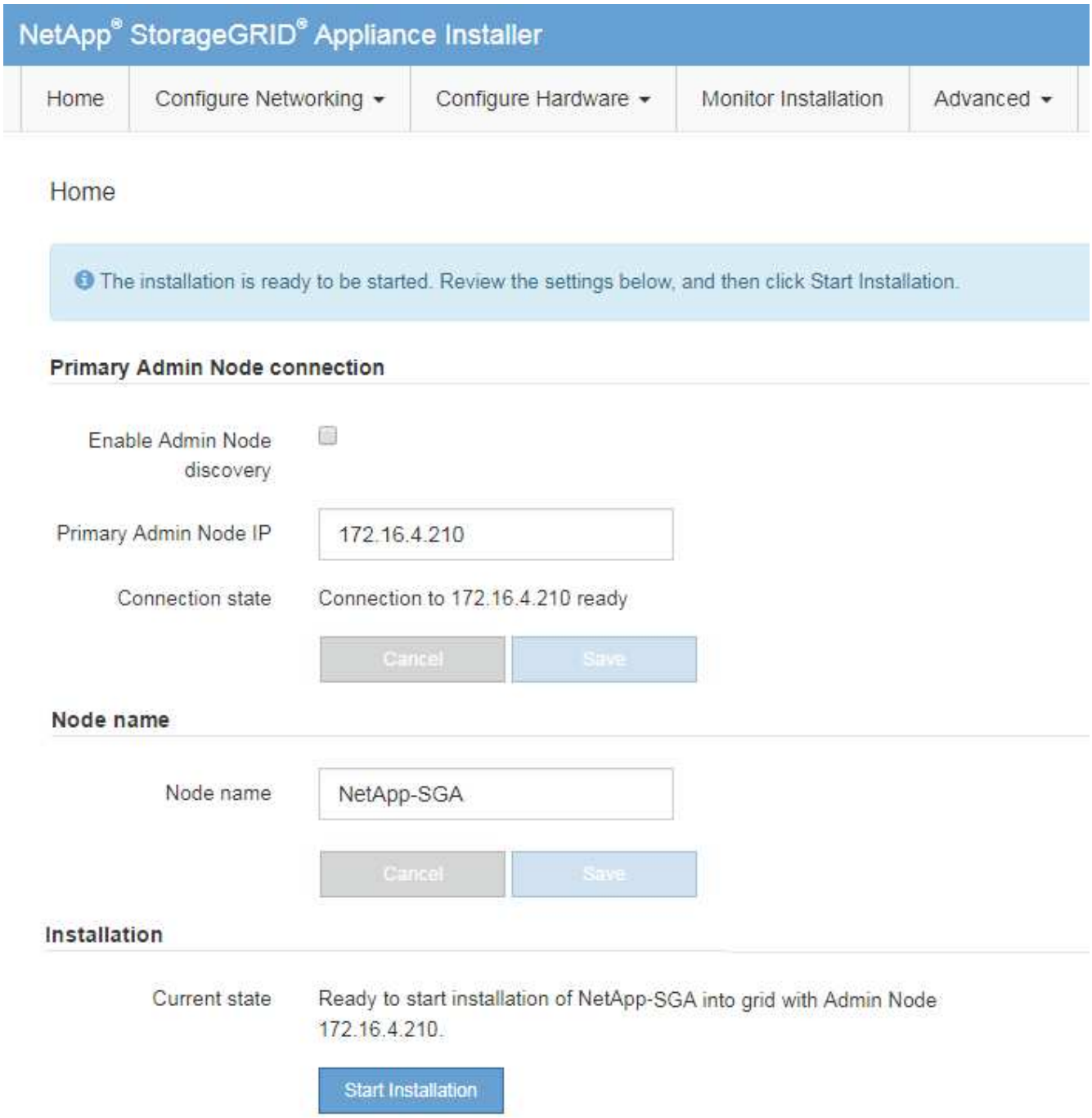
> 한 번에 여러 어플라이언스 노드를 구축해야 하는 경우 'configure-sGA.py' 어플라이언스 설치 스크립트를 사용하여 설치 프로세스를 자동화할 수 있습니다.

- 확장 또는 복구 작업을 수행하는 경우 해당 지침을 따르십시오.
  - 기존 StorageGRID 시스템에 어플라이언스 스토리지 노드를 추가하려면 StorageGRID 시스템 확장 지침을 참조하십시오.
  - 복구 작업의 일부로 어플라이언스 스토리지 노드를 배포하려면 복구 및 유지 관리 지침을 참조하십시오.

단계

1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.



2. Primary Admin Node connection * 섹션에서 Primary Admin Node의 IP 주소를 지정해야 하는지 여부를 확인합니다.

   이전에 이 데이터 센터에 다른 노드를 설치한 경우 StorageGRID 어플라이언스 설치 관리자는 기본 관리 노드 또는 admin_IP가 구성된 다른 그리드 노드가 동일한 서브넷에 있다고 가정하여 이 IP 주소를 자동으로 검색할 수 있습니다.

3. 이 IP 주소가 표시되지 않거나 변경해야 하는 경우 주소를 지정합니다.

옵션을 선택합니다	설명
수동 IP 입력	a. 관리자 노드 검색 사용 * 확인란의 선택을 취소합니다. b. IP 주소를 수동으로 입력합니다. c. 저장 * 을 클릭합니다. d. 새 IP 주소가 준비될 때까지 연결 상태를 기다립니다.
연결된 모든 운영 관리 노드의 자동 검색	a. 관리자 노드 검색 사용 * 확인란을 선택합니다. b. 검색된 IP 주소 목록이 표시될 때까지 기다립니다. c. 이 어플라이언스 스토리지 노드를 구축할 그리드의 기본 관리 노드를 선택합니다. d. 저장 * 을 클릭합니다. e. 새 IP 주소가 준비될 때까지 연결 상태를 기다립니다.

4. 노드 이름 * 필드에 이 어플라이언스 노드에 사용할 이름을 입력하고 * 저장 * 을 클릭합니다.

   노드 이름은 StorageGRID 시스템의 이 어플라이언스 노드에 할당됩니다. 그리드 관리자의 노드 페이지(개요 탭)에 표시됩니다. 필요한 경우 노드를 승인할 때 이름을 변경할 수 있습니다.

5. 설치 * 섹션에서 현재 상태가 "기본 관리 노드 "*admin_ip*"이(가) 있는 그리드에 "*node name*"의 설치를 시작할 준비가 되었으며 * 설치 시작 * 버튼이 활성화되어 있는지 확인합니다.

   설치 시작 * 버튼이 활성화되지 않은 경우 네트워크 구성 또는 포트 설정을 변경해야 할 수 있습니다. 자세한 내용은 제품의 설치 및 유지보수 지침을 참조하십시오.

   > 스토리지 노드 어플라이언스를 노드 클론 생성 타겟으로 구축하는 경우 여기서 구축 프로세스를 중지하고 복구 및 유지 관리에서 노드 클론 생성 절차를 계속 진행하십시오. 를 누릅니다복구 및 유지 관리

6. StorageGRID 어플라이언스 설치 관리자 홈 페이지에서 * 설치 시작 * 을 클릭합니다.

   현재 상태가 ""설치 진행 중""으로 변경되고 모니터 설치 페이지가 표시됩니다.

   > 모니터 설치 페이지에 수동으로 액세스해야 하는 경우 * 모니터 설치 * 를 클릭합니다.

7. 그리드에 여러 어플라이언스 스토리지 노드가 포함된 경우 각 어플라이언스에 대해 이 단계를 반복합니다.

   > 한 번에 여러 어플라이언스 스토리지 노드를 구축해야 하는 경우 "configure-sGA.py" 어플라이언스 설치 스크립트를 사용하여 설치 프로세스를 자동화할 수 있습니다.

관련 정보

그리드를 확장합니다

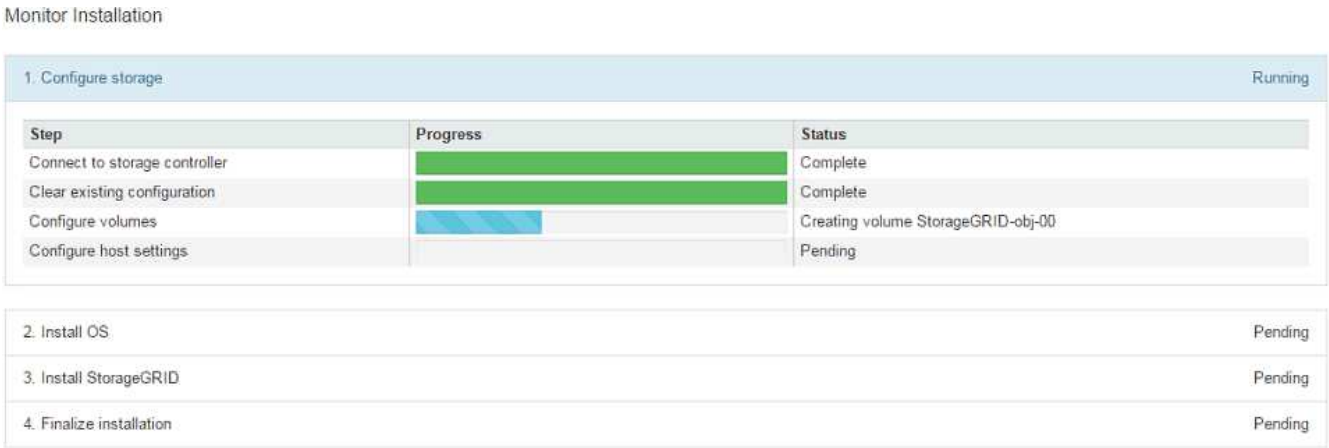
스토리지 어플라이언스 설치를 모니터링합니다

StorageGRID 어플라이언스 설치 프로그램은 설치가 완료될 때까지 상태를 제공합니다. 소프트웨어 설치가 완료되면 어플라이언스가 재부팅됩니다.

단계

1. 설치 진행률을 모니터링하려면 * 모니터 설치 * 를 클릭합니다.

   Monitor Installation(모니터 설치) 페이지에 설치 진행률이 표시됩니다.

   파란색 상태 표시줄은 현재 진행 중인 작업을 나타냅니다. 녹색 상태 표시줄은 성공적으로 완료된 작업을 나타냅니다.

   > 설치 프로그램은 이전 설치에서 완료된 작업이 다시 실행되지 않도록 합니다. 설치를 다시 실행할 경우 다시 실행할 필요가 없는 작업은 녹색 상태 표시줄과 "중단" 상태로 표시됩니다.

2. 처음 두 설치 단계의 진행 상황을 검토합니다.

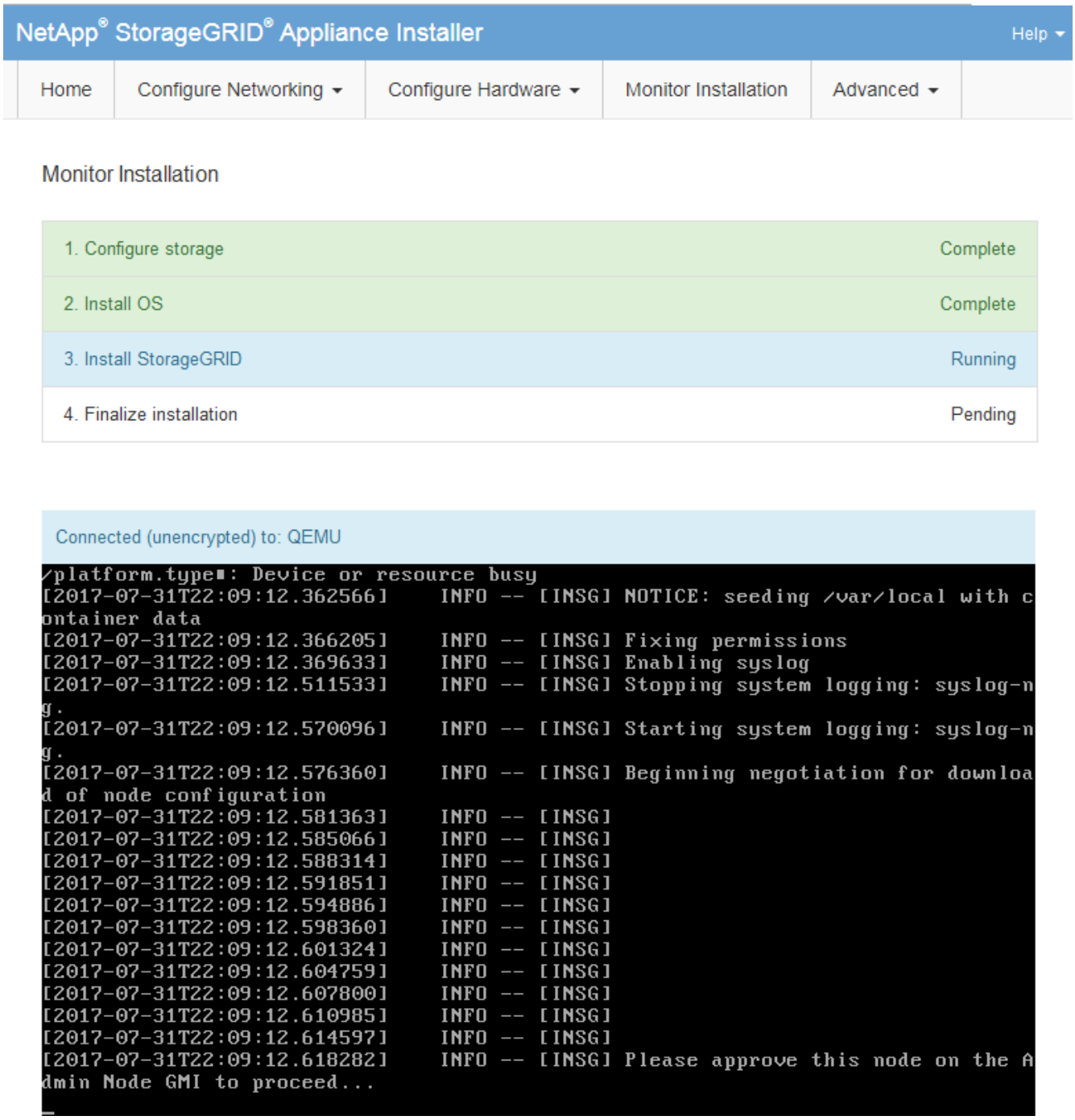
   - 1. 스토리지 구성 *

     이 단계에서 설치 관리자는 스토리지 컨트롤러에 연결하고, 기존 구성을 지우고, SANtricity 소프트웨어와 통신하여 볼륨을 구성하고, 호스트 설정을 구성합니다.

   - 2. OS * 를 설치합니다

   이 단계에서 설치 프로그램은 StorageGRID의 기본 운영 체제 이미지를 어플라이언스에 복사합니다.

3. StorageGRID* 설치 단계가 일시 중지되고 그리드 관리자를 사용하여 관리 노드에서 이 노드를 승인하라는 메시지가 포함된 콘솔에 표시될 때까지 설치 진행 상태를 계속 모니터링합니다. 다음 단계로 이동합니다.



4. 운영 관리 노드의 그리드 관리자로 이동하여 보류 중인 스토리지 노드를 승인하고 StorageGRID 설치 프로세스를 완료합니다.

   Grid Manager에서 * Install * 을 클릭하면 단계 3이 완료되고 단계 4, * 설치 완료 * 가 시작됩니다. 4단계가 완료되면 컨트롤러가 재부팅됩니다.

어플라이언스 설치 및 구성 자동화(SG6000)

어플라이언스의 설치 및 구성과 전체 StorageGRID 시스템의 구성을 자동화할 수 있습니다.

이 작업에 대해

설치 및 구성 자동화는 여러 StorageGRID 인스턴스 또는 하나의 크고 복잡한 StorageGRID 인스턴스를 구축하는 데 유용할 수 있습니다.

설치 및 구성을 자동화하려면 다음 옵션 중 하나 이상을 사용하십시오.

- 어플라이언스의 구성 설정을 지정하는 JSON 파일을 생성합니다. StorageGRID 어플라이언스 설치 프로그램을 사용하여 JSON 파일을 업로드합니다.

  동일한 파일을 사용하여 여러 어플라이언스를 구성할 수 있습니다.

- StorageGRID ``configure-sGA.py'' Python 스크립트를 사용하여 어플라이언스 구성을 자동화합니다.
- 추가 Python 스크립트를 사용하여 전체 StorageGRID 시스템의 다른 구성 요소("그리드")를 구성합니다.

  StorageGRID 자동화 Python 스크립트를 직접 사용하거나 직접 개발한 그리드 구축 및 구성 도구에서 StorageGRID 설치 REST API를 사용하는 방법의 예로 사용할 수 있습니다. 에 대한 정보를 참조하십시오 StorageGRID 설치 파일 다운로드 및 추출.

StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스 구성을 자동화합니다

구성 정보가 포함된 JSON 파일을 사용하여 어플라이언스 구성을 자동화할 수 있습니다. StorageGRID 어플라이언스 설치 프로그램을 사용하여 파일을 업로드합니다.

필요한 것

- 어플라이언스는 StorageGRID 11.5 이상과 호환되는 최신 펌웨어에 있어야 합니다.
- 를 사용하여 구성하는 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램에 연결되어 있어야 합니다 지원되는 웹 브라우저.

이 작업에 대해

다음과 같은 어플라이언스 구성 작업을 자동화할 수 있습니다.

- Grid Network, Admin Network 및 Client Network IP 주소입니다
- BMC 인터페이스
- 네트워크 링크
  - 포트 결합 모드
  - 네트워크 연결 모드
  - 링크 속도

업로드된 JSON 파일을 사용하여 어플라이언스를 구성하는 것이 StorageGRID 어플라이언스 설치 프로그램에서 여러 페이지를 사용하여 수동으로 구성하는 것보다 더 효율적인 경우가 많습니다. 특히 여러 노드를 구성해야 하는 경우 더욱 그렇습니다. 각 노드에 대해 한 번에 하나씩 구성 파일을 적용해야 합니다.

어플라이언스의 설치와 구성을 모두 자동화하려는 숙련된 사용자는 'configure-sGA.py' 스크립트를 사용할 수 있습니다. 를 누릅니다configure-sga.py 스크립트를 사용하여 어플라이언스 노드의 설치 및 구성을 자동화합니다

단계

1. 다음 방법 중 하나를 사용하여 JSON 파일을 생성합니다.
   - ConfigBuilder 응용 프로그램

     "ConfigBuilder.netapp.com"

   - 'configure-sGA.py' 어플라이언스 구성 스크립트 StorageGRID 어플라이언스 설치 프로그램(* 도움말*>* 어플라이언스 구성 스크립트*)에서 스크립트를 다운로드할 수 있습니다. configure-sga.py 스크립트를 사용하여 구성 자동화에 대한 지침을 참조하십시오.

     configure-sga.py 스크립트를 사용하여 어플라이언스 노드의 설치 및 구성을 자동화합니다

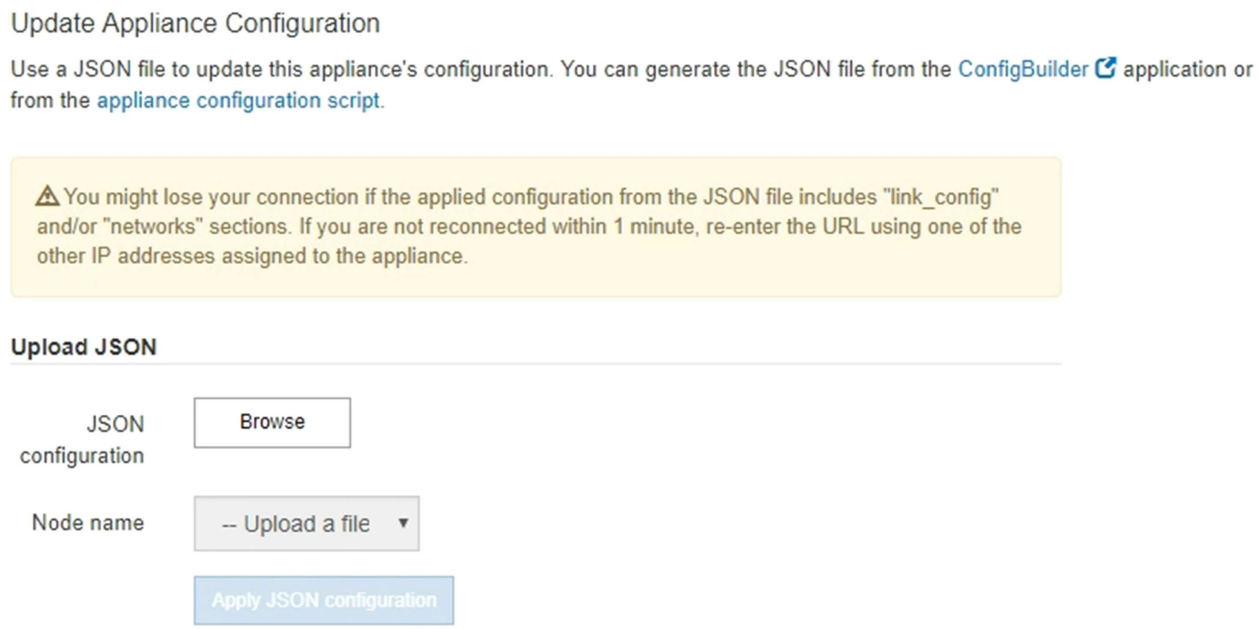
     JSON 파일의 노드 이름은 다음 요구사항을 충족해야 합니다.

   - 1자 이상 32자 이하의 유효한 호스트 이름이어야 합니다
   - 문자, 숫자 및 하이픈을 사용할 수 있습니다
   - 하이픈으로 시작하거나 끝날 수 없습니다
   - 숫자만 포함할 수 없습니다

     JSON 파일의 노드 이름(최상위 이름)이 고유한지 확인하십시오. 그렇지 않으면 JSON 파일을 사용하여 둘 이상의 노드를 구성할 수 없습니다.

2. Advanced * > * Update Appliance Configuration * 을 선택합니다.

   어플라이언스 구성 업데이트 페이지가 나타납니다.

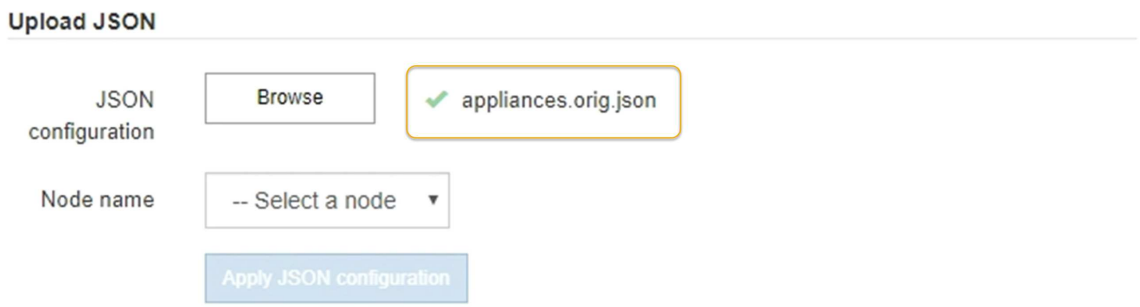


3. 업로드할 구성이 있는 JSON 파일을 선택합니다.
   a. 찾아보기 * 를 선택합니다.
   b. 파일을 찾아 선택합니다.

c. 열기 * 를 선택합니다.

파일이 업로드되고 검증됩니다. 유효성 검사 프로세스가 완료되면 녹색 확인 표시 옆에 파일 이름이 표시됩니다.

> JSON 파일의 구성에 "link_config", "networks" 또는 둘 다에 대한 섹션이 포함된 경우 어플라이언스에 대한 연결이 끊어질 수 있습니다. 1분 이내에 다시 연결되지 않으면 어플라이언스에 할당된 다른 IP 주소 중 하나를 사용하여 어플라이언스 URL을 다시 입력하십시오.

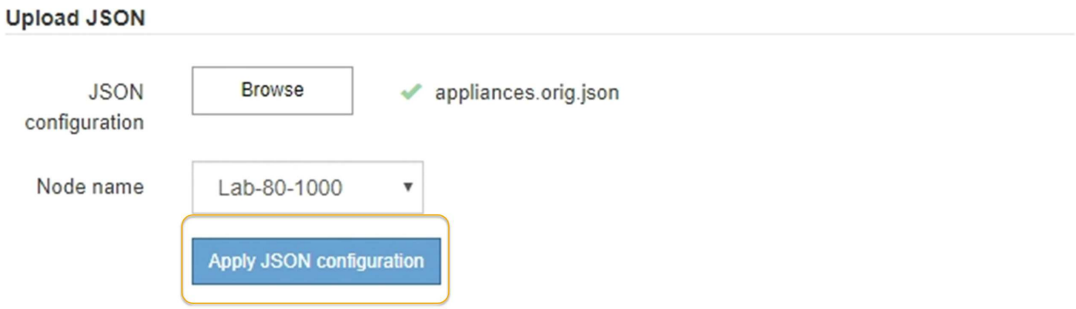


노드 이름 * 드롭다운은 JSON 파일에 정의된 최상위 노드 이름으로 채워집니다.

> 파일이 유효하지 않으면 파일 이름이 빨간색으로 표시되고 오류 메시지가 노란색 배너에 표시됩니다. 잘못된 파일이 어플라이언스에 적용되지 않습니다. ConfigBuilder를 사용하여 올바른 JSON 파일이 있는지 확인할 수 있습니다.

4. 노드 이름 * 드롭다운 목록에서 노드를 선택합니다.

   JSON 설정 적용 * 버튼이 활성화됩니다.



5. JSON 구성 적용 * 을 선택합니다.

   선택한 노드에 구성이 적용됩니다.

configure-sga.py 스크립트를 사용하여 어플라이언스 노드의 설치 및 구성을 자동화합니다

'configure-sGA.py' 스크립트를 사용하면 기본 관리 노드의 설치 및 구성을 포함하여 StorageGRID 어플라이언스 노드에 대한 많은 설치 및 구성 작업을 자동화할 수 있습니다. 이

스크립트는 구성할 어플라이언스가 많은 경우 유용할 수 있습니다. 또한 스크립트를 사용하여 어플라이언스 구성 정보가 포함된 JSON 파일을 생성할 수도 있습니다.

필요한 것

- 이 어플라이언스는 랙에 설치되어 있고 네트워크에 연결되어 있으며 전원이 켜져 있습니다.
- 네트워크 링크 및 IP 주소는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 기본 관리 노드에 대해 구성되었습니다.
- 기본 관리 노드를 설치하는 경우 해당 IP 주소를 알 수 있습니다.
- 다른 노드를 설치 및 구성하는 경우 기본 관리 노드가 배포되었으며 해당 IP 주소를 알고 있는 것입니다.
- 기본 관리 노드 이외의 모든 노드의 경우 StorageGRID 어플라이언스 설치 프로그램의 IP 구성 페이지에 나열된 모든 그리드 네트워크 서브넷이 기본 관리 노드의 그리드 네트워크 서브넷 목록에 정의되어 있습니다.
- 'configure-sGA.py' 파일을 다운로드했습니다. 이 파일은 설치 아카이브에 포함되어 있거나 StorageGRID 어플라이언스 설치 프로그램에서 * 도움말 * > * 어플라이언스 설치 스크립트 * 를 클릭하여 액세스할 수 있습니다.

> 이 절차는 명령줄 인터페이스를 사용하는 일부 경험이 있는 고급 사용자를 위한 것입니다. 또는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 구성을 자동화할 수도 있습니다. 를 누릅니다StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스 구성을 자동화합니다

단계

1. Python 스크립트를 실행하기 위해 사용 중인 Linux 시스템에 로그인합니다.
2. 스크립트 구문에 대한 일반적인 도움말과 사용 가능한 매개 변수 목록을 보려면 다음을 입력합니다.

   ```
   configure-sga.py --help
   ```

   'configure-sGA.py' 스크립트는 5개의 하위 명령을 사용합니다.

   - BMC 구성 및 어플라이언스의 현재 구성이 포함된 JSON 파일을 생성하는 등 고급 StorageGRID 어플라이언스 상호 작용을 위한 '고급' 기능입니다
   - RAID 모드, 노드 이름 및 네트워킹 매개 변수를 구성하기 위한 'configure'
   - StorageGRID 설치 시작을 위한 '설치'입니다
   - StorageGRID 설치 모니터링을 위한 모니터
   - 어플라이언스를 재부팅하기 위한 재부팅

   하위 명령(advanced, configure, install, monitor, reboot) 인수 뒤에 '--help' 옵션을 입력하면 해당 하위 명령 내에서 사용할 수 있는 옵션에 대한 자세한 내용을 제공하는 다른 도움말 텍스트가 표시됩니다. + "configure-sga.py_subcommand_—help

3. 어플라이언스 노드의 현재 구성을 확인하려면 다음과 같이 입력합니다. 여기서 "*SGA-INSTALL-IP*"는 어플라이언스 노드의 IP 주소 중 하나입니다. + "configure-sga.py configure_sGA-install-ip_

   이 결과는 기본 관리 노드의 IP 주소와 관리, 그리드 및 클라이언트 네트워크에 대한 정보를 포함하여 어플라이언스에 대한 현재 IP 정보를 표시합니다.

   ```
   ```

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200

  StorageGRID Appliance
    Name:        LAB-SGA-2-30
    Node type:   storage

  StorageGRID primary Admin Node
    IP:        172.16.1.170
    State:     unknown
    Message:   Initializing...
    Version:   Unknown

  Network Link Configuration
    Link Status
          Link      State      Speed (Gbps)
          ----      -----      -----
          1         Up         10
          2         Up         10
          3         Up         10
          4         Up         10
          5         Up         1
          6         Down       N/A

    Link Settings
        Port bond mode:      FIXED
        Link speed:          10GBE

        Grid Network:        ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

        Admin Network:       ENABLED
            Bonding mode:    no-bond
            MAC Addresses:   00:80:e5:29:70:f4
```

```
        Client Network:      ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

  Grid Network
    CIDR:      172.16.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:8A
    Gateway:   172.16.0.1
    Subnets:   172.17.0.0/21
               172.18.0.0/21
               192.168.0.0/21
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

#################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#################################################################
```

4. 현재 설정의 값을 변경해야 하는 경우 '설정' 하위 명령을 사용하여 값을 업데이트합니다. 예를 들어, 어플라이언스가 기본 관리 노드에 연결하기 위해 사용하는 IP 주소를 ' 172.16.2.99 '로 변경하려면 + ' configure-sga.py configure - -admin -ip 172.16.2.99_sga -install -ip_'를 입력합니다
5. 어플라이언스 구성을 JSON 파일로 백업하려면 고급 및 백업 파일 하위 명령을 사용하십시오. 예를 들어, IP 주소 '*SGA-INSTALL-IP*'를 사용하는 어플라이언스 구성을 어플라이언스-SG1000.json'이라는 파일에 백업하려면 + "configure-sga.py advanced—backup-file appliance-SG1000.json_sga-install-ip_"를 입력합니다

   구성 정보가 포함된 JSON 파일은 에서 스크립트를 실행한 디렉토리에 작성됩니다.

   > 생성된 JSON 파일의 최상위 노드 이름이 어플라이언스 이름과 일치하는지 확인하십시오. 숙련된 사용자이고 StorageGRID API에 대한 철저한 이해가 없는 경우 이 파일을 변경하지 마십시오.

6. 어플라이언스 구성이 만족스러우면 "install" 및 "monitor" 하위 명령을 사용하여 어플라이언스를 설치합니다. + "configure-sga.py install—monitor_sga-install-ip_"
7. 어플라이언스를 재부팅하려면 + "configure-sga.py reboot_sga-install-ip_"를 입력합니다

StorageGRID 구성 자동화

그리드 노드를 구축한 후 StorageGRID 시스템 구성을 자동화할 수 있습니다.

필요한 것

- 설치 아카이브에서 다음 파일의 위치를 알고 있습니다.

파일 이름	설명
configure-StorageGrid.py의 약어입니다	구성을 자동화하는 데 사용되는 Python 스크립트입니다
configure-StorageGrid.sample.json	스크립트와 함께 사용할 샘플 구성 파일
configure-StorageGrid.blank.json	스크립트에 사용할 빈 구성 파일입니다

- "configure-StorageGrid.json" 구성 파일을 만들었습니다. 이 파일을 만들려면 샘플 구성 파일('configure-StorageGrid.sample.json') 또는 빈 구성 파일('configure-StorageGrid.blank.json')을 수정할 수 있습니다.

이 작업에 대해

configure-StorageGrid.py Python 스크립트와 configure-StorageGrid.json 구성 파일을 사용하여 StorageGRID 시스템 구성을 자동화할 수 있습니다.

> 그리드 관리자 또는 설치 API를 사용하여 시스템을 구성할 수도 있습니다.

단계

1. Python 스크립트를 실행하기 위해 사용 중인 Linux 시스템에 로그인합니다.
2. 설치 아카이브를 추출한 디렉토리로 변경합니다.

   예: + 'cd StorageGRID-Webscale -*version/platform*

   여기서, 'platform'은 'dEBS', 'rpms', 'vSphere'입니다.

3. Python 스크립트를 실행하고 생성한 구성 파일을 사용합니다.

   예를 들면 다음과 같습니다.

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

작업을 마친 후

복구 패키지 '.zip' 파일은 구성 프로세스 중에 생성되며 설치 및 구성 프로세스를 실행 중인 디렉토리에 다운로드됩니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 백업해야 합니다. 예를 들어, 안전한 백업 네트워크 위치 및 안전한 클라우드 저장소 위치에 복사합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

임의 암호를 생성해야 한다고 지정한 경우 "passwords.txt" 파일을 추출하고 StorageGRID 시스템에 액세스하는 데 필요한 암호를 찾아야 합니다.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                  StorageGRID node recovery.                #####
######################################################################
```

확인 메시지가 표시되면 StorageGRID 시스템이 설치 및 구성됩니다.

```
StorageGRID has been configured and installed.
```

REST API 설치 개요

StorageGRID는 설치 작업을 수행하기 위한 두 가지 REST API, 즉 StorageGRID 설치 API와 StorageGRID 어플라이언스 설치 관리자 API를 제공합니다.

두 API 모두 Swagger 오픈 소스 API 플랫폼을 사용하여 API 문서를 제공합니다. swagger를 사용하면 개발자와 개발자가 아닌 사용자가 API가 매개 변수 및 옵션에 어떻게 응답하는지 보여주는 사용자 인터페이스에서 API와 상호 작용할 수 있습니다. 이 문서에서는 표준 웹 기술 및 JSON(JavaScript Object Notation) 데이터 형식에 대해 잘 알고 있다고 가정합니다.

> API Docs 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

각 REST API 명령에는 API의 URL, HTTP 작업, 필수 또는 선택적 URL 매개 변수, 그리고 예상되는 API 응답이 포함됩니다.

StorageGRID 설치 API

StorageGRID 설치 API는 StorageGRID 시스템을 처음 구성할 때와 기본 관리자 노드 복구를 수행해야 하는 경우에만 사용할 수 있습니다. 설치 API는 Grid Manager에서 HTTPS를 통해 액세스할 수 있습니다.

API 설명서에 액세스하려면 기본 관리 노드의 설치 웹 페이지로 이동하여 메뉴 모음에서 * 도움말 * > * API 설명서 * 를 선택합니다.

StorageGRID 설치 API에는 다음 섹션이 포함되어 있습니다.

- * config * — 제품 릴리스 및 API 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 API의 주요 버전을 나열할 수 있습니다.
- * 그리드 * — 그리드 레벨 구성 작업. 그리드 세부 정보, 그리드 네트워크 서브넷, 그리드 암호, NTP 및 DNS 서버 IP

주소를 포함한 그리드 설정을 얻고 업데이트할 수 있습니다.

- * 노드 * — 노드 레벨 구성 작업 그리드 노드 목록을 검색하고, 그리드 노드를 삭제하고, 그리드 노드를 구성하고, 그리드 노드를 보고, 그리드 노드의 구성을 재설정할 수 있습니다.
- * 프로비저닝 * — 프로비저닝 작업. 프로비저닝 작업을 시작하고 프로비저닝 작업의 상태를 볼 수 있습니다.
- * 복구 * — 기본 관리 노드 복구 작업 정보를 재설정하고, 복구 패키지를 업로드하고, 복구를 시작하고, 복구 작업의 상태를 볼 수 있습니다.
- * recovery-package * — 복구 패키지를 다운로드하기 위한 작업.
- * 사이트 * — 사이트 수준 구성 작업 사이트를 만들고, 보고, 삭제하고, 수정할 수 있습니다.

StorageGRID 어플라이언스 설치 관리자 **API**입니다

StorageGRID 어플라이언스 설치 프로그램 API는 HTTPS를 통해 '*Controller_IP*:8443'에서 액세스할 수 있습니다.

API 설명서에 액세스하려면 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램으로 이동하여 메뉴 모음에서 * 도움말 * > * API Docs * 를 선택합니다.

StorageGRID 어플라이언스 설치 관리자 API에는 다음 섹션이 포함되어 있습니다.

- * 클론 * — 노드 클로닝을 구성하고 제어하는 작업.
- * 암호화 * — 암호화를 관리하고 암호화 상태를 확인하는 작업.
- * 하드웨어 구성 * — 연결된 하드웨어에서 시스템 설정을 구성하는 작업.
- * 설치 * — 어플라이언스 설치 시작 및 설치 상태 모니터링을 위한 작업.
- * 네트워킹 * — StorageGRID 어플라이언스 및 어플라이언스 포트 설정에 대한 그리드, 관리자 및 클라이언트 네트워크 구성과 관련된 작업.
- * setup * — 시스템에 대한 정보를 얻고 기본 관리 노드 IP를 업데이트하는 요청을 포함하여 초기 어플라이언스 설치 설정에 도움이 되는 작업.
- * 지원 * — 컨트롤러 재부팅 및 로그 가져오기에 대한 운영
- * 업그레이드 * — 어플라이언스 펌웨어 업그레이드와 관련된 작업.
- * 업로그램 * — StorageGRID 설치 파일을 업로드하는 작업.

하드웨어 설치 문제 해결(**SG6000**)

설치 중에 문제가 발생하는 경우 하드웨어 설정 및 연결 문제와 관련된 문제 해결 정보를 검토하는 것이 도움이 될 수 있습니다.

SG6000-CN 컨트롤러의 부팅 코드를 봅니다

어플라이언스에 전원을 공급하면 BMC는 SG6000-CN 컨트롤러에 대한 일련의 부팅 코드를 기록합니다. 이러한 코드는 여러 가지 방법으로 볼 수 있습니다.

필요한 것

- BMC 대시보드에 액세스하는 방법을 알고 있습니다.
- SOL(Serial-over-LAN)을 사용하려는 경우 IPMI SOL 콘솔 애플리케이션을 사용하는 경험이 있습니다.

단계

1. 어플라이언스 컨트롤러의 부팅 코드를 보려면 다음 방법 중 하나를 선택하고 필요한 장비를 수집합니다.

방법	필수 장비
VGA 콘솔	• VGA 지원 모니터 • VGA 케이블
KVM	• RJ-45 케이블
직렬 포트	• DB-9 직렬 케이블 • 가상 직렬 터미널
솔	• 가상 직렬 터미널

2. VGA 콘솔을 사용하는 경우 다음 단계를 수행하십시오.
   a. VGA 지원 모니터를 제품 뒷면의 VGA 포트에 연결합니다.
   b. 모니터에 표시된 코드를 봅니다.
3. BMC KVM을 사용하는 경우 다음 단계를 수행하십시오.
   a. BMC 관리 포트에 연결하고 BMC 웹 인터페이스에 로그인합니다.
   b. 리모컨 * 을 선택합니다.
   c. KVM을 실행합니다.
   d. 가상 모니터에서 코드를 봅니다.
4. 직렬 포트 및 터미널을 사용하는 경우 다음 단계를 수행하십시오.
   a. 어플라이언스 뒷면의 DB-9 직렬 포트에 연결합니다.
   b. '115200 8-N-1' 설정을 사용합니다.
   c. 직렬 터미널에 인쇄된 코드를 봅니다.
5. SOL을 사용하는 경우 다음 단계를 수행하십시오.
   a. BMC IP 주소 및 로그인 자격 증명을 사용하여 IPMI SOL에 연결합니다.

      BMC 루트 계정 암호를 변경하지 않은 경우 공장 출하시 기본값은 "calvin"일 수 있습니다.

      'ipmitool-i lanplus-H_BMC_Port_IP_-U root-P_Password_SOL activate

   b. 가상 시리얼 터미널에서 코드를 봅니다.
6. 표를 사용하여 제품의 코드를 찾습니다.

코드	를 나타냅니다
안녕	마스터 부트 스크립트가 시작되었습니다.

코드	를 나타냅니다
HP	시스템에서 네트워크 인터페이스 카드(NIC) 펌웨어를 업데이트해야 하는지 확인합니다.
RB	펌웨어 업데이트를 적용한 후 시스템이 재부팅되고 있습니다.
FP	하드웨어 하위 시스템 펌웨어 업데이트 검사가 완료되었습니다. 컨트롤러 간 통신 서비스가 시작됩니다.
그는	어플라이언스 스토리지 노드 전용: 시스템이 스토리지 컨트롤러와의 연결을 기다리고 있으며 SANtricity 운영 체제와의 동기화를 기다리고 있습니다. • 참고: * 부팅 절차가 이 단계 이후 진행되지 않을 경우 다음 단계를 수행하십시오. a. SG6000-CN 컨트롤러와 2개의 스토리지 컨트롤러 사이의 4개의 상호 연결 케이블이 단단히 연결되어 있는지 확인합니다. b. 필요에 따라 하나 이상의 케이블을 교체하고 다시 시도하십시오. c. 그래도 문제가 해결되지 않으면 기술 지원 부서에 문의하십시오.
HC	시스템에서 기존 StorageGRID 설치 데이터를 확인하고 있습니다.
호	StorageGRID 어플라이언스 설치 프로그램이 실행 중입니다.
HA	StorageGRID가 실행 중입니다.

SG6000-CN 컨트롤러의 오류 코드를 봅니다

SG6000-CN 컨트롤러가 부팅 중일 때 하드웨어 오류가 발생하면 BMC가 오류 코드를 기록합니다. 필요한 경우 BMC 인터페이스를 사용하여 이러한 오류 코드를 확인한 다음 기술 지원 팀과 협력하여 문제를 해결할 수 있습니다.

필요한 것

- BMC 대시보드에 액세스하는 방법을 알고 있습니다.

단계

1. BMC 대시보드에서 * BIOS POST 코드 * 를 선택합니다.

2. 현재 코드 및 이전 코드에 대해 표시된 정보를 검토합니다.

   다음 오류 코드 중 하나가 표시되면 기술 지원 부서의 도움을 받고 문제를 해결하십시오.

코드	를 나타냅니다
0x0E	마이크로코드를 찾을 수 없습니다
0x0F	마이크로코드가 로드되지 않았습니다
0x50	메모리 초기화 오류. 잘못된 메모리 유형 또는 호환되지 않는 메모리 속도입니다.
0x51	메모리 초기화 오류. SPD 판독에 실패했습니다.
0x52	메모리 초기화 오류. 잘못된 메모리 크기 또는 메모리 모듈이 일치하지 않습니다.
0x53	메모리 초기화 오류. 사용 가능한 메모리가 없습니다.
0x54	지정되지 않은 메모리 초기화 오류입니다
0x55	메모리가 설치되지 않았습니다
0x56	잘못된 CPU 유형 또는 속도입니다
0x57	CPU가 일치하지 않습니다
0x58	CPU 자체 테스트에 실패했거나 CPU 캐시 오류가 발생했을 수 있습니다
0x59	CPU 마이크로 코드를 찾을 수 없거나 마이크로 코드를 업데이트하지 못했습니다
0x5A	내부 CPU 오류입니다
0x5B	PPI 재설정을 사용할 수 없습니다
0x5C	PEI 단계 BMC 자체 테스트에 실패했습니다
0xD0	CPU 초기화 오류
0xD1	노스 브리지 초기화 오류

코드	를 나타냅니다
0xD2	South bridge 초기화 오류
3	일부 아키텍처 프로토콜은 사용할 수 없습니다
0xD4	PCI 리소스 할당 오류입니다. 리소스 부족.
0xD5	레거시 옵션 ROM에 대한 공간이 없습니다
0xD6	콘솔 출력 장치를 찾을 수 없습니다
0xD7	콘솔 입력 장치를 찾을 수 없습니다
0xD8	잘못된 암호입니다
0xD9	부팅 옵션 로드 중 오류 발생(LoadImage가 오류를 반환함)
0xDA	부팅 옵션 실패(StartImage가 오류를 반환함)
0xDB입니다	플래시를 업데이트하지 못했습니다
0xDC	재설정 프로토콜을 사용할 수 없습니다
0xDD	DXE 단계 BMC 자체 테스트 실패
0xE8	MRC:ERR_NO_MEMORY
0xE9	MRC:ERR_LT_LOCK
0xEA	MRC:ERR_DDR_INIT
0xEB	MRC:ERR_MEM_TEST
0xEC	MRC:ERR_VENDOR_VENDOR_VENCE
0XED	MRC:ERR_DIMM_COMPAT
0xEE	MRC:ERR_MRC_compatibility
0xEF	MRC:ERR_MRC_struct
0xF0	MRC:ERR_SET_VDD

코드	를 나타냅니다
0xF1	MRC:ERR_IOT_MEM_BUFFER
0xF2	MRC:ERR_RC_INTERNAL입니다
0xF3	MRC:ERR_INVALID_REG_ACCESS
0xF4	MRC:ERR_SET_MC_Freq
0xF5	MRC:ERR_READ_MC_Freq
0x70	MRC:ERR_DIMM_CHANNEL
0x74	MRC:ERR_BIST_CHECK
0xF6	MRC:ERR_SMBus를 선택합니다
0xF7	MRC:ERR_PCU
0xF8	MRC:ERR_NGN
0xF9	MRC:ERR_interLeave_failure

하드웨어 설치가 중단된 것 같습니다**(SG6000).**

하드웨어 장애 또는 케이블 연결 오류로 인해 스토리지 컨트롤러 또는 SG6000-CN 컨트롤러가 부팅 처리를 완료하지 못하는 경우 StorageGRID 어플라이언스 설치 프로그램을 사용할 수 없습니다.

단계

1. 스토리지 컨트롤러의 경우 7세그먼트 디스플레이에서 코드를 확인합니다.

   전원을 켜는 동안 하드웨어가 초기화되는 동안 2개의 7세그먼트 디스플레이에는 일련의 코드가 표시됩니다. 하드웨어가 성공적으로 부팅되면 7세그먼트 디스플레이 모두 99로 표시됩니다.

2. SG6000-CN 컨트롤러의 LED와 BMC에 표시되는 부팅 및 오류 코드를 검토합니다.
3. 문제 해결에 도움이 필요한 경우 기술 지원 부서에 문의하십시오.

관련 정보

SG6000 스토리지 컨트롤러의 부팅 상태 코드를 봅니다

"E5700 및 E2800 시스템 모니터링 가이드"

SG6000-CN 컨트롤러의 상태 표시등 및 단추를 봅니다

SG6000-CN 컨트롤러의 부팅 코드를 봅니다

SG6000-CN 컨트롤러의 오류 코드를 봅니다

연결 문제 해결**(SG6000)**

StorageGRID 어플라이언스 설치 중에 연결 문제가 발생하면 나열된 수정 조치 단계를 수행해야 합니다.

어플라이언스에 연결할 수 없습니다

어플라이언스에 연결할 수 없는 경우 네트워크 문제가 있거나 하드웨어 설치가 성공적으로 완료되지 않았을 수 있습니다.

단계

1. SANtricity 시스템 관리자에 연결할 수 없는 경우:
   a. SANtricity 시스템 관리자의 관리 네트워크에 있는 스토리지 컨트롤러의 IP 주소(+'* ping_storage_controller_ip_ * ')를 사용하여 어플라이언스를 ping합니다
   b. Ping에서 응답이 없는 경우 올바른 IP 주소를 사용하고 있는지 확인합니다.

      스토리지 컨트롤러의 관리 포트 1에 대한 IP 주소를 사용합니다.

   c. IP 주소가 올바른 경우 어플라이언스 케이블 연결 및 네트워크 설정을 확인하십시오.

      그래도 문제가 해결되지 않으면 기술 지원 부서에 문의하십시오.

   d. Ping에 성공하면 웹 브라우저를 엽니다.
   e. SANtricity 시스템 관리자의 URL을 입력합니다: + `https://Storage_Controller_IP*`

      SANtricity 시스템 관리자의 로그인 페이지가 나타납니다.

2. SG6000-CN 컨트롤러에 연결할 수 없는 경우:
   a. SG6000-CN 컨트롤러의 IP 주소를 사용하여 어플라이언스에 ping을 시도해 보십시오: + '* PING_SG6000-CN_Controller_IP_ * '
   b. Ping에서 응답이 없는 경우 올바른 IP 주소를 사용하고 있는지 확인합니다.

      그리드 네트워크, 관리 네트워크 또는 클라이언트 네트워크에서 어플라이언스의 IP 주소를 사용할 수 있습니다.

   c. IP 주소가 올바른 경우 어플라이언스 케이블 연결, SFP 트랜시버 및 네트워크 설정을 확인하십시오.
   d. SG6000-CN에 물리적으로 액세스할 수 있는 경우 영구 링크 로컬 IP인 169.254.0.1에 직접 연결하여 컨트롤러 네트워킹 구성을 확인하고 필요한 경우 업데이트할 수 있습니다. 자세한 지침은 의 2단계를 참조하십시오 StorageGRID 어플라이언스 설치 프로그램에 액세스합니다.

      그래도 문제가 해결되지 않으면 기술 지원 부서에 문의하십시오.

   e. Ping에 성공하면 웹 브라우저를 엽니다.
   f. StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. + `https://SG6000-CN_Controller_IP:8443*`

홈 페이지가 나타납니다.

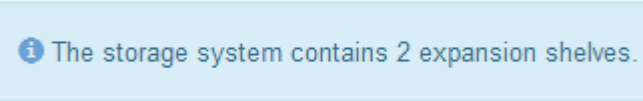
확장 셸프가 **Appliance Installer**에 나타나지 않습니다

SG6060 또는 SG6060X용 확장 셸프가 설치되어 있고 StorageGRID 어플라이언스 설치 프로그램에 나타나지 않는 경우 셸프가 완전히 설치되고 전원이 켜져 있는지 확인해야 합니다.

이 작업에 대해

StorageGRID 어플라이언스 설치 프로그램에서 다음 정보를 확인하여 확장 쉘프가 어플라이언스에 연결되어 있는지 확인할 수 있습니다.

- 홈 * 페이지에는 확장 셸프에 대한 메시지가 포함되어 있습니다.



- 고급 * > * RAID 모드 * 페이지는 어플라이언스에 확장 쉘프가 포함되어 있는지 여부에 관계 없이 드라이브 수로 표시됩니다. 예를 들어, 다음 스크린 샷에서는 SSD 2개와 178 HDD가 표시되어 있습니다. 2개의 확장 쉘프가 있는 SG6060에는 총 180개의 드라이브가 포함됩니다.

Configure RAID Mode

This appliance contains the following drives.

Type	Size	Number of drives
SSD	800 GB	2
HDD	11.8 TB	178

StorageGRID 어플라이언스 설치 프로그램 페이지에 확장 셸프가 있는 것으로 표시되지 않으면 다음 절차를 따르십시오.

단계

1. 확인합니다 필요한 모든 케이블이 단단히 연결되었습니다.
2. 이 있는지 확인하십시오 확장 셸프의 전원을 켭니다.
3. 문제 해결에 도움이 필요한 경우 기술 지원 부서에 문의하십시오.

StorageGRID 어플라이언스 설치 프로그램이 실행되는 동안 **SG6000-CN** 컨트롤러를 재부팅합니다

StorageGRID 어플라이언스 설치 프로그램이 실행되는 동안 SG6000-CN 컨트롤러를 재부팅해야 할 수 있습니다. 예를 들어, 설치에 실패한 경우 컨트롤러를 재부팅해야 할 수 있습니다.

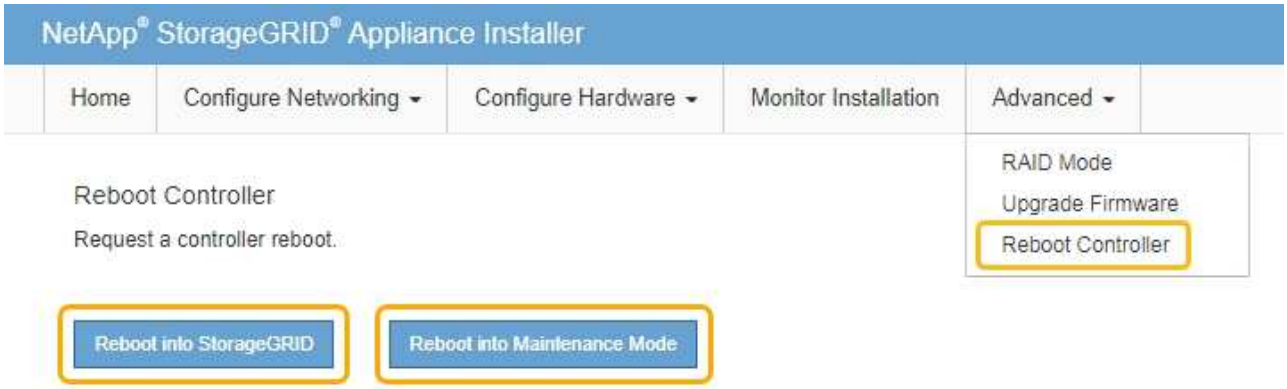
이 작업에 대해

이 절차는 SG6000-CN 컨트롤러가 StorageGRID 어플라이언스 설치 프로그램을 실행하는 경우에만 적용됩니다. 설치가 완료되면 StorageGRID 어플라이언스 설치 프로그램을 더 이상 사용할 수 없기 때문에 이 단계가 더 이상 작동하지 않습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 클릭한 후 다음 옵션 중 하나를 선택합니다.

   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



   SG6000-CN 컨트롤러가 재부팅된다.

SG6000 어플라이언스를 유지보수하십시오

SG6000 어플라이언스에서 유지보수 절차를 수행해야 할 수 있습니다. 이 섹션의 절차에서는 어플라이언스가 이미 StorageGRID 시스템의 스토리지 노드로 구축되었다고 가정합니다.

서비스 중단을 방지하려면 서비스 중단 기간이 허용되는 예약된 유지 관리 기간 동안 어플라이언스를 종료하거나 종료하기 전에 다른 모든 스토리지 노드가 그리드에 연결되어 있는지 확인하십시오. 에 대한 정보를 참조하십시오 노드 연결 상태를 모니터링합니다.

> 개체의 복사본을 하나만 만드는 ILM 규칙을 사용한 적이 있는 경우 예정된 유지 관리 기간 동안 어플라이언스를 종료해야 합니다. 그렇지 않으면 스토리지 노드의 서비스가 중지되는 유지보수 절차 중에 이러한 개체에 일시적으로 액세스할 수 없게 될 수 있습니다. 에 대한 정보를 참조하십시오 정보 수명 주기 관리로 개체 관리.

제품을 유지보수 모드로 전환합니다

특정 유지보수 절차를 수행하기 전에 제품을 유지보수 모드로 전환해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

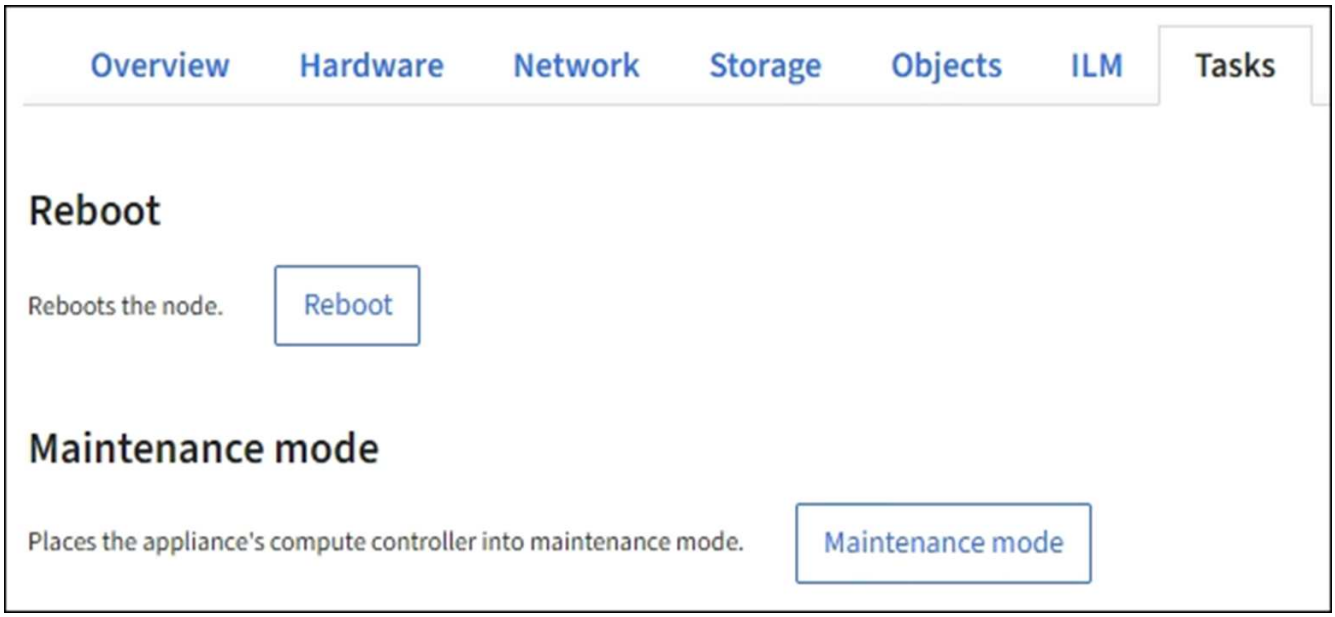
이 작업에 대해

StorageGRID 어플라이언스를 유지보수 모드로 전환하면 원격 액세스가 불가능한 경우가 드물게 있습니다.

> 유지보수 모드에서 StorageGRID 어플라이언스에 대한 admin 계정 암호 및 SSH 호스트 키는 어플라이언스가 서비스 중일 때와 동일하게 유지됩니다.

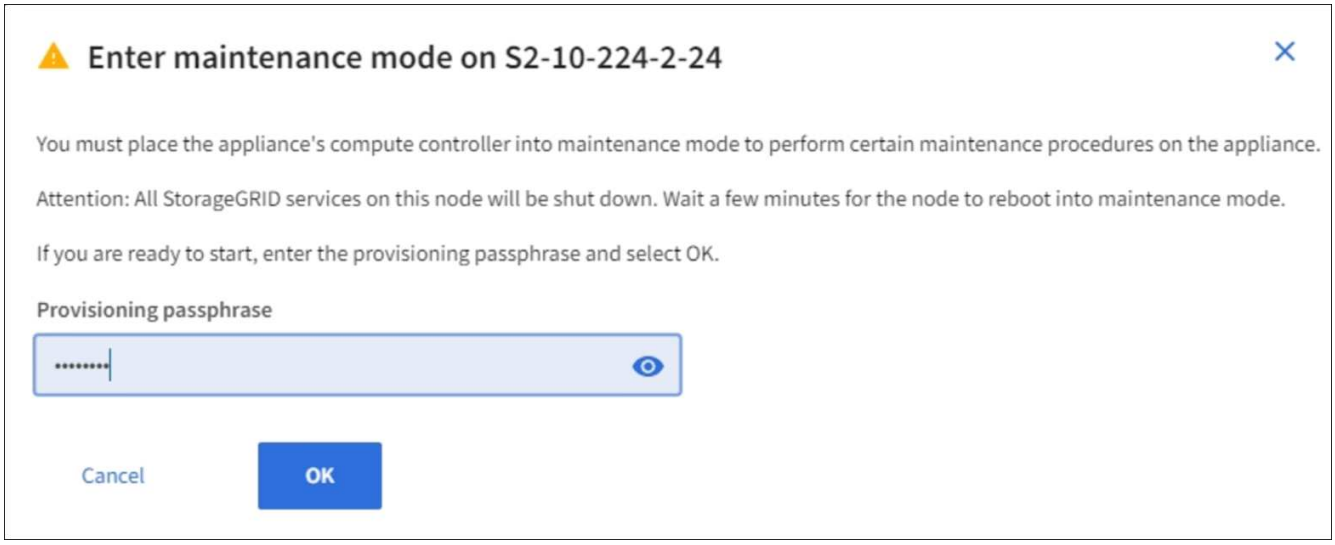
단계

1. Grid Manager에서 * nodes * 를 선택합니다.
2. 노드 페이지의 트리 뷰에서 어플라이언스 스토리지 노드를 선택합니다.
3. 작업 * 을 선택합니다.



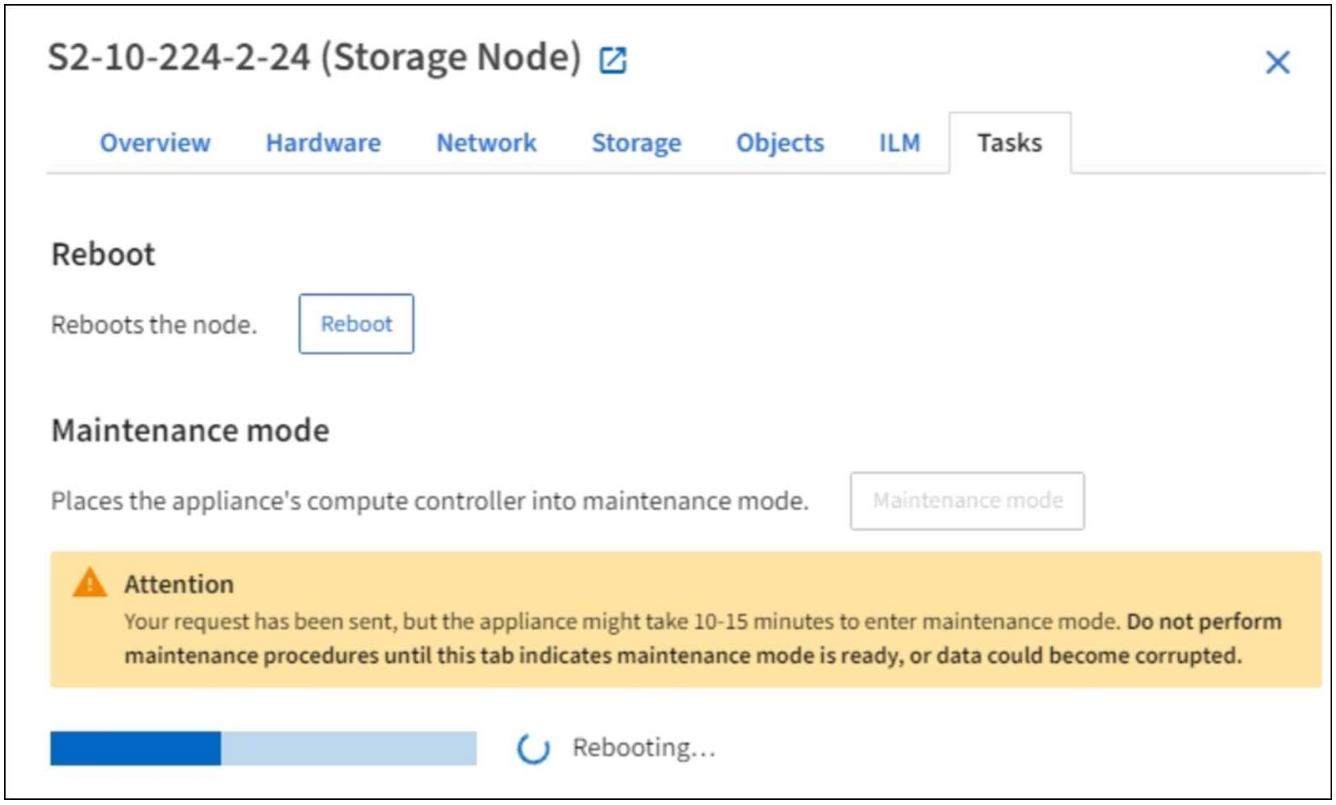
4. 유지보수 모드 * 를 선택합니다.

   확인 대화 상자가 나타납니다.

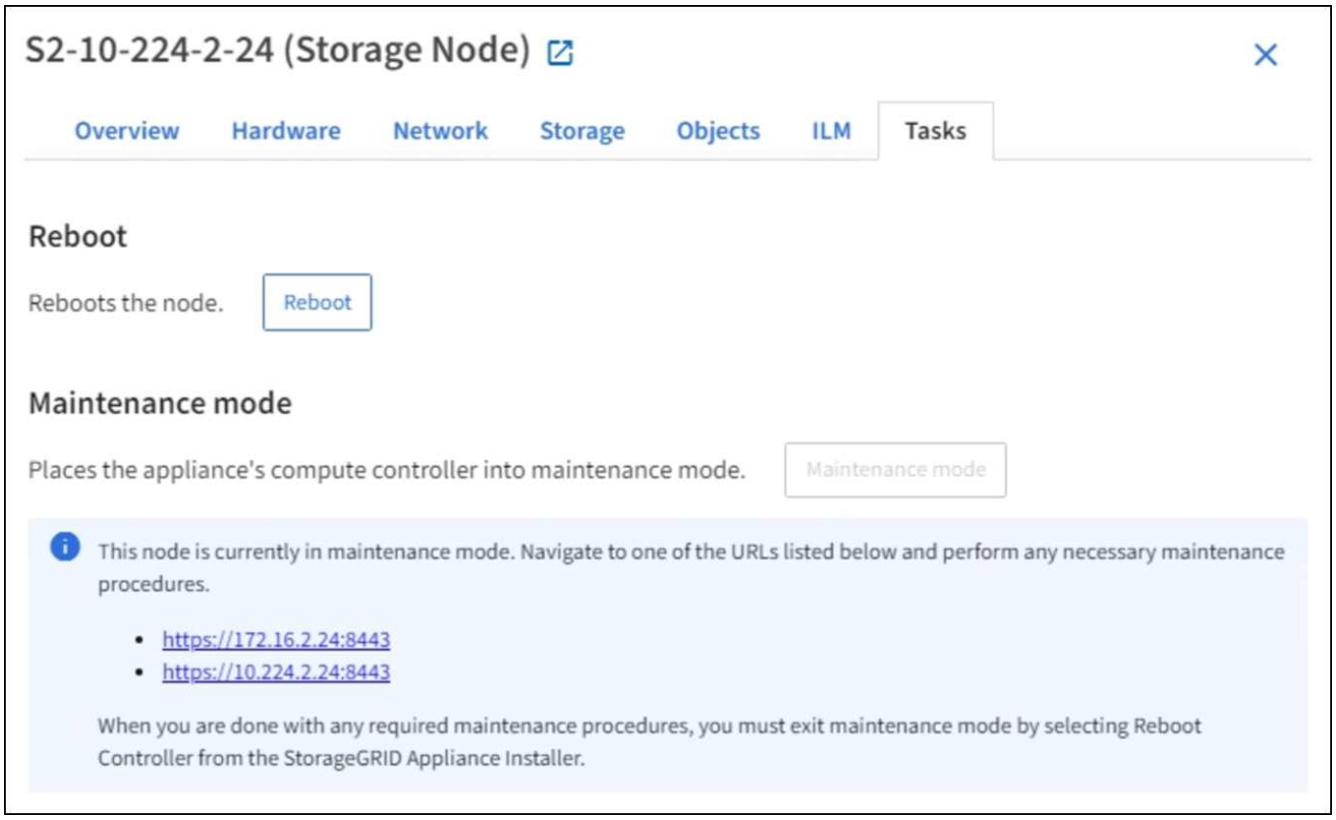


5. 프로비저닝 암호를 입력하고 * OK * 를 선택합니다.

진행 표시줄과 "전송 요청", "StorageGRID 중지" 및 "재부팅"을 포함한 일련의 메시지는 어플라이언스가 유지보수 모드로 들어가기 위한 단계를 완료하고 있음을 나타냅니다.



어플라이언스가 유지보수 모드일 때 확인 메시지에 StorageGRID 어플라이언스 설치 프로그램에 액세스하는 데 사용할 수 있는 URL이 나열됩니다.



6. StorageGRID 어플라이언스 설치 프로그램에 액세스하려면 표시된 URL 중 하나를 찾습니다.

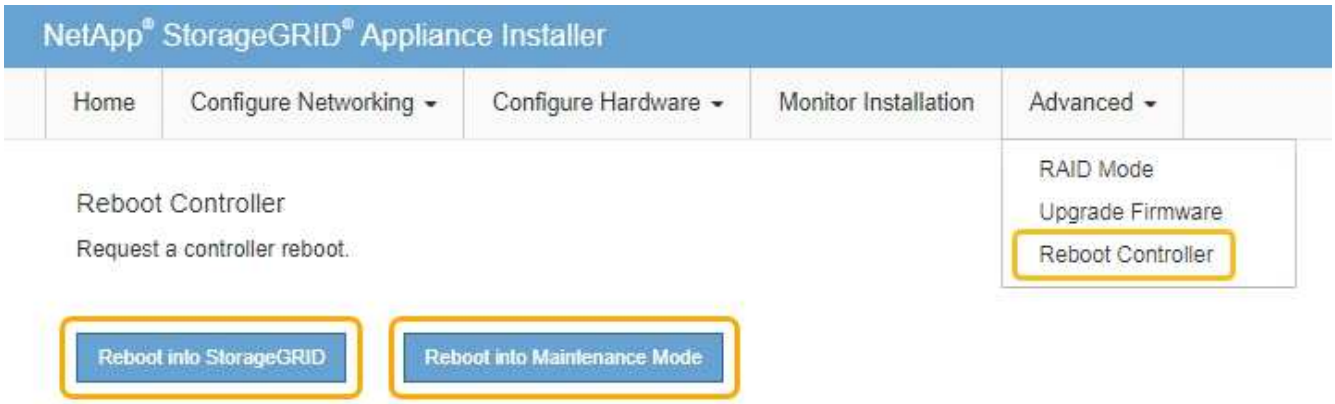
   가능한 경우 어플라이언스의 관리 네트워크 포트의 IP 주소가 포함된 URL을 사용하십시오.

   > 어플라이언스의 관리 포트에 직접 연결되어 있는 경우, 'https://169.254.0.1:8443` 을 사용하여 StorageGRID 어플라이언스 설치 프로그램 페이지에 액세스하십시오.

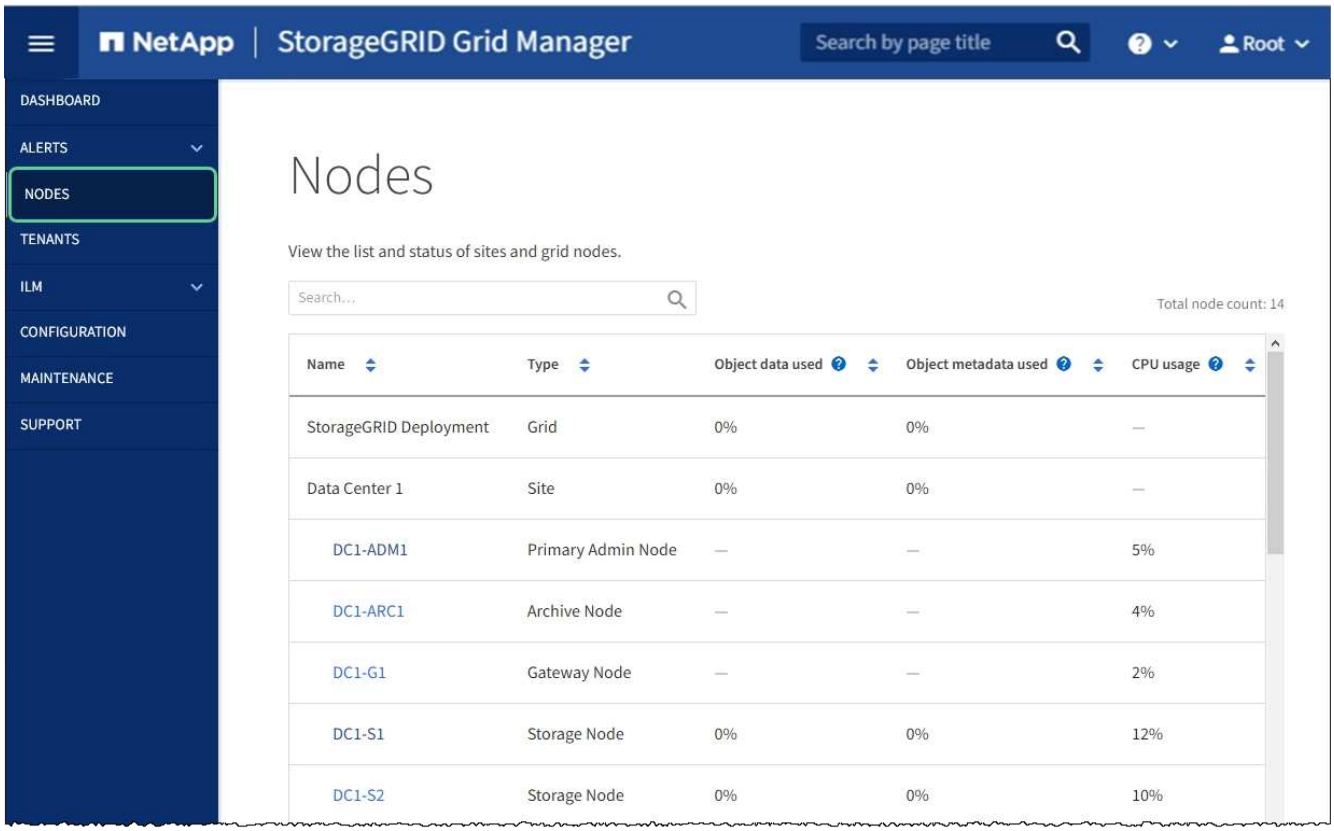
7. StorageGRID 어플라이언스 설치 프로그램에서 어플라이언스가 유지보수 모드인지 확인합니다.

   ⚠ This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to reboot the controller.

8. 필요한 유지보수 작업을 수행합니다.
9. 유지보수 작업을 완료한 후 유지보수 모드를 종료하고 정상 노드 운영을 재개합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * StorageGRID * 으로 재부팅 * 을 선택합니다.



   어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



스토리지 컨트롤러에서 **SANtricity OS**를 업그레이드합니다

스토리지 컨트롤러가 최적의 상태로 작동하도록 하려면 StorageGRID 어플라이언스에 적합한 SANtricity OS의 최신 유지 관리 릴리즈로 업그레이드해야 합니다. NetApp 상호 운용성 매트릭스 툴(IMT) 을 참조하여 사용해야 하는 버전을 확인하십시오. 도움이 필요한 경우 기술 지원 팀에 문의하십시오.

현재 설치된 SANtricity OS 버전에 따라 다음 절차 중 하나를 사용하십시오.

- 스토리지 컨트롤러가 SANtricity OS 08.42.20.00(11.42) 이상을 사용하는 경우 그리드 관리자를 사용하여 업그레이드를 수행합니다.

  그리드 관리자를 사용하여 스토리지 컨트롤러의 SANtricity OS를 업그레이드합니다

- 스토리지 컨트롤러가 08.42.20.00(11.42) 이전의 SANtricity OS 버전을 사용하는 경우 유지보수 모드를 사용하여 업그레이드를 수행합니다.

  유지보수 모드를 사용하여 스토리지 컨트롤러에서 SANtricity OS를 업그레이드합니다

> 스토리지 어플라이언스에 대한 SANtricity OS를 업그레이드할 때는 StorageGRID 설명서의 지침을 따라야 합니다. 다른 지침을 사용하면 제품이 작동하지 않을 수 있습니다.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

"NetApp 다운로드: StorageGRID 어플라이언스"

그리드 관리자를 사용하여 스토리지 컨트롤러의 **SANtricity OS**를 업그레이드합니다

현재 SANtricity OS 08.42.20.00(11.42) 이상을 사용하는 스토리지 컨트롤러의 경우 그리드 관리자를 사용하여 업그레이드를 적용해야 합니다.

필요한 것

- 업그레이드에 사용 중인 SANtricity OS 버전이 어플라이언스와 호환되는지 확인하려면 NetApp 상호 운용성 매트릭스 툴(IMT)을 참조하십시오.
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 프로비저닝 암호가 있습니다.
- SANtricity OS의 NetApp 다운로드 페이지에 액세스할 수 있습니다.

이 작업에 대해

SANtricity OS 업그레이드 프로세스를 완료할 때까지 다른 소프트웨어 업데이트(StorageGRID 소프트웨어 업그레이드 또는 핫픽스)를 수행할 수 없습니다. SANtricity OS 업그레이드 프로세스가 완료되기 전에 핫픽스 또는 StorageGRID 소프트웨어 업그레이드를 시작하려고 하면 SANtricity OS 업그레이드 페이지로 리디렉션됩니다.

SANtricity OS 업그레이드가 업그레이드를 위해 선택된 모든 적용 가능한 노드에 적용되기 전에는 절차가 완료되지 않습니다. 각 노드에서 SANtricity OS를 로드하는 데 30분 이상, 각 StorageGRID 스토리지 어플라이언스를 재부팅하는 데 최대 90분이 걸릴 수 있습니다.

> 다음 단계는 그리드 관리자를 사용하여 업그레이드를 수행하는 경우에만 적용됩니다. 컨트롤러가 08.42.20.00(11.42) 이전의 SANtricity OS를 사용하는 경우 그리드 관리자를 사용하여 어플라이언스의 스토리지 컨트롤러를 업그레이드할 수 없습니다.

> 이 절차에서는 NVSRAM을 SANtricity OS 업그레이드와 관련된 최신 버전으로 자동 업그레이드합니다. 별도의 NVSRAM 업그레이드 파일을 적용할 필요가 없습니다.

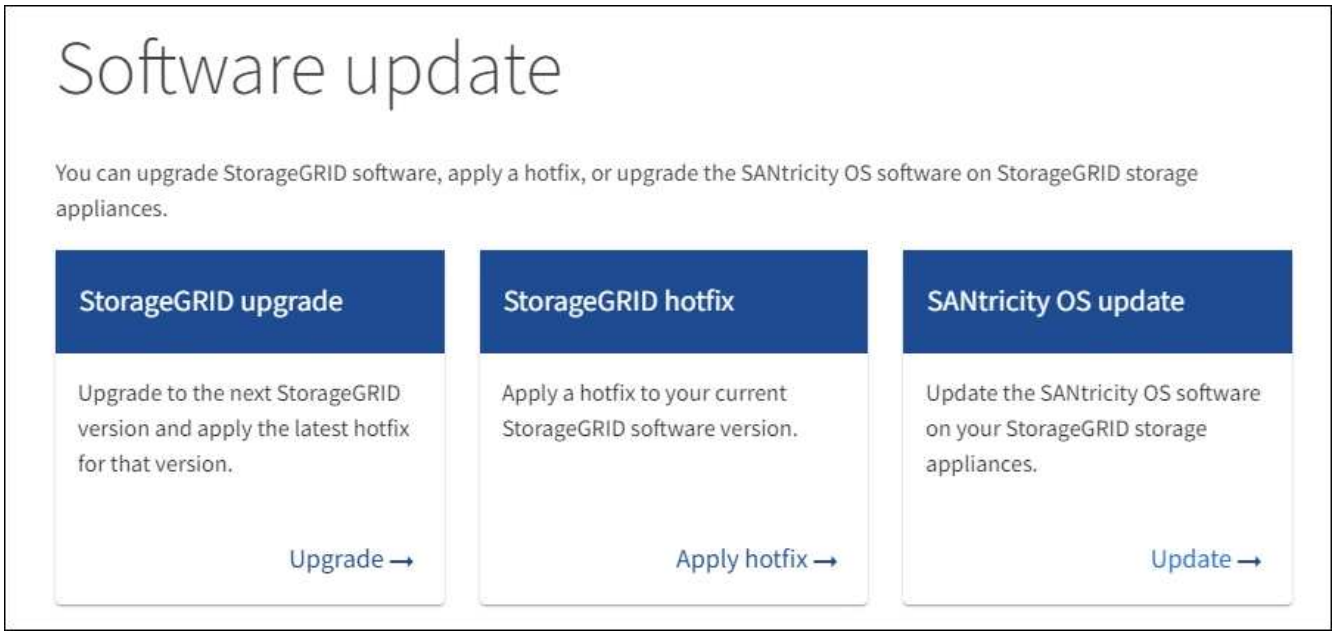
단계

1. NetApp Support 사이트에서 새로운 SANtricity OS 소프트웨어 파일을 다운로드합니다.

   스토리지 컨트롤러의 SANtricity OS 버전을 선택해야 합니다.

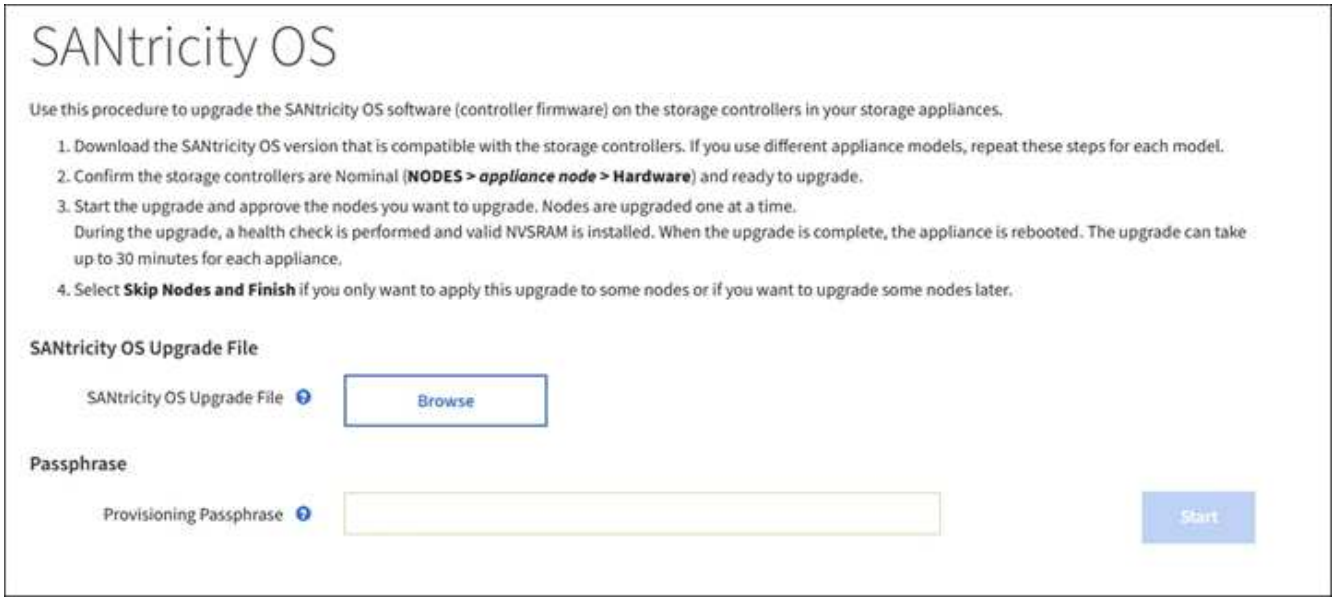
   "NetApp 다운로드: StorageGRID 어플라이언스"

2. 유지보수 * > * 시스템 * > * 소프트웨어 업데이트 * 를 선택합니다.



3. SANtricity OS 업데이트 섹션에서 * 업데이트 * 를 선택합니다.

   SANtricity OS 업그레이드 페이지가 나타납니다.



4. NetApp Support 사이트에서 다운로드한 SANtricity OS 업그레이드 파일을 선택합니다.

   a. 찾아보기 * 를 선택합니다.

   b. 파일을 찾아 선택합니다.

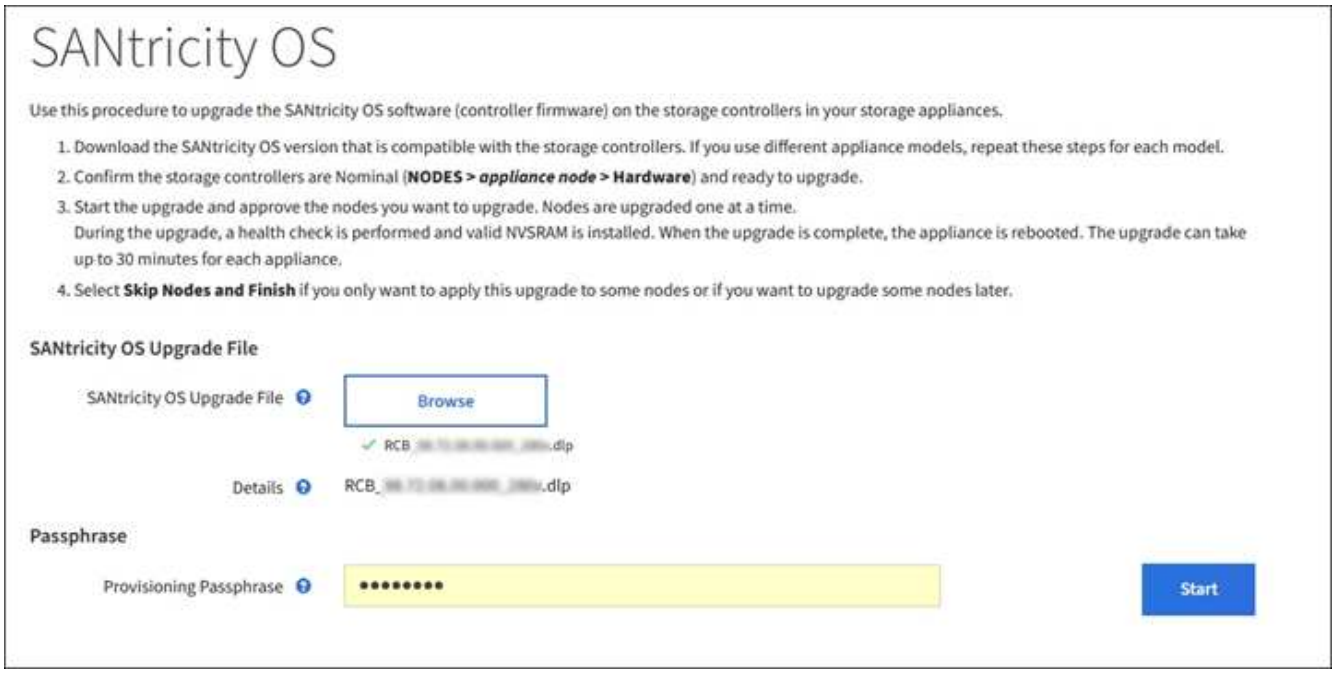
   c. 열기 * 를 선택합니다.

      파일이 업로드되고 검증됩니다. 유효성 검사 프로세스가 완료되면 * 찾아보기 * 버튼 옆에 파일 이름이 표시됩니다.

      ⓘ 파일 이름은 확인 프로세스의 일부이므로 변경하지 마십시오.

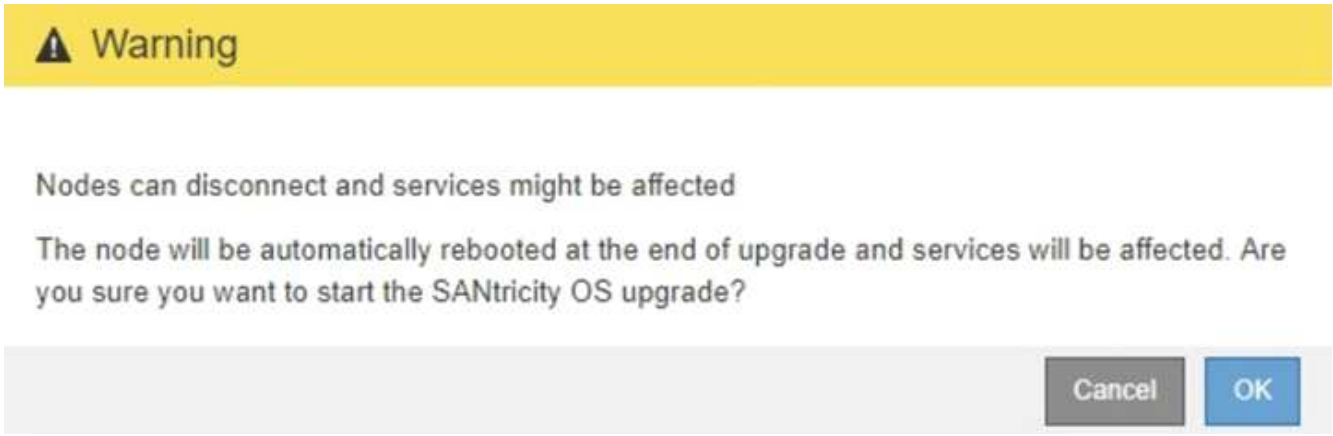
5. 프로비저닝 암호를 입력합니다.

   시작 * 버튼이 활성화됩니다.



6. 시작 * 을 선택합니다.

   업그레이드된 노드의 서비스가 다시 시작됨에 따라 브라우저의 연결이 일시적으로 끊길 수 있다는 경고 상자가 나타납니다.



7. SANtricity OS 업그레이드 파일을 기본 관리 노드로 스테이징하려면 * OK * 를 선택하십시오.

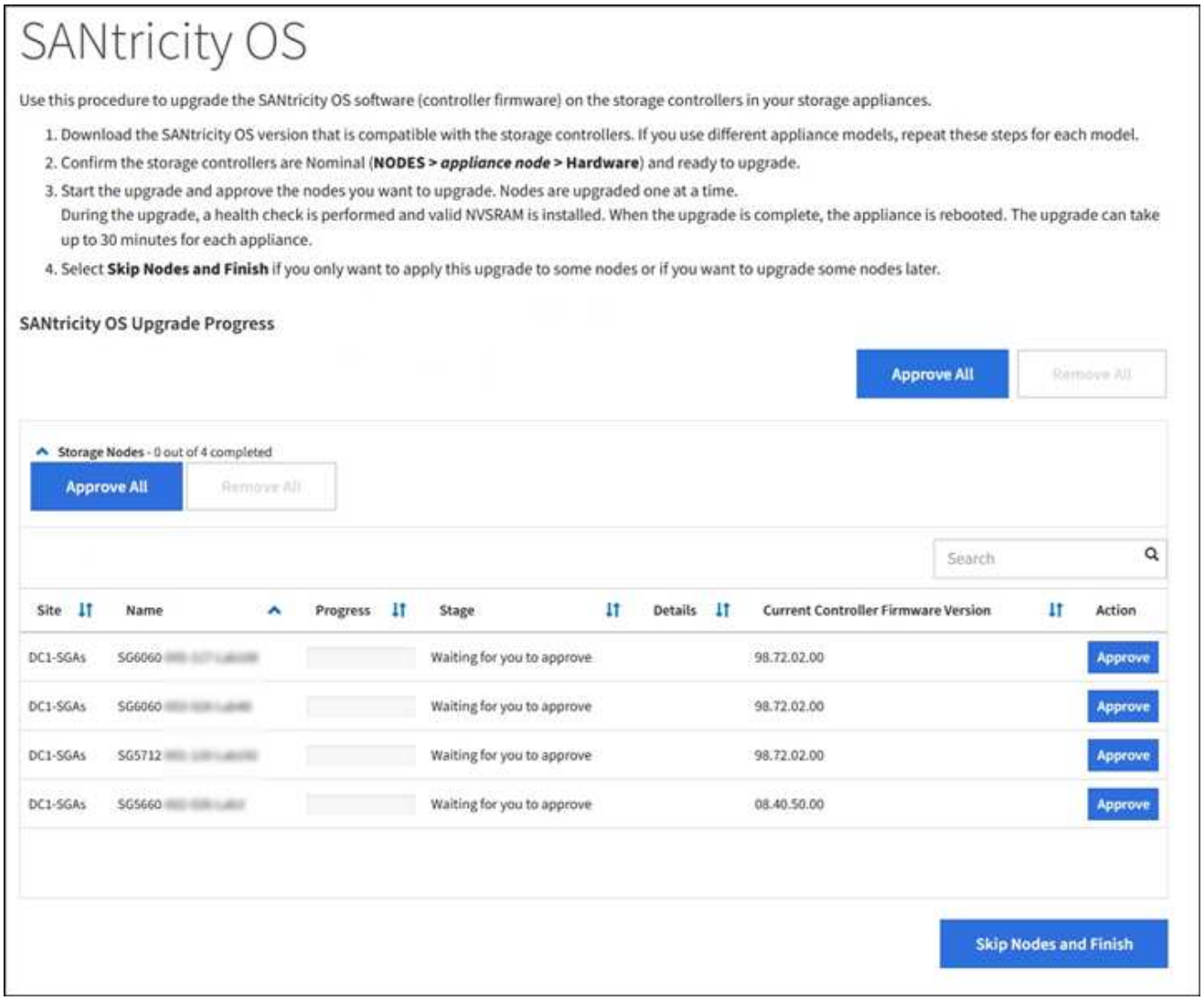
   SANtricity OS 업그레이드가 시작될 때:

   a. 상태 점검이 실행됩니다. 이 프로세스에서는 노드 상태가 주의 필요 인지 확인합니다.

      ⓘ 오류가 보고되면 이를 해결하고 * 시작 * 을 다시 선택합니다.

   b. SANtricity OS 업그레이드 진행률 테이블이 나타납니다. 이 표에는 그리드의 모든 스토리지 노드 및 각 노드의 현재 업그레이드 단계가 나와 있습니다.

이 표에는 모든 어플라이언스 스토리지 노드가 표시됩니다. 소프트웨어 기반 스토리지 노드가 표시되지 않습니다. 업그레이드가 필요한 모든 노드에 대해 * Approve * 를 선택합니다.



8. 선택적으로 * Site *, * Name *, * Progress *, * Stage *, * Details *, * Site *, * Site *, *, * Details *, 또는 * 현재 컨트롤러 펌웨어 버전 *. 또는 * 검색 * 상자에 용어를 입력하여 특정 노드를 검색합니다.

   섹션의 오른쪽 아래 모서리에 있는 왼쪽 및 오른쪽 화살표를 사용하여 노드 목록을 스크롤할 수 있습니다.

9. 업그레이드 대기열에 추가할 준비가 된 그리드 노드를 승인합니다. 동일한 유형의 승인된 노드는 한 번에 하나씩 업그레이드됩니다.

   노드를 중지하고 재부팅할 준비가 되어 있는지 확실하지 않은 경우 어플라이언스 스토리지 노드에 대한 SANtricity OS 업그레이드를 승인하지 마십시오. 노드에서 SANtricity OS 업그레이드가 승인되면 해당 노드의 서비스가 중지되고 업그레이드 프로세스가 시작됩니다. 나중에 노드 업그레이드가 완료되면 어플라이언스 노드가 재부팅됩니다. 이러한 작업은 노드와 통신하는 클라이언트에 대해 서비스 중단을 일으킬 수 있습니다.

   - 모든 스토리지 노드를 SANtricity OS 업그레이드 대기열에 추가하려면 * 모두 승인 * 버튼 중 하나를 선택합니다.

> 노드 업그레이드 순서가 중요한 경우 노드 또는 노드 그룹을 한 번에 하나씩 승인하고 다음 노드를 승인하기 전에 각 노드에서 업그레이드가 완료될 때까지 기다립니다.

- 하나 이상의 * Approve * (승인 *) 버튼을 선택하여 하나 이상의 노드를 SANtricity OS 업그레이드 대기열에 추가합니다.

  Approve * 를 선택하면 업그레이드 프로세스에서 노드를 업그레이드할 수 있는지 여부를 결정합니다. 노드를 업그레이드할 수 있는 경우 업그레이드 대기열에 추가됩니다.

일부 노드의 경우 선택한 업그레이드 파일이 의도적으로 적용되지 않으며 이러한 특정 노드를 업그레이드하지 않고 업그레이드 프로세스를 완료할 수 있습니다. 의도적으로 업그레이드되지 않은 노드는 완료(업그레이드 시도) 단계를 표시하고 세부 정보 열에 노드가 업그레이드되지 않은 이유를 표시합니다.

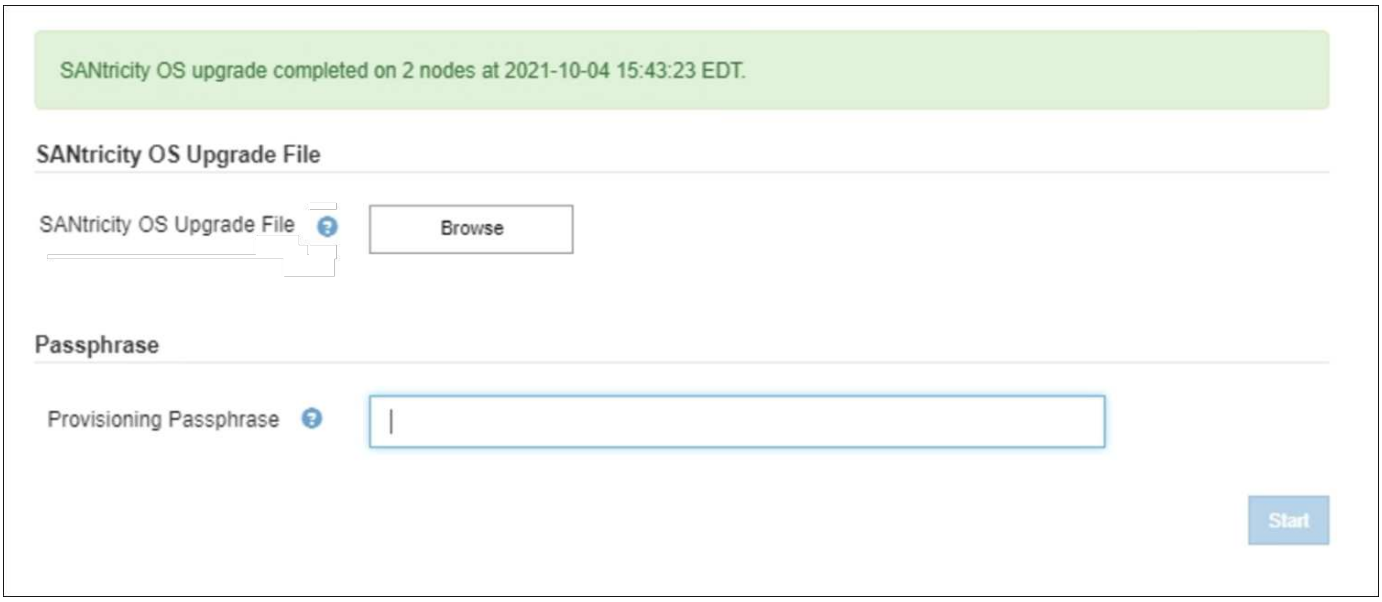
10. SANtricity OS 업그레이드 대기열에서 노드 또는 모든 노드를 제거해야 하는 경우 * 제거 * 또는 * 모두 제거 * 를 선택합니다.

    스테이지가 대기 모드 를 넘어 진행되면 * 제거 * 버튼이 숨겨지고 더 이상 SANtricity OS 업그레이드 프로세스에서 노드를 제거할 수 없습니다.

11. SANtricity OS 업그레이드가 승인된 각 그리드 노드에 적용될 때까지 기다립니다.

    - SANtricity OS 업그레이드를 적용하는 동안 노드에 오류 단계가 표시되는 경우 해당 노드에 대한 업그레이드가 실패한 것입니다. 기술 지원의 도움을 받아 어플라이언스를 유지보수 모드로 전환하여 복구해야 할 수도 있습니다.
    - 노드의 펌웨어가 너무 오래되어 그리드 관리자로 업그레이드되지 않는 경우, 노드에 오류 단계가 표시됩니다: ""이 노드에서 SANtricity OS를 업그레이드하려면 유지보수 모드를 사용해야 합니다. 제품의 설치 및 유지관리 지침을 참조하십시오. 업그레이드 후 향후 업그레이드를 위해 이 유틸리티를 사용할 수 있습니다." 오류를 해결하려면 다음을 수행합니다.
      i. 유지보수 모드를 사용하여 오류 단계가 표시된 노드에서 SANtricity OS를 업그레이드합니다.
      ii. 그리드 관리자를 사용하여 SANtricity OS 업그레이드를 다시 시작하고 완료합니다.

    승인된 모든 노드에서 SANtricity OS 업그레이드가 완료되면 SANtricity OS 업그레이드 진행률 테이블이 닫히고 SANtricity OS 업그레이드가 완료된 날짜와 시간이 녹색 배너에 표시됩니다.



1. 노드를 업그레이드할 수 없는 경우 세부 정보 열에 표시된 이유를 기록하고 적절한 조치를 취하십시오.
   - "스토리지 노드가 이미 업그레이드되었습니다." 추가 조치가 필요하지 않습니다.
   - "SANtricity OS 업그레이드는 이 노드에 적용되지 않습니다." 노드에는 StorageGRID 시스템에서 관리할 수 있는 스토리지 컨트롤러가 없습니다. 이 메시지가 표시된 노드를 업그레이드하지 않고 업그레이드 프로세스를 완료합니다.
   - "'SANtricity OS 파일이 이 노드와 호환되지 않습니다.'" 노드에는 선택한 것과 다른 SANtricity OS 파일이 필요합니다. 현재 업그레이드를 완료한 후 노드에 대한 올바른 SANtricity OS 파일을 다운로드하고 업그레이드 프로세스를 반복합니다.

> 나열된 모든 스토리지 노드에서 SANtricity OS 업그레이드를 승인할 때까지 SANtricity OS 업그레이드 프로세스가 완료되지 않습니다.

1. 노드 승인을 종료하여 SANtricity OS 페이지로 돌아가 새 SANtricity OS 파일 업로드를 허용하려면 다음을 수행합니다.
   a. 노드 건너뛰기 및 마침 * 을 선택합니다.

      모든 노드를 업그레이드하지 않고 업그레이드 프로세스를 완료할지 묻는 경고가 나타납니다.

   b. SANtricity OS * 페이지로 돌아가려면 * OK * 를 선택하십시오.
   c. 노드 승인을 계속할 준비가 되면 로 이동합니다 SANtricity OS를 다운로드합니다 를 눌러 업그레이드 프로세스를 다시 시작합니다.

      > 노드가 이미 승인되었으며 오류 없이 업그레이드되었습니다.

2. 다른 SANtricity OS 업그레이드 파일이 필요한 전체 단계가 있는 노드에 대해 이 업그레이드 절차를 반복합니다.

> Needs Attention(주의 필요) 상태인 모든 노드의 경우 유지보수 모드를 사용하여 업그레이드를 수행합니다.

> 업그레이드 절차를 반복하면 이전에 업그레이드된 노드를 승인해야 합니다.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

유지보수 모드를 사용하여 스토리지 컨트롤러에서 SANtricity OS를 업그레이드합니다

유지보수 모드를 사용하여 스토리지 컨트롤러에서 **SANtricity OS**를 업그레이드합니다

현재 08.42.20.00(11.42) 이전의 SANtricity OS를 사용하는 스토리지 컨트롤러의 경우, 업그레이드를 적용하려면 유지보수 모드 절차를 사용해야 합니다.

필요한 것

- 업그레이드에 사용 중인 SANtricity OS 버전이 어플라이언스와 호환되는지 확인하려면 NetApp 상호 운용성 매트릭스 툴(IMT)을 참조하십시오.
- StorageGRID 어플라이언스가 StorageGRID 시스템에서 실행 중인 경우 SG6000-CN 컨트롤러는 입니다 유지보수 모드로 전환됩니다.

> 유지보수 모드는 스토리지 컨트롤러에 대한 연결을 중단합니다.

이 작업에 대해

한 번에 두 개 이상의 StorageGRID 어플라이언스에 있는 E-Series 컨트롤러의 SANtricity OS 또는 NVSRAM을 업그레이드하지 마십시오.

> 배포 모델 및 ILM 정책에 따라 한 번에 둘 이상의 StorageGRID 어플라이언스를 업그레이드할 경우 데이터를 사용할 수 없게 될 수 있습니다.

단계

1. 제품이 에 있는지 확인하십시오 유지보수 모드.
2. 서비스 랩톱에서 SANtricity System Manager에 액세스하고 로그인합니다.
3. 관리 클라이언트에 새 SANtricity OS 소프트웨어 파일 및 NVSRAM 파일을 다운로드합니다.

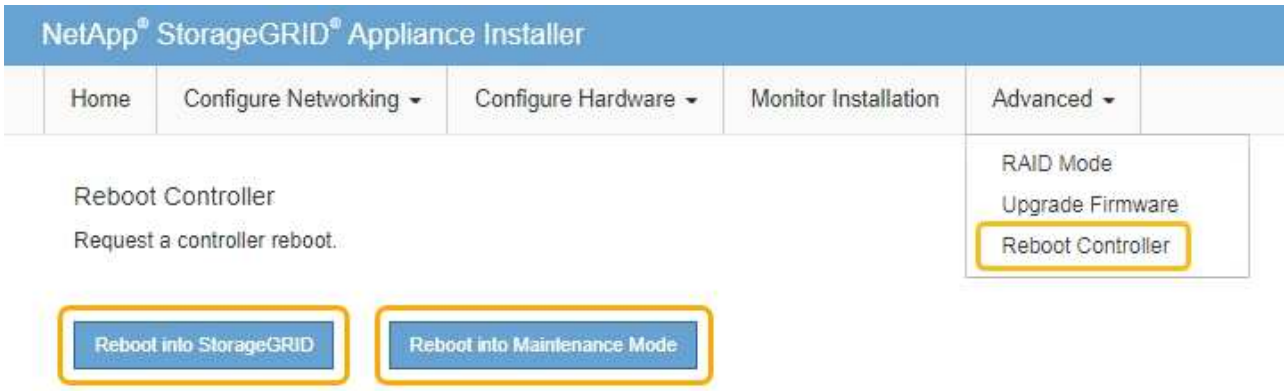
   > NVSRAM은 StorageGRID 어플라이언스에만 적용됩니다. 표준 NVSRAM 다운로드를 사용하지 마십시오.

4. 펌웨어 및 NVSRAM을 업그레이드하려면, _Upgrading SANtricity OS_guide 또는 SANtricity 시스템 관리자 온라인 도움말의 지침을 따르십시오.

   > 업그레이드 파일을 즉시 활성화합니다. 활성화를 지연하지 마십시오.

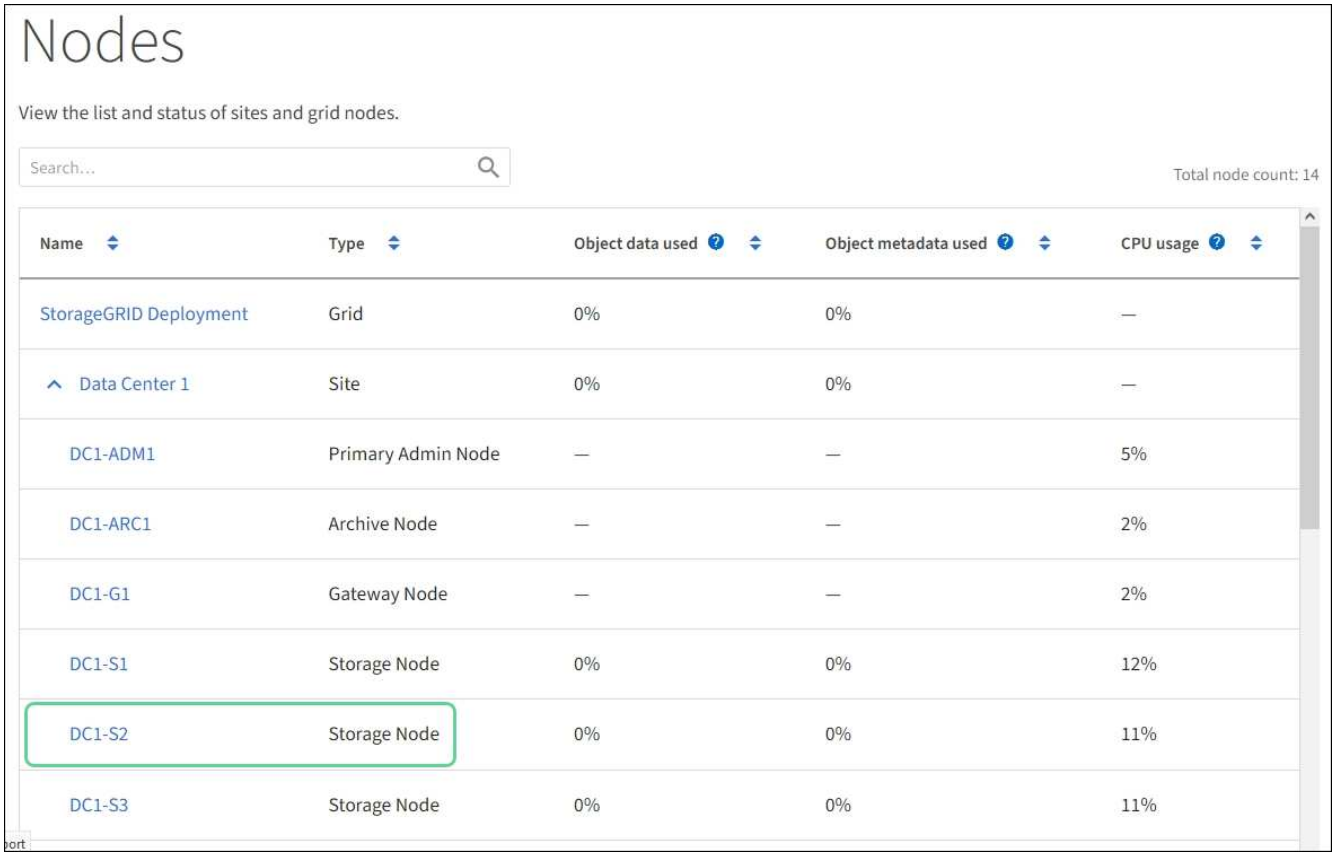
5. 이 절차가 성공적으로 완료되었고 노드가 유지보수 모드일 때 수행할 추가 절차가 있는 경우 지금 수행합니다. 작업을 완료했거나 오류가 발생하여 다시 시작하려면 * 고급 * > * 컨트롤러 재부팅 * 을 선택하고 다음 옵션 중 하나를 선택합니다.

   - StorageGRID * 로 재부팅 * 을 선택합니다
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. 절차 중에 오류가 발생하여 다시 시작하려면 이 옵션을 선택합니다. 노드가 유지보수 모드로 재부팅된 후 장애가 발생한 절차의 적절한 단계에서 다시 시작하십시오.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. 노드 페이지에는 어플라이언스

노드에 대한 정상 상태(노드 이름 왼쪽에 아이콘이 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

"NetApp 상호 운용성 매트릭스 툴"

그리드 관리자를 사용하여 스토리지 컨트롤러의 SANtricity OS를 업그레이드합니다

SANtricity 시스템 관리자를 사용하여 드라이브 펌웨어를 업그레이드합니다

드라이브 펌웨어를 업그레이드하여 최신 기능 및 버그 수정 사항이 모두 있는지 확인합니다.

필요한 것

- 스토리지 어플라이언스 상태가 최적입니다.
- 모든 드라이브가 최적 상태입니다.
- 사용 중인 StorageGRID 버전과 호환되는 최신 버전의 SANtricity 시스템 관리자가 설치되어 있습니다.
- 있습니다 StorageGRID 어플라이언스를 유지보수 모드로 놓았습니다.

> 유지보수 모드는 스토리지 컨트롤러에 대한 연결을 중단하여 모든 I/O 작업을 중지하고 모든 드라이브를 오프라인으로 전환합니다.

> 한 번에 둘 이상의 StorageGRID 어플라이언스에서 드라이브 펌웨어를 업그레이드하지 마십시오. 따라서 배포 모델 및 ILM 정책에 따라 데이터를 사용할 수 없게 될 수 있습니다.

단계

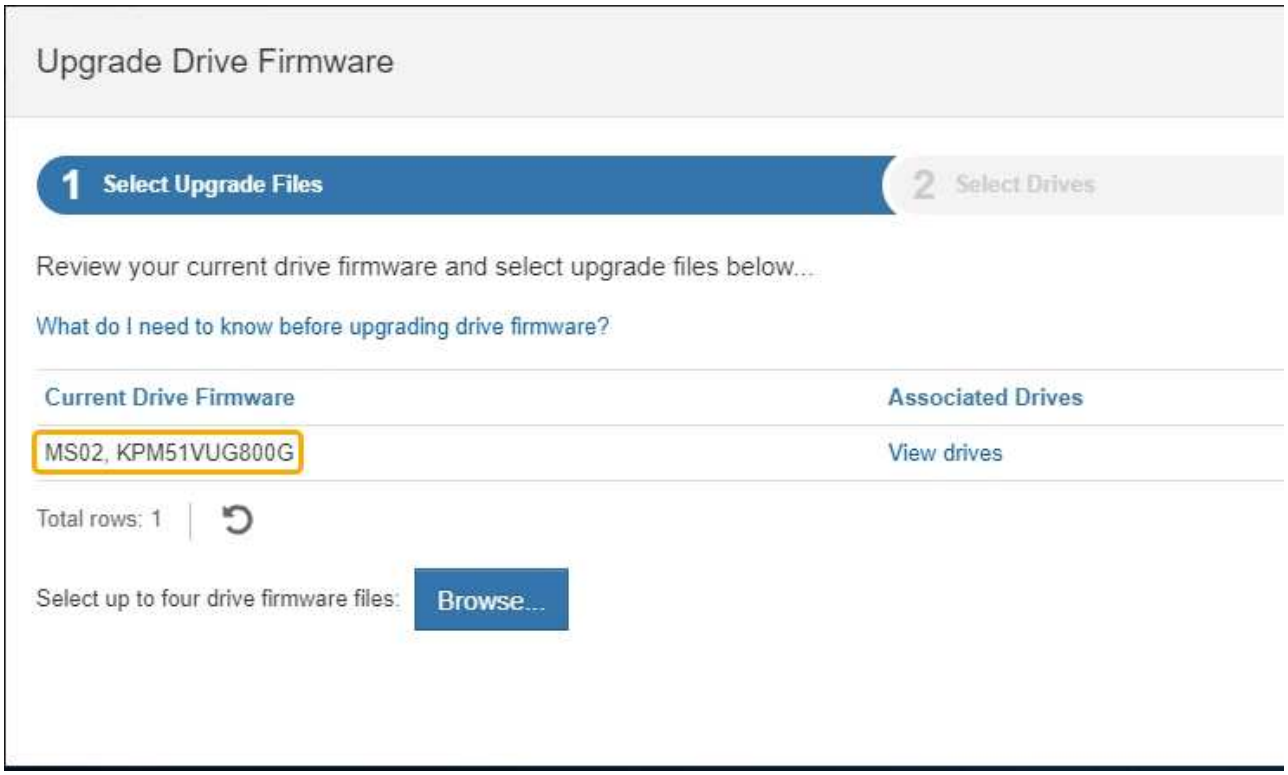
1. 제품이 에 있는지 확인하십시오 유지보수 모드.
2. 다음 방법 중 하나를 사용하여 SANtricity System Manager에 액세스합니다.
   - StorageGRID 어플라이언스 설치 프로그램을 사용하여 * 고급 * > * SANtricity 시스템 관리자 * 를 선택합니다
   - 스토리지 컨트롤러 IP:+(* https://*Storage_Controller_IP**`) 로 이동하여 SANtricity 시스템 관리자를 사용합니다
3. 필요한 경우 SANtricity 시스템 관리자 사용자 이름과 암호를 입력합니다.
4. 스토리지 어플라이언스에 현재 설치된 드라이브 펌웨어 버전을 확인합니다.

   a. SANtricity 시스템 관리자에서 * 지원 * > * 업그레이드 센터 * 를 선택합니다.

   b. 드라이브 펌웨어 업그레이드 에서 * 업그레이드 시작 * 을 선택합니다.

      드라이브 펌웨어 업그레이드에는 현재 설치된 드라이브 펌웨어 파일이 표시됩니다.

   c. Current Drive Firmware(현재 드라이브 펌웨어) 열에서 현재 드라이브 펌웨어 개정 및 드라이브 식별자를 확인합니다.



      이 예에서

      - 드라이브 펌웨어 버전은 * MS02 * 입니다.
      - 드라이브 식별자는 * KPM51VUG800G * 입니다.

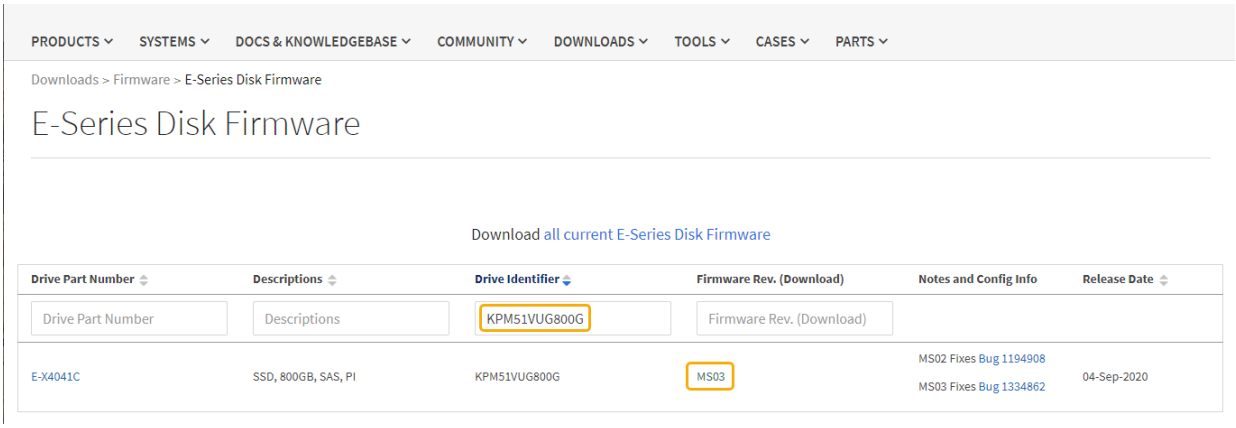
   연결된 드라이브 열에서 * 드라이브 보기 * 를 선택하여 스토리지 어플라이언스에서 해당 드라이브가 설치된 위치를 표시합니다.

   a. Upgrade Drive Firmware(드라이브 펌웨어 업그레이드) 창을 닫습니다.

5. 사용 가능한 드라이브 펌웨어 업그레이드를 다운로드하고 준비합니다.
   a. 드라이브 펌웨어 업그레이드 에서 * NetApp 지원 * 을 선택합니다.
   b. NetApp Support 웹 사이트에서 * Downloads * 탭을 선택한 다음, * E-Series Disk Drive Firmware * 를 선택합니다.

      E-Series 디스크 펌웨어 페이지가 표시됩니다.

   c. 스토리지 어플라이언스에 설치된 각 * 드라이브 식별자 * 를 검색하고 각 드라이브 ID에 최신 펌웨어 버전이 있는지 확인합니다.
      - 펌웨어 개정판이 링크가 아닌 경우 이 드라이브 식별자는 최신 펌웨어 개정판을 가지고 있습니다.
      - 드라이브 식별자에 대해 하나 이상의 드라이브 부품 번호가 나열되면 해당 드라이브에 대해 펌웨어 업그레이드를 사용할 수 있습니다. 펌웨어 파일을 다운로드할 링크를 선택할 수 있습니다.



   d. 최신 펌웨어 개정판이 나열된 경우 펌웨어 개정판에서 링크를 선택합니다 (다운로드) 열을 클릭하여 펌웨어 파일이 포함된 '.zip' 아카이브를 다운로드합니다.
   e. 지원 사이트에서 다운로드한 드라이브 펌웨어 아카이브 파일의 압축을 풉니다.
6. 드라이브 펌웨어 업그레이드를 설치합니다.
   a. SANtricity 시스템 관리자의 드라이브 펌웨어 업그레이드 아래에서 * 업그레이드 시작 * 을 선택합니다.
   b. 찾아보기 * 를 선택하고 Support 사이트에서 다운로드한 새 드라이브 펌웨어 파일을 선택합니다.

      드라이브 펌웨어 파일의 파일 이름은 +D_HUC101212CSS600_30602291_MS01_2800_0002.DLP와 비슷합니다.

      한 번에 하나씩 최대 4개의 드라이브 펌웨어 파일을 선택할 수 있습니다. 둘 이상의 드라이브 펌웨어 파일이 동일한 드라이브와 호환되는 경우 파일 충돌 오류가 발생합니다. 업그레이드에 사용할 드라이브 펌웨어 파일을 결정하고 다른 드라이브 펌웨어 파일을 제거합니다.

   c. 다음 * 을 선택합니다.
      - 드라이브 선택 * 은 선택한 펌웨어 파일로 업그레이드할 수 있는 드라이브를 나열합니다.

        호환되는 드라이브만 나타납니다.

      선택한 드라이브의 펌웨어가 * 제안된 펌웨어 * 에 나타납니다. 이 펌웨어를 변경해야 하는 경우 * Back * 을 선택합니다.

d. Offline (parallel) * upgrade를 선택합니다.

어플라이언스가 유지보수 모드이므로 오프라인 업그레이드 방법을 사용할 수 있습니다. 이 경우 모든 드라이브 및 모든 볼륨에 대해 I/O 작업이 중지됩니다.

> 제품이 유지보수 모드인지 확실하지 않은 경우 작업을 진행하지 마십시오. 오프라인 드라이브 펌웨어 업데이트를 시작하기 전에 어플라이언스를 유지 관리 모드로 전환하지 않으면 데이터가 손실될 수 있습니다.

e. 테이블의 첫 번째 열에서 업그레이드할 드라이브를 선택합니다.

모범 사례는 동일한 모델의 모든 드라이브를 동일한 펌웨어 개정판으로 업그레이드하는 것입니다.

f. 시작 * 을 선택하고 업그레이드를 수행할지 확인합니다.

업그레이드를 중지해야 하는 경우 * Stop * (중지 *)을 선택합니다. 현재 진행 중인 모든 펌웨어 다운로드가 완료되었습니다. 시작되지 않은 모든 펌웨어 다운로드는 취소됩니다.

> 드라이브 펌웨어 업그레이드를 중지하면 데이터가 손실되거나 드라이브를 사용할 수 없게 될 수 있습니다.

g. (선택 사항) 업그레이드된 항목 목록을 보려면 * Save Log * 를 선택합니다.

로그 파일은 브라우저의 다운로드 폴더에 'latest-upgrade-log-timestamp.txt'라는 이름으로 저장됩니다.

업그레이드 절차 중에 다음 오류가 발생하는 경우 적절한 권장 조치를 취하십시오.

- * 할당된 드라이브 실패 *

  이 오류가 발생하는 한 가지 이유는 드라이브에 적절한 서명이 없을 수 있기 때문입니다. 영향을 받는 드라이브가 승인된 드라이브인지 확인합니다. 자세한 내용은 기술 지원 부서에 문의하십시오.

드라이브를 교체할 때 교체 드라이브의 용량이 교체 중인 드라이브의 용량보다 크거나 같은지 확인하십시오.

스토리지 배열이 I/O를 수신하는 동안 오류가 발생한 드라이브를 교체할 수 있습니다

- * 스토리지 배열 확인 *
  - 각 컨트롤러에 IP 주소가 할당되었는지 확인합니다.
  - 컨트롤러에 연결된 모든 케이블이 손상되지 않았는지 확인합니다.
  - 모든 케이블이 단단히 연결되어 있는지 확인합니다.
- * 통합 핫 스페어 드라이브 *

  펌웨어를 업그레이드하기 전에 이 오류 상태를 수정해야 합니다.

- * 불완전한 볼륨 그룹 *

  하나 이상의 볼륨 그룹 또는 디스크 풀이 불완전하면 펌웨어를 업그레이드하기 전에 이 오류 조건을 수정해야 합니다.

- * 현재 모든 볼륨 그룹에서 실행 중인 독점 작업(백그라운드 미디어/패리티 검사 제외) *

  하나 이상의 배타적 작업이 진행 중인 경우 펌웨어를 업그레이드하기 전에 작업을 완료해야 합니다. System Manager를 사용하여 작업 진행률을 모니터링합니다.

- * 볼륨 없음 *

  펌웨어를 업그레이드하기 전에 누락된 볼륨 상태를 수정해야 합니다.

- * 두 컨트롤러 중 하나가 최적 상태 * 가 아닌 다른 상태입니다

  스토리지 어레이 컨트롤러 중 하나에 주의가 필요합니다. 펌웨어를 업그레이드하기 전에 이 상태를 수정해야 합니다.

- * 컨트롤러 오브젝트 그래프 * 간에 스토리지 파티션 정보가 일치하지 않습니다

  컨트롤러의 데이터를 검증하는 동안 오류가 발생했습니다. 이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

- * SPM 데이터베이스 컨트롤러 확인 실패 *

  컨트롤러에서 스토리지 파티션 매핑 데이터베이스 오류가 발생했습니다. 이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

- * 구성 데이터베이스 검증(스토리지 배열의 컨트롤러 버전에서 지원되는 경우) *

  컨트롤러에서 구성 데이터베이스 오류가 발생했습니다. 이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

- * MEL 관련 점검 *

  이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

- * 최근 7일 동안 10개가 넘는 DDE 정보 또는 중요 MEL 이벤트가 보고되었습니다 *

  이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

- * 지난 7일 동안 2개 이상의 2c 페이지 중요 MEL 이벤트가 보고되었습니다 *

  이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

- * 최근 7일 동안 성능이 저하된 드라이브 채널 중요 MEL 이벤트가 2개 이상 보고되었습니다 *

  이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

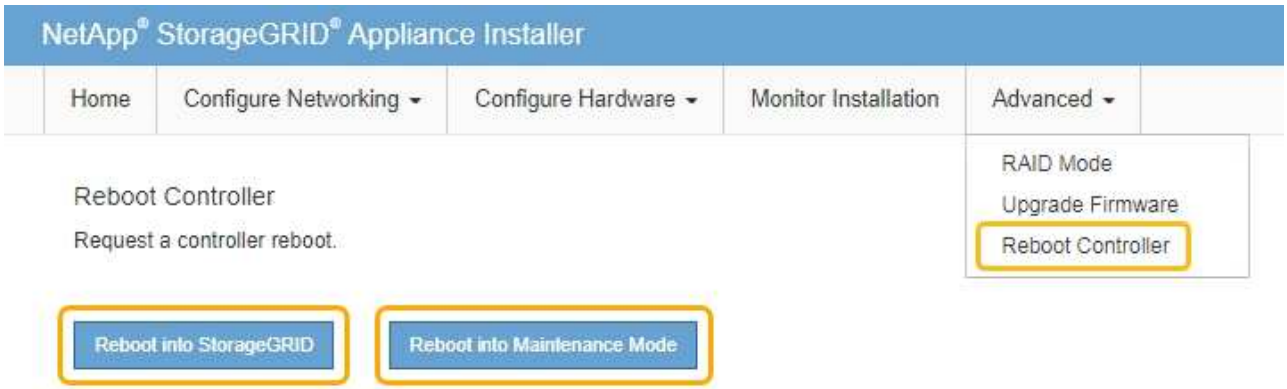
- * 지난 7일 동안 4개 이상의 중요한 MEL 항목 *

  이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

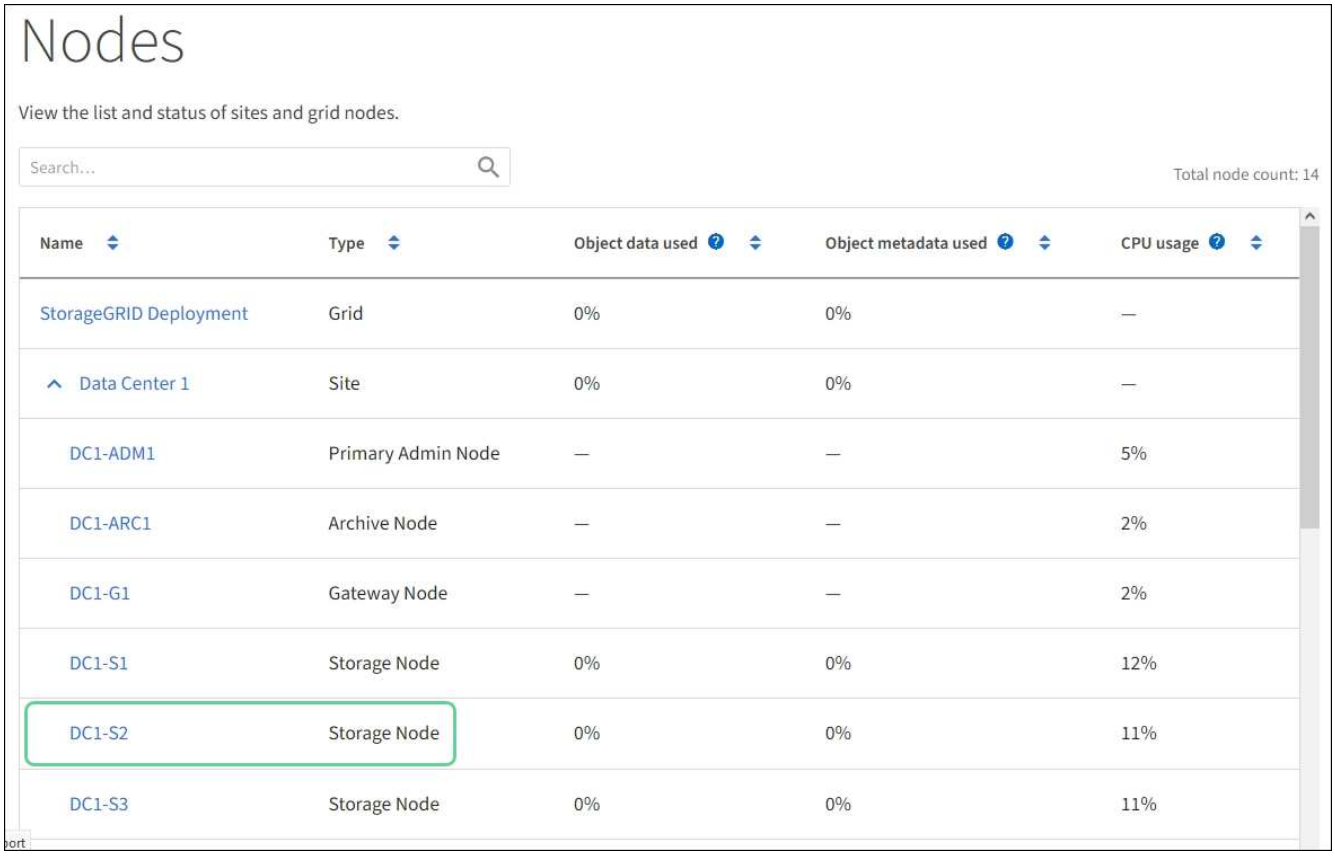
7. 이 절차가 성공적으로 완료되었고 노드가 유지보수 모드일 때 수행할 추가 절차가 있는 경우 지금 수행합니다. 작업을 완료했거나 오류가 발생하여 다시 시작하려면 * 고급 * > * 컨트롤러 재부팅 * 을 선택하고 다음 옵션 중 하나를 선택합니다.

   - StorageGRID * 로 재부팅 * 을 선택합니다

- 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. 절차 중에 오류가 발생하여 다시 시작하려면 이 옵션을 선택합니다. 노드가 유지보수 모드로 재부팅된 후 장애가 발생한 절차의 적절한 단계에서 다시 시작하십시오.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. 노드 페이지에는 어플라이언스 노드에 대한 정상 상태(노드 이름 왼쪽에 아이콘이 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

스토리지 컨트롤러에서 SANtricity OS를 업그레이드합니다

구축된 **SG6060**에 확장 쉘프를 추가합니다

스토리지 용량을 늘리려면 StorageGRID 시스템에 이미 구축된 SG6060 또는 SG6060X에 확장 쉘프를 하나 또는 두 개 추가할 수 있습니다.

필요한 것

- 프로비저닝 암호가 있어야 합니다.
- StorageGRID 11.4 이상을 실행해야 합니다.
- 확장 쉘프와 각 확장 쉘프의 SAS 케이블을 2개 사용합니다.
- 데이터 센터에 확장 쉘프를 추가할 스토리지 어플라이언스를 물리적으로 배치했습니다.

  데이터 센터에서 컨트롤러를 찾습니다

이 작업에 대해

확장 쉘프를 추가하려면 다음 단계를 높은 수준으로 수행해야 합니다.

- 캐비닛 또는 랙에 하드웨어를 설치합니다.
- SG6060 또는 SG6060X를 유지보수 모드로 설정합니다.
- 확장 쉘프를 E2860 컨트롤러 쉘프 또는 다른 확장 쉘프에 연결합니다.
- StorageGRID 어플라이언스 설치 프로그램을 사용하여 확장을 시작합니다
- 새 볼륨이 구성될 때까지 기다립니다.

하나 또는 두 개의 확장 셸프에 대한 절차를 완료하는 데는 어플라이언스 노드당 1시간 이하가 걸립니다. 가동 중지 시간을 최소화하기 위해 다음 단계에서는 SG6060 또는 SG6060X를 유지보수 모드로 설정하기 전에 새 확장 셸프 및 드라이브를 설치하도록 지시합니다. 나머지 단계는 어플라이언스 노드당 약 20~30분 정도 소요됩니다.

단계

1. 캐비닛 또는 랙에 60-드라이브 쉘프를 설치하기 위한 지침을 따릅니다.

   SG6060 및 SG6060X: 캐비닛 또는 랙에 60 드라이브 쉘프를 설치합니다

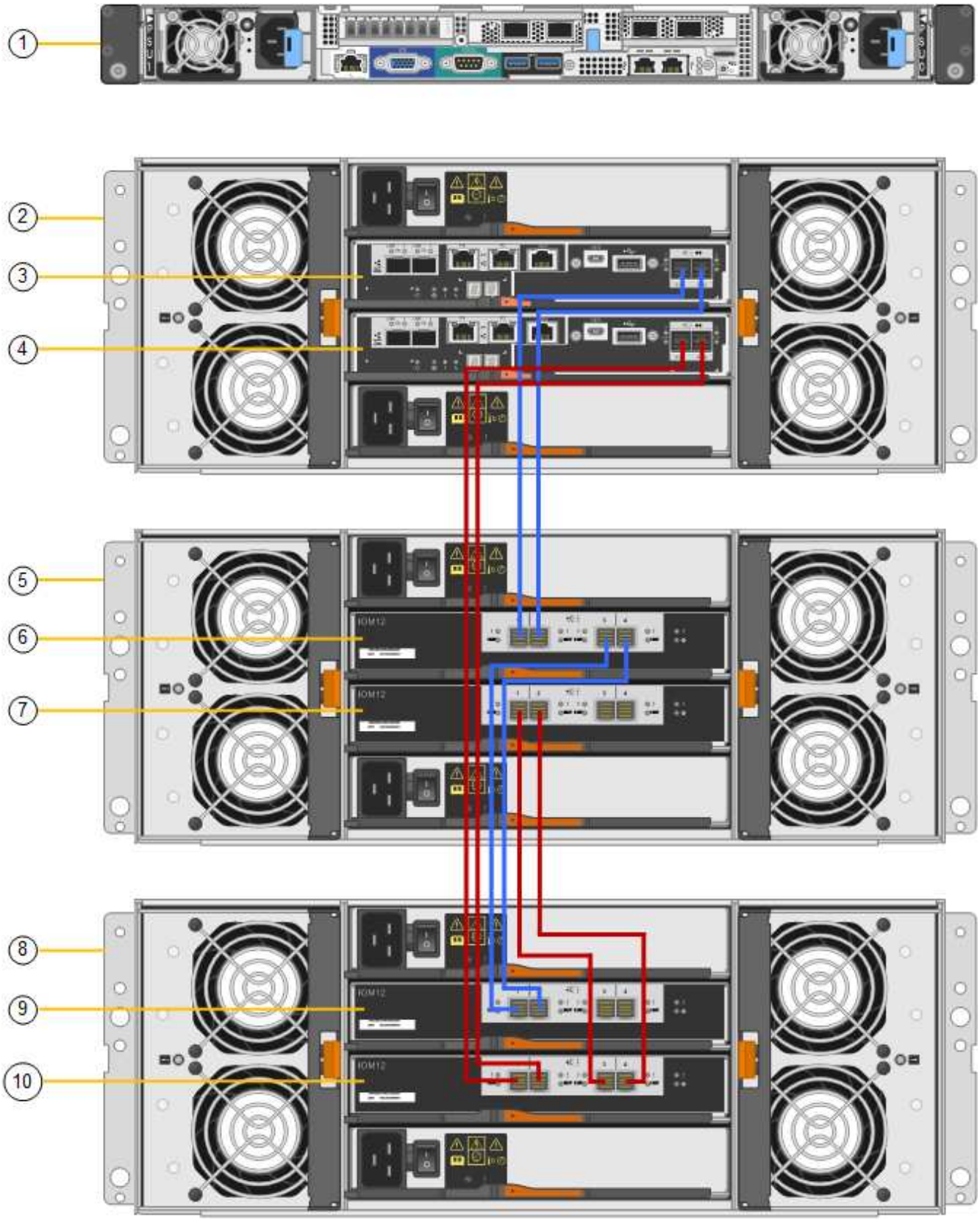
2. 드라이브 설치 지침을 따릅니다.

   SG6060 및 SG6060X: 드라이브를 설치합니다

3. Grid Manager에서 SG6000-CN 컨트롤러를 유지보수 모드로 설정합니다.
4. 다이어그램에 표시된 대로 각 확장 쉘프를 E2860 컨트롤러 쉘프에 연결합니다.

   이 도면에는 2개의 확장 쉘프가 나와 있습니다. IOM A가 하나만 있는 경우 IOM A를 컨트롤러 A에 연결하고 IOM B를 컨트롤러 B에 연결합니다

   SG6060이 표시됩니다. SG6060X의 확장 케이블은 동일합니다.



속성 표시기	설명
1	SG6000-CN

속성 표시기	설명
2	E2860 컨트롤러 쉘프
3	컨트롤러 A
4	컨트롤러 B
5	확장 쉘프 1
6	확장 쉘프 1의 경우 IOM A
7	확장 쉘프 1의 IOM B
8	확장 쉘프 2
9	확장 쉘프 2의 경우 IOM A
10	확장 쉘프 2의 IOM B

5. 전원 코드를 연결하고 확장 셸프에 전원을 공급합니다.
   a. 각 확장 쉘프에 있는 2개의 전원 공급 장치 각각에 전원 코드를 연결합니다.
   b. 각 확장 셸프의 전원 코드 2개를 캐비닛이나 랙에 있는 서로 다른 PDU 2개에 연결합니다.
   c. 각 확장 셸프에 대해 2개의 전원 스위치를 켭니다.
      - 전원을 켜는 동안 전원 스위치를 끄지 마십시오.
      - 확장 선반의 팬은 처음 시작할 때 매우 클 수 있습니다. 시동 중 큰 소음이 정상입니다.
6. StorageGRID 어플라이언스 설치 프로그램의 홈 페이지를 모니터링합니다.

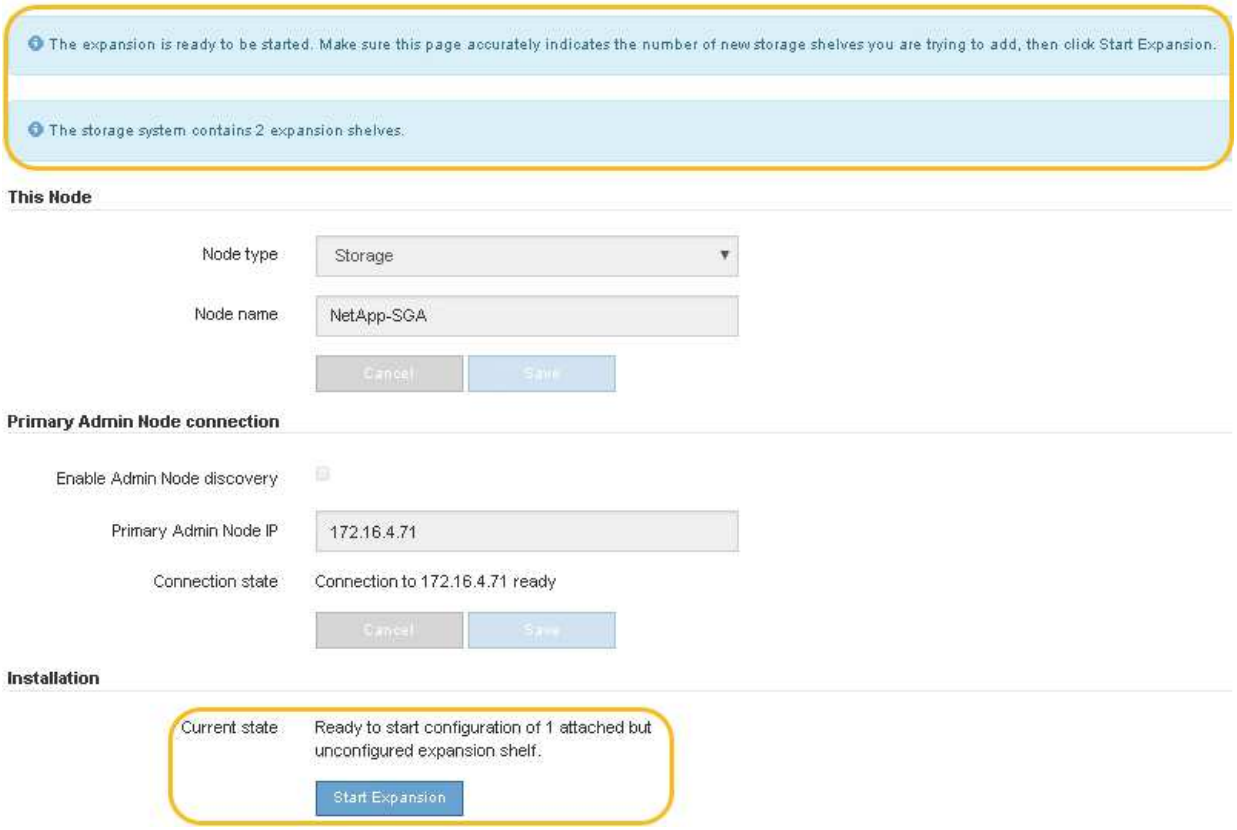
   약 5분 후 확장 셸프의 전원이 꺼지고 시스템에 의해 감지됩니다. 홈 페이지에는 감지된 새 확장 셸프의 수가 표시되고 확장 시작 버튼이 활성화됩니다.

   스크린샷은 다음과 같이 기존 또는 새 확장 셸프 수에 따라 홈 페이지에 표시될 수 있는 메시지의 예를 보여 줍니다.

   - 페이지 상단에 동그라미로 표시된 배너는 감지된 총 확장 셸프 수를 나타냅니다.
     - 배너는 셸프의 구성 및 구축 또는 신규/구성되지 않은 총 확장 셸프 수를 나타냅니다.
     - 확장 셸프가 감지되지 않으면 배너가 나타나지 않습니다.
   - 페이지 하단에 동그라미 표시된 메시지는 확장을 시작할 준비가 되었음을 나타냅니다.
     - 이 메시지는 StorageGRID에서 감지하는 새 확장 쉘프의 수를 나타냅니다. "부착됨"은 선반이 감지되었음을 나타냅니다. "'Unconfigured'"는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 셸프가 새로 추가되었으며 아직 구성되지 않았음을 나타냅니다.

> 이미 구축된 확장 쉘프가 이 메시지에 포함되어 있지 않습니다. 페이지 상단의 배너에 있는 카운트에 포함됩니다.

- 새 확장 쉘프가 감지되지 않으면 메시지가 나타나지 않습니다.



7. 필요한 경우 홈 페이지의 메시지에 설명된 문제를 해결합니다.

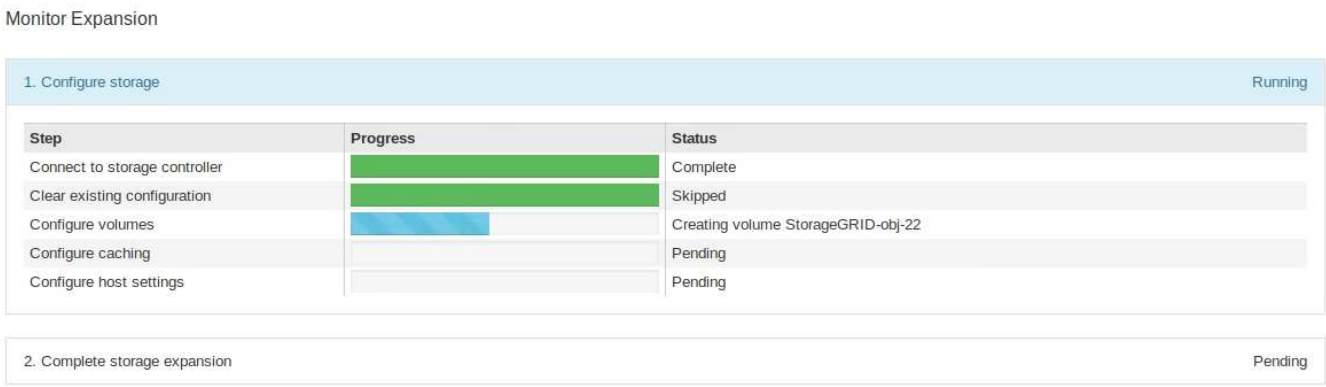
   예를 들어, SANtricity 시스템 관리자를 사용하여 스토리지 하드웨어 문제를 해결할 수 있습니다.

8. 홈 페이지에 표시되는 확장 셸프 수가 추가하려는 확장 셸프 수와 일치하는지 확인합니다.

   > 새 확장 쉘프가 감지되지 않은 경우 케이블이 올바르게 연결되고 전원이 켜져 있는지 확인합니다.

9. * 확장 시작 * 을 클릭하여 확장 쉘프를 구성하고 오브젝트 스토리지에 사용할 수 있도록 합니다.
10. 확장 쉘프 구성의 진행률을 모니터링합니다.

    진행 표시줄은 초기 설치 중에 나타나는 것처럼 웹 페이지에 나타납니다.



구성이 완료되면 어플라이언스가 자동으로 재부팅되어 유지 관리 모드를 종료하고 그리드에 다시 연결됩니다. 이 프로세스는 최대 20분 정도 소요될 수 있습니다.

> 확장 셸프 구성이 실패할 경우 다시 시도하려면 StorageGRID 어플라이언스 설치 프로그램으로 이동하여 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * 유지보수 모드로 재부팅 * 을 선택합니다. 노드가 재부팅된 후 를 재시도하십시오 확장 쉘프 구성.

재부팅이 완료되면 * Tasks * 탭이 다음 스크린샷과 같이 표시됩니다.

11. 어플라이언스 스토리지 노드 및 새 확장 셸프의 상태를 확인합니다.
    a. Grid Manager에서 * nodes * 를 선택하고 어플라이언스 스토리지 노드에 녹색 확인 표시 아이콘이 있는지 확인합니다.

       녹색 확인 표시 아이콘은 활성화된 알림이 없고 노드가 그리드에 연결되어 있음을 의미합니다. 노드 아이콘에 대한 설명은 StorageGRID 모니터링 및 문제 해결 지침을 참조하십시오.

    b. Storage * 탭을 선택하고 추가한 확장 셸프마다 Object Storage 테이블에 16개의 새 오브젝트 저장소가 표시되는지 확인합니다.
    c. 각 새 확장 셸프의 쉘프 상태가 공칭 이고 구성 상태가 구성됨 인지 확인합니다.

관련 정보

박스 포장 풀기(SG6000 및 SG6060X)

SG6060 및 SG6060X: 캐비닛 또는 랙에 60 드라이브 쉘프를 설치합니다

컨트롤러 식별 **LED**를 켜고 끕니다

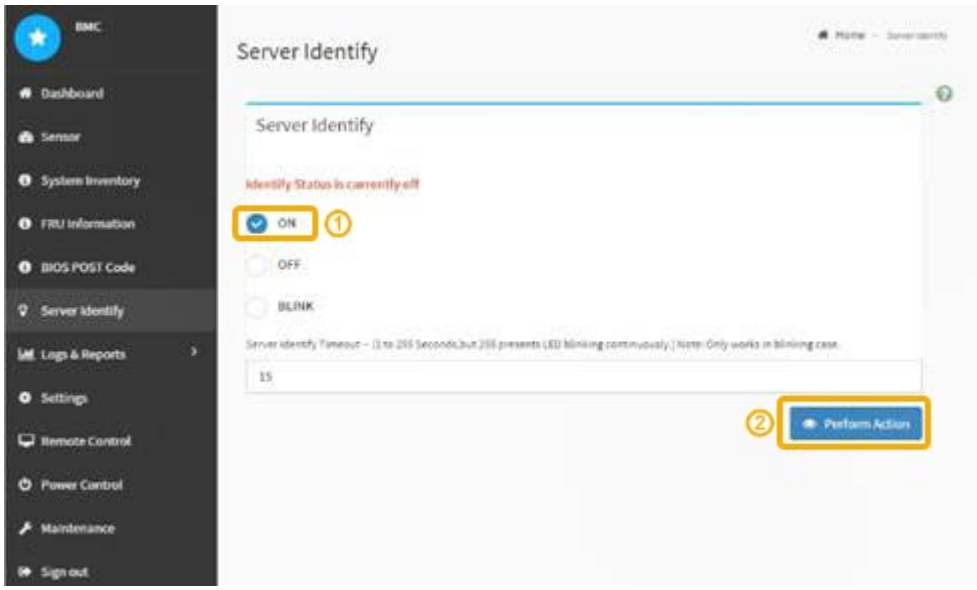
컨트롤러 앞면과 뒷면의 청색 식별 LED를 켜면 데이터 센터에서 제품을 쉽게 찾을 수 있습니다.

필요한 것

식별하려는 컨트롤러의 BMC IP 주소가 있어야 합니다.

단계

1. 컨트롤러 BMC 인터페이스에 액세스합니다.
2. 서버 식별 * 을 선택합니다.
3. On * 을 선택한 다음 * Perform Action * 을 선택합니다.



결과

파란색은 컨트롤러 전면(그림 참조)과 후면에 있는 LED 표시등을 나타냅니다.

베젤이 컨트롤러에 설치되어 있는 경우 전면 식별 LED를 확인하기 어려울 수 있습니다.

작업을 마친 후

컨트롤러 식별 LED를 끄려면:

- 컨트롤러 전면 패널의 식별 LED 스위치를 누릅니다.
- 컨트롤러 BMC 인터페이스에서 * 서버 식별 * 을 선택하고 * 꺼짐 * 을 선택한 다음 * 작업 수행 * 을 선택합니다.

파란색은 컨트롤러 전면과 후면에 있는 LED를 식별합니다.

관련 정보

교체할 Fibre Channel HBA를 확인합니다

데이터 센터에서 컨트롤러를 찾습니다

BMC 인터페이스에 액세스합니다

데이터 센터에서 컨트롤러를 찾습니다

하드웨어 유지보수 또는 업그레이드를 수행할 수 있는 컨트롤러를 찾습니다.

필요한 것

- 유지보수가 필요한 컨트롤러를 확인했습니다.

  (선택 사항) 데이터 센터에서 컨트롤러를 찾으려면 청색 식별 LED를 켭니다.

  컨트롤러 식별 LED를 켜고 끕니다

단계

1. 데이터 센터에서 유지보수가 필요한 컨트롤러를 찾습니다.
   - 컨트롤러 전면 또는 후면에 있는 파란색 식별 LED가 켜져 있는지 확인합니다.

     전면 식별 LED는 컨트롤러 전면 베젤 뒤에 있으며 베젤이 설치되었는지 확인하기 어려울 수 있습니다.

- 각 컨트롤러 전면에 부착된 태그에 일치하는 부품 번호가 있는지 확인합니다.

2. 컨트롤러 전면 베젤이 설치된 경우 전면 패널 컨트롤 및 표시등에 액세스하려면 전면 베젤을 분리합니다.
3. 선택 사항: 컨트롤러를 찾는 데 사용한 경우 청색 식별 LED를 끕니다.
   - 컨트롤러 전면 패널의 식별 LED 스위치를 누릅니다.
   - 컨트롤러 BMC 인터페이스를 사용합니다.

     컨트롤러 식별 LED를 켜고 끕니다

관련 정보

Fibre Channel HBA를 제거합니다

캐비닛 또는 랙에서 SG6000-CN 컨트롤러를 제거합니다

SG6000-CN 컨트롤러를 종료합니다

SG6000에서 스토리지 컨트롤러를 교체합니다

E2800 시리즈 컨트롤러 또는 EF570 컨트롤러는 최적의 상태로 작동하지 않거나 장애가 발생한 경우에 교체해야 할 수 있습니다.

필요한 것

- 교체할 컨트롤러와 부품 번호가 동일한 교체 컨트롤러가 있습니다.
- 컨트롤러에 연결된 각 케이블을 식별하는 라벨이 있습니다.
- ESD 밴드를 가지고 있거나 다른 정전기 방지 예방 조치를 취했습니다.
- 1 십자 드라이버가 있습니다.
- 이중 구성의 컨트롤러 교체를 위한 E-Series 지침이 있습니다.

> 절차가 동일하지 않으므로 E-Series 지침에 따라 StorageGRID 어플라이언스의 컨트롤러를 교체하지 마십시오.

- 데이터 센터에서 컨트롤러를 교체하는 스토리지 어플라이언스를 물리적으로 배치했습니다.

  데이터 센터에서 컨트롤러를 찾습니다

이 작업에 대해

두 가지 방법으로 오류가 발생한 컨트롤러가 있는지 확인할 수 있습니다.

- SANtricity 시스템 관리자의 Recovery Guru에서 컨트롤러를 교체하도록 안내합니다.
- 컨트롤러의 주황색 주의 LED가 켜져 컨트롤러에 장애가 있음을 나타냅니다.

> 쉘프 내의 두 컨트롤러 모두에 주의 LED가 켜져 있는 경우 기술 지원 팀에 지원을 요청하십시오.

어플라이언스에 2개의 스토리지 컨트롤러가 포함되어 있는 경우 다음 조건이 충족될 경우 어플라이언스 전원이 켜져 있고 읽기/쓰기 작업을 수행하는 동안 컨트롤러 중 하나를 교체할 수 있습니다.

- 쉘프 내의 두 번째 컨트롤러가 Optimal(최적) 상태입니다.
- SANtricity 시스템 관리자의 Recovery Guru 세부 정보 영역에 있는 ""제거 확인"" 필드가 "예"로 표시되어 이 구성 요소를 제거해도 안전함을 나타냅니다.

> 가능한 경우 예기치 못한 오류나 고장으로 인한 잠재적인 영향을 최소화하기 위해 이 교체 절차를 위해 어플라이언스를 유지보수 모드로 두십시오.

> 쉘프의 두 번째 컨트롤러가 최적의 상태가 아니거나 Recovery Guru에서 컨트롤러를 제거할 수 없는 경우 기술 지원 부서에 문의하십시오.

컨트롤러를 교체할 때는 원래 컨트롤러에서 배터리를 분리하여 교체 컨트롤러에 설치해야 합니다. 경우에 따라 원래 컨트롤러에서 호스트 인터페이스 카드를 제거하고 교체 컨트롤러에 설치해야 할 수도 있습니다.

> 대부분의 어플라이언스 모델의 스토리지 컨트롤러에는 HIC(호스트 인터페이스 카드)가 포함되지 않습니다.

이 작업은 다음과 같은 부분으로 구성됩니다.

1. 준비
2. 컨트롤러를 오프라인으로 전환합니다
3. 컨트롤러를 제거합니다
4. 배터리를 새 컨트롤러로 이동합니다
5. 필요한 경우 HIC를 새 컨트롤러로 이동합니다
6. 컨트롤러를 교체합니다

준비

단계

1. 새 컨트롤러의 포장을 풀고 정전기가 없는 평평한 표면에 놓습니다.

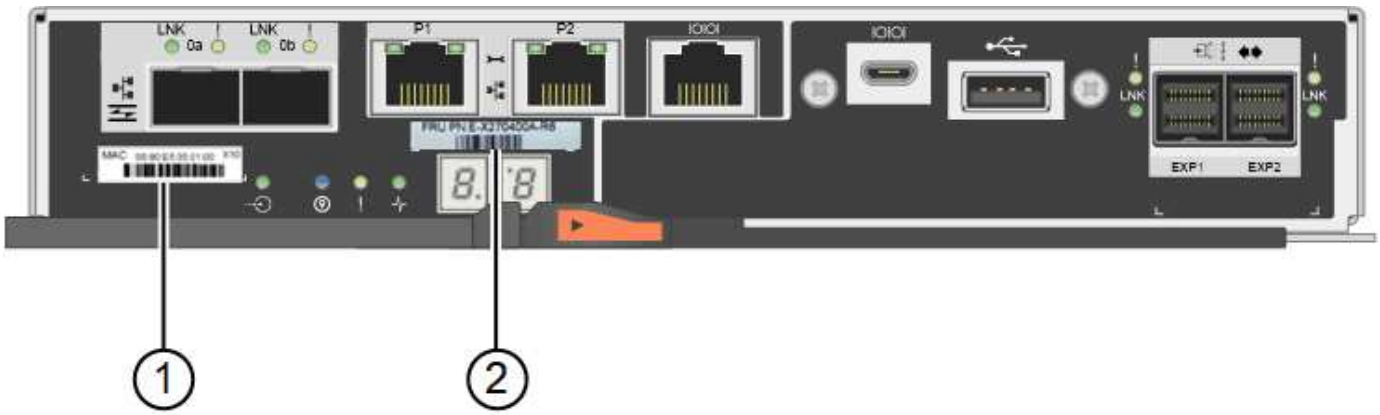
   오류가 발생한 컨트롤러를 배송할 때 사용할 포장재를 보관합니다.

2. 교체 컨트롤러 뒷면에서 MAC 주소 및 FRU 부품 번호 레이블을 찾습니다.

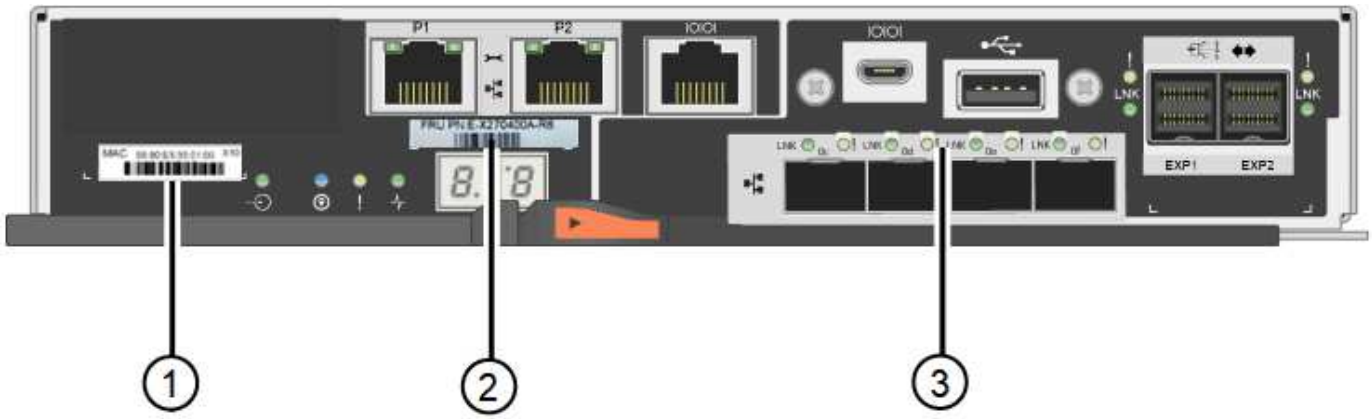
이러한 수치는 E2800A 컨트롤러 및 E2800B 컨트롤러를 보여줍니다. E2800 시리즈 컨트롤러 및 EF570 컨트롤러를

교체하는 절차는 동일합니다.

- E2800A 스토리지 컨트롤러 *



- E2800B 스토리지 컨트롤러 *



라벨	구성 요소	설명
1	MAC 주소	관리 포트 1의 MAC 주소("'E2800A의 P1, E2800B의 0a"). DHCP를 사용하여 원래 컨트롤러의 IP 주소를 얻은 경우 이 주소가 새 컨트롤러에 연결되어 있어야 합니다.
2	FRU 부품 번호입니다	FRU 부품 번호입니다. 이 번호는 현재 설치된 컨트롤러의 교체 부품 번호와 일치해야 합니다.
3	4-포트 HIC	4-포트 HIC(호스트 인터페이스 카드) 교체 작업을 수행할 때 이 카드를 새 컨트롤러로 옮겨야 합니다. • 참고 *: E2800A 컨트롤러에는 HIC가 없습니다.

컨트롤러를 오프라인으로 전환합니다

단계

1. 컨트롤러 제거를 준비합니다. SANtricity 시스템 관리자를 사용하여 다음 단계를 수행합니다.

a. 장애가 발생한 컨트롤러의 교체 부품 번호가 교체 컨트롤러의 FRU 부품 번호와 같은지 확인합니다.

   컨트롤러에 장애가 발생하여 교체해야 하는 경우 Recovery Guru의 세부 정보 영역에 교체 부품 번호가 표시됩니다. 이 번호를 수동으로 찾아야 하는 경우 컨트롤러의 * Base * 탭을 보면 됩니다.

   * 데이터 액세스 및 # 8212; * 두 부품 번호가 동일하지 않은 경우, 이 절차를 시도하지 마십시오.

a. 구성 데이터베이스를 백업합니다.

   컨트롤러를 제거할 때 문제가 발생하면 저장된 파일을 사용하여 구성을 복원할 수 있습니다.

b. 어플라이언스에 대한 지원 데이터를 수집합니다.

   구성 요소를 교체하기 전과 교체 후에 지원 데이터를 수집하면 교체로 문제가 해결되지 않을 경우 기술 지원 부서에 전체 로그 세트를 보낼 수 있습니다.

c. 오프라인 상태에서 교체할 컨트롤러를 가지고 가십시오.

컨트롤러를 분리합니다

단계

1. 제품에서 컨트롤러를 분리합니다.
   a. ESD 밴드를 착용하거나 정전기 방지 조치를 취하십시오.
   b. 케이블에 레이블을 지정한 다음 케이블 및 SFP를 분리합니다.

      성능 저하를 방지하려면 케이블을 비틀거나 접거나 끼거나 밟지 마십시오.

   c. 캠 핸들의 래치를 눌러 제품에서 컨트롤러를 분리한 다음 캠 핸들을 오른쪽으로 엽니다.
   d. 양손과 캠 손잡이를 사용하여 제어기를 제품에서 밀어 꺼냅니다.

      컨트롤러의 무게를 지탱하려면 항상 두 손을 사용하십시오.

   e. 착탈식 덮개가 위를 향하도록 하여 정전기가 없는 평평한 표면에 컨트롤러를 놓습니다.
   f. 단추를 누르고 덮개를 밀어 덮개를 분리합니다.

배터리를 새 컨트롤러로 이동합니다

단계

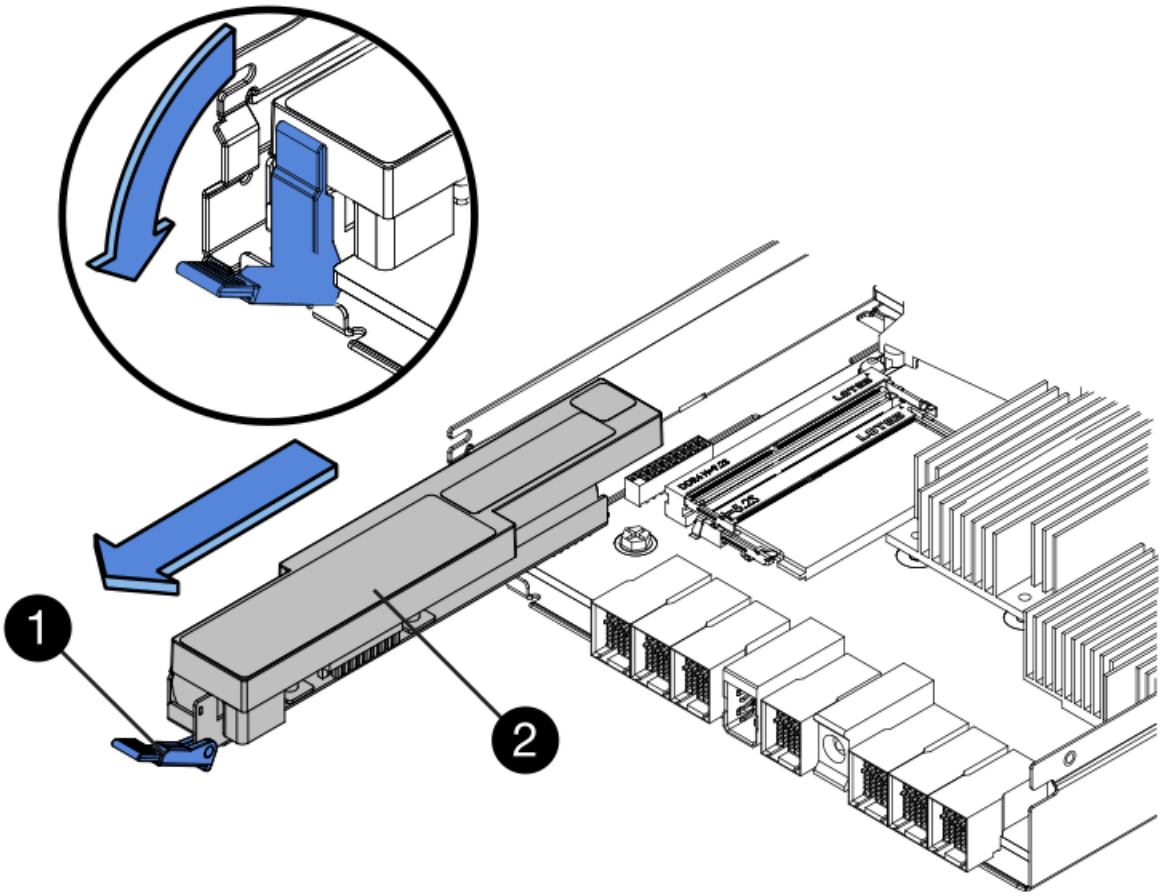
1. 장애가 발생한 컨트롤러에서 배터리를 분리하고 교체 컨트롤러에 설치합니다.
   a. 컨트롤러 내부(배터리와 DIMM 사이)의 녹색 LED가 꺼져 있는지 확인합니다.

      이 녹색 LED가 켜져 있으면 컨트롤러는 여전히 배터리 전원을 사용하고 있습니다. 구성 요소를 제거하기 전에 이 LED가 꺼질 때까지 기다려야 합니다.

항목	설명
1	내부 캐시 활성 LED
2	배터리

b. 배터리의 파란색 분리 래치를 찾습니다.

c. 분리 래치를 아래로 눌러 배터리를 분리합니다.



항목	설명
1	배터리 분리 래치
2	배터리

d. 배터리를 들어 올려 컨트롤러에서 꺼냅니다.

e. 교체용 컨트롤러에서 덮개를 분리합니다.

f. 교체용 컨트롤러의 방향을 조정하여 배터리 슬롯이 사용자를 향하도록 합니다.

g. 배터리를 약간 아래쪽으로 비스듬히 컨트롤러에 삽입합니다.

   배터리 전면의 금속 플랜지를 컨트롤러 하단의 슬롯에 삽입하고 배터리 상단을 컨트롤러 왼쪽의 작은 정렬 핀 아래에 밀어 넣어야 합니다.

h. 배터리 래치를 위로 이동하여 배터리를 고정합니다.

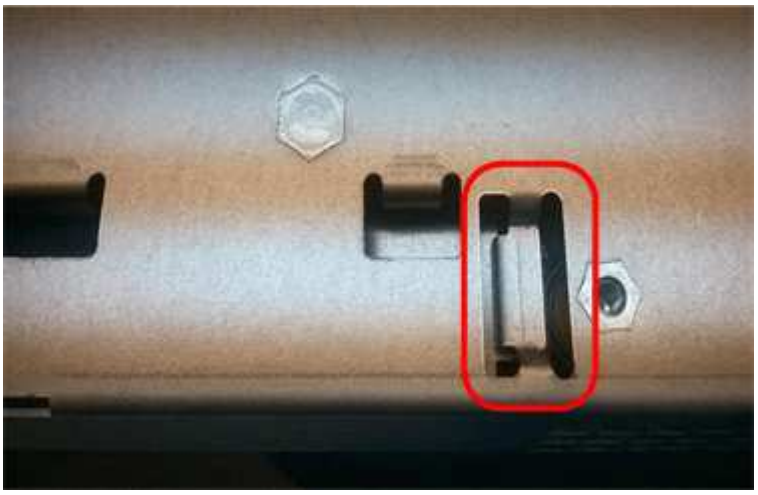
   래치가 제자리에 고정되면 래치 하단이 섀시의 금속 슬롯에 후크됩니다.

i. 컨트롤러를 뒤집어 배터리가 올바르게 설치되었는지 확인합니다.

> * 하드웨어 손상 가능성 * — 배터리 전면의 금속 플랜지가 컨트롤러의 슬롯에 완전히 삽입되어야 합니다(첫 번째 그림 참조). 배터리가 올바르게 설치되지 않은 경우(두 번째 그림 참조) 금속 플랜지가 컨트롤러 보드에 닿으면 손상이 발생할 수 있습니다.

- * 정답입니다.- 배터리의 금속 플랜지가 컨트롤러의 슬롯에 완전히 삽입됩니다. *

- * 잘못됨 — 배터리의 금속 플랜지가 컨트롤러의 슬롯에 삽입되지 않음: *



2. 컨트롤러 덮개를 장착합니다.

필요한 경우 **HIC**를 새 컨트롤러로 이동합니다

단계

1. 장애 컨트롤러에 HIC(호스트 인터페이스 카드)가 포함된 경우 장애가 발생한 컨트롤러에서 교체 컨트롤러로 HIC를 이동합니다.

   E2800B 컨트롤러에만 별도의 HIC가 사용됩니다. HIC는 메인 컨트롤러 보드에 장착되며 SPF 커넥터 2개를 포함합니다.

   > 이 절차의 그림에서는 2-포트 HIC를 보여 줍니다. 컨트롤러의 HIC는 포트 수가 다를 수 있습니다.

2. 컨트롤러에 HIC(E2800A)가 없는 경우 컨트롤러 덮개를 교체합니다. 컨트롤러에 HIC(E2800B)가 있는 경우 로

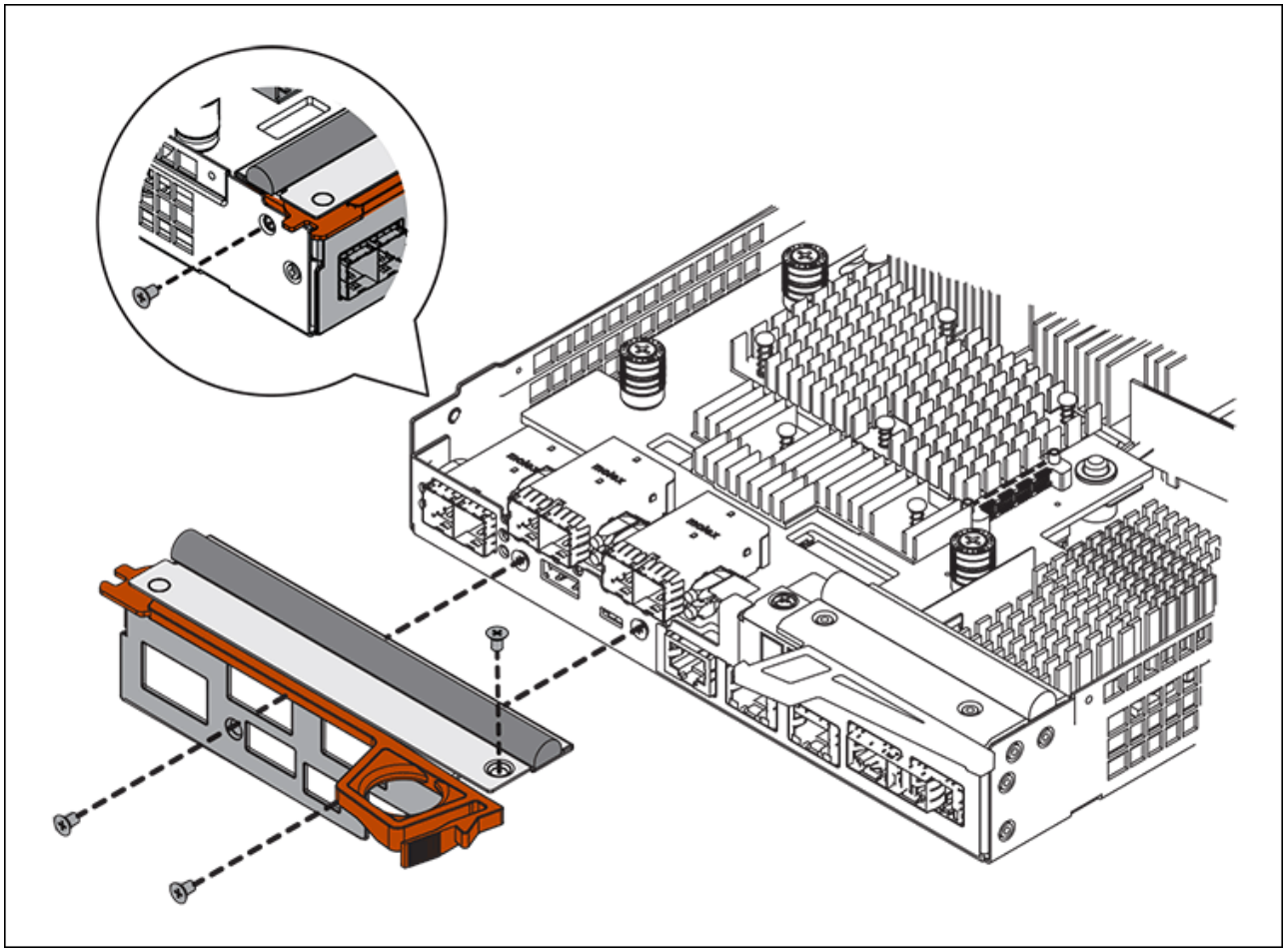
이동합니다 HIC를 장애 컨트롤러에서 교체 컨트롤러로 이동합니다.

a. HIC가 장착된 경우 HIC를 장애가 발생한 컨트롤러에서 교체 컨트롤러로 이동합니다.

b. HIC에서 모든 SFP를 제거합니다.

c. 1 십자 드라이버를 사용하여 HIC 페이스플레이트를 컨트롤러에 연결하는 나사를 제거합니다.

나사는 상단에 1개, 측면에 1개, 전면에 2개 등 4개가 있습니다.

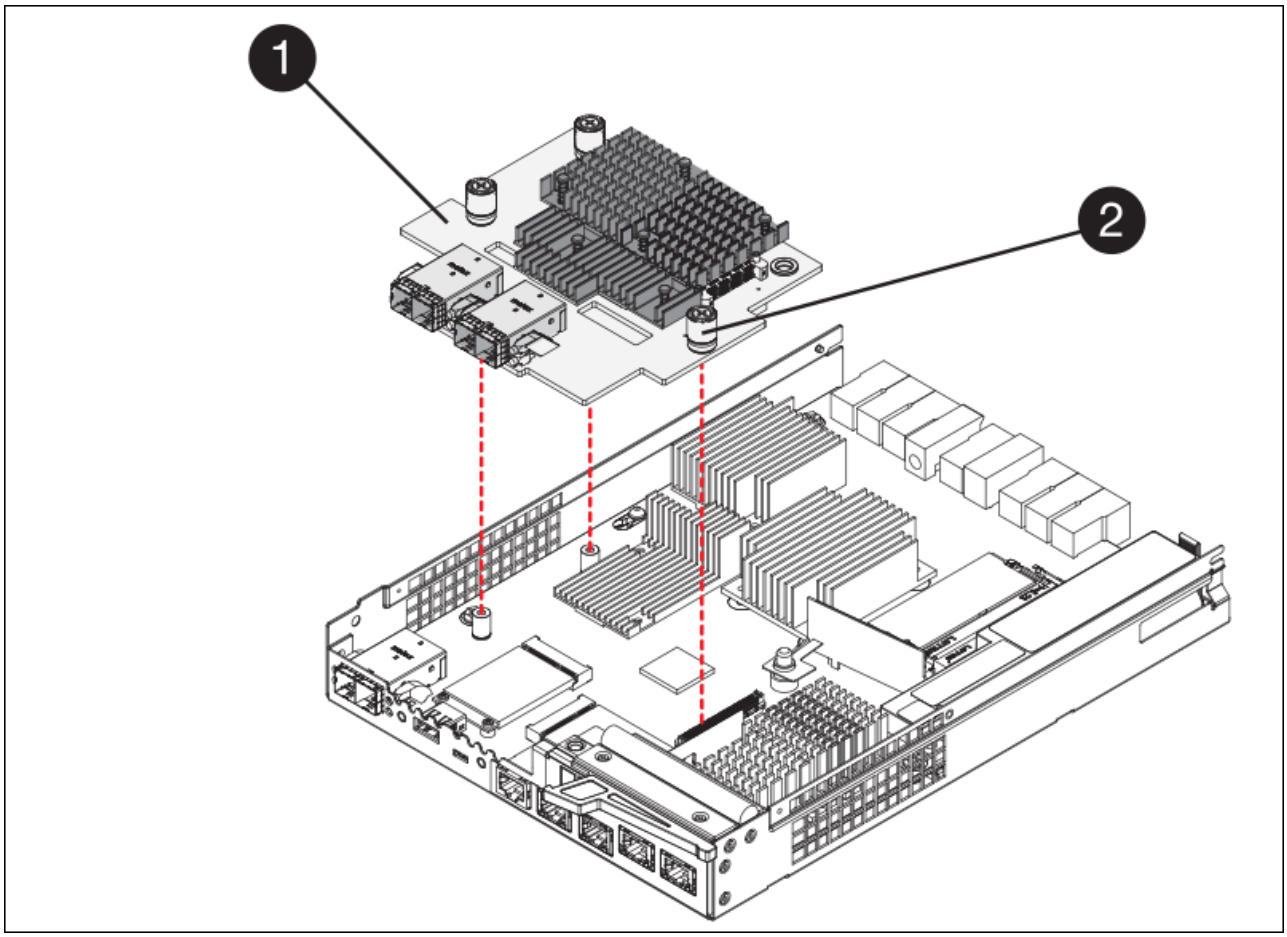


d. HIC 페이스플레이트를 탈거하십시오.

e. 손가락이나 십자 드라이버를 사용하여 HIC를 컨트롤러 카드에 고정하는 세 개의 나비 나사를 풉니다.

f. 카드를 들어 올리고 다시 밀어 컨트롤러 카드에서 HIC를 조심스럽게 분리합니다.

HIC 하단 또는 컨트롤러 카드 상단에 있는 구성 요소가 긁히거나 범프되지 않도록 주의하십시오.



라벨	설명
1	호스트 인터페이스 카드
2	나비 나사

g. HIC를 정전기가 없는 표면에 놓습니다.

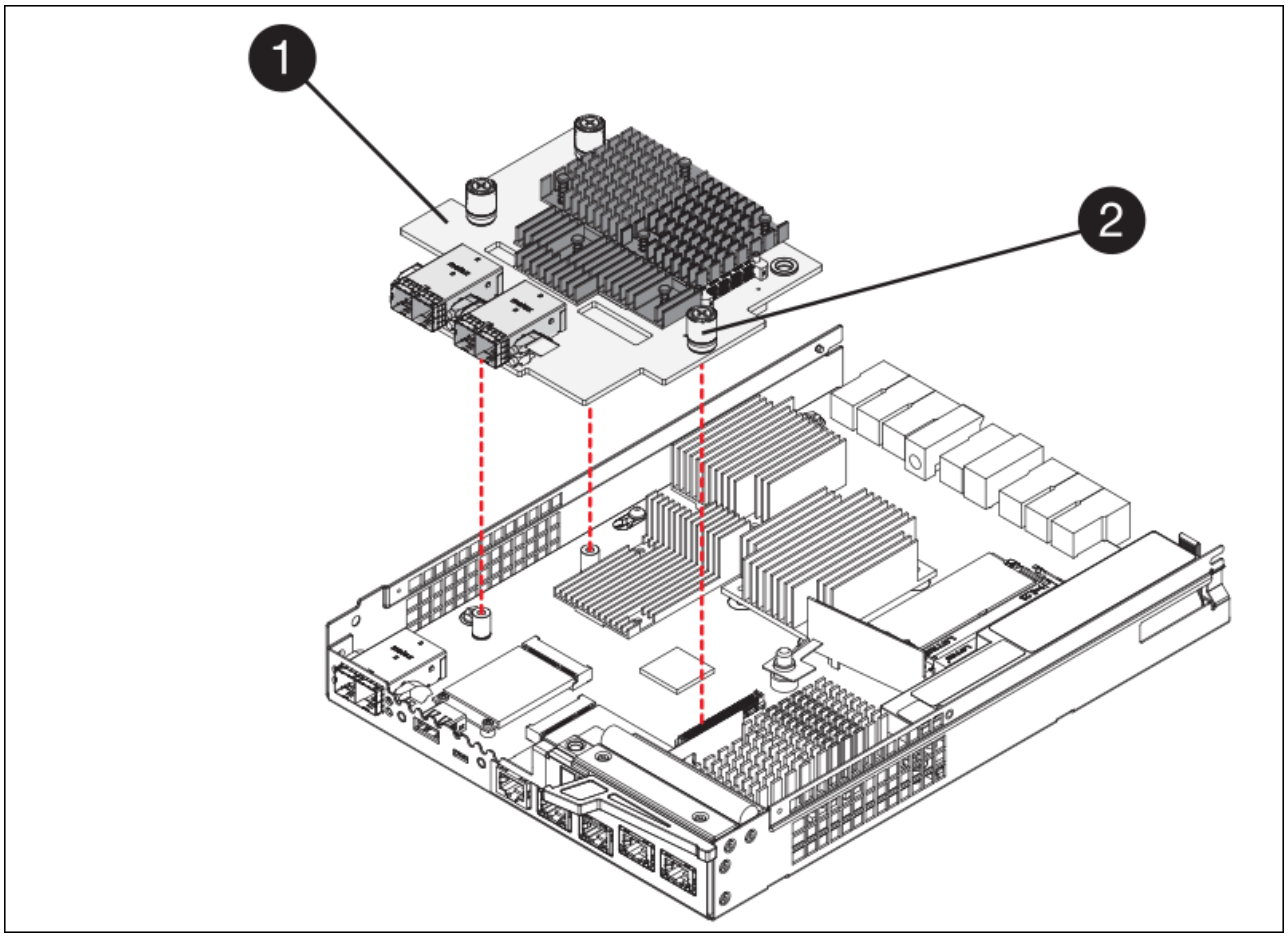
h. 1 Phillips 드라이버를 사용하여 블랭크 페이스 플레이트를 교체 컨트롤러에 연결하는 나사 4개를 분리하고 전면판을 분리하십시오.

i. HIC의 3개의 나비 나사를 교체 컨트롤러의 해당 구멍에 맞추고 HIC 아래쪽에 있는 커넥터를 컨트롤러 카드의 HIC 인터페이스 커넥터와 맞춥니다.

   HIC 하단 또는 컨트롤러 카드 상단에 있는 구성 요소가 긁히거나 범프되지 않도록 주의하십시오.

j. HIC를 조심스럽게 제자리로 내리고 HIC 커넥터를 가볍게 눌러 HIC 커넥터를 장착합니다.

> * 장비 손상 가능성 * — HIC와 나비 나사 사이의 컨트롤러 LED에 골드 리본 커넥터가 끼이지 않도록 매우 조심하십시오.

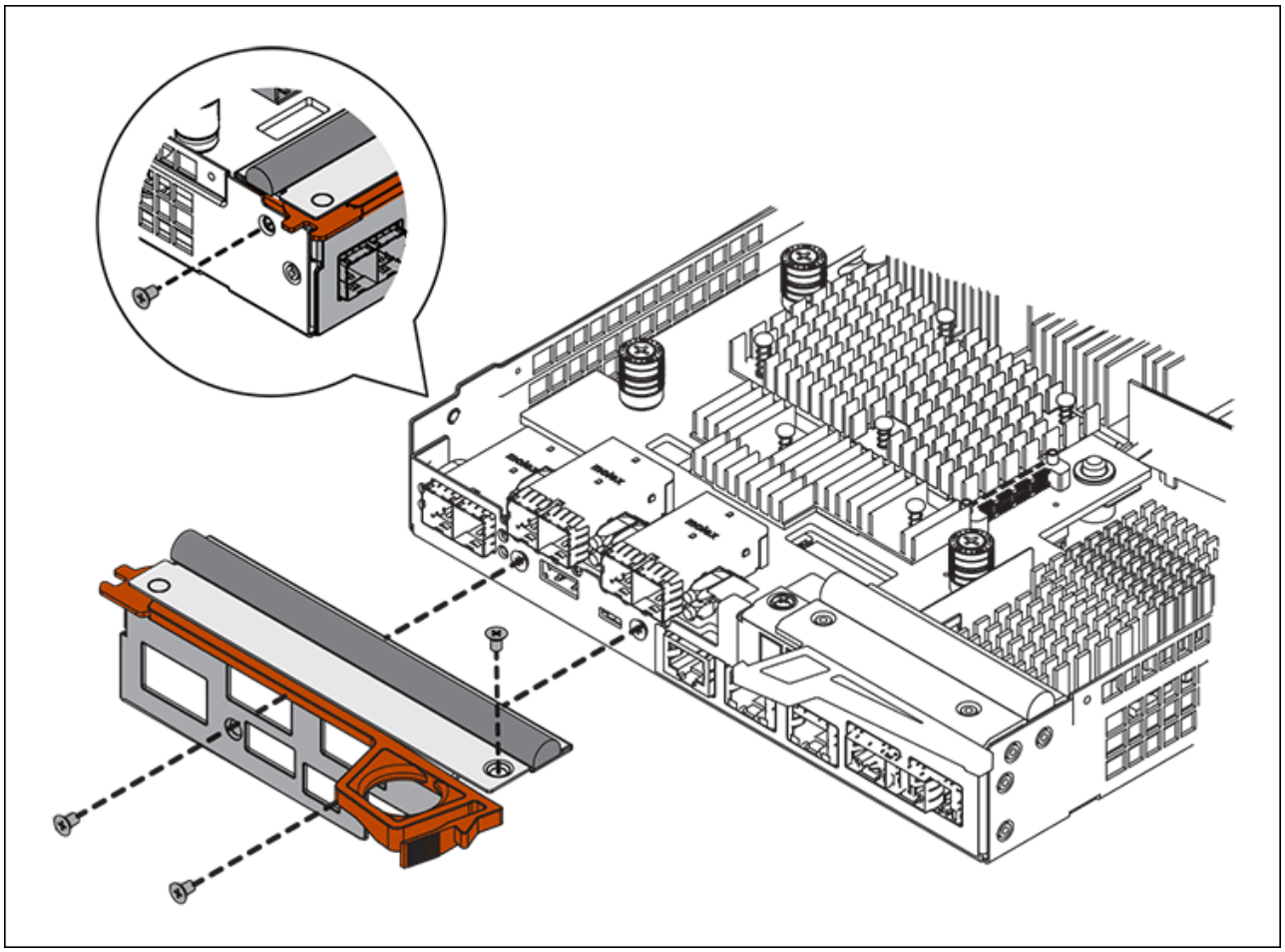


라벨	설명
1	호스트 인터페이스 카드
2	나비 나사

a. HIC 나비 나사를 손으로 조입니다.

   드라이버를 사용하지 마십시오. 또는 나사를 너무 세게 조일 수 있습니다.

b. 1 십자 드라이버를 사용하여 원래 컨트롤러에서 제거한 HIC 면판을 4개의 나사로 새 컨트롤러에 부착합니다.



c. 제거된 SFP를 HIC에 다시 설치합니다.

컨트롤러를 교체합니다

단계

1. 교체 컨트롤러를 제품에 설치합니다.
   a. 이동식 덮개가 아래를 향하도록 컨트롤러를 뒤집습니다.
   b. 캠 손잡이를 열린 상태에서 컨트롤러를 제품 안으로 끝까지 밀어 넣습니다.
   c. 캠 핸들을 왼쪽으로 이동하여 컨트롤러를 제자리에 고정합니다.
   d. 케이블 및 SFP를 교체합니다.
   e. 원래 컨트롤러가 IP 주소에 DHCP를 사용한 경우 교체 컨트롤러 후면의 레이블에 있는 MAC 주소를 찾습니다. 제거한 컨트롤러의 DNS/네트워크 및 IP 주소를 대체 컨트롤러의 MAC 주소와 연관시킬 것을 네트워크 관리자에게 요청합니다.

   > 원래 컨트롤러가 IP 주소에 DHCP를 사용하지 않은 경우 새 컨트롤러는 제거한 컨트롤러의 IP 주소를 채택합니다.

2. SANtricity 시스템 관리자를 사용하여 컨트롤러를 온라인 상태로 전환합니다.
   a. 하드웨어 * 를 선택합니다.
   b. 그래픽에 드라이브가 표시되면 * Show back of shelf * 를 선택합니다.

c. 온라인으로 설정하려는 컨트롤러를 선택합니다.

d. 상황에 맞는 메뉴에서 * 온라인 위치 * 를 선택하고 작업을 수행할지 확인합니다.

e. 7세그먼트 디스플레이에 99 상태가 표시되는지 확인합니다.

3. 새 컨트롤러가 최적의 상태인지 확인하고 지원 데이터를 수집합니다.

부품을 교체한 후 키트와 함께 제공된 RMA 지침에 따라 오류가 발생한 부품을 NetApp에 반환합니다. 를 참조하십시오 "부품 반품 및 앰프, 교체" 페이지를 참조하십시오.

관련 정보

"NetApp E-Series 시스템 문서 사이트"

스토리지 컨트롤러 쉘프의 하드웨어 구성요소를 교체합니다

하드웨어 문제가 발생할 경우 스토리지 컨트롤러 쉘프에 있는 구성 요소를 교체해야 할 수 있습니다.

필요한 것

- E-Series 하드웨어 교체 절차가 있습니다.
- 데이터 센터의 스토리지 쉘프 하드웨어 구성요소를 교체할 스토리지 어플라이언스를 물리적으로 배치했습니다.

  데이터 센터에서 컨트롤러를 찾습니다

이 작업에 대해

저장 장치 컨트롤러의 전지를 교체하려면 저장 장치 컨트롤러 교체에 관한 지침을 참조하십시오. 이 지침은 제품에서 컨트롤러를 분리하고, 컨트롤러에서 배터리를 분리하고, 배터리를 설치하고, 컨트롤러를 교체하는 방법을 설명합니다.

컨트롤러 쉘프의 다른 현장 교체 장치(FRU)에 대한 지침을 보려면 시스템 유지 관리를 위한 E-Series 절차를 참조하십시오.

FRU	지침을 참조하십시오
배터리	StorageGRID(다음 지침): 스토리지 컨트롤러 교체
드라이브	E-Series: • 드라이브 교체(60 드라이브) • 드라이브 교체(12 드라이브 또는 24 드라이브)
전원 캐니스터	E-Series 를 참조하십시오 • 전원 캐니스터 교체(60 드라이브) • 전원 공급 장치 교체(12 드라이브 또는 24 드라이브)
팬 캐니스터(60 드라이브 쉘프만)	E-Series: 팬 캐니스터 교체(60 드라이브)

FRU	지침을 참조하십시오
드라이브 드로어(60-드라이브 쉘프만)	E-Series: 드라이브 드로어 교체(60 드라이브)

관련 정보

"NetApp E-Series 시스템 문서 사이트"

스토리지 컨트롤러를 교체합니다

옵션 **60-**드라이브 확장 쉘프로 하드웨어 구성요소 교체

확장 쉘프에 있는 입출력 모듈, 전원 공급 장치 또는 팬을 교체해야 할 수 있습니다.

필요한 것

- E-Series 하드웨어 교체 절차가 있습니다.
- 데이터 센터의 확장 셸프 하드웨어 구성 요소를 교체하는 스토리지 어플라이언스를 물리적으로 배치했습니다.

  데이터 센터에서 컨트롤러를 찾습니다

이 작업에 대해

60-드라이브 확장 쉘프로 IOM(입력/출력 모듈)을 교체하려면 스토리지 컨트롤러 교체에 대한 지침을 참조하십시오.

60-드라이브 확장 쉘프의 전원 공급 장치 또는 팬을 교체하려면 E-Series의 60-드라이브 하드웨어 유지보수 절차를 참조하십시오.

FRU	에 대한 **E-Series** 지침을 참조하십시오
입력/출력 모듈(IOM)	IOM 교체
전원 캐니스터	전원 캐니스터 교체(60 드라이브)
팬 캐니스터	팬 캐니스터 교체(60 드라이브)

SG6000-CN 컨트롤러를 종료합니다

SG6000-CN 컨트롤러를 종료하여 하드웨어 유지 관리를 수행합니다.

필요한 것

데이터 센터의 유지 관리가 필요한 SG6000-CN 컨트롤러를 물리적으로 배치했습니다. 을 참조하십시오 데이터 센터에서 컨트롤러를 찾습니다.

이 작업에 대해

서비스 중단을 방지하려면 서비스 중단 기간이 허용되는 예약된 유지 관리 기간 동안 컨트롤러를 종료하거나 시작하기 전에 다른 모든 스토리지 노드가 그리드에 연결되어 있는지 확인하십시오. 에 대한 정보를 참조하십시오 노드 연결 상태를 모니터링합니다.

개체의 복사본을 하나만 만드는 ILM 규칙을 사용한 적이 있는 경우에는 예약된 유지 관리 기간 동안 컨트롤러를 종료해야 합니다. 그렇지 않으면 이 절차 중에 해당 개체에 대한 액세스가 일시적으로 끊어질 수 있습니다. 을 참조하십시오 "정보 수명 주기 관리를 통해 개체 관리".

단계

1. SG6000-CN 컨트롤러를 종료합니다.

   아래에 지정된 명령을 입력하여 컨트롤러 종료를 제어해야 합니다. 불필요한 경고를 방지하고, 전체 로그를 사용하고, 서비스 중단을 방지하기 위해 가능하면 제어된 종료를 수행하는 것이 좋습니다.

   a. 그리드 노드에 아직 로그인하지 않은 경우 PuTTY 또는 다른 ssh 클라이언트를 사용하여 로그인합니다.
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

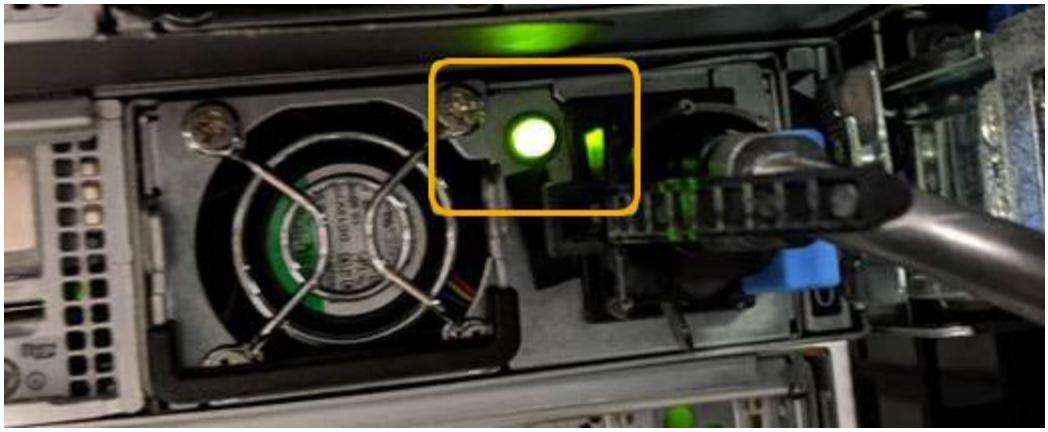
   b. SG6000-CN 컨트롤러를 종료합니다.

```
shutdown -h now
```

   이 명령을 완료하는 데 최대 10분이 걸릴 수 있습니다.

2. 다음 방법 중 하나를 사용하여 SG6000-CN 컨트롤러의 전원이 꺼져 있는지 확인합니다.
   - 컨트롤러 전면에 있는 파란색 전원 LED를 확인하여 꺼져 있는지 확인합니다.

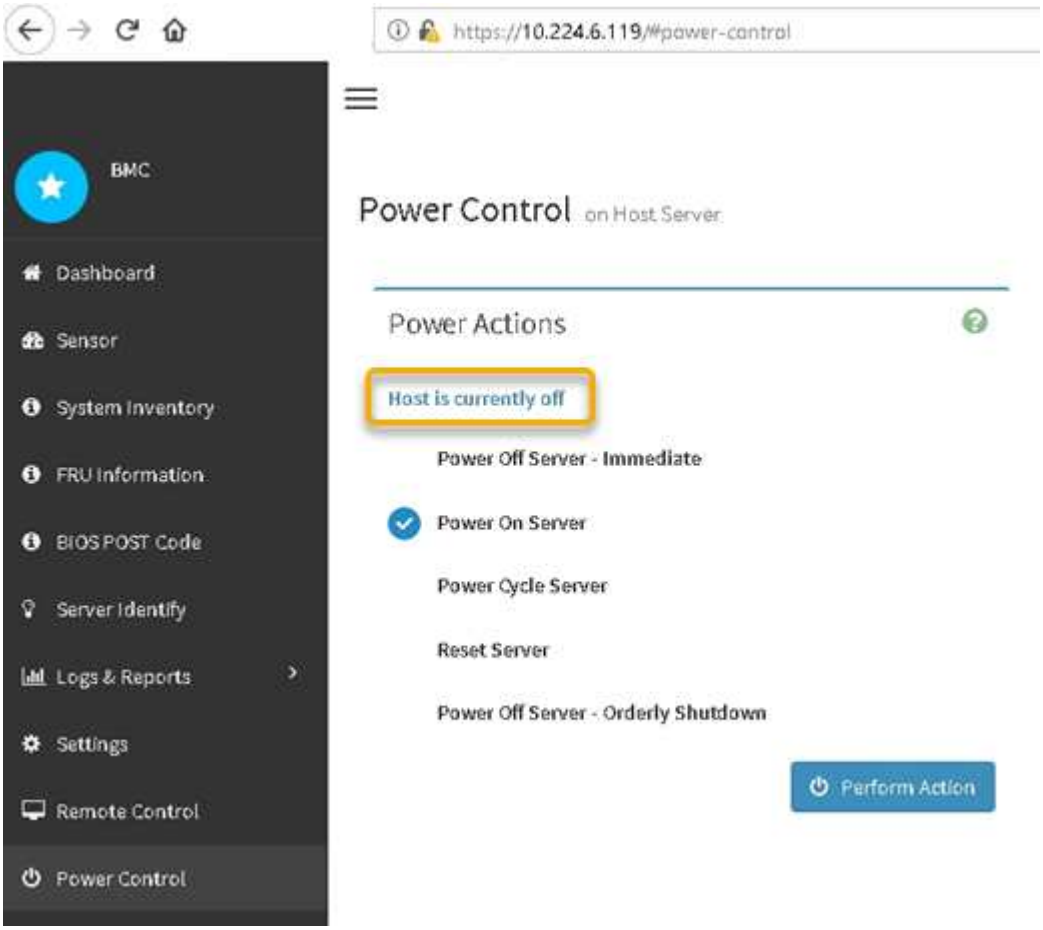
   - 컨트롤러 후면에 있는 두 전원 공급 장치의 녹색 LED를 살펴보고 정상 속도로 깜박이는지 확인합니다(초당 약 1회 깜박임).



- 컨트롤러 BMC 인터페이스 사용:
  i. 컨트롤러 BMC 인터페이스에 액세스합니다.

     BMC 인터페이스에 액세스합니다

  ii. 전원 제어 * 를 선택합니다.
  iii. 전원 작업에서 호스트가 현재 꺼져 있음을 나타내는지 확인합니다.



관련 정보

캐비닛 또는 랙에서 SG6000-CN 컨트롤러를 제거합니다

SG6000-CN 컨트롤러의 전원을 켜고 작동을 확인합니다

유지 관리를 완료한 후 컨트롤러 전원을 켭니다.

필요한 것

- 캐비닛이나 랙에 컨트롤러를 설치하고 데이터 및 전원 케이블을 연결했습니다.

  캐비닛 또는 랙에 SG6000-CN 컨트롤러를 다시 설치합니다

- 데이터 센터에서 물리적으로 컨트롤러를 찾은 경우

  데이터 센터에서 컨트롤러를 찾습니다

단계

1. SG6000-CN 컨트롤러의 전원을 켜고 다음 방법 중 하나를 사용하여 컨트롤러 LED 및 부팅 코드를 모니터링합니다.

   - 컨트롤러 전면에 있는 전원 스위치를 누릅니다.

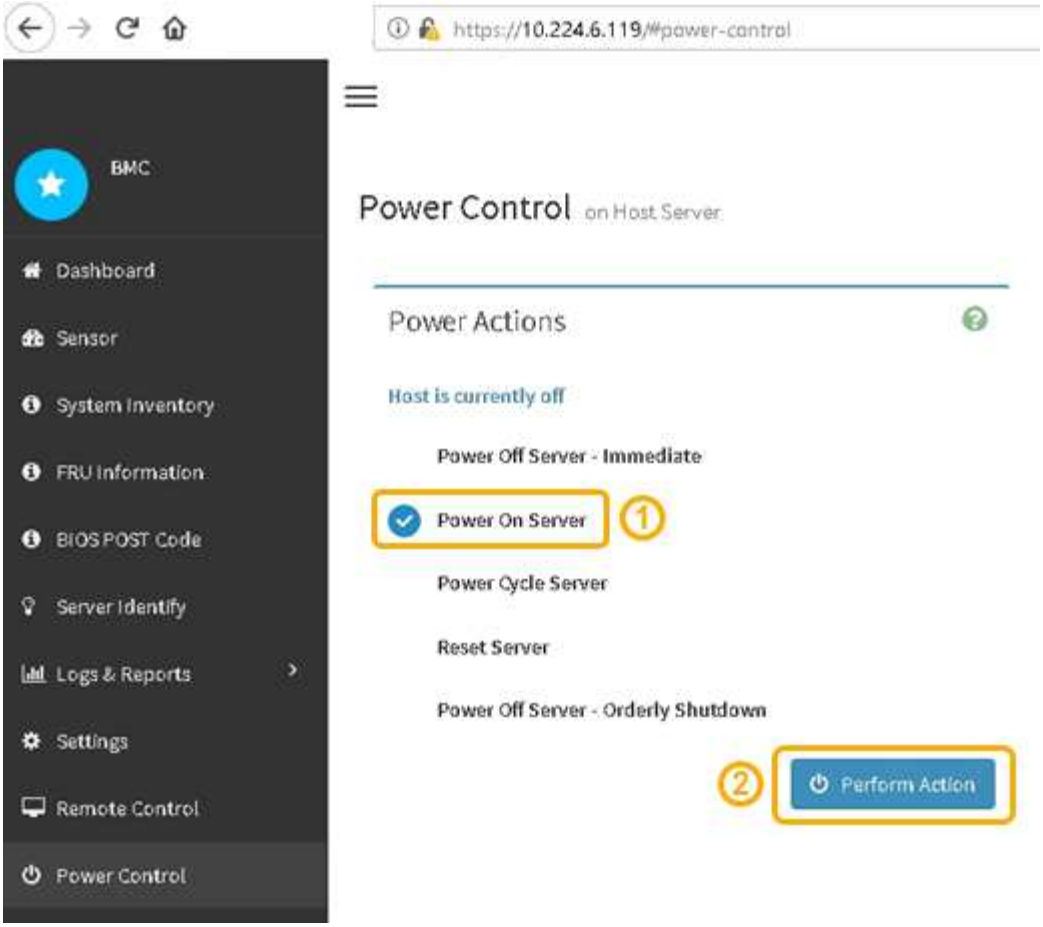
   - 컨트롤러 BMC 인터페이스 사용:

     i. 컨트롤러 BMC 인터페이스에 액세스합니다.

     BMC 인터페이스에 액세스합니다

     ii. 전원 제어 * 를 선택합니다.

     iii. Power On Server * 를 선택한 다음 * Perform Action * 을 선택합니다.



BMC 인터페이스를 사용하여 시작 상태를 모니터링합니다.

2. 어플라이언스 컨트롤러가 그리드 관리자에 표시되고 경고가 표시되지 않는지 확인합니다.

   컨트롤러가 그리드 관리자에 표시되는 데 최대 20분이 걸릴 수 있습니다.

3. 새 SG6000-CN 컨트롤러가 완전히 작동하는지 확인합니다.

   a. PuTTY 또는 다른 ssh 클라이언트를 사용하여 그리드 노드에 로그인합니다.

      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      iii. 루트로 전환하려면 다음 명령을 입력합니다

      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

   b. 다음 명령을 입력하고 예상 출력을 반환하는지 확인합니다. + "cat/sys/class/fc_host/ * /port_state

      예상 출력:

```
Online
Online
Online
Online
```

예상 결과가 반환되지 않으면 기술 지원 부서에 문의하십시오.

c. 다음 명령을 입력하고 예상 출력을 반환하는지 확인합니다. + "cat/sys/class/fc_host/ * /speed

예상 출력:

```
16 Gbit
16 Gbit
16 Gbit
16 Gbit
```

+
예상 결과가 반환되지 않으면 기술 지원 부서에 문의하십시오.

a. 그리드 관리자의 노드 페이지에서 어플라이언스 노드가 그리드에 연결되어 있고 경고가 없는지 확인합니다.

> 이 어플라이언스에 녹색 아이콘이 없으면 다른 어플라이언스 노드를 오프라인으로 전환하지 마십시오.

4. 선택 사항: 앞면 베젤이 분리된 경우 설치합니다.

관련 정보

SG6000-CN 컨트롤러의 상태 표시등 및 단추를 봅니다

SG6000 스토리지 컨트롤러의 부팅 상태 코드를 봅니다

SG6000-CN 컨트롤러를 교체합니다

SG6000-CN 컨트롤러가 최적의 상태로 작동하지 않거나 오류가 발생한 경우 교체해야 할 수 있습니다.

필요한 것

- 교체할 컨트롤러와 부품 번호가 동일한 교체 컨트롤러가 있습니다.
- 컨트롤러에 연결된 각 케이블을 식별하는 라벨이 있습니다.
- 데이터 센터에서 물리적으로 교체할 컨트롤러를 가지고 있습니다.

  데이터 센터에서 컨트롤러를 찾습니다

이 작업에 대해

SG6000-CN 컨트롤러를 교체할 때 어플라이언스 스토리지 노드에 액세스할 수 없습니다. SG6000-CN 컨트롤러가

충분히 작동하는 경우 이 절차를 시작할 때 제어된 종료를 수행할 수 있습니다.

> StorageGRID 소프트웨어를 설치하기 전에 컨트롤러를 교체하는 경우 이 절차를 완료한 후 즉시 StorageGRID 어플라이언스 설치 프로그램에 액세스하지 못할 수 있습니다. 어플라이언스와 동일한 서브넷에 있는 다른 호스트에서 StorageGRID 어플라이언스 설치 프로그램에 액세스할 수 있지만 다른 서브넷에 있는 호스트에서는 액세스할 수 없습니다. 이 조건은 15분 내에 해결되어야 하며(원래 컨트롤러의 ARP 캐시 항목이 시간 초과될 때), 또는 로컬 라우터 또는 게이트웨이에서 수동으로 이전의 ARP 캐시 항목을 삭제하여 즉시 조건을 지울 수 있습니다.

단계

1. 어플라이언스의 현재 구성을 표시하고 기록하십시오.
   a. 교체할 어플라이언스에 로그인합니다.
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
   b. 입력: **`run-host-command ipmitool lan print`** 어플라이언스의 현재 BMC 구성을 표시합니다.
2. SG6000-CN 컨트롤러가 제어된 종료를 허용하기 위해 충분히 작동하는 경우 SG6000-CN 컨트롤러를 종료합니다.

   SG6000-CN 컨트롤러를 종료합니다
3. 이 StorageGRID 어플라이언스의 네트워크 인터페이스 중 DHCP를 사용하도록 구성된 경우 교체 어플라이언스의 MAC 주소를 참조하도록 DHCP 서버의 영구 DHCP 임대 할당을 업데이트해야 할 수 있습니다. 업데이트는 어플라이언스에 예상 IP 주소가 할당되도록 합니다.
   a. SG6000-CN 컨트롤러 전면에서 MAC 주소 레이블을 찾아 관리 네트워크 포트의 MAC 주소를 확인합니다.

      > MAC 주소 레이블에는 BMC 관리 포트의 MAC 주소가 나열됩니다.
      >
      > 관리 네트워크 포트의 MAC 주소를 확인하려면 레이블의 16진수에 * 2 * 를 추가해야 합니다. 예를 들어 레이블의 MAC 주소가 * 09 * 로 끝나는 경우 관리 포트의 MAC 주소는 * 0B * 로 끝납니다. 레이블의 MAC 주소가 * (*y*) FF * 로 끝나는 경우 관리 포트의 MAC 주소는 * (*y*+1) 01 * 로 끝납니다. Windows에서 계산기를 열고, Programmer 모드로 설정하고, Hex를 선택하고, MAC 주소를 입력한 다음, * + 2 = * 를 입력하여 이 계산을 쉽게 수행할 수 있습니다.
   b. 제거한 컨트롤러의 DNS/네트워크 및 IP 주소를 대체 컨트롤러의 MAC 주소와 연관시킬 것을 네트워크 관리자에게 요청합니다.

      > 교체 컨트롤러에 전원을 켜기 전에 원래 컨트롤러의 모든 IP 주소가 업데이트되었는지 확인해야 합니다. 그렇지 않으면 컨트롤러가 부팅될 때 새 DHCP IP 주소를 가져오며 StorageGRID에 다시 연결되지 않을 수 있습니다. 이 단계는 컨트롤러에 연결된 모든 StorageGRID 네트워크에 적용됩니다.

> 원래 컨트롤러가 정적 IP 주소를 사용하는 경우 새 컨트롤러는 제거된 컨트롤러의 IP 주소를 자동으로 채택합니다.

4. SG6000-CN 컨트롤러 분리 및 교체:
   a. 케이블에 레이블을 지정한 다음 케이블과 모든 SFP+ 또는 SFP28 트랜시버를 분리합니다.

      > 성능 저하를 방지하려면 케이블을 비틀거나 접거나 끼거나 밟지 마십시오.

   b. 캐비닛 또는 랙에서 장애가 발생한 컨트롤러를 분리합니다.
   c. 캐비닛 또는 랙에 교체용 컨트롤러를 설치합니다.
   d. 케이블 및 SFP+ 또는 SFP28 트랜시버를 교체합니다.
   e. 컨트롤러 전원을 켜고 컨트롤러 LED 및 부팅 코드를 모니터링합니다.
5. 컨트롤러를 교체한 어플라이언스에서 KMS(키 관리 서버)를 사용하여 데이터를 암호화한 경우 노드를 그리드에 가입하기 전에 추가 구성이 필요할 수 있습니다. 노드가 그리드에 자동으로 연결되지 않는 경우, 이러한 구성 설정이 새 컨트롤러로 전송되었는지 확인하고 필요한 구성이 없는 설정을 수동으로 구성합니다.
   - "StorageGRID 연결을 구성합니다"
   - "어플라이언스에 대한 노드 암호화를 구성합니다"
6. 교체한 컨트롤러를 사용하여 어플라이언스에 로그인합니다.
   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.
7. 어플라이언스에 대한 BMC 네트워크 연결을 복구합니다. 두 가지 옵션이 있습니다.
   - 고정 IP, 넷마스크 및 게이트웨이를 사용합니다
   - DHCP를 사용하여 IP, 넷마스크 및 게이트웨이를 얻습니다
     i. 정적 IP, 넷마스크 및 게이트웨이를 사용하도록 BMC 구성을 복원하려면 다음 명령을 입력합니다.

```
run-host-command ipmitool lan set 1 ipsrc static

run-host-command ipmitool lan set 1 ipaddr Appliance_IP

run-host-command ipmitool lan set 1 netmask Netmask_IP

run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```

     i. DHCP를 사용하여 IP, 넷마스크 및 게이트웨이를 가져오도록 BMC 구성을 복원하려면 다음 명령을 입력합니다.

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```

8. BMC 네트워크 연결을 복원한 후 BMC 인터페이스에 연결하여 추가 사용자 정의 BMC 구성을 감사하고 복원합니다. 예를 들어, SNMP 트랩 대상 및 e-메일 알림에 대한 설정을 확인해야 합니다. 을 참조하십시오 "BMC 인터페이스를 구성합니다".

9. 어플라이언스 노드가 그리드 관리자에 표시되고 경고가 나타나지 않는지 확인합니다.

관련 정보

SG6000-CN: 캐비닛 또는 랙에 설치합니다

SG6000-CN 컨트롤러의 상태 표시등 및 단추를 봅니다

SG6000-CN 컨트롤러의 부팅 코드를 봅니다

SG6000-CN 컨트롤러의 전원 공급 장치 중 하나 또는 둘 다를 교체합니다

SG6000-CN 컨트롤러에는 이중화를 위한 2개의 전원 공급 장치가 있습니다. 전원 공급 장치 중 하나에 장애가 발생하면 가능한 한 빨리 교체해야 컴퓨팅 컨트롤러에 중복 전원이 공급되는지 확인할 수 있습니다. 컨트롤러에서 작동하는 두 전원 공급 장치의 모델 및 와트는 동일해야 합니다.

필요한 것

- 교체할 전원 공급 장치가 있는 컨트롤러의 데이터 센터에서 물리적 위치를 확인했습니다.

  데이터 센터에서 컨트롤러 찾기

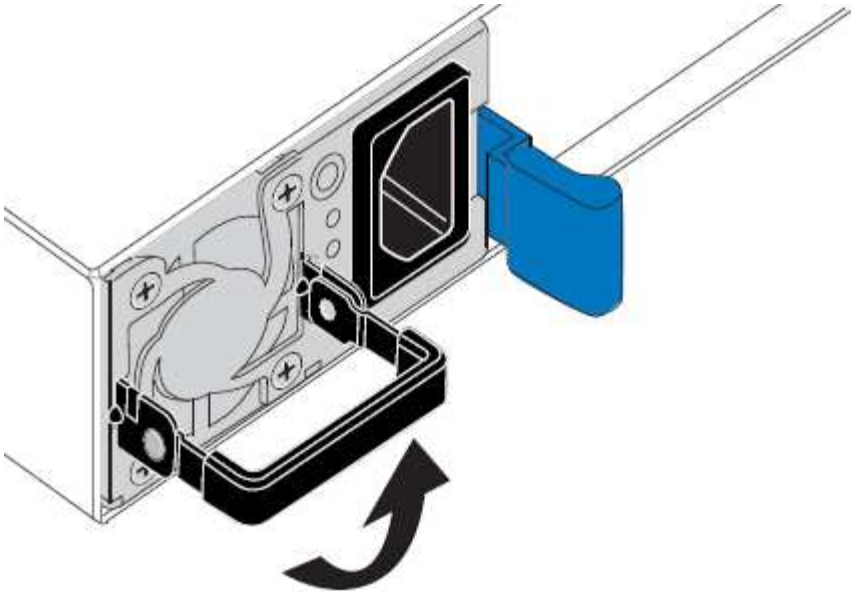
- 하나의 전원 공급 장치만 교체하는 경우:
  - 교체 전원 공급 장치의 포장을 풀고 교체할 전원 공급 장치와 동일한 모델 및 와트인지 확인했습니다.
  - 다른 전원 공급 장치가 설치되어 실행 중인지 확인했습니다.
- 두 전원 공급 장치를 동시에 교체하는 경우:
  - 교체 전원 공급 장치의 포장을 풀고 동일한 모델 및 와트인지 확인했습니다.

이 작업에 대해

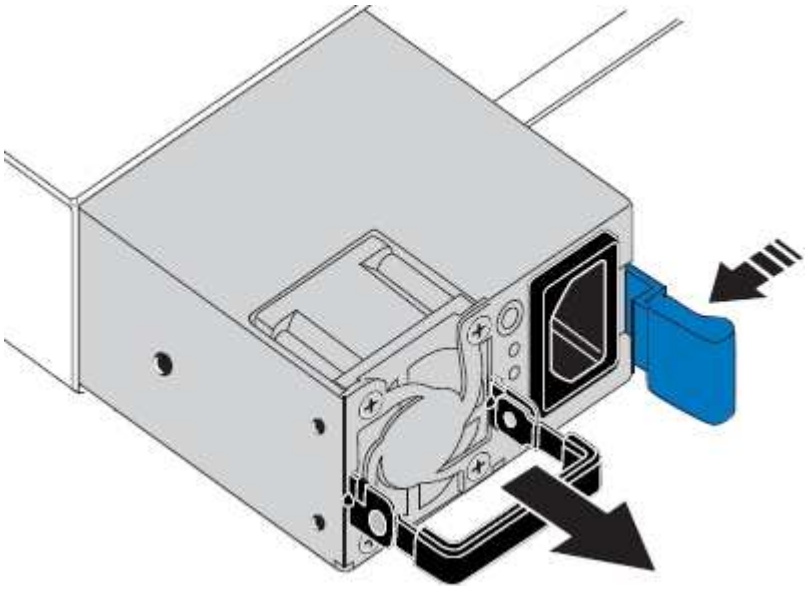
그림에서는 컨트롤러 후면에서 액세스할 수 있는 SG6000-CN 컨트롤러용 전원 공급 장치 2개를 보여 줍니다. 다음 절차를 사용하여 전원 공급 장치 중 하나 또는 모두를 교체합니다. 두 전원 공급 장치를 모두 교체하는 경우 먼저 제품의 제어된 종료를 수행해야 합니다.

단계

1. 하나의 전원 공급 장치만 교체하는 경우 제품을 종료할 필요가 없습니다. 로 이동합니다 전원 코드를 뽑습니다 단계. 두 전원 공급 장치를 동시에 교체하는 경우 전원 코드를 뽑기 전에 다음을 수행하십시오.
   a. 유지 관리 모드로 제품을 두십시오.
   b. 제품을 종료하십시오.
2. 교체할 각 전원 공급 장치에서 전원 코드를 뽑습니다.
3. 교체할 첫 번째 공급 장치의 캠 핸들을 들어 올립니다.



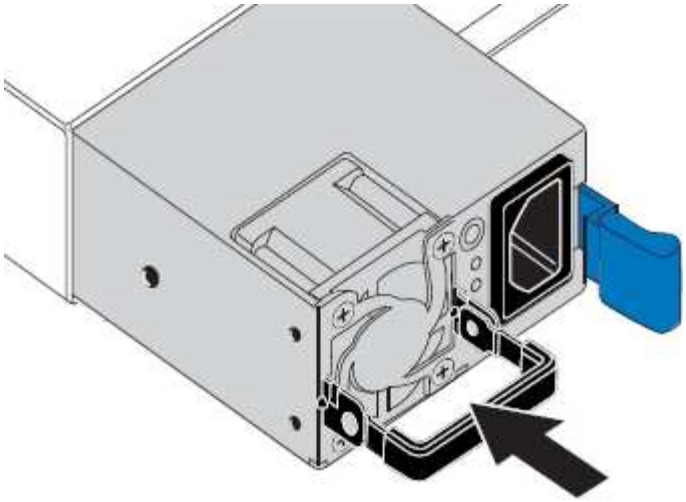
4. 파란색 래치를 누르고 전원 공급 장치를 당겨 빼냅니다.



5. 오른쪽에 있는 파란색 걸쇠를 사용하여 교체 전원 공급 장치를 섀시에 밀어 넣습니다.

> 두 전원 공급 장치 모두 모델 및 와트가 동일해야 합니다.

교체 장치를 밀어 넣을 때 파란색 걸쇠가 오른쪽에 있는지 확인합니다.



6. 캠 핸들을 아래로 눌러 교체용 전원 공급 장치를 고정합니다.
7. 두 전원 공급 장치를 모두 교체하는 경우 2-6단계를 반복하여 두 번째 전원 공급 장치를 교체합니다.
8. 전원 코드를 교체한 장치에 연결하고 전원을 공급합니다.
9. 어플라이언스를 유지보수 모드로 설정한 경우 유지보수 모드를 종료하십시오. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * StorageGRID * 으로 재부팅 * 을 선택합니다.

캐비닛 또는 랙에서 **SG6000-CN** 컨트롤러를 제거합니다

캐비닛 또는 랙에서 SG6000-CN 컨트롤러를 분리하여 상단 덮개에 액세스하거나 컨트롤러를 다른 위치로 이동합니다.

필요한 것

- SG6000-CN 컨트롤러에 연결된 각 케이블을 식별하는 라벨이 있습니다.
- 데이터 센터에서 유지 관리를 수행하는 SG6000-CN 컨트롤러를 물리적으로 배치했습니다.

  데이터 센터에서 컨트롤러를 찾습니다

- SG6000-CN 컨트롤러를 종료했습니다.

  SG6000-CN 컨트롤러를 종료합니다

  전원 스위치를 사용하여 컨트롤러를 종료하지 마십시오.

단계

1. 컨트롤러 전원 케이블에 레이블을 지정한 다음 케이블을 분리합니다.
2. ESD 밴드의 스트랩 끝을 손목 둘레에 감고 클립 끝을 금속 바닥에 단단히 고정하여 정전기 방전을 방지하십시오.
3. 컨트롤러 데이터 케이블과 SFP+ 또는 SFP28 트랜시버에 레이블을 지정한 다음 연결을 끊으십시오.

   성능 저하를 방지하려면 케이블을 비틀거나 접거나 끼거나 밟지 마십시오.

4. 컨트롤러 전면 패널에서 2개의 조임 나사를 풉니다.

5. 장착 레일이 완전히 확장되고 양쪽의 래치가 딸깍하는 소리가 날 때까지 SG6000-CN 컨트롤러를 랙에서 앞쪽으로 밉니다.

   컨트롤러 상단 덮개에 액세스할 수 있습니다.

6. 옵션: 캐비닛이나 랙에서 컨트롤러를 완전히 분리하는 경우 레일 키트의 지침에 따라 레일에서 컨트롤러를 분리합니다.

관련 정보

SG6000-CN 컨트롤러 덮개를 분리합니다

캐비닛 또는 랙에 **SG6000-CN** 컨트롤러를 다시 설치합니다

하드웨어 유지 관리가 완료되면 컨트롤러를 캐비닛 또는 랙에 다시 설치합니다.

필요한 것

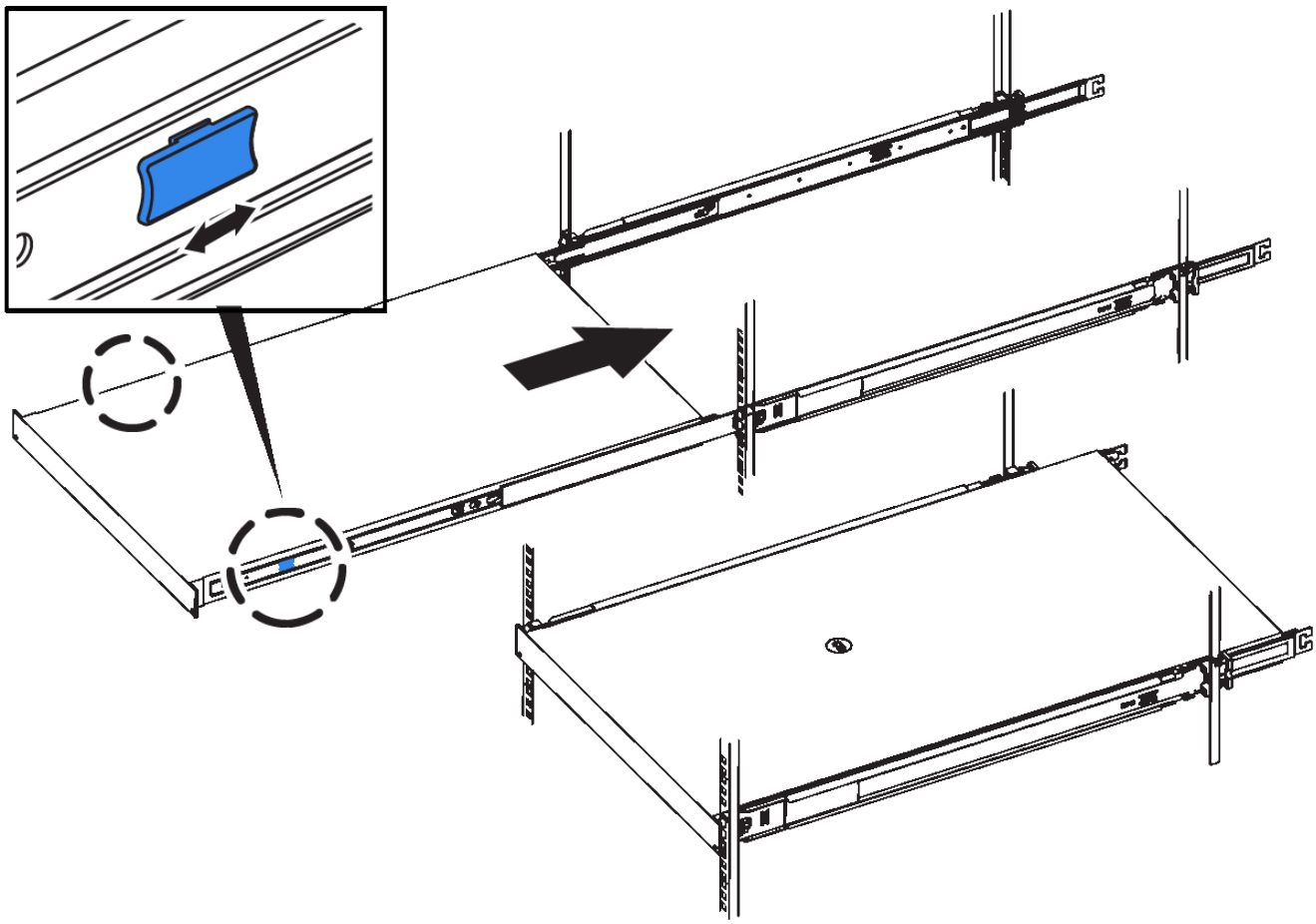
컨트롤러 덮개를 다시 설치했습니다.

SG6000-CN 컨트롤러 덮개를 다시 설치합니다

단계

1. 파란색 레일을 누르면 두 랙 레일이 동시에 풀릴 수 있으며 SG6000-CN 컨트롤러가 완전히 장착될 때까지 랙에 밀어 넣습니다.

   컨트롤러를 더 이상 이동할 수 없는 경우 섀시 양쪽에 있는 파란색 래치를 당겨 컨트롤러를 완전히 밀어 넣습니다.



컨트롤러의 전원을 켜기 전에는 전면 베젤을 연결하지 마십시오.

2. 컨트롤러 전면 패널의 조임 나사를 조여 컨트롤러를 랙에 고정합니다.

3. ESD 밴드의 스트랩 끝을 손목 둘레에 감고 클립 끝을 금속 바닥에 단단히 고정하여 정전기 방전을 방지하십시오.
4. 컨트롤러 데이터 케이블과 모든 SFP+ 또는 SFP28 트랜시버를 다시 연결합니다.

성능 저하를 방지하려면 케이블을 비틀거나 접거나 끼거나 밟지 마십시오.

케이블 어플라이언스(SG6000)

5. 컨트롤러 전원 케이블을 다시 연결합니다.

전원 코드 연결 및 전원 공급(SG6000)

작업을 마친 후

컨트롤러를 다시 시작할 수 있습니다.

SG6000-CN 컨트롤러의 전원을 켜고 작동을 확인합니다

SG6000-CN 컨트롤러 덮개를 분리합니다

컨트롤러 덮개를 분리하여 내부 구성요소에 유지보수 액세스를 제공합니다.

필요한 것

캐비닛 또는 랙에서 컨트롤러를 제거하여 상단 덮개에 액세스합니다.

캐비닛 또는 랙에서 SG6000-CN 컨트롤러를 제거합니다

단계

1. SG6000-CN 컨트롤러 덮개 래치가 잠겨 있지 않은지 확인합니다. 필요한 경우 래치 잠금 장치에 표시된 대로 파란색 플라스틱 래치 잠금 장치를 잠금 해제 방향으로 1/4바퀴 돌립니다.
2. 걸쇠를 위로 돌려 SG6000-CN 컨트롤러 섀시의 후면을 향해 멈출 때까지 돌린 다음 섀시에서 덮개를 조심스럽게 들어 올려 한 쪽에 둡니다.

SG6000-CN 컨트롤러 내부에서 작업할 때 정전기 방전을 방지하려면 ESD 밴드의 스트랩 끝을 손목 둘레에 감고 클립 끝을 금속 바닥에 고정합니다.

관련 정보

Fibre Channel HBA를 제거합니다

SG6000-CN 컨트롤러 덮개를 다시 설치합니다

내부 하드웨어 유지보수가 완료되면 컨트롤러 덮개를 다시 설치합니다.

필요한 것

컨트롤러 내의 모든 유지보수 절차를 완료했습니다.

단계

1. 덮개 래치를 연 상태에서 섀시 위의 덮개를 잡고 상단 덮개 래치의 구멍을 섀시의 핀에 맞춥니다. 덮개가 정렬되면 섀시 위로 내립니다.

2. 덮개가 멈추고 덮개가 섀시에 완전히 장착될 때까지 덮개 래치를 앞으로 또는 아래로 돌립니다. 덮개의 전면 가장자리를 따라 틈이 없는지 확인합니다.

   덮개가 완전히 장착되지 않은 경우 SG6000-CN 컨트롤러를 랙에 밀어 넣을 수 없을 수 있습니다.

3. 선택 사항: 래치 잠금 장치에 표시된 것처럼 파란색 플라스틱 래치 잠금 장치를 잠금 방향으로 1/4바퀴 돌려 잠급니다.

작업을 마친 후

캐비닛 또는 랙에 컨트롤러를 다시 설치합니다.

캐비닛 또는 랙에 SG6000-CN 컨트롤러를 다시 설치합니다

SG6000-CN 컨트롤러의 파이버 채널 **HBA**를 교체합니다

SG6000-CN 컨트롤러의 파이버 채널 호스트 버스 어댑터(HBA)가 최적의 상태로 작동하지 않거나 장애가 발생한 경우 이를 교체해야 할 수 있습니다.

교체할 **Fibre Channel HBA**를 확인합니다

교체할 Fibre Channel HBA(호스트 버스 어댑터)가 확실하지 않은 경우 이 절차를 수행하여 확인하십시오.

필요한 것

- Fibre Channel HBA를 교체해야 하는 스토리지 어플라이언스 또는 SG6000-CN 컨트롤러의 일련 번호가 있습니다.

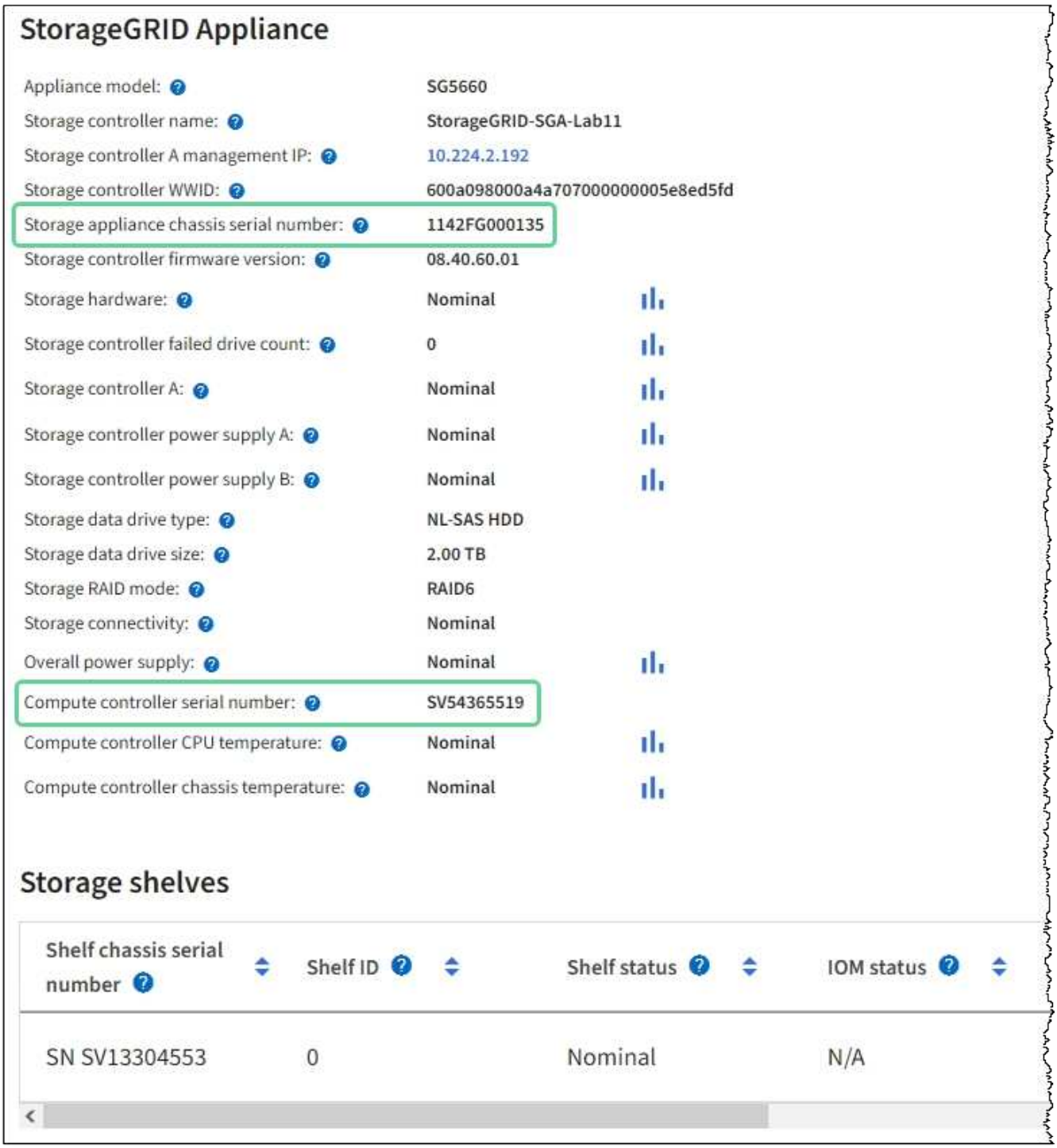
> 교체할 Fibre Channel HBA가 포함된 스토리지 어플라이언스의 일련 번호가 문자 Q로 시작하는 경우 그리드 관리자에 나열되지 않습니다. 일치하는 항목을 찾을 때까지 데이터 센터의 각 SG6000-CN 컨트롤러 전면에 부착된 태그를 확인해야 합니다.

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

단계

1. Grid Manager에서 * nodes * 를 선택합니다.
2. 노드 페이지의 표에서 어플라이언스 스토리지 노드를 선택합니다.
3. 하드웨어 * 탭을 선택합니다.

   StorageGRID 어플라이언스 섹션에서 * 스토리지 어플라이언스 섀시 일련 번호 * 와 * 컴퓨팅 컨트롤러 일련 번호 * 를 확인합니다. 이러한 일련 번호 중 하나가 Fibre Channel HBA를 교체할 스토리지 어플라이언스의 일련 번호와 일치하는지 확인합니다. 일련 번호가 일치하면 올바른 어플라이언스를 찾은 것입니다.



   - StorageGRID 어플라이언스 섹션이 표시되지 않는 경우 선택한 노드는 StorageGRID 어플라이언스가 아닙니다. 트리 뷰에서 다른 노드를 선택합니다.

- 어플라이언스 모델이 SG6060 또는 SG6060X가 아닌 경우 트리 뷰에서 다른 노드를 선택합니다.
- 제품 번호가 일치하지 않으면 트리 뷰에서 다른 노드를 선택합니다.

4. Fibre Channel HBA를 교체해야 하는 노드를 찾은 후 StorageGRID 어플라이언스 섹션에 나열된 컴퓨팅 컨트롤러 BMC IP 주소를 기록합니다.

   이 IP 주소를 사용하여 컴퓨팅 컨트롤러 식별 LED를 켜면 데이터 센터에서 어플라이언스를 찾을 수 있습니다.

   컨트롤러 식별 LED를 켜고 끕니다

관련 정보

Fibre Channel HBA를 제거합니다

Fibre Channel HBA를 제거합니다

SG6000-CN 컨트롤러의 파이버 채널 호스트 버스 어댑터(HBA)가 최적의 상태로 작동하지 않거나 장애가 발생한 경우 이를 교체해야 할 수 있습니다.

필요한 것

- 올바른 교체용 Fibre Channel HBA가 있습니다.
- 있습니다 "교체할 파이버 채널 HBA가 포함된 SG6000-CN 컨트롤러를 확인했습니다".
- 있습니다 "SG6000-CN 컨트롤러를 물리적으로 위치했다" 데이터 센터 내에서,
- 있습니다 "SG6000-CN 컨트롤러를 종료합니다".

  컨트롤러를 랙에서 분리하기 전에 제어된 방식으로 종료해야 합니다.

- 있습니다 "캐비닛이나 랙에서 컨트롤러를 제거했습니다".
- 있습니다 "컨트롤러 덮개를 분리했습니다".

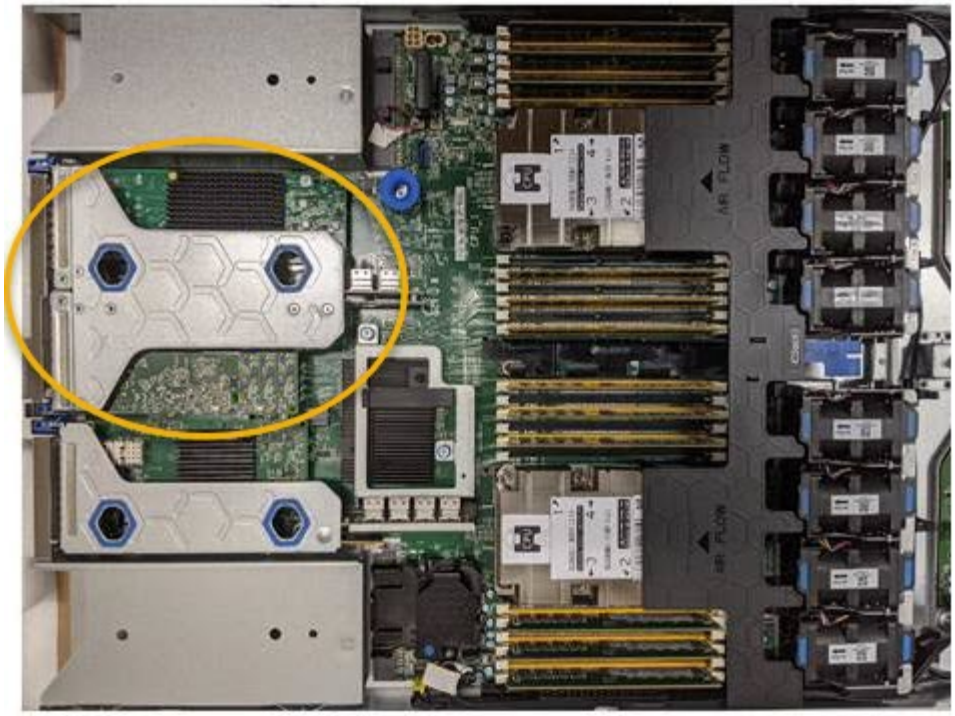
이 작업에 대해

서비스 중단을 방지하려면 Fibre Channel HBA 교체를 시작하기 전에 다른 모든 스토리지 노드가 그리드에 연결되어 있는지 확인하거나 서비스 중단이 정상적으로 예상되는 예약된 유지 보수 기간 동안 어댑터를 교체하십시오. 에 대한 정보를 참조하십시오 "노드 연결 상태를 모니터링합니다".

개체의 복사본을 하나만 생성하는 ILM 규칙을 사용한 적이 있는 경우 예약된 유지 관리 기간 동안 파이버 채널 HBA를 교체해야 합니다. 그렇지 않으면 이 절차 중에 해당 개체에 대한 액세스가 일시적으로 끊어질 수 있습니다. 에 대한 정보를 참조하십시오 "단일 복사본 복제를 사용하지 않아야 하는 이유".

단계

1. ESD 밴드의 스트랩 끝을 손목 둘레에 감고 클립 끝을 금속 바닥에 단단히 고정하여 정전기 방전을 방지하십시오.
2. 파이버 채널 HBA를 포함하는 컨트롤러 후면에서 라이저 어셈블리를 찾습니다.



3. 파란색 표시가 있는 구멍을 통해 라이저 조립품을 잡고 조심스럽게 위로 들어 올립니다. 라이저 조립품을 들어 올릴 때 섀시 앞쪽으로 이동하여 설치된 어댑터의 외부 커넥터가 섀시에서 분리되도록 합니다.
4. 라이저 카드를 금속 프레임 면이 아래로 향하게 하여 평평한 정전기 방지 표면에 놓고 어댑터에 액세스합니다.

라이저 어셈블리에는 파이버 채널 HBA와 이더넷 네트워크 어댑터의 두 어댑터가 있습니다. Fibre Channel HBA는 그림에 나와 있습니다.

5. 파란색 어댑터 래치(원으로 표시됨)를 열고 라이저 어셈블리에서 파이버 채널 HBA를 조심스럽게 분리합니다. 어댑터를 살짝 흔들어 커넥터에서 어댑터를 분리합니다. 과도한 힘을 가하지 마십시오.
6. 어댑터를 평평한 정전기 방지 표면에 놓습니다.

작업을 마친 후

교체용 Fibre Channel HBA를 설치합니다.

Fibre Channel HBA를 다시 설치합니다

교체용 Fibre Channel HBA가 제거된 위치와 동일한 위치에 설치됩니다.

필요한 것

- 올바른 교체용 Fibre Channel HBA가 있습니다.
- 기존 Fibre Channel HBA를 제거했습니다.

  Fibre Channel HBA를 제거합니다

단계

1. ESD 밴드의 스트랩 끝을 손목 둘레에 감고 클립 끝을 금속 바닥에 단단히 고정하여 정전기 방전을 방지하십시오.
2. 교체용 Fibre Channel HBA를 포장에서 꺼냅니다.
3. 파란색 어댑터 걸쇠가 열린 상태에서 파이버 채널 HBA를 라이저 어셈블리의 커넥터와 맞춘 다음 어댑터가 완전히 장착될 때까지 커넥터에 조심스럽게 누릅니다.

   라이저 어셈블리에는 파이버 채널 HBA와 이더넷 네트워크 어댑터의 두 어댑터가 있습니다. Fibre Channel HBA는 그림에 나와 있습니다.

4. 라이저 어셈블리의 올바른 위치를 위해 시스템 보드의 가이드 핀에 맞춰진 라이저 어셈블리(원으로 표시됨)의 정렬 구멍을 찾습니다.

5. 라이저 조립품을 섀시에 놓고 시스템 보드의 커넥터 및 가이드 핀에 맞춥니다. 그런 다음 라이저 조립품을 삽입합니다.

6. 라이저 조립품이 파란색 표시가 있는 구멍 옆에 있는 중앙 라인을 따라 완전히 장착될 때까지 조심스럽게 누르십시오.
7. 케이블을 다시 설치할 Fibre Channel HBA 포트에서 보호 캡을 제거합니다.

작업을 마친 후

컨트롤러에서 수행할 다른 유지보수 절차가 없는 경우 컨트롤러 덮개를 다시 설치합니다.

SG6000-CN 컨트롤러 덮개를 다시 설치합니다

SG6000-CN 컨트롤러의 링크 구성을 변경합니다

SG6000-CN 컨트롤러의 이더넷 링크 구성을 변경할 수 있습니다. 포트 연결 모드, 네트워크 연결 모드 및 링크 속도를 변경할 수 있습니다.

필요한 것

제품이 다 되었습니다 유지보수 모드로 전환되었습니다.

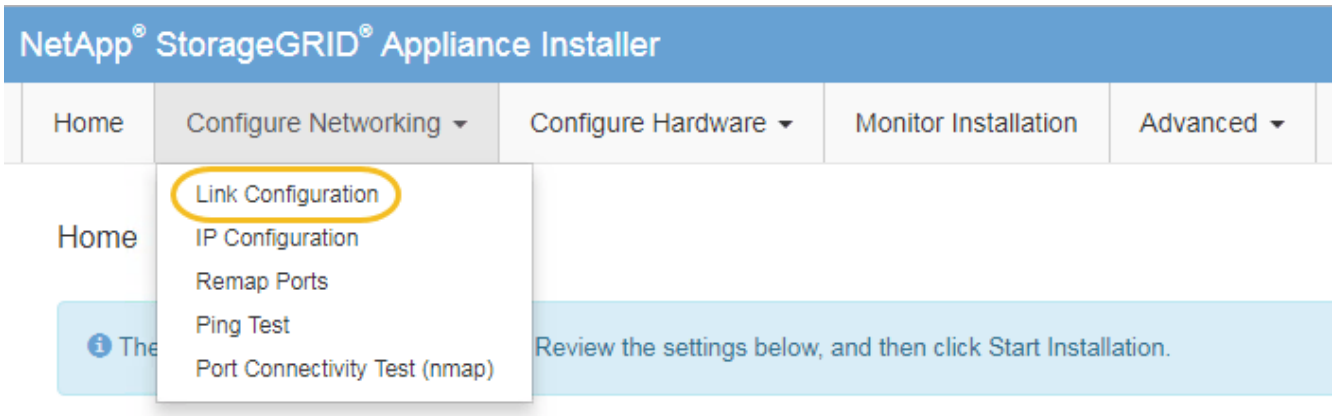
이 작업에 대해

SG6000-CN 컨트롤러의 이더넷 링크 구성을 변경하는 옵션은 다음과 같습니다.

- 포트 결합 모드 * 를 고정에서 집계로, 또는 Aggregate에서 고정으로 변경
- Active-Backup에서 LACP로 또는 LACP에서 Active-Backup으로 * 네트워크 결합 모드 * 변경
- VLAN 태그 지정 활성화 또는 비활성화 또는 VLAN 태그 값 변경
- 링크 속도 변경

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * 링크 구성 * 을 선택합니다.



2. 링크 설정을 원하는 대로 변경합니다.

   옵션에 대한 자세한 내용은 을 참조하십시오 네트워크 링크 구성(SG6000).

3. 선택 사항에 만족하면 * 저장 * 을 클릭합니다.

> 연결된 네트워크 또는 링크를 변경한 경우 연결이 끊어질 수 있습니다. 1분 내에 다시 연결되지 않으면 어플라이언스에 할당된 다른 IP 주소 중 하나를 사용하여 StorageGRID 어플라이언스 설치 프로그램의 URL을 다시 입력합니다. + " * https://*Appliance_Controller_IP*:8443*`

VLAN 설정을 변경한 경우 어플라이언스의 서브넷이 변경되었을 수 있습니다. 어플라이언스의 IP 주소를 변경해야 하는 경우 에 따르십시오 IP 주소를 구성합니다 지침.

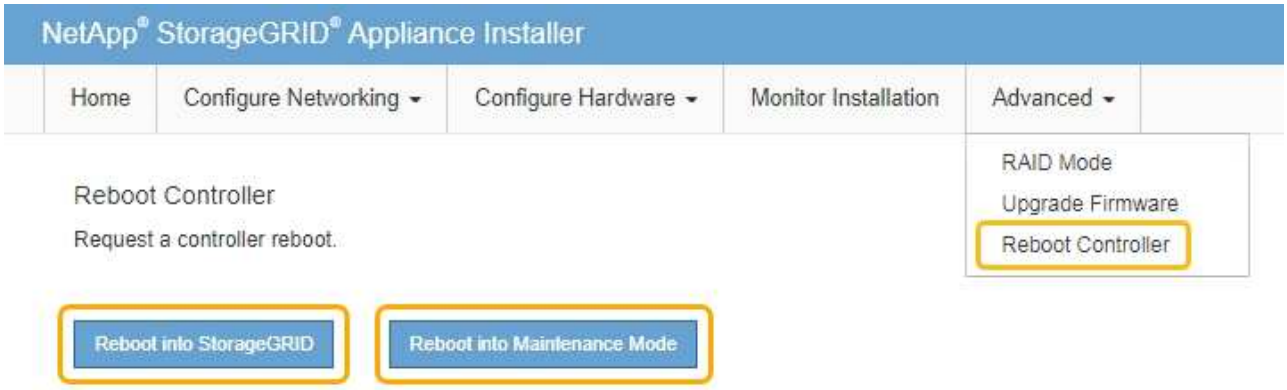
StorageGRID IP 주소를 구성합니다

4. 메뉴에서 * 네트워킹 구성 * > * Ping 테스트 * 를 선택합니다.
5. Ping 테스트 도구를 사용하여 에서 변경한 링크 구성의 영향을 받을 수 있는 네트워크의 IP 주소에 대한 연결을 확인합니다 링크 구성 변경 단계.

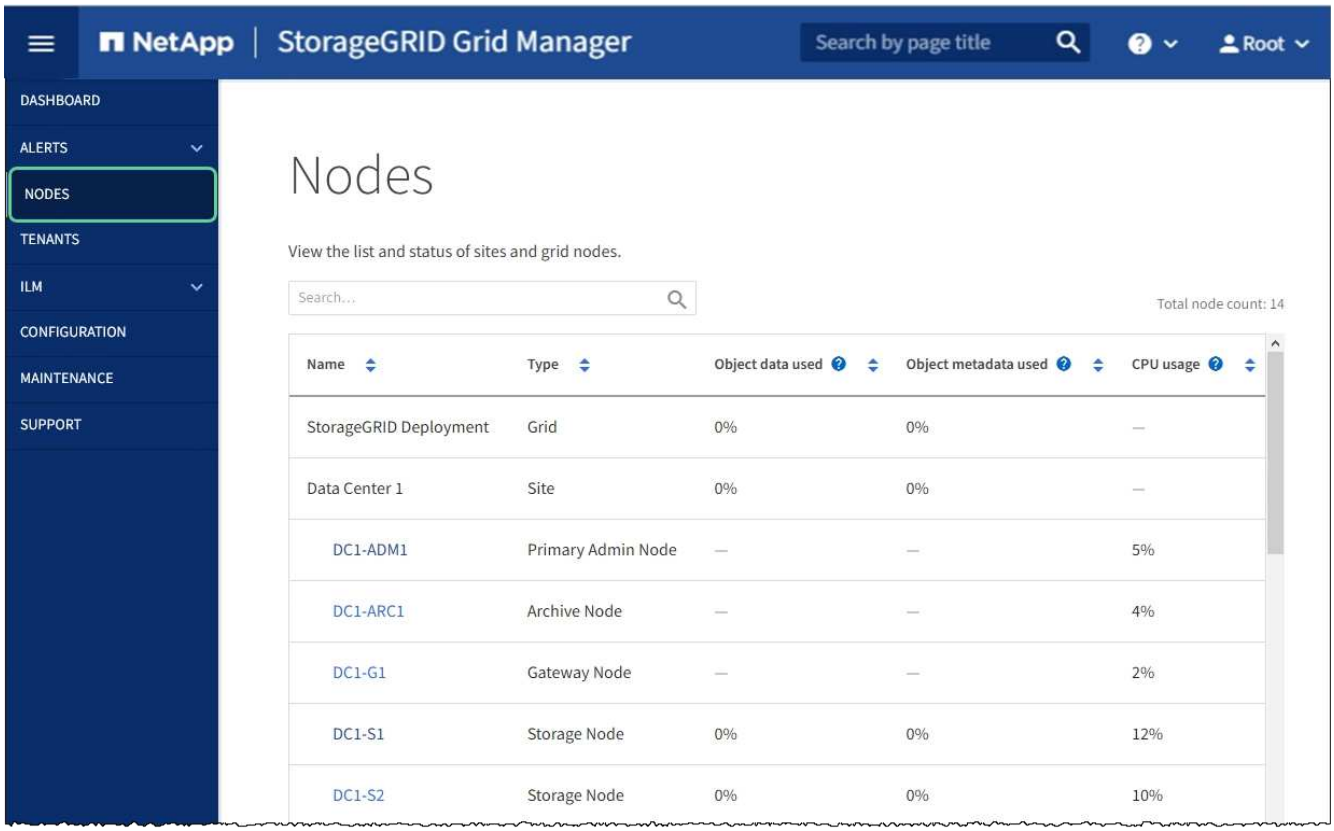
   수행할 다른 테스트 외에도 기본 관리 노드의 그리드 네트워크 IP 주소와 하나 이상의 다른 스토리지 노드의 그리드 네트워크 IP 주소를 ping할 수 있는지 확인합니다. 필요한 경우 로 돌아갑니다 링크 구성 변경 링크 구성 문제를 단계별로 해결합니다.

6. 링크 구성 변경이 작동 중이고 노드가 유지보수 모드일 때 수행할 추가 절차가 있으면 지금 수행합니다. 작업을 완료했거나 오류가 발생하여 다시 시작하려면 * 고급 * > * 컨트롤러 재부팅 * 을 선택하고 다음 옵션 중 하나를 선택합니다.

   - StorageGRID * 로 재부팅 * 을 선택합니다
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. 절차 중에 오류가 발생하여 다시 시작하려면 이 옵션을 선택합니다. 노드가 유지보수 모드로 재부팅된 후 장애가 발생한 절차의 적절한 단계에서 다시 시작하십시오.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



MTU 설정을 변경합니다

어플라이언스 노드에 대한 IP 주소를 구성할 때 할당한 MTU 설정을 변경할 수 있습니다.

이 작업에 대해

네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

어플라이언스 노드를 재부팅하지 않고 MTU 설정을 변경하려면 IP 변경 도구를 사용합니다.

초기 설치 중에 StorageGRID 어플라이언스 설치 프로그램에서 클라이언트 또는 관리자 네트워크가 구성되지 않은 경우 유지보수 모드를 사용하여 MTU 설정을 변경합니다.

IP 변경 도구를 사용하여 **MTU** 설정을 변경합니다

필요한 것

Change IP 툴을 사용할 수 있는 "passwords.txt" 파일이 있습니다.

단계

IP 변경 도구에 액세스하여 에 설명된 대로 MTU 설정을 업데이트합니다 노드 네트워크 구성을 변경합니다.

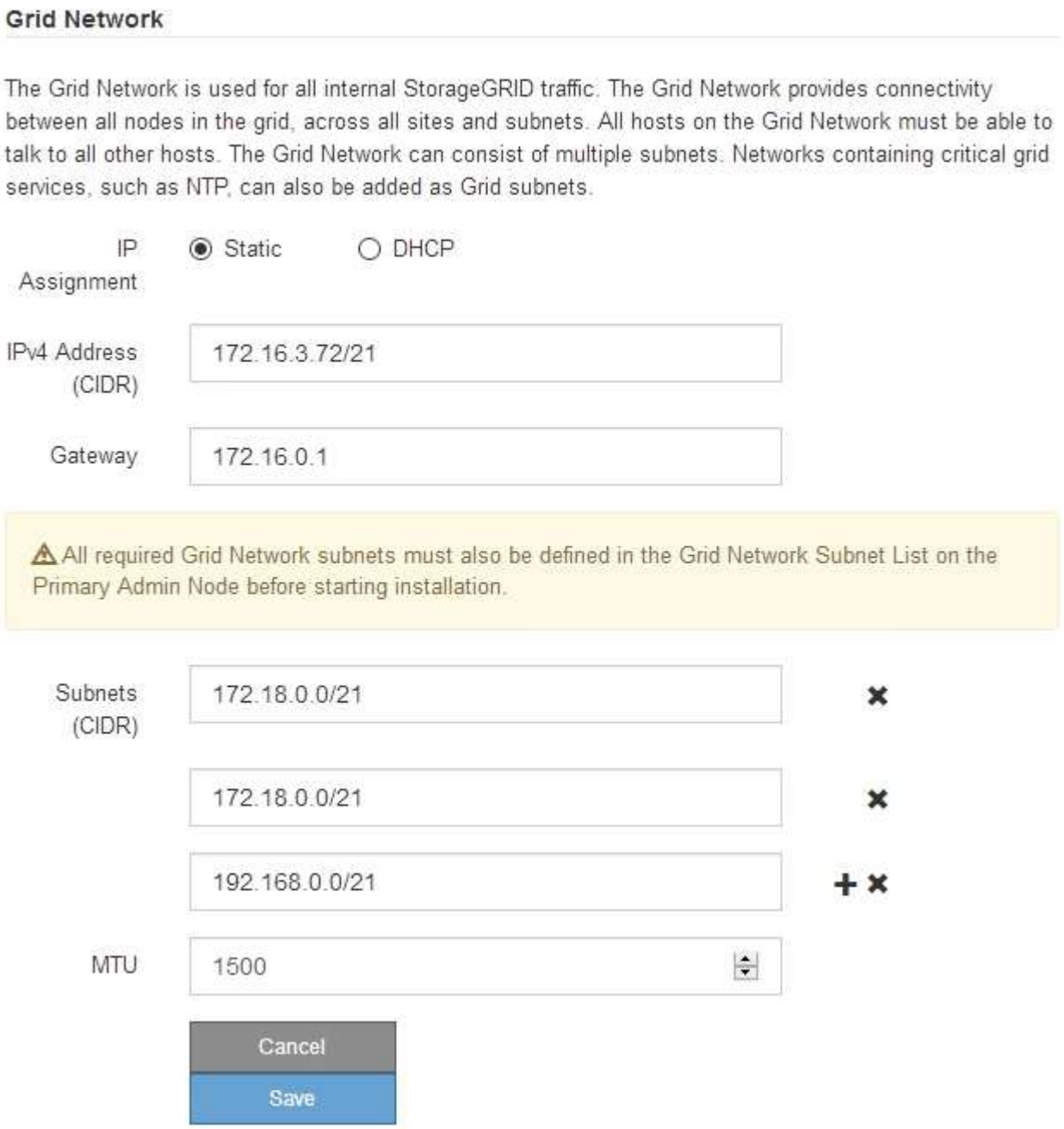
Change IP(IP 변경) 도구를 사용하여 이러한 설정에 액세스할 수 없는 경우 유지보수 모드를 사용하여 MTU 설정을 변경합니다.

필요한 것

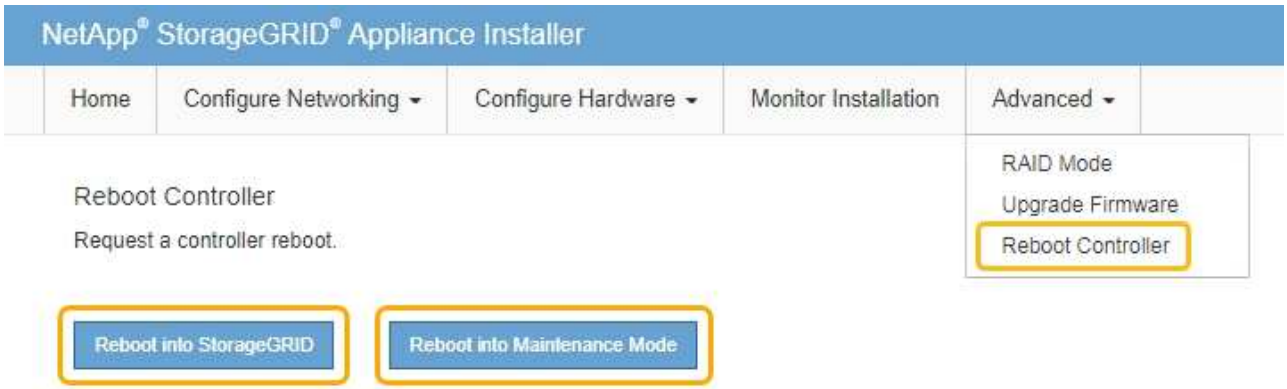
제품이 다 되었습니다 유지보수 모드로 전환되었습니다.

단계

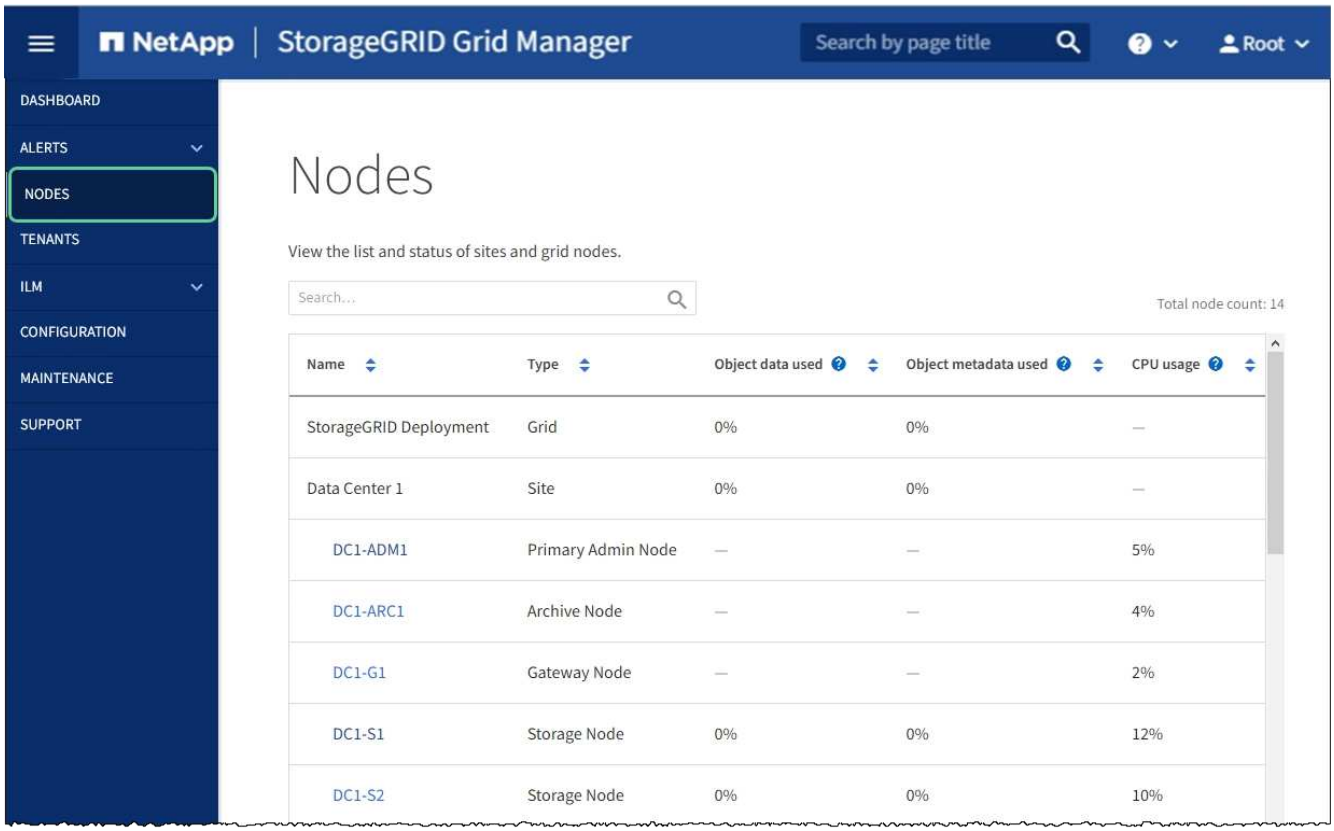
1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * IP 구성 * 을 선택합니다.
2. 그리드 네트워크, 관리자 네트워크 및 클라이언트 네트워크에 대한 MTU 설정을 원하는 대로 변경합니다.



3. 설정이 만족스러우면 * 저장 * 을 선택합니다.
4. 이 절차가 성공적으로 완료되었고 노드가 유지보수 모드일 때 수행할 추가 절차가 있는 경우 지금 수행합니다. 작업을 완료했거나 오류가 발생하여 다시 시작하려면 * 고급 * > * 컨트롤러 재부팅 * 을 선택하고 다음 옵션 중 하나를 선택합니다.
    - StorageGRID * 로 재부팅 * 을 선택합니다
    - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. 절차 중에 오류가 발생하여 다시 시작하려면 이 옵션을 선택합니다. 노드가 유지보수 모드로 재부팅된 후 장애가 발생한 절차의 적절한 단계에서 다시 시작하십시오.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

StorageGRID 관리

DNS 서버 구성을 확인합니다

이 어플라이언스 노드에서 현재 사용 중인 DNS(Domain Name System) 서버를 확인하고 일시적으로 변경할 수 있습니다.

필요한 것

제품이 다 되었습니다 유지보수 모드로 전환되었습니다.

이 작업에 대해

KMS의 호스트 이름이 IP 주소 대신 도메인 이름으로 지정되었기 때문에 암호화된 어플라이언스가 KMS(키 관리 서버) 또는 KMS 클러스터에 연결할 수 없는 경우 DNS 서버 설정을 변경해야 할 수 있습니다. 어플라이언스에 대한 DNS 설정에 대한 모든 변경 사항은 일시적이며 유지 관리 모드를 종료할 때 손실됩니다. 이러한 변경 사항을 영구적으로 적용하려면 Grid Manager(* 유지 관리 * > * 네트워크 * > * DNS 서버 *)에서 DNS 서버를 지정합니다.

- KMS 서버가 호스트 이름에 대해 IP 주소 대신 정규화된 도메인 이름을 사용하여 정의된 노드 암호화 어플라이언스인 경우에만 DNS 구성을 일시적으로 변경해야 합니다.
- 노드 암호화 어플라이언스가 도메인 이름을 사용하여 KMS에 연결되는 경우 그리드에 정의된 DNS 서버 중 하나에 연결해야 합니다. 그런 다음 이러한 DNS 서버 중 하나가 도메인 이름을 IP 주소로 변환합니다.
- 노드가 그리드의 DNS 서버에 연결할 수 없거나 노드 암호화 어플라이언스 노드가 오프라인일 때 그리드 전체 DNS 설정을 변경한 경우 노드가 KMS에 연결할 수 없습니다. DNS 문제가 해결될 때까지 어플라이언스에 있는 암호화된 데이터를 해독할 수 없습니다.

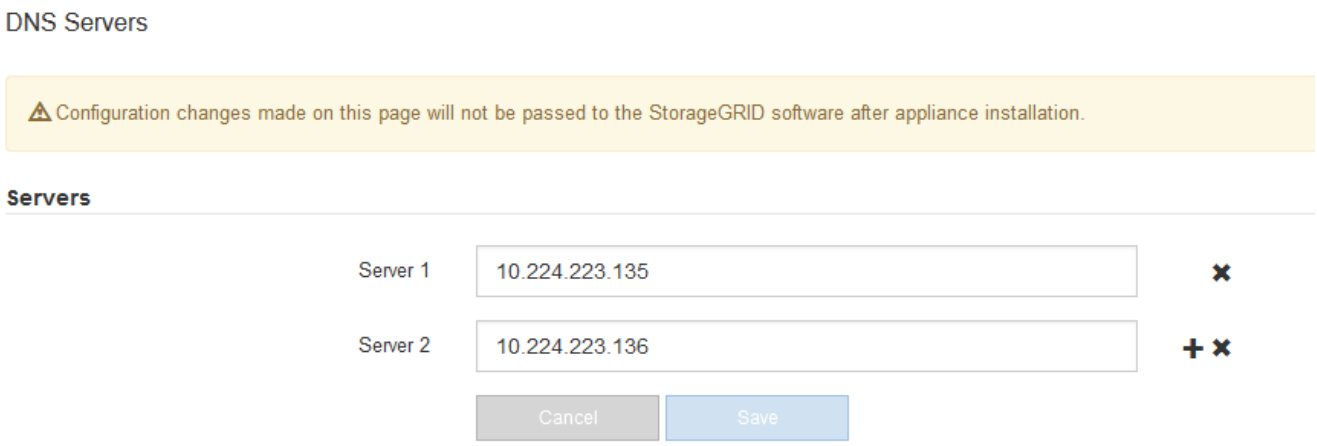
KMS 연결을 방해하는 DNS 문제를 해결하려면 StorageGRID 어플라이언스 설치 프로그램에서 하나 이상의 DNS

서버의 IP 주소를 지정하십시오. 이러한 임시 DNS 설정을 사용하면 어플라이언스가 KMS에 연결하고 노드의 데이터를 해독할 수 있습니다.

예를 들어, 암호화된 노드가 오프라인 상태일 때 그리드의 DNS 서버가 변경되면 노드가 다시 온라인 상태가 될 때 KMS에 도달할 수 없습니다. KMS는 이전 DNS 값을 계속 사용하고 있기 때문입니다. StorageGRID 어플라이언스 설치 프로그램에 새 DNS 서버 IP 주소를 입력하면 임시 KMS 연결을 통해 노드 데이터를 해독할 수 있습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * DNS 구성 * 을 선택합니다.
2. 지정된 DNS 서버가 올바른지 확인합니다.



3. 필요한 경우 DNS 서버를 변경합니다.

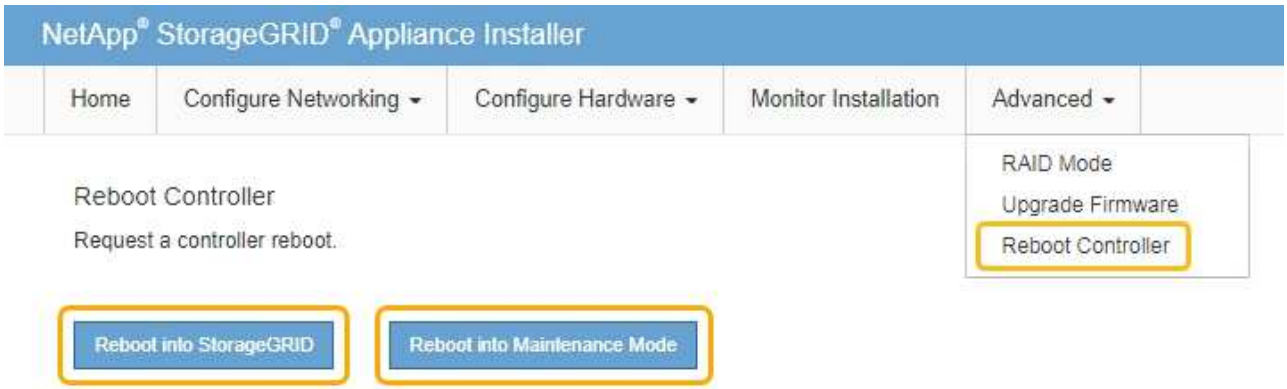
   DNS 설정에 대한 변경 사항은 일시적이며 유지 관리 모드를 종료할 때 손실됩니다.

4. 임시 DNS 설정이 만족스러우면 * Save * 를 선택합니다.

   노드는 이 페이지에 지정된 DNS 서버 설정을 사용하여 KMS에 다시 연결하여 노드의 데이터를 해독할 수 있도록 합니다.

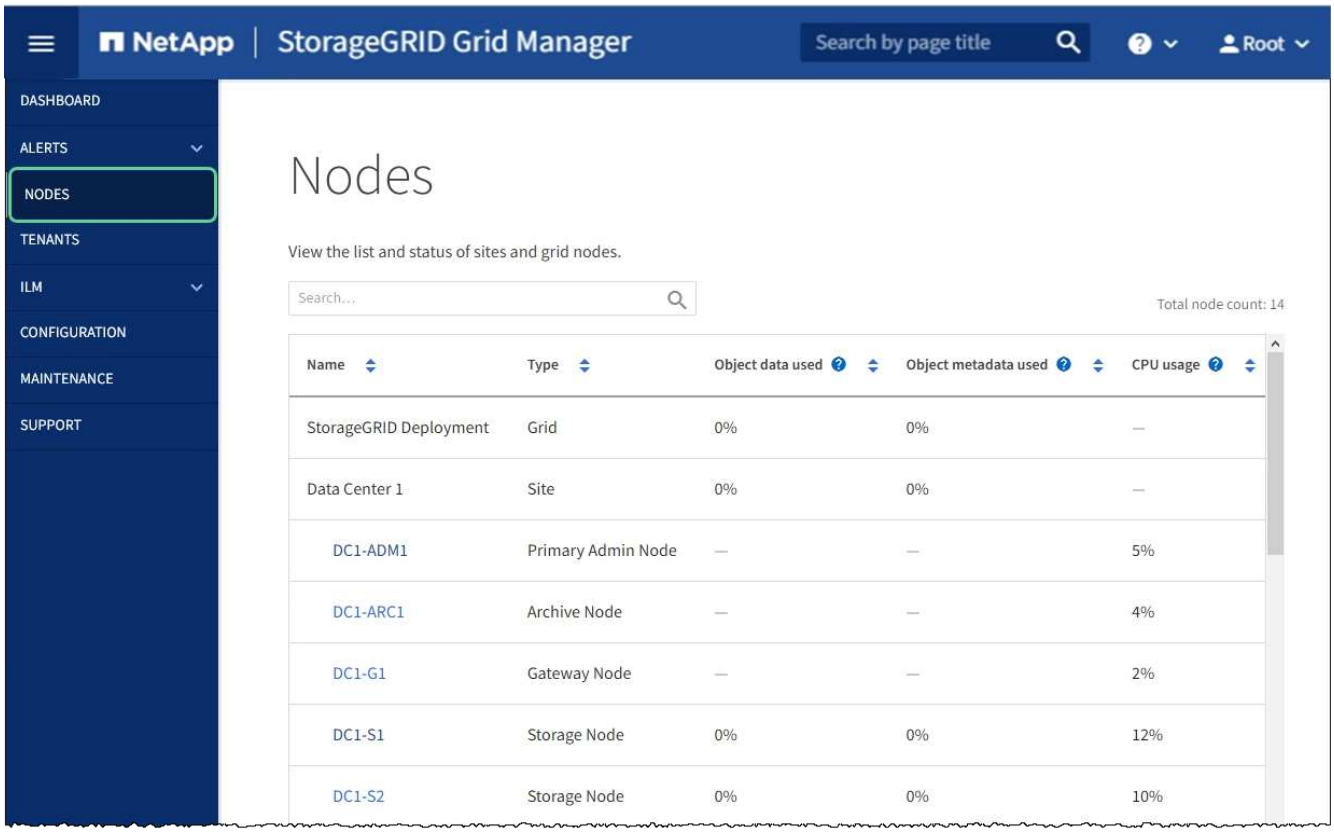
5. 노드 데이터가 해독된 후 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.

   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



노드가 재부팅되고 그리드에 다시 연결되면 Grid Manager에 나열된 시스템 전체 DNS 서버가 사용됩니다. 그리드를 다시 연결한 후 어플라이언스는 어플라이언스가 유지보수 모드일 때 StorageGRID 어플라이언스 설치 프로그램에 지정된 임시 DNS 서버를 더 이상 사용하지 않습니다.

어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



유지보수 모드(**SG6000**)에서 노드 암호화 모니터링

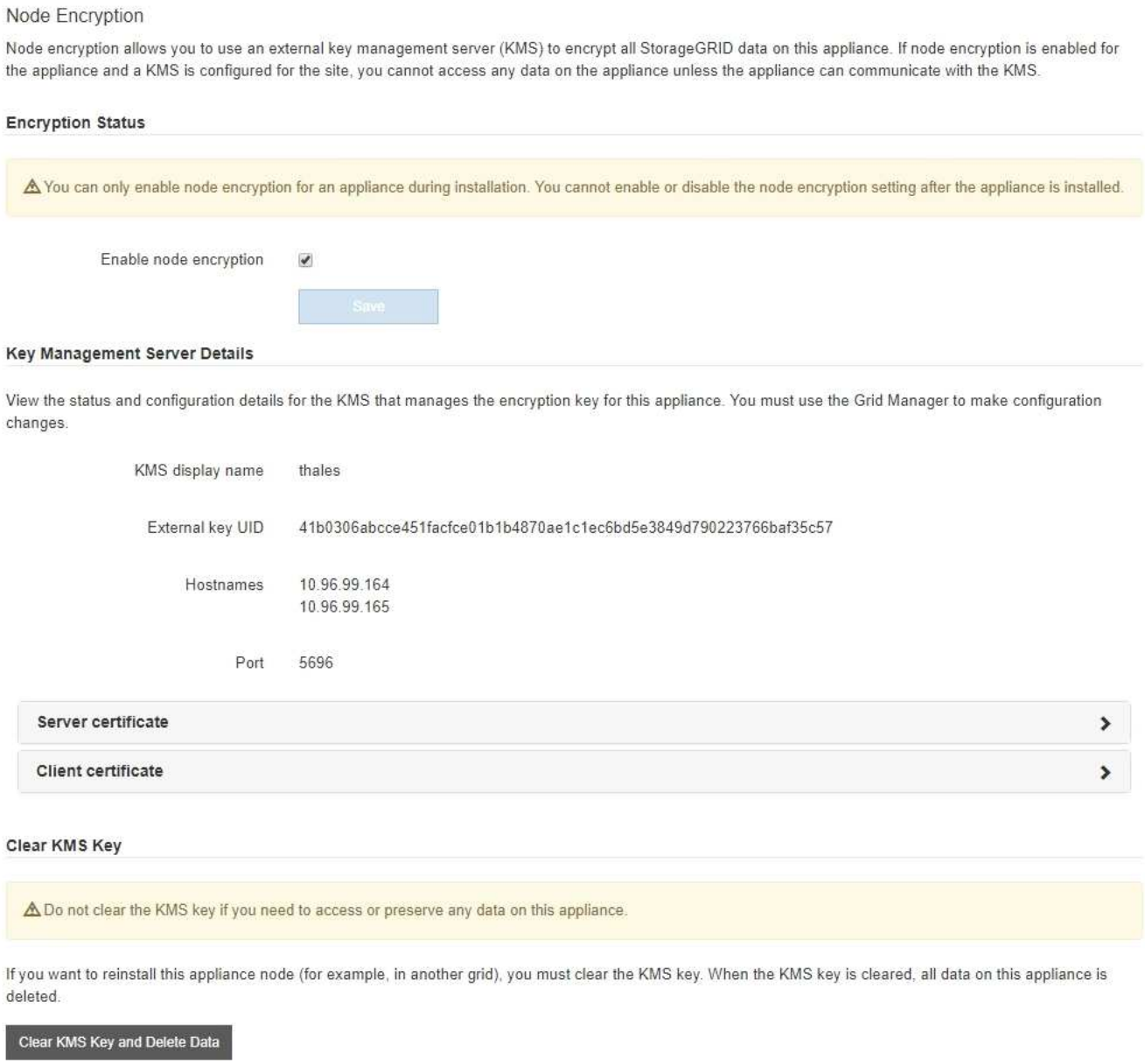
설치 중에 어플라이언스에 대한 노드 암호화를 활성화한 경우 노드 암호화 상태 및 키 관리 서버(KMS) 세부 정보를 포함하여 각 어플라이언스 노드의 노드 암호화 상태를 모니터링할 수 있습니다.

필요한 것

- 설치하는 동안 어플라이언스에 대해 노드 암호화가 활성화되어 있어야 합니다. 어플라이언스를 설치한 후에는 노드 암호화를 활성화할 수 없습니다.
- 있습니다 제품을 유지보수 모드로 놓았습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.



노드 암호화 페이지에는 다음 세 가지 섹션이 있습니다.

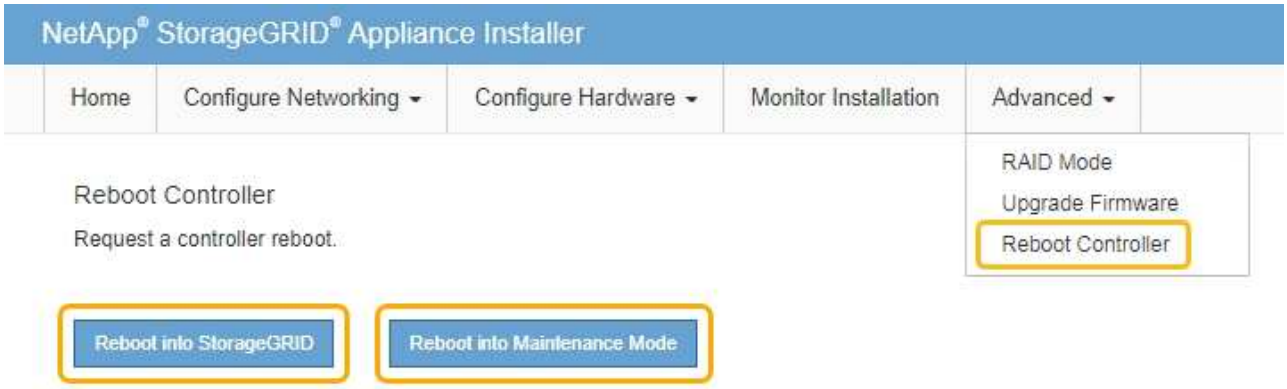
- 암호화 상태 는 어플라이언스에 대해 노드 암호화가 활성화되었는지 여부를 표시합니다.
- 키 관리 서버 세부 정보 는 어플라이언스를 암호화하는 데 사용되는 KMS에 대한 정보를 보여 줍니다. 서버 및 클라이언트 인증서 섹션을 확장하여 인증서 세부 정보 및 상태를 볼 수 있습니다.
  - 만료된 인증서 갱신과 같은 인증서 자체의 문제를 해결하려면 StorageGRID 관리 지침의 KMS 정보를 참조하십시오.
  - KMS 호스트에 연결할 때 예기치 않은 문제가 발생하는 경우 DNS(Domain Name System) 서버가 올바르고 어플라이언스 네트워킹이 올바르게 구성되었는지 확인합니다.

    DNS 서버 구성을 확인합니다

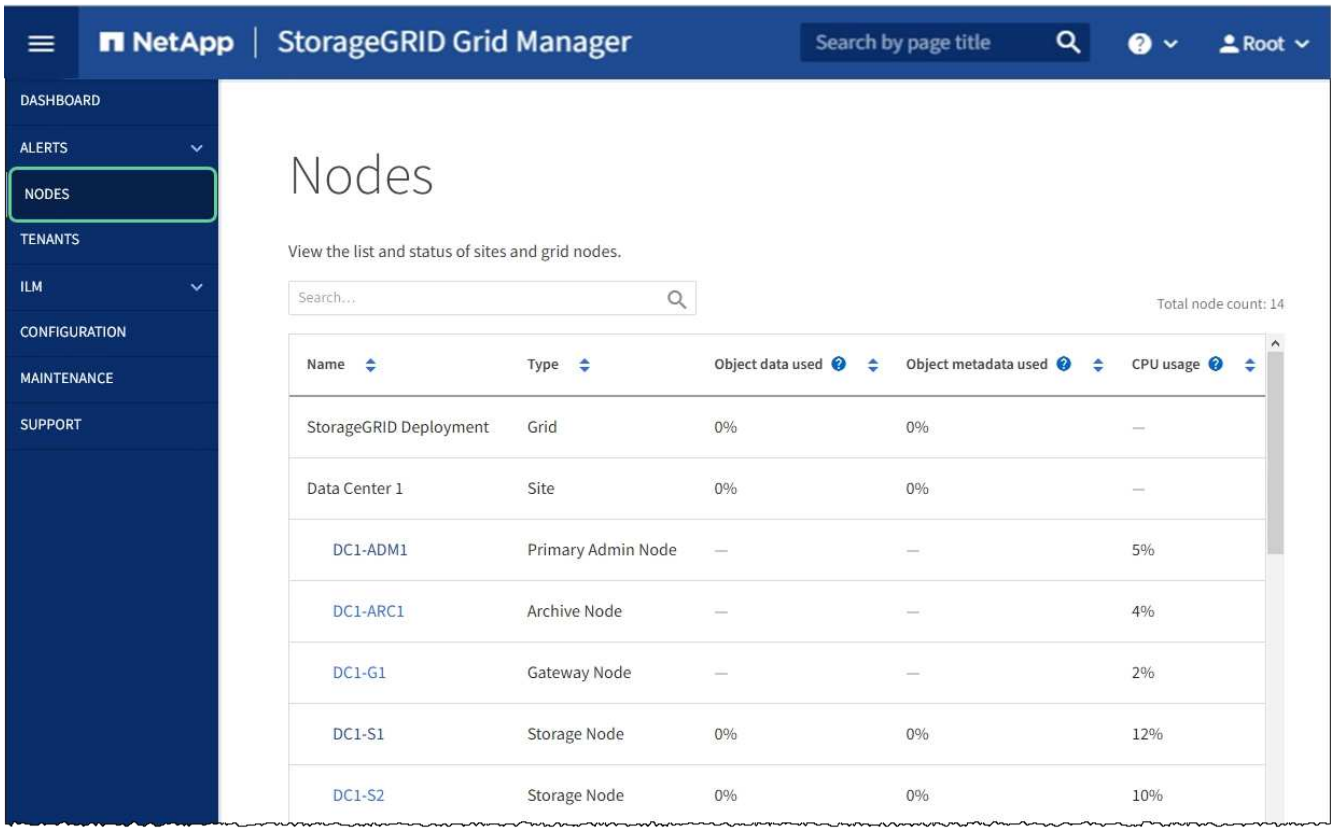
  - 인증서 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.
- KMS 키 지우기(Clear KMS Key)는 어플라이언스에 대한 노드 암호화를 해제하고, StorageGRID 사이트에 구성된 키 관리 서버와 어플라이언스를 제거하고, 어플라이언스에서 모든 데이터를 삭제합니다. 반드시 해야 합니다 KMS 키를 지웁니다 다른 StorageGRID 시스템에 제품을 설치하기 전에

> KMS 구성을 지우면 어플라이언스에서 데이터가 삭제되어 영구적으로 액세스할 수 없게 됩니다. 이 데이터는 복구할 수 없습니다.

2. 노드 암호화 상태 확인을 마쳤으면 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.
   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

StorageGRID 관리

키 관리 서버 구성을 지웁니다

KMS(키 관리 서버) 구성을 지우면 어플라이언스에서 노드 암호화가 비활성화됩니다. KMS 구성을 삭제한 후에는 어플라이언스의 데이터가 영구적으로 삭제되며 더 이상 액세스할 수 없습니다. 이 데이터는 복구할 수 없습니다.

필요한 것

어플라이언스의 데이터를 보존해야 하는 경우 KMS 구성을 지우기 전에 노드 서비스 해제 절차를 수행하거나 노드를 복제해야 합니다.

> KMS를 삭제하면 제품의 데이터가 영구적으로 삭제되고 더 이상 액세스할 수 없게 됩니다. 이 데이터는 복구할 수 없습니다.

노드 서비스 해제 포함된 데이터를 StorageGRID의 다른 노드로 이동하려면 다음을 사용합니다.

이 작업에 대해

어플라이언스 KMS 구성을 지우면 노드 암호화가 비활성화되므로 어플라이언스 노드와 StorageGRID 사이트의 KMS 구성 간의 연결이 제거됩니다. 그러면 어플라이언스의 데이터가 삭제되고 어플라이언스가 사전 설치 상태로 유지됩니다. 이 프로세스는 되돌릴 수 없습니다.

KMS 구성을 지워야 합니다.

- KMS를 사용하지 않거나 다른 KMS를 사용하는 다른 StorageGRID 시스템에 제품을 설치하기 전에

> 동일한 KMS 키를 사용하는 StorageGRID 시스템에 어플라이언스 노드를 재설치하려는 경우 KMS 구성을 지우지 마십시오.

- KMS 구성이 손실되고 KMS 키를 복구할 수 없는 노드를 복구 및 재설치할 수 있습니다.
- 이전에 현장에서 사용 중이던 제품을 반환하기 전에
- 노드 암호화가 설정된 어플라이언스를 서비스 해제 후

> KMS를 제거하기 전에 어플라이언스의 전원을 해제하여 StorageGRID 시스템의 다른 노드로 데이터를 이동합니다. KMS를 폐기하기 전에 제거하면 데이터가 손실되고 어플라이언스가 작동하지 않을 수 있습니다.

단계

1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption ☑

Save

Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate >

Client certificate >

Clear KMS Key

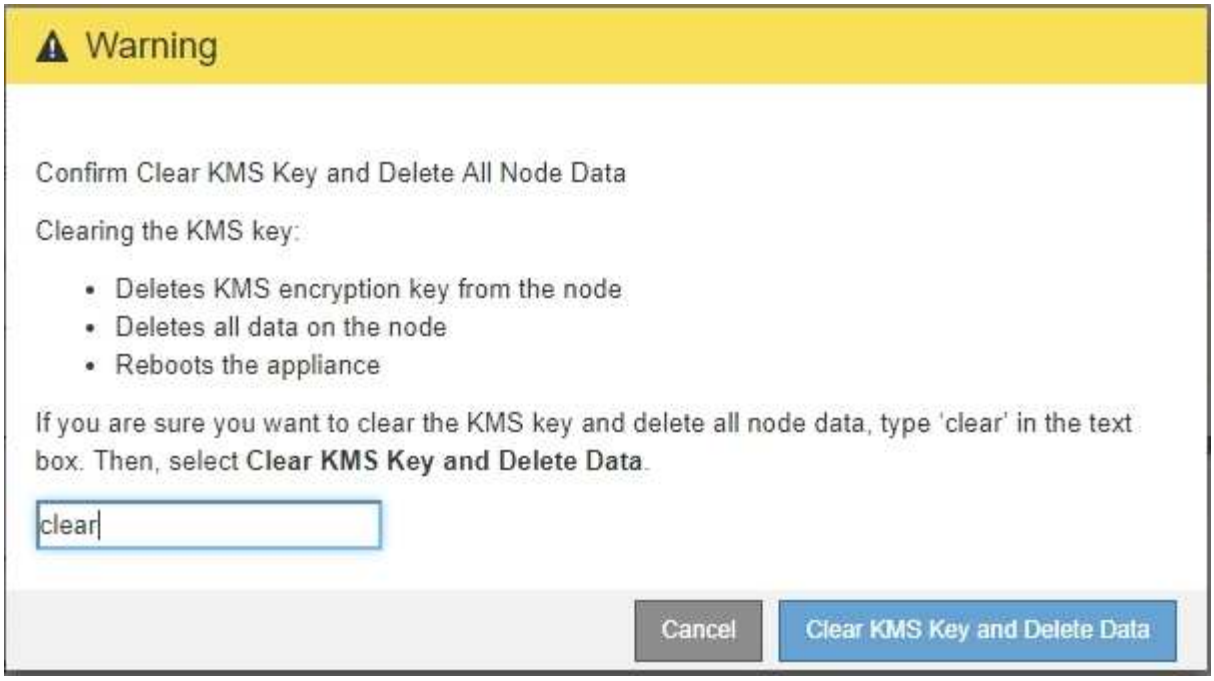
Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

> KMS 구성이 삭제된 경우 어플라이언스의 데이터가 영구적으로 삭제됩니다. 이 데이터는 복구할 수 없습니다.

3. 창 아래쪽에서 * KMS 키 삭제 및 데이터 삭제 * 를 선택합니다.
4. KMS 구성을 지우려면 + " * clear * "+를 입력하고 * KMS 키 삭제 및 데이터 삭제 * 를 선택합니다.



KMS 암호화 키 및 모든 데이터가 노드에서 삭제되고 어플라이언스가 재부팅됩니다. 이 작업은 최대 20분이 소요될 수 있습니다.

5. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

6. 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.
7. 노드 암호화가 비활성화되었으며 * 키 관리 서버 세부 정보 * 및 * KMS 키 지우기 및 데이터 삭제 * 컨트롤의 키 및 인증서 정보가 창에서 제거되었는지 확인합니다.

   그리드에 다시 설치할 때까지 어플라이언스에서 노드 암호화를 다시 활성화할 수 없습니다.

작업을 마친 후

어플라이언스가 재부팅되고 KMS가 삭제되었으며 제품이 사전 설치 상태인지 확인한 후에는 StorageGRID 시스템에서 어플라이언스를 물리적으로 제거할 수 있습니다. 를 참조하십시오 어플라이언스 재설치 준비 지침.

관련 정보

StorageGRID 관리

SG5700 스토리지 어플라이언스

StorageGRID SG5700 어플라이언스 개요

SG5700 StorageGRID 어플라이언스는 StorageGRID 그리드에서 스토리지 노드로 작동하는 통합 스토리지 및 컴퓨팅 플랫폼입니다. 어플라이언스는 어플라이언스 스토리지 노드와 가상

(소프트웨어 기반) 스토리지 노드를 결합하는 하이브리드 그리드 환경에서 사용할 수 있습니다.

StorageGRID SG5700 시리즈 어플라이언스는 다음 기능을 제공합니다.

- StorageGRID 스토리지 노드의 스토리지 및 컴퓨팅 요소 통합
- 스토리지 노드 구축 및 구성을 단순화하기 위해 StorageGRID 어플라이언스 설치 프로그램을 포함합니다.
- 하드웨어 관리 및 모니터링을 위한 E-Series SANtricity System Manager 포함.
- StorageGRID 그리드 네트워크 및 클라이언트 네트워크에 대한 10GbE 또는 25GbE 연결을 최대 4개까지 지원합니다.
- FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브를 지원합니다. 이러한 드라이브를 SANtricity 시스템 관리자의 드라이브 보안 기능과 함께 사용하면 데이터에 대한 무단 액세스가 방지됩니다.

SG5712 및 SG5712X, SG5760 및 SG5760X의 4가지 모델에서 SG57어플라이언스를 사용할 수 있습니다. 스토리지 컨트롤러의 상호 연결 포트 위치를 제외하고는 SG5712와 SG5712X 간에 사양 또는 기능 차이가 없습니다. 마찬가지로, 스토리지 컨트롤러에서 상호 연결 포트의 위치를 제외하고 SG5760과 SG5760X 사이에는 사양 또는 기능 차이가 없습니다.

모델에는 다음과 같은 구성 요소가 포함되어 있습니다.

구성 요소	**SG5712**	**SG5712X**	**SG5760**	**SG5760X**
컴퓨팅 컨트롤러	E5500SG 컨트롤러	E5500SG 컨트롤러	E5500SG 컨트롤러	E5500SG 컨트롤러
스토리지 컨트롤러	E2800A 컨트롤러	E2800B 컨트롤러	E2800A 컨트롤러	E2800B 컨트롤러
섀시	E-Series DE212C 엔클로저, 2개의 랙 유닛(2U) 엔클로저	E-Series DE212C 엔클로저, 2개의 랙 유닛(2U) 엔클로저	E-Series DE460C 엔클로저, 4개의 랙 유닛(4U) 엔클로저	E-Series DE460C 엔클로저, 4개의 랙 유닛(4U) 엔클로저
드라이브	NL-SAS 드라이브 12개(3.5인치)	NL-SAS 드라이브 12개(3.5인치)	NL-SAS 드라이브 60개(3.5인치)	NL-SAS 드라이브 60개(3.5인치)
중복 전원 공급 장치 및 팬	2개의 전원 팬 캐니스터	2개의 전원 팬 캐니스터	두 개의 전원 캐니스터 및 두 개의 팬 캐니스터	두 개의 전원 캐니스터 및 두 개의 팬 캐니스터

StorageGRID 어플라이언스에서 사용할 수 있는 최대 기본 스토리지는 각 엔클로저의 드라이브 수에 따라 고정됩니다. 쉘프를 추가하려면 드라이브를 추가할 때 사용 가능한 스토리지를 확장할 수 없습니다.

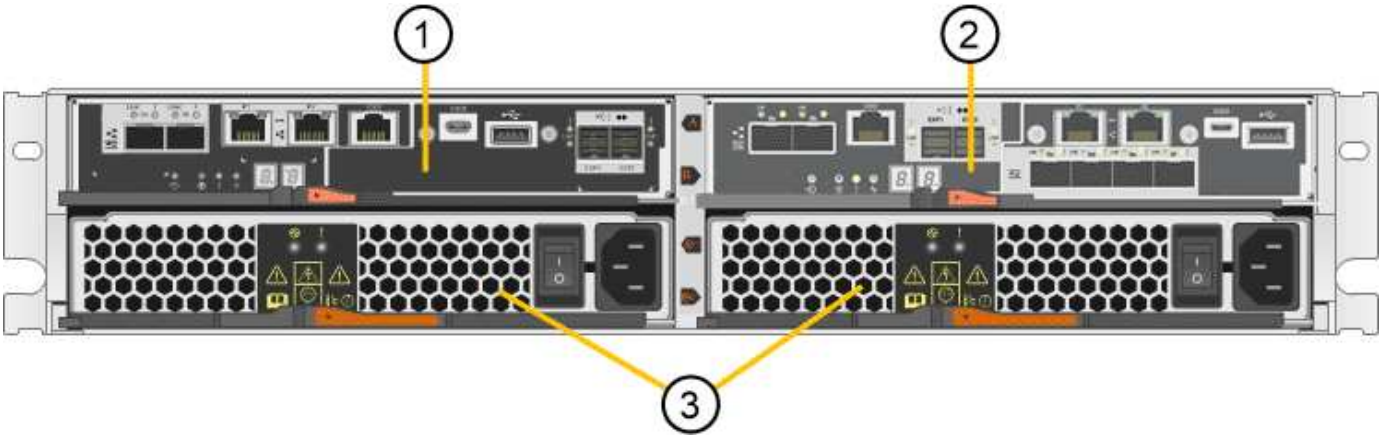
모델 **SG5712** 및 **5712X**

그림에서는 12개의 드라이브를 포함하는 2U 엔클로저인 SG5712 및 SG5712X 모델의 전면과 후면을 보여 줍니다.

- SG5712 전면 및 후면 모습 *

SG5712에는 컨트롤러 2개와 전원 팬 캐니스터 2개가 포함되어 있습니다.

- SG5712 구성 요소 *



속성 표시기	설명
1	E2800A 컨트롤러(스토리지 컨트롤러)
2	E5500SG 컨트롤러(컴퓨팅 컨트롤러)
3	전원 팬 캐니스터

- SG5712X 전면 및 후면 모습 *

SG5712X에는 컨트롤러 2개와 전원 팬 캐니스터 2개가 포함되어 있습니다.

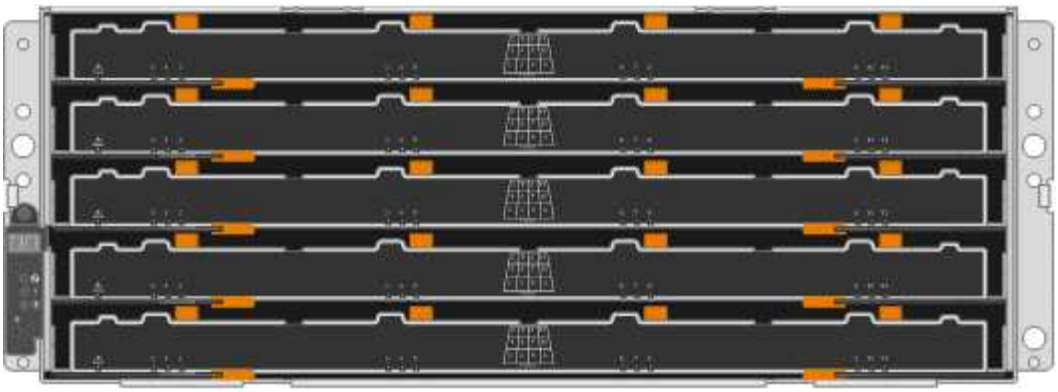
- SG5712X 구성 요소 *

속성 표시기	설명
1	E2800B 컨트롤러(스토리지 컨트롤러)
2	E5500SG 컨트롤러(컴퓨팅 컨트롤러)
3	전원 팬 캐니스터

모델 **SG5760** 및 **SG5760X**

그림에서는 SG5760 및 SG5760X 모델의 전면과 후면, 5개의 드라이브 드로어에 60개의 드라이브를 보관하는 4U 엔클로저를 보여 줍니다.

- SG5760 전면 및 후면 모습 *

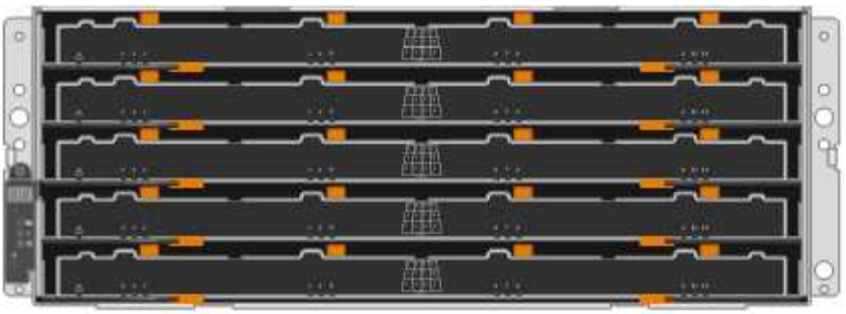


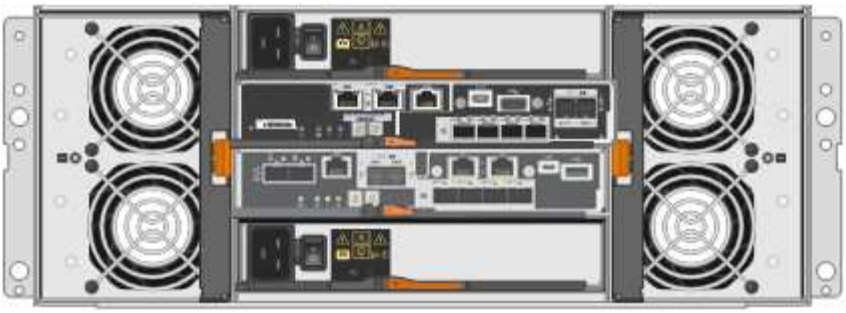
SG5760에는 컨트롤러 2개, 팬 캐니스터 2개, 전원 캐니스터 2개가 있습니다.

- SG5760 구성 요소 *

속성 표시기	설명
1	E2800A 컨트롤러(스토리지 컨트롤러)
2	E5500SG 컨트롤러(컴퓨팅 컨트롤러)
3	팬 캐니스터(1/2)
4	전원 캐니스터(1/2)

- SG5760X 전면 및 후면 모습 *





SG5760S에는 컨트롤러 2개, 팬 캐니스터 2개, 전원 캐니스터 2개가 있습니다.

- SG5760X 구성 요소 *

속성 표시기	설명
1	E2800B 컨트롤러(스토리지 컨트롤러)
2	E5500SG 컨트롤러(컴퓨팅 컨트롤러)
3	팬 캐니스터(1/2)
4	전원 캐니스터(1/2)

관련 정보

"NetApp E-Series 시스템 문서 사이트"

StorageGRID 5700 어플라이언스의 컨트롤러

StorageGRID 어플라이언스의 12 드라이브 SG5712 및 SG5712X 및 60 드라이브 SG5760 및 SG5760X 모델에는 모두 E5500SG 컴퓨팅 컨트롤러와 E-Series E2800 스토리지 컨트롤러가 포함됩니다.

- SG5712 및 SG5760은 E2800A 컨트롤러를 사용합니다.
- SG5712X 및 SG5760X는 E2800B 컨트롤러를 사용합니다.

```
The E2800A and E2800B controllers are identical in specification and
function except for the location of the interconnect ports.
```

컨트롤러 간의 차이점을 알아보려면 다이어그램을 검토해야 합니다.

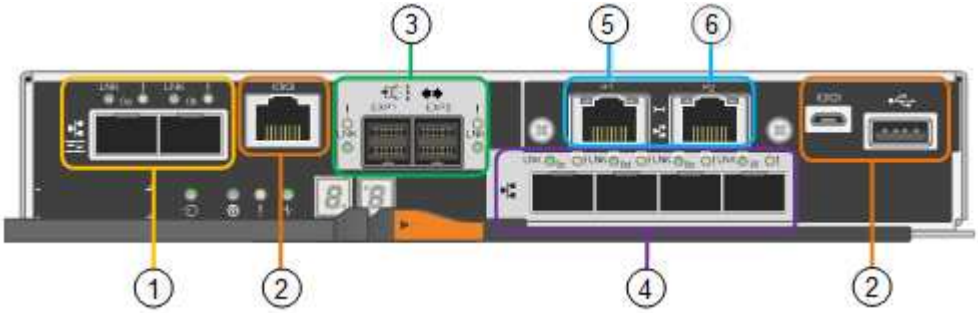
E5500SG 컨트롤러

- 어플라이언스의 컴퓨팅 서버로 작동합니다.
- StorageGRID 어플라이언스 설치 프로그램을 포함합니다.

> StorageGRID 소프트웨어는 어플라이언스에 사전 설치되어 있지 않습니다. 이 소프트웨어는 어플라이언스를 배포할 때 관리 노드에서 액세스합니다.

- 는 그리드 네트워크, 관리자 네트워크 및 클라이언트 네트워크를 포함하여 세 개의 StorageGRID 네트워크에 모두 연결할 수 있습니다.
- E2800 컨트롤러에 연결하고 이니시에이터로 작동합니다.

이 그림은 E5500SG 컨트롤러 후면의 커넥터를 보여 줍니다.



	포트	유형	사용
1	상호 연결 포트 1 및 2	16Gb/s 파이버 채널(FC), 광 SFPa	E5500SG 컨트롤러를 E2800 컨트롤러에 연결합니다.
2	진단 및 지원 포트	• RJ-45 직렬 포트 • 마이크로 USB 직렬 포트 • USB 포트	기술 지원용으로 예약되어 있습니다.
3	드라이브 확장 포트	12Gb/s SAS	사용 안 합니다. StorageGRID 어플라이언스는 확장 드라이브 쉘프를 지원하지 않습니다.

	포트	유형	사용
4	네트워크 포트 1-4	SFP 트랜시버 유형, 스위치 속도 및 구성된 링크 속도를 기반으로 한 10GbE 또는 25GbE	그리드 네트워크 및 StorageGRID용 클라이언트 네트워크에 연결합니다.
5	관리 포트 1	1Gb(RJ-45) 이더넷	StorageGRID용 관리자 네트워크에 연결합니다.
6	관리 포트 2	1Gb(RJ-45) 이더넷	옵션: • StorageGRID용 관리 네트워크에 대한 중복 연결을 위해 관리 포트 1과 연결합니다. • 유선을 해제하고 임시 로컬 액세스(IP 169.254.0.1)를 위해 사용 가능한 상태로 둡니다. • 설치하는 동안 DHCP 할당 IP 주소를 사용할 수 없는 경우 IP 구성에 포트 2를 사용합니다.

E2800 시리즈 스토리지 컨트롤러

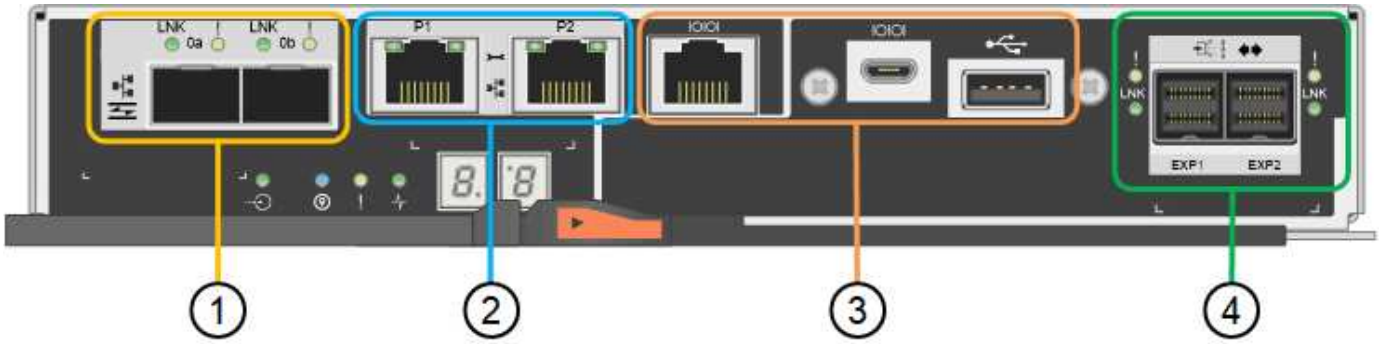
SG5700에는 E2800A 및 E2800B의 2가지 버전의 E2800 스토리지 컨트롤러가 사용됩니다. E2800A에는 HIC가 없으며 E2800B에는 4포트 HIC가 있습니다. 두 컨트롤러 버전은 상호 연결 포트의 위치를 제외하고 동일한 사양과 기능을 가집니다.

E2800 시리즈 스토리지 컨트롤러의 사양은 다음과 같습니다.

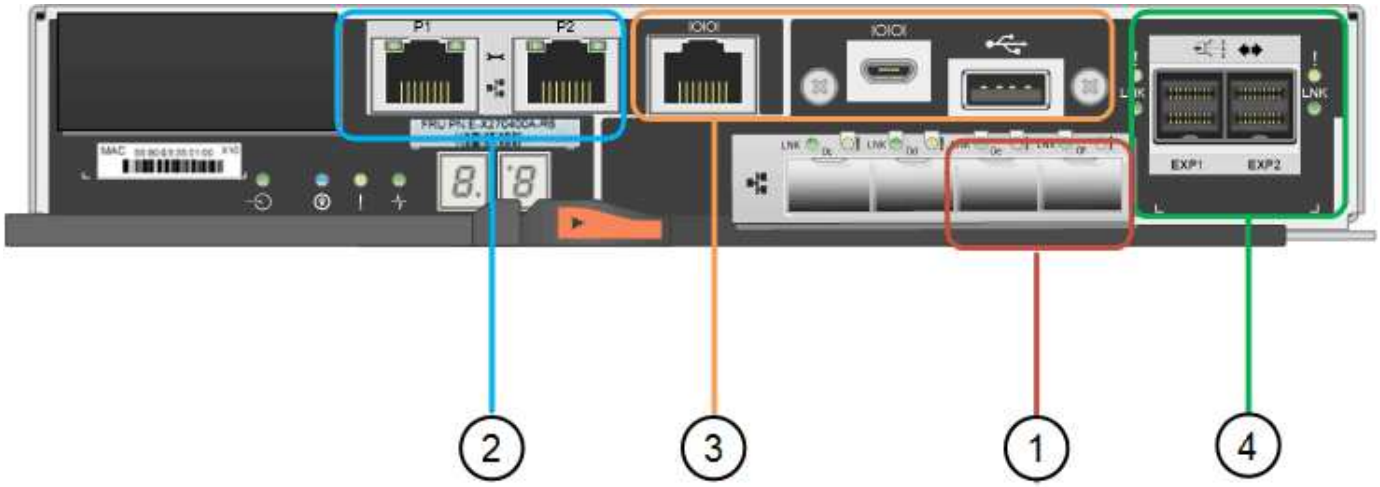
- 어플라이언스에 대한 스토리지 컨트롤러로 작동합니다.
- 드라이브의 데이터 스토리지를 관리합니다.
- 단일 모드에서 표준 E-Series 컨트롤러로 사용됩니다.
- SANtricity OS 소프트웨어(컨트롤러 펌웨어) 포함.
- 어플라이언스 하드웨어를 모니터링하고 경고, AutoSupport 기능 및 드라이브 보안 기능을 관리하기 위한 SANtricity System Manager를 포함합니다.
- E5500SG 컨트롤러에 연결하고 타겟으로 작동합니다.

다음 그림은 E2800A 및 E2800B 컨트롤러 후면의 커넥터를 보여줍니다.

- E2800A 뒷면의 커넥터 *



- E2800B 뒷면의 커넥터 *



	포트	유형	사용
1	상호 연결 포트 1 및 2	16Gb/s FC 광 SFPa	E2800 컨트롤러를 E5500SG 컨트롤러에 연결합니다.

	포트	유형	사용
2	관리 포트 1 및 2	1Gb(RJ-45) 이더넷	• 포트 1 옵션: ◦ 관리 네트워크에 연결하여 SANtricity 시스템 관리자에 대한 직접 TCP/IP 액세스를 활성화합니다 ◦ 스위치 포트 및 IP 주소를 저장하려면 유선 연결을 해제하십시오. 그리드 관리자 또는 스토리지 그리드 어플라이언스 설치 관리자 UI를 사용하여 SANtricity System Manager에 액세스합니다. • 참고 *: 정확한 로그 타임스탬프를 위한 NTP 동기화와 같은 일부 선택적 SANtricity 기능은 포트 1을 유선으로 남겨 두도록 선택한 경우 사용할 수 없습니다. • 참고 *: 포트 1을 유선으로 연결하지 않은 상태로 두면 StorageGRID 11.5 이상 및 SANtricity 11.70 이상이 필요합니다. • 포트 2는 기술 지원용으로 예약되어 있습니다.
3	진단 및 지원 포트	• RJ-45 직렬 포트 • 마이크로 USB 직렬 포트 • USB 포트	기술 지원용으로 예약되어 있습니다.
4	드라이브 확장 포트:	12Gb/s SAS	사용 안 합니다.

설치 및 구축 개요

StorageGRID를 처음 구축할 때 하나 이상의 StorageGRID 어플라이언스를 설치하거나 나중에 확장을 위해 어플라이언스 스토리지 노드를 추가할 수 있습니다. 복구 작업의 일부로 어플라이언스 스토리지 노드를 설치해야 할 수도 있습니다.

StorageGRID 스토리지 어플라이언스를 StorageGRID 시스템에 추가하는 작업은 다음과 같은 네 가지 주요 단계로 이루어집니다.

1. 설치 준비:
    - 설치 사이트 준비 중
    - 박스 포장 풀기 및 내용물 확인
    - 추가 장비 및 도구 확보
    - IP 주소 및 네트워크 정보를 수집하는 중입니다
    - 선택 사항: 모든 어플라이언스 데이터를 암호화하려는 경우 외부 키 관리 서버(KMS) 구성 StorageGRID 관리 지침에 있는 외부 키 관리에 대한 자세한 내용을 참조하십시오.
2. 하드웨어 설치:
    - 하드웨어를 등록하는 중입니다
    - 캐비닛 또는 랙에 제품 설치
    - 드라이브 설치(SG5760만 해당)
    - 어플라이언스 케이블 연결
    - 전원 코드 연결 및 전원 공급
    - 부팅 상태 코드 보기
3. 하드웨어 구성:
    - SANtricity System Manager에 액세스하여 E2800 컨트롤러에서 관리 포트 1의 정적 IP 주소를 설정하고 SANtricity System Manager 설정을 구성합니다
    - StorageGRID 어플라이언스 설치 프로그램에 액세스하고 StorageGRID 네트워크에 연결하는 데 필요한 링크 및 네트워크 IP 설정을 구성합니다
    - 선택 사항: 외부 KMS를 사용하여 어플라이언스 데이터를 암호화하려는 경우 노드 암호화 사용
    - 선택 사항: RAID 모드 변경
4. 어플라이언스를 스토리지 노드로 구축:

작업	지침
새로운 StorageGRID 시스템에 어플라이언스 스토리지 노드 구축	어플라이언스 스토리지 노드 구축
기존 StorageGRID 시스템에 어플라이언스 스토리지 노드 추가	StorageGRID 시스템 확장을 위한 지침

작업	지침
스토리지 노드 복구 작업의 일부로 어플라이언스 스토리지 노드 구축	복구 및 유지 관리 지침

관련 정보

설치 준비(SG5700)

하드웨어를 설치합니다

하드웨어 구성(SG5700)

VMware를 설치합니다

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

Ubuntu 또는 Debian을 설치합니다

SG100 및 SG1000 서비스 어플라이언스

그리드를 확장합니다

복구 및 유지 관리

StorageGRID 관리

설치 준비(SG5700)

StorageGRID 어플라이언스 설치를 준비하는 과정에서 사이트 준비 및 필요한 모든 하드웨어, 케이블 및 도구 확보 작업이 수반됩니다. 또한 IP 주소와 네트워크 정보도 수집해야 합니다.

관련 정보

웹 브라우저 요구 사항

사이트 준비(SG5700)

제품을 설치하기 전에 StorageGRID 어플라이언스의 사양을 충족하는 사이트와 캐비닛 또는 랙이 맞는지 확인해야 합니다.

단계

1. 사이트가 온도, 습도, 고도 범위, 공기 흐름, 열 손실 요구 사항을 충족하는지 확인합니다. 배선, 전원 및 접지. 자세한 내용은 NetApp Hardware Universe를 참조하십시오.
2. SG5760 모델을 설치하는 경우 해당 위치에서 240V AC 전원을 제공하는지 확인하십시오.
3. 이 크기의 선반에 맞게 19인치(48.3-cm) 캐비닛 또는 랙을 준비합니다(케이블 제외).

어플라이언스 모델	높이	너비	깊이	최대 중량
SG5712 (12개 드라이브)	3.41in. (8.68cm)	17.6인치 (44.7cm)	21.1in. (53.6cm)	63.9lb (29.0kg)
SG5760 (60개 드라이브)	6.87in. (17.46cm)	17.66in. (44.86cm)	38.25in. (97.16cm)	250lb. (113kg)

4. 필요한 네트워크 스위치를 설치합니다. 호환성 정보는 NetApp 상호 운용성 매트릭스 툴을 참조하십시오.

관련 정보

"NetApp Hardware Universe를 참조하십시오"

"NetApp 상호 운용성 매트릭스 툴"

박스 포장 풀기**(SG5700)**

StorageGRID 제품을 설치하기 전에 모든 상자의 포장을 풀고 내용물을 포장 명세서에 있는 품목과 비교합니다.

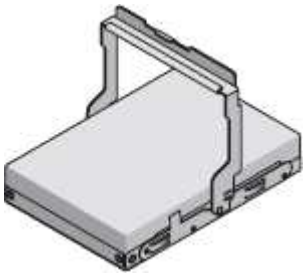
- 12개의 드라이브가 설치된 * SG5712 어플라이언스

- * 드라이브가 설치되지 않은 SG5760 어플라이언스 *

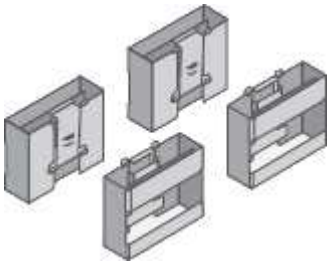
- * 제품의 전면 베젤 *

- * 지침이 포함된 레일 키트 *

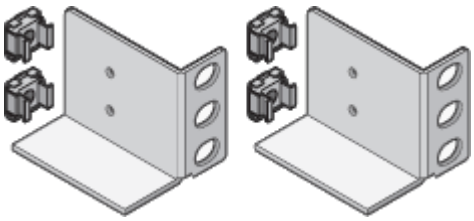
- * SG5760: 60개 드라이브 *



- * SG5760: 핸들 *



- * SG5760: 사각 구멍 랙 설치용 후면 브래킷 및 케이지 너트 *



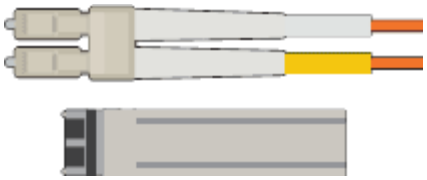
케이블 및 커넥터

StorageGRID 어플라이언스에는 다음과 같은 케이블 및 커넥터가 포함되어 있습니다.

- * 해당 국가용 전원 코드 2개 *

  캐비닛에는 제품과 함께 제공된 전원 코드 대신 사용하는 특수 전원 코드가 있을 수 있습니다.

- * 광 케이블 및 SFP 트랜시버 *



FC 상호 연결 포트를 위한 광 케이블 2개

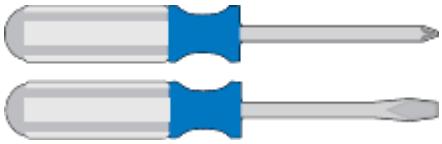
4개의 16Gb/s FC 상호 연결 포트 및 4개의 10GbE 네트워크 포트와 호환되는 8개의 SFP+ 트랜시버입니다

추가 장비 및 도구 확보**(SG5700)**

StorageGRID 제품을 설치하기 전에 필요한 추가 장비와 도구가 모두 있는지 확인하십시오.

하드웨어를 설치하고 구성하려면 다음 추가 장비가 필요합니다.

- * 스크류드라이버 *

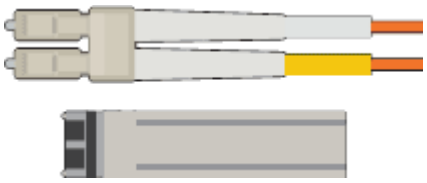


필립스 번호 2 드라이버

중형 일자 드라이버

- * ESD 손목 스트랩 *

- * 광 케이블 및 SFP 트랜시버 *



사용하려는 10/25-GbE 포트의 광 케이블

선택 사항: 25GbE 링크 속도를 사용하려는 경우 SFP28 트랜시버

- * 이더넷 케이블 *

- * 서비스 노트북 *

지원되는 웹 브라우저

PuTTY와 같은 SSH 클라이언트

1Gb(RJ-45) 이더넷 포트

- * 옵션 도구 *

Phillips 헤드 비트를 이용한 파워 드릴

플래시

SG5760의 기계식 리프트

어플라이언스 네트워크 연결 검토(**SG5700**)

StorageGRID 어플라이언스를 설치하기 전에 어플라이언스에 연결할 수 있는 네트워크와 각 컨트롤러의 포트가 어떻게 사용되는지 이해해야 합니다.

StorageGRID 어플라이언스 네트워크

StorageGRID 어플라이언스를 StorageGRID 그리드에 스토리지 노드로 구축할 경우 다음 네트워크에 연결할 수 있습니다.

- * StorageGRID * 용 그리드 네트워크: 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용됩니다. 그리드에서 모든 사이트 및 서브넷의 모든 노드 간에 연결을 제공합니다. 그리드 네트워크가 필요합니다.

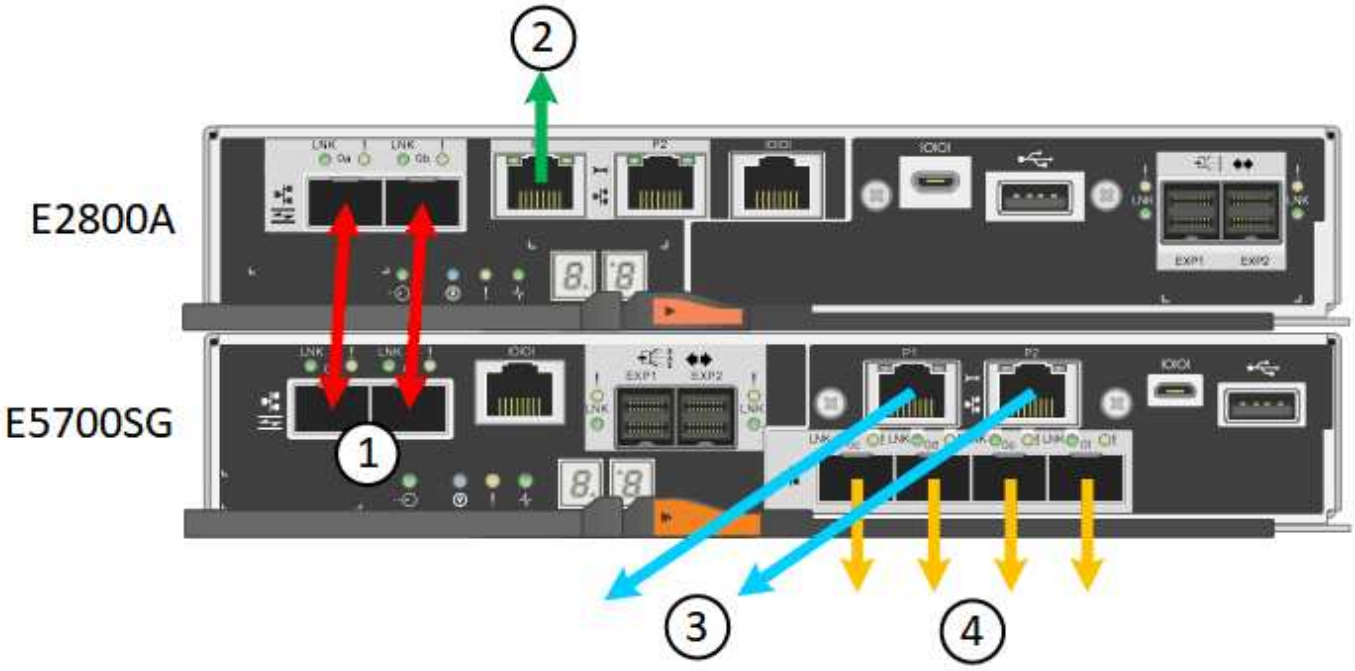
- StorageGRID*용 관리자 네트워크: 관리자 네트워크는 시스템 관리 및 유지 보수에 사용되는 폐쇄된 네트워크입니다. 관리 네트워크는 일반적으로 사설 네트워크이며 사이트 간에 라우팅할 필요가 없습니다. 관리 네트워크는 선택 사항입니다.
- * StorageGRID용 클라이언트 네트워크: * 클라이언트 네트워크는 S3 및 Swift를 포함한 클라이언트 애플리케이션에 대한 액세스를 제공하는 데 사용되는 개방형 네트워크입니다. 클라이언트 네트워크는 그리드에 대한 클라이언트 프로토콜 액세스를 제공하므로 그리드 네트워크를 격리하고 보호할 수 있습니다. 클라이언트 네트워크는 선택 사항입니다.
- * SANtricity 시스템 관리자용 관리 네트워크 * (선택 사항): 이 네트워크는 E2800 컨트롤러에서 SANtricity 시스템 관리자에 대한 액세스를 제공하므로 어플라이언스의 하드웨어 구성요소를 모니터링하고 관리할 수 있습니다. 이 관리 네트워크는 StorageGRID용 관리 네트워크와 같을 수도 있고 독립 관리 네트워크일 수도 있습니다.

  옵션 SANtricity System Manager 네트워크가 연결되지 않은 경우 일부 SANtricity 기능을 사용하지 못할 수 있습니다.

StorageGRID 네트워크에 대한 자세한 내용은 _Grid Primer_를 참조하십시오.

StorageGRID 어플라이언스 연결부

StorageGRID 어플라이언스를 설치할 경우 두 컨트롤러를 서로 필요한 네트워크에 연결해야 합니다. 이 그림은 SG5760의 컨트롤러 2개와 E2800 컨트롤러가 상단에 있고 E5500SG 컨트롤러 아래쪽은 입니다. SG5712에서 E2800 컨트롤러는 E5500SG 컨트롤러의 왼쪽에 있습니다.



	포트	포트의 유형입니다	기능
1	각 컨트롤러에 2개의 인터커넥트 포트	16Gb/s FC 광 SFP+	두 컨트롤러를 서로 연결합니다.

	포트	포트의 유형입니다	기능
2	E2800 컨트롤러의 관리 포트 1	1GbE(RJ-45)	SANtricity 시스템 관리자에 액세스하는 네트워크에 연결합니다. StorageGRID용 관리 네트워크 또는 독립 관리 네트워크를 사용할 수 있습니다.
2	E2800 컨트롤러의 관리 포트 2	1GbE(RJ-45)	기술 지원용으로 예약되어 있습니다.
3	E5500SG 컨트롤러의 관리 포트 1	1GbE(RJ-45)	StorageGRID용 관리 네트워크에 E5500SG 컨트롤러를 연결합니다.
3	E5500SG 컨트롤러의 관리 포트 2	1GbE(RJ-45)	• 관리 네트워크에 대한 중복 연결을 원할 경우 관리 포트 1에 연결할 수 있습니다. • 유선을 해제하고 임시 로컬 액세스(IP 169.254.0.1)에 사용할 수 있습니다. • 설치하는 동안 DHCP 할당 IP 주소를 사용할 수 없는 경우 E700SG 컨트롤러를 서비스 랩톱에 연결하는 데 사용할 수 있습니다.
4	E5500SG 컨트롤러의 10/25-GbE 포트 1-4	10GbE 또는 25GbE • 참고: * 어플라이언스에 포함된 SFP+ 트랜시버는 10GbE 링크 속도를 지원합니다. 네트워크 포트 4개에 25GbE 링크 속도를 사용하려면 SFP28 트랜시버를 제공해야 합니다.	그리드 네트워크 및 StorageGRID용 클라이언트 네트워크에 연결합니다. "'E700SG 컨트롤러의 10/25-GbE 포트 연결'을 참조하십시오."

관련 정보

설치 정보 수집(SG5700)

케이블 어플라이언스(SG5700)

E5500SG 컨트롤러 포트의 포트 연결 모드

네트워킹 지침

VMware를 설치합니다

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

Ubuntu 또는 Debian을 설치합니다

E5500SG 컨트롤러 포트의 포트 연결 모드

E5500SG 컨트롤러 포트에 대한 네트워크 링크를 구성할 때 그리드 네트워크 및 선택적 클라이언트 네트워크에 연결되는 10GbE/25GbE 포트와 선택적 관리 네트워크에 연결되는 1GbE 관리 포트에 포트 결합을 사용할 수 있습니다. 포트 본딩을 사용하면 StorageGRID 네트워크와 어플라이언스 간에 중복 경로를 제공하여 데이터를 보호할 수 있습니다.

관련 정보

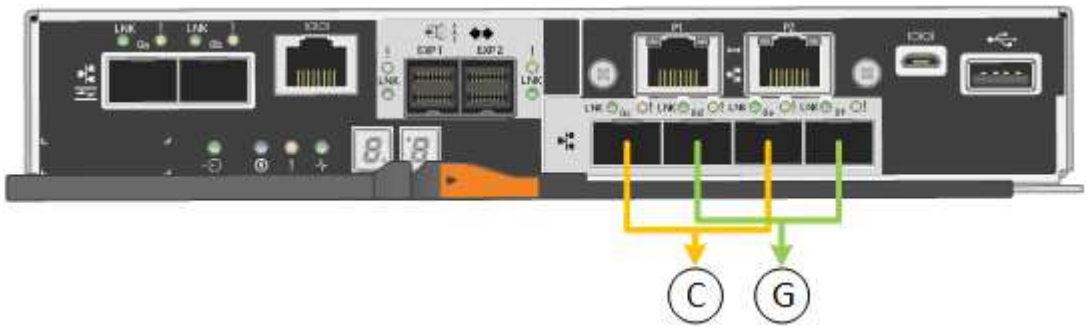
네트워크 링크 구성(SG5700)

10/25-GbE 포트의 네트워크 연결 모드

E5500SG 컨트롤러의 10/25GbE 네트워킹 포트는 그리드 네트워크 및 클라이언트 네트워크 연결을 위한 고정 포트 결합 모드 또는 애그리게이트 포트 결합 모드를 지원합니다.

고정 포트 결합 모드

고정 모드는 10/25-GbE 네트워킹 포트의 기본 구성입니다.



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
c	이 네트워크를 사용하는 경우 포트 1과 3이 클라이언트 네트워크에 대해 함께 연결됩니다.
g	포트 2와 4는 그리드 네트워크를 위해 서로 연결되어 있습니다.

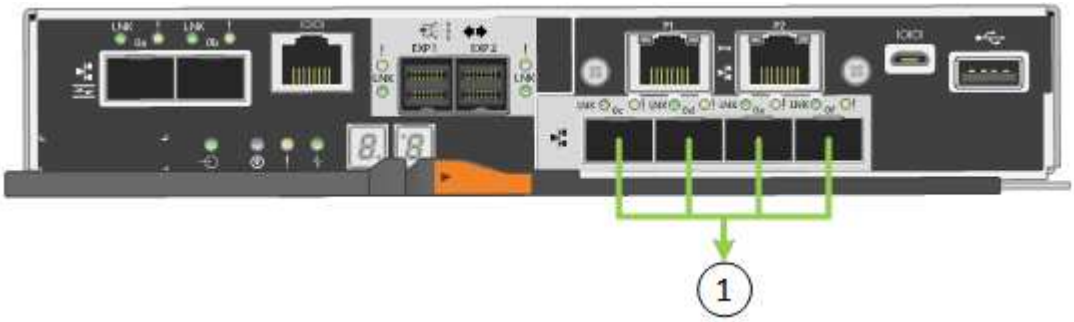
고정 포트 결합 모드를 사용하는 경우 두 가지 네트워크 결합 모드 중 하나인 액티브-백업 또는 링크 통합 제어 프로토콜(LACP) 중 하나를 사용할 수 있습니다.

- Active-Backup 모드(기본값)에서는 한 번에 하나의 포트만 활성화됩니다. 활성 포트에 장애가 발생하면 백업 포트가 자동으로 페일오버 연결을 제공합니다. 포트 4는 포트 2(그리드 네트워크)에 대한 백업 경로를 제공하고 포트 3은 포트 1(클라이언트 네트워크)에 대한 백업 경로를 제공합니다.
- LACP 모드에서 각 포트 쌍은 컨트롤러와 네트워크 간에 논리 채널을 형성하므로 더 높은 처리량을 허용합니다. 한 포트에 장애가 발생해도 다른 포트는 계속 채널을 제공합니다. 처리량은 감소하지만 연결성은 영향을 받지 않습니다.

> 중복 연결이 필요하지 않은 경우 각 네트워크에 대해 하나의 포트만 사용할 수 있습니다. 그러나 StorageGRID가 설치된 후 그리드 관리자에서 경보가 발생하므로 케이블이 분리되었음을 나타냅니다. 이 알람을 안전하게 확인할 수 있습니다.

애그리게이트 포트 결합 모드

애그리게이트 포트 결합 모드는 각 StorageGRID 네트워크의 성능을 크게 높이고 추가 페일오버 경로를 제공합니다.



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
1	연결된 모든 포트는 단일 LACP 결합으로 그룹화되므로 모든 포트를 그리드 네트워크 및 클라이언트 네트워크 트래픽에 사용할 수 있습니다.

Aggregate 포트 결합 모드를 사용하려는 경우:

- LACP 네트워크 결합 모드를 사용해야 합니다.
- 각 네트워크에 대해 고유한 VLAN 태그를 지정해야 합니다. 이 VLAN 태그는 네트워크 트래픽이 올바른 네트워크로 라우팅되도록 각 네트워크 패킷에 추가됩니다.
- VLAN 및 LACP를 지원할 수 있는 스위치에 포트를 연결해야 합니다. LACP 결합에 여러 스위치가 사용되는 경우 스위치는 MLAG(Multi-Chassis Link Aggregation Group) 또는 이와 동등한 스위치를 지원해야 합니다.
- VLAN, LACP, MLAG 또는 이와 동등한 기능을 사용하도록 스위치를 구성하는 방법을 이해해야 합니다.

4개의 10GbE 포트 모두를 사용하지 않으려면 1개, 2개 또는 3개의 포트를 사용할 수 있습니다. 둘 이상의 포트를 사용하면 10/25-GbE 포트 중 하나에 장애가 발생하더라도 일부 네트워크 연결이 계속 유지될 가능성을 극대화할 수 있습니다.

> 포트 수를 4개 이하로 선택하면 어플라이언스 노드가 설치된 후 그리드 관리자에서 * 서비스 어플라이언스 연결 해제 * 경고가 트리거되어 케이블이 분리되었음을 나타냅니다. 트리거된 경고에 대해 이 경고 규칙을 안전하게 비활성화할 수 있습니다. Grid Manager에서 * alerts * > * rules * 를 선택하고 규칙을 선택한 다음 * Edit rule * 을 클릭합니다. 그런 다음 * 사용 * 확인란의 선택을 취소합니다.

1GbE 관리 포트의 네트워크 연결 모드

E5500SG 컨트롤러에 있는 2개의 1GbE 관리 포트의 경우 독립 네트워크 연결 모드 또는 Active-Backup 네트워크 연결 모드를 선택하여 옵션 관리 네트워크에 연결할 수 있습니다.

독립 모드에서는 관리 포트 1만 관리 네트워크에 연결됩니다. 이 모드는 중복 경로를 제공하지 않습니다. 관리 포트 2는 유선으로 남겨두고 임시 로컬 연결에 사용할 수 있습니다(IP 주소 169.254.0.1 사용).

Active-Backup 모드에서는 관리 포트 1과 2가 모두 관리 네트워크에 연결됩니다. 한 번에 하나의 포트만 활성화됩니다. 활성 포트에 장애가 발생하면 백업 포트가 자동으로 페일오버 연결을 제공합니다. 이러한 두 개의 물리적 포트를 하나의 논리 관리 포트에 연결하면 관리 네트워크에 대한 중복 경로가 제공됩니다.

> 1GbE 관리 포트가 Active-Backup 모드로 구성되어 있을 때 E5500SG 컨트롤러에 임시로 로컬 연결해야 하는 경우, 두 관리 포트에서 케이블을 분리하고 임시 케이블을 관리 포트 2에 연결한 다음 IP 주소 169.254.0.1을 사용하여 어플라이언스에 액세스합니다.

설치 정보 수집**(SG5700)**

StorageGRID 어플라이언스를 설치 및 구성할 때 이더넷 스위치 포트, IP 주소, 포트 및 네트워크 연결 모드에 대한 정보를 결정하고 수집해야 합니다.

이 작업에 대해

다음 표를 사용하여 어플라이언스에 연결하는 각 네트워크에 필요한 정보를 기록할 수 있습니다. 이러한 값은 하드웨어를 설치하고 구성하는 데 필요합니다.

E2800 컨트롤러의 **SANtricity System Manager**에 연결하는 데 필요한 정보입니다

E2800 컨트롤러를 SANtricity 시스템 관리자에 사용할 관리 네트워크에 연결해야 합니다.

정보가 필요합니다	귀사의 가치
관리 포트 1에 연결할 이더넷 스위치 포트	
관리 포트 1의 MAC 주소(E2800A 컨트롤러의 경우 포트 P1, E2800B 컨트롤러의 경우 0a 근처의 레이블에 인쇄되어 있음)	

정보가 필요합니다	귀사의 가치
전원을 켠 후 사용할 수 있는 경우 관리 포트 1에 대해 DHCP 할당 IP 주소입니다 • 참고: * E2800 컨트롤러에 연결할 네트워크에 DHCP 서버가 포함된 경우 네트워크 관리자는 MAC 주소를 사용하여 DHCP 서버에서 할당한 IP 주소를 확인할 수 있습니다.	
속도 및 이중 모드 • 참고: * SANtricity 시스템 관리자 관리 네트워크의 이더넷 스위치가 자동 교섭으로 설정되어 있는지 확인해야 합니다.	반드시: • 자동 협상(기본값)
IP 주소 형식입니다	다음 중 하나를 선택하십시오. • IPv4 • IPv6
관리 네트워크에서 어플라이언스에 사용할 고정 IP 주소입니다	IPv4의 경우: • IPv4 주소: • 서브넷 마스크: • 게이트웨이: IPv6의 경우: • IPv6 주소: • 라우팅 가능한 IP 주소: • E2800 컨트롤러 라우터 IP 주소:

E700SG 컨트롤러를 관리 네트워크에 연결하는 데 필요한 정보입니다

StorageGRID용 관리 네트워크는 시스템 관리 및 유지 보수에 사용되는 선택적 네트워크입니다. 어플라이언스는 E5500SG 컨트롤러의 1GbE 관리 포트를 사용하여 관리 네트워크에 연결됩니다.

정보가 필요합니다	귀사의 가치
관리자 네트워크가 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요 • 예(기본값)

정보가 필요합니다	귀사의 가치
네트워크 연결 모드	다음 중 하나를 선택하십시오. • 독립적입니다 • Active - 백업
포트 1의 스위치 포트	
포트 2용 스위치 포트(Active-Backup 네트워크 연결 모드만 해당)	
전원을 켠 후 사용할 수 있는 경우 관리 포트 1에 대해 DHCP 할당 IP 주소입니다 • 참고: * 관리 네트워크에 DHCP 서버가 포함된 경우, E700SG 컨트롤러는 부팅 후 7개 세그먼트 디스플레이에 DHCP 할당 IP 주소를 표시합니다. MAC 주소를 사용하여 할당된 IP를 조회하여 DHCP 할당 IP 주소를 확인할 수도 있습니다.	• IPv4 주소(CIDR): • 게이트웨이:
관리 네트워크의 어플라이언스 스토리지 노드에 사용할 고정 IP 주소입니다 • 참고: * 네트워크에 게이트웨이가 없는 경우 게이트웨이에 대해 동일한 정적 IPv4 주소를 지정합니다.	• IPv4 주소(CIDR): • 게이트웨이:
관리 네트워크 서브넷(CIDR)	

E5500SG 컨트롤러에서 **10/25-GbE** 포트를 연결 및 구성하는 데 필요한 정보입니다

E5500SG 컨트롤러에 있는 4개의 10/25-GbE 포트는 StorageGRID 그리드 네트워크 및 클라이언트 네트워크에 연결됩니다.

> 이러한 포트의 옵션에 대한 자세한 내용은 "E5500SG 컨트롤러의 10/25-GbE 포트 연결"을 참조하십시오.

정보가 필요합니다	귀사의 가치
링크 속도 • 참고: * 25GbE를 선택한 경우 SPF28 트랜시버를 설치해야 합니다. 자동 협상은 지원되지 않으므로 25GbE 포트 및 연결된 스위치도 구성해야 합니다.	다음 중 하나를 선택하십시오. • 10GbE(기본값) • 25GbE

정보가 필요합니다	귀사의 가치
포트 결합 모드	다음 중 하나를 선택하십시오. • 고정(기본값) • 집계
포트 1용 스위치 포트(클라이언트 네트워크)	
포트 2용 스위치 포트(그리드 네트워크)	
포트 3용 스위치 포트(클라이언트 네트워크)	
포트 4용 스위치 포트(그리드 네트워크)	

E700SG 컨트롤러를 그리드 네트워크에 연결하는 데 필요한 정보입니다

StorageGRID용 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용되는 필수 네트워크입니다. 이 어플라이언스는 E5500SG 컨트롤러의 10/25-GbE 포트를 사용하여 그리드 네트워크에 연결됩니다.

> 이러한 포트의 옵션에 대한 자세한 내용은 "E5500SG 컨트롤러의 10/25-GbE 포트 연결"을 참조하십시오.

정보가 필요합니다	귀사의 가치
네트워크 연결 모드	다음 중 하나를 선택하십시오. • Active-Backup(기본값) • LACP(802.3ad)
VLAN 태그 지정이 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요(기본값) • 예
VLAN 태그(VLAN 태그 지정이 활성화된 경우)	0에서 4095 사이의 값을 입력합니다.
전원을 켠 후 사용할 수 있는 경우 그리드 네트워크에 대해 DHCP 할당 IP 주소입니다 • 참고: * 그리드 네트워크에 DHCP 서버가 포함된 경우, E700SG 컨트롤러는 부팅된 후 7세그먼트 디스플레이에 그리드 네트워크에 대해 DHCP 할당 IP 주소를 표시합니다.	• IPv4 주소(CIDR): • 게이트웨이:

정보가 필요합니다	귀사의 가치
그리드 네트워크에서 어플라이언스 스토리지 노드에 사용할 고정 IP 주소입니다 • 참고: * 네트워크에 게이트웨이가 없는 경우 게이트웨이에 대해 동일한 정적 IPv4 주소를 지정합니다.	• IPv4 주소(CIDR): • 게이트웨이:
그리드 네트워크 서브넷(CIDR) • 참고: * 클라이언트 네트워크가 활성화되지 않은 경우 컨트롤러의 기본 라우트는 여기에 지정된 게이트웨이를 사용합니다.	

E700SG 컨트롤러를 클라이언트 네트워크에 연결하는 데 필요한 정보입니다

StorageGRID용 클라이언트 네트워크는 일반적으로 그리드에 대한 클라이언트 프로토콜 액세스를 제공하는 데 사용되는 선택적 네트워크입니다. 어플라이언스는 E5500SG 컨트롤러의 10/25-GbE 포트를 사용하여 클라이언트 네트워크에 연결됩니다.

> 이러한 포트의 옵션에 대한 자세한 내용은 "E5500SG 컨트롤러의 10/25-GbE 포트 연결"을 참조하십시오.

정보가 필요합니다	귀사의 가치
클라이언트 네트워크가 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요(기본값) • 예
네트워크 연결 모드	다음 중 하나를 선택하십시오. • Active-Backup(기본값) • LACP(802.3ad)
VLAN 태그 지정이 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요(기본값) • 예
VLAN 태그 (VLAN 태그 지정이 설정된 경우)	0에서 4095 사이의 값을 입력합니다.

정보가 필요합니다	귀사의 가치
전원을 켠 후 사용할 수 있는 경우 클라이언트 네트워크에 대해 DHCP 할당 IP 주소입니다	• IPv4 주소(CIDR): • 게이트웨이:
클라이언트 네트워크의 어플라이언스 스토리지 노드에 사용할 고정 IP 주소입니다 • 참고: * 클라이언트 네트워크가 활성화된 경우 컨트롤러의 기본 라우트는 여기에 지정된 게이트웨이를 사용합니다.	• IPv4 주소(CIDR): • 게이트웨이:

관련 정보

어플라이언스 네트워크 연결 검토(SG5700)

E5500SG 컨트롤러 포트의 포트 연결 모드

하드웨어 구성(SG5700)

하드웨어 설치(SG5700)

하드웨어 설치에는 제품을 캐비닛이나 랙에 설치하고, 케이블을 연결하고, 전원을 공급해야 합니다.

하드웨어 등록

어플라이언스 하드웨어를 등록하면 지원 혜택이 제공됩니다.

단계

1. 섀시 일련 번호를 찾습니다.

   포장 명세서, 확인 이메일 또는 제품의 포장을 푼 후 제품에서 번호를 확인할 수 있습니다.

2. NetApp Support 사이트 로 이동합니다 "mysupport.netapp.com".
3. 하드웨어를 등록해야 하는지 여부를 확인합니다.

귀하의 경우...	다음 단계를 따르십시오...
더 많은 워크로드 추가)	a. 사용자 이름과 암호를 사용하여 로그인합니다. b. 제품 * > * 내 제품 * 을 선택합니다. c. 새 일련 번호가 나열되는지 확인합니다. d. 그렇지 않은 경우 새 NetApp 고객에 대한 지침을 따르십시오.

귀하의 경우...	다음 단계를 따르십시오...
신규 NetApp 고객	a. 지금 등록 * 을 클릭하고 계정을 만듭니다. b. 제품 * > * 제품 등록 * 을 선택합니다. c. 제품 일련 번호 및 요청된 세부 정보를 입력합니다. 등록이 승인되면 필요한 소프트웨어를 다운로드할 수 있습니다. 승인 프로세스는 최대 24시간이 걸릴 수 있습니다.

캐비닛 또는 랙에 어플라이언스 설치**(SG5700)**

캐비닛이나 랙에 레일을 설치한 다음 제품을 레일에 밀어 넣으십시오. SG5760을 사용하는 경우 어플라이언스를 설치한 후 드라이브도 설치해야 합니다.

필요한 것

- 상자에 포함된 안전 고지 문서를 검토하고 하드웨어 이동 및 설치에 대한 예방 조치를 이해했습니다.
- 레일 키트와 함께 제공된 지침이 있습니다.
- 본 제품의 설치 및 설정 방법은 _ 입니다.

장비가 넘어지지 않도록 랙 또는 캐비닛 또는 랙의 하단에서 하드웨어를 설치하십시오.

SG5712의 중량은 드라이브와 함께 완전히 장착된 경우 약 29kg(64lb)입니다. SG5712를 안전하게 옮기려면 2명 또는 기계화된 리프트가 필요합니다.

SG5760의 중량은 드라이브가 설치되지 않은 상태에서 약 60kg(132lb)입니다. 빈 SG5760을 안전하게 옮기려면 4명 또는 기계화된 리프트가 필요합니다.

하드웨어 손상을 방지하려면 드라이브가 설치된 경우 SG5760을 이동하지 마십시오. 쉘프를 이동하기 전에 모든 드라이브를 제거해야 합니다.

단계

1. 레일 키트의 지침에 따라 캐비닛이나 랙에 레일을 설치합니다.
2. SG5760을 사용하는 경우, 어플라이언스 이동을 준비하려면 다음 단계를 따르십시오.
   a. 외부 포장 상자를 제거합니다. 그런 다음 안쪽 상자의 플랩을 아래로 접습니다.
   b. SG5760을 손으로 들어올릴 경우, 섀시의 측면에 4개의 핸들을 부착합니다.

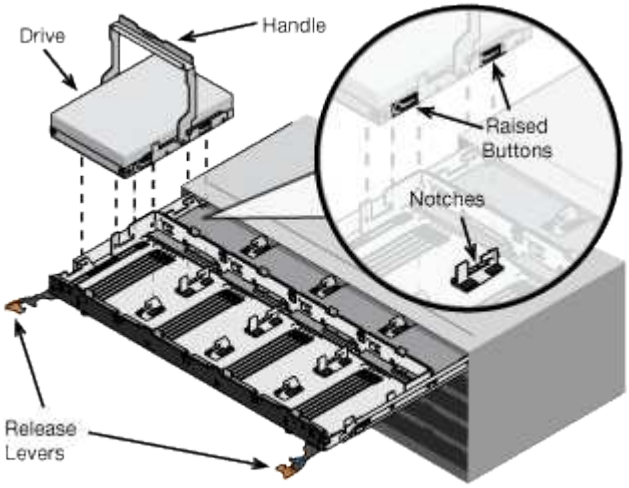
      제품을 레일에 밀어 넣을 때 손잡이를 분리하십시오.
3. 설치 및 설정 지침 _ 을(를) 참조하여 제품을 캐비닛 또는 랙에 밀어 넣습니다.
4. 설치 및 설정 지침 _ 을(를) 참조하여 제품을 캐비닛이나 랙에 고정합니다.

   SG5760을 사용하는 경우, 후면 브래킷을 사용하여 제품을 랙 또는 캐비닛 후면에 고정시키십시오. 랙 또는 캐비닛에 사각 구멍이 있는 경우 케이지 너트를 사용하십시오.

5. SG5760을 사용하는 경우 5개의 드라이브 드로어에 12개의 드라이브를 설치합니다.

   올바르게 작동하려면 60개의 드라이브를 모두 설치해야 합니다.

   a. ESD 밴드를 착용하고 포장재에서 드라이브를 제거합니다.
   b. 상단 드라이브 드로어의 레버를 분리하고 레버를 사용하여 드로어를 밀어 꺼냅니다.
   c. 드라이브 손잡이를 수직으로 올리고 드라이브의 단추를 드로어의 노치에 맞춥니다.



   d. 드라이브 상단을 부드럽게 눌러 드라이브가 제자리에 끼워질 때까지 드라이브 핸들을 아래로 돌립니다.
   e. 처음 12개의 드라이브를 설치한 후 중앙을 누르고 양쪽 레버를 부드럽게 닫아 드로어를 다시 밀어 넣습니다.
   f. 다른 4개의 문서함에 대해 이 단계를 반복합니다.
6. 전면 베젤을 부착합니다.

케이블 어플라이언스(**SG5700** 시리즈)

두 컨트롤러를 서로 연결하고, 각 컨트롤러의 관리 포트를 연결한 다음, E5500SG 컨트롤러의 10/25-GbE 포트를 그리드 네트워크 및 StorageGRID용 클라이언트 네트워크 옵션에 연결해야 합니다.

필요한 것

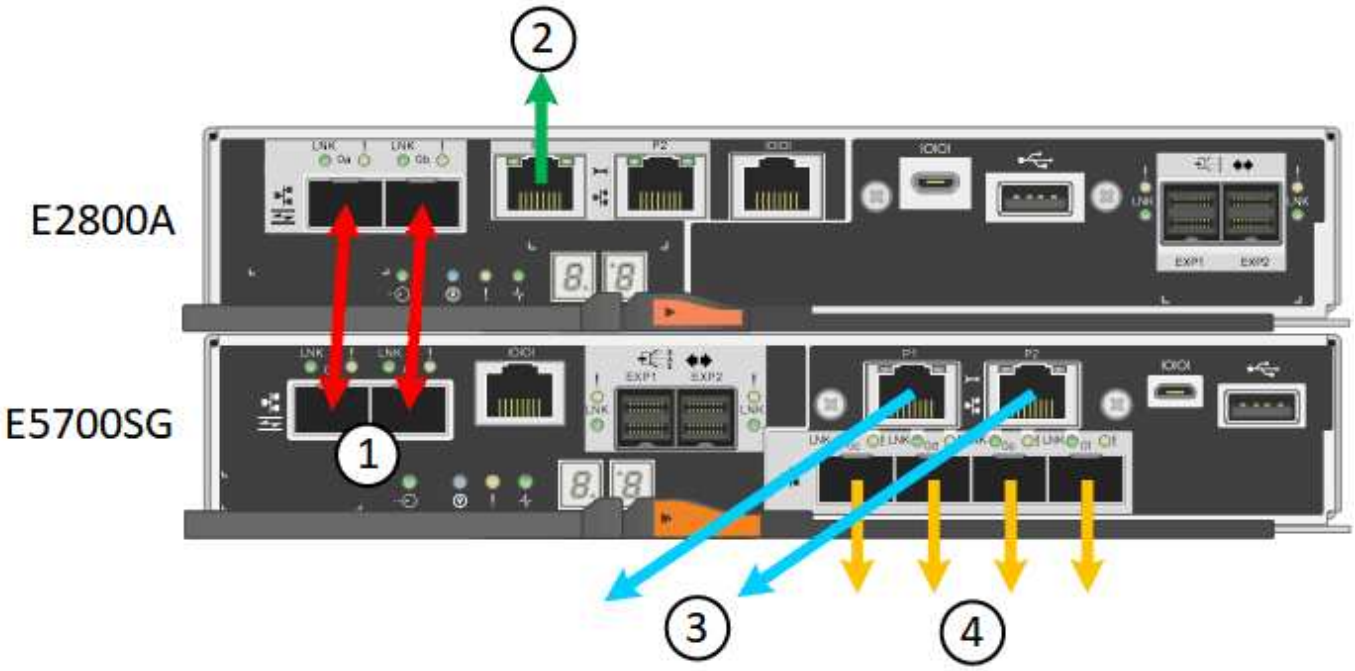
- 제품에 포함된 다음 품목을 개봉했습니다.
  - 전원 코드 2개
  - 컨트롤러의 FC 인터커넥트 포트에 대한 광 케이블 2개.
  - 10GbE 또는 16Gbps FC를 지원하는 SFP+ 트랜시버 8개 트랜시버는 두 컨트롤러의 상호 연결 포트 2개와 E700SG 컨트롤러의 10/25-GbE 네트워크 포트 4개와 함께 사용할 수 있습니다. 단, 네트워크 포트에서 10GbE 링크 속도를 사용하려는 경우에는 가능합니다.
- 다음 품목은 제품에 포함되어 있지 않습니다.
  - 사용하려는 10/25-GbE 포트에 대해 1-4개의 광 케이블을 사용합니다.
  - 25-GbE 링크 속도를 사용하려는 경우 SFP28 트랜시버 1~4개
  - 관리 포트 연결용 이더넷 케이블

* 레이저 방사선에 노출될 위험 * — SFP 트랜시버를 분해하거나 제거하지 마십시오. 레이저 방사선에 노출될 수 있습니다.

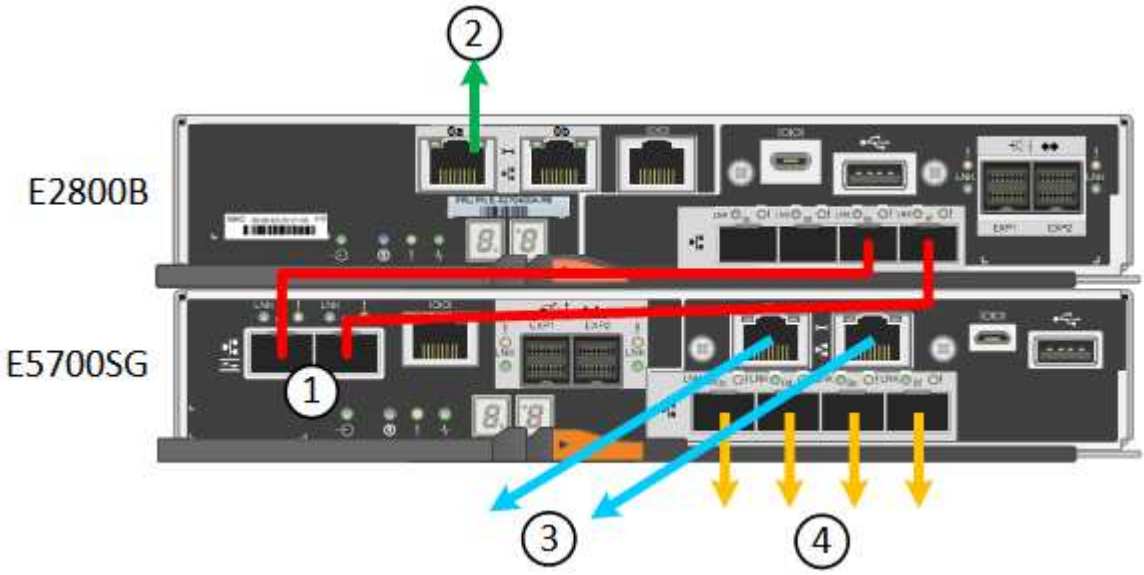
이 작업에 대해

이 그림은 SG5760 및 SG5760X의 컨트롤러 2개와 E2800 시리즈 스토리지 컨트롤러 위쪽 및 E5500SG 컨트롤러 맨 아래에 있는 컨트롤러 2개를 보여 줍니다. SG5712 및 SG5712X에서는 E2800 시리즈 스토리지 컨트롤러를 후면에서 볼 때 E5500SG 컨트롤러의 왼쪽에 연결합니다.

- SG5760 연결 *



- SG5760X 연결 *



	포트	포트의 유형입니다	기능
1	각 컨트롤러에 2개의 인터커넥트 포트	16Gb/s FC 광 SFP+	두 컨트롤러를 서로 연결합니다.
2	E2800 시리즈 컨트롤러의 관리 포트 1	1GbE(RJ-45)	SANtricity 시스템 관리자에 액세스하는 네트워크에 연결합니다. StorageGRID용 관리 네트워크 또는 독립 관리 네트워크를 사용할 수 있습니다.
2	E2800 시리즈 컨트롤러의 관리 포트 2	1GbE(RJ-45)	기술 지원용으로 예약되어 있습니다.
3	E5500SG 컨트롤러의 관리 포트 1	1GbE(RJ-45)	StorageGRID용 관리 네트워크에 E5500SG 컨트롤러를 연결합니다.
3	E5500SG 컨트롤러의 관리 포트 2	1GbE(RJ-45)	• 관리 네트워크에 대한 중복 연결을 원할 경우 관리 포트 1에 연결할 수 있습니다. • 유선을 해제하고 임시 로컬 액세스(IP 169.254.0.1)에 사용할 수 있습니다. • 설치하는 동안 DHCP 할당 IP 주소를 사용할 수 없는 경우 E700SG 컨트롤러를 서비스 랩톱에 연결하는 데 사용할 수 있습니다.
4	E5500SG 컨트롤러의 10/25-GbE 포트 1-4	10GbE 또는 25GbE • 참고: * 어플라이언스에 포함된 SFP+ 트랜시버는 10GbE 링크 속도를 지원합니다. 네트워크 포트 4개에 25GbE 링크 속도를 사용하려면 SFP28 트랜시버를 제공해야 합니다.	그리드 네트워크 및 StorageGRID용 클라이언트 네트워크에 연결합니다. "'E700SG 컨트롤러의 10/25-GbE 포트 연결'을 참조하십시오."

단계

1. 광 케이블 2개와 SFP+ 트랜시버 8개 중 4개를 사용하여 E2800 컨트롤러를 E5500SG 컨트롤러에 연결합니다.

이 포트 연결...	이 포트로...
E2800 컨트롤러의 상호 연결 포트 1입니다	E5500SG 컨트롤러의 상호 연결 포트 1
E2800 컨트롤러의 상호 연결 포트 2	E5500SG 컨트롤러의 상호 연결 포트 2

2. SANtricity System Manager를 사용하려면 이더넷 케이블을 사용하여 E2800 컨트롤러(왼쪽의 RJ-45 포트)의 관리 포트 1(E2800A의 P1, E2800B의 0a)을 SANtricity System Manager용 관리 네트워크에 연결합니다.

   E2800 컨트롤러(오른쪽의 RJ-45 포트)에서 관리 포트 2(E2800A의 P2 및 E2800B의 0b)를 사용하지 마십시오. 이 포트는 기술 지원을 위해 예약되어 있습니다.

3. StorageGRID용 관리 네트워크를 사용하려는 경우 이더넷 케이블을 사용하여 E5500SG 컨트롤러(왼쪽의 RJ-45 포트)의 관리 포트 1을 관리 네트워크에 연결합니다.

   관리 네트워크에 대해 액티브-백업 네트워크 연결 모드를 사용하려는 경우 이더넷 케이블을 사용하여 E700SG 컨트롤러(오른쪽의 RJ-45 포트)의 관리 포트 2를 관리 네트워크에 연결합니다.

4. 광 케이블과 SFP+ 또는 SFP28 트랜시버를 사용하여 E5500SG 컨트롤러의 10/25-GbE 포트를 해당 네트워크 스위치에 연결합니다.

   > 모든 포트는 동일한 링크 속도를 사용해야 합니다. 10GbE 링크 속도를 사용하려는 경우 SFP+ 트랜시버를 설치합니다. 25GbE 링크 속도를 사용하려는 경우 SFP28 트랜시버를 설치합니다.

   - 고정 포트 결합 모드(기본값)를 사용하려는 경우 표 에 나와 있는 대로 포트를 StorageGRID 그리드 및 클라이언트 네트워크에 연결합니다.

포트	연결 대상...
포트 1	클라이언트 네트워크(옵션)
포트 2	그리드 네트워크
포트 3	클라이언트 네트워크(옵션)
포트 4	그리드 네트워크

   - Aggregate 포트 결합 모드를 사용하려는 경우 하나 이상의 네트워크 포트를 하나 이상의 스위치에 연결합니다. 단일 장애 지점이 발생하지 않도록 4개 포트 중 2개 이상을 연결해야 합니다. 단일 LACP 결합에 둘 이상의 스위치를 사용하는 경우 스위치는 MLAG 또는 동급 스위치를 지원해야 합니다.

관련 정보

StorageGRID 어플라이언스 설치 프로그램에 액세스합니다

E5500SG 컨트롤러 포트의 포트 연결 모드

전원 코드 연결 및 전원 공급**(SG5700)**

어플라이언스에 전원을 공급하면 두 컨트롤러가 모두 부팅됩니다.

필요한 것

전원을 연결하기 전에 두 제품의 전원 스위치를 모두 꺼야 합니다.

* 감전 위험 * — 전원 코드를 연결하기 전에 제품의 두 전원 스위치가 꺼져 있는지 확인하십시오.

단계

1. 제품의 전원 스위치 2개가 꺼져 있는지 확인하십시오.
2. 전원 코드 2개를 제품에 연결합니다.
3. 2개의 전원 코드를 캐비닛이나 랙의 서로 다른 PDU(Power Distribution Unit)에 연결합니다.
4. 제품의 전원 스위치 2개를 켜십시오.
   - 전원을 켜는 동안 전원 스위치를 끄지 마십시오.
   - 팬이 처음 시작될 때 매우 시끄럽습니다. 시동 중 큰 소음이 정상입니다.
5. 컨트롤러가 부팅된 후 7개의 세그먼트 디스플레이를 확인합니다.

SG5700 부팅 상태 코드를 봅니다

각 컨트롤러에 7개의 세그먼트가 표시되면 어플라이언스 전원이 켜질 때 상태 및 오류 코드가 표시됩니다.

이 작업에 대해

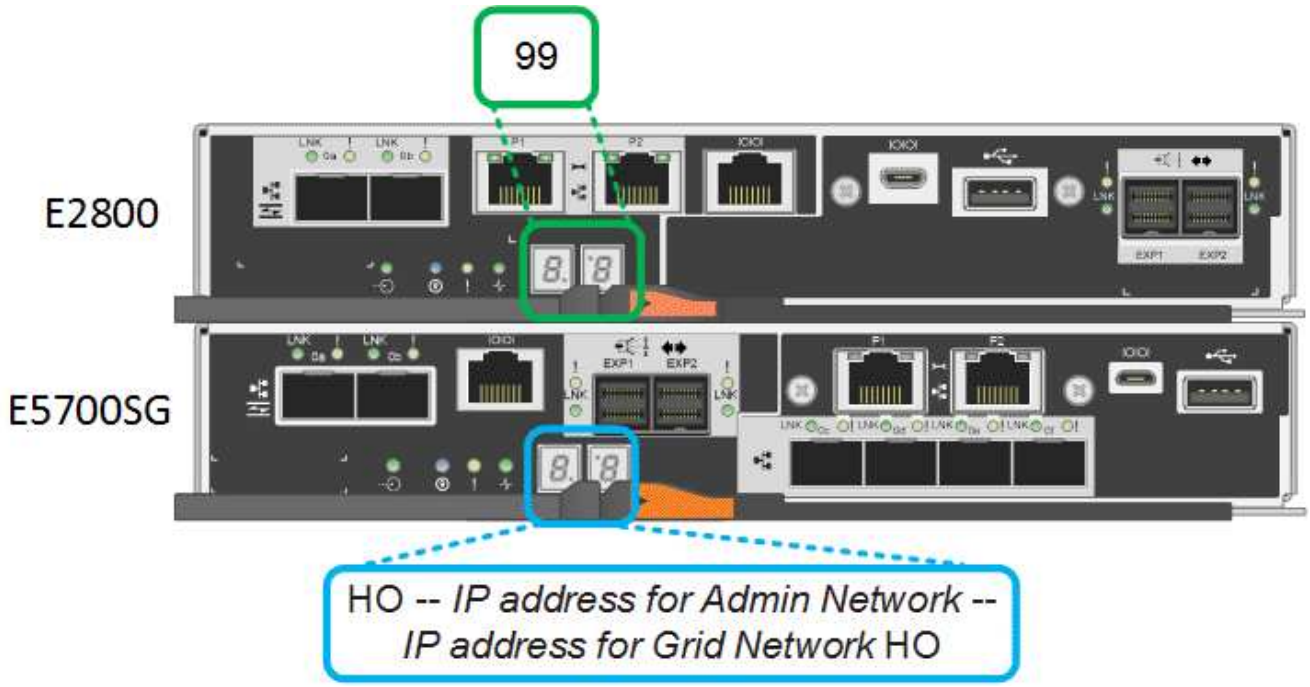
E2800 컨트롤러 및 E5500SG 컨트롤러는 다양한 상태 및 오류 코드를 표시합니다.

이러한 코드의 의미를 이해하려면 다음 리소스를 참조하십시오.

컨트롤러	참조하십시오
E2800 컨트롤러	_E5700 및 E2800 시스템 모니터링 가이드 _ • 참고: * E-Series E5700 컨트롤러에 대해 나열된 코드는 어플라이언스의 E5500SG 컨트롤러에 적용되지 않습니다.
E5500SG 컨트롤러	"E5700SG 컨트롤러의 상태 표시기"

단계

1. 부팅 중에 7세그먼트 디스플레이에 표시된 코드를 확인하여 진행 상황을 모니터링합니다.
   - E2800 컨트롤러의 7세그먼트 디스플레이에는 * OS *, * SD *, ' **blank* * ' 반복 시퀀스가 표시되어 시작 프로세싱을 수행하고 있음을 나타냅니다.
   - E5500SG 컨트롤러의 7개 세그먼트 디스플레이에는 * AA * 및 * FF * 로 끝나는 코드 시퀀스가 표시됩니다.
2. 컨트롤러가 부팅된 후 7세그먼트 디스플레이에 다음이 표시되는지 확인합니다.



컨트롤러	7개 세그먼트 디스플레이
E2800 컨트롤러	에는 99가 나와 있습니다. 이 ID는 E-Series 컨트롤러 쉘프의 기본 ID입니다.
E5500SG 컨트롤러	에는 * HO * 가 표시되고 그 뒤에 두 개의 숫자가 반복됩니다. `HO -- IP address for Admin Network -- IP address for Grid Network HO` 순서대로 첫 번째 숫자 세트는 컨트롤러의 관리 포트 1에 대해 DHCP가 할당한 IP 주소입니다. 이 주소는 컨트롤러를 StorageGRID용 관리 네트워크에 연결하는 데 사용됩니다. 두 번째 숫자 세트는 어플라이언스를 StorageGRID용 그리드 네트워크에 연결하는 데 사용되는 DHCP 할당 IP 주소입니다. • 참고: * DHCP를 사용하여 IP 주소를 할당할 수 없는 경우 0.0.0.0이 표시됩니다.

3. 7개 세그먼트가 표시되면 다른 값을 표시합니다. 을 참조하십시오 하드웨어 설치 문제 해결(SG5700) 설치 단계를 올바르게 완료했는지 확인합니다. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

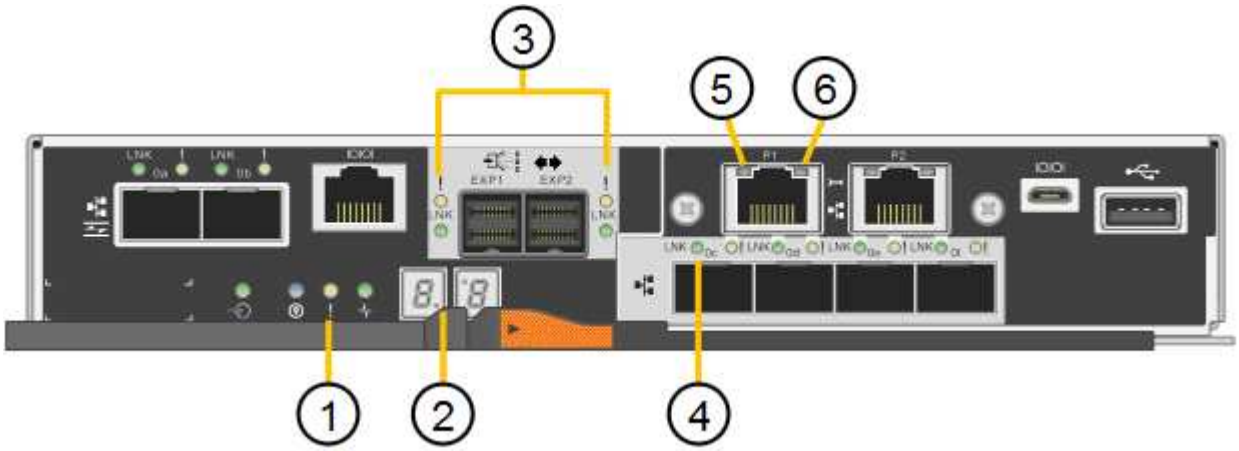
관련 정보

E5500SG 컨트롤러의 상태 표시등

"E5700 및 E2800 시스템 모니터링 가이드"

어플라이언스 전원이 켜지고 하드웨어가 초기화되는 동안 E700SG 컨트롤러의 7세그먼트 디스플레이와 LED에 상태 및 오류 코드가 표시됩니다. 이러한 디스플레이를 사용하여 상태를 확인하고 오류를 해결할 수 있습니다.

StorageGRID 어플라이언스 설치 프로그램을 시작한 후에는 정기적으로 E5500SG 컨트롤러의 상태 표시등을 검토해야 합니다.



	디스플레이	설명
1	주의 LED	황색: 컨트롤러에 결함이 있으며 운영자의 주의가 필요하거나 설치 스크립트를 찾을 수 없습니다. Off(끄기): 컨트롤러가 정상적으로 작동하고 있습니다.
2	7개 세그먼트 디스플레이	에서는 진단 코드를 보여 줍니다 7개 세그먼트 디스플레이 시퀀스를 통해 어플라이언스의 오류 및 작동 상태를 파악할 수 있습니다.
3	확장 포트 주의 LED	황색: 본 제품은 확장 포트를 사용하지 않으므로 LED는 항상 주황색으로 켜져 있습니다(링크가 설정되지 않음).
4	호스트 포트 링크 상태 LED	녹색: 링크가 작동 중입니다. 꺼짐: 링크가 다운되었습니다.
5	이더넷 링크 상태 LED	녹색: 링크가 설정되었습니다. 꺼짐: 링크가 설정되지 않았습니다.

	디스플레이	설명
6	이더넷 작동 LED	녹색: 관리 포트와 연결된 장치(예: 이더넷 스위치) 사이의 링크가 작동 중입니다. 꺼짐: 컨트롤러와 연결된 장치 사이에 링크가 없습니다. 녹색으로 깜박임: 이더넷이 작동 중입니다.

일반 부팅 코드

부팅하거나 제품을 하드 리셋한 후 다음과 같은 현상이 발생합니다.

1. E5500SG 컨트롤러의 7개 세그먼트 디스플레이에는 컨트롤러와 관련이 없는 일반적인 코드 시퀀스가 표시됩니다. 일반 시퀀스는 AA 및 FF 코드로 끝납니다.
2. E5500SG 컨트롤러에 고유한 부팅 코드가 나타납니다.

E5500SG 컨트롤러 부팅 코드

정상적인 어플라이언스 부팅 중에 E700SG 컨트롤러의 7세그먼트 디스플레이에는 다음 코드가 나열된 순서대로 표시됩니다.

코드	를 나타냅니다
안녕	마스터 부트 스크립트가 시작되었습니다.
PP	시스템에서 FPGA 업데이트 여부를 확인 중입니다.
HP	시스템에서 10/25-GbE 컨트롤러 펌웨어를 업데이트해야 하는지 확인합니다.
RB	펌웨어 업데이트를 적용한 후 시스템이 재부팅되고 있습니다.
FP	하드웨어 하위 시스템 펌웨어 업데이트 검사가 완료되었습니다. 컨트롤러 간 통신 서비스가 시작됩니다.
그는	시스템이 E2800 컨트롤러와의 연결을 기다리고 있으며 SANtricity 운영 체제와의 동기화를 기다리고 있습니다. • 참고: * 이 부팅 절차가 이 단계 이후 진행되지 않을 경우 두 컨트롤러 사이의 연결을 확인하십시오.
HC	시스템에서 기존 StorageGRID 설치 데이터를 확인하고 있습니다.

코드	를 나타냅니다
호	StorageGRID 어플라이언스 설치 프로그램이 실행 중입니다.
HA	StorageGRID가 실행 중입니다.

E5500SG 컨트롤러 오류 코드

이러한 코드는 어플라이언스 부팅 시 E5500SG 컨트롤러에 표시될 수 있는 오류 상태를 나타냅니다. 특정 하위 수준 하드웨어 오류가 발생할 경우 추가 2자리 16진수 코드가 표시됩니다. 이러한 코드 중 하나라도 1초 또는 2초 이상 지속되거나 규정된 문제 해결 절차 중 하나를 수행하여 오류를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

코드	를 나타냅니다
22	부팅 장치에서 마스터 부트 레코드를 찾을 수 없습니다.
23	내부 플래시 디스크가 연결되어 있지 않습니다.
2A, 2B	버스 고착, DIMM SPD 데이터를 읽을 수 없음.
40	DIMM이 잘못되었습니다.
41	DIMM이 잘못되었습니다.
42	메모리 테스트에 실패했습니다.
51	SPD 읽기 오류입니다.
92에서 96	PCI 버스 초기화.
A0에서 A3까지	SATA 드라이브 초기화
복부	대체 부팅 코드.
AE	OS 부팅 중.
EA	DDR4 교육에 실패했습니다.
E8	설치된 메모리가 없습니다.
EU	설치 스크립트를 찾을 수 없습니다.
EP	E2800 컨트롤러 설치 또는 통신에 실패했습니다.

관련 정보

하드웨어 설치 문제 해결(SG5700)

"NetApp 지원"

하드웨어 구성(SG5700)

어플라이언스에 전원을 적용한 후 하드웨어를 모니터링하는 데 사용할 소프트웨어인 SANtricity 시스템 관리자를 구성해야 합니다. StorageGRID에서 사용할 네트워크 연결도 구성해야 합니다.

StorageGRID 연결 구성(SG5700)

StorageGRID 어플라이언스를 StorageGRID 그리드에 스토리지 노드로 구축하기 전에 어플라이언스와 사용할 네트워크 간의 연결을 구성해야 합니다. E700SG 컨트롤러(어플라이언스의 컴퓨팅 컨트롤러)에 포함된 StorageGRID 어플라이언스 설치 프로그램으로 이동하여 네트워킹을 구성할 수 있습니다.

단계

- StorageGRID 어플라이언스 설치 프로그램에 액세스합니다
- StorageGRID 어플라이언스 설치 프로그램 버전을 확인하고 업그레이드합니다
- 네트워크 링크 구성(SG5700)
- IP 구성을 설정합니다
- 네트워크 연결을 확인합니다
- 포트 수준 네트워크 연결을 확인합니다

StorageGRID 어플라이언스 설치 프로그램에 액세스합니다

어플라이언스와 세 StorageGRID 네트워크(그리드 네트워크, 관리자 네트워크(옵션) 및 클라이언트 네트워크(선택 사항) 간의 연결을 구성하려면 StorageGRID 어플라이언스 설치 프로그램에 액세스해야 합니다.

필요한 것

- 을(를) 사용하고 있습니다 지원되는 웹 브라우저.
- 이 어플라이언스는 사용하려는 모든 StorageGRID 네트워크에 연결되어 있습니다.
- 이러한 네트워크에서 어플라이언스의 IP 주소, 게이트웨이 및 서브넷을 알고 있습니다.
- 사용할 네트워크 스위치를 구성했습니다.

이 작업에 대해

StorageGRID 어플라이언스 설치 프로그램에 처음 액세스할 때 관리 네트워크에 대해 DHCP 할당 IP 주소(어플라이언스가 관리 네트워크에 연결되어 있다고 가정) 또는 그리드 네트워크에 대해 DHCP 할당 IP 주소를 사용할 수 있습니다. 관리 네트워크의 IP 주소를 사용하는 것이 좋습니다. 그렇지 않으면 그리드 네트워크의 DHCP 주소를 사용하여 StorageGRID 어플라이언스 설치 프로그램에 액세스하는 경우 링크 설정을 변경하거나 고정 IP를 입력할 때 StorageGRID 어플라이언스 설치 프로그램과의 연결이 끊어질 수 있습니다.

단계

1. 관리 네트워크(연결된 경우) 또는 그리드 네트워크(관리 네트워크가 연결되어 있지 않은 경우)에서 어플라이언스의 DHCP 주소를 얻습니다.

   다음 중 하나를 수행할 수 있습니다.

   - E5500SG 컨트롤러에서 7개 세그먼트 디스플레이를 확인합니다. E5500SG 컨트롤러의 관리 포트 1 및 10/25GbE 포트 2 및 4가 DHCP 서버를 통해 네트워크에 연결되어 있는 경우, 컨트롤러는 엔클로저의 전원을 켤 때 동적으로 할당된 IP 주소를 가져오려고 시도합니다. 컨트롤러가 전원 켜기 프로세스를 완료하면 7개 세그먼트 디스플레이에 * HO * 가 표시되고, 그 뒤에 2개의 숫자가 반복됩니다.

     ```
     HO -- IP address for Admin Network -- IP address for Grid Network HO
     ```

     시퀀스:

     - 첫 번째 번호 세트는 연결된 경우 관리 네트워크의 어플라이언스 스토리지 노드에 대한 DHCP 주소입니다. 이 IP 주소는 E5500SG 컨트롤러의 관리 포트 1에 할당됩니다.
     - 두 번째 숫자 세트는 그리드 네트워크의 어플라이언스 스토리지 노드에 대한 DHCP 주소입니다. 이 IP 주소는 어플라이언스에 처음 전원을 공급하면 10/25GbE 포트 2 및 4에 할당됩니다.

       DHCP를 사용하여 IP 주소를 할당할 수 없는 경우 0.0.0.0이 표시됩니다.

   - 관리 포트 1의 MAC 주소를 네트워크 관리자에게 제공하여 관리 네트워크에서 이 포트의 DHCP 주소를 찾을 수 있도록 합니다. MAC 주소는 포트 옆에 있는 E5500SG 컨트롤러의 레이블에 인쇄되어 있습니다.

2. DHCP 주소 중 하나를 얻을 수 있는 경우:

   a. 서비스 랩톱에서 웹 브라우저를 엽니다.

   b. StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. +
      `https://*E5700SG_Controller_IP*:8443*

      '*E700SG_Controller_IP*'의 경우 컨트롤러의 DHCP 주소를 사용합니다(관리자 네트워크가 있는 경우 IP 주소 사용).

   c. 보안 경고 메시지가 나타나면 브라우저의 설치 마법사를 사용하여 인증서를 보고 설치합니다.

      다음에 이 URL에 액세스할 때 알림이 나타나지 않습니다.

      StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다. 이 페이지에 처음 액세스할 때 표시되는 정보와 메시지는 어플라이언스가 현재 StorageGRID 네트워크에 연결되어 있는 방식에 따라 다릅니다. 오류 메시지가 나타날 수 있으며, 이 메시지는 이후 단계에서 해결될 것입니다.

NetApp® StorageGRID® Appliance Installer

Home | Configure Networking | Configure Hardware | Monitor Installation | Advanced

Home

The installation is ready to be started. Review the settings below, and then click Start Installation.

This Node

Node type: Storage

Node name: MM-2-108-SGA-lab25

Cancel Save

Primary Admin Node connection

Enable Admin Node discovery: ☐

Primary Admin Node IP: 172.16.1.178

Connection state: Connection to 172.16.1.178 ready

Cancel Save

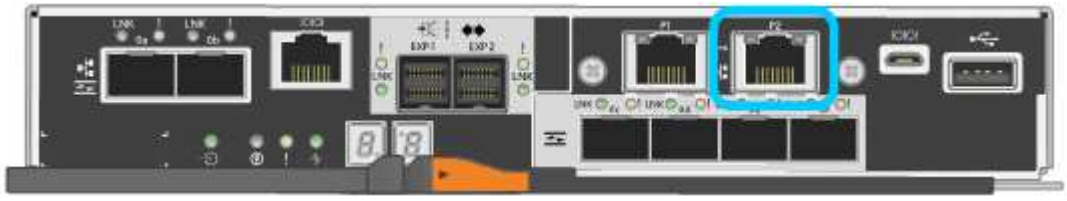
Installation

Current state: Ready to start installation of MM-2-108-SGA-lab25 into grid with Admin Node 172.16.1.178 running StorageGRID 11.2.0, using StorageGRID software downloaded from the Admin Node.

Start Installation

3. E5500SG 컨트롤러가 DHCP를 사용하여 IP 주소를 가져올 수 없는 경우:

   a. 이더넷 케이블을 사용하여 서비스 랩톱을 E5500SG 컨트롤러의 관리 포트 2에 연결합니다.



b. 서비스 랩톱에서 웹 브라우저를 엽니다.

c. StorageGRID 어플라이언스 설치 프로그램에 대한 이 URL을 입력합니다: + `* https://169.254.0.1:8443*

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다. 이 페이지에 처음 액세스할 때 표시되는 정보 및 메시지는 어플라이언스가 현재 연결되어 있는 방식에 따라 다릅니다.

> 링크 로컬 연결을 통해 홈 페이지에 액세스할 수 없는 경우 서비스 랩톱 IP 주소를 "169.254.0.2"로 구성한 후 다시 시도하십시오.

4. 홈 페이지에 표시되는 메시지를 검토하고 필요에 따라 링크 구성 및 IP 구성을 구성합니다.

관련 정보

웹 브라우저 요구 사항

StorageGRID 어플라이언스 설치 프로그램 버전을 확인하고 업그레이드합니다

어플라이언스의 StorageGRID 어플라이언스 설치 프로그램 버전은 StorageGRID 시스템에 설치된 소프트웨어 버전과 일치해야 모든 StorageGRID 기능이 지원됩니다.

필요한 것

StorageGRID 어플라이언스 설치 프로그램에 액세스했습니다.

이 작업에 대해

StorageGRID 어플라이언스는 StorageGRID 어플라이언스 설치 프로그램이 사전 설치된 상태로 제공됩니다. 최근에 업그레이드된 StorageGRID 시스템에 어플라이언스를 추가하는 경우 어플라이언스를 새 노드로 설치하기 전에 StorageGRID 어플라이언스 설치 프로그램을 수동으로 업그레이드해야 할 수 있습니다.

새 StorageGRID 버전으로 업그레이드하면 StorageGRID 어플라이언스 설치 프로그램이 자동으로 업그레이드됩니다. 설치된 어플라이언스 노드에서 StorageGRID 어플라이언스 설치 프로그램을 업그레이드할 필요가 없습니다. 이 절차는 이전 버전의 StorageGRID 어플라이언스 설치 프로그램이 포함된 어플라이언스를 설치하는 경우에만 필요합니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 펌웨어 업그레이드 * 를 선택합니다.

2. 현재 펌웨어 버전을 StorageGRID 시스템에 설치된 소프트웨어 버전과 비교합니다. (그리드 관리자 상단에서 도움말 아이콘을 선택하고 * 정보 * 를 선택합니다.)

   두 버전의 두 번째 숫자가 일치해야 합니다. 예를 들어, StorageGRID 시스템에서 버전 11. * 6 *.*x*._y_를 실행하는 경우 StorageGRID 어플라이언스 설치 프로그램 버전은 3. * 6 *._z_이어야 합니다.

3. 어플라이언스에 StorageGRID 어플라이언스 설치 프로그램의 하위 수준 버전이 있는 경우 로 이동합니다 "NetApp 다운로드: StorageGRID 어플라이언스".

   NetApp 계정의 사용자 이름과 암호를 사용하여 로그인합니다.

4. StorageGRID Appliances*용 * 지원 파일의 적절한 버전과 해당 체크섬 파일을 다운로드하십시오.

   StorageGRID 어플라이언스 파일의 지원 파일은 모든 StorageGRID 어플라이언스 모델의 현재 및 이전 펌웨어 버전을 포함하는 '.zip' 아카이브로, 각 컨트롤러 유형의 하위 디렉토리에 있습니다.

StorageGRID 어플라이언스 파일용 지원 파일을 다운로드한 후 '.zip' 아카이브의 압축을 풀고 StorageGRID 어플라이언스 설치 프로그램 설치에 대한 중요 정보는 README 파일을 참조하십시오.

5. StorageGRID 어플라이언스 설치 프로그램의 펌웨어 업그레이드 페이지에 있는 지침에 따라 다음 단계를 수행합니다.
   a. 컨트롤러 유형 및 체크섬 파일에 적합한 지원 파일(펌웨어 이미지)을 업로드합니다.
   b. 비활성 파티션을 업그레이드합니다.
   c. 재부팅하고 파티션을 바꿉니다.
   d. 두 번째(비활성) 파티션을 업그레이드합니다.

관련 정보

StorageGRID 어플라이언스 설치 프로그램에 액세스합니다

네트워크 링크 구성**(SG5700)**

어플라이언스를 그리드 네트워크, 클라이언트 네트워크 및 관리 네트워크에 연결하는 데 사용되는 포트에 대한 네트워크 링크를 구성할 수 있습니다. 링크 속도와 포트 및 네트워크 연결 모드를 설정할 수 있습니다.

필요한 것

10/25-GbE 포트에 25-GbE 링크 속도를 사용하려는 경우:

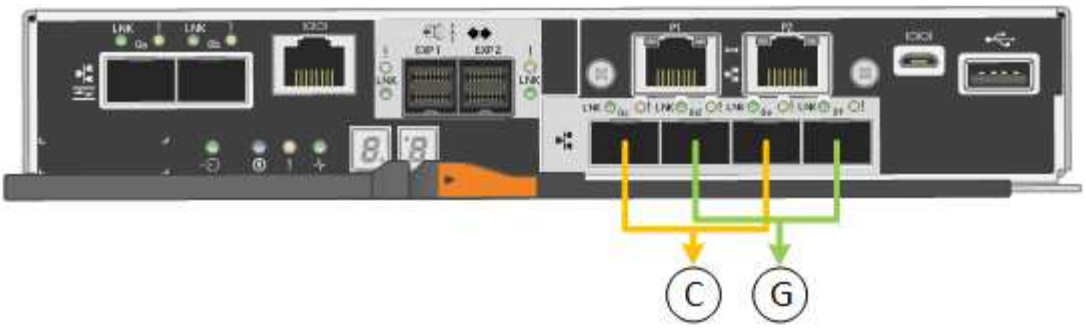
- 사용하려는 포트에 SFP28 트랜시버를 설치했습니다.
- 이러한 기능을 지원할 수 있는 스위치에 포트를 연결했습니다.
- 이 고속 스위치를 사용하도록 스위치를 구성하는 방법을 이해할 수 있습니다.

Aggregate 포트 결합 모드, LACP 네트워크 결합 모드 또는 10/25-GbE 포트에 대한 VLAN 태그 지정을 사용하려면 다음을 수행합니다.

- 어플라이언스의 포트를 VLAN 및 LACP를 지원할 수 있는 스위치에 연결했습니다.
- LACP 결합에 여러 스위치가 사용되는 경우 스위치는 MLAG(Multi-Chassis Link Aggregation Group) 또는 이와 동등한 스위치를 지원합니다.
- VLAN, LACP, MLAG 또는 이와 동등한 기능을 사용하도록 스위치를 구성하는 방법을 이해합니다.
- 각 네트워크에 사용할 고유 VLAN 태그를 알고 있습니다. 이 VLAN 태그는 네트워크 트래픽이 올바른 네트워크로 라우팅되도록 각 네트워크 패킷에 추가됩니다.
- 관리 네트워크에 Active-Backup 모드를 사용하려는 경우 컨트롤러의 두 관리 포트에 이더넷 케이블을 연결했습니다.

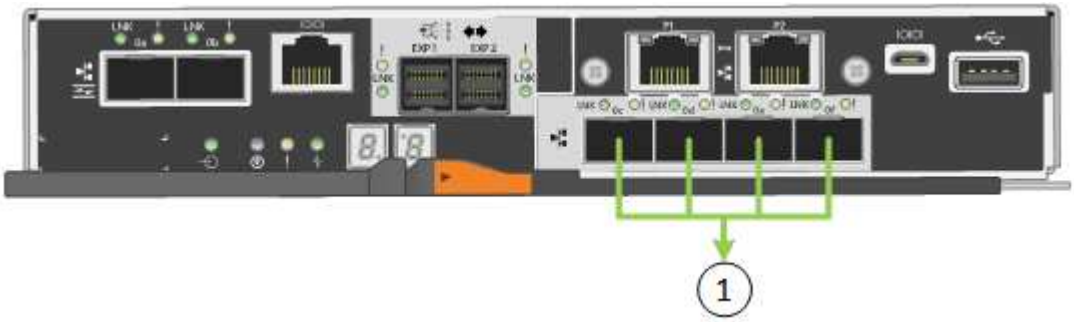
이 작업에 대해

이 그림은 4개의 10/25-GbE 포트가 고정 포트 결합 모드(기본 구성)에서 접합되는 방식을 보여줍니다.



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
c	이 네트워크를 사용하는 경우 포트 1과 3이 클라이언트 네트워크에 대해 함께 연결됩니다.
g	포트 2와 4는 그리드 네트워크를 위해 서로 연결되어 있습니다.

이 그림은 4개의 10/25-GbE 포트가 Aggregate 포트 결합 모드에서 결합되는 방식을 보여줍니다.



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
1	4개 포트 모두 단일 LACP 결합으로 그룹화되므로 모든 포트를 그리드 네트워크 및 클라이언트 네트워크 트래픽에 사용할 수 있습니다.

이 표에는 4개의 10/25-GbE 포트를 구성하는 옵션이 요약되어 있습니다. 기본 설정은 굵게 표시됩니다. 기본이 아닌 설정을 사용하려면 구성 연결 페이지에서 설정을 구성하기만 하면 됩니다.

- * 고정(기본값) 포트 결합 모드 *

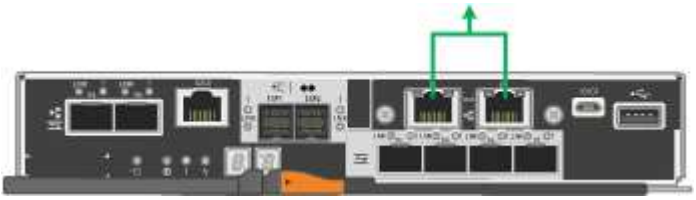
네트워크 연결 모드	클라이언트 네트워크 비활성화 (기본값)	클라이언트 네트워크가 활성화되었습니다
Active-Backup(기본값)	• 포트 2와 4는 그리드 네트워크에 액티브-백업 결합을 사용합니다. • 포트 1과 3은 사용되지 않습니다. • VLAN 태그는 선택 사항입니다.	• 포트 2와 4는 그리드 네트워크에 액티브-백업 결합을 사용합니다. • 포트 1과 3은 클라이언트 네트워크에 대해 액티브-백업 연결을 사용합니다. • VLAN 태그는 두 네트워크에 대해 모두 지정할 수 있습니다.
LACP(802.3ad)	• 포트 2와 4는 그리드 네트워크에 LACP 결합을 사용합니다. • 포트 1과 3은 사용되지 않습니다. • VLAN 태그는 선택 사항입니다.	• 포트 2와 4는 그리드 네트워크에 LACP 결합을 사용합니다. • 포트 1과 3은 클라이언트 네트워크에 LACP 결합을 사용합니다. • VLAN 태그는 두 네트워크에 대해 모두 지정할 수 있습니다.

- * 집계 포트 결합 모드 *

네트워크 연결 모드	클라이언트 네트워크 비활성화 (기본값)	클라이언트 네트워크가 활성화되었습니다
LACP(802.3ad)만 해당	• 포트 1-4는 그리드 네트워크에 단일 LACP 결합을 사용합니다. • 단일 VLAN 태그는 그리드 네트워크 패킷을 식별합니다.	• 포트 1-4는 그리드 네트워크 및 클라이언트 네트워크에 단일 LACP 결합을 사용합니다. • 두 개의 VLAN 태그를 통해 그리드 네트워크 패킷을 클라이언트 네트워크 패킷과 분리할 수 있습니다.

포트 결합 및 네트워크 결합 모드에 대한 자세한 내용은 E5500SG 컨트롤러의 10/25-GbE 포트 연결 정보를 참조하십시오.

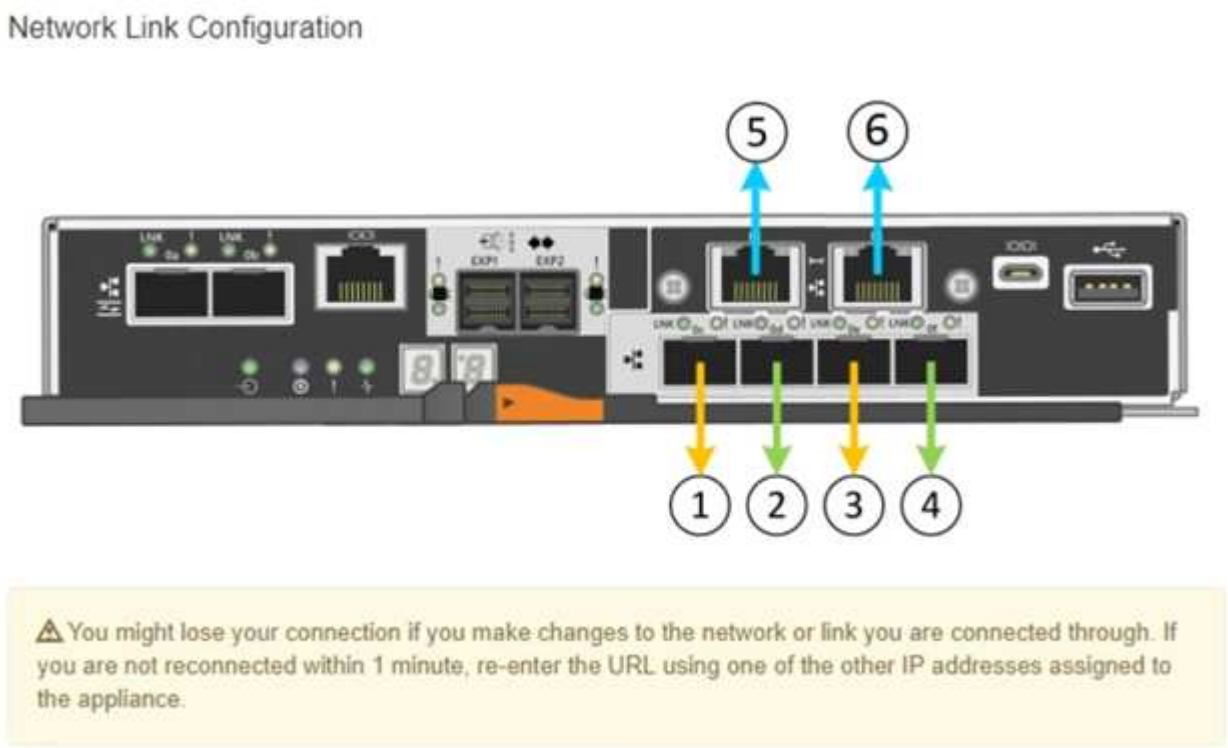
이 그림에서는 E700SG 컨트롤러의 1GbE 관리 포트 2개가 관리 네트워크의 Active-Backup 네트워크 연결 모드로 연결되는 방식을 보여 줍니다.



단계

1. StorageGRID 어플라이언스 설치 프로그램의 메뉴 모음에서 * 네트워킹 구성 * > * 링크 구성 * 을 클릭합니다.

네트워크 링크 구성 페이지에는 네트워크 및 관리 포트 번호가 지정된 어플라이언스 다이어그램이 표시됩니다.



링크 상태 테이블에는 번호가 매겨진 포트의 링크 상태(위/아래) 및 속도(1/10/25/40/100Gbps)가 나열됩니다.

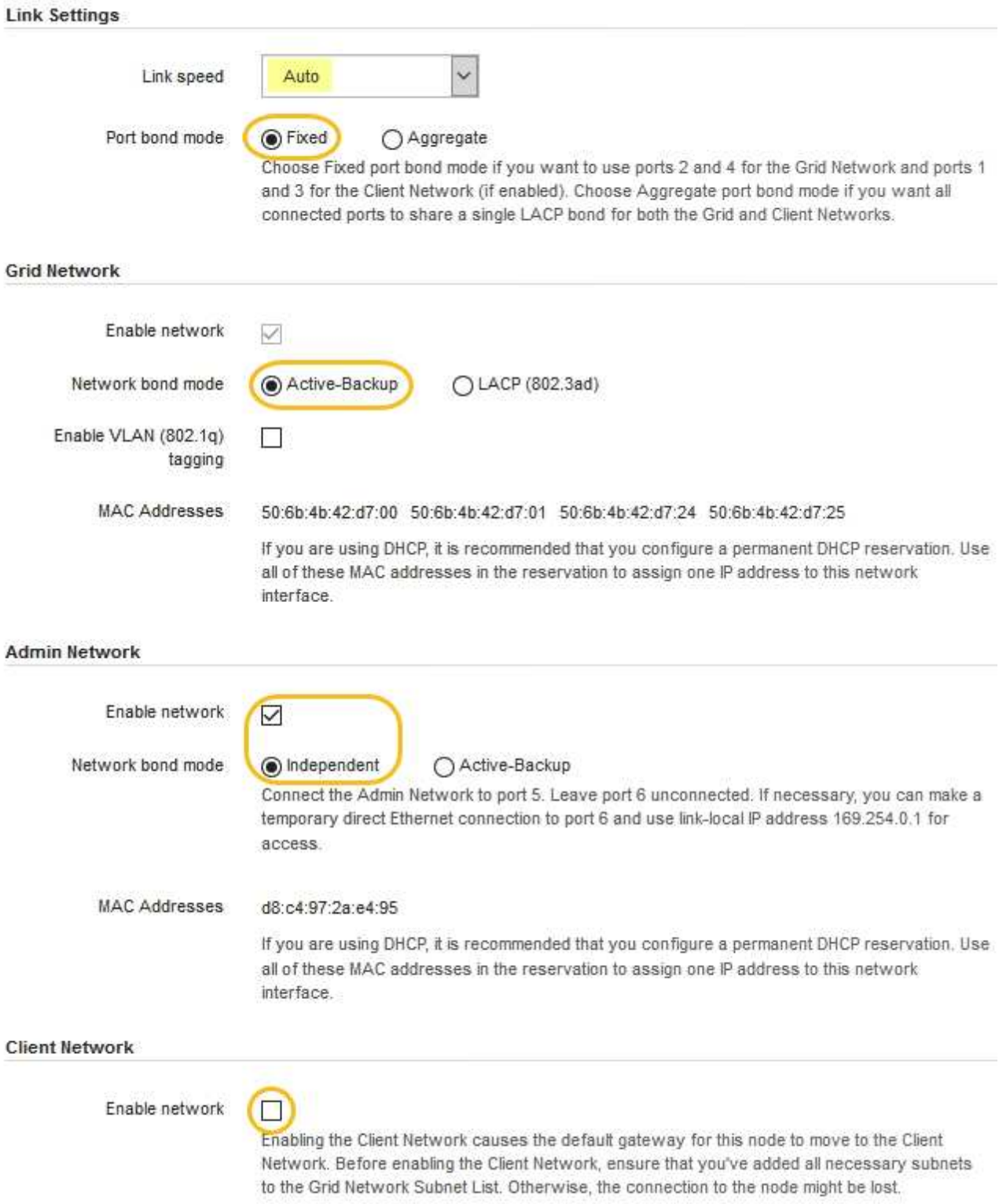
Link Status

Link	State	Speed (Gbps)
1	Up	25
2	Up	25
3	Up	25
4	Up	25
5	Up	1
6	Up	1

이 페이지에 처음 액세스하는 경우:

- * 링크 속도 * 는 * 10GbE * 로 설정됩니다.
- * 포트 결합 모드 * 가 * 고정 * 으로 설정됩니다.
- 그리드 네트워크의 * 네트워크 결합 모드 * 가 * 액티브-백업 * 으로 설정됩니다.
- Admin Network*가 활성화되고 네트워크 연결 모드가 * Independent * 로 설정됩니다.

◦ 클라이언트 네트워크 * 가 비활성화됩니다.



2. 10/25 GbE 포트에 대해 25 GbE 링크 속도를 사용하려는 경우 링크 속도 드롭다운 목록에서 * 25GbE * 를 선택합니다.

   그리드 네트워크 및 클라이언트 네트워크에 대해 사용 중인 네트워크 스위치도 이 속도를 지원하고 구성해야 합니다. SFP28 트랜시버는 포트에 설치해야 합니다.

3. 사용하려는 StorageGRID 네트워크를 활성화 또는 비활성화합니다.

   그리드 네트워크가 필요합니다. 이 네트워크를 비활성화할 수 없습니다.

   a. 어플라이언스가 관리 네트워크에 연결되어 있지 않은 경우 관리 네트워크의 * 네트워크 활성화 * 확인란을 선택 취소합니다.

      Admin Network

      Enable network ☐

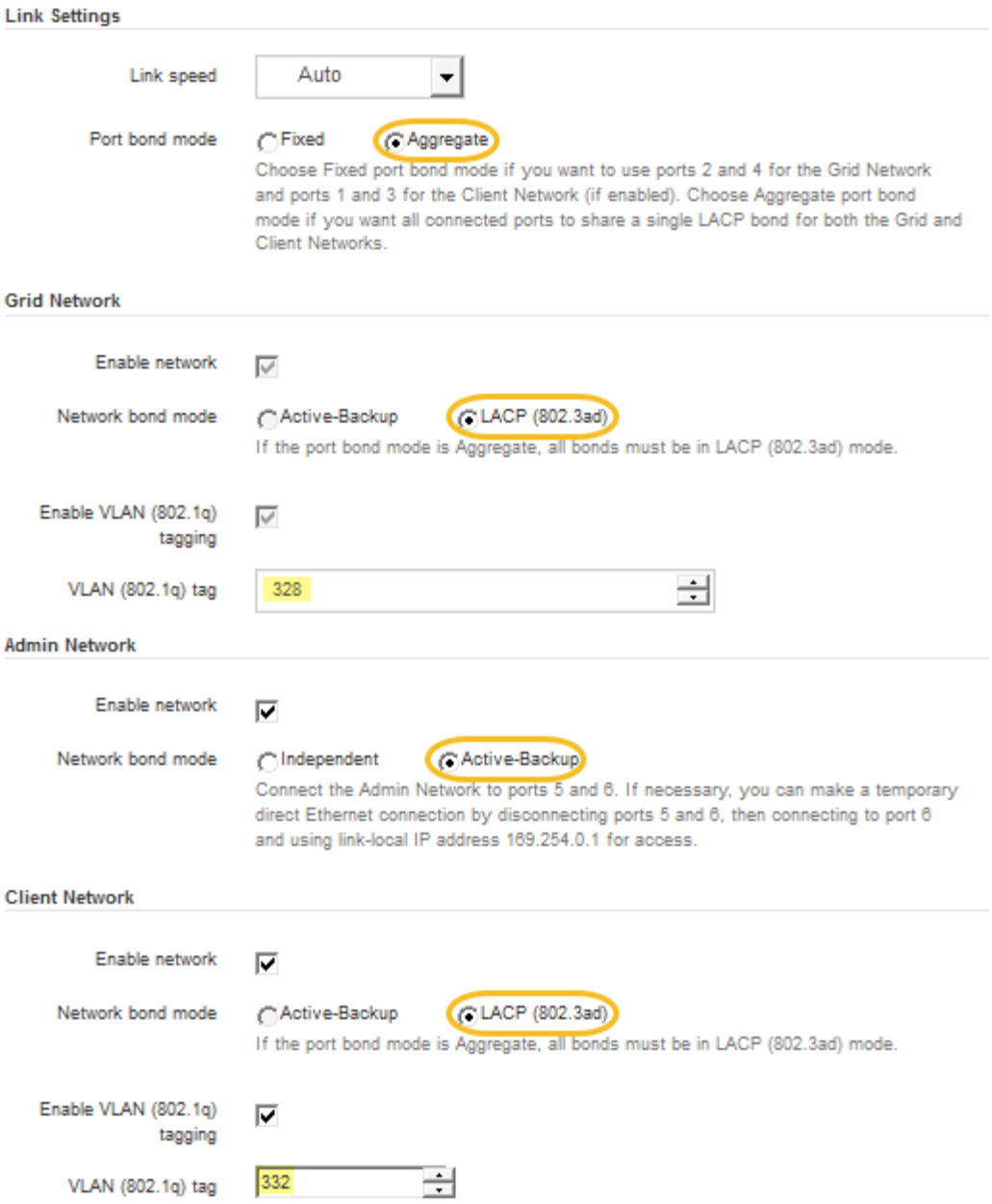
   b. 어플라이언스가 클라이언트 네트워크에 연결되어 있는 경우 클라이언트 네트워크의 * 네트워크 활성화 * 확인란을 선택합니다.

      이제 10/25-GbE 포트의 클라이언트 네트워크 설정이 표시됩니다.

4. 표를 참조하여 포트 결합 모드 및 네트워크 연결 모드를 구성합니다.

   예를 들면 다음과 같습니다.

   - 그리드 및 클라이언트 네트워크에 대해 * 집계 * 및 * LACP * 선택. 각 네트워크에 대해 고유한 VLAN 태그를 지정해야 합니다. 0에서 4095 사이의 값을 선택할 수 있습니다.
   - 관리자 네트워크에 대해 * Active-Backup * 이 선택되었습니다.



5. 선택 사항에 만족하면 * 저장 * 을 클릭합니다.

> 연결된 네트워크 또는 링크를 변경한 경우 연결이 끊어질 수 있습니다. 1분 내에 다시 연결되지 않으면 어플라이언스에 할당된 다른 IP 주소 중 하나를 사용하여 StorageGRID 어플라이언스 설치 프로그램의 URL을 다시 입력합니다. + " * https://*E5700SG_Controller_IP*:8443*`

관련 정보

E5500SG 컨트롤러 포트의 포트 연결 모드

IP 구성을 설정합니다

StorageGRID 어플라이언스 설치 프로그램을 사용하여 StorageGRID 그리드, 관리자 및 클라이언트 네트워크의 어플라이언스 스토리지 노드에 사용되는 IP 주소 및 라우팅 정보를 구성합니다.

이 작업에 대해

연결된 각 네트워크에서 어플라이언스에 대해 고정 IP를 할당하거나 DHCP 서버의 주소에 대해 영구 임대를 할당해야 합니다.

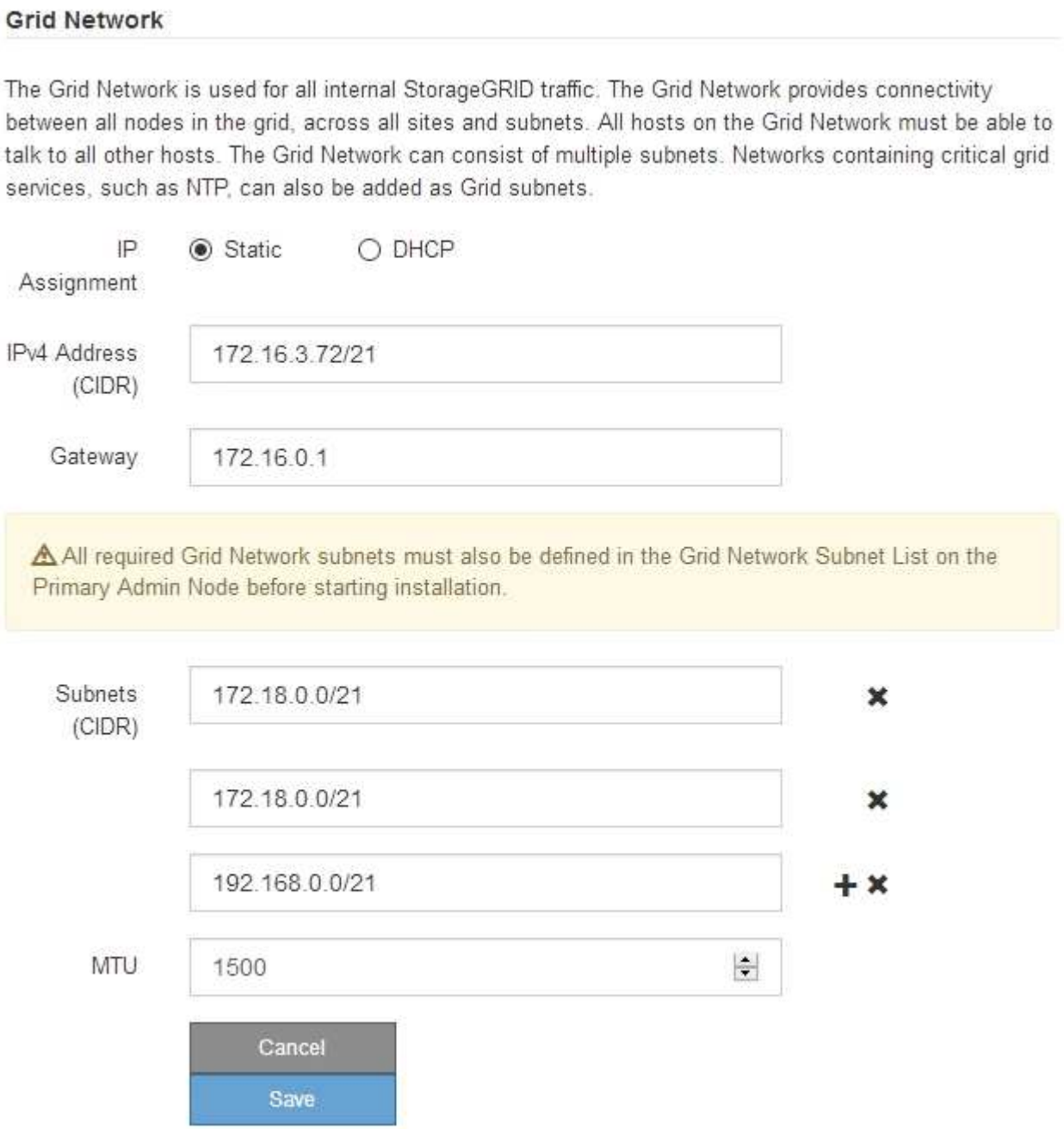
링크 구성을 변경하려면 E5500SG 컨트롤러의 링크 구성을 변경하는 지침을 참조하십시오.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * IP 구성 * 을 선택합니다.

   IP 구성 페이지가 나타납니다.

2. 그리드 네트워크를 구성하려면 페이지의 * 그리드 네트워크 * 섹션에서 * 정적 * 또는 * DHCP * 를 선택합니다.



3. Static * (정적 *)을 선택한 경우 다음 단계에 따라 Grid Network(그리드 네트워크)를 구성합니다.
   a. CIDR 표기법을 사용하여 정적 IPv4 주소를 입력합니다.
   b. 게이트웨이를 입력합니다.

      네트워크에 게이트웨이가 없는 경우 동일한 정적 IPv4 주소를 다시 입력합니다.

   c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

      > 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

      > 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

   d. 저장 * 을 클릭합니다.

      IP 주소를 변경하면 게이트웨이와 서브넷 목록도 변경될 수 있습니다.

      StorageGRID 어플라이언스 설치 프로그램에 대한 연결이 끊어진 경우 방금 할당한 새 고정 IP 주소를 사용하여 URL을 다시 입력합니다. 예: + `https://services_appliance_IP:8443*

   e. 그리드 네트워크 서브넷 목록이 올바른지 확인합니다.

      그리드 서브넷이 있는 경우 그리드 네트워크 게이트웨이가 필요합니다. 지정된 모든 그리드 서브넷은 이 게이트웨이를 통해 연결할 수 있어야 합니다. 이러한 그리드 네트워크 서브넷은 StorageGRID 설치를 시작할 때 기본 관리 노드의 그리드 네트워크 서브넷 목록에도 정의되어 있어야 합니다.

      > 기본 라우트는 나열되지 않습니다. 클라이언트 네트워크가 활성화되지 않은 경우 기본 라우트는 그리드 네트워크 게이트웨이를 사용합니다.

      - 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
      - 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

   f. 저장 * 을 클릭합니다.
4. DHCP * 를 선택한 경우 다음 단계에 따라 그리드 네트워크를 구성합니다.
   a. DHCP * 라디오 버튼을 선택한 후 * 저장 * 을 클릭합니다.

      IPv4 주소 *, * 게이트웨이 * 및 * 서브넷 * 필드가 자동으로 채워집니다. DHCP 서버가 MTU 값을 할당하도록 설정된 경우 * MTU * 필드가 해당 값으로 채워지고 필드는 읽기 전용이 됩니다.

      웹 브라우저가 자동으로 StorageGRID 어플라이언스 설치 프로그램의 새 IP 주소로 리디렉션됩니다.

   b. 그리드 네트워크 서브넷 목록이 올바른지 확인합니다.

      그리드 서브넷이 있는 경우 그리드 네트워크 게이트웨이가 필요합니다. 지정된 모든 그리드 서브넷은 이

게이트웨이를 통해 연결할 수 있어야 합니다. 이러한 그리드 네트워크 서브넷은 StorageGRID 설치를 시작할 때 기본 관리 노드의 그리드 네트워크 서브넷 목록에도 정의되어 있어야 합니다.

> 기본 라우트는 나열되지 않습니다. 클라이언트 네트워크가 활성화되지 않은 경우 기본 라우트는 그리드 네트워크 게이트웨이를 사용합니다.

- 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
- 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

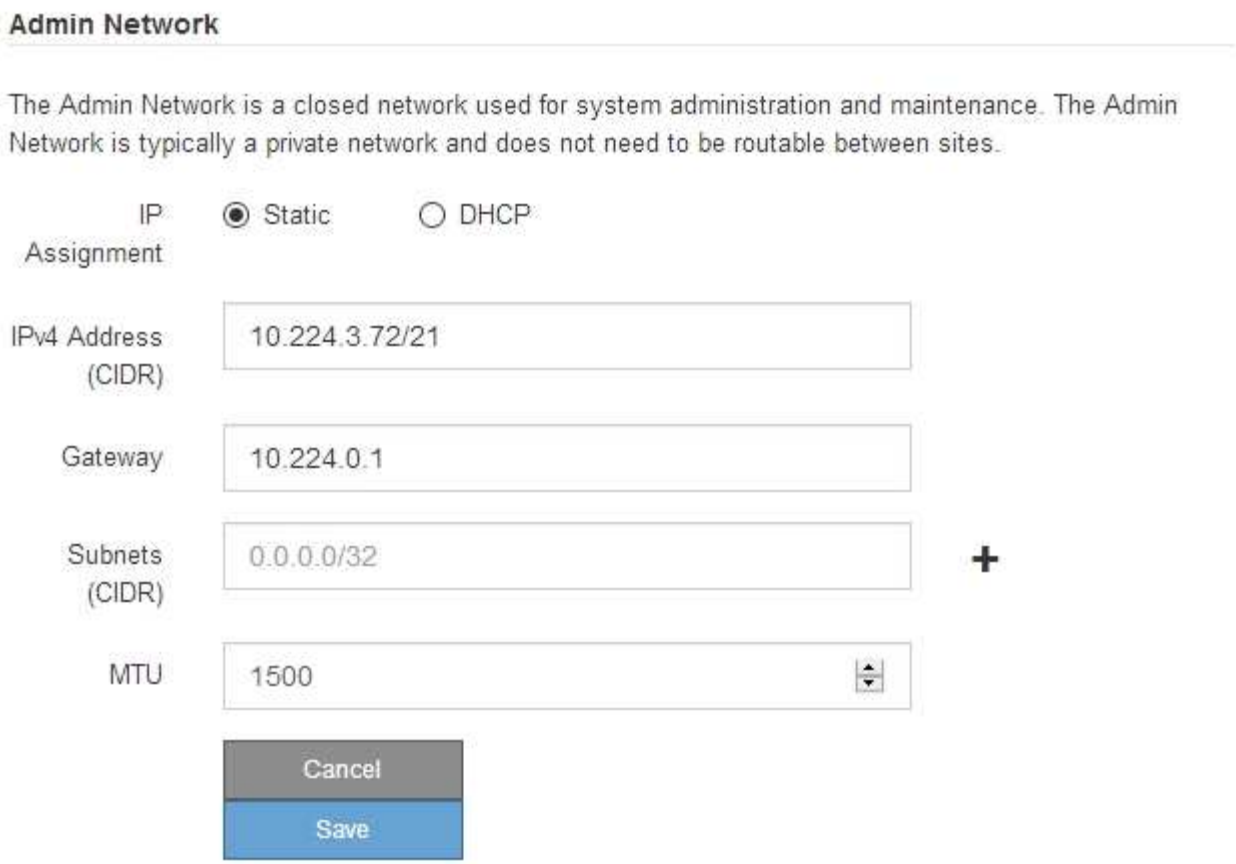
> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

> 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

a. 저장 * 을 클릭합니다.

5. 관리 네트워크를 구성하려면 페이지의 관리 네트워크 섹션에서 * 정적 * 또는 * DHCP * 를 선택합니다.

> 관리 네트워크를 구성하려면 링크 구성 페이지에서 관리 네트워크를 활성화해야 합니다.



6. 정적 * 을 선택한 경우 다음 단계에 따라 관리 네트워크를 구성합니다.
   a. 어플라이언스의 관리 포트 1에 대한 CIDR 표기법을 사용하여 정적 IPv4 주소를 입력합니다.

      관리 포트 1은 어플라이언스의 오른쪽 끝에 있는 2개의 1GbE RJ45 포트 왼쪽에 있습니다.

   b. 게이트웨이를 입력합니다.

      네트워크에 게이트웨이가 없는 경우 동일한 정적 IPv4 주소를 다시 입력합니다.

   c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

      > 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

   d. 저장 * 을 클릭합니다.

      IP 주소를 변경하면 게이트웨이와 서브넷 목록도 변경될 수 있습니다.

      StorageGRID 어플라이언스 설치 프로그램에 대한 연결이 끊어진 경우 방금 할당한 새 고정 IP 주소를 사용하여 URL을 다시 입력합니다. 예: + `https://services_appliance:8443*

   e. 관리자 네트워크 서브넷 목록이 올바른지 확인합니다.

      입력한 게이트웨이를 사용하여 모든 서브넷에 연결할 수 있는지 확인해야 합니다.

> 관리자 네트워크 게이트웨이를 사용하도록 기본 경로를 설정할 수 없습니다.

- 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
- 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

f. 저장 * 을 클릭합니다.

7. DHCP * 를 선택한 경우 다음 단계에 따라 관리 네트워크를 구성합니다.

a. DHCP * 라디오 버튼을 선택한 후 * 저장 * 을 클릭합니다.

IPv4 주소 *, * 게이트웨이 * 및 * 서브넷 * 필드가 자동으로 채워집니다. DHCP 서버가 MTU 값을 할당하도록 설정된 경우 * MTU * 필드가 해당 값으로 채워지고 필드는 읽기 전용이 됩니다.

웹 브라우저가 자동으로 StorageGRID 어플라이언스 설치 프로그램의 새 IP 주소로 리디렉션됩니다.

b. 관리자 네트워크 서브넷 목록이 올바른지 확인합니다.

입력한 게이트웨이를 사용하여 모든 서브넷에 연결할 수 있는지 확인해야 합니다.

> 관리자 네트워크 게이트웨이를 사용하도록 기본 경로를 설정할 수 없습니다.

- 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
- 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

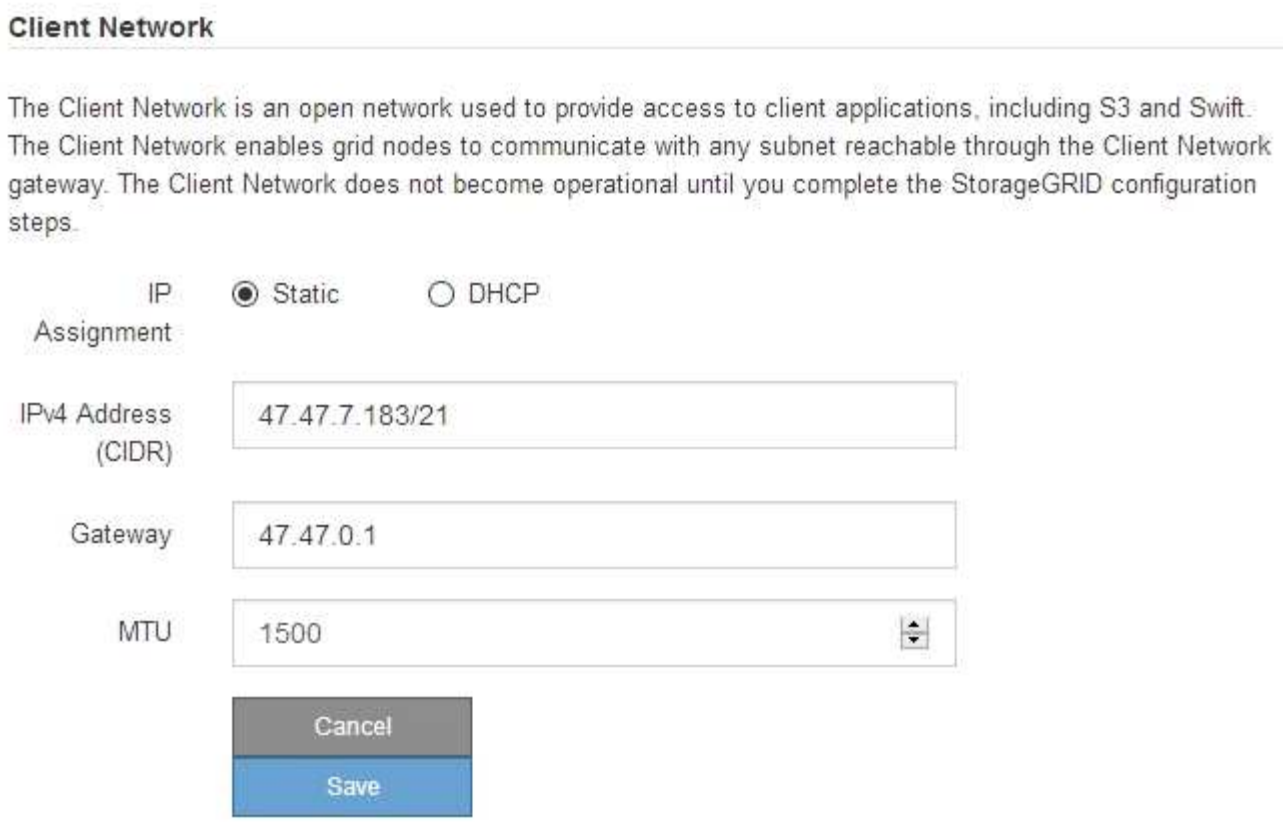
c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

d. 저장 * 을 클릭합니다.

8. 클라이언트 네트워크를 구성하려면 페이지의 * 클라이언트 네트워크 * 섹션에서 * 정적 * 또는 * DHCP * 를 선택합니다.

> 클라이언트 네트워크를 구성하려면 링크 구성 페이지에서 클라이언트 네트워크를 활성화해야 합니다.



9. 정적 * 을 선택한 경우 다음 단계에 따라 클라이언트 네트워크를 구성합니다.
   a. CIDR 표기법을 사용하여 정적 IPv4 주소를 입력합니다.
   b. 저장 * 을 클릭합니다.
   c. 클라이언트 네트워크 게이트웨이의 IP 주소가 올바른지 확인합니다.

   > 클라이언트 네트워크가 활성화된 경우 기본 경로가 표시됩니다. 기본 라우트는 클라이언트 네트워크 게이트웨이를 사용하며 클라이언트 네트워크가 활성화된 동안에는 다른 인터페이스로 이동할 수 없습니다.

   d. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

   > 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

   e. 저장 * 을 클릭합니다.
10. DHCP * 를 선택한 경우 다음 단계에 따라 클라이언트 네트워크를 구성합니다.
   a. DHCP * 라디오 버튼을 선택한 후 * 저장 * 을 클릭합니다.

      IPv4 주소 * 및 * 게이트웨이 * 필드가 자동으로 채워집니다. DHCP 서버가 MTU 값을 할당하도록 설정된 경우 * MTU * 필드가 해당 값으로 채워지고 필드는 읽기 전용이 됩니다.

웹 브라우저가 자동으로 StorageGRID 어플라이언스 설치 프로그램의 새 IP 주소로 리디렉션됩니다.

a. 게이트웨이가 올바른지 확인합니다.

> 클라이언트 네트워크가 활성화된 경우 기본 경로가 표시됩니다. 기본 라우트는 클라이언트 네트워크 게이트웨이를 사용하며 클라이언트 네트워크가 활성화된 동안에는 다른 인터페이스로 이동할 수 없습니다.

b. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

관련 정보

E5500SG 컨트롤러의 링크 구성을 변경합니다

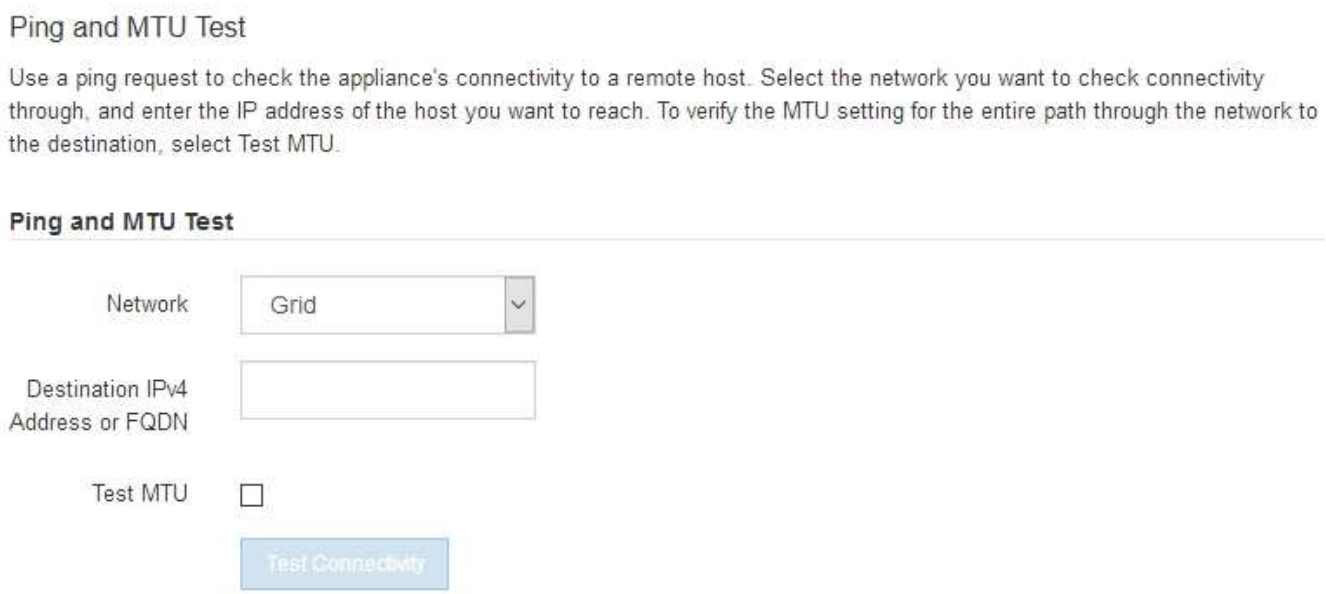
네트워크 연결을 확인합니다

어플라이언스에서 사용 중인 StorageGRID 네트워크에 액세스할 수 있는지 확인해야 합니다. 네트워크 게이트웨이를 통한 라우팅의 유효성을 검사하려면 StorageGRID 어플라이언스 설치 프로그램과 다른 서브넷의 IP 주소 간의 연결을 테스트해야 합니다. MTU 설정을 확인할 수도 있습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램의 메뉴 모음에서 * 네트워킹 구성 * > * Ping 및 MTU 테스트 * 를 클릭합니다.

   Ping 및 MTU 테스트 페이지가 나타납니다.



2. 네트워크 * 드롭다운 상자에서 테스트할 네트워크(그리드, 관리자 또는 클라이언트)를 선택합니다.
3. 해당 네트워크의 호스트에 대한 IPv4 주소 또는 FQDN(정규화된 도메인 이름)을 입력합니다.

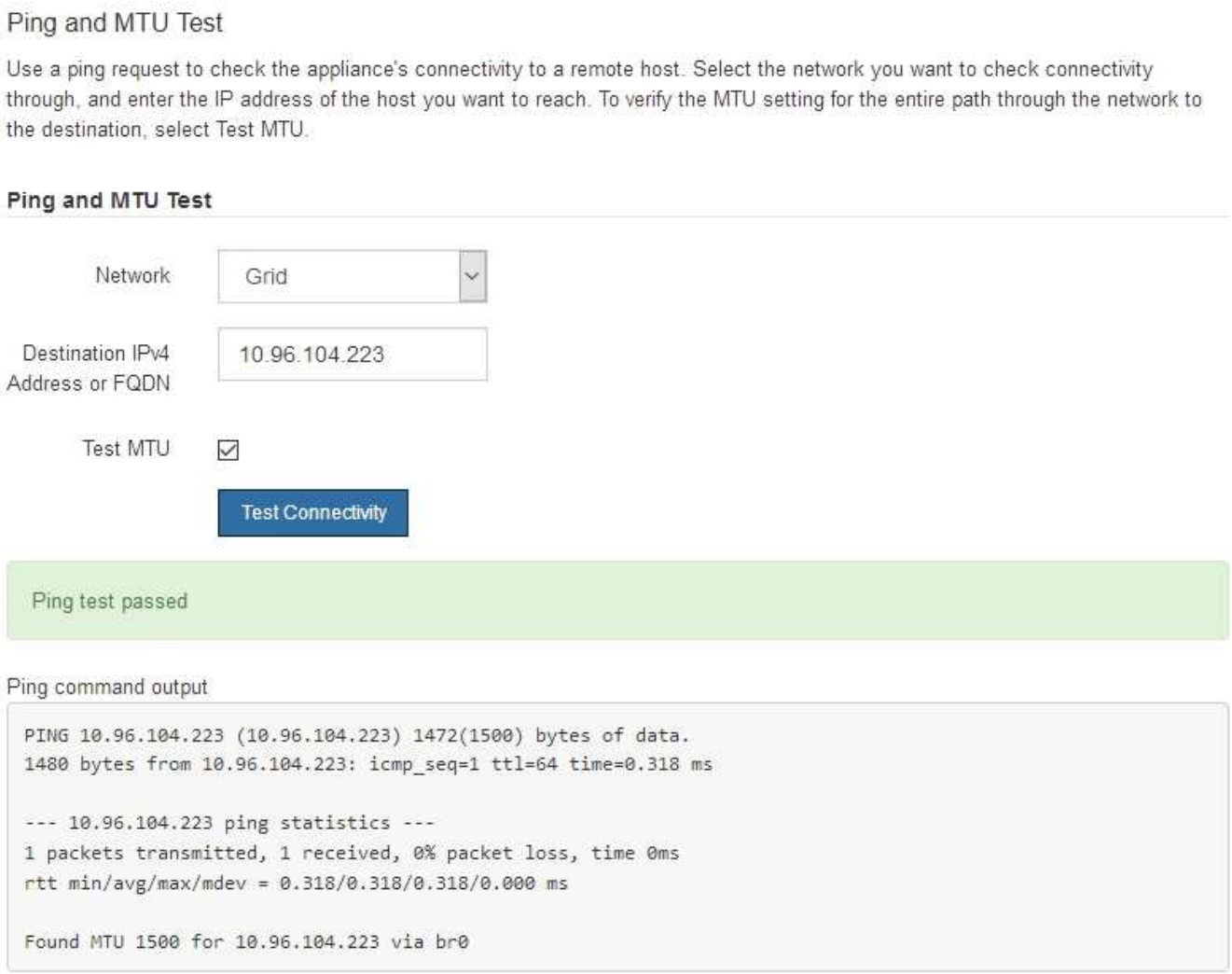
예를 들어 네트워크 또는 기본 관리 노드의 게이트웨이를 Ping할 수 있습니다.

4. 선택적으로 * Test MTU * 확인란을 선택하여 네트워크를 통해 대상으로 가는 전체 경로에 대한 MTU 설정을 확인합니다.

   예를 들어, 어플라이언스 노드와 다른 사이트의 노드 간 경로를 테스트할 수 있습니다.

5. 연결 테스트 * 를 클릭합니다.

   네트워크 연결이 유효한 경우 ping 명령 출력이 나열된 "Ping test Passed" 메시지가 나타납니다.



관련 정보

네트워크 링크 구성(SG5700)

MTU 설정을 변경합니다

포트 수준 네트워크 연결을 확인합니다

StorageGRID 어플라이언스 설치 프로그램과 다른 노드 간의 액세스가 방화벽에 의해 방해 받지 않도록 하려면 StorageGRID 어플라이언스 설치 관리자가 지정된 IP 주소 또는 주소 범위의

특정 TCP 포트 또는 포트 집합에 연결할 수 있는지 확인합니다.

이 작업에 대해

StorageGRID 어플라이언스 설치 프로그램에 제공된 포트 목록을 사용하여 어플라이언스와 그리드 네트워크의 다른 노드 간의 연결을 테스트할 수 있습니다.

또한 외부 NFS 또는 DNS 서버에 사용되는 것과 같은 UDP 포트와 Admin 및 Client Networks에서 연결을 테스트할 수 있습니다. 이러한 포트 목록은 StorageGRID 네트워킹 지침의 포트 참조를 참조하십시오.

> 포트 연결 테이블에 나열된 그리드 네트워크 포트는 StorageGRID 버전 11.6.0에만 유효합니다. 각 노드 유형에 맞는 포트를 확인하려면 사용 중인 StorageGRID 버전에 대한 네트워킹 지침을 항상 참조해야 합니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * 포트 연결 테스트(nmap) * 를 클릭합니다.

   포트 연결 테스트 페이지가 나타납니다.

   포트 연결 표에는 그리드 네트워크에서 TCP 연결이 필요한 노드 유형이 나와 있습니다. 각 노드 유형에 대해 표에는 어플라이언스에 액세스할 수 있어야 하는 그리드 네트워크 포트가 나열되어 있습니다.

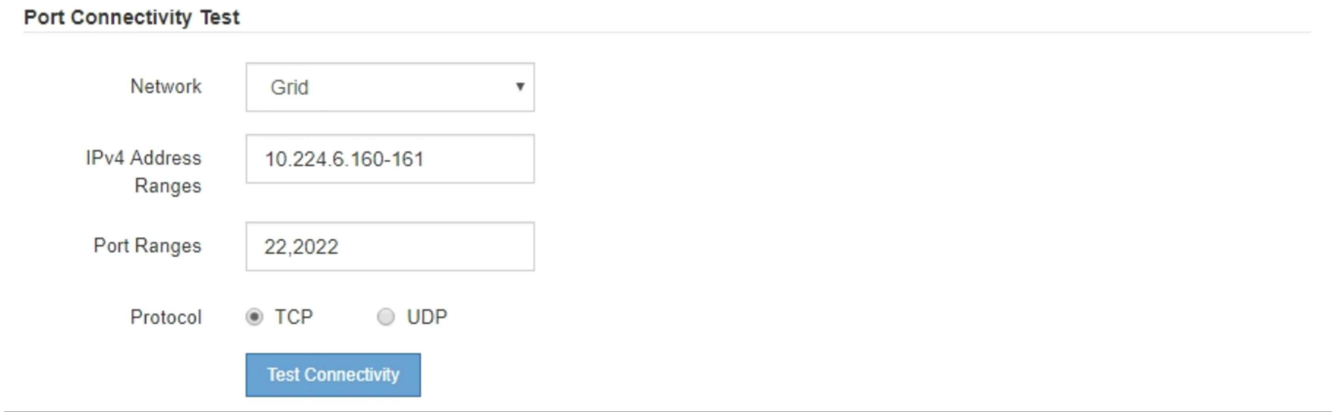
   표에 나열된 어플라이언스 포트와 그리드 네트워크의 다른 노드 간의 연결을 테스트할 수 있습니다.

2. Network * (네트워크 **)** 드롭다운에서 *** Grid * (**그리드 ***), * Admin * (** 관리자 *) 또는 * Client * (클라이언트 *)와 같이 테스트할 네트워크를 선택합니다.
3. 해당 네트워크의 호스트에 대한 IPv4 주소 범위를 지정합니다.

   예를 들어 네트워크 또는 기본 관리 노드의 게이트웨이를 조사할 수 있습니다.

   예제에 표시된 대로 하이픈을 사용하여 범위를 지정합니다.

4. TCP 포트 번호, 쉼표로 구분된 포트 목록 또는 포트 범위를 입력합니다.



5. 연결 테스트 * 를 클릭합니다.

   - 선택한 포트 수준 네트워크 연결이 유효하면 ""포트 연결 테스트 통과"" 메시지가 녹색 배너에 나타납니다. nmap 명령 출력은 배너 아래에 나열되어 있습니다.

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- 원격 호스트에 대한 포트 수준 네트워크 연결이 이루어졌지만 호스트가 선택한 포트 중 하나 이상의 포트에서 수신 대기 중이 아니면 ""포트 연결 테스트 실패" 메시지가 노란색 배너에 나타납니다. nmap 명령 출력은 배너 아래에 나열되어 있습니다.

  호스트가 청취하지 않는 모든 원격 포트는 ""닫힘"" 상태입니다. 예를 들어 연결하려는 노드가 사전 설치된 상태이고 StorageGRID NMS 서비스가 아직 실행되지 않은 경우 이 노란색 배너가 나타날 수 있습니다.

Port connectivity test failed
Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
1504/tcp closed evb-elm
1505/tcp open   funkproxy
1506/tcp open   utcd
1508/tcp open   diagmond
7443/tcp open   oracleas-https
9999/tcp open   abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- 하나 이상의 선택한 포트에 대해 포트 수준 네트워크 연결을 설정할 수 없는 경우 빨간색 배너에 ""포트 연결 테스트 실패" 메시지가 나타납니다. nmap 명령 출력은 배너 아래에 나열되어 있습니다.

  빨간색 배너는 원격 호스트의 포트에 대한 TCP 연결 시도가 이루어졌지만 보낸 사람에게 반환된 것이 없음을 나타냅니다. 응답이 반환되지 않으면 포트에 "필터링된" 상태가 있으며 방화벽에 의해 차단될 수 있습니다.

  ⓘ 폐쇄된 항만 목록에 있다.

Port connectivity test failed
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT     STATE    SERVICE
22/tcp   open     ssh
79/tcp   filtered finger
80/tcp   open     http
443/tcp  open     https
1504/tcp closed   evb-elm
1505/tcp open     funkproxy
1506/tcp open     utcd
1508/tcp open     diagmond
7443/tcp open     oracleas-https
9999/tcp open     abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

관련 정보

네트워킹 지침

SANtricity 시스템 관리자(SG5700) 액세스 및 구성

SANtricity 시스템 관리자를 사용하여 스토리지 컨트롤러 쉘프에 있는 스토리지 컨트롤러, 스토리지 디스크 및 기타 하드웨어 구성 요소의 상태를 모니터링할 수 있습니다. 또한 관리 포트를 사용하지 않고 어플라이언스에서 AutoSupport 메시지를 보낼 수 있도록 E-Series AutoSupport에 대한 프록시를 구성할 수도 있습니다.

SANtricity 시스템 관리자를 설정하고 액세스합니다

스토리지 컨트롤러의 하드웨어를 모니터링하거나 E-Series AutoSupport를 구성하려면 스토리지 컨트롤러의 SANtricity System Manager에 액세스해야 할 수 있습니다.

필요한 것

- 을(를) 사용하고 있습니다 지원되는 웹 브라우저.
- 그리드 관리자를 통해 SANtricity 시스템 관리자에 액세스하려면 StorageGRID가 설치되어 있어야 하며 스토리지 어플라이언스 관리자 권한이나 루트 액세스 권한이 있어야 합니다.
- StorageGRID 어플라이언스 설치 프로그램을 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 시스템 관리자 사용자 이름과 암호가 있어야 합니다.
- 웹 브라우저를 통해 SANtricity System Manager에 직접 액세스하려면 SANtricity System Manager 관리자의 사용자 이름과 암호가 있어야 합니다.

> 그리드 관리자 또는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 펌웨어 8.70(11.70) 이상이 있어야 합니다. StorageGRID 어플라이언스 설치 프로그램을 사용하여 * 도움말 * > * 정보 * 를 선택하여 펌웨어 버전을 확인할 수 있습니다.

> 그리드 관리자 또는 어플라이언스 설치 프로그램에서 SANtricity 시스템 관리자에 액세스하는 것은 일반적으로 하드웨어를 모니터링하고 E-Series AutoSupport를 구성하는 데만 사용됩니다. 펌웨어 업그레이드와 같은 SANtricity System Manager 내의 많은 기능과 작업은 StorageGRID 어플라이언스 모니터링에는 적용되지 않습니다. 문제를 방지하려면 항상 어플라이언스에 대한 하드웨어 설치 및 유지 관리 지침을 따르십시오.

이 작업에 대해

설치 및 구성 프로세스 단계에 따라 SANtricity System Manager에 액세스하는 방법에는 세 가지가 있습니다.

- 어플라이언스가 아직 StorageGRID 시스템에 노드로 배포되지 않은 경우 StorageGRID 어플라이언스 설치 프로그램의 고급 탭을 사용해야 합니다.

  > 노드가 배포되면 StorageGRID 어플라이언스 설치 프로그램을 사용하여 SANtricity 시스템 관리자에 액세스할 수 없습니다.

- 어플라이언스가 StorageGRID 시스템에서 노드로 구축된 경우 그리드 관리자의 노드 페이지에서 SANtricity 시스템 관리자 탭을 사용합니다.
- StorageGRID 어플라이언스 설치 관리자 또는 그리드 관리자를 사용할 수 없는 경우 관리 포트에 연결된 웹 브라우저를 사용하여 SANtricity 시스템 관리자에 직접 액세스할 수 있습니다.

이 절차에는 SANtricity 시스템 관리자에 대한 초기 액세스 단계가 포함되어 있습니다. SANtricity 시스템 관리자를 이미 설정한 경우 로 이동합니다 하드웨어 경고를 구성합니다 단계.

> 그리드 관리자 또는 StorageGRID 어플라이언스 설치 프로그램을 사용하면 어플라이언스의 관리 포트를 구성하거나 연결하지 않고도 SANtricity 시스템 관리자에 액세스할 수 있습니다.

SANtricity 시스템 관리자를 사용하여 다음을 모니터링할 수 있습니다.

- 스토리지 어레이 레벨 성능, I/O 지연 시간, CPU 활용률, 처리량 등의 성능 데이터
- 하드웨어 구성 요소 상태입니다
- 진단 데이터 보기를 포함한 지원 기능

SANtricity 시스템 관리자를 사용하여 다음 설정을 구성할 수 있습니다.

- 스토리지 컨트롤러 쉘프에 있는 구성 요소에 대한 e-메일 경고, SNMP 경고 또는 syslog 알림을 제공합니다
- 스토리지 컨트롤러 쉘프의 구성요소에 대한 E-Series AutoSupport 설정입니다.

  E-Series AutoSupport에 대한 자세한 내용은 E-Series 문서 센터를 참조하십시오.

  "NetApp E-Series 시스템 문서 사이트"

- 드라이브 보안 키 - 보안 드라이브 잠금을 해제하는 데 필요(드라이브 보안 기능이 활성화된 경우 이 단계 필요)
- SANtricity 시스템 관리자에 액세스하기 위한 관리자 암호입니다

단계

1. StorageGRID 어플라이언스 설치 프로그램을 사용하여 * 고급 * > * SANtricity 시스템 관리자 * 를 선택합니다

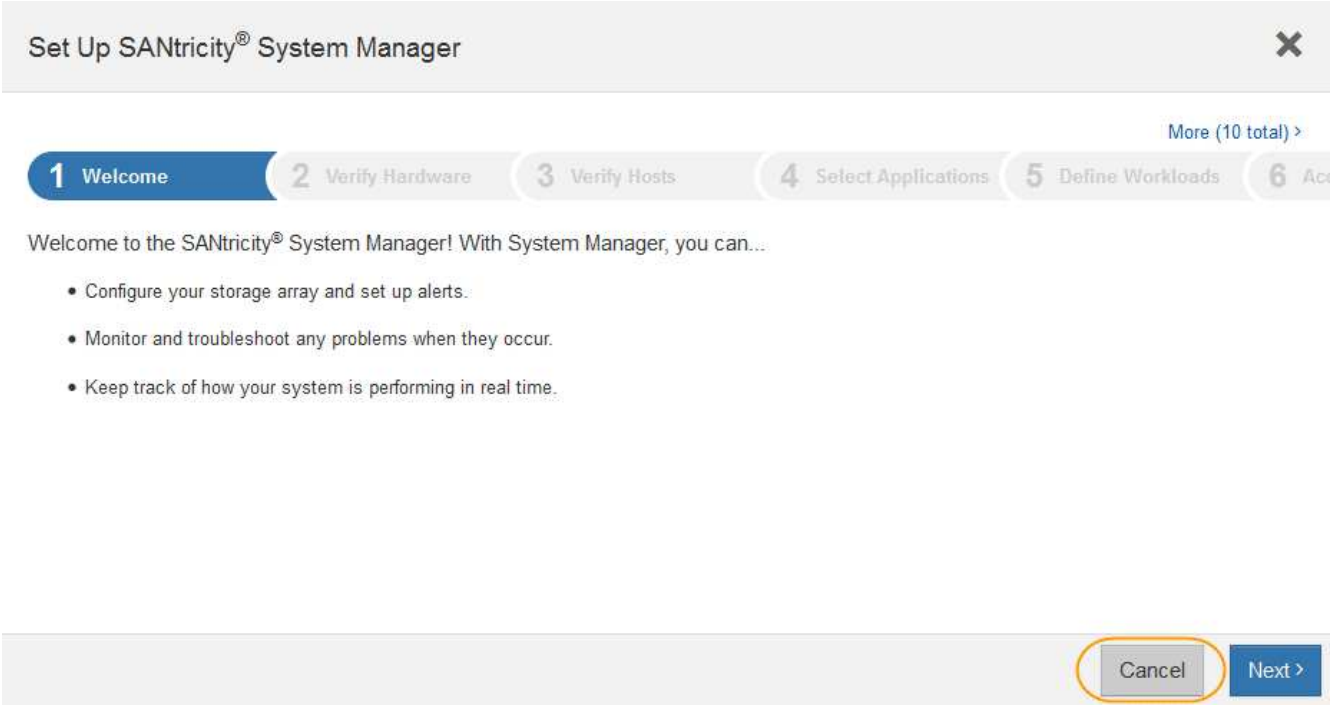
> StorageGRID 어플라이언스 설치 프로그램을 사용할 수 없거나 로그인 페이지가 나타나지 않으면 스토리지 컨트롤러의 IP 주소를 사용해야 합니다. 스토리지 컨트롤러 IP:+' * https://*Storage_Controller_IP**` 검색하여 SANtricity System Manager에 액세스합니다

SANtricity 시스템 관리자의 로그인 페이지가 나타납니다.

2. 관리자 암호를 설정하거나 입력합니다.

> SANtricity 시스템 관리자는 모든 사용자가 공유하는 단일 관리자 암호를 사용합니다.

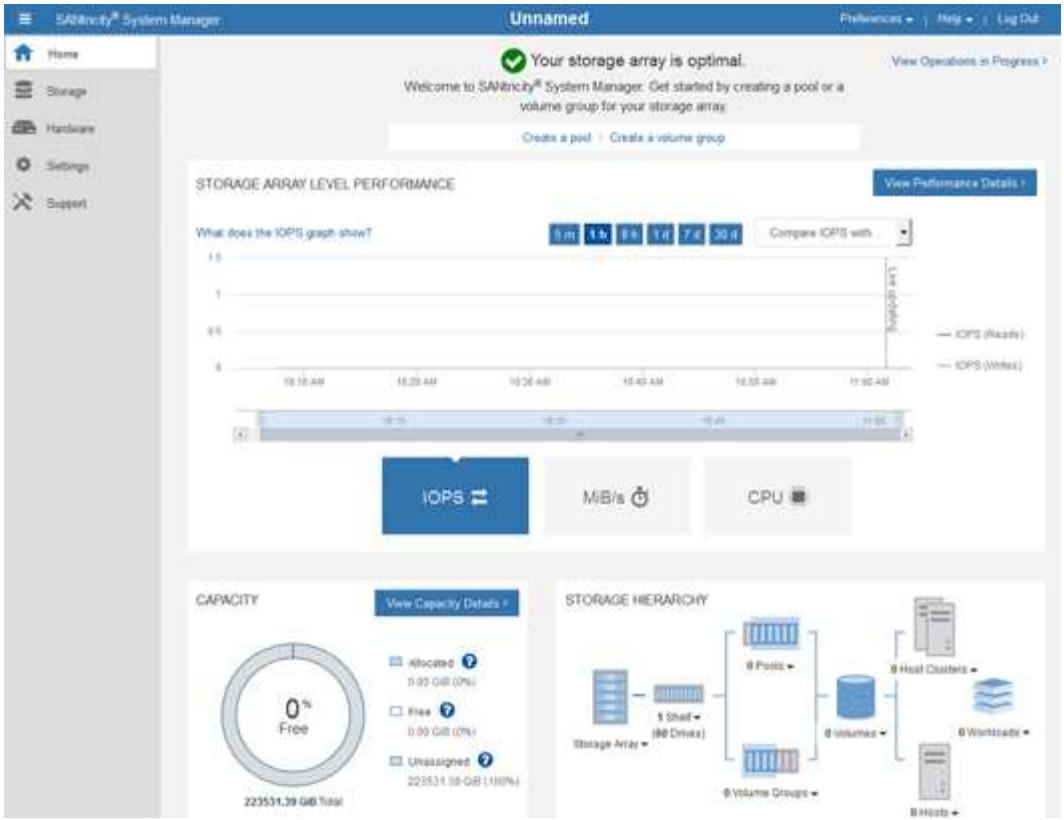
설정 마법사가 나타납니다.



3. 마법사를 닫으려면 * 취소 * 를 선택하십시오.

> StorageGRID 어플라이언스에 대한 설정 마법사를 완료하지 마십시오.

SANtricity 시스템 관리자 홈 페이지가 나타납니다.



4. 하드웨어 경고를 구성합니다.
   a. SANtricity 시스템 관리자의 온라인 도움말을 보려면 * 도움말 * 을 선택하십시오.
   b. 온라인 도움말의 * 설정 * > * 알림 * 섹션을 사용하여 알림에 대해 알아보십시오.
   c. ""방법" 지침에 따라 e-메일 경고, SNMP 경고 또는 syslog 알림을 설정합니다.
5. 스토리지 컨트롤러 쉘프의 구성요소에 대한 AutoSupport를 관리합니다.
   a. SANtricity 시스템 관리자의 온라인 도움말을 보려면 * 도움말 * 을 선택하십시오.
   b. 온라인 도움말의 * 지원 * > * 지원 센터 * 섹션을 사용하여 AutoSupport 기능에 대해 알아보십시오.
   c. AutoSupport를 관리하려면 ""방법" 지침을 따르십시오.

      관리 포트를 사용하지 않고 E-Series AutoSupport 메시지를 보내기 위해 StorageGRID 프록시를 구성하는 방법에 대한 자세한 내용은 StorageGRID 관리 지침으로 이동하여 "E-Series AutoSupport에 대한 프록시 설정"을 검색하십시오.

StorageGRID 관리

6. 어플라이언스에 대해 드라이브 보안 기능이 활성화된 경우 보안 키를 생성하고 관리합니다.
   a. SANtricity 시스템 관리자의 온라인 도움말을 보려면 * 도움말 * 을 선택하십시오.
   b. 드라이브 보안에 대해 알아보려면 온라인 도움말의 * 설정 * > * 시스템 * > * 보안 키 관리 * 섹션을 사용하십시오.
   c. ""방법" 지침에 따라 보안 키를 만들고 관리합니다.
7. 필요에 따라 관리자 암호를 변경합니다.
   a. SANtricity 시스템 관리자의 온라인 도움말을 보려면 * 도움말 * 을 선택하십시오.

b. 온라인 도움말의 * Home * > * 스토리지 배열 관리 * 섹션을 사용하여 관리자 암호에 대해 알아보십시오.

c. "방법" 지침에 따라 암호를 변경합니다.

SANtricity 시스템 관리자에서 하드웨어 상태를 검토합니다

SANtricity 시스템 관리자를 사용하여 스토리지 컨트롤러 쉘프의 개별 하드웨어 구성요소를 모니터링 및 관리하고 하드웨어 진단 및 환경 정보(예: 구성요소 온도)와 드라이브 관련 문제를 검토할 수 있습니다.

필요한 것

- 을(를) 사용하고 있습니다 지원되는 웹 브라우저.
- 그리드 관리자를 통해 SANtricity 시스템 관리자에 액세스하려면 스토리지 어플라이언스 관리자 권한이나 루트 액세스 권한이 있어야 합니다.
- StorageGRID 어플라이언스 설치 프로그램을 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 시스템 관리자 사용자 이름과 암호가 있어야 합니다.
- 웹 브라우저를 통해 SANtricity System Manager에 직접 액세스하려면 SANtricity System Manager 관리자의 사용자 이름과 암호가 있어야 합니다.

> 그리드 관리자 또는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 펌웨어 8.70(11.70) 이상이 있어야 합니다.

> 그리드 관리자 또는 어플라이언스 설치 프로그램에서 SANtricity 시스템 관리자에 액세스하는 것은 일반적으로 하드웨어를 모니터링하고 E-Series AutoSupport를 구성하는 데만 사용됩니다. 펌웨어 업그레이드와 같은 SANtricity System Manager 내의 많은 기능과 작업은 StorageGRID 어플라이언스 모니터링에는 적용되지 않습니다. 문제를 방지하려면 항상 어플라이언스에 대한 하드웨어 설치 및 유지 관리 지침을 따르십시오.

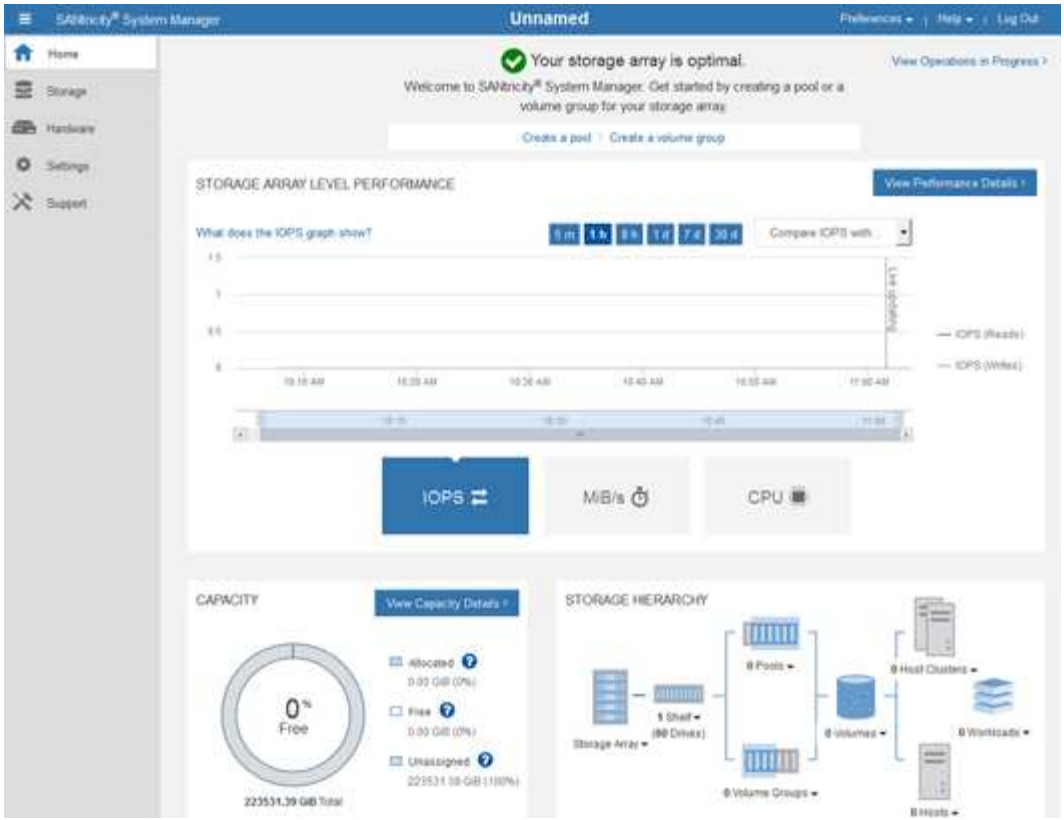
단계

1. SANtricity 시스템 관리자에 액세스합니다.

   SANtricity 시스템 관리자를 설정하고 액세스합니다

2. 필요한 경우 관리자 사용자 이름과 암호를 입력합니다.
3. 설정 마법사를 닫고 SANtricity 시스템 관리자 홈 페이지를 표시하려면 * 취소 * 를 클릭합니다.

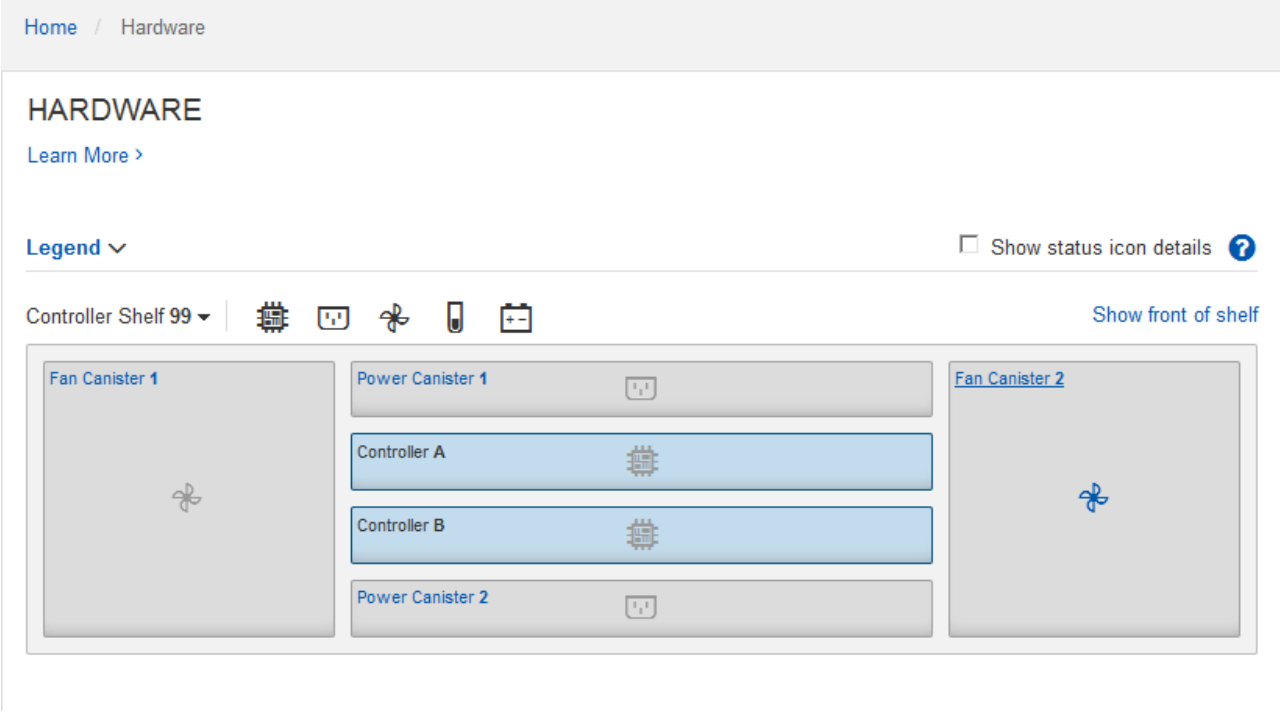
   SANtricity 시스템 관리자 홈 페이지가 나타납니다. SANtricity 시스템 관리자에서 컨트롤러 쉘프는 스토리지 어레이라고 합니다.



4. 어플라이언스 하드웨어에 대해 표시된 정보를 검토하고 모든 하드웨어 구성 요소의 상태가 Optimal(최적)인지 확인합니다.

   a. 하드웨어 * 탭을 클릭합니다.

   b. Show back of shelf * 를 클릭합니다.



쉘프 후면에서 각 스토리지 컨트롤러의 배터리, 2개의 전원 캐니스터, 2개의 팬 캐니스터 및 확장 쉘프(있는 경우)를

모두 볼 수 있습니다. 부품 온도를 볼 수도 있습니다.

a. 각 스토리지 컨트롤러의 설정을 보려면 컨트롤러를 선택하고 컨텍스트 메뉴에서 * 설정 보기 * 를 선택합니다.

b. 쉘프 뒷면에 있는 다른 구성 요소의 설정을 보려면 보려는 구성 요소를 선택합니다.

c. Show front of shelf * 를 클릭하고 보려는 부품을 선택합니다.

   쉘프 전면에서 스토리지 컨트롤러 쉘프 또는 확장 쉘프(있는 경우)에 대한 드라이브 및 드라이브 드로어를 볼 수 있습니다.

구성 요소의 상태에 주의가 필요한 경우 Recovery Guru의 단계에 따라 문제를 해결하거나 기술 지원 부서에 문의하십시오.

StorageGRID 어플라이언스 설치 프로그램을 사용하여 스토리지 컨트롤러의 **IP** 주소를 설정합니다

각 스토리지 컨트롤러의 관리 포트 1은 어플라이언스를 SANtricity 시스템 관리자의 관리 네트워크에 연결합니다. StorageGRID 어플라이언스 설치 프로그램에서 SANtricity 시스템 관리자에 액세스할 수 없는 경우 각 스토리지 컨트롤러의 고정 IP 주소를 설정하여 컨트롤러 쉘프에 있는 하드웨어 및 컨트롤러 펌웨어에 대한 관리 연결이 끊어지지 않도록 해야 합니다.

필요한 것

- StorageGRID 관리 네트워크에 연결할 수 있는 관리 클라이언트를 사용 중이거나 서비스 랩톱을 사용 중입니다.
- 클라이언트 또는 서비스 랩톱에 지원되는 웹 브라우저가 있습니다.

이 작업에 대해

DHCP 할당 주소는 언제든지 변경할 수 있습니다. 고정 IP 주소를 컨트롤러에 할당하여 일관성 있는 접근성을 보장합니다.

> StorageGRID 어플라이언스 설치 프로그램(* 고급*>* SANtricity 시스템 관리자*) 또는 그리드 관리자(* 노드*>* SANtricity 시스템 관리자*)에서 SANtricity 시스템 관리자에 액세스할 수 없는 경우에만 이 절차를 따르십시오.

단계

1. 클라이언트에서 StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. + `https://Appliance_Controller_IP:8443*`

   '*Appliance_Controller_IP*'의 경우 StorageGRID 네트워크에서 어플라이언스의 IP 주소를 사용합니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 하드웨어 구성 * > * 스토리지 컨트롤러 네트워크 구성 * 을 선택합니다.

   스토리지 컨트롤러 네트워크 구성 페이지가 나타납니다.

3. 네트워크 구성에 따라 IPv4, IPv6 또는 둘 다에 대해 * Enabled * 를 선택합니다.
4. 자동으로 표시되는 IPv4 주소를 기록해 둡니다.

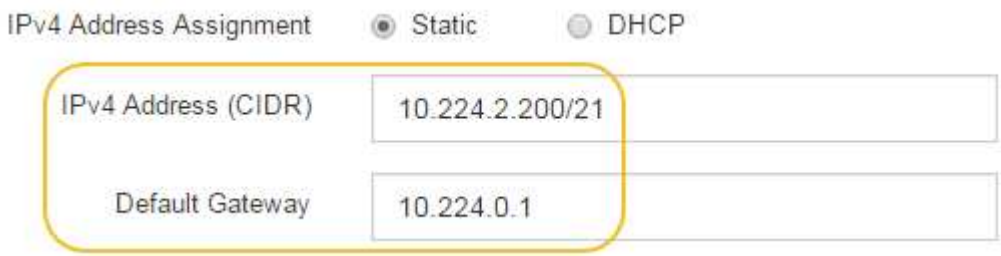
   DHCP는 스토리지 컨트롤러 관리 포트에 IP 주소를 할당하는 기본 방법입니다.

DHCP 값이 나타나려면 몇 분 정도 걸릴 수 있습니다.

5. 필요에 따라 스토리지 컨트롤러 관리 포트에 대한 정적 IP 주소를 설정합니다.

   관리 포트에 고정 IP를 할당하거나 DHCP 서버의 주소에 영구 임대를 할당해야 합니다.

   a. Static * 을 선택합니다.
   b. CIDR 표기법을 사용하여 IPv4 주소를 입력합니다.
   c. 기본 게이트웨이를 입력합니다.



   d. 저장 * 을 클릭합니다.

      변경 사항을 적용하는 데 몇 분 정도 걸릴 수 있습니다.

   SANtricity System Manager에 연결할 때 새 고정 IP 주소를 URL: + `https://*Storage_Controller_IP*` 사용합니다

선택 사항: 노드 암호화를 활성화합니다

노드 암호화를 사용하는 경우 어플라이언스의 디스크는 물리적 손실 또는 사이트 제거로부터 보안 키 관리 서버(KMS) 암호화로 보호할 수 있습니다. 어플라이언스 설치 중에 노드 암호화를 선택하고 활성화해야 하며 KMS 암호화 프로세스가 시작되면 노드 암호화를 선택 취소할 수 없습니다.

필요한 것

StorageGRID 관리 지침에 따라 KMS에 대한 정보를 검토합니다.

이 작업에 대해

노드 암호화가 활성화된 어플라이언스는 StorageGRID 사이트에 대해 구성된 외부 키 관리 서버(KMS)에 연결됩니다. 각 KMS(또는 KMS 클러스터)는 사이트의 모든 어플라이언스 노드에 대한 암호화 키를 관리합니다. 이러한 키는 노드 암호화가 활성화된 어플라이언스에서 각 디스크의 데이터를 암호화하고 해독합니다.

KMS는 제품을 StorageGRID에 설치하기 전이나 설치한 후에 그리드 관리자에서 설정할 수 있습니다. 자세한 내용은 StorageGRID 관리 지침의 KMS 및 어플라이언스 구성에 대한 정보를 참조하십시오.

- KMS가 어플라이언스를 설치하기 전에 설정된 경우 어플라이언스에서 노드 암호화를 사용하도록 설정하고 KMS가 구성된 StorageGRID 사이트에 추가하면 KMS 제어 암호화가 시작됩니다.
- KMS가 어플라이언스를 설치하기 전에 설정되지 않은 경우 KMS가 구성되고 어플라이언스 노드가 포함된 사이트에 대해 사용 가능한 즉시 노드 암호화가 활성화된 각 어플라이언스에 대해 KMS 제어 암호화가 수행됩니다.

> 노드 암호화가 활성화된 어플라이언스에서 KMS에 연결하기 전에 존재하는 데이터는 안전하지 않은 임시 키로 암호화됩니다. KMS에서 제공하는 값으로 키를 설정할 때까지 제품은 제거 또는 도난으로부터 보호되지 않습니다.

디스크 암호를 해독하는 데 필요한 KMS 키가 없으면 어플라이언스의 데이터를 검색할 수 없으며 효과적으로 손실됩니다. 이 경우 암호 해독 키를 KMS에서 검색할 수 없습니다. KMS 구성을 지우거나, KMS 키가 만료되거나, KMS에 대한 연결이 끊어지거나, KMS 키가 설치된 StorageGRID 시스템에서 어플라이언스를 제거하면 이 키에 액세스할 수 없습니다.

단계

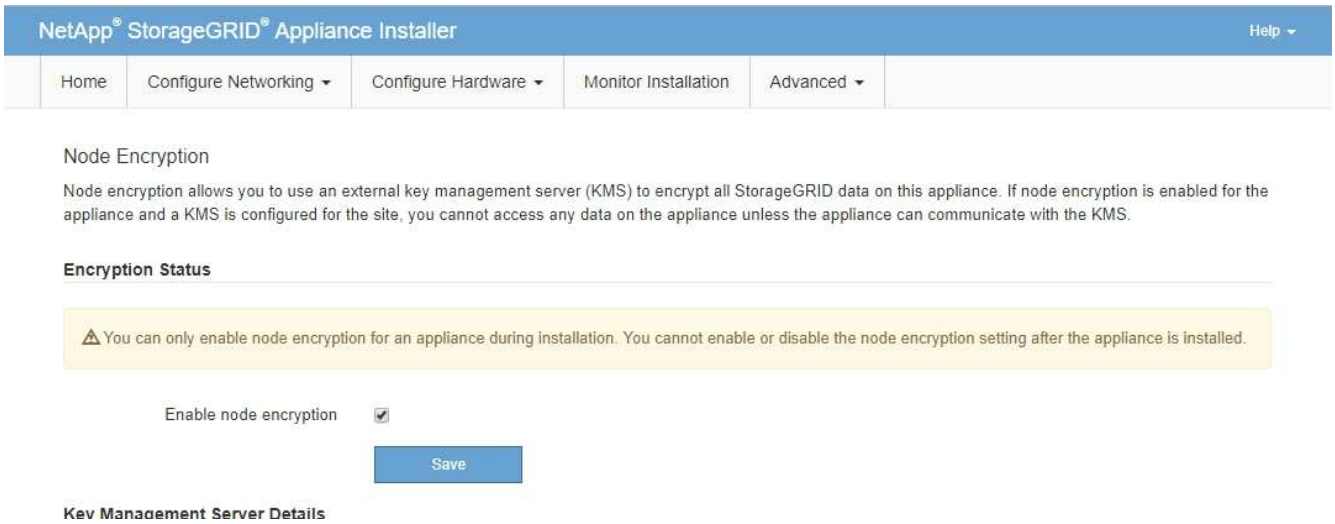
1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

   > KMS 키로 어플라이언스를 암호화한 후에는 동일한 KMS 키를 사용하지 않으면 어플라이언스 디스크를 해독할 수 없습니다.

2. 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.



3. 노드 암호화 사용 * 을 선택합니다.

   어플라이언스를 설치하기 전에 데이터 손실 위험 없이 * 노드 암호화 활성화 * 를 선택 취소할 수 있습니다. 설치가 시작되면 어플라이언스 노드가 StorageGRID 시스템의 KMS 암호화 키에 액세스하여 디스크 암호화를 시작합니다. 어플라이언스를 설치한 후에는 노드 암호화를 비활성화할 수 없습니다.

> KMS가 있는 StorageGRID 사이트에 노드 암호화가 활성화된 어플라이언스를 추가한 후에는 해당 노드에 대해 KMS 암호화 사용을 중지할 수 없습니다.

4. 저장 * 을 선택합니다.
5. 어플라이언스를 StorageGRID 시스템에 노드로 구축하십시오.

   킬로미터 제어 암호화는 어플라이언스가 StorageGRID 사이트에 구성된 KMS 키에 액세스할 때 시작됩니다. KMS 암호화 프로세스 중에 설치 프로그램이 진행률 메시지를 표시합니다. 이 과정은 어플라이언스에 있는 디스크 볼륨 수에 따라 몇 분 정도 걸릴 수 있습니다.

   > 어플라이언스는 처음에 각 디스크 볼륨에 할당된 임의의 비 KMS 암호화 키로 구성됩니다. 이 디스크는 노드 암호화가 활성화된 어플라이언스가 StorageGRID 사이트에 구성된 KMS 키에 액세스할 때까지 안전하지 않은 임시 암호화 키를 사용하여 암호화됩니다.

작업을 마친 후

어플라이언스 노드가 유지보수 모드일 때 노드 암호화 상태, KMS 세부 정보 및 사용 중인 인증서를 볼 수 있습니다.

관련 정보

StorageGRID 관리

유지보수 모드에서 노드 암호화 모니터링(SG5700)

선택 사항**: RAID** 모드 변경**(SG5760**만 해당**)**

드라이브가 60개인 SG5760을 사용하는 경우, 스토리지 및 복구 요구사항을 수용하기 위해 다른 RAID 모드로 변경할 수 있습니다. StorageGRID 어플라이언스 스토리지 노드를 구축하기 전에만 모드를 변경할 수 있습니다.

필요한 것

- SG5760을 가지고 있습니다. SG5712를 사용하는 경우 DDP 모드를 사용해야 합니다.
- StorageGRID에 연결할 수 있는 모든 클라이언트를 사용 중입니다.
- 클라이언트에 가 있습니다 지원되는 웹 브라우저.

이 작업에 대해

SG5760 어플라이언스를 스토리지 노드로 배포하기 전에 다음 볼륨 구성 옵션 중 하나를 선택할 수 있습니다.

- * DDP *: 이 모드는 데이터 드라이브 8개마다 2개의 패리티 드라이브를 사용합니다. 모든 어플라이언스에 대한 기본 권장 모드입니다. RAID6와 비교하여 DDP는 시스템 성능을 향상하고, 드라이브 장애 후 리빌드 시간을 줄이고, 관리를 간소화합니다. DDP는 또한 60-드라이브 어플라이언스에서 드로어 손실을 보호합니다.
- * DDP16 *: 이 모드는 데이터 드라이브 16개마다 2개의 패리티 드라이브를 사용하므로 DDP에 비해 스토리지 효율성이 높습니다. RAID6와 비교했을 때 DDP16은 시스템 성능이 향상되고 드라이브 장애 후 리빌드 시간이 줄어들며 관리가 용이하며 스토리지 효율성이 비슷합니다. DDP16 모드를 사용하려면 구성에 최소 20개의 드라이브가 있어야 합니다. DDP16은 드로어 손실 방지 기능을 제공하지 않습니다.
- * RAID6 *: 이 모드는 16개 이상의 데이터 드라이브마다 2개의 패리티 드라이브를 사용합니다. RAID 6 모드를 사용하려면 구성에 최소 20개의 드라이브가 포함되어 있어야 합니다. RAID6는 DDP와 비교할 때 어플라이언스의 스토리지 효율성을 높일 수 있지만 대부분의 StorageGRID 환경에서는 권장되지 않습니다.

> 볼륨이 이미 구성되었거나 StorageGRID가 이전에 설치된 경우 RAID 모드를 변경하면 볼륨이 제거되고 교체됩니다. 해당 볼륨의 모든 데이터가 손실됩니다.

단계

1. 서비스 랩톱을 사용하여 웹 브라우저를 열고 StorageGRID 어플라이언스 설치 프로그램: + `https://*E5700SG_Controller_IP*:8443* 액세스합니다

   여기서, '*E700SG_Controller_IP*'는 E700SG 컨트롤러의 IP 주소 중 하나를 나타냅니다.

2. 고급 * > * RAID 모드 * 를 선택합니다.
3. RAID 모드 구성 * 페이지의 모드 드롭다운 목록에서 원하는 RAID 모드를 선택합니다.
4. 저장 * 을 클릭합니다.

관련 정보

"NetApp E-Series 시스템 문서 사이트"

옵션: 어플라이언스인 네트워크 포트를 재활용합니다

어플라이언스 스토리지 노드의 내부 포트를 다른 외부 포트에 다시 매핑해야 할 수 있습니다. 예를 들어, 방화벽 문제로 인해 포트를 다시 매핑해야 할 수 있습니다.

필요한 것

- 이전에 StorageGRID 어플라이언스 설치 프로그램에 액세스했습니다.
- 로드 밸런서 엔드포인트를 구성하지 않았거나 구성하지 않을 계획입니다.

> 포트를 재매핑하는 경우 동일한 포트를 사용하여 로드 밸런서 끝점을 구성할 수 없습니다. 로드 밸런서 끝점을 구성하고 이미 포트를 다시 매핑하려면 의 단계를 따릅니다 포트 재맵을 제거합니다.

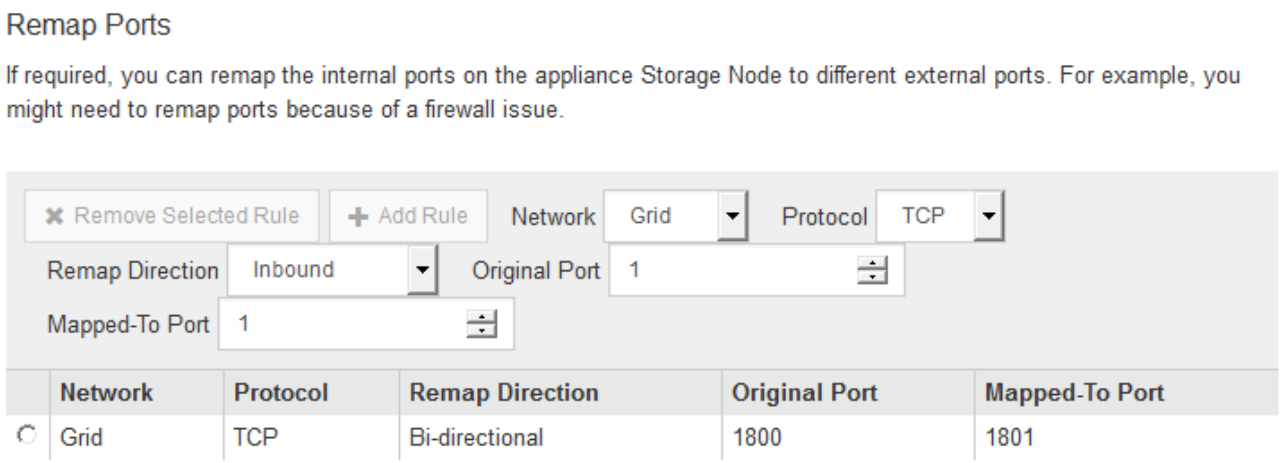
단계

1. StorageGRID 어플라이언스 설치 프로그램의 메뉴 모음에서 * 네트워킹 구성 * > * 재매핑 포트 * 를 클릭합니다.

   Remap Port(재매핑 포트) 페이지가 나타납니다.

2. 네트워크 * 드롭다운 상자에서 그리드, 관리자 또는 클라이언트 중 다시 매핑할 포트의 네트워크를 선택합니다.
3. 프로토콜 * 드롭다운 상자에서 IP 프로토콜(TCP 또는 UDP)을 선택합니다.
4. Remap Direction * (재매핑 방향 *) 드롭다운 상자에서 이 포트에 대해 재매핑할 트래픽 방향(Inbound, Outbound 또는 Bi-directional)을 선택합니다.
5. 원래 포트 * 의 경우 재매핑할 포트 번호를 입력합니다.
6. Mapped-to Port*의 경우 대신 사용할 포트 번호를 입력합니다.
7. 규칙 추가 * 를 클릭합니다.

   새 포트 매핑이 테이블에 추가되고 다시 매핑이 즉시 적용됩니다.



8. 포트 매핑을 제거하려면 제거할 규칙의 라디오 버튼을 선택하고 * 선택한 규칙 제거 * 를 클릭합니다.

어플라이언스 스토리지 노드 구축

스토리지 어플라이언스를 설치 및 구성한 후 StorageGRID 시스템에서 스토리지 노드로 구축할 수 있습니다. 어플라이언스를 스토리지 노드로 배포할 때는 어플라이언스에 포함된 StorageGRID 어플라이언스 설치 프로그램을 사용합니다.

필요한 것

- 어플라이언스 노드를 클론 생성하는 경우 복구 및 유지 보수 프로세스를 계속 수행합니다.

  복구 및 유지 관리

- 이 제품은 랙 또는 캐비닛에 설치되었고 네트워크에 연결되어 있으며 전원이 켜져 있습니다.
- StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스에 대해 네트워크 링크, IP 주소 및 포트 재매핑(필요한 경우)이 구성되었습니다.
- 어플라이언스의 컴퓨팅 컨트롤러에 할당된 IP 주소 중 하나를 알고 있습니다. 연결된 모든 StorageGRID 네트워크에 대해 IP 주소를 사용할 수 있습니다.
- StorageGRID 시스템의 기본 관리 노드가 배포되었습니다.
- StorageGRID 어플라이언스 설치 프로그램의 IP 구성 페이지에 나열된 모든 그리드 네트워크 서브넷은 기본 관리 노드의 그리드 네트워크 서브넷 목록에 정의되어 있습니다.
- 지원되는 웹 브라우저가 있는 서비스 랩톱이 있습니다.

이 작업에 대해

각 스토리지 어플라이언스는 단일 스토리지 노드로 작동합니다. 모든 어플라이언스는 그리드 네트워크, 관리 네트워크 및 클라이언트 네트워크에 연결할 수 있습니다

어플라이언스 스토리지 노드를 StorageGRID 시스템에 배포하려면 StorageGRID 어플라이언스 설치 프로그램에 액세스하여 다음 단계를 수행합니다.

- 운영 관리 노드의 IP 주소와 스토리지 노드의 이름을 지정하거나 확인합니다.
- 구축을 시작하고 볼륨이 구성되고 소프트웨어가 설치될 때까지 기다립니다.

- 어플라이언스 설치 작업이 중간에 일시 중지되면 그리드 관리자에 로그인하고 모든 그리드 노드를 승인하고 StorageGRID 설치 및 배포 프로세스를 완료하여 설치를 다시 시작합니다.

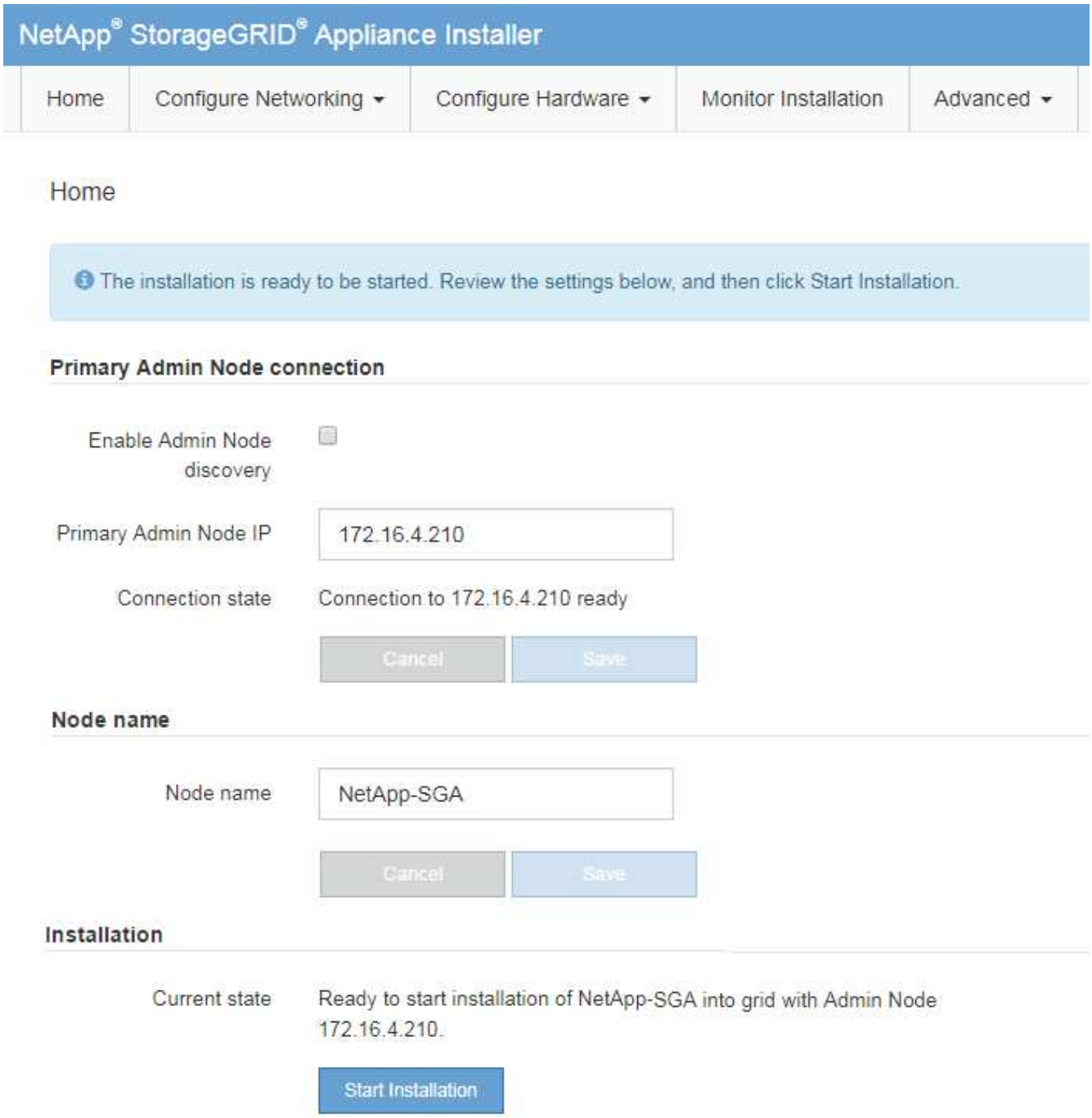
> 한 번에 여러 어플라이언스 노드를 구축해야 하는 경우 'configure-sGA.py' 어플라이언스 설치 스크립트를 사용하여 설치 프로세스를 자동화할 수 있습니다.

- 확장 또는 복구 작업을 수행하는 경우 해당 지침을 따르십시오.
  - 기존 StorageGRID 시스템에 어플라이언스 스토리지 노드를 추가하려면 StorageGRID 시스템 확장 지침을 참조하십시오.
  - 복구 작업의 일부로 어플라이언스 스토리지 노드를 배포하려면 복구 및 유지 관리 지침을 참조하십시오.

단계

1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.



2. Primary Admin Node connection * 섹션에서 Primary Admin Node의 IP 주소를 지정해야 하는지 여부를 확인합니다.

   이전에 이 데이터 센터에 다른 노드를 설치한 경우 StorageGRID 어플라이언스 설치 관리자는 기본 관리 노드 또는 admin_IP가 구성된 다른 그리드 노드가 동일한 서브넷에 있다고 가정하여 이 IP 주소를 자동으로 검색할 수 있습니다.

3. 이 IP 주소가 표시되지 않거나 변경해야 하는 경우 주소를 지정합니다.

옵션을 선택합니다	설명
수동 IP 입력	a. 관리자 노드 검색 사용 * 확인란의 선택을 취소합니다. b. IP 주소를 수동으로 입력합니다. c. 저장 * 을 클릭합니다. d. 새 IP 주소가 준비될 때까지 연결 상태를 기다립니다.
연결된 모든 운영 관리 노드의 자동 검색	a. 관리자 노드 검색 사용 * 확인란을 선택합니다. b. 검색된 IP 주소 목록이 표시될 때까지 기다립니다. c. 이 어플라이언스 스토리지 노드를 구축할 그리드의 기본 관리 노드를 선택합니다. d. 저장 * 을 클릭합니다. e. 새 IP 주소가 준비될 때까지 연결 상태를 기다립니다.

4. 노드 이름 * 필드에 이 어플라이언스 노드에 사용할 이름을 입력하고 * 저장 * 을 클릭합니다.

   노드 이름은 StorageGRID 시스템의 이 어플라이언스 노드에 할당됩니다. 그리드 관리자의 노드 페이지(개요 탭)에 표시됩니다. 필요한 경우 노드를 승인할 때 이름을 변경할 수 있습니다.

5. 설치 * 섹션에서 현재 상태가 "기본 관리 노드 "*admin_ip*"이(가) 있는 그리드에 "*node name*"의 설치를 시작할 준비가 되었으며 * 설치 시작 * 버튼이 활성화되어 있는지 확인합니다.

   설치 시작 * 버튼이 활성화되지 않은 경우 네트워크 구성 또는 포트 설정을 변경해야 할 수 있습니다. 자세한 내용은 제품의 설치 및 유지보수 지침을 참조하십시오.

   > 스토리지 노드 어플라이언스를 노드 클론 생성 타겟으로 구축하는 경우 여기서 구축 프로세스를 중지하고 복구 및 유지 관리에서 노드 클론 생성 절차를 계속 진행하십시오.

   복구 및 유지 관리

6. StorageGRID 어플라이언스 설치 관리자 홈 페이지에서 * 설치 시작 * 을 클릭합니다.

   현재 상태가 ""설치 진행 중""으로 변경되고 모니터 설치 페이지가 표시됩니다.

   > 모니터 설치 페이지에 수동으로 액세스해야 하는 경우 * 모니터 설치 * 를 클릭합니다.

7. 그리드에 여러 어플라이언스 스토리지 노드가 포함된 경우 각 어플라이언스에 대해 이 단계를 반복합니다.

   > 한 번에 여러 어플라이언스 스토리지 노드를 구축해야 하는 경우 "configure-sGA.py" 어플라이언스 설치 스크립트를 사용하여 설치 프로세스를 자동화할 수 있습니다.

관련 정보

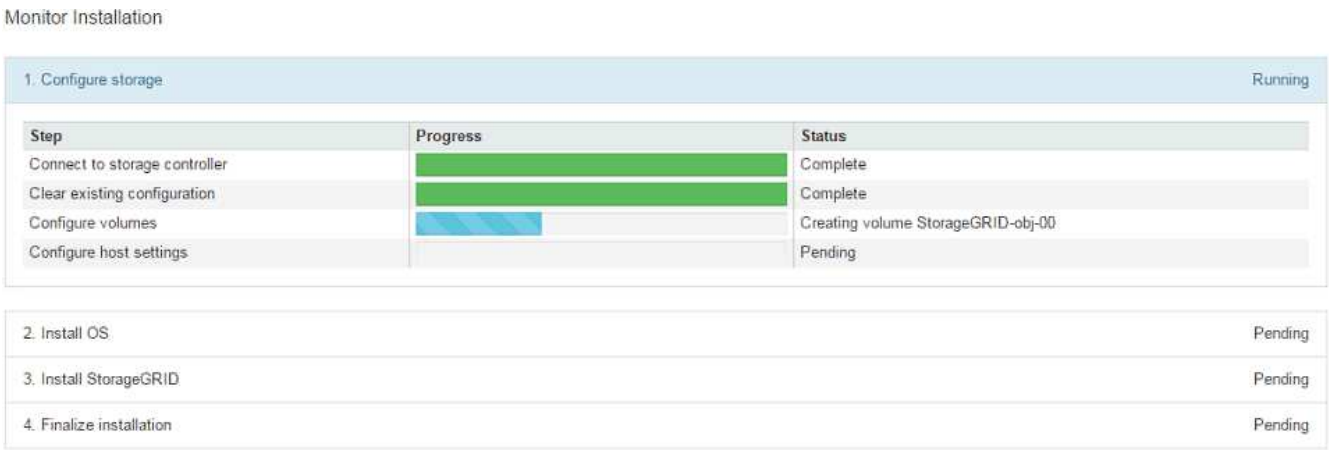
스토리지 어플라이언스 설치를 모니터링합니다

StorageGRID 어플라이언스 설치 프로그램은 설치가 완료될 때까지 상태를 제공합니다. 소프트웨어 설치가 완료되면 어플라이언스가 재부팅됩니다.

단계

1. 설치 진행률을 모니터링하려면 * 모니터 설치 * 를 클릭합니다.

   Monitor Installation(모니터 설치) 페이지에 설치 진행률이 표시됩니다.

   파란색 상태 표시줄은 현재 진행 중인 작업을 나타냅니다. 녹색 상태 표시줄은 성공적으로 완료된 작업을 나타냅니다.

   > 설치 프로그램은 이전 설치에서 완료된 작업이 다시 실행되지 않도록 합니다. 설치를 다시 실행할 경우 다시 실행할 필요가 없는 작업은 녹색 상태 표시줄과 "중단" 상태로 표시됩니다.

2. 처음 두 설치 단계의 진행 상황을 검토합니다.

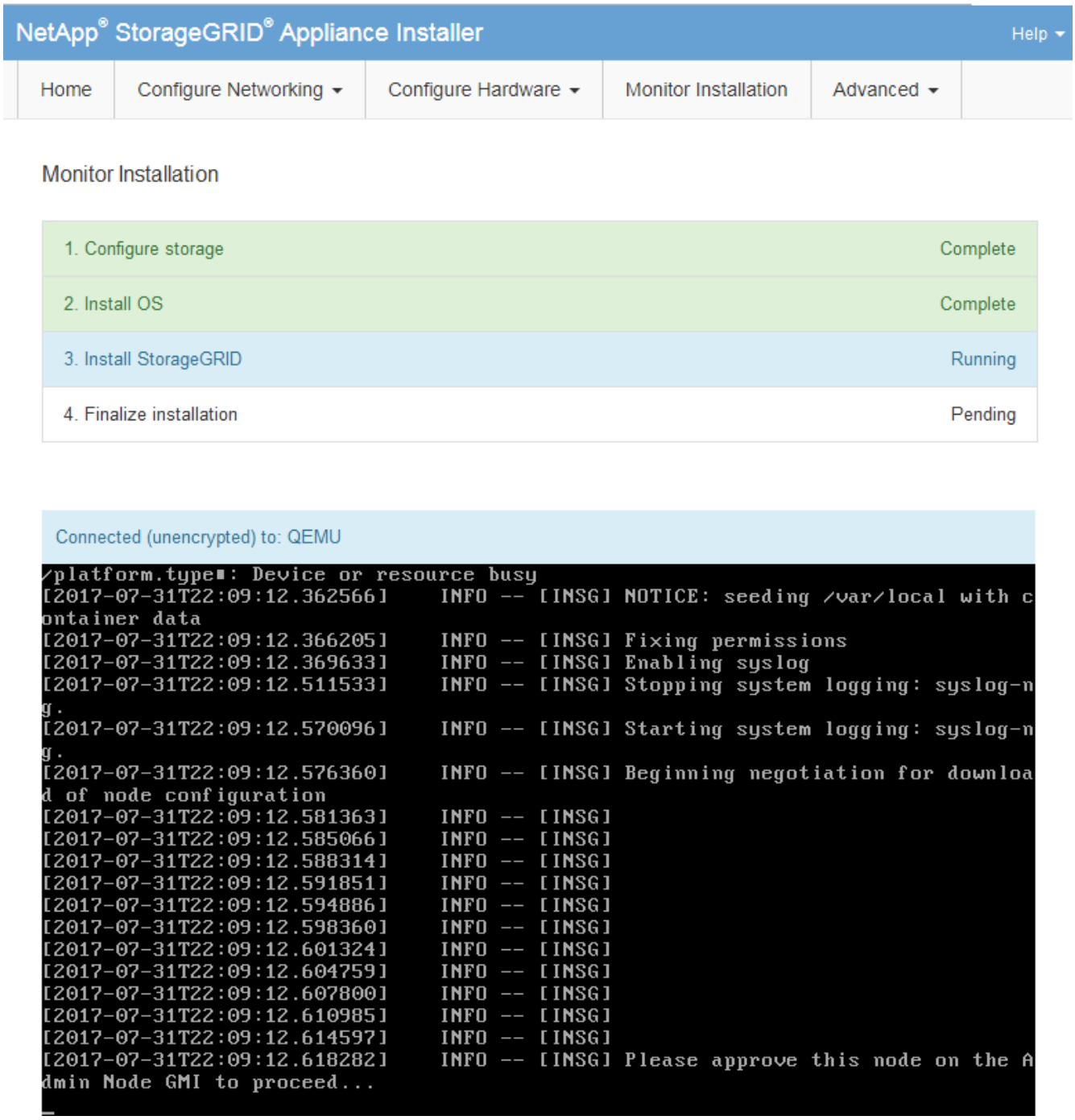
   - 1. 스토리지 구성 *

     이 단계에서 설치 관리자는 스토리지 컨트롤러에 연결하고, 기존 구성을 지우고, SANtricity 소프트웨어와 통신하여 볼륨을 구성하고, 호스트 설정을 구성합니다.

   - 2. OS * 를 설치합니다

   이 단계에서 설치 프로그램은 StorageGRID의 기본 운영 체제 이미지를 어플라이언스에 복사합니다.

3. StorageGRID* 설치 단계가 일시 중지되고 그리드 관리자를 사용하여 관리 노드에서 이 노드를 승인하라는 메시지가 포함된 콘솔에 표시될 때까지 설치 진행 상태를 계속 모니터링합니다. 다음 단계로 이동합니다.



4. 운영 관리 노드의 그리드 관리자로 이동하여 보류 중인 스토리지 노드를 승인하고 StorageGRID 설치 프로세스를 완료합니다.

   Grid Manager에서 * Install * 을 클릭하면 단계 3이 완료되고 단계 4, * 설치 완료 * 가 시작됩니다. 4단계가 완료되면 컨트롤러가 재부팅됩니다.

어플라이언스 설치 및 구성 자동화(SG5700)

어플라이언스의 설치 및 구성과 전체 StorageGRID 시스템의 구성을 자동화할 수 있습니다.

이 작업에 대해

설치 및 구성 자동화는 여러 StorageGRID 인스턴스 또는 하나의 크고 복잡한 StorageGRID 인스턴스를 구축하는 데 유용할 수 있습니다.

설치 및 구성을 자동화하려면 다음 옵션 중 하나 이상을 사용하십시오.

- 어플라이언스의 구성 설정을 지정하는 JSON 파일을 생성합니다. StorageGRID 어플라이언스 설치 프로그램을 사용하여 JSON 파일을 업로드합니다.

  동일한 파일을 사용하여 여러 어플라이언스를 구성할 수 있습니다.

- StorageGRID ``configure-sGA.py'' Python 스크립트를 사용하여 어플라이언스 구성을 자동화합니다.
- 추가 Python 스크립트를 사용하여 전체 StorageGRID 시스템의 다른 구성 요소("그리드")를 구성합니다.

  StorageGRID 자동화 Python 스크립트를 직접 사용하거나 직접 개발한 그리드 구축 및 구성 도구에서 StorageGRID 설치 REST API를 사용하는 방법의 예로 사용할 수 있습니다. 에 대한 정보를 참조하십시오 StorageGRID 설치 파일 다운로드 및 추출 을 참조하십시오.

StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스 구성을 자동화합니다

구성 정보가 포함된 JSON 파일을 사용하여 어플라이언스 구성을 자동화할 수 있습니다. StorageGRID 어플라이언스 설치 프로그램을 사용하여 파일을 업로드합니다.

필요한 것

- 어플라이언스는 StorageGRID 11.5 이상과 호환되는 최신 펌웨어에 있어야 합니다.
- 를 사용하여 구성하는 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램에 연결되어 있어야 합니다 지원되는 웹 브라우저.

이 작업에 대해

다음과 같은 어플라이언스 구성 작업을 자동화할 수 있습니다.

- Grid Network, Admin Network 및 Client Network IP 주소입니다
- BMC 인터페이스
- 네트워크 링크
  - 포트 결합 모드
  - 네트워크 연결 모드
  - 링크 속도

업로드된 JSON 파일을 사용하여 어플라이언스를 구성하는 것이 StorageGRID 어플라이언스 설치 프로그램에서 여러 페이지를 사용하여 수동으로 구성하는 것보다 더 효율적인 경우가 많습니다. 특히 여러 노드를 구성해야 하는 경우 더욱 그렇습니다. 각 노드에 대해 한 번에 하나씩 구성 파일을 적용해야 합니다.

어플라이언스의 설치와 구성을 모두 자동화하려는 숙련된 사용자는 'configure-sGA.py' 스크립트를 사용할 수 있습니다. 를 누릅니다configure-sga.py 스크립트를 사용하여 어플라이언스 노드의 설치 및 구성을 자동화합니다

단계

1. 다음 방법 중 하나를 사용하여 JSON 파일을 생성합니다.
   - ConfigBuilder 응용 프로그램

     "ConfigBuilder.netapp.com"

   - 'configure-sGA.py' 어플라이언스 구성 스크립트 StorageGRID 어플라이언스 설치 프로그램(* 도움말*>* 어플라이언스 구성 스크립트*)에서 스크립트를 다운로드할 수 있습니다. configure-sga.py 스크립트를 사용하여 구성 자동화에 대한 지침을 참조하십시오.

     configure-sga.py 스크립트를 사용하여 어플라이언스 노드의 설치 및 구성을 자동화합니다

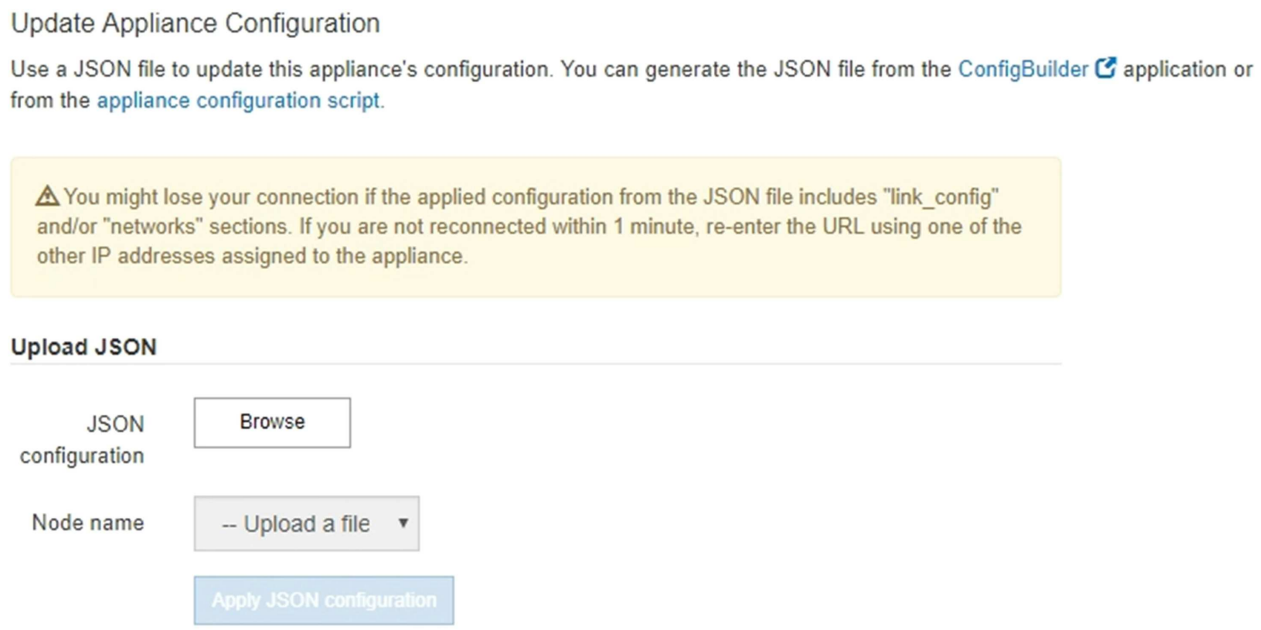
     JSON 파일의 노드 이름은 다음 요구사항을 충족해야 합니다.

     - 1자 이상 32자 이하의 유효한 호스트 이름이어야 합니다
     - 문자, 숫자 및 하이픈을 사용할 수 있습니다
     - 하이픈으로 시작하거나 끝날 수 없습니다
     - 숫자만 포함하거나 사용할 수 없습니다

     > JSON 파일의 노드 이름(최상위 이름)이 고유한지 확인하십시오. 그렇지 않으면 JSON 파일을 사용하여 둘 이상의 노드를 구성할 수 없습니다.

2. Advanced * > * Update Appliance Configuration * 을 선택합니다.

   어플라이언스 구성 업데이트 페이지가 나타납니다.

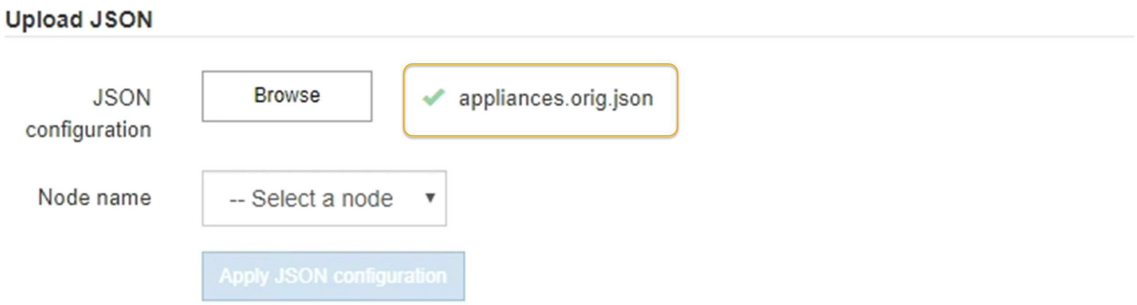


3. 업로드할 구성이 있는 JSON 파일을 선택합니다.
   a. 찾아보기 * 를 선택합니다.
   b. 파일을 찾아 선택합니다.

c. 열기 * 를 선택합니다.

파일이 업로드되고 검증됩니다. 유효성 검사 프로세스가 완료되면 녹색 확인 표시 옆에 파일 이름이 표시됩니다.

> JSON 파일의 구성에 "link_config", "networks" 또는 둘 다에 대한 섹션이 포함된 경우 어플라이언스에 대한 연결이 끊어질 수 있습니다. 1분 이내에 다시 연결되지 않으면 어플라이언스에 할당된 다른 IP 주소 중 하나를 사용하여 어플라이언스 URL을 다시 입력하십시오.

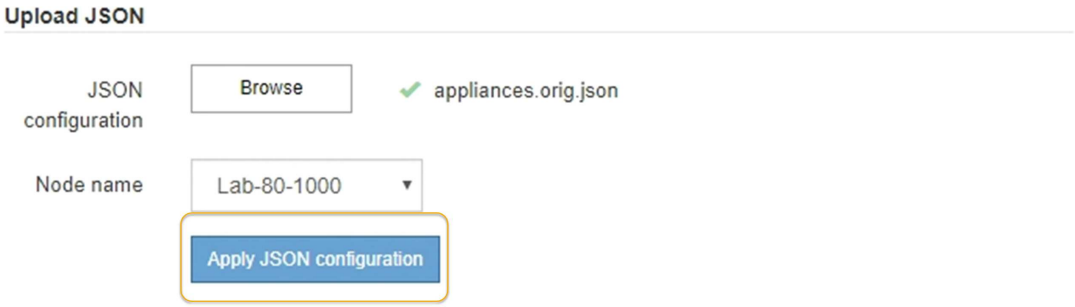


노드 이름 * 드롭다운은 JSON 파일에 정의된 최상위 노드 이름으로 채워집니다.

> 파일이 유효하지 않으면 파일 이름이 빨간색으로 표시되고 오류 메시지가 노란색 배너에 표시됩니다. 잘못된 파일이 어플라이언스에 적용되지 않습니다. ConfigBuilder를 사용하여 올바른 JSON 파일이 있는지 확인할 수 있습니다.

4. 노드 이름 * 드롭다운 목록에서 노드를 선택합니다.

   JSON 설정 적용 * 버튼이 활성화됩니다.



5. JSON 구성 적용 * 을 선택합니다.

   선택한 노드에 구성이 적용됩니다.

configure-sga.py 스크립트를 사용하여 어플라이언스 노드의 설치 및 구성을 자동화합니다

'configure-sGA.py' 스크립트를 사용하면 기본 관리 노드의 설치 및 구성을 포함하여 StorageGRID 어플라이언스 노드에 대한 많은 설치 및 구성 작업을 자동화할 수 있습니다. 이

스크립트는 구성할 어플라이언스가 많은 경우 유용할 수 있습니다. 또한 스크립트를 사용하여 어플라이언스 구성 정보가 포함된 JSON 파일을 생성할 수도 있습니다.

이 작업에 대해

- 이 어플라이언스는 랙에 설치되어 있고 네트워크에 연결되어 있으며 전원이 켜져 있습니다.
- 네트워크 링크 및 IP 주소는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 기본 관리 노드에 대해 구성되었습니다.
- 기본 관리 노드를 설치하는 경우 해당 IP 주소를 알 수 있습니다.
- 다른 노드를 설치 및 구성하는 경우 기본 관리 노드가 배포되었으며 해당 IP 주소를 알고 있는 것입니다.
- 기본 관리 노드 이외의 모든 노드의 경우 StorageGRID 어플라이언스 설치 프로그램의 IP 구성 페이지에 나열된 모든 그리드 네트워크 서브넷이 기본 관리 노드의 그리드 네트워크 서브넷 목록에 정의되어 있습니다.
- 'configure-sGA.py' 파일을 다운로드했습니다. 이 파일은 설치 아카이브에 포함되어 있거나 StorageGRID 어플라이언스 설치 프로그램에서 * 도움말 * > * 어플라이언스 설치 스크립트 * 를 클릭하여 액세스할 수 있습니다.

> 이 절차는 명령줄 인터페이스를 사용하는 일부 경험이 있는 고급 사용자를 위한 것입니다. 또는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 구성을 자동화할 수도 있습니다. 를 누릅니다StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스 구성을 자동화합니다

단계

1. Python 스크립트를 실행하기 위해 사용 중인 Linux 시스템에 로그인합니다.
2. 스크립트 구문에 대한 일반적인 도움말과 사용 가능한 매개 변수 목록을 보려면 다음을 입력합니다.

   ```
   configure-sga.py --help
   ```

   'configure-sGA.py' 스크립트는 5개의 하위 명령을 사용합니다.

   - BMC 구성 및 어플라이언스의 현재 구성이 포함된 JSON 파일을 생성하는 등 고급 StorageGRID 어플라이언스 상호 작용을 위한 '고급' 기능입니다
   - RAID 모드, 노드 이름 및 네트워킹 매개 변수를 구성하기 위한 'configure'
   - StorageGRID 설치 시작을 위한 '설치'입니다
   - StorageGRID 설치 모니터링을 위한 모니터
   - 어플라이언스를 재부팅하기 위한 재부팅

   하위 명령(advanced, configure, install, monitor, reboot) 인수 뒤에 '--help' 옵션을 입력하면 해당 하위 명령 내에서 사용할 수 있는 옵션에 대한 자세한 내용을 제공하는 다른 도움말 텍스트가 표시됩니다. + "configure-sga.py_subcommand_—help

3. 어플라이언스 노드의 현재 구성을 확인하려면 다음과 같이 입력합니다. 여기서 "*SGA-INSTALL-IP*"는 어플라이언스 노드의 IP 주소 중 하나입니다. + "configure-sga.py configure_sGA-install-ip_

   이 결과는 기본 관리 노드의 IP 주소와 관리, 그리드 및 클라이언트 네트워크에 대한 정보를 포함하여 어플라이언스에 대한 현재 IP 정보를 표시합니다.

   ```
   Connecting to +https://10.224.2.30:8443+ (Checking version and
   ```

```
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200

  StorageGRID Appliance
    Name:        LAB-SGA-2-30
    Node type:   storage

  StorageGRID primary Admin Node
    IP:        172.16.1.170
    State:     unknown
    Message:   Initializing...
    Version:   Unknown

  Network Link Configuration
    Link Status
          Link      State      Speed (Gbps)
          ----      -----      -----
          1         Up         10
          2         Up         10
          3         Up         10
          4         Up         10
          5         Up         1
          6         Down       N/A

    Link Settings
        Port bond mode:      FIXED
        Link speed:          10GBE

        Grid Network:        ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

        Admin Network:       ENABLED
            Bonding mode:    no-bond
            MAC Addresses:   00:80:e5:29:70:f4
```

```
        Client Network:      ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

  Grid Network
    CIDR:      172.16.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:8A
    Gateway:   172.16.0.1
    Subnets:   172.17.0.0/21
               172.18.0.0/21
               192.168.0.0/21
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

#################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#################################################################
```

4. 현재 설정의 값을 변경해야 하는 경우 '설정' 하위 명령을 사용하여 값을 업데이트합니다. 예를 들어, 어플라이언스가 기본 관리 노드에 연결하기 위해 사용하는 IP 주소를 ' 172.16.2.99 '로 변경하려면 + ' configure-sga.py configure - -admin -ip 172.16.2.99_sga -install -ip_'를 입력합니다
5. 어플라이언스 구성을 JSON 파일로 백업하려면 고급 및 백업 파일 하위 명령을 사용하십시오. 예를 들어, IP 주소 '*SGA-INSTALL-IP*'를 사용하는 어플라이언스 구성을 어플라이언스-SG1000.json'이라는 파일에 백업하려면 + "configure-sga.py advanced—backup-file appliance-SG1000.json_sga-install-ip_"를 입력합니다

   구성 정보가 포함된 JSON 파일은 에서 스크립트를 실행한 디렉토리에 작성됩니다.

   > 생성된 JSON 파일의 최상위 노드 이름이 어플라이언스 이름과 일치하는지 확인하십시오. 숙련된 사용자이고 StorageGRID API에 대한 철저한 이해가 없는 경우 이 파일을 변경하지 마십시오.

6. 어플라이언스 구성이 만족스러우면 "install" 및 "monitor" 하위 명령을 사용하여 어플라이언스를 설치합니다. + "configure-sga.py install—monitor_sga-install-ip_"
7. 어플라이언스를 재부팅하려면 + "configure-sga.py reboot_sga-install-ip_"를 입력합니다

StorageGRID 구성 자동화

그리드 노드를 구축한 후 StorageGRID 시스템 구성을 자동화할 수 있습니다.

필요한 것

- 설치 아카이브에서 다음 파일의 위치를 알고 있습니다.

파일 이름	설명
configure-StorageGrid.py의 약어입니다	구성을 자동화하는 데 사용되는 Python 스크립트입니다
configure-StorageGrid.sample.json	스크립트와 함께 사용할 샘플 구성 파일
configure-StorageGrid.blank.json	스크립트에 사용할 빈 구성 파일입니다

- "configure-StorageGrid.json" 구성 파일을 만들었습니다. 이 파일을 만들려면 샘플 구성 파일('configure-StorageGrid.sample.json') 또는 빈 구성 파일('configure-StorageGrid.blank.json')을 수정할 수 있습니다.

이 작업에 대해

configure-StorageGrid.py Python 스크립트와 configure-StorageGrid.json 구성 파일을 사용하여 StorageGRID 시스템 구성을 자동화할 수 있습니다.

> 그리드 관리자 또는 설치 API를 사용하여 시스템을 구성할 수도 있습니다.

단계

1. Python 스크립트를 실행하기 위해 사용 중인 Linux 시스템에 로그인합니다.
2. 설치 아카이브를 추출한 디렉토리로 변경합니다.

   예: + 'cd StorageGRID-Webscale -*version/platform*

   여기서, 'platform'은 'dEBS', 'rpms', 'vSphere'입니다.

3. Python 스크립트를 실행하고 생성한 구성 파일을 사용합니다.

   예를 들면 다음과 같습니다.

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

작업을 마친 후

복구 패키지 '.zip' 파일은 구성 프로세스 중에 생성되며 설치 및 구성 프로세스를 실행 중인 디렉토리에 다운로드됩니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 백업해야 합니다. 예를 들어, 안전한 백업 네트워크 위치 및 안전한 클라우드 저장소 위치에 복사합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

임의 암호를 생성해야 한다고 지정한 경우 "passwords.txt" 파일을 추출하고 StorageGRID 시스템에 액세스하는 데 필요한 암호를 찾아야 합니다.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                  StorageGRID node recovery.                #####
######################################################################
```

확인 메시지가 표시되면 StorageGRID 시스템이 설치 및 구성됩니다.

```
StorageGRID has been configured and installed.
```

REST API 설치 개요

StorageGRID는 설치 작업을 수행하기 위한 두 가지 REST API, 즉 StorageGRID 설치 API와 StorageGRID 어플라이언스 설치 관리자 API를 제공합니다.

두 API 모두 Swagger 오픈 소스 API 플랫폼을 사용하여 API 문서를 제공합니다. swagger를 사용하면 개발자와 개발자가 아닌 사용자가 API가 매개 변수 및 옵션에 어떻게 응답하는지 보여주는 사용자 인터페이스에서 API와 상호 작용할 수 있습니다. 이 문서에서는 표준 웹 기술 및 JSON(JavaScript Object Notation) 데이터 형식에 대해 잘 알고 있다고 가정합니다.

> API Docs 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

각 REST API 명령에는 API의 URL, HTTP 작업, 필수 또는 선택적 URL 매개 변수, 그리고 예상되는 API 응답이 포함됩니다.

StorageGRID 설치 API

StorageGRID 설치 API는 StorageGRID 시스템을 처음 구성할 때와 기본 관리자 노드 복구를 수행해야 하는 경우에만 사용할 수 있습니다. 설치 API는 Grid Manager에서 HTTPS를 통해 액세스할 수 있습니다.

API 설명서에 액세스하려면 기본 관리 노드의 설치 웹 페이지로 이동하여 메뉴 모음에서 * 도움말 * > * API 설명서 * 를 선택합니다.

StorageGRID 설치 API에는 다음 섹션이 포함되어 있습니다.

- * config * — 제품 릴리스 및 API 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 API의 주요 버전을 나열할 수 있습니다.
- * 그리드 * — 그리드 레벨 구성 작업. 그리드 세부 정보, 그리드 네트워크 서브넷, 그리드 암호, NTP 및 DNS 서버 IP

주소를 포함한 그리드 설정을 얻고 업데이트할 수 있습니다.

- * 노드 * — 노드 레벨 구성 작업 그리드 노드 목록을 검색하고, 그리드 노드를 삭제하고, 그리드 노드를 구성하고, 그리드 노드를 보고, 그리드 노드의 구성을 재설정할 수 있습니다.
- * 프로비저닝 * — 프로비저닝 작업. 프로비저닝 작업을 시작하고 프로비저닝 작업의 상태를 볼 수 있습니다.
- * 복구 * — 기본 관리 노드 복구 작업 정보를 재설정하고, 복구 패키지를 업로드하고, 복구를 시작하고, 복구 작업의 상태를 볼 수 있습니다.
- * recovery-package * — 복구 패키지를 다운로드하기 위한 작업.
- * 사이트 * — 사이트 수준 구성 작업 사이트를 만들고, 보고, 삭제하고, 수정할 수 있습니다.

StorageGRID 어플라이언스 설치 관리자 **API**입니다

StorageGRID 어플라이언스 설치 프로그램 API는 HTTPS를 통해 '*Controller_IP*:8443'에서 액세스할 수 있습니다.

API 설명서에 액세스하려면 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램으로 이동하여 메뉴 모음에서 * 도움말 * > * API Docs * 를 선택합니다.

StorageGRID 어플라이언스 설치 관리자 API에는 다음 섹션이 포함되어 있습니다.

- * 클론 * — 노드 클로닝을 구성하고 제어하는 작업.
- * 암호화 * — 암호화를 관리하고 암호화 상태를 확인하는 작업.
- * 하드웨어 구성 * — 연결된 하드웨어에서 시스템 설정을 구성하는 작업.
- * 설치 * — 어플라이언스 설치 시작 및 설치 상태 모니터링을 위한 작업.
- * 네트워킹 * — StorageGRID 어플라이언스 및 어플라이언스 포트 설정에 대한 그리드, 관리자 및 클라이언트 네트워크 구성과 관련된 작업.
- * setup * — 시스템에 대한 정보를 얻고 기본 관리 노드 IP를 업데이트하는 요청을 포함하여 초기 어플라이언스 설치 설정에 도움이 되는 작업.
- * 지원 * — 컨트롤러 재부팅 및 로그 가져오기에 대한 운영
- * 업그레이드 * — 어플라이언스 펌웨어 업그레이드와 관련된 작업.
- * 업로그램 * — StorageGRID 설치 파일을 업로드하는 작업.

하드웨어 설치 문제 해결**(SG5700)**

설치 중에 문제가 발생하는 경우 하드웨어 설정 및 연결 문제와 관련된 문제 해결 정보를 검토하는 것이 도움이 될 수 있습니다.

하드웨어 설정이 중단**(SG5700)**되는 것 같습니다**.**

하드웨어 장애 또는 케이블 연결 오류로 인해 E700SG 컨트롤러가 부팅 프로세스를 완료하지 못하는 경우 StorageGRID 어플라이언스 설치 프로그램을 사용할 수 없습니다.

단계

1. 7세그먼트 디스플레이에서 코드를 확인합니다.

   전원을 켜는 동안 하드웨어가 초기화되는 동안 2개의 7세그먼트 디스플레이에는 일련의 코드가 표시됩니다.

하드웨어가 성공적으로 부팅되면 7개의 세그먼트에서 각 컨트롤러에 대해 서로 다른 코드를 표시합니다.

2. E700SG 컨트롤러에 대한 7세그먼트 디스플레이의 코드를 검토합니다.

> 설치 및 프로비저닝에 시간이 걸립니다. 일부 설치 단계에서는 몇 분 동안 StorageGRID 어플라이언스 설치 프로그램에 업데이트를 보고하지 않습니다.

오류가 발생하면 7개 세그먼트 디스플레이에서 그와 같은 시퀀스가 깜박입니다.

3. 이러한 코드의 의미를 이해하려면 다음 리소스를 참조하십시오.

컨트롤러	참조하십시오
E5500SG 컨트롤러	• "E5700SG 컨트롤러의 상태 표시기" • ""SANtricity OS 소프트웨어와 동기화 중 오류 발생""
E2800 컨트롤러	_E5700 및 E2800 시스템 모니터링 가이드 _ • 참고: * E-Series E5700 컨트롤러에 관해 설명된 코드는 어플라이언스의 E5500SG 컨트롤러에 적용되지 않습니다.

4. 그래도 문제가 해결되지 않으면 기술 지원 부서에 문의하십시오.

관련 정보

E5500SG 컨트롤러의 상태 표시등

SANtricity OS 소프트웨어와 동기화하는 동안 오류가 발생했습니다

"NetApp E-Series 시스템 문서 사이트"

SANtricity OS 소프트웨어와 동기화하는 동안 오류가 발생했습니다

StorageGRID 어플라이언스 설치 프로그램이 SANtricity OS 소프트웨어와 동기화할 수 없는 경우 컴퓨팅 컨트롤러의 7세그먼트 디스플레이에 해당 오류 코드가 표시됩니다.

이 작업에 대해

오류 코드가 표시되는 경우 이 수정 조치를 수행하십시오.

단계

1. 두 컨트롤러 사이에 있는 두 개의 상호 연결 케이블을 확인하고 케이블과 SFP+ 트랜시버가 단단히 연결되어 있는지 확인합니다.
2. 필요에 따라 케이블 또는 SFP+ 트랜시버 중 하나 또는 둘 다를 교체하고 다시 시도하십시오.
3. 그래도 문제가 해결되지 않으면 기술 지원 부서에 문의하십시오.

연결 문제 해결**(SG5700)**

StorageGRID 어플라이언스 설치 중에 연결 문제가 발생하면 나열된 수정 조치 단계를 수행해야 합니다.

제품에 연결할 수 없습니다

어플라이언스에 연결할 수 없는 경우 네트워크 문제가 있거나 하드웨어 설치가 성공적으로 완료되지 않았을 수 있습니다.

단계

1. SANtricity 시스템 관리자에 연결할 수 없는 경우:
   a. SANtricity 시스템 관리자의 관리 네트워크에 있는 E2800 컨트롤러의 IP 주소를 사용하여 어플라이언스에 ping을 시도합니다(+'* ping_E2800_Controller_IP_ * ')
   b. Ping에서 응답이 없는 경우 올바른 IP 주소를 사용하고 있는지 확인합니다.

      E2800 컨트롤러의 관리 포트 1의 IP 주소를 사용합니다.

   c. IP 주소가 올바른 경우 어플라이언스 케이블 연결 및 네트워크 설정을 확인하십시오.

      그래도 문제가 해결되지 않으면 기술 지원 부서에 문의하십시오.

   d. Ping에 성공하면 웹 브라우저를 엽니다.
   e. SANtricity 시스템 관리자의 URL을 입력합니다: + `https://*E2800_Controller_IP*`

      SANtricity 시스템 관리자의 로그인 페이지가 나타납니다.

2. E5500SG 컨트롤러에 연결할 수 없는 경우:
   a. E5500SG 컨트롤러의 IP 주소를 사용하여 어플라이언스에 ping을 시도합니다. + " * PING_E700SG_Controller_IP_ * "
   b. Ping에서 응답이 없는 경우 올바른 IP 주소를 사용하고 있는지 확인합니다.

      그리드 네트워크, 관리 네트워크 또는 클라이언트 네트워크에서 어플라이언스의 IP 주소를 사용할 수 있습니다.

   c. IP 주소가 올바른 경우 어플라이언스 케이블 연결, SFP 트랜시버 및 네트워크 설정을 확인하십시오.

      그래도 문제가 해결되지 않으면 기술 지원 부서에 문의하십시오.

   d. Ping에 성공하면 웹 브라우저를 엽니다.
   e. StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. + `https://*E5700SG_Controller_IP*:8443`

      홈 페이지가 나타납니다.

StorageGRID 어플라이언스 설치 프로그램이 실행되는 동안 컨트롤러를 재부팅합니다

StorageGRID 어플라이언스 설치 프로그램이 실행되는 동안 컴퓨팅 컨트롤러를 재부팅해야 할 수도 있습니다. 예를 들어, 설치에 실패한 경우 컨트롤러를 재부팅해야 할 수 있습니다.

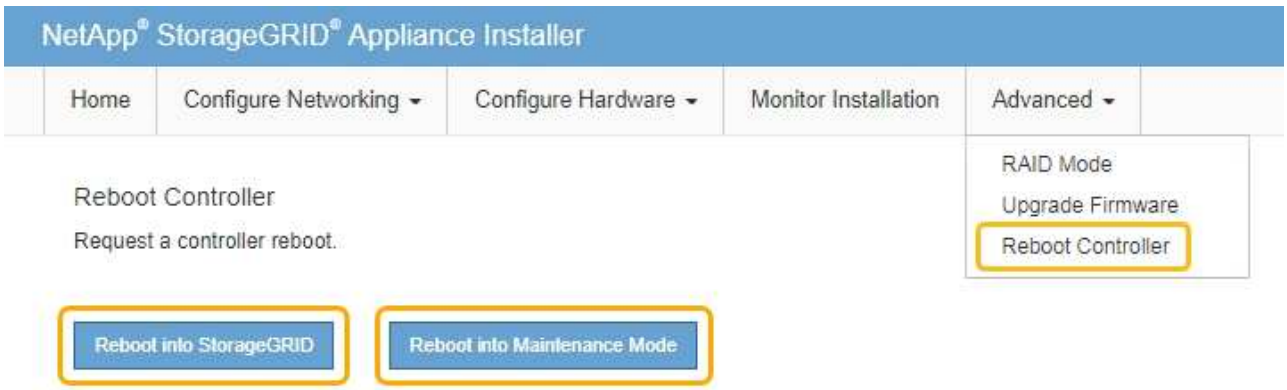
이 작업에 대해

이 절차는 컴퓨팅 컨트롤러가 StorageGRID 어플라이언스 설치 프로그램을 실행하는 경우에만 적용됩니다. 설치가 완료되면 StorageGRID 어플라이언스 설치 프로그램을 더 이상 사용할 수 없기 때문에 이 단계가 더 이상 작동하지 않습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 클릭한 후 다음 옵션 중 하나를 선택합니다.

   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



   컨트롤러가 재부팅됩니다.

SG5700 어플라이언스 유지

E2800 컨트롤러에서 SANtricity OS 소프트웨어를 업그레이드하거나, E5500SG 컨트롤러의 이더넷 링크 구성을 변경하거나, E2800 컨트롤러 또는 E5500SG 컨트롤러를 교체하거나, 특정 구성 요소를 교체해야 할 수 있습니다. 이 섹션의 절차에서는 어플라이언스가 이미 StorageGRID 시스템의 스토리지 노드로 구축되었다고 가정합니다.

제품을 유지보수 모드로 전환합니다

특정 유지보수 절차를 수행하기 전에 제품을 유지보수 모드로 전환해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

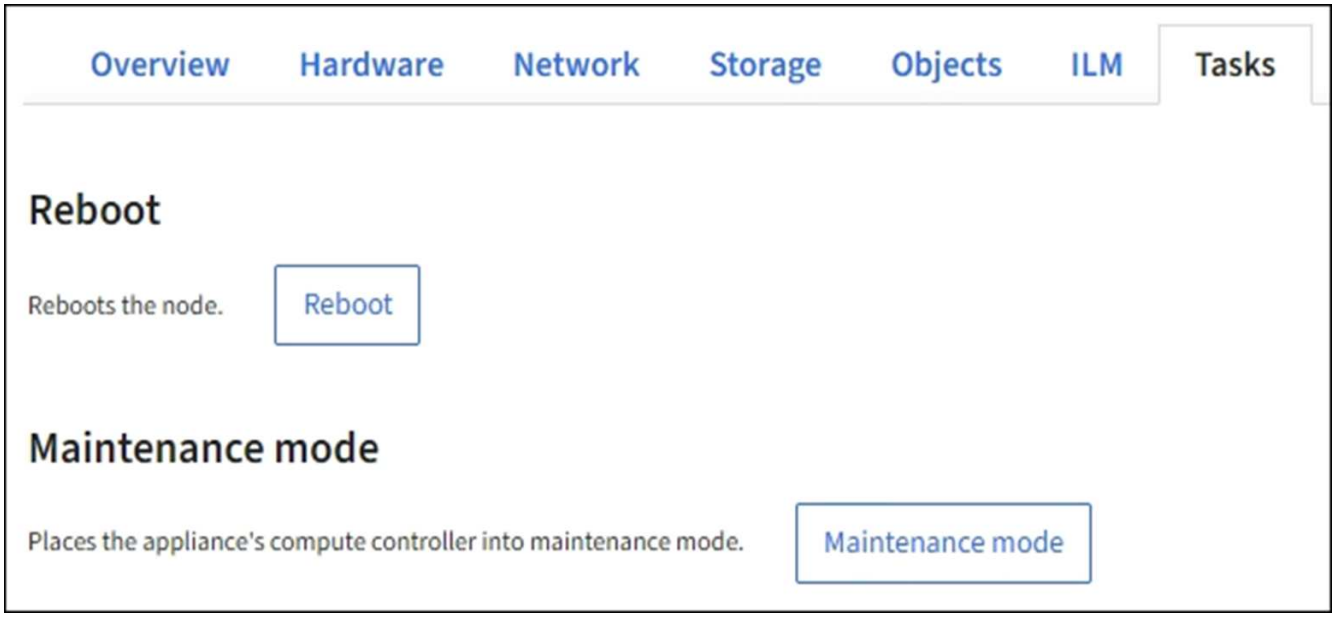
이 작업에 대해

StorageGRID 어플라이언스를 유지보수 모드로 전환하면 원격 액세스가 불가능한 경우가 드물게 있습니다.

유지보수 모드에서 StorageGRID 어플라이언스에 대한 admin 계정 암호 및 SSH 호스트 키는 어플라이언스가 서비스 중일 때와 동일하게 유지됩니다.

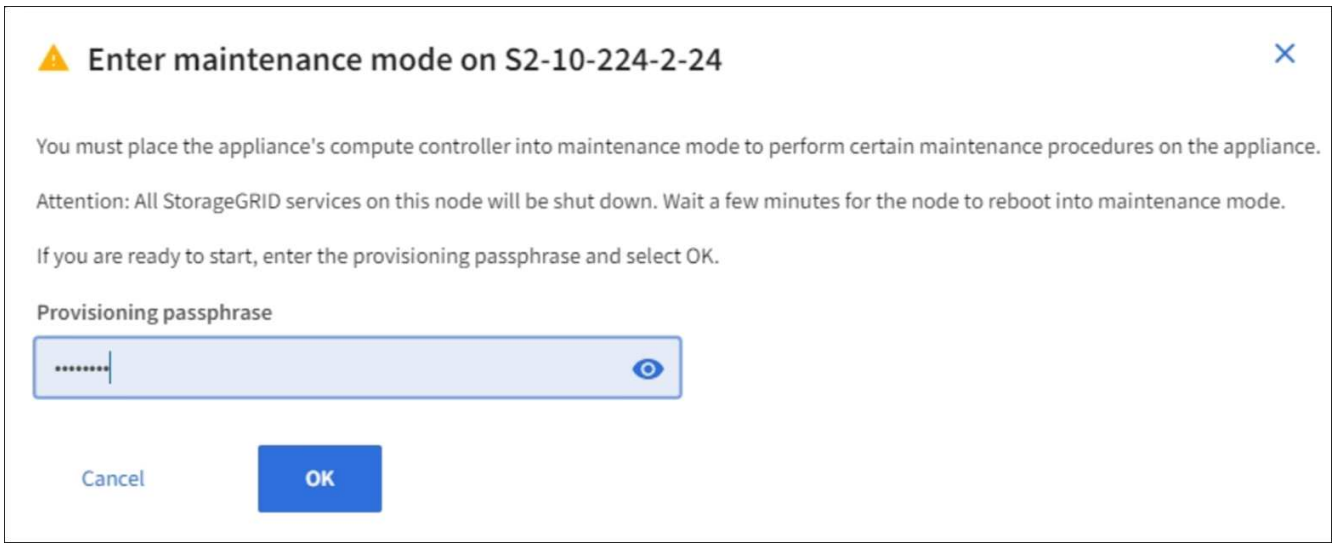
단계

1. Grid Manager에서 * nodes * 를 선택합니다.
2. 노드 페이지의 트리 뷰에서 어플라이언스 스토리지 노드를 선택합니다.
3. 작업 * 을 선택합니다.



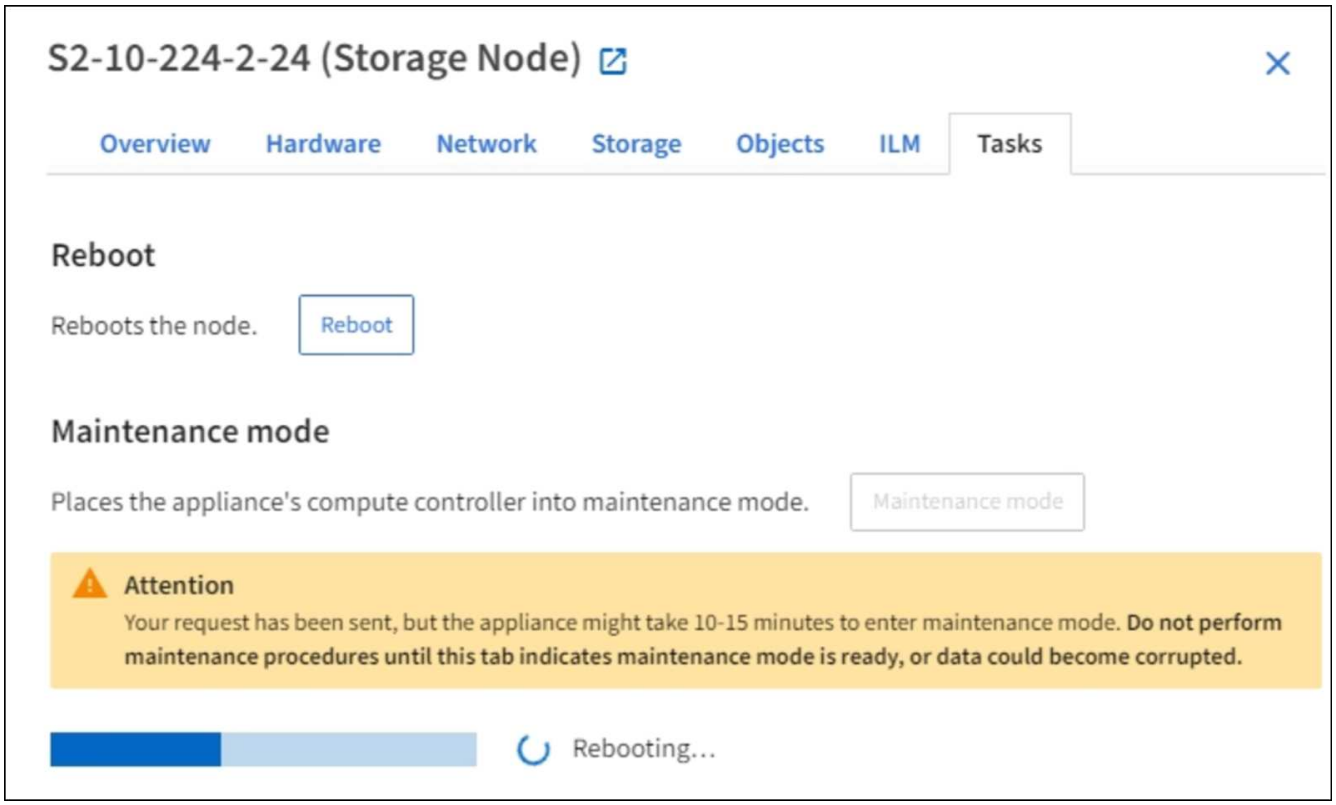
4. 유지보수 모드 * 를 선택합니다.

   확인 대화 상자가 나타납니다.

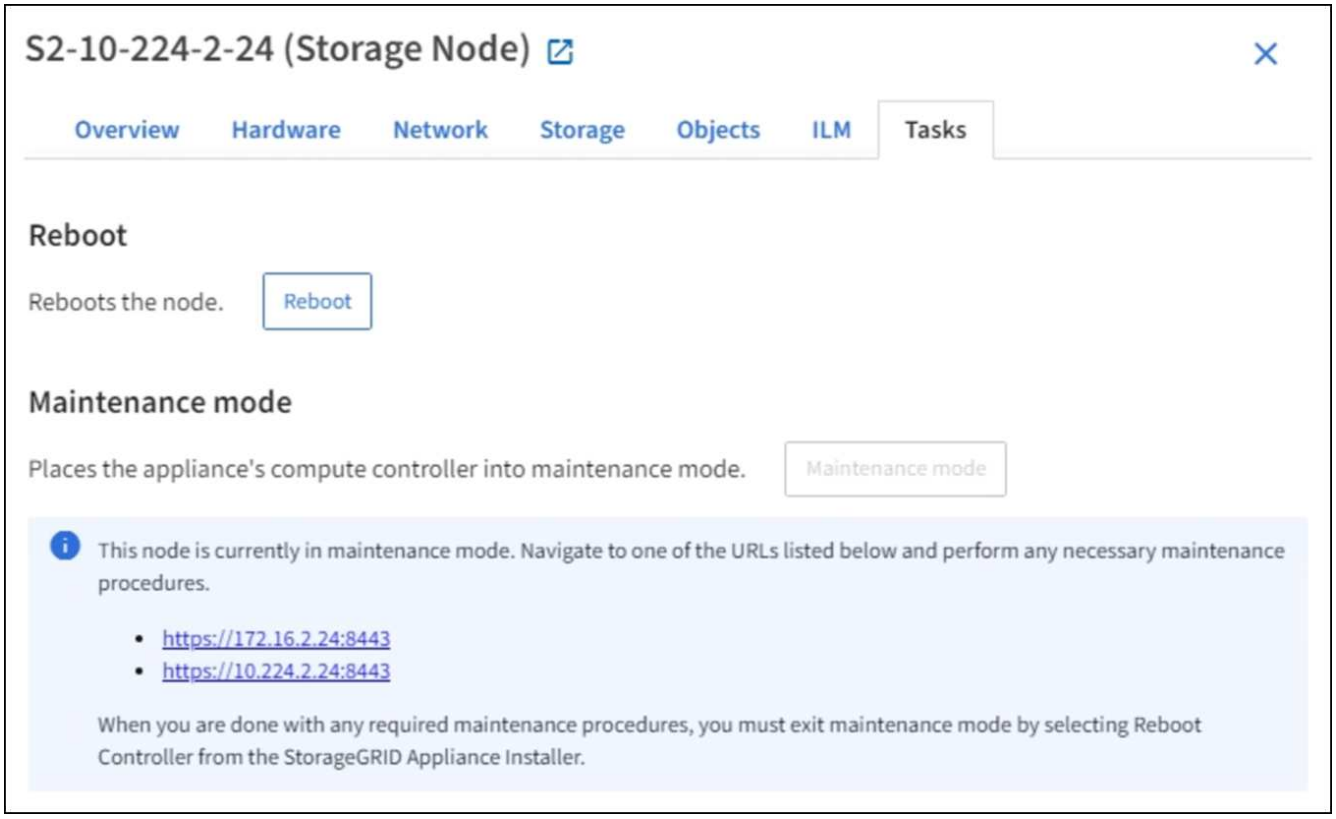


5. 프로비저닝 암호를 입력하고 * OK * 를 선택합니다.

   진행 표시줄과 "전송 요청", "StorageGRID 중지", "재부팅 중"과 같은 일련의 메시지는 어플라이언스가 유지보수 모드로 들어가기 위한 단계를 완료하고 있음을 나타냅니다.



어플라이언스가 유지보수 모드일 때 확인 메시지에 StorageGRID 어플라이언스 설치 프로그램에 액세스하는 데 사용할 수 있는 URL이 나열됩니다.



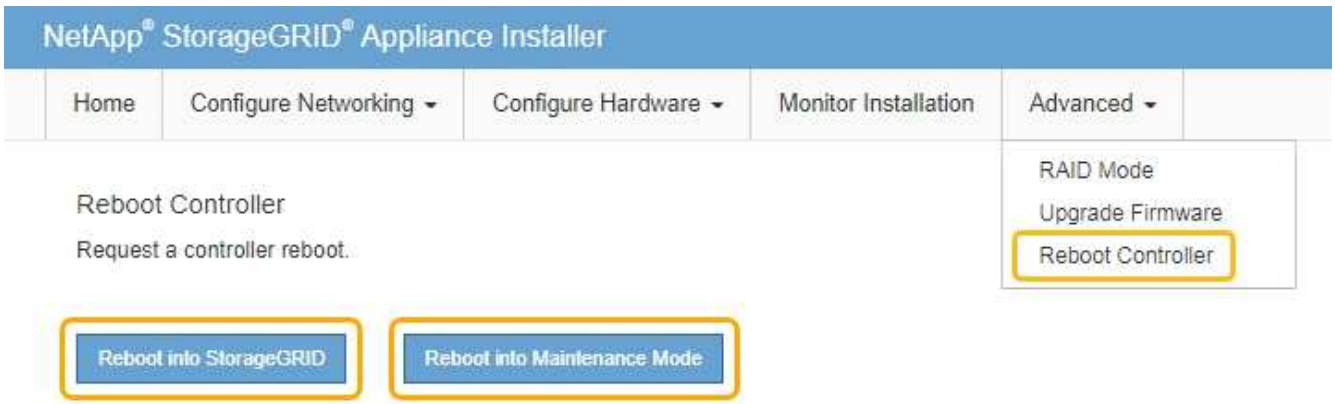
6. StorageGRID 어플라이언스 설치 프로그램에 액세스하려면 표시된 URL 중 하나를 찾습니다.

   가능한 경우 어플라이언스의 관리 네트워크 포트의 IP 주소가 포함된 URL을 사용하십시오.

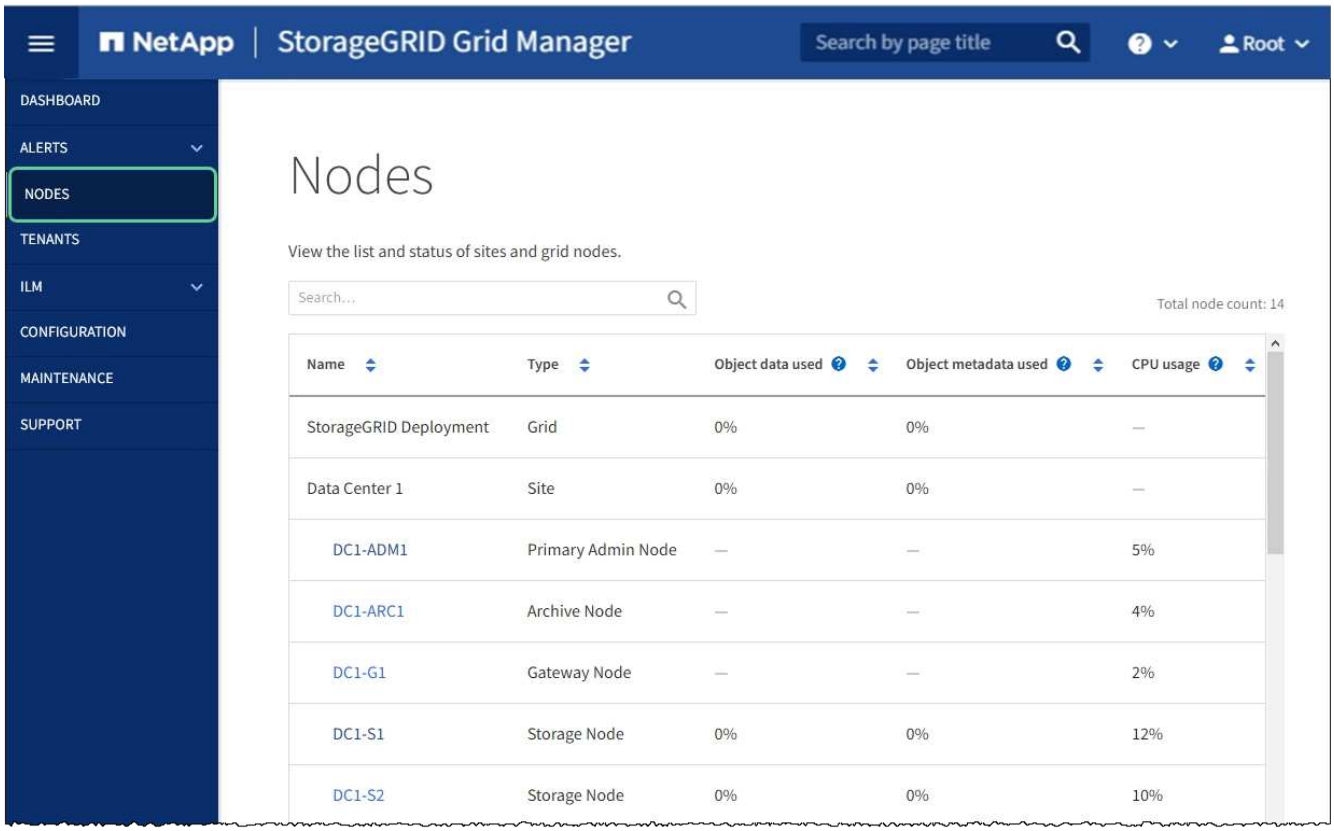
> 어플라이언스의 관리 포트에 직접 연결되어 있는 경우, 'https://169.254.0.1:8443` 을 사용하여 StorageGRID 어플라이언스 설치 프로그램 페이지에 액세스하십시오.

7. StorageGRID 어플라이언스 설치 프로그램에서 어플라이언스가 유지보수 모드인지 확인합니다.

8. 필요한 유지보수 작업을 수행합니다.
9. 유지보수 작업을 완료한 후 유지보수 모드를 종료하고 정상 노드 운영을 재개합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * StorageGRID * 으로 재부팅 * 을 선택합니다.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



스토리지 컨트롤러에서 **SANtricity OS**를 업그레이드합니다

스토리지 컨트롤러가 최적의 상태로 작동하도록 하려면 StorageGRID 어플라이언스에 적합한 SANtricity OS의 최신 유지 관리 릴리즈로 업그레이드해야 합니다. NetApp 상호 운용성 매트릭스 툴(IMT) 을 참조하여 사용해야 하는 버전을 확인하십시오. 도움이 필요한 경우 기술 지원 팀에 문의하십시오.

- 스토리지 컨트롤러가 SANtricity OS 08.42.20.00(11.42) 이상을 사용하는 경우 그리드 관리자를 사용하여 업그레이드를 수행합니다.

  그리드 관리자를 사용하여 스토리지 컨트롤러의 SANtricity OS를 업그레이드합니다

- 스토리지 컨트롤러가 08.42.20.00(11.42) 이전의 SANtricity OS 버전을 사용하는 경우 유지보수 모드를 사용하여 업그레이드를 수행합니다.

  유지보수 모드를 사용하여 E2800 컨트롤러에서 SANtricity OS를 업그레이드합니다

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

"NetApp 다운로드: StorageGRID 어플라이언스"

모니터링하고 문제를 해결합니다

현재 SANtricity OS 08.42.20.00(11.42) 이상을 사용하는 스토리지 컨트롤러의 경우 그리드 관리자를 사용하여 업그레이드를 적용해야 합니다.

필요한 것

- 업그레이드에 사용 중인 SANtricity OS 버전이 어플라이언스와 호환되는지 확인하려면 NetApp 상호 운용성 매트릭스 툴(IMT)을 참조하십시오.
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 프로비저닝 암호가 있습니다.
- SANtricity OS의 NetApp 다운로드 페이지에 액세스할 수 있습니다.

이 작업에 대해

SANtricity OS 업그레이드 프로세스를 완료할 때까지 다른 소프트웨어 업데이트(StorageGRID 소프트웨어 업그레이드 또는 핫픽스)를 수행할 수 없습니다. SANtricity OS 업그레이드 프로세스가 완료되기 전에 핫픽스 또는 StorageGRID 소프트웨어 업그레이드를 시작하려고 하면 SANtricity OS 업그레이드 페이지로 리디렉션됩니다.

SANtricity OS 업그레이드가 업그레이드를 위해 선택된 모든 적용 가능한 노드에 적용되기 전에는 절차가 완료되지 않습니다. 각 노드에서 SANtricity OS를 로드하는 데 30분 이상, 각 StorageGRID 스토리지 어플라이언스를 재부팅하는 데 최대 90분이 걸릴 수 있습니다.

> 다음 단계는 그리드 관리자를 사용하여 업그레이드를 수행하는 경우에만 적용됩니다. 컨트롤러가 08.42.20.00(11.42) 이전의 SANtricity OS를 사용하는 경우 그리드 관리자를 사용하여 어플라이언스의 스토리지 컨트롤러를 업그레이드할 수 없습니다.

> 이 절차에서는 NVSRAM을 SANtricity OS 업그레이드와 관련된 최신 버전으로 자동 업그레이드합니다. 별도의 NVSRAM 업그레이드 파일을 적용할 필요가 없습니다.

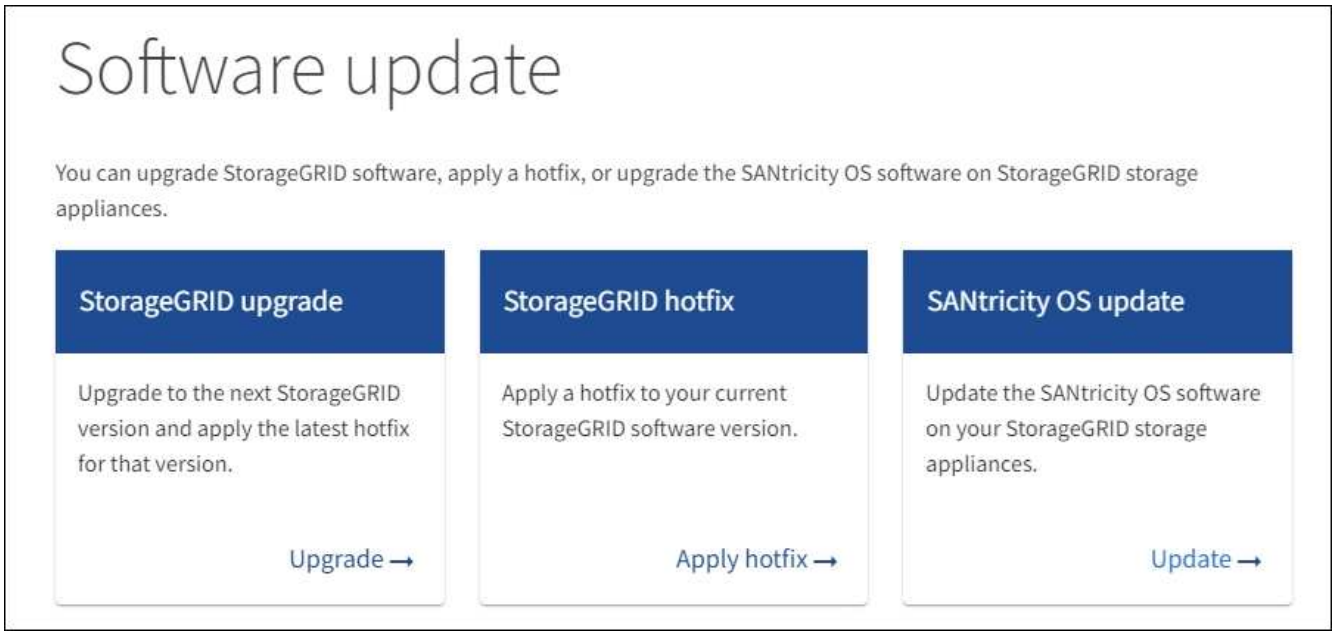
단계

1. NetApp Support 사이트에서 새로운 SANtricity OS 소프트웨어 파일을 다운로드합니다.

   스토리지 컨트롤러의 SANtricity OS 버전을 선택해야 합니다.

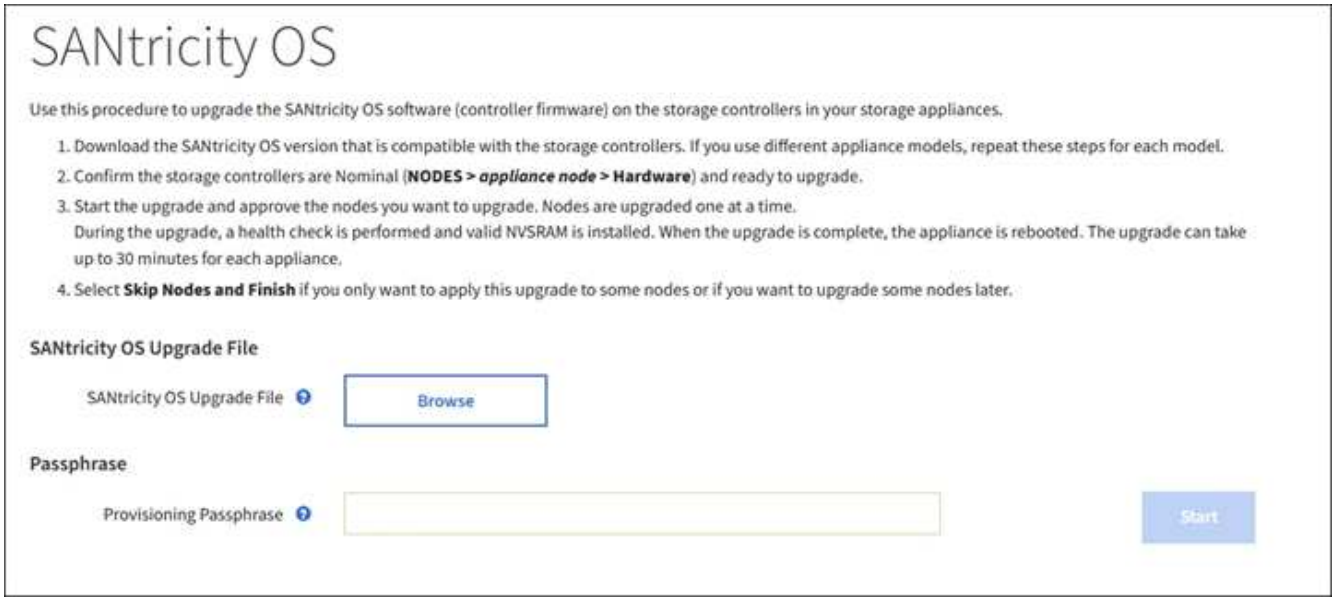
   "NetApp 다운로드: StorageGRID 어플라이언스"

2. 유지보수 * > * 시스템 * > * 소프트웨어 업데이트 * 를 선택합니다.



3. SANtricity OS 업데이트 섹션에서 * 업데이트 * 를 선택합니다.

   SANtricity OS 업그레이드 페이지가 나타납니다.



4. NetApp Support 사이트에서 다운로드한 SANtricity OS 업그레이드 파일을 선택합니다.

   a. 찾아보기 * 를 선택합니다.

   b. 파일을 찾아 선택합니다.

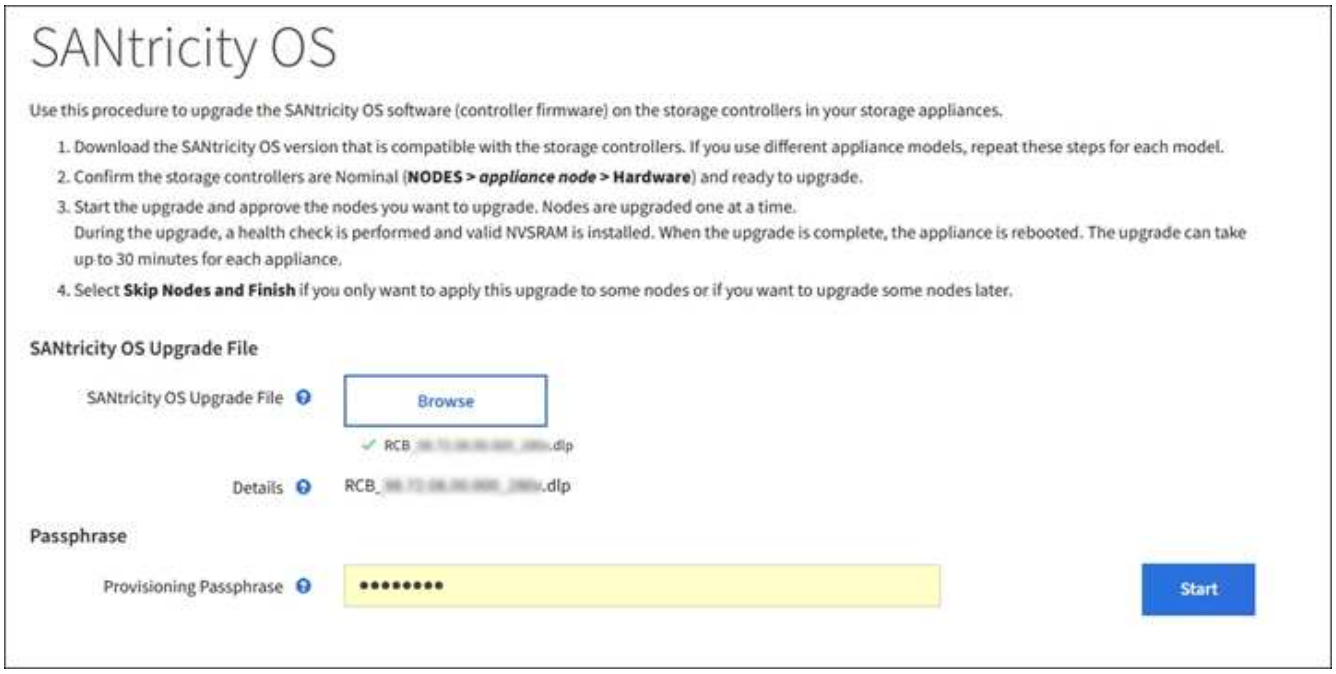
   c. 열기 * 를 선택합니다.

      파일이 업로드되고 검증됩니다. 유효성 검사 프로세스가 완료되면 * 찾아보기 * 버튼 옆에 파일 이름이 표시됩니다.

      ⓘ 파일 이름은 확인 프로세스의 일부이므로 변경하지 마십시오.

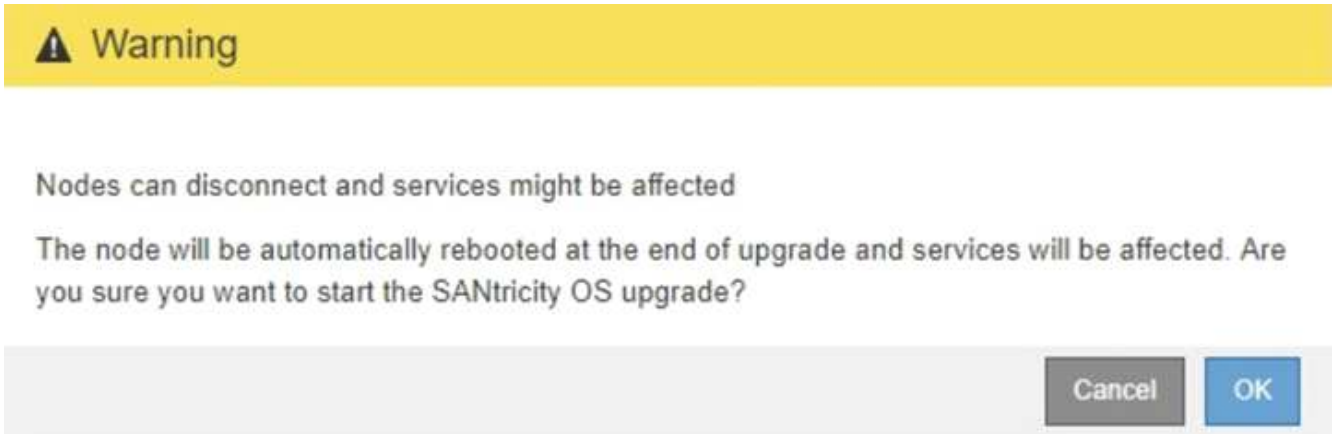
5. 프로비저닝 암호를 입력합니다.

   시작 * 버튼이 활성화됩니다.



6. 시작 * 을 선택합니다.

   업그레이드된 노드의 서비스가 다시 시작됨에 따라 브라우저의 연결이 일시적으로 끊길 수 있다는 경고 상자가 나타납니다.



7. SANtricity OS 업그레이드 파일을 기본 관리 노드로 스테이징하려면 * OK * 를 선택하십시오.

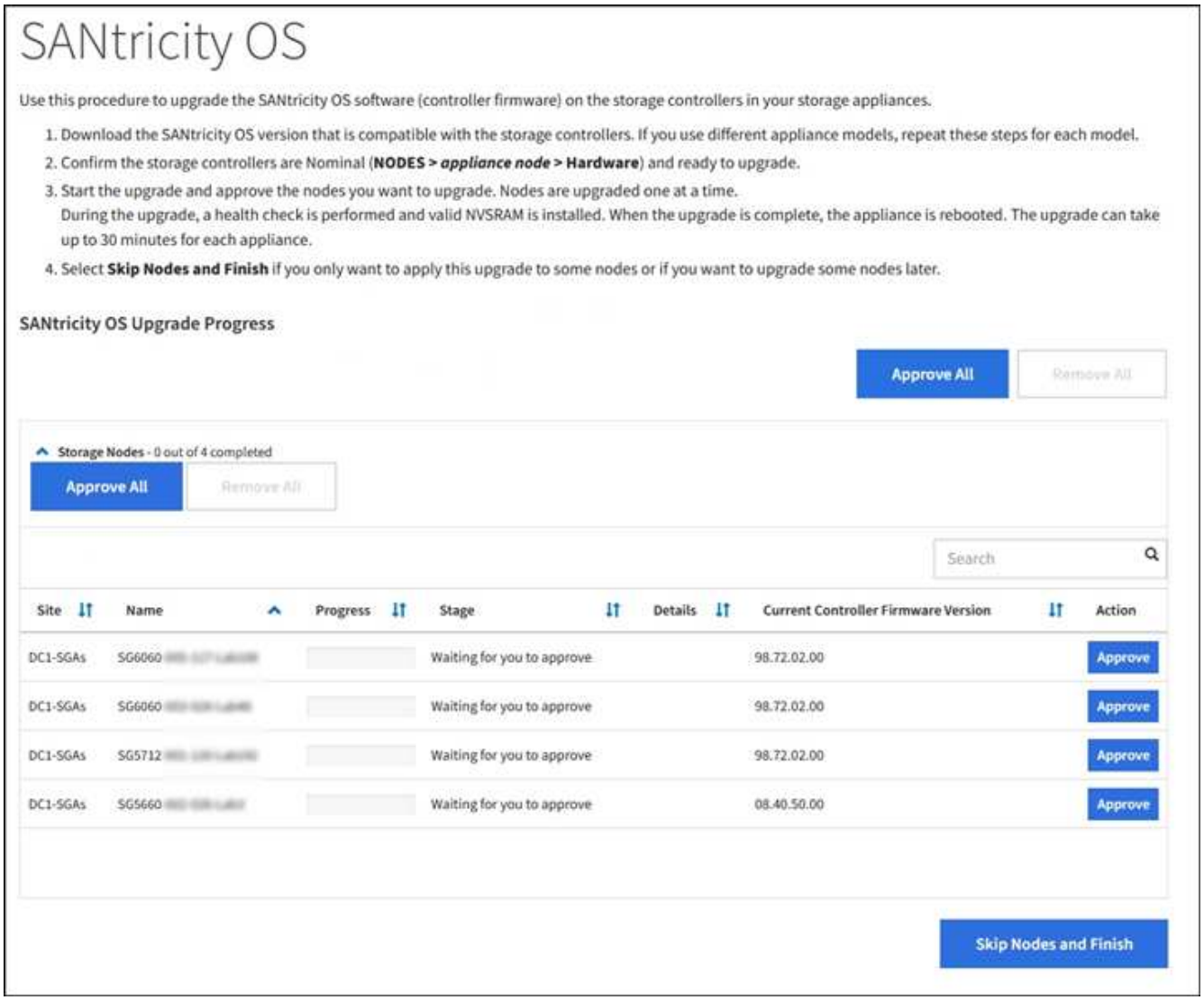
   SANtricity OS 업그레이드가 시작될 때:

   a. 상태 점검이 실행됩니다. 이 프로세스에서는 노드 상태가 주의 필요 인지 확인합니다.

      ⓘ 오류가 보고되면 이를 해결하고 * 시작 * 을 다시 선택합니다.

   b. SANtricity OS 업그레이드 진행률 테이블이 나타납니다. 이 표에는 그리드의 모든 스토리지 노드 및 각 노드의 현재 업그레이드 단계가 나와 있습니다.

이 표에는 모든 어플라이언스 스토리지 노드가 표시됩니다. 소프트웨어 기반 스토리지 노드가 표시되지 않습니다. 업그레이드가 필요한 모든 노드에 대해 * Approve * 를 선택합니다.



8. 선택적으로 * Site *, * Name *, * Progress *, * Stage *, * Details *, * Site *, * Site *, *, * Details *, 또는 * 현재 컨트롤러 펌웨어 버전 *. 또는 * 검색 * 상자에 용어를 입력하여 특정 노드를 검색합니다.

   섹션의 오른쪽 아래 모서리에 있는 왼쪽 및 오른쪽 화살표를 사용하여 노드 목록을 스크롤할 수 있습니다.

9. 업그레이드 대기열에 추가할 준비가 된 그리드 노드를 승인합니다. 동일한 유형의 승인된 노드는 한 번에 하나씩 업그레이드됩니다.

   노드를 중지하고 재부팅할 준비가 되어 있는지 확실하지 않은 경우 어플라이언스 스토리지 노드에 대한 SANtricity OS 업그레이드를 승인하지 마십시오. 노드에서 SANtricity OS 업그레이드가 승인되면 해당 노드의 서비스가 중지되고 업그레이드 프로세스가 시작됩니다. 나중에 노드 업그레이드가 완료되면 어플라이언스 노드가 재부팅됩니다. 이러한 작업은 노드와 통신하는 클라이언트에 대해 서비스 중단을 일으킬 수 있습니다.

   - 모든 스토리지 노드를 SANtricity OS 업그레이드 대기열에 추가하려면 * 모두 승인 * 버튼 중 하나를 선택합니다.

> 노드 업그레이드 순서가 중요한 경우 노드 또는 노드 그룹을 한 번에 하나씩 승인하고 다음 노드를 승인하기 전에 각 노드에서 업그레이드가 완료될 때까지 기다립니다.

- 하나 이상의 * Approve * (승인 *) 버튼을 선택하여 하나 이상의 노드를 SANtricity OS 업그레이드 대기열에 추가합니다.

  Approve * 를 선택하면 업그레이드 프로세스에서 노드를 업그레이드할 수 있는지 여부를 결정합니다. 노드를 업그레이드할 수 있는 경우 업그레이드 대기열에 추가됩니다.

일부 노드의 경우 선택한 업그레이드 파일이 의도적으로 적용되지 않으며 이러한 특정 노드를 업그레이드하지 않고 업그레이드 프로세스를 완료할 수 있습니다. 의도적으로 업그레이드되지 않은 노드는 완료(업그레이드 시도) 단계를 표시하고 세부 정보 열에 노드가 업그레이드되지 않은 이유를 표시합니다.

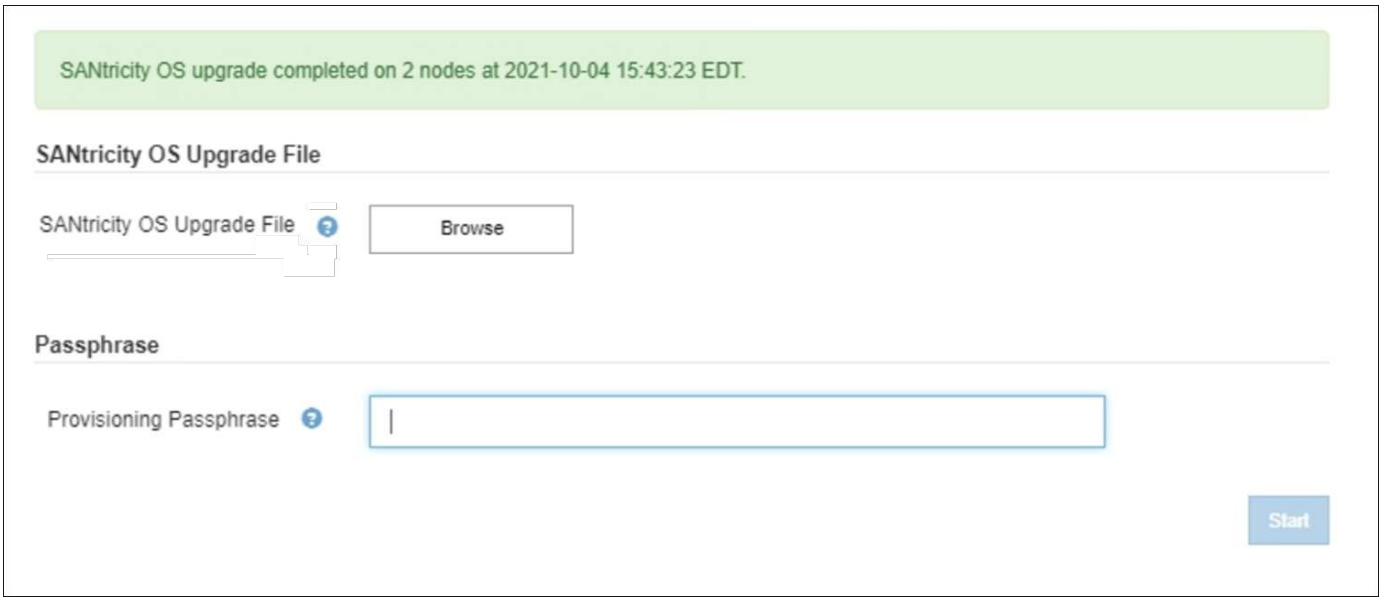
10. SANtricity OS 업그레이드 대기열에서 노드 또는 모든 노드를 제거해야 하는 경우 * 제거 * 또는 * 모두 제거 * 를 선택합니다.

    스테이지가 대기 모드 를 넘어 진행되면 * 제거 * 버튼이 숨겨지고 더 이상 SANtricity OS 업그레이드 프로세스에서 노드를 제거할 수 없습니다.

11. SANtricity OS 업그레이드가 승인된 각 그리드 노드에 적용될 때까지 기다립니다.

    - SANtricity OS 업그레이드를 적용하는 동안 노드에 오류 단계가 표시되는 경우 해당 노드에 대한 업그레이드가 실패한 것입니다. 기술 지원의 도움을 받아 어플라이언스를 유지보수 모드로 전환하여 복구해야 할 수도 있습니다.
    - 노드의 펌웨어가 너무 오래되어 그리드 관리자로 업그레이드되지 않는 경우, 노드에 오류 단계가 표시됩니다: ""이 노드에서 SANtricity OS를 업그레이드하려면 유지보수 모드를 사용해야 합니다. 제품의 설치 및 유지관리 지침을 참조하십시오. 업그레이드 후 향후 업그레이드를 위해 이 유틸리티를 사용할 수 있습니다." 오류를 해결하려면 다음을 수행합니다.
      i. 유지보수 모드를 사용하여 오류 단계가 표시된 노드에서 SANtricity OS를 업그레이드합니다.
      ii. 그리드 관리자를 사용하여 SANtricity OS 업그레이드를 다시 시작하고 완료합니다.

    승인된 모든 노드에서 SANtricity OS 업그레이드가 완료되면 SANtricity OS 업그레이드 진행률 테이블이 닫히고 SANtricity OS 업그레이드가 완료된 날짜와 시간이 녹색 배너에 표시됩니다.



1. 노드를 업그레이드할 수 없는 경우 세부 정보 열에 표시된 이유를 기록하고 적절한 조치를 취하십시오.
   - "스토리지 노드가 이미 업그레이드되었습니다." 추가 조치가 필요하지 않습니다.
   - "SANtricity OS 업그레이드는 이 노드에 적용되지 않습니다." 노드에는 StorageGRID 시스템에서 관리할 수 있는 스토리지 컨트롤러가 없습니다. 이 메시지가 표시된 노드를 업그레이드하지 않고 업그레이드 프로세스를 완료합니다.
   - "'SANtricity OS 파일이 이 노드와 호환되지 않습니다.'" 노드에는 선택한 것과 다른 SANtricity OS 파일이 필요합니다. 현재 업그레이드를 완료한 후 노드에 대한 올바른 SANtricity OS 파일을 다운로드하고 업그레이드 프로세스를 반복합니다.

> 나열된 모든 스토리지 노드에서 SANtricity OS 업그레이드를 승인할 때까지 SANtricity OS 업그레이드 프로세스가 완료되지 않습니다.

1. 노드 승인을 종료하여 SANtricity OS 페이지로 돌아가 새 SANtricity OS 파일 업로드를 허용하려면 다음을 수행합니다.
   a. 노드 건너뛰기 및 마침 * 을 선택합니다.

      모든 노드를 업그레이드하지 않고 업그레이드 프로세스를 완료할지 묻는 경고가 나타납니다.

   b. SANtricity OS * 페이지로 돌아가려면 * OK * 를 선택하십시오.
   c. 노드 승인을 계속할 준비가 되면 로 이동합니다 SANtricity OS를 다운로드합니다 를 눌러 업그레이드 프로세스를 다시 시작합니다.

      > 노드가 이미 승인되었으며 오류 없이 업그레이드되었습니다.

2. 다른 SANtricity OS 업그레이드 파일이 필요한 전체 단계가 있는 노드에 대해 이 업그레이드 절차를 반복합니다.

> Needs Attention(주의 필요) 상태인 모든 노드의 경우 유지보수 모드를 사용하여 업그레이드를 수행합니다.

> 업그레이드 절차를 반복하면 이전에 업그레이드된 노드를 승인해야 합니다.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

유지보수 모드를 사용하여 E2800 컨트롤러에서 SANtricity OS를 업그레이드합니다

유지보수 모드를 사용하여 **E2800** 컨트롤러에서 **SANtricity OS**를 업그레이드합니다

현재 08.42.20.00(11.42) 이전의 SANtricity OS를 사용하는 스토리지 컨트롤러의 경우, 업그레이드를 적용하려면 유지보수 모드 절차를 사용해야 합니다.

필요한 것

- 업그레이드에 사용 중인 SANtricity OS 버전이 어플라이언스와 호환되는지 확인하려면 NetApp 상호 운용성 매트릭스 툴(IMT)을 참조하십시오.
- E5500SG 컨트롤러를 에 장착해야 합니다 유지보수 모드E2800 컨트롤러와의 연결을 중단합니다.

> StorageGRID 어플라이언스를 유지보수 모드로 전환하면 원격 액세스가 불가능한 경우가 드물게 있습니다.

이 작업에 대해

한 번에 두 개 이상의 StorageGRID 어플라이언스에 있는 E-Series 컨트롤러의 SANtricity OS 또는 NVSRAM을 업그레이드하지 마십시오.

> 배포 모델 및 ILM 정책에 따라 한 번에 둘 이상의 StorageGRID 어플라이언스를 업그레이드할 경우 데이터를 사용할 수 없게 될 수 있습니다.

단계

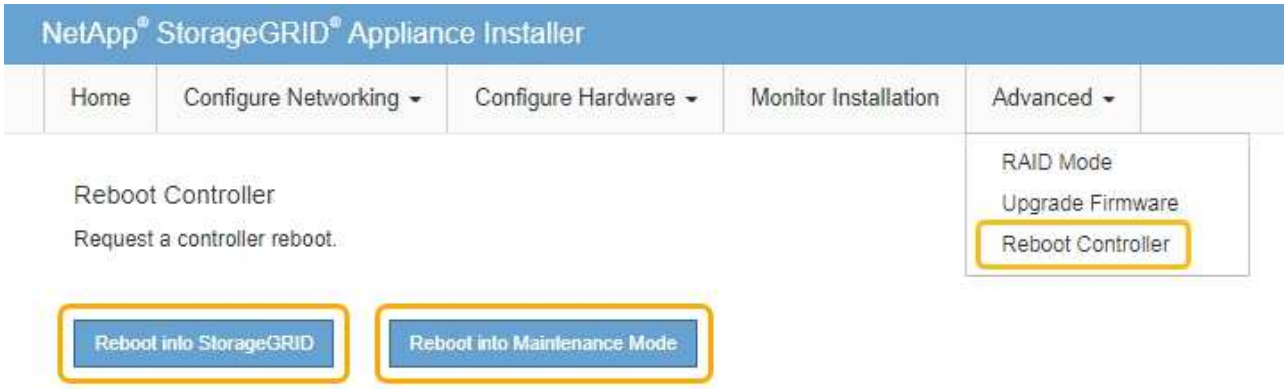
1. 제품이 에 있는지 확인하십시오 유지보수 모드.
2. 서비스 랩톱에서 SANtricity System Manager에 액세스하고 로그인합니다.
3. 관리 클라이언트에 새 SANtricity OS 소프트웨어 파일 및 NVSRAM 파일을 다운로드합니다.

   > NVSRAM은 StorageGRID 어플라이언스에만 적용됩니다. 표준 NVSRAM 다운로드를 사용하지 마십시오.

4. E2800 및 E5700 SANtricity 소프트웨어 및 펌웨어 업그레이드 가이드 _ 또는 SANtricity 시스템 관리자 온라인 도움말의 지침에 따라 E2800 컨트롤러의 펌웨어 및 NVSRAM을 업그레이드합니다.

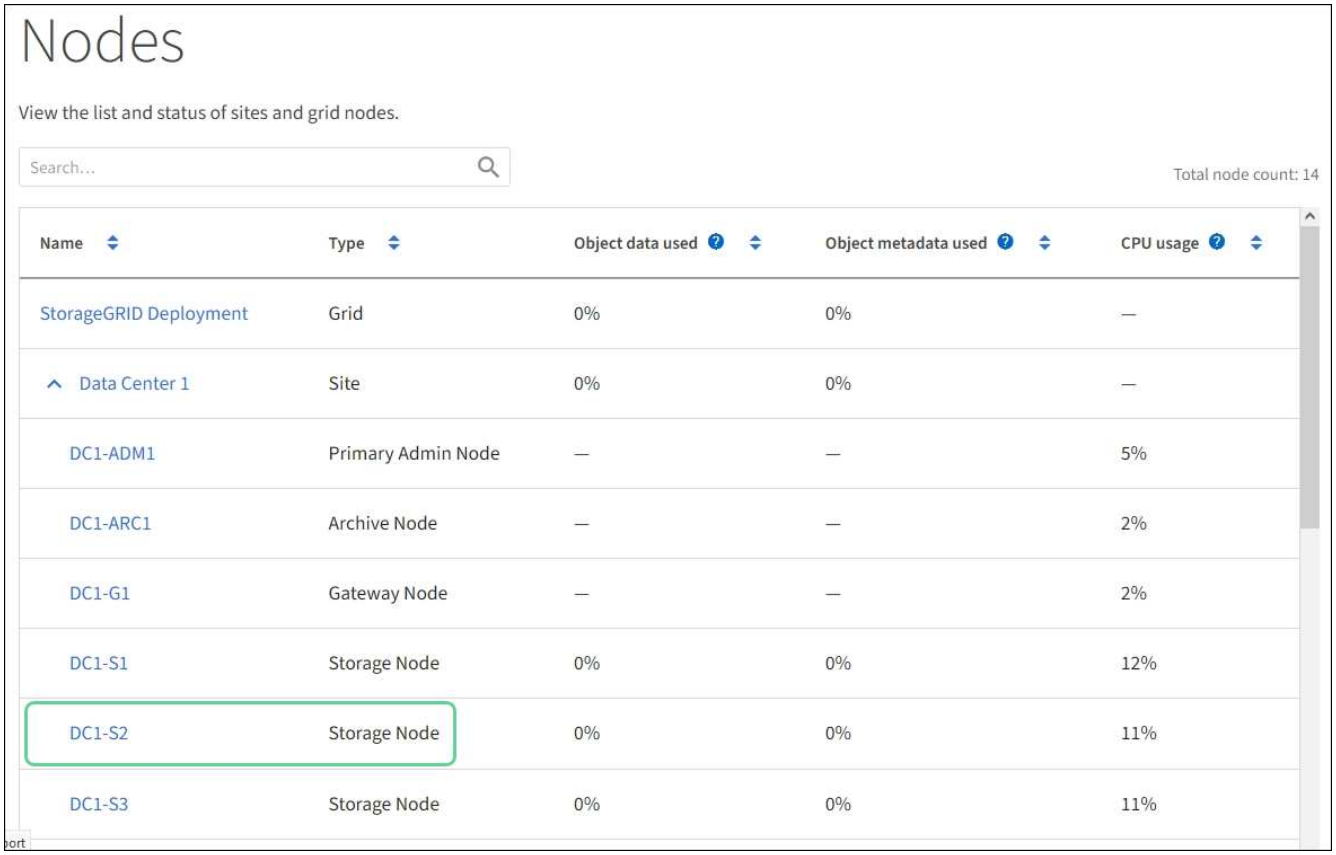
   > 업그레이드 파일을 즉시 활성화합니다. 활성화를 지연하지 마십시오.

5. 이 절차가 성공적으로 완료되었고 노드가 유지보수 모드일 때 수행할 추가 절차가 있는 경우 지금 수행합니다. 작업을 완료했거나 오류가 발생하여 다시 시작하려면 * 고급 * > * 컨트롤러 재부팅 * 을 선택하고 다음 옵션 중 하나를 선택합니다.
   - StorageGRID * 로 재부팅 * 을 선택합니다
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. 절차 중에 오류가 발생하여 다시 시작하려면 이 옵션을 선택합니다. 노드가 유지보수 모드로 재부팅된 후 장애가 발생한 절차의 적절한 단계에서 다시 시작하십시오.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고

노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. 노드 페이지에는 어플라이언스 노드에 대한 정상 상태(노드 이름 왼쪽에 아이콘이 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

그리드 관리자를 사용하여 스토리지 컨트롤러의 SANtricity OS를 업그레이드합니다

SANtricity 시스템 관리자를 사용하여 드라이브 펌웨어를 업그레이드합니다

드라이브 펌웨어를 업그레이드하여 최신 기능 및 버그 수정 사항이 모두 있는지 확인합니다.

필요한 것

- 스토리지 어플라이언스 상태가 최적입니다.
- 모든 드라이브가 최적 상태입니다.
- 사용 중인 StorageGRID 버전과 호환되는 최신 버전의 SANtricity 시스템 관리자가 설치되어 있습니다.
- 있습니다 StorageGRID 어플라이언스를 유지보수 모드로 놓았습니다.

> 유지보수 모드는 스토리지 컨트롤러에 대한 연결을 중단하여 모든 I/O 작업을 중지하고 모든 드라이브를 오프라인으로 전환합니다.

> 한 번에 둘 이상의 StorageGRID 어플라이언스에서 드라이브 펌웨어를 업그레이드하지 마십시오. 따라서 배포 모델 및 ILM 정책에 따라 데이터를 사용할 수 없게 될 수 있습니다.

단계

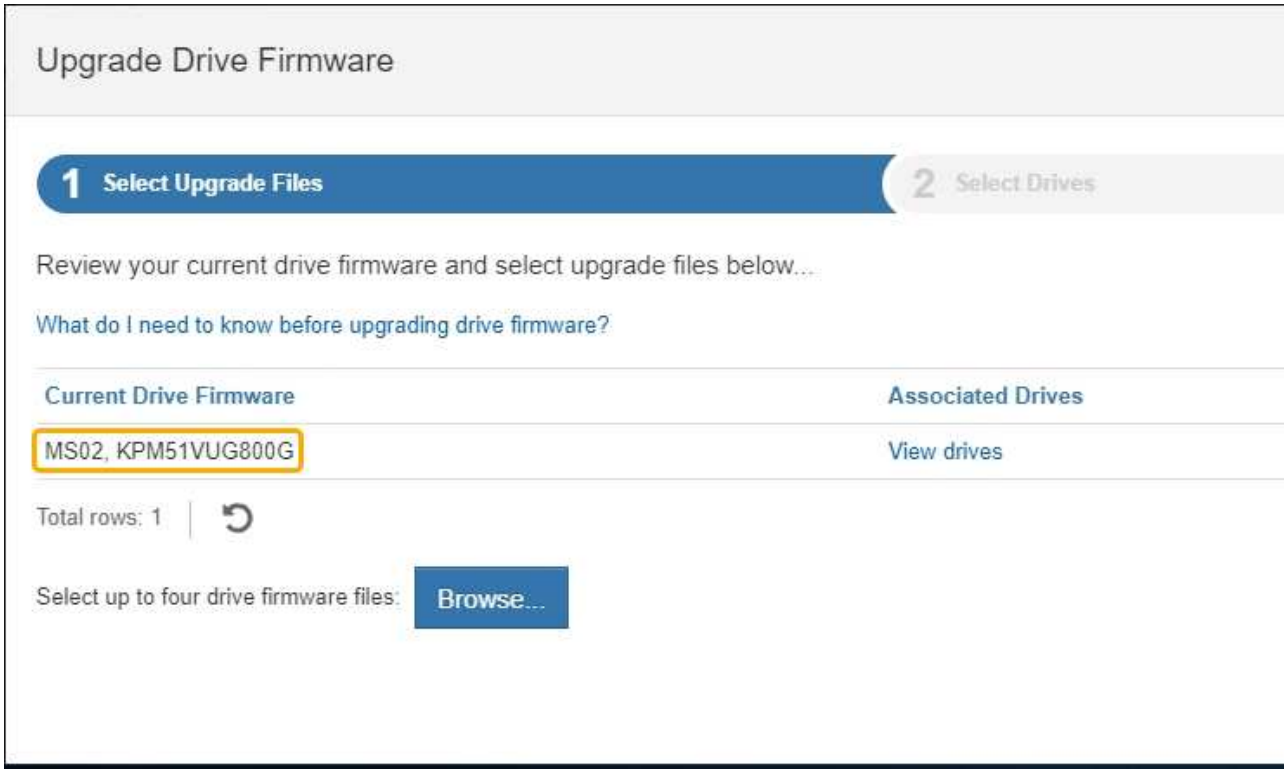
1. 제품이 에 있는지 확인하십시오 유지보수 모드.
2. 다음 방법 중 하나를 사용하여 SANtricity System Manager에 액세스합니다.
   - StorageGRID 어플라이언스 설치 프로그램을 사용하여 * 고급 * > * SANtricity 시스템 관리자 * 를 선택합니다
   - 스토리지 컨트롤러 IP:+(* https://*Storage_Controller_IP**`) 로 이동하여 SANtricity 시스템 관리자를 사용합니다
3. 필요한 경우 SANtricity 시스템 관리자 사용자 이름과 암호를 입력합니다.
4. 스토리지 어플라이언스에 현재 설치된 드라이브 펌웨어 버전을 확인합니다.

   a. SANtricity 시스템 관리자에서 * 지원 * > * 업그레이드 센터 * 를 선택합니다.

   b. 드라이브 펌웨어 업그레이드 에서 * 업그레이드 시작 * 을 선택합니다.

      드라이브 펌웨어 업그레이드에는 현재 설치된 드라이브 펌웨어 파일이 표시됩니다.

   c. Current Drive Firmware(현재 드라이브 펌웨어) 열에서 현재 드라이브 펌웨어 개정 및 드라이브 식별자를 확인합니다.



      이 예에서

      - 드라이브 펌웨어 버전은 * MS02 * 입니다.
      - 드라이브 식별자는 * KPM51VUG800G * 입니다.

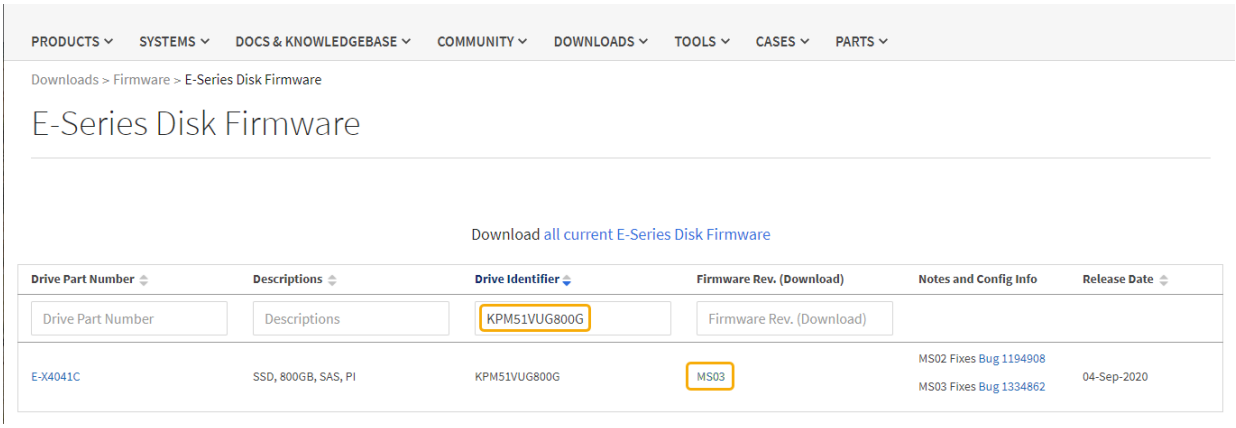
   연결된 드라이브 열에서 * 드라이브 보기 * 를 선택하여 스토리지 어플라이언스에서 해당 드라이브가 설치된 위치를 표시합니다.

   a. Upgrade Drive Firmware(드라이브 펌웨어 업그레이드) 창을 닫습니다.

5. 사용 가능한 드라이브 펌웨어 업그레이드를 다운로드하고 준비합니다.
   a. 드라이브 펌웨어 업그레이드 에서 * NetApp 지원 * 을 선택합니다.
   b. NetApp Support 웹 사이트에서 * Downloads * 탭을 선택한 다음, * E-Series Disk Drive Firmware * 를 선택합니다.

      E-Series 디스크 펌웨어 페이지가 표시됩니다.

   c. 스토리지 어플라이언스에 설치된 각 * 드라이브 식별자 * 를 검색하고 각 드라이브 ID에 최신 펌웨어 버전이 있는지 확인합니다.
      - 펌웨어 개정판이 링크가 아닌 경우 이 드라이브 식별자는 최신 펌웨어 개정판을 가지고 있습니다.
      - 드라이브 식별자에 대해 하나 이상의 드라이브 부품 번호가 나열되면 해당 드라이브에 대해 펌웨어 업그레이드를 사용할 수 있습니다. 펌웨어 파일을 다운로드할 링크를 선택할 수 있습니다.



   d. 최신 펌웨어 개정판이 나열된 경우 펌웨어 개정판에서 링크를 선택합니다 (다운로드) 열을 클릭하여 펌웨어 파일이 포함된 '.zip' 아카이브를 다운로드합니다.
   e. 지원 사이트에서 다운로드한 드라이브 펌웨어 아카이브 파일의 압축을 풉니다.
6. 드라이브 펌웨어 업그레이드를 설치합니다.
   a. SANtricity 시스템 관리자의 드라이브 펌웨어 업그레이드 아래에서 * 업그레이드 시작 * 을 선택합니다.
   b. 찾아보기 * 를 선택하고 Support 사이트에서 다운로드한 새 드라이브 펌웨어 파일을 선택합니다.

      드라이브 펌웨어 파일의 파일 이름은 +D_HUC101212CSS600_30602291_MS01_2800_0002.DLP와 비슷합니다

      한 번에 하나씩 최대 4개의 드라이브 펌웨어 파일을 선택할 수 있습니다. 둘 이상의 드라이브 펌웨어 파일이 동일한 드라이브와 호환되는 경우 파일 충돌 오류가 발생합니다. 업그레이드에 사용할 드라이브 펌웨어 파일을 결정하고 다른 드라이브 펌웨어 파일을 제거합니다.

   c. 다음 * 을 선택합니다.
      - 드라이브 선택 * 은 선택한 펌웨어 파일로 업그레이드할 수 있는 드라이브를 나열합니다.

        호환되는 드라이브만 나타납니다.

      선택한 드라이브의 펌웨어가 * 제안된 펌웨어 * 에 나타납니다. 이 펌웨어를 변경해야 하는 경우 * Back * 을 선택합니다.

d. Offline (parallel) * upgrade를 선택합니다.

어플라이언스가 유지보수 모드이므로 오프라인 업그레이드 방법을 사용할 수 있습니다. 이 경우 모든 드라이브 및 모든 볼륨에 대해 I/O 작업이 중지됩니다.

> 제품이 유지보수 모드인지 확실하지 않은 경우 작업을 진행하지 마십시오. 오프라인 드라이브 펌웨어 업데이트를 시작하기 전에 어플라이언스를 유지 관리 모드로 전환하지 않으면 데이터가 손실될 수 있습니다.

e. 테이블의 첫 번째 열에서 업그레이드할 드라이브를 선택합니다.

모범 사례는 동일한 모델의 모든 드라이브를 동일한 펌웨어 개정판으로 업그레이드하는 것입니다.

f. 시작 * 을 선택하고 업그레이드를 수행할지 확인합니다.

업그레이드를 중지해야 하는 경우 * Stop * (중지 *)을 선택합니다. 현재 진행 중인 모든 펌웨어 다운로드가 완료되었습니다. 시작되지 않은 모든 펌웨어 다운로드는 취소됩니다.

> 드라이브 펌웨어 업그레이드를 중지하면 데이터가 손실되거나 드라이브를 사용할 수 없게 될 수 있습니다.

g. (선택 사항) 업그레이드된 항목 목록을 보려면 * Save Log * 를 선택합니다.

로그 파일은 브라우저의 다운로드 폴더에 'latest-upgrade-log-timestamp.txt'라는 이름으로 저장됩니다.

업그레이드 절차 중에 다음 오류가 발생하는 경우 적절한 권장 조치를 취하십시오.

- * 할당된 드라이브 실패 *

  이 오류가 발생하는 한 가지 이유는 드라이브에 적절한 서명이 없을 수 있기 때문입니다. 영향을 받는 드라이브가 승인된 드라이브인지 확인합니다. 자세한 내용은 기술 지원 부서에 문의하십시오.

드라이브를 교체할 때 교체 드라이브의 용량이 교체 중인 드라이브의 용량보다 크거나 같은지 확인하십시오.

스토리지 배열이 I/O를 수신하는 동안 오류가 발생한 드라이브를 교체할 수 있습니다

- * 스토리지 배열 확인 *
  - 각 컨트롤러에 IP 주소가 할당되었는지 확인합니다.
  - 컨트롤러에 연결된 모든 케이블이 손상되지 않았는지 확인합니다.
  - 모든 케이블이 단단히 연결되어 있는지 확인합니다.
- * 통합 핫 스페어 드라이브 *

  펌웨어를 업그레이드하기 전에 이 오류 상태를 수정해야 합니다.

- * 불완전한 볼륨 그룹 *

  하나 이상의 볼륨 그룹 또는 디스크 풀이 불완전하면 펌웨어를 업그레이드하기 전에 이 오류 조건을 수정해야 합니다.

- * 현재 모든 볼륨 그룹에서 실행 중인 독점 작업(백그라운드 미디어/패리티 검사 제외) *

  하나 이상의 배타적 작업이 진행 중인 경우 펌웨어를 업그레이드하기 전에 작업을 완료해야 합니다. System Manager를 사용하여 작업 진행률을 모니터링합니다.

- * 볼륨 없음 *

  펌웨어를 업그레이드하기 전에 누락된 볼륨 상태를 수정해야 합니다.

- * 두 컨트롤러 중 하나가 최적 상태 * 가 아닌 다른 상태입니다

  스토리지 어레이 컨트롤러 중 하나에 주의가 필요합니다. 펌웨어를 업그레이드하기 전에 이 상태를 수정해야 합니다.

- * 컨트롤러 오브젝트 그래프 * 간에 스토리지 파티션 정보가 일치하지 않습니다

  컨트롤러의 데이터를 검증하는 동안 오류가 발생했습니다. 이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

- * SPM 데이터베이스 컨트롤러 확인 실패 *

  컨트롤러에서 스토리지 파티션 매핑 데이터베이스 오류가 발생했습니다. 이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

- * 구성 데이터베이스 검증(스토리지 배열의 컨트롤러 버전에서 지원되는 경우) *

  컨트롤러에서 구성 데이터베이스 오류가 발생했습니다. 이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

- * MEL 관련 점검 *

  이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

- * 최근 7일 동안 10개가 넘는 DDE 정보 또는 중요 MEL 이벤트가 보고되었습니다 *

  이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

- * 지난 7일 동안 2개 이상의 2c 페이지 중요 MEL 이벤트가 보고되었습니다 *

  이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

- * 최근 7일 동안 성능이 저하된 드라이브 채널 중요 MEL 이벤트가 2개 이상 보고되었습니다 *

  이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

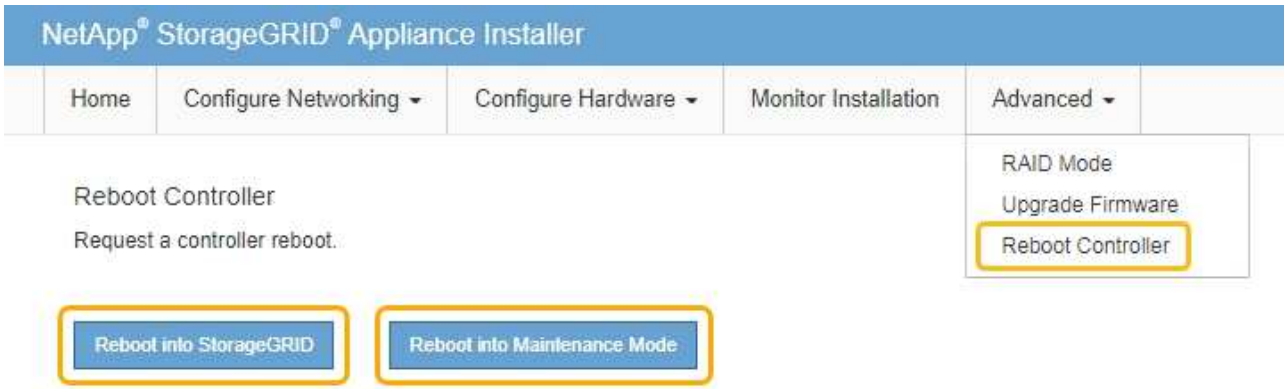
- * 지난 7일 동안 4개 이상의 중요한 MEL 항목 *

  이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

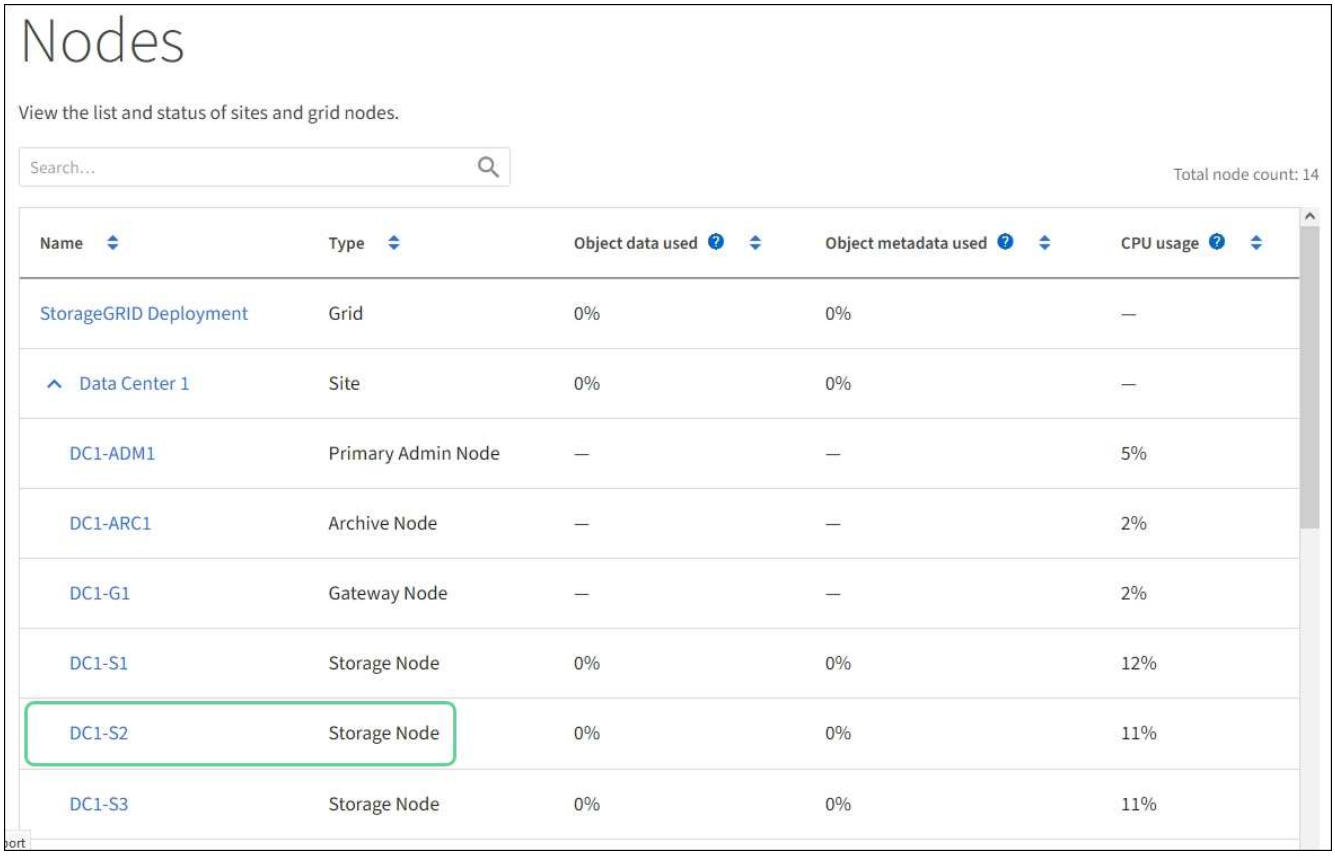
7. . 이 절차가 성공적으로 완료되었고 노드가 유지보수 모드일 때 수행할 추가 절차가 있는 경우 지금 수행합니다. 작업을 완료했거나 오류가 발생하여 다시 시작하려면 * 고급 * > * 컨트롤러 재부팅 * 을 선택하고 다음 옵션 중 하나를 선택합니다.

   - StorageGRID * 로 재부팅 * 을 선택합니다

- 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. 절차 중에 오류가 발생하여 다시 시작하려면 이 옵션을 선택합니다. 노드가 유지보수 모드로 재부팅된 후 장애가 발생한 절차의 적절한 단계에서 다시 시작하십시오.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. 노드 페이지에는 어플라이언스 노드에 대한 정상 상태(노드 이름 왼쪽에 아이콘이 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

스토리지 컨트롤러에서 SANtricity OS를 업그레이드합니다

SG5700에서 **E2800** 시리즈 스토리지 컨트롤러를 교체합니다

E2800 시리즈 컨트롤러가 최적의 상태로 작동하지 않거나 오류가 발생한 경우에는 컨트롤러를 교체해야 할 수 있습니다.

이 작업에 대해

- 교체할 컨트롤러와 부품 번호가 동일한 교체 컨트롤러가 있습니다.

> 절차가 동일하지 않으므로 E-Series 지침에 따라 StorageGRID 어플라이언스의 컨트롤러를 교체하지 마십시오.

- 컨트롤러에 연결된 각 케이블을 식별하는 라벨이 있습니다.
- 모든 드라이브가 보안된 경우, Simplex E2800 시리즈 컨트롤러 교체 절차의 단계를 검토했습니다. 여기에는 NetApp Support 사이트에서 E-Series SANtricity 스토리지 관리자를 다운로드 및 설치한 다음, EMW(엔터프라이즈 관리 창)를 사용하여 컨트롤러를 교체한 후 보안 드라이브를 잠금 해제하는 것이 포함됩니다.

> 저장된 키로 드라이브를 잠금 해제할 때까지 제품을 사용할 수 없습니다.

- 특정 액세스 권한이 있어야 합니다.
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

이 작업에 대해

다음 두 가지 방법으로 오류가 발생한 컨트롤러 캐니스터가 있는지 확인할 수 있습니다.

- SANtricity 시스템 관리자의 Recovery Guru에서 컨트롤러를 교체하도록 안내합니다.
- 컨트롤러의 주황색 주의 LED가 켜져 컨트롤러에 장애가 있음을 나타냅니다.

컨트롤러를 교체할 때 어플라이언스 스토리지 노드에 액세스할 수 없습니다. E2800 시리즈 컨트롤러가 충분히 작동할 경우 E5500SG 컨트롤러를 유지보수 모드로 설정합니다.

컨트롤러를 교체할 때는 원래 컨트롤러에서 배터리를 분리하여 교체 컨트롤러에 설치해야 합니다. 경우에 따라 원래 컨트롤러에서 호스트 인터페이스 카드를 제거하고 교체 컨트롤러에 설치해야 할 수도 있습니다.

> 대부분의 어플라이언스 모델의 스토리지 컨트롤러에는 HIC(호스트 인터페이스 카드)가 포함되지 않습니다.

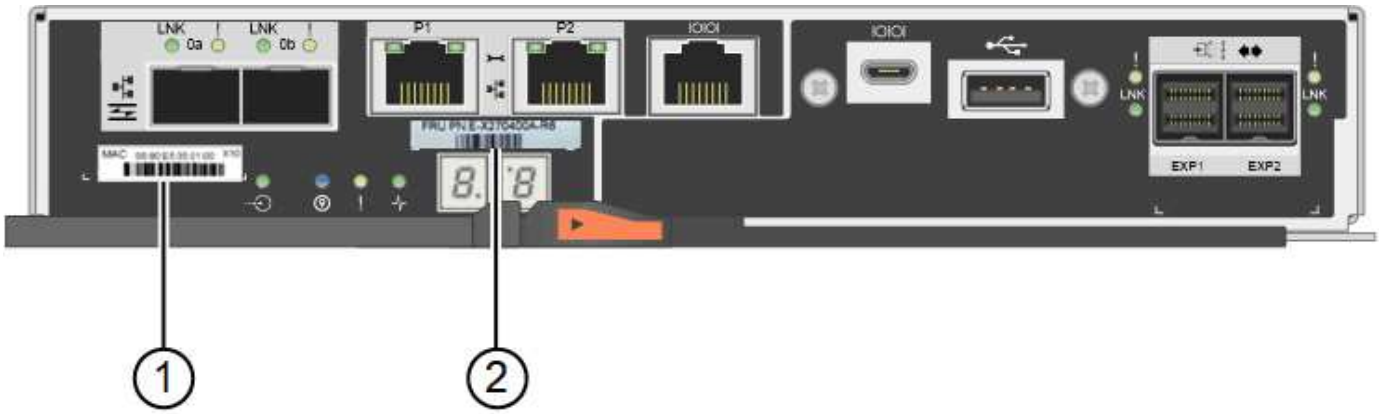
이 작업은 다음과 같은 부분으로 구성됩니다.

1. 준비
2. 컨트롤러를 오프라인으로 전환합니다
3. 컨트롤러를 제거합니다
4. 배터리를 새 컨트롤러로 이동합니다
5. 필요한 경우 HIC를 새 컨트롤러로 이동합니다
6. 컨트롤러를 교체합니다

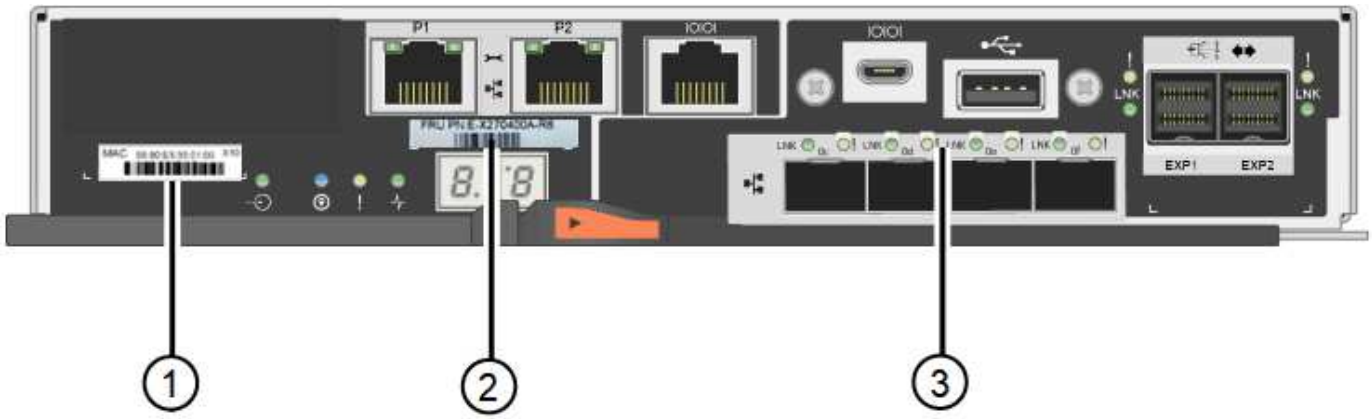
준비

이러한 수치는 E2800A 컨트롤러 및 E2800B 컨트롤러를 보여줍니다. E2800 시리즈 컨트롤러 및 EF570 컨트롤러를 교체하는 절차는 동일합니다.

- E2800A 스토리지 컨트롤러 *



- E2800B 스토리지 컨트롤러 *



라벨	구성 요소	설명
1	MAC 주소	관리 포트 1의 MAC 주소("'E2800A의 P1, E2800B의 0a"). DHCP를 사용하여 원래 컨트롤러의 IP 주소를 얻은 경우 이 주소가 새 컨트롤러에 연결되어 있어야 합니다.
2	FRU 부품 번호입니다	FRU 부품 번호입니다. 이 번호는 현재 설치된 컨트롤러의 교체 부품 번호와 일치해야 합니다.
3	4-포트 HIC	4-포트 HIC(호스트 인터페이스 카드) 교체 작업을 수행할 때 이 카드를 새 컨트롤러로 옮겨야 합니다. • 참고 *: E2800A 컨트롤러에는 HIC가 없습니다.

단계

1. E2800 컨트롤러 교체 절차의 지침에 따라 컨트롤러 제거를 준비합니다.

SANtricity 시스템 관리자를 사용하여 다음 단계를 수행합니다.

a. 현재 컨트롤러에 설치되어 있는 SANtricity OS 소프트웨어 버전을 기록해 둡니다.

b. 현재 설치된 NVSRAM 버전을 기록해 둡니다.

c. 드라이브 보안 기능이 활성화된 경우, 저장된 키가 있는지, 설치에 필요한 암호를 알고 있는지 확인하십시오.

> * 데이터 액세스 손실 및 # 8212; * 어플라이언스의 모든 드라이브가 보안이 활성화된 경우 SANtricity 스토리지 관리자의 엔터프라이즈 관리 창을 사용하여 보안 드라이브의 잠금을 해제할 때까지 새 컨트롤러가 어플라이언스에 액세스할 수 없습니다.

d. 구성 데이터베이스를 백업합니다.

컨트롤러를 제거할 때 문제가 발생하면 저장된 파일을 사용하여 구성을 복원할 수 있습니다.

e. 어플라이언스에 대한 지원 데이터를 수집합니다.

> 구성 요소를 교체하기 전과 교체 후에 지원 데이터를 수집하면 교체로 문제가 해결되지 않을 경우 기술 지원 부서에 전체 로그 세트를 보낼 수 있습니다.

컨트롤러를 오프라인으로 전환합니다

단계

1. StorageGRID 어플라이언스가 StorageGRID 시스템에서 실행 중인 경우 E5500SG 컨트롤러를 유지보수 모드로 설정합니다.
2. E2800 컨트롤러가 제어된 종료를 수행할 수 있을 만큼 충분히 작동하는지 확인하려면 모든 작업이 완료되었는지 확인합니다.
   a. SANtricity 시스템 관리자의 홈 페이지에서 * 진행 중인 작업 보기 * 를 선택합니다.
   b. 모든 작업이 완료되었는지 확인합니다.

컨트롤러를 분리합니다

단계

1. 제품에서 컨트롤러를 분리합니다.
   a. ESD 밴드를 착용하거나 정전기 방지 조치를 취하십시오.
   b. 케이블에 레이블을 지정한 다음 케이블 및 SFP를 분리합니다.

   > 성능 저하를 방지하려면 케이블을 비틀거나 접거나 끼거나 밟지 마십시오.

   c. 캠 핸들의 래치를 눌러 제품에서 컨트롤러를 분리한 다음 캠 핸들을 오른쪽으로 엽니다.
   d. 양손과 캠 손잡이를 사용하여 제어기를 제품에서 밀어 꺼냅니다.

   > 컨트롤러의 무게를 지탱하려면 항상 두 손을 사용하십시오.

   e. 착탈식 덮개가 위를 향하도록 하여 정전기가 없는 평평한 표면에 컨트롤러를 놓습니다.

f. 단추를 누르고 덮개를 밀어 덮개를 분리합니다.

배터리를 새 컨트롤러로 이동합니다

단계

1. 장애가 발생한 컨트롤러에서 배터리를 분리하고 교체 컨트롤러에 설치합니다.

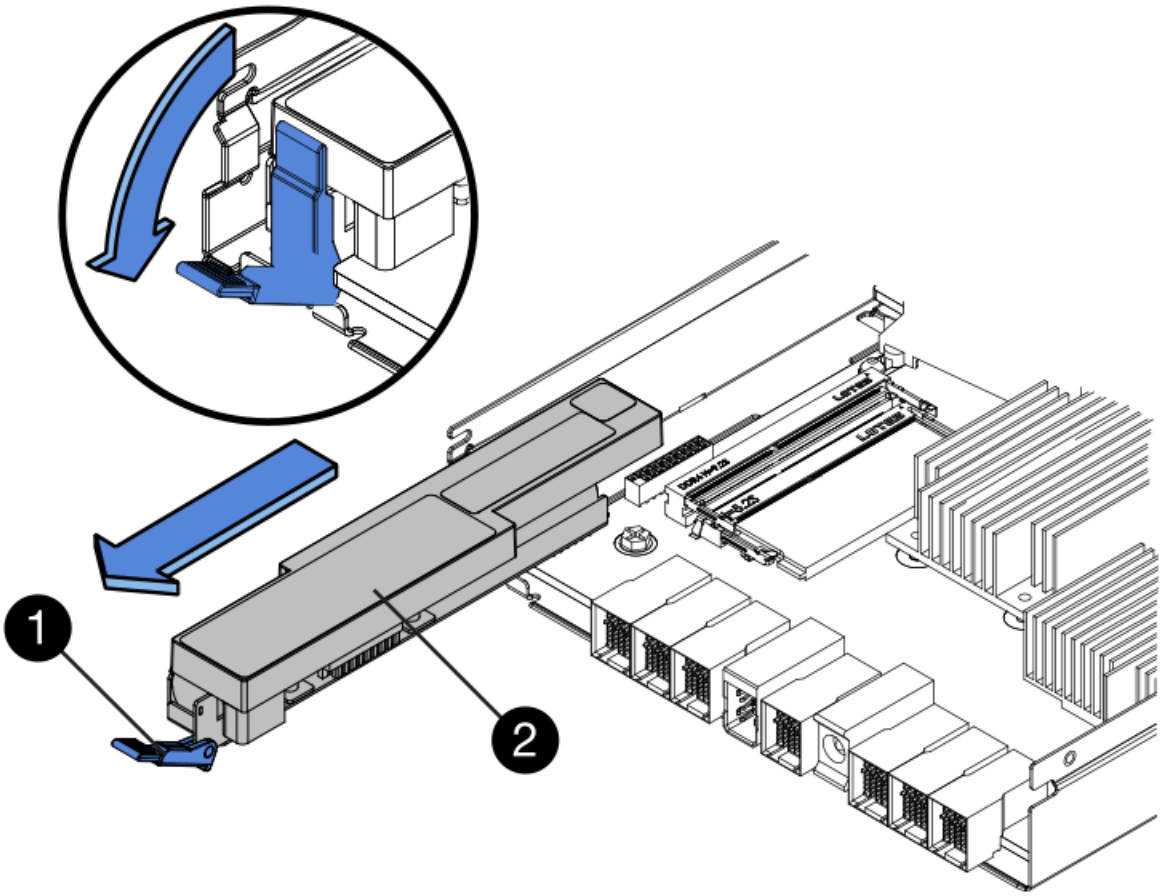
   a. 컨트롤러 내부(배터리와 DIMM 사이)의 녹색 LED가 꺼져 있는지 확인합니다.

      이 녹색 LED가 켜져 있으면 컨트롤러는 여전히 배터리 전원을 사용하고 있습니다. 구성 요소를 제거하기 전에 이 LED가 꺼질 때까지 기다려야 합니다.

항목	설명
1	내부 캐시 활성 LED
2	배터리

   b. 배터리의 파란색 분리 래치를 찾습니다.

   c. 분리 래치를 아래로 눌러 배터리를 분리합니다.



항목	설명
1	배터리 분리 래치
2	배터리

d. 배터리를 들어 올려 컨트롤러에서 꺼냅니다.

e. 교체용 컨트롤러에서 덮개를 분리합니다.

f. 교체용 컨트롤러의 방향을 조정하여 배터리 슬롯이 사용자를 향하도록 합니다.

g. 배터리를 약간 아래쪽으로 비스듬히 컨트롤러에 삽입합니다.

   배터리 전면의 금속 플랜지를 컨트롤러 하단의 슬롯에 삽입하고 배터리 상단을 컨트롤러 왼쪽의 작은 정렬 핀 아래에 밀어 넣어야 합니다.

h. 배터리 래치를 위로 이동하여 배터리를 고정합니다.

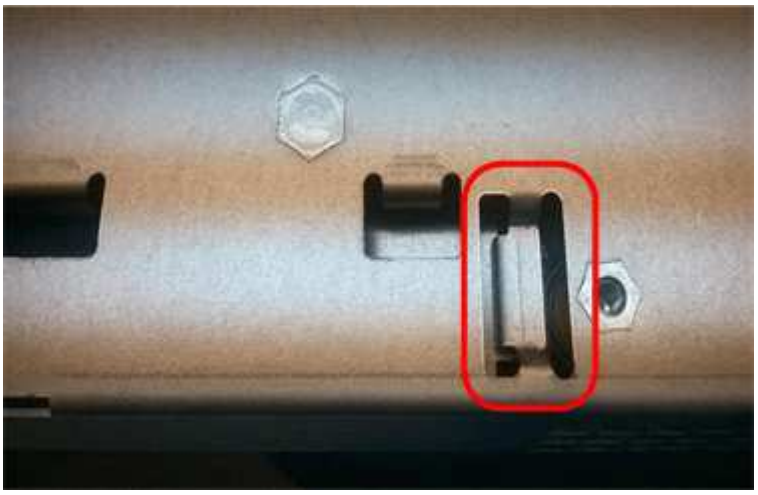
   래치가 제자리에 고정되면 래치 하단이 섀시의 금속 슬롯에 후크됩니다.

i. 컨트롤러를 뒤집어 배터리가 올바르게 설치되었는지 확인합니다.

> * 하드웨어 손상 가능성 * — 배터리 전면의 금속 플랜지가 컨트롤러의 슬롯에 완전히 삽입되어야 합니다(첫 번째 그림 참조). 배터리가 올바르게 설치되지 않은 경우(두 번째 그림 참조) 금속 플랜지가 컨트롤러 보드에 닿으면 손상이 발생할 수 있습니다.

- * 정답입니다.- 배터리의 금속 플랜지가 컨트롤러의 슬롯에 완전히 삽입됩니다. *

- * 잘못됨 — 배터리의 금속 플랜지가 컨트롤러의 슬롯에 삽입되지 않음: *



2. 컨트롤러 덮개를 장착합니다.

필요한 경우 **HIC**를 새 컨트롤러로 이동합니다

단계

1. 장애 컨트롤러에 HIC(호스트 인터페이스 카드)가 포함된 경우 장애가 발생한 컨트롤러에서 교체 컨트롤러로 HIC를 이동합니다.

   E2800B 컨트롤러에만 별도의 HIC가 사용됩니다. HIC는 메인 컨트롤러 보드에 장착되며 SPF 커넥터 2개를 포함합니다.

   > 이 절차의 그림에서는 2-포트 HIC를 보여 줍니다. 컨트롤러의 HIC는 포트 수가 다를 수 있습니다.

2. 컨트롤러에 HIC(E2800A)가 없는 경우 컨트롤러 덮개를 교체합니다. 컨트롤러에 HIC(E2800B)가 있는 경우 로

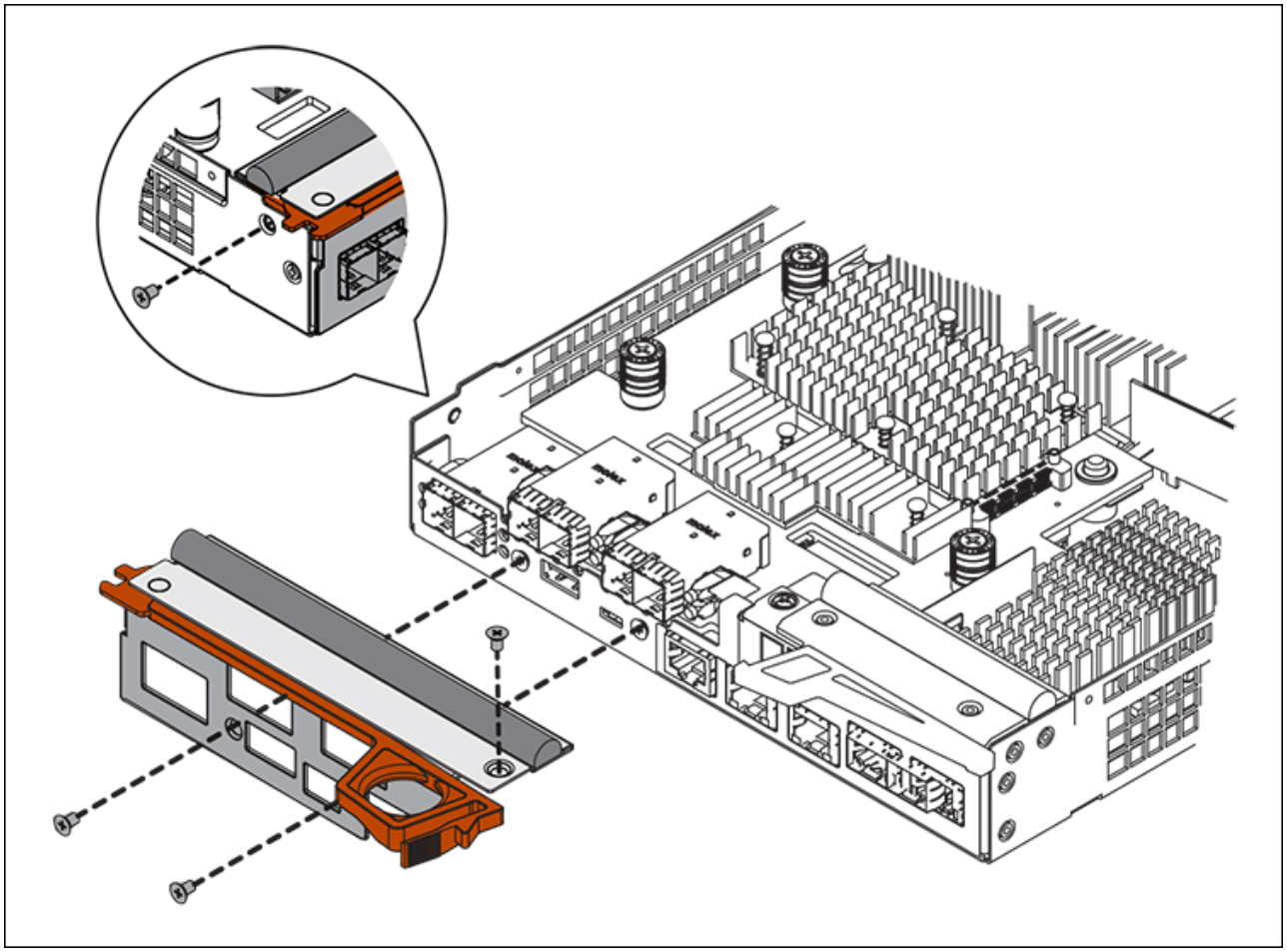
이동합니다 HIC를 장애 컨트롤러에서 교체 컨트롤러로 이동합니다.

a. HIC가 장착된 경우 HIC를 장애가 발생한 컨트롤러에서 교체 컨트롤러로 이동합니다.

b. HIC에서 모든 SFP를 제거합니다.

c. 1 십자 드라이버를 사용하여 HIC 페이스플레이트를 컨트롤러에 연결하는 나사를 제거합니다.

나사는 상단에 1개, 측면에 1개, 전면에 2개 등 4개가 있습니다.

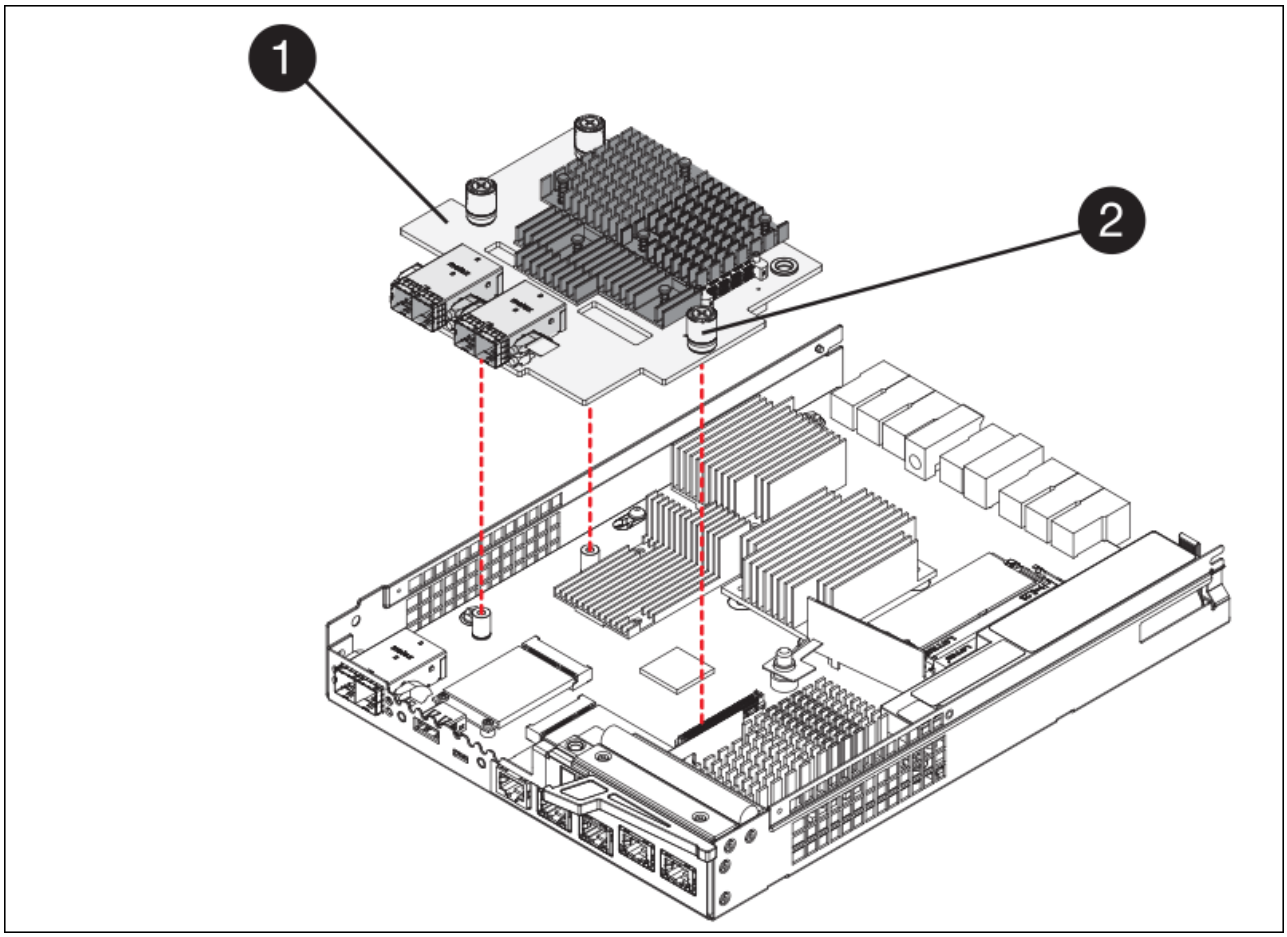


d. HIC 페이스플레이트를 탈거하십시오.

e. 손가락이나 십자 드라이버를 사용하여 HIC를 컨트롤러 카드에 고정하는 세 개의 나비 나사를 풉니다.

f. 카드를 들어 올리고 다시 밀어 컨트롤러 카드에서 HIC를 조심스럽게 분리합니다.

> HIC 하단 또는 컨트롤러 카드 상단에 있는 구성 요소가 긁히거나 범프되지 않도록 주의하십시오.



라벨	설명
1	호스트 인터페이스 카드
2	나비 나사

g. HIC를 정전기가 없는 표면에 놓습니다.

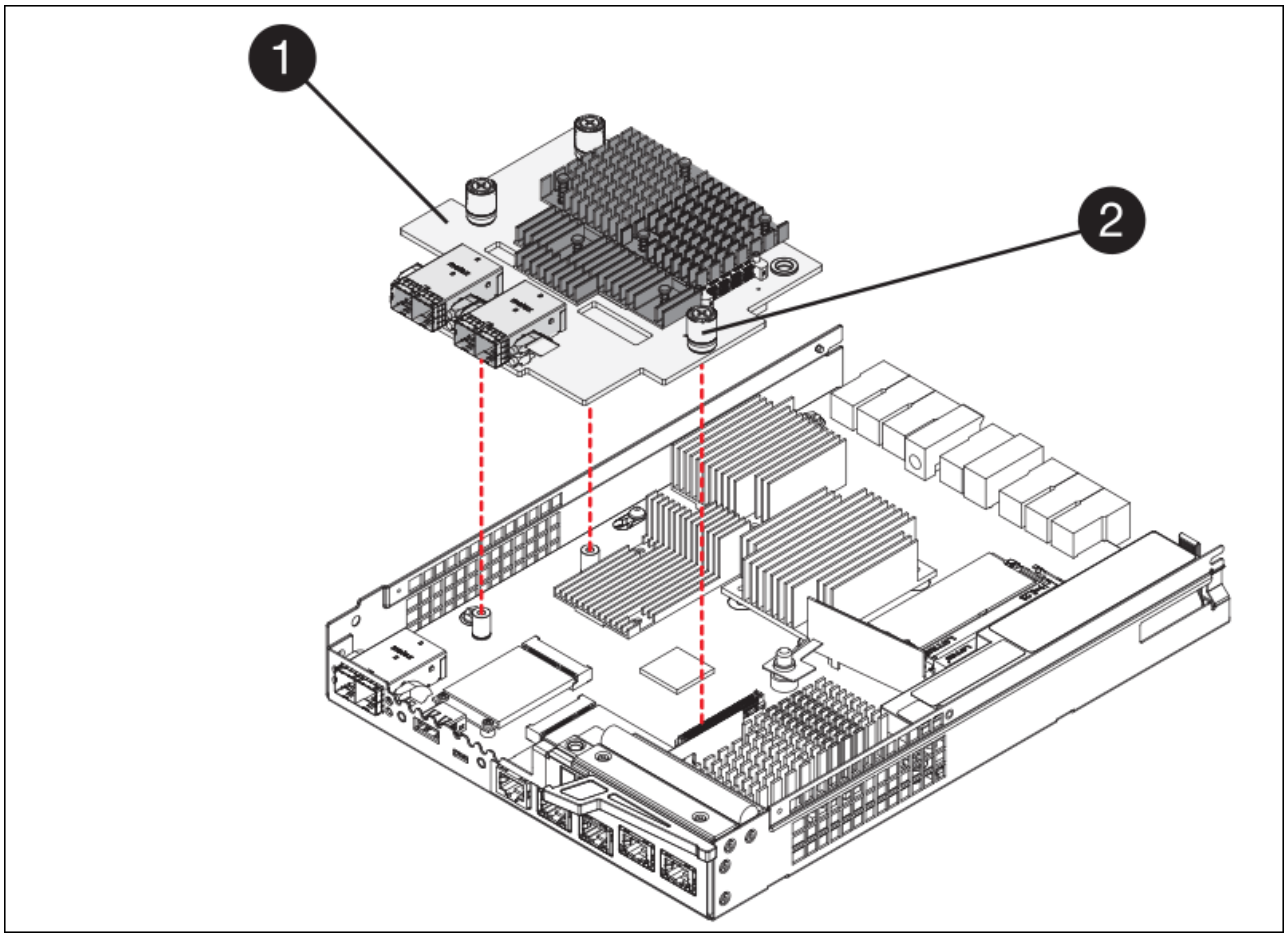
h. 1 Phillips 드라이버를 사용하여 블랭크 페이스 플레이트를 교체 컨트롤러에 연결하는 나사 4개를 분리하고 전면판을 분리하십시오.

i. HIC의 3개의 나비 나사를 교체 컨트롤러의 해당 구멍에 맞추고 HIC 아래쪽에 있는 커넥터를 컨트롤러 카드의 HIC 인터페이스 커넥터와 맞춥니다.

   HIC 하단 또는 컨트롤러 카드 상단에 있는 구성 요소가 긁히거나 범프되지 않도록 주의하십시오.

j. HIC를 조심스럽게 제자리로 내리고 HIC 커넥터를 가볍게 눌러 HIC 커넥터를 장착합니다.

> * 장비 손상 가능성 * — HIC와 나비 나사 사이의 컨트롤러 LED에 골드 리본 커넥터가 끼이지 않도록 매우 조심하십시오.

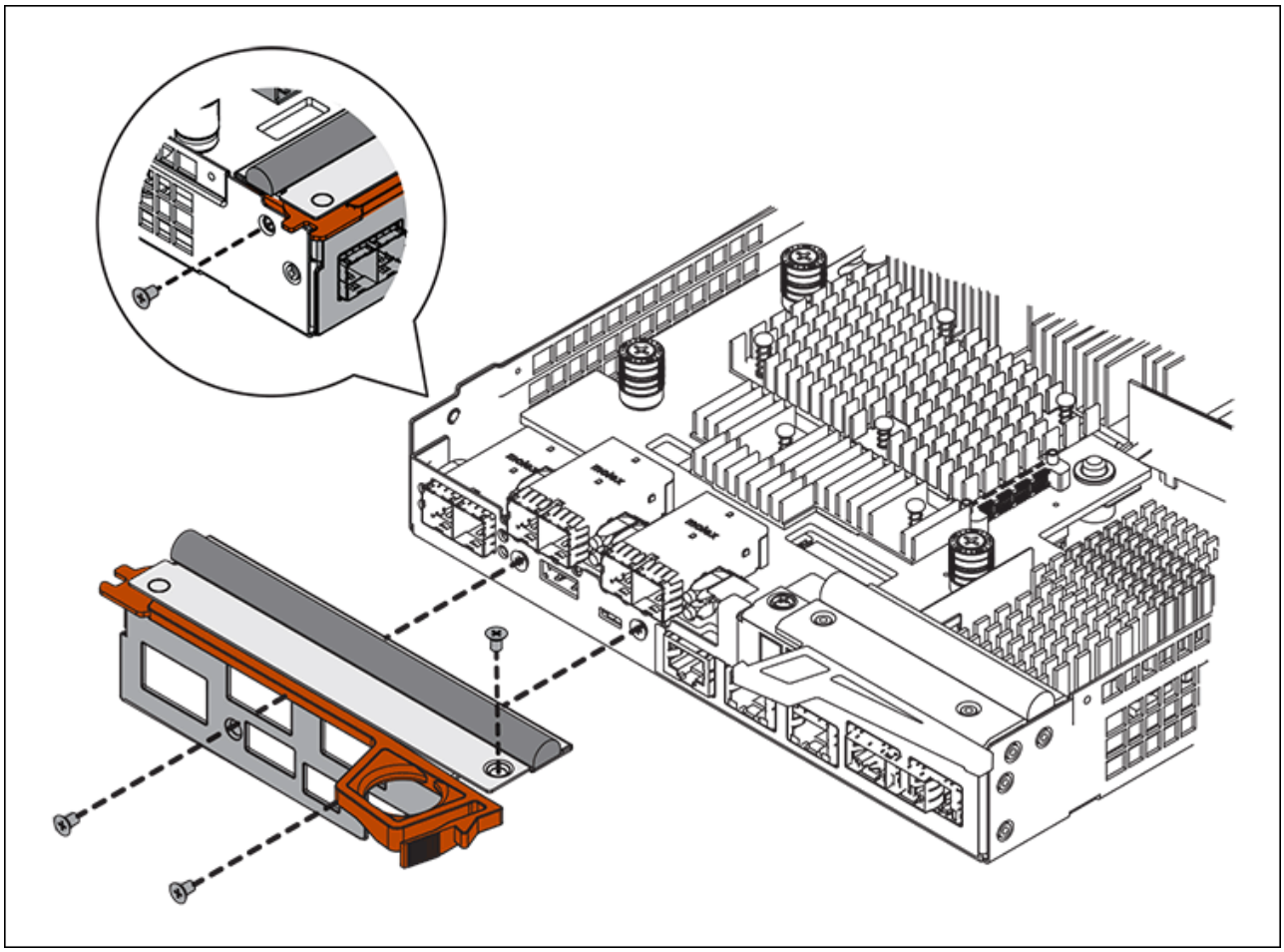


라벨	설명
1	호스트 인터페이스 카드
2	나비 나사

a. HIC 나비 나사를 손으로 조입니다.

   드라이버를 사용하지 마십시오. 또는 나사를 너무 세게 조일 수 있습니다.

b. 1 십자 드라이버를 사용하여 원래 컨트롤러에서 제거한 HIC 면판을 4개의 나사로 새 컨트롤러에 부착합니다.



c. 제거된 SFP를 HIC에 다시 설치합니다.

컨트롤러를 교체합니다

단계

1. 교체 컨트롤러를 제품에 설치합니다.

   a. 이동식 덮개가 아래를 향하도록 컨트롤러를 뒤집습니다.

   b. 캠 손잡이를 열린 상태에서 컨트롤러를 제품 안으로 끝까지 밀어 넣습니다.

   c. 캠 핸들을 왼쪽으로 이동하여 컨트롤러를 제자리에 고정합니다.

   d. 케이블 및 SFP를 교체합니다.

   e. E2800 컨트롤러가 재부팅될 때까지 기다립니다. 7세그먼트 디스플레이에 99 상태가 표시되는지 확인합니다.

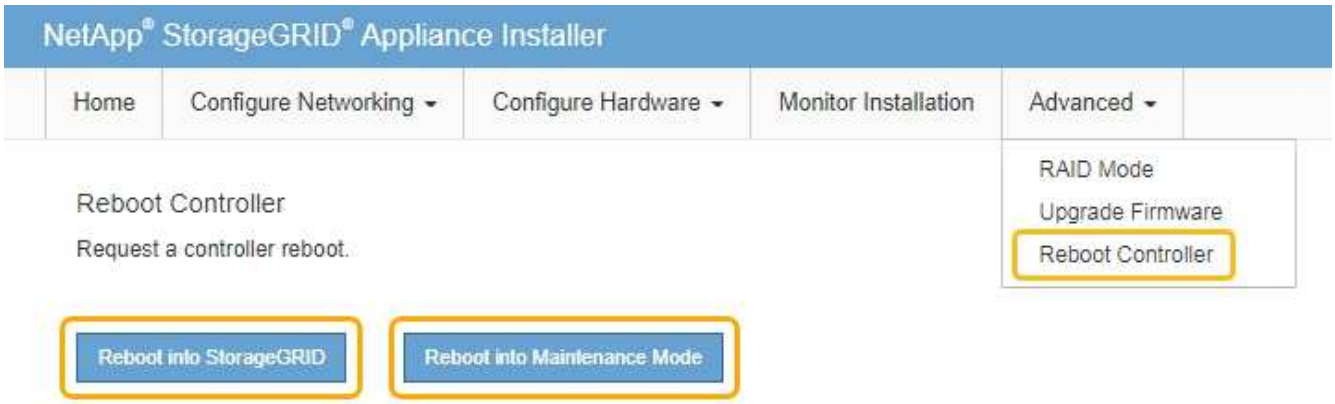
   f. 교체 컨트롤러에 IP 주소를 할당하는 방법을 결정합니다.

   > 교체 컨트롤러에 IP 주소를 할당하는 단계는 관리 포트 1을 DHCP 서버가 있는 네트워크에 연결했는지 여부 및 모든 드라이브가 보호되는지 여부에 따라 달라집니다.

   관리 포트 1이 DHCP 서버가 있는 네트워크에 연결되어 있는 경우 새 컨트롤러는 DHCP 서버에서 해당 IP 주소를 가져옵니다. 이 값은 원래 컨트롤러의 IP 주소와 다를 수 있습니다.

2. 보안 드라이브를 사용하는 어플라이언스의 경우 E2800 컨트롤러 교체 절차의 지침에 따라 드라이브 보안 키를 가져옵니다.

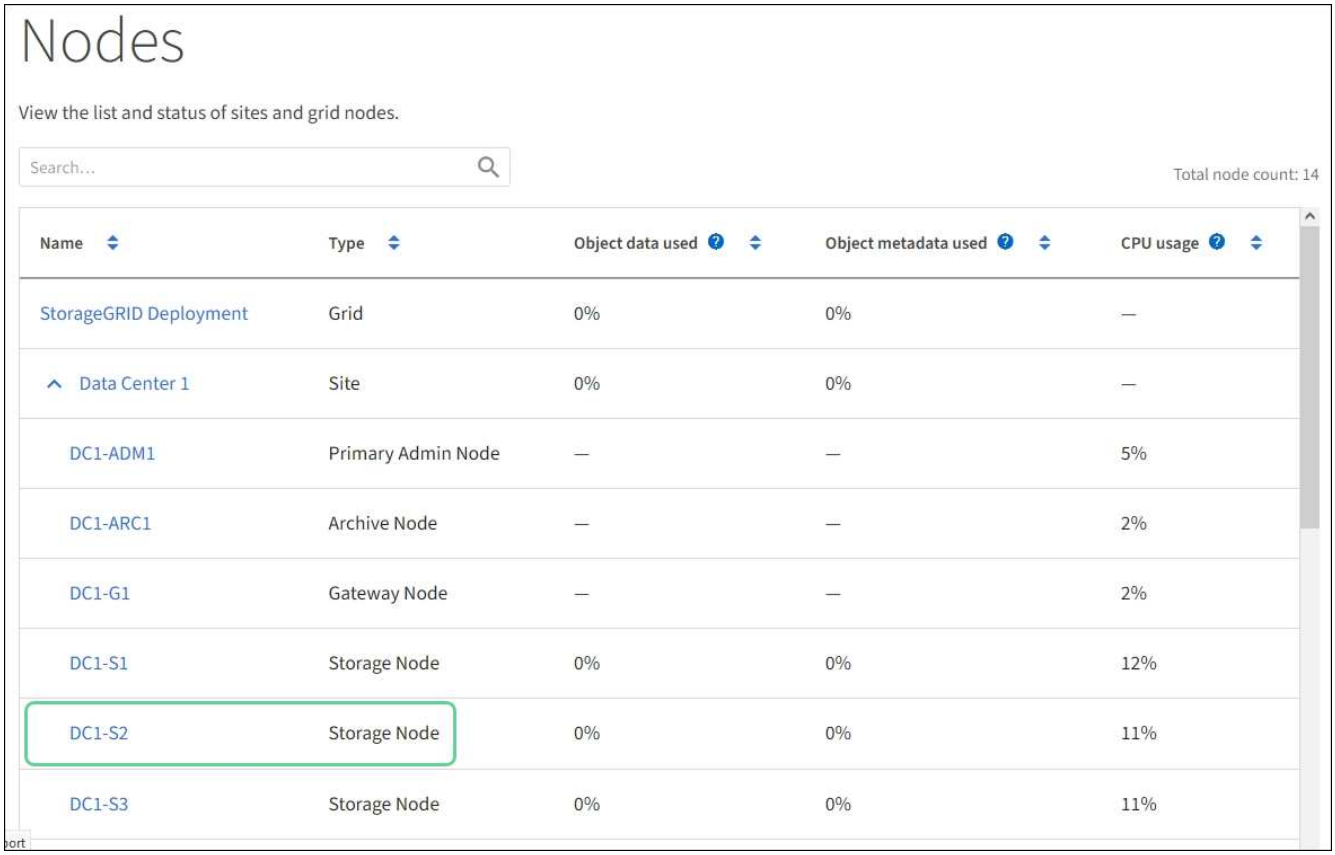
3. 제품을 정상 작동 모드로 되돌리십시오. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * StorageGRID * 으로 재부팅 * 을 선택합니다.



4. 재부팅 중에 노드의 상태를 모니터링하여 노드가 그리드에 재결합되었는지 확인합니다.

   어플라이언스가 재부팅되고 그리드에 다시 추가됩니다. 이 프로세스는 최대 20분 정도 소요될 수 있습니다.

5. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인합니다. 그리드 관리자에서 노드 페이지에 어플라이언스 노드에 대한 정상 상태(노드 이름 왼쪽에 아이콘이 없음)가 표시되는지 확인합니다. 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



6. SANtricity 시스템 관리자에서 새 컨트롤러가 최적화되었는지 확인하고 지원 데이터를 수집합니다.

부품을 교체한 후 키트와 함께 제공된 RMA 지침에 따라 오류가 발생한 부품을 NetApp에 반환합니다. 를 참조하십시오 "부품 반품 및 앰프, 교체" 페이지를 참조하십시오.

관련 정보

"NetApp E-Series 시스템 문서 사이트"

E5500SG 컨트롤러를 교체합니다

E700SG 컨트롤러가 최적의 상태로 작동하지 않거나 장애가 발생한 경우 교체해야 할 수 있습니다.

필요한 것

- 교체할 컨트롤러와 부품 번호가 동일한 교체 컨트롤러가 있습니다.
- 장애가 발생한 E5700 컨트롤러 교체를 위한 E-Series 지침을 다운로드했습니다.

> 특정 단계를 수행하기 위한 추가 세부 정보가 필요한 경우에만 E-Series 지침을 참조할 수 있습니다. 절차가 동일하지 않으므로 E-Series 지침에 따라 StorageGRID 어플라이언스의 컨트롤러를 교체하지 마십시오. 예를 들어, E5700 컨트롤러의 E-Series 지침은 장애가 발생한 컨트롤러에서 배터리와 호스트 인터페이스 카드(HIC)를 제거하여 교체 컨트롤러에 설치하는 방법을 설명합니다. 이러한 단계는 E5500SG 컨트롤러에는 적용되지 않습니다.

- 컨트롤러에 연결된 각 케이블을 식별하는 라벨이 있습니다.
- 제품이 다 되었습니다 유지보수 모드로 전환되었습니다.

이 작업에 대해

컨트롤러를 교체할 때 어플라이언스 스토리지 노드에 액세스할 수 없습니다. E5500SG 컨트롤러가 충분히 작동하는 경우 이 절차를 시작할 때 제어된 종료를 수행할 수 있습니다.

> StorageGRID 소프트웨어를 설치하기 전에 컨트롤러를 교체하는 경우 이 절차를 완료한 후 즉시 StorageGRID 어플라이언스 설치 프로그램에 액세스하지 못할 수 있습니다. 어플라이언스와 동일한 서브넷에 있는 다른 호스트에서 StorageGRID 어플라이언스 설치 프로그램에 액세스할 수 있지만 다른 서브넷에 있는 호스트에서는 액세스할 수 없습니다. 이 조건은 15분 내에 해결되어야 하며(원래 컨트롤러의 ARP 캐시 항목이 시간 초과될 때), 또는 로컬 라우터 또는 게이트웨이에서 수동으로 이전의 ARP 캐시 항목을 삭제하여 즉시 조건을 지울 수 있습니다.

단계

1. 어플라이언스를 유지보수 모드로 전환한 후 E5500SG 컨트롤러를 종료합니다.
   a. 그리드 노드에 로그인합니다.
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

   b. E700SG 컨트롤러를 종료합니다. + " * shutdown -h now * "

c. 캐시 메모리의 데이터가 드라이브에 기록될 때까지 기다립니다.

   E2800 컨트롤러 후면의 녹색 캐시 활성 LED는 캐시된 데이터를 드라이브에 기록해야 할 때 켜집니다. 이 LED가 꺼질 때까지 기다려야 합니다.

2. 전원을 끕니다.
   a. SANtricity 시스템 관리자의 홈 페이지에서 * 진행 중인 작업 보기 * 를 선택합니다.
   b. 모든 작업이 완료되었는지 확인합니다.
   c. 제품의 두 전원 스위치를 모두 끕니다.
   d. 모든 LED가 꺼질 때까지 기다립니다.
3. 컨트롤러에 연결된 StorageGRID 네트워크가 DHCP 서버를 사용하는 경우:
   a. 교체용 컨트롤러의 포트에 대한 MAC 주소를 확인합니다(컨트롤러의 레이블에 위치).
   b. 네트워크 관리자에게 문의하여 교체 컨트롤러의 MAC 주소를 반영하도록 원본 컨트롤러의 IP 주소 설정을 업데이트하십시오.

   > 교체 컨트롤러에 전원을 켜기 전에 원래 컨트롤러의 IP 주소가 업데이트되었는지 확인해야 합니다. 그렇지 않으면 컨트롤러가 부팅될 때 새 DHCP IP 주소를 가져오며 StorageGRID에 다시 연결되지 않을 수 있습니다. 이 단계는 컨트롤러에 연결된 모든 StorageGRID 네트워크에 적용됩니다.

4. 제품에서 컨트롤러를 분리합니다.
   a. ESD 밴드를 착용하거나 정전기 방지 조치를 취하십시오.
   b. 케이블에 레이블을 지정한 다음 케이블 및 SFP를 분리합니다.

   > 성능 저하를 방지하려면 케이블을 비틀거나 접거나 끼거나 밟지 마십시오.

   c. 캠 핸들의 래치를 눌러 제품에서 컨트롤러를 분리한 다음 캠 핸들을 오른쪽으로 엽니다.
   d. 양손과 캠 손잡이를 사용하여 제어기를 제품에서 밀어 꺼냅니다.

   > 컨트롤러의 무게를 지탱하려면 항상 두 손을 사용하십시오.

5. 교체 컨트롤러를 제품에 설치합니다.
   a. 이동식 덮개가 아래를 향하도록 컨트롤러를 뒤집습니다.
   b. 캠 손잡이를 열린 상태에서 컨트롤러를 제품 안으로 끝까지 밀어 넣습니다.
   c. 캠 핸들을 왼쪽으로 이동하여 컨트롤러를 제자리에 고정합니다.
   d. 케이블 및 SFP를 교체합니다.
6. 어플라이언스 전원을 켜고 컨트롤러 LED와 7개 세그먼트 디스플레이를 모니터링합니다.

   컨트롤러가 성공적으로 부팅되면 7개 세그먼트 디스플레이에 다음이 표시됩니다.

   - E2800 컨트롤러:

     최종 국가는 99다.

- E5500SG 컨트롤러:

  마지막 상태는 HA입니다.

7. 어플라이언스 스토리지 노드가 그리드 관리자에 표시되고 경보가 나타나지 않는지 확인합니다.

관련 정보

"NetApp E-Series 시스템 문서 사이트"

다른 하드웨어 구성 요소를 교체합니다

StorageGRID 제품에서 컨트롤러 배터리, 드라이브, 팬 또는 전원 공급 장치를 교체해야 할 수 있습니다.

필요한 것

- E-Series 하드웨어 교체 절차가 있습니다.
- 제품이 다 되었습니다 유지보수 모드로 전환되었습니다 구성 요소 교체 절차에서 제품을 종료해야 하는 경우

이 작업에 대해

E2800 컨트롤러의 배터리를 교체하려면 E2800 컨트롤러 교체에 대한 지침을 참조하십시오. 이 지침은 제품에서 컨트롤러를 분리하고, 컨트롤러에서 배터리를 분리하고, 배터리를 설치하고, 컨트롤러를 교체하는 방법을 설명합니다.

어플라이언스에 있는 드라이브, 전원 팬 캐니스터, 팬 캐니스터, 전원 캐니스터 또는 드라이브 드로어를 교체하려면 E-Series의 E2800 하드웨어 유지보수 절차에 액세스하십시오.

SG5712 구성 요소 교체 지침

FRU	에 대한 **E-Series** 지침을 참조하십시오
드라이브	E2800 12 드라이브 또는 24 드라이브 쉘프의 드라이브 교체
전원 팬 캐니스터	E2800 쉘프의 전원 팬 캐니스터 교체

SG5760 구성 요소 교체 지침

FRU	에 대한 **E-Series** 지침을 참조하십시오
드라이브	E2860 쉘프의 드라이브 교체
전원 캐니스터	E2860 쉘프의 전원 캐니스터 교체
팬 캐니스터	E2860 쉘프의 팬 캐니스터 교체
드라이브 드로어	E2860 쉘프의 드라이브 드로어 교체

관련 정보

E2800 컨트롤러를 교체합니다

"NetApp E-Series 시스템 문서 사이트"

E5500SG 컨트롤러의 링크 구성을 변경합니다

E5500SG 컨트롤러의 이더넷 링크 구성을 변경할 수 있습니다. 포트 연결 모드, 네트워크 연결 모드 및 링크 속도를 변경할 수 있습니다.

필요한 것

E5500SG 컨트롤러를 유지보수 모드로 설정합니다.

> StorageGRID 어플라이언스를 유지보수 모드로 전환하면 원격 액세스가 불가능한 경우가 드물게 있습니다.

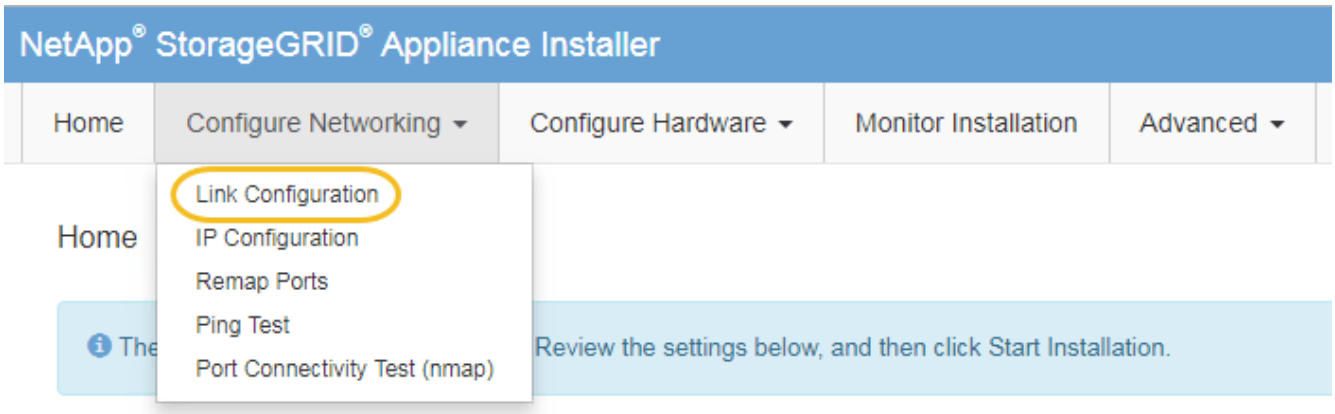
이 작업에 대해

E5500SG 컨트롤러의 이더넷 링크 구성을 변경하는 옵션은 다음과 같습니다.

- 포트 결합 모드 * 를 고정에서 집계로, 또는 Aggregate에서 고정으로 변경
- Active-Backup에서 LACP로 또는 LACP에서 Active-Backup으로 * 네트워크 결합 모드 * 변경
- VLAN 태그 지정 활성화 또는 비활성화 또는 VLAN 태그 값 변경
- 링크 속도를 10GbE에서 25GbE로, 25GbE에서 10GbE로 변경합니다

단계

1. 메뉴에서 * 네트워킹 구성 * > * 링크 구성 * 을 선택합니다.



2. 링크 설정을 원하는 대로 변경합니다.

   옵션에 대한 자세한 내용은 ""네트워크 링크 구성"을 참조하십시오.

3. 선택 사항에 만족하면 * 저장 * 을 클릭합니다.

> 연결된 네트워크 또는 링크를 변경한 경우 연결이 끊어질 수 있습니다. 1분 내에 다시 연결되지 않으면 어플라이언스에 할당된 다른 IP 주소 중 하나를 사용하여 StorageGRID 어플라이언스 설치 프로그램의 URL을 다시 입력합니다. + " * https://*E5700SG_Controller_IP*:8443*`

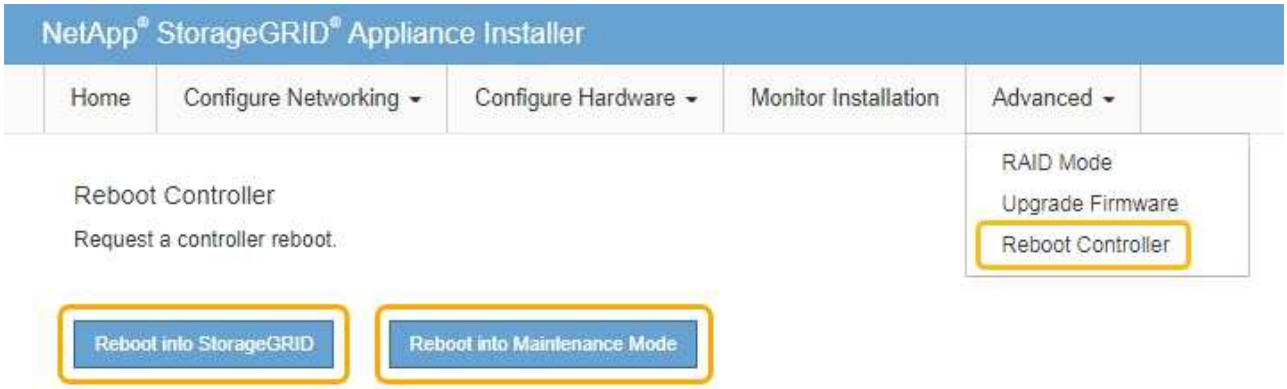
VLAN 설정을 변경한 경우 어플라이언스의 서브넷이 변경되었을 수 있습니다. 어플라이언스의 IP 주소를 변경해야 하는 경우 에 따르십시오 IP 구성을 설정합니다 지침.

4. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * 핑 테스트 * 를 선택합니다.
5. Ping 테스트 도구를 사용하여 에서 변경한 링크 구성의 영향을 받을 수 있는 네트워크의 IP 주소에 대한 연결을 확인합니다 링크 구성을 변경합니다 단계.

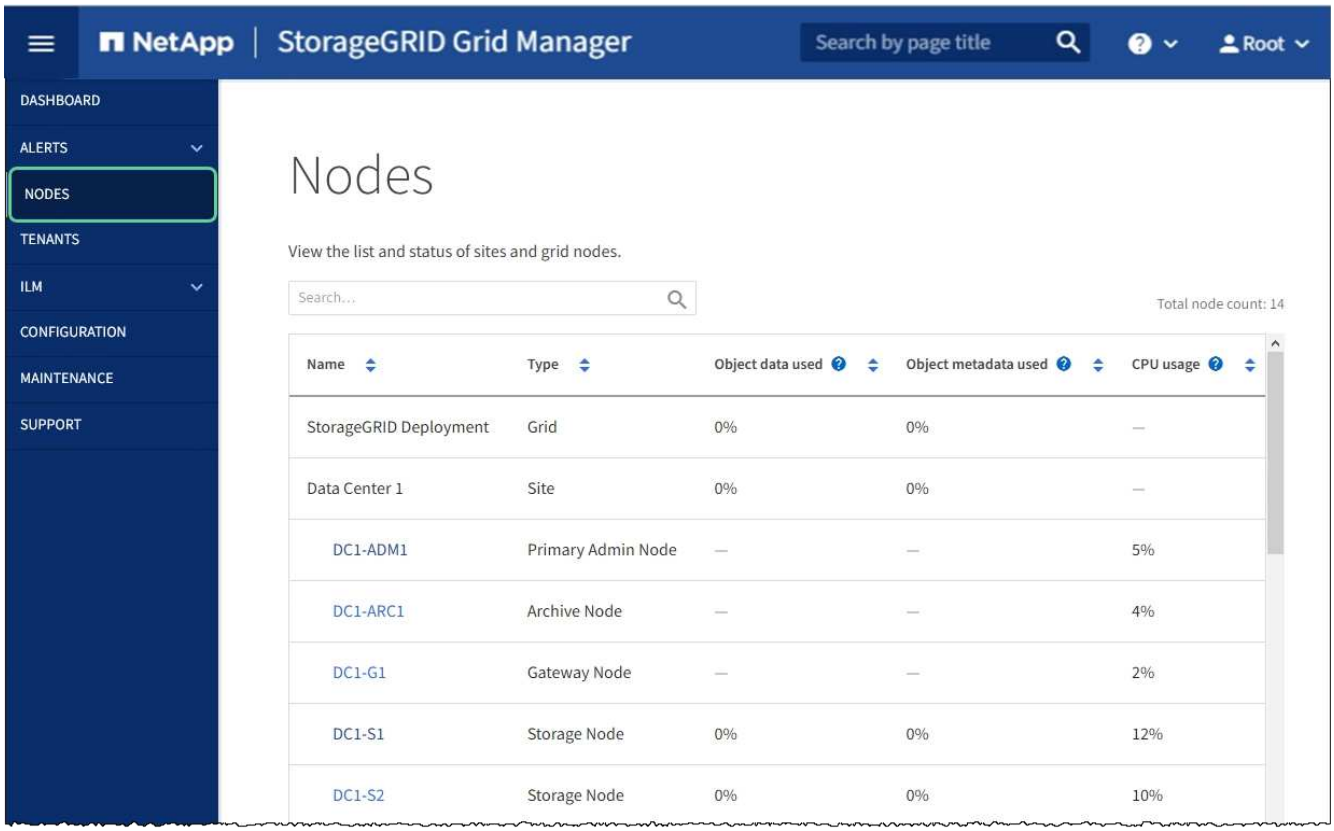
   수행할 다른 테스트 외에도 운영 관리 노드의 그리드 IP 주소와 하나 이상의 다른 스토리지 노드의 그리드 IP 주소를 ping할 수 있는지 확인합니다. 필요한 경우 링크 구성 문제를 해결하십시오.

6. 링크 구성 변경 사항이 작동한다고 만족하면 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.

   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



   어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

네트워크 링크 구성(SG5700)

MTU 설정을 변경합니다

어플라이언스 노드에 대한 IP 주소를 구성할 때 할당한 MTU 설정을 변경할 수 있습니다.

이 작업에 대해

네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

어플라이언스 노드를 재부팅하지 않고 MTU 설정을 변경하려면 IP 변경 도구를 사용합니다.

초기 설치 중에 StorageGRID 어플라이언스 설치 프로그램에서 클라이언트 또는 관리자 네트워크가 구성되지 않은 경우 유지보수 모드를 사용하여 MTU 설정을 변경합니다.

IP 변경 도구를 사용하여 **MTU** 설정을 변경합니다

필요한 것

Change IP 툴을 사용할 수 있는 "passwords.txt" 파일이 있습니다.

단계

IP 변경 도구에 액세스하여 에 설명된 대로 MTU 설정을 업데이트합니다 노드 네트워크 구성을 변경합니다.

유지보수 모드를 사용하여 **MTU** 설정을 변경합니다

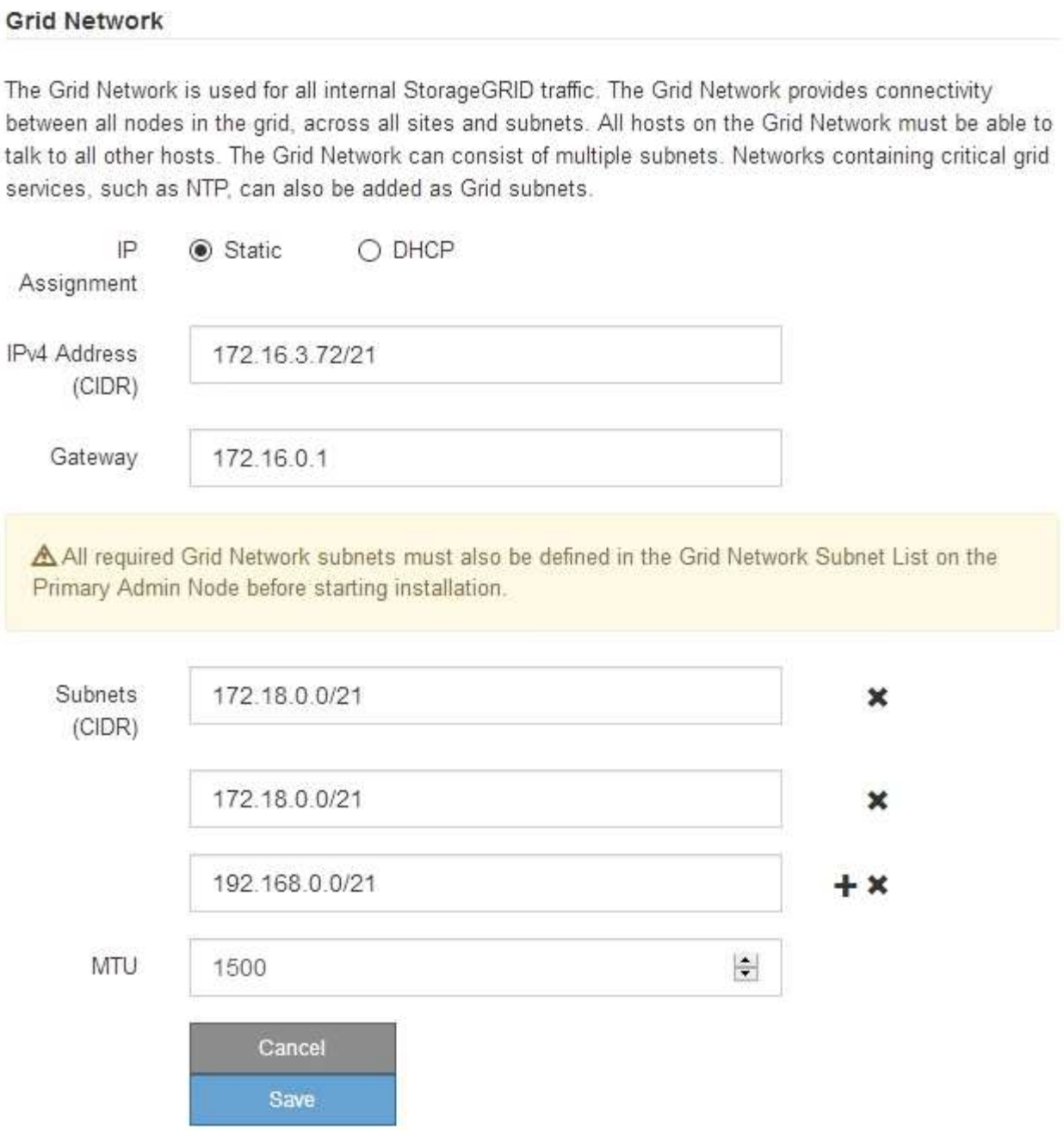
Change IP(IP 변경) 도구를 사용하여 이러한 설정에 액세스할 수 없는 경우 유지보수 모드를 사용하여 MTU 설정을 변경합니다.

필요한 것

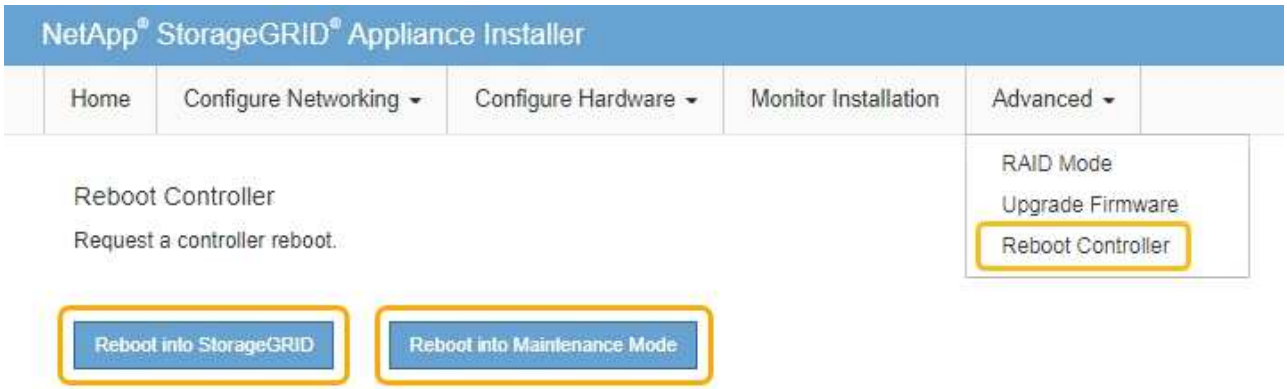
제품이 다 되었습니다 유지보수 모드로 전환되었습니다.

단계

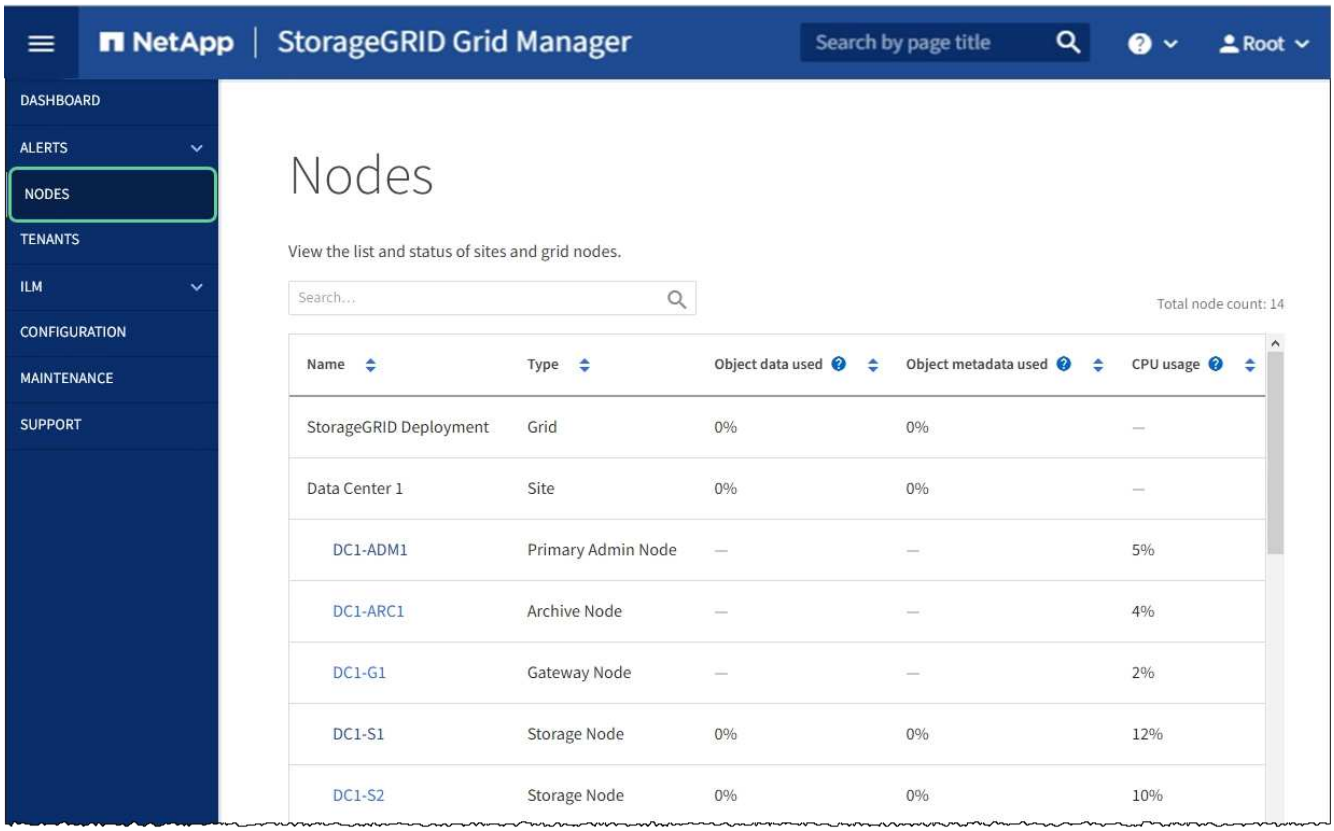
1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * IP 구성 * 을 선택합니다.
2. 그리드 네트워크, 관리자 네트워크 및 클라이언트 네트워크에 대한 MTU 설정을 원하는 대로 변경합니다.



3. 설정이 만족스러우면 * 저장 * 을 선택합니다.
4. 이 절차가 성공적으로 완료되었고 노드가 유지보수 모드일 때 수행할 추가 절차가 있는 경우 지금 수행합니다. 작업을 완료했거나 오류가 발생하여 다시 시작하려면 * 고급 * > * 컨트롤러 재부팅 * 을 선택하고 다음 옵션 중 하나를 선택합니다.
    - StorageGRID * 로 재부팅 * 을 선택합니다
    - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. 절차 중에 오류가 발생하여 다시 시작하려면 이 옵션을 선택합니다. 노드가 유지보수 모드로 재부팅된 후 장애가 발생한 절차의 적절한 단계에서 다시 시작하십시오.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

StorageGRID 관리

DNS 서버 구성을 확인합니다

이 어플라이언스 노드에서 현재 사용 중인 DNS(Domain Name System) 서버를 확인하고 일시적으로 변경할 수 있습니다.

필요한 것

제품이 다 되었습니다 유지보수 모드로 전환되었습니다.

이 작업에 대해

KMS의 호스트 이름이 IP 주소 대신 도메인 이름으로 지정되었기 때문에 암호화된 어플라이언스가 KMS(키 관리 서버) 또는 KMS 클러스터에 연결할 수 없는 경우 DNS 서버 설정을 변경해야 할 수 있습니다. 어플라이언스에 대한 DNS 설정에 대한 모든 변경 사항은 일시적이며 유지 관리 모드를 종료할 때 손실됩니다. 이러한 변경 사항을 영구적으로 적용하려면 Grid Manager(* 유지 관리 * > * 네트워크 * > * DNS 서버 *)에서 DNS 서버를 지정합니다.

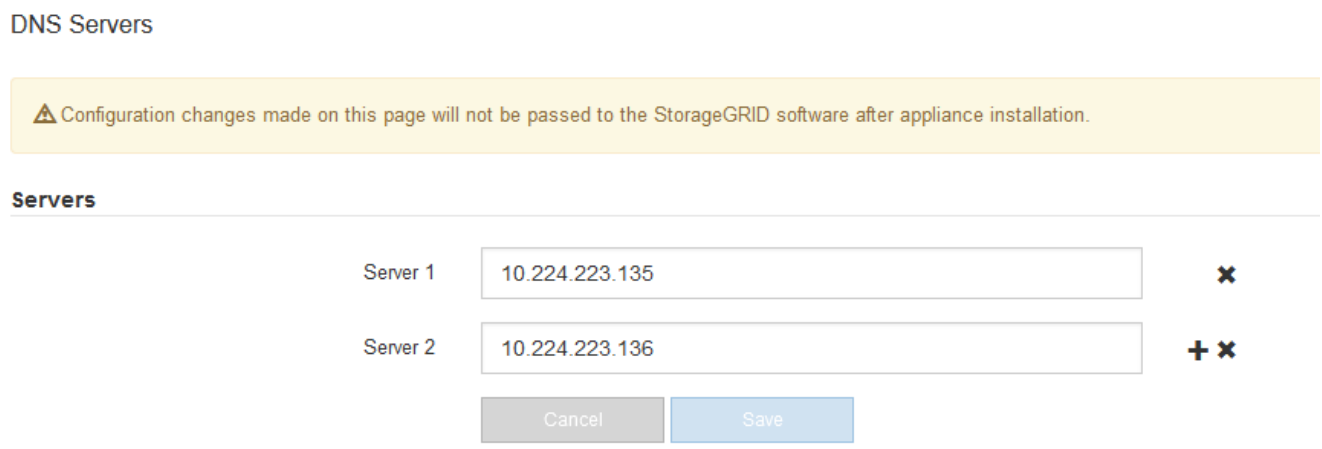
- KMS 서버가 호스트 이름에 대해 IP 주소 대신 정규화된 도메인 이름을 사용하여 정의된 노드 암호화 어플라이언스인 경우에만 DNS 구성을 일시적으로 변경해야 합니다.
- 노드 암호화 어플라이언스가 도메인 이름을 사용하여 KMS에 연결되는 경우 그리드에 정의된 DNS 서버 중 하나에 연결해야 합니다. 그런 다음 이러한 DNS 서버 중 하나가 도메인 이름을 IP 주소로 변환합니다.
- 노드가 그리드의 DNS 서버에 연결할 수 없거나 노드 암호화 어플라이언스 노드가 오프라인일 때 그리드 전체 DNS 설정을 변경한 경우 노드가 KMS에 연결할 수 없습니다. DNS 문제가 해결될 때까지 어플라이언스에 있는 암호화된 데이터를 해독할 수 없습니다.

KMS 연결을 방해하는 DNS 문제를 해결하려면 StorageGRID 어플라이언스 설치 프로그램에서 하나 이상의 DNS 서버의 IP 주소를 지정하십시오. 이러한 임시 DNS 설정을 사용하면 어플라이언스가 KMS에 연결하고 노드의 데이터를 해독할 수 있습니다.

예를 들어, 암호화된 노드가 오프라인 상태일 때 그리드의 DNS 서버가 변경되면 노드가 다시 온라인 상태가 될 때 KMS에 도달할 수 없습니다. KMS는 이전 DNS 값을 계속 사용하고 있기 때문입니다. StorageGRID 어플라이언스 설치 프로그램에 새 DNS 서버 IP 주소를 입력하면 임시 KMS 연결을 통해 노드 데이터를 해독할 수 있습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * DNS 구성 * 을 선택합니다.
2. 지정된 DNS 서버가 올바른지 확인합니다.



3. 필요한 경우 DNS 서버를 변경합니다.

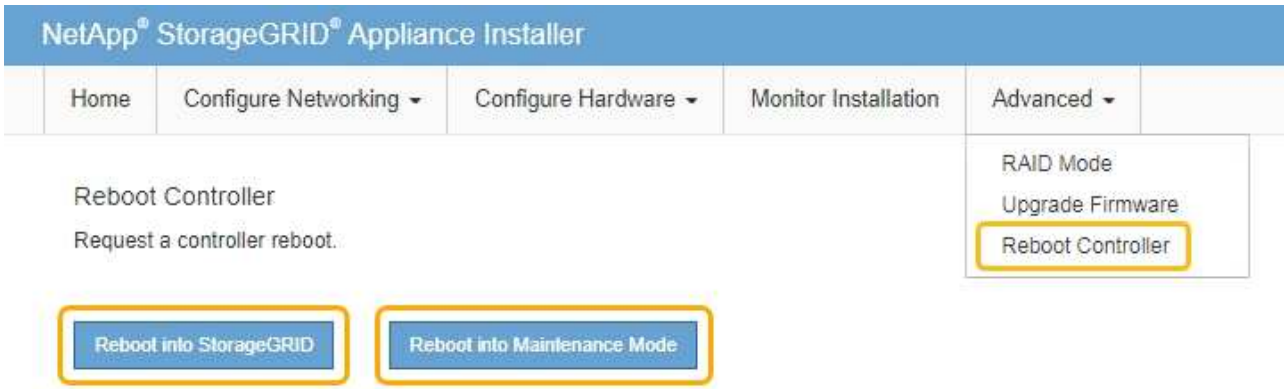
> DNS 설정에 대한 변경 사항은 일시적이며 유지 관리 모드를 종료할 때 손실됩니다.

4. 임시 DNS 설정이 만족스러우면 * Save * 를 선택합니다.

노드는 이 페이지에 지정된 DNS 서버 설정을 사용하여 KMS에 다시 연결하여 노드의 데이터를 해독할 수 있도록 합니다.

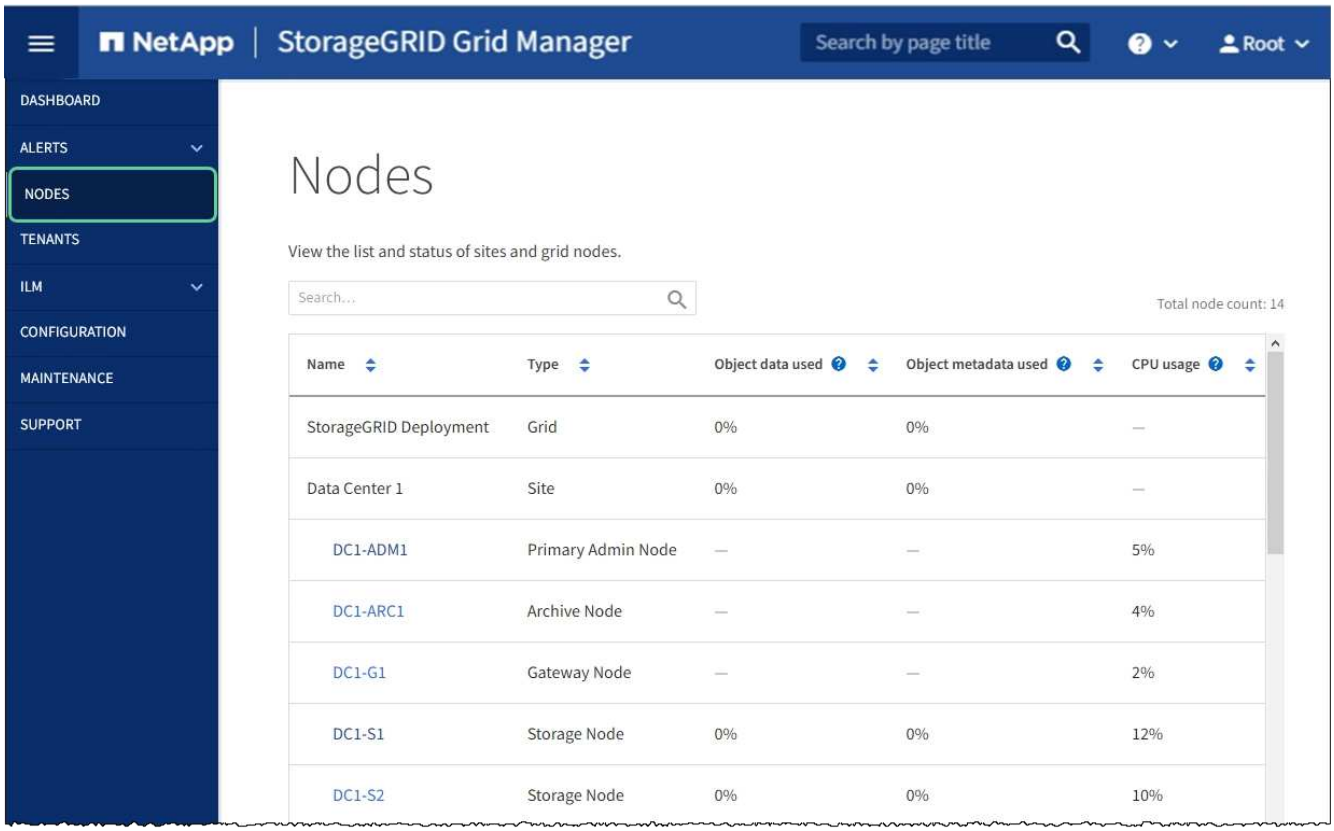
5. 노드 데이터가 해독된 후 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.

   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



> 노드가 재부팅되고 그리드에 다시 연결되면 Grid Manager에 나열된 시스템 전체 DNS 서버가 사용됩니다. 그리드를 다시 연결한 후 어플라이언스는 어플라이언스가 유지보수 모드일 때 StorageGRID 어플라이언스 설치 프로그램에 지정된 임시 DNS 서버를 더 이상 사용하지 않습니다.

어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



유지보수 모드에서 노드 암호화 모니터링**(SG5700)**

설치 중에 어플라이언스에 대한 노드 암호화를 활성화한 경우 노드 암호화 상태 및 키 관리 서버(KMS) 세부 정보를 포함하여 각 어플라이언스 노드의 노드 암호화 상태를 모니터링할 수 있습니다.

필요한 것

- 설치하는 동안 어플라이언스에 대해 노드 암호화가 활성화되어 있어야 합니다. 어플라이언스를 설치한 후에는 노드 암호화를 활성화할 수 없습니다.
- 제품이 다 되었습니다 유지보수 모드로 전환됩니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption ☑

Save

Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate >

Client certificate >

Clear KMS Key

Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

노드 암호화 페이지에는 다음 세 가지 섹션이 있습니다.

- 암호화 상태 는 어플라이언스에 대해 노드 암호화가 활성화되었는지 여부를 표시합니다.
- 키 관리 서버 세부 정보 는 어플라이언스를 암호화하는 데 사용되는 KMS에 대한 정보를 보여 줍니다. 서버 및 클라이언트 인증서 섹션을 확장하여 인증서 세부 정보 및 상태를 볼 수 있습니다.
  - 만료된 인증서 갱신과 같은 인증서 자체의 문제를 해결하려면 StorageGRID 관리 지침의 KMS 정보를 참조하십시오.
  - KMS 호스트에 연결할 때 예기치 않은 문제가 발생하는 경우 DNS(Domain Name System) 서버가 올바르고 어플라이언스 네트워킹이 올바르게 구성되었는지 확인합니다.

    DNS 서버 구성을 확인합니다

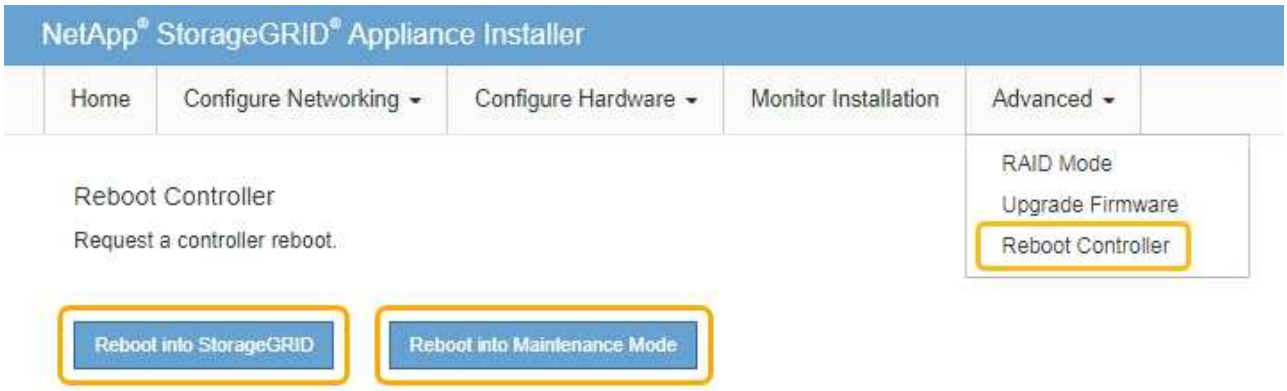
  - 인증서 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.
- KMS 키 지우기(Clear KMS Key)는 어플라이언스에 대한 노드 암호화를 해제하고, StorageGRID 사이트에 구성된 키 관리 서버와 어플라이언스를 제거하고, 어플라이언스에서 모든 데이터를 삭제합니다. KMS 키를

지워야 제품을 다른 StorageGRID 시스템에 설치할 수 있습니다.

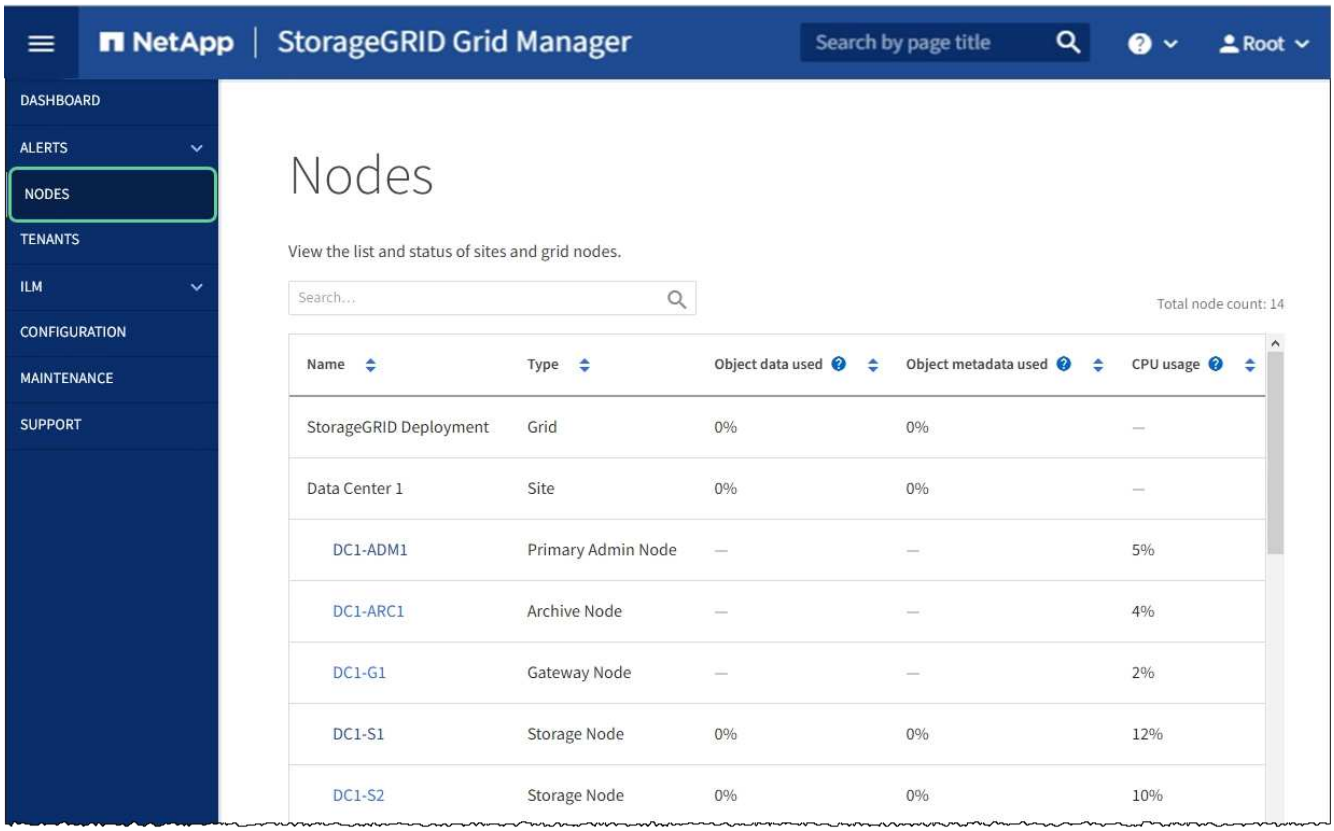
키 관리 서버 구성을 지웁니다

> KMS 구성을 지우면 어플라이언스에서 데이터가 삭제되어 영구적으로 액세스할 수 없게 됩니다. 이 데이터는 복구할 수 없습니다.

2. 노드 암호화 상태 확인을 마쳤으면 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.
   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

StorageGRID 관리

키 관리 서버 구성을 지웁니다

KMS(키 관리 서버) 구성을 지우면 어플라이언스에서 노드 암호화가 비활성화됩니다. KMS 구성을 삭제한 후에는 어플라이언스의 데이터가 영구적으로 삭제되며 더 이상 액세스할 수 없습니다. 이 데이터는 복구할 수 없습니다.

필요한 것

어플라이언스의 데이터를 보존해야 하는 경우 KMS 구성을 지우기 전에 노드 서비스 해제 절차를 수행하거나 노드를 복제해야 합니다.

> KMS를 삭제하면 제품의 데이터가 영구적으로 삭제되고 더 이상 액세스할 수 없게 됩니다. 이 데이터는 복구할 수 없습니다.

노드 서비스 해제 포함된 데이터를 StorageGRID의 다른 노드로 이동하려면 다음을 사용합니다.

이 작업에 대해

어플라이언스 KMS 구성을 지우면 노드 암호화가 비활성화되므로 어플라이언스 노드와 StorageGRID 사이트의 KMS 구성 간의 연결이 제거됩니다. 그러면 어플라이언스의 데이터가 삭제되고 어플라이언스가 사전 설치 상태로 유지됩니다. 이 프로세스는 되돌릴 수 없습니다.

KMS 구성을 지워야 합니다.

- KMS를 사용하지 않거나 다른 KMS를 사용하는 다른 StorageGRID 시스템에 제품을 설치하기 전에

> 동일한 KMS 키를 사용하는 StorageGRID 시스템에 어플라이언스 노드를 재설치하려는 경우 KMS 구성을 지우지 마십시오.

- KMS 구성이 손실되고 KMS 키를 복구할 수 없는 노드를 복구 및 재설치할 수 있습니다.
- 이전에 현장에서 사용 중이던 제품을 반환하기 전에
- 노드 암호화가 설정된 어플라이언스를 서비스 해제 후

> KMS를 제거하기 전에 어플라이언스의 전원을 해제하여 StorageGRID 시스템의 다른 노드로 데이터를 이동합니다. KMS를 폐기하기 전에 제거하면 데이터가 손실되고 어플라이언스가 작동하지 않을 수 있습니다.

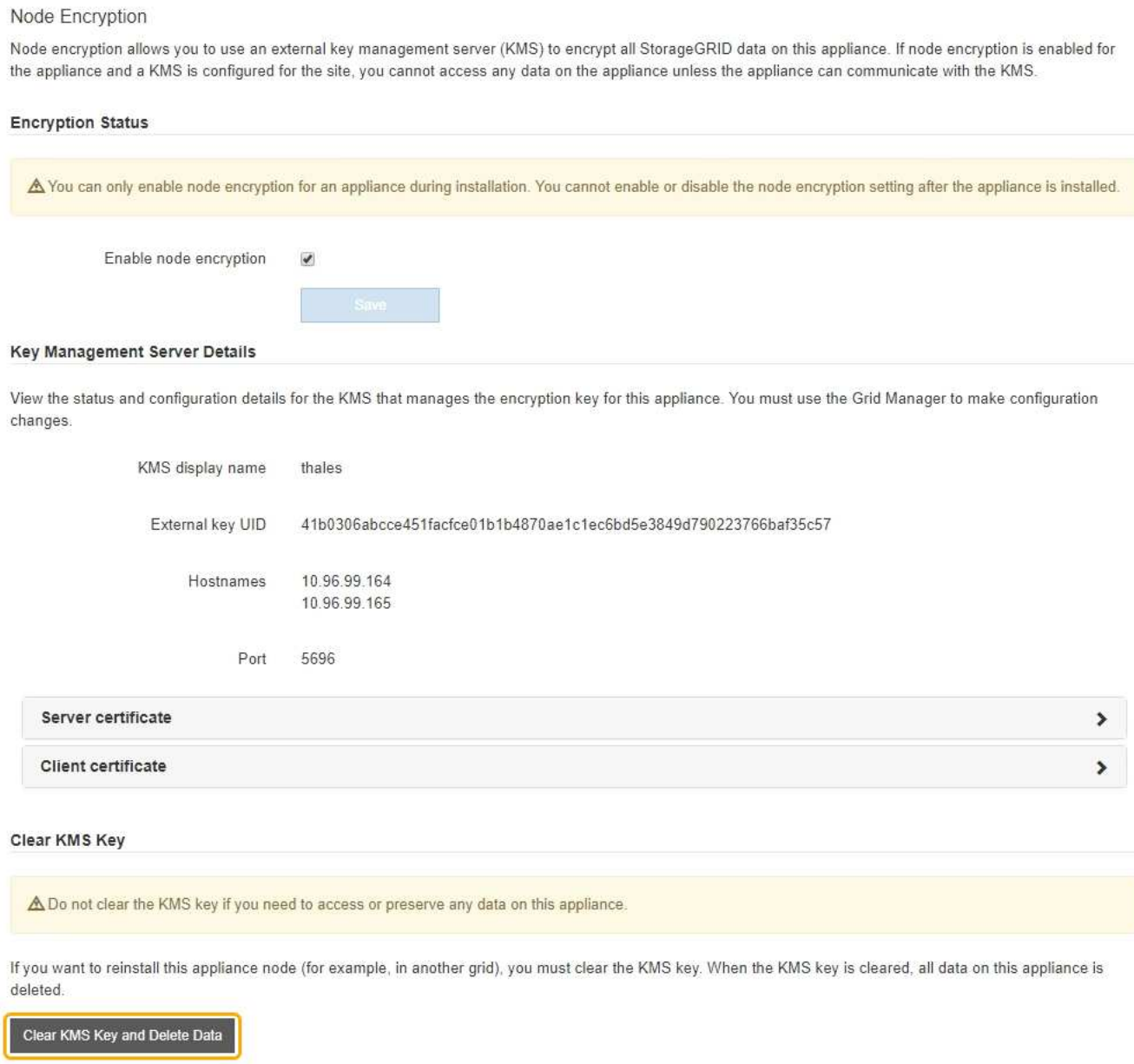
단계

1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

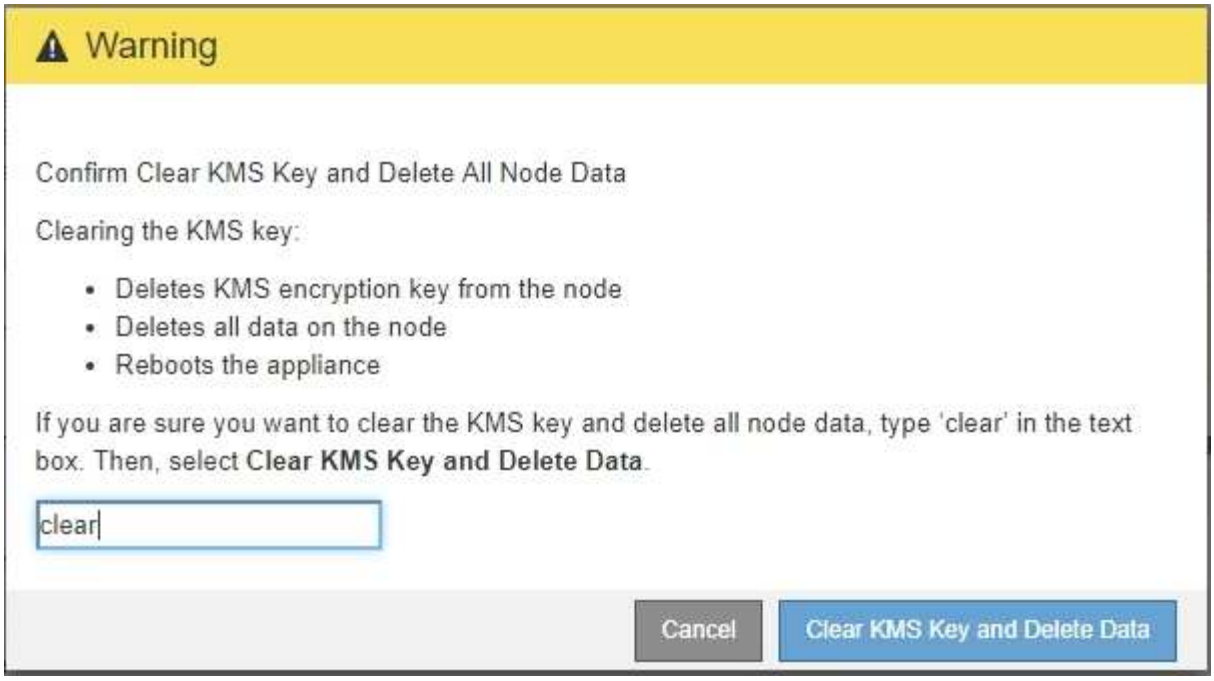
   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.



> KMS 구성이 삭제된 경우 어플라이언스의 데이터가 영구적으로 삭제됩니다. 이 데이터는 복구할 수 없습니다.

3. 창 아래쪽에서 * KMS 키 삭제 및 데이터 삭제 * 를 선택합니다.
4. KMS 구성을 지우려면 + " * clear * "+를 입력하고 * KMS 키 삭제 및 데이터 삭제 * 를 선택합니다.



KMS 암호화 키 및 모든 데이터가 노드에서 삭제되고 어플라이언스가 재부팅됩니다. 이 작업은 최대 20분이 소요될 수 있습니다.

5. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

6. 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.
7. 노드 암호화가 비활성화되었으며 * 키 관리 서버 세부 정보 * 및 * KMS 키 지우기 및 데이터 삭제 * 컨트롤의 키 및 인증서 정보가 창에서 제거되었는지 확인합니다.

   그리드에 다시 설치할 때까지 어플라이언스에서 노드 암호화를 다시 활성화할 수 없습니다.

작업을 마친 후

어플라이언스가 재부팅되고 KMS가 삭제되었으며 사전 설치 상태의 제품이 검증된 경우 StorageGRID 시스템에서 어플라이언스를 물리적으로 제거할 수 있습니다. 에 대한 자세한 내용은 복구 및 유지 관리 지침을 참조하십시오 어플라이언스 재설치를 준비합니다.

관련 정보

StorageGRID 관리

SG5600 스토리지 어플라이언스

SG5600 어플라이언스: 개요

StorageGRID SG5600 어플라이언스는 StorageGRID 그리드에서 스토리지 노드로 작동하는

통합 스토리지 및 컴퓨팅 플랫폼입니다.

StorageGRID SG5600 어플라이언스에는 다음과 같은 구성 요소가 포함되어 있습니다.

구성 요소	설명
E5500SG 컨트롤러	컴퓨팅 서버E5600SG 컨트롤러는 Linux 운영 체제와 StorageGRID 소프트웨어를 실행합니다. 이 컨트롤러는 다음 장치에 연결됩니다. • StorageGRID 시스템용 관리자, 그리드 및 클라이언트 네트워크 • E2700은 이중 SAS 경로(액티브/액티브)를 사용하며, E54600SG 컨트롤러를 이니시에이터로 작동합니다
E2700 컨트롤러	스토리지 컨트롤러E2700 컨트롤러는 표준 E-Series 스토리지 어레이로 작동하며 SANtricity 운영 체제(컨트롤러 펌웨어)를 실행합니다. 이 컨트롤러는 다음 장치에 연결됩니다. • SANtricity 스토리지 관리자가 설치된 관리 네트워크입니다 • E5500SG 컨트롤러, 이중 SAS 경로(액티브/액티브)를 사용하고 E2700 컨트롤러가 대상으로 작동

SG5600 어플라이언스에는 모델에 따라 다음과 같은 구성 요소도 포함되어 있습니다.

구성 요소	모델 **SG5612**	모델 **SG5660**
드라이브	NL-SAS 드라이브 12개	NL-SAS 드라이브 60개
엔클로저	DE1600 엔클로저 - 드라이브와 컨트롤러가 장착된 2개의 랙 유닛(2U) 섀시	DE6600 엔클로저, 드라이브와 컨트롤러가 장착된 4개의 랙 유닛(4U) 섀시
전원 공급 장치 및 팬	2개의 전원 팬 캐니스터	전원 공급 장치 2개 및 팬 2개

> E5500SG 컨트롤러는 StorageGRID 어플라이언스에 사용할 수 있도록 고도로 커스터마이징되었습니다. 다른 모든 구성 요소는 E-Series 문서에 설명된 대로 작동합니다. 단, 이러한 지침 에는 나와 있습니다.

각 StorageGRID 어플라이언스 스토리지 노드에서 사용할 수 있는 최대 기본 스토리지는 어플라이언스 모델 및 구성에 따라 고정됩니다. 쉘프를 추가하려면 드라이브를 추가할 때 사용 가능한 스토리지를 확장할 수 없습니다.

StorageGRID 어플라이언스 기능

StorageGRID SG5600 어플라이언스는 새로운 StorageGRID 시스템을 구축하거나 기존 시스템의 용량을 확장하기 위한 통합 스토리지 솔루션을 제공합니다.

StorageGRID 어플라이언스는 다음과 같은 기능을 제공합니다.

- StorageGRID 스토리지 노드 컴퓨팅 및 스토리지 요소를 효율적이고 통합된 단일 솔루션으로 결합합니다
- 스토리지 노드의 설치 및 구성을 단순화하여 필요한 대부분의 프로세스를 자동화합니다
- 2개의 엔클로저 옵션이 포함된 고밀도 스토리지 솔루션을 제공합니다. 하나는 2U이고 다른 하나는 4U입니다
- FC 또는 iSCSI와 같은 중간 스토리지 인터페이스가 필요 없이 스토리지 노드에 직접 10GbE IP 인터페이스를 사용합니다
- StorageGRID 어플라이언스 및 가상(소프트웨어 기반) 스토리지 노드를 사용하는 하이브리드 그리드 환경에서 사용할 수 있습니다
- 사전 구성된 스토리지가 포함되어 있으며 현장에서 즉시 사용할 수 있는 소프트웨어 배포 및 통합을 위해 StorageGRID 어플라이언스 설치 프로그램(E5500SG 컨트롤러)과 함께 사전 설치됩니다

하드웨어 다이어그램

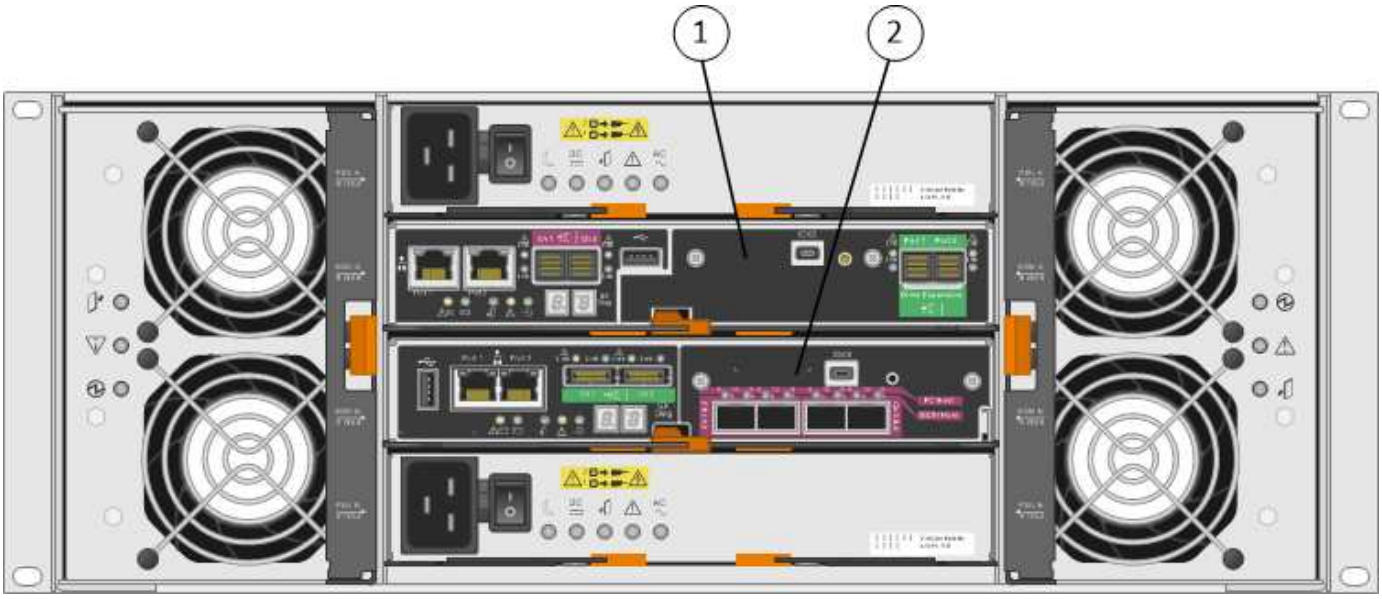
SG5612 및 SG5660 모델의 StorageGRID 어플라이언스 모델은 모두 E2700 컨트롤러와 E5500SG 컨트롤러를 포함합니다. 다이어그램을 검토하여 모델과 컨트롤러 간의 차이점을 확인해야 합니다.

모델 **SG5612 2U: E2700** 컨트롤러 및 **E5500SG** 컨트롤러 후면

속성 표시기	설명
1	E2700 컨트롤러
2	E5500SG 컨트롤러

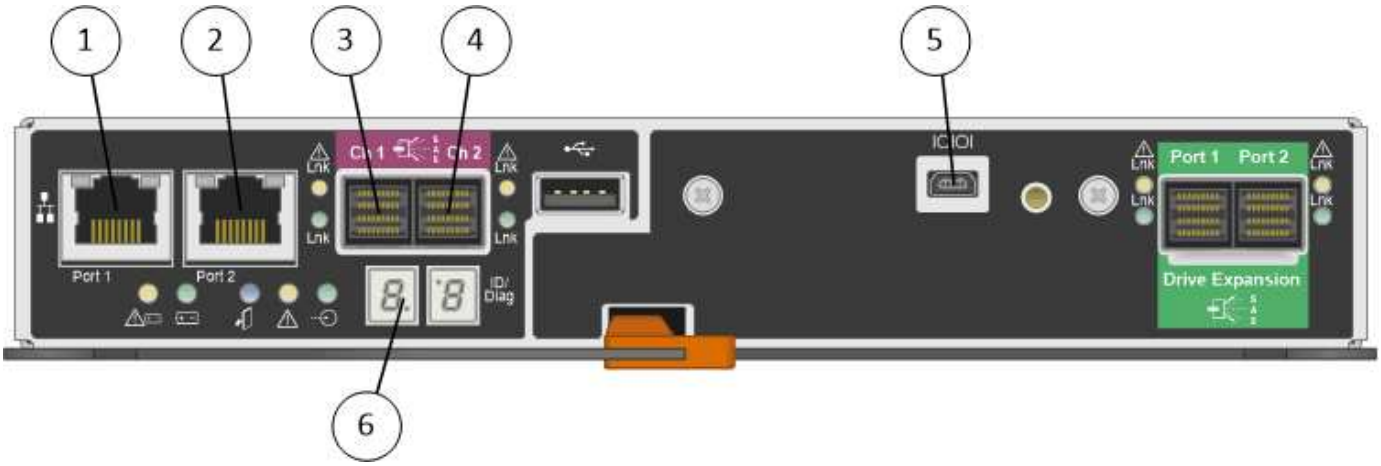
모델 **SG5660 4U: E2700** 컨트롤러 및 **E5500SG** 컨트롤러 후면

E2700 컨트롤러가 E5500SG 컨트롤러 위에 있습니다.



속성 표시기	설명
1	E2700 컨트롤러
2	E5500SG 컨트롤러

E2700 컨트롤러 후면

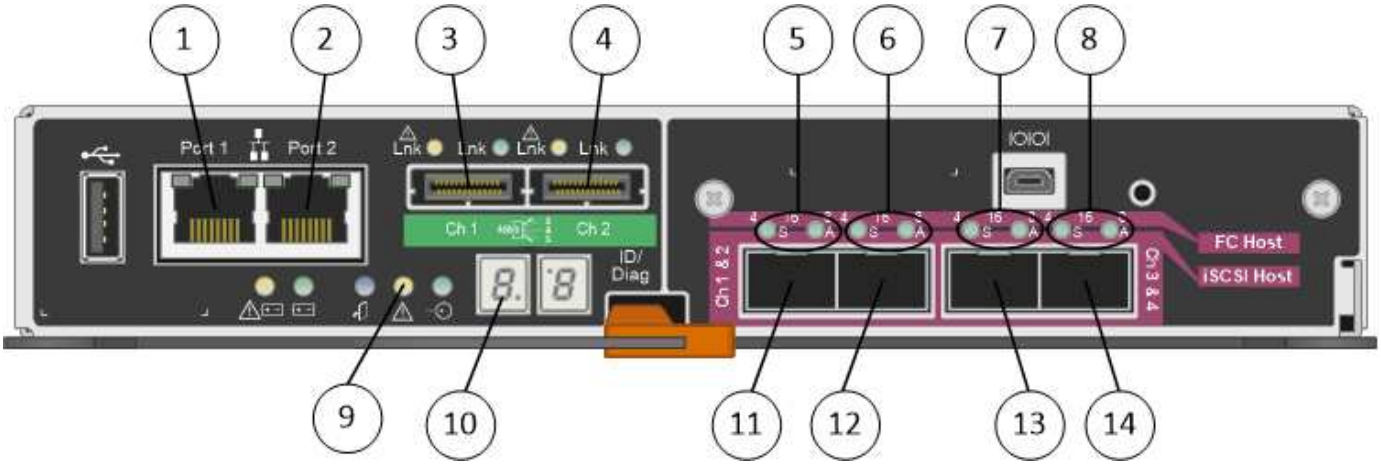


속성 표시기	설명
1	관리 포트 1(SANtricity 저장소 관리자가 설치된 네트워크에 연결)
2	관리 포트 2(설치 중에 노트북에 연결하는 데 사용)
3	SAS 인터커넥트 포트 1
4	SAS 인터커넥트 포트 2

속성 표시기	설명
5	직렬 연결 포트
6	7개 세그먼트 디스플레이

E2700 컨트롤러 후면의 드라이브 확장(녹색) SAS 포트 2개는 사용되지 않습니다. StorageGRID 어플라이언스는 확장 드라이브 쉘프를 지원하지 않습니다.

E5500SG 컨트롤러 후면



속성 표시기	설명
1	관리 포트 1 StorageGRID용 관리 네트워크에 연결합니다.
2	관리 포트 2 옵션: • StorageGRID용 관리 네트워크에 대한 중복 연결을 위해 관리 포트 1과 연결합니다. • 유선을 해제하고 임시 로컬 액세스(IP 169.254.0.1)를 위해 사용 가능한 상태로 둡니다. • 설치하는 동안 DHCP 할당 IP 주소를 사용할 수 없는 경우 IP 구성에 를 사용합니다.
3	SAS 인터커넥트 포트 1
4	SAS 인터커넥트 포트 2
5	10GbE 네트워크 포트 1의 장애 및 활성 상태 표시등
6	10GbE 네트워크 포트 2의 장애 및 활성 상태 표시등

속성 표시기	설명
7	10GbE 네트워크 포트 3의 장애 및 활성 상태 표시등
8	10GbE 네트워크 포트 4의 장애 및 활성 상태 표시등
9	주의 LED가 필요합니다
10	7개 세그먼트 디스플레이
11	10GbE 네트워크 포트 1
12	10GbE 네트워크 포트 2
13	10GbE 네트워크 포트 3
14	10GbE 네트워크 포트 4

StorageGRID 어플라이언스 E5500SG 컨트롤러의 호스트 인터페이스 카드(HIC)는 10Gb 이더넷 연결만 지원합니다. iSCSI 연결에는 사용할 수 없습니다.

설치 및 구축 개요

StorageGRID를 처음 구축할 때 하나 이상의 StorageGRID 어플라이언스를 설치하거나 나중에 확장을 위해 어플라이언스 스토리지 노드를 추가할 수 있습니다. 복구 작업의 일부로 어플라이언스 스토리지 노드를 설치해야 할 수도 있습니다.

StorageGRID 스토리지 어플라이언스를 StorageGRID 시스템에 추가하는 작업은 다음과 같은 네 가지 주요 단계로 이루어집니다.

1. 설치 준비:
    - 설치 사이트 준비 중
    - 박스 포장 풀기 및 내용물 확인
    - 추가 장비 및 도구 확보
    - IP 주소 및 네트워크 정보를 수집하는 중입니다
    - 선택 사항: 모든 어플라이언스 데이터를 암호화하려는 경우 외부 키 관리 서버(KMS) 구성 StorageGRID 관리 지침에 있는 외부 키 관리에 대한 자세한 내용을 참조하십시오.
2. 하드웨어 설치:
    - 하드웨어를 등록하는 중입니다
    - 캐비닛 또는 랙에 제품 설치
    - 드라이브 설치(SG5660만 해당)
    - 어플라이언스 케이블 연결

- 전원 코드 연결 및 전원 공급
- 부팅 상태 코드 보기

3. 하드웨어 구성:
   - SANtricity 스토리지 관리자에 액세스하고, E2700 컨트롤러에서 관리 포트 1의 정적 IP 주소를 설정하고 SANtricity 스토리지 관리자 설정을 구성합니다
   - StorageGRID 어플라이언스 설치 프로그램에 액세스하고 StorageGRID 네트워크에 연결하는 데 필요한 링크 및 네트워크 IP 설정을 구성합니다
   - 선택 사항: 외부 KMS를 사용하여 어플라이언스 데이터를 암호화하려는 경우 노드 암호화 사용
   - 선택 사항: RAID 모드 변경
4. 어플라이언스를 스토리지 노드로 구축:

작업	을 참조하십시오
새로운 StorageGRID 시스템에 어플라이언스 스토리지 노드 구축	어플라이언스 스토리지 노드 구축
기존 StorageGRID 시스템에 어플라이언스 스토리지 노드 추가	StorageGRID 시스템 확장을 위한 지침
스토리지 노드 복구 작업의 일부로 어플라이언스 스토리지 노드 구축	복구 및 유지 관리 지침

관련 정보

설치 준비(SG5600)

하드웨어 설치(SG5600)

하드웨어 구성(SG5600)

그리드를 확장합니다

복구 및 유지 관리

StorageGRID 관리

설치 준비(SG5600)

StorageGRID 어플라이언스 설치를 준비하는 과정에서 사이트 준비 및 필요한 모든 하드웨어, 케이블 및 도구 확보 작업이 수반됩니다. 또한 IP 주소와 네트워크 정보도 수집해야 합니다.

관련 정보

웹 브라우저 요구 사항

사이트 준비**(SG5600)**

제품을 설치하기 전에 StorageGRID 어플라이언스의 사양을 충족하는 사이트와 캐비닛 또는 랙이 맞는지 확인해야 합니다.

단계

1. 사이트가 온도, 습도, 고도 범위, 공기 흐름, 열 손실 요구 사항을 충족하는지 확인합니다. 배선, 전원 및 접지. 자세한 내용은 NetApp Hardware Universe를 참조하십시오.
2. 이 크기의 선반에 맞게 19인치(48.3-cm) 캐비닛 또는 랙을 준비합니다(케이블 제외).

어플라이언스 모델	높이	너비	깊이	최대 중량
SG5612 (12개 드라이브)	3.40in. (8.64cm)	19.0인치 (48.26cm)	21.75in. (55.25cm)	59.5lb (27kg)
SG5660 (60개 드라이브)	7.00인치 (17.78cm)	17.75인치 (45.08cm)	32.50in. (82.55cm)	2,36.2lb. (107.1kg)

3. 필요한 네트워크 스위치를 설치합니다. 호환성 정보는 NetApp 상호 운용성 매트릭스 툴을 참조하십시오.

관련 정보

"NetApp Hardware Universe를 참조하십시오"

"NetApp 상호 운용성"

박스 포장 풀기**(SG5600)**

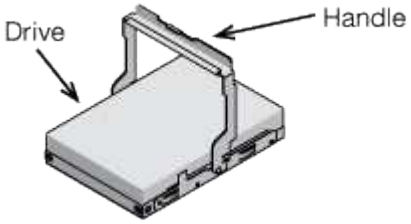
StorageGRID 제품을 설치하기 전에 모든 상자의 포장을 풀고 내용물을 포장 명세서에 있는 품목과 비교합니다.

- * SG5660 엔클로저, 60개 드라이브로 구성된 4U 섀시 *

- * SG5612 엔클로저, 12개 드라이브를 지원하는 2U 섀시 *

- * 4U 베젤 또는 2U 엔드캡 *

- NL-SAS 드라이브 *



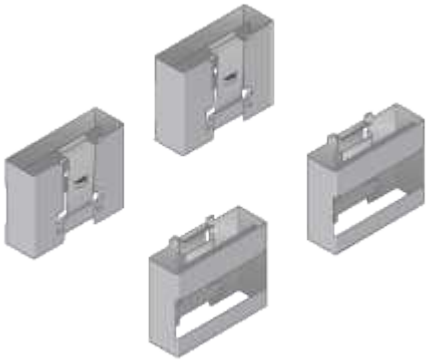
2U SG5612에 드라이브가 사전 설치되어 있지만 4U SG5660에서는 배송 안전을 위해 드라이브를 사용할 수 없습니다.

- * E5500SG 컨트롤러 *

- * E2700 컨트롤러 *

- * 장착 레일 및 나사 *

- * 엔클로저 핸들(4U 엔클로저만) *



케이블 및 커넥터

StorageGRID 어플라이언스에는 다음과 같은 케이블 및 커넥터가 포함되어 있습니다.

- * 해당 국가의 전원 코드 *

본 제품은 벽면 플러그와 같은 외부 전원에 연결하기 위한 AC 전원 코드 2개가 함께 제공됩니다. 캐비닛에는 제품과 함께 제공된 전원 코드 대신 사용하는 특수 전원 코드가 있을 수 있습니다.

- SAS 인터커넥트 케이블 *

미니 SAS-HD 및 미니 SAS 커넥터가 있는 0.5미터 SAS 상호 연결 케이블 2개.

사각형 커넥터는 E2700 컨트롤러에 연결되며 직사각형 커넥터는 E5600SG 컨트롤러에 연결합니다.

추가 장비 및 툴 확보**(SG5600)**

SG5600 어플라이언스를 설치하기 전에 필요한 추가 장비 및 툴이 모두 있는지 확인하십시오.

- * 스크류드라이버 *

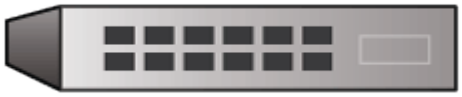
필립스 번호 2 드라이버

중형 일자 스크루드라이버

- * ESD 손목 스트랩 *

- * 이더넷 케이블 *

- * 이더넷 스위치 *



- * 서비스 노트북 *지원되는 웹 브라우저

서비스 랩톱 요구 사항

StorageGRID 어플라이언스 하드웨어를 설치하기 전에 서비스 랩톱에 필요한 최소 리소스가 있는지 확인해야 합니다.

하드웨어 설치에 필요한 서비스 랩톱은 다음 요구 사항을 충족해야 합니다.

- Microsoft Windows 운영 체제
- 네트워크 포트
- 지원되는 웹 브라우저
- NetApp SANtricity 스토리지 관리자 버전 11.40 이상
- SSH 클라이언트(예: PuTTY)

관련 정보

웹 브라우저 요구 사항

"NetApp 문서: SANtricity 스토리지 관리자"

어플라이언스 네트워크 연결 검토**(SG5600)**

StorageGRID 어플라이언스를 설치하기 전에 어플라이언스에 연결할 수 있는 네트워크와 각 컨트롤러의 포트가 어떻게 사용되는지 이해해야 합니다.

StorageGRID 어플라이언스 네트워크

StorageGRID 어플라이언스를 스토리지 노드로 구축할 경우 다음 네트워크에 연결할 수 있습니다.

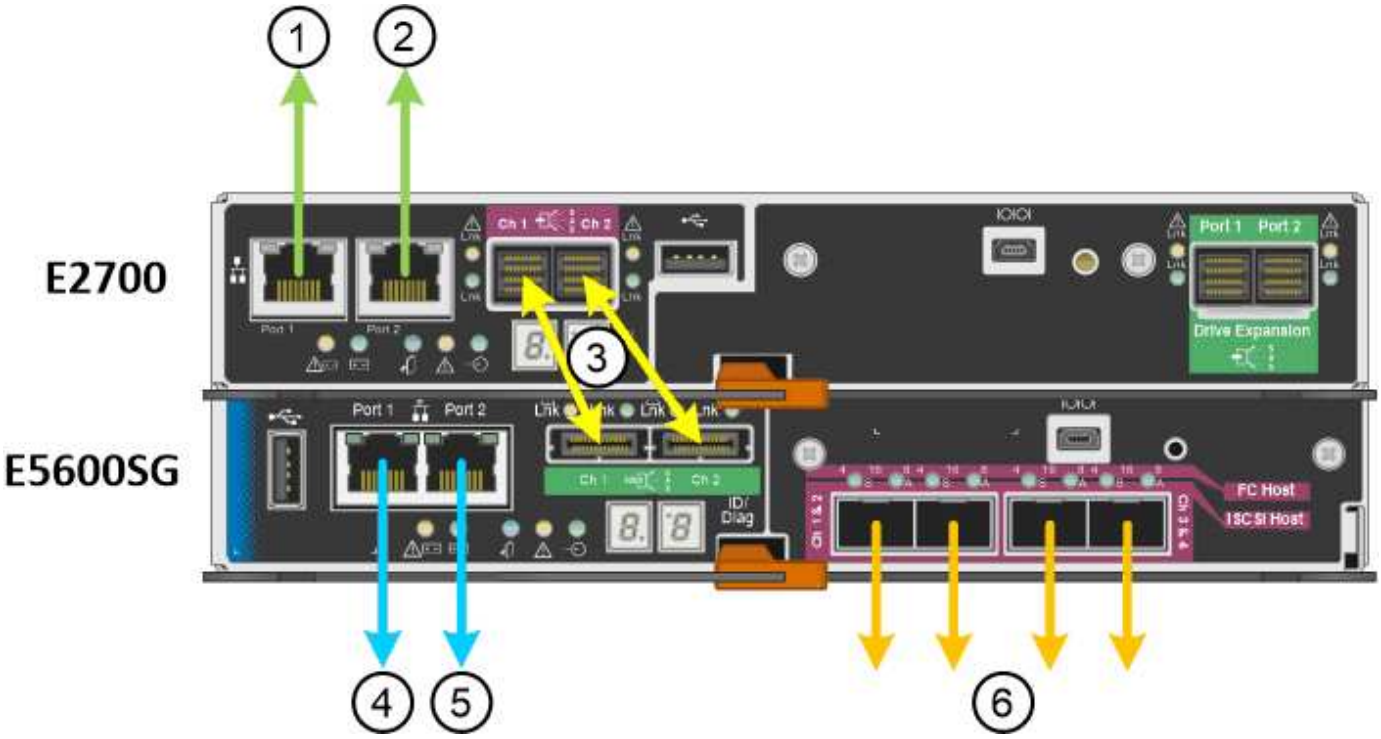
- * StorageGRID * 용 그리드 네트워크: 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용됩니다. 그리드에서 모든 사이트 및 서브넷의 모든 노드 간에 연결을 제공합니다. 그리드 네트워크가 필요합니다.
- StorageGRID*용 관리자 네트워크: 관리자 네트워크는 시스템 관리 및 유지 보수에 사용되는 폐쇄된 네트워크입니다. 관리 네트워크는 일반적으로 사설 네트워크이며 사이트 간에 라우팅할 필요가 없습니다. 관리 네트워크는 선택 사항입니다.
- * StorageGRID * 용 클라이언트 네트워크: 클라이언트 네트워크는 S3 및 Swift를 포함한 클라이언트 응용 프로그램에 대한 액세스를 제공하는 데 사용되는 개방형 네트워크입니다. 클라이언트 네트워크는 그리드에 대한 클라이언트 프로토콜 액세스를 제공하므로 그리드 네트워크를 격리하고 보호할 수 있습니다. 클라이언트 네트워크는 선택 사항입니다.
- * SANtricity 스토리지 관리자용 관리 네트워크 * (선택 사항): E2700 컨트롤러는 SANtricity 스토리지 관리자가 설치된 관리 네트워크에 연결되므로 어플라이언스의 하드웨어 구성요소를 모니터링하고 관리할 수 있습니다. 이 관리 네트워크는 StorageGRID용 관리 네트워크와 같을 수도 있고 독립 관리 네트워크일 수도 있습니다.

  선택적 SANtricity 스토리지 관리자 네트워크가 연결되지 않은 경우 일부 SANtricity 기능을 사용하지 못할 수 있습니다.

> StorageGRID 네트워크에 대한 자세한 내용은 _Grid Primer_를 참조하십시오.

StorageGRID 어플라이언스 연결부

StorageGRID 어플라이언스를 설치할 경우 두 컨트롤러를 서로 필요한 네트워크에 연결해야 합니다. 그림에서는 SG5660의 컨트롤러 2개를 보여 주며 E2700 컨트롤러는 상단, E5500SG 컨트롤러는 하단에 있습니다. SG5612에서 E2700 컨트롤러는 E5500SG 컨트롤러의 왼쪽에 있습니다.



항목	포트	포트의 유형입니다	기능
1	E2700 컨트롤러의 관리 포트 1	1Gb(RJ-45) 이더넷	SANtricity Storage Manager가 설치된 네트워크에 E2700 컨트롤러를 연결합니다.
2	E2700 컨트롤러의 관리 포트 2	1Gb(RJ-45) 이더넷	설치 중에 서비스 랩톱에 E2700 컨트롤러를 연결합니다.
3	각 컨트롤러에 Ch 1 및 Ch 2 라고 표시된 2개의 SAS 상호 연결 포트	E2700 컨트롤러: mini-SAS-HD E5500SG 컨트롤러: 미니 SAS	두 컨트롤러를 서로 연결합니다.
4	E5500SG 컨트롤러의 관리 포트 1	1Gb(RJ-45) 이더넷	StorageGRID용 관리 네트워크에 E5500SG 컨트롤러를 연결합니다.
5	E5500SG 컨트롤러의 관리 포트 2	1Gb(RJ-45) 이더넷	• 관리 네트워크에 대한 중복 연결을 원할 경우 관리 포트 1에 연결할 수 있습니다. • 유선을 해제하고 임시 로컬 액세스(IP 169.254.0.1)에 사용할 수 있습니다. • DHCP 할당 IP 주소를 사용할 수 없는 경우 설치 중에 E5500SG 컨트롤러를 서비스 랩톱에 연결하는 데 사용할 수 있습니다.
6	E5500SG 컨트롤러의 네트워크 포트 4개	10GbE(광)	그리드 네트워크 및 StorageGRID용 클라이언트 네트워크에 연결합니다. ""E600SG 컨트롤러용 10GbE 포트 연결"을 참조하십시오.

관련 정보

E5500SG 컨트롤러 포트의 포트 연결 모드

설치 정보 수집(SG5600)

케이블 어플라이언스(SG5600)

네트워킹 지침

VMware를 설치합니다

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

Ubuntu 또는 Debian을 설치합니다

E5500SG 컨트롤러 포트의 포트 연결 모드

E5500SG 컨트롤러 포트에 대한 네트워크 링크를 구성할 때 그리드 네트워크 및 선택적 클라이언트 네트워크에 연결되는 10GbE 포트와 선택적 관리 네트워크에 연결되는 1GbE 관리 포트에 포트 결합을 사용할 수 있습니다. 포트 본딩을 사용하면 StorageGRID 네트워크와 어플라이언스 간에 중복 경로를 제공하여 데이터를 보호할 수 있습니다.

관련 정보

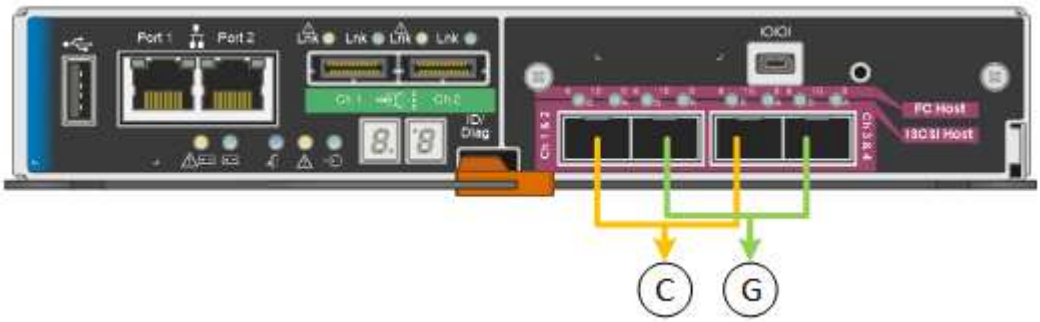
네트워크 링크 구성(SG5600)

10GbE 포트의 네트워크 연결 모드입니다

E5500SG 컨트롤러의 10GbE 네트워킹 포트는 그리드 네트워크 및 클라이언트 네트워크 연결을 위한 고정 포트 결합 모드 또는 애그리게이트 포트 결합 모드를 지원합니다.

고정 포트 결합 모드

고정 모드는 10GbE 네트워킹 포트의 기본 구성입니다.



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
c	이 네트워크를 사용하는 경우 포트 1과 3이 클라이언트 네트워크에 대해 함께 연결됩니다.
g	포트 2와 4는 그리드 네트워크를 위해 서로 연결되어 있습니다.

고정 포트 결합 모드를 사용할 때 포트는 액티브-백업 모드 또는 링크 통합 제어 프로토콜 모드(802.3ad)를 사용하여 본드 결합할 수 있습니다.

- 액티브-백업 모드(기본값)에서는 한 번에 하나의 포트만 활성화됩니다. 활성 포트에 장애가 발생하면 백업 포트가

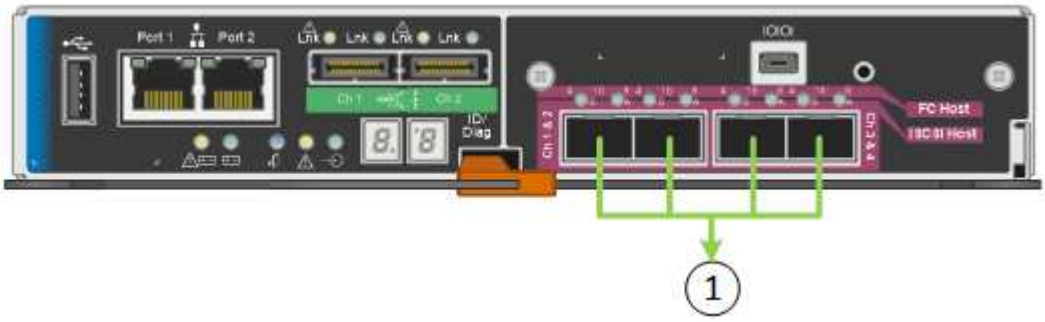
자동으로 페일오버 연결을 제공합니다. 포트 4는 포트 2(그리드 네트워크)에 대한 백업 경로를 제공하고 포트 3은 포트 1(클라이언트 네트워크)에 대한 백업 경로를 제공합니다.

- LACP 모드에서 각 포트 쌍은 컨트롤러와 네트워크 간에 논리 채널을 형성하므로 더 높은 처리량을 허용합니다. 한 포트에 장애가 발생해도 다른 포트는 계속 채널을 제공합니다. 처리량은 감소하지만 연결성은 영향을 받지 않습니다.

> 중복 연결이 필요하지 않은 경우 각 네트워크에 대해 하나의 포트만 사용할 수 있습니다. 그러나 StorageGRID가 설치된 후 그리드 관리자에서 경보가 발생하므로 케이블이 분리되었음을 나타냅니다. 이 알람을 안전하게 확인할 수 있습니다.

애그리게이트 포트 결합 모드

애그리게이트 포트 결합 모드는 각 StorageGRID 네트워크의 성능을 크게 높이고 추가 페일오버 경로를 제공합니다.



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
1	연결된 모든 포트는 단일 LACP 결합으로 그룹화되므로 모든 포트를 그리드 네트워크 및 클라이언트 네트워크 트래픽에 사용할 수 있습니다.

Aggregate 포트 결합 모드를 사용하려는 경우:

- LACP 네트워크 결합 모드를 사용해야 합니다.
- 각 네트워크에 대해 고유한 VLAN 태그를 지정해야 합니다. 이 VLAN 태그는 네트워크 트래픽이 올바른 네트워크로 라우팅되도록 각 네트워크 패킷에 추가됩니다.
- VLAN 및 LACP를 지원할 수 있는 스위치에 포트를 연결해야 합니다. LACP 결합에 여러 스위치가 사용되는 경우 스위치는 MLAG(Multi-Chassis Link Aggregation Group) 또는 이와 동등한 스위치를 지원해야 합니다.
- VLAN, LACP, MLAG 또는 이와 동등한 기능을 사용하도록 스위치를 구성하는 방법을 이해해야 합니다.

4개의 10GbE 포트를 모두 사용하지 않으려는 경우 1개, 2개 또는 3개의 포트를 사용할 수 있습니다. 두 개 이상의 포트를 사용하면 10GbE 포트 중 하나에 장애가 발생하더라도 일부 네트워크 연결이 계속 유지될 가능성을 극대화할 수 있습니다.

> 포트 수를 4개 이하로 선택하면 어플라이언스 노드가 설치된 후 그리드 관리자에서 * 서비스 어플라이언스 연결 해제 * 경고가 트리거되어 케이블이 분리되었음을 나타냅니다. 트리거된 경고에 대해 이 경고 규칙을 안전하게 비활성화할 수 있습니다. Grid Manager에서 * alerts * > * rules * 를 선택하고 규칙을 선택한 다음 * Edit rule * 을 클릭합니다. 그런 다음 * 사용 * 확인란의 선택을 취소합니다.

1GbE 관리 포트의 네트워크 연결 모드

E5500SG 컨트롤러에 있는 2개의 1GbE 관리 포트의 경우 독립 네트워크 연결 모드 또는 Active-Backup 네트워크 연결 모드를 선택하여 옵션 관리 네트워크에 연결할 수 있습니다.

독립 모드에서는 관리 포트 1만 관리 네트워크에 연결됩니다. 이 모드는 중복 경로를 제공하지 않습니다. 관리 포트 2는 유선으로 남겨두고 임시 로컬 연결에 사용할 수 있습니다(IP 주소 169.254.0.1 사용).

Active-Backup 모드에서는 관리 포트 1과 2가 모두 관리 네트워크에 연결됩니다. 한 번에 하나의 포트만 활성화됩니다. 활성 포트에 장애가 발생하면 백업 포트가 자동으로 페일오버 연결을 제공합니다. 이러한 두 개의 물리적 포트를 하나의 논리 관리 포트에 연결하면 관리 네트워크에 대한 중복 경로가 제공됩니다.

> 1GbE 관리 포트가 Active-Backup 모드로 구성되어 있을 때 E5500SG 컨트롤러에 임시로 로컬 연결해야 하는 경우, 두 관리 포트에서 케이블을 분리하고 임시 케이블을 관리 포트 2에 연결한 다음 IP 주소 169.254.0.1을 사용하여 어플라이언스에 액세스합니다.

설치 정보 수집**(SG5600)**

StorageGRID 어플라이언스를 설치 및 구성할 때 이더넷 스위치 포트, IP 주소, 포트 및 네트워크 연결 모드에 대한 정보를 결정하고 수집해야 합니다.

이 작업에 대해

다음 표를 사용하여 어플라이언스에 연결하는 각 네트워크에 대한 정보를 기록할 수 있습니다. 이러한 값은 하드웨어를 설치하고 구성하는 데 필요합니다.

E2700 컨트롤러를 **SANtricity** 스토리지 관리자에 연결하는 데 필요한 정보

SANtricity 스토리지 관리자에 사용할 관리 네트워크에 E2700 컨트롤러를 연결해야 합니다.

정보가 필요합니다	귀사의 가치
관리 포트 1에 연결할 이더넷 스위치 포트	
관리 포트 1의 MAC 주소(포트 P1 근처의 레이블에 인쇄되어 있음)	
전원을 켠 후 사용할 수 있는 경우 관리 포트 1에 대해 DHCP 할당 IP 주소입니다 • 참고: * E2700 컨트롤러에 연결할 네트워크에 DHCP 서버가 포함되어 있는 경우 네트워크 관리자는 MAC 주소를 사용하여 DHCP 서버가 할당한 IP 주소를 확인할 수 있습니다.	

정보가 필요합니다	귀사의 가치
속도 및 이중 모드 • 참고: * SANtricity 스토리지 관리자 관리 네트워크의 이더넷 스위치가 자동 교섭으로 설정되어 있는지 확인해야 합니다.	반드시: • 자동 협상(기본값)
IP 주소 형식입니다	다음 중 하나를 선택하십시오. • IPv4 • IPv6
관리 네트워크에서 어플라이언스에 사용할 고정 IP 주소입니다	IPv4의 경우: • IPv4 주소: • 서브넷 마스크: • 게이트웨이: IPv6의 경우: • IPv6 주소: • 라우팅 가능한 IP 주소: • E2700 컨트롤러 라우터 IP 주소:

관리 네트워크에 **E600SG** 컨트롤러를 연결하는 데 필요한 정보입니다

StorageGRID용 관리 네트워크는 시스템 관리 및 유지 보수에 사용되는 선택적 네트워크입니다. 어플라이언스는 E5500SG 컨트롤러의 1GbE 관리 포트를 사용하여 관리 네트워크에 연결됩니다.

정보가 필요합니다	귀사의 가치
관리자 네트워크가 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요 • 예(기본값)
네트워크 연결 모드	다음 중 하나를 선택하십시오. • 독립적입니다 • Active - 백업
관리 포트 1(P1)용 스위치 포트	

정보가 필요합니다	귀사의 가치
관리 포트 2용 스위치 포트(P2, Active-Backup 네트워크 연결 모드만 해당)	
관리 포트 1의 MAC 주소(포트 P1 근처의 레이블에 인쇄되어 있음)	
전원을 켠 후 사용할 수 있는 경우 관리 포트 1에 대해 DHCP 할당 IP 주소입니다 • 참고: * 관리 네트워크에 DHCP 서버가 포함된 경우, E5600SG 컨트롤러는 부팅 후 7개 세그먼트 디스플레이에 DHCP 할당 IP 주소를 표시합니다. MAC 주소를 사용하여 할당된 IP를 조회하여 DHCP 할당 IP 주소를 확인할 수도 있습니다.	• IPv4 주소(CIDR): • 게이트웨이:
관리 네트워크의 어플라이언스 스토리지 노드에 사용할 고정 IP 주소입니다 • 참고: * 네트워크에 게이트웨이가 없는 경우 게이트웨이에 대해 동일한 정적 IPv4 주소를 지정합니다.	• IPv4 주소(CIDR): • 게이트웨이:
관리 네트워크 서브넷(CIDR)	

E5500SG 컨트롤러에 **10GbE** 포트를 연결하고 구성하는 데 필요한 정보입니다

E5500SG 컨트롤러의 10GbE 포트 4개는 StorageGRID 그리드 네트워크 및 클라이언트 네트워크에 연결됩니다.

이러한 포트의 옵션에 대한 자세한 내용은 "E5500SG 컨트롤러의 10GbE 포트 연결"을 참조하십시오.

정보가 필요합니다	귀사의 가치
포트 결합 모드	다음 중 하나를 선택하십시오. • 고정(기본값) • 집계
포트 1용 스위치 포트(고정 모드용 클라이언트 네트워크)	
포트 2용 스위치 포트(고정 모드용 그리드 네트워크)	
포트 3용 스위치 포트(고정 모드용 클라이언트 네트워크)	
포트 4용 스위치 포트(고정 모드용 그리드 네트워크)	

E600SG 컨트롤러를 그리드 네트워크에 연결하는 데 필요한 정보입니다

StorageGRID용 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용되는 필수 네트워크입니다. 어플라이언스는 E5500SG 컨트롤러의 10GbE 포트를 사용하여 그리드 네트워크에 연결됩니다.

이러한 포트의 옵션에 대한 자세한 내용은 "E5500SG 컨트롤러의 10GbE 포트 연결"을 참조하십시오.

정보가 필요합니다	귀사의 가치
네트워크 연결 모드	다음 중 하나를 선택하십시오. • Active-Backup(기본값) • LACP(802.3ad)
VLAN 태그 지정이 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요(기본값) • 예
VLAN 태그(VLAN 태그 지정이 활성화된 경우)	0에서 4095 사이의 값을 입력합니다.
전원을 켠 후 사용할 수 있는 경우 그리드 네트워크에 대해 DHCP 할당 IP 주소입니다 • 참고: * 그리드 네트워크에 DHCP 서버가 포함된 경우, E5600SG 컨트롤러는 부팅된 후 7세그먼트 디스플레이에 그리드 네트워크에 대해 DHCP 할당 IP 주소를 표시합니다.	• IPv4 주소(CIDR): • 게이트웨이:
그리드 네트워크에서 어플라이언스 스토리지 노드에 사용할 고정 IP 주소입니다 • 참고: * 네트워크에 게이트웨이가 없는 경우 게이트웨이에 대해 동일한 정적 IPv4 주소를 지정합니다.	• IPv4 주소(CIDR): • 게이트웨이:
그리드 네트워크 서브넷(CIDR) • 참고: * 클라이언트 네트워크가 활성화되지 않은 경우 컨트롤러의 기본 라우트는 여기에 지정된 게이트웨이를 사용합니다.	

클라이언트 네트워크에 **E600SG** 컨트롤러를 연결하는 데 필요한 정보

StorageGRID용 클라이언트 네트워크는 그리드에 대한 클라이언트 프로토콜 액세스를 제공하는 데 사용되는 선택적 네트워크입니다. 어플라이언스는 E5500SG 컨트롤러의 10GbE 포트를 사용하여 클라이언트 네트워크에 연결됩니다.

이러한 포트의 옵션에 대한 자세한 내용은 "E5500SG 컨트롤러의 10GbE 포트 연결"을 참조하십시오.

정보가 필요합니다	귀사의 가치
클라이언트 네트워크가 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요(기본값) • 예
네트워크 연결 모드	다음 중 하나를 선택하십시오. • Active-Backup(기본값) • LACP(802.3ad)
VLAN 태그 지정이 활성화되었습니다	다음 중 하나를 선택하십시오. • 아니요(기본값) • 예
VLAN 태그(VLAN 태그 지정이 활성화된 경우)	0에서 4095 사이의 값을 입력합니다.
전원을 켠 후 사용할 수 있는 경우 클라이언트 네트워크에 대해 DHCP 할당 IP 주소입니다	• IPv4 주소(CIDR): • 게이트웨이:
클라이언트 네트워크의 어플라이언스 스토리지 노드에 사용할 고정 IP 주소입니다 • 참고: * 클라이언트 네트워크가 활성화된 경우 컨트롤러의 기본 라우트는 여기에 지정된 게이트웨이를 사용합니다.	• IPv4 주소(CIDR): • 게이트웨이:

관련 정보

어플라이언스 네트워크 연결 검토(SG5600)

하드웨어 구성(SG5600)

E5500SG 컨트롤러 포트의 포트 연결 모드

하드웨어 설치(SG5600)

하드웨어 설치에는 하드웨어 구성 요소 설치, 구성 요소 케이블 연결 및 포트 구성 등 몇 가지 주요 작업이 포함됩니다.

하드웨어 등록

어플라이언스 하드웨어를 등록하면 지원 혜택이 제공됩니다.

단계

1. 섀시 일련 번호를 찾습니다.

   포장 명세서, 확인 이메일 또는 제품의 포장을 푼 후 제품에서 번호를 확인할 수 있습니다.

2. NetApp Support 사이트 로 이동합니다 "mysupport.netapp.com".
3. 하드웨어를 등록해야 하는지 여부를 확인합니다.

귀하의 경우...	다음 단계를 따르십시오...
더 많은 워크로드 추가)	a. 사용자 이름과 암호를 사용하여 로그인합니다. b. 제품 * > * 내 제품 * 을 선택합니다. c. 새 일련 번호가 나열되는지 확인합니다. d. 그렇지 않은 경우 새 NetApp 고객에 대한 지침을 따르십시오.
신규 NetApp 고객	a. 지금 등록 * 을 클릭하고 계정을 만듭니다. b. 제품 * > * 제품 등록 * 을 선택합니다. c. 제품 일련 번호 및 요청된 세부 정보를 입력합니다. 등록이 승인되면 필요한 소프트웨어를 다운로드할 수 있습니다. 승인 프로세스는 최대 24시간이 걸릴 수 있습니다.

캐비닛 또는 랙에 어플라이언스 설치**(SG5600)**

캐비닛이나 랙에 레일을 설치한 다음 제품을 레일에 밀어 넣으십시오. SG5660을 사용하는 경우 어플라이언스를 설치한 후 드라이브를 설치해야 합니다.

필요한 것

- 상자에 포함된 안전 고지 문서를 검토하고 하드웨어 이동 및 설치에 대한 예방 조치를 이해했습니다.
- 하드웨어에 대한 E-Series 설치 지침이 있습니다.

장비가 넘어지지 않도록 랙 또는 캐비닛 또는 랙의 하단에서 하드웨어를 설치하십시오.

SG5612의 중량은 드라이브를 완전히 장착할 때 약 27kg(60파운드)입니다. SG5612를 안전하게 옮기려면 두 사람 또는 기계화된 리프트가 필요합니다.

SG5660의 중량은 드라이브가 설치되지 않은 상태에서 약 60kg(132lb)입니다. 빈 SG5660을 안전하게 옮기려면 4명 또는 기계화된 리프트가 필요합니다.

> 하드웨어 손상을 방지하려면 드라이브가 설치된 경우 SG5660을 이동하지 마십시오. 제품을 이동하기 전에 모든 드라이브를 제거해야 합니다.

이 작업에 대해

SG5660 어플라이언스를 캐비닛 또는 랙에 설치하려면 다음 작업을 완료하십시오.

- * 장착 레일 설치 *

  캐비닛 또는 랙에 장착 레일을 설치합니다.

  E2700 또는 E5600의 E-Series 설치 지침을 참조하십시오.

- * 캐비닛 또는 랙에 제품을 설치합니다 *

  제품을 캐비닛 또는 랙에 밀어 넣고 고정합니다.

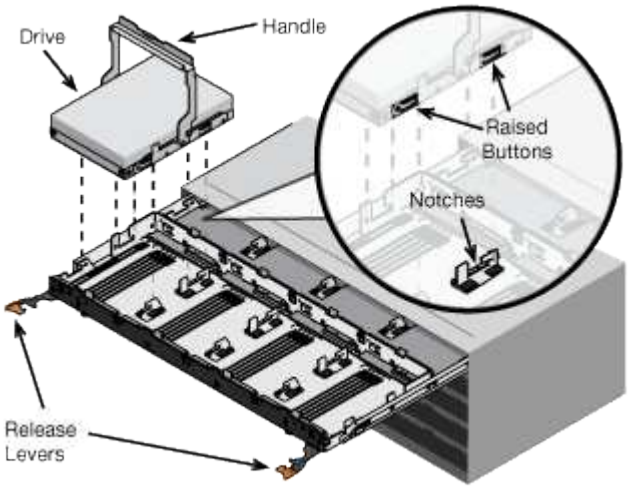
  > SG5660을 손으로 들어올릴 경우 섀시 측면에 4개의 핸들을 부착합니다. 제품을 레일에 밀어 넣을 때 손잡이를 분리하십시오.

- * 드라이브를 설치합니다 *

  SG5660을 사용하는 경우 5개의 드라이브 드로어 각각에 12개의 드라이브를 설치합니다.

  올바르게 작동하려면 60개의 드라이브를 모두 설치해야 합니다.

  a. ESD 밴드를 착용하고 포장재에서 드라이브를 제거합니다.
  b. 상단 드라이브 드로어의 레버를 분리하고 레버를 사용하여 드로어를 밀어 꺼냅니다.
  c. 드라이브 손잡이를 수직으로 올리고 드라이브의 단추를 드로어의 노치에 맞춥니다.



  d. 드라이브 상단을 부드럽게 눌러 드라이브가 제자리에 끼워질 때까지 드라이브 핸들을 아래로 돌립니다.
  e. 처음 12개의 드라이브를 설치한 후 중앙을 누르고 양쪽 레버를 부드럽게 닫아 드로어를 다시 밀어 넣습니다.
  f. 다른 4개의 문서함에 대해 이 단계를 반복합니다.

- * 전면 베젤을 부착합니다 *

- SG5612 *: 왼쪽 및 오른쪽 엔드 캡을 전면에 장착합니다.
- SG5660 *: 베젤을 전면에 장착합니다.

관련 정보

"E2700 컨트롤러 - 드라이브 트레이 및 관련 드라이브 트레이 설치 가이드"

"E5600 컨트롤러 - 드라이브 트레이 및 관련 드라이브 트레이 설치 가이드"

케이블 어플라이언스**(SG5600)**

SAS 인터커넥트 케이블을 사용하여 두 컨트롤러를 서로 연결하고, 관리 포트를 해당 관리 네트워크에 연결하고, E5500SG 컨트롤러의 10GbE 포트를 그리드 네트워크 및 StorageGRID용 선택적 클라이언트 네트워크에 연결해야 합니다.

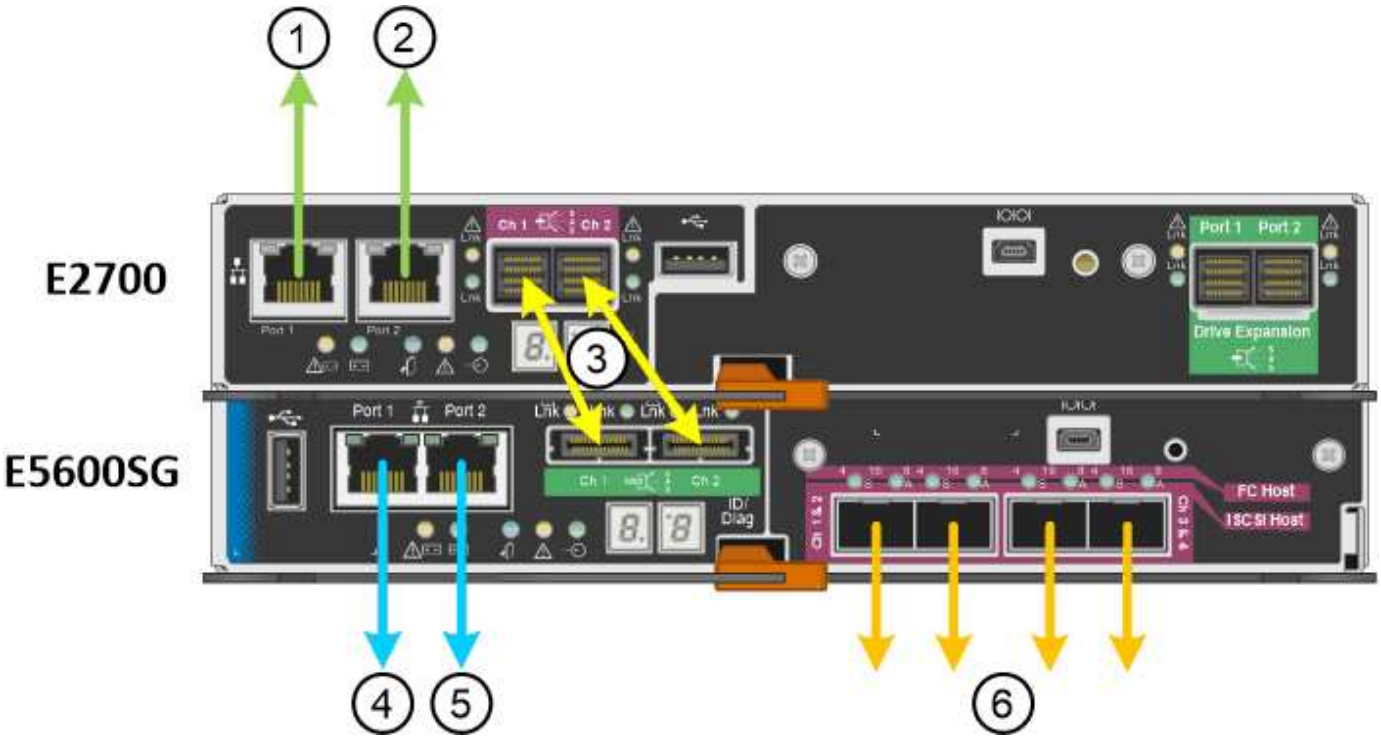
필요한 것

- 관리 포트를 연결하기 위한 이더넷 케이블이 있습니다.
- 10GbE 포트 4개를 연결하기 위한 광 케이블이 있습니다(이 케이블은 어플라이언스와 함께 제공되지 않음).

> * 레이저 방사선에 노출될 위험 * — SFP 트랜시버를 분해하거나 제거하지 마십시오. 레이저 방사선에 노출될 수 있습니다.

이 작업에 대해

케이블을 연결할 때는 다음 다이어그램을 참조하여 E2700 컨트롤러 위쪽 및 아래쪽에 있는 E5500SG 컨트롤러를 표시합니다. 이 다이어그램은 SG5660 모델을 보여 주며 SG5612 모델의 컨트롤러가 스택 대신 나란히 표시됩니다.



항목	포트	포트의 유형입니다	기능
1	E2700 컨트롤러의 관리 포트 1	1Gb(RJ-45) 이더넷	SANtricity Storage Manager가 설치된 네트워크에 E2700 컨트롤러를 연결합니다.
2	E2700 컨트롤러의 관리 포트 2	1Gb(RJ-45) 이더넷	설치 중에 서비스 랩톱에 E2700 컨트롤러를 연결합니다.
3	각 컨트롤러에 Ch 1 및 Ch 2 라고 표시된 2개의 SAS 상호 연결 포트	E2700 컨트롤러: mini-SAS-HD E5500SG 컨트롤러: 미니 SAS	두 컨트롤러를 서로 연결합니다.
4	E5500SG 컨트롤러의 관리 포트 1	1Gb(RJ-45) 이더넷	StorageGRID용 관리 네트워크에 E5500SG 컨트롤러를 연결합니다.
5	E5500SG 컨트롤러의 관리 포트 2	1Gb(RJ-45) 이더넷	• 관리 네트워크에 대한 중복 연결을 원할 경우 관리 포트 1에 연결할 수 있습니다. • 유선을 해제하고 임시 로컬 액세스(IP 169.254.0.1)에 사용할 수 있습니다. • DHCP 할당 IP 주소를 사용할 수 없는 경우 설치 중에 E5500SG 컨트롤러를 서비스 랩톱에 연결하는 데 사용할 수 있습니다.
6	E5500SG 컨트롤러의 네트워크 포트 4개	10GbE(광)	E5500SG 컨트롤러를 그리드 네트워크 및 StorageGRID용 클라이언트 네트워크(사용되는 경우)에 연결합니다. 포트를 함께 결합하여 컨트롤러에 중복 경로를 제공할 수 있습니다.

단계

1. SAS 인터커넥트 케이블 2개를 사용하여 E2700 컨트롤러를 E5500SG 컨트롤러에 연결합니다.

이 포트 연결...	이 포트로...
SAS 인터커넥트 포트 1(Ch 1 레이블): E2700 컨트롤러	E5500SG 컨트롤러의 SAS 인터커넥트 포트 1(Ch 1 레이블
SAS 인터커넥트 포트 2(Ch 2 레이블): E2700 컨트롤러	E5500SG 컨트롤러의 SAS 인터커넥트 포트 2(Ch 2 레이블)

E2700 컨트롤러용 사각형 커넥터(미니 SAS HD)를 사용하고 E54600 SG 컨트롤러용 직사각형 커넥터(미니 SAS)를 사용하십시오.

> SAS 커넥터의 당기기 탭이 하단에 있는지 확인하고 딸깍 소리가 나면서 제자리에 고정될 때까지 조심스럽게 각 커넥터를 삽입합니다. 저항이 있을 경우 커넥터를 누르지 마십시오. 계속하기 전에 당김 탭의 위치를 확인하십시오.

2. 이더넷 케이블을 사용하여 SANtricity 스토리지 관리자 소프트웨어가 설치된 관리 네트워크에 E2700 컨트롤러를 연결합니다.

이 포트 연결...	이 포트로...
E2700 컨트롤러의 포트 1(왼쪽의 RJ-45 포트)	SANtricity 스토리지 관리자에 사용되는 관리 네트워크의 스위치 포트입니다
E2700 컨트롤러의 포트 2	서비스 랩톱(DHCP를 사용하지 않는 경우

3. StorageGRID용 관리 네트워크를 사용하려는 경우 이더넷 케이블을 사용하여 E5500SG 컨트롤러를 연결합니다.

이 포트 연결...	이 포트로...
E5500SG 컨트롤러의 포트 1(왼쪽의 RJ-45 포트)	StorageGRID용 관리 네트워크의 포트를 전환합니다
E5500SG 컨트롤러의 포트 2	서비스 랩톱(DHCP를 사용하지 않는 경우

4. 광 케이블과 SFP+ 트랜시버를 사용하여 E5500SG 컨트롤러의 10GbE 포트를 해당 네트워크 스위치에 연결합니다.
   - 고정 포트 결합 모드(기본값)를 사용하려는 경우 표 에 나와 있는 대로 포트를 StorageGRID 그리드 및 클라이언트 네트워크에 연결합니다.

포트	연결 대상...
포트 1	클라이언트 네트워크(옵션)
포트 2	그리드 네트워크
포트 3	클라이언트 네트워크(옵션)

포트	연결 대상...
포트 4	그리드 네트워크

- Aggregate 포트 결합 모드를 사용하려는 경우 하나 이상의 네트워크 포트를 하나 이상의 스위치에 연결합니다. 단일 장애 지점이 발생하지 않도록 4개 포트 중 2개 이상을 연결해야 합니다. 단일 LACP 결합에 둘 이상의 스위치를 사용하는 경우 스위치는 MLAG 또는 동급 스위치를 지원해야 합니다.

관련 정보

E5500SG 컨트롤러 포트의 포트 연결 모드

StorageGRID 어플라이언스 설치 프로그램에 액세스합니다

AC 전원 코드 연결**(SG5600)**

AC 전원 코드를 외부 전원과 각 컨트롤러의 AC 전원 커넥터에 연결해야 합니다. 전원 코드를 연결한 후 전원을 켤 수 있습니다.

필요한 것

전원을 연결하기 전에 두 제품의 전원 스위치를 모두 꺼야 합니다.

* 감전 위험 * — 전원 코드를 연결하기 전에 제품의 두 전원 스위치가 꺼져 있는지 확인하십시오.

이 작업에 대해

- 각 전원 공급 장치마다 별도의 전원을 사용해야 합니다.

  독립 전원에 연결하면 전원 중복성이 유지됩니다.

- 무정전 전원 공급 장치(UPS)의 벽 콘센트와 같이 대상 국가에서 사용되는 일반 콘센트가 있는 컨트롤러와 함께 제공된 전원 코드를 사용할 수 있습니다.

  그러나 이러한 전원 코드는 대부분의 EIA 준수 캐비닛에서 사용할 수 없습니다.

단계

1. 인클로저 또는 섀시의 전원 스위치를 끕니다.
2. 컨트롤러의 전원 스위치를 끕니다.
3. 주 전원 코드를 캐비닛의 외부 전원에 연결합니다.
4. 각 컨트롤러의 AC 전원 커넥터에 전원 코드를 연결합니다.

전원 켜기**(SG5600)**

엔클로저의 전원을 켜면 두 컨트롤러에 전원이 제공됩니다.

단계

1. 엔클로저 후면에서 전원 공급 장치 스위치 2개를 켭니다.

   전원이 공급되는 동안 컨트롤러의 LED가 간헐적으로 켜지거나 꺼집니다.

전원 켜기 프로세스를 완료하는 데 최대 10분이 걸릴 수 있습니다. 초기 시작 시퀀스 중에 컨트롤러가 여러 번 재부팅되면 팬이 회전/다운되고 LED가 깜박입니다.

2. 각 컨트롤러의 전원 LED 및 호스트 링크 활성 LED를 확인하여 전원이 켜졌는지 점검합니다.
3. 모든 드라이브에 녹색 LED가 계속 켜져 온라인 상태임을 나타낼 때까지 기다립니다.
4. 엔클로저의 전면과 후면에 녹색 LED가 있는지 확인합니다.

   주황색 LED가 나타나면 위치를 기록해 둡니다.

5. E5500SG 컨트롤러에 대한 7개 세그먼트 디스플레이를 살펴봅니다.

   이 디스플레이에는 * HO * 가 표시되고 그 뒤에 두 자리 숫자가 반복됩니다.

```
HO -- IP address for Admin Network -- IP address for Grid Network HO
```

   순서대로 첫 번째 숫자 세트는 컨트롤러의 관리 포트 1에 대해 DHCP가 할당한 IP 주소입니다. 이 주소는 컨트롤러를 StorageGRID용 관리 네트워크에 연결하는 데 사용됩니다. 두 번째 숫자 세트는 어플라이언스를 StorageGRID용 그리드 네트워크에 연결하는 데 사용되는 DHCP 할당 IP 주소입니다.

   DHCP를 사용하여 IP 주소를 할당할 수 없는 경우 0.0.0.0이 표시됩니다.

SG5600 컨트롤러에서 부팅 상태 및 오류 코드 검토

각 컨트롤러에 있는 7세그먼트 디스플레이는 어플라이언스 전원이 켜질 때, 하드웨어가 초기화되는 동안, 그리고 하드웨어가 실패하여 초기화에서 다시 나올 때 상태 및 오류 코드를 표시합니다. 진행 상황 또는 문제 해결을 모니터링하는 경우, 코드의 순서를 순서대로 살펴봐야 합니다.

이 작업에 대해

E5500SG 컨트롤러의 상태 및 오류 코드는 E2700 컨트롤러의 상태 및 오류 코드와 다릅니다.

단계

1. 부팅 중에 7세그먼트 디스플레이에 표시된 코드를 보고 진행 상황을 모니터링합니다.
2. E5500SG 컨트롤러에 대한 오류 코드를 검토하려면 7세그먼트 디스플레이 상태 및 오류 코드 정보를 참조하십시오.
3. E2700 컨트롤러의 오류 코드를 검토하려면 지원 사이트 에서 E2700 컨트롤러 설명서를 참조하십시오.

관련 정보

E5500SG 컨트롤러 7세그먼트 디스플레이 코드

"NetApp 설명서: E2700 시리즈"

E5500SG 컨트롤러 **7**세그먼트 디스플레이 코드

어플라이언스 전원이 켜지고 하드웨어가 초기화되는 동안 E5500SG 컨트롤러의 7세그먼트

디스플레이에 상태 및 오류 코드가 표시됩니다. 이러한 코드를 사용하여 상태를 확인하고 오류를 해결할 수 있습니다.

E5500SG 컨트롤러에서 상태 및 오류 코드를 검토할 때는 다음 코드 유형을 확인해야 합니다.

- * 일반 부팅 코드 *

  표준 부팅 이벤트를 나타냅니다.

- * 일반 부팅 코드 *

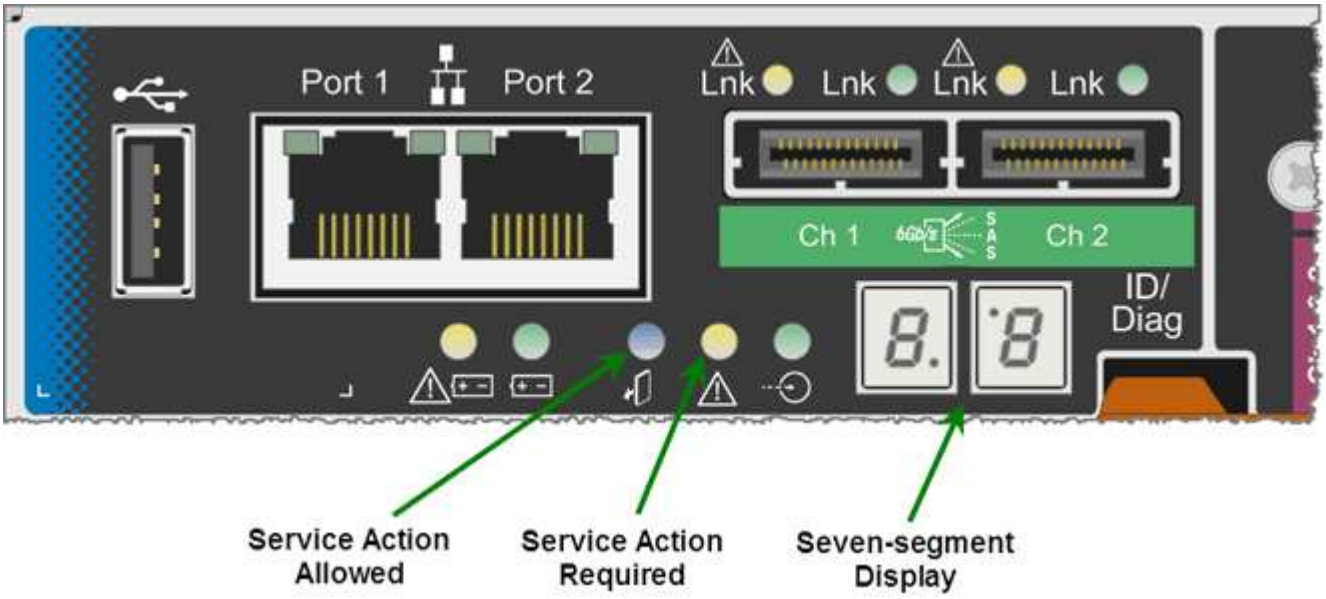
  어플라이언스에서 발생하는 일반적인 부팅 이벤트를 나타냅니다.

- * 오류 코드 *

  부팅 이벤트 중에 문제를 나타냅니다.

StorageGRID는 StorageGRID 어플라이언스 설치 프로그램이 시작된 후에만 E54600 SG 컨트롤러에서 다음 상태 표시등만 제어합니다.

- 서비스 작업 허용 LED
- 서비스 조치 필요 LED
- 7개 세그먼트 디스플레이



7세그먼트 디스플레이에서 소수점 이하 자릿수는 StorageGRID 제품에서 사용되지 않습니다.

- 최소 유효 자릿수 근처의 상위 소수점은 플랫폼 진단 LED입니다.

  재설정 및 초기 하드웨어 구성 중에 켜집니다. 그렇지 않으면 꺼집니다.

- 가장 중요한 숫자에 인접한 하위 소수점이 꺼집니다.

다른 문제를 진단하려면 다음 리소스를 살펴볼 수 있습니다.

- 기타 모든 하드웨어 및 환경 진단 정보를 보려면 E-Series 운영 체제 하드웨어 진단 유틸리티를 참조하십시오.

  여기에는 전원, 온도 및 디스크 드라이브와 같은 하드웨어 문제를 찾는 작업이 포함됩니다. 어플라이언스는 E-Series 운영 체제를 사용하여 모든 플랫폼 환경 상태를 모니터링합니다.

- 펌웨어 및 드라이버 문제를 확인하려면 SAS 및 네트워크 포트의 링크 표시등을 확인합니다.

  자세한 내용은 E-Series E5600 설명서를 참조하십시오.

일반 부팅 코드

부팅 중 또는 하드웨어 하드 리셋 후 하드웨어 초기화 중에 서비스 작업이 허용되고 서비스 작업 필요 LED가 켜집니다. 7세그먼트 디스플레이에는 E-Series 하드웨어와 동일하고 E5600SG 컨트롤러에만 한정되지 않는 일련의 코드가 표시됩니다.

부팅 중에 FPGA(Field Programmable Gate Array)는 하드웨어의 기능과 초기화를 제어합니다.

코드	표시
19	FPGA 초기화
68	FPGA 초기화
…	FPGA 초기화, 빠른 코드 승계이다.
AA	플랫폼 BIOS 부팅.
FF	BIOS 부팅 완료. E600SG 컨트롤러가 초기화되고 상태를 나타내도록 LED를 관리하기 전의 중간 상태입니다.

AA 및 FF 코드가 나타나면 일반 부팅 코드가 나타나거나 오류 코드가 나타납니다. 또한 허용되는 서비스 작업 및 필요한 서비스 작업 LED가 꺼집니다.

일반적인 부팅 코드입니다

이러한 코드는 시간 순으로 어플라이언스에서 발생하는 일반적인 부팅 이벤트를 나타냅니다.

코드	표시
안녕	마스터 부트 스크립트가 시작되었습니다.
PP	플랫폼 FPGA 펌웨어가 업데이트를 확인하고 있습니다.
HP	HIC(호스트 인터페이스 카드)에서 업데이트를 확인하고 있습니다.

코드	표시
RB	펌웨어 업데이트 후, 필요한 경우 시스템이 재부팅 중입니다.
FP	펌웨어 업데이트 검사가 완료되었습니다. E2700 컨트롤러와 통신 및 관리하기 위한 프로세스(utmagent)를 시작합니다. 이 프로세스는 어플라이언스 프로비저닝을 용이하게 합니다.
그는	시스템이 E-Series 운영 체제와 동기화되고 있습니다.
HC	StorageGRID 설치를 확인하는 중입니다.
호	설치 관리 및 활성 인터페이스 발생
HA	Linux 운영 체제와 StorageGRID가 실행 중입니다.

E5500SG 컨트롤러 오류 코드

이러한 코드는 어플라이언스 부팅 시 E5500SG 컨트롤러에 표시될 수 있는 오류 상태를 나타냅니다. 특정 하위 수준 하드웨어 오류가 발생할 경우 추가 2자리 16진수 코드가 표시됩니다. 이러한 코드 중 하나라도 1초 또는 2초 이상 지속되거나 규정된 문제 해결 절차 중 하나를 수행하여 오류를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

코드	표시
22	부팅 장치에서 마스터 부트 레코드를 찾을 수 없습니다.
23	설치된 SATA 드라이브가 없습니다.
2A, 2B	버스 고착, DIMM SPD 데이터를 읽을 수 없음.
40	DIMM이 잘못되었습니다.
41	DIMM이 잘못되었습니다.
42	메모리 테스트에 실패했습니다.
51	SPD 읽기 오류입니다.
92에서 96	PCI 버스 초기화.
A0에서 A3까지	SATA 드라이브 초기화
복부	대체 부팅 코드.

코드	표시
AE	OS 부팅 중.
EA	DDR3 교육에 실패했습니다.
E8	설치된 메모리가 없습니다.
EU	설치 스크립트를 찾을 수 없습니다.
EP	"ManageSGA" 코드는 E2700 컨트롤러와 사전 그리드 통신이 실패했음을 나타냅니다.

관련 정보

하드웨어 설치 문제 해결(SG5600)

"NetApp 지원"

하드웨어 구성(SG5600)

어플라이언스에 전원을 적용한 후 하드웨어를 모니터링하는 데 사용할 소프트웨어인 SANtricity 스토리지 관리자를 구성해야 합니다. StorageGRID에서 사용할 네트워크 연결도 구성해야 합니다.

StorageGRID 연결 구성(SG5600)

StorageGRID 어플라이언스를 StorageGRID 그리드에 스토리지 노드로 구축하기 전에 어플라이언스와 사용할 네트워크 간의 연결을 구성해야 합니다. E54600 SG 컨트롤러(어플라이언스의 컴퓨팅 컨트롤러)에 포함된 StorageGRID 어플라이언스 설치 프로그램으로 이동하여 네트워킹을 구성할 수 있습니다.

StorageGRID 어플라이언스 설치 프로그램에 액세스합니다

어플라이언스와 세 StorageGRID 네트워크(그리드 네트워크, 관리자 네트워크(옵션) 및 클라이언트 네트워크(선택 사항) 간의 연결을 구성하려면 StorageGRID 어플라이언스 설치 프로그램에 액세스해야 합니다.

필요한 것

- 을(를) 사용하고 있습니다 지원되는 웹 브라우저.
- 이 어플라이언스는 사용하려는 모든 StorageGRID 네트워크에 연결되어 있습니다.
- 이러한 네트워크에서 어플라이언스의 IP 주소, 게이트웨이 및 서브넷을 알고 있습니다.
- 사용할 네트워크 스위치를 구성했습니다.

이 작업에 대해

StorageGRID 어플라이언스 설치 프로그램에 처음 액세스할 때 관리 네트워크에 대해 DHCP 할당 IP 주소

(어플라이언스가 관리 네트워크에 연결되어 있다고 가정) 또는 그리드 네트워크에 대해 DHCP 할당 IP 주소를 사용할 수 있습니다. 관리 네트워크의 IP 주소를 사용하는 것이 좋습니다. 그렇지 않으면 그리드 네트워크의 DHCP 주소를 사용하여 StorageGRID 어플라이언스 설치 프로그램에 액세스하는 경우 링크 설정을 변경하거나 고정 IP를 입력할 때 StorageGRID 어플라이언스 설치 프로그램과의 연결이 끊어질 수 있습니다.

단계

1. 관리 네트워크(연결된 경우) 또는 그리드 네트워크(관리 네트워크가 연결되어 있지 않은 경우)에서 어플라이언스의 DHCP 주소를 얻습니다.

   다음 중 하나를 수행할 수 있습니다.

   - 관리 포트 1의 MAC 주소를 네트워크 관리자에게 제공하여 관리 네트워크에서 이 포트의 DHCP 주소를 찾을 수 있도록 합니다. MAC 주소는 포트 옆에 있는 E5500SG 컨트롤러의 레이블에 인쇄되어 있습니다.
   - E5500SG 컨트롤러에서 7개 세그먼트 디스플레이를 확인합니다. E5500SG 컨트롤러의 관리 포트 1 및 10GbE 포트 2 및 4가 DHCP 서버를 통해 네트워크에 연결되어 있는 경우, 컨트롤러는 엔클로저의 전원을 켤 때 동적으로 할당된 IP 주소를 가져오려고 시도합니다. 컨트롤러가 전원 켜기 프로세스를 완료하면 7개 세그먼트 디스플레이에 * HO * 가 표시되고, 그 뒤에 2개의 숫자가 반복됩니다.

     ```
     HO -- IP address for Admin Network -- IP address for Grid Network HO
     ```

     시퀀스:

     - 첫 번째 번호 세트는 연결된 경우 관리 네트워크의 어플라이언스 스토리지 노드에 대한 DHCP 주소입니다. 이 IP 주소는 E5500SG 컨트롤러의 관리 포트 1에 할당됩니다.
     - 두 번째 숫자 세트는 그리드 네트워크의 어플라이언스 스토리지 노드에 대한 DHCP 주소입니다. 이 IP 주소는 어플라이언스에 처음 전원을 공급하면 10GbE 포트 2 및 4에 할당됩니다.

       DHCP를 사용하여 IP 주소를 할당할 수 없는 경우 0.0.0.0이 표시됩니다.

2. DHCP 주소 중 하나를 얻을 수 있는 경우:

   a. 서비스 랩톱에서 웹 브라우저를 엽니다.

   b. StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. + `https://*E5600SG_Controller_IP*:8443*

      '*E600SG_Controller_IP*'의 경우 컨트롤러의 DHCP 주소를 사용합니다(관리자 네트워크가 있는 경우 IP 주소 사용).

   c. 보안 경고 메시지가 나타나면 브라우저의 설치 마법사를 사용하여 인증서를 보고 설치합니다.

      다음에 이 URL에 액세스할 때 알림이 나타나지 않습니다.

      StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다. 이 페이지에 처음 액세스할 때 표시되는 정보와 메시지는 어플라이언스가 현재 StorageGRID 네트워크에 연결되어 있는 방식에 따라 다릅니다. 오류 메시지가 나타날 수 있으며, 이 메시지는 이후 단계에서 해결될 것입니다.

NetApp® StorageGRID® Appliance Installer

Home | Configure Networking | Configure Hardware | Monitor Installation | Advanced

Home

The installation is ready to be started. Review the settings below, and then click Start Installation.

This Node

Node type: Storage

Node name: MM-2-108-SGA-lab25

Cancel Save

Primary Admin Node connection

Enable Admin Node discovery: ☐

Primary Admin Node IP: 172.16.1.178

Connection state: Connection to 172.16.1.178 ready

Cancel Save

Installation

Current state: Ready to start installation of MM-2-108-SGA-lab25 into grid with Admin Node 172.16.1.178 running StorageGRID 11.2.0, using StorageGRID software downloaded from the Admin Node.

Start Installation

3. E5500SG 컨트롤러가 DHCP를 사용하여 IP 주소를 가져올 수 없는 경우:

   a. 이더넷 케이블을 사용하여 E54600 SG 컨트롤러의 관리 포트 2에 서비스 랩톱을 연결합니다.

b. 서비스 랩톱에서 웹 브라우저를 엽니다.

c. StorageGRID 어플라이언스 설치 프로그램에 대한 이 URL을 입력합니다: + `* https://169.254.0.1:8443*

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다. 이 페이지에 처음 액세스할 때 표시되는 정보 및 메시지는 어플라이언스가 현재 연결되어 있는 방식에 따라 다릅니다.

> 링크 로컬 연결을 통해 홈 페이지에 액세스할 수 없는 경우 서비스 랩톱 IP 주소를 "169.254.0.2"로 구성한 후 다시 시도하십시오.

4. 홈 페이지에 표시되는 메시지를 검토하고 필요에 따라 링크 구성 및 IP 구성을 구성합니다.

관련 정보

웹 브라우저 요구 사항

StorageGRID 어플라이언스 설치 프로그램 버전을 확인하고 업그레이드합니다

어플라이언스의 StorageGRID 어플라이언스 설치 프로그램 버전은 StorageGRID 시스템에 설치된 소프트웨어 버전과 일치해야 모든 StorageGRID 기능이 지원됩니다.

필요한 것

StorageGRID 어플라이언스 설치 프로그램에 액세스했습니다.

StorageGRID 어플라이언스는 StorageGRID 어플라이언스 설치 프로그램이 사전 설치된 상태로 제공됩니다. 최근에 업그레이드된 StorageGRID 시스템에 어플라이언스를 추가하는 경우 어플라이언스를 새 노드로 설치하기 전에 StorageGRID 어플라이언스 설치 프로그램을 수동으로 업그레이드해야 할 수 있습니다.

새 StorageGRID 버전으로 업그레이드하면 StorageGRID 어플라이언스 설치 프로그램이 자동으로 업그레이드됩니다. 설치된 어플라이언스 노드에서 StorageGRID 어플라이언스 설치 프로그램을 업그레이드할 필요가 없습니다. 이 절차는 이전 버전의 StorageGRID 어플라이언스 설치 프로그램이 포함된 어플라이언스를 설치하는 경우에만 필요합니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 펌웨어 업그레이드 * 를 선택합니다.

2. 현재 펌웨어 버전을 StorageGRID 시스템에 설치된 소프트웨어 버전과 비교합니다. (그리드 관리자 상단에서 도움말 아이콘을 선택하고 * 정보 * 를 선택합니다.)

   두 버전의 두 번째 숫자가 일치해야 합니다. 예를 들어, StorageGRID 시스템에서 버전 11. * 6 *.*x*._y_를 실행하는 경우 StorageGRID 어플라이언스 설치 프로그램 버전은 3. * 6 *._z_이어야 합니다.

3. 어플라이언스에 StorageGRID 어플라이언스 설치 프로그램의 하위 수준 버전이 있는 경우 로 이동합니다https://mysupport.netapp.com/site/products/all/details/storagegrid-appliance/downloads-tab["NetApp 다운로드: StorageGRID 어플라이언스"^].

   NetApp 계정의 사용자 이름과 암호를 사용하여 로그인합니다.

4. StorageGRID Appliances*용 * 지원 파일의 적절한 버전과 해당 체크섬 파일을 다운로드하십시오.

   StorageGRID 어플라이언스 파일의 지원 파일은 모든 StorageGRID 어플라이언스 모델의 현재 및 이전 펌웨어 버전을 포함하는 '.zip' 아카이브로, 각 컨트롤러 유형의 하위 디렉토리에 있습니다.

StorageGRID 어플라이언스 파일용 지원 파일을 다운로드한 후 '.zip' 아카이브의 압축을 풀고 StorageGRID 어플라이언스 설치 프로그램 설치에 대한 중요 정보는 README 파일을 참조하십시오.

5. StorageGRID 어플라이언스 설치 프로그램의 펌웨어 업그레이드 페이지에 있는 지침에 따라 다음 단계를 수행합니다.
   a. 컨트롤러 유형 및 체크섬 파일에 적합한 지원 파일(펌웨어 이미지)을 업로드합니다.
   b. 비활성 파티션을 업그레이드합니다.
   c. 재부팅하고 파티션을 바꿉니다.
   d. 두 번째(비활성) 파티션을 업그레이드합니다.

관련 정보

StorageGRID 어플라이언스 설치 프로그램에 액세스합니다

네트워크 링크 구성**(SG5600)**

어플라이언스를 그리드 네트워크, 클라이언트 네트워크 및 관리 네트워크에 연결하는 데 사용되는 포트에 대한 네트워크 링크를 구성할 수 있습니다. 링크 속도와 포트 및 네트워크 연결 모드를 설정할 수 있습니다.

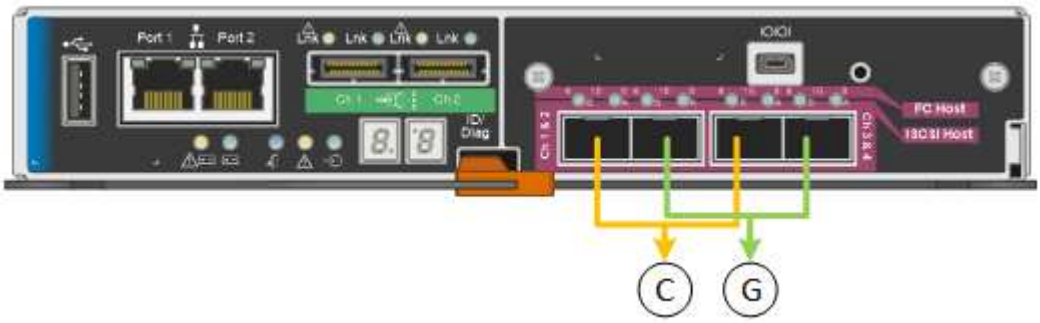
필요한 것

Aggregate 포트 결합 모드, LACP 네트워크 결합 모드 또는 VLAN 태그 지정을 사용하려면 다음을 수행합니다.

- 어플라이언스의 10GbE 포트를 VLAN 및 LACP를 지원할 수 있는 스위치에 연결했습니다.
- LACP 결합에 여러 스위치가 사용되는 경우 스위치는 MLAG(Multi-Chassis Link Aggregation Group) 또는 이와 동등한 스위치를 지원합니다.
- VLAN, LACP, MLAG 또는 이와 동등한 기능을 사용하도록 스위치를 구성하는 방법을 이해합니다.
- 각 네트워크에 사용할 고유 VLAN 태그를 알고 있습니다. 이 VLAN 태그는 네트워크 트래픽이 올바른 네트워크로 라우팅되도록 각 네트워크 패킷에 추가됩니다.

이 작업에 대해

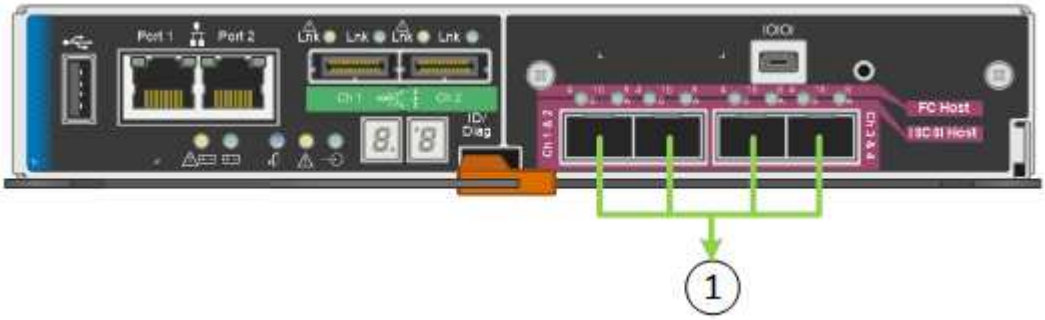
이 그림은 4개의 10GbE 포트가 고정 포트 결합 모드(기본 구성)에서 결합되는 방식을 보여 줍니다.



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
c	이 네트워크를 사용하는 경우 포트 1과 3이 클라이언트 네트워크에 대해 함께 연결됩니다.

속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
g	포트 2와 4는 그리드 네트워크를 위해 서로 연결되어 있습니다.

이 그림은 4개의 10GbE 포트가 애그리게이트 포트 결합 모드에서 결합되는 방식을 보여줍니다.



속성 표시기	어떤 포트가 연결되어 있는지 확인합니다
1	4개 포트 모두 단일 LACP 결합으로 그룹화되므로 모든 포트를 그리드 네트워크 및 클라이언트 네트워크 트래픽에 사용할 수 있습니다.

이 표에는 4개의 10GbE 포트를 구성하는 옵션이 요약되어 있습니다. 기본이 아닌 설정을 사용하려면 구성 연결 페이지에서 설정을 구성하기만 하면 됩니다.

- * 고정(기본값) 포트 결합 모드 *

네트워크 연결 모드	클라이언트 네트워크 비활성화 (기본값)	클라이언트 네트워크가 활성화되었습니다
Active-Backup(기본값)	• 포트 2와 4는 그리드 네트워크에 액티브-백업 결합을 사용합니다. • 포트 1과 3은 사용되지 않습니다. • VLAN 태그는 선택 사항입니다.	• 포트 2와 4는 그리드 네트워크에 액티브-백업 결합을 사용합니다. • 포트 1과 3은 클라이언트 네트워크에 대해 액티브-백업 연결을 사용합니다. • VLAN 태그는 두 네트워크에 대해 모두 지정할 수 있습니다.
LACP(802.3ad)	• 포트 2와 4는 그리드 네트워크에 LACP 결합을 사용합니다. • 포트 1과 3은 사용되지 않습니다. • VLAN 태그는 선택 사항입니다.	• 포트 2와 4는 그리드 네트워크에 LACP 결합을 사용합니다. • 포트 1과 3은 클라이언트 네트워크에 LACP 결합을 사용합니다. • VLAN 태그는 두 네트워크에 대해 모두 지정할 수 있습니다.

- * 집계 포트 결합 모드 *

네트워크 연결 모드	클라이언트 네트워크 비활성화 (기본값)	클라이언트 네트워크가 활성화되었습니다
LACP(802.3ad)만 해당	• 포트 1-4는 그리드 네트워크에 단일 LACP 결합을 사용합니다. • 단일 VLAN 태그는 그리드 네트워크 패킷을 식별합니다.	• 포트 1-4는 그리드 네트워크 및 클라이언트 네트워크에 단일 LACP 결합을 사용합니다. • 두 개의 VLAN 태그를 통해 그리드 네트워크 패킷을 클라이언트 네트워크 패킷과 분리할 수 있습니다.

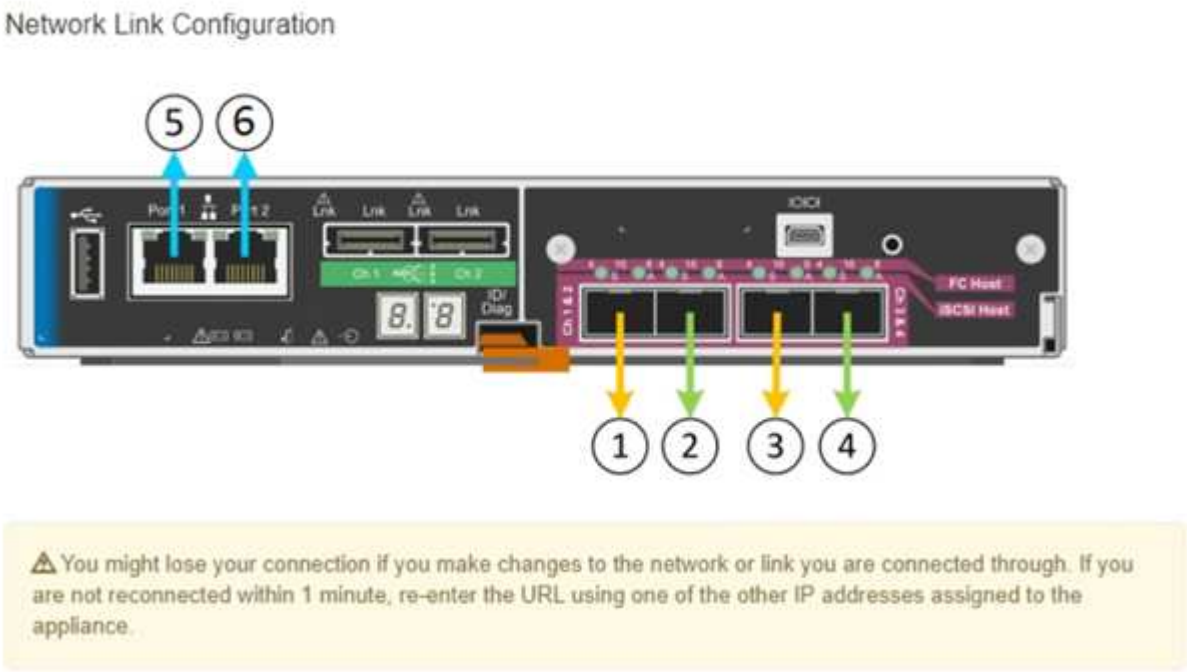
포트 본드 및 네트워크 결합 모드에 대한 자세한 내용은 ""E54600 SG 컨트롤러의 10GbE 포트 연결""을 참조하십시오.

이 그림에서는 E54600 SG 컨트롤러의 1GbE 관리 포트 2개가 관리 네트워크의 Active-Backup 네트워크 연결 모드로 연결되는 방식을 보여 줍니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램의 메뉴 모음에서 * 네트워킹 구성 * > * 링크 구성 * 을 클릭합니다.

   네트워크 링크 구성 페이지에는 네트워크 및 관리 포트 번호가 지정된 어플라이언스 다이어그램이 표시됩니다.



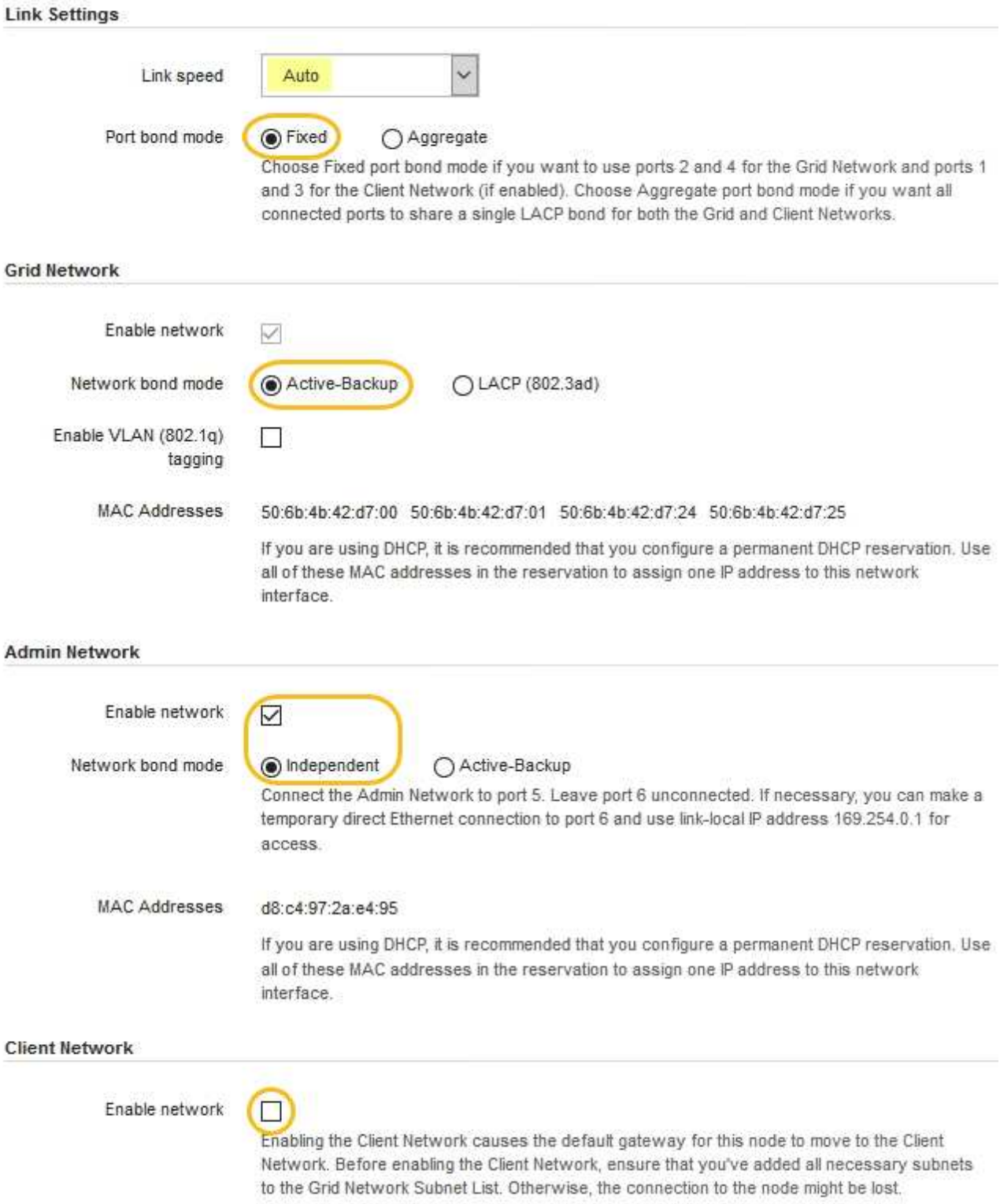
   링크 상태 테이블에는 번호가 매겨진 포트의 링크 상태(위/아래) 및 속도(1/10/25/40/100Gbps)가 나열됩니다.

Link Status

Link	State	Speed (Gbps)
1	Down	N/A
2	Up	10
3	Up	10
4	Down	N/A
5	Up	1
6	Up	1

이 페이지에 처음 액세스하는 경우:

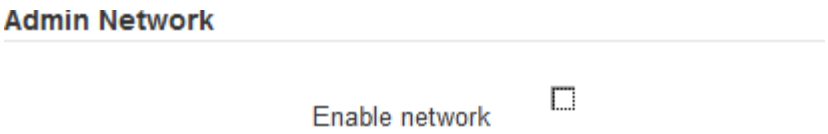
- * 링크 속도 * 는 * 10GbE * 로 설정됩니다. 이 속도는 E5500SG 컨트롤러에 사용할 수 있는 유일한 링크 속도입니다.
- * 포트 결합 모드 * 가 * 고정 * 으로 설정됩니다.
- 그리드 네트워크의 * 네트워크 결합 모드 * 가 * 액티브-백업 * 으로 설정됩니다.
- Admin Network*가 활성화되고 네트워크 연결 모드가 * Independent * 로 설정됩니다.
- 클라이언트 네트워크 * 가 비활성화됩니다.



2. 사용하려는 StorageGRID 네트워크를 활성화 또는 비활성화합니다.

   그리드 네트워크가 필요합니다. 이 네트워크를 비활성화할 수 없습니다.

   a. 어플라이언스가 관리 네트워크에 연결되어 있지 않은 경우 관리 네트워크의 * 네트워크 활성화 * 확인란을 선택 취소합니다.



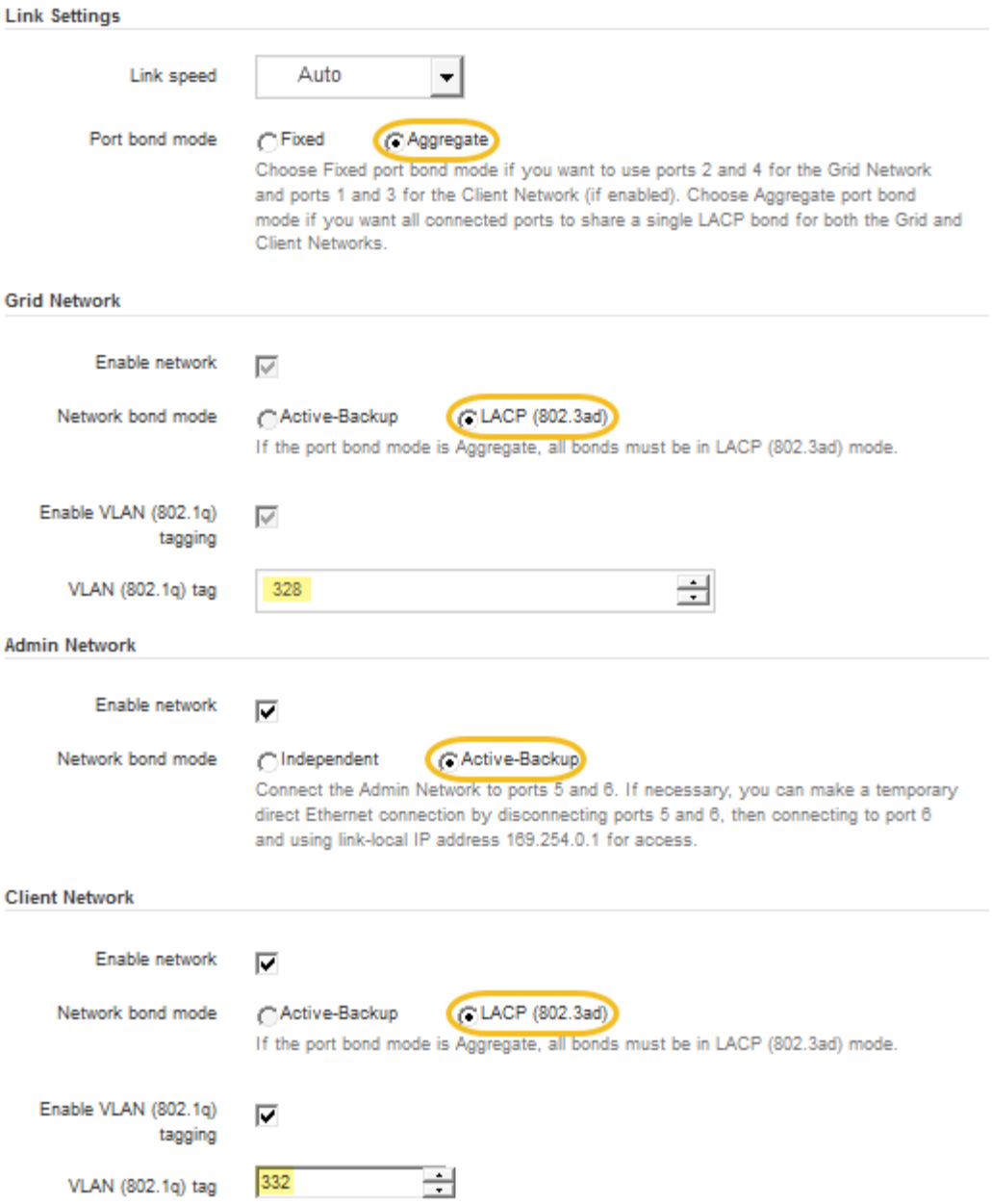
b. 어플라이언스가 클라이언트 네트워크에 연결되어 있는 경우 클라이언트 네트워크의 * 네트워크 활성화 * 확인란을 선택합니다.

   이제 10GbE 포트의 클라이언트 네트워크 설정이 표시됩니다.

3. 표를 참조하여 포트 결합 모드 및 네트워크 연결 모드를 구성합니다.

   예를 들면 다음과 같습니다.

   - 그리드 및 클라이언트 네트워크에 대해 * 집계 * 및 * LACP * 선택. 각 네트워크에 대해 고유한 VLAN 태그를 지정해야 합니다. 0에서 4095 사이의 값을 선택할 수 있습니다.
   - 관리자 네트워크에 대해 * Active-Backup * 이 선택되었습니다.



4. 선택 사항에 만족하면 * 저장 * 을 클릭합니다.

> 연결된 네트워크 또는 링크를 변경한 경우 연결이 끊어질 수 있습니다. 1분 내에 다시 연결되지 않으면 어플라이언스에 할당된 다른 IP 주소 중 하나를 사용하여 StorageGRID 어플라이언스 설치 프로그램의 URL을 다시 입력합니다. + " * https://*E5600SG_Controller_IP*:8443*`

관련 정보

E5500SG 컨트롤러 포트의 포트 연결 모드

IP 구성을 설정합니다

StorageGRID 어플라이언스 설치 프로그램을 사용하여 StorageGRID 그리드, 관리자 및 클라이언트 네트워크의 어플라이언스 스토리지 노드에 사용되는 IP 주소 및 라우팅 정보를 구성합니다.

이 작업에 대해

연결된 각 네트워크에서 어플라이언스에 대해 고정 IP를 할당하거나 DHCP 서버의 주소에 대해 영구 임대를 할당해야 합니다.

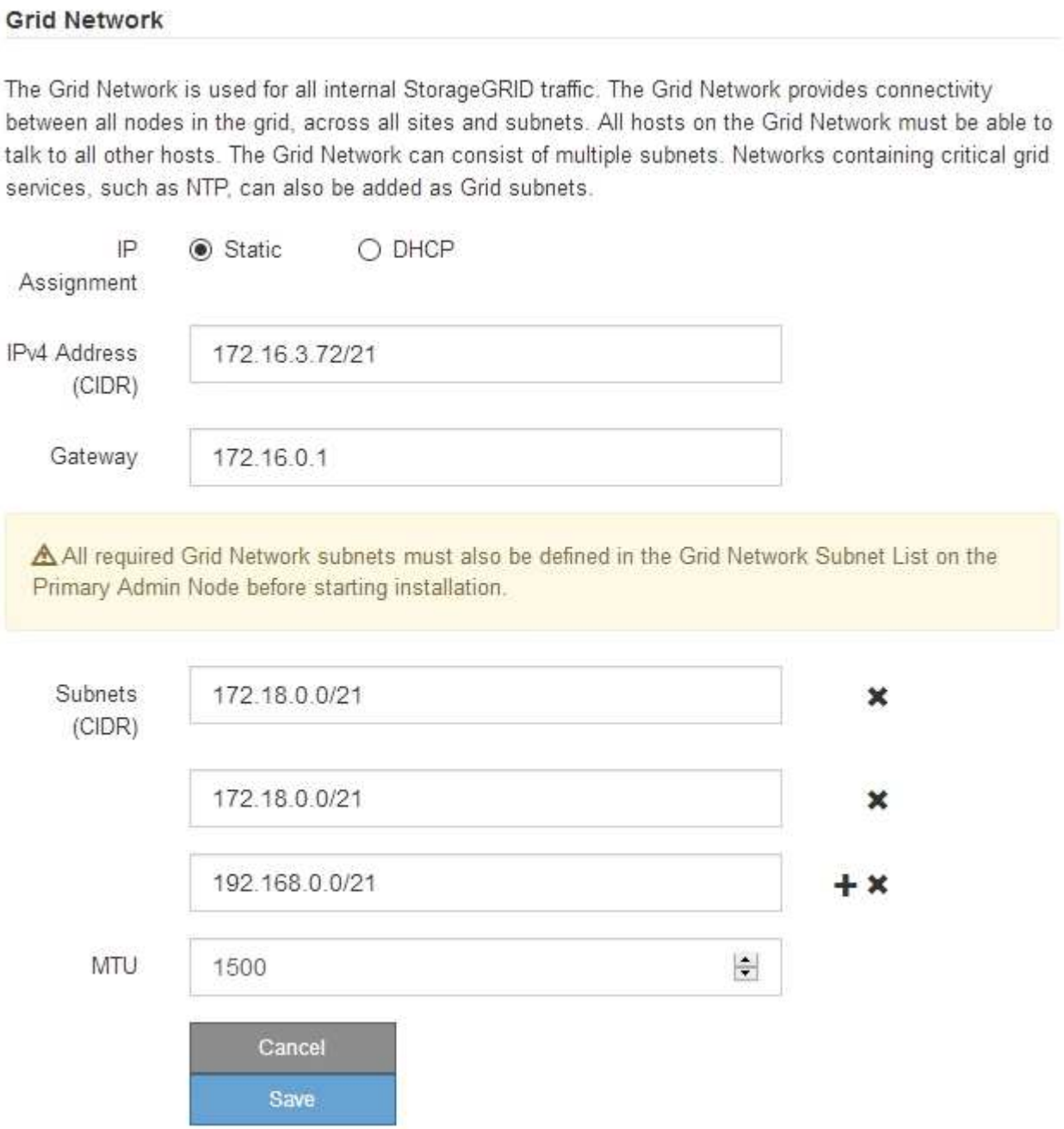
링크 구성을 변경하려면 E5500SG 컨트롤러의 링크 구성 변경 지침을 참조하십시오.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * IP 구성 * 을 선택합니다.

   IP 구성 페이지가 나타납니다.

2. 그리드 네트워크를 구성하려면 페이지의 * 그리드 네트워크 * 섹션에서 * 정적 * 또는 * DHCP * 를 선택합니다.



3. Static * (정적 *)을 선택한 경우 다음 단계에 따라 Grid Network(그리드 네트워크)를 구성합니다.
   a. CIDR 표기법을 사용하여 정적 IPv4 주소를 입력합니다.
   b. 게이트웨이를 입력합니다.

      네트워크에 게이트웨이가 없는 경우 동일한 정적 IPv4 주소를 다시 입력합니다.

   c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

      > 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

      > 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

   d. 저장 * 을 클릭합니다.

      IP 주소를 변경하면 게이트웨이와 서브넷 목록도 변경될 수 있습니다.

      StorageGRID 어플라이언스 설치 프로그램에 대한 연결이 끊어진 경우 방금 할당한 새 고정 IP 주소를 사용하여 URL을 다시 입력합니다. 예: + `https://services_appliance_IP:8443*

   e. 그리드 네트워크 서브넷 목록이 올바른지 확인합니다.

      그리드 서브넷이 있는 경우 그리드 네트워크 게이트웨이가 필요합니다. 지정된 모든 그리드 서브넷은 이 게이트웨이를 통해 연결할 수 있어야 합니다. 이러한 그리드 네트워크 서브넷은 StorageGRID 설치를 시작할 때 기본 관리 노드의 그리드 네트워크 서브넷 목록에도 정의되어 있어야 합니다.

      > 기본 라우트는 나열되지 않습니다. 클라이언트 네트워크가 활성화되지 않은 경우 기본 라우트는 그리드 네트워크 게이트웨이를 사용합니다.

      - 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
      - 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

   f. 저장 * 을 클릭합니다.
4. DHCP * 를 선택한 경우 다음 단계에 따라 그리드 네트워크를 구성합니다.
   a. DHCP * 라디오 버튼을 선택한 후 * 저장 * 을 클릭합니다.

      IPv4 주소 *, * 게이트웨이 * 및 * 서브넷 * 필드가 자동으로 채워집니다. DHCP 서버가 MTU 값을 할당하도록 설정된 경우 * MTU * 필드가 해당 값으로 채워지고 필드는 읽기 전용이 됩니다.

      웹 브라우저가 자동으로 StorageGRID 어플라이언스 설치 프로그램의 새 IP 주소로 리디렉션됩니다.

   b. 그리드 네트워크 서브넷 목록이 올바른지 확인합니다.

      그리드 서브넷이 있는 경우 그리드 네트워크 게이트웨이가 필요합니다. 지정된 모든 그리드 서브넷은 이

게이트웨이를 통해 연결할 수 있어야 합니다. 이러한 그리드 네트워크 서브넷은 StorageGRID 설치를 시작할 때 기본 관리 노드의 그리드 네트워크 서브넷 목록에도 정의되어 있어야 합니다.

> 기본 라우트는 나열되지 않습니다. 클라이언트 네트워크가 활성화되지 않은 경우 기본 라우트는 그리드 네트워크 게이트웨이를 사용합니다.

- 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
- 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

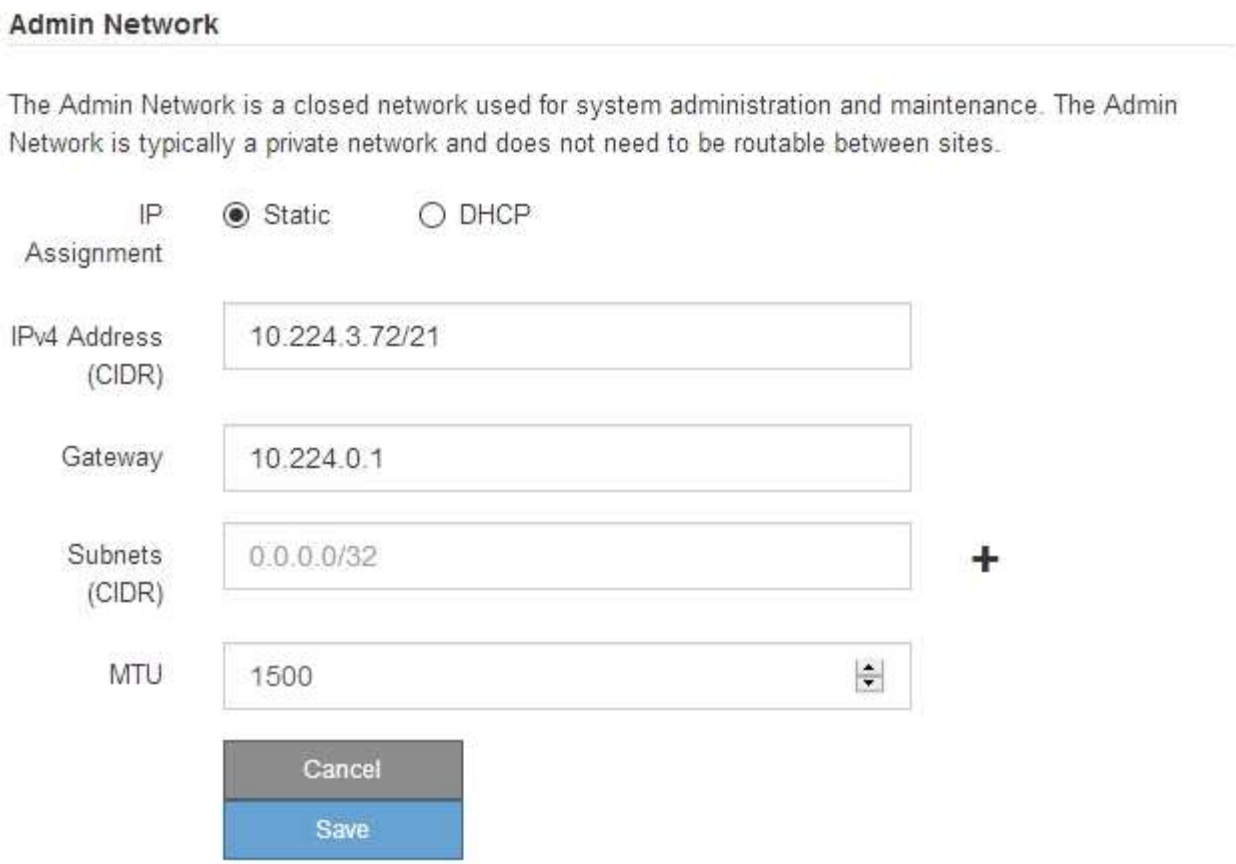
> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

> 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

a. 저장 * 을 클릭합니다.

5. 관리 네트워크를 구성하려면 페이지의 관리 네트워크 섹션에서 * 정적 * 또는 * DHCP * 를 선택합니다.

> 관리 네트워크를 구성하려면 링크 구성 페이지에서 관리 네트워크를 활성화해야 합니다.



6. 정적 * 을 선택한 경우 다음 단계에 따라 관리 네트워크를 구성합니다.
   a. 어플라이언스의 관리 포트 1에 대한 CIDR 표기법을 사용하여 정적 IPv4 주소를 입력합니다.

      관리 포트 1은 어플라이언스의 오른쪽 끝에 있는 2개의 1GbE RJ45 포트 왼쪽에 있습니다.

   b. 게이트웨이를 입력합니다.

      네트워크에 게이트웨이가 없는 경우 동일한 정적 IPv4 주소를 다시 입력합니다.

   c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

      > 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

   d. 저장 * 을 클릭합니다.

      IP 주소를 변경하면 게이트웨이와 서브넷 목록도 변경될 수 있습니다.

      StorageGRID 어플라이언스 설치 프로그램에 대한 연결이 끊어진 경우 방금 할당한 새 고정 IP 주소를 사용하여 URL을 다시 입력합니다. 예: + `https://services_appliance:8443*

   e. 관리자 네트워크 서브넷 목록이 올바른지 확인합니다.

      입력한 게이트웨이를 사용하여 모든 서브넷에 연결할 수 있는지 확인해야 합니다.

> 관리자 네트워크 게이트웨이를 사용하도록 기본 경로를 설정할 수 없습니다.

- 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
- 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

f. 저장 * 을 클릭합니다.

7. DHCP * 를 선택한 경우 다음 단계에 따라 관리 네트워크를 구성합니다.

a. DHCP * 라디오 버튼을 선택한 후 * 저장 * 을 클릭합니다.

IPv4 주소 *, * 게이트웨이 * 및 * 서브넷 * 필드가 자동으로 채워집니다. DHCP 서버가 MTU 값을 할당하도록 설정된 경우 * MTU * 필드가 해당 값으로 채워지고 필드는 읽기 전용이 됩니다.

웹 브라우저가 자동으로 StorageGRID 어플라이언스 설치 프로그램의 새 IP 주소로 리디렉션됩니다.

b. 관리자 네트워크 서브넷 목록이 올바른지 확인합니다.

입력한 게이트웨이를 사용하여 모든 서브넷에 연결할 수 있는지 확인해야 합니다.

> 관리자 네트워크 게이트웨이를 사용하도록 기본 경로를 설정할 수 없습니다.

- 서브넷을 추가하려면 삽입 아이콘을 클릭합니다 ➕ 마지막 항목 오른쪽에 있습니다.
- 사용하지 않는 서브넷을 제거하려면 삭제 아이콘을 클릭합니다 ✖.

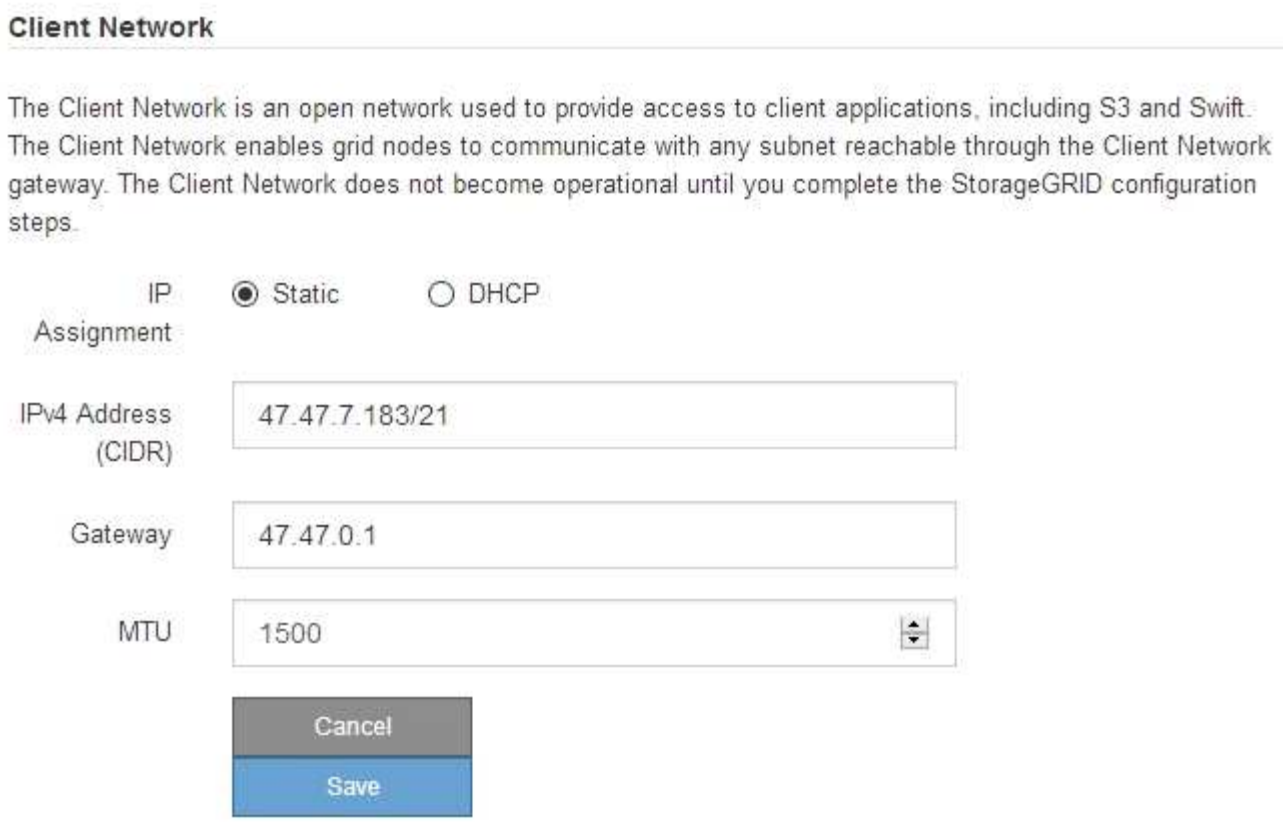
c. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

d. 저장 * 을 클릭합니다.

8. 클라이언트 네트워크를 구성하려면 페이지의 * 클라이언트 네트워크 * 섹션에서 * 정적 * 또는 * DHCP * 를 선택합니다.

> 클라이언트 네트워크를 구성하려면 링크 구성 페이지에서 클라이언트 네트워크를 활성화해야 합니다.



9. 정적 * 을 선택한 경우 다음 단계에 따라 클라이언트 네트워크를 구성합니다.
   a. CIDR 표기법을 사용하여 정적 IPv4 주소를 입력합니다.
   b. 저장 * 을 클릭합니다.
   c. 클라이언트 네트워크 게이트웨이의 IP 주소가 올바른지 확인합니다.

   > 클라이언트 네트워크가 활성화된 경우 기본 경로가 표시됩니다. 기본 라우트는 클라이언트 네트워크 게이트웨이를 사용하며 클라이언트 네트워크가 활성화된 동안에는 다른 인터페이스로 이동할 수 없습니다.

   d. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

   > 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

   e. 저장 * 을 클릭합니다.
10. DHCP * 를 선택한 경우 다음 단계에 따라 클라이언트 네트워크를 구성합니다.
   a. DHCP * 라디오 버튼을 선택한 후 * 저장 * 을 클릭합니다.

      IPv4 주소 * 및 * 게이트웨이 * 필드가 자동으로 채워집니다. DHCP 서버가 MTU 값을 할당하도록 설정된 경우 * MTU * 필드가 해당 값으로 채워지고 필드는 읽기 전용이 됩니다.

웹 브라우저가 자동으로 StorageGRID 어플라이언스 설치 프로그램의 새 IP 주소로 리디렉션됩니다.

a. 게이트웨이가 올바른지 확인합니다.

> 클라이언트 네트워크가 활성화된 경우 기본 경로가 표시됩니다. 기본 라우트는 클라이언트 네트워크 게이트웨이를 사용하며 클라이언트 네트워크가 활성화된 동안에는 다른 인터페이스로 이동할 수 없습니다.

b. 점보 프레임을 사용하려면 MTU 필드를 9000과 같은 점보 프레임에 적합한 값으로 변경합니다. 그렇지 않으면 기본값 1500을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

관련 정보

E5500SG 컨트롤러의 링크 구성을 변경합니다

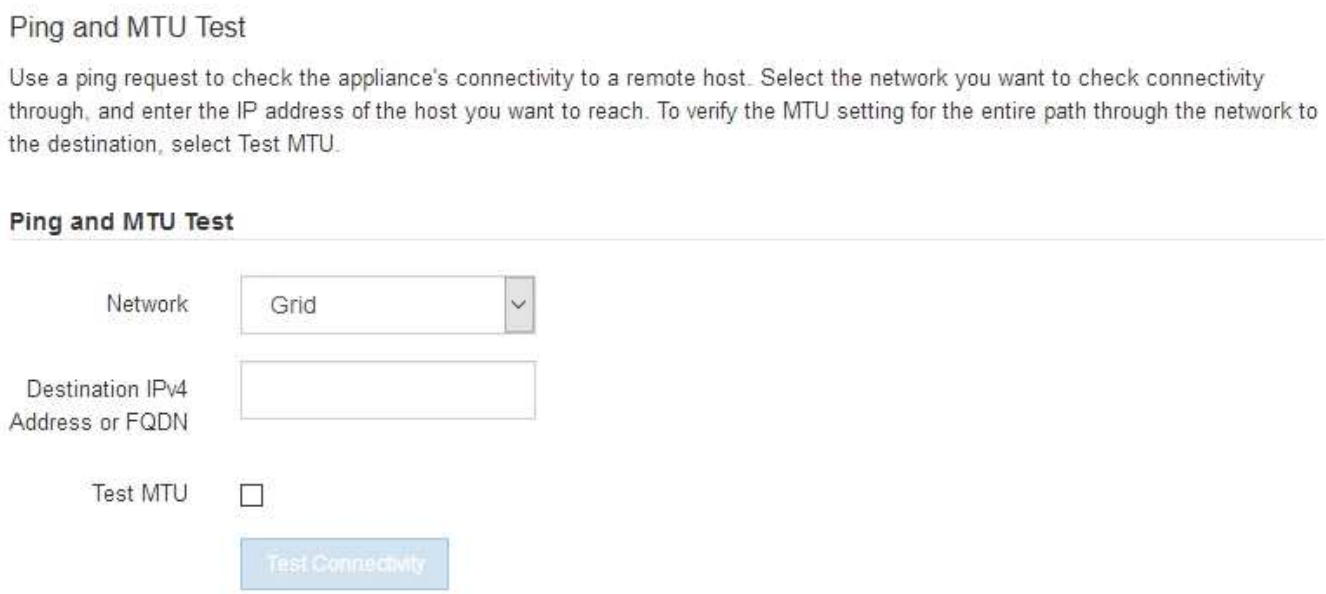
네트워크 연결을 확인합니다

어플라이언스에서 사용 중인 StorageGRID 네트워크에 액세스할 수 있는지 확인해야 합니다. 네트워크 게이트웨이를 통한 라우팅의 유효성을 검사하려면 StorageGRID 어플라이언스 설치 프로그램과 다른 서브넷의 IP 주소 간의 연결을 테스트해야 합니다. MTU 설정을 확인할 수도 있습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램의 메뉴 모음에서 * 네트워킹 구성 * > * Ping 및 MTU 테스트 * 를 클릭합니다.

   Ping 및 MTU 테스트 페이지가 나타납니다.



2. 네트워크 * 드롭다운 상자에서 테스트할 네트워크(그리드, 관리자 또는 클라이언트)를 선택합니다.
3. 해당 네트워크의 호스트에 대한 IPv4 주소 또는 FQDN(정규화된 도메인 이름)을 입력합니다.

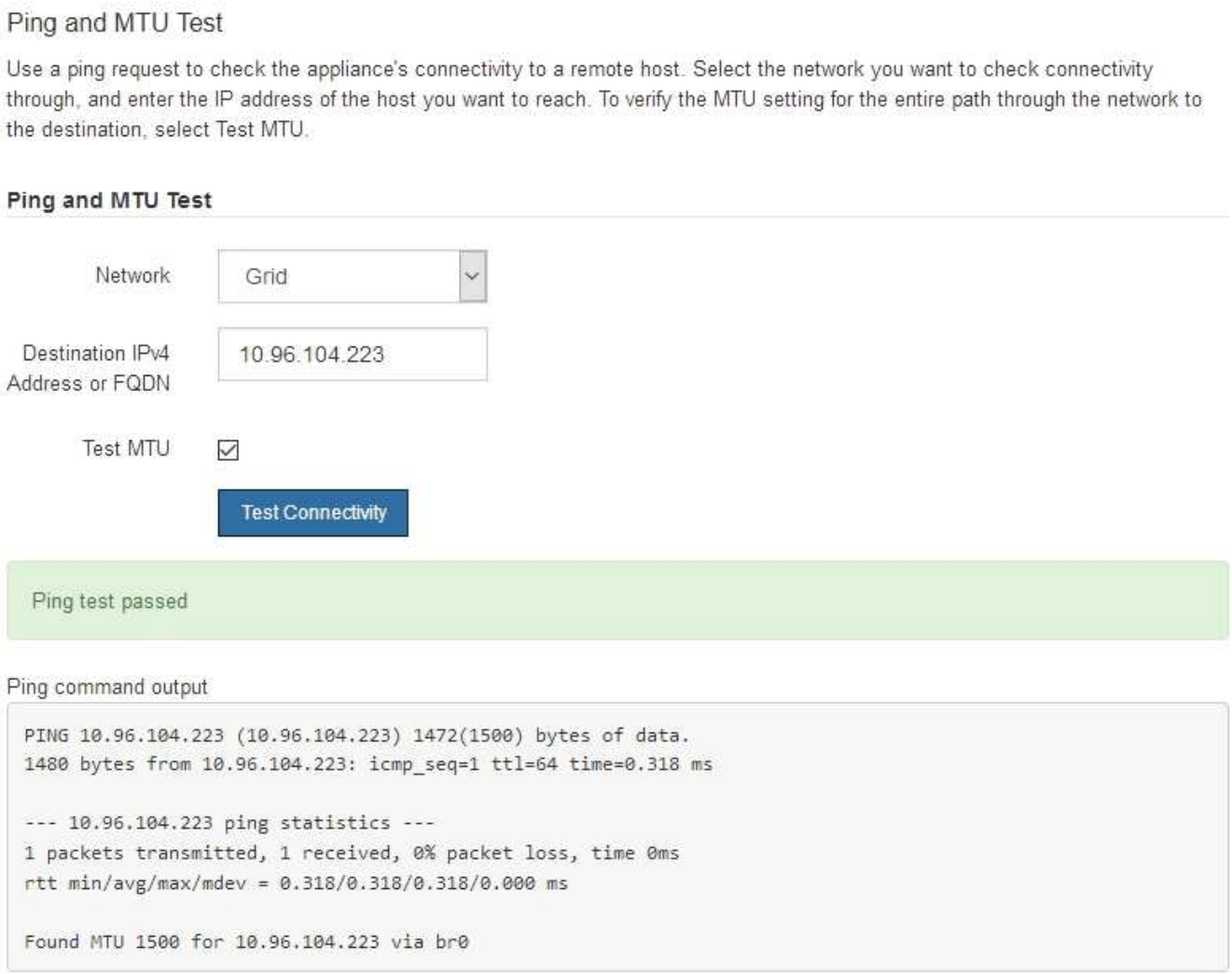
예를 들어 네트워크 또는 기본 관리 노드의 게이트웨이를 Ping할 수 있습니다.

4. 선택적으로 * Test MTU * 확인란을 선택하여 네트워크를 통해 대상으로 가는 전체 경로에 대한 MTU 설정을 확인합니다.

   예를 들어, 어플라이언스 노드와 다른 사이트의 노드 간 경로를 테스트할 수 있습니다.

5. 연결 테스트 * 를 클릭합니다.

   네트워크 연결이 유효한 경우 ping 명령 출력이 나열된 "Ping test Passed" 메시지가 나타납니다.



관련 정보

네트워크 링크 구성(SG5600)

MTU 설정을 변경합니다

포트 수준 네트워크 연결을 확인합니다

StorageGRID 어플라이언스 설치 프로그램과 다른 노드 간의 액세스가 방화벽에 의해 방해 받지 않도록 하려면 StorageGRID 어플라이언스 설치 관리자가 지정된 IP 주소 또는 주소 범위의

특정 TCP 포트 또는 포트 집합에 연결할 수 있는지 확인합니다.

이 작업에 대해

StorageGRID 어플라이언스 설치 프로그램에 제공된 포트 목록을 사용하여 어플라이언스와 그리드 네트워크의 다른 노드 간의 연결을 테스트할 수 있습니다.

또한 외부 NFS 또는 DNS 서버에 사용되는 것과 같은 UDP 포트와 Admin 및 Client Networks에서 연결을 테스트할 수 있습니다. 이러한 포트 목록은 StorageGRID 네트워킹 지침의 포트 참조를 참조하십시오.

> 포트 연결 테이블에 나열된 그리드 네트워크 포트는 StorageGRID 버전 11.6.0에만 유효합니다. 각 노드 유형에 맞는 포트를 확인하려면 사용 중인 StorageGRID 버전에 대한 네트워킹 지침을 항상 참조해야 합니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * 포트 연결 테스트(nmap) * 를 클릭합니다.

   포트 연결 테스트 페이지가 나타납니다.

   포트 연결 표에는 그리드 네트워크에서 TCP 연결이 필요한 노드 유형이 나와 있습니다. 각 노드 유형에 대해 표에는 어플라이언스에 액세스할 수 있어야 하는 그리드 네트워크 포트가 나열되어 있습니다.

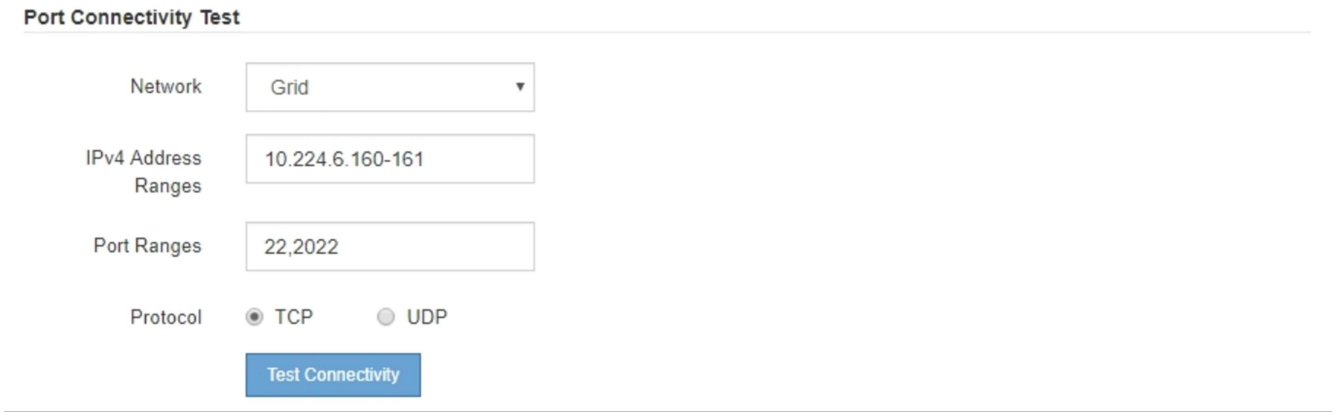
   표에 나열된 어플라이언스 포트와 그리드 네트워크의 다른 노드 간의 연결을 테스트할 수 있습니다.

2. Network * (네트워크 **)** 드롭다운에서 *** Grid * (**그리드 ***), * Admin * (** 관리자 *) 또는 * Client * (클라이언트 *)와 같이 테스트할 네트워크를 선택합니다.
3. 해당 네트워크의 호스트에 대한 IPv4 주소 범위를 지정합니다.

   예를 들어 네트워크 또는 기본 관리 노드의 게이트웨이를 조사할 수 있습니다.

   예제에 표시된 대로 하이픈을 사용하여 범위를 지정합니다.

4. TCP 포트 번호, 쉼표로 구분된 포트 목록 또는 포트 범위를 입력합니다.



5. 연결 테스트 * 를 클릭합니다.

   - 선택한 포트 수준 네트워크 연결이 유효하면 ""포트 연결 테스트 통과"" 메시지가 녹색 배너에 나타납니다. nmap 명령 출력은 배너 아래에 나열되어 있습니다.

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- 원격 호스트에 대한 포트 수준 네트워크 연결이 이루어졌지만 호스트가 선택한 포트 중 하나 이상의 포트에서 수신 대기 중이 아니면 ""포트 연결 테스트 실패" 메시지가 노란색 배너에 나타납니다. nmap 명령 출력은 배너 아래에 나열되어 있습니다.

  호스트가 청취하지 않는 모든 원격 포트는 ""닫힘"" 상태입니다. 예를 들어 연결하려는 노드가 사전 설치된 상태이고 StorageGRID NMS 서비스가 아직 실행되지 않은 경우 이 노란색 배너가 나타날 수 있습니다.

Port connectivity test failed
Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
1504/tcp closed evb-elm
1505/tcp open   funkproxy
1506/tcp open   utcd
1508/tcp open   diagmond
7443/tcp open   oracleas-https
9999/tcp open   abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- 하나 이상의 선택한 포트에 대해 포트 수준 네트워크 연결을 설정할 수 없는 경우 빨간색 배너에 ""포트 연결 테스트 실패" 메시지가 나타납니다. nmap 명령 출력은 배너 아래에 나열되어 있습니다.

  빨간색 배너는 원격 호스트의 포트에 대한 TCP 연결 시도가 이루어졌지만 보낸 사람에게 반환된 것이 없음을 나타냅니다. 응답이 반환되지 않으면 포트에 "필터링된" 상태가 있으며 방화벽에 의해 차단될 수 있습니다.

  ⓘ 폐쇄된 항만 목록에 있다.

Port connectivity test failed
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT     STATE    SERVICE
22/tcp   open     ssh
79/tcp   filtered finger
80/tcp   open     http
443/tcp  open     https
1504/tcp closed   evb-elm
1505/tcp open     funkproxy
1506/tcp open     utcd
1508/tcp open     diagmond
7443/tcp open     oracleas-https
9999/tcp open     abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

관련 정보

네트워킹 지침

SANtricity 스토리지 관리자를 구성합니다

SANtricity 스토리지 관리자를 사용하여 StorageGRID 어플라이언스에서 스토리지 디스크 및 하드웨어 구성 요소의 상태를 모니터링할 수 있습니다. 이 소프트웨어에 액세스하려면 E2700 컨트롤러(어플라이언스의 스토리지 컨트롤러)의 관리 포트 1의 IP 주소를 알아야 합니다.

E2700 컨트롤러의 IP 주소를 설정합니다

E2700 컨트롤러의 관리 포트 1은 SANtricity 스토리지 관리자를 위한 관리 네트워크에 어플라이언스를 연결합니다. StorageGRID 어플라이언스의 하드웨어 및 컨트롤러 펌웨어에 대한 관리 연결이 끊어지지 않도록 하려면 E2700 컨트롤러의 정적 IP 주소를 설정해야 합니다.

필요한 것

을(를) 사용하고 있습니다 지원되는 웹 브라우저.

이 작업에 대해

DHCP 할당 주소는 언제든지 변경될 수 있습니다. 고정 IP 주소를 컨트롤러에 할당하여 일관성 있는 접근성을 보장합니다.

단계

1. 클라이언트에서 StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다. + `https://E5600SG_Controller_IP:8443*`

   '*E600SG_Controller_IP*'의 경우 StorageGRID 네트워크에서 어플라이언스의 IP 주소를 사용합니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 하드웨어 구성 * > * 스토리지 컨트롤러 네트워크 구성 * 을 선택합니다.

스토리지 컨트롤러 네트워크 구성 페이지가 나타납니다.

3. 네트워크 구성에 따라 IPv4, IPv6 또는 둘 다에 대해 * Enabled * 를 선택합니다.
4. 자동으로 표시되는 IPv4 주소를 기록해 둡니다.

   DHCP는 이 포트에 IP 주소를 할당하는 기본 방법입니다.

   ⓘ DHCP 값이 나타나려면 몇 분 정도 걸릴 수 있습니다.

5. 선택적으로 E2700 컨트롤러 관리 포트의 정적 IP 주소를 설정합니다.

   ⓘ 관리 포트에 고정 IP를 할당하거나 DHCP 서버의 주소에 영구 임대를 할당해야 합니다.

   a. Static * 을 선택합니다.
   b. CIDR 표기법을 사용하여 IPv4 주소를 입력합니다.
   c. 기본 게이트웨이를 입력합니다.

   d. 저장 * 을 클릭합니다.

      변경 사항을 적용하는 데 몇 분 정도 걸릴 수 있습니다.

   SANtricity 저장소 관리자에 연결할 때 새 고정 IP 주소를 URL: + `https://*E2700_Controller_IP*` 사용합니다

관련 정보

"NetApp 문서: SANtricity 스토리지 관리자"

SANtricity 스토리지 관리자에 어플라이언스를 추가합니다

어플라이언스의 E2700 컨트롤러를 SANtricity 스토리지 관리자에 연결한 다음 어플라이언스를 스토리지 어레이로 추가합니다.

필요한 것

을(를) 사용하고 있습니다 지원되는 웹 브라우저.

이 작업에 대해

자세한 내용은 SANtricity 스토리지 관리자 설명서를 참조하십시오.

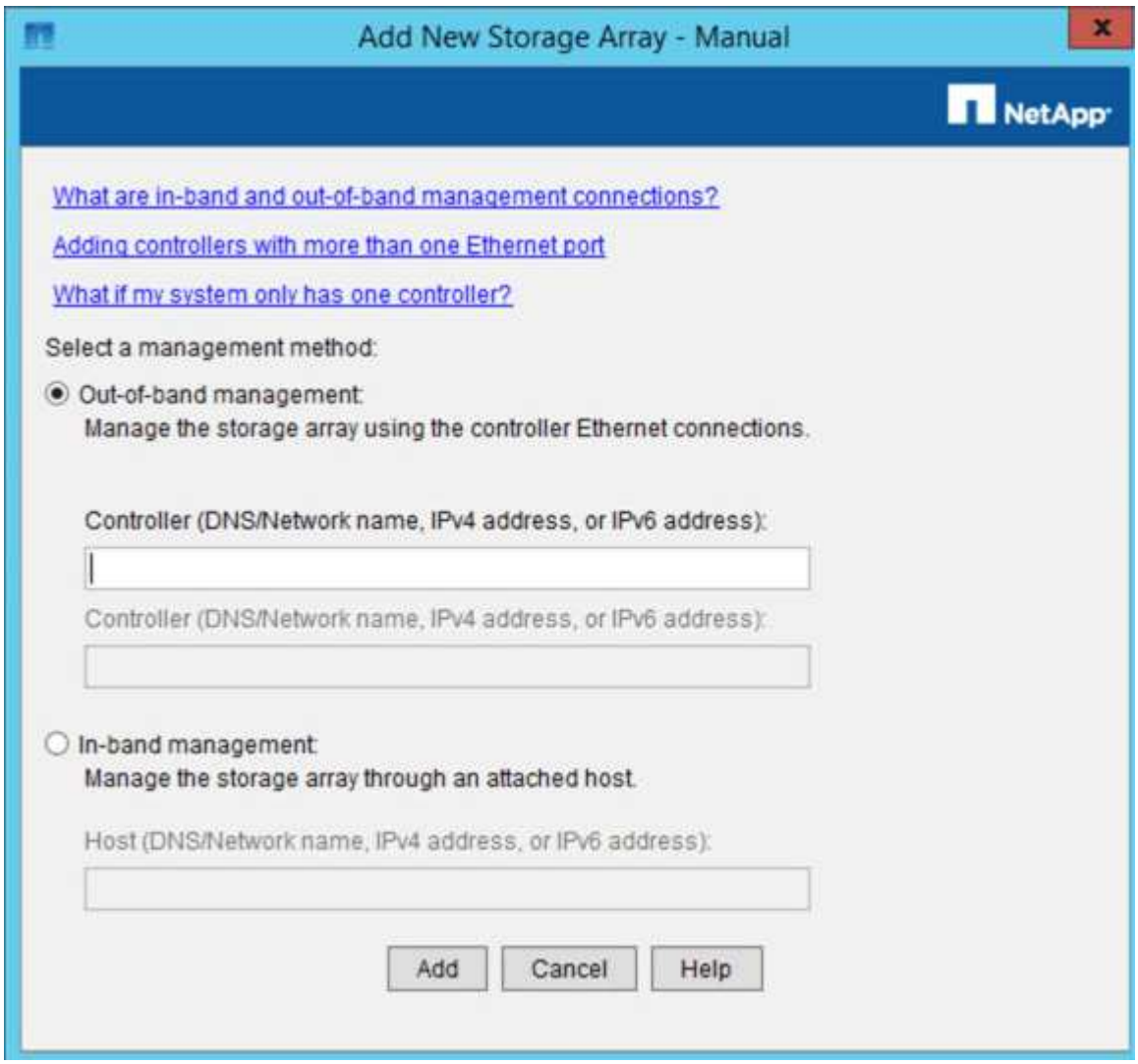
단계

1. 웹 브라우저를 열고 IP 주소를 SANtricity 저장소 관리자(+' * https://*E2700_Controller_IP**`)의 URL로 입력합니다

   SANtricity 스토리지 관리자의 로그인 페이지가 나타납니다.

2. 추가 방법 선택 * 페이지에서 * 수동 * 을 선택하고 * 확인 * 을 클릭합니다.
3. Edit * > * Add Storage Array * 를 선택합니다.

   Add New Storage Array - Manual 페이지가 나타납니다.



4. 대역외 관리 * 상자에 다음 값 중 하나를 입력합니다.
   - * DHCP 사용: * DHCP 서버가 E2700 컨트롤러의 관리 포트 1에 할당한 IP 주소입니다

- [DHCP를 사용하지 않음: * ' 192.168.128.101'

> 어플라이언스의 컨트롤러 중 하나만 SANtricity 스토리지 관리자에 연결되므로 하나의 IP 주소만 입력하면 됩니다.

5. 추가 * 를 클릭합니다.

관련 정보

"NetApp 문서: SANtricity 스토리지 관리자"

SANtricity 저장소 관리자를 설정합니다

SANtricity 저장소 관리자에 액세스한 후 이를 사용하여 하드웨어 설정을 구성할 수 있습니다. 일반적으로 StorageGRID 시스템에서 어플라이언스를 스토리지 노드로 구축하기 전에 이러한 설정을 구성합니다.

AutoSupport를 구성합니다

AutoSupport 도구는 어플라이언스에서 고객 지원 번들의 데이터를 수집하고 자동으로 기술 지원 부서에 전송합니다. AutoSupport를 구성하면 원격 문제 해결 및 문제 분석에 대한 기술 지원을 받을 수 있습니다.

필요한 것

- 제품에서 AutoSupport 기능을 활성화 및 활성화해야 합니다.

  AutoSupport 기능은 저장소 관리 스테이션에서 전역적으로 활성화 및 비활성화됩니다.

- Storage Manager 이벤트 모니터는 어플라이언스에 액세스할 수 있는 하나 이상의 시스템에서 실행되고 있어야 하며, 둘 이상의 시스템에서 실행하는 것이 좋습니다.

이 작업에 대해

모든 데이터는 사용자가 지정한 위치에서 압축된 단일 아카이브 파일 형식(.7z)으로 압축됩니다.

AutoSupport에서는 다음과 같은 유형의 메시지를 제공합니다.

메시지 유형	설명
이벤트 메시지	• 관리 대상 어플라이언스에서 지원 이벤트가 발생할 때 발송됩니다 • 시스템 구성 및 진단 정보를 포함합니다
매일 메시지	• 사용자가 구성할 수 있는 시간 간격 동안 매일 어플라이언스 현지 시간에 한 번씩 전송됩니다 • 현재 시스템 이벤트 로그 및 성능 데이터를 포함합니다

메시지 유형	설명
주간 메시지	• 사용자가 구성할 수 있는 시간 간격 동안 매주 한 번씩 제품의 현지 시간으로 전송됩니다 • 구성 및 시스템 상태 정보를 포함합니다

단계

1. SANtricity 스토리지 관리자의 엔터프라이즈 관리 창에서 * 장치 * 탭을 선택한 다음 * 검색된 스토리지 배열 * 을 선택합니다.
2. 도구 * > * AutoSupport * > * 구성 * 을 선택합니다.
3. 필요한 경우 SANtricity 스토리지 관리자 온라인 도움말을 사용하여 작업을 완료합니다.

관련 정보

"NetApp 문서: SANtricity 스토리지 관리자"

AutoSupport 수령 확인

기술 지원 부서에서 AutoSupport 메시지를 수신하고 있는지 확인해야 합니다. 시스템에 대한 AutoSupport의 상태는 Active IQ 포털에서 확인할 수 있습니다. 이러한 메시지가 수신되었는지 확인하면 도움이 필요한 경우 기술 지원 부서에서 귀하의 정보를 확인할 수 있습니다.

이 작업에 대해

AutoSupport는 다음 상태 중 하나를 표시할 수 있습니다.

- * 켜짐 *

  켜짐 상태는 기술 지원 부서에서 현재 시스템에서 AutoSupport 메시지를 수신하고 있음을 나타냅니다.

- * 꺼짐 *

  꺼짐 상태는 지난 15일 동안 기술 지원 부서에서 시스템으로부터 주간 로그를 수신하지 못했거나 환경 또는 구성(예:)이 변경되었을 수 있기 때문에 AutoSupport를 사용하지 않도록 설정했을 수 있음을 나타냅니다.

- * 거절 *

  거부 상태는 기술 지원 부서에 AutoSupport를 활성화하지 않을 것이라는 알림을 전달했음을 의미합니다.

기술 지원 부서에서 시스템에서 주별 로그를 수신하면 AutoSupport 상태가 On으로 변경됩니다.

단계

1. NetApp Support 사이트 로 이동합니다 "mysupport.netapp.com"Active IQ 포털에 로그인합니다.
2. AutoSupport 상태가 OFF인 상태에서 잘못된 것으로 판단될 경우 다음을 수행하십시오.
   a. 시스템 구성을 확인하여 AutoSupport가 켜져 있는지 확인합니다.
   b. 네트워크 환경 및 구성을 확인하여 시스템이 기술 지원 부서에 메시지를 보낼 수 있는지 확인합니다.

e-메일 및 **SNMP** 트랩 경고 알림을 구성합니다

SANtricity 스토리지 관리자는 어플라이언스 또는 해당 구성 요소 중 하나의 상태가 변경될 때 사용자에게 알릴 수 있습니다. 이를 알림 알림이라고 합니다. e-메일과 SNMP 트랩의 두 가지 방법으로 경고 알림을 받을 수 있습니다. 수신할 알림 알림을 구성해야 합니다.

단계

1. SANtricity 저장소 관리자의 엔터프라이즈 관리 창에서 * 장치 * 탭을 선택한 다음 노드를 선택합니다.
2. Edit * > * Configure Alerts * 를 선택합니다.
3. e-메일 알림 알림을 구성하려면 * e-메일 * 탭을 선택합니다.
4. SNMP 트랩 경고 알림을 구성하려면 * SNMP * 탭을 선택합니다.
5. 필요한 경우 SANtricity 스토리지 관리자 온라인 도움말을 사용하여 작업을 완료합니다.

SANtricity 저장소 관리자의 암호를 설정합니다

SANtricity 저장소 관리자에서 어플라이언스에 사용되는 암호를 설정할 수 있습니다. 암호를 설정하면 시스템 보안이 유지됩니다.

단계

1. SANtricity 스토리지 관리자의 엔터프라이즈 관리 창에서 컨트롤러를 두 번 클릭합니다.
2. Array Management 창에서 * Storage Array * 메뉴를 선택하고 * Security * > * Set Password * 를 선택합니다.
3. 암호를 구성합니다.
4. 필요한 경우 SANtricity 스토리지 관리자 온라인 도움말을 사용하여 작업을 완료합니다.

선택 사항**:** 노드 암호화를 활성화합니다

노드 암호화를 사용하는 경우 어플라이언스의 디스크는 물리적 손실 또는 사이트 제거로부터 보안 키 관리 서버(KMS) 암호화로 보호할 수 있습니다. 어플라이언스 설치 중에 노드 암호화를 선택하고 활성화해야 하며 KMS 암호화 프로세스가 시작되면 노드 암호화를 선택 취소할 수 없습니다.

필요한 것

StorageGRID 관리 지침에 따라 KMS에 대한 정보를 검토합니다.

이 작업에 대해

노드 암호화가 활성화된 어플라이언스는 StorageGRID 사이트에 대해 구성된 외부 키 관리 서버(KMS)에 연결됩니다. 각 KMS(또는 KMS 클러스터)는 사이트의 모든 어플라이언스 노드에 대한 암호화 키를 관리합니다. 이러한 키는 노드 암호화가 활성화된 어플라이언스에서 각 디스크의 데이터를 암호화하고 해독합니다.

KMS는 제품을 StorageGRID에 설치하기 전이나 설치한 후에 그리드 관리자에서 설정할 수 있습니다. 자세한 내용은 StorageGRID 관리 지침의 KMS 및 어플라이언스 구성에 대한 정보를 참조하십시오.

- KMS가 어플라이언스를 설치하기 전에 설정된 경우 어플라이언스에서 노드 암호화를 사용하도록 설정하고 KMS가 구성된 StorageGRID 사이트에 추가하면 KMS 제어 암호화가 시작됩니다.
- KMS가 어플라이언스를 설치하기 전에 설정되지 않은 경우 KMS가 구성되고 어플라이언스 노드가 포함된 사이트에

대해 사용 가능한 즉시 노드 암호화가 활성화된 각 어플라이언스에 대해 KMS 제어 암호화가 수행됩니다.

> 노드 암호화가 활성화된 어플라이언스에서 KMS에 연결하기 전에 존재하는 데이터는 안전하지 않은 임시 키로 암호화됩니다. KMS에서 제공하는 값으로 키를 설정할 때까지 제품은 제거 또는 도난으로부터 보호되지 않습니다.

디스크 암호를 해독하는 데 필요한 KMS 키가 없으면 어플라이언스의 데이터를 검색할 수 없으며 효과적으로 손실됩니다. 이 경우 암호 해독 키를 KMS에서 검색할 수 없습니다. KMS 구성을 지우거나, KMS 키가 만료되거나, KMS에 대한 연결이 끊어지거나, KMS 키가 설치된 StorageGRID 시스템에서 어플라이언스를 제거하면 이 키에 액세스할 수 없습니다.

단계

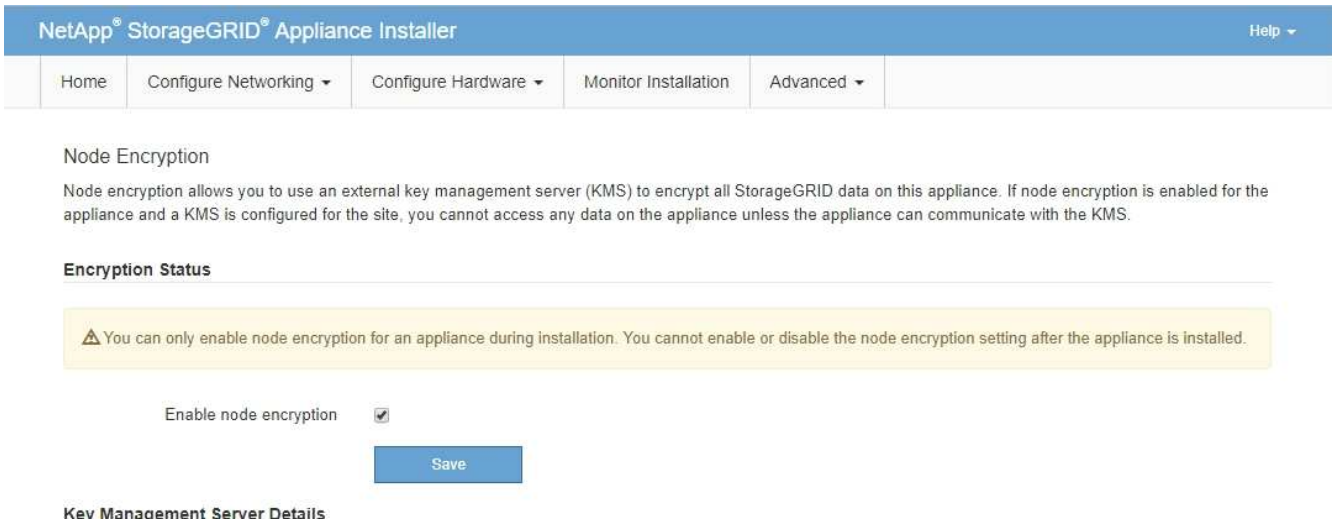
1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

   > KMS 키로 어플라이언스를 암호화한 후에는 동일한 KMS 키를 사용하지 않으면 어플라이언스 디스크를 해독할 수 없습니다.

2. 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.



3. 노드 암호화 사용 * 을 선택합니다.

   어플라이언스를 설치하기 전에 데이터 손실 위험 없이 * 노드 암호화 활성화 * 를 선택 취소할 수 있습니다. 설치가 시작되면 어플라이언스 노드가 StorageGRID 시스템의 KMS 암호화 키에 액세스하여 디스크 암호화를 시작합니다. 어플라이언스를 설치한 후에는 노드 암호화를 비활성화할 수 없습니다.

   > KMS가 있는 StorageGRID 사이트에 노드 암호화가 활성화된 어플라이언스를 추가한 후에는 해당 노드에 대해 KMS 암호화 사용을 중지할 수 없습니다.

4. 저장 * 을 선택합니다.

5. 어플라이언스를 StorageGRID 시스템에 노드로 구축하십시오.

   킬로미터 제어 암호화는 어플라이언스가 StorageGRID 사이트에 구성된 KMS 키에 액세스할 때 시작됩니다. KMS 암호화 프로세스 중에 설치 프로그램이 진행률 메시지를 표시합니다. 이 과정은 어플라이언스에 있는 디스크 볼륨 수에 따라 몇 분 정도 걸릴 수 있습니다.

   > 어플라이언스는 처음에 각 디스크 볼륨에 할당된 임의의 비 KMS 암호화 키로 구성됩니다. 이 디스크는 노드 암호화가 활성화된 어플라이언스가 StorageGRID 사이트에 구성된 KMS 키에 액세스할 때까지 안전하지 않은 임시 암호화 키를 사용하여 암호화됩니다.

작업을 마친 후

어플라이언스 노드가 유지보수 모드일 때 노드 암호화 상태, KMS 세부 정보 및 사용 중인 인증서를 볼 수 있습니다.

관련 정보

StorageGRID 관리

유지보수 모드(SG5600)에서 노드 암호화 모니터링

선택 사항**: RAID6** 모드로 변경**(SG5660**만 해당**)**

60개 드라이브가 포함된 SG5660을 사용하는 경우 볼륨 구성을 기본 권장 설정인 DDP(Dynamic Disk Pools)에서 RAID6로 변경할 수 있습니다. StorageGRID 어플라이언스 스토리지 노드를 구축하기 전에만 모드를 변경할 수 있습니다.

필요한 것

- SG5660을 이미 사용하고 있습니다. SG5612는 RAID6를 지원하지 않습니다. SG5612를 사용하는 경우 DDP 모드를 사용해야 합니다.

> 볼륨이 이미 구성되었거나 StorageGRID가 이전에 설치된 경우 RAID 모드를 변경하면 볼륨이 제거되고 교체됩니다. 해당 볼륨의 모든 데이터가 손실됩니다.

이 작업에 대해

StorageGRID 어플라이언스 스토리지 노드를 구축하기 전에 다음 두 가지 볼륨 구성 옵션 중에서 선택할 수 있습니다.

- * DDP(동적 디스크 풀) * — 기본값 및 권장 설정입니다. DDP는 향상된 하드웨어 데이터 보호 구성표로, 시스템 성능을 향상하고, 드라이브 장애 후 리빌드 시간을 단축하고, 관리를 간소화합니다.
- * RAID6 * — 이 시스템은 각 디스크의 패리티 스트라이프를 사용하는 하드웨어 보호 스키마로서, 데이터가 손실되기 전에 RAID 세트 내에서 2개의 디스크 장애를 허용합니다.

> 대부분의 StorageGRID 환경에서는 RAID6를 사용하지 않는 것이 좋습니다. RAID6는 스토리지 효율성을 DDP의 80%에 비해 88%까지 높일 수 있지만 DDP 모드는 드라이브 장애를 더욱 효율적으로 복구합니다.

단계

1. 서비스 랩톱을 사용하여 웹 브라우저를 열고 StorageGRID 어플라이언스 설치 프로그램: + `https://E5600SG_Controller_IP:8443* 액세스합니다

여기서, '*E600SG_Controller_IP*'는 E5500SG 컨트롤러의 IP 주소입니다.

2. 메뉴 모음에서 * 고급 * > * RAID 모드 * 를 선택합니다.
3. RAID 모드 구성 * 페이지의 모드 드롭다운 목록에서 * RAID6 * 을 선택합니다.
4. 저장 * 을 클릭합니다.

옵션**:** 어플라이언스인 네트워크 포트를 재활용합니다

어플라이언스 스토리지 노드의 내부 포트를 다른 외부 포트에 다시 매핑해야 할 수 있습니다. 예를 들어, 방화벽 문제로 인해 포트를 다시 매핑해야 할 수 있습니다.

필요한 것

- 이전에 StorageGRID 어플라이언스 설치 프로그램에 액세스했습니다.
- 로드 밸런서 엔드포인트를 구성하지 않았거나 구성하지 않을 계획입니다.

> 포트를 재매핑하는 경우 동일한 포트를 사용하여 로드 밸런서 끝점을 구성할 수 없습니다. 로드 밸런서 끝점을 구성하고 이미 포트를 다시 매핑하려면 의 단계를 따릅니다 포트 재맵을 제거합니다.

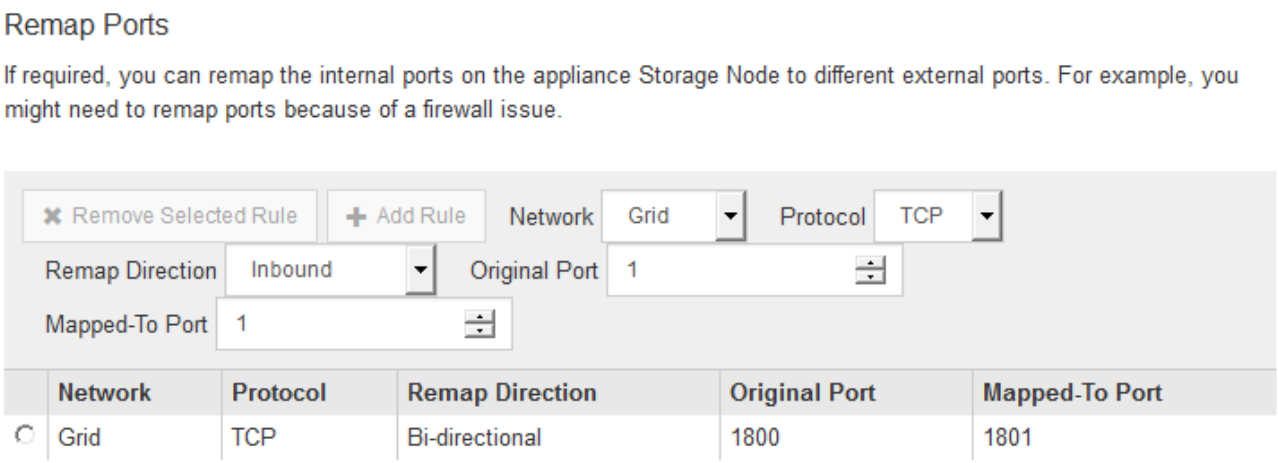
단계

1. StorageGRID 어플라이언스 설치 프로그램의 메뉴 모음에서 * 네트워킹 구성 * > * 재매핑 포트 * 를 클릭합니다.

   Remap Port(재매핑 포트) 페이지가 나타납니다.

2. 네트워크 * 드롭다운 상자에서 그리드, 관리자 또는 클라이언트 중 다시 매핑할 포트의 네트워크를 선택합니다.
3. 프로토콜 * 드롭다운 상자에서 IP 프로토콜(TCP 또는 UDP)을 선택합니다.
4. Remap Direction * (재매핑 방향 *) 드롭다운 상자에서 이 포트에 대해 재매핑할 트래픽 방향(Inbound, Outbound 또는 Bi-directional)을 선택합니다.
5. 원래 포트 * 의 경우 재매핑할 포트 번호를 입력합니다.
6. Mapped-to Port*의 경우 대신 사용할 포트 번호를 입력합니다.
7. 규칙 추가 * 를 클릭합니다.

   새 포트 매핑이 테이블에 추가되고 다시 매핑이 즉시 적용됩니다.



8. 포트 매핑을 제거하려면 제거할 규칙의 라디오 버튼을 선택하고 * 선택한 규칙 제거 * 를 클릭합니다.

관련 정보

복구 및 유지 관리

어플라이언스 스토리지 노드 구축

스토리지 어플라이언스를 설치 및 구성한 후 StorageGRID 시스템에서 스토리지 노드로 구축할 수 있습니다. 어플라이언스를 스토리지 노드로 배포할 때는 어플라이언스에 포함된 StorageGRID 어플라이언스 설치 프로그램을 사용합니다.

필요한 것

- 어플라이언스 노드를 클론 생성하는 경우 복구 및 유지 보수 프로세스를 계속 수행합니다.

  복구 및 유지 관리

- 이 제품은 랙 또는 캐비닛에 설치되었고 네트워크에 연결되어 있으며 전원이 켜져 있습니다.
- StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스에 대해 네트워크 링크, IP 주소 및 포트 재매핑(필요한 경우)이 구성되었습니다.
- 어플라이언스의 컴퓨팅 컨트롤러에 할당된 IP 주소 중 하나를 알고 있습니다. 연결된 모든 StorageGRID 네트워크에 대해 IP 주소를 사용할 수 있습니다.
- StorageGRID 시스템의 기본 관리 노드가 배포되었습니다.
- StorageGRID 어플라이언스 설치 프로그램의 IP 구성 페이지에 나열된 모든 그리드 네트워크 서브넷은 기본 관리 노드의 그리드 네트워크 서브넷 목록에 정의되어 있습니다.
- 지원되는 웹 브라우저가 있는 서비스 랩톱이 있습니다.

이 작업에 대해

각 스토리지 어플라이언스는 단일 스토리지 노드로 작동합니다. 모든 어플라이언스는 그리드 네트워크, 관리 네트워크 및 클라이언트 네트워크에 연결할 수 있습니다

어플라이언스 스토리지 노드를 StorageGRID 시스템에 배포하려면 StorageGRID 어플라이언스 설치 프로그램에 액세스하여 다음 단계를 수행합니다.

- 운영 관리 노드의 IP 주소와 스토리지 노드의 이름을 지정하거나 확인합니다.
- 구축을 시작하고 볼륨이 구성되고 소프트웨어가 설치될 때까지 기다립니다.
- 어플라이언스 설치 작업이 중간에 일시 중지되면 그리드 관리자에 로그인하고 모든 그리드 노드를 승인하고 StorageGRID 설치 및 배포 프로세스를 완료하여 설치를 다시 시작합니다.

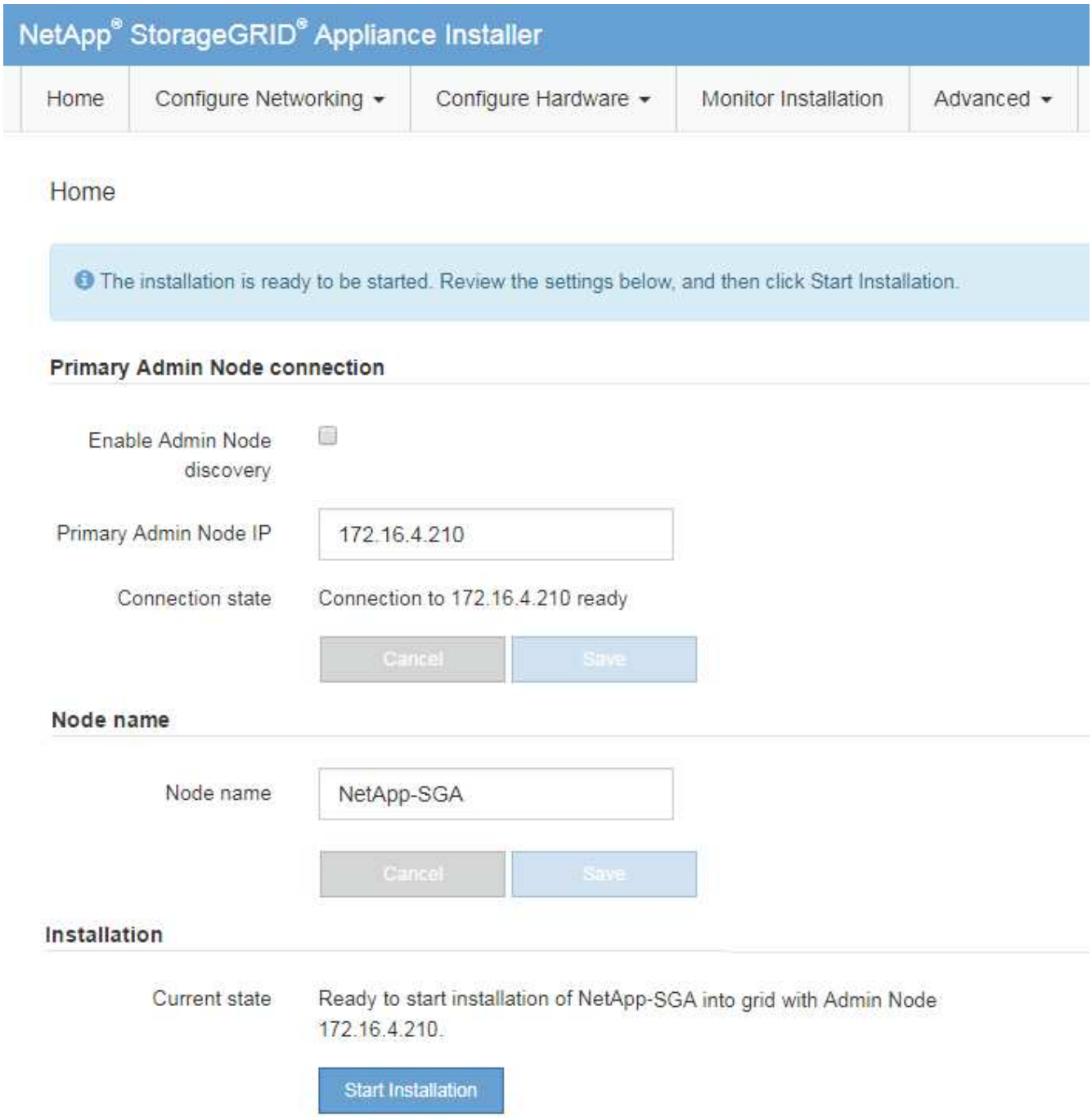
> 한 번에 여러 어플라이언스 노드를 구축해야 하는 경우 'configure-sGA.py' 어플라이언스 설치 스크립트를 사용하여 설치 프로세스를 자동화할 수 있습니다.

- 확장 또는 복구 작업을 수행하는 경우 해당 지침을 따르십시오.
  - 기존 StorageGRID 시스템에 어플라이언스 스토리지 노드를 추가하려면 StorageGRID 시스템 확장 지침을 참조하십시오.
  - 복구 작업의 일부로 어플라이언스 스토리지 노드를 배포하려면 복구 및 유지 관리 지침을 참조하십시오.

단계

1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.



2. Primary Admin Node* 연결 섹션에서 기본 관리 노드의 IP 주소를 지정해야 하는지 여부를 확인합니다.

   이전에 이 데이터 센터에 다른 노드를 설치한 경우 StorageGRID 어플라이언스 설치 관리자는 기본 관리 노드 또는 admin_IP가 구성된 다른 그리드 노드가 동일한 서브넷에 있다고 가정하여 이 IP 주소를 자동으로 검색할 수 있습니다.

3. 이 IP 주소가 표시되지 않거나 변경해야 하는 경우 주소를 지정합니다.

옵션을 선택합니다	설명
수동 IP 입력	a. 관리자 노드 검색 사용 * 확인란의 선택을 취소합니다. b. IP 주소를 수동으로 입력합니다. c. 저장 * 을 클릭합니다. d. 새 IP 주소가 준비될 때까지 연결 상태를 기다립니다.
연결된 모든 운영 관리 노드의 자동 검색	a. 관리자 노드 검색 사용 * 확인란을 선택합니다. b. 검색된 IP 주소 목록이 표시될 때까지 기다립니다. c. 이 어플라이언스 스토리지 노드를 구축할 그리드의 기본 관리 노드를 선택합니다. d. 저장 * 을 클릭합니다. e. 새 IP 주소가 준비될 때까지 연결 상태를 기다립니다.

4. 노드 이름 * 필드에 이 어플라이언스 노드에 사용할 이름을 입력하고 * 저장 * 을 클릭합니다.

   노드 이름은 StorageGRID 시스템의 이 어플라이언스 노드에 할당됩니다. 그리드 관리자의 노드 페이지(개요 탭)에 표시됩니다. 필요한 경우 노드를 승인할 때 이름을 변경할 수 있습니다.

5. 설치 섹션에서 현재 상태가 기본 관리 노드 '*admin_ip*'을(를) 사용하는 그리드에 '*node name*'의 설치를 시작할 준비가 되었으며 * 설치 시작 * 버튼이 활성화되어 있는지 확인합니다.

   설치 시작 * 버튼이 활성화되지 않은 경우 네트워크 구성 또는 포트 설정을 변경해야 할 수 있습니다. 자세한 내용은 제품의 설치 및 유지보수 지침을 참조하십시오.

   > 스토리지 노드 어플라이언스를 노드 클론 생성 타겟으로 구축하는 경우 여기서 구축 프로세스를 중지하고 복구 및 유지 관리에서 노드 클론 생성 절차를 계속 진행하십시오.

   복구 및 유지 관리

6. StorageGRID 어플라이언스 설치 관리자 홈 페이지에서 * 설치 시작 * 을 클릭합니다.

   현재 상태가 ""설치 진행 중""으로 변경되고 모니터 설치 페이지가 표시됩니다.

   > 모니터 설치 페이지에 수동으로 액세스해야 하는 경우 * 모니터 설치 * 를 클릭합니다.

7. 그리드에 여러 어플라이언스 스토리지 노드가 포함된 경우 각 어플라이언스에 대해 이 단계를 반복합니다.

   > 한 번에 여러 어플라이언스 스토리지 노드를 구축해야 하는 경우 'configure-sGA.py' 어플라이언스 설치 스크립트를 사용하여 설치 프로세스를 자동화할 수 있습니다.

관련 정보

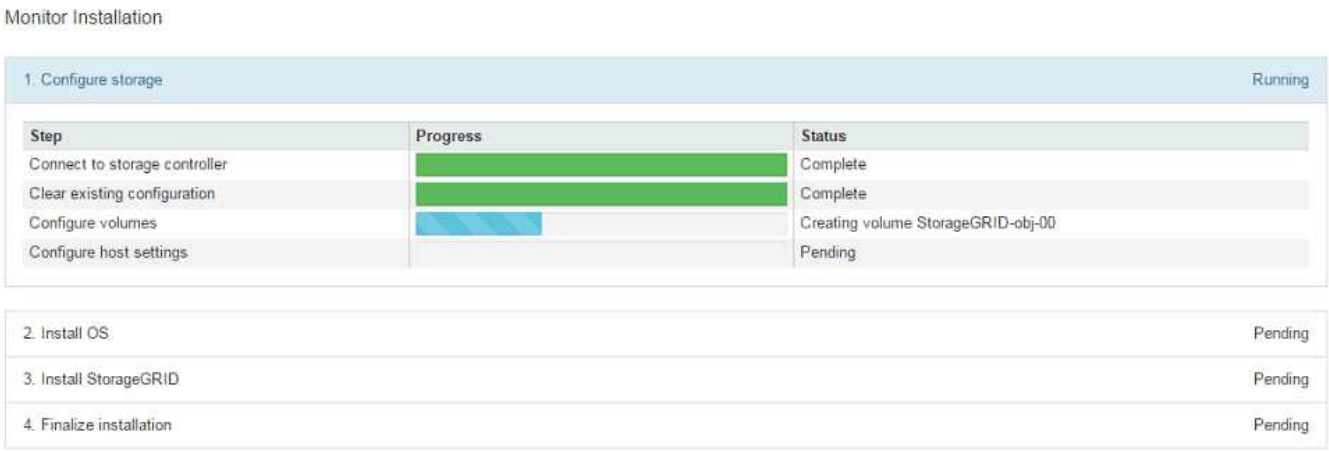
스토리지 어플라이언스 설치를 모니터링합니다

StorageGRID 어플라이언스 설치 프로그램은 설치가 완료될 때까지 상태를 제공합니다. 소프트웨어 설치가 완료되면 어플라이언스가 재부팅됩니다.

단계

1. 설치 진행률을 모니터링하려면 * 모니터 설치 * 를 클릭합니다.

   Monitor Installation(모니터 설치) 페이지에 설치 진행률이 표시됩니다.

   파란색 상태 표시줄은 현재 진행 중인 작업을 나타냅니다. 녹색 상태 표시줄은 성공적으로 완료된 작업을 나타냅니다.

   > 설치 프로그램은 이전 설치에서 완료된 작업이 다시 실행되지 않도록 합니다. 설치를 다시 실행할 경우 다시 실행할 필요가 없는 작업은 녹색 상태 표시줄과 "중단" 상태로 표시됩니다.

2. 처음 두 설치 단계의 진행 상황을 검토합니다.

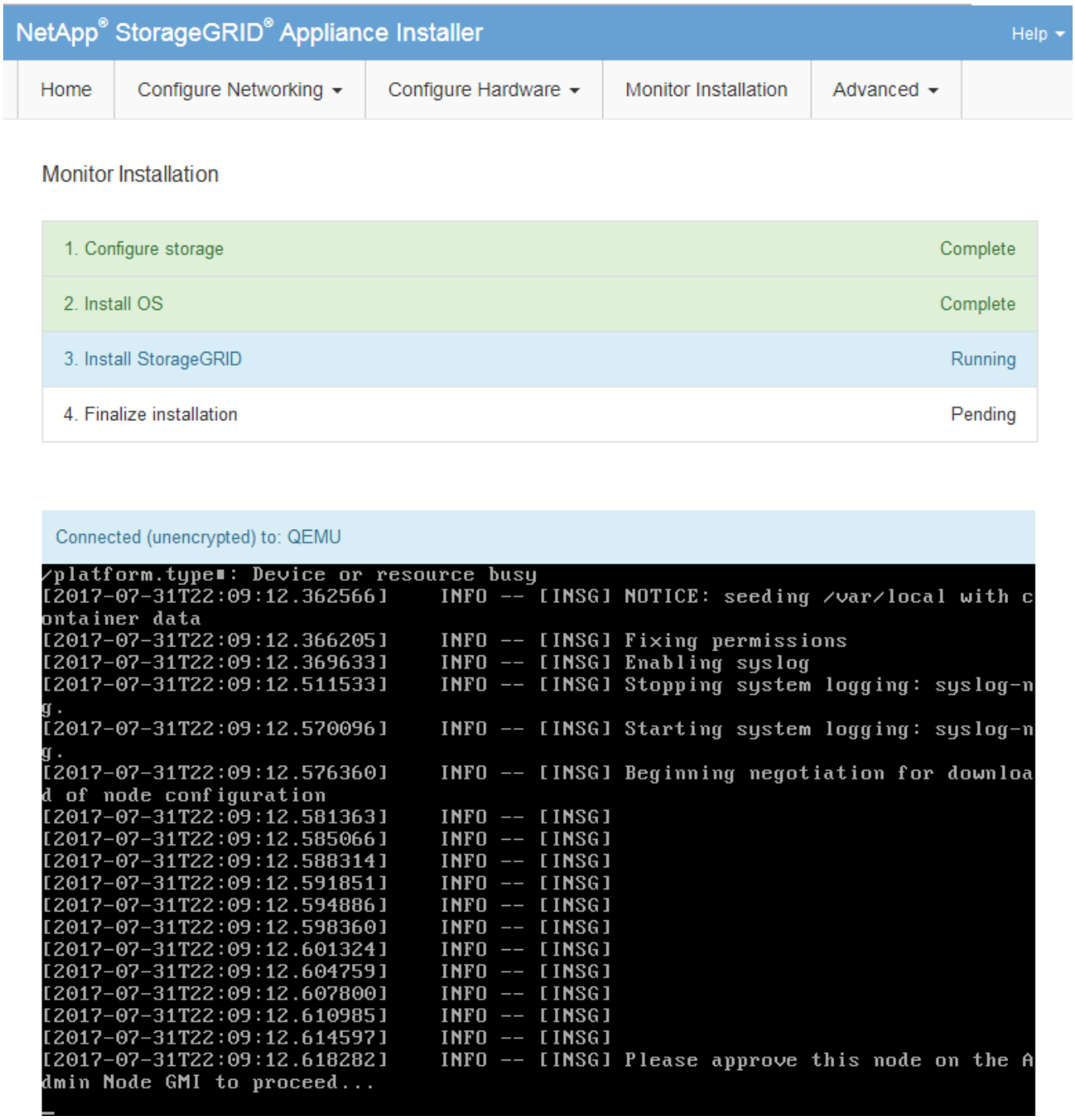
   - 1. 스토리지 구성 *

     이 단계에서 설치 관리자는 스토리지 컨트롤러에 연결하고, 기존 구성을 지우고, SANtricity 소프트웨어와 통신하여 볼륨을 구성하고, 호스트 설정을 구성합니다.

   - 2. OS * 를 설치합니다

   이 단계에서 설치 프로그램은 StorageGRID의 기본 운영 체제 이미지를 어플라이언스에 복사합니다.

3. StorageGRID* 설치 단계가 일시 중지되고 그리드 관리자를 사용하여 관리 노드에서 이 노드를 승인하라는 메시지가 포함된 콘솔에 표시될 때까지 설치 진행 상태를 계속 모니터링합니다. 다음 단계로 이동합니다.



4. 운영 관리 노드의 그리드 관리자로 이동하여 보류 중인 스토리지 노드를 승인하고 StorageGRID 설치 프로세스를 완료합니다.

   Grid Manager에서 * Install * 을 클릭하면 단계 3이 완료되고 단계 4, * 설치 완료 * 가 시작됩니다. 4단계가 완료되면 컨트롤러가 재부팅됩니다.

어플라이언스 설치 및 구성 자동화(SG5600)

어플라이언스의 설치 및 구성과 전체 StorageGRID 시스템의 구성을 자동화할 수 있습니다.

이 작업에 대해

설치 및 구성 자동화는 여러 StorageGRID 인스턴스 또는 하나의 크고 복잡한 StorageGRID 인스턴스를 구축하는 데 유용할 수 있습니다.

설치 및 구성을 자동화하려면 다음 옵션 중 하나 이상을 사용하십시오.

- 어플라이언스의 구성 설정을 지정하는 JSON 파일을 생성합니다. StorageGRID 어플라이언스 설치 프로그램을 사용하여 JSON 파일을 업로드합니다.

  동일한 파일을 사용하여 여러 어플라이언스를 구성할 수 있습니다.

- StorageGRID ``configure-sGA.py'' Python 스크립트를 사용하여 어플라이언스 구성을 자동화합니다.
- 추가 Python 스크립트를 사용하여 전체 StorageGRID 시스템의 다른 구성 요소("그리드")를 구성합니다.

  StorageGRID 자동화 Python 스크립트를 직접 사용하거나 직접 개발한 그리드 구축 및 구성 도구에서 StorageGRID 설치 REST API를 사용하는 방법의 예로 사용할 수 있습니다. 에 대한 정보를 참조하십시오 StorageGRID 설치 파일 다운로드 및 추출.

StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스 구성을 자동화합니다

구성 정보가 포함된 JSON 파일을 사용하여 어플라이언스 구성을 자동화할 수 있습니다. StorageGRID 어플라이언스 설치 프로그램을 사용하여 파일을 업로드합니다.

필요한 것

- 어플라이언스는 StorageGRID 11.5 이상과 호환되는 최신 펌웨어에 있어야 합니다.
- 를 사용하여 구성하는 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램에 연결되어 있어야 합니다 지원되는 웹 브라우저.

이 작업에 대해

다음과 같은 어플라이언스 구성 작업을 자동화할 수 있습니다.

- Grid Network, Admin Network 및 Client Network IP 주소입니다
- BMC 인터페이스
- 네트워크 링크
  - 포트 결합 모드
  - 네트워크 연결 모드
  - 링크 속도

업로드된 JSON 파일을 사용하여 어플라이언스를 구성하는 것이 StorageGRID 어플라이언스 설치 프로그램에서 여러 페이지를 사용하여 수동으로 구성하는 것보다 더 효율적인 경우가 많습니다. 특히 여러 노드를 구성해야 하는 경우 더욱 그렇습니다. 각 노드에 대해 한 번에 하나씩 구성 파일을 적용해야 합니다.

어플라이언스의 설치와 구성을 모두 자동화하려는 숙련된 사용자는 'configure-sGA.py' 스크립트를 사용할 수 있습니다. 를 누릅니다configure-sga.py 스크립트를 사용하여 어플라이언스 노드의 설치 및 구성을 자동화합니다

단계

1. 다음 방법 중 하나를 사용하여 JSON 파일을 생성합니다.
   - ConfigBuilder 응용 프로그램

     "ConfigBuilder.netapp.com"

   - 'configure-sGA.py' 어플라이언스 구성 스크립트 StorageGRID 어플라이언스 설치 프로그램(* 도움말*>* 어플라이언스 구성 스크립트*)에서 스크립트를 다운로드할 수 있습니다. configure-sga.py 스크립트를 사용하여 구성 자동화에 대한 지침을 참조하십시오.

     configure-sga.py 스크립트를 사용하여 어플라이언스 노드의 설치 및 구성을 자동화합니다

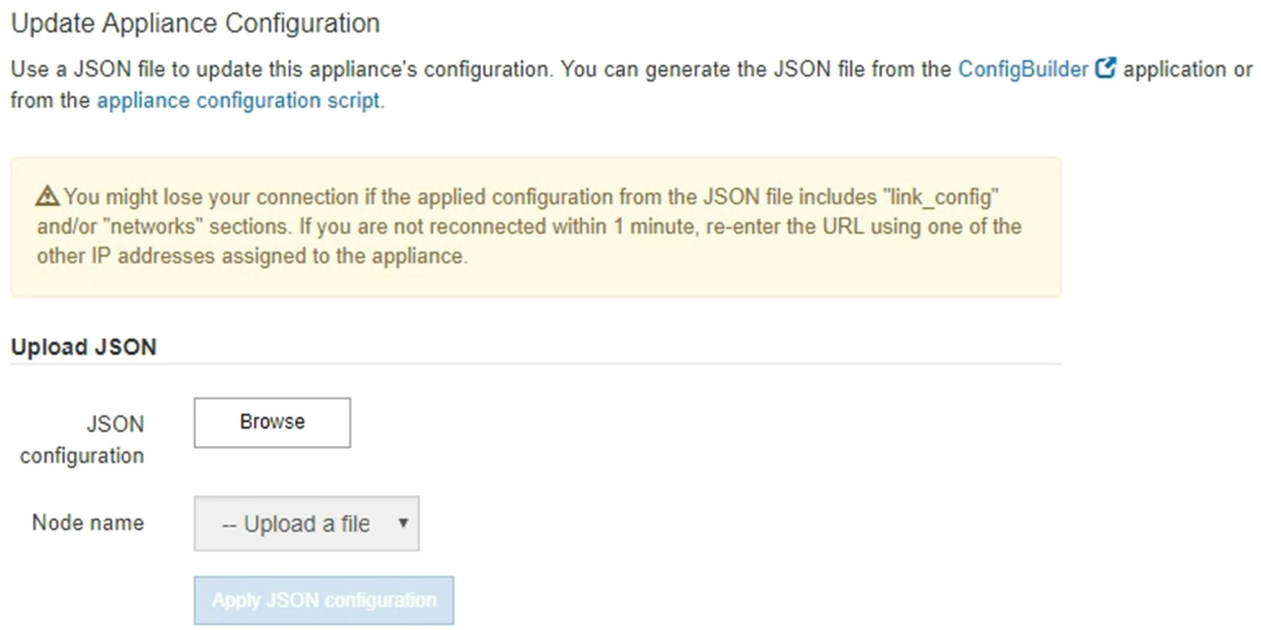
     JSON 파일의 노드 이름은 다음 요구사항을 충족해야 합니다.

     - 1자 이상 32자 이하의 유효한 호스트 이름이어야 합니다
     - 문자, 숫자 및 하이픈을 사용할 수 있습니다
     - 하이픈으로 시작하거나 끝날 수 없습니다
     - 숫자만 포함할 수 없습니다

     > JSON 파일의 노드 이름(최상위 이름)이 고유한지 확인하십시오. 그렇지 않으면 JSON 파일을 사용하여 둘 이상의 노드를 구성할 수 없습니다.

2. Advanced * > * Update Appliance Configuration * 을 선택합니다.

   어플라이언스 구성 업데이트 페이지가 나타납니다.

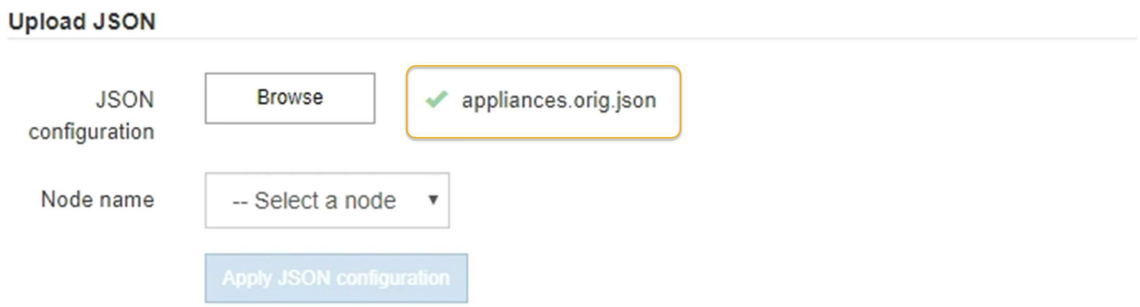


3. 업로드할 구성이 있는 JSON 파일을 선택합니다.
   a. 찾아보기 * 를 선택합니다.
   b. 파일을 찾아 선택합니다.

c. 열기 * 를 선택합니다.

파일이 업로드되고 검증됩니다. 유효성 검사 프로세스가 완료되면 녹색 확인 표시 옆에 파일 이름이 표시됩니다.

> JSON 파일의 구성에 "link_config", "networks" 또는 둘 다에 대한 섹션이 포함된 경우 어플라이언스에 대한 연결이 끊어질 수 있습니다. 1분 이내에 다시 연결되지 않으면 어플라이언스에 할당된 다른 IP 주소 중 하나를 사용하여 어플라이언스 URL을 다시 입력하십시오.

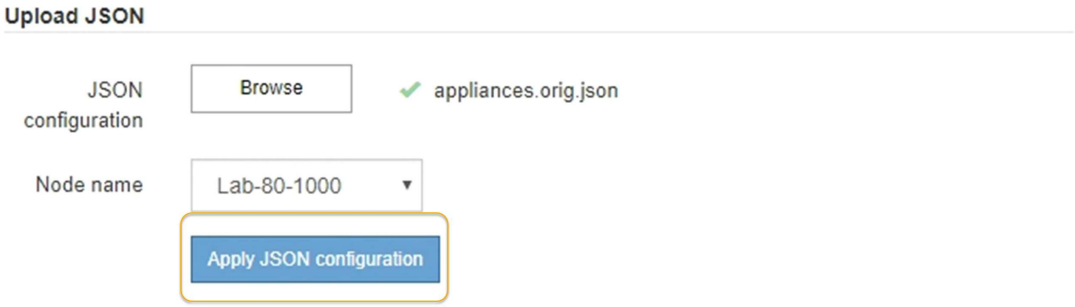


노드 이름 * 드롭다운은 JSON 파일에 정의된 최상위 노드 이름으로 채워집니다.

> 파일이 유효하지 않으면 파일 이름이 빨간색으로 표시되고 오류 메시지가 노란색 배너에 표시됩니다. 잘못된 파일이 어플라이언스에 적용되지 않습니다. ConfigBuilder를 사용하여 올바른 JSON 파일이 있는지 확인할 수 있습니다.

4. 노드 이름 * 드롭다운 목록에서 노드를 선택합니다.

   JSON 설정 적용 * 버튼이 활성화됩니다.



5. JSON 구성 적용 * 을 선택합니다.

   선택한 노드에 구성이 적용됩니다.

configure-sga.py 스크립트를 사용하여 어플라이언스 노드의 설치 및 구성을 자동화합니다

'configure-sGA.py' 스크립트를 사용하면 기본 관리 노드의 설치 및 구성을 포함하여 StorageGRID 어플라이언스 노드에 대한 많은 설치 및 구성 작업을 자동화할 수 있습니다. 이

스크립트는 구성할 어플라이언스가 많은 경우 유용할 수 있습니다. 또한 스크립트를 사용하여 어플라이언스 구성 정보가 포함된 JSON 파일을 생성할 수도 있습니다.

필요한 것

- 이 어플라이언스는 랙에 설치되어 있고 네트워크에 연결되어 있으며 전원이 켜져 있습니다.
- 네트워크 링크 및 IP 주소는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 기본 관리 노드에 대해 구성되었습니다.
- 기본 관리 노드를 설치하는 경우 해당 IP 주소를 알 수 있습니다.
- 다른 노드를 설치 및 구성하는 경우 기본 관리 노드가 배포되었으며 해당 IP 주소를 알고 있는 것입니다.
- 기본 관리 노드 이외의 모든 노드의 경우 StorageGRID 어플라이언스 설치 프로그램의 IP 구성 페이지에 나열된 모든 그리드 네트워크 서브넷이 기본 관리 노드의 그리드 네트워크 서브넷 목록에 정의되어 있습니다.
- 'configure-sGA.py' 파일을 다운로드했습니다. 이 파일은 설치 아카이브에 포함되어 있거나 StorageGRID 어플라이언스 설치 프로그램에서 * 도움말 * > * 어플라이언스 설치 스크립트 * 를 클릭하여 액세스할 수 있습니다.

> 이 절차는 명령줄 인터페이스를 사용하는 일부 경험이 있는 고급 사용자를 위한 것입니다. 또는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 구성을 자동화할 수도 있습니다. 를 누릅니다StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스 구성을 자동화합니다

단계

1. Python 스크립트를 실행하기 위해 사용 중인 Linux 시스템에 로그인합니다.
2. 스크립트 구문에 대한 일반적인 도움말과 사용 가능한 매개 변수 목록을 보려면 다음을 입력합니다.

   ```
   configure-sga.py --help
   ```

   'configure-sGA.py' 스크립트는 5개의 하위 명령을 사용합니다.

   - BMC 구성 및 어플라이언스의 현재 구성이 포함된 JSON 파일을 생성하는 등 고급 StorageGRID 어플라이언스 상호 작용을 위한 '고급' 기능입니다
   - RAID 모드, 노드 이름 및 네트워킹 매개 변수를 구성하기 위한 'configure'
   - StorageGRID 설치 시작을 위한 '설치'입니다
   - StorageGRID 설치 모니터링을 위한 모니터
   - 어플라이언스를 재부팅하기 위한 재부팅

   하위 명령(advanced, configure, install, monitor, reboot) 인수 뒤에 '--help' 옵션을 입력하면 해당 하위 명령 내에서 사용할 수 있는 옵션에 대한 자세한 내용을 제공하는 다른 도움말 텍스트가 표시됩니다. + "configure-sga.py_subcommand_—help

3. 어플라이언스 노드의 현재 구성을 확인하려면 다음과 같이 입력합니다. 여기서 "*SGA-INSTALL-IP*"는 어플라이언스 노드의 IP 주소 중 하나입니다. + "configure-sga.py configure_sGA-install-ip_

   이 결과는 기본 관리 노드의 IP 주소와 관리, 그리드 및 클라이언트 네트워크에 대한 정보를 포함하여 어플라이언스에 대한 현재 IP 정보를 표시합니다.

   ```
   Connecting to +https://10.224.2.30:8443+ (Checking version and
   ```

```
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200

  StorageGRID Appliance
    Name:        LAB-SGA-2-30
    Node type:   storage

  StorageGRID primary Admin Node
    IP:        172.16.1.170
    State:     unknown
    Message:   Initializing...
    Version:   Unknown

  Network Link Configuration
    Link Status
          Link      State      Speed (Gbps)
          ----      -----      -----
          1         Up         10
          2         Up         10
          3         Up         10
          4         Up         10
          5         Up         1
          6         Down       N/A

    Link Settings
        Port bond mode:      FIXED
        Link speed:          10GBE

        Grid Network:        ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

        Admin Network:       ENABLED
            Bonding mode:    no-bond
            MAC Addresses:   00:80:e5:29:70:f4
```

```
        Client Network:      ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

  Grid Network
    CIDR:      172.16.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:8A
    Gateway:   172.16.0.1
    Subnets:   172.17.0.0/21
               172.18.0.0/21
               192.168.0.0/21
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

#################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#################################################################
```

4. 현재 설정의 값을 변경해야 하는 경우 '설정' 하위 명령을 사용하여 값을 업데이트합니다. 예를 들어, 어플라이언스가 기본 관리 노드에 연결하기 위해 사용하는 IP 주소를 ' 172.16.2.99 '로 변경하려면 + ' configure-sga.py configure - -admin -ip 172.16.2.99_sga -install -ip_'를 입력합니다
5. 어플라이언스 구성을 JSON 파일로 백업하려면 고급 및 백업 파일 하위 명령을 사용하십시오. 예를 들어, IP 주소 '*SGA-INSTALL-IP*'를 사용하는 어플라이언스 구성을 어플라이언스-SG1000.json'이라는 파일에 백업하려면 + "configure-sga.py advanced—backup-file appliance-SG1000.json_sga-install-ip_"를 입력합니다

   구성 정보가 포함된 JSON 파일은 에서 스크립트를 실행한 디렉토리에 작성됩니다.

   > 생성된 JSON 파일의 최상위 노드 이름이 어플라이언스 이름과 일치하는지 확인하십시오. 숙련된 사용자이고 StorageGRID API에 대한 철저한 이해가 없는 경우 이 파일을 변경하지 마십시오.

6. 어플라이언스 구성이 만족스러우면 "install" 및 "monitor" 하위 명령을 사용하여 어플라이언스를 설치합니다. + "configure-sga.py install—monitor_sga-install-ip_"
7. 어플라이언스를 재부팅하려면 + "configure-sga.py reboot_sga-install-ip_"를 입력합니다

StorageGRID 구성 자동화

그리드 노드를 구축한 후 StorageGRID 시스템 구성을 자동화할 수 있습니다.

필요한 것

- 설치 아카이브에서 다음 파일의 위치를 알고 있습니다.

파일 이름	설명
configure-StorageGrid.py의 약어입니다	구성을 자동화하는 데 사용되는 Python 스크립트입니다
configure-StorageGrid.sample.json	스크립트와 함께 사용할 샘플 구성 파일
configure-StorageGrid.blank.json	스크립트에 사용할 빈 구성 파일입니다

- "configure-StorageGrid.json" 구성 파일을 만들었습니다. 이 파일을 만들려면 샘플 구성 파일('configure-StorageGrid.sample.json') 또는 빈 구성 파일('configure-StorageGrid.blank.json')을 수정할 수 있습니다.

이 작업에 대해

configure-StorageGrid.py Python 스크립트와 configure-StorageGrid.json 구성 파일을 사용하여 StorageGRID 시스템 구성을 자동화할 수 있습니다.

> 그리드 관리자 또는 설치 API를 사용하여 시스템을 구성할 수도 있습니다.

단계

1. Python 스크립트를 실행하기 위해 사용 중인 Linux 시스템에 로그인합니다.
2. 설치 아카이브를 추출한 디렉토리로 변경합니다.

   예: + 'cd StorageGRID-Webscale -*version/platform*

   여기서, 'platform'은 'dEBS', 'rpms', 'vSphere'입니다.

3. Python 스크립트를 실행하고 생성한 구성 파일을 사용합니다.

   예를 들면 다음과 같습니다.

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

작업을 마친 후

복구 패키지 '.zip' 파일은 구성 프로세스 중에 생성되며 설치 및 구성 프로세스를 실행 중인 디렉토리에 다운로드됩니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 백업해야 합니다. 예를 들어, 안전한 백업 네트워크 위치 및 안전한 클라우드 저장소 위치에 복사합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

임의 암호를 생성해야 한다고 지정한 경우 "passwords.txt" 파일을 추출하고 StorageGRID 시스템에 액세스하는 데 필요한 암호를 찾아야 합니다.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                  StorageGRID node recovery.                #####
######################################################################
```

확인 메시지가 표시되면 StorageGRID 시스템이 설치 및 구성됩니다.

```
StorageGRID has been configured and installed.
```

REST API 설치 개요

StorageGRID는 설치 작업을 수행하기 위한 두 가지 REST API, 즉 StorageGRID 설치 API와 StorageGRID 어플라이언스 설치 관리자 API를 제공합니다.

두 API 모두 Swagger 오픈 소스 API 플랫폼을 사용하여 API 문서를 제공합니다. swagger를 사용하면 개발자와 개발자가 아닌 사용자가 API가 매개 변수 및 옵션에 어떻게 응답하는지 보여주는 사용자 인터페이스에서 API와 상호 작용할 수 있습니다. 이 문서에서는 표준 웹 기술 및 JSON(JavaScript Object Notation) 데이터 형식에 대해 잘 알고 있다고 가정합니다.

> API Docs 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

각 REST API 명령에는 API의 URL, HTTP 작업, 필수 또는 선택적 URL 매개 변수, 그리고 예상되는 API 응답이 포함됩니다.

StorageGRID 설치 API

StorageGRID 설치 API는 StorageGRID 시스템을 처음 구성할 때와 기본 관리자 노드 복구를 수행해야 하는 경우에만 사용할 수 있습니다. 설치 API는 Grid Manager에서 HTTPS를 통해 액세스할 수 있습니다.

API 설명서에 액세스하려면 기본 관리 노드의 설치 웹 페이지로 이동하여 메뉴 모음에서 * 도움말 * > * API 설명서 * 를 선택합니다.

StorageGRID 설치 API에는 다음 섹션이 포함되어 있습니다.

- * config * — 제품 릴리스 및 API 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 API의 주요 버전을 나열할 수 있습니다.
- * 그리드 * — 그리드 레벨 구성 작업. 그리드 세부 정보, 그리드 네트워크 서브넷, 그리드 암호, NTP 및 DNS 서버 IP

주소를 포함한 그리드 설정을 얻고 업데이트할 수 있습니다.

- * 노드 * — 노드 레벨 구성 작업 그리드 노드 목록을 검색하고, 그리드 노드를 삭제하고, 그리드 노드를 구성하고, 그리드 노드를 보고, 그리드 노드의 구성을 재설정할 수 있습니다.
- * 프로비저닝 * — 프로비저닝 작업. 프로비저닝 작업을 시작하고 프로비저닝 작업의 상태를 볼 수 있습니다.
- * 복구 * — 기본 관리 노드 복구 작업 정보를 재설정하고, 복구 패키지를 업로드하고, 복구를 시작하고, 복구 작업의 상태를 볼 수 있습니다.
- * recovery-package * — 복구 패키지를 다운로드하기 위한 작업.
- * 사이트 * — 사이트 수준 구성 작업 사이트를 만들고, 보고, 삭제하고, 수정할 수 있습니다.

StorageGRID 어플라이언스 설치 관리자 **API**입니다

StorageGRID 어플라이언스 설치 프로그램 API는 HTTPS를 통해 '*Controller_IP*:8443'에서 액세스할 수 있습니다.

API 설명서에 액세스하려면 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램으로 이동하여 메뉴 모음에서 * 도움말 * > * API Docs * 를 선택합니다.

StorageGRID 어플라이언스 설치 관리자 API에는 다음 섹션이 포함되어 있습니다.

- * 클론 * — 노드 클로닝을 구성하고 제어하는 작업.
- * 암호화 * — 암호화를 관리하고 암호화 상태를 확인하는 작업.
- * 하드웨어 구성 * — 연결된 하드웨어에서 시스템 설정을 구성하는 작업.
- * 설치 * — 어플라이언스 설치 시작 및 설치 상태 모니터링을 위한 작업.
- * 네트워킹 * — StorageGRID 어플라이언스 및 어플라이언스 포트 설정에 대한 그리드, 관리자 및 클라이언트 네트워크 구성과 관련된 작업.
- * setup * — 시스템에 대한 정보를 얻고 기본 관리 노드 IP를 업데이트하는 요청을 포함하여 초기 어플라이언스 설치 설정에 도움이 되는 작업.
- * 지원 * — 컨트롤러 재부팅 및 로그 가져오기에 대한 운영
- * 업그레이드 * — 어플라이언스 펌웨어 업그레이드와 관련된 작업.
- * 업로그램 * — StorageGRID 설치 파일을 업로드하는 작업.

하드웨어 설치 문제 해결**(SG5600)**

설치 중에 문제가 발생하는 경우 하드웨어 설정 및 연결 문제와 관련된 문제 해결 정보를 검토하는 것이 도움이 될 수 있습니다.

하드웨어 설정이 멈춘 것 같습니다**(SG5600).**

하드웨어 장애 또는 케이블 연결 오류로 인해 E5600SG 컨트롤러가 부팅 처리를 완료하지 못하는 경우 StorageGRID 어플라이언스 설치 프로그램을 사용할 수 없습니다.

단계

1. 두 컨트롤러 중 하나에서 Needs Attention(주의 필요) LED를 확인하고 깜박이는 오류 코드를 확인합니다.

   전원이 켜지는 동안 하드웨어 초기화 중에 허용되는 서비스 조치 및 서비스 조치 필요 LED가 켜집니다. 하위

자릿수의 상위 소수점인 _DIAGNOSTIC LED_도 켜집니다. 7세그먼트 디스플레이는 두 컨트롤러에 공통되는 일련의 코드를 통해 실행됩니다. 이는 정상적인 현상이며 오류를 나타내는 것은 아닙니다. 하드웨어가 성공적으로 부팅되면 Service Action(서비스 작업) LED가 꺼지고 디스플레이가 펌웨어에 의해 구동됩니다.

2. E600SG 컨트롤러에 대한 7세그먼트 디스플레이의 코드를 검토합니다.

> 설치 및 프로비저닝에 시간이 걸립니다. 일부 설치 단계에서는 몇 분 동안 StorageGRID 어플라이언스 설치 프로그램에 업데이트를 보고하지 않습니다.

오류가 발생하면 7개 세그먼트 디스플레이에서 그와 같은 시퀀스가 깜박입니다.

3. 이러한 코드의 의미를 이해하려면 다음 리소스를 참조하십시오.

컨트롤러	참조하십시오
E5500SG 컨트롤러	• ""SANtricity OS 소프트웨어와 동기화 중 오류 발생"" • "'E600SG 컨트롤러 7세그먼트 디스플레이 코드'"
E2700 컨트롤러	E-Series 설명서를 참조하십시오 • 참고: * E-Series E5600 컨트롤러에 대해 설명된 코드는 어플라이언스의 E5500SG 컨트롤러에 적용되지 않습니다.

4. 그래도 문제가 해결되지 않으면 기술 지원 부서에 문의하십시오.

관련 정보

E5500SG 컨트롤러 7세그먼트 디스플레이 코드

SANtricity OS 소프트웨어와 동기화하는 동안 오류가 발생했습니다

"E2700 컨트롤러 - 드라이브 트레이 및 관련 드라이브 트레이 설치 가이드"

"NetApp 설명서: E2700 시리즈"

SANtricity OS 소프트웨어와 동기화하는 동안 오류가 발생했습니다

StorageGRID 어플라이언스 설치 프로그램이 SANtricity OS 소프트웨어와 동기화할 수 없는 경우 컴퓨팅 컨트롤러의 7세그먼트 디스플레이에 해당 오류 코드가 표시됩니다.

이 작업에 대해

오류 코드가 표시되는 경우 이 수정 조치를 수행하십시오.

단계

1. 2개의 SAS 인터커넥트 케이블이 정상인지 점검하고 단단히 연결되어 있는지 확인하십시오.
2. 필요에 따라 하나 또는 두 케이블을 교체하고 다시 시도하십시오.
3. 그래도 문제가 해결되지 않으면 기술 지원 부서에 문의하십시오.

연결 문제 해결**(SG5600)**

StorageGRID 어플라이언스 설치 중에 연결 문제가 발생하면 나열된 수정 조치 단계를 수행해야 합니다.

네트워크를 통해 **StorageGRID** 어플라이언스에 연결할 수 없습니다

어플라이언스에 연결할 수 없는 경우 네트워크 문제가 있거나 하드웨어 설치가 성공적으로 완료되지 않았을 수 있습니다.

- * 문제 *

  제품에 연결할 수 없습니다.

- * 원인 *

  이 문제는 네트워크 문제가 있거나 하드웨어 설치가 성공적으로 완료되지 않은 경우에 발생할 수 있습니다.

- * 시정 조치 *

  a. 어플라이언스를 Ping합니다: + `* PING_E5600_CONTROLLER_IP_ * '

  b. 브라우저를 열고 다음을 입력하여 StorageGRID 어플라이언스 설치 프로그램에 액세스합니다. + `https://*Management_Port_IP*:8443*`

     Management_Port_IP의 경우, E600SG 컨트롤러의 관리 포트 1에 대한 IP 주소를 입력합니다(물리적 설치 중에 프로비저닝됨).

  c. Configure Admin network * 를 클릭하고 IP를 확인합니다.

  d. ping에서 응답을 받는 경우 포트 8443이 방화벽에서 열려 있는지 확인합니다.

  e. 어플라이언스를 재부팅합니다.

  f. 설치 웹 페이지를 새로 고칩니다.

  g. 그래도 연결 문제가 해결되지 않으면 NetApp Support 사이트 에서 기술 지원을 문의하십시오 "mysupport.netapp.com".

관련 정보

E5500SG 컨트롤러 7세그먼트 디스플레이 코드

StorageGRID 어플라이언스 설치 프로그램이 실행되는 동안 컨트롤러를 재부팅합니다

StorageGRID 어플라이언스 설치 프로그램이 실행되는 동안 컴퓨팅 컨트롤러를 재부팅해야 할 수도 있습니다. 예를 들어, 설치에 실패한 경우 컨트롤러를 재부팅해야 할 수 있습니다.

이 작업에 대해

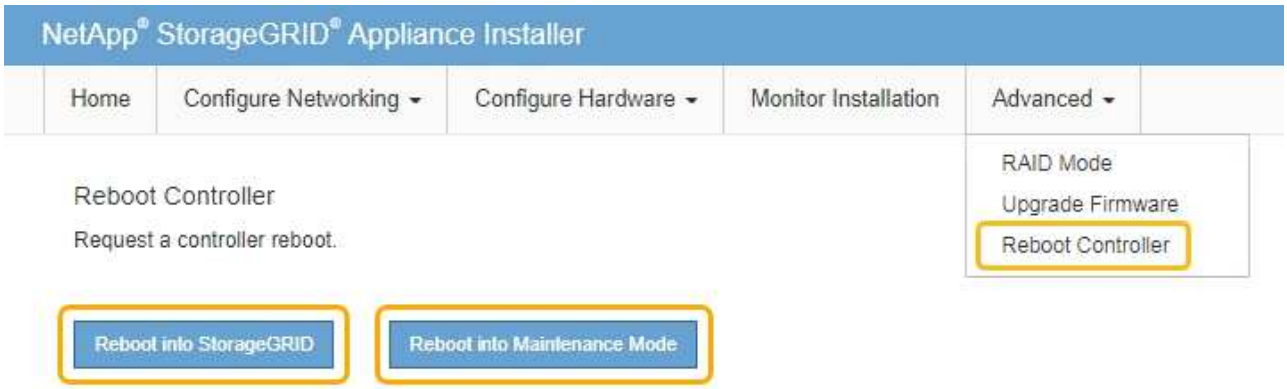
이 절차는 컴퓨팅 컨트롤러가 StorageGRID 어플라이언스 설치 프로그램을 실행하는 경우에만 적용됩니다. 설치가 완료되면 StorageGRID 어플라이언스 설치 프로그램을 더 이상 사용할 수 없기 때문에 이 단계가 더 이상 작동하지 않습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 클릭한 후 다음 옵션 중 하나를

선택합니다.

- 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
- 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



컨트롤러가 재부팅됩니다.

SG5600 어플라이언스 유지

E2700 컨트롤러에서 SANtricity OS 소프트웨어를 업그레이드하거나 E2700 컨트롤러 또는 E5500SG 컨트롤러를 교체하거나 특정 구성요소를 교체해야 할 수 있습니다. 이 섹션의 절차에서는 어플라이언스가 이미 StorageGRID 시스템의 스토리지 노드로 구축되었다고 가정합니다.

제품을 유지보수 모드로 전환합니다

특정 유지보수 절차를 수행하기 전에 제품을 유지보수 모드로 전환해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

이 작업에 대해

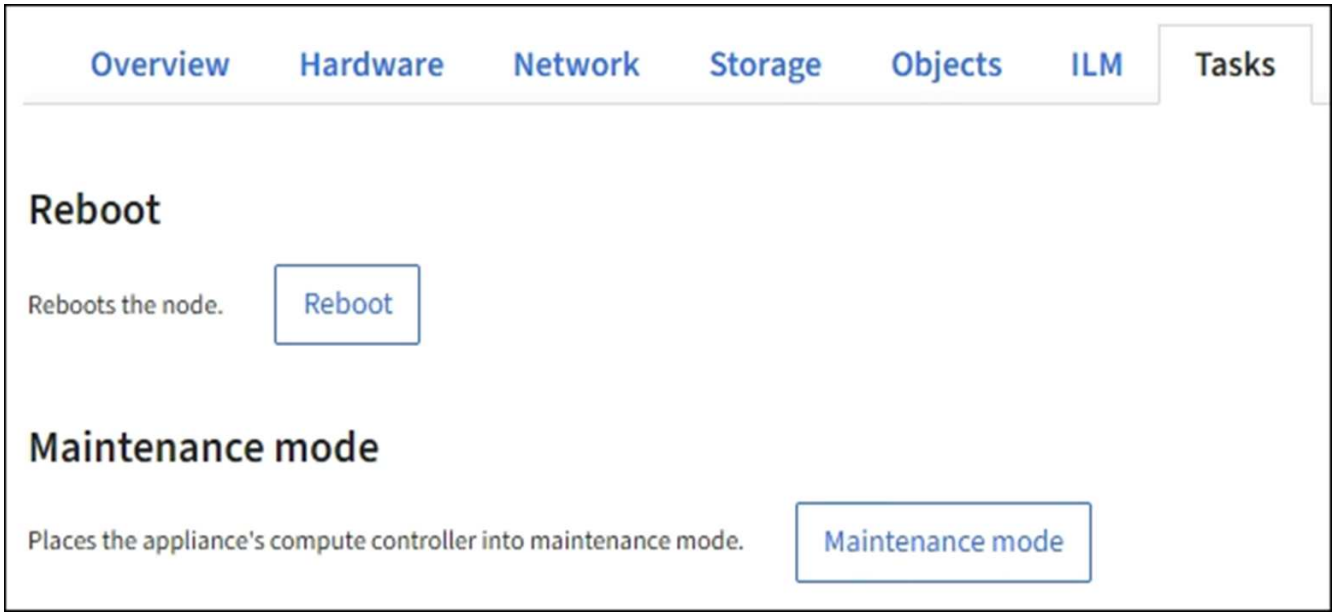
StorageGRID 어플라이언스를 유지보수 모드로 전환하면 원격 액세스가 불가능한 경우가 드물게 있습니다.

> 유지보수 모드에서 StorageGRID 어플라이언스에 대한 admin 계정 암호 및 SSH 호스트 키는 어플라이언스가 서비스 중일 때와 동일하게 유지됩니다.

단계

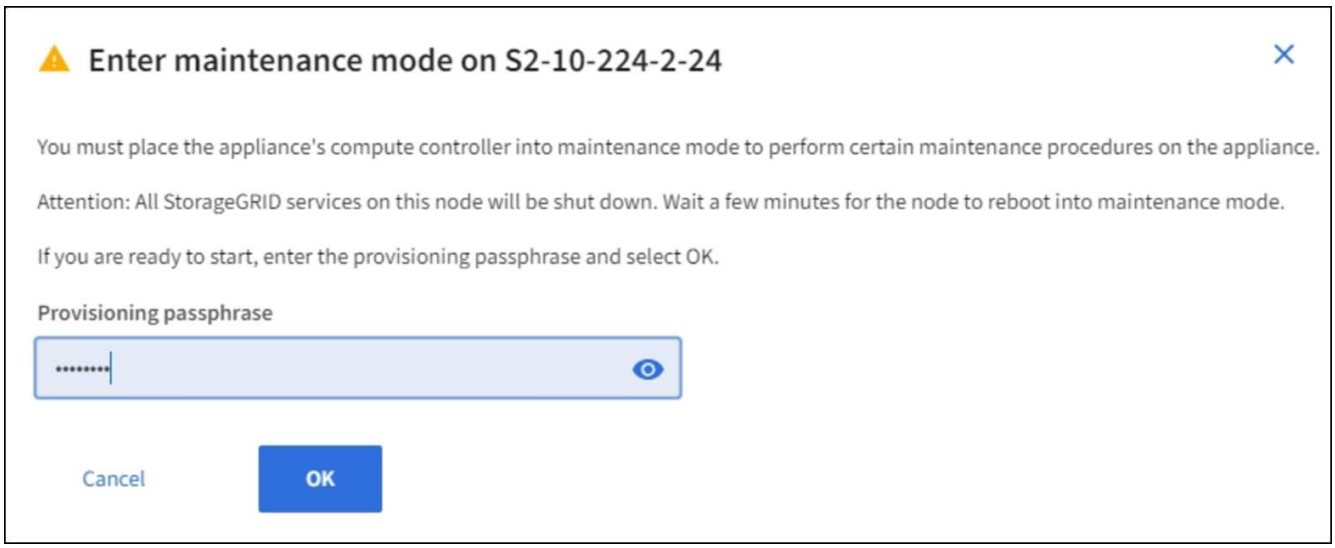
1. Grid Manager에서 * nodes * 를 선택합니다.

2. 노드 페이지의 트리 뷰에서 어플라이언스 스토리지 노드를 선택합니다.
3. 작업 * 을 선택합니다.



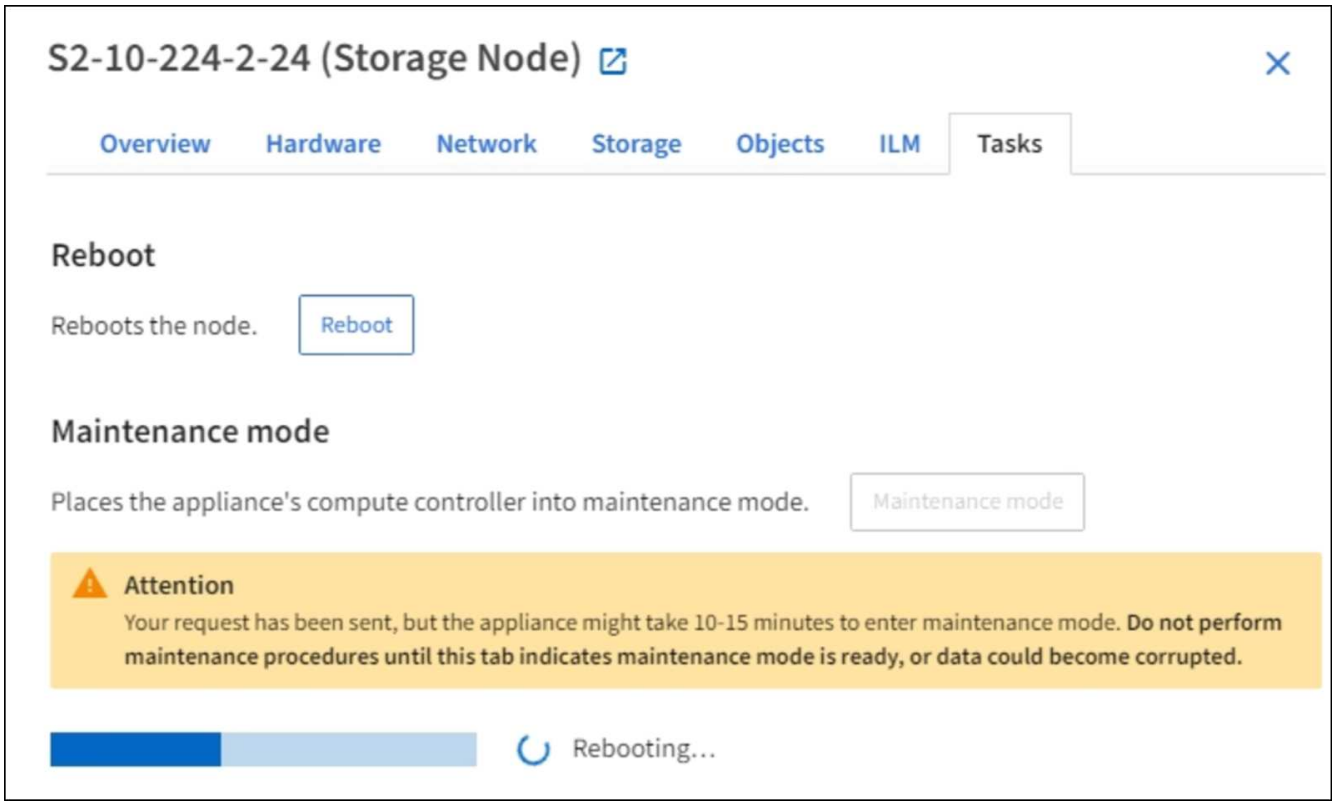
4. 유지보수 모드 * 를 선택합니다.

   확인 대화 상자가 나타납니다.

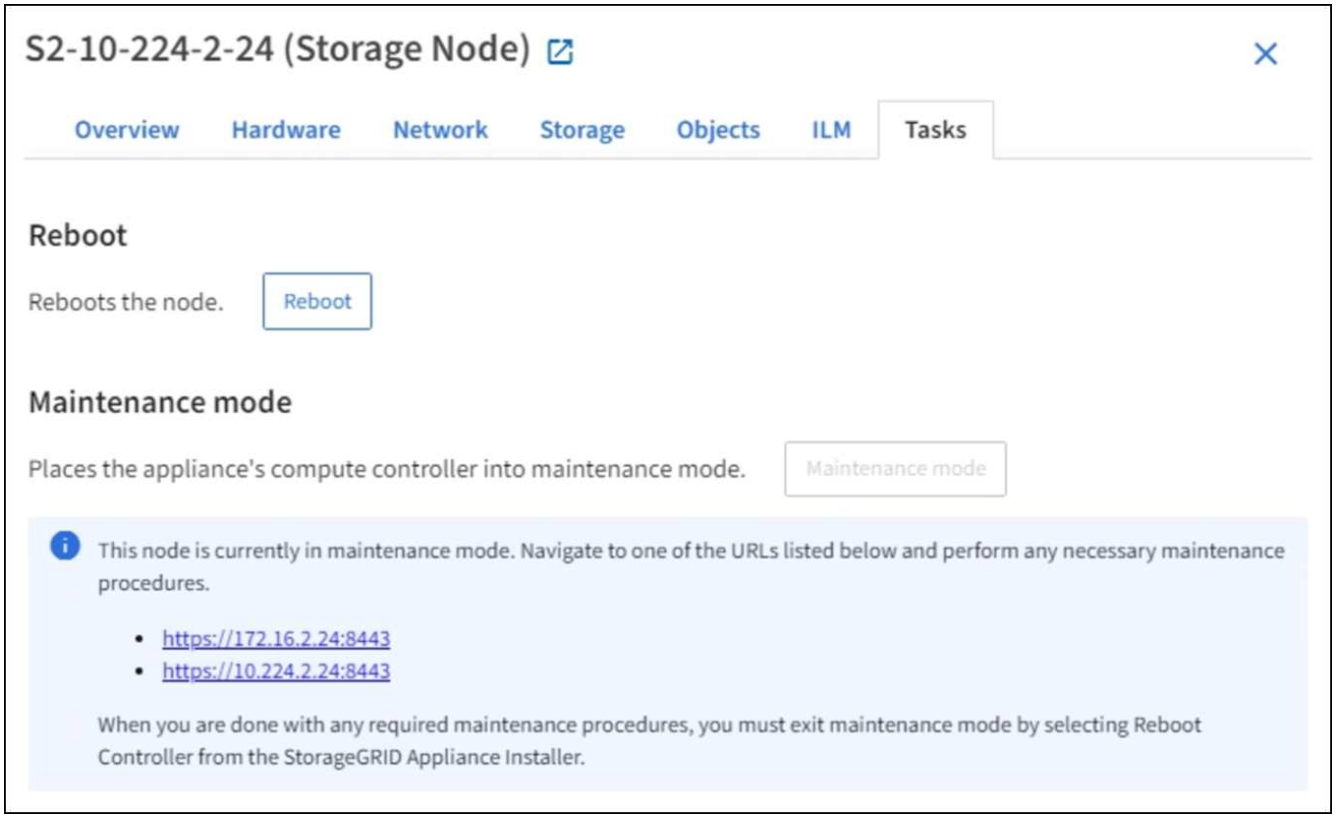


5. 프로비저닝 암호를 입력하고 * OK * 를 선택합니다.

   진행 표시줄과 "전송 요청", "StorageGRID 중지", "재부팅 중"과 같은 일련의 메시지는 어플라이언스가 유지보수 모드로 들어가기 위한 단계를 완료하고 있음을 나타냅니다.



어플라이언스가 유지보수 모드일 때 확인 메시지에 StorageGRID 어플라이언스 설치 프로그램에 액세스하는 데 사용할 수 있는 URL이 나열됩니다.



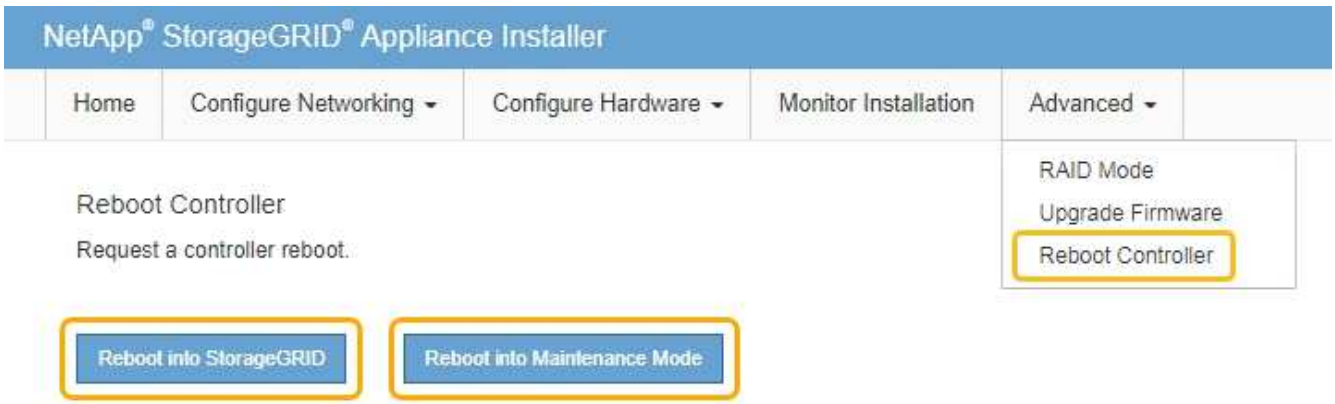
6. StorageGRID 어플라이언스 설치 프로그램에 액세스하려면 표시된 URL 중 하나를 찾습니다.

   가능한 경우 어플라이언스의 관리 네트워크 포트의 IP 주소가 포함된 URL을 사용하십시오.

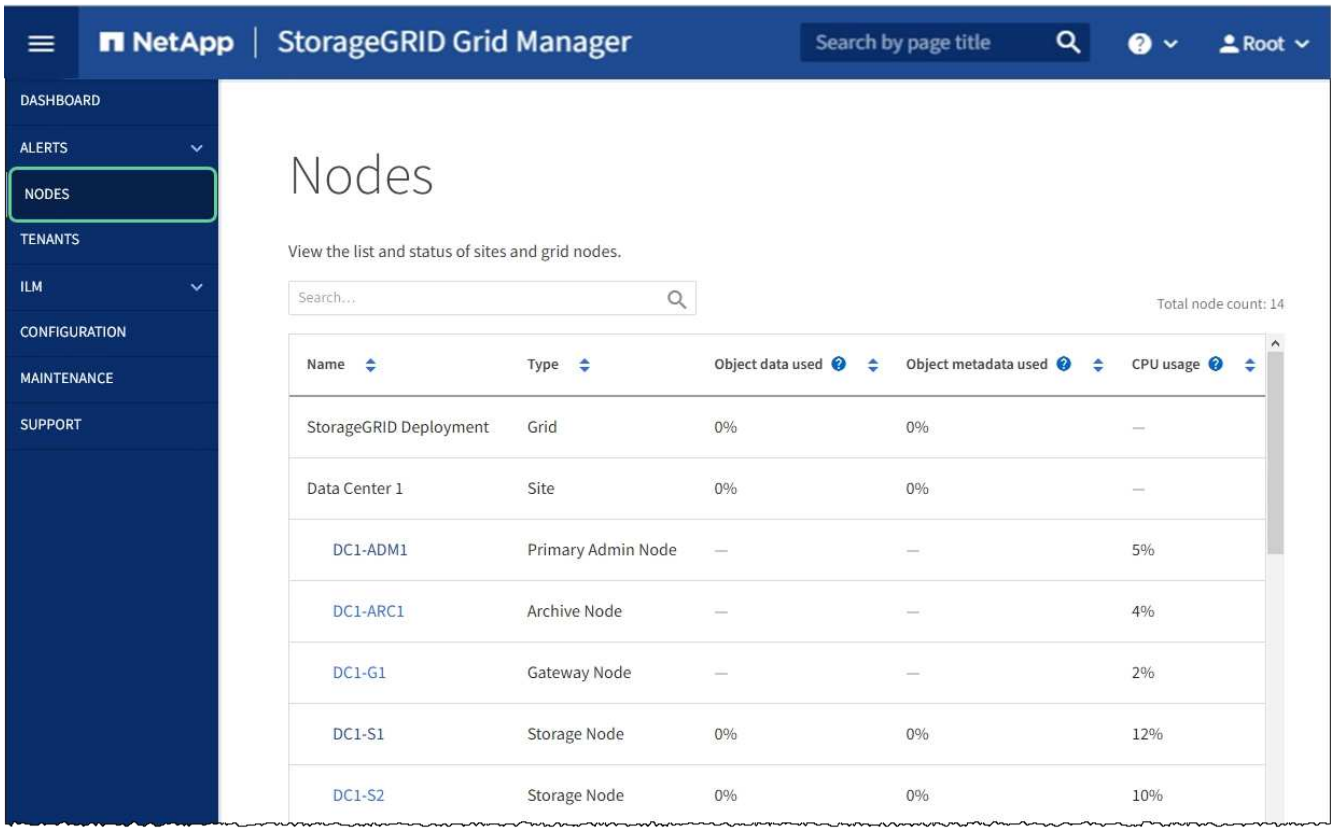
> 어플라이언스의 관리 포트에 직접 연결되어 있는 경우, 'https://169.254.0.1:8443` 을 사용하여 StorageGRID 어플라이언스 설치 프로그램 페이지에 액세스하십시오.

7. StorageGRID 어플라이언스 설치 프로그램에서 어플라이언스가 유지보수 모드인지 확인합니다.

8. 필요한 유지보수 작업을 수행합니다.
9. 유지보수 작업을 완료한 후 유지보수 모드를 종료하고 정상 노드 운영을 재개합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * StorageGRID * 으로 재부팅 * 을 선택합니다.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



그리드 관리자를 사용하여 스토리지 컨트롤러의 **SANtricity OS**를 업그레이드합니다

현재 SANtricity OS 08.42.20.00(11.42) 이상을 사용하는 스토리지 컨트롤러의 경우 그리드 관리자를 사용하여 업그레이드를 적용해야 합니다.

필요한 것

- 업그레이드에 사용 중인 SANtricity OS 버전이 어플라이언스와 호환되는지 확인하려면 NetApp 상호 운용성 매트릭스 툴(IMT)을 참조하십시오.
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 프로비저닝 암호가 있습니다.
- SANtricity OS의 NetApp 다운로드 페이지에 액세스할 수 있습니다.

이 작업에 대해

SANtricity OS 업그레이드 프로세스를 완료할 때까지 다른 소프트웨어 업데이트(StorageGRID 소프트웨어 업그레이드 또는 핫픽스)를 수행할 수 없습니다. SANtricity OS 업그레이드 프로세스가 완료되기 전에 핫픽스 또는 StorageGRID 소프트웨어 업그레이드를 시작하려고 하면 SANtricity OS 업그레이드 페이지로 리디렉션됩니다.

SANtricity OS 업그레이드가 업그레이드를 위해 선택된 모든 적용 가능한 노드에 적용되기 전에는 절차가 완료되지 않습니다. 각 노드에서 SANtricity OS를 로드하는 데 30분 이상, 각 StorageGRID 스토리지 어플라이언스를 재부팅하는 데 최대 90분이 걸릴 수 있습니다.

다음 단계는 그리드 관리자를 사용하여 업그레이드를 수행하는 경우에만 적용됩니다. 컨트롤러가 08.42.20.00(11.42) 이전의 SANtricity OS를 사용하는 경우 그리드 관리자를 사용하여 어플라이언스의 스토리지 컨트롤러를 업그레이드할 수 없습니다.

이 절차에서는 NVSRAM을 SANtricity OS 업그레이드와 관련된 최신 버전으로 자동 업그레이드합니다. 별도의 NVSRAM 업그레이드 파일을 적용할 필요가 없습니다.

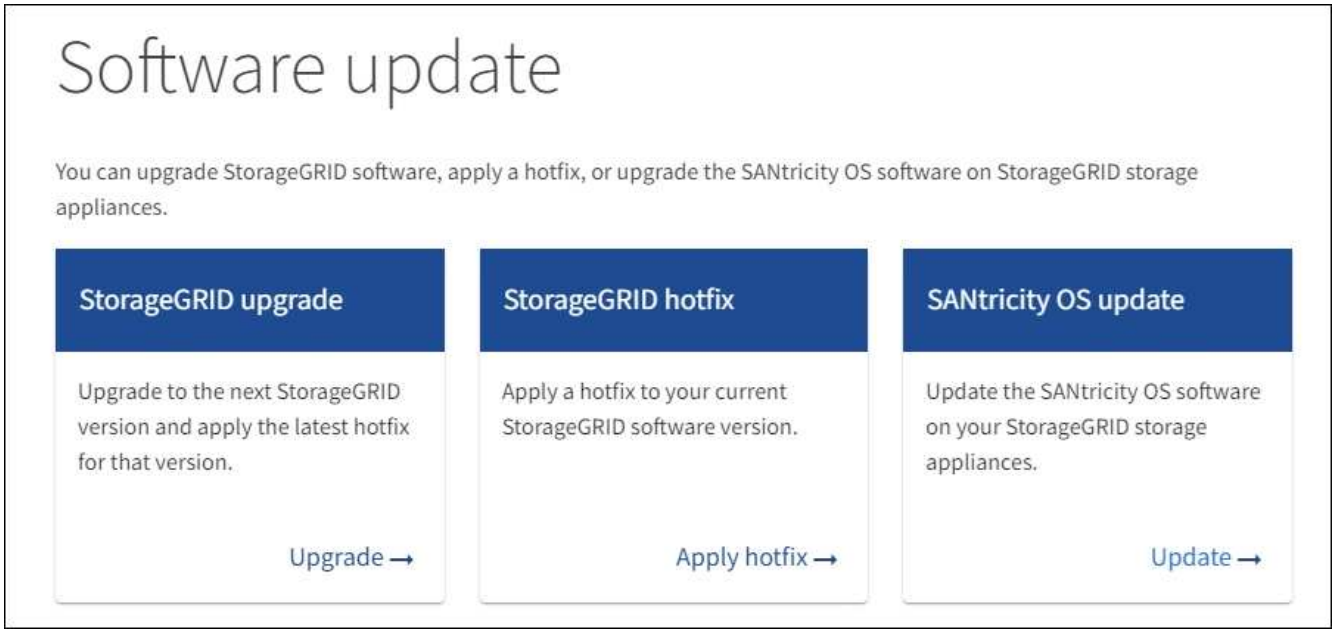
단계

1. NetApp Support 사이트에서 새로운 SANtricity OS 소프트웨어 파일을 다운로드합니다.

   스토리지 컨트롤러의 SANtricity OS 버전을 선택해야 합니다.

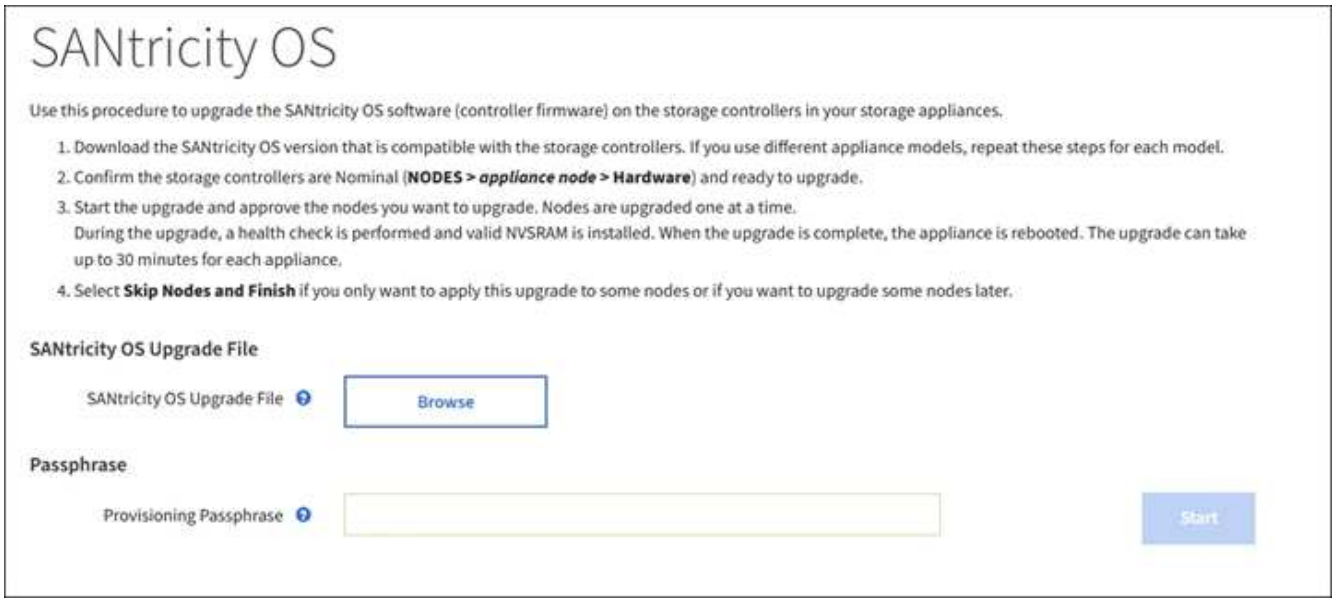
   "NetApp 다운로드: StorageGRID 어플라이언스"

2. 유지보수 * > * 시스템 * > * 소프트웨어 업데이트 * 를 선택합니다.



3. SANtricity OS 업데이트 섹션에서 * 업데이트 * 를 선택합니다.

   SANtricity OS 업그레이드 페이지가 나타납니다.



4. NetApp Support 사이트에서 다운로드한 SANtricity OS 업그레이드 파일을 선택합니다.

   a. 찾아보기 * 를 선택합니다.

   b. 파일을 찾아 선택합니다.

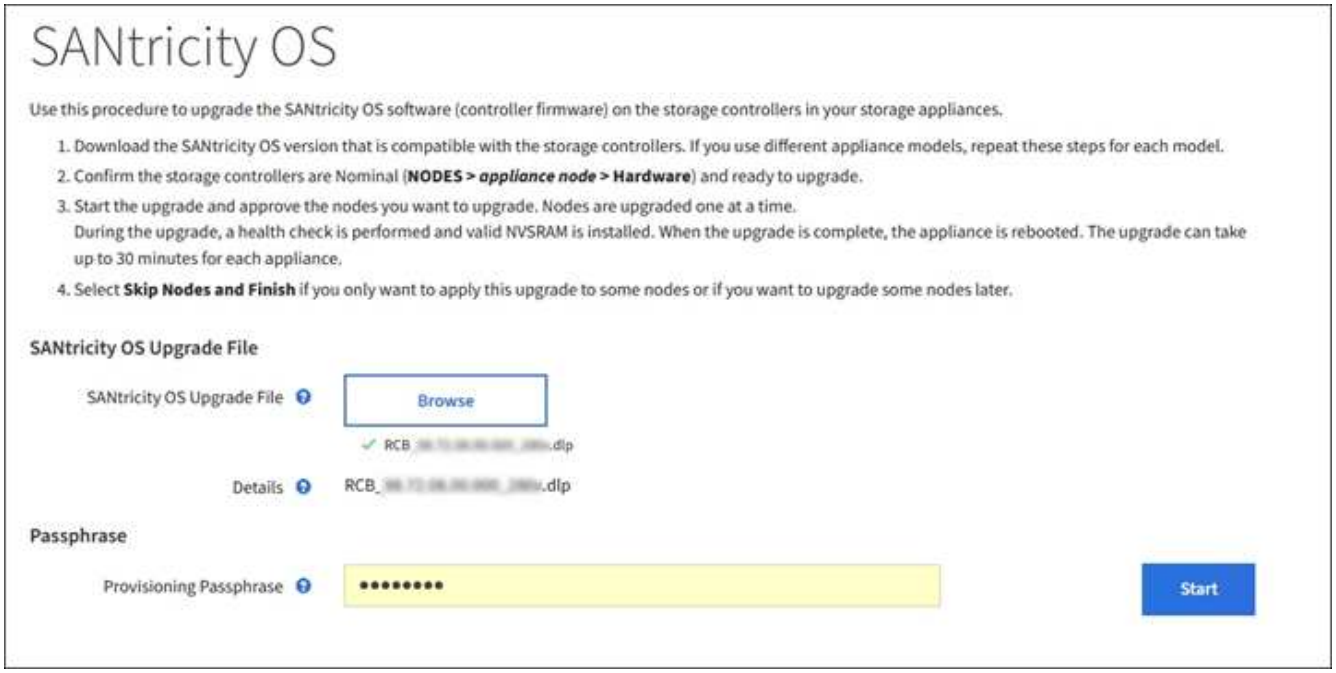
   c. 열기 * 를 선택합니다.

   파일이 업로드되고 검증됩니다. 유효성 검사 프로세스가 완료되면 * 찾아보기 * 버튼 옆에 파일 이름이 표시됩니다.

   ⓘ 파일 이름은 확인 프로세스의 일부이므로 변경하지 마십시오.

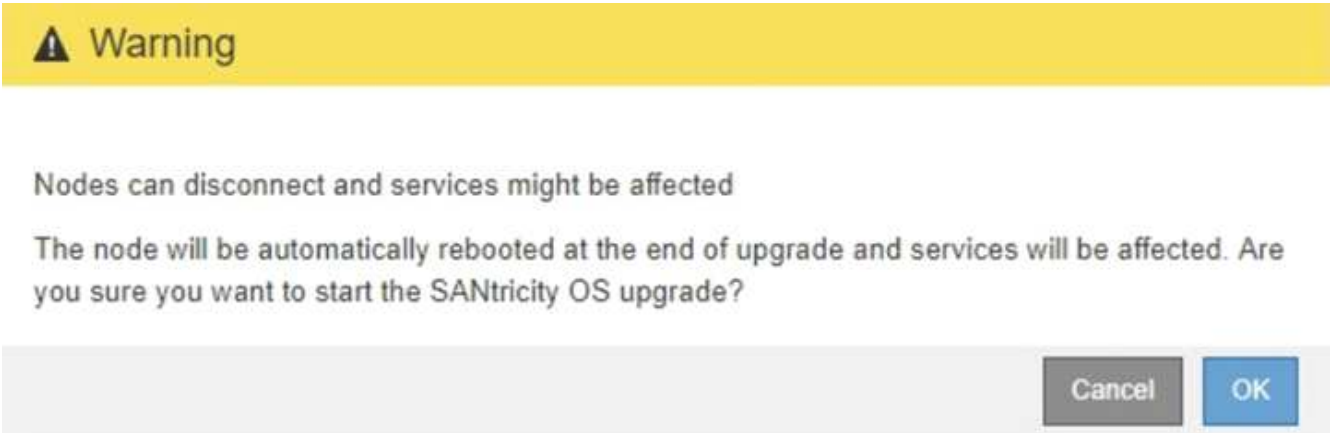
5. 프로비저닝 암호를 입력합니다.

   시작 * 버튼이 활성화됩니다.



6. 시작 * 을 선택합니다.

   업그레이드된 노드의 서비스가 다시 시작됨에 따라 브라우저의 연결이 일시적으로 끊길 수 있다는 경고 상자가 나타납니다.



7. SANtricity OS 업그레이드 파일을 기본 관리 노드로 스테이징하려면 * OK * 를 선택하십시오.

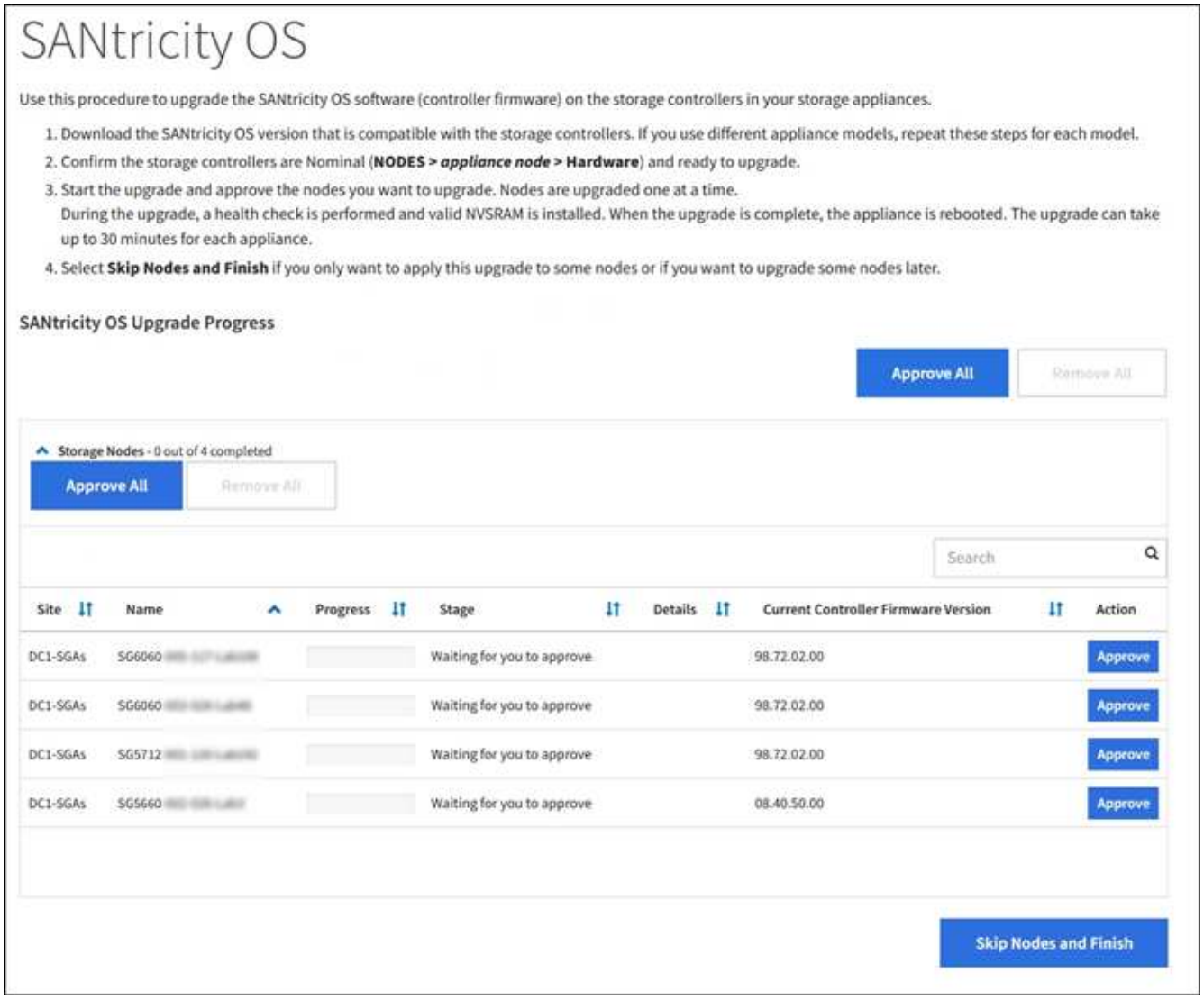
   SANtricity OS 업그레이드가 시작될 때:

   a. 상태 점검이 실행됩니다. 이 프로세스에서는 노드 상태가 주의 필요 인지 확인합니다.

      ⓘ 오류가 보고되면 이를 해결하고 * 시작 * 을 다시 선택합니다.

   b. SANtricity OS 업그레이드 진행률 테이블이 나타납니다. 이 표에는 그리드의 모든 스토리지 노드 및 각 노드의 현재 업그레이드 단계가 나와 있습니다.

      ⓘ 이 표에는 모든 어플라이언스 스토리지 노드가 표시됩니다. 소프트웨어 기반 스토리지 노드가 표시되지 않습니다. 업그레이드가 필요한 모든 노드에 대해 * Approve * 를 선택합니다.



8. 선택적으로 * Site *, * Name *, * Progress *, * Stage *, * Details *, * Site *, * Site *, *, * Details *, 또는 * 현재 컨트롤러 펌웨어 버전 *. 또는 * 검색 * 상자에 용어를 입력하여 특정 노드를 검색합니다.

   섹션의 오른쪽 아래 모서리에 있는 왼쪽 및 오른쪽 화살표를 사용하여 노드 목록을 스크롤할 수 있습니다.

9. 업그레이드 대기열에 추가할 준비가 된 그리드 노드를 승인합니다. 동일한 유형의 승인된 노드는 한 번에 하나씩 업그레이드됩니다.

   > 노드를 중지하고 재부팅할 준비가 되어 있는지 확실하지 않은 경우 어플라이언스 스토리지 노드에 대한 SANtricity OS 업그레이드를 승인하지 마십시오. 노드에서 SANtricity OS 업그레이드가 승인되면 해당 노드의 서비스가 중지되고 업그레이드 프로세스가 시작됩니다. 나중에 노드 업그레이드가 완료되면 어플라이언스 노드가 재부팅됩니다. 이러한 작업은 노드와 통신하는 클라이언트에 대해 서비스 중단을 일으킬 수 있습니다.

   - 모든 스토리지 노드를 SANtricity OS 업그레이드 대기열에 추가하려면 * 모두 승인 * 버튼 중 하나를 선택합니다.

     > 노드 업그레이드 순서가 중요한 경우 노드 또는 노드 그룹을 한 번에 하나씩 승인하고 다음 노드를 승인하기 전에 각 노드에서 업그레이드가 완료될 때까지 기다립니다.

- 하나 이상의 * Approve * (승인 *) 버튼을 선택하여 하나 이상의 노드를 SANtricity OS 업그레이드 대기열에 추가합니다.

  Approve * 를 선택하면 업그레이드 프로세스에서 노드를 업그레이드할 수 있는지 여부를 결정합니다. 노드를 업그레이드할 수 있는 경우 업그레이드 대기열에 추가됩니다.

일부 노드의 경우 선택한 업그레이드 파일이 의도적으로 적용되지 않으며 이러한 특정 노드를 업그레이드하지 않고 업그레이드 프로세스를 완료할 수 있습니다. 의도적으로 업그레이드되지 않은 노드는 완료(업그레이드 시도) 단계를 표시하고 세부 정보 열에 노드가 업그레이드되지 않은 이유를 표시합니다.

10. SANtricity OS 업그레이드 대기열에서 노드 또는 모든 노드를 제거해야 하는 경우 * 제거 * 또는 * 모두 제거 * 를 선택합니다.

    스테이지가 대기 모드 를 넘어 진행되면 * 제거 * 버튼이 숨겨지고 더 이상 SANtricity OS 업그레이드 프로세스에서 노드를 제거할 수 없습니다.

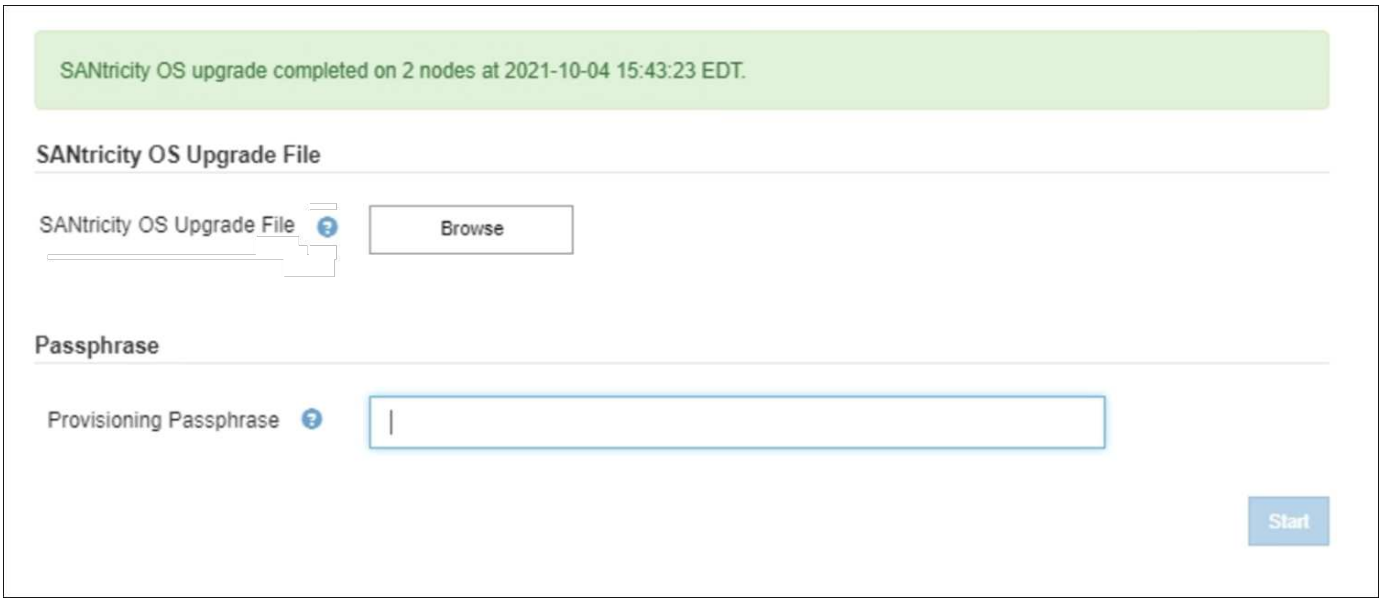
11. SANtricity OS 업그레이드가 승인된 각 그리드 노드에 적용될 때까지 기다립니다.

    - SANtricity OS 업그레이드를 적용하는 동안 노드에 오류 단계가 표시되는 경우 해당 노드에 대한 업그레이드가 실패한 것입니다. 기술 지원의 도움을 받아 어플라이언스를 유지보수 모드로 전환하여 복구해야 할 수도 있습니다.
    - 노드의 펌웨어가 너무 오래되어 그리드 관리자로 업그레이드되지 않는 경우, 노드에 오류 단계가 표시됩니다: ""이 노드에서 SANtricity OS를 업그레이드하려면 유지보수 모드를 사용해야 합니다. 제품의 설치 및 유지관리 지침을 참조하십시오. 업그레이드 후 향후 업그레이드를 위해 이 유틸리티를 사용할 수 있습니다." 오류를 해결하려면 다음을 수행합니다.

      i. 유지보수 모드를 사용하여 오류 단계가 표시된 노드에서 SANtricity OS를 업그레이드합니다.

      ii. 그리드 관리자를 사용하여 SANtricity OS 업그레이드를 다시 시작하고 완료합니다.

    승인된 모든 노드에서 SANtricity OS 업그레이드가 완료되면 SANtricity OS 업그레이드 진행률 테이블이 닫히고 SANtricity OS 업그레이드가 완료된 날짜와 시간이 녹색 배너에 표시됩니다.



1. 노드를 업그레이드할 수 없는 경우 세부 정보 열에 표시된 이유를 기록하고 적절한 조치를 취하십시오.
   - "스토리지 노드가 이미 업그레이드되었습니다." 추가 조치가 필요하지 않습니다.

- "SANtricity OS 업그레이드는 이 노드에 적용되지 않습니다." 노드에는 StorageGRID 시스템에서 관리할 수 있는 스토리지 컨트롤러가 없습니다. 이 메시지가 표시된 노드를 업그레이드하지 않고 업그레이드 프로세스를 완료합니다.
- "'SANtricity OS 파일이 이 노드와 호환되지 않습니다.'" 노드에는 선택한 것과 다른 SANtricity OS 파일이 필요합니다. 현재 업그레이드를 완료한 후 노드에 대한 올바른 SANtricity OS 파일을 다운로드하고 업그레이드 프로세스를 반복합니다.

> 나열된 모든 스토리지 노드에서 SANtricity OS 업그레이드를 승인할 때까지 SANtricity OS 업그레이드 프로세스가 완료되지 않습니다.

1. 노드 승인을 종료하여 SANtricity OS 페이지로 돌아가 새 SANtricity OS 파일 업로드를 허용하려면 다음을 수행합니다.

   a. 노드 건너뛰기 및 마침 * 을 선택합니다.

      모든 노드를 업그레이드하지 않고 업그레이드 프로세스를 완료할지 묻는 경고가 나타납니다.

   b. SANtricity OS * 페이지로 돌아가려면 * OK * 를 선택하십시오.

   c. 노드 승인을 계속할 준비가 되면 로 이동합니다 SANtricity OS를 다운로드합니다 를 눌러 업그레이드 프로세스를 다시 시작합니다.

      > 노드가 이미 승인되었으며 오류 없이 업그레이드되었습니다.

2. 다른 SANtricity OS 업그레이드 파일이 필요한 전체 단계가 있는 노드에 대해 이 업그레이드 절차를 반복합니다.

   > Needs Attention(주의 필요) 상태인 모든 노드의 경우 유지보수 모드를 사용하여 업그레이드를 수행합니다.

   > 업그레이드 절차를 반복하면 이전에 업그레이드된 노드를 승인해야 합니다.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

유지보수 모드를 사용하여 E2700 컨트롤러에서 SANtricity OS를 업그레이드합니다

유지보수 모드를 사용하여 **E2700** 컨트롤러에서 **SANtricity OS**를 업그레이드합니다

그리드 관리자를 사용하여 SANtricity OS 소프트웨어를 업그레이드할 수 없는 경우 유지보수 모드 절차를 사용하여 업그레이드를 적용하십시오.

필요한 것

- 업그레이드에 사용 중인 SANtricity OS 버전이 어플라이언스와 호환되는지 확인하려면 NetApp 상호 운용성 매트릭스 툴(IMT)을 참조하십시오.
- E5600 컨트롤러를 에 장착해야 합니다 유지보수 모드 Grid Manager를 사용하지 않는 경우 컨트롤러를 유지보수 모드로 전환하면 E2700 컨트롤러 연결이 중단됩니다.

> StorageGRID 어플라이언스를 유지보수 모드로 전환하면 원격 액세스가 불가능한 경우가 드물게 있습니다.

이 작업에 대해

한 번에 두 개 이상의 StorageGRID 어플라이언스에 있는 E-Series 컨트롤러의 SANtricity OS 또는 NVSRAM을 업그레이드하지 마십시오.

> 배포 모델 및 ILM 정책에 따라 한 번에 둘 이상의 StorageGRID 어플라이언스를 업그레이드할 경우 데이터를 사용할 수 없게 될 수 있습니다.

단계

1. 제품이 에 있는지 확인하십시오 유지보수 모드.
2. 서비스 랩톱에서 SANtricity 저장소 관리자 에 액세스하고 로그인합니다.
3. 관리 클라이언트에 새 SANtricity OS 소프트웨어 파일 및 NVSRAM 파일을 다운로드합니다.

   > NVSRAM은 StorageGRID 어플라이언스에만 적용됩니다. 표준 NVSRAM 다운로드를 사용하지 마십시오.

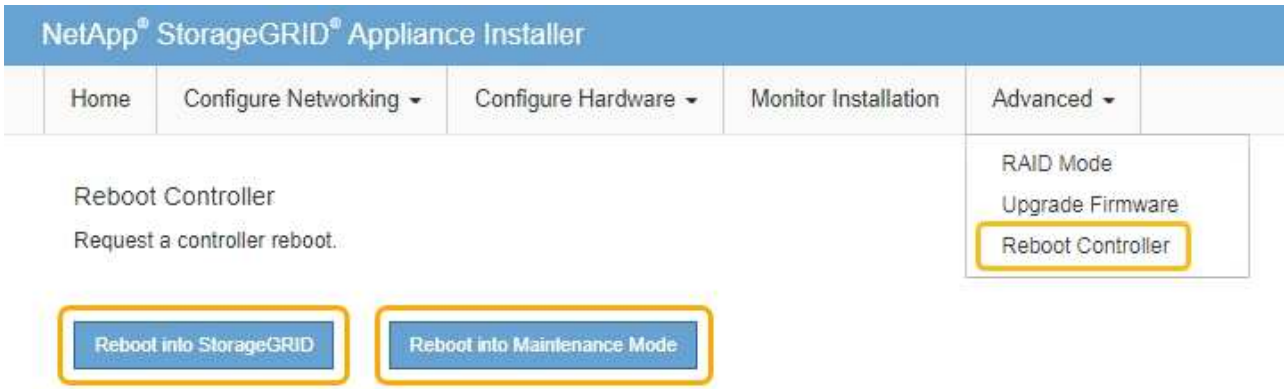
4. E2700 및 E5600 SANtricity 소프트웨어 및 펌웨어 업그레이드 지침_ 또는 SANtricity 스토리지 관리자 온라인 도움말의 지침을 따르고 E2700 컨트롤러의 펌웨어, NVSRAM 또는 둘 모두를 업그레이드하십시오.

   > E2700 컨트롤러에서 NVSRAM을 업그레이드해야 하는 경우, 다운로드한 SANtricity OS 파일이 StorageGRID 어플라이언스와 호환되도록 지정되었는지 확인해야 합니다.

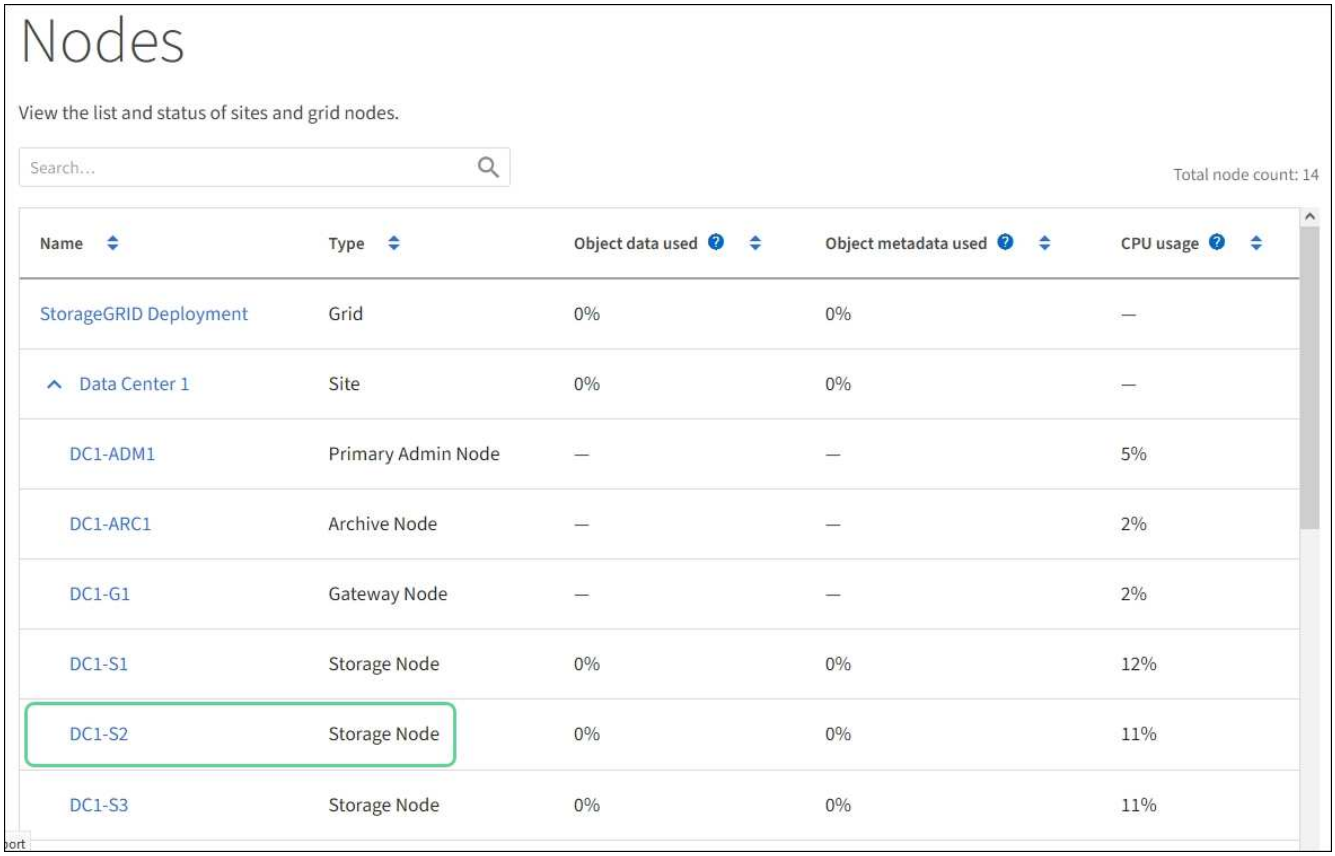
   > 업그레이드 파일을 즉시 활성화합니다. 활성화를 지연하지 마십시오.

5. 이 절차가 성공적으로 완료되었고 노드가 유지보수 모드일 때 수행할 추가 절차가 있는 경우 지금 수행합니다. 작업을 완료했거나 오류가 발생하여 다시 시작하려면 * 고급 * > * 컨트롤러 재부팅 * 을 선택하고 다음 옵션 중 하나를 선택합니다.

   - StorageGRID * 로 재부팅 * 을 선택합니다
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. 절차 중에 오류가 발생하여 다시 시작하려면 이 옵션을 선택합니다. 노드가 유지보수 모드로 재부팅된 후 장애가 발생한 절차의 적절한 단계에서 다시 시작하십시오.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. 노드 페이지에는 어플라이언스 노드에 대한 정상 상태(노드 이름 왼쪽에 아이콘이 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



SANtricity 저장소 관리자를 사용하여 드라이브 펌웨어를 업그레이드합니다

드라이브 펌웨어를 업그레이드하여 최신 기능 및 버그 수정 사항이 모두 있는지 확인합니다.

필요한 것

- 스토리지 어플라이언스 상태가 최적입니다.

- 모든 드라이브가 최적 상태입니다.
- StorageGRID 버전과 호환되는 최신 버전의 SANtricity 스토리지 관리자가 설치되어 있습니다.

  그리드 관리자를 사용하여 스토리지 컨트롤러의 SANtricity OS를 업그레이드합니다

  유지보수 모드를 사용하여 E2700 컨트롤러에서 SANtricity OS를 업그레이드합니다

- 있습니다 StorageGRID 어플라이언스를 유지보수 모드로 놓았습니다.

> 유지보수 모드는 스토리지 컨트롤러에 대한 연결을 중단하여 모든 I/O 작업을 중지하고 모든 드라이브를 오프라인으로 전환합니다.

> 한 번에 둘 이상의 StorageGRID 어플라이언스에서 드라이브 펌웨어를 업그레이드하지 마십시오. 따라서 배포 모델 및 ILM 정책에 따라 데이터를 사용할 수 없게 될 수 있습니다.

단계

1. 제품이 에 있는지 확인하십시오 유지보수 모드.
2. 웹 브라우저를 열고 IP 주소를 SANtricity 저장소 관리자(+' * https://*E2700_Controller_IP**`)의 URL로 입력합니다
3. 필요한 경우 SANtricity 스토리지 관리자 사용자 이름과 암호를 입력합니다.
4. SANtricity 엔터프라이즈 관리에서 * 장치 * 탭을 선택합니다.

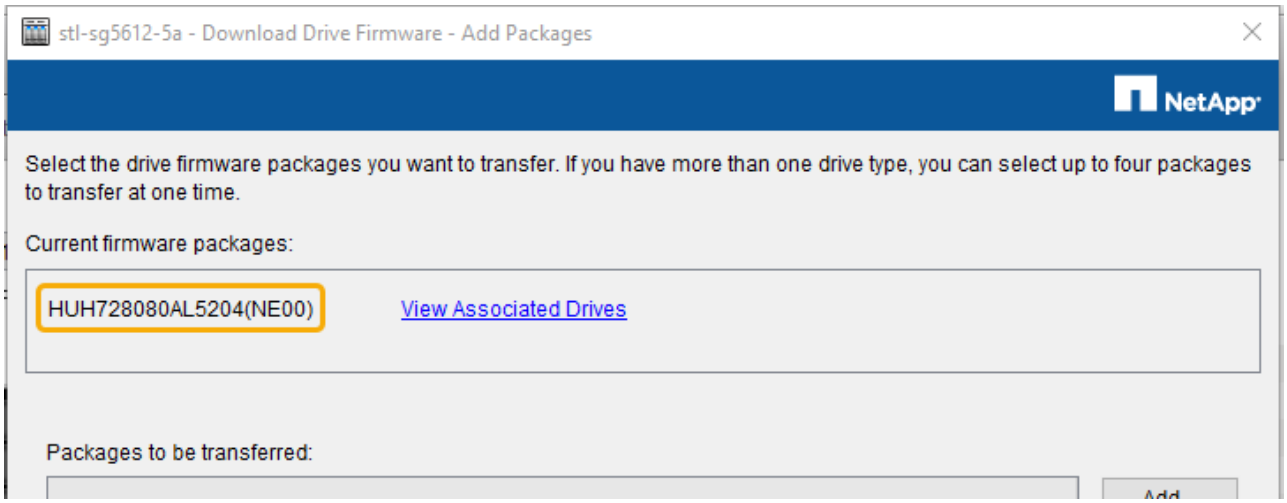
   SANtricity 어레이 관리 창이 열립니다.

5. SANtricity 어레이 관리에서 업그레이드할 드라이브가 있는 스토리지 어레이를 두 번 클릭합니다.
6. 스토리지 배열 및 드라이브가 모두 최적 상태인지 확인합니다.
7. 스토리지 어플라이언스에 현재 설치된 드라이브 펌웨어 버전을 확인합니다.

   a. SANtricity 엔터프라이즈 관리에서 * 업그레이드 * > * 드라이브 펌웨어 * 를 선택합니다.

      Download Drive Firmware - Add Packages(드라이브 펌웨어 다운로드 - 패키지 추가) 창에는 현재 사용 중인 드라이브 펌웨어 파일이 표시됩니다.

   b. 현재 펌웨어 패키지의 드라이브 펌웨어 개정 버전 및 드라이브 식별자를 확인합니다.



이 예에서

- 드라이브 펌웨어 버전은 * NE00 * 입니다.
- 드라이브 식별자는 * HUH7280AL5204 * 입니다.

View associated Drives * 를 선택하여 스토리지 어플라이언스에서 해당 드라이브가 설치된 위치를 표시합니다.

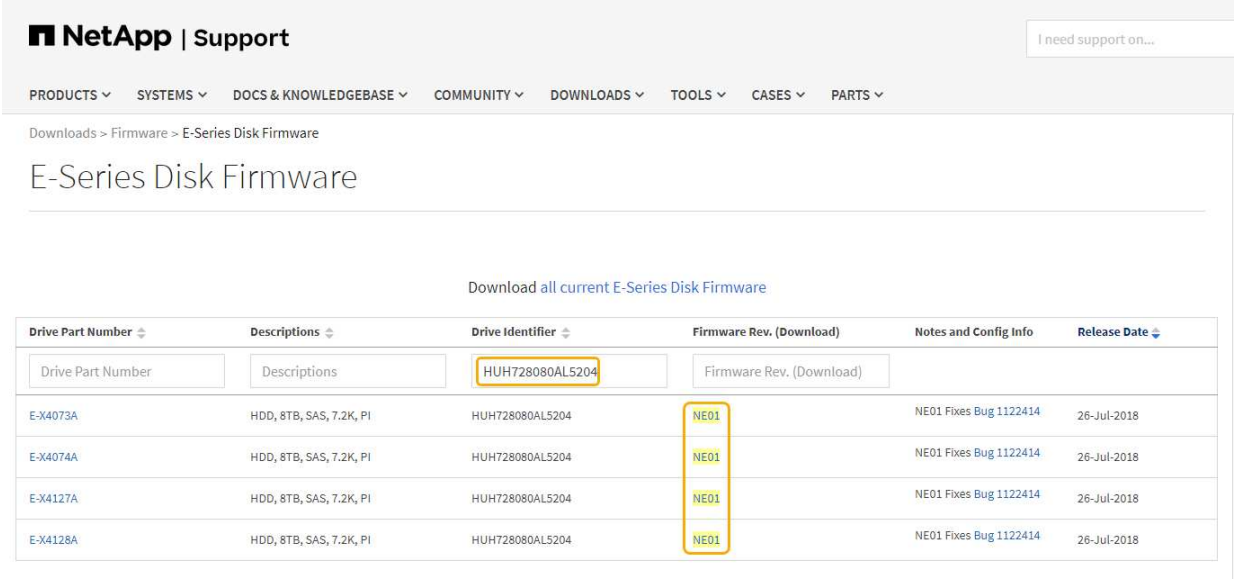
8. 사용 가능한 드라이브 펌웨어 업그레이드를 다운로드하고 준비합니다.
   a. 웹 브라우저를 열고 NetApp Support 웹 사이트로 이동한 다음 ID 및 암호를 사용하여 로그인합니다.

      "NetApp 지원"

   b. NetApp Support 웹 사이트에서 * Downloads * 탭을 선택한 다음, * E-Series Disk Drive Firmware * 를 선택합니다.

      E-Series 디스크 펌웨어 페이지가 표시됩니다.

   c. 스토리지 어플라이언스에 설치된 각 * 드라이브 식별자 * 를 검색하고 각 드라이브 ID에 최신 펌웨어 버전이 있는지 확인합니다.
      - 펌웨어 개정판이 링크가 아닌 경우 이 드라이브 식별자는 최신 펌웨어 개정판을 가지고 있습니다.
      - 드라이브 식별자에 대해 하나 이상의 드라이브 부품 번호가 나열되면 해당 드라이브에 대해 펌웨어 업그레이드를 사용할 수 있습니다. 펌웨어 파일을 다운로드할 링크를 선택할 수 있습니다.



d. 최신 펌웨어 개정판이 나열된 경우 펌웨어 개정판에서 링크를 선택합니다 (다운로드) 열을 클릭하여 펌웨어 파일이 포함된 '.zip' 아카이브를 다운로드합니다.

e. 지원 사이트에서 다운로드한 드라이브 펌웨어 아카이브 파일의 압축을 풉니다.

9. 드라이브 펌웨어 업그레이드를 설치합니다.

a. SANtricity 스토리지 관리자 드라이브 펌웨어 다운로드 - 패키지 추가 창에서 * 추가 * 를 선택합니다.

b. 펌웨어 파일이 포함된 디렉터리로 이동하여 최대 4개의 펌웨어 파일을 선택합니다.

드라이브 펌웨어 파일의 파일 이름은 +D_HUC101212CSS600_30602291_MS01_2800_0002.DLP와 비슷합니다

동일한 드라이브의 펌웨어를 업그레이드할 펌웨어 파일을 두 개 이상 선택하면 파일 충돌 오류가 발생할 수 있습니다. 파일 충돌 오류가 발생하면 오류 대화 상자가 나타납니다. 이 오류를 해결하려면 * 확인 * 을 선택하고 드라이브의 펌웨어 업그레이드에 사용할 펌웨어 파일을 제외한 다른 모든 펌웨어 파일을 제거합니다. 펌웨어 파일을 제거하려면 전송할 패키지 정보 영역에서 펌웨어 파일을 선택하고 * 제거 * 를 선택합니다. 또한 한 번에 최대 4개의 드라이브 펌웨어 패키지만 선택할 수 있습니다.

c. OK * 를 선택합니다.

시스템에서 전송할 패키지 정보 영역을 선택한 펌웨어 파일로 업데이트합니다.

d. 다음 * 을 선택합니다.

드라이브 펌웨어 다운로드 - 드라이브 선택 창이 열립니다.

- 어플라이언스의 모든 드라이브에서 구성 정보 및 업그레이드 자격이 검사됩니다.
- 선택한 펌웨어로 업그레이드할 수 있는 호환 가능한 드라이브의 선택(스토리지 배열에 있는 드라이브의 종류에 따라 다름)이 표시됩니다. 온라인 작업으로 업그레이드할 수 있는 드라이브는 기본적으로 표시됩니다.
- 드라이브의 선택한 펌웨어가 제안된 펌웨어 정보 영역에 나타납니다. 펌웨어를 변경해야 하는 경우 * Back * 을 선택하여 이전 대화 상자로 돌아갑니다.

e. Drive 업그레이드 기능에서 * Parallel * 다운로드 작업 또는 * All * 을 선택합니다.

어플라이언스가 유지보수 모드일 때 모든 드라이브 및 모든 볼륨에 대해 I/O 작업이 중지되므로 이러한 업그레이드 방법 중 하나를 사용할 수 있습니다.

f. 호환 드라이브에서 선택한 펌웨어 파일을 업그레이드할 드라이브를 선택합니다.

- 하나 이상의 드라이브에 대해 업그레이드할 각 드라이브를 선택합니다.
- 모든 호환 드라이브에 대해 * 모두 선택 * 을 선택합니다.

  모범 사례는 동일한 모델의 모든 드라이브를 동일한 펌웨어 개정판으로 업그레이드하는 것입니다.

g. 마침 * 을 선택한 다음 "예"를 입력하고 * 확인 * 을 선택합니다.

- 드라이브 펌웨어의 다운로드 및 업그레이드가 시작되며, 모든 드라이브의 펌웨어 전송 상태를 나타내는 Drive Firmware - Progress(드라이브 펌웨어 다운로드 - 진행) 가 표시됩니다.
- 업그레이드에 참여하는 각 드라이브의 상태가 업데이트된 장치의 전송 진행 열에 나타납니다.

  모든 드라이브가 24 드라이브 시스템에서 업그레이드된 경우 드라이브 펌웨어의 병렬 업그레이드 작업을 완료하는 데 90초 정도 걸릴 수 있습니다. 더 큰 시스템에서는 실행 시간이 약간 더 길어집니다.

h. 펌웨어 업그레이드 프로세스 중에 다음을 수행할 수 있습니다. +

- 진행 중인 펌웨어 업그레이드를 중지하려면 * Stop * 을 선택합니다. 현재 진행 중인 펌웨어 업그레이드가 모두 완료되었습니다. 펌웨어 업그레이드를 시도한 모든 드라이브는 개별 상태를 표시합니다. 나머지 드라이브는 시도되지 않음 상태로 나열됩니다.

  > 진행 중인 드라이브 펌웨어 업그레이드를 중지하면 데이터가 손실되거나 드라이브를 사용할 수 없게 될 수 있습니다.

- 펌웨어 업그레이드 진행률 요약의 텍스트 보고서를 저장하려면 * 다른 이름으로 저장 * 을 선택합니다. 보고서는 기본 .log 파일 확장자로 저장됩니다. 파일 확장자나 디렉터리를 변경하려면 드라이브 다운로드 로그 저장 에서 매개 변수를 변경합니다.

i. 드라이브 펌웨어 다운로드 - 진행 을 사용하여 드라이브 펌웨어 업그레이드 진행률을 모니터링합니다. Drives Updated 영역에는 펌웨어 업그레이드를 위해 예약된 드라이브 목록과 각 드라이브의 다운로드 및 업그레이드 전송 상태가 포함되어 있습니다.

   업그레이드에 참여하는 각 드라이브의 진행 상황과 상태가 전송 진행 열에 나타납니다. 업그레이드 중에 오류가 발생하면 적절한 권장 조치를 취하십시오.

   - * 보류 중 *

     이 상태는 예약되었지만 아직 시작되지 않은 온라인 펌웨어 다운로드 작업에 대해 표시됩니다.

   - * 진행 중 *

     펌웨어가 드라이브로 전송되고 있습니다.

   - * 재구성 진행 중 *

     이 상태는 드라이브를 빠르게 재구성할 때 볼륨 전송이 발생하는 경우에 표시됩니다. 이는 일반적으로 컨트롤러 재설정 또는 오류 때문에 컨트롤러 소유자가 볼륨을 전송했기 때문입니다.

시스템에서 드라이브의 전체 재구성을 시작합니다.

- * 실패 - 부분 *

  문제가 발생하여 나머지 파일이 전송되지 않도록 하기 전에는 펌웨어가 드라이브에 일부만 전송되었습니다.

- * 실패 - 잘못된 상태 *

  펌웨어가 유효하지 않습니다.

- * 실패 - 기타 *

  드라이브의 물리적 문제로 인해 펌웨어를 다운로드할 수 없습니다.

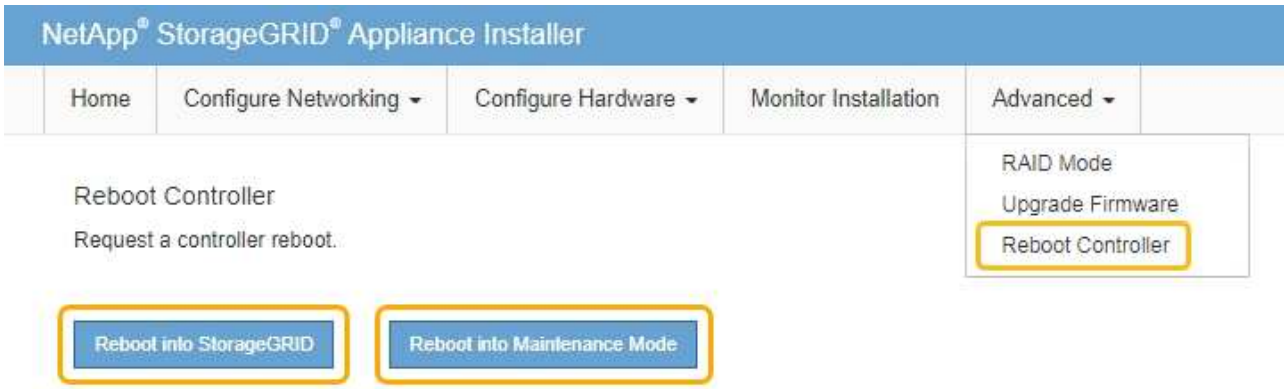
- * 시도 안 함 *

  펌웨어가 다운로드되지 않았습니다. 이러한 이유로 인해 다운로드가 중지되었거나 드라이브가 업그레이드를 받을 수 없거나 오류로 인해 다운로드가 발생하지 않았습니다.

- * 성공 *

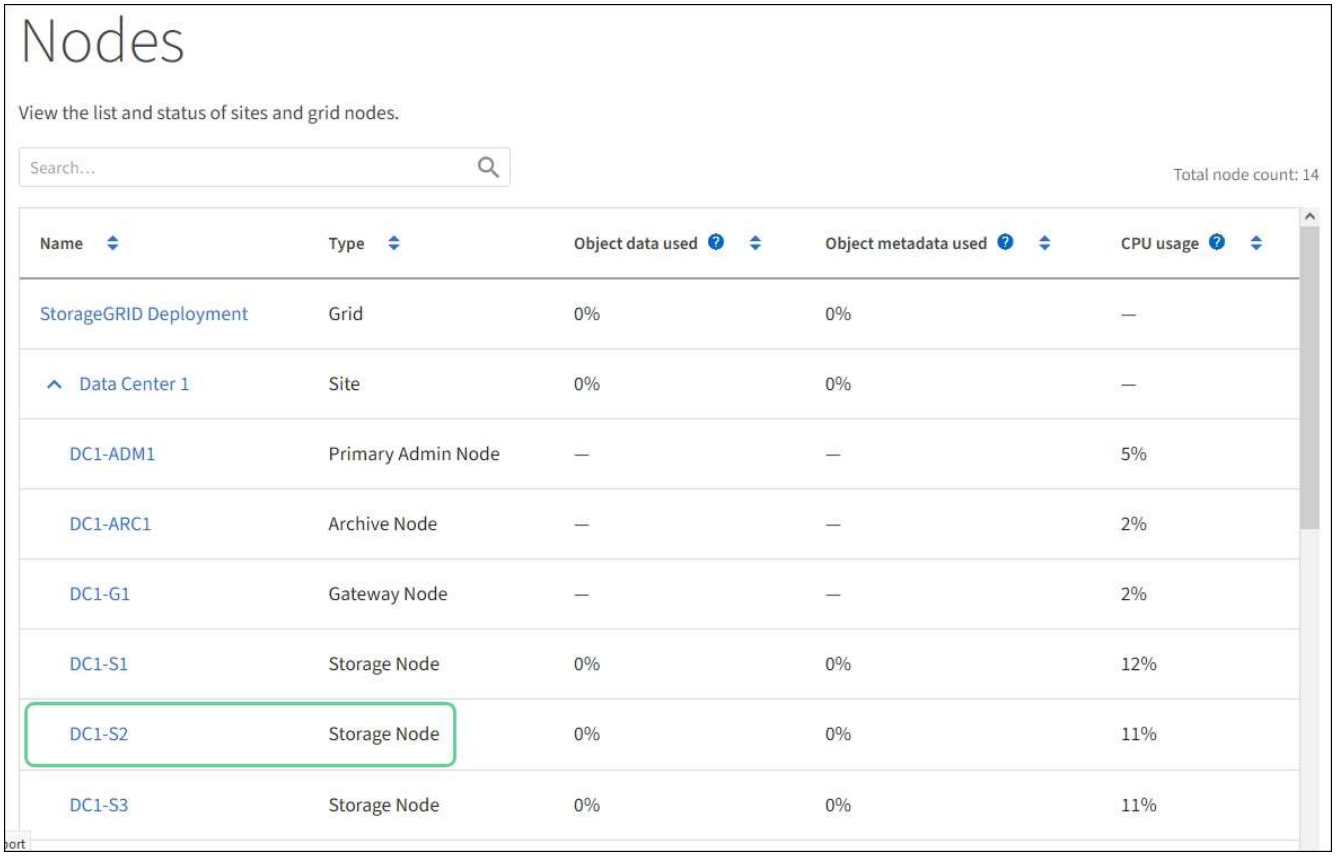
  펌웨어를 성공적으로 다운로드했습니다.

10. 드라이브 펌웨어 업그레이드가 완료된 후:
    - 드라이브 펌웨어 다운로드 마법사를 닫으려면 * 닫기 * 를 선택합니다.
    - 마법사를 다시 시작하려면 * 전송 추가 * 를 선택합니다.
11. 이 절차가 성공적으로 완료되었고 노드가 유지보수 모드일 때 수행할 추가 절차가 있는 경우 지금 수행합니다. 작업을 완료했거나 오류가 발생하여 다시 시작하려면 * 고급 * > * 컨트롤러 재부팅 * 을 선택하고 다음 옵션 중 하나를 선택합니다.
    - StorageGRID * 로 재부팅 * 을 선택합니다
    - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. 절차 중에 오류가 발생하여 다시 시작하려면 이 옵션을 선택합니다. 노드가 유지보수 모드로 재부팅된 후 장애가 발생한 절차의 적절한 단계에서 다시 시작하십시오.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. 노드 * 페이지는 어플라이언스 노드에 대한 정상 상태(노드 이름 왼쪽에 아이콘이 없음)를 표시해야 합니다. 이는 활성화된 알림이 없고 노드가

그리드에 연결되었음을 나타냅니다.



E2700 컨트롤러를 교체합니다

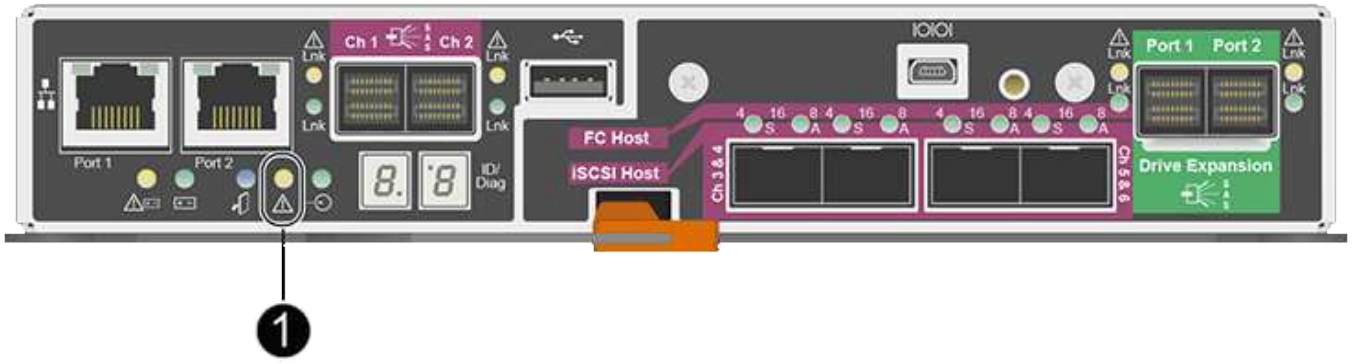
E2700 컨트롤러가 최적의 상태로 작동하지 않거나 오류가 발생한 경우 교체해야 할 수 있습니다.

필요한 것

- 교체할 컨트롤러와 부품 번호가 동일한 교체 컨트롤러가 있습니다.
- 컨트롤러에 연결된 각 케이블을 식별하는 라벨이 있습니다.
- 정전기 방지 보호 기능이 있습니다.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

이 작업에 대해

컨트롤러에서 황색 서비스 조치 필요 LED(그림 1에 표시됨)를 확인하여 컨트롤러에 장애가 있는지 확인할 수 있습니다. 이 LED가 켜져 있으면 컨트롤러를 교체해야 합니다.



컨트롤러를 교체할 때 어플라이언스 스토리지 노드에 액세스할 수 없습니다. E2700 컨트롤러가 충분히 작동하는 경우 E5500SG 컨트롤러를 유지보수 모드로 전환할 수 있습니다.

컨트롤러를 교체할 때는 원래 컨트롤러에서 배터리를 분리하여 교체 컨트롤러에 설치해야 합니다.

단계

1. 컨트롤러 제거를 준비합니다.

   SANtricity 저장소 관리자를 사용하여 다음 단계를 수행합니다.

   a. 현재 컨트롤러에 설치되어 있는 SANtricity OS 소프트웨어 버전을 기록해 둡니다.
   b. 현재 설치된 NVSRAM 버전을 기록해 둡니다.
   c. 드라이브 보안 기능이 활성화된 경우, 저장된 키가 있는지, 설치에 필요한 암호를 알고 있는지 확인하십시오.

   > * 데이터 액세스 손실 및 # 8212; * 어플라이언스의 모든 드라이브가 보안이 활성화된 경우 SANtricity 스토리지 관리자의 엔터프라이즈 관리 창을 사용하여 보안 드라이브의 잠금을 해제할 때까지 새 컨트롤러가 어플라이언스에 액세스할 수 없습니다.

   d. 구성 데이터베이스를 백업합니다.

      컨트롤러를 제거할 때 문제가 발생하면 저장된 파일을 사용하여 구성을 복원할 수 있습니다.

   e. 어플라이언스에 대한 지원 데이터를 수집합니다.

   > 구성 요소를 교체하기 전과 교체 후에 지원 데이터를 수집하면 교체로 문제가 해결되지 않을 경우 기술 지원 부서에 전체 로그 세트를 보낼 수 있습니다.

2. StorageGRID 어플라이언스가 StorageGRID 시스템에서 실행 중인 경우 E5500SG 컨트롤러를 유지보수 모드로 설정합니다.
3. E2700 컨트롤러가 제어된 방식으로 종료가 가능하도록 충분히 작동하는지 확인하려면 모든 작업이 완료되었는지 확인하십시오.

   a. Array Management 창의 제목 표시줄에서 * Monitor * > * Reports * > * Operations in Progress * 를 선택합니다.
   b. 모든 작업이 완료되었는지 확인합니다.

4. 단일 E2700 컨트롤러 교체 절차의 지침을 따라 다음 단계를 완료하십시오.

a. 케이블에 레이블을 지정한 다음 케이블을 분리합니다.

> 성능 저하를 방지하려면 케이블을 비틀거나 접거나 끼거나 밟지 마십시오.

b. 오류가 발생한 컨트롤러를 제품에서 분리합니다.

c. 컨트롤러 덮개를 분리합니다.

d. 나비 나사를 풀고 오류가 발생한 컨트롤러에서 배터리를 분리합니다.

e. 교체 컨트롤러에 배터리를 설치하고 컨트롤러 덮개를 장착합니다.

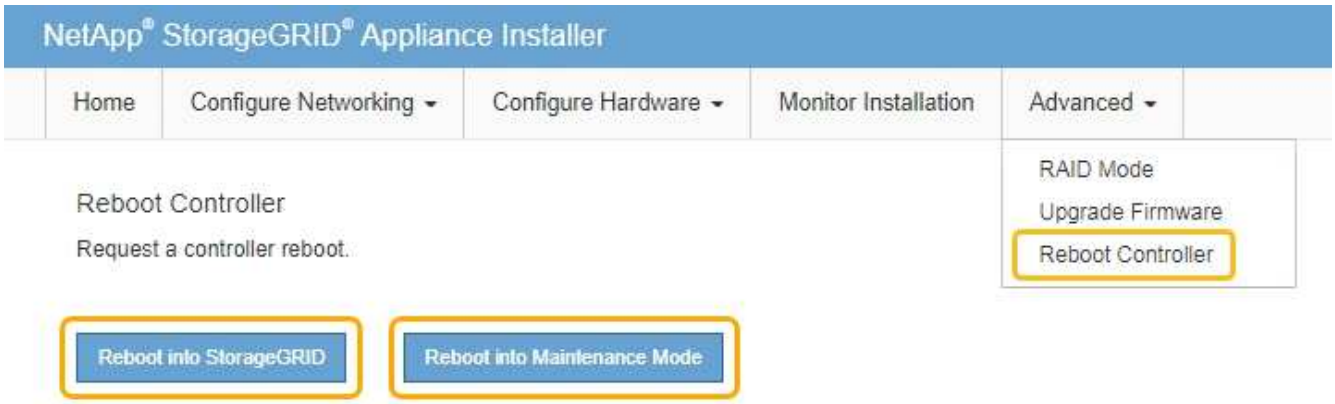
f. 교체 컨트롤러를 제품에 설치합니다.

g. 케이블을 교체합니다.

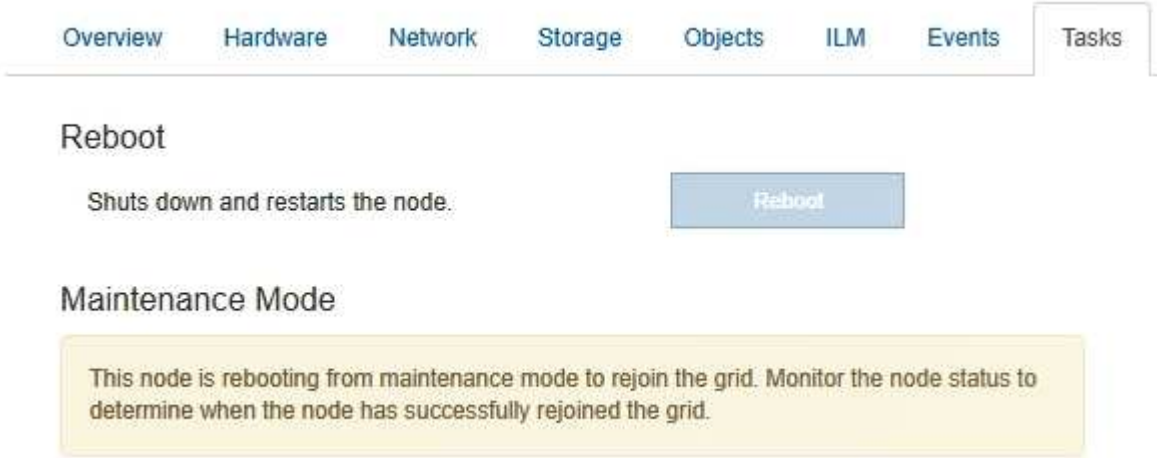
h. E2700 컨트롤러가 재부팅될 때까지 기다립니다. 7세그먼트 디스플레이에 99 상태가 표시되는지 확인합니다.

5. 보안 드라이브를 사용하는 경우 드라이브 보안 키를 가져옵니다.

6. 제품을 정상 작동 모드로 되돌리십시오. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * StorageGRID * 으로 재부팅 * 을 선택합니다.

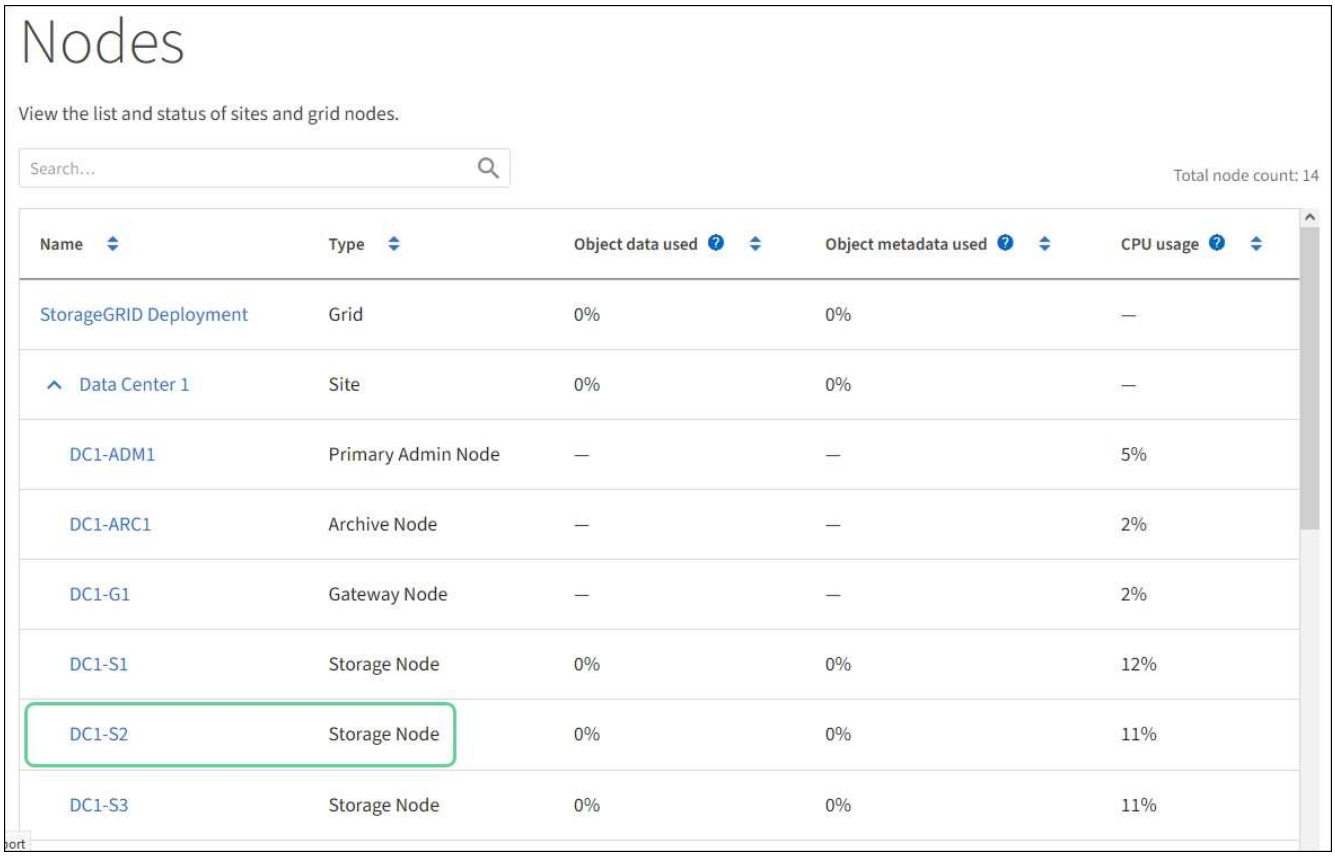


재부팅 중 다음 화면이 나타납니다.



어플라이언스가 재부팅되고 그리드에 다시 추가됩니다. 이 프로세스는 최대 20분 정도 소요될 수 있습니다.

7. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인합니다. 그리드 관리자에서 노드 페이지에 어플라이언스 노드에 대한 정상 상태(노드 이름 왼쪽에 아이콘이 없음)가 표시되는지 확인합니다. 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



8. SANtricity 스토리지 관리자에서 새 컨트롤러가 최적화되었는지 확인하고 지원 데이터를 수집합니다.

관련 정보

"NetApp E-Series 및 EF-Series 하드웨어 교체 절차 를 참조하십시오"

"NetApp 설명서: E2700 시리즈"

E5500SG 컨트롤러를 교체합니다

E5500SG 컨트롤러를 교체해야 할 수 있습니다.

필요한 것

다음 리소스에 대한 액세스 권한이 있어야 합니다.

- E-Series 하드웨어 교체 정보는 NetApp Support 사이트(+)에서 확인할 수 있습니다http://mysupport.netapp.com/["mysupport.netapp.com"^]
- E5600 설명서를 참조하십시오
- 제품이 다 되었습니다 유지보수 모드로 전환되었습니다.

이 작업에 대해

두 컨트롤러가 모두 정상적으로 작동하는 경우 제어된 종료를 허용하기 전에 E5500SG 컨트롤러를 먼저 종료하여 E2700 컨트롤러에 대한 연결을 중단할 수 있습니다.

> StorageGRID 소프트웨어를 설치하기 전에 컨트롤러를 교체하는 경우 이 절차를 완료한 후 즉시 StorageGRID 어플라이언스 설치 프로그램에 액세스하지 못할 수 있습니다. 어플라이언스와 동일한 서브넷에 있는 다른 호스트에서 StorageGRID 어플라이언스 설치 프로그램에 액세스할 수 있지만 다른 서브넷에 있는 호스트에서는 액세스할 수 없습니다. 이 조건은 15분 내에 해결되어야 하며(원래 컨트롤러의 ARP 캐시 항목이 시간 초과될 때), 또는 로컬 라우터 또는 게이트웨이에서 수동으로 이전의 ARP 캐시 항목을 삭제하여 즉시 조건을 지울 수 있습니다.

단계

1. 정전기 방지 보호 장치를 사용합니다.
2. E54600 SG 컨트롤러에 연결된 각 케이블에 레이블을 지정하여 케이블을 올바르게 다시 연결할 수 있습니다.

   > 성능 저하를 방지하려면 케이블을 비틀거나 접거나 끼거나 밟지 마십시오. 케이블을 5cm(2인치) 반경보다 더 구부리지 마십시오.

3. 어플라이언스를 유지보수 모드로 전환한 후 E5500SG 컨트롤러를 종료합니다.
   a. 그리드 노드에 로그인합니다.
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

   b. E5500SG 컨트롤러를 종료합니다. + " * shutdown -h now * "
4. 엔클로저의 전원을 끄고 컨트롤러 후면의 모든 LED 및 7개 세그먼트 디스플레이 작동이 멈출 때까지 기다립니다.
5. 케이블을 분리합니다.
6. E54600 SG 컨트롤러 설명서에 설명된 대로 컨트롤러를 분리합니다.
7. E54600 SG 컨트롤러 설명서에 설명된 대로 새 컨트롤러를 삽입합니다.
8. 모든 케이블을 교체합니다.
9. 엔클로저의 전원을 다시 켭니다.
10. 7개 세그먼트 코드를 모니터링합니다.
    - E2700 컨트롤러:

      마지막 LED 상태는 99입니다.

    - E5500SG 컨트롤러:

      마지막 LED 상태는 HA입니다.

11. Grid Manager에서 어플라이언스 스토리지 노드의 상태를 모니터링합니다.

어플라이언스 스토리지 노드가 예상 상태로 돌아가는지 확인합니다.

관련 정보

"NetApp E-Series 및 EF-Series 하드웨어 교체 절차 를 참조하십시오"

"NetApp 설명서: E5600 시리즈"

다른 하드웨어 구성 요소를 교체합니다

StorageGRID 제품에서 드라이브, 팬, 전원 공급 장치 또는 배터리를 교체해야 할 수 있습니다.

필요한 것

- E-Series 하드웨어 교체 절차가 있습니다.
- 제품이 다 되었습니다 유지보수 모드로 전환 구성 요소 교체 절차에서 제품을 종료해야 하는 경우

이 작업에 대해

드라이브, 전원 팬 캐니스터, 팬 캐니스터, 전원 캐니스터, 배터리 교체 또는 드라이브 드로어는 E2700 및 E5600 스토리지 어레이의 표준 절차를 참조하십시오. 하드웨어 자체의 제거 및 교체에 대한 단계별 지침에 초점을 맞춥니다. 대부분의 SANtricity 스토리지 관리자 절차는 어플라이언스에 적용되지 않습니다.

SG5612 구성 요소 교체 지침

FRU	을 참조하십시오
드라이브	E2600, E2700, E5400, E5500, E5600 또는 12 드라이브 또는 24 드라이브 트레이의 드라이브 교체를 위한 E-Series 지침의 단계를 따르십시오.
전원 팬 캐니스터	E5612 또는 E5624 컨트롤러-드라이브 트레이에서 장애가 발생한 전원 팬 캐니스터를 교체하는 E-Series 지침에 따라 작업을 수행하십시오
E2700 컨트롤러의 배터리(컨트롤러 분리 필요)	의 단계를 따릅니다 E2700 컨트롤러를 교체합니다기존 컨트롤러에 새 배터리를 설치합니다.

SG5660 구성요소 교체 지침

FRU	을 참조하십시오
드라이브	E2660, E2760, E5460, E5560 또는 E5660 트레이의 드라이브 교체에 대한 E-Series 지침 의 단계를 따릅니다.
전원 캐니스터	E5660 컨트롤러-드라이브 트레이에서 장애가 발생한 전원 캐니스터를 교체하는 E-Series 지침에 따라 작업을 수행합니다

FRU	을 참조하십시오
팬 캐니스터	E5660 컨트롤러-드라이브 트레이에서 장애가 발생한 팬 캐니스터를 교체하는 E-Series 지침에 따라 작업을 수행합니다
E2700 컨트롤러의 배터리(컨트롤러 분리 필요)	의 단계를 따릅니다 E2700 컨트롤러를 교체합니다기존 컨트롤러에 새 배터리를 설치합니다.

관련 정보

"NetApp E-Series 및 EF-Series 하드웨어 교체 절차 를 참조하십시오"

"NetApp 설명서: E2700 시리즈"

"NetApp 설명서: E5600 시리즈"

E5500SG 컨트롤러의 링크 구성을 변경합니다

E5500SG 컨트롤러의 이더넷 링크 구성을 변경할 수 있습니다. 포트 연결 모드, 네트워크 연결 모드 및 링크 속도를 변경할 수 있습니다.

필요한 것

E5500SG 컨트롤러를 유지보수 모드로 설정합니다.

> StorageGRID 어플라이언스를 유지보수 모드로 전환하면 원격 액세스가 불가능한 경우가 드물게 있습니다.

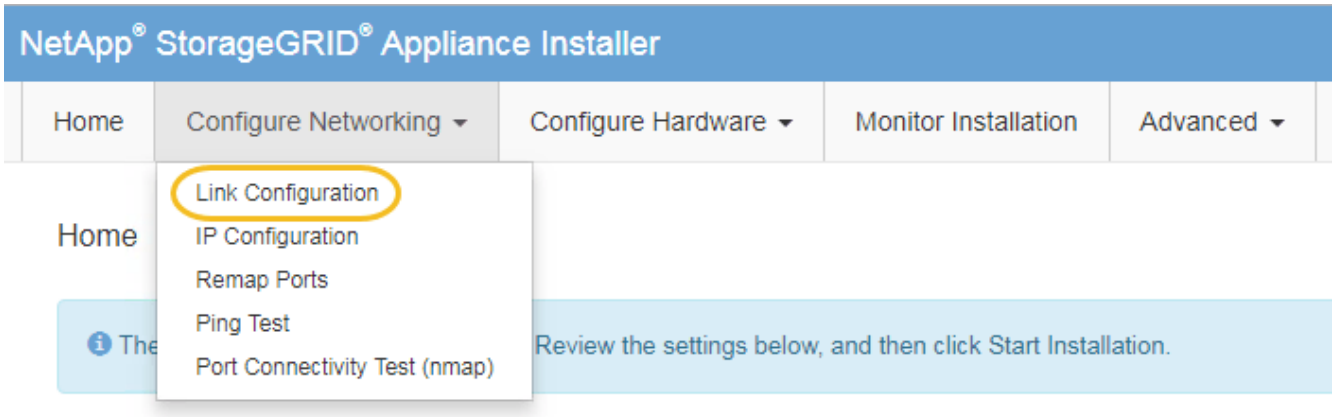
이 작업에 대해

E5500SG 컨트롤러의 이더넷 링크 구성을 변경하는 옵션은 다음과 같습니다.

- 포트 결합 모드 * 를 고정에서 집계로, 또는 Aggregate에서 고정으로 변경
- Active-Backup에서 LACP로 또는 LACP에서 Active-Backup으로 * 네트워크 결합 모드 * 변경
- VLAN 태그 지정 활성화 또는 비활성화 또는 VLAN 태그 값 변경
- 링크 속도를 10GbE에서 25GbE로, 25GbE에서 10GbE로 변경합니다

단계

1. 메뉴에서 * 네트워킹 구성 * > * 링크 구성 * 을 선택합니다.



2. 링크 구성을 원하는 대로 변경합니다.

   옵션에 대한 자세한 내용은 ""네트워크 링크 구성"을 참조하십시오.

3. 선택 사항에 만족하면 * 저장 * 을 클릭합니다.

   > 연결된 네트워크 또는 링크를 변경한 경우 연결이 끊어질 수 있습니다. 1분 내에 다시 연결되지 않으면 어플라이언스에 할당된 다른 IP 주소 중 하나를 사용하여 StorageGRID 어플라이언스 설치 프로그램의 URL을 다시 입력합니다. + " * https://*E5600SG_Controller_IP*:8443*`

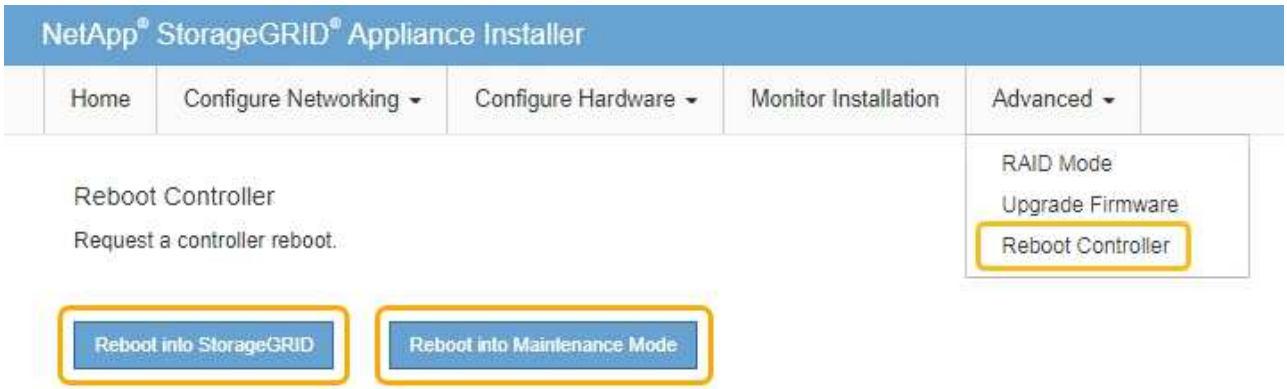
   VLAN 설정을 변경한 경우 어플라이언스의 서브넷이 변경되었을 수 있습니다. 어플라이언스의 IP 주소를 변경해야 하는 경우 에 따르십시오 IP 구성을 설정합니다 지침.

4. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * 핑 테스트 * 를 선택합니다.
5. Ping 테스트 도구를 사용하여 에서 변경한 링크 구성 변경의 영향을 받을 수 있는 네트워크의 IP 주소에 대한 연결을 확인합니다 링크 구성을 변경합니다 단계.

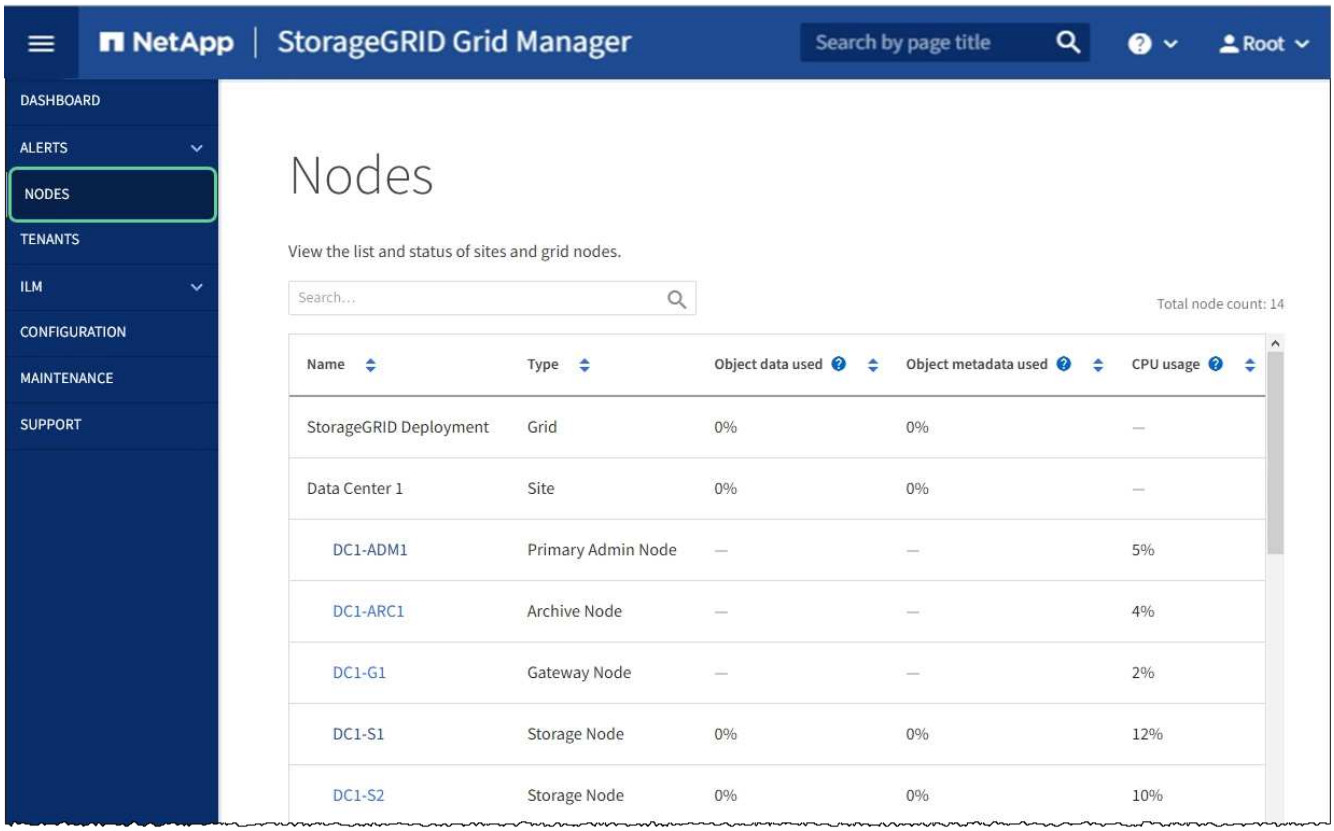
   수행할 다른 테스트 외에도 운영 관리 노드의 그리드 IP 주소와 하나 이상의 다른 스토리지 노드의 그리드 IP 주소를 ping할 수 있는지 확인합니다. 필요한 경우 링크 구성 문제를 해결하십시오.

6. 링크 구성 변경 사항이 작동한다고 만족하면 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.

   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

네트워크 링크 구성(SG5600)

MTU 설정을 변경합니다

어플라이언스 노드에 대한 IP 주소를 구성할 때 할당한 MTU 설정을 변경할 수 있습니다.

이 작업에 대해

네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

어플라이언스 노드를 재부팅하지 않고 MTU 설정을 변경하려면 IP 변경 도구를 사용합니다.

초기 설치 중에 StorageGRID 어플라이언스 설치 프로그램에서 클라이언트 또는 관리자 네트워크가 구성되지 않은 경우 유지보수 모드를 사용하여 MTU 설정을 변경합니다.

IP 변경 도구를 사용하여 MTU 설정을 변경합니다

필요한 것

Change IP 툴을 사용할 수 있는 "passwords.txt" 파일이 있습니다.

단계

IP 변경 도구에 액세스하여 에 설명된 대로 MTU 설정을 업데이트합니다 노드 네트워크 구성을 변경합니다.

유지보수 모드를 사용하여 MTU 설정을 변경합니다

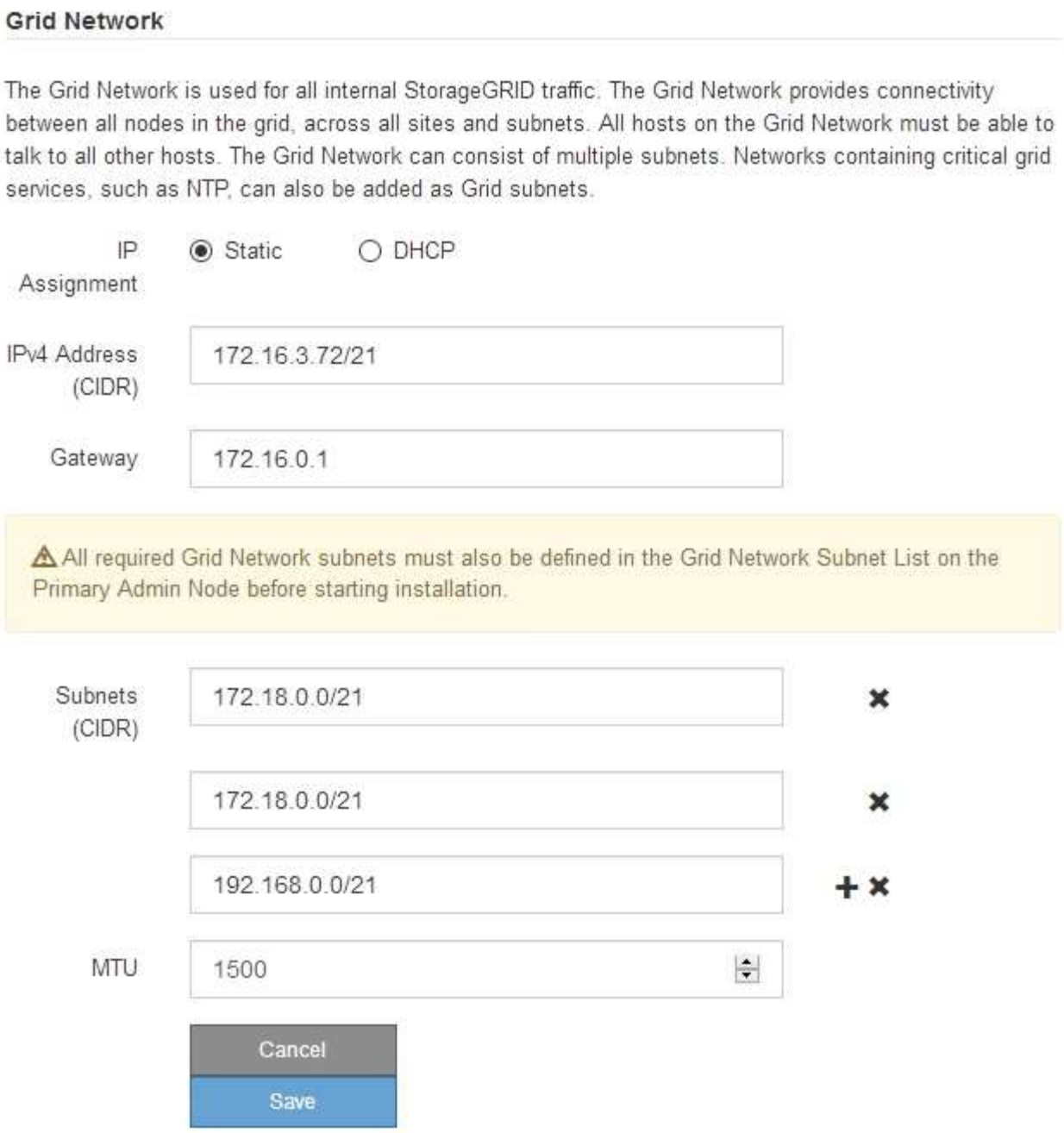
Change IP(IP 변경) 도구를 사용하여 이러한 설정에 액세스할 수 없는 경우 유지보수 모드를 사용하여 MTU 설정을 변경합니다.

필요한 것

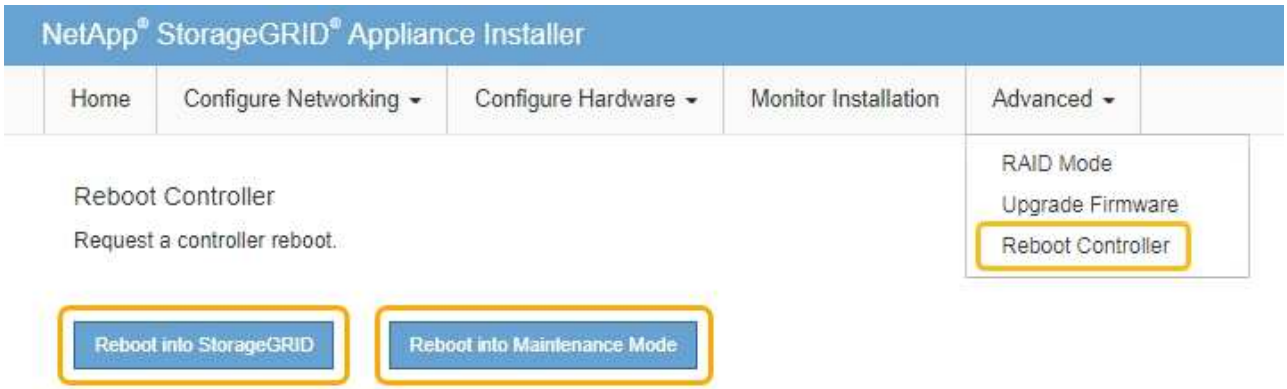
제품이 다 되었습니다 유지보수 모드로 전환되었습니다.

단계

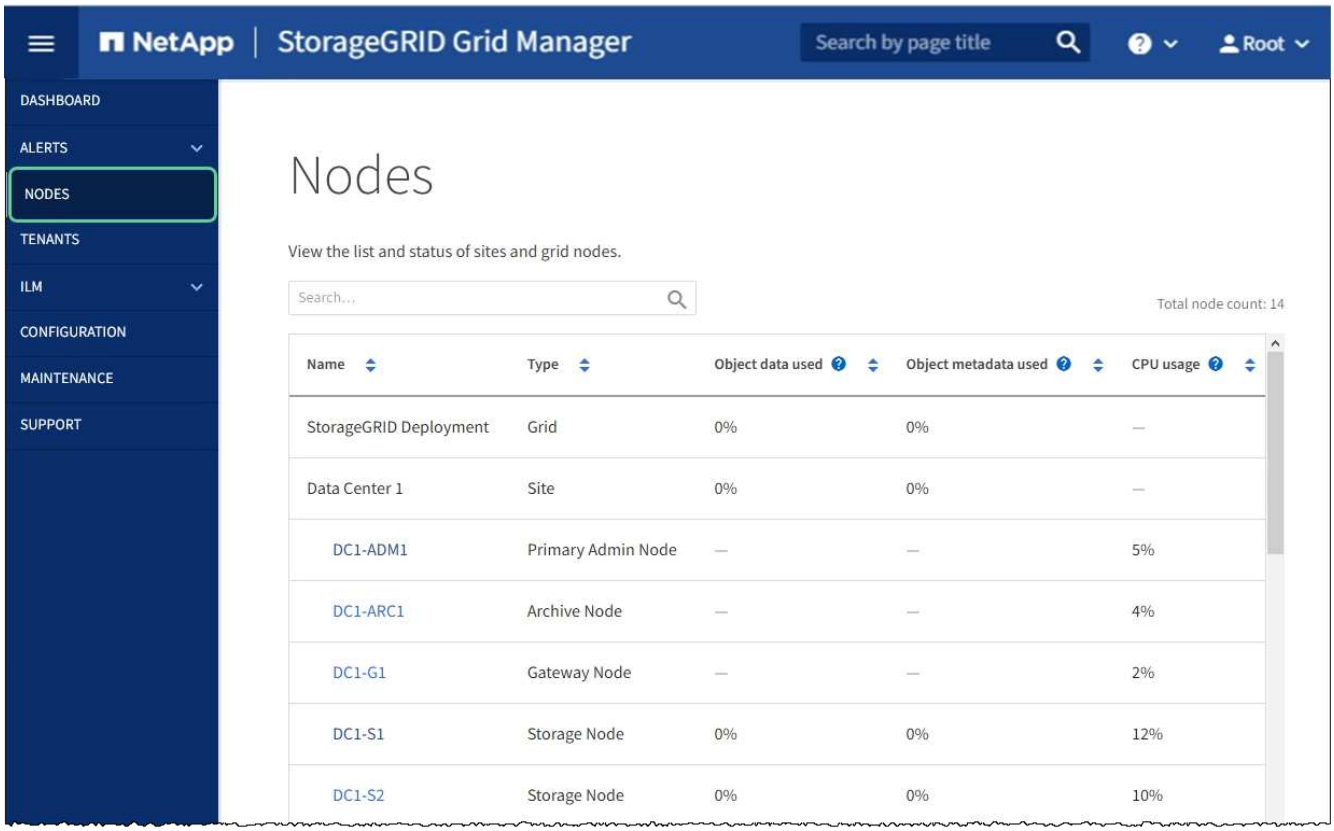
1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * IP 구성 * 을 선택합니다.
2. 그리드 네트워크, 관리자 네트워크 및 클라이언트 네트워크에 대한 MTU 설정을 원하는 대로 변경합니다.



3. 설정이 만족스러우면 * 저장 * 을 선택합니다.
4. 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.
   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

StorageGRID 관리

DNS 서버 구성을 확인합니다

이 어플라이언스 노드에서 현재 사용 중인 DNS(Domain Name System) 서버를 확인하고 일시적으로 변경할 수 있습니다.

필요한 것

제품이 다 되었습니다 유지보수 모드로 전환되었습니다.

이 작업에 대해

KMS의 호스트 이름이 IP 주소 대신 도메인 이름으로 지정되었기 때문에 암호화된 어플라이언스가 KMS(키 관리 서버) 또는 KMS 클러스터에 연결할 수 없는 경우 DNS 서버 설정을 변경해야 할 수 있습니다. 어플라이언스에 대한 DNS 설정에 대한 모든 변경 사항은 일시적이며 유지 관리 모드를 종료할 때 손실됩니다. 이러한 변경 사항을 영구적으로 적용하려면 Grid Manager(* 유지 관리 * > * 네트워크 * > * DNS 서버 *)에서 DNS 서버를 지정합니다.

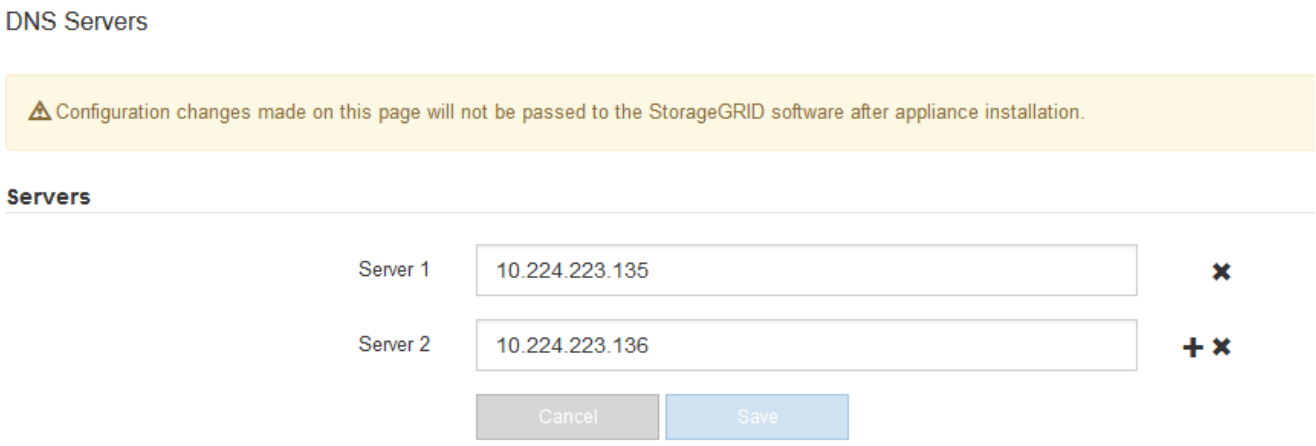
- KMS 서버가 호스트 이름에 대해 IP 주소 대신 정규화된 도메인 이름을 사용하여 정의된 노드 암호화 어플라이언스인 경우에만 DNS 구성을 일시적으로 변경해야 합니다.
- 노드 암호화 어플라이언스가 도메인 이름을 사용하여 KMS에 연결되는 경우 그리드에 정의된 DNS 서버 중 하나에 연결해야 합니다. 그런 다음 이러한 DNS 서버 중 하나가 도메인 이름을 IP 주소로 변환합니다.
- 노드가 그리드의 DNS 서버에 연결할 수 없거나 노드 암호화 어플라이언스 노드가 오프라인일 때 그리드 전체 DNS 설정을 변경한 경우 노드가 KMS에 연결할 수 없습니다. DNS 문제가 해결될 때까지 어플라이언스에 있는 암호화된 데이터를 해독할 수 없습니다.

KMS 연결을 방해하는 DNS 문제를 해결하려면 StorageGRID 어플라이언스 설치 프로그램에서 하나 이상의 DNS 서버의 IP 주소를 지정하십시오. 이러한 임시 DNS 설정을 사용하면 어플라이언스가 KMS에 연결하고 노드의 데이터를 해독할 수 있습니다.

예를 들어, 암호화된 노드가 오프라인 상태일 때 그리드의 DNS 서버가 변경되면 노드가 다시 온라인 상태가 될 때 KMS에 도달할 수 없습니다. KMS는 이전 DNS 값을 계속 사용하고 있기 때문입니다. StorageGRID 어플라이언스 설치 프로그램에 새 DNS 서버 IP 주소를 입력하면 임시 KMS 연결을 통해 노드 데이터를 해독할 수 있습니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 네트워킹 구성 * > * DNS 구성 * 을 선택합니다.
2. 지정된 DNS 서버가 올바른지 확인합니다.



3. 필요한 경우 DNS 서버를 변경합니다.

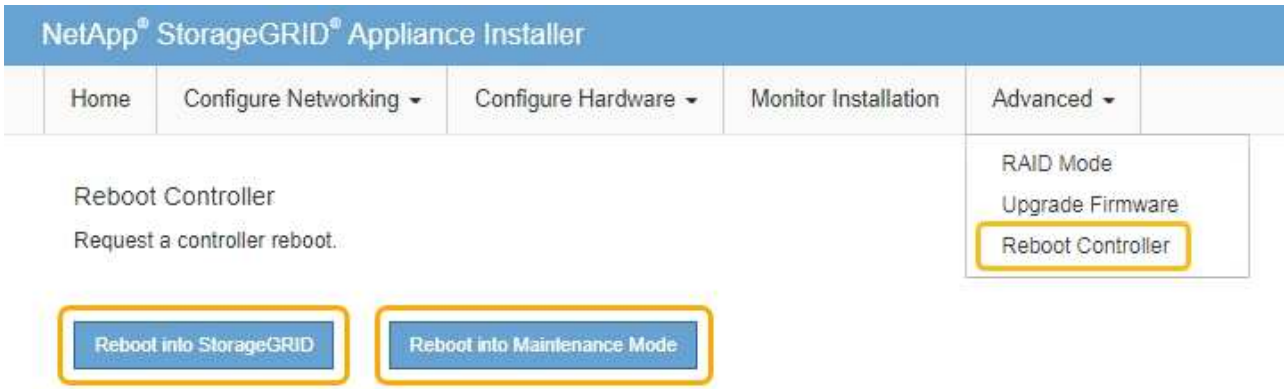
> DNS 설정에 대한 변경 사항은 일시적이며 유지 관리 모드를 종료할 때 손실됩니다.

4. 임시 DNS 설정이 만족스러우면 * Save * 를 선택합니다.

노드는 이 페이지에 지정된 DNS 서버 설정을 사용하여 KMS에 다시 연결하여 노드의 데이터를 해독할 수 있도록 합니다.

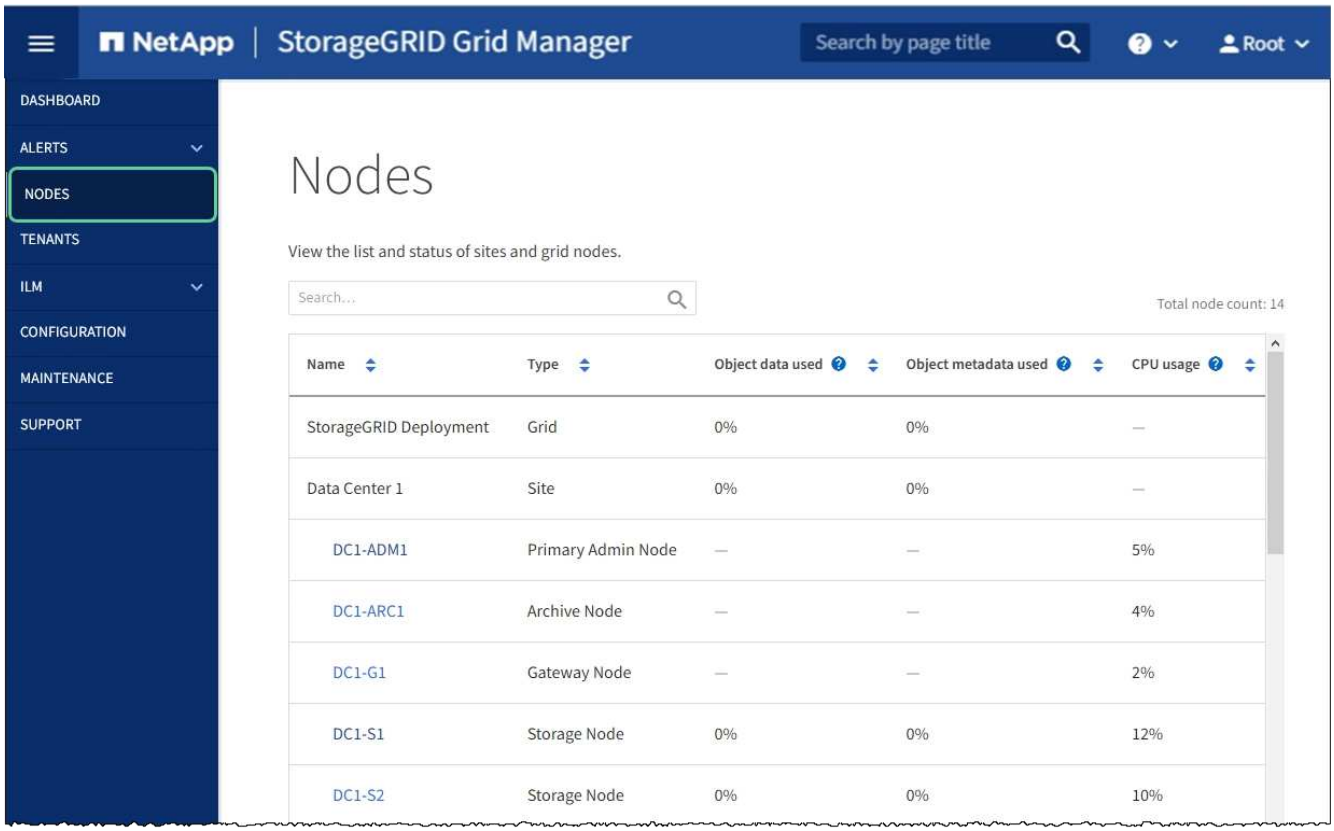
5. 노드 데이터가 해독된 후 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.

   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



> 노드가 재부팅되고 그리드에 다시 연결되면 Grid Manager에 나열된 시스템 전체 DNS 서버가 사용됩니다. 그리드를 다시 연결한 후 어플라이언스는 어플라이언스가 유지보수 모드일 때 StorageGRID 어플라이언스 설치 프로그램에 지정된 임시 DNS 서버를 더 이상 사용하지 않습니다.

어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



유지보수 모드(**SG5600**)에서 노드 암호화 모니터링

설치 중에 어플라이언스에 대한 노드 암호화를 활성화한 경우 노드 암호화 상태 및 키 관리 서버(KMS) 세부 정보를 포함하여 각 어플라이언스 노드의 노드 암호화 상태를 모니터링할 수 있습니다.

필요한 것

- 설치하는 동안 어플라이언스에 대해 노드 암호화가 활성화되어 있어야 합니다. 어플라이언스를 설치한 후에는 노드 암호화를 활성화할 수 없습니다.
- 제품이 다 되었습니다 유지보수 모드로 전환됩니다.

단계

1. StorageGRID 어플라이언스 설치 프로그램에서 * 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption ☑

Save

Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate >

Client certificate >

Clear KMS Key

Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

노드 암호화 페이지에는 다음 세 가지 섹션이 있습니다.

- 암호화 상태 는 어플라이언스에 대해 노드 암호화가 활성화되었는지 여부를 표시합니다.
- 키 관리 서버 세부 정보 는 어플라이언스를 암호화하는 데 사용되는 KMS에 대한 정보를 보여 줍니다. 서버 및 클라이언트 인증서 섹션을 확장하여 인증서 세부 정보 및 상태를 볼 수 있습니다.
  - 만료된 인증서 갱신과 같은 인증서 자체의 문제를 해결하려면 StorageGRID 관리 지침의 KMS 정보를 참조하십시오.
  - KMS 호스트에 연결할 때 예기치 않은 문제가 발생하는 경우 DNS(Domain Name System) 서버가 올바르고 어플라이언스 네트워킹이 올바르게 구성되었는지 확인합니다.

    DNS 서버 구성을 확인합니다

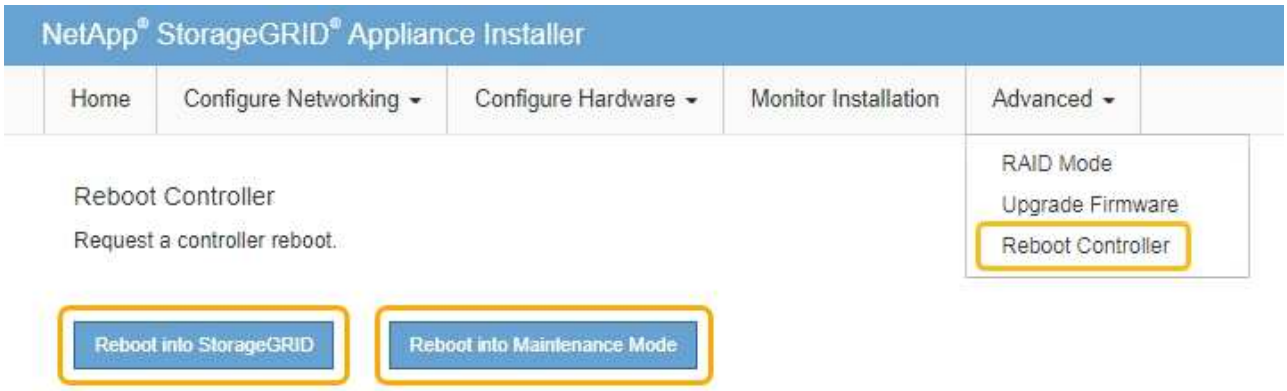
  - 인증서 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.
- KMS 키 지우기(Clear KMS Key)는 어플라이언스에 대한 노드 암호화를 해제하고, StorageGRID 사이트에 구성된 키 관리 서버와 어플라이언스를 제거하고, 어플라이언스에서 모든 데이터를 삭제합니다. KMS 키를

지워야 제품을 다른 StorageGRID 시스템에 설치할 수 있습니다.

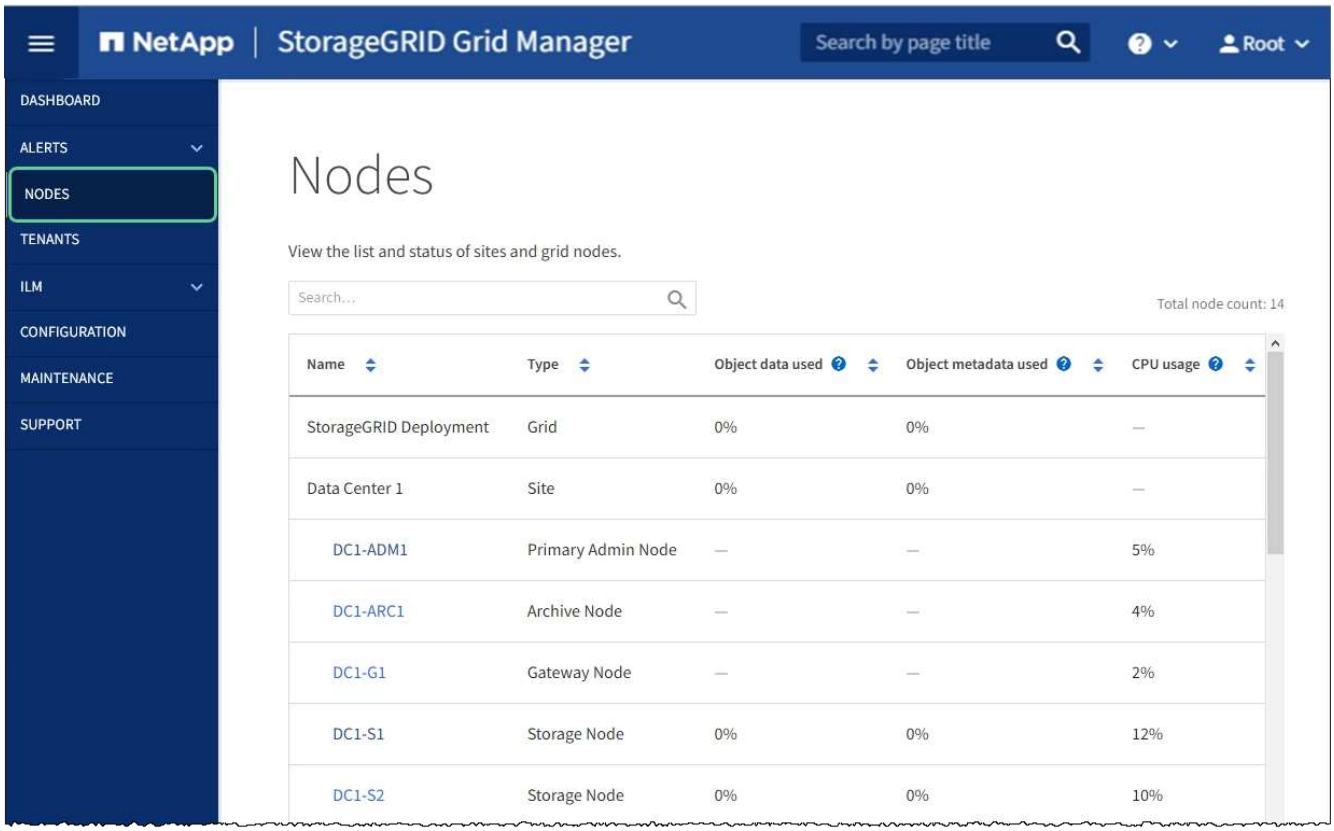
키 관리 서버 구성을 지웁니다

> KMS 구성을 지우면 어플라이언스에서 데이터가 삭제되어 영구적으로 액세스할 수 없게 됩니다. 이 데이터는 복구할 수 없습니다.

2. 노드 암호화 상태 확인을 마쳤으면 노드를 재부팅합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.
   - 노드를 그리드에 다시 조인하는 상태에서 컨트롤러를 재부팅하려면 * StorageGRID로 재부팅 * 을 선택합니다. 유지보수 모드에서 작업을 수행하고 노드를 정상 운영으로 전환할 준비가 되었으면 이 옵션을 선택합니다.
   - 유지보수 모드로 재부팅 * 을 선택하여 유지보수 모드로 남아 있는 노드를 사용하여 컨트롤러를 재부팅합니다. (이 옵션은 컨트롤러가 유지보수 모드일 때만 사용할 수 있습니다.) 그리드에 다시 연결하기 전에 노드에서 수행해야 하는 추가 유지보수 작업이 있는 경우 이 옵션을 선택합니다.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. nodes * 페이지에 어플라이언스 노드에 대한 정상 상태(아이콘 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



관련 정보

StorageGRID 관리

키 관리 서버 구성을 지웁니다

KMS(키 관리 서버) 구성을 지우면 어플라이언스에서 노드 암호화가 비활성화됩니다. KMS 구성을 삭제한 후에는 어플라이언스의 데이터가 영구적으로 삭제되며 더 이상 액세스할 수 없습니다. 이 데이터는 복구할 수 없습니다.

필요한 것

어플라이언스의 데이터를 보존해야 하는 경우 KMS 구성을 지우기 전에 노드 서비스 해제 절차를 수행하거나 노드를 복제해야 합니다.

> KMS를 삭제하면 제품의 데이터가 영구적으로 삭제되고 더 이상 액세스할 수 없게 됩니다. 이 데이터는 복구할 수 없습니다.

노드 서비스 해제 포함된 데이터를 StorageGRID의 다른 노드로 이동하려면 다음을 사용합니다.

이 작업에 대해

어플라이언스 KMS 구성을 지우면 노드 암호화가 비활성화되므로 어플라이언스 노드와 StorageGRID 사이트의 KMS 구성 간의 연결이 제거됩니다. 그러면 어플라이언스의 데이터가 삭제되고 어플라이언스가 사전 설치 상태로 유지됩니다. 이 프로세스는 되돌릴 수 없습니다.

KMS 구성을 지워야 합니다.

- KMS를 사용하지 않거나 다른 KMS를 사용하는 다른 StorageGRID 시스템에 제품을 설치하기 전에

> 동일한 KMS 키를 사용하는 StorageGRID 시스템에 어플라이언스 노드를 재설치하려는 경우 KMS 구성을 지우지 마십시오.

- KMS 구성이 손실되고 KMS 키를 복구할 수 없는 노드를 복구 및 재설치할 수 있습니다.
- 이전에 현장에서 사용 중이던 제품을 반환하기 전에
- 노드 암호화가 설정된 어플라이언스를 서비스 해제 후

> KMS를 제거하기 전에 어플라이언스의 전원을 해제하여 StorageGRID 시스템의 다른 노드로 데이터를 이동합니다. KMS를 폐기하기 전에 제거하면 데이터가 손실되고 어플라이언스가 작동하지 않을 수 있습니다.

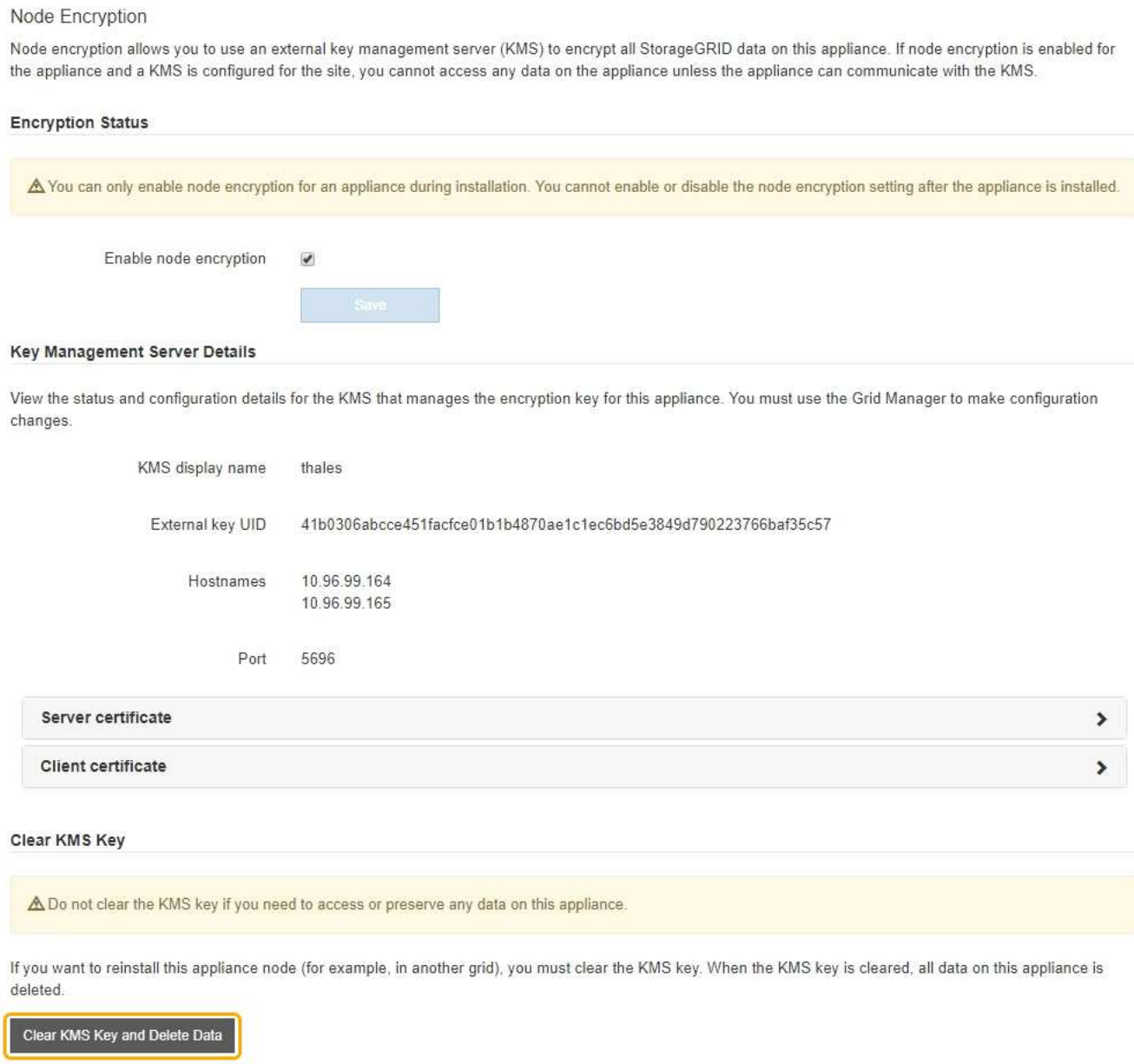
단계

1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

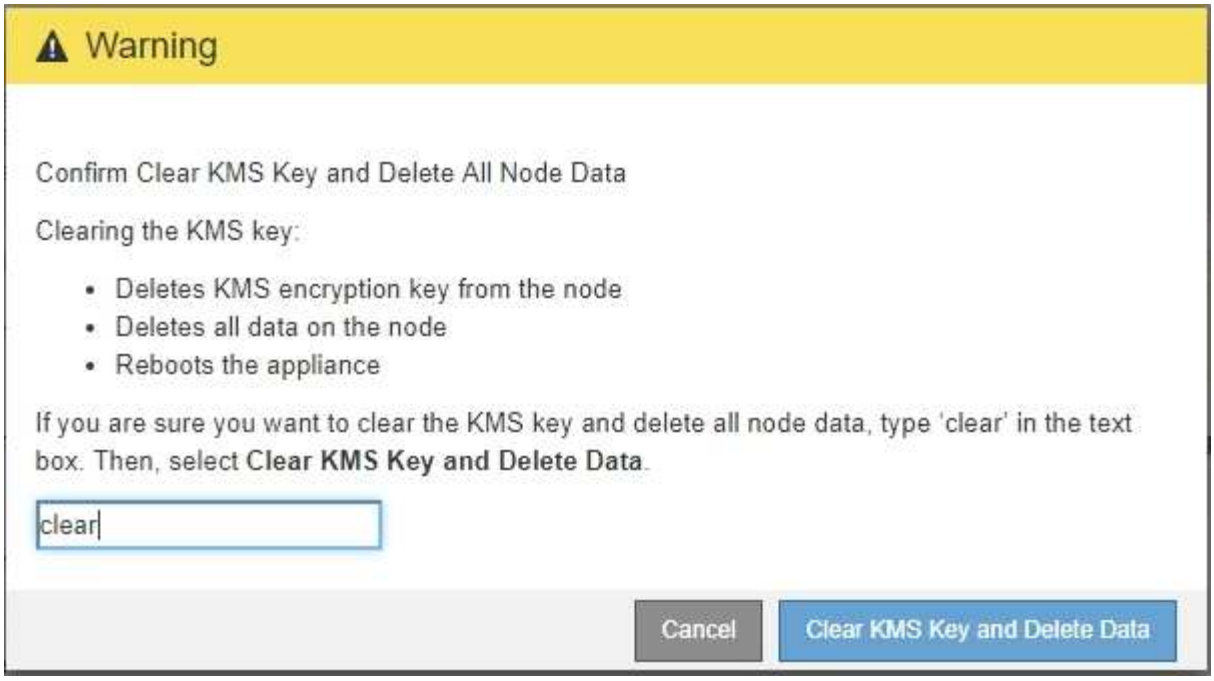
   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.



> KMS 구성이 삭제된 경우 어플라이언스의 데이터가 영구적으로 삭제됩니다. 이 데이터는 복구할 수 없습니다.

3. 창 아래쪽에서 * KMS 키 삭제 및 데이터 삭제 * 를 선택합니다.
4. KMS 구성을 지우려면 + " * clear * "+를 입력하고 * KMS 키 삭제 및 데이터 삭제 * 를 선택합니다.



KMS 암호화 키 및 모든 데이터가 노드에서 삭제되고 어플라이언스가 재부팅됩니다. 이 작업은 최대 20분이 소요될 수 있습니다.

5. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다. (+) * https://*Controller_IP*:8443*`

   '*Controller_IP*'는 3개의 StorageGRID 네트워크 중 어느 한 곳의 컴퓨팅 컨트롤러(스토리지 컨트롤러가 아님)의 IP 주소입니다.

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

6. 하드웨어 구성 * > * 노드 암호화 * 를 선택합니다.
7. 노드 암호화가 비활성화되었으며 * 키 관리 서버 세부 정보 * 및 * KMS 키 지우기 및 데이터 삭제 * 컨트롤의 키 및 인증서 정보가 창에서 제거되었는지 확인합니다.

   그리드에 다시 설치할 때까지 어플라이언스에서 노드 암호화를 다시 활성화할 수 없습니다.

작업을 마친 후

어플라이언스가 재부팅되고 KMS가 삭제되었으며 사전 설치 상태의 제품이 검증된 경우 StorageGRID 시스템에서 어플라이언스를 물리적으로 제거할 수 있습니다. 에 대한 자세한 내용은 복구 및 유지 관리 지침을 참조하십시오 어플라이언스 재설치를 준비합니다.

관련 정보

StorageGRID 관리

소프트웨어 설치 및 업그레이드

StorageGRID 소프트웨어를 업그레이드합니다

StorageGRID 소프트웨어 업그레이드: 개요

다음 지침에 따라 StorageGRID 시스템을 새 릴리즈로 업그레이드하십시오.

참조하십시오

다음 지침은 StorageGRID 11.6의 새로운 기능에 대해 설명하고 StorageGRID 시스템의 모든 노드를 새 릴리즈로 업그레이드하기 위한 단계별 지침을 제공합니다.

시작하기 전에

이 항목을 검토하여 StorageGRID 11.6의 새로운 기능 및 향상된 기능에 대해 알아보고, 더 이상 사용되지 않거나 제거된 기능이 있는지 확인하고, StorageGRID API의 변경 사항에 대해 알아보십시오.

- StorageGRID 11.6의 새로운 기능
- 제거되거나 사용되지 않는 기능
- Grid Management API 변경
- 테넌트 관리 API의 변경 사항

StorageGRID 11.6의 새로운 기능

이번 StorageGRID 릴리즈에는 다음과 같은 기능이 도입되었습니다.

사용 편의성 향상

Grid Manager 사용자 인터페이스는 사용자 환경을 개선하기 위해 크게 재설계되었습니다.

- 새로운 사이드바가 이전 사용자 인터페이스의 풀다운 메뉴를 대체합니다.
- 관련 옵션을 함께 유지하기 위해 여러 메뉴가 재구성되었습니다. 예를 들어, * 구성 * 메뉴에는 인증서, 키 관리 서버, 프록시 설정 및 신뢰할 수 없는 클라이언트 네트워크 옵션에 대한 새로운 * 보안 * 섹션이 포함되어 있습니다.
- 머리글 표시줄의 * 검색 * 필드를 사용하면 그리드 관리자 페이지로 빠르게 이동할 수 있습니다.
- 노드 * 페이지의 요약 테이블은 사용된 개체 데이터 및 사용된 개체 메타데이터와 같은 모든 사이트 및 노드에 대한 상위 수준의 정보를 제공하며 새로운 검색 필드를 포함합니다. 경고 아이콘은 활성 경고가 있는 노드 옆에 표시됩니다.
- 새로운 마법사는 관리 그룹, 관리 사용자, 테넌트, 로드 밸런서 엔드포인트, 고가용성(HA) 그룹에 대한 워크플로우 등 더욱 복잡한 구성을 안내합니다.
- 모든 UI 페이지는 업데이트된 글꼴, 단추 스타일 및 표 형식으로 다시 스타일을 지정했습니다.

> 기능 변경이 없는 한 StorageGRID 11.6 문서 사이트의 스크린샷은 새로운 그리드 관리자 페이지 스타일을 반영하도록 업데이트되지 않았습니다.

다음을 참조하십시오.

- StorageGRID 관리
- 모니터링하고 문제를 해결합니다

여러 **VLAN** 인터페이스

이제 관리 노드 및 게이트웨이 노드에 대한 VLAN(가상 LAN) 인터페이스를 생성할 수 있습니다. HA 그룹 및 로드 밸런서 끝점에서 VLAN 인터페이스를 사용하여 클라이언트 트래픽을 격리하고 파티셔닝하여 보안, 유연성 및 성능을 확보할 수 있습니다.

- 새로운 * VLAN 인터페이스 생성 * 마법사는 VLAN ID를 입력하고 하나 이상의 노드에서 상위 인터페이스를 선택하는 과정을 안내합니다. 상위 인터페이스는 그리드 네트워크, 클라이언트 네트워크 또는 VM 또는 베어 메탈 호스트에 대한 추가 트렁크 인터페이스가 될 수 있습니다. 을 참조하십시오 VLAN 인터페이스를 구성합니다.
- 이제 노드에 추가 트렁크 또는 액세스 인터페이스를 추가할 수 있습니다. 트렁크 인터페이스를 추가하는 경우 VLAN 인터페이스를 구성해야 합니다. 액세스 인터페이스를 추가할 경우 인터페이스를 HA 그룹에 직접 추가할 수 있으며, VLAN 인터페이스를 구성할 필요가 없습니다. 다음을 참조하십시오.
  - * Linux(노드 설치 전) *: 설치 개선 사항
  - * Linux(노드 설치 후) *: Linux: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다
  - * VMware(노드 설치 후) *: 배포 환경에 대한 정보를 수집합니다

Azure AD를 사용하여 **ID** 페더레이션을 수행할 수 있습니다

이제 그리드 관리자 또는 테넌트 관리자에 대한 ID 페더레이션을 구성할 때 Azure Active Directory(Azure AD)를 ID 소스로 선택할 수 있습니다. 을 참조하십시오 ID 페더레이션을 사용합니다.

Azure AD 및 **PingFederate**를 **SSO**에 사용할 수 있습니다

이제 그리드에 대한 SSO(Single Sign-On)를 구성할 때 Azure AD 또는 PingFederate를 SSO 유형으로 선택할 수 있습니다. 그런 다음 sandbox 모드를 사용하여 각 StorageGRID 관리 노드에 대한 Azure AD 엔터프라이즈 애플리케이션 또는 PingFederate 서비스 공급자(SP) 연결을 구성 및 테스트할 수 있습니다. 을 참조하십시오 Single Sign-On 구성.

중앙 집중식 인증서 관리

- 새 인증서 페이지(* 구성 * > * 보안 * > * 인증서 *)는 모든 StorageGRID 보안 인증서에 대한 정보를 단일 위치로 통합합니다. 새 페이지에서 StorageGRID 글로벌, 그리드 CA 및 클라이언트 인증서를 관리하거나 로드 밸런서 엔드포인트, 테넌트 및 ID 통합에 사용되는 인증서 등의 다른 인증서에 대한 정보를 볼 수 있습니다. 을 참조하십시오 보안 인증서 정보.
- 이 변경의 일환으로 다음 글로벌 인증서의 이름이 변경되었습니다.
  - 관리 인터페이스 서버 인증서 * 는 이제 * 관리 인터페이스 인증서 * 입니다.
  - 이제 * 오브젝트 스토리지 API 서비스 엔드포인트 서버 인증서 * (스토리지 API 서버 인증서라고도 함)가 * S3 및 Swift API 인증서 * 입니다.
  - 내부 CA 인증서 *, * 시스템 CA 인증서 *, * CA 인증서 * 및 * 기본 CA 인증서 * 는 이제 항상 * 그리드 CA 인증서 * 라고 합니다.

기타 그리드 관리자 기능 향상

- * 고가용성(HA) 그룹에 대한 업데이트 *. 이제 마법사가 HA 그룹 생성 프로세스를 안내합니다. 을 참조하십시오 고가용성 그룹을 구성합니다.
  - 그리드 네트워크(eth0) 또는 클라이언트 네트워크(eth2)에서 인터페이스를 선택하는 것 외에도 이제 VLAN 인터페이스 또는 노드에 추가한 액세스 인터페이스를 선택할 수 있습니다.
  - 이제 인터페이스의 우선 순위 순서를 지정할 수 있습니다. 기본 인터페이스를 선택하고 각 백업 인터페이스의 순서를 지정할 수 있습니다.
  - S3, Swift, 관리 또는 테넌트 클라이언트가 다른 서브넷의 HA 그룹에 대한 VIP 주소에 액세스할 경우 이제 게이트웨이의 IP 주소를 제공할 수 있습니다.
- * 밸런서 엔드포인트를 로드하기 위한 업데이트 *. 로드 밸런서 끝점을 만드는 과정을 안내하는 새 마법사도 있습니다. 을 참조하십시오 로드 밸런서 엔드포인트를 구성합니다.
  - 이제 엔드포인트를 생성한 후 이 세부 정보를 추가하는 대신 끝점을 처음 생성할 때 클라이언트 유형(S3 또는 Swift)을 선택합니다.
  - 이제 별도의 인증서를 업로드하거나 생성하는 대신 로드 밸런서 끝점에 글로벌 * StorageGRID S3 및 Swift 인증서 * 를 사용할 수 있습니다.

> 이 글로벌 인증서는 이전에 사용되지 않는 CLB 서비스 및 스토리지 노드에 연결하는 데 사용되었습니다. 로드 밸런서 끝점에 글로벌 인증서를 사용하려면 S3 및 Swift API 인증서 페이지에 사용자 지정 인증서를 업로드해야 합니다.

새로운 테넌트 관리자 기능

- * 새로운 실험 S3 콘솔 *. 테넌트 관리자의 Bucket 페이지에서 링크로 사용할 수 있는 새로운 실험 S3 콘솔을 통해 S3 테넌트 사용자는 버킷의 오브젝트를 보고 관리할 수 있습니다. 을 참조하십시오 Experimental S3 Console을 사용합니다.

> 실험적인 S3 콘솔은 완전히 테스트되지 않았으며 대량의 오브젝트 관리 또는 운영 환경에서 사용하기 위한 것이 아닙니다. 테넌트는 소수의 오브젝트 또는 개념 증명 또는 비운영 그리드를 사용하는 경우에만 S3 콘솔을 사용해야 합니다.

- * 여러 S3 버킷을 삭제할 수 있습니다 *. 이제 테넌트 사용자는 한 번에 둘 이상의 S3 버킷을 삭제할 수 있습니다. 삭제할 각 버킷은 비어 있어야 합니다. 을 참조하십시오 S3 버킷을 삭제합니다.
- * 테넌트 계정 권한 업데이트 *. 테넌트 계정 권한이 있는 그룹에 속하는 관리자 사용자는 이제 기존 트래픽 분류 정책을 볼 수 있습니다. 이전에는 이러한 메트릭을 보려면 사용자에게 루트 액세스 권한이 있어야 했습니다.

새로운 업그레이드 및 핫픽스 프로세스

- StorageGRID 업그레이드 * 페이지가 다시 설계되었습니다(* 유지보수 * > * 시스템 * > * 소프트웨어 업데이트 * > * StorageGRID 업그레이드 *).
- StorageGRID 11.6으로의 업그레이드가 완료된 후 그리드 관리자를 사용하여 향후 릴리스로 업그레이드하고 해당 릴리스에 대한 핫픽스를 동시에 적용할 수 있습니다. StorageGRID 업그레이드 페이지에는 권장 업그레이드 경로가 표시되며 올바른 다운로드 페이지로 직접 연결됩니다.
- AutoSupport 페이지의 새 * 소프트웨어 업데이트 확인 * 확인란을 사용하여 이 기능을 제어할 수 있습니다(* 지원 * > * 도구 * > * AutoSupport *). 시스템에 WAN 액세스 권한이 없는 경우 사용 가능한 소프트웨어 업데이트 확인을 비활성화할 수 있습니다. 을 참조하십시오 AutoSupport GT 구성, 소프트웨어 업데이트 확인 비활성화.

> StorageGRID 11.6으로 업그레이드하려면 스크립트를 사용하여 동시에 핫픽스를 업그레이드하고 적용할 수도 있습니다. 을 참조하십시오 "NetApp 기술 자료: StorageGRID에 대한 주요 업그레이드 및 핫픽스 스크립트를 모두 실행하는 방법".

- 이제 나중에 업그레이드를 완료해야 하는 경우 SANtricity OS 업그레이드를 일시 중지하고 일부 노드의 업그레이드를 건너뛸 수 있습니다. 스토리지 어플라이언스에 대한 지침을 참조하십시오.
  - 그리드 관리자(SG5600)를 사용하여 스토리지 컨트롤러의 SANtricity OS 업그레이드
  - 그리드 관리자(SG5700)를 사용하여 스토리지 컨트롤러에서 SANtricity OS 업그레이드
  - SG6000(Grid Manager)를 사용하여 스토리지 컨트롤러에서 SANtricity OS 업그레이드

외부 **syslog** 서버 지원

- 이제 감사 메시지와 StorageGRID 로그의 하위 집합을 원격으로 저장하고 관리하려는 경우 외부 syslog 서버를 구성할 수 있습니다(* 구성 * > * 모니터링 * > * 감사 및 syslog 서버 *). 외부 syslog 서버를 구성한 후 감사 메시지와 특정 로그 파일을 로컬, 원격 또는 둘 다 저장할 수 있습니다. 감사 정보의 대상을 구성하면 관리 노드의 네트워크 트래픽을 줄일 수 있습니다. 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다.
- 이 기능과 관련하여 로그 페이지(* support*>* Tools*>* Logs*)의 새 확인란을 사용하면 특정 응용 프로그램 로그, 감사 로그, 네트워크 디버깅에 사용되는 로그 및 Prometheus 데이터베이스 로그 등 수집할 로그 유형을 지정할 수 있습니다. 을 참조하십시오 로그 파일 및 시스템 데이터를 수집합니다.

S3 를 선택합니다

이제 S3 테넌트가 개별 오브젝트에 SelectObjectContent 요청을 발급하도록 선택적으로 허용할 수 있습니다. S3 Select를 사용하면 데이터베이스와 관련 리소스를 배치하지 않고도 대량의 데이터를 효율적으로 검색할 수 있습니다. 또한, 데이터를 검색하는 데 드는 비용과 대기 시간도 줄어듭니다. 을 참조하십시오 관리 S3 테넌트 계정에 대해 선택 및 S3 Select를 사용합니다.

S3 선택 작업에 대한 Grafana 차트도 추가되었습니다. 을 참조하십시오 지원 메트릭을 검토합니다.

S3 오브젝트 잠금 기본 버킷 보존 기간

S3 오브젝트 잠금을 사용하는 경우 이제 버킷의 기본 보존 기간을 지정할 수 있습니다. 기본 보존 기간은 고유한 보존 설정이 없는 버킷에 추가된 모든 객체에 적용됩니다. 을 참조하십시오 S3 오브젝트 잠금을 사용합니다.

Google Cloud Platform 지원

이제 GCP(Google Cloud Platform)를 클라우드 스토리지 풀 및 CloudMirror 플랫폼 서비스의 엔드포인트로 사용할 수 있습니다. 을 참조하십시오 플랫폼 서비스 끝점의 URN을 지정합니다 및 클라우드 스토리지 풀을 생성합니다.

AWS C2S 지원

이제 CloudMirror 복제에 AWS C2S(Commercial Cloud Services) 엔드포인트를 사용할 수 있습니다. 을 참조하십시오 플랫폼 서비스 끝점을 만듭니다.

기타 **S3** 변경

- * 다중 파트 개체에 대한 객체 및 헤드 객체 지원 *. 이전에는 StorageGRID가 객체 가져오기 또는 헤드 객체 요청에서 'PARTNUMBER' 요청 매개 변수를 지원하지 않았습니다. 이제 가져오기 및 헤드 요청을 발급하여 다중 파트 개체의 특정 부분을 검색할 수 있습니다. Get 및 Head Object 는 또한 X-amz-MP-parts-count 응답 요소를 지원하여 개체에 포함된 파트 수를 나타냅니다.

- * "사용 가능한" 정합성 보장 컨트롤로 변경 *. 이제 "사용 가능한" 정합성 제어는 "새 쓰기 후 읽기" 정합성 보장 수준과 동일하게 작동하지만 헤드 및 GET 작업에 대한 최종 일관성을 제공합니다. "사용 가능한" 일관성 제어는 스토리지 노드를 사용할 수 없는 경우 "새 쓰기 후 읽기"보다 헤드 및 GET 작업에 더 높은 가용성을 제공합니다. 헤드 및 GET 작업에 대한 Amazon S3 정합성 보장과 다릅니다.

  S3을 사용합니다

성능 향상

- * 스토리지 노드는 20억 개의 오브젝트를 지원할 수 있습니다 *. 스토리지 노드의 기본 디렉토리 구조는 확장성 및 성능 향상을 위해 최적화되었습니다. 이제 스토리지 노드는 추가 하위 디렉토리를 사용하여 최대 20억 개의 복제된 객체를 저장하고 성능을 최대화합니다. StorageGRID 11.6으로 업그레이드하면 노드 하위 디렉토리가 수정되지만 기존 객체가 새 디렉토리에 재배포되지 않습니다.
- * 고성능 어플라이언스 * 에서 ILM 기반 삭제 성능이 향상되었습니다. ILM 삭제 작업을 수행하는 데 사용되는 리소스 및 처리량은 이제 각 StorageGRID 어플라이언스 노드의 크기와 기능에 맞게 조정됩니다. SG5600 어플라이언스의 경우 처리량은 StorageGRID 11.5의 처리량과 동일합니다. SG5700 어플라이언스의 경우 ILM 삭제 성능이 소개선되었습니다. RAM이 더 많고 CPU가 더 많은 SG6000 어플라이언스의 경우 ILM이 더 빠르게 처리됩니다. 이러한 성능 향상은 All-Flash SGF6024 어플라이언스에서 특히 두드러집니다.
- * 최적화된 스토리지 볼륨 워터마크 *. 이전 릴리즈에서는 모든 스토리지 노드의 모든 스토리지 볼륨에 세 개의 스토리지 볼륨 워터마크가 적용되었습니다. 이제 StorageGRID는 스토리지 노드의 크기와 볼륨의 상대적 용량을 기준으로 각 스토리지 볼륨에 대해 이러한 워터마크를 최적화할 수 있습니다. 을 참조하십시오 스토리지 볼륨 워터마크란 무엇입니까.

  최적화된 배경무늬는 모든 신규 및 대부분의 업그레이드된 StorageGRID 11.6 시스템에 자동으로 적용됩니다. 최적화된 워터마크는 이전 기본 설정보다 큽니다.

  사용자 지정 워터마크를 사용하는 경우 업그레이드 후 * 읽기 전용 로우 워터마크 무시 * 알림이 트리거될 수 있습니다. 이 알림을 통해 사용자 지정 배경무늬 설정이 너무 작지 여부를 알 수 있습니다. 을 참조하십시오 낮은 읽기 전용 배경무늬 재정의 알림 문제 해결.

  이 변경의 일환으로 두 가지 Prometheus 메트릭이 추가되었습니다.

  - 'toragegrid_storage_volume_minimum_optimized_soft_readonly_watermark'
  - 'toragegrid_storage_volume_maximum_optimized_soft_readonly_watermark'
- * 허용되는 최대 메타데이터 공간이 증가되었습니다 *. 스토리지 노드에 허용되는 최대 메타데이터 공간은 용량이 더 큰 노드의 경우 3.96TB(2.64TB)로 증가했으며, 이는 4TB가 넘는 메타데이터에 대해 실제 예약된 공간이 있는 노드입니다. 이 새로운 값을 통해 더 많은 오브젝트 메타데이터를 특정 스토리지 노드에 저장할 수 있으며 StorageGRID 메타데이터 용량을 최대 50% 늘릴 수 있습니다.

  > 아직 그렇게 하지 않은 경우 스토리지 노드의 RAM이 충분하고 볼륨 0에 충분한 공간이 있으면 이 작업을 수행할 수 있습니다 설치 또는 업그레이드 후 메타데이터 예약 공간 설정을 수동으로 최대 8TB까지 늘립니다.

  - 오브젝트 메타데이터 스토리지 및 GT 관리, 허용되는 메타데이터 공간
  - 메타데이터 예약 공간 증가 설정을 사용합니다

유지 관리 절차 및 지원 도구의 개선 사항

- * 노드 콘솔 암호를 변경할 수 있습니다 **.** 이제 그리드 관리자를 사용하여 노드 콘솔 암호를 변경할 수 있습니다(구성 * > * 액세스 제어 * > * 그리드 암호 *). 이러한 암호는 SSH를 사용하여 노드에 "admin"으로 로그인하거나

VM/물리적 콘솔 연결의 루트 사용자에게 로그인하는 데 사용됩니다. 을 참조하십시오 노드 콘솔 암호를 변경합니다.

- * 새 개체 존재 확인 마법사 **.** 이제 포그라운드 확인 절차를 대체하는 사용하기 쉬운 개체 존재 확인 마법사(maintenance*>* Tasks*>* Object existence check*)를 사용하여 개체 무결성을 확인할 수 있습니다. 새로운 절차를 완료하는 데 걸리는 시간은 1/3로, 동시에 여러 노드를 확인할 수 있습니다. 을 참조하십시오 개체 무결성을 확인합니다.
- * EC 재조정 및 EC 수리 작업에 대한 "예상 완료 시간" 차트 *. 이제 현재 EC 재조정 또는 EC 수리 작업의 예상 완료 시간 및 완료 비율을 볼 수 있습니다.
- * 복제된 데이터 복구에 대한 예상 완료율 *. 이제 'show-replicated-repair-status' 옵션을 'repair-data' 명령에 추가하여 복제된 복구에 대한 예상 완료율을 확인할 수 있습니다.

> StorageGRID 11.6의 기술 미리 보기에는 '복제된-수리-상태' 옵션이 제공됩니다. 이 기능은 개발 중이며 반환된 값이 잘못되었거나 지연될 수 있습니다. 수리가 완료되었는지 확인하려면 복구 절차에 설명된 대로 * Awaiting-all *, * repair attemptated(XRPA *) 및 * Scan Period - Estimated(XSCM) * 를 계속 사용합니다.

- 이제 진단 페이지(* 지원 * > * 도구 * > * 진단 *)의 결과가 심각도별로 정렬된 다음 알파벳순으로 정렬됩니다.
- Prometheus 및 Grafana가 수정된 인터페이스 및 차트를 사용하여 최신 버전으로 업데이트되었습니다. 이 변경의 일환으로 일부 메트릭의 레이블이 변경되었습니다.
  - node_network_up의 레이블을 사용한 사용자 지정 쿼리가 있는 경우 대신 node_network_info의 레이블을 사용해야 합니다.
  - NODE_NETWORK 메트릭의 레이블 이름 "interface"를 사용했다면 대신 DEVICE 레이블을 사용해야 합니다.
- 이전에는 Prometheus 메트릭이 31일 동안 관리 노드에 저장되었습니다. 이제 Prometheus 데이터에 예약된 공간이 가득 찰 때까지 메트릭이 저장되므로 기간별 메트릭을 사용할 수 있는 시간이 크게 증가할 수 있습니다.

  '/var/local/mysql_ibdata/' 볼륨이 용량에 도달하면 가장 오래된 메트릭이 먼저 삭제됩니다.

설치 개선 사항

- 이제 Red Hat Enterprise Linux를 설치하는 동안 Podman을 컨테이너로 사용할 수 있습니다. 이전에는 StorageGRID에서 Docker 컨테이너만 지원했습니다.
- StorageGRID용 API 스키마는 이제 RedHat Enterprise Linux/CentOS, Ubuntu/Debian 및 VMware 플랫폼의 설치 아카이브에 포함됩니다. 아카이브를 추출한 후 '/Extras/API-schemas' 폴더에서 스키마를 찾을 수 있습니다.
- 이제 베어 메탈 배포를 위한 노드 구성 파일의 'BLOCK_DEVICE_RANGEDB' 키는 2자리 숫자가 아니라 3자리 숫자가 되어야 합니다. 즉, block_device_RANGEDB_nn 대신 block_device_RANGEDB_nnn을 지정해야 합니다.

  기존 배포와의 호환성을 위해 업그레이드된 노드에는 2자리 키가 계속 지원됩니다.

- 베어 메탈 배포를 위해 새 'interfaces_target_nnnn' 키의 인스턴스를 노드 구성 파일에 선택적으로 추가할 수 있습니다. 각 키는 베어 메탈 호스트의 물리적 인터페이스에 대한 이름과 설명을 제공하며, 이 이름은 VLAN 인터페이스 페이지와 HA 그룹 페이지에 표시됩니다.
  - Red Hat Enterprise Linux 또는 CentOS 배포용 노드 구성 파일을 생성합니다
  - Ubuntu 또는 Debian 배포용 노드 구성 파일을 만듭니다

새 경고

StorageGRID 11.6에 대해 다음과 같은 새 경고가 추가되었습니다.

- 감사 로그가 인메모리 대기열에 추가되고 있습니다
- Cassandra 테이블 손상
- EC 재조정 실패
- EC 복구 실패
- EC 복구가 중단되었습니다
- S3 및 Swift API에 대한 글로벌 서버 인증서 만료
- 외부 syslog CA 인증서 만료
- 외부 syslog 클라이언트 인증서 만료
- 외부 syslog 서버 인증서 만료
- 외부 syslog 서버 전달 오류입니다
- 테넌트의 ID 페더레이션 동기화 실패
- 레거시 CLB 로드 밸런서 활동이 감지되었습니다
- 로그가 디스크 대기열에 추가되고 있습니다
- 읽기 전용 로우 워터마크가 무시됩니다
- tmp 디렉토리 여유 공간이 부족합니다
- 개체 존재 여부를 확인하지 못했습니다
- 개체 존재 검사가 중단되었습니다
- S3 PUT 오브젝트 크기가 너무 큽니다

를 참조하십시오 경고 참조.

감사 메시지의 변경

- ORLM: 개체 규칙이 감사 메시지를 충족했습니다. 새 * BUID * 필드가 ORLM: 개체 규칙에 추가되었습니다. BUID * 필드에는 내부 작업에 사용되는 버킷 ID가 표시됩니다. 새 필드는 메시지 상태가 PRGD인 경우에만 나타납니다.
- 새 * SGRP * 필드가 다음 감사 메시지에 추가되었습니다. SGRP * 필드는 인제스트된 위치와 다른 사이트에서 객체가 삭제된 경우에만 표시됩니다.
  - IDEL: ILM 삭제 시작
  - OVWR: 개체 덮어쓰기
  - SDEL: S3 삭제
  - WDEL: Swift 삭제

을 참조하십시오 감사 로그를 검토합니다.

StorageGRID 설명서 변경 사항

StorageGRID 11.6 설명서 사이트의 모양과 느낌이 수정되었으며 이제 GitHub를 기본 플랫폼으로 사용합니다.

NetApp은 콘텐츠에 대한 피드백을 감사하며 제품 문서의 모든 페이지에서 제공되는 새로운 "문서 변경 요청" 기능을 이용하도록 권장합니다. 또한 문서 플랫폼은 GitHub 사용자를 위한 임베디드 콘텐츠 기여 기능을 제공합니다.

이 문서를 살펴보고 이 문서에 기고하십시오. 편집, 변경 요청 또는 피드백 전송만 가능합니다.

제거되거나 사용되지 않는 기능

일부 기능은 이 릴리즈에서 제거되었거나 더 이상 사용되지 않습니다. 업그레이드 전에 클라이언트 응용 프로그램을 업데이트하거나 구성을 수정해야 하는지 여부를 이해하려면 이 항목을 검토하십시오.

알람 시스템 및 알람 기반 **API**는 더 이상 사용되지 않습니다

StorageGRID 11.6 릴리스 현재 레거시 알람 시스템은 더 이상 사용되지 않습니다. 레거시 알람 시스템의 사용자 인터페이스 및 API는 향후 릴리즈에서 제거될 예정입니다.

> 기존 경보를 계속 사용하는 경우 StorageGRID 11.6으로 업그레이드한 후 알림 시스템으로 완전히 전환하십시오. 을 참조하십시오 경보 및 경보 관리: 개요 알림에 대해 자세히 알아보십시오.

11.6 릴리스는 모든 알람 기반 API를 중단합니다. 다음 API는 이러한 변경의 영향을 받습니다.

- Get/Grid/alarms: fully deprecated
- 'Get/Grid/Health/Topology': 완전히 사용되지 않습니다
- Get/Grid/Health: 응답의 alarm-counts 섹션은 더 이상 사용되지 않습니다

향후 릴리즈에서는 **Put Object**에 대해 **5TiB**의 최대 개체 크기를 지원하지 않습니다

향후 StorageGRID 릴리즈에서는 단일 PUT 오브젝트 작업의 최대 크기가 5TiB가 아닌 5GiB가 됩니다. 5GiB보다 큰 개체에 대해 최대 5TiB(5,497,558,138,880바이트)까지 멀티파트 업로드를 사용할 수 있습니다.

클라이언트가 Put Object에서 더 작은 오브젝트 크기를 사용하도록 전환할 수 있도록 S3 클라이언트가 5GiB를 초과하는 개체를 업로드하려고 하면 StorageGRID 11.6에서 * S3 Put Object size Too Large * 경고가 트리거됩니다.

NAS Bridge 기능은 더 이상 사용되지 않습니다

NAS 브리지 기능은 이전에 StorageGRID 11.4 릴리즈에서 제한된 액세스를 입력했습니다. NAS 브리지 기능은 제한된 액세스로 유지되며 StorageGRID 11.6부터 더 이상 사용되지 않습니다.

NAS 브리지 11.4는 최종 릴리즈이며 StorageGRID 11.6과 계속 호환됩니다. 를 검토합니다 "NetApp 상호 운용성 매트릭스 툴" NAS Bridge 11.4와 StorageGRID 버전 간의 지속적인 호환성

에 대한 NetApp Support 사이트를 검토합니다 "NAS 브리지에 대한 지원 스케줄입니다".

Grid Management API 변경

StorageGRID 11.6은 그리드 관리 API 버전 3을 사용합니다. 버전 3은 버전 2를 사용하지 않지만 버전 1과 버전 2는 계속 지원됩니다.

> StorageGRID 11.6에서 관리 API 버전 1 및 버전 2를 계속 사용할 수 있지만, 이러한 API 버전에 대한 지원은 StorageGRID의 향후 릴리스에서 제거됩니다. StorageGRID 11.6으로 업그레이드한 후, 'Put/grid/config/management' API를 사용하여 더 이상 사용되지 않는 v1 및 v2 API를 비활성화할 수 있다.

자세한 내용은 를 참조하십시오 Grid Management API를 사용합니다.

전용 API 작업을 위해 Swagger 문서에 액세스할 수 있습니다

이제 Grid Manager에서 전용 API에 대한 Swagger 문서에 액세스할 수 있습니다. 사용 가능한 작업을 보려면 Grid Manager 도움말 아이콘을 선택하고 * API Documentation * 을 선택합니다. 그런 다음 StorageGRID 관리 API 페이지에서 * 전용 API 설명서 * 로 이동 * 을 선택합니다.

StorageGRID 프라이빗 API는 사전 통지 없이 변경될 수 있습니다. StorageGRID 전용 엔드포인트도 요청의 API 버전을 무시합니다.

알람 기반 API는 더 이상 사용되지 않습니다

11.6 릴리스는 모든 알람 기반 API를 중단합니다. 다음 API는 이러한 변경의 영향을 받습니다.

- Get/Grid/alarms: fully deprecated
- 'Get/Grid/Health/Topology': 완전히 사용되지 않습니다
- Get/Grid/Health: 응답의 alarm-counts 섹션은 더 이상 사용되지 않습니다

S3 액세스 키를 가져올 수 있습니다

이제 그리드 관리 API를 사용하여 테넌트 사용자용 S3 액세스 키를 가져올 수 있습니다. 예를 들어, 다른 S3 공급자의 액세스 키를 StorageGRID로 마이그레이션하거나 이 기능을 사용하여 그리드 간에 사용자 자격 증명을 동일하게 유지할 수 있습니다.

> 이 기능을 활성화하면 테넌트 루트 암호 변경 권한이 있는 Grid Manager 사용자는 테넌트 데이터에 대한 모든 액세스 권한을 갖습니다. 테넌트 데이터를 보호하기 위해 사용 후 즉시 이 기능을 비활성화합니다.

신규 고객 운영

세 가지 새로운 '그리드/계정' API 작업이 추가되었습니다.

- 'POST/gridentsport/account-enable-s3-key-import': 이 요청은 S3 자격 증명 가져오기 기능을 활성화합니다. 이 기능을 사용하려면 루트 액세스 권한이 있어야 합니다.
- 'POST/gridi./accountsstsstimer/{id}si./{user_id}sihifacer/s3-access-keys': 이 요청은 테넌트 계정에서 지정된 사용자에 대한 S3 자격 증명을 가져옵니다. 루트 액세스 또는 테넌트 루트 암호 변경 권한이 있어야 하며 사용자 ID와 테넌트 계정 ID를 알고 있어야 합니다.
- 'POST/gridentsport/account-disable-s3-key-import': 이 요청은 S3 자격 증명 가져오기 기능을 비활성화합니다.

이 기능을 해제하려면 루트 액세스 권한이 있어야 합니다.

패치 메소드는 사용되지 않습니다

이제 패치 방법이 더 이상 사용되지 않으며 향후 릴리스에서 제거될 것입니다. 필요한 경우 패치 작업을 사용하여 리소스를 수정하는 대신 PUT 작업을 수행하여 리소스를 교체합니다.

에 추가 `grid/logs/collect` 엔드포인트

'grid/logs/collect' 끝점에 4개의 boolean 값이 추가되었습니다.

- "applicationLogs": 기술 지원 부서에서 문제 해결을 위해 가장 자주 사용하는 응용 프로그램별 로그입니다. 수집된 로그는 사용 가능한 애플리케이션 로그의 하위 집합입니다. 기본값은 true입니다.
- auditLogs: 정상적인 시스템 작동 중에 생성된 감사 메시지가 포함된 로그입니다. 기본값은 true입니다.
- 네트워크 추적: 네트워크 디버깅에 사용되는 로그입니다. 기본값은 false 입니다.
- 'prometheusDatabase': 모든 노드의 서비스에서 시계열 지표. 기본값은 false 입니다.

신규 `node-details /grid/service-ids` 엔드포인트

새로운 's./gridi./service-ids' 엔드포인트는 노드 UUID를 연관된 노드 이름, 서비스 ID 및 서비스 유형에 매핑하는 기능을 제공합니다.

그리드 노드 콘솔 암호를 검색할 수 있습니다

이제 'POST'(POST) 인수와 모눈인/노드-콘솔-비밀번호'를 사용하여 그리드 노드 및 관련 콘솔 비밀번호 목록을 검색할 수 있습니다.

테넌트 관리 **API**의 변경 사항

StorageGRID 11.6은 테넌트 관리 API 버전 3을 사용합니다. 버전 3은 버전 2를 사용하지 않지만 버전 1과 버전 2는 계속 지원됩니다.

> StorageGRID 11.6에서 관리 API 버전 1 및 버전 2를 계속 사용할 수 있지만, 이러한 API 버전에 대한 지원은 StorageGRID의 향후 릴리스에서 제거됩니다. StorageGRID 11.6으로 업그레이드한 후, 'Put/grid/config/management' API를 사용하여 더 이상 사용되지 않는 v1 및 v2 API를 비활성화할 수 있다.

자세한 내용은 를 참조하십시오 테넌트 관리 API 이해.

패치 메소드는 사용되지 않습니다

이제 패치 방법이 더 이상 사용되지 않으며 향후 릴리스에서 제거될 것입니다. 필요한 경우 패치 작업을 사용하여 리소스를 수정하는 대신 PUT 작업을 수행하여 리소스를 교체합니다.

업그레이드를 계획하고 준비합니다

업그레이드를 완료하는 데 걸리는 시간을 예상합니다

StorageGRID 11.6으로의 업그레이드를 계획할 때는 업그레이드 기간을 기준으로 업그레이드 시기를 고려해야 합니다. 또한 업그레이드의 각 단계에서 수행할 수 있는 작업과 수행할 수 없는 작업을 알고 있어야 합니다.

이 작업에 대해

StorageGRID 업그레이드를 완료하는 데 필요한 시간은 클라이언트 로드 및 하드웨어 성능과 같은 다양한 요인에 따라 달라집니다.

이 표에는 주요 업그레이드 작업이 요약되어 있으며 각 작업에 필요한 대략적인 시간이 나와 있습니다. 표 다음에 나오는 단계에서는 시스템의 업그레이드 시간을 추정하는 데 사용할 수 있는 지침을 제공합니다.

업그레이드 작업	설명	필요한 대략적인 시간입니다	수행해야 합니다
업그레이드 서비스를 시작합니다	업그레이드 사전 점검을 실행하고 소프트웨어 파일을 배포하며 업그레이드 서비스를 시작합니다.	유효성 검사 오류가 보고되지 않은 경우 그리드 노드당 3분	필요한 경우 예약된 업그레이드 유지 관리 기간 전에 수동으로 업그레이드 사전 점검을 실행할 수 있습니다.
업그레이드 그리드 노드 (기본 관리 노드)	운영 관리자 노드가 중지, 업그레이드 및 재시작됩니다.	SG100 및 SG1000 어플라이언스 노드에서 최대 시간이 필요하므로 30분에서 1시간까지 걸립니다.	기본 관리자 노드에 액세스할 수 없습니다. 연결 오류가 보고되며 무시할 수 있습니다.
업그레이드 그리드 노드 (다른 모든 노드)	다른 모든 그리드 노드의 소프트웨어는 노드를 승인하는 순서대로 업그레이드됩니다. 시스템의 모든 노드는 한 번에 하나씩 몇 분 동안 다운됩니다.	노드당 15분~1시간, 어플라이언스 노드에서 가장 많은 시간이 필요함 • 참고: * 어플라이언스 노드의 경우 StorageGRID 어플라이언스 설치 프로그램이 자동으로 최신 릴리즈로 업데이트됩니다.	• 그리드 구성을 변경하지 마십시오. • 감사 수준 구성을 변경하지 마십시오. • ILM 구성을 업데이트하지 마십시오. • 핫픽스, 서비스 해제 또는 확장과 같은 다른 유지 관리 절차를 수행할 수 없습니다. • 참고: * 복구를 수행해야 하는 경우 기술 지원 부서에 문의하십시오.

업그레이드 작업	설명	필요한 대략적인 시간입니다	수행해야 합니다
기능 사용	새 버전의 새 기능이 활성화됩니다.	5분 미만	• 그리드 구성을 변경하지 마십시오. • 감사 수준 구성을 변경하지 마십시오. • ILM 구성을 업데이트하지 마십시오. • 다른 유지보수 절차는 수행할 수 없습니다.
데이터베이스 업그레이드	업그레이드 프로세스에서는 각 노드를 검사하여 Cassandra 데이터베이스를 업데이트할 필요가 없는지 확인합니다.	노드당 10초 또는 전체 그리드에 대해 몇 분	StorageGRID 11.5에서 11.6으로의 업그레이드는 Cassandra 데이터베이스 업그레이드가 필요하지 않지만 Cassandra 서비스는 각 스토리지 노드에서 중지되었다가 다시 시작됩니다. 향후 StorageGRID 기능 릴리즈를 위해 Cassandra 데이터베이스 업데이트 단계를 완료하는 데 며칠이 걸릴 수 있습니다.
최종 업그레이드 단계	임시 파일이 제거되고 새 릴리스로의 업그레이드가 완료됩니다.	5분	최종 업그레이드 단계 * 작업이 완료되면 모든 유지보수 절차를 수행할 수 있습니다.

단계

1. 모든 그리드 노드를 업그레이드하는 데 필요한 시간을 예상합니다.
   a. StorageGRID 시스템의 노드 수에 노드당 1시간을 곱합니다.

      일반적으로 어플라이언스 노드는 소프트웨어 기반 노드보다 업그레이드하는 데 더 오래 걸립니다.

   b. 이 시간에 1시간을 더하여 '.upgrade' 파일을 다운로드하고, 사전 확인 검증을 실행하고, 최종 업그레이드 단계를 완료하는 데 필요한 시간을 고려하십시오.
2. Linux 노드가 있는 경우 RPM 또는 DEB 패키지를 다운로드하고 설치하는 데 필요한 시간을 고려하여 각 노드에 대해 15분을 추가하십시오.
3. 1단계와 2단계의 결과를 추가하여 총 업그레이드 예상 시간을 계산합니다.

예**: StorageGRID 11.6**으로 업그레이드할 예상 시간

시스템에 14개의 그리드 노드가 있고 그 중 8개가 Linux 노드라고 가정합니다.

1. 14에 노드당 1시간을 곱합니다.

2. 다운로드, 사전 확인 및 최종 단계를 고려하여 1시간을 추가하십시오.

   모든 노드의 업그레이드 예상 시간은 15시간입니다.

3. Linux 노드에 RPM 또는 DEB 패키지를 설치하는 시간을 고려하려면 노드당 8에 15분을 곱하십시오.

   이 단계의 예상 시간은 2시간입니다.

4. 값을 함께 추가합니다.

   StorageGRID 11.6.0으로 시스템 업그레이드를 완료하는 데 최대 17시간이 소요됩니다.

업그레이드 중 시스템에 미치는 영향

업그레이드 중에 StorageGRID 시스템이 어떻게 영향을 받는지 알아야 합니다.

StorageGRID 업그레이드는 무중단으로 수행할 수 있습니다

StorageGRID 시스템은 업그레이드 프로세스 전반에서 클라이언트 애플리케이션의 데이터를 수집하고 검색할 수 있습니다. 그리드 노드는 업그레이드 중에 한 번에 하나씩 다운되므로 모든 그리드 노드를 사용할 수 없는 시간은 없습니다.

지속적인 가용성을 보장하려면 적절한 ILM 정책을 사용하여 개체가 중복적으로 저장되도록 해야 합니다. 또한 모든 외부 S3 또는 Swift 클라이언트가 다음 중 하나로 요청을 보내도록 구성되어 있는지 확인해야 합니다.

- 고가용성(HA) 그룹으로 구성된 StorageGRID 끝점
- 고가용성 타사 로드 밸런서
- 각 클라이언트에 대해 여러 게이트웨이 노드가 있습니다
- 각 클라이언트에 대해 여러 스토리지 노드

어플라이언스 펌웨어가 업그레이드되었습니다

StorageGRID 11.6 업그레이드 중:

- 모든 StorageGRID 어플라이언스 노드는 StorageGRID 어플라이언스 설치 관리자 펌웨어 버전 3.6으로 자동으로 업그레이드됩니다.
- SG6060 및 SGF6024 어플라이언스는 BIOS 펌웨어 버전 3B07.EX 및 BMC 펌웨어 버전 BMC 3.93.07로 자동 업그레이드됩니다.
- SG100 및 SG1000 어플라이언스는 BIOS 펌웨어 버전 3B12.EC 및 BMC 펌웨어 버전 4.67.07로 자동 업그레이드됩니다.

알림이 트리거될 수 있습니다

서비스가 시작 및 중지되거나 StorageGRID 시스템이 혼합 버전 환경으로 작동 중일 때(이전 버전을 실행하는 일부 그리드 노드와 이후 버전으로 업그레이드된 경우) 경고가 트리거될 수 있습니다. 업그레이드가 완료된 후 다른 알림이 트리거될 수 있습니다.

예를 들어, 서비스가 중지되었을 때 * 노드 * 와 통신할 수 없음 경고가 표시되거나 일부 노드가 StorageGRID 11.6으로 업그레이드되었지만 다른 노드가 여전히 StorageGRID 11.5를 실행 중일 때 * Cassandra 통신 오류 * 경고가 표시될

수 있습니다. 일반적으로 이러한 알림은 업그레이드가 완료되면 지워집니다.

StorageGRID 11.6으로 업그레이드하는 동안 스토리지 노드가 중지되면 * ILM 배치를 달성 불가능으로 * 경고가 트리거될 수 있습니다. 이 알림은 업그레이드가 완료된 후 1일 동안 지속될 수 있습니다.

스토리지 볼륨 워터마크에 사용자 지정 값을 사용하는 경우 업그레이드가 완료된 후 * 읽기 전용 로우 워터마크 재정의 * 알림이 트리거될 수 있습니다. 을 참조하십시오 낮은 읽기 전용 배경무늬 재정의 알림 문제 해결 를 참조하십시오.

업그레이드가 완료된 후 Grid Manager 대시보드에서 * Recently Resolved alerts * 또는 * Current alerts * 를 선택하여 업그레이드 관련 경고를 검토할 수 있습니다.

많은 **SNMP** 알림이 생성됩니다

업그레이드 중에 그리드 노드를 중지하고 다시 시작할 때 많은 수의 SNMP 알림이 생성될 수 있습니다. 과도한 알림을 방지하려면 업그레이드를 시작하기 전에 SNMP 알림을 비활성화하려면 * SNMP 에이전트 알림 사용 * 확인란(* 구성 * > * 모니터링 * > * SNMP 에이전트 *)을 선택 취소합니다. 그런 다음 업그레이드가 완료된 후 알림을 다시 활성화합니다.

구성 변경이 제한됩니다

> 제한된 구성 변경 목록은 릴리즈에서 릴리즈로 변경될 수 있습니다. 다른 StorageGRID 릴리즈로 업그레이드할 때는 해당 업그레이드 지침의 목록을 참조하십시오.

새 기능 사용 * 작업이 완료될 때까지 다음을 수행합니다.

- 그리드 구성을 변경하지 마십시오.
- 감사 수준 구성을 변경하거나 외부 syslog 서버를 구성하지 마십시오.
- 새 기능을 사용하거나 사용하지 않도록 설정하지 마십시오.
- ILM 구성을 업데이트하지 마십시오. 그렇지 않으면 일관되지 않고 예기치 않은 ILM 동작이 발생할 수 있습니다.
- 핫픽스를 적용하거나 그리드 노드를 복구하지 마십시오.
- StorageGRID 11.6으로 업그레이드하는 동안에는 HA 그룹, VLAN 인터페이스 또는 로드 밸런서 엔드포인트를 관리할 수 없습니다.

최종 업그레이드 단계 * 작업이 완료될 때까지:

- 확장 절차를 수행하지 마십시오.
- 서비스 해제 절차를 수행하지 마십시오.

테넌트 관리자에서는 버킷 세부 정보를 보거나 버킷을 관리할 수 없습니다

StorageGRID 11.6으로 업그레이드하는 동안(즉, 시스템이 혼합 버전 환경으로 작동하는 동안), 버킷 세부 정보를 보거나 테넌트 관리자를 사용하여 버킷을 관리할 수 없습니다. Tenant Manager의 Bucket 페이지에 다음 오류 중 하나가 나타납니다.

- "11.6으로 업그레이드하는 동안에는 이 API를 사용할 수 없습니다."
- 11.6으로 업그레이드하는 동안에는 테넌트 관리자에서 버킷 버전 정보를 볼 수 없습니다."

11.6으로의 업그레이드가 완료된 후 이 오류가 해결됩니다.

해결 방법

11.6 업그레이드가 진행 중인 동안 테넌트 관리자를 사용하는 대신 다음 툴을 사용하여 버킷 세부 정보를 보거나 버킷을 관리합니다.

- 버킷에서 표준 S3 작업을 수행하려면 S3 REST API 또는 테넌트 관리 API를 사용합니다.
- 버킷에 대한 StorageGRID 사용자 지정 작업(예: 버킷 정합성 보장 수준 보기 및 수정, 마지막 액세스 시간 업데이트 활성화 또는 비활성화, 검색 통합 구성)을 수행하려면 테넌트 관리 API를 사용합니다.

을 참조하십시오 테넌트 관리 API 이해 및 S3을 사용합니다 를 참조하십시오.

그룹 및 사용자 계정에 대한 업그레이드의 영향

업그레이드가 완료된 후 그룹 및 사용자 계정을 적절하게 업데이트할 수 있도록 StorageGRID 업그레이드의 영향을 이해해야 합니다.

그룹 권한 및 옵션에 대한 변경

StorageGRID 11.6으로 업그레이드한 후 필요에 따라 다음과 같은 업데이트된 권한 또는 새 권한 및 옵션을 선택합니다(* 구성 * > * 액세스 제어 * > * 관리 그룹 *).

권한 또는 옵션	설명
테넌트 계정	사용자가 테넌트 계정을 생성, 편집 및 제거할 수 있도록 허용하는 것 외에도, 이 권한을 통해 관리자는 기존 트래픽 분류 정책(* 구성 * > * 네트워크 * > * 트래픽 분류 *)을 볼 수 있습니다.

을 참조하십시오 관리 그룹을 관리합니다.

설치된 **StorageGRID** 버전을 확인합니다

업그레이드를 시작하기 전에 사용 가능한 최신 핫픽스가 적용된 이전 버전의 StorageGRID가 현재 설치되어 있는지 확인해야 합니다.

이 작업에 대해

StorageGRID 11.6으로 업그레이드하기 전에 그리드에 StorageGRID 11.5가 설치되어 있어야 합니다. 현재 이전 버전의 StorageGRID를 사용 중인 경우 그리드의 현재 버전이 StorageGRID 11.5._x.y_가 될 때까지 최신 핫픽스(적극 권장)와 함께 이전 업그레이드 파일을 모두 설치해야 합니다.

가능한 업그레이드 경로 하나가 에 표시됩니다 예.

> 다음 버전으로 업그레이드하기 전에 각 StorageGRID 버전에 최신 핫픽스를 적용하고 설치하는 각 새 버전에 최신 핫픽스를 적용할 것을 적극 권장합니다. 경우에 따라 데이터 손실 위험을 방지하기 위해 핫픽스를 적용해야 합니다. 을 참조하십시오 "NetApp 다운로드: StorageGRID" 각 핫픽스에 대한 릴리스 노트를 참조하십시오.

한 단계에서 11.3.0.13+에서 11.4.0._y_로, 11.4.0.7+에서 11.5.0._y_로 업데이트하는 스크립트를 실행할 수 있습니다. 을 참조하십시오 "NetApp 기술 자료: StorageGRID에 대한 주요 업그레이드 및 핫픽스 스크립트를 모두 실행하는 방법".

단계

1. 를 사용하여 Grid Manager에 로그인합니다 지원되는 웹 브라우저.
2. 그리드 관리자 상단에서 * 도움말 * > * 정보 * 를 선택합니다.
3. 버전 * 이 11.5._x.y_인지 확인합니다.

   StorageGRID 11.5._x. y_version 번호:

   - 주요 릴리스 * 의 _x_값은 0(11.5.0)입니다.
   - 핫픽스 * 가 적용된 경우 _y_값(예: 11.5.0.1)이 있습니다.
4. 버전 * 이 11.5._x.y_가 아니면 로 이동합니다 "NetApp 다운로드: StorageGRID" 각 릴리스에 대한 최신 핫픽스를 포함하여 이전 릴리스마다 파일을 다운로드합니다.
5. 다운로드한 각 릴리스에 대한 업그레이드 지침을 확인합니다. 그런 다음 해당 릴리스에 대해 소프트웨어 업그레이드 절차를 수행하고 해당 릴리스에 대한 최신 핫픽스를 적용합니다(적극 권장).

   를 참조하십시오 StorageGRID 핫픽스 절차.

예: 버전 **11.3.0.8**에서 **StorageGRID 11.5**로 업그레이드합니다

다음 예에서는 StorageGRID 11.6 업그레이드를 준비하는 StorageGRID 버전 11.3.0.8에서 버전 11.5로 업그레이드하는 단계를 보여 줍니다.

> 선택적으로 스크립트를 실행하여 2단계와 3단계를 결합하고(11.3.0.13+에서 11.4.0.*y*) 4단계와 5단계를 결합할 수 있습니다(11.4.0.7+에서 11.5.0.*y*). 을 참조하십시오 "NetApp 기술 자료: StorageGRID에 대한 주요 업그레이드 및 핫픽스 스크립트를 모두 실행하는 방법".

시스템을 업그레이드할 수 있도록 다음 순서로 소프트웨어를 다운로드하여 설치합니다.

1. 최신 StorageGRID 11.3.0._y_HotFix를 적용합니다.
2. StorageGRID 11.4.0 주요 릴리즈로 업그레이드하십시오.
3. 최신 StorageGRID 11.4.0._y_HotFix를 적용합니다.
4. StorageGRID 11.5.0 주요 릴리즈로 업그레이드하십시오.
5. 최신 StorageGRID 11.5.0._y_HotFix를 적용합니다.

소프트웨어 업그레이드에 필요한 자료를 확보합니다

소프트웨어 업그레이드를 시작하기 전에 업그레이드를 성공적으로 완료할 수 있도록 필요한 모든 자료를 확보해야 합니다.

항목	참고
StorageGRID 업그레이드 파일	StorageGRID 업그레이드 파일을 다운로드합니다 서비스 랩톱으로 이동합니다.

항목	참고
서비스 노트북	서비스 랩톱의 구성 요소: • 네트워크 포트 • SSH 클라이언트(예: PuTTY)
지원되는 웹 브라우저	브라우저 지원은 일반적으로 각 StorageGRID 릴리스에 대한 변경 사항을 적용합니다. 브라우저가 새 StorageGRID 버전과 호환되는지 확인합니다.
복구 패키지(".zip") 파일	복구 패키지를 다운로드합니다 업그레이드하기 전에 파일을 안전한 위치에 저장하십시오. 복구 패키지 파일을 사용하면 오류가 발생할 경우 시스템을 복원할 수 있습니다.
"passwords.txt" 파일	이 파일은 복구 패키지 .zip 파일의 일부인 해당 패키지에 포함되어 있습니다. 최신 버전의 복구 패키지를 구해야 합니다.
프로비저닝 암호	StorageGRID 시스템을 처음 설치할 때 암호가 생성되고 문서화됩니다. 프로비저닝 암호는 passwords.txt 파일에 나열되지 않습니다.

관련 문서	• 릴리스 정보 StorageGRID 11.6용. 업그레이드를 시작하기 전에 이 내용을 주의 깊게 읽으십시오.
	• 에 대한 지침 StorageGRID 관리.
	• Linux 배포를 업그레이드하는 경우 Linux 플랫폼에 대한 StorageGRID 설치 지침:
	  ◦ Red Hat Enterprise Linux 또는 CentOS를 설치합니다
	  ◦ Ubuntu 또는 Debian을 설치합니다
	• 기타 StorageGRID 문서(필요 시)

StorageGRID 업그레이드 파일을 다운로드합니다

노드가 설치된 위치에 따라 하나 이상의 파일을 다운로드해야 합니다.

- 모든 플랫폼 *: '.upgrade' 파일

Linux 호스트에 노드가 배포된 경우 업그레이드를 시작하기 전에 설치할 RPM 또는 DEB 아카이브도 다운로드해야 합니다.

- * Red Hat Enterprise Linux 또는 CentOS *: 추가 RPM 파일(".zip" 또는".tgz")
- * Ubuntu 또는 Debian *: 추가 DEB 파일(".zip" 또는".tgz")

단계

1. 로 이동합니다 "NetApp 다운로드: StorageGRID".
2. 최신 릴리스를 다운로드하려면 버튼을 선택하거나 드롭다운 메뉴에서 다른 버전을 선택하고 * GO * 를 선택합니다.

   StorageGRID 소프트웨어 버전의 형식은 11._x. y _ 입니다. StorageGRID 핫픽스의 형식은 11._x.x.x.z _ 입니다.

3. NetApp 계정의 사용자 이름과 암호를 사용하여 로그인합니다.
4. Caution/MustRead 문이 나타나면 해당 문을 읽고 확인란을 선택합니다.

   이 설명은 릴리스에 필요한 핫픽스가 있는 경우에 나타납니다.

5. 최종 사용자 사용권 계약을 읽고 확인란을 선택한 다음 * 동의 및 계속 * 을 선택합니다.

   선택한 버전의 다운로드 페이지가 나타납니다. 이 페이지에는 세 개의 열이 있습니다.

   - StorageGRID를 설치합니다
   - StorageGRID를 업그레이드합니다
   - StorageGRID 어플라이언스에 대한 지원 파일
6. Upgrade StorageGRID * 열에서 '.upgrade' 아카이브를 선택하여 다운로드합니다.

   모든 플랫폼에는 '.upgrade' 아카이브가 필요합니다.

7. Linux 호스트에 노드가 배포된 경우 RPM 또는 DEB 아카이브도 '.tgz' 또는 '.zip' 형식으로 다운로드합니다. 서비스 랩톱에서 Windows를 실행 중인 경우 '.zip' 파일을 선택합니다.

   - Red Hat Enterprise Linux 또는 CentOS +'s torageGRID-Webscale-*version*-RPM-*UniqueID*.zip" +'torageGRID-Webscale-*version*-RPM-*UniqueID*.tgz'
   - Ubuntu 또는 Debian+'torageGRID-Webscale-*version*-deb-*UniqueID*.zip"+'torageGRID-Webscale-*version*-deb-*UniqueID*.tgz"

   SG100 또는 SG1000에는 추가 파일이 필요하지 않습니다.

복구 패키지를 다운로드합니다

복구 패키지 파일을 사용하면 오류가 발생할 경우 StorageGRID 시스템을 복원할 수 있습니다. 그리드 토폴로지를 StorageGRID 시스템으로 변경하거나 소프트웨어를 업그레이드하기 전에 현재 복구 패키지 파일을 다운로드합니다. 그런 다음 그리드 토폴로지를 변경한 후 또는 소프트웨어를 업그레이드한 후 복구 패키지의 새 복사본을 다운로드합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 프로비저닝 암호가 있어야 합니다.
- 특정 액세스 권한이 있어야 합니다.

단계

1. 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
2. 프로비저닝 암호를 입력하고 * 다운로드 시작 * 을 선택합니다.

   다운로드가 즉시 시작됩니다.

3. 다운로드가 완료되면 다음을 수행합니다.

   a. '.zip' 파일을 엽니다.

b. GPT-backup 디렉토리와 내부 .zip 파일이 포함되어 있는지 확인합니다.

c. 안쪽 '.zip' 파일의 압축을 풉니다.

d. 비밀번호.txt 파일을 열 수 있는지 확인합니다.

4. 다운로드한 복구 패키지 파일('.zip')을 두 개의 안전하고 서로 다른 위치에 복사합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

시스템 상태를 확인합니다

StorageGRID 시스템을 업그레이드하기 전에 시스템이 업그레이드를 수용할 준비가 되었는지 확인해야 합니다. 시스템이 정상적으로 실행되고 있고 모든 그리드 노드가 작동 중인지 확인해야 합니다.

단계

1. 를 사용하여 Grid Manager에 로그인합니다 지원되는 웹 브라우저.
2. 활성 경고를 확인하고 해결합니다.

   특정 경고에 대한 자세한 내용은 를 참조하십시오 경고 참조.

3. 충돌하는 그리드 작업이 활성 또는 보류 중이 아닌지 확인합니다.

   a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.

   b. Site_ * > * *primary Admin Node* * > * CMN * > * Grid Tasks * > * Configuration * 을 선택합니다.

      ILME(정보 수명 주기 관리 평가) 작업은 소프트웨어 업그레이드와 동시에 실행할 수 있는 유일한 그리드 작업입니다.

   c. 다른 그리드 작업이 활성 또는 보류 중인 경우 작업이 완료될 때까지 기다리거나 잠금을 해제합니다.

      > 작업이 완료되지 않거나 잠금이 해제되면 기술 지원 부서에 문의하십시오.

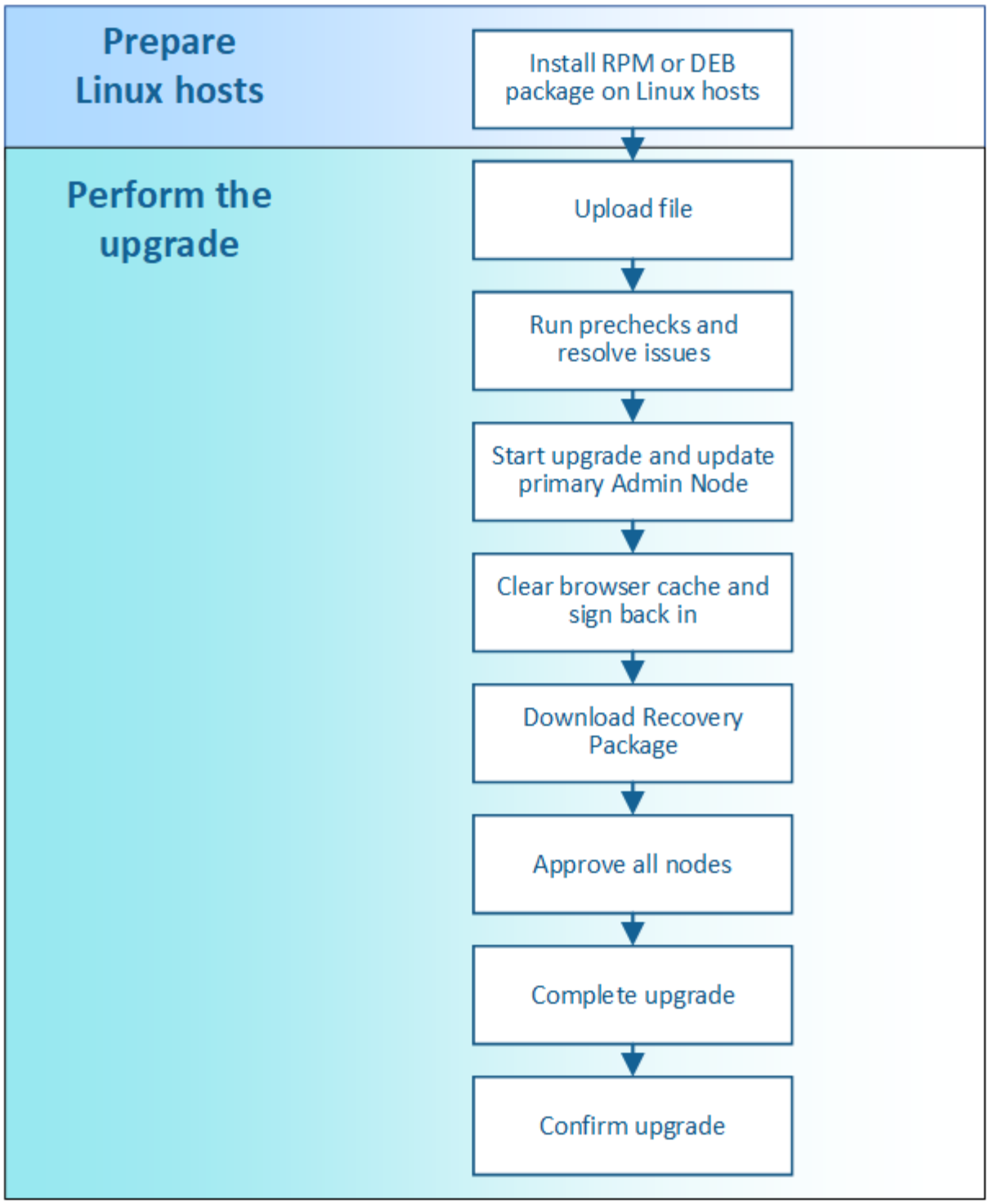
4. 을 참조하십시오 내부 그리드 노드 통신 및 외부 통신 업그레이드하기 전에 StorageGRID 11.6에 필요한 모든 포트가 열려 있는지 확인합니다.

   > 사용자 지정 방화벽 포트를 연 경우 업그레이드 사전 확인 중에 알림이 표시됩니다. 업그레이드를 진행하기 전에 기술 지원 부서에 문의해야 합니다.

StorageGRID 소프트웨어를 업그레이드합니다

워크플로우 업그레이드

업그레이드를 시작하기 전에 일반 워크플로를 검토하십시오. StorageGRID 업그레이드 페이지에서는 각 업그레이드 단계를 안내합니다.



1. Linux 호스트에 StorageGRID 노드가 구축된 경우 각 호스트에 RPM 또는 DEB 패키지를 설치합니다 업그레이드를 시작하기 전에
2. 기본 관리자 노드에서 StorageGRID 업그레이드 페이지에 액세스하여 업그레이드 파일을 업로드합니다.
3. 선택적으로 업그레이드 사전 점검을 실행하여 실제 업그레이드를 시작하기 전에 문제를 감지하고 해결합니다.
4. 사전 점검을 실행하고 기본 관리 노드를 자동으로 업그레이드하는 업그레이드를 시작합니다. 기본 관리자 노드가 업그레이드 중인 동안에는 그리드 관리자에 액세스할 수 없습니다. 감사 로그도 사용할 수 없습니다. 이 업그레이드에는 최대 30분이 소요될 수 있습니다.
5. 기본 관리 노드를 업그레이드한 후 웹 브라우저의 캐시를 지우고 다시 로그인한 다음 StorageGRID 업그레이드

페이지로 돌아갑니다.

6. 새 복구 패키지를 다운로드합니다.
7. 그리드 노드를 승인합니다. 개별 그리드 노드, 그리드 노드 그룹 또는 모든 그리드 노드를 승인할 수 있습니다.

> 노드를 중지하고 재부팅할 준비가 되어 있는지 확실하지 않은 경우 그리드 노드의 업그레이드를 승인하지 마십시오.

8. 작업을 재개합니다. 모든 그리드 노드가 업그레이드되면 새 기능이 활성화되고 작업을 재개할 수 있습니다. 백그라운드 * 데이터베이스 업그레이드 * 작업 및 * 최종 업그레이드 단계 * 작업이 완료될 때까지 서비스 해제 또는 확장 절차를 수행해야 합니다.
9. 업그레이드가 완료되면 소프트웨어 버전을 확인하고 핫픽스를 적용합니다.

관련 정보

업그레이드를 완료하는 데 걸리는 시간을 예상합니다

Linux: 모든 호스트에 **RPM** 또는 **DEB** 패키지를 설치합니다

StorageGRID 노드가 Linux 호스트에 배포된 경우 업그레이드를 시작하기 전에 각 호스트에 추가 RPM 또는 DEB 패키지를 설치해야 합니다.

필요한 것

StorageGRID용 NetApp 다운로드 페이지에서 다음 '.tgz' 또는 '.zip' 파일 중 하나를 다운로드해야 합니다.

> 서비스 랩톱에서 Windows를 실행 중인 경우 '.zip' 파일을 사용합니다.

Linux 플랫폼	추가 파일(하나 선택)
Red Hat Enterprise Linux 또는 CentOS	• 'STORageGRID-Webscale-*VERSION*-RPM-*UniqueID*.zip' • S torageGRID-Webscale-*version*-RPM-*UniqueID*.tgz
Ubuntu 또는 Debian	• 'storageGRID-Webscale-*version*-deb-*UniqueID*.zip' • 'storageGRID-Webscale-*version*-deb-*UniqueID*.tgz'

단계

1. 설치 파일에서 RPM 또는 DEB 패키지를 추출합니다.
2. 모든 Linux 호스트에 RPM 또는 DEB 패키지를 설치합니다.

   Linux 플랫폼의 설치 지침에서 StorageGRID 호스트 서비스 설치 단계를 참조하십시오.

   - Red Hat Enterprise Linux 또는 CentOS를 설치합니다
   - Ubuntu 또는 Debian을 설치합니다

   새 패키지는 추가 패키지로 설치됩니다. 기존 패키지를 제거하지 마십시오.

업그레이드를 수행합니다

업그레이드를 수행할 준비가 되면 '.upgrade' 아카이브를 선택하고 프로비저닝 암호를 입력합니다. 옵션으로 실제 업그레이드를 수행하기 전에 업그레이드 사전 점검을 실행할 수 있습니다.

필요한 것

모든 고려 사항을 검토하고 모든 계획 및 준비 단계를 완료했습니다.

업그레이드 파일을 업로드합니다

1. 를 사용하여 Grid Manager에 로그인합니다 지원되는 웹 브라우저.
2. 유지보수 * > * 시스템 * > * 소프트웨어 업데이트 * 를 선택합니다.

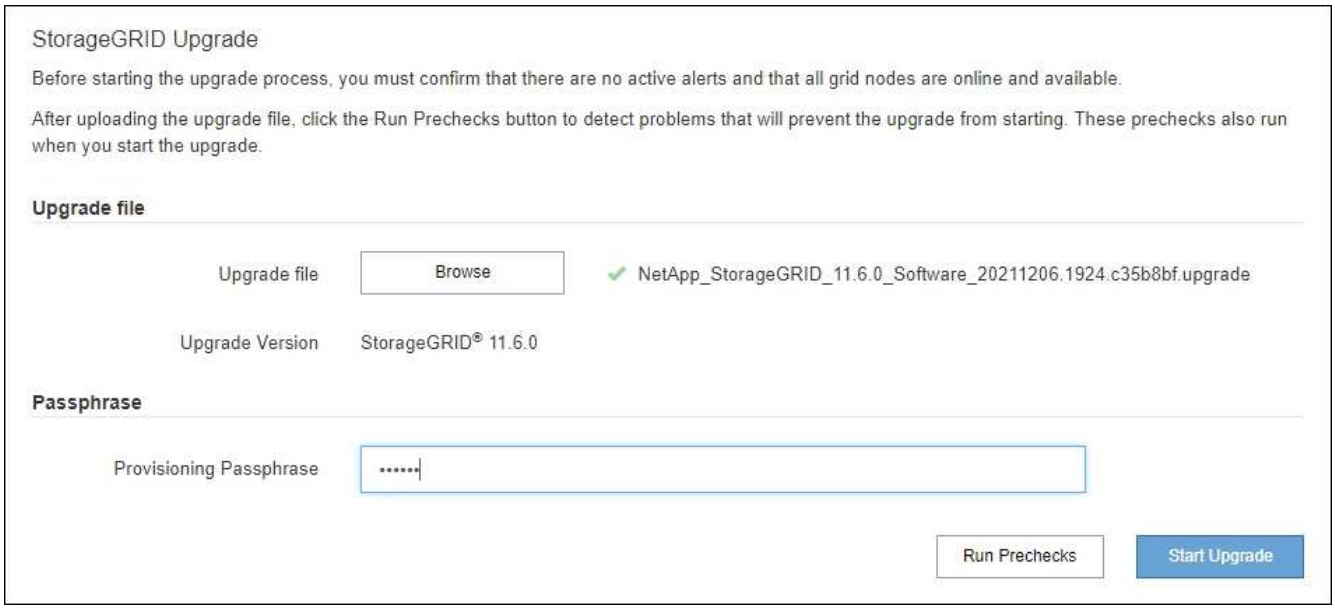
   소프트웨어 업데이트 페이지가 나타납니다.

3. StorageGRID 업그레이드 * 를 선택합니다.
4. StorageGRID 업그레이드 페이지에서 '.upgrade' 아카이브를 선택합니다.
   a. 찾아보기 * 를 선택합니다.
   b. 'NetApp_StorageGRID_11.6.0_Software_UniqueID.upgrade' 파일을 찾아 선택합니다
   c. 열기 * 를 선택합니다.

      파일이 업로드되고 검증됩니다. 검증 프로세스가 완료되면 업그레이드 파일 이름 옆에 녹색 확인 표시가 나타납니다.

5. 텍스트 상자에 프로비저닝 암호를 입력합니다.

   Prechecks 실행 * 및 * 업그레이드 시작 * 버튼이 활성화됩니다.



사전 점검을 실행합니다

선택적으로 실제 업그레이드를 시작하기 전에 시스템 상태를 확인할 수 있습니다. Prechecks 실행 * 을 선택하면 업그레이드를 시작하기 전에 문제를 감지하고 해결할 수 있습니다. 업그레이드를 시작할 때 동일한 사전 점검을 수행합니다. PreCheck 실패로 인해 업그레이드 프로세스가 중단되고 일부 오류는 해결을 위해 기술 지원 부서의 개입이 필요할 수 있습니다.

1. 사전 검사 실행 * 을 선택합니다.
2. 사전 점검을 완료할 때까지 기다립니다.
3. 지침에 따라 보고된 모든 사전 점검 오류를 해결하십시오.

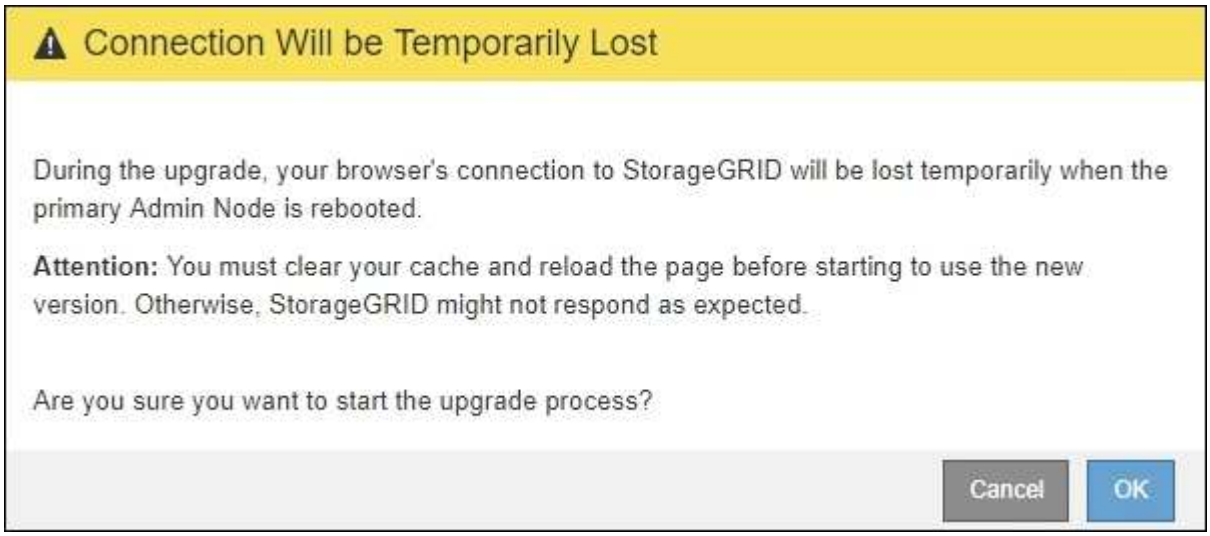
> 사용자 지정 방화벽 포트를 연 경우 사전 검사 확인 중에 알림을 받습니다. 업그레이드를 진행하기 전에 기술 지원 부서에 문의해야 합니다.

업그레이드를 시작하고 기본 관리 노드를 업데이트합니다

업그레이드가 시작되면 업그레이드 사전 점검을 수행하고 서비스 중지, 소프트웨어 업그레이드 및 서비스 재시작이 포함된 기본 관리 노드가 업그레이드됩니다. 기본 관리자 노드가 업그레이드 중인 동안에는 그리드 관리자에 액세스할 수 없습니다. 감사 로그도 사용할 수 없습니다. 이 업그레이드에는 최대 30분이 소요될 수 있습니다.

1. 업그레이드를 수행할 준비가 되면 * 업그레이드 시작 * 을 선택합니다.

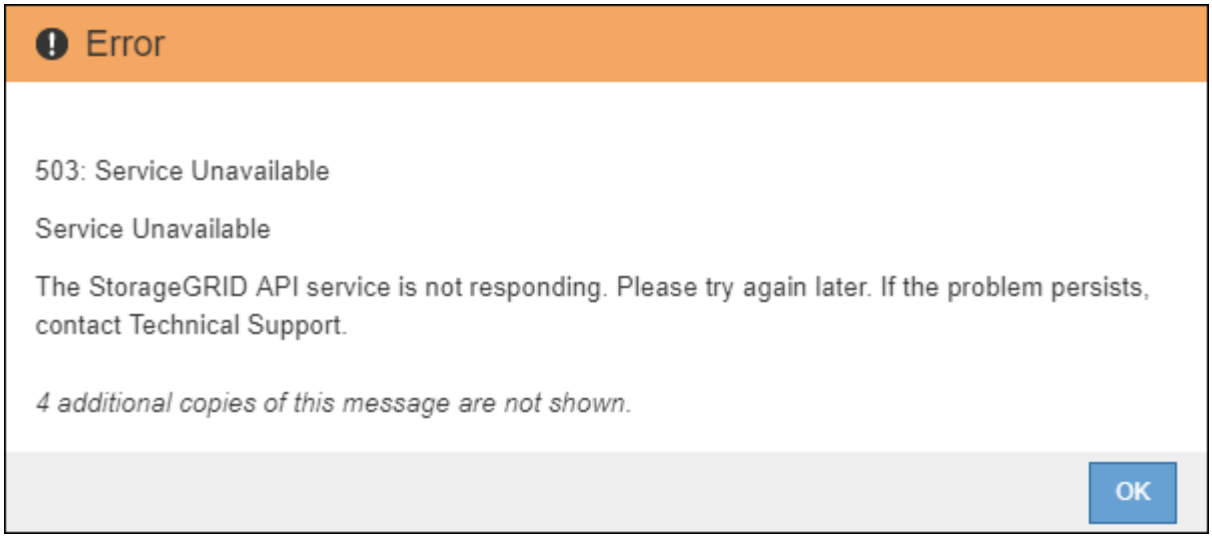
   기본 관리 노드가 재부팅되면 브라우저의 연결이 끊어진다는 경고 메시지가 나타납니다.



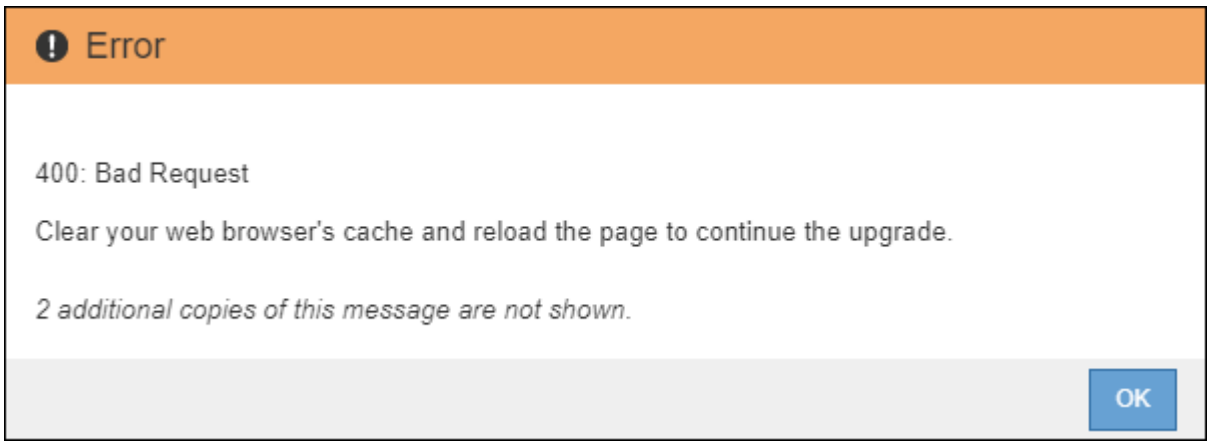
2. 경고를 확인하고 업그레이드 프로세스를 시작하려면 * OK * 를 선택합니다.
3. 업그레이드 사전 점검을 수행하고 운영 관리 노드를 업그레이드할 때까지 기다립니다.

   > 사전 점검 오류가 보고되면 이를 해결하고 * 업그레이드 시작 * 을 다시 선택하십시오.

   기본 관리 노드를 업그레이드하는 동안 여러 * 503: 서비스 사용 불가 * 및 * 서버에 연결하는 중 문제 * 메시지가 나타납니다. 이 메시지는 무시해도 됩니다.



4. 400: Bad Request * 메시지가 표시되면 다음 단계로 이동합니다. 관리자 노드 업그레이드가 완료되었습니다.



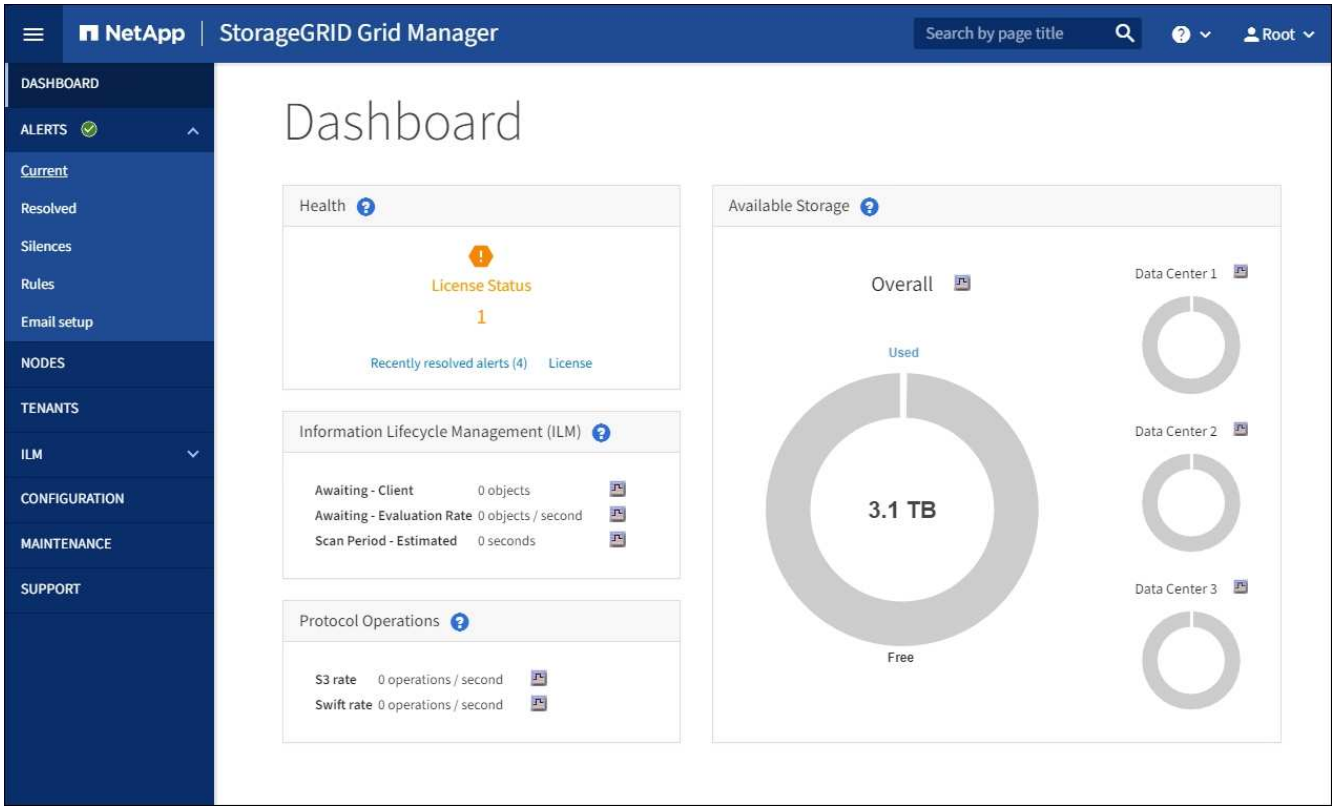
브라우저 캐시를 지우고 다시 로그인합니다

1. 기본 관리 노드를 업그레이드한 후 웹 브라우저의 캐시를 지우고 다시 로그인합니다.

   자세한 내용은 웹 브라우저 설명서를 참조하십시오.

이전 버전의 소프트웨어에서 사용된 오래된 리소스를 제거하려면 웹 브라우저의 캐시를 지워야 합니다.

기본 관리 노드가 업그레이드되었음을 나타내는 다시 설계된 Grid Manager 인터페이스가 나타납니다.



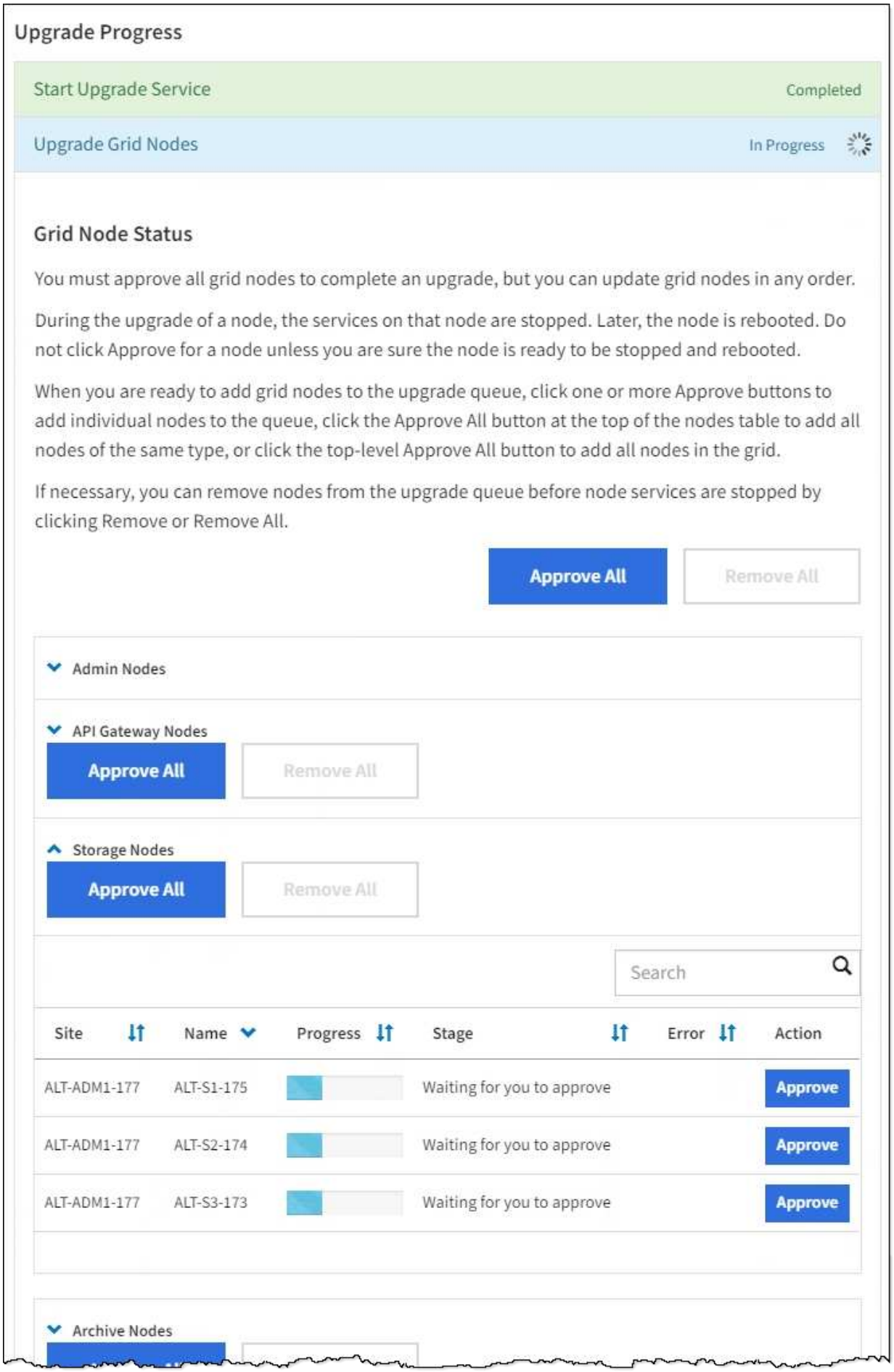
2. 측면 표시줄에서 * maintenance * 를 선택하여 Maintenance(유지 관리) 메뉴를 엽니다.
3. 시스템 * 섹션에서 * 소프트웨어 업데이트 * 를 선택합니다.
4. StorageGRID 업그레이드 * 섹션에서 * 업그레이드 * 를 선택합니다.
5. 각 주요 업그레이드 작업에 대한 정보를 제공하는 StorageGRID 업그레이드 페이지의 업그레이드 진행률 섹션을 검토합니다.
   a. * 업그레이드 서비스 시작 * 은 첫 번째 업그레이드 작업입니다. 이 작업 중에 소프트웨어 파일이 그리드 노드로 배포되고 업그레이드 서비스가 시작됩니다.
   b. 업그레이드 서비스 * 작업 시작이 완료되면 * 그리드 노드 업그레이드 * 작업이 시작됩니다.
   c. 업그레이드 그리드 노드 * 작업이 진행 중인 동안 그리드 노드 상태 테이블이 나타나고 시스템의 각 그리드 노드에 대한 업그레이드 단계가 표시됩니다.

복구 패키지를 다운로드하고 모든 그리드 노드를 업그레이드합니다

1. 그리드 노드가 그리드 노드 상태 테이블에 나타난 후 그리드 노드를 승인하기 전에 복구 패키지의 새 복사본을 다운로드합니다.

기본 관리 노드에서 소프트웨어 버전을 업그레이드한 후 복구 패키지 파일의 새 복사본을 다운로드해야 합니다. 복구 패키지 파일을 사용하면 오류가 발생할 경우 시스템을 복원할 수 있습니다.

2. Grid Node Status 테이블의 정보를 검토합니다. 그리드 노드는 관리 노드, API 게이트웨이 노드, 스토리지 노드 및 아카이브 노드 유형별로 섹션에 정렬됩니다.


Upgrade Progress
Start Upgrade Service
Completed
Upgrade Grid Nodes
In Progress
Grid Node Status
You must approve all grid nodes to complete an upgrade, but you can update grid nodes in any order.
During the upgrade of a node, the services on that node are stopped. Later, the node is rebooted. Do not click Approve for a node unless you are sure the node is ready to be stopped and rebooted.
When you are ready to add grid nodes to the upgrade queue, click one or more Approve buttons to add individual nodes to the queue, click the Approve All button at the top of the nodes table to add all nodes of the same type, or click the top-level Approve All button to add all nodes in the grid.
If necessary, you can remove nodes from the upgrade queue before node services are stopped by clicking Remove or Remove All.
Approve All
Remove All
Admin Nodes
API Gateway Nodes
Approve All
Remove All
Storage Nodes
Approve All
Remove All
Search
Site
Name
Progress
Stage
Error
Action
ALT-ADM1-177
ALT-S1-175
Waiting for you to approve
Approve
ALT-ADM1-177
ALT-S2-174
Waiting for you to approve
Approve
ALT-ADM1-177
ALT-S3-173
Waiting for you to approve
Approve
Archive Nodes

그리드 노드는 이 페이지가 처음 나타날 때 다음 단계 중 하나일 수 있습니다.

- 완료(기본 관리 노드만 해당)
- 업그레이드를 준비하는 중입니다
- 소프트웨어 다운로드가 대기 중입니다
- 다운로드 중입니다
- 승인을 기다리는 중입니다

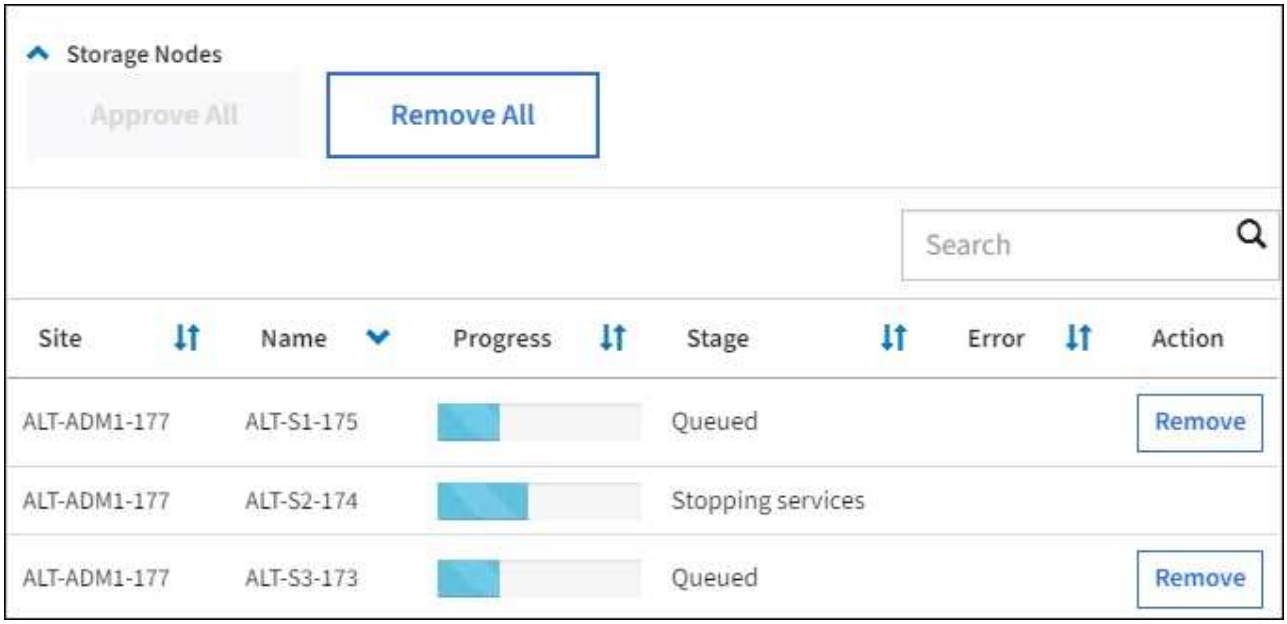
3. 업그레이드 대기열에 추가할 준비가 된 그리드 노드를 승인합니다.

> 그리드 노드에서 업그레이드가 시작되면 해당 노드의 서비스가 중지됩니다. 나중에 그리드 노드가 재부팅됩니다. 노드와 통신하는 클라이언트 애플리케이션의 서비스 중단을 방지하기 위해 노드를 중지 및 재부팅할 준비가 되어 있는지 확실하지 않은 경우 노드에 대한 업그레이드를 승인하지 마십시오. 필요에 따라 유지 보수 기간을 예약하거나 고객에게 알립니다.

StorageGRID 시스템의 모든 그리드 노드를 업그레이드해야 하지만 업그레이드 순서를 사용자 지정할 수 있습니다. 개별 그리드 노드, 그리드 노드 그룹 또는 모든 그리드 노드를 승인할 수 있습니다.

노드 업그레이드 순서가 중요한 경우, 노드 또는 노드 그룹을 한 번에 하나씩 승인하고 다음 노드 또는 노드 그룹을 승인하기 전에 각 노드에서 업그레이드가 완료될 때까지 기다리십시오.

- 하나 이상의 개별 노드를 업그레이드 대기열에 추가하려면 * Approve * 버튼을 하나 이상 선택합니다. 동일한 유형의 노드를 두 개 이상 승인하는 경우 노드는 한 번에 하나씩 업그레이드됩니다.
- 각 섹션에서 * Approve All * 버튼을 선택하여 동일한 유형의 모든 노드를 업그레이드 대기열에 추가합니다.
- 최상위 * 모두 승인 * 버튼을 선택하여 그리드의 모든 노드를 업그레이드 대기열에 추가합니다.
- 업그레이드 대기열에서 노드 또는 모든 노드를 제거하려면 * 제거 * 또는 * 모두 제거 * 를 선택합니다. 스테이지가 * 서비스 중지 * 에 도달하면 노드를 제거할 수 없습니다. 제거 * 버튼이 표시되지 않습니다.



4. 각 노드가 대기 중, 서비스 중지, 컨테이너 중지, Docker 이미지 정리, 기본 OS 패키지 업그레이드, 재부팅, 재부팅 후 단계 수행, 서비스 시작 및 완료 등의 업그레이드 단계를 진행할 때까지 기다립니다.

> 어플라이언스 노드가 기본 OS 패키지 업그레이드 단계에 도달하면 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램 소프트웨어가 업데이트됩니다. 이러한 자동 프로세스를 통해 StorageGRID 어플라이언스 설치 프로그램 버전이 StorageGRID 소프트웨어 버전과 동기화된 상태로 유지됩니다.

업그레이드를 완료합니다

모든 그리드 노드가 업그레이드 단계를 완료하면 * 그리드 노드 업그레이드 * 작업이 완료된 것으로 표시됩니다. 나머지 업그레이드 작업은 백그라운드에서 자동으로 수행됩니다.

1. 기능 사용 * 작업이 완료되는 즉시(빠르게 발생) 업그레이드된 StorageGRID 버전의 새 기능을 사용할 수도 있습니다.
2. 업그레이드 데이터베이스 * 작업 중에 업그레이드 프로세스에서는 각 노드를 검사하여 Cassandra 데이터베이스를 업데이트할 필요가 없는지 확인합니다.

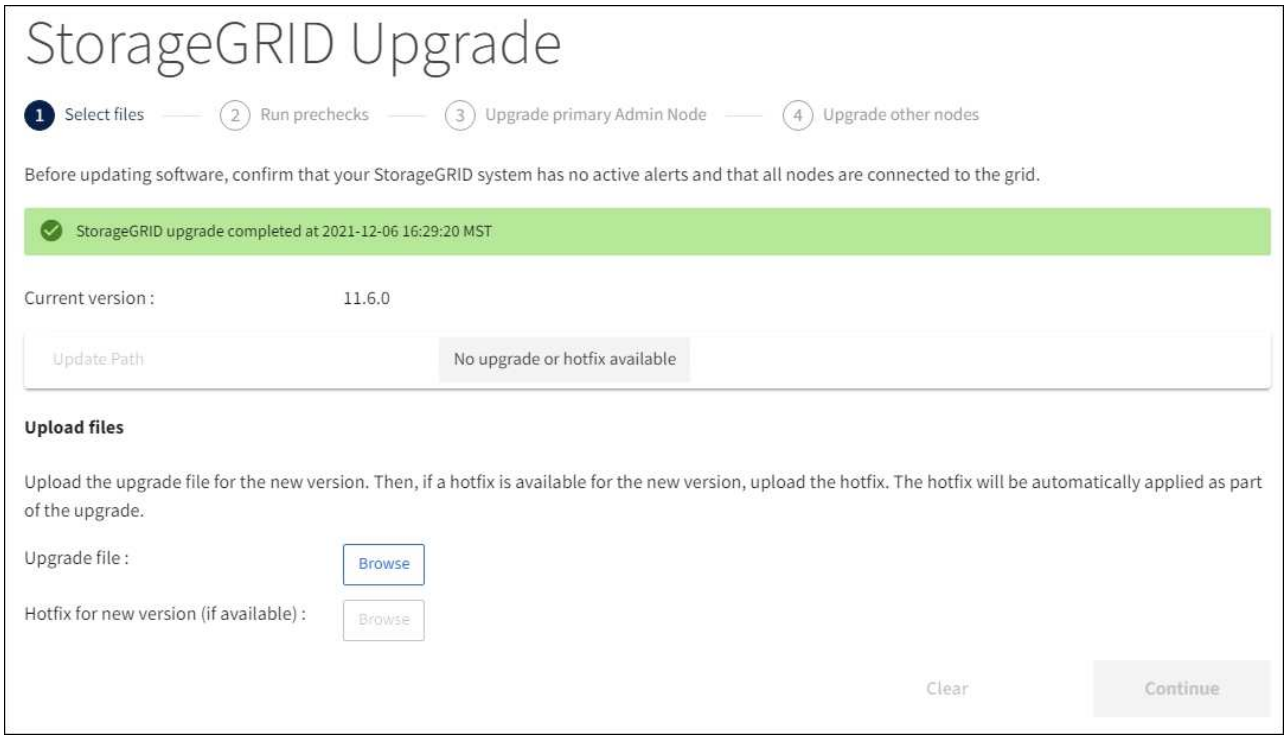
> StorageGRID 11.5에서 11.6으로의 업그레이드는 Cassandra 데이터베이스 업그레이드가 필요하지 않지만 Cassandra 서비스는 각 스토리지 노드에서 중지되었다가 다시 시작됩니다. 향후 StorageGRID 기능 릴리즈를 위해 Cassandra 데이터베이스 업데이트 단계를 완료하는 데 며칠이 걸릴 수 있습니다.

3. 데이터베이스 업그레이드 * 작업이 완료되면 * 최종 업그레이드 단계 * 작업이 완료될 때까지 몇 분 정도 기다립니다.

   최종 업그레이드 단계 작업이 완료되면 업그레이드가 완료됩니다.

업그레이드를 확인합니다

1. 업그레이드가 성공적으로 완료되었는지 확인합니다.
   a. 그리드 관리자 상단에서 도움말 아이콘을 선택하고 * 정보 * 를 선택합니다.
   b. 표시된 버전이 예상한 버전인지 확인합니다.
   c. 유지보수 * > * 시스템 * > * 소프트웨어 업데이트 * 를 선택합니다.
   d. StorageGRID 업그레이드 * 섹션에서 * 업그레이드 * 를 선택합니다.
   e. 녹색 배너에 예상 날짜 및 시간에 소프트웨어 업그레이드가 완료되었다는 메시지가 표시되는지 확인합니다.



2. StorageGRID 업그레이드 페이지에서 현재 StorageGRID 버전에 사용 가능한 핫픽스가 있는지 확인합니다.

> 업데이트 경로가 표시되지 않으면 브라우저에서 NetApp Support 사이트에 연결할 수 없는 것일 수 있습니다. 또는 AutoSupport 페이지(* 지원 * > * 도구 * > * AutoSupport *)의 * 소프트웨어 업데이트 확인 * 확인란이 비활성화될 수 있습니다.

3. 핫픽스를 사용할 수 있는 경우 파일을 다운로드합니다. 그런 다음 를 사용합니다 StorageGRID 핫픽스 절차 를 눌러 핫픽스를 적용합니다.
4. 그리드 작업이 정상으로 돌아갔는지 확인합니다.
   a. 서비스가 정상적으로 작동하고 있으며 예기치 않은 경고가 없는지 확인합니다.
   b. StorageGRID 시스템에 대한 클라이언트 연결이 예상대로 작동하고 있는지 확인합니다.

업그레이드 문제를 해결합니다

업그레이드가 완료되지 않습니다

업그레이드가 성공적으로 완료되지 않으면 직접 문제를 해결할 수 있습니다. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하기 전에 필요한 정보를 수집해야 합니다.

다음 섹션에서는 업그레이드가 부분적으로 실패한 상황에서 복구하는 방법에 대해 설명합니다. 업그레이드 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

업그레이드 사전 점검 오류

문제를 감지하고 해결하려면 실제 업그레이드를 시작하기 전에 업그레이드 사전 점검을 수동으로 실행할 수 있습니다. 대부분의 사전 검사 오류는 문제 해결 방법에 대한 정보를 제공합니다. 도움이 필요한 경우 기술 지원 팀에 문의하십시오.

프로비저닝 실패

자동 프로비저닝 프로세스가 실패하면 기술 지원 팀에 문의하십시오.

그리드 노드가 충돌하거나 시작되지 않습니다

업그레이드 프로세스 중에 그리드 노드가 작동 중단되거나 업그레이드가 완료된 후 성공적으로 시작되지 않는 경우 기술 지원 부서에 문의하여 기본적인 문제를 조사하고 해결하십시오.

수집 또는 데이터 검색이 중단됩니다

그리드 노드를 업그레이드하지 않을 때 데이터 수집 또는 검색이 예기치 않게 중단되면 기술 지원 부서에 문의하십시오.

데이터베이스 업그레이드 오류

데이터베이스 업그레이드에 오류가 발생하면 업그레이드를 다시 시도하십시오. 다시 실패하면 기술 지원 부서에 문의하십시오.

관련 정보

소프트웨어를 업그레이드하기 전에 시스템 상태를 확인합니다

사용자 인터페이스 문제를 해결합니다

새 버전의 StorageGRID 소프트웨어로 업그레이드한 후 그리드 관리자 또는 테넌트 관리자에 문제가 발생할 수 있습니다.

웹 인터페이스가 예상대로 응답하지 않습니다

StorageGRID 소프트웨어를 업그레이드한 후 그리드 관리자 또는 테넌트 관리자가 예상대로 응답하지 않을 수 있습니다.

웹 인터페이스에 문제가 있는 경우:

- 를 사용하고 있는지 확인합니다 지원되는 웹 브라우저.

  > 브라우저 지원은 일반적으로 각 StorageGRID 릴리스에 대한 변경 사항을 적용합니다.

- 웹 브라우저 캐시를 지웁니다.

  캐시를 지우면 이전 버전의 StorageGRID 소프트웨어에서 사용된 오래된 리소스가 제거되고 사용자 인터페이스가 다시 올바르게 작동할 수 있습니다. 자세한 내용은 웹 브라우저 설명서를 참조하십시오.

"Docker 이미지 가용성 검사**"** 오류 메시지

업그레이드 프로세스를 시작하려고 할 때 ""다음 문제는 Docker 이미지 가용성 검사 검증 제품군으로 확인되었습니다."라는 오류 메시지가 나타날 수 있습니다. 업그레이드를 완료하기 전에 모든 문제를 해결해야 합니다.

식별된 문제를 해결하는 데 필요한 변경 사항을 잘 모르는 경우 기술 지원 부서에 문의하십시오.

메시지	원인	해결 방법
업그레이드 버전을 확인할 수 없습니다. 업그레이드 버전 정보 파일 '{file_path}'이(가) 예상 형식과 일치하지 않습니다.	업그레이드 패키지가 손상되었습니다.	업그레이드 패키지를 다시 업로드하고 다시 시도하십시오. 문제가 지속되면 기술 지원 팀에 문의하십시오.
업그레이드 버전 정보 파일 "{file_path}"을(를) 찾을 수 없습니다. 업그레이드 버전을 확인할 수 없습니다.	업그레이드 패키지가 손상되었습니다.	업그레이드 패키지를 다시 업로드하고 다시 시도하십시오. 문제가 지속되면 기술 지원 팀에 문의하십시오.
"{node_name}"에 현재 설치된 릴리스 버전을 확인할 수 없습니다.	노드의 중요 파일이 손상되었습니다.	기술 지원 부서에 문의하십시오.
"{node_name}"에 버전을 나열하려고 시도하는 중 연결 오류가 발생했습니다	노드가 오프라인이거나 연결이 끊어졌습니다.	모든 노드가 온라인 상태이고 운영 관리 노드에서 연결할 수 있는지 확인한 후 다시 시도하십시오.
노드 "{node_name}의 호스트에 로드된 StorageGRID "{upgrade_version}" 이미지가 없습니다. 업그레이드를 진행하기 전에 이미지와 서비스를 호스트에 설치해야 합니다.	업그레이드 RPM 또는 DEB 패키지가 노드가 실행 중인 호스트에 설치되지 않았거나 이미지를 가져오는 중입니다. • 참고: * 이 오류는 Linux에서 컨테이너로 실행되는 노드에만 적용됩니다.	노드가 실행 중인 모든 Linux 호스트에 RPM 또는 DEB 패키지가 설치되었는지 확인합니다. 서비스 및 이미지 파일 모두에 대해 버전이 올바른지 확인합니다. 몇 분 정도 기다린 후 다시 시도하십시오. 을 참조하십시오 Linux: 모든 호스트에 RPM 또는 DEB 패키지를 설치합니다.
노드 "{node_name}"을(를) 확인하는 동안 오류가 발생했습니다	예기치 않은 오류가 발생했습니다.	몇 분 정도 기다린 후 다시 시도하십시오.
사전 점검을 실행하는 동안 오류가 발생했습니다. '{error_string}'	예기치 않은 오류가 발생했습니다.	몇 분 정도 기다린 후 다시 시도하십시오.

메타데이터 예약 공간 증가 설정을 사용합니다

StorageGRID 11.6으로 업그레이드한 후 스토리지 노드가 RAM 및 사용 가능한 공간에 대한 특정 요구 사항을 충족하는 경우 메타데이터 예약 공간 시스템 설정을 늘릴 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한 또는 그리드 토폴로지 페이지 구성 및 기타 그리드 구성 권한이 있어야 합니다.
- StorageGRID 11.6 업그레이드를 완료했습니다.

이 작업에 대해

StorageGRID 11.6으로 업그레이드한 후 시스템 전체의 메타데이터 예약 공간 설정을 8TB까지 수동으로 늘릴 수

있습니다. 11.6 업그레이드 후 추가 메타데이터 공간을 예약하면 향후 하드웨어 및 소프트웨어 업그레이드가 간소화됩니다.

다음 두 문이 모두 참인 경우에만 시스템 전체의 메타데이터 예약된 공간 설정 값을 늘릴 수 있습니다.

- 시스템의 모든 사이트에 있는 스토리지 노드에는 각각 128GB 이상의 RAM이 있습니다.
- 시스템의 모든 사이트에 있는 스토리지 노드에는 스토리지 볼륨 0에 사용 가능한 공간이 충분합니다.

이 설정을 높이는 경우 모든 스토리지 노드의 스토리지 볼륨 0에서 오브젝트 스토리지에 사용할 수 있는 공간을 동시에 줄일 수 있습니다. 따라서 메타데이터 예약 공간을 예상 오브젝트 메타데이터 요구 사항에 따라 8TB 미만의 값으로 설정하는 것이 좋습니다.

> 일반적으로 더 낮은 값 대신 더 높은 값을 사용하는 것이 좋습니다. 메타데이터 예약 공간 설정이 너무 큰 경우 나중에 줄일 수 있습니다. 반대로 값을 나중에 증가해도 시스템에서 공간을 확보하기 위해 오브젝트 데이터를 이동해야 할 수 있습니다.

메타데이터 예약 공간 설정이 특정 스토리지 노드의 개체 메타데이터 저장소에 대해 허용되는 공간에 미치는 영향에 대한 자세한 설명은 로 이동하십시오 오브젝트 메타데이터 스토리지 관리.

단계

1. 를 사용하여 Grid Manager에 로그인합니다 지원되는 웹 브라우저.
2. 현재 메타데이터 예약 공간 설정을 확인합니다.
   a. 구성 * > * 시스템 * > * 스토리지 옵션 * 을 선택합니다.
   b. Storage Watermarks 섹션에서 * Metadata Reserved Space * 값을 확인합니다.
3. 각 스토리지 노드의 스토리지 볼륨 0에 이 값을 늘릴 수 있는 충분한 공간이 있는지 확인합니다.
   a. 노드 * 를 선택합니다.
   b. 그리드에서 첫 번째 스토리지 노드를 선택합니다.
   c. Storage 탭을 선택합니다.
   d. Volumes 섹션에서 * /var/local/rangedb/0 * 항목을 찾습니다.
   e. 사용할 수 있는 값이 사용하려는 새 값과 현재 메타데이터 예약된 공간 값의 차이와 같거나 큰지 확인합니다.

      예를 들어 메타데이터 예약 공간 설정이 현재 4TB이고 이 설정을 6TB로 늘리려면 사용 가능한 값이 2TB 이상이어야 합니다.

   f. 모든 스토리지 노드에 대해 이 단계를 반복합니다.
      - 하나 이상의 스토리지 노드에 사용 가능한 공간이 충분하지 않으면 메타데이터 예약 공간 값을 늘릴 수 없습니다. 이 절차를 계속 진행하지 마십시오.
      - 각 스토리지 노드에 볼륨 0에 사용 가능한 공간이 충분한 경우 다음 단계로 이동합니다.
4. 각 스토리지 노드에 128MB 이상의 RAM이 있는지 확인합니다.
   a. 노드 * 를 선택합니다.
   b. 그리드에서 첫 번째 스토리지 노드를 선택합니다.
   c. 하드웨어 * 탭을 선택합니다.
   d. 메모리 사용량 차트 위에 커서를 놓습니다. 총 메모리 * 가 128GB 이상인지 확인합니다.

e. 모든 스토리지 노드에 대해 이 단계를 반복합니다.

- 하나 이상의 스토리지 노드에 사용 가능한 총 메모리가 충분하지 않으면 메타데이터 예약 공간 값을 늘릴 수 없습니다. 이 절차를 계속 진행하지 마십시오.
- 각 스토리지 노드에 총 메모리가 최소 128GB인 경우 다음 단계로 이동합니다.

5. 메타데이터 예약 공간 설정을 업데이트합니다.

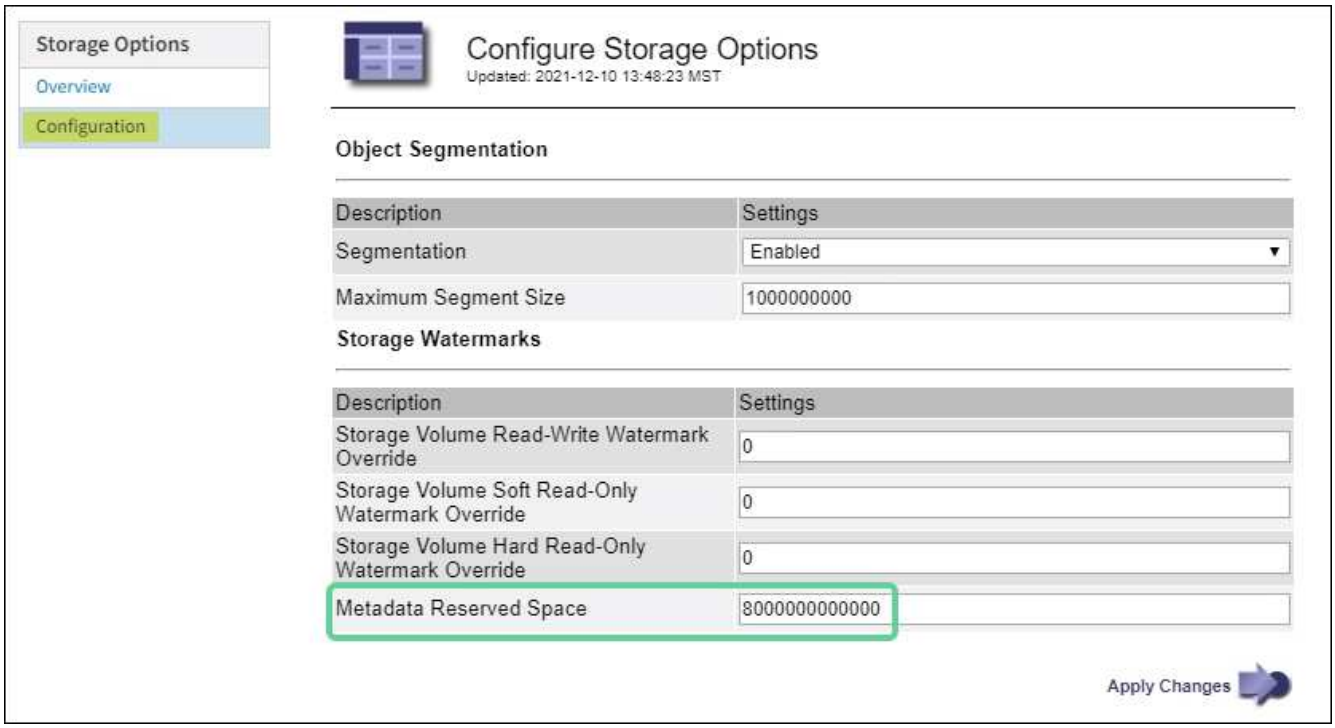
a. 구성 * > * 시스템 * > * 스토리지 옵션 * 을 선택합니다.

b. 구성 탭을 선택합니다.

c. Storage Watermarks 섹션에서 * Metadata Reserved Space * 를 선택합니다.

d. 새 값을 입력합니다.

예를 들어, 지원되는 최대 값인 8TB를 입력하려면 * 8000000000000 * (8, 0이 12개 있음)을 입력합니다.



a. Apply Changes * 를 선택합니다.

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

Red Hat Enterprise Linux 또는 CentOS 설치: 개요

RHEL(Red Hat Enterprise Linux) 또는 CentOS Linux 환경에 StorageGRID 시스템을 설치하는 과정은 세 가지 기본 단계로 구성됩니다.

1. * 준비 *: 계획 및 준비 중에 다음 작업을 수행합니다.
   - StorageGRID의 하드웨어 및 스토리지 요구사항에 대해 알아보십시오.
   - 의 세부 사항에 대해 자세히 알아보십시오 StorageGRID 네트워킹 따라서 네트워크를 적절하게 구성할 수 있습니다.

- StorageGRID 그리드 노드를 호스팅하는 데 사용할 물리적 또는 가상 서버를 식별하고 준비합니다.
- 준비한 서버:
  - Linux를 설치합니다
  - 호스트 네트워크를 구성합니다
  - 호스트 스토리지를 구성합니다
  - 컨테이너 엔진을 장착하십시오
  - StorageGRID 호스트 서비스를 설치합니다

2. * 배포 *: 적절한 사용자 인터페이스를 사용하여 그리드 노드를 배포합니다. 그리드 노드를 구축하면 StorageGRID 시스템의 일부로 생성되고 하나 이상의 네트워크에 연결됩니다.
   a. Linux 명령줄 및 노드 구성 파일을 사용하여 1단계에서 준비한 호스트에 소프트웨어 기반 그리드 노드를 배포합니다.
   b. StorageGRID 어플라이언스 설치 프로그램을 사용하여 StorageGRID 어플라이언스 노드를 배포합니다.

> 하드웨어 관련 설치 및 통합 지침은 StorageGRID 설치 절차에 포함되어 있지 않습니다. StorageGRID 어플라이언스를 설치하는 방법에 대한 자세한 내용은 해당 어플라이언스의 설치 및 유지 관리 지침을 참조하십시오.

3. * 구성 *: 모든 노드가 배포되면 그리드 관리자를 사용하여 그리드를 구성하고 설치를 완료합니다.

이 지침은 StorageGRID 시스템을 배포하고 구성하는 표준 접근 방식을 권장합니다. 다음 대체 접근 방법에 대한 정보도 참조하십시오.

- Ansible, Puppet 또는 Chef와 같은 표준 오케스트레이션 프레임워크를 사용하여 RHEL 또는 CentOS를 설치하고, 네트워킹 및 스토리지를 구성하고, 컨테이너 엔진 및 StorageGRID 호스트 서비스를 설치하고, 가상 그리드 노드를 배포합니다.
- 설치 아카이브에 제공되는 Python 구성 스크립트를 사용하여 StorageGRID 시스템의 구축 및 구성을 자동화합니다.
- Python 구성 스크립트(설치 아카이브나 StorageGRID 어플라이언스 설치 프로그램에서 사용 가능)를 사용하여 어플라이언스 그리드 노드의 구축 및 구성을 자동화합니다.
- StorageGRID 배포의 고급 개발자인 경우 설치 REST API를 사용하여 StorageGRID 그리드 노드 설치를 자동화합니다.

Red Hat 또는 **CentOS** 설치를 계획하고 준비합니다

설치하기 전에**(Red Hat** 또는 **CentOS)**

그리드 노드를 배포하고 StorageGRID 그리드를 구성하기 전에 절차를 완료하기 위한 단계와 요구 사항을 숙지해야 합니다.

StorageGRID 배포 및 구성 절차에서는 StorageGRID 시스템의 아키텍처 및 작동에 대해 잘 알고 있다고 가정합니다.

단일 사이트 또는 여러 사이트를 한 번에 배포할 수 있지만, 모든 사이트는 최소 3개의 스토리지 노드를 보유해야 하는 최소 요구 사항을 충족해야 합니다.

StorageGRID 설치를 시작하기 전에 다음을 수행해야 합니다.

- 각 노드의 최소 CPU 및 RAM 요구사항을 비롯한 StorageGRID의 컴퓨팅 요구사항 이해
- StorageGRID가 트래픽 분리, 보안 및 관리의 편의를 위해 여러 네트워크를 지원하는 방법을 이해하고 각 StorageGRID 노드에 연결할 네트워크를 계획합니다.

  StorageGRID 네트워킹 지침을 참조하십시오.

- 각 그리드 노드 유형의 스토리지 및 성능 요구 사항을 이해합니다.
- 구축할 StorageGRID 노드의 수와 유형을 지원하기에 충분한 리소스를 제공하는 물리적 서버 세트, 가상 서버 또는 둘 다 식별합니다.
- 서비스 중단 없이 물리적 호스트에 대해 예약된 유지 관리를 수행하려는 경우 노드 마이그레이션에 대한 요구 사항을 파악합니다.
- 모든 네트워킹 정보를 미리 수집합니다. DHCP를 사용하지 않는 경우 각 그리드 노드에 할당할 IP 주소와 사용할 DNS(Domain Name System) 및 NTP(Network Time Protocol) 서버의 IP 주소를 수집합니다.
- 모든 StorageGRID 어플라이언스를 포함하여 필요한 모든 하드웨어를 사양에 맞게 설치, 연결 및 구성합니다.

> 하드웨어 관련 설치 및 통합 지침은 StorageGRID 설치 절차에 포함되어 있지 않습니다. StorageGRID 어플라이언스를 설치하는 방법에 대한 자세한 내용은 해당 어플라이언스의 설치 및 유지 관리 지침을 참조하십시오.

- 사용할 수 있는 배포 및 구성 도구 중에서 선택합니다.

관련 정보

네트워킹 지침

SG100 및 SG1000 서비스 어플라이언스

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG5600 스토리지 어플라이언스

필수 자료

StorageGRID를 설치하기 전에 필요한 자료를 수집하고 준비해야 합니다.

항목	참고
NetApp StorageGRID 라이센스	디지털 서명된 유효한 NetApp 라이센스가 있어야 합니다. • 참고 *: StorageGRID 설치 아카이브에는 테스트 및 개념 증명 그리드에 사용할 수 있는 비운영 라이센스가 포함되어 있습니다.
StorageGRID 설치 아카이브	반드시 해야 합니다 StorageGRID 설치 아카이브를 다운로드하고 파일의 압축을 풉니다.

항목	참고
서비스 노트북	StorageGRID 시스템은 서비스 랩톱을 통해 설치됩니다. 서비스 랩톱의 구성 요소: • 네트워크 포트 • SSH 클라이언트(예: PuTTY) • 지원되는 웹 브라우저
StorageGRID 설명서	• 릴리스 정보 • StorageGRID 관리 지침

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

StorageGRID 설치 파일을 다운로드하고 압축을 풉니다

StorageGRID 설치 아카이브를 다운로드하고 필요한 파일을 추출해야 합니다.

단계

1. 로 이동합니다 "StorageGRID용 NetApp 다운로드 페이지".
2. 최신 릴리스를 다운로드하려면 버튼을 선택하거나 드롭다운 메뉴에서 다른 버전을 선택하고 * GO * 를 선택합니다.
3. NetApp 계정의 사용자 이름과 암호를 사용하여 로그인합니다.
4. Caution/MustRead 문이 나타나면 해당 문을 읽고 확인란을 선택합니다.

   StorageGRID 릴리스를 설치한 후 필요한 핫픽스를 적용해야 합니다. 자세한 내용은 를 참조하십시오 복구 및 유지 관리 지침의 핫픽스 절차.

5. 최종 사용자 사용권 계약을 읽고 확인란을 선택한 다음 * 동의 및 계속 * 을 선택합니다.
6. StorageGRID * 설치 열에서 Red Hat Enterprise Linux 또는 CentOS에 대한 .tgz 또는 .zip 파일을 선택합니다.

   서비스 랩톱에서 Windows를 실행 중인 경우 '.zip' 파일을 선택합니다.

7. 아카이브 파일을 저장하고 압축을 풉니다.
8. 다음 목록에서 필요한 파일을 선택합니다.

   필요한 파일은 계획된 그리드 토폴로지와 StorageGRID 시스템을 구축하는 방법에 따라 다릅니다.

   표에 나열된 경로는 추출된 설치 아카이브에서 설치한 최상위 디렉토리에 상대적입니다

경로 및 파일 이름입니다	설명
	StorageGRID 다운로드 파일에 포함된 모든 파일을 설명하는 텍스트 파일입니다.
	제품에 대한 지원 권한을 제공하지 않는 무료 라이센스입니다.
	RHEL 또는 CentOS 호스트에 StorageGRID 노드 이미지를 설치하기 위한 rpm 패키지입니다.
	RHEL 또는 CentOS 호스트에 StorageGRID 호스트 서비스를 설치하기 위한 rpm 패키지입니다.
배포 스크립팅 도구	설명
	StorageGRID 시스템 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
	StorageGRID 어플라이언스 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
/rpms/configure -StorageGrid.sample.json	"configure-StorageGrid.py" 스크립트와 함께 사용할 구성 파일의 예
	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/rpms/configure -StorageGrid.blank.json을 지정합니다	configure-StorageGrid.py 스크립트와 함께 사용할 빈 구성 파일입니다.
	StorageGRID 컨테이너 배포를 위한 RHEL 또는 CentOS 호스트 구성을 위한 Ansible 역할 및 플레이북의 예 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.
/rpms/Extras/API-schemas	StorageGRID에 대한 API 스키마입니다. • 참고 *: 업그레이드를 수행하기 전에 이러한 스키마를 사용하여 StorageGRID 관리 API를 사용하도록 작성한 코드가 업그레이드 호환성 테스트를 위한 비프로덕션 StorageGRID 환경이 없는 경우 새 StorageGRID 릴리스와 호환되는지 확인할 수 있습니다.

CPU 및 RAM 요구 사항

StorageGRID 소프트웨어를 설치하기 전에 StorageGRID 시스템을 지원할 준비가 되도록 하드웨어를 확인 및 구성하십시오.

지원되는 서버에 대한 자세한 내용은 상호 운용성 매트릭스 를 참조하십시오.

각 StorageGRID 노드에는 다음과 같은 최소 리소스가 필요합니다.

- CPU 코어: 노드당 8개
- RAM: 사용 가능한 총 RAM과 시스템에서 실행 중인 비 StorageGRID 소프트웨어의 양에 따라 노드당 최소 24GB, 총 시스템 RAM보다 2GB ~ 16GB 이상

각 물리적 또는 가상 호스트에서 실행하려는 StorageGRID 노드 수가 사용 가능한 CPU 코어 수 또는 물리적 RAM을 초과하지 않는지 확인합니다. 호스트가 StorageGRID 실행 전용이 아닌 경우(권장되지 않음) 다른 애플리케이션의 리소스 요구 사항을 고려해야 합니다.

> CPU 및 메모리 사용량을 정기적으로 모니터링하여 이러한 리소스가 작업 부하를 지속적으로 수용할 수 있도록 합니다. 예를 들어, 가상 스토리지 노드에 대한 RAM 및 CPU 할당을 두 배로 하면 StorageGRID 어플라이언스 노드에 제공되는 것과 유사한 리소스를 제공할 수 있습니다. 또한 노드당 메타데이터 양이 500GB를 초과하는 경우 노드당 RAM을 48GB 이상으로 늘리는 것이 좋습니다. 개체 메타데이터 저장소 관리, 메타데이터 예약 공간 설정 증가 및 CPU 및 메모리 사용량 모니터링에 대한 자세한 내용은 StorageGRID 관리, 모니터링 및 업그레이드에 대한 지침을 참조하십시오.

하이퍼스레딩이 기본 물리적 호스트에서 활성화된 경우 노드당 8개의 가상 코어(4개의 물리적 코어)를 제공할 수 있습니다. 하이퍼스레딩이 기본 물리적 호스트에서 사용되지 않는 경우 노드당 8개의 물리적 코어를 제공해야 합니다.

가상 시스템을 호스트로 사용하고 VM의 크기와 수를 제어하는 경우 각 StorageGRID 노드에 대해 단일 VM을 사용하고 그에 따라 VM 크기를 조정해야 합니다.

운영 구축 환경에서는 동일한 물리적 스토리지 하드웨어 또는 가상 호스트에서 여러 스토리지 노드를 실행하지 않아야 합니다. 단일 StorageGRID 구축 환경의 각 스토리지 노드는 자체 격리된 장애 도메인에 있어야 합니다. 단일 하드웨어 장애가 단일 스토리지 노드에만 영향을 줄 수 있도록 하는 경우 오브젝트 데이터의 내구성과 가용성을 최대화할 수 있습니다.

스토리지 요구 사항에 대한 정보도 참조하십시오.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

요구사항을 충족해야 합니다

StorageGRID 관리

모니터링하고 문제를 해결합니다

소프트웨어 업그레이드

요구사항을 충족해야 합니다

초기 구성과 향후 스토리지 확장을 지원할 충분한 공간을 제공할 수 있도록 StorageGRID

노드의 스토리지 요구사항을 이해해야 합니다.

StorageGRID 노드에는 다음과 같은 세 가지 논리적 스토리지 범주가 필요합니다.

- * 컨테이너 풀 * — StorageGRID 노드를 지원할 호스트에 컨테이너 엔진을 설치 및 구성할 때 컨테이너 엔진 스토리지 드라이버에 할당되는 노드 컨테이너용 성능 계층(10K SAS 또는 SSD) 스토리지입니다.
- * 시스템 데이터 * — StorageGRID 호스트 서비스가 사용하고 개별 노드에 매핑하는 시스템 데이터 및 트랜잭션 로그의 노드당 영구 스토리지를 위한 성능 계층(10K SAS 또는 SSD) 스토리지입니다.
- * 오브젝트 데이터 * — 객체 데이터 및 객체 메타데이터의 영구 스토리지를 위한 Performance-Tier(10K SAS 또는 SSD) 스토리지 및 Capacity-Tier(NL-SAS/SATA) 대용량 스토리지

모든 스토리지 범주에 RAID 지원 블록 장치를 사용해야 합니다. 비중복 디스크, SSD 또는 JBOD는 지원되지 않습니다. 모든 스토리지 범주에서 공유 또는 로컬 RAID 스토리지를 사용할 수 있지만 StorageGRID의 노드 마이그레이션 기능을 사용하려면 시스템 데이터와 오브젝트 데이터를 공유 스토리지에 모두 저장해야 합니다.

성능 요구사항

컨테이너 풀, 시스템 데이터 및 오브젝트 메타데이터에 사용되는 볼륨의 성능은 시스템의 전반적인 성능에 큰 영향을 미칩니다. 이러한 볼륨에 성능 계층(10K SAS 또는 SSD) 스토리지를 사용하면 지연 시간, IOPS(초당 입출력 작업) 및 처리량 측면에서 디스크 성능이 적절하게 보장됩니다. 객체 데이터의 영구 스토리지를 위해 용량 계층(NL-SAS/SATA) 스토리지를 사용할 수 있습니다.

컨테이너 풀, 시스템 데이터 및 오브젝트 데이터에 사용되는 볼륨에는 다시 쓰기 캐시가 설정되어 있어야 합니다. 캐시는 보호되거나 영구 미디어에 있어야 합니다.

NetApp ONTAP 스토리지를 사용하는 호스트에 대한 요구사항

StorageGRID 노드에서 NetApp ONTAP 시스템에서 할당된 스토리지를 사용하는 경우 볼륨에 FabricPool 계층화 정책이 활성화되어 있지 않은지 확인합니다. StorageGRID 노드와 함께 사용되는 볼륨에 대해 FabricPool 계층화를 사용하지 않도록 설정하면 문제 해결과 스토리지 작업이 간소화됩니다.

> FabricPool를 사용하여 StorageGRID 관련 데이터를 StorageGRID 자체로 계층화하지 마십시오. StorageGRID 데이터를 StorageGRID로 다시 계층화하면 문제 해결과 운영 복잡성이 늘어납니다.

필요한 호스트 수입니다

각 StorageGRID 사이트에는 최소 3개의 스토리지 노드가 필요합니다.

> 운영 구축 시 단일 물리적 호스트 또는 가상 호스트에서 스토리지 노드를 두 개 이상 실행하지 마십시오. 각 스토리지 노드에 대해 전용 호스트를 사용하면 격리된 장애 도메인이 제공됩니다.

관리 노드 또는 게이트웨이 노드와 같은 다른 유형의 노드는 동일한 호스트에 구축하거나 필요에 따라 전용 호스트에 구축할 수 있습니다.

각 호스트의 스토리지 볼륨 수입니다

다음 표에는 각 호스트에 필요한 스토리지 볼륨(LUN) 수와 해당 호스트에 구축할 노드를 기준으로 각 LUN에 필요한 최소 크기가 나와 있습니다.

테스트된 최대 LUN 크기는 39TB입니다.

이러한 숫자는 전체 그리드가 아닌 각 호스트에 대한 것입니다.

LUN의 용도	스토리지 범주입니다	**LUN** 수입니다	최소 크기/**LUN**
컨테이너 엔진 스토리지 풀입니다	컨테이너 풀입니다	1	총 노드 수 × 100GB
'/var/local' 볼륨	시스템 데이터	이 호스트의 각 노드에 대해 1개	90GB
스토리지 노드	오브젝트 데이터	이 호스트의 각 스토리지 노드에 대해 3개 • 참고: * 소프트웨어 기반 스토리지 노드는 1-16개의 스토리지 볼륨을 가질 수 있습니다. 최소 3개의 스토리지 볼륨을 사용하는 것이 좋습니다.	12TB(4TB/LUN) 참조 스토리지 노드의 스토리지 요구 사항 를 참조하십시오.
관리자 노드 감사 로그	시스템 데이터	이 호스트의 각 관리 노드에 대해 1개	200GB
관리자 노드 테이블	시스템 데이터	이 호스트의 각 관리 노드에 대해 1개	200GB

구성된 감사 레벨, S3 오브젝트 키 이름 등의 사용자 입력 크기 및 보존해야 하는 감사 로그 데이터의 양에 따라 각 관리 노드에서 감사 로그 LUN의 크기를 늘려야 할 수 있습니다. 일반적으로, 그리드는 S3 작업당 약 1KB의 감사 데이터를 생성합니다. 즉, 200GB LUN이 하루에 7000만 개의 작업을 지원하거나 2~3일 동안 초당 800개의 작업을 지원합니다.

호스트의 최소 스토리지 공간입니다

다음 표에는 각 노드 유형에 필요한 최소 스토리지 공간이 나와 있습니다. 이 표를 사용하여 각 스토리지 범주에서 호스트에 구축해야 하는 최소 스토리지 양을 해당 호스트에 구축될 노드를 기반으로 결정할 수 있습니다.

디스크 스냅샷을 사용하여 그리드 노드를 복원할 수 없습니다. 대신 각 노드 유형에 대한 복구 및 유지보수 절차를 참조하십시오.

노드 유형입니다	컨테이너 풀입니다	시스템 데이터	오브젝트 데이터
스토리지 노드	100GB	90GB	4,000GB
관리자 노드	100GB	490GB(LUN 3개)	_해당 사항 없음 _
게이트웨이 노드	100GB	90GB	_해당 사항 없음 _

노드 유형입니다	컨테이너 풀입니다	시스템 데이터	오브젝트 데이터
아카이브 노드	100GB	90GB	_해당 사항 없음 _

예: 호스트에 대한 스토리지 요구 사항 계산

동일한 호스트에 스토리지 노드 1개, 관리 노드 1개, 게이트웨이 노드 1개 등 3개의 노드를 구축하려고 한다고 가정해 보겠습니다. 호스트에 최소 9개의 스토리지 볼륨을 제공해야 합니다. 노드 컨테이너용 300GB 이상의 성능 계층 스토리지, 시스템 데이터 및 트랜잭션 로그용 670GB 성능 계층 스토리지, 오브젝트 데이터를 위한 12TB의 용량 계층 스토리지가 필요합니다.

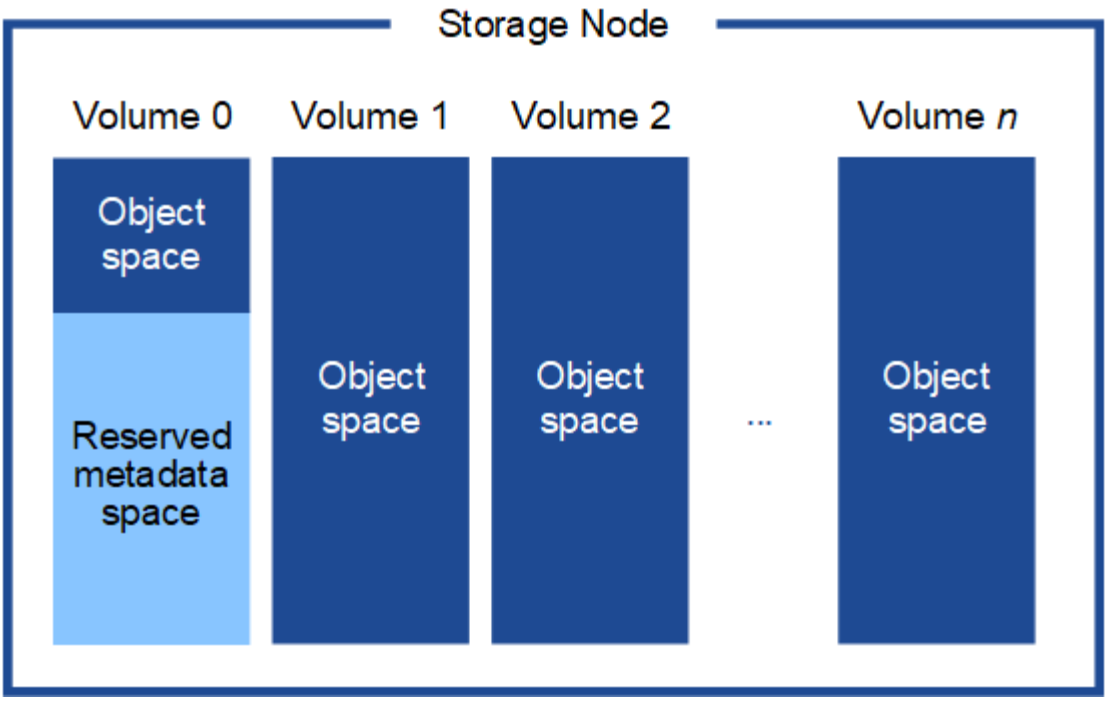
노드 유형입니다	**LUN**의 용도	**LUN** 수입니다	**LUN** 크기입니다
스토리지 노드	컨테이너 엔진 스토리지 풀입니다	1	300GB(100GB/노드)
스토리지 노드	'/var/local' 볼륨	1	90GB
스토리지 노드	오브젝트 데이터	3	12TB(4TB/LUN)
관리자 노드	'/var/local' 볼륨	1	90GB
관리자 노드	관리자 노드 감사 로그	1	200GB
관리자 노드	관리자 노드 테이블	1	200GB
게이트웨이 노드	'/var/local' 볼륨	1	90GB
• 합계 *		• 9 *	• 컨테이너 풀: * 300GB • 시스템 데이터: * 670GB • 오브젝트 데이터: * 12,000GB

스토리지 노드의 스토리지 요구 사항

소프트웨어 기반 스토리지 노드는 1-16개의 스토리지 볼륨을 가질 수 있습니다. -3개 이상의 스토리지 볼륨을 사용하는 것이 좋습니다. 각 스토리지 볼륨은 4TB 이상이어야 합니다.

> 어플라이언스 스토리지 노드는 최대 48개의 스토리지 볼륨을 가질 수 있습니다.

그림에 나와 있는 것처럼 StorageGRID는 각 스토리지 노드의 스토리지 볼륨 0에 객체 메타데이터를 위한 공간을 예약합니다. 스토리지 볼륨 0 및 스토리지 노드의 다른 스토리지 볼륨의 나머지 공간은 오브젝트 데이터에만 사용됩니다.



이중화를 제공하고 개체 메타데이터를 손실로부터 보호하기 위해 StorageGRID는 각 사이트의 시스템 모든 개체에 대한 메타데이터 복사본을 3개 저장합니다. 오브젝트 메타데이터의 복사본 3개는 각 사이트의 모든 스토리지 노드에 균등하게 분산됩니다.

새 스토리지 노드의 볼륨 0에 공간을 할당하는 경우 모든 오브젝트 메타데이터의 해당 노드에 적절한 공간이 있는지 확인해야 합니다.

- 적어도 볼륨 0에 4TB 이상을 할당해야 합니다.

> 스토리지 노드에 대해 하나의 스토리지 볼륨만 사용하고 볼륨에 4TB 이하를 할당하는 경우 스토리지 노드는 시작 시 스토리지 읽기 전용 상태로 전환되어 객체 메타데이터만 저장할 수 있습니다.

- 새 StorageGRID 11.6 시스템을 설치하고 각 스토리지 노드에 128GB 이상의 RAM이 있는 경우 볼륨 0에 8TB 이상을 할당해야 합니다. 볼륨 0에 더 큰 값을 사용하면 각 스토리지 노드에서 메타데이터에 허용되는 공간이 증가할 수 있습니다.
- 사이트에 대해 서로 다른 스토리지 노드를 구성할 때 가능하면 볼륨 0에 대해 동일한 설정을 사용합니다. 사이트에 크기가 다른 스토리지 노드가 있는 경우 볼륨이 0인 스토리지 노드가 해당 사이트의 메타데이터 용량을 결정합니다.

자세한 내용은 를 참조하십시오 오브젝트 메타데이터 스토리지 관리.

관련 정보

노드 컨테이너 마이그레이션 요구사항

복구 및 유지 관리

노드 컨테이너 마이그레이션 요구사항

노드 마이그레이션 기능을 사용하면 노드를 한 호스트에서 다른 호스트로 수동으로 이동할 수 있습니다. 일반적으로 두 호스트는 동일한 물리적 데이터 센터에 있습니다.

노드 마이그레이션을 통해 그리드 작업을 중단하지 않고 물리적 호스트 유지 관리를 수행할 수 있습니다. 물리적 호스트를 오프라인으로 전환하기 전에 한 번에 하나씩 모든 StorageGRID 노드를 다른 호스트로 이동하기만 하면 됩니다. 노드를 마이그레이션하려면 각 노드의 다운타임만 짧고 그리드 서비스의 운영 또는 가용성에 영향을 미치지 않아야 합니다.

StorageGRID 노드 마이그레이션 기능을 사용하려면 배포가 추가 요구 사항을 충족해야 합니다.

- 단일 물리적 데이터 센터의 호스트 전반에서 일관된 네트워크 인터페이스 이름
- 단일 물리적 데이터 센터의 모든 호스트에서 액세스할 수 있는 StorageGRID 메타데이터 및 오브젝트 저장소 볼륨을 위한 공유 스토리지입니다. 예를 들어, NetApp E-Series 스토리지 어레이를 사용할 수 있습니다.

가상 호스트를 사용 중이고 기본 하이퍼바이저 계층에서 VM 마이그레이션을 지원하는 경우 StorageGRID의 노드 마이그레이션 기능 대신 이 기능을 사용할 수 있습니다. 이 경우 이러한 추가 요구 사항을 무시할 수 있습니다.

마이그레이션 또는 하이퍼바이저 유지 보수를 수행하기 전에 노드를 정상적으로 종료합니다. 의 지침을 참조하십시오 그리드 노드 종료.

VMware Live Migration은 지원되지 않습니다

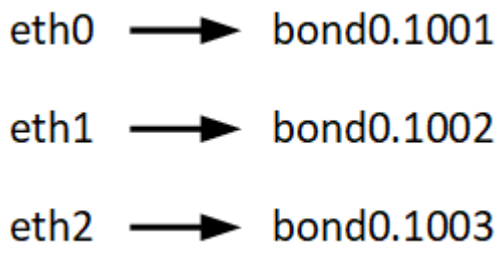
OpenStack Live Migration 및 VMware LIVE vMotion을 사용하면 가상 머신 클록 시간이 단축되며 모든 유형의 그리드 노드에서는 지원되지 않습니다. 드물지만 잘못된 클럭 시간으로 인해 데이터 또는 구성 업데이트가 손실될 수 있습니다.

콜드 마이그레이션이 지원됩니다. 콜드 마이그레이션에서는 StorageGRID 노드를 호스트 간에 마이그레이션하기 전에 종료해야 합니다. 의 지침을 참조하십시오 그리드 노드 종료.

일관된 네트워크 인터페이스 이름

한 호스트에서 다른 호스트로 노드를 이동하려면 StorageGRID 호스트 서비스가 노드가 현재 위치에 있는 외부 네트워크 연결이 새 위치에서 복제될 수 있다는 확신을 가져야 합니다. 호스트에서 일관된 네트워크 인터페이스 이름을 사용하면 이러한 자신감을 얻을 수 있습니다.

예를 들어 호스트 1에서 실행되는 StorageGRID NodeA가 다음과 같은 인터페이스 매핑으로 구성되었다고 가정합니다.



화살표의 왼쪽 면은 StorageGRID 컨테이너 내에서 보는 기존 인터페이스(즉, 그리드, 관리자 및 클라이언트 네트워크 인터페이스)에 해당합니다. 화살표의 오른쪽은 동일한 물리적 인터페이스 결합에 종속된 세 개의 VLAN 인터페이스인 이러한 네트워크를 제공하는 실제 호스트 인터페이스에 해당합니다.

이제 NodeA를 Host2로 마이그레이션한다고 가정해 보겠습니다. Host2에 bond0.1001, bond0.1002 및 bond0.1003이라는 인터페이스도 있는 경우 시스템은 Host1에서와 같이 같은 이름의 인터페이스가 Host2에서 동일한 연결을 제공한다고 가정하여 이동을 허용합니다. 호스트 2에 동일한 이름의 인터페이스가 없으면 이동이 허용되지 않습니다.

여러 호스트에 걸쳐 일관된 네트워크 인터페이스 이름 지정을 달성하는 방법은 여러 가지가 있습니다. 를 참조하십시오

호스트 네트워크 구성 몇 가지 예를 참조하십시오.

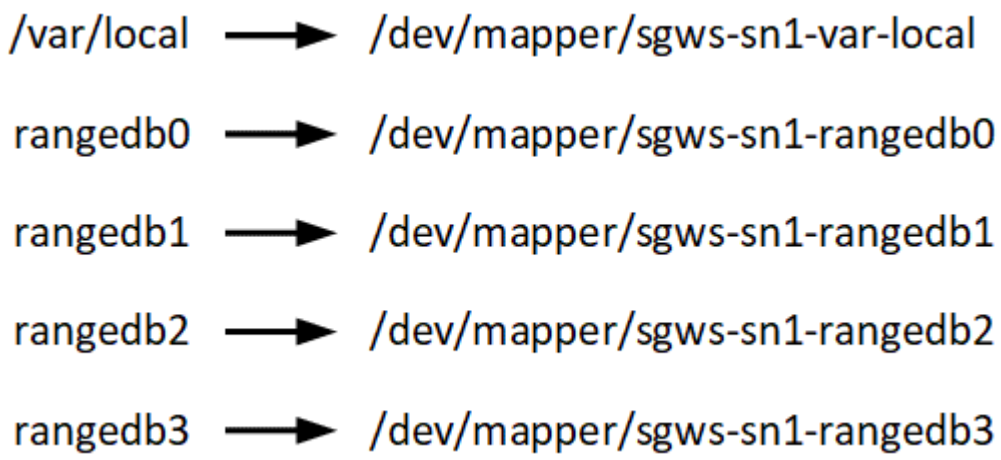
공유 스토리지

오버헤드가 낮은 노드를 신속하게 마이그레이션하기 위해 StorageGRID 노드 마이그레이션 기능은 노드 데이터를 물리적으로 이동하지 않습니다. 대신 노드 마이그레이션은 다음과 같이 한 쌍의 엑스포트 및 임포트 작업으로 수행됩니다.

1. "노드 내보내기" 작업 중에 호스트 A에서 실행되는 노드 컨테이너에서 소량의 영구 상태 데이터가 추출되어 해당 노드의 시스템 데이터 볼륨에 캐시됩니다. 그런 다음 HostA의 노드 컨테이너가 인스턴스화됩니다.
2. "노드 가져오기" 작업 중에 HostA에 적용되는 것과 동일한 네트워크 인터페이스를 사용하는 호스트 B의 노드 컨테이너와 블록 스토리지 매핑이 인스턴스화됩니다. 그런 다음 캐시된 영구 상태 데이터가 새 인스턴스에 삽입됩니다.

이 작업 모드가 주어지면 마이그레이션을 허용하고 작동하기 위해서는 노드의 모든 시스템 데이터와 객체 스토리지 볼륨을 HostA와 HostB에서 액세스할 수 있어야 합니다. 또한 HostA 및 HostB에서 동일한 LUN을 참조하도록 보장된 이름을 사용하여 노드에 매핑되어야 합니다.

다음 예에서는 호스트에서 DM 다중 경로를 사용하고 있는 StorageGRID 스토리지 노드에 대한 블록 디바이스 매핑을 위한 단일 솔루션을 보여 주며, 별칭 필드는 모든 호스트에서 사용할 수 있는 일관되고 친숙한 블록 디바이스 이름을 제공하기 위해 '/etc/multipath.conf'에서 사용되었습니다.



구축 툴

StorageGRID 설치의 일부 또는 전부를 자동화할 수 있습니다.

구축 자동화는 다음 경우에 유용할 수 있습니다.

- 이미 Ansible, Puppet 또는 Chef와 같은 표준 오케스트레이션 프레임워크를 사용하여 물리적 호스트 또는 가상 호스트를 구축 및 구성합니다.
- 여러 StorageGRID 인스턴스를 배포하려고 합니다.
- 크고 복잡한 StorageGRID 인스턴스를 구축하고 있습니다.

StorageGRID 호스트 서비스는 패키지에 의해 설치되며 수동 설치 중에 대화형으로 만들 수 있는 구성 파일에 의해 구동되거나, 표준 오케스트레이션 프레임워크를 사용하여 자동 설치를 지원하기 위해 미리 준비되거나 프로그래밍 방식으로 준비됩니다. StorageGRID는 StorageGRID 어플라이언스 및 전체 StorageGRID 시스템(""그리드")의 구성을 자동화하는 옵션 Python 스크립트를 제공합니다. 이러한 스크립트를 직접 사용하거나 을 사용하는 방법을

알아볼 수 있습니다 StorageGRID 설치 REST API 그리드 배포 및 구성 도구에서는 스스로 개발할 수 있습니다.

StorageGRID 구축의 전부 또는 일부를 자동화하려는 경우 을 검토하십시오 설치를 자동화합니다 설치 프로세스를 시작하기 전에

호스트 준비(**Red Hat** 또는 **CentOS**)

Linux를 설치합니다

모든 그리드 호스트에 Linux를 설치해야 합니다. 를 사용합니다 "NetApp 상호 운용성 매트릭스 툴" 를 클릭하여 지원되는 버전 목록을 가져옵니다.

단계

1. 배포자의 지침 또는 표준 절차에 따라 모든 물리적 또는 가상 그리드 호스트에 Linux를 설치합니다.

   표준 Linux 설치 프로그램을 사용하는 경우 "컴퓨팅 노드" 소프트웨어 구성(있는 경우)이나 "최소 설치" 기반 환경을 선택하는 것이 좋습니다. 그래픽 데스크톱 환경을 설치하지 마십시오.

2. Extras 채널을 포함하여 모든 호스트가 패키지 리포지토리에 액세스할 수 있는지 확인합니다.

   이 설치 절차의 뒷부분에서 이러한 추가 패키지가 필요할 수 있습니다.

3. 스왑이 활성화된 경우:

   a. '$sudo swapoff - -all' 명령을 실행합니다

   b. 설정을 유지하려면 '/etc/fstab'에서 모든 스왑 항목을 제거하십시오.

   스왑을 완전히 사용하지 않도록 설정하면 성능이 크게 저하될 수 있습니다.

호스트 네트워크 구성(**Red Hat Enterprise Linux** 또는 **CentOS**)

호스트에서 Linux 설치를 완료한 후 나중에 배포할 StorageGRID 노드에 매핑하는 데 적합한 네트워크 인터페이스 세트를 준비하기 위해 몇 가지 추가 구성을 수행해야 할 수 있습니다.

필요한 것

- 을(를) 검토했습니다 StorageGRID 네트워킹 지침.
- 에 대한 정보를 검토했습니다 노드 컨테이너 마이그레이션 요구사항.
- 가상 호스트를 사용하는 경우 를 읽었습니다 MAC 주소 복제에 대한 고려 사항 및 권장 사항 호스트 네트워크를 구성하기 전에

VM을 호스트로 사용하는 경우 가상 네트워크 어댑터로 VMXNET 3을 선택해야 합니다. VMware E1000 네트워크 어댑터로 인해 특정 Linux 배포판에 배포된 StorageGRID 컨테이너의 연결 문제가 발생했습니다.

이 작업에 대해

그리드 노드는 그리드 네트워크와 선택적으로 관리자 및 클라이언트 네트워크에 액세스할 수 있어야 합니다. 호스트의 물리적 인터페이스를 각 그리드 노드의 가상 인터페이스에 연결하는 매핑을 생성하여 이 액세스를 제공합니다. 호스트 인터페이스를 생성할 때 이름을 friendly 로 사용하여 모든 호스트에 쉽게 구축하고 마이그레이션을 설정할 수 있습니다.

호스트와 하나 이상의 노드 간에 동일한 인터페이스를 공유할 수 있습니다. 예를 들어, 호스트 액세스 및 노드 관리 네트워크 액세스에 동일한 인터페이스를 사용하여 호스트 및 노드 유지 관리를 용이하게 할 수 있습니다. 호스트와 개별 노드 간에 동일한 인터페이스를 공유할 수 있지만 모두 IP 주소가 서로 달라야 합니다. IP 주소는 노드 간 또는 호스트와 노드 간에 공유할 수 없습니다.

동일한 호스트 네트워크 인터페이스를 사용하여 호스트의 모든 StorageGRID 노드에 그리드 네트워크 인터페이스를 제공하거나, 각 노드에 대해 다른 호스트 네트워크 인터페이스를 사용하거나, 둘 사이에 작업을 수행할 수 있습니다. 그러나 일반적으로 단일 노드에 대한 Grid 및 Admin Network 인터페이스와 동일한 호스트 네트워크 인터페이스를 제공하거나 한 노드에 대한 Grid Network 인터페이스와 다른 노드에 대한 Client Network 인터페이스를 제공하지 않습니다.

이 작업은 여러 가지 방법으로 완료할 수 있습니다. 예를 들어, 호스트가 가상 머신이고 각 호스트에 대해 하나 또는 두 개의 StorageGRID 노드를 구축하는 경우 하이퍼바이저에서 올바른 수의 네트워크 인터페이스를 생성하고 일대일 매핑을 사용할 수 있습니다. 운영 용도로 베어 메탈 호스트에 여러 노드를 구축하는 경우 Linux 네트워킹 스택이 VLAN 및 LACP 지원을 활용하여 내결함성 및 대역폭 공유를 제공할 수 있습니다. 다음 섹션에서는 이러한 두 가지 예에 대해 자세히 설명합니다. 이러한 예제 중 하나를 사용할 필요가 없습니다. 필요에 맞는 방법을 사용할 수 있습니다.

> 연결 또는 브리지 장치를 컨테이너 네트워크 인터페이스로 직접 사용하지 마십시오. 이렇게 하면 컨테이너 네임스페이스의 연결 및 브리지 장치와 함께 MACVLAN을 사용하는 커널 문제로 인해 노드 시작이 방지될 수 있습니다. 대신 VLAN 또는 가상 이더넷(veth) 쌍과 같은 비연결 장치를 사용하십시오. 이 디바이스를 노드 구성 파일의 네트워크 인터페이스로 지정합니다.

관련 정보

노드 구성 파일을 만드는 중입니다

MAC 주소 복제에 대한 고려 사항 및 권장 사항

MAC 주소 클로닝은 컨테이너가 호스트의 MAC 주소를 사용하고 호스트는 사용자가 지정한 주소나 임의로 생성된 주소의 MAC 주소를 사용하게 합니다. 무차별 모드 네트워크 구성을 사용하지 않으려면 MAC 주소 복제를 사용해야 합니다.

MAC 클론 생성 활성화

특정 환경에서는 관리 네트워크, 그리드 네트워크 및 클라이언트 네트워크에 전용 가상 NIC를 사용할 수 있으므로 MAC 주소 클로닝을 통해 보안을 강화할 수 있습니다. 컨테이너가 호스트에 있는 전용 NIC의 MAC 주소를 사용하도록 하면 무차별 모드 네트워크 구성을 사용하지 않도록 할 수 있습니다.

> MAC 주소 복제는 가상 서버 설치에 사용하기 위한 것이며 모든 물리적 어플라이언스 구성에서 제대로 작동하지 않을 수 있습니다.

> MAC 클론 대상 인터페이스가 사용 중이어서 노드가 시작되지 않는 경우 노드를 시작하기 전에 링크를 "다운"으로 설정해야 할 수 있습니다. 또한 링크가 작동 중일 때 가상 환경에서 네트워크 인터페이스에서 MAC 클로닝을 방지할 수 있습니다. 노드가 MAC 주소를 설정하지 못하고 사용 중인 인터페이스로 인해 시작되는 경우 노드를 시작하기 전에 링크를 "다운"으로 설정하면 문제가 해결될 수 있습니다.

MAC 주소 복제는 기본적으로 해제되어 있으며 노드 구성 키로 설정해야 합니다. StorageGRID를 설치할 때 활성화해야 합니다.

각 네트워크마다 하나의 키가 있습니다.

- 'admin_network_target_type_interface_clone_MAC'
- 'GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC
- 'client_network_target_type_interface_clone_MAC'

키를 "true"로 설정하면 컨테이너가 호스트 NIC의 MAC 주소를 사용하게 됩니다. 또한 호스트는 지정된 컨테이너 네트워크의 MAC 주소를 사용합니다. 기본적으로 컨테이너 주소는 임의로 생성된 주소이지만 '_network_mac' 노드 설정 키를 사용하여 설정한 경우에는 해당 주소가 대신 사용됩니다. 호스트와 컨테이너의 MAC 주소는 항상 다릅니다.

> 하이퍼바이저에서 무차별 모드를 설정하지 않고 가상 호스트에서 MAC 클로닝을 활성화하면 호스트의 인터페이스를 사용하는 Linux 호스트 네트워킹이 작동하지 않을 수 있습니다.

Mac 클론 복제 활용 사례

MAC 클로닝에는 다음 두 가지 사용 사례를 고려해야 합니다.

- MAC 클로닝이 활성화되지 않음: 노드 구성 파일의 '_clone_mac' 키가 설정되지 않았거나 "false"로 설정된 경우, 호스트는 호스트 NIC MAC을 사용하고 컨테이너는 "_network_mac" 키에 MAC이 지정되지 않은 경우 StorageGRID로 생성된 MAC을 갖게 됩니다. '_network_mac' 키에 주소가 설정되어 있으면 '_network_mac' 키에 지정된 주소가 컨테이너에 지정됩니다. 이러한 키 구성을 위해서는 무차별 모드를 사용해야 합니다.
- MAC 클론 생성 활성화: 노드 구성 파일의 '_clone_mac' 키가 "true"로 설정되면 컨테이너는 호스트 NIC MAC을 사용하고 호스트는 "_network_mac" 키에 MAC을 지정하지 않는 한 StorageGRID 생성 MAC을 사용합니다. '_network_mac' 키에 주소가 설정되어 있으면 호스트는 생성된 주소 대신 지정된 주소를 사용합니다. 이 키 구성에서 무차별 모드를 사용해서는 안 됩니다.

> MAC 주소 클로닝을 사용하지 않고 모든 인터페이스가 하이퍼바이저에 의해 할당된 것이 아닌 MAC 주소에 대한 데이터를 수신 및 전송하도록 허용하는 경우, 가상 스위치 및 포트 그룹 수준의 보안 속성이 Promiscuous Mode, MAC Address 변경 및 Forged 전송에 대해 * Accept * 로 설정되어 있는지 확인합니다. 가상 스위치에 설정된 값은 포트 그룹 수준의 값으로 재정의할 수 있으므로 두 위치에서 설정이 동일한지 확인합니다.

MAC 클로닝을 활성화하려면 를 참조하십시오 노드 구성 파일 생성 지침.

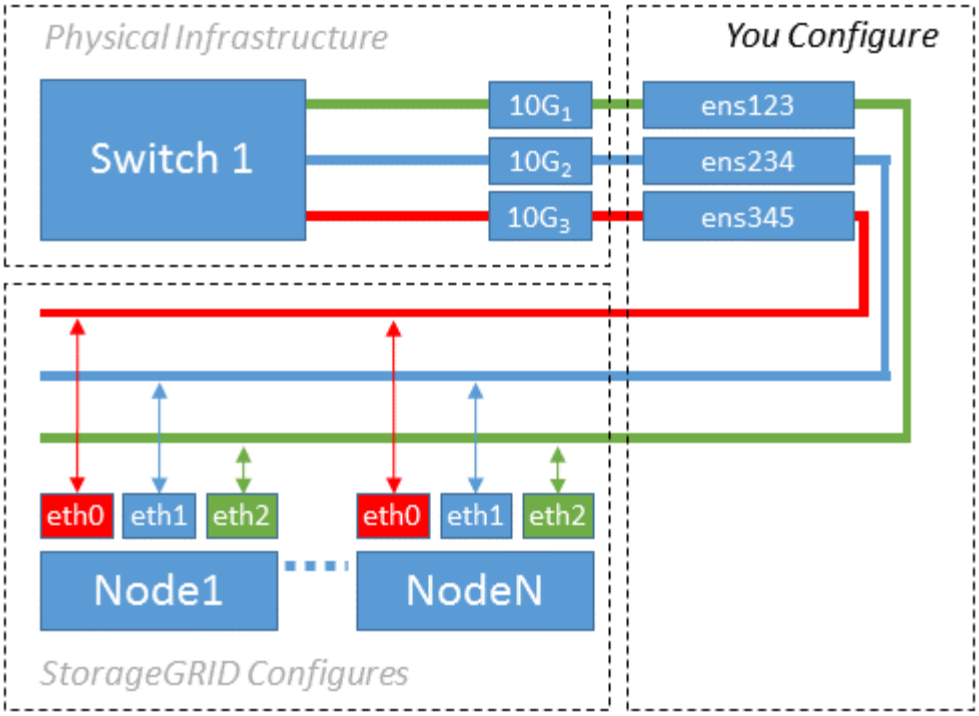
Mac 클론 복제의 예

인터페이스 ens256의 경우 MAC 주소가 11:22:33:44:55:66이고 노드 구성 파일의 경우 다음 키가 있는 호스트에서 활성화된 MAC 클론 복제의 예:

- 'admin_network_target=ens256'
- 'admin_network_MAC=B2:9c:02:C2:27:10'
- 'admin_network_target_type_interface_clone_MAC=TRUE'
- 결과 *: en256의 호스트 MAC은 B2:9c:02:C2:27:10이고 관리 네트워크 MAC은 11:22:33:44:55:66입니다

예 **1:** 물리적 **NIC** 또는 가상 **NIC**에 **1:1** 대 **1** 매핑

예제 1에서는 호스트측 구성이 거의 또는 전혀 필요하지 않은 간단한 물리적 인터페이스 매핑에 대해 설명합니다.



Linux 운영 체제는 설치 또는 부팅 시 또는 인터페이스가 핫 추가되는 경우 자동으로 'ensXYZ' 인터페이스를 생성합니다. 부팅 후 인터페이스가 자동으로 실행되도록 설정하는 것 외에는 구성이 필요하지 않습니다. 나중에 구성 프로세스에서 올바른 매핑을 제공할 수 있도록 StorageGRID 네트워크(그리드, 관리자 또는 클라이언트)에 해당하는 "ensXYZ"를 결정해야 합니다.

이 그림에서는 여러 StorageGRID 노드를 보여 줍니다. 그러나 일반적으로 단일 노드 VM에 이 구성을 사용합니다.

스위치 1이 물리적 스위치인 경우 액세스 모드에 대해 인터페이스 10G1 - 10G3에 연결된 포트를 구성하고 해당 VLAN에 배치해야 합니다.

예 **2: VLAN**을 전달하는 **LACP** 결합

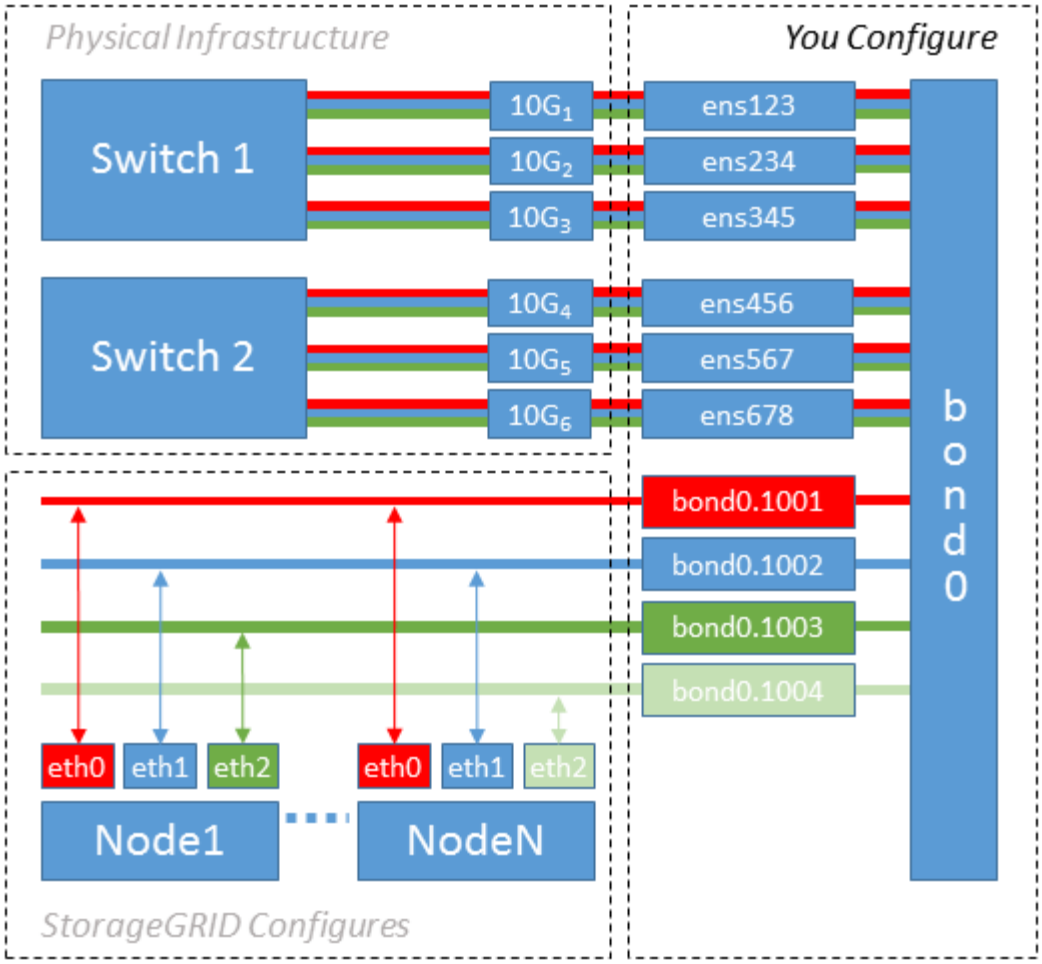
이 작업에 대해

예제 2에서는 네트워크 인터페이스를 결합하거나 사용 중인 Linux 배포판에서 VLAN 인터페이스를 만드는 방법에 대해 잘 알고 있다고 가정합니다.

예제 2에서는 단일 호스트의 모든 노드에서 사용 가능한 모든 네트워크 대역폭을 쉽게 공유할 수 있도록 지원하는 일반, 유연한 VLAN 기반 체계를 설명합니다. 이 예는 특히 베어 메탈 호스트에 적용할 수 있습니다.

이 예제를 이해하려면 각 데이터 센터에 그리드, 관리자 및 클라이언트 네트워크에 대한 세 개의 개별 서브넷이 있다고 가정합니다. 서브넷은 별도의 VLAN(1001, 1002 및 1003)에 있으며 LACP 결합 트렁크 포트(bond0)의 호스트에 제공됩니다. Bond.0.1001, bond0.1002 및 bond0.1003의 세 가지 VLAN 인터페이스를 구성합니다.

동일한 호스트에서 노드 네트워크에 대해 별도의 VLAN과 서브넷이 필요한 경우, 결합에 VLAN 인터페이스를 추가하고 이를 호스트에 매핑할 수 있습니다(그림에서 bond0.1004로 표시됨).



단계

1. StorageGRID 네트워크 연결에 사용할 모든 물리적 네트워크 인터페이스를 단일 LACP 결합으로 통합합니다.

   모든 호스트에서 본드에도 동일한 이름을 사용합니다. 예를 들어, 'bond0'과 같습니다.

2. 표준 VLAN 인터페이스 명명 규칙인 physdev-name.vlan ID를 사용하여 이 결합을 연결된 "물리적 장치"로 사용하는 VLAN 인터페이스를 만듭니다.

   1단계와 2단계는 네트워크 링크의 다른 끝을 종료하는 에지 스위치에 적절한 구성이 필요합니다. 에지 스위치 포트도 LACP 포트 채널로 집계되고 트렁크로 구성되어 필요한 모든 VLAN을 통과할 수 있도록 허용해야 합니다.

   호스트별 네트워킹 구성 체계에 대한 샘플 인터페이스 구성 파일이 제공됩니다.

관련 정보

예 /etc/sysconfig/network-scripts

호스트 스토리지를 구성합니다

각 호스트에 블록 스토리지 볼륨을 할당해야 합니다.

필요한 것

이 과제를 수행하는 데 필요한 정보를 제공하는 다음 주제를 검토했습니다.

요구사항을 충족해야 합니다

노드 컨테이너 마이그레이션 요구사항

이 작업에 대해

호스트에 블록 스토리지 볼륨(LUN)을 할당할 때는 "스토리지 요구 사항"의 표를 사용하여 다음 사항을 확인하십시오.

- 각 호스트에 필요한 볼륨 수(해당 호스트에 구축할 노드 수 및 유형 기준)
- 각 볼륨의 스토리지 범주(즉, 시스템 데이터 또는 오브젝트 데이터)
- 각 볼륨의 크기입니다

호스트에 StorageGRID 노드를 배포할 때 이 정보와 Linux가 각 물리적 볼륨에 할당한 영구 이름을 사용합니다.

> 이러한 볼륨을 파티션, 포맷 또는 마운트할 필요가 없습니다. 호스트가 볼 수 있도록 해야 합니다.

볼륨 이름 목록을 작성할 때 ""raw"" 특수 장치 파일("/dev/sdb" 등)을 사용하지 마십시오. 이러한 파일은 호스트의 재부팅 시 변경될 수 있으며, 이는 시스템의 올바른 작동에 영향을 줍니다. iSCSI LUN 및 장치 매퍼 다중 경로를 사용하는 경우, 특히 SAN 토폴로지에 공유 스토리지에 대한 중복 네트워크 경로가 포함된 경우 "/dev/mapper" 디렉토리에 다중 경로 별칭을 사용하는 것이 좋습니다. 또는 영구 디바이스 이름에 대해 '/dev/disk/by-path/' 아래에 있는 시스템 생성 소프트링크를 사용할 수 있습니다.

예를 들면 다음과 같습니다.

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

각 설치 환경에 따라 결과가 달라집니다.

각 블록 스토리지 볼륨에 알기 쉬운 이름을 할당하여 초기 StorageGRID 설치 및 향후 유지 관리 절차를 간소화하십시오. 공유 스토리지 볼륨에 대한 중복 액세스를 위해 장치 매퍼 다중 경로 드라이버를 사용하는 경우, '/etc/multipath.conf' 파일에서 "alias" 필드를 사용할 수 있습니다.

예를 들면 다음과 같습니다.

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

이렇게 하면 별칭이 호스트의 '/dev/mapper' 디렉토리에 블록 디바이스로 표시되므로 구성 또는 유지 관리 작업에서 블록 스토리지 볼륨을 지정해야 할 때마다 친숙하고 유효성이 검증된 이름을 지정할 수 있습니다.

> StorageGRID 노드 마이그레이션을 지원하고 장치 매퍼 다중 경로를 사용하도록 공유 스토리지를 설정하는 경우 모든 동일 위치에 있는 호스트에 공통 '/etc/multipath.conf'를 생성하고 설치할 수 있습니다. 각 호스트에서 다른 컨테이너 엔진 스토리지 볼륨을 사용해야 합니다. 별칭을 사용하고 각 컨테이너 엔진 스토리지 볼륨 LUN의 별칭에 타겟 호스트 이름을 포함시키면 기억하기 쉽고 권장됩니다.

관련 정보

컨테이너 엔진 저장소 볼륨을 구성합니다

컨테이너 엔진 저장소 볼륨을 구성합니다

컨테이너 엔진(Docker 또는 Podman)을 설치하기 전에 스토리지 볼륨을 포맷하고 마운트해야 할 수 있습니다.

이 작업에 대해

Docker 또는 Podman 스토리지 볼륨에 로컬 스토리지를 사용할 계획이고 Docker용 '/var/lib/docker'와 Podman용 '/var/lib/containers'가 포함된 호스트 파티션에 충분한 공간이 있는 경우 이 단계를 건너뛸 수 있습니다.

> Podman은 Red Hat Enterprise Linux(RHEL)에서만 지원됩니다.

단계

1. 컨테이너 엔진 스토리지 볼륨에 파일 시스템을 생성합니다.

```
sudo mkfs.ext4 container-engine-storage-volume-device
```

2. 컨테이너 엔진 저장소 볼륨을 마운트합니다.
   - Docker의 경우:

```
sudo mkdir -p /var/lib/docker
sudo mount container-storage-volume-device /var/lib/docker
```

   - Podman의 경우:

```
sudo mkdir -p /var/lib/containers
sudo mount container-storage-volume-device /var/lib/containers
```

3. /etc/fstab에 container-storage-volume-device에 대한 항목을 추가합니다.

   이 단계를 수행하면 호스트가 재부팅된 후 스토리지 볼륨이 자동으로 다시 마운트됩니다.

Docker를 설치합니다

StorageGRID 시스템은 Red Hat Enterprise Linux 또는 CentOS에서 컨테이너 모음으로 실행됩니다. Docker 컨테이너 엔진을 사용하도록 선택한 경우 다음 단계에 따라 Docker를 설치합니다. 그렇지 않으면 Podman을 설치합니다.

단계

1. Linux 배포에 대한 지침에 따라 Docker를 설치합니다.

> Docker가 Linux 배포판에 포함되어 있지 않은 경우 Docker 웹 사이트에서 다운로드할 수 있습니다.

2. 다음 두 명령을 실행하여 Docker를 활성화하고 시작했는지 확인합니다.

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. 다음을 입력하여 예상 버전의 Docker를 설치했는지 확인합니다.

```
sudo docker version
```

클라이언트 및 서버 버전은 1.11.0 이상이어야 합니다.

Podman을 설치합니다

StorageGRID 시스템은 Red Hat Enterprise Linux에서 컨테이너 모음으로 실행됩니다. Podman 컨테이너 엔진을 사용하도록 선택한 경우 다음 단계에 따라 Podman을 설치합니다. 그렇지 않으면 Docker를 설치합니다.

> Podman은 Red Hat Enterprise Linux(RHEL)에서만 지원됩니다.

단계

1. Linux 배포에 대한 지침에 따라 Podman 및 Podman-Docker를 설치합니다.

> Podman을 설치할 때 Podman-docker 패키지도 설치해야 합니다.

2. 다음을 입력하여 예상 버전의 Podman 및 Podman-Docker를 설치했는지 확인합니다.

```
sudo docker version
```

> Podman-Docker 패키지를 사용하면 Docker 명령을 사용할 수 있습니다.

클라이언트 및 서버 버전은 3.2.3 이상이어야 합니다.

```
Version: 3.2.3
API Version: 3.2.3
Go Version: go1.15.7
Built: Tue Jul 27 03:29:39 2021
OS/Arch: linux/amd64
```

StorageGRID 호스트 서비스를 설치합니다

StorageGRID RPM 패키지를 사용하여 StorageGRID 호스트 서비스를 설치합니다.

이 작업에 대해

다음 지침은 RPM 패키지에서 호스트 서비스를 설치하는 방법을 설명합니다. 또는 설치 아카이브에 포함된 Yum 리포지토리 메타데이터를 사용하여 RPM 패키지를 원격으로 설치할 수 있습니다. Linux 운영 체제에 대한 Yum 리포지토리 지침을 참조하십시오.

단계

1. 각 호스트에 StorageGRID RPM 패키지를 복사하거나 공유 스토리지에서 사용할 수 있도록 합니다.

   예를 들어, 다음 단계에서 예제 명령을 사용할 수 있도록 이 명령을 `/tmp' 디렉토리에 배치합니다.

2. 각 호스트에 루트로 로그인하거나 sudo 권한이 있는 계정을 사용하여 다음 명령을 지정된 순서대로 실행합니다.

```
sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-
version-SHA.rpm
```

```
sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-
version-SHA.rpm
```

   먼저 이미지 패키지를 설치하고 서비스 패키지를 다시 설치해야 합니다.

   패키지를 '/tmp' 이외의 디렉토리에 배치한 경우 사용한 경로를 반영하도록 명령을 수정합니다.

가상 그리드 노드 배포(Red Hat 또는 CentOS)

Red Hat Enterprise Linux 또는 CentOS 배포용 노드 구성 파일을 생성합니다

노드 구성 파일은 StorageGRID 호스트 서비스에서 노드를 시작하고 적절한 네트워크 및 블록 스토리지 리소스에 연결하는 데 필요한 정보를 제공하는 작은 텍스트 파일입니다. 노드 구성 파일은 가상 노드에 사용되며 어플라이언스 노드에는 사용되지 않습니다.

노드 구성 파일은 어디에 배치합니까?

노드가 실행될 호스트의 '/etc/StorageGrid/nodes' 디렉토리에 각 StorageGRID 노드의 구성 파일을 배치해야 합니다. 예를 들어 HostA에서 관리 노드 1개, 게이트웨이 노드 1개 및 스토리지 노드 1개를 실행하려는 경우 HostA의 '/etc/StorageGrid//nodes'에 노드 구성 파일 3개를 배치해야 합니다. vim 또는 nano와 같은 텍스트 편집기를 사용하여 각 호스트에서 직접 구성 파일을 만들거나 다른 곳에서 구성 파일을 만들어 각 호스트로 이동할 수 있습니다.

노드 구성 파일의 이름은 무엇입니까?

구성 파일의 이름이 중요합니다. node-name.conf 형식이며, 여기서 node-name은 노드에 할당하는 이름입니다. 이 이름은 StorageGRID Installer에 나타나며 노드 마이그레이션과 같은 노드 유지 관리 작업에 사용됩니다.

노드 이름은 다음 규칙을 따라야 합니다.

- 고유해야 합니다
- 문자로 시작해야 합니다
- A ~ Z 및 a ~ z 문자를 포함할 수 있습니다
- 0에서 9 사이의 숫자를 포함할 수 있습니다
- 하나 이상의 하이픈(-)을 포함할 수 있습니다.

- '.conf' 확장자는 포함되지 않고 32자 이하여야 합니다

이러한 명명 규칙을 따르지 않는 '/etc/StorageGrid/nodes'의 파일은 호스트 서비스에서 구문 분석되지 않습니다.

그리드에 대해 멀티 사이트 토폴로지를 계획한 경우 일반적인 노드 명명 규칙은 다음과 같습니다.

```
site-nodetype-nodenumber.conf
```

예를 들어 데이터 센터 1의 첫 번째 관리 노드에 dC1-adm1.conf를 사용하고 데이터 센터 2의 세 번째 스토리지 노드에 대해 dC2-SN3.conf를 사용할 수 있습니다. 그러나 모든 노드 이름이 명명 규칙을 따른다 하더라도 원하는 스키마를 사용할 수 있습니다.

노드 구성 파일이란 무엇입니까?

구성 파일에는 키/값 쌍이 포함되어 있으며, 한 줄에 하나의 키와 하나의 값이 있습니다. 각 키/값 쌍에 대해 다음 규칙을 따라야 합니다.

- 키와 값은 등호('=')와 선택적 공백으로 구분해야 합니다.
- 키에는 공백이 포함될 수 없습니다.
- 값에는 포함된 공백이 포함될 수 있습니다.
- 선행 또는 후행 공백은 무시됩니다.

일부 키는 모든 노드에 대해 필요하지만, 일부 키는 선택 사양이거나 특정 노드 유형에만 필요합니다.

이 표는 지원되는 모든 키에 대해 허용되는 값을 정의합니다. 가운데 열:

- R *: 필수 + BP: 모범 사례 + O: 선택 사항

키	**R, BP** 또는 **O?**	값
관리_IP	BP	이 노드가 속한 그리드에 대한 운영 관리 노드의 Grid Network IPv4 주소입니다. node_type=VM_Admin_Node 및 admin_role=Primary를 사용하는 그리드 노드에 대해 GRID_NETWORK_IP에 지정한 것과 동일한 값을 사용합니다. 이 매개 변수를 생략하면 노드가 mDNS를 사용하여 기본 관리 노드를 검색합니다. 그리드 노드가 기본 관리자 노드를 검색하는 방법 • 참고 *: 이 값은 기본 관리 노드에서 무시되고 금지될 수 있습니다.
관리 네트워크 구성	o	DHCP, 정적 또는 비활성
관리_네트워크_ESL	o	쉼표로 구분된 서브넷 목록으로, 이 노드가 Admin Network 게이트웨이를 통해 통신해야 하는 CIDR 표기법을 사용합니다. 예: 172.16.0.0/21,172.17.0.0/21

키	**R, BP** 또는 **O?**	값
Admin_network_Gateway를 선택합니다	O(* R *)	이 노드에 대한 로컬 관리 네트워크 게이트웨이의 IPv4 주소입니다. admin_network_ip 및 admin_network_mask에 의해 정의된 서브넷에 있어야 합니다. DHCP 구성 네트워크에서는 이 값이 무시됩니다. • 참고 *: admin_network_ESL이 지정된 경우 이 매개 변수가 필요합니다. 예: 1.1.1.1 10.224.4.81
admin_network_ip을 선택합니다	o	관리 네트워크에서 이 노드의 IPv4 주소입니다. 이 키는 admin_network_Config = static인 경우에만 필요합니다. 다른 값에 대해서는 지정하지 마십시오. 예: 1.1.1.1 10.224.4.81
admin_network_MAC입니다	o	컨테이너의 관리 네트워크 인터페이스에 대한 MAC 주소입니다. 이 필드는 선택 사항입니다. 생략할 경우 MAC 주소가 자동으로 생성됩니다. 콜론으로 구분된 6쌍의 16진수 숫자이어야 합니다. 예: 'B2:9c:02:C2:27:10'
admin_network_mask를 선택합니다	o	이 노드의 IPv4 넷마스크는 관리자 네트워크에서 설정합니다. 이 키는 admin_network_Config = static인 경우에만 필요합니다. 다른 값에 대해서는 지정하지 마십시오. 예: 255.255.255.0 255.255.248.0

키	**R, BP** 또는 **O?**	값
admin_network_mtu	o	Admin Network의 이 노드에 대한 MTU(Maximum Transmission Unit)입니다. admin_network_Config = DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 이 인수를 생략하면 1500이 사용됩니다. 점보 프레임을 사용하려면 MTU를 9000과 같은 점보 프레임에 적합한 값으로 설정합니다. 그렇지 않으면 기본값을 유지합니다. • 중요 *: 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다. 예: 1500입니다 8192
admin_network_target 을 선택합니다	BP	StorageGRID 노드에서 관리자 네트워크 액세스에 사용할 호스트 디바이스의 이름입니다. 네트워크 인터페이스 이름만 지원됩니다. 일반적으로 GRID_NETWORK_TARGET 또는 CLIENT_NETWORK_TARGET에 지정된 것과 다른 인터페이스 이름을 사용합니다. • 참고 *: 네트워크 대상으로 연결 또는 브리지 장치를 사용하지 마십시오. 연결 디바이스 위에 VLAN(또는 기타 가상 인터페이스)을 구성하거나 브리지 및 가상 이더넷(veth) 쌍을 사용합니다. • 모범 사례 *: 이 노드에 처음에 관리 네트워크 IP 주소가 없을 경우에도 값을 지정하십시오. 그런 다음 나중에 호스트에서 노드를 다시 구성하지 않고도 관리 네트워크 IP 주소를 추가할 수 있습니다. 예: 속박 0.1002 펜스256
admin_network_target_type입니다	o	인터페이스 (지원되는 유일한 값입니다.)

키	**R, BP** 또는 **O?**	값
admin_network_target_type_interface_clone_MAC	BP	참 또는 거짓 StorageGRID 컨테이너가 관리자 네트워크에서 호스트 호스트 대상 인터페이스의 MAC 주소를 사용하도록 하려면 키를 "true"로 설정합니다. • 모범 사례: * promiscuous 모드가 필요한 네트워크에서는 admin_network_target_type_interface_clone_MAC 키를 대신 사용합니다. MAC 클로닝에 대한 자세한 내용: MAC 주소 복제에 대한 고려 사항 및 권장 사항(Red Hat Enterprise Linux 또는 CentOS) MAC 주소 복제에 대한 고려 사항 및 권장 사항(Ubuntu 또는 Debian)
admin_role을 선택합니다	• R *	Primary 또는 Non-Primary입니다 이 키는 node_type = VM_Admin_Node인 경우에만 필요하며 다른 노드 유형에 대해서는 지정하지 마십시오.
Block_device_audit_logs	• R *	이 노드가 감사 로그의 영구 저장에 사용할 블록 디바이스 특수 파일의 경로 및 이름입니다. 이 키는 node_type=vm_Admin_Node인 노드에만 필요하며 다른 노드 유형에 대해서는 지정하지 마십시오. 예: '/dev/disk/by-path/PCI-0000:03:00.0 - SCSI-0:0:0:0:0:0' '/dev/disk/by-id/WWN-0x600a09800059d6df000060d757b475fd' '/dev/mapper/SGWs-adm1-audit-logs'

키	R, BP 또는 O?	값
Block_device_RANGEDB_000 BLOCK_DEVICE_RANGEDB_001 Block_device_RANGEDB_002 Block_device_RANGEDB_003 Block_device_RANGEDB_004 BLOCK_DEVICE_RANGEDB_005 BLOCK_DEVICE_RANGEDB_006 BLOCK_DEVICE_RANGEDB_007 Block_device_RANGEDB_008 Block_device_RANGEDB_009 BLOCK_DEVICE_RANGEDB_010 BLOCK_DEVICE_RANGEDB_011 BLOCK_DEVICE_RANGEDB_012 BLOCK_DEVICE_RANGEDB_013 BLOCK_DEVICE_RANGEDB_014 Block_device_RANGEDB_015	• R *	이 노드가 영구 오브젝트 스토리지에 사용할 블록 디바이스 특수 파일의 경로 및 이름입니다. 이 키는 node_type=vm_Storage_Node인 노드에만 필요하며 다른 노드 유형에 대해서는 지정하지 마십시오. block_device_RANGEDB_000 만 필요하며 나머지는 선택 사항입니다. block_device_RANGEDB_000 에 지정된 블록 디바이스는 4TB 이상이어야 하며 다른 블록 디바이스는 더 작을 수 있습니다. 간격을 두지 마십시오. BLOCK_DEVICE_RANGEDB_005를 지정하는 경우 BLOCK_DEVICE_RANGEDB_004도 지정해야 합니다. • 참고 *: 기존 배포와의 호환성을 위해 업그레이드된 노드에 대해 2자리 키가 지원됩니다. 예: '/dev/disk/by-path/PCI-0000:03:00.0 - SCSI-0:0:0:0:0:0' '/dev/disk/by-id/WWN-0x600a09800059d6df000060d757b475fd' '/dev/mapper/SGWs-sn1-rangedb-000'

키	**R, BP** 또는 **O?**	값
BLOCK_DEVICE_Tables	• R *	이 노드가 데이터베이스 테이블의 영구 저장에 사용할 블록 디바이스 특수 파일의 경로 및 이름입니다. 이 키는 node_type=vm_Admin_Node인 노드에만 필요하며 다른 노드 유형에 대해서는 지정하지 마십시오. 예: '/dev/disk/by-path/PCI-0000:03:00.0 - SCSI-0:0:0:0:0:0' '/dev/disk/by-id/WWN-0x600a09800059d6df000060d757b475fd' '/dev/mapper/SGWs-adm1-tables'
BLOCK_DEVICE_VAR_LOCAL	• R *	이 노드가 해당 /var/local 영구 스토리지에 사용할 블록 디바이스 특수 파일의 경로 및 이름입니다. 예: '/dev/disk/by-path/PCI-0000:03:00.0 - SCSI-0:0:0:0:0:0' '/dev/disk/by-id/WWN-0x600a09800059d6df000060d757b475fd' '/dev/mapper/SGWS-sn1-var-local'
client_network_Config	o	DHCP, 정적 또는 비활성
CLIENT_NETWORK_GATEWAY	o	client_network_ip 및 client_network_mask에 의해 정의된 서브넷에 있어야 하는 이 노드에 대한 로컬 클라이언트 네트워크 게이트웨이의 IPv4 주소입니다. DHCP 구성 네트워크에서는 이 값이 무시됩니다. 예: 1.1.1.1 10.224.4.81
client_network_ip	o	클라이언트 네트워크에서 이 노드의 IPv4 주소입니다. 이 키는 client_network_Config = static 일 때만 필요합니다. 다른 값에 대해서는 지정하지 마십시오. 예: 1.1.1.1 10.224.4.81

키	**R, BP** 또는 **O?**	값
client_network_MAC	o	컨테이너에 있는 클라이언트 네트워크 인터페이스의 MAC 주소입니다. 이 필드는 선택 사항입니다. 생략할 경우 MAC 주소가 자동으로 생성됩니다. 콜론으로 구분된 6쌍의 16진수 숫자이어야 합니다. 예: 'B2:9c:02:C2:27:20
client_network_mask.(클라이언트 네트워크 마스크	o	클라이언트 네트워크의 이 노드에 대한 IPv4 넷마스크입니다. 이 키는 client_network_Config = static 일 때만 필요합니다. 다른 값에 대해서는 지정하지 마십시오. 예: 255.255.255.0 255.255.248.0
client_network_mtu	o	Client Network의 이 노드에 대한 MTU(Maximum Transmission Unit)입니다. client_network_Config = DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 이 인수를 생략하면 1500이 사용됩니다. 점보 프레임을 사용하려면 MTU를 9000과 같은 점보 프레임에 적합한 값으로 설정합니다. 그렇지 않으면 기본값을 유지합니다. • 중요 *: 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다. 예: 1500입니다 8192

키	**R, BP 또는 O?**	값
client_network_target 을 선택합니다	BP	StorageGRID 노드에서 클라이언트 네트워크 액세스에 사용할 호스트 디바이스의 이름입니다. 네트워크 인터페이스 이름만 지원됩니다. 일반적으로 GRID_NETWORK_TARGET 또는 ADMIN_NETWORK_TARGET에 지정된 것과 다른 인터페이스 이름을 사용합니다. • 참고 *: 네트워크 대상으로 연결 또는 브리지 장치를 사용하지 마십시오. 연결 디바이스 위에 VLAN(또는 기타 가상 인터페이스)을 구성하거나 브리지 및 가상 이더넷(veth) 쌍을 사용합니다. • 모범 사례: * 이 노드에 클라이언트 네트워크 IP 주소가 없을 경우에도 값을 지정하십시오. 그런 다음 나중에 호스트에서 노드를 다시 구성하지 않고도 클라이언트 네트워크 IP 주소를 추가할 수 있습니다. 예: 속박 0.1003 엔스423
CLIENT_NETWORK_TARGET_TYPE	o	인터페이스 (이 값은 지원되는 값일 뿐입니다.)
client_network_target_type_interface_clone_MAC	BP	참 또는 거짓 StorageGRID 컨테이너가 클라이언트 네트워크의 호스트 대상 인터페이스의 MAC 주소를 사용하도록 하려면 키를 "true"로 설정합니다. • 모범 사례: * promiscuous 모드가 필요한 네트워크에서는 대신 client_network_target_type_interface_clone_mac 키를 사용합니다. MAC 클로닝에 대한 자세한 내용: MAC 주소 복제에 대한 고려 사항 및 권장 사항(Red Hat Enterprise Linux 또는 CentOS) MAC 주소 복제에 대한 고려 사항 및 권장 사항(Ubuntu 또는 Debian)
GRID_NETWORK_CONFIG(그리드 네트워크 구성	BP	고정 또는 DHCP (지정되지 않은 경우 기본값은 static)

키	**R, BP** 또는 **O?**	값
GRID_NETWORK_Gateway 를 참조하십시오	• R *	GRID_NETWORK_IP 및 GRID_NETWORK_MASK로 정의된 서브넷에 있어야 하는 이 노드에 대한 로컬 Grid Network 게이트웨이의 IPv4 주소입니다. DHCP 구성 네트워크에서는 이 값이 무시됩니다. 그리드 네트워크가 게이트웨이가 없는 단일 서브넷인 경우, 서브넷(X. Y.Z.1)의 표준 게이트웨이 주소 또는 이 노드의 GRID_NETWORK_IP 값을 사용합니다. 두 값 중 하나를 사용하면 미래의 그리드 네트워크 확장이 단순화됩니다.
GRID_NETWORK_IP입니다	• R *	Grid Network에서 이 노드의 IPv4 주소입니다. 이 키는 GRID_NETWORK_CONFIG = static 일 때만 필요합니다. 다른 값에 대해서는 지정하지 마십시오. 예: 1.1.1.1 10.224.4.81
GRID_NETWORK_MAC을 선택합니다	o	컨테이너의 그리드 네트워크 인터페이스에 대한 MAC 주소입니다. 이 필드는 선택 사항입니다. 생략할 경우 MAC 주소가 자동으로 생성됩니다. 콜론으로 구분된 6쌍의 16진수 숫자이어야 합니다. 예: 'B2:9c:02:C2:27:30
GRID_NETWORK_MASK 를 참조하십시오	o	그리드 네트워크에서 이 노드에 대한 IPv4 넷마스크입니다. 이 키는 GRID_NETWORK_CONFIG = static 일 때만 필요합니다. 다른 값에 대해서는 지정하지 마십시오. 예: 255.255.255.0 255.255.248.0

키	**R, BP** 또는 **O?**	값
GRID_NETWORK_MTU 를 참조하십시오	o	Grid Network의 이 노드에 대한 MTU(Maximum Transmission Unit)입니다. GRID_NETWORK_CONFIG=DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 이 인수를 생략하면 1500이 사용됩니다. 점보 프레임을 사용하려면 MTU를 9000과 같은 점보 프레임에 적합한 값으로 설정합니다. 그렇지 않으면 기본값을 유지합니다. • 중요 *: 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다. • 중요 *: 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다. 예: 1,500 8192
GRID_NETWORK_TARGET	• R *	StorageGRID 노드에서 그리드 네트워크 액세스에 사용할 호스트 디바이스의 이름입니다. 네트워크 인터페이스 이름만 지원됩니다. 일반적으로 admin_network_target 또는 client_network_target 에 지정된 것과 다른 인터페이스 이름을 사용합니다. • 참고 *: 네트워크 대상으로 연결 또는 브리지 장치를 사용하지 마십시오. 연결 디바이스 위에 VLAN(또는 기타 가상 인터페이스)을 구성하거나 브리지 및 가상 이더넷(veth) 쌍을 사용합니다. 예: 속박 0.1001 ens192
GRID_NETWORK_TARGET_TYPE	o	인터페이스 (지원되는 유일한 값입니다.)

키	**R, BP** 또는 **O?**	값
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	• BP *	참 또는 거짓 StorageGRID 컨테이너가 그리드 네트워크에서 호스트 대상 인터페이스의 MAC 주소를 사용하도록 키 값을 "true"로 설정합니다. • 모범 사례: * promiscuous 모드가 필요한 네트워크에서는 grid_network_target_type_interface_clone_mac 키를 대신 사용합니다. MAC 클로닝에 대한 자세한 내용: MAC 주소 복제에 대한 고려 사항 및 권장 사항(Red Hat Enterprise Linux 또는 CentOS) MAC 주소 복제에 대한 고려 사항 및 권장 사항(Ubuntu 또는 Debian)
Interfaces_target_nnnn	o	이 노드에 추가할 추가 인터페이스의 이름 및 선택적 설명입니다. 각 노드에 여러 개의 인터페이스를 추가할 수 있습니다. nnnn_의 경우 추가하려는 각 interface_target 항목에 대해 고유 번호를 지정하십시오. 값에 대해 베어 메탈 호스트의 물리적 인터페이스 이름을 지정합니다. 그런 다음 필요에 따라 쉼표를 추가하고 인터페이스에 대한 설명을 입력합니다. 이 설명은 VLAN 인터페이스 페이지와 HA 그룹 페이지에 표시됩니다. 예: 'interfaces_target_01=en256, Trunk' 트렁크 인터페이스를 추가하는 경우 StorageGRID에서 VLAN 인터페이스를 구성해야 합니다. 액세스 인터페이스를 추가할 경우 인터페이스를 HA 그룹에 직접 추가할 수 있으며, VLAN 인터페이스를 구성할 필요가 없습니다.

키	**R, BP 또는 O?**	값
최대 RAM	o	이 노드가 사용할 수 있는 최대 RAM 양입니다. 이 키를 생략하면 노드의 메모리 제한 사항이 없게 됩니다. 운영 레벨 노드에 대해 이 필드를 설정할 때 총 시스템 RAM보다 최소 24GB 및 16 ~ 32GB 적은 값을 지정합니다. • 참고 *: RAM 값은 노드의 실제 메타데이터 예약 공간에 영향을 줍니다. 를 참조하십시오 StorageGRID 관리 지침 메타데이터 예약된 공간에 대한 설명은 을 참조하십시오. 이 필드의 형식은 '<number><unit>'이며 여기서 '<unit>'는 'b', 'k', 'mb', 'g'가 될 수 있습니다. 예: 24g 38654705664b • 참고 *: 이 옵션을 사용하려면 메모리 cgroup에 대한 커널 지원을 활성화해야 합니다.
node_type입니다	• R *	노드 유형: VM_Admin_Node VM_Storage_Node VM_Archive_Node VM_API_Gateway
port_remap 을 참조하십시오	o	노드에서 내부 그리드 노드 통신 또는 외부 통신을 위해 사용하는 모든 포트를 다시 매핑합니다. "내부 그리드 노드 통신" 또는 "외부 통신"에서 설명한 대로 엔터프라이즈 네트워킹 정책이 StorageGRID에서 사용하는 하나 이상의 포트를 제한하는 경우 포트를 재매핑해야 합니다. • 중요 *: 로드 밸런서 엔드포인트를 구성하기 위해 사용하려는 포트를 다시 매핑하지 마십시오. • 참고 *: port_remap 만 설정된 경우 지정하는 매핑이 인바운드 및 아웃바운드 통신 모두에 사용됩니다. port_remap_inbound 도 지정된 경우 port_remap 은 아웃바운드 통신에만 적용됩니다. 사용되는 형식은 "<네트워크 유형>/<프로토콜>/<그리드 노드에 사용되는 기본 포트>/<새 포트>"입니다. 여기서 "<네트워크 유형>"은 그리드, 관리자 또는 클라이언트이고 프로토콜은 TCP 또는 UDP입니다. 예를 들면 다음과 같습니다. 'port_remap=client/tcp/18082/443'

키	R, BP 또는 O?	값
port_remap_inbound 를 참조하십시오	o	인바운드 통신을 지정된 포트에 다시 매핑합니다. port_remap_inbound 를 지정하지만 port_remap 의 값을 지정하지 않으면 포트의 아웃바운드 통신이 변경되지 않습니다. • 중요 *: 로드 밸런서 엔드포인트를 구성하기 위해 사용하려는 포트를 다시 매핑하지 마십시오. 사용되는 형식은 "<network type>/<protocol:>/<remapped port>/<default port used by grid node>"이며 여기서 "<network type>"은 그리드, 관리자 또는 클라이언트이고 프로토콜은 TCP 또는 UDP입니다. 예를 들면 다음과 같습니다. 'PORT_REmap_INbound=GRID/TCP/3022/22'

관련 정보

네트워킹 지침

그리드 노드가 기본 관리자 노드를 검색하는 방법

그리드 노드는 구성 및 관리를 위해 기본 관리 노드와 통신합니다. 각 그리드 노드는 그리드 네트워크에 있는 기본 관리 노드의 IP 주소를 알아야 합니다.

그리드 노드가 기본 관리 노드에 액세스할 수 있도록 노드를 배포할 때 다음 중 하나를 수행할 수 있습니다.

- admin_ip 매개 변수를 사용하여 기본 관리 노드의 IP 주소를 수동으로 입력할 수 있습니다.
- admin_ip 매개 변수를 생략하여 그리드 노드가 값을 자동으로 검색하도록 할 수 있습니다. 자동 검색은 그리드 네트워크가 DHCP를 사용하여 기본 관리 노드에 IP 주소를 할당할 때 특히 유용합니다.

운영 관리자 노드의 자동 검색은 멀티캐스트 도메인 이름 시스템(mDNS)을 사용하여 수행됩니다. 운영 관리 노드가 처음 시작되면 mDNS를 사용하여 해당 IP 주소를 게시합니다. 그런 다음 동일한 서브넷에 있는 다른 노드에서 IP 주소를 쿼리하고 자동으로 가져올 수 있습니다. 그러나 멀티캐스트 IP 트래픽은 일반적으로 서브넷 간에 라우팅할 수 없기 때문에 다른 서브넷의 노드는 기본 관리 노드의 IP 주소를 직접 획득할 수 없습니다.

> 자동 검색을 사용하는 경우:
>
> - 기본 관리 노드가 직접 연결되지 않은 서브넷에 있는 하나 이상의 그리드 노드에 대해 admin_IP 설정을 포함해야 합니다. 이 그리드 노드는 mDNS로 검색할 서브넷의 다른 노드에 대한 기본 관리 노드의 IP 주소를 게시합니다.
> - 네트워크 인프라스트럭처가 서브넷 내의 다중 캐스트 IP 트래픽 전달을 지원하는지 확인합니다.

노드 구성 파일의 예

예제 노드 구성 파일을 사용하여 StorageGRID 시스템의 노드 구성 파일을 설정할 수 있습니다. 이 예제에서는 모든 유형의 그리드 노드에 대한 노드 구성 파일을 보여 줍니다.

대부분의 노드의 경우 그리드 관리자 또는 설치 API를 사용하여 그리드를 구성할 때 관리 및 클라이언트 네트워크 주소 지정 정보(IP, 마스크, 게이트웨이 등)를 추가할 수 있습니다. 기본 관리 노드는 예외입니다. 그리드 네트워크가 라우팅되지 않는 등의 이유로 기본 관리 노드의 관리 네트워크 IP를 탐색하여 그리드 구성을 완료하려면 노드 구성 파일에서 기본 관리 노드에 대한 관리 네트워크 연결을 구성해야 합니다. 이 예제는 에 나와 있습니다.

> 이 예에서는 클라이언트 네트워크가 기본적으로 비활성화되어 있더라도 클라이언트 네트워크 타겟이 모범 사례로 구성되었습니다.

기본 관리자 노드의 예

- 파일 이름 예 *: `/etc/StorageGrid/nodes/dc1-adm1.conf'
- 파일 내용 예: *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

스토리지 노드의 예

- 파일 이름 예: * ``etc/StorageGrid/nodes/dc1-sn1.conf'
- 파일 내용 예: *

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

아카이브 노드의 예

- 파일 이름 예: * ``etc/StorageGrid/nodes/dc1-arc1.conf'
- 파일 내용 예: *

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

게이트웨이 노드의 예

- 파일 이름 예: * ``etc/StorageGrid/nodes/dc1-gw1.conf'
- 파일 내용 예: *

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

운영 관리자 노드가 아닌 노드의 예

- 파일 이름 예: * ``etc/StorageGrid/nodes/dc1-adm2.conf'
- 파일 내용 예: *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

StorageGRID 구성을 검증합니다

각 StorageGRID 노드에 대해 '/etc/StorageGrid/nodes'에서 구성 파일을 생성한 후 해당 파일의 내용을 확인해야 합니다.

구성 파일의 내용을 확인하려면 각 호스트에서 다음 명령을 실행합니다.

```
sudo storagegrid node validate all
```

파일이 올바른 경우, 예제에 표시된 대로 각 구성 파일에 대해 * Passed * 가 출력됩니다.

```
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
```

> 자동 설치의 경우 StorageGRID 명령(예: StorageGRID—quiet…)에서 '-q' 또는 '--quiet' 옵션을 사용하여 이 출력을 억제할 수 있습니다. 출력을 표시하지 않으면 구성 경고 또는 오류가 감지된 경우 명령에 0이 아닌 종료 값이 있는 것입니다.

구성 파일이 잘못된 경우, 이 예에서와 같이 문제가 * warning * 및 * error * 로 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 노드를 시작하고 호스트를 재부팅한 후 다시 시작하려면 StorageGRID 호스트 서비스를 설정하고 시작해야 합니다.

단계

1. 각 호스트에서 다음 명령을 실행합니다.

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. 다음 명령을 실행하여 구축이 진행되고 있는지 확인합니다.

```
sudo storagegrid node status node-name
```

"not-running" 또는 "scope" 상태를 반환하는 노드에 대해 다음 명령을 실행합니다.

```
sudo storagegrid node start node-name
```

3. 이전에 StorageGRID 호스트 서비스를 설정 및 시작한 경우(또는 서비스가 활성화 및 시작되었는지 확실하지 않은 경우) 다음 명령을 실행합니다.

```
sudo systemctl reload-or-restart storagegrid
```

그리드 및 전체 설치 구성(Red Hat 또는 CentOS)

그리드 관리자로 이동합니다

그리드 관리자를 사용하여 StorageGRID 시스템을 구성하는 데 필요한 모든 정보를 정의합니다.

필요한 것

기본 관리 노드를 구축하고 초기 시작 시퀀스를 완료해야 합니다.

단계

1. 웹 브라우저를 열고 다음 주소 중 하나로 이동합니다.

```
https://primary_admin_node_ip

client_network_ip
```

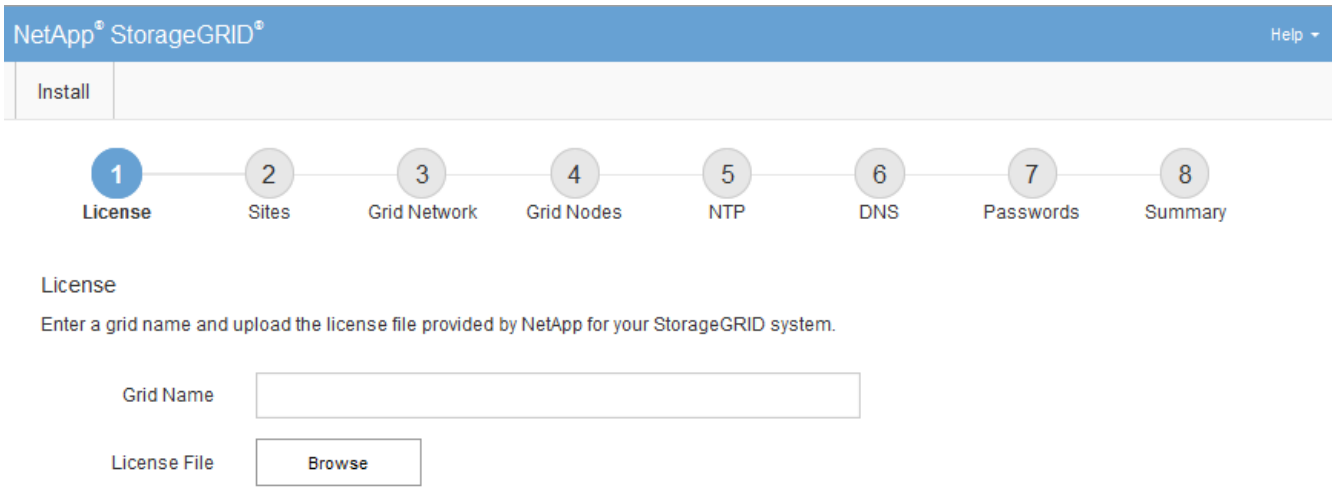
또는 포트 8443에서 그리드 관리자에 액세스할 수 있습니다.

```
https://primary_admin_node_ip:8443
```

> 네트워크 구성에 따라 그리드 네트워크 또는 관리 네트워크의 기본 관리 노드 IP에 대한 IP 주소를 사용할 수 있습니다.

1. StorageGRID 시스템 설치 * 를 클릭합니다.

   StorageGRID 시스템을 구성하는 데 사용되는 페이지가 나타납니다.



StorageGRID 라이센스 정보를 지정합니다

StorageGRID 시스템의 이름을 지정하고 NetApp에서 제공하는 라이센스 파일을 업로드해야 합니다.

단계

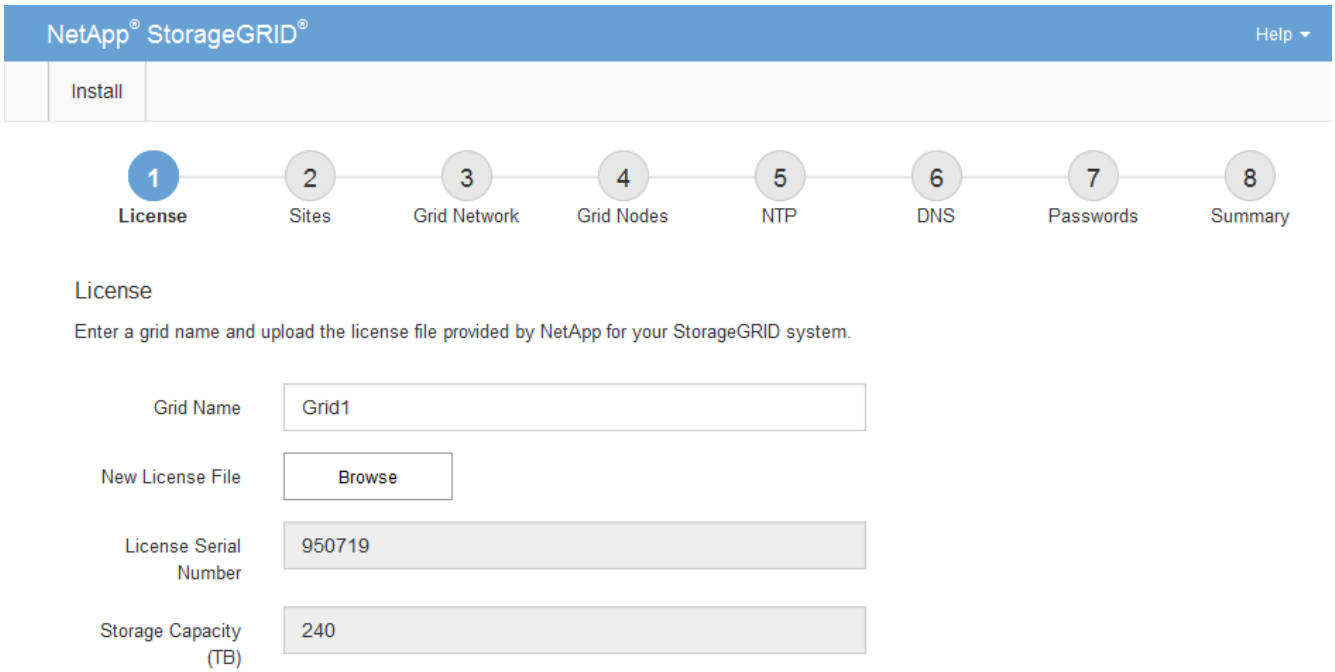
1. 라이센스 페이지의 * 그리드 이름 * 에 StorageGRID 시스템에 대한 의미 있는 이름을 입력합니다.

   설치 후, 이름이 Nodes 메뉴 맨 위에 표시됩니다.

2. 찾아보기 * 를 클릭하고 NetApp 라이센스 파일('NLFunique_id.txt')을 찾은 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.

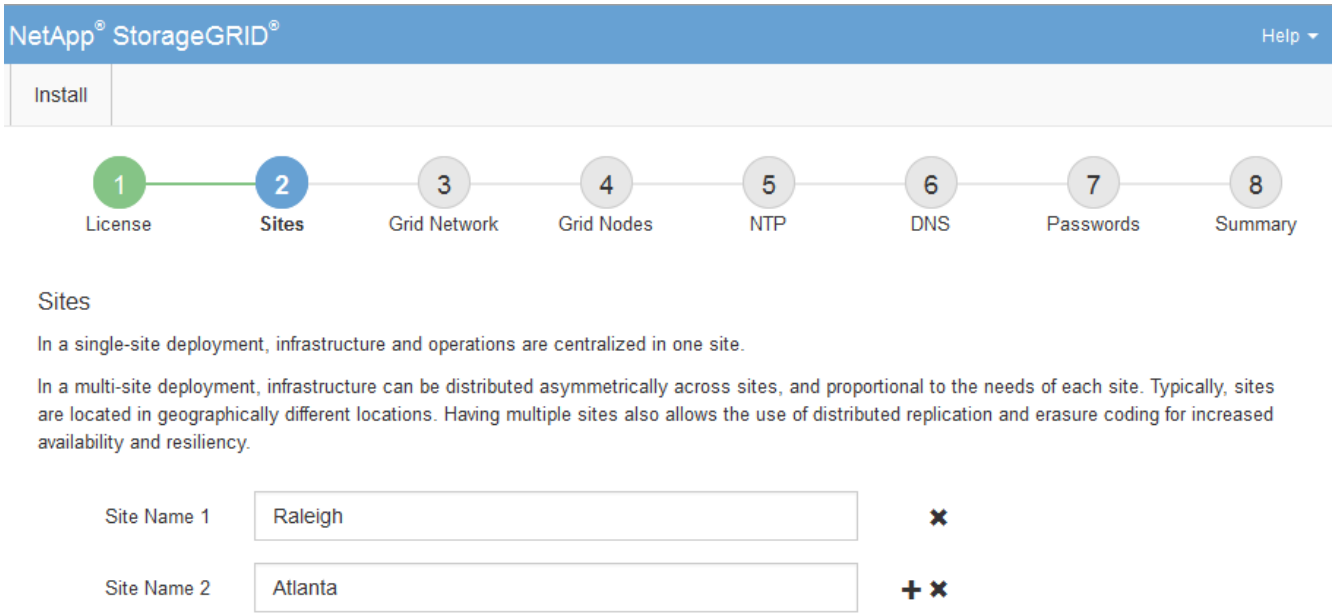
사이트를 추가합니다

StorageGRID를 설치할 때 사이트를 하나 이상 만들어야 합니다. StorageGRID 시스템의 안정성과 스토리지 용량을 늘리기 위해 사이트를 추가로 생성할 수 있습니다.

단계

1. 사이트 페이지에서 * 사이트 이름 * 을 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.

그리드 네트워크 서브넷을 지정합니다

그리드 네트워크에서 사용되는 서브넷을 지정해야 합니다.

이 작업에 대해

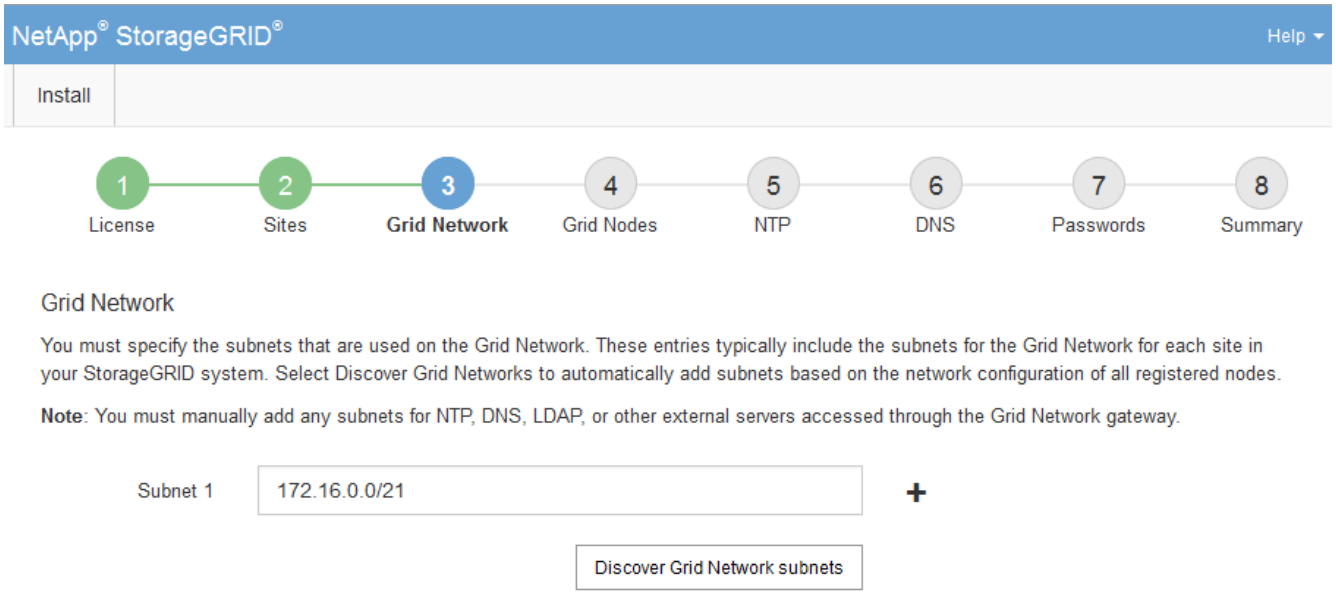
서브넷 항목에는 그리드 네트워크를 통해 연결할 수 있어야 하는 서브넷과 함께 StorageGRID 시스템의 각 사이트에 대한 그리드 네트워크의 서브넷이 포함됩니다.

그리드 서브넷이 여러 개인 경우 그리드 네트워크 게이트웨이가 필요합니다. 지정된 모든 그리드 서브넷은 이 게이트웨이를 통해 연결할 수 있어야 합니다.

단계

1. 서브넷 1 * 텍스트 상자에 하나 이상의 그리드 네트워크에 대한 CIDR 네트워크 주소를 지정합니다.
2. 마지막 항목 옆에 있는 더하기 기호를 클릭하여 추가 네트워크 항목을 추가합니다.

하나 이상의 노드를 이미 배포한 경우 * 그리드 네트워크 서브넷 검색 * 을 클릭하여 그리드 관리자에 등록된 그리드 노드에 의해 보고된 서브넷으로 그리드 네트워크 서브넷 목록을 자동으로 채웁니다.



3. 다음 * 을 클릭합니다.

보류 중인 그리드 노드를 승인합니다

StorageGRID 시스템에 가입하려면 각 그리드 노드를 승인해야 합니다.

필요한 것

모든 가상 및 StorageGRID 어플라이언스 그리드 노드를 구축했습니다.

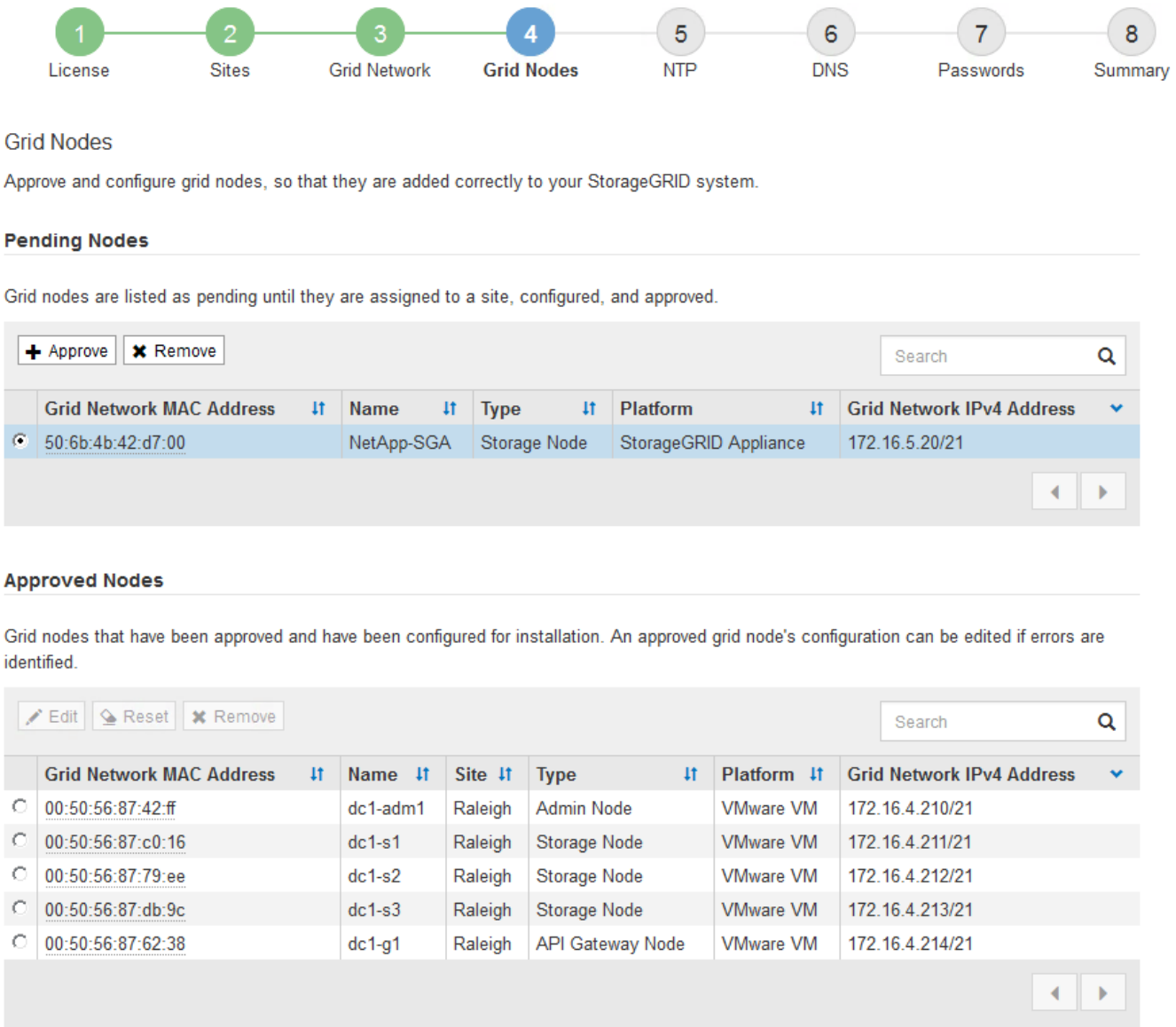
> 일부 노드를 나중에 설치하는 대신 모든 노드를 한 번 설치하는 것이 더 효율적입니다.

단계

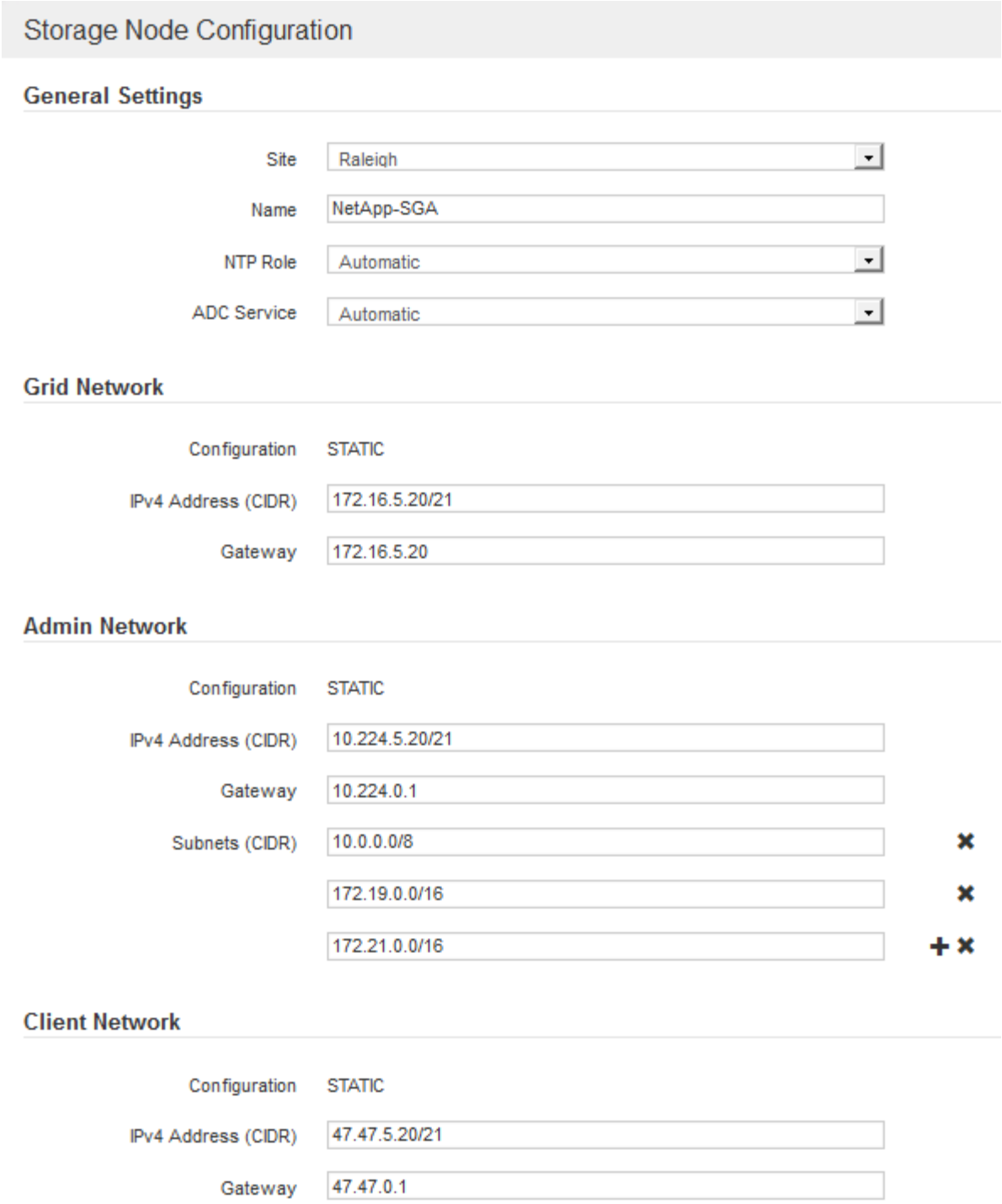
1. Pending Nodes(보류 중인 노드) 목록을 검토하고 배포된 모든 그리드 노드가 표시되는지 확인합니다.

   > 그리드 노드가 누락된 경우 성공적으로 배포되었는지 확인합니다.

2. 승인하려는 보류 중인 노드 옆에 있는 라디오 버튼을 선택합니다.



3. Approve * (승인 *)를 클릭합니다.
4. 일반 설정에서 필요에 따라 다음 속성의 설정을 수정합니다.



- * Site *: 이 그리드 노드가 연결될 사이트의 이름입니다.
- * 이름 *: 노드에 할당될 이름 및 그리드 관리자에 표시될 이름입니다. 기본적으로 노드를 구성할 때 지정한 이름이 지정됩니다. 설치 프로세스의 이 단계에서 필요에 따라 이름을 변경할 수 있습니다.

> 설치를 완료한 후에는 노드 이름을 변경할 수 없습니다.

> VMware 노드의 경우 여기에서 이름을 변경할 수 있지만 이 작업은 vSphere에서 가상 머신의 이름을 변경하지 않습니다.

- * NTP 역할 *: 그리드 노드의 NTP(Network Time Protocol) 역할입니다. 옵션은 * 자동 *, * 기본 * 및 * 클라이언트 * 입니다. Automatic * 을 선택하면 기본 역할이 관리 노드, ADC 서비스가 있는 스토리지 노드, 게이트웨이 노드 및 비정적 IP 주소가 있는 모든 그리드 노드에 할당됩니다. 다른 모든 그리드 노드에는 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 노드 전용): 시스템에서 노드가 관리 도메인 컨트롤러(ADC) 서비스를 필요로 하는지 여부를 결정하도록 하려면 * 자동 * 을 선택합니다. ADC 서비스는 그리드 서비스의 위치 및 가용성을 추적합니다. 각 사이트에 적어도 3개의 스토리지 노드가 ADC 서비스를 포함해야 합니다. ADC 서비스를 배포한 후에는 노드에 추가할 수 없습니다.

5. Grid Network에서 필요에 따라 다음 속성의 설정을 수정합니다.

   - * IPv4 주소(CIDR) *: 그리드 네트워크 인터페이스(컨테이너 내부의 eth0)의 CIDR 네트워크 주소입니다. 예: 192.168.1.234/21
   - * 게이트웨이 *: 그리드 네트워크 게이트웨이. 예: 192.168.0.1

     그리드 서브넷이 여러 개인 경우 게이트웨이가 필요합니다.

     > 그리드 네트워크 구성에 대해 DHCP를 선택하고 여기서 값을 변경하면 새 값이 노드의 정적 주소로 구성됩니다. 결과 IP 주소가 DHCP 주소 풀 내에 있지 않은지 확인해야 합니다.

6. 그리드 노드에 대해 관리자 네트워크를 구성하려면 필요에 따라 관리 네트워크 섹션에서 설정을 추가하거나 업데이트합니다.

   이 인터페이스에서 나오는 라우트의 대상 서브넷을 * 서브넷(CIDR) * 텍스트 상자에 입력합니다. 관리 서브넷이 여러 개인 경우 관리 게이트웨이가 필요합니다.

   > Admin Network 구성에 대해 DHCP를 선택하고 여기서 값을 변경하면 새 값이 노드의 정적 주소로 구성됩니다. 결과 IP 주소가 DHCP 주소 풀 내에 있지 않은지 확인해야 합니다.

   - 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. 어플라이언스 재부팅: 어플라이언스 설치 프로그램에서 * 고급 * > * 재부팅 * 을 선택합니다.

        재부팅하는 데 몇 분 정도 걸릴 수 있습니다.

     b. 네트워크 구성 * > * 링크 구성 * 을 선택하고 해당 네트워크를 활성화합니다.

     c. 네트워킹 구성 * > * IP 구성 * 을 선택하고 활성화된 네트워크를 구성합니다.

     d. 홈 페이지로 돌아가서 * 설치 시작 * 을 클릭합니다.

     e. Grid Manager(그리드 관리자): 노드가 Approved Nodes(승인된 노드) 테이블에 나열된 경우 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.

   클라이언트 네트워크 구성에 대해 DHCP를 선택하고 여기서 값을 변경하면 새 값이 노드의 정적 주소로 구성됩니다. 결과 IP 주소가 DHCP 주소 풀 내에 있지 않은지 확인해야 합니다.

   - 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. 어플라이언스 재부팅: 어플라이언스 설치 프로그램에서 * 고급 * > * 재부팅 * 을 선택합니다.

        재부팅하는 데 몇 분 정도 걸릴 수 있습니다.

     b. 네트워크 구성 * > * 링크 구성 * 을 선택하고 해당 네트워크를 활성화합니다.

     c. 네트워킹 구성 * > * IP 구성 * 을 선택하고 활성화된 네트워크를 구성합니다.

     d. 홈 페이지로 돌아가서 * 설치 시작 * 을 클릭합니다.

     e. Grid Manager(그리드 관리자): 노드가 Approved Nodes(승인된 노드) 테이블에 나열된 경우 노드를 재설정합니다.

     f. Pending Nodes 테이블에서 노드를 제거합니다.

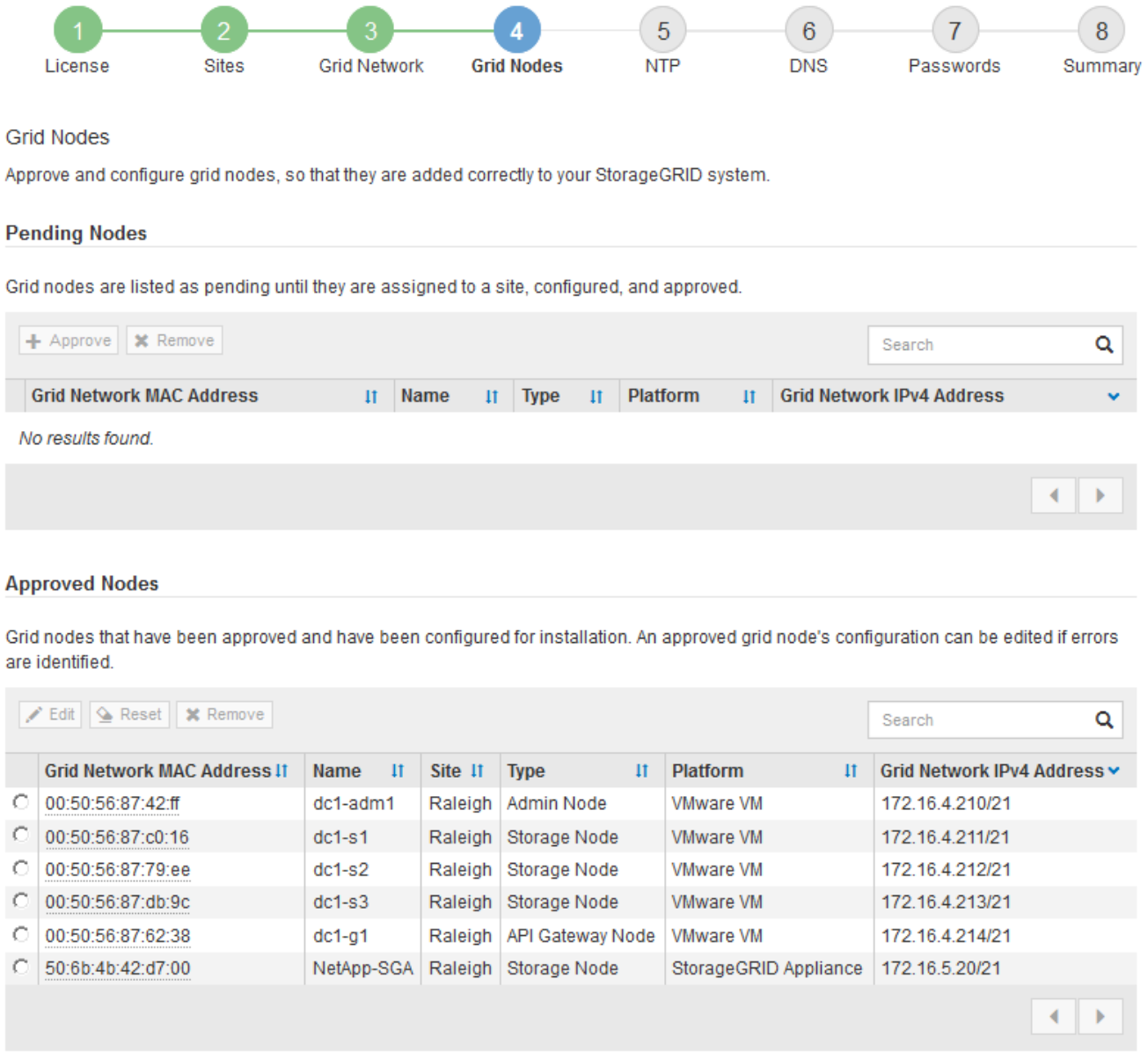
     g. 대기 중인 노드 목록에 노드가 다시 나타날 때까지 기다립니다.

     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. 승인하려는 보류 중인 각 그리드 노드에 대해 이 단계를 반복합니다.

   그리드에서 원하는 모든 노드를 승인해야 합니다. 그러나 요약 페이지에서 * 설치 * 를 클릭하기 전에 언제든지 이 페이지로 돌아갈 수 있습니다. 라디오 버튼을 선택하고 * Edit * 를 클릭하여 승인된 그리드 노드의 속성을 수정할 수 있습니다.

10. 그리드 노드 승인이 완료되면 * 다음 * 을 클릭합니다.

Network Time Protocol 서버 정보를 지정합니다

StorageGRID 시스템에 대해 NTP(네트워크 시간 프로토콜) 구성 정보를 지정해야 별도의 서버에서 수행되는 작업을 동기화할 수 있습니다.

이 작업에 대해

NTP 서버의 IPv4 주소를 지정해야 합니다.

외부 NTP 서버를 지정해야 합니다. 지정된 NTP 서버는 NTP 프로토콜을 사용해야 합니다.

시간 드리프트와 관련된 문제를 방지하려면 Stratum 3 이상의 NTP 서버 참조를 4개 지정해야 합니다.

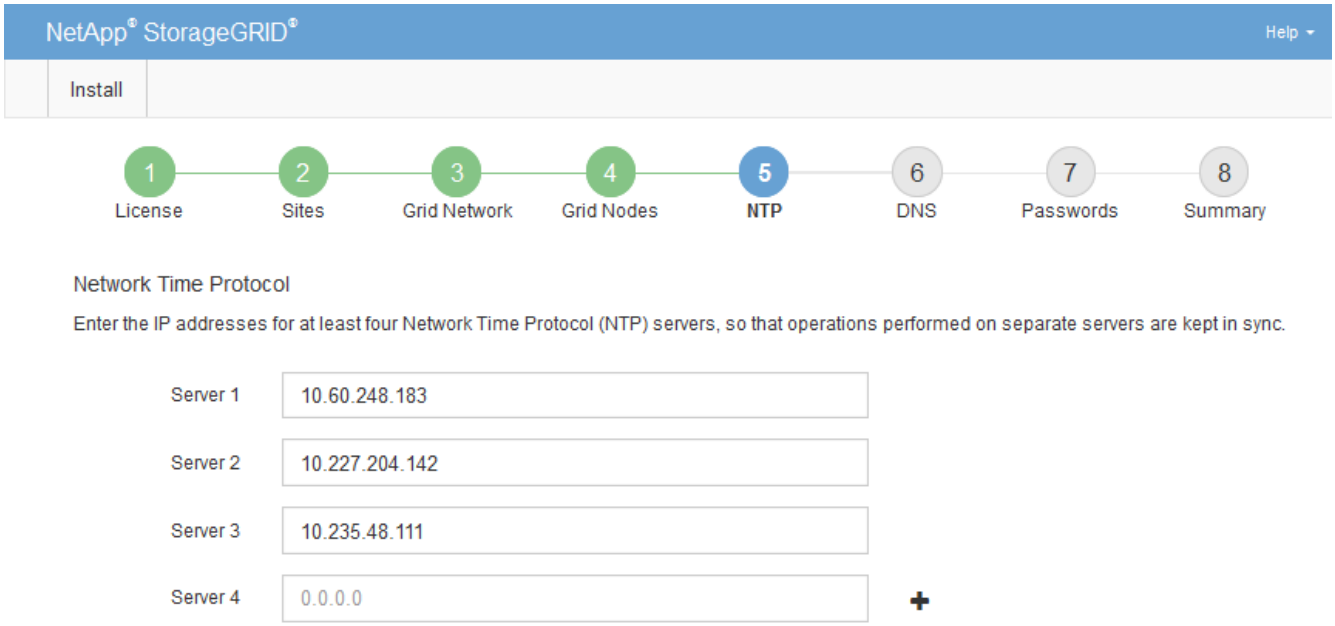
> 프로덕션 수준 StorageGRID 설치에 외부 NTP 소스를 지정할 때 Windows Server 2016 이전 버전의 Windows에서는 Windows 시간(W32Time) 서비스를 사용하지 마십시오. 이전 버전의 Windows의 시간 서비스는 정확하지 않으며 StorageGRID와 같은 고정밀 환경에서 사용하기 위해 Microsoft에서 지원되지 않습니다.
>
> "정확도가 높은 환경에 대한 Windows 시간 서비스를 구성하기 위한 경계를 지원합니다"

외부 NTP 서버는 이전에 기본 NTP 역할을 할당한 노드에서 사용됩니다.

> 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.

단계

1. Server 1 * 에서 * Server 4 * 텍스트 상자에 NTP 서버 4대 이상에 대한 IPv4 주소를 지정합니다.
2. 필요한 경우 마지막 항목 옆에 있는 더하기 기호를 선택하여 추가 서버 항목을 추가합니다.



3. 다음 * 을 선택합니다.

도메인 이름 시스템 서버 정보를 지정합니다

IP 주소 대신 호스트 이름을 사용하여 외부 서버에 액세스할 수 있도록 StorageGRID 시스템에 대한 DNS(도메인 이름 시스템) 정보를 지정해야 합니다.

이 작업에 대해

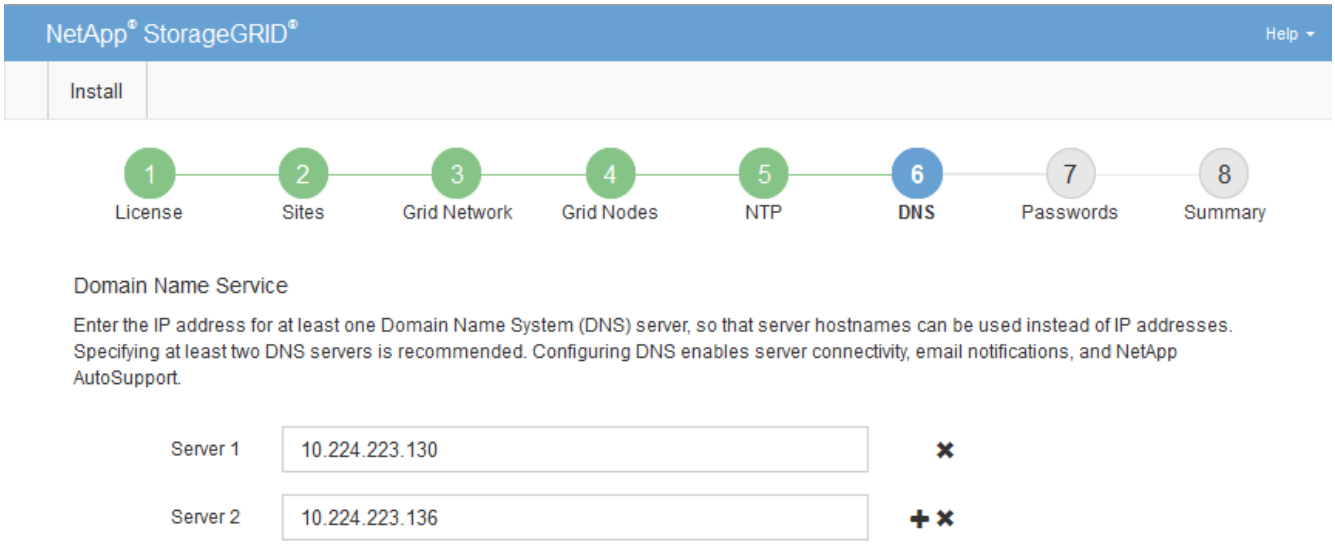
DNS 서버 정보를 지정하면 e-메일 알림 및 AutoSupport에 IP 주소 대신 FQDN(정규화된 도메인 이름) 호스트 이름을 사용할 수 있습니다. DNS 서버를 두 개 이상 지정하는 것이 좋습니다.

> DNS 서버에 2-6개의 IPv4 주소를 제공합니다. 네트워크 연결 시 각 사이트에서 로컬로 액세스할 수 있는 DNS 서버를 선택해야 합니다. 이는 Is착륙한 사이트가 계속해서 DNS 서비스에 액세스할 수 있도록 하기 위한 것입니다. 그리드 전체 DNS 서버 목록을 구성한 후 각 노드에 대해 DNS 서버 목록을 추가로 사용자 지정할 수 있습니다. 자세한 내용은 복구 및 유지 관리 지침 에서 DNS 구성 수정에 대한 정보를 참조하십시오.

DNS 서버 정보가 생략되거나 잘못 구성된 경우 각 그리드 노드의 SSM 서비스에서 NST 알람이 트리거됩니다. DNS가 올바르게 구성되고 새 서버 정보가 모든 그리드 노드에 도달하면 경보가 해제됩니다.

단계

1. Server 1 * 텍스트 상자에 하나 이상의 DNS 서버에 대한 IPv4 주소를 지정합니다.
2. 필요한 경우 마지막 항목 옆에 있는 더하기 기호를 선택하여 추가 서버 항목을 추가합니다.



   가장 좋은 방법은 DNS 서버를 두 개 이상 지정하는 것입니다. 최대 6개의 DNS 서버를 지정할 수 있습니다.

3. 다음 * 을 선택합니다.

StorageGRID 시스템 암호를 지정합니다

StorageGRID 시스템을 설치하는 과정에서 시스템 보안을 유지하고 유지 관리 작업을 수행하는 데 사용할 암호를 입력해야 합니다.

이 작업에 대해

암호 설치 페이지를 사용하여 프로비저닝 암호 및 그리드 관리 루트 사용자 암호를 지정합니다.

- 프로비저닝 암호는 암호화 키로 사용되며 StorageGRID 시스템에 저장되지 않습니다.
- 복구 패키지 다운로드를 포함하여 설치, 확장 및 유지 관리 절차를 위한 프로비저닝 암호가 있어야 합니다. 따라서 프로비저닝 암호를 안전한 위치에 저장하는 것이 중요합니다.
- 현재 프로비저닝 암호가 있는 경우 Grid Manager에서 프로비저닝 암호를 변경할 수 있습니다.
- 그리드 관리 루트 사용자 암호는 Grid Manager를 사용하여 변경할 수 있습니다.
- 임의로 생성된 명령줄 콘솔 및 SSH 암호는 복구 패키지의 Passwords.txt 파일에 저장됩니다.

단계

1. Provisioning Passphrase * 에서 StorageGRID 시스템의 그리드 토폴로지를 변경하는 데 필요한 프로비저닝 암호를 입력합니다.

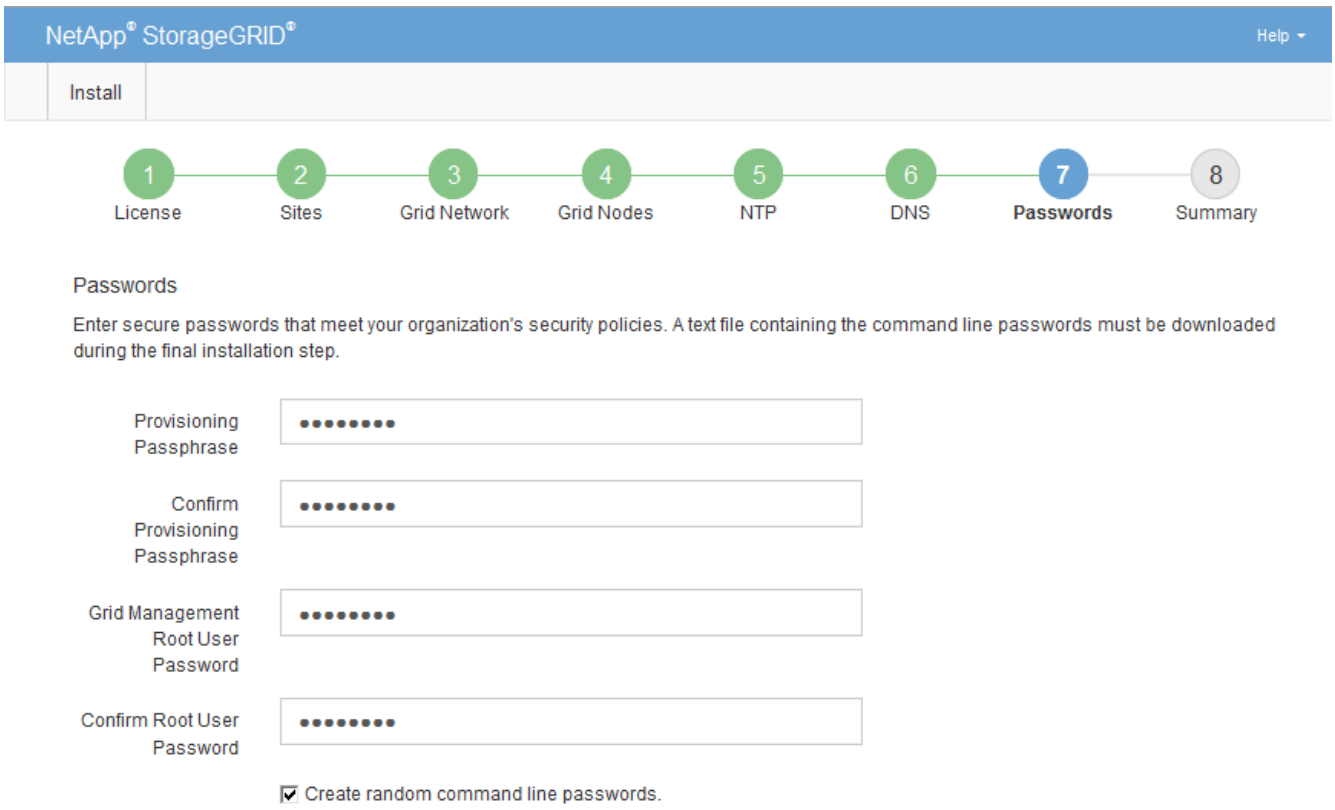
   프로비저닝 암호를 안전한 장소에 보관합니다.

   > 설치가 완료되고 나중에 프로비저닝 암호를 변경하려는 경우 Grid Manager를 사용할 수 있습니다. 구성 * > * 액세스 제어 * > * 그리드 비밀번호 * 를 선택합니다.

2. Provisioning Passphrase * 확인 에서 프로비저닝 암호를 다시 입력하여 확인합니다.
3. Grid Management Root User Password * 에서 Grid Manager에 ""root" 사용자로 액세스하는 데 사용할 암호를 입력합니다.

   암호를 안전한 곳에 보관하십시오.

4. 루트 사용자 암호 확인 * 에서 그리드 관리자 암호를 다시 입력하여 확인합니다.



5. 개념 증명이나 데모 목적으로 그리드를 설치하는 경우 * 임의의 명령줄 암호 만들기 * 확인란을 선택 취소합니다.

   프로덕션 배포의 경우 보안을 위해 항상 무작위 암호를 사용해야 합니다. ""root" 또는 ""admin" 계정을 사용하여 명령줄에서 그리드 노드에 액세스하기 위해 기본 암호를 사용하려는 경우 * 무작위 명령줄 암호 만들기 * 를 선택 취소합니다.

   > 요약 페이지에서 * Install * 을 클릭하면 복구 패키지 파일('s GW-recovery-package-id-revision.zip')을 다운로드하라는 메시지가 표시됩니다. 반드시 해야 합니다 이 파일을 다운로드합니다 를 눌러 설치를 완료합니다. 시스템에 액세스하는 데 필요한 암호는 복구 패키지 파일에 포함된 "passwords.txt" 파일에 저장됩니다.

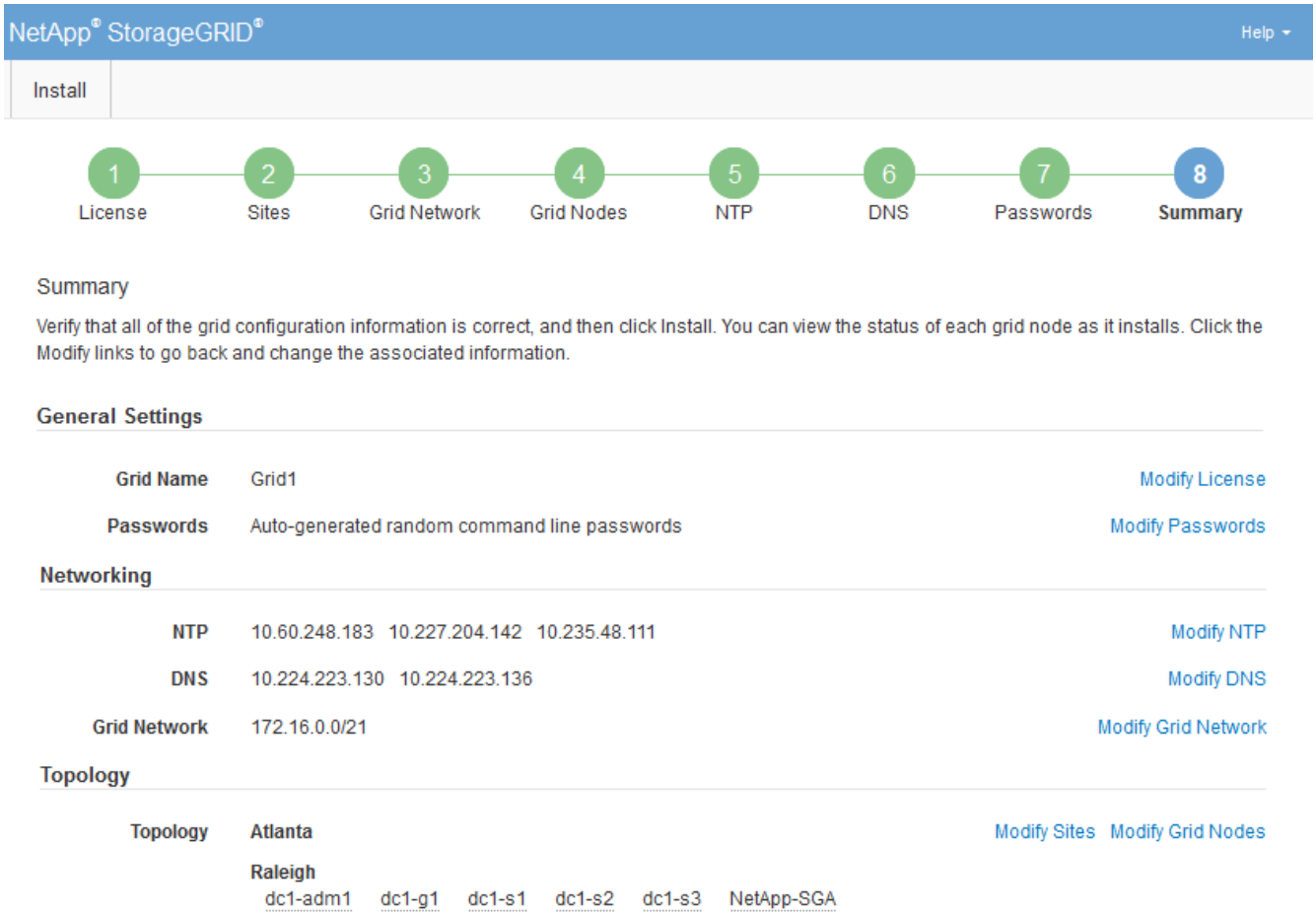
6. 다음 * 을 클릭합니다.

구성을 검토하고 설치를 완료합니다

설치를 성공적으로 완료하려면 입력한 구성 정보를 주의 깊게 검토해야 합니다.

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 끊어지면 액세스 가능한 서브넷을 통해 기본 관리 노드에 액세스하는지 확인해야 합니다. 을 참조하십시오 네트워킹 지침 를 참조하십시오.

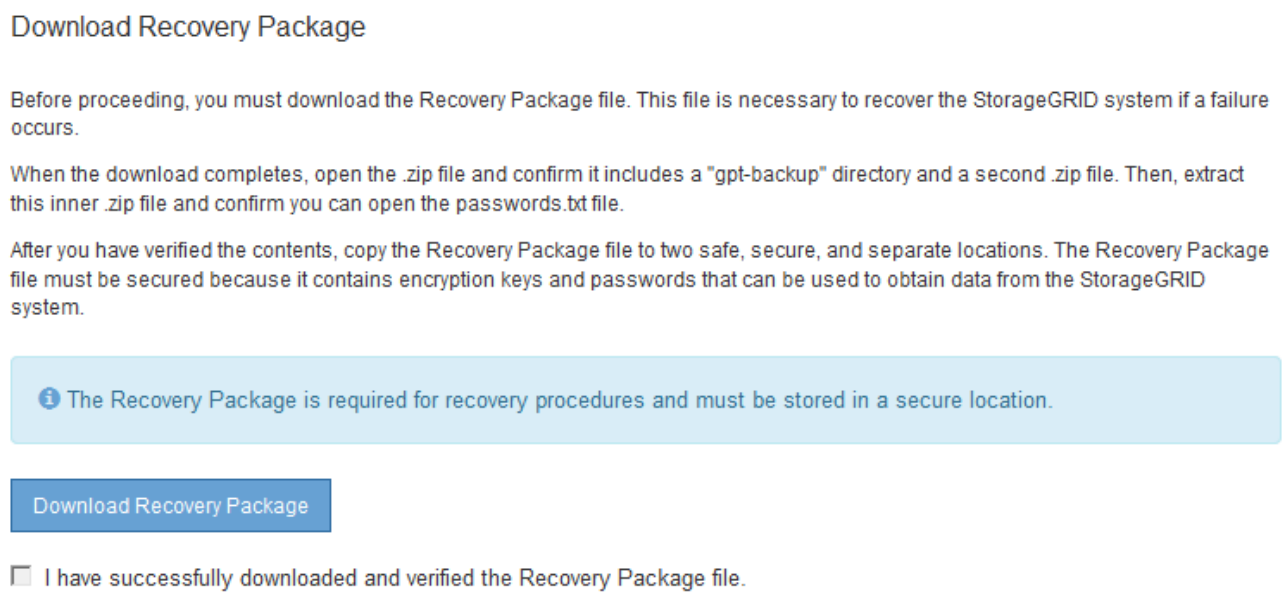
4. 복구 패키지 다운로드 * 를 클릭합니다.

   설치가 GRID 토폴로지를 정의한 지점으로 진행되면 복구 패키지 파일(".zip")을 다운로드하라는 메시지가 표시되고 이 파일의 내용에 액세스할 수 있는지 확인합니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 다운로드해야 합니다. 설치가 백그라운드에서 계속되지만 이 파일을 다운로드하여 확인하기 전에는 설치를 완료하고 StorageGRID 시스템에 액세스할 수 없습니다.

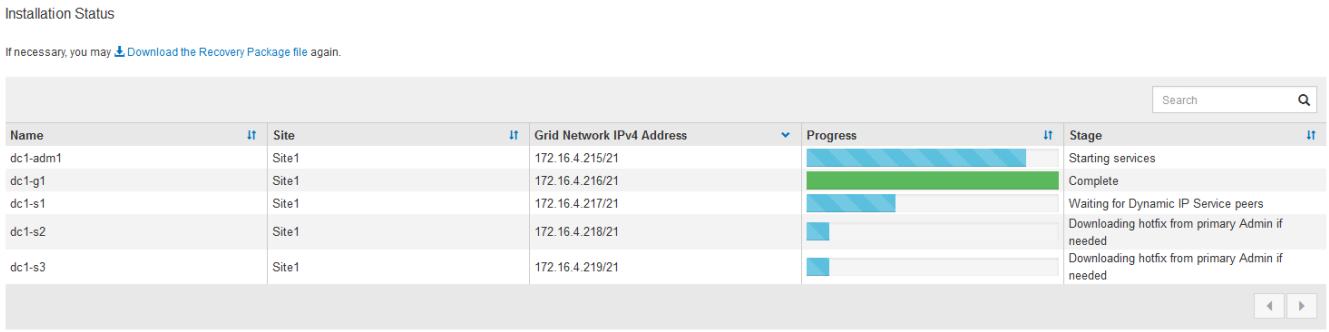
5. '.zip' 파일의 내용을 추출하여 안전한 별도의 두 위치에 저장할 수 있는지 확인합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

6. 복구 패키지 파일을 성공적으로 다운로드하고 확인했습니다. * 확인란을 선택하고 * 다음 * 을 클릭합니다.



설치가 진행 중인 경우 상태 페이지가 나타납니다. 이 페이지에는 각 그리드 노드의 설치 진행률이 표시됩니다.



모든 그리드 노드에 대해 전체 단계에 도달하면 그리드 관리자의 로그인 페이지가 나타납니다.

7. "루트" 사용자 및 설치 중에 지정한 암호를 사용하여 Grid Manager에 로그인합니다.

설치 후 지침

그리드 노드 배포 및 구성을 완료한 후 DHCP 주소 지정 및 네트워크 구성 변경에 대한 다음 지침을 따르십시오.

- DHCP를 사용하여 IP 주소를 할당한 경우 사용 중인 네트워크의 각 IP 주소에 대해 DHCP 예약을 구성합니다.

  배포 단계에서는 DHCP만 설정할 수 있습니다. 구성 중에는 DHCP를 설정할 수 없습니다.

> IP 주소가 변경되면 노드가 재부팅되므로 DHCP 주소 변경이 동시에 여러 노드에 영향을 미칠 경우 작동이 중단될 수 있습니다.

- 그리드 노드의 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 변경하려면 IP 변경 절차를 사용해야 합니다. 을 참조하십시오 IP 주소를 구성합니다.
- 라우팅 및 게이트웨이 변경을 비롯한 네트워킹 구성을 변경하면 기본 관리 노드 및 다른 그리드 노드에 대한 클라이언트 연결이 손실될 수 있습니다. 적용된 네트워킹 변경 사항에 따라 이러한 연결을 다시 설정해야 할 수 있습니다.

설치 자동화(**Red Hat Enterprise Linux** 또는 **CentOS**)

StorageGRID 호스트 서비스 설치 및 그리드 노드 구성을 자동화할 수 있습니다.

구축 자동화는 다음 경우에 유용할 수 있습니다.

- 이미 Ansible, Puppet 또는 Chef와 같은 표준 오케스트레이션 프레임워크를 사용하여 물리적 호스트 또는 가상 호스트를 구축 및 구성합니다.
- 여러 StorageGRID 인스턴스를 배포하려고 합니다.
- 크고 복잡한 StorageGRID 인스턴스를 구축하고 있습니다.

StorageGRID 호스트 서비스는 패키지에 의해 설치되며 구성 파일에 의해 구동됩니다. 다음 방법 중 하나를 사용하여 구성 파일을 만들 수 있습니다.

- 구성 파일을 만듭니다 수동 설치 중에 대화형으로.
- 이 문서에 설명되어 있는 대로 표준 오케스트레이션 프레임워크를 사용하여 자동 설치를 수행할 수 있도록 구성 파일을 사전에(또는 프로그래밍 방식으로) 준비합니다.

  StorageGRID는 StorageGRID 어플라이언스 및 전체 StorageGRID 시스템(""그리드")의 구성을 자동화하는 옵션 Python 스크립트를 제공합니다. 이러한 스크립트를 직접 사용하거나 직접 개발한 그리드 배포 및 구성 도구에서 StorageGRID 설치 REST API를 사용하는 방법을 알아보기 위해 스크립트를 검사할 수 있습니다.

StorageGRID 호스트 서비스의 설치 및 구성을 자동화합니다

Anabilities, Puppet, Chef, Fabric 또는 SaltStack과 같은 표준 오케스트레이션 프레임워크를 사용하여 StorageGRID 호스트 서비스의 설치를 자동화할 수 있습니다.

StorageGRID 호스트 서비스는 RPM으로 패키징되며 자동 설치를 위해 미리 준비하거나 프로그래밍 방식으로 준비할 수 있는 구성 파일에 의해 구동됩니다. 표준 오케스트레이션 프레임워크를 사용하여 RHEL 또는 CentOS를 설치 및 구성하는 경우 플레이북이나 레시피에 StorageGRID를 추가하는 것이 간단해야 합니다.

설치 아카이브와 함께 제공된 '/Extras' 폴더에서 Ansible 역할 및 플레이북의 예를 참조하십시오. Ansible 플레이북은 'StorageGRID' 역할이 호스트를 준비하고 타겟 서버에 StorageGRID를 설치하는 방법을 보여줍니다. 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.

> 예제 플레이북에는 StorageGRID 호스트 서비스를 시작하기 전에 네트워크 디바이스를 생성하는 데 필요한 단계가 포함되어 있지 않습니다. 이 단계를 추가한 후 플레이북을 사용하여 작업을 완료합니다.

호스트 준비 및 가상 그리드 노드 구축을 위한 모든 단계를 자동화할 수 있습니다.

StorageGRID의 구성을 자동화합니다

그리드 노드를 구축한 후 StorageGRID 시스템 구성을 자동화할 수 있습니다.

필요한 것

- 설치 아카이브에서 다음 파일의 위치를 알고 있습니다.

파일 이름	설명
configure-storagegrid.py	구성을 자동화하는 데 사용되는 Python 스크립트입니다
configure -StorageGrid.sample.json	스크립트와 함께 사용할 샘플 구성 파일
configure -StorageGrid.blank.json을 지정합니다	스크립트에 사용할 빈 구성 파일입니다

- "configure-StorageGrid.json" 구성 파일을 만들었습니다. 이 파일을 만들려면 샘플 구성 파일('configure-StorageGrid.sample.json') 또는 빈 구성 파일('configure-StorageGrid.blank.json')을 수정할 수 있습니다.

이 작업에 대해

configure-StorageGrid.py Python 스크립트와 configure-StorageGrid.json 구성 파일을 사용하여 StorageGRID 시스템 구성을 자동화할 수 있습니다.

> 그리드 관리자 또는 설치 API를 사용하여 시스템을 구성할 수도 있습니다.

단계

1. Python 스크립트를 실행하기 위해 사용 중인 Linux 시스템에 로그인합니다.
2. 설치 아카이브를 추출한 디렉토리로 변경합니다.

   예를 들면 다음과 같습니다.

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   여기서 플랫폼은 'EBS', 'rpms', 'vSphere'입니다.

3. Python 스크립트를 실행하고 생성한 구성 파일을 사용합니다.

   예를 들면 다음과 같습니다.

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

결과

복구 패키지 '.zip' 파일은 구성 프로세스 중에 생성되며 설치 및 구성 프로세스를 실행 중인 디렉토리에 다운로드됩니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 백업해야 합니다. 예를 들어, 안전한 백업 네트워크 위치 및 안전한 클라우드 저장소 위치에 복사합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

임의 암호를 생성해야 한다고 지정한 경우 "passwords.txt" 파일을 추출하고 StorageGRID 시스템에 액세스하는 데 필요한 암호를 찾아야 합니다.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

확인 메시지가 표시되면 StorageGRID 시스템이 설치 및 구성됩니다.

```
StorageGRID has been configured and installed.
```

관련 정보

설치 REST API 개요

설치 **REST API** 개요

StorageGRID는 설치 작업을 수행하기 위한 StorageGRID 설치 API를 제공합니다.

API는 Swagger 오픈 소스 API 플랫폼을 사용하여 API 문서를 제공합니다. swagger를 사용하면 개발자와 개발자가 아닌 사용자가 API가 매개 변수 및 옵션에 어떻게 응답하는지 보여주는 사용자 인터페이스에서 API와 상호 작용할 수 있습니다. 이 문서에서는 표준 웹 기술 및 JSON(JavaScript Object Notation) 데이터 형식에 대해 잘 알고 있다고 가정합니다.

> API Docs 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

각 REST API 명령에는 API의 URL, HTTP 작업, 필수 또는 선택적 URL 매개 변수, 그리고 예상되는 API 응답이 포함됩니다.

StorageGRID 설치 **API**

StorageGRID 설치 API는 StorageGRID 시스템을 처음 구성할 때와 기본 관리자 노드 복구를 수행해야 하는 경우에만 사용할 수 있습니다. 설치 API는 Grid Manager에서 HTTPS를 통해 액세스할 수 있습니다.

API 설명서에 액세스하려면 기본 관리 노드의 설치 웹 페이지로 이동하여 메뉴 모음에서 * 도움말 * > * API 설명서 * 를 선택합니다.

StorageGRID 설치 API에는 다음 섹션이 포함되어 있습니다.

- * config * — 제품 릴리스 및 API 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 API의 주요 버전을 나열할 수 있습니다.

- * 그리드 * — 그리드 레벨 구성 작업. 그리드 세부 정보, 그리드 네트워크 서브넷, 그리드 암호, NTP 및 DNS 서버 IP 주소를 포함한 그리드 설정을 얻고 업데이트할 수 있습니다.
- * 노드 * — 노드 레벨 구성 작업 그리드 노드 목록을 검색하고, 그리드 노드를 삭제하고, 그리드 노드를 구성하고, 그리드 노드를 보고, 그리드 노드의 구성을 재설정할 수 있습니다.
- * 프로비저닝 * — 프로비저닝 작업. 프로비저닝 작업을 시작하고 프로비저닝 작업의 상태를 볼 수 있습니다.
- * 복구 * — 기본 관리 노드 복구 작업 정보를 재설정하고, 복구 패키지를 업로드하고, 복구를 시작하고, 복구 작업의 상태를 볼 수 있습니다.
- * recovery-package * — 복구 패키지를 다운로드하기 위한 작업.
- 고급 배포를 위한 * 스키마 * — API 스키마
- * 사이트 * — 사이트 수준 구성 작업 사이트를 만들고, 보고, 삭제하고, 수정할 수 있습니다.

다음 단계로 넘어갑니다

설치를 완료한 후에는 일련의 통합 및 구성 단계를 수행해야 합니다. 일부 단계는 필수 사항이고 다른 단계는 선택 사항입니다.

필수 작업

- StorageGRID 시스템에 오브젝트를 저장하는 데 사용할 각 클라이언트 프로토콜(Swift 또는 S3)에 대한 테넌트 계정을 생성합니다.
- 그룹 및 사용자 계정을 구성하여 시스템 액세스를 제어합니다. 필요에 따라 관리 그룹 및 사용자를 가져올 수 있도록 통합 ID 소스(예: Active Directory 또는 OpenLDAP)를 구성할 수 있습니다. 또는 로컬 그룹 및 사용자를 만들 수 있습니다.
- 오브젝트를 StorageGRID 시스템에 업로드하는 데 사용할 S3 또는 Swift API 클라이언트 애플리케이션을 통합 및 테스트합니다.
- 준비가 되면 개체 데이터를 보호하는 데 사용할 ILM(정보 수명 주기 관리) 규칙 및 ILM 정책을 구성합니다.

  StorageGRID를 설치하면 기본 ILM 정책, 즉 기본 2 복사본 정책이 활성화됩니다. 이 정책에는 재고 ILM 규칙(복사본 2개 만들기)이 포함되며 다른 정책이 활성화되지 않은 경우 적용됩니다.

- 설치에 어플라이언스 스토리지 노드가 포함된 경우 SANtricity 소프트웨어를 사용하여 다음 작업을 완료합니다.
  - 각 StorageGRID 어플라이언스에 연결하십시오.
  - AutoSupport 데이터가 수신되었는지 확인합니다.
- StorageGRID 시스템에 아카이브 노드가 포함된 경우 아카이브 노드의 대상 외부 아카이브 스토리지 시스템에 대한 접속을 구성합니다.

  아카이브 노드에서 Tivoli Storage Manager를 외부 아카이브 스토리지 시스템으로 사용하는 경우 Tivoli Storage Manager도 구성해야 합니다.

- StorageGRID 시스템 강화 지침을 검토하고 준수하여 보안 위험을 제거합니다.
- 시스템 경고에 대한 이메일 알림을 구성합니다.

선택적 태스크입니다

- (레거시) 알람 시스템에서 알림을 수신하려면 알람에 대한 메일 그룹 및 이메일 알림을 구성합니다.
- 배포를 계획하고 복구 패키지를 생성한 이후에 변경된 경우 그리드 노드 IP 주소를 업데이트합니다. 복구 및 유지 관리 지침에서 IP 주소 변경에 대한 정보를 참조하십시오.
- 필요한 경우 스토리지 암호화를 구성합니다.
- 필요한 경우 스토리지 압축을 구성하여 저장된 개체의 크기를 줄입니다.
- 감사 클라이언트 액세스를 구성합니다. NFS 또는 CIFS 파일 공유를 통해 감사 목적으로 시스템에 대한 액세스를 구성할 수 있습니다. StorageGRID 관리 지침을 참조하십시오.

> CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

관련 정보

StorageGRID 관리

S3을 사용합니다

Swift를 사용합니다

ILM을 사용하여 개체를 관리합니다

모니터링하고 문제를 해결합니다

복구 및 유지 관리

SG100 및 SG1000 서비스 어플라이언스

SG5600 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG6000 스토리지 어플라이언스

릴리스 정보

시스템 강화

감사 로그를 검토합니다

소프트웨어 업그레이드

설치 문제를 해결합니다

StorageGRID 시스템을 설치하는 동안 문제가 발생하면 설치 로그 파일에 액세스할 수 있습니다. 기술 지원 부서에서는 설치 로그 파일을 사용하여 문제를 해결해야 할 수도 있습니다.

각 노드를 실행 중인 컨테이너에서 다음 설치 로그 파일을 사용할 수 있습니다.

- '/var/local/log/install.log'(모든 그리드 노드에 있음)
- (/var/local/log/gdu-server.log"(기본 관리 노드에서 찾을 수 있음)

호스트에서 다음 설치 로그 파일을 사용할 수 있습니다.

- '/var/log/StorageGrid/daemon.log'입니다
- '/var/log/StorageGrid/nodes/node-name.log'

로그 파일에 액세스하는 방법은 StorageGRID 모니터링 및 문제 해결 지침을 참조하십시오. 어플라이언스 설치 문제 해결에 대한 도움말은 어플라이언스의 설치 및 유지 관리 지침을 참조하십시오. 추가 지원이 필요한 경우 기술 지원 부서에 문의하십시오.

관련 정보

모니터링하고 문제를 해결합니다

SG100 및 SG1000 서비스 어플라이언스

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG5600 스토리지 어플라이언스

"NetApp 지원"

예 /etc/sysconfig/network-scripts

예제 파일을 사용하여 4개의 Linux 물리적 인터페이스를 단일 LACP 결합으로 집계한 다음 StorageGRID 그리드, 관리 및 클라이언트 네트워크 인터페이스로 사용할 본드를 포함하는 3개의 VLAN 인터페이스를 설정할 수 있습니다.

물리적 인터페이스

링크의 다른 쪽 끝에 있는 스위치도 4개의 포트를 단일 LACP 트렁크 또는 포트 채널로 처리해야 하며, 태그가 있는 3개 이상의 참조된 VLAN을 통과해야 합니다.

'*/etc/sysconfig/network-scripts/ifcfg-ens160 *'

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

' * /etc/sysconfig/network-scripts/ifcfg-ens192 *'

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

' * /etc/sysconfig/network-scripts/ifcfg-ens224 *'

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

'*/etc/sysconfig/network-scripts/ifcfg-ens256 *'

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

본드 인터페이스

' * /etc/sysconfig/network-scripts/ifcfg-bond0 * '

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

VLAN 인터페이스

'*/etc/sysconfig/network-scripts/ifcfg-bond0.1001 *'

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

'*/etc/sysconfig/network-scripts/ifcfg-bond0.1002 *'

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

'*/etc/sysconfig/network-scripts/ifcfg-bond0.1003 *'

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

Ubuntu 또는 Debian을 설치합니다

Ubuntu 또는 Debian 설치: 개요

Ubuntu 또는 Debian 환경에 StorageGRID 시스템을 설치하는 과정은 세 가지 기본 단계로 구성됩니다.

1. * 준비 *: 계획 및 준비 중에 다음 작업을 수행합니다.

- StorageGRID의 하드웨어 및 스토리지 요구사항에 대해 알아보십시오.
- 의 세부 사항에 대해 자세히 알아보십시오 StorageGRID 네트워킹 따라서 네트워크를 적절하게 구성할 수 있습니다.
- StorageGRID 그리드 노드를 호스팅하는 데 사용할 물리적 또는 가상 서버를 식별하고 준비합니다.
- 준비한 서버:
  - Linux를 설치합니다
  - 호스트 네트워크를 구성합니다
  - 호스트 스토리지를 구성합니다
  - Docker를 설치합니다
  - StorageGRID 호스트 서비스를 설치합니다

2. * 배포 *: 적절한 사용자 인터페이스를 사용하여 그리드 노드를 배포합니다. 그리드 노드를 구축하면 StorageGRID 시스템의 일부로 생성되고 하나 이상의 네트워크에 연결됩니다.
   a. Linux 명령줄 및 노드 구성 파일을 사용하여 1단계에서 준비한 호스트에 가상 그리드 노드를 배포합니다.
   b. StorageGRID 어플라이언스 설치 프로그램을 사용하여 StorageGRID 어플라이언스 노드를 배포합니다.

> 하드웨어 관련 설치 및 통합 지침은 StorageGRID 설치 절차에 포함되어 있지 않습니다. StorageGRID 어플라이언스를 설치하는 방법에 대한 자세한 내용은 해당 어플라이언스의 설치 및 유지 관리 지침을 참조하십시오.

3. * 구성 *: 모든 노드가 배포되면 그리드 관리자를 사용하여 그리드를 구성하고 설치를 완료합니다.

이 지침은 Ubuntu 또는 Debian 환경에서 StorageGRID 시스템을 배포하고 구성하는 표준 접근 방법을 권장합니다. 다음 대체 접근 방법에 대한 정보도 참조하십시오.

- Anabilities, Puppet 또는 Chef와 같은 표준 오케스트레이션 프레임워크를 사용하여 Ubuntu 또는 Debian을 설치하고, 네트워킹 및 스토리지를 구성하고, Docker 및 StorageGRID 호스트 서비스를 설치하고, 가상 그리드 노드를 배포합니다.
- 설치 아카이브에 제공되는 Python 구성 스크립트를 사용하여 StorageGRID 시스템의 구축 및 구성을 자동화합니다.
- Python 구성 스크립트(설치 아카이브나 StorageGRID 어플라이언스 설치 프로그램에서 사용 가능)를 사용하여 어플라이언스 그리드 노드의 구축 및 구성을 자동화합니다.
- StorageGRID 배포의 고급 개발자인 경우 설치 REST API를 사용하여 StorageGRID 그리드 노드 설치를 자동화합니다.

Ubuntu 또는 Debian 설치를 계획하고 준비합니다

설치하기 전에**(Ubuntu** 또는 **Debian)**

그리드 노드를 배포하고 StorageGRID 그리드를 구성하기 전에 절차를 완료하기 위한 단계와 요구 사항을 숙지해야 합니다.

StorageGRID 배포 및 구성 절차에서는 StorageGRID 시스템의 아키텍처 및 작동에 대해 잘 알고 있다고 가정합니다.

단일 사이트 또는 여러 사이트를 한 번에 배포할 수 있지만, 모든 사이트는 최소 3개의 스토리지 노드를 보유해야 하는

최소 요구 사항을 충족해야 합니다.

StorageGRID 설치를 시작하기 전에 다음을 수행해야 합니다.

- 각 노드의 최소 CPU 및 RAM 요구사항을 비롯한 StorageGRID의 컴퓨팅 요구사항 이해
- StorageGRID가 트래픽 분리, 보안 및 관리의 편의를 위해 여러 네트워크를 지원하는 방법을 이해하고 각 StorageGRID 노드에 연결할 네트워크를 계획합니다.

  StorageGRID 네트워킹 지침을 참조하십시오.

- 각 그리드 노드 유형의 스토리지 및 성능 요구 사항을 이해합니다.
- 구축할 StorageGRID 노드의 수와 유형을 지원하기에 충분한 리소스를 제공하는 물리적 서버 세트, 가상 서버 또는 둘 다 식별합니다.
- 서비스 중단 없이 물리적 호스트에 대해 예약된 유지 관리를 수행하려는 경우 노드 마이그레이션에 대한 요구 사항을 파악합니다.
- 모든 네트워킹 정보를 미리 수집합니다. DHCP를 사용하지 않는 경우 각 그리드 노드에 할당할 IP 주소와 사용할 DNS(Domain Name System) 및 NTP(Network Time Protocol) 서버의 IP 주소를 수집합니다.
- 모든 StorageGRID 어플라이언스를 포함하여 필요한 모든 하드웨어를 사양에 맞게 설치, 연결 및 구성합니다.

> 하드웨어 관련 설치 및 통합 지침은 StorageGRID 설치 절차에 포함되어 있지 않습니다. StorageGRID 어플라이언스를 설치하는 방법에 대한 자세한 내용은 해당 어플라이언스의 설치 및 유지 관리 지침을 참조하십시오.

- 사용할 수 있는 배포 및 구성 도구 중에서 선택합니다.

관련 정보

네트워킹 지침

SG100 및 SG1000 서비스 어플라이언스

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG5600 스토리지 어플라이언스

노드 컨테이너 마이그레이션 요구사항

필수 자료

StorageGRID를 설치하기 전에 필요한 자료를 수집하고 준비해야 합니다.

항목	참고
NetApp StorageGRID 라이센스	디지털 서명된 유효한 NetApp 라이센스가 있어야 합니다. • 참고 *: StorageGRID 설치 아카이브에는 테스트 및 개념 증명 그리드에 사용할 수 있는 비운영 라이센스가 포함되어 있습니다.
StorageGRID 설치 아카이브	반드시 해야 합니다 StorageGRID 설치 아카이브를 다운로드하고 파일의 압축을 풉니다.
서비스 노트북	StorageGRID 시스템은 서비스 랩톱을 통해 설치됩니다. 서비스 랩톱의 구성 요소: • 네트워크 포트 • SSH 클라이언트(예: PuTTY) • 지원되는 웹 브라우저
StorageGRID 설명서	• 릴리스 정보 • StorageGRID 관리 지침

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

StorageGRID 설치 파일을 다운로드하고 압축을 풉니다

StorageGRID 설치 아카이브를 다운로드하고 필요한 파일을 추출해야 합니다.

단계

1. 로 이동합니다 "StorageGRID용 NetApp 다운로드 페이지".
2. 최신 릴리스를 다운로드하려면 버튼을 선택하거나 드롭다운 메뉴에서 다른 버전을 선택하고 * GO * 를 선택합니다.
3. NetApp 계정의 사용자 이름과 암호를 사용하여 로그인합니다.
4. Caution/MustRead 문이 나타나면 해당 문을 읽고 확인란을 선택합니다.

   StorageGRID 릴리스를 설치한 후 필요한 핫픽스를 적용해야 합니다. 자세한 내용은 를 참조하십시오 복구 및 유지 관리 지침의 핫픽스 절차

5. 최종 사용자 사용권 계약을 읽고 확인란을 선택한 다음 * 동의 및 계속 * 을 선택합니다.

   선택한 버전의 다운로드 페이지가 나타납니다. 이 페이지에는 세 개의 열이 있습니다.

6. StorageGRID* 설치 열에서 Ubuntu 또는 Debian용 .tgz 또는 .zip 파일을 선택합니다.

   서비스 랩톱에서 Windows를 실행 중인 경우 '.zip' 파일을 선택합니다.

7. 아카이브 파일을 저장하고 압축을 풉니다.
8. 다음 목록에서 필요한 파일을 선택합니다.

   필요한 파일 세트는 계획된 그리드 토폴로지와 StorageGRID 그리드를 구축하는 방법에 따라 달라집니다.

   표에 나열된 경로는 추출된 설치 아카이브에서 설치한 최상위 디렉토리에 상대적입니다.

경로 및 파일 이름입니다	설명
	StorageGRID 다운로드 파일에 포함된 모든 파일을 설명하는 텍스트 파일입니다.
/debs/NLF000000.txt 를 참조하십시오	테스트 및 개념 증명 배포에 사용할 수 있는 비프로덕션 NetApp 라이센스 파일.
/debs/storagegrid-webscale-images-version-SHA.deb 를 참조하십시오	StorageGRID 노드 이미지를 Ubuntu 또는 Debian 호스트에 설치하기 위한 DEB 패키지.
/debs/storagegrid-webscale-images-version-SHA.deb.md5 를 참조하십시오	파일 '/debs/storagegrid-webscale-images-version-SHA.deb` 에 대한 MD5 체크섬입니다.
/debs/storagegrid-webscale-service-version-SHA.deb 를 참조하십시오	Ubuntu 또는 Debian 호스트에 StorageGRID 호스트 서비스를 설치하기 위한 DEB 패키지.
배포 스크립팅 도구	설명
/debs/configure-storagegrid.py 를 참조하십시오	StorageGRID 시스템 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
/debs/configure-sga.py 를 참조하십시오	StorageGRID 어플라이언스 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
/debs/storagegrid-ssoauth.py 를 참조하십시오	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/debs/configure -StorageGrid.sample.json 을 참조하십시오	"configure-StorageGrid.py" 스크립트와 함께 사용할 구성 파일의 예
/debs/configure -StorageGrid.blank.json 을 참조하십시오	configure-StorageGrid.py 스크립트와 함께 사용할 빈 구성 파일입니다.
	StorageGRID 컨테이너 배포를 위한 Ubuntu 또는 Debian 호스트 구성을 위한 Ansible 역할 및 플레이북 예 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.

경로 및 파일 이름입니다	설명
/debs/Extras/API-schemas	StorageGRID에 대한 API 스키마입니다. • 참고 *: 업그레이드를 수행하기 전에 이러한 스키마를 사용하여 StorageGRID 관리 API를 사용하도록 작성한 코드가 업그레이드 호환성 테스트를 위한 비프로덕션 StorageGRID 환경이 없는 경우 새 StorageGRID 릴리스와 호환되는지 확인할 수 있습니다.

관련 정보

복구 및 유지 관리

CPU 및 **RAM** 요구 사항

StorageGRID 소프트웨어를 설치하기 전에 StorageGRID 시스템을 지원할 준비가 되도록 하드웨어를 확인 및 구성하십시오.

지원되는 서버에 대한 자세한 내용은 상호 운용성 매트릭스 를 참조하십시오.

각 StorageGRID 노드에는 다음과 같은 최소 리소스가 필요합니다.

- CPU 코어: 노드당 8개
- RAM: 사용 가능한 총 RAM과 시스템에서 실행 중인 비 StorageGRID 소프트웨어의 양에 따라 노드당 최소 24GB, 총 시스템 RAM보다 2GB ~ 16GB 이상

각 물리적 또는 가상 호스트에서 실행하려는 StorageGRID 노드 수가 사용 가능한 CPU 코어 수 또는 물리적 RAM을 초과하지 않는지 확인합니다. 호스트가 StorageGRID 실행 전용이 아닌 경우(권장되지 않음) 다른 애플리케이션의 리소스 요구 사항을 고려해야 합니다.

> CPU 및 메모리 사용량을 정기적으로 모니터링하여 이러한 리소스가 작업 부하를 지속적으로 수용할 수 있도록 합니다. 예를 들어, 가상 스토리지 노드에 대한 RAM 및 CPU 할당을 두 배로 하면 StorageGRID 어플라이언스 노드에 제공되는 것과 유사한 리소스를 제공할 수 있습니다. 또한 노드당 메타데이터 양이 500GB를 초과하는 경우 노드당 RAM을 48GB 이상으로 늘리는 것이 좋습니다. 개체 메타데이터 저장소 관리, 메타데이터 예약 공간 설정 증가 및 CPU 및 메모리 사용량 모니터링에 대한 자세한 내용은 StorageGRID 관리, 모니터링 및 업그레이드에 대한 지침을 참조하십시오.

하이퍼스레딩이 기본 물리적 호스트에서 활성화된 경우 노드당 8개의 가상 코어(4개의 물리적 코어)를 제공할 수 있습니다. 하이퍼스레딩이 기본 물리적 호스트에서 사용되지 않는 경우 노드당 8개의 물리적 코어를 제공해야 합니다.

가상 시스템을 호스트로 사용하고 VM의 크기와 수를 제어하는 경우 각 StorageGRID 노드에 대해 단일 VM을 사용하고 그에 따라 VM 크기를 조정해야 합니다.

운영 구축 환경에서는 동일한 물리적 스토리지 하드웨어 또는 가상 호스트에서 여러 스토리지 노드를 실행하지 않아야 합니다. 단일 StorageGRID 구축 환경의 각 스토리지 노드는 자체 격리된 장애 도메인에 있어야 합니다. 단일 하드웨어 장애가 단일 스토리지 노드에만 영향을 줄 수 있도록 하는 경우 오브젝트 데이터의 내구성과 가용성을 최대화할 수 있습니다.

스토리지 요구 사항에 대한 정보도 참조하십시오.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

요구사항을 충족해야 합니다

StorageGRID 관리

모니터링하고 문제를 해결합니다

소프트웨어 업그레이드

요구사항을 충족해야 합니다

초기 구성과 향후 스토리지 확장을 지원할 충분한 공간을 제공할 수 있도록 StorageGRID 노드의 스토리지 요구사항을 이해해야 합니다.

StorageGRID 노드에는 다음과 같은 세 가지 논리적 스토리지 범주가 필요합니다.

- StorageGRID 노드를 지원할 호스트에 Docker를 설치 및 구성할 때 Docker 스토리지 드라이버에 할당되는 노드 컨테이너용 * 컨테이너 풀 * — 성능 계층(10K SAS 또는 SSD) 스토리지입니다.
- * 시스템 데이터 * — StorageGRID 호스트 서비스가 사용하고 개별 노드에 매핑하는 시스템 데이터 및 트랜잭션 로그의 노드당 영구 스토리지를 위한 성능 계층(10K SAS 또는 SSD) 스토리지입니다.
- * 오브젝트 데이터 * — 객체 데이터 및 객체 메타데이터의 영구 스토리지를 위한 Performance-Tier(10K SAS 또는 SSD) 스토리지 및 Capacity-Tier(NL-SAS/SATA) 대용량 스토리지

모든 스토리지 범주에 RAID 지원 블록 장치를 사용해야 합니다. 비중복 디스크, SSD 또는 JBOD는 지원되지 않습니다. 모든 스토리지 범주에서 공유 또는 로컬 RAID 스토리지를 사용할 수 있지만 StorageGRID의 노드 마이그레이션 기능을 사용하려면 시스템 데이터와 오브젝트 데이터를 공유 스토리지에 모두 저장해야 합니다.

성능 요구사항

컨테이너 풀, 시스템 데이터 및 오브젝트 메타데이터에 사용되는 볼륨의 성능은 시스템의 전반적인 성능에 큰 영향을 미칩니다. 이러한 볼륨에 성능 계층(10K SAS 또는 SSD) 스토리지를 사용하면 지연 시간, IOPS(초당 입출력 작업) 및 처리량 측면에서 디스크 성능이 적절하게 보장됩니다. 객체 데이터의 영구 스토리지를 위해 용량 계층(NL-SAS/SATA) 스토리지를 사용할 수 있습니다.

컨테이너 풀, 시스템 데이터 및 오브젝트 데이터에 사용되는 볼륨에는 다시 쓰기 캐시가 설정되어 있어야 합니다. 캐시는 보호되거나 영구 미디어에 있어야 합니다.

NetApp ONTAP 스토리지를 사용하는 호스트에 대한 요구사항

StorageGRID 노드에서 NetApp ONTAP 시스템에서 할당된 스토리지를 사용하는 경우 볼륨에 FabricPool 계층화 정책이 활성화되어 있지 않은지 확인합니다. StorageGRID 노드와 함께 사용되는 볼륨에 대해 FabricPool 계층화를 사용하지 않도록 설정하면 문제 해결과 스토리지 작업이 간소화됩니다.

> FabricPool를 사용하여 StorageGRID 관련 데이터를 StorageGRID 자체로 계층화하지 마십시오. StorageGRID 데이터를 StorageGRID로 다시 계층화하면 문제 해결과 운영 복잡성이 늘어납니다.

필요한 호스트 수입니다

각 StorageGRID 사이트에는 최소 3개의 스토리지 노드가 필요합니다.

> 운영 구축 시 단일 물리적 호스트 또는 가상 호스트에서 스토리지 노드를 두 개 이상 실행하지 마십시오. 각 스토리지 노드에 대해 전용 호스트를 사용하면 격리된 장애 도메인이 제공됩니다.

관리 노드 또는 게이트웨이 노드와 같은 다른 유형의 노드는 동일한 호스트에 구축하거나 필요에 따라 전용 호스트에 구축할 수 있습니다.

각 호스트의 스토리지 볼륨 수입니다

다음 표에는 각 호스트에 필요한 스토리지 볼륨(LUN) 수와 해당 호스트에 구축할 노드를 기준으로 각 LUN에 필요한 최소 크기가 나와 있습니다.

테스트된 최대 LUN 크기는 39TB입니다.

> 이러한 숫자는 전체 그리드가 아닌 각 호스트에 대한 것입니다.

LUN의 용도	스토리지 범주입니다	**LUN** 수입니다	최소 크기/**LUN**
컨테이너 엔진 스토리지 풀입니다	컨테이너 풀입니다	1	총 노드 수 × 100GB
'/var/local' 볼륨	시스템 데이터	이 호스트의 각 노드에 대해 1개	90GB
스토리지 노드	오브젝트 데이터	이 호스트의 각 스토리지 노드에 대해 3개 • 참고: * 소프트웨어 기반 스토리지 노드는 1-16개의 스토리지 볼륨을 가질 수 있습니다. 최소 3개의 스토리지 볼륨을 사용하는 것이 좋습니다.	12TB(4TB/LUN) 자세한 내용은 스토리지 노드의 스토리지 요구 사항 을 참조하십시오.
관리자 노드 감사 로그	시스템 데이터	이 호스트의 각 관리 노드에 대해 1개	200GB
관리자 노드 테이블	시스템 데이터	이 호스트의 각 관리 노드에 대해 1개	200GB

> 구성된 감사 레벨, S3 오브젝트 키 이름 등의 사용자 입력 크기 및 보존해야 하는 감사 로그 데이터의 양에 따라 각 관리 노드에서 감사 로그 LUN의 크기를 늘려야 할 수 있습니다. 일반적으로, 그리드는 S3 작업당 약 1KB의 감사 데이터를 생성합니다. 즉, 200GB LUN이 하루에 7000만 개의 작업을 지원하거나 2~3일 동안 초당 800개의 작업을 지원합니다.

호스트의 최소 스토리지 공간입니다

다음 표에는 각 노드 유형에 필요한 최소 스토리지 공간이 나와 있습니다. 이 표를 사용하여 각 스토리지 범주에서 호스트에 구축해야 하는 최소 스토리지 양을 해당 호스트에 구축될 노드를 기반으로 결정할 수 있습니다.

> 디스크 스냅샷을 사용하여 그리드 노드를 복원할 수 없습니다. 대신 각 노드 유형에 대한 복구 및 유지보수 절차를 참조하십시오.

노드 유형입니다	컨테이너 풀입니다	시스템 데이터	오브젝트 데이터
스토리지 노드	100GB	90GB	4,000GB
관리자 노드	100GB	490GB(LUN 3개)	_해당 사항 없음 _
게이트웨이 노드	100GB	90GB	_해당 사항 없음 _
아카이브 노드	100GB	90GB	_해당 사항 없음 _

예: 호스트에 대한 스토리지 요구 사항 계산

동일한 호스트에 스토리지 노드 1개, 관리 노드 1개, 게이트웨이 노드 1개 등 3개의 노드를 구축하려고 한다고 가정해 보겠습니다. 호스트에 최소 9개의 스토리지 볼륨을 제공해야 합니다. 노드 컨테이너용 300GB 이상의 성능 계층 스토리지, 시스템 데이터 및 트랜잭션 로그용 670GB 성능 계층 스토리지, 오브젝트 데이터를 위한 12TB의 용량 계층 스토리지가 필요합니다.

노드 유형입니다	**LUN**의 용도	**LUN** 수입니다	**LUN** 크기입니다
스토리지 노드	Docker 스토리지 풀	1	300GB(100GB/노드)
스토리지 노드	'/var/local' 볼륨	1	90GB
스토리지 노드	오브젝트 데이터	3	12TB(4TB/LUN)
관리자 노드	'/var/local' 볼륨	1	90GB
관리자 노드	관리자 노드 감사 로그	1	200GB
관리자 노드	관리자 노드 테이블	1	200GB
게이트웨이 노드	'/var/local' 볼륨	1	90GB

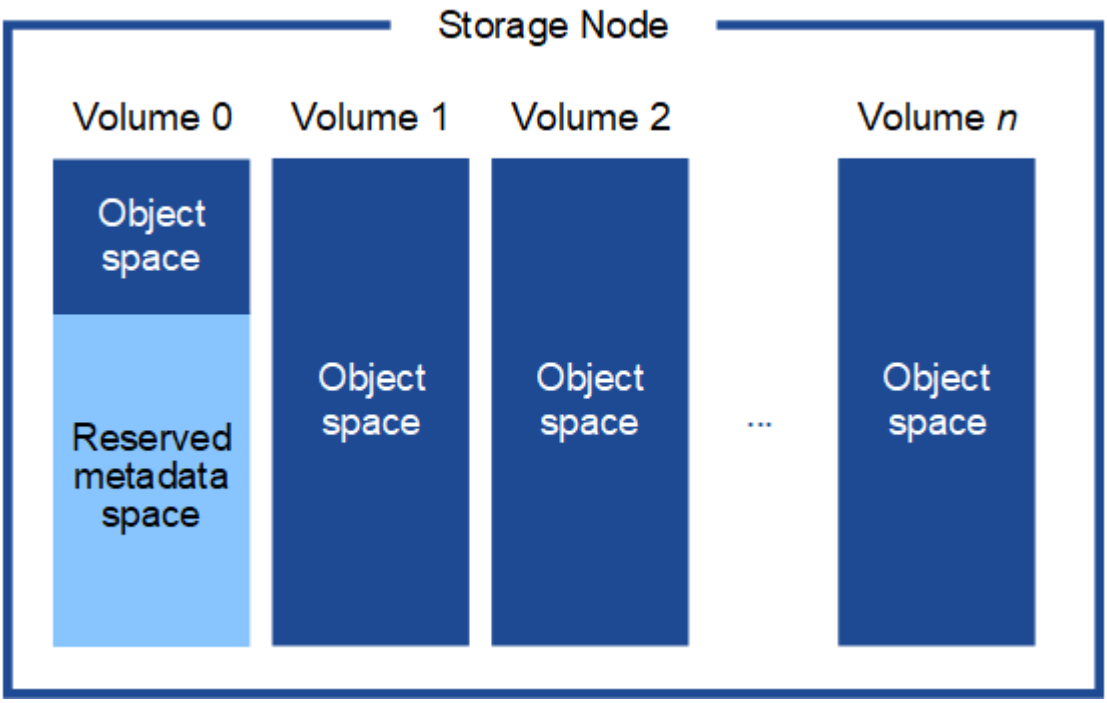
노드 유형입니다	**LUN**의 용도	**LUN** 수입니다	**LUN** 크기입니다
• 합계 *		• 9 *	• 컨테이너 풀: * 300GB • 시스템 데이터: * 670GB • 오브젝트 데이터: * 12,000GB

스토리지 노드의 스토리지 요구 사항

소프트웨어 기반 스토리지 노드는 1-16개의 스토리지 볼륨을 가질 수 있습니다. -3개 이상의 스토리지 볼륨을 사용하는 것이 좋습니다. 각 스토리지 볼륨은 4TB 이상이어야 합니다.

> 어플라이언스 스토리지 노드는 최대 48개의 스토리지 볼륨을 가질 수 있습니다.

그림에 나와 있는 것처럼 StorageGRID는 각 스토리지 노드의 스토리지 볼륨 0에 객체 메타데이터를 위한 공간을 예약합니다. 스토리지 볼륨 0 및 스토리지 노드의 다른 스토리지 볼륨의 나머지 공간은 오브젝트 데이터에만 사용됩니다.



이중화를 제공하고 개체 메타데이터를 손실로부터 보호하기 위해 StorageGRID는 각 사이트의 시스템 모든 개체에 대한 메타데이터 복사본을 3개 저장합니다. 오브젝트 메타데이터의 복사본 3개는 각 사이트의 모든 스토리지 노드에 균등하게 분산됩니다.

새 스토리지 노드의 볼륨 0에 공간을 할당하는 경우 모든 오브젝트 메타데이터의 해당 노드에 적절한 공간이 있는지 확인해야 합니다.

- 적어도 볼륨 0에 4TB 이상을 할당해야 합니다.

> 스토리지 노드에 대해 하나의 스토리지 볼륨만 사용하고 볼륨에 4TB 이하를 할당하는 경우 스토리지 노드는 시작 시 스토리지 읽기 전용 상태로 전환되어 객체 메타데이터만 저장할 수 있습니다.

- 새 StorageGRID 11.6 시스템을 설치하고 각 스토리지 노드에 128GB 이상의 RAM이 있는 경우 볼륨 0에 8TB 이상을 할당해야 합니다. 볼륨 0에 더 큰 값을 사용하면 각 스토리지 노드에서 메타데이터에 허용되는 공간이 증가할 수 있습니다.
- 사이트에 대해 서로 다른 스토리지 노드를 구성할 때 가능하면 볼륨 0에 대해 동일한 설정을 사용합니다. 사이트에 크기가 다른 스토리지 노드가 있는 경우 볼륨이 0인 스토리지 노드가 해당 사이트의 메타데이터 용량을 결정합니다.

자세한 내용은 를 참조하십시오 오브젝트 메타데이터 스토리지 관리.

관련 정보

노드 컨테이너 마이그레이션 요구사항

복구 및 유지 관리

노드 컨테이너 마이그레이션 요구사항

노드 마이그레이션 기능을 사용하면 노드를 한 호스트에서 다른 호스트로 수동으로 이동할 수 있습니다. 일반적으로 두 호스트는 동일한 물리적 데이터 센터에 있습니다.

노드 마이그레이션을 통해 그리드 작업을 중단하지 않고 물리적 호스트 유지 관리를 수행할 수 있습니다. 물리적 호스트를 오프라인으로 전환하기 전에 한 번에 하나씩 모든 StorageGRID 노드를 다른 호스트로 이동하기만 하면 됩니다. 노드를 마이그레이션하려면 각 노드의 다운타임만 짧고 그리드 서비스의 운영 또는 가용성에 영향을 미치지 않아야 합니다.

StorageGRID 노드 마이그레이션 기능을 사용하려면 배포가 추가 요구 사항을 충족해야 합니다.

- 단일 물리적 데이터 센터의 호스트 전반에서 일관된 네트워크 인터페이스 이름
- 단일 물리적 데이터 센터의 모든 호스트에서 액세스할 수 있는 StorageGRID 메타데이터 및 오브젝트 저장소 볼륨을 위한 공유 스토리지입니다. 예를 들어, NetApp E-Series 스토리지 어레이를 사용할 수 있습니다.

가상 호스트를 사용 중이고 기본 하이퍼바이저 계층에서 VM 마이그레이션을 지원하는 경우 StorageGRID의 노드 마이그레이션 기능 대신 이 기능을 사용할 수 있습니다. 이 경우 이러한 추가 요구 사항을 무시할 수 있습니다.

마이그레이션 또는 하이퍼바이저 유지 보수를 수행하기 전에 노드를 정상적으로 종료합니다. 의 지침을 참조하십시오 그리드 노드 종료.

VMware Live Migration은 지원되지 않습니다

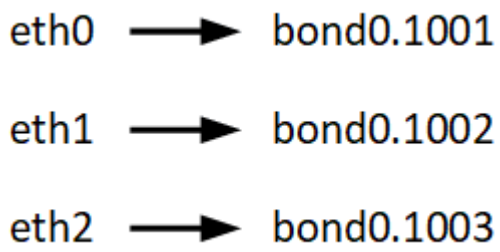
OpenStack Live Migration 및 VMware LIVE vMotion을 사용하면 가상 머신 클록 시간이 단축되며 모든 유형의 그리드 노드에서는 지원되지 않습니다. 드물지만 잘못된 클럭 시간으로 인해 데이터 또는 구성 업데이트가 손실될 수 있습니다.

콜드 마이그레이션이 지원됩니다. 콜드 마이그레이션에서는 StorageGRID 노드를 호스트 간에 마이그레이션하기 전에 종료해야 합니다. 의 지침을 참조하십시오 그리드 노드 종료.

일관된 네트워크 인터페이스 이름

한 호스트에서 다른 호스트로 노드를 이동하려면 StorageGRID 호스트 서비스가 노드가 현재 위치에 있는 외부 네트워크 연결이 새 위치에서 복제될 수 있다는 확신을 가져야 합니다. 호스트에서 일관된 네트워크 인터페이스 이름을 사용하면 이러한 자신감을 얻을 수 있습니다.

예를 들어 호스트 1에서 실행되는 StorageGRID NodeA가 다음과 같은 인터페이스 매핑으로 구성되었다고 가정합니다.



화살표의 왼쪽 면은 StorageGRID 컨테이너 내에서 보는 기존 인터페이스(즉, 그리드, 관리자 및 클라이언트 네트워크 인터페이스)에 해당합니다. 화살표의 오른쪽은 동일한 물리적 인터페이스 결합에 종속된 세 개의 VLAN 인터페이스인 이러한 네트워크를 제공하는 실제 호스트 인터페이스에 해당합니다.

이제 NodeA를 Host2로 마이그레이션한다고 가정해 보겠습니다. Host2에 bond0.1001, bond0.1002 및 bond0.1003이라는 인터페이스도 있는 경우 시스템은 Host1에서와 같이 같은 이름의 인터페이스가 Host2에서 동일한 연결을 제공한다고 가정하여 이동을 허용합니다. 호스트 2에 동일한 이름의 인터페이스가 없으면 이동이 허용되지 않습니다.

여러 호스트에 걸쳐 일관된 네트워크 인터페이스 이름 지정을 달성하는 방법은 여러 가지가 있습니다. 를 참조하십시오 호스트 네트워크를 구성합니다 몇 가지 예를 참조하십시오.

공유 스토리지

오버헤드가 낮은 노드를 신속하게 마이그레이션하기 위해 StorageGRID 노드 마이그레이션 기능은 노드 데이터를 물리적으로 이동하지 않습니다. 대신 노드 마이그레이션은 다음과 같이 한 쌍의 엑스포트 및 임포트 작업으로 수행됩니다.

단계

1. "노드 내보내기" 작업 중에 호스트 A에서 실행되는 노드 컨테이너에서 소량의 영구 상태 데이터가 추출되어 해당 노드의 시스템 데이터 볼륨에 캐시됩니다. 그런 다음 HostA의 노드 컨테이너가 인스턴스화됩니다.
2. "노드 가져오기" 작업 중에 HostA에 적용되는 것과 동일한 네트워크 인터페이스를 사용하는 호스트 B의 노드 컨테이너와 블록 스토리지 매핑이 인스턴스화됩니다. 그런 다음 캐시된 영구 상태 데이터가 새 인스턴스에 삽입됩니다.

이 작업 모드가 주어지면 마이그레이션을 허용하고 작동하기 위해서는 노드의 모든 시스템 데이터와 객체 스토리지 볼륨을 HostA와 HostB에서 액세스할 수 있어야 합니다. 또한 HostA 및 HostB에서 동일한 LUN을 참조하도록 보장된 이름을 사용하여 노드에 매핑되어야 합니다.

다음 예에서는 호스트에서 DM 다중 경로를 사용하고 있는 StorageGRID 스토리지 노드에 대한 블록 디바이스 매핑을 위한 단일 솔루션을 보여 주며, 별칭 필드는 모든 호스트에서 사용할 수 있는 일관되고 친숙한 블록 디바이스 이름을 제공하기 위해 '/etc/multipath.conf'에서 사용되었습니다.

/var/local → /dev/mapper/sgws-sn1-var-local

rangedb0 → /dev/mapper/sgws-sn1-rangedb0

rangedb1 → /dev/mapper/sgws-sn1-rangedb1

rangedb2 → /dev/mapper/sgws-sn1-rangedb2

rangedb3 → /dev/mapper/sgws-sn1-rangedb3

구축 툴

StorageGRID 설치의 일부 또는 전부를 자동화할 수 있습니다.

구축 자동화는 다음 경우에 유용할 수 있습니다.

- 이미 Ansible, Puppet 또는 Chef와 같은 표준 오케스트레이션 프레임워크를 사용하여 물리적 호스트 또는 가상 호스트를 구축 및 구성합니다.
- 여러 StorageGRID 인스턴스를 배포하려고 합니다.
- 크고 복잡한 StorageGRID 인스턴스를 구축하고 있습니다.

StorageGRID 호스트 서비스는 패키지에 의해 설치되며 수동 설치 중에 대화형으로 만들 수 있는 구성 파일에 의해 구동되거나, 표준 오케스트레이션 프레임워크를 사용하여 자동 설치를 지원하기 위해 미리 준비되거나 프로그래밍 방식으로 준비됩니다. StorageGRID는 StorageGRID 어플라이언스 및 전체 StorageGRID 시스템(""그리드")의 구성을 자동화하는 옵션 Python 스크립트를 제공합니다. 이러한 스크립트를 직접 사용하거나 직접 개발한 그리드 배포 및 구성 도구에서 StorageGRID 설치 REST API를 사용하는 방법을 알아보기 위해 스크립트를 검사할 수 있습니다.

StorageGRID 구축의 전부 또는 일부를 자동화하려는 경우 을 검토하십시오 설치를 자동화합니다 설치 프로세스를 시작하기 전에

호스트 준비(**Ubuntu** 또는 **Debian**)

Linux를 설치합니다

모든 그리드 호스트에 Linux를 설치해야 합니다. 를 사용합니다 "NetApp 상호 운용성 매트릭스 툴" 를 클릭하여 지원되는 버전 목록을 가져옵니다.

단계

1. 배포자의 지침 또는 표준 절차에 따라 모든 물리적 또는 가상 그리드 호스트에 Linux를 설치합니다.

> 그래픽 데스크톱 환경을 설치하지 마십시오. Ubuntu를 설치할 때 * 표준 시스템 유틸리티 * 를 선택해야 합니다. Ubuntu 호스트에 대한 ssh 액세스를 활성화하려면 * OpenSSH 서버 * 를 선택하는 것이 좋습니다. 다른 모든 옵션은 선택되지 않은 상태로 둘 수 있습니다.

2. 모든 호스트가 Ubuntu 또는 Debian 패키지 리포지토리에 액세스할 수 있는지 확인합니다.

3. 스왑이 활성화된 경우:

   a. '$sudo swapoff - -all' 명령을 실행합니다

   b. 설정을 유지하려면 '/etc/fstab'에서 모든 스왑 항목을 제거하십시오.

   스왑을 완전히 사용하지 않도록 설정하면 성능이 크게 저하될 수 있습니다.

AppArmor 프로필 설치를 이해합니다

사용자가 자체 배포된 Ubuntu 환경에서 AppArmor 필수 액세스 제어 시스템을 사용하는 경우 기본 시스템에 설치하는 패키지와 관련된 AppArmor 프로필이 StorageGRID와 함께 설치된 해당 패키지에 의해 차단될 수 있습니다.

기본적으로 AppArmor 프로필은 기본 운영 체제에 설치하는 패키지에 설치됩니다. StorageGRID 시스템 컨테이너에서 이러한 패키지를 실행하면 AppArmor 프로필이 차단됩니다. DHCP, MySQL, NTP 및 tcdump 기본 패키지가 AppArmor와 충돌하고 다른 기본 패키지도 충돌할 수 있습니다.

AppArmor 프로필을 처리할 수 있는 두 가지 옵션이 있습니다.

- StorageGRID 시스템 컨테이너의 패키지와 겹치는 기본 시스템에 설치된 패키지의 개별 프로필을 비활성화합니다. 개별 프로필을 비활성화하면 AppArmor가 활성화되었음을 나타내는 항목이 StorageGRID 로그 파일에 나타납니다.

  다음 명령을 사용합니다.

  ```
  sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
  ```

- 예: *

  ```
  sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/bin.ping
  ```

- AppArmor를 모두 비활성화합니다. Ubuntu 9.10 이상의 경우 Ubuntu 온라인 커뮤니티의 지침을 따릅니다. "AppArmor를 비활성화합니다".

  AppArmor를 비활성화하면 AppArmor가 활성화되었음을 나타내는 항목이 StorageGRID 로그 파일에 나타나지 않습니다.

호스트 네트워크 구성**(Ubuntu** 또는 **Debian)**

호스트에서 Linux 설치를 완료한 후 나중에 배포할 StorageGRID 노드에 매핑하는 데 적합한 네트워크 인터페이스 세트를 준비하기 위해 몇 가지 추가 구성을 수행해야 할 수 있습니다.

필요한 것

- 을(를) 검토했습니다 StorageGRID 네트워킹 지침.

- 에 대한 정보를 검토했습니다 노드 컨테이너 마이그레이션 요구사항.
- 가상 호스트를 사용하는 경우 를 읽었습니다 MAC 주소 복제에 대한 고려 사항 및 권장 사항 호스트 네트워크를 구성하기 전에

> VM을 호스트로 사용하는 경우 가상 네트워크 어댑터로 VMXNET 3을 선택해야 합니다. VMware E1000 네트워크 어댑터로 인해 특정 Linux 배포판에 배포된 StorageGRID 컨테이너의 연결 문제가 발생했습니다.

이 작업에 대해

그리드 노드는 그리드 네트워크와 선택적으로 관리자 및 클라이언트 네트워크에 액세스할 수 있어야 합니다. 호스트의 물리적 인터페이스를 각 그리드 노드의 가상 인터페이스에 연결하는 매핑을 생성하여 이 액세스를 제공합니다. 호스트 인터페이스를 생성할 때 이름을 friendly 로 사용하여 모든 호스트에 쉽게 구축하고 마이그레이션을 설정할 수 있습니다.

호스트와 하나 이상의 노드 간에 동일한 인터페이스를 공유할 수 있습니다. 예를 들어, 호스트 액세스 및 노드 관리 네트워크 액세스에 동일한 인터페이스를 사용하여 호스트 및 노드 유지 관리를 용이하게 할 수 있습니다. 호스트와 개별 노드 간에 동일한 인터페이스를 공유할 수 있지만 모두 IP 주소가 서로 달라야 합니다. IP 주소는 노드 간 또는 호스트와 노드 간에 공유할 수 없습니다.

동일한 호스트 네트워크 인터페이스를 사용하여 호스트의 모든 StorageGRID 노드에 그리드 네트워크 인터페이스를 제공하거나, 각 노드에 대해 다른 호스트 네트워크 인터페이스를 사용하거나, 둘 사이에 작업을 수행할 수 있습니다. 그러나 일반적으로 단일 노드에 대한 Grid 및 Admin Network 인터페이스와 동일한 호스트 네트워크 인터페이스를 제공하거나 한 노드에 대한 Grid Network 인터페이스와 다른 노드에 대한 Client Network 인터페이스를 제공하지 않습니다.

이 작업은 여러 가지 방법으로 완료할 수 있습니다. 예를 들어, 호스트가 가상 머신이고 각 호스트에 대해 하나 또는 두 개의 StorageGRID 노드를 구축하는 경우 하이퍼바이저에서 올바른 수의 네트워크 인터페이스를 생성하고 일대일 매핑을 사용할 수 있습니다. 운영 용도로 베어 메탈 호스트에 여러 노드를 구축하는 경우 Linux 네트워킹 스택이 VLAN 및 LACP 지원을 활용하여 내결함성 및 대역폭 공유를 제공할 수 있습니다. 다음 섹션에서는 이러한 두 가지 예에 대해 자세히 설명합니다. 이러한 예제 중 하나를 사용할 필요가 없습니다. 필요에 맞는 방법을 사용할 수 있습니다.

> 연결 또는 브리지 장치를 컨테이너 네트워크 인터페이스로 직접 사용하지 마십시오. 이렇게 하면 컨테이너 네임스페이스의 연결 및 브리지 장치와 함께 MACVLAN을 사용하는 커널 문제로 인해 노드 시작이 방지될 수 있습니다. 대신 VLAN 또는 가상 이더넷(veth) 쌍과 같은 비연결 장치를 사용하십시오. 이 디바이스를 노드 구성 파일의 네트워크 인터페이스로 지정합니다.

MAC 주소 복제에 대한 고려 사항 및 권장 사항

MAC 주소 클로닝은 컨테이너가 호스트의 MAC 주소를 사용하고 호스트는 사용자가 지정한 주소나 임의로 생성된 주소의 MAC 주소를 사용하게 합니다. 무차별 모드 네트워크 구성을 사용하지 않으려면 MAC 주소 복제를 사용해야 합니다.

MAC 클론 생성 활성화

특정 환경에서는 관리 네트워크, 그리드 네트워크 및 클라이언트 네트워크에 전용 가상 NIC를 사용할 수 있으므로 MAC 주소 클로닝을 통해 보안을 강화할 수 있습니다. 컨테이너가 호스트에 있는 전용 NIC의 MAC 주소를 사용하도록 하면 무차별 모드 네트워크 구성을 사용하지 않도록 할 수 있습니다.

> MAC 주소 복제는 가상 서버 설치에 사용하기 위한 것이며 모든 물리적 어플라이언스 구성에서 제대로 작동하지 않을 수 있습니다.

> MAC 클론 대상 인터페이스가 사용 중이어서 노드가 시작되지 않는 경우 노드를 시작하기 전에 링크를 "다운"으로 설정해야 할 수 있습니다. 또한 링크가 작동 중일 때 가상 환경에서 네트워크 인터페이스에서 MAC 클로닝을 방지할 수 있습니다. 노드가 MAC 주소를 설정하지 못하고 사용 중인 인터페이스로 인해 시작되는 경우 노드를 시작하기 전에 링크를 "다운"으로 설정하면 문제가 해결될 수 있습니다.

MAC 주소 복제는 기본적으로 해제되어 있으며 노드 구성 키로 설정해야 합니다. StorageGRID를 설치할 때 활성화해야 합니다.

각 네트워크마다 하나의 키가 있습니다.

- 'admin_network_target_type_interface_clone_MAC'
- 'GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC
- 'client_network_target_type_interface_clone_MAC'

키를 "true"로 설정하면 컨테이너가 호스트 NIC의 MAC 주소를 사용하게 됩니다. 또한 호스트는 지정된 컨테이너 네트워크의 MAC 주소를 사용합니다. 기본적으로 컨테이너 주소는 임의로 생성된 주소이지만 '_network_mac' 노드 설정 키를 사용하여 설정한 경우에는 해당 주소가 대신 사용됩니다. 호스트와 컨테이너의 MAC 주소는 항상 다릅니다.

> 하이퍼바이저에서 무차별 모드를 설정하지 않고 가상 호스트에서 MAC 클로닝을 활성화하면 호스트의 인터페이스를 사용하는 Linux 호스트 네트워킹이 작동하지 않을 수 있습니다.

Mac 클론 복제 활용 사례

MAC 클로닝에는 다음 두 가지 사용 사례를 고려해야 합니다.

- MAC 클로닝이 활성화되지 않음: 노드 구성 파일의 '_clone_mac' 키가 설정되지 않았거나 "false"로 설정된 경우, 호스트는 호스트 NIC MAC을 사용하고 컨테이너는 "_network_mac" 키에 MAC이 지정되지 않은 경우 StorageGRID로 생성된 MAC을 갖게 됩니다. '_network_mac' 키에 주소가 설정되어 있으면 '_network_mac' 키에 지정된 주소가 컨테이너에 지정됩니다. 이러한 키 구성을 위해서는 무차별 모드를 사용해야 합니다.
- MAC 클론 생성 활성화: 노드 구성 파일의 '_clone_mac' 키가 "true"로 설정되면 컨테이너는 호스트 NIC MAC을 사용하고 호스트는 "_network_mac" 키에 MAC을 지정하지 않는 한 StorageGRID 생성 MAC을 사용합니다. '_network_mac' 키에 주소가 설정되어 있으면 호스트는 생성된 주소 대신 지정된 주소를 사용합니다. 이 키 구성에서 무차별 모드를 사용해서는 안 됩니다.

> MAC 주소 클로닝을 사용하지 않고 모든 인터페이스가 하이퍼바이저에 의해 할당된 것이 아닌 MAC 주소에 대한 데이터를 수신 및 전송하도록 허용하는 경우, 가상 스위치 및 포트 그룹 수준의 보안 속성이 Promiscuous Mode, MAC Address 변경 및 Forged 전송에 대해 * Accept * 로 설정되어 있는지 확인합니다. 가상 스위치에 설정된 값은 포트 그룹 수준의 값으로 재정의할 수 있으므로 두 위치에서 설정이 동일한지 확인합니다.

MAC 클로닝을 활성화하려면 를 참조하십시오 노드 구성 파일 생성 지침.

Mac 클론 복제의 예

인터페이스 ens256의 경우 MAC 주소가 11:22:33:44:55:66이고 노드 구성 파일의 경우 다음 키가 있는 호스트에서 활성화된 MAC 클론 복제의 예:

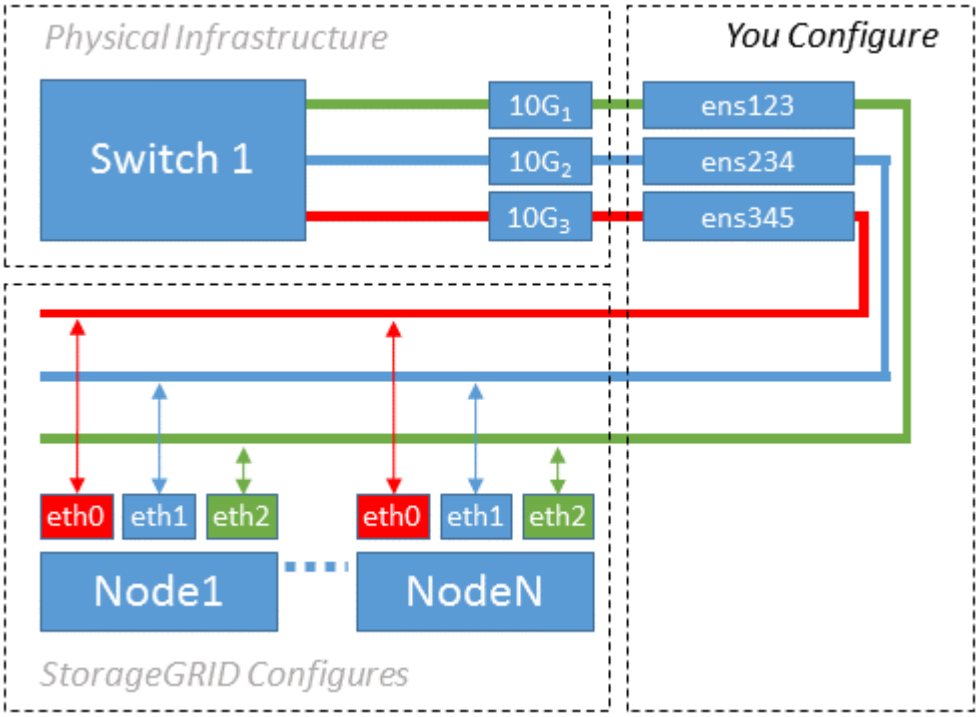
- 'admin_network_target=ens256'
- 'admin_network_MAC=B2:9c:02:C2:27:10'

- 'admin_network_target_type_interface_clone_MAC=TRUE'

결과: en256의 호스트 MAC은 B2:9c:02:C2:27:10이고 관리 네트워크 MAC은 11:22:33:44:55:66입니다

예 **1:** 물리적 **NIC** 또는 가상 **NIC**에 **1:1** 대 **1** 매핑

예제 1에서는 호스트측 구성이 거의 또는 전혀 필요하지 않은 간단한 물리적 인터페이스 매핑에 대해 설명합니다.



Linux 운영 체제는 설치 또는 부팅 중에 또는 인터페이스가 핫 애드 상태일 때 자동으로 ensXYZ 인터페이스를 생성합니다. 부팅 후 인터페이스가 자동으로 실행되도록 설정하는 것 외에는 구성이 필요하지 않습니다. 나중에 구성 프로세스에서 올바른 매핑을 제공할 수 있도록 StorageGRID 네트워크(그리드, 관리자 또는 클라이언트)에 해당하는 ensXYZ를 결정해야 합니다.

이 그림에서는 여러 StorageGRID 노드를 보여 줍니다. 그러나 일반적으로 단일 노드 VM에 이 구성을 사용합니다.

스위치 1이 물리적 스위치인 경우 액세스 모드에 대해 인터페이스 $10G_1$$10G_3$에 연결된 포트를 구성하고 해당 VLAN에 배치해야 합니다.

예 **2: VLAN**을 전달하는 **LACP** 결합

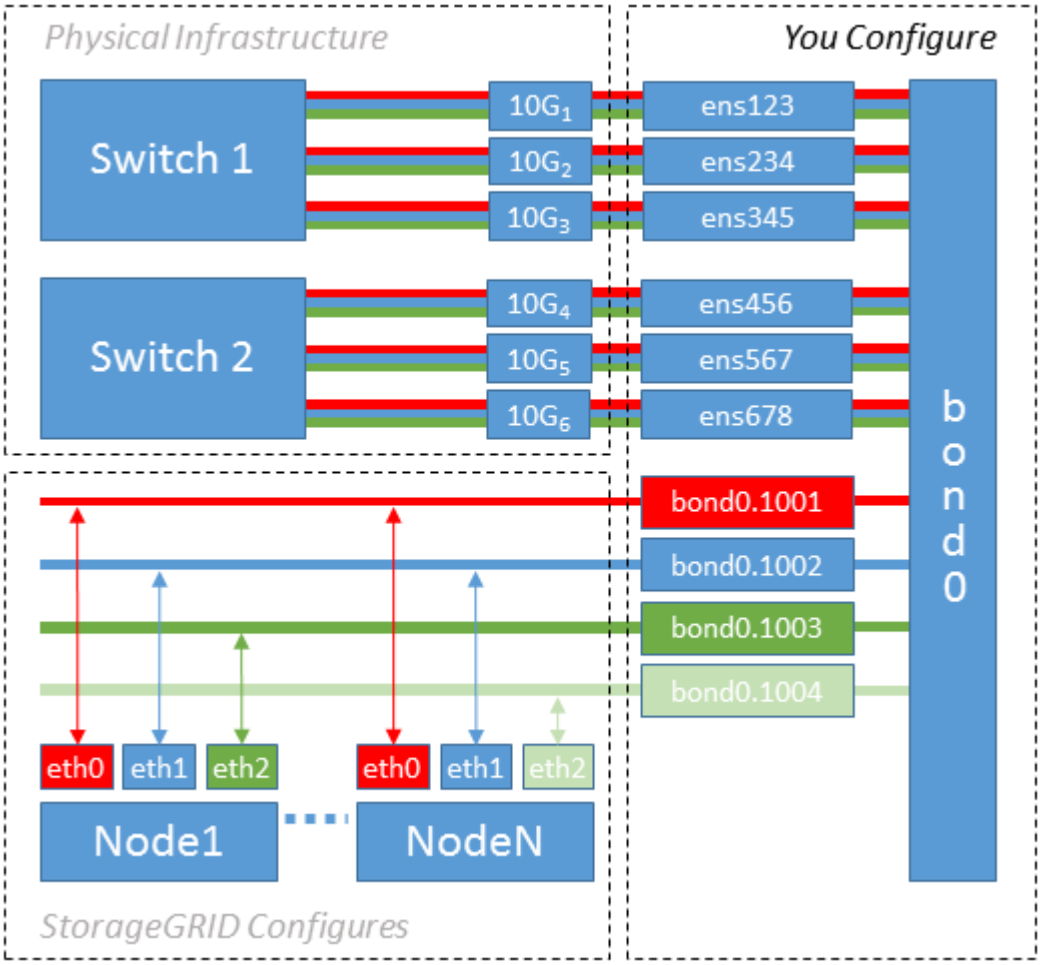
예제 2에서는 네트워크 인터페이스를 결합하거나 사용 중인 Linux 배포판에서 VLAN 인터페이스를 만드는 방법에 대해 잘 알고 있다고 가정합니다.

이 작업에 대해

예제 2에서는 단일 호스트의 모든 노드에서 사용 가능한 모든 네트워크 대역폭을 쉽게 공유할 수 있도록 지원하는 일반, 유연한 VLAN 기반 체계를 설명합니다. 이 예는 특히 베어 메탈 호스트에 적용할 수 있습니다.

이 예제를 이해하려면 각 데이터 센터에 그리드, 관리자 및 클라이언트 네트워크에 대한 세 개의 개별 서브넷이 있다고 가정합니다. 서브넷은 별도의 VLAN(1001, 1002 및 1003)에 있으며 LACP 결합 트렁크 포트(bond0)의 호스트에 제공됩니다. Bond.0.1001, bond0.1002 및 bond0.1003의 세 가지 VLAN 인터페이스를 구성합니다.

동일한 호스트에서 노드 네트워크에 대해 별도의 VLAN과 서브넷이 필요한 경우, 결합에 VLAN 인터페이스를 추가하고 이를 호스트에 매핑할 수 있습니다(그림에서 bond0.1004로 표시됨).



단계

1. StorageGRID 네트워크 연결에 사용할 모든 물리적 네트워크 인터페이스를 단일 LACP 결합으로 통합합니다.

   예를 들어, bond0과 같이 모든 호스트의 본드 결합에 동일한 이름을 사용합니다.

2. 표준 VLAN 인터페이스 명명 규칙인 physdev-name.vlan ID를 사용하여 이 결합을 연결된 "물리적 장치"로 사용하는 VLAN 인터페이스를 만듭니다.

   1단계와 2단계는 네트워크 링크의 다른 끝을 종료하는 에지 스위치에 적절한 구성이 필요합니다. 에지 스위치 포트도 LACP 포트 채널로 집계되고 트렁크로 구성되어 필요한 모든 VLAN을 통과할 수 있도록 허용해야 합니다.

   호스트별 네트워킹 구성 체계에 대한 샘플 인터페이스 구성 파일이 제공됩니다.

관련 정보

예 /etc/network/interfaces

호스트 스토리지를 구성합니다

각 호스트에 블록 스토리지 볼륨을 할당해야 합니다.

필요한 것

이 과제를 수행하는 데 필요한 정보를 제공하는 다음 주제를 검토했습니다.

요구사항을 충족해야 합니다

노드 컨테이너 마이그레이션 요구사항

이 작업에 대해

호스트에 블록 스토리지 볼륨(LUN)을 할당할 때는 "스토리지 요구 사항"의 표를 사용하여 다음 사항을 확인하십시오.

- 각 호스트에 필요한 볼륨 수(해당 호스트에 구축할 노드 수 및 유형 기준)
- 각 볼륨의 스토리지 범주(즉, 시스템 데이터 또는 오브젝트 데이터)
- 각 볼륨의 크기입니다

호스트에 StorageGRID 노드를 배포할 때 이 정보와 Linux가 각 물리적 볼륨에 할당한 영구 이름을 사용합니다.

> 이러한 볼륨을 파티션, 포맷 또는 마운트할 필요가 없습니다. 호스트가 볼 수 있도록 해야 합니다.

볼륨 이름 목록을 작성할 때 ""raw"" 특수 장치 파일("/dev/sdb" 등)을 사용하지 마십시오. 이러한 파일은 호스트의 재부팅 시 변경될 수 있으며, 이는 시스템의 올바른 작동에 영향을 줍니다. iSCSI LUN 및 장치 매퍼 다중 경로를 사용하는 경우, 특히 SAN 토폴로지에 공유 스토리지에 대한 중복 네트워크 경로가 포함된 경우 "/dev/mapper" 디렉토리에 다중 경로 별칭을 사용하는 것이 좋습니다. 또는 영구 디바이스 이름에 대해 '/dev/disk/by-path/' 아래에 있는 시스템 생성 소프트링크를 사용할 수 있습니다.

예를 들면 다음과 같습니다.

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

각 설치 환경에 따라 결과가 달라집니다.

각 블록 스토리지 볼륨에 알기 쉬운 이름을 할당하여 초기 StorageGRID 설치 및 향후 유지 관리 절차를 간소화하십시오. 공유 스토리지 볼륨에 대한 중복 액세스를 위해 장치 매퍼 다중 경로 드라이버를 사용하는 경우,

'/etc/multipath.conf' 파일에서 "alias" 필드를 사용할 수 있습니다.

예를 들면 다음과 같습니다.

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

이렇게 하면 별칭이 호스트의 '/dev/mapper' 디렉토리에 블록 디바이스로 표시되므로 구성 또는 유지 관리 작업에서 블록 스토리지 볼륨을 지정해야 할 때마다 친숙하고 유효성이 검증된 이름을 지정할 수 있습니다.

> StorageGRID 노드 마이그레이션을 지원하고 장치 매퍼 다중 경로를 사용하도록 공유 스토리지를 설정하는 경우 모든 동일 위치에 있는 호스트에 공통 '/etc/multipath.conf'를 생성하고 설치할 수 있습니다. 각 호스트에서 다른 Docker 스토리지 볼륨을 사용하기만 하면 됩니다. 각 Docker 스토리지 볼륨 LUN의 별칭에 타겟 호스트 이름을 포함하여 별칭을 사용하면 기억하기 쉽고 이 방법이 권장됩니다.

관련 정보

요구사항을 충족해야 합니다

Docker 스토리지 볼륨을 구성합니다

Docker를 설치하기 전에 Docker 스토리지 볼륨을 포맷하고 이를 '/var/lib/docker'에 마운트해야 할 수 있습니다.

이 작업에 대해

Docker 스토리지 볼륨에 로컬 스토리지를 사용할 계획이고 '/var/lib'가 포함된 호스트 파티션에 충분한 공간이 있는 경우 이 단계를 건너뛸 수 있습니다.

단계

1. Docker 스토리지 볼륨에 파일 시스템을 생성합니다.

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Docker 스토리지 볼륨을 마운트합니다.

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

3. /etc/fstab에 Docker-storage-volume-device 항목을 추가합니다.

   이 단계를 수행하면 호스트가 재부팅된 후 스토리지 볼륨이 자동으로 다시 마운트됩니다.

Docker를 설치합니다

StorageGRID 시스템은 Linux에서 Docker 컨테이너 모음으로 실행됩니다. StorageGRID를 설치하기 전에 Docker를 설치해야 합니다.

단계

1. Linux 배포에 대한 지침에 따라 Docker를 설치합니다.

   Docker가 Linux 배포판에 포함되어 있지 않은 경우 Docker 웹 사이트에서 다운로드할 수 있습니다.

2. 다음 두 명령을 실행하여 Docker를 활성화하고 시작했는지 확인합니다.

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. 다음을 입력하여 예상 버전의 Docker를 설치했는지 확인합니다.

```
sudo docker version
```

클라이언트 및 서버 버전은 1.11.0 이상이어야 합니다.

관련 정보

호스트 스토리지를 구성합니다

StorageGRID 호스트 서비스를 설치합니다

StorageGRID DEB 패키지를 사용하여 StorageGRID 호스트 서비스를 설치합니다.

이 작업에 대해

이 지침은 DEB 패키지에서 호스트 서비스를 설치하는 방법을 설명합니다. 또는 설치 아카이브에 포함된 APT 리포지토리 메타데이터를 사용하여 DEB 패키지를 원격으로 설치할 수 있습니다. Linux 운영 체제에 대한 APT 리포지토리 지침을 참조하십시오.

단계

1. 각 호스트에 StorageGRID DEB 패키지를 복사하거나 공유 스토리지에서 사용할 수 있도록 설정합니다.

   예를 들어, 다음 단계에서 예제 명령을 사용할 수 있도록 이 명령을 `/tmp' 디렉토리에 배치합니다.

2. 각 호스트에 루트로 로그인하거나 sudo 권한이 있는 계정을 사용하여 다음 명령을 실행합니다.

   먼저 이미지 패키지를 설치하고 서비스 패키지를 다시 설치해야 합니다. 패키지를 '/tmp' 이외의 디렉토리에 배치한 경우 사용한 경로를 반영하도록 명령을 수정합니다.

```
sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
```

> StorageGRID 패키지를 설치하기 전에 Python 2.7이 이미 설치되어 있어야 합니다. 'SUDO dpkg — install /tmp/storagegrid-webscale-images-version-SHA.deb` 명령은 작업을 완료할 때까지 실패합니다.

가상 그리드 노드 배포(**Ubuntu** 또는 **Debian**)

Ubuntu 또는 **Debian** 배포용 노드 구성 파일을 만듭니다

노드 구성 파일은 StorageGRID 호스트 서비스에서 노드를 시작하고 적절한 네트워크 및 블록 스토리지 리소스에 연결하는 데 필요한 정보를 제공하는 작은 텍스트 파일입니다. 노드 구성 파일은 가상 노드에 사용되며 어플라이언스 노드에는 사용되지 않습니다.

노드 구성 파일은 어디에 배치합니까?

노드가 실행될 호스트의 '/etc/StorageGrid/nodes' 디렉토리에 각 StorageGRID 노드의 구성 파일을 배치해야 합니다. 예를 들어 HostA에서 관리 노드 1개, 게이트웨이 노드 1개 및 스토리지 노드 1개를 실행하려는 경우 HostA의 '/etc/StorageGrid//nodes'에 노드 구성 파일 3개를 배치해야 합니다. vim 또는 nano와 같은 텍스트 편집기를 사용하여 각 호스트에서 직접 구성 파일을 만들거나 다른 곳에서 구성 파일을 만들어 각 호스트로 이동할 수 있습니다.

노드 구성 파일의 이름은 무엇입니까?

구성 파일의 이름이 중요합니다. node-name.conf 형식이며, 여기서 node-name은 노드에 할당하는 이름입니다. 이 이름은 StorageGRID Installer에 나타나며 노드 마이그레이션과 같은 노드 유지 관리 작업에 사용됩니다.

노드 이름은 다음 규칙을 따라야 합니다.

- 고유해야 합니다
- 문자로 시작해야 합니다
- A ~ Z 및 a ~ z 문자를 포함할 수 있습니다
- 0에서 9 사이의 숫자를 포함할 수 있습니다
- 하나 이상의 하이픈(-)을 포함할 수 있습니다.
- '.conf' 확장자는 포함되지 않고 32자 이하여야 합니다

이러한 명명 규칙을 따르지 않는 '/etc/StorageGrid/nodes'의 파일은 호스트 서비스에서 구문 분석되지 않습니다.

그리드에 대해 멀티 사이트 토폴로지를 계획한 경우 일반적인 노드 명명 규칙은 다음과 같습니다.

```
site-nodetype-nodenumber.conf
```

예를 들어 데이터 센터 1의 첫 번째 관리 노드에 dC1-adm1.conf를 사용하고 데이터 센터 2의 세 번째 스토리지 노드에 대해 dC2-SN3.conf를 사용할 수 있습니다. 그러나 모든 노드 이름이 명명 규칙을 따른다 하더라도 원하는 스키마를 사용할 수 있습니다.

노드 구성 파일이란 무엇입니까?

구성 파일에는 키/값 쌍이 포함되어 있으며, 한 줄에 하나의 키와 하나의 값이 있습니다. 각 키/값 쌍에 대해 다음 규칙을 따라야 합니다.

- 키와 값은 등호('=')와 선택적 공백으로 구분해야 합니다.
- 키에는 공백이 포함될 수 없습니다.
- 값에는 포함된 공백이 포함될 수 있습니다.
- 선행 또는 후행 공백은 무시됩니다.

일부 키는 모든 노드에 대해 필요하지만, 일부 키는 선택 사양이거나 특정 노드 유형에만 필요합니다.

이 표는 지원되는 모든 키에 대해 허용되는 값을 정의합니다. 가운데 열:

- R *: 필수 + BP: 모범 사례 + O: 선택 사항

키	**R, BP** 또는 **O?**	값
관리_IP	BP	이 노드가 속한 그리드에 대한 운영 관리 노드의 Grid Network IPv4 주소입니다. node_type=VM_Admin_Node 및 admin_role=Primary를 사용하는 그리드 노드에 대해 GRID_NETWORK_IP에 지정한 것과 동일한 값을 사용합니다. 이 매개 변수를 생략하면 노드가 mDNS를 사용하여 기본 관리 노드를 검색합니다. 그리드 노드가 기본 관리자 노드를 검색하는 방법 • 참고 *: 이 값은 기본 관리 노드에서 무시되고 금지될 수 있습니다.
관리 네트워크 구성	o	DHCP, 정적 또는 비활성
관리_네트워크_ESL	o	쉼표로 구분된 서브넷 목록으로, 이 노드가 Admin Network 게이트웨이를 통해 통신해야 하는 CIDR 표기법을 사용합니다. 예: 172.16.0.0/21,172.17.0.0/21
Admin_network_Gateway를 선택합니다	O(* R *)	이 노드에 대한 로컬 관리 네트워크 게이트웨이의 IPv4 주소입니다. admin_network_ip 및 admin_network_mask에 의해 정의된 서브넷에 있어야 합니다. DHCP 구성 네트워크에서는 이 값이 무시됩니다. • 참고 *: admin_network_ESL이 지정된 경우 이 매개 변수가 필요합니다. 예: 1.1.1.1 10.224.4.81
admin_network_ip을 선택합니다	o	관리 네트워크에서 이 노드의 IPv4 주소입니다. 이 키는 admin_network_Config = static인 경우에만 필요합니다. 다른 값에 대해서는 지정하지 마십시오. 예: 1.1.1.1 10.224.4.81

키	**R, BP** 또는 **O?**	값
admin_network_MAC입니다	o	컨테이너의 관리 네트워크 인터페이스에 대한 MAC 주소입니다. 이 필드는 선택 사항입니다. 생략할 경우 MAC 주소가 자동으로 생성됩니다. 콜론으로 구분된 6쌍의 16진수 숫자이어야 합니다. 예: 'B2:9c:02:C2:27:10'
admin_network_mask를 선택합니다	o	이 노드의 IPv4 넷마스크는 관리자 네트워크에서 설정합니다. 이 키는 admin_network_Config = static인 경우에만 필요합니다. 다른 값에 대해서는 지정하지 마십시오. 예: 255.255.255.0 255.255.248.0
admin_network_mtu	o	Admin Network의 이 노드에 대한 MTU(Maximum Transmission Unit)입니다. admin_network_Config = DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 이 인수를 생략하면 1500이 사용됩니다. 점보 프레임을 사용하려면 MTU를 9000과 같은 점보 프레임에 적합한 값으로 설정합니다. 그렇지 않으면 기본값을 유지합니다. • 중요 *: 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다. 예: 1500입니다 8192

키	**R, BP** 또는 **O?**	값
admin_network_target 을 선택합니다	BP	StorageGRID 노드에서 관리자 네트워크 액세스에 사용할 호스트 디바이스의 이름입니다. 네트워크 인터페이스 이름만 지원됩니다. 일반적으로 GRID_NETWORK_TARGET 또는 CLIENT_NETWORK_TARGET에 지정된 것과 다른 인터페이스 이름을 사용합니다. • 참고 *: 네트워크 대상으로 연결 또는 브리지 장치를 사용하지 마십시오. 연결 디바이스 위에 VLAN(또는 기타 가상 인터페이스)을 구성하거나 브리지 및 가상 이더넷(veth) 쌍을 사용합니다. • 모범 사례 *: 이 노드에 처음에 관리 네트워크 IP 주소가 없을 경우에도 값을 지정하십시오. 그런 다음 나중에 호스트에서 노드를 다시 구성하지 않고도 관리 네트워크 IP 주소를 추가할 수 있습니다. 예: 속박 0.1002 펜스256
admin_network_target_type입니다	o	인터페이스 (지원되는 유일한 값입니다.)
admin_network_target_type_interface_clone_MAC	BP	참 또는 거짓 StorageGRID 컨테이너가 관리자 네트워크에서 호스트 호스트 대상 인터페이스의 MAC 주소를 사용하도록 하려면 키를 "true"로 설정합니다. • 모범 사례: * promiscuous 모드가 필요한 네트워크에서는 admin_network_target_type_interface_clone_MAC 키를 대신 사용합니다. MAC 클로닝에 대한 자세한 내용: MAC 주소 복제에 대한 고려 사항 및 권장 사항(Red Hat Enterprise Linux 또는 CentOS) MAC 주소 복제에 대한 고려 사항 및 권장 사항(Ubuntu 또는 Debian)
admin_role을 선택합니다	• R *	Primary 또는 Non-Primary입니다 이 키는 node_type = VM_Admin_Node인 경우에만 필요하며 다른 노드 유형에 대해서는 지정하지 마십시오.

키	**R, BP** 또는 **O?**	값
Block_device_audit_logs	• R *	이 노드가 감사 로그의 영구 저장에 사용할 블록 디바이스 특수 파일의 경로 및 이름입니다. 이 키는 node_type=vm_Admin_Node인 노드에만 필요하며 다른 노드 유형에 대해서는 지정하지 마십시오. 예: '/dev/disk/by-path/PCI-0000:03:00.0 - SCSI-0:0:0:0:0:0' '/dev/disk/by-id/WWN-0x600a09800059d6df000060d757b475fd' '/dev/mapper/SGWs-adm1-audit-logs'

키	R, BP 또는 O?	값
Block_device_RANGEDB_000 BLOCK_DEVICE_RANGEDB_001 Block_device_RANGEDB_002 Block_device_RANGEDB_003 Block_device_RANGEDB_004 BLOCK_DEVICE_RANGEDB_005 BLOCK_DEVICE_RANGEDB_006 BLOCK_DEVICE_RANGEDB_007 Block_device_RANGEDB_008 Block_device_RANGEDB_009 BLOCK_DEVICE_RANGEDB_010 BLOCK_DEVICE_RANGEDB_011 BLOCK_DEVICE_RANGEDB_012 BLOCK_DEVICE_RANGEDB_013 BLOCK_DEVICE_RANGEDB_014 Block_device_RANGEDB_015	• R *	이 노드가 영구 오브젝트 스토리지에 사용할 블록 디바이스 특수 파일의 경로 및 이름입니다. 이 키는 node_type=vm_Storage_Node인 노드에만 필요하며 다른 노드 유형에 대해서는 지정하지 마십시오. block_device_RANGEDB_000 만 필요하며 나머지는 선택 사항입니다. block_device_RANGEDB_000 에 지정된 블록 디바이스는 4TB 이상이어야 하며 다른 블록 디바이스는 더 작을 수 있습니다. 간격을 두지 마십시오. BLOCK_DEVICE_RANGEDB_005를 지정하는 경우 BLOCK_DEVICE_RANGEDB_004도 지정해야 합니다. • 참고 *: 기존 배포와의 호환성을 위해 업그레이드된 노드에 대해 2자리 키가 지원됩니다. 예: '/dev/disk/by-path/PCI-0000:03:00.0 - SCSI-0:0:0:0:0:0' '/dev/disk/by-id/WWN-0x600a09800059d6df000060d757b475fd' '/dev/mapper/SGWs-sn1-rangedb-000'

키	**R, BP** 또는 **O?**	값
BLOCK_DEVICE_Tables	• R *	이 노드가 데이터베이스 테이블의 영구 저장에 사용할 블록 디바이스 특수 파일의 경로 및 이름입니다. 이 키는 node_type=vm_Admin_Node인 노드에만 필요하며 다른 노드 유형에 대해서는 지정하지 마십시오. 예: '/dev/disk/by-path/PCI-0000:03:00.0 - SCSI-0:0:0:0:0:0' '/dev/disk/by-id/WWN-0x600a09800059d6df000060d757b475fd' '/dev/mapper/SGWs-adm1-tables'
BLOCK_DEVICE_VAR_LOCAL	• R *	이 노드가 해당 /var/local 영구 스토리지에 사용할 블록 디바이스 특수 파일의 경로 및 이름입니다. 예: '/dev/disk/by-path/PCI-0000:03:00.0 - SCSI-0:0:0:0:0:0' '/dev/disk/by-id/WWN-0x600a09800059d6df000060d757b475fd' '/dev/mapper/SGWS-sn1-var-local'
client_network_Config	o	DHCP, 정적 또는 비활성
CLIENT_NETWORK_GATEWAY	o	client_network_ip 및 client_network_mask에 의해 정의된 서브넷에 있어야 하는 이 노드에 대한 로컬 클라이언트 네트워크 게이트웨이의 IPv4 주소입니다. DHCP 구성 네트워크에서는 이 값이 무시됩니다. 예: 1.1.1.1 10.224.4.81
client_network_ip	o	클라이언트 네트워크에서 이 노드의 IPv4 주소입니다. 이 키는 client_network_Config = static 일 때만 필요합니다. 다른 값에 대해서는 지정하지 마십시오. 예: 1.1.1.1 10.224.4.81

키	**R, BP** 또는 **O?**	값
client_network_MAC	o	컨테이너에 있는 클라이언트 네트워크 인터페이스의 MAC 주소입니다. 이 필드는 선택 사항입니다. 생략할 경우 MAC 주소가 자동으로 생성됩니다. 콜론으로 구분된 6쌍의 16진수 숫자이어야 합니다. 예: 'B2:9c:02:C2:27:20
client_network_mask.(클라이언트 네트워크 마스크	o	클라이언트 네트워크의 이 노드에 대한 IPv4 넷마스크입니다. 이 키는 client_network_Config = static 일 때만 필요합니다. 다른 값에 대해서는 지정하지 마십시오. 예: 255.255.255.0 255.255.248.0
client_network_mtu	o	Client Network의 이 노드에 대한 MTU(Maximum Transmission Unit)입니다. client_network_Config = DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 이 인수를 생략하면 1500이 사용됩니다. 점보 프레임을 사용하려면 MTU를 9000과 같은 점보 프레임에 적합한 값으로 설정합니다. 그렇지 않으면 기본값을 유지합니다. • 중요 *: 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다. 예: 1500입니다 8192

키	**R, BP 또는 O?**	값
client_network_target 을 선택합니다	BP	StorageGRID 노드에서 클라이언트 네트워크 액세스에 사용할 호스트 디바이스의 이름입니다. 네트워크 인터페이스 이름만 지원됩니다. 일반적으로 GRID_NETWORK_TARGET 또는 ADMIN_NETWORK_TARGET에 지정된 것과 다른 인터페이스 이름을 사용합니다. • 참고 *: 네트워크 대상으로 연결 또는 브리지 장치를 사용하지 마십시오. 연결 디바이스 위에 VLAN(또는 기타 가상 인터페이스)을 구성하거나 브리지 및 가상 이더넷(veth) 쌍을 사용합니다. • 모범 사례: * 이 노드에 클라이언트 네트워크 IP 주소가 없을 경우에도 값을 지정하십시오. 그런 다음 나중에 호스트에서 노드를 다시 구성하지 않고도 클라이언트 네트워크 IP 주소를 추가할 수 있습니다. 예: 속박 0.1003 엔스423
CLIENT_NETWORK_TARGET_TYPE	o	인터페이스 (이 값은 지원되는 값일 뿐입니다.)
client_network_target_type_interface_clone_MAC	BP	참 또는 거짓 StorageGRID 컨테이너가 클라이언트 네트워크의 호스트 대상 인터페이스의 MAC 주소를 사용하도록 하려면 키를 "true"로 설정합니다. • 모범 사례: * promiscuous 모드가 필요한 네트워크에서는 대신 client_network_target_type_interface_clone_mac 키를 사용합니다. MAC 클로닝에 대한 자세한 내용: MAC 주소 복제에 대한 고려 사항 및 권장 사항(Red Hat Enterprise Linux 또는 CentOS) MAC 주소 복제에 대한 고려 사항 및 권장 사항(Ubuntu 또는 Debian)
GRID_NETWORK_CONFIG(그리드 네트워크 구성	BP	고정 또는 DHCP (지정되지 않은 경우 기본값은 static)

키	**R, BP** 또는 **O?**	값
GRID_NETWORK_Gateway를 참조하십시오	• R *	GRID_NETWORK_IP 및 GRID_NETWORK_MASK로 정의된 서브넷에 있어야 하는 이 노드에 대한 로컬 Grid Network 게이트웨이의 IPv4 주소입니다. DHCP 구성 네트워크에서는 이 값이 무시됩니다. 그리드 네트워크가 게이트웨이가 없는 단일 서브넷인 경우, 서브넷(X. Y.Z.1)의 표준 게이트웨이 주소 또는 이 노드의 GRID_NETWORK_IP 값을 사용합니다. 두 값 중 하나를 사용하면 미래의 그리드 네트워크 확장이 단순화됩니다.
GRID_NETWORK_IP입니다	• R *	Grid Network에서 이 노드의 IPv4 주소입니다. 이 키는 GRID_NETWORK_CONFIG = static 일 때만 필요합니다. 다른 값에 대해서는 지정하지 마십시오. 예: 1.1.1.1 10.224.4.81
GRID_NETWORK_MAC을 선택합니다	o	컨테이너의 그리드 네트워크 인터페이스에 대한 MAC 주소입니다. 이 필드는 선택 사항입니다. 생략할 경우 MAC 주소가 자동으로 생성됩니다. 콜론으로 구분된 6쌍의 16진수 숫자이어야 합니다. 예: 'B2:9c:02:C2:27:30
GRID_NETWORK_MASK 를 참조하십시오	o	그리드 네트워크에서 이 노드에 대한 IPv4 넷마스크입니다. 이 키는 GRID_NETWORK_CONFIG = static 일 때만 필요합니다. 다른 값에 대해서는 지정하지 마십시오. 예: 255.255.255.0 255.255.248.0

키	**R, BP** 또는 **O?**	값
GRID_NETWORK_MTU 를 참조하십시오	o	Grid Network의 이 노드에 대한 MTU(Maximum Transmission Unit)입니다. GRID_NETWORK_CONFIG=DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 이 인수를 생략하면 1500이 사용됩니다. 점보 프레임을 사용하려면 MTU를 9000과 같은 점보 프레임에 적합한 값으로 설정합니다. 그렇지 않으면 기본값을 유지합니다. • 중요 *: 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다. • 중요 *: 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다. 예: 1,500 8192
GRID_NETWORK_TARGET	• R *	StorageGRID 노드에서 그리드 네트워크 액세스에 사용할 호스트 디바이스의 이름입니다. 네트워크 인터페이스 이름만 지원됩니다. 일반적으로 admin_network_target 또는 client_network_target 에 지정된 것과 다른 인터페이스 이름을 사용합니다. • 참고 *: 네트워크 대상으로 연결 또는 브리지 장치를 사용하지 마십시오. 연결 디바이스 위에 VLAN(또는 기타 가상 인터페이스)을 구성하거나 브리지 및 가상 이더넷(veth) 쌍을 사용합니다. 예: 속박 0.1001 ens192
GRID_NETWORK_TARGET_TYPE	o	인터페이스 (지원되는 유일한 값입니다.)

키	**R, BP** 또는 **O?**	값
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	• BP *	참 또는 거짓 StorageGRID 컨테이너가 그리드 네트워크에서 호스트 대상 인터페이스의 MAC 주소를 사용하도록 키 값을 "true"로 설정합니다. • 모범 사례: * promiscuous 모드가 필요한 네트워크에서는 grid_network_target_type_interface_clone_mac 키를 대신 사용합니다. MAC 클로닝에 대한 자세한 내용: MAC 주소 복제에 대한 고려 사항 및 권장 사항(Red Hat Enterprise Linux 또는 CentOS) MAC 주소 복제에 대한 고려 사항 및 권장 사항(Ubuntu 또는 Debian)
Interfaces_target_nnnn	o	이 노드에 추가할 추가 인터페이스의 이름 및 선택적 설명입니다. 각 노드에 여러 개의 인터페이스를 추가할 수 있습니다. nnnn_의 경우 추가하려는 각 interface_target 항목에 대해 고유 번호를 지정하십시오. 값에 대해 베어 메탈 호스트의 물리적 인터페이스 이름을 지정합니다. 그런 다음 필요에 따라 쉼표를 추가하고 인터페이스에 대한 설명을 입력합니다. 이 설명은 VLAN 인터페이스 페이지와 HA 그룹 페이지에 표시됩니다. 예: 'interfaces_target_01=en256, Trunk' 트렁크 인터페이스를 추가하는 경우 StorageGRID에서 VLAN 인터페이스를 구성해야 합니다. 액세스 인터페이스를 추가할 경우 인터페이스를 HA 그룹에 직접 추가할 수 있으며, VLAN 인터페이스를 구성할 필요가 없습니다.

키	**R, BP** 또는 **O?**	값
최대 RAM	o	이 노드가 사용할 수 있는 최대 RAM 양입니다. 이 키를 생략하면 노드의 메모리 제한 사항이 없게 됩니다. 운영 레벨 노드에 대해 이 필드를 설정할 때 총 시스템 RAM보다 최소 24GB 및 16 ~ 32GB 적은 값을 지정합니다. • 참고 *: RAM 값은 노드의 실제 메타데이터 예약 공간에 영향을 줍니다. 를 참조하십시오 StorageGRID 관리 지침 메타데이터 예약된 공간에 대한 설명은 을 참조하십시오. 이 필드의 형식은 '<number><unit>'이며 여기서 '<unit>'는 'b', 'k', 'mb', 'g'가 될 수 있습니다. 예: 24g 38654705664b • 참고 *: 이 옵션을 사용하려면 메모리 cgroup에 대한 커널 지원을 활성화해야 합니다.
node_type입니다	• R *	노드 유형: VM_Admin_Node VM_Storage_Node VM_Archive_Node VM_API_Gateway
port_remap 을 참조하십시오	o	노드에서 내부 그리드 노드 통신 또는 외부 통신을 위해 사용하는 모든 포트를 다시 매핑합니다. "내부 그리드 노드 통신" 또는 "외부 통신"에서 설명한 대로 엔터프라이즈 네트워킹 정책이 StorageGRID에서 사용하는 하나 이상의 포트를 제한하는 경우 포트를 재매핑해야 합니다. • 중요 *: 로드 밸런서 엔드포인트를 구성하기 위해 사용하려는 포트를 다시 매핑하지 마십시오. • 참고 *: port_remap 만 설정된 경우 지정하는 매핑이 인바운드 및 아웃바운드 통신 모두에 사용됩니다. port_remap_inbound 도 지정된 경우 port_remap 은 아웃바운드 통신에만 적용됩니다. 사용되는 형식은 "<네트워크 유형>/<프로토콜>/<그리드 노드에 사용되는 기본 포트>/<새 포트>"입니다. 여기서 "<네트워크 유형>"은 그리드, 관리자 또는 클라이언트이고 프로토콜은 TCP 또는 UDP입니다. 예를 들면 다음과 같습니다. 'port_remap=client/tcp/18082/443'

키	R, BP 또는 O?	값
port_remap_inbound 를 참조하십시오	o	인바운드 통신을 지정된 포트에 다시 매핑합니다. port_remap_inbound 를 지정하지만 port_remap 의 값을 지정하지 않으면 포트의 아웃바운드 통신이 변경되지 않습니다. • 중요 *: 로드 밸런서 엔드포인트를 구성하기 위해 사용하려는 포트를 다시 매핑하지 마십시오. 사용되는 형식은 "<network type>/<protocol:>/<remapped port>/<default port used by grid node>"이며 여기서 "<network type>"은 그리드, 관리자 또는 클라이언트이고 프로토콜은 TCP 또는 UDP입니다. 예를 들면 다음과 같습니다. 'PORT_REmap_INbound=GRID/TCP/3022/22'

관련 정보

네트워킹 지침

그리드 노드가 기본 관리자 노드를 검색하는 방법

그리드 노드는 구성 및 관리를 위해 기본 관리 노드와 통신합니다. 각 그리드 노드는 그리드 네트워크에 있는 기본 관리 노드의 IP 주소를 알아야 합니다.

그리드 노드가 기본 관리 노드에 액세스할 수 있도록 노드를 배포할 때 다음 중 하나를 수행할 수 있습니다.

- admin_ip 매개 변수를 사용하여 기본 관리 노드의 IP 주소를 수동으로 입력할 수 있습니다.
- admin_ip 매개 변수를 생략하여 그리드 노드가 값을 자동으로 검색하도록 할 수 있습니다. 자동 검색은 그리드 네트워크가 DHCP를 사용하여 기본 관리 노드에 IP 주소를 할당할 때 특히 유용합니다.

운영 관리자 노드의 자동 검색은 멀티캐스트 도메인 이름 시스템(mDNS)을 사용하여 수행됩니다. 운영 관리 노드가 처음 시작되면 mDNS를 사용하여 해당 IP 주소를 게시합니다. 그런 다음 동일한 서브넷에 있는 다른 노드에서 IP 주소를 쿼리하고 자동으로 가져올 수 있습니다. 그러나 멀티캐스트 IP 트래픽은 일반적으로 서브넷 간에 라우팅할 수 없기 때문에 다른 서브넷의 노드는 기본 관리 노드의 IP 주소를 직접 획득할 수 없습니다.

> 자동 검색을 사용하는 경우:
>
> - 기본 관리 노드가 직접 연결되지 않은 서브넷에 있는 하나 이상의 그리드 노드에 대해 admin_IP 설정을 포함해야 합니다. 이 그리드 노드는 mDNS로 검색할 서브넷의 다른 노드에 대한 기본 관리 노드의 IP 주소를 게시합니다.
> - 네트워크 인프라스트럭처가 서브넷 내의 다중 캐스트 IP 트래픽 전달을 지원하는지 확인합니다.

노드 구성 파일의 예

예제 노드 구성 파일을 사용하여 StorageGRID 시스템의 노드 구성 파일을 설정할 수 있습니다. 이 예제에서는 모든 유형의 그리드 노드에 대한 노드 구성 파일을 보여 줍니다.

대부분의 노드의 경우 그리드 관리자 또는 설치 API를 사용하여 그리드를 구성할 때 관리 및 클라이언트 네트워크 주소 지정 정보(IP, 마스크, 게이트웨이 등)를 추가할 수 있습니다. 기본 관리 노드는 예외입니다. 그리드 네트워크가 라우팅되지 않는 등의 이유로 기본 관리 노드의 관리 네트워크 IP를 탐색하여 그리드 구성을 완료하려면 노드 구성 파일에서 기본 관리 노드에 대한 관리 네트워크 연결을 구성해야 합니다. 이 예제는 에 나와 있습니다.

> 이 예에서는 클라이언트 네트워크가 기본적으로 비활성화되어 있더라도 클라이언트 네트워크 타겟이 모범 사례로 구성되었습니다.

기본 관리자 노드의 예

- 파일 이름 예 *: `/etc/StorageGrid/nodes/dc1-adm1.conf'
- 파일 내용 예: *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

스토리지 노드의 예

- 파일 이름 예: * ``etc/StorageGrid/nodes/dc1-sn1.conf'
- 파일 내용 예: *

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

아카이브 노드의 예

- 파일 이름 예: * ``etc/StorageGrid/nodes/dc1-arc1.conf'
- 파일 내용 예: *

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

게이트웨이 노드의 예

- 파일 이름 예: * ``etc/StorageGrid/nodes/dc1-gw1.conf'
- 파일 내용 예: *

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

운영 관리자 노드가 아닌 노드의 예

- 파일 이름 예: * ``etc/StorageGrid/nodes/dc1-adm2.conf'
- 파일 내용 예: *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

StorageGRID 구성을 검증합니다

각 StorageGRID 노드에 대해 '/etc/StorageGrid/nodes'에서 구성 파일을 생성한 후 해당 파일의 내용을 확인해야 합니다.

구성 파일의 내용을 확인하려면 각 호스트에서 다음 명령을 실행합니다.

```
sudo storagegrid node validate all
```

파일이 올바른 경우, 예제에 표시된 대로 각 구성 파일에 대해 * Passed * 가 출력됩니다.

```
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
```

> 자동 설치의 경우 StorageGRID 명령(예: StorageGRID—quiet…)에서 '-q' 또는 '--quiet' 옵션을 사용하여 이 출력을 억제할 수 있습니다. 출력을 표시하지 않으면 구성 경고 또는 오류가 감지된 경우 명령에 0이 아닌 종료 값이 있는 것입니다.

구성 파일이 잘못된 경우, 이 예에서와 같이 문제가 * warning * 및 * error * 로 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 노드를 시작하고 호스트를 재부팅한 후 다시 시작하려면 StorageGRID 호스트 서비스를 설정하고 시작해야 합니다.

단계

1. 각 호스트에서 다음 명령을 실행합니다.

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. 다음 명령을 실행하여 구축이 진행되고 있는지 확인합니다.

```
sudo storagegrid node status node-name
```

"not running" 또는 "scope" 상태를 반환하는 노드에 대해 다음 명령을 실행합니다.

```
sudo storagegrid node start node-name
```

3. 이전에 StorageGRID 호스트 서비스를 설정 및 시작한 경우(또는 서비스가 활성화 및 시작되었는지 확실하지 않은 경우) 다음 명령을 실행합니다.

```
sudo systemctl reload-or-restart storagegrid
```

그리드 구성 및 전체 설치(Ubuntu 또는 Debian)

그리드 관리자로 이동합니다

그리드 관리자를 사용하여 StorageGRID 시스템을 구성하는 데 필요한 모든 정보를 정의합니다.

필요한 것

기본 관리 노드를 구축하고 초기 시작 시퀀스를 완료해야 합니다.

단계

1. 웹 브라우저를 열고 다음 주소 중 하나로 이동합니다.

```
https://primary_admin_node_ip

client_network_ip
```

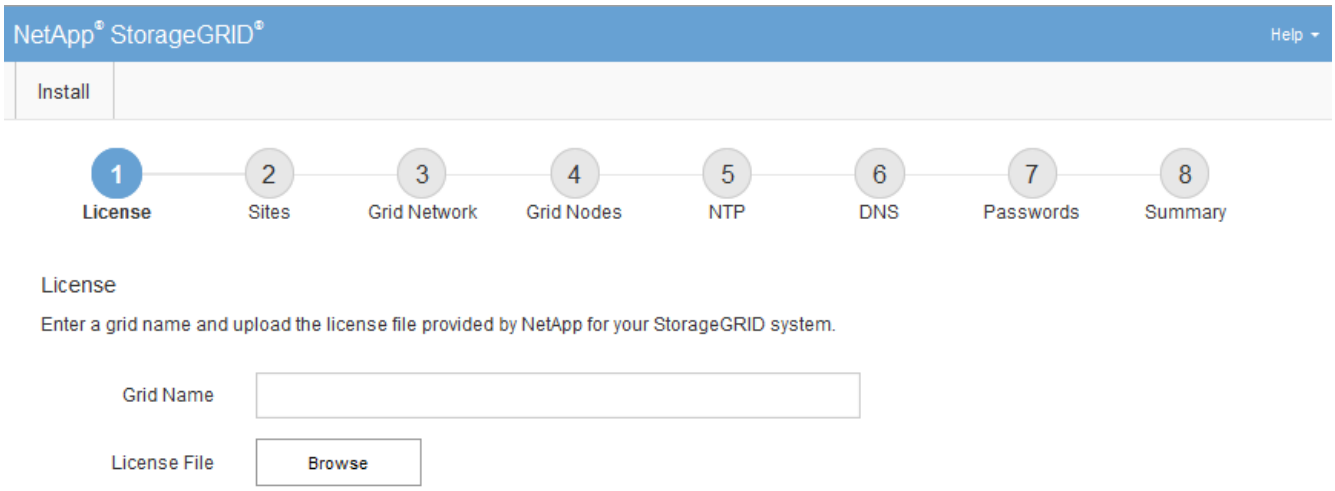
또는 포트 8443에서 그리드 관리자에 액세스할 수 있습니다.

```
https://primary_admin_node_ip:8443
```

> 네트워크 구성에 따라 그리드 네트워크 또는 관리 네트워크의 기본 관리 노드 IP에 대한 IP 주소를 사용할 수 있습니다.

1. StorageGRID 시스템 설치 * 를 클릭합니다.

   StorageGRID 그리드를 구성하는 데 사용되는 페이지가 나타납니다.



StorageGRID 라이센스 정보를 지정합니다

StorageGRID 시스템의 이름을 지정하고 NetApp에서 제공하는 라이센스 파일을 업로드해야 합니다.

단계

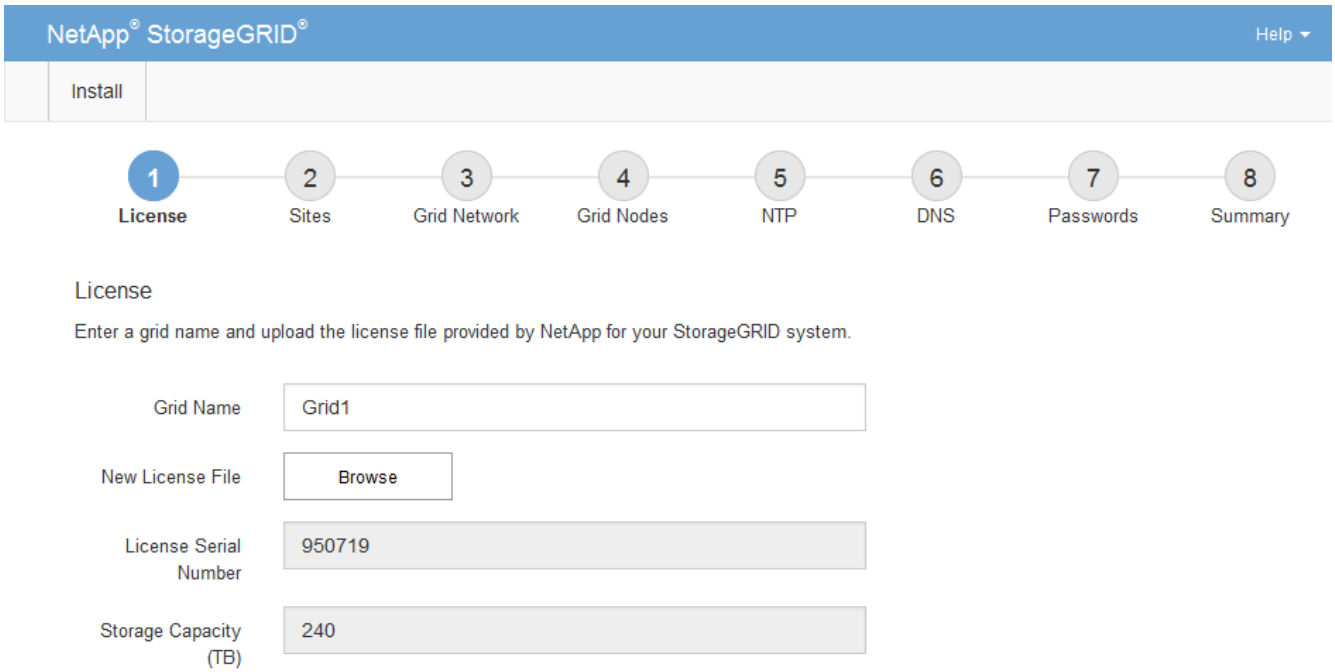
1. 라이센스 페이지의 * 그리드 이름 * 에 StorageGRID 시스템에 대한 의미 있는 이름을 입력합니다.

   설치 후, 이름이 Nodes 메뉴 맨 위에 표시됩니다.

2. 찾아보기 * 를 클릭하고 NetApp 라이센스 파일('NLFunique_id.txt')을 찾은 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.



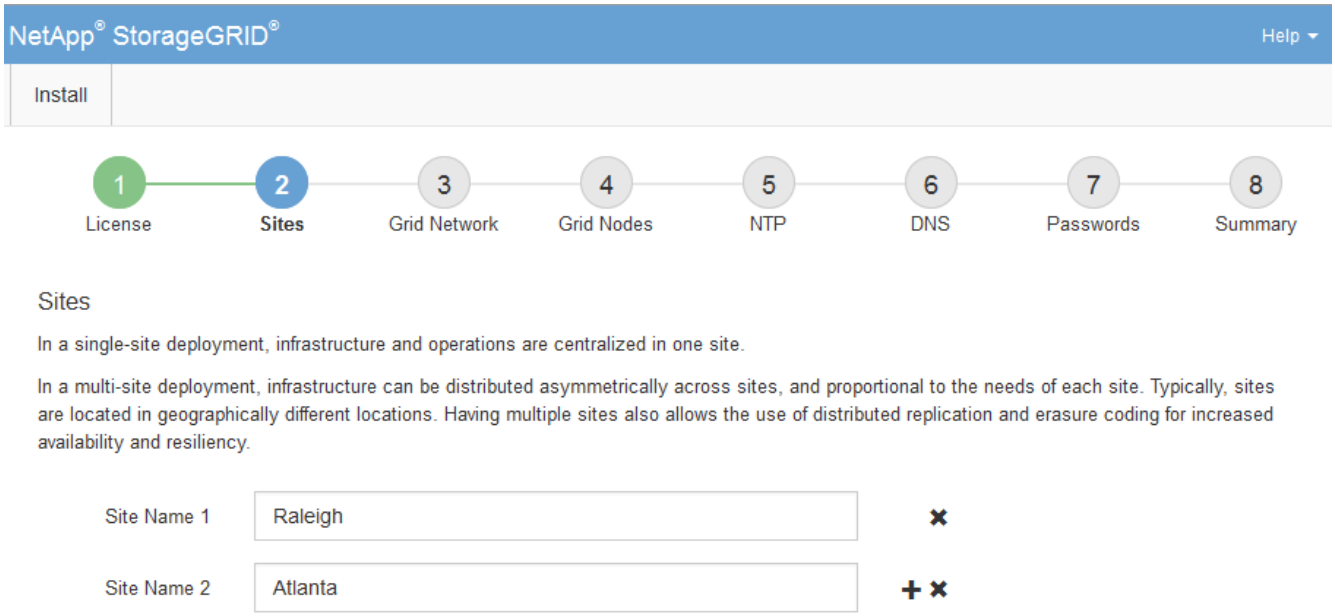
3. 다음 * 을 클릭합니다.

사이트를 추가합니다

StorageGRID를 설치할 때 사이트를 하나 이상 만들어야 합니다. StorageGRID 시스템의 안정성과 스토리지 용량을 늘리기 위해 사이트를 추가로 생성할 수 있습니다.

1. 사이트 페이지에서 * 사이트 이름 * 을 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.

그리드 네트워크 서브넷을 지정합니다

그리드 네트워크에서 사용되는 서브넷을 지정해야 합니다.

이 작업에 대해

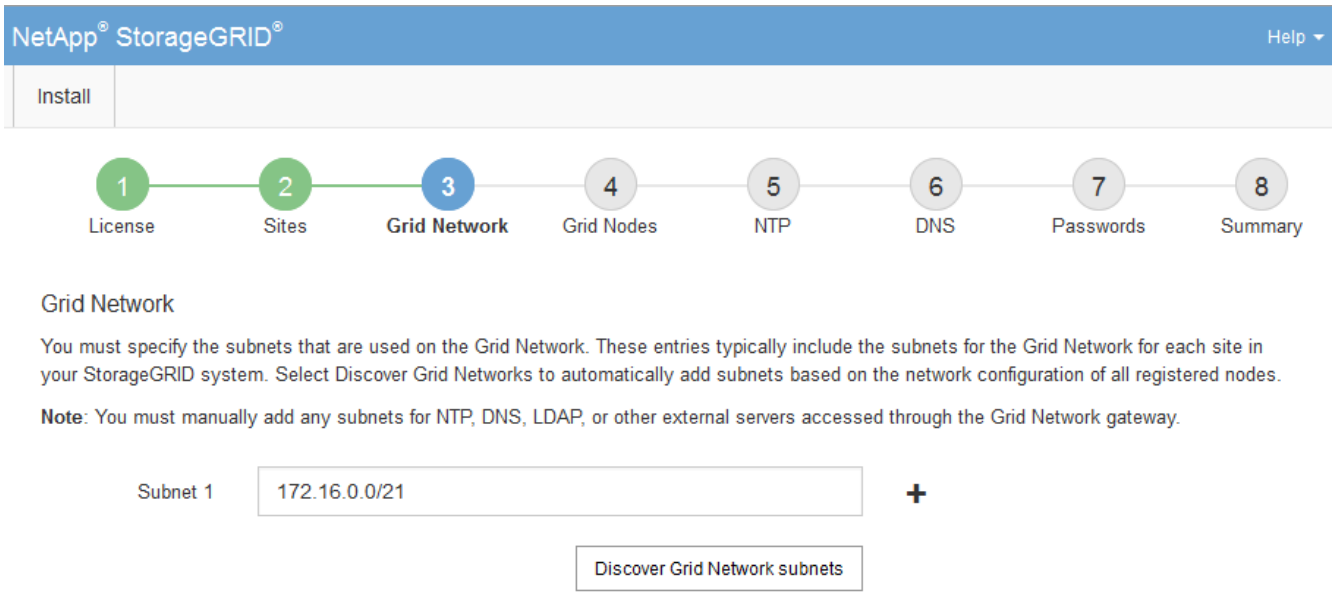
서브넷 항목에는 그리드 네트워크를 통해 연결할 수 있어야 하는 서브넷과 함께 StorageGRID 시스템의 각 사이트에 대한 그리드 네트워크의 서브넷이 포함됩니다.

그리드 서브넷이 여러 개인 경우 그리드 네트워크 게이트웨이가 필요합니다. 지정된 모든 그리드 서브넷은 이 게이트웨이를 통해 연결할 수 있어야 합니다.

단계

1. 서브넷 1 * 텍스트 상자에 하나 이상의 그리드 네트워크에 대한 CIDR 네트워크 주소를 지정합니다.
2. 마지막 항목 옆에 있는 더하기 기호를 클릭하여 추가 네트워크 항목을 추가합니다.

   하나 이상의 노드를 이미 배포한 경우 * 그리드 네트워크 서브넷 검색 * 을 클릭하여 그리드 관리자에 등록된 그리드 노드에 의해 보고된 서브넷으로 그리드 네트워크 서브넷 목록을 자동으로 채웁니다.



3. 다음 * 을 클릭합니다.

보류 중인 그리드 노드를 승인합니다

StorageGRID 시스템에 가입하려면 각 그리드 노드를 승인해야 합니다.

필요한 것

모든 가상 및 StorageGRID 어플라이언스 그리드 노드를 구축했습니다.

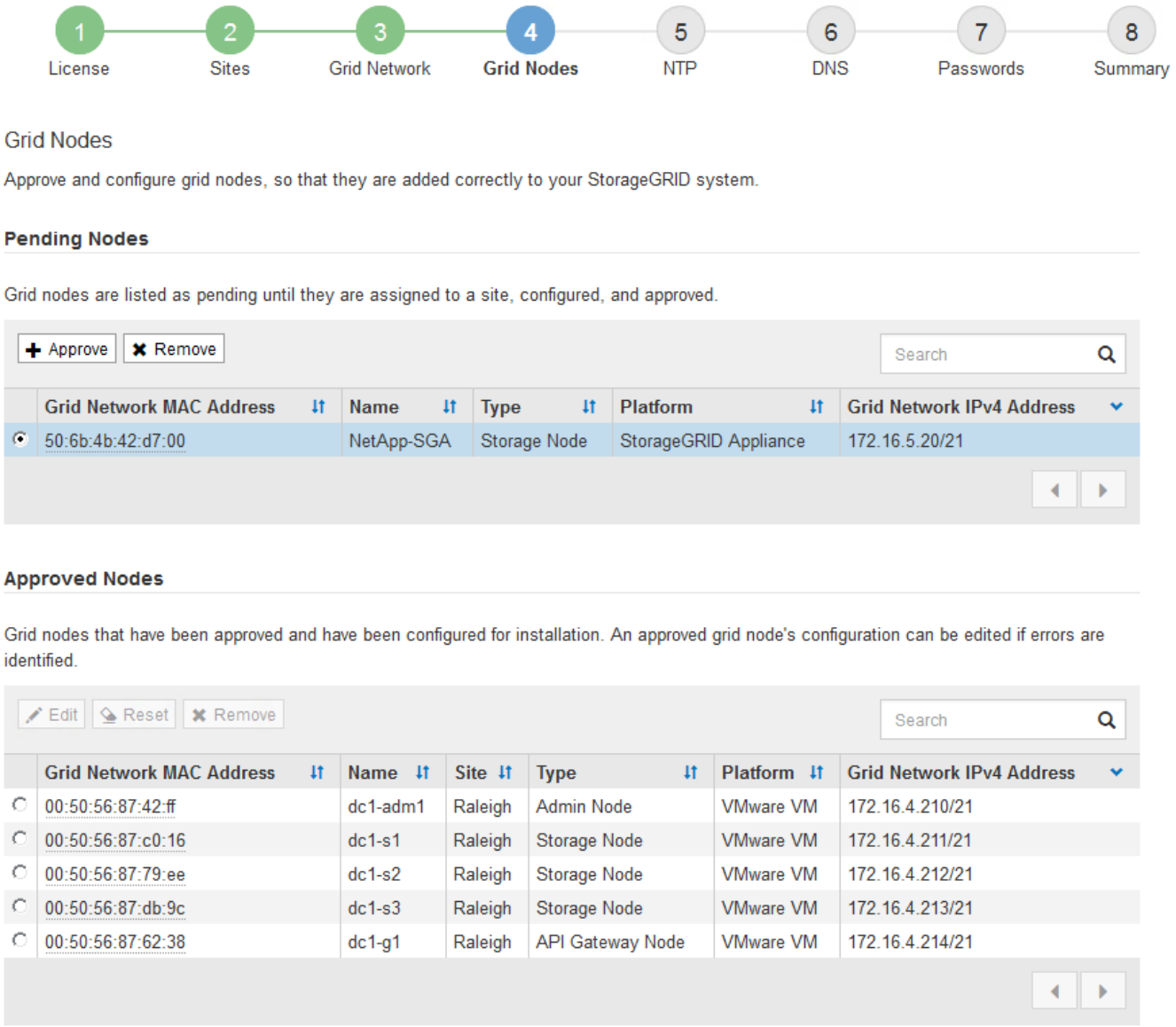
> 일부 노드를 나중에 설치하는 대신 모든 노드를 한 번 설치하는 것이 더 효율적입니다.

단계

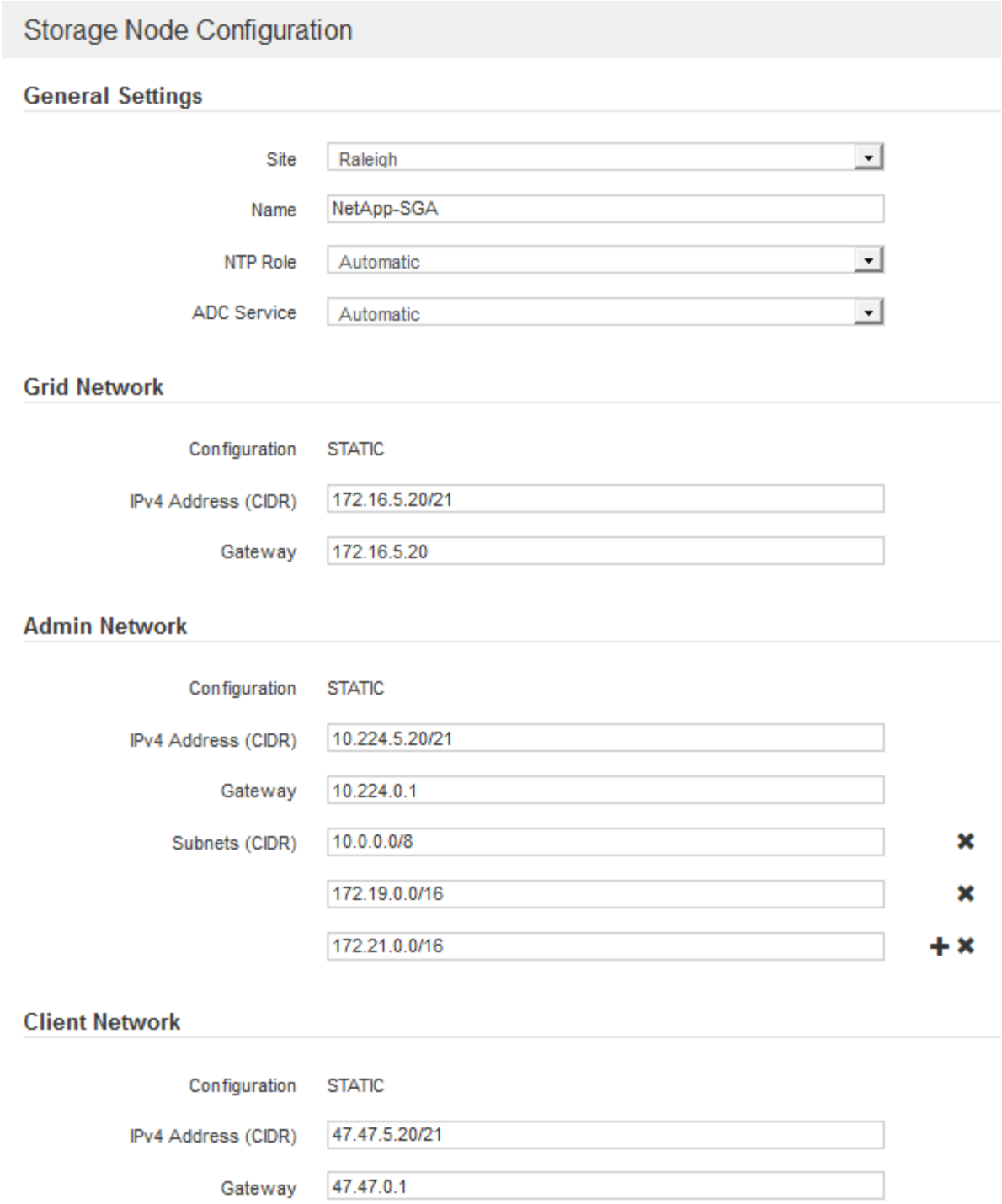
1. Pending Nodes(보류 중인 노드) 목록을 검토하고 배포된 모든 그리드 노드가 표시되는지 확인합니다.

   > 그리드 노드가 누락된 경우 성공적으로 배포되었는지 확인합니다.

2. 승인하려는 보류 중인 노드 옆에 있는 라디오 버튼을 선택합니다.



3. Approve * (승인 *)를 클릭합니다.
4. 일반 설정에서 필요에 따라 다음 속성의 설정을 수정합니다.



- * Site *: 이 그리드 노드가 연결될 사이트의 이름입니다.
- * 이름 *: 노드에 할당될 이름 및 그리드 관리자에 표시될 이름입니다. 기본적으로 노드를 구성할 때 지정한 이름이 지정됩니다. 설치 프로세스의 이 단계에서 필요에 따라 이름을 변경할 수 있습니다.

> 설치를 완료한 후에는 노드 이름을 변경할 수 없습니다.

> VMware 노드의 경우 여기에서 이름을 변경할 수 있지만 이 작업은 vSphere에서 가상 머신의 이름을 변경하지 않습니다.

- * NTP 역할 *: 그리드 노드의 NTP(Network Time Protocol) 역할입니다. 옵션은 * 자동 *, * 기본 * 및 * 클라이언트 * 입니다. Automatic * 을 선택하면 기본 역할이 관리 노드, ADC 서비스가 있는 스토리지 노드, 게이트웨이 노드 및 비정적 IP 주소가 있는 모든 그리드 노드에 할당됩니다. 다른 모든 그리드 노드에는 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 노드 전용): 시스템에서 노드가 관리 도메인 컨트롤러(ADC) 서비스를 필요로 하는지 여부를 결정하도록 하려면 * 자동 * 을 선택합니다. ADC 서비스는 그리드 서비스의 위치 및 가용성을 추적합니다. 각 사이트에 적어도 3개의 스토리지 노드가 ADC 서비스를 포함해야 합니다. ADC 서비스를 배포한 후에는 노드에 추가할 수 없습니다.

5. Grid Network에서 필요에 따라 다음 속성의 설정을 수정합니다.

   - * IPv4 주소(CIDR) *: 그리드 네트워크 인터페이스(컨테이너 내부의 eth0)의 CIDR 네트워크 주소입니다. 예: 192.168.1.234/21
   - * 게이트웨이 *: 그리드 네트워크 게이트웨이. 예: 192.168.0.1

     그리드 서브넷이 여러 개인 경우 게이트웨이가 필요합니다.

     > 그리드 네트워크 구성에 대해 DHCP를 선택하고 여기서 값을 변경하면 새 값이 노드의 정적 주소로 구성됩니다. 결과 IP 주소가 DHCP 주소 풀 내에 있지 않은지 확인해야 합니다.

6. 그리드 노드에 대해 관리자 네트워크를 구성하려면 필요에 따라 관리 네트워크 섹션에서 설정을 추가하거나 업데이트합니다.

   이 인터페이스에서 나오는 라우트의 대상 서브넷을 * 서브넷(CIDR) * 텍스트 상자에 입력합니다. 관리 서브넷이 여러 개인 경우 관리 게이트웨이가 필요합니다.

   > Admin Network 구성에 대해 DHCP를 선택하고 여기서 값을 변경하면 새 값이 노드의 정적 주소로 구성됩니다. 결과 IP 주소가 DHCP 주소 풀 내에 있지 않은지 확인해야 합니다.

   - 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. 어플라이언스 재부팅: 어플라이언스 설치 프로그램에서 * 고급 * > * 재부팅 * 을 선택합니다.

        재부팅하는 데 몇 분 정도 걸릴 수 있습니다.

     b. 네트워크 구성 * > * 링크 구성 * 을 선택하고 해당 네트워크를 활성화합니다.

     c. 네트워킹 구성 * > * IP 구성 * 을 선택하고 활성화된 네트워크를 구성합니다.

     d. 홈 페이지로 돌아가서 * 설치 시작 * 을 클릭합니다.

     e. Grid Manager(그리드 관리자): 노드가 Approved Nodes(승인된 노드) 테이블에 나열된 경우 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.

   클라이언트 네트워크 구성에 대해 DHCP를 선택하고 여기서 값을 변경하면 새 값이 노드의 정적 주소로 구성됩니다. 결과 IP 주소가 DHCP 주소 풀 내에 있지 않은지 확인해야 합니다.

   - 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. 어플라이언스 재부팅: 어플라이언스 설치 프로그램에서 * 고급 * > * 재부팅 * 을 선택합니다.

        재부팅하는 데 몇 분 정도 걸릴 수 있습니다.

     b. 네트워크 구성 * > * 링크 구성 * 을 선택하고 해당 네트워크를 활성화합니다.

     c. 네트워킹 구성 * > * IP 구성 * 을 선택하고 활성화된 네트워크를 구성합니다.

     d. 홈 페이지로 돌아가서 * 설치 시작 * 을 클릭합니다.

     e. Grid Manager(그리드 관리자): 노드가 Approved Nodes(승인된 노드) 테이블에 나열된 경우 노드를 재설정합니다.

     f. Pending Nodes 테이블에서 노드를 제거합니다.

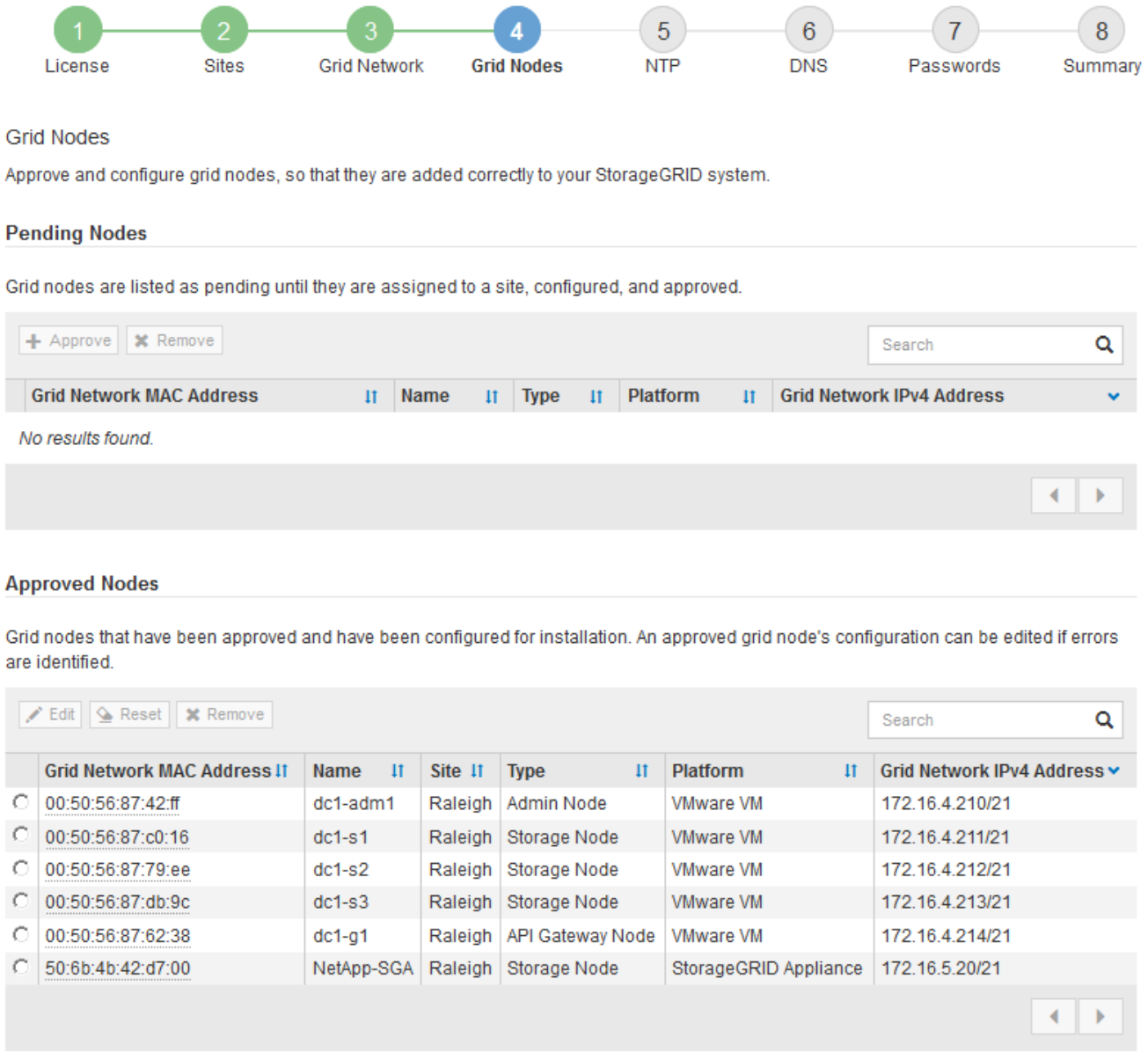
     g. 대기 중인 노드 목록에 노드가 다시 나타날 때까지 기다립니다.

     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. 승인하려는 보류 중인 각 그리드 노드에 대해 이 단계를 반복합니다.

   그리드에서 원하는 모든 노드를 승인해야 합니다. 그러나 요약 페이지에서 * 설치 * 를 클릭하기 전에 언제든지 이 페이지로 돌아갈 수 있습니다. 라디오 버튼을 선택하고 * Edit * 를 클릭하여 승인된 그리드 노드의 속성을 수정할 수 있습니다.

10. 그리드 노드 승인이 완료되면 * 다음 * 을 클릭합니다.

Network Time Protocol 서버 정보를 지정합니다

StorageGRID 시스템에 대해 NTP(네트워크 시간 프로토콜) 구성 정보를 지정해야 별도의 서버에서 수행되는 작업을 동기화할 수 있습니다.

이 작업에 대해

NTP 서버의 IPv4 주소를 지정해야 합니다.

외부 NTP 서버를 지정해야 합니다. 지정된 NTP 서버는 NTP 프로토콜을 사용해야 합니다.

시간 드리프트와 관련된 문제를 방지하려면 Stratum 3 이상의 NTP 서버 참조를 4개 지정해야 합니다.

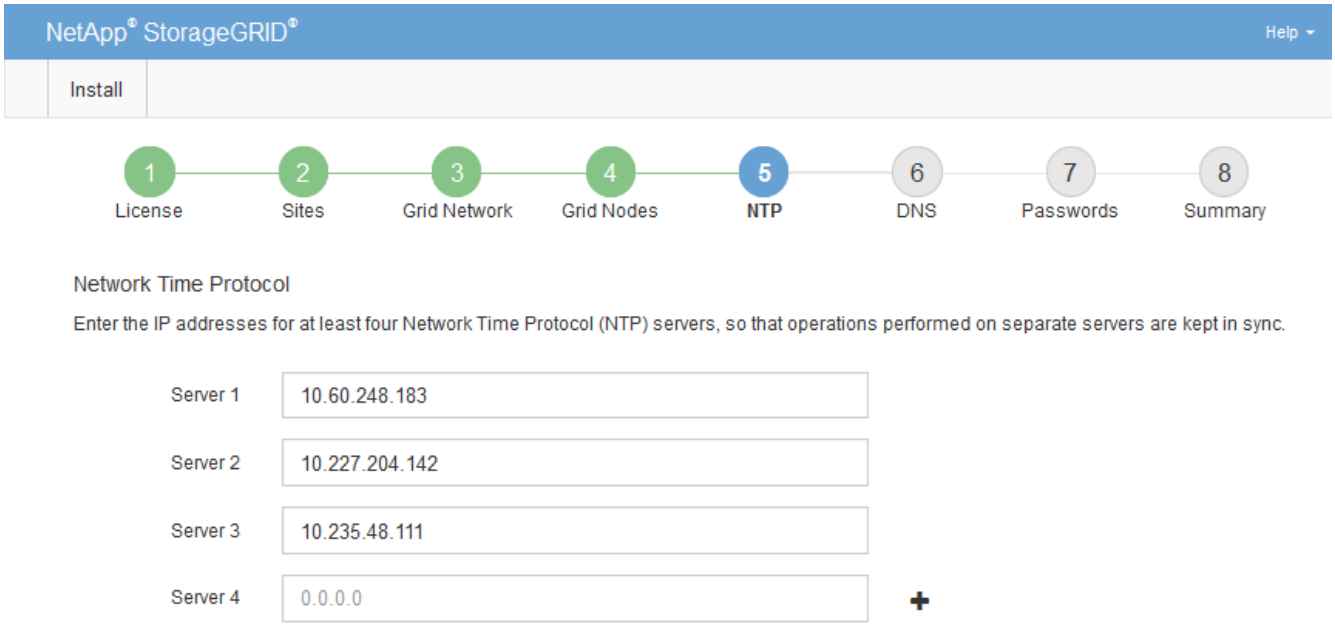
> 프로덕션 수준 StorageGRID 설치에 외부 NTP 소스를 지정할 때 Windows Server 2016 이전 버전의 Windows에서는 Windows 시간(W32Time) 서비스를 사용하지 마십시오. 이전 버전의 Windows의 시간 서비스는 정확하지 않으며 StorageGRID와 같은 고정밀 환경에서 사용하기 위해 Microsoft에서 지원되지 않습니다.
>
> "정확도가 높은 환경에 대한 Windows 시간 서비스를 구성하기 위한 경계를 지원합니다"

외부 NTP 서버는 이전에 기본 NTP 역할을 할당한 노드에서 사용됩니다.

> 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.

단계

1. Server 1 * 에서 * Server 4 * 텍스트 상자에 NTP 서버 4대 이상에 대한 IPv4 주소를 지정합니다.
2. 필요한 경우 마지막 항목 옆에 있는 더하기 기호를 선택하여 추가 서버 항목을 추가합니다.



3. 다음 * 을 선택합니다.

관련 정보

네트워킹 지침

도메인 이름 시스템 서버 정보를 지정합니다

IP 주소 대신 호스트 이름을 사용하여 외부 서버에 액세스할 수 있도록 StorageGRID 시스템에 대한 DNS(도메인 이름 시스템) 정보를 지정해야 합니다.

이 작업에 대해

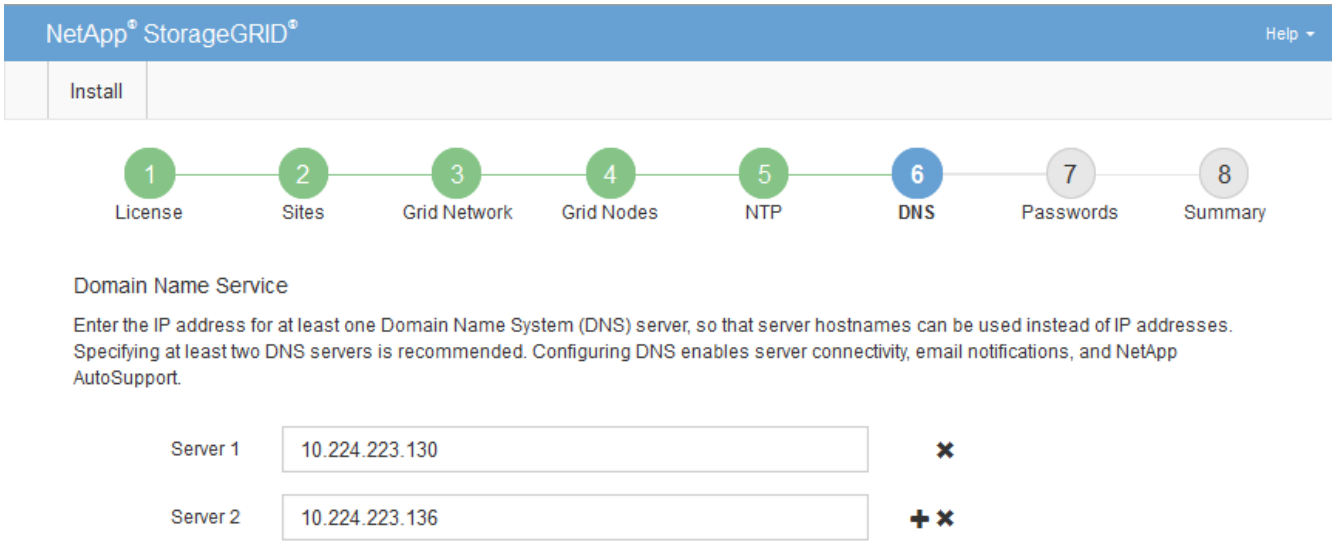
DNS 서버 정보를 지정하면 e-메일 알림 및 AutoSupport에 IP 주소 대신 FQDN(정규화된 도메인 이름) 호스트 이름을 사용할 수 있습니다. DNS 서버를 두 개 이상 지정하는 것이 좋습니다.

> DNS 서버에 2-6개의 IPv4 주소를 제공합니다. 네트워크 연결 시 각 사이트에서 로컬로 액세스할 수 있는 DNS 서버를 선택해야 합니다. 이는 Is착륙한 사이트가 계속해서 DNS 서비스에 액세스할 수 있도록 하기 위한 것입니다. 그리드 전체 DNS 서버 목록을 구성한 후 각 노드에 대해 DNS 서버 목록을 추가로 사용자 지정할 수 있습니다. 자세한 내용은 복구 및 유지 관리 지침 에서 DNS 구성 수정에 대한 정보를 참조하십시오.

DNS 서버 정보가 생략되거나 잘못 구성된 경우 각 그리드 노드의 SSM 서비스에서 NST 알람이 트리거됩니다. DNS가 올바르게 구성되고 새 서버 정보가 모든 그리드 노드에 도달하면 경보가 해제됩니다.

단계

1. Server 1 * 텍스트 상자에 하나 이상의 DNS 서버에 대한 IPv4 주소를 지정합니다.
2. 필요한 경우 마지막 항목 옆에 있는 더하기 기호를 선택하여 추가 서버 항목을 추가합니다.



   가장 좋은 방법은 DNS 서버를 두 개 이상 지정하는 것입니다. 최대 6개의 DNS 서버를 지정할 수 있습니다.

3. 다음 * 을 선택합니다.

StorageGRID 시스템 암호를 지정합니다

StorageGRID 시스템을 설치하는 과정에서 시스템 보안을 유지하고 유지 관리 작업을 수행하는 데 사용할 암호를 입력해야 합니다.

이 작업에 대해

암호 설치 페이지를 사용하여 프로비저닝 암호 및 그리드 관리 루트 사용자 암호를 지정합니다.

- 프로비저닝 암호는 암호화 키로 사용되며 StorageGRID 시스템에 저장되지 않습니다.
- 복구 패키지 다운로드를 포함하여 설치, 확장 및 유지 관리 절차를 위한 프로비저닝 암호가 있어야 합니다. 따라서 프로비저닝 암호를 안전한 위치에 저장하는 것이 중요합니다.
- 현재 프로비저닝 암호가 있는 경우 Grid Manager에서 프로비저닝 암호를 변경할 수 있습니다.

- 그리드 관리 루트 사용자 암호는 Grid Manager를 사용하여 변경할 수 있습니다.
- 임의로 생성된 명령줄 콘솔 및 SSH 암호는 복구 패키지의 Passwords.txt 파일에 저장됩니다.

단계

1. Provisioning Passphrase * 에서 StorageGRID 시스템의 그리드 토폴로지를 변경하는 데 필요한 프로비저닝 암호를 입력합니다.

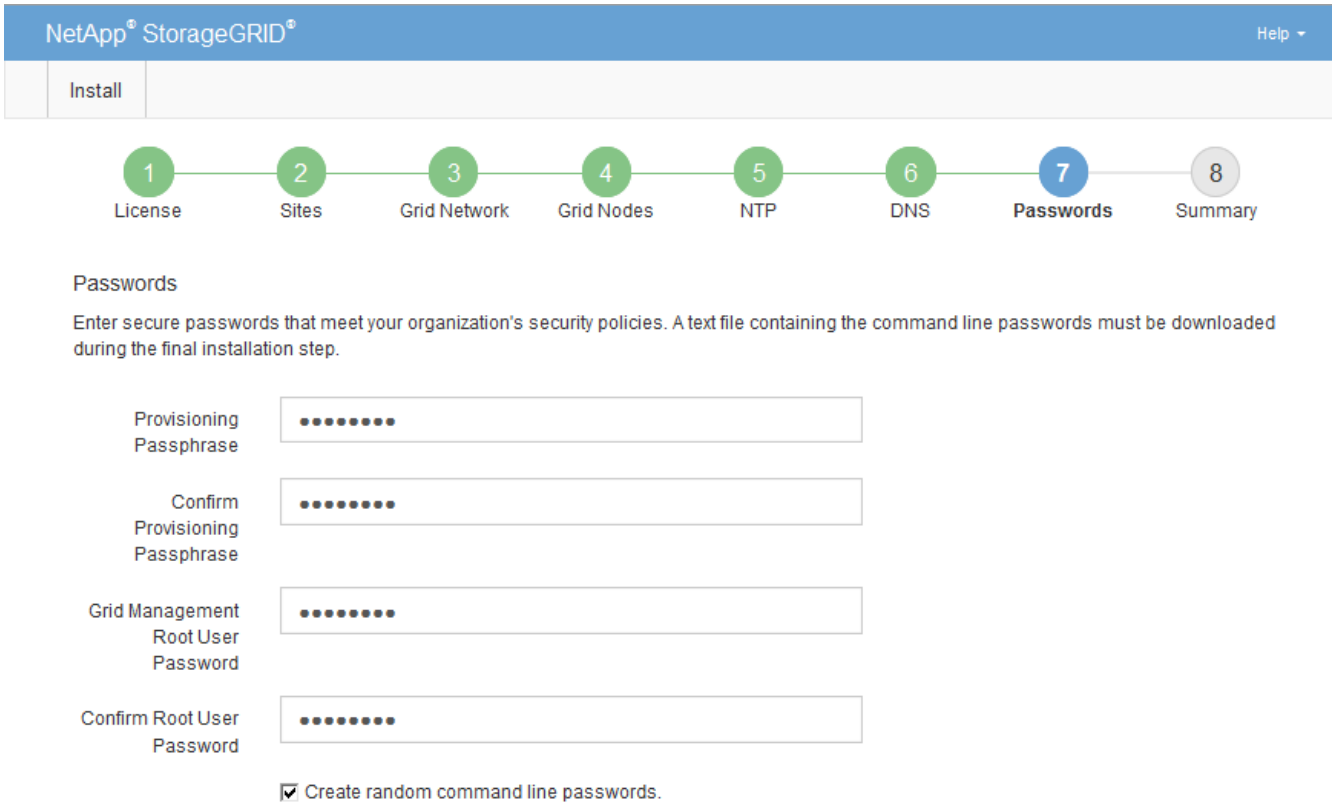
   프로비저닝 암호를 안전한 장소에 보관합니다.

   > 설치가 완료되고 나중에 프로비저닝 암호를 변경하려는 경우 Grid Manager를 사용할 수 있습니다. 구성 * > * 액세스 제어 * > * 그리드 비밀번호 * 를 선택합니다.

2. Provisioning Passphrase * 확인 에서 프로비저닝 암호를 다시 입력하여 확인합니다.
3. Grid Management Root User Password * 에서 Grid Manager에 ""root" 사용자로 액세스하는 데 사용할 암호를 입력합니다.

   암호를 안전한 곳에 보관하십시오.

4. 루트 사용자 암호 확인 * 에서 그리드 관리자 암호를 다시 입력하여 확인합니다.



5. 개념 증명이나 데모 목적으로 그리드를 설치하는 경우 * 임의의 명령줄 암호 만들기 * 확인란을 선택 취소합니다.

   프로덕션 배포의 경우 보안을 위해 항상 무작위 암호를 사용해야 합니다. ""root" 또는 ""admin" 계정을 사용하여 명령줄에서 그리드 노드에 액세스하기 위해 기본 암호를 사용하려는 경우 * 무작위 명령줄 암호 만들기 * 를 선택 취소합니다.

> 요약 페이지에서 * Install * 을 클릭하면 복구 패키지 파일('s GW-recovery-package-id-revision.zip')을 다운로드하라는 메시지가 표시됩니다. 반드시 해야 합니다 이 파일을 다운로드합니다 를 눌러 설치를 완료합니다. 시스템에 액세스하는 데 필요한 암호는 복구 패키지 파일에 포함된 Passwords.txt 파일에 저장됩니다.

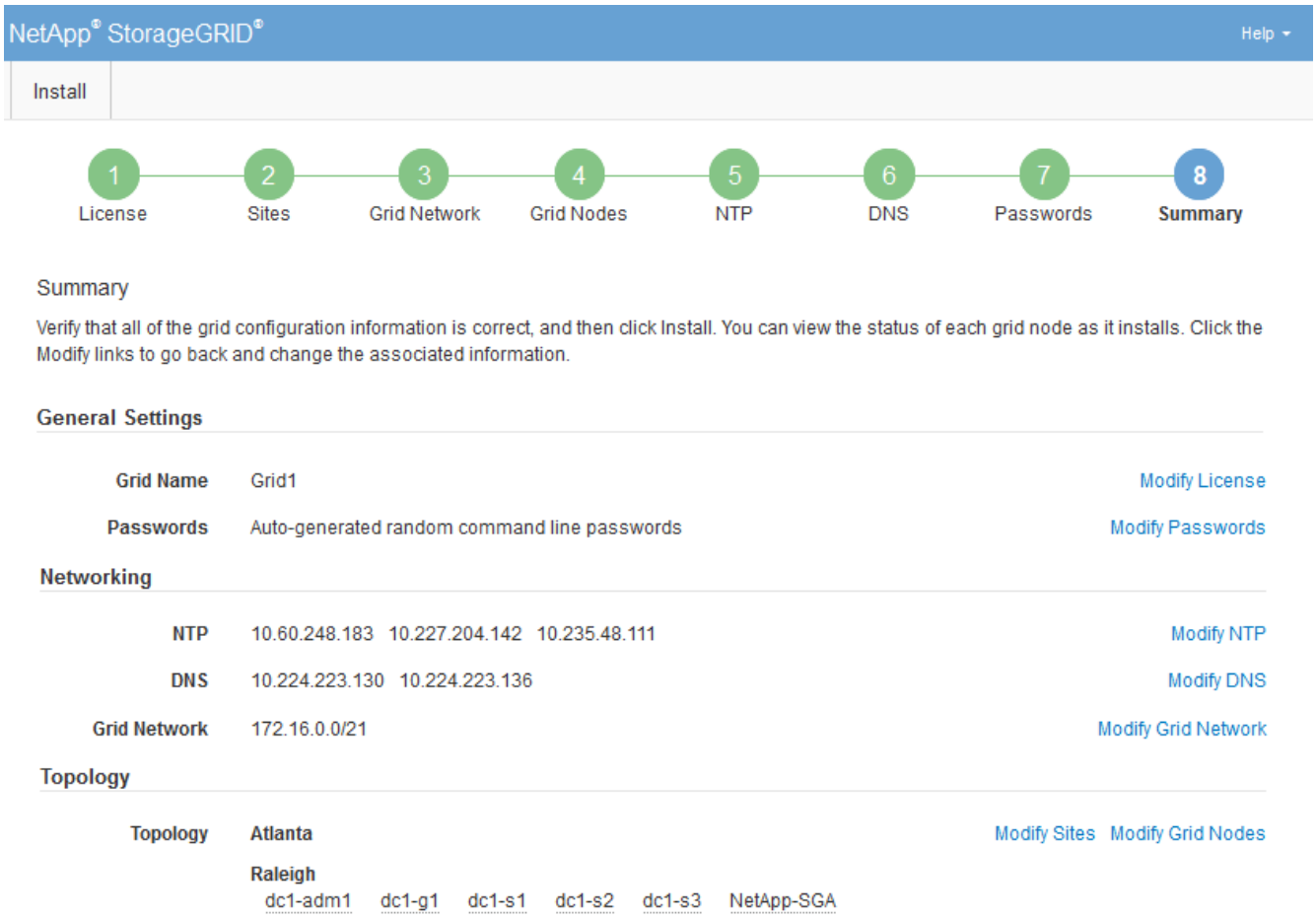
6. 다음 * 을 클릭합니다.

구성을 검토하고 설치를 완료합니다

설치를 성공적으로 완료하려면 입력한 구성 정보를 주의 깊게 검토해야 합니다.

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 끊어지면 액세스 가능한 서브넷을 통해 기본 관리 노드에 액세스하는지 확인해야 합니다. 을 참조하십시오 네트워킹 지침 를 참조하십시오.

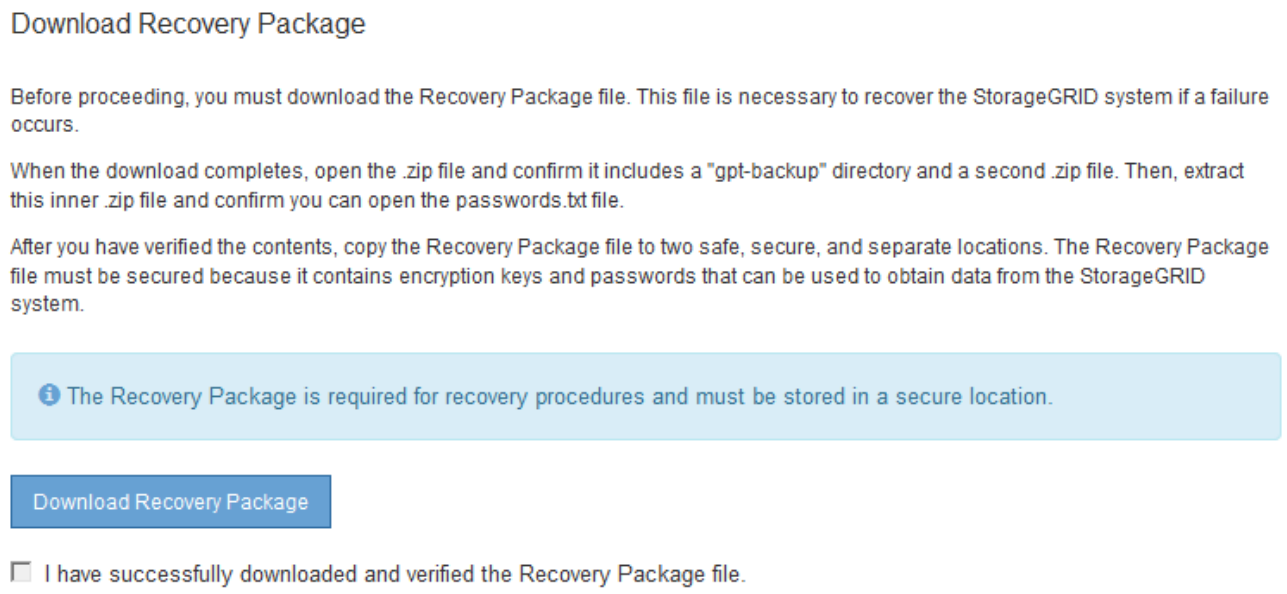
4. 복구 패키지 다운로드 * 를 클릭합니다.

   설치가 GRID 토폴로지를 정의한 지점으로 진행되면 복구 패키지 파일(".zip")을 다운로드하라는 메시지가 표시되고 이 파일의 내용에 액세스할 수 있는지 확인합니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 다운로드해야 합니다. 설치가 백그라운드에서 계속되지만 이 파일을 다운로드하여 확인하기 전에는 설치를 완료하고 StorageGRID 시스템에 액세스할 수 없습니다.

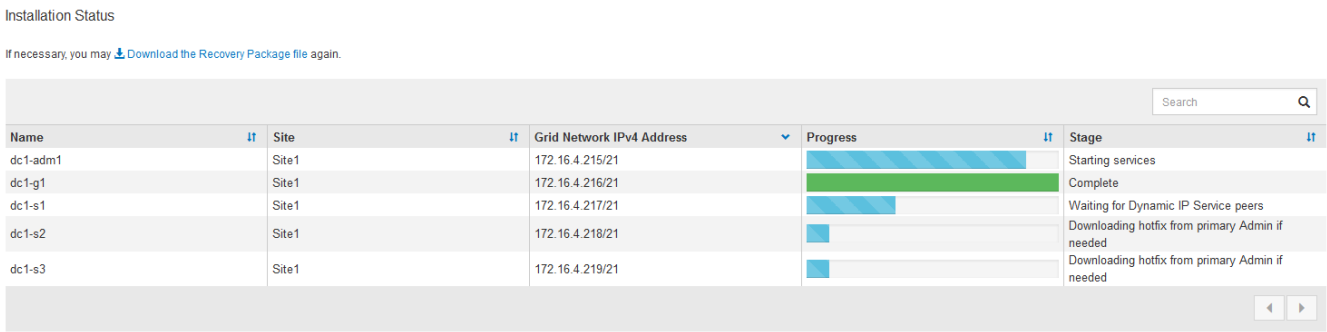
5. '.zip' 파일의 내용을 추출하여 안전한 별도의 두 위치에 저장할 수 있는지 확인합니다.

   > 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

6. 복구 패키지 파일을 성공적으로 다운로드하고 확인했습니다. * 확인란을 선택하고 * 다음 * 을 클릭합니다.



   설치가 진행 중인 경우 상태 페이지가 나타납니다. 이 페이지에는 각 그리드 노드의 설치 진행률이 표시됩니다.



   모든 그리드 노드에 대해 전체 단계에 도달하면 그리드 관리자의 로그인 페이지가 나타납니다.

7. "루트" 사용자 및 설치 중에 지정한 암호를 사용하여 Grid Manager에 로그인합니다.

설치 후 지침

그리드 노드 배포 및 구성을 완료한 후 DHCP 주소 지정 및 네트워크 구성 변경에 대한 다음

지침을 따르십시오.

- DHCP를 사용하여 IP 주소를 할당한 경우 사용 중인 네트워크의 각 IP 주소에 대해 DHCP 예약을 구성합니다.

  배포 단계에서는 DHCP만 설정할 수 있습니다. 구성 중에는 DHCP를 설정할 수 없습니다.

  > IP 주소가 변경되면 노드가 재부팅되므로 DHCP 주소 변경이 동시에 여러 노드에 영향을 미칠 경우 작동이 중단될 수 있습니다.

- 그리드 노드의 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 변경하려면 IP 변경 절차를 사용해야 합니다. 을 참조하십시오 IP 주소를 구성합니다.
- 라우팅 및 게이트웨이 변경을 비롯한 네트워킹 구성을 변경하면 기본 관리 노드 및 다른 그리드 노드에 대한 클라이언트 연결이 손실될 수 있습니다. 적용된 네트워킹 변경 사항에 따라 이러한 연결을 다시 설정해야 할 수 있습니다.

설치 자동화(**Ubuntu** 또는 **Debian**)

StorageGRID 호스트 서비스 설치 및 그리드 노드 구성을 자동화할 수 있습니다.

이 작업에 대해

구축 자동화는 다음 경우에 유용할 수 있습니다.

- 이미 Ansible, Puppet 또는 Chef와 같은 표준 오케스트레이션 프레임워크를 사용하여 물리적 호스트 또는 가상 호스트를 구축 및 구성합니다.
- 여러 StorageGRID 인스턴스를 배포하려고 합니다.
- 크고 복잡한 StorageGRID 인스턴스를 구축하고 있습니다.

StorageGRID 호스트 서비스는 패키지에 의해 설치되며 수동 설치 중에 대화형으로 만들 수 있는 구성 파일에 의해 구동되거나, 표준 오케스트레이션 프레임워크를 사용하여 자동 설치를 지원하기 위해 미리 준비되거나 프로그래밍 방식으로 준비됩니다. StorageGRID는 StorageGRID 어플라이언스 및 전체 StorageGRID 시스템(""그리드")의 구성을 자동화하는 옵션 Python 스크립트를 제공합니다. 이러한 스크립트를 직접 사용하거나 직접 개발한 그리드 배포 및 구성 도구에서 StorageGRID 설치 REST API를 사용하는 방법을 알아보기 위해 스크립트를 검사할 수 있습니다.

StorageGRID 호스트 서비스의 설치 및 구성을 자동화합니다

Anabilities, Puppet, Chef, Fabric 또는 SaltStack과 같은 표준 오케스트레이션 프레임워크를 사용하여 StorageGRID 호스트 서비스의 설치를 자동화할 수 있습니다.

StorageGRID 호스트 서비스는 DEB에 패키징되며 자동 설치를 활성화하기 위해 미리 준비하거나 프로그래밍 방식으로 준비할 수 있는 구성 파일에 의해 구동됩니다. 표준 오케스트레이션 프레임워크를 사용하여 Ubuntu 또는 Debian을 설치 및 구성하는 경우 플레이북이나 레시피에 StorageGRID를 추가하는 것이 간단해야 합니다.

다음과 같은 작업을 자동화할 수 있습니다.

1. Linux를 설치하는 중입니다
2. Linux 구성
3. StorageGRID 요구 사항을 충족하도록 호스트 네트워크 인터페이스 구성
4. StorageGRID 요구 사항을 충족하도록 호스트 스토리지 구성

5. Docker 설치 중
6. StorageGRID 호스트 서비스 설치
7. '/etc/StorageGrid/nodes'에서 StorageGRID 노드 구성 파일 생성
8. StorageGRID 노드 구성 파일의 유효성을 검사하는 중입니다
9. StorageGRID 호스트 서비스를 시작합니다

Ansible 역할 및 플레이북 예

예제 Ansible 역할 및 플레이북에는 /Extras 폴더에 설치 아카이브가 제공됩니다. Ansible 플레이북은 'StorageGRID' 역할이 호스트를 준비하고 타겟 서버에 StorageGRID를 설치하는 방법을 보여줍니다. 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.

StorageGRID의 구성을 자동화합니다

그리드 노드를 구축한 후 StorageGRID 시스템 구성을 자동화할 수 있습니다.

필요한 것

- 설치 아카이브에서 다음 파일의 위치를 알고 있습니다.

파일 이름	설명
configure-storagegrid.py	구성을 자동화하는 데 사용되는 Python 스크립트입니다
configure -StorageGrid.sample.json	스크립트와 함께 사용할 샘플 구성 파일
configure -StorageGrid.blank.json을 지정합니다	스크립트에 사용할 빈 구성 파일입니다

- "configure-StorageGrid.json" 구성 파일을 만들었습니다. 이 파일을 만들려면 샘플 구성 파일('configure-StorageGrid.sample.json') 또는 빈 구성 파일('configure-StorageGrid.blank.json')을 수정할 수 있습니다.

이 작업에 대해

configure-StorageGrid.py Python 스크립트와 configure-StorageGrid.json 구성 파일을 사용하여 StorageGRID 시스템 구성을 자동화할 수 있습니다.

> 그리드 관리자 또는 설치 API를 사용하여 시스템을 구성할 수도 있습니다.

단계

1. Python 스크립트를 실행하기 위해 사용 중인 Linux 시스템에 로그인합니다.
2. 설치 아카이브를 추출한 디렉토리로 변경합니다.

   예를 들면 다음과 같습니다.

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   여기서 플랫폼은 'EBS', 'rpms', 'vSphere'입니다.

3. Python 스크립트를 실행하고 생성한 구성 파일을 사용합니다.

   예를 들면 다음과 같습니다.

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

결과

복구 패키지 '.zip' 파일은 구성 프로세스 중에 생성되며 설치 및 구성 프로세스를 실행 중인 디렉토리에 다운로드됩니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 백업해야 합니다. 예를 들어, 안전한 백업 네트워크 위치 및 안전한 클라우드 저장소 위치에 복사합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

임의 암호를 생성해야 한다고 지정한 경우 "passwords.txt" 파일을 추출하고 StorageGRID 시스템에 액세스하는 데 필요한 암호를 찾아야 합니다.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

확인 메시지가 표시되면 StorageGRID 시스템이 설치 및 구성됩니다.

```
StorageGRID has been configured and installed.
```

관련 정보

설치 REST API 개요

설치 **REST API** 개요

StorageGRID는 설치 작업을 수행하기 위한 StorageGRID 설치 API를 제공합니다.

API는 Swagger 오픈 소스 API 플랫폼을 사용하여 API 문서를 제공합니다. swagger를 사용하면 개발자와 개발자가 아닌 사용자가 API가 매개 변수 및 옵션에 어떻게 응답하는지 보여주는 사용자 인터페이스에서 API와 상호 작용할 수 있습니다. 이 문서에서는 표준 웹 기술 및 JSON(JavaScript Object Notation) 데이터 형식에 대해 잘 알고 있다고 가정합니다.

> API Docs 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

각 REST API 명령에는 API의 URL, HTTP 작업, 필수 또는 선택적 URL 매개 변수, 그리고 예상되는 API 응답이

포함됩니다.

StorageGRID 설치 API

StorageGRID 설치 API는 StorageGRID 시스템을 처음 구성할 때와 기본 관리자 노드 복구를 수행해야 하는 경우에만 사용할 수 있습니다. 설치 API는 Grid Manager에서 HTTPS를 통해 액세스할 수 있습니다.

API 설명서에 액세스하려면 기본 관리 노드의 설치 웹 페이지로 이동하여 메뉴 모음에서 * 도움말 * > * API 설명서 * 를 선택합니다.

StorageGRID 설치 API에는 다음 섹션이 포함되어 있습니다.

- * config * — 제품 릴리스 및 API 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 API의 주요 버전을 나열할 수 있습니다.
- * 그리드 * — 그리드 레벨 구성 작업. 그리드 세부 정보, 그리드 네트워크 서브넷, 그리드 암호, NTP 및 DNS 서버 IP 주소를 포함한 그리드 설정을 얻고 업데이트할 수 있습니다.
- * 노드 * — 노드 레벨 구성 작업 그리드 노드 목록을 검색하고, 그리드 노드를 삭제하고, 그리드 노드를 구성하고, 그리드 노드를 보고, 그리드 노드의 구성을 재설정할 수 있습니다.
- * 프로비저닝 * — 프로비저닝 작업. 프로비저닝 작업을 시작하고 프로비저닝 작업의 상태를 볼 수 있습니다.
- * 복구 * — 기본 관리 노드 복구 작업 정보를 재설정하고, 복구 패키지를 업로드하고, 복구를 시작하고, 복구 작업의 상태를 볼 수 있습니다.
- * recovery-package * — 복구 패키지를 다운로드하기 위한 작업.
- 고급 배포를 위한 * 스키마 * — API 스키마
- * 사이트 * — 사이트 수준 구성 작업 사이트를 만들고, 보고, 삭제하고, 수정할 수 있습니다.

관련 정보

설치 자동화

다음 단계로 넘어갑니다

설치를 완료한 후에는 일련의 통합 및 구성 단계를 수행해야 합니다. 일부 단계는 필수 사항이고 다른 단계는 선택 사항입니다.

필수 작업

- StorageGRID 시스템에 오브젝트를 저장하는 데 사용할 각 클라이언트 프로토콜(Swift 또는 S3)에 대한 테넌트 계정을 생성합니다.
- 그룹 및 사용자 계정을 구성하여 시스템 액세스를 제어합니다. 필요에 따라 관리 그룹 및 사용자를 가져올 수 있도록 통합 ID 소스(예: Active Directory 또는 OpenLDAP)를 구성할 수 있습니다. 또는 로컬 그룹 및 사용자를 만들 수 있습니다.
- 오브젝트를 StorageGRID 시스템에 업로드하는 데 사용할 S3 또는 Swift API 클라이언트 애플리케이션을 통합 및 테스트합니다.
- 준비가 되면 개체 데이터를 보호하는 데 사용할 ILM(정보 수명 주기 관리) 규칙 및 ILM 정책을 구성합니다.

> StorageGRID를 설치하면 기본 ILM 정책, 즉 기본 2 복사본 정책이 활성화됩니다. 이 정책에는 재고 ILM 규칙(복사본 2개 만들기)이 포함되며 다른 정책이 활성화되지 않은 경우 적용됩니다.

- 설치에 어플라이언스 스토리지 노드가 포함된 경우 SANtricity 소프트웨어를 사용하여 다음 작업을 완료합니다.
  - 각 StorageGRID 어플라이언스에 연결하십시오.
  - AutoSupport 데이터가 수신되었는지 확인합니다.
- StorageGRID 시스템에 아카이브 노드가 포함된 경우 아카이브 노드의 대상 외부 아카이브 스토리지 시스템에 대한 접속을 구성합니다.

> 아카이브 노드에서 Tivoli Storage Manager를 외부 아카이브 스토리지 시스템으로 사용하는 경우 Tivoli Storage Manager도 구성해야 합니다.

- StorageGRID 시스템 강화 지침을 검토하고 준수하여 보안 위험을 제거합니다.
- 시스템 경고에 대한 이메일 알림을 구성합니다.

선택적 태스크입니다

- (레거시) 알람 시스템에서 알림을 수신하려면 알람에 대한 메일 그룹 및 이메일 알림을 구성합니다.
- 배포를 계획하고 복구 패키지를 생성한 이후에 변경된 경우 그리드 노드 IP 주소를 업데이트합니다. 복구 및 유지 관리 지침에서 IP 주소 변경에 대한 정보를 참조하십시오.
- 필요한 경우 스토리지 암호화를 구성합니다.
- 필요한 경우 스토리지 압축을 구성하여 저장된 개체의 크기를 줄입니다.
- 감사 클라이언트 액세스를 구성합니다. NFS 또는 CIFS 파일 공유를 통해 감사 목적으로 시스템에 대한 액세스를 구성할 수 있습니다. StorageGRID 관리 지침을 참조하십시오.

> CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

관련 정보

StorageGRID 관리

S3을 사용합니다

Swift를 사용합니다

ILM을 사용하여 개체를 관리합니다

모니터링하고 문제를 해결합니다

복구 및 유지 관리

SG100 및 SG1000 서비스 어플라이언스

SG5600 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG6000 스토리지 어플라이언스

릴리스 정보

시스템 강화

감사 로그를 검토합니다

소프트웨어 업그레이드

설치 문제를 해결합니다

StorageGRID 시스템을 설치하는 동안 문제가 발생하면 설치 로그 파일에 액세스할 수 있습니다. 기술 지원 부서에서는 설치 로그 파일을 사용하여 문제를 해결해야 할 수도 있습니다.

각 노드를 실행 중인 컨테이너에서 다음 설치 로그 파일을 사용할 수 있습니다.

- '/var/local/log/install.log'(모든 그리드 노드에 있음)
- (/var/local/log/gdu-server.log"(기본 관리 노드에서 찾을 수 있음)

호스트에서 다음 설치 로그 파일을 사용할 수 있습니다.

- '/var/log/StorageGrid/daemon.log'입니다
- "/var/log/StorageGrid/nodes/<node-name>.log"를 입력합니다

로그 파일에 액세스하는 방법은 StorageGRID 모니터링 및 문제 해결 지침을 참조하십시오. 어플라이언스 설치 문제 해결에 대한 도움말은 어플라이언스의 설치 및 유지 관리 지침을 참조하십시오. 추가 지원이 필요한 경우 기술 지원 부서에 문의하십시오.

관련 정보

모니터링하고 문제를 해결합니다

SG100 및 SG1000 서비스 어플라이언스

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG5600 스토리지 어플라이언스

"NetApp 지원"

예 **/etc/network/interfaces**

'/etc/network/interfaces' 파일에는 물리적 인터페이스, 본드 인터페이스 및 VLAN 인터페이스를 정의하는 세 개의 섹션이 포함되어 있습니다. 3개의 예제 섹션을 단일 파일로 결합하여 4개의 Linux 물리적 인터페이스를 단일 LACP 결합으로 통합한 다음 StorageGRID 그리드, 관리 및 클라이언트 네트워크 인터페이스로 사용할 수 있는 결합을 형성하는 3개의 VLAN 인터페이스를 설정합니다.

물리적 인터페이스

링크의 다른 쪽 끝에 있는 스위치도 4개의 포트를 단일 LACP 트렁크 또는 포트 채널로 처리해야 하며, 태그가 있는 3개

이상의 참조된 VLAN을 통과해야 합니다.

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

본드 인터페이스

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

VLAN 인터페이스

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

VMware를 설치합니다

VMware 설치: 개요

VMware 환경에 StorageGRID 시스템을 설치하는 과정은 세 가지 기본 단계로 구성됩니다.

1. * 준비 *: 계획 및 준비 중에 다음 작업을 수행합니다.
   - StorageGRID의 하드웨어, 소프트웨어, 가상 시스템, 스토리지 및 성능 요구 사항에 대해 알아보십시오.
   - 의 세부 사항에 대해 자세히 알아보십시오 StorageGRID 네트워킹 따라서 네트워크를 적절하게 구성할 수 있습니다.
   - StorageGRID 그리드 노드를 호스팅하는 데 사용할 물리적 서버를 식별하고 준비합니다.
   - 준비한 서버:
     - VMware vSphere 하이퍼바이저를 설치합니다
     - ESX 호스트를 구성합니다
     - VMware vSphere 및 vCenter를 설치하고 구성합니다
2. * 구축 *: VMware vSphere Web Client를 사용하여 그리드 노드를 구축합니다. 그리드 노드를 구축하면 StorageGRID 시스템의 일부로 생성되고 하나 이상의 네트워크에 연결됩니다.
   a. VMware vSphere Web Client, .vmdk 파일 및 .ovf 파일 템플릿 집합을 사용하여 1단계에서 준비한 서버에 소프트웨어 기반 노드를 VM(가상 머신)으로 배포합니다.
   b. StorageGRID 어플라이언스 설치 프로그램을 사용하여 StorageGRID 어플라이언스 노드를 배포합니다.

   > 하드웨어 관련 설치 및 통합 지침은 StorageGRID 설치 절차에 포함되어 있지 않습니다. StorageGRID 어플라이언스를 설치하는 방법에 대한 자세한 내용은 해당 어플라이언스의 설치 및 유지 관리 지침을 참조하십시오.
3. * 구성 *: 모든 노드가 배포되면 그리드 관리자를 사용하여 그리드를 구성하고 설치를 완료합니다.

이 지침은 VMware 환경에서 StorageGRID 시스템을 구축 및 구성하는 표준 접근 방식을 권장합니다. 다음 대체 접근 방법에 대한 정보도 참조하십시오.

- 설치 아카이브에서 제공되는 deploy-vsphere-ovftool.sh Bash 스크립트를 사용하여 VMware vSphere에 그리드 노드를 구축합니다.
- 설치 아카이브에 제공되는 Python 구성 스크립트를 사용하여 StorageGRID 시스템의 구축 및 구성을 자동화합니다.
- Python 구성 스크립트(설치 아카이브나 StorageGRID 어플라이언스 설치 프로그램에서 사용 가능)를 사용하여 어플라이언스 그리드 노드의 구축 및 구성을 자동화합니다.
- StorageGRID 배포의 고급 개발자인 경우 설치 REST API를 사용하여 StorageGRID 그리드 노드 설치를 자동화합니다.

VMware 설치 계획 및 준비

설치 전**(VMware)**

그리드 노드를 배포하고 StorageGRID 그리드를 구성하기 전에 절차를 완료하기 위한 단계와 요구 사항을 숙지해야 합니다.

StorageGRID 배포 및 구성 절차에서는 StorageGRID 시스템의 아키텍처 및 운영 기능에 익숙하다고 가정합니다.

단일 사이트 또는 여러 사이트를 한 번에 배포할 수 있지만, 모든 사이트는 최소 3개의 스토리지 노드를 보유해야 하는 최소 요구 사항을 충족해야 합니다.

> 기본 디스크 보호는 하드웨어 RAID가 아니기 때문에 StorageGRID는 가상 SAN(Storage Area Network)의 사용을 지원하지 않습니다.

노드 배포 및 그리드 구성 절차를 시작하기 전에 다음을 수행해야 합니다.

- StorageGRID 구축 계획
- 모든 StorageGRID 어플라이언스를 포함하여 필요한 모든 하드웨어를 사양에 맞게 설치, 연결 및 구성합니다.

> 하드웨어 관련 설치 및 통합 지침은 StorageGRID 설치 절차에 포함되어 있지 않습니다. StorageGRID 어플라이언스를 설치하는 방법에 대한 자세한 내용은 해당 어플라이언스의 설치 및 유지 관리 지침을 참조하십시오.

- 을(를) 이해합니다 사용 가능한 네트워크 옵션 및 그리드 노드에서 각 네트워크 옵션을 구현하는 방법.
- 모든 네트워킹 정보를 미리 수집합니다. DHCP를 사용하지 않는 경우 각 그리드 노드에 할당할 IP 주소와 사용할 DNS(Domain Name System) 및 NTP(Network Time Protocol) 서버의 IP 주소를 수집합니다.
- 사용할 수 있는 배포 및 구성 도구 중에서 선택합니다.

관련 정보

SG100 및 SG1000 서비스 어플라이언스

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

필수 자료

StorageGRID를 설치하기 전에 필요한 자료를 수집하고 준비해야 합니다.

항목	참고
NetApp StorageGRID 라이센스	디지털 서명된 유효한 NetApp 라이센스가 있어야 합니다. • 참고 *: StorageGRID 설치 아카이브에는 제품에 대한 지원 권한이 없는 무료 라이센스가 포함되어 있습니다.
StorageGRID 설치 아카이브	반드시 해야 합니다 StorageGRID 설치 아카이브를 다운로드하고 파일의 압축을 풉니다.
VMware 소프트웨어 및 설명서	설치 중에 VMware vSphere Web Client를 사용하여 가상 머신에 가상 그리드 노드를 구축합니다. 지원되는 버전은 상호 운용성 매트릭스 를 참조하십시오.
서비스 노트북	StorageGRID 시스템은 서비스 포어를 통해 설치됩니다.서비스 랩톱에는 다음이 있어야 합니다. • 네트워크 포트 • SSH 클라이언트(예: PuTTY) • 지원되는 웹 브라우저
StorageGRID 설명서	• 릴리스 정보 • StorageGRID 관리 지침

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

StorageGRID 설치 파일을 다운로드하고 압축을 풉니다

StorageGRID 설치 아카이브를 다운로드하고 파일을 추출해야 합니다.

단계

1. 로 이동합니다 "StorageGRID용 NetApp 다운로드 페이지".
2. 최신 릴리스를 다운로드하려면 버튼을 선택하거나 드롭다운 메뉴에서 다른 버전을 선택하고 * GO * 를 선택합니다.
3. NetApp 계정의 사용자 이름과 암호를 사용하여 로그인합니다.
4. Caution/MustRead 문이 나타나면 해당 문을 읽고 확인란을 선택합니다.

> StorageGRID 릴리스를 설치한 후 필요한 핫픽스를 적용해야 합니다. 자세한 내용은 를 참조하십시오 복구 및 유지 관리 지침의 핫픽스 절차

5. 최종 사용자 사용권 계약을 읽고 확인란을 선택한 다음 * 동의 및 계속 * 을 선택합니다.
6. Install StorageGRID * 열에서 VMware의 .tgz 또는 .zip 파일을 선택합니다.

> 서비스 랩톱에서 Windows를 실행 중인 경우 '.zip' 파일을 사용합니다.

7. 아카이브 파일을 저장하고 압축을 풉니다.
8. 다음 목록에서 필요한 파일을 선택합니다.

필요한 파일은 계획된 그리드 토폴로지와 StorageGRID 시스템을 구축하는 방법에 따라 다릅니다.

> 표에 나열된 경로는 추출된 설치 아카이브에서 설치한 최상위 디렉토리에 상대적입니다.

경로 및 파일 이름입니다	설명
	StorageGRID 다운로드 파일에 포함된 모든 파일을 설명하는 텍스트 파일입니다.
	제품에 대한 지원 권한을 제공하지 않는 무료 라이센스입니다.
	그리드 노드 가상 머신을 생성하기 위한 템플릿으로 사용되는 가상 머신 디스크 파일입니다.
	기본 관리 노드를 배포하기 위한 오픈 가상화 형식 템플릿 파일(".ovf") 및 매니페스트 파일(".mf")입니다.
	비기본 관리 노드를 배포하기 위한 템플릿 파일(".ovf")과 매니페스트 파일(".mf")입니다.
/vSphere/vSphere-archive.ovf./vSphere/vSphere-archive.mf	아카이브 노드 배포를 위한 템플릿 파일(".ovf")과 매니페스트 파일(".mf")입니다.
	게이트웨이 노드를 배포하기 위한 템플릿 파일(".ovf")과 매니페스트 파일(".mf")입니다.
	가상 머신 기반 스토리지 노드 구축을 위한 템플릿 파일('.ovf') 및 매니페스트 파일('.mf')입니다.
배포 스크립팅 도구	설명
	가상 그리드 노드의 배포를 자동화하는 데 사용되는 Bash 쉘 스크립트입니다.
	'deploy-vsphere-ovftool.sh' 스크립트와 함께 사용할 구성 파일의 예.

경로 및 파일 이름입니다	설명
	StorageGRID 시스템 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
	StorageGRID 어플라이언스 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/vSphere/configure -StorageGrid.sample.json을 참조하십시오	"configure-StorageGrid.py" 스크립트와 함께 사용할 구성 파일의 예
/vSphere/configure -StorageGrid.blank.json 을 참조하십시오	configure-StorageGrid.py 스크립트와 함께 사용할 빈 구성 파일입니다.
/vSphere/Extras/API-schemas	StorageGRID에 대한 API 스키마입니다. • 참고 *: 업그레이드를 수행하기 전에 이러한 스키마를 사용하여 StorageGRID 관리 API를 사용하도록 작성한 코드가 업그레이드 호환성 테스트를 위한 비프로덕션 StorageGRID 환경이 없는 경우 새 StorageGRID 릴리스와 호환되는지 확인할 수 있습니다.

관련 정보

복구 및 유지 관리

소프트웨어 요구 사항

가상 머신을 사용하여 모든 유형의 StorageGRID 그리드 노드를 호스팅할 수 있습니다. VMware 서버에 설치된 각 그리드 노드에 하나의 가상 시스템이 필요합니다.

VMware vSphere 하이퍼바이저

준비된 물리적 서버에 VMware vSphere 하이퍼바이저를 설치해야 합니다. VMware 소프트웨어를 설치하기 전에 하드웨어를 올바르게 구성해야 합니다(펌웨어 버전 및 BIOS 설정 포함).

- 설치할 StorageGRID 시스템에 대한 네트워킹을 지원하기 위해 필요에 따라 하이퍼바이저에서 네트워킹을 구성합니다.

  네트워킹 지침

- 데이터 저장소가 그리드 노드를 호스팅하는 데 필요한 가상 머신 및 가상 디스크에 충분히 큰지 확인합니다.
- 둘 이상의 데이터 저장소를 생성하는 경우 가상 머신을 생성할 때 각 그리드 노드에 사용할 데이터 저장소를 쉽게 식별할 수 있도록 각 데이터 저장소의 이름을 지정합니다.

ESX 호스트 구성 요구 사항

> 각 ESX 호스트에서 NTP(네트워크 시간 프로토콜)를 적절히 구성해야 합니다. 호스트 시간이 올바르지 않으면 데이터 손실을 비롯한 부정적인 영향이 발생할 수 있습니다.

VMware 구성 요구 사항

StorageGRID 그리드 노드를 구축하기 전에 VMware vSphere 및 vCenter를 설치하고 구성해야 합니다.

지원되는 VMware vSphere 하이퍼바이저 버전과 VMware vCenter Server 소프트웨어 버전은 상호 운용성 매트릭스를 참조하십시오.

이러한 VMware 제품을 설치하는 데 필요한 단계는 VMware 설명서를 참조하십시오.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

CPU 및 **RAM** 요구 사항

StorageGRID 소프트웨어를 설치하기 전에 StorageGRID 시스템을 지원할 준비가 되도록 하드웨어를 확인 및 구성하십시오.

지원되는 서버에 대한 자세한 내용은 상호 운용성 매트릭스 를 참조하십시오.

각 StorageGRID 노드에는 다음과 같은 최소 리소스가 필요합니다.

- CPU 코어: 노드당 8개
- RAM: 사용 가능한 총 RAM과 시스템에서 실행 중인 비 StorageGRID 소프트웨어의 양에 따라 노드당 최소 24GB, 총 시스템 RAM보다 2GB ~ 16GB 이상

각 물리적 또는 가상 호스트에서 실행하려는 StorageGRID 노드 수가 사용 가능한 CPU 코어 수 또는 물리적 RAM을 초과하지 않는지 확인합니다. 호스트가 StorageGRID 실행 전용이 아닌 경우(권장되지 않음) 다른 애플리케이션의 리소스 요구 사항을 고려해야 합니다.

> CPU 및 메모리 사용량을 정기적으로 모니터링하여 이러한 리소스가 작업 부하를 지속적으로 수용할 수 있도록 합니다. 예를 들어, 가상 스토리지 노드에 대한 RAM 및 CPU 할당을 두 배로 하면 StorageGRID 어플라이언스 노드에 제공되는 것과 유사한 리소스를 제공할 수 있습니다. 또한 노드당 메타데이터 양이 500GB를 초과하는 경우 노드당 RAM을 48GB 이상으로 늘리는 것이 좋습니다. 개체 메타데이터 저장소 관리, 메타데이터 예약 공간 설정 증가 및 CPU 및 메모리 사용량 모니터링에 대한 자세한 내용은 StorageGRID 관리, 모니터링 및 업그레이드에 대한 지침을 참조하십시오.

하이퍼스레딩이 기본 물리적 호스트에서 활성화된 경우 노드당 8개의 가상 코어(4개의 물리적 코어)를 제공할 수 있습니다. 하이퍼스레딩이 기본 물리적 호스트에서 사용되지 않는 경우 노드당 8개의 물리적 코어를 제공해야 합니다.

가상 시스템을 호스트로 사용하고 VM의 크기와 수를 제어하는 경우 각 StorageGRID 노드에 대해 단일 VM을 사용하고 그에 따라 VM 크기를 조정해야 합니다.

운영 구축 환경에서는 동일한 물리적 스토리지 하드웨어 또는 가상 호스트에서 여러 스토리지 노드를 실행하지 않아야 합니다. 단일 StorageGRID 구축 환경의 각 스토리지 노드는 자체 격리된 장애 도메인에 있어야 합니다. 단일 하드웨어 장애가 단일 스토리지 노드에만 영향을 줄 수 있도록 하는 경우 오브젝트 데이터의 내구성과 가용성을 최대화할 수 있습니다.

스토리지 요구 사항에 대한 정보도 참조하십시오.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

요구사항을 충족해야 합니다

StorageGRID 관리

모니터링하고 문제를 해결합니다

소프트웨어 업그레이드

요구사항을 충족해야 합니다

가상 시스템에서 호스팅되는 StorageGRID 노드의 스토리지 및 성능 요구 사항을 이해해야 초기 구성과 향후 스토리지 확장을 지원할 수 있는 충분한 공간을 제공할 수 있습니다.

성능 요구사항

OS 볼륨 및 첫 번째 스토리지 볼륨의 성능은 시스템의 전반적인 성능에 큰 영향을 줍니다. 지연 시간, IOPS(Input/Output Operation per Second) 및 처리량 측면에서 적절한 디스크 성능을 제공해야 합니다.

모든 StorageGRID 노드에는 운영 체제 드라이브 및 모든 스토리지 볼륨에 write-back 캐시가 설정되어 있어야 합니다. 캐시는 보호되거나 영구 미디어에 있어야 합니다.

NetApp ONTAP 스토리지를 사용하는 가상 머신의 요구 사항

NetApp ONTAP 시스템에서 할당된 스토리지를 가진 가상 머신으로 StorageGRID 노드를 구축하는 경우 해당 볼륨에 FabricPool 계층화 정책이 활성화되어 있지 않음을 확인합니다. 예를 들어 StorageGRID 노드가 VMware 호스트에서 가상 머신으로 실행 중인 경우 데이터 저장소를 백업하는 볼륨에 FabricPool 계층화 정책이 설정되어 있지 않은지 확인합니다. StorageGRID 노드와 함께 사용되는 볼륨에 대해 FabricPool 계층화를 사용하지 않도록 설정하면 문제 해결과 스토리지 작업이 간소화됩니다.

> FabricPool를 사용하여 StorageGRID 관련 데이터를 StorageGRID 자체로 계층화하지 마십시오. StorageGRID 데이터를 StorageGRID로 다시 계층화하면 문제 해결과 운영 복잡성이 늘어납니다.

필요한 가상 머신의 수입니다

각 StorageGRID 사이트에는 최소 3개의 스토리지 노드가 필요합니다.

> 운영 구축 시 단일 가상 머신 서버에서 스토리지 노드를 두 개 이상 실행하지 마십시오. 각 스토리지 노드에 대해 전용 가상 머신 호스트를 사용하면 격리된 장애 도메인이 제공됩니다.

관리 노드 또는 게이트웨이 노드와 같은 다른 유형의 노드는 동일한 가상 머신 호스트에 구축하거나 필요에 따라 전용 가상 머신 호스트에 구축할 수 있습니다. 그러나 같은 유형의 여러 노드(예: 게이트웨이 노드 2개)가 있는 경우 동일한 가상 머신 호스트에 모든 인스턴스를 설치하지 마십시오.

노드 유형별 스토리지 요구 사항

운영 환경에서 StorageGRID 그리드 노드의 가상 시스템은 노드 유형에 따라 서로 다른 요구 사항을 충족해야 합니다.

디스크 스냅샷을 사용하여 그리드 노드를 복원할 수 없습니다. 대신 각 노드 유형에 대한 복구 및 유지보수 절차를 참조하십시오.

노드 유형	스토리지
관리자 노드	OS용 100GB LUN 관리자 노드 테이블용 200GB LUN 관리자 노드 감사 로그용 200GB LUN
스토리지 노드	OS용 100GB LUN 이 호스트의 각 스토리지 노드에 대해 3개의 LUN • 참고 *: 스토리지 노드에는 스토리지 LUN이 1-16개까지 포함될 수 있습니다. 최소 3개의 스토리지 LUN을 사용하는 것이 좋습니다. LUN당 최소 크기: 4TB 테스트된 최대 LUN 크기: 39TB.
게이트웨이 노드	OS용 100GB LUN
아카이브 노드	OS용 100GB LUN

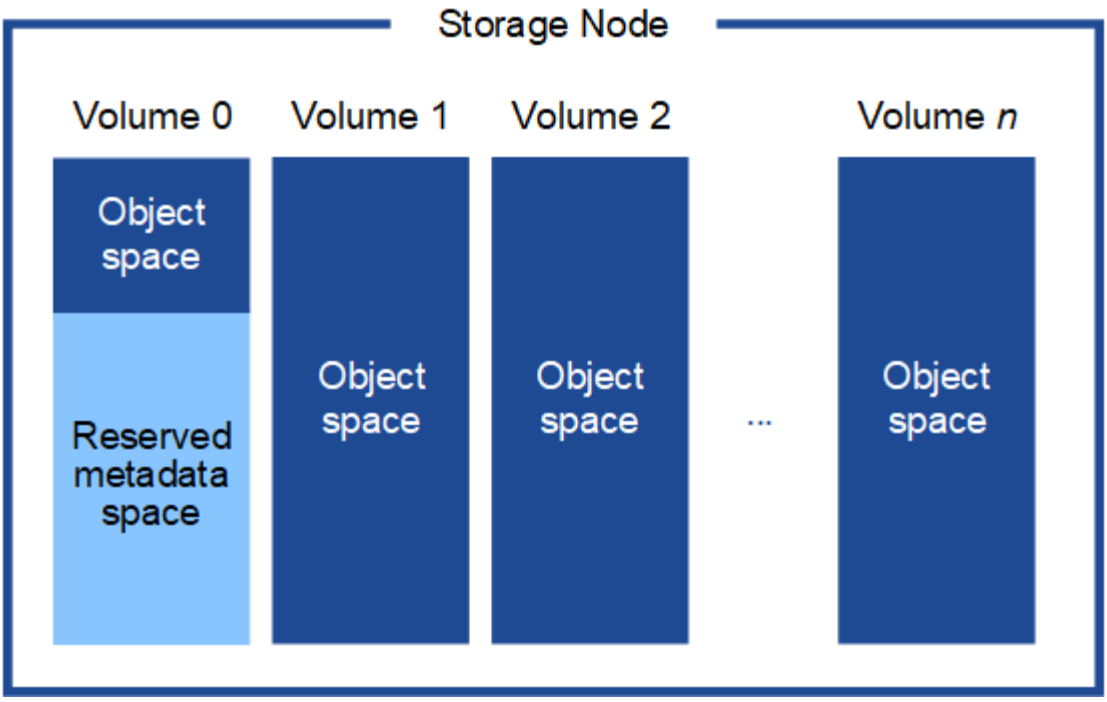
구성된 감사 레벨, S3 오브젝트 키 이름 등의 사용자 입력 크기 및 보존해야 하는 감사 로그 데이터의 양에 따라 각 관리 노드에서 감사 로그 LUN의 크기를 늘려야 할 수 있습니다. 일반적으로, 그리드는 S3 작업당 약 1KB의 감사 데이터를 생성합니다. 즉, 200GB LUN이 하루에 7000만 개의 작업을 지원하거나 2~3일 동안 초당 800개의 작업을 지원합니다.

스토리지 노드의 스토리지 요구 사항

소프트웨어 기반 스토리지 노드는 1-16개의 스토리지 볼륨을 가질 수 있습니다. -3개 이상의 스토리지 볼륨을 사용하는 것이 좋습니다. 각 스토리지 볼륨은 4TB 이상이어야 합니다.

어플라이언스 스토리지 노드는 최대 48개의 스토리지 볼륨을 가질 수 있습니다.

그림에 나와 있는 것처럼 StorageGRID는 각 스토리지 노드의 스토리지 볼륨 0에 객체 메타데이터를 위한 공간을 예약합니다. 스토리지 볼륨 0 및 스토리지 노드의 다른 스토리지 볼륨의 나머지 공간은 오브젝트 데이터에만 사용됩니다.



이중화를 제공하고 개체 메타데이터를 손실로부터 보호하기 위해 StorageGRID는 각 사이트의 시스템 모든 개체에 대한 메타데이터 복사본을 3개 저장합니다. 오브젝트 메타데이터의 복사본 3개는 각 사이트의 모든 스토리지 노드에 균등하게 분산됩니다.

새 스토리지 노드의 볼륨 0에 공간을 할당하는 경우 모든 오브젝트 메타데이터의 해당 노드에 적절한 공간이 있는지 확인해야 합니다.

- 적어도 볼륨 0에 4TB 이상을 할당해야 합니다.

> 스토리지 노드에 대해 하나의 스토리지 볼륨만 사용하고 볼륨에 4TB 이하를 할당하는 경우 스토리지 노드는 시작 시 스토리지 읽기 전용 상태로 전환되어 객체 메타데이터만 저장할 수 있습니다.

- 새 StorageGRID 11.6 시스템을 설치하고 각 스토리지 노드에 128GB 이상의 RAM이 있는 경우 볼륨 0에 8TB 이상을 할당해야 합니다. 볼륨 0에 더 큰 값을 사용하면 각 스토리지 노드에서 메타데이터에 허용되는 공간이 증가할 수 있습니다.
- 사이트에 대해 서로 다른 스토리지 노드를 구성할 때 가능하면 볼륨 0에 대해 동일한 설정을 사용합니다. 사이트에 크기가 다른 스토리지 노드가 있는 경우 볼륨이 0인 스토리지 노드가 해당 사이트의 메타데이터 용량을 결정합니다.

자세한 내용은 를 참조하십시오 오브젝트 메타데이터 스토리지 관리.

관련 정보

복구 및 유지 관리

가상 머신 그리드 노드 구축(VMware)

배포 환경에 대한 정보를 수집합니다

그리드 노드를 구축하기 전에 네트워크 구성 및 VMware 환경에 대한 정보를 수집해야 합니다.

> 일부 노드를 나중에 설치하는 대신 모든 노드를 한 번 설치하는 것이 더 효율적입니다.

VMware 정보입니다

배포 환경에 액세스하여 VMware 환경, 그리드, 관리자 및 클라이언트 네트워크용으로 생성된 네트워크, 스토리지 노드에 사용할 스토리지 볼륨 유형에 대한 정보를 수집해야 합니다.

다음을 포함하여 VMware 환경에 대한 정보를 수집해야 합니다.

- 구축을 완료할 수 있는 적절한 권한이 있는 VMware vSphere 계정의 사용자 이름 및 암호입니다.
- 각 StorageGRID 그리드 노드 가상 머신에 대한 호스트, 데이터 저장소 및 네트워크 구성 정보

> VMware Live vMotion을 사용하면 가상 머신 클록 시간이 점프를 일으키며 모든 유형의 그리드 노드에서는 지원되지 않습니다. 드물지만 잘못된 클럭 시간으로 인해 데이터 또는 구성 업데이트가 손실될 수 있습니다.

그리드 네트워크 정보

StorageGRID 그리드 네트워크(필수)용으로 생성된 VMware 네트워크에 대한 정보를 수집해야 합니다. 여기에는 다음이 포함됩니다.

- 네트워크 이름입니다.
- DHCP를 사용하지 않는 경우 각 그리드 노드에 필요한 네트워킹 세부 정보(IP 주소, 게이트웨이 및 네트워크 마스크)가 표시됩니다.
- DHCP를 사용하지 않는 경우 그리드 네트워크에 있는 기본 관리 노드의 IP 주소입니다. 자세한 내용은 ""그리드 노드가 기본 관리 노드를 검색하는 방법"을 참조하십시오.

관리자 네트워크 정보

선택적 StorageGRID 관리자 네트워크에 연결될 노드의 경우 이 네트워크에 대해 생성된 VMware 네트워크 관련 정보를 수집해야 합니다. 여기에는 다음이 포함됩니다.

- 네트워크 이름입니다.
- 고정 또는 DHCP 중 IP 주소를 할당하는 데 사용되는 방법입니다.
- 고정 IP 주소를 사용하는 경우 각 그리드 노드에 필요한 네트워킹 세부 정보(IP 주소, 게이트웨이, 네트워크 마스크)가 표시됩니다.
- 관리 네트워크의 외부 서브넷 목록(ESL).

클라이언트 네트워크 정보

선택적 StorageGRID 클라이언트 네트워크에 연결될 노드의 경우 이 네트워크에 대해 생성된 VMware 네트워크 관련 정보를 수집해야 합니다. 여기에는 다음이 포함됩니다.

- 네트워크 이름입니다.
- 고정 또는 DHCP 중 IP 주소를 할당하는 데 사용되는 방법입니다.
- 고정 IP 주소를 사용하는 경우 각 그리드 노드에 필요한 네트워킹 세부 정보(IP 주소, 게이트웨이, 네트워크 마스크)가 표시됩니다.

추가 인터페이스에 대한 정보입니다

노드를 설치한 후 vCenter에서 VM에 트렁크 또는 액세스 인터페이스를 선택적으로 추가할 수 있습니다. 예를 들어, 관리 또는 게이트웨이 노드에 트렁크 인터페이스를 추가하여 VLAN 인터페이스를 사용하여 다른 애플리케이션이나 테넌트에 속한 트래픽을 분리할 수 있습니다. 또는 고가용성(HA) 그룹에서 사용할 액세스 인터페이스를 추가할 수도 있습니다.

추가한 인터페이스는 VLAN 인터페이스 페이지와 Grid Manager의 HA 그룹 페이지에 표시됩니다.

- 트렁크 인터페이스를 추가하는 경우 각각의 새 상위 인터페이스에 대해 하나 이상의 VLAN 인터페이스를 구성합니다. 을 참조하십시오 VLAN 인터페이스를 구성합니다.
- 액세스 인터페이스를 추가할 경우 HA 그룹에 직접 추가해야 합니다. 을 참조하십시오 고가용성 그룹을 구성합니다.

가상 스토리지 노드의 스토리지 볼륨

가상 머신 기반 스토리지 노드에 대한 다음 정보를 수집해야 합니다.

- 추가할 스토리지 볼륨(스토리지 LUN)의 수와 크기입니다. "스토리지 및 성능 요구 사항"을 참조하십시오.

그리드 구성 정보

그리드를 구성하려면 정보를 수집해야 합니다.

- 그리드 사용권
- NTP(Network Time Protocol) 서버 IP 주소입니다
- DNS(Domain Name System) 서버 IP 주소입니다

관련 정보

그리드 노드가 기본 관리자 노드를 검색하는 방법

요구사항을 충족해야 합니다

그리드 노드가 기본 관리자 노드를 검색하는 방법

그리드 노드는 구성 및 관리를 위해 기본 관리 노드와 통신합니다. 각 그리드 노드는 그리드 네트워크에 있는 기본 관리 노드의 IP 주소를 알아야 합니다.

그리드 노드가 기본 관리 노드에 액세스할 수 있도록 노드를 배포할 때 다음 중 하나를 수행할 수 있습니다.

- admin_ip 매개 변수를 사용하여 기본 관리 노드의 IP 주소를 수동으로 입력할 수 있습니다.
- admin_ip 매개 변수를 생략하여 그리드 노드가 값을 자동으로 검색하도록 할 수 있습니다. 자동 검색은 그리드 네트워크가 DHCP를 사용하여 기본 관리 노드에 IP 주소를 할당할 때 특히 유용합니다.

운영 관리자 노드의 자동 검색은 멀티캐스트 도메인 이름 시스템(mDNS)을 사용하여 수행됩니다. 운영 관리 노드가 처음 시작되면 mDNS를 사용하여 해당 IP 주소를 게시합니다. 그런 다음 동일한 서브넷에 있는 다른 노드에서 IP 주소를 쿼리하고 자동으로 가져올 수 있습니다. 그러나 멀티캐스트 IP 트래픽은 일반적으로 서브넷 간에 라우팅할 수 없기 때문에 다른 서브넷의 노드는 기본 관리 노드의 IP 주소를 직접 획득할 수 없습니다.

자동 검색을 사용하는 경우:

- 기본 관리 노드가 직접 연결되지 않은 서브넷에 있는 하나 이상의 그리드 노드에 대해 admin_IP 설정을 포함해야 합니다. 이 그리드 노드는 mDNS로 검색할 서브넷의 다른 노드에 대한 기본 관리 노드의 IP 주소를 게시합니다.
- 네트워크 인프라스트럭처가 서브넷 내의 다중 캐스트 IP 트래픽 전달을 지원하는지 확인합니다.

StorageGRID 노드를 가상 머신으로 구축합니다

VMware vSphere Web Client를 사용하여 각 그리드 노드를 가상 머신으로 구축합니다. 배포 중에는 각 그리드 노드가 하나 이상의 StorageGRID 네트워크에 생성되고 연결됩니다.

StorageGRID 어플라이언스 스토리지 노드를 배포해야 하는 경우 어플라이언스의 설치 및 유지 관리 지침을 참조하십시오.

선택적으로 노드의 전원을 켜기 전에 노드 포트를 재매핑하거나 노드의 CPU 또는 메모리 설정을 늘릴 수 있습니다.

필요한 것

- 방법을 검토했습니다 설치 계획 및 준비소프트웨어, CPU 및 RAM, 스토리지 및 성능에 대한 요구 사항을 이해하고 있습니다.
- VMware vSphere 하이퍼바이저에 대해 잘 알고 있으며 이 환경에서 가상 머신을 구축한 경험이 있습니다.

  StorageGRID 가상 시스템에는 VMware Tools와 유사한 오픈 소스 구축 방식인 오픈 VM 툴 패키지가 포함되어 있습니다. VMware Tools를 수동으로 설치할 필요는 없습니다.

- VMware용 StorageGRID 설치 아카이브의 올바른 버전을 다운로드하고 압축을 풀었습니다.

  확장 또는 복구 작업의 일부로 새 노드를 구축하는 경우 현재 그리드에서 실행 중인 StorageGRID 버전을 사용해야 합니다.

- StorageGRID 가상 머신 디스크(".vmdk") 파일이 있습니다.

```
NetApp-SG-version-SHA.vmdk
```

- 배포하려는 그리드 노드 유형별로 ".ovf" 및 ".mf" 파일이 있습니다.

파일 이름	설명
vsphere-primary-admin.ovf vsphere-primary-admin.mf	기본 관리 노드의 템플릿 파일 및 매니페스트 파일
vsphere - non-primary-admin.ovf vsphere - non-primary-admin.mf	비 기본 관리 노드에 대한 템플릿 파일 및 매니페스트 파일입니다.
vsphere-archive.ovf vsphere-archive.mf를 참조하십시오	아카이브 노드의 템플릿 파일 및 매니페스트 파일입니다.

파일 이름	설명
vsphere-gateway.ovf vsphere-gateway.mf	게이트웨이 노드의 템플릿 파일 및 매니페스트 파일
vsphere-storage.ovf vsphere-storage.mf	스토리지 노드의 템플릿 파일 및 매니페스트 파일

- 같은 디렉토리에 .vdmk, .ovf, .mf 파일이 모두 있습니다.
- 장애 도메인을 최소화할 계획이 있습니다. 예를 들어, 단일 가상 시스템 서버에 모든 게이트웨이 노드를 배포해서는 안 됩니다.

> 운영 구축 시 단일 가상 머신 서버에서 스토리지 노드를 두 개 이상 실행하지 마십시오. 각 스토리지 노드에 대해 전용 가상 머신 호스트를 사용하면 격리된 장애 도메인이 제공됩니다.

- 확장 또는 복구 작업의 일부로 노드를 구축하는 경우 를 사용할 수 있습니다 StorageGRID 시스템 확장을 위한 지침 또는 을 누릅니다 복구 및 유지 관리 지침.
- NetApp ONTAP 시스템에서 할당된 스토리지를 가진 가상 머신으로 StorageGRID 노드를 구축하는 경우 해당 볼륨에 FabricPool 계층화 정책이 활성화되어 있지 않음을 확인합니다. 예를 들어 StorageGRID 노드가 VMware 호스트에서 가상 머신으로 실행 중인 경우 데이터 저장소를 백업하는 볼륨에 FabricPool 계층화 정책이 설정되어 있지 않은지 확인합니다. StorageGRID 노드와 함께 사용되는 볼륨에 대해 FabricPool 계층화를 사용하지 않도록 설정하면 문제 해결과 스토리지 작업이 간소화됩니다.

> FabricPool를 사용하여 StorageGRID 관련 데이터를 StorageGRID 자체로 계층화하지 마십시오. StorageGRID 데이터를 StorageGRID로 다시 계층화하면 문제 해결과 운영 복잡성이 늘어납니다.

이 작업에 대해

이 지침에 따라 초기에 VMware 노드를 배포하거나, 확장 시 새 VMware 노드를 추가하거나, 복구 작업의 일부로 VMware 노드를 대체하십시오. 단계에서 설명한 경우를 제외하고 노드 배포 절차는 관리 노드, 스토리지 노드, 게이트웨이 노드 및 아카이브 노드를 비롯한 모든 노드 유형에 대해 동일합니다.

새 StorageGRID 시스템을 설치하는 경우:

- 다른 그리드 노드를 배포하기 전에 기본 관리자 노드를 배포해야 합니다.
- 각 가상 시스템이 그리드 네트워크를 통해 기본 관리 노드에 연결할 수 있는지 확인해야 합니다.
- 그리드를 구성하기 전에 모든 그리드 노드를 배포해야 합니다.

확장 또는 복구 작업을 수행하는 경우:

- 새 가상 머신이 그리드 네트워크를 통해 기본 관리 노드에 연결할 수 있는지 확인해야 합니다.

노드의 포트를 다시 매핑해야 하는 경우 포트 재매핑 구성이 완료될 때까지 새 노드의 전원을 켜서는 안 됩니다.

단계

1. vCenter를 사용하여 OVF 템플릿을 구축합니다.

   URL을 지정하는 경우 다음 파일이 포함된 폴더를 가리킵니다. 그렇지 않으면 로컬 디렉토리에서 각 파일을 선택합니다.

```
NetApp-SG-version-SHA.vmdk
vsphere-node.ovf
vsphere-node.mf
```

예를 들어 처음 구축하는 노드인 경우 다음 파일을 사용하여 StorageGRID 시스템의 기본 관리 노드를 배포합니다.

```
NetApp-SG-version-SHA.vmdk
sphere-primary-admin.ovf
sphere-primary-admin.mf
```

2. 가상 머신의 이름을 지정합니다.

   표준 방법은 가상 머신과 그리드 노드 모두에 동일한 이름을 사용하는 것입니다.

3. 가상 머신을 적절한 vApp 또는 리소스 풀에 배치합니다.
4. 기본 관리자 노드를 배포하는 경우 최종 사용자 라이센스 계약을 읽고 동의합니다.

   vCenter 버전에 따라 최종 사용자 라이센스 계약에 동의하고, 가상 머신의 이름을 지정하고, 데이터 저장소를 선택할 때 단계의 순서가 달라집니다.

5. 가상 머신에 사용할 스토리지를 선택합니다.

   복구 작업의 일부로 노드를 구축하는 경우 의 지침을 수행합니다 스토리지 복구 단계입니다 새 가상 디스크를 추가하려면 오류가 발생한 그리드 노드에서 가상 하드 디스크를 다시 연결하거나 둘 다 다시 연결합니다.

   스토리지 노드를 구축할 때는 3개 이상의 스토리지 볼륨을 사용하고 각 스토리지 볼륨은 4TB 이상을 사용합니다. 볼륨 0에 4TB 이상을 할당해야 합니다.

   > Storage Node.ovf 파일은 스토리지를 위한 여러 VMDK를 정의합니다. 이러한 VMDK가 스토리지 요구 사항을 충족하지 않는 경우 노드의 전원을 켜기 전에 해당 VMDK를 제거하고 스토리지에 적절한 VMDK 또는 RDM을 할당해야 합니다. vmdks는 VMware 환경에서 일반적으로 사용되며 관리하기가 더 쉽습니다. 반면 RDM은 100MB 이상의 큰 개체 크기를 사용하는 워크로드에 더 나은 성능을 제공할 수 있습니다.

   > 일부 StorageGRID 설치에서는 일반 가상화 워크로드보다 더 크고 사용 빈도가 높은 스토리지 볼륨을 사용할 수 있습니다. 최적의 성능을 얻으려면 MaxAddressableSpaceTB와 같은 일부 하이퍼바이저 매개 변수를 조정해야 할 수 있습니다. 성능 저하가 발생하는 경우 가상화 지원 리소스에 문의하여 작업 부하별 구성 조정을 통해 해당 환경이 이점을 누릴 수 있는지 확인하십시오.

6. 네트워크를 선택합니다.

   각 소스 네트워크의 대상 네트워크를 선택하여 노드가 사용할 StorageGRID 네트워크를 결정합니다.

   - 그리드 네트워크가 필요합니다. vSphere 환경에서 대상 네트워크를 선택해야 합니다.
   - 관리 네트워크를 사용하는 경우 vSphere 환경에서 다른 대상 네트워크를 선택합니다. 관리 네트워크를 사용하지 않는 경우 그리드 네트워크에 대해 선택한 것과 동일한 대상을 선택합니다.

- 클라이언트 네트워크를 사용하는 경우 vSphere 환경에서 다른 대상 네트워크를 선택합니다. 클라이언트 네트워크를 사용하지 않는 경우 그리드 네트워크에 대해 선택한 것과 동일한 대상을 선택합니다.

7. 템플릿 사용자 정의 * 에서 필요한 StorageGRID 노드 속성을 구성합니다.

   a. 노드 이름 * 을 입력합니다.

   > 그리드 노드를 복구하는 경우 복구할 노드의 이름을 입력해야 합니다.

   b. Grid Network(eth0) * 섹션에서 * Grid 네트워크 IP 구성 * 에 대해 static 또는 DHCP를 선택합니다.

      - 정자를 선택한 경우 * 그리드 네트워크 IP *, * 그리드 네트워크 마스크 *, * 그리드 네트워크 게이트웨이 * 및 * 그리드 네트워크 MTU * 를 입력합니다.
      - DHCP를 선택하면 * 그리드 네트워크 IP *, * 그리드 네트워크 마스크 * 및 * 그리드 네트워크 게이트웨이 * 가 자동으로 할당됩니다.

   c. Primary Admin IP * 필드에 Grid Network에 대한 기본 관리 노드의 IP 주소를 입력합니다.

   > 구축하는 노드가 기본 관리 노드인 경우에는 이 단계가 적용되지 않습니다.

   기본 관리 노드 IP 주소를 생략하면 기본 관리 노드 또는 admin_IP가 구성된 다른 그리드 노드가 동일한 서브넷에 있는 경우 IP 주소가 자동으로 검색됩니다. 그러나 여기서 기본 관리 노드 IP 주소를 설정하는 것이 좋습니다.

   a. 관리 네트워크(eth1) * 섹션에서 * 관리 네트워크 IP 구성 * 에 대해 정적, DHCP 또는 비활성화를 선택합니다.

      - 관리 네트워크를 사용하지 않으려면 비활성화를 선택하고 관리 네트워크 IP에 * 0.0.0.0 * 을 입력합니다. 다른 필드는 비워 둘 수 있습니다.
      - static을 선택한 경우 * Admin network ip *, * Admin network mask *, * Admin network gateway *, * Admin network mtu * 를 입력합니다.
      - static을 선택한 경우 * Admin network external subnet list * 를 입력합니다. 또한 게이트웨이를 구성해야 합니다.
      - DHCP를 선택하면 * 관리 네트워크 IP *, * 관리 네트워크 마스크 * 및 * 관리 네트워크 게이트웨이 * 가 자동으로 할당됩니다.

   b. 클라이언트 네트워크(eth2) * 섹션에서 * 클라이언트 네트워크 IP 구성 * 에 대해 정적, DHCP 또는 비활성화를 선택합니다.

      - 클라이언트 네트워크를 사용하지 않으려면 비활성화를 선택하고 클라이언트 네트워크 IP에 * 0.0.0.0 * 을 입력합니다. 다른 필드는 비워 둘 수 있습니다.
      - static을 선택한 경우 * Client network IP *, * Client network mask *, * Client network gateway *, * Client network mtu * 를 입력합니다.
      - DHCP를 선택하면 * 클라이언트 네트워크 IP *, * 클라이언트 네트워크 마스크 * 및 * 클라이언트 네트워크 게이트웨이 * 가 자동으로 할당됩니다.

8. 가상 시스템 구성을 검토하고 필요한 사항을 변경합니다.
9. 완료할 준비가 되면 * 마침 * 을 선택하여 가상 머신 업로드를 시작합니다.
10. 이 노드를 복구 작업의 일부로 배포했으며 전체 노드 복구가 아닌 경우 구축이 완료된 후 다음 단계를 수행하십시오.

    a. 가상 컴퓨터를 마우스 오른쪽 단추로 클릭하고 * 설정 편집 * 을 선택합니다.

    b. 스토리지에 지정된 각 기본 가상 하드 디스크를 선택하고 * 제거 * 를 선택합니다.

c. 데이터 복구 상황에 따라 저장소 요구 사항에 따라 새 가상 디스크를 추가하거나 이전에 제거된 장애 그리드 노드에서 보존된 가상 하드 디스크를 다시 연결하거나 두 디스크 모두를 다시 연결합니다.

다음 중요 지침을 참고하십시오.

- 새 디스크를 추가하는 경우 노드 복구 전에 사용한 것과 동일한 유형의 스토리지 디바이스를 사용해야 합니다.
- Storage Node.ovf 파일은 스토리지를 위한 여러 VMDK를 정의합니다. 이러한 VMDK가 스토리지 요구 사항을 충족하지 않는 경우 노드의 전원을 켜기 전에 해당 VMDK를 제거하고 스토리지에 적절한 VMDK 또는 RDM을 할당해야 합니다. vmdks는 VMware 환경에서 일반적으로 사용되며 관리하기가 더 쉽습니다. 반면 RDM은 100MB 이상의 큰 개체 크기를 사용하는 워크로드에 더 나은 성능을 제공할 수 있습니다.

11. 이 노드에서 사용하는 포트를 다시 매핑해야 하는 경우 다음 단계를 수행하십시오.

엔터프라이즈 네트워킹 정책이 StorageGRID에서 사용하는 하나 이상의 포트에 대한 액세스를 제한하는 경우 포트를 다시 매핑해야 할 수 있습니다. 를 참조하십시오 네트워킹 지침 StorageGRID에서 사용하는 포트의 경우

> 로드 밸런서 끝점에 사용되는 포트를 다시 매핑하지 마십시오.

a. 새 VM을 선택합니다.

b. 구성 탭에서 * 설정 * > * vApp 옵션 * 을 선택합니다. vApp 옵션 * 의 위치는 vCenter 버전에 따라 다릅니다.

c. Properties * 표에서 port_remap_inbound 및 port_remap을 찾습니다.

d. 포트의 인바운드 및 아웃바운드 통신을 대칭적으로 매핑하려면 * port_remap * 을 선택합니다.

> port_remap 만 설정된 경우 지정하는 매핑이 인바운드 및 아웃바운드 통신 모두에 적용됩니다. port_remap_inbound 도 지정된 경우 port_remap 은 아웃바운드 통신에만 적용됩니다.

i. 테이블 맨 위로 스크롤하여 * Edit * 를 선택합니다.

ii. 유형 탭에서 * 사용자 구성 가능 * 을 선택하고 * 저장 * 을 선택합니다.

iii. Set Value * 를 선택합니다.

iv. 포트 매핑을 입력합니다.

```
<network type>/<protocol>/<default port used by grid node>/<new
port>
```

'<network type>'은(는) 그리드, 관리자 또는 클라이언트이며, '<protocol>'은(는) TCP 또는 UDP입니다.

예를 들어 포트 22에서 포트 3022로 ssh 트래픽을 재매핑하려면 다음을 입력합니다.

```
client/tcp/22/3022
```

i. OK * 를 선택합니다.

e. 노드에 대한 인바운드 통신에 사용되는 포트를 지정하려면 * port_remap_inbound * 를 선택합니다.

> port_remap_inbound 를 지정하고 port_remap 의 값을 지정하지 않으면 포트의 아웃바운드 통신이 변경되지 않습니다.

i. 테이블 맨 위로 스크롤하여 * Edit * 를 선택합니다.

ii. 유형 탭에서 * 사용자 구성 가능 * 을 선택하고 * 저장 * 을 선택합니다.

iii. Set Value * 를 선택합니다.

iv. 포트 매핑을 입력합니다.

```
<network type>/<protocol>/<remapped inbound port>/<default inbound
port used by grid node>
```

'<network type>'은(는) 그리드, 관리자 또는 클라이언트이며, '<protocol>'은(는) TCP 또는 UDP입니다.

예를 들어, 포트 3022로 전송된 인바운드 SSH 트래픽을 그리드 노드가 포트 22에서 수신하도록 재매핑하려면 다음을 입력합니다.

```
client/tcp/3022/22
```

i. OK * 를 선택합니다

12. 노드의 CPU 또는 메모리를 기본 설정에서 늘리려면 다음을 수행합니다.

a. 가상 컴퓨터를 마우스 오른쪽 단추로 클릭하고 * 설정 편집 * 을 선택합니다.

b. 필요한 경우 CPU 수 또는 메모리 양을 변경합니다.

메모리 예약 * 을 가상 머신에 할당된 * 메모리 * 와 동일한 크기로 설정합니다.

c. OK * 를 선택합니다.

13. 가상 머신의 전원을 켭니다.

작업을 마친 후

이 노드를 확장 또는 복구 절차의 일부로 배포한 경우 해당 지침으로 돌아가 절차를 완료하십시오.

그리드 구성 및 설치 완료(VMware)

그리드 관리자로 이동합니다

그리드 관리자를 사용하여 StorageGRID 시스템을 구성하는 데 필요한 모든 정보를 정의합니다.

필요한 것

기본 관리 노드를 구축하고 초기 시작 시퀀스를 완료해야 합니다.

단계

1. 웹 브라우저를 열고 다음 주소 중 하나로 이동합니다.

"https://*primary_admin_node_ip*`

'*client_network_ip*'

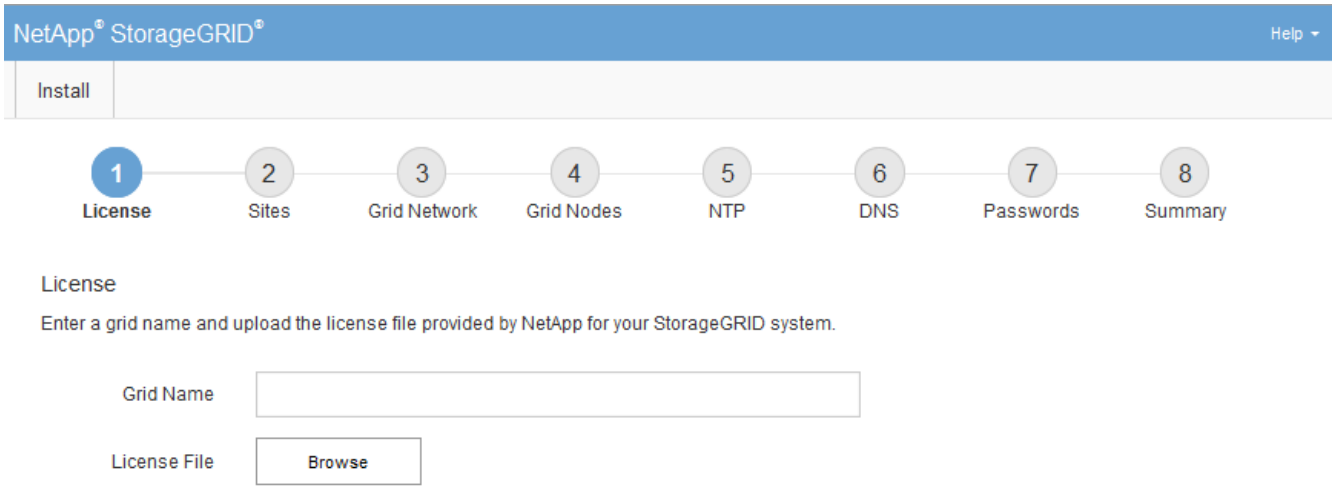
또는 포트 8443에서 그리드 관리자에 액세스할 수 있습니다.

"https://*primary_admin_node_ip*:8443`

> 네트워크 구성에 따라 그리드 네트워크 또는 관리 네트워크의 기본 관리 노드 IP에 대한 IP 주소를 사용할 수 있습니다.

2. StorageGRID 시스템 설치 * 를 클릭합니다.

   StorageGRID 그리드를 구성하는 데 사용되는 페이지가 나타납니다.



StorageGRID 라이센스 정보를 지정합니다

StorageGRID 시스템의 이름을 지정하고 NetApp에서 제공하는 라이센스 파일을 업로드해야 합니다.

단계

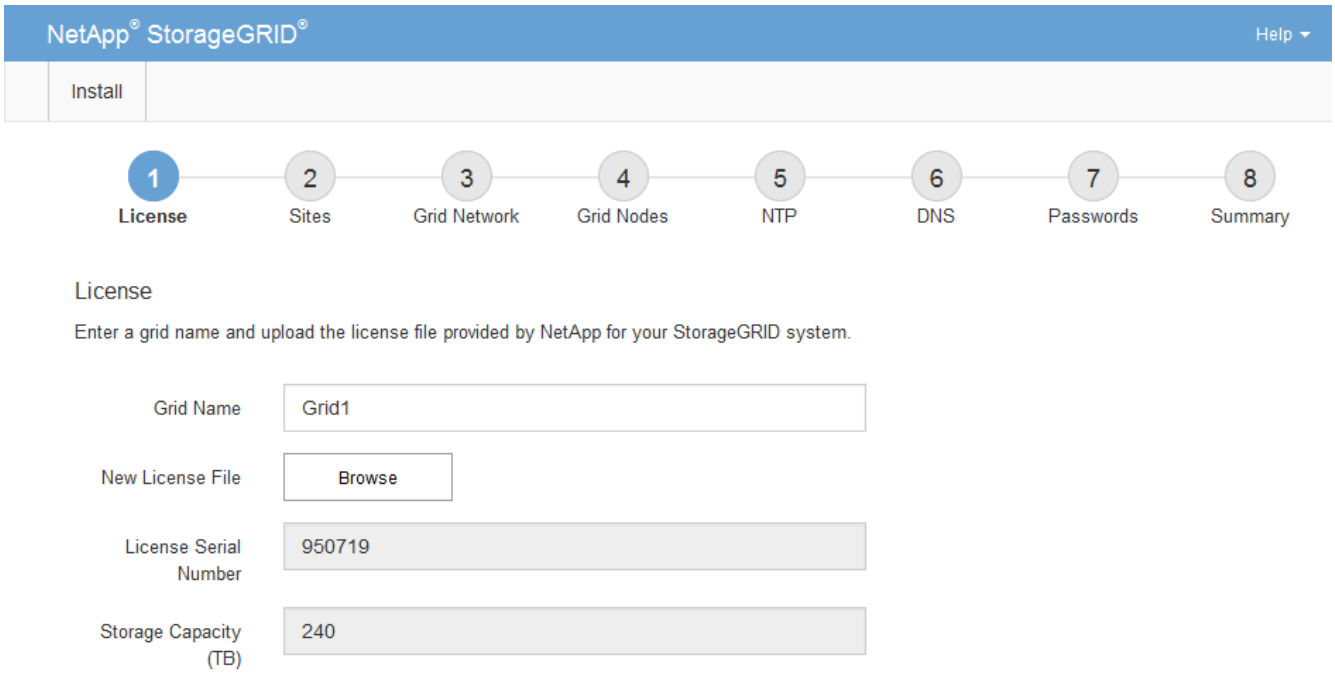
1. 라이센스 페이지의 * 그리드 이름 * 에 StorageGRID 시스템에 대한 의미 있는 이름을 입력합니다.

   설치 후, 이름이 Nodes 메뉴 맨 위에 표시됩니다.

2. 찾아보기 * 를 클릭하고 NetApp 라이센스 파일('NLFunique_id.txt')을 찾은 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.

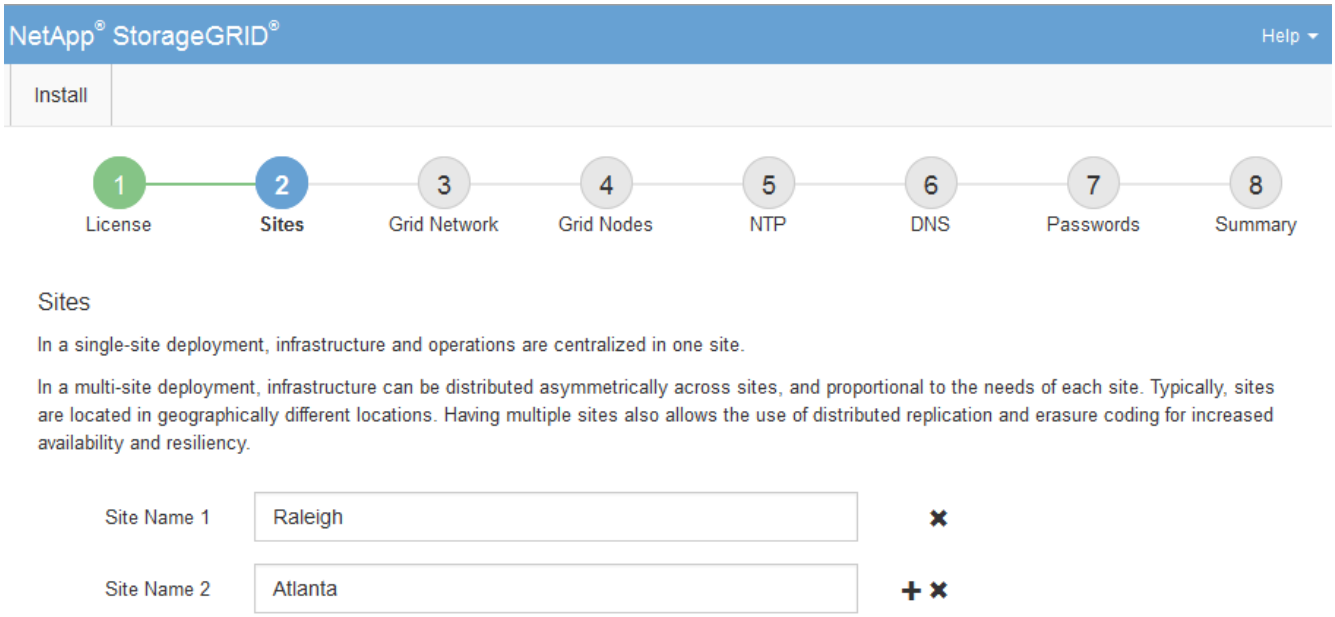
사이트를 추가합니다

StorageGRID를 설치할 때 사이트를 하나 이상 만들어야 합니다. StorageGRID 시스템의 안정성과 스토리지 용량을 늘리기 위해 사이트를 추가로 생성할 수 있습니다.

단계

1. 사이트 페이지에서 * 사이트 이름 * 을 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.

그리드 네트워크 서브넷을 지정합니다

그리드 네트워크에서 사용되는 서브넷을 지정해야 합니다.

이 작업에 대해

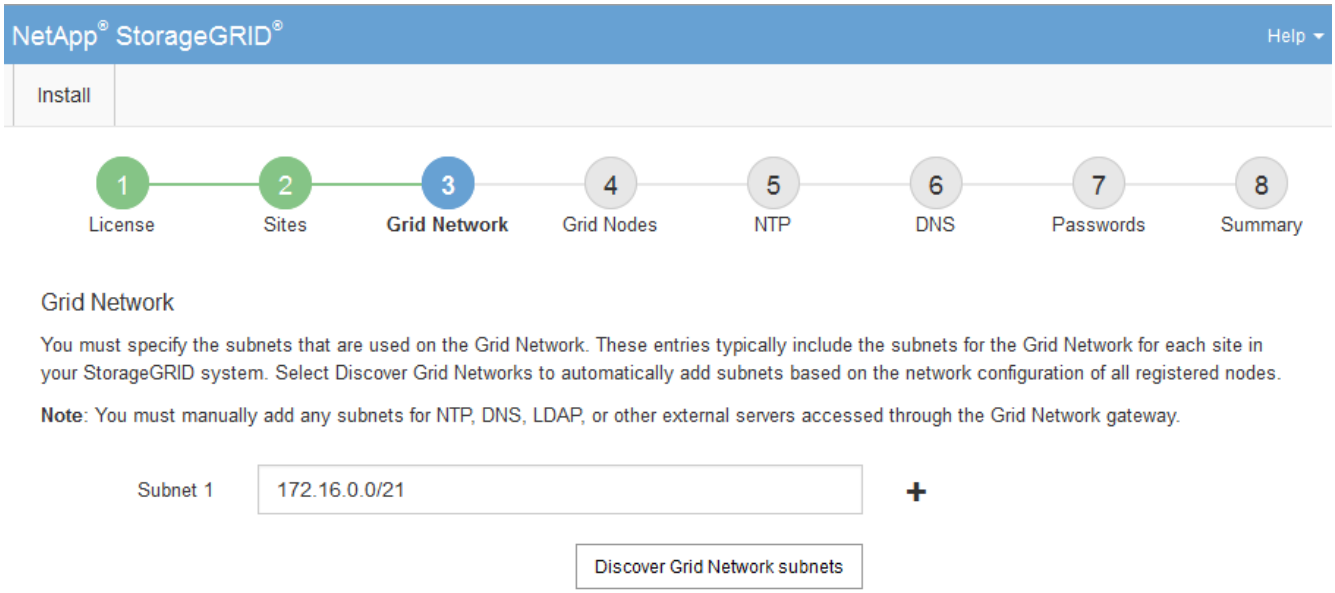
서브넷 항목에는 그리드 네트워크를 통해 연결할 수 있어야 하는 서브넷과 함께 StorageGRID 시스템의 각 사이트에 대한 그리드 네트워크의 서브넷이 포함됩니다.

그리드 서브넷이 여러 개인 경우 그리드 네트워크 게이트웨이가 필요합니다. 지정된 모든 그리드 서브넷은 이 게이트웨이를 통해 연결할 수 있어야 합니다.

단계

1. 서브넷 1 * 텍스트 상자에 하나 이상의 그리드 네트워크에 대한 CIDR 네트워크 주소를 지정합니다.
2. 마지막 항목 옆에 있는 더하기 기호를 클릭하여 추가 네트워크 항목을 추가합니다.

   하나 이상의 노드를 이미 배포한 경우 * 그리드 네트워크 서브넷 검색 * 을 클릭하여 그리드 관리자에 등록된 그리드 노드에 의해 보고된 서브넷으로 그리드 네트워크 서브넷 목록을 자동으로 채웁니다.



3. 다음 * 을 클릭합니다.

보류 중인 그리드 노드를 승인합니다

StorageGRID 시스템에 가입하려면 각 그리드 노드를 승인해야 합니다.

필요한 것

모든 가상 및 StorageGRID 어플라이언스 그리드 노드를 구축했습니다.

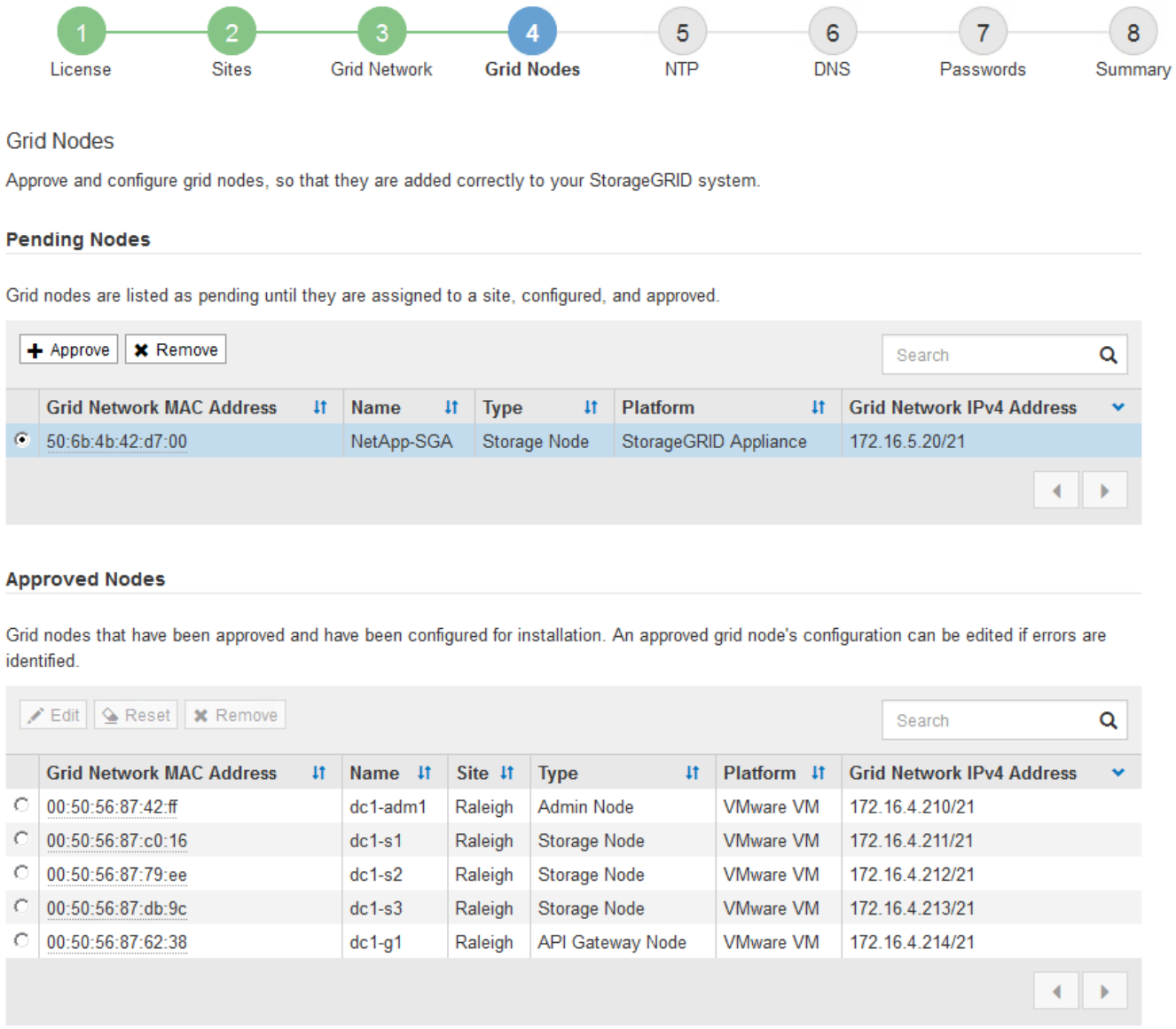
> 일부 노드를 나중에 설치하는 대신 모든 노드를 한 번 설치하는 것이 더 효율적입니다.

단계

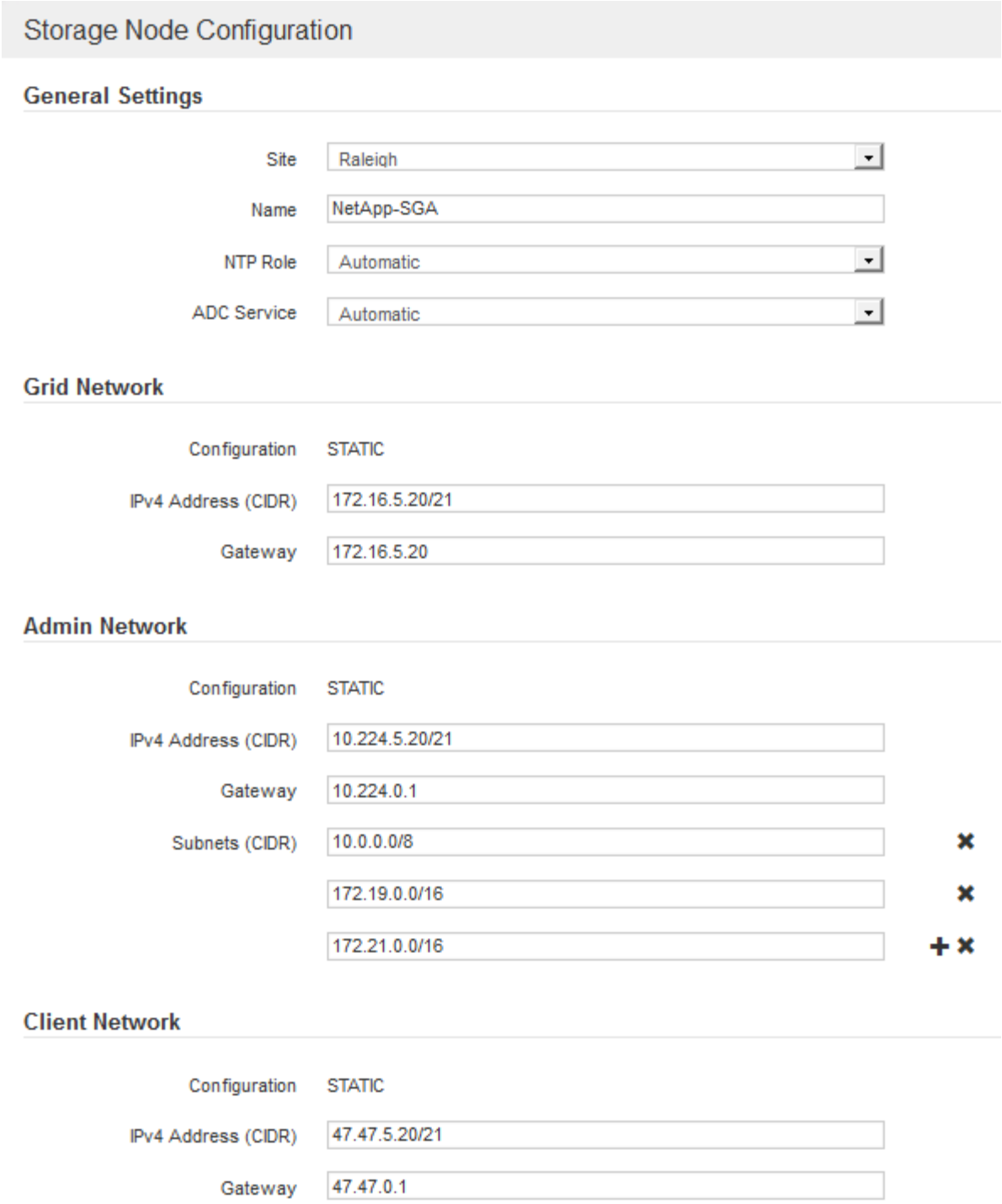
1. Pending Nodes(보류 중인 노드) 목록을 검토하고 배포된 모든 그리드 노드가 표시되는지 확인합니다.

> 그리드 노드가 누락된 경우 성공적으로 배포되었는지 확인합니다.

2. 승인하려는 보류 중인 노드 옆에 있는 라디오 버튼을 선택합니다.



3. Approve * (승인 *)를 클릭합니다.
4. 일반 설정에서 필요에 따라 다음 속성의 설정을 수정합니다.



- * Site *: 이 그리드 노드가 연결될 사이트의 이름입니다.
- * 이름 *: 노드에 할당될 이름 및 그리드 관리자에 표시될 이름입니다. 기본적으로 노드를 구성할 때 지정한 이름이 지정됩니다. 설치 프로세스의 이 단계에서 필요에 따라 이름을 변경할 수 있습니다.

> 설치를 완료한 후에는 노드 이름을 변경할 수 없습니다.

> VMware 노드의 경우 여기에서 이름을 변경할 수 있지만 이 작업은 vSphere에서 가상 머신의 이름을 변경하지 않습니다.

- * NTP 역할 *: 그리드 노드의 NTP(Network Time Protocol) 역할입니다. 옵션은 * 자동 *, * 기본 * 및 * 클라이언트 * 입니다. Automatic * 을 선택하면 기본 역할이 관리 노드, ADC 서비스가 있는 스토리지 노드, 게이트웨이 노드 및 비정적 IP 주소가 있는 모든 그리드 노드에 할당됩니다. 다른 모든 그리드 노드에는 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 노드 전용): 시스템에서 노드가 관리 도메인 컨트롤러(ADC) 서비스를 필요로 하는지 여부를 결정하도록 하려면 * 자동 * 을 선택합니다. ADC 서비스는 그리드 서비스의 위치 및 가용성을 추적합니다. 각 사이트에 적어도 3개의 스토리지 노드가 ADC 서비스를 포함해야 합니다. ADC 서비스를 배포한 후에는 노드에 추가할 수 없습니다.

5. Grid Network에서 필요에 따라 다음 속성의 설정을 수정합니다.

   - * IPv4 주소(CIDR) *: 그리드 네트워크 인터페이스(컨테이너 내부의 eth0)의 CIDR 네트워크 주소입니다. 예: 192.168.1.234/21
   - * 게이트웨이 *: 그리드 네트워크 게이트웨이. 예: 192.168.0.1

     > 그리드 서브넷이 여러 개인 경우 게이트웨이가 필요합니다.

   > 그리드 네트워크 구성에 대해 DHCP를 선택하고 여기서 값을 변경하면 새 값이 노드의 정적 주소로 구성됩니다. 결과 IP 주소가 DHCP 주소 풀 내에 있지 않은지 확인해야 합니다.

6. 그리드 노드에 대해 관리자 네트워크를 구성하려면 필요에 따라 관리 네트워크 섹션에서 설정을 추가하거나 업데이트합니다.

   이 인터페이스에서 나오는 라우트의 대상 서브넷을 * 서브넷(CIDR) * 텍스트 상자에 입력합니다. 관리 서브넷이 여러 개인 경우 관리 게이트웨이가 필요합니다.

   > Admin Network 구성에 대해 DHCP를 선택하고 여기서 값을 변경하면 새 값이 노드의 정적 주소로 구성됩니다. 결과 IP 주소가 DHCP 주소 풀 내에 있지 않은지 확인해야 합니다.

   - 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. 어플라이언스 재부팅: 어플라이언스 설치 프로그램에서 * 고급 * > * 재부팅 * 을 선택합니다.

        재부팅하는 데 몇 분 정도 걸릴 수 있습니다.

     b. 네트워크 구성 * > * 링크 구성 * 을 선택하고 해당 네트워크를 활성화합니다.

     c. 네트워킹 구성 * > * IP 구성 * 을 선택하고 활성화된 네트워크를 구성합니다.

     d. 홈 페이지로 돌아가서 * 설치 시작 * 을 클릭합니다.

     e. Grid Manager(그리드 관리자): 노드가 Approved Nodes(승인된 노드) 테이블에 나열된 경우 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.

   클라이언트 네트워크 구성에 대해 DHCP를 선택하고 여기서 값을 변경하면 새 값이 노드의 정적 주소로 구성됩니다. 결과 IP 주소가 DHCP 주소 풀 내에 있지 않은지 확인해야 합니다.

   - 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. 어플라이언스 재부팅: 어플라이언스 설치 프로그램에서 * 고급 * > * 재부팅 * 을 선택합니다.

        재부팅하는 데 몇 분 정도 걸릴 수 있습니다.

     b. 네트워크 구성 * > * 링크 구성 * 을 선택하고 해당 네트워크를 활성화합니다.

     c. 네트워킹 구성 * > * IP 구성 * 을 선택하고 활성화된 네트워크를 구성합니다.

     d. 홈 페이지로 돌아가서 * 설치 시작 * 을 클릭합니다.

     e. Grid Manager(그리드 관리자): 노드가 Approved Nodes(승인된 노드) 테이블에 나열된 경우 노드를 재설정합니다.

     f. Pending Nodes 테이블에서 노드를 제거합니다.

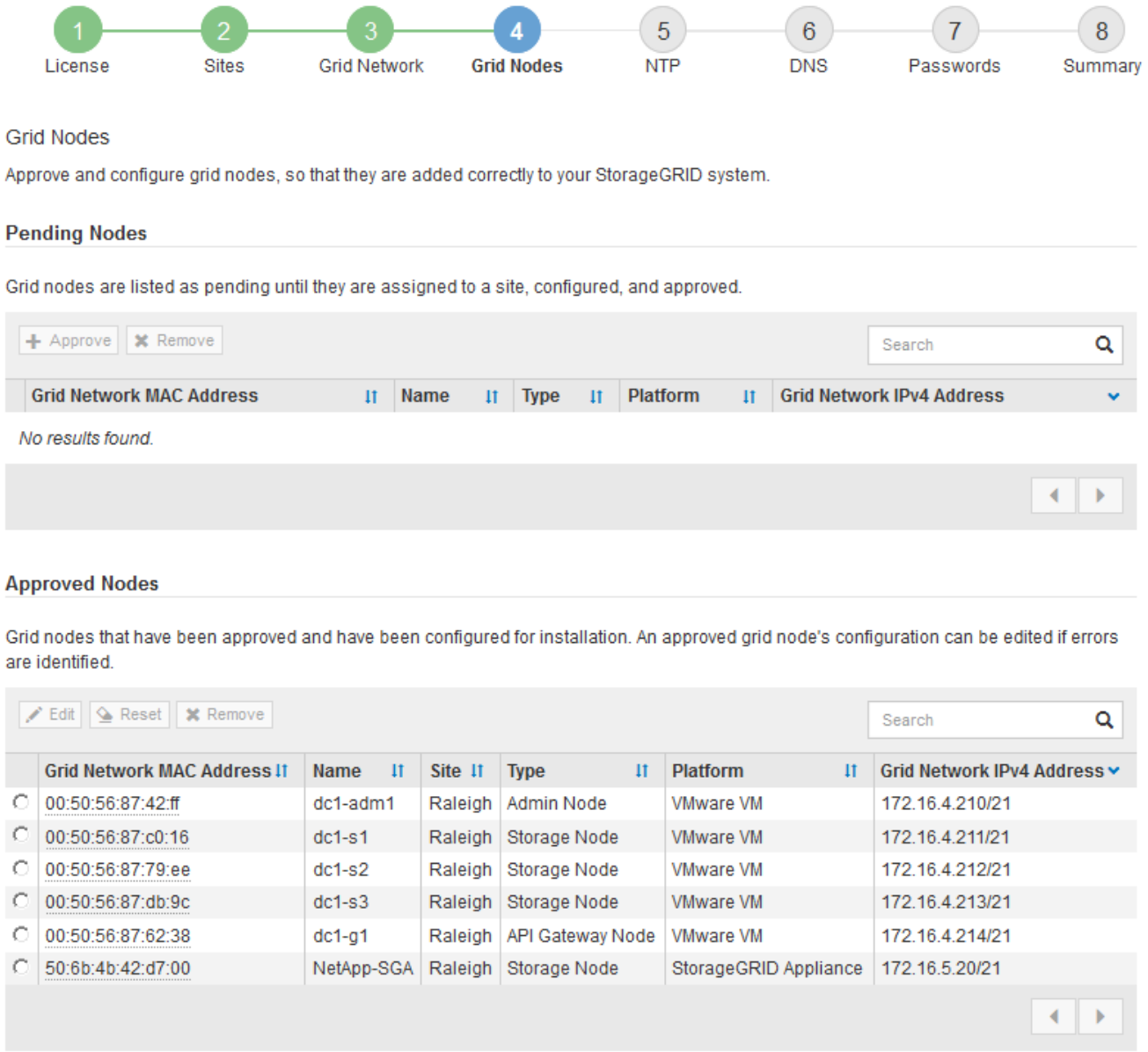
     g. 대기 중인 노드 목록에 노드가 다시 나타날 때까지 기다립니다.

     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. 승인하려는 보류 중인 각 그리드 노드에 대해 이 단계를 반복합니다.

   그리드에서 원하는 모든 노드를 승인해야 합니다. 그러나 요약 페이지에서 * 설치 * 를 클릭하기 전에 언제든지 이 페이지로 돌아갈 수 있습니다. 라디오 버튼을 선택하고 * Edit * 를 클릭하여 승인된 그리드 노드의 속성을 수정할 수 있습니다.

10. 그리드 노드 승인이 완료되면 * 다음 * 을 클릭합니다.

Network Time Protocol 서버 정보를 지정합니다

StorageGRID 시스템에 대해 NTP(네트워크 시간 프로토콜) 구성 정보를 지정해야 별도의 서버에서 수행되는 작업을 동기화할 수 있습니다.

이 작업에 대해

NTP 서버의 IPv4 주소를 지정해야 합니다.

외부 NTP 서버를 지정해야 합니다. 지정된 NTP 서버는 NTP 프로토콜을 사용해야 합니다.

시간 드리프트와 관련된 문제를 방지하려면 Stratum 3 이상의 NTP 서버 참조를 4개 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 Windows의 시간 서비스는 정확하지 않으며 StorageGRID와 같은 고정밀 환경에서 사용하기 위해 Microsoft에서 지원되지 않습니다.

"정확도가 높은 환경에 대한 Windows 시간 서비스를 구성하기 위한 경계를 지원합니다"

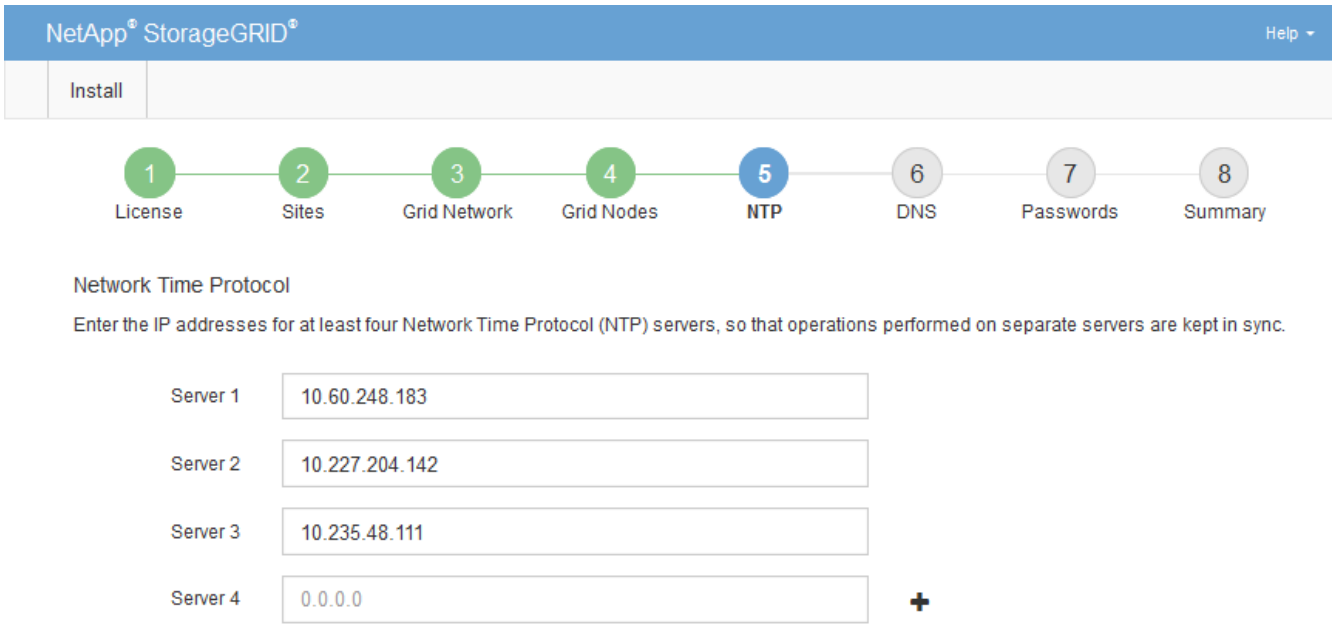
외부 NTP 서버는 이전에 기본 NTP 역할을 할당한 노드에서 사용됩니다.

> 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.

하이퍼바이저가 가상 머신과 동일한 NTP 소스를 사용하는지 확인하고 VMTools를 사용하여 하이퍼바이저와 StorageGRID 가상 머신 간의 시간 동기화를 해제하는 등 VMware에 대한 추가 검사를 수행합니다.

단계

1. Server 1 * 에서 * Server 4 * 텍스트 상자에 NTP 서버 4대 이상에 대한 IPv4 주소를 지정합니다.
2. 필요한 경우 마지막 항목 옆에 있는 더하기 기호를 선택하여 추가 서버 항목을 추가합니다.



3. 다음 * 을 선택합니다.

도메인 이름 시스템 서버 정보를 지정합니다

IP 주소 대신 호스트 이름을 사용하여 외부 서버에 액세스할 수 있도록 StorageGRID 시스템에 대한 DNS(도메인 이름 시스템) 정보를 지정해야 합니다.

이 작업에 대해

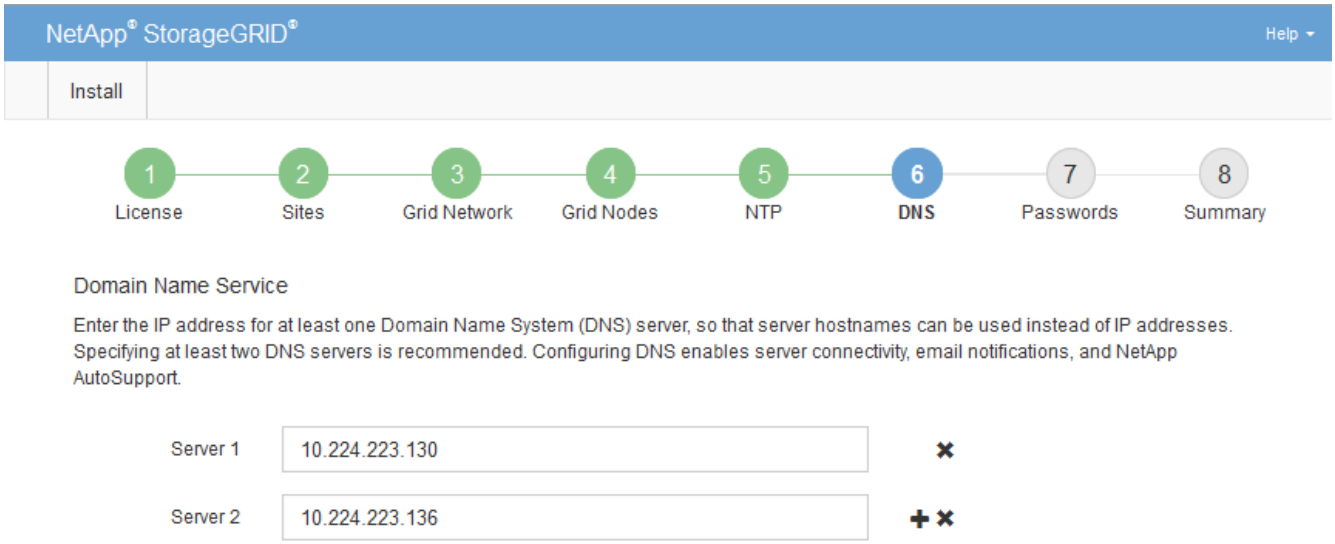
DNS 서버 정보를 지정하면 e-메일 알림 및 AutoSupport에 IP 주소 대신 FQDN(정규화된 도메인 이름) 호스트 이름을 사용할 수 있습니다. DNS 서버를 두 개 이상 지정하는 것이 좋습니다.

> DNS 서버에 2-6개의 IPv4 주소를 제공합니다. 네트워크 연결 시 각 사이트에서 로컬로 액세스할 수 있는 DNS 서버를 선택해야 합니다. 이는 Is착륙한 사이트가 계속해서 DNS 서비스에 액세스할 수 있도록 하기 위한 것입니다. 그리드 전체 DNS 서버 목록을 구성한 후 각 노드에 대해 DNS 서버 목록을 추가로 사용자 지정할 수 있습니다. 자세한 내용은 복구 및 유지 관리 지침 에서 DNS 구성 수정에 대한 정보를 참조하십시오.

DNS 서버 정보가 생략되거나 잘못 구성된 경우 각 그리드 노드의 SSM 서비스에서 NST 알람이 트리거됩니다. DNS가 올바르게 구성되고 새 서버 정보가 모든 그리드 노드에 도달하면 경보가 해제됩니다.

단계

1. Server 1 * 텍스트 상자에 하나 이상의 DNS 서버에 대한 IPv4 주소를 지정합니다.
2. 필요한 경우 마지막 항목 옆에 있는 더하기 기호를 선택하여 추가 서버 항목을 추가합니다.



   가장 좋은 방법은 DNS 서버를 두 개 이상 지정하는 것입니다. 최대 6개의 DNS 서버를 지정할 수 있습니다.

3. 다음 * 을 선택합니다.

관련 정보

복구 및 유지 관리

StorageGRID 시스템 암호를 지정합니다

StorageGRID 시스템을 설치하는 과정에서 시스템 보안을 유지하고 유지 관리 작업을 수행하는 데 사용할 암호를 입력해야 합니다.

이 작업에 대해

암호 설치 페이지를 사용하여 프로비저닝 암호 및 그리드 관리 루트 사용자 암호를 지정합니다.

- 프로비저닝 암호는 암호화 키로 사용되며 StorageGRID 시스템에 저장되지 않습니다.
- 복구 패키지 다운로드를 포함하여 설치, 확장 및 유지 관리 절차를 위한 프로비저닝 암호가 있어야 합니다. 따라서

프로비저닝 암호를 안전한 위치에 저장하는 것이 중요합니다.

- 현재 프로비저닝 암호가 있는 경우 Grid Manager에서 프로비저닝 암호를 변경할 수 있습니다.
- 그리드 관리 루트 사용자 암호는 Grid Manager를 사용하여 변경할 수 있습니다.
- 임의로 생성된 명령줄 콘솔 및 SSH 암호는 복구 패키지의 "passwords.txt" 파일에 저장됩니다.

단계

1. Provisioning Passphrase * 에서 StorageGRID 시스템의 그리드 토폴로지를 변경하는 데 필요한 프로비저닝 암호를 입력합니다.

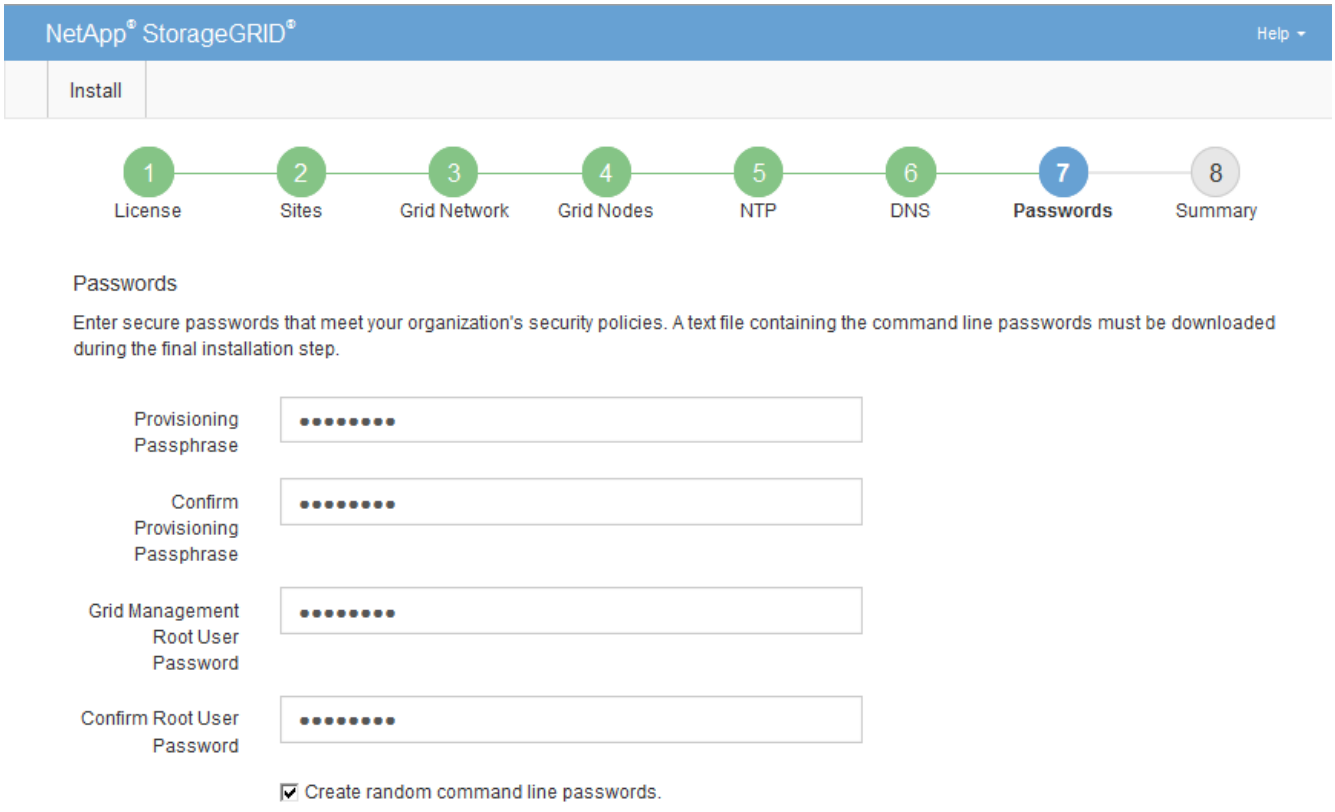
   프로비저닝 암호를 안전한 장소에 보관합니다.

   > 설치가 완료되고 나중에 프로비저닝 암호를 변경하려는 경우 Grid Manager를 사용할 수 있습니다. 구성 * > * 액세스 제어 * > * 그리드 비밀번호 * 를 선택합니다.

2. Provisioning Passphrase * 확인 에서 프로비저닝 암호를 다시 입력하여 확인합니다.
3. Grid Management Root User Password * 에서 Grid Manager에 ""root" 사용자로 액세스하는 데 사용할 암호를 입력합니다.

   암호를 안전한 곳에 보관하십시오.

4. 루트 사용자 암호 확인 * 에서 그리드 관리자 암호를 다시 입력하여 확인합니다.



5. 개념 증명이나 데모 목적으로 그리드를 설치하는 경우 * 임의의 명령줄 암호 만들기 * 확인란을 선택 취소합니다.

   프로덕션 배포의 경우 보안을 위해 항상 무작위 암호를 사용해야 합니다. ""root" 또는 ""admin" 계정을 사용하여 명령줄에서 그리드 노드에 액세스하기 위해 기본 암호를 사용하려는 경우 * 무작위 명령줄 암호 만들기 * 를 선택

취소합니다.

> 요약 페이지에서 * Install * 을 클릭하면 복구 패키지 파일('s GW-recovery-package-id-revision.zip')을 다운로드하라는 메시지가 표시됩니다. 반드시 해야 합니다 이 파일을 다운로드합니다 를 눌러 설치를 완료합니다. 시스템에 액세스하는 데 필요한 암호는 복구 패키지 파일에 포함된 "passwords.txt" 파일에 저장됩니다.

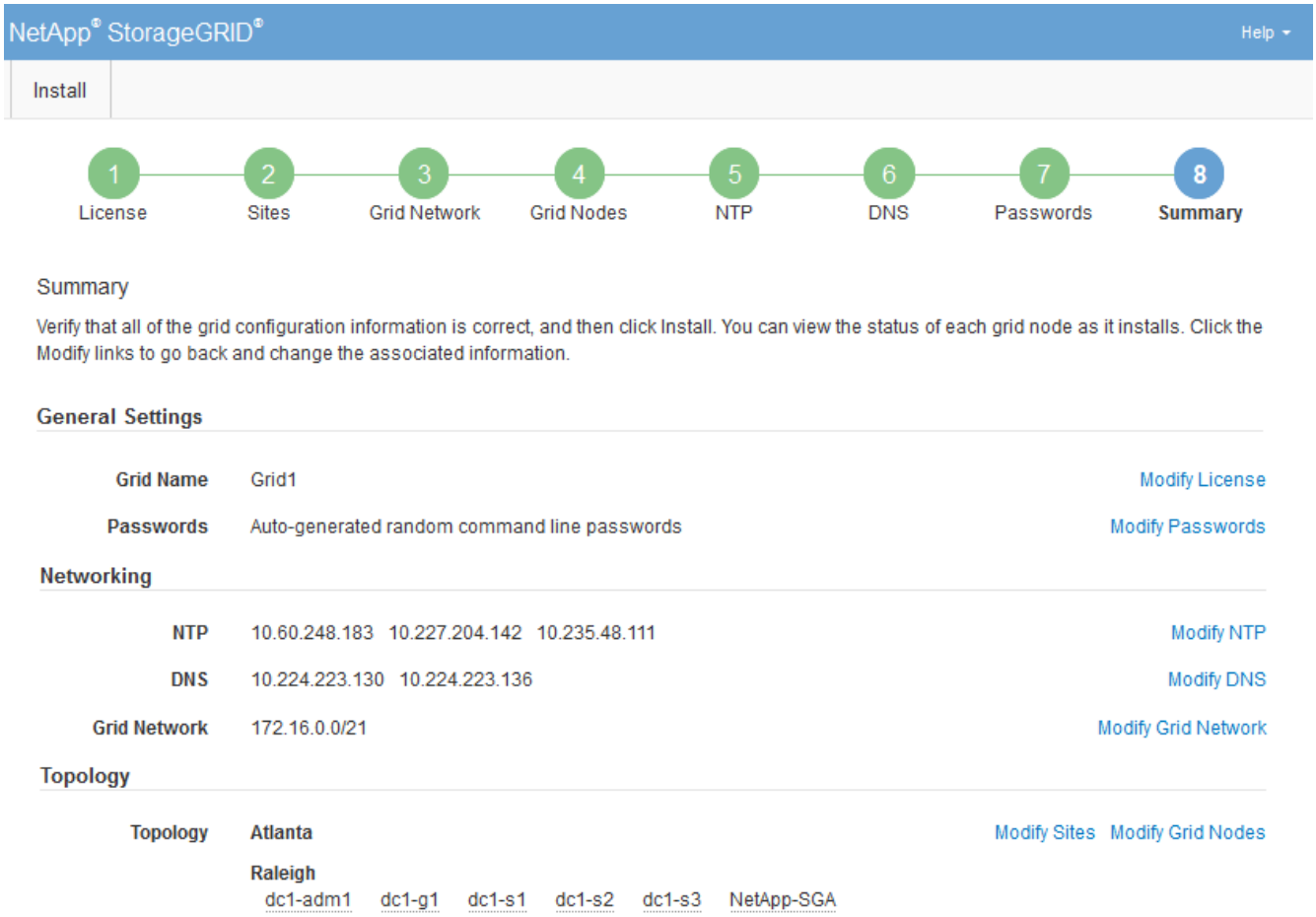
6. 다음 * 을 클릭합니다.

구성을 검토하고 설치를 완료합니다

설치를 성공적으로 완료하려면 입력한 구성 정보를 주의 깊게 검토해야 합니다.

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 끊어지면 액세스 가능한 서브넷을 통해 기본 관리 노드에 액세스하는지 확인해야 합니다. 을 참조하십시오 네트워킹 지침 를 참조하십시오.

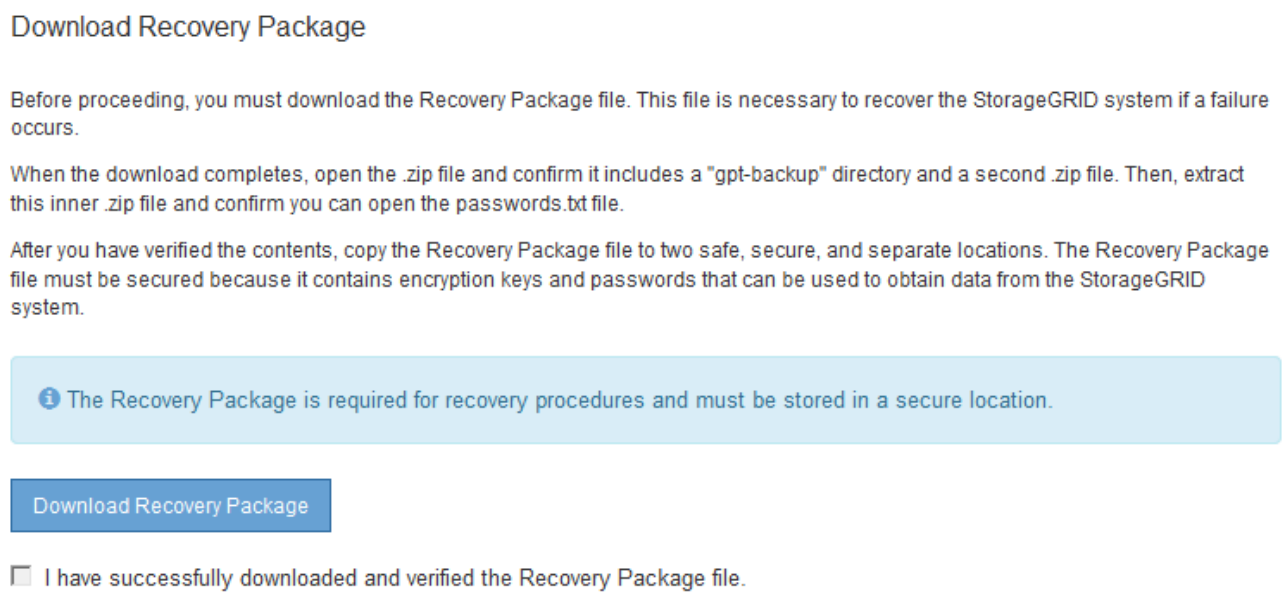
4. 복구 패키지 다운로드 * 를 클릭합니다.

   설치가 GRID 토폴로지를 정의한 지점으로 진행되면 복구 패키지 파일(".zip")을 다운로드하라는 메시지가 표시되고 이 파일의 내용에 액세스할 수 있는지 확인합니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 다운로드해야 합니다. 설치가 백그라운드에서 계속되지만 이 파일을 다운로드하여 확인하기 전에는 설치를 완료하고 StorageGRID 시스템에 액세스할 수 없습니다.

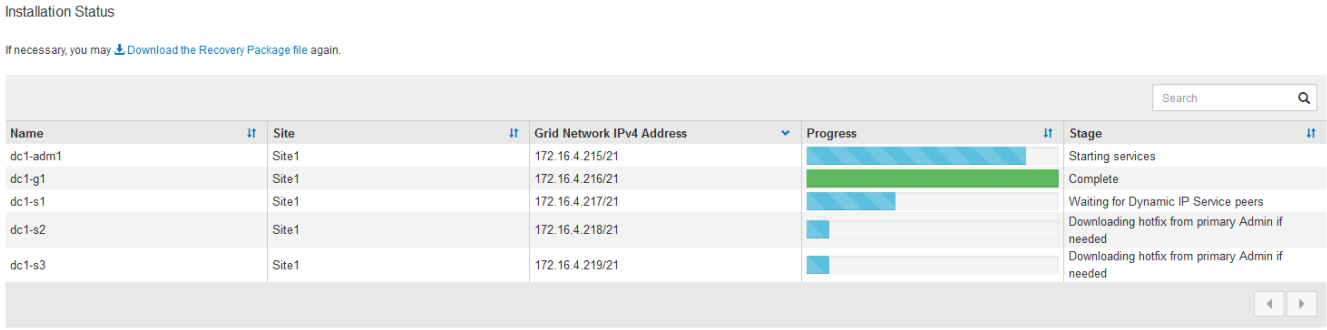
5. '.zip' 파일의 내용을 추출하여 안전한 별도의 두 위치에 저장할 수 있는지 확인합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

6. 복구 패키지 파일을 성공적으로 다운로드하고 확인했습니다. * 확인란을 선택하고 * 다음 * 을 클릭합니다.



설치가 진행 중인 경우 상태 페이지가 나타납니다. 이 페이지에는 각 그리드 노드의 설치 진행률이 표시됩니다.



모든 그리드 노드에 대해 전체 단계에 도달하면 그리드 관리자의 로그인 페이지가 나타납니다.

7. ""root" 사용자와 설치 중에 지정한 암호를 사용하여 Grid Manager에 로그인합니다.

설치 후 지침

그리드 노드 배포 및 구성을 완료한 후 DHCP 주소 지정 및 네트워크 구성 변경에 대한 다음 지침을 따르십시오.

- DHCP를 사용하여 IP 주소를 할당한 경우 사용 중인 네트워크의 각 IP 주소에 대해 DHCP 예약을 구성합니다.

  배포 단계에서는 DHCP만 설정할 수 있습니다. 구성 중에는 DHCP를 설정할 수 없습니다.

  > IP 주소가 변경되면 노드가 재부팅되므로 DHCP 주소 변경이 동시에 여러 노드에 영향을 미칠 경우 작동이 중단될 수 있습니다.

- 그리드 노드의 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 변경하려면 IP 변경 절차를 사용해야 합니다. 을 참조하십시오 IP 주소를 구성합니다.
- 라우팅 및 게이트웨이 변경을 비롯한 네트워킹 구성을 변경하면 기본 관리 노드 및 다른 그리드 노드에 대한 클라이언트 연결이 손실될 수 있습니다. 적용된 네트워킹 변경 사항에 따라 이러한 연결을 다시 설정해야 할 수 있습니다.

설치 자동화(VMware)

VMware vSphere를 사용하여 그리드 노드 구축을 자동화할 수 있습니다. StorageGRID의 구성을 자동화할 수도 있습니다.

그리드 노드 구축을 자동화합니다

VMware vSphere를 사용하여 그리드 노드의 구축 자동화

필요한 것

- Bash 3.2 이상이 설치된 Linux/Unix 시스템에 액세스할 수 있습니다.
- VMware OVF Tool 4.1이 설치되고 올바르게 구성되었습니다.
- OVF 툴을 사용하여 VMware vSphere에 액세스하는 데 필요한 사용자 이름과 암호를 알고 있습니다.
- StorageGRID 가상 머신을 구축할 vSphere의 위치에 대한 VI(가상 인프라) URL을 알고 있습니다. 이 URL은 일반적으로 vApp 또는 리소스 풀이 됩니다. 예: 'vi://vcenter.example.com/vi/sgws`

  > VMware "ovftool" 유틸리티를 사용하여 이 값을 확인할 수 있습니다(자세한 내용은 "ovftool" 설명서 참조).

  > vApp에 구축할 경우 가상 머신이 처음 시작될 때 자동으로 시작되지 않으며 수동으로 전원을 설정해야 합니다.

- 구성 파일에 필요한 모든 정보를 수집했습니다. 을 참조하십시오 배포 환경에 대한 정보를 수집합니다 를 참조하십시오.
- StorageGRID용 VMware 설치 아카이브에서 다음 파일에 액세스할 수 있습니다.

파일 이름	설명
NetApp-SG-version-SHA.vmdk입니다	그리드 노드 가상 머신을 생성하기 위한 템플릿으로 사용되는 가상 머신 디스크 파일입니다. • 참고: * 이 파일은 '.ovf' 및 '.mf' 파일과 같은 폴더에 있어야 합니다.
vsphere-primary-admin.ovf vsphere-primary-admin.mf	기본 관리 노드를 배포하기 위한 오픈 가상화 형식 템플릿 파일(".ovf") 및 매니페스트 파일(".mf")입니다.
vsphere - non-primary-admin.ovf vsphere - non-primary-admin.mf	비기본 관리 노드를 배포하기 위한 템플릿 파일(".ovf")과 매니페스트 파일(".mf")입니다.
vsphere-archive.ovf vsphere-archive.mf를 참조하십시오	아카이브 노드 배포를 위한 템플릿 파일(".ovf")과 매니페스트 파일(".mf")입니다.
vsphere-gateway.ovf vsphere-gateway.mf	게이트웨이 노드를 배포하기 위한 템플릿 파일(".ovf")과 매니페스트 파일(".mf")입니다.
vsphere-storage.ovf vsphere-storage.mf	가상 머신 기반 스토리지 노드 구축을 위한 템플릿 파일('.ovf') 및 매니페스트 파일('.mf')입니다.
deploy-vsphere-ovftool.sh	가상 그리드 노드의 배포를 자동화하는 데 사용되는 Bash 쉘 스크립트입니다.
deploy-vsphere-ovftool-sample.ini	이 샘플 구성 파일은 'deploy-vsphere-ovftool.sh' 스크립트와 함께 사용됩니다.

배포를 위한 구성 파일을 정의합니다

구성 파일에 StorageGRID용 가상 그리드 노드를 구축하는 데 필요한 정보를 지정합니다. 이 정보는 'Deploy-vSphere-ovftool.sh' Bash 스크립트에 사용됩니다. 파일을 처음부터 만들지 않도록 샘플 구성 파일을 수정할 수 있습니다.

단계

1. 샘플 구성 파일(ddeploy-vsphere-ovftool.sample.ini` )의 복사본을 만듭니다. 새 파일을 dedploy-vsphere-ovftool.sh와 같은 디렉토리에 dddeploy-vsphere-ovftool.ini` 로 저장합니다.
2. dddeploy-vsphere-ovftool.ini` 를 엽니다.
3. VMware 가상 그리드 노드를 구축하는 데 필요한 모든 정보를 입력합니다.

   을 참조하십시오 구성 파일 설정 를 참조하십시오.

4. 필요한 모든 정보를 입력하고 확인했으면 파일을 저장하고 닫습니다.

구성 파일 설정

deploy-vsphere-ovftool.ini` 구성 파일에는 가상 그리드 노드를 배포하는 데 필요한 설정이 포함되어 있습니다.

구성 파일은 먼저 글로벌 매개 변수를 나열한 다음 노드 이름으로 정의된 섹션에 노드별 매개 변수를 나열합니다. 파일이 사용되는 경우:

- _Global parameters_는 모든 그리드 노드에 적용됩니다.
- _노드별 parameters_override 전역 매개 변수입니다.

전역 매개 변수

전역 매개 변수는 개별 섹션의 설정에 의해 재정의되지 않는 한 모든 그리드 노드에 적용됩니다. 전역 매개 변수 섹션에서 여러 노드에 적용되는 매개 변수를 배치한 다음 필요에 따라 개별 노드의 섹션에서 이러한 설정을 재정의합니다.

- * OVFTOOL_Arguments *: OVFTOOL_Arguments을 전역 설정으로 지정하거나 특정 노드에 인수를 개별적으로 적용할 수 있습니다. 예를 들면 다음과 같습니다.

  ```
  OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
  --datastore='datastore_name'
  ```

  '--powerOffTarget' 및 '--overwrite' 옵션을 사용하여 기존 가상 시스템을 종료하고 교체할 수 있습니다.

  > 노드를 서로 다른 데이터 저장소에 배포하고 전역이 아닌 각 노드에 대해 OVFTOOL_MOUMENT를 지정해야 합니다.

- * source *: 개별 그리드 노드에 대한 StorageGRID 가상 머신 템플릿 파일(".vmdk") 및 ".ovf" 및 ".mf" 파일의 경로입니다. 이 기본값은 현재 디렉터리입니다.

  ```
  SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
  ```

- * 타겟 *: StorageGRID를 구축할 위치의 VMware vSphere 가상 인프라(vi) URL입니다. 예를 들면 다음과 같습니다.

  ```
  TARGET = vi://vcenter.example.com/vm/sgws
  ```

- * GRID_NETWORK_CONFIG *: 고정 또는 DHCP 중 IP 주소를 획득하는 데 사용되는 방법입니다. 기본값은 정적입니다. 모든 노드 또는 대부분의 노드가 동일한 방법으로 IP 주소를 획득하는 경우 여기에서 해당 방법을 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

  ```
  GRID_NETWORK_CONFIG = DHCP
  ```

- * GRID_NETWORK_TARGET *: 그리드 네트워크에 사용할 기존 VMware 네트워크의 이름입니다. 모든 노드 또는 대부분의 노드가 동일한 네트워크 이름을 사용하는 경우 여기에서 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
GRID_NETWORK_TARGET = SG-Admin-Network
```

- grid_network_mask *: 그리드 네트워크의 네트워크 마스크. 모든 노드 또는 대부분의 노드가 동일한 네트워크 마스크를 사용하는 경우 여기에서 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
GRID_NETWORK_MASK = 255.255.255.0
```

- grid_network_gateway *: 그리드 네트워크의 네트워크 게이트웨이. 모든 노드 또는 대부분의 노드가 동일한 네트워크 게이트웨이를 사용하는 경우 여기에서 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- *GRID_NETWORK_MTU *: 선택 사항. Grid Network의 MTU(Maximum Transmission Unit)입니다. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 예를 들면 다음과 같습니다.

```
GRID_NETWORK_MTU = 8192
```

이 인수를 생략하면 1400이 사용됩니다.

점보 프레임을 사용하려면 MTU를 9000과 같은 점보 프레임에 적합한 값으로 설정합니다. 그렇지 않으면 기본값을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 스위치 포트에 구성된 값과 일치해야 합니다. 그렇지 않으면 네트워크 성능 문제 또는 패킷 손실이 발생할 수 있습니다.

> 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

- * admin_network_Config *: IP 주소를 획득하는 데 사용되는 방법으로, 비활성화, 정적 또는 DHCP입니다. 기본값은 사용 안 함으로 설정되어 있습니다. 모든 노드 또는 대부분의 노드가 동일한 방법으로 IP 주소를 획득하는 경우 여기에서 해당 방법을 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
ADMIN_NETWORK_CONFIG = STATIC
```

- * admin_network_target *: 관리 네트워크에 사용할 기존 VMware 네트워크의 이름입니다. 이 설정은 관리 네트워크를 사용하지 않는 한 필요합니다. 모든 노드 또는 대부분의 노드가 동일한 네트워크 이름을 사용하는 경우 여기에서 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
ADMIN_NETWORK_TARGET = SG-Admin-Network
```

- * admin_network_mask *: 관리 네트워크의 네트워크 마스크입니다. 이 설정은 고정 IP 주소 지정을 사용하는 경우에 필요합니다. 모든 노드 또는 대부분의 노드가 동일한 네트워크 마스크를 사용하는 경우 여기에서 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- * admin_network_gateway *: 관리 네트워크의 네트워크 게이트웨이입니다. 이 설정은 정적 IP 주소 지정을 사용하고 admin_network_ESL 설정에서 외부 서브넷을 지정하는 경우에 필요합니다. (즉, admin_network_ESL이 비어 있으면 필요하지 않습니다.) 모든 노드 또는 대부분의 노드가 동일한 네트워크 게이트웨이를 사용하는 경우 여기에서 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- * admin_network_ESL *: 쉼표로 구분된 CIDR 라우트 대상 목록으로 지정된 관리 네트워크의 외부 서브넷 목록(라우트). 모든 노드 또는 대부분의 노드가 동일한 외부 서브넷 목록을 사용하는 경우 여기에서 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- * admin_network_mtu *: 선택 사항. 관리자 네트워크의 MTU(Maximum Transmission Unit) admin_network_Config = DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 이 인수를 생략하면 1400이 사용됩니다. 점보 프레임을 사용하려면 MTU를 9000과 같은 점보 프레임에 적합한 값으로 설정합니다. 그렇지 않으면 기본값을 유지합니다. 모든 노드 또는 대부분의 노드가 Admin Network에 대해 동일한 MTU를 사용하는 경우 여기에서 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
ADMIN_NETWORK_MTU = 8192
```

- * CLIENT_NETWORK_CONFIG *: IP 주소를 획득하는 데 사용되는 방법으로, 비활성화, 정적 또는 DHCP 입니다. 기본값은 사용 안 함으로 설정되어 있습니다. 모든 노드 또는 대부분의 노드가 동일한 방법으로 IP 주소를 획득하는 경우 여기에서 해당 방법을 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
CLIENT_NETWORK_CONFIG = STATIC
```

- * client_network_target *: 클라이언트 네트워크에 사용할 기존 VMware 네트워크의 이름입니다. 이 설정은 클라이언트 네트워크를 사용하지 않는 경우에만 필요합니다. 모든 노드 또는 대부분의 노드가 동일한 네트워크 이름을 사용하는 경우 여기에서 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여

전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
CLIENT_NETWORK_TARGET = SG-Client-Network
```

- * client_network_mask *: 클라이언트 네트워크의 네트워크 마스크입니다. 이 설정은 고정 IP 주소 지정을 사용하는 경우에 필요합니다. 모든 노드 또는 대부분의 노드가 동일한 네트워크 마스크를 사용하는 경우 여기에서 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- * client_network_gateway *: 클라이언트 네트워크의 네트워크 게이트웨이입니다. 이 설정은 고정 IP 주소 지정을 사용하는 경우에 필요합니다. 모든 노드 또는 대부분의 노드가 동일한 네트워크 게이트웨이를 사용하는 경우 여기에서 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- * client_network_mtu *: 선택 사항. 클라이언트 네트워크의 MTU(Maximum Transmission Unit) client_network_Config = DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 이 인수를 생략하면 1400이 사용됩니다. 점보 프레임을 사용하려면 MTU를 9000과 같은 점보 프레임에 적합한 값으로 설정합니다. 그렇지 않으면 기본값을 유지합니다. 모든 노드 또는 대부분의 노드가 클라이언트 네트워크에 동일한 MTU를 사용하는 경우 여기에서 지정할 수 있습니다. 그런 다음 하나 이상의 개별 노드에 대해 다른 설정을 지정하여 전역 설정을 재정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
CLIENT_NETWORK_MTU = 8192
```

- * port_remap *: 내부 그리드 노드 통신 또는 외부 통신을 위해 노드에서 사용하는 포트를 다시 매핑합니다. 엔터프라이즈 네트워킹 정책이 StorageGRID에서 사용하는 하나 이상의 포트를 제한하는 경우 포트를 다시 매핑해야 합니다. StorageGRID에서 사용하는 포트 목록은 의 내부 그리드 노드 통신 및 외부 통신 을 참조하십시오 네트워킹 지침.

> 로드 밸런서 엔드포인트를 구성하는 데 사용할 포트를 다시 매핑하지 마십시오.

> port_remap 만 설정된 경우 지정하는 매핑이 인바운드 및 아웃바운드 통신 모두에 사용됩니다. port_remap_inbound 도 지정된 경우 port_remap 은 아웃바운드 통신에만 적용됩니다.

사용되는 형식은 '*network type/protocol/default port by GRID node/new port*'이며, 여기서 네트워크 유형은 GRID, admin 또는 client이고 프로토콜은 TCP 또는 UDP입니다.

예를 들면 다음과 같습니다.

```
PORT_REMAP = client/tcp/18082/443
```

단독으로 사용하는 경우 이 예제 설정은 그리드 노드에 대한 인바운드 및 아웃바운드 통신을 포트 18082에서 포트 443으로 대칭적으로 매핑합니다. port_remap_inbound 와 함께 사용할 경우 이 예제 설정은 포트 18082에서 포트 443으로 아웃바운드 통신을 매핑합니다.

- * port_remap_inbound *: 지정된 포트에 대한 인바운드 통신을 다시 매핑합니다. port_remap_inbound 를 지정하지만 port_remap 의 값을 지정하지 않으면 포트의 아웃바운드 통신이 변경되지 않습니다.

  로드 밸런서 엔드포인트를 구성하는 데 사용할 포트를 다시 매핑하지 마십시오.

사용되는 형식은 '*network type/protocol/_default port used by GRID node/new port*'입니다. 여기서 네트워크 유형은 GRID, admin 또는 client이고 프로토콜은 TCP 또는 UDP입니다.

예를 들면 다음과 같습니다.

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

이 예에서는 포트 443으로 전송된 트래픽을 내부 방화벽을 통과하여 그리드 노드가 S3 요청을 수신하는 포트 18082로 전달합니다.

노드별 매개 변수

각 노드는 구성 파일의 자체 섹션에 있습니다. 각 노드에는 다음과 같은 설정이 필요합니다.

- 섹션 헤드는 그리드 관리자에 표시될 노드 이름을 정의합니다. 노드에 대해 선택 사항인 node_name 매개 변수를 지정하여 이 값을 재정의할 수 있습니다.
- * node_type *: VM_Admin_Node, VM_Storage_Node, VM_Archive_Node 또는 VM_API_Gateway_Node
- * GRID_NETWORK_IP *: 그리드 네트워크의 노드에 대한 IP 주소입니다.
- * admin_network_ip *: 관리 네트워크의 노드에 대한 IP 주소입니다. 노드가 Admin Network에 연결되어 있고 admin_network_Config가 static으로 설정된 경우에만 필요합니다.
- * client_network_ip *: 클라이언트 네트워크의 노드에 대한 IP 주소입니다. 노드가 클라이언트 네트워크에 연결되어 있고 이 노드의 client_network_Config가 static으로 설정된 경우에만 필요합니다.
- * admin_IP *: 그리드 네트워크의 기본 관리 노드에 대한 IP 주소입니다. 기본 관리 노드에 대해 GRID_NETWORK_IP로 지정하는 값을 사용합니다. 이 매개 변수를 생략하면 노드가 mDNS를 사용하여 운영 관리 노드 IP를 검색합니다. 자세한 내용은 을 참조하십시오 그리드 노드가 기본 관리자 노드를 검색하는 방법.

  admin_ip 매개 변수는 기본 관리 노드에 대해 무시됩니다.

- 전역적으로 설정되지 않은 모든 매개변수. 예를 들어, 노드가 관리 네트워크에 연결되어 있고 admin_network 매개 변수를 전역으로 지정하지 않은 경우 노드에 대해 이러한 매개 변수를 지정해야 합니다.

기본 관리자 노드

기본 관리 노드에는 다음과 같은 추가 설정이 필요합니다.

- * node_type *: vm_Admin_Node
- * admin_role *: 기본

이 예제 항목은 세 네트워크 모두에 있는 기본 관리 노드에 대한 것입니다.

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_IP = 10.1.0.2
  ADMIN_NETWORK_IP = 10.3.0.2
  CLIENT_NETWORK_IP = 10.4.0.2
```

기본 관리 노드에는 다음과 같은 추가 설정이 선택 사항입니다.

- * 디스크 *: 기본적으로 감사 및 데이터베이스 사용을 위해 관리자 노드에 두 개의 추가 200GB 하드 디스크가 할당됩니다. disk 매개 변수를 사용하여 이러한 설정을 늘릴 수 있습니다. 예를 들면 다음과 같습니다.

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  관리 노드의 경우 인스턴스는 항상 2가 되어야 합니다.

스토리지 노드

스토리지 노드에는 다음과 같은 추가 설정이 필요합니다.

- * node_type *: vm_storage_Node

  이 예제 항목은 그리드 및 관리 네트워크에 있지만 클라이언트 네트워크에 없는 스토리지 노드에 대한 것입니다. 이 노드는 admin_ip 설정을 사용하여 그리드 네트워크에서 기본 관리 노드의 IP 주소를 지정합니다.

  ```
  [DC1-S1]
    NODE_TYPE = VM_Storage_Node

    GRID_NETWORK_IP = 10.1.0.3
    ADMIN_NETWORK_IP = 10.3.0.3

    ADMIN_IP = 10.1.0.2
  ```

  이 두 번째 예제 항목은 고객의 엔터프라이즈 네트워킹 정책에서 포트 80 또는 443을 사용하여 스토리지 노드에 액세스할 수 있다고 명시하는 클라이언트 네트워크의 스토리지 노드에 대한 것입니다. 예제 구성 파일은 port_remap을 사용하여 스토리지 노드가 포트 443에서 S3 메시지를 보내고 받을 수 있도록 합니다.

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

마지막 예에서는 포트 22에서 포트 3022로 ssh 트래픽에 대한 대칭 재매핑을 생성하지만 인바운드 및 아웃바운드 트래픽에 대한 값을 명시적으로 설정합니다.

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

스토리지 노드의 경우 다음 추가 설정은 선택 사항입니다.

- * disk *: 기본적으로 스토리지 노드에는 RangeDB 사용을 위해 3 개의 4TB 디스크가 할당됩니다. 디스크 매개변수를 사용하여 이러한 설정을 늘릴 수 있습니다. 예를 들면 다음과 같습니다.

```
DISK = INSTANCES=16, CAPACITY=4096
```

아카이브 노드

아카이브 노드에 대해 다음 추가 설정이 필요합니다.

- * node_type *: vm_Archive_Node

이 예제 항목은 그리드 및 관리 네트워크에 있지만 클라이언트 네트워크에 없는 아카이브 노드에 대한 것입니다.

```
[DC1-ARC1]
  NODE_TYPE = VM_Archive_Node

  GRID_NETWORK_IP = 10.1.0.4
  ADMIN_NETWORK_IP = 10.3.0.4

  ADMIN_IP = 10.1.0.2
```

게이트웨이 노드

게이트웨이 노드에는 다음과 같은 추가 설정이 필요합니다.

- * node_type *: vm_api_Gateway

이 예제 항목은 세 네트워크 모두에서 게이트웨이 노드의 예입니다. 이 예에서는 구성 파일의 전역 섹션에 클라이언트 네트워크 매개 변수가 지정되지 않아 노드에 대해 지정해야 합니다.

```
[DC1-G1]
  NODE_TYPE = VM_API_Gateway

  GRID_NETWORK_IP = 10.1.0.5
  ADMIN_NETWORK_IP = 10.3.0.5

  CLIENT_NETWORK_CONFIG = STATIC
  CLIENT_NETWORK_TARGET = SG-Client-Network
  CLIENT_NETWORK_MASK = 255.255.255.0
  CLIENT_NETWORK_GATEWAY = 10.4.0.1
  CLIENT_NETWORK_IP = 10.4.0.5

  ADMIN_IP = 10.1.0.2
```

운영 관리자 노드가 아닌 노드

운영 관리자 노드가 아닌 경우 다음과 같은 추가 설정이 필요합니다.

- * node_type *: vm_Admin_Node
- * admin_role *: Non-Primary

이 예제 항목은 클라이언트 네트워크에 없는 비 기본 관리 노드에 대한 것입니다.

```
[DC2-ADM1]
  ADMIN_ROLE = Non-Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_TARGET = SG-Grid-Network
  GRID_NETWORK_IP = 10.1.0.6
  ADMIN_NETWORK_IP = 10.3.0.6

  ADMIN_IP = 10.1.0.2
```

다음 추가 설정은 운영 관리자 노드가 아닌 경우 선택 사항입니다.

- * 디스크 *: 기본적으로 감사 및 데이터베이스 사용을 위해 관리자 노드에 두 개의 추가 200GB 하드 디스크가 할당됩니다. disk 매개 변수를 사용하여 이러한 설정을 늘릴 수 있습니다. 예를 들면 다음과 같습니다.

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

> 관리 노드의 경우 인스턴스는 항상 2가 되어야 합니다.

Bash 스크립트를 실행합니다

VMware vSphere에서 StorageGRID 그리드 노드 구축을 자동화하기 위해 수정한 deploy-vsphere-ovftool.ini 구성 파일과 dedploy-vsphere-ovftool.sh" bash 스크립트를 사용할 수 있습니다.

필요한 것

- 사용자 환경에 대한 deploy-vsphere-ovftool.ini 구성 파일을 만들었습니다.

도움말 명령('-h/- help')을 입력하여 Bash 스크립트에서 사용할 수 있는 도움말을 사용할 수 있습니다. 예를 들면 다음과 같습니다.

```
./deploy-vsphere-ovftool.sh -h
```

또는

```
./deploy-vsphere-ovftool.sh --help
```

단계

1. Bash 스크립트를 실행하기 위해 사용 중인 Linux 시스템에 로그인합니다.
2. 설치 아카이브를 추출한 디렉토리로 변경합니다.

   예를 들면 다음과 같습니다.

```
cd StorageGRID-Webscale-version/vsphere
```

3. 모든 그리드 노드를 배포하려면 환경에 적합한 옵션을 사용하여 Bash 스크립트를 실행합니다.

   예를 들면 다음과 같습니다.

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-
vsphere-ovftool.ini
```

4. 오류로 인해 그리드 노드를 배포하지 못한 경우 오류를 해결하고 해당 노드에 대해서만 Bash 스크립트를 다시 실행합니다.

   예를 들면 다음과 같습니다.

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd --single
-node="DC1-S3" ./deploy-vsphere-ovftool.ini
```

각 노드의 상태가 Passed가 되면 배포가 완료됩니다.

```
Deployment Summary
+------------------------------+----------+----------------------+
| node                         | attempts | status               |
+------------------------------+----------+----------------------+
| DC1-ADM1                     |        1 | Passed               |
| DC1-G1                       |        1 | Passed               |
| DC1-S1                       |        1 | Passed               |
| DC1-S2                       |        1 | Passed               |
| DC1-S3                       |        1 | Passed               |
+------------------------------+----------+----------------------+
```

StorageGRID의 구성을 자동화합니다

그리드 노드를 구축한 후 StorageGRID 시스템 구성을 자동화할 수 있습니다.

필요한 것

- 설치 아카이브에서 다음 파일의 위치를 알고 있습니다.

파일 이름	설명
configure-storagegrid.py	구성을 자동화하는 데 사용되는 Python 스크립트입니다
configure -StorageGrid.sample.json	스크립트와 함께 사용할 샘플 구성 파일

파일 이름	설명
configure -StorageGrid.blank.json을 지정합니다	스크립트에 사용할 빈 구성 파일입니다

- "configure-StorageGrid.json" 구성 파일을 만들었습니다. 이 파일을 만들려면 샘플 구성 파일('configure-StorageGrid.sample.json') 또는 빈 구성 파일('configure-StorageGrid.blank.json')을 수정할 수 있습니다.

configure-StorageGrid.py Python 스크립트와 configure-StorageGrid.json 구성 파일을 사용하여 StorageGRID 시스템 구성을 자동화할 수 있습니다.

> 그리드 관리자 또는 설치 API를 사용하여 시스템을 구성할 수도 있습니다.

단계

1. Python 스크립트를 실행하기 위해 사용 중인 Linux 시스템에 로그인합니다.
2. 설치 아카이브를 추출한 디렉토리로 변경합니다.

   예를 들면 다음과 같습니다.

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   여기서 '플랫폼'은 debs, rpms 또는 vSphere입니다.

3. Python 스크립트를 실행하고 생성한 구성 파일을 사용합니다.

   예를 들면 다음과 같습니다.

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

결과

복구 패키지 .zip 파일은 구성 프로세스 중에 생성되며 설치 및 구성 프로세스를 실행 중인 디렉터리에 다운로드됩니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 백업해야 합니다. 예를 들어, 안전한 백업 네트워크 위치 및 안전한 클라우드 저장소 위치에 복사합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

임의 암호를 생성해야 한다고 지정한 경우 Passwords.txt 파일을 추출하고 StorageGRID 시스템에 액세스하는 데 필요한 암호를 찾아야 합니다.

```
#####################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
#####################################################################
```

확인 메시지가 표시되면 StorageGRID 시스템이 설치 및 구성됩니다.

```
StorageGRID has been configured and installed.
```

관련 정보

그리드 관리자로 이동합니다

설치 REST API 개요

설치 **REST API** 개요

StorageGRID는 설치 작업을 수행하기 위한 StorageGRID 설치 API를 제공합니다.

API는 Swagger 오픈 소스 API 플랫폼을 사용하여 API 문서를 제공합니다. swagger를 사용하면 개발자와 개발자가 아닌 사용자가 API가 매개 변수 및 옵션에 어떻게 응답하는지 보여주는 사용자 인터페이스에서 API와 상호 작용할 수 있습니다. 이 문서에서는 표준 웹 기술 및 JSON(JavaScript Object Notation) 데이터 형식에 대해 잘 알고 있다고 가정합니다.

> API Docs 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

각 REST API 명령에는 API의 URL, HTTP 작업, 필수 또는 선택적 URL 매개 변수, 그리고 예상되는 API 응답이 포함됩니다.

StorageGRID 설치 **API**

StorageGRID 설치 API는 StorageGRID 시스템을 처음 구성할 때와 기본 관리자 노드 복구를 수행해야 하는 경우에만 사용할 수 있습니다. 설치 API는 Grid Manager에서 HTTPS를 통해 액세스할 수 있습니다.

API 설명서에 액세스하려면 기본 관리 노드의 설치 웹 페이지로 이동하여 메뉴 모음에서 * 도움말 * > * API 설명서 * 를 선택합니다.

StorageGRID 설치 API에는 다음 섹션이 포함되어 있습니다.

- * config * — 제품 릴리스 및 API 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 API의 주요 버전을 나열할 수 있습니다.
- * 그리드 * — 그리드 레벨 구성 작업. 그리드 세부 정보, 그리드 네트워크 서브넷, 그리드 암호, NTP 및 DNS 서버 IP 주소를 포함한 그리드 설정을 얻고 업데이트할 수 있습니다.
- * 노드 * — 노드 레벨 구성 작업 그리드 노드 목록을 검색하고, 그리드 노드를 삭제하고, 그리드 노드를 구성하고,

그리드 노드를 보고, 그리드 노드의 구성을 재설정할 수 있습니다.

- * 프로비저닝 * — 프로비저닝 작업. 프로비저닝 작업을 시작하고 프로비저닝 작업의 상태를 볼 수 있습니다.
- * 복구 * — 기본 관리 노드 복구 작업 정보를 재설정하고, 복구 패키지를 업로드하고, 복구를 시작하고, 복구 작업의 상태를 볼 수 있습니다.
- * recovery-package * — 복구 패키지를 다운로드하기 위한 작업.
- 고급 배포를 위한 * 스키마 * — API 스키마
- * 사이트 * — 사이트 수준 구성 작업 사이트를 만들고, 보고, 삭제하고, 수정할 수 있습니다.

다음 단계로 넘어갑니다

설치를 완료한 후에는 일련의 통합 및 구성 단계를 수행해야 합니다. 일부 단계는 필수 사항이고 다른 단계는 선택 사항입니다.

필수 작업

- 자동 재시작을 위해 VMware vSphere 하이퍼바이저를 구성합니다.

  서버가 다시 시작될 때 가상 머신을 다시 시작하도록 하이퍼바이저를 구성해야 합니다. 자동 다시 시작이 없으면 서버가 다시 시작된 후에도 가상 머신과 그리드 노드는 계속 종료됩니다. 자세한 내용은 VMware vSphere 하이퍼바이저 설명서를 참조하십시오.

- StorageGRID 시스템에 오브젝트를 저장하는 데 사용할 각 클라이언트 프로토콜(Swift 또는 S3)에 대한 테넌트 계정을 생성합니다.
- 그룹 및 사용자 계정을 구성하여 시스템 액세스를 제어합니다. 필요에 따라 관리 그룹 및 사용자를 가져올 수 있도록 통합 ID 소스(예: Active Directory 또는 OpenLDAP)를 구성할 수 있습니다. 또는 로컬 그룹 및 사용자를 만들 수 있습니다.
- 오브젝트를 StorageGRID 시스템에 업로드하는 데 사용할 S3 또는 Swift API 클라이언트 애플리케이션을 통합 및 테스트합니다.
- 준비가 되면 개체 데이터를 보호하는 데 사용할 ILM(정보 수명 주기 관리) 규칙 및 ILM 정책을 구성합니다.

  > StorageGRID를 설치하면 기본 ILM 정책, 즉 기본 2 복사본 정책이 활성화됩니다. 이 정책에는 재고 ILM 규칙(복사본 2개 만들기)이 포함되며 다른 정책이 활성화되지 않은 경우 적용됩니다.

- 설치에 어플라이언스 스토리지 노드가 포함된 경우 SANtricity 소프트웨어를 사용하여 다음 작업을 완료합니다.
  - 각 StorageGRID 어플라이언스에 연결하십시오.
  - AutoSupport 데이터가 수신되었는지 확인합니다.
- StorageGRID 시스템에 아카이브 노드가 포함된 경우 아카이브 노드의 대상 외부 아카이브 스토리지 시스템에 대한 접속을 구성합니다.

  > 아카이브 노드에서 Tivoli Storage Manager를 외부 아카이브 스토리지 시스템으로 사용하는 경우 Tivoli Storage Manager도 구성해야 합니다.

- StorageGRID 시스템 강화 지침을 검토하고 준수하여 보안 위험을 제거합니다.
- 시스템 경고에 대한 이메일 알림을 구성합니다.

선택적 태스크입니다

- (레거시) 알람 시스템에서 알림을 수신하려면 알람에 대한 메일 그룹 및 이메일 알림을 구성합니다.
- 배포를 계획하고 복구 패키지를 생성한 이후에 변경된 경우 그리드 노드 IP 주소를 업데이트합니다. 복구 및 유지 관리 지침에서 IP 주소 변경에 대한 정보를 참조하십시오.
- 필요한 경우 스토리지 암호화를 구성합니다.
- 필요한 경우 스토리지 압축을 구성하여 저장된 개체의 크기를 줄입니다.
- 감사 클라이언트 액세스를 구성합니다. NFS 또는 CIFS 파일 공유를 통해 감사 목적으로 시스템에 대한 액세스를 구성할 수 있습니다. StorageGRID 관리 지침을 참조하십시오.

> CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

관련 정보

StorageGRID 관리

S3을 사용합니다

Swift를 사용합니다

ILM을 사용하여 개체를 관리합니다

모니터링하고 문제를 해결합니다

복구 및 유지 관리

SG100 및 SG1000 서비스 어플라이언스

SG5600 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG6000 스토리지 어플라이언스

릴리스 정보

시스템 강화

감사 로그를 검토합니다

소프트웨어 업그레이드

설치 문제를 해결합니다

StorageGRID 시스템을 설치하는 동안 문제가 발생하면 설치 로그 파일에 액세스할 수 있습니다.

다음은 문제를 해결하기 위해 기술 지원 부서에서 필요로 하는 기본 설치 로그 파일입니다.

- '/var/local/log/install.log'(모든 그리드 노드에 있음)
- (/var/local/log/gdu-server.log"(기본 관리 노드에서 찾을 수 있음)

로그 파일에 액세스하는 방법은 를 참조하십시오 StorageGRID 모니터링 및 문제 해결 지침. 어플라이언스 설치 문제 해결에 대한 도움말은 어플라이언스의 설치 및 유지 관리 지침을 참조하십시오. 추가 지원이 필요한 경우 기술 지원 부서에 문의하십시오.

SG100 및 SG1000 서비스 어플라이언스

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG5600 스토리지 어플라이언스

"NetApp 지원"

가상 머신 리소스 예약을 조정해야 합니다

OVF 파일에는 각 그리드 노드가 효율적으로 작동할 수 있는 충분한 RAM 및 CPU를 포함하도록 설계된 리소스 예약이 포함됩니다. VMware에 이러한 OVF 파일을 구축하여 가상 머신을 생성하는 경우 미리 정의된 리소스 수를 사용할 수 없으면 가상 머신이 시작되지 않습니다.

이 작업에 대해

VM 호스트에 각 그리드 노드에 대한 리소스가 충분하다고 확신하는 경우 각 가상 머신에 할당된 리소스를 수동으로 조정한 다음 가상 머신을 시작합니다.

단계

1. VMware vSphere 하이퍼바이저 클라이언트 트리에서 시작되지 않은 가상 머신을 선택합니다.
2. 가상 머신을 마우스 오른쪽 버튼으로 클릭하고 * 설정 편집 * 을 선택합니다.
3. 가상 머신 속성 창에서 * 리소스 * 탭을 선택합니다.
4. 가상 머신에 할당된 리소스를 조정합니다.
   a. CPU * 를 선택한 다음 예약 슬라이더를 사용하여 이 가상 머신에 예약된 MHz를 조정합니다.
   b. Memory*를 선택한 다음 Reservation 슬라이더를 사용하여 이 가상 머신에 예약된 MB를 조정합니다.
5. 확인 * 을 클릭합니다.
6. 동일한 VM 호스트에서 호스팅되는 다른 가상 머신에 대해 필요에 따라 이 작업을 반복합니다.

시스템 관리를 수행합니다

StorageGRID 관리

StorageGRID 관리: 개요

다음 지침에 따라 StorageGRID 시스템을 구성하고 관리합니다.

참조하십시오

이 지침은 그리드 관리자를 사용하여 그룹 및 사용자를 설정하고, S3 및 Swift 클라이언트 애플리케이션이 오브젝트를 저장 및 검색하고, StorageGRID 네트워크를 구성 및 관리하고, AutoSupport를 구성하고, 노드 설정을 관리하는 등의 작업을 수행할 수 있도록 테넌트 계정을 생성하는 방법을 설명합니다.

이 지침은 StorageGRID 시스템을 설치한 후 구성, 관리 및 지원할 기술 담당자를 위한 것입니다.

시작하기 전에

- StorageGRID 시스템에 대해 전반적으로 이해하고 있습니다.
- Linux 명령 셸, 네트워킹 및 서버 하드웨어 설정 및 구성에 대한 매우 상세한 지식을 보유하고 있습니다.

StorageGRID를 시작하십시오

웹 브라우저 요구 사항

지원되는 웹 브라우저를 사용해야 합니다.

웹 브라우저	최소 지원 버전
Google Chrome	96
Microsoft Edge를 참조하십시오	96
Mozilla Firefox	94

브라우저 창을 권장 너비로 설정해야 합니다.

브라우저 폭	픽셀
최소	1024
최적	1280

Grid Manager에 로그인합니다

지원되는 웹 브라우저의 주소 표시줄에 FQDN(정규화된 도메인 이름) 또는 관리 노드의 IP

주소를 입력하여 Grid Manager 로그인 페이지에 액세스합니다.

필요한 것

- 로그인 자격 증명이 있습니다.
- 그리드 관리자의 URL이 있습니다.
- 을(를) 사용하고 있습니다 지원되는 웹 브라우저.
- 쿠키는 웹 브라우저에서 활성화됩니다.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

각 StorageGRID 시스템에는 1개의 기본 관리 노드와 1차 관리자가 아닌 노드 수가 포함되어 있습니다. 관리자 노드의 그리드 관리자에 로그인하여 StorageGRID 시스템을 관리할 수 있습니다. 그러나 관리 노드는 정확히 동일하지 않습니다.

- 한 관리 노드에서 이루어진 알람 승인(레거시 시스템)은 다른 관리 노드에 복사되지 않습니다. 이러한 이유로 알람에 대해 표시되는 정보는 각 관리 노드에서 동일하지 않을 수 있습니다.
- 일부 유지 보수 절차는 기본 관리 노드에서만 수행할 수 있습니다.

HA(고가용성) 그룹에 관리 노드가 포함된 경우 HA 그룹의 가상 IP 주소 또는 가상 IP 주소에 매핑되는 정규화된 도메인 이름을 사용하여 연결합니다. 기본 관리 노드를 그룹의 기본 인터페이스로 선택해야 그리드 관리자에 액세스할 때 기본 관리 노드를 사용할 수 없는 경우를 제외하고 기본 관리 노드에서 액세스할 수 있습니다.

단계

1. 지원되는 웹 브라우저를 실행합니다.
2. 브라우저의 주소 표시줄에 Grid Manager의 URL을 입력합니다.

   "https://*FQDN_or_Admin_Node_IP*/`

   여기서, '*FQDN_OR_Admin_Node_IP*'는 관리자 노드의 정규화된 도메인 이름 또는 관리 노드의 HA 그룹의 가상 IP 주소입니다.

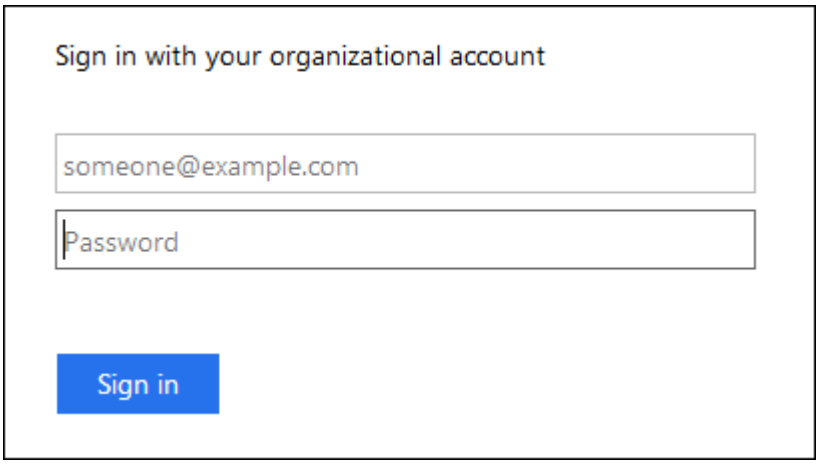
   HTTPS의 표준 포트(443)가 아닌 포트에서 Grid Manager에 액세스해야 하는 경우 다음을 입력합니다. 여기서, '*FQDN_or_Admin_Node_IP*'는 정규화된 도메인 이름 또는 IP 주소이고 port는 포트 번호입니다.

   "https://*FQDN_or_Admin_Node_IP:port*/`

3. 보안 경고 메시지가 나타나면 브라우저의 설치 마법사를 사용하여 인증서를 설치합니다(참조) 보안 인증서 정보)를 클릭합니다.
4. Grid Manager에 로그인:
   - SSO(Single Sign-On)를 StorageGRID 시스템에 사용하지 않는 경우:
     i. Grid Manager의 사용자 이름과 암호를 입력합니다.
     ii. 로그인 * 을 선택합니다.

- StorageGRID 시스템에서 SSO가 활성화되어 있고 이 브라우저에서 URL에 처음 액세스한 경우:
  i. 로그인 * 을 선택합니다. 계정 ID 필드는 비워 둘 수 있습니다.

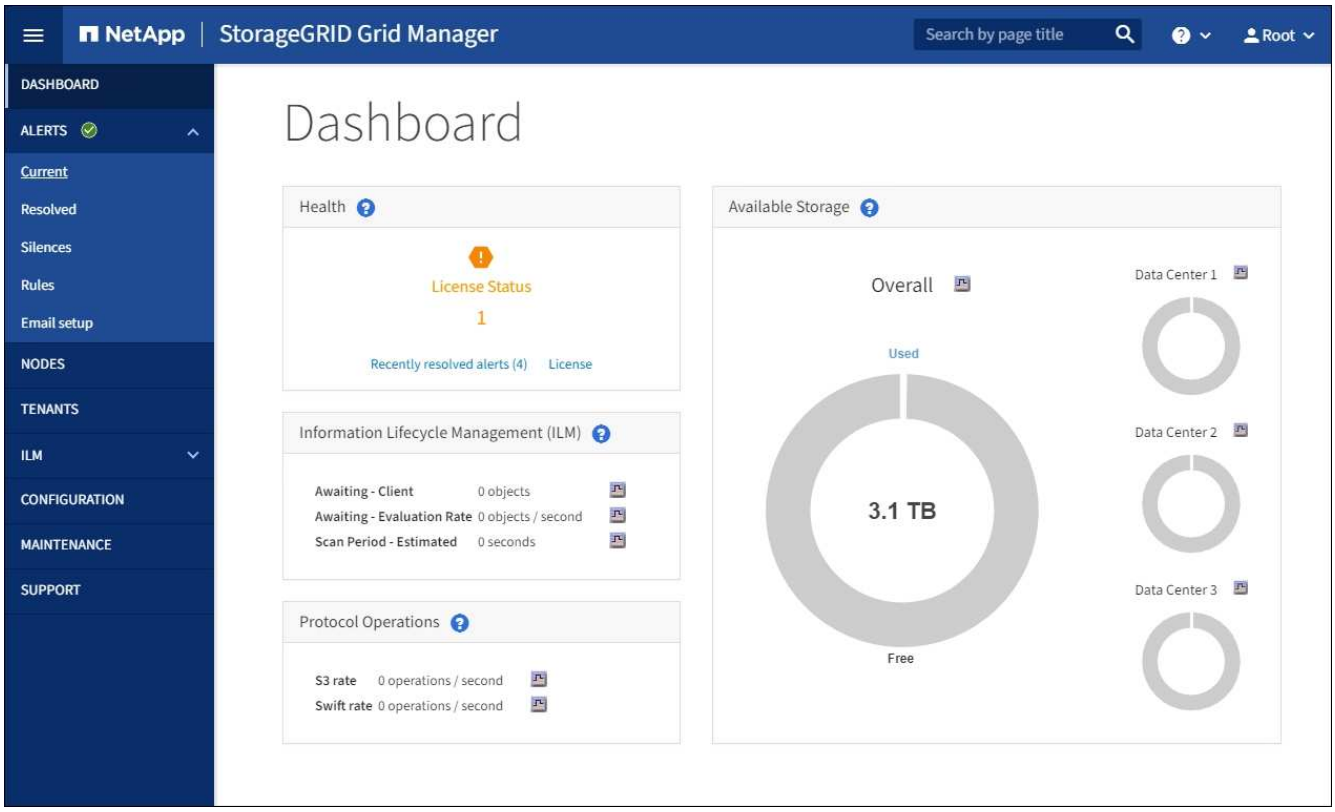
  ii. 조직의 SSO 로그인 페이지에 표준 SSO 자격 증명을 입력합니다. 예를 들면 다음과 같습니다.



- StorageGRID 시스템에 대해 SSO가 활성화되어 있고 이전에 그리드 관리자 또는 테넌트 계정에 액세스한 경우:
  i. 다음 중 하나를 수행합니다.

- 0 * (그리드 관리자의 계정 ID)을 입력하고 * 로그인 * 을 선택합니다.
- 최근 계정 목록에 나타나는 경우 * Grid Manager * 를 선택하고 * Sign in * 을 선택합니다.

ii. 조직의 SSO 로그인 페이지에서 표준 SSO 자격 증명을 사용하여 로그인합니다. 로그인하면 대시보드가 포함된 그리드 관리자의 홈 페이지가 나타납니다. 제공되는 정보에 대한 자세한 내용은 을 참조하십시오 대시보드 보기.



5. 다른 관리자 노드에 로그인하려면:

옵션을 선택합니다	단계
SSO가 활성화되지 않았습니다	a. 브라우저의 주소 표시줄에 다른 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력합니다. 필요에 따라 포트 번호를 포함시킵니다. b. Grid Manager의 사용자 이름과 암호를 입력합니다. c. 로그인 * 을 선택합니다.
SSO가 활성화되었습니다	브라우저의 주소 표시줄에 다른 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력합니다. 한 관리 노드에 로그인한 경우 다시 로그인하지 않고도 다른 관리 노드에 액세스할 수 있습니다. 그러나 SSO 세션이 만료되면 자격 증명을 다시 입력하라는 메시지가 표시됩니다. • 참고: * SSO는 제한된 Grid Manager 포트에서 사용할 수 없습니다. 사용자가 SSO(Single Sign-On)로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다.

관련 정보

- 방화벽을 통한 액세스 제어
- Single Sign-On 구성
- 관리 그룹을 관리합니다
- 고가용성 그룹을 관리합니다
- 테넌트 계정을 사용합니다
- 모니터링하고 문제를 해결합니다

Grid Manager에서 로그아웃합니다

그리드 관리자 작업을 마치면 로그아웃하여 권한이 없는 사용자가 StorageGRID 시스템에 액세스할 수 없도록 해야 합니다. 브라우저를 닫아도 브라우저 쿠키 설정에 따라 시스템에서 로그아웃되지 않을 수 있습니다.

단계

1. 오른쪽 위 모서리에서 사용자 이름을 선택합니다.

2. 로그아웃 * 을 선택합니다.

옵션을 선택합니다	설명
SSO가 사용되지 않습니다	관리자 노드에서 로그아웃되었습니다. 그리드 관리자 로그인 페이지가 표시됩니다. • 참고: * 둘 이상의 관리자 노드에 로그인한 경우 각 노드에서 로그아웃해야 합니다.
SSO가 활성화되었습니다	액세스 중인 모든 관리 노드에서 로그아웃되었습니다. StorageGRID 로그인 페이지가 표시됩니다. * 그리드 관리자 * 는 * 최근 계정 * 드롭다운에 기본값으로 나열되고 * 계정 ID * 필드는 0으로 표시됩니다. • 참고: * SSO가 활성화되어 있고 테넌트 관리자에도 로그인한 경우, SSO에서 로그아웃하려면 테넌트 계정에서도 로그아웃해야 합니다.

관련 정보

- Single Sign-On 구성
- 테넌트 계정을 사용합니다

암호를 변경합니다

Grid Manager의 로컬 사용자인 경우 사용자 고유의 암호를 변경할 수 있습니다.

필요한 것

를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

이 작업에 대해

통합 사용자로 StorageGRID에 로그인하거나 SSO(Single Sign-On)가 활성화된 경우 그리드 관리자에서 암호를 변경할 수 없습니다. 대신 Active Directory 또는 OpenLDAP와 같은 외부 ID 소스에서 암호를 변경해야 합니다.

단계

1. Grid Manager 헤더에서 *사용자 이름 * > * 암호 변경 * 을 선택합니다.
2. 현재 암호를 입력합니다.
3. 새 암호를 입력합니다.

   암호는 8자 이상 32자 이하여야 합니다. 암호는 대/소문자를 구분합니다.

4. 새 암호를 다시 입력합니다.
5. 저장 * 을 선택합니다.

브라우저 세션 제한 시간을 변경합니다

특정 시간 이상 사용하지 않는 경우 Grid Manager 및 Tenant Manager 사용자가 로그아웃되는지 여부를 제어할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

GUI 비활성 시간 초과 기본값은 900초(15분)입니다. 사용자의 브라우저 세션이 이 시간 동안 활성 상태가 아니면 세션 시간이 초과됩니다.

필요한 경우 GUI 비활성 시간 초과 표시 옵션을 설정하여 시간 초과 기간을 늘리거나 줄일 수 있습니다.

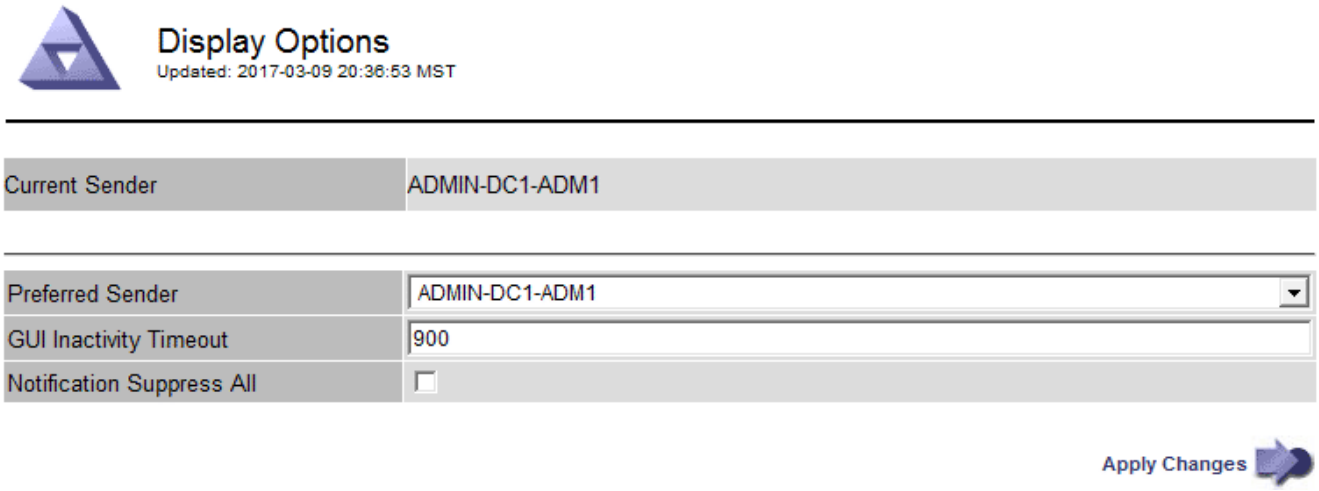
SSO(Single Sign-On)가 활성화되어 있고 사용자의 브라우저 세션 시간이 초과되면 시스템은 사용자가 * 로그아웃 * 수동으로 선택한 것처럼 작동합니다. 사용자가 SSO 자격 증명을 다시 입력하여 StorageGRID에 다시 액세스해야 합니다. 을 참조하십시오 Single Sign-On 구성.

> 사용자 세션 시간 초과는 다음을 통해서도 제어할 수 있습니다.
>
> - 시스템 보안을 위해 포함되어 있는 별도의 구성 불가능한 StorageGRID 타이머입니다. 기본적으로 각 사용자의 인증 토큰은 사용자가 로그인 한 후 16시간 후에 만료됩니다. 사용자의 인증이 만료되면 GUI 비활성 시간 제한 값에 도달하지 않았더라도 해당 사용자는 자동으로 로그아웃됩니다. 토큰을 갱신하려면 사용자가 다시 로그인해야 합니다.
> - StorageGRID에 대해 SSO가 활성화된 경우 ID 공급자에 대한 시간 제한 설정

단계

1. 구성 * > * 시스템 * > * 디스플레이 옵션 * 을 선택합니다.
2. GUI 비활성 시간 초과 * 의 경우 시간 초과 기간을 60초 이상으로 입력합니다.

   이 기능을 사용하지 않으려면 이 필드를 0으로 설정합니다. 사용자는 로그인 후 16시간 후에 인증 토큰이 만료되었을 때 로그아웃됩니다.



3. Apply Changes * 를 선택합니다.

   새 설정은 현재 로그인한 사용자에게는 영향을 주지 않습니다. 사용자는 다시 로그인하거나 브라우저를 새로 고쳐야 새 시간 초과 설정을 적용할 수 있습니다.

StorageGRID 라이센스 정보를 봅니다

필요한 경우 그리드의 최대 스토리지 용량과 같은 StorageGRID 시스템에 대한 라이센스 정보를 볼 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

이 작업에 대해

이 StorageGRID 시스템의 소프트웨어 라이센스에 문제가 있는 경우 대시보드의 상태 패널에 라이센스 상태 아이콘과 * 라이센스 * 링크가 포함됩니다. 이 숫자는 라이센스 관련 문제가 얼마나 많은가를 나타냅니다.

단계

라이센스를 보려면 다음 중 하나를 수행합니다.

- 대시보드의 상태 패널에서 라이센스 상태 아이콘 또는 * 라이센스 * 링크를 선택합니다. 이 링크는 라이센스에 문제가 있는 경우에만 나타납니다.
- 유지 관리 * > * 시스템 * > * 라이센스 * 를 선택합니다.

라이센스 페이지가 나타나고 현재 라이센스에 대한 다음과 같은 읽기 전용 정보가 제공됩니다.

- StorageGRID 시스템 ID로, 이 StorageGRID 설치의 고유 식별 번호입니다
- 라이센스 일련 번호입니다
- 그리드의 라이센스가 부여된 스토리지 용량입니다
- 소프트웨어 라이센스 종료 날짜입니다
- 지원 서비스 계약 종료 날짜입니다
- 라이센스 텍스트 파일의 내용입니다

> StorageGRID 10.3 이전에 발급된 라이센스의 경우 라이센스 저장 용량은 라이센스 파일에 포함되지 않으며 값 대신 "사용권 계약 참조" 메시지가 표시됩니다.

StorageGRID 라이센스 정보를 업데이트합니다

라이센스 조건이 변경될 때마다 StorageGRID 시스템의 라이센스 정보를 업데이트해야 합니다. 예를 들어 그리드에 대한 추가 스토리지 용량을 구입한 경우 라이센스 정보를 업데이트해야

합니다.

필요한 것

- StorageGRID 시스템에 적용할 새 라이센스 파일이 있습니다.
- 특정 액세스 권한이 있습니다.
- 프로비저닝 암호가 있습니다.

단계

1. 유지 관리 * > * 시스템 * > * 라이센스 * 를 선택합니다.
2. Provisioning Passphrase * 텍스트 상자에 StorageGRID 시스템의 프로비저닝 암호를 입력합니다.
3. 찾아보기 * 를 선택합니다.
4. 열기 대화 상자에서 새 사용권 파일('.txt')을 찾아 선택하고 * 열기 * 를 선택합니다.

   새 라이센스 파일의 유효성을 검사한 후 표시합니다.

5. 저장 * 을 선택합니다.

API를 사용합니다

Grid Management API를 사용합니다

Grid Manager 사용자 인터페이스 대신 Grid Management REST API를 사용하여 시스템 관리 작업을 수행할 수 있습니다. 예를 들어, API를 사용하여 작업을 자동화하거나 사용자와 같은 여러 엔터티를 더 빠르게 생성할 수 있습니다.

최고 수준의 리소스

Grid Management API는 다음과 같은 최상위 리소스를 제공합니다.

- '/grid': 그리드 관리자 사용자로 액세스가 제한되며 구성된 그룹 권한에 따라 달라집니다.
- '/org': 테넌트 계정의 로컬 또는 통합 LDAP 그룹에 속한 사용자로 액세스가 제한됩니다. 자세한 내용은 을 참조하십시오 테넌트 계정을 사용합니다.
- '/private': 액세스 권한은 Grid Manager 사용자로 제한되며 구성된 그룹 권한에 따라 결정됩니다. 사설 API는 사전 통보 없이 변경될 수 있습니다. StorageGRID 전용 엔드포인트도 요청의 API 버전을 무시합니다.

API 요청을 발행합니다

Grid Management API는 Swagger 오픈 소스 API 플랫폼을 사용합니다. Swagger는 개발자와 개발자가 아닌 사용자가 API를 사용하여 StorageGRID에서 실시간 작업을 수행할 수 있도록 직관적인 사용자 인터페이스를 제공합니다.

Swagger 사용자 인터페이스는 각 API 작동에 대한 전체 세부 정보와 문서를 제공합니다.

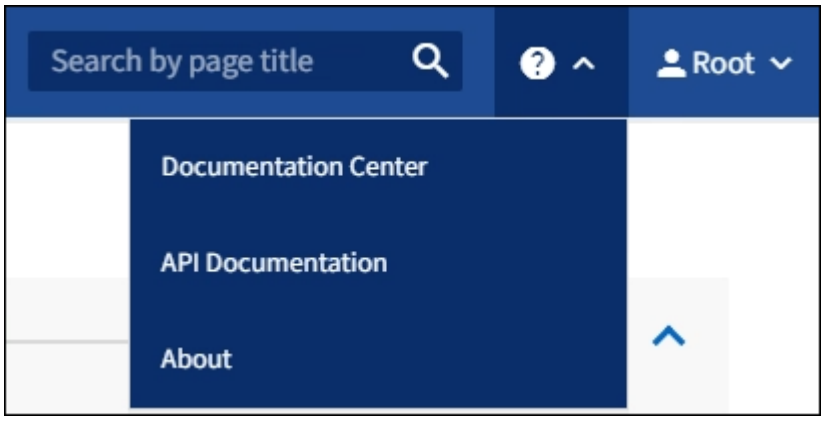
필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

API Docs 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

단계

1. Grid Manager 헤더에서 도움말 아이콘을 선택하고 * API Documentation * 을 선택합니다.



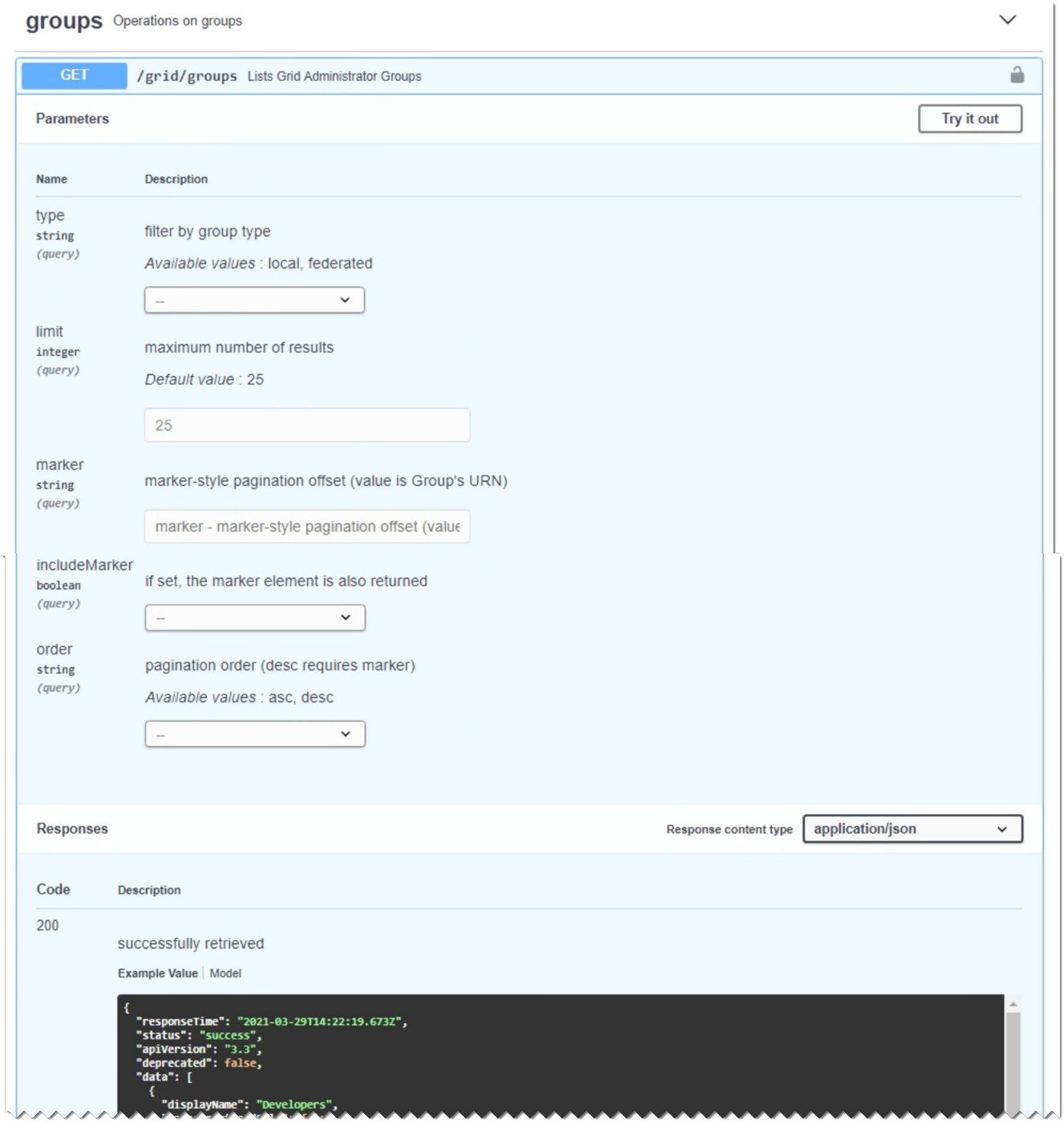
2. 전용 API로 작업을 수행하려면 StorageGRID 관리 API 페이지에서 * 전용 API 설명서 * 로 이동 * 을 선택합니다.

   사설 API는 사전 통보 없이 변경될 수 있습니다. StorageGRID 전용 엔드포인트도 요청의 API 버전을 무시합니다.

3. 원하는 작업을 선택합니다.

   API 작업을 확장하면 가져오기, 가져오기, 업데이트 및 삭제와 같은 사용 가능한 HTTP 작업을 볼 수 있습니다.

4. 끝점 URL, 필수 또는 선택적 매개 변수 목록, 요청 본문(필요한 경우) 예제 및 가능한 응답을 비롯한 요청 세부 정보를 보려면 HTTP 작업을 선택합니다.



5. 요청에 그룹 또는 사용자 ID와 같은 추가 매개 변수가 필요한지 확인합니다. 그런 다음 이 값을 구합니다. 필요한 정보를 얻기 위해 먼저 다른 API 요청을 발급해야 할 수도 있습니다.
6. 예제 요청 본문을 수정해야 하는지 확인합니다. 이 경우 * Model * 을 선택하여 각 필드의 요구 사항을 확인할 수 있습니다.
7. 체험하기 * 를 선택합니다.
8. 필요한 매개 변수를 제공하거나 요청 본문을 필요에 따라 수정합니다.
9. Execute * 를 선택합니다.
10. 응답 코드를 검토하여 요청이 성공했는지 확인합니다.

Grid Management API는 사용 가능한 작업을 다음 섹션으로 구성합니다.

> 이 목록에는 공용 API에서 사용할 수 있는 작업만 포함됩니다.

- * ACCOUNT * — 새 계정 생성 및 지정된 계정의 스토리지 사용량 검색을 포함하여 스토리지 테넌트 계정을 관리하는 작업입니다.
- * ALARMS * — 현재 경보(레거시 시스템)를 나열하고, 현재 경고와 노드 연결 상태 요약을 포함하여 그리드의 상태에 대한 정보를 반환하는 작업.
- * alert-history * — 해결된 경고에 대한 작업.
- 알림 메시지 수신자 * — 경고 알림 수신자(이메일)에 대한 작업.
- * alert-rules * — 경고 규칙에 대한 작업.
- * alert-silences * — 경고 작동 중.
- * 경고 * — 경고 작업.
- * 감사 * — 감사 구성을 나열하고 업데이트하는 작업.
- * auth * — 사용자 세션 인증을 수행하기 위한 작업.

  Grid Management API는 Bearer Token Authentication Scheme을 지원한다. 로그인하려면 인증 요청의 JSON 본문('POST/API/v3/authorize')에 사용자 이름과 암호를 입력합니다. 사용자가 성공적으로 인증되면 보안 토큰이 반환됩니다. 이 토큰은 후속 API 요청 헤더("Authorization:Bearer_token_")에 제공되어야 합니다.

  > StorageGRID 시스템에 대해 Single Sign-On이 활성화된 경우 인증을 위해 다른 단계를 수행해야 합니다. SSO(Single Sign-On)가 활성화된 경우 API에 대한 인증"을 참조하십시오.

  인증 보안 개선에 대한 자세한 내용은 사이트 간 요청 위조 방지 를 참조하십시오.

- * client-certificates * — 외부 모니터링 도구를 사용하여 StorageGRID에 안전하게 액세스할 수 있도록 클라이언트 인증서를 구성하는 작업.
- * config * — 그리드 관리 API 제품 릴리스 및 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 Grid Management API의 주요 버전을 나열할 수 있으며 더 이상 사용되지 않는 API 버전을 사용하지 않도록 설정할 수 있습니다.
- * deactivated - features * — 비활성화된 기능을 보기 위한 작업.
- * DNS-서버 * — 구성된 외부 DNS 서버를 나열하고 변경하는 작업.
- **endpoint-domain-names** — 끝점 도메인 이름을 나열하고 변경하는 작업.
- * 삭제 코딩 * — 삭제 코딩 프로파일에서 작업.
- * 확장 * — 확장 작업(절차 수준).
- * expansion-nodes * — 확장 시 작업(노드 레벨).
- * 확장 사이트 * — 확장 시 운영(사이트 레벨)
- * GRID-NETWORKS * — 그리드 네트워크 목록을 나열하고 변경하는 작업.
- * GRID-Passwords * — 그리드 암호 관리 작업.

- * 그룹 * — 로컬 그리드 관리자 그룹을 관리하고 외부 LDAP 서버에서 통합 그리드 관리자 그룹을 검색하는 작업.
- * identity-source * — 외부 ID 소스를 구성하고 통합 그룹 및 사용자 정보를 수동으로 동기화하는 작업.
- * ILM * — 정보 수명 주기 관리(ILM)에 대한 운영.
- * license * — StorageGRID 라이센스를 검색하고 업데이트하는 작업.
- * 로그 * — 로그 파일을 수집하고 다운로드하기 위한 작업.
- * 메트릭 * — 일정 기간 동안 단일 시점 및 범위 메트릭 쿼리에 대한 즉석 메트릭 쿼리를 비롯한 StorageGRID 메트릭의 운영 Grid Management API는 Prometheus 시스템 모니터링 도구를 백엔드 데이터 소스로 사용합니다. Prometheus 쿼리 구성에 대한 자세한 내용은 Prometheus 웹 사이트를 참조하십시오.

  > 이름에 '*private*'가 포함된 메트릭은 내부용으로만 사용됩니다. 이러한 메트릭은 사전 통지 없이 StorageGRID 릴리스 간에 변경될 수 있습니다.

- * node-details * — 노드 세부 정보에 대한 작업.
- * 노드 상태 * — 노드 상태에 대한 작업
- * NTP-서버 * — 외부 NTP(Network Time Protocol) 서버를 나열하거나 업데이트하는 작업.
- * 오브젝트 * — 오브젝트 및 오브젝트 메타데이터 작업
- * 복구 * — 복구 절차를 위한 작업.
- * recovery-package * — 복구 패키지를 다운로드하기 위한 작업.
- * 지역 * — 영역을 보고 작성하는 작업.
- * S3-오브젝트 잠금 * — 글로벌 S3 오브젝트 잠금 설정에서 작업.
- * server-certificate * — Grid Manager 서버 인증서를 보고 업데이트하는 작업.
- * SNMP * — 현재 SNMP 구성에 대한 작업.
- * traffic-classes * — 트래픽 분류 정책을 위한 운영.
- * 신뢰할 수 없는 클라이언트-네트워크 * — 신뢰할 수 없는 클라이언트 네트워크 구성에서의 작업.
- * 사용자 * — 그리드 관리자 사용자를 보고 관리하는 작업.

Grid Management API 버전 관리

Grid Management API는 버전 관리를 사용하여 무중단 업그레이드를 지원합니다.

예를 들어 이 요청 URL은 API의 버전 3을 지정합니다.

"https://*hostname_or_ip_address*/api/v3/authorize`

테넌트 관리 API의 주요 버전은 이전 버전과 * _호환되지 않는 _ * 변경 사항이 있을 때 충돌합니다. 테넌트 관리 API의 부 버전은 * _ 이(가) 이전 버전과 호환된다는 변경 사항이 있을 때 충돌합니다. 호환 가능한 변경 사항에는 새 끝점 또는 새 속성 추가가 포함됩니다. 다음 예제에서는 변경 유형에 따라 API 버전을 충돌하는 방법을 보여 줍니다.

API 변경 유형입니다	이전 버전	새 버전
이전 버전과 호환 가능합니다	2.1	2.2

API 변경 유형입니다	이전 버전	새 버전
이전 버전과 호환되지 않습니다	2.1	3.0

StorageGRID 소프트웨어를 처음 설치하는 경우 가장 최신 버전의 그리드 관리 API만 활성화됩니다. 그러나 StorageGRID의 새 기능 릴리즈로 업그레이드하면 하나 이상의 StorageGRID 기능 릴리즈에 대한 이전 API 버전에 계속 액세스할 수 있습니다.

> Grid Management API를 사용하여 지원되는 버전을 구성할 수 있습니다. 자세한 내용은 Swagger API 설명서의 ""구성"" 섹션을 참조하십시오. 최신 버전을 사용하도록 모든 Grid Management API 클라이언트를 업데이트한 후에는 이전 버전에 대한 지원을 비활성화해야 합니다.

오래된 요청은 다음과 같은 방법으로 더 이상 사용되지 않는 것으로 표시됩니다.

- 응답 헤더가 "DEPRECATED:TRUE"입니다.
- JSON 응답 본문에는 "DEPRECATED"가 포함됩니다. TRUE
- 더 이상 사용되지 않는 경고가 NMS.log에 추가됩니다. 예를 들면 다음과 같습니다.

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

현재 릴리즈에서 지원되는 **API** 버전을 확인합니다

다음 API 요청을 사용하여 지원되는 API 주요 버전 목록을 반환합니다.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

요청에 대한 **API** 버전을 지정합니다

PATH 파라미터('/api/v3')나 header('api-Version:3')를 이용하여 API 버전을 지정할 수 있다. 두 값을 모두 제공하면 헤더 값이 경로 값을 재정의합니다.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

CSRF 토큰을 사용하여 쿠키를 사용하는 인증을 강화하면 StorageGRID에 대한 CSRF(사이트 간 요청 위조) 공격으로부터 보호할 수 있습니다. Grid Manager 및 Tenant Manager는 이 보안 기능을 자동으로 활성화합니다. 다른 API 클라이언트는 로그인할 때 활성화 여부를 선택할 수 있습니다.

HTTP 양식 POST와 같이 다른 사이트에 대한 요청을 트리거할 수 있는 공격자는 로그인한 사용자의 쿠키를 사용하여 특정 요청을 만들 수 있습니다.

StorageGRID는 CSRF 토큰을 사용하여 CSRF 공격으로부터 보호합니다. 활성화된 경우 특정 쿠키의 내용은 특정 헤더 또는 특정 POST 본문 매개 변수의 내용과 일치해야 합니다.

이 기능을 활성화하려면 인증 중에 csrfToken 매개 변수를 true로 설정하십시오. 기본값은 false 입니다.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

true이면 Grid Manager에 로그인할 때 임의의 값으로 GridCsrfToken 쿠키가 설정되고 테넌트 관리자에 로그인할 때 임의의 값으로 AccountCsrfToken 쿠키가 설정됩니다.

쿠키가 있는 경우 시스템 상태(POST, PUT, 패치, 삭제)를 수정할 수 있는 모든 요청에 다음 중 하나가 포함되어야 합니다.

- CSRF 토큰 쿠키의 값으로 설정된 헤더의 X-CSRF-Token 헤더입니다.
- 폼 인코딩된 본문을 허용하는 끝점의 경우 "csrfToken" 형식 인코딩된 요청 본문 매개 변수입니다.

추가 예제 및 세부 정보는 온라인 API 설명서를 참조하십시오.

> CSRF 토큰 쿠키 세트를 가진 요청은 또한 JSON 요청 본문을 CSRF 공격에 대한 추가 보호로서 기대하는 모든 요청에 대해 ""Content-Type:application/json"" 헤더를 적용합니다.

SSO(Single Sign-On)가 활성화된 경우 **API**를 사용합니다

SSO(Single Sign-On)가 활성화된 경우 **API** 사용**(Active Directory)**

있는 경우 SSO(Single Sign-On) 구성 및 활성화 Active Directory를 SSO 공급자로 사용하는 경우, 그리드 관리 API 또는 테넌트 관리 API에 유효한 인증 토큰을 얻기 위해 일련의 API 요청을 실행해야 합니다.

SSO(Single Sign-On)가 활성화된 경우 **API**에 로그인합니다

Active Directory를 SSO ID 공급자로 사용하는 경우 다음 지침이 적용됩니다.

필요한 것

- StorageGRID 사용자 그룹에 속한 페더레이션 사용자의 SSO 사용자 이름과 암호를 알고 있습니다.
- 테넌트 관리 API에 액세스하려면 테넌트 계정 ID를 알고 있어야 합니다.

이 작업에 대해

인증 토큰을 얻으려면 다음 예 중 하나를 사용할 수 있습니다.

- StorageGRID 설치 파일 디렉토리(Red Hat Enterprise Linux 또는 CentOS의 경우 ./rpms, Ubuntu 또는 Debian의 경우 ./debs, VMware의 경우 ./vsphere)에 있는 toragegrid-ssoauth.py Python 스크립트입니다.
- curl 요청의 워크플로 예

  컬을 너무 느리게 수행하면 컬링 작업 시간이 초과될 수 있습니다. "이 응답에 유효한 SubjectConfirmation을 찾을 수 없습니다."라는 오류가 표시될 수 있습니다.

  > 예제 curl 워크플로는 다른 사용자가 암호를 볼 수 없도록 보호하지 않습니다.

URL 인코딩 문제가 있는 경우 '지원되지 않는 SAML 버전' 오류가 표시될 수 있습니다.

단계

1. 인증 토큰을 얻으려면 다음 방법 중 하나를 선택합니다.
   - toragegrid-soauth.py Python 스크립트를 사용하십시오. 2단계로 이동합니다.
   - curl 요청을 사용합니다. 3단계로 이동합니다.
2. 'toragegrid-ssoauth.py' 스크립트를 사용하려면 스크립트를 Python 해석기로 전달하고 스크립트를 실행합니다.

   프롬프트가 표시되면 다음 인수에 대한 값을 입력합니다.

   - SSO 방법 ADFS 또는 ADFS를 입력합니다.
   - SSO 사용자 이름입니다
   - StorageGRID가 설치된 도메인입니다
   - StorageGRID의 주소입니다
   - 테넌트 관리 API에 액세스하려는 경우 테넌트 계정 ID입니다.

```
python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*******************************************************************************

*******************************************************************************
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

StorageGRID 인증 토큰은 출력에 제공됩니다. 이제 SSO가 사용되지 않는 경우 API를 사용하는 방법과 유사하게 다른 요청에 토큰을 사용할 수 있습니다.

3. curl 요청을 사용하려면 다음 절차를 따르십시오.

   a. 로그인에 필요한 변수를 선언합니다.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

> Grid Management API에 액세스하려면 0을 "TENANTACCOUNTID"로 사용합니다.

   b. 서명된 인증 URL을 받으려면 '/api/v3/authorize-SAML'에 POST 요청을 보내고 응답에서 추가 JSON 인코딩을 제거합니다.

   이 예제에서는 "TENANTACCOUNTID"에 대한 서명된 인증 URL에 대한 POST 요청을 보여 줍니다. 결과는 JSON 인코딩을 제거하기 위해 python-m json.tool으로 전달됩니다.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

   이 예제의 응답에는 URL로 인코딩된 서명된 URL이 포함되어 있지만 추가 JSON 인코딩 계층은 포함되지 않습니다.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 후속 명령어에 사용하기 위해 응답에서 'AMLRequest'를 저장한다.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. AD FS에서 클라이언트 요청 ID가 포함된 전체 URL을 가져옵니다.

한 가지 옵션은 이전 응답의 URL을 사용하여 로그인 양식을 요청하는 것입니다.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

응답에는 클라이언트 요청 ID:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. 응답에서 클라이언트 요청 ID를 저장합니다.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. 이전 응답에서 양식 작업으로 자격 증명을 보냅니다.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS는 헤더에 추가 정보가 포함된 302 리디렉션을 반환합니다.

> SSO 시스템에 대해 MFA(다중 요소 인증)가 활성화된 경우 양식 게시물에는 두 번째 암호 또는 다른 자격 증명도 포함됩니다.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. 응답에서 MISAuth 쿠키를 저장합니다.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. 인증 POST에서 쿠키를 사용하여 지정된 위치로 GET 요청을 보냅니다.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

응답 헤더에는 나중에 로그아웃 사용을 위한 AD FS 세션 정보가 포함되며 응답 본문에는 숨겨진 양식 필드에 SALMLResponse가 포함됩니다.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. 숨겨진 필드에서 '응답'을 저장합니다.

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 저장된 'SAMLResponse'를 사용하여 StorageGRID 인증 토큰을 생성하기 위한 StorageGRID '/API/SAML-RESPONSE' 요청을 생성합니다.

RelayState의 경우, Grid Management API에 로그인하려면 테넌트 계정 ID를 사용하거나 0을 사용하십시오.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

응답에는 인증 토큰이 포함됩니다.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 응답에 인증 토큰을 MYTOKEN으로 저장합니다.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

이제 다른 요청에는 MYTOKEN을 사용할 수 있습니다. SSO를 사용하지 않을 경우 API를 사용하는 방법과 비슷합니다.

SSO(Single Sign-On)가 활성화된 경우 API에서 로그아웃합니다

SSO(Single Sign-On)가 활성화된 경우 그리드 관리 API 또는 테넌트 관리 API에서 로그아웃하기 위해 일련의 API 요청을 실행해야 합니다. Active Directory를 SSO ID 공급자로 사용하는 경우 다음 지침이 적용됩니다

이 작업에 대해

필요한 경우 조직의 단일 로그아웃 페이지에서 로그아웃하기만 하면 StorageGRID API에서 로그아웃할 수 있습니다. 또는 StorageGRID에서 유효한 StorageGRID 베어러 토큰이 필요한 단일 로그아웃(SLO)을 트리거할 수 있습니다.

단계

1. 서명된 로그아웃 요청을 생성하려면 SLO API에 쿠키 "SSO=true""를 전달합니다.

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

로그아웃 URL이 반환됩니다.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. 로그아웃 URL을 저장합니다.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. 로그아웃 URL에 요청을 보내 SLO를 트리거하고 StorageGRID로 다시 리디렉션합니다.

```
curl --include "$LOGOUT_REQUEST"
```

302 응답이 반환됩니다. 리디렉션 위치는 API 전용 로그아웃에는 적용되지 않습니다.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. StorageGRID bearer token을 삭제한다.

StorageGRID 베어러 토큰을 삭제하는 것은 SSO를 사용하지 않는 것과 동일한 방식으로 작동합니다. cookie "sso=true"'를 제공하지 않으면 SSO 상태에 영향을 주지 않고 StorageGRID에서 로그아웃됩니다.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

204 콘텐츠 없음 응답은 사용자가 로그아웃되었음을 나타냅니다.

```
HTTP/1.1 204 No Content
```

SSO(Single Sign-On)가 활성화된 경우 **API** 사용**(Azure)**

있는 경우 SSO(Single Sign-On) 구성 및 활성화 Azure를 SSO 공급자로 사용하는 경우, 두 개의 예제 스크립트를 사용하여 Grid Management API 또는 Tenant Management API에 유효한 인증 토큰을 얻을 수 있습니다.

Azure Single Sign-On이 활성화된 경우 **API**에 로그인합니다

Azure를 SSO ID 공급자로 사용하는 경우 다음 지침이 적용됩니다

필요한 것

- StorageGRID 사용자 그룹에 속한 페더레이션 사용자의 SSO 전자 메일 주소와 암호를 알고 있습니다.
- 테넌트 관리 API에 액세스하려면 테넌트 계정 ID를 알고 있어야 합니다.

이 작업에 대해

인증 토큰을 얻으려면 다음 예제 스크립트를 사용할 수 있습니다.

- 토라게르흐산스소auth-soauth-so.py 파이썬 스크립트
- toragegrid-soauth-Azure.js의 Node.js 스크립트

두 스크립트는 모두 StorageGRID 설치 파일 디렉토리(Red Hat Enterprise Linux 또는 CentOS의 경우 ./rpms, Ubuntu 또는 Debian의 경우 ./debs, VMware의 경우 ./vsphere)에 있습니다.

Azure와의 API 통합 기능을 직접 작성하려면 'toragegrid-soauth-Azure.py' 스크립트를 참조하십시오. Python 스크립트는 StorageGRID에 직접 두 개의 요청을 하고(먼저 SAMLRequest를 받고 나중에 인증 토큰을 얻기 위해) Node.js 스크립트를 호출하여 Azure와 상호 작용하여 SSO 작업을 수행합니다.

SSO 작업은 일련의 API 요청을 사용하여 실행할 수 있지만, 그렇게 하는 것은 간단하지 않습니다. Puppeteer Node.js 모듈은 Azure SSO 인터페이스를 스크레핑하는 데 사용됩니다.

URL 인코딩 문제가 있는 경우 '지원되지 않는 SAML 버전' 오류가 표시될 수 있습니다.

단계

1. 다음과 같이 필요한 종속성을 설치합니다.
   a. Node.js를 설치합니다(참조) "https://nodejs.org/en/download/")를 클릭합니다.
   b. 필요한 Node.js 모듈(puppeteer 및 jsdom)을 설치합니다.

      "NPM INSTALL-g<MODULE>'

2. Python 스크립트를 Python 인터프리터로 전달하여 스크립트를 실행합니다.

   그런 다음 Python 스크립트는 해당 Node.js 스크립트를 호출하여 Azure SSO 상호 작용을 수행합니다.

3. 프롬프트가 표시되면 다음 인수에 대한 값을 입력하거나 매개 변수를 사용하여 전달합니다.
   - Azure에 로그인하는 데 사용되는 SSO 이메일 주소입니다
   - StorageGRID의 주소입니다
   - 테넌트 관리 API에 액세스하려는 경우 테넌트 계정 ID입니다
4. 메시지가 표시되면 암호를 입력하고 요청 시 Azure에 MFA 권한을 제공할 준비를 합니다.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
*******************************************************************************

Watch for and approve a 2FA authorization request
*******************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

> 이 스크립트는 MFA가 Microsoft Authenticator를 사용하여 수행된 것으로 가정합니다. 텍스트 메시지를 통해 받은 코드를 입력하는 등 다른 형태의 MFA를 지원하도록 스크립트를 수정해야 할 수도 있습니다.

StorageGRID 인증 토큰은 출력에 제공됩니다. 이제 SSO가 사용되지 않는 경우 API를 사용하는 방법과 유사하게 다른 요청에 토큰을 사용할 수 있습니다.

SSO(Single Sign-On)가 활성화된 경우 **API** 사용**(PingFederate)**

있는 경우 SSO(Single Sign-On) 구성 및 활성화 그리고 PingFederate를 SSO 공급자로 사용하는 경우 일련의 API 요청을 발급하여 Grid Management API 또는 Tenant Management API에 유효한 인증 토큰을 얻어야 합니다.

SSO(Single Sign-On)가 활성화된 경우 **API**에 로그인합니다

이 지침은 PingFederate를 SSO ID 공급자로 사용하는 경우 적용됩니다

필요한 것

- StorageGRID 사용자 그룹에 속한 페더레이션 사용자의 SSO 사용자 이름과 암호를 알고 있습니다.
- 테넌트 관리 API에 액세스하려면 테넌트 계정 ID를 알고 있어야 합니다.

이 작업에 대해

인증 토큰을 얻으려면 다음 예 중 하나를 사용할 수 있습니다.

- StorageGRID 설치 파일 디렉토리(Red Hat Enterprise Linux 또는 CentOS의 경우 ./rpms, Ubuntu 또는 Debian의 경우 ./debs, VMware의 경우 ./vsphere)에 있는 toragegrid-ssoauth.py Python 스크립트입니다.
- curl 요청의 워크플로 예

  컬을 너무 느리게 수행하면 컬링 작업 시간이 초과될 수 있습니다. "이 응답에 유효한 SubjectConfirmation을 찾을 수 없습니다."라는 오류가 표시될 수 있습니다.

  > 예제 curl 워크플로는 다른 사용자가 암호를 볼 수 없도록 보호하지 않습니다.

  URL 인코딩 문제가 있는 경우 '지원되지 않는 SAML 버전' 오류가 표시될 수 있습니다.

단계

1. 인증 토큰을 얻으려면 다음 방법 중 하나를 선택합니다.
   - toragegrid-soauth.py Python 스크립트를 사용하십시오. 2단계로 이동합니다.
   - curl 요청을 사용합니다. 3단계로 이동합니다.
2. 'toragegrid-ssoauth.py' 스크립트를 사용하려면 스크립트를 Python 해석기로 전달하고 스크립트를 실행합니다.

   프롬프트가 표시되면 다음 인수에 대한 값을 입력합니다.

   - SSO 방법 ""핑남부연합"(PINGFEDERATE, 핑남부연합 등)의 모든 변형을 입력할 수 있습니다.
   - SSO 사용자 이름입니다

- StorageGRID가 설치된 도메인입니다. 이 필드는 PingFederate에 사용되지 않습니다. 빈 칸으로 두거나 원하는 값을 입력할 수 있습니다.
- StorageGRID의 주소입니다
- 테넌트 관리 API에 액세스하려는 경우 테넌트 계정 ID입니다.

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_domain:
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*******************************************************************************

*******************************************************************************
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

StorageGRID 인증 토큰은 출력에 제공됩니다. 이제 SSO가 사용되지 않는 경우 API를 사용하는 방법과 유사하게 다른 요청에 토큰을 사용할 수 있습니다.

3. curl 요청을 사용하려면 다음 절차를 따르십시오.

   a. 로그인에 필요한 변수를 선언합니다.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

> Grid Management API에 액세스하려면 0을 "TENANTACCOUNTID"로 사용합니다.

   b. 서명된 인증 URL을 받으려면 '/api/v3/authorize-SAML'에 POST 요청을 보내고 응답에서 추가 JSON 인코딩을 제거합니다.

   이 예제에서는 TENANTACCOUNTID에 대한 서명된 인증 URL에 대한 POST 요청을 보여 줍니다. 결과는 python-m json.tool에 전달되어 JSON 인코딩을 제거합니다.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

   이 예제의 응답에는 URL로 인코딩된 서명된 URL이 포함되어 있지만 추가 JSON 인코딩 계층은 포함되지 않습니다.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 후속 명령어에 사용하기 위해 응답에서 'AMLRequest'를 저장한다.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. 응답과 쿠키를 내보내고 응답을 에코합니다.

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. 'pf.adapterId' 값을 내보내고 응답을 에코합니다.

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. 'href' 값을 내보내고(후행 슬래시/ 제거) 응답을 에코합니다.

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. '조치' 값 내보내기:

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. 자격 증명과 함께 쿠키 보내기:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. 숨겨진 필드에서 '응답'을 저장합니다.

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 저장된 'SAMLResponse'를 사용하여 StorageGRID 인증 토큰을 생성하기 위한 StorageGRID '/API/SAML-RESPONSE' 요청을 생성합니다.

RelayState의 경우, Grid Management API에 로그인하려면 테넌트 계정 ID를 사용하거나 0을 사용하십시오.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

응답에는 인증 토큰이 포함됩니다.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 응답에 인증 토큰을 MYTOKEN으로 저장합니다.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

이제 다른 요청에는 MYTOKEN을 사용할 수 있습니다. SSO를 사용하지 않을 경우 API를 사용하는 방법과 비슷합니다.

SSO(Single Sign-On)가 활성화된 경우 **API**에서 로그아웃합니다

SSO(Single Sign-On)가 활성화된 경우 그리드 관리 API 또는 테넌트 관리 API에서 로그아웃하기 위해 일련의 API 요청을 실행해야 합니다. 이 지침은 PingFederate를 SSO ID 공급자로 사용하는 경우 적용됩니다

이 작업에 대해

필요한 경우 조직의 단일 로그아웃 페이지에서 로그아웃하기만 하면 StorageGRID API에서 로그아웃할 수 있습니다. 또는 StorageGRID에서 유효한 StorageGRID 베어러 토큰이 필요한 단일 로그아웃(SLO)을 트리거할 수 있습니다.

단계

1. 서명된 로그아웃 요청을 생성하려면 SLO API에 쿠키 "SSO=true""를 전달합니다.

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

로그아웃 URL이 반환됩니다.

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. 로그아웃 URL을 저장합니다.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. 로그아웃 URL에 요청을 보내 SLO를 트리거하고 StorageGRID로 다시 리디렉션합니다.

```
curl --include "$LOGOUT_REQUEST"
```

302 응답이 반환됩니다. 리디렉션 위치는 API 전용 로그아웃에는 적용되지 않습니다.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. StorageGRID bearer token을 삭제한다.

StorageGRID 베어러 토큰을 삭제하는 것은 SSO를 사용하지 않는 것과 동일한 방식으로 작동합니다. cookie "sso=true"'를 제공하지 않으면 SSO 상태에 영향을 주지 않고 StorageGRID에서 로그아웃됩니다.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

204 콘텐츠 없음 응답은 사용자가 로그아웃되었음을 나타냅니다.

```
HTTP/1.1 204 No Content
```

StorageGRID에 대한 액세스를 제어합니다

프로비저닝 암호를 변경합니다

StorageGRID 프로비저닝 암호를 변경하려면 다음 절차를 따르십시오. 복구, 확장 및 유지 보수 절차에 필요한 암호 문구입니다. 또한 그리드 토폴로지 정보, 그리드 노드 콘솔 암호 및 StorageGRID 시스템용 암호화 키가 포함된 복구 패키지 백업을 다운로드하려면 암호문이 필요합니다.

필요한 것

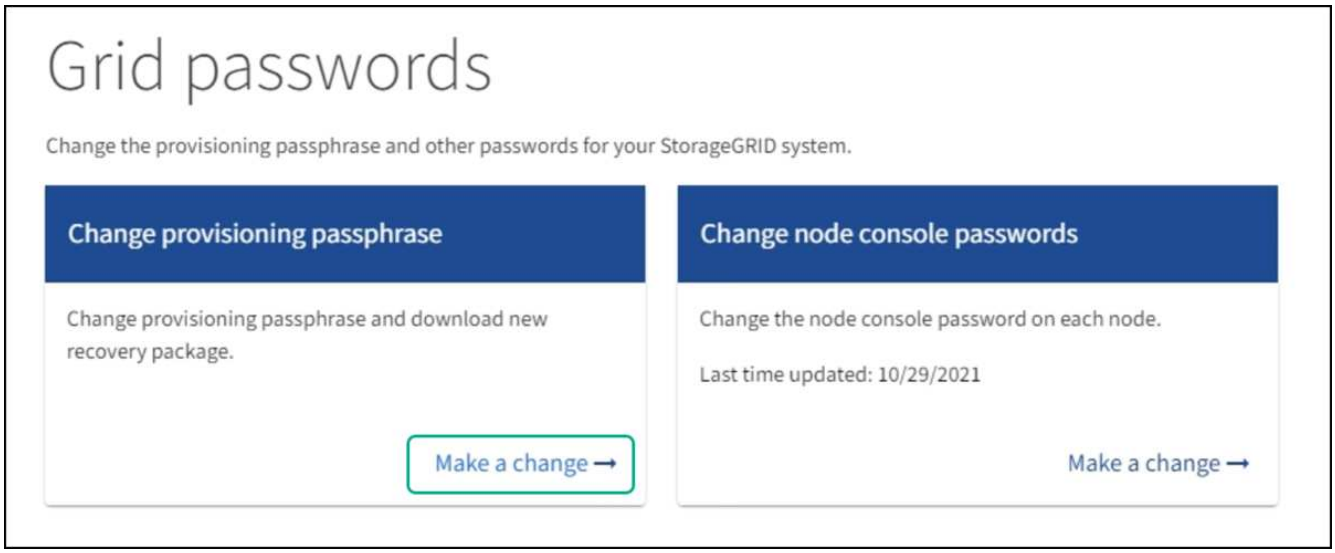
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 현재 프로비저닝 암호가 있습니다.

이 작업에 대해

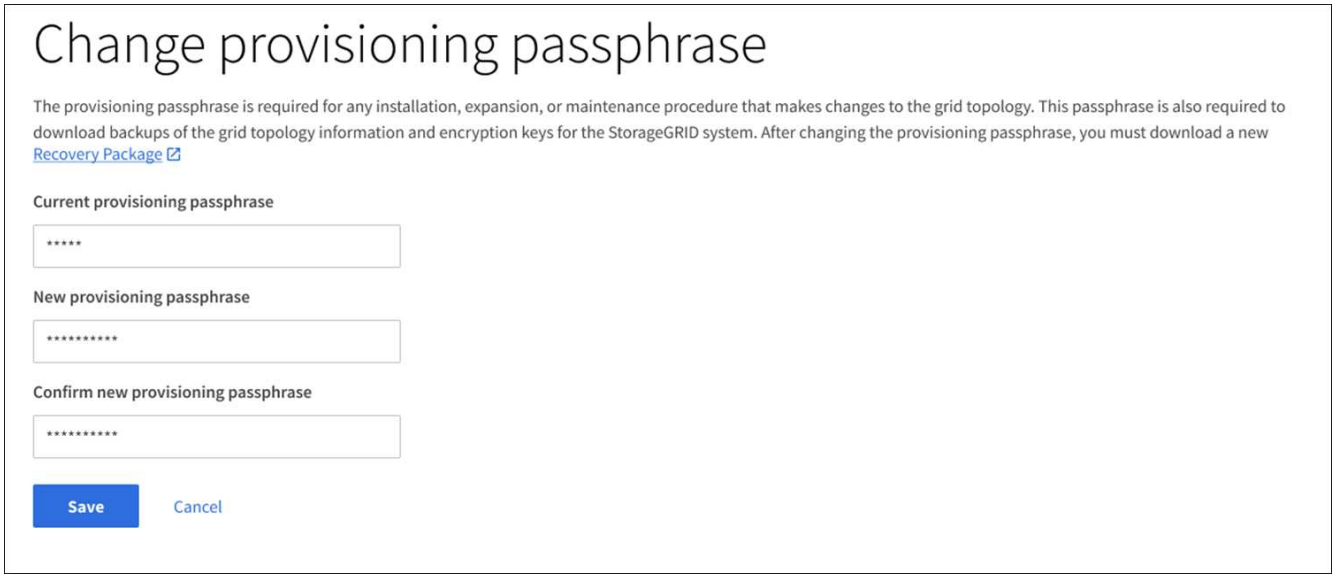
프로비저닝 암호는 많은 설치 및 유지 관리 절차와 에 필요합니다 복구 패키지 다운로드 중. 프로비저닝 암호는 passwords.txt 파일에 나열되지 않습니다. 프로비저닝 암호를 문서화하고 안전한 장소에 보관해야 합니다.

단계

1. 구성 * > * 액세스 제어 * > * 그리드 비밀번호 * 를 선택합니다.

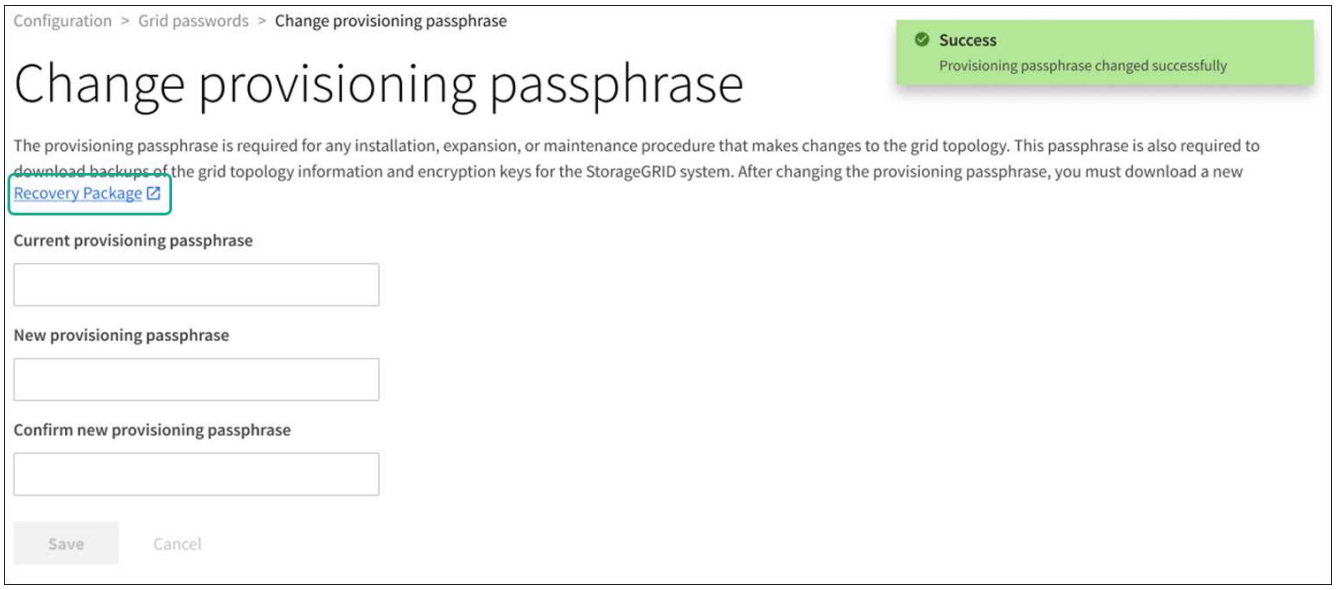


2. Change provisioning passphrase * 에서 * 변경 * 을 선택합니다.



3. 현재 프로비저닝 암호를 입력합니다.
4. 새 암호를 입력합니다. 암호는 8자 이상 32자 이하여야 합니다. 암호는 대/소문자를 구분합니다.
5. 새 프로비저닝 암호를 안전한 위치에 저장합니다. 설치, 확장 및 유지보수 절차에 필요합니다.
6. 새 암호를 다시 입력하고 * Save * 를 선택합니다.

   프로비저닝 암호 변경이 완료되면 녹색 성공 배너가 표시됩니다.



7. 복구 패키지 * 를 선택합니다.
8. 새 프로비저닝 암호를 입력하여 새 복구 패키지를 다운로드합니다.

> 프로비저닝 암호를 변경한 후에는 즉시 새 복구 패키지를 다운로드해야 합니다. 복구 패키지 파일을 사용하면 오류가 발생할 경우 시스템을 복원할 수 있습니다.

노드 콘솔 암호를 변경합니다

그리드의 각 노드에는 노드에 로그인해야 하는 고유한 노드 콘솔 암호가 있습니다. 다음 단계를 사용하여 그리드의 각 노드에 대한 고유한 노드 콘솔 암호를 변경합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 "지원되는 웹 브라우저".
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 현재 프로비저닝 암호가 있습니다.

이 작업에 대해

노드 콘솔 암호를 사용하여 SSH를 사용하여 노드에 "admin"으로 로그인하거나 VM/물리적 콘솔 연결의 루트 사용자에게 로그인할 수 있습니다. 노드 콘솔 암호 변경 프로세스에서는 그리드의 각 노드에 대해 새 암호를 생성하고 암호를 업데이트된 에 저장합니다 `Passwords.txt` 복구 패키지에 있는 파일. 암호는 의 암호 열에 나열됩니다 `Passwords.txt` 파일.

> 노드 간 통신에 사용되는 SSH 키에 대해 별도의 SSH 액세스 암호가 있습니다. 이 절차에서는 SSH 액세스 암호를 변경하지 않습니다.

마법사에 액세스합니다

단계

1. 구성 * > * 액세스 제어 * > * 그리드 비밀번호 * 를 선택합니다.
2. 노드 콘솔 암호 변경 * 에서 * 변경 * 을 선택합니다.

프로비저닝 암호를 입력합니다

단계

1. 그리드의 프로비저닝 암호를 입력합니다.
2. Continue * 를 선택합니다.

현재 복구 패키지를 다운로드합니다

노드 콘솔 암호를 변경하기 전에 현재 복구 패키지를 다운로드하십시오. 노드에 대한 암호 변경 프로세스가 실패할 경우 이 파일의 암호를 사용할 수 있습니다.

단계

1. 복구 패키지 다운로드 * 를 선택합니다.
2. 복구 패키지 파일을 복사합니다 (`.zip`)를 사용하여 두 개의 안전하고 서로 다른 위치에 안전하게 보관합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

3. Continue * 를 선택합니다.
4. 확인 대화 상자가 나타나면 노드 콘솔 암호 변경을 시작할 준비가 되었으면 * 예 * 를 선택합니다.

이 프로세스가 시작된 후에는 취소할 수 없습니다.

노드 콘솔 암호를 변경합니다

노드 콘솔 암호 프로세스가 시작되면 새 암호를 포함하는 새 복구 패키지가 생성됩니다. 그런 다음 각 노드에서 암호가 업데이트됩니다.

단계

1. 새 복구 패키지가 생성될 때까지 기다립니다. 몇 분 정도 걸릴 수 있습니다.
2. 새 복구 패키지 다운로드 * 를 선택합니다.
3. 다운로드가 완료되면 다음을 수행합니다.

   a. '.zip' 파일을 엽니다.

   b. 를 포함하여 콘텐츠에 액세스할 수 있는지 확인합니다 `Passwords.txt` 새 노드 콘솔 암호가 들어 있는 파일입니다.

   c. 새 복구 패키지 파일을 복사합니다 (`.zip`)를 사용하여 두 개의 안전하고 서로 다른 위치에 안전하게 보관합니다.

   > 이전 복구 패키지를 덮어쓰지 마십시오.

   복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

4. 새 복구 패키지를 다운로드하고 콘텐츠를 확인했음을 나타내려면 확인란을 선택합니다.
5. 노드 콘솔 암호 변경 * 을 선택하고 모든 노드가 새 암호로 업데이트될 때까지 기다립니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.

   모든 노드에 대한 암호가 변경되면 녹색 성공 배너가 나타납니다. 다음 단계로 이동합니다.

   업데이트 프로세스 중에 오류가 발생하면 배너 메시지에 암호가 변경되지 않은 노드 수가 표시됩니다. 암호가 변경되지 않은 노드에서 프로세스가 자동으로 다시 시도됩니다. 일부 노드의 암호를 변경하지 않고 프로세스가 종료되면 * Retry * (재시도 *) 버튼이 나타납니다.

   하나 이상의 노드에 대한 암호 업데이트가 실패한 경우:

   a. 표에 나열된 오류 메시지를 검토합니다.

   b. 문제를 해결합니다.

   c. 재시도 * 를 선택합니다.

   > 다시 시도하면 이전 암호 변경 시도 중에 실패한 노드의 노드 콘솔 암호만 변경됩니다.

6. 모든 노드에 대해 노드 콘솔 암호를 변경한 후 을 삭제합니다 다운로드한 첫 번째 복구 패키지.
7. 필요에 따라 * 복구 패키지 * 링크를 사용하여 새 복구 패키지의 추가 복사본을 다운로드합니다.

방화벽을 통한 액세스 제어

방화벽을 통해 액세스를 제어하려면 외부 방화벽에서 특정 포트를 열거나 닫습니다.

외부 방화벽에서 액세스를 제어합니다

외부 방화벽에서 특정 포트를 열거나 닫아 StorageGRID 관리 노드의 사용자 인터페이스 및 API에 대한 액세스를 제어할 수 있습니다. 예를 들어, 테넌트가 다른 방법을 사용하여 시스템 액세스를 제어하는 것 외에도 방화벽에서 Grid Manager에 연결할 수 없도록 할 수 있습니다.

포트	설명	포트가 열려 있는 경우...
443	관리 노드의 기본 HTTPS 포트	웹 브라우저 및 관리 API 클라이언트는 Grid Manager, Grid Management API, Tenant Manager 및 Tenant Management API에 액세스할 수 있습니다. • 참고: * 포트 443은 일부 내부 트래픽에도 사용됩니다.
8443	관리 노드의 제한된 그리드 관리자 포트	• 웹 브라우저 및 관리 API 클라이언트는 HTTPS를 사용하여 그리드 관리자 및 그리드 관리 API에 액세스할 수 있습니다. • 웹 브라우저 및 관리 API 클라이언트는 테넌트 관리자 또는 테넌트 관리 API에 액세스할 수 없습니다. • 내부 콘텐츠 요청은 거부됩니다.
9443	관리 노드의 제한된 테넌트 관리자 포트	• 웹 브라우저 및 관리 API 클라이언트는 HTTPS를 사용하여 테넌트 관리자 및 테넌트 관리 API에 액세스할 수 있습니다. • 웹 브라우저 및 관리 API 클라이언트는 그리드 관리자 또는 그리드 관리 API에 액세스할 수 없습니다. • 내부 콘텐츠 요청은 거부됩니다.

제한된 Grid Manager 또는 테넌트 관리자 포트에서는 SSO(Single Sign-On)를 사용할 수 없습니다. 사용자가 SSO(Single Sign-On)로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다.

관련 정보

- Grid Manager에 로그인합니다
- 테넌트 계정을 생성합니다
- 외부 통신

ID 페더레이션을 사용합니다

ID 페더레이션을 사용하면 그룹 및 사용자를 더 빠르게 설정할 수 있으며, 사용자는 익숙한 자격 증명을 사용하여 StorageGRID에 로그인할 수 있습니다.

Grid Manager의 ID 페더레이션을 구성합니다

Active Directory, Azure Active Directory(Azure AD), OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 관리 그룹 및 사용자를 관리하려는 경우 Grid Manager에서 ID 페더레이션을 구성할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- Active Directory, Azure AD, OpenLDAP 또는 Oracle Directory Server를 ID 공급자로 사용하고 있습니다.

> 목록에 없는 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의하십시오.

- OpenLDAP를 사용하려면 OpenLDAP 서버를 구성해야 합니다. 을 참조하십시오 OpenLDAP 서버 구성 지침.
- SSO(Single Sign-On)를 사용하려는 경우 을 검토했습니다 Single Sign-On 사용에 대한 요구 사항.
- LDAP 서버와의 통신에 TLS(Transport Layer Security)를 사용하려는 경우 ID 공급자는 TLS 1.2 또는 1.3을 사용합니다. 을 참조하십시오 발신 TLS 연결에 지원되는 암호.

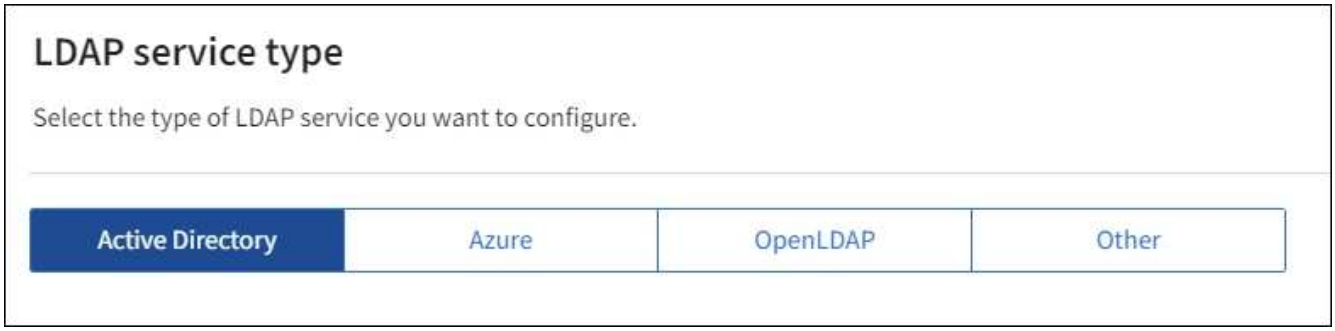
이 작업에 대해

Active Directory, Azure AD, OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 그룹을 가져오려면 Grid Manager의 ID 소스를 구성할 수 있습니다. 다음 유형의 그룹을 가져올 수 있습니다.

- 관리 그룹: 관리자 그룹의 사용자는 그룹에 할당된 관리 권한에 따라 Grid Manager에 로그인하여 작업을 수행할 수 있습니다.
- 자신의 ID 소스를 사용하지 않는 테넌트의 테넌트 사용자 그룹 테넌트 그룹의 사용자는 테넌트 관리자의 그룹에 할당된 권한을 기반으로 테넌트 관리자에 로그인하여 작업을 수행할 수 있습니다. 을 참조하십시오 테넌트 계정을 생성합니다 및 테넌트 계정을 사용합니다 를 참조하십시오.

구성을 입력합니다

1. 구성 * > * 액세스 제어 * > * ID 페더레이션 * 을 선택합니다.
2. ID 페더레이션 사용 * 을 선택합니다.
3. LDAP 서비스 유형 섹션에서 구성할 LDAP 서비스 유형을 선택합니다.



Oracle Directory Server를 사용하는 LDAP 서버의 값을 구성하려면 * 기타 * 를 선택합니다.

4. 기타 * 를 선택한 경우 LDAP 속성 섹션의 필드를 작성합니다. 그렇지 않으면 다음 단계로 이동합니다.
   - * 사용자 고유 이름 *: LDAP 사용자의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 Active Directory의 경우 'AMAccountName', OpenLDAP의 경우 'uid'와 같습니다. Oracle Directory Server를 구성하는 경우

"uid"를 입력합니다.

- * 사용자 UUID *: LDAP 사용자의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 Active Directory의 경우 objectGUID, OpenLDAP의 경우 entryUUID와 같습니다. Oracle Directory Server를 구성하는 경우 "n스uniqueid"를 입력합니다. 지정된 속성에 대한 각 사용자의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.
- * 그룹 고유 이름 *: LDAP 그룹의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 Active Directory의 경우 'AMAccountName', OpenLDAP의 경우 'cn'과 같습니다. Oracle Directory Server를 구성하는 경우 cn을 입력합니다.
- * 그룹 UUID *: LDAP 그룹의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 Active Directory의 경우 objectGUID, OpenLDAP의 경우 entryUUID와 같습니다. Oracle Directory Server를 구성하는 경우 "n스uniqueid"를 입력합니다. 지정된 속성에 대한 각 그룹의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.

5. 모든 LDAP 서비스 유형에 대해 LDAP 서버 구성 섹션에 필요한 LDAP 서버 및 네트워크 연결 정보를 입력합니다.
   - * 호스트 이름 *: LDAP 서버의 FQDN(정규화된 도메인 이름) 또는 IP 주소입니다.
   - * 포트 *: LDAP 서버에 연결하는 데 사용되는 포트입니다.

     STARTTLS의 기본 포트는 389이고 LDAPS의 기본 포트는 636입니다. 그러나 방화벽이 올바르게 구성된 경우 모든 포트를 사용할 수 있습니다.

   - * 사용자 이름 *: LDAP 서버에 연결할 사용자의 DN(고유 이름)의 전체 경로입니다.

     Active Directory의 경우 아래쪽 로그온 이름 또는 사용자 기본 이름을 지정할 수도 있습니다.

     지정된 사용자는 그룹 및 사용자를 나열하고 다음 속성에 액세스할 수 있는 권한이 있어야 합니다.

     - '사계정 이름' 또는 'uid'
     - objectGUID, entryUUID, n스uniqueid
     - 'cn'입니다
     - 'emberOf' 또는 'isMemberOf'
     - Active Directory *: objectSid, primaryGroupID, userAccountControl, userPrincipalName
     - * Azure *:'accountEnabled' 및 'userPrincipalName'
   - * 암호 *: 사용자 이름과 연결된 암호입니다.
   - * Group Base DN *: 그룹을 검색할 LDAP 하위 트리에 대한 DN(고유 이름)의 전체 경로입니다. Active Directory 예제(아래)에서 고유 이름이 기본 DN(DC=StorageGrid, DC=example, DC=com)과 관련된 모든 그룹을 통합 그룹으로 사용할 수 있습니다.

     그룹 고유 이름 * 값은 * 그룹 기본 DN * 내에서 고유해야 합니다.

   - * 사용자 기본 DN *: 사용자를 검색할 LDAP 하위 트리의 고유 이름(DN)의 전체 경로입니다.

     사용자 고유 이름 * 값은 * 사용자 기본 DN * 내에서 고유해야 합니다.

   - * 사용자 이름 형식 바인딩 * (선택 사항): 패턴을 자동으로 확인할 수 없는 경우 StorageGRID에서 기본 사용자 이름 패턴을 사용해야 합니다.

StorageGRID가 서비스 계정에 바인딩할 수 없는 경우 사용자가 로그인할 수 있으므로 * 사용자 이름 형식 바인딩 * 을 제공하는 것이 좋습니다.

다음 패턴 중 하나를 입력합니다.

- * UserPrincipalName 패턴(Active Directory 및 Azure) *: '[UserName]@*example*.com'
- * 하위 수준 로그온 이름 패턴(Active Directory 및 Azure) *: `*example*\[사용자 이름]'
- * 고유 이름 패턴 *:'CN=[UserName],CN=Users,DC=*Example*,DC=com'

  [UserName] * 을 서면 그대로 포함합니다.

6. TLS(전송 계층 보안) 섹션에서 보안 설정을 선택합니다.
   - * STARTTLS 사용 *: STARTTLS를 사용하여 LDAP 서버와의 통신 보안을 설정합니다. 이 옵션은 Active Directory, OpenLDAP 또는 기타 에 대해 권장되지만 Azure에서는 지원되지 않습니다.
   - * LDAPS * 사용: LDAPS(LDAP over SSL) 옵션은 TLS를 사용하여 LDAP 서버에 연결합니다. Azure의 경우 이 옵션을 선택해야 합니다.
   - * TLS * 사용 안 함: StorageGRID 시스템과 LDAP 서버 간의 네트워크 트래픽은 보호되지 않습니다. 이 옵션은 Azure에서 지원되지 않습니다.

     Active Directory 서버가 LDAP 서명을 적용하는 경우 * TLS 사용 안 함 * 옵션을 사용할 수 없습니다. STARTTLS 또는 LDAPS를 사용해야 합니다.

7. STARTTLS 또는 LDAPS를 선택한 경우 연결 보안에 사용되는 인증서를 선택합니다.
   - * 운영 체제 CA 인증서 사용 *: 운영 체제에 설치된 기본 그리드 CA 인증서를 사용하여 연결을 보호합니다.
   - * 사용자 지정 CA 인증서 사용 *: 사용자 지정 보안 인증서를 사용합니다.

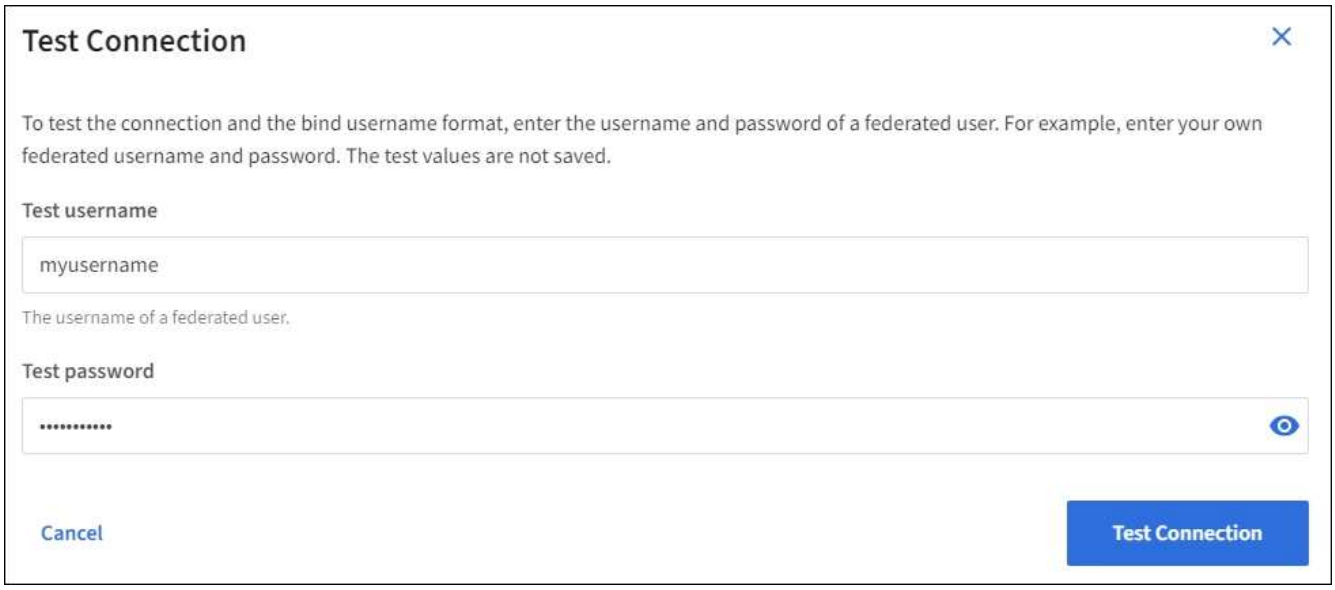
     이 설정을 선택한 경우 사용자 지정 보안 인증서를 복사하여 CA 인증서 텍스트 상자에 붙여 넣습니다.

연결을 테스트하고 구성을 저장합니다

모든 값을 입력한 후 구성을 저장하기 전에 연결을 테스트해야 합니다. StorageGRID는 LDAP 서버에 대한 연결 설정과 바인딩 사용자 이름 형식(제공한 경우)을 확인합니다.

1. Test connection * 을 선택합니다.
2. 바인딩 사용자 이름 형식을 제공하지 않은 경우:
   - 연결 설정이 유효하면 "Test connection successful(연결 테스트 성공)" 메시지가 나타납니다. Save * 를 선택하여 설정을 저장합니다.
   - 연결 설정이 잘못된 경우 ""테스트 연결을 설정할 수 없습니다"" 메시지가 나타납니다. 닫기 * 를 선택합니다. 그런 다음 문제를 해결하고 연결을 다시 테스트합니다.
3. 바인딩 사용자 이름 형식을 제공한 경우 유효한 통합 사용자의 사용자 이름과 암호를 입력합니다.

   예를 들어 사용자 이름과 암호를 입력합니다. @ 또는 / 같은 특수 문자를 사용자 이름에 포함하지 마십시오.



- 연결 설정이 유효하면 "Test connection successful(연결 테스트 성공)" 메시지가 나타납니다. Save * 를 선택하여 설정을 저장합니다.
- 연결 설정, 바인딩 사용자 이름 형식 또는 테스트 사용자 이름과 암호가 올바르지 않으면 오류 메시지가 나타납니다. 모든 문제를 해결하고 연결을 다시 테스트합니다.

ID 소스와 강제로 동기화합니다

StorageGRID 시스템은 ID 소스에서 페더레이션 그룹과 사용자를 정기적으로 동기화합니다. 사용자 권한을 최대한 빨리 설정하거나 제한하려는 경우 동기화를 강제로 시작할 수 있습니다.

단계

1. ID 페더레이션 페이지로 이동합니다.
2. 페이지 맨 위에서 * 서버 동기화 * 를 선택합니다.

   동기화 프로세스는 환경에 따라 다소 시간이 걸릴 수 있습니다.

   ID 소스에서 페더레이션 그룹과 사용자를 동기화하는 데 문제가 있는 경우 * ID 페더레이션 동기화 실패 * 경고가 트리거됩니다.

ID 페더레이션을 비활성화합니다

그룹 및 사용자에 대한 ID 페더레이션을 일시적으로 또는 영구적으로 비활성화할 수 있습니다. ID 페더레이션을 사용하지 않도록 설정하면 StorageGRID와 ID 소스 간에 통신이 이루어지지 않습니다. 그러나 구성한 설정은 그대로 유지되므로 나중에 ID 페더레이션을 쉽게 다시 사용할 수 있습니다.

이 작업에 대해

ID 페더레이션을 사용하지 않도록 설정하기 전에 다음 사항을 확인해야 합니다.

- 페더레이션 사용자는 로그인할 수 없습니다.
- 현재 로그인한 페더레이션 사용자는 세션이 만료될 때까지 StorageGRID 시스템에 대한 액세스 권한을 유지하지만 세션이 만료된 후에는 로그인할 수 없습니다.
- StorageGRID 시스템과 ID 소스 간의 동기화는 수행되지 않으며 동기화되지 않은 계정에 대해 알림 또는 경보가

발생하지 않습니다.

- SSO(Single Sign-On)가 * Enabled * 또는 * Sandbox Mode * 로 설정된 경우 * Enable identity federation *(ID 페더레이션 사용 *) 확인란이 비활성화됩니다. ID 페더레이션을 비활성화하려면 Single Sign-On 페이지의 SSO 상태가 * 사용 안 함 * 이어야 합니다. 을 참조하십시오 SSO(Single Sign-On)를 비활성화합니다.

단계

1. ID 페더레이션 페이지로 이동합니다.
2. ID 페더레이션 사용 * 확인란의 선택을 취소합니다.

OpenLDAP 서버 구성 지침

OpenLDAP 서버를 ID 페더레이션에 사용하려면 OpenLDAP 서버에서 특정 설정을 구성해야 합니다.

> ActiveDirectory 또는 Azure가 아닌 ID 소스의 경우 StorageGRID는 외부에서 비활성화된 사용자에 대한 S3 액세스를 자동으로 차단하지 않습니다. S3 액세스를 차단하려면 사용자의 S3 키를 삭제하고 모든 그룹에서 사용자를 제거합니다.

MemberOf 및 구체화 오버레이

MemberOf 및 구체화 오버레이를 활성화해야 합니다. 자세한 내용은 의 역방향 그룹 구성원 유지 관리 지침을 참조하십시오http://www.openldap.org/doc/admin24/index.html["OpenLDAP 설명서: 버전 2.4 관리자 가이드"^].

인덱싱

지정된 인덱스 키워드를 사용하여 다음 OpenLDAP 속성을 구성해야 합니다.

- olcDbIndex:objectClass eq
- "olcDbIndex:uid eq,pres,sub'
- 올크DbIndex=cn eq,pres,sub
- olcDbIndex: entryUUID eq

또한 최적의 성능을 위해 사용자 이름 도움말에 언급된 필드를 인덱싱해야 합니다.

에서 역방향 그룹 구성원 유지 관리에 대한 정보를 참조하십시오http://www.openldap.org/doc/admin24/index.html["OpenLDAP 설명서: 버전 2.4 관리자 가이드"^].

관리 그룹을 관리합니다

관리자 그룹을 만들어 하나 이상의 관리자 사용자에 대한 보안 권한을 관리할 수 있습니다. StorageGRID 시스템에 대한 액세스 권한을 부여하려면 사용자가 그룹에 속해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- 통합 그룹을 가져오려는 경우 ID 페더레이션을 구성하고 통합 그룹이 이미 구성된 ID 소스에 있습니다.

관리자 그룹을 생성합니다

관리자 그룹을 사용하면 그리드 관리자 및 그리드 관리 API에서 어떤 기능과 작업에 액세스할 수 있는지 확인할 수 있습니다.

마법사에 액세스합니다

1. 구성 * > * 액세스 제어 * > * 관리 그룹 * 을 선택합니다.
2. Create group * 을 선택합니다.

그룹 유형을 선택합니다

로컬 그룹을 생성하거나 통합 그룹을 가져올 수 있습니다.

- 로컬 사용자에게 권한을 할당하려면 로컬 그룹을 만듭니다.
- 통합 그룹을 생성하여 ID 소스에서 사용자를 가져옵니다.

로컬 그룹

1. 로컬 그룹 * 을 선택합니다.
2. 나중에 필요에 따라 업데이트할 수 있는 그룹의 표시 이름을 입력합니다. 예를 들어, "유지 보수 사용자" 또는 ""ILM 관리자""가 있습니다.
3. 나중에 업데이트할 수 없는 그룹의 고유 이름을 입력합니다.
4. Continue * 를 선택합니다.

통합 그룹

1. 페더레이션 그룹 * 을 선택합니다.
2. 구성된 ID 소스에 표시된 대로 가져올 그룹의 이름을 정확하게 입력합니다.
   - Active Directory 및 Azure의 경우 sAMAccountName을 사용합니다.
   - OpenLDAP의 경우 CN(일반 이름)을 사용합니다.
   - 다른 LDAP의 경우 LDAP 서버에 적절한 고유한 이름을 사용합니다.
3. Continue * 를 선택합니다.

그룹 권한을 관리합니다

1. 액세스 모드 * 의 경우 그룹의 사용자가 그리드 관리자 및 그리드 관리 API에서 설정을 변경하고 작업을 수행할 수 있는지 또는 설정과 기능만 볼 수 있는지 여부를 선택합니다.
   - * 읽기-쓰기 * (기본값): 사용자는 설정을 변경하고 관리 권한에서 허용하는 작업을 수행할 수 있습니다.
   - * 읽기 전용 *: 사용자는 설정 및 기능만 볼 수 있습니다. 그리드 관리자 또는 그리드 관리 API에서 어떠한 변경이나 작업도 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 암호를 변경할 수 있습니다.

> 사용자가 여러 그룹에 속해 있고 모든 그룹이 * 읽기 전용 * 으로 설정된 경우 사용자는 선택된 모든 설정 및 기능에 대한 읽기 전용 액세스 권한을 갖게 됩니다.

2. 하나 이상의 를 선택합니다 그룹 권한.

   각 그룹에 적어도 하나의 권한을 할당해야 합니다. 그렇지 않으면 그룹에 속한 사용자가 StorageGRID에 로그인할 수 없습니다.

3. 로컬 그룹을 만드는 경우 * 계속 * 을 선택합니다. 통합 그룹을 만드는 경우 * 그룹 생성 * 및 * 마침 * 을 선택합니다.

사용자 추가(로컬 그룹만 해당)

1. 필요에 따라 이 그룹에 대해 하나 이상의 로컬 사용자를 선택합니다.

   아직 로컬 사용자를 만들지 않은 경우 사용자를 추가하지 않고 그룹을 저장할 수 있습니다. 사용자 페이지에서 이 그룹을 사용자에게 추가할 수 있습니다. 을 참조하십시오사용자 관리 를 참조하십시오.

2. Create group * 과 * Finish * 를 선택합니다.

관리 그룹을 보고 편집합니다

기존 그룹에 대한 세부 정보를 보거나 그룹을 수정하거나 그룹을 복제할 수 있습니다.

- 모든 그룹의 기본 정보를 보려면 그룹 페이지의 표를 검토하십시오.
- 특정 그룹에 대한 모든 세부 정보를 보거나 그룹을 편집하려면 * 작업 * 메뉴 또는 세부 정보 페이지를 사용하십시오.

작업	작업 메뉴	세부 정보 페이지
그룹 세부 정보를 봅니다	a. 그룹의 확인란을 선택합니다. b. Actions * > * View group details * 를 선택합니다.	테이블에서 그룹 이름을 선택합니다.
표시 이름 편집(로컬 그룹만 해당)	a. 그룹의 확인란을 선택합니다. b. Actions * > * Edit group name * 을 선택합니다. c. 새 이름을 입력합니다. d. 변경 내용 저장 * 을 선택합니다.	a. 세부 정보를 표시할 그룹 이름을 선택합니다. b. 편집 아이콘을 선택합니다 . c. 새 이름을 입력합니다. d. 변경 내용 저장 * 을 선택합니다.
액세스 모드 또는 권한을 편집합니다	a. 그룹의 확인란을 선택합니다. b. Actions * > * View group details * 를 선택합니다. c. 선택적으로 그룹의 액세스 모드를 변경합니다. d. 필요에 따라 을 선택하거나 선택을 취소합니다 그룹 권한. e. 변경 내용 저장 * 을 선택합니다.	a. 세부 정보를 표시할 그룹 이름을 선택합니다. b. 선택적으로 그룹의 액세스 모드를 변경합니다. c. 필요에 따라 을 선택하거나 선택을 취소합니다 그룹 권한. d. 변경 내용 저장 * 을 선택합니다.

그룹을 복제합니다

1. 그룹의 확인란을 선택합니다.
2. Actions * > * Duplicate group * 을 선택합니다.
3. 복제 그룹 마법사를 완료합니다.

그룹을 삭제합니다

시스템에서 그룹을 제거하고 그룹과 관련된 모든 권한을 제거하려면 관리자 그룹을 삭제할 수 있습니다. 관리자 그룹을 삭제하면 그룹에서 모든 사용자가 제거되지만 사용자는 삭제되지 않습니다.

1. 그룹 페이지에서 제거할 각 그룹에 대한 확인란을 선택합니다.
2. Actions * > * Delete group * 을 선택합니다.
3. 그룹 삭제 * 를 선택합니다.

그룹 권한

관리자 사용자 그룹을 만들 때 그리드 관리자의 특정 기능에 대한 액세스를 제어하는 권한을 하나 이상 선택합니다. 그런 다음 각 사용자를 이러한 관리 그룹 중 하나 이상에 할당하여 사용자가 수행할 수 있는 작업을 결정할 수 있습니다.

각 그룹에 적어도 하나의 권한을 할당해야 합니다. 그렇지 않으면 해당 그룹에 속한 사용자가 Grid Manager 또는 Grid Management API에 로그인할 수 없습니다.

기본적으로 하나 이상의 사용 권한이 있는 그룹에 속한 사용자는 다음 작업을 수행할 수 있습니다.

- Grid Manager에 로그인합니다
- 대시보드 보기
- 노드 페이지를 봅니다
- 그리드 토폴로지를 모니터링합니다
- 현재 및 해결된 경고를 봅니다
- 현재 및 과거 알람 보기(레거시 시스템)
- 자신의 암호 변경(로컬 사용자만 해당)
- 구성 및 유지 관리 페이지에서 특정 정보를 봅니다

사용 권한과 액세스 모드 간의 상호 작용

모든 권한에 대해 그룹의 * 액세스 모드 * 설정은 사용자가 설정을 변경하고 작업을 수행할 수 있는지 또는 관련 설정 및 기능만 볼 수 있는지 여부를 결정합니다. 사용자가 여러 그룹에 속해 있고 모든 그룹이 * 읽기 전용 * 으로 설정된 경우 사용자는 선택된 모든 설정 및 기능에 대한 읽기 전용 액세스 권한을 갖게 됩니다.

다음 섹션에서는 관리자 그룹을 만들거나 편집할 때 할당할 수 있는 권한에 대해 설명합니다. 명시적으로 언급되지 않은 기능을 사용하려면 * 루트 액세스 * 권한이 필요합니다.

루트 액세스

이 권한은 모든 그리드 관리 기능에 대한 액세스를 제공합니다.

알람 확인(레거시)

이 권한을 통해 알람(레거시 시스템)을 확인하고 이에 대응할 수 있습니다. 로그인한 모든 사용자는 현재 및 과거 알람을 볼 수 있습니다.

사용자가 그리드 토폴로지를 모니터링하고 알람을 확인하려면 이 권한을 할당해야 합니다.

테넌트 루트 암호를 변경합니다

이 권한은 테넌트 페이지의 * 루트 암호 변경 * 옵션에 대한 액세스를 제공하므로 테넌트의 로컬 루트 사용자의 암호를 변경할 수 있는 사용자를 제어할 수 있습니다. 이 권한은 S3 키 가져오기 기능이 활성화된 경우 S3 키를 마이그레이션하는 데도 사용됩니다. 이 권한이 없는 사용자는 * 루트 암호 변경 * 옵션을 볼 수 없습니다.

> 루트 암호 변경 * 옵션이 포함된 테넌트 페이지에 대한 액세스 권한을 부여하려면 * 테넌트 계정 * 권한도 할당합니다.

그리드 토폴로지 페이지 구성

이 권한은 * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지의 구성 탭에 대한 액세스를 제공합니다.

ILM을 참조하십시오

이 권한은 다음 * ILM * 메뉴 옵션에 대한 액세스를 제공합니다.

- 규칙
- 정책
- 삭제 코딩
- 지역
- 지원합니다

> 사용자는 * 기타 그리드 구성 * 및 * 그리드 토폴로지 페이지 구성 * 권한이 있어야 스토리지 등급을 관리할 수 있습니다.

유지 관리

다음 옵션을 사용하려면 사용자에게 유지 관리 권한이 있어야 합니다.

- * 구성 * > * 액세스 제어 *:
  - 그리드 암호
- * 유지보수 * > * 작업 *:
  - 서비스 해제
  - 확장
  - 개체 존재 여부 검사
  - 복구
- * 유지보수 * > * 시스템 *:

    - 복구 패키지
    - 소프트웨어 업데이트
- 지원 * > * 툴 *:
    - 로그

유지보수 권한이 없는 사용자는 다음 페이지를 볼 수 있지만 편집할 수는 없습니다.

- * 유지보수 * > * 네트워크 *:
    - DNS 서버
    - 그리드 네트워크
    - NTP 서버
- * 유지보수 * > * 시스템 *:
    - 라이센스
- * 구성 * > * 보안 *:
    - 인증서
    - 도메인 이름
- * 구성 * > * 모니터링 *:
    - 감사 및 syslog 서버

알림을 관리합니다

이 권한은 알림 관리 옵션에 대한 액세스를 제공합니다. 사용자는 이 권한을 가지고 있어야 Silence, 경고 알림 및 경고 규칙을 관리할 수 있습니다.

메트릭 쿼리

이 권한은 * 지원 * > * 도구 * > * 메트릭 * 페이지에 대한 액세스를 제공합니다. 이 권한은 또한 Grid Management API의 * Metrics * 섹션을 사용하여 맞춤형 Prometheus 메트릭 쿼리에 대한 액세스를 제공합니다.

개체 메타데이터 조회

이 권한은 * ILM * > * 개체 메타데이터 조회 * 페이지에 대한 액세스를 제공합니다.

기타 그리드 구성

이 권한은 추가 그리드 구성 옵션에 대한 액세스를 제공합니다.

> 이러한 추가 옵션을 보려면 사용자에게 * 그리드 토폴로지 페이지 구성 * 권한도 있어야 합니다.

- * ILM *:
    - 보관 등급
- * 구성 * > * 네트워크 *:
    - 링크 비용

- * 구성 * > * 시스템 *:
  - 표시 옵션
  - 그리드 옵션
  - 스토리지 옵션
- 지원 * > * 알람(레거시) *:
  - 사용자 지정 이벤트
  - 전체 알람
  - 레거시 전자 메일 설정

스토리지 어플라이언스 관리자

이 권한은 그리드 관리자를 통해 스토리지 어플라이언스에서 E-Series SANtricity System Manager에 대한 액세스를 제공합니다.

테넌트 계정

이 권한은 테넌트 페이지를 액세스하여 테넌트 계정을 생성, 편집 및 제거할 수 있습니다. 또한 이 권한을 통해 사용자는 기존 트래픽 분류 정책을 볼 수 있습니다.

API를 사용하여 기능을 비활성화합니다

그리드 관리 API를 사용하여 StorageGRID 시스템의 특정 기능을 완전히 비활성화할 수 있습니다. 기능이 비활성화되면 해당 기능과 관련된 작업을 수행할 수 있는 권한을 아무도 할당할 수 없습니다.

이 작업에 대해

비활성화된 기능 시스템을 사용하면 StorageGRID 시스템의 특정 기능에 액세스하지 못하게 할 수 있습니다. 루트 사용자 또는 * 루트 액세스 * 권한이 있는 관리자 그룹에 속한 사용자가 해당 기능을 사용할 수 없도록 하는 유일한 방법은 기능을 비활성화하는 것입니다.

이 기능이 어떻게 유용한지 이해하려면 다음 시나리오를 고려해 보십시오.

_Company A는 테넌트 계정을 생성하여 StorageGRID 시스템의 스토리지 용량을 임대하는 서비스 공급자입니다. 회사 A는 임차자의 객체 보안을 보호하기 위해 계정이 배포된 후 자신의 직원이 테넌트 계정에 액세스할 수 없도록 하려고 합니다. _

_회사 A는 그리드 관리 API에서 기능 비활성화 시스템을 사용하여 이 목표를 달성할 수 있습니다. 그리드 관리자(UI 및 API 모두)에서 * 테넌트 루트 암호 변경 * 기능을 완전히 비활성화함으로써 회사 A는 루트 사용자 및 * 루트 액세스 * 권한이 있는 그룹에 속하는 사용자를 포함하여 관리자 사용자가 테넌트 계정의 루트 사용자에 대한 암호를 변경할 수 없도록 할 수 있습니다. _

단계

1. Grid Management API에 대한 Swagger 문서에 액세스합니다. 을 참조하십시오 Grid Management API를 사용합니다.
2. 기능 비활성화 끝점을 찾습니다.
3. 테넌트 루트 암호 변경 등의 기능을 비활성화하려면 다음과 같이 API로 본문을 보냅니다.

"{"grid":{"changeTenantRootPassword":true}}"

요청이 완료되면 테넌트 루트 암호 변경 기능이 비활성화됩니다. 사용자 인터페이스에 * 테넌트 루트 암호 변경 * 관리 권한이 더 이상 나타나지 않으며 테넌트의 루트 암호를 변경하려고 시도하는 모든 API 요청이 "'403 사용 금지'"로 실패합니다.

비활성화된 피처를 다시 활성화합니다

기본적으로 그리드 관리 API를 사용하여 비활성화된 기능을 다시 활성화할 수 있습니다. 그러나 비활성화된 피처가 다시 활성화되지 않도록 하려면 * activateFeatures * 기능 자체를 비활성화할 수 있습니다.

> activateFeatures * 기능은 다시 활성화할 수 없습니다. 이 기능을 비활성화하려는 경우 비활성화된 다른 모든 기능을 다시 활성화할 수 있는 기능이 영구적으로 손실됩니다. 손실된 기능을 복원하려면 기술 지원 부서에 문의해야 합니다.

단계

1. Grid Management API에 대한 Swagger 문서에 액세스합니다.
2. 기능 비활성화 끝점을 찾습니다.
3. 모든 기능을 다시 활성화하려면 다음과 같이 API로 본문을 보내십시오.

   `{"grid":null}'

   이 요청이 완료되면 테넌트 루트 암호 변경 기능을 포함한 모든 기능이 다시 활성화됩니다. 이제 사용자 인터페이스에 * 테넌트 루트 암호 변경 * 관리 권한이 표시되며, 사용자에게 * 루트 액세스 * 또는 * 테넌트 루트 암호 변경 * 관리 권한이 있는 경우 테넌트의 루트 암호를 변경하려고 시도하는 모든 API 요청이 성공합니다.

> 이전 예에서는 _ALL_DEACTED 피처가 재활성화됩니다. 비활성화된 상태로 유지되어야 하는 다른 기능이 비활성화된 경우, PUT 요청에 명시적으로 지정해야 합니다. 예를 들어 테넌트 루트 암호 변경 기능을 다시 활성화하고 경보 승인 기능을 계속 비활성화하려면 다음 PUT 요청을 보내십시오.
>
> `{"grid":{"alarmAcknowledgement":true}}'

사용자 관리

로컬 및 통합 사용자를 볼 수 있습니다. 로컬 사용자를 만들고 로컬 관리자 그룹에 할당하여 이러한 사용자가 액세스할 수 있는 그리드 관리자 기능을 결정할 수도 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

로컬 사용자를 생성합니다

하나 이상의 로컬 사용자를 생성하고 각 사용자를 하나 이상의 로컬 그룹에 할당할 수 있습니다. 그룹의 권한은 사용자가 액세스할 수 있는 Grid Manager 및 Grid Management API 기능을 제어합니다.

로컬 사용자만 생성할 수 있습니다. 외부 ID 소스를 사용하여 연결된 사용자 및 그룹을 관리합니다.

Grid Manager에는 ""root""라는 이름의 미리 정의된 로컬 사용자가 하나 있습니다. 루트 사용자는 제거할 수 없습니다.

> SSO(Single Sign-On)가 활성화된 경우 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

마법사에 액세스합니다

1. 구성 * > * 액세스 제어 * > * 관리자 사용자 * 를 선택합니다.
2. 사용자 생성 * 을 선택합니다.

사용자 자격 증명을 입력합니다

1. 사용자의 전체 이름, 고유한 사용자 이름 및 암호를 입력합니다.
2. 이 사용자가 그리드 관리자 또는 그리드 관리 API에 액세스할 수 없는 경우 * 예 * 를 선택합니다(선택 사항).
3. Continue * 를 선택합니다.

그룹에 할당합니다

1. 필요에 따라 사용자를 하나 이상의 그룹에 할당하여 사용자의 권한을 결정합니다.

   아직 그룹을 만들지 않은 경우 그룹을 선택하지 않고 사용자를 저장할 수 있습니다. 이 사용자를 그룹 페이지의 그룹에 추가할 수 있습니다.

   사용자가 여러 그룹에 속한 경우 권한은 누적됩니다. 을 참조하십시오관리 그룹을 관리합니다 를 참조하십시오.

2. Create user * 를 선택하고 * Finish * 를 선택합니다.

로컬 사용자를 보고 편집합니다

기존 로컬 및 통합 사용자에 대한 세부 정보를 볼 수 있습니다. 로컬 사용자를 수정하여 사용자의 전체 이름, 암호 또는 그룹 구성원을 변경할 수 있습니다. 사용자가 그리드 관리자 및 그리드 관리 API에 일시적으로 액세스하지 못하도록 할 수도 있습니다.

로컬 사용자만 편집할 수 있습니다. 외부 ID 소스를 사용하여 페더레이션 사용자를 관리합니다.

- 모든 로컬 및 통합 사용자에 대한 기본 정보를 보려면 사용자 페이지의 표를 검토하십시오.
- 특정 사용자의 모든 세부 정보를 보거나, 로컬 사용자를 편집하거나, 로컬 사용자 암호를 변경하려면 * 작업 * 메뉴 또는 세부 정보 페이지를 사용하십시오.

  다음에 사용자가 로그아웃한 다음 다시 그리드 관리자에 로그인할 때 모든 편집 내용이 적용됩니다.

  > 로컬 사용자는 Grid Manager 배너의 * Change Password * 옵션을 사용하여 자신의 암호를 변경할 수 있습니다.

작업	작업 메뉴	세부 정보 페이지
사용자 세부 정보를 봅니다	a. 사용자의 확인란을 선택합니다. b. Actions * > * View user details * 를 선택합니다.	테이블에서 사용자 이름을 선택합니다.

작업	작업 메뉴	세부 정보 페이지
전체 이름 편집(로컬 사용자만 해당)	a. 사용자의 확인란을 선택합니다. b. 작업 * > * 전체 이름 편집 * 을 선택합니다. c. 새 이름을 입력합니다. d. 변경 내용 저장 * 을 선택합니다.	a. 사용자 이름을 선택하여 세부 정보를 표시합니다. b. 편집 아이콘을 선택합니다 . c. 새 이름을 입력합니다. d. 변경 내용 저장 * 을 선택합니다.
StorageGRID 액세스를 거부하거나 허용합니다	a. 사용자의 확인란을 선택합니다. b. Actions * > * View user details * 를 선택합니다. c. 액세스 탭을 선택합니다. d. 사용자가 그리드 관리자 또는 그리드 관리 API에 로그인하지 못하도록 하려면 * 예 * 를 선택하고, 사용자가 로그인할 수 있도록 하려면 * 아니요 * 를 선택합니다. e. 변경 내용 저장 * 을 선택합니다.	a. 사용자 이름을 선택하여 세부 정보를 표시합니다. b. 액세스 탭을 선택합니다. c. 사용자가 그리드 관리자 또는 그리드 관리 API에 로그인하지 못하도록 하려면 * 예 * 를 선택하고, 사용자가 로그인할 수 있도록 하려면 * 아니요 * 를 선택합니다. d. 변경 내용 저장 * 을 선택합니다.
암호 변경(로컬 사용자만 해당)	a. 사용자의 확인란을 선택합니다. b. Actions * > * View user details * 를 선택합니다. c. 암호 탭을 선택합니다. d. 새 암호를 입력합니다. e. 암호 변경 * 을 선택합니다.	a. 사용자 이름을 선택하여 세부 정보를 표시합니다. b. 암호 탭을 선택합니다. c. 새 암호를 입력합니다. d. 암호 변경 * 을 선택합니다.
그룹 변경(로컬 사용자만 해당)	a. 사용자의 확인란을 선택합니다. b. Actions * > * View user details * 를 선택합니다. c. 그룹 탭을 선택합니다. d. 필요에 따라 그룹 이름 뒤에 있는 링크를 선택하여 새 브라우저 탭에서 그룹의 세부 정보를 봅니다. e. 다른 그룹을 선택하려면 * Edit groups * 를 선택합니다. f. 변경 내용 저장 * 을 선택합니다.	a. 사용자 이름을 선택하여 세부 정보를 표시합니다. b. 그룹 탭을 선택합니다. c. 필요에 따라 그룹 이름 뒤에 있는 링크를 선택하여 새 브라우저 탭에서 그룹의 세부 정보를 봅니다. d. 다른 그룹을 선택하려면 * Edit groups * 를 선택합니다. e. 변경 내용 저장 * 을 선택합니다.

사용자를 복제합니다

기존 사용자를 복제하여 동일한 권한을 가진 새 사용자를 만들 수 있습니다.

1. 사용자의 확인란을 선택합니다.
2. Actions * > * Duplicate user * 를 선택합니다.
3. 사용자 복제 마법사를 완료합니다.

사용자를 삭제합니다

로컬 사용자를 삭제하여 해당 사용자를 시스템에서 영구적으로 제거할 수 있습니다.

> 루트 사용자는 삭제할 수 없습니다.

1. 사용자 페이지에서 제거할 각 사용자에 대한 확인란을 선택합니다.
2. Actions * > * Delete user * 를 선택합니다.
3. 사용자 삭제 * 를 선택합니다.

SSO(Single Sign-On) 사용

Single Sign-On 구성

SSO(Single Sign-On)가 활성화된 경우 사용자는 조직에서 구현한 SSO 로그인 프로세스를 사용하여 자격 증명이 승인된 경우에만 Grid Manager, Tenant Manager, Grid Management API 또는 Tenant Management API에 액세스할 수 있습니다. 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

Single Sign-On의 작동 방식

StorageGRID 시스템은 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용하여 SSO(Single Sign-On)를 지원합니다.

SSO(Single Sign-On)를 활성화하기 전에 SSO를 사용할 때 StorageGRID 로그인 및 로그아웃 프로세스가 어떻게 영향을 받는지 검토하십시오.

SSO가 활성화되면 로그인하십시오

SSO가 활성화되어 있고 StorageGRID에 로그인하면 조직의 SSO 페이지로 리디렉션되어 자격 증명을 검증합니다.

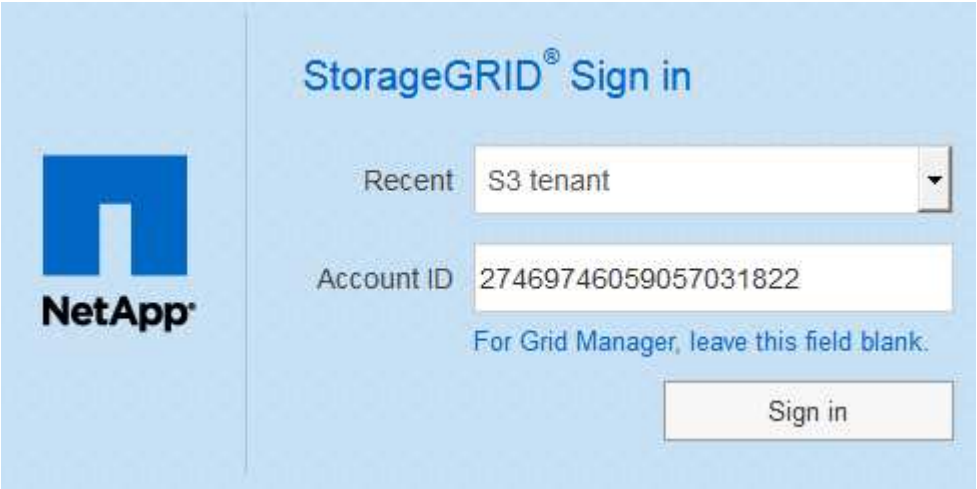
단계

1. 웹 브라우저에 StorageGRID 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력합니다.

   StorageGRID 로그인 페이지가 나타납니다.

   - 이 브라우저에서 URL에 처음 액세스한 경우 계정 ID를 입력하라는 메시지가 표시됩니다.

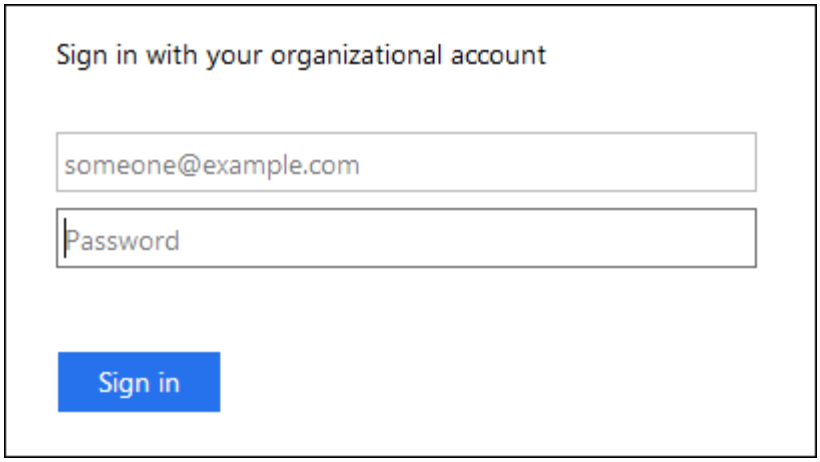
- 이전에 Grid Manager 또는 Tenant Manager에 액세스한 경우, 최근 계정을 선택하거나 계정 ID를 입력하라는 메시지가 나타납니다.



> 테넌트 계정에 대한 전체 URL(즉, 정규화된 도메인 이름 또는 IP 주소 다음에 "/?accountId=*20-digit-account-id*")을 입력하면 StorageGRID 로그인 페이지가 표시되지 않습니다. 대신 조직의 SSO 로그인 페이지로 즉시 리디렉션됩니다. 여기에서 해당 페이지로 이동할 수 있습니다 SSO 자격 증명으로 로그인합니다.

2. 그리드 관리자 또는 테넌트 관리자에 액세스할지 여부를 지정합니다.
   - Grid Manager에 액세스하려면 * Account ID * 필드를 비워 두고 계정 ID로 * 0 * 을 입력하거나, 최근 계정 목록에 * Grid Manager * 를 선택합니다.
   - Tenant Manager에 액세스하려면 20자리 테넌트 계정 ID를 입력하거나 최근 계정 목록에 나타나는 경우 이름으로 Tenant를 선택합니다.
3. 로그인 * 을 선택합니다

StorageGRID가 조직의 SSO 로그인 페이지로 리디렉션합니다. 예를 들면 다음과 같습니다.



4. SSO 자격 증명으로 로그인합니다.

   SSO 자격 증명이 올바른 경우:

   a. IDP(Identity Provider)는 StorageGRID에 인증 응답을 제공합니다.
   b. StorageGRID는 인증 응답을 검증합니다.
   c. 응답이 유효하고 StorageGRID 액세스 권한이 있는 통합 그룹에 속해 있는 경우 선택한 계정에 따라 그리드 관리자 또는 테넌트 관리자에 로그인됩니다.

   > 서비스 계정에 액세스할 수 없는 경우 StorageGRID 액세스 권한이 있는 통합 그룹에 속한 기존 사용자라면 계속 로그인할 수 있습니다.

5. 필요한 경우 다른 관리 노드에 액세스하거나 적절한 권한이 있는 경우 그리드 관리자 또는 테넌트 관리자에 액세스합니다.

   SSO 자격 증명을 다시 입력하지 않아도 됩니다.

SSO가 활성화되면 로그아웃합니다

StorageGRID에 대해 SSO가 활성화된 경우 로그아웃할 때 발생하는 작업은 로그인한 대상 및 로그아웃 위치에 따라 달라집니다.

단계

1. 사용자 인터페이스의 오른쪽 상단 모서리에 있는 * 로그아웃 * 링크를 찾습니다.
2. 로그아웃 * 을 선택합니다.

   StorageGRID 로그인 페이지가 나타납니다. 최근 계정 * 드롭다운은 * 그리드 관리자 * 또는 테넌트 이름을 포함하도록 업데이트되므로 나중에 이러한 사용자 인터페이스에 보다 빠르게 액세스할 수 있습니다.

에 로그인한 경우...	에서 로그아웃합니다.	에서 로그아웃되었습니다...
하나 이상의 관리 노드에서 그리드 관리자	모든 관리 노드의 그리드 관리자	모든 관리 노드의 그리드 관리자 • 참고: * SSO에 Azure를 사용하는 경우 모든 관리 노드에서 로그아웃하는 데 몇 분 정도 걸릴 수 있습니다.
하나 이상의 관리 노드에서 테넌트 관리자	모든 관리 노드의 테넌트 관리자	모든 관리 노드의 테넌트 관리자
Grid Manager와 Tenant Manager 모두	그리드 관리자	그리드 관리자 전용. SSO에서 로그아웃하려면 테넌트 관리자에서 로그아웃해야 합니다.

이 표에는 단일 브라우저 세션을 사용하는 경우 로그아웃할 때 발생하는 동작이 요약되어 있습니다. 여러 브라우저 세션에서 StorageGRID에 로그인한 경우 모든 브라우저 세션에서 별도로 로그아웃해야 합니다.

Single Sign-On 사용에 대한 요구 사항

StorageGRID 시스템에 대해 SSO(Single Sign-On)를 활성화하기 전에 이 섹션의 요구 사항을 검토하십시오.

ID 공급자 요구 사항

StorageGRID는 다음 SSO ID 공급자(IDP)를 지원합니다.

- AD FS(Active Directory Federation Service)
- Azure Active Directory(Azure AD)
- PingFederate(PingFederate)

SSO ID 공급자를 구성하려면 먼저 StorageGRID 시스템에 대한 ID 페더레이션을 구성해야 합니다. ID 페더레이션에 사용하는 LDAP 서비스 유형은 구현할 수 있는 SSO 유형을 제어합니다.

구성된 **LDAP** 서비스 유형입니다	**SSO ID** 공급자에 대한 옵션
Active Directory를 클릭합니다	• Active Directory를 클릭합니다 • Azure를 지원합니다 • PingFederate(PingFederate)
Azure를 지원합니다	Azure를 지원합니다

AD FS 요구 사항

다음 버전의 AD FS를 사용할 수 있습니다.

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016에서 을 사용해야 합니다 "KB3201845 업데이트"또는 그 이상.

- AD FS 3.0, Windows Server 2012 R2 업데이트 이상에 포함되어 있습니다.

추가 요구 사항

- TLS(전송 계층 보안) 1.2 또는 1.3
- Microsoft .NET Framework 버전 3.5.1 이상

서버 인증서 요구 사항

기본적으로 StorageGRID는 각 관리 노드의 관리 인터페이스 인증서를 사용하여 그리드 관리자, 테넌트 관리자, 그리드 관리 API 및 테넌트 관리 API에 대한 액세스를 보호합니다. AD FS(사용자 트러스트), Azure(엔터프라이즈 응용 프로그램) 또는 StorageGRID에 대한 서비스 공급자 연결(PingFederate)을 구성하는 경우 서버 인증서를 StorageGRID 요청에 대한 서명 인증서로 사용합니다.

아직 등록하지 않은 경우 관리 인터페이스에 대한 사용자 지정 인증서를 구성했습니다이제 그렇게 해야 합니다. 사용자 지정 서버 인증서는 모든 관리 노드에 사용되며 모든 StorageGRID 신뢰할 수 있는 당사자, 엔터프라이즈 응용 프로그램 또는 SP 연결에서 사용할 수 있습니다.

> 사용 중인 신뢰, 엔터프라이즈 응용 프로그램 또는 SP 연결에서 관리 노드의 기본 서버 인증서를 사용하는 것은 권장되지 않습니다. 노드가 실패하고 복구되면 새로운 기본 서버 인증서가 생성됩니다. 복구된 노드에 로그인하려면 먼저 신뢰할 수 있는 당사자 신뢰, 엔터프라이즈 애플리케이션 또는 SP 연결을 새 인증서로 업데이트해야 합니다.

노드의 명령 셸에 로그인하고 '/var/local/mgmt-api' 디렉토리로 이동하여 관리 노드의 서버 인증서에 액세스할 수 있습니다. 사용자 지정 서버 인증서는 사용자 지정 서버 .crt로 명명됩니다. 노드의 기본 서버 인증서는 'server.crt' 입니다.

포트 요구 사항

제한된 Grid Manager 또는 테넌트 관리자 포트에서는 SSO(Single Sign-On)를 사용할 수 없습니다. 사용자가 SSO(Single Sign-On)로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다. 을 참조하십시오 방화벽을 통한 액세스 제어.

페더레이션 사용자가 로그인할 수 있는지 확인합니다

SSO(Single Sign-On)를 활성화하기 전에 하나 이상의 통합 사용자가 Grid Manager에 로그인하고 기존 테넌트 계정에 대한 테넌트 관리자에 로그인할 수 있는지 확인해야 합니다.

필요한 것

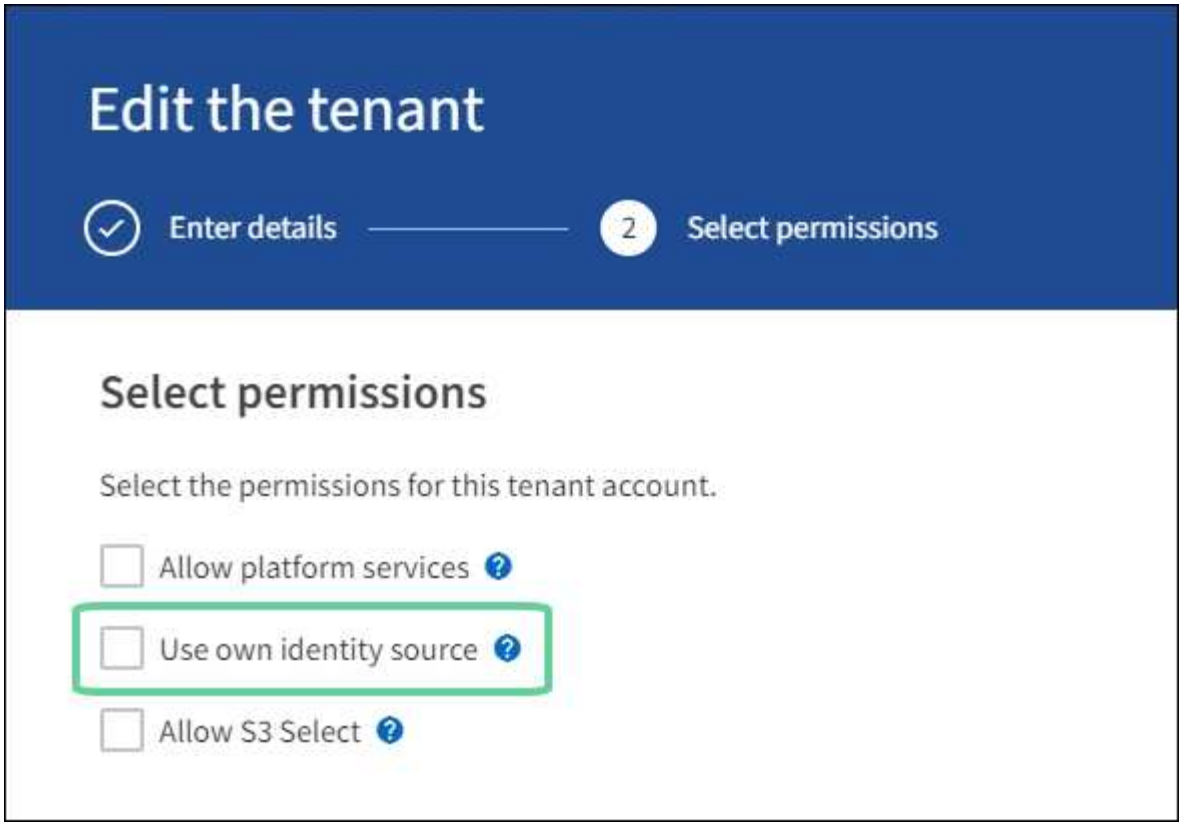
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- ID 페더레이션을 이미 구성했습니다.

단계

1. 기존 테넌트 계정이 있는 경우 해당 테넌트가 자신의 ID 소스를 사용하고 있지 않은지 확인합니다.

> SSO를 활성화하면 테넌트 관리자에 구성된 ID 소스가 그리드 관리자에 구성된 ID 소스에 의해 재정의됩니다. 테넌트의 ID 소스에 속하는 사용자는 Grid Manager ID 소스의 계정이 없으면 더 이상 로그인할 수 없습니다.

   a. 각 테넌트 계정의 테넌트 관리자에 로그인합니다.
   b. 액세스 관리 * > * ID 페더레이션 * 을 선택합니다.
   c. ID 페더레이션 사용 * 확인란이 선택되어 있지 않은지 확인합니다.
   d. 이 경우 이 테넌트 계정에 사용 중인 모든 통합 그룹이 더 이상 필요하지 않은지 확인하고 확인란의 선택을 취소하고 * Save * 를 선택합니다.
2. 통합 사용자가 Grid Manager에 액세스할 수 있는지 확인합니다.
   a. Grid Manager에서 * 구성 * > * 액세스 제어 * > * 관리 그룹 * 을 선택합니다.
   b. Active Directory ID 소스에서 하나 이상의 통합 그룹을 가져오고 루트 액세스 권한이 할당되었는지 확인합니다.
   c. 로그아웃합니다.
   d. 통합 그룹의 사용자로 그리드 관리자에 다시 로그인할 수 있는지 확인합니다.
3. 기존 테넌트 계정이 있는 경우 루트 액세스 권한이 있는 페더레이션 사용자가 로그인할 수 있는지 확인합니다.
   a. Grid Manager에서 * Tenants * 를 선택합니다.
   b. 테넌트 계정을 선택하고 * 작업 * > * 편집 * 을 선택합니다.
   c. 세부 정보 입력 탭에서 * 계속 * 을 선택합니다.
   d. Use own identity source * (고유 ID 소스 사용 *) 확인란을 선택한 경우 이 상자의 선택을 취소하고 * Save * (저장 *)를 선택합니다.



테넌트 페이지가 나타납니다.

a. 테넌트 계정을 선택하고 * 로그인 * 을 선택한 다음 테넌트 계정에 로컬 루트 사용자로 로그인합니다.
b. 테넌트 관리자에서 * 액세스 관리 * > * 그룹 * 을 선택합니다.
c. Grid Manager에서 하나 이상의 통합 그룹에 이 테넌트에 대한 루트 액세스 권한이 할당되었는지 확인합니다.
d. 로그아웃합니다.
e. 통합 그룹의 사용자로 테넌트에 다시 로그인할 수 있는지 확인합니다.

관련 정보

- Single Sign-On 사용에 대한 요구 사항
- 관리 그룹을 관리합니다
- 테넌트 계정을 사용합니다

sandbox 모드를 사용합니다

sandbox 모드를 사용하면 모든 StorageGRID 사용자가 SSO(Single Sign-On)를 사용하도록 설정하기 전에 이를 구성하고 테스트할 수 있습니다. SSO가 활성화된 후에는 구성을 변경하거나 다시 테스트해야 할 때마다 샌드박스 모드로 돌아갈 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.
- StorageGRID 시스템에 대해 ID 페더레이션을 구성했습니다.

- ID 페더레이션 * LDAP 서비스 유형 * 의 경우 사용하려는 SSO ID 공급자에 따라 Active Directory 또는 Azure를 선택했습니다.

구성된 **LDAP** 서비스 유형입니다	**SSO ID** 공급자에 대한 옵션
Active Directory를 클릭합니다	• Active Directory를 클릭합니다 • Azure를 지원합니다 • PingFederate(PingFederate)
Azure를 지원합니다	Azure를 지원합니다

이 작업에 대해

SSO가 활성화되어 있고 사용자가 관리자 노드에 로그인을 시도하면 StorageGRID는 인증 요청을 SSO ID 공급자에 보냅니다. 또한 SSO ID 공급자는 인증 요청이 성공했는지 여부를 나타내는 인증 응답을 StorageGRID로 다시 보냅니다. 성공적인 요청의 경우:

- Active Directory 또는 PingFederate의 응답에는 사용자의 UUID(Universally Unique Identifier)가 포함됩니다.
- Azure의 응답에는 UPN(User Principal Name)이 포함됩니다.

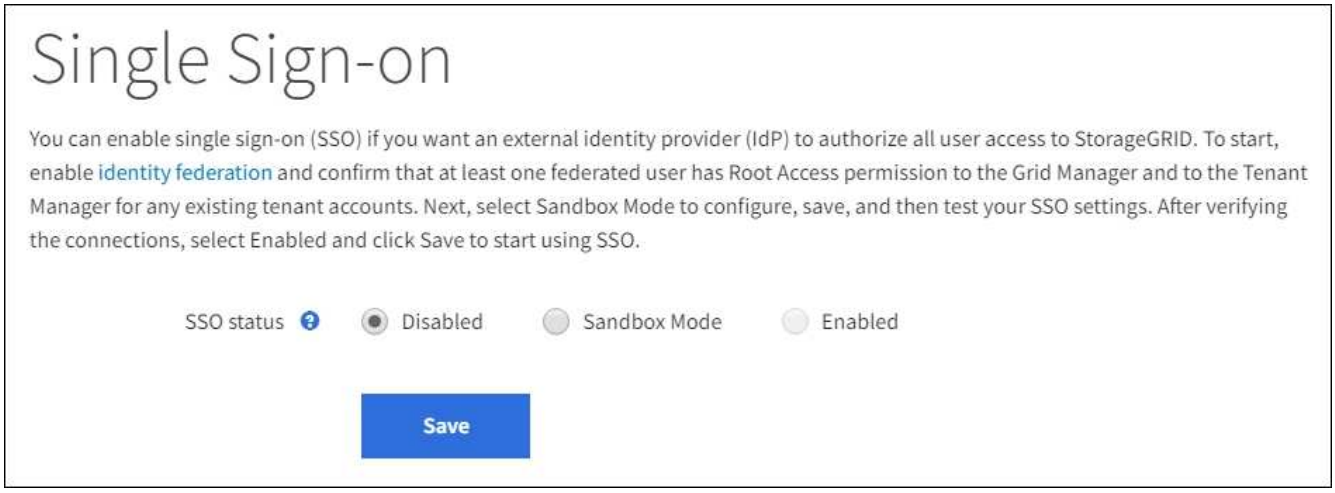
StorageGRID(서비스 공급자)와 SSO ID 공급자가 사용자 인증 요청에 대해 안전하게 통신할 수 있도록 하려면 StorageGRID에서 특정 설정을 구성해야 합니다. 그런 다음 SSO ID 공급자의 소프트웨어를 사용하여 각 관리 노드에 대한 기반 AD FS(파티 트러스트), Azure(엔터프라이즈 애플리케이션) 또는 서비스 공급자(PingFederate)를 만들어야 합니다. 마지막으로 StorageGRID로 돌아가서 SSO를 활성화해야 합니다.

sandbox 모드를 사용하면 SSO를 활성화하기 전에 이 전면과 후면을 간편하게 구성하고 모든 설정을 테스트할 수 있습니다. 샌드박스 모드를 사용하는 경우 사용자는 SSO를 사용하여 로그인할 수 없습니다.

sandbox 모드에 액세스합니다

1. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.

   단일 사인온 페이지가 나타나고 * 비활성화 * 옵션이 선택됩니다.



> SSO 상태 옵션이 나타나지 않으면 ID 공급자를 통합 ID 소스로 구성했는지 확인합니다. 을 참조하십시오 Single Sign-On 사용에 대한 요구 사항.

2. Sandbox 모드 * 를 선택합니다.

   ID 공급자 섹션이 나타납니다.

ID 공급자 세부 정보를 입력합니다

1. 드롭다운 목록에서 * SSO 유형 * 을 선택합니다.
2. 선택한 SSO 유형에 따라 ID 공급자 섹션의 필드를 작성합니다.

Active Directory를 클릭합니다

1. AD FS(Active Directory Federation Service)에 표시되는 것과 동일하게 ID 공급자에 대한 * 페더레이션 서비스 이름 * 을 입력합니다.

   > 페더레이션 서비스 이름을 찾으려면 Windows Server Manager로 이동합니다. Tools * > * AD FS Management * 를 선택합니다. 작업 메뉴에서 * 페더레이션 서비스 속성 편집 * 을 선택합니다. 두 번째 필드에 페더레이션 서비스 이름이 표시됩니다.

2. ID 공급자가 StorageGRID 요청에 대한 응답으로 SSO 구성 정보를 보낼 때 연결을 보호하는 데 사용할 TLS 인증서를 지정합니다.
   - * 운영 체제 CA 인증서 사용 *: 운영 체제에 설치된 기본 CA 인증서를 사용하여 연결을 보호합니다.
   - * 사용자 지정 CA 인증서 사용 *: 사용자 지정 CA 인증서를 사용하여 연결을 보호합니다.

     이 설정을 선택한 경우 사용자 지정 인증서의 텍스트를 복사하여 * CA 인증서 * 텍스트 상자에 붙여 넣습니다.

   - * TLS * 사용 안 함: TLS 인증서를 사용하여 연결을 보호하지 마십시오.
3. StorageGRID에 대한 * 사용 당사자 식별자 * 를 관련 당사자 섹션에서 지정합니다. 이 값은 AD FS의 각 기반 당사자 신뢰에 사용하는 이름을 제어합니다.
   - 예를 들어, 그리드에 관리 노드가 하나뿐이고 향후 관리 노드를 더 추가할 것으로 예상되지 않을 경우 'G' 또는 'StorageGRID'를 입력합니다.
   - 그리드에 두 개 이상의 관리 노드가 포함된 경우 식별자에 문자열 '[HOSTNAME]'을 포함합니다. 예: 'SG-[HOSTNAME]'. 그러면 노드의 호스트 이름을 기반으로 시스템의 각 관리 노드에 대한 기반 당사자 식별자가 표시되는 테이블이 생성됩니다.

   > StorageGRID 시스템의 각 관리 노드에 대한 신뢰할 수 있는 상대 신뢰를 만들어야 합니다. 각 관리 노드에 대한 신뢰할 수 있는 당사자 덕분에 사용자는 모든 관리 노드에 안전하게 로그인할 수 있습니다.

4. 저장 * 을 선택합니다.

   몇 초 동안 * Save * (저장 *) 버튼에 녹색 확인 표시가 나타납니다.

Azure를 지원합니다

1. ID 공급자가 StorageGRID 요청에 대한 응답으로 SSO 구성 정보를 보낼 때 연결을 보호하는 데 사용할 TLS 인증서를 지정합니다.
   - * 운영 체제 CA 인증서 사용 *: 운영 체제에 설치된 기본 CA 인증서를 사용하여 연결을 보호합니다.
   - * 사용자 지정 CA 인증서 사용 *: 사용자 지정 CA 인증서를 사용하여 연결을 보호합니다.

     이 설정을 선택한 경우 사용자 지정 인증서의 텍스트를 복사하여 * CA 인증서 * 텍스트 상자에 붙여 넣습니다.

- * TLS * 사용 안 함: TLS 인증서를 사용하여 연결을 보호하지 마십시오.

2. 엔터프라이즈 응용 프로그램 섹션에서 StorageGRID의 * 엔터프라이즈 응용 프로그램 이름 * 을 지정합니다. 이 값은 Azure AD의 각 엔터프라이즈 애플리케이션에 사용하는 이름을 제어합니다.

   - 예를 들어, 그리드에 관리 노드가 하나뿐이고 향후 관리 노드를 더 추가할 것으로 예상되지 않을 경우 'G' 또는 'StorageGRID'를 입력합니다.
   - 그리드에 두 개 이상의 관리 노드가 포함된 경우 식별자에 문자열 '[HOSTNAME]'을 포함합니다. 예: 'SG-[HOSTNAME]'. 이렇게 하면 노드의 호스트 이름을 기반으로 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션 이름을 표시하는 테이블이 생성됩니다.

   > StorageGRID 시스템의 각 관리 노드에 대해 엔터프라이즈 애플리케이션을 만들어야 합니다. 각 관리 노드에 엔터프라이즈 애플리케이션을 사용하면 사용자가 관리자 노드에 안전하게 로그인할 수 있습니다.

3. 의 단계를 따릅니다 Azure AD에서 엔터프라이즈 애플리케이션을 생성합니다 테이블에 나열된 각 관리 노드에 대해 엔터프라이즈 애플리케이션을 생성합니다.
4. Azure AD에서 각 엔터프라이즈 애플리케이션의 연합 메타데이터 URL을 복사합니다. 그런 다음 이 URL을 StorageGRID의 해당 * 페더레이션 메타데이터 URL * 필드에 붙여 넣습니다.
5. 모든 관리 노드에 대한 통합 메타데이터 URL을 복사하여 붙여넣은 후 * 저장 * 을 선택합니다.

   몇 초 동안 * Save * (저장 *) 버튼에 녹색 확인 표시가 나타납니다.

PingFederate(PingFederate)

1. ID 공급자가 StorageGRID 요청에 대한 응답으로 SSO 구성 정보를 보낼 때 연결을 보호하는 데 사용할 TLS 인증서를 지정합니다.
   - * 운영 체제 CA 인증서 사용 *: 운영 체제에 설치된 기본 CA 인증서를 사용하여 연결을 보호합니다.
   - * 사용자 지정 CA 인증서 사용 *: 사용자 지정 CA 인증서를 사용하여 연결을 보호합니다.

     이 설정을 선택한 경우 사용자 지정 인증서의 텍스트를 복사하여 * CA 인증서 * 텍스트 상자에 붙여 넣습니다.

   - * TLS * 사용 안 함: TLS 인증서를 사용하여 연결을 보호하지 마십시오.
2. 서비스 공급자(SP) 섹션에서 StorageGRID에 대한 * SP 접속 ID * 를 지정합니다. 이 값은 PingFederate의 각 SP 연결에 사용할 이름을 제어합니다.

   - 예를 들어, 그리드에 관리 노드가 하나뿐이고 향후 관리 노드를 더 추가할 것으로 예상되지 않을 경우 'G' 또는 'StorageGRID'를 입력합니다.
   - 그리드에 두 개 이상의 관리 노드가 포함된 경우 식별자에 문자열 '[HOSTNAME]'을 포함합니다. 예: 'SG-[HOSTNAME]'. 그러면 노드의 호스트 이름을 기준으로 시스템의 각 관리 노드에 대한 SP 접속 ID가 표시되는 테이블이 생성됩니다.

StorageGRID 시스템의 각 관리 노드에 대해 SP 접속을 생성해야 합니다. 각 관리 노드에 대해 SP를 연결하면 사용자가 관리자 노드에 안전하게 로그인할 수 있습니다.

3. Federation metadata URL * 필드에서 각 관리 노드에 대한 페더레이션 메타데이터 URL을 지정합니다.

   다음 형식을 사용합니다.

   ```
   https://<Federation Service Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection ID>
   ```

4. 저장 * 을 선택합니다.

   몇 초 동안 * Save * (저장 *) 버튼에 녹색 확인 표시가 나타납니다.

신뢰할 수 있는 파티 트러스트, 엔터프라이즈 애플리케이션 또는 **SP** 연결을 구성합니다

구성이 저장되면 Sandbox 모드 확인 알림이 나타납니다. 이 알림은 이제 sandbox 모드가 활성화되었음을 확인하고 개요 지침을 제공합니다.

StorageGRID는 필요한 경우 샌드박스 모드로 유지될 수 있습니다. 그러나 단일 사인온 페이지에서 * Sandbox 모드 * 를 선택하면 모든 StorageGRID 사용자에 대해 SSO가 비활성화됩니다. 로컬 사용자만 로그인할 수 있습니다.

다음 단계에 따라 사용자 트러스트(Active Directory), 엔터프라이즈 응용 프로그램(Azure) 완료 또는 SP 연결(PingFederate)을 구성합니다.

Active Directory를 클릭합니다

1. AD FS(Active Directory Federation Services)로 이동합니다.
2. StorageGRID 단일 사인온 페이지의 표에 표시된 각 기반 당사자 식별자를 사용하여 StorageGRID에 대한 하나 이상의 신뢰할 수 있는 상대 트러스트를 만듭니다.

   테이블에 표시된 각 관리 노드에 대해 하나의 신뢰를 만들어야 합니다.

   자세한 내용은 를 참조하십시오 AD FS에서 기반 당사자 트러스트를 생성합니다.

Azure를 지원합니다

1. 현재 로그인한 Admin Node의 Single Sign-On 페이지에서 SAML 메타데이터를 다운로드하고 저장할 버튼을 선택합니다.
2. 그리드에서 다른 관리 노드에 대해 다음 단계를 반복합니다.
   a. 노드에 로그인합니다.
   b. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.
   c. 해당 노드에 대한 SAML 메타데이터를 다운로드하고 저장합니다.
3. Azure Portal로 이동합니다.
4. 의 단계를 따릅니다 Azure AD에서 엔터프라이즈 애플리케이션을 생성합니다 각 관리 노드에 대한 SAML 메타데이터 파일을 해당 Azure 엔터프라이즈 애플리케이션에 업로드합니다.

PingFederate(PingFederate)

1. 현재 로그인한 Admin Node의 Single Sign-On 페이지에서 SAML 메타데이터를 다운로드하고 저장할 버튼을 선택합니다.
2. 그리드에서 다른 관리 노드에 대해 다음 단계를 반복합니다.
   a. 노드에 로그인합니다.
   b. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.
   c. 해당 노드에 대한 SAML 메타데이터를 다운로드하고 저장합니다.
3. PingFederate로 이동합니다.
4. StorageGRID에 대한 SP(서비스 공급자) 연결을 하나 이상 생성합니다. 각 관리 노드에 대해 SP 연결 ID(StorageGRID 단일 사인온 페이지의 표에 표시됨)와 해당 관리 노드에 대해 다운로드한 SAML 메타데이터를 사용합니다.

   표에 표시된 각 관리 노드에 대해 하나의 SP 접속을 생성해야 합니다.

SSO 연결을 테스트합니다

전체 StorageGRID 시스템에 대해 SSO(Single Sign-On)를 사용하기 전에 각 관리 노드에 대해 SSO(Single Sign-On)와 단일 로그아웃이 올바르게 구성되어 있는지 확인해야 합니다.

Active Directory를 클릭합니다

1. StorageGRID 단일 사인온 페이지의 Sandbox 모드 메시지에서 링크를 찾습니다.

   URL은 * 페더레이션 서비스 이름 * 필드에 입력한 값에서 파생됩니다.

   Sandbox mode

   Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

   1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
   2. Go to your identity provider's sign-on page: https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm
   3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

   When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

2. ID 공급자의 로그인 페이지에 액세스하려면 링크를 선택하거나 URL을 복사하여 브라우저에 붙여 넣으십시오.
3. SSO를 사용하여 StorageGRID에 로그인할 수 있는지 확인하려면 * 다음 사이트 중 하나에 로그인 * 을 선택하고, 기본 관리자 노드에 대한 보조 당사자 식별자를 선택한 다음 * 로그인 * 을 선택합니다.

   You are not signed in.

   ○ Sign in to this site.

   ◉ Sign in to one of the following sites:

   SG-DC1-ADM1

   Sign in

4. 통합 사용자 이름과 암호를 입력합니다.
   - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 나타납니다.

     ✔ Single sign-on authentication and logout test completed successfully.

   - SSO 작업이 실패하면 오류 메시지가 나타납니다. 문제를 해결하고 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
5. 이 단계를 반복하여 그리드의 각 관리 노드에 대한 SSO 연결을 확인합니다.

Azure를 지원합니다

1. Azure 포털의 Single Sign-On 페이지로 이동합니다.

2. 이 응용 프로그램 테스트 * 를 선택합니다.
3. 통합 사용자의 자격 증명을 입력합니다.
   - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 나타납니다.

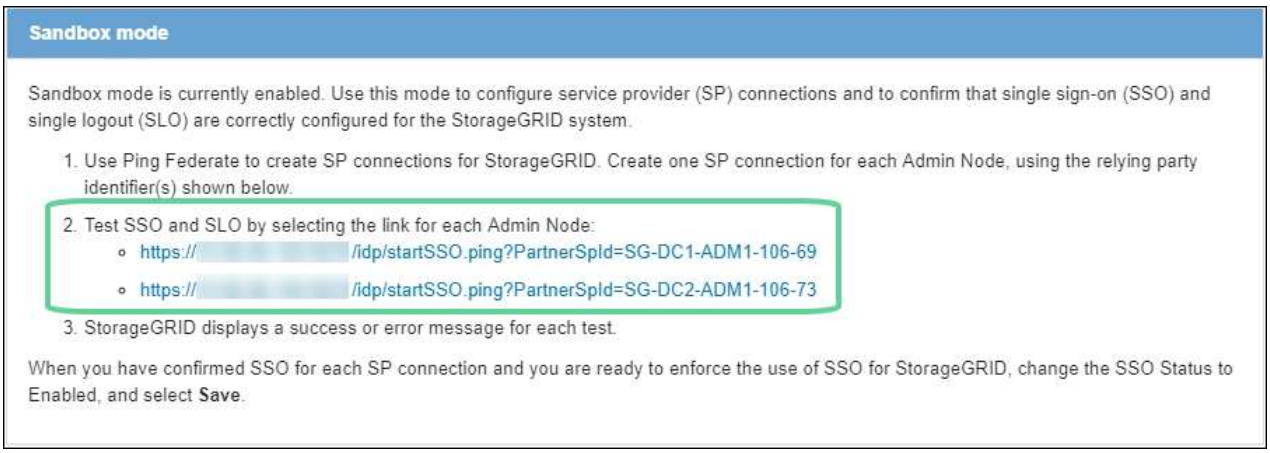
     ✔ Single sign-on authentication and logout test completed successfully.

   - SSO 작업이 실패하면 오류 메시지가 나타납니다. 문제를 해결하고 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
4. 이 단계를 반복하여 그리드의 각 관리 노드에 대한 SSO 연결을 확인합니다.

PingFederate(PingFederate)

1. StorageGRID 단일 사인온 페이지에서 Sandbox 모드 메시지의 첫 번째 링크를 선택합니다.

   링크를 한 번에 하나씩 선택하여 테스트합니다.

2. 통합 사용자의 자격 증명을 입력합니다.
   - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 나타납니다.

     ✔ Single sign-on authentication and logout test completed successfully.

   - SSO 작업이 실패하면 오류 메시지가 나타납니다. 문제를 해결하고 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
3. 다음 링크를 선택하여 그리드의 각 관리 노드에 대한 SSO 연결을 확인합니다.

   페이지 만료 메시지가 표시되면 브라우저에서 * 뒤로 * 버튼을 선택하고 자격 증명을 다시 제출하십시오.

SSO(Single Sign-On)를 활성화합니다

SSO를 사용하여 각 관리 노드에 로그인할 수 있는지 확인한 후 전체 StorageGRID 시스템에 대해 SSO를 활성화할 수 있습니다.

> SSO가 활성화된 경우 모든 사용자는 SSO를 사용하여 Grid Manager, Tenant Manager, Grid Management API 및 Tenant Management API에 액세스해야 합니다. 로컬 사용자는 더 이상 StorageGRID에 액세스할 수 없습니다.

1. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.
2. SSO 상태를 * Enabled * 로 변경합니다.
3. 저장 * 을 선택합니다.
4. 경고 메시지를 검토하고 * OK * 를 선택합니다.

   이제 SSO(Single Sign-On)가 활성화됩니다.

> Azure 포털을 사용 중이고 Azure에 액세스하는 데 사용하는 컴퓨터에서 StorageGRID에 액세스하는 경우 Azure Portal 사용자가 승인된 StorageGRID 사용자인지 확인합니다(StorageGRID로 가져온 통합 그룹의 사용자). 또는 StorageGRID에 로그인하기 전에 Azure 포털에서 로그아웃합니다.

AD FS에서 기반 당사자 트러스트를 생성합니다

AD FS(Active Directory Federation Services)를 사용하여 시스템의 각 관리 노드에 대한 기반 당사자 신뢰를 만들어야 합니다. PowerShell 명령을 사용하거나, StorageGRID에서 SAML 메타데이터를 가져오거나, 데이터를 수동으로 입력하여 의존할 수 있는 회사 트러스트를 만들 수 있습니다.

필요한 것

- StorageGRID에 대해 Single Sign-On을 구성하고 SSO 유형으로 * AD FS * 를 선택했습니다.
- * Sandbox 모드 * 는 Grid Manager의 Single Sign-On 페이지에서 선택됩니다. 을 참조하십시오 sandbox 모드를 사용합니다.
- 시스템의 각 관리 노드에 대한 정규화된 도메인 이름(또는 IP 주소)과 관련 당사자 식별자를 알고 있습니다. 이러한 값은 StorageGRID 단일 사인온 페이지의 관리 노드 세부 정보 테이블에서 찾을 수 있습니다.

> StorageGRID 시스템의 각 관리 노드에 대한 신뢰할 수 있는 상대 신뢰를 만들어야 합니다. 각 관리 노드에 대한 신뢰할 수 있는 당사자 덕분에 사용자는 모든 관리 노드에 안전하게 로그인할 수 있습니다.

- AD FS에서 기반 당사자 트러스트를 만드는 경험이 있거나 Microsoft AD FS 문서에 액세스할 수 있습니다.
- AD FS 관리 스냅인을 사용하고 있으며 사용자는 Administrators 그룹에 속해 있습니다.
- 수동으로 신뢰할 수 있는 상대 신뢰를 만드는 경우 StorageGRID 관리 인터페이스에 대해 업로드된 사용자 지정 인증서가 있거나 명령 셸에서 관리 노드에 로그인하는 방법을 알고 있어야 합니다.

이 작업에 대해

이 지침은 Windows Server 2016 AD FS에 적용됩니다. 다른 버전의 AD FS를 사용하는 경우 절차에 약간의 차이가 있을 수 있습니다. 질문이 있는 경우 Microsoft AD FS 설명서를 참조하십시오.

Windows PowerShell을 사용하여 신뢰할 수 있는 사용자 신뢰를 만듭니다

Windows PowerShell을 사용하여 하나 이상의 신뢰할 수 있는 파티 트러스트를 빠르게 만들 수 있습니다.

단계

1. Windows 시작 메뉴에서 PowerShell 아이콘을 마우스 오른쪽 버튼으로 선택하고 * 관리자 권한으로 실행 * 을 선택합니다.
2. PowerShell 명령 프롬프트에서 다음 명령을 입력합니다.

   'Add-AdfsRelyingPartyTrust - Name'Admin_Node_Identififer" - MetadataURL "<a href="https://Admin_Node_FQDN/api/saml-metadata"`" class="bare">https://<em>Admin_Node_FQDN</em>/api/saml-metadata"`

   - '*Admin_Node_Identifier*'의 경우 단일 사인온 페이지에 표시된 대로 관리 노드에 대한 기반 당사자 식별자를 입력합니다. 예: 'SG-DC1-ADM1'입니다.
   - '*Admin_Node_FQDN*'의 경우 동일한 관리 노드에 대해 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)
3. Windows Server Manager에서 * Tools * > * AD FS Management * 를 선택합니다.

   AD FS 관리 도구가 나타납니다.
4. AD FS * > * 기반 당사자 신뢰 * 를 선택합니다.

   신뢰할 수 있는 당사자 목록이 나타납니다.
5. 새로 만든 신뢰할 수 있는 상대 신뢰에 액세스 제어 정책 추가:
   a. 방금 만든 신뢰할 수 있는 상대자를 찾습니다.
   b. 트러스트를 마우스 오른쪽 단추로 클릭하고 * 액세스 제어 정책 편집 * 을 선택합니다.
   c. 액세스 제어 정책을 선택합니다.
   d. Apply * 를 선택하고 * OK * 를 선택합니다
6. 새로 생성된 신뢰할 수 있는 당사자 신탁에 클레임 발급 정책 추가:
   a. 방금 만든 신뢰할 수 있는 상대자를 찾습니다.
   b. 신뢰를 마우스 오른쪽 버튼으로 클릭하고 * 클레임 발급 정책 편집 * 을 선택합니다.
   c. 규칙 추가 * 를 선택합니다.
   d. 규칙 템플릿 선택 페이지의 목록에서 * 청구로 LDAP 속성 보내기 * 를 선택하고 * 다음 * 을 선택합니다.
   e. 규칙 구성 페이지에서 이 규칙의 표시 이름을 입력합니다.

      예를 들어, 이름 ID*에 대한 * objectGUID.

   f. 특성 저장소의 경우 * Active Directory * 를 선택합니다.
   g. 매핑 테이블의 LDAP 속성 열에 * objectGUID * 를 입력합니다.
   h. 매핑 테이블의 발신 클레임 유형 열에서 드롭다운 목록에서 * 이름 ID * 를 선택합니다.
   i. 마침 * 을 선택하고 * 확인 * 을 선택합니다.
7. 메타데이터를 성공적으로 가져왔는지 확인합니다.
   a. 신뢰할 수 있는 상대 신뢰를 마우스 오른쪽 단추로 클릭하여 속성을 엽니다.

b. Endpoints *, * Identifiers * 및 * Signature * 탭의 필드가 채워져 있는지 확인합니다.

   메타데이터가 누락된 경우 페더레이션 메타데이터 주소가 올바른지 확인하거나 값을 수동으로 입력합니다.

8. 이 단계를 반복하여 StorageGRID 시스템의 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 구성합니다.
9. 작업을 마치면 StorageGRID로 돌아가 모든 신뢰할 수 있는 상대 트러스트를 테스트하여 올바르게 구성되었는지 확인합니다. 을 참조하십시오 Sandbox 모드를 사용합니다 를 참조하십시오.

페더레이션 메타데이터를 가져와 사용 상대 신뢰를 만듭니다

각 관리 노드에 대한 SAML 메타데이터에 액세스하여 각 의존자 신뢰의 값을 가져올 수 있습니다.

단계

1. Windows Server Manager에서 * Tools * 를 선택한 다음 * AD FS Management * 를 선택합니다.
2. 작업에서 * 신뢰할 수 있는 당사자 신뢰 추가 * 를 선택합니다.
3. 시작 페이지에서 * 클레임 인식 * 을 선택하고 * 시작 * 을 선택합니다.
4. 온라인 또는 로컬 네트워크에 게시된 의존자에 대한 데이터 가져오기 * 를 선택합니다.
5. Federation 메타데이터 주소(호스트 이름 또는 URL) * 에 이 관리 노드에 대한 SAML 메타데이터의 위치를 입력합니다.

   "https://*Admin_Node_FQDN*/api/saml-metadata`

   '*Admin_Node_FQDN*'의 경우 동일한 관리 노드에 대해 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)

6. 신뢰할 수 있는 당사자 신뢰 마법사를 완료하고 신뢰할 수 있는 상대 신뢰를 저장한 다음 마법사를 닫습니다.

   표시 이름을 입력할 때 그리드 관리자의 단일 사인온 페이지에 나타나는 것과 동일하게 관리 노드에 대한 기반 당사자 식별자를 사용합니다. 예: 'SG-DC1-ADM1'입니다.

7. 청구 규칙 추가:
   a. 신뢰를 마우스 오른쪽 버튼으로 클릭하고 * 클레임 발급 정책 편집 * 을 선택합니다.
   b. 규칙 추가 * 선택:
   c. 규칙 템플릿 선택 페이지의 목록에서 * 청구로 LDAP 속성 보내기 * 를 선택하고 * 다음 * 을 선택합니다.
   d. 규칙 구성 페이지에서 이 규칙의 표시 이름을 입력합니다.

      예를 들어, 이름 ID*에 대한 * objectGUID.

   e. 특성 저장소의 경우 * Active Directory * 를 선택합니다.
   f. 매핑 테이블의 LDAP 속성 열에 * objectGUID * 를 입력합니다.
   g. 매핑 테이블의 발신 클레임 유형 열에서 드롭다운 목록에서 * 이름 ID * 를 선택합니다.
   h. 마침 * 을 선택하고 * 확인 * 을 선택합니다.
8. 메타데이터를 성공적으로 가져왔는지 확인합니다.

a. 신뢰할 수 있는 상대 신뢰를 마우스 오른쪽 단추로 클릭하여 속성을 엽니다.

b. Endpoints *, * Identifiers * 및 * Signature * 탭의 필드가 채워져 있는지 확인합니다.

   메타데이터가 누락된 경우 페더레이션 메타데이터 주소가 올바른지 확인하거나 값을 수동으로 입력합니다.

9. 이 단계를 반복하여 StorageGRID 시스템의 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 구성합니다.
10. 작업을 마치면 StorageGRID로 돌아가 모든 신뢰할 수 있는 상대 트러스트를 테스트하여 올바르게 구성되었는지 확인합니다. 을 참조하십시오 Sandbox 모드를 사용합니다 를 참조하십시오.

수동으로 신뢰할 수 있는 상대 신뢰를 만듭니다

의존 파트 트러스트의 데이터를 불러오지 않도록 선택하면 값을 직접 입력할 수 있습니다.

단계

1. Windows Server Manager에서 * Tools * 를 선택한 다음 * AD FS Management * 를 선택합니다.
2. 작업에서 * 신뢰할 수 있는 당사자 신뢰 추가 * 를 선택합니다.
3. 시작 페이지에서 * 클레임 인식 * 을 선택하고 * 시작 * 을 선택합니다.
4. [의지하는 자에 대한 데이터 입력]을 선택하고 * [다음]을 선택합니다.
5. 신뢰할 수 있는 당사자 신뢰 마법사를 완료합니다.

   a. 이 관리 노드의 표시 이름을 입력합니다.

      일관성을 위해 그리드 관리자의 단일 사인온 페이지에 표시되는 것과 동일하게 관리자 노드에 대한 기반 당사자 식별자를 사용합니다. 예: 'SG-DC1-ADM1'입니다.

   b. 선택적 토큰 암호화 인증서를 구성하려면 단계를 건너뜁니다.

   c. URL 구성 페이지에서 SAML 2.0 WebSSO 프로토콜 * 지원 활성화 확인란을 선택합니다.

   d. 관리 노드에 대한 SAML 서비스 끝점 URL을 입력합니다.

      "https://*Admin_Node_FQDN*/api/saml-response`

      '*Admin_Node_FQDN*'에 대해 관리자 노드의 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)

   e. 식별자 구성 페이지에서 동일한 관리 노드에 대한 기반 당사자 식별자를 지정합니다.

      '*Admin_Node_Identifier*'

      '*Admin_Node_Identifier*'의 경우 단일 사인온 페이지에 표시된 대로 관리 노드에 대한 기반 당사자 식별자를 입력합니다. 예: 'SG-DC1-ADM1'입니다.

   f. 설정을 검토하고 신뢰할 수 있는 상대 신뢰를 저장한 다음 마법사를 닫습니다.

      청구 발급 정책 편집 대화 상자가 나타납니다.

      > 대화 상자가 나타나지 않으면 트러스트를 마우스 오른쪽 단추로 클릭하고 * 클레임 발급 정책 편집 * 을 선택합니다.

6. 클레임 규칙 마법사를 시작하려면 * 규칙 추가 * 를 선택합니다.
   a. 규칙 템플릿 선택 페이지의 목록에서 * 청구로 LDAP 속성 보내기 * 를 선택하고 * 다음 * 을 선택합니다.
   b. 규칙 구성 페이지에서 이 규칙의 표시 이름을 입력합니다.

      예를 들어, 이름 ID*에 대한 * objectGUID.

   c. 특성 저장소의 경우 * Active Directory * 를 선택합니다.
   d. 매핑 테이블의 LDAP 속성 열에 * objectGUID * 를 입력합니다.
   e. 매핑 테이블의 발신 클레임 유형 열에서 드롭다운 목록에서 * 이름 ID * 를 선택합니다.
   f. 마침 * 을 선택하고 * 확인 * 을 선택합니다.
7. 신뢰할 수 있는 상대 신뢰를 마우스 오른쪽 단추로 클릭하여 속성을 엽니다.
8. 엔드포인트 * 탭에서 단일 로그아웃(SLO)에 대한 엔드포인트를 구성합니다.
   a. SAML 추가 * 를 선택합니다.
   b. Endpoint Type * > * SAML Logout * 을 선택합니다.
   c. Binding * > * Redirect * 를 선택합니다.
   d. 신뢰할 수 있는 URL * 필드에 이 관리 노드에서 단일 로그아웃(SLO)에 사용되는 URL을 입력합니다.

      "https://*Admin_Node_FQDN*/api/saml-logout`

   '*Admin_Node_FQDN*'에 대해 관리자 노드의 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)

   a. OK * 를 선택합니다.
9. 서명* 탭에서 이 신뢰할 수 있는 당사자 트러스트의 서명 인증서를 지정합니다.
   a. 사용자 지정 인증서 추가:
      - StorageGRID에 업로드한 사용자 지정 관리 인증서가 있는 경우 해당 인증서를 선택합니다.
      - 사용자 정의 인증서가 없는 경우 Admin Node에 로그인하여 Admin Node의 '/var/local/mgmt-api' 디렉토리로 이동한 후 'custom-server.crt' 인증서 파일을 추가합니다.
        - 참고: * 관리 노드의 기본 인증서('server.crt')를 사용하는 것은 권장되지 않습니다. 관리자 노드에 장애가 발생하면 노드를 복구할 때 기본 인증서가 다시 생성되고, 신뢰할 수 있는 상대 트러스트를 업데이트해야 합니다.
   b. Apply * 를 선택하고 * OK * 를 선택합니다.

      종속된 당사자 속성이 저장되고 닫힙니다.
10. 이 단계를 반복하여 StorageGRID 시스템의 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 구성합니다.
11. 작업을 마치면 StorageGRID로 돌아가 모든 신뢰할 수 있는 상대 트러스트를 테스트하여 올바르게 구성되었는지 확인합니다. 을 참조하십시오 sandbox 모드를 사용합니다 를 참조하십시오.

Azure AD를 사용하여 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 생성합니다.

필요한 것

- StorageGRID에 대한 SSO(Single Sign-On) 구성을 시작했으며 SSO 유형으로 * Azure * 를 선택했습니다.
- * Sandbox 모드 * 는 Grid Manager의 Single Sign-On 페이지에서 선택됩니다. 을 참조하십시오 sandbox 모드를 사용합니다.
- 시스템의 각 관리 노드에 대해 * 엔터프라이즈 애플리케이션 이름 * 이 있습니다. 이러한 값은 StorageGRID 단일 사인온 페이지의 관리 노드 세부 정보 테이블에서 복사할 수 있습니다.

> StorageGRID 시스템의 각 관리 노드에 대해 엔터프라이즈 애플리케이션을 만들어야 합니다. 각 관리 노드에 엔터프라이즈 애플리케이션을 사용하면 사용자가 관리자 노드에 안전하게 로그인할 수 있습니다.

- Azure Active Directory에서 엔터프라이즈 응용 프로그램을 만든 경험이 있습니다.
- Azure 계정에 활성 구독이 있습니다.
- Azure 계정에는 글로벌 관리자, 클라우드 응용 프로그램 관리자, 응용 프로그램 관리자 또는 서비스 보안 주체의 소유자인 다음 역할 중 하나가 있습니다.

Azure AD에 액세스합니다

1. 에 로그인합니다 "Azure 포털".
2. 로 이동합니다 "Azure Active Directory를 클릭합니다".
3. 를 선택합니다 "엔터프라이즈 애플리케이션".

엔터프라이즈 애플리케이션을 생성하고 **StorageGRID SSO** 구성을 저장합니다

StorageGRID에서 Azure에 대한 SSO 구성을 저장하려면 Azure를 사용하여 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 만들어야 합니다. Azure에서 페더레이션 메타데이터 URL을 복사하여 StorageGRID 단일 사인온 페이지의 해당 * 페더레이션 메타데이터 URL * 필드에 붙여 넣습니다.

1. 각 관리 노드에 대해 다음 단계를 반복합니다.
   a. Azure Enterprise 응용 프로그램 창에서 * 새 응용 프로그램 * 을 선택합니다.
   b. 사용자 정의 응용 프로그램 만들기 * 를 선택합니다.
   c. 이름으로 StorageGRID 단일 사인온 페이지의 관리 노드 세부 정보 테이블에서 복사한 * 엔터프라이즈 응용 프로그램 이름 * 을 입력합니다.
   d. 갤러리에서 찾을 수 없는 * 다른 응용 프로그램 통합(갤러리 외) * 라디오 버튼을 선택된 상태로 둡니다.
   e. Create * 를 선택합니다.
   f. 2에서 * 시작하기 * 링크를 선택합니다. Single Sign On * 상자를 설정하거나 왼쪽 여백에서 * Single Sign-On * 링크를 선택합니다.
   g. SAML * 상자를 선택합니다.
   h. 앱 페더레이션 메타데이터 URL * 을 복사합니다. * 3단계 SAML 서명 인증서 * 에서 찾을 수 있습니다.
   i. StorageGRID 단일 사인온 페이지로 이동하여 사용한 * 엔터프라이즈 응용 프로그램 이름 * 에 해당하는 * 통합

메타데이터 URL * 필드에 URL을 붙여 넣습니다.

2. 각 관리 노드에 대한 페더레이션 메타데이터 URL을 붙여 넣고 SSO 구성에 필요한 다른 모든 변경 사항을 적용한 후 StorageGRID 단일 사인온 페이지에서 * 저장 * 을 선택합니다.

모든 관리 노드에 대해 **SAML** 메타데이터를 다운로드합니다

SSO 구성을 저장한 후 StorageGRID 시스템의 각 관리 노드에 대해 SAML 메타데이터 파일을 다운로드할 수 있습니다.

각 관리 노드에 대해 다음 단계를 반복합니다.

1. 관리자 노드에서 StorageGRID에 로그인합니다.
2. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.
3. 버튼을 선택하여 해당 Admin Node에 대한 SAML 메타데이터를 다운로드합니다.
4. Azure AD에 업로드할 파일을 저장합니다.

각 엔터프라이즈 애플리케이션에 **SAML** 메타데이터를 업로드합니다

각 StorageGRID 관리 노드에 대해 SAML 메타데이터 파일을 다운로드한 후 Azure AD에서 다음 단계를 수행하십시오.

1. Azure 포털로 돌아갑니다.
2. 각 엔터프라이즈 애플리케이션에 대해 다음 단계를 반복합니다.

> 이전에 목록에 추가한 응용 프로그램을 보려면 엔터프라이즈 응용 프로그램 페이지를 새로 고쳐야 할 수 있습니다.

   a. 엔터프라이즈 애플리케이션의 속성 페이지로 이동합니다.
   b. 할당 필요 * 를 * 아니오 * 로 설정합니다(할당을 별도로 구성하지 않는 경우).
   c. Single Sign-On 페이지로 이동합니다.
   d. SAML 구성을 완료합니다.
   e. Upload metadata file * 버튼을 선택하고 해당 Admin Node에 대해 다운로드한 SAML 메타데이터 파일을 선택합니다.
   f. 파일을 로드한 후 * Save * 를 선택하고 * X * 를 선택하여 창을 닫습니다. SAML로 단일 사인온 설정 페이지로 돌아갑니다.

3. 의 단계를 따릅니다 sandbox 모드를 사용합니다 각 응용 프로그램을 테스트합니다.

PingFederate에서 서비스 공급자**(SP)** 연결을 생성합니다

PingFederate를 사용하여 시스템의 각 관리 노드에 대한 서비스 공급자(SP) 연결을 만듭니다. 프로세스 속도를 높이기 위해 StorageGRID에서 SAML 메타데이터를 가져옵니다.

필요한 것

- StorageGRID에 대한 SSO(Single Sign-On)를 구성하고 SSO 유형으로 * Ping 남부연합을 선택했습니다.
- * Sandbox 모드 * 는 Grid Manager의 Single Sign-On 페이지에서 선택됩니다. 을 참조하십시오 sandbox 모드를 사용합니다.

- 시스템의 각 관리 노드에 대해 * SP 접속 ID * 가 있습니다. 이러한 값은 StorageGRID 단일 사인온 페이지의 관리 노드 세부 정보 테이블에서 찾을 수 있습니다.
- 시스템의 각 관리 노드에 대해 * SAML 메타데이터 * 를 다운로드했습니다.
- PingFederate Server에서 SP 연결을 생성하는 경험이 있습니다.
- 을(를) 보유하고 있습니다https://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html["관리자 참조 안내서"^] PingFederate Server의 경우 PingFederate 설명서는 자세한 단계별 지침과 설명을 제공합니다.
- PingFederate Server에 대한 관리자 권한이 있습니다.

이 작업에 대해

이 지침은 PingFederate Server 버전 10.3을 StorageGRID의 SSO 공급자로 구성하는 방법을 요약합니다. 다른 버전의 PingFederate를 사용하는 경우 이 지침을 조정해야 할 수 있습니다. 릴리스에 대한 자세한 지침은 PingFederate Server 설명서를 참조하십시오.

PingFederate에서 필수 구성 요소를 완료합니다

StorageGRID에 사용할 SP 연결을 생성하려면 PingFederate에서 사전 요구 작업을 완료해야 합니다. SP 접속을 구성할 때 이러한 사전 요구 사항의 정보를 사용합니다.

데이터 저장소 생성

아직 연결하지 않은 경우 데이터 저장소를 생성하여 PingFederate를 AD FS LDAP 서버에 연결합니다. 사용 시 사용한 값을 사용합니다 ID 페더레이션을 구성하는 중입니다 StorageGRID에서

- * 유형 *: 디렉토리(LDAP)
- * LDAP 유형 *: Active Directory
- * 바이너리 특성 이름 *: LDAP 바이너리 특성 탭의 * objectGUID * 를 그림과 같이 정확하게 입력합니다.

암호 자격 증명 유효성 검사기 **[[**암호 유효성 검사기**]]** 만들기

아직 설치하지 않은 경우 암호 자격 증명 유효성 검사기를 만듭니다.

- * 유형 *: LDAP 사용자 이름 암호 자격 증명 검사기
- * 데이터 저장소 *: 만든 데이터 저장소를 선택합니다.
- * 검색 기준 *: LDAP의 정보를 입력합니다(예: DC=SAML, DC=SGWs).
- * 검색 필터 *: sAMAccountName=${username}
- * 범위 *: 하위 트리

IDP 어댑터 인스턴스 만들기

아직 IDP 어댑터 인스턴스를 만들지 않은 경우 생성합니다.

1. 인증 * > * 통합 * > * IDP 어댑터 * 로 이동합니다.
2. 새 인스턴스 만들기 * 를 선택합니다.
3. 유형 탭에서 * HTML 양식 IDP 어댑터 * 를 선택합니다.

4. IDP Adapter 탭에서 * Add a new row to 'Credential Validators' * 를 선택합니다.
5. 를 선택합니다 암호 자격 증명 유효성 검사기가 있습니다 을(를) 만들었습니다.
6. 어댑터 특성 탭에서 * 가명 * 에 대한 * 사용자 이름 * 속성을 선택합니다.
7. 저장 * 을 선택합니다.

서명 인증서 만들기 또는 가져오기

서명 인증서를 아직 만들지 않은 경우 서명 인증서를 만들거나 가져옵니다.

1. 보안 * > * 서명 및 암호 해독 키 및 인증서 * 로 이동합니다.
2. 서명 인증서를 만들거나 가져옵니다.

PingFederate에서 **SP** 접속을 생성합니다

PingFederate에서 SP 연결을 생성할 때 StorageGRID에서 다운로드한 SAML 메타데이터를 관리자 노드에 대해 가져옵니다. 메타데이터 파일에는 필요한 많은 특정 값이 들어 있습니다.

> 사용자가 모든 노드에 안전하게 로그인할 수 있도록 StorageGRID 시스템의 각 관리 노드에 대해 SP 접속을 생성해야 합니다. 이 지침에 따라 첫 번째 SP 접속을 생성합니다. 그런 다음 로 이동합니다 추가 SP 접속을 생성합니다 필요한 추가 연결을 생성합니다.

SP 접속 유형을 선택합니다

1. 응용 프로그램 * > * 통합 * > * SP 연결 * 으로 이동합니다.
2. Create Connection * 을 선택합니다.
3. 이 연결에 템플릿을 사용하지 않음 * 을 선택합니다.
4. 프로토콜로 * Browser SSO Profiles * 및 * SAML 2.0 * 을 선택합니다.

SP 메타데이터를 가져옵니다

1. 메타데이터 가져오기 탭에서 * 파일 * 을 선택합니다.
2. 관리자 노드의 StorageGRID Single Sign-On 페이지에서 다운로드한 SAML 메타데이터 파일을 선택합니다.
3. 메타데이터 요약 및 일반 정보 탭의 정보를 검토합니다.

   파트너의 엔티티 ID와 연결 이름은 StorageGRID SP 연결 ID로 설정됩니다. (예: 10.96.105.200-DC1-ADM1-105-200). 기본 URL은 StorageGRID 관리 노드의 IP입니다.

4. 다음 * 을 선택합니다.

IDP 브라우저 **SSO**를 구성합니다

1. Browser SSO(브라우저 SSO) 탭에서 * Configure Browser SSO *(브라우저 SSO * 구성) 를 선택합니다.
2. SAML 프로필 탭에서 * SP 시작 SSO *, * SP 초기 SLO *, * IDP 시작 SSO * 및 * IDP 시작 SLO * 옵션을 선택합니다.
3. 다음 * 을 선택합니다.

4. 어설션 수명 탭에서 변경하지 않습니다.
5. 어설션 작성 탭에서 * 어설션 작성 설정 * 을 선택합니다.
   a. ID 매핑 탭에서 * 표준 * 을 선택합니다.
   b. [속성 계약] 탭에서 [속성 계약] 및 가져온 지정되지 않은 이름 형식으로 * SAML_subject * 를 사용합니다.
6. 계약 연장 에서 * 삭제 * 를 선택하여 사용되지 않는 'urn:OID'를 제거합니다.

어댑터 인스턴스를 매핑합니다

1. 인증 소스 매핑 탭에서 * 새 어댑터 인스턴스 매핑 * 을 선택합니다.
2. 어댑터 인스턴스 탭에서 를 선택합니다 어댑터 인스턴스 을(를) 만들었습니다.
3. 매핑 방법 탭에서 * 데이터 저장소에서 추가 특성 검색 * 을 선택합니다.
4. 특성 원본 및 사용자 조회 탭에서 * 특성 원본 추가 * 를 선택합니다.
5. Data Store(데이터 저장소) 탭에서 설명을 입력하고 를 선택합니다 데이터 저장소 을(를) 추가했습니다.
6. LDAP 디렉토리 검색 탭에서 다음을 수행합니다.
   - 기본 DN * 을 입력합니다. 이 값은 LDAP 서버에 대해 StorageGRID에 입력한 값과 정확히 일치해야 합니다.
   - 검색 범위 에서 * 하위 트리 * 를 선택합니다.
   - 루트 개체 클래스의 경우 * objectGUID * 특성을 검색하여 추가합니다.
7. LDAP 바이너리 특성 인코딩 형식 탭에서 * objectGUID * 특성에 대해 * Base64 * 를 선택합니다.
8. LDAP 필터 탭에서 * sAMAccountName=${username} * 을 입력합니다.
9. [속성 계약 이행] 탭의 [소스] 드롭다운에서 * LDAP(속성) * 를 선택하고 값 드롭다운에서 * objectGUID * 를 선택합니다.
10. 특성 소스를 검토한 후 저장합니다.
11. Failsave 특성 소스 탭에서 * SSO 트랜잭션 중단 * 을 선택합니다.
12. 요약을 검토하고 * 완료 * 를 선택합니다.
13. 완료 * 를 선택합니다.

프로토콜 설정을 구성합니다

1. SP Connection * > * Browser SSO * > * Protocol Settings * 탭에서 * Configure Protocol Settings * 를 선택합니다.
2. 어설션 소비자 서비스 URL 탭에서 StorageGRID SAML 메타데이터에서 가져온 기본값을 그대로 사용합니다(바인딩 시 * POST *, 끝점 URL의 경우 '/API/SAML-RESPONSE').
3. SLO 서비스 URL 탭에서 StorageGRID SAML 메타데이터에서 가져온 기본값을 그대로 사용합니다(바인딩 시 * redirect *, 끝점 URL의 경우 '/api/SAML-logout').
4. 허용 가능한 SAML 바인딩 탭에서 * Artifact * 및 * SOAP * 를 선택 취소합니다. POST * 및 * REDIRECT * 만 필요합니다.
5. 서명 정책 탭에서 * Authn 요청 서명 필요 * 및 * 항상 어설션 * 확인란을 선택된 상태로 둡니다.
6. 암호화 정책 탭에서 * 없음 * 을 선택합니다.
7. 요약을 검토하고 * Done * (완료 *)을 선택하여 프로토콜 설정을 저장합니다.

8. 요약을 검토하고 * 완료 * 를 선택하여 브라우저 SSO 설정을 저장합니다.

자격 증명을 구성합니다

1. SP 연결 탭에서 * 자격 증명 * 을 선택합니다.
2. 자격 증명 탭에서 * 자격 증명 구성 * 을 선택합니다.
3. 를 선택합니다 서명 인증서 만들거나 가져왔습니다.
4. 다음 * 을 선택하여 * 서명 확인 설정 관리 * 로 이동합니다.
   a. 보안 모델 탭에서 * 앵커 지정되지 않음 * 을 선택합니다.
   b. 서명 확인 인증서 탭에서 StorageGRID SAML 메타데이터에서 가져온 서명 인증서 정보를 검토합니다.
5. 요약 화면을 검토하고 * 저장 * 을 선택하여 SP 접속을 저장합니다.

추가 **SP** 접속을 생성합니다

첫 번째 SP 접속을 복제하여 그리드의 각 관리 노드에 필요한 SP 접속을 생성할 수 있습니다. 각 복사본에 대한 새 메타데이터를 업로드합니다.

> 파트너의 엔티티 ID, 기본 URL, 연결 ID, 연결 이름, 서명 확인을 제외하고 서로 다른 관리 노드의 SP 연결은 동일한 설정을 사용합니다. SLO 응답 URL이 있습니다.

1. 각 추가 관리 노드에 대한 초기 SP 연결의 복제본을 생성하려면 * Action * > * Copy * 를 선택합니다.
2. 복사본의 연결 ID와 연결 이름을 입력하고 * 저장 * 을 선택합니다.
3. 관리 노드에 해당하는 메타데이터 파일을 선택합니다.
   a. 작업 * > * 메타데이터 업데이트 * 를 선택합니다.
   b. 파일 선택 * 을 선택하고 메타데이터를 업로드합니다.
   c. 다음 * 을 선택합니다.
   d. 저장 * 을 선택합니다.
4. 미사용 속성으로 인한 오류를 해결합니다.
   a. 새 연결을 선택합니다.
   b. Configure Browser SSO > Configure Assertion Creation > Attribute Contract * 를 선택합니다.
   c. urn:OID*에 대한 항목을 삭제합니다.
   d. 저장 * 을 선택합니다.

SSO(Single Sign-On)를 비활성화합니다

이 기능을 더 이상 사용하지 않으려면 SSO(Single Sign-On)를 사용하지 않도록 설정할 수 있습니다. ID 페더레이션을 비활성화하려면 먼저 SSO(Single Sign-On)를 비활성화해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

- 특정 액세스 권한이 있습니다.

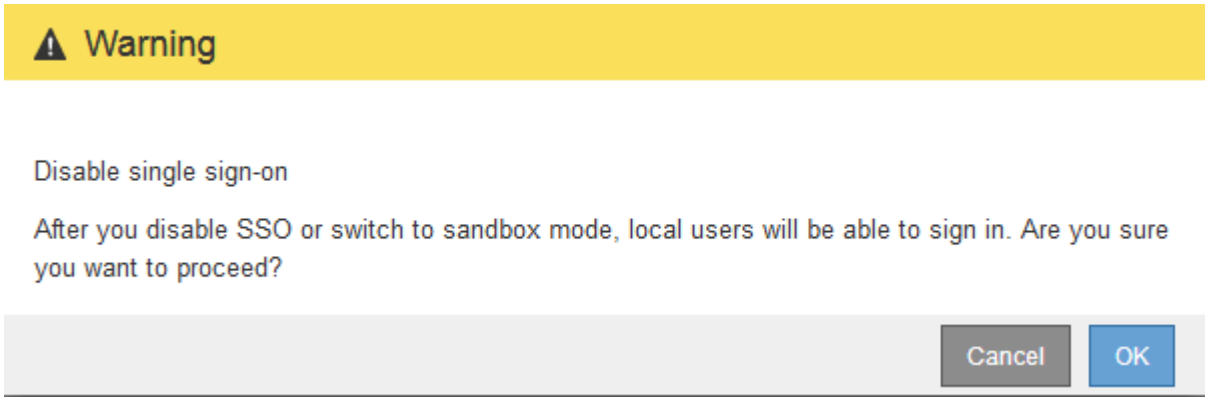
단계

1. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.

   단일 사인온 페이지가 나타납니다.

2. 사용 안 함 * 옵션을 선택합니다.
3. 저장 * 을 선택합니다.

   로컬 사용자가 로그인할 수 있음을 나타내는 경고 메시지가 나타납니다.



4. OK * 를 선택합니다.

   다음에 StorageGRID에 로그인할 때 StorageGRID 로그인 페이지가 나타나고 로컬 또는 통합 StorageGRID 사용자의 사용자 이름과 암호를 입력해야 합니다.

하나의 관리 노드에 대해 **SSO(Single Sign-On)**를 일시적으로 비활성화 및 다시 활성화합니다

SSO(Single Sign-On) 시스템이 다운되면 Grid Manager에 로그인하지 못할 수 있습니다. 이 경우 한 관리 노드에 대해 SSO를 일시적으로 비활성화 및 다시 활성화할 수 있습니다. SSO를 사용하지 않도록 설정한 다음 다시 사용하도록 설정하려면 노드의 명령 셸에 액세스해야 합니다.

필요한 것

- 특정 액세스 권한이 있습니다.
- "passwords.txt" 파일이 있습니다.
- 로컬 루트 사용자의 암호를 알고 있습니다.

이 작업에 대해

한 관리 노드에 대해 SSO를 비활성화한 후 그리드 관리자에 로컬 루트 사용자로 로그인할 수 있습니다. StorageGRID 시스템을 보호하려면 로그아웃하는 즉시 노드의 명령 셸을 사용하여 관리자 노드에서 SSO를 다시 활성화해야 합니다.

> 한 관리 노드에 대해 SSO를 비활성화해도 그리드의 다른 관리 노드에 대한 SSO 설정에는 영향을 주지 않습니다. Grid Manager의 Single Sign-On 페이지에 있는 * Enable SSO * (SSO * 활성화) 확인란은 선택된 상태로 남아 있으며, 기존 SSO 설정은 모두 업데이트하지 않는 한 유지됩니다.

단계

1. 관리자 노드에 로그인:
   a. ssh admin@Admin_Node_IP' 명령어를 입력한다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. dispable-SAML 명령을 실행합니다

   명령이 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

3. SSO를 비활성화할지 확인합니다.

   노드에서 SSO(Single Sign-On)가 비활성화되었다는 메시지가 표시됩니다.

4. 웹 브라우저에서 동일한 관리 노드의 그리드 관리자에 액세스합니다.

   이제 SSO가 비활성화되어 Grid Manager 로그인 페이지가 표시됩니다.

5. 사용자 이름 루트와 로컬 루트 사용자 암호를 사용하여 로그인합니다.
6. SSO 구성을 수정해야 하므로 SSO를 일시적으로 비활성화한 경우:
   a. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.
   b. 잘못된 또는 오래된 SSO 설정을 변경합니다.
   c. 저장 * 을 선택합니다.

      단일 사인온 페이지에서 * 저장 * 을 선택하면 전체 그리드에 대한 SSO가 자동으로 다시 활성화됩니다.

7. 다른 이유로 인해 그리드 관리자에 액세스해야 하기 때문에 SSO를 일시적으로 비활성화한 경우:

   a. 수행해야 할 작업 또는 작업을 모두 수행합니다.
   b. 로그아웃 * 을 선택하고 그리드 관리자를 닫습니다.
   c. 관리자 노드에서 SSO를 다시 활성화합니다. 다음 단계 중 하나를 수행할 수 있습니다.

      - Enable-SAML 명령을 실행합니다

        명령이 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

      SSO를 활성화할지 확인합니다.

   노드에서 Single Sign-On이 설정되었음을 나타내는 메시지가 표시됩니다.

   - 그리드 노드를 다시 부팅한다
8. 웹 브라우저에서 동일한 관리 노드에서 그리드 관리자에 액세스합니다.
9. StorageGRID 로그인 페이지가 나타나고 그리드 관리자에 액세스하려면 SSO 자격 증명을 입력해야 합니다.

보안 설정을 관리합니다

인증서를 관리합니다

보안 인증서 정보

보안 인증서는 StorageGRID 구성 요소와 StorageGRID 구성 요소 및 외부 시스템 간에 안전하고 신뢰할 수 있는 연결을 만드는 데 사용되는 작은 데이터 파일입니다.

StorageGRID는 두 가지 유형의 보안 인증서를 사용합니다.

- HTTPS 연결을 사용할 때는 * 서버 인증서 * 가 필요합니다. 서버 인증서는 클라이언트와 서버 간의 보안 연결을 설정하고, 클라이언트에 대한 서버 ID를 인증하고, 데이터에 대한 보안 통신 경로를 제공하는 데 사용됩니다. 서버와 클라이언트마다 인증서의 복사본이 있습니다.
- * 클라이언트 인증서 * 는 서버에 대한 클라이언트 또는 사용자 ID를 인증하여 암호만 사용하는 것보다 더 안전한 인증을 제공합니다. 클라이언트 인증서는 데이터를 암호화하지 않습니다.

클라이언트가 HTTPS를 사용하여 서버에 연결하면 서버는 공개 키가 포함된 서버 인증서로 응답합니다. 클라이언트는 서버 서명을 인증서 사본의 서명과 비교하여 이 인증서를 확인합니다. 서명이 일치하면 클라이언트는 동일한 공개 키를 사용하여 서버와 세션을 시작합니다.

StorageGRID는 로드 밸런서 끝점과 같은 일부 연결에 대한 서버 또는 CloudMirror 복제 서비스와 같은 다른 연결에 대한 클라이언트로 작동합니다.

- 기본 그리드 CA 인증서 *

StorageGRID에는 시스템 설치 중에 내부 그리드 CA 인증서를 생성하는 내장 CA(인증 기관)가 포함되어 있습니다. 그리드 CA 인증서는 기본적으로 내부 StorageGRID 트래픽을 보호하기 위해 사용됩니다. 외부 CA(인증 기관)는 조직의 정보 보안 정책을 완벽하게 준수하는 사용자 지정 인증서를 발급할 수 있습니다. 비프로덕션 환경에 대해 Grid CA 인증서를 사용할 수 있지만 프로덕션 환경에 가장 적합한 방법은 외부 인증 기관에서 서명한 사용자 지정 인증서를 사용하는 것입니다. 인증서가 없는 비보안 연결도 지원되지만 권장되지 않습니다.

- 사용자 지정 CA 인증서는 내부 인증서를 제거하지 않지만 사용자 지정 인증서는 서버 연결을 확인하기 위해 지정된 인증서여야 합니다.
- 모든 사용자 지정 인증서는 을 충족해야 합니다 시스템 강화 지침 서버 인증서용.
- StorageGRID는 CA의 인증서를 단일 파일(CA 인증서 번들이라고 함)로 번들링하는 것을 지원합니다.

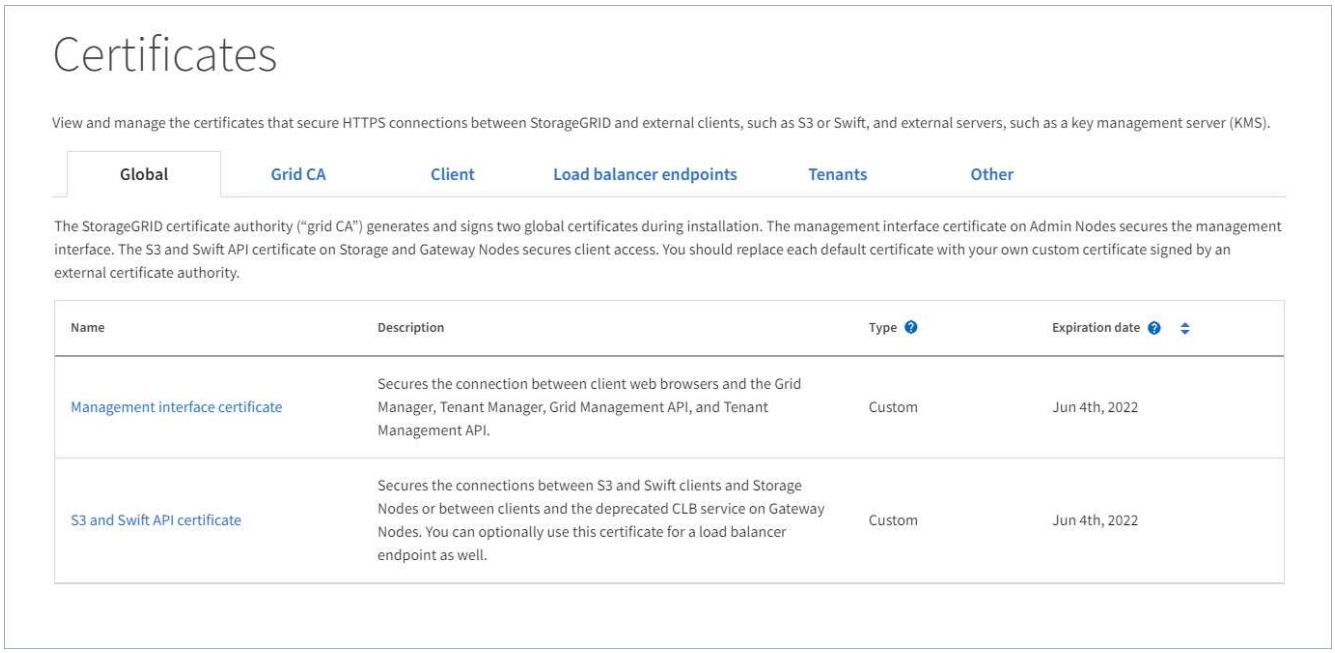
> StorageGRID에는 모든 그리드에서 동일한 운영 체제 CA 인증서도 포함됩니다. 프로덕션 환경에서는 운영 체제 CA 인증서 대신 외부 인증 기관에서 서명한 사용자 지정 인증서를 지정해야 합니다.

서버 및 클라이언트 인증서 유형의 변형은 여러 가지 방법으로 구현됩니다. 시스템을 구성하기 전에 특정 StorageGRID 구성에 필요한 모든 인증서를 준비해야 합니다.

보안 인증서에 액세스합니다

각 인증서의 구성 워크플로 링크와 함께 모든 StorageGRID 인증서에 대한 정보에 액세스할 수 있습니다.

1. Grid Manager에서 * configuraton * > * 보안 * > * 인증서 * 를 선택합니다.



2. 인증서 페이지에서 탭을 선택하여 각 인증서 범주에 대한 정보를 확인하고 인증서 설정에 액세스합니다. 적절한 권한이 있는 경우에만 탭에 액세스할 수 있습니다.
   - * 글로벌 *: 웹 브라우저 및 외부 API 클라이언트에서 StorageGRID 액세스를 보호합니다.
   - * 그리드 CA *: 내부 StorageGRID 트래픽을 보호합니다.
   - * 클라이언트 *: 외부 클라이언트와 StorageGRID Prometheus 데이터베이스 간의 연결을 보호합니다.
   - * 로드 밸런서 엔드포인트 *: S3 및 Swift 클라이언트와 StorageGRID 로드 밸런서 간의 연결을 보호합니다.
   - * 테넌트 *: ID 페더레이션 서버 또는 플랫폼 서비스 끝점에서 S3 스토리지 리소스에 대한 연결을 보호합니다.
   - * 기타 *: 특정 인증서가 필요한 StorageGRID 연결을 보호합니다.

   각 탭은 아래에 추가 인증서 세부 정보에 대한 링크와 함께 설명되어 있습니다.

글로벌

글로벌 인증서는 웹 브라우저 및 외부 S3 및 Swift API 클라이언트에서 StorageGRID 액세스를 보호합니다. 두 개의 글로벌 인증서는 처음에 설치 중에 StorageGRID 인증 기관에서 생성합니다. 프로덕션 환경의 모범 사례는 외부 인증 기관에서 서명한 사용자 지정 인증서를 사용하는 것입니다.

- 관리 인터페이스 인증서입니다: StorageGRID 관리 인터페이스에 대한 클라이언트 웹 브라우저 연결을 보호합니다.
- S3 및 Swift API 인증서: S3 및 Swift 클라이언트 애플리케이션이 오브젝트 데이터를 업로드 및 다운로드하는 데 사용하는 스토리지 노드, 관리 노드 및 게이트웨이 노드에 대한 클라이언트 API 연결을 보호합니다.

설치된 글로벌 인증서에 대한 정보는 다음과 같습니다.

- * 이름 *: 인증서 관리 링크가 있는 인증서 이름입니다.
- * 설명 *
- * 유형 *: 사용자 정의 또는 기본값 + 그리드 보안을 강화하기 위해 항상 사용자 지정 인증서를 사용해야 합니다.
- * 만료 날짜 *: 기본 인증서를 사용하는 경우 만료 날짜가 표시되지 않습니다.

다음을 수행할 수 있습니다.

- 기본 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 교체하여 그리드 보안 강화:
  - 기본 StorageGRID 생성 관리 인터페이스 인증서를 교체합니다 Grid Manager 및 Tenant Manager 연결에 사용됩니다.
  - S3 및 Swift API 인증서를 교체합니다 스토리지 노드, CLB 서비스(더 이상 사용되지 않음) 및 로드 밸런서 엔드포인트(옵션) 연결에 사용됩니다.
- 기본 관리 인터페이스 인증서를 복원합니다.
- 기본 S3 및 Swift API 인증서를 복원합니다.
- 스크립트를 사용하여 자체 서명된 새 관리 인터페이스 인증서를 생성합니다.
- 를 복사 또는 다운로드합니다 관리 인터페이스 인증서입니다 또는 S3 및 Swift API 인증서.

그리드 **CA**

를 클릭합니다 Grid CA 인증서StorageGRID 설치 중에 StorageGRID 인증 기관에서 생성한 는 모든 내부 StorageGRID 트래픽을 보호합니다.

인증서 정보에는 인증서 만료 날짜 및 인증서 내용이 포함됩니다.

가능합니다 Grid CA 인증서를 복사하거나 다운로드합니다하지만 변경할 수는 없습니다.

클라이언트

클라이언트 인증서외부 인증 기관에서 생성한 외부 모니터링 도구와 StorageGRID Prometheus 데이터베이스 간의 연결을 보호합니다.

인증서 테이블에는 구성된 각 클라이언트 인증서에 대한 행이 있으며 인증서 만료 날짜와 함께 인증서를 Prometheus 데이터베이스 액세스에 사용할 수 있는지 여부를 나타냅니다.

다음을 수행할 수 있습니다.

- 새 클라이언트 인증서를 업로드하거나 생성합니다.
- 인증서 이름을 선택하면 다음 작업을 수행할 수 있는 인증서 세부 정보가 표시됩니다.
  - 클라이언트 인증서 이름을 변경합니다.
  - Prometheus 액세스 권한을 설정합니다.
  - 클라이언트 인증서를 업로드하고 교체합니다.
  - 클라이언트 인증서를 복사하거나 다운로드합니다.
  - 클라이언트 인증서를 제거합니다.
- 빠른 작업을 하려면 * Actions * 를 선택합니다 편집, 첨부, 또는 제거 클라이언트 인증서. 클라이언트 인증서를 최대 10개까지 선택하고 * Actions * > * Remove * 를 사용하여 한 번에 제거할 수 있습니다.

부하 분산 장치 엔드포인트

로드 밸런서 끝점 인증서업로드하거나 생성한 경우 게이트웨이 노드와 관리 노드에서 S3 및 Swift 클라이언트와 StorageGRID 로드 밸런서 서비스 간의 연결을 보호합니다.

로드 밸런서 끝점 테이블에는 구성된 각 로드 밸런서 끝점에 대한 행이 있으며 전역 S3 및 Swift API 인증서나 사용자 지정 로드 밸런서 끝점 인증서가 끝점에 사용되고 있는지 여부를 나타냅니다. 각 인증서의 만료 날짜도 표시됩니다.

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

다음을 수행할 수 있습니다.

- 끝점 이름을 선택하여 인증서 세부 정보를 비롯하여 로드 밸런서 끝점에 대한 정보가 있는 브라우저 탭을 엽니다.
- FabricPool에 대한 로드 밸런서 끝점 인증서를 지정합니다.
- 글로벌 S3 및 Swift API 인증서를 사용합니다 새 로드 밸런서 끝점 인증서를 생성하는 대신

테넌트

테넌트가 를 사용할 수 있습니다 ID 페더레이션 서버 인증서 또는 플랫폼 서비스 끝점 인증서 StorageGRID에 대한 연결을 보호합니다.

테넌트 테이블에는 각 테넌트에 대한 행이 있으며 각 테넌트가 자체 ID 소스 또는 플랫폼 서비스를 사용할 수 있는 권한이 있는지 여부를 나타냅니다.

다음을 수행할 수 있습니다.

- 테넌트 관리자에 로그인할 테넌트 이름을 선택합니다
- 테넌트 이름을 선택하여 테넌트 ID 페더레이션 세부 정보를 봅니다
- 테넌트 이름을 선택하여 테넌트 플랫폼 서비스 세부 정보를 봅니다
- 엔드포인트 생성 중에 플랫폼 서비스 끝점 인증서를 지정합니다

기타

StorageGRID는 특정 목적으로 다른 보안 인증서를 사용합니다. 이러한 인증서는 기능 이름으로 나열됩니다. 기타 보안 인증서에는 다음이 포함됩니다.

- ID 페더레이션 인증서
- 클라우드 스토리지 풀 인증서
- KMS(키 관리 서버) 인증서
- SSO(Single Sign-On) 인증서
- 이메일 경고 알림 인증서
- 외부 syslog 서버 인증서

정보는 함수에 사용되는 인증서 유형과 해당 서버 및 클라이언트 인증서 만료 날짜를 나타냅니다. 기능 이름을 선택하면 인증서 세부 정보를 보고 편집할 수 있는 브라우저 탭이 열립니다.

> 적절한 권한이 있는 경우에만 다른 인증서에 대한 정보를 보고 액세스할 수 있습니다.

다음을 수행할 수 있습니다.

- ID 페더레이션 인증서를 보고 편집합니다
- KMS(키 관리 서버) 서버 및 클라이언트 인증서를 업로드합니다
- S3, C2S S3 또는 Azure에 대한 클라우드 스토리지 풀 인증서를 지정합니다
- 신뢰할 수 있는 당사자 신뢰를 위해 SSO 인증서를 수동으로 지정합니다
- 경고 e-메일 알림에 사용할 인증서를 지정합니다
- 외부 syslog 서버 인증서를 지정합니다

보안 인증서 세부 정보입니다

각 보안 인증서 유형은 아래에 설명되어 있으며 구현 지침이 포함된 문서에 대한 링크를 제공합니다.

관리 인터페이스 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	클라이언트 웹 브라우저와 StorageGRID 관리 인터페이스 간의 연결을 인증하여 사용자가 보안 경고 없이 그리드 관리자 및 테넌트 관리자에 액세스할 수 있도록 합니다. 또한 이 인증서는 Grid Management API 및 테넌트 관리 API 연결을 인증합니다. 설치 중에 생성된 기본 인증서를 사용하거나 사용자 지정 인증서를 업로드할 수 있습니다.	• 구성 * > * 보안 * > * 인증서 * 에서 * 글로벌 * 탭을 선택한 다음 * 관리 인터페이스 인증서 * 를 선택합니다	관리 인터페이스 인증서를 구성합니다

S3 및 **Swift API** 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	게이트웨이 노드의 더 이상 사용되지 않는 CLB(Connection Load Balancer) 서비스와 로드 밸런서 엔드포인트(선택 사항)에 대한 스토리지 노드에 대한 보안 S3 또는 Swift 클라이언트 연결을 인증합니다.	• 구성 * > * 보안 * > * 인증서 * 에서 * 글로벌 * 탭을 선택한 다음 * S3 및 Swift API 인증서 * 를 선택합니다	S3 및 Swift API 인증서를 구성합니다

Grid CA 인증서

를 참조하십시오 기본 그리드 CA 인증서 설명입니다.

관리자 클라이언트 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
클라이언트	각 클라이언트에 설치되어 StorageGRID에서 외부 클라이언트 액세스를 인증할 수 있습니다. • 권한이 있는 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있습니다. • 외부 도구를 사용하여 StorageGRID를 안전하게 모니터링할 수 있습니다.	구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 클라이언트 * 탭을 선택합니다	클라이언트 인증서를 구성합니다

로드 밸런서 끝점 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	게이트웨이 노드와 관리 노드에서 S3 또는 Swift 클라이언트와 StorageGRID 로드 밸런서 서비스 간의 연결을 인증합니다. 로드 밸런서 끝점을 구성할 때 로드 밸런서 인증서를 업로드하거나 생성할 수 있습니다. 클라이언트 응용 프로그램은 StorageGRID에 연결할 때 로드 밸런서 인증서를 사용하여 개체 데이터를 저장하고 검색합니다. 사용자 지정 버전의 Global을 사용할 수도 있습니다 S3 및 Swift API 인증서 로드 밸런서 서비스에 대한 연결을 인증하는 인증서입니다. 글로벌 인증서를 사용하여 로드 밸런서 연결을 인증하는 경우 각 로드 밸런서 끝점에 대해 별도의 인증서를 업로드하거나 생성할 필요가 없습니다. • 참고: * 로드 밸런서 인증에 사용되는 인증서는 일반적인 StorageGRID 작업 중에 가장 많이 사용되는 인증서입니다.	구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 *	• 로드 밸런서 엔드포인트를 구성합니다 • FabricPool용 로드 밸런서 끝점을 만듭니다

ID 페더레이션 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	Active Directory, OpenLDAP 또는 Oracle Directory Server와 같은 외부 ID 공급자와 StorageGRID 간의 연결을 인증합니다. ID 페더레이션에 사용됩니다. 이 페더레이션을 사용하면 외부 시스템에서 관리 그룹 및 사용자를 관리할 수 있습니다.	• 구성 * > * 액세스 제어 * > * ID 페더레이션 *	ID 페더레이션을 사용합니다

플랫폼 서비스 끝점 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	StorageGRID 플랫폼 서비스에서 S3 스토리지 리소스에 대한 연결을 인증합니다.	• 테넌트 관리자 * > * 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 *	플랫폼 서비스 끝점을 만듭니다 플랫폼 서비스 끝점을 편집합니다

Cloud Storage Pool 엔드포인트 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	StorageGRID 클라우드 스토리지 풀에서 S3 Glacier 또는 Microsoft Azure Blob 스토리지와 같은 외부 스토리지 위치로 연결을 인증합니다. 각 클라우드 공급자 유형에는 다른 인증서가 필요합니다.	ILM * > * 스토리지 풀 *	클라우드 스토리지 풀을 생성합니다

KMS(키 관리 서버) 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버 및 클라이언트	StorageGRID와 StorageGRID 어플라이언스 노드에 암호화 키를 제공하는 외부 키 관리 서버(KMS) 간의 연결을 인증합니다.	구성 * > * 보안 * > * 키 관리 서버 *	KMS(키 관리 서버) 추가

SSO(Single Sign-On) 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	AD FS(Active Directory Federation Services)와 같은 ID 페더레이션 서비스와 SSO(Single Sign-On) 요청에 사용되는 StorageGRID 간의 연결을 인증합니다.	• 구성 * > * 액세스 제어 * > * Single Sign-On *	Single Sign-On 구성

이메일 경고 알림 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버 및 클라이언트	SMTP 이메일 서버와 알림 알림에 사용되는 StorageGRID 간의 연결을 인증합니다. • SMTP 서버와의 통신에 TLS(Transport Layer Security)가 필요한 경우 전자 메일 서버 CA 인증서를 지정해야 합니다. • SMTP 전자 메일 서버에 인증을 위해 클라이언트 인증서가 필요한 경우에만 클라이언트 인증서를 지정합니다.	• 알림 * > * 이메일 설정 *	알림에 대한 이메일 알림을 설정합니다

외부 **syslog** 서버 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	StorageGRID에서 이벤트를 기록하는 외부 syslog 서버 간의 TLS 또는 RELP/TLS 연결을 인증합니다. • 참고: * 외부 syslog 서버에 대한 TCP, RELP/TCP 및 UDP 연결에는 외부 syslog 서버 인증서가 필요하지 않습니다.	• 구성 * > * 모니터링 * > * 감사 및 syslog 서버 * 를 선택한 다음 * 외부 syslog 서버 구성 * 을 선택합니다	외부 syslog 서버를 구성합니다

인증서 예

예 **1:** 부하 분산 서비스

이 예에서 StorageGRID는 서버 역할을 합니다.

1. 로드 밸런서 끝점을 구성하고 StorageGRID에서 서버 인증서를 업로드하거나 생성합니다.
2. 로드 밸런서 끝점에 S3 또는 Swift 클라이언트 연결을 구성하고 동일한 인증서를 클라이언트에 업로드합니다.
3. 클라이언트가 데이터를 저장하거나 검색하려는 경우 HTTPS를 사용하여 로드 밸런서 끝점에 연결합니다.
4. StorageGRID는 공개 키가 포함된 서버 인증서와 개인 키를 기반으로 하는 서명으로 응답합니다.
5. 클라이언트는 서버 서명을 인증서 사본의 서명과 비교하여 이 인증서를 확인합니다. 서명이 일치하면 클라이언트는 동일한 공개 키를 사용하여 세션을 시작합니다.
6. 클라이언트가 StorageGRID로 개체 데이터를 보냅니다.

예 **2:** 외부 키 관리 서버**(KMS)**

이 예에서 StorageGRID는 클라이언트 역할을 합니다.

1. 외부 키 관리 서버 소프트웨어를 사용하면 StorageGRID를 KMS 클라이언트로 구성하고 CA 서명된 서버 인증서, 공용 클라이언트 인증서 및 클라이언트 인증서에 대한 개인 키를 얻을 수 있습니다.
2. Grid Manager를 사용하여 KMS 서버를 구성하고 서버 및 클라이언트 인증서와 클라이언트 개인 키를 업로드합니다.
3. StorageGRID 노드에 암호화 키가 필요한 경우, 이 노드는 인증서의 데이터와 개인 키를 기반으로 하는 서명을 포함하는 KMS 서버에 요청합니다.
4. KMS 서버는 인증서 서명의 유효성을 검사하고 StorageGRID를 신뢰할 수 있는지 결정합니다.
5. KMS 서버는 검증된 연결을 사용하여 응답합니다.

서버 인증서를 구성합니다

지원되는 서버 인증서 유형입니다

StorageGRID 시스템은 RSA 또는 ECDSA(Elliptic Curve Digital Signature Algorithm)로 암호화된 사용자 지정 인증서를 지원합니다.

StorageGRID가 REST API에 대한 클라이언트 연결을 보호하는 방법에 대한 자세한 내용은 을 참조하십시오 S3을 사용합니다 또는 Swift를 사용합니다.

관리 인터페이스 인증서를 구성합니다

기본 관리 인터페이스 인증서를 단일 사용자 지정 인증서로 대체하면 보안 경고가 발생하지 않고 사용자가 Grid Manager 및 Tenant Manager에 액세스할 수 있습니다. 기본 관리 인터페이스 인증서로 되돌리거나 새 인증서를 생성할 수도 있습니다.

이 작업에 대해

기본적으로 모든 관리 노드에는 그리드 CA에서 서명한 인증서가 발급됩니다. 이러한 CA 서명 인증서는 단일 공통 사용자 지정 관리 인터페이스 인증서 및 해당 개인 키로 대체할 수 있습니다.

모든 관리 노드에 하나의 사용자 지정 관리 인터페이스 인증서가 사용되므로 클라이언트가 Grid Manager 및 Tenant Manager에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 사용자 지정 인증서를 정의하여 그리드의 모든 관리 노드와 일치시킵니다.

서버에서 구성을 완료해야 하며 사용 중인 루트 인증 기관(CA)에 따라 사용자가 그리드 관리자 및 테넌트 관리자에 액세스하는 데 사용할 웹 브라우저에 그리드 CA 인증서를 설치해야 할 수도 있습니다.

> 실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 이 서버 인증서가 곧 만료될 때 * Management Interface * 용 서버 인증서 만료 알림이 트리거됩니다. 필요에 따라 * 구성 * > * 보안 * > * 인증서 * 를 선택하고 글로벌 탭에서 관리 인터페이스 인증서의 만료 날짜를 보면 현재 인증서가 만료되는 시점을 확인할 수 있습니다.

> IP 주소 대신 도메인 이름을 사용하여 Grid Manager 또는 Tenant Manager에 액세스하는 경우, 다음 중 하나가 발생할 경우 브라우저에 인증서 오류가 표시되지 않고 무시하도록 옵션이 표시되지 않습니다.
>
> - 사용자 지정 관리 인터페이스 인증서가 만료됩니다.
> - 여러분 사용자 지정 관리 인터페이스 인증서에서 기본 서버 인증서로 되돌립니다.

사용자 지정 관리 인터페이스 인증서를 추가합니다

사용자 지정 관리 인터페이스 인증서를 추가하려면 고유한 인증서를 제공하거나 Grid Manager를 사용하여 인증서를 생성할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택합니다.
2. 글로벌 * 탭에서 * 관리 인터페이스 인증서 * 를 선택합니다.
3. 사용자 정의 인증서 사용 * 을 선택합니다.
4. 인증서를 업로드하거나 생성합니다.

인증서를 업로드합니다

필요한 서버 인증서 파일을 업로드합니다.

a. 인증서 업로드 * 를 선택합니다.

b. 필요한 서버 인증서 파일을 업로드합니다.

   - * 서버 인증서 *: 사용자 정의 서버 인증서 파일(PEM 인코딩).
   - * 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일('.key')입니다.

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

   - * CA 번들 *: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 선택적 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.

c. 업로드한 각 인증서의 메타데이터를 보려면 * 인증서 세부 정보 * 를 확장합니다. 선택적 CA 번들을 업로드한 경우 각 인증서는 자체 탭에 표시됩니다.

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

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

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

d. 저장 * 을 선택합니다. + 사용자 지정 관리 인터페이스 인증서는 Grid Manager, Tenant Manager, Grid Manager API 또는 Tenant Manager API에 대한 이후의 모든 새 연결에 사용됩니다.

인증서를 생성합니다

서버 인증서 파일을 생성합니다.

프로덕션 환경의 모범 사례는 외부 인증 기관에서 서명한 사용자 지정 관리 인터페이스 인증서를 사용하는 것입니다.

a. 인증서 생성 * 을 선택합니다.

b. 인증서 정보를 지정합니다.

   - * 도메인 이름 *: 인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
   - * IP *: 인증서에 포함할 하나 이상의 IP 주소입니다.
   - * subject *: X.509 주체 또는 인증서 소유자의 고유 이름(DN)
   - * 일 유효 *: 인증서 만료 후 일 수입니다.

c. Generate * 를 선택합니다.

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

- 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

  인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

  예를 들어, 'toragegrid_certificate.pem'

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

e. 저장 * 을 선택합니다. + 사용자 지정 관리 인터페이스 인증서는 Grid Manager, Tenant Manager, Grid Manager API 또는 Tenant Manager API에 대한 이후의 모든 새 연결에 사용됩니다.

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

> 새 인증서를 업로드하거나 생성한 후에는 관련 인증서 만료 알림을 지울 수 있도록 최대 하루 동안 기다립니다.

6. 사용자 지정 관리 인터페이스 인증서를 추가하면 관리 인터페이스 인증서 페이지에 사용 중인 인증서에 대한 자세한 인증서 정보가 표시됩니다. + 필요에 따라 인증서 PEM을 다운로드하거나 복사할 수 있습니다.

기본 관리 인터페이스 인증서를 복원합니다

Grid Manager 및 Tenant Manager 연결에 기본 관리 인터페이스 인증서를 사용하도록 되돌릴 수 있습니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택합니다.
2. 글로벌 * 탭에서 * 관리 인터페이스 인증서 * 를 선택합니다.
3. 기본 인증서 사용 * 을 선택합니다.

   기본 관리 인터페이스 인증서를 복원하면 구성한 사용자 지정 서버 인증서 파일이 삭제되고 시스템에서 복구할 수 없습니다. 이후의 모든 새 클라이언트 연결에 기본 관리 인터페이스 인증서가 사용됩니다.

4. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

스크립트를 사용하여 자체 서명된 새 관리 인터페이스 인증서를 생성합니다

엄격한 호스트 이름 확인이 필요한 경우 스크립트를 사용하여 관리 인터페이스 인증서를 생성할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있습니다.
- "passwords.txt" 파일이 있습니다.

이 작업에 대해

프로덕션 환경의 모범 사례는 외부 인증 기관에서 서명한 인증서를 사용하는 것입니다.

단계

1. 각 관리 노드의 FQDN(정규화된 도메인 이름)을 얻습니다.
2. 기본 관리자 노드에 로그인합니다.

a. 'ssh admin@primary_Admin_Node_IP' 명령어를 입력한다
b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
c. 루트로 전환하려면 다음 명령을 입력합니다
d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

3. 자체 서명된 새 인증서를 사용하여 StorageGRID를 구성합니다.

   '$sudo make-certificate—domain_wildcard-admin-node-FQDN_—type management'

   - '- 도메인'의 경우 와일드카드를 사용하여 모든 관리 노드의 정규화된 도메인 이름을 나타냅니다. 예를 들어, '*.ui.storagegrid.example.com'은 ' admin1.ui.storagegrid.example.com ' 및 ' admin2.ui.storagegrid.example.com ' 을 나타내는 * 와일드카드를 사용합니다.
   - 그리드 관리자 및 테넌트 관리자가 사용하는 관리 인터페이스 인증서를 구성하려면 '--type'을 '관리'로 설정합니다.
   - 기본적으로 생성된 인증서는 1년(365일) 동안 유효하며 만료되기 전에 다시 만들어야 합니다. '--days' 인증서를 사용하여 기본 유효 기간을 재정의할 수 있습니다.

     > 인증서의 유효 기간은 make-certificate를 실행하면 시작됩니다. 관리 클라이언트가 StorageGRID와 동일한 시간 소스와 동기화되어 있는지 확인해야 합니다. 그렇지 않으면 클라이언트가 인증서를 거부할 수 있습니다.

     ```
     $ sudo make-certificate --domains *.ui.storagegrid.example.com --type
     management --days 720
     ```

     결과 출력에는 관리 API 클라이언트에 필요한 공용 인증서가 포함됩니다.

4. 인증서를 선택하고 복사합니다.

   선택 항목에 BEGIN 및 END 태그를 포함합니다.

5. 명령 셸에서 로그아웃합니다. '$exit'
6. 인증서가 구성되었는지 확인합니다.
   a. 그리드 관리자에 액세스합니다.
   b. 구성 * > * 보안 * > * 인증서 * 를 선택합니다
   c. 글로벌 * 탭에서 * 관리 인터페이스 인증서 * 를 선택합니다.
7. 복사한 공용 인증서를 사용하도록 관리 클라이언트를 구성합니다. BEGIN 및 END Tags를 포함합니다.

관리 인터페이스 인증서를 다운로드하거나 복사합니다

다른 곳에서 사용할 관리 인터페이스 인증서 내용을 저장하거나 복사할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택합니다.

2. 글로벌 * 탭에서 * 관리 인터페이스 인증서 * 를 선택합니다.
3. 서버 * 또는 * CA 번들 * 탭을 선택한 다음 인증서를 다운로드하거나 복사합니다.

인증서 파일 또는 **CA** 번들을 다운로드합니다

인증서 또는 CA 번들 '.pem' 파일을 다운로드합니다. 선택적 CA 번들을 사용하는 경우 번들의 각 인증서가 자체 하위 탭에 표시됩니다.

a. 인증서 다운로드 * 또는 * CA 번들 다운로드 * 를 선택합니다.

   CA 번들을 다운로드하는 경우 CA 번들 보조 탭의 모든 인증서가 단일 파일로 다운로드됩니다.

b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

인증서 또는 **CA** 번들 **PEM**을 복사합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다. 선택적 CA 번들을 사용하는 경우 번들의 각 인증서가 자체 하위 탭에 표시됩니다.

a. Copy certificate pem * 또는 * Copy CA bundle pem * 을 선택합니다.

   CA 번들을 복사하는 경우 CA 번들 보조 탭의 모든 인증서가 함께 복사됩니다.

b. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.
c. 텍스트 파일을 확장자 '.pem'으로 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

S3 및 **Swift API** 인증서를 구성합니다

스토리지 노드에 대한 S3 또는 Swift 클라이언트 연결에 사용되는 서버 인증서, 게이트웨이 노드의 더 이상 사용되지 않는 CLB(Connection Load Balancer) 서비스 또는 밸런서 엔드포인트를 로드하기 위해 서버 인증서를 교체하거나 복원할 수 있습니다. 교체 사용자 지정 서버 인증서는 조직에 따라 다릅니다.

이 작업에 대해

기본적으로 모든 스토리지 노드에는 그리드 CA에서 서명한 X.509 서버 인증서가 발급됩니다. 이러한 CA 서명 인증서는 하나의 공통 사용자 지정 서버 인증서 및 해당 개인 키로 대체할 수 있습니다.

단일 사용자 지정 서버 인증서가 모든 스토리지 노드에 사용되므로 클라이언트가 스토리지 끝점에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 사용자 지정 인증서를 정의하여 그리드의 모든 스토리지 노드와 일치시킵니다.

서버 구성을 완료한 후 사용 중인 루트 CA(인증 기관)에 따라 시스템에 액세스하는 데 사용할 S3 또는 Swift API 클라이언트에 그리드 CA 인증서를 설치해야 할 수도 있습니다.

> 실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 루트 서버 인증서가 곧 만료될 때 * S3 및 Swift API * 용 글로벌 서버 인증서 만료 알림이 트리거됩니다. 필요에 따라 * 구성 * > * 보안 * > * 인증서 * 를 선택하고 글로벌 탭에서 S3 및 Swift API 인증서의 만료 날짜를 보면 현재 인증서가 만료되는 시점을 확인할 수 있습니다.

사용자 지정 S3 및 Swift API 인증서를 업로드하거나 생성할 수 있습니다.

사용자 지정 **S3** 및 **Swift API** 인증서를 추가합니다

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택합니다.
2. 글로벌 * 탭에서 * S3 및 Swift API 인증서 * 를 선택합니다.
3. 사용자 정의 인증서 사용 * 을 선택합니다.
4. 인증서를 업로드하거나 생성합니다.

인증서를 업로드합니다

필요한 서버 인증서 파일을 업로드합니다.

a. 인증서 업로드 * 를 선택합니다.

b. 필요한 서버 인증서 파일을 업로드합니다.

   - * 서버 인증서 *: 사용자 정의 서버 인증서 파일(PEM 인코딩).
   - * 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일('.key')입니다.

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

   - * CA 번들 *: 각 중간 발급 인증 기관의 인증서를 포함하는 단일 선택적 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.

c. 업로드된 각 사용자 정의 S3 및 Swift API 인증서에 대한 메타데이터와 PEM을 표시하려면 인증서 세부 정보를 선택합니다. 선택적 CA 번들을 업로드한 경우 각 인증서는 자체 탭에 표시됩니다.

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

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

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

d. 저장 * 을 선택합니다.

   사용자 지정 서버 인증서는 이후에 새 S3 및 Swift 클라이언트 연결에 사용됩니다.

인증서를 생성합니다

서버 인증서 파일을 생성합니다.

a. 인증서 생성 * 을 선택합니다.

b. 인증서 정보를 지정합니다.

   - * 도메인 이름 *: 인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
   - * IP *: 인증서에 포함할 하나 이상의 IP 주소입니다.
   - * subject *: X.509 주체 또는 인증서 소유자의 고유 이름(DN)
   - * 일 유효 *: 인증서 만료 후 일 수입니다.

c. Generate * 를 선택합니다.

d. 생성된 사용자 정의 S3 및 Swift API 인증서에 대한 메타데이터와 PEM을 표시하려면 * 인증서 세부 정보 * 를 선택합니다.

   - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

예를 들어, 'toragegrid_certificate.pem'

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

e. 저장 * 을 선택합니다.

사용자 지정 서버 인증서는 이후에 새 S3 및 Swift 클라이언트 연결에 사용됩니다.

5. 탭을 선택하여 기본 StorageGRID 서버 인증서, 업로드된 CA 서명 인증서 또는 생성된 사용자 지정 인증서의 메타데이터를 표시합니다.

> 새 인증서를 업로드하거나 생성한 후에는 관련 인증서 만료 알림을 지울 수 있도록 최대 하루 동안 기다립니다.

6. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.
7. 사용자 지정 S3 및 Swift API 인증서를 추가하면 S3 및 Swift API 인증서 페이지에 사용 중인 사용자 지정 S3 및 Swift API 인증서에 대한 자세한 인증서 정보가 표시됩니다. + 필요에 따라 인증서 PEM을 다운로드하거나 복사할 수 있습니다.

기본 **S3** 및 **Swift API** 인증서를 복원합니다

스토리지 노드에 대한 S3 및 Swift 클라이언트 연결에 대해 기본 S3 및 Swift API 인증서를 사용하고 게이트웨이 노드에서 더 이상 사용되지 않는 CLB 서비스로 되돌릴 수 있습니다. 그러나 로드 밸런서 끝점에는 기본 S3 및 Swift API 인증서를 사용할 수 없습니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택합니다.
2. 글로벌 * 탭에서 * S3 및 Swift API 인증서 * 를 선택합니다.
3. 기본 인증서 사용 * 을 선택합니다.

   글로벌 S3 및 Swift API 인증서의 기본 버전을 복원하면 구성한 사용자 지정 서버 인증서 파일이 삭제되고 시스템에서 복구할 수 없습니다. 기본 S3 및 Swift API 인증서는 이후에 스토리지 노드에 대한 새 S3 및 Swift 클라이언트 연결과 게이트웨이 노드의 더 이상 사용되지 않는 CLB 서비스에 사용됩니다.

4. 경고를 확인하고 기본 S3 및 Swift API 인증서를 복원하려면 * OK * 를 선택합니다.

   루트 액세스 권한이 있고 사용자 지정 S3 및 Swift API 인증서가 로드 밸런서 엔드포인트 연결에 사용된 경우 기본 S3 및 Swift API 인증서를 사용하여 더 이상 액세스할 수 없는 로드 밸런서 끝점의 목록이 표시됩니다. 로 이동합니다 로드 밸런서 엔드포인트를 구성합니다 영향을 받는 끝점을 편집하거나 제거합니다.

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

S3 및 **Swift API** 인증서를 다운로드하거나 복사합니다

다른 곳에서 사용할 수 있도록 S3 및 Swift API 인증서 내용을 저장하거나 복사할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택합니다.
2. 글로벌 * 탭에서 * S3 및 Swift API 인증서 * 를 선택합니다.
3. 서버 * 또는 * CA 번들 * 탭을 선택한 다음 인증서를 다운로드하거나 복사합니다.

인증서 파일 또는 **CA** 번들을 다운로드합니다

인증서 또는 CA 번들 '.pem' 파일을 다운로드합니다. 선택적 CA 번들을 사용하는 경우 번들의 각 인증서가 자체 하위 탭에 표시됩니다.

a. 인증서 다운로드 * 또는 * CA 번들 다운로드 * 를 선택합니다.

   CA 번들을 다운로드하는 경우 CA 번들 보조 탭의 모든 인증서가 단일 파일로 다운로드됩니다.

b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

인증서 또는 **CA** 번들 **PEM**을 복사합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다. 선택적 CA 번들을 사용하는 경우 번들의 각 인증서가 자체 하위 탭에 표시됩니다.

a. Copy certificate pem * 또는 * Copy CA bundle pem * 을 선택합니다.

   CA 번들을 복사하는 경우 CA 번들 보조 탭의 모든 인증서가 함께 복사됩니다.

b. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.
c. 텍스트 파일을 확장자 '.pem'으로 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

관련 정보

- S3을 사용합니다
- Swift를 사용합니다
- S3 API 엔드포인트 도메인 이름을 구성합니다

Grid CA 인증서를 복사합니다

StorageGRID는 내부 CA(인증 기관)를 사용하여 내부 트래픽을 보호합니다. 인증서를 업로드해도 이 인증서는 변경되지 않습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

사용자 지정 서버 인증서가 구성된 경우 클라이언트 응용 프로그램은 사용자 지정 서버 인증서를 사용하여 서버를 확인해야 합니다. StorageGRID 시스템에서 CA 인증서를 복사해서는 안 됩니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 그리드 CA * 탭을 선택합니다.
2. 인증서 PEM * 섹션에서 인증서를 다운로드하거나 복사합니다.

인증서 파일을 다운로드합니다

인증서 '.pem' 파일을 다운로드합니다.

a. 인증서 다운로드 * 를 선택합니다.
b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

인증서 **PEM**을 복사합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다.

a. 인증서 PEM 복사 * 를 선택합니다.
b. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.
c. 텍스트 파일을 확장자 '.pem'으로 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

FabricPool용 **StorageGRID** 인증서를 구성합니다

엄격한 호스트 이름 유효성 검사를 수행하고 FabricPool를 사용하는 ONTAP 클라이언트와 같은 엄격한 호스트 이름 유효성 검사를 사용하지 않는 S3 클라이언트의 경우 로드 밸런서 끝점을 구성할 때 서버 인증서를 생성하거나 업로드할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

이 작업에 대해

로드 밸런서 끝점을 만들 때 자체 서명된 서버 인증서를 생성하거나 알려진 CA(인증 기관)에서 서명한 인증서를 업로드할 수 있습니다. 프로덕션 환경에서는 알려진 CA가 서명한 인증서를 사용해야 합니다. CA에서 서명한 인증서는 중단 없이 회전할 수 있습니다. 또한 중간자 공격에 대한 보호 기능이 강화되어 보안이 더욱 강화되고 있습니다.

다음 단계에서는 FabricPool를 사용하는 S3 클라이언트에 대한 일반 지침을 제공합니다. 자세한 정보 및 절차는 를 참조하십시오 FabricPool용 StorageGRID를 구성합니다.

> 게이트웨이 노드의 별도의 CLB(연결 로드 밸런서) 서비스는 더 이상 사용되지 않으며 FabricPool와 함께 사용하지 않는 것이 좋습니다.

단계

1. 선택적으로 FabricPool에서 사용할 고가용성(HA) 그룹을 구성합니다.
2. FabricPool에서 사용할 S3 로드 밸런서 끝점을 만듭니다.

   HTTPS 로드 밸런서 끝점을 만들면 서버 인증서, 인증서 개인 키 및 선택적 CA 번들을 업로드하라는 메시지가 표시됩니다.

3. StorageGRID을 ONTAP의 클라우드 계층으로 연결

   로드 밸런서 끝점 포트와 업로드한 CA 인증서에 사용된 정규화된 도메인 이름을 지정합니다. 그런 다음 CA 인증서를 제공합니다.

   > 중간 CA에서 StorageGRID 인증서를 발급한 경우 중간 CA 인증서를 제공해야 합니다. StorageGRID 인증서가 루트 CA에서 직접 발급된 경우 루트 CA 인증서를 제공해야 합니다.

클라이언트 인증서를 구성합니다

클라이언트 인증서를 사용하면 권한이 있는 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있으므로 외부 도구에서 StorageGRID를 모니터링하는 안전한 방법이 제공됩니다.

외부 모니터링 도구를 사용하여 StorageGRID에 액세스해야 하는 경우 그리드 관리자를 사용하여 클라이언트 인증서를 업로드하거나 생성하고 인증서 정보를 외부 도구에 복사해야 합니다.

에 대한 정보를 참조하십시오 일반 보안 인증서 사용 및 사용자 지정 서버 인증서를 구성하는 중입니다.

> 실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 이 서버 인증서가 곧 만료될 때 인증서 페이지 * 알림에 구성된 * 클라이언트 인증서 만료가 트리거됩니다. 필요에 따라 * 구성 * > * 보안 * > * 인증서 * 를 선택하고 클라이언트 탭에서 클라이언트 인증서의 만료 날짜를 보면 현재 인증서가 만료되는 시점을 확인할 수 있습니다.

> KMS(키 관리 서버)를 사용하여 특수하게 구성된 어플라이언스 노드의 데이터를 보호하는 경우 에 대한 특정 정보를 참조하십시오 KMS 클라이언트 인증서 업로드.

필요한 것

- 루트 액세스 권한이 있습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 클라이언트 인증서를 구성하려면 다음을 따르십시오.
  - 관리 노드의 IP 주소 또는 도메인 이름이 있습니다.
  - StorageGRID 관리 인터페이스 인증서를 구성한 경우 관리 인터페이스 인증서를 구성하는 데 사용되는 CA, 클라이언트 인증서 및 개인 키가 있습니다.
  - 인증서를 업로드하려면 로컬 컴퓨터에서 인증서의 개인 키를 사용할 수 있습니다.
  - 개인 키는 생성 시 저장 또는 기록되어야 합니다. 원래 개인 키가 없으면 새 개인 키를 만들어야 합니다.
- 클라이언트 인증서를 편집하려면 다음을 따르십시오.

- 관리 노드의 IP 주소 또는 도메인 이름이 있습니다.
- 자체 인증서 또는 새 인증서를 업로드하려면 로컬 컴퓨터에서 개인 키, 클라이언트 인증서 및 CA(사용되는 경우)를 사용할 수 있습니다.

클라이언트 인증서를 추가합니다

시나리오에 따라 클라이언트 인증서를 추가합니다.

- 관리 인터페이스 인증서가 이미 구성되어 있습니다
- CA 발급 클라이언트 인증서
- Grid Manager에서 인증서를 생성했습니다

관리 인터페이스 인증서가 이미 구성되어 있습니다

고객이 제공한 CA, 클라이언트 인증서 및 개인 키를 사용하여 관리 인터페이스 인증서가 이미 구성된 경우 이 절차를 사용하여 클라이언트 인증서를 추가합니다.

단계

1. 그리드 관리자에서 * 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 클라이언트 * 탭을 선택합니다.
2. 추가 * 를 선택합니다.
3. 최소 1자 이상 32자 이하의 인증서 이름을 입력하십시오.
4. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
5. 인증서 종류 * 섹션에서 관리 인터페이스 인증서 '.pem' 파일을 업로드합니다.
   a. 인증서 업로드 * 를 선택한 다음 * 계속 * 을 선택합니다.
   b. 관리 인터페이스 인증서 파일('.pem')을 업로드합니다.
      - 인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.
      - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.
   c. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

      새 인증서가 클라이언트 탭에 나타납니다.
6. Grafana와 같은 외부 모니터링 도구에서 다음 설정을 구성합니다.
   a. * 이름 *: 연결 이름을 입력합니다.

      StorageGRID에는 이 정보가 필요하지 않지만 연결을 테스트하려면 이름을 입력해야 합니다.
   b. * URL *: 관리자 노드의 도메인 이름 또는 IP 주소를 입력합니다. HTTPS 및 포트 9091을 지정합니다.

      예: "https://admin-node.example.com:9091`
   c. TLS 클라이언트 인증 * 및 * CA 인증 * 을 활성화합니다.
   d. TLS/SSL 인증 세부 정보 에서 다음을 복사하여 붙여 넣습니다. +
      - CA 인증서** 에 대한 관리 인터페이스 CA 인증서입니다

- 클라이언트 인증서**
- 클라이언트 키에 대한 개인 키입니다

e. * ServerName *: 관리 노드의 도메인 이름을 입력합니다.

servername은 관리 인터페이스 인증서에 표시된 도메인 이름과 일치해야 합니다.

f. StorageGRID 또는 로컬 파일에서 복사한 인증서 및 개인 키를 저장하고 테스트합니다.

이제 외부 모니터링 툴을 사용하여 StorageGRID에서 Prometheus 메트릭에 액세스할 수 있습니다.

메트릭에 대한 자세한 내용은 를 참조하십시오 StorageGRID 모니터링 지침.

CA 발급 클라이언트 인증서

관리 인터페이스 인증서가 구성되어 있지 않고 CA에서 발급한 클라이언트 인증서 및 개인 키를 사용하는 Prometheus에 대한 클라이언트 인증서를 추가하려는 경우 이 절차를 사용하여 관리자 클라이언트 인증서를 추가하십시오.

단계

1. 의 단계를 수행합니다 관리 인터페이스 인증서를 구성합니다.
2. 그리드 관리자에서 * 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 클라이언트 * 탭을 선택합니다.
3. 추가 * 를 선택합니다.
4. 최소 1자 이상 32자 이하의 인증서 이름을 입력하십시오.
5. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
6. 인증서 유형 * 섹션에서 클라이언트 인증서, 개인 키 및 CA 번들 '.pem' 파일을 업로드합니다.
   a. 인증서 업로드 * 를 선택한 다음 * 계속 * 을 선택합니다.
   b. 클라이언트 인증서, 개인 키 및 CA 번들 파일('.pem')을 업로드합니다.
      - 인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.
      - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.
   c. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

      새 인증서가 클라이언트 탭에 나타납니다.
7. Grafana와 같은 외부 모니터링 도구에서 다음 설정을 구성합니다.
   a. * 이름 *: 연결 이름을 입력합니다.

      StorageGRID에는 이 정보가 필요하지 않지만 연결을 테스트하려면 이름을 입력해야 합니다.
   b. * URL *: 관리자 노드의 도메인 이름 또는 IP 주소를 입력합니다. HTTPS 및 포트 9091을 지정합니다.

      예: "https://admin-node.example.com:9091`
   c. TLS 클라이언트 인증 * 및 * CA 인증 * 을 활성화합니다.
   d. TLS/SSL 인증 세부 정보 에서 다음을 복사하여 붙여 넣습니다. +

- CA 인증서** 에 대한 관리 인터페이스 CA 인증서입니다
- 클라이언트 인증서**
- 클라이언트 키에 대한 개인 키입니다

e. * ServerName *: 관리 노드의 도메인 이름을 입력합니다.

servername은 관리 인터페이스 인증서에 표시된 도메인 이름과 일치해야 합니다.

f. StorageGRID 또는 로컬 파일에서 복사한 인증서 및 개인 키를 저장하고 테스트합니다.

이제 외부 모니터링 툴을 사용하여 StorageGRID에서 Prometheus 메트릭에 액세스할 수 있습니다.

메트릭에 대한 자세한 내용은 를 참조하십시오 StorageGRID 모니터링 지침.

Grid Manager에서 인증서를 생성했습니다

관리 인터페이스 인증서가 구성되어 있지 않고 Grid Manager에서 인증서 생성 기능을 사용하는 Prometheus에 대한 클라이언트 인증서를 추가하려는 경우 이 절차를 사용하여 관리자 클라이언트 인증서를 추가하십시오.

단계

1. 그리드 관리자에서 * 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 클라이언트 * 탭을 선택합니다.
2. 추가 * 를 선택합니다.
3. 최소 1자 이상 32자 이하의 인증서 이름을 입력하십시오.
4. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
5. 인증서 유형 * 섹션에서 * 인증서 생성 * 을 선택합니다.
6. 인증서 정보를 지정합니다.
   - * 도메인 이름 *: 인증서에 포함할 관리자 노드의 정규화된 도메인 이름 하나 이상. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
   - * IP *: 인증서에 포함할 하나 이상의 관리 노드 IP 주소입니다.
   - * subject *: X.509 주체 또는 인증서 소유자의 고유 이름(DN)
7. Generate * 를 선택합니다.
8. [[CLIENT_CERT_DETAILS] 인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.

   > 대화 상자를 닫은 후에는 인증서 개인 키를 볼 수 없습니다. 키를 안전한 위치에 복사하거나 다운로드합니다.

   - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.
   - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

   - 다른 곳에 붙여넣을 인증서 개인 키를 복사하려면 * 개인 키 복사 * 를 선택합니다.

- 개인 키를 파일로 저장하려면 * 개인 키 다운로드 * 를 선택합니다.

  개인 키 파일 이름과 다운로드 위치를 지정합니다.

9. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

   새 인증서가 클라이언트 탭에 나타납니다.

10. 그리드 관리자에서 * 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 글로벌 * 탭을 선택합니다.
11. Management Interface certificate * 를 선택합니다.
12. 사용자 정의 인증서 사용 * 을 선택합니다.
13. 에서 certificate.pem 및 private_key.pem 파일을 업로드합니다 클라이언트 인증서 세부 정보입니다 단계. CA 번들을 업로드할 필요가 없습니다.
    a. 인증서 업로드 * 를 선택한 다음 * 계속 * 을 선택합니다.
    b. 각 인증서 파일('.pem')을 업로드합니다.
    c. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

       새 인증서가 클라이언트 탭에 나타납니다.

14. Grafana와 같은 외부 모니터링 도구에서 다음 설정을 구성합니다.
    a. * 이름 *: 연결 이름을 입력합니다.

       StorageGRID에는 이 정보가 필요하지 않지만 연결을 테스트하려면 이름을 입력해야 합니다.

    b. * URL *: 관리자 노드의 도메인 이름 또는 IP 주소를 입력합니다. HTTPS 및 포트 9091을 지정합니다.

       예: "https://admin-node.example.com:9091`

    c. TLS 클라이언트 인증 * 및 * CA 인증 * 을 활성화합니다.
    d. TLS/SSL 인증 세부 정보 에서 다음을 복사하여 붙여 넣습니다. +
       - CA 인증서 및 클라이언트 인증서 모두에 대한 관리 인터페이스 클라이언트 인증서
       - 클라이언트 키에 대한 개인 키입니다
    e. * ServerName *: 관리 노드의 도메인 이름을 입력합니다.

       servername은 관리 인터페이스 인증서에 표시된 도메인 이름과 일치해야 합니다.

    f. StorageGRID 또는 로컬 파일에서 복사한 인증서 및 개인 키를 저장하고 테스트합니다.

       이제 외부 모니터링 툴을 사용하여 StorageGRID에서 Prometheus 메트릭에 액세스할 수 있습니다.

   메트릭에 대한 자세한 내용은 를 참조하십시오 StorageGRID 모니터링 지침.

클라이언트 인증서를 편집합니다

관리자 클라이언트 인증서를 편집하여 이름을 변경하거나, Prometheus 액세스를 활성화 또는 비활성화하거나, 현재 인증서가 만료되면 새 인증서를 업로드할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 클라이언트 * 탭을 선택합니다.

   인증서 만료 날짜 및 Prometheus 액세스 권한이 표에 나열되어 있습니다. 인증서가 곧 만료되거나 이미 만료된 경우 테이블에 메시지가 나타나고 경고가 트리거됩니다.

2. 편집할 인증서를 선택합니다.
3. 편집 * 을 선택한 다음 * 이름 및 권한 편집 * 을 선택합니다
4. 최소 1자 이상 32자 이하의 인증서 이름을 입력하십시오.
5. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
6. Grid Manager에 인증서를 저장하려면 * Continue * 를 선택합니다.

   업데이트된 인증서가 클라이언트 탭에 표시됩니다.

새 클라이언트 인증서를 연결합니다

현재 인증서가 만료되면 새 인증서를 업로드할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 클라이언트 * 탭을 선택합니다.

   인증서 만료 날짜 및 Prometheus 액세스 권한이 표에 나열되어 있습니다. 인증서가 곧 만료되거나 이미 만료된 경우 테이블에 메시지가 나타나고 경고가 트리거됩니다.

2. 편집할 인증서를 선택합니다.
3. 편집 * 을 선택한 다음 편집 옵션을 선택합니다.

인증서를 업로드합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다.

a. 인증서 업로드 * 를 선택한 다음 * 계속 * 을 선택합니다.
b. 클라이언트 인증서 이름('.pem')을 업로드합니다.

   인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.

   - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

   - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.
c. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

   업데이트된 인증서가 클라이언트 탭에 표시됩니다.

인증서를 생성합니다

다른 곳에 붙여 넣을 인증서 텍스트를 생성합니다.

a. 인증서 생성 * 을 선택합니다.
b. 인증서 정보를 지정합니다.
   - * 도메인 이름 *: 인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
   - * IP *: 인증서에 포함할 하나 이상의 IP 주소입니다.
   - * subject *: X.509 주체 또는 인증서 소유자의 고유 이름(DN)
   - * 일 유효 *: 인증서 만료 후 일 수입니다.
c. Generate * 를 선택합니다.
d. 인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.

   > 대화 상자를 닫은 후에는 인증서 개인 키를 볼 수 없습니다. 키를 안전한 위치에 복사하거나 다운로드합니다.

   - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.
   - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

   - 다른 곳에 붙여넣을 인증서 개인 키를 복사하려면 * 개인 키 복사 * 를 선택합니다.
   - 개인 키를 파일로 저장하려면 * 개인 키 다운로드 * 를 선택합니다.

개인 키 파일 이름과 다운로드 위치를 지정합니다.

e. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

   새 인증서가 클라이언트 탭에 나타납니다.

클라이언트 인증서를 다운로드하거나 복사합니다

다른 곳에서 사용할 클라이언트 인증서를 다운로드하거나 복사할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 클라이언트 * 탭을 선택합니다.
2. 복사 또는 다운로드할 인증서를 선택합니다.
3. 인증서를 다운로드하거나 복사합니다.

   인증서 파일을 다운로드합니다
   인증서 '.pem' 파일을 다운로드합니다.

   a. 인증서 다운로드 * 를 선택합니다.
   b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

      예를 들어, 'toragegrid_certificate.pem'

   인증서를 복사합니다
   인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다.

   a. 인증서 PEM 복사 * 를 선택합니다.
   b. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.
   c. 텍스트 파일을 확장자 '.pem'으로 저장합니다.

      예를 들어, 'toragegrid_certificate.pem'

클라이언트 인증서를 제거합니다

더 이상 관리자 클라이언트 인증서가 필요하지 않으면 제거할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 클라이언트 * 탭을 선택합니다.
2. 제거할 인증서를 선택합니다.
3. 삭제 * 를 선택한 다음 확인합니다.

> 최대 10개의 인증서를 제거하려면 클라이언트 탭에서 제거할 각 인증서를 선택한 다음 * 작업 * > * 삭제 * 를 선택합니다.

인증서가 제거된 후에는 인증서를 사용한 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스하기 위해 새 클라이언트 인증서를 지정해야 합니다.

키 관리 서버를 구성합니다

키 관리 서버 구성: 개요

특별히 구성된 어플라이언스 노드의 데이터를 보호하도록 하나 이상의 외부 키 관리 서버(KMS)를 구성할 수 있습니다.

KMS(키 관리 서버)란 무엇입니까?

KMS(Key Management Server)는 KMIP(Key Management Interoperability Protocol)를 사용하여 관련 StorageGRID 사이트의 StorageGRID 어플라이언스 노드에 암호화 키를 제공하는 외부 타사 시스템입니다.

하나 이상의 키 관리 서버를 사용하여 설치 중에 * 노드 암호화 * 설정이 활성화된 모든 StorageGRID 어플라이언스 노드에 대한 노드 암호화 키를 관리할 수 있습니다. 이러한 어플라이언스 노드에 키 관리 서버를 사용하면 어플라이언스를 데이터 센터에서 제거하더라도 데이터를 보호할 수 있습니다. 어플라이언스 볼륨이 암호화된 후에는 노드에서 KMS와 통신할 수 없는 한 어플라이언스의 데이터에 액세스할 수 없습니다.

> StorageGRID는 어플라이언스 노드를 암호화하고 해독하는 데 사용되는 외부 키를 생성하거나 관리하지 않습니다. 외부 키 관리 서버를 사용하여 StorageGRID 데이터를 보호하려는 경우 해당 서버를 설정하는 방법을 이해하고 암호화 키를 관리하는 방법을 이해해야 합니다. 주요 관리 작업을 수행하는 것은 이 지침의 범위를 벗어납니다. 도움이 필요한 경우 키 관리 서버 설명서를 참조하거나 기술 지원 부서에 문의하십시오.

StorageGRID 암호화 방법을 검토합니다

StorageGRID는 데이터 암호화를 위한 다양한 옵션을 제공합니다. 사용 가능한 방법을 검토하여 데이터 보호 요구 사항을 충족하는 방법을 결정해야 합니다.

이 표는 StorageGRID에서 사용할 수 있는 암호화 방법에 대한 상위 수준의 요약을 제공합니다.

암호화 옵션	작동 방식	적용 대상
Grid Manager의 키 관리 서버(KMS)	StorageGRID 사이트(* 구성 * > * 보안 * > * 키 관리 서버 *)에 대한 키 관리 서버를 구성하고 어플라이언스에 대한 노드 암호화를 활성화합니다. 그런 다음 어플라이언스 노드가 KMS에 연결하여 키 암호화 키(KEK)를 요청합니다. 이 키는 각 볼륨의 DEK(데이터 암호화 키)를 암호화하고 해독합니다.	설치 중에 * 노드 암호화 * 가 활성화된 어플라이언스 노드 어플라이언스의 모든 데이터는 물리적 손실이나 데이터 센터에서 제거되는 것을 방지합니다. KMS로 암호화 키 관리는 스토리지 노드 및 서비스 어플라이언스에만 지원됩니다.

암호화 옵션	작동 방식	적용 대상
SANtricity 시스템 관리자의 드라이브 보안	스토리지 어플라이언스에 대해 드라이브 보안 기능이 설정된 경우 SANtricity 시스템 관리자를 사용하여 보안 키를 생성하고 관리할 수 있습니다. 보안 드라이브의 데이터에 액세스하려면 키가 필요합니다.	FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브를 사용하는 스토리지 어플라이언스 보안 드라이브의 모든 데이터는 데이터 센터에서 물리적 손실 또는 제거로부터 보호됩니다. 일부 스토리지 어플라이언스 또는 서비스 어플라이언스와 함께 사용할 수 없습니다. • SG6000 스토리지 어플라이언스 • SG5700 스토리지 어플라이언스 • SG5600 스토리지 어플라이언스
저장 객체 암호화 그리드 옵션	저장된 개체 암호화 * 옵션은 그리드 관리자(* 구성 * > * 시스템 * > * 그리드 옵션 *)에서 활성화할 수 있습니다. 활성화되면 버킷 레벨 또는 오브젝트 레벨에서 암호화되지 않은 새로운 객체는 수집 중에 암호화됩니다.	새로 수집된 S3 및 Swift 오브젝트 데이터 저장된 기존 객체는 암호화되지 않습니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다. • 저장된 개체 암호화를 구성합니다
S3 버킷 암호화	버킷에 대한 암호화를 활성화하기 위해 Put Bucket 암호화 요청을 발급합니다. 오브젝트 레벨에서 암호화되지 않은 새로운 모든 오브젝트는 수집 중에 암호화됩니다.	새로 수집된 S3 오브젝트 데이터만 버킷에 대해 암호화를 지정해야 합니다. 기존 버킷 객체는 암호화되지 않습니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다. • S3을 사용합니다
S3 오브젝트 서버 측 암호화(SSE)	오브젝트를 저장할 S3 요청을 발행하고 'x-amz-서버측-암호화' 요청 헤더를 포함시킵니다.	새로 수집된 S3 오브젝트 데이터만 객체에 대해 암호화를 지정해야 합니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다. StorageGRID가 키를 관리합니다. • S3을 사용합니다

암호화 옵션	작동 방식	적용 대상
고객이 제공한 키(SSE-C)를 사용한 S3 오브젝트 서버 측 암호화	S3 요청을 발급하여 오브젝트를 저장하고 세 개의 요청 헤더를 포함시킵니다. • 'X-amz-서버측-암호화-고객-알고리즘' • 'X-amz-서버측-암호화-고객-키' • X-amz-서버측-암호화-고객-키-MD5	새로 수집된 S3 오브젝트 데이터만 객체에 대해 암호화를 지정해야 합니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다. 키는 StorageGRID 외부에서 관리됩니다. • S3을 사용합니다
외부 볼륨 또는 데이터 저장소 암호화	구축 플랫폼에서 지원하는 경우 StorageGRID 외부의 암호화 방법을 사용하여 전체 볼륨 또는 데이터 저장소를 암호화합니다.	모든 볼륨 또는 데이터 저장소가 암호화되었다고 가정할 때 모든 오브젝트 데이터, 메타데이터 및 시스템 구성 데이터입니다. 외부 암호화 방법을 사용하면 암호화 알고리즘 및 키를 보다 강력하게 제어할 수 있습니다. 나열된 다른 방법과 결합할 수 있습니다.
StorageGRID 외부에서 개체 암호화	StorageGRID 외부에서 암호화 방법을 사용하여 오브젝트 데이터 및 메타데이터를 StorageGRID에 수집하기 전에 암호화합니다.	오브젝트 데이터 및 메타데이터만 (시스템 구성 데이터는 암호화되지 않음). 외부 암호화 방법을 사용하면 암호화 알고리즘 및 키를 보다 강력하게 제어할 수 있습니다. 나열된 다른 방법과 결합할 수 있습니다. • "Amazon Simple Storage Service - 개발자 가이드: 클라이언트측 암호화를 사용하여 데이터 보호"

여러 암호화 방법을 사용합니다

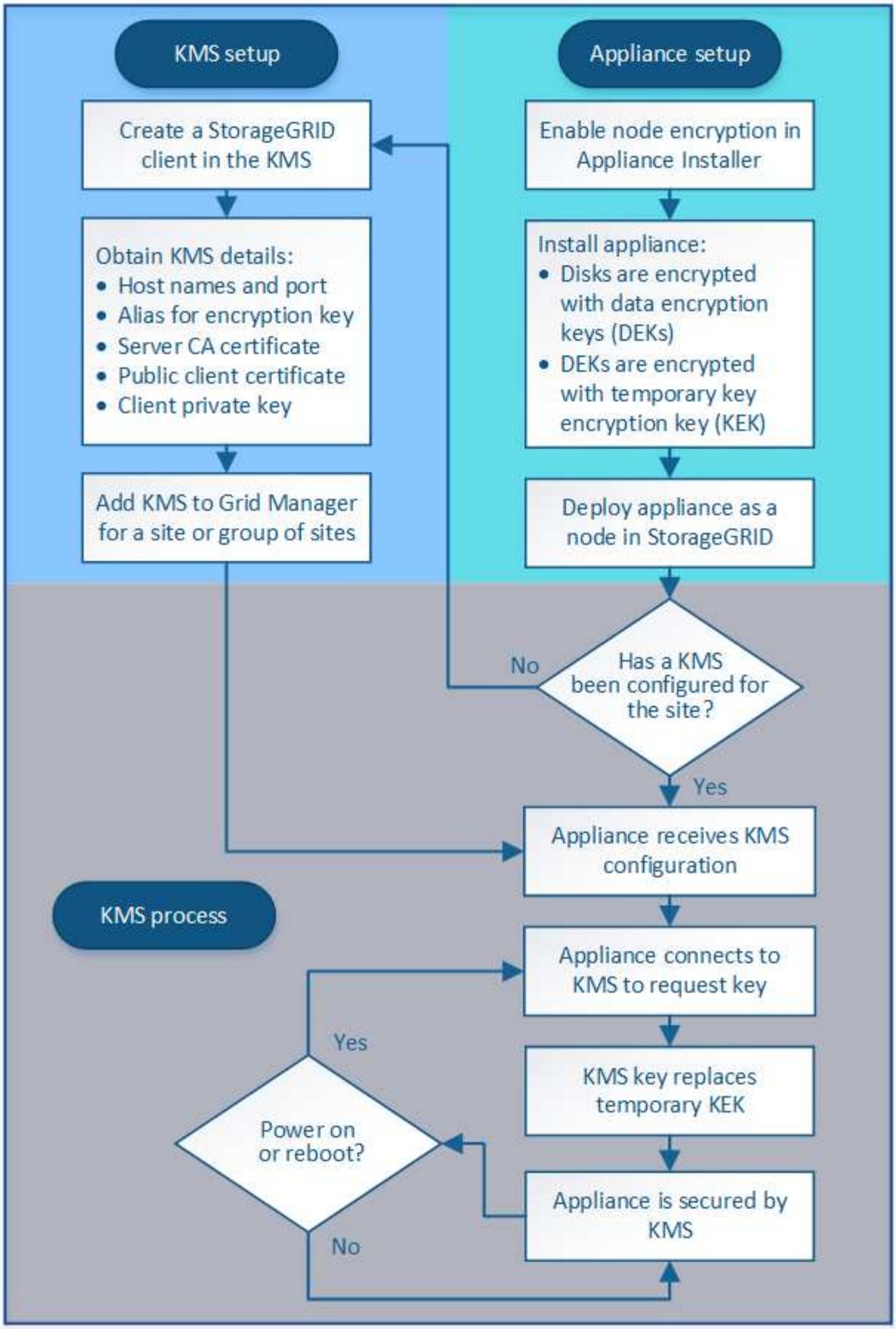
요구 사항에 따라 한 번에 두 가지 이상의 암호화 방법을 사용할 수 있습니다. 예를 들면 다음과 같습니다.

- KMS를 사용하여 어플라이언스 노드를 보호하고 SANtricity 시스템 관리자의 드라이브 보안 기능을 사용하여 동일한 어플라이언스에 있는 자체 암호화 드라이브의 데이터를 "이중 암호화"할 수 있습니다.
- KMS를 사용하여 어플라이언스 노드의 데이터를 보호하고 저장된 개체 암호화 그리드 옵션을 사용하여 모든 개체를 인제스트할 때 암호화할 수 있습니다.

오브젝트의 일부 부분만 암호화해야 하는 경우 대신 버킷 또는 개별 오브젝트 수준에서 암호화를 제어하는 것이 좋습니다. 여러 수준의 암호화를 사용하면 추가 성능 비용이 듭니다.

KMS(키 관리 서버)를 사용하여 어플라이언스 노드에서 StorageGRID 데이터를 보호하려면 먼저 하나 이상의 KMS 서버 설정 및 어플라이언스 노드에 대한 노드 암호화 활성화라는 두 가지 구성 작업을 완료해야 합니다. 이러한 두 구성 작업이 완료되면 키 관리 프로세스가 자동으로 수행됩니다.

이 순서도는 KMS를 사용하여 어플라이언스 노드의 StorageGRID 데이터를 보호하는 상위 단계를 보여 줍니다.



순서도는 KMS 설정 및 어플라이언스 설정이 병렬로 이루어지지만, 요구 사항에 따라 새 어플라이언스 노드에 대한 노드

암호화를 활성화하기 전이나 후에 키 관리 서버를 설정할 수 있습니다.

KMS(키 관리 서버**)** 설정

키 관리 서버를 설정하는 단계는 다음과 같습니다.

단계	을 참조하십시오
KMS 소프트웨어에 액세스하고 각 KMS 또는 KMS 클러스터에 StorageGRID용 클라이언트를 추가합니다.	KMS에서 StorageGRID를 클라이언트로 구성합니다
KMS에서 StorageGRID 클라이언트에 필요한 정보를 얻습니다.	KMS에서 StorageGRID를 클라이언트로 구성합니다
KMS를 Grid Manager에 추가하고, 단일 사이트 또는 기본 사이트 그룹에 할당하고, 필요한 인증서를 업로드하고, KMS 구성을 저장합니다.	KMS(키 관리 서버) 추가

제품을 설치합니다

KMS 사용을 위해 어플라이언스 노드를 설정하는 단계는 다음과 같습니다.

1. 어플라이언스 설치 시 하드웨어 구성 단계에서 StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스에 대한 * 노드 암호화 * 설정을 활성화합니다.

   > 어플라이언스를 그리드에 추가한 후에는 * 노드 암호화 * 설정을 활성화할 수 없으며 노드 암호화가 활성화되지 않은 어플라이언스의 경우 외부 키 관리를 사용할 수 없습니다.

2. StorageGRID 어플라이언스 설치 프로그램을 실행합니다. 설치 중에 각 어플라이언스 볼륨에 DEK(임의 데이터 암호화 키)가 다음과 같이 할당됩니다.
   - DEK는 각 볼륨의 데이터를 암호화하는 데 사용됩니다. 이러한 키는 어플라이언스 OS에서 LUKS(Linux Unified Key Setup) 디스크 암호화를 사용하여 생성되며 변경할 수 없습니다.
   - 각 개별 DEK는 마스터 키 암호화 키(KEK)로 암호화됩니다. 초기 KEK는 어플라이언스가 KMS에 연결할 수 있을 때까지 DEK를 암호화하는 임시 키입니다.
3. 어플라이언스 노드를 StorageGRID에 추가합니다.

자세한 내용은 다음을 참조하십시오.

- SG100 및 SG1000 서비스 어플라이언스
- SG6000 스토리지 어플라이언스
- SG5700 스토리지 어플라이언스
- SG5600 스토리지 어플라이언스

키 관리 암호화 프로세스**(**자동으로 발생**)**

키 관리 암호화에는 자동으로 수행되는 다음과 같은 높은 수준의 단계가 포함됩니다.

1. 노드 암호화가 활성화된 어플라이언스를 그리드에 설치하는 경우 StorageGRID는 새 노드가 포함된 사이트에 대해 KMS 구성이 존재하는지 여부를 결정합니다.
    - KMS가 사이트에 대해 이미 구성된 경우 어플라이언스는 KMS 구성을 받습니다.
    - KMS가 사이트에 대해 아직 구성되지 않은 경우 사이트에 대해 KMS를 구성하고 어플라이언스가 KMS 구성을 받을 때까지 어플라이언스의 데이터는 임시 KK에 의해 계속 암호화됩니다.
2. 이 어플라이언스는 KMS 구성을 사용하여 KMS에 연결하고 암호화 키를 요청합니다.
3. KMS는 암호화 키를 어플라이언스에 보냅니다. KMS의 새 키는 임시 KEK를 대체하며, 이제 어플라이언스 볼륨의 DEK를 암호화하고 해독하는 데 사용됩니다.

> 암호화된 어플라이언스 노드가 구성된 KMS에 연결하기 전에 존재하는 모든 데이터는 임시 키로 암호화됩니다. 그러나 임시 키를 KMS 암호화 키로 교체할 때까지 어플라이언스 볼륨을 데이터 센터에서 제거하지 않도록 보호해서는 안 됩니다.

4. 제품의 전원이 켜져 있거나 재부팅된 경우 KMS에 다시 연결하여 키를 요청합니다. 휘발성 메모리에 저장된 키는 전원 손실이나 재부팅 시에도 계속 유지될 수 없습니다.

키 관리 서버 사용에 대한 고려 사항 및 요구 사항

외부 키 관리 서버(KMS)를 구성하기 전에 고려 사항 및 요구 사항을 이해해야 합니다.

KMIP 요구사항은 무엇입니까**?**

StorageGRID는 KMIP 버전 1.4를 지원합니다.

"키 관리 상호 운용성 프로토콜 사양 버전 1.4"

어플라이언스 노드와 구성된 KMS 간의 통신은 보안 TLS 연결을 사용합니다. StorageGRID는 KMIP에 대해 다음 TLS v1.2 암호를 지원합니다.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

노드 암호화를 사용하는 각 어플라이언스 노드에서 사이트에 대해 구성한 KMS 또는 KMS 클러스터에 대한 네트워크 액세스 권한이 있는지 확인해야 합니다.

네트워크 방화벽 설정을 통해 각 어플라이언스 노드가 KMIP(Key Management Interoperability Protocol) 통신에 사용되는 포트를 통해 통신할 수 있어야 합니다. 기본 KMIP 포트는 5696입니다.

어떤 어플라이언스가 지원됩니까**?**

KMS(키 관리 서버)를 사용하여 * 노드 암호화 * 설정이 활성화된 그리드에 있는 StorageGRID 어플라이언스의 암호화 키를 관리할 수 있습니다. 이 설정은 StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스 설치의 하드웨어 구성 단계에서만 활성화할 수 있습니다.

> 어플라이언스를 그리드에 추가한 후에는 노드 암호화를 활성화할 수 없으며 노드 암호화가 활성화되지 않은 어플라이언스의 경우 외부 키 관리를 사용할 수 없습니다.

다음 StorageGRID 어플라이언스 및 어플라이언스 노드에 대해 구성된 KMS를 사용할 수 있습니다.

어플라이언스	노드 유형입니다
SG1000 서비스 어플라이언스	관리자 노드 또는 게이트웨이 노드
SG100 서비스 어플라이언스	관리자 노드 또는 게이트웨이 노드
SG6000 스토리지 어플라이언스	스토리지 노드
SG5700 스토리지 어플라이언스	스토리지 노드
SG5600 스토리지 어플라이언스	스토리지 노드

다음을 포함하여 소프트웨어 기반(비어플라이언스) 노드에 대해 구성된 KMS를 사용할 수 없습니다.

- 가상 머신(VM)으로 구축된 노드
- Linux 호스트의 컨테이너 엔진 내에 구축된 노드

이러한 다른 플랫폼에 구축된 노드는 StorageGRID 외부의 데이터 저장소 또는 디스크 레벨에서 암호화를 사용할 수 있습니다.

키 관리 서버는 언제 구성해야 합니까?

새 설치의 경우 일반적으로 테넌트를 생성하기 전에 Grid Manager에서 하나 이상의 키 관리 서버를 설정해야 합니다. 이 순서를 사용하면 오브젝트 데이터가 노드에 저장되기 전에 노드가 보호됩니다.

어플라이언스 노드를 설치하기 전이나 설치한 후에 Grid Manager에서 키 관리 서버를 구성할 수 있습니다.

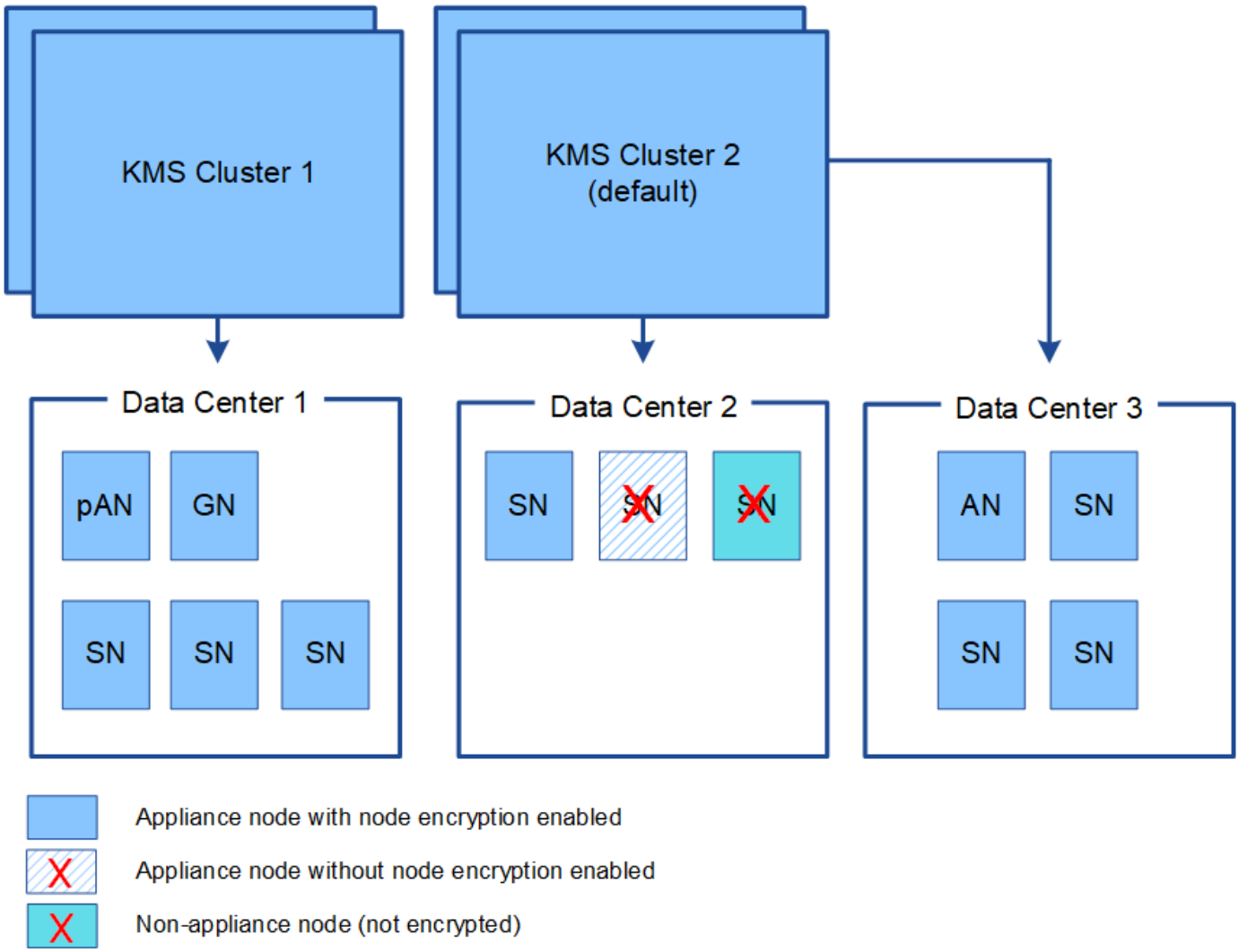
몇 개의 키 관리 서버가 필요합니까?

StorageGRID 시스템의 어플라이언스 노드에 암호화 키를 제공하도록 하나 이상의 외부 키 관리 서버를 구성할 수 있습니다. 각 KMS는 단일 사이트 또는 사이트 그룹의 StorageGRID 어플라이언스 노드에 단일 암호화 키를 제공합니다.

StorageGRID는 KMS 클러스터 사용을 지원합니다. 각 KMS 클러스터에는 구성 설정 및 암호화 키를 공유하는 여러 개의 복제된 키 관리 서버가 포함되어 있습니다. KMS 클러스터를 사용하여 키 관리를 수행하는 것이 좋습니다. KMS 클러스터는 고가용성 구성의 장애 조치 기능을 개선하므로 이 기능을 사용하는 것이 좋습니다.

예를 들어, StorageGRID 시스템에 데이터 센터 사이트가 3개 있다고 가정합니다. 다른 모든 사이트의 모든 어플라이언스 노드에 키를 제공하도록 하나의 KMS 클러스터를 구성하여 Data Center 1의 모든 어플라이언스 노드와 두 번째 KMS 클러스터에 키를 제공할 수 있습니다. 두 번째 KMS 클러스터를 추가하면 데이터 센터 2 및 데이터 센터 3에 대한 기본 KMS를 구성할 수 있습니다.

비어플라이언스 노드나 설치 중에 * 노드 암호화 * 설정이 활성화되지 않은 어플라이언스 노드에 대해 KMS를 사용할 수 없습니다.



키를 회전하면 어떻게 됩니까?

보안 모범 사례로서 구성된 각 KMS에서 사용하는 암호화 키를 주기적으로 순환시켜야 합니다.

암호화 키를 회전할 때 KMS 소프트웨어를 사용하여 마지막으로 사용된 키 버전에서 동일한 키의 새 버전으로 회전합니다. 완전히 다른 키로 회전하지 마십시오.

> Grid Manager에서 KMS의 키 이름(별칭)을 변경하여 키를 회전하려고 하지 마십시오. 대신 KMS 소프트웨어의 키 버전을 업데이트하여 키를 돌리십시오. 이전 키에 사용된 것과 동일한 키 별칭을 새 키에 사용합니다. 구성된 KMS의 키 별칭을 변경하면 StorageGRID에서 데이터의 암호를 해독하지 못할 수 있습니다.

새 키 버전을 사용할 수 있는 경우:

- KMS와 관련된 사이트 또는 사이트의 암호화된 어플라이언스 노드에 자동으로 배포됩니다. 키는 회전된 후 1시간 내에 분포되어야 합니다.
- 새 키 버전이 배포될 때 암호화된 어플라이언스 노드가 오프라인이면 재부팅되는 즉시 새 키가 노드에 수신됩니다.
- 새 키 버전을 사용하여 어플라이언스 볼륨을 암호화할 수 없는 경우 어플라이언스 노드에 대해 * KMS 암호화 키 회전 실패 * 경고가 트리거됩니다. 이 경고를 해결하려면 기술 지원 부서에 문의해야 할 수도 있습니다.

어플라이언스 노드를 암호화한 후 다시 사용할 수 있습니까?

암호화된 어플라이언스를 다른 StorageGRID 시스템에 설치해야 하는 경우 오브젝트 데이터를 다른 노드로 이동하려면 먼저 그리드 노드를 해제해야 합니다. 그런 다음 StorageGRID 어플라이언스 설치 프로그램을 사용하여 KMS 구성을 지울 수 있습니다. KMS 구성을 지우면 * 노드 암호화 * 설정이 비활성화되고 StorageGRID 사이트에 대한 어플라이언스 노드와 KMS 구성 간의 연결이 제거됩니다.

> KMS 암호화 키에 액세스할 수 없으므로 어플라이언스에 남아 있는 데이터는 더 이상 액세스할 수 없으며 영구적으로 잠깁니다.

관련 정보

- SG100 및 SG1000 서비스 어플라이언스
- SG6000 스토리지 어플라이언스
- SG5700 스토리지 어플라이언스
- SG5600 스토리지 어플라이언스

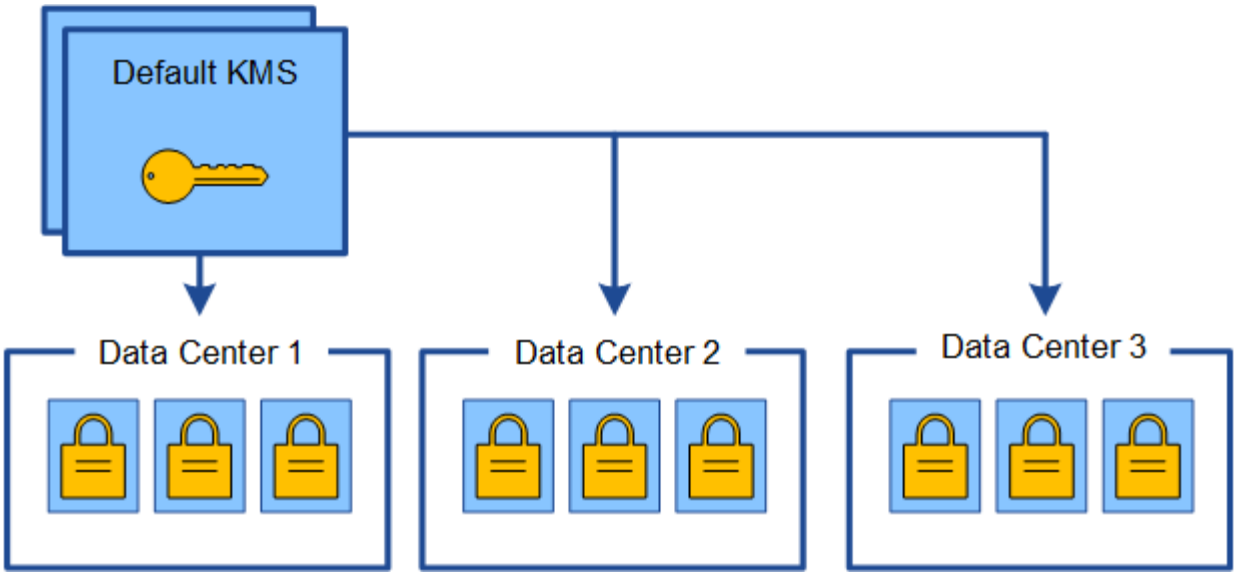
사이트의 **KMS**를 변경할 때의 고려 사항

각 KMS(Key Management Server) 또는 KMS 클러스터는 단일 사이트 또는 사이트 그룹의 모든 어플라이언스 노드에 암호화 키를 제공합니다. 사이트에 사용되는 KMS를 변경해야 하는 경우 암호화 키를 한 KMS에서 다른 KMS로 복사해야 할 수 있습니다.

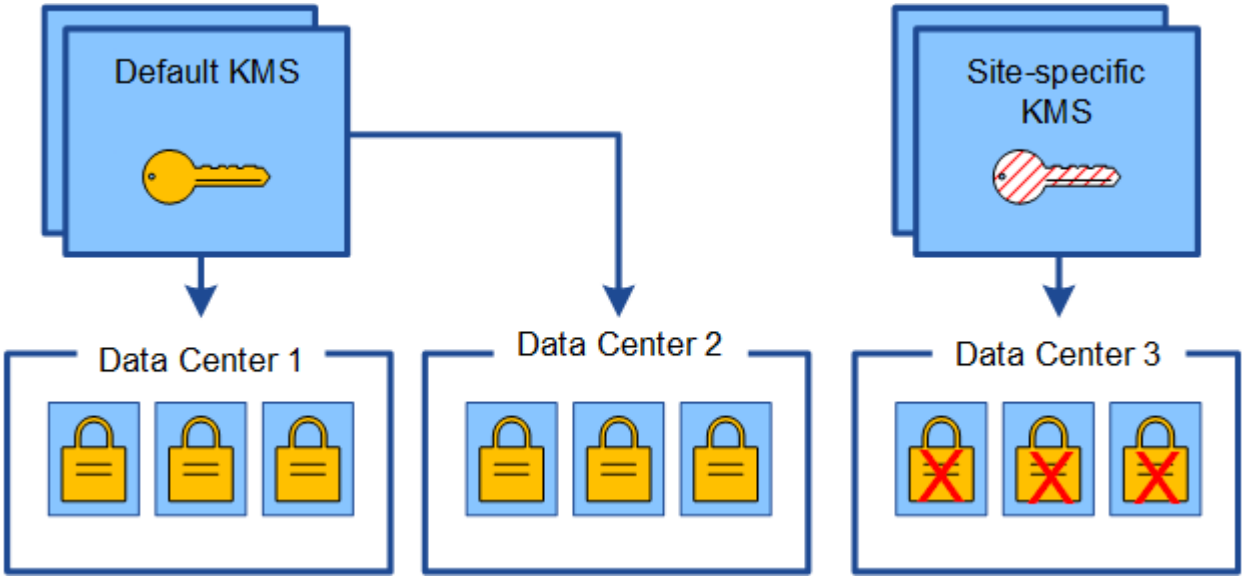
사이트에 사용되는 KMS를 변경하는 경우 해당 사이트에서 이전에 암호화된 어플라이언스 노드를 새 KMS에 저장된 키를 사용하여 해독할 수 있는지 확인해야 합니다. 경우에 따라 기존 KMS에서 새 KMS로 최신 버전의 암호화 키를 복사해야 할 수도 있습니다. KMS가 사이트에서 암호화된 어플라이언스 노드를 해독할 수 있는 올바른 키를 가지고 있는지 확인해야 합니다.

예를 들면 다음과 같습니다.

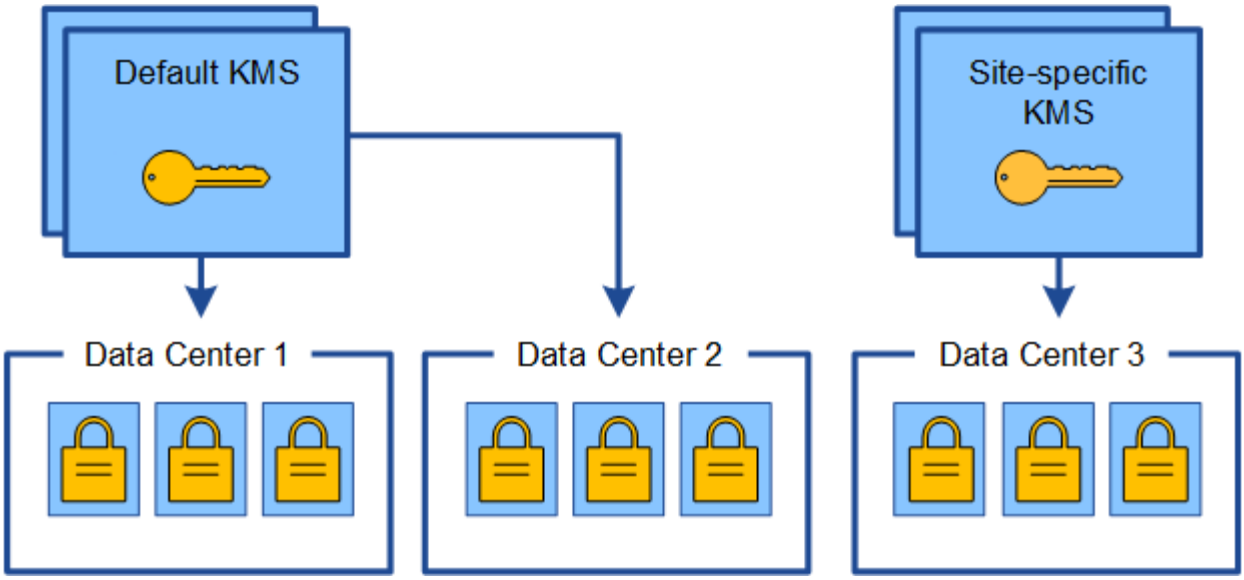
1. 처음에는 전용 KMS가 없는 모든 사이트에 적용되는 기본 KMS를 구성합니다.
2. KMS가 저장되면 * 노드 암호화 * 설정이 활성화된 모든 어플라이언스 노드가 KMS에 연결하여 암호화 키를 요청합니다. 이 키는 모든 사이트에서 어플라이언스 노드를 암호화하는 데 사용됩니다. 이러한 어플라이언스의 암호를 해독하는 데에도 이 동일한 키를 사용해야 합니다.



3. 한 사이트에 대해 사이트별 KMS를 추가하기로 결정합니다(그림의 데이터 센터 3). 그러나 어플라이언스 노드는 이미 암호화되어 있으므로 사이트별 KMS에 대한 구성을 저장하려고 하면 유효성 검사 오류가 발생합니다. 이 오류는 사이트별 KMS에 해당 사이트의 노드를 해독할 수 있는 올바른 키가 없기 때문에 발생합니다.



4. 이 문제를 해결하려면 기본 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사합니다. (원칙적으로 원래 키를 동일한 별칭이 있는 새 키에 복사합니다. 원래 키는 새 키의 이전 버전이 됩니다.) 이제 사이트별 KMS에는 데이터 센터 3의 어플라이언스 노드를 해독하는 올바른 키가 있으므로 StorageGRID에 저장할 수 있습니다.



사이트에 사용되는 **KMS**를 변경하는 사용 사례

이 표에는 사이트에 대한 KMS를 변경하는 가장 일반적인 경우를 위한 필수 단계가 요약되어 있습니다.

사이트의 **KMS**를 변경하는 사용 사례	필요한 단계
하나 이상의 사이트별 KMS 항목이 있으며 이 중 하나를 기본 KMS로 사용하려고 합니다.	사이트별 KMS를 편집합니다. [에 대한 키 관리] 필드에서 * 다른 KMS에 의해 관리되지 않는 사이트(기본 KMS) * 를 선택합니다. 이제 사이트별 KMS가 기본 KMS로 사용됩니다. 이 내용은 전용 KMS가 없는 사이트에 적용됩니다. KMS(키 관리 서버) 편집
기본 KMS가 있으며 확장 시 새 사이트를 추가합니다. 새 사이트에 기본 KMS를 사용하지 않으려는 경우	1. 새 사이트의 어플라이언스 노드가 기본 KMS에 의해 이미 암호화된 경우 KMS 소프트웨어를 사용하여 기본 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사합니다. 2. Grid Manager를 사용하여 새 KMS를 추가하고 사이트를 선택합니다. KMS(키 관리 서버) 추가
사이트의 KMS가 다른 서버를 사용하도록 해야 합니다.	1. 사이트의 어플라이언스 노드가 기존 KMS에 의해 이미 암호화된 경우 KMS 소프트웨어를 사용하여 기존 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사합니다. 2. Grid Manager를 사용하여 기존 KMS 구성을 편집하고 새 호스트 이름 또는 IP 주소를 입력합니다. KMS(키 관리 서버) 추가

KMS를 StorageGRID에 추가하려면 각 외부 키 관리 서버 또는 KMS 클러스터에 대해 StorageGRID를 클라이언트로 구성해야 합니다.

이 작업에 대해

이러한 지침은 Thales CipherTrust Manager k170v, 버전 2.0, 2.1 및 2.2에 적용됩니다. StorageGRID에서 다른 키 관리 서버를 사용하는 방법에 대한 질문이 있는 경우 기술 지원 부서에 문의하십시오.

"Thales CipherTrust 관리자"

단계

1. KMS 소프트웨어에서 사용하려는 각 KMS 또는 KMS 클러스터에 대해 StorageGRID 클라이언트를 만듭니다.

   각 KMS는 단일 사이트 또는 사이트 그룹에서 StorageGRID 어플라이언스 노드에 대한 단일 암호화 키를 관리합니다.

2. KMS 소프트웨어에서 각 KMS 또는 KMS 클러스터에 대한 AES 암호화 키를 만듭니다.

   암호화 키를 내보낼 수 있어야 합니다.

3. 각 KMS 또는 KMS 클러스터에 대해 다음 정보를 기록합니다.

   KMS를 StorageGRID에 추가할 때 이 정보가 필요합니다.

   - 각 서버의 호스트 이름 또는 IP 주소입니다.
   - KMS에서 KMIP 포트를 사용합니다.
   - KMS의 암호화 키에 대한 키 별칭입니다.

   > 암호화 키는 KMS에 이미 있어야 합니다. StorageGRID는 KMS 키를 만들거나 관리하지 않습니다.

4. 각 KMS 또는 KMS 클러스터에 대해 CA(인증 기관)가 서명한 서버 인증서 또는 인증서 체인 순서에 따라 연결된 PEM 인코딩된 CA 인증서 파일이 들어 있는 인증서 번들을 받습니다.

   서버 인증서를 사용하면 외부 KMS가 StorageGRID에 자신을 인증할 수 있습니다.

   - 인증서는 PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식을 사용해야 합니다.
   - 각 서버 인증서의 주체 대체 이름(SAN) 필드에는 StorageGRID가 연결할 정규화된 도메인 이름(FQDN) 또는 IP 주소가 포함되어야 합니다.

     > StorageGRID에서 KMS를 구성할 때 * 호스트 이름 * 필드에 동일한 FQDN 또는 IP 주소를 입력해야 합니다.

   - 서버 인증서는 KMS의 KMIP 인터페이스에서 사용하는 인증서와 일치해야 하며, 일반적으로 포트 5696을 사용합니다.

5. 외부 KMS 및 클라이언트 인증서의 개인 키로 StorageGRID에 발급된 공용 클라이언트 인증서를 얻습니다.

   클라이언트 인증서를 사용하면 StorageGRID가 KMS에 대한 인증을 받을 수 있습니다.

StorageGRID 키 관리 서버 마법사를 사용하여 각 KMS 또는 KMS 클러스터를 추가합니다.

필요한 것

- 을(를) 검토했습니다 키 관리 서버 사용에 대한 고려 사항 및 요구 사항.
- 있습니다 KMS에서 StorageGRID를 클라이언트로 구성했습니다또한 각 KMS 또는 KMS 클러스터에 필요한 정보가 있습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.

이 작업에 대해

가능하면 다른 KMS에서 관리하지 않는 모든 사이트에 적용되는 기본 KMS를 구성하기 전에 사이트별 키 관리 서버를 구성하십시오. 기본 KMS를 먼저 만들면 그리드의 모든 노드 암호화 어플라이언스는 기본 KMS로 암호화됩니다. 나중에 사이트별 KMS를 만들려면 먼저 기본 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사해야 합니다. 을 참조하십시오 사이트의 KMS를 변경할 때의 고려 사항 를 참조하십시오.

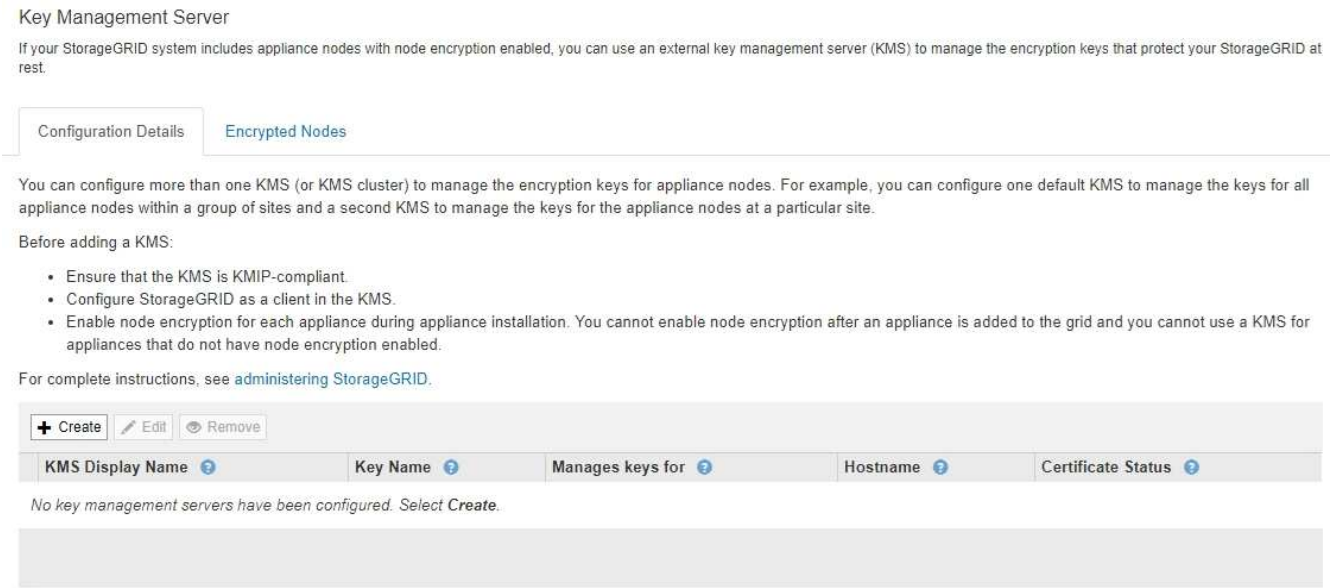
1단계: KMS 세부 정보를 입력합니다

키 관리 서버 추가 마법사의 1단계(KMS 세부 정보 입력)에서 KMS 또는 KMS 클러스터에 대한 세부 정보를 제공합니다.

단계

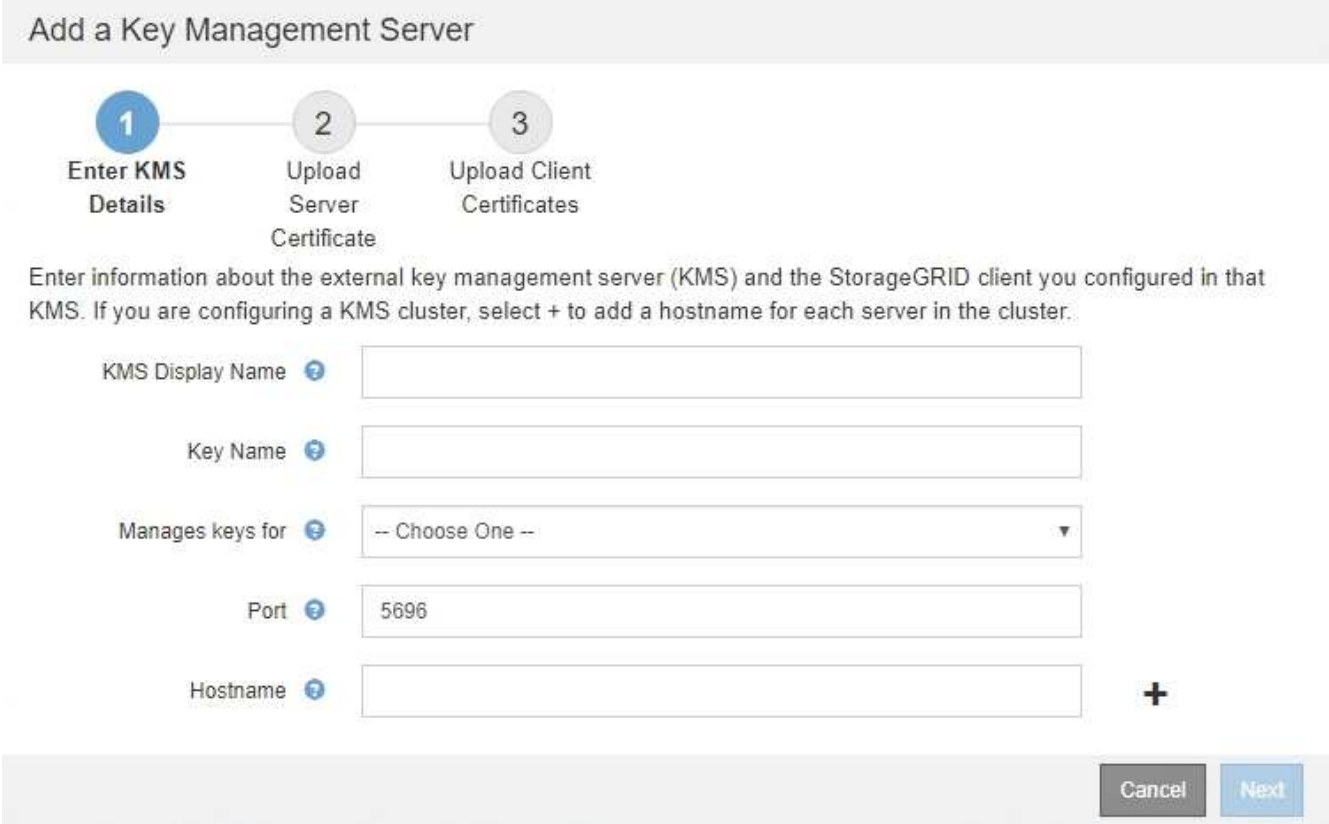
1. 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   구성 세부 정보 탭이 선택된 상태로 키 관리 서버 페이지가 나타납니다.



2. Create * 를 선택합니다.

   키 관리 서버 추가 마법사의 1단계(KMS 세부 정보 입력)가 나타납니다.



3. KMS에 구성한 KMS 및 StorageGRID 클라이언트에 대한 다음 정보를 입력합니다.

필드에 입력합니다	설명
KMS 표시 이름	이 KMS를 식별하는 데 도움이 되는 설명 이름입니다. 1자에서 64자 사이여야 합니다.
키 이름	KMS에서 StorageGRID 클라이언트에 대한 정확한 키 별칭입니다. 1자에서 255자 사이여야 합니다.
의 키를 관리합니다	이 KMS와 관련된 StorageGRID 사이트입니다. 가능하면 다른 KMS에서 관리하지 않는 모든 사이트에 적용되는 기본 KMS를 구성하기 전에 사이트별 키 관리 서버를 구성해야 합니다. • 이 KMS가 특정 사이트의 어플라이언스 노드에 대한 암호화 키를 관리하는 경우 사이트를 선택합니다. • 다른 KMS(기본 KMS)에서 관리하지 않는 사이트 * 를 선택하여 전용 KMS가 없는 사이트 및 이후 확장에 추가한 사이트에 적용되는 기본 KMS를 구성합니다. ◦ 참고:* KMS 구성을 저장하면 검증 오류가 발생합니다. KMS 기본 KMS에 의해 이전에 암호화된 사이트를 선택했지만 새 KMS에 원본 암호화 키의 현재 버전을 제공하지 않은 경우 KMS 구성을 저장하면 오류가 발생합니다.

필드에 입력합니다	설명
포트	KMS 서버가 KMIP(Key Management Interoperability Protocol) 통신에 사용하는 포트입니다. 기본값은 5696으로, KMIP 표준 포트입니다.
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. • 참고: * 서버 인증서의 SAN 필드에는 여기에 입력한 FQDN 또는 IP 주소가 포함되어야 합니다. 그렇지 않으면 StorageGRID는 KMS 또는 KMS 클러스터의 모든 서버에 연결할 수 없습니다.

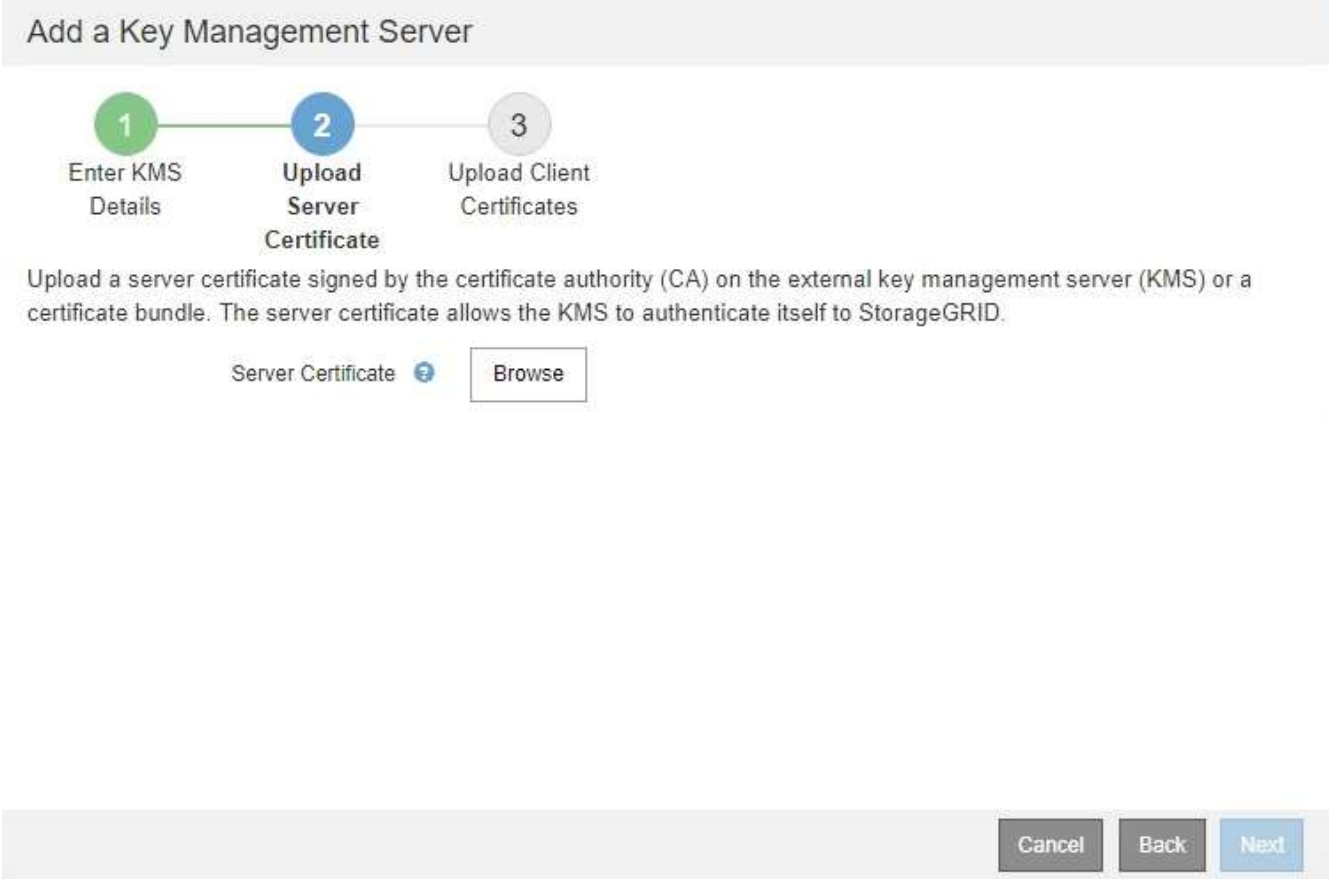
4. KMS 클러스터를 사용하는 경우 더하기 기호를 선택합니다 ✚ 클러스터에 있는 각 서버의 호스트 이름을 추가합니다.
5. 다음 * 을 선택합니다.

2단계**:** 서버 인증서 업로드

키 관리 서버 추가 마법사의 2단계(서버 인증서 업로드)에서 KMS에 대한 서버 인증서(또는 인증서 번들)를 업로드합니다. 서버 인증서를 사용하면 외부 KMS가 StorageGRID에 자신을 인증할 수 있습니다.

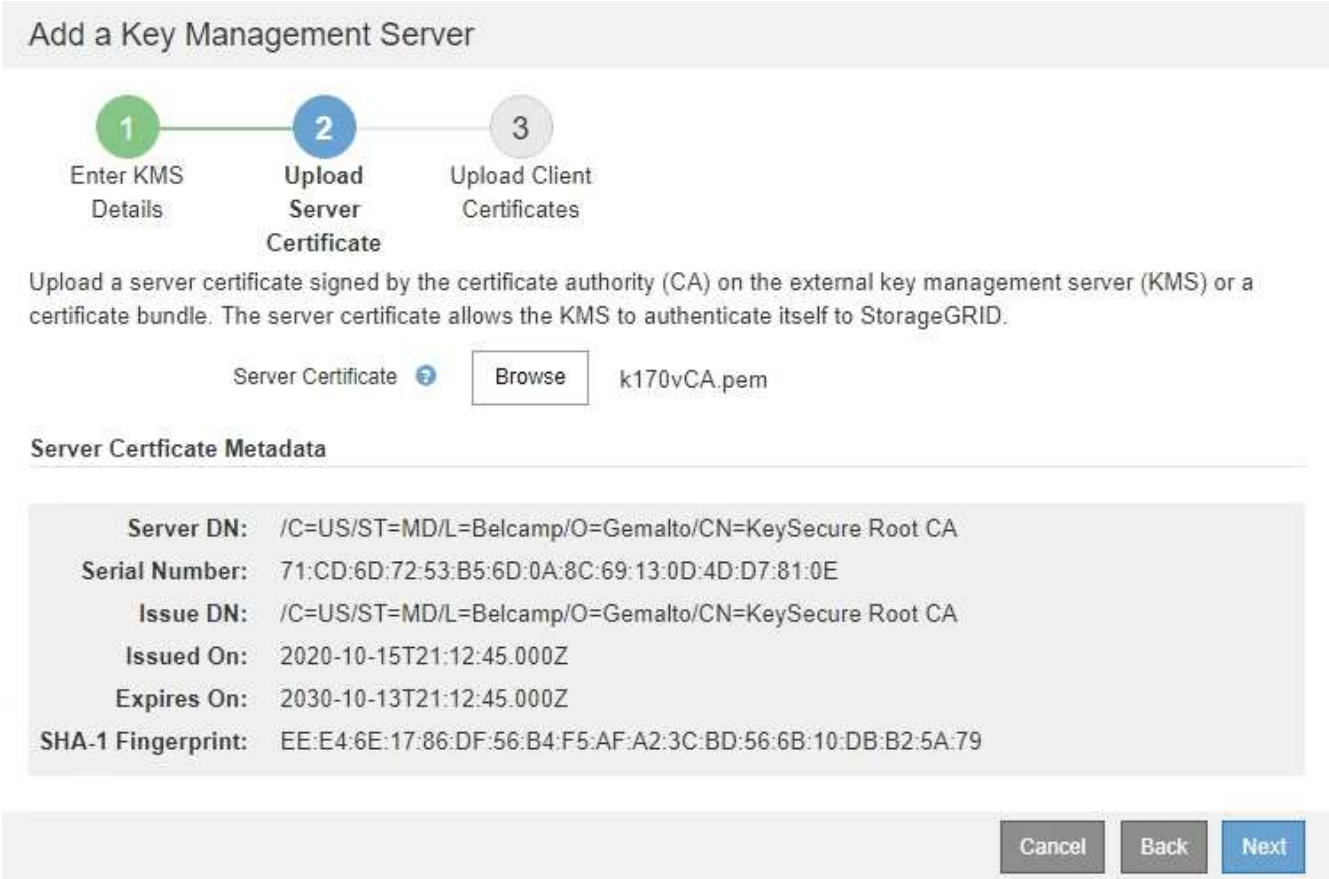
단계

1. 2단계(서버 인증서 업로드) * 에서 저장된 서버 인증서 또는 인증서 번들의 위치를 찾습니다.



2. 인증서 파일을 업로드합니다.

   서버 인증서 메타데이터가 나타납니다.



> 인증서 번들을 업로드한 경우 각 인증서의 메타데이터가 해당 탭에 표시됩니다.

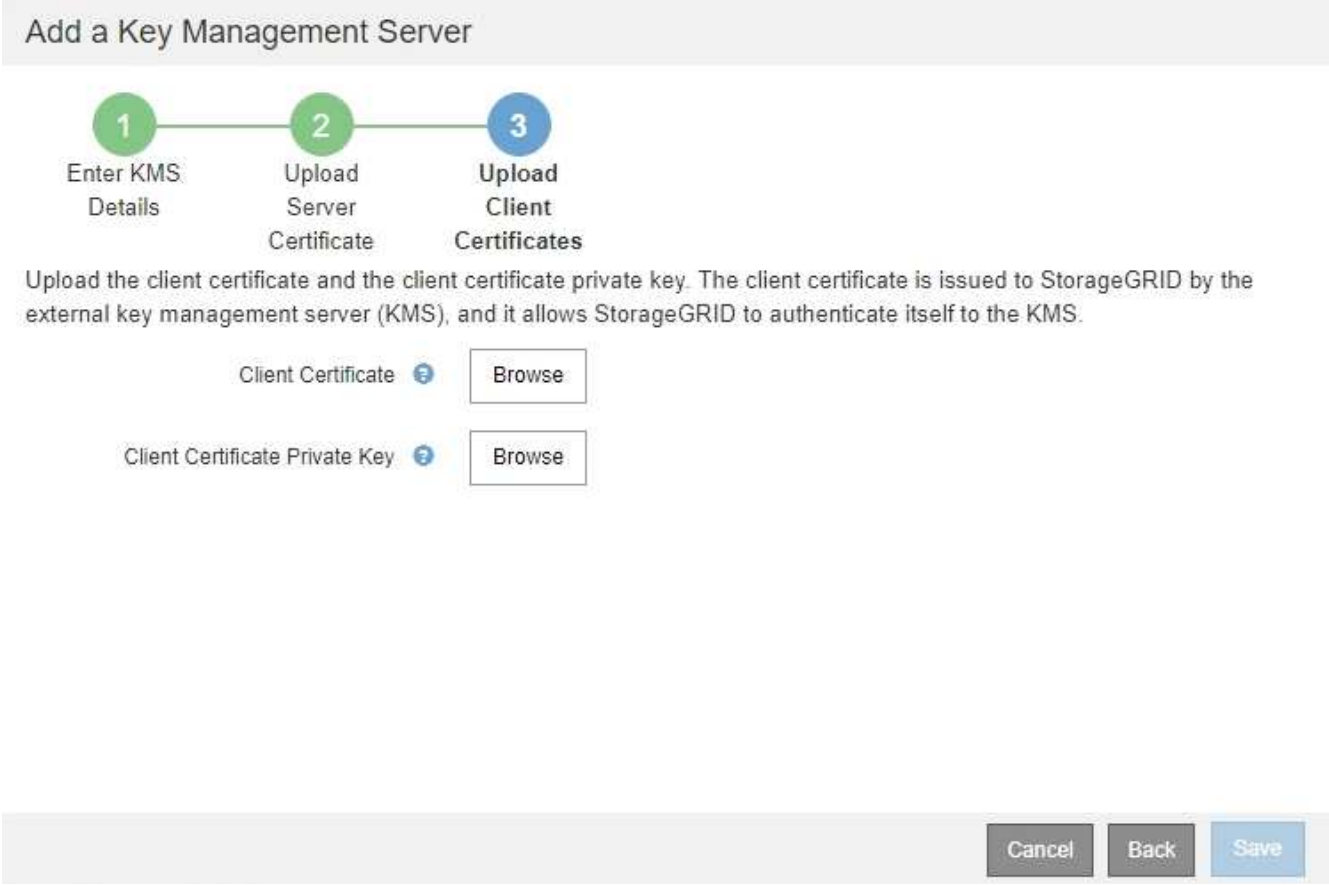
3. 다음 * 을 선택합니다.

3단계**:** 클라이언트 인증서 업로드

키 관리 서버 추가 마법사의 3단계(클라이언트 인증서 업로드)에서 클라이언트 인증서와 클라이언트 인증서 개인 키를 업로드합니다. 클라이언트 인증서를 사용하면 StorageGRID가 KMS에 대한 인증을 받을 수 있습니다.

단계

1. 3단계(클라이언트 인증서 업로드) * 에서 클라이언트 인증서 위치를 찾습니다.

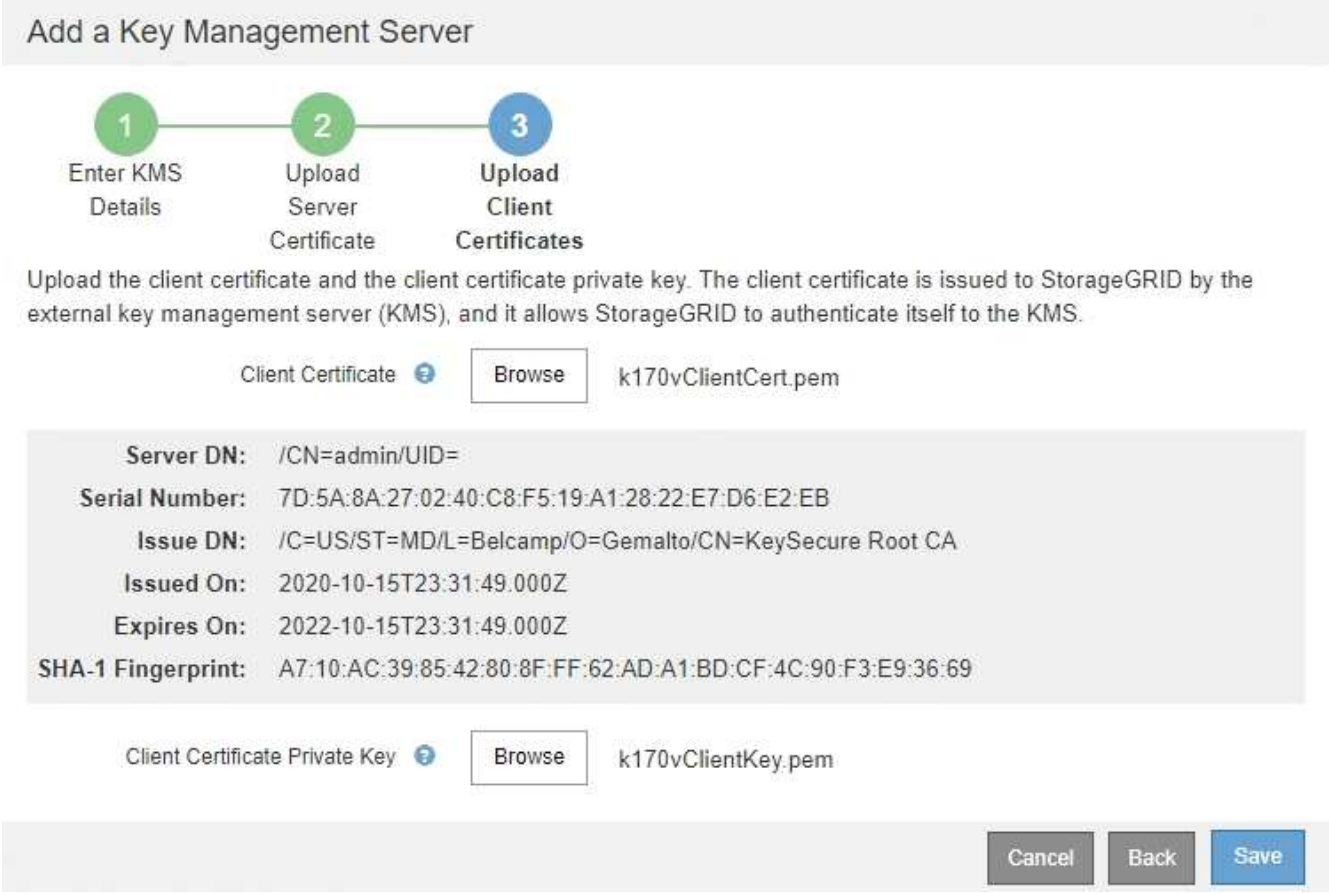


2. 클라이언트 인증서 파일을 업로드합니다.

   클라이언트 인증서 메타데이터가 나타납니다.

3. 클라이언트 인증서의 개인 키 위치를 찾습니다.
4. 개인 키 파일을 업로드합니다.

   클라이언트 인증서 및 클라이언트 인증서 개인 키에 대한 메타데이터가 나타납니다.



5. 저장 * 을 선택합니다.

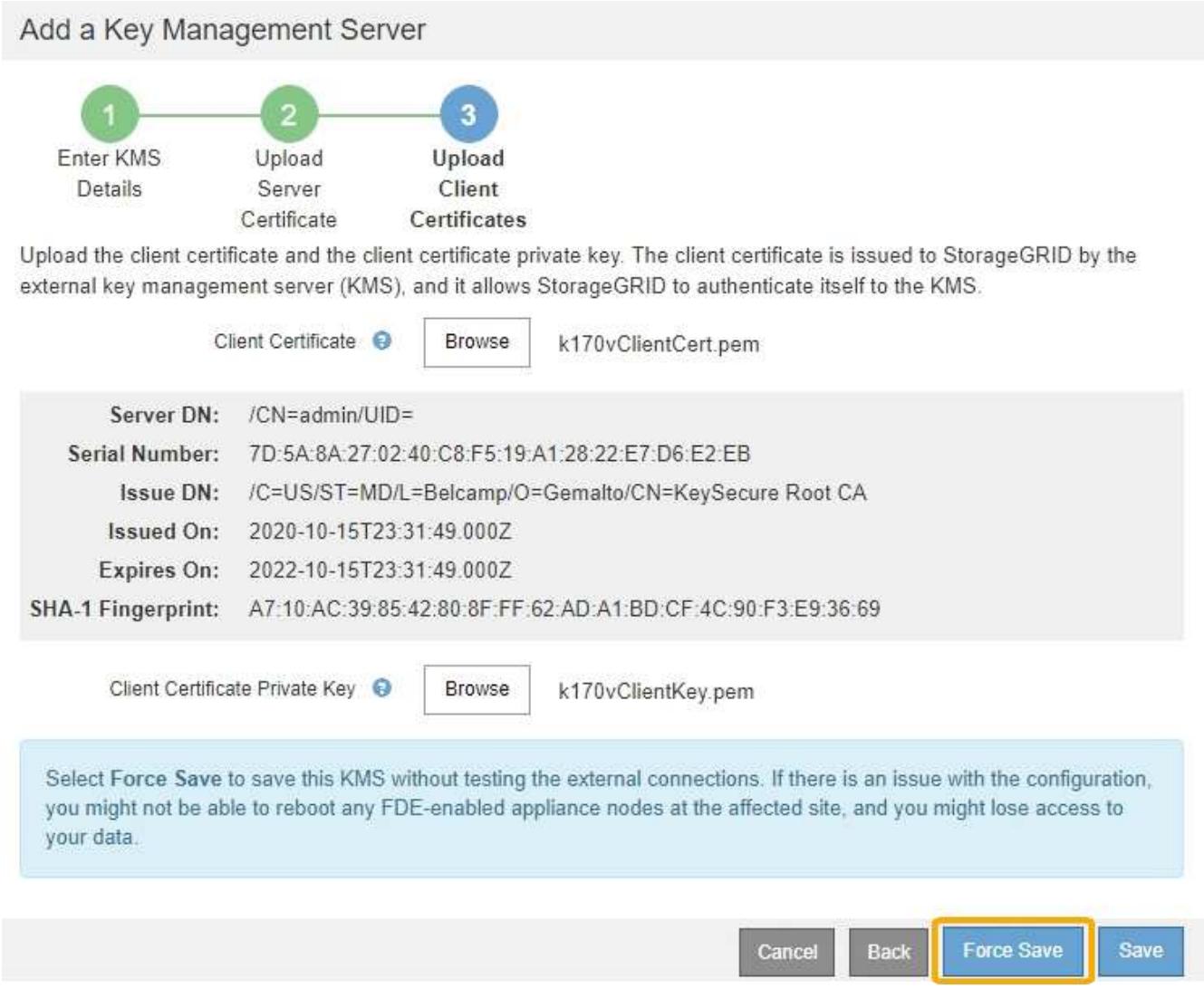
   키 관리 서버와 어플라이언스 노드 간의 연결은 테스트를 거칩니다. 모든 연결이 올바르고 KMS에서 올바른 키를 찾으면 키 관리 서버 페이지의 표에 새 키 관리 서버가 추가됩니다.

   > KMS를 추가한 직후 키 관리 서버 페이지의 인증서 상태는 알 수 없음으로 표시됩니다. 각 인증서의 실제 상태를 가져오는 데 30분 정도 StorageGRID 걸릴 수 있습니다. 현재 상태를 보려면 웹 브라우저를 새로 고쳐야 합니다.

6. 저장 * 을 선택할 때 오류 메시지가 나타나면 메시지 세부 정보를 검토한 다음 * 확인 * 을 선택합니다.

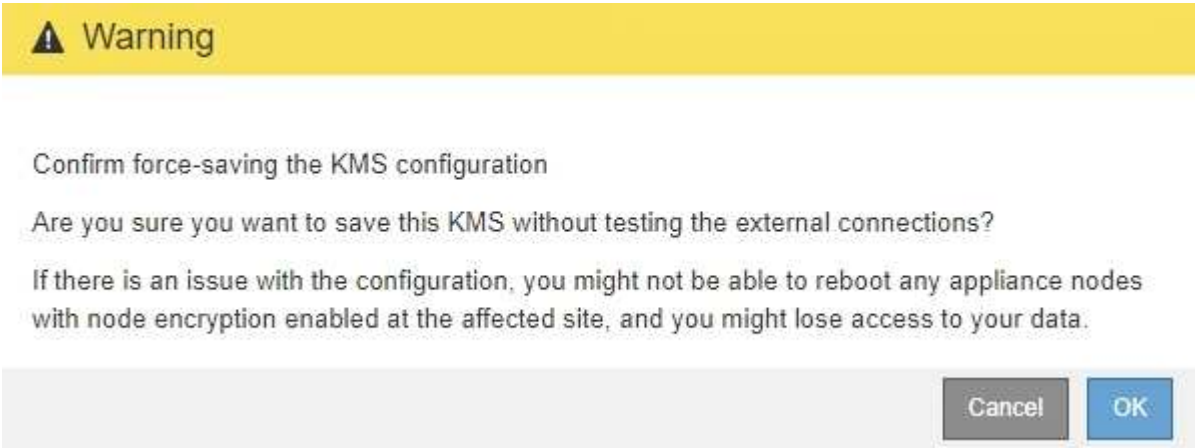
   예를 들어 연결 테스트에 실패한 경우 422:처리할 수 없는 엔터티 오류가 발생할 수 있습니다.

7. 외부 연결을 테스트하지 않고 현재 구성을 저장해야 하는 경우 * 강제 저장 * 을 선택합니다.



강제 저장 * 을 선택하면 KMS 구성이 저장되지만 각 제품에서 해당 KMS로의 외부 연결은 테스트되지 않습니다. 구성에 문제가 있을 경우 해당 사이트에서 노드 암호화가 활성화된 어플라이언스 노드를 재부팅하지 못할 수 있습니다. 문제가 해결될 때까지 데이터에 액세스하지 못할 수 있습니다.

8. 확인 경고를 검토하고 구성을 강제 저장하려면 * OK * 를 선택합니다.



KMS 구성은 저장되지만 KMS에 대한 연결은 테스트되지 않습니다.

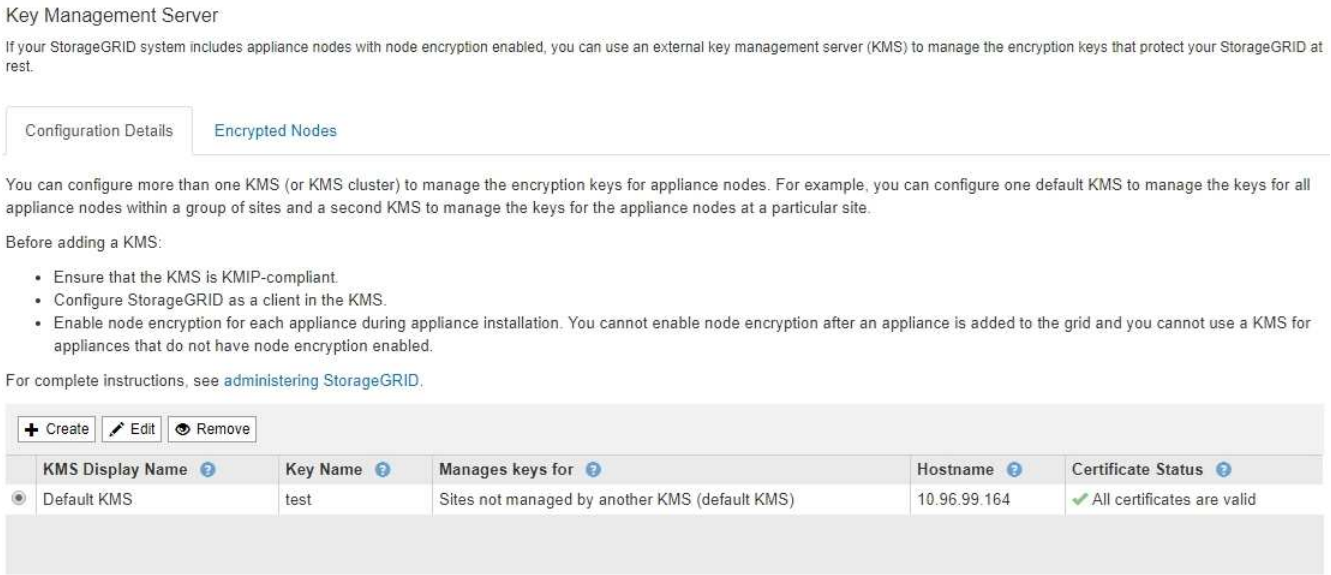
KMS 세부 정보 보기

서버 및 클라이언트 인증서의 현재 상태를 포함하여 StorageGRID 시스템의 각 키 관리 서버(KMS)에 대한 정보를 볼 수 있습니다.

단계

1. 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   키 관리 서버 페이지가 나타납니다. 구성 세부 정보 탭에는 구성된 모든 키 관리 서버가 표시됩니다.



2. 각 KMS에 대한 표의 정보를 검토합니다.

필드에 입력합니다	설명
KMS 표시 이름	KMS의 설명 이름입니다.
키 이름	KMS에서 StorageGRID 클라이언트의 키 별칭입니다.
의 키를 관리합니다	KMS와 관련된 StorageGRID 사이트 이 필드에는 특정 StorageGRID 사이트 또는 다른 KMS(기본 KMS)가 관리하지 않는 사이트의 이름이 표시됩니다.*

필드에 입력합니다	설명
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. 두 개의 키 관리 서버로 구성된 클러스터가 있는 경우 두 서버의 정규화된 도메인 이름 또는 IP 주소가 나열됩니다. 클러스터에 키 관리 서버가 두 개 이상 있는 경우 첫 번째 KMS의 정규화된 도메인 이름 또는 IP 주소가 클러스터에 있는 추가 키 관리 서버의 수와 함께 나열됩니다. 예를 들어 10.10.10.10과 10.10.10.11이나 10.10.10.10과 기타 2개 등이 있습니다. 클러스터의 모든 호스트 이름을 보려면 KMS를 선택한 다음 * 편집 * 을 선택합니다.
인증서 상태입니다	서버 인증서, 선택적 CA 인증서 및 클라이언트 인증서의 현재 상태: 유효, 만료, 만료 임박 또는 알 수 없음. • 참고: * StorageGRID 인증서 상태를 업데이트하는 데 30분 정도 걸릴 수 있습니다. 현재 값을 보려면 웹 브라우저를 새로 고쳐야 합니다.

3. 인증서 상태가 알 수 없음 인 경우 최대 30분 동안 기다린 다음 웹 브라우저를 새로 고칩니다.

> KMS를 추가한 직후 키 관리 서버 페이지의 인증서 상태는 알 수 없음으로 표시됩니다. 각 인증서의 실제 상태를 가져오는 데 30분 정도 StorageGRID 걸릴 수 있습니다. 실제 상태를 보려면 웹 브라우저를 새로 고쳐야 합니다.

4. 인증서 상태 열에 인증서가 만료되었거나 만료 시기가 임박했다는 메시지가 표시되면 가능한 한 빨리 문제를 해결하십시오.

   의 지침에 따라 * KMS CA 인증서 만료 *, * KMS 클라이언트 인증서 만료 * 및 * KMS 서버 인증서 만료 * 알림에 대한 권장 조치를 참조하십시오 StorageGRID 모니터링 및 문제 해결.

> 데이터 액세스를 유지하려면 가능한 한 빨리 인증서 문제를 해결해야 합니다.

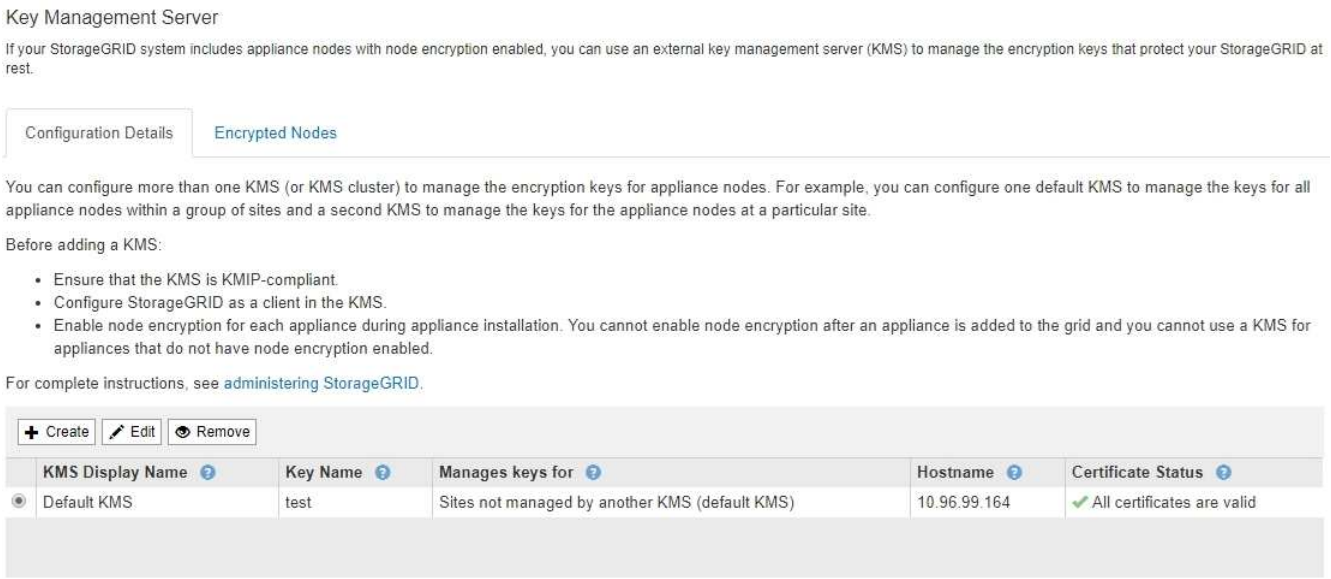
암호화된 노드를 봅니다

노드 암호화 * 설정이 활성화된 StorageGRID 시스템의 어플라이언스 노드에 대한 정보를 볼 수 있습니다.

단계

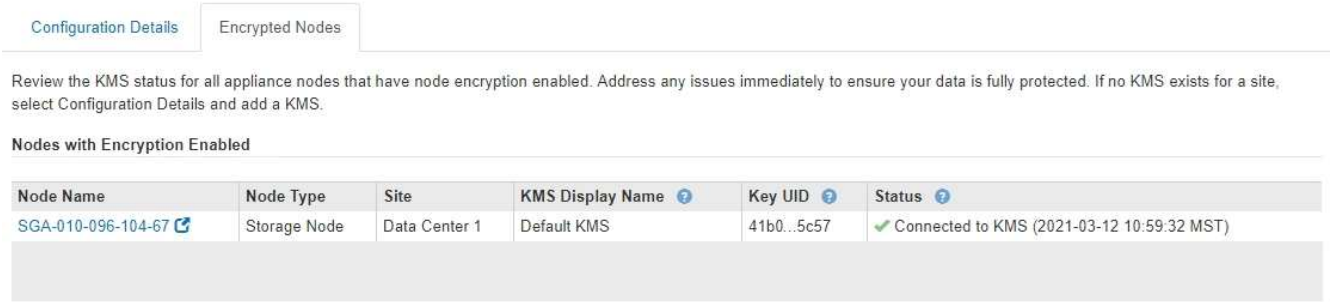
1. 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   키 관리 서버 페이지가 나타납니다. 구성 세부 정보 탭에는 구성된 모든 키 관리 서버가 표시됩니다.



2. 페이지 상단에서 * 암호화된 노드 * 탭을 선택합니다.

암호화된 노드 탭에는 * 노드 암호화 * 설정이 활성화된 StorageGRID 시스템의 어플라이언스 노드가 나열됩니다.



3. 각 어플라이언스 노드에 대해 표의 정보를 검토합니다.

열	설명
노드 이름	어플라이언스 노드의 이름입니다.
노드 유형	노드 유형: 스토리지, 관리자 또는 게이트웨이
사이트	노드가 설치된 StorageGRID 사이트의 이름입니다.

열	설명
KMS 표시 이름	노드에 사용된 KMS의 설명 이름입니다. KMS가 나열되지 않은 경우 구성 세부 정보 탭을 선택하여 KMS를 추가합니다. KMS(키 관리 서버) 추가
키 UID	어플라이언스 노드에서 데이터를 암호화하고 해독하는 데 사용되는 암호화 키의 고유 ID입니다. 전체 키 UID를 보려면 셀 위로 커서를 이동합니다. 대시(--)는 어플라이언스 노드와 KMS 사이의 연결 문제로 인해 키 UID를 알 수 없음을 나타냅니다.
상태	KMS와 어플라이언스 노드 간의 연결 상태입니다. 노드가 연결되어 있으면 타임스탬프가 30분마다 업데이트됩니다. KMS 구성이 변경된 후 연결 상태를 업데이트하는 데 몇 분 정도 걸릴 수 있습니다. • 참고: * 새 값을 보려면 웹 브라우저를 새로 고쳐야 합니다.

4. 상태 열에 KMS 문제가 표시되면 즉시 문제를 해결하십시오.

   KMS가 정상적으로 작동하는 동안 KMS*에 연결됨 상태로 표시됩니다. 노드가 그리드에서 연결이 끊어지면 노드 연결 상태가 표시됩니다(관리자 다운 또는 알 수 없음).

   다른 상태 메시지는 이름이 같은 StorageGRID 알림에 해당합니다.

   - KMS 구성을 로드하지 못했습니다
   - KMS 연결 오류입니다
   - KMS 암호화 키 이름을 찾을 수 없습니다
   - KMS 암호화 키 회전이 실패했습니다
   - 킬로미터 키가 어플라이언스 볼륨을 해독하지 못했습니다
   - KMS가 구성되지 않았습니다

   의 지침에 따라 이러한 경고에 대한 권장 조치를 참조하십시오 StorageGRID 모니터링 및 문제 해결.

   데이터를 완벽하게 보호하려면 모든 문제를 즉시 해결해야 합니다.

KMS(키 관리 서버**)** 편집

예를 들어 인증서가 곧 만료될 경우 키 관리 서버의 구성을 편집해야 할 수 있습니다.

필요한 것

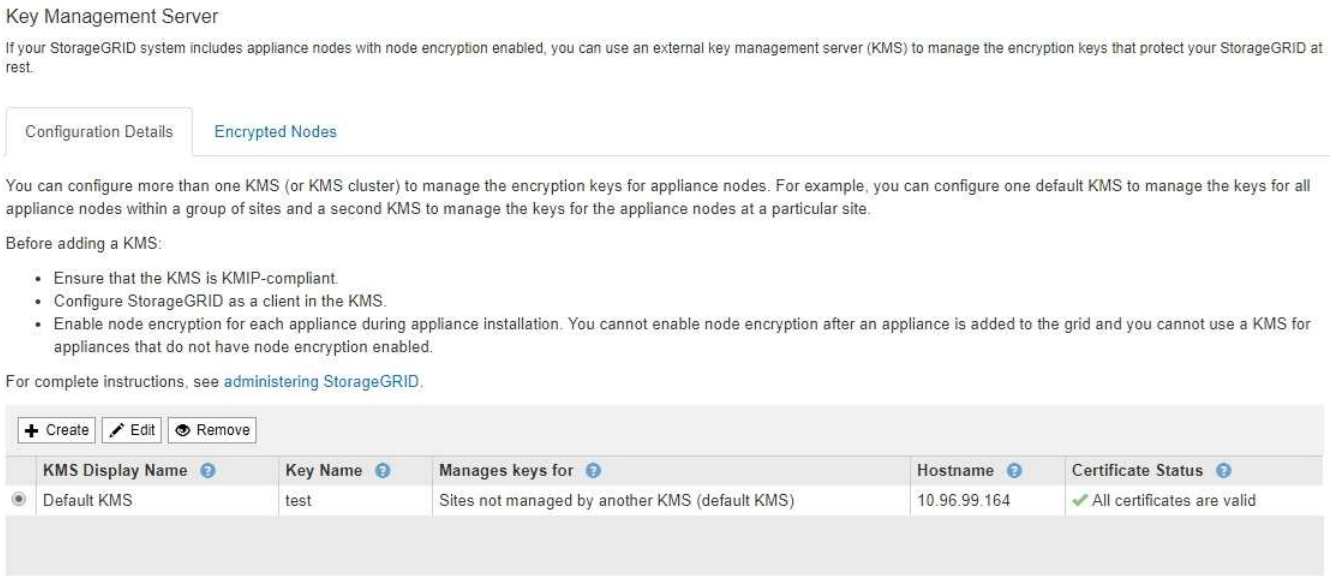
- 을(를) 검토했습니다 키 관리 서버 사용에 대한 고려 사항 및 요구 사항.
- KMS에 대해 선택한 사이트를 업데이트할 계획이라면 을 검토했습니다 사이트의 KMS를 변경할 때의 고려 사항.

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.

단계

1. 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   Key Management Server 페이지가 나타나고 구성된 모든 키 관리 서버가 표시됩니다.



2. 편집할 KMS를 선택하고 * 편집 * 을 선택합니다.
3. 필요한 경우 키 관리 서버 편집 마법사의 * 1단계(KMS 세부 정보 입력) * 에 있는 세부 정보를 업데이트합니다.

필드에 입력합니다	설명
KMS 표시 이름	이 KMS를 식별하는 데 도움이 되는 설명 이름입니다. 1자에서 64자 사이여야 합니다.
키 이름	KMS에서 StorageGRID 클라이언트에 대한 정확한 키 별칭입니다. 1자에서 255자 사이여야 합니다. 키 이름은 드문 경우지만 편집하면 됩니다. 예를 들어, KMS에서 별칭의 이름이 바뀌거나 이전 키의 모든 버전이 새 별칭의 버전 기록으로 복사된 경우 키 이름을 편집해야 합니다. KMS의 키 이름(별칭)을 변경하여 키를 회전하려고 하지 마십시오. 대신 KMS 소프트웨어의 키 버전을 업데이트하여 키를 돌리십시오. StorageGRID를 사용하려면 KMS에서 동일한 키 별칭을 사용하여 이전에 사용한 모든 키 버전과 향후 모든 키 버전에 액세스할 수 있어야 합니다. 구성된 KMS의 키 별칭을 변경하면 StorageGRID에서 데이터의 암호를 해독하지 못할 수 있습니다. 키 관리 서버 사용에 대한 고려 사항 및 요구 사항

필드에 입력합니다	설명
의 키를 관리합니다	사이트별 KMS를 편집하고 있고 기본 KMS가 아직 없는 경우 선택적으로 * 다른 KMS에 의해 관리되지 않는 사이트(기본 KMS) * 를 선택합니다. 이 항목을 선택하면 사이트별 KMS가 기본 KMS로 변환되며, 이 KMS는 전용 KMS가 없는 모든 사이트와 확장 시 추가된 사이트에 적용됩니다. • 참고: * 사이트별 KMS를 편집하는 경우에는 다른 사이트를 선택할 수 없습니다. 기본 KMS를 편집하는 경우 특정 사이트를 선택할 수 없습니다.
포트	KMS 서버가 KMIP(Key Management Interoperability Protocol) 통신에 사용하는 포트입니다. 기본값은 5696으로, KMIP 표준 포트입니다.
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. • 참고: * 서버 인증서의 SAN 필드에는 여기에 입력한 FQDN 또는 IP 주소가 포함되어야 합니다. 그렇지 않으면 StorageGRID는 KMS 또는 KMS 클러스터의 모든 서버에 연결할 수 없습니다.

4. KMS 클러스터를 구성하는 경우 더하기 기호를 선택합니다 ✚ 클러스터에 있는 각 서버의 호스트 이름을 추가합니다.
5. 다음 * 을 선택합니다.

   키 관리 서버 편집 마법사의 2단계(서버 인증서 업로드)가 나타납니다.

6. 서버 인증서를 교체해야 하는 경우 * 찾아보기 * 를 선택하고 새 파일을 업로드합니다.
7. 다음 * 을 선택합니다.

   키 관리 서버 편집 마법사의 3단계(클라이언트 인증서 업로드)가 나타납니다.

8. 클라이언트 인증서와 클라이언트 인증서 개인 키를 교체해야 하는 경우 * 찾아보기 * 를 선택하고 새 파일을 업로드합니다.
9. 저장 * 을 선택합니다.

   영향을 받는 사이트에서 키 관리 서버와 모든 노드 암호화 어플라이언스 노드 간의 연결을 테스트합니다. 모든 노드 연결이 유효하고 KMS에서 올바른 키를 찾으면 키 관리 서버가 키 관리 서버 페이지의 테이블에 추가됩니다.

10. 오류 메시지가 나타나면 메시지 세부 정보를 검토하고 * OK * 를 선택합니다.

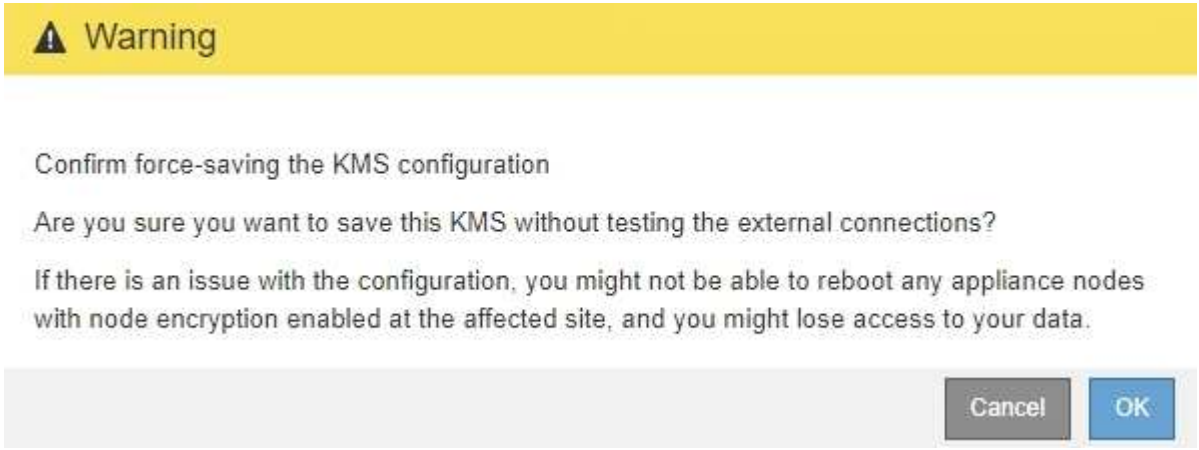
    예를 들어, 이 KMS에 대해 선택한 사이트가 다른 KMS에 의해 이미 관리되고 있거나 연결 테스트에 실패한 경우 422:처리할 수 없는 엔터티 오류가 발생할 수 있습니다.

11. 연결 오류를 해결하기 전에 현재 설정을 저장해야 하는 경우 * 강제 저장 * 을 선택합니다.

> ⓘ 강제 저장 * 을 선택하면 KMS 구성이 저장되지만 각 제품에서 해당 KMS로의 외부 연결은 테스트되지 않습니다. 구성에 문제가 있을 경우 해당 사이트에서 노드 암호화가 활성화된 어플라이언스 노드를 재부팅하지 못할 수 있습니다. 문제가 해결될 때까지 데이터에 액세스하지 못할 수 있습니다.

KMS 구성이 저장됩니다.

12. 확인 경고를 검토하고 구성을 강제 저장하려면 * OK * 를 선택합니다.



KMS 구성은 저장되지만 KMS에 대한 연결은 테스트되지 않습니다.

KMS(키 관리 서버**)** 제거

경우에 따라 키 관리 서버를 제거할 수 있습니다. 예를 들어 사이트를 해체한 경우 사이트별 KMS를 제거할 수 있습니다.

필요한 것

- 을(를) 검토했습니다 키 관리 서버 사용에 대한 고려 사항 및 요구 사항.
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.

이 작업에 대해

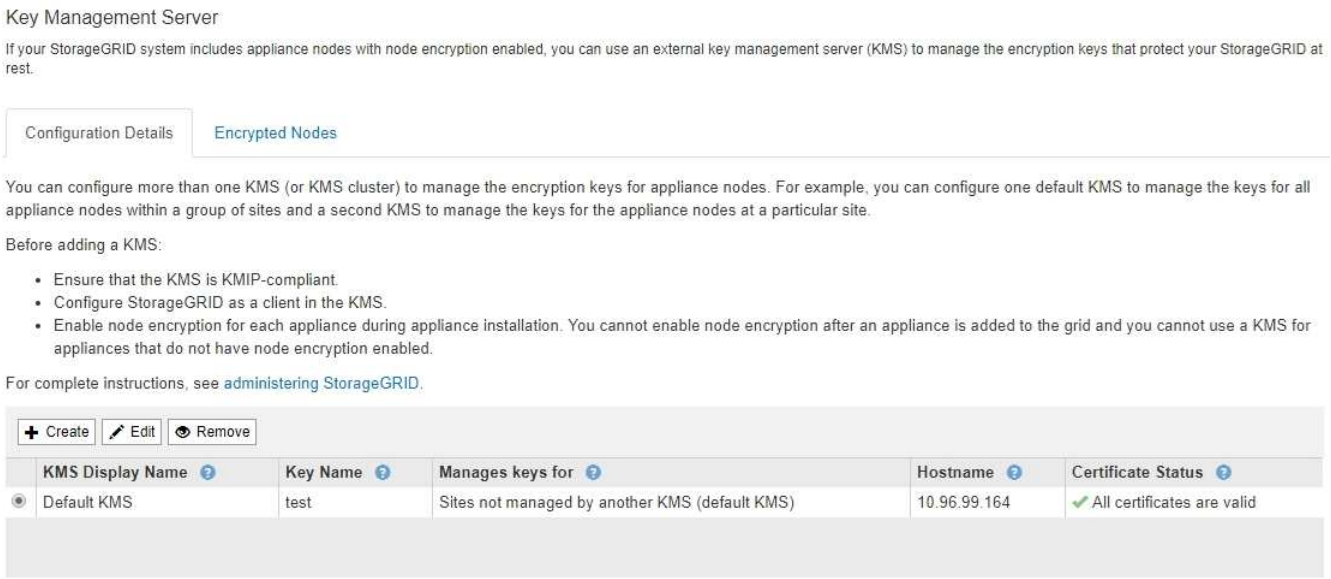
다음과 같은 경우 KMS를 제거할 수 있습니다.

- 사이트를 폐기했거나 사이트에 노드 암호화가 활성화된 어플라이언스 노드가 없는 경우 사이트별 KMS를 제거할 수 있습니다.
- 노드 암호화가 활성화된 어플라이언스 노드가 있는 각 사이트에 대해 사이트별 KMS가 이미 있는 경우 기본 KMS를 제거할 수 있습니다.

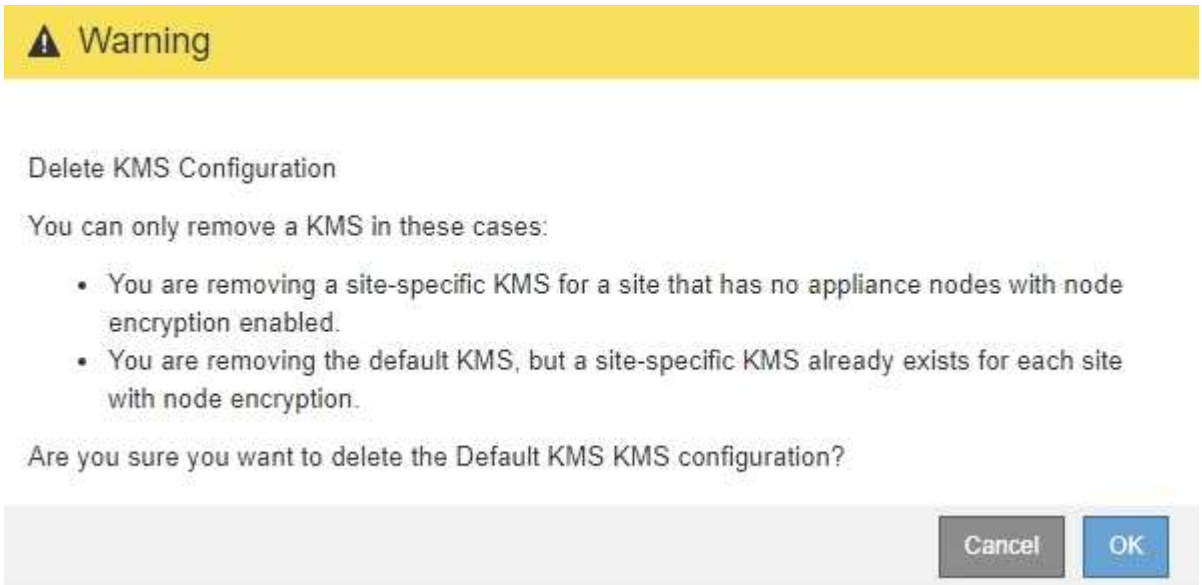
단계

1. 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   Key Management Server 페이지가 나타나고 구성된 모든 키 관리 서버가 표시됩니다.



2. 제거할 KMS의 라디오 단추를 선택하고 * 제거 * 를 선택합니다.
3. 경고 대화 상자에서 고려 사항을 검토합니다.



4. OK * 를 선택합니다.

   KMS 구성이 제거되었습니다.

프록시 설정을 관리합니다

스토리지 프록시 설정을 구성합니다

플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 스토리지 노드와 외부 S3 엔드포인트 간에 투명하지 않은 프록시를 구성할 수 있습니다. 예를 들어, 플랫폼 서비스 메시지를 인터넷의 끝점과 같은 외부 끝점으로 보내려면 투명하지 않은 프록시가 필요할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

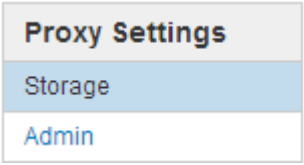
이 작업에 대해

단일 스토리지 프록시에 대한 설정을 구성할 수 있습니다.

단계

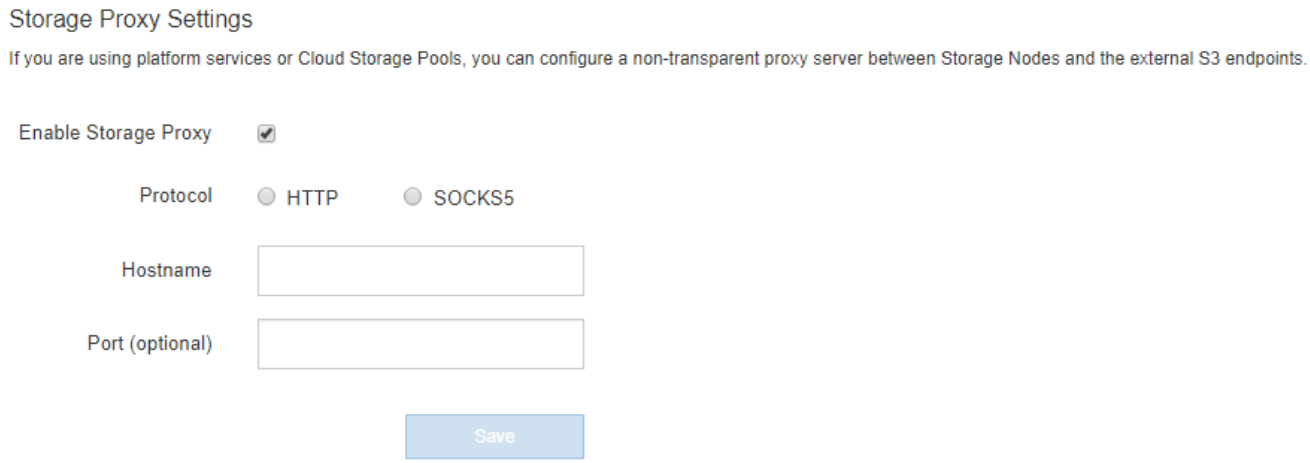
1. 구성 * > * 보안 * > * 프록시 설정 * 을 선택합니다.

   스토리지 프록시 설정 페이지가 나타납니다. 기본적으로 보조 아이콘 메뉴에서 * 스토리지 * 가 선택됩니다.



2. 스토리지 프록시 사용 * 확인란을 선택합니다.

   스토리지 프록시 구성에 대한 필드가 나타납니다.



3. 투명하지 않은 스토리지 프록시에 대한 프로토콜을 선택합니다.
4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. 필요에 따라 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.

   프로토콜의 기본 포트(HTTP의 경우 80, SOCKS5의 경우 1080)를 사용하는 경우 이 필드를 비워 둘 수 있습니다.

6. 저장 * 을 선택합니다.

   스토리지 프록시를 저장한 후 플랫폼 서비스 또는 클라우드 스토리지 풀의 새 엔드포인트를 구성 및 테스트할 수 있습니다.

   > 프록시 변경 사항이 적용되려면 최대 10분이 소요될 수 있습니다.

7. 프록시 서버의 설정을 확인하여 StorageGRID의 플랫폼 서비스 관련 메시지가 차단되지 않는지 확인합니다.

작업을 마친 후

스토리지 프록시를 비활성화해야 하는 경우 * 스토리지 프록시 사용 * 확인란의 선택을 취소하고 * 저장 * 을 선택합니다.

관련 정보

- 플랫폼 서비스를 위한 네트워크 및 포트
- ILM을 사용하여 개체를 관리합니다

관리자 프록시 설정을 구성합니다

HTTP 또는 HTTPS를 사용하여 AutoSupport 메시지를 보내는 경우(참조 AutoSupport를 구성합니다)에서 관리자 노드와 기술 지원(AutoSupport) 간에 투명하지 않은 프록시 서버를 구성할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

이 작업에 대해

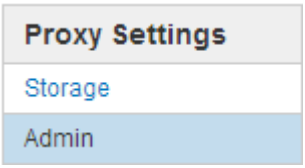
단일 관리 프록시에 대한 설정을 구성할 수 있습니다.

단계

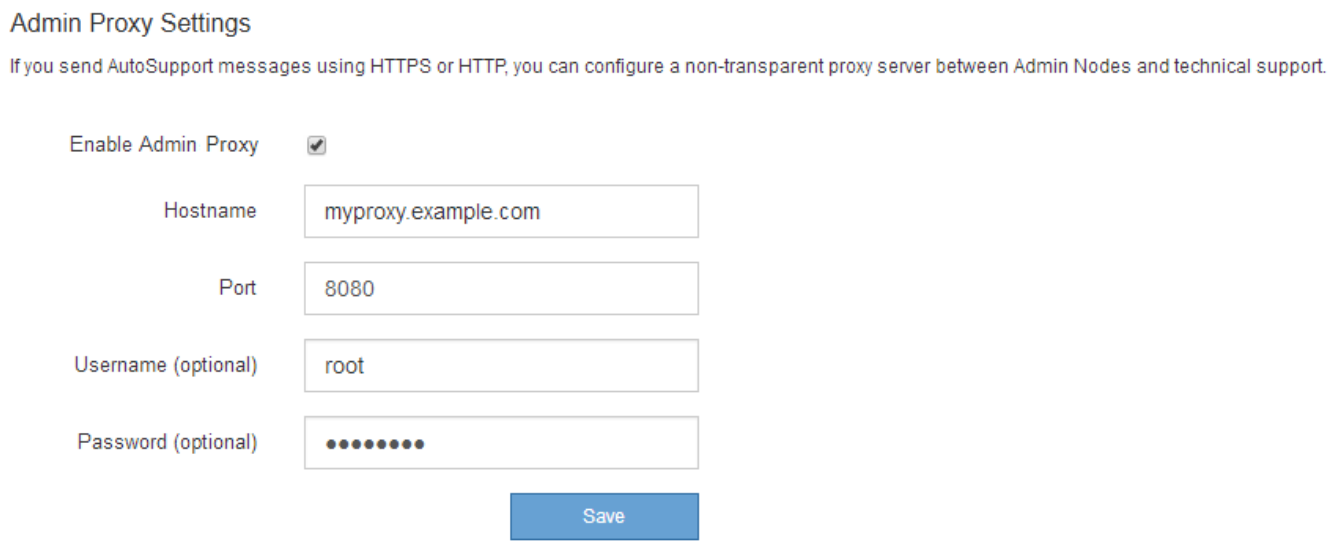
1. 구성 * > * 보안 * > * 프록시 설정 * 을 선택합니다.

   관리자 프록시 설정 페이지가 나타납니다. 기본적으로 보조 아이콘 메뉴에서 * 스토리지 * 가 선택됩니다.

2. 측면 표시줄 메뉴에서 * Admin * 을 선택합니다.



3. 관리자 프록시 사용 * 확인란을 선택합니다.



4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.
6. 필요에 따라 프록시 사용자 이름을 입력합니다.

   프록시 서버에 사용자 이름이 필요하지 않은 경우 이 필드를 비워 둡니다.

7. 필요에 따라 프록시 암호를 입력합니다.

   프록시 서버에 암호가 필요하지 않은 경우 이 필드를 비워 둡니다.

8. 저장 * 을 선택합니다.

   관리자 프록시가 저장되면 관리 노드와 기술 지원 사이의 프록시 서버가 구성됩니다.

   프록시 변경 사항이 적용되려면 최대 10분이 소요될 수 있습니다.

9. 프록시를 비활성화해야 하는 경우 * 관리자 프록시 사용 * 확인란의 선택을 취소하고 * 저장 * 을 선택합니다.

신뢰할 수 없는 클라이언트 네트워크를 관리합니다

신뢰할 수 없는 클라이언트 네트워크 관리: 개요

클라이언트 네트워크를 사용하는 경우 명시적으로 구성된 끝점에서만 인바운드 클라이언트 트래픽을 허용하여 악의적인 공격으로부터 StorageGRID를 보호할 수 있습니다.

기본적으로 각 그리드 노드의 클라이언트 네트워크는 _ trusted _ 입니다. 즉, 기본적으로 StorageGRID는 사용 가능한 모든 외부 포트의 각 그리드 노드에 대한 인바운드 연결을 신뢰합니다(의 외부 통신에 대한 정보 참조) 네트워킹 지침)를 클릭합니다.

각 노드의 클라이언트 네트워크가 _untrusted_로 지정함으로써 StorageGRID 시스템에 대한 악의적인 공격의 위협을 줄일 수 있습니다. 노드의 클라이언트 네트워크를 신뢰할 수 없는 경우 노드는 로드 밸런서 끝점으로 명시적으로 구성된 포트의 인바운드 연결만 허용합니다. 을 참조하십시오 로드 밸런서 엔드포인트를 구성합니다.

예 **1:** 게이트웨이 노드는 **HTTPS S3** 요청만 허용합니다

게이트웨이 노드가 HTTPS S3 요청을 제외한 클라이언트 네트워크의 모든 인바운드 트래픽을 거부하도록 한다고 가정합니다. 다음과 같은 일반 단계를 수행합니다.

1. 로드 밸런서 엔드포인트 페이지에서 포트 443에서 HTTPS를 통해 S3에 대한 로드 밸런서 끝점을 구성합니다.
2. 신뢰할 수 없는 클라이언트 네트워크 페이지에서 게이트웨이 노드의 클라이언트 네트워크를 신뢰할 수 없도록 지정합니다.

구성을 저장한 후 게이트웨이 노드의 클라이언트 네트워크의 모든 인바운드 트래픽은 포트 443 및 ICMP 에코(ping) 요청의 HTTPS S3 요청을 제외하고 삭제됩니다.

예 **2:** 스토리지 노드가 **S3** 플랫폼 서비스 요청을 전송합니다

스토리지 노드에서 아웃바운드 S3 플랫폼 서비스 트래픽을 활성화하되 클라이언트 네트워크의 해당 스토리지 노드에 대한 인바운드 연결을 차단하려는 경우를 가정해 봅니다. 이 일반 단계를 수행합니다.

- 신뢰할 수 없는 클라이언트 네트워크 페이지에서 스토리지 노드의 클라이언트 네트워크를 신뢰할 수 없음을 나타냅니다.

구성을 저장한 후 스토리지 노드는 더 이상 클라이언트 네트워크에서 들어오는 트래픽을 허용하지 않지만 Amazon Web Services에 대한 아웃바운드 요청은 계속 허용합니다.

노드의 클라이언트 네트워크를 신뢰할 수 없습니다

클라이언트 네트워크를 사용하는 경우 각 노드의 클라이언트 네트워크를 신뢰할 수 있는지 신뢰할 수 없는지 여부를 지정할 수 있습니다. 또한 확장에 추가된 새 노드의 기본 설정을 지정할 수도 있습니다.

필요한 것

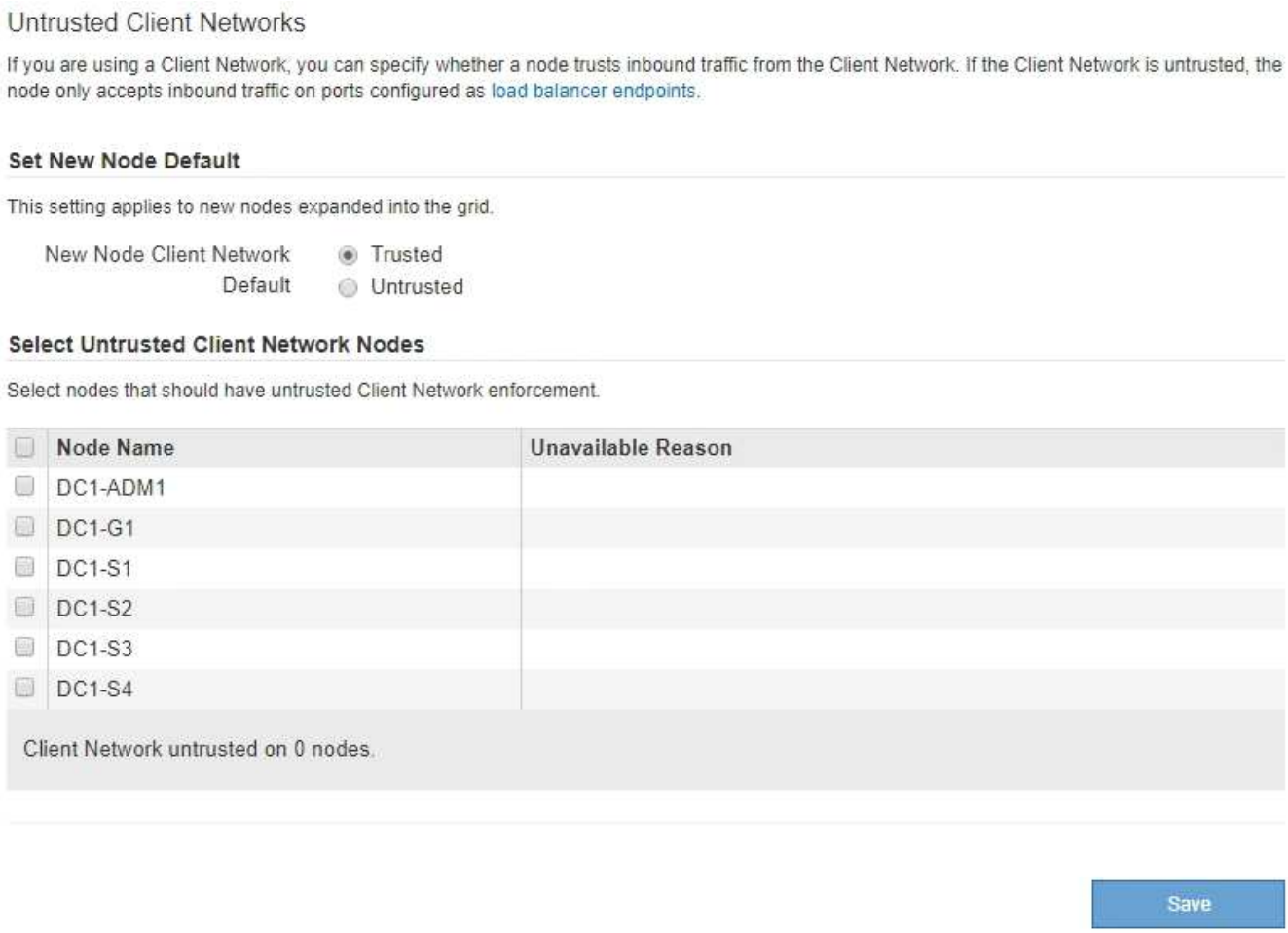
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.
- 관리자 노드 또는 게이트웨이 노드가 명시적으로 구성된 끝점에서만 인바운드 트래픽을 수락하도록 하려면 로드 밸런서 끝점을 정의해야 합니다.

> 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 신뢰할 수 없는 클라이언트 네트워크 * 를 선택합니다.

   신뢰할 수 없는 클라이언트 네트워크 페이지에는 StorageGRID 시스템의 모든 노드가 나열됩니다. 노드의 클라이언트 네트워크를 신뢰할 수 있어야 하는 경우 사용할 수 없는 이유 열에 항목이 포함됩니다.



2. 새 노드 기본값 설정 * 섹션에서 확장 절차에서 그리드에 새 노드를 추가할 때 기본 설정을 지정합니다.
   - * 신뢰 *: 확장 시 노드가 추가되면 해당 클라이언트 네트워크를 신뢰할 수 있습니다.
   - * 신뢰할 수 없음 *: 확장 시 노드가 추가되면 해당 클라이언트 네트워크를 신뢰할 수 없습니다. 필요에 따라 이 페이지로 돌아가 특정 새 노드의 설정을 변경할 수 있습니다.

     이 설정은 StorageGRID 시스템의 기존 노드에는 영향을 주지 않습니다.

3. 신뢰할 수 없는 클라이언트 네트워크 노드 선택 * 섹션에서 명시적으로 구성된 로드 밸런서 끝점에서만 클라이언트 연결을 허용할 노드를 선택합니다.

   제목에서 확인란을 선택하거나 선택 취소하여 모든 노드를 선택하거나 선택 취소할 수 있습니다.

4. 저장 * 을 선택합니다.

   새 방화벽 규칙이 즉시 추가되고 적용됩니다. 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

테넌트 관리

테넌트 관리

그리드 관리자는 S3 및 Swift 클라이언트가 StorageGRID 시스템을 사용하여 오브젝트를 저장

및 검색하고, 스토리지 사용량을 모니터링하고, 클라이언트가 수행할 수 있는 작업을 관리하는 데 사용하는 테넌트 계정을 생성하고 관리합니다.

테넌트 계정이란 무엇입니까?

테넌트 계정을 사용하면 S3(Simple Storage Service) REST API 또는 Swift REST API를 사용하는 클라이언트 애플리케이션이 StorageGRID에 개체를 저장하고 검색할 수 있습니다.

각 테넌트 계정은 계정을 생성할 때 지정하는 단일 프로토콜 사용을 지원합니다. 두 프로토콜을 모두 사용하는 StorageGRID 시스템에 오브젝트를 저장하고 검색하려면 S3 버킷 및 오브젝트, Swift 컨테이너 및 오브젝트, 두 개의 테넌트 계정을 만들어야 합니다. 각 테넌트 계정에는 고유한 계정 ID, 인증된 그룹 및 사용자, 버킷 또는 컨테이너 및 객체가 있습니다.

필요에 따라 시스템에 저장된 객체를 다른 엔터티로 분리하려는 경우 추가 테넌트 계정을 생성할 수 있습니다. 예를 들어, 다음과 같은 사용 사례에서 여러 테넌트 계정을 설정할 수 있습니다.

- * 기업 활용 사례: * 엔터프라이즈 애플리케이션에서 StorageGRID 시스템을 관리하는 경우 조직의 여러 부서에서 그리드의 객체 스토리지를 분리할 수 있습니다. 이 경우 마케팅 부서, 고객 지원 부서, 인사 부서 등에 대한 테넌트 계정을 만들 수 있습니다.

  > S3 클라이언트 프로토콜을 사용하는 경우 S3 버킷 및 버킷 정책을 사용하여 엔터프라이즈의 부서 간에 오브젝트를 분리할 수 있습니다. 테넌트 계정은 사용할 필요가 없습니다. 자세한 내용은 S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

- * 서비스 공급자 활용 사례: * StorageGRID 시스템을 서비스 공급자로 관리하는 경우 그리드의 객체 스토리지를 그리드의 스토리지를 임대할 다른 엔터티로 분리할 수 있습니다. 이 경우 회사 A, 회사 B, 회사 C 등에 대한 테넌트 계정을 생성합니다.

테넌트 계정을 생성하고 구성합니다

테넌트 계정을 생성할 때 다음 정보를 지정합니다.

- 테넌트 계정의 표시 이름입니다.
- 테넌트 계정(S3 또는 Swift)에서 사용할 클라이언트 프로토콜입니다.
- S3 테넌트 계정의 경우: 테넌트 계정에 S3 버킷을 포함하는 플랫폼 서비스를 사용할 수 있는 권한이 있는지 여부 테넌트 계정에서 플랫폼 서비스를 사용하도록 허용하는 경우 해당 사용자의 사용을 지원하도록 그리드가 구성되어 있는지 확인해야 합니다. "플랫폼 서비스"를 참조하십시오.
- 필요한 경우 테넌트 계정의 스토리지 할당량 — 테넌트의 객체에 사용할 수 있는 최대 GB, 테라바이트 또는 PB입니다. 할당량이 초과되면 테넌트가 새 객체를 생성할 수 없습니다.

  > 테넌트의 스토리지 할당량은 물리적 크기(디스크 크기)가 아닌 논리적 양(오브젝트 크기)을 나타냅니다.

- StorageGRID 시스템에 대해 ID 페더레이션이 설정된 경우 테넌트 계정을 구성할 수 있는 루트 액세스 권한이 있는 통합 그룹입니다.
- StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하지 않는 경우 테넌트 계정이 자체 ID 소스를 사용할지 또는 그리드의 ID 소스를 공유할지 여부 및 테넌트의 로컬 루트 사용자의 초기 암호를 공유할지 여부

테넌트 계정이 생성된 후 다음 작업을 수행할 수 있습니다.

- * GRID용 플랫폼 서비스 관리 *: 테넌트 계정에 대해 플랫폼 서비스를 사용하는 경우, 플랫폼 서비스 메시지가 전달되는 방법과 StorageGRID 배포에서 플랫폼 서비스를 사용하는 데 필요한 네트워킹 요구 사항을 이해해야 합니다.
- * 테넌트 계정의 스토리지 사용량 모니터링 *: 테넌트가 해당 계정을 사용하기 시작한 후 Grid Manager를 사용하여 각 테넌트가 사용하는 스토리지 양을 모니터링할 수 있습니다.

  > 노드가 그리드의 다른 노드로부터 격리되면 테넌트의 스토리지 사용량 값이 최신 상태가 아닐 수 있습니다. 네트워크 연결이 복원되면 합계가 업데이트됩니다.

  테넌트에 대해 할당량을 설정한 경우 * 테넌트 할당량 사용량 높음 * 알림을 설정하여 테넌트가 할당량을 사용하고 있는지 확인할 수 있습니다. 활성화된 경우 테넌트가 할당량의 90%를 사용한 경우 이 경고가 트리거됩니다. 자세한 내용은 StorageGRID 모니터링 및 문제 해결 설명서의 경고 참조를 참조하십시오.

- * 클라이언트 작업 구성 *: 일부 클라이언트 작업이 금지되는지 여부를 구성할 수 있습니다.

S3 테넌트를 구성합니다

S3 테넌트 계정이 생성된 후 테넌트 사용자는 테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 통합을 설정하고(ID 소스를 그리드와 공유하지 않는 경우) 로컬 그룹 및 사용자를 생성합니다
- S3 액세스 키 관리
- S3 버킷 생성 및 관리
- 스토리지 사용량 모니터링
- 플랫폼 서비스 사용(활성화된 경우)

> S3 테넌트 사용자는 테넌트 관리자를 사용하여 S3 액세스 키 및 버킷을 생성 및 관리할 수 있지만, S3 클라이언트 애플리케이션을 사용하여 오브젝트를 수집 및 관리해야 합니다.

Swift 테넌트를 구성합니다

Swift 테넌트 계정이 생성된 후 테넌트의 루트 사용자는 테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 통합을 설정하고(ID 소스를 그리드와 공유하지 않는 경우) 로컬 그룹 및 사용자를 만듭니다
- 스토리지 사용량 모니터링

> Swift 사용자는 테넌트 관리자에 액세스하려면 루트 액세스 권한이 있어야 합니다. 그러나 루트 액세스 권한은 사용자가 Swift REST API에 인증하여 컨테이너를 생성하고 객체를 수집하는 것을 허용하지 않습니다. 사용자는 Swift REST API에 인증할 수 있는 Swift 관리자 권한이 있어야 합니다.

관련 정보

테넌트 계정을 사용합니다

테넌트 계정을 생성합니다

StorageGRID 시스템의 스토리지에 대한 액세스를 제어하려면 하나 이상의 테넌트 계정을 생성해야 합니다.

테넌트 계정을 생성할 때 이름, 클라이언트 프로토콜 및 선택적으로 스토리지 할당량을 지정합니다. StorageGRID에 대해 SSO(Single Sign-On)를 사용하는 경우 테넌트 계정을 구성할 루트 액세스 권한이 있는 통합 그룹도 지정합니다. StorageGRID에서 SSO(Single Sign-On)를 사용하지 않는 경우 테넌트 계정에서 자체 ID 소스를 사용할지 여부를 지정하고 테넌트의 로컬 루트 사용자에 대한 초기 암호를 구성해야 합니다.

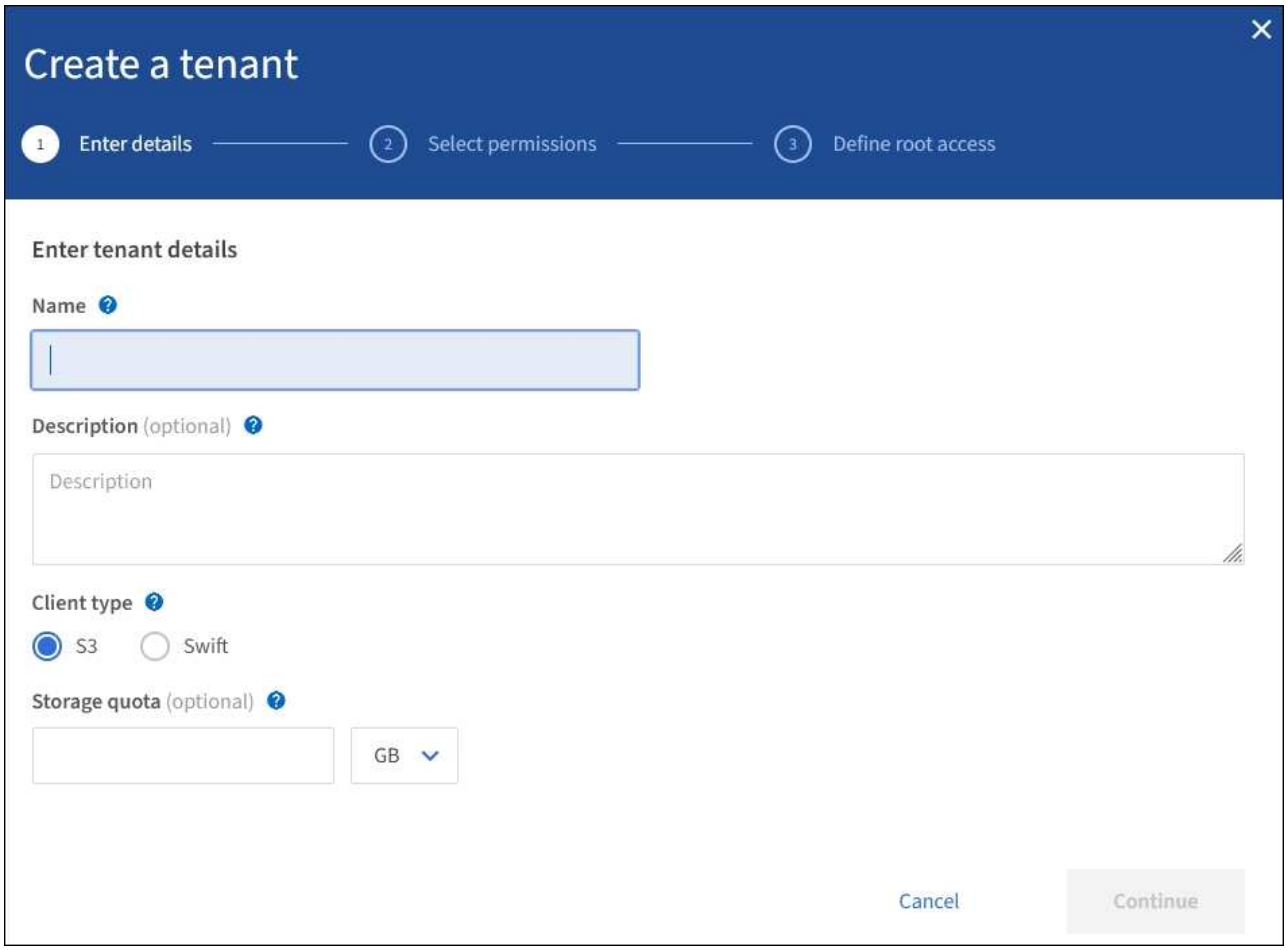
Grid Manager는 테넌트 계정 생성 단계를 안내하는 마법사를 제공합니다. 단계는 에 따라 다릅니다 ID 제휴 및 SSO(Single Sign-On) 테넌트 계정을 만드는 데 사용하는 Grid Manager 계정이 루트 액세스 권한이 있는 관리자 그룹에 속하는지 여부 및 가 구성됩니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- 테넌트 계정에서 Grid Manager에 대해 구성된 ID 소스를 사용하고 테넌트 계정에 대한 루트 액세스 권한을 통합 그룹에 부여하려는 경우 해당 통합 그룹을 Grid Manager로 가져온 것입니다. 이 관리 그룹에 그리드 관리자 권한을 할당할 필요는 없습니다. 를 참조하십시오 관리 그룹 관리 지침.

단계

1. Tenants * 를 선택합니다.
2. Create * 를 선택하고 테넌트에 대해 다음 정보를 입력합니다.
   a. * 이름 *: 테넌트 계정의 이름을 입력합니다. 테넌트 이름은 고유해야 할 필요가 없습니다. 테넌트 계정이 생성되면 고유한 숫자 계정 ID를 받습니다.
   b. * Description * (선택 사항): 테넌트를 식별하는 데 도움이 되는 설명을 입력합니다.
   c. * 클라이언트 유형 *: * S3 * 또는 * Swift * 의 클라이언트 유형을 선택합니다.
   d. * 스토리지 할당량 * (선택 사항): 이 테넌트에 스토리지 할당량을 지정하려면 할당량에 대한 숫자 값을 입력하고 올바른 단위(GB, TB 또는 PB)를 선택합니다.



3. 계속 * 을 선택하고 S3 또는 Swift 테넌트를 구성합니다.

S3 테넌트

테넌트에 대한 적절한 권한을 선택합니다. 이러한 권한 중 일부는 추가 요구 사항이 있습니다. 자세한 내용은 각 권한에 대한 온라인 도움말을 참조하십시오.

- 플랫폼 서비스를 허용합니다
- 자체 ID 소스 사용(SSO를 사용하지 않는 경우에만 선택 가능)
- S3 선택 허용(참조 관리 S3 테넌트 계정에 대해 선택)

Swift 테넌트

테넌트가 자체 ID 소스를 사용할 경우 * 고유 ID 소스 사용 * 을 선택합니다(SSO를 사용하지 않는 경우에만 선택 가능).

1. Continue * 를 선택하고 테넌트 계정에 대한 루트 액세스를 정의합니다.

ID 페더레이션이 구성되지 않았습니다

1. 로컬 루트 사용자의 암호를 입력합니다.
2. 테넌트 생성 * 을 선택합니다.

SSO가 활성화되었습니다

StorageGRID에 대해 SSO가 활성화된 경우 테넌트는 그리드 관리자에 대해 구성된 ID 소스를 사용해야 합니다. 로컬 사용자는 로그인할 수 없습니다. 테넌트 계정을 구성할 루트 액세스 권한이 있는 통합 그룹을 지정합니다.

1. 테넌트에 대한 초기 루트 액세스 권한을 가지려면 그리드 관리자에서 기존 통합 그룹을 선택합니다.

> 적절한 권한이 있는 경우 필드를 선택하면 그리드 관리자의 기존 통합 그룹이 나열됩니다. 그렇지 않으면 그룹의 고유 이름을 입력합니다.

2. 테넌트 생성 * 을 선택합니다.

SSO가 활성화되지 않았습니다

1. 테넌트가 자신의 그룹 및 사용자를 관리하는지 또는 Grid Manager에 대해 구성된 ID 소스를 사용하는지에 따라 표에 설명된 단계를 완료합니다.

테넌트가...	수행할 작업...
자체 그룹 및 사용자를 관리합니다	a. Use own identity source * 를 선택합니다. ◦ 참고 *: 이 확인란을 선택하고 테넌트 그룹 및 사용자에 대해 ID 페더레이션을 사용하려면 테넌트가 자체 ID 소스를 구성해야 합니다. 를 참조하십시오 테넌트 계정 사용 지침. b. 테넌트의 로컬 루트 사용자에 대한 암호를 지정한 다음 * Create tenant * 를 선택합니다. c. 테넌트를 구성하려면 * root * 로 로그인 * 을 선택하고, 나중에 테넌트를 구성하려면 * 마침 * 을 선택합니다.
Grid Manager에 대해 구성된 그룹 및 사용자를 사용합니다	a. 다음 중 하나 또는 모두를 수행합니다. ◦ 테넌트에 대한 초기 루트 액세스 권한이 있어야 하는 기존 통합 그룹을 그리드 관리자에서 선택합니다. ▪ 참고 *: 적절한 권한이 있으면 필드를 선택할 때 그리드 관리자의 기존 통합 그룹이 나열됩니다. 그렇지 않으면 그룹의 고유 이름을 입력합니다. ◦ 테넌트의 로컬 루트 사용자에 대한 암호를 지정합니다. b. 테넌트 생성 * 을 선택합니다.

1. 지금 테넌트에 로그인하려면:
   - 제한된 포트에서 그리드 관리자에 액세스하는 경우 테넌트 테이블에서 * 제한된 * 를 선택하여 이 테넌트 계정에 액세스하는 방법에 대해 자세히 알아보십시오.

테넌트 관리자의 URL 형식은 다음과 같습니다.

"https://*FQDN_or_Admin_Node_IP*:*port*/?accountId=*20-digit-account-id*/`

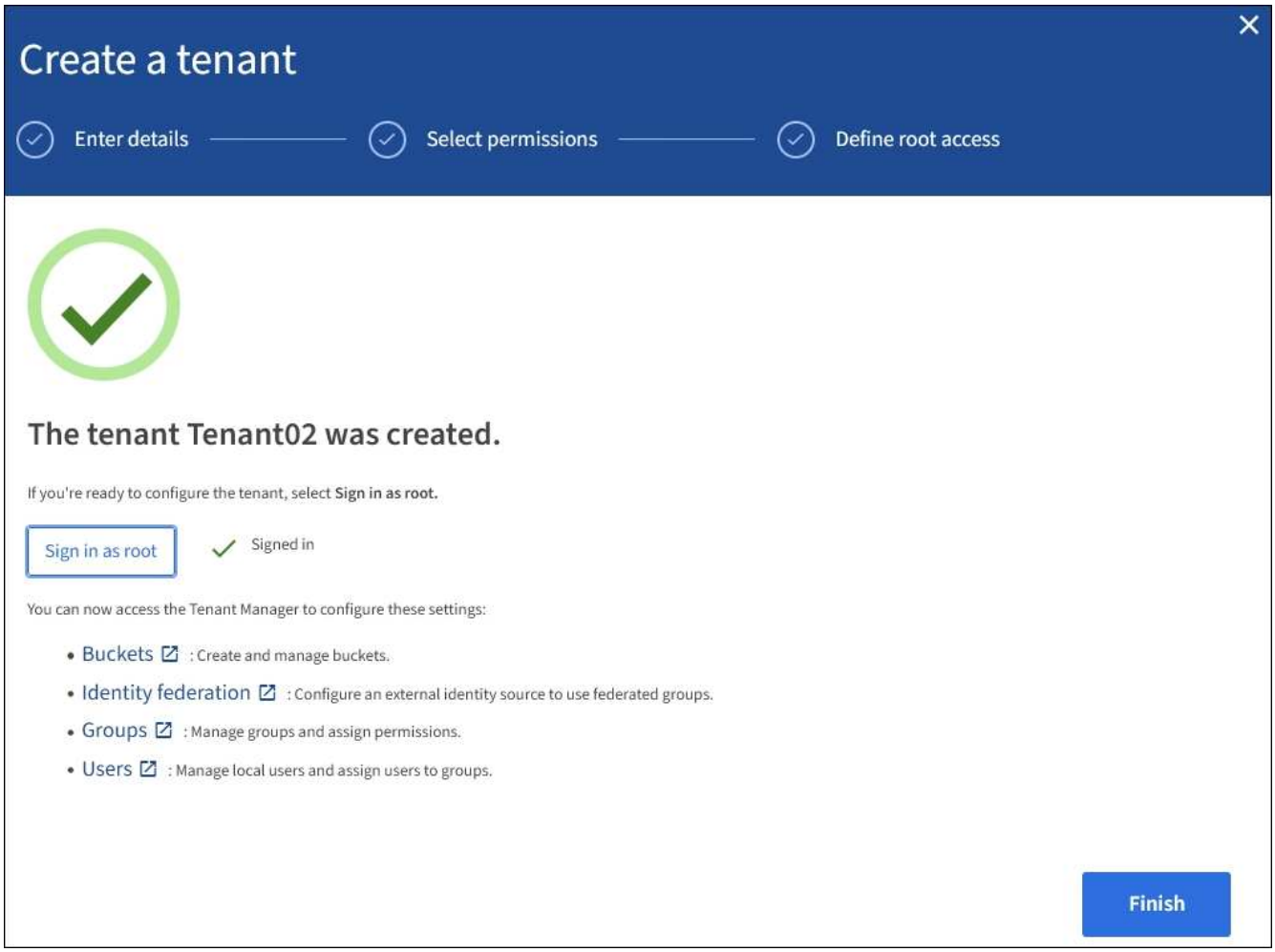
- '*FQDN_or_Admin_Node_IP*'는 정규화된 도메인 이름 또는 관리 노드의 IP 주소입니다
- '*port*'는 테넌트 전용 포트입니다
- `*20-digit-account-id*'는 테넌트의 고유 계정 ID입니다

◦ 포트 443에서 그리드 관리자에 액세스하지만 로컬 루트 사용자의 암호를 설정하지 않은 경우 그리드 관리자의 테넌트 테이블에서 * 로그인 * 을 선택하고 루트 액세스 통합 그룹에 사용자의 자격 증명을 입력합니다.

◦ 포트 443에서 Grid Manager에 액세스하고 로컬 루트 사용자의 암호를 설정하는 경우:

i. 지금 테넌트를 구성하려면 * root로 로그인 * 을 선택합니다.

로그인하면 버킷 또는 컨테이너, ID 페더레이션, 그룹 및 사용자를 구성하기 위한 링크가 표시됩니다.



i. 테넌트 계정을 구성할 링크를 선택합니다.

각 링크는 테넌트 관리자에서 해당 페이지를 엽니다. 페이지를 완료하려면 을 참조하십시오 테넌트 계정 사용 지침.

ii. 그렇지 않으면 * 마침 * 을 선택하여 나중에 테넌트에 액세스하십시오.

2. 나중에 테넌트에 액세스하려면 다음을 수행합니다.

사용 중인 경우...	다음 중 하나를 수행합니다.
포트 443	• Grid Manager에서 * Tenants * 를 선택하고 테넌트 이름 오른쪽에 있는 * 로그인 * 을 선택합니다. • 웹 브라우저에 테넌트의 URL을 입력합니다. "https://*FQDN_or_Admin_Node_IP*/?accountId=*20-digit-account-id*/` ◦ '*FQDN_or_Admin_Node_IP*'는 정규화된 도메인 이름 또는 관리 노드의 IP 주소입니다 ◦ `*20-digit-account-id*'는 테넌트의 고유 계정 ID입니다
제한된 포트	• Grid Manager에서 * Tenants * 를 선택하고 * Restricted * 를 선택합니다. • 웹 브라우저에 테넌트의 URL을 입력합니다. "https://*FQDN_or_Admin_Node_IP:port*/?accountId=*20-digit-account-id*` ◦ '*FQDN_or_Admin_Node_IP*'는 정규화된 도메인 이름 또는 관리 노드의 IP 주소입니다 ◦ '*port*'는 테넌트 전용 제한 포트입니다 ◦ `*20-digit-account-id*'는 테넌트의 고유 계정 ID입니다

관련 정보

- 방화벽을 통한 액세스 제어
- S3 테넌트 계정에 대한 플랫폼 서비스 관리

테넌트의 로컬 루트 사용자에 대한 암호를 변경합니다

루트 사용자가 계정에서 잠겨 있는 경우 테넌트의 로컬 루트 사용자의 암호를 변경해야 할 수 있습니다.

필요한 것

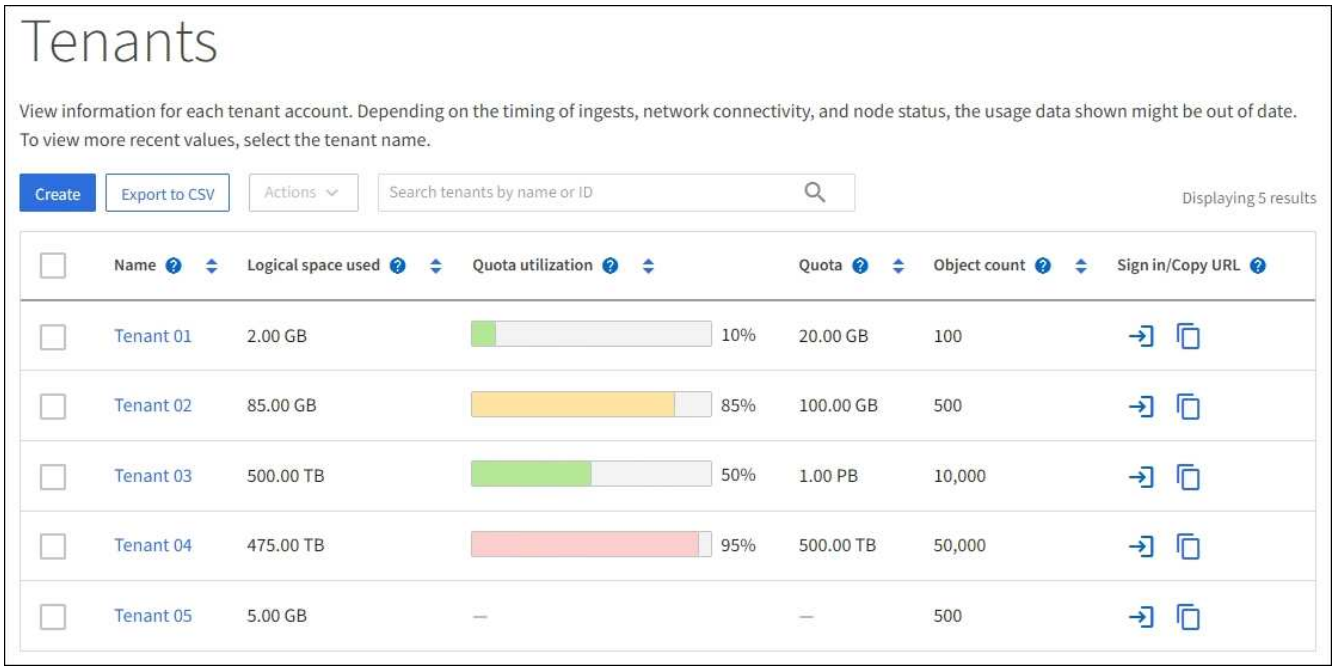
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 로컬 루트 사용자는 테넌트 계정에 로그인할 수 없습니다. 루트 사용자 작업을 수행하려면 사용자가 테넌트에 대한 루트 액세스 권한이 있는 통합 그룹에 속해야 합니다.

단계

1. Tenants * 를 선택합니다.



2. 편집할 테넌트 계정을 선택합니다.

   작업 단추가 활성화됩니다.

3. Actions * 드롭다운에서 * Change root password * 를 선택합니다.
4. 테넌트 계정의 새 암호를 입력합니다.
5. 저장 * 을 선택합니다.

테넌트 계정을 편집합니다

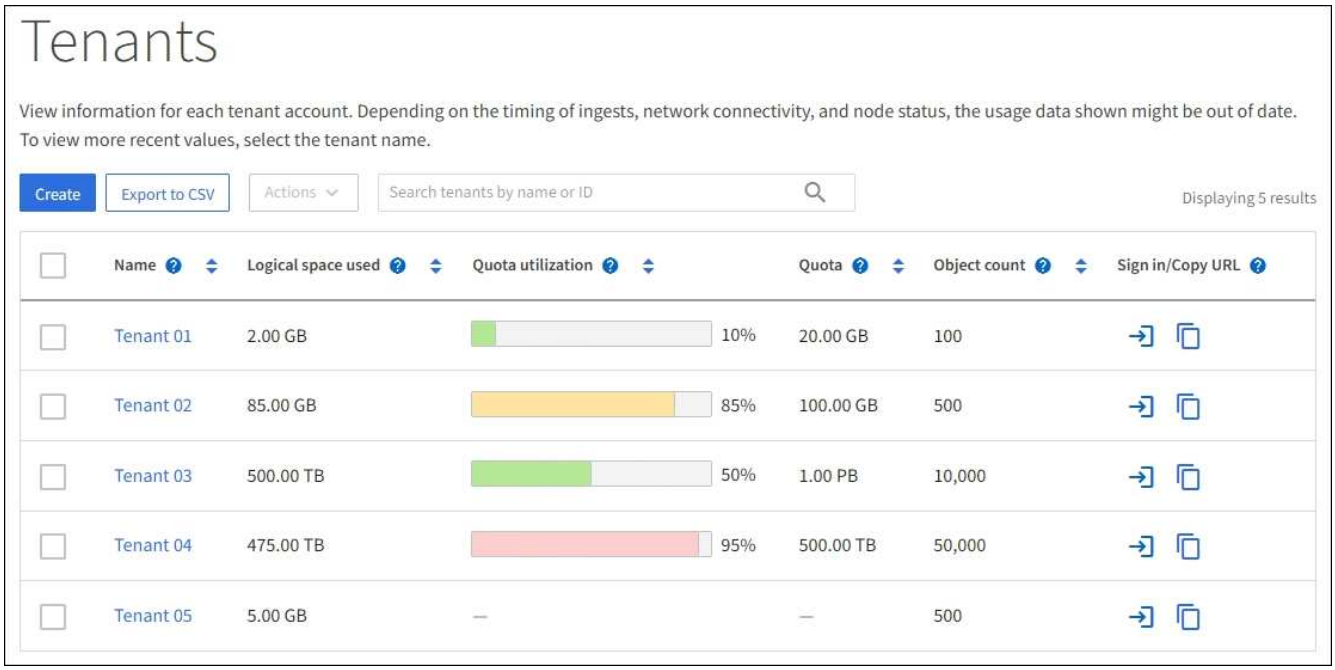
테넌트 계정을 편집하여 표시 이름을 변경하거나, ID 소스 설정을 변경하거나, 플랫폼 서비스를 허용 또는 금지하거나, 스토리지 할당량을 입력할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

단계

1. Tenants * 를 선택합니다.

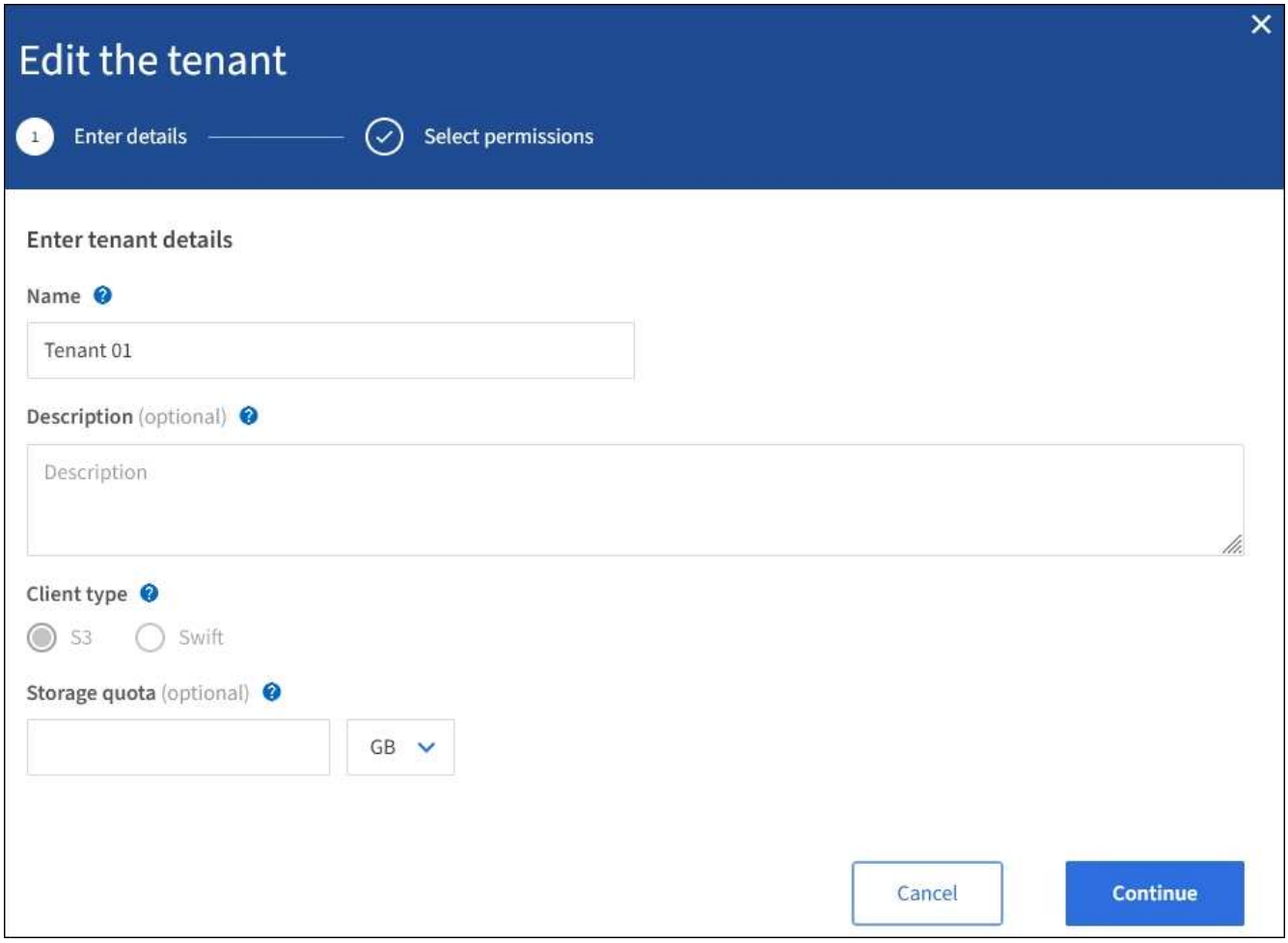


2. 편집할 테넌트 계정을 선택합니다.

   검색 상자를 사용하여 이름 또는 테넌트 ID로 테넌트 계정을 검색합니다.

3. 작업 드롭다운에서 * 편집 * 을 선택합니다.

   이 예제는 SSO(Single Sign-On)를 사용하지 않는 그리드에 대한 것입니다. 이 테넌트 계정은 자체 ID 소스를 구성하지 않았습니다.



4. 필요에 따라 다음 필드의 값을 변경합니다.
   - * 이름 *
   - * 설명 *
   - * 클라이언트 유형 *
   - * 스토리지 할당량 *
5. Continue * 를 선택합니다.
6. 테넌트 계정에 대한 사용 권한을 선택하거나 선택 취소합니다.
   - 이미 사용 중인 테넌트에 대해 * 플랫폼 서비스 * 를 비활성화하면 해당 S3 버킷에 대해 구성된 서비스가 작동을 멈춥니다. 테넌트에 오류 메시지가 전송되지 않습니다. 예를 들어, 테넌트가 S3 버킷에 대해 CloudMirror 복제를 구성한 경우 버킷에 오브젝트를 저장할 수 있지만 해당 오브젝트의 복사본은 더 이상 엔드포인트로 구성된 외부 S3 버킷에서 생성할 수 없습니다.
   - 사용자 지정 ID 소스 사용 * 확인란의 설정을 변경하여 테넌트 계정에서 자체 ID 소스를 사용할지 또는 Grid Manager용으로 구성된 ID 소스를 사용할지 여부를 결정합니다.

     고유 ID 원본 사용 * 확인란이 다음과 같은 경우:

     - 비활성화된 후 선택한 경우 테넌트는 이미 자체 ID 소스를 사용하도록 설정되어 있습니다. 테넌트는 그리드 관리자에 대해 구성된 ID 소스를 사용하기 전에 해당 ID 소스를 비활성화해야 합니다.
     - 비활성화되고 선택 취소되며 StorageGRID 시스템에 대해 SSO가 활성화됩니다. 테넌트는 Grid Manager에 대해 구성된 ID 소스를 사용해야 합니다.

    - 필요에 따라 * S3 Select * 를 활성화 또는 비활성화합니다. 을 참조하십시오 관리 S3 테넌트 계정에 대해 선택.
7. 저장 * 을 선택합니다.

관련 정보

- S3 테넌트 계정에 대한 플랫폼 서비스 관리
- 테넌트 계정을 사용합니다

테넌트 계정을 삭제합니다

테넌트의 시스템 액세스를 영구적으로 제거하려면 테넌트 계정을 삭제할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.
- 테넌트 계정과 연결된 모든 버킷(S3), 컨테이너(Swift) 및 개체를 제거해야 합니다.

단계

1. Tenants * 를 선택합니다.
2. 삭제할 테넌트 계정을 선택합니다.

   검색 상자를 사용하여 이름 또는 테넌트 ID로 테넌트 계정을 검색합니다.

3. 작업 * 드롭다운에서 * 삭제 * 를 선택합니다.
4. OK * 를 선택합니다.

플랫폼 서비스 관리

S3 테넌트 계정에 대한 플랫폼 서비스 관리

S3 테넌트 계정에 대해 플랫폼 서비스를 설정하는 경우 테넌트가 이러한 서비스를 사용하는 데 필요한 외부 리소스에 액세스할 수 있도록 그리드를 구성해야 합니다.

플랫폼 서비스란 무엇입니까**?**

플랫폼 서비스에는 CloudMirror 복제, 이벤트 알림 및 검색 통합 서비스가 포함됩니다.

이러한 서비스를 통해 테넌트는 자신의 S3 버킷에서 다음 기능을 사용할 수 있습니다.

- * CloudMirror 복제 *: StorageGRID CloudMirror 복제 서비스는 StorageGRID 버킷에서 지정된 외부 대상으로 특정 객체를 미러링하는 데 사용됩니다.

  예를 들어, CloudMirror 복제를 사용하여 특정 고객 레코드를 Amazon S3에 미러링한 다음 AWS 서비스를 활용하여 데이터에 대한 분석을 수행할 수 있습니다.

  ⓘ 소스 버킷에 S3 오브젝트 잠금이 설정된 경우 CloudMirror 복제가 지원되지 않습니다.

- * 알림 *: 버킷당 이벤트 알림은 지정된 외부 SNS(Amazon Simple Notification Service ™)에 객체에서 수행된

특정 작업에 대한 알림을 보내는 데 사용됩니다.

예를 들어, 버킷에 추가된 각 오브젝트에 대해 관리자에게 경고가 전송되도록 구성할 수 있습니다. 여기서 객체는 중요한 시스템 이벤트와 연결된 로그 파일을 나타냅니다.

> S3 오브젝트 잠금이 활성화된 버킷에서 이벤트 알림을 구성할 수 있지만 오브젝트의 S3 오브젝트 잠금 메타데이터(마지막 보존 날짜 및 법적 보류 상태 포함)는 알림 메시지에 포함되지 않습니다.

- * 검색 통합 서비스 *: 검색 통합 서비스는 외부 서비스를 사용하여 메타데이터를 검색하거나 분석할 수 있는 지정된 Elasticsearch 인덱스에 S3 오브젝트 메타데이터를 전송하는 데 사용됩니다.

  예를 들어, S3 오브젝트 메타데이터를 원격 Elasticsearch 서비스로 전송하도록 버킷을 구성할 수 있습니다. 그런 다음 Elasticsearch를 사용하여 버킷에 대한 검색을 수행하고 객체 메타데이터에 있는 패턴에 대한 정교한 분석을 수행할 수 있습니다.

  > S3 오브젝트 잠금이 활성화된 버킷에서 Elasticsearch 통합을 구성할 수 있지만 오브젝트의 S3 오브젝트 잠금 메타데이터(보존 기한 및 법적 보류 상태 포함)는 알림 메시지에 포함되지 않습니다.

플랫폼 서비스를 통해 테넌트는 외부 스토리지 리소스, 알림 서비스 및 데이터에 대한 검색 또는 분석 서비스를 사용할 수 있습니다. 플랫폼 서비스의 대상 위치는 일반적으로 StorageGRID 배포 외부에 있으므로 테넌트가 이러한 서비스를 사용하도록 허용할지 여부를 결정해야 합니다. 이 경우 테넌트 계정을 만들거나 편집할 때 플랫폼 서비스 사용을 활성화해야 합니다. 또한 테넌트가 생성하는 플랫폼 서비스 메시지가 대상에 도달할 수 있도록 네트워크를 구성해야 합니다.

플랫폼 서비스 사용을 위한 권장 사항

플랫폼 서비스를 사용하기 전에 다음 권장 사항을 숙지하십시오.

- StorageGRID 시스템의 S3 버킷에서 버전 관리 및 CloudMirror 복제가 모두 활성화된 경우 대상 엔드포인트에 대해 S3 버킷 버전 관리를 활성화해야 합니다. 이를 통해 CloudMirror 복제가 엔드포인트에 비슷한 개체 버전을 생성할 수 있습니다.
- CloudMirror 복제, 알림 및 검색 통합이 필요한 S3 요청이 있는 100개 이상의 활성 테넌트를 사용해서는 안 됩니다. 활성 테넌트가 100개 이상인 경우 S3 클라이언트 성능이 저하될 수 있습니다.
- 완료할 수 없는 엔드포인트에 대한 요청은 최대 500,000개의 요청에 대해 대기됩니다. 이 제한은 활성 테넌트 간에 동일하게 공유됩니다. 새 테넌트는 이 500,000개 제한을 일시적으로 초과할 수 있으므로 새로 생성된 테넌트가 불공평하게 처벌되지 않습니다.

관련 정보

- 테넌트 계정을 사용합니다
- 스토리지 프록시 설정을 구성합니다
- 모니터링하고 문제를 해결합니다

플랫폼 서비스를 위한 네트워크 및 포트

S3 테넌트가 플랫폼 서비스를 사용할 수 있도록 허용하는 경우 플랫폼 서비스 메시지가 대상으로 전달될 수 있도록 그리드에 대한 네트워킹을 구성해야 합니다.

테넌트 계정을 생성하거나 업데이트할 때 S3 테넌트 계정에 대해 플랫폼 서비스를 활성화할 수 있습니다. 플랫폼 서비스가 설정된 경우 테넌트는 CloudMirror 복제, 이벤트 알림 또는 S3 버킷에서 통합 메시지를 검색할 대상으로

사용되는 엔드포인트를 생성할 수 있습니다. 이러한 플랫폼 서비스 메시지는 ADC 서비스를 실행하는 스토리지 노드에서 대상 끝점으로 전송됩니다.

예를 들어, 테넌트는 다음과 같은 유형의 대상 엔드포인트를 구성할 수 있습니다.

- 로컬로 호스팅되는 Elasticsearch 클러스터입니다
- SNS(Simple Notification Service) 메시지 수신을 지원하는 로컬 애플리케이션입니다
- StorageGRID의 동일한 인스턴스 또는 다른 인스턴스에서 로컬로 호스팅되는 S3 버킷
- Amazon Web Services의 엔드포인트와 같은 외부 엔드포인트입니다.

플랫폼 서비스 메시지가 전달될 수 있도록 ADC 스토리지 노드가 포함된 네트워크를 구성해야 합니다. 다음 포트를 사용하여 플랫폼 서비스 메시지를 대상 끝점에 보낼 수 있는지 확인해야 합니다.

기본적으로 플랫폼 서비스 메시지는 다음 포트로 전송됩니다.

- * 80 *: http로 시작하는 끝점 URI입니다
- * 443 *: https로 시작하는 끝점 URI의 경우

테넌트는 끝점을 만들거나 편집할 때 다른 포트를 지정할 수 있습니다.

> StorageGRID 배포를 CloudMirror 복제의 대상으로 사용하는 경우 80 또는 443 이외의 포트에서 복제 메시지를 받을 수 있습니다. 대상 StorageGRID 배포에서 S3에 사용 중인 포트가 끝점에 지정되었는지 확인합니다.

투명하지 않은 프록시 서버를 사용하는 경우에도 필요합니다 스토리지 프록시 설정을 구성합니다 인터넷의 끝점과 같은 외부 끝점으로 메시지를 보낼 수 있도록 합니다.

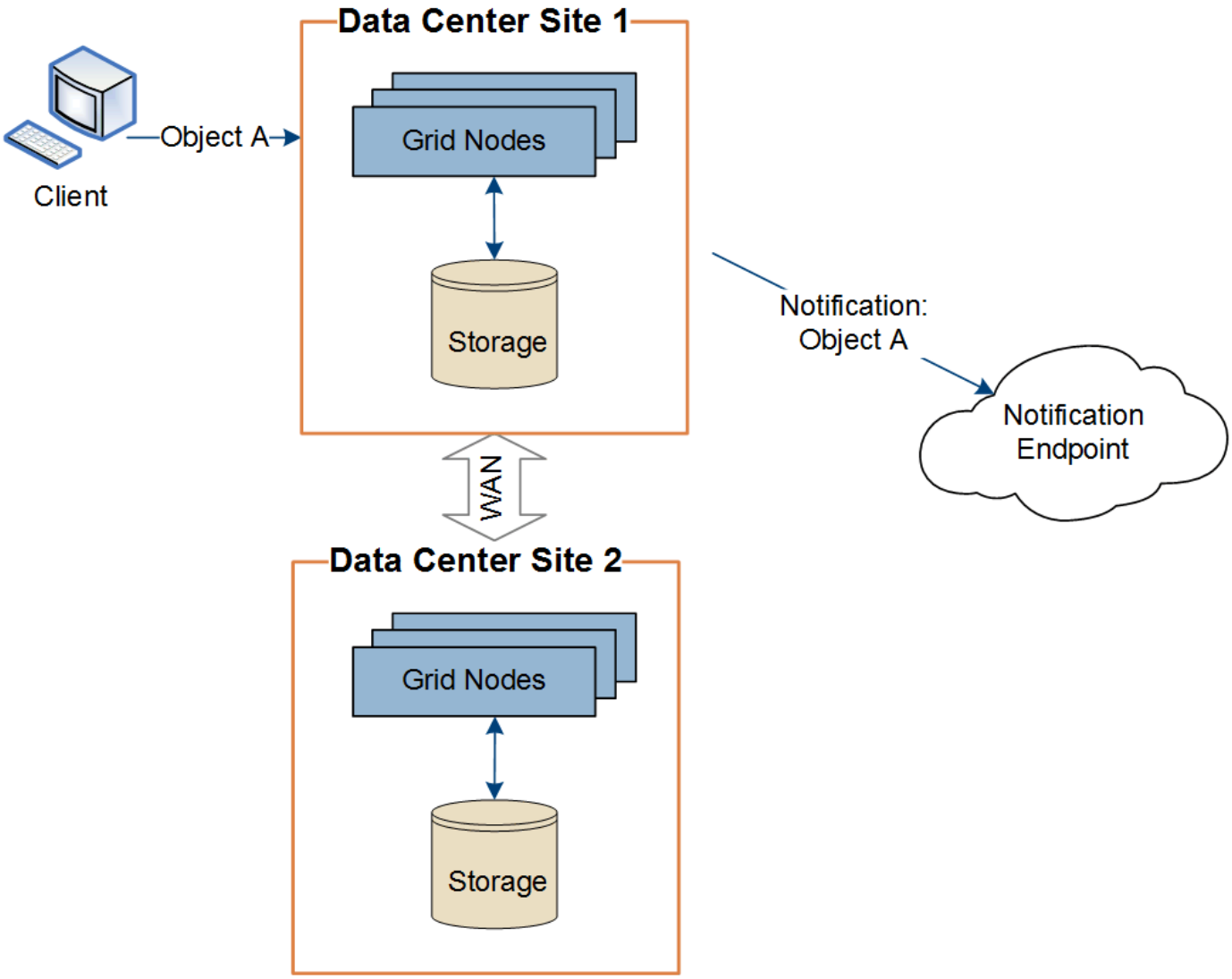
관련 정보

- 테넌트 계정을 사용합니다

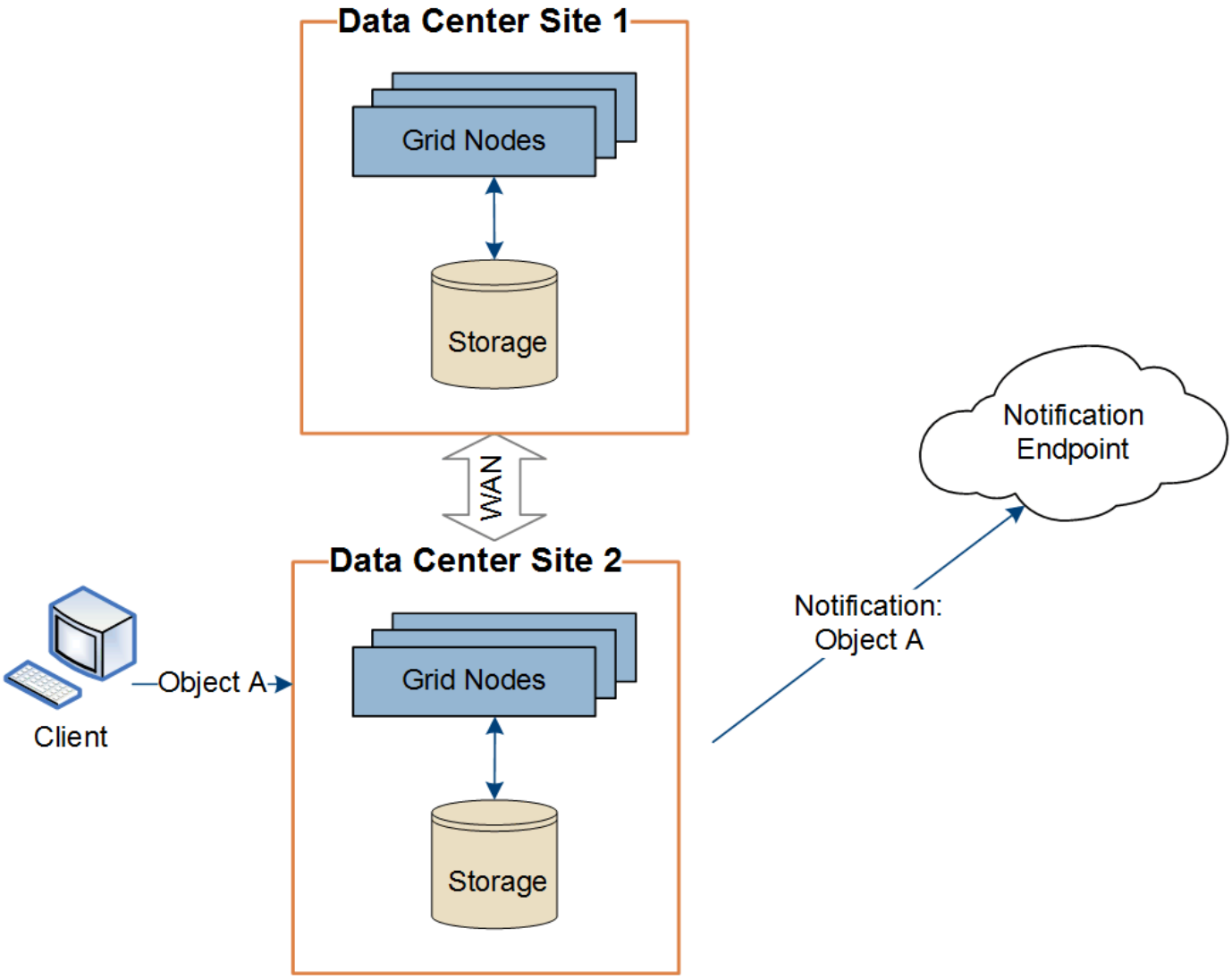
플랫폼 서비스 메시지를 사이트별로 전달

모든 플랫폼 서비스 작업은 사이트별로 수행됩니다.

즉, 테넌트가 클라이언트를 사용하여 데이터 센터 사이트 1의 게이트웨이 노드에 연결하여 오브젝트에 대해 S3 API 생성 작업을 수행하는 경우 해당 작업에 대한 알림이 트리거되고 데이터 센터 사이트 1에서 전송됩니다.



이후에 클라이언트가 데이터 센터 사이트 2에서 동일한 개체에 대해 S3 API 삭제 작업을 수행하면 삭제 작업에 대한 알림이 트리거되어 데이터 센터 사이트 2에서 전송됩니다.



각 사이트의 네트워킹이 플랫폼 서비스 메시지를 해당 대상에 전달할 수 있도록 구성되어 있는지 확인합니다.

플랫폼 서비스 문제 해결

플랫폼 서비스에 사용되는 엔드포인트는 테넌트 관리자의 테넌트 사용자가 생성 및 유지 관리합니다. 그러나 테넌트에 플랫폼 서비스를 구성하거나 사용하는 데 문제가 있는 경우 Grid Manager를 사용하여 문제를 해결할 수 있습니다.

새 끝점에 문제가 있습니다

테넌트가 플랫폼 서비스를 사용하려면 먼저 테넌트 관리자를 사용하여 하나 이상의 엔드포인트를 생성해야 합니다. 각 엔드포인트는 StorageGRID S3 버킷, Amazon 웹 서비스 버킷, 간단한 알림 서비스 주제 또는 로컬 또는 AWS에서 호스팅되는 Elasticsearch 클러스터와 같은 단일 플랫폼 서비스의 외부 대상을 나타냅니다. 각 끝점에는 외부 리소스의 위치와 해당 리소스에 액세스하는 데 필요한 자격 증명이 모두 포함됩니다.

테넌트가 끝점을 만들 때 StorageGRID 시스템은 끝점이 있는지, 그리고 지정된 자격 증명을 사용하여 해당 끝점에 도달할 수 있는지 검증합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

끝점 유효성 검사에 실패하면 끝점 유효성 검사가 실패한 이유를 설명하는 오류 메시지가 표시됩니다. 테넌트 사용자가 문제를 해결한 다음 엔드포인트를 다시 생성해 보십시오.

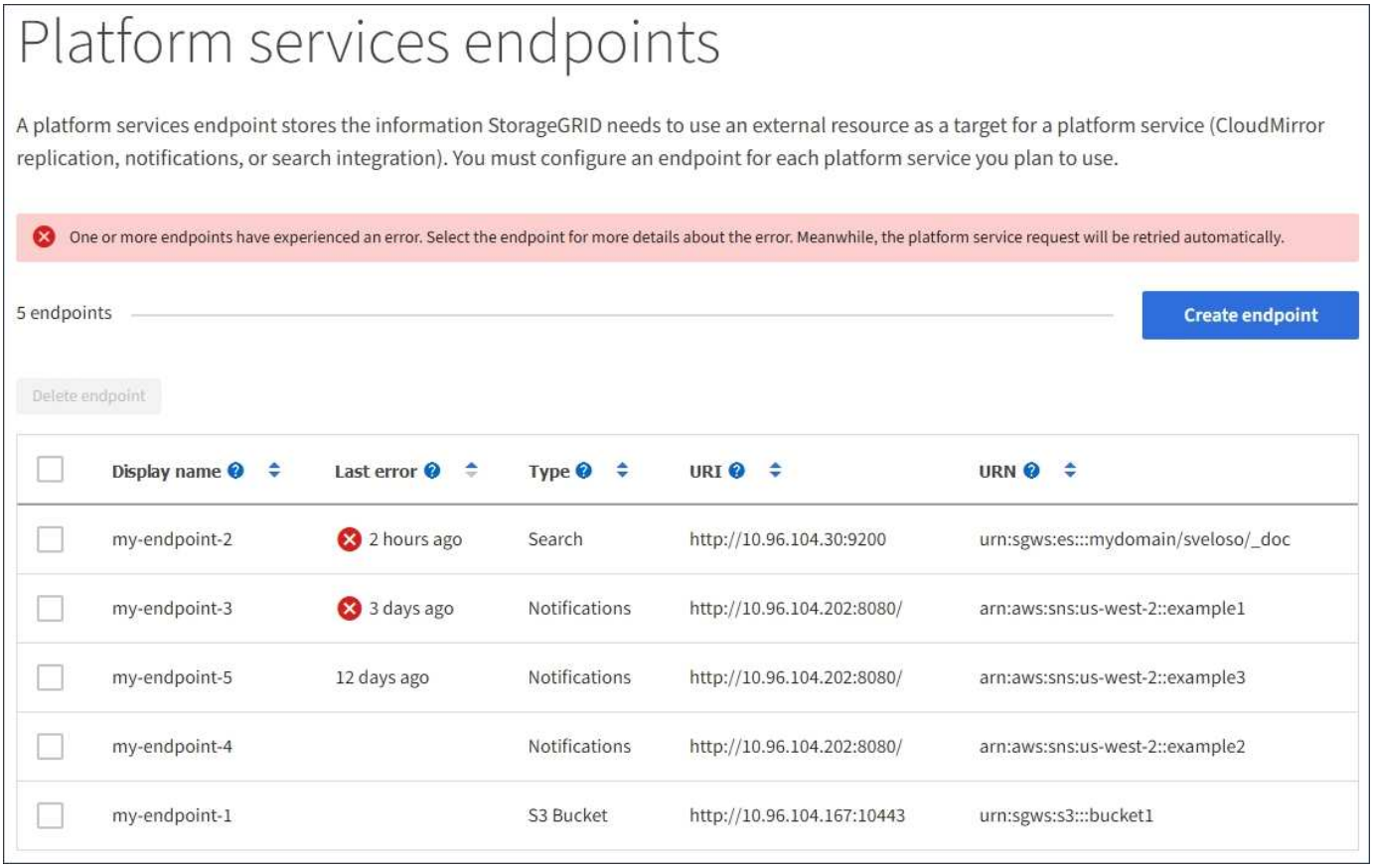
테넌트 계정에 대해 플랫폼 서비스가 활성화되어 있지 않으면 엔드포인트 생성이 실패합니다.

기존 엔드포인트에 문제가 있습니다

StorageGRID가 기존 엔드포인트에 도달하려고 할 때 오류가 발생하면 테넌트 관리자의 대시보드에 메시지가 표시됩니다.

One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

테넌트 사용자는 끝점 페이지로 이동하여 각 끝점에 대한 가장 최근의 오류 메시지를 검토하고 오류가 발생한 시간을 확인할 수 있습니다. 마지막 오류 * 열은 각 끝점에 대한 가장 최근 오류 메시지를 표시하고 오류가 발생한 시간을 나타냅니다. 에 포함된 오류 지난 7일 내에 아이콘이 발생했습니다.



마지막 오류 * 열에 있는 일부 오류 메시지에는 괄호 안에 로그 ID가 포함될 수 있습니다. 그리드 관리자 또는 기술 지원에서는 이 ID를 사용하여 bycast.log의 오류에 대한 자세한 정보를 찾을 수 있습니다.

프록시 서버와 관련된 문제

스토리지 노드와 플랫폼 서비스 엔드포인트 간에 스토리지 프록시를 구성한 경우 프록시 서비스에서 StorageGRID의 메시지를 허용하지 않으면 오류가 발생할 수 있습니다. 이러한 문제를 해결하려면 프록시 서버의 설정을 확인하여 플랫폼 서비스 관련 메시지가 차단되지 않았는지 확인합니다.

오류가 발생했는지 확인합니다

지난 7일 이내에 엔드포인트 오류가 발생한 경우 테넌트 관리자의 대시보드에 경고 메시지가 표시됩니다. 끝점 페이지로 이동하여 오류에 대한 자세한 정보를 볼 수 있습니다.

클라이언트 작업이 실패했습니다

일부 플랫폼 서비스 문제로 인해 S3 버킷의 클라이언트 작업이 실패할 수 있습니다. 예를 들어 RSM(Internal Replicated State Machine) 서비스가 중지되거나 너무 많은 플랫폼 서비스 메시지가 배달 대기 중인 경우 S3 클라이언트 작업이 실패합니다.

서비스 상태를 확인하려면

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. site_ * > **Storage Node* * > * SSM * > * Services * 를 선택합니다.

복구할 수 없는 끝점 오류입니다

엔드포인트가 생성된 후 다양한 이유로 플랫폼 서비스 요청 오류가 발생할 수 있습니다. 일부 오류는 사용자 개입으로 복구할 수 있습니다. 예를 들어 다음과 같은 이유로 복구 가능한 오류가 발생할 수 있습니다.

- 사용자의 자격 증명이 삭제되었거나 만료되었습니다.
- 대상 버킷이 없습니다.
- 알림을 전달할 수 없습니다.

StorageGRID에서 복구 가능한 오류가 발생하면 성공할 때까지 플랫폼 서비스 요청이 재시도됩니다.

다른 오류는 복구할 수 없습니다. 예를 들어, 끝점이 삭제되면 복구할 수 없는 오류가 발생합니다.

StorageGRID에서 복구할 수 없는 끝점 오류가 발생하면 그리드 관리자에서 SMTT(Total Events) 레거시 경보가 트리거됩니다. Total Events Legacy(총 이벤트 레거시) 알람을 보려면

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. site_ * > **node* * > * SSM * > * Events * 를 선택합니다.
3. 테이블 상단의 마지막 이벤트 보기

   이벤트 메시지는 '/var/local/log/bycast-err.log'에도 나열됩니다.

4. SMTT 알람 내용물에 제공된 지침을 따라 문제를 해결하십시오.
5. 구성 * 탭을 선택하여 이벤트 수를 재설정합니다.
6. 플랫폼 서비스 메시지가 전달되지 않은 객체를 테넌트에 알립니다.
7. 테넌트에게 개체의 메타데이터 또는 태그를 업데이트하여 실패한 복제 또는 알림을 다시 트리거하도록 지시합니다.

   테넌트는 불필요한 변경을 방지하기 위해 기존 값을 다시 제출할 수 있습니다.

플랫폼 서비스 메시지를 전달할 수 없습니다

대상에 플랫폼 서비스 메시지를 수락하지 못하는 문제가 발생하면 버킷에 대한 클라이언트 작업은 성공하지만 플랫폼

서비스 메시지는 전달되지 않습니다. 예를 들어, StorageGRID가 더 이상 대상 서비스에 인증할 수 없도록 대상에서 자격 증명이 업데이트되는 경우 이 오류가 발생할 수 있습니다.

복구할 수 없는 오류로 인해 플랫폼 서비스 메시지를 전달할 수 없는 경우 그리드 관리자에서 SMTT(Total Events) 레거시 경보가 트리거됩니다.

플랫폼 서비스 요청에 대한 성능 저하

요청이 전송되는 속도가 대상 엔드포인트에서 요청을 수신할 수 있는 속도를 초과하는 경우 StorageGRID 소프트웨어는 버킷에 대한 수신 S3 요청을 스로틀할 수 있습니다. 임계치 조절은 대상 끝점으로 보내려고 기다리는 요청의 백로그가 있는 경우에만 발생합니다.

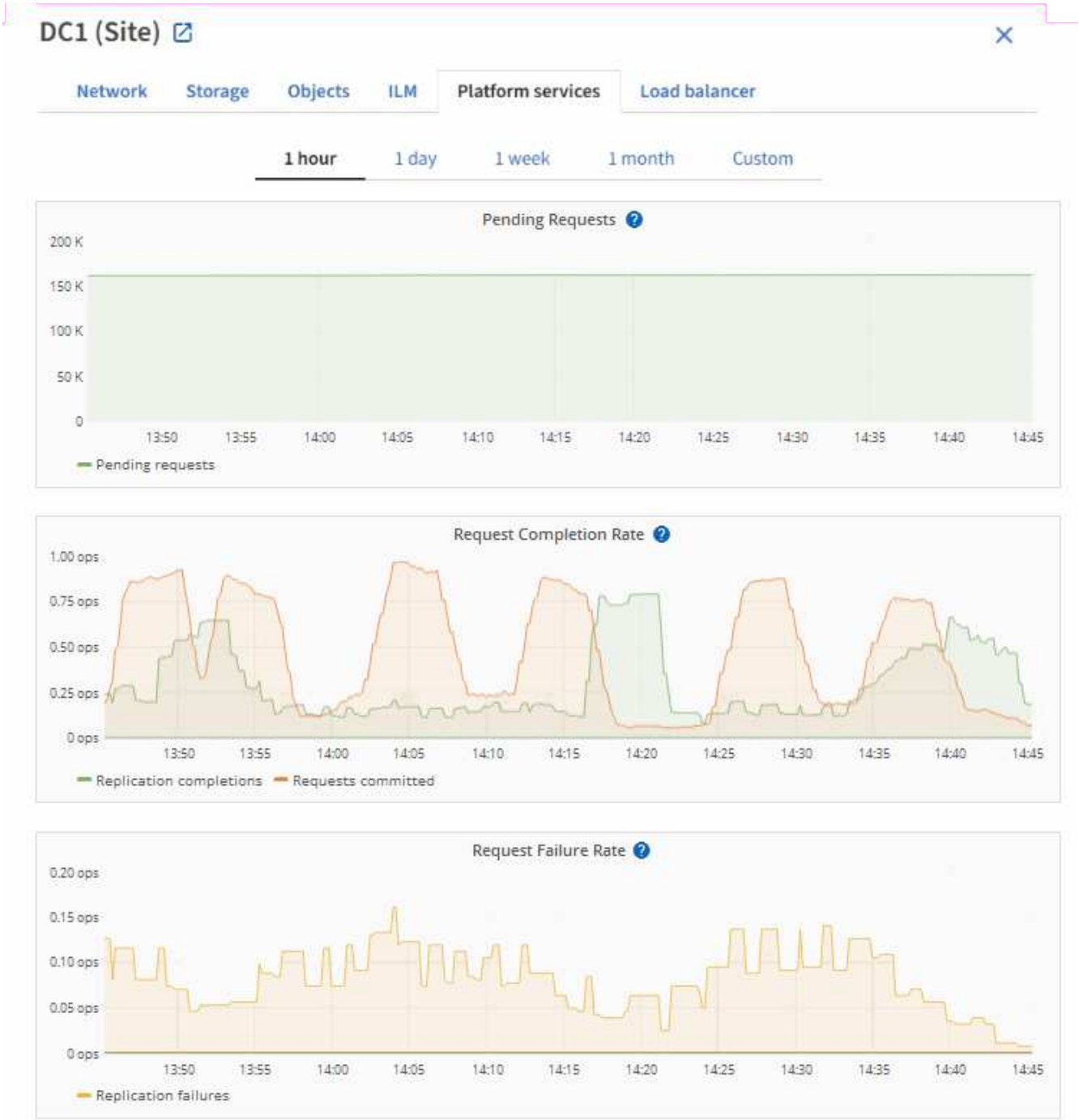
단, 들어오는 S3 요청의 실행 시간이 더 오래 걸린다는 점을 알 수 있습니다. 속도가 현저히 느린 성능을 감지하기 시작하는 경우 수집 속도를 줄이거나 용량이 더 큰 엔드포인트를 사용해야 합니다. 요청 백로그가 계속 증가하는 경우 PUT 요청과 같은 클라이언트 S3 작업이 결국 실패합니다.

CloudMirror 요청은 일반적으로 검색 통합 또는 이벤트 알림 요청보다 더 많은 데이터 전송을 포함하므로 대상 엔드포인트의 성능에 영향을 받을 가능성이 더 높습니다.

플랫폼 서비스 요청에 실패했습니다

플랫폼 서비스에 대한 요청 실패율을 보려면

1. 노드 * 를 선택합니다.
2. *_site* * > * 플랫폼 서비스 * 를 선택합니다.
3. 요청 오류율 차트를 봅니다.



플랫폼 서비스를 사용할 수 없음 경고

플랫폼 서비스 사용 불가 * 경고는 RSM 서비스가 실행 중이거나 사용 가능한 스토리지 노드가 너무 적어서 사이트에서 플랫폼 서비스 작업을 수행할 수 없음을 나타냅니다.

RSM 서비스는 플랫폼 서비스 요청이 각 끝점으로 전송되도록 합니다.

이 경고를 해결하려면 사이트에서 RSM 서비스를 포함하는 스토리지 노드를 확인합니다. (RSM 서비스는 ADC 서비스도 포함하는 스토리지 노드에 있습니다.) 그런 다음 이러한 스토리지 노드 중 대부분이 실행 중이고 사용 가능한지 확인합니다.

> 사이트에서 RSM 서비스를 포함하는 스토리지 노드가 두 개 이상 장애가 발생하면 해당 사이트에 대한 보류 중인 플랫폼 서비스 요청이 손실됩니다.

플랫폼 서비스 끝점에 대한 추가 문제 해결 지침

플랫폼 서비스 끝점 문제 해결에 대한 자세한 내용은 의 지침을 참조하십시오 테넌트 계정 사용.

관련 정보

- 모니터링하고 문제를 해결합니다
- 스토리지 프록시 설정을 구성합니다

관리 **S3** 테넌트 계정에 대해 선택

특정 S3 테넌트가 S3 선택을 사용하여 개별 오브젝트에 SelectObjectContent 요청을 발급하도록 허용할 수 있습니다.

S3 Select를 사용하면 데이터베이스와 관련 리소스를 배치하지 않고도 대량의 데이터를 효율적으로 검색할 수 있습니다. 또한, 데이터를 검색하는 데 드는 비용과 대기 시간도 줄어듭니다.

S3 Select란 무엇입니까**?**

S3 Select를 사용하면 S3 클라이언트가 SelectObjectContent 요청을 사용하여 오브젝트에서 필요한 데이터만 필터링 및 검색할 수 있습니다. S3 Select의 StorageGRID 구현에는 S3 Select 명령 및 기능의 하위 집합이 포함됩니다.

S3 Select 사용에 대한 고려 사항 및 요구 사항

StorageGRID에서 S3 선택 쿼리에 대해 다음을 수행해야 합니다.

- 쿼리할 객체가 CSV 형식이거나 CSV 형식 파일이 포함된 GZIP 또는 BZIP2 압축 파일입니다.
- 테넌트는 그리드 관리자가 S3 선택 기능을 부여해야 합니다. Allow S3 Select * When(S3 선택 허용 * 시기) 을 선택합니다 테넌트 생성 또는 테넌트 편집.
- SelectObjectContent 요청은 로 보내야 합니다 StorageGRID 로드 밸런서 엔드포인트. 엔드포인트에서 사용하는 관리 및 게이트웨이 노드는 SG100 또는 SG1000 어플라이언스 노드 또는 VMware 기반 소프트웨어 노드여야 합니다.

다음 제한 사항을 참고하십시오.

- 베어 메탈 로드 밸런서 노드는 지원되지 않습니다.
- 쿼리는 스토리지 노드로 직접 보낼 수 없습니다.
- 더 이상 사용되지 않는 CLB 서비스를 통해 전송된 쿼리는 지원되지 않습니다.

> SelectObjectContent 요청은 모든 S3 클라이언트 및 모든 테넌트의 로드 밸런서 성능을 줄일 수 있습니다. 신뢰할 수 있는 테넌트에만 필요한 경우에만 이 기능을 사용하도록 설정합니다.

를 참조하십시오 S3 Select 사용에 대한 지침.

를 눌러 봅니다 Grafana 차트 시간의 경과에 따른 S3 Select 작업의 경우 Grid Manager에서 * 지원 * > * 도구 * > * 메트릭 * 을 선택합니다.

S3 및 Swift 클라이언트 연결을 구성합니다

S3 및 Swift 클라이언트 연결에 대해 설명합니다

그리드 관리자는 S3 및 Swift 테넌트가 클라이언트 애플리케이션을 StorageGRID 시스템에 연결하여 데이터를 저장 및 검색하는 방법을 제어하는 구성 옵션을 관리합니다. 다양한 클라이언트 및 테넌트 요구 사항을 충족하는 여러 가지 옵션이 있습니다.

클라이언트 응용 프로그램은 다음 중 하나를 연결하여 개체를 저장하거나 검색할 수 있습니다.

- 관리 노드 또는 게이트웨이 노드의 부하 분산 서비스 또는 선택적으로 관리 노드 또는 게이트웨이 노드의 고가용성(HA) 그룹의 가상 IP 주소입니다
- 게이트웨이 노드의 CLB 서비스 또는 게이트웨이 노드의 고가용성 그룹의 가상 IP 주소(선택 사항)입니다

> CLB 서비스는 더 이상 사용되지 않습니다. StorageGRID 11.3 릴리스 전에 구성된 클라이언트는 게이트웨이 노드에서 CLB 서비스를 계속 사용할 수 있습니다. 로드 밸런싱을 제공하기 위해 StorageGRID에 의존하는 다른 모든 클라이언트 애플리케이션은 로드 밸런서 서비스를 사용하여 연결해야 합니다.

- 외부 로드 밸런서가 있거나 없는 스토리지 노드

StorageGRID 시스템에서 다음 기능을 선택적으로 구성할 수 있습니다.

- * VLAN 인터페이스 *: 관리 노드와 게이트웨이 노드에서 가상 LAN(VLAN) 인터페이스를 생성하여 보안, 유연성 및 성능을 위해 클라이언트 및 테넌트 트래픽을 격리하고 분할할 수 있습니다. VLAN 인터페이스를 생성한 후 고가용성(HA) 그룹에 추가합니다.
- * 고가용성 그룹 *: 게이트웨이 노드 또는 관리 노드에 대한 인터페이스의 HA 그룹을 생성하여 액티브-백업 구성을 생성하거나 라운드 로빈 DNS 또는 타사 로드 밸런서 및 다중 HA 그룹을 사용하여 액티브-액티브 구성을 달성할 수 있습니다. HA 그룹의 가상 IP 주소를 사용하여 클라이언트 연결이 이루어집니다.
- * 로드 밸런서 서비스 *: 클라이언트가 클라이언트 연결을 위한 로드 밸런서 끝점을 만들어 로드 밸런서 서비스를 사용하도록 설정할 수 있습니다. 로드 밸런서 끝점을 만들 때 끝점에서 HTTP 또는 HTTPS 연결을 허용하는지 여부, 끝점을 사용할 클라이언트 유형(S3 또는 Swift) 및 HTTPS 연결에 사용할 인증서(해당하는 경우)를 포트 번호로 지정합니다.
- * 신뢰할 수 없는 클라이언트 네트워크 *: 클라이언트 네트워크를 신뢰할 수 없음으로 구성하여 보안을 강화할 수 있습니다. 클라이언트 네트워크를 신뢰할 수 없는 경우 클라이언트는 로드 밸런서 끝점만 사용하여 연결할 수 있습니다.

또한 StorageGRID에 직접 연결하는 클라이언트나 CLB 서비스(사용되지 않음)를 사용하는 클라이언트에 대해 HTTP를 사용하도록 설정할 수 있으며 S3 클라이언트에 대해 S3 API 엔드포인트 도메인 이름을 구성할 수 있습니다.

요약: 클라이언트 연결을 위한 IP 주소 및 포트

클라이언트 애플리케이션은 그리드 노드의 IP 주소와 해당 노드에 있는 서비스의 포트 번호를 사용하여 StorageGRID에 연결할 수 있습니다. HA(고가용성) 그룹이 구성되어 있는 경우 클라이언트 애플리케이션은 HA 그룹의 가상 IP 주소를 사용하여 연결할 수 있습니다.

이 작업에 대해

이 표에는 클라이언트가 StorageGRID에 연결할 수 있는 다양한 방법과 각 연결 유형에 사용되는 IP 주소 및 포트가

요약되어 있습니다. 이 지침은 로드 밸런서 끝점과 HA(고가용성) 그룹이 이미 구성되어 있는 경우 그리드 관리자에서 이 정보를 찾는 방법을 설명합니다.

연결 위치	클라이언트가 연결하는 서비스입니다	**IP** 주소입니다	포트
HA 그룹	로드 밸런서	HA 그룹의 가상 IP 주소입니다	• 로드 밸런서 엔드포인트 포트
HA 그룹	CLB • 참고: * CLB 서비스는 더 이상 사용되지 않습니다.	HA 그룹의 가상 IP 주소입니다	기본 S3 포트: • HTTPS: 8082 • HTTP: 8084 기본 Swift 포트: • HTTPS: 8083 • HTTP: 8085
관리자 노드	로드 밸런서	관리 노드의 IP 주소입니다	• 로드 밸런서 엔드포인트 포트
게이트웨이 노드	로드 밸런서	게이트웨이 노드의 IP 주소입니다	• 로드 밸런서 엔드포인트 포트
게이트웨이 노드	CLB • 참고: * CLB 서비스는 더 이상 사용되지 않습니다.	게이트웨이 노드의 IP 주소입니다 • 참고: * 기본적으로 CLB 및 LDR용 HTTP 포트는 사용되지 않습니다.	기본 S3 포트: • HTTPS: 8082 • HTTP: 8084 기본 Swift 포트: • HTTPS: 8083 • HTTP: 8085
스토리지 노드	LDR	스토리지 노드의 IP 주소입니다	기본 S3 포트: • HTTPS: 18082 • HTTP: 18084 기본 Swift 포트: • HTTPS: 18083 • HTTP: 18085

예

S3 클라이언트를 게이트웨이 노드 HA 그룹의 로드 밸런서 끝점에 연결하려면 아래와 같이 구조화된 URL을 사용합니다.

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

예를 들어 HA 그룹의 가상 IP 주소가 192.0.2.5이고 S3 로드 밸런서 끝점의 포트 번호가 10443인 경우 S3 클라이언트는 다음 URL을 사용하여 StorageGRID에 연결할 수 있습니다.

- 'https://192.0.2.5:10443`

Swift 클라이언트를 게이트웨이 노드 HA 그룹의 로드 밸런서 끝점에 연결하려면 아래와 같이 구조화된 URL을 사용합니다.

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

예를 들어 HA 그룹의 가상 IP 주소가 192.0.2.6이고 Swift 로드 밸런서 끝점의 포트 번호가 10444인 경우 Swift 클라이언트는 다음 URL을 사용하여 StorageGRID에 연결할 수 있습니다.

- 'https://192.0.2.6:10444`

클라이언트가 StorageGRID에 연결하는 데 사용하는 IP 주소에 대한 DNS 이름을 구성할 수 있습니다. 로컬 네트워크 관리자에게 문의하십시오.

단계

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

      클라이언트 응용 프로그램에서 목록의 IP 주소로의 연결을 설정할 수 있습니다.

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

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

3. 고가용성 그룹의 가상 IP 주소를 찾으려면 다음을 수행합니다.
   a. 구성 * > * 네트워크 * > * 고가용성 그룹 * 을 선택합니다.
   b. 표에서 HA 그룹의 가상 IP 주소를 확인합니다.
4. 로드 밸런서 끝점의 포트 번호를 찾으려면 다음을 수행합니다.
   a. 구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 * 를 선택합니다.

      로드 밸런서 끝점 페이지가 나타나고 이미 구성된 끝점 목록이 표시됩니다.

b. 끝점을 선택하고 * 끝점 편집 * 을 선택합니다.

   끝점 편집 창이 열리고 끝점에 대한 추가 세부 정보가 표시됩니다.

c. 선택한 끝점이 올바른 프로토콜(S3 또는 Swift)과 함께 사용하도록 구성되었는지 확인한 후 * Cancel * (취소 *)을 선택합니다.

d. 클라이언트 연결에 사용할 끝점의 포트 번호를 확인합니다.

> 포트 번호가 80 또는 443이면 해당 포트가 관리 노드에 예약되므로 끝점이 게이트웨이 노드에서만 구성됩니다. 다른 모든 포트는 게이트웨이 노드와 관리 노드 모두에서 구성됩니다.

VLAN 인터페이스를 구성합니다

관리 노드와 게이트웨이 노드에서 VLAN(가상 LAN) 인터페이스를 생성하고 HA 그룹 및 로드 밸런서 끝점에서 사용하여 트래픽을 격리하고 파티셔닝하여 보안, 유연성 및 성능을 확보할 수 있습니다.

VLAN 인터페이스에 대한 고려 사항

- VLAN ID를 입력하고 하나 이상의 노드에서 상위 인터페이스를 선택하여 VLAN 인터페이스를 생성합니다.
- 상위 인터페이스는 스위치에서 트렁크 인터페이스로 구성되어야 합니다.
- 상위 인터페이스는 Grid Network(eth0), Client Network(eth2) 또는 VM 또는 베어 메탈 호스트(예: ens256)용 추가 트렁크 인터페이스가 될 수 있습니다.
- 각 VLAN 인터페이스에 대해 특정 노드에 대해 하나의 상위 인터페이스만 선택할 수 있습니다. 예를 들어 동일한 게이트웨이 노드에서 그리드 네트워크 인터페이스와 클라이언트 네트워크 인터페이스를 같은 VLAN의 부모 인터페이스와 함께 사용할 수 없습니다.
- VLAN 인터페이스가 그리드 관리자 및 테넌트 관리자와 관련된 트래픽을 포함하는 관리 노드 트래픽용 VLAN인 경우 관리 노드에서만 인터페이스를 선택합니다.
- VLAN 인터페이스가 S3 또는 Swift 클라이언트 트래픽용 VLAN인 경우 관리 노드 또는 게이트웨이 노드에서 인터페이스를 선택합니다.
- 트렁크 인터페이스를 추가해야 하는 경우 자세한 내용은 다음을 참조하십시오.
  - * VMware(노드 설치 후) *: VMware: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다
  - * RHEL 또는 CentOS(노드 설치 전) *: 노드 구성 파일을 생성합니다
  - * Ubuntu 또는 Debian(노드 설치 전) *: 노드 구성 파일을 생성합니다
  - * RHEL, CentOS, Ubuntu 또는 Debian(노드 설치 후) *: Linux: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다

VLAN 인터페이스를 생성합니다

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.
- 트렁크 인터페이스가 네트워크에서 구성되었으며 VM 또는 Linux 노드에 연결되었습니다. 트렁크 인터페이스의 이름을 알고 있습니다.

- 구성하려는 VLAN의 ID를 알고 있습니다.

이 작업에 대해

네트워크 관리자가 하나 이상의 트렁크 인터페이스와 하나 이상의 VLAN을 구성하여 다른 애플리케이션이나 테넌트에 속한 클라이언트 또는 관리 트래픽을 분리했을 수 있습니다. 각 VLAN은 숫자 ID 또는 태그로 식별됩니다. 예를 들어 네트워크에서 FabricPool 트래픽에는 VLAN 100을 사용하고 아카이브 애플리케이션에는 VLAN 200을 사용할 수 있습니다.

그리드 관리자를 사용하여 클라이언트가 특정 VLAN에서 StorageGRID에 액세스할 수 있도록 하는 VLAN 인터페이스를 생성할 수 있습니다. VLAN 인터페이스를 생성할 때 VLAN ID를 지정하고 하나 이상의 노드에서 상위(트렁크) 인터페이스를 선택합니다.

마법사에 액세스합니다

1. 구성 * > * 네트워크 * > * VLAN 인터페이스 * 를 선택합니다.
2. Create * 를 선택합니다.

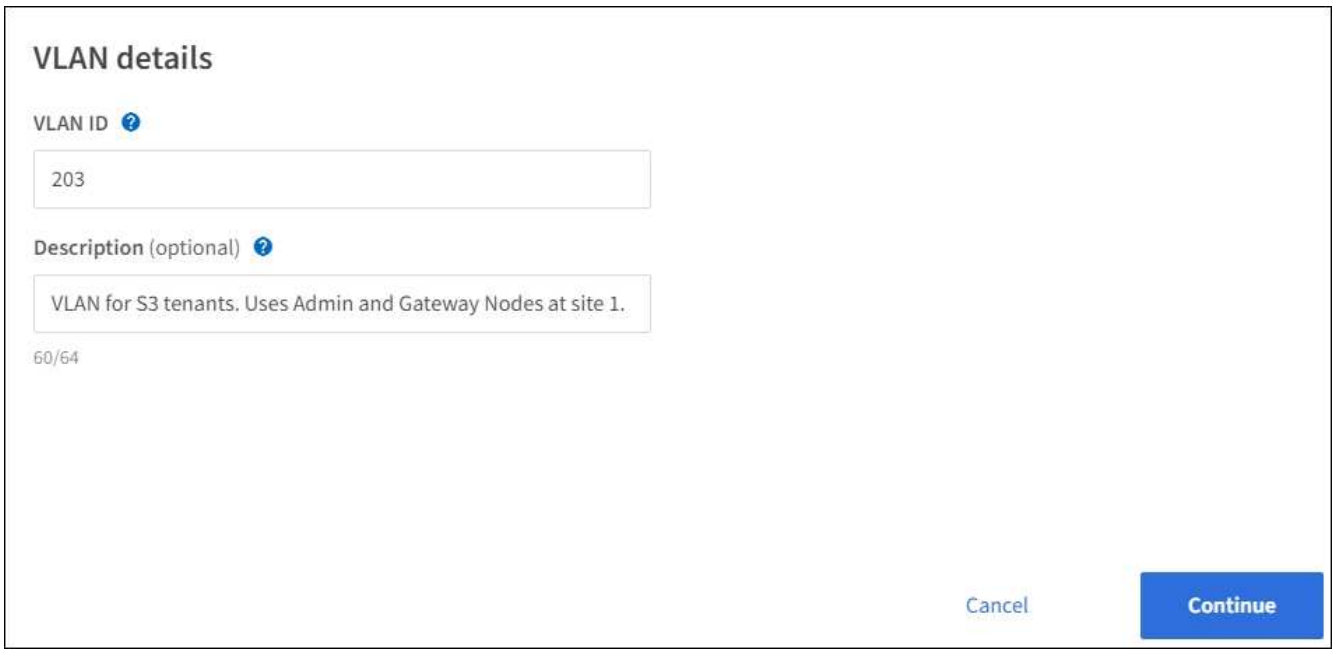
VLAN 인터페이스에 대한 세부 정보를 입력합니다

1. 네트워크에 있는 VLAN의 ID를 지정합니다. 1에서 4094 사이의 값을 입력할 수 있습니다.

   VLAN ID는 고유하지 않아도 됩니다. 예를 들어 한 사이트의 관리 트래픽에는 VLAN ID 200을 사용하고 다른 사이트의 클라이언트 트래픽에는 동일한 VLAN ID를 사용할 수 있습니다. 각 사이트에서 서로 다른 상위 인터페이스 집합을 사용하여 별도의 VLAN 인터페이스를 만들 수 있습니다. 그러나 동일한 ID를 가진 두 VLAN 인터페이스가 노드에서 동일한 인터페이스를 공유할 수 없습니다.

   이미 사용된 ID를 지정하면 메시지가 나타납니다. 동일한 VLAN ID에 대해 다른 VLAN 인터페이스를 계속 만들거나 * Cancel * 을 선택한 다음 기존 ID를 편집할 수 있습니다.

2. 선택적으로 VLAN 인터페이스에 대한 간단한 설명을 입력합니다.



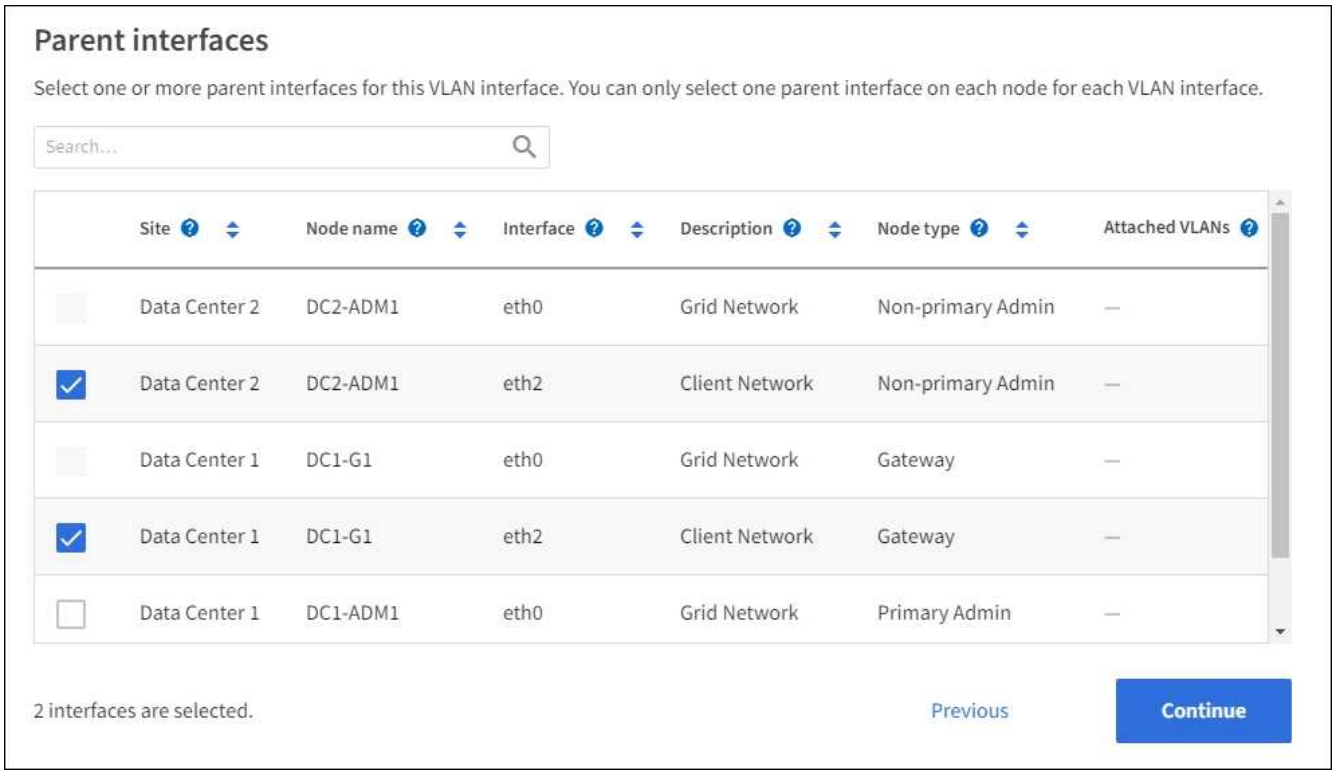
3. Continue * 를 선택합니다.

상위 인터페이스를 선택합니다

표에는 그리드의 각 사이트에 있는 모든 관리 노드 및 게이트웨이 노드에 대해 사용 가능한 인터페이스가 나열됩니다. 관리 네트워크(eth1) 인터페이스는 상위 인터페이스로 사용할 수 없으며 표시되지 않습니다.

1. 이 VLAN을 연결할 상위 인터페이스를 하나 이상 선택하십시오.

   예를 들어, 게이트웨이 노드 및 관리 노드에 대한 클라이언트 네트워크(eth2) 인터페이스에 VLAN을 연결할 수 있습니다.



2. Continue * 를 선택합니다.

설정을 확인합니다

1. 구성을 검토하고 변경합니다.
   - VLAN ID 또는 설명을 변경해야 하는 경우 페이지 맨 위에서 * VLAN 세부 정보 입력 * 을 선택합니다.
   - 상위 인터페이스를 변경해야 하는 경우 페이지 맨 위에서 * 상위 인터페이스 선택 * 을 선택하거나 * 이전 * 을 선택합니다.
   - 상위 인터페이스를 제거해야 하는 경우 휴지통 을 선택합니다 .
2. 저장 * 을 선택합니다.
3. 새 인터페이스가 High Availability 그룹 페이지에서 선택 항목으로 표시되고 해당 노드에 대한 * Network interfaces * 표에 나열될 때까지 최대 5분 정도 기다립니다(* nodes * > **parent interface node* * > * Network *).

VLAN 인터페이스를 편집합니다

VLAN 인터페이스를 편집할 때 다음과 같은 유형의 변경을 수행할 수 있습니다.

- VLAN ID 또는 설명을 변경합니다.

- 부모 인터페이스를 추가하거나 제거합니다.

예를 들어, 연결된 노드의 서비스를 해제하려는 경우 VLAN 인터페이스에서 상위 인터페이스를 제거할 수 있습니다.

다음 사항에 유의하십시오.

- VLAN 인터페이스가 HA 그룹에서 사용되는 경우 VLAN ID를 변경할 수 없습니다.
- 상위 인터페이스가 HA 그룹에서 사용되는 경우에는 상위 인터페이스를 제거할 수 없습니다.

  예를 들어, VLAN 200이 노드 A와 B의 부모 인터페이스에 연결되어 있다고 가정합니다 HA 그룹이 노드 A에 대한 VLAN 200 인터페이스와 노드 B에 대한 eth2 인터페이스를 사용하는 경우 노드 B에 대해 사용되지 않는 부모 인터페이스를 제거할 수 있지만 노드 A에 대해 사용된 부모 인터페이스는 제거할 수 없습니다

단계

1. 구성 * > * 네트워크 * > * VLAN 인터페이스 * 를 선택합니다.
2. 편집할 VLAN 인터페이스의 확인란을 선택합니다. 그런 다음 * Actions * > * Edit * 를 선택합니다.
3. 필요에 따라 VLAN ID 또는 설명을 업데이트합니다. 그런 다음 * 계속 * 을 선택합니다.

   VLAN이 HA 그룹에서 사용되는 경우 VLAN ID를 업데이트할 수 없습니다.

4. 필요에 따라 확인란을 선택하거나 선택 취소하여 부모 인터페이스를 추가하거나 사용하지 않는 인터페이스를 제거합니다. 그런 다음 * 계속 * 을 선택합니다.
5. 구성을 검토하고 변경합니다.
6. 저장 * 을 선택합니다.

VLAN 인터페이스를 제거합니다

하나 이상의 VLAN 인터페이스를 제거할 수 있습니다.

VLAN 인터페이스가 현재 HA 그룹에서 사용되고 있으면 제거할 수 없습니다. VLAN 인터페이스를 제거하려면 먼저 HA 그룹에서 VLAN 인터페이스를 제거해야 합니다.

클라이언트 트래픽의 중단을 방지하려면 다음 중 하나를 수행하는 것이 좋습니다.

- 이 VLAN 인터페이스를 제거하기 전에 HA 그룹에 새 VLAN 인터페이스를 추가하십시오.
- 이 VLAN 인터페이스를 사용하지 않는 새 HA 그룹을 생성합니다.
- 제거하려는 VLAN 인터페이스가 현재 활성 인터페이스인 경우 HA 그룹을 편집합니다. 제거하려는 VLAN 인터페이스를 우선 순위 목록의 맨 아래로 이동합니다. 새 기본 인터페이스에 통신이 설정될 때까지 기다린 다음 HA 그룹에서 이전 인터페이스를 제거합니다. 마지막으로 해당 노드에서 VLAN 인터페이스를 삭제합니다.

단계

1. 구성 * > * 네트워크 * > * VLAN 인터페이스 * 를 선택합니다.
2. 제거할 각 VLAN 인터페이스의 확인란을 선택합니다. 그런 다음 * 작업 * > * 삭제 * 를 선택합니다.
3. 예 * 를 선택하여 선택을 확인합니다.

   선택한 모든 VLAN 인터페이스가 제거됩니다. VLAN 인터페이스 페이지에 녹색 성공 배너가 나타납니다.

고가용성 그룹을 관리합니다

고가용성**(HA)** 그룹 관리**:** 개요

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

HA 그룹이란 무엇입니까**?**

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

각 HA 그룹은 선택한 노드의 공유 서비스에 대한 액세스를 제공합니다.

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

HA 그룹을 어떻게 생성합니까**?**

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

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

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

자세한 내용은 을 참조하십시오 고가용성 그룹을 구성합니다.

액티브 인터페이스란 무엇입니까**?**

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

마찬가지로 정상 작동 중에는 HA 그룹에 대한 우선 순위가 낮은 인터페이스가 "백업" 인터페이스 역할을 합니다. 이러한 백업 인터페이스는 운영(현재 활성) 인터페이스를 사용할 수 없는 경우가 아니면 사용되지 않습니다.

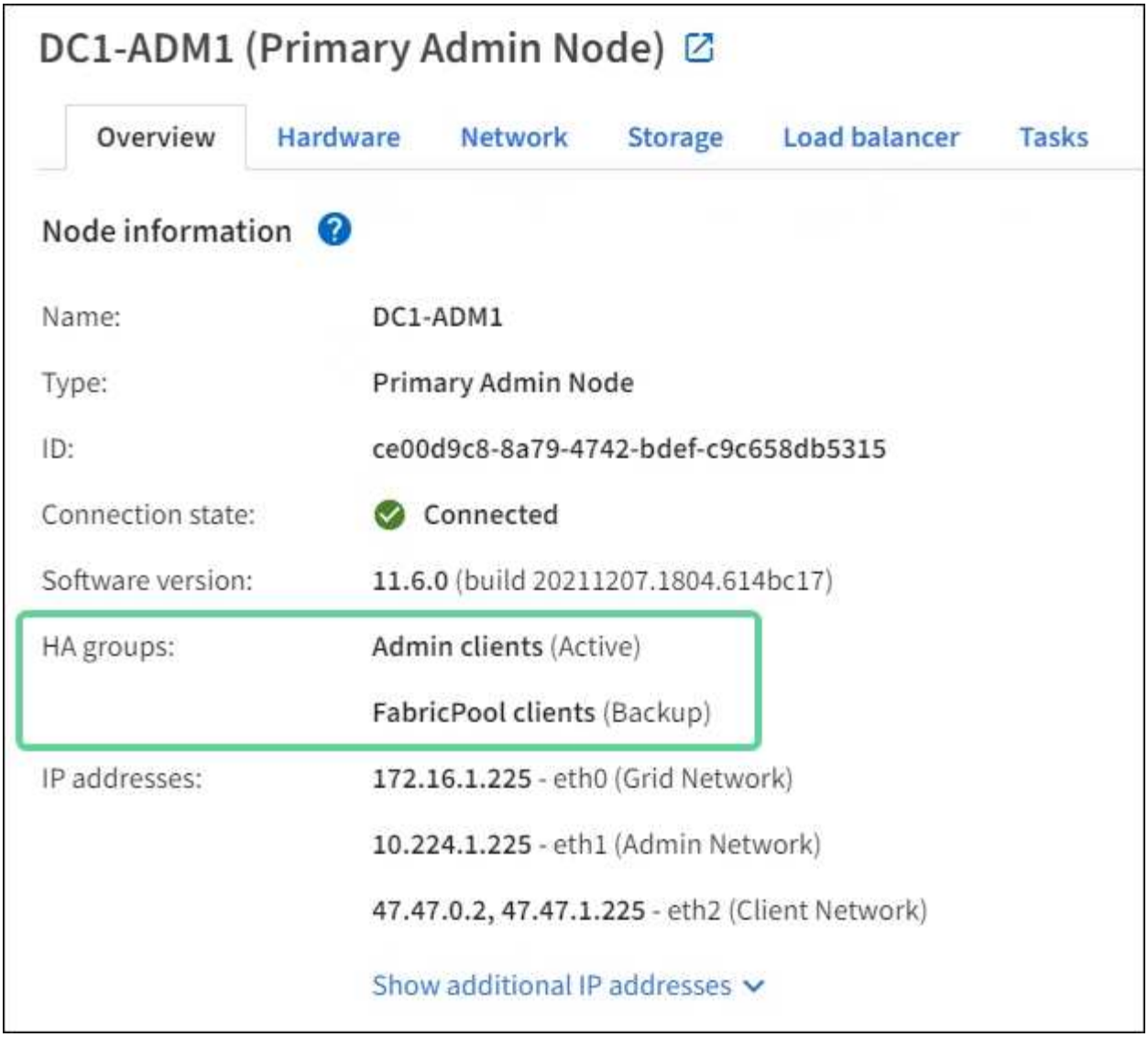
노드의 현재 **HA** 그룹 상태를 봅니다

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

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

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

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



활성 인터페이스가 실패하면 어떻게 됩니까?

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

페일오버는 다음과 같은 이유로 트리거될 수 있습니다.

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

> 활성 인터페이스를 호스팅하는 노드 외부의 네트워크 장애로 인해 페일오버가 트리거되지 않을 수 있습니다. 마찬가지로, 페일오버는 CLB 서비스 장애(더 이상 사용되지 않음) 또는 Grid Manager 또는 테넌트 관리자에 대한 서비스에 의해 트리거되지 않습니다.

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

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

HA 그룹은 어떻게 사용됩니까**?**

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

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

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

- * 관리 노드 *: 로드 밸런서 서비스를 포함하고 그리드 관리자 또는 테넌트 관리자에 대한 액세스를 활성화합니다.
- * 게이트웨이 노드 *: 로드 밸런서 서비스 및 CLB 서비스(더 이상 사용되지 않음)를 포함합니다.

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

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

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

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

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

CLB 서비스에 **HA** 그룹 사용 제한

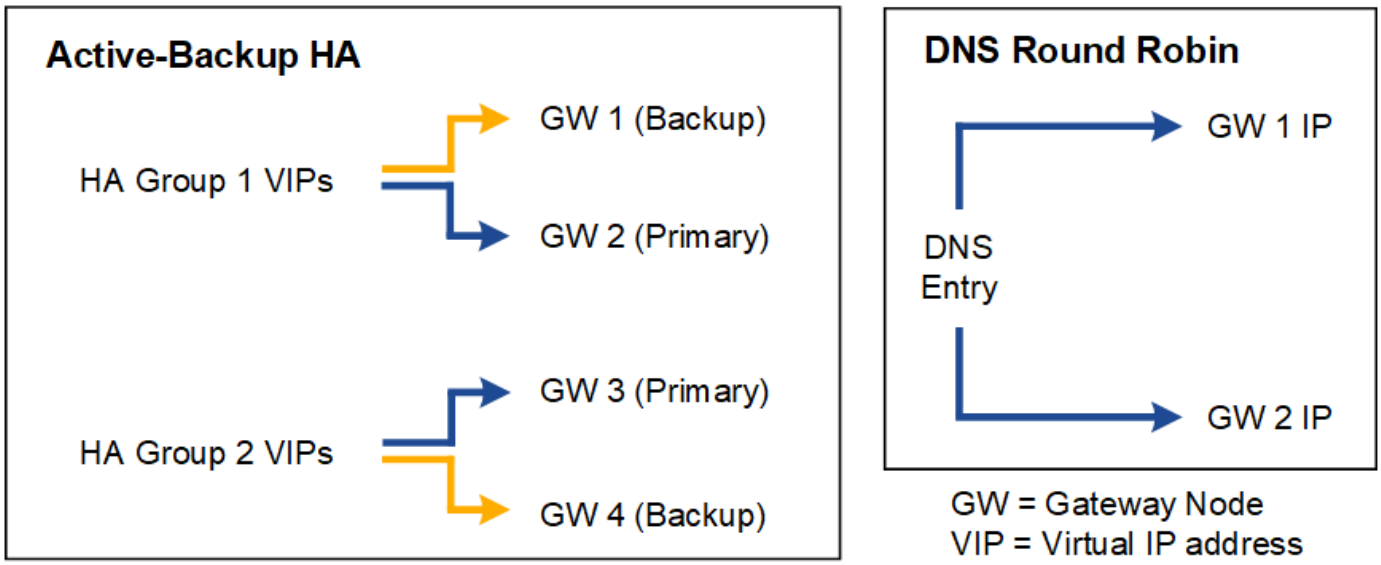
CLB 서비스가 실패해도 HA 그룹 내에서 대체 작동이 트리거되지 않습니다.

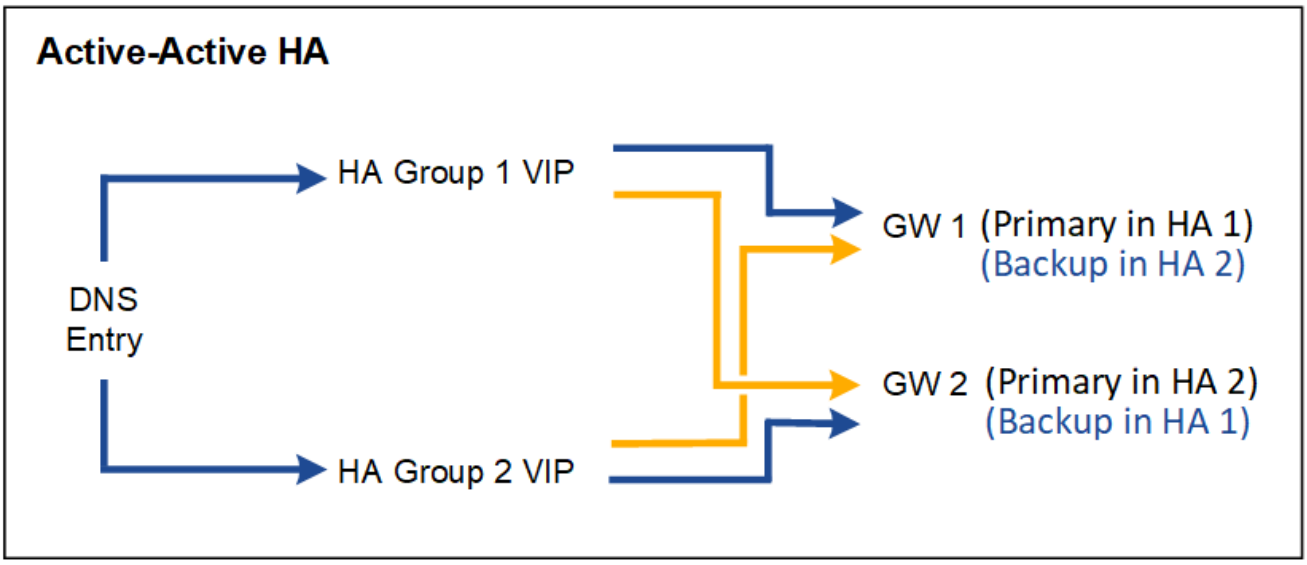
> CLB 서비스는 더 이상 사용되지 않습니다.

HA 그룹에 대한 구성 옵션

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

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





이 표에는 다이어그램에 표시된 각 HA 구성의 이점이 요약되어 있습니다.

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

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

고가용성 그룹을 구성합니다

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

필요한 것

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

고가용성 그룹을 생성합니다

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

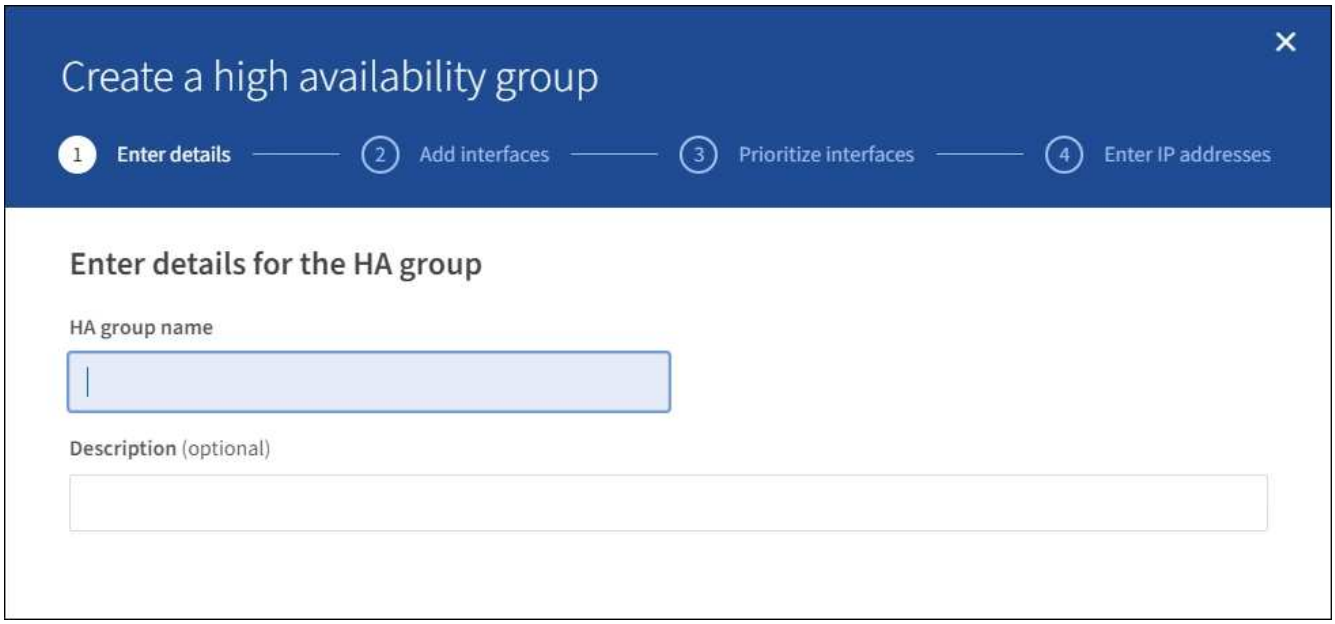
HA 그룹에 포함되려면 게이트웨이 노드 또는 관리 노드에 대한 인터페이스가 있어야 합니다. HA 그룹은 특정 노드에 대해 하나의 인터페이스만 사용할 수 있지만, 동일한 노드에 대한 다른 인터페이스는 다른 HA 그룹에서 사용할 수 있습니다.

마법사에 액세스합니다

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

HA 그룹에 대한 세부 정보를 입력합니다

1. HA 그룹에 고유한 이름을 제공하십시오.

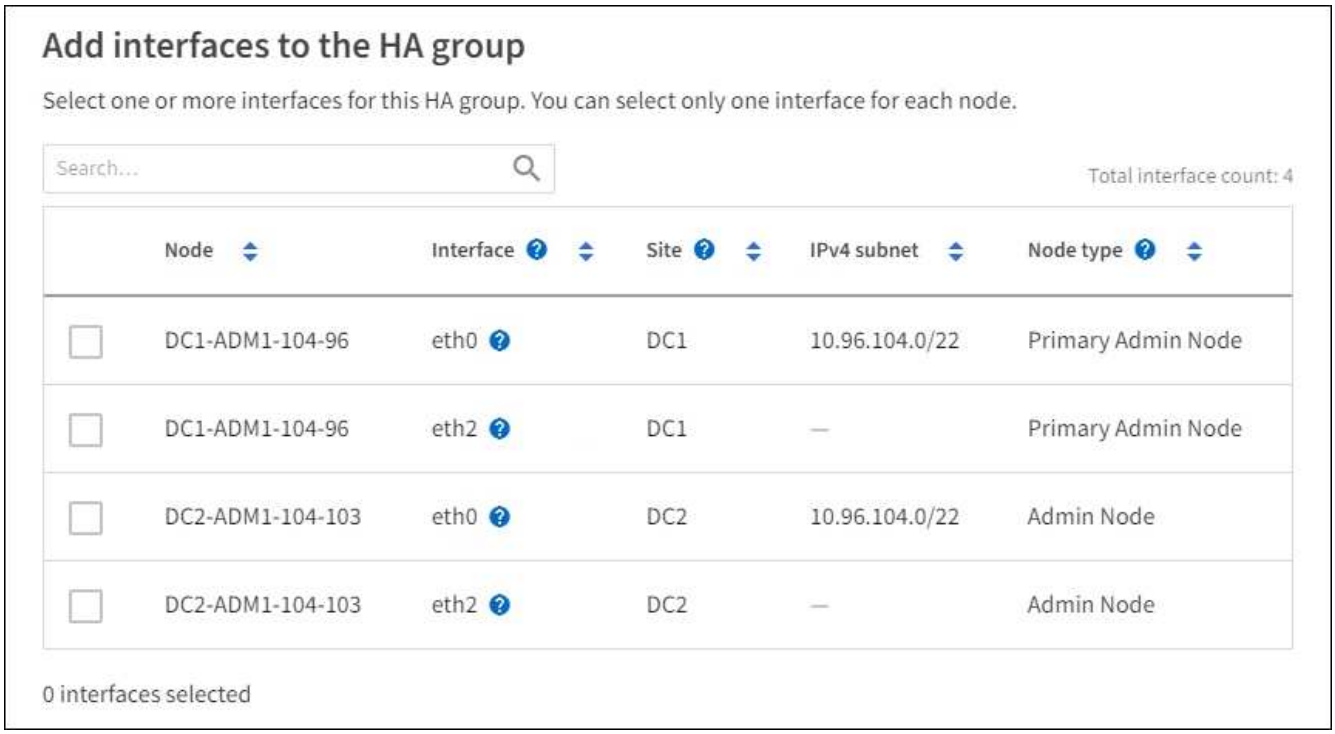


2. 필요에 따라 HA 그룹에 대한 설명을 입력합니다.
3. Continue * 를 선택합니다.

HA 그룹에 인터페이스를 추가합니다

1. 이 HA 그룹에 추가할 인터페이스를 하나 이상 선택하십시오.

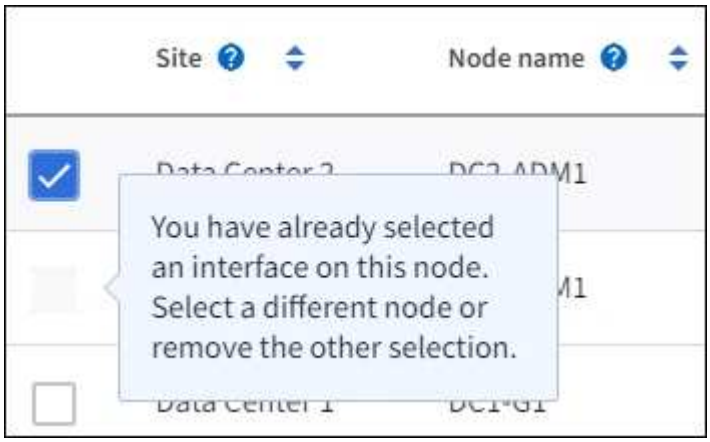
   열 머리글을 사용하여 행을 정렬하거나 검색어를 입력하여 인터페이스를 보다 빠르게 찾을 수 있습니다.



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

인터페이스 선택을 위한 지침

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



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

2. Continue * 를 선택합니다.

우선 순위 순서를 결정합니다

1. 이 HA 그룹에 대한 기본 인터페이스 및 백업(페일오버) 인터페이스를 결정합니다.

   행을 끌어 놓아서 * Priority order * 열의 값을 변경합니다.

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order	Node	Interface	Node type
1 (Primary interface)	DC1-ADM1-104-96	eth2	Primary Admin Node
2	DC2-ADM1-104-103	eth2	Admin Node

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

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

HA 그룹에 둘 이상의 인터페이스가 포함되어 있고 기본 인터페이스에 장애가 발생하면 VIP 주소가 사용 가능한 가장 높은 우선 순위 인터페이스로 이동합니다. 이 인터페이스에 장애가 발생하면 VIP 주소는 사용 가능한 다음 우선 순위 인터페이스로 이동합니다.

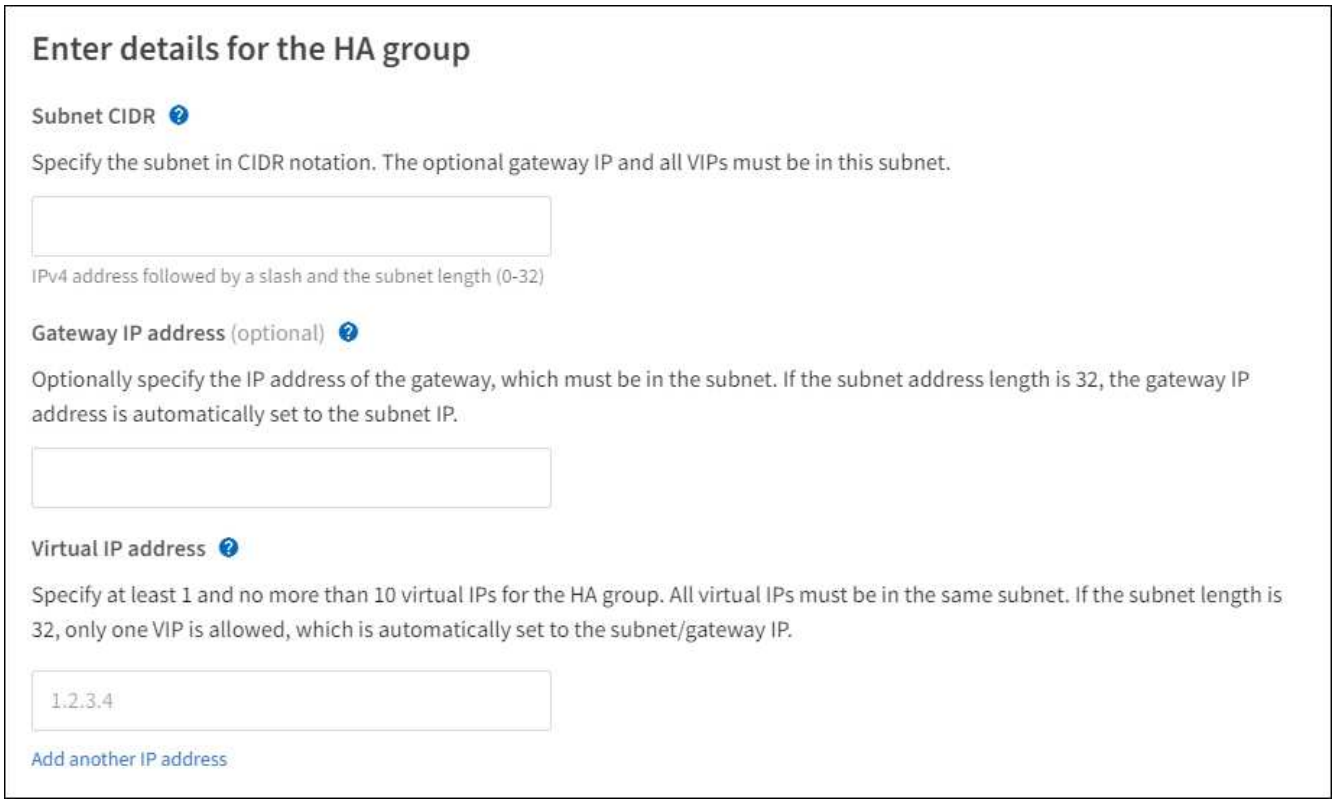
2. Continue * 를 선택합니다.

IP 주소를 입력합니다

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

   네트워크 주소에는 호스트 비트가 설정되어 있지 않아야 합니다. 예를 들어, '192.16.0.0/22'가 있습니다.

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



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

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

3. HA 그룹에 대해 하나 이상의 * 가상 IP 주소 * 를 입력합니다. 최대 10개의 IP 주소를 추가할 수 있습니다. 모든 VIP는 VIP 서브넷 내에 있어야 합니다.

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

4. HA 그룹 생성 * 을 선택하고 * 마침 * 을 선택합니다.

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

> HA 그룹의 변경 사항이 모든 노드에 적용될 때까지 최대 15분간 기다립니다.

다음 단계

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

High Availability 그룹을 편집합니다

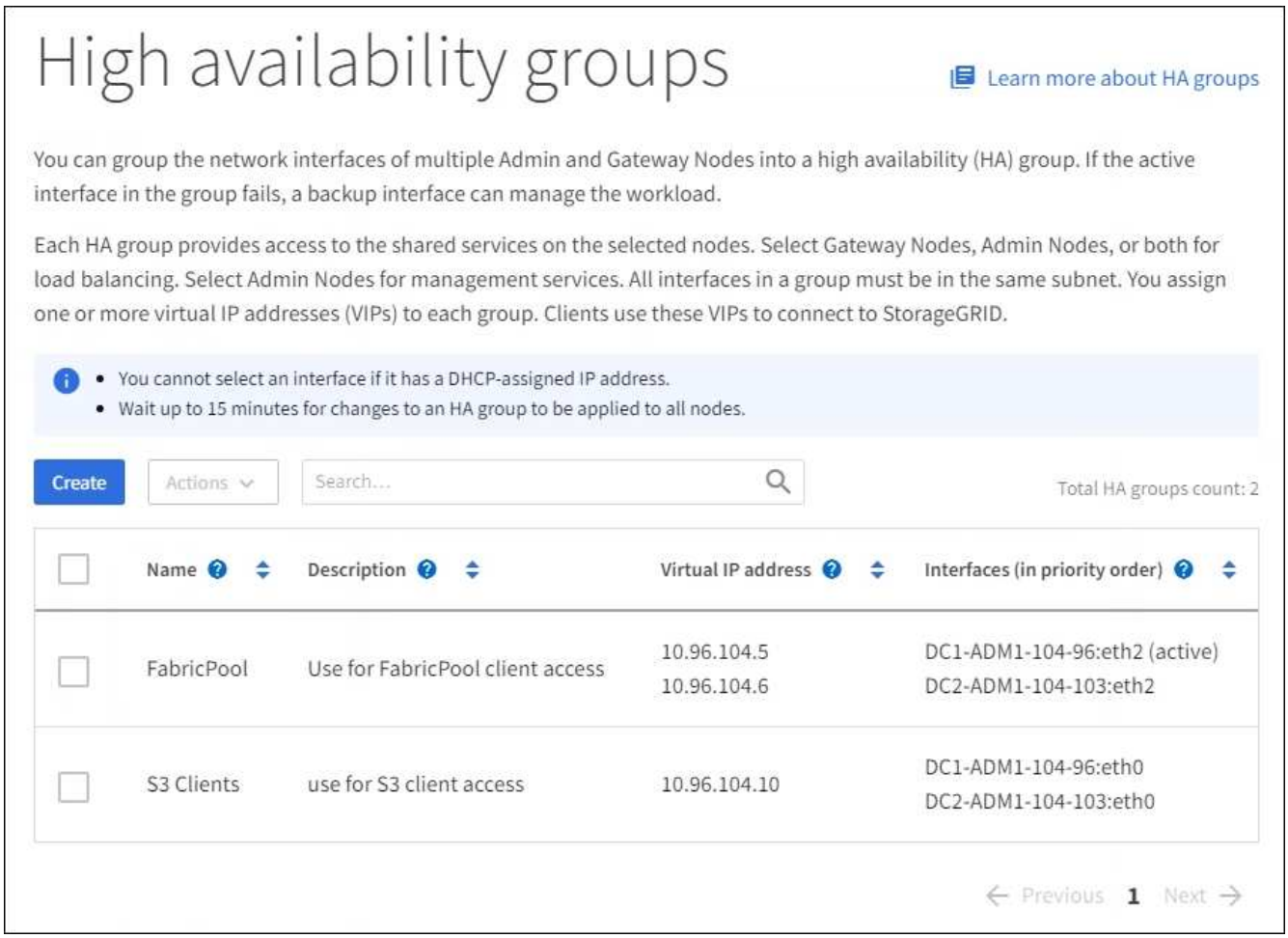
HA(고가용성) 그룹을 편집하여 이름과 설명을 변경하거나, 인터페이스를 추가 또는 제거하거나, 우선 순위 순서를 변경하거나, 가상 IP 주소를 추가 또는 업데이트할 수 있습니다.

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

단계

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

   고가용성 그룹 페이지에는 기존의 모든 HA 그룹이 표시됩니다.



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

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

c. 필요에 따라 행을 끌어서 놓아 이 HA 그룹에 대한 기본 인터페이스 및 백업 인터페이스의 우선 순위를 변경합니다.

d. 필요에 따라 가상 IP 주소를 업데이트합니다.

e. Save * 를 선택한 다음 * Finish * 를 선택합니다.

> HA 그룹의 변경 사항이 모든 노드에 적용될 때까지 최대 15분간 기다립니다.

High Availability 그룹을 제거합니다

HA(고가용성) 그룹을 한 번에 하나 이상 제거할 수 있습니다. 그러나 하나 이상의 로드 밸런서 끝점에 바인딩되어 있는 HA 그룹은 제거할 수 없습니다.

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

단계

1. 구성 * > * 네트워크 * > * 고가용성 그룹 * 을 선택합니다.
2. 제거할 각 HA 그룹에 대한 확인란을 선택합니다. 그런 다음 * 작업 * > * HA 그룹 제거 * 를 선택합니다.
3. 메시지를 검토하고 * Delete HA group * 을 선택하여 선택 사항을 확인합니다.

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

로드 밸런싱 관리

부하 분산 관리: 개요

StorageGRID 로드 밸런싱 기능을 사용하여 S3 및 Swift 클라이언트에서 수집 및 검색 워크로드를 처리할 수 있습니다. 로드 밸런싱은 여러 스토리지 노드에 워크로드와 연결을 분산하여 속도와 연결 용량을 극대화합니다.

다음과 같은 방법으로 클라이언트 워크로드의 로드 밸런싱을 수행할 수 있습니다.

- 관리 노드 및 게이트웨이 노드에 설치된 로드 밸런서 서비스를 사용합니다. 로드 밸런서 서비스는 계층 7 로드 밸런싱을 제공하고 클라이언트 요청에 대한 TLS 종료를 수행하고 요청을 검사하며 스토리지 노드에 대한 새로운 보안 연결을 설정합니다. 이것은 권장되는 로드 밸런싱 메커니즘입니다.

  을 참조하십시오 로드 밸런싱 작동 방식 - 로드 밸런서 서비스.

- 게이트웨이 노드에만 설치된 더 이상 사용되지 않는 CLB(연결 로드 밸런서) 서비스를 사용합니다. CLB 서비스는 계층 4 로드 밸런싱을 제공하고 링크 비용을 지원합니다.

  을 참조하십시오 로드 밸런싱 작동 방식 - CLB 서비스(더 이상 사용되지 않음).

- 타사 로드 밸런서를 통합합니다. 자세한 내용은 NetApp 어카운트 담당자에게 문의하십시오.

로드 밸런싱 작동 방식 - 로드 밸런서 서비스

로드 밸런서 서비스는 들어오는 네트워크 연결을 클라이언트 애플리케이션에서 스토리지 노드로 배포합니다. 로드 밸런싱을 사용하려면 Grid Manager를 사용하여 부하 분산 엔드포인트를 구성해야 합니다.

이러한 노드 유형에는 로드 밸런서 서비스가 포함되어 있으므로 관리 노드 또는 게이트웨이 노드에 대해서만 로드 밸런서 끝점을 구성할 수 있습니다. 스토리지 노드 또는 아카이브 노드의 끝점은 구성할 수 없습니다.

각 로드 밸런서 끝점은 포트, 네트워크 프로토콜(HTTP 또는 HTTPS), 클라이언트 유형(S3 또는 Swift) 및 바인딩 모드를 지정합니다. HTTPS 엔드포인트에는 서버 인증서가 필요합니다. 바인딩 모드를 사용하면 엔드포인트 포트의 액세스를 다음과 같이 제한할 수 있습니다.

- 특정 HA(고가용성) 그룹의 가상 IP 주소(VIP
- 특정 관리 및 게이트웨이 노드의 특정 네트워크 인터페이스

포트 고려 사항

클라이언트는 로드 밸런서 서비스를 실행하는 노드에서 구성한 모든 끝점에 액세스할 수 있습니다. 단, 포트 80과 443은 관리 노드에 예약되므로 이러한 포트에 구성된 끝점은 게이트웨이 노드에서만 로드 밸런싱 작업을 지원합니다.

포트를 다시 매핑한 경우 동일한 포트를 사용하여 로드 밸런서 끝점을 구성할 수 없습니다. 다시 매핑된 포트를 사용하여 끝점을 만들 수 있지만 이러한 끝점은 로드 밸런서 서비스가 아닌 원래 CLB 포트 및 서비스에 다시 매핑됩니다. 의 단계를 따릅니다 포트 재맵을 제거합니다.

> CLB 서비스는 더 이상 사용되지 않습니다.

CPU 가용성

각 관리 노드와 게이트웨이 노드의 로드 밸런서 서비스는 S3 또는 Swift 트래픽을 스토리지 노드로 전달할 때 독립적으로 작동합니다. 로드 밸런서 서비스는 가중 프로세스를 통해 더 많은 요청을 CPU 가용성이 높은 스토리지 노드로 라우팅합니다. 노드 CPU 로드 정보는 몇 분마다 업데이트되지만 가중치는 더 자주 업데이트될 수 있습니다. 모든 스토리지 노드에는 최소 기본 가중치 값이 할당됩니다. 이는 노드에서 100% 사용률을 보고하거나 사용률을 보고하지 않는 경우에도 마찬가지입니다.

경우에 따라 CPU 가용성에 대한 정보는 로드 밸런서 서비스가 있는 사이트로 제한됩니다.

로드 밸런서 엔드포인트를 구성합니다

로드 밸런서 끝점은 게이트웨이 및 관리 노드의 StorageGRID 로드 밸런서에 연결할 때 사용할 수 있는 포트 및 네트워크 프로토콜 S3 및 Swift 클라이언트를 결정합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.
- 로드 밸런서 끝점에 사용할 포트를 이전에 다시 매핑한 경우 포트 재맵을 제거했습니다.

- 사용할 고가용성(HA) 그룹을 만들었습니다. HA 그룹이 권장되지만 필수는 아닙니다. 을 참조하십시오 고가용성 그룹을 관리합니다.
- 에서 로드 밸런서 끝점을 사용하는 경우 S3 테넌트를 선택합니다, Bare-Metal 노드의 IP 주소 또는 FQDN을 사용해서는 안 됩니다. S3 Select에 사용되는 로드 밸런싱 장치 엔드포인트에는 SG100 또는 SG1000 어플라이언스 및 VMware 기반 소프트웨어 노드만 허용됩니다.
- 사용할 VLAN 인터페이스를 구성했습니다. 을 참조하십시오 VLAN 인터페이스를 구성합니다.
- HTTPS 끝점을 만드는 경우(권장) 서버 인증서에 대한 정보가 있습니다.

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

  - 인증서를 업로드하려면 서버 인증서, 인증서 개인 키 및 선택적으로 CA 번들이 필요합니다.
  - 인증서를 생성하려면 S3 또는 Swift 클라이언트가 끝점에 액세스하는 데 사용할 모든 도메인 이름과 IP 주소가 필요합니다. 제목(고유 이름)도 알아야 합니다.
  - StorageGRID S3 및 Swift API 인증서(스토리지 노드에 직접 연결하는 데에도 사용 가능)를 사용하려면 이미 기본 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 교체했습니다. 을 참조하십시오S3 및 Swift API 인증서를 구성합니다.

    이 인증서는 와일드카드를 사용하여 로드 밸런서 서비스를 실행하는 모든 관리 노드 및 게이트웨이 노드의 정규화된 도메인 이름을 나타낼 수 있습니다. 예를 들어, '* .storagegrid.*example*.com'은 ' adm1.storagegrid.*example*.com ' 및 ' gn1.storagegrid.*example*.com ' 을 나타내는 * 와일드카드를 사용합니다. 을 참조하십시오 S3 API 엔드포인트 도메인 이름을 구성합니다.

로드 밸런서 끝점을 만듭니다

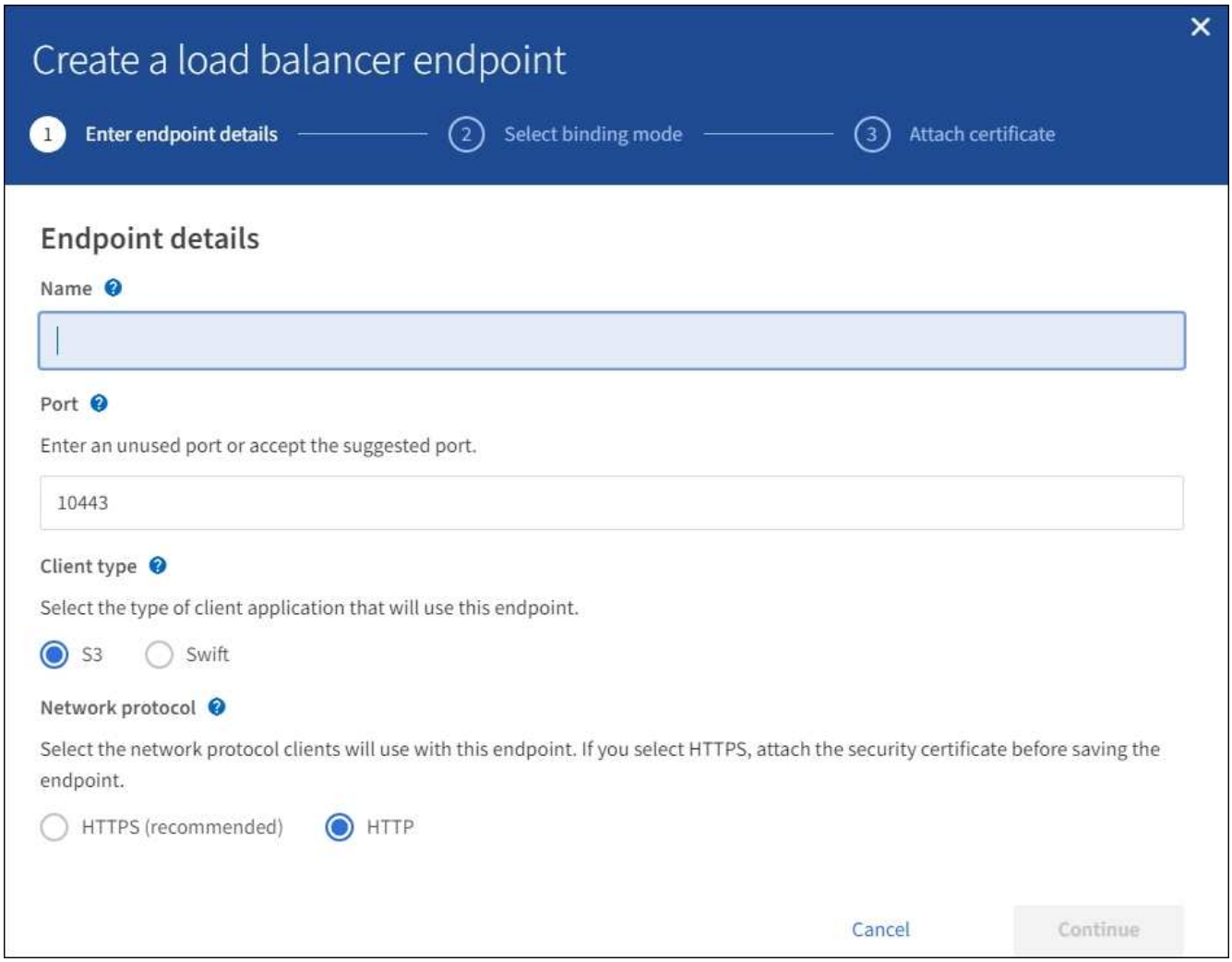
각 로드 밸런서 끝점은 포트, 클라이언트 유형(S3 또는 Swift) 및 네트워크 프로토콜(HTTP 또는 HTTPS)을 지정합니다.

마법사에 액세스합니다

1. 구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 * 를 선택합니다.
2. Create * 를 선택합니다.

끝점 세부 정보를 입력합니다

1. 끝점의 세부 정보를 입력합니다.



필드에 입력합니다	설명
이름	Load Balancer Endpoints(분산 장치 끝점 로드) 페이지의 테이블에 표시되는 끝점에 대한 설명 이름입니다.
포트	포트 클라이언트는 를 사용하여 관리 노드 및 게이트웨이 노드의 로드 밸런서 서비스에 연결합니다. 제안된 포트 번호를 수락하거나 다른 그리드 서비스에서 사용되지 않는 외부 포트를 입력합니다. 1에서 65535 사이의 값을 입력합니다. 80 * 또는 * 443 * 을 입력하면 끝점이 게이트웨이 노드에서만 구성됩니다. 이러한 포트는 관리 노드에 예약되어 있습니다. 를 참조하십시오 네트워킹 지침 외부 포트에 대한 자세한 내용은 를 참조하십시오.
클라이언트 유형입니다	이 끝점을 사용할 클라이언트 응용 프로그램 유형, * S3 * 또는 * Swift *.

필드에 입력합니다	설명
네트워크 프로토콜	클라이언트가 이 끝점에 연결할 때 사용할 네트워크 프로토콜입니다. • TLS 암호화 보안 통신을 위해 * HTTPS * 를 선택합니다(권장). 끝점을 저장하려면 먼저 보안 인증서를 연결해야 합니다. • 보안이 취약한 암호화되지 않은 통신을 위해 * HTTP * 를 선택합니다. 비프로덕션 그리드에만 HTTP를 사용합니다.

2. Continue * 를 선택합니다.

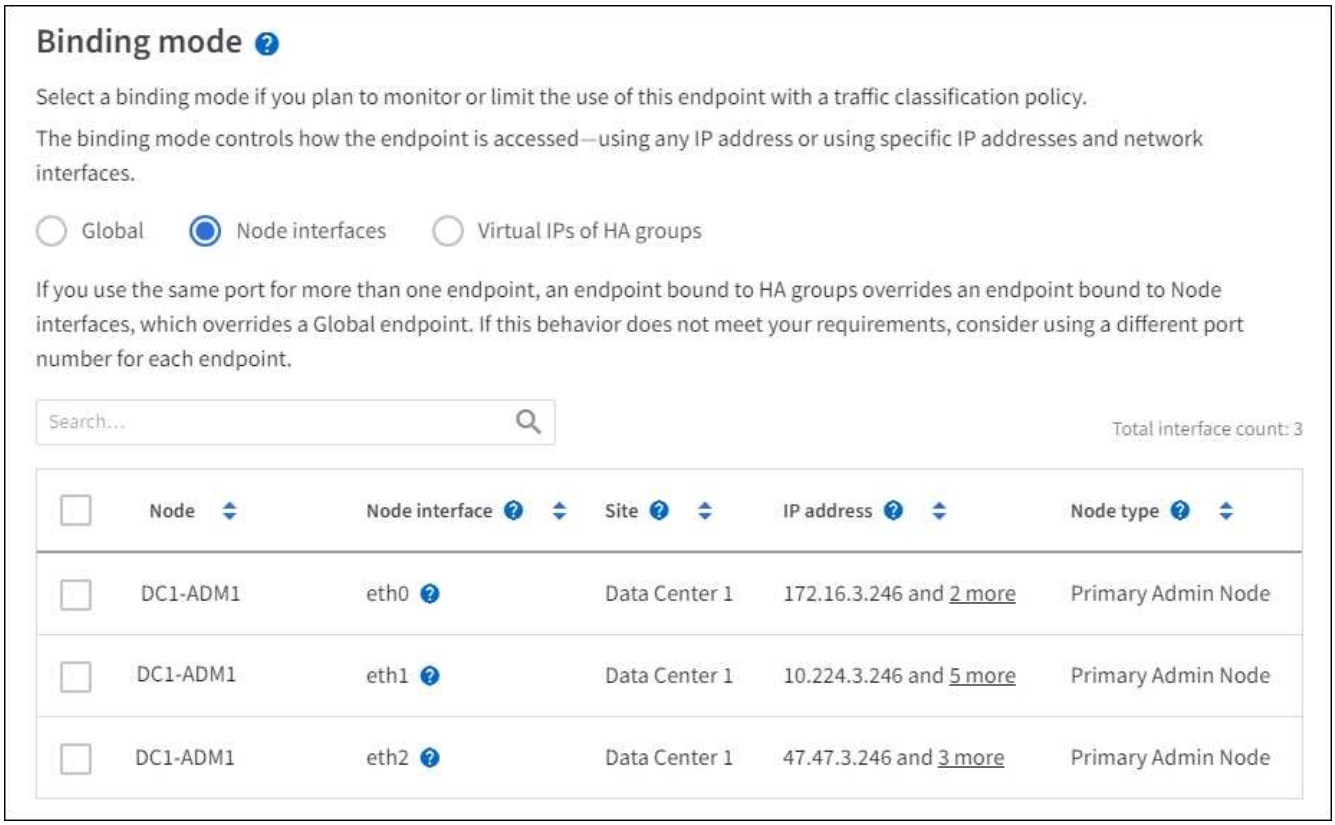
바인딩 모드를 선택합니다

1. 끝점에 대한 바인딩 모드를 선택하여 끝점에 액세스하는 방법을 제어합니다.

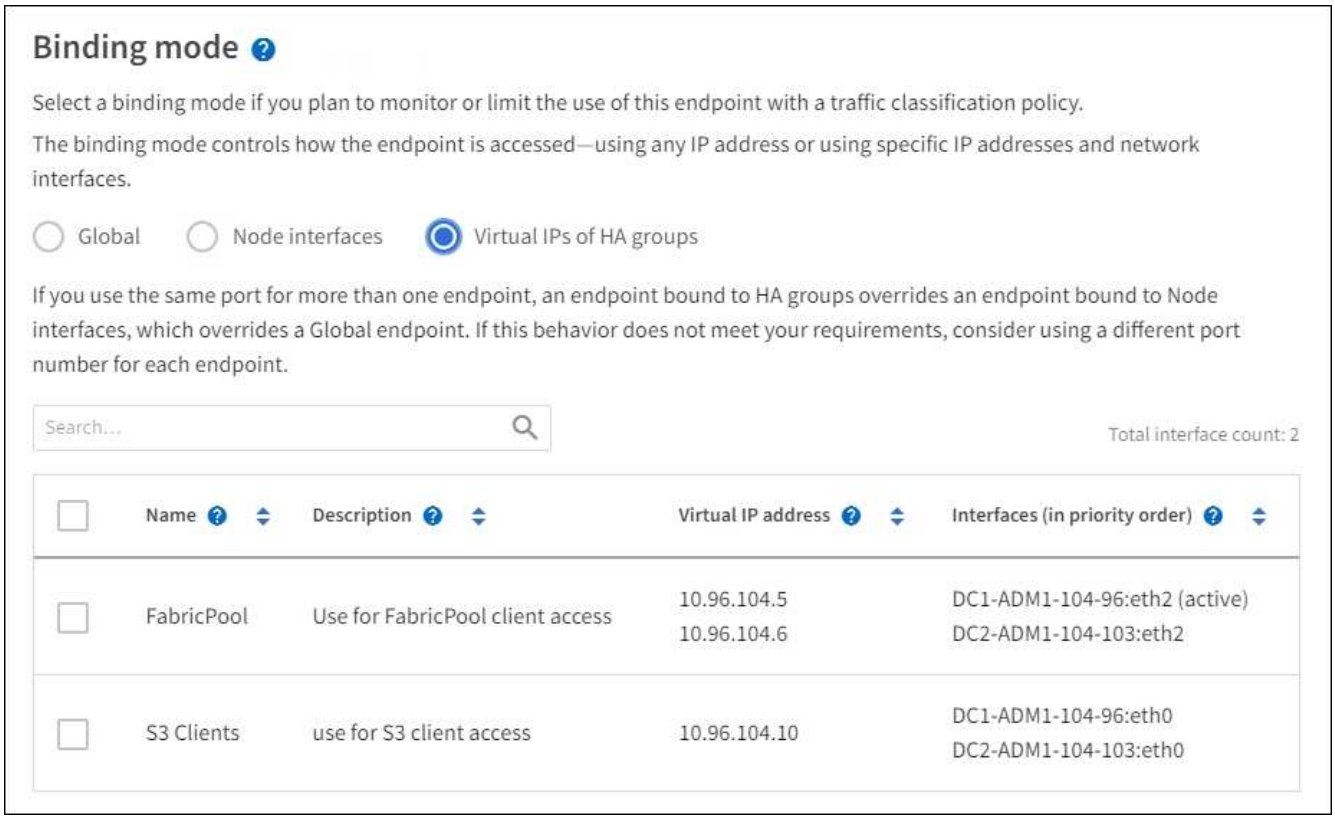
옵션을 선택합니다	설명
글로벌(기본값)	클라이언트는 FQDN(정규화된 도메인 이름), 게이트웨이 노드 또는 관리 노드의 IP 주소 또는 네트워크에 있는 HA 그룹의 가상 IP 주소를 사용하여 끝점에 액세스할 수 있습니다. 이 끝점의 접근성을 제한할 필요가 없는 경우 * Global * (글로벌 *) 설정(기본값)을 사용합니다.
노드 인터페이스	클라이언트는 선택한 노드와 네트워크 인터페이스의 IP 주소를 사용하여 이 끝점에 액세스해야 합니다.
HA 그룹의 가상 IP입니다	클라이언트는 이 끝점에 액세스하기 위해 HA 그룹의 가상 IP 주소를 사용해야 합니다. 이 바인딩 모드의 엔드포인트는 엔드포인트에 대해 선택한 HA 그룹이 겹치지 않는 한 모두 동일한 포트 번호를 사용할 수 있습니다. 이 모드를 사용하는 끝점은 끝점에 대해 선택한 인터페이스가 겹치지 않는 한 모두 동일한 포트 번호를 사용할 수 있습니다.

> 두 개 이상의 끝점에 대해 동일한 포트를 사용하는 경우 * HA 그룹의 가상 IP * 모드를 사용하는 끝점은 * 글로벌 * 모드를 사용하여 끝점을 재정의하는 * 노드 인터페이스 * 모드를 사용하는 끝점에 우선합니다.

2. 노드 인터페이스 * 를 선택한 경우 이 끝점과 연결할 각 관리 노드 또는 게이트웨이 노드에 대해 하나 이상의 노드 인터페이스를 선택합니다.



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



4. HTTP* 끝점을 만드는 경우에는 인증서를 첨부할 필요가 없습니다. 새 로드 밸런서 끝점을 추가하려면 * Create * 를 선택합니다. 그런 다음 로 이동합니다 작업을 마친 후. 그렇지 않으면 * 계속 * 을 선택하여 인증서를 첨부하십시오.

인증서를 첨부합니다

1. HTTPS* 끝점을 만드는 경우 끝점에 연결할 보안 인증서 유형을 선택합니다.

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

   - * 인증서 업로드 *. 업로드할 사용자 지정 인증서가 있는 경우 이 옵션을 선택합니다.
   - * 인증서 생성 *. 사용자 지정 인증서를 생성하는 데 필요한 값이 있는 경우 이 옵션을 선택합니다.
   - * StorageGRID S3 및 Swift 인증서 사용 *. 글로벌 S3 및 Swift API 인증서를 사용하려면 이 옵션을 선택합니다. 스토리지 노드에 직접 연결하는 데에도 이 인증서를 사용할 수 있습니다.

     GRID CA에서 서명한 기본 S3 및 Swift API 인증서를 외부 인증 기관이 서명한 사용자 지정 인증서로 대체하지 않으면 이 옵션을 선택할 수 없습니다. 을 참조하십시오S3 및 Swift API 인증서를 구성합니다.

2. StorageGRID S3 및 Swift 인증서를 사용하지 않는 경우 인증서를 업로드하거나 생성합니다.

인증서를 업로드합니다

a. 인증서 업로드 * 를 선택합니다.

b. 필요한 서버 인증서 파일을 업로드합니다.

   - * 서버 인증서 *: PEM 인코딩의 사용자 정의 서버 인증서 파일.
   - * 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일('.key')입니다.

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

   - * CA 번들 *: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 선택적 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.

c. 업로드한 각 인증서의 메타데이터를 보려면 * 인증서 세부 정보 * 를 확장합니다. 선택적 CA 번들을 업로드한 경우 각 인증서는 자체 탭에 표시됩니다.

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

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

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

d. Create * 를 선택합니다. + 로드 밸런서 끝점이 생성됩니다. 사용자 지정 인증서는 S3 및 Swift 클라이언트와 끝점 간의 이후의 모든 새 연결에 사용됩니다.

인증서를 생성합니다

a. 인증서 생성 * 을 선택합니다.

b. 인증서 정보를 지정합니다.

   - * 도메인 이름 *: 인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
   - * IP *: 인증서에 포함할 하나 이상의 IP 주소입니다.
   - * subject *: X.509 주체 또는 인증서 소유자의 고유 이름(DN)
   - * 일 유효 *: 인증서 만료 후 일 수입니다.

c. Generate * 를 선택합니다.

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

   - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

     인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자가 '.pem'인 파일을 저장합니다.

   예를 들어, 'toragegrid_certificate.pem'

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

e. Create * 를 선택합니다.

로드 밸런서 끝점이 생성됩니다. 사용자 지정 인증서는 S3 및 Swift 클라이언트와 이 엔드포인트 간의 이후의 모든 새 연결에 사용됩니다.

를 클릭합니다

1. DNS(도메인 이름 시스템)를 사용하는 경우 DNS에 StorageGRID 정규화된 도메인 이름을 클라이언트가 연결하는 데 사용할 각 IP 주소에 연결하는 레코드가 포함되어 있는지 확인합니다.

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

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

     또한 DNS 레코드가 와일드카드 이름을 포함하여 필요한 모든 끝점 도메인 이름을 참조하는지 확인해야 합니다.

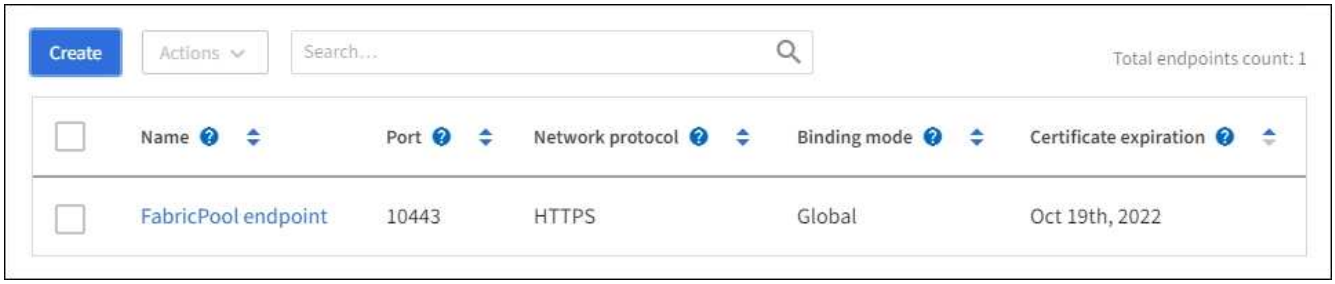
2. S3 및 Swift 클라이언트에 엔드포인트에 연결하는 데 필요한 정보 제공:
   - 포트 번호입니다
   - 정규화된 도메인 이름 또는 IP 주소입니다
   - 필요한 인증서 세부 정보입니다

로드 밸런서 끝점을 보고 편집합니다

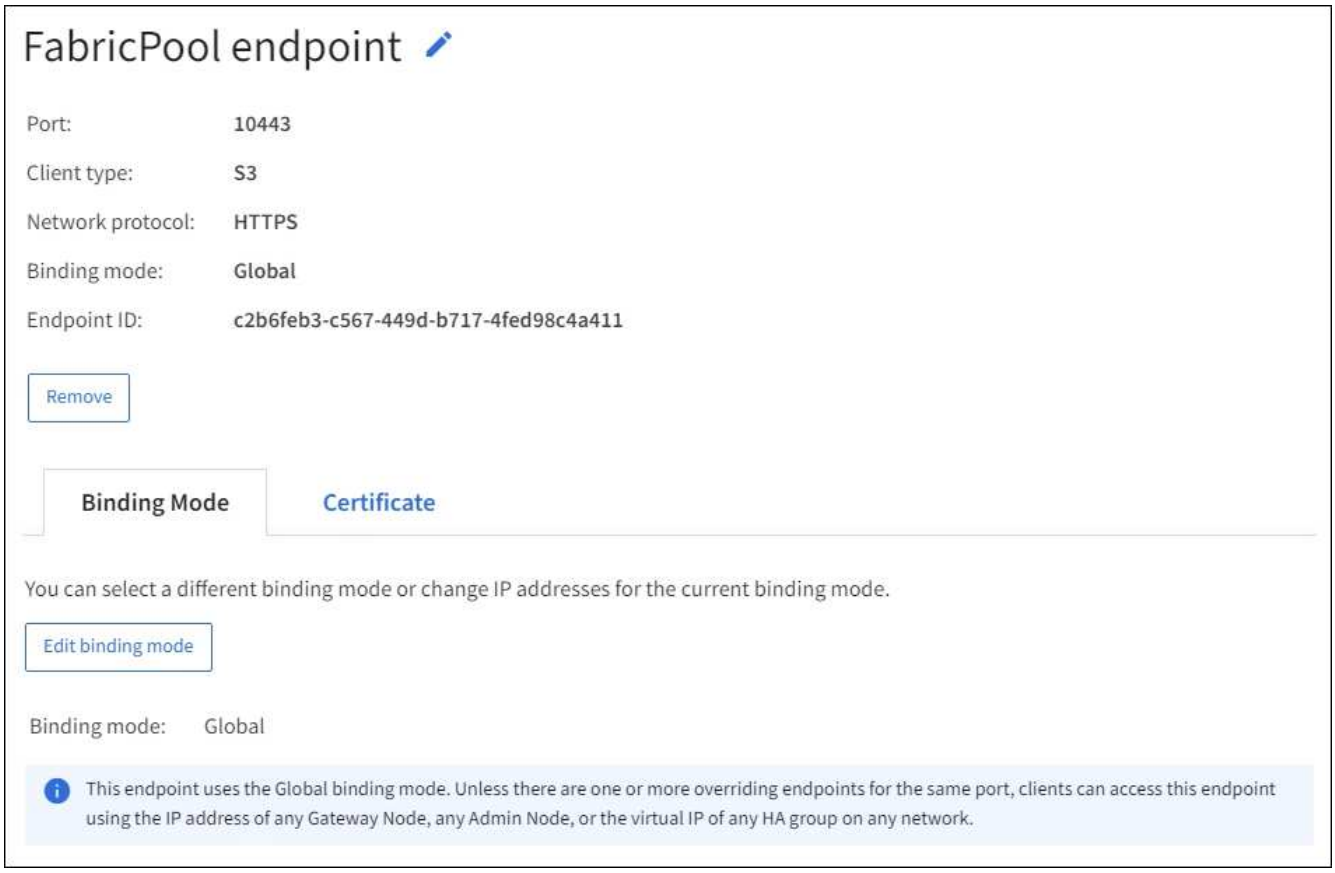
보안 끝점의 인증서 메타데이터를 포함하여 기존 로드 밸런서 끝점에 대한 세부 정보를 볼 수 있습니다. 또한 끝점의 이름 또는 바인딩 모드를 변경하고 연결된 인증서를 업데이트할 수 있습니다.

서비스 유형(S3 또는 Swift), 포트 또는 프로토콜(HTTP 또는 HTTPS)은 변경할 수 없습니다.

- 모든 로드 밸런서 끝점에 대한 기본 정보를 보려면 부하 분산 장치 끝점 페이지의 표를 검토하십시오.



- 인증서 메타데이터를 포함하여 특정 끝점에 대한 모든 세부 정보를 보려면 테이블에서 끝점 이름을 선택합니다.



- 끝점을 편집하려면 부하 분산 끝점 페이지의 * 작업 * 메뉴 또는 특정 끝점의 세부 정보 페이지를 사용합니다.

> 끝점을 편집한 후 변경 내용이 모든 노드에 적용될 때까지 최대 15분 정도 기다려야 할 수 있습니다.

작업	작업 메뉴	세부 정보 페이지
끝점 이름을 편집합니다	a. 끝점의 확인란을 선택합니다. b. 작업 * > * 끝점 이름 편집 * 을 선택합니다. c. 새 이름을 입력합니다. d. 저장 * 을 선택합니다.	a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. 편집 아이콘을 선택합니다 . c. 새 이름을 입력합니다. d. 저장 * 을 선택합니다.
끝점 바인딩 모드를 편집합니다	a. 끝점의 확인란을 선택합니다. b. 작업 * > * 끝점 바인딩 모드 편집 * 을 선택합니다. c. 필요에 따라 바인딩 모드를 업데이트합니다. d. 변경 내용 저장 * 을 선택합니다.	a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. 바인딩 모드 편집 * 을 선택합니다. c. 필요에 따라 바인딩 모드를 업데이트합니다. d. 변경 내용 저장 * 을 선택합니다.

작업	작업 메뉴	세부 정보 페이지
끝점 인증서를 편집합니다	a. 끝점의 확인란을 선택합니다. b. 작업 * > * 끝점 인증서 편집 * 을 선택합니다. c. 필요에 따라 새 사용자 지정 인증서를 업로드하거나 생성하거나 글로벌 S3 및 Swift 인증서를 사용하기 시작합니다. d. 변경 내용 저장 * 을 선택합니다.	a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. Certificate * 탭을 선택합니다. c. 인증서 편집 * 을 선택합니다. d. 필요에 따라 새 사용자 지정 인증서를 업로드하거나 생성하거나 글로벌 S3 및 Swift 인증서를 사용하기 시작합니다. e. 변경 내용 저장 * 을 선택합니다.

로드 밸런서 끝점을 제거합니다

Actions * 메뉴를 사용하여 하나 이상의 끝점을 제거하거나 세부 정보 페이지에서 단일 끝점을 제거할 수 있습니다.

> 클라이언트 중단을 방지하려면 로드 밸런서 엔드포인트를 제거하기 전에 영향을 받는 S3 또는 Swift 클라이언트 애플리케이션을 모두 업데이트하십시오. 다른 로드 밸런서 끝점에 할당된 포트를 사용하여 연결할 각 클라이언트를 업데이트합니다. 필요한 인증서 정보도 업데이트해야 합니다.

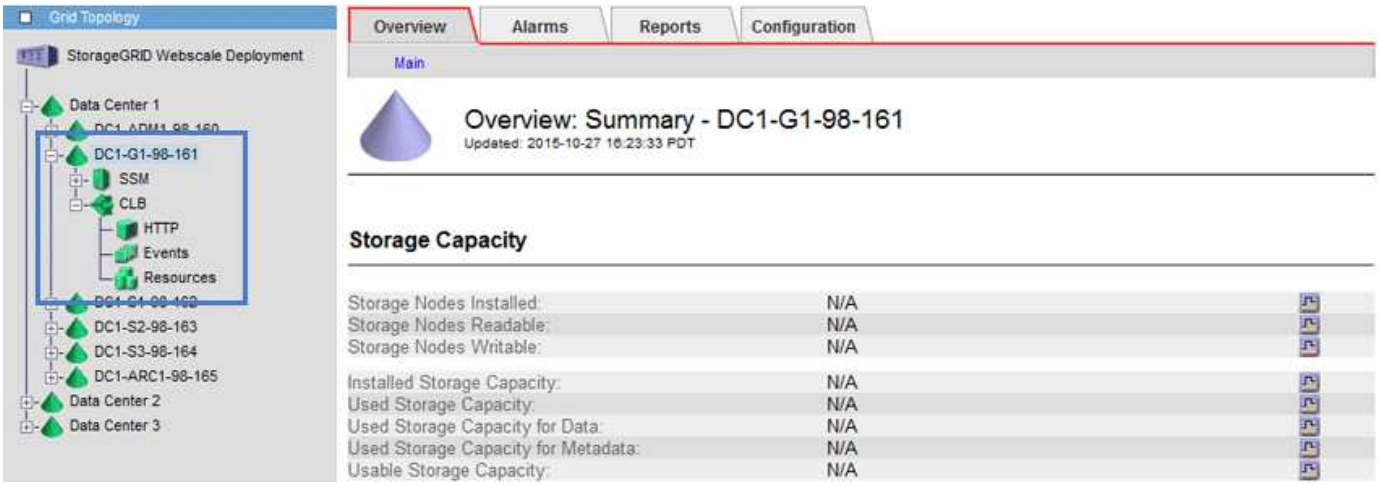
- 하나 이상의 끝점을 제거하려면:
  a. 부하 분산 장치 페이지에서 제거할 각 끝점에 대한 확인란을 선택합니다.
  b. Actions * > * Remove * 를 선택합니다.
  c. OK * 를 선택합니다.
- 세부 정보 페이지에서 끝점 하나를 제거하려면 다음을 수행합니다.
  a. 로드 밸런서 페이지에서 끝점 이름을 선택합니다.
  b. 세부 정보 페이지에서 * 제거 * 를 선택합니다.
  c. OK * 를 선택합니다.

로드 밸런싱 작동 방식 **- CLB** 서비스**(**더 이상 사용되지 않음**)**

게이트웨이 노드의 CLB(연결 로드 밸런서) 서비스는 더 이상 사용되지 않습니다. 이제 로드 밸런서 서비스가 권장되는 로드 밸런싱 메커니즘입니다.

CLB 서비스는 Layer 4 로드 밸런싱을 사용하여 클라이언트 응용 프로그램에서 들어오는 TCP 네트워크 연결을 가용성, 시스템 로드 및 관리자 구성 링크 비용에 따라 최적의 스토리지 노드로 배포합니다. 최적의 스토리지 노드를 선택하면 CLB 서비스는 양방향 네트워크 연결을 설정하고 선택한 노드로 트래픽을 전달합니다. CLB는 들어오는 네트워크 연결을 연결할 때 그리드 네트워크 구성을 고려하지 않습니다.

CLB 서비스에 대한 정보를 보려면 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택한 다음 * CLB * 와 그 아래 옵션을 선택할 때까지 게이트웨이 노드를 확장합니다.



CLB 서비스를 사용하도록 선택한 경우 StorageGRID 시스템에 대한 링크 비용을 구성하는 것이 좋습니다.

- 링크 비용은 얼마입니까
- 링크 비용을 업데이트합니다

S3 API 엔드포인트 도메인 이름을 구성합니다

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

필요한 것

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

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

이 작업에 대해

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

- 그리드 관리자를 사용하여 StorageGRID 시스템에 S3 끝점 도메인 이름을 추가합니다.
- 클라이언트가 StorageGRID에 대한 HTTPS 연결에 사용하는 인증서가 클라이언트에 필요한 모든 도메인 이름에 서명되었는지 확인합니다.

  예를 들어, 끝점이 '3.company.com` 이면 HTTPS 연결에 사용되는 인증서에 '3.company.com` 끝점 및 끝점 와일드카드 주체 대체 이름(SAN):' * .s3.company.com` 이 포함되어 있는지 확인해야 합니다.

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

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

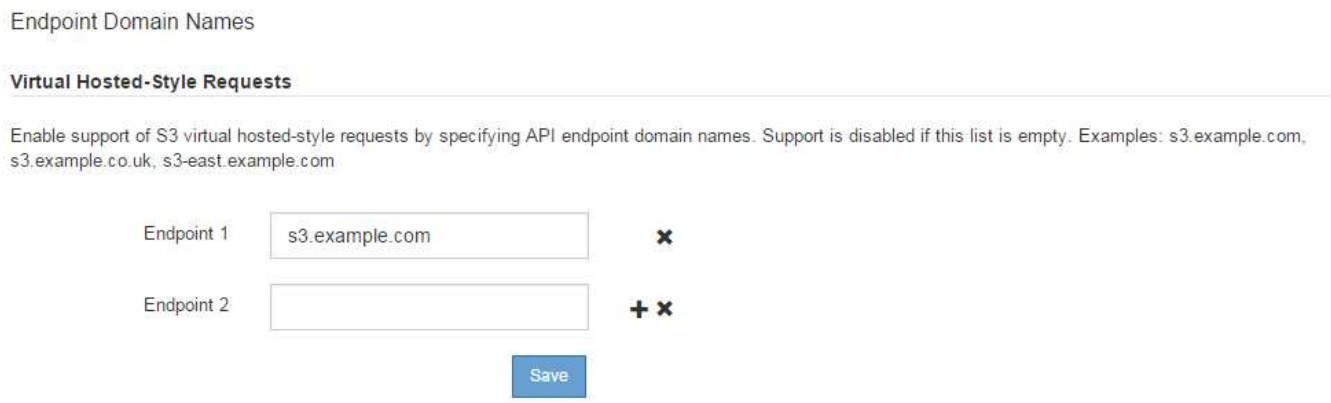
그리드에 HTTPS 연결(권장)을 사용하는 클라이언트는 다음 인증서 중 하나를 사용할 수 있습니다.

- 로드 밸런서 끝점에 연결하는 클라이언트는 해당 끝점에 대해 사용자 지정 인증서를 사용할 수 있습니다. 각 로드 밸런서 끝점은 서로 다른 끝점 도메인 이름을 인식하도록 구성할 수 있습니다.
- 로드 밸런서 끝점에 직접 연결하거나 스토리지 노드에 직접 연결하거나 게이트웨이 노드에서 더 이상 사용되지 않는 CLB 서비스에 직접 연결하는 클라이언트는 글로벌 S3 및 Swift API 인증서를 사용자 지정하여 필요한 모든 끝점 도메인 이름을 포함할 수 있습니다.

단계

1. 구성 * > * 네트워크 * > * 도메인 이름 * 을 선택합니다.

   끝점 도메인 이름 페이지가 나타납니다.



2. 끝점 * 필드에 S3 API 끝점 도메인 이름 목록을 입력합니다. 를 사용합니다 + 아이콘을 클릭하여 추가 필드를 추가합니다.

   이 목록이 비어 있으면 S3 가상 호스팅 스타일 요청에 대한 지원이 비활성화됩니다.

3. 저장 * 을 선택합니다.
4. 클라이언트가 사용하는 서버 인증서가 필요한 끝점 도메인 이름과 일치하는지 확인합니다.
   - 클라이언트가 자체 인증서를 사용하는 로드 밸런서 끝점에 연결하는 경우 끝점과 연결된 인증서를 업데이트합니다.
   - 클라이언트가 글로벌 S3 및 Swift API 인증서를 사용하는 로드 밸런서 끝점에 직접 연결하거나 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 연결하는 경우 글로벌 S3 및 Swift API 인증서를 업데이트합니다.
5. 엔드포인트 도메인 이름 요청을 확인하는 데 필요한 DNS 레코드를 추가합니다.

결과

이제 클라이언트가 끝점 bucket.s3.company.com` 을 사용하면 DNS 서버가 올바른 끝점으로 확인되고 인증서가 예상대로 끝점을 인증합니다.

관련 정보

- S3을 사용합니다
- IP 주소를 봅니다
- 고가용성 그룹을 구성합니다
- S3 및 Swift API 인증서를 구성합니다

- 로드 밸런서 엔드포인트를 구성합니다

클라이언트 통신을 위해 **HTTP**를 활성화합니다

기본적으로 클라이언트 응용 프로그램은 스토리지 노드에 대한 모든 연결 또는 게이트웨이 노드의 더 이상 사용되지 않는 CLB 서비스에 대해 HTTPS 네트워크 프로토콜을 사용합니다. 비프로덕션 그리드를 테스트할 때와 같이 이러한 연결에 대해 HTTP를 선택적으로 활성화할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

S3 및 Swift 클라이언트가 HTTP를 스토리지 노드 또는 게이트웨이 노드의 더 이상 사용되지 않는 CLB 서비스에 직접 연결해야 하는 경우에만 이 작업을 완료합니다.

HTTPS 연결만 사용하는 클라이언트 또는 로드 밸런서 서비스에 연결된 클라이언트에 대해서는 이 작업을 완료할 필요가 없습니다. 각 로드 밸런서 끝점에서 HTTP 또는 HTTPS를 사용하도록 구성할 수 있기 때문입니다. 자세한 내용은 로드 밸런서 엔드포인트 구성에 대한 정보를 참조하십시오.

을 참조하십시오 요약: 클라이언트 연결을 위한 IP 주소 및 포트 스토리지 노드에 연결할 때 또는 HTTP 또는 HTTPS를 사용하여 더 이상 사용되지 않는 CLB 서비스에 연결할 때 사용하는 S3 및 Swift 포트에 대해 알아봅니다

> 요청이 암호화되지 않은 상태로 전송되므로 프로덕션 그리드에 대해 HTTP를 설정할 때는 주의해야 합니다.

단계

1. 구성 * > * 시스템 * > * 그리드 옵션 * 을 선택합니다.
2. 네트워크 옵션 섹션에서 * HTTP 연결 사용 * 확인란을 선택합니다.

3. 저장 * 을 선택합니다.

관련 정보

- 로드 밸런서 엔드포인트를 구성합니다
- S3을 사용합니다
- Swift를 사용합니다

허용되는 클라이언트 작업을 제어합니다

클라이언트 수정 방지 그리드 옵션을 선택하여 특정 HTTP 클라이언트 작업을 거부할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

클라이언트 수정 방지 는 시스템 전체 설정입니다. 클라이언트 수정 방지 옵션을 선택하면 다음 요청이 거부됩니다.

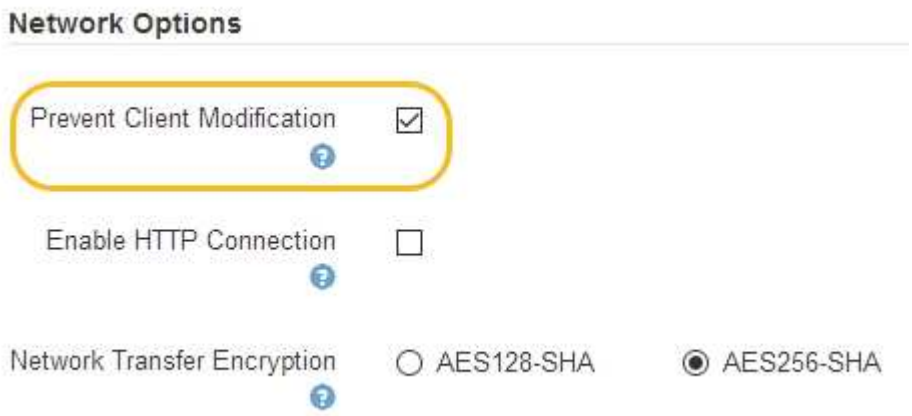
- * S3 REST API *
  - 버킷 요청을 삭제합니다
  - 기존 오브젝트의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태그 지정을 수정하는 요청

> 이 설정은 버전 관리가 활성화된 버킷에는 적용되지 않습니다. 버전 관리를 사용하면 이미 개체 데이터, 사용자 정의 메타데이터 및 개체 태그 지정을 수정할 수 없습니다.

- * Swift REST API *
  - 컨테이너 요청을 삭제합니다
  - 기존 객체 수정 요청. 예를 들어, 덮어쓰기, 삭제, 메타데이터 업데이트 등의 작업이 거부됩니다.

단계

1. 구성 * > * 시스템 * > * 그리드 옵션 * 을 선택합니다.
2. 네트워크 옵션 섹션에서 * 클라이언트 수정 방지 * 확인란을 선택합니다.



3. 저장 * 을 선택합니다.

네트워크 및 연결을 관리합니다

StorageGRID 네트워크 지침

그리드 관리자를 사용하여 StorageGRID 네트워크 및 연결을 구성하고 관리할 수 있습니다.

을 참조하십시오 S3 및 Swift 클라이언트 연결을 구성합니다 S3 또는 Swift 클라이언트를 연결하는 방법에 대해 알아보십시오.

기본 **StorageGRID** 네트워크

기본적으로 StorageGRID는 그리드 노드당 세 개의 네트워크 인터페이스를 지원하므로 각 개별 그리드 노드에 대한 네트워킹을 보안 및 액세스 요구 사항에 맞게 구성할 수 있습니다.

네트워크 토폴로지에 대한 자세한 내용은 을 참조하십시오 네트워킹 지침.

그리드 네트워크

필수 요소입니다. 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용됩니다. 그리드에서 모든 사이트 및 서브넷의 모든 노드 간에 연결을 제공합니다.

관리자 네트워크

선택 사항. 관리 네트워크는 일반적으로 시스템 관리 및 유지 보수에 사용됩니다. 클라이언트 프로토콜 액세스에도 사용할 수 있습니다. 관리 네트워크는 일반적으로 사설 네트워크이며 사이트 간에 라우팅할 필요가 없습니다.

클라이언트 네트워크

선택 사항. 클라이언트 네트워크는 일반적으로 S3 및 Swift 클라이언트 애플리케이션에 대한 액세스를 제공하는 데 사용되는 개방형 네트워크이므로 그리드 네트워크를 격리하고 보호할 수 있습니다. 클라이언트 네트워크는 로컬 게이트웨이를 통해 연결할 수 있는 모든 서브넷과 통신할 수 있습니다.

지침

- 각 StorageGRID 그리드 노드에는 할당된 각 네트워크에 대한 전용 네트워크 인터페이스, IP 주소, 서브넷 마스크 및 게이트웨이가 필요합니다.
- 그리드 노드는 네트워크에 둘 이상의 인터페이스를 가질 수 없습니다.
- 네트워크 당, 그리드 노드별로 단일 게이트웨이가 지원되며 노드와 동일한 서브넷에 있어야 합니다. 필요한 경우 게이트웨이에서 보다 복잡한 라우팅을 구현할 수 있습니다.
- 각 노드에서 각 네트워크는 특정 네트워크 인터페이스에 매핑됩니다.

네트워크	인터페이스 이름입니다
그리드	eth0
관리자(선택 사항)	eth1
클라이언트(선택 사항)	eth2

- 노드가 StorageGRID 어플라이언스에 연결된 경우 각 네트워크에 대해 특정 포트가 사용됩니다. 자세한 내용은 어플라이언스 설치 지침을 참조하십시오.

- 기본 라우트는 노드당 자동으로 생성됩니다. eth2가 활성화된 경우 0.0.0.0/0 은 eth2의 클라이언트 네트워크를 사용합니다. eth2가 활성화되지 않은 경우 0.0.0.0/0 은 eth0의 그리드 네트워크를 사용합니다.
- 그리드 노드가 그리드에 가입될 때까지 클라이언트 네트워크가 작동하지 않습니다
- 그리드 노드를 구축하는 동안 관리 네트워크를 구성하여 그리드를 완전히 설치하기 전에 설치 사용자 인터페이스에 액세스할 수 있습니다.

선택적 인터페이스

선택적으로 노드에 인터페이스를 추가할 수 있습니다. 예를 들어, 를 사용할 수 있도록 트렁크 인터페이스를 관리자 또는 게이트웨이 노드에 추가할 수 있습니다 VLAN 인터페이스 서로 다른 애플리케이션 또는 테넌트에 속한 트래픽을 분리합니다. 또는 에서 사용할 액세스 인터페이스를 추가할 수도 있습니다 고가용성(HA) 그룹.

트렁크 또는 액세스 인터페이스를 추가하려면 다음을 참조하십시오.

- * VMware(노드 설치 후) *: VMware: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다
- * RHEL 또는 CentOS(노드 설치 전) *: 노드 구성 파일을 생성합니다
- * Ubuntu 또는 Debian(노드 설치 전) *: 노드 구성 파일을 생성합니다
- * RHEL, CentOS, Ubuntu 또는 Debian(노드 설치 후) *: Linux: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다

IP 주소를 봅니다

StorageGRID 시스템의 각 그리드 노드에 대한 IP 주소를 볼 수 있습니다. 그런 다음 이 IP 주소를 사용하여 명령줄에서 그리드 노드에 로그인하고 다양한 유지보수 절차를 수행할 수 있습니다.

필요한 것

를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

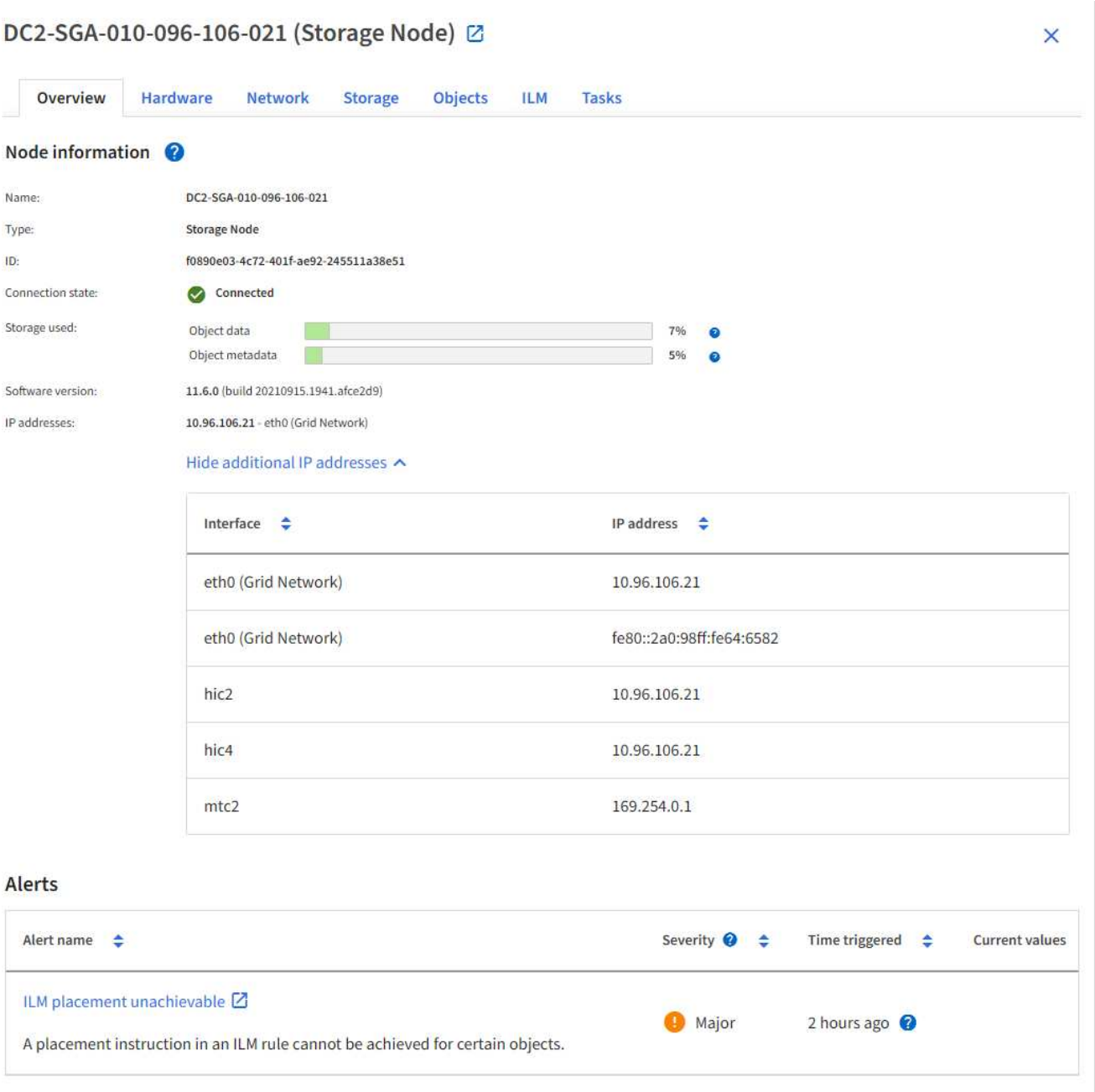
이 작업에 대해

IP 주소 변경에 대한 자세한 내용은 을 참조하십시오 복구 및 유지 관리.

단계

1. nodes * > **GRID node* * > * Overview * 를 선택합니다.
2. IP 주소 제목 오른쪽에 있는 * 더 보기 * 를 선택합니다.

   해당 그리드 노드의 IP 주소가 테이블에 나열됩니다.



발신 **TLS** 연결에 지원되는 암호

StorageGRID 시스템은 ID 페더레이션 및 클라우드 스토리지 풀에 사용되는 외부 시스템에 대한 TLS(Transport Layer Security) 연결을 위한 제한된 암호화 그룹 세트를 지원합니다.

지원되는 **TLS** 버전입니다

StorageGRID는 ID 페더레이션 및 클라우드 스토리지 풀에 사용되는 외부 시스템에 대한 연결을 위해 TLS 1.2 및 TLS 1.3을 지원합니다.

외부 시스템과 호환되도록 외부 시스템에 사용할 수 있도록 지원되는 TLS 암호가 선택되었습니다. 이 목록은 S3 또는 Swift 클라이언트 애플리케이션에서 사용할 수 있도록 지원되는 암호화 목록보다 큽니다.

> 프로토콜 버전, 암호, 키 교환 알고리즘 및 MAC 알고리즘과 같은 TLS 구성 옵션은 StorageGRID에서 구성할 수 없습니다. 이러한 설정에 대한 구체적인 요청이 있을 경우 NetApp 어카운트 담당자에게 문의하십시오.

지원되는 **TLS 1.2** 암호 그룹

지원되는 TLS 1.2 암호 제품군은 다음과 같습니다.

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_with_CHACH20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACH20_POLY1305
- TLS_RSA_with_AES_128_GCM_SHA256
- TLS_RSA_WITED_AES_256_GCM_SHA384

지원되는 **TLS 1.3** 암호 그룹

지원되는 TLS 1.3 암호 제품군은 다음과 같습니다.

- TLS_AES_256_GCM_SHA384
- TLS_CHACH20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

네트워크 전송 암호화를 변경합니다

StorageGRID 시스템은 TLS(Transport Layer Security)를 사용하여 그리드 노드 간의 내부 제어 트래픽을 보호합니다. 네트워크 전송 암호화 옵션은 TLS가 그리드 노드 간의 제어 트래픽을 암호화하는 데 사용하는 알고리즘을 설정합니다. 이 설정은 데이터 암호화에 영향을 주지 않습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

기본적으로 네트워크 전송 암호화는 AES256-SHA 알고리즘을 사용합니다. AES128-SHA 알고리즘을 사용하여 제어 트래픽을 암호화할 수도 있습니다.

단계

1. 구성 * > * 시스템 * > * 그리드 옵션 * 을 선택합니다.
2. 네트워크 옵션 섹션에서 네트워크 전송 암호화를 * AES128-SHA * 또는 * AES256-SHA * (기본값)로 변경합니다.

3. 저장 * 을 선택합니다.

트래픽 분류 정책을 관리합니다

트래픽 분류 정책을 관리합니다

서비스 품질(QoS) 오퍼링을 향상하기 위해 트래픽 분류 정책을 생성하여 다양한 유형의 네트워크 트래픽을 식별 및 모니터링할 수 있습니다. 이러한 정책은 트래픽 제한 및 모니터링을 지원할 수 있습니다.

트래픽 분류 정책은 게이트웨이 노드 및 관리 노드에 대한 StorageGRID 로드 밸런서 서비스의 끝점에 적용됩니다. 트래픽 분류 정책을 생성하려면 로드 밸런서 엔드포인트를 이미 생성해야 합니다.

일치하는 규칙

각 트래픽 분류 정책에는 다음 항목 중 하나 이상에 관련된 네트워크 트래픽을 식별하기 위한 하나 이상의 일치하는 규칙이 포함되어 있습니다.

- 버킷
- 테넌트
- 서브넷(클라이언트가 포함된 IPv4 서브넷)
- 엔드포인트(로드 밸런서 엔드포인트)

StorageGRID는 규칙의 목적에 따라 정책 내의 규칙과 일치하는 트래픽을 모니터링합니다. 정책에 대한 규칙과 일치하는 모든 트래픽은 해당 정책에 의해 처리됩니다. 반대로, 지정된 엔터티를 제외한 모든 트래픽에 일치시키는 규칙을 설정할 수 있습니다.

트래픽 제한

필요에 따라 다음 매개 변수를 기반으로 정책에 대한 제한을 설정할 수 있습니다.

- 총 대역폭
- 총 대역폭 출력
- 동시 읽기 요청
- 동시 쓰기 요청
- 요청 당 대역폭
- 요청 당 대역폭 출력

- 읽기 요청 속도
- 쓰기 요청 속도

제한 값은 부하 분산 장치별로 적용됩니다. 트래픽이 여러 부하 분산 장치에 동시에 분산되는 경우 총 최대 속도는 사용자가 지정한 속도 제한의 배수입니다.

> 정책을 생성하여 애그리게이트 대역폭을 제한하거나 요청당 대역폭을 제한할 수 있습니다. 그러나 StorageGRID는 두 가지 유형의 대역폭을 동시에 제한할 수 없습니다. 애그리게이트 대역폭 제한은 제한 없는 트래픽에 약간의 성능 영향을 줄 수 있습니다.

애그리게이트 또는 요청별 대역폭 제한의 경우 요청은 사용자가 설정한 속도로 스트림 인 또는 아웃됩니다. StorageGRID는 단 하나의 속도만 적용할 수 있으므로 가장 구체적인 정책 매칭은 매처 유형별로 적용됩니다. 다른 모든 제한 유형의 경우 클라이언트 요청이 250밀리초 지연되고 일치하는 정책 제한을 초과하는 요청에 대해 503 느린 응답 응답을 수신합니다.

Grid Manager에서 트래픽 차트를 보고 정책이 기대하는 트래픽 제한을 적용하고 있는지 확인할 수 있습니다.

SLA와 함께 트래픽 분류 정책을 사용합니다

용량 제한 및 데이터 보호와 함께 트래픽 분류 정책을 사용하여 용량, 데이터 보호 및 성능에 대한 세부 정보를 제공하는 서비스 수준 계약(SLA)을 적용할 수 있습니다.

트래픽 분류 제한은 부하 분산 장치에 따라 구현됩니다. 트래픽이 여러 부하 분산 장치에 동시에 분산되는 경우 총 최대 속도는 사용자가 지정한 속도 제한의 배수입니다.

다음 예에서는 SLA의 세 가지 계층을 보여 줍니다. 트래픽 분류 정책을 작성하여 각 SLA 계층의 성능 목표를 달성할 수 있습니다.

서비스 수준 계층	용량	데이터 보호	성능	비용
골드	1PB의 스토리지가 허용됩니다	3 ILM 규칙을 복사합니다	초당 25K 요청 5GB/sec(40Gbps) 대역폭	$$/월
실버	250TB 저장 가능	2 ILM 규칙을 복사합니다	초당 10K 요청 1.25GB/sec(10Gbps) 대역폭	$$/월
브론즈	100TB 스토리지 허용	2 ILM 규칙을 복사합니다	초당 5K 요청 1 GB/sec(8Gbps) 대역폭	$/월

트래픽 분류 정책을 생성합니다

버킷, 테넌트, IP 서브넷 또는 로드 밸런서 끝점별로 네트워크 트래픽을 모니터링하고 선택적으로 제한하려는 경우 트래픽 분류 정책을 생성합니다. 필요에 따라 대역폭, 동시 요청 수 또는 요청 속도를 기준으로 정책에 대한 제한을 설정할 수 있습니다.

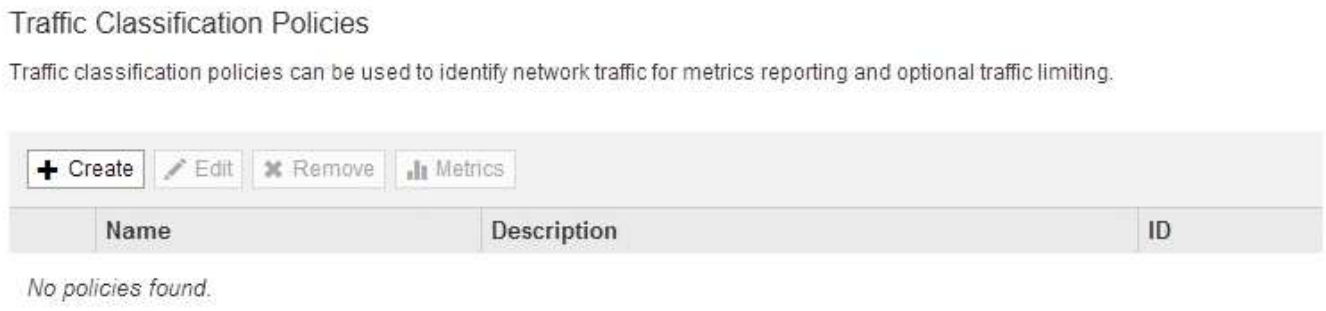
필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.
- 일치시킬 로드 밸런서 끝점을 만들었습니다.
- 일치시킬 테넌트를 만들었습니다.

단계

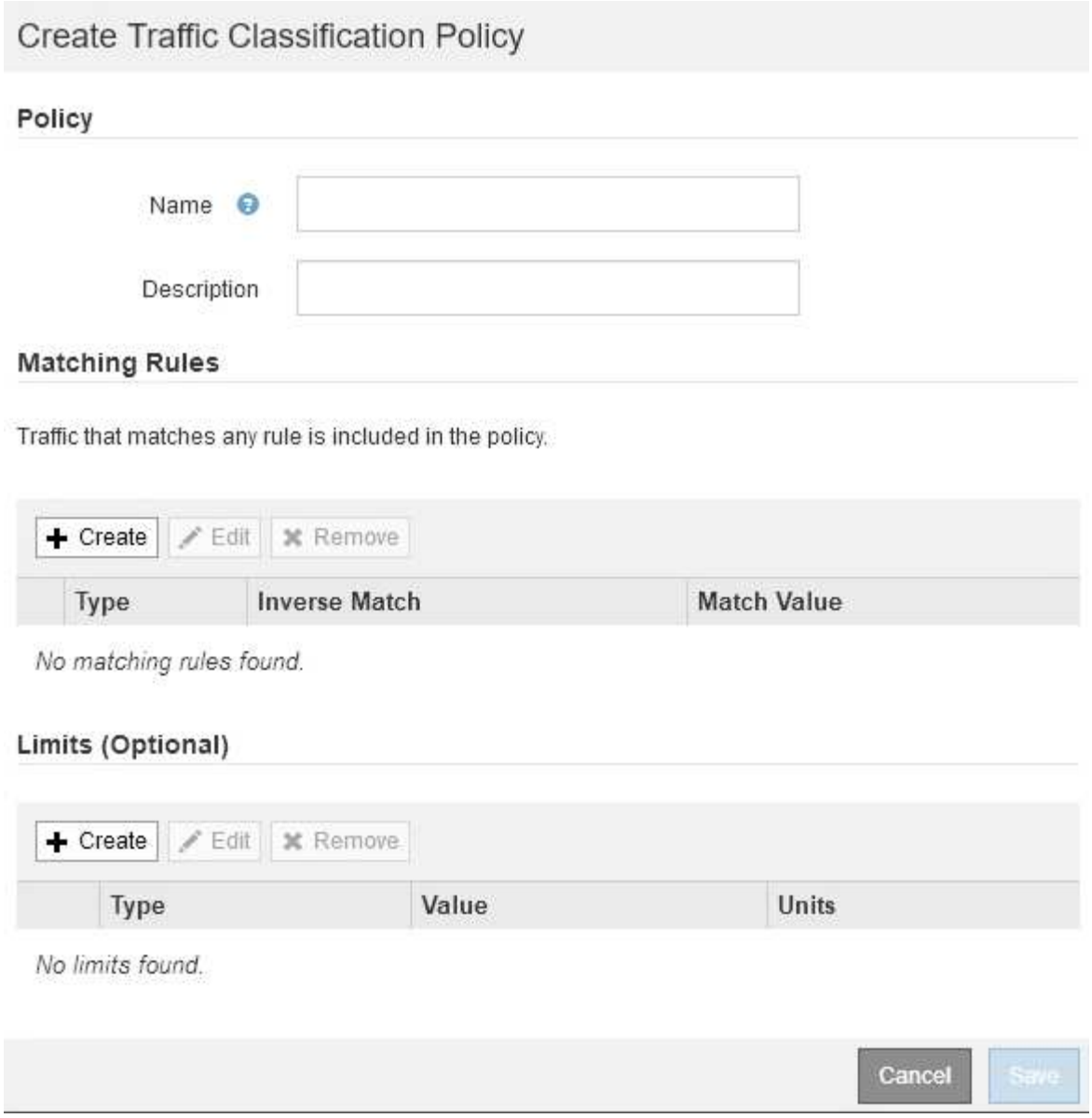
1. 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택합니다.

   교통 분류 정책 페이지가 나타납니다.

2. Create * 를 선택합니다.

   트래픽 분류 정책 생성 대화 상자가 나타납니다.



3. 이름 * 필드에 정책의 이름을 입력합니다.

   정책을 인식할 수 있도록 설명 이름을 입력합니다.

4. 필요에 따라 * Description * (설명 *) 필드에 정책에 대한 설명을 추가합니다.

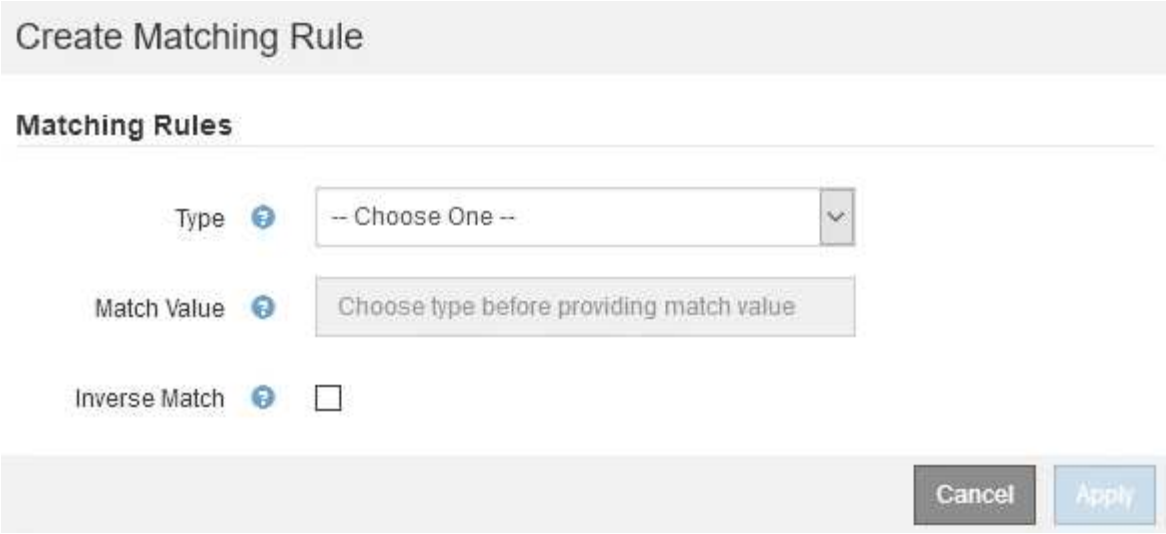
   예를 들어, 이 트래픽 분류 정책이 적용되는 대상 및 제한할 내용에 대해 설명하십시오.

5. 정책에 일치하는 규칙을 하나 이상 생성합니다.

   일치 규칙은 이 트래픽 분류 정책의 영향을 받을 엔터티를 제어합니다. 예를 들어 특정 테넌트의 네트워크 트래픽에 이 정책을 적용하려면 Tenant를 선택합니다. 또는 이 정책을 특정 로드 밸런싱 장치 끝점의 네트워크 트래픽에 적용하려면 끝점 을 선택합니다.

   a. 일치 규칙 * 섹션에서 * 만들기 * 를 선택합니다.

      일치 규칙 만들기 대화 상자가 나타납니다.



b. Type * 드롭다운에서 일치하는 규칙에 포함할 요소의 유형을 선택합니다.

c. 일치 값 * 필드에 선택한 요소의 유형에 따라 일치 값을 입력합니다.

- 버킷: 버킷 이름을 입력합니다.
- Bucket Regex: 버킷 이름 집합과 일치시키는 데 사용할 정규식을 입력합니다.

  정규식이 고정 해제됩니다. {캐럿} 앵커를 사용하여 버킷 이름의 시작 부분에 일치시키고 $ 앵커를 사용하여 이름 끝에 일치시킵니다.

- CIDR: 원하는 서브넷과 일치하는 IPv4 서브넷을 CIDR 표기법으로 입력합니다.
- 끝점: 기존 끝점 목록에서 끝점을 선택합니다. 로드 밸런서 엔드포인트 페이지에서 정의한 로드 밸런서 엔드포인입니다. 을 참조하십시오 로드 밸런서 엔드포인트를 구성합니다.
- 테넌트: 기존 테넌트 목록에서 테넌트를 선택합니다. 테넌트 일치는 액세스 중인 버킷의 소유권을 기반으로 합니다. 버킷에 대한 익명 액세스는 버킷을 소유하는 테넌트와 일치합니다.

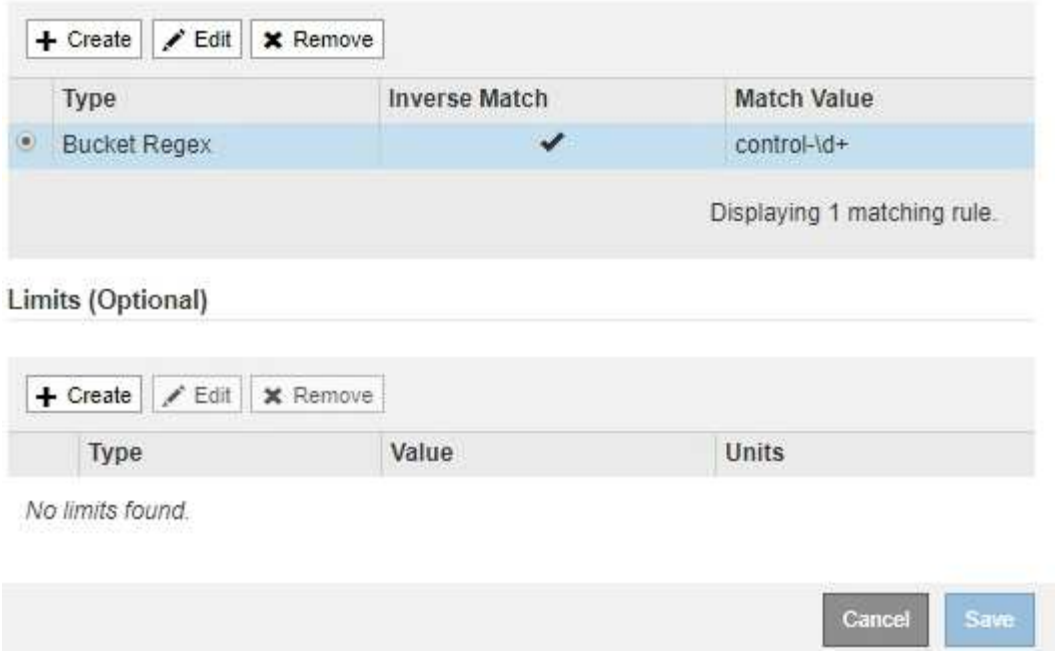
d. 방금 정의한 유형 및 일치 값과 일치하는 모든 network traffic_except_traffic을 일치시키려면 * Inverse * 확인란을 선택합니다. 그렇지 않으면 확인란을 선택하지 않은 상태로 둡니다.

   예를 들어, 이 정책이 로드 밸런서 끝점 중 하나를 제외한 모든 항목에 적용되도록 하려면 제외할 로드 밸런서 끝점을 지정하고 * Inverse * 를 선택합니다.

   > 하나 이상의 교자가 역마쳐인 여러 마처를 포함하는 정책의 경우 모든 요청과 일치하는 정책을 만들지 않도록 주의하십시오.

e. Apply * 를 선택합니다.

   규칙이 만들어지고 일치하는 규칙 테이블에 나열됩니다.



a. 정책에 대해 생성할 각 규칙에 대해 이 단계를 반복합니다.

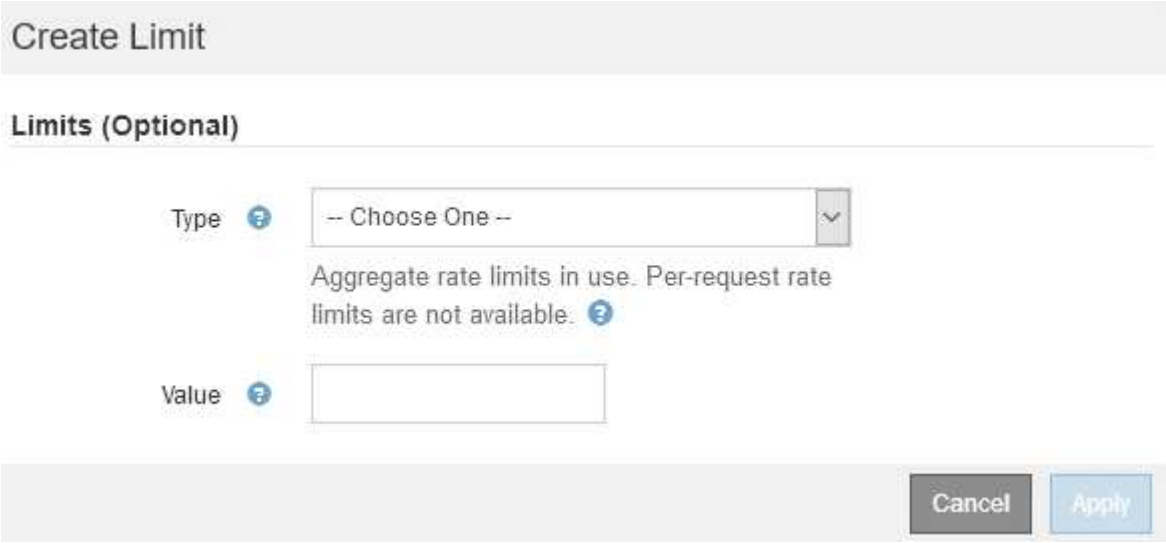
> 모든 규칙과 일치하는 트래픽은 정책에 의해 처리됩니다.

6. 필요에 따라 정책에 대한 제한을 생성합니다.

> 제한을 만들지 않더라도 StorageGRID는 정책과 일치하는 네트워크 트래픽을 모니터링할 수 있도록 메트릭을 수집합니다.

a. Limits * 섹션에서 * Create * 를 선택합니다.

Create Limit 대화상자가 나타납니다.



b. Type * 드롭다운에서 정책에 적용할 제한 유형을 선택합니다.

다음 목록에서 * in * 은 S3 또는 Swift 클라이언트에서 StorageGRID 로드 밸런서로의 트래픽을 나타내고 *

out * 은 로드 밸런서에서 S3 또는 Swift 클라이언트로 보내는 트래픽을 나타냅니다.

- 총 대역폭
- 총 대역폭 출력
- 동시 읽기 요청
- 동시 쓰기 요청
- 요청 당 대역폭
- 요청 당 대역폭 출력
- 읽기 요청 속도
- 쓰기 요청 속도

> 정책을 생성하여 애그리게이트 대역폭을 제한하거나 요청당 대역폭을 제한할 수 있습니다. 그러나 StorageGRID는 두 가지 유형의 대역폭을 동시에 제한할 수 없습니다.
> 애그리게이트 대역폭 제한은 제한 없는 트래픽에 약간의 성능 영향을 줄 수 있습니다.

대역폭 제한에 대해 StorageGRID는 설정된 제한 유형과 가장 일치하는 정책을 적용합니다. 예를 들어, 트래픽을 한 방향으로만 제한하는 정책이 있는 경우 대역폭 제한이 있는 추가 정책과 일치하는 트래픽이 있더라도 반대 방향의 트래픽은 무제한입니다. StorageGRID는 대역폭 제한에 대해 다음 순서로 ""가장 적합한"" 일치 항목을 구현합니다.

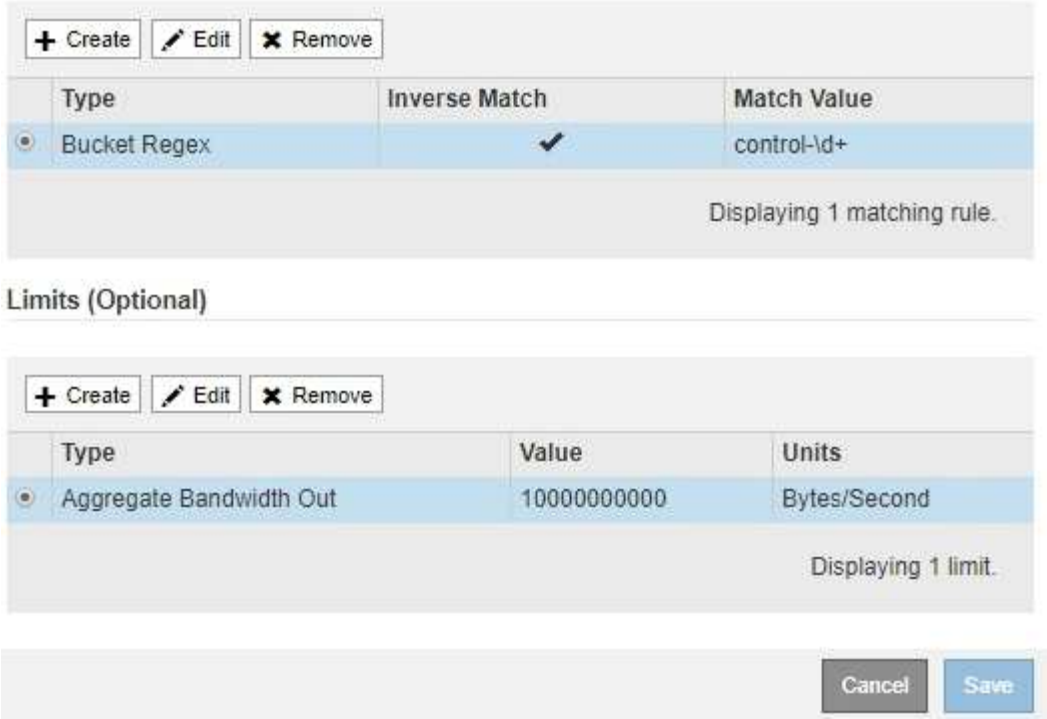
- 정확한 IP 주소(/32 마스크)
- 정확한 버킷 이름입니다
- 버킷 regex
- 테넌트
- 엔드포인트
- 일치하지 않는 CIDR 일치(NOT/32)
- 역 일치

c. 값 * 필드에 선택한 제한 유형의 숫자 값을 입력합니다.

한계를 선택하면 예상 단위가 표시됩니다.

d. Apply * 를 선택합니다.

제한이 생성되고 Limits 테이블에 나열됩니다.



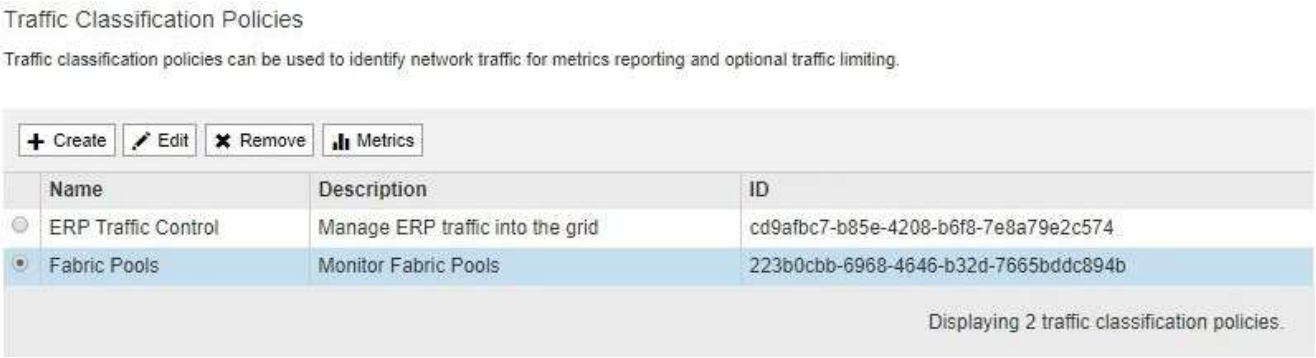
e. 정책에 추가할 각 제한에 대해 이 단계를 반복합니다.

예를 들어, SLA 계층에 대해 40Gbps 대역폭 제한을 생성하려면 한도 내의 총 대역폭 및 총 대역폭 제한을 생성하고 각 대역폭을 40Gbps로 설정합니다.

> 초당 메가바이트를 초당 기가비트 수로 변환하려면 8을 곱합니다. 예를 들어, 125MB/s는 1,000Mbps 또는 1Gbps와 동일합니다.

7. 규칙 및 제한 만들기를 마치면 * 저장 * 을 선택합니다.

정책이 저장되고 트래픽 분류 정책 표에 나열됩니다.



이제 S3 및 Swift 클라이언트 트래픽이 트래픽 분류 정책에 따라 처리됩니다. 트래픽 차트를 보고 정책이 기대하는 트래픽 제한을 적용하고 있는지 확인할 수 있습니다. 을 참조하십시오 네트워크 트래픽 메트릭을 확인합니다.

트래픽 분류 정책을 편집합니다

트래픽 분류 정책을 편집하여 이름 또는 설명을 변경하거나 정책에 대한 규칙 또는 제한을 생성, 편집 또는 삭제할 수 있습니다.

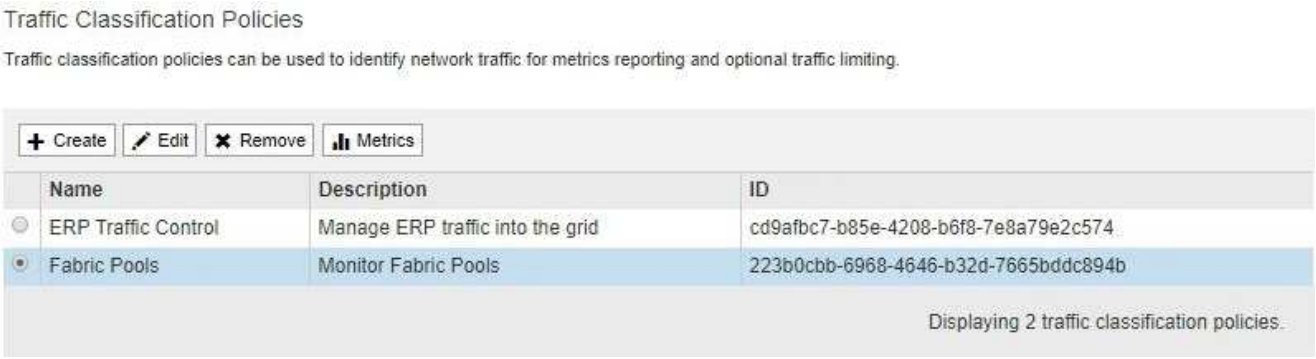
필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.

단계

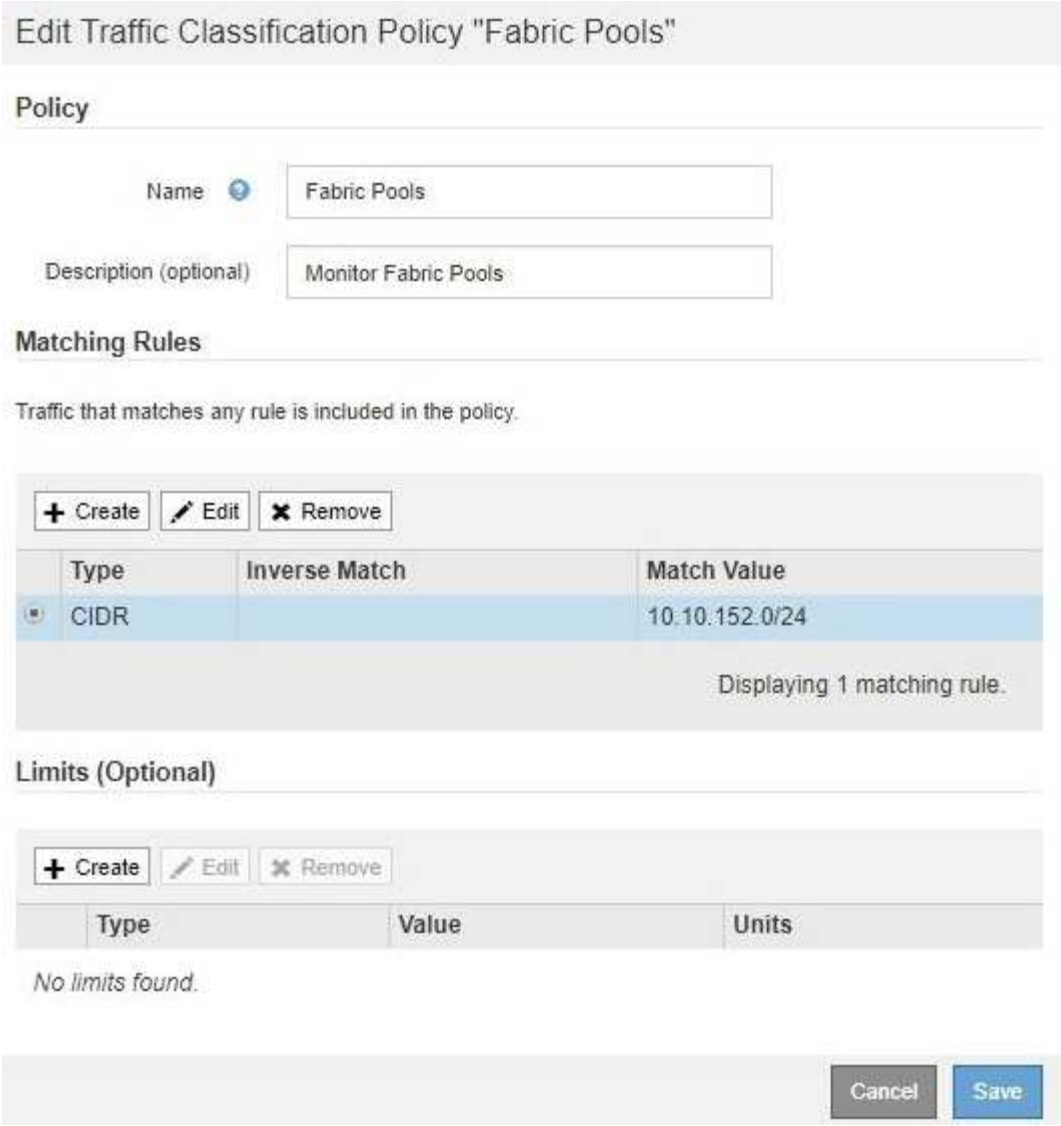
1. 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택합니다.

   트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.



2. 편집할 정책 왼쪽의 라디오 버튼을 선택합니다.
3. 편집 * 을 선택합니다.

   트래픽 분류 정책 편집 대화 상자가 나타납니다.



4. 필요에 따라 일치하는 규칙 및 제한을 생성, 편집 또는 제거합니다.
   a. 일치하는 규칙 또는 제한을 만들려면 * 만들기 * 를 선택하고 규칙을 만들거나 제한을 만드는 방법에 대한 지침을 따릅니다.
   b. 일치하는 규칙 또는 제한을 편집하려면 규칙 또는 제한에 대한 라디오 버튼을 선택하고 * 일치 규칙 * 섹션 또는 * 제한 * 섹션에서 * 편집 * 을 선택한 다음 규칙 생성 또는 제한 생성 지침을 따릅니다.
   c. 일치하는 규칙 또는 제한을 제거하려면 규칙 또는 제한에 대한 라디오 단추를 선택하고 * 제거 * 를 선택합니다. 그런 다음 * 확인 * 을 선택하여 규칙 또는 제한을 제거할 것인지 확인합니다.
5. 규칙 또는 제한을 만들거나 편집한 후에는 * 적용 * 을 선택합니다.
6. 정책 편집을 마치면 * Save * 를 선택합니다.

   정책 변경 사항이 저장되고 이제 트래픽 분류 정책에 따라 네트워크 트래픽이 처리됩니다. 트래픽 차트를 보고 정책이 기대하는 트래픽 제한을 적용하고 있는지 확인할 수 있습니다.

트래픽 분류 정책을 삭제합니다

트래픽 분류 정책이 더 이상 필요하지 않으면 삭제할 수 있습니다.

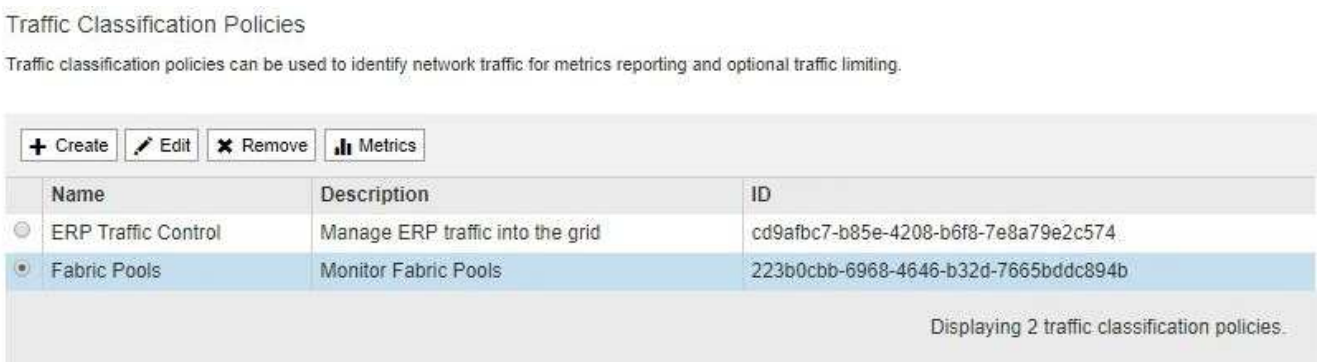
필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.

단계

1. 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택합니다.

   트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.



2. 삭제할 정책의 왼쪽에 있는 라디오 버튼을 선택합니다.
3. 제거 * 를 선택합니다.

   경고 대화 상자가 나타납니다.

4. 정책 삭제를 확인하려면 * OK * 를 선택합니다.

   정책이 삭제됩니다.

네트워크 트래픽 메트릭을 확인합니다

트래픽 분류 정책 페이지에서 사용할 수 있는 그래프를 보고 네트워크 트래픽을 모니터링할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한 또는 테넌트 계정 권한이 있습니다.

이 작업에 대해

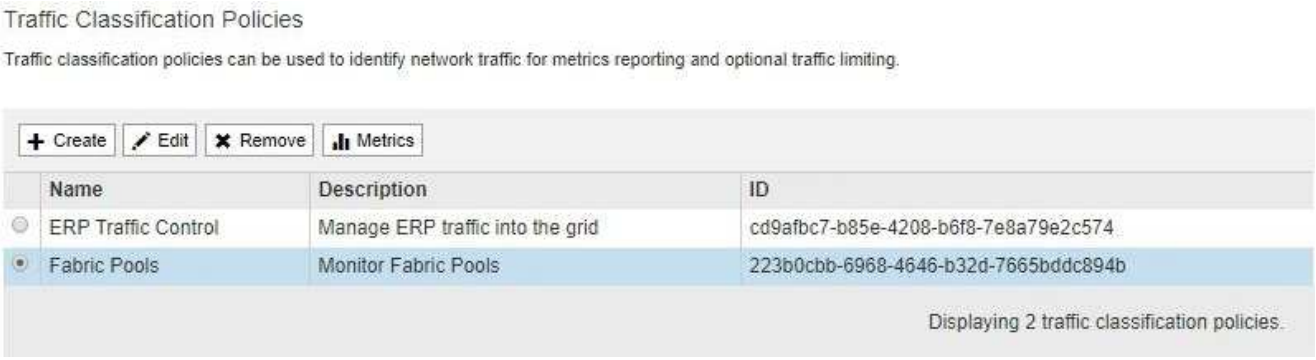
기존 트래픽 분류 정책에 대해 로드 밸런서 서비스에 대한 메트릭을 확인하여 정책이 네트워크 전체의 트래픽을 성공적으로 제한하고 있는지 확인할 수 있습니다. 그래프의 데이터를 통해 정책을 조정해야 하는지 확인할 수 있습니다.

트래픽 분류 정책에 대해 설정된 제한이 없더라도 메트릭이 수집되고 그래프는 트래픽 추세를 이해하는 데 유용한 정보를 제공합니다.

단계

1. 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택합니다.

   트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.



   테넌트 계정 권한이 있지만 루트 액세스 권한이 없는 경우 * 생성 *, * 편집 * 및 * 제거 * 버튼이 비활성화됩니다.

2. 메트릭을 보려는 정책 왼쪽의 라디오 버튼을 선택합니다.
3. 메트릭 * 을 선택합니다.

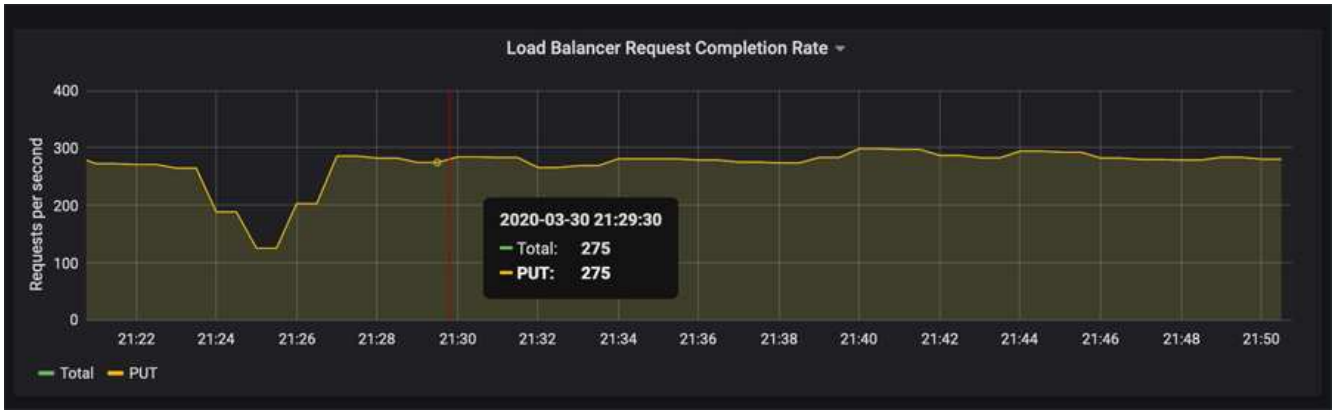
   새 브라우저 창이 열리고 트래픽 분류 정책 그래프가 나타납니다. 그래프에는 선택한 정책과 일치하는 트래픽에 대한 메트릭만 표시됩니다.

   policy * 풀다운을 사용하여 확인할 다른 정책을 선택할 수 있습니다.

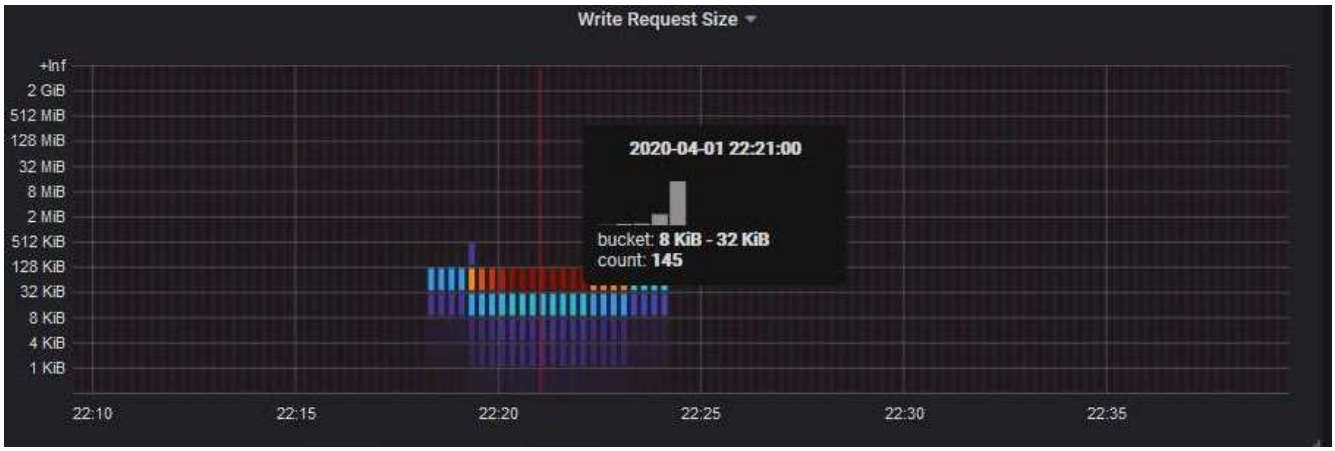
다음 그래프는 웹 페이지에 포함되어 있습니다.

- 로드 밸런서 요청 트래픽: 이 그래프는 로드 밸런서 끝점과 요청을 하는 클라이언트 간에 전송되는 데이터 처리량의 3분 이동 평균을 초당 비트 수로 제공합니다.
- 부하 분산 요청 완료율: 이 그래프는 초당 완료된 요청 수(GET, PUT, HEAD 및 DELETE)에 대한 3분의 이동 평균을 요청 유형별로 제공합니다. 이 값은 새 요청의 헤더가 검증되면 업데이트됩니다.
- 오류 응답 속도: 이 그래프는 오류 응답 코드로 분리된 초당 클라이언트에 반환된 오류 응답 수의 이동 평균을 3분으로 제공합니다.
- 평균 요청 기간(오류 없음): 이 그래프는 요청 유형(GET, PUT, HEAD, DELETE)별로 분류되는 요청 지속 시간의 3분 이동 평균을 제공합니다. 각 요청 기간은 부하 분산 서비스에서 요청 헤더를 구문 분석할 때 시작되어 완전한 응답 본문이 클라이언트로 반환될 때 종료됩니다.
- 개체 크기별 쓰기 요청 속도: 이 히트맵은 개체 크기에 따라 쓰기 요청이 완료되는 속도의 이동 평균을 3분으로 제공합니다. 이 컨텍스트에서 쓰기 요청은 PUT 요청에만 참조됩니다.
- 개체 크기별 읽기 요청 속도: 이 히트맵은 개체 크기에 따라 읽기 요청이 완료되는 속도에 대한 3분의 이동 평균을 제공합니다. 이 컨텍스트에서 읽기 요청은 요청 가져오기만 참조합니다. 히트맵의 색상은 개별 그래프 내의 개체 크기의 상대적 주파수를 나타냅니다. 차가운 색(예: 자주색 및 파란색)은 상대적으로 낮은 비율을 나타내고 따뜻한 색(예: 주황색 및 빨간색)은 상대적으로 높은 비율을 나타냅니다.

4. 커서를 선 그래프 위로 이동하면 그래프의 특정 부분에 있는 값의 팝업이 표시됩니다.



5. Heatmap 위로 커서를 이동하면 샘플의 날짜 및 시간, 카운트로 집계된 개체 크기 및 해당 기간 동안 초당 요청 수를 보여 주는 팝업이 표시됩니다.



6. 왼쪽 상단의 * 정책 * 풀다운을 사용하여 다른 정책을 선택합니다.

   선택한 정책에 대한 그래프가 나타납니다.

7. 또는 * 지원 * 메뉴에서 그래프에 액세스하십시오.
   a. 지원 * > * 도구 * > * 메트릭 * 을 선택합니다.
   b. 페이지의 * Grafana * 섹션에서 * 트래픽 분류 정책 * 을 선택합니다.
   c. 페이지 왼쪽 상단의 풀다운 메뉴에서 정책을 선택합니다.

      트래픽 분류 정책은 ID로 식별됩니다. 정책 ID는 트래픽 분류 정책 페이지에 나열되어 있습니다.

8. 그래프를 분석하여 정책에 따라 트래픽이 제한되는 빈도와 정책을 조정해야 하는지 여부를 결정합니다.

관련 정보

모니터링하고 문제를 해결합니다

링크 비용 관리

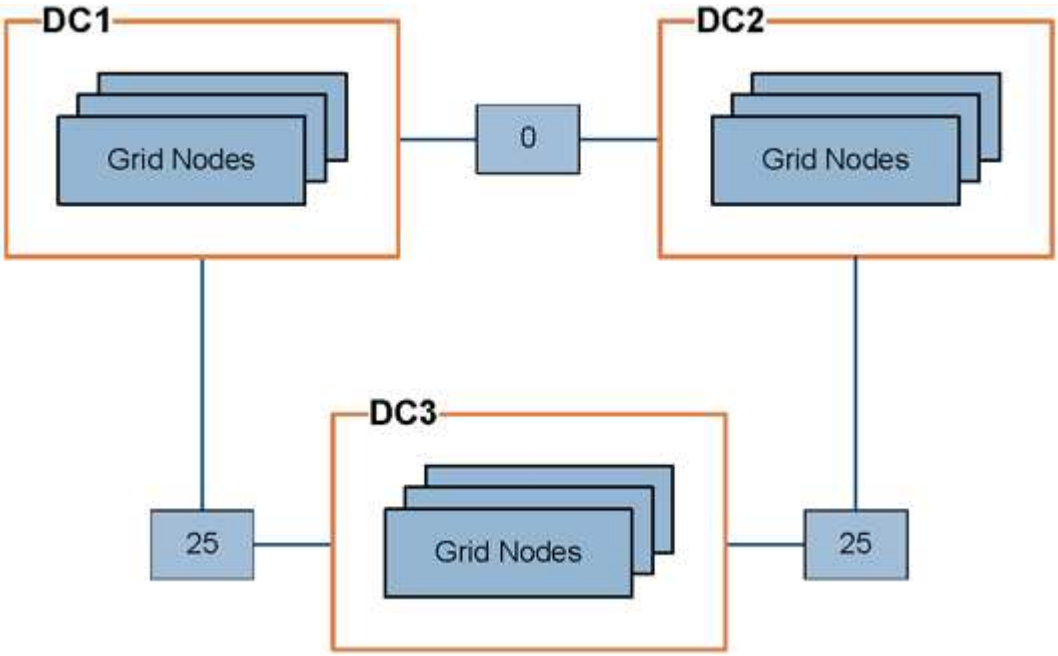
링크 비용은 얼마입니까

링크 비용을 사용하면 둘 이상의 데이터 센터 사이트가 있을 때 요청된 서비스를 제공하는 데이터 센터 사이트의 우선 순위를 지정할 수 있습니다. 링크 비용을 조정하여 사이트 간 지연 시간을

반영할 수 있습니다.

- 링크 비용은 오브젝트 검색을 수행하는 데 사용되는 오브젝트 복사본의 우선 순위를 지정하는 데 사용됩니다.
- 링크 비용은 그리드 관리 API 및 테넌트 관리 API에서 사용할 내부 StorageGRID 서비스를 결정하는 데 사용됩니다.
- 링크 비용은 게이트웨이 노드의 더 이상 사용되지 않는 CLB(연결 로드 밸런서) 서비스에서 클라이언트 연결을 연결하는 데 사용됩니다. 을 참조하십시오 로드 균형 조정 작동 방식 - CLB 서비스.

다이어그램에는 사이트 간에 구성된 링크 비용이 있는 세 개의 사이트 표가 표시됩니다.



- 게이트웨이 노드의 CLB 서비스는 동일한 데이터 센터 사이트의 모든 스토리지 노드 및 링크 비용이 0인 모든 데이터 센터 사이트에 클라이언트 연결을 균등하게 분산합니다.

  이 예에서는 데이터 센터 사이트 1(DC1)의 게이트웨이 노드가 DC1의 스토리지 노드 및 DC2의 스토리지 노드로 클라이언트 접속을 균등하게 분산합니다. DC3의 게이트웨이 노드는 DC3의 스토리지 노드에만 클라이언트 접속을 전송합니다.

- 여러 개의 복제된 복제본으로 존재하는 객체를 검색할 때 StorageGRID는 가장 낮은 링크 비용을 가진 데이터 센터에서 복제본을 검색합니다.

  이 예제에서 DC2의 클라이언트 응용 프로그램이 DC1과 DC3에 둘 다 저장된 개체를 검색할 경우 DC1에서 D2까지의 링크 비용은 DC3에서 DC2로 링크 비용보다 낮은 0이므로 DC2의 클라이언트 응용 프로그램이 DC1에서 개체를 검색합니다.

링크 비용은 특정 측정 단위가 없는 임의의 상대 숫자입니다. 예를 들어 링크 비용 50은 링크 비용 25보다 우선적으로 사용됩니다. 이 표에는 일반적으로 사용되는 링크 비용이 나와 있습니다.

링크	링크 비용	참고
데이터를 안전하게 보호	25(기본값)	WAN 링크로 연결된 데이터 센터

링크	링크 비용	참고
동일한 물리적 위치의 논리적 데이터 센터 사이트 간	0	LAN으로 연결된 동일한 물리적 건물 또는 캠퍼스의 논리적 데이터 센터

링크 비용을 업데이트합니다

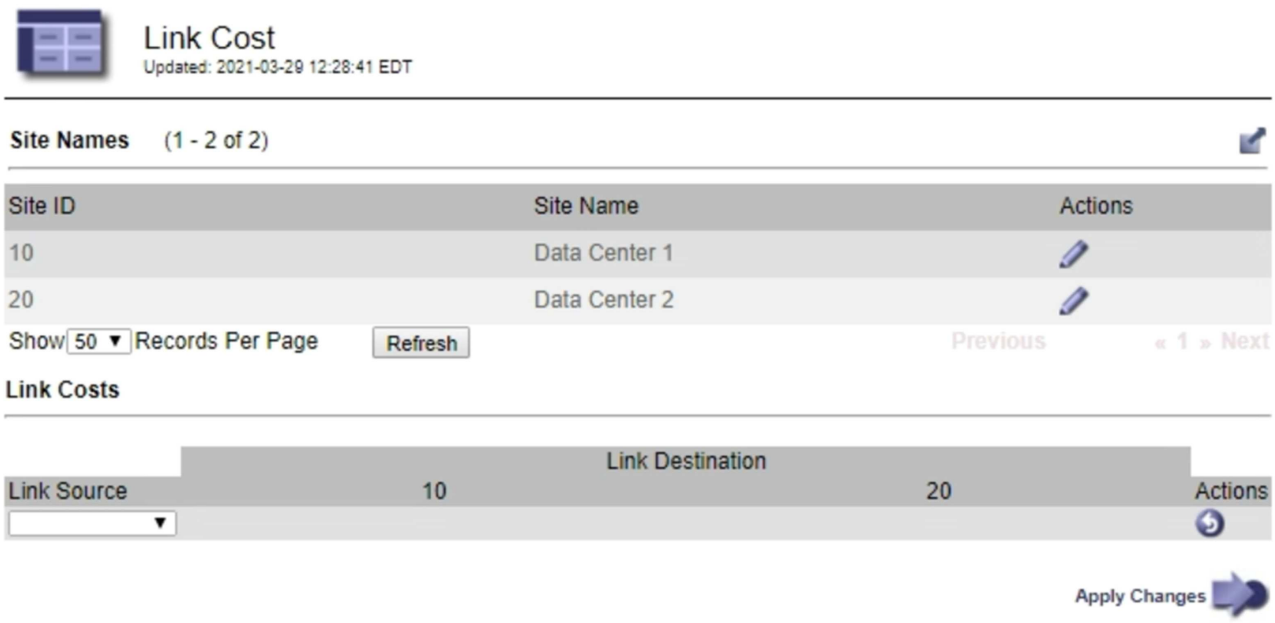
사이트 간 지연 시간을 반영하기 위해 데이터 센터 사이트 간의 링크 비용을 업데이트할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 그리드 토폴로지 페이지 구성 권한이 있습니다.

단계

1. 구성 * > * 네트워크 * > * 링크 비용 * 을 선택합니다.



2. 링크 원본 * 에서 사이트를 선택하고 * 링크 대상 * 에서 0에서 100 사이의 비용 값을 입력합니다.

   소스가 대상과 동일한 경우 링크 비용을 변경할 수 없습니다.

   변경 사항을 취소하려면 를 선택합니다 * 되돌리기 *.

3. Apply Changes * 를 선택합니다.

AutoSupport를 사용합니다

AutoSupport란 무엇입니까?

AutoSupport 기능을 사용하면 StorageGRID 시스템에서 상태 및 상태 메시지를 기술 지원 부서에 보낼 수 있습니다.

AutoSupport를 사용하면 문제를 빠르게 확인하고 해결할 수 있습니다. 기술 지원 부서에서는 시스템의 스토리지 요구 사항을 모니터링하여 새 노드나 사이트를 추가해야 하는지 여부를 결정할 수 있습니다. 선택적으로 AutoSupport 메시지를 하나의 추가 대상으로 보내도록 구성할 수 있습니다.

AutoSupport 메시지에 포함된 정보입니다

AutoSupport 메시지에는 다음과 같은 정보가 포함됩니다.

- StorageGRID 소프트웨어 버전입니다
- 운영 체제 버전입니다
- 시스템 레벨 및 위치 레벨 속성 정보
- 최근 알림 및 알람(기존 시스템)
- 내역 데이터를 포함하여 모든 그리드 작업의 현재 상태입니다
- 관리 노드 데이터베이스 사용
- 손실되거나 누락된 개체 수입니다
- 그리드 구성 설정
- NMS 요소
- 활성 ILM 정책
- 프로비저닝된 그리드 사양 파일
- 진단 메트릭

StorageGRID를 처음 설치할 때 AutoSupport 기능 및 개별 AutoSupport 옵션을 활성화하거나 나중에 활성화할 수 있습니다. AutoSupport가 활성화되어 있지 않으면 그리드 관리자 대시보드에 메시지가 나타납니다. 이 메시지에는 AutoSupport 구성 페이지에 대한 링크가 포함되어 있습니다.

메시지를 닫으면 AutoSupport가 비활성화된 경우에도 브라우저 캐시가 지워질 때까지 메시지가 다시 표시되지 않습니다.

Active IQ란 무엇입니까?

Active IQ는 NetApp 설치 기반에서 예측 분석 및 커뮤니티 지혜를 활용하는 클라우드 기반 디지털 자문업체입니다. 지속적인 위험 평가, 예측 경고, 규범적 지침 및 자동화된 작업을 통해 문제가 발생하기 전에 이를 방지함으로써 시스템 상태를 개선하고 시스템 가용성을 높일 수 있습니다.

NetApp Support 사이트에서 Active IQ 대시보드 및 기능을 사용하려면 AutoSupport를 사용하도록 설정해야 합니다.

"Active IQ 디지털 자문 문서"

AutoSupport 메시지를 보내는 프로토콜입니다

다음 세 가지 프로토콜 중 하나를 선택하여 AutoSupport 메시지를 보낼 수 있습니다.

- HTTPS
- HTTP
- SMTP

HTTPS 또는 HTTP를 사용하여 AutoSupport 메시지를 보내는 경우 관리자 노드와 기술 지원 간에 투명하지 않은 프록시 서버를 구성할 수 있습니다.

AutoSupport 메시지의 프로토콜로 SMTP를 사용하는 경우 SMTP 메일 서버를 구성해야 합니다.

AutoSupport 옵션

다음 옵션을 조합하여 기술 지원 부서에 AutoSupport 메시지를 보낼 수 있습니다.

- * Weekly *: AutoSupport 메시지를 매주 한 번씩 자동으로 전송합니다. 기본 설정: 사용.
- * 이벤트 트리거 *: 1시간마다 또는 중요한 시스템 이벤트가 발생할 때 AutoSupport 메시지를 자동으로 전송합니다. 기본 설정: 사용.
- * 주문형 *: 기술 지원 부서에서 StorageGRID 시스템에서 AutoSupport 메시지를 자동으로 보내도록 요청할 수 있습니다. 이 메시지는 문제가 활발하게 발생하는 경우 유용합니다(HTTPS AutoSupport 전송 프로토콜 필요). 기본 설정: 사용 안 함
- * 사용자 트리거 *: 언제든지 수동으로 AutoSupport 메시지를 보냅니다.

관련 정보

"NetApp 지원"

AutoSupport를 구성합니다

StorageGRID를 처음 설치할 때 AutoSupport 기능 및 개별 AutoSupport 옵션을 활성화하거나 나중에 활성화할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 또는 기타 그리드 구성 권한이 있습니다.
- AutoSupport 메시지를 보내는 데 HTTPS 또는 HTTP 프로토콜을 사용할 경우 직접 또는 프록시 서버를 사용하여 기본 관리자 노드에 대한 아웃바운드 인터넷 액세스를 제공했습니다(인바운드 연결은 필요하지 않음).
- HTTPS 또는 HTTP 프로토콜을 사용하고 프록시 서버를 사용하려는 경우 을(를) 가지고 있습니다 관리자 프록시 서버를 구성했습니다.
- AutoSupport 메시지의 프로토콜로 SMTP를 사용할 경우 SMTP 메일 서버를 구성했습니다. 알람 이메일 알림(레거시 시스템)에 동일한 메일 서버 구성이 사용됩니다.

AutoSupport 메시지의 프로토콜을 지정합니다

다음 프로토콜을 사용하여 AutoSupport 메시지를 보낼 수 있습니다.

- * HTTPS *: 새 설치에 대한 기본 권장 설정입니다. HTTPS 프로토콜은 포트 443을 사용합니다. AutoSupport 온디맨드 기능을 활성화하려면 HTTPS 프로토콜을 사용해야 합니다.
- * HTTP *: 인터넷을 통해 데이터를 전송할 때 프록시 서버가 HTTPS로 변환되는 신뢰할 수 있는 환경에서 사용되지 않는 한 이 프로토콜은 안전하지 않습니다. HTTP 프로토콜은 포트 80을 사용합니다.
- * SMTP **: AutoSupport** 메시지를 이메일로 보내려면 이 옵션을 사용합니다**. AutoSupport** 메시지의 프로토콜로 **SMTP**를 사용하는 경우 레거시 전자 메일 설정 페이지**(** 지원*>* 알람(레거시)**>** 레거시 전자 메일 설정*)에서 SMTP 메일 서버를 구성해야 합니다.

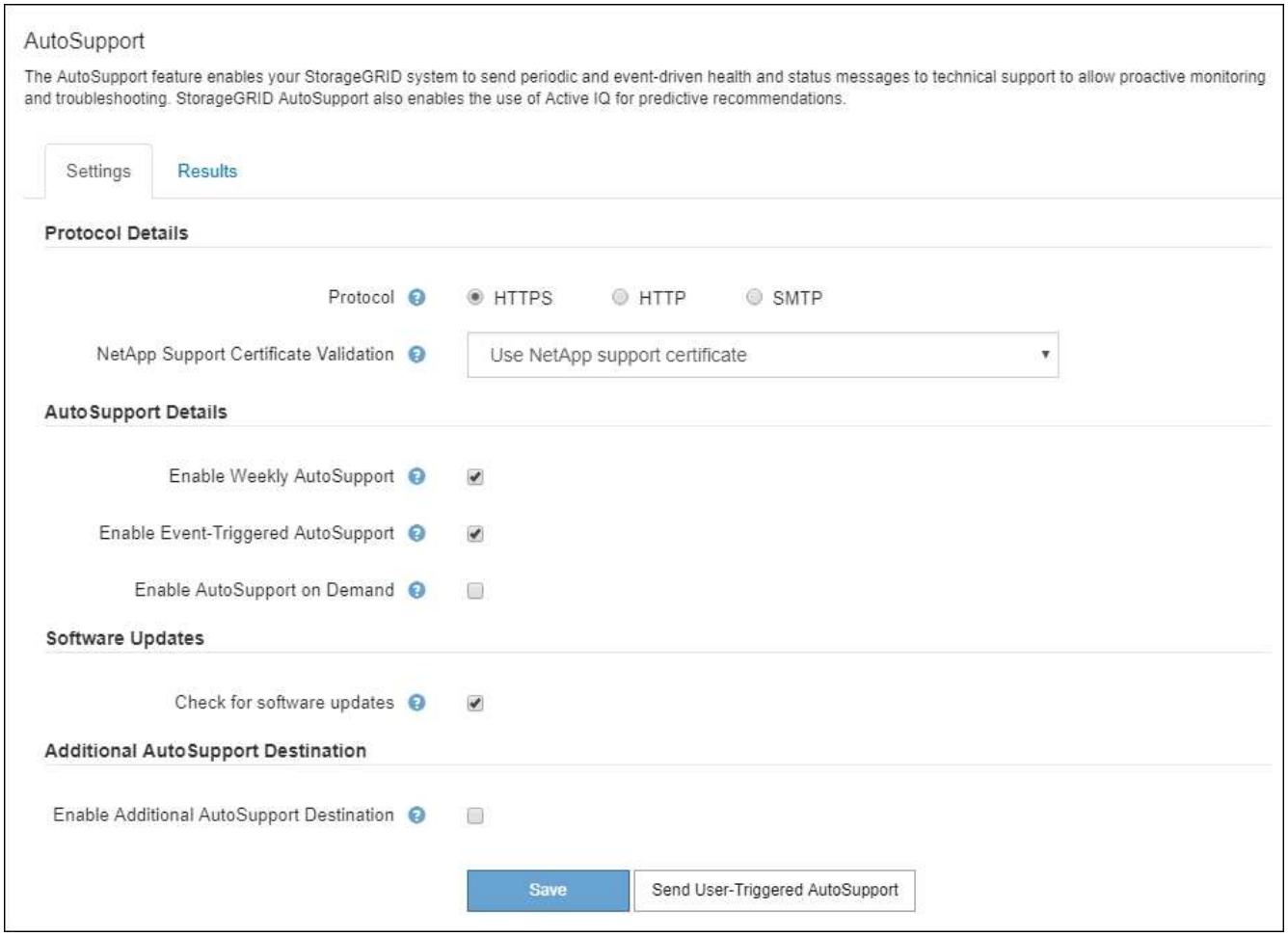
> SMTP는 StorageGRID 11.2 릴리스 이전에 AutoSupport 메시지에 사용할 수 있는 유일한 프로토콜이었습니다. 처음에 이전 버전의 StorageGRID를 설치한 경우 SMTP가 선택된 프로토콜일 수 있습니다.

설정한 프로토콜은 모든 유형의 AutoSupport 메시지를 전송하는 데 사용됩니다.

단계

1. 지원 * > * 도구 * > * AutoSupport * 를 선택합니다.

   AutoSupport 페이지가 나타나고 * 설정 * 탭이 선택됩니다.



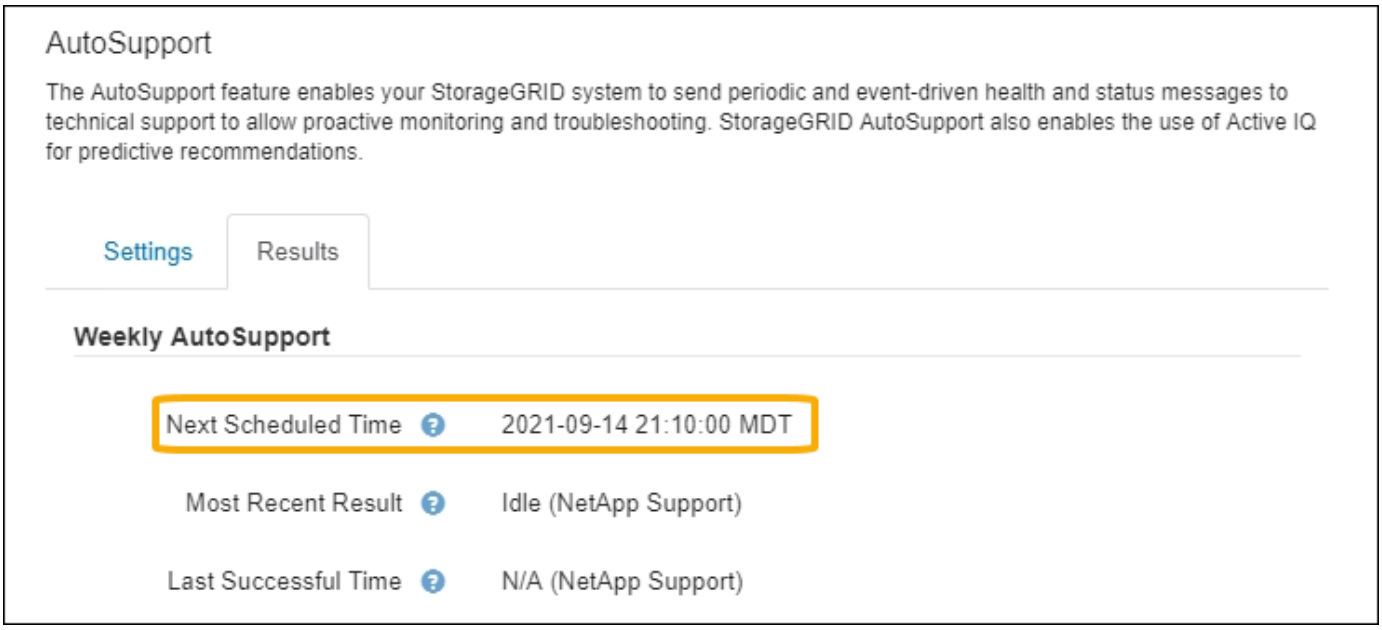
2. AutoSupport 메시지를 보내는 데 사용할 프로토콜을 선택합니다.
3. HTTPS * 를 선택한 경우 TLS 인증서를 사용하여 NetApp 지원 서버에 대한 연결을 보호할지 여부를 선택합니다.
   - * NetApp 지원 인증서 사용 * (기본값): 인증서 검증으로 AutoSupport 메시지를 안전하게 전송할 수 있습니다. NetApp 지원 인증서는 StorageGRID 소프트웨어와 함께 이미 설치되어 있습니다.
   - 인증서 확인 안 함 *: 인증서에 일시적인 문제가 있는 경우와 같이 인증서 유효성 검사를 사용하지 않는 것이 좋은 경우에만 이 옵션을 선택합니다.
4. 저장 * 을 선택합니다.

   매주, 사용자 트리거 및 이벤트 트리거 메시지는 선택한 프로토콜을 사용하여 전송됩니다.

주간 **AutoSupport** 메시지를 비활성화합니다

기본적으로 StorageGRID 시스템은 AutoSupport 메시지를 일주일에 한 번 NetApp Support에 보내도록 구성됩니다.

Weekly AutoSupport 메시지가 언제 전송되는지 확인하려면 * AutoSupport * > * Results * 탭으로 이동하십시오. Weekly AutoSupport * 섹션에서 * Next Scheduled Time * 값을 확인합니다.



매주 AutoSupport 메시지를 자동으로 전송하지 않도록 설정할 수 있습니다.

단계

1. 지원 * > * 도구 * > * AutoSupport * 를 선택합니다.
2. Weekly AutoSupport * 활성화 확인란의 선택을 취소합니다.
3. 저장 * 을 선택합니다.

이벤트 트리거 **AutoSupport** 메시지를 비활성화합니다

기본적으로 StorageGRID 시스템은 중요한 알림 또는 기타 중요한 시스템 이벤트가 발생할 경우 NetApp 지원에 AutoSupport 메시지를 보내도록 구성됩니다.

언제든지 이벤트 트리거 AutoSupport 메시지를 사용하지 않도록 설정할 수 있습니다.

e-메일 알림 시스템 전체를 억제하면 이벤트 트리거 AutoSupport 메시지도 표시되지 않습니다. (* 구성 * > * 시스템 * > * 디스플레이 옵션 * 을 선택합니다. 그런 다음 * 알림 모두 표시 안 함 * 을 선택합니다.)

단계

1. 지원 * > * 도구 * > * AutoSupport * 를 선택합니다.
2. 이벤트 트리거 AutoSupport* 활성화 확인란의 선택을 취소합니다.
3. 저장 * 을 선택합니다.

AutoSupport 온디맨드 를 활성화합니다

AutoSupport On Demand는 기술 지원이 활발하게 진행 중인 문제를 해결하는 데 도움이 될 수 있습니다.

기본적으로 AutoSupport On Demand는 비활성화되어 있습니다. 이 기능을 활성화하면 기술 지원 부서에서 StorageGRID 시스템에 AutoSupport 메시지가 자동으로 전송되도록 요청할 수 있습니다. 기술 지원 부서에서는 AutoSupport 주문형 쿼리에 대한 폴링 시간 간격을 설정할 수도 있습니다.

기술 지원 부서에서 AutoSupport On Demand를 활성화하거나 비활성화할 수 없습니다.

단계

1. 지원 * > * 도구 * > * AutoSupport * 를 선택합니다.
2. 프로토콜에 대해 * HTTPS * 를 선택합니다.
3. Weekly AutoSupport * 활성화 확인란을 선택합니다.
4. AutoSupport On Demand * 활성화 확인란을 선택합니다.
5. 저장 * 을 선택합니다.

   AutoSupport On Demand가 활성화되어 있으면 기술 지원 부서에서 AutoSupport On Demand 요청을 StorageGRID로 보낼 수 있습니다.

소프트웨어 업데이트 확인을 비활성화합니다

기본적으로 StorageGRID은 NetApp에 문의하여 사용 가능한 소프트웨어 업데이트가 있는지 확인합니다. StorageGRID 핫픽스 또는 새 버전을 사용할 수 있는 경우 새 버전이 StorageGRID 업그레이드 페이지에 표시됩니다.

필요에 따라 소프트웨어 업데이트 확인을 비활성화할 수도 있습니다. 예를 들어 시스템에 WAN 액세스가 없는 경우 다운로드 오류를 방지하려면 검사를 비활성화해야 합니다.

단계

1. 지원 * > * 도구 * > * AutoSupport * 를 선택합니다.
2. 소프트웨어 업데이트 확인 * 확인란의 선택을 취소합니다.
3. 저장 * 을 선택합니다.

AutoSupport 대상을 추가합니다

AutoSupport를 활성화하면 상태 및 상태 메시지가 NetApp 지원으로 전송됩니다. 모든 AutoSupport 메시지에 대해 하나의 추가 대상을 지정할 수 있습니다.

AutoSupport 메시지를 보내는 데 사용되는 프로토콜을 확인하거나 변경하려면 에 대한 지침을 참조하십시오

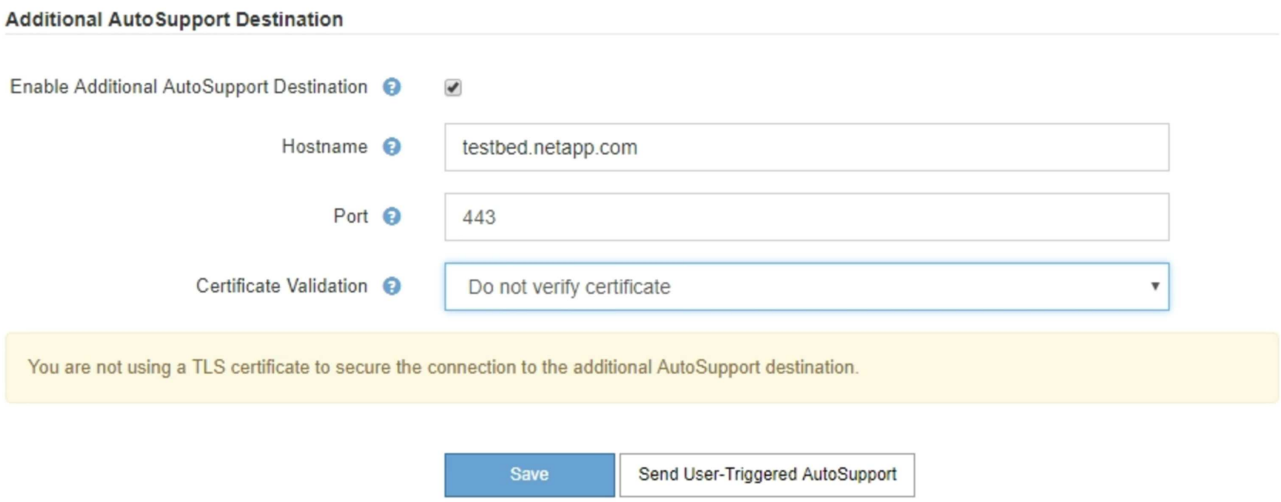
AutoSupport 메시지의 프로토콜을 지정합니다.

> SMTP 프로토콜을 사용하여 AutoSupport 메시지를 추가 대상으로 보낼 수는 없습니다.

단계

1. 지원 * > * 도구 * > * AutoSupport * 를 선택합니다.
2. 추가 AutoSupport 대상 사용 * 을 선택합니다.

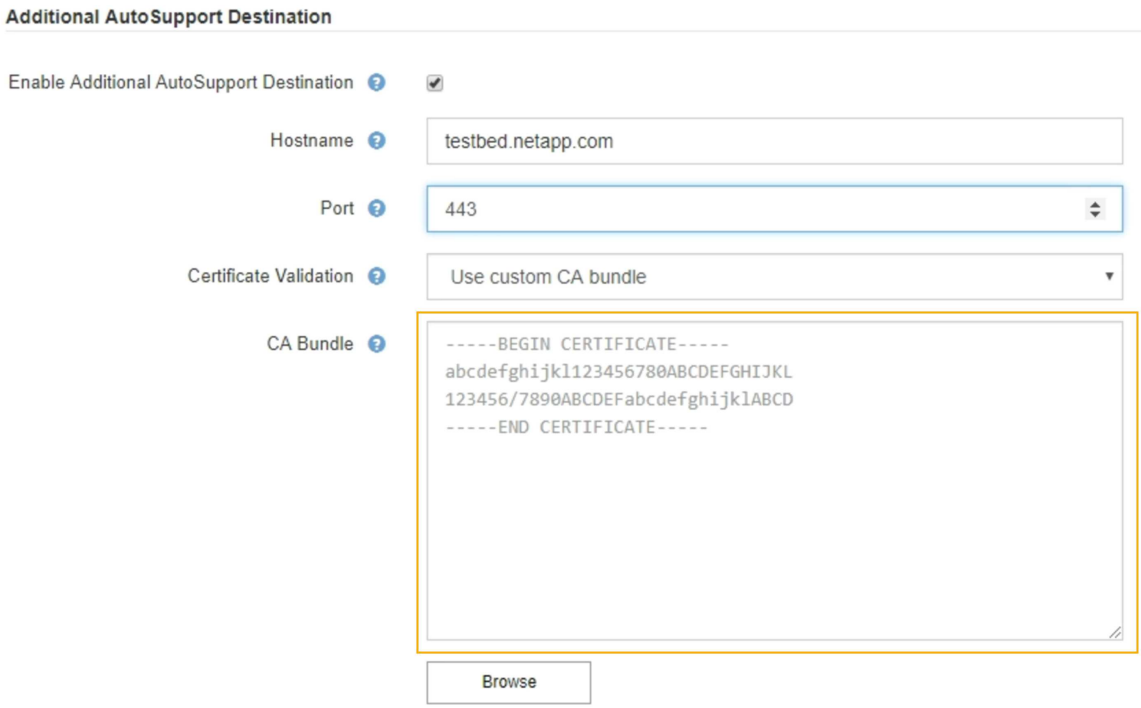
   추가 AutoSupport 대상 필드가 나타납니다.



3. 추가 AutoSupport 대상 서버의 서버 호스트 이름 또는 IP 주소를 입력합니다.

   > 하나의 추가 대상만 입력할 수 있습니다.

4. 추가 AutoSupport 대상 서버에 연결하는 데 사용되는 포트를 입력합니다. 기본값은 HTTP의 경우 포트 80, HTTPS의 경우 포트 443입니다.
5. 인증서 유효성 검사와 함께 AutoSupport 메시지를 보내려면 * 인증서 유효성 검사 * 드롭다운에서 * 사용자 지정 CA 번들 사용 * 을 선택합니다. 그런 다음 다음 다음 중 하나를 수행합니다.
   - 편집 도구를 사용하여 인증서 체인 순서대로 연결된 * CA 번들 * 필드에 PEM 인코딩된 각 CA 인증서 파일의 모든 내용을 복사하여 붙여 넣습니다. 선택 항목에 '----BEGIN CERIFICATE----' 및 '----end certificate--'를 포함해야 합니다.



- 찾아보기 * 를 선택하고 인증서가 포함된 파일을 찾은 다음 * 열기 * 를 선택하여 파일을 업로드합니다. 인증서 유효성 검사를 통해 AutoSupport 메시지를 안전하게 전송할 수 있습니다.

6. 인증서 유효성 검사 없이 AutoSupport 메시지를 보내려면 * 인증서 유효성 검사 * 드롭다운에서 * 인증서 확인 안 함 * 을 선택합니다.

   인증서에 일시적인 문제가 있는 경우와 같이 인증서 유효성 검사를 사용하지 않는 좋은 이유가 있는 경우에만 이 옵션을 선택합니다.

   "추가 AutoSupport 대상에 대한 연결을 보호하기 위해 TLS 인증서를 사용하고 있지 않습니다."라는 메시지가 나타납니다.

7. 저장 * 을 선택합니다.

   향후 모든 주별, 이벤트 트리거 및 사용자 트리거 AutoSupport 메시지가 추가 대상으로 전송됩니다.

AutoSupport 메시지를 수동으로 트리거합니다

StorageGRID 시스템 관련 문제 해결에 대한 기술 지원을 받으려면 AutoSupport 메시지를 수동으로 전송할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 또는 기타 그리드 구성 권한이 있습니다.

단계

1. 지원 * > * 도구 * > * AutoSupport * 를 선택합니다.

   AutoSupport 페이지가 나타나고 * 설정 * 탭이 선택됩니다.

2. Send User-triggered AutoSupport * 를 선택합니다.

   StorageGRID는 기술 지원 부서에 AutoSupport 메시지를 보내려고 시도합니다. 시도가 성공하면 * Results * 탭의 * Most Recent Result * 및 * Last Successful Time * 값이 업데이트됩니다. 문제가 있는 경우 * 가장 최근의 결과 * 값이 "실패"로 업데이트되고 StorageGRID는 AutoSupport 메시지를 다시 전송하지 않습니다.

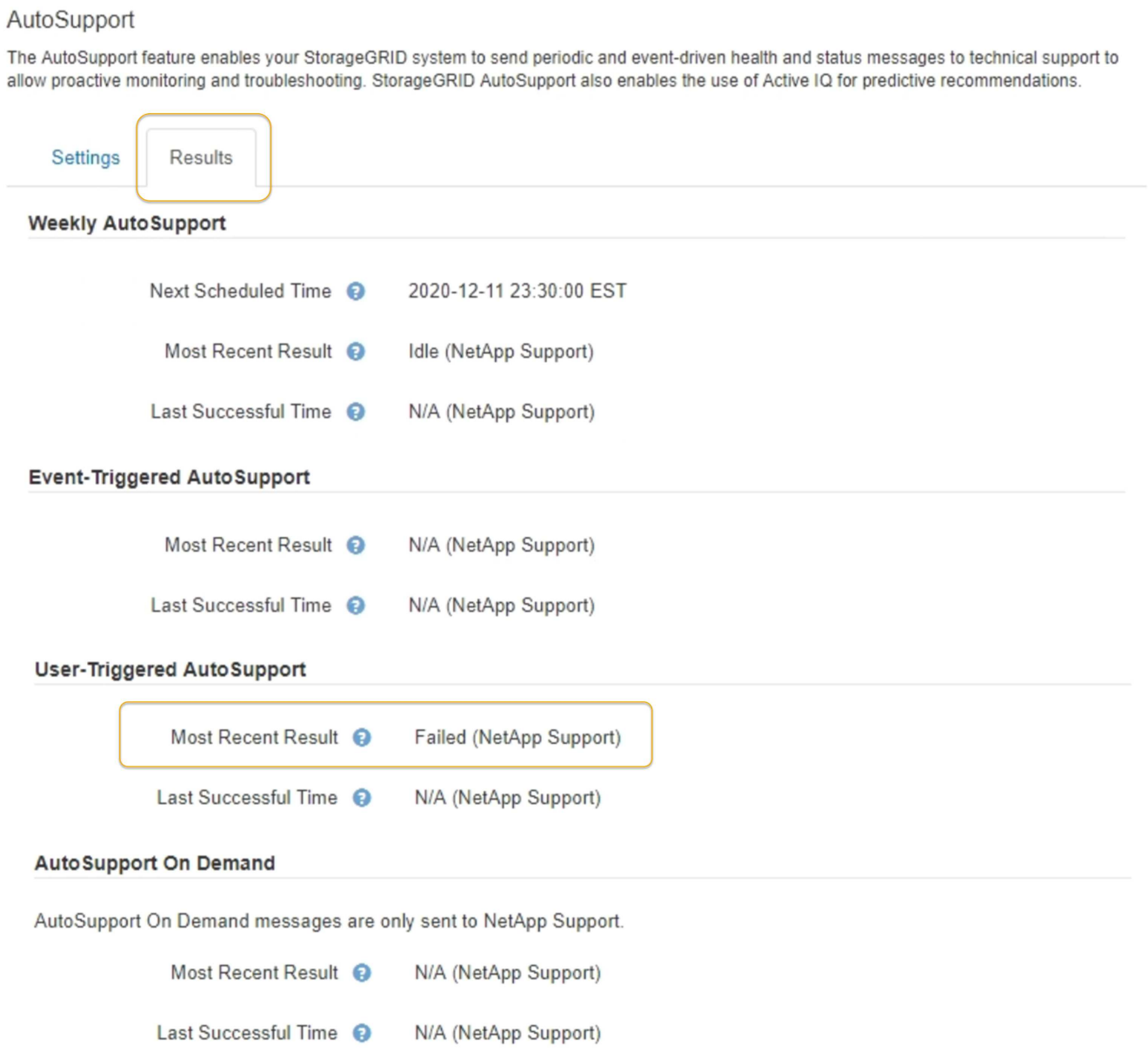
   > 사용자 트리거 AutoSupport 메시지를 보낸 후 1분 후 브라우저에서 AutoSupport 페이지를 새로 고쳐 가장 최근 결과에 액세스합니다.

AutoSupport 메시지 문제 해결

AutoSupport 메시지 전송 시도가 실패하면 StorageGRID 시스템은 AutoSupport 메시지 유형에 따라 다른 작업을 수행합니다. 지원 * > * 도구 * > * AutoSupport * > * 결과 * 를 선택하여 AutoSupport 메시지의 상태를 확인할 수 있습니다.

> e-메일 알림 시스템 전체를 억제하면 이벤트 트리거 AutoSupport 메시지가 표시되지 않습니다. (* 구성 * > * 시스템 * > * 디스플레이 옵션 * 을 선택합니다. 그런 다음 * 알림 모두 표시 안 함 * 을 선택합니다.)

AutoSupport 메시지가 전송되지 않으면 * AutoSupport * 페이지의 * 결과 * 탭에 ""실패""가 나타납니다.



Weekly AutoSupport 메시지 실패

Weekly AutoSupport 메시지가 전송되지 않으면 StorageGRID 시스템에서 다음 작업을 수행합니다.

1. 가장 최근의 결과 속성을 다시 시도하도록 업데이트합니다.
2. 1시간 동안 4분마다 15회 AutoSupport 메시지를 재전송하려고 시도합니다.
3. 전송 실패 1시간 후 는 가장 최근의 결과 속성을 실패 로 업데이트합니다.
4. 다음에 예약된 시간에 AutoSupport 메시지를 다시 보내려고 시도합니다.
5. NMS 서비스를 사용할 수 없어 메시지 실패 시, 7일 이전에 메시지를 보낸 경우, 정규 AutoSupport 일정을 유지 관리합니다.
6. NMS 서비스를 다시 사용할 수 있는 경우 7일 이상 메시지를 보내지 않은 경우 에서 즉시 AutoSupport 메시지를 보냅니다.

사용자가 트리거하거나 이벤트가 트리거된 **AutoSupport** 메시지 오류입니다

사용자 트리거 또는 이벤트 트리거 AutoSupport 메시지가 전송되지 않으면 StorageGRID 시스템에서 다음 작업을 수행합니다.

1. 오류가 알려진 경우 오류 메시지를 표시합니다. 예를 들어, 사용자가 올바른 이메일 구성 설정을 제공하지 않고 SMTP 프로토콜을 선택하면 이메일 서버 페이지의 잘못된 설정으로 인해 SMTP 프로토콜을 사용하여 AutoSupport 메시지를 보낼 수 없습니다 라는 오류가 표시됩니다
2. 메시지를 다시 보내지 않습니다.
3. NMS.log에 오류를 기록합니다.

오류가 발생하고 SMTP가 선택된 프로토콜인 경우, StorageGRID 시스템의 이메일 서버가 올바르게 구성되어 있고 이메일 서버가 실행 중인지 확인하십시오(* support * > * Alarms (legacy) * > * > 레거시 이메일 설정 *). AutoSupport 페이지에 '이메일 서버 페이지의 잘못된 설정으로 인해 SMTP 프로토콜을 사용하여 AutoSupport 메시지를 보낼 수 없습니다.'라는 오류 메시지가 나타날 수 있습니다

에서 전자 메일 서버 설정을 구성하는 방법에 대해 알아봅니다 지침을 모니터링하고 문제를 해결합니다.

AutoSupport 메시지 오류를 해결합니다

오류가 발생하고 SMTP가 선택한 프로토콜인 경우 StorageGRID 시스템의 이메일 서버가 올바르게 구성되어 있고 이메일 서버가 실행 중인지 확인합니다. AutoSupport 페이지에 '이메일 서버 페이지의 잘못된 설정으로 인해 SMTP 프로토콜을 사용하여 AutoSupport 메시지를 보낼 수 없습니다.'라는 오류 메시지가 나타날 수 있습니다

StorageGRID를 통해 **E-Series AutoSupport** 메시지 전송

스토리지 어플라이언스 관리 포트가 아니라 StorageGRID 관리 노드를 통해 E-Series SANtricity System Manager AutoSupport 메시지를 기술 지원 부서에 보낼 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 스토리지 어플라이언스 관리자 권한이나 루트 액세스 권한이 있습니다.

> 그리드 관리자를 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 펌웨어 8.70(11.7) 이상이 있어야 합니다.

이 작업에 대해

E-Series AutoSupport 메시지에는 스토리지 하드웨어의 세부 정보가 포함되어 있으며 StorageGRID 시스템에서 보내는 다른 AutoSupport 메시지보다 더 구체적으로 나타납니다.

어플라이언스의 관리 포트를 사용하지 않고 StorageGRID 관리 노드를 통해 AutoSupport 메시지가 전송되도록 SANtricity 시스템 관리자에서 특수 프록시 서버 주소를 구성합니다. 이렇게 전송되는 AutoSupport 메시지는 그리드 관리자에서 구성되었을 수 있는 기본 설정 보낸 사람 및 관리자 프록시 설정을 기준으로 합니다.

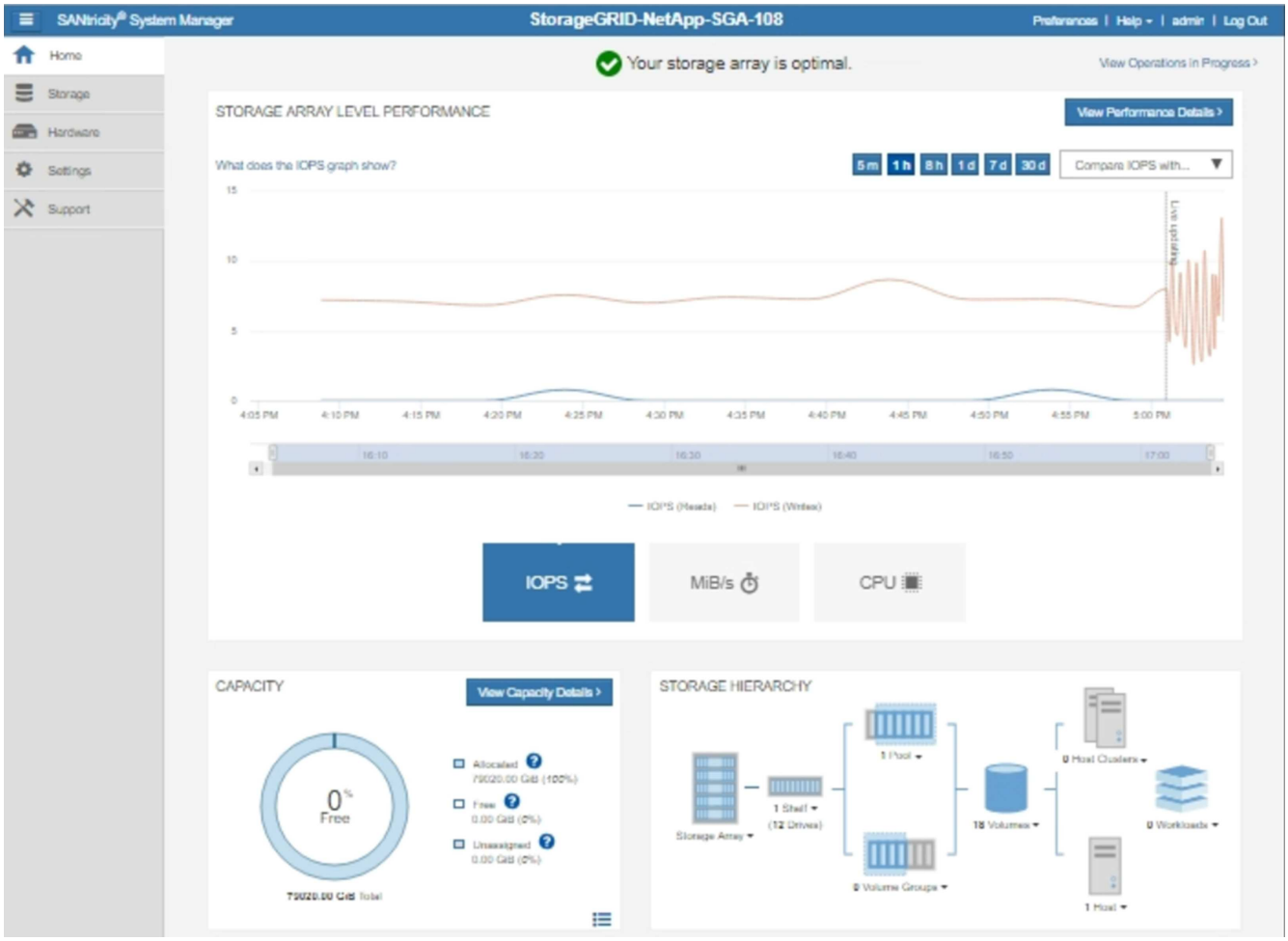
Grid Manager에서 Admin 프록시 서버를 구성하려면 을 참조하십시오 관리자 프록시 설정을 구성합니다.

> 이 절차는 E-Series AutoSupport 메시지용으로 StorageGRID 프록시 서버를 구성하는 경우에만 적용됩니다. E-Series AutoSupport 구성에 대한 자세한 내용은 를 참조하십시오 "NetApp E-Series 및 SANtricity 문서".

단계

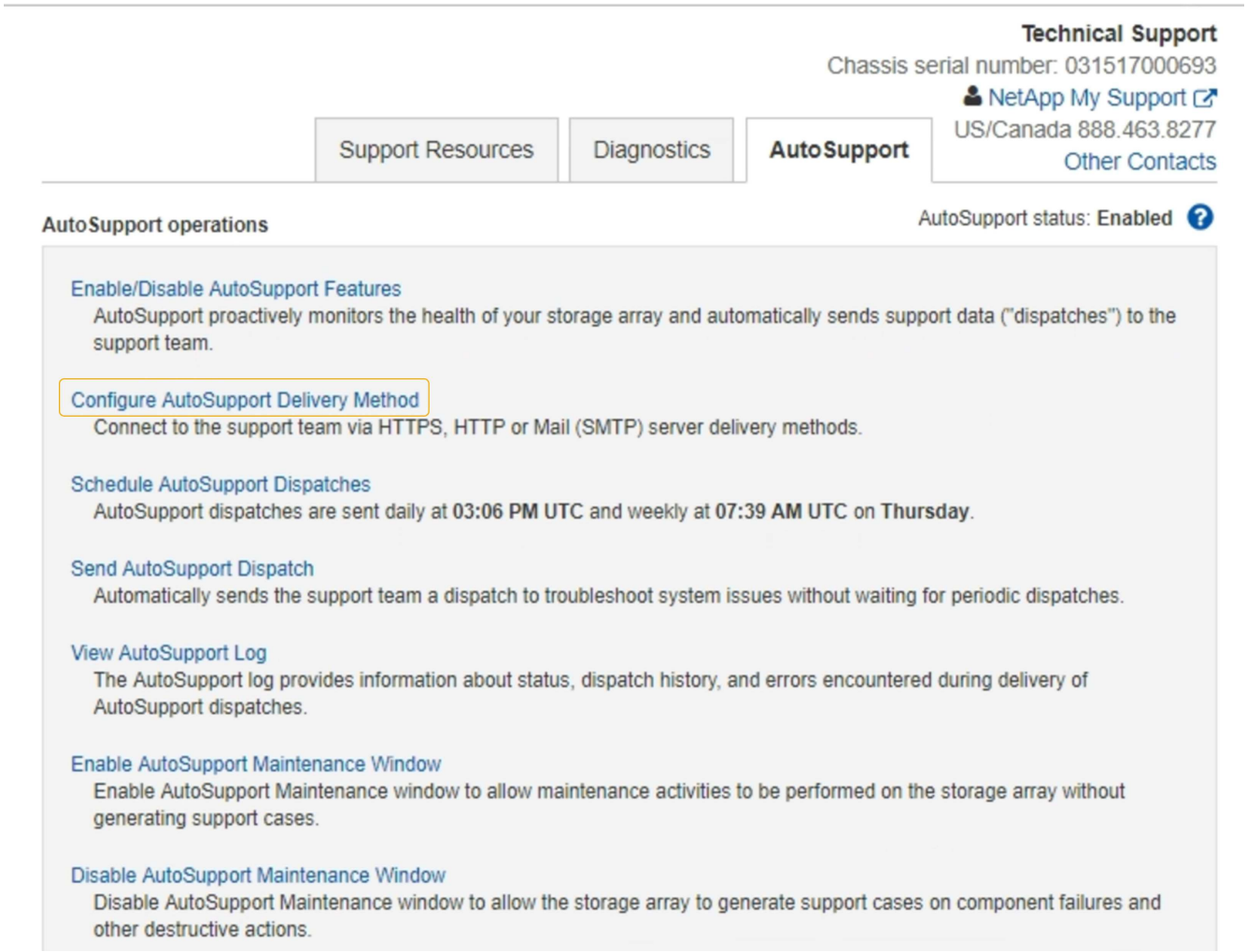
1. Grid Manager에서 * nodes * 를 선택합니다.
2. 왼쪽의 노드 목록에서 구성할 스토리지 어플라이언스 노드를 선택합니다.
3. SANtricity 시스템 관리자 * 를 선택합니다.

   SANtricity 시스템 관리자 홈 페이지가 나타납니다.



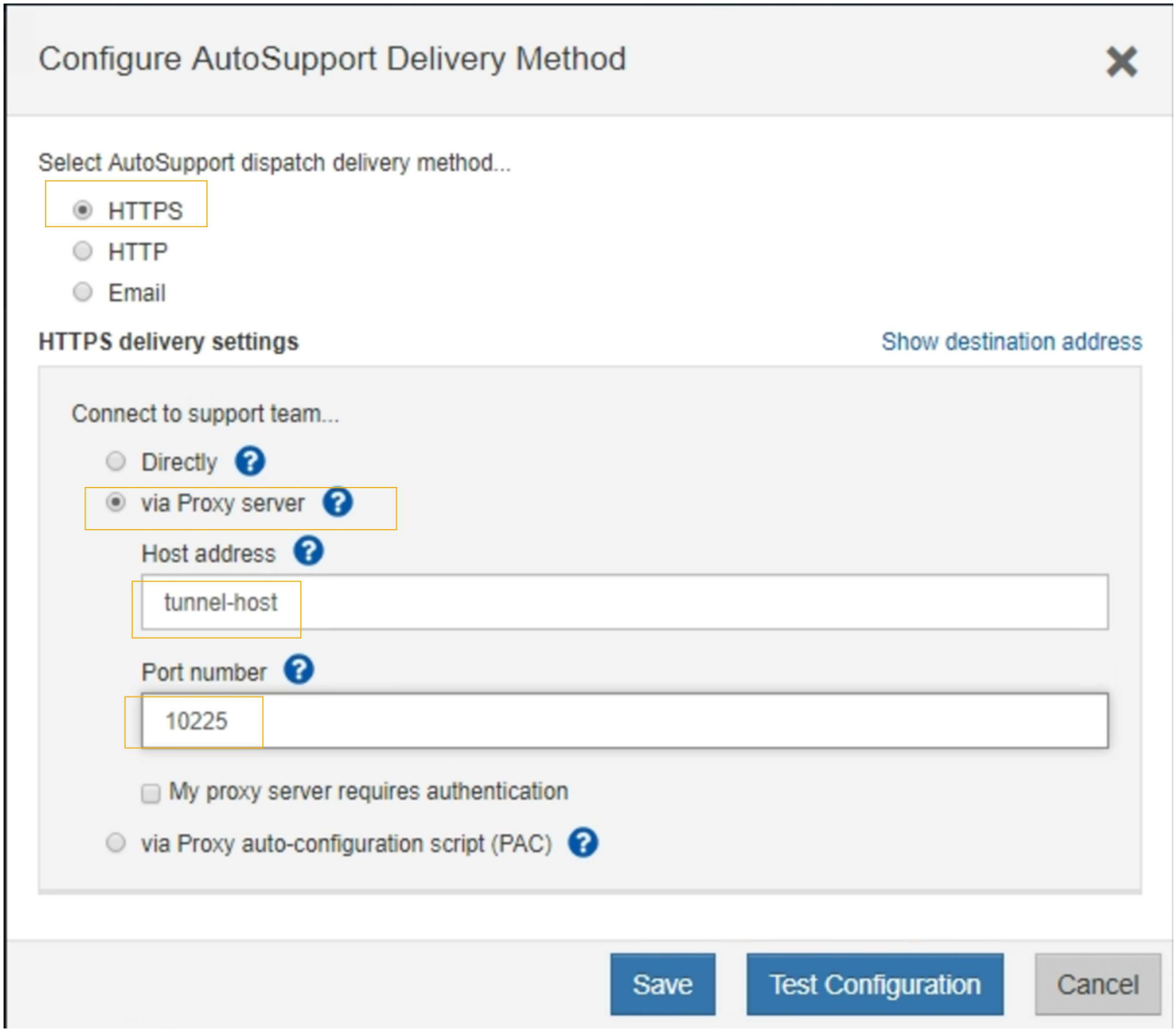
4. 지원 * > * 지원 센터 * > * AutoSupport * 를 선택합니다.

   AutoSupport 작업 페이지가 나타납니다.



5. AutoSupport 제공 방법 구성 * 을 선택합니다.

   AutoSupport 배달 방법 구성 페이지가 나타납니다.



6. 전달 방법으로 * HTTPS * 를 선택합니다.

   HTTPS 프로토콜을 활성화하는 인증서가 미리 설치되어 있습니다.

7. 프록시 서버를 통해 * 를 선택합니다.
8. Host address * 로 tunnel-host를 입력한다.

   Tunnel-host는 관리 노드를 사용하여 E-Series AutoSupport 메시지를 보내는 특수 주소입니다.

9. Port number * 로 10225 를 입력한다.

   10225는 어플라이언스의 E-Series 컨트롤러에서 AutoSupport 메시지를 수신하는 StorageGRID 프록시 서버의 포트 번호입니다.

10. AutoSupport 프록시 서버의 라우팅 및 구성을 테스트하려면 * 구성 테스트 * 를 선택합니다.

    올바른 경우 녹색 배너에 "'Your AutoSupport configuration has been verified(사용자의 구성이 확인되었습니다)' 메시지가 나타납니다.

테스트에 실패하면 빨간색 배너에 오류 메시지가 나타납니다. StorageGRID DNS 설정 및 네트워킹을 확인하고 기본 센더 관리자 노드가 NetApp Support 사이트에 연결할 수 있는지 확인한 다음 테스트를 다시 시도하십시오.

11. 저장 * 을 선택합니다.

    구성이 저장되고 "'AutoSupport delivery method has been configured(전달 방법이 구성되었습니다)' 확인 메시지가 나타납니다.

스토리지 노드 관리

스토리지 노드 관리 정보

스토리지 노드는 디스크 스토리지 용량 및 서비스를 제공합니다. 스토리지 노드 관리는 다음을 수반합니다.

- 스토리지 옵션 관리
- 스토리지 볼륨 워터마크의 정의 및 워터마크 덮어쓰기를 사용하여 스토리지 노드가 읽기 전용이 되는 시점을 제어하는 방법을 이해합니다
- 오브젝트 메타데이터에 사용되는 공간 모니터링 및 관리
- 저장된 개체에 대한 전역 설정 구성
- 스토리지 노드 구성 설정을 적용하는 중입니다
- 전체 스토리지 노드 관리

스토리지 노드란?

스토리지 노드: 오브젝트 데이터 및 메타데이터를 관리하고 저장합니다. 각 StorageGRID 시스템에는 3개 이상의 스토리지 노드가 있어야 합니다. 여러 사이트가 있는 경우 StorageGRID 시스템 내의 각 사이트에도 3개의 스토리지 노드가 있어야 합니다.

스토리지 노드에는 디스크에서 오브젝트 데이터와 메타데이터를 저장, 이동, 확인 및 검색하는 데 필요한 서비스와 프로세스가 포함되어 있습니다. 노드 * 페이지에서 스토리지 노드에 대한 자세한 정보를 볼 수 있습니다.

ADC 서비스란 무엇입니까?

ADC(관리 도메인 컨트롤러) 서비스는 그리드 노드와 상호 연결을 인증합니다. ADC 서비스는 사이트의 처음 세 스토리지 노드 각각에 호스팅됩니다.

ADC 서비스는 서비스의 위치 및 가용성을 포함한 토폴로지 정보를 유지합니다. 그리드 노드에 다른 그리드 노드의 정보가 필요하거나 다른 그리드 노드에서 작업을 수행해야 하는 경우 ADC 서비스에 문의하여 요청을 처리할 최적의 그리드 노드를 찾습니다. 또한 ADC 서비스는 StorageGRID 배포의 구성 번들의 복사본을 유지하여 그리드 노드가 현재 구성 정보를 검색할 수 있도록 합니다. 그리드 토폴로지 페이지에서 스토리지 노드에 대한 ADC 정보를 볼 수 있습니다(* support*>* Grid topology*).

분산 및 분산 작업을 용이하게 하기 위해 각 ADC 서비스는 인증서, 구성 번들 및 서비스 및 토폴로지에 대한 정보를 StorageGRID 시스템의 다른 ADC 서비스와 동기화합니다.

일반적으로 모든 그리드 노드는 하나 이상의 ADC 서비스에 대한 연결을 유지합니다. 이렇게 하면 그리드 노드가 항상 최신 정보에 액세스할 수 있습니다. 그리드 노드가 연결되면 다른 그리드 노드 "" 인증서를 캐시하여 ADC 서비스를

사용할 수 없는 경우에도 시스템이 알려진 그리드 노드를 계속 사용할 수 있도록 합니다. 새 그리드 노드는 ADC 서비스를 통해서만 연결을 설정할 수 있습니다.

ADC 서비스는 각 그리드 노드의 연결을 통해 토폴로지 정보를 수집할 수 있습니다. 이 그리드 노드 정보에는 CPU 로드, 사용 가능한 디스크 공간(스토리지가 있는 경우), 지원되는 서비스 및 그리드 노드의 사이트 ID가 포함됩니다. 다른 서비스에서는 ADC 서비스에 토폴로지 쿼리를 통한 토폴로지 정보를 요청합니다. ADC 서비스는 StorageGRID 시스템에서 수신한 최신 정보로 각 쿼리에 응답합니다.

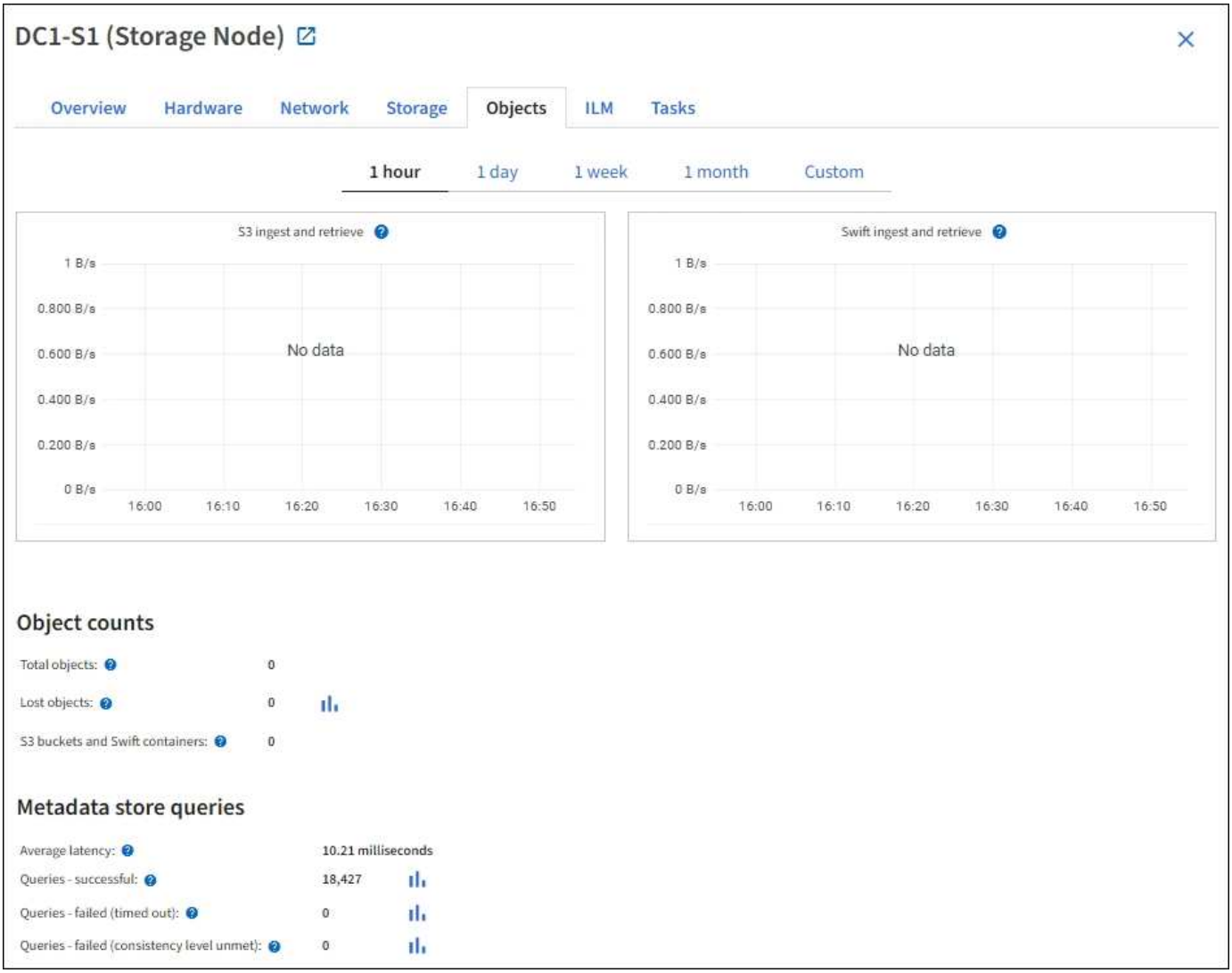
DDS 서비스란 무엇입니까**?**

스토리지 노드에서 호스팅되는 DDS(Distributed Data Store) 서비스는 Cassandra 데이터베이스와 상호 작용하여 StorageGRID 시스템에 저장된 객체 메타데이터에 대한 백그라운드 작업을 수행합니다.

개체 수

DDS 서비스는 StorageGRID 시스템으로 수집된 총 객체 수와 시스템의 지원되는 인터페이스(S3 또는 Swift)를 통해 수집된 총 객체 수를 추적합니다.

모든 스토리지 노드의 노드 페이지 > 개체 탭에서 총 개체 수를 확인할 수 있습니다.



쿼리

특정 DDS 서비스를 통해 메타데이터 저장소에 대한 쿼리를 실행하는 데 걸리는 평균 시간, 성공한 총 쿼리 수 및 제한 시간 문제로 인해 실패한 총 쿼리 수를 확인할 수 있습니다.

쿼리 정보를 검토하여 메타데이터 저장소, Cassandra의 상태를 모니터링할 수 있으며, 이는 시스템의 수집 및 검색 성능에 영향을 줍니다. 예를 들어, 평균 쿼리의 지연 시간이 느리고 시간 초과로 인해 실패한 쿼리의 수가 많은 경우 메타데이터 저장소의 로드가 높거나 다른 작업을 수행해야 할 수 있습니다.

일관성 오류로 인해 실패한 총 쿼리 수를 볼 수도 있습니다. 정합성 보장 레벨 오류는 특정 DDS 서비스를 통해 쿼리를 수행할 때 사용 가능한 메타데이터 저장소의 수가 부족하기 때문에 발생합니다.

진단 페이지를 사용하여 그리드의 현재 상태에 대한 추가 정보를 얻을 수 있습니다. 을 참조하십시오 진단 유틸리티를 실행합니다.

일관성 보장 및 제어

StorageGRID는 새로 생성된 개체에 대해 쓰기 후 읽기 일관성을 보장합니다. 성공적으로 완료된 PUT 작업 이후의 모든 GET 작업은 새로 작성된 데이터를 읽을 수 있습니다. 기존 오브젝트, 메타데이터 업데이트 및 삭제를 덮어쓰더라도 결국 일관성이 유지됩니다.

LDR 서비스란?

각 스토리지 노드에 의해 호스팅되는 LDR(Local Distribution Router) 서비스는 StorageGRID 시스템의 콘텐츠 전송을 처리합니다. 콘텐츠 전송에는 데이터 저장, 라우팅 및 요청 처리를 비롯한 다양한 작업이 포함됩니다. LDR 서비스는 데이터 전송 로드 및 데이터 트래픽 기능을 처리하여 StorageGRID 시스템의 대부분의 작업을 수행합니다.

LDR 서비스는 다음 작업을 처리합니다.

- 쿼리
- ILM(정보 수명 주기 관리) 작업
- 개체 삭제
- 오브젝트 데이터 스토리지
- 다른 LDR 서비스(스토리지 노드)에서 오브젝트 데이터 전송
- 데이터 스토리지 관리
- 프로토콜 인터페이스(S3 및 Swift)

또한 LDR 서비스는 StorageGRID 시스템이 수집된 각 오브젝트에 할당하는 고유 "UUID(Content Handles)"(UUID)에 S3 및 Swift 객체의 매핑을 관리합니다.

쿼리

LDR 쿼리에는 검색 및 아카이브 작업 중 개체 위치에 대한 쿼리가 포함됩니다. 쿼리를 실행하는 데 걸리는 평균 시간, 성공한 쿼리의 총 수 및 제한 시간 문제로 인해 실패한 쿼리의 총 수를 확인할 수 있습니다.

쿼리 정보를 검토하여 메타데이터 저장소의 상태를 모니터링하여 시스템의 수집 및 검색 성능에 영향을 줄 수 있습니다. 예를 들어, 평균 쿼리의 지연 시간이 느리고 시간 초과로 인해 실패한 쿼리의 수가 많은 경우 메타데이터 저장소의 로드가 높거나 다른 작업을 수행해야 할 수 있습니다.

일관성 오류로 인해 실패한 총 쿼리 수를 볼 수도 있습니다. 정합성 보장 수준 오류는 특정 LDR 서비스를 통해 쿼리를

수행할 때 사용 가능한 메타데이터 저장소의 수가 부족하여 발생합니다.

진단 페이지를 사용하여 그리드의 현재 상태에 대한 추가 정보를 얻을 수 있습니다. 을 참조하십시오 진단 유틸리티를 실행합니다.

ILM 활동

ILM(정보 수명 주기 관리) 메트릭을 통해 ILM 구현을 위해 개체가 평가되는 속도를 모니터링할 수 있습니다. 이러한 메트릭은 대시보드 또는 * 노드 * > *스토리지 노드 * > * ILM * 에서 볼 수 있습니다.

오브젝트 저장소

LDR 서비스의 기본 데이터 스토리지는 고정된 수의 오브젝트 저장소(스토리지 볼륨이라고도 함)로 나뉩니다. 각 오브젝트 저장소는 별도의 마운트 지점입니다.

노드 페이지 > 스토리지 탭에서 스토리지 노드의 객체 저장소를 확인할 수 있습니다.

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

스토리지 노드의 오브젝트 저장소는 002F의 16진수 번호로 식별되며 볼륨 ID라고도 합니다. Cassandra 데이터베이스의 오브젝트 메타데이터에 대한 첫 번째 오브젝트 저장소(볼륨 0)에 공간이 예약되며, 해당 볼륨의 나머지 공간은 오브젝트 데이터에 사용됩니다. 다른 모든 오브젝트 저장소는 복제된 복사본 및 삭제 코딩 조각이 포함된 오브젝트 데이터에만 사용됩니다.

복제된 복사본에 대한 공간 사용이 고르게 되도록 지정된 개체의 개체 데이터는 사용 가능한 스토리지 공간을 기반으로 한 하나의 개체 저장소에 저장됩니다. 하나 이상의 오브젝트 저장소에서 용량을 채우는 경우, 나머지 오브젝트 저장소는 스토리지 노드에 더 이상 공간이 없을 때까지 오브젝트를 계속 저장합니다.

메타데이터 보호

오브젝트 메타데이터는 오브젝트 수정 시간 또는 저장 위치와 같은 오브젝트의 설명이나 이와 관련된 정보입니다. StorageGRID는 LDR 서비스와 상호 작용하는 Cassandra 데이터베이스에 개체 메타데이터를 저장합니다.

이중화를 보장하고 손실을 방지하기 위해 각 사이트에 오브젝트 메타데이터의 복사본 3개가 유지됩니다. 각 사이트의 모든 스토리지 노드에 복사본이 균등하게 분산됩니다. 이 복제는 구성이 불가능하며 자동으로 수행됩니다.

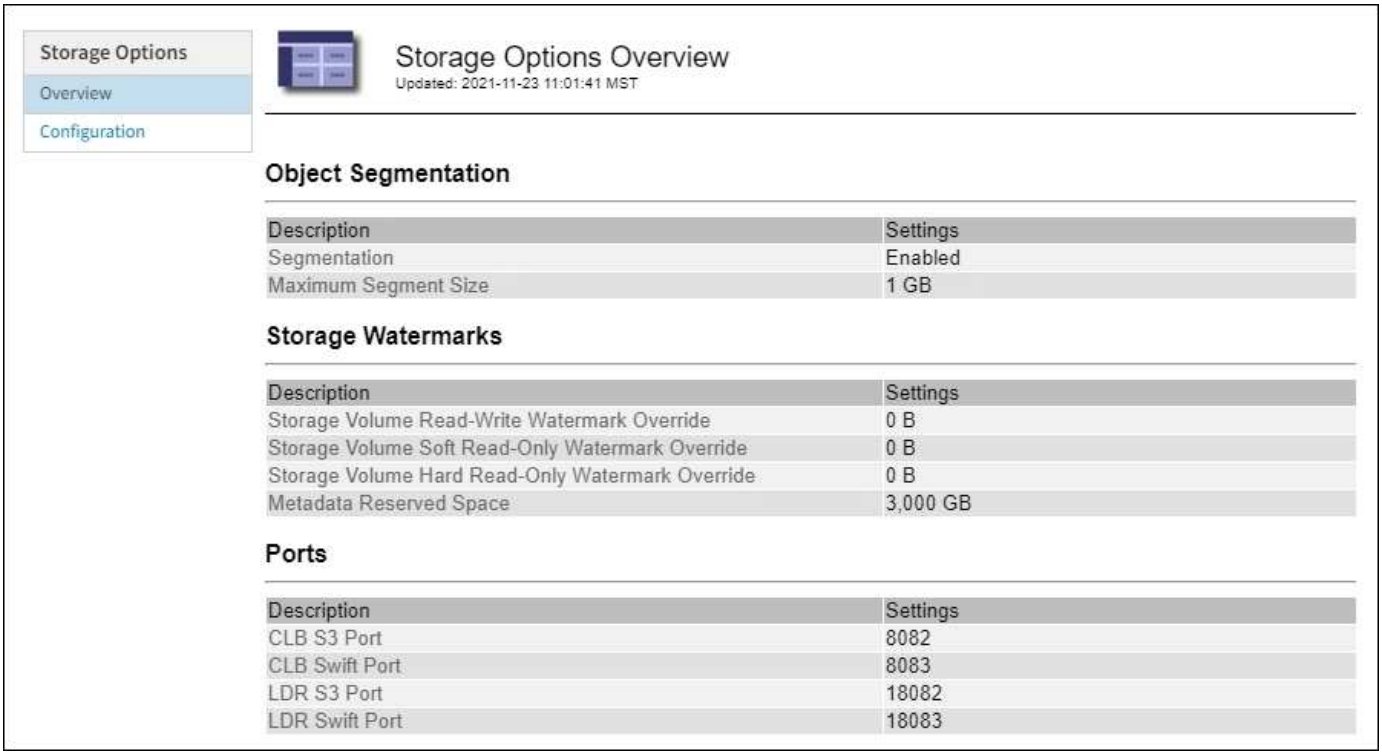
오브젝트 메타데이터 스토리지 관리

스토리지 옵션 관리

저장소 옵션에는 개체 분할 설정, 스토리지 볼륨 워터마크의 현재 값 및 메타데이터 예약된 공간 설정이 포함됩니다. 또한 게이트웨이 노드에서 더 이상 사용되지 않는 CLB 서비스와 스토리지

노드의 LDR 서비스에서 사용하는 S3 및 Swift 포트를 볼 수 있습니다.

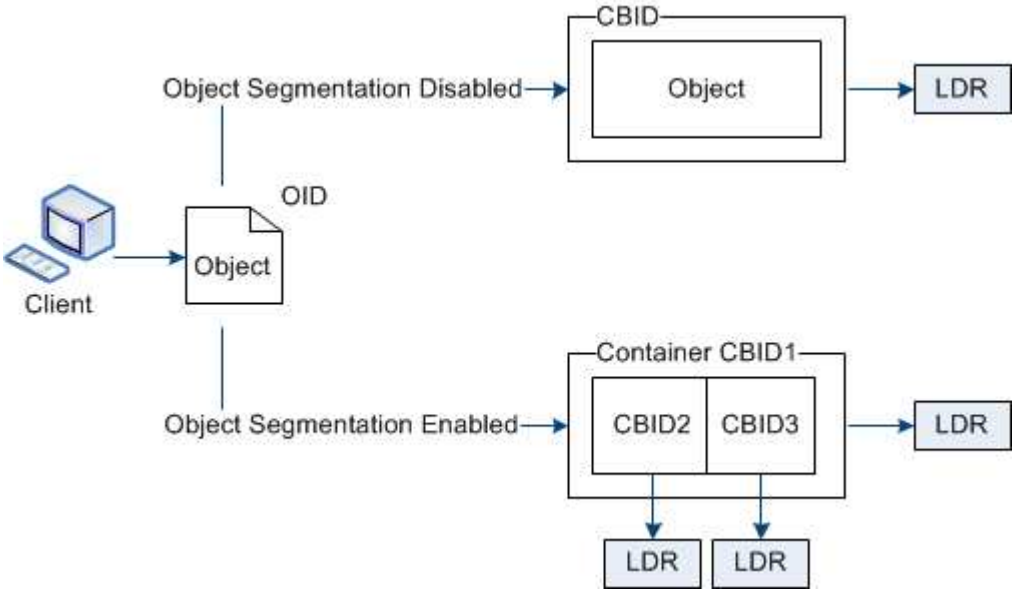
포트 할당에 대한 자세한 내용은 을 참조하십시오 요약: 클라이언트 연결을 위한 IP 주소 및 포트.



객체 분할이란 무엇입니까?

객체 분할은 큰 객체에 대한 스토리지 및 리소스 사용을 최적화하기 위해 객체를 작은 고정 크기 객체 컬렉션으로 분할하는 프로세스입니다. S3 다중 파트 업로드는 또한 각 파트를 나타내는 오브젝트와 함께 분할된 오브젝트를 만듭니다.

개체가 StorageGRID 시스템으로 수집되면 LDR 서비스는 개체를 세그먼트로 분할하고 모든 세그먼트의 헤더 정보를 내용으로 나열하는 세그먼트 컨테이너를 만듭니다.



세그먼트 컨테이너를 검색할 때 LDR 서비스는 세그먼트에서 원래 개체를 어셈블하고 개체를 클라이언트에 반환합니다.

컨테이너와 세그먼트가 반드시 동일한 스토리지 노드에 저장되지는 않습니다. 컨테이너 및 세그먼트는 ILM 규칙에 지정된 스토리지 풀 내의 모든 스토리지 노드에 저장할 수 있습니다.

각 세그먼트는 StorageGRID 시스템에 의해 독립적으로 처리되고 관리되는 개체 및 저장된 개체와 같은 특성의 카운트에 기여합니다. 예를 들어, StorageGRID 시스템에 저장된 객체가 두 세그먼트로 분할되면 다음과 같이 수집 완료 후 관리 객체 값이 3씩 증가합니다.

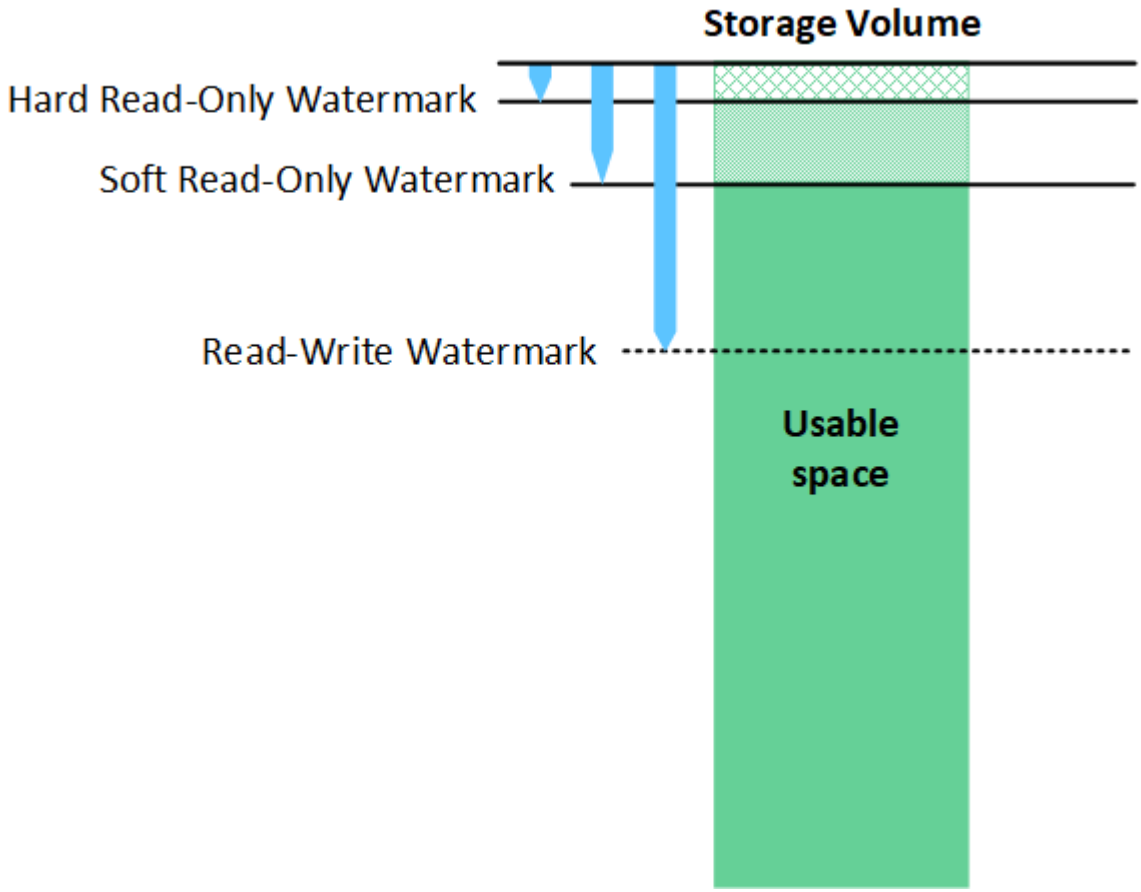
세그먼트 컨테이너 + 세그먼트 1 + 세그먼트 2 = 저장된 오브젝트 3개

다음과 같은 방법으로 큰 물체를 다룰 때 성능을 향상시킬 수 있습니다.

- 각 게이트웨이 및 스토리지 노드에는 필요한 처리량을 위한 충분한 네트워크 대역폭이 있습니다. 예를 들어 10Gbps 이더넷 인터페이스에서 별도의 그리드 및 클라이언트 네트워크를 구성합니다.
- 필요한 처리량에 대해 충분한 게이트웨이 및 스토리지 노드가 구축됩니다.
- 각 스토리지 노드에는 필요한 처리량을 위한 충분한 디스크 입출력 성능이 있습니다.

스토리지 볼륨 워터마크란 무엇입니까?

StorageGRID는 세 개의 스토리지 볼륨 워터마크를 사용하여 공간이 매우 부족하기 전에 스토리지 노드가 읽기 전용 상태로 안전하게 전환되도록 하고 읽기 전용 상태로 전환된 스토리지 노드가 다시 읽기-쓰기로 전환되도록 합니다.



> 스토리지 볼륨 워터마크는 복제되고 삭제 코딩 오브젝트 데이터에 사용되는 공간에만 적용됩니다. 볼륨 0의 오브젝트 메타데이터에 예약된 공간에 대한 자세한 내용은 로 이동하십시오오브젝트 메타데이터 스토리지 관리.

소프트 읽기 전용 워터마크로 무엇이 있습니까?

스토리지 볼륨 소프트 읽기 전용 워터마크 * 는 스토리지 노드의 사용 가능한 오브젝트 데이터 공간이 가득 차있음을 나타내는 첫 번째 워터마크입니다.

스토리지 노드의 각 볼륨에 해당 볼륨의 소프트 읽기 전용 워터마크에 비해 사용 가능한 공간이 적을 경우 스토리지 노드가 _읽기 전용 모드_로 전환됩니다. 읽기 전용 모드는 스토리지 노드가 나머지 StorageGRID 시스템에 읽기 전용 서비스를 알리는 반면 보류 중인 모든 쓰기 요청을 처리하는 것을 의미합니다.

예를 들어 스토리지 노드의 각 볼륨에 10GB의 소프트 읽기 전용 워터마크가 있다고 가정합니다. 각 볼륨의 사용 가능한 공간이 10GB 미만이면 스토리지 노드가 소프트 읽기 전용 모드로 전환됩니다.

하드 읽기 전용 워터마크로 무엇이 있습니까?

스토리지 볼륨 하드 읽기 전용 워터마크 * 는 노드의 사용 가능한 오브젝트 데이터 공간이 가득 차있음을 나타내는 다음 워터마크입니다.

볼륨의 사용 가능한 공간이 해당 볼륨의 하드 읽기 전용 배경무늬 보다 적은 경우 볼륨에 대한 쓰기가 실패합니다. 그러나 다른 볼륨에 대한 쓰기는 해당 볼륨의 사용 가능한 공간이 하드 읽기 전용 워터마크보다 작을 때까지 계속될 수 있습니다.

예를 들어, 스토리지 노드의 각 볼륨에 5GB의 하드 읽기 전용 워터마크가 있다고 가정합니다. 각 볼륨의 사용 가능한 공간이 5GB 미만이면 스토리지 노드가 더 이상 쓰기 요청을 수락하지 않습니다.

하드 읽기 전용 배경무늬 는 항상 소프트 읽기 전용 배경무늬 보다 작습니다.

읽기-쓰기 워터마크가 무엇입니까?

스토리지 볼륨 읽기-쓰기 워터마크 * 는 읽기 전용 모드로 전환된 스토리지 노드에만 적용됩니다. 노드가 다시 읽기-쓰기가 될 수 있는 시기를 결정합니다. 스토리지 노드의 한 스토리지 볼륨에서 사용 가능한 공간이 해당 볼륨의 읽기-쓰기 워터마크보다 크면 노드가 자동으로 읽기-쓰기 상태로 전환됩니다.

예를 들어 스토리지 노드가 읽기 전용 모드로 전환되었다고 가정해 보겠습니다. 또한 각 볼륨에 30GB의 읽기/쓰기 워터마크가 있다고 가정합니다. 볼륨의 사용 가능한 공간이 30GB로 증가하는 즉시 노드는 다시 읽기-쓰기가 됩니다.

읽기-쓰기 워터마크가 항상 소프트 읽기 전용 워터마크와 하드 읽기 전용 워터마크보다 큽니다.

스토리지 볼륨 워터마크를 봅니다

현재 워터마크 설정 및 시스템 최적화 값을 볼 수 있습니다. 최적화된 워터마크를 사용하지 않는 경우 설정을 조정할 수 있는지 또는 조정할 수 있는지 여부를 결정할 수 있습니다.

필요한 것

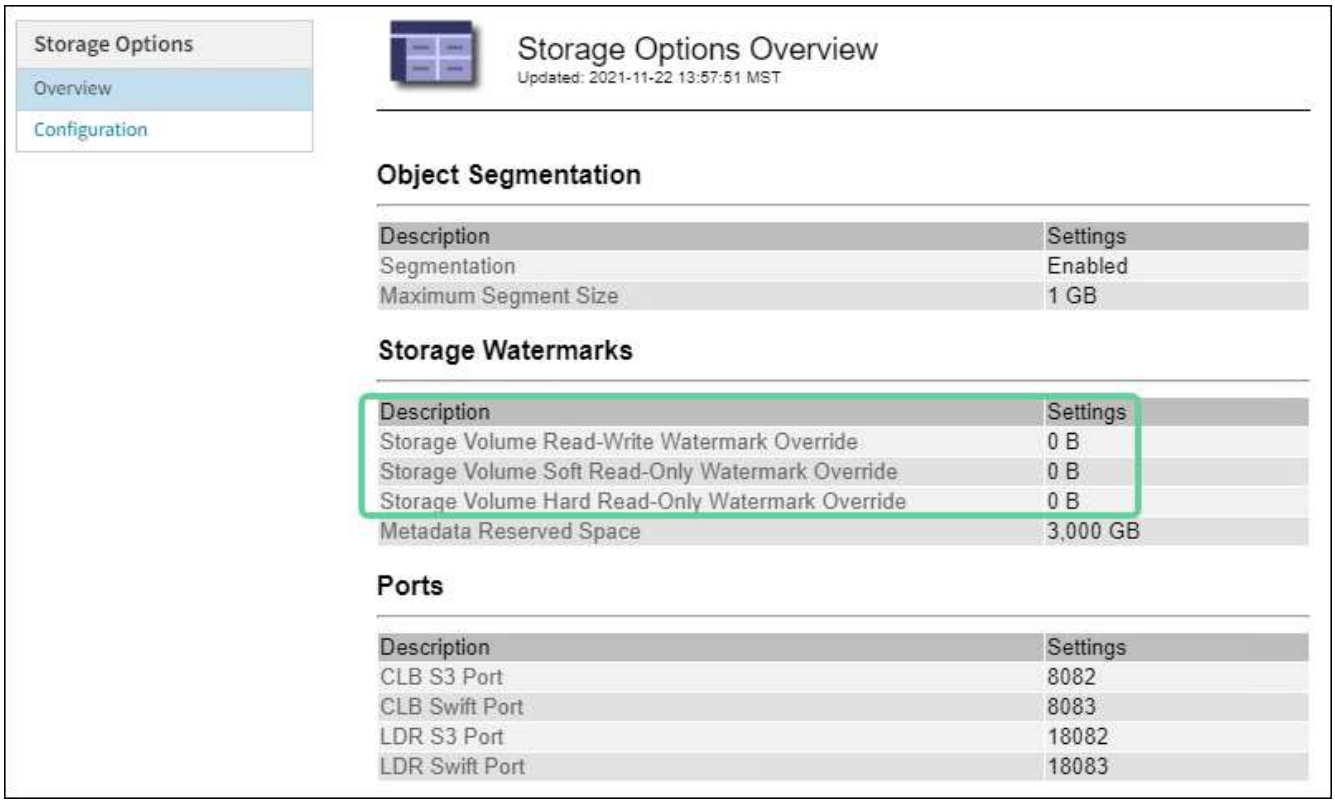
- StorageGRID 11.6으로의 업그레이드를 완료했습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.

현재 워터마크 설정을 봅니다

그리드 관리자에서 현재 스토리지 워터마크 설정을 볼 수 있습니다.

단계

1. 구성 * > * 시스템 * > * 스토리지 옵션 * 을 선택합니다.
2. Storage Watermarks 섹션에서 세 개의 스토리지 볼륨 워터마크 재정의에 대한 설정을 확인합니다.



   - 워터마크 재정의가 * 0 * 인 경우 스토리지 노드의 크기와 볼륨의 상대 용량을 기준으로 모든 스토리지 노드의 모든 스토리지 볼륨에 대해 세 가지 워터마크가 모두 최적화됩니다.

     이 설정이 기본값이며 권장 설정입니다. 이러한 값은 업데이트하지 않아야 합니다. 필요에 따라 원하는 대로 할 수 있습니다 최적화된 스토리지 워터마크를 봅니다.

   - 워터마크 재정의가 0이 아닌 값이면 사용자 지정(최적화되지 않은) 워터마크가 사용됩니다. 사용자 지정 배경무늬 설정은 사용하지 않는 것이 좋습니다. 의 지침을 사용합니다 낮은 읽기 전용 배경무늬 재정의 알림 문제 해결 설정을 조정할 수 있는지 또는 조정할 수 있는지 확인합니다.

최적화된 스토리지 워터마크를 봅니다

StorageGRID는 두 개의 Prometheus 메트릭을 사용하여 * 스토리지 볼륨 소프트 읽기 전용 워터마크 * 에 대해 계산된 최적화 값을 표시합니다. 그리드의 각 스토리지 노드에 대해 최적화된 최소 및 최대 값을 볼 수 있습니다.

1. 지원 * > * 도구 * > * 메트릭 * 을 선택합니다.
2. Prometheus 섹션에서 Prometheus 사용자 인터페이스에 액세스할 링크를 선택합니다.
3. 권장되는 최소 소프트 읽기 전용 워터마크를 보려면 다음 Prometheus 메트릭을 입력하고 * Execute * 를 선택합니다.

'toragegrid_storage_volume_minimum_optimized_soft_readonly_watermark'

마지막 열에는 각 스토리지 노드의 모든 스토리지 볼륨에 대해 소프트 읽기 전용 워터마크의 최적화된 최소값이 표시됩니다. 이 값이 * 스토리지 볼륨 소프트 읽기 전용 워터마크 * 에 대한 사용자 정의 설정보다 크면 * 읽기 전용 로우 워터마크 재정의 * 알림이 스토리지 노드에 대해 트리거됩니다.

4. 권장되는 최대 소프트 읽기 전용 워터마크를 보려면 다음 Prometheus 메트릭을 입력하고 * Execute * 를 선택합니다.

   'toragegrid_storage_volume_maximum_optimized_soft_readonly_watermark'

   마지막 열에는 각 스토리지 노드의 모든 스토리지 볼륨에 대해 소프트 읽기 전용 워터마크의 최대 최적화 값이 표시됩니다.

오브젝트 메타데이터 스토리지 관리

StorageGRID 시스템의 오브젝트 메타데이터 용량은 해당 시스템에 저장할 수 있는 최대 오브젝트 수를 제어합니다. StorageGRID 시스템에 새 개체를 저장할 충분한 공간이 있는지 확인하려면 StorageGRID에서 개체 메타데이터를 저장하는 위치와 방법을 알아야 합니다.

오브젝트 메타데이터란?

개체 메타데이터는 개체를 설명하는 정보입니다. StorageGRID는 오브젝트 메타데이터를 사용하여 그리드 전체의 모든 오브젝트의 위치를 추적하고 각 오브젝트의 라이프사이클 관리를 제공합니다.

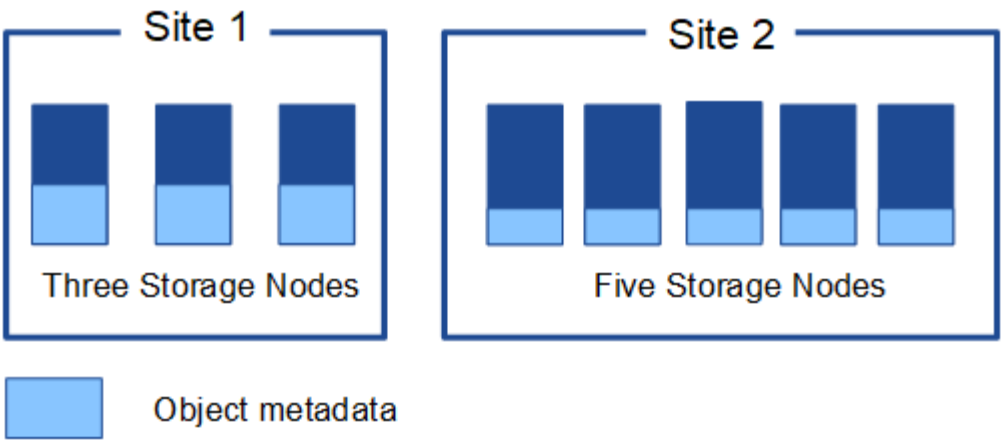
StorageGRID의 개체에 대한 개체 메타데이터에는 다음 유형의 정보가 포함됩니다.

- 각 개체의 고유 ID(UUID), 개체 이름, S3 버킷 또는 Swift 컨테이너의 이름, 테넌트 계정 이름 또는 ID, 개체의 논리적 크기, 개체를 처음 만든 날짜 및 시간을 포함한 시스템 메타데이터 및 객체가 마지막으로 수정된 날짜 및 시간입니다.
- 객체와 연결된 모든 사용자 메타데이터 키 값 쌍입니다.
- S3 오브젝트의 경우 오브젝트와 연결된 오브젝트 태그 키 값 쌍이 됩니다.
- 복제된 오브젝트 복사본의 경우 각 복제본의 현재 스토리지 위치입니다.
- 삭제 코딩 오브젝트 복사본의 경우 각 분절의 현재 스토리지 위치입니다.
- 클라우드 스토리지 풀의 오브젝트 복사본의 경우 외부 버킷의 이름 및 오브젝트의 고유 식별자를 비롯한 오브젝트의 위치가 포함됩니다.
- 분할된 오브젝트 및 다중 파트 오브젝트의 경우 세그먼트 식별자 및 데이터 크기가 사용됩니다.

오브젝트 메타데이터는 어떻게 저장됩니까?

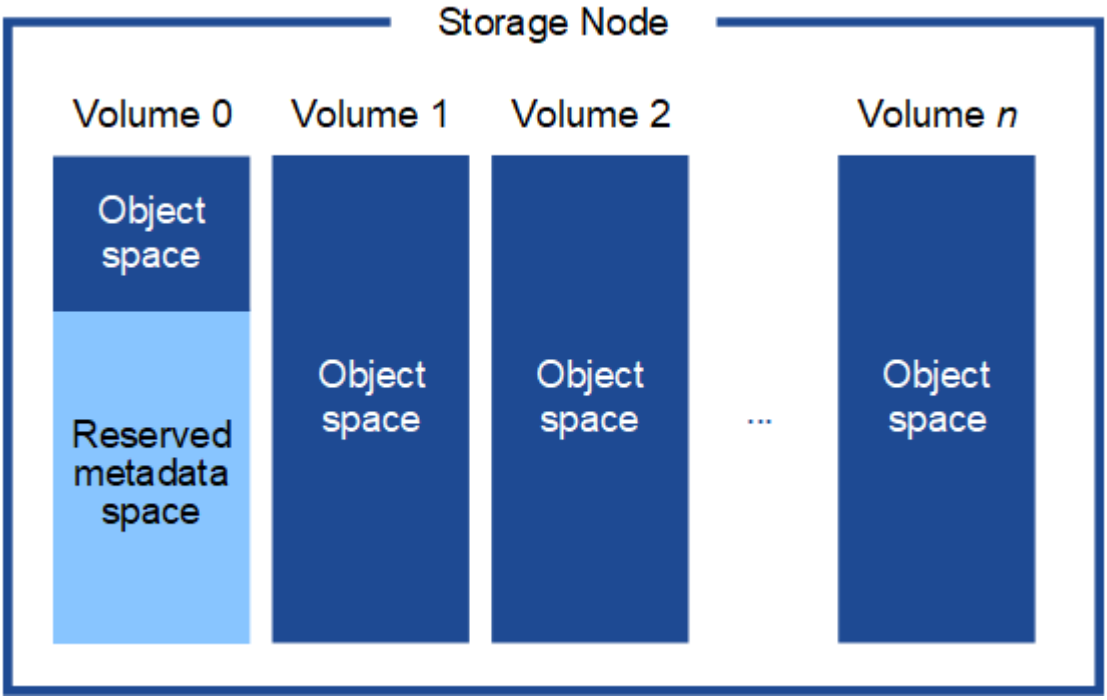
StorageGRID는 오브젝트 메타데이터를 Cassandra 데이터베이스에 유지하며, 이 데이터베이스는 오브젝트 데이터와 독립적으로 저장됩니다. 이중화를 제공하고 개체 메타데이터를 손실로부터 보호하기 위해 StorageGRID는 각 사이트의 시스템 모든 개체에 대한 메타데이터 복사본을 3개 저장합니다. 오브젝트 메타데이터의 복사본 3개는 각 사이트의 모든 스토리지 노드에 균등하게 분산됩니다.

이 그림은 두 사이트의 스토리지 노드를 나타냅니다. 각 사이트에는 동일한 양의 오브젝트 메타데이터가 있으며, 이 메타데이터는 해당 사이트의 스토리지 노드 전체에 균등하게 분산됩니다.



오브젝트 메타데이터는 어디에 저장됩니까?

이 그림은 단일 스토리지 노드의 스토리지 볼륨을 나타냅니다.



그림에 나와 있는 것처럼 StorageGRID는 각 스토리지 노드의 스토리지 볼륨 0에 객체 메타데이터를 위한 공간을 예약합니다. 이 경우 예약된 공간을 사용하여 오브젝트 메타데이터를 저장하고 중요한 데이터베이스 작업을 수행합니다. 스토리지 볼륨 0 및 스토리지 노드의 다른 모든 스토리지 볼륨의 나머지 공간은 오브젝트 데이터(복제된 복사본 및 삭제 코딩 단편)에만 사용됩니다.

특정 스토리지 노드에서 오브젝트 메타데이터에 예약된 공간의 양은 아래에 설명된 여러 요인에 따라 달라집니다.

메타데이터 예약 공간 설정입니다

Metadata Reserved Space_는 모든 스토리지 노드의 볼륨 0에 있는 메타데이터에 예약된 공간의 양을 나타내는 시스템 전체 설정입니다. 표에서 볼 수 있듯이 StorageGRID 11.6에 대한 이 설정의 기본값은 다음과 같습니다.

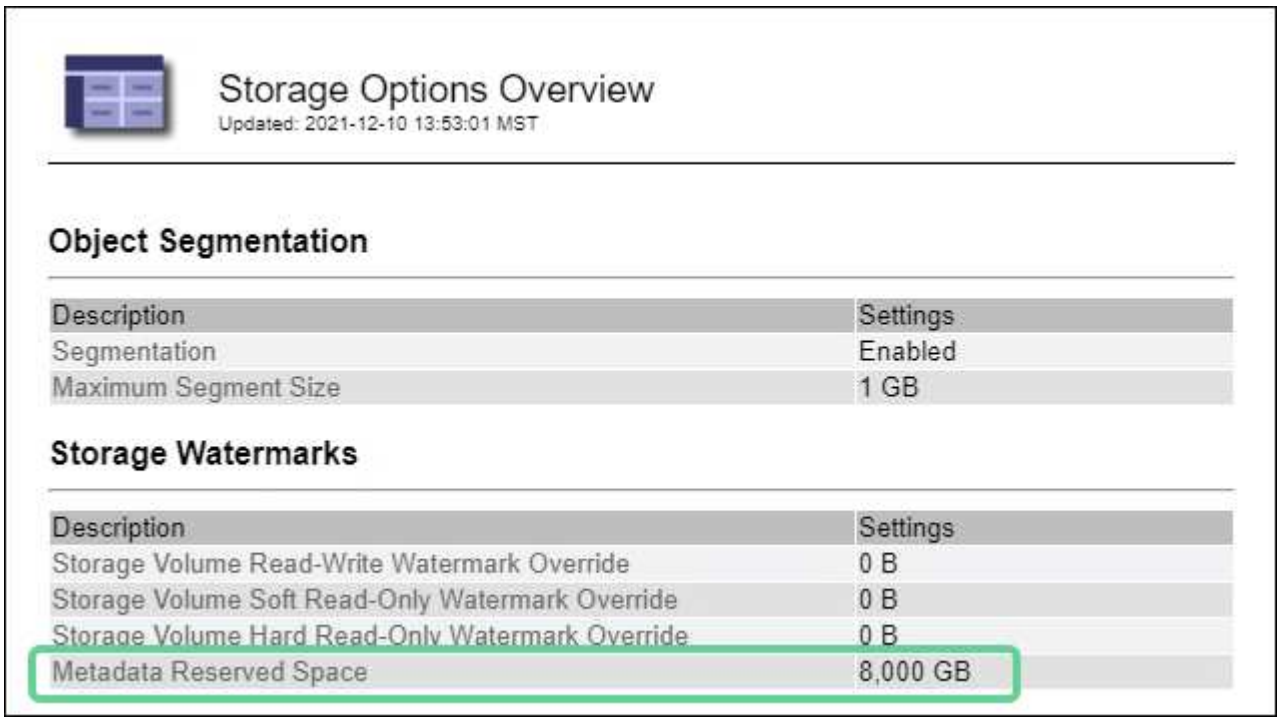
- StorageGRID를 처음 설치할 때 사용한 소프트웨어 버전입니다.

- 각 스토리지 노드의 RAM 용량입니다.

초기 **StorageGRID** 설치에 사용되는 버전입니다	스토리지 노드의 **RAM** 크기입니다	**StorageGRID 11.6**의 기본 메타데이터 예약 공간 설정
11.5 / 11.6	그리드의 각 스토리지 노드에 128GB 이상	8TB(8,000GB)
	그리드의 스토리지 노드에서 128GB 미만	3TB(3,000GB)
11.1 ~ 11.4	한 사이트의 각 스토리지 노드에 128GB 이상	4TB(4,000GB)
	각 사이트의 스토리지 노드에 128GB 미만	3TB(3,000GB)
11.0 이전 버전	금액	2TB(2,000GB)

StorageGRID 시스템에 대한 메타데이터 예약 공간 설정을 보려면

1. 구성 * > * 시스템 * > * 스토리지 옵션 * 을 선택합니다.
2. Storage Watermarks 테이블에서 * Metadata Reserved Space * 를 찾습니다.



스크린샷에서 * Metadata Reserved Space * 값은 8,000GB(8TB)입니다. 각 스토리지 노드에 128GB 이상의 RAM이 있는 새로운 StorageGRID 11.6 설치의 기본 설정입니다.

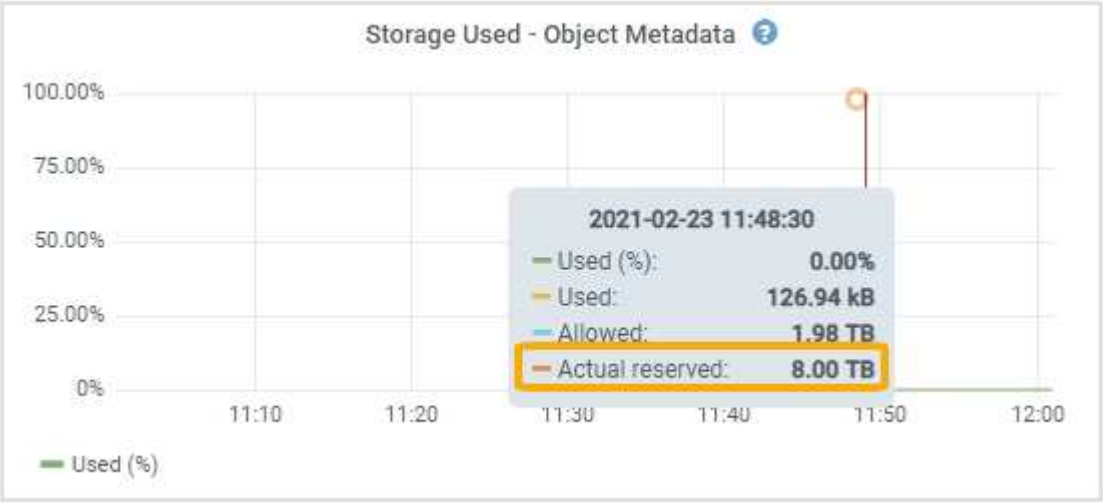
메타데이터의 실제 예약 공간입니다

시스템 전체의 메타데이터 예약 공간 설정과 달리, 객체 메타데이터에 대한 _실제 예약된 공간_은 각 스토리지 노드에 대해 결정됩니다. 특정 스토리지 노드에 대해 메타데이터에 대한 실제 예약된 공간은 노드에 대한 볼륨 0의 크기 및 시스템 전반의 * 메타데이터 예약 공간 * 설정에 따라 달라집니다.

노드에 대한 볼륨 **0**의 크기입니다	메타데이터의 실제 예약 공간입니다
500GB 미만(비운영 용도)	볼륨 0의 10%
500GB 이상	다음 값 중 더 작은 값: • 볼륨 0 • 메타데이터 예약 공간 설정입니다

특정 스토리지 노드의 메타데이터에 대한 실제 예약 공간을 보려면 다음을 따르십시오.

1. Grid Manager에서 * nodes * > **Storage Node* * 를 선택합니다.
2. Storage * 탭을 선택합니다.
3. 커서를 Storage Used — Object Metadata 차트 위에 놓고 * Actual Reserved * 값을 찾습니다.



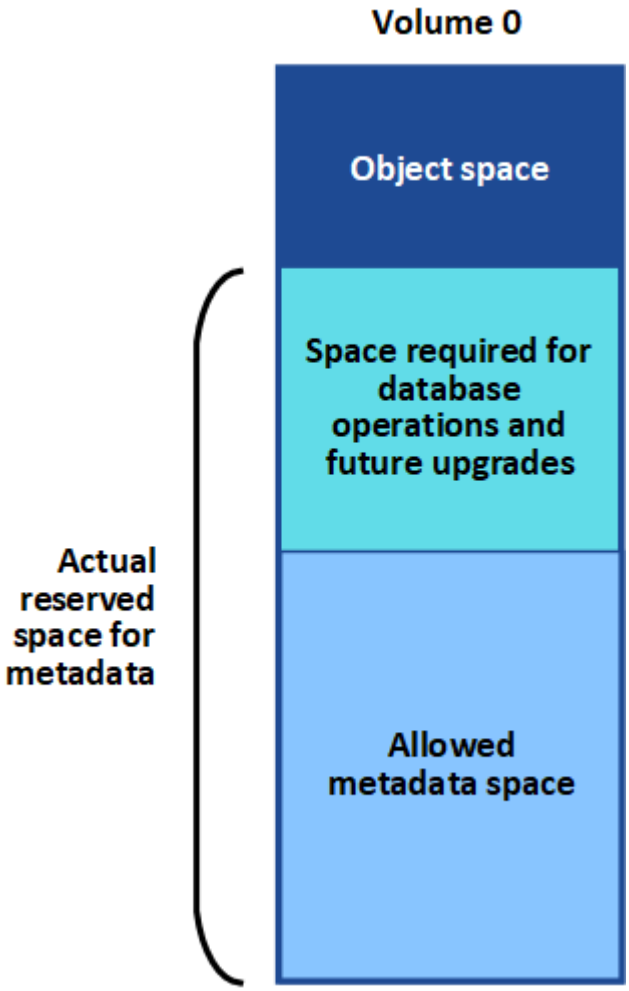
스크린샷에서 * Actual Reserved * 값은 8TB입니다. 이 스크린샷은 새 StorageGRID 11.6 설치의 대용량 스토리지 노드에 대한 것입니다. 시스템 전체의 메타데이터 예약 공간 설정이 이 스토리지 노드의 볼륨 0보다 작기 때문에 이 노드에 대한 실제 예약 공간은 메타데이터 예약 공간 설정과 같습니다.

실제 예약 메타데이터 공간의 예

버전 11.6을 사용하여 새 StorageGRID 시스템을 설치한다고 가정합니다. 이 예에서는 각 스토리지 노드에 128MB 이상의 RAM이 있고 SN1(Storage Node 1)의 볼륨 0이 6TB라고 가정합니다. 다음 값을 기준으로 합니다.

- 시스템 전체 * 메타데이터 예약 공간 * 은 8TB로 설정됩니다. (각 스토리지 노드에 128GB RAM이 넘는 경우 새 StorageGRID 11.6 설치의 기본값입니다.)
- SN1의 메타데이터에 대한 실제 예약 공간은 6TB입니다. (볼륨 0이 * Metadata Reserved Space * 설정보다 작기 때문에 전체 볼륨이 예약됩니다.)

각 스토리지 노드의 실제 메타데이터 예약 공간은 오브젝트 메타데이터(*allowed metadata space*)에 사용할 수 있는 공간과 필수 데이터베이스 작업(예: 컴팩션 및 복구)에 필요한 공간, 향후 하드웨어 및 소프트웨어 업그레이드로 세분화됩니다. 허용되는 메타데이터 공간은 전체 오브젝트 용량을 관리합니다.



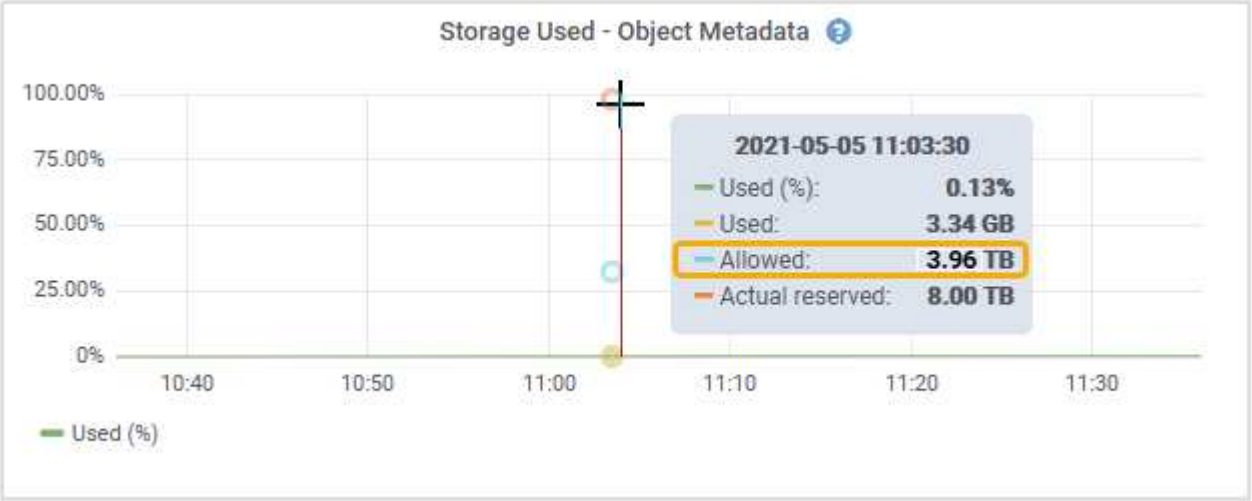
다음 표에서는 StorageGRID가 노드에 대한 메모리 양과 메타데이터에 대한 실제 예약된 공간을 기준으로 서로 다른 스토리지 노드에 대해 * 허용된 메타데이터 공간 * 을 계산하는 방법을 보여 줍니다.

		• 스토리지 노드의 메모리 양 *	
	lt; 128GB	GT; = 128GB	• 메타데이터에 대한 실제 예약 공간 *
< = 4TB	메타데이터를 위해 실제 예약된 공간의 60%, 최대 1.32TB의 공간	메타데이터를 위해 실제 예약된 공간의 60%, 최대 1.98TB	GT; 4TB

스토리지 노드에 대해 허용되는 메타데이터 공간을 보려면 다음을 따르십시오.

1. Grid Manager에서 * nodes * 를 선택합니다.

2. 스토리지 노드를 선택합니다.
3. Storage * 탭을 선택합니다.
4. 커서를 Storage Used — Object Metadata 차트 위에 놓고 * Allowed * 값을 찾습니다.



스크린샷에서 * Allowed * 값은 3.96TB로, 메타데이터에 대한 실제 예약된 공간이 4TB를 초과하는 스토리지 노드의 최대값입니다.

허용 * 값은 다음 Prometheus 메트릭에 해당합니다.

'toragegrid_storage_Utilization_metadata_allowed_bytes'

허용되는 메타데이터 공간의 예

버전 11.6을 사용하여 StorageGRID 시스템을 설치한다고 가정합니다. 이 예에서는 각 스토리지 노드에 128MB 이상의 RAM이 있고 SN1(Storage Node 1)의 볼륨 0이 6TB라고 가정합니다. 다음 값을 기준으로 합니다.

- 시스템 전체 * 메타데이터 예약 공간 * 은 8TB로 설정됩니다. 각 스토리지 노드에 128GB RAM이 넘는 경우 StorageGRID 11.6의 기본값입니다.
- SN1의 메타데이터에 대한 실제 예약 공간은 6TB입니다. (볼륨 0이 * Metadata Reserved Space * 설정보다 작기 때문에 전체 볼륨이 예약됩니다.)
- SN1에서 허용되는 메타데이터 공간은 에 나와 있는 계산에 따라 3TB입니다 메타데이터에 허용되는 공간에 대한 테이블입니다(메타데이터의 실제 예약된 공간 −1TB) × 60%, 최대 3.96TB.

서로 다른 크기의 스토리지 노드가 오브젝트 용량에 미치는 영향

위에서 설명한 것처럼 StorageGRID는 각 사이트의 스토리지 노드에 오브젝트 메타데이터를 균등하게 분산합니다. 따라서 사이트에 크기가 다른 스토리지 노드가 있는 경우 사이트의 가장 작은 노드가 사이트의 메타데이터 용량을 결정합니다.

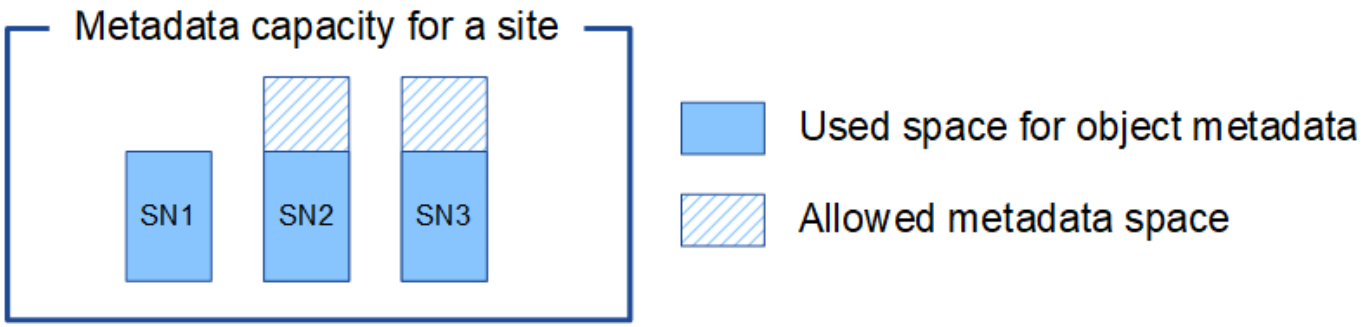
다음 예제를 고려해 보십시오.

- 크기가 다른 세 개의 스토리지 노드가 포함된 단일 사이트 그리드가 있습니다.
- 메타데이터 예약 공간 * 설정은 4TB입니다.

- 스토리지 노드에는 실제 예약된 메타데이터 공간과 허용되는 메타데이터 공간에 대해 다음 값이 있습니다.

스토리지 노드	볼륨 **0**의 크기입니다	실제 예약된 메타데이터 공간입니다	허용된 메타데이터 공간입니다
SN1	2.2TB	2.2TB	1.32TB
Sn2	5TB	4TB	1.98TB
SN3	6TB	4TB	1.98TB

개체 메타데이터는 사이트의 스토리지 노드에 균등하게 분산되므로 이 예제의 각 노드는 1.32TB의 메타데이터만 보유할 수 있습니다. sn2 및 SN3에 대해 허용되는 추가 0.66TB의 메타데이터 공간은 사용할 수 없습니다.



마찬가지로, StorageGRID는 각 사이트에서 StorageGRID 시스템의 모든 개체 메타데이터를 유지하므로 StorageGRID 시스템의 전체 메타데이터 용량은 가장 작은 사이트의 개체 메타데이터 용량에 따라 결정됩니다.

또한 오브젝트 메타데이터 용량은 최대 오브젝트 수를 제어하므로 한 노드에 메타데이터 용량이 부족한 경우 이 그리드는 효과적으로 가득 차게 됩니다.

관련 정보

- 각 스토리지 노드의 객체 메타데이터 용량을 모니터링하는 방법에 대한 자세한 내용은 로 이동하십시오 모니터링하고 문제를 해결합니다.
- 시스템의 오브젝트 메타데이터 용량을 늘리려면 새 스토리지 노드를 추가합니다. 로 이동합니다 그리드를 확장합니다.

저장된 개체에 대한 전역 설정을 구성합니다

저장된 개체 압축을 구성합니다

저장된 개체 압축 그리드 옵션을 사용하여 StorageGRID에 저장된 개체의 크기를 줄여 개체가 더 적은 스토리지를 사용하도록 할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

저장된 개체 그리드 압축 옵션은 기본적으로 비활성화되어 있습니다. 이 옵션을 활성화하면 StorageGRID는 무손실 압축을 사용하여 저장할 때 각 개체의 압축을 시도합니다.

> 이 설정을 변경하면 새 설정을 적용하는 데 약 1분이 걸립니다. 구성된 값이 성능 및 확장을 위해 캐싱됩니다.

이 옵션을 활성화하기 전에 다음 사항에 유의하십시오.

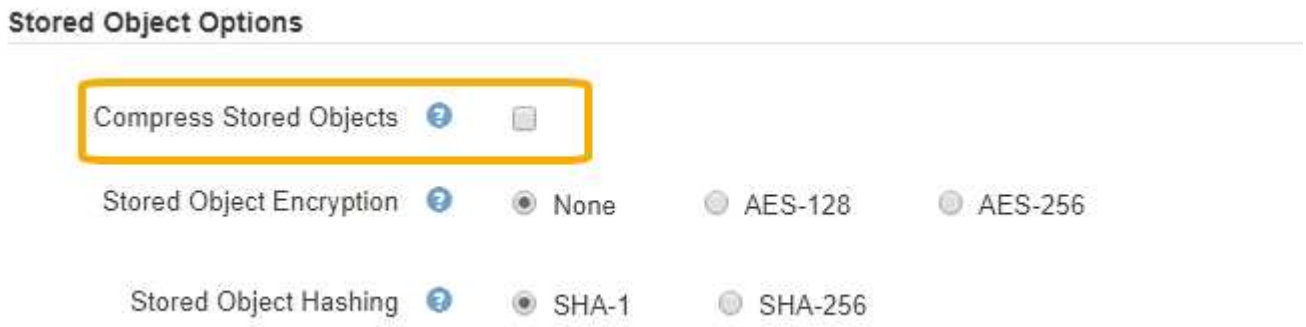
- 저장되는 데이터가 압축 가능한지 여부를 모를 경우 압축을 사용해서는 안 됩니다.
- 개체를 StorageGRID에 저장하는 응용 프로그램은 개체를 저장하기 전에 압축할 수 있습니다. 클라이언트 응용 프로그램에서 개체를 StorageGRID에 저장하기 전에 이미 압축한 경우 저장된 개체 압축을 설정하면 개체의 크기가 더 작아지지 않습니다.
- StorageGRID에서 NetApp FabricPool를 사용하는 경우 압축을 활성화하지 마십시오.
- Compress Stored Objects(저장된 오브젝트 압축) 그리드 옵션이 활성화된 경우 S3 및 Swift 클라이언트 애플리케이션은 바이트 범위를 지정하는 Get Object(오브젝트 가져오기) 작업을 수행하지 않아야 합니다. 이러한 ""범위 읽기"" 작업은 StorageGRID가 요청된 바이트에 액세스하기 위해 개체의 압축을 효과적으로 해제해야 하기 때문에 비효율적입니다. 매우 큰 개체에서 작은 바이트 범위를 요청하는 Get Object 작업은 특히 비효율적입니다. 예를 들어, 50GB의 압축 개체에서 10MB 범위를 읽는 것은 비효율적입니다.

  압축된 개체에서 범위를 읽으면 클라이언트 요청이 시간 초과될 수 있습니다.

  > 개체를 압축해야 하고 클라이언트 응용 프로그램에서 범위 읽기를 사용해야 하는 경우 응용 프로그램의 읽기 시간 초과를 늘리십시오.

단계

1. 구성 * > * 시스템 * > * 그리드 옵션 * 을 선택합니다.
2. 저장 개체 옵션 구역에서 저장된 개체 압축 * 확인란을 선택합니다.



3. 저장 * 을 선택합니다.

저장된 개체 암호화를 구성합니다

개체 저장소가 손상된 경우 읽을 수 있는 형식으로 데이터를 검색할 수 없도록 하려면 저장된 개체를 암호화할 수 있습니다. 기본적으로 객체는 암호화되지 않습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

- 특정 액세스 권한이 있습니다.

이 작업에 대해

저장된 오브젝트 암호화를 사용하면 S3 또는 Swift를 통해 수집되는 모든 오브젝트 데이터를 암호화할 수 있습니다. 이 설정을 활성화하면 새로 수집된 모든 객체가 암호화되지만 기존 저장된 객체는 변경되지 않습니다. 암호화를 사용하지 않도록 설정하면 현재 암호화된 개체는 암호화된 상태로 유지되지만 새로 수집된 개체는 암호화되지 않습니다.

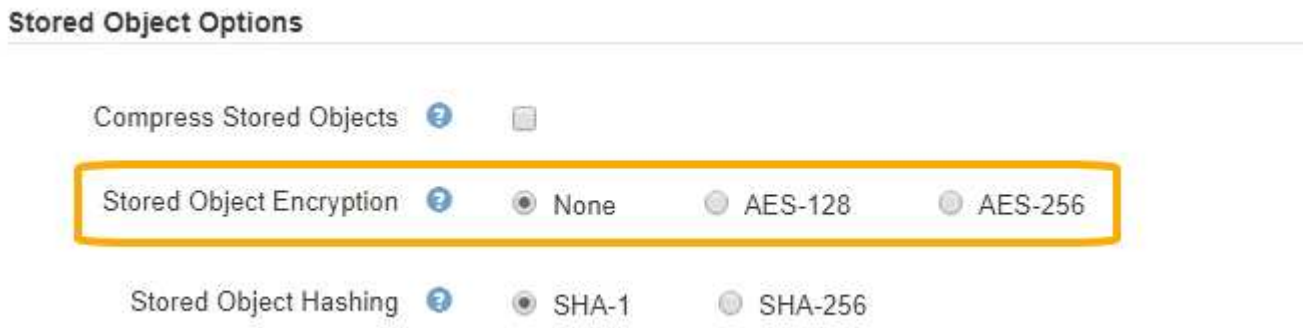
> 이 설정을 변경하면 새 설정을 적용하는 데 약 1분이 걸립니다. 구성된 값이 성능 및 확장을 위해 캐싱됩니다.

저장된 오브젝트는 AES - 128 또는 AES - 256 암호화 알고리즘을 사용하여 암호화할 수 있습니다.

저장된 오브젝트 암호화 설정은 버킷 레벨 또는 오브젝트 레벨 암호화로 암호화되지 않은 S3 오브젝트에만 적용됩니다.

단계

1. 구성 * > * 시스템 * > * 그리드 옵션 * 을 선택합니다.
2. 저장된 개체 옵션 섹션에서 저장된 개체 암호화를 * 없음 * (기본값), * AES-128 * 또는 * AES-256 * 으로 변경합니다.



3. 저장 * 을 선택합니다.

저장된 객체 해싱을 구성합니다

저장된 개체 해싱 옵션은 개체 무결성을 확인하는 데 사용되는 해시 알고리즘을 지정합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

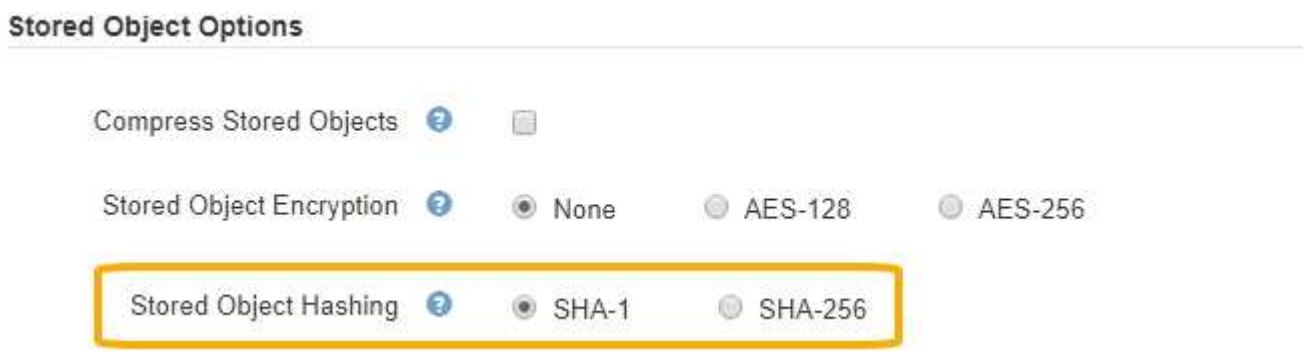
이 작업에 대해

기본적으로 오브젝트 데이터는 SHA-1 알고리즘을 사용하여 해시됩니다. SHA-256 알고리즘에는 추가 CPU 리소스가 필요하며 일반적으로 무결성 검증에 권장되지 않습니다.

> 이 설정을 변경하면 새 설정을 적용하는 데 약 1분이 걸립니다. 구성된 값이 성능 및 확장을 위해 캐싱됩니다.

단계

1. 구성 * > * 시스템 * > * 그리드 옵션 * 을 선택합니다.
2. 저장된 개체 옵션 섹션에서 저장된 개체 해시를 * SHA-1 * (기본값) 또는 * SHA-256 * 로 변경합니다.



3. 저장 * 을 선택합니다.

스토리지 노드 구성 설정입니다

각 스토리지 노드는 여러 가지 구성 설정 및 카운터를 사용합니다. 현재 설정을 보거나 카운터를 재설정하여 알람을 소거해야 할 수 있습니다(기존 시스템).

> 설명서에 구체적으로 명시된 경우를 제외하고 스토리지 노드 구성 설정을 수정하기 전에 기술 지원 부서에 문의해야 합니다. 필요에 따라 이벤트 카운터를 재설정하여 기존 알람을 지울 수 있습니다.

스토리지 노드의 구성 설정 및 카운터에 액세스하려면 다음을 수행합니다.

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. 사이트 _ * > * _ 스토리지 노드 _ * 를 선택합니다.
3. 스토리지 노드를 확장하고 서비스 또는 구성 요소를 선택합니다.
4. Configuration * 탭을 선택합니다.

다음 표에는 스토리지 노드 구성 설정이 요약되어 있습니다.

LDR

속성 이름	코드	설명
HTTP 상태	HSTE	S3, Swift 및 기타 내부 StorageGRID 트래픽에 대한 HTTP 프로토콜의 현재 상태: • 오프라인: 작업이 허용되지 않으며 LDR 서비스에 대한 HTTP 세션을 열려고 하는 모든 클라이언트 응용 프로그램에서 오류 메시지가 표시됩니다. 활성 세션이 정상적으로 닫힙니다. • Online(온라인): 작업이 정상적으로 계속됩니다

속성 이름	코드	설명
HTTP를 자동으로 시작합니다	HTAS	• 이 옵션을 선택하면 재시작 시 시스템 상태는 * LDR * > * 스토리지 * 구성 요소의 상태에 따라 달라집니다. 재시작 시 * LDR * > * 스토리지 * 구성 요소가 읽기 전용인 경우 HTTP 인터페이스도 읽기 전용입니다. LDR * > * 스토리지 * 구성 요소가 온라인인 경우 HTTP도 온라인입니다. 그렇지 않으면 HTTP 인터페이스가 오프라인 상태로 유지됩니다. • 선택되지 않은 경우 HTTP 인터페이스는 명시적으로 활성화될 때까지 오프라인 상태로 유지됩니다.

LDR > 데이터 저장소 를 선택합니다

속성 이름	코드	설명
손실된 개체 수를 재설정합니다	RCOR	이 서비스의 손실된 개체 수에 대한 카운터를 재설정합니다.

LDR > 스토리지

속성 이름	코드	설명
Storage State — 원하는 상태입니다	SSD를 지원합니다	스토리지 구성 요소의 원하는 상태에 대해 사용자가 구성할 수 있는 설정입니다. LDR 서비스는 이 값을 읽고 이 속성에 표시된 상태와 일치시킵니다. 이 값은 다시 시작할 때 영구적으로 유지됩니다. 예를 들어 사용 가능한 저장 공간이 충분한 경우에도 이 설정을 사용하여 저장소를 읽기 전용으로 만들 수 있습니다. 이는 문제 해결에 유용할 수 있습니다. 특성은 다음 값 중 하나를 사용할 수 있습니다. • 오프라인: 원하는 상태가 오프라인이면 LDR 서비스에서 * LDR * > * 스토리지 * 구성 요소를 오프라인으로 전환합니다. • 읽기 전용: 원하는 상태가 읽기 전용인 경우 LDR 서비스는 스토리지 상태를 읽기 전용으로 이동하고 새 콘텐츠 수신을 중지합니다. 열려 있는 세션이 닫힐 때까지 콘텐츠가 잠시 동안 스토리지 노드에 계속 저장될 수 있습니다. • Online(온라인): 일반 시스템 작업 중에 값을 Online(온라인)으로 유지합니다. 스토리지 구성 요소의 스토리지 상태 — 현재 상태는 LDR 서비스의 상태(예: 사용 가능한 오브젝트 스토리지 공간)를 기준으로 서비스에 의해 동적으로 설정됩니다. 공간이 부족하면 구성 요소가 읽기 전용이 됩니다.

속성 이름	코드	설명
상태 점검 시간 초과	SHCT	스토리지 볼륨이 양호한 것으로 간주되려면 상태 점검 테스트를 완료해야 하는 시간 제한(초)입니다. 지원 부서에서 이 값을 변경하도록 지시하는 경우에만 이 값을 변경하십시오.

LDR > 확인 을 누릅니다

속성 이름	코드	설명
누락된 개체 수를 재설정합니다	VCMI	감지된 누락된 개체 수(OMIS)를 재설정합니다. 개체 존재 확인이 완료된 후에만 사용합니다. 누락된 복제 객체 데이터는 StorageGRID 시스템에 의해 자동으로 복구됩니다.
검증 비율	VPRI	백그라운드 검증이 실행되는 속도를 설정합니다. 백그라운드 검증 비율 구성에 대한 자세한 내용은 을 참조하십시오.
손상된 개체 수를 재설정합니다	VCCR	백그라운드 확인 중에 발견된 손상된 복제된 개체 데이터에 대한 카운터를 재설정합니다. 이 옵션은 손상된 물체 감지(OCOR) 알람 조건을 지우는 데 사용할 수 있습니다. 자세한 내용은 StorageGRID 모니터링 및 문제 해결 지침을 참조하십시오.
격리된 개체 삭제	합니다	격리 디렉터리에서 손상된 개체를 삭제하고, 격리된 개체의 수를 0으로 재설정하고, 격리된 개체 감지(OQRT) 경보를 지웁니다. 이 옵션은 손상된 개체가 StorageGRID 시스템에 의해 자동으로 복구된 후에 사용됩니다. 개체 손실 경보가 트리거되면 기술 지원 부서에서 격리된 개체에 액세스하려고 할 수 있습니다. 경우에 따라 격리된 개체는 데이터 복구나 손상된 개체 복사본을 발생시킨 기본 문제를 디버깅하는 데 유용할 수 있습니다.

LDR > 삭제 코딩

속성 이름	코드	설명
쓰기 실패 횟수를 재설정합니다	RSWF	삭제 코딩 오브젝트 데이터의 쓰기 실패에 대한 카운터를 스토리지 노드로 재설정합니다.
재설정 읽기 실패 횟수	SRF	스토리지 노드에서 삭제 코딩 오브젝트 데이터의 읽기 실패에 대한 카운터를 재설정합니다.
재설정 실패 횟수를 삭제합니다	RSDF	스토리지 노드에서 삭제 코딩 오브젝트 데이터의 삭제 실패에 대한 카운터를 재설정합니다.

속성 이름	코드	설명
손상된 복제본 감지 수를 재설정합니다	RSCC	스토리지 노드에서 삭제 코딩 오브젝트 데이터의 손상된 복제본 수에 대한 카운터를 재설정합니다.
손상된 조각 감지됨 카운트 재설정	RSCCD를 참조하십시오	스토리지 노드에서 삭제 코딩 오브젝트 데이터의 손상된 조각에 대한 카운터를 재설정합니다.
누락된 조각 감지 횟수를 재설정합니다	RSMD	스토리지 노드에서 삭제 코딩 오브젝트 데이터의 누락된 조각에 대한 카운터를 재설정합니다. 개체 존재 확인이 완료된 후에만 사용합니다.

LDR > 복제

속성 이름	코드	설명
인바운드 복제 실패 수를 재설정합니다	RICR	인바운드 복제 실패에 대한 카운터를 재설정합니다. RIRF(Inbound Replication - - Failed) 경보를 지우는 데 사용할 수 있습니다.
아웃바운드 복제 실패 수를 재설정합니다	ROCR	아웃바운드 복제 실패에 대한 카운터를 재설정합니다. RORF(아웃바운드 복제 - - 실패) 경보를 지우는 데 사용할 수 있습니다.
인바운드 복제를 비활성화합니다	DSIR	유지 관리 또는 테스트 절차의 일부로 인바운드 복제를 사용하지 않도록 설정하려면 선택합니다. 정상 작동 중에 선택하지 않은 상태로 둡니다. 인바운드 복제를 비활성화하면 StorageGRID 시스템의 다른 위치로 복사하기 위해 스토리지 노드에서 객체를 검색할 수 있지만 다른 위치에서는 이 스토리지 노드에 객체를 복사할 수 없습니다. 즉, LDR 서비스는 읽기 전용입니다.
아웃바운드 복제를 비활성화합니다	DSOR	유지 관리 또는 테스트 절차의 일부로 아웃바운드 복제(HTTP 검색을 위한 콘텐츠 요청 포함)를 사용하지 않도록 설정하려면 선택합니다. 정상 작동 중에 선택하지 않은 상태로 둡니다. 아웃바운드 복제를 사용하지 않도록 설정하면 객체를 이 스토리지 노드에 복제할 수 있지만 StorageGRID 시스템의 다른 위치로 복제할 스토리지 노드에서 객체를 검색할 수는 없습니다. LDR 서비스는 쓰기 전용입니다.

관련 정보

모니터링하고 문제를 해결합니다

전체 스토리지 노드 관리

스토리지 노드가 용량에 도달하면 새 스토리지를 추가하여 StorageGRID 시스템을 확장해야 합니다. 스토리지 볼륨 추가, 스토리지 확장 쉘프 추가, 스토리지 노드 추가의 세 가지 옵션을 사용할 수 있습니다.

스토리지 볼륨을 추가합니다

각 스토리지 노드는 최대 개수의 스토리지 볼륨을 지원합니다. 정의된 최대값은 플랫폼에 따라 다릅니다. 스토리지 노드에 최대 스토리지 볼륨 수보다 적은 수의 볼륨이 포함된 경우 볼륨을 추가하여 용량을 늘릴 수 있습니다. 의 지침을 참조하십시오 StorageGRID 시스템 확장.

스토리지 확장 쉘프를 추가합니다

SG6060과 같은 일부 StorageGRID 어플라이언스 스토리지 노드는 추가 스토리지 쉘프를 지원할 수 있습니다. 최대 용량으로 아직 확장되지 않은 확장 기능을 갖춘 StorageGRID 어플라이언스를 사용하는 경우 스토리지 쉘프를 추가하여 용량을 늘릴 수 있습니다. 의 지침을 참조하십시오 StorageGRID 시스템 확장.

스토리지 노드 추가

스토리지 노드를 추가하여 스토리지 용량을 늘릴 수 있습니다. 스토리지를 추가할 때 현재 활성 상태인 ILM 규칙 및 용량 요구 사항을 신중하게 고려해야 합니다. 의 지침을 참조하십시오 StorageGRID 시스템 확장.

관리 노드 관리

관리 노드의 정의

관리 노드는 시스템 구성, 모니터링 및 로깅과 같은 관리 서비스를 제공합니다. 각 그리드에는 1개의 기본 관리 노드가 있어야 하며 이중화를 위해 여러 개의 비기본 관리 노드가 있을 수 있습니다.

그리드 관리자 또는 테넌트 관리자에 로그인할 때 관리 노드에 연결됩니다. 모든 관리 노드에 연결할 수 있으며 각 관리 노드에는 StorageGRID 시스템의 유사한 보기가 표시됩니다. 그러나 기본 관리 노드를 사용하여 유지 관리 절차를 수행해야 합니다.

관리 노드를 사용하여 S3 및 Swift 클라이언트 트래픽의 로드 밸런싱을 수행할 수도 있습니다.

관리 노드는 다음 서비스를 호스팅합니다.

- AMS 서비스
- CMN 서비스
- NMS 서비스
- Prometheus 서비스
- 로드 밸런서 및 고가용성 서비스(S3 및 Swift 클라이언트 트래픽 지원)

관리 노드는 그리드 관리 API 및 테넌트 관리 API의 요청을 처리하는 관리 애플리케이션 프로그램 인터페이스(mgmt-API)도 지원합니다. 을 참조하십시오 Grid Management API를 사용합니다.

AMS 서비스의 정의

AMS(Audit Management System) 서비스는 시스템 활동 및 이벤트를 추적합니다.

CMN 서비스의 정의

CMN(Configuration Management Node) 서비스는 모든 서비스에 필요한 시스템 전반의 연결 및 프로토콜 기능을 관리합니다. 또한 CMN 서비스는 그리드 작업을 실행하고 모니터링하는 데 사용됩니다. StorageGRID 배포당 하나의 CMN 서비스만 있습니다. CMN 서비스를 호스팅하는 관리 노드를 기본 관리 노드라고 합니다.

NMS 서비스의 정의

NMS(네트워크 관리 시스템) 서비스는 StorageGRID 시스템의 브라우저 기반 인터페이스인 그리드 관리자를 통해 표시되는 모니터링, 보고 및 구성 옵션을 강화합니다.

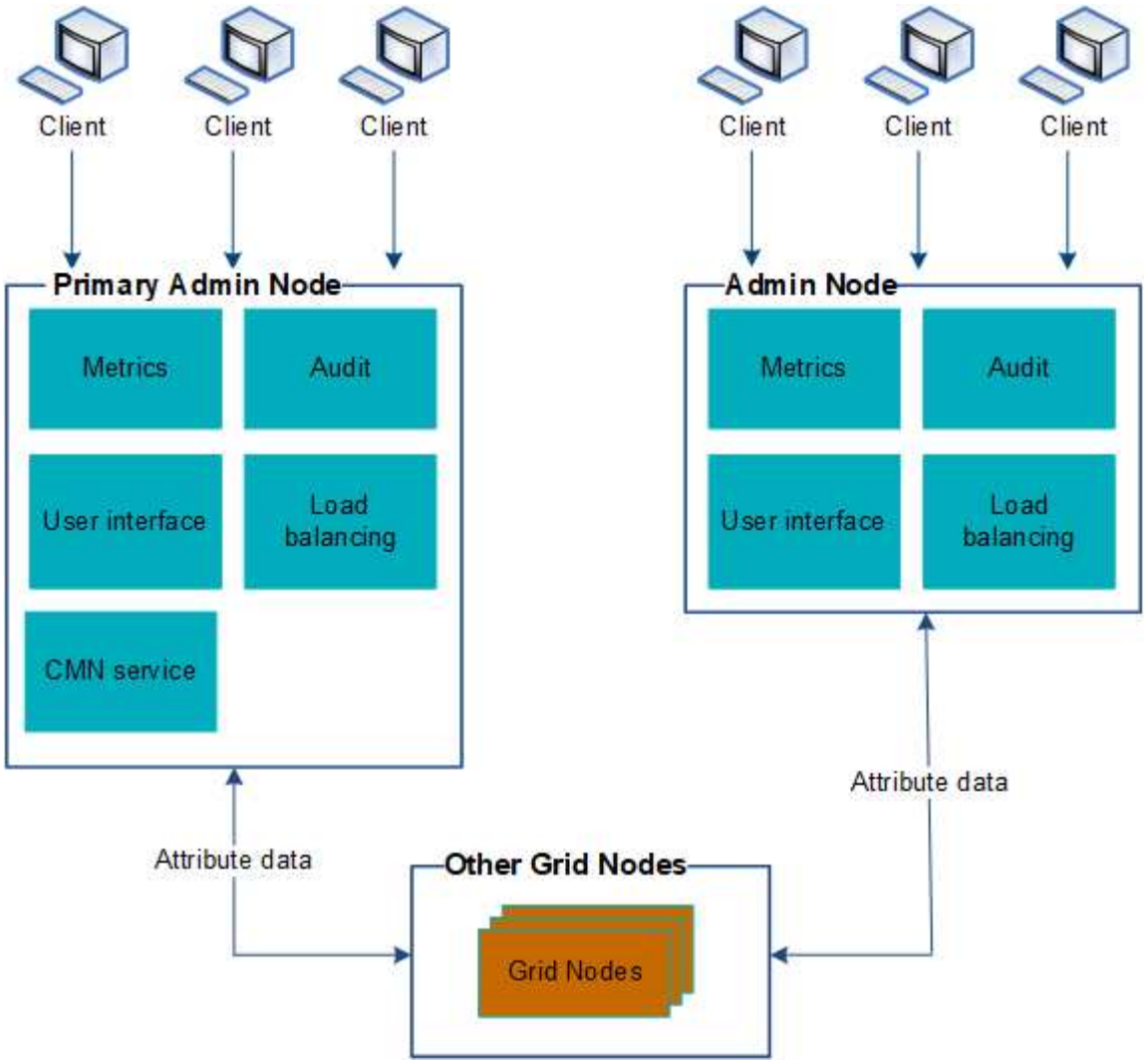
Prometheus 서비스의 정의

Prometheus 서비스는 모든 노드의 서비스에서 시계열 메트릭을 수집합니다.

여러 관리자 노드 사용

StorageGRID 시스템에는 여러 관리 노드가 포함되어 있어 하나의 관리 노드에 장애가 발생하더라도 StorageGRID 시스템을 지속적으로 모니터링하고 구성할 수 있습니다.

관리 노드를 사용할 수 없게 되면 속성 처리가 계속되고 경고 및 경보(레거시 시스템)가 계속 트리거되며 이메일 알림 및 AutoSupport 메시지가 계속 전송됩니다. 그러나 여러 개의 관리 노드가 있으면 알림 및 AutoSupport 메시지를 제외한 페일오버 보호가 제공되지 않습니다. 특히 한 관리 노드에서 발생한 알람 확인응답을 다른 관리 노드로 복사하지 않습니다.



관리 노드에 장애가 발생할 경우 StorageGRID 시스템을 계속 보고 구성할 수 있는 두 가지 옵션이 있습니다.

- 웹 클라이언트는 사용 가능한 다른 관리 노드에 다시 연결할 수 있습니다.
- 시스템 관리자가 고가용성 관리 노드 그룹을 구성한 경우 웹 클라이언트는 HA 그룹의 가상 IP 주소를 사용하여 그리드 관리자 또는 테넌트 관리자에 계속 액세스할 수 있습니다. 을 참조하십시오 고가용성 그룹을 관리합니다.

> HA 그룹을 사용하는 경우 마스터 관리자 노드에 장애가 발생하면 액세스가 중단됩니다. 사용자는 HA 그룹의 가상 IP 주소가 그룹의 다른 관리 노드로 페일오버된 후 다시 로그인해야 합니다.

일부 유지 보수 작업은 기본 관리 노드를 통해서만 수행할 수 있습니다. 기본 관리 노드에 장애가 발생할 경우 StorageGRID 시스템이 다시 정상적으로 작동하기 전에 해당 노드를 복구해야 합니다.

기본 관리 노드를 식별합니다

기본 관리 노드는 CMN 서비스를 호스팅합니다. 일부 유지 관리 절차는 기본 관리 노드를 사용해서만 수행할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

- 특정 액세스 권한이 있습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. site_ * > * Admin Node * 를 선택한 후 를 선택합니다 ➕ 토폴로지 트리를 확장하고 이 관리 노드에서 호스팅되는 서비스를 표시합니다.

   기본 관리 노드는 CMN 서비스를 호스팅합니다.

3. 이 관리 노드가 CMN 서비스를 호스팅하지 않는 경우 다른 관리 노드를 확인합니다.

선호하는 송신자를 선택합니다

StorageGRID 배포에 여러 관리 노드가 포함된 경우 알림을 보내는 기본 설정 관리자 노드를 선택할 수 있습니다. 기본적으로 기본 관리 노드가 선택되지만 모든 관리 노드가 기본 설정 송신자가 될 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

구성 * > * 시스템 * > * 디스플레이 옵션 * 페이지에는 현재 기본 설정 발신인으로 선택된 관리 노드가 표시됩니다. 기본 관리 노드는 기본적으로 선택됩니다.

정상적인 시스템 작업에서 기본 설정 보낸 사람만이 다음 알림을 보냅니다.

- AutoSupport 메시지
- SNMP 알림
- 경고 이메일
- 알람 이메일(기존 시스템)

그러나 다른 모든 관리 노드(대기 보낸 사람)는 기본 설정 보낸 사람을 모니터링합니다. 문제가 감지되면 대기 보낸 사람이 이러한 알림을 보낼 수도 있습니다.

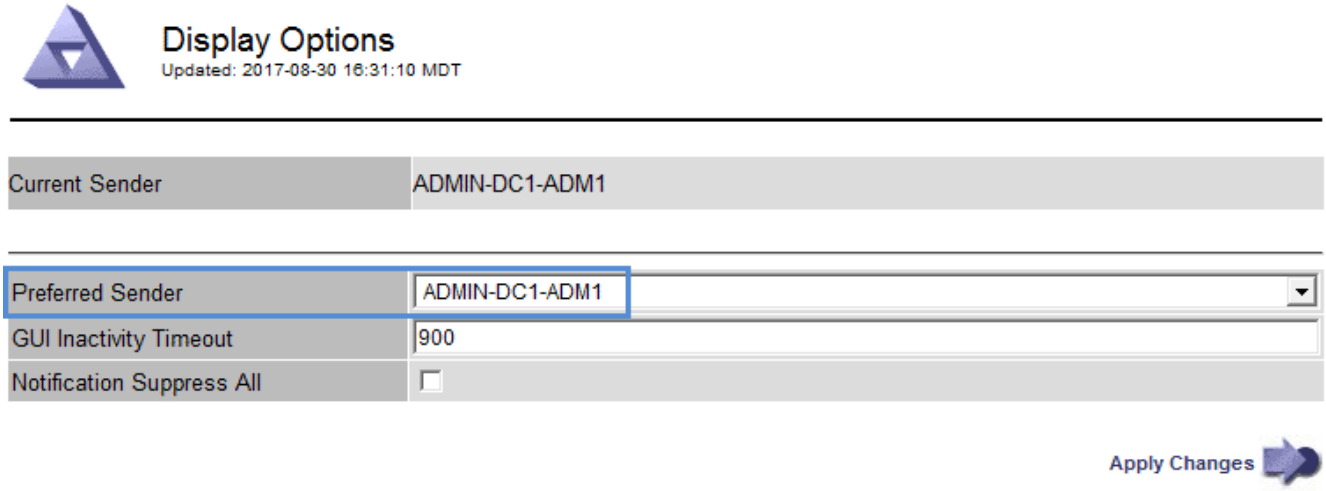
다음과 같은 경우 기본 발신자와 대기 발신자는 모두 알림을 보낼 수 있습니다.

- 관리 노드가 서로 "isfand"가 되면 기본 발신자와 대기 보낸 사람 모두 알림 전송을 시도하며 여러 개의 알림 복사본이 수신될 수 있습니다.
- 대기 보낸 사람이 기본 설정 보낸 사람과 관련된 문제를 감지하고 알림을 보내기 시작하면 기본 설정 보낸 사람이 알림을 다시 보낼 수 있습니다. 이 경우 중복 알림이 전송될 수 있습니다. 대기 보낸 사람이 더 이상 기본 설정 보낸 사람의 오류를 감지하지 않으면 알림 전송을 중지합니다.

> 알람 알림 및 AutoSupport 메시지를 테스트할 때 모든 관리 노드가 테스트 이메일을 보냅니다. 알림 알림을 테스트할 때는 모든 관리 노드에 로그인하여 연결을 확인해야 합니다.

단계

1. 구성 * > * 시스템 * > * 디스플레이 옵션 * 을 선택합니다.
2. 표시 옵션 메뉴에서 * 옵션 * 을 선택합니다.
3. 드롭다운 목록에서 기본 설정 발신자로 설정할 관리 노드를 선택합니다.



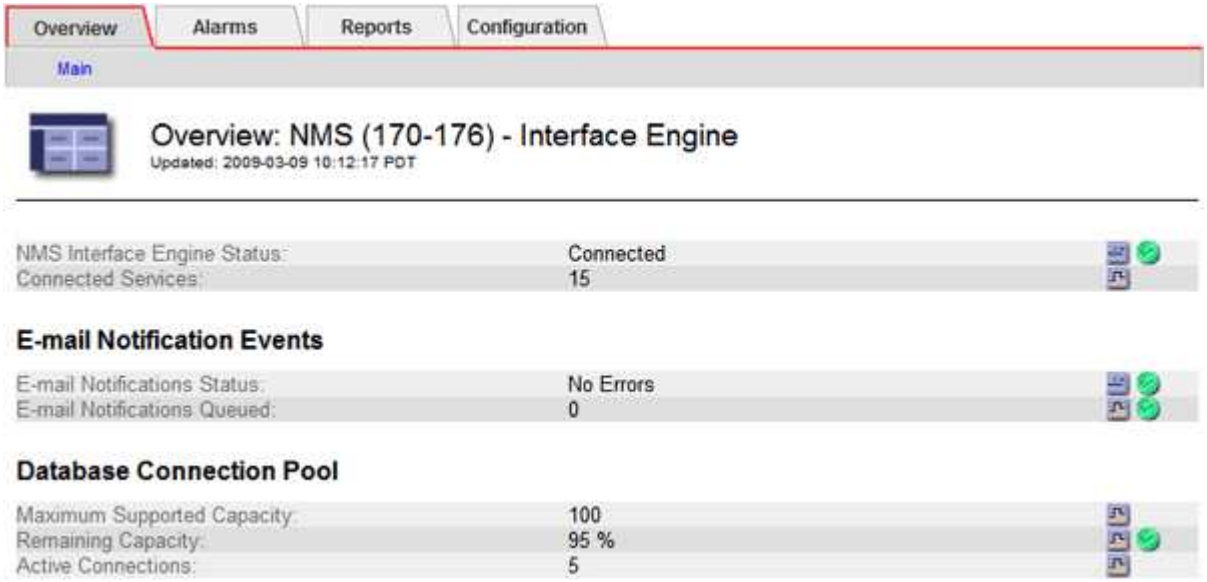
4. Apply Changes * 를 선택합니다.

   관리 노드는 알림의 기본 보낸 사람으로 설정됩니다.

알림 상태 및 대기열을 봅니다

관리 노드의 NMS(네트워크 관리 시스템) 서비스는 메일 서버에 알림을 보냅니다. 인터페이스 엔진 페이지에서 NMS 서비스의 현재 상태와 해당 알림 대기열의 크기를 볼 수 있습니다.

인터페이스 엔진 페이지에 액세스하려면 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 마지막으로 **site* * > **Admin Node* * > * NMS * > * Interface Engine * 을 선택합니다.



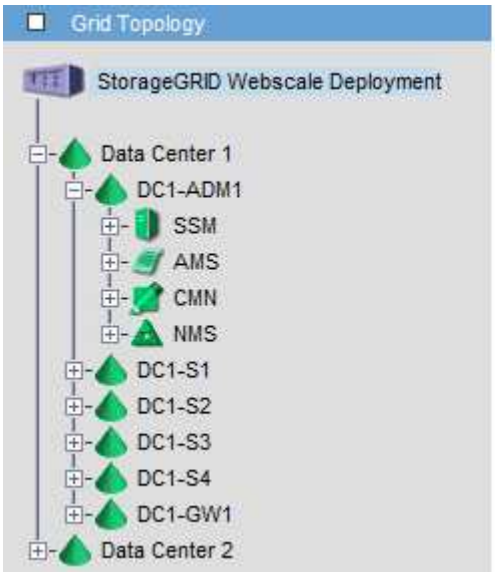
알림은 이메일 알림 대기열을 통해 처리되며, 트리거된 순서대로 하나씩 메일 서버로 전송됩니다. 네트워크 연결 오류 등의 문제가 있고 메일 서버를 사용할 수 없는 경우 알림 전송을 시도할 때 메일 서버에 알림을 다시 보내려는 최선의 노력을 60초 동안 계속합니다. 60초 후에 메일 서버로 알림이 전송되지 않으면 알림 대기열에서 알림이 삭제되어

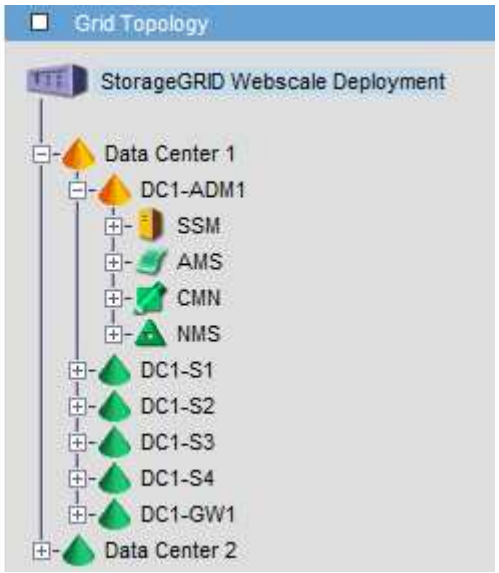
대기열의 다음 알림을 보내려고 시도합니다. 알림을 보내지 않고 알림 대기열에서 놓을 수 있으므로 알림을 보내지 않고 경보를 트리거할 수 있습니다. 알림이 전송되지 않고 대기열에서 삭제된 경우 Minor(분)(이메일 알림 상태) 경보가 트리거됩니다.

관리자 노드가 확인된 경보를 표시하는 방법(레거시 시스템)

한 관리 노드에서 알람을 확인하면 확인된 알람이 다른 관리 노드에 복사되지 않습니다. 승인 내용이 다른 관리 노드에 복사되지 않기 때문에 그리드 토폴로지 트리가 각 관리 노드에 대해 동일하게 보이지 않을 수 있습니다.

이 차이는 웹 클라이언트를 연결할 때 유용할 수 있습니다. 웹 클라이언트는 관리자 요구에 따라 StorageGRID 시스템에 대한 다양한 보기를 가질 수 있습니다.





알림은 확인이 발생하는 관리 노드에서 전송됩니다.

감사 클라이언트 액세스를 구성합니다

AMS(감사 관리 시스템) 서비스를 통해 관리 노드는 감사 공유를 통해 사용 가능한 로그 파일에 모든 감사 시스템 이벤트를 기록하며, 이 로그 파일은 설치 시 각 관리 노드에 추가됩니다. 감사 로그에 쉽게 액세스할 수 있도록 CIFS 및 NFS 모두에 대한 감사 공유에 대한 클라이언트 액세스를 구성할 수 있습니다.

StorageGRID 시스템은 감사 메시지를 로그 파일에 쓰기 전에 손실을 방지하기 위해 긍정 승인을 사용합니다. AMS 서비스 또는 중간 감사 릴레이 서비스가 해당 제어 권한을 확인할 때까지 메시지는 서비스 대기 상태로 유지됩니다.

자세한 내용은 을 참조하십시오 감사 로그를 검토합니다.

> CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다. CIFS 또는 NFS를 사용할 수 있는 옵션이 있으면 NFS를 선택합니다.

CIFS에 대한 감사 클라이언트를 구성합니다

감사 클라이언트를 구성하는 절차는 Windows Workgroup 또는 Windows AD(Active

Directory)의 인증 방법에 따라 다릅니다. 추가된 감사 공유는 읽기 전용 공유로 자동 설정됩니다.

> CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

Workgroup에 대한 감사 클라이언트를 구성합니다

감사 메시지를 검색할 StorageGRID 배포의 각 관리자 노드에 대해 이 절차를 수행합니다.

필요한 것

- 루트/관리자 계정 암호(해당 패키지에서 사용 가능)가 있는 "passwords.txt" 파일이 있습니다.
- "Configuration.txt" 파일이 있습니다(해당 패키지에서 사용 가능).

이 작업에 대해

CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
2. 모든 서비스가 실행 중 또는 확인됨: 'toragegrid-status' 상태인지 확인합니다

   모든 서비스가 실행 중이거나 확인되지 않은 경우 계속하기 전에 문제를 해결하십시오.
3. 명령줄로 돌아가 * Ctrl * + * C * 를 누릅니다.
4. CIFS 구성 유틸리티 'config_cifs.rb'를 시작합니다

```
----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
----------------------------------------------------------------------
```

5. Windows Workgroup에 대한 인증을 설정합니다.

   인증이 이미 설정된 경우 권고 메시지가 나타납니다. 인증이 이미 설정된 경우 다음 단계로 이동합니다.

   a. Set-authentication을 입력한다
   b. Windows Workgroup 또는 Active Directory 설치를 묻는 메시지가 나타나면 워크그룹 을 입력합니다
   c. 메시지가 나타나면 워크그룹 이름('*workgroup_name*')을 입력합니다
   d. 메시지가 나타나면 의미 있는 NetBIOS 이름('*netbios_name*')을 만듭니다

      또는

      관리자 노드의 호스트 이름을 NetBIOS 이름으로 사용하려면 * Enter * 를 누릅니다.

   이 스크립트는 Samba 서버를 다시 시작하고 변경 사항이 적용됩니다. 이 작업은 1분 이내에 수행해야 합니다. 인증을 설정한 후 감사 클라이언트를 추가합니다.

   a. 메시지가 표시되면 * Enter * 를 누릅니다.

      CIFS 구성 유틸리티가 표시됩니다.

6. 감사 클라이언트 추가:

   a. add-audit-share를 입력합니다

      > 공유는 자동으로 읽기 전용으로 추가됩니다.

   b. 메시지가 나타나면 사용자 또는 그룹('*user*')을 추가합니다
   c. 메시지가 나타나면 감사 사용자 이름('*audit_user_name*')을 입력합니다
   d. 메시지가 나타나면 감사 사용자의 암호를 입력합니다: '*password*'
   e. 메시지가 나타나면 같은 암호를 다시 입력하여 확인합니다. '*password*'
   f. 메시지가 표시되면 * Enter * 를 누릅니다.

      CIFS 구성 유틸리티가 표시됩니다.

      > 디렉토리를 입력할 필요가 없습니다. 감사 디렉토리 이름이 미리 정의되어 있습니다.

7. 둘 이상의 사용자 또는 그룹이 감사 공유에 액세스할 수 있는 경우 추가 사용자를 추가합니다.

   a. Add-user-to-share를 입력합니다

      활성화된 공유의 번호 매기기 목록이 표시됩니다.

   b. 메시지가 나타나면 감사 내보내기 공유 번호('*share_number*')를 입력합니다
   c. 메시지가 나타나면 사용자 또는 그룹 'user'를 추가합니다

      또는 '그룹'을 선택합니다

   d. 메시지가 나타나면 감사 사용자 또는 그룹의 이름('*audit_user or audit_group*')을 입력합니다

e. 메시지가 표시되면 * Enter * 를 누릅니다.

   CIFS 구성 유틸리티가 표시됩니다.

f. 감사 공유에 대한 액세스 권한이 있는 추가 사용자 또는 그룹에 대해 이러한 하위 단계를 반복합니다.

8. 필요에 따라 'validate-config' 구성을 확인합니다

   서비스가 확인 및 표시됩니다. 다음 메시지는 무시해도 됩니다.

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

   a. 메시지가 표시되면 * Enter * 를 누릅니다.

      감사 클라이언트 구성이 표시됩니다.

   b. 메시지가 표시되면 * Enter * 를 누릅니다.

      CIFS 구성 유틸리티가 표시됩니다.

9. CIFS 구성 유틸리티 'exit'를 닫습니다
10. 삼바 서비스를 시작한다: 'service smbd start'
11. StorageGRID 배포가 단일 사이트인 경우 다음 단계로 이동합니다.

    또는

    필요한 경우 StorageGRID 배포에 다른 사이트의 관리자 노드가 포함된 경우 필요에 따라 다음 감사 공유를 활성화합니다.

    a. 사이트의 관리 노드에 원격으로 로그인:
       i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
       ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
       iii. 루트로 전환하려면 다음 명령을 입력합니다
       iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.
    b. 각 추가 관리 노드에 대한 감사 공유를 구성하려면 단계를 반복합니다.
    c. 원격 관리 노드에 대한 원격 보안 셸 로그인을 'exit'로 닫습니다
12. 명령 셸에서 'exit'를 로그아웃합니다

Active Directory에 대한 감사 클라이언트를 구성합니다

감사 메시지를 검색할 StorageGRID 배포의 각 관리자 노드에 대해 이 절차를 수행합니다.

필요한 것

- 루트/관리자 계정 암호(해당 패키지에서 사용 가능)가 있는 "passwords.txt" 파일이 있습니다.
- CIFS Active Directory 사용자 이름과 암호가 있습니다.
- "Configuration.txt" 파일이 있습니다(해당 패키지에서 사용 가능).

> CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
2. 모든 서비스가 실행 중 또는 확인됨: 'toragegrid-status' 상태인지 확인합니다

   모든 서비스가 실행 중이거나 확인되지 않은 경우 계속하기 전에 문제를 해결하십시오.
3. 명령줄로 돌아가 * Ctrl * + * C * 를 누릅니다.
4. CIFS 구성 유틸리티 'config_cifs.rb'를 시작합니다

```
----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
----------------------------------------------------------------------
```

5. Active Directory에 대한 인증을 'Set-authentication'으로 설정합니다

   대부분의 배포에서는 감사 클라이언트를 추가하기 전에 인증을 설정해야 합니다. 인증이 이미 설정된 경우 권고 메시지가 나타납니다. 인증이 이미 설정된 경우 다음 단계로 이동합니다.

   a. Workgroup 또는 Active Directory 설치를 묻는 메시지가 나타나면 "ad"를 선택합니다
   b. 메시지가 표시되면 AD 도메인 이름(짧은 도메인 이름)을 입력합니다.

c. 메시지가 표시되면 도메인 컨트롤러의 IP 주소 또는 DNS 호스트 이름을 입력합니다.

d. 메시지가 표시되면 전체 도메인 영역 이름을 입력합니다.

   대문자를 사용합니다.

e. winbind 지원을 활성화하라는 메시지가 나타나면 * y * 를 입력합니다.

   Winbind는 AD 서버에서 사용자 및 그룹 정보를 확인하는 데 사용됩니다.

f. 메시지가 표시되면 NetBIOS 이름을 입력합니다.

g. 메시지가 표시되면 * Enter * 를 누릅니다.

   CIFS 구성 유틸리티가 표시됩니다.

6. 도메인 가입:

   a. 아직 시작되지 않은 경우 CIFS 구성 유틸리티 'config_cifs.rb'를 시작합니다

   b. 도메인에 가입하세요

   c. 관리자 노드가 현재 도메인의 유효한 구성원인지 테스트하라는 메시지가 표시됩니다. 이 관리 노드가 이전에 도메인에 가입하지 않은 경우 '아니요'를 입력합니다

   d. 메시지가 표시되면 관리자 사용자 이름('*administrator_username*')을 입력합니다

      여기서 '*administrator_username*'은 StorageGRID 사용자 이름이 아닌 CIFS Active Directory 사용자 이름입니다.

   e. 메시지가 표시되면 관리자 암호(_ administrator_password_)를 입력합니다

      파일 '*administrator_password*'는 StorageGRID 암호가 아닌 CIFS Active Directory 사용자 이름입니다.

   f. 메시지가 표시되면 * Enter * 를 누릅니다.

      CIFS 구성 유틸리티가 표시됩니다.

7. 도메인에 올바르게 가입했는지 확인합니다.

   a. 도메인에 가입하세요

   b. 서버가 현재 도메인의 유효한 구성원인지 테스트하라는 메시지가 나타나면 y를 입력합니다

      "Join is OK"라는 메시지가 표시되면 도메인에 성공적으로 참가한 것입니다. 이 응답이 없으면 인증을 설정하고 도메인에 다시 가입해 보십시오.

   c. 메시지가 표시되면 * Enter * 를 누릅니다.

      CIFS 구성 유틸리티가 표시됩니다.

8. Add-audit-share 감사 클라이언트를 추가한다

   a. 사용자 또는 그룹을 추가하라는 메시지가 나타나면 'user'를 입력합니다

   b. 감사 사용자 이름을 입력하라는 메시지가 나타나면 감사 사용자 이름을 입력합니다.

   c. 메시지가 표시되면 * Enter * 를 누릅니다.

CIFS 구성 유틸리티가 표시됩니다.

9. 하나 이상의 사용자 또는 그룹이 감사 공유에 액세스할 수 있는 경우 'add-user-to-share'라는 사용자를 추가합니다

   활성화된 공유의 번호 매기기 목록이 표시됩니다.

   a. 감사 내보내기 공유의 번호를 입력합니다.
   b. 사용자 또는 그룹을 추가하라는 메시지가 나타나면 '그룹'을 입력합니다

      감사 그룹 이름을 묻는 메시지가 표시됩니다.

   c. 감사 그룹 이름을 묻는 메시지가 표시되면 감사 사용자 그룹의 이름을 입력합니다.
   d. 메시지가 표시되면 * Enter * 를 누릅니다.

      CIFS 구성 유틸리티가 표시됩니다.

   e. 감사 공유에 액세스할 수 있는 추가 사용자 또는 그룹에 대해 이 단계를 반복합니다.
10. 필요에 따라 'validate-config' 구성을 확인합니다

    서비스가 확인 및 표시됩니다. 다음 메시지는 무시해도 됩니다.

    - Include 파일 '/etc/samba/include/cifs-interfaces.inc` 찾을 수 없습니다
    - Include 파일 '/etc/samba/include/cifs-filesystem.inc` 찾을 수 없습니다
    - Include 파일 '/etc/samba/include/cifs-interfaces.inc` 찾을 수 없습니다
    - Include 파일 '/etc/samba/include/cifs-custom-config.inc` 찾을 수 없습니다
    - Include 파일 '/etc/samba/include/cifs-shares.inc` 찾을 수 없습니다
    - rlimit_max: rlimit_max(1024)를 최소 윈도우 한계(16384)로 증가

    > '보안 = 광고' 설정을 '암호 서버' 매개변수와 결합하지 마십시오. (기본적으로 Samba는 자동으로 연락할 올바른 DC를 검색합니다.)

    i. 메시지가 표시되면 * Enter * 를 눌러 감사 클라이언트 구성을 표시합니다.
    ii. 메시지가 표시되면 * Enter * 를 누릅니다.

       CIFS 구성 유틸리티가 표시됩니다.

11. CIFS 구성 유틸리티 'exit'를 닫습니다
12. StorageGRID 배포가 단일 사이트인 경우 다음 단계로 이동합니다.

    또는

    필요에 따라 StorageGRID 구축에 다른 사이트의 관리 노드가 포함되는 경우 필요에 따라 다음 감사 공유를 활성화합니다.

    a. 사이트의 관리 노드에 원격으로 로그인:

       i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.

iii. 루트로 전환하려면 다음 명령을 입력합니다

iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

b. 각 관리 노드에 대한 감사 공유를 구성하려면 다음 단계를 반복합니다.

c. 관리자 노드에 대한 원격 보안 셸 로그인 'exit'를 닫습니다

13. 명령 셸에서 'exit'를 로그아웃합니다

CIFS 감사 공유에 사용자 또는 그룹을 추가합니다

AD 인증과 통합된 CIFS 감사 공유에 사용자 또는 그룹을 추가할 수 있습니다.

필요한 것

- 루트/관리자 계정 암호(해당 패키지에서 사용 가능)가 있는 "passwords.txt" 파일이 있습니다.
- "Configuration.txt" 파일이 있습니다(해당 패키지에서 사용 가능).

이 작업에 대해

다음 절차는 AD 인증과 통합된 감사 공유에 대한 것입니다.

> CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

단계

1. 기본 관리자 노드에 로그인합니다.

   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 모든 서비스의 상태가 실행 중 또는 확인인지 확인합니다. 'toragegrid-status'를 입력합니다

   모든 서비스가 실행 중이거나 확인되지 않은 경우 계속하기 전에 문제를 해결하십시오.

3. 명령줄로 돌아가 * Ctrl * + * C * 를 누릅니다.

4. CIFS 구성 유틸리티 'config_cifs.rb'를 시작합니다

```
-----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-----------------------------------------------------------------------
```

5. 사용자 또는 그룹 추가:'add-user-to-share'를 시작합니다

   구성된 감사 공유의 번호가 매겨진 목록이 표시됩니다.

6. 메시지가 표시되면 감사 공유(감사-내보내기) 번호('*audit_share_number*')를 입력합니다

   사용자 또는 그룹에 이 감사 공유에 대한 액세스 권한을 부여할지 묻는 메시지가 표시됩니다.

7. 메시지가 나타나면 사용자 또는 그룹(사용자 또는 그룹)을 추가합니다
8. 이 AD 감사 공유에 대한 사용자 또는 그룹 이름을 묻는 메시지가 나타나면 이름을 입력합니다.

   사용자 또는 그룹은 서버의 운영 체제와 CIFS 서비스 모두에서 감사 공유에 대해 읽기 전용으로 추가됩니다. 사용자 또는 그룹이 감사 클라이언트 공유에 액세스할 수 있도록 Samba 구성이 다시 로드됩니다.

9. 메시지가 표시되면 * Enter * 를 누릅니다.

   CIFS 구성 유틸리티가 표시됩니다.

10. 감사 공유에 액세스할 수 있는 각 사용자 또는 그룹에 대해 이 단계를 반복합니다.
11. 필요에 따라 'validate-config' 구성을 확인합니다

    서비스가 확인 및 표시됩니다. 다음 메시지는 무시해도 됩니다.

    - include 파일 /etc/samba/include/cifs-interfaces.in c를 찾을 수 없습니다
    - include 파일 /etc/samba/include/cifs-filesystem.in c를 찾을 수 없습니다
    - include 파일 /etc/samba/include/cifs-custom-config.in c를 찾을 수 없습니다
    - include 파일 /etc/samba/include/cifs-shares.in c를 찾을 수 없습니다
      i. 메시지가 표시되면 * Enter * 를 눌러 감사 클라이언트 구성을 표시합니다.
      ii. 메시지가 표시되면 * Enter * 를 누릅니다.

12. CIFS 구성 유틸리티 'exit'를 닫습니다
13. 다음과 같이 추가 감사 공유를 설정해야 하는지 확인합니다.
    - StorageGRID 배포가 단일 사이트인 경우 다음 단계로 이동합니다.

- StorageGRID 구축에 다른 사이트의 관리 노드가 포함되는 경우 필요에 따라 다음 감사 공유를 활성화합니다.
  i. 사이트의 관리 노드에 원격으로 로그인:
    A. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
    B. "passwords.txt" 파일에 나열된 암호를 입력합니다.
    C. 루트로 전환하려면 다음 명령을 입력합니다
    D. "passwords.txt" 파일에 나열된 암호를 입력합니다.
  ii. 각 관리 노드에 대한 감사 공유를 구성하려면 다음 단계를 반복합니다.
  iii. 원격 관리 노드에 대한 원격 보안 셸 로그인을 'exit'로 닫습니다

14. 명령 셸에서 'exit'를 로그아웃합니다

CIFS 감사 공유에서 사용자 또는 그룹을 제거합니다

감사 공유에 액세스할 수 있는 마지막 사용자 또는 그룹은 제거할 수 없습니다.

필요한 것

- 루트 계정 암호(해당 패키지에서 사용 가능)가 있는 "passwords.txt" 파일이 있습니다.
- "Configuration.txt" 파일이 있습니다(해당 패키지에서 사용 가능).

이 작업에 대해

CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. CIFS 구성 유틸리티 'config_cifs.rb'를 시작합니다

```
-----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-----------------------------------------------------------------------
```

3. 사용자 또는 그룹 제거 시작: remove-user-from-share'

   관리 노드에 대해 사용 가능한 감사 공유 목록이 번호가 매겨진 형식으로 표시됩니다. 감사 공유는 audit-export로 표시됩니다.

4. 감사 공유 번호('*audit_share_number*')를 입력합니다
5. 사용자 또는 그룹을 제거하라는 메시지가 표시되면 사용자 또는 그룹 을 선택합니다

   감사 공유의 사용자 또는 그룹 번호가 매겨진 목록이 표시됩니다.

6. 제거할 사용자 또는 그룹에 해당하는 번호('*number*')를 입력합니다

   감사 공유가 업데이트되고 사용자 또는 그룹이 더 이상 감사 공유에 액세스할 수 없습니다. 예를 들면 다음과 같습니다.

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. CIFS 구성 유틸리티 'exit'를 닫습니다
8. StorageGRID 배포에 다른 사이트의 관리자 노드가 포함된 경우 필요에 따라 각 사이트에서 감사 공유를 비활성화합니다.
9. 구성이 완료되면 각 명령 셸에서 로그아웃합니다: "exit"

CIFS 감사 공유 사용자 또는 그룹 이름을 변경합니다

새 사용자 또는 그룹을 추가한 다음 이전 사용자 또는 그룹을 삭제하여 CIFS 감사 공유의 사용자 또는 그룹 이름을 변경할 수 있습니다.

이 작업에 대해

CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

단계

1. 업데이트된 이름이 있는 새 사용자 또는 그룹을 감사 공유에 추가합니다.
2. 이전 사용자 또는 그룹 이름을 삭제합니다.

관련 정보

- CIFS 감사 공유에 사용자 또는 그룹을 추가합니다
- CIFS 감사 공유에서 사용자 또는 그룹을 제거합니다

CIFS 감사 통합을 확인합니다

감사 공유는 읽기 전용입니다. 로그 파일은 컴퓨터 응용 프로그램에서 읽기 위한 것이며 파일 열기에 대한 확인은 포함되지 않습니다. 감사 로그 파일이 Windows 탐색기 창에 표시된다는 것은 충분한 검증으로 간주됩니다. 연결 확인 후 모든 창을 닫습니다.

NFS에 대한 감사 클라이언트를 구성합니다

감사 공유는 읽기 전용 공유로 자동 설정됩니다.

필요한 것

- 루트/관리자 암호가 있는 "passwords.txt" 파일이 있습니다(해당 패키지에서 사용 가능).
- "Configuration.txt" 파일이 있습니다(해당 패키지에서 사용 가능).
- 감사 클라이언트가 NFS 버전 3(NFSv3)을 사용하고 있습니다.

이 작업에 대해

감사 메시지를 검색할 StorageGRID 배포의 각 관리자 노드에 대해 이 절차를 수행합니다.

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
2. 모든 서비스의 상태가 실행 중 또는 확인인지 확인합니다. 'toragegrid-status'를 입력합니다

실행 중 또는 확인으로 나열되지 않은 서비스가 있는 경우 계속하기 전에 문제를 해결합니다.

3. 명령줄로 돌아갑니다. Ctrl * + * C * 를 누릅니다.
4. NFS 구성 유틸리티를 시작합니다. config_nfs.rb를 입력합니다

```
----------------------------------------------------------------
| Shares                | Clients               | Config          |
----------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
----------------------------------------------------------------
```

5. 감사 클라이언트를 'add-audit-share'로 추가합니다
   a. 메시지가 표시되면 감사 공유의 감사 클라이언트의 IP 주소 또는 IP 주소 범위를 'client_ip_address'로 입력합니다
   b. 메시지가 표시되면 * Enter * 를 누릅니다.
6. 둘 이상의 감사 클라이언트가 감사 공유에 액세스할 수 있는 경우 추가 사용자의 IP 주소('add-ip-to-share')를 추가합니다
   a. 감사 공유 번호('*audit_share_number*')를 입력합니다
   b. 메시지가 표시되면 감사 공유에 대한 감사 클라이언트의 IP 주소 또는 IP 주소 범위를 '*client_ip_address*'로 입력합니다
   c. 메시지가 표시되면 * Enter * 를 누릅니다.

      NFS 구성 유틸리티가 표시됩니다.

   d. 감사 공유에 대한 액세스 권한이 있는 각 추가 감사 클라이언트에 대해 이러한 하위 단계를 반복합니다.
7. 필요한 경우 구성을 확인합니다.
   a. 'validate-config'를 입력한다

      서비스가 확인 및 표시됩니다.

   b. 메시지가 표시되면 * Enter * 를 누릅니다.

      NFS 구성 유틸리티가 표시됩니다.

   c. NFS 구성 유틸리티 'exit'를 닫습니다
8. 다른 사이트에서 감사 공유를 사용하도록 설정해야 하는지 확인합니다.
   - StorageGRID 배포가 단일 사이트인 경우 다음 단계로 이동합니다.
   - StorageGRID 구축에 다른 사이트의 관리 노드가 포함되는 경우 필요에 따라 다음 감사 공유를 활성화합니다.
     i. 사이트의 관리 노드에 원격으로 로그인:
        A. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

B. "passwords.txt" 파일에 나열된 암호를 입력합니다.

C. 루트로 전환하려면 다음 명령을 입력합니다

D. "passwords.txt" 파일에 나열된 암호를 입력합니다.

ii. 이 단계를 반복하여 각 추가 관리 노드에 대한 감사 공유를 구성합니다.

iii. 원격 관리 노드에 대한 원격 보안 셸 로그인을 닫습니다. 'exit'로 진입합니다

9. 명령 셸에서 'exit'를 로그아웃합니다

NFS 감사 클라이언트는 IP 주소를 기반으로 감사 공유에 대한 액세스 권한이 부여됩니다. 공유에 IP 주소를 추가하여 새 NFS 감사 클라이언트에 감사 공유에 대한 액세스 권한을 부여하거나 IP 주소를 제거하여 기존 감사 클라이언트를 제거합니다.

NFS 감사 클라이언트를 감사 공유에 추가합니다

NFS 감사 클라이언트는 IP 주소를 기반으로 감사 공유에 대한 액세스 권한이 부여됩니다. 감사 공유에 IP 주소를 추가하여 새 NFS 감사 클라이언트에 감사 공유에 대한 액세스 권한을 부여합니다.

필요한 것

- 루트/관리자 계정 암호(해당 패키지에서 사용 가능)가 있는 "passwords.txt" 파일이 있습니다.
- "Configuration.txt" 파일이 있습니다(해당 패키지에서 사용 가능).
- 감사 클라이언트가 NFS 버전 3(NFSv3)을 사용하고 있습니다.

단계

1. 기본 관리자 노드에 로그인합니다.

   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. NFS 구성 유틸리티 'config_nfs.rb'를 시작합니다

```
-----------------------------------------------------------------
| Shares                | Clients               | Config          |
-----------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
-----------------------------------------------------------------
```

3. add-ip-to-share를 입력합니다

   관리 노드에 설정된 NFS 감사 공유 목록이 표시됩니다. 감사 공유는 '/var/local/audit/export'로 나열됩니다

4. 감사 공유 번호('*audit_share_number*')를 입력합니다
5. 메시지가 표시되면 감사 공유에 대한 감사 클라이언트의 IP 주소 또는 IP 주소 범위를 '*client_ip_address*'로 입력합니다

   감사 클라이언트가 감사 공유에 추가됩니다.

6. 메시지가 표시되면 * Enter * 를 누릅니다.

   NFS 구성 유틸리티가 표시됩니다.

7. 감사 공유에 추가해야 하는 각 감사 클라이언트에 대해 이 단계를 반복합니다.
8. 필요에 따라 'validate-config' 구성을 확인합니다

   서비스가 확인 및 표시됩니다.

   a. 메시지가 표시되면 * Enter * 를 누릅니다.

      NFS 구성 유틸리티가 표시됩니다.

9. NFS 구성 유틸리티 'exit'를 닫습니다
10. StorageGRID 배포가 단일 사이트인 경우 다음 단계로 이동합니다.

    그렇지 않으면 StorageGRID 구축에 다른 사이트의 관리 노드가 포함되는 경우 필요에 따라 다음 감사 공유를 활성화합니다.

    a. 사이트의 관리 노드에 원격으로 로그인:

       i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

       ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.

       iii. 루트로 전환하려면 다음 명령을 입력합니다

       iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

    b. 각 관리 노드에 대한 감사 공유를 구성하려면 다음 단계를 반복합니다.

    c. 원격 관리 노드에 대한 원격 보안 셸 로그인을 'exit'로 닫습니다

11. 명령 셸에서 'exit'를 로그아웃합니다

NFS 감사 통합을 검증합니다

감사 공유를 구성하고 NFS 감사 클라이언트를 추가한 후에는 감사 클라이언트 공유를 마운트하고 감사 공유에서 해당 파일을 사용할 수 있는지 확인할 수 있습니다.

단계

1. AMS 서비스를 호스팅하는 관리 노드의 클라이언트 측 IP 주소를 사용하여 연결(또는 클라이언트 시스템의 변형)을 확인합니다. ping ip_address를 입력한다

서버가 응답하여 연결을 나타내는지 확인합니다.

2. 클라이언트 운영 체제에 적합한 명령을 사용하여 감사 읽기 전용 공유를 마운트합니다. Linux 명령의 예는 다음과 같습니다(한 줄에 입력).

   mount -t nfs -o hard, intr_Admin_Node_IP_address_:/var/local/audit/export_myAudit_

   AMS 서비스를 호스팅하는 관리 노드의 IP 주소와 감사 시스템에 대해 미리 정의된 공유 이름을 사용합니다. 마운트 지점은 클라이언트에서 선택한 모든 이름(예: 이전 명령에서 '*myAudit*')일 수 있습니다.

3. 감사 공유에서 파일을 사용할 수 있는지 확인합니다. 'ls_myAudit_/ *'을 입력합니다

   여기서, '*myAudit*'는 감사 공유의 마운트 지점입니다. 하나 이상의 로그 파일이 나열되어야 합니다.

감사 공유에서 **NFS** 감사 클라이언트를 제거합니다

NFS 감사 클라이언트는 IP 주소를 기반으로 감사 공유에 대한 액세스 권한이 부여됩니다. IP 주소를 제거하여 기존 감사 클라이언트를 제거할 수 있습니다.

필요한 것

- 루트/관리자 계정 암호(해당 패키지에서 사용 가능)가 있는 "passwords.txt" 파일이 있습니다.
- "Configuration.txt" 파일이 있습니다(해당 패키지에서 사용 가능).

이 작업에 대해

감사 공유에 액세스할 수 있는 마지막 IP 주소는 제거할 수 없습니다.

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. NFS 구성 유틸리티 'config_nfs.rb'를 시작합니다

```
-----------------------------------------------------------------
| Shares                | Clients               | Config          |
-----------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
-----------------------------------------------------------------
```

3. Audit share에서 IP address를 remove-ip-from-share에서 삭제한다

   서버에 구성된 감사 공유의 번호가 매겨진 목록이 표시됩니다. 감사 공유는 '/var/local/audit/export'로 나열됩니다

4. 감사 공유에 해당하는 번호('*audit_share_number*')를 입력합니다

   감사 공유에 액세스할 수 있는 번호가 매겨진 IP 주소 목록이 표시됩니다.

5. 제거할 IP 주소에 해당하는 번호를 입력합니다.

   감사 공유가 업데이트되며 이 IP 주소를 가진 감사 클라이언트에서 더 이상 액세스가 허용되지 않습니다.

6. 메시지가 표시되면 * Enter * 를 누릅니다.

   NFS 구성 유틸리티가 표시됩니다.

7. NFS 구성 유틸리티 'exit'를 닫습니다
8. StorageGRID 배포가 다른 사이트에 추가 관리 노드가 있는 다중 데이터 센터 사이트 배포인 경우 필요에 따라 다음 감사 공유를 비활성화합니다.
   a. 각 사이트의 관리자 노드에 원격으로 로그인:
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   b. 이 단계를 반복하여 각 추가 관리 노드에 대한 감사 공유를 구성합니다.
   c. 원격 관리 노드에 대한 원격 보안 셸 로그인을 'exit'로 닫습니다
9. 명령 셸에서 'exit'를 로그아웃합니다

NFS 감사 클라이언트의 **IP** 주소를 변경합니다

NFS 감사 클라이언트의 IP 주소를 변경해야 하는 경우 다음 단계를 완료합니다.

단계

1. 기존 NFS 감사 공유에 새 IP 주소를 추가합니다.
2. 원래 IP 주소를 제거합니다.

관련 정보

- NFS 감사 클라이언트를 감사 공유에 추가합니다
- 감사 공유에서 NFS 감사 클라이언트를 제거합니다

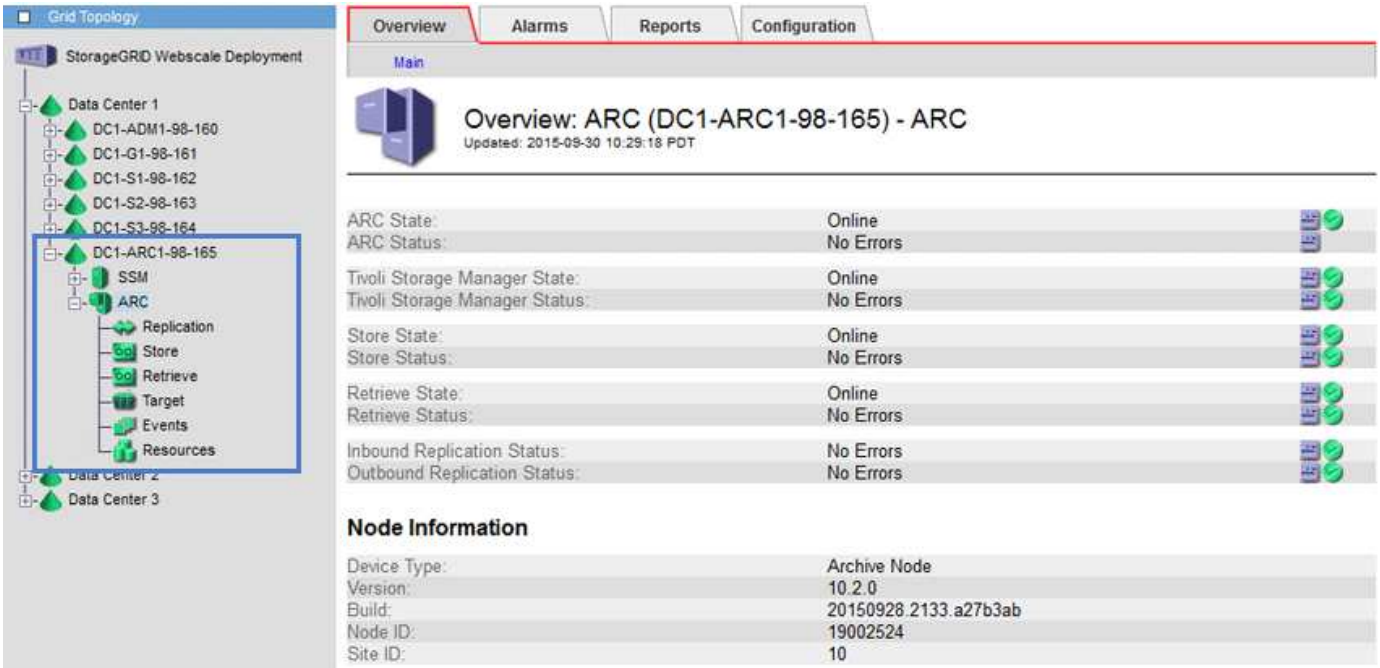
아카이브 노드 관리

아카이브 노드의 정의

선택적으로 각 StorageGRID 데이터 센터 사이트를 아카이브 노드와 함께 구축할 수 있습니다.

그러면 TSM(Tivoli Storage Manager)과 같은 타겟 외부 아카이브 스토리지 시스템에 연결할 수 있습니다.

아카이브 노드는 객체 데이터의 장기 저장을 위해 외부 아카이브 스토리지 시스템을 대상으로 지정할 수 있는 인터페이스를 제공합니다. 또한 아카이브 노드는 이 연결과 StorageGRID 시스템과 대상 외부 아카이브 스토리지 시스템 간의 개체 데이터 전송을 모니터링합니다.



외부 타겟에 대한 접속을 구성한 후 TSM 성능을 최적화하도록 아카이브 노드를 구성하고, TSM 서버가 용량 또는 사용 불가 상태에 근접할 때 아카이브 노드를 오프라인으로 전환하고, 복제 및 검색 설정을 구성할 수 있습니다. 아카이브 노드에 대한 사용자 지정 알람을 설정할 수도 있습니다.

삭제할 수 없지만 정기적으로 액세스하지 않는 오브젝트 데이터는 언제든지 스토리지 노드의 회전식 디스크에서 벗어나 클라우드 또는 테이프와 같은 외부 아카이브 스토리지로 이동할 수 있습니다. 이러한 오브젝트 데이터 아카이빙은 데이터 센터 사이트의 아카이브 노드 구성과 이 아카이브 노드가 콘텐츠 배치 지침을 위한 "대상"으로 선택된 ILM 규칙 구성을 통해 수행됩니다. 아카이브 노드는 아카이빙된 객체 데이터 자체를 관리하지 않으며, 이는 외부 아카이브 디바이스가 수행합니다.

> 오브젝트 메타데이터는 아카이빙되지 않지만 스토리지 노드에 유지됩니다.

ARC 서비스의 정의

아카이브 노드의 아카이브(ARC) 서비스는 TSM 미들웨어를 통해 테이프와 같은 외부 아카이브 스토리지에 대한 연결을 구성하는 데 사용할 수 있는 관리 인터페이스를 제공합니다.

이 서비스는 외부 아카이브 스토리지 시스템과 상호 작용하여 니어라인 스토리지에 대한 오브젝트 데이터를 전송하고 클라이언트 애플리케이션이 아카이빙된 객체를 요청할 때 검색을 수행하는 ARC 서비스입니다. 클라이언트 애플리케이션이 아카이빙된 객체를 요청하면 스토리지 노드는 ARC 서비스에서 객체 데이터를 요청합니다. ARC 서비스는 외부 아카이브 스토리지 시스템에 요청을 하여 요청된 개체 데이터를 검색하여 ARC 서비스로 전송합니다. ARC 서비스는 객체 데이터를 확인하고 이를 스토리지 노드로 전달하여 객체를 요청한 클라이언트 애플리케이션으로 반환합니다.

TSM 미들웨어를 통해 테이프로 아카이빙된 오브젝트 데이터에 대한 요청은 검색 효율성을 위해 관리됩니다. 테이프에 순차적으로 저장된 객체가 동일한 순서로 요청되도록 요청을 주문할 수 있습니다. 그런 다음 요청이 스토리지

디바이스에 제출될 때까지 대기합니다. 아카이브 장치에 따라 서로 다른 볼륨에 있는 개체에 대한 여러 요청을 동시에 처리할 수 있습니다.

S3 API를 통해 클라우드에 아카이브

아카이브 노드를 구성하여 AWS(Amazon Web Services)에 직접 연결하거나 S3 API를 통해 StorageGRID 시스템에 연결할 수 있는 다른 시스템에 연결할 수 있습니다.

> S3 API를 통해 아카이브 노드에서 외부 아카이브 스토리지 시스템으로 오브젝트를 이동한 후 ILM 클라우드 스토리지 풀로 대체되었으며 더 많은 기능을 제공합니다. Cloud Tiering - S3(Simple Storage Service) * 옵션은 계속 지원되지만 Cloud Storage Pool을 대신 구현하는 것이 좋습니다.

현재 * Cloud Tiering - Simple Storage Service(S3) * 옵션과 함께 아카이브 노드를 사용 중인 경우 오브젝트를 클라우드 스토리지 풀로 마이그레이션하는 것을 고려해 보십시오. 의 지침을 참조하십시오 ILM을 사용하여 개체 관리.

S3 API에 대한 연결 설정을 구성합니다

S3 인터페이스를 사용하여 아카이브 노드에 연결하는 경우 S3 API에 대한 연결 설정을 구성해야 합니다. 이러한 설정이 구성될 때까지 ARC 서비스는 외부 아카이브 스토리지 시스템과 통신할 수 없기 때문에 주요 알람 상태를 유지합니다.

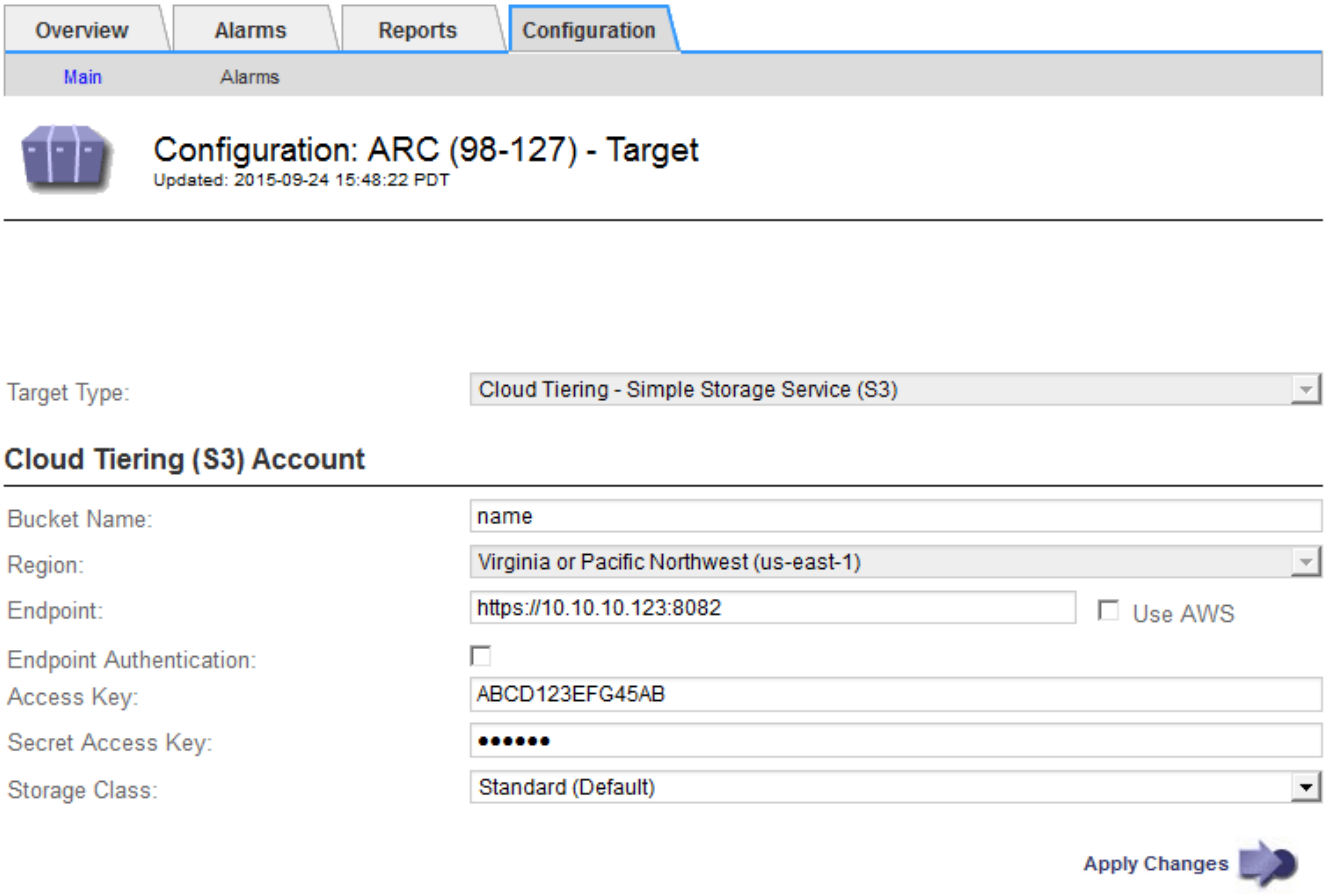
> S3 API를 통해 아카이브 노드에서 외부 아카이브 스토리지 시스템으로 오브젝트를 이동한 후 ILM 클라우드 스토리지 풀로 대체되었으며 더 많은 기능을 제공합니다. Cloud Tiering - S3(Simple Storage Service) * 옵션은 계속 지원되지만 Cloud Storage Pool을 대신 구현하는 것이 좋습니다.
>
> 현재 * Cloud Tiering - Simple Storage Service(S3) * 옵션과 함께 아카이브 노드를 사용 중인 경우 오브젝트를 클라우드 스토리지 풀로 마이그레이션하는 것을 고려해 보십시오. 을 참조하십시오 ILM을 사용하여 개체를 관리합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- 타겟 아카이브 스토리지 시스템에 버킷을 생성했습니다.
  - 버킷은 단일 아카이브 노드 전용입니다. 다른 아카이브 노드 또는 다른 응용 프로그램에서는 사용할 수 없습니다.
  - 버킷에는 해당 위치에 적합한 영역이 선택되어 있습니다.
  - 버킷을 버전 관리가 일시 중지되도록 구성해야 합니다.
- 오브젝트 분할이 활성화되고 최대 세그먼트 크기가 4.5GiB(4,831,838,208바이트) 이하입니다. S3를 외부 아카이브 스토리지 시스템으로 사용하면 이 값을 초과하는 S3 API 요청이 실패합니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node * > * ARC * > * Target * 을 선택합니다.
3. Configuration * > * Main * 을 선택합니다.



4. Target Type 드롭다운 목록에서 * Cloud Tiering - Simple Storage Service (S3) * 를 선택합니다.

   대상 유형을 선택할 때까지 구성 설정을 사용할 수 없습니다.

5. 아카이브 노드가 타겟 외부 S3 지원 아카이브 스토리지 시스템에 연결하는 데 사용할 클라우드 계층화(S3) 계정을 구성합니다.

   이 페이지의 대부분의 필드는 설명이 필요 없습니다. 다음은 지침이 필요한 필드에 대한 설명입니다.

   - * 지역 *: * AWS 사용 * 이 선택된 경우에만 사용할 수 있습니다. 선택한 지역은 버킷 지역과 일치해야 합니다.
   - * 엔드포인트 * 및 * AWS 사용 *: AWS(Amazon Web Services)의 경우 * AWS 사용 * 을 선택합니다. 그러면 * Endpoint * 가 버킷 이름 및 영역 속성에 따라 끝점 URL로 자동으로 채워집니다. 예를 들면 다음과 같습니다.

     'https://bucket.region.amazonaws.com`

     비 AWS 타겟의 경우 포트 번호를 포함하여 버킷을 호스팅하는 시스템의 URL을 입력합니다. 예를 들면 다음과 같습니다.

   'https://system.com:1080`

   - * 엔드포인트 인증 *: 기본적으로 사용됩니다. 외부 아카이브 스토리지 시스템에 대한 네트워크를 신뢰할 수 있는 경우 확인란을 선택 취소하여 대상 외부 아카이브 스토리지 시스템에 대한 엔드포인트 SSL 인증서 및 호스트 이름 확인을 비활성화할 수 있습니다. StorageGRID 시스템의 다른 인스턴스가 대상 아카이브 스토리지 디바이스이고 시스템에서 공개적으로 서명된 인증서를 구성한 경우 확인란을 선택한 상태로 유지할 수 있습니다.

- * 스토리지 클래스 *: 일반 스토리지로 * 표준(기본값) * 을 선택합니다. 쉽게 다시 만들 수 있는 개체에 대해서만 * Reduced Redundancy * 를 선택합니다. * 감소된 중복 * 은 낮은 신뢰성을 통해 저렴한 저장 공간을 제공합니다. 대상 아카이브 스토리지 시스템이 StorageGRID 시스템의 또 다른 인스턴스인 경우 * 스토리지 클래스 * 는 오브젝트가 인제스트될 때 이중 커밋이 사용되는 경우 대상 시스템에서 인제스트할 때 오브젝트의 중간 복제본 수를 제어합니다.

6. Apply Changes * 를 선택합니다.

   지정된 구성 설정이 검증되어 StorageGRID 시스템에 적용됩니다. 구성이 완료되면 타겟을 변경할 수 없습니다.

S3 API에 대한 연결 설정을 수정합니다

S3 API를 통해 아카이브 노드가 외부 아카이브 스토리지 시스템에 연결되도록 구성된 후 연결이 변경될 경우 일부 설정을 수정할 수 있습니다.

필요한 것

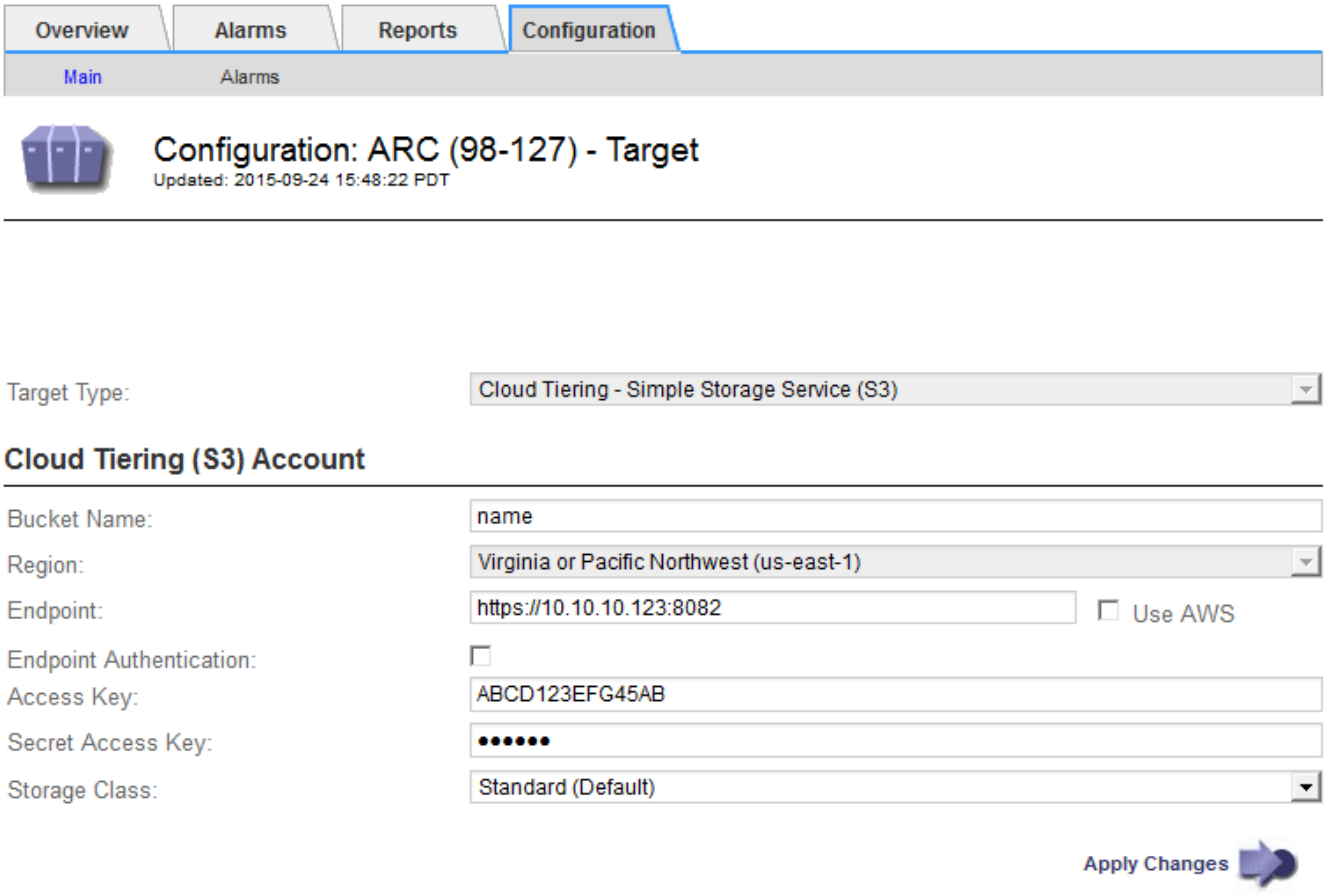
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

Cloud Tiering(S3) 계정을 변경하는 경우 이전에 아카이브 노드에서 버킷으로 수집했던 모든 오브젝트를 비롯하여 사용자 액세스 자격 증명이 버킷에 대한 읽기/쓰기 액세스를 가져야 합니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node_ * > * ARC * > * Target * 을 선택합니다.
3. Configuration * > * Main * 을 선택합니다.



4. 필요에 따라 계정 정보를 수정합니다.

   스토리지 클래스를 변경하면 새 오브젝트 데이터가 새 스토리지 클래스에 저장됩니다. 기존 객체는 인제스트할 때 스토리지 클래스 세트 아래에 계속 저장됩니다.

   버킷 이름, 지역 및 종점, AWS 값을 사용하며 변경할 수 없습니다.

5. Apply Changes * 를 선택합니다.

Cloud Tiering Service 상태를 수정합니다

Cloud Tiering Service의 상태를 변경하여 S3 API를 통해 연결되는 타겟 외부 아카이브 스토리지 시스템에 대한 아카이브 노드의 읽기 및 쓰기 기능을 제어할 수 있습니다.

필요한 것

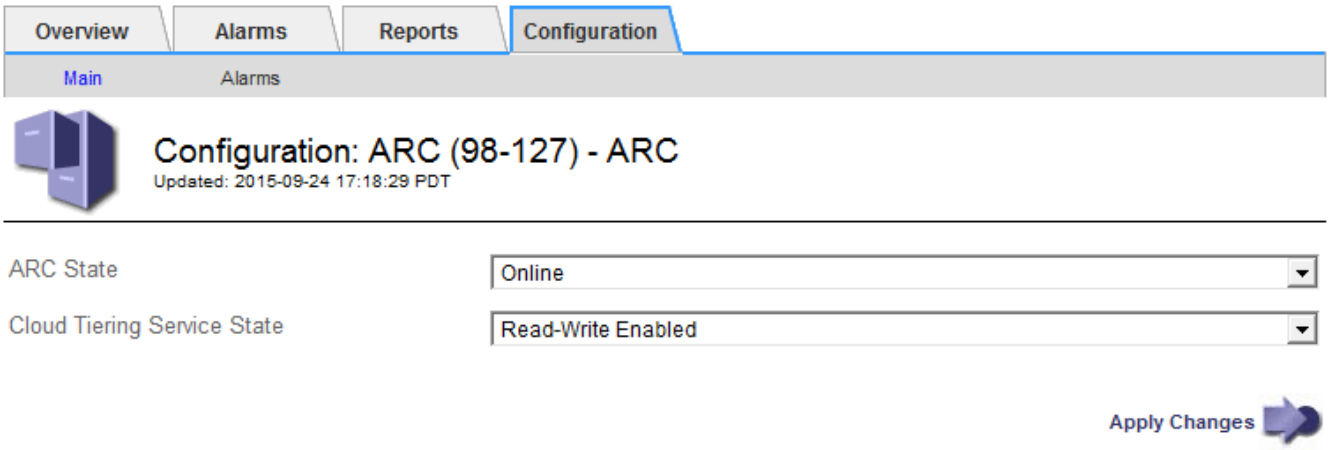
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.
- 아카이브 노드를 구성해야 합니다.

이 작업에 대해

Cloud Tiering Service State를 * Read-Write Disabled * 로 변경하면 아카이브 노드를 효과적으로 오프라인 상태로 전환할 수 있습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node_ * > * ARC * 를 선택합니다.
3. Configuration * > * Main * 을 선택합니다.



4. Cloud Tiering Service State * 를 선택합니다.
5. Apply Changes * 를 선택합니다.

S3 API 연결에 대한 저장소 실패 횟수를 재설정합니다

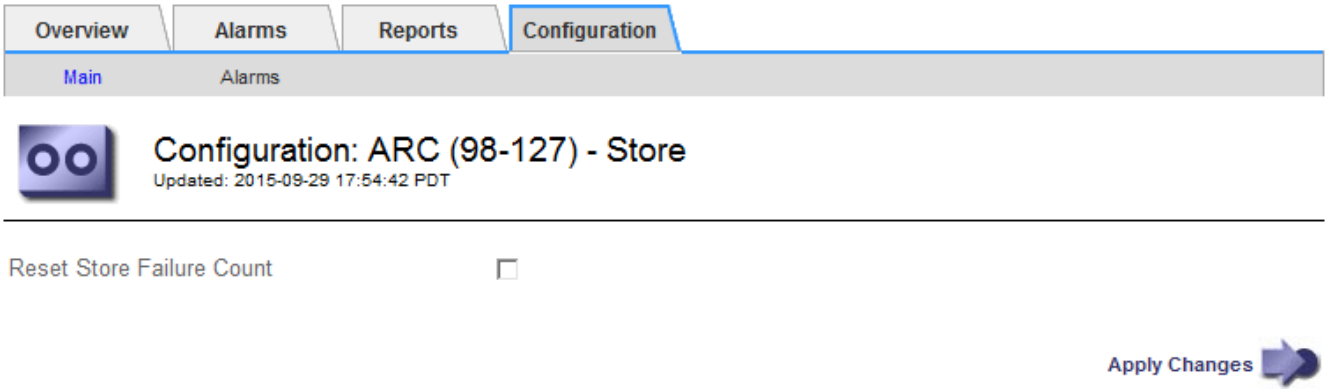
아카이브 노드가 S3 API를 통해 아카이브 스토리지 시스템에 연결된 경우 ARVF(Store Failure Count) 경보를 지우는 데 사용할 수 있는 저장소 오류 카운트를 재설정할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node_ * > * ARC * > * Store * 를 선택합니다.
3. Configuration * > * Main * 을 선택합니다.



4. Reset Store Failure Count * 를 선택합니다.

5. Apply Changes * 를 선택합니다.

   Store Failures 속성이 0으로 재설정됩니다.

Cloud Tiering-S3에서 **Cloud Storage Pool**로 오브젝트 마이그레이션

현재 * Cloud Tiering - S3(Simple Storage Service) * 기능을 사용하여 오브젝트 데이터를 S3 버킷으로 계층화하려는 경우 대신 오브젝트를 Cloud Storage Pool로 마이그레이션하는 것을 고려해 보십시오. 클라우드 스토리지 풀은 StorageGRID 시스템의 모든 스토리지 노드를 활용하는 확장 가능한 접근 방식을 제공합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- Cloud Tiering에 구성된 S3 버킷에 오브젝트를 이미 저장했습니다.

> 오브젝트 데이터를 마이그레이션하기 전에 NetApp 고객 담당자에게 연락하여 관련 비용을 파악하고 관리하십시오.

이 작업에 대해

ILM 관점에서 Cloud Storage Pool은 스토리지 풀과 유사합니다. 그러나 스토리지 풀은 StorageGRID 시스템 내의 스토리지 노드 또는 아카이브 노드로 구성되지만, 클라우드 스토리지 풀은 외부 S3 버킷으로 구성됩니다.

Cloud Tiering-S3에서 클라우드 스토리지 풀로 오브젝트를 마이그레이션하기 전에 먼저 S3 버킷을 생성한 다음 StorageGRID에서 클라우드 스토리지 풀을 생성해야 합니다. 그런 다음 새 ILM 정책을 생성하고 Cloud Tiering 버킷에 오브젝트를 저장하는 데 사용되는 ILM 규칙을 Cloud Storage Pool에 동일한 오브젝트를 저장하는 클론 생성된 ILM 규칙으로 대체할 수 있습니다.

> 오브젝트를 클라우드 스토리지 풀에 저장할 경우 해당 오브젝트의 복사본도 StorageGRID 내에 저장할 수 없습니다. 현재 Cloud Tiering에 사용 중인 ILM 규칙이 개체를 동시에 여러 위치에 저장하도록 구성된 경우 해당 기능이 손실되므로 이 선택적 마이그레이션을 계속 수행할지 여부를 고려하십시오. 이 마이그레이션을 계속할 경우 기존 규칙을 복제하는 대신 새 규칙을 만들어야 합니다.

단계

1. 클라우드 스토리지 풀을 생성합니다.

   Cloud Storage Pool에 새로운 S3 버킷을 사용하여 Cloud Storage Pool에서 관리하는 데이터만 포함되도록 합니다.

2. 활성 ILM 정책에서 객체가 Cloud Tiering 버킷에 저장되도록 하는 ILM 규칙을 찾습니다.
3. 이러한 각 규칙을 복제합니다.
4. 클론 복제된 규칙에서 배치 위치를 새 Cloud Storage Pool로 변경합니다.
5. 복제된 규칙을 저장합니다.
6. 새 규칙을 사용하는 새 정책을 만듭니다.
7. 새 정책을 시뮬레이션하고 활성화합니다.

새 정책이 활성화되어 ILM 평가가 발생하면 Cloud Tiering에 구성된 S3 버킷에서 Cloud Storage Pool에 구성된 S3 버킷으로 오브젝트가 이동됩니다. 그리드의 사용 가능한 공간은 영향을 받지 않습니다. 오브젝트를 Cloud Storage Pool로 이동한 후 Cloud Tiering 버킷에서 제거됩니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

TSM 미들웨어를 통해 테이프로 아카이빙

테이프 라이브러리를 포함하여 랜덤 또는 순차 액세스 스토리지 디바이스에 오브젝트 데이터를 저장하고 검색하기 위한 논리 인터페이스를 제공하는 TSM(Tivoli Storage Manager) 서버를 대상으로 아카이브 노드를 구성할 수 있습니다.

아카이브 노드의 ARC 서비스는 TSM 서버에 대한 클라이언트 역할을 하며 Tivoli Storage Manager를 아카이빙 스토리지 시스템과 통신하는 미들웨어로 사용합니다.

TSM 관리 클래스

TSM 미들웨어에 의해 정의된 관리 클래스는 TSM의 백업 및 아카이브 작업이 작동하는 방식을 요약하고 TSM 서버에 의해 적용되는 콘텐츠에 대한 규칙을 지정하는 데 사용할 수 있습니다. 이러한 규칙은 StorageGRID 시스템의 ILM 정책과 독립적으로 작동하며, 객체가 영구적으로 저장되고 아카이브 노드에서 검색할 수 있도록 항상 사용 가능한 StorageGRID 시스템의 요구 사항과 일치해야 합니다. 아카이브 노드에서 TSM 서버로 객체 데이터를 전송한 후 TSM 서버에서 관리하는 테이프에 객체 데이터를 저장하는 동안 TSM 수명주기 및 보존 규칙이 적용됩니다.

TSM 관리 클래스는 아카이브 노드에서 TSM 서버로 객체가 전송된 후 데이터 위치 또는 보존에 대한 규칙을 적용하기 위해 TSM 서버에서 사용됩니다. 예를 들어, 데이터베이스 백업으로 식별된 객체(최신 데이터로 덮어쓸 수 있는 임시 컨텐츠)는 애플리케이션 데이터(무기한으로 보존되어야 하는 고정 컨텐츠)와 다르게 처리될 수 있습니다.

TSM 미들웨어에 대한 연결을 구성합니다

아카이브 노드가 TSM(Tivoli Storage Manager) 미들웨어와 통신하려면 먼저 여러 설정을 구성해야 합니다.

필요한 것

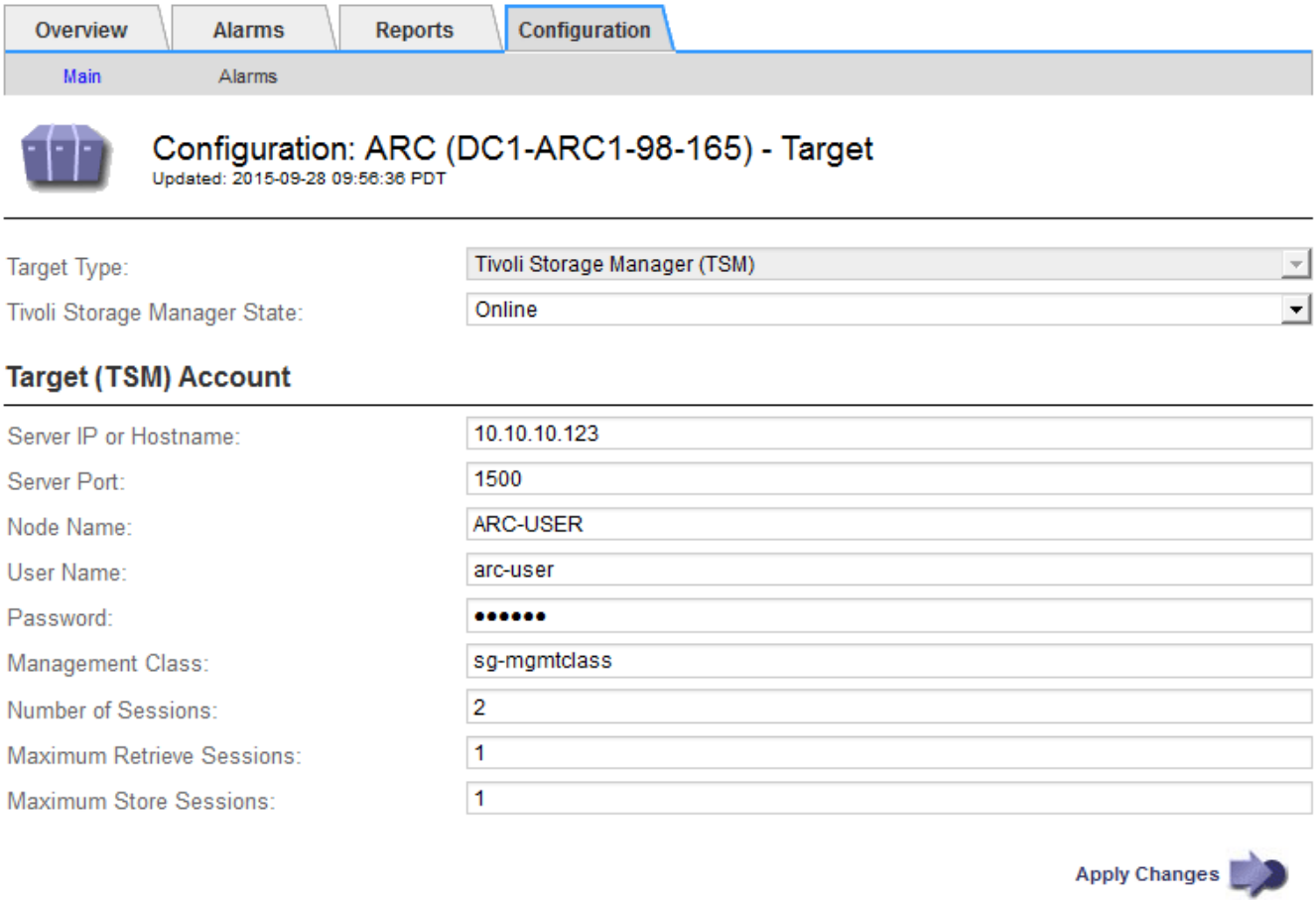
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

이러한 설정이 구성될 때까지 ARC 서비스는 Tivoli Storage Manager와 통신할 수 없기 때문에 주요 알람 상태를 유지합니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node_ * > * ARC * > * Target * 을 선택합니다.
3. Configuration * > * Main * 을 선택합니다.



4. Target Type * 드롭다운 목록에서 * TSM(Tivoli Storage Manager) * 을 선택합니다.
5. Tivoli Storage Manager State * 의 경우 * Offline * 을 선택하여 TSM 미들웨어 서버에서 검색을 방지합니다.

   기본적으로 Tivoli Storage Manager State는 Online으로 설정되어 있으므로 Archive Node는 TSM 미들웨어 서버에서 객체 데이터를 검색할 수 있습니다.

6. 다음 정보를 입력합니다.

   - * 서버 IP 또는 호스트 이름 *: ARC 서비스에서 사용하는 TSM 미들웨어 서버의 IP 주소 또는 정규화된 도메인 이름을 지정합니다. 기본 IP 주소는 127.0.0.1입니다.
   - * 서버 포트*: TSM 미들웨어 서버에서 ARC 서비스가 연결할 포트 번호를 지정합니다. 기본값은 1500입니다.
   - * 노드 이름 *: 아카이브 노드의 이름을 지정합니다. TSM 미들웨어 서버에 등록한 이름(arc - user)을 입력해야 합니다.
   - * 사용자 이름 *: ARC 서비스가 TSM 서버에 로그인하는 데 사용하는 사용자 이름을 지정합니다. 아카이브 노드에 대해 지정한 기본 사용자 이름(arc - user) 또는 관리 사용자를 입력합니다.
   - * 암호 *: ARC 서비스가 TSM 서버에 로그인하기 위해 사용하는 암호를 지정합니다.
   - * 관리 클래스 *: 객체가 StorageGRID 시스템에 저장될 때 관리 클래스가 지정되지 않았거나 지정된 관리 클래스가 TSM 미들웨어 서버에 정의되지 않은 경우 사용할 기본 관리 클래스를 지정합니다.
   - * Number of Sessions *: 아카이브 노드 전용 TSM 미들웨어 서버의 테이프 드라이브 수를 지정합니다. 아카이브 노드는 마운트 지점당 최대 1개의 세션을 동시에 생성하고 적은 수의 추가 세션(5개 미만)을 생성합니다.

     보관 노드를 등록 또는 업데이트할 때 MAXNUMMP(최대 탑재 지점 수)에 대해 설정된 값과 같도록 이 값을

변경해야 합니다. (설정된 값이 없는 경우 REGISTER 명령에서 사용되는 MAXNUMMP의 기본값은 1입니다.)

또한 TSM 서버에 대한 MAXSESSIONS 값을 최소한 ARC 서비스에 대해 설정된 세션 수 만큼 큰 숫자로 변경해야 합니다. TSM 서버의 MAXSESSIONS 기본값은 25입니다.

- * Maximum Retrieve Sessions *: ARC 서비스가 검색 작업을 위해 TSM 미들웨어 서버에 열 수 있는 최대 세션 수를 지정합니다. 대부분의 경우 적절한 값은 세션 수에서 최대 저장소 세션을 뺀 수입니다. 저장 및 검색을 위해 하나의 테이프 드라이브를 공유해야 하는 경우 세션 수 와 동일한 값을 지정하십시오.
- * Maximum Store Sessions *: 아카이브 작업을 위해 ARC 서비스가 TSM 미들웨어 서버에 열 수 있는 최대 동시 세션 수를 지정합니다.

  타겟 아카이브 스토리지 시스템이 꽉 차고 검색할 수만 있는 경우를 제외하고 이 값은 1로 설정해야 합니다. 검색을 위해 모든 세션을 사용하려면 이 값을 0으로 설정합니다.

7. Apply Changes * 를 선택합니다.

TSM 미들웨어 세션에 맞게 아카이브 노드를 최적화합니다

아카이브 노드의 세션을 구성하여 TSM(Tivoli Server Manager)에 연결되는 아카이브 노드의 성능을 최적화할 수 있습니다.

필요한 것

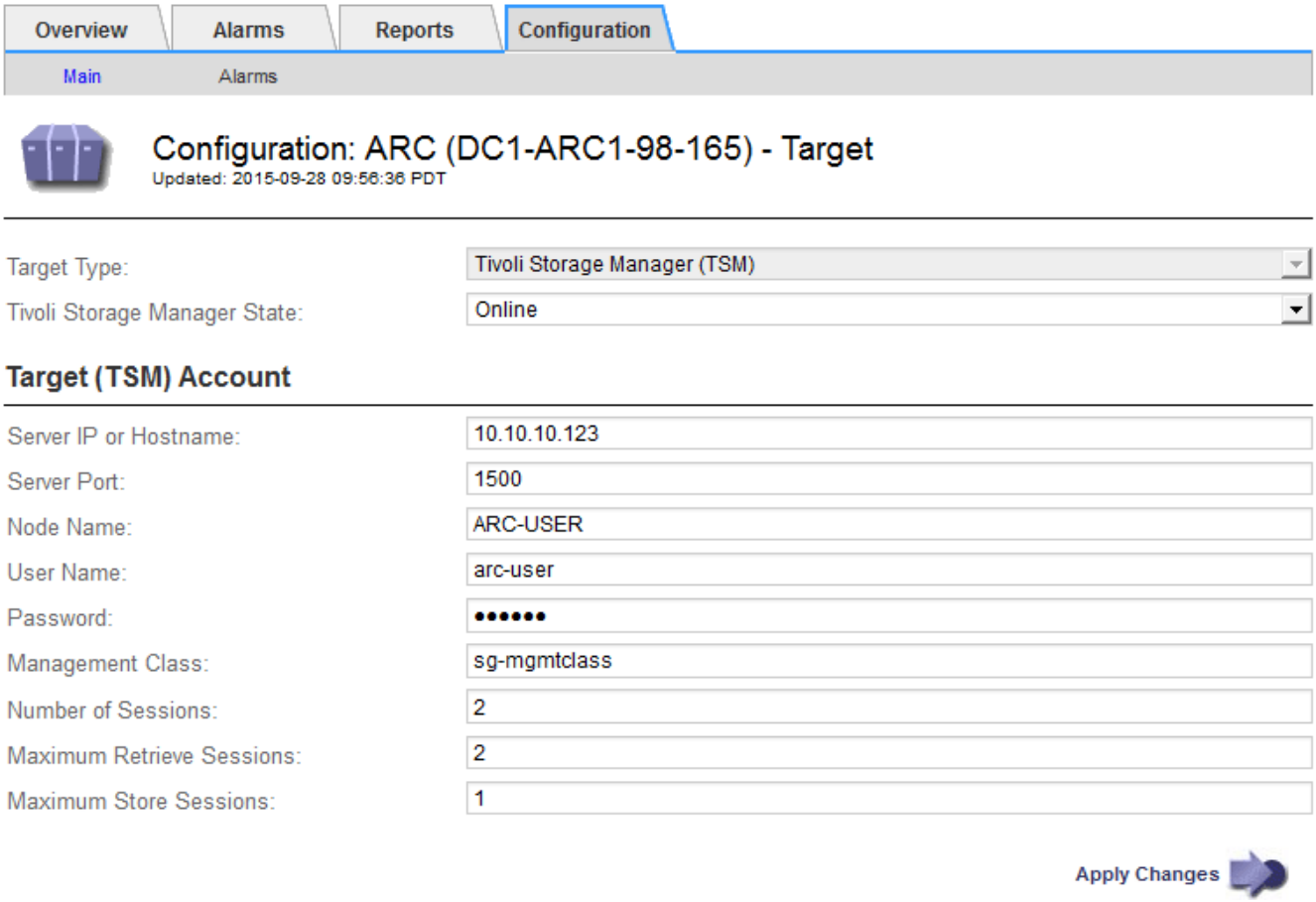
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

일반적으로 아카이브 노드가 TSM 미들웨어 서버에 열려 있는 동시 세션 수는 TSM 서버가 아카이브 노드 전용으로 사용하는 테이프 드라이브 수로 설정됩니다. 나머지 테이프 드라이브는 검색을 위해 할당되는 동안 보관을 위해 하나의 테이프 드라이브가 할당됩니다. 그러나 스토리지 노드가 아카이브 노드 복제본에서 재구축되거나 아카이브 노드가 읽기 전용 모드로 작동하는 경우 최대 검색 세션 수를 동시 세션 수와 같도록 설정하여 TSM 서버 성능을 최적화할 수 있습니다. 그 결과, 모든 드라이브를 동시에 검색할 수 있으며, 해당하는 경우 이들 드라이브 중 하나를 스토리지에도 사용할 수 있습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node_ * > * ARC * > * Target * 을 선택합니다.
3. Configuration * > * Main * 을 선택합니다.
4. 최대 검색 세션 * 을 * 세션 수 * 와 동일하게 변경합니다.



5. Apply Changes * 를 선택합니다.

TSM에 대한 아카이브 상태 및 카운터를 구성합니다

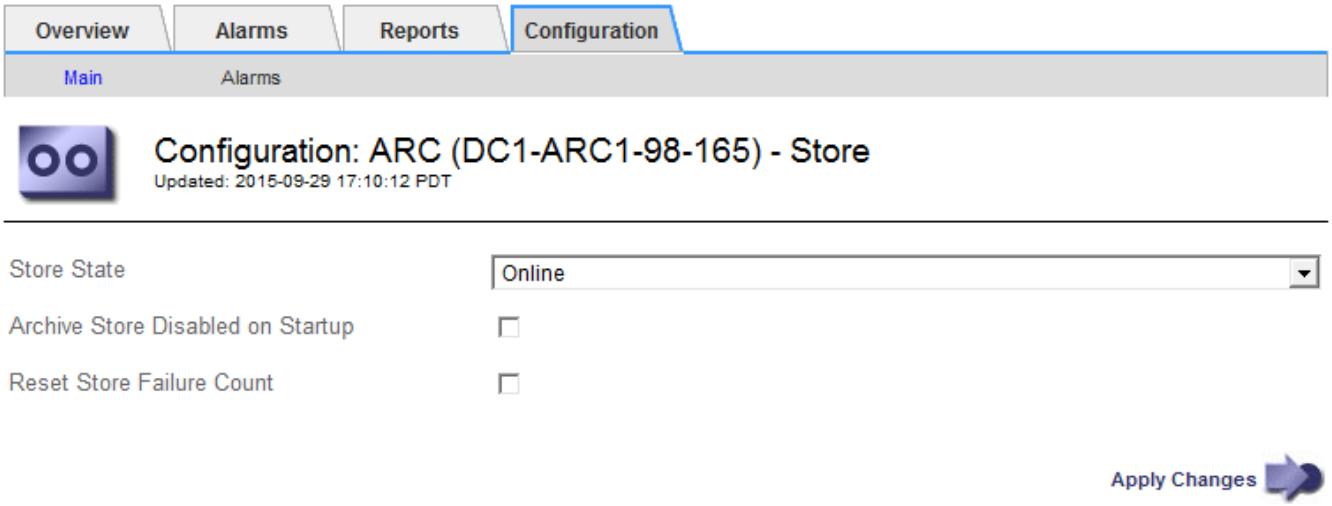
아카이브 노드가 TSM 미들웨어 서버에 연결된 경우 아카이브 노드의 아카이브 저장소 상태를 온라인 또는 오프라인으로 구성할 수 있습니다. 또한 아카이브 노드가 처음 시작될 때 아카이브 저장소를 비활성화하거나 관련 알람에 대해 추적 중인 실패 수를 재설정할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node_ * > * ARC * > * Store * 를 선택합니다.
3. Configuration * > * Main * 을 선택합니다.



4. 필요에 따라 다음 설정을 수정합니다.
   - Store State(상태 저장): 구성 요소 상태를 다음 중 하나로 설정합니다.
     - 온라인: 아카이브 노드는 스토리지의 객체 데이터를 아카이브 스토리지 시스템에 처리하는 데 사용할 수 있습니다.
     - 오프라인: 아카이브 노드는 스토리지의 객체 데이터를 아카이브 스토리지 시스템에 처리하는 데 사용할 수 없습니다.
   - 시작할 때 아카이브 저장소 사용 안 함: 이 옵션을 선택하면 아카이브 저장소 구성 요소는 다시 시작할 때 읽기 전용 상태로 유지됩니다. 대상 아카이브 스토리지 시스템에 대한 스토리지를 영구적으로 해제하는 데 사용됩니다. 대상 아카이브 스토리지 시스템에서 콘텐츠를 수락할 수 없는 경우에 유용합니다.
   - Reset Store Failure Count(저장 실패 카운트 재설정): 저장소 오류에 대한 카운터를 재설정합니다. ARVF(Store Failure) 알람을 소거하는 데 사용할 수 있습니다.
5. Apply Changes * 를 선택합니다.

관련 정보

TSM 서버가 용량에 도달하면 아카이브 노드를 관리합니다

TSM 서버가 용량에 도달하면 아카이브 노드를 관리합니다

TSM 서버에서 관리하는 TSM 데이터베이스나 아카이브 미디어 스토리지가 용량에 근접하는 경우 TSM 서버에서 아카이브 노드를 알릴 수 없습니다. TSM 서버의 사전 모니터링을 통해 이러한 상황을 방지할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

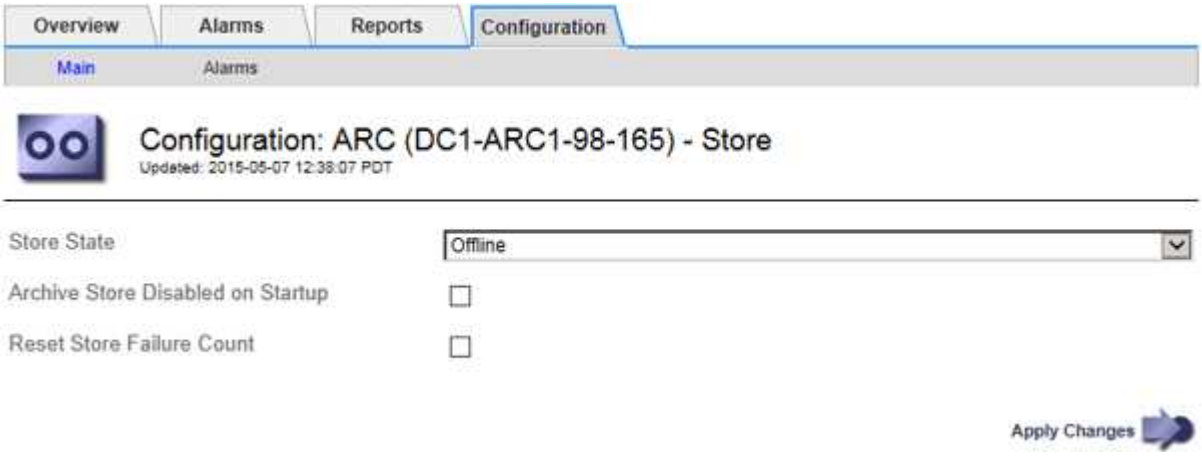
아카이브 노드는 TSM 서버가 새 컨텐츠 수신을 중지한 후에도 TSM 서버로 전송하기 위한 객체 데이터를 계속 수락합니다. 이 콘텐츠는 TSM 서버에서 관리하는 미디어에 쓸 수 없습니다. 이 경우 알람이 트리거됩니다.

ARC 서비스가 **TSM** 서버로 콘텐츠를 전송하지 않도록 합니다

ARC 서비스가 TSM 서버로 추가 콘텐츠를 전송하지 않도록 하려면 * ARC * > * Store * 구성 요소를 오프라인으로 전환하여 아카이브 노드를 오프라인으로 전환할 수 있습니다. 이 절차는 TSM 서버를 유지 보수할 수 없는 경우 알람을 방지하는 데에도 유용할 수 있습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node_ * > * ARC * > * Store * 를 선택합니다.
3. Configuration * > * Main * 을 선택합니다.



4. Store State * 를 Offline 으로 변경합니다.
5. 시작 시 * 아카이브 저장소 사용 안 함 * 을 선택합니다.
6. Apply Changes * 를 선택합니다.

TSM 미들웨어가 용량에 도달하면 아카이브 노드를 읽기 전용으로 설정합니다

대상 TSM 미들웨어 서버가 용량에 도달하면 아카이브 노드를 최적화하여 검색을 수행할 수 있습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node_ * > * ARC * > * Target * 을 선택합니다.
3. Configuration * > * Main * 을 선택합니다.
4. 최대 검색 세션을 세션 수에 나열된 동시 세션 수와 동일하게 변경합니다.
5. 최대 저장 세션을 0으로 변경합니다.

> 아카이브 노드가 읽기 전용인 경우 최대 저장소 세션을 0으로 변경할 필요가 없습니다. 저장 세션이 생성되지 않습니다.

6. Apply Changes * 를 선택합니다.

아카이브 노드 검색 설정을 구성합니다

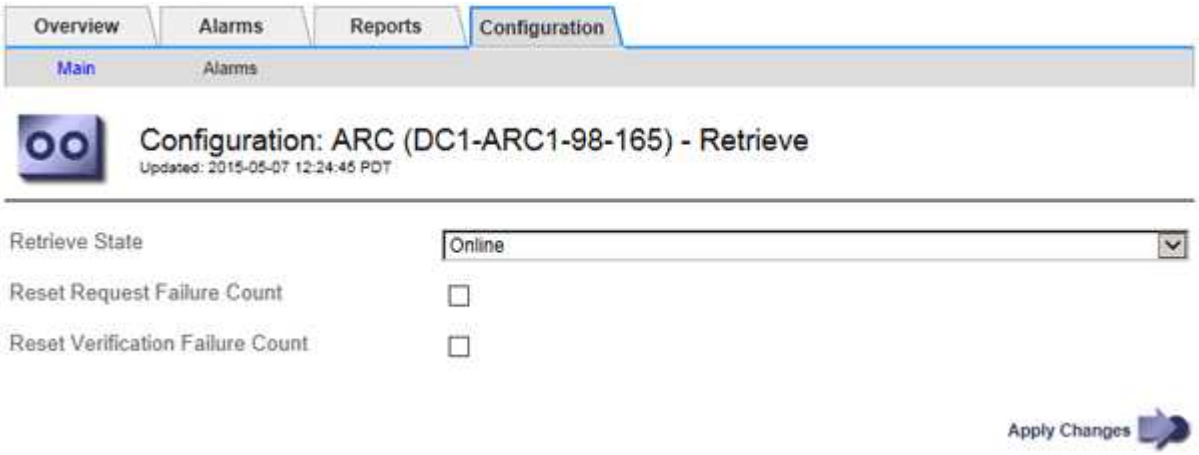
아카이브 노드의 검색 설정을 구성하여 상태를 온라인 또는 오프라인으로 설정하거나 관련 알람에 대해 추적되는 실패 수를 재설정할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node * > * ARC * > * Retrieve * 를 선택합니다.
3. Configuration * > * Main * 을 선택합니다.



4. 필요에 따라 다음 설정을 수정합니다.
   - * 상태 검색 *: 구성 요소 상태를 다음 중 하나로 설정합니다.
     - 온라인: 그리드 노드를 사용하여 보관 미디어 장치에서 오브젝트 데이터를 검색할 수 있습니다.
     - 오프라인: 그리드 노드를 사용하여 오브젝트 데이터를 검색할 수 없습니다.
   - Reset Request Failures Count(요청 실패 카운트 재설정): 요청 실패에 대한 카운터를 재설정하려면 확인란을 선택합니다. ARRF(Request Failures) 알람을 소거하는 데 사용할 수 있습니다.
   - 검증 실패 카운트 재설정: 체크 박스를 선택하면 검색된 개체 데이터에 대한 검증 실패 시 카운터가 재설정됩니다. 이는 ARRV (Verification Failures) 알람을 지우는 데 사용할 수 있습니다.
5. Apply Changes * 를 선택합니다.

아카이브 노드 복제를 구성합니다

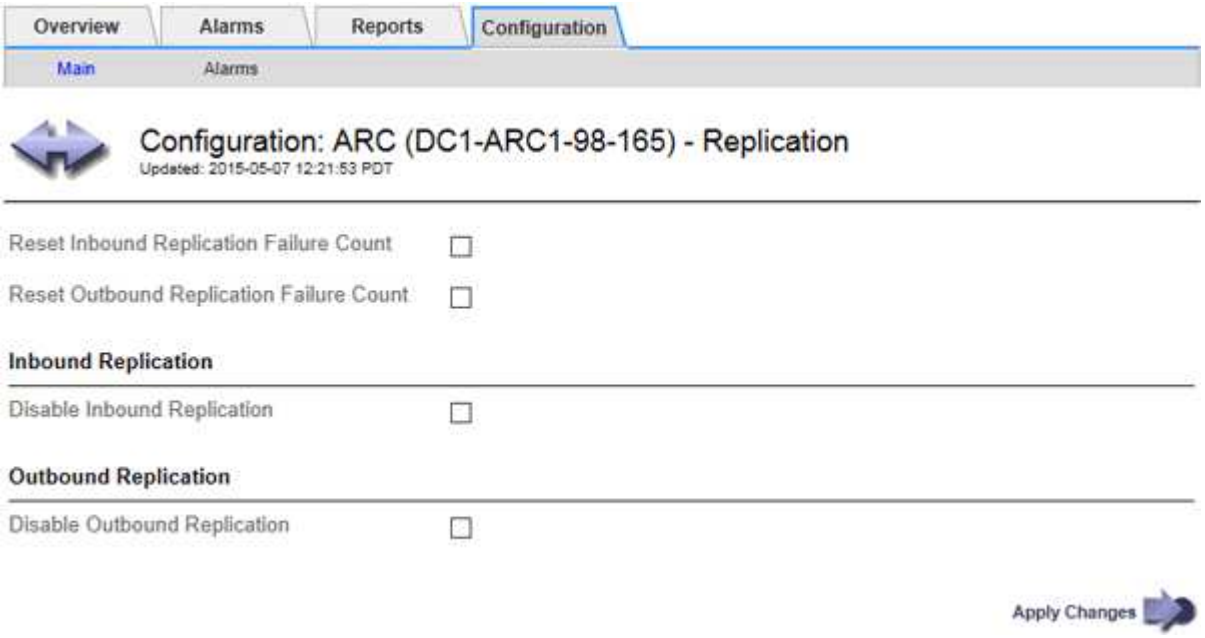
아카이브 노드에 대한 복제 설정을 구성하고 인바운드 및 아웃바운드 복제를 비활성화하거나 관련 알람에 대해 추적되는 실패 수를 재설정할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node_ * > * ARC * > * Replication * 을 선택합니다.
3. Configuration * > * Main * 을 선택합니다.



4. 필요에 따라 다음 설정을 수정합니다.
   - * 인바운드 복제 실패 횟수 재설정 *: 인바운드 복제 실패에 대한 카운터를 재설정하려면 선택합니다. RIRF(인바운드 복제 - - 실패) 경보를 지우는 데 사용할 수 있습니다.
   - * 아웃바운드 복제 실패 횟수 재설정 *: 아웃바운드 복제 실패에 대한 카운터를 재설정하려면 선택합니다. RORF(아웃바운드 복제 - - 실패) 경보를 지우는 데 사용할 수 있습니다.
   - * 인바운드 복제 비활성화 *: 유지 관리 또는 테스트 절차의 일부로 인바운드 복제를 비활성화하려면 선택합니다. 정상 작동 중에 선택을 취소합니다.

     인바운드 복제가 비활성화된 경우 StorageGRID 시스템의 다른 위치로 복제하기 위해 ARC 서비스에서 개체 데이터를 검색할 수 있지만 다른 시스템 위치에서 이 ARC 서비스로 개체를 복제할 수는 없습니다. ARC 서비스는 읽기 전용입니다.

   - * 아웃바운드 복제 비활성화 *: 유지 관리 또는 테스트 절차의 일환으로 아웃바운드 복제(HTTP 검색을 위한 콘텐츠 요청 포함)를 비활성화하려면 이 확인란을 선택합니다. 정상 작동 중에 선택하지 않은 상태로 둡니다.

     아웃바운드 복제를 비활성화하면 개체 데이터를 이 ARC 서비스로 복사하여 ILM 규칙을 충족할 수 있지만, StorageGRID 시스템의 다른 위치로 복제하기 위해 ARC 서비스에서 개체 데이터를 검색할 수는 없습니다. ARC 서비스는 쓰기 전용입니다.

5. Apply Changes * 를 선택합니다.

보관 노드에 대한 사용자 정의 경보를 설정합니다

아카이브 노드에서 아카이브 스토리지 시스템의 객체 데이터 검색 속도와 효율성을 모니터링하는 데 사용되는 ARQL 및 ARRL 속성에 대한 사용자 지정 경보를 설정해야 합니다.

- ARQL:평균 대기열 길이. 오브젝트 데이터가 아카이브 스토리지 시스템에서 검색을 위해 대기할 때까지 걸리는 평균 시간(마이크로초)입니다.
- ARRL: 평균 요청 지연 시간 아카이브 노드에서 아카이브 스토리지 시스템의 오브젝트 데이터를 검색하는 데 필요한 평균 시간(마이크로초)입니다.

이러한 속성에 허용되는 값은 아카이브 스토리지 시스템의 구성 및 사용 방식에 따라 달라집니다. (* ARC * > * Retrieve * > * Overview * > * Main * 로 이동합니다.) 요청 시간 초과 및 검색 요청에 사용할 수 있는 세션 수에 대해 설정된 값은 특히 영향을 줍니다.

통합이 완료된 후 아카이브 노드의 오브젝트 데이터 검색을 모니터링하여 일반적인 검색 시간 및 대기열 길이 값을 설정합니다. 그런 다음 비정상적인 작동 조건이 발생할 경우 트리거되는 ARQL 및 ARRL에 대한 사용자 지정 알람을 생성합니다. 을 참조하십시오 모니터링하고 문제를 해결합니다.

Tivoli Storage Manager 통합

아카이브 노드 구성 및 작업

StorageGRID 시스템은 아카이브 노드를 무기한으로 저장되고 항상 액세스할 수 있는 위치로 관리합니다.

오브젝트가 수집되면 StorageGRID 시스템에 정의된 ILM(정보 수명 주기 관리) 규칙에 따라 아카이브 노드를 비롯한 모든 필요한 위치에 복사본이 만들어집니다. 아카이브 노드는 TSM 서버에 대한 클라이언트 역할을 하며 TSM 클라이언트 라이브러리는 StorageGRID 소프트웨어 설치 프로세스에 의해 아카이브 노드에 설치됩니다. 스토리지의 아카이브 노드에 대한 객체 데이터는 수신된 TSM 서버에 직접 저장됩니다. 아카이브 노드는 TSM 서버에 저장하기 전에 객체 데이터를 스테이징하지 않으며 객체 집계를 수행하지 않습니다. 그러나 데이터 속도가 필요한 경우 아카이브 노드는 하나의 트랜잭션에서 TSM 서버에 여러 복제본을 제출할 수 있습니다.

아카이브 노드가 TSM 서버에 객체 데이터를 저장한 후 TSM 서버에서 해당 수명주기/보존 정책을 사용하여 객체 데이터를 관리합니다. 이러한 보존 정책은 아카이브 노드의 작업과 호환되도록 정의해야 합니다. 즉, 아카이브 노드에서 저장한 개체 데이터는 보관 노드에서 삭제하지 않는 한 영구적으로 저장해야 하며 항상 아카이브 노드에서 액세스할 수 있어야 합니다.

StorageGRID 시스템의 ILM 규칙과 TSM 서버의 수명주기/보존 정책 간에는 연결이 없습니다. 각 개체는 서로 독립적으로 작동하지만, 각 개체는 StorageGRID 시스템으로 수집되므로 TSM 관리 클래스를 할당할 수 있습니다. 이 관리 클래스는 객체 데이터와 함께 TSM 서버로 전달됩니다. 여러 객체 유형에 서로 다른 관리 클래스를 할당하면 TSM 서버가 서로 다른 스토리지 풀에 객체 데이터를 배치하도록 구성하거나 필요에 따라 다른 마이그레이션 또는 보존 정책을 적용하도록 구성할 수 있습니다. 예를 들어 데이터베이스 백업으로 식별된 개체(최신 데이터로 덮어쓸 수 있는 임시 콘텐츠)는 응용 프로그램 데이터(영구적으로 보존해야 하는 고정 콘텐츠)와 다르게 처리될 수 있습니다.

아카이브 노드는 새 TSM 서버 또는 기존 TSM 서버와 통합할 수 있으며 전용 TSM 서버가 필요하지 않습니다. TSM 서버의 크기가 최대 예상 로드에 맞게 적절히 지정되면 TSM 서버를 다른 클라이언트와 공유할 수 있습니다. TSM은 아카이브 노드와 분리된 서버 또는 가상 머신에 설치해야 합니다.

동일한 TSM 서버에 쓰기 위해 아카이브 노드를 두 개 이상 구성할 수 있지만 아카이브 노드가 서로 다른 데이터 세트를 TSM 서버에 쓰는 경우에만 이 구성이 권장됩니다. 각 아카이브 노드가 동일한 객체 데이터의 복제본을 아카이브에 쓸 때 동일한 TSM 서버에 쓰기 위해 아카이브 노드를 두 개 이상 구성하는 것은 권장되지 않습니다. 두 복제본 모두 독립적인 중복 객체 데이터 복제본에 대해 단일 장애 지점(TSM 서버)에 해당합니다.

아카이브 노드는 TSM의 HSM(Hierarchical Storage Management) 구성 요소를 사용하지 않습니다.

TSM 서버를 사이징하고 구성할 때는 아카이브 노드와 함께 작동하도록 최적화하기 위해 이를 최적화하는 모범 사례를 적용해야 합니다.

TSM 서버를 사이징하고 구성할 때는 다음 요소를 고려해야 합니다.

- 아카이브 노드는 TSM 서버에 저장하기 전에 객체를 집계하지 않기 때문에 아카이브 노드에 기록될 모든 객체에 대한 참조를 보유할 수 있도록 TSM 데이터베이스의 크기를 조정해야 합니다.
- 아카이브 노드 소프트웨어는 테이프 또는 기타 이동식 미디어에 직접 개체를 쓰는 데 수반되는 지연 시간을 허용할 수 없습니다. 따라서 이동식 미디어를 사용할 때마다 아카이브 노드에서 저장한 데이터의 초기 스토리지를 위해 TSM 서버를 디스크 스토리지 풀로 구성해야 합니다.
- 이벤트 기반 보존을 사용하려면 TSM 보존 정책을 구성해야 합니다. 아카이브 노드는 생성 기반 TSM 보존 정책을 지원하지 않습니다. 보존 정책에서 retmin=0 및 retver=0의 권장 설정을 사용합니다. 보존 정책은 보관 노드가 보존 이벤트를 트리거할 때 보존이 시작되고 그 후 0일 동안 유지됨을 나타냅니다. 그러나 retmin 및 retver에 대한 이러한 값은 선택 사항입니다.

데이터를 테이프 풀로 마이그레이션하도록 디스크 풀을 구성해야 합니다. 즉, 테이프 풀은 디스크 풀의 NXTSTOOL이어야 합니다. 테이프 풀은 두 풀에 동시에 쓰는 디스크 풀의 복제 풀로 구성해서는 안 됩니다. 즉, 테이프 풀은 디스크 풀의 COPYSTGPOOL이 될 수 없습니다. 아카이브 노드 데이터를 포함하는 테이프의 오프라인 복사본을 생성하려면 아카이브 노드 데이터에 사용되는 테이프 풀의 복사본 풀인 두 번째 테이프 풀을 사용하여 TSM 서버를 구성합니다.

아카이브 노드 설정을 완료합니다

설치 프로세스를 완료한 후에는 아카이브 노드가 작동하지 않습니다. StorageGRID 시스템에서 TSM 아카이브 노드에 객체를 저장하려면 먼저 TSM 서버의 설치 및 구성을 완료하고 TSM 서버와 통신하도록 아카이브 노드를 구성해야 합니다.

StorageGRID 시스템에서 아카이브 노드와 통합되도록 TSM 서버를 준비할 때 필요한 경우 다음 IBM 설명서를 참조하십시오.

- "IBM 테이프 장치 드라이버 설치 및 사용 설명서"
- "IBM 테이프 장치 드라이버 프로그래밍 참조"

새 **TSM** 서버를 설치합니다

아카이브 노드를 새 TSM 서버 또는 기존 TSM 서버와 통합할 수 있습니다. 새 TSM 서버를 설치하는 경우 TSM 설명서의 지침에 따라 설치를 완료합니다.

> 아카이브 노드는 TSM 서버와 함께 호스팅할 수 없습니다.

TSM 서버를 구성합니다

이 섹션에서는 TSM Best Practice에 따라 TSM 서버를 준비하는 방법에 대한 샘플 지침을 제공합니다.

다음 지침은 의 프로세스를 안내합니다.

- TSM 서버에서 디스크 스토리지 풀 및 테이프 스토리지 풀(필요한 경우) 정의
- 아카이브 노드에서 저장된 데이터에 대해 TSM 관리 클래스를 사용하는 도메인 정책을 정의하고 이 도메인 정책을 사용하도록 노드를 등록합니다

이 지침은 참조용으로만 제공됩니다. TSM 설명서를 교체하거나 모든 구성에 적합한 완전하고 포괄적인 지침을 제공하기 위한 지침은 아닙니다. 자세한 요구 사항 및 전체 TSM 서버 설명서를 모두 숙지한 TSM 관리자가 배포별 지침을 제공해야 합니다.

TSM 테이프 및 디스크 스토리지 풀을 정의합니다

아카이브 노드는 디스크 스토리지 풀에 씁니다. 콘텐츠를 테이프에 아카이빙하려면 테이프 스토리지 풀로 콘텐츠를 이동하도록 디스크 스토리지 풀을 구성해야 합니다.

이 작업에 대해

TSM 서버의 경우 Tivoli Storage Manager 내에서 테이프 스토리지 풀과 디스크 스토리지 풀을 정의해야 합니다. 디스크 풀을 정의한 후 디스크 볼륨을 생성하여 디스크 풀에 할당합니다. TSM 서버에서 디스크 전용 스토리지를 사용하는 경우에는 테이프 풀이 필요하지 않습니다.

테이프 스토리지 풀을 생성하려면 TSM 서버에서 여러 단계를 완료해야 합니다. 테이프 라이브러리와 테이프 라이브러리에 하나 이상의 드라이브를 만듭니다. 서버에서 라이브러리까지, 서버에서 드라이브까지 경로를 정의한 다음 드라이브의 디바이스 클래스를 정의합니다.) 이러한 단계에 대한 자세한 내용은 사이트의 하드웨어 구성 및 스토리지 요구 사항에 따라 다를 수 있습니다. 자세한 내용은 TSM 설명서를 참조하십시오.

다음 지침은 프로세스를 보여 줍니다. 사이트 요구 사항은 배포 요구 사항에 따라 다를 수 있습니다. 구성 세부 정보 및 지침은 TSM 설명서를 참조하십시오.

관리자 권한으로 서버에 로그온하고 dsmadmc 도구를 사용하여 다음 명령을 실행해야 합니다.

단계

1. 테이프 라이브러리를 생성합니다.

   Define library_tapelibrary_libtype=*scsi*

   여기서, '*tapelibrary*'는 테이프 라이브러리에 대해 선택한 임의 이름이고 libtype의 값은 테이프 라이브러리 유형에 따라 다를 수 있습니다.

2. 서버에서 테이프 라이브러리로의 경로를 정의합니다.

   Define path_servername tapelibrary_srctype=server desttype=library device=*lib-devicename*'

   - '*servername*'은 TSM 서버의 이름입니다
   - '*tapelibrary*'는 사용자가 정의한 테이프 라이브러리 이름입니다
   - 테이프 라이브러리의 디바이스 이름은 '*lib-devicename*'입니다

3. 라이브러리의 드라이브를 정의합니다.

   Define drive_tapelibrary__drivename _

   - '*drivename*'은 드라이브에 지정할 이름입니다
   - '*tapelibrary*'는 사용자가 정의한 테이프 라이브러리 이름입니다

하드웨어 구성에 따라 추가 드라이브 또는 드라이브를 구성할 수 있습니다. 예를 들어 TSM 서버가 테이프 라이브러리에서 두 개의 입력이 있는 Fibre Channel 스위치에 연결되어 있는 경우 각 입력에 대해 드라이브를 정의할 수 있습니다.

4. 서버에서 정의한 드라이브까지의 경로를 정의합니다.

   Define path_servername_drivename srctype=server desttype=드라이브 라이브러리 =*tapelibrary_device=_drive-dname*"

   - '*drive-dname*'은(는) 드라이브의 장치 이름입니다
   - '*tapelibrary*'는 사용자가 정의한 테이프 라이브러리 이름입니다

     각 드라이브에 대해 별도의 '*drivename*' 및 '*drive-dname*'을 사용하여 테이프 라이브러리에 대해 정의한 각 드라이브에 대해 이 과정을 반복합니다.

5. 드라이브의 디바이스 클래스를 정의합니다.

   define devclass_DeviceClassName_devtype=*LTO_library=_tapelibrary_format=_tapetype*'

   - '*DeviceClassName*'은 장치 클래스의 이름입니다
   - '*LTO*'는 서버에 연결된 드라이브 유형입니다
   - '*tapelibrary*'는 사용자가 정의한 테이프 라이브러리 이름입니다
   - '*tapetype*'은(는) 테이프 유형입니다(예: ultri3)

6. 라이브러리의 인벤토리에 테이프 볼륨을 추가합니다.

   'checkin libvolume_tapelibrary_'

   '*tapelibrary*'는 사용자가 정의한 테이프 라이브러리 이름입니다.

7. 운영 테이프 스토리지 풀을 생성합니다.

   Define stgpool_SGWSTapePool*DeviceClassName_description = descriptioncollocate=filespace_maxscratch=_XX*'입니다

   - '*SGWSTapePool*'은 아카이브 노드의 테이프 스토리지 풀의 이름입니다. 이름이 TSM 서버에서 예상하는 구문 규칙을 사용하는 경우 테이프 스토리지 풀의 이름을 선택할 수 있습니다.
   - '*DeviceClassName*'은 테이프 라이브러리의 디바이스 클래스 이름입니다.
   - '*description*'은 'query stgpool' 명령을 사용하여 TSM 서버에 표시할 수 있는 스토리지 풀에 대한 설명입니다. 예: ""아카이브 노드의 테이프 스토리지 풀""
   - '*collocate=filespace*'는 TSM 서버가 동일한 파일 공간의 객체를 단일 테이프에 기록하도록 지정합니다.
   - 'XX'는 다음 중 하나입니다.
     - 테이프 라이브러리의 빈 테이프 수(라이브러리를 사용하는 유일한 애플리케이션인 경우)
     - StorageGRID 시스템에서 사용하도록 할당된 테이프 수(테이프 라이브러리가 공유되는 경우)

8. TSM 서버에서 디스크 스토리지 풀을 생성합니다. TSM 서버의 관리 콘솔에서 를 입력합니다

   define stgpool_SGWSDiskPool_DISK DESCRIPTION=*DESCRIPTION_maxsize=_maximum_file_size nextstgpool=SGWSTapePool_highmig=_percent_high_lowmig=_percent_low*'입니다

- '*SGWSDiskPool*'은 아카이브 노드의 디스크 풀 이름입니다. 이름이 TSM에서 예상하는 구문 규칙을 사용하는 경우 디스크 스토리지 풀의 이름을 선택할 수 있습니다.
- '*description*'은 'query stgpool' 명령을 사용하여 TSM 서버에 표시할 수 있는 스토리지 풀에 대한 설명입니다. 예: "아카이브 노드의 경우 디스크 스토리지 풀""
- '*maximum_file_size*'는 디스크 풀에 캐시되지 않고 이 크기보다 큰 객체를 테이프에 직접 쓰도록 합니다. '*maximum_file_size*'를 10GB로 설정하는 것이 좋습니다.
- '*nextstgpool=SGWSTapePool*'은 디스크 스토리지 풀을 아카이브 노드에 대해 정의된 테이프 스토리지 풀로 나타냅니다.
- '*%_high*'는 디스크 풀의 내용을 테이프 풀로 마이그레이션하는 데 사용되는 값을 설정합니다. 데이터 마이그레이션이 즉시 시작될 수 있도록 '*%_high*'를 0으로 설정하는 것이 좋습니다
- '*%_low*' 테이프 풀로의 마이그레이션이 중지되는 값을 설정합니다. 디스크 풀을 지우려면 '_ percent_low_'를 0으로 설정하는 것이 좋습니다.

9. TSM 서버에서 디스크 볼륨(또는 볼륨)을 생성하여 디스크 풀에 할당합니다.

   Define volume_SGWSDiskPool__volume_name_formatsize=*size*'

   - '*SGWSDiskPool*'은(는) 디스크 풀 이름입니다.
   - '*VOLUME_NAME*'은(는) 테이프 전송을 준비하기 위해 디스크 풀의 내용을 쓰는 TSM 서버의 볼륨 위치(예: '/var/local/arc/stage6.dsm')에 대한 전체 경로입니다.
   - '*size*'는 디스크 볼륨의 크기(MB)입니다.

     예를 들어, 디스크 풀의 컨텐츠가 단일 테이프를 채우도록 단일 디스크 볼륨을 생성하려면 테이프 볼륨의 용량이 200GB인 경우 크기 값을 200000으로 설정합니다.

     그러나 TSM 서버가 디스크 풀의 각 볼륨에 쓸 수 있으므로 더 작은 크기의 여러 디스크 볼륨을 생성하는 것이 좋습니다. 예를 들어 테이프 크기가 250GB인 경우 각각 10GB(10000)의 크기로 25개의 디스크 볼륨을 생성합니다.

   TSM 서버는 디스크 볼륨의 디렉토리에 공간을 사전 할당합니다. 완료하는 데 시간이 걸릴 수 있습니다(200GB 디스크 볼륨의 경우 3시간 이상).

도메인 정책을 정의하고 노드를 등록합니다

아카이브 노드에서 저장된 데이터에 대해 TSM 관리 클래스를 사용하는 도메인 정책을 정의한 다음 이 도메인 정책을 사용하도록 노드를 등록해야 합니다.

> TSM(Tivoli Storage Manager)의 아카이브 노드에 대한 클라이언트 암호가 만료되면 아카이브 노드 프로세스에서 메모리가 누수될 수 있습니다. 아카이브 노드의 클라이언트 사용자 이름/암호가 만료되지 않도록 TSM 서버가 구성되어 있는지 확인합니다.

아카이브 노드를 사용하거나 기존 노드를 업데이트하기 위해 TSM 서버에 노드를 등록할 때 MAXNUMMP 매개 변수를 REGISTER NODE 명령에 지정하여 쓰기 작업에 사용할 수 있는 마운트 지점의 수를 지정해야 합니다. 마운트 지점의 수는 일반적으로 아카이브 노드에 할당된 테이프 드라이브 헤드의 수와 같습니다. TSM 서버의 MAXNUMMP에 지정된 숫자는 최소한 * ARC * > * Target * > * Configuration * > * Main * > * Maximum Store Sessions * 에 설정된 값보다 큰 값이어야 합니다. 동시 저장소 세션은 아카이브 노드에서 지원되지 않으므로 0 또는 1 값으로 설정됩니다.

TSM 서버에 대해 설정된 MAXSESSIONS 값은 모든 클라이언트 애플리케이션이 TSM 서버에 열 수 있는 최대 세션

수를 제어합니다. TSM에 지정된 MAXSESSIONS 값은 아카이브 노드의 Grid Manager에서 * ARC * > * Target * > * Configuration * > * Main * > * Number of Sessions * 에 지정된 값보다 크거나 같아야 합니다. 아카이브 노드는 마운트 지점당 최대 하나의 세션과 작은 수의(<5) 추가 세션을 동시에 생성합니다.

아카이브 노드에 할당된 TSM 노드는 맞춤형 도메인 정책 'TSM-DOMAIN'을 사용합니다. TSM-DOMAIN 도메인 정책은 테이프에 기록하고 아카이브 대상이 StorageGRID 시스템의 스토리지 풀(_ SGWSDiskPool_)으로 설정된 "표준" 도메인 정책의 수정된 버전입니다.

> 관리자 권한으로 TSM 서버에 로그인하고 dsmadmc 도구를 사용하여 도메인 정책을 생성하고 활성화해야 합니다.

도메인 정책을 만들고 활성화합니다

아카이브 노드에서 전송된 데이터를 저장하도록 TSM 서버를 구성하려면 도메인 정책을 생성한 다음 활성화해야 합니다.

단계

1. 도메인 정책을 생성합니다.

   도메인 표준 TSM-DOMAIN 복사

2. 기존 관리 클래스를 사용하지 않는 경우 다음 중 하나를 입력합니다.

   '정책 세트 TSM-도메인 표준'

   Define mgmtd class TSM-domain standard_default_'입니다

   '*default*'는 배포의 기본 관리 클래스입니다.

3. 적절한 스토리지 풀에 카피그룹을 생성합니다. 입력(한 줄에):

   define copygroup TSM-domain standard_default_type=archive destination=SGWSDiskPool retinit=event retmin=0 retver=0"입니다

   아카이브 노드의 기본 관리 클래스는 '*default*'입니다. 현재 Archive Node에서 사용하는 보존 동작을 반영하기 위해 'retinit', 'retmin', 'reTver' 값이 선택되었습니다

   > 이 재설정을 retinit=create로 설정하지 마십시오. retinit=create를 설정하면 TSM 서버에서 컨텐츠를 제거하는 데 보존 이벤트가 사용되므로 아카이브 노드가 콘텐츠를 삭제하지 못하도록 차단합니다.

4. 관리 클래스를 기본값으로 할당합니다.

   "defmgmtd_TSM-domain_standard_default_ 할당'

5. 새 정책 세트를 활성으로 설정합니다.

   '정책 세트 TSM-도메인 표준 활성화

   activate 명령을 입력할 때 나타나는 ""백업 복사 그룹 없음"" 경고는 무시하십시오.

6. TSM 서버에 설정된 새 정책을 사용하려면 노드를 등록합니다. TSM 서버에서 (한 줄에) 다음을 입력합니다.

   노드 arc-user arc-password passexp=0 domain=TSM-domain MAXNUMMP=세션 수'입니다

   arc-user 및 arc-password는 Archive Node에서 정의한 클라이언트 노드 이름 및 암호와 동일하며, MAXNUMMP 값은 Archive Node store 세션에 예약된 테이프 드라이브 수로 설정됩니다.

   > 기본적으로 노드를 등록하면 노드에 대해 정의된 암호를 사용하여 클라이언트 소유자 권한에 관리 사용자 ID가 생성됩니다.

데이터를 **StorageGRID**로 마이그레이션

대량의 데이터를 StorageGRID 시스템으로 마이그레이션하는 동시에 일상적인 작업을 위해 StorageGRID 시스템을 사용할 수 있습니다.

다음 섹션에서는 대량의 데이터를 StorageGRID 시스템으로 마이그레이션하는 방법을 이해하고 계획하는 방법을 안내합니다. 이 가이드는 데이터 마이그레이션의 일반적인 가이드가 아니며 마이그레이션을 수행하기 위한 자세한 단계는 포함되어 있지 않습니다. 이 섹션의 지침과 지침을 따라 일상적인 작업을 방해하지 않으면서 데이터가 StorageGRID 시스템으로 효율적으로 마이그레이션되고 마이그레이션된 데이터가 StorageGRID 시스템에서 적절하게 처리되도록 하십시오.

StorageGRID 시스템의 용량을 확인합니다

대량의 데이터를 StorageGRID 시스템으로 마이그레이션하기 전에 StorageGRID 시스템에 예상되는 볼륨을 처리할 수 있는 디스크 용량이 있는지 확인하십시오.

StorageGRID 시스템에 아카이브 노드가 포함되어 있고 마이그레이션된 객체의 복제본이 니어라인 스토리지(예: 테이프)에 저장된 경우 아카이브 노드의 스토리지가 마이그레이션된 데이터의 예상 볼륨에 충분한 용량을 가지고 있는지 확인하십시오.

용량 평가의 일환으로 마이그레이션할 객체의 데이터 프로파일을 살펴보고 필요한 디스크 용량을 계산합니다. StorageGRID 시스템의 디스크 용량을 모니터링하는 방법에 대한 자세한 내용은 을 참조하십시오 스토리지 노드 관리 및 모니터링하고 문제를 해결합니다.

마이그레이션된 데이터에 대한 **ILM** 정책을 결정합니다

StorageGRID 시스템의 ILM 정책은 복사본 수, 복사본이 저장되는 위치 및 복사본 보유 기간을 결정합니다. ILM 정책은 시간 경과에 따라 개체를 필터링하고 개체 데이터를 관리하는 방법을 설명하는 ILM 규칙 집합으로 구성되어 있습니다.

마이그레이션된 데이터의 사용 방법과 마이그레이션된 데이터의 요구 사항에 따라 일상적인 작업에 사용되는 ILM 규칙과 다른 마이그레이션 데이터에 대한 고유한 ILM 규칙을 정의할 수 있습니다. 예를 들어, 마이그레이션에 포함된 데이터에 대한 규정 요구사항과 일상적인 데이터 관리에 대한 규정 요구사항이 서로 다른 경우 다른 등급의 스토리지에 마이그레이션된 데이터의 복사본을 여러 개 만들어야 할 수 있습니다.

마이그레이션된 데이터와 일상적인 작업과 저장된 오브젝트 데이터를 고유하게 구분할 수 있는 경우 마이그레이션된 데이터에만 적용되는 규칙을 구성할 수 있습니다.

메타데이터 기준 중 하나를 사용하여 데이터 유형을 안정적으로 구분할 수 있는 경우, 이 기준을 사용하여 마이그레이션된 데이터에만 적용되는 ILM 규칙을 정의할 수 있습니다.

데이터 마이그레이션을 시작하기 전에 StorageGRID 시스템의 ILM 정책과 마이그레이션 데이터에 적용되는 방법을 이해하고 ILM 정책에 대한 모든 변경 사항을 적용 및 테스트해야 합니다. 을 참조하십시오 ILM을 사용하여 개체를 관리합니다.

> 잘못 지정된 ILM 정책으로 인해 복구할 수 없는 데이터 손실이 발생할 수 있습니다. ILM 정책을 활성화하기 전에 변경한 모든 내용을 주의 깊게 검토하여 정책이 의도한 대로 작동하는지 확인합니다.

마이그레이션이 운영에 미치는 영향

StorageGRID 시스템은 오브젝트 스토리지 및 검색을 위한 효율적인 작업을 제공하고 오브젝트 데이터 및 메타데이터의 중복 복사본을 지속적으로 생성하여 데이터 손실로부터 데이터를 완벽하게 보호하도록 설계되었습니다.

그러나 일상적인 시스템 운영에 영향을 주지 않도록 이 장의 지침에 따라 데이터 마이그레이션을 주의 깊게 관리해야 합니다. 그렇지 않을 경우, 극단적인 경우 StorageGRID 시스템에 장애가 발생할 경우 데이터가 손실될 위험이 있습니다.

대량의 데이터를 마이그레이션하면 시스템에 추가 부하가 걸린 것입니다. StorageGRID 시스템이 로드가 많은 경우 객체를 저장하고 검색하는 요청에 더 느리게 응답합니다. 이로 인해 일상적인 작업에 필수적인 저장 및 검색 요청이 방해를 받을 수 있습니다. 마이그레이션으로 인해 다른 운영 문제가 발생할 수도 있습니다. 예를 들어, 스토리지 노드의 용량이 거의 다 되면 배치 수집으로 인한 과중한 간헐적 로드로 인해 스토리지 노드가 읽기 전용과 읽기-쓰기 간에 순환되어 알림을 생성할 수 있습니다.

로드가 많은 경우 큐는 StorageGRID 시스템에서 수행하는 다양한 작업에 대해 개발되어 오브젝트 데이터 및 메타데이터의 완전한 이중화를 보장할 수 있습니다.

마이그레이션 중에 StorageGRID 시스템을 안전하고 효율적으로 운영할 수 있도록 이 문서의 지침에 따라 데이터 마이그레이션을 신중하게 관리해야 합니다. 데이터를 마이그레이션할 때는 오브젝트를 일괄적으로 수집하거나 지속적으로 스로틀로 인제스트합니다. 그런 다음 StorageGRID 시스템을 지속적으로 모니터링하여 다양한 속성 값을 초과하지 않는지 확인합니다.

데이터 마이그레이션 예약 및 모니터링

필요한 기간 내에 ILM 정책에 따라 데이터를 배치할 수 있도록 데이터 마이그레이션을 예약하고 모니터링해야 합니다.

데이터 마이그레이션을 예약합니다

핵심 운영 시간 중에는 데이터 마이그레이션을 하지 마십시오. 시스템 사용량이 적은 야간, 주말 및 기타 시간으로 데이터 마이그레이션을 제한합니다.

가능한 경우 활동이 많은 기간 동안에는 데이터 마이그레이션을 예약하지 마십시오. 그러나 높은 활동 기간을 완전히 피하는 것이 실용적이지 않은 경우에는 관련 특성을 면밀히 모니터링하고 허용 가능한 값을 초과하는 경우 조치를 취하는 한 계속 진행하는 것이 안전합니다.

데이터 마이그레이션을 모니터링합니다

이 표에는 데이터 마이그레이션 중에 모니터링해야 하는 속성과 이러한 특성이 나타내는 문제가 나열되어 있습니다.

트래픽 분류 정책을 사용하여 수집 임계치를 조절할 경우, 다음 표에 설명된 통계와 함께 관찰된 비율을 모니터링하고 필요한 경우 제한을 줄일 수 있습니다.

모니터링	설명
ILM 평가를 기다리는 개체의 수입니다	1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 2. 배포 * > * 개요 * > * 기본 * 을 선택합니다. 3. ILM 활동 섹션에서 다음 특성에 대해 표시된 개체 수를 모니터링합니다. ◦ * Awaiting-all(XQUZ) *: ILM 평가를 기다리는 총 개체 수. ◦ * Awaiting-Client(XCQZ) *: 클라이언트 작업에서 ILM 평가를 기다리는 총 오브젝트 수(예: 수집). 4. 이러한 속성 중 하나에 대해 표시되는 오브젝트 수가 100,000개를 초과할 경우 개체의 수집 속도를 조절하여 StorageGRID 시스템의 로드를 줄입니다.
타겟 아카이브 시스템의 스토리지 용량	ILM 정책이 마이그레이션된 데이터의 복사본을 대상 아카이브 스토리지 시스템(테이프 또는 클라우드)에 저장하는 경우 대상 아카이브 스토리지 시스템의 용량을 모니터링하여 마이그레이션된 데이터에 충분한 용량이 있는지 확인하십시오.
• Archive Node * > * ARC * > * Store *	ARVF(Store Failures) * 속성에 대한 알람이 트리거되면 대상 아카이브 스토리지 시스템의 용량이 한계에 도달했을 수 있습니다. 대상이 되는 아카이브 스토리지 시스템을 확인하고 알람을 트리거한 문제를 모두 해결합니다.

ILM을 사용하여 개체를 관리합니다

ILM을 사용하여 개체 관리: 개요

ILM(정보 수명 주기 관리) 규칙 및 정책을 구성하여 StorageGRID 시스템의 개체를 관리할 수 있습니다. ILM 규칙 및 정책은 StorageGRID이 개체 데이터의 복사본을 만들고 배포하는 방법과 시간이 지남에 따라 이러한 복사본을 관리하는 방법을 지시합니다.

참조하십시오

ILM 규칙 및 ILM 정책을 설계하고 구현하려면 신중한 계획이 필요합니다. 운영 요구사항, StorageGRID 시스템의 토폴로지, 오브젝트 보호 요구사항 및 사용 가능한 스토리지 유형을 이해해야 합니다. 그런 다음 여러 유형의 개체를 복사, 배포 및 저장할 방법을 결정해야 합니다.

다음 지침을 따르십시오.

- ILM이 개체 수명 전반에 걸쳐 작동하는 방식과 ILM 정책 및 규칙이 무엇인지 등 StorageGRID ILM에 대해 알아보십시오.
- 스토리지 풀, 삭제 코딩 프로필 및 ILM 규칙을 구성하는 방법에 대해 알아봅니다.
- 하나 이상의 사이트에서 오브젝트 데이터를 보호하는 ILM 정책을 만들고 활성화하는 방법을 알아보십시오.
- S3 오브젝트 잠금을 통해 오브젝트를 관리하는 방법에 대해 알아보십시오. S3 오브젝트 잠금은 특정 S3 버킷의 오브젝트가 지정된 시간 동안 삭제 또는 덮어쓰지 않도록 보장합니다.

자세한 정보

자세한 내용은 다음 비디오를 참조하십시오.

- "비디오: StorageGRID ILM 규칙: 시작하기"

- "비디오: StorageGRID ILM 정책"

ILM 및 오브젝트 라이프사이클

ILM이 개체 수명 전반에 걸쳐 작동하는 방식

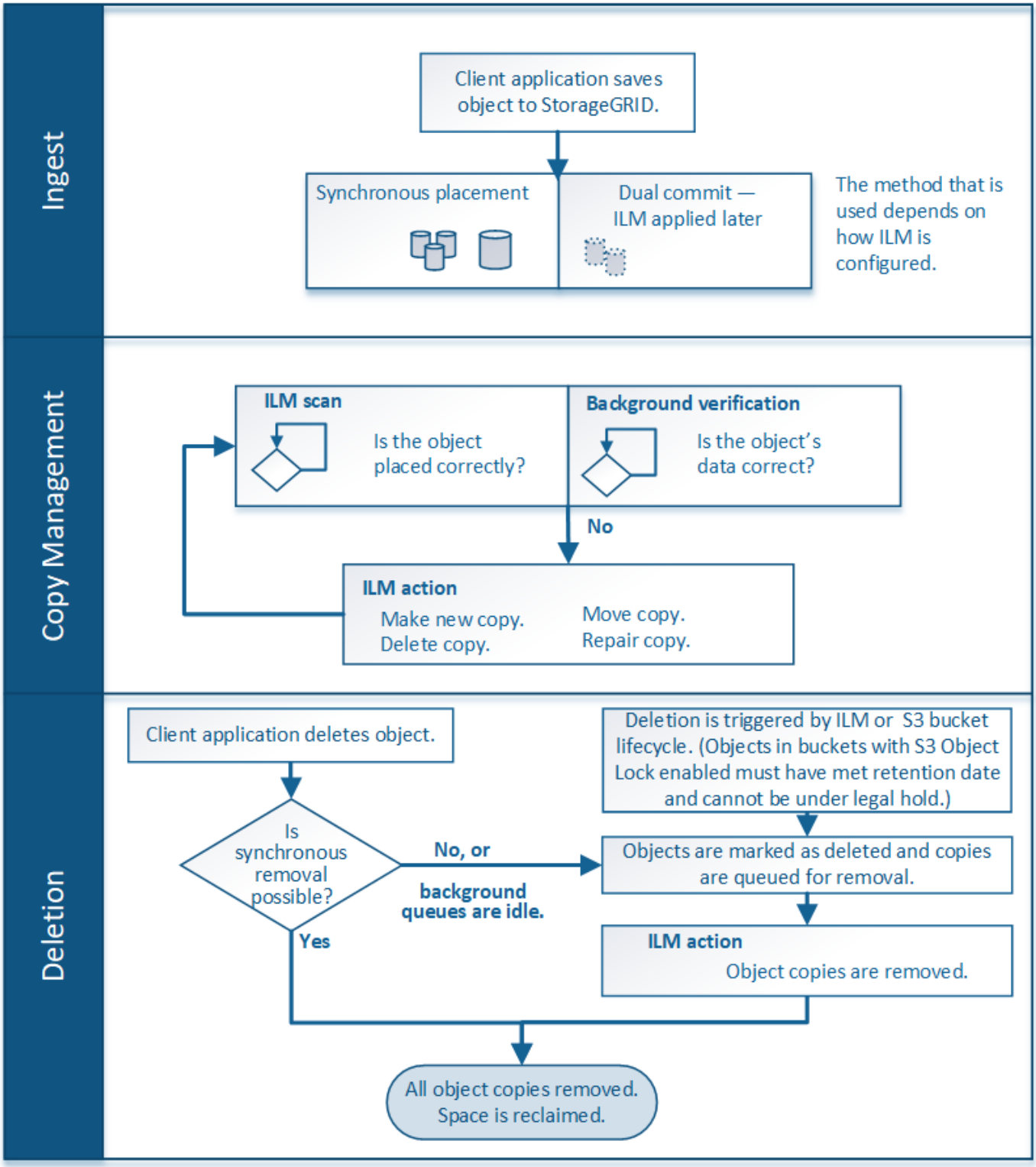
StorageGRID에서 ILM을 사용하여 삶의 모든 단계에서 개체를 관리하는 방법을 이해하면 더 효과적인 정책을 설계하는 데 도움이 됩니다.

- * Ingest *: Ingest는 S3 또는 Swift 클라이언트 응용 프로그램이 StorageGRID 시스템에 개체를 저장하기 위한 연결을 설정할 때 시작되며, StorageGRID가 ""수집 성공" 메시지를 클라이언트에 반환할 때 완료됩니다. ILM 요구 사항이 지정된 방식에 따라 즉시(동기식 배치) ILM 명령을 적용하거나 나중에 ILM(이중 커밋)을 적용하여 수집 중에 오브젝트 데이터를 보호합니다.

- * 복사본 관리 *: ILM의 배치 명령에 지정된 오브젝트 복사본의 수와 유형을 생성한 후 StorageGRID는 오브젝트 위치를 관리하고 개체로부터 손실을 보호합니다.
  - ILM 스캔 및 평가:StorageGRID은 그리드에 저장된 오브젝트 목록을 지속적으로 스캔하고 현재 복사본이 ILM 요구 사항을 충족하는지 확인합니다. 오브젝트 복사본의 유형, 숫자 또는 위치가 서로 다른 경우 StorageGRID은 필요에 따라 복사본을 생성, 삭제 또는 이동합니다.
  - 백그라운드 검증: StorageGRID는 개체 데이터의 무결성을 확인하기 위해 백그라운드 검증을 지속적으로 수행합니다. 문제가 발견되면 StorageGRID는 현재 ILM 요구사항을 충족하는 위치에 새 오브젝트 복사본 또는 삭제 코딩 된 대체 오브젝트 조각을 자동으로 생성합니다. 의 지침을 참조하십시오 StorageGRID 모니터링 및 문제 해결.
- * 개체 삭제 *: StorageGRID 시스템에서 모든 복사본이 제거될 때 개체 관리가 종료됩니다. 클라이언트의 삭제 요청 결과로 또는 ILM에 의한 삭제 또는 S3 버킷 라이프사이클의 만료로 인한 삭제로 인해 오브젝트를 제거할 수 있습니다.

> S3 오브젝트 잠금이 활성화된 버킷의 오브젝트는 법적 증거 자료 보관 중이거나 보존 기한이 지정되었지만 아직 충족되지 않은 경우 삭제할 수 없습니다.

이 다이어그램은 ILM이 개체 수명 주기 동안 어떻게 작동하는지를 요약합니다.



오브젝트를 섭취하는 방법

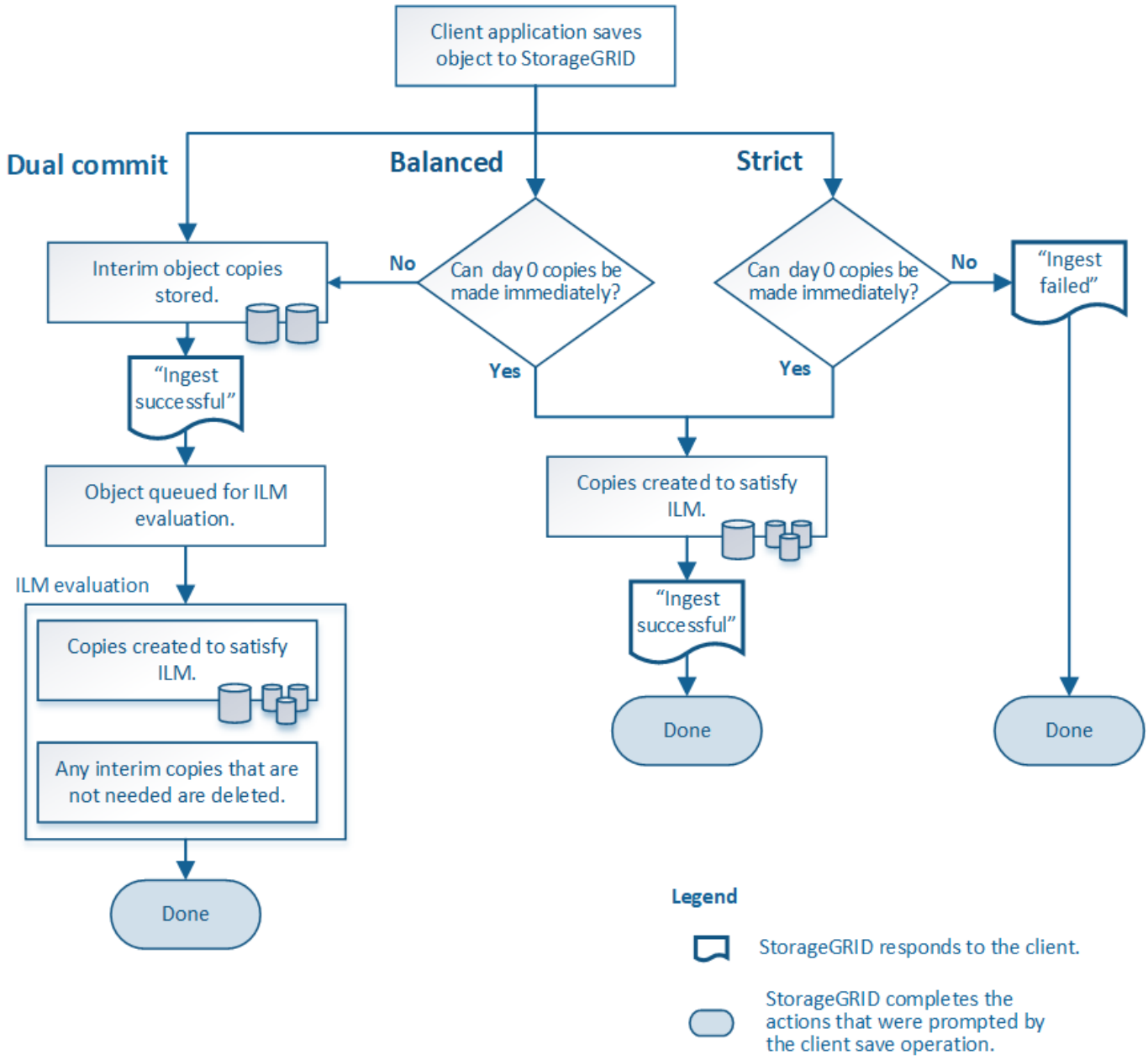
데이터 보호를 위한 수집 옵션

ILM 규칙을 생성할 때 수집 시 개체를 보호하기 위한 세 가지 옵션 중 하나인 이중 커밋, 균형 또는 엄격 을 지정합니다. 선택한 사항에 따라 StorageGRID은 임시 복사본을 만들고 나중에 ILM 평가를 위해 오브젝트를 큐에 대기시키거나 동기식 배치를 사용하여 ILM 요구 사항을

충족하도록 즉시 복사본을 만듭니다.

수집 옵션 **3**개의 흐름도

이 순서도는 세 가지 수집 옵션 각각을 사용하는 ILM 규칙에 따라 오브젝트가 일치할 때 발생하는 상황을 보여 줍니다.



이중 커밋

이중 커밋 옵션을 선택하면 StorageGRID는 즉시 두 개의 다른 스토리지 노드에서 중간 오브젝트 복사본을 만들고 ""수집 성공" 메시지를 클라이언트에 반환합니다. 개체는 ILM 평가를 위해 대기하며 규칙의 배치 지침을 충족하는 복사본은 나중에 만들어집니다.

이중 커밋 옵션을 사용하는 경우

다음 두 경우 중 하나에서 이중 커밋 옵션을 사용합니다.

- 멀티 사이트 ILM 규칙을 사용 중이며 클라이언트 수집 지연 시간이 중요하게 고려해야 합니다. 이중 커밋을 사용할 때 그리드에서 ILM을 충족하지 않는 경우 이중 커밋 복사본을 만들고 제거하는 추가 작업을 수행할 수 있는지 확인해야 합니다. 주요 내용은 다음과 같습니다.
  - ILM 백로그를 방지할 수 있을 정도로 그리드의 부하가 낮아야 합니다.
  - 그리드에는 초과 하드웨어 리소스(IOPS, CPU, 메모리, 네트워크 대역폭 등)가 있어야 합니다.
- 다중 사이트 ILM 규칙을 사용 중이며 사이트 간 WAN 연결에 일반적으로 지연 시간이 길거나 대역폭이 제한되어 있습니다. 이 시나리오에서 이중 커밋 옵션을 사용하면 클라이언트 시간 초과를 방지할 수 있습니다. 이중 커밋 옵션을 선택하기 전에 실제 워크로드로 클라이언트 애플리케이션을 테스트해야 합니다.

엄격한

Strict 옵션을 선택하면 StorageGRID에서는 수집 시 동기식 배치를 사용하고 규칙의 배치 지침에 지정된 모든 오브젝트 복사본을 즉시 생성합니다. 필요한 스토리지 위치를 일시적으로 사용할 수 없기 때문에 StorageGRID에서 모든 복사본을 생성할 수 없는 경우 수집에 실패합니다. 클라이언트가 작업을 재시도해야 합니다.

Strict 옵션을 사용하는 경우

ILM 규칙에 요약된 위치에만 개체를 즉시 저장해야 하는 운영 또는 규정 요구사항이 있는 경우 Strict 옵션을 사용합니다. 예를 들어, 규정 요구 사항을 충족하려면 Strict 옵션 및 Location Constraint 고급 필터를 사용하여 개체가 특정 데이터 센터에 저장되지 않도록 해야 할 수 있습니다.

예 5: 엄격한 수집 동작을 위한 ILM 규칙 및 정책

균형

균형 옵션을 선택하면 StorageGRID는 수집 시 동기식 배치를 사용하고 규칙의 배치 지침에 지정된 모든 복사본을 즉시 생성합니다. Strict 옵션과 달리 StorageGRID 에서 즉시 모든 복사본을 만들 수 없으면 대신 이중 커밋을 사용합니다.

균형 옵션을 사용하는 경우

균형 옵션을 사용하면 데이터 보호, 그리드 성능 및 수집 성공을 최적으로 조합하여 달성할 수 있습니다. ILM 규칙 마법사의 기본 옵션은 밸런스입니다.

데이터 보호 옵션의 장점, 단점 및 제한

수집 시 데이터를 보호하기 위한 세 가지 옵션(균형, 엄격 또는 이중 커밋)의 각 장단점을 이해하면 ILM 규칙에 대해 선택할 항목을 결정하는 데 도움이 됩니다.

균형 및 엄격 옵션의 장점

수집하는 동안 임시 사본을 생성하는 이중 커밋과 비교할 때 두 개의 동기식 배치 옵션은 다음과 같은 이점을 제공합니다.

- * 더 나은 데이터 보안 *: ILM 규칙의 배치 지침에 지정된 대로 개체 데이터가 즉시 보호됩니다. ILM은 둘 이상의 스토리지 위치 장애를 포함하여 다양한 장애 조건을 보호하도록 구성할 수 있습니다. 이중 커밋은 단일 로컬 복사본의 손실로부터 보호할 수 있습니다.
- * 더 효율적인 그리드 작업 *: 각 오브젝트는 수집될 때 한 번만 처리됩니다. StorageGRID 시스템은 중간 복사본을 추적하거나 삭제할 필요가 없으므로 처리 부하가 줄어들고 데이터베이스 공간이 더 적게 사용됩니다.
- * (Balanced) 권장 *: 최적의 ILM 효율성을 제공하는 균형 잡힌 옵션입니다. 엄격한 수집 동작이 필요하거나

그리드가 이중 커밋에 사용하기 위한 모든 기준을 충족하지 않는 한 균형 옵션을 사용하는 것이 좋습니다.

- * (Strict) 개체 위치에 대한 확실성 * : Strict 옵션은 ILM 규칙의 배치 지침에 따라 개체를 즉시 저장합니다.

균형 및 엄격 옵션의 단점

이중 커밋과 비교할 때 균형 및 엄격 옵션에는 다음과 같은 몇 가지 단점이 있습니다.

- * 더 긴 클라이언트 인제스트 *: 클라이언트 인제스트 지연 시간이 더 길어질 수 있습니다. Balanced 및 Strict 옵션을 사용하면 삭제 코딩 조각이나 복제된 복사본을 모두 생성하여 저장할 때까지 ""수집 성공" 메시지가 클라이언트에 반환되지 않습니다. 하지만 오브젝트 데이터는 최종 위치에 훨씬 더 빠르게 도달할 수 있습니다.
- * (Strict) 수집 실패 비율 증가 *: Strict 옵션을 사용하면 StorageGRID에서 ILM 규칙에 지정된 모든 복사본을 즉시 만들 수 없을 때마다 수집 작업이 실패합니다. 필요한 스토리지 위치가 일시적으로 오프라인이거나 네트워크 문제로 인해 사이트 간에 오브젝트 복제가 지연될 경우 수집 장애가 발생할 가능성이 높습니다.
- * (Strict) S3 멀티파트 업로드 배치가 일부 상황에서 예상과 다를 수 있습니다. *: Strict 를 사용하면 ILM 규칙에 설명된 대로 개체를 배치하거나 수집하지 못할 수 있습니다. 하지만 S3 멀티파트 업로드를 사용하면 수집될 때 개체의 각 부분과 멀티파트 업로드가 완료될 때 개체의 ILM을 전체적으로 평가합니다. 다음과 같은 상황에서는 예상과 다른 배치를 초래할 수 있습니다.
  - * S3 멀티파트 업로드가 진행 중일 때 ILM이 변경되는 경우 *: 각 파트는 파트를 인제스트할 때 활성 규칙에 따라 배치되므로 멀티파트 업로드가 완료될 때 개체의 일부 부분이 현재 ILM 요구 사항을 충족하지 못할 수 있습니다. 이 경우 오브젝트 수집은 실패하지 않습니다. 대신 올바르게 배치되지 않은 모든 부품은 ILM 재평가를 위해 대기하다가 나중에 올바른 위치로 이동됩니다.
  - * ILM 규칙이 크기 * 를 기준으로 필터링할 때: 파트에 대한 ILM을 평가할 때 StorageGRID은 개체의 크기가 아닌 파트 크기를 필터링합니다. 즉, 개체의 일부를 개체의 ILM 요구 사항을 전체가 충족하지 않는 위치에 저장할 수 있습니다. 예를 들어, 규칙이 모든 오브젝트 10GB 이상이 DC1에 저장되는 반면 모든 작은 오브젝트는 DC2에 저장되는 것으로 지정하는 경우 10개 부분 멀티파트 업로드의 각 1GB 부분은 DC2에 저장됩니다. 개체에 대한 ILM을 평가할 때 개체의 모든 부분이 DC1로 이동합니다.
- * (Strict) Ingest는 오브젝트 태그 또는 메타데이터를 업데이트하고 새로 필요한 배치를 만들 수 없을 때 실패합니다. * : Strict 를 사용하면 ILM 규칙에 설명된 대로 개체를 배치하거나 수집 실패가 발생할 수 있습니다. 하지만 이미 그리드에 저장된 개체의 메타데이터 또는 태그를 업데이트하는 경우 객체가 다시 수집되지 않습니다. 즉, 업데이트로 인해 트리거되는 개체 배치의 변경 내용은 즉시 적용되지 않습니다. ILM을 정상적인 배경 ILM 프로세스에 의해 재평가할 때 배치 변경이 이루어집니다. 필요한 위치를 변경할 수 없는 경우(예: 새로 필요한 위치를 사용할 수 없는 경우), 업데이트된 개체는 배치를 변경할 수 있을 때까지 현재 위치를 유지합니다.

균형 또는 엄격 옵션을 사용한 개체 배치 제한

다음 배치 지침이 있는 ILM 규칙에는 균형 또는 엄격 옵션을 사용할 수 없습니다.

- 0일에 클라우드 스토리지 풀에 배치.
- 0일째 아카이브 노드에 배치.
- 규칙에 참조 시간으로 사용자 정의 생성 시간이 있는 경우 클라우드 스토리지 풀 또는 아카이브 노드의 배치.

이러한 제한은 StorageGRID가 클라우드 스토리지 풀 또는 아카이브 노드에 동기식 복제를 수행할 수 없고 사용자 정의 생성 시간이 현재로 해결될 수 있기 때문입니다.

ILM 규칙 및 일관성 제어가 데이터 보호에 영향을 미치는 방식

ILM 규칙 및 선택한 일관성 제어 모두 개체의 보호 방법에 영향을 줍니다. 이러한 설정은 상호 작용할 수 있습니다.

예를 들어, ILM 규칙에 대해 선택된 수집 동작은 오브젝트 복사본의 초기 배치에 영향을 주며, 오브젝트가 저장될 때

사용되는 일관성 컨트롤은 오브젝트 메타데이터의 초기 배치에 영향을 줍니다. StorageGRID에서는 클라이언트 요청을 이행하기 위해 오브젝트의 메타데이터와 해당 데이터에 모두 액세스해야 하므로 일관성 수준과 수집 동작에 적합한 보호 수준을 선택하면 초기 데이터 보호 수준을 높이고 시스템 응답을 더욱 정확하게 예측할 수 있습니다.

다음은 StorageGRID에서 사용할 수 있는 일관성 컨트롤을 간략하게 요약한 것입니다.

- * All *: 모든 노드가 개체 메타데이터를 즉시 수신하거나 요청이 실패합니다.
- * strong-global *: 개체 메타데이터는 즉시 모든 사이트에 배포됩니다. 모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 정합성을 보장합니다.
- * strong-site *: 개체 메타데이터는 사이트의 다른 노드로 즉시 배포됩니다. 사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
- * read-after-new-write *: 새 객체에 대한 읽기 후 쓰기 정합성을 보장하고 객체 업데이트에 대한 최종 일관성을 제공합니다. 고가용성 및 데이터 보호 보장 제공
- * Available * (헤드 작업의 최종 일관성): "read-after-new-write" 정합성 수준과 동일하게 동작하지만 헤드 작업에 대한 최종 정합성 보장만 제공합니다.

> 정합성 보장 레벨을 선택하기 전에 의 지침에 있는 정합성 보장 제어에 대한 전체 설명을 읽어보십시오 S3 또는 스위프트 클라이언트 응용 프로그램. 기본값을 변경하기 전에 이점과 제한 사항을 이해해야 합니다.

일관성 제어 및 **ILM** 규칙이 상호 작용하는 방법의 예

다음 ILM 규칙 및 다음 일관성 수준 설정이 있는 두 사이트 그리드가 있다고 가정합니다.

- * ILM 규칙 *: 로컬 사이트와 원격 사이트에 각각 하나씩, 두 개의 오브젝트 복사본을 만듭니다. Strict 수집 동작이 선택됩니다.
- * Consistency level *: "trong-global"(개체 메타데이터가 모든 사이트에 즉시 배포됩니다.)

클라이언트가 오브젝트를 그리드에 저장할 때 StorageGRID는 오브젝트 복사본을 둘 다 만들고 메타데이터를 두 사이트에 분산한 다음 클라이언트에 성공을 반환합니다.

수집 성공 메시지가 표시된 시점에 객체가 손실로부터 완벽하게 보호됩니다. 예를 들어, 수집 직후 로컬 사이트가 손실되면 오브젝트 데이터와 오브젝트 메타데이터의 복사본이 원격 사이트에 계속 존재합니다. 개체를 완전히 검색할 수 있습니다.

대신 동일한 ILM 규칙 및 "'strong-site' 정합성 보장 수준을 사용한 경우 객체 데이터가 원격 사이트에 복제되었지만 객체 메타데이터가 그 위치에 배포되기 전에 클라이언트에 성공 메시지가 표시될 수 있습니다. 이 경우 오브젝트 메타데이터의 보호 수준이 오브젝트 데이터의 보호 수준과 일치하지 않습니다. 수집 후 곧바로 로컬 사이트가 손실되면 오브젝트 메타데이터가 손실됩니다. 객체를 검색할 수 없습니다.

일관성 수준과 ILM 규칙 간의 상호 관계는 복잡할 수 있습니다. 도움이 필요한 경우 NetApp에 문의하십시오.

관련 정보

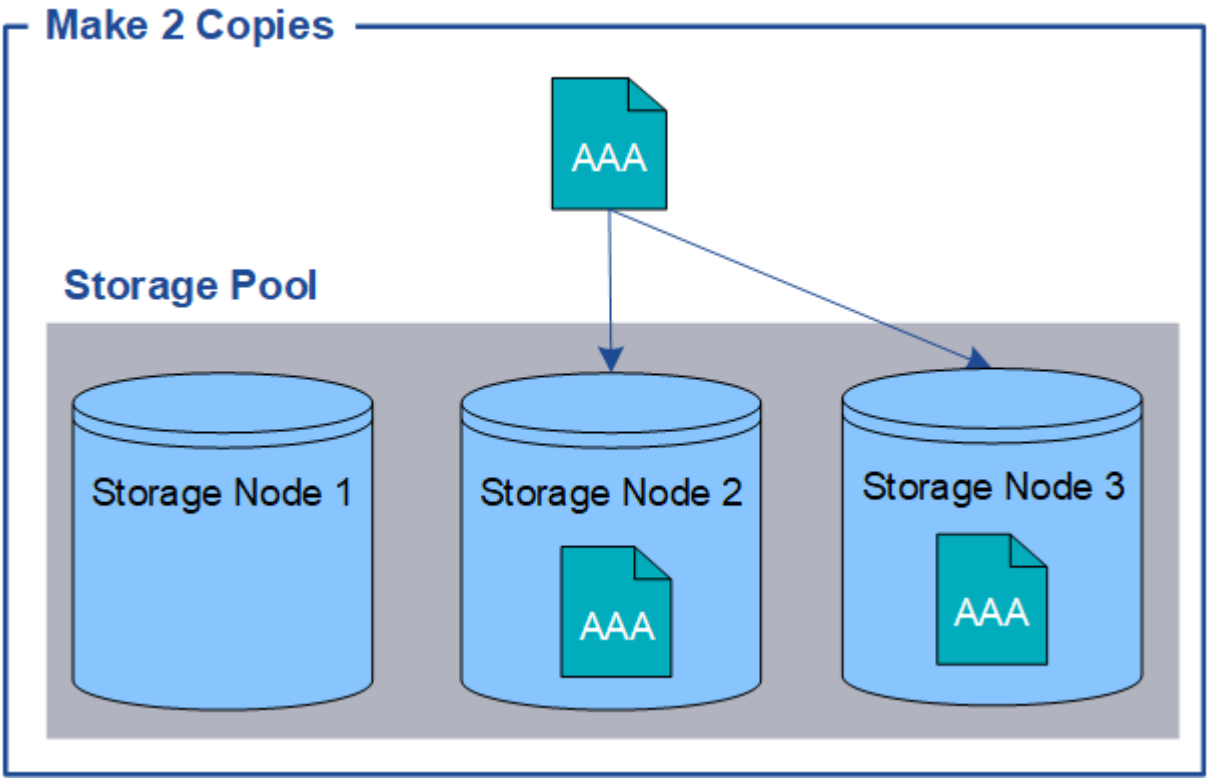
- 예 5: 엄격한 수집 동작을 위한 ILM 규칙 및 정책

오브젝트 저장 방법(복제 또는 삭제 코딩)

복제는 StorageGRID에서 오브젝트 데이터를 저장하는 데 사용하는 두 가지 방법 중 하나입니다. 객체가 복제를 사용하는 ILM 규칙과 일치하면 시스템에서 정확한 오브젝트 데이터 복사본을 생성하고 스토리지 노드 또는 아카이브 노드에 복사본을 저장합니다.

ILM 규칙을 구성하여 복제된 복사본을 생성할 때는 생성할 복사본 수, 복사본 배치 위치 및 각 위치에 복사본을 저장할 기간을 지정합니다.

다음 예제에서 ILM 규칙은 세 개의 스토리지 노드가 포함된 스토리지 풀에 각 개체의 복제된 복사본 2개를 배치하도록 지정합니다.



StorageGRID가 오브젝트를 이 규칙과 일치시키면 스토리지 풀의 다른 스토리지 노드에 각 복사본을 배치하여 객체의 복제본이 두 개 생성됩니다. 두 복제본은 세 개의 사용 가능한 스토리지 노드 중 어느 두 개에 배치될 수 있습니다. 이 경우 규칙은 스토리지 노드 2와 3에 오브젝트 복사본을 배치합니다. 두 개의 복제본이 있기 때문에 스토리지 풀의 노드 중 하나에 장애가 발생할 경우 객체를 검색할 수 있습니다.

> StorageGRID는 지정된 스토리지 노드에 복제된 객체 복제본을 하나만 저장할 수 있습니다. 그리드에 스토리지 노드 3개가 포함된 경우 4개 복사본 ILM 규칙을 생성하면 각 스토리지 노드에 대해 복사본 1개가 생성됩니다. ILM 규칙을 완전히 적용할 수 없음을 나타내기 위해 * ILM 배치 달성 안 됨 * 경고가 트리거됩니다.

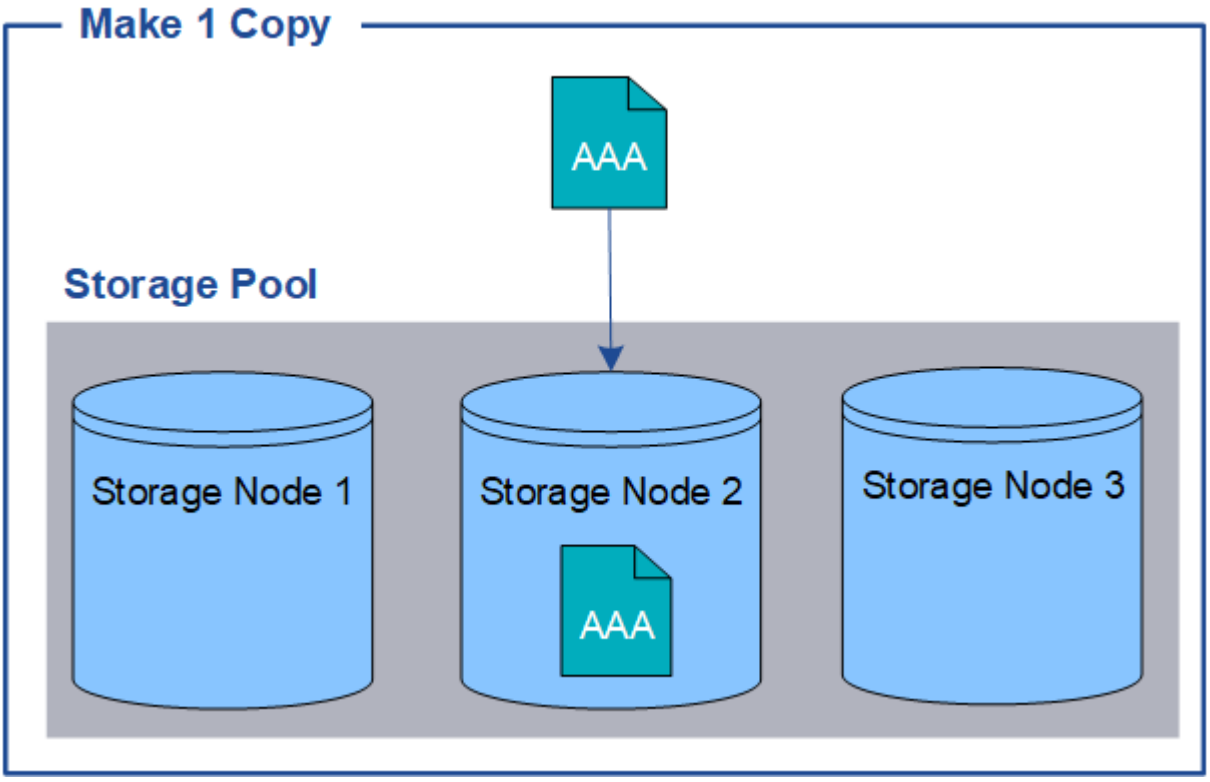
관련 정보

- 스토리지 풀의 정의
- 사이트 간 복제에 여러 스토리지 풀을 사용합니다

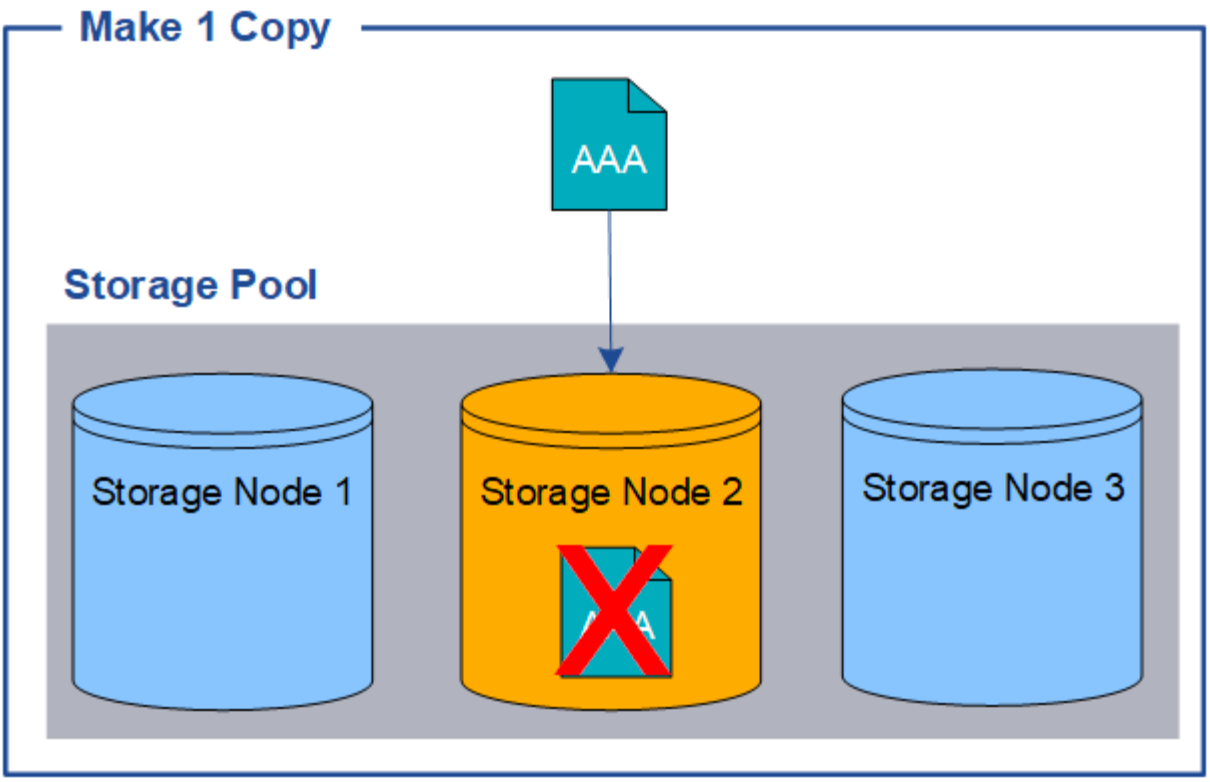
ILM 규칙을 생성하여 복제된 복사본을 만들 때는 항상 배치 지침에 두 개 이상의 복사본을 지정해야 합니다.

> 특정 기간 동안 복제된 복사본을 하나만 생성하는 ILM 규칙을 사용하지 마십시오. 복제된 객체 복제본이 하나만 있는 경우 스토리지 노드에 장애가 발생하거나 심각한 오류가 발생한 경우 해당 객체가 손실됩니다. 또한 업그레이드와 같은 유지보수 절차 중에는 개체에 대한 액세스가 일시적으로 중단됩니다.

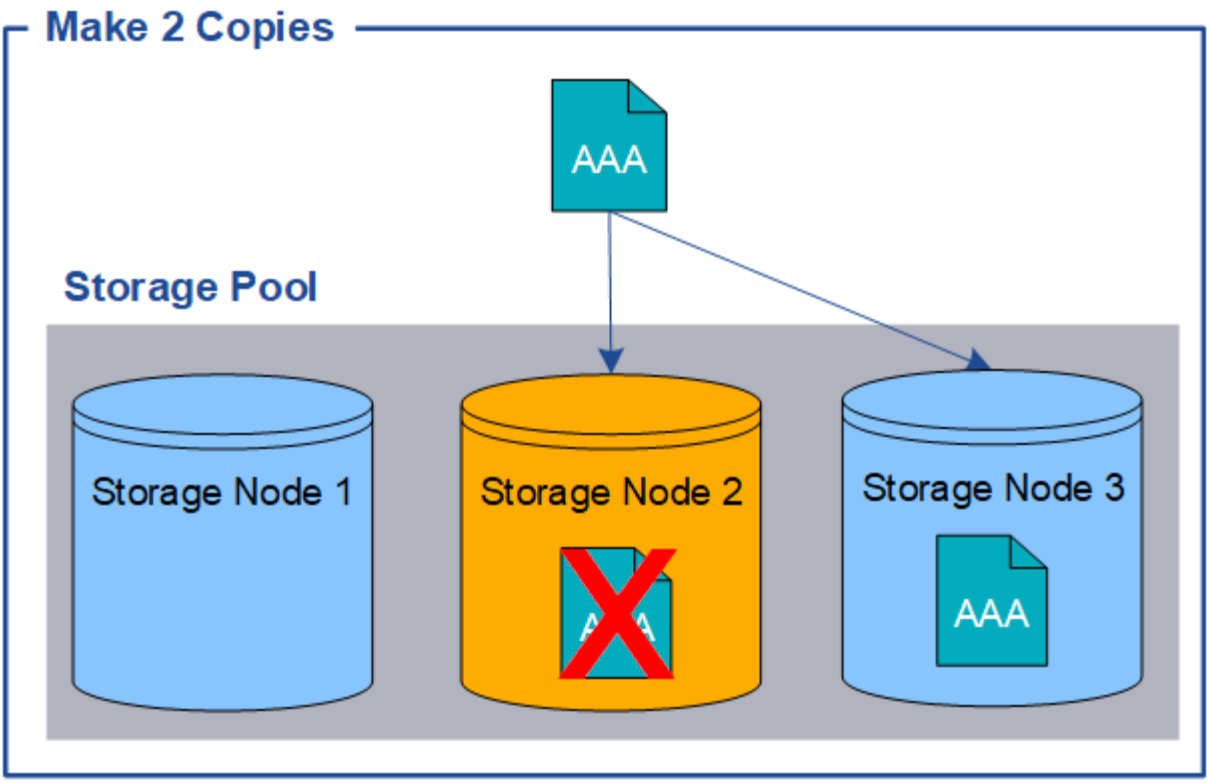
다음 예제에서 Make 1 Copy ILM 규칙은 세 개의 스토리지 노드가 포함된 스토리지 풀에 개체의 복제된 복사본 하나를 배치하도록 지정합니다. 이 규칙과 일치하는 객체가 수집되면 StorageGRID는 하나의 스토리지 노드에만 단일 복제본을 배치합니다.



ILM 규칙이 개체의 복제된 복사본을 하나만 만들면 스토리지 노드를 사용할 수 없을 때 개체에 액세스할 수 없게 됩니다. 이 예제에서는 업그레이드 또는 기타 유지 관리 절차 중에 스토리지 노드 2가 오프라인일 때마다 객체 AAA에 대한 액세스가 일시적으로 끊어집니다. 스토리지 노드 2에 장애가 발생하면 객체 AAA가 완전히 손실됩니다.



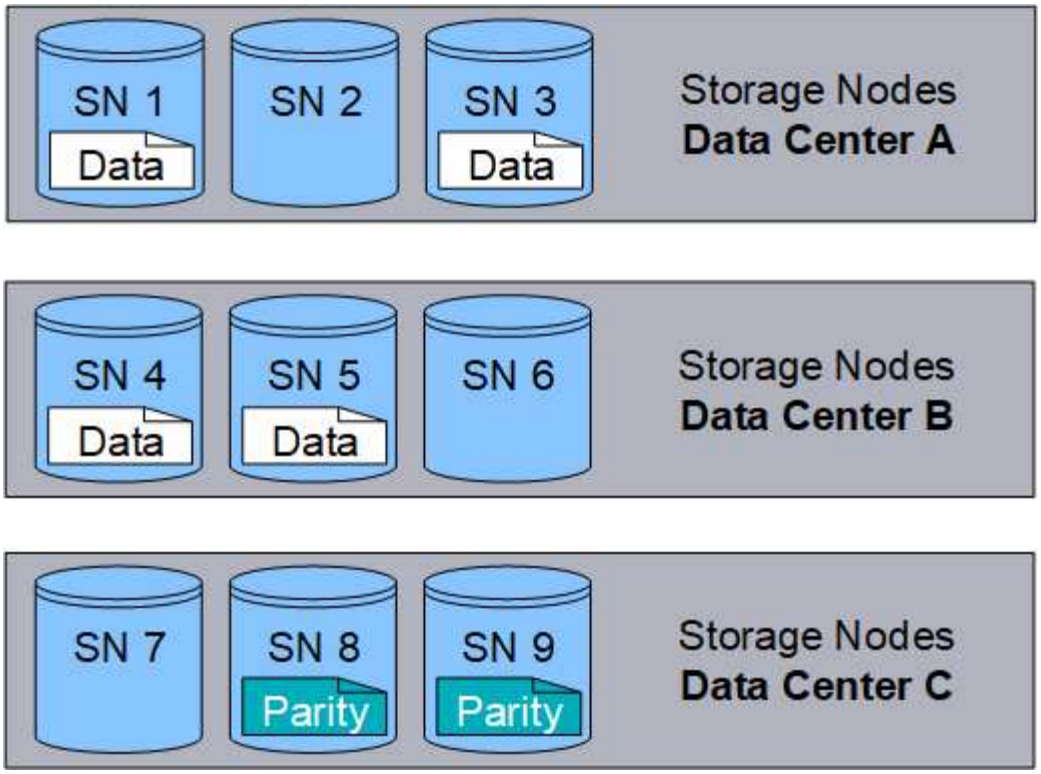
오브젝트 데이터의 손실을 방지하려면 항상 복제로 보호할 모든 오브젝트의 복사본을 두 개 이상 만들어야 합니다. 두 개 이상의 복제본이 있는 경우에도 하나의 스토리지 노드에 장애가 발생하거나 오프라인 상태가 되더라도 개체에 액세스할 수 있습니다.



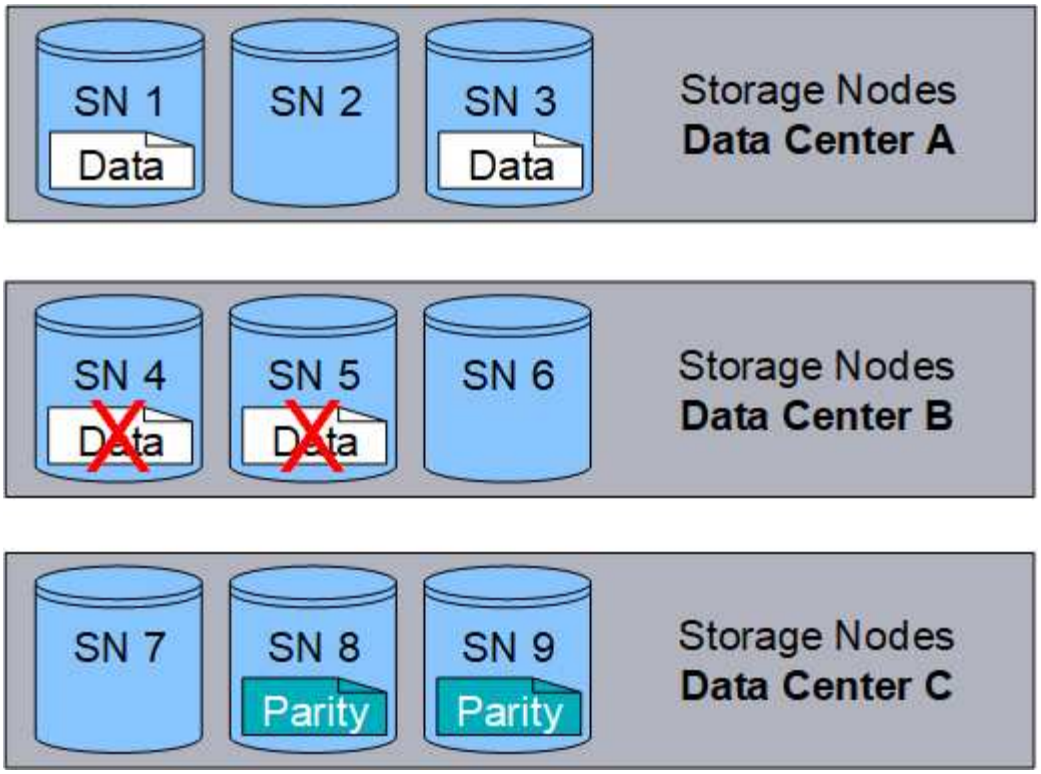
삭제 코딩이란 무엇입니까

삭제 코딩은 StorageGRID에서 오브젝트 데이터를 저장하는 데 사용하는 두 번째 방법입니다. StorageGRID가 오브젝트를 삭제 코딩 복사본을 만들도록 구성된 ILM 규칙과 일치시키는 경우 오브젝트 데이터를 데이터 조각으로 슬라이스하고, 추가 패리티 조각을 계산하고, 각 조각을 다른 스토리지 노드에 저장합니다. 개체에 액세스하면 저장된 조각을 사용하여 다시 조립됩니다. 데이터 또는 패리티 조각이 손상되거나 손실될 경우, 삭제 코딩 알고리즘이 나머지 데이터 및 패리티 조각의 일부를 사용하여 해당 조각을 다시 생성할 수 있습니다.

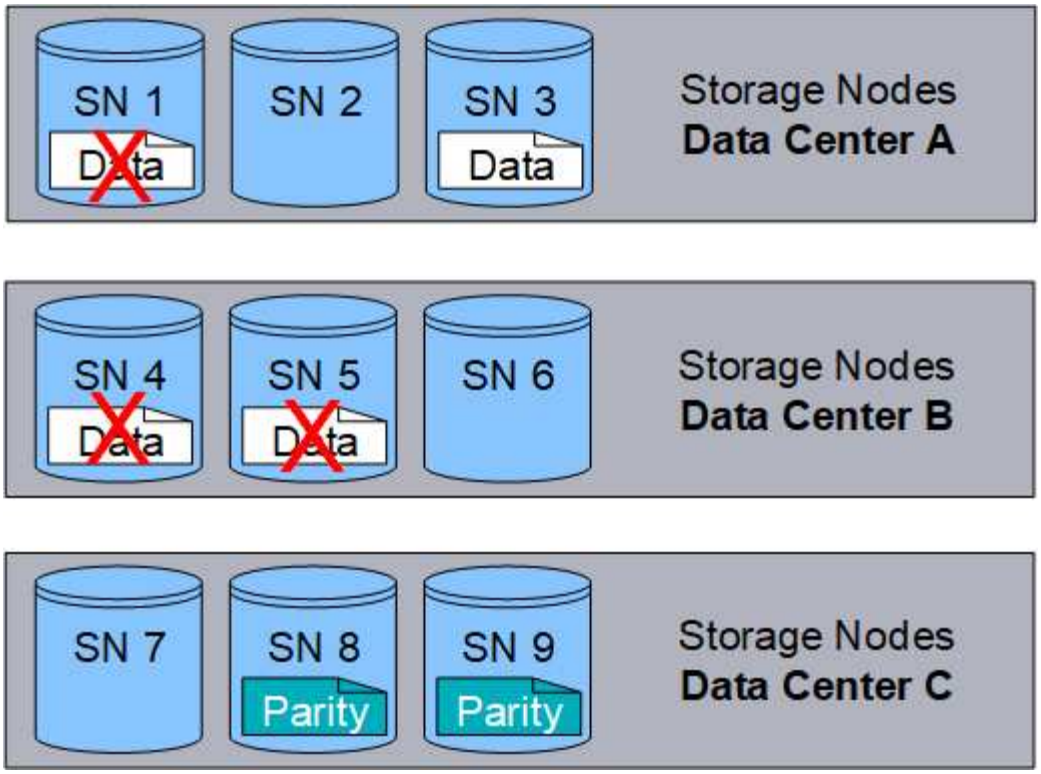
다음 예제에서는 오브젝트의 데이터에서 삭제 코딩 알고리즘을 사용하는 방법을 보여 줍니다. 이 예제에서 ILM 규칙은 4+2 삭제 코딩 체계를 사용합니다. 각 개체는 4개의 동일한 데이터 조각으로 분할되며 두 개의 패리티 조각은 개체 데이터에서 계산됩니다. 6개의 각 단편은 3개의 데이터 센터 사이트에서 서로 다른 노드에 저장되어 노드 장애 또는 사이트 손실에 대한 데이터 보호를 제공합니다.



4+2 삭제 코딩 구성에는 최소 9개의 스토리지 노드가 필요하며, 3개의 서로 다른 사이트에 3개의 스토리지 노드가 있습니다. 6개의 조각(데이터 또는 패리티) 중 4개를 사용할 수 있는 한 오브젝트를 검색할 수 있습니다. 개체 데이터를 손실하지 않고 최대 2개의 조각을 잃을 수 있습니다. 전체 데이터 센터 사이트가 손실되더라도 다른 모든 조각에 액세스할 수 있는 한 개체를 검색하거나 복구할 수 있습니다.



두 개 이상의 스토리지 노드가 손실되면 객체를 검색할 수 없습니다.



관련 정보

- 스토리지 풀의 정의
- 어떤 삭제 코딩 구성인지
- 삭제 코딩 프로필을 생성합니다

어떤 삭제 코딩 구성인지

ILM 규칙에 대한 삭제 코딩 프로파일을 구성할 때 사용할 스토리지 풀을 구성하는 스토리지 노드 및 사이트의 수에 따라 사용 가능한 삭제 코딩 체계를 선택합니다. 삭제 코딩 스키마를 통해 각 오브젝트에 대해 생성되는 데이터 조각과 패리티 조각의 수를 제어합니다.

StorageGRID 시스템은 Reed-Solomon 삭제 코딩 알고리즘을 사용합니다. 알고리즘은 개체를 k 데이터 조각으로 슬라이스하고 m 패리티 조각을 계산합니다. k+m=n 조각은 n 스토리지 노드에 분산되므로 데이터를 보호할 수 있습니다. 개체는 손실되거나 손상된 조각을 최대 m 까지 유지할 수 있습니다. K 파편은 개체를 검색하거나 복구하는 데 필요합니다.

삭제 코딩 프로필을 구성할 때는 스토리지 풀에 대해 다음 지침을 따르십시오.

- 스토리지 풀에는 3개 이상의 사이트 또는 정확히 하나의 사이트가 포함되어야 합니다.

  ⓘ 스토리지 풀에 두 개의 사이트가 포함된 경우 삭제 코딩 프로필을 구성할 수 없습니다.

  - 3개 이상의 사이트가 포함된 스토리지 풀의 삭제 코딩 체계
  - 단일 사이트 스토리지 풀에 대한 삭제 코딩 구성표
- 기본 스토리지 풀, 모든 스토리지 노드 또는 기본 사이트인 모든 사이트가 포함된 스토리지 풀을 사용하지 마십시오.
- 스토리지 풀에는 최소 *k*+*m*+1 스토리지 노드가 포함되어야 합니다.

필요한 최소 스토리지 노드 수는 _k+m_입니다. 그러나 필요한 스토리지 노드를 일시적으로 사용할 수 없는 경우 하나 이상의 추가 스토리지 노드를 사용하면 수집 실패 또는 ILM 백로그를 방지할 수 있습니다.

삭제 코딩 체계의 스토리지 오버헤드는 패리티 단편 수(*m*)를 데이터 조각 수(*k*)로 나누어 계산됩니다. 스토리지 오버헤드를 사용하여 각 삭제 코딩 오브젝트에 필요한 디스크 공간을 계산할 수 있습니다.

'*DISK SPACE=OBJECT SIZE*+(*OBJECT SIZE * STORAGE OBLOAhead*)'

예를 들어, 스토리지 오버헤드가 50%인 4+2 체계를 사용하여 10MB 오브젝트를 저장할 경우 오브젝트는 15MB의 그리드 스토리지를 사용합니다. 스토리지 오버헤드가 33%인 6+2 체계를 사용하여 동일한 10MB 개체를 저장하는 경우, 개체는 약 13.3MB를 사용합니다.

요구 사항에 맞는 가장 낮은 총 값 _k+m_의 삭제 코딩 방법을 선택하십시오. 조각의 수가 적은 삭제 코딩 스키마를 사용하면 개체당 생성 및 분산(또는 검색)되는 조각 수가 적고 더 큰 조각 크기로 인해 성능이 향상될 수 있으며 더 많은 스토리지가 필요할 때 확장에 추가할 노드 수를 줄일 수 있으므로 전체적으로 계산 효율이 향상됩니다. 스토리지 확장 계획에 대한 자세한 내용은 StorageGRID 확장 지침을 참조하십시오.

3개 이상의 사이트가 포함된 스토리지 풀의 삭제 코딩 체계

다음 표에서는 3개 이상의 사이트가 포함된 스토리지 풀에 대해 StorageGRID에서 현재 지원하는 삭제 코딩 스키마를 설명합니다. 이러한 모든 체계는 사이트 손실을 보호합니다. 한 사이트는 손실될 수 있으며 개체는 계속 액세스할 수 있습니다.

사이트 손실 보호를 제공하는 삭제 코딩 체계의 경우 각 사이트에 최소 3개의 스토리지 노드가 필요하므로 스토리지 풀의 권장 스토리지 노드 수가 _k+m_1을 초과합니다.

삭제 코딩 체계 (*k+m*)	배포된 사이트의 최소 수입니다	각 사이트에 권장되는 스토리지 노드 수입니다	총 권장 스토리지 노드 수입니다	사이트 손실 방지	스토리지 오버헤드
4+2	3	3	9	예	50%
6+2	4	3	12	예	33%
8+2	5	3	15	예	25%
6 + 3	3	4	12	예	50%
9+3	4	4	16	예	33%
2+1	3	3	9	예	50%
4+1	5	3	15	예	25%
6+1	7	3	21	예	17%
7+5	3	5	15	예	71%

> StorageGRID에는 사이트당 최소 3개의 스토리지 노드가 필요합니다. 7+5 스키마를 사용하려면 각 사이트에 최소 4개의 스토리지 노드가 필요합니다. 사이트당 5개의 스토리지 노드를 사용하는 것이 좋습니다.

사이트 보호를 제공하는 삭제 코딩 스키마를 선택할 때는 다음 요소의 상대적 중요도를 균형 있게 조정합니다.

- * 조각 수 *: 전체 조각 수가 적으면 성능과 확장 유연성이 일반적으로 더 좋습니다.
- * 내결함성 *: 더 많은 패리티 세그먼트(즉, _m_의 값이 더 높은 경우)를 보유하여 내결함성 증가
- * 네트워크 트래픽 *: 오류가 발생한 상태에서 복구할 때 더 많은 조각(_k+m_의 경우 더 높은 합계)이 포함된 구성표를 사용하면 더 많은 네트워크 트래픽이 생성됩니다.
- * 스토리지 오버헤드 *: 오버헤드가 높은 구성일수록 오브젝트당 스토리지 공간이 더 필요합니다.

예를 들어, 4+2 체계와 6+3 체계(둘 다 50%의 스토리지 오버헤드를 가짐) 중에서 결정할 때 추가 내결함성을 필요로 하는 경우 6+3 체계를 선택합니다. 네트워크 리소스가 제한된 경우 4+2 구성표를 선택합니다. 다른 모든 요소가 같으면 총 단편 수가 더 낮기 때문에 4+2를 선택합니다.

> 사용할 체계가 확실하지 않으면 4+2 또는 6+3을 선택하거나 기술 지원 부서에 문의하십시오.

단일 사이트 스토리지 풀에 대한 삭제 코딩 구성표

사이트에 충분한 스토리지 노드가 있는 경우 한 사이트 스토리지 풀은 세 개 이상의 사이트에 대해 정의된 모든 삭제 코딩 스키마를 지원합니다.

필요한 최소 스토리지 노드 수는 *k+m*_이지만 _*k+m*+1 스토리지 노드가 있는 스토리지 풀을 사용하는 것이 좋습니다. 예를 들어, 2+1 삭제 코딩 구성표에 최소 3개의 스토리지 노드가 있는 스토리지 풀이 필요하지만 4개의 스토리지 노드를 사용하는 것이 좋습니다.

삭제 코딩 체계(*k+m*)	최소 스토리지 노드 수입니다	권장되는 스토리지 노드 수입니다	스토리지 오버헤드
4+2	6	7	50%
6+2	8	9	33%
8+2	10	11	25%
6 + 3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

관련 정보

그리드를 확장합니다

삭제 코딩의 장점, 단점 및 요구 사항

오브젝트 데이터의 손실로부터 보호하기 위해 복제 또는 삭제 코딩을 사용할지 결정하기 전에 삭제 코딩의 장점, 단점 및 요구 사항을 이해해야 합니다.

삭제 코딩의 장점

삭제 코딩은 복제와 비교할 때 안정성, 가용성 및 스토리지 효율성을 향상시킵니다.

- * 안정성 *: 신뢰성은 내결함성의 관점에서 측정되며, 즉 데이터 손실 없이 동시에 장애가 발생할 수 있는 횟수를 나타냅니다. 복제를 사용하면 동일한 여러 복사본이 여러 노드와 사이트 전체에 저장됩니다. 삭제 코딩을 사용하면 오브젝트는 데이터 및 패리티 조각으로 인코딩되어 여러 노드와 사이트에 분산됩니다. 이 분산은 사이트 및 노드 장애 보호를 모두 제공합니다. 복제와 비교할 때 삭제 코딩은 비슷한 스토리지 비용으로 향상된 안정성을 제공합니다.
- * 가용성 *: 스토리지 노드에 장애가 발생하거나 액세스할 수 없는 경우 객체를 검색하는 기능으로 가용성을 정의할 수 있습니다. 복제와 비교할 때 삭제 코딩은 비슷한 스토리지 비용으로 향상된 가용성을 제공합니다.
- * 스토리지 효율성 *: 유사한 수준의 가용성과 안정성을 위해 삭제 코딩을 통해 보호되는 오브젝트는 복제를 통해 보호될 경우 동일한 오브젝트보다 더 적은 디스크 공간을 사용합니다. 예를 들어, 두 개의 사이트에 복제된 10MB 오브젝트는 20MB의 디스크 공간(복사본 2개)을 사용하지만 삭제 코딩 구성표 6+3을 사용하여 세 사이트에서 삭제 코딩되는 오브젝트는 15MB의 디스크 공간만 사용합니다.

> 삭제 코딩 오브젝트를 위한 디스크 공간은 오브젝트 크기와 스토리지 오버헤드로 계산됩니다. 스토리지 오버헤드 비율은 패리티 조각 수를 데이터 조각 수로 나눈 값입니다.

삭제 코딩의 단점

복제와 비교할 때 삭제 코딩에는 다음과 같은 단점이 있습니다.

- 스토리지 노드 및 사이트의 수가 증가해야 합니다. 예를 들어, 삭제 코딩 구성표 6+3을 사용하는 경우 3개의 다른 사이트에 3개 이상의 스토리지 노드가 있어야 합니다. 반면, 오브젝트 데이터만 복제하면 각 복제본마다 스토리지 노드가 하나만 필요합니다.
- 스토리지 확장의 비용 및 복잡성 증가 복제를 사용하는 배포를 확장하려면 개체 복사본이 만들어지는 모든 위치에 스토리지 용량을 추가하기만 하면 됩니다. 삭제 코딩을 사용하는 배포를 확장하려면 사용 중인 삭제 코딩 체계와 기존 스토리지 노드의 전체 용량을 고려해야 합니다. 예를 들어 기존 노드가 100% 꽉 찰 때까지 기다리는 경우 최소한 _k+m_스토리지 노드를 추가해야 하지만 기존 노드가 70% 가득 찬 경우 사이트 당 두 개의 노드를 추가하여 가용 스토리지 용량을 최대화할 수 있습니다. 자세한 내용은 을 참조하십시오 삭제 코딩 오브젝트를 위한 스토리지 용량을 추가합니다.
- 지리적으로 분산된 사이트에서 삭제 코딩을 사용하면 검색 지연 시간이 늘어납니다. 원격 사이트에 삭제 코딩되고 분산된 오브젝트의 오브젝트 조각은 로컬에서 복제 및 사용할 수 있는 오브젝트(클라이언트가 연결하는 동일한 사이트)보다 WAN 연결을 통해 검색하는 데 시간이 더 오래 걸립니다.
- 지리적으로 분산된 사이트에서 삭제 코딩을 사용하는 경우 검색 및 복구를 위해 WAN 네트워크 트래픽 사용량이 증가하고, 특히 자주 검색하는 오브젝트 또는 WAN 네트워크 연결을 통한 오브젝트 복구에서 더욱 그렇습니다.
- 여러 사이트에서 삭제 코딩을 사용하면 사이트 간의 네트워크 지연 시간이 증가함에 따라 최대 오브젝트 처리량이 급격히 줄어듭니다. 이러한 감소는 StorageGRID 시스템이 개체 조각을 저장하고 검색하는 데 영향을 미치는 TCP 네트워크 처리량이 감소하기 때문입니다.

- 컴퓨팅 리소스 사용량 증가.

삭제 코딩 사용 시기

삭제 코딩은 다음 요구사항에 가장 적합합니다.

- 크기가 1MB를 초과하는 객체

> 삭제 코딩은 1MB 이상의 오브젝트에 가장 적합합니다. 매우 작은 삭제 코딩 조각을 관리해야 하는 오버헤드를 방지하기 위해 200KB 미만의 오브젝트에 삭제 코딩을 사용하지 마십시오.

- 자주 검색되지 않는 콘텐츠의 장기 또는 콜드 스토리지
- 높은 데이터 가용성 및 안정성
- 전체 사이트 및 노드 장애로부터 보호
- 스토리지 효율성:
- 여러 개의 복제된 복사본이 아닌 하나의 삭제 코딩 복사본만으로 효율적인 데이터 보호가 필요한 단일 사이트 배포
- 사이트 간 지연 시간이 100ms 미만인 다중 사이트 구축

개체 보존이 결정되는 방식

StorageGRID는 그리드 관리자와 개별 테넌트 사용자 모두에게 개체 저장 기간을 지정할 수 있는 옵션을 제공합니다. 일반적으로 테넌트 사용자가 제공한 보존 지침은 그리드 관리자가 제공한 보존 지침보다 우선합니다.

테넌트 사용자가 객체 보존을 제어하는 방식

테넌트 사용자는 세 가지 주요 방법으로 StorageGRID에 객체가 저장되는 기간을 제어할 수 있습니다.

- 그리드에 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 S3 테넌트 사용자는 S3 오브젝트 잠금이 활성화된 버킷을 생성한 다음 S3 REST API를 사용하여 해당 버킷에 추가된 각 오브젝트 버전에 대한 보관 기한 및 법적 보류 설정을 지정할 수 있습니다.
  - 법적 증거 자료 보관 중인 개체 버전은 어떤 방법으로도 삭제할 수 없습니다.
  - 개체 버전의 보존 기한 에 도달하기 전에 어떤 방법으로도 해당 버전을 삭제할 수 없습니다.
  - S3 오브젝트 잠금이 활성화된 버킷의 오브젝트는 ILM ""영구""에 의해 유지됩니다. 그러나 보존 기한에 도달한 후에는 클라이언트 요청 또는 버킷 라이프사이클의 만료에 의해 오브젝트 버전을 삭제할 수 있습니다. 을 참조하십시오 S3 오브젝트 잠금으로 오브젝트 관리.
- S3 테넌트 사용자는 만료 작업을 지정하는 버킷에 라이프사이클 구성을 추가할 수 있습니다. 버킷 라이프사이클이 있는 경우 StorageGRID는 클라이언트가 먼저 오브젝트를 삭제하지 않는 한 만료 작업에 지정된 날짜 또는 일 수가 충족될 때까지 오브젝트를 저장합니다. 을 참조하십시오 S3 라이프사이클 구성을 생성합니다.
- S3 또는 Swift 클라이언트가 오브젝트 삭제 요청을 실행할 수 있습니다. StorageGRID는 항상 S3 버킷 라이프사이클 또는 ILM을 통해 클라이언트 삭제 요청의 우선순위를 지정하고 오브젝트를 삭제 또는 보존 할 것인지 결정합니다.

그리드 관리자가 개체 보존을 제어하는 방법

그리드 관리자는 ILM 배치 지침을 사용하여 오브젝트가 저장되는 기간을 제어합니다. ILM 규칙에 따라 오브젝트가

일치하는 경우 StorageGRID는 ILM 규칙의 마지막 기간이 경과할 때까지 해당 오브젝트를 저장합니다. 배치 명령에 ""영구""를 지정하면 오브젝트가 무기한 유지됩니다.

누가 개체의 보존 기간을 제어하든 ILM 설정은 저장된 개체 복사본(복제 또는 삭제 코딩)의 유형과 복사본의 위치(스토리지 노드, 클라우드 스토리지 풀 또는 아카이브 노드)를 제어합니다.

S3 버킷 수명 주기와 ILM이 상호 작용하는 방식

S3 버킷 라이프사이클의 만료 작업은 항상 ILM 설정을 재정의합니다. 따라서 개체를 배치하기 위한 ILM 명령이 만료된 후에도 개체가 그리드에 유지될 수 있습니다.

오브젝트 보존의 예

S3 오브젝트 잠금, 버킷 수명 주기 설정, 클라이언트 삭제 요청 및 ILM 간의 상호 작용을 더 잘 이해하려면 다음 예제를 고려해 보십시오.

예 1: S3 버킷 수명 주기는 ILM보다 개체를 더 오래 유지합니다

ILM을 참조하십시오

1년(365일) 동안 2부 보관

버킷 수명 주기

2년 후 개체 만료(730일)

결과

StorageGRID 는 개체를 730일 동안 저장합니다. StorageGRID는 버킷 수명 주기 설정을 사용하여 오브젝트를 삭제 또는 유지할지 여부를 결정합니다.

> 버킷 라이프사이클에서 ILM에서 지정한 것보다 더 오래 개체를 유지해야 한다고 지정하는 경우 StorageGRID는 저장할 복사본의 수와 유형을 결정할 때 ILM 배치 지침을 계속 사용합니다. 이 예제에서는 두 개의 개체 복사본이 StorageGRID에 계속 저장됩니다. 이 기간은 366일에서 730일입니다.

예 2: S3 버킷 라이프사이클이 ILM 전에 오브젝트를 만기합니다

ILM을 참조하십시오

2년(730일) 동안 2부 보관

버킷 수명 주기

1년 후 개체 만료(365일)

결과

StorageGRID에서는 365일 이후에 개체의 복사본을 모두 삭제합니다.

예 3: 클라이언트 삭제는 버킷 수명 주기와 ILM을 재정의합니다

ILM을 참조하십시오

스토리지 노드 ""영구""에 두 개의 복사본 저장

버킷 수명 주기

2년 후 개체 만료(730일)

클라이언트 삭제 요청

400일째 발행

결과

StorageGRID는 클라이언트 삭제 요청에 대한 응답으로 400일째에 두 객체 복제본을 모두 삭제합니다.

예 **4: S3** 오브젝트 잠금이 클라이언트 삭제 요청을 재정의합니다

S3 오브젝트 잠금

개체 버전에 대한 보존 기한은 2026-03-31입니다. 법적 증거 자료 보관 은 적용되지 않습니다.

ILM 규칙 준수

스토리지 노드 ""영구""에 두 개의 복사본을 저장합니다.

클라이언트 삭제 요청

2024-03-31에 발행.

결과

보존 기한이 2년 남지 않았으므로 StorageGRID는 개체 버전을 삭제하지 않습니다.

오브젝트 삭제 방법

StorageGRID는 클라이언트 요청에 직접 응답하거나 S3 버킷 라이프사이클의 만료 또는 ILM 정책 요구사항으로 인해 자동으로 오브젝트를 삭제할 수 있습니다. 개체를 삭제할 수 있는 다양한 방법과 StorageGRID에서 삭제 요청을 처리하는 방법을 이해하면 개체를 보다 효율적으로 관리할 수 있습니다.

StorageGRID는 다음 두 가지 방법 중 하나를 사용하여 오브젝트를 삭제할 수 있습니다.

- 동기 삭제: StorageGRID가 클라이언트 삭제 요청을 받으면 모든 개체 복사본이 즉시 제거됩니다. 복제본이 제거된 후 성공적으로 삭제되었다는 메시지가 클라이언트에 표시됩니다.
- 객체가 삭제 대기열에 저장됨: StorageGRID에서 삭제 요청을 수신하면 객체가 삭제 대기열에 추가되고 삭제 성공 사실을 즉시 클라이언트에 알립니다. 개체 복사본은 나중에 백그라운드 ILM 처리에 의해 제거됩니다.

오브젝트를 삭제할 때 StorageGRID는 삭제 성능을 최적화하고 잠재적인 삭제 백로그를 최소화하며 공간을 가장 빠르게 확보하는 방법을 사용합니다.

이 표에는 StorageGRID에서 각 방법을 사용하는 경우가 요약되어 있습니다.

삭제 수행 방법	사용 시
오브젝트는 삭제 대기열에 추가됩니다	다음 조건 중 * 어느 * 가 참일 경우: • 자동 개체 삭제는 다음 이벤트 중 하나에 의해 트리거되었습니다. ◦ S3 버킷에 대한 라이프사이클 구성의 만료 날짜 또는 일 수에 도달했습니다. ◦ ILM 규칙에 지정된 마지막 기간이 경과됩니다. • 참고: * S3 오브젝트 잠금이 활성화된 버킷의 오브젝트는 법적 보류 중이거나 보존 기한이 지정되었지만 아직 충족되지 않은 경우 삭제할 수 없습니다. • S3 또는 Swift 클라이언트가 삭제를 요청하고 다음 조건 중 하나 이상이 TRUE입니다. ◦ 예를 들어, 개체 위치를 일시적으로 사용할 수 없기 때문에 복사본을 30초 이내에 삭제할 수 없습니다. ◦ 백그라운드 삭제 대기열은 유휴 상태입니다.
객체가 즉시 제거됩니다(동기식 삭제).	S3 또는 Swift 클라이언트가 삭제 요청을 하고 다음 조건 중 * 모두 * 가 충족되는 경우: • 모든 사본은 30초 이내에 제거할 수 있습니다. • 백그라운드 삭제 대기열에는 처리할 객체가 포함됩니다.

S3 또는 Swift 클라이언트가 삭제 요청을 하면 StorageGRID가 삭제 대기열에 많은 오브젝트를 추가하여 시작합니다. 그런 다음 동기식 삭제 수행 으로 전환됩니다. 백그라운드 삭제 큐에 처리할 개체가 있는지 확인함으로써 StorageGRID는 특히 동시 접속 수가 적은 클라이언트의 경우 삭제 작업을 보다 효율적으로 처리할 수 있으며 클라이언트 삭제 백로그를 방지할 수 있습니다.

객체를 삭제하는 데 시간이 얼마나 걸립니까

StorageGRID에서 객체를 삭제하는 방법은 시스템이 수행하는 방식에 영향을 미칠 수 있습니다.

- StorageGRID가 동기 삭제를 수행할 때 결과를 클라이언트에 반환하는 데 StorageGRID가 최대 30초가 걸릴 수 있습니다. 즉, StorageGRID에서 삭제할 개체를 큐에 대기할 때보다 복사본이 실제로 더 빠르게 제거되더라도 삭제가 더 느리게 진행되는 것처럼 보일 수 있습니다.
- 대량 삭제 중에 삭제 성능을 면밀히 모니터링하는 경우, 특정 수의 객체가 삭제된 후 삭제 속도가 느려질 수 있습니다. 이 변경은 StorageGRID가 삭제를 위해 오브젝트 큐잉에서 동기식 삭제 수행으로 변경될 때 발생합니다. 삭제 속도가 명백히 감소하는 것은 오브젝트 복사본이 더 느리게 제거된다는 의미가 아닙니다. 반면, 공간은 평균적으로 더 빠르게 확보되고 있음을 나타냅니다.

많은 수의 개체를 삭제하는 경우 우선 순위가 공간을 빠르게 확보하는 것이라면 클라이언트 요청을 사용하여 ILM 또는 다른 방법을 사용하여 개체를 삭제하지 않고 개체를 삭제하는 것이 좋습니다. 일반적으로 StorageGRID에서는 동기 삭제를 사용할 수 있으므로 클라이언트에서 삭제할 때 공간이 더 빠르게 확보됩니다.

객체를 삭제한 후 공간을 확보하는 데 필요한 시간은 다음과 같은 여러 요인에 따라 달라집니다.

- 오브젝트 복사본이 동기식으로 제거되는지, 아니면 나중에 제거를 위해 대기하는지(클라이언트 삭제 요청) 여부를 나타냅니다.

- 클라이언트 삭제 및 기타 방법 모두에 대해 개체 복사본이 제거용으로 대기될 때 그리드 내의 개체 수 또는 그리드 리소스의 사용 가능성 등의 기타 요소

S3 버전 오브젝트 삭제 방법

S3 버킷에 대해 버전 관리가 활성화된 경우 StorageGRID는 삭제 요청에 응답할 때 Amazon S3 동작을 따릅니다. 이러한 요청이 S3 클라이언트에서 온 것인지, S3 버킷 라이프사이클의 만료 또는 ILM 정책 요구사항이 있는지 여부에 관계없이 이 동작을 따릅니다.

오브젝트 버전이 지정된 경우 오브젝트 삭제 요청은 오브젝트의 현재 버전을 삭제하지 않고 공간을 확보하지 않습니다. 대신 개체 삭제 요청은 단순히 개체의 현재 버전으로 삭제 마커를 만들어 이전 버전의 개체를 ""비현재""로 만듭니다.

개체가 제거되지 않았더라도 StorageGRID 는 개체의 현재 버전을 더 이상 사용할 수 없는 것처럼 동작합니다. 해당 개체에 대한 요청은 404 NotFound 를 반환합니다. 그러나 현재 개체 데이터가 제거되지 않았으므로 개체의 현재 버전이 아닌 버전을 지정하는 요청은 성공할 수 있습니다.

버전이 지정된 개체를 삭제할 때 공간을 확보하려면 다음 중 하나를 수행해야 합니다.

- * S3 클라이언트 요청 *: S3 삭제 오브젝트 요청(삭제/오브젝트? versionId=ID')에서 오브젝트 버전 번호를 지정합니다. 이 요청은 지정된 버전의 오브젝트 복사본만 제거합니다(다른 버전은 계속 공간을 소모함).
- * 버킷 수명 주기 *: 버킷 수명 주기 구성에서 'NoncurrentVersionExpiration' 작업을 사용합니다. 지정된 NoncurrentDays 수가 충족되면 StorageGRID에서 현재 버전이 아닌 개체 버전의 모든 복사본을 영구적으로 제거합니다. 이러한 개체 버전은 복구할 수 없습니다.
- * ILM *: ILM 정책에 ILM 규칙 2개를 추가합니다. 첫 번째 규칙에서 * 비현재 시간 * 을 참조 시간으로 사용하여 개체의 비현재 버전과 일치시킵니다. 두 번째 규칙에 * Ingest Time * 을 사용하여 현재 버전과 일치시킵니다. noncurrent time * 규칙은 * Ingest time * 규칙 위의 정책에 나타나야 합니다.

관련 정보

- S3을 사용합니다
- 예 4: S3 버전 오브젝트에 대한 ILM 규칙 및 정책

ILM 정책이란 무엇인가

ILM(정보 수명 주기 관리) 정책은 StorageGRID 시스템이 시간 경과에 따라 오브젝트 데이터를 관리하는 방법을 결정하는 일련의 정렬된 ILM 규칙 세트입니다.

ILM 정책은 개체를 어떻게 평가합니까**?**

StorageGRID 시스템에 대한 활성 ILM 정책은 모든 개체의 배치, 기간 및 데이터 보호를 제어합니다.

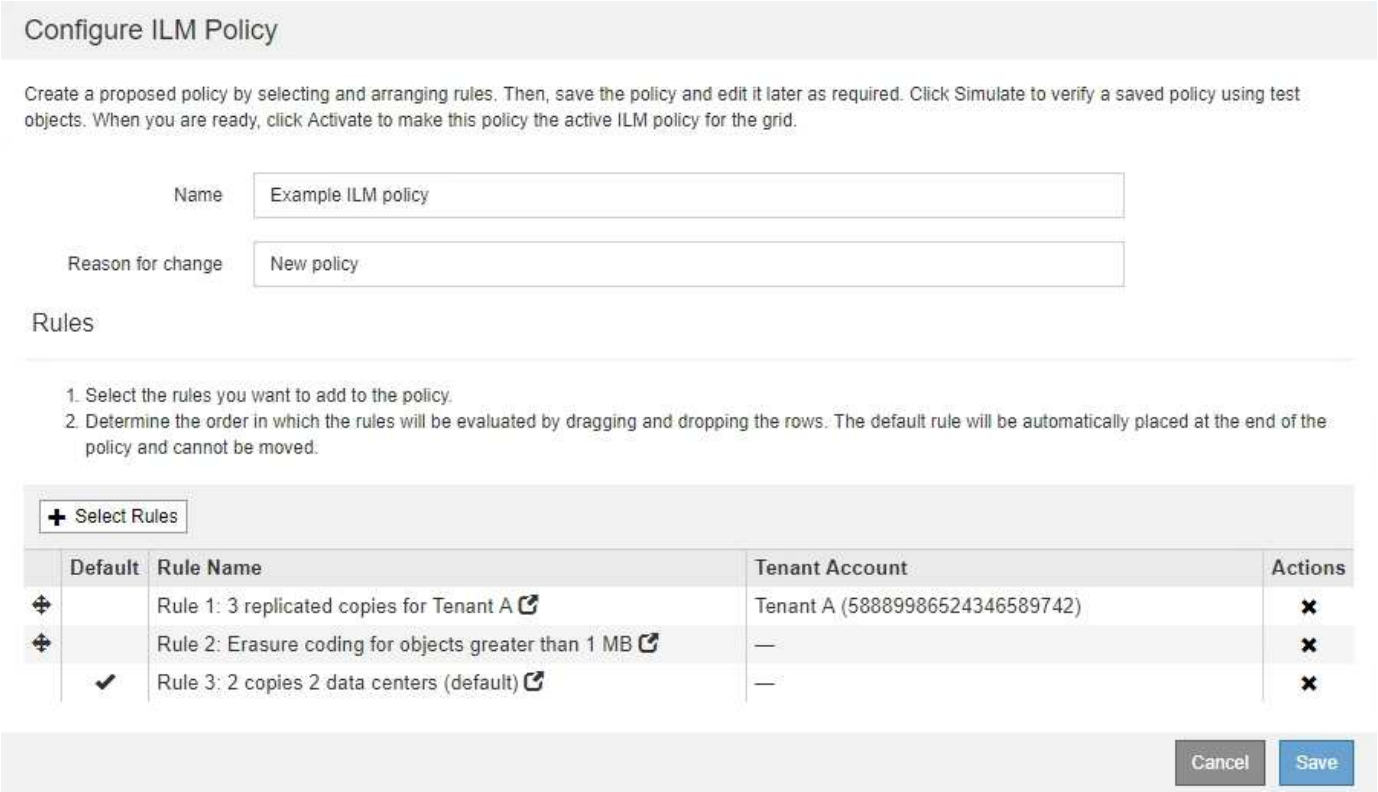
클라이언트가 개체를 StorageGRID에 저장하면 활성 정책에서 정렬된 ILM 규칙 집합에 대해 다음과 같이 개체가 평가됩니다.

1. 정책의 첫 번째 규칙에 대한 필터가 개체와 일치하면 해당 규칙의 수집 동작에 따라 개체가 수집되고 해당 규칙의 배치 지침에 따라 저장됩니다.
2. 첫 번째 규칙의 필터가 개체와 일치하지 않으면 일치하는 항목이 될 때까지 해당 개체가 정책의 다음 각 규칙에 대해 평가됩니다.
3. 개체와 일치하는 규칙이 없으면 정책의 기본 규칙에 대한 수집 동작 및 배치 지침이 적용됩니다. 기본 규칙은 정책의 마지막 규칙입니다. 기본 규칙은 모든 테넌트, 모든 버킷 및 모든 오브젝트 버전에 적용되며 고급 필터를 사용할 수

없습니다.

ILM 정책의 예

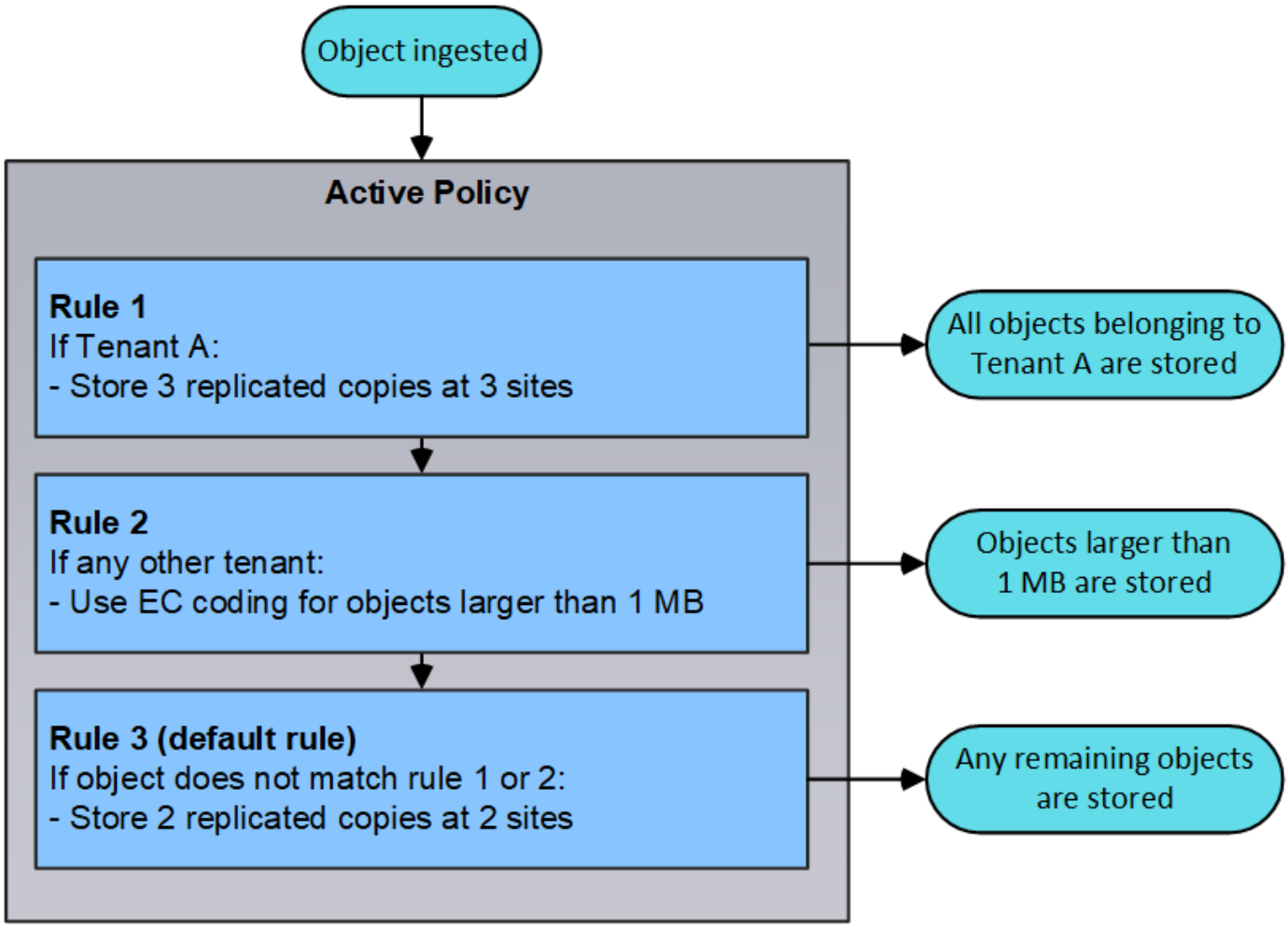
이 ILM 정책은 세 가지 ILM 규칙을 사용합니다.



이 예제에서 규칙 1은 테넌트 A에 속하는 모든 객체를 일치시킵니다 이러한 오브젝트는 3개의 사이트에 3개의 복제된 복사본으로 저장됩니다. 다른 테넌트에 속한 개체는 규칙 1에 의해 일치하지 않으므로 규칙 2에 대해 평가됩니다.

규칙 2는 다른 테넌트의 모든 객체를 일치하지만 1MB 이상인 경우에만 일치합니다. 이러한 큰 오브젝트는 3개의 사이트에서 6+3 삭제 코딩을 사용하여 저장됩니다. 규칙 2가 1MB 이하의 객체와 일치하지 않으므로 규칙 3에 대해 이러한 객체가 평가됩니다.

규칙 3은 정책의 마지막 기본 규칙이며 필터를 사용하지 않습니다. 규칙 3은 규칙 1 또는 규칙 2(1MB 이하의 테넌트 A에 속하지 않는 객체)에 의해 일치하지 않는 모든 객체의 복제된 복제본을 두 개 만듭니다.



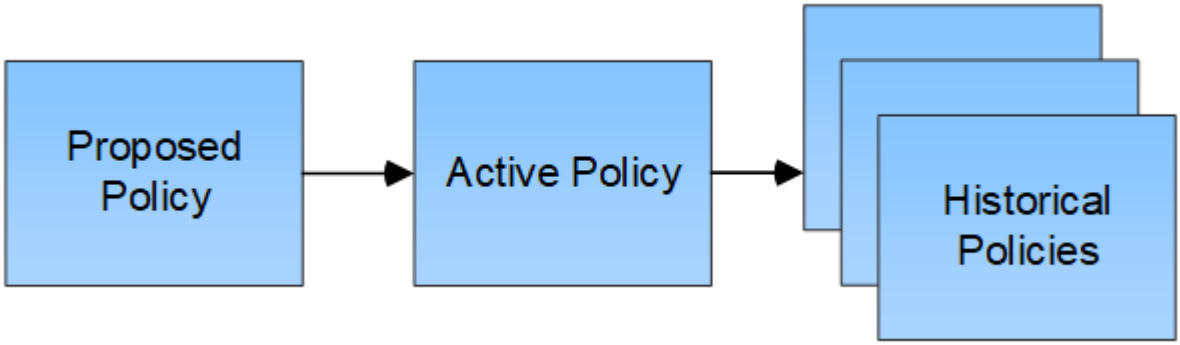
제안 정책, 활성 정책 및 기간별 정책이란 무엇입니까?

모든 StorageGRID 시스템에는 하나의 활성 ILM 정책이 있어야 합니다. StorageGRID 시스템에는 한 가지 제안된 ILM 정책과 수많은 기간별 정책도 포함될 수 있습니다.

ILM 정책을 처음 만들 때는 하나 이상의 ILM 규칙을 선택하고 특정 순서로 배열하여 제안된 정책을 만듭니다. 제안된 정책의 동작을 확인하기 위해 제안된 정책을 시뮬레이션한 후에는 이를 활성화하여 활성 정책을 생성합니다.

새로운 ILM 정책을 활성화하면 StorageGRID은 해당 정책을 사용하여 기존 오브젝트 및 새로 수집된 오브젝트를 포함한 모든 오브젝트를 관리합니다. 새 정책의 ILM 규칙을 구현할 때 기존 개체를 새 위치로 이동할 수 있습니다.

제안된 정책을 활성화하면 이전에 활성화된 정책이 기간별 정책이 됩니다. 내역 ILM 정책을 삭제할 수 없습니다.



관련 정보

ILM 규칙이란 무엇입니까

개체를 관리하려면 ILM(정보 수명 주기 관리) 규칙 집합을 만들어 ILM 정책으로 구성합니다. 시스템으로 수집된 모든 오브젝트는 활성 정책에 따라 평가됩니다. 정책의 규칙이 개체의 메타데이터와 일치하면 규칙의 지침에 따라 StorageGRID에서 해당 개체를 복사 및 저장하기 위해 수행할 작업이 결정됩니다.

ILM 규칙 정의:

- 어떤 오브젝트를 저장해야 하는지. 규칙은 모든 개체에 적용할 수 있으며, 규칙을 적용할 개체를 식별하는 필터를 지정할 수도 있습니다. 예를 들어, 규칙은 특정 테넌트 계정, 특정 S3 버킷 또는 Swift 컨테이너 또는 특정 메타데이터 값과 연결된 오브젝트에만 적용할 수 있습니다.
- 스토리지 유형 및 위치입니다. 오브젝트는 스토리지 노드, 클라우드 스토리지 풀 또는 아카이브 노드에 저장할 수 있습니다.
- 생성된 오브젝트 복사본의 유형입니다. 복사본을 복제하거나 삭제 코딩할 수 있습니다.
- 복제된 복사본의 경우 생성된 복사본 수입니다.
- 삭제 코딩 복사본의 경우 삭제 코딩 방법을 사용합니다.
- 시간이 지나면서 개체의 스토리지 위치 및 복사본 유형이 변경됩니다.
- 오브젝트를 그리드에 수집하면서 오브젝트 데이터를 보호하는 방법(동기식 배치 또는 이중 커밋)

개체 메타데이터는 ILM 규칙에 의해 관리되지 않습니다. 대신 오브젝트 메타데이터는 메타데이터 저장소라고 하는 Cassandra 데이터베이스에 저장됩니다. 데이터가 손실되지 않도록 보호하기 위해 각 사이트에 오브젝트 메타데이터의 복사본 3개가 자동으로 유지됩니다. 복제본은 모든 스토리지 노드에 균등하게 분산됩니다.

ILM 규칙 요소

ILM 규칙에는 다음 세 가지 요소가 있습니다.

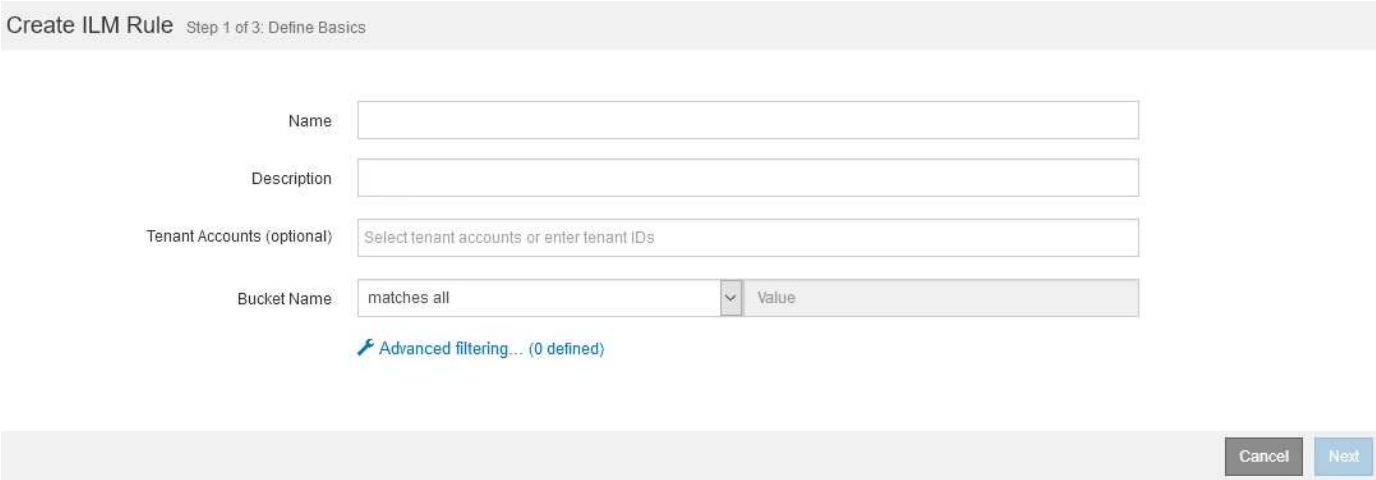
- * 필터링 기준 *: 규칙의 기본 및 고급 필터는 규칙이 적용되는 개체를 정의합니다. 개체가 모든 필터와 일치하면 StorageGRID는 규칙을 적용하고 규칙의 배치 지침에 지정된 개체 복사본을 만듭니다.
- * 배치 지침 *: 규칙의 배치 지침은 개체 사본의 수, 유형 및 위치를 정의합니다. 각 규칙에는 시간에 따라 개체 복사본의 수, 유형 및 위치를 변경하는 배치 지침 시퀀스가 포함될 수 있습니다. 한 배치의 기간이 만료되면 다음 배치의 지침은 다음 ILM 평가에 의해 자동으로 적용됩니다.
- * Ingest 동작 *: S3 또는 Swift 클라이언트가 오브젝트를 그리드에 저장할 때 규칙의 수집 동작이 발생하는 상황을 정의합니다. 수집 동작은 규칙의 지침에 따라 오브젝트 복사본을 즉시 배치할지, 중간 복사본을 만들어 나중에 배치 지침을 적용할지 여부를 제어합니다.

ILM 규칙 필터링이란 무엇입니까

ILM 규칙을 만들 때 규칙이 적용되는 개체를 식별하는 필터를 지정합니다.

가장 간단한 경우 규칙에서 필터를 사용하지 않을 수 있습니다. 필터를 사용하지 않는 규칙은 모든 개체에 적용되므로 ILM 정책의 마지막(기본) 규칙이어야 합니다. 기본 규칙은 다른 규칙의 필터와 일치하지 않는 개체에 대한 저장 지침을 제공합니다.

기본 필터를 사용하면 크고 서로 다른 개체 그룹에 다른 규칙을 적용할 수 있습니다. ILM 규칙 생성 마법사의 기본 정의 페이지에 있는 기본 필터를 사용하면 특정 테넌트 계정, 특정 S3 버킷 또는 Swift 컨테이너 또는 둘 다에 규칙을 적용할 수 있습니다.



이러한 기본 필터를 사용하면 여러 개체에 다른 규칙을 간단히 적용할 수 있습니다. 예를 들어, 회사의 재무 기록을 규정 요구 사항에 맞게 저장해야 할 수 있고 마케팅 부서의 데이터를 저장하여 일상적인 운영을 용이하게 해야 할 수 있습니다. 각 부서에 대해 별도의 테넌트 계정을 생성하거나 서로 다른 부서의 데이터를 별도의 S3 버킷으로 분리한 후에는 모든 재무 레코드에 적용되는 하나의 규칙과 모든 마케팅 데이터에 적용되는 두 번째 규칙을 쉽게 생성할 수 있습니다.

ILM 규칙 생성 마법사의 * 고급 필터링 * 페이지에서 세부적인 제어가 가능합니다. 필터를 만들어 다음 개체 속성을 기준으로 개체를 선택할 수 있습니다.

- 수집 시간
- 마지막 액세스 시간입니다
- 개체 이름의 전체 또는 일부(키)
- S3 버킷 영역(위치 제한)
- 개체 크기
- 사용자 메타데이터
- S3 오브젝트 태그

매우 구체적인 기준에 따라 개체를 필터링할 수 있습니다. 예를 들어, 병원 영상 촬영 부서에서 저장한 객체는 30일 미만이고 나중에 자주 사용되지 않을 수 있으며, 환자 방문 정보가 포함된 객체는 의료 네트워크 본사의 청구 부서에 복사해야 할 수 있습니다. 오브젝트 이름, 크기, S3 오브젝트 태그 또는 기타 관련 기준을 기반으로 각 오브젝트 유형을 식별하는 필터를 생성한 다음, 각 오브젝트 세트를 적절히 저장하는 별도의 규칙을 생성할 수 있습니다.

필요에 따라 기본 필터와 고급 필터를 단일 규칙으로 결합할 수도 있습니다. 예를 들어, 마케팅 부서는 큰 이미지 파일을 공급업체 기록과 다르게 저장하기를 원할 수 있으며 인사 부서에서는 특정 지역 및 정책 정보에 직원 레코드를 중앙 집중식으로 저장해야 할 수 있습니다. 이 경우 테넌트 계정을 기준으로 필터링하여 각 부서의 레코드를 분리하는 규칙을 만들 수 있으며, 각 규칙에서 고급 필터를 사용하여 규칙이 적용되는 특정 유형의 개체를 식별할 수 있습니다.

ILM 규칙 배치 지침은 무엇입니까

배치 지침은 오브젝트 데이터의 저장 위치, 시기 및 방법을 결정합니다. ILM 규칙에는 하나 이상의 배치 지침이 포함될 수 있습니다. 각 배치 지침은 단일 기간에 적용됩니다.

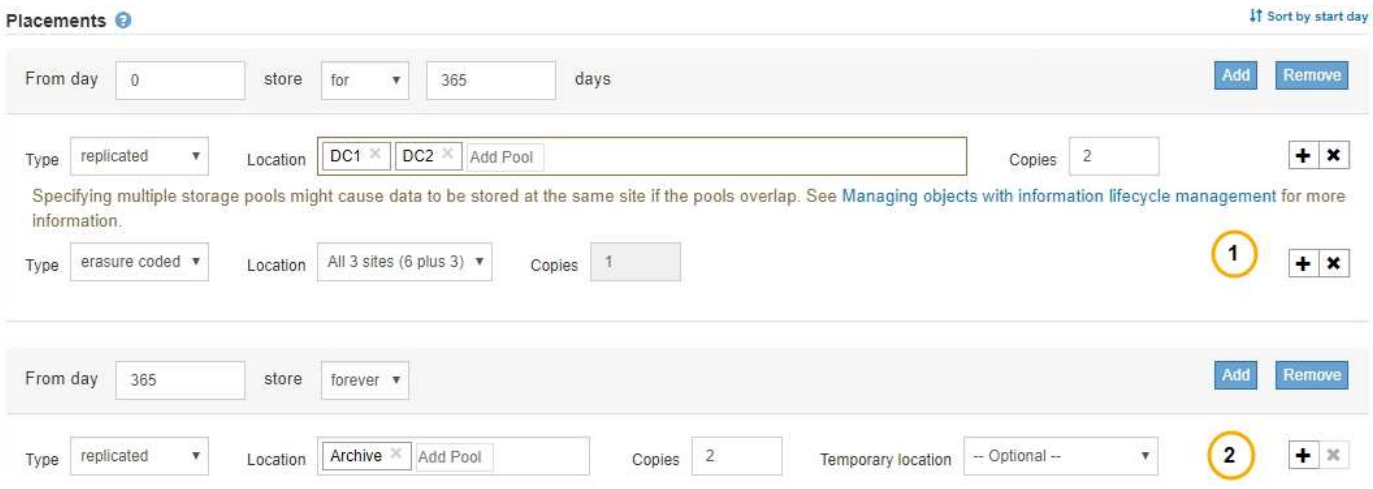
배치 지침을 작성할 때:

- 시작 시간은 참조 시간을 지정하며, 이 시간은 배치 지침이 시작되는 시점을 결정합니다. 참조 시간은 개체가 수집되거나, 개체에 액세스할 때, 버전이 지정된 개체가 최신 상태가 아니거나, 사용자가 정의한 시간이 될 수 있습니다.
- 그런 다음 참조 시간을 기준으로 배치 적용 시점을 지정합니다. 예를 들어, 오브젝트가 수집된 시점을 기준으로 0일부터 365일 동안 배치가 시작될 수 있습니다.
- 마지막으로 복사본의 유형(복제 또는 삭제 코딩) 및 복사본이 저장되는 위치를 지정합니다. 예를 들어 두 개의 복제된 복사본을 서로 다른 사이트에 저장할 수 있습니다.

각 규칙은 단일 기간에 대해 여러 배치를 정의하고 다른 기간에 대해 여러 배치를 정의할 수 있습니다.

- 단일 기간 동안 여러 위치에 오브젝트를 배치하려면 더하기 기호 아이콘을 선택합니다 ✚ 를 눌러 해당 기간에 대해 두 개 이상의 라인을 추가합니다.
- 서로 다른 기간의 다른 위치에 오브젝트를 배치하려면 * 추가 * 버튼을 선택하여 다음 기간을 추가합니다. 그런 다음 기간 내에 하나 이상의 라인을 지정합니다.

이 예에서는 ILM 규칙 생성 마법사의 배치 정의 페이지를 보여 줍니다.



1	첫 번째 배치 지침은 첫 해에 두 줄로 표시됩니다. 1. 첫 번째 줄에서는 두 개의 데이터 센터 사이트에 두 개의 복제된 개체 복사본을 만듭니다. 2. 두 번째 줄에서는 세 개의 데이터 센터 사이트를 사용하여 6+3 삭제 코딩 복사본을 만듭니다.
2	두 번째 배치 지침은 1년 후에 두 개의 보관 사본을 생성하고 해당 사본을 영구적으로 보관합니다.

규칙에 대한 배치 지침 집합을 정의할 때는 적어도 1개의 배치 지침이 0일차에 시작되는지, 정의한 기간 사이에 간격이 없는지 확인해야 합니다. 그리고 최종 배치 지침은 영구 또는 더 이상 오브젝트 복사본이 필요하지 않을 때까지 계속됩니다.

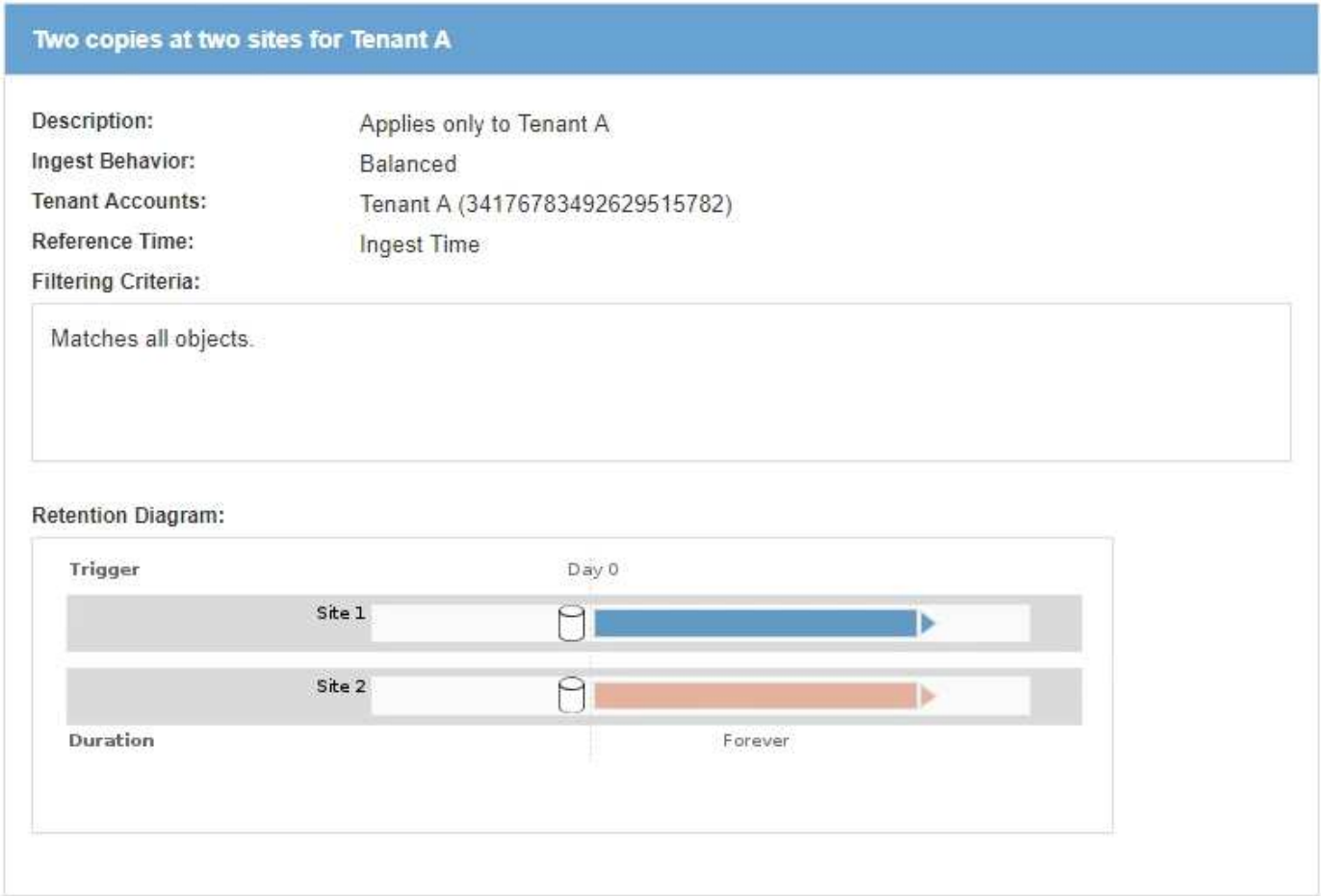
규칙의 각 기간이 만료되면 다음 기간에 대한 콘텐츠 배치 지침이 적용됩니다. 새 오브젝트 복사본이 생성되고 불필요한

복사본이 삭제됩니다.

ILM 규칙 예

이 ILM 규칙 예는 테넌트 A에 속하는 객체에 적용됩니다 즉, 이러한 객체의 복제본을 두 개 생성하고 각 복제본을 다른 사이트에 저장합니다. 두 개의 사본은 영구 보관되어 있습니다. 즉, StorageGRID는 이를 자동으로 삭제하지 않습니다. 대신, StorageGRID는 이러한 객체가 클라이언트 삭제 요청에 의해 삭제되거나 버킷 수명 주기가 만료될 때까지 해당 객체를 유지합니다.

이 규칙은 수집 동작에 균형 옵션을 사용합니다. 테넌트 A가 개체를 StorageGRID에 저장하는 즉시 두 사이트 배치 명령이 적용됩니다. 단, 두 필요한 복제본을 모두 즉시 생성할 수 없습니다. 예를 들어 테넌트 A가 객체를 저장할 때 사이트 2에 연결할 수 없는 경우 StorageGRID는 사이트 1의 스토리지 노드에 두 개의 중간 복제본을 만듭니다. 사이트 2를 사용할 수 있게 되면 StorageGRID는 해당 사이트에서 필요한 복사본을 만듭니다.



관련 정보

- 데이터 보호를 위한 수집 옵션
- 스토리지 풀의 정의
- 클라우드 스토리지 풀은 무엇입니까

스토리지 등급, 스토리지 풀, **EC** 프로파일 및 영역을 생성합니다

저장 점수를 생성하고 할당합니다

스토리지 등급은 스토리지 노드에서 사용하는 스토리지 유형을 식별합니다. ILM 규칙이 사이트의 모든 노드 대신 특정 스토리지 노드에 특정 객체를 배치하도록 하려는 경우 스토리지 성적을 생성할 수 있습니다. 예를 들어, StorageGRID All-Flash 스토리지 어플라이언스 와 같이 가장 빠른 스토리지 노드에 특정 오브젝트를 저장할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

둘 이상의 스토리지 유형을 사용하는 경우 필요에 따라 스토리지 등급을 생성하여 각 유형을 식별할 수 있습니다. 스토리지 등급을 생성하면 스토리지 풀을 구성할 때 특정 유형의 스토리지 노드를 선택할 수 있습니다.

스토리지 등급이 문제가 되지 않는 경우(예: 모든 스토리지 노드가 동일함), 이 절차를 건너뛰고 스토리지 풀을 구성할 때 모든 스토리지 노드 기본 스토리지 등급을 사용할 수 있습니다.

확장 시 새 스토리지 노드를 추가하면 해당 노드가 모든 스토리지 노드 기본 스토리지 등급에 추가됩니다. 그 결과,

- ILM 규칙이 모든 스토리지 노드 등급이 있는 스토리지 풀을 사용하는 경우 확장이 완료된 직후 새 노드를 사용할 수 있습니다.
- ILM 규칙이 사용자 지정 스토리지 등급이 있는 스토리지 풀을 사용하는 경우 아래 설명된 대로 사용자 지정 스토리지 등급을 노드에 수동으로 할당해야 새 노드가 사용됩니다.

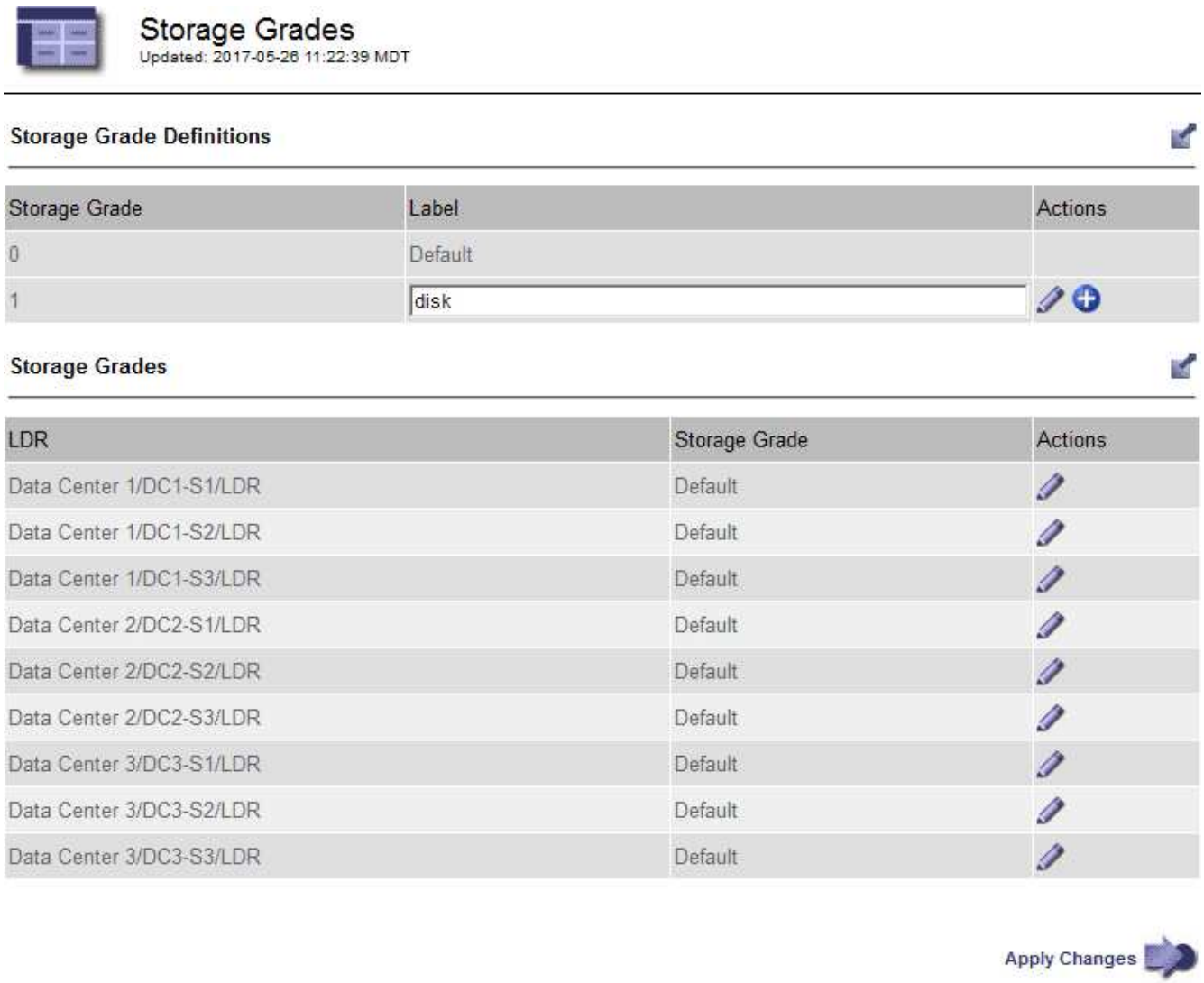
> 저장 등급을 생성할 때 필요한 것보다 더 많은 저장 등급을 생성하지 마십시오. 예를 들어, 각 스토리지 노드에 대해 하나의 스토리지 등급을 생성하지 마십시오. 대신 각 스토리지 등급을 2개 이상의 노드에 할당합니다. 한 노드에만 할당된 스토리지 등급은 해당 노드를 사용할 수 없게 될 경우 ILM 백로그를 유발할 수 있습니다.

단계

1. ILM * > * 스토리지 등급 * 을 선택합니다.
2. 스토리지 등급 생성:

   a. 정의해야 하는 각 스토리지 등급에 대해 * Insert * 를 선택합니다 ⊕ 행을 추가하고 스토리지 평점의 레이블을 입력합니다.

      기본 스토리지 등급은 수정할 수 없습니다. 이 노드는 StorageGRID 시스템 확장 중에 추가된 새 스토리지 노드용으로 예약되어 있습니다.



a. 기존 스토리지 평점을 편집하려면 * Edit * 를 선택합니다 레이블을 필요에 따라 수정합니다.

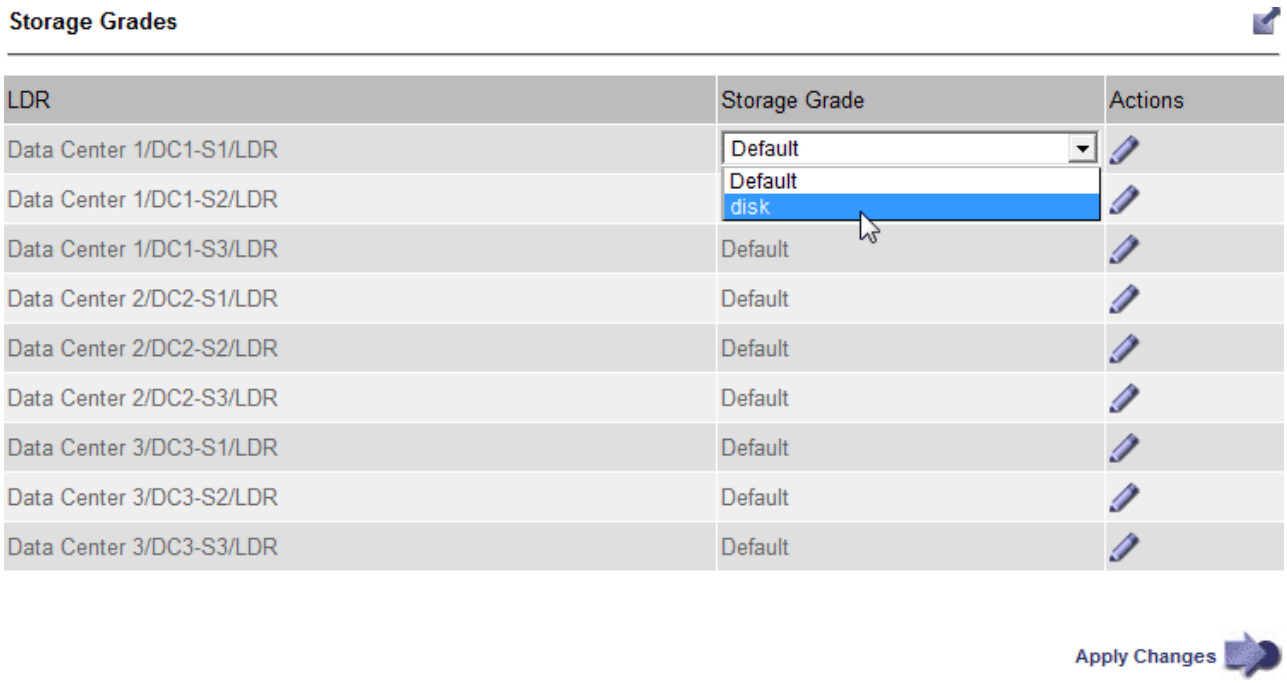
> 저장 평점을 삭제할 수 없습니다.

b. Apply Changes * 를 선택합니다.

이러한 스토리지 등급은 이제 스토리지 노드에 할당할 수 있습니다.

3. 스토리지 노드에 스토리지 등급 할당:

a. 각 스토리지 노드의 LDR 서비스에 대해 * Edit * 를 선택합니다 목록에서 스토리지 평점을 선택합니다.



> 지정된 스토리지 노드에 스토리지 등급을 한 번만 할당합니다. 장애에서 복구된 스토리지 노드는 이전에 할당된 스토리지 등급을 유지합니다. ILM 정책이 활성화된 후에는 이 할당을 변경하지 마십시오. 할당이 변경되면 새 스토리지 등급에 따라 데이터가 저장됩니다.

a. Apply Changes * 를 선택합니다.

스토리지 풀을 구성합니다

스토리지 풀의 정의

스토리지 풀은 스토리지 노드 또는 아카이브 노드의 논리적 그룹입니다. 스토리지 풀을 구성하여 StorageGRID 시스템에서 객체 데이터를 저장하는 위치와 사용된 스토리지 유형을 결정합니다.

스토리지 풀에는 두 가지 특성이 있습니다.

- * 스토리지 등급 *: 스토리지 노드의 경우 백업 스토리지의 상대적 성능을 나타냅니다.
- * 사이트 *: 오브젝트를 저장할 데이터 센터.

스토리지 풀은 ILM 규칙에 따라 오브젝트 데이터가 저장되는 위치를 결정하는 데 사용됩니다. 복제에 대한 ILM 규칙을 구성할 때 스토리지 노드 또는 아카이브 노드를 포함하는 하나 이상의 스토리지 풀을 선택합니다. 삭제 코딩 프로필을 생성할 때 스토리지 노드를 포함하는 스토리지 풀을 선택합니다.

스토리지 풀 생성 지침

스토리지 풀을 구성 및 사용할 때는 다음 지침을 따르십시오.

모든 스토리지 풀에 대한 지침입니다

- StorageGRID에는 기본 사이트, 모든 사이트 및 기본 스토리지 등급인 모든 스토리지 노드를 사용하는 기본 스토리지 풀인 모든 스토리지 노드가 포함됩니다. 새 데이터 센터 사이트를 추가할 때마다 모든 스토리지 노드 스토리지 풀이 자동으로 업데이트됩니다.

> 모든 스토리지 노드 스토리지 풀 또는 모든 사이트 사이트를 사용하는 것은 권장되지 않습니다. 이러한 항목은 확장에 추가한 새 사이트를 포함하도록 자동으로 업데이트되기 때문에 원하는 동작이 아닐 수 있습니다. 모든 스토리지 노드 스토리지 풀 또는 기본 사이트를 사용하기 전에 복제된 복사본 및 삭제 코딩 복사본에 대한 지침을 주의 깊게 검토하십시오.

- 스토리지 풀 구성을 가능한 한 단순하게 유지합니다. 필요한 것보다 더 많은 스토리지 풀을 생성하지 마십시오.
- 가능한 한 많은 노드를 포함하는 스토리지 풀을 생성합니다. 각 스토리지 풀에는 둘 이상의 노드가 포함되어야 합니다. 노드가 부족한 스토리지 풀은 노드를 사용할 수 없게 될 경우 ILM 백로그를 유발할 수 있습니다.
- 중복되는 스토리지 풀을 생성하거나 사용하지 마십시오(동일한 노드 중 하나 이상 포함). 스토리지 풀이 중복될 경우 오브젝트 데이터의 복제본이 동일한 노드에 저장될 수 있습니다.

복제된 복제본에 사용되는 스토리지 풀에 대한 지침입니다

- 각 사이트에 대해 다른 스토리지 풀을 생성합니다. 그런 다음 각 규칙의 배치 지침에 하나 이상의 사이트별 스토리지 풀을 지정합니다. 각 사이트에 스토리지 풀을 사용하면 복제된 개체 복사본이 원하는 위치에 정확하게 배치됩니다. 예를 들어, 사이트 손실 방지를 위해 각 사이트에 있는 모든 개체의 복사본이 하나씩 배치됩니다.
- 확장 시 사이트를 추가하는 경우 새 사이트의 새 스토리지 풀을 생성합니다. 그런 다음 ILM 규칙을 업데이트하여 새 사이트에 저장된 개체를 제어합니다.
- 일반적으로 기본 스토리지 풀, 모든 스토리지 노드 또는 기본 사이트, 모든 사이트를 포함하는 스토리지 풀을 사용하지 마십시오.

삭제 코딩 복사본에 사용되는 스토리지 풀에 대한 지침입니다

- 삭제 코딩 데이터에는 아카이브 노드를 사용할 수 없습니다.
- 스토리지 풀에 포함된 스토리지 노드 및 사이트의 수에 따라 사용 가능한 삭제 코딩 체계가 결정됩니다.
- 스토리지 풀에 사이트가 두 개만 포함된 경우 해당 스토리지 풀을 삭제 코딩에 사용할 수 없습니다. 두 개의 사이트가 있는 스토리지 풀에는 삭제 코딩 스키마를 사용할 수 없습니다.
- 일반적으로 기본 스토리지 풀, 모든 스토리지 노드 또는 기본 사이트, 삭제 코딩 프로필의 모든 사이트를 포함하는 스토리지 풀을 사용하지 마십시오.

> 그리드에 사이트가 하나만 포함된 경우 모든 스토리지 노드 스토리지 풀 또는 모든 사이트 기본 사이트를 삭제 코딩 프로파일에서 사용할 수 없습니다. 이 동작은 두 번째 사이트가 추가된 경우 삭제 코딩 프로필이 무효로 되는 것을 방지합니다.

- 처리량이 많은 경우 사이트 간 네트워크 지연 시간이 100ms를 초과하는 경우 여러 사이트를 포함하는 스토리지 풀을 생성하지 않는 것이 좋습니다. 지연 시간이 늘어날수록 StorageGRID에서 TCP 네트워크 처리량이 감소하기 때문에 개체 조각을 생성, 배치 및 검색할 수 있는 속도가 급격하게 줄어듭니다. 처리량 감소는 오브젝트 수집 및 검색의 최대 달성 가능 속도(Ingest 동작으로 Strict 또는 Balanced를 선택한 경우)에 영향을 미치거나 ILM 대기열 백로그(Ingest 동작으로 이중 커밋을 선택한 경우)로 이어질 수 있습니다.
- 가능한 경우 스토리지 풀에 선택한 삭제 코딩 체계에 필요한 최소 스토리지 노드 수보다 많은 수가 포함되어야 합니다. 예를 들어, 6+3 삭제 코딩 체계를 사용하는 경우 9개 이상의 스토리지 노드가 있어야 합니다. 그러나 사이트당 스토리지 노드를 하나 이상 추가하는 것이 좋습니다.
- 가능한 한 사이트 간에 스토리지 노드를 균등하게 분산합니다. 예를 들어, 6+3 삭제 코딩 체계를 지원하려면 세 개 사이트에 세 개 이상의 스토리지 노드를 포함하는 스토리지 풀을 구성합니다.

아카이빙된 복제본에 사용되는 스토리지 풀에 대한 지침입니다

- 스토리지 노드와 아카이브 노드를 모두 포함하는 스토리지 풀은 생성할 수 없습니다. 아카이빙된 복제본에는 아카이브 노드만 포함된 스토리지 풀이 필요합니다.
- 아카이브 노드가 포함된 스토리지 풀을 사용하는 경우 스토리지 노드가 포함된 스토리지 풀에서 하나 이상의 복제된 복사본 또는 삭제 코딩 복사본도 유지 관리해야 합니다.
- 글로벌 S3 오브젝트 잠금 설정이 활성화되어 있고 호환되는 ILM 규칙을 생성하는 경우 아카이브 노드가 포함된 스토리지 풀을 사용할 수 없습니다. S3 오브젝트 잠금을 사용하여 오브젝트를 관리하는 지침을 참조하십시오.
- 아카이브 노드의 타겟 유형이 Cloud Tiering - Simple Storage Service(S3)인 경우 아카이브 노드는 자체 스토리지 풀에 있어야 합니다. 을 참조하십시오 StorageGRID 관리.

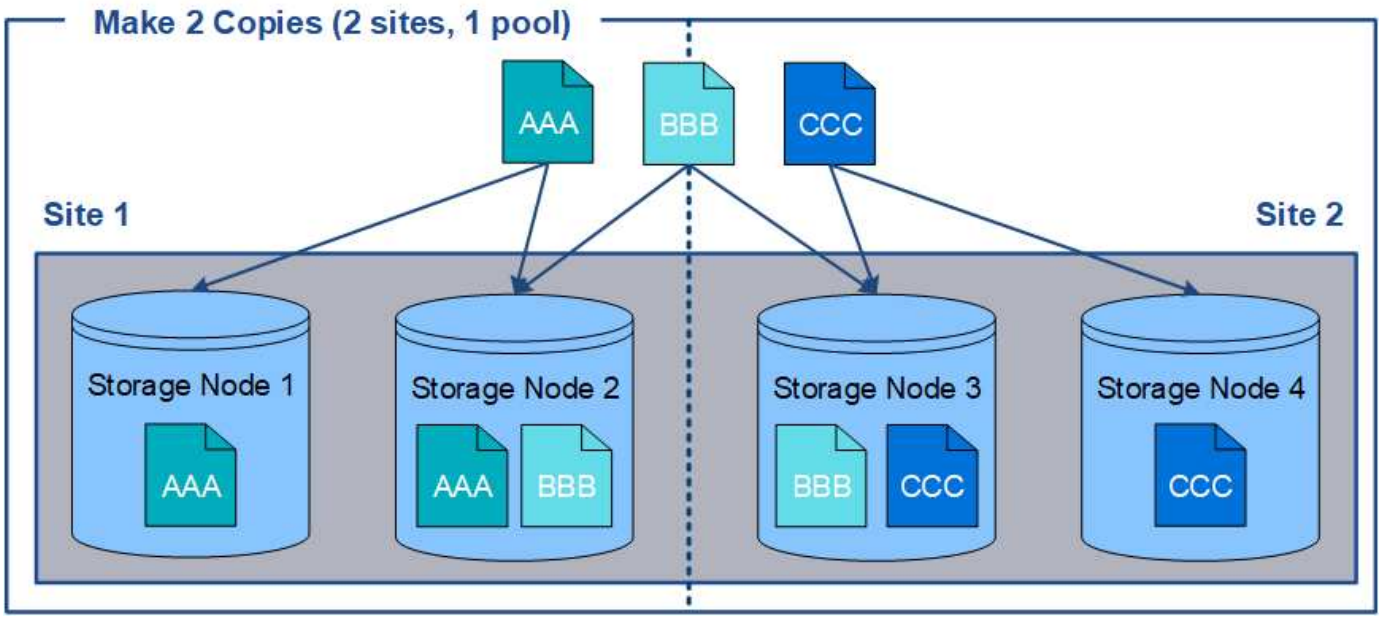
관련 정보

- 복제란
- 삭제 코딩이란 무엇입니까
- 어떤 삭제 코딩 구성인지
- 사이트 간 복제에 여러 스토리지 풀을 사용합니다

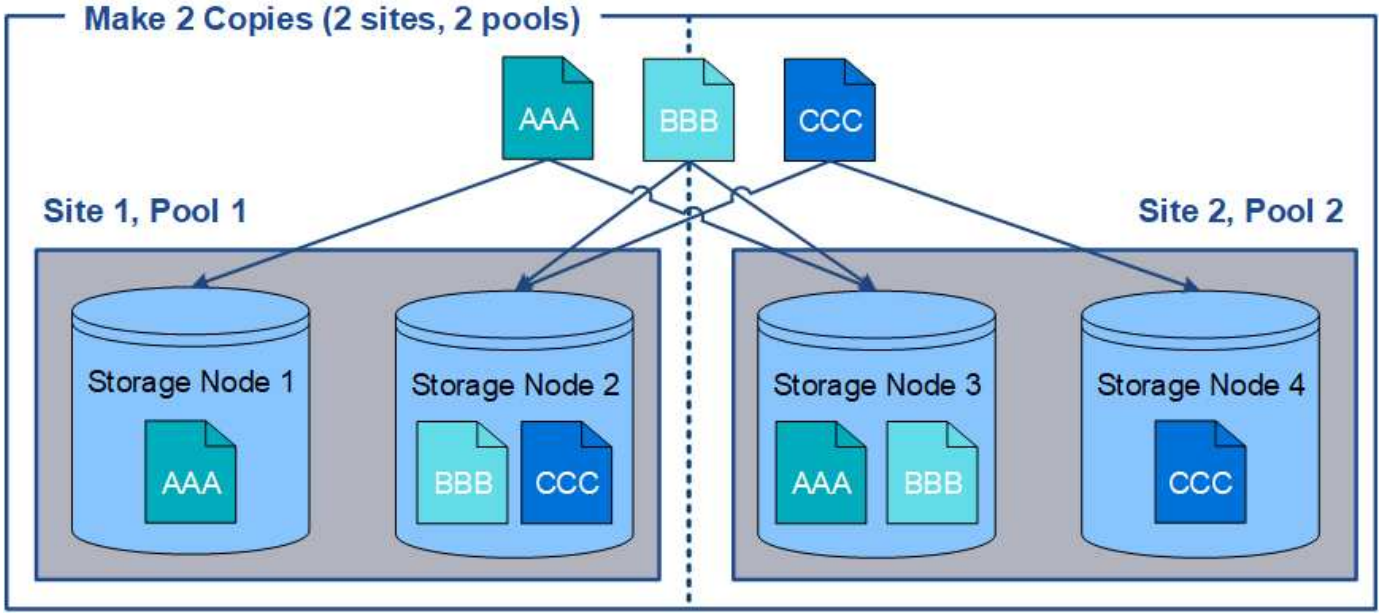
사이트 간 복제에 여러 스토리지 풀을 사용합니다

StorageGRID 구축에 사이트가 두 개 이상 포함된 경우 각 사이트에 대해 스토리지 풀을 생성하고 규칙 배치 지침에 두 스토리지 풀을 모두 지정하여 사이트 손실 보호를 설정할 수 있습니다. 예를 들어, ILM 규칙을 구성하여 두 개의 복제된 복사본을 만들고 두 사이트의 스토리지 풀을 지정하는 경우 각 개체의 복사본이 각 사이트에 배치됩니다. 복제본을 두 개 생성하고 스토리지 풀을 세 개 지정하도록 규칙을 구성하면 복제본이 분산되어 스토리지 풀 간에 디스크 사용량을 분산하고 두 복제본이 서로 다른 사이트에 저장되도록 합니다.

다음 예에서는 ILM 규칙이 두 사이트의 스토리지 노드가 포함된 단일 스토리지 풀에 복제된 오브젝트 복사본을 배치하는 경우 발생할 수 있는 작업을 보여 줍니다. 시스템은 복제된 복사본을 저장할 때 스토리지 풀에서 사용 가능한 노드를 사용하기 때문에 사이트 중 하나에 일부 객체의 모든 복제본을 배치할 수 있습니다. 이 예에서 시스템은 사이트 1의 스토리지 노드에 2개의 AAA 객체 복사본과 사이트 2의 스토리지 노드에 CCC 객체 복사본을 저장했습니다. 사이트 중 하나에 장애가 발생하거나 액세스할 수 없게 되면 객체 BBB만 보호됩니다.



반면, 이 예제에서는 여러 스토리지 풀을 사용할 때 객체가 저장되는 방식을 보여 줍니다. 이 예제에서 ILM 규칙은 각 개체의 복제된 복사본 2개를 생성하고 해당 복사본을 두 스토리지 풀에 분산하도록 지정합니다. 각 스토리지 풀에는 한 사이트의 모든 스토리지 노드가 포함됩니다. 각 개체의 복사본은 각 사이트에 저장되므로 사이트 장애나 액세스 불가능성 으로부터 개체 데이터가 보호됩니다.



여러 스토리지 풀을 사용할 때는 다음 규칙을 염두에 두십시오.

- n개의 복제본을 생성하는 경우 n 개 이상의 스토리지 풀을 추가해야 합니다. 예를 들어, 규칙이 세 개의 복제본을 만들 수 있도록 구성된 경우 스토리지 풀을 세 개 이상 지정해야 합니다.
- 복제본 수가 스토리지 풀 수와 같으면 객체 복제본 하나가 각 스토리지 풀에 저장됩니다.
- 복제본 수가 스토리지 풀 수보다 적은 경우 시스템은 복제본을 분산하여 풀 간에 디스크 사용량을 균형 있게 유지하고 두 개 이상의 복제본이 동일한 스토리지 풀에 저장되지 않도록 합니다.
- 스토리지 풀이 겹칠 경우(동일한 스토리지 노드 포함) 개체의 모든 복제본이 하나의 사이트에만 저장될 수 있습니다. 선택한 스토리지 풀에 동일한 스토리지 노드가 포함되어 있지 않은지 확인해야 합니다.

스토리지 풀을 임시 위치로 사용(더 이상 사용 안 함)

단일 스토리지 풀이 포함된 개체 배치로 ILM 규칙을 생성할 때 임시 위치로 사용할 두 번째 스토리지 풀을 지정하라는 메시지가 표시됩니다.

임시 위치는 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다. 새 ILM 규칙을 위한 임시 위치로 스토리지 풀을 선택해서는 안 됩니다.

> ILM 규칙 생성 마법사의 3단계(Strict 수집 동작)를 선택하면 임시 위치가 무시됩니다.

관련 정보

데이터 보호를 위한 수집 옵션

스토리지 풀을 생성합니다

스토리지 풀을 생성하여 StorageGRID 시스템에서 오브젝트 데이터를 저장하는 위치와 사용된 스토리지 유형을 결정합니다. 각 스토리지 풀에는 하나 이상의 사이트와 하나 이상의 스토리지 등급이 포함됩니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- 스토리지 풀 생성에 대한 지침을 검토했습니다.

이 작업에 대해

스토리지 풀은 오브젝트 데이터가 저장되는 위치를 결정합니다. 필요한 스토리지 풀 수는 그리드에 있는 사이트 수와 원하는 복제본 유형(복제 또는 삭제 코딩)에 따라 달라집니다.

- 복제 및 단일 사이트 삭제 코딩의 경우 각 사이트에 대한 스토리지 풀을 생성합니다. 예를 들어, 복제된 오브젝트 복사본을 세 사이트에 저장하려면 세 개의 스토리지 풀을 생성합니다.
- 3개 이상의 사이트에서 삭제 코딩하려면 각 사이트에 대한 항목이 포함된 스토리지 풀 하나를 생성합니다. 예를 들어, 세 사이트에서 오브젝트를 삭제하려면 스토리지 풀 하나를 생성합니다. 더하기 아이콘을 선택합니다 ➕ 각 사이트에 대한 항목을 추가합니다.

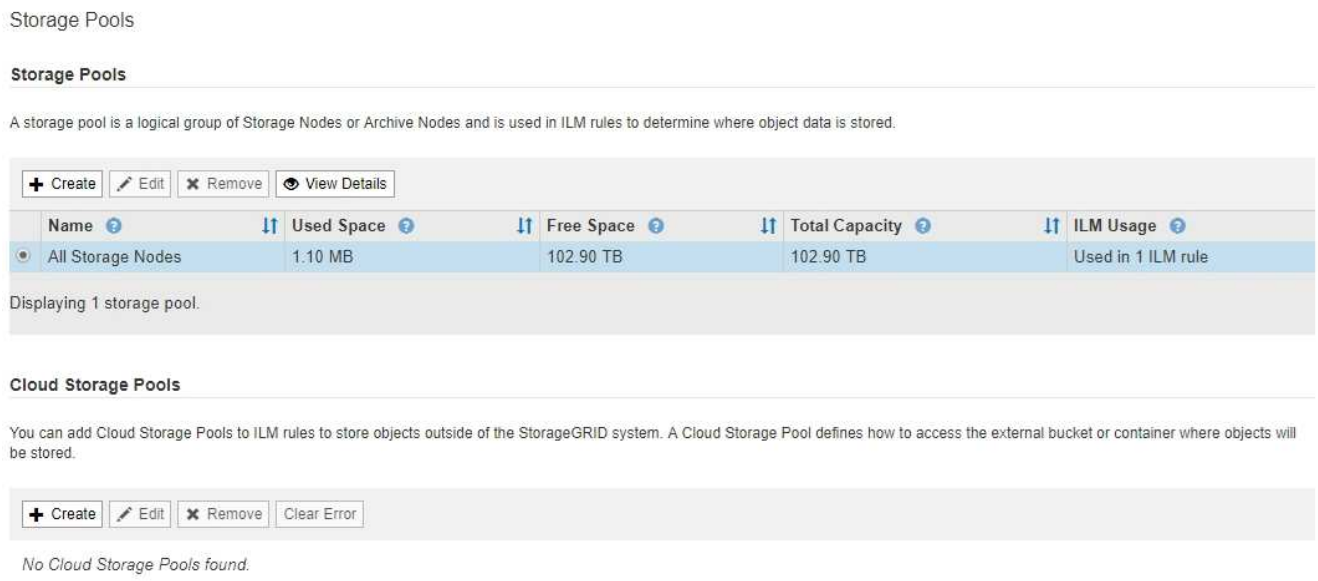
> 삭제 코딩 프로필에 사용할 스토리지 풀의 기본 모든 사이트 사이트를 포함하지 마십시오. 대신 삭제 코딩 데이터를 저장할 각 사이트의 스토리지 풀에 별도의 항목을 추가합니다. 을 참조하십시오 이 단계 예를 들어,

- 스토리지 등급이 두 개 이상인 경우 단일 사이트에서 서로 다른 스토리지 등급이 포함된 스토리지 풀을 생성하지 마십시오. 를 참조하십시오 스토리지 풀 생성 지침.

단계

1. ILM * > * 스토리지 풀 * 을 선택합니다.

   스토리지 풀 페이지가 나타나고 정의된 모든 스토리지 풀이 나열됩니다.

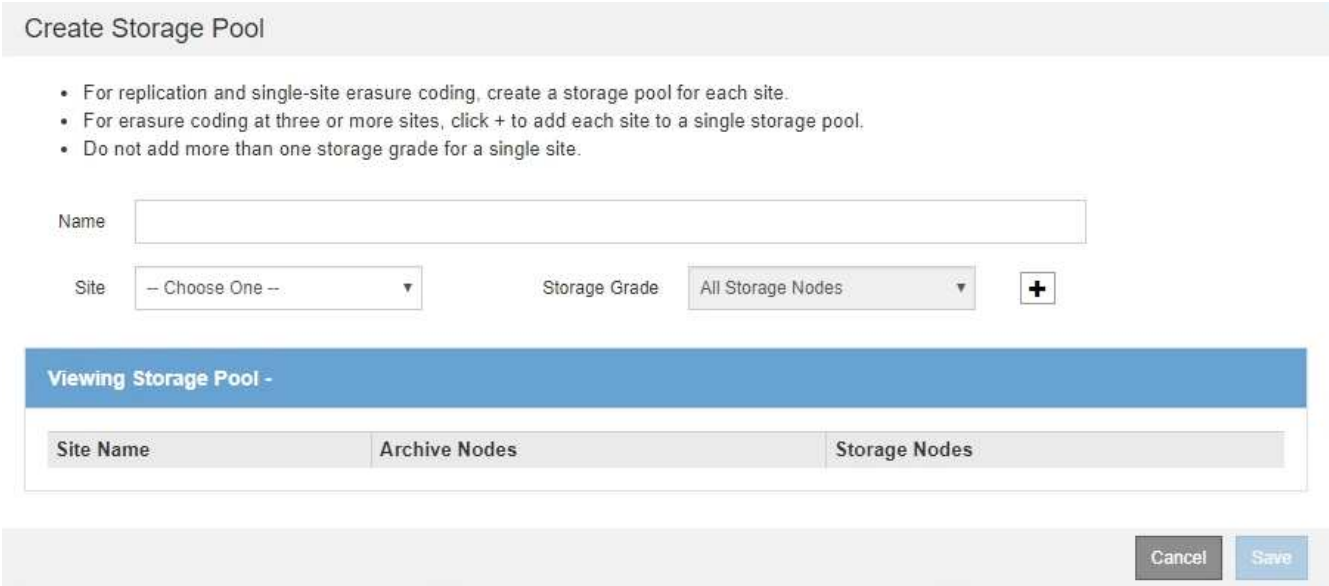


목록에는 시스템 기본 스토리지 풀, 시스템 기본 사이트, 모든 사이트, 기본 스토리지 등급인 모든 스토리지 노드를 사용하는 모든 스토리지 노드가 포함됩니다.

> 모든 스토리지 노드 스토리지 풀은 새 데이터 센터 사이트를 추가할 때마다 자동으로 업데이트되므로 ILM 규칙에서 이 스토리지 풀을 사용하는 것은 권장되지 않습니다.

2. 새 스토리지 풀을 생성하려면 * Create * 를 선택합니다.

   Create Storage Pool 대화상자가 나타납니다.



3. 스토리지 풀의 고유한 이름을 입력합니다.

   삭제 코딩 프로필 및 ILM 규칙을 구성할 때 쉽게 식별할 수 있는 이름을 사용하십시오.

4. Site * (사이트 *) 드롭다운 목록에서 이 스토리지 풀의 사이트를 선택합니다.

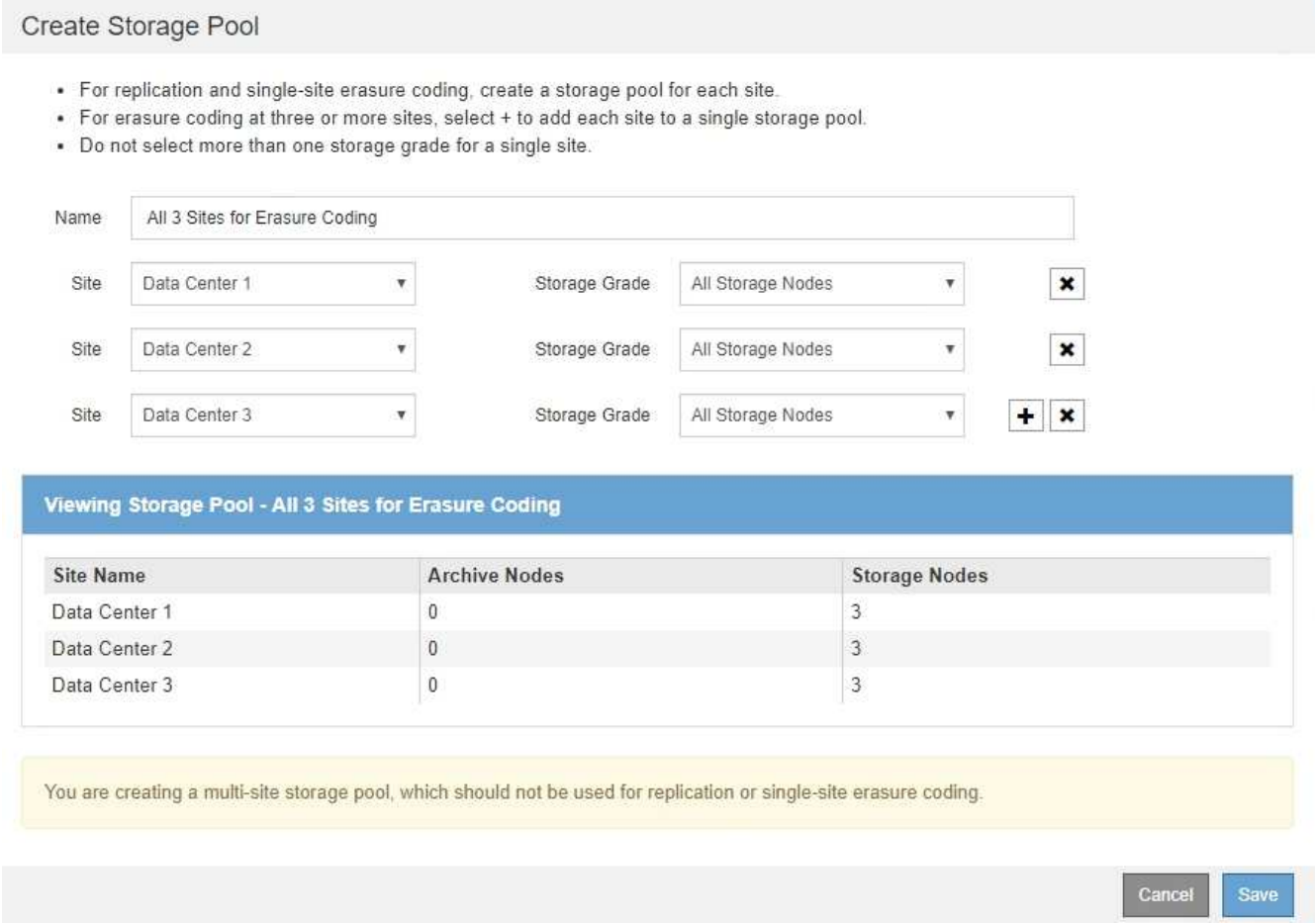
   사이트를 선택하면 테이블의 스토리지 노드 및 아카이브 노드 수가 자동으로 업데이트됩니다.

일반적으로 스토리지 풀에서 기본 모든 사이트 사이트를 사용하지 마십시오. 모든 사이트 스토리지 풀을 사용하는 ILM 규칙은 사용 가능한 모든 사이트에 개체를 배치하므로 개체 배치를 덜 제어할 수 있습니다. 또한 모든 사이트 스토리지 풀은 새 사이트의 스토리지 노드를 즉시 사용하며, 이는 사용자가 기대하는 동작이 아닐 수도 있습니다.

5. ILM 규칙이 이 스토리지 풀을 사용하는 경우 * 스토리지 등급 * 드롭다운 목록에서 사용할 스토리지 유형을 선택합니다.

   기본 모든 스토리지 노드 스토리지 등급에는 선택한 사이트의 모든 스토리지 노드가 포함됩니다. 기본 아카이브 노드 스토리지 평점에는 선택한 사이트의 모든 아카이브 노드가 포함됩니다. 그리드에 스토리지 노드에 대한 추가 스토리지 점수를 생성한 경우 해당 스토리지 등급이 드롭다운에 나열됩니다.

6. 다중 사이트 삭제 코딩 프로파일에서 스토리지 풀을 사용하려면 을 선택합니다 ✚ 각 사이트에 대한 항목을 스토리지 풀에 추가합니다.



> 중복 항목을 생성하거나 * 아카이브 노드 * 스토리지 등급과 스토리지 노드가 포함된 모든 스토리지 등급을 포함하는 스토리지 풀을 생성할 수 없습니다.
>
> 한 사이트에 대해 여러 항목을 추가하지만 저장소 평점이 다른 경우 경고가 표시됩니다.

항목을 제거하려면 를 선택합니다 ✖.

7. 선택 사항에 만족하면 * 저장 * 을 선택합니다.

   새 스토리지 풀이 목록에 추가됩니다.

스토리지 풀의 세부 정보를 확인하여 스토리지 풀이 사용되는 위치를 확인하고 포함된 노드와 스토리지 등급을 확인할 수 있습니다.

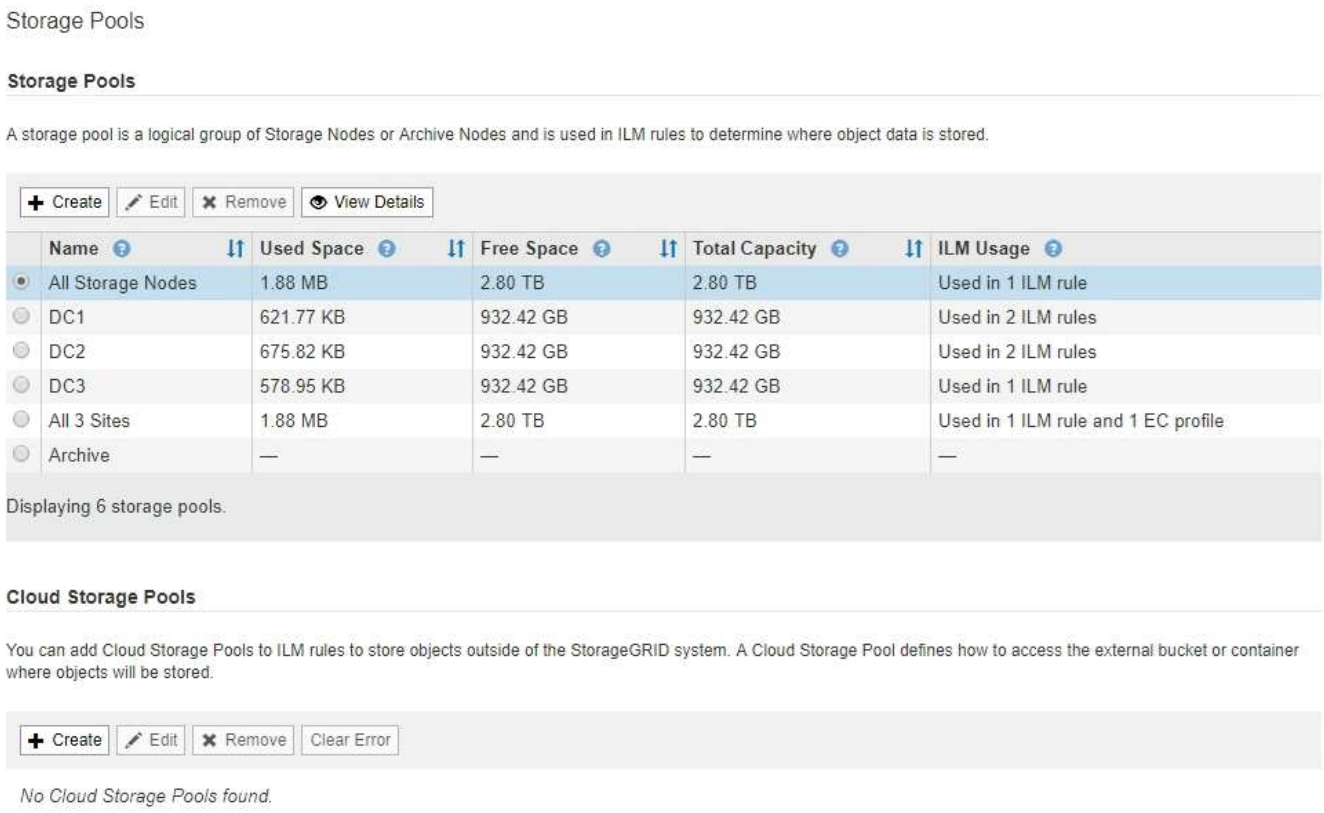
필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

단계

1. ILM * > * 스토리지 풀 * 을 선택합니다.

   스토리지 풀 페이지가 나타납니다. 이 페이지에는 정의된 모든 스토리지 풀이 나열됩니다.



   이 표에는 스토리지 노드가 포함된 각 스토리지 풀에 대한 다음 정보가 포함되어 있습니다.

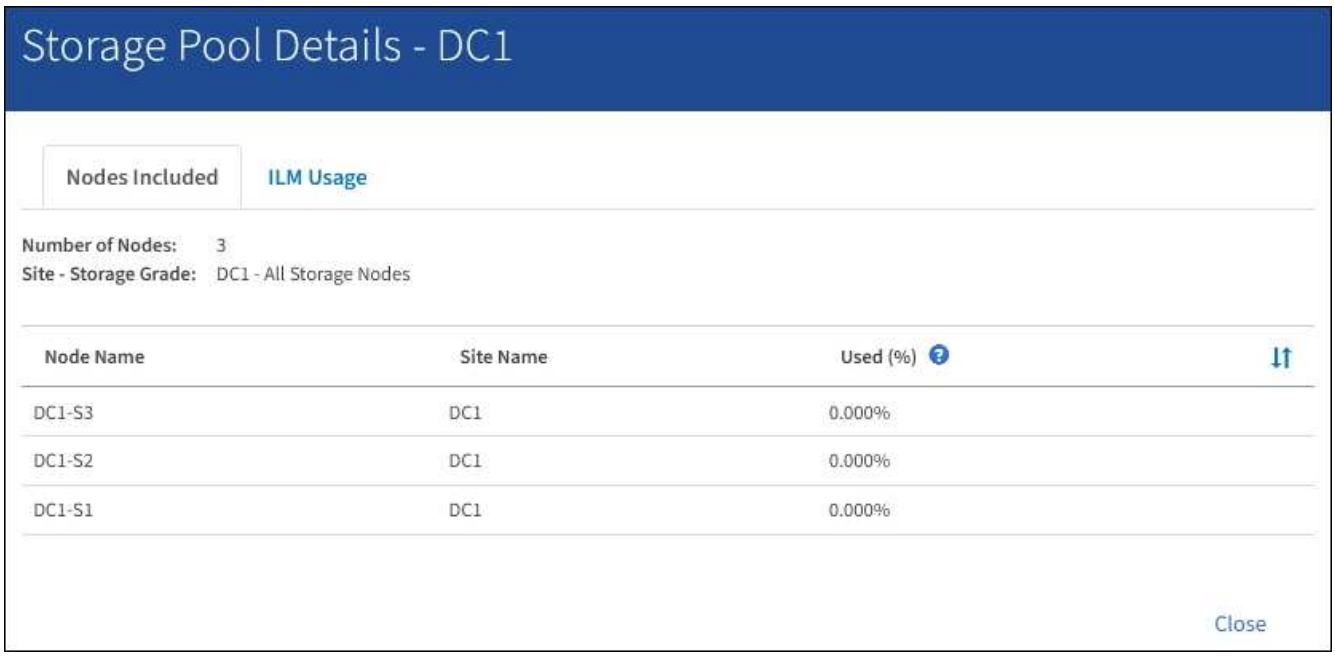
   - * 이름 *: 스토리지 풀의 고유한 표시 이름입니다.
   - * Used Space *: 스토리지 풀에 객체를 저장하는 데 현재 사용 중인 공간의 양입니다.
   - * 여유 공간 *: 스토리지 풀에 객체를 저장하는 데 사용할 수 있는 남아 있는 공간 크기입니다.
   - * 총 용량 *: 스토리지 풀의 크기로, 스토리지 풀의 모든 노드에 대해 오브젝트 데이터에 사용할 수 있는 총 공간의 양과 같습니다.
   - * ILM 사용법 *: 스토리지 풀이 현재 사용 중인 방법 스토리지 풀이 사용되지 않거나 하나 이상의 ILM 규칙, 삭제 코딩 프로필 또는 둘 다에서 사용될 수 있습니다.

> 사용 중인 스토리지 풀은 제거할 수 없습니다.

2. 특정 스토리지 풀에 대한 세부 정보를 보려면 해당 라디오 버튼을 선택하고 * View Details * 를 선택합니다.

   스토리지 풀 세부 정보 모달 이 나타납니다.

3. 포함된 * 노드 * 탭을 보고 스토리지 풀에 포함된 스토리지 노드 또는 아카이브 노드에 대해 알아보십시오.



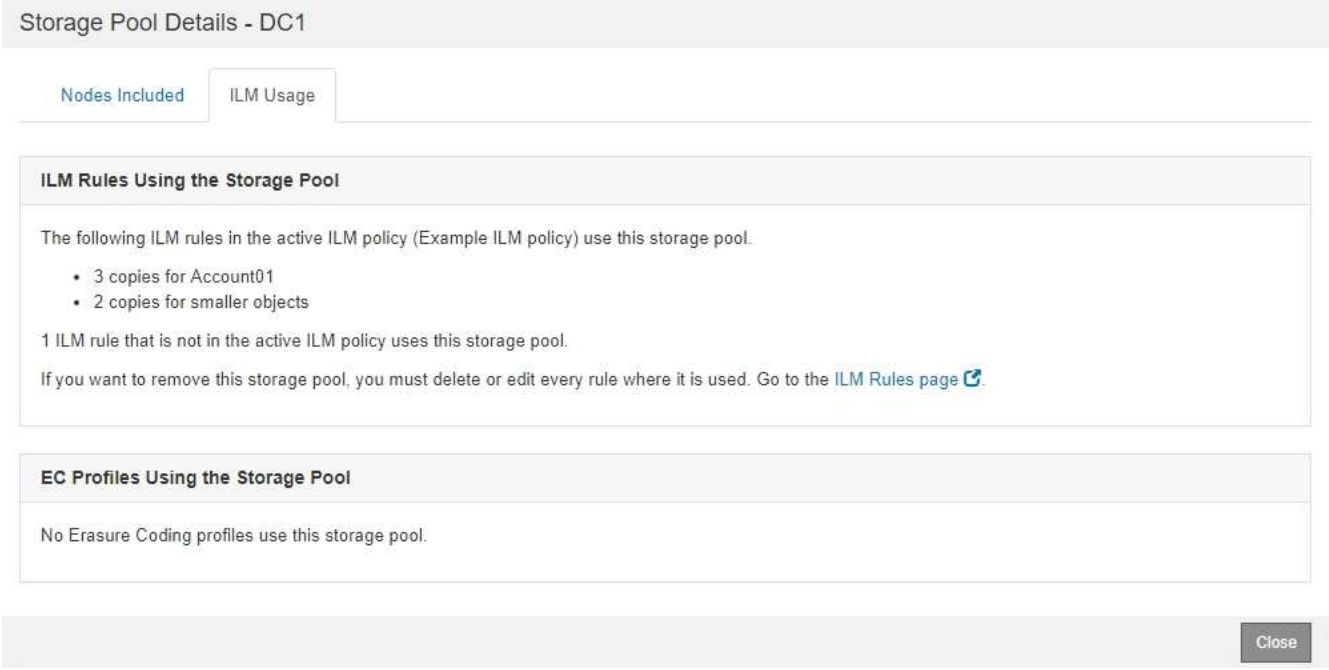
   표에는 각 노드에 대한 다음 정보가 나와 있습니다.

   - 노드 이름
   - 사이트 이름
   - 사용됨(%): 스토리지 노드의 경우 사용된 오브젝트 데이터에 대한 총 사용 가능 공간의 비율입니다. 이 값에는 개체 메타데이터가 포함되지 않습니다.

> 각 스토리지 노드에 대해 사용된 스토리지 객체 데이터 차트에도 동일한 사용된(%) 값이 표시됩니다(* nodes * > **Storage Node* * > * Storage * 선택).

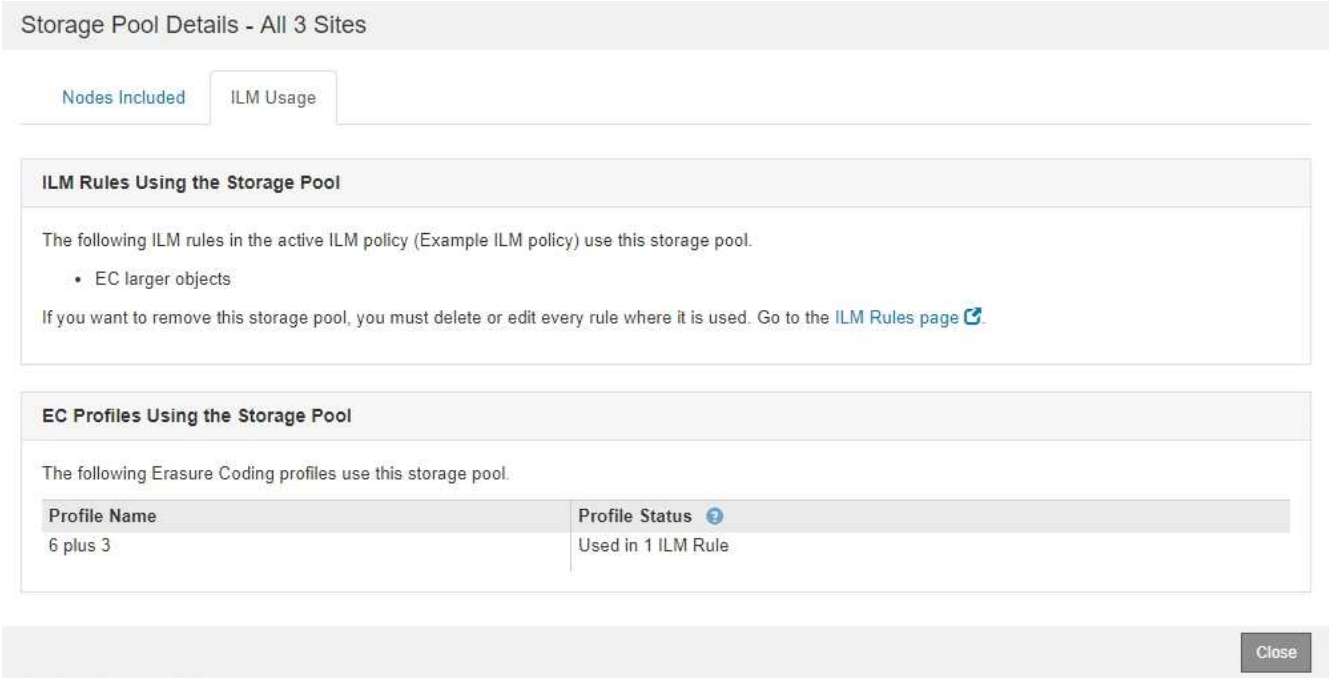
4. ILM Usage * 탭을 선택하여 스토리지 풀이 현재 ILM 규칙 또는 삭제 코딩 프로파일에서 사용되고 있는지 확인합니다.

   이 예에서는 DC1 스토리지 풀이 세 가지 ILM 규칙, 즉 활성 ILM 정책에 있는 두 가지 규칙과 활성 정책에 없는 한 가지 규칙에 사용됩니다.



ILM 규칙에 사용되는 스토리지 풀은 제거할 수 없습니다.

이 예에서는 삭제 코딩 프로파일에서 3개 사이트 스토리지 풀을 모두 사용합니다. 그러면 삭제 코딩 프로파일이 활성 ILM 정책의 한 ILM 규칙에 의해 사용됩니다.



삭제 코딩 프로파일에서 스토리지 풀을 사용하는 경우에는 스토리지 풀을 제거할 수 없습니다.

5. 필요한 경우 * ILM 규칙 페이지 * 로 이동하여 스토리지 풀을 사용하는 모든 규칙에 대해 알아보고 관리하십시오.

   ILM 규칙 작업에 대한 지침을 참조하십시오.

6. 스토리지 풀 세부 정보를 모두 확인했으면 * Close * 를 선택합니다.

관련 정보

ILM 규칙 및 ILM 정책 작업

스토리지 풀을 편집합니다

스토리지 풀을 편집하여 이름을 변경하거나 사이트 및 스토리지 등급을 업데이트할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- 스토리지 풀 생성에 대한 지침을 검토했습니다.
- 활성 ILM 정책의 규칙에 의해 사용되는 스토리지 풀을 편집하려는 경우 변경 사항이 개체 데이터 배치에 미치는 영향을 고려했습니다.

이 작업에 대해

활성 ILM 정책에 사용되는 스토리지 풀에 새 스토리지 등급을 추가하는 경우 새 스토리지 등급의 스토리지 노드가 자동으로 사용되지 않는다는 점에 유의하십시오. StorageGRID에서 새 스토리지 등급을 사용하도록 강제하려면 편집된 스토리지 풀을 저장한 후 새 ILM 정책을 활성화해야 합니다.

단계

1. ILM * > * 스토리지 풀 * 을 선택합니다.

   스토리지 풀 페이지가 나타납니다.

2. 편집할 스토리지 풀의 라디오 버튼을 선택합니다.

   모든 스토리지 노드 스토리지 풀은 편집할 수 없습니다.

3. 편집 * 을 선택합니다.
4. 필요에 따라 스토리지 풀 이름을 변경합니다.
5. 필요에 따라 다른 사이트 및 저장 등급을 선택합니다.

   > 스토리지 풀이 삭제 코딩 프로필에 사용되고 변경 시 삭제 코딩 체계가 유효하지 않게 되는 경우 사이트 또는 스토리지 등급을 변경할 수 없습니다. 예를 들어, 삭제 코딩 프로필에 사용된 스토리지 풀에 현재 사이트가 하나뿐인 스토리지 평점이 포함되어 있는 경우 삭제 코딩 체계가 잘못될 수 있으므로 두 개의 사이트에 스토리지 평점을 사용할 수 없습니다.

6. 저장 * 을 선택합니다.

작업을 마친 후

활성 ILM 정책에 사용된 스토리지 풀에 새 스토리지 등급을 추가한 경우 새 ILM 정책을 활성화하여 StorageGRID이 새 스토리지 등급을 사용하도록 강제합니다. 예를 들어, 기존 ILM 정책을 클론 복제한 다음 클론을 활성화합니다.

스토리지 풀을 제거합니다

사용되지 않는 스토리지 풀을 제거할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

단계

1. ILM * > * 스토리지 풀 * 을 선택합니다.

   스토리지 풀 페이지가 나타납니다.

2. 표에서 ILM 사용 열을 확인하여 스토리지 풀을 제거할 수 있는지 확인합니다.

   스토리지 풀이 ILM 규칙 또는 삭제 코딩 프로파일에서 사용 중인 경우에는 스토리지 풀을 제거할 수 없습니다. 필요한 경우 * View Details * > * ILM Usage * 를 선택하여 스토리지 풀이 사용되는 위치를 확인합니다.

3. 제거하려는 스토리지 풀을 사용하지 않는 경우 라디오 버튼을 선택합니다.
4. 제거 * 를 선택합니다.
5. OK * 를 선택합니다.

클라우드 스토리지 풀 사용

클라우드 스토리지 풀은 무엇입니까

클라우드 스토리지 풀을 사용하면 ILM을 사용하여 StorageGRID 시스템 외부로 오브젝트 데이터를 이동할 수 있습니다. 예를 들어, 자주 액세스하지 않는 오브젝트를 Amazon S3 Glacier, S3 Glacier Deep Archive 또는 Microsoft Azure Blob 스토리지의 아카이브 액세스 계층과 같은 저비용 클라우드 스토리지로 이동할 수 있습니다. 또는 StorageGRID 오브젝트의 클라우드 백업을 유지하여 재해 복구를 강화하는 경우도 있습니다.

ILM 관점에서 Cloud Storage Pool은 스토리지 풀과 유사합니다. 두 위치 중 하나에 오브젝트를 저장하려면 ILM 규칙에 대한 배치 지침을 생성할 때 풀을 선택합니다. 그러나 스토리지 풀은 StorageGRID 시스템 내의 스토리지 노드 또는 아카이브 노드로 구성되지만, 클라우드 스토리지 풀은 외부 버킷(S3) 또는 컨테이너(Azure Blob 스토리지)로 구성됩니다.

다음 표에서는 스토리지 풀을 클라우드 스토리지 풀과 비교하여 개괄적인 유사점과 차이점을 보여 줍니다.

	스토리지 풀	클라우드 스토리지 풀
어떻게 만들어집니까?	Grid Manager에서 * ILM * > * 스토리지 풀 * 옵션 사용 스토리지 풀을 생성하려면 먼저 스토리지 등급을 설정해야 합니다.	Grid Manager에서 * ILM * > * 스토리지 풀 * 옵션 사용 클라우드 스토리지 풀을 생성하려면 먼저 외부 버킷 또는 컨테이너를 설정해야 합니다.
풀을 몇 개나 생성할 수 있습니까?	무제한.	최대 10개까지 가능합니다.

	스토리지 풀	클라우드 스토리지 풀
오브젝트는 어디에 저장됩니까?	StorageGRID 내의 하나 이상의 스토리지 노드 또는 아카이브 노드에서	StorageGRID 시스템 외부에 있는 Amazon S3 버킷 또는 Azure Blob 스토리지 컨테이너 Cloud Storage Pool이 Amazon S3 버킷인 경우: • 원하는 경우 버킷 라이프사이클을 구성하여 Amazon S3 Glacier 또는 S3 Glacier Deep Archive와 같은 저비용, 장기 스토리지로 오브젝트를 전환할 수 있습니다. 외부 스토리지 시스템은 Glacier 저장소 클래스 및 S3 POST 오브젝트 복원 API를 지원해야 합니다. • AWS C2S(Commercial Cloud Services)와 함께 사용할 클라우드 스토리지 풀을 생성할 수 있습니다. C2S는 AWS Secret Region을 지원합니다. 클라우드 스토리지 풀이 Azure Blob 스토리지 컨테이너인 경우 StorageGRID는 개체를 아카이브 계층으로 전환합니다. • 참고: * 일반적으로 클라우드 스토리지 풀에 사용되는 컨테이너에 대한 Azure Blob 스토리지 라이프사이클 관리를 구성하지 않습니다. Cloud Storage Pool의 객체에 대한 사후 오브젝트 복원 작업은 구성된 수명주기의 영향을 받을 수 있습니다.
개체 배치를 제어하는 것은 무엇입니까?	활성 ILM 정책의 ILM 규칙	활성 ILM 정책의 ILM 규칙
어떤 데이터 보호 방법이 사용됩니까?	복제 또는 삭제 코딩.	복제:
각 오브젝트의 복사본을 몇 개 허용할 수 있습니까?	다중.	클라우드 스토리지 풀에 복사본 1개, StorageGRID에 복사본 1개 이상(선택 사항) • 참고: * 한 번에 둘 이상의 클라우드 스토리지 풀에 개체를 저장할 수 없습니다.
이점은 무엇입니까?	개체는 언제든지 신속하게 액세스할 수 있습니다.	저렴한 스토리지:

클라우드 스토리지 풀을 구현하기 전에 각 유형의 클라우드 스토리지 풀에 저장된 개체의 라이프사이클을 검토하십시오.

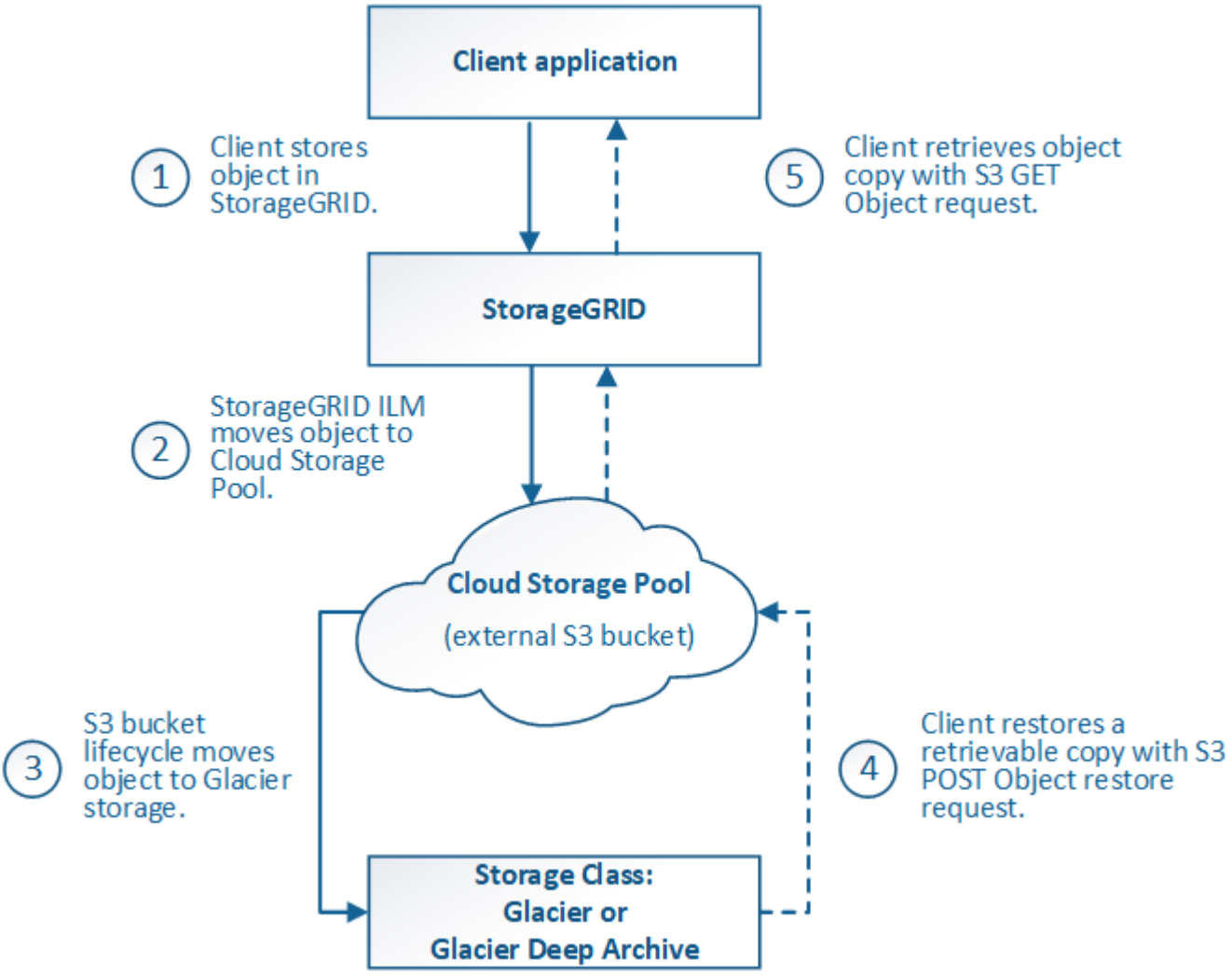
- S3: 클라우드 스토리지 풀 오브젝트의 수명 주기
- Azure: Cloud Storage Pool 개체의 수명 주기

S3: 클라우드 스토리지 풀 오브젝트의 수명 주기

이 그림에서는 S3 클라우드 스토리지 풀에 저장된 개체의 라이프사이클 단계를 보여 줍니다.

> 그림과 설명에서는 "빙하"는 빙하 저장소 클래스와 Glacier Deep Archive 저장소 클래스를 모두 지칭합니다. 단, 빙하 딥 아카이브 저장소 클래스는 빠른 복원 계층을 지원하지 않습니다. 대량 또는 표준 검색만 지원됩니다.

> Google Cloud Platform(GCP)은 POST 복원 작업 없이 장기 저장소에서 개체 검색을 지원합니다.



1. * StorageGRID * 에 저장된 개체

수명 주기를 시작하기 위해 클라이언트 응용 프로그램은 StorageGRID에 개체를 저장합니다.

2. * 오브젝트가 S3 클라우드 스토리지 풀로 이동됨 *
   - 오브젝트가 S3 클라우드 스토리지 풀을 사용하여 배치 위치로 사용되는 ILM 규칙에 따라 대응되면 StorageGRID은 오브젝트를 클라우드 스토리지 풀에 지정된 외부 S3 버킷으로 이동합니다.
   - 오브젝트가 S3 클라우드 스토리지 풀로 이동된 경우 오브젝트 가 Glacier 스토리지로 이전되지 않는 한 클라이언트 애플리케이션이 StorageGRID에서 S3 오브젝트 가져오기 요청을 사용하여 오브젝트를 검색할 수 있습니다.
3. * 객체가 Glacier로 전환됨(검색할 수 없는 상태) *
   - 필요에 따라 오브젝트를 Glacier 스토리지로 전환할 수 있습니다. 예를 들어, 외부 S3 버킷은 라이프사이클 구성을 사용하여 오브젝트를 Glacier 스토리지로 즉시 또는 며칠 후 전환할 수 있습니다.

     오브젝트를 이전하려면 외부 S3 버킷에 대한 라이프사이클 구성을 생성해야 하며, Glacier 스토리지 클래스를 구현하고 S3 POST 오브젝트 복원 API를 지원하는 스토리지 솔루션을 사용해야 합니다.

     Swift 클라이언트가 인제스트한 객체에는 Cloud Storage Pool을 사용하지 마십시오. Swift는 POST 오브젝트 복원 요청을 지원하지 않으므로 StorageGRID는 S3 Glacier 스토리지로 전환된 Swift 오브젝트를 검색할 수 없습니다. 이러한 객체를 검색하기 위한 Swift GET 오브젝트 요청을 발급할 수 없습니다(403 사용 금지).

   - 전환 중에 클라이언트 애플리케이션은 S3 헤드 오브젝트 요청을 사용하여 오브젝트의 상태를 모니터링할 수 있습니다.
4. * Glacier 스토리지에서 개체 복원 *

   오브젝트가 Glacier 스토리지로 전환된 경우 클라이언트 애플리케이션이 S3 POST 오브젝트 복원 요청을 발행하여 검색 가능한 복사본을 S3 클라우드 스토리지 풀로 복원할 수 있습니다. 요청은 클라우드 스토리지 풀 및 복구 작업에 사용할 데이터 액세스 계층(빠른 참조, 표준 또는 대량)에서 복제본을 사용할 수 있는 기간을 지정합니다. 복구할 수 있는 복사본의 만료 날짜에 도달하면 복사본은 자동으로 복구할 수 없는 상태로 돌아갑니다.

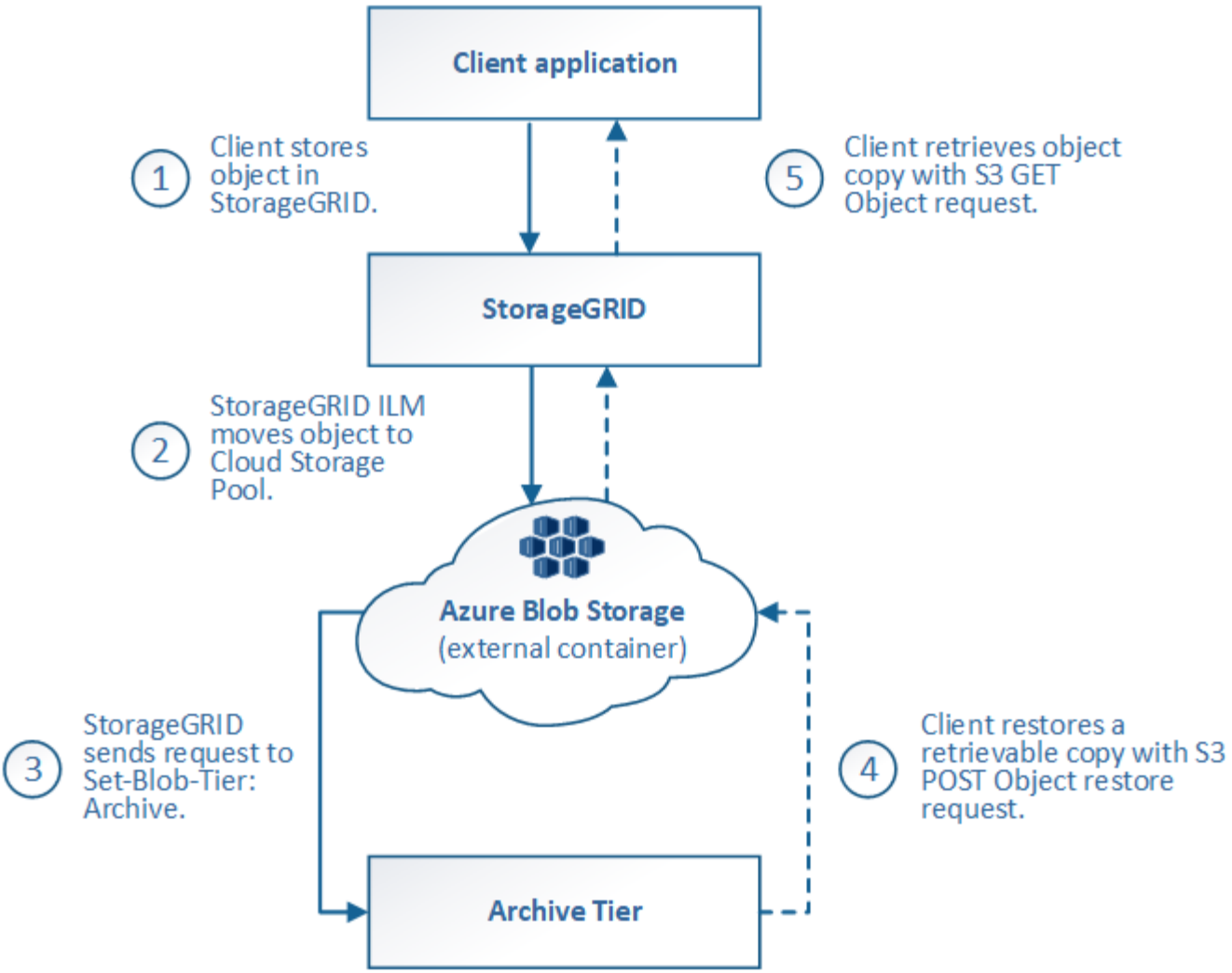
   StorageGRID 내의 스토리지 노드에도 하나 이상의 개체 복사본이 있는 경우 POST 개체 복원 요청을 실행하여 Glacier에서 개체를 복원할 필요가 없습니다. 대신 Get Object 요청을 사용하여 로컬 복사본을 직접 검색할 수 있습니다.

5. * 객체 검색됨 *

   개체가 복원되면 클라이언트 응용 프로그램에서 개체 가져오기 요청을 발행하여 복원된 개체를 검색할 수 있습니다.

Azure: Cloud Storage Pool 개체의 수명 주기

이 그림에서는 Azure Cloud Storage Pool에 저장된 개체의 라이프사이클 단계를 보여 줍니다.



1. * StorageGRID * 에 저장된 개체

   수명 주기를 시작하기 위해 클라이언트 응용 프로그램은 StorageGRID에 개체를 저장합니다.

2. * Azure 클라우드 스토리지 풀로 이동된 객체 *

   Azure Cloud Storage Pool을 위치 위치로 사용하는 ILM 규칙에 따라 오브젝트가 일치하는 경우 StorageGRID은 해당 오브젝트를 클라우드 스토리지 풀에 지정된 외부 Azure Blob 스토리지 컨테이너로 이동합니다

   > Swift 클라이언트가 인제스트한 객체에는 Cloud Storage Pool을 사용하지 마십시오. Swift는 POST 오브젝트 복원 요청을 지원하지 않으므로 StorageGRID는 Azure Blob 스토리지 아카이브 계층으로 전환된 Swift 오브젝트를 검색할 수 없습니다. 이러한 객체를 검색하기 위한 Swift GET 오브젝트 요청을 발급할 수 없습니다(403 사용 금지).

3. * 객체가 아카이브 계층으로 전환됨(검색할 수 없는 상태) *

   오브젝트를 Azure 클라우드 스토리지 풀로 이동한 직후 StorageGRID은 오브젝트를 Azure Blob 스토리지 아카이브 계층으로 자동으로 전환합니다.

4. * 아카이브 계층에서 객체 복원 *

   객체가 아카이브 계층으로 전환된 경우 클라이언트 애플리케이션은 S3 POST 오브젝트 복원 요청을 발행하여 검색

가능한 복제본을 Azure Cloud Storage Pool에 복구할 수 있습니다.

StorageGRID에서 POST 개체 복원을 수신하면 개체를 Azure Blob 저장소 Cool 계층으로 일시적으로 전환합니다. POST 개체 복원 요청의 만료 날짜에 도달하면 StorageGRID가 개체를 아카이브 계층으로 다시 전환합니다.

> StorageGRID 내의 스토리지 노드에도 하나 이상의 개체 복사본이 있는 경우 POST 개체 복원 요청을 실행하여 아카이브 액세스 계층에서 개체를 복원할 필요가 없습니다. 대신 Get Object 요청을 사용하여 로컬 복사본을 직접 검색할 수 있습니다.

5. * 객체 검색됨 *

   Azure Cloud Storage Pool에 오브젝트가 복원되면 클라이언트 애플리케이션이 객체 가져오기 요청을 발행하여 복원된 객체를 검색할 수 있습니다.

관련 정보

S3을 사용합니다

클라우드 스토리지 풀을 사용하는 경우

Cloud Storage Pool은 다양한 사용 사례에서 상당한 이점을 제공할 수 있습니다.

외부 위치에 **StorageGRID** 데이터 백업

클라우드 스토리지 풀을 사용하여 StorageGRID 객체를 외부 위치에 백업할 수 있습니다.

StorageGRID의 복사본에 액세스할 수 없는 경우 클라우드 스토리지 풀의 오브젝트 데이터를 사용하여 클라이언트 요청을 처리할 수 있습니다. 그러나 클라우드 스토리지 풀의 백업 오브젝트 복사본에 액세스하려면 S3 POST 오브젝트 복원 요청을 실행해야 할 수도 있습니다.

스토리지 볼륨 또는 스토리지 노드 장애로 인해 클라우드 스토리지 풀의 오브젝트 데이터를 사용하여 StorageGRID에서 손실된 데이터를 복구할 수도 있습니다. 개체의 나머지 복사본만 클라우드 스토리지 풀에 있는 경우 StorageGRID는 개체를 일시적으로 복원하고 복구된 스토리지 노드에 새 복사본을 생성합니다.

백업 솔루션을 구축하려면 다음을 따르십시오.

1. 단일 Cloud Storage Pool을 생성합니다.
2. 스토리지 노드에 오브젝트 복사본(복제된 복사본 또는 삭제 코딩 복사본)을 동시에 저장하고 클라우드 스토리지 풀에 단일 오브젝트 복사본을 저장하는 ILM 규칙을 구성합니다.
3. ILM 정책에 규칙을 추가합니다. 그런 다음 정책을 시뮬레이션하고 활성화합니다.

StorageGRID에서 외부 위치로 데이터 계층화

클라우드 스토리지 풀을 사용하여 StorageGRID 시스템 외부에 개체를 저장할 수 있습니다. 예를 들어, 보존해야 하는 오브젝트가 많은 경우 해당 오브젝트에 거의 액세스하지 않을 것으로 예상한다고 가정합니다. 클라우드 스토리지 풀을 사용하여 오브젝트를 저비용 스토리지로 계층화하거나 StorageGRID에서 공간을 확보할 수 있습니다.

계층화 솔루션을 구축하려면 다음을 따르십시오.

1. 단일 Cloud Storage Pool을 생성합니다.

2. 거의 사용되지 않는 오브젝트를 스토리지 노드에서 클라우드 스토리지 풀로 이동하는 ILM 규칙을 구성합니다.
3. ILM 정책에 규칙을 추가합니다. 그런 다음 정책을 시뮬레이션하고 활성화합니다.

여러 클라우드 엔드포인트 유지 관리

오브젝트 데이터를 두 개 이상의 클라우드에 계층화하거나 백업하려는 경우 여러 클라우드 스토리지 풀을 구성할 수 있습니다. ILM 규칙의 필터를 사용하여 각 클라우드 스토리지 풀에 저장할 오브젝트를 지정할 수 있습니다. 예를 들어, 일부 테넌트 또는 버킷의 오브젝트를 Amazon S3 빙하에 저장하고 다른 테넌트 또는 버킷의 오브젝트를 Azure Blob 스토리지에 저장할 수 있습니다. 또는 Amazon S3 Glacier와 Azure Blob 스토리지 간에 데이터를 이동할 수 있습니다. 여러 클라우드 스토리지 풀을 사용할 때는 한 번에 하나의 클라우드 스토리지 풀에만 오브젝트를 저장할 수 있습니다.

여러 클라우드 엔드포인트를 구현하려면:

1. 최대 10개의 클라우드 스토리지 풀을 생성합니다.
2. 각 Cloud Storage Pool에 적절한 시간에 적절한 오브젝트 데이터를 저장하도록 ILM 규칙을 구성합니다. 예를 들어, 버킷 A의 오브젝트를 클라우드 스토리지 풀 A에 저장하고 버킷 B의 오브젝트를 클라우드 스토리지 풀 B에 저장합니다 또는, 객체를 Cloud Storage Pool A에 일정 시간 저장한 다음 Cloud Storage Pool B로 이동합니다
3. ILM 정책에 규칙을 추가합니다. 그런 다음 정책을 시뮬레이션하고 활성화합니다.

클라우드 스토리지 풀에 대한 고려 사항

클라우드 스토리지 풀을 사용하여 StorageGRID 시스템 외부로 오브젝트를 이동하려는 경우 클라우드 스토리지 풀을 구성 및 사용하기 위한 고려 사항을 검토해야 합니다.

일반 고려 사항

- 일반적으로 Amazon S3 Glacier 또는 Azure Blob 스토리지와 같은 클라우드 아카이브 스토리지는 오브젝트 데이터를 저장할 수 있는 저렴한 장소입니다. 그러나 클라우드 아카이브 스토리지에서 데이터를 검색하는 데 드는 비용은 비교적 높은 편입니다. 전체 비용을 가장 낮게 달성하려면 Cloud Storage Pool에서 개체에 액세스하는 시기와 빈도를 고려해야 합니다. 클라우드 스토리지 풀은 자주 액세스하지 않는 콘텐츠에만 사용하는 것이 좋습니다.
- Swift 클라이언트가 인제스트한 객체에는 Cloud Storage Pool을 사용하지 마십시오. Swift는 POST 오브젝트 복원 요청을 지원하지 않으므로 StorageGRID는 S3 Glacier 스토리지 또는 Azure Blob 스토리지 아카이브 계층으로 전환된 Swift 오브젝트를 검색할 수 없습니다. 이러한 객체를 검색하기 위한 Swift GET 오브젝트 요청을 발급할 수 없습니다(403 사용 금지).
- FabricPool에서 클라우드 스토리지 풀 타겟의 객체를 검색하는 지연 시간이 추가되었기 때문에 클라우드 스토리지 풀을 사용할 수 없습니다.

Cloud Storage Pool을 생성하는 데 필요한 정보입니다

Cloud Storage Pool을 생성하려면 먼저 외부 S3 버킷 또는 Cloud Storage Pool에 사용할 외부 Azure Blob 스토리지 컨테이너를 생성해야 합니다. 그런 다음 StorageGRID에서 클라우드 스토리지 풀을 생성할 때 다음 정보를 지정해야 합니다.

- 공급자 유형: Amazon S3 또는 Azure Blob 스토리지
- Amazon S3를 선택한 경우 클라우드 스토리지 풀이 AWS Secret Region(* CAP(C2S Access Portal) *)과 함께 사용할 것인지 여부를 지정합니다.
- 버킷 또는 컨테이너의 정확한 이름입니다.

- 버킷 또는 컨테이너에 액세스하는 데 필요한 서비스 엔드포인트입니다.
- 버킷 또는 컨테이너에 액세스하는 데 필요한 인증:
  - * S3 *: 선택적으로 액세스 키 ID 및 비밀 액세스 키.
  - * C2S *: CAP 서버에서 임시 자격 증명을 얻기 위한 전체 URL, 서버 CA 인증서, 클라이언트 인증서, 클라이언트 인증서의 개인 키, 개인 키가 암호화된 경우 암호 해독을 위한 암호 문구입니다.
  - * Azure Blob 저장소 *: 계정 이름 및 계정 키입니다. 이러한 자격 증명에는 컨테이너에 대한 모든 권한이 있어야 합니다.
- 필요에 따라 버킷이나 컨테이너에 대한 TLS 연결을 확인하기 위한 사용자 지정 CA 인증서입니다.

클라우드 스토리지 풀에 사용되는 포트에 대한 고려 사항

ILM 규칙이 지정된 클라우드 스토리지 풀 간에 오브젝트를 이동할 수 있도록 하려면 시스템의 스토리지 노드가 포함된 네트워크를 구성해야 합니다. 다음 포트가 Cloud Storage Pool과 통신할 수 있는지 확인해야 합니다.

기본적으로 Cloud Storage Pool은 다음 포트를 사용합니다.

- * 80 *: http로 시작하는 끝점 URI입니다
- * 443 *: https로 시작하는 끝점 URI의 경우

클라우드 스토리지 풀을 생성하거나 편집할 때 다른 포트를 지정할 수 있습니다.

투명하지 않은 프록시 서버를 사용하는 경우에도 필요합니다 스토리지 프록시를 구성합니다 인터넷의 끝점과 같은 외부 끝점으로 메시지를 보낼 수 있도록 합니다.

비용에 대한 고려 사항

클라우드 스토리지 풀을 사용하여 클라우드의 스토리지에 액세스하려면 클라우드에 대한 네트워크 연결이 필요합니다. 클라우드 스토리지 풀을 사용하여 StorageGRID과 클라우드 간에 이동할 것으로 예상되는 데이터 양에 따라 클라우드 액세스에 사용할 네트워크 인프라 비용을 고려하고 적절하게 프로비저닝해야 합니다.

StorageGRID가 외부 클라우드 스토리지 풀 엔드포인트에 연결되면 다양한 요청을 보내 연결을 모니터링하고 필요한 작업을 수행할 수 있도록 합니다. 이러한 요청에 추가 비용이 발생할 수 있지만, Cloud Storage Pool 모니터링 비용은 S3 또는 Azure에서 오브젝트를 저장하는 데 드는 전체 비용의 극히 일부에 불과합니다.

외부 클라우드 스토리지 풀 엔드포인트에서 StorageGRID로 오브젝트를 다시 이동해야 하는 경우 더 많은 비용이 발생할 수 있습니다. 다음과 같은 경우 오브젝트를 StorageGRID로 다시 이동할 수 있습니다.

- 개체의 유일한 복사본은 클라우드 스토리지 풀에 있으며 대신 StorageGRID에 개체를 저장하기로 결정합니다. 이 경우 ILM 규칙 및 정책을 다시 구성하면 됩니다. ILM 평가가 발생하면 StorageGRID은 여러 요청을 발급하여 클라우드 스토리지 풀에서 오브젝트를 검색합니다. 그런 다음 StorageGRID는 복제된 복사본 또는 삭제 코딩 복사본을 로컬에 지정된 수만큼 생성합니다. 오브젝트를 StorageGRID으로 다시 이동한 후 클라우드 스토리지 풀의 복사본이 삭제됩니다.
- 스토리지 노드 장애로 인해 객체가 손실됩니다. 개체의 나머지 복사본만 클라우드 스토리지 풀에 있는 경우 StorageGRID는 개체를 일시적으로 복원하고 복구된 스토리지 노드에 새 복사본을 생성합니다.

> 오브젝트를 클라우드 스토리지 풀에서 StorageGRID로 다시 이동할 경우 StorageGRID은 각 오브젝트의 클라우드 스토리지 풀 엔드포인트에 여러 요청을 발급합니다. 많은 수의 오브젝트를 이동하기 전에 기술 지원 부서에 문의하여 기간 및 관련 비용을 추정하십시오.

S3: 클라우드 스토리지 풀 버킷에 대한 권한이 필요합니다

클라우드 스토리지 풀에 사용되는 외부 S3 버킷의 버킷 정책은 StorageGRID에 오브젝트를 버킷으로 이동, 오브젝트 상태 가져오기, 필요한 경우 Glacier 스토리지에서 오브젝트 복원 등의 권한을 부여해야 합니다. StorageGRID는 버킷에 대한 전체 제어 액세스 권한('3: *')을 갖는 것이 바람직하지만, 이것이 가능하지 않을 경우 버킷 정책은 StorageGRID에 다음과 같은 S3 권한을 부여해야 합니다.

- '3:AbortMultipartUpload'를 선택합니다
- '3: DeleteObject'
- '3:GetObject'
- '3목록 버킷'
- '3: ListBuckketMultipartUploads'
- '3:ListMultipartUploadParts'를 선택합니다
- '3: PutObject'
- '3:RestoreObject'입니다

S3: 외부 버킷의 수명 주기에 대한 고려 사항

StorageGRID와 클라우드 스토리지 풀에 지정된 외부 S3 버킷 간에 오브젝트를 이동하는 것은 ILM 규칙 및 StorageGRID의 활성 ILM 정책에 의해 제어됩니다. 반면, Cloud Storage Pool에 지정된 외부 S3 버킷에서 Amazon S3 Glacier 또는 S3 Glacier Deep Archive(또는 Glacier 스토리지 클래스를 구현하는 스토리지 솔루션)로 오브젝트 전환은 해당 버킷의 라이프사이클 구성에 의해 제어됩니다.

클라우드 스토리지 풀에서 오브젝트를 전환하려는 경우 외부 S3 버킷에 적절한 라이프사이클 구성을 생성해야 하며, Glacier 스토리지 클래스를 구현하고 S3 POST 오브젝트 복원 API를 지원하는 스토리지 솔루션을 사용해야 합니다.

예를 들어, StorageGRID에서 클라우드 스토리지 풀로 이동된 모든 오브젝트를 즉시 Amazon S3 Glacier 스토리지로 전환하려고 합니다. 다음과 같이 단일 작업(* Transition*)을 지정하는 외부 S3 버킷에 라이프사이클 구성을 작성합니다.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

이 규칙은 모든 버킷 오브젝트를 생성 당일 Amazon S3 Glacier로 전환합니다(즉, StorageGRID에서 클라우드 스토리지 풀로 이동 날짜).

> 외부 버킷의 수명 주기를 구성할 때 * Expiration * (만료 *) 작업을 사용하여 개체 만료 시기를 정의하지 마십시오. 만료 작업으로 인해 외부 스토리지 시스템이 만료된 객체를 삭제합니다. 나중에 StorageGRID에서 만료된 개체에 액세스하려고 하면 삭제된 개체를 찾을 수 없습니다.

Cloud Storage Pool의 오브젝트를 Amazon S3 Glacier가 아닌 S3 Glacier Deep Archive로 이전하려면 버킷 라이프사이클에서 "<StorageClass>Deep_archive</StorageClass>"를 지정합니다. 그러나 "빠른" 계층을 사용하여 S3 Glacier Deep Archive에서 개체를 복원할 수는 없습니다.

Azure: 액세스 계층에 대한 고려 사항

Azure 저장소 계정을 구성할 때 기본 액세스 계층을 핫 또는 쿨 으로 설정할 수 있습니다. 클라우드 스토리지 풀에서 사용할 스토리지 계정을 생성할 때는 핫 계층을 기본 계층으로 사용해야 합니다. StorageGRID는 개체를 클라우드 스토리지 풀로 이동할 때 즉시 계층을 보관으로 설정하지만 기본 설정 핫 을 사용하면 최소 30일 전에 쿨 계층에서 제거된 개체에 대한 조기 삭제 요금이 부과되지 않습니다.

Azure: 수명 주기 관리가 지원되지 않습니다

Cloud Storage Pool과 함께 사용되는 컨테이너에 Azure Blob Storage 라이프사이클 관리를 사용하지 마십시오. 라이프사이클 작업은 Cloud Storage Pool 작업을 방해할 수 있습니다.

관련 정보

- 클라우드 스토리지 풀을 생성합니다
- S3: 클라우드 스토리지 풀에 대한 인증 세부 정보를 지정합니다
- C2S S3: 클라우드 스토리지 풀에 대한 인증 세부 정보를 지정합니다
- Azure: 클라우드 스토리지 풀에 대한 인증 세부 정보를 지정합니다

클라우드 스토리지 풀 및 **CloudMirror** 복제 비교

클라우드 스토리지 풀을 사용할 때는 클라우드 스토리지 풀과 StorageGRID CloudMirror 복제 서비스의 유사점과 차이점을 이해하는 것이 좋습니다.

	클라우드 스토리지 풀	**CloudMirror** 복제 서비스
주요 목적은 무엇입니까?	클라우드 스토리지 풀은 아카이브 타겟 역할을 수행합니다. Cloud Storage Pool의 오브젝트 복사본은 개체의 유일한 복사본이거나 추가 복사본일 수 있습니다. 즉, 사내에 두 개의 복사본을 유지하는 대신 StorageGRID 내에 하나의 복사본만 유지하고 복사본을 클라우드 스토리지 풀에 보낼 수 있습니다.	CloudMirror 복제 서비스를 사용하면 테넌트가 StorageGRID(소스)의 버킷에서 외부 S3 버킷(대상)으로 오브젝트를 자동으로 복제할 수 있습니다. CloudMirror 복제는 독립 S3 인프라에서 개체의 독립적인 복사본을 생성합니다.
어떻게 설정합니까?	클라우드 스토리지 풀은 Grid Manager 또는 Grid Management API를 사용하여 스토리지 풀과 동일한 방식으로 정의됩니다. ILM 규칙에서 Cloud Storage Pool을 배치 위치로 선택할 수 있습니다. 스토리지 풀은 스토리지 노드 그룹으로 구성되지만, 클라우드 스토리지 풀은 원격 S3 또는 Azure 엔드포인트(IP 주소, 자격 증명 등)를 사용하여 정의됩니다.	테넌트 사용자입니다 CloudMirror 복제 구성 테넌트 관리자 또는 S3 API를 사용하여 CloudMirror 엔드포인트(IP 주소, 자격 증명 등)를 정의합니다. CloudMirror 엔드포인트를 설정한 후 해당 테넌트 계정이 소유한 모든 버킷이 CloudMirror 엔드포인트를 가리키도록 구성할 수 있습니다.

	클라우드 스토리지 풀	**CloudMirror** 복제 서비스
누가 설정해야 합니까?	일반적으로 그리드 관리자	일반적으로 테넌트 사용자입니다
대상은 무엇입니까?	• 호환 가능한 S3 인프라(Amazon S3 포함) • Azure Blob 아카이브 계층입니다	• 호환 가능한 S3 인프라(Amazon S3 포함)
오브젝트를 대상으로 이동하는 원인은 무엇입니까?	활성 ILM 정책에 있는 하나 이상의 ILM 규칙. ILM 규칙은 StorageGRID이 클라우드 스토리지 풀로 이동하는 오브젝트와 오브젝트를 이동할 시기를 정의합니다.	CloudMirror 엔드포인트로 구성된 소스 버킷에 새 객체를 인스팅하는 작업. 버킷이 CloudMirror 엔드포인트로 구성되기 전에 소스 버킷에 있던 객체는 수정되지 않으면 복제되지 않습니다.
객체를 검색하는 방법은 무엇입니까?	애플리케이션이 StorageGRID에 요청을 보내 클라우드 스토리지 풀로 이동된 객체를 검색해야 합니다. 개체의 복사본만 아카이브 스토리지로 전환된 경우 StorageGRID는 개체를 복원하는 프로세스를 관리하여 검색할 수 있습니다.	타겟 버킷의 미러링된 복사본은 독립 복사본이므로 애플리케이션이 StorageGRID 또는 S3 타겟에 요청을 함으로써 오브젝트를 검색할 수 있습니다. 예를 들어 CloudMirror 복제를 사용하여 객체를 파트너 조직에 미러링한다고 가정합니다. 파트너는 자체 애플리케이션을 사용하여 S3 대상에서 직접 오브젝트를 읽거나 업데이트할 수 있습니다. StorageGRID를 사용할 필요가 없습니다.
목적지에서 직접 읽을 수 있습니까?	아니요 클라우드 스토리지 풀로 이동된 오브젝트는 StorageGRID에서 관리합니다. 읽기 요청은 StorageGRID으로 전달되어야 합니다(StorageGRID은 클라우드 스토리지 풀에서 검색을 담당함).	예, 미러링된 복사본은 독립 복사본이므로 그렇습니다.
소스에서 개체를 삭제하면 어떻게 됩니까?	이 오브젝트는 클라우드 스토리지 풀에서도 삭제됩니다.	삭제 작업은 복제되지 않습니다. 삭제된 객체가 StorageGRID 버킷에 더 이상 존재하지 않지만 대상 버킷에는 계속 존재합니다. 마찬가지로, 소스에 영향을 주지 않고 대상 버킷의 오브젝트를 삭제할 수 있습니다.
재해 발생 후 개체에 어떻게 액세스합니까(StorageGRID 시스템이 작동하지 않음)?	장애가 발생한 StorageGRID 노드를 복구해야 합니다. 이 프로세스 중에 Cloud Storage Pool의 복사본을 사용하여 복제된 개체의 복사본을 복원할 수 있습니다.	CloudMirror 대상에 있는 오브젝트 복사본은 StorageGRID와 독립적이므로 StorageGRID 노드를 복구하기 전에 직접 액세스할 수 있습니다.

클라우드 스토리지 풀을 생성합니다

클라우드 스토리지 풀을 생성할 때 StorageGRID에서 오브젝트를 저장할 외부 버킷 또는 컨테이너의 이름과 위치, 클라우드 공급자 유형(Amazon S3 또는 Azure Blob Storage) 및 StorageGRID이 외부 버킷 또는 컨테이너에 액세스하는 데 필요한 정보를 지정합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- 클라우드 스토리지 풀 구성에 대한 지침을 검토했습니다.
- 클라우드 스토리지 풀에서 참조하는 외부 버킷 또는 컨테이너가 이미 있습니다.
- 버킷이나 컨테이너에 액세스하는 데 필요한 모든 인증 정보가 있습니다.

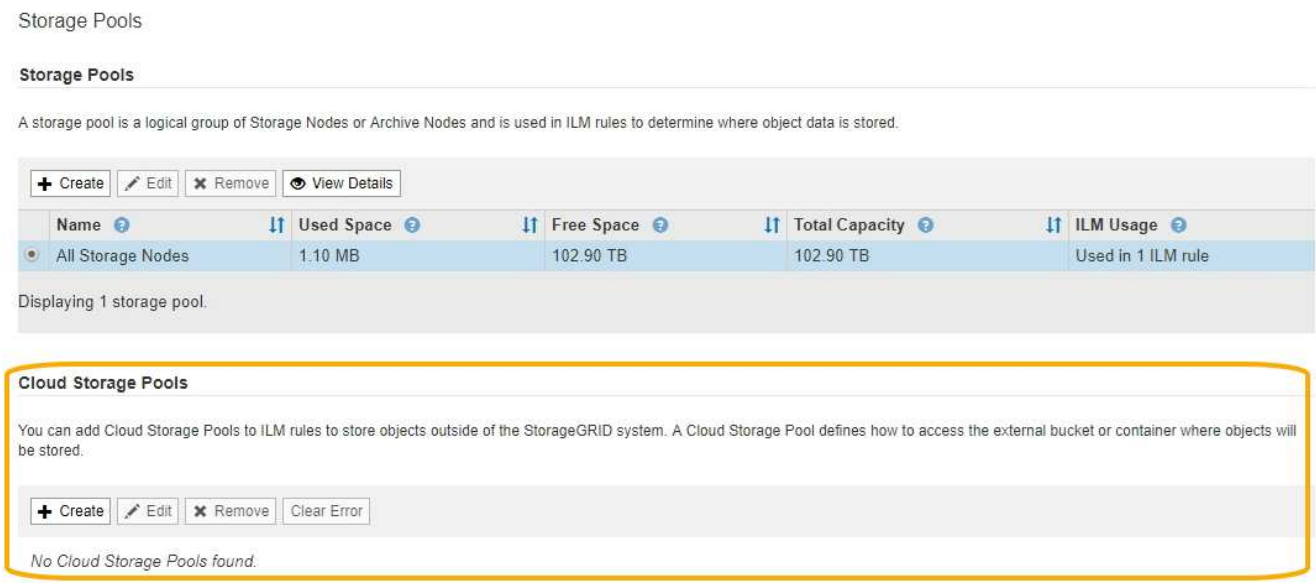
이 작업에 대해

Cloud Storage Pool은 단일 외부 S3 버킷 또는 Azure Blob 스토리지 컨테이너를 지정합니다. StorageGRID는 저장하는 즉시 클라우드 스토리지 풀을 검증하므로, 클라우드 스토리지 풀에 지정된 버킷이나 컨테이너가 존재하고 연결 가능한지 확인해야 합니다.

단계

1. ILM * > * 스토리지 풀 * 을 선택합니다.

   스토리지 풀 페이지가 나타납니다. 이 페이지에는 스토리지 풀과 클라우드 스토리지 풀의 두 섹션이 있습니다.



2. 페이지의 클라우드 스토리지 풀 섹션에서 * 생성 * 을 선택합니다.

   Create Cloud Storage Pool 대화상자가 나타납니다.

3. 다음 정보를 입력합니다.

필드에 입력합니다	설명
표시 이름	Cloud Storage Pool과 그 용도를 간략하게 설명하는 이름입니다. ILM 규칙을 구성할 때 쉽게 식별할 수 있는 이름을 사용합니다.
공급자 유형	이 클라우드 스토리지 풀에 사용할 클라우드 공급자: • * Amazon S3 *: S3, C2S S3 또는 Google Cloud Platform (GCP) 엔드포인트에 대해 이 옵션을 선택합니다. • * Azure Blob 저장소 * ◦ 참고: * 공급자 유형을 선택하면 서비스 끝점, 인증 및 서버 검증 섹션이 페이지 하단에 나타납니다.
버킷 또는 컨테이너	Cloud Storage Pool용으로 생성한 외부 S3 버킷 또는 Azure 컨테이너의 이름입니다. 여기서 지정하는 이름은 버킷 또는 컨테이너의 이름과 정확히 일치해야 합니다. 그렇지 않으면 클라우드 스토리지 풀을 생성하지 못합니다. 클라우드 스토리지 풀을 저장한 후에는 이 값을 변경할 수 없습니다.

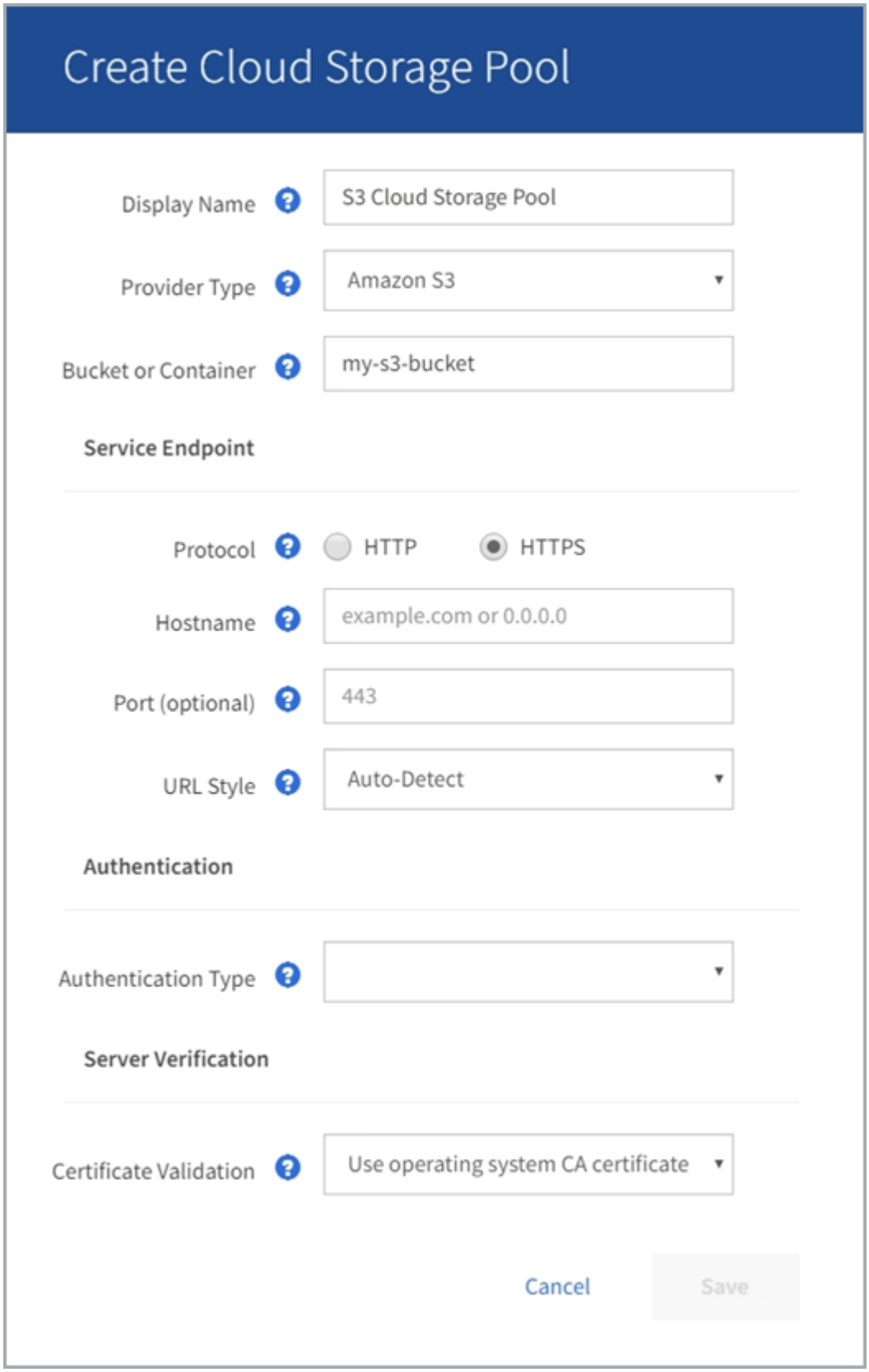
4. 선택한 공급자 유형에 따라 페이지의 서비스 엔드포인트, 인증 및 서버 검증 섹션을 완료합니다.
   - S3: 클라우드 스토리지 풀에 대한 인증 세부 정보를 지정합니다
   - C2S S3: 클라우드 스토리지 풀에 대한 인증 세부 정보를 지정합니다
   - Azure: 클라우드 스토리지 풀에 대한 인증 세부 정보를 지정합니다

S3: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정

S3용 Cloud Storage Pool을 생성할 때 Cloud Storage Pool 엔드포인트를 위해 필요한 인증 유형을 선택해야 합니다. 익명 을 지정하거나 액세스 키 ID 및 비밀 액세스 키를 입력할 수 있습니다.

필요한 것

- 클라우드 스토리지 풀에 대한 기본 정보를 입력하고 공급자 유형으로 * Amazon S3 * 를 지정했습니다.



- 액세스 키 인증을 사용하는 경우 외부 S3 버킷의 액세스 키 ID 및 비밀 액세스 키를 알고 있어야 합니다.

단계

1. 서비스 끝점 * 섹션에서 다음 정보를 제공합니다.

   a. 클라우드 스토리지 풀에 연결할 때 사용할 프로토콜을 선택합니다.

      기본 프로토콜은 HTTPS입니다.

   b. 클라우드 스토리지 풀의 서버 호스트 이름 또는 IP 주소를 입력합니다.

      예를 들면 다음과 같습니다.

      '3-*aws-region*.amazonaws.com'을 선택합니다

      > 이 필드에 버킷 이름을 포함하지 마십시오. 버킷 이름은 * 버킷 또는 컨테이너 * 필드에 포함합니다.

   a. 필요에 따라 클라우드 스토리지 풀에 연결할 때 사용할 포트를 지정합니다.

      기본 포트(HTTPS의 경우 포트 443, HTTP의 경우 포트 80)를 사용하려면 이 필드를 비워 둡니다.

   b. 클라우드 스토리지 풀 버킷의 URL 스타일 선택:

옵션을 선택합니다	설명
가상 호스트 스타일	가상 호스팅 방식의 URL을 사용하여 버킷을 액세스합니다. 가상 호스팅 방식의 URL에는 'https://bucket-name.s3.company.com/key-name` 과 같이 도메인 이름의 일부로 버킷 이름이 포함됩니다.
경로 스타일	경로 스타일 URL을 사용하여 버킷에 액세스합니다. 경로 스타일 URL의 끝에는 'https://s3.company.com/bucket-name/key-name` 과 같은 버킷 이름이 포함됩니다. • 참고: * 경로 스타일 URL은 더 이상 사용되지 않습니다.
자동 감지	제공된 정보를 기반으로 사용할 URL 스타일을 자동으로 감지해 봅니다. 예를 들어, IP 주소를 지정하면 StorageGRID는 경로 스타일 URL을 사용합니다. 사용할 특정 스타일을 모르는 경우에만 이 옵션을 선택합니다.

2. Authentication * 섹션에서 Cloud Storage Pool 엔드포인트에 필요한 인증 유형을 선택합니다.

옵션을 선택합니다	설명
액세스 키	클라우드 스토리지 풀 버킷을 액세스하려면 액세스 키 ID와 비밀 액세스 키가 필요합니다.
익명	모든 사용자가 Cloud Storage Pool 버킷에 액세스할 수 있습니다. 액세스 키 ID와 비밀 액세스 키는 필요하지 않습니다.
CAP(C2S 액세스 포털)	C2S S3에만 사용됩니다. 로 이동합니다 C2S S3: 클라우드 스토리지 풀에 대한 인증 세부 정보 지정.

3. Access Key를 선택한 경우 다음 정보를 입력합니다.

옵션을 선택합니다	설명
액세스 키 ID	외부 버킷을 소유하는 계정의 액세스 키 ID입니다.
비밀 액세스 키	연결된 비밀 액세스 키.

4. 서버 확인 섹션에서 클라우드 스토리지 풀에 대한 TLS 연결에 대한 인증서 유효성을 검사하는 데 사용할 방법을 선택합니다.

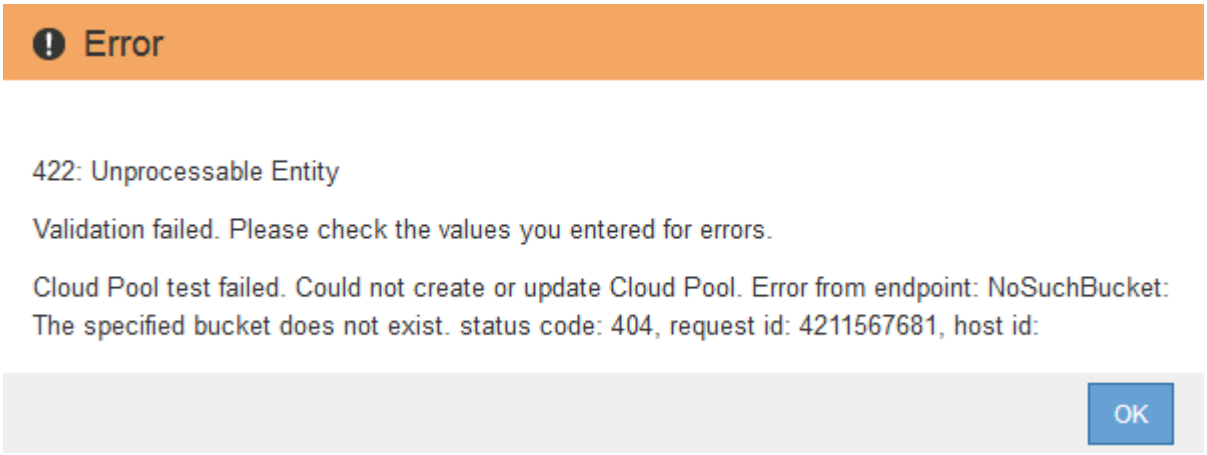
옵션을 선택합니다	설명
운영 체제 CA 인증서를 사용합니다	운영 체제에 설치된 기본 그리드 CA 인증서를 사용하여 연결을 보호합니다.
사용자 지정 CA 인증서를 사용합니다	사용자 지정 CA 인증서를 사용합니다. Select New * 를 선택하고 PEM 인코딩된 CA 인증서를 업로드합니다.
인증서를 확인하지 않습니다	TLS 연결에 사용되는 인증서가 검증되지 않았습니다.

5. 저장 * 을 선택합니다.

클라우드 스토리지 풀을 저장할 때 StorageGRID은 다음을 수행합니다.

- 버킷과 서비스 끝점이 있는지, 그리고 지정한 자격 증명을 사용하여 도달할 수 있는지 검증합니다.
- 버킷에 마커 파일을 쓰면 버킷이 클라우드 스토리지 풀임을 식별할 수 있습니다. x-ntap-sgs-cloud-pool-uuuid라는 이름의 이 파일은 제거하지 마십시오.

Cloud Storage Pool 검증이 실패하면 검증에 실패한 이유를 설명하는 오류 메시지가 표시됩니다. 예를 들어 인증서 오류가 있거나 지정한 버킷이 이미 없는 경우 오류가 보고될 수 있습니다.



의 지침을 참조하십시오 클라우드 스토리지 풀 문제 해결그런 다음 문제를 해결한 다음 Cloud Storage Pool을 다시 저장해 보십시오.

C2S S3: 클라우드 스토리지 풀에 대한 인증 세부 정보를 지정합니다

C2S(Commercial Cloud Services) S3 서비스를 클라우드 스토리지 풀로 사용하려면 C2S 액세스 포털(CAP)을 인증 유형으로 구성해야 합니다. 그러면 StorageGRID가 C2S 계정의 S3 버킷을 액세스하기 위한 임시 자격 증명을 요청할 수 있습니다.

필요한 것

- 서비스 엔드포인트를 포함하여 Amazon S3 Cloud Storage Pool에 대한 기본 정보를 입력했습니다.
- C2S 계정에 할당된 모든 필수 및 선택적 API 매개 변수를 포함하여 StorageGRID가 CAP 서버에서 임시 자격 증명을 얻는 데 사용할 전체 URL을 알고 있습니다.
- 적절한 정부 인증 기관(CA)에서 발급한 서버 CA 인증서가 있습니다. StorageGRID는 이 인증서를 사용하여 CAP 서버의 ID를 확인합니다. 서버 CA 인증서는 PEM 인코딩을 사용해야 합니다.
- 적절한 정부 인증 기관(CA)에서 발급한 클라이언트 인증서가 있습니다. StorageGRID는 이 인증서를 사용하여 CAP 서버에 대한 자체 ID를 만듭니다. 클라이언트 인증서는 PEM 인코딩을 사용해야 하며 C2S 계정에 대한 액세스 권한이 부여되어야 합니다.
- 클라이언트 인증서에 대한 PEM 인코딩된 개인 키가 있습니다.
- 클라이언트 인증서의 개인 키가 암호화된 경우 암호를 해독하기 위한 암호가 있습니다.

단계

1. 인증 * 섹션의 * 인증 유형 * 드롭다운에서 * CAP(C2S 액세스 포털) * 를 선택합니다.

   CAP C2S 인증 필드가 나타납니다.

Create Cloud Storage Pool

Display Name: C2S Cloud Storage Pool

Provider Type: Amazon S3

Bucket or Container: my-c2s-bucket

Service Endpoint

Protocol: HTTP HTTPS

Hostname: s3-aws-region.amazonaws.com

Port (optional): 443

URL Style: Auto-Detect

Authentication

Authentication Type: CAP (C2S Access Portal)

Temporary Credentials URL: https://example.com/CAP/api/v1/cred

Server CA Certificate: Select New

Client Certificate: Select New

Client Private Key: Select New

Client Private Key Passphrase (optional):

Server Verification

Certificate Validation: Use operating system CA certificate

Cancel Save

2. 다음 정보를 제공합니다.
   a. 임시 자격 증명 URL * 의 경우 StorageGRID가 C2S 계정에 할당된 모든 필수 및 선택적 API 매개 변수를 포함하여 CAP 서버에서 임시 자격 증명을 얻는 데 사용할 전체 URL을 입력합니다.
   b. 서버 CA 인증서 * 의 경우 * 새로 선택 * 을 선택하고 StorageGRID가 CAP 서버를 확인하는 데 사용할 PEM 인코딩된 CA 인증서를 업로드합니다.
   c. 클라이언트 인증서 * 의 경우 * 새 항목 선택 * 을 선택하고 StorageGRID가 CAP 서버에 자신을 식별하는 데 사용할 PEM 인코딩된 인증서를 업로드합니다.
   d. 클라이언트 개인 키 * 의 경우 * 새 항목 선택 * 을 선택하고 클라이언트 인증서에 대한 PEM 인코딩 개인 키를 업로드합니다.

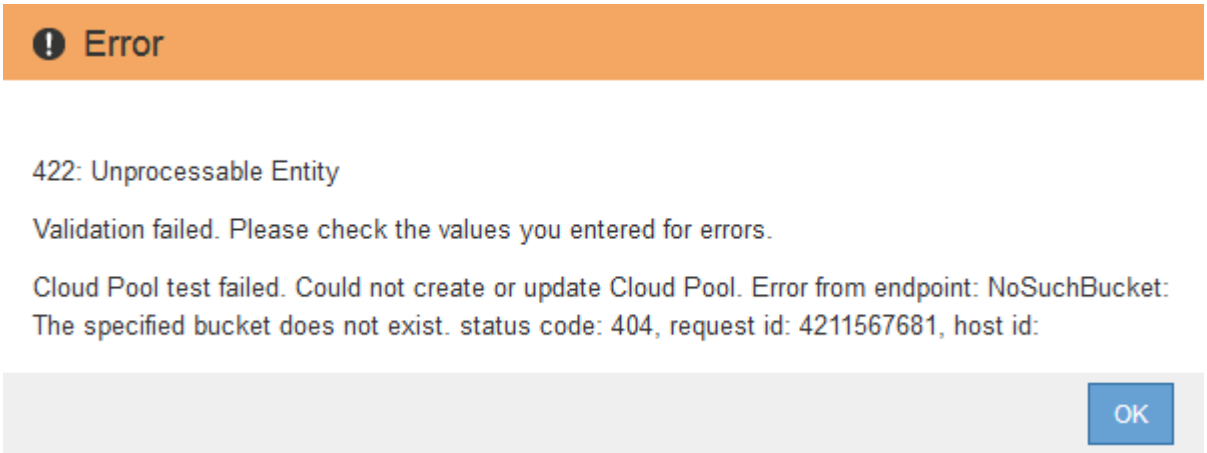
      개인 키가 암호화된 경우 기존 형식을 사용해야 합니다. (PKCS #8 암호화된 형식은 지원되지 않습니다.)

   e. 클라이언트 개인 키가 암호화된 경우 클라이언트 개인 키의 암호를 해독하기 위한 암호를 입력합니다. 그렇지 않으면 * Client Private Key Passphrase * 필드를 비워 둡니다.
3. 서버 확인 섹션에서 다음 정보를 제공합니다.
   a. 인증서 유효성 검사 * 의 경우 * 사용자 지정 CA 인증서 사용 * 을 선택합니다.
   b. Select New * 를 선택하고 PEM 인코딩된 CA 인증서를 업로드합니다.
4. 저장 * 을 선택합니다.

클라우드 스토리지 풀을 저장할 때 StorageGRID은 다음을 수행합니다.

- 버킷과 서비스 끝점이 있는지, 그리고 지정한 자격 증명을 사용하여 도달할 수 있는지 검증합니다.
- 버킷에 마커 파일을 쓰면 버킷이 클라우드 스토리지 풀임을 식별할 수 있습니다. x-ntap-sgs-cloud-pool-uuuid라는 이름의 이 파일은 제거하지 마십시오.

Cloud Storage Pool 검증이 실패하면 검증에 실패한 이유를 설명하는 오류 메시지가 표시됩니다. 예를 들어 인증서 오류가 있거나 지정한 버킷이 이미 없는 경우 오류가 보고될 수 있습니다.



의 지침을 참조하십시오 클라우드 스토리지 풀 문제 해결그런 다음 문제를 해결한 다음 Cloud Storage Pool을 다시 저장해 보십시오.

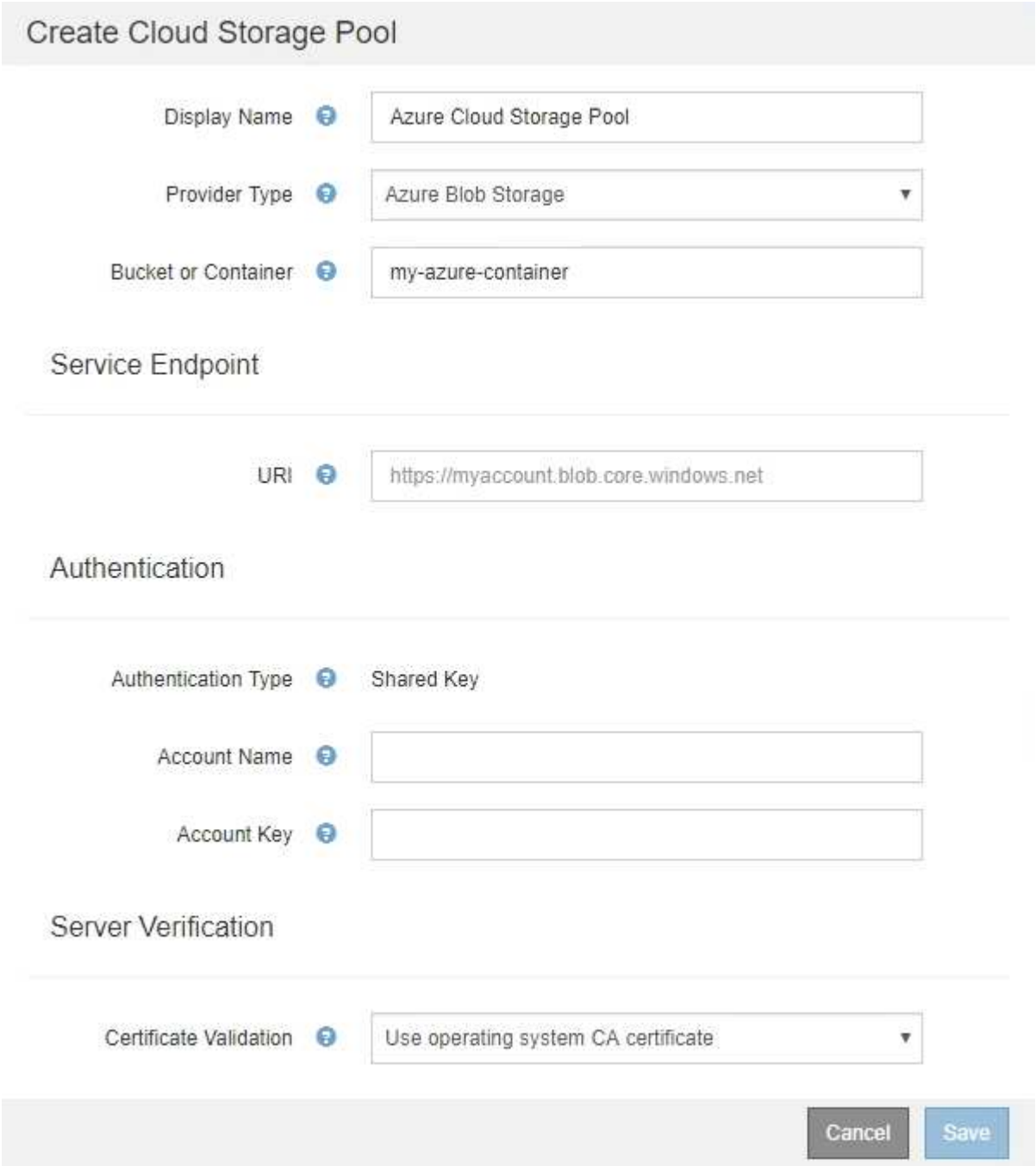
Azure: 클라우드 스토리지 풀에 대한 인증 세부 정보를 지정합니다

Azure Blob 스토리지용 Cloud Storage Pool을 생성할 때 StorageGRID에서 개체를 저장하는

데 사용할 외부 컨테이너의 계정 이름 및 계정 키를 지정해야 합니다.

필요한 것

- 클라우드 스토리지 풀에 대한 기본 정보를 입력하고 공급자 유형으로 * Azure Blob Storage * 를 지정했습니다. * 공유 키 * 가 * 인증 유형 * 필드에 나타납니다.



- 클라우드 스토리지 풀에 사용되는 Blob 스토리지 컨테이너에 액세스하는 데 사용되는 URI(Uniform Resource Identifier)를 알고 있습니다.
- 스토리지 계정의 이름과 암호 키를 알고 있습니다. Azure 포털을 사용하여 이러한 값을 찾을 수 있습니다.

단계

1. Service Endpoint * 섹션에서 Cloud Storage Pool에 사용되는 Blob 저장소 컨테이너에 액세스하는 데 사용되는 URI(Uniform Resource Identifier)를 입력합니다.

다음 형식 중 하나로 URI를 지정합니다.

- (https://host:port`)
- (http://host:port`)

포트를 지정하지 않으면 기본적으로 포트 443이 HTTPS URI에 사용되고 포트 80은 HTTP URI에 사용됩니다. Azure Blob 저장소 컨테이너용 ++ * 예제 URI *: + `https://myaccount.blob.core.windows.net`

2. 인증 * 섹션에서 다음 정보를 제공합니다.

   a. 계정 이름 * 에 대해 외부 서비스 컨테이너를 소유한 Blob 저장소 계정의 이름을 입력합니다.

   b. 계정 키 * 의 경우 Blob 저장소 계정의 암호 키를 입력합니다.

   Azure 끝점의 경우 공유 키 인증을 사용해야 합니다.

3. 서버 검증 * 섹션에서 클라우드 스토리지 풀에 대한 TLS 연결에 대한 인증서 유효성을 검사하는 데 사용할 방법을 선택합니다.

옵션을 선택합니다	설명
운영 체제 CA 인증서를 사용합니다	운영 체제에 설치된 Grid CA 인증서를 사용하여 연결을 보호합니다.
사용자 지정 CA 인증서를 사용합니다	사용자 지정 CA 인증서를 사용합니다. Select New * 를 선택하고 PEM 인코딩된 인증서를 업로드합니다.
인증서를 확인하지 않습니다	TLS 연결에 사용되는 인증서가 검증되지 않았습니다.

4. 저장 * 을 선택합니다.

클라우드 스토리지 풀을 저장할 때 StorageGRID은 다음을 수행합니다.

- 컨테이너와 URI가 있는지, 지정한 자격 증명을 사용하여 해당 컨테이너에 연결할 수 있는지 확인합니다.
- 컨테이너에 마커 파일을 기록하여 클라우드 스토리지 풀로 식별합니다. x-ntap-sgs-cloud-pool-uuuid라는 이름의 이 파일은 제거하지 마십시오.

Cloud Storage Pool 검증이 실패하면 검증에 실패한 이유를 설명하는 오류 메시지가 표시됩니다. 예를 들어 인증서 오류가 있거나 지정한 컨테이너가 이미 없는 경우 오류가 보고될 수 있습니다.

의 지침을 참조하십시오 클라우드 스토리지 풀 문제 해결그런 다음 문제를 해결한 다음 Cloud Storage Pool을 다시 저장해 보십시오.

클라우드 스토리지 풀을 편집합니다

Cloud Storage Pool을 편집하여 이름, 서비스 끝점 또는 기타 세부 정보를 변경할 수 있지만 Cloud Storage Pool의 S3 버킷 또는 Azure 컨테이너를 변경할 수는 없습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

- 특정 액세스 권한이 있습니다.
- 을(를) 검토했습니다 클라우드 스토리지 풀에 대한 고려 사항.

단계

1. ILM * > * 스토리지 풀 * 을 선택합니다.

   스토리지 풀 페이지가 나타납니다. 클라우드 스토리지 풀 테이블에는 기존 클라우드 스토리지 풀이 나열됩니다.

   Cloud Storage Pools

   You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

   + Create | Edit | Remove | Clear Error

	Pool Name	URI	Pool Type	Container	Used in ILM Rule	Last Error
◉	azure-endpoint	https://storagegrid.blob.core.windows.net	azure	azure-3	✔	
○	s3-endpoint	https://s3.amazonaws.com	s3	s3-1	✔	

   Displaying 2 pools.

2. 편집할 클라우드 스토리지 풀의 라디오 버튼을 선택합니다.
3. 편집 * 을 선택합니다.
4. 필요에 따라 표시 이름, 서비스 끝점, 인증 자격 증명 또는 인증서 유효성 검사 방법을 변경합니다.

   > 클라우드 스토리지 풀의 공급자 유형 또는 S3 버킷 또는 Azure 컨테이너는 변경할 수 없습니다.

   이전에 서버 또는 클라이언트 인증서를 업로드한 경우 * 현재 보기 * 를 선택하여 현재 사용 중인 인증서를 검토할 수 있습니다.

5. 저장 * 을 선택합니다.

   클라우드 스토리지 풀을 저장할 때 StorageGRID는 버킷 또는 컨테이너와 서비스 엔드포인트가 있는지 확인하고 지정한 자격 증명을 사용하여 해당 풀에 연결할 수 있는지 검증합니다.

   Cloud Storage Pool 검증이 실패하면 오류 메시지가 표시됩니다. 예를 들어 인증서 오류가 있는 경우 오류가 보고될 수 있습니다.

   의 지침을 참조하십시오 클라우드 스토리지 풀 문제 해결그런 다음 문제를 해결한 다음 Cloud Storage Pool을 다시 저장해 보십시오.

클라우드 스토리지 풀을 제거합니다

ILM 규칙에 사용되지 않고 오브젝트 데이터가 없는 클라우드 스토리지 풀을 제거할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- S3 버킷 또는 Azure 컨테이너에 오브젝트가 포함되지 않음을 확인했습니다. 클라우드 스토리지 풀에 객체가 포함된 경우 해당 풀을 제거하려고 하면 오류가 발생합니다. 을 참조하십시오 클라우드 스토리지 풀 문제 해결.

> 클라우드 스토리지 풀을 생성할 때 StorageGRID은 마커 파일을 버킷 또는 컨테이너에 작성하여 클라우드 스토리지 풀로 식별합니다. x-ntap-sgs-cloud-pool-uuuid라는 이름의 이 파일은 제거하지 마십시오.

- 풀을 사용했을 수 있는 ILM 규칙을 이미 제거했습니다.

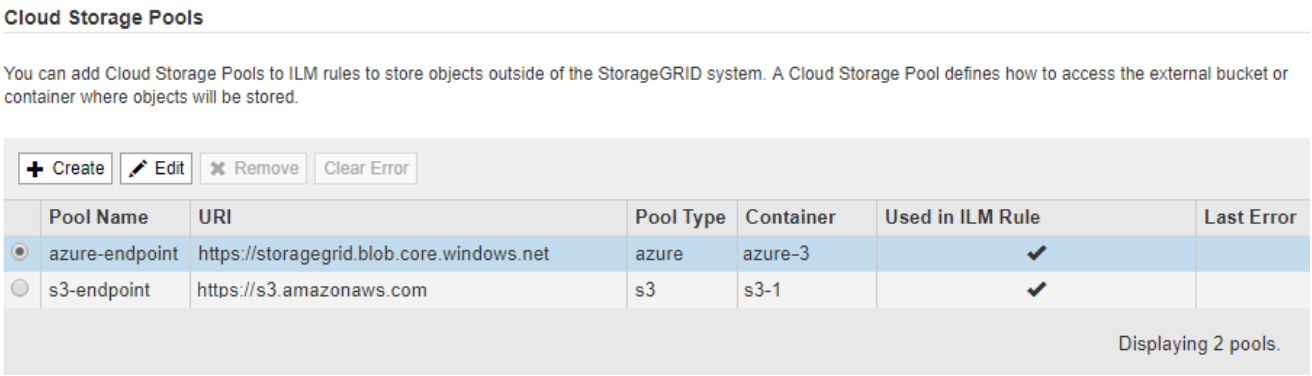
단계

1. ILM * > * 스토리지 풀 * 을 선택합니다.

   스토리지 풀 페이지가 나타납니다.

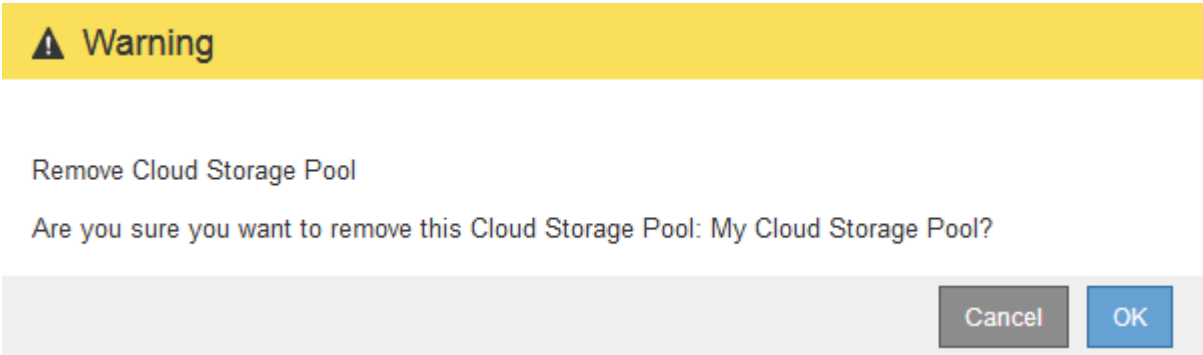
2. 현재 ILM 규칙에 사용되지 않는 클라우드 스토리지 풀의 라디오 버튼을 선택합니다.

   ILM 규칙에 사용되는 Cloud Storage Pool은 제거할 수 없습니다. 제거 * 버튼이 비활성화됩니다.



3. 제거 * 를 선택합니다.

   확인 경고가 표시됩니다.



4. OK * 를 선택합니다.

   클라우드 스토리지 풀이 제거됩니다.

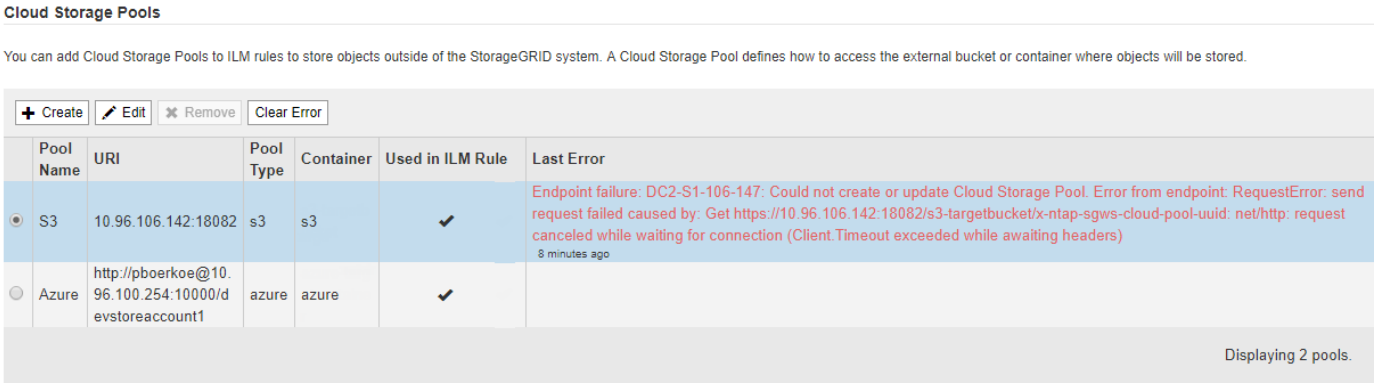
클라우드 스토리지 풀 문제 해결

클라우드 스토리지 풀을 생성, 편집 또는 삭제할 때 오류가 발생하는 경우 다음 문제 해결 단계를 사용하여 문제를 해결하십시오.

오류가 발생했는지 확인합니다

StorageGRID은 모든 클라우드 스토리지 풀에 대해 1분에 한 번씩 간단한 상태 점검을 수행하여 클라우드 스토리지 풀에 액세스할 수 있으며 올바르게 작동하는지 확인합니다. 상태 점검 시 문제가 감지되면 스토리지 풀 페이지의 클라우드 스토리지 풀 테이블의 마지막 오류 열에 메시지가 표시됩니다.

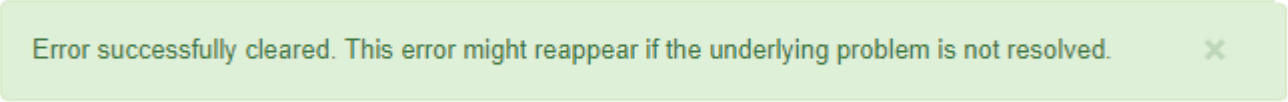
이 표에는 각 클라우드 스토리지 풀에 대해 감지된 가장 최근 오류가 표시되며 오류가 발생한 시간이 표시됩니다.



또한, 상태 점검 시 지난 5분 내에 하나 이상의 새 Cloud Storage Pool 오류가 발생한 것을 감지하면 * Cloud Storage Pool connectivity error * 경고가 트리거됩니다. 이 알림에 대한 e-메일 알림을 받으면 스토리지 풀 페이지(* ILM * > * 스토리지 풀 * 선택)로 이동하여 마지막 오류 열의 오류 메시지를 검토하고 아래의 문제 해결 지침을 참조하십시오.

오류가 해결되었는지 확인합니다

근본적인 문제를 해결한 후 오류가 해결되었는지 확인할 수 있습니다. 클라우드 스토리지 풀 페이지에서 끝점의 라디오 버튼을 선택하고 * 오류 지우기 * 를 선택합니다. 확인 메시지는 StorageGRID에서 클라우드 스토리지 풀에 대한 오류를 제거했음을 나타냅니다.



기본 문제가 해결된 경우 오류 메시지가 더 이상 표시되지 않습니다. 그러나 기본 문제가 해결되지 않았거나 다른 오류가 발생한 경우 몇 분 내에 마지막 오류 열에 오류 메시지가 표시됩니다.

오류: 이 클라우드 스토리지 풀에 예기치 않은 콘텐츠가 있습니다

클라우드 스토리지 풀을 생성, 편집 또는 삭제하려고 하면 이 오류가 발생할 수 있습니다. 이 오류는 버킷 또는 컨테이너에 'x-NTAP-SGWs-cloud-pool-uuuid' 마커 파일이 포함되어 있지만 해당 파일에 예상 UUID가 없는 경우에 발생합니다.

일반적으로 새 클라우드 스토리지 풀을 생성하고 StorageGRID의 다른 인스턴스가 이미 동일한 클라우드 스토리지 풀을 사용 중인 경우에만 이 오류가 표시됩니다.

다음 단계를 수행하여 문제를 해결하십시오.

- 귀사에서 이 클라우드 스토리지 풀을 사용하고 있는 사람이 없는지 확인하십시오.
- 'x-ntap-SGWS-cloud-pool-uuid' 파일을 삭제하고 클라우드 스토리지 풀을 다시 구성하십시오.

오류: 클라우드 스토리지 풀을 생성하거나 업데이트할 수 없습니다. 끝점에서 오류가 발생했습니다

클라우드 스토리지 풀을 생성하거나 편집하려고 할 때 이 오류가 발생할 수 있습니다. 이 오류는 일부 연결 또는 구성 문제로 인해 StorageGRID가 클라우드 스토리지 풀에 데이터를 쓸 수 없음을 나타냅니다.

문제를 해결하려면 끝점에서 오류 메시지를 검토하십시오.

- 오류 메시지에 'get_url_:EOF'가 포함된 경우 Cloud Storage Pool에 사용되는 서비스 엔드포인트에서 HTTPS가 필요한 컨테이너 또는 버킷에 대해 HTTP 프로토콜을 사용하지 않는지 확인합니다.
- 오류 메시지에 'get_url_:net/http:request cancelled While waiting for connection'이 포함되어 있으면 네트워크 구성에서 스토리지 노드가 클라우드 스토리지 풀에 사용되는 서비스 엔드포인트에 액세스할 수 있는지 확인합니다.
- 다른 모든 끝점 오류 메시지에 대해 다음 중 하나 이상을 시도합니다.
  - Cloud Storage Pool에 입력한 것과 동일한 이름의 외부 컨테이너 또는 버킷을 생성한 다음, 새 Cloud Storage Pool을 다시 저장하십시오.
  - Cloud Storage Pool에 지정한 컨테이너 또는 버킷 이름을 수정하고 새 Cloud Storage Pool을 다시 저장하십시오.

오류: **CA** 인증서를 구문 분석하지 못했습니다

클라우드 스토리지 풀을 생성하거나 편집하려고 할 때 이 오류가 발생할 수 있습니다. StorageGRID에서 클라우드 스토리지 풀을 구성할 때 입력한 인증서를 구문 분석할 수 없는 경우 오류가 발생합니다.

문제를 해결하려면 제공한 CA 인증서에 문제가 있는지 확인하십시오.

오류: 이 **ID**가 인 클라우드 스토리지 풀을 찾을 수 없습니다

Cloud Storage Pool을 편집하거나 삭제하려고 하면 이 오류가 발생할 수 있습니다. 이 오류는 끝점에서 404 응답을 반환할 때 발생하며, 이는 다음 중 하나를 의미할 수 있습니다.

- Cloud Storage Pool에 사용된 자격 증명에 버킷에 대한 읽기 권한이 없습니다.
- 클라우드 스토리지 풀에 사용되는 버킷에는 'x-ntap-sgs-cloud-pool-uuuid' 마커 파일이 포함되지 않습니다.

다음 단계 중 하나 이상을 시도하여 문제를 해결하십시오.

- 구성된 액세스 키와 연결된 사용자에게 필요한 권한이 있는지 확인합니다.
- 필요한 권한이 있는 자격 증명을 사용하여 클라우드 스토리지 풀을 편집합니다.
- 사용 권한이 올바르면 지원 부서에 문의하십시오.

오류: 클라우드 스토리지 풀의 콘텐츠를 확인할 수 없습니다. 끝점에서 오류가 발생했습니다

클라우드 스토리지 풀을 삭제하려고 하면 이 오류가 발생할 수 있습니다. 이 오류는 StorageGRID에서 클라우드 스토리지 풀 버킷의 내용을 읽지 못하는 연결 또는 구성 문제가 발생했음을 나타냅니다.

문제를 해결하려면 끝점에서 오류 메시지를 검토하십시오.

오류: 객체가 이 버킷에 이미 배치되었습니다

클라우드 스토리지 풀을 삭제하려고 하면 이 오류가 발생할 수 있습니다. ILM에 의해 이동한 데이터, Cloud Storage Pool을 구성하기 전에 버킷에 있던 데이터 또는 Cloud Storage Pool을 생성한 후 다른 소스에서 버킷을 포함한

데이터가 Cloud Storage Pool에 포함된 경우에는 Cloud Storage Pool을 삭제할 수 없습니다.

다음 단계 중 하나 이상을 시도하여 문제를 해결하십시오.

- "'클라우드 스토리지 풀 객체 라이프사이클"에서 객체를 StorageGRID로 다시 이동하는 지침을 따르십시오."
- ILM을 통해 나머지 객체가 Cloud Storage Pool에 포함되지 않은 것으로 확신하는 경우 버킷에서 객체를 수동으로 삭제하십시오.

> ILM에 의해 배치된 클라우드 스토리지 풀에서 개체를 수동으로 삭제하지 마십시오. 나중에 StorageGRID에서 수동으로 삭제된 개체에 액세스하려고 하면 삭제된 개체를 찾을 수 없습니다.

오류: 프록시에서 클라우드 스토리지 풀에 연결하려고 시도하는 동안 외부 오류가 발생했습니다

스토리지 노드와 클라우드 스토리지 풀에 사용되는 외부 S3 엔드포인트 간에 투명하지 않은 스토리지 프록시를 구성한 경우 이 오류가 발생할 수 있습니다. 이 오류는 외부 프록시 서버가 클라우드 스토리지 풀 끝점에 도달할 수 없는 경우에 발생합니다. 예를 들어 DNS 서버가 호스트 이름을 확인할 수 없거나 외부 네트워킹 문제가 있을 수 있습니다.

다음 단계 중 하나 이상을 시도하여 문제를 해결하십시오.

- 클라우드 스토리지 풀(* ILM * > * 스토리지 풀 *)의 설정을 확인합니다.
- 스토리지 프록시 서버의 네트워킹 구성을 확인합니다.

관련 정보

Cloud Storage Pool 개체의 수명주기입니다

삭제 코딩 프로파일을 구성합니다

삭제 코딩 프로필을 생성합니다

삭제 코딩 프로필을 생성하려면 스토리지 노드가 포함된 스토리지 풀을 삭제 코딩 체계와 연결합니다. 이 연관은 생성된 데이터 및 패리티 조각의 수와 시스템이 이러한 조각을 배포하는 위치를 결정합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- 정확히 하나의 사이트 또는 세 개 이상의 사이트가 포함된 스토리지 풀이 포함된 스토리지 풀을 생성했습니다. 사이트가 두 개뿐인 스토리지 풀에는 삭제 코딩 스키마를 사용할 수 없습니다.

이 작업에 대해

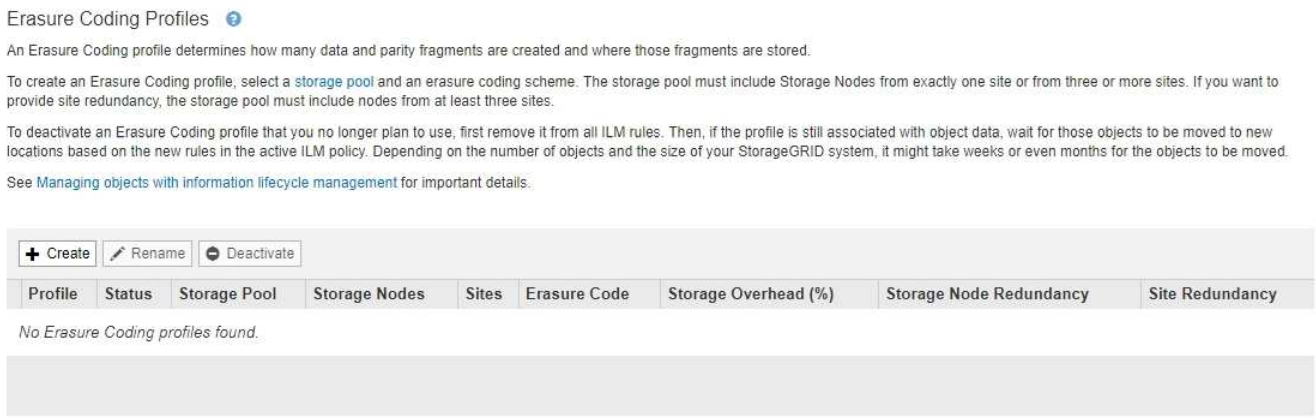
삭제 코딩 프로필에 사용되는 스토리지 풀에는 정확히 하나의 사이트 또는 세 개 이상의 사이트가 포함되어야 합니다. 사이트 이중화를 제공하려면 스토리지 풀에 사이트가 3개 이상 있어야 합니다.

> 스토리지 노드가 포함된 스토리지 풀을 선택해야 합니다. 삭제 코딩 데이터에는 아카이브 노드를 사용할 수 없습니다.

단계

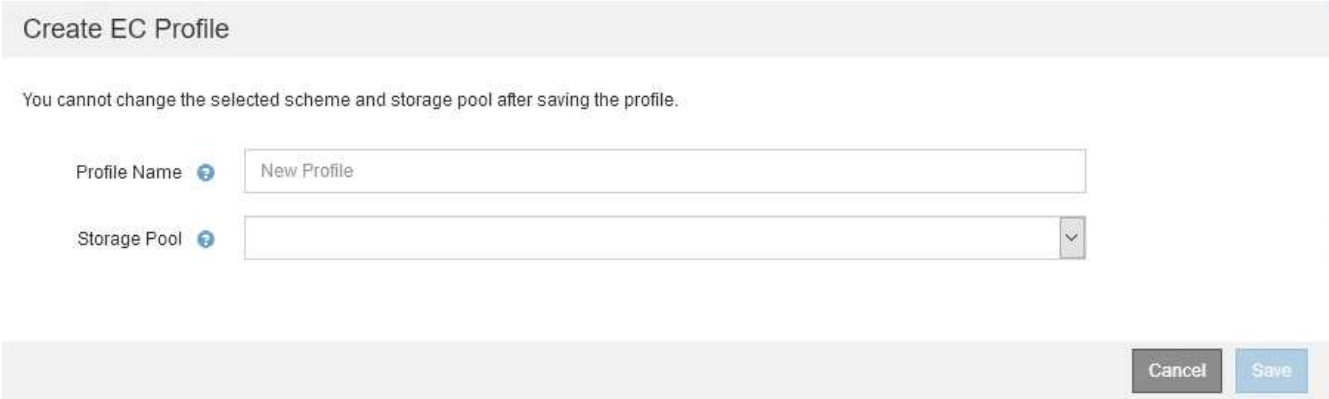
1. ILM * > * 삭제 코딩 * 을 선택합니다.

   삭제 코딩 프로필 페이지가 나타납니다.



2. Create * 를 선택합니다.

   EC 프로파일 만들기 대화 상자가 나타납니다.



3. 삭제 코딩 프로필의 고유한 이름을 입력합니다.

   삭제 코딩 프로필 이름은 고유해야 합니다. 기존 프로파일의 이름을 사용하면 프로파일이 비활성화된 경우에도 유효성 검사 오류가 발생합니다.

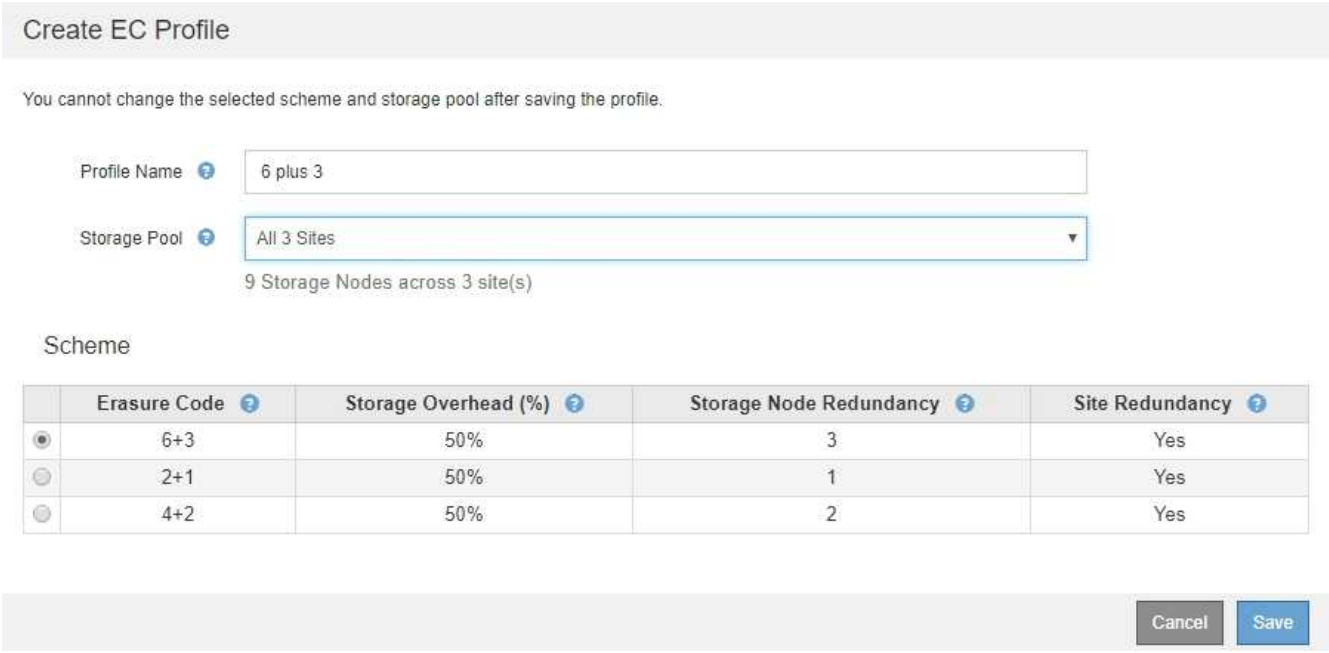
   > 삭제 코딩 프로파일 이름은 ILM 규칙에 대한 배치 지침의 스토리지 풀 이름에 추가됩니다.

4. 이 삭제 코딩 프로파일에 대해 생성한 스토리지 풀을 선택합니다.

   > 그리드에 현재 사이트가 하나만 포함된 경우 기본 스토리지 풀, 모든 스토리지 노드 또는 기본 사이트, 모든 사이트를 포함하는 스토리지 풀을 사용할 수 없습니다. 이 동작은 두 번째 사이트가 추가된 경우 삭제 코딩 프로필이 무효로 되는 것을 방지합니다.

> 스토리지 풀에 정확히 두 개의 사이트가 포함된 경우 해당 스토리지 풀을 삭제 코딩에 사용할 수 없습니다. 두 개의 사이트가 있는 스토리지 풀에는 삭제 코딩 스키마를 사용할 수 없습니다.

스토리지 풀을 선택하면 풀의 스토리지 노드 및 사이트 수에 따라 사용 가능한 삭제 코딩 구성표 목록이 표시됩니다.



사용 가능한 각 삭제 코딩 구성표에 대해 다음 정보가 나열됩니다.

- * 삭제 코드 *: 삭제 코딩 체계의 이름(데이터 조각 + 패리티 단편).
- * 스토리지 오버헤드(%) *: 오브젝트의 데이터 크기에 상대적인 패리티 조각에 필요한 추가 스토리지 스토리지 오버헤드 = 총 패리티 조각 수/총 데이터 조각 수
- * 스토리지 노드 이중화 *: 객체 데이터 검색 기능을 유지하면서 손실될 수 있는 스토리지 노드 수입니다.
- * 사이트 이중화 *: 사이트가 손실된 경우 선택한 삭제 코드로 오브젝트 데이터를 검색할 수 있는지 여부.

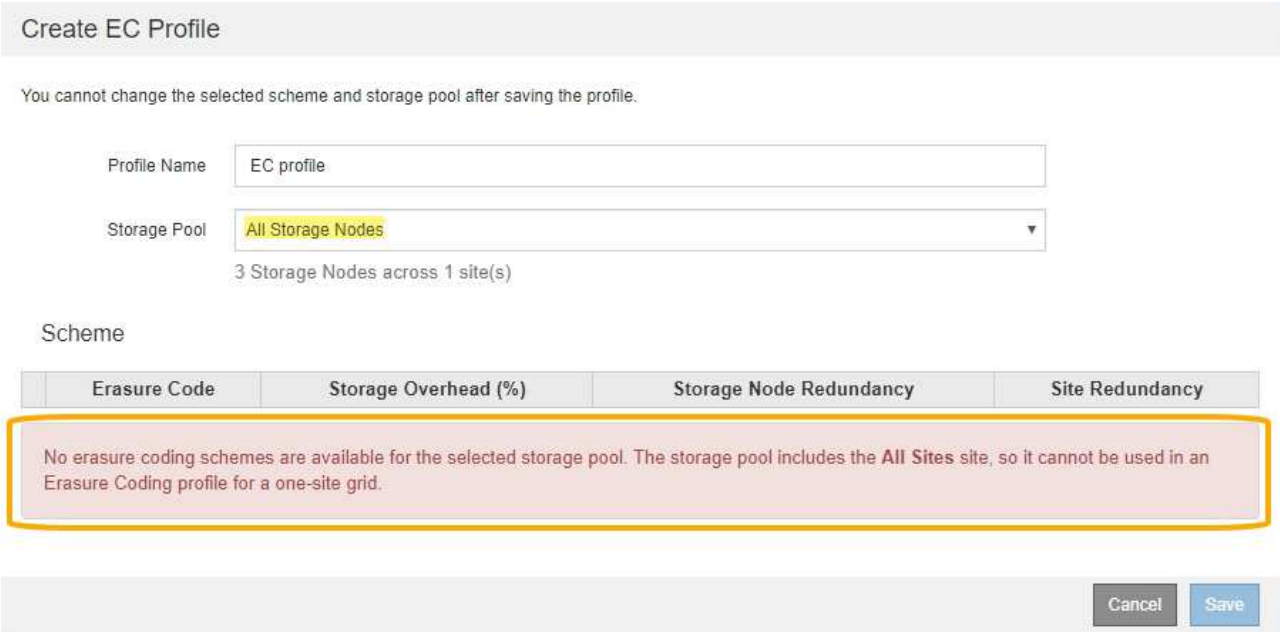
  사이트 이중화를 지원하려면 선택한 스토리지 풀에 사이트 손실을 허용할 수 있는 충분한 스토리지 노드가 있는 여러 사이트가 포함되어 있어야 합니다. 예를 들어, 6+3 삭제 코딩 체계를 사용하여 사이트 이중화를 지원하려면 선택한 스토리지 풀에 각 사이트에 3개 이상의 스토리지 노드가 포함된 사이트가 3개 이상 포함되어야 합니다.

  다음과 같은 경우 메시지가 표시됩니다.

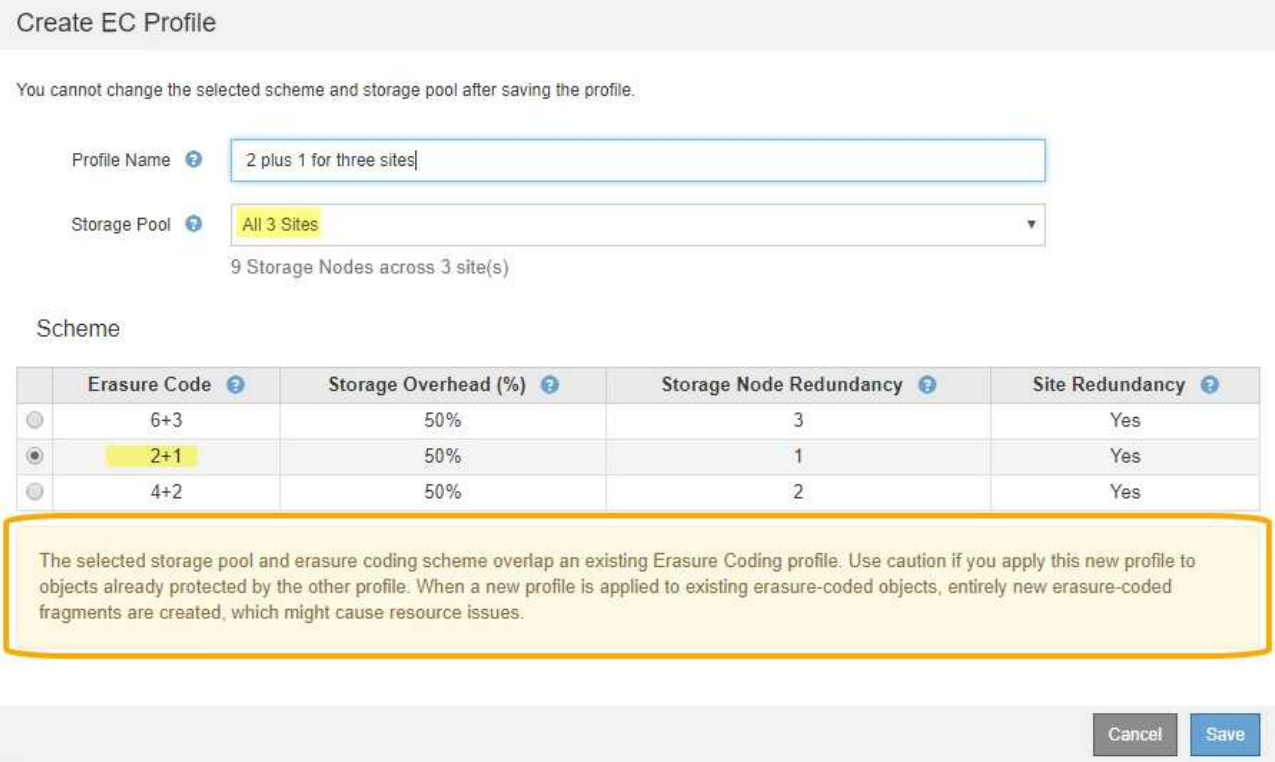
- 선택한 스토리지 풀은 사이트 이중화를 제공하지 않습니다. 선택한 스토리지 풀에 사이트가 하나만 포함된 경우 다음 메시지가 표시됩니다. ILM 규칙에서 이 삭제 코딩 프로파일을 사용하여 노드 장애로부터 보호할 수 있습니다.

- 선택한 스토리지 풀이 삭제 코딩 체계에 대한 요구 사항을 충족하지 않습니다. 예를 들어 선택한 스토리지 풀에 정확히 두 개의 사이트가 포함된 경우 다음 메시지가 표시됩니다. 삭제 코딩을 사용하여 오브젝트 데이터를 보호하려면 정확히 하나의 사이트가 있는 스토리지 풀을 선택하거나 세 개 이상의 사이트가 있는 스토리지 풀을 선택해야 합니다.

- 그리드에는 사이트가 하나만 포함되며 기본 스토리지 풀, 모든 스토리지 노드 또는 기본 사이트인 모든 사이트가 포함된 스토리지 풀을 선택했습니다.



- 선택한 삭제 코딩 체계와 스토리지 풀이 다른 삭제 코딩 프로파일과 겹칩니다.



이 예에서는 다른 삭제 코딩 프로파일에서 2+1 구성표를 사용하고 다른 프로파일의 스토리지 풀에서도 3개 사이트 모두 스토리지 풀의 사이트 중 하나를 사용하므로 경고 메시지가 나타납니다.

이 새 프로파일을 만들 수 있는 것은 아니지만 ILM 정책에서 사용할 때는 매우 주의해야 합니다. 이 새 프로필이 이미 다른 프로필에 의해 보호되는 기존의 삭제 코딩 개체에 적용되는 경우 StorageGRID는 완전히 새로운 오브젝트 조각 세트를 생성합니다. 기존 2 + 1 조각은 재사용하지 않습니다. 삭제 코딩 방식이 동일하더라도 한 삭제 코딩 프로필에서 다른 프로필로 마이그레이션할 때 리소스 문제가 발생할 수 있습니다.

5. 둘 이상의 삭제 코딩 체계가 나열되어 있는 경우 사용할 삭제 코딩 방법을 선택합니다.

   사용할 삭제 코딩 체계를 결정할 때는 복구를 위한 네트워크 트래픽 요구 사항과 내결함성(패리티 세그먼트를 더 많이 보유함으로써 달성됨)을 균형 있게 조정해야 합니다(조각은 많을수록 네트워크 트래픽이 증가함). 예를 들어, 4+2 체계와 6+3 체계 중 하나를 결정할 때 추가적인 패리티 및 내결함성을 필요로 하는 경우 6+3 체계를 선택합니다. 노드 복구 중에 네트워크 리소스가 네트워크 사용량을 줄이도록 제한되는 경우 4+2 스키마를 선택합니다.

6. 저장 * 을 선택합니다.

삭제 코딩 프로파일의 이름을 바꿉니다

삭제 코딩 프로필의 이름을 변경하여 프로필이 수행하는 작업을 보다 명확히 할 수 있습니다.

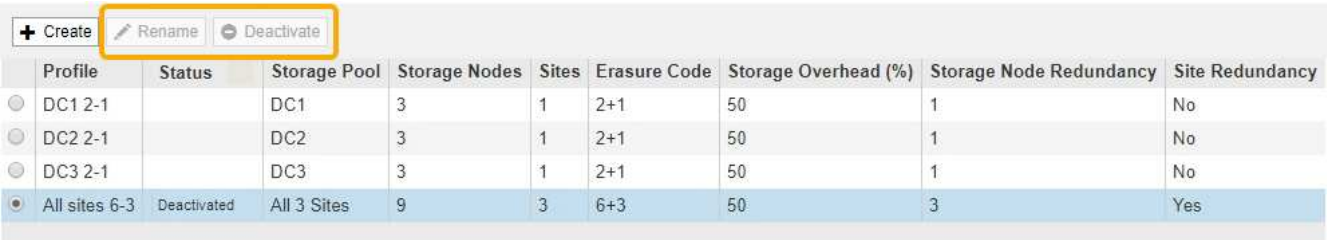
필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

단계

1. ILM * > * 삭제 코딩 * 을 선택합니다.

삭제 코딩 프로필 페이지가 나타납니다. 이름 바꾸기 * 및 * 비활성화 * 버튼이 모두 비활성화됩니다.



Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
DC1 2-1		DC1	3	1	2+1	50	1	No
DC2 2-1		DC2	3	1	2+1	50	1	No
DC3 2-1		DC3	3	1	2+1	50	1	No
All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

2. 이름을 바꿀 프로파일을 선택합니다.

   이름 바꾸기 * 및 * 비활성화 * 버튼이 활성화됩니다.

3. 이름 바꾸기 * 를 선택합니다.

   EC 프로파일 이름 바꾸기 대화 상자가 나타납니다.

4. 삭제 코딩 프로필의 고유한 이름을 입력합니다.

   삭제 코딩 프로파일 이름은 ILM 규칙에 대한 배치 지침의 스토리지 풀 이름에 추가됩니다.

> 삭제 코딩 프로필 이름은 고유해야 합니다. 기존 프로파일의 이름을 사용하면 프로파일이 비활성화된 경우에도 유효성 검사 오류가 발생합니다.

5. 저장 * 을 선택합니다.

삭제 코딩 프로필을 비활성화합니다

더 이상 사용할 계획이 없고 프로필이 현재 ILM 규칙에서 사용되지 않는 경우 삭제 코딩 프로필을 비활성화할 수 있습니다.

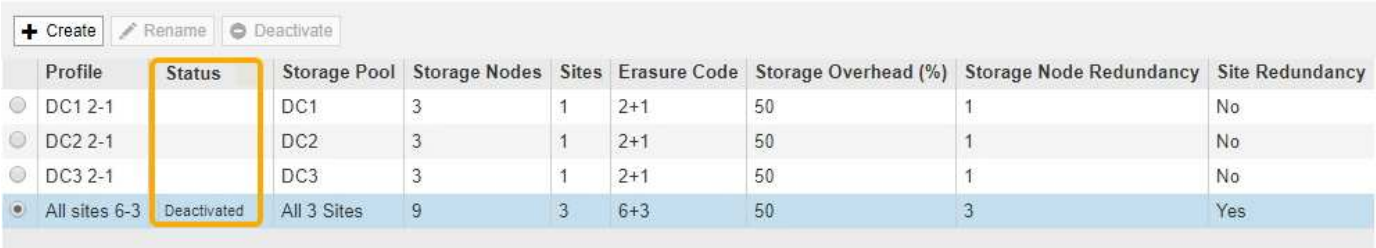
필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

- 삭제 코딩 데이터 복구 작업 또는 서비스 해제 절차가 진행 중인 것을 확인했습니다. 삭제 코딩 프로파일을 비활성화하려고 할 때 이러한 작업 중 하나가 진행 중일 때 오류 메시지가 반환됩니다.

이 작업에 대해

삭제 코딩 프로필을 비활성화하면 해당 프로필은 여전히 삭제 코딩 프로필 페이지에 표시되지만 상태는 * 비활성화 * 입니다.



Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
DC1 2-1		DC1	3	1	2+1	50	1	No
DC2 2-1		DC2	3	1	2+1	50	1	No
DC3 2-1		DC3	3	1	2+1	50	1	No
All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

비활성화된 삭제 코딩 프로필을 더 이상 사용할 수 없습니다. ILM 규칙에 대한 배치 지침을 생성할 때는 비활성화된 프로파일이 표시되지 않습니다. 비활성화된 프로필은 다시 활성화할 수 없습니다.

다음 중 하나에 해당하면 StorageGRID에서 삭제 코딩 프로필을 비활성화할 수 없습니다.

- 삭제 코딩 프로필은 현재 ILM 규칙에서 사용되고 있습니다.
- 삭제 코딩 프로파일은 더 이상 ILM 규칙에서 사용되지 않지만 프로파일의 객체 데이터 및 패리티 조각은 여전히 존재합니다.

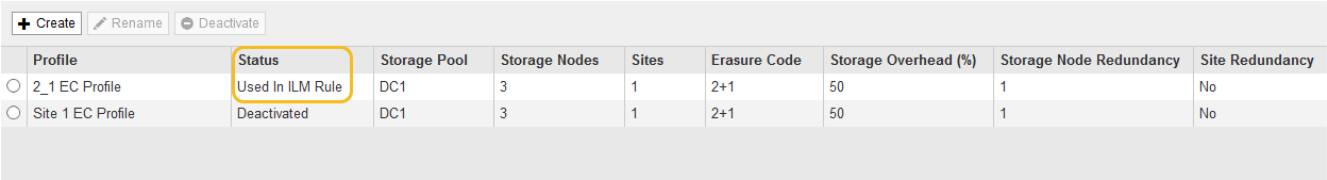
단계

1. ILM * > * 삭제 코딩 * 을 선택합니다.

   삭제 코딩 프로필 페이지가 나타납니다. 이름 바꾸기 * 및 * 비활성화 * 버튼이 모두 비활성화됩니다.

2. 상태 * 열을 검토하여 비활성화하려는 삭제 코딩 프로필이 ILM 규칙에서 사용되지 않는지 확인합니다.

   ILM 규칙에서 삭제 코딩 프로필을 사용하는 경우에는 비활성화할 수 없습니다. 이 예에서 * 2_1 EC 프로파일 * 은 적어도 하나의 ILM 규칙에서 사용됩니다.



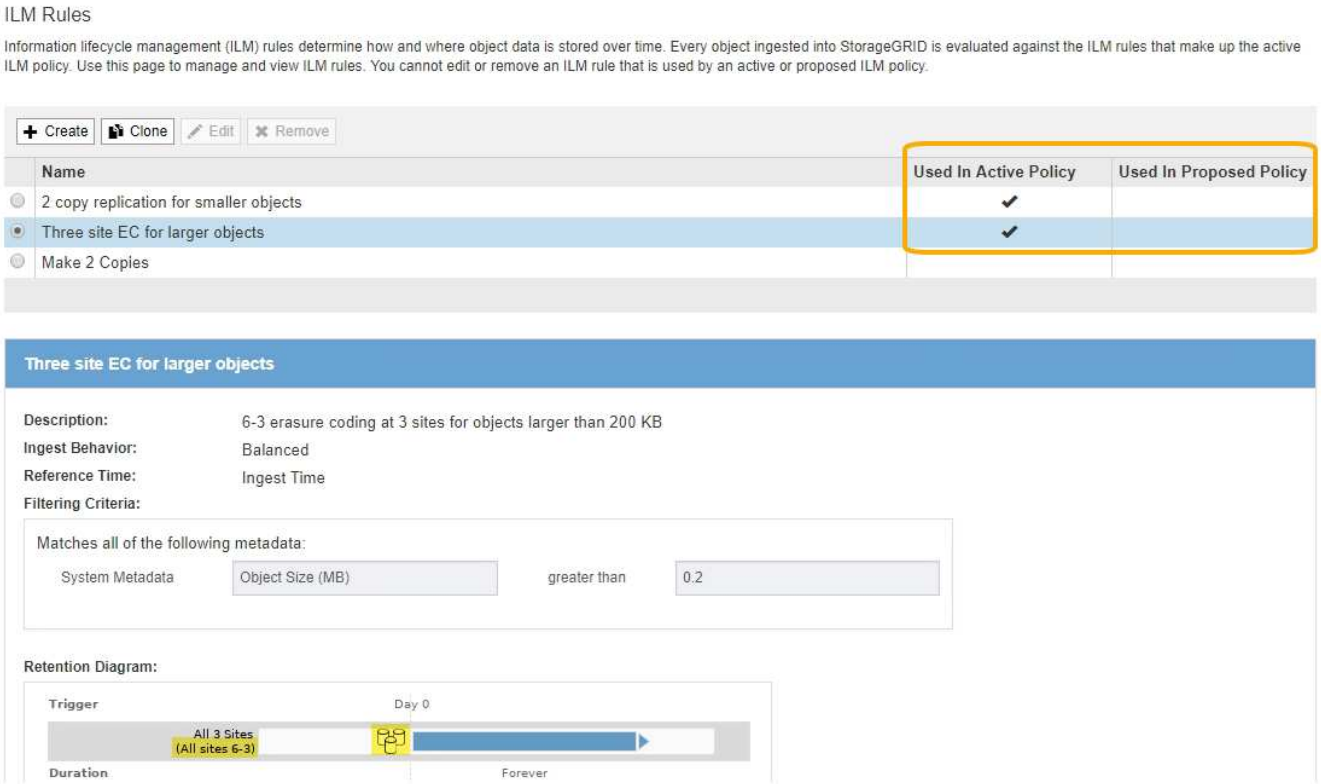
Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
2_1 EC Profile	Used In ILM Rule	DC1	3	1	2+1	50	1	No
Site 1 EC Profile	Deactivated	DC1	3	1	2+1	50	1	No

3. ILM 규칙에서 프로파일을 사용하는 경우 다음 단계를 따릅니다.

   a. ILM * > * 규칙 * 을 선택합니다.

   b. 나열된 각 규칙에 대해 라디오 버튼을 선택하고 보존 다이어그램을 검토하여 비활성화하려는 삭제 코딩 프로필을 규칙을 사용하는지 확인합니다.

      이 예에서 * 세 사이트 EC for larger objects * 규칙은 * all 3 sites * 라는 스토리지 풀과 * all sites 6-3 * 삭제 코딩 프로파일을 사용합니다. 삭제 코딩 프로필은 다음 아이콘으로 표시됩니다.



a. ILM 규칙이 비활성화하려는 삭제 코딩 프로파일을 사용하는 경우 활성 ILM 정책 또는 제안된 정책에서 규칙이 사용되는지 확인합니다.

   이 예에서는 활성 ILM 정책에서 * 3 site EC for larger objects * 규칙이 사용됩니다.

b. 삭제 코딩 프로필을 사용하는 위치에 따라 표의 추가 단계를 완료합니다.

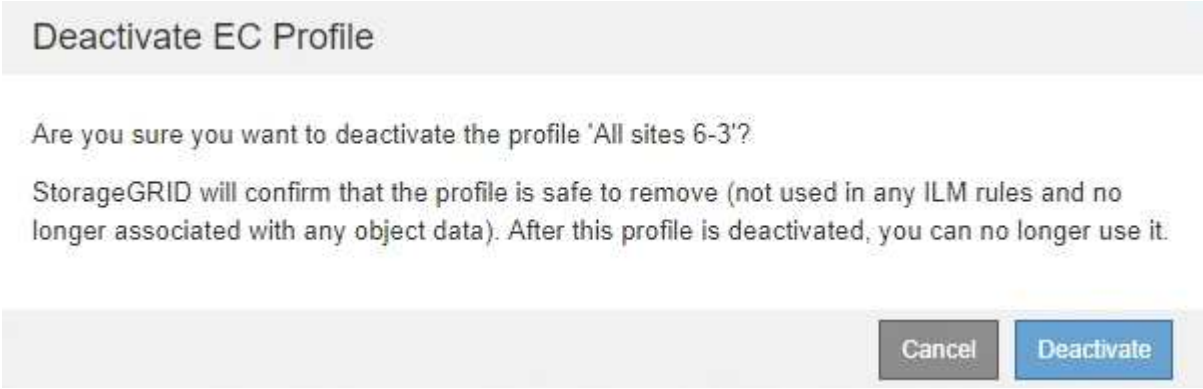
프로필은 어디에 사용되었습니까?	프로필을 비활성화하기 전에 수행할 추가 단계입니다	다음 추가 지침을 참조하십시오
어떤 ILM 규칙에도 사용하지 마십시오	추가 단계가 필요하지 않습니다. 이 절차를 계속합니다.	없음
ILM 정책에 사용된 적이 없는 ILM 규칙에서	i. 영향을 받는 모든 ILM 규칙을 편집하거나 삭제합니다. 규칙을 편집하는 경우 삭제 코딩 프로필을 사용하는 모든 배치를 제거합니다. ii. 이 절차를 계속합니다.	ILM 규칙 및 ILM 정책 작업

프로필은 어디에 사용되었습니까?	프로필을 비활성화하기 전에 수행할 추가 단계입니다	다음 추가 지침을 참조하십시오
현재 활성 ILM 정책에 있는 ILM 규칙에서	i. 활성 정책의 클론을 생성합니다. ii. 삭제 코딩 프로필을 사용하는 ILM 규칙을 제거합니다. iii. 하나 이상의 새 ILM 규칙을 추가하여 개체가 보호되도록 합니다. iv. 새 정책을 저장, 시뮬레이션 및 활성화합니다. v. 새 정책이 적용될 때까지 기다리며, 새로 추가한 규칙에 따라 기존 객체가 새 위치로 이동합니다. ◦ 참고: * StorageGRID ILM 운영 부서가 새로운 ILM 규칙을 기준으로 개체를 새 위치로 이동하는 데 몇 주 또는 몇 달이 걸릴 수 있습니다. 데이터가 연결되어 있는 동안 삭제 코딩 프로필을 안전하게 비활성화할 수 있지만 비활성화 작업이 실패합니다. 프로필이 아직 비활성화될 준비가 되지 않은 경우 오류 메시지가 표시됩니다. vi. 정책에서 제거한 규칙을 편집하거나 삭제합니다. 규칙을 편집하는 경우 삭제 코딩 프로필을 사용하는 모든 배치를 제거합니다. vii. 이 절차를 계속합니다.	• ILM 정책을 생성합니다 • ILM 규칙 및 ILM 정책 작업
현재 제안된 ILM 정책에 있는 ILM 규칙에서	i. 제안된 정책을 편집합니다. ii. 삭제 코딩 프로필을 사용하는 ILM 규칙을 제거합니다. iii. 하나 이상의 새 ILM 규칙을 추가하여 모든 개체가 보호되도록 합니다. iv. 제안된 정책을 저장합니다. v. 정책에서 제거한 규칙을 편집하거나 삭제합니다. 규칙을 편집하는 경우 삭제 코딩 프로필을 사용하는 모든 배치를 제거합니다. vi. 이 절차를 계속합니다.	• ILM 정책을 생성합니다 • ILM 규칙 및 ILM 정책 작업
ILM 정책에 기록 중인 ILM 규칙	i. 규칙을 편집하거나 삭제합니다. 규칙을 편집하는 경우 삭제 코딩 프로필을 사용하는 모든 배치를 제거합니다. (이제 규칙이 기록 정책에서 기록 규칙으로 표시됩니다.) ii. 이 절차를 계속합니다.	ILM 규칙 및 ILM 정책 작업

c. 삭제 코딩 프로파일 페이지를 새로 고쳐 프로파일이 ILM 규칙에 사용되지 않도록 합니다.

4. 프로파일이 ILM 규칙에 사용되지 않으면 라디오 버튼을 선택하고 * Deactivate * 를 선택합니다.

   EC 프로파일 비활성화 대화 상자가 나타납니다.



5. 프로필을 비활성화하려면 * Deactivate * 를 선택합니다.
   - StorageGRID가 삭제 코딩 프로필을 비활성화할 수 있는 경우 해당 상태는 * deactivated * 입니다. 더 이상 ILM 규칙에 대해 이 프로파일을 선택할 수 없습니다.
   - StorageGRID에서 프로파일을 비활성화할 수 없는 경우 오류 메시지가 나타납니다. 예를 들어, 개체 데이터가 이 프로필과 연결되어 있으면 오류 메시지가 나타납니다. 비활성화 프로세스를 다시 시도하기 전에 몇 주를 기다려야 할 수 있습니다.

영역 구성(옵션 및 **S3**만 해당)

ILM 규칙은 S3 버킷을 생성한 영역을 기준으로 오브젝트를 필터링할 수 있으므로 여러 지역의 오브젝트를 다른 스토리지 위치에 저장할 수 있습니다. 규칙에서 S3 버킷 영역을 필터로 사용하려면 먼저 시스템의 버킷에서 사용할 수 있는 영역을 생성해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

S3 버킷을 생성할 때 특정 영역에서 버킷을 생성하도록 지정할 수 있습니다. 지역을 지정하면 버킷이 지리적으로 사용자와 가까운 곳에 있어 지연 시간을 최적화하고 비용을 최소화하며 규정 요구 사항을 해결할 수 있습니다.

ILM 규칙을 생성할 때 S3 버킷과 연결된 영역을 고급 필터로 사용할 수 있습니다. 예를 들어, us-west-2 영역에서 생성된 S3 버킷의 오브젝트에만 적용되는 규칙을 설계할 수 있습니다. 그런 다음 해당 지역 내의 데이터 센터 사이트에서 스토리지 노드에 이러한 오브젝트의 복사본을 배치하도록 지정하여 지연 시간을 최적화할 수 있습니다.

영역을 구성할 때 다음 지침을 따르십시오.

- 기본적으로 모든 버킷은 us-east-1 지역에 속하는 것으로 간주됩니다.
- 테넌트 관리자 또는 테넌트 관리 API를 사용하여 버킷을 생성할 때 또는 S3 PUT Bucket API 요청에 대한 LocationConstraint 요청 요소와 함께 기본 영역이 아닌 영역을 지정하려면 먼저 Grid Manager를 사용하여 영역을 생성해야 합니다. PUT 버킷 요청이 StorageGRID에 정의되지 않은 영역을 사용하는 경우 오류가 발생합니다.
- S3 버킷을 생성할 때 정확한 지역 이름을 사용해야 합니다. 지역 이름은 대/소문자를 구분하며 2자 이상 32자 이하여야 합니다. 유효한 문자는 숫자, 문자 및 하이픈입니다.

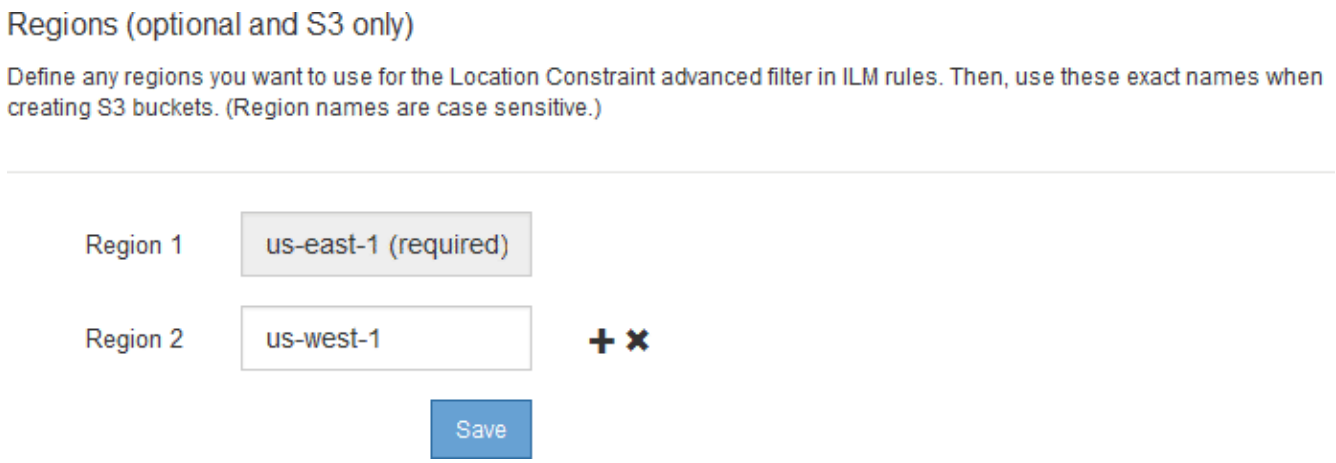
EU는 EU-West-1의 별칭으로 간주되지 않습니다. EU 또는 EU-West-1 지역을 사용하려면 정확한 이름을 사용해야 합니다.

- 현재 활성 ILM 정책 또는 제안된 ILM 정책 내에서 사용되고 있는 영역은 삭제하거나 수정할 수 없습니다.
- ILM 규칙에서 고급 필터로 사용되는 영역이 잘못된 경우에도 제안된 정책에 해당 규칙을 추가할 수 있습니다. 그러나 제안된 정책을 저장하거나 활성화하려고 하면 오류가 발생합니다. (ILM 규칙에서 영역을 고급 필터로 사용하지만 나중에 해당 영역을 삭제할 경우 또는 그리드 관리 API를 사용하여 규칙을 만들고 정의되지 않은 영역을 지정할 경우 잘못된 영역이 발생할 수 있습니다.)
- 영역을 사용하여 S3 버킷을 생성한 후 삭제하면 위치 제약 조건 고급 필터를 사용하여 해당 버킷에서 오브젝트를 찾으려면 영역을 다시 추가해야 합니다.

단계

1. ILM * > * 지역 * 을 선택합니다.

   현재 정의된 영역이 나열된 영역 페이지가 나타납니다. * 지역 1 * 은 기본 영역인 us-east-1(수정 또는 제거할 수 없음)을 표시합니다.

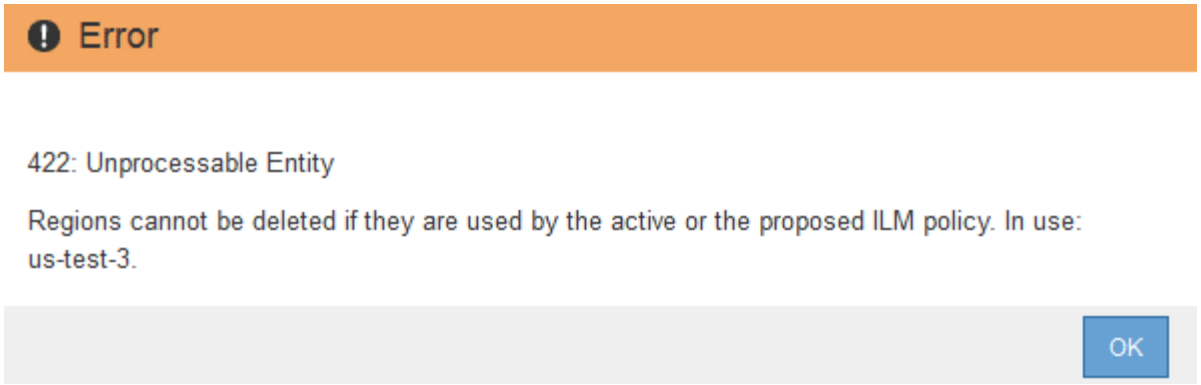
   

2. 영역을 추가하려면:
   a. 삽입 아이콘을 선택합니다 ✚ 마지막 항목 오른쪽에 있습니다.
   b. S3 버킷을 생성할 때 사용할 영역의 이름을 입력합니다.

      해당 S3 버킷을 생성할 때 이 정확한 영역 이름을 LocationConstraint 요청 요소로 사용해야 합니다.

3. 사용하지 않는 영역을 제거하려면 삭제 아이콘을 선택합니다 ✖.

   현재 활성 정책 또는 제안된 정책에서 사용 중인 지역을 제거하려고 하면 오류 메시지가 나타납니다.



4. 변경을 완료하면 * Save * 를 선택합니다.

   이제 ILM 규칙 만들기 마법사의 고급 필터링 페이지에 있는 * 위치 제약 조건 * 목록에서 이러한 영역을 선택할 수 있습니다. 을 참조하십시오ILM 규칙에서 고급 필터를 사용합니다.

ILM 규칙을 생성합니다

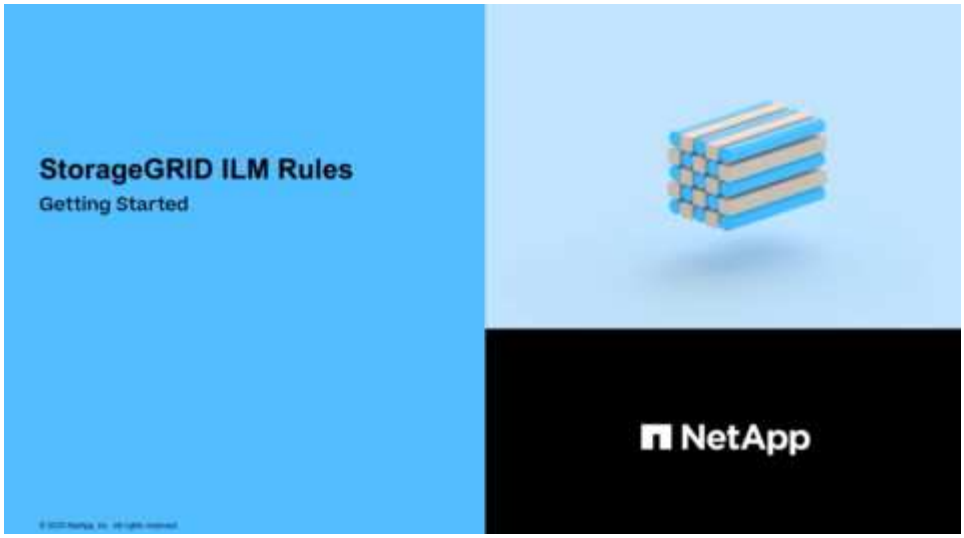
ILM 규칙 생성 마법사에 액세스합니다

ILM 규칙을 사용하여 시간에 따른 오브젝트 데이터 배치를 관리할 수 있습니다. ILM 규칙을 만들려면 ILM 규칙 만들기 마법사를 사용합니다.

> 정책에 대한 기본 ILM 규칙을 만드는 경우에는 대신 다음 절차를 사용하십시오. 기본 ILM 규칙을 생성합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- 이 규칙이 적용되는 테넌트 계정을 지정하려면 테넌트 계정 권한이 있거나 각 계정의 계정 ID를 알고 있어야 합니다.
- 규칙이 마지막 액세스 시간 메타데이터에서 오브젝트를 필터링하려면 S3 또는 Swift용 컨테이너에서 마지막 액세스 시간 업데이트를 활성화해야 합니다.
- 복제된 복사본을 생성하는 경우 사용할 스토리지 풀 또는 클라우드 스토리지 풀을 구성했습니다. 을 참조하십시오 스토리지 풀을 생성합니다 및 클라우드 스토리지 풀을 생성합니다.
- 삭제 코딩 복사본을 만드는 경우 삭제 코딩 프로필을 구성했습니다. 을 참조하십시오 삭제 코딩 프로필을 생성합니다.
- 에 익숙합니다 데이터 보호를 위한 수집 옵션.
- S3 오브젝트 잠금에 사용하기 위해 규정 준수 규칙을 만들어야 하는 경우 에 익숙한 것입니다 S3 오브젝트 잠금에 대한 요구사항.
- 선택적으로 비디오를 시청했습니다. "비디오: StorageGRID ILM 규칙: 시작하기".



이 작업에 대해

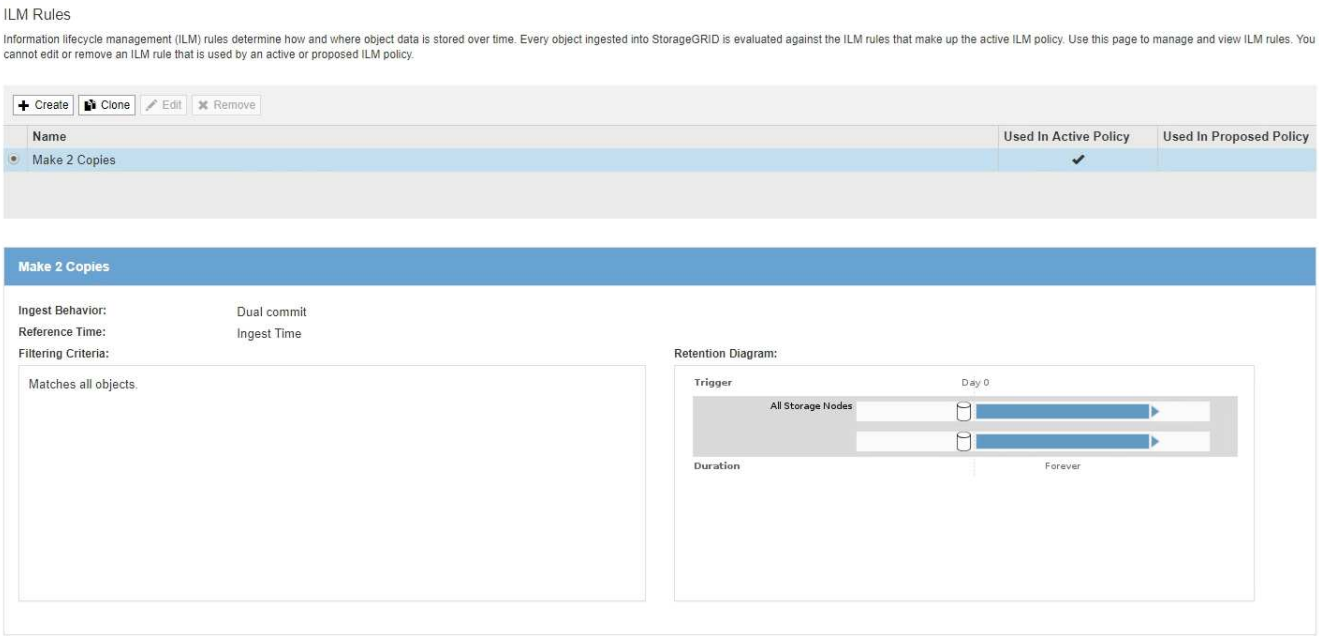
ILM 규칙 생성 시:

- StorageGRID 시스템의 토폴로지 및 스토리지 구성을 고려하십시오.
- 생성할 오브젝트 복사본 유형(복제 또는 삭제 코딩)과 필요한 각 오브젝트의 복사본 수를 고려하십시오.
- StorageGRID 시스템에 연결하는 응용 프로그램에서 사용되는 개체 메타데이터 유형을 확인합니다. ILM 규칙은 해당 메타데이터를 기반으로 개체를 필터링합니다.
- 시간에 따라 오브젝트 복사본을 배치할 위치를 고려합니다.
- 수집 시 데이터 보호 옵션에 사용할 옵션을 결정합니다(균형, 엄격 또는 이중 커밋).

단계

1. ILM * > * 규칙 * 을 선택합니다.

   재고 규칙과 함께 ILM 규칙 페이지가 나타나며 Make 2 Copies(2개 복사본 만들기) 가 선택됩니다.



> StorageGRID 시스템에서 전역 S3 개체 잠금 설정이 활성화된 경우 ILM 규칙 페이지가 약간 다르게 표시됩니다. 요약 테이블에는 * 규격 * 열이 포함되며 선택한 규칙에 대한 세부 정보에는 * 규격 * 필드가 포함됩니다.

2. Create * 를 선택합니다.

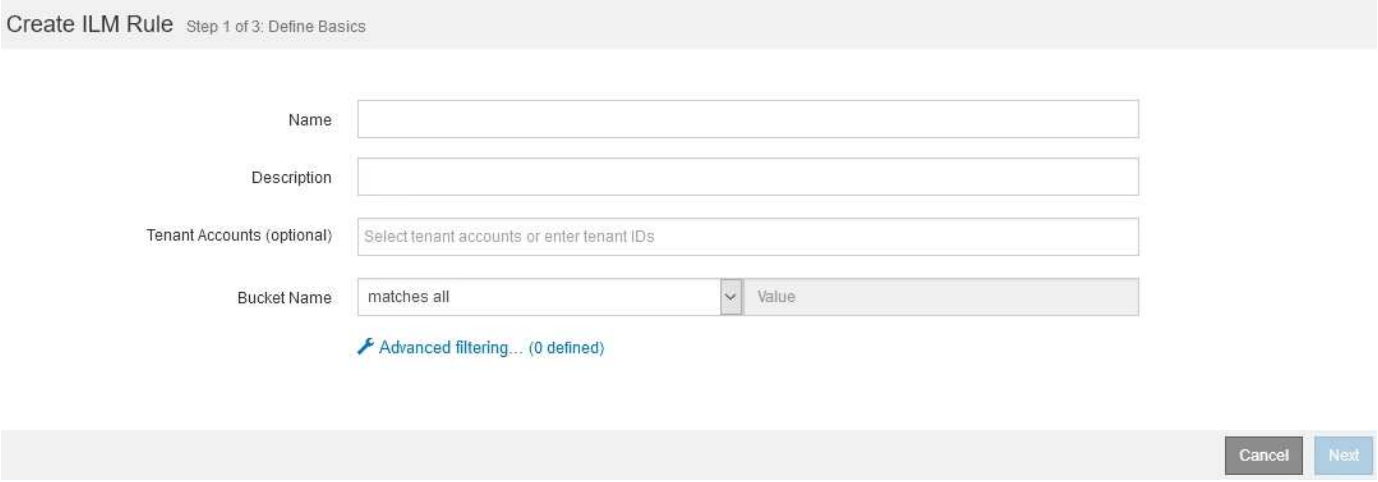
   ILM 규칙 생성 마법사의 1단계(기본 정의)가 나타납니다. 기본 사항 정의 페이지를 사용하여 규칙이 적용되는 개체를 정의합니다.

단계 **1/3:** 기본 사항 정의

ILM 규칙 만들기 마법사의 1단계(기본 정의)를 사용하여 규칙의 기본 및 고급 필터를 정의할 수 있습니다.

이 작업에 대해

ILM 규칙을 기준으로 개체를 평가할 때 StorageGRID은 개체 메타데이터를 규칙의 필터와 비교합니다. 개체 메타데이터가 모든 필터와 일치하면 StorageGRID는 규칙을 사용하여 개체를 배치합니다. 모든 개체에 적용할 규칙을 설계하거나 하나 이상의 테넌트 계정 또는 버킷 이름과 같은 기본 필터 또는 오브젝트의 크기나 사용자 메타데이터와 같은 고급 필터를 지정할 수 있습니다.



단계

1. 이름 * 필드에 규칙의 고유 이름을 입력합니다.

   1자에서 64자 사이여야 합니다.

2. 필요에 따라 * Description * (설명 *) 필드에 규칙에 대한 간단한 설명을 입력합니다.

   나중에 규칙을 인식할 수 있도록 규칙의 목적 또는 기능을 설명해야 합니다.

Name	Make 3 Copies
Description	Save 1 copy at 3 sites for 1 year. Then, save EC copy forever

3. 또는 이 규칙이 적용되는 하나 이상의 S3 또는 Swift 테넌트 계정을 선택합니다. 이 규칙이 모든 테넌트에 적용되는 경우 이 필드를 비워 둡니다.

루트 액세스 권한이나 테넌트 계정 권한이 없으면 목록에서 테넌트를 선택할 수 없습니다. 대신 테넌트 ID를 입력하거나 쉼표로 구분된 문자열로 여러 ID를 입력합니다.

4. 이 규칙이 적용되는 S3 버킷 또는 Swift 컨테이너를 선택적으로 지정합니다.

   Matches All * (모두 일치 *)을 선택한 경우(기본값) 규칙은 모든 S3 버킷 또는 Swift 컨테이너에 적용됩니다.

5. 선택적으로 * 고급 필터링 * 을 선택하여 추가 필터를 지정합니다.

   고급 필터링을 구성하지 않으면 기본 필터와 일치하는 모든 개체에 규칙이 적용됩니다.

   이 규칙이 삭제 코딩 복사본을 만드는 경우 * 개체 크기(MB) * 고급 필터를 추가하고 1 * 보다 큼 * 으로 설정합니다. 크기 필터는 1MB 이하의 오브젝트가 삭제 코딩되지 않도록 합니다.

   > 삭제 코딩은 1MB 이상의 오브젝트에 가장 적합합니다. 매우 작은 삭제 코딩 조각을 관리해야 하는 오버헤드를 방지하기 위해 200KB 미만의 오브젝트에 삭제 코딩을 사용하지 마십시오.

6. 다음 * 을 선택합니다.

   2단계(배치 정의)가 나타납니다.

관련 정보

- ILM 규칙이란 무엇입니까
- ILM 규칙에서 고급 필터를 사용합니다
- 단계 2/3: 배치 정의

ILM 규칙에서 고급 필터를 사용합니다

고급 필터링을 사용하면 메타데이터 기반의 특정 개체에만 적용되는 ILM 규칙을 만들 수 있습니다. 규칙에 대한 고급 필터링을 설정할 때 일치시킬 메타데이터 유형을 선택하고 연산자를 선택한 다음 메타데이터 값을 지정합니다. 개체가 평가되면 고급 필터와 일치하는 메타데이터가 있는 개체에만 ILM 규칙이 적용됩니다.

이 표에는 고급 필터에 지정할 수 있는 메타데이터 유형, 각 메타데이터 유형에 사용할 수 있는 연산자 및 필요한 메타데이터 값이 나와 있습니다.

메타데이터 유형입니다	지원되는 연산자	메타데이터 값입니다
수집 시간(마이크로초)	• 같음 • 같지 않습니다 • 보다 작음 • 보다 작음 또는 같음 • 보다 큼 • 크거나 같음	객체가 수집된 시간 및 날짜입니다. • 참고: * 새 ILM 정책을 활성화할 때 리소스 문제를 방지하려면 많은 수의 기존 오브젝트의 위치를 변경할 수 있는 모든 규칙에서 Ingest Time 고급 필터를 사용할 수 있습니다. 기존 개체가 불필요하게 이동되지 않도록 새 정책이 적용되는 대략적인 시간과 같거나 큰 수집 시간을 설정합니다.

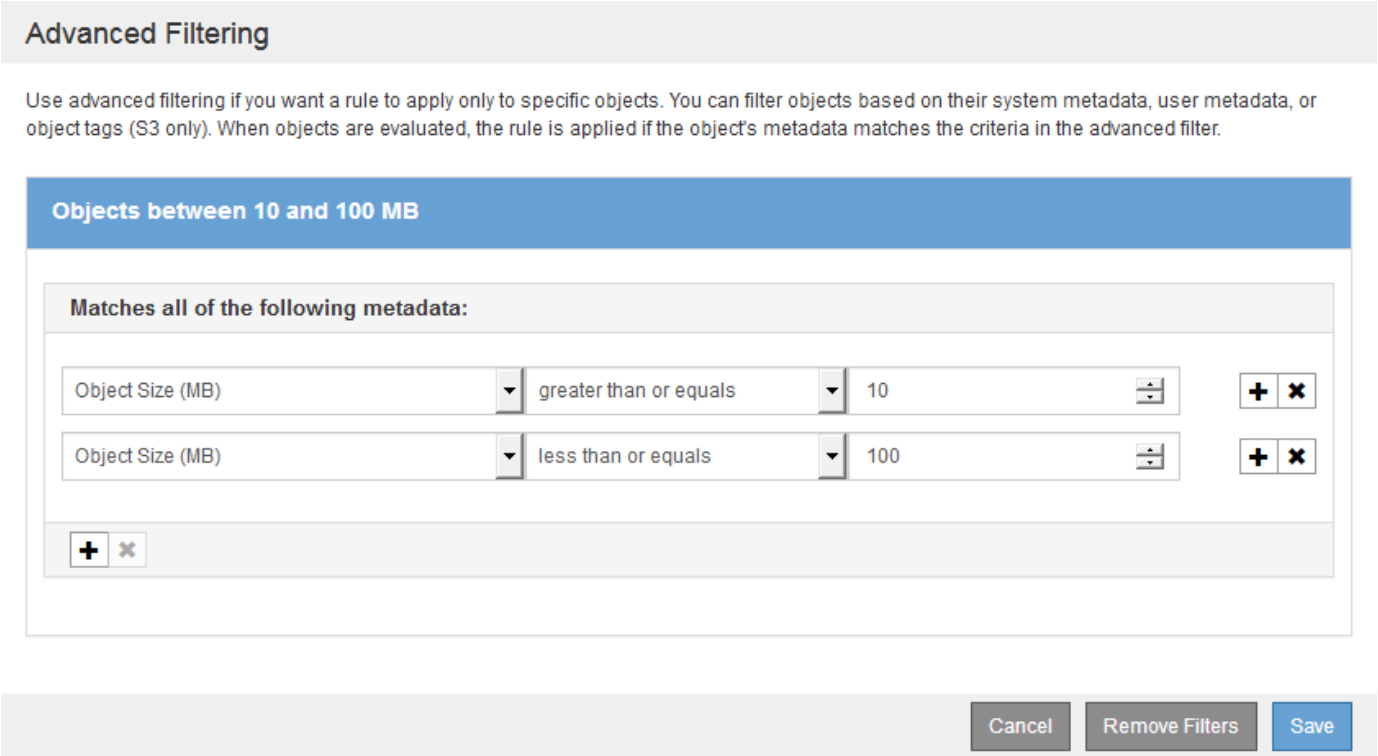
메타데이터 유형입니다	지원되는 연산자	메타데이터 값입니다
키	• 같음 • 같지 않습니다 • 포함 • 포함하지 않음 • 로 시작합니다 • 로 시작하지 않습니다 • 로 끝납니다 • 로 끝나지는 않습니다	고유한 S3 또는 Swift 오브젝트 키의 전체 또는 일부. 예를 들어, '.txt'로 끝나는 개체를 일치시키거나 'test-object/'로 시작할 수 있습니다.
마지막 액세스 시간(마이크로초)	• 같음 • 같지 않습니다 • 보다 작음 • 보다 작음 또는 같음 • 보다 큼 • 크거나 같음 • 있습니다 • 존재하지 않습니다	개체를 마지막으로 검색한 시간 및 날짜(읽기 또는 보기). • 참고: * 마지막 액세스 시간을 고급 필터로 사용하려면 S3 버킷 또는 Swift 컨테이너에 대해 마지막 액세스 시간 업데이트를 활성화해야 합니다. ILM 규칙에서 마지막 액세스 시간을 사용합니다
위치 제약 조건(S3만 해당)	• 같음 • 같지 않습니다	S3 버킷을 생성한 영역입니다. ILM * > * 지역 * 을 사용하여 표시된 영역을 정의합니다. • 참고: * us-east-1의 값은 us-east-1 지역에서 생성된 버킷의 오브젝트와 지정된 영역이 없는 버킷의 오브젝트와 일치합니다. 영역 구성(옵션 및 S3만 해당)
개체 크기(MB)	• 같음 • 등가 아님 • 보다 작음 • 보다 작음 또는 같음 • 보다 큼 • 크거나 같음	개체 크기(MB)입니다. 삭제 코딩은 1MB 이상의 오브젝트에 가장 적합합니다. 매우 작은 삭제 코딩 조각을 관리해야 하는 오버헤드를 방지하기 위해 200KB 미만의 오브젝트에 삭제 코딩을 사용하지 마십시오. • 참고: * 1MB보다 작은 개체 크기를 필터링하려면 10진수 값을 입력합니다. 브라우저 종류 및 로캘 설정은 마침표를 소수 구분 기호로 사용할지 아니면 쉼표를 사용할지 여부를 제어합니다.

메타데이터 유형입니다	지원되는 연산자	메타데이터 값입니다
사용자 메타데이터	• 포함 • 로 끝납니다 • 같음 • 있습니다 • 포함하지 않음 • 로 끝나지는 않습니다 • 같지 않습니다 • 존재하지 않습니다 • 로 시작하지 않습니다 • 로 시작합니다	키 값 쌍. 여기서 * 사용자 메타데이터 이름 * 은 키이고 * 사용자 메타데이터 값 * 은 값입니다. 예를 들어, 사용자 메타데이터가 'color=blue'인 객체를 필터링하려면 * 사용자 메타데이터 이름 * 에 대해 'color'를, 연산자에 대해서는 'equals'를, * 사용자 메타데이터 값 * 에 대해서는 'blue'를 지정합니다. • 참고: * 사용자 메타데이터 이름은 대/소문자를 구분하지 않으며 사용자 메타데이터 값은 대/소문자를 구분합니다.
오브젝트 태그(S3만 해당)	• 포함 • 로 끝납니다 • 같음 • 있습니다 • 포함하지 않음 • 로 끝나지는 않습니다 • 같지 않습니다 • 존재하지 않습니다 • 로 시작하지 않습니다 • 로 시작합니다	키 값 쌍. 여기서 * 개체 태그 이름 * 은 키이고 * 개체 태그 값 * 은 값입니다. 예를 들어, 개체 태그가 "Image=True"인 개체를 필터링하려면 * 개체 태그 이름 * 에 대해 "Image"를 지정하고 연산자에 대해 "equals"를 지정하고 * 개체 태그 값 * 에 대해 "True"를 지정합니다. • 참고: * 개체 태그 이름 및 개체 태그 값은 대/소문자를 구분합니다. 이러한 항목은 개체에 대해 정의된 대로 정확하게 입력해야 합니다.

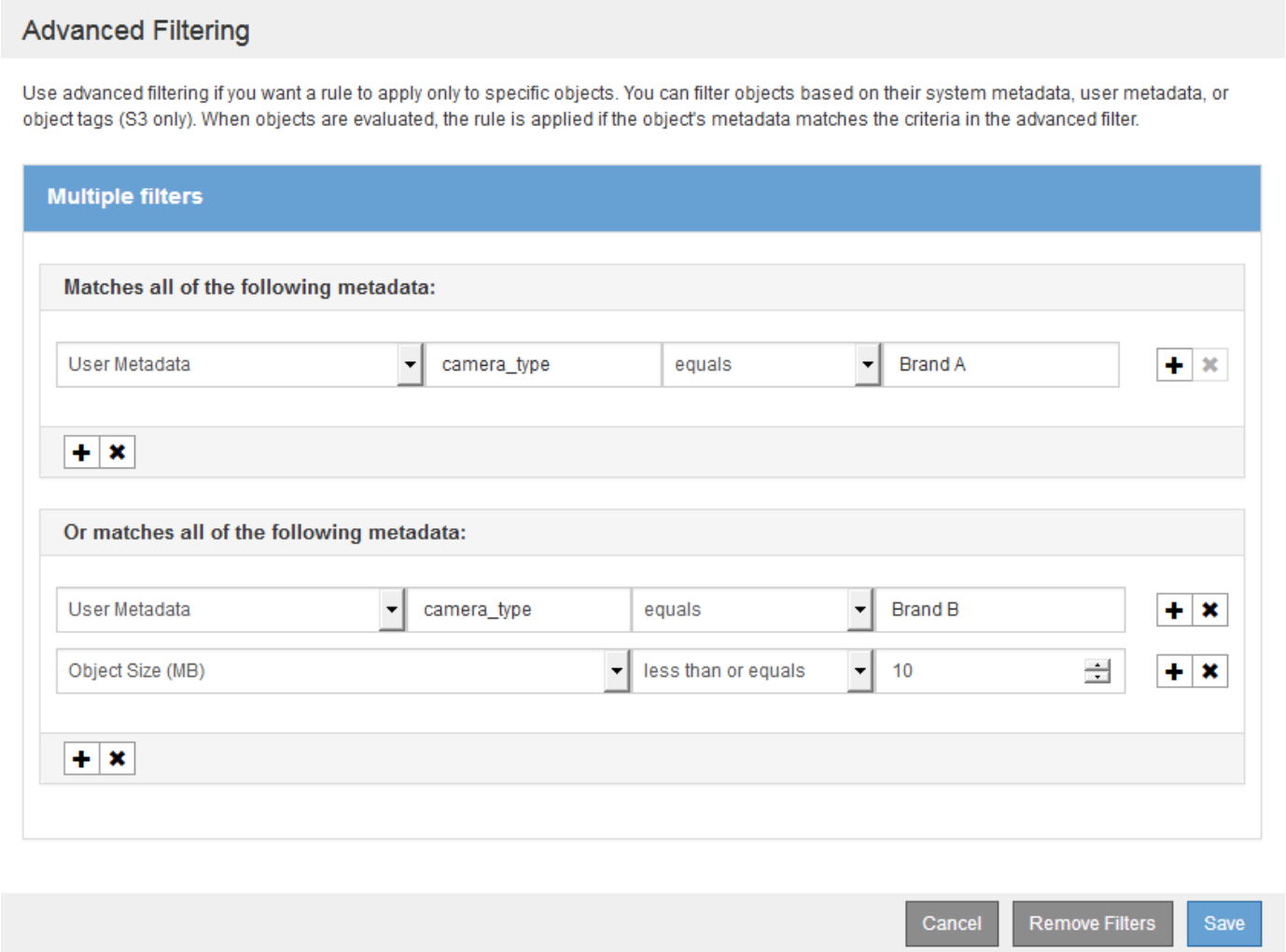
여러 메타데이터 형식 및 값 지정

고급 필터링을 정의할 때 여러 유형의 메타데이터와 여러 메타데이터 값을 지정할 수 있습니다. 예를 들어 규칙이 10MB에서 100MB 사이의 객체와 일치하게 하려면 * 개체 크기 * 메타데이터 유형을 선택하고 두 개의 메타데이터 값을 지정합니다.

- 첫 번째 메타데이터 값은 10MB보다 크거나 같은 객체를 지정합니다.
- 두 번째 메타데이터 값은 100MB 이하의 객체를 지정합니다.



여러 항목을 사용하면 일치하는 개체를 정밀하게 제어할 수 있습니다. 다음 예제에서 규칙은 Brand A 또는 Brand B가 camera_type 사용자 메타데이터의 값으로 설정된 개체에 적용됩니다. 그러나 이 규칙은 10MB보다 작은 브랜드 B 객체에만 적용됩니다.



단계 **2/3:** 배치 정의

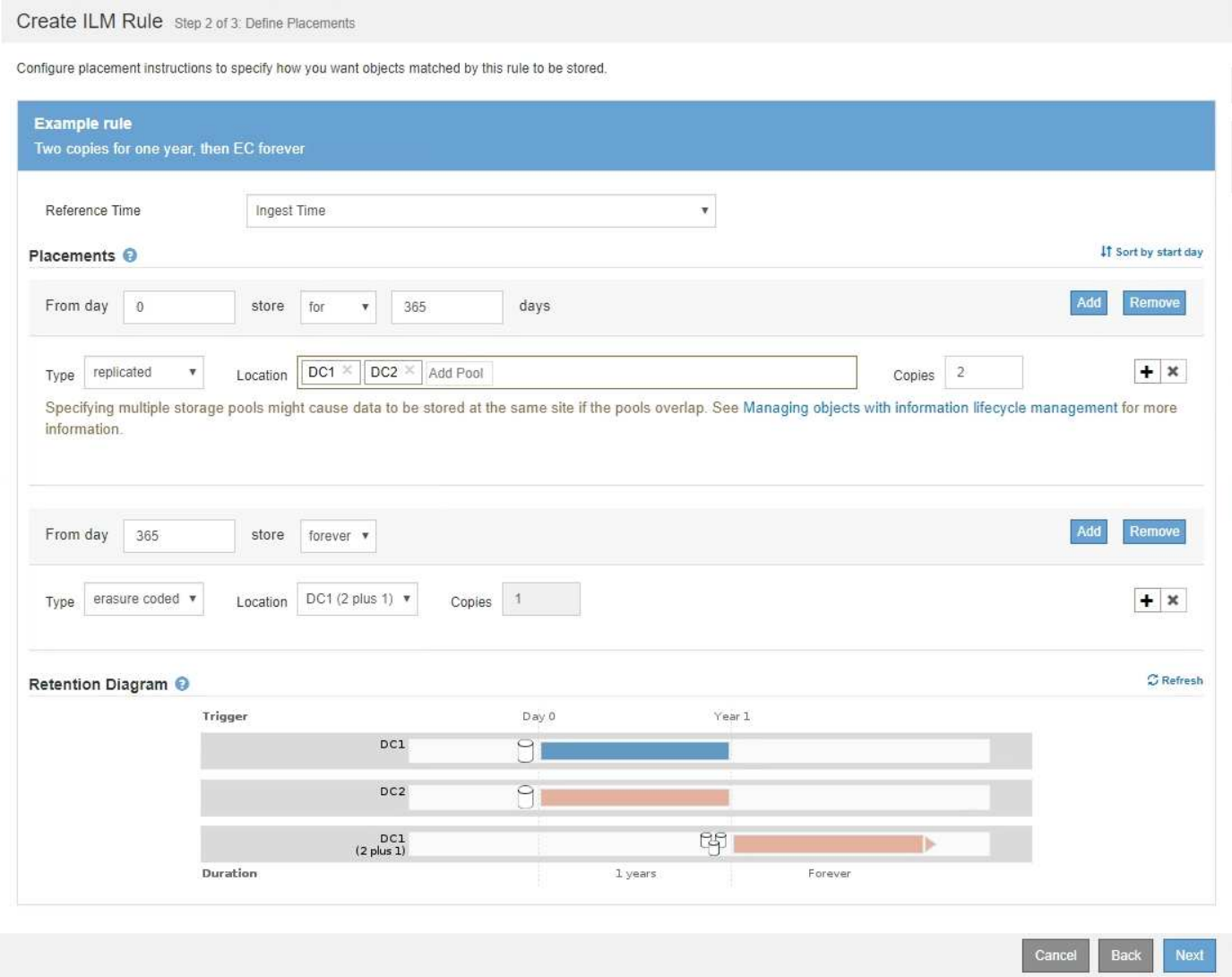
ILM 규칙 생성 마법사의 2단계(배치 정의)를 통해 개체 저장 기간, 복사본 유형(복제되거나 삭제 코딩), 스토리지 위치 및 복사본 수를 결정하는 배치 지침을 정의할 수 있습니다.

이 작업에 대해

ILM 규칙에는 하나 이상의 배치 지침이 포함될 수 있습니다. 각 배치 지침은 단일 기간에 적용됩니다. 두 개 이상의 명령을 사용하는 경우 기간은 연속적이어야 하며, 적어도 하나의 명령은 0일째부터 시작해야 합니다. 지침은 계속 진행할 수 있으며, 더 이상 오브젝트 복사본이 필요하지 않을 때까지 계속됩니다.

다른 유형의 사본을 만들거나 해당 기간 동안 다른 위치를 사용하려는 경우 각 배치 지침에는 여러 줄이 있을 수 있습니다.

이 ILM 규칙 예에서는 첫 해에 두 개의 복제된 복사본을 만듭니다. 각 복제본은 다른 사이트의 스토리지 풀에 저장됩니다. 1년 후에는 2+1 삭제 코딩 복사본을 만들어 하나의 사이트에만 저장합니다.



단계

1. 참조 시간 * 에서 배치 지침의 시작 시간을 계산할 때 사용할 시간 유형을 선택합니다.

옵션을 선택합니다	설명
수집 시간	객체가 수집된 시간입니다.
마지막 액세스 시간입니다	개체를 마지막으로 검색한 시간(읽기 또는 보기) • 참고: * 이 옵션을 사용하려면 S3 버킷 또는 Swift 컨테이너에 대해 마지막 액세스 시간에 대한 업데이트를 활성화해야 합니다. 을 참조하십시오 ILM 규칙에서 마지막 액세스 시간을 사용합니다.

옵션을 선택합니다	설명
현재 시간이 아닙니다	새 버전이 수집되어 현재 버전으로 대체되었기 때문에 개체 버전이 최신 버전이 아닌 시간입니다. • 참고: * 비현재 시간은 버전 관리가 활성화된 버킷의 S3 오브젝트에만 적용됩니다. 이 옵션을 사용하면 버전이 아닌 개체 버전을 필터링하여 버전이 지정된 개체의 스토리지 영향을 줄일 수 있습니다. 을 참조하십시오 예 4: S3 버전 오브젝트에 대한 ILM 규칙 및 정책.
사용자 정의 생성 시간입니다	사용자 정의 메타데이터에 지정된 시간입니다.

호환 규칙을 만들려면 * Ingest Time * 을 선택해야 합니다.

2. Placements * 섹션에서 시작 시간과 첫 번째 기간의 기간을 선택합니다.

   예를 들어 첫 해의 개체를 저장할 위치를 지정할 수 있습니다("365일의 경우 0일"). 적어도 하나의 명령은 0일에 시작해야 합니다.

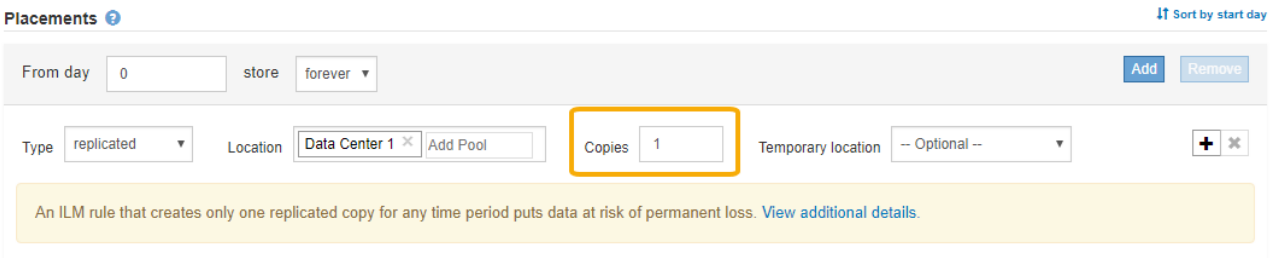
3. 복제된 복사본을 생성하려면 다음을 수행합니다.
   a. Type * 드롭다운 목록에서 * replicated * 를 선택합니다.
   b. Location * 필드에서 추가하려는 각 스토리지 풀에 대해 * Add Pool * 을 선택합니다.
      - 스토리지 풀을 하나만 지정하는 경우 * StorageGRID는 지정된 스토리지 노드에 복제된 객체 복사본을 하나만 저장할 수 있습니다. 그리드에 스토리지 노드 3개가 포함된 경우 복제본 수로 4를 선택하면 각 스토리지 노드에 대해 복제본 3개만 만들어집니다.

        ILM 규칙을 완전히 적용할 수 없음을 나타내기 위해 * ILM 배치 달성 안 됨 * 경고가 트리거됩니다.

      - 둘 이상의 스토리지 풀을 지정하는 경우 * 다음 규칙을 염두에 두십시오.
        - 복제본 수는 스토리지 풀 수보다 클 수 없습니다.
        - 복제본 수가 스토리지 풀 수와 같으면 객체 복제본 하나가 각 스토리지 풀에 저장됩니다.
        - 복제본 수가 스토리지 풀 수보다 적은 경우 하나의 복제본이 수집 사이트에 저장된 다음 나머지 복제본을 분산하여 풀 간에 디스크 사용량을 균형 있게 유지하는 한편, 어느 사이트에서든 객체의 복제본을 두 개 이상 확보하지 못하도록 합니다.
        - 스토리지 풀이 겹칠 경우(동일한 스토리지 노드 포함) 개체의 모든 복제본이 하나의 사이트에만 저장될 수 있습니다. 따라서 기본 모든 스토리지 노드 스토리지 풀 및 다른 스토리지 풀을 지정하지 마십시오.

c. 복사할 매수를 선택합니다.

매수를 1로 변경하면 경고가 나타납니다. 특정 기간 동안 복제된 복사본을 하나만 생성하는 ILM 규칙은 데이터가 영구적으로 손실될 위험이 있습니다. 을 참조하십시오 단일 복사본 복제를 사용하지 않아야 하는 이유.



이러한 위험을 방지하려면 다음 중 하나 이상을 수행하십시오.

- 해당 기간의 사본 수를 늘립니다.
- 더하기 기호 아이콘을 선택합니다 ✚ 를 눌러 해당 기간 동안 추가 사본을 생성합니다. 그런 다음 다른 스토리지 풀 또는 클라우드 스토리지 풀을 선택합니다.
- 유형 에 대해 * 복제된 * 대신 * 삭제 코딩 * 을 선택합니다. 이 규칙이 모든 기간에 대해 여러 복사본을 이미 생성한 경우 이 경고를 무시해도 됩니다.

d. 스토리지 풀을 하나만 지정한 경우에는 * 임시 위치 * 필드를 무시하십시오.

> ⓘ 임시 위치는 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다. 을 참조하십시오 스토리지 풀을 임시 위치로 사용(더 이상 사용 안 함).

4. 삭제 코딩 복사본을 만들려면:

a. 유형 * 드롭다운 목록에서 * 삭제 코딩 * 을 선택합니다.

인쇄 매수가 1로 변경됩니다. 규칙에 200KB 이하의 객체를 무시하는 고급 필터가 없는 경우 경고가 표시됩니다.

> Erasure coding is best suited for objects greater than 1 MB. Do not use erasure coding for objects that are 200 KB or smaller. Select **Back** to return to Step 1. Then, use **Advanced filtering** to set the Object Size (MB) filter to any value greater than 0.2.

> ⓘ 삭제 코딩은 1MB 이상의 오브젝트에 가장 적합합니다. 매우 작은 삭제 코딩 조각을 관리해야 하는 오버헤드를 방지하기 위해 200KB 미만의 오브젝트에 삭제 코딩을 사용하지 마십시오.

b. 개체 크기 경고가 나타나면 * Back * 을 선택하여 1단계로 돌아갑니다. 그런 다음 * 고급 필터링 * 을 선택하고 개체 크기(MB) 필터를 0.2보다 큰 값으로 설정합니다.

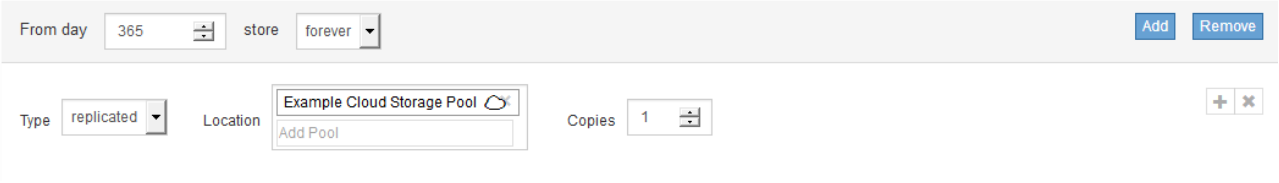
c. 저장 위치를 선택합니다.

삭제 코딩 복사본의 스토리지 위치에는 스토리지 풀의 이름, 삭제 코딩 프로필 이름이 포함됩니다.

5. 필요에 따라 다른 기간을 추가하거나 다른 위치에 추가 사본을 생성할 수 있습니다.
   - 더하기 아이콘을 선택하여 동일한 기간 동안 다른 위치에 추가 사본을 생성합니다.
   - 배치 지침에 다른 기간을 추가하려면 * 추가 * 를 선택합니다.

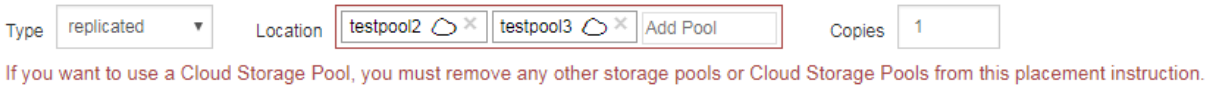
> 최종 기간이 * Forever * 로 끝나는 경우를 제외하고 최종 기간 종료 시 객체가 자동으로 삭제됩니다.

6. 클라우드 스토리지 풀에 오브젝트를 저장하려면 다음을 수행합니다.
   a. Type * 드롭다운 목록에서 * replicated * 를 선택합니다.
   b. Location * 필드에서 * Add Pool * 을 선택합니다. 그런 다음 클라우드 스토리지 풀을 선택합니다.

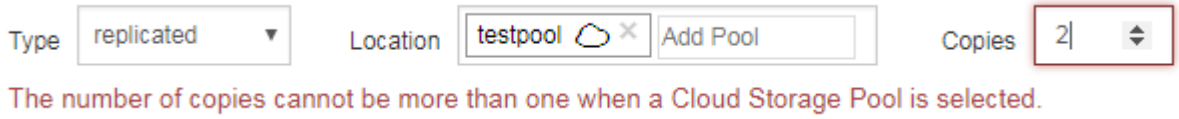


클라우드 스토리지 풀을 사용할 때는 다음 규칙을 염두에 두십시오.

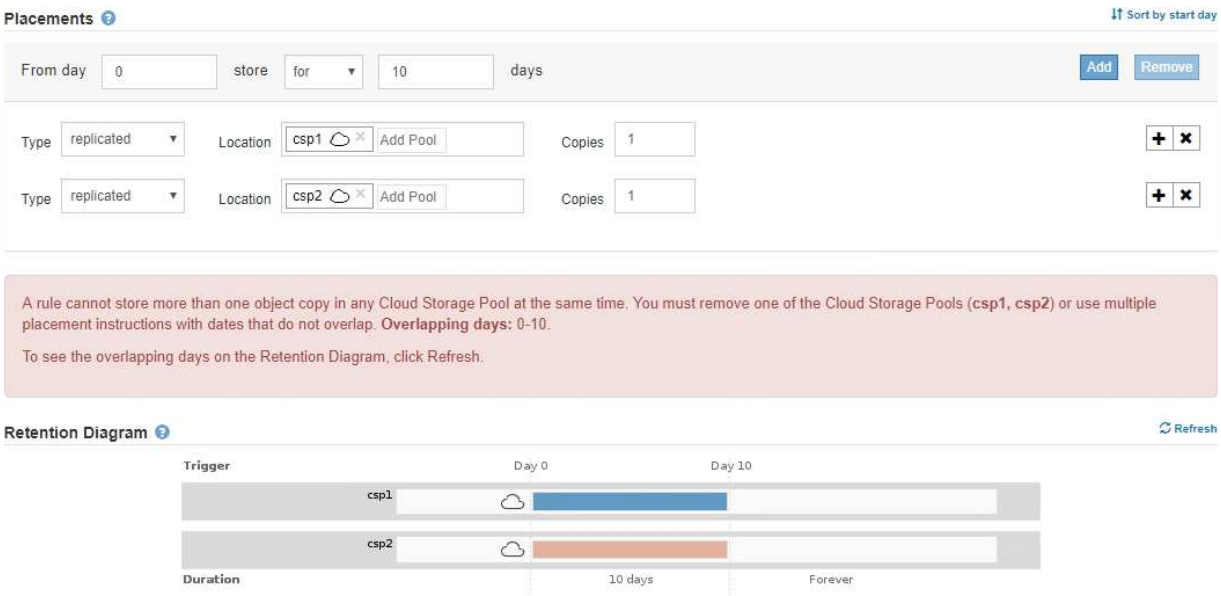
- 단일 배치 지침에서는 여러 클라우드 스토리지 풀을 선택할 수 없습니다. 마찬가지로, 동일한 배치 지침에서는 클라우드 스토리지 풀과 스토리지 풀을 선택할 수 없습니다.



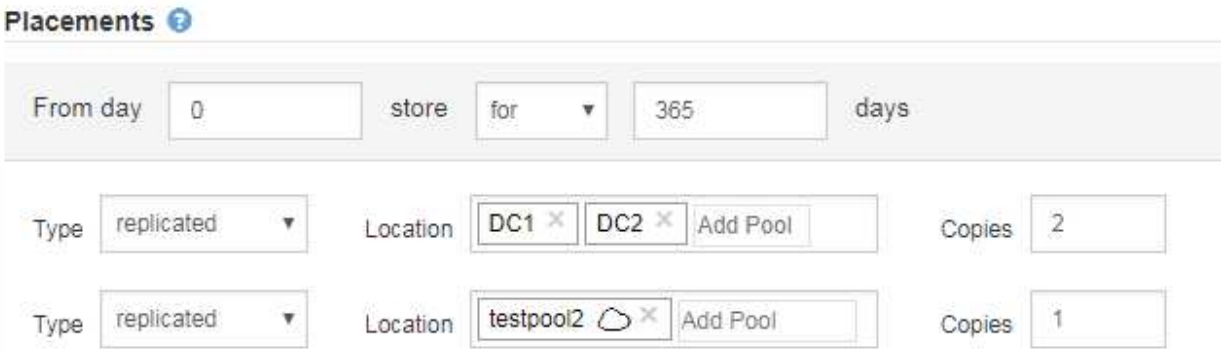
- 특정 Cloud Storage Pool에서는 오브젝트 복사본을 하나만 저장할 수 있습니다. Copies * 를 2개 이상으로 설정하면 오류 메시지가 나타납니다.



- 클라우드 스토리지 풀에 동시에 둘 이상의 오브젝트 복사본을 저장할 수 없습니다. Cloud Storage Pool을 사용하는 여러 배치에서 날짜가 중복되거나 같은 배치의 여러 라인이 Cloud Storage Pool을 사용하는 경우 오류 메시지가 나타납니다.



- StorageGRID에서 오브젝트를 복제 또는 삭제 코딩 복사본으로 저장하는 동시에 클라우드 스토리지 풀에 오브젝트를 저장할 수 있습니다. 그러나 이 예제에서 볼 수 있듯이, 각 위치에 대한 사본의 수와 유형을 지정할 수 있도록 해당 기간의 배치 지침에 두 줄 이상을 포함해야 합니다.

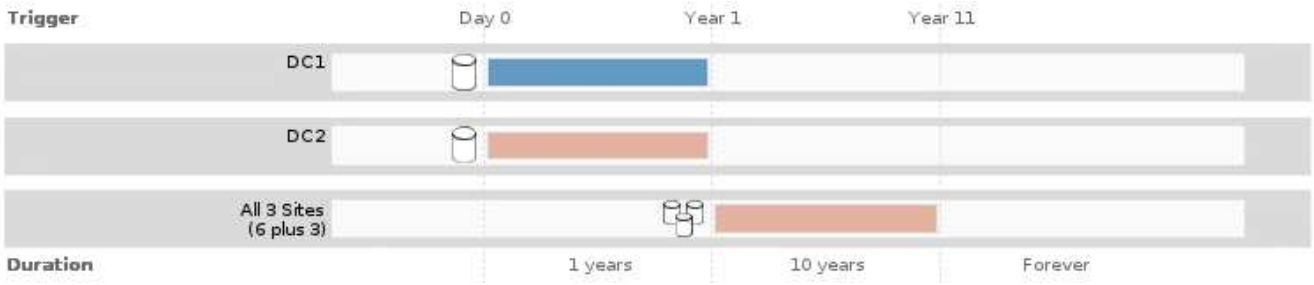


7. 보존 다이어그램을 업데이트하고 배치 지침을 확인하려면 * Refresh * 를 선택합니다.

   다이어그램의 각 줄은 개체 복사본을 배치할 위치와 시기를 보여 줍니다. 복사 유형은 다음 아이콘 중 하나로 표시됩니다.

	복제된 복사본입니다
	삭제 코딩 복사본
	Cloud Storage Pool 복사본

   이 예에서는 복제된 복사본 2개가 1년 동안 2개의 스토리지 풀(DC1 및 DC2)에 저장됩니다. 그런 다음, 삭제 코딩 복사본을 3개의 사이트에서 6+3 삭제 코딩 체계를 사용하여 10년 더 절약할 수 있습니다. 11년이 지나면 StorageGRID에서 객체가 삭제됩니다.



8. 다음 * 을 선택합니다.

   3단계(Ingest 동작 정의)가 나타납니다.

관련 정보

- ILM 규칙이란 무엇입니까
- S3 오브젝트 잠금으로 오브젝트 관리
- 3단계 중 3단계: 수집 동작 정의

ILM 규칙에서 마지막 액세스 시간을 사용합니다

ILM 규칙에서 마지막 액세스 시간을 참조 시간으로 사용할 수 있습니다. 예를 들어, 최근 3개월 동안 표시된 객체를 로컬 스토리지 노드에 그대로 두고, 최근에 외부 위치로 표시되지 않은 객체를 이동할 수 있습니다. ILM 규칙을 특정 날짜에 마지막으로 액세스한 개체에만 적용하려면 마지막 액세스 시간을 고급 필터로 사용할 수도 있습니다.

이 작업에 대해

ILM 규칙에서 마지막 액세스 시간을 사용하기 전에 다음 고려 사항을 검토하십시오.

- 마지막 액세스 시간을 참조 시간으로 사용하는 경우 개체에 대한 마지막 액세스 시간을 변경해도 즉각적인 ILM 평가가 트리거되지 않습니다. 그 대신, 개체의 배치를 평가하고 배경 ILM이 개체를 평가할 때 필요에 따라 개체를 이동합니다. 개체에 액세스한 후 2주 이상이 걸릴 수 있습니다.

  마지막 액세스 시간을 기반으로 ILM 규칙을 생성할 때 이 지연 시간을 고려하고 짧은 기간(1개월 미만)을 사용하는 배치를 피하십시오.

- 마지막 액세스 시간을 고급 필터 또는 참조 시간으로 사용하는 경우 S3 버킷에 대한 마지막 액세스 시간 업데이트를 활성화해야 합니다. 테넌트 관리자 또는 테넌트 관리 API를 사용할 수 있습니다.

> ⓘ 마지막 액세스 시간 업데이트는 항상 Swift 컨테이너에 대해 활성화되지만 S3 버킷에 대해서는 기본적으로 비활성화됩니다.

> ⓘ 마지막 액세스 시간 업데이트를 사용하면 특히 개체가 작은 시스템에서 성능이 저하될 수 있습니다. 개체가 검색될 때마다 StorageGRID에서 새 타임스탬프로 개체를 업데이트해야 하므로 성능에 미치는 영향이 발생합니다.

다음 표에는 버킷의 모든 오브젝트에 대해 서로 다른 유형의 요청에 대해 마지막 액세스 시간이 업데이트되었는지 여부가 요약되어 있습니다.

요청 유형입니다	마지막 액세스 시간 업데이트가 비활성화되었을 때 마지막 액세스 시간을 업데이트할지 여부를 나타냅니다	마지막 액세스 시간 업데이트를 사용할 때 마지막 액세스 시간을 업데이트할지 여부를 나타냅니다
개체, 해당 액세스 제어 목록 또는 해당 메타데이터를 검색하는 요청입니다	아니요	예
개체의 메타데이터를 업데이트하도록 요청합니다	예	예
한 버킷에서 다른 버킷으로 오브젝트 복사 요청	• 아니요, 소스 복제본입니다 • 예, 대상 복사본에 대해 입니다	• 예. 소스 복제본에 대해 가능합니다 • 예, 대상 복사본에 대해 입니다
여러 부분 업로드를 완료하도록 요청합니다	예. 조립된 개체에 대해 가능합니다	예. 조립된 개체에 대해 가능합니다

관련 정보

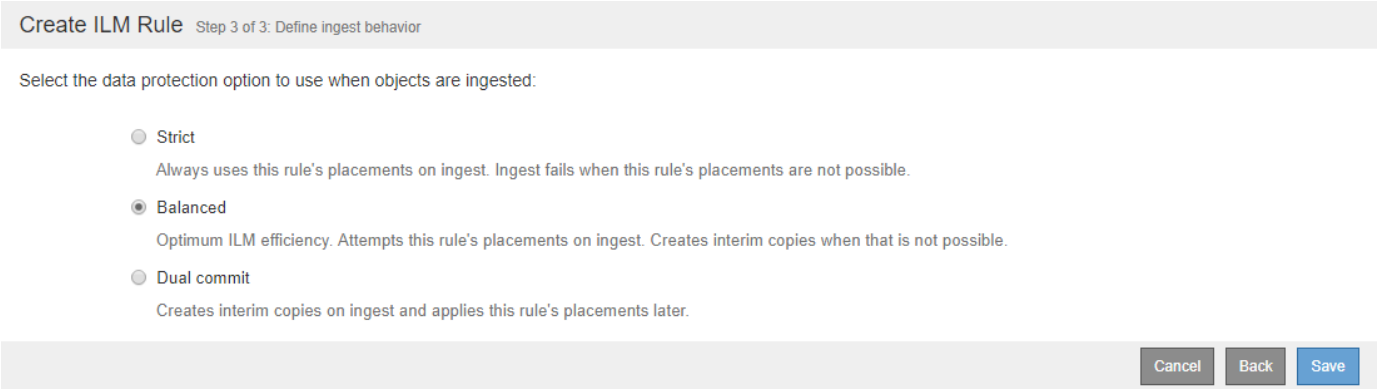
- S3을 사용합니다
- 테넌트 계정을 사용합니다

3단계 중 **3**단계**:** 수집 동작 정의

ILM 규칙 생성 마법사의 3단계(수집 동작 정의)를 사용하면 이 규칙으로 필터링되는 개체가 수집될 때 보호되는 방법을 선택할 수 있습니다.

이 작업에 대해

StorageGRID는 나중에 ILM 평가를 위해 임시 복사본을 만들고 개체를 대기열에 지정하거나 규칙의 배치 지침을 즉시 충족하도록 복사본을 만들 수 있습니다.



단계

1. 오브젝트가 수집될 때 사용할 데이터 보호 옵션을 선택합니다.

옵션을 선택합니다	설명
엄격한	수집 시 항상 이 규칙의 배치를 사용합니다. 이 규칙의 배치를 사용할 수 없는 경우 인제스트가 실패합니다.
균형	최적의 ILM 효율성 수집 시 이 규칙의 배치를 시도합니다. 가능하지 않은 경우 임시 사본을 생성합니다.
이중 커밋	수집 시 중간 복사본을 생성하고 이 규칙의 배치를 나중에 적용합니다.

Balanced는 대부분의 경우에 적합한 데이터 보안과 효율성을 함께 제공합니다. 엄격한 커밋 또는 이중 커밋은 일반적으로 특정 요구 사항을 충족하는 데 사용됩니다.

을 참조하십시오 데이터 보호를 위한 수집 옵션 및 데이터 보호 옵션의 장점, 단점 및 제한 를 참조하십시오.

> Strict 또는 Balanced 옵션을 선택하고 규칙에서 다음 배치 중 하나를 사용하는 경우 오류 메시지가 나타납니다.
>
> - 0일의 클라우드 스토리지 풀
> - 0일의 아카이브 노드
> - 규칙이 사용자 정의 생성 시간을 참조 시간으로 사용하는 경우 클라우드 스토리지 풀 또는 아카이브 노드

2. 저장 * 을 선택합니다.

   ILM 규칙이 저장됩니다. ILM 정책에 추가되고 정책이 활성화될 때까지 규칙이 활성 상태가 되지 않습니다.

관련 정보

- 예 5: 엄격한 수집 동작을 위한 ILM 규칙 및 정책
- ILM 정책을 생성합니다

기본 **ILM** 규칙을 생성합니다

ILM 정책을 만들기 전에 정책의 다른 규칙과 일치하지 않는 개체를 배치하기 위한 기본 규칙을 만들어야 합니다. 기본 규칙에서는 필터를 사용할 수 없습니다. 모든 테넌트, 모든 버킷 및 모든 오브젝트 버전에 적용되어야 합니다.

필요한 것

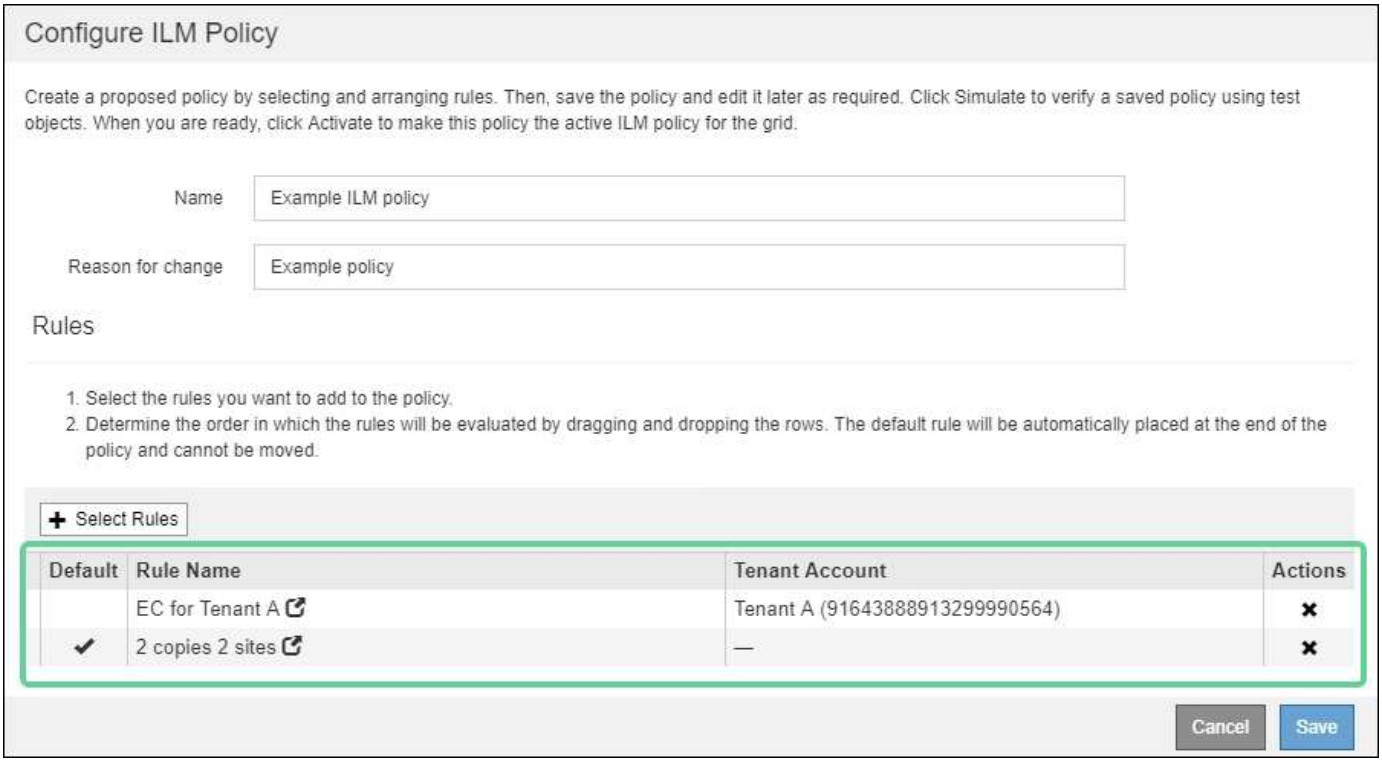
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

기본 규칙은 ILM 정책에서 평가할 마지막 규칙이므로 필터 또는 비현재 참조 시간을 사용할 수 없습니다. 기본 규칙의 배치 지침은 정책의 다른 규칙과 일치하지 않는 모든 개체에 적용됩니다.

이 예제 정책에서 첫 번째 규칙은 테넌트 A에 속하는 객체에만 적용됩니다 마지막 기본 규칙은 다른 모든 테넌트 계정에

속한 개체에 적용됩니다.



기본 규칙을 만들 때 다음 요구 사항을 염두에 두십시오.

- 기본 규칙은 정책의 마지막 규칙으로 자동 설정됩니다.
- 기본 규칙에서는 기본 필터 또는 고급 필터를 사용할 수 없습니다.
- 기본 규칙은 모든 개체 버전에 적용되어야 하므로 비현재 시간 참조 시간을 사용할 수 없습니다.
- 기본 규칙은 복제된 복사본을 만들어야 합니다.

> 삭제 코딩 복사본을 정책의 기본 규칙으로 만드는 규칙을 사용하지 마십시오. 삭제 코딩 규칙은 더 작은 오브젝트가 삭제 코딩되지 않도록 고급 필터를 사용해야 합니다.

- 일반적으로 기본 규칙은 개체를 영구적으로 유지해야 합니다.
- 전역 S3 오브젝트 잠금 설정을 사용(또는 사용하려는 경우)하는 경우 활성 또는 제안된 정책의 기본 규칙이 호환되어야 합니다.

단계

1. ILM * > * 규칙 * 을 선택합니다.

   ILM 규칙 페이지가 나타납니다.

2. Create * 를 선택합니다.

   ILM 규칙 생성 마법사의 1단계(기본 정의)가 나타납니다.

3. 이름 * 필드에 규칙의 고유 이름을 입력합니다.
4. 필요에 따라 * Description * (설명 *) 필드에 규칙에 대한 간단한 설명을 입력합니다.

5. Tenant Accounts * 필드는 비워 둡니다.

   기본 규칙은 모든 테넌트 계정에 적용해야 합니다.

6. Bucket Name * 필드는 비워 둡니다.

   기본 규칙은 모든 S3 버킷 및 Swift 컨테이너에 적용되어야 합니다.

7. 고급 필터링 * 을 선택하지 마십시오

   기본 규칙은 필터를 지정할 수 없습니다.

8. 다음 * 을 선택합니다.

   2단계(배치 정의)가 나타납니다.

9. 참조 시간의 경우 * 비현재 시간 * 을 제외한 모든 옵션을 선택합니다.

   기본 규칙은 모든 개체 버전을 적용해야 합니다.

10. 기본 규칙의 배치 지침을 지정합니다.
    - 기본 규칙은 개체를 영구적으로 유지해야 합니다. 기본 규칙이 개체를 영구적으로 유지하지 않는 경우 새 정책을 활성화하면 경고가 표시됩니다. 이 동작이 예상되는 동작인지 확인해야 합니다.
    - 기본 규칙은 복제된 복사본을 만들어야 합니다.

      > 삭제 코딩 복사본을 정책의 기본 규칙으로 만드는 규칙을 사용하지 마십시오. 삭제 코딩 규칙에는 0.2 * 이상의 * 오브젝트 크기(MB) 고급 필터가 포함되어 있어 더 작은 오브젝트가 삭제 코딩되지 않도록 해야 합니다.

    - 전역 S3 오브젝트 잠금 설정을 사용(또는 활성화하려는 경우)하는 경우 기본 규칙은 다음과 같아야 합니다.
      - 복제된 오브젝트 복사본 2개 이상 또는 삭제 코딩 복사본 1개를 생성해야 합니다.
      - 이러한 복제본은 배치 지침에서 각 행의 전체 기간 동안 스토리지 노드에 있어야 합니다.
      - 오브젝트 복사본은 클라우드 스토리지 풀에 저장할 수 없습니다.
      - 오브젝트 복사본은 아카이브 노드에 저장할 수 없습니다.
      - Ingest Time을 참조 시간으로 사용하여 배치 지침의 최소 한 줄이 0일에 시작되어야 합니다.
      - 적어도 한 줄의 배치 지침은 영원히 있어야 합니다.
11. 보존 다이어그램을 업데이트하고 배치 지침을 확인하려면 * Refresh * 를 선택합니다.
12. 다음 * 을 선택합니다.

    3단계(Ingest 동작 정의)가 나타납니다.

13. 오브젝트가 수집될 때 사용할 데이터 보호 옵션을 선택하고 * 저장 * 을 선택합니다.

ILM 정책을 생성합니다

ILM 정책 생성: 개요

ILM 정책을 만들 때는 먼저 ILM 규칙을 선택하고 정렬해야 합니다. 그런 다음 이전에 수집된 개체에 대해 제안된 정책을 시뮬레이션하여 해당 정책의 동작을 확인합니다. 제안된 정책이 의도한 대로 작동하고 있다고 만족하면 이를 활성화하여 활성 정책을 생성할 수 있습니다.

> 잘못 구성된 ILM 정책으로 인해 복구할 수 없는 데이터 손실이 발생할 수 있습니다. ILM 정책을 활성화하기 전에 ILM 정책 및 ILM 규칙을 주의 깊게 검토한 다음 ILM 정책을 시뮬레이션합니다. ILM 정책이 의도한 대로 작동할 것인지 항상 확인하십시오.

ILM 정책을 생성할 때의 고려 사항

- 테스트 시스템에서만 시스템의 기본 제공 정책인 Baseline 2 Copies 정책을 사용합니다. 이 정책의 복사본 2개 만들기 규칙은 모든 사이트가 포함된 모든 스토리지 노드 스토리지 풀을 사용합니다. StorageGRID 시스템에 사이트가 두 개 이상 있는 경우 한 개체의 복사본을 같은 사이트에 둘 수 있습니다.
- 새 정책을 설계할 때는 그리드에 인제스트될 수 있는 다양한 유형의 모든 객체를 고려하십시오. 정책에 이러한 개체를 일치시키고 필요한 경우 배치할 규칙이 포함되어 있는지 확인합니다.
- ILM 정책을 최대한 단순하게 유지하십시오. 이렇게 하면 시간이 지남에 따라 StorageGRID 시스템을 변경할 때 의도된 대로 오브젝트 데이터가 보호되지 않는 잠재적으로 위험한 상황을 방지할 수 있습니다.
- 정책의 규칙이 올바른 순서로 되어 있는지 확인합니다. 정책이 활성화되면 위에서 시작하여 나열된 순서대로 새 개체와 기존 개체가 평가됩니다. 예를 들어 정책의 첫 번째 규칙이 개체와 일치하면 다른 규칙이 해당 규칙을 평가하지 않습니다.
- 모든 ILM 정책의 마지막 규칙은 필터를 사용할 수 없는 기본 ILM 규칙입니다. 개체가 다른 규칙과 일치하지 않으면 기본 규칙은 개체가 배치된 위치와 유지되는 기간을 제어합니다.
- 새 정책을 활성화하기 전에 정책이 기존 개체의 배치에 대해 적용하는 모든 변경 사항을 검토하십시오. 기존 오브젝트의 위치를 변경하면 새로운 배치가 평가되고 구현될 때 일시적인 리소스 문제가 발생할 수 있습니다.

제안된 ILM 정책을 생성합니다

제안된 ILM 정책을 처음부터 새로 만들거나 동일한 규칙 집합으로 시작하려는 경우 현재 활성 정책을 복제할 수 있습니다.

> 전역 S3 오브젝트 잠금 설정이 활성화된 경우 다음 절차를 대신 사용하십시오. S3 오브젝트 잠금이 활성화된 후 ILM 정책을 생성합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- 제안된 정책에 추가할 ILM 규칙을 만들었습니다. 필요에 따라 제안된 정책을 저장하고 규칙을 추가한 다음 제안된 정책을 편집하여 새 규칙을 추가할 수 있습니다.
- 있습니다 기본 ILM 규칙을 만들었습니다 필터를 포함하지 않는 정책의 경우.
- 선택적으로 비디오를 시청했습니다. "비디오: StorageGRID ILM 정책"

이 작업에 대해

제안된 ILM 정책을 생성하는 일반적인 이유는 다음과 같습니다.

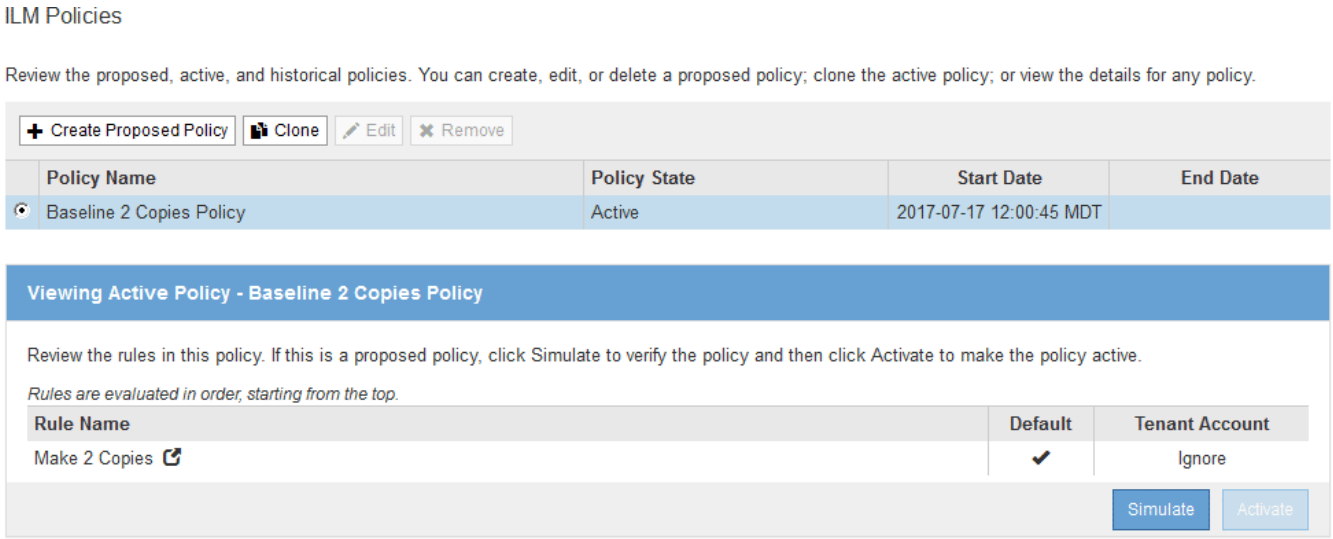
- 새 사이트를 추가하고 새 ILM 규칙을 사용하여 해당 사이트에 개체를 배치해야 합니다.
- 사이트를 사용 중지하려는 경우 사이트를 참조하는 모든 규칙을 제거해야 합니다.
- 특별한 데이터 보호 요구 사항이 있는 새 테넌트를 추가했습니다.
- 클라우드 스토리지 풀을 사용하기 시작했습니다.

> 테스트 시스템에서만 시스템의 기본 제공 정책인 Baseline 2 Copies 정책을 사용합니다. 이 정책의 복사본 2개 만들기 규칙은 모든 사이트가 포함된 모든 스토리지 노드 스토리지 풀을 사용합니다. StorageGRID 시스템에 사이트가 두 개 이상 있는 경우 한 개체의 복사본을 같은 사이트에 둘 수 있습니다.

단계

1. ILM * > * 정책 * 을 선택합니다.

   ILM 정책 페이지가 나타납니다. 이 페이지에서는 제안, 활성 및 과거 정책의 목록을 검토할 수 있으며, 생성, 편집, 또는 제안된 정책을 제거하거나, 활성 정책을 복제하거나, 정책에 대한 세부 정보를 봅니다.

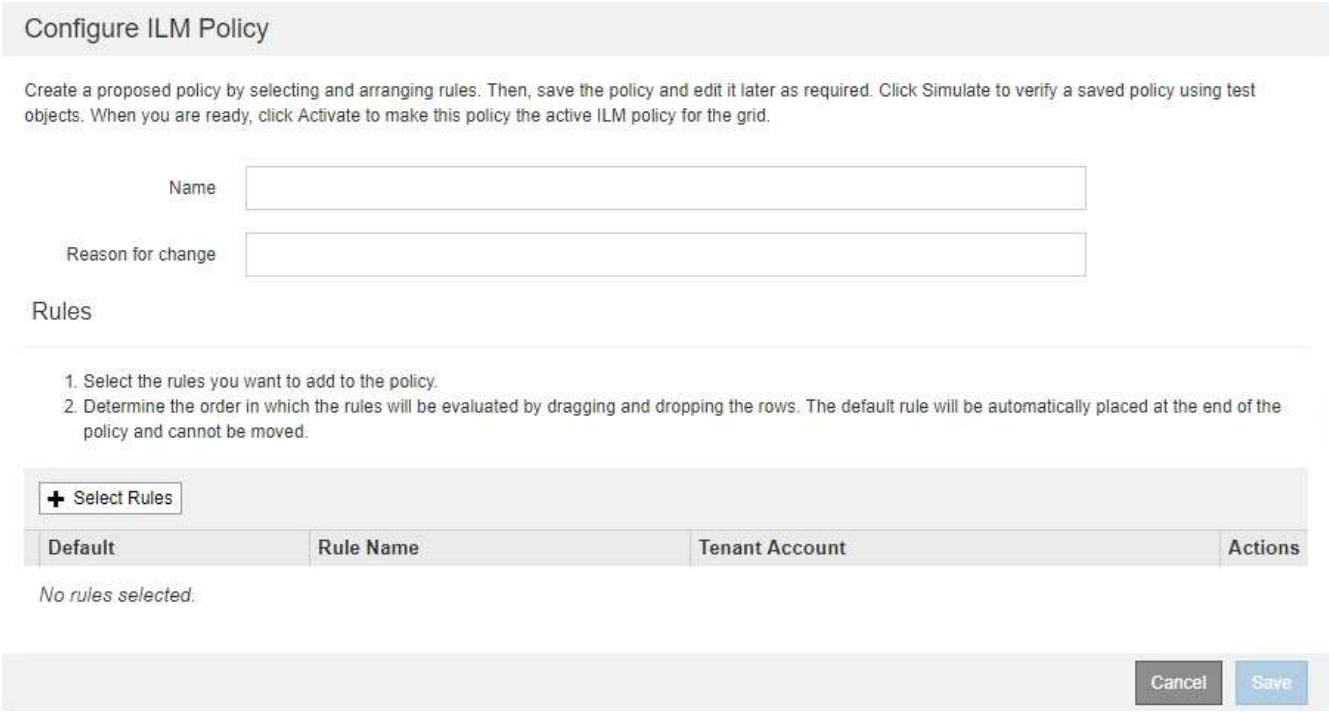


2. 제안된 ILM 정책을 생성할 방법을 결정합니다.

옵션을 선택합니다	단계
이미 선택된 규칙이 없는 제안된 새 정책을 생성합니다	a. 제안된 ILM 정책이 현재 존재하는 경우 해당 정책을 선택하고 * 제거 * 를 선택합니다. 제안된 정책이 이미 있는 경우 새 제안된 정책을 생성할 수 없습니다. b. 제안된 정책 생성 * 을 선택합니다.
활성 정책을 기반으로 제안된 정책을 생성합니다	a. 제안된 ILM 정책이 현재 존재하는 경우 해당 정책을 선택하고 * 제거 * 를 선택합니다. 제안된 정책이 이미 있는 경우 활성 정책을 복제할 수 없습니다. b. 테이블에서 활성 정책을 선택합니다. c. 클론 * 을 선택합니다.
기존의 제안된 정책을 편집합니다	a. 테이블에서 제안된 정책을 선택합니다. b. 편집 * 을 선택합니다.

ILM 정책 구성 대화 상자가 나타납니다.

새 제안 정책을 작성하는 경우 모든 필드가 비어 있고 규칙이 선택되지 않습니다.



활성 정책을 복제하는 경우 * 이름 * 필드에 버전 번호(""v2"")가 추가된 활성 정책의 이름이 표시됩니다. 활성 정책에 사용된 규칙이 선택되고 현재 순서로 표시됩니다.

3. 이름 * 필드에 제안된 정책의 고유한 이름을 입력합니다.

   최소 1자 이상 64자 이하여야 합니다. 활성 정책을 복제하는 경우 현재 이름에 추가된 버전 번호를 사용하거나 새 이름을 입력할 수 있습니다.

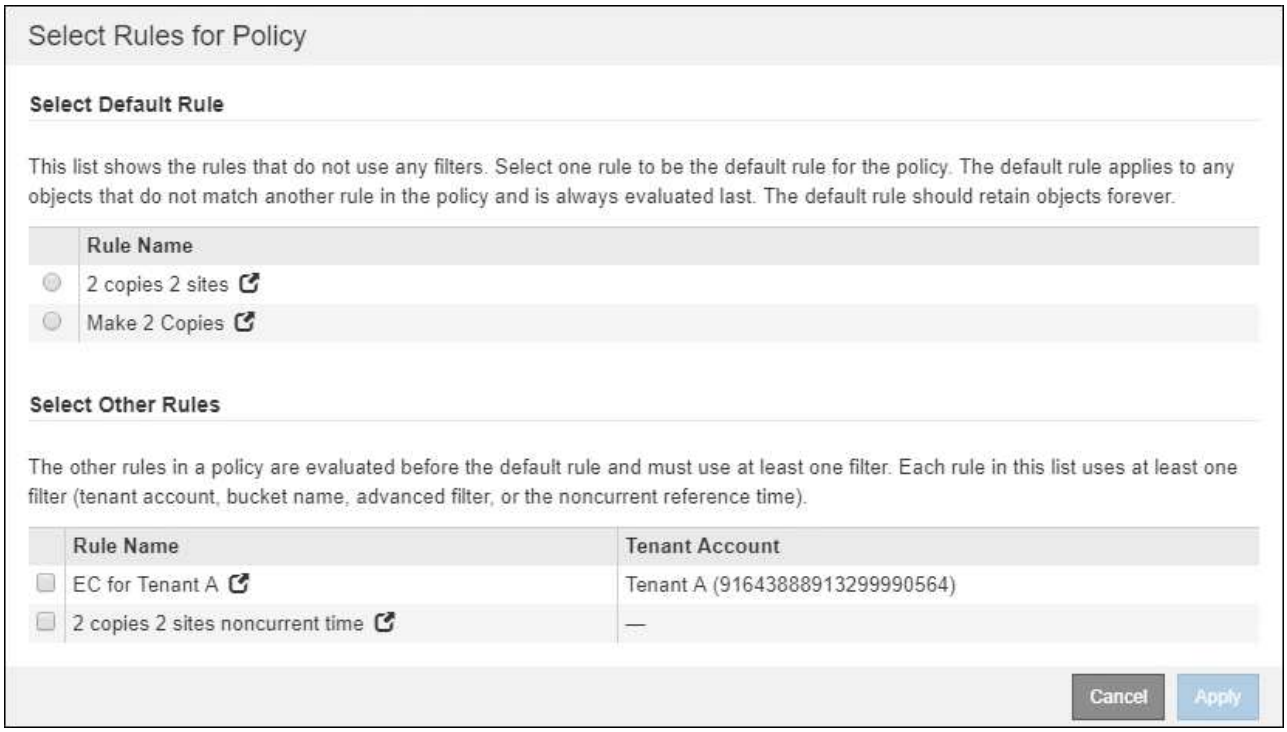
4. [변경 사유] * 필드에 새 제안 정책을 작성하는 이유를 입력합니다.

   1자 이상 128자 이하여야 합니다.

5. 정책에 규칙을 추가하려면 * 규칙 선택 * 을 선택합니다.

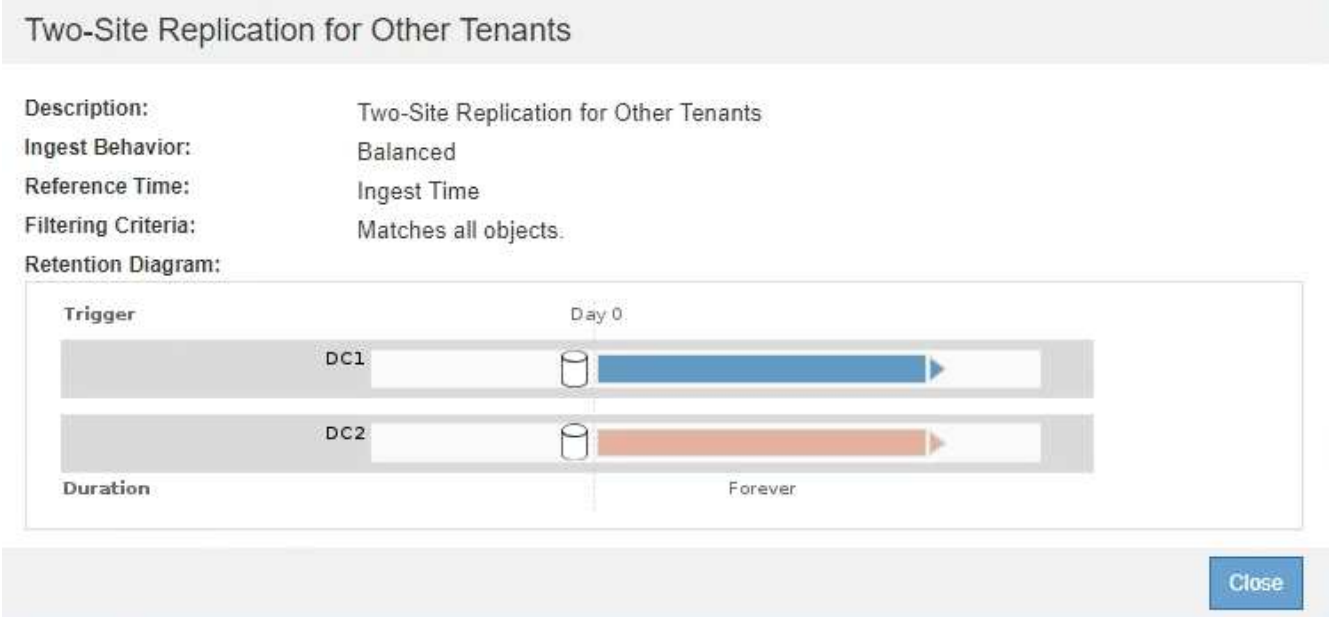
   정의된 모든 규칙이 나열된 상태로 정책 규칙 선택 대화 상자가 나타납니다. 정책을 클론 생성하는 경우:

   - 클론 생성 중인 정책에 사용되는 규칙이 선택됩니다.
   - 클론 생성 중인 정책에서 기본 규칙이 아닌 필터가 없는 규칙을 사용한 경우 해당 규칙 중 하나만 제외하고 모두 제거하라는 메시지가 표시됩니다.
   - 기본 규칙에서 필터나 비현재 참조 시간을 사용한 경우 새 기본 규칙을 선택하라는 메시지가 표시됩니다.
   - 기본 규칙이 마지막 규칙이 아닌 경우 버튼을 사용하여 새 정책의 끝으로 규칙을 이동할 수 있습니다.



6. 규칙 이름 또는 추가 세부 정보 아이콘을 선택합니다 를 눌러 해당 규칙의 설정을 봅니다.

   이 예에서는 두 사이트에서 두 개의 복제된 복사본을 만드는 ILM 규칙의 세부 정보를 보여줍니다.



7. 기본 규칙 선택 * 섹션에서 제안된 정책에 대한 기본 규칙 하나를 선택합니다.

   기본 규칙은 정책의 다른 규칙과 일치하지 않는 모든 개체에 적용됩니다. 기본 규칙은 필터를 사용할 수 없으며 항상 마지막으로 평가됩니다.

   > 기본 규칙 선택 섹션에 규칙이 없으면 ILM 정책 페이지 및 를 종료해야 합니다 기본 ILM 규칙을 생성합니다.

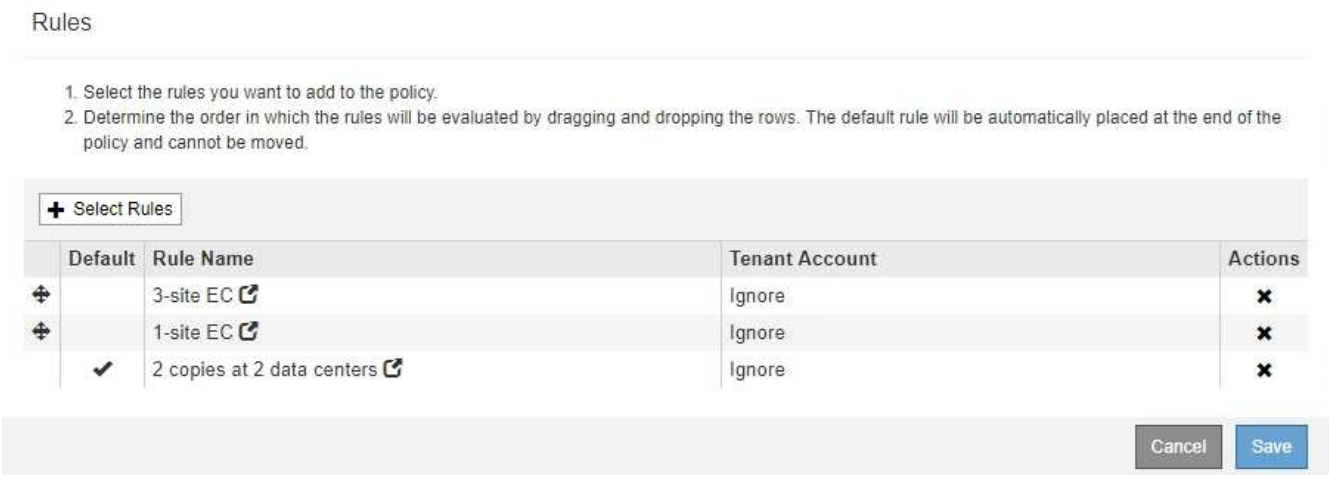
   > Make 2 Copies 재고 규칙을 정책의 기본 규칙으로 사용하지 마십시오. 2개 복제본 만들기 규칙은 모든 사이트를 포함하는 단일 스토리지 풀인 모든 스토리지 노드를 사용합니다. StorageGRID 시스템에 사이트가 두 개 이상 있는 경우 한 개체의 복사본을 같은 사이트에 둘 수 있습니다.

8. 다른 규칙 선택 * 섹션에서 정책에 포함할 다른 규칙을 선택합니다.

   다른 규칙은 기본 규칙 전에 평가되며 하나 이상의 필터(테넌트 계정, 버킷 이름, 고급 필터 또는 현재 참조 시간)를 사용해야 합니다.

9. 규칙 선택을 마치면 * 적용 * 을 선택합니다.

   선택한 규칙이 나열됩니다. 기본 규칙은 끝에 있으며 다른 규칙은 그 위에 있습니다.



기본 규칙에서 개체를 영구적으로 유지하지 않으면 경고가 나타납니다. 이 정책을 활성화할 때 버킷 수명 주기에 따라 개체를 더 오래 보존하지 않는 한 기본 규칙에 대한 배치 지침이 경과할 때 StorageGRID에서 개체를 삭제할 것인지 확인해야 합니다.

10. 기본 규칙이 아닌 규칙의 행을 끌어서 놓아 이러한 규칙이 평가되는 순서를 결정합니다.

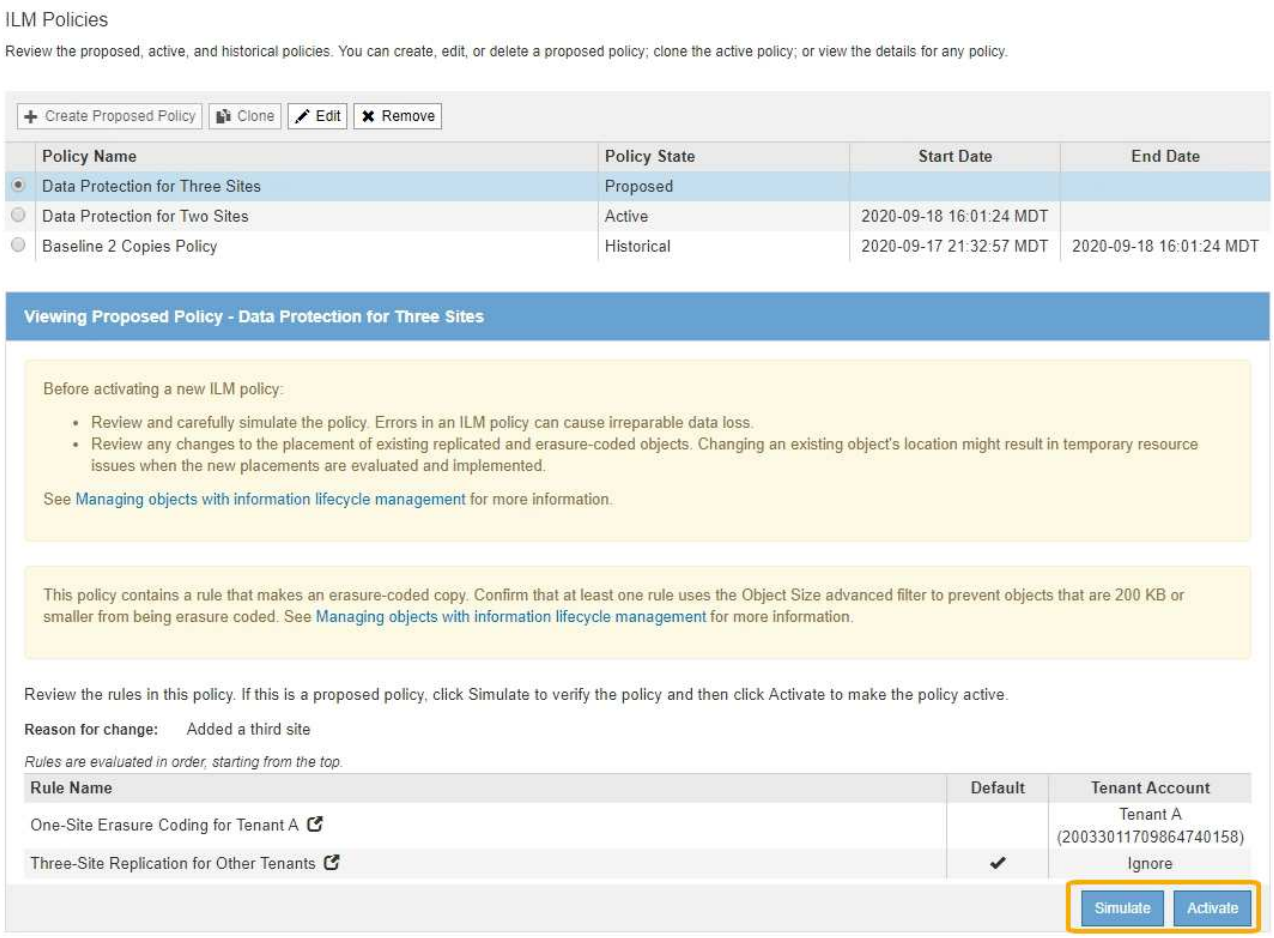
    기본 규칙을 이동할 수 없습니다.

    ILM 규칙이 올바른 순서로 되어 있는지 확인해야 합니다. 정책이 활성화되면 위에서 시작하여 나열된 순서대로 새 개체와 기존 개체가 평가됩니다.

11. 필요에 따라 삭제 아이콘을 선택합니다 ✖ 정책에서 원하지 않는 규칙을 삭제하려면 * 규칙 선택 * 을 선택하여 규칙을 더 추가합니다.
12. 완료되면 * Save * 를 선택합니다.

    ILM 정책 페이지가 업데이트됩니다.

    - 저장한 정책이 제안으로 표시됩니다. 제안된 정책에는 시작 및 종료 날짜가 없습니다.
    - 시뮬레이션 * 및 * 활성화 * 버튼이 활성화됩니다.



13. 로 이동합니다 ILM 정책을 시뮬레이션합니다.

관련 정보

- ILM 정책이란 무엇인가
- S3 오브젝트 잠금으로 오브젝트 관리

S3 오브젝트 잠금이 활성화된 후 **ILM** 정책을 생성합니다

전역 S3 개체 잠금 설정이 활성화된 경우 정책 생성 단계가 약간 다릅니다. ILM 정책이 S3 오브젝트 잠금이 설정된 버킷의 요구사항을 준수하는지 확인해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 이미 활성화되어 있습니다.

> 전역 S3 오브젝트 잠금 설정이 활성화되지 않은 경우 의 일반 지침을 사용합니다 제안된 ILM 정책 생성.

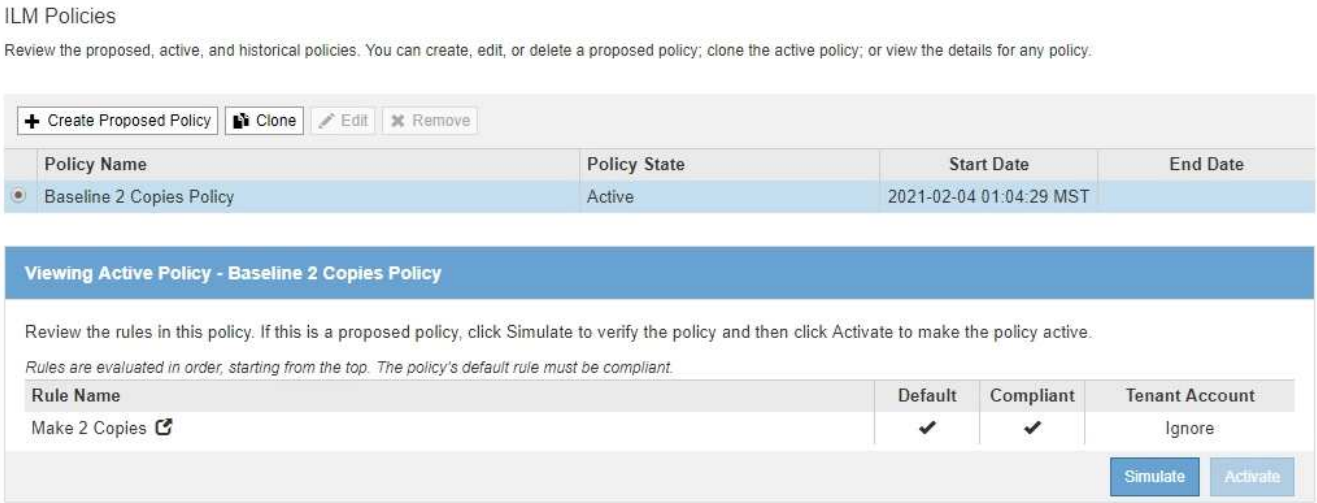
- 제안된 정책에 추가하려는 규정 준수 및 비준수 ILM 규칙을 만들었습니다. 필요에 따라 제안된 정책을 저장하고 규칙을 추가한 다음 제안된 정책을 편집하여 새 규칙을 추가할 수 있습니다. 을 참조하십시오예 7: S3 오브젝트 잠금에 대한 규정 준수 ILM 정책.

- 있습니다 기본 ILM 규칙을 만들었습니다 정책을 준수하는 경우.
- 선택적으로 비디오를 시청했습니다. "비디오: StorageGRID ILM 정책"

단계

1. ILM * > * 정책 * 을 선택합니다.

   ILM 정책 페이지가 나타납니다. 전역 S3 개체 잠금 설정이 활성화된 경우 ILM 정책 페이지에는 호환되는 ILM 규칙이 표시됩니다.



2. 이름 * 필드에 제안된 정책의 고유한 이름을 입력합니다.

   최소 1자 이상 64자 이하여야 합니다.

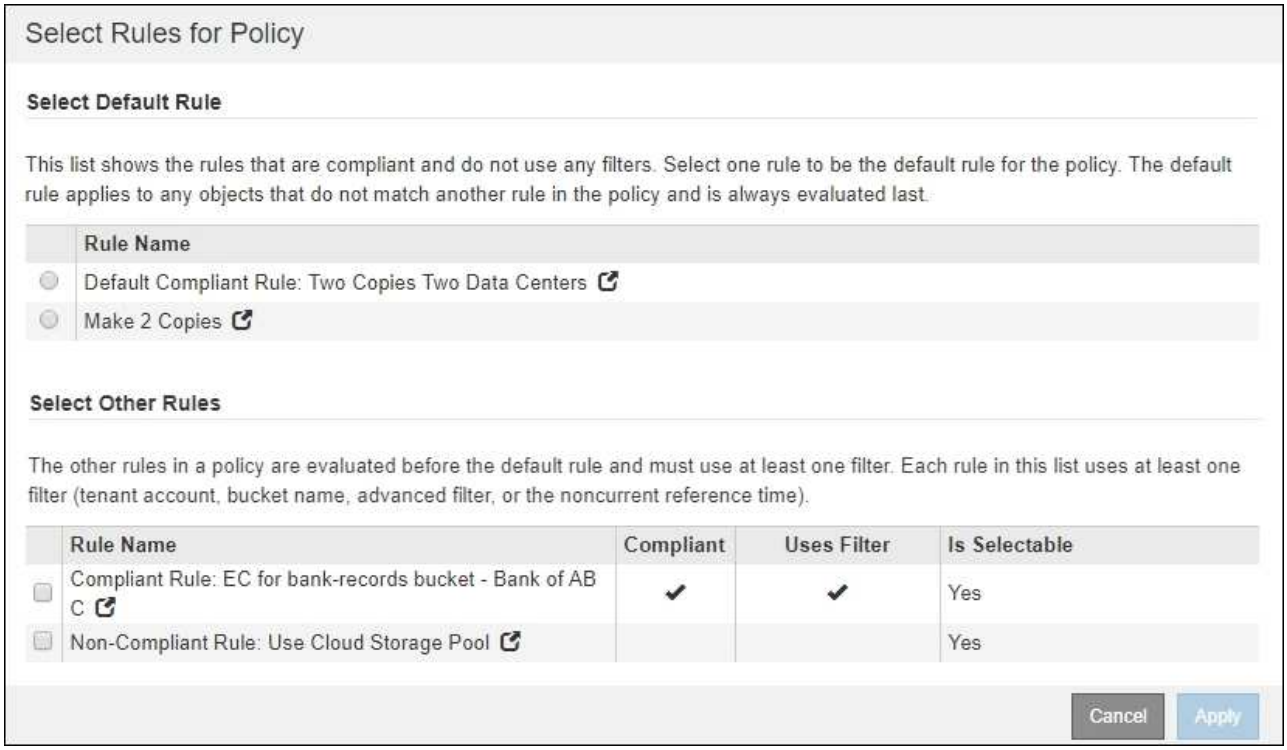
3. [변경 사유] * 필드에 새 제안 정책을 작성하는 이유를 입력합니다.

   1자 이상 128자 이하여야 합니다.

4. 정책에 규칙을 추가하려면 * 규칙 선택 * 을 선택합니다.

   정의된 모든 규칙이 나열된 상태로 정책 규칙 선택 대화 상자가 나타납니다.

- 기본 규칙 선택 섹션에는 규정 준수 정책의 기본값으로 사용할 수 있는 규칙이 나열됩니다. 필터 또는 비현재 참조 시간을 사용하지 않는 규정 준수 규칙이 포함되어 있습니다.
- 다른 규칙 선택 섹션에는 이 정책에 대해 선택할 수 있는 다른 규정 준수 및 비준수 규칙이 나열됩니다.



5. 규칙 이름 또는 추가 세부 정보 아이콘을 선택합니다 를 눌러 해당 규칙의 설정을 봅니다.
6. 기본 규칙 선택 * 섹션에서 제안된 정책에 대한 기본 규칙 하나를 선택합니다.

   이 섹션의 표에는 규정을 준수하며 필터를 사용하지 않는 규칙만 나열되어 있습니다.

   > 기본 규칙 선택 섹션에 규칙이 없으면 ILM 정책 페이지 및 를 종료해야 합니다 기본 ILM 규칙을 생성합니다 준수해야 합니다.

   > Make 2 Copies 재고 규칙을 정책의 기본 규칙으로 사용하지 마십시오. 2개 복제본 만들기 규칙은 모든 사이트를 포함하는 단일 스토리지 풀인 모든 스토리지 노드를 사용합니다. 이 규칙을 사용하는 경우 오브젝트의 여러 복사본이 동일한 사이트에 배치될 수 있습니다.

7. 다른 규칙 선택 * 섹션에서 정책에 포함할 다른 규칙을 선택합니다.

   a. 비규격 S3 버킷의 오브젝트에 대해 다른 "기본값" 규칙이 필요한 경우 필터를 사용하지 않는 비준수 규칙 하나를 선택할 수도 있습니다.

      예를 들어, 클라우드 스토리지 풀 또는 아카이브 노드를 사용하여 S3 오브젝트 잠금이 활성화되지 않은 버킷에 오브젝트를 저장할 수 있습니다.

      > 필터를 사용하지 않는 비준수 규칙을 하나만 선택할 수 있습니다. 하나의 규칙을 선택하는 즉시 * 선택 가능 * 열에 필터가 없는 다른 비준수 규칙에 대해 * 아니요 * 가 표시됩니다.

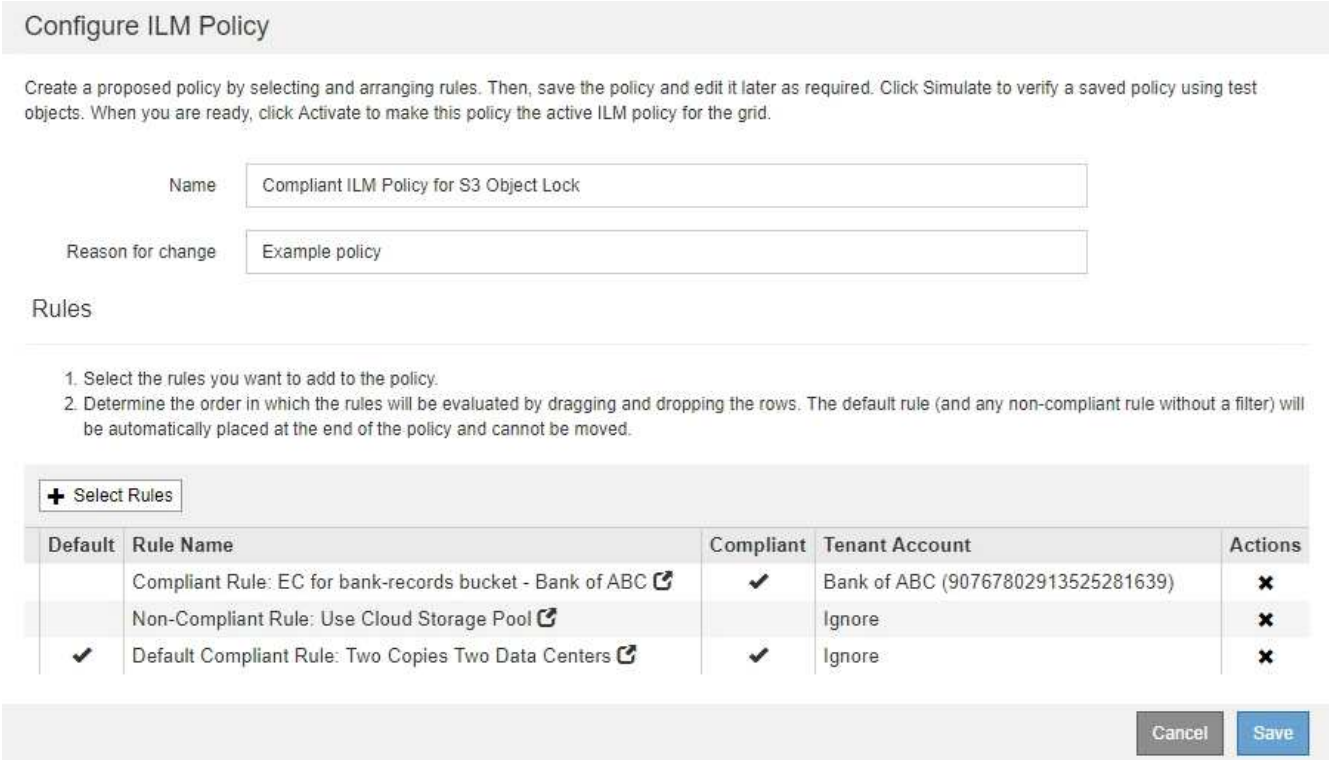
   a. 정책에 사용할 다른 규정 준수 또는 비준수 규칙을 선택합니다.

다른 규칙에서는 하나 이상의 필터(테넌트 계정, 버킷 이름 또는 객체 크기와 같은 고급 필터)를 사용해야 합니다.

8. 규칙 선택을 마치면 * 적용 * 을 선택합니다.

   선택한 규칙이 나열됩니다. 기본 규칙은 끝에 있으며 다른 규칙은 그 위에 있습니다. 비준수 "기본값" 규칙도 선택한 경우 해당 규칙이 정책의 두 번째 대 마지막 규칙으로 추가됩니다.

   이 예에서 마지막 규칙인 2개의 복사본 2개의 데이터 센터가 기본 규칙입니다. 즉, 이 규칙은 준수되며 필터가 없습니다. 두 번째, 마지막 규칙인 클라우드 스토리지 풀에도 필터가 없지만 규정을 준수하지 않습니다.



9. 기본 규칙이 아닌 규칙의 행을 끌어서 놓아 이러한 규칙이 평가되는 순서를 결정합니다.

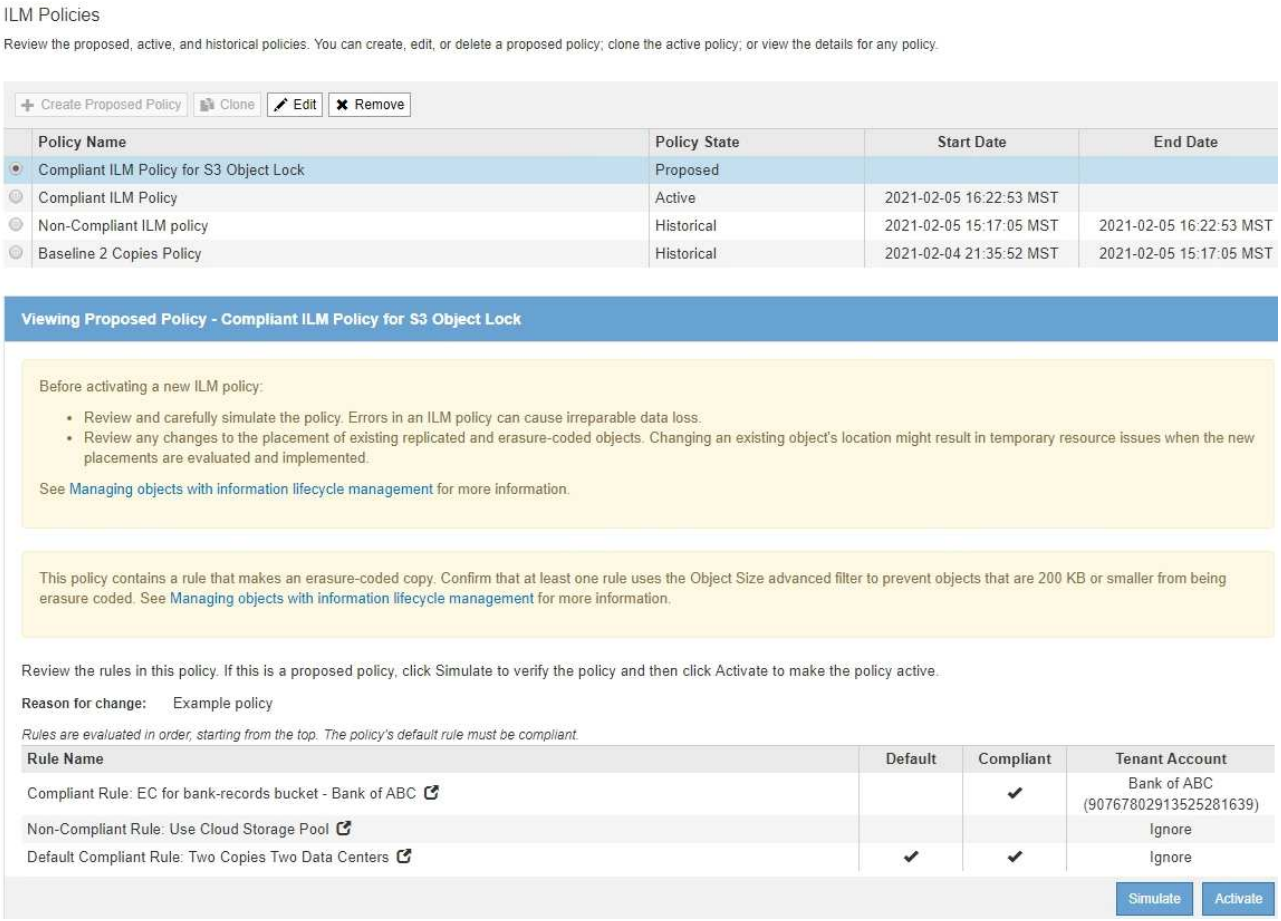
   기본 규칙 또는 비준수 "기본값" 규칙은 이동할 수 없습니다.

   > ILM 규칙이 올바른 순서로 되어 있는지 확인해야 합니다. 정책이 활성화되면 위에서 시작하여 나열된 순서대로 새 개체와 기존 개체가 평가됩니다.

10. 필요에 따라 삭제 아이콘을 선택합니다 ✖ 정책에서 원하지 않는 규칙을 삭제하려면 * 규칙 * 을 선택하고 규칙을 더 추가하려면 * 를 선택합니다.
11. 완료되면 * Save * 를 선택합니다.

    ILM 정책 페이지가 업데이트됩니다.

    - 저장한 정책이 제안으로 표시됩니다. 제안된 정책에는 시작 및 종료 날짜가 없습니다.
    - 시뮬레이션 * 및 * 활성화 * 버튼이 활성화됩니다.



12. 로 이동합니다 ILM 정책을 시뮬레이션합니다.

ILM 정책을 시뮬레이션합니다

정책을 활성화하고 운영 데이터에 적용하기 전에 테스트 개체에 대해 제안된 정책을 시뮬레이션해야 합니다. 시뮬레이션 창은 정책을 활성화하고 생산 환경의 데이터에 적용하기 전에 테스트를 위해 안전한 독립 실행형 환경을 제공합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- 테스트할 각 개체의 S3 버킷/오브젝트 키 또는 Swift 컨테이너/오브젝트 이름을 알고 있으며, 이미 오브젝트를 수집했습니다.

이 작업에 대해

제안된 정책을 테스트할 객체를 신중하게 선택해야 합니다. 정책을 철저히 시뮬레이션하려면 각 규칙에서 각 필터에 대해 하나 이상의 개체를 테스트해야 합니다.

예를 들어, 정책에 버킷 A의 오브젝트와 버킷 B의 오브젝트와 일치하는 다른 규칙이 포함된 경우, 정책을 철저히 테스트하기 위해 버킷 A에서 하나 이상의 오브젝트와 버킷 B에서 한 개의 오브젝트를 선택해야 합니다. 또한 기본 규칙을 테스트하려면 다른 버킷에서 하나 이상의 오브젝트를 선택해야 합니다.

정책을 시뮬레이션할 때 다음과 같은 고려 사항이 적용됩니다.

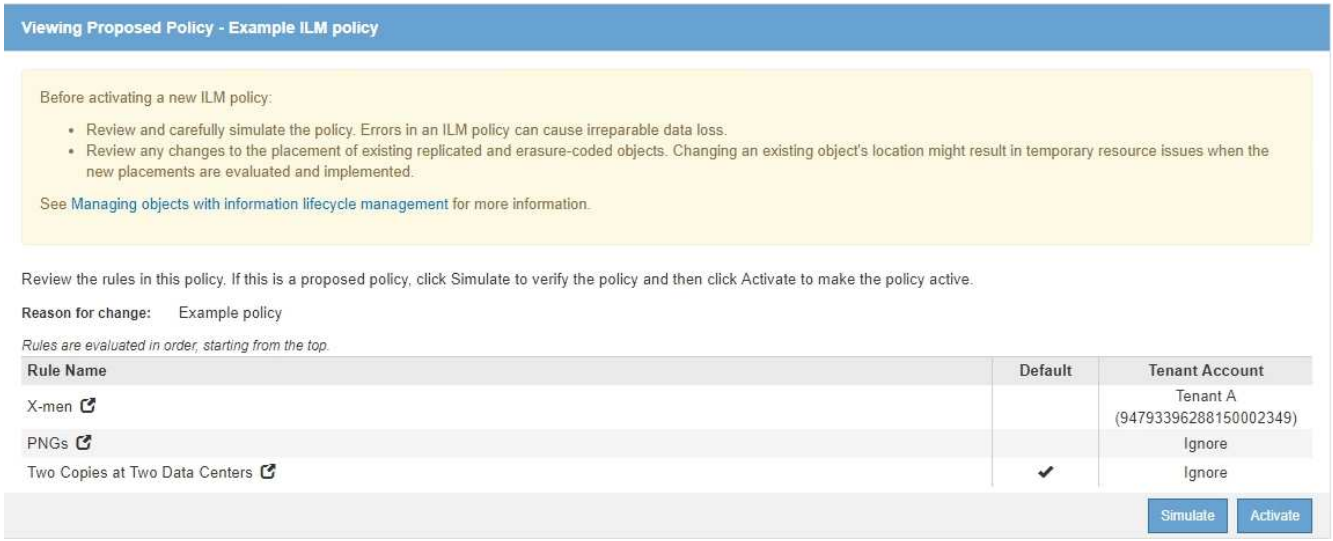
- 정책을 변경한 후 제안된 정책을 저장합니다. 그런 다음 저장된 제안 정책의 동작을 시뮬레이션합니다.
- 정책을 시뮬레이션하면 정책의 ILM 규칙이 테스트 개체를 필터링하여 각 개체에 적용된 규칙을 확인할 수 있습니다. 그러나 오브젝트 복사본은 만들지 않고 오브젝트는 배치되지 않습니다. 시뮬레이션을 실행해도 데이터, 규칙 또는 정책은 어떠한 방식으로도 수정되지 않습니다.
- Simulation 페이지는 ILM 정책 페이지를 닫거나, 탐색하거나, 새로 고칠 때까지 테스트한 개체를 유지합니다.
- Simulation은 일치하는 규칙의 이름을 반환합니다. 적용되는 스토리지 풀 또는 삭제 코딩 프로필을 확인하려면 규칙 이름 또는 추가 세부 정보 아이콘을 선택하여 보존 다이어그램을 볼 수 있습니다.
- S3 버전 관리가 활성화된 경우 정책은 현재 버전의 오브젝트에서만 시뮬레이션됩니다.

단계

1. 규칙을 선택 및 정렬하고 제안된 정책을 저장합니다.

   이 예제의 정책에는 다음 세 가지 규칙이 있습니다.

규칙 이름	필터	사본 유형	보존
X - 남성	• 테넌트 A • 사용자 메타데이터 (시리즈 = x-MEN)	2개의 데이터 센터에 2개의 복사본 생성	2년
PNG	키는 .png로 끝납니다	2개의 데이터 센터에 2개의 복사본 생성	5년
2개의 복사본 2개의 데이터 센터	없음	2개의 데이터 센터에 2개의 복사본 생성	영원히



2. S3, Swift 클라이언트 또는 를 사용합니다 Experimental S3 Console을 선택합니다각 테넌트의 테넌트 관리자에서 사용할 수 있는 에서는 각 규칙을 테스트하는 데 필요한 객체를 수집해야 합니다.
3. 시뮬레이션 * 을 선택합니다.

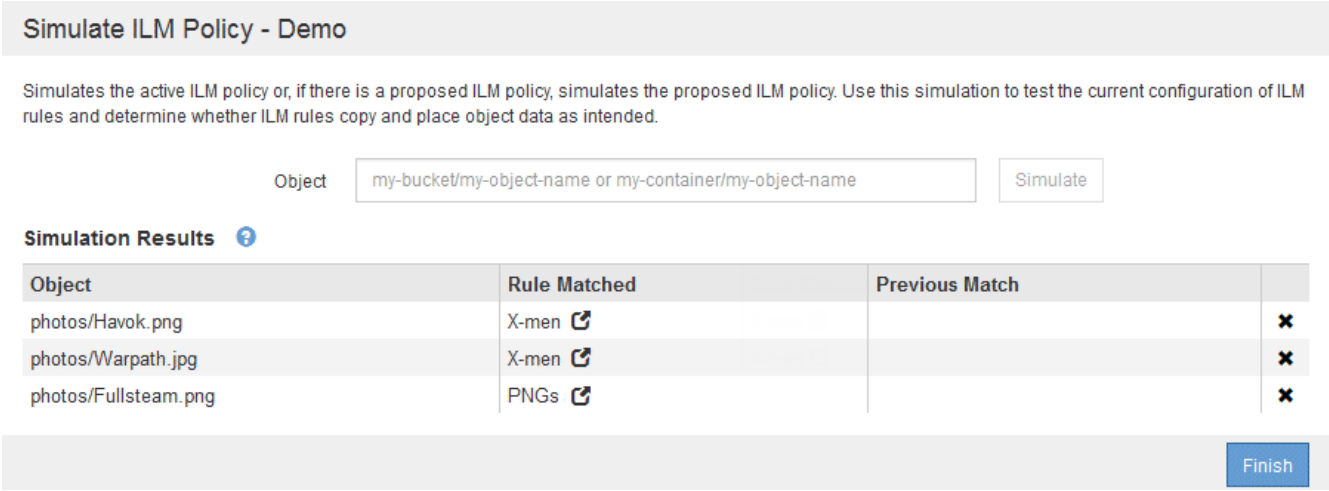
   Simulation ILM 정책 대화 상자가 나타납니다.

4. 오브젝트 * 필드에 테스트 오브젝트의 S3 버킷/오브젝트 키 또는 Swift 컨테이너/오브젝트 이름을 입력하고 * 시뮬레이션 * 을 선택합니다.

수집되지 않은 개체를 지정하면 메시지가 나타납니다.

5. Simulation Results * 에서 각 개체가 올바른 규칙과 일치하는지 확인합니다.

이 예에서 'Havok.png'와 'Warpath.jpg` 객체가 X-MEN 규칙에 의해 올바르게 일치했습니다. Series=x-Men의 사용자 메타데이터를 포함하지 않는 FullSteam.png의 객체는 X-MEN 규칙에 맞지 않지만 PNG 규칙에 의해 올바르게 일치되었습니다. 세 개의 개체가 모두 다른 규칙에 일치했기 때문에 기본 규칙이 사용되지 않았습니다.

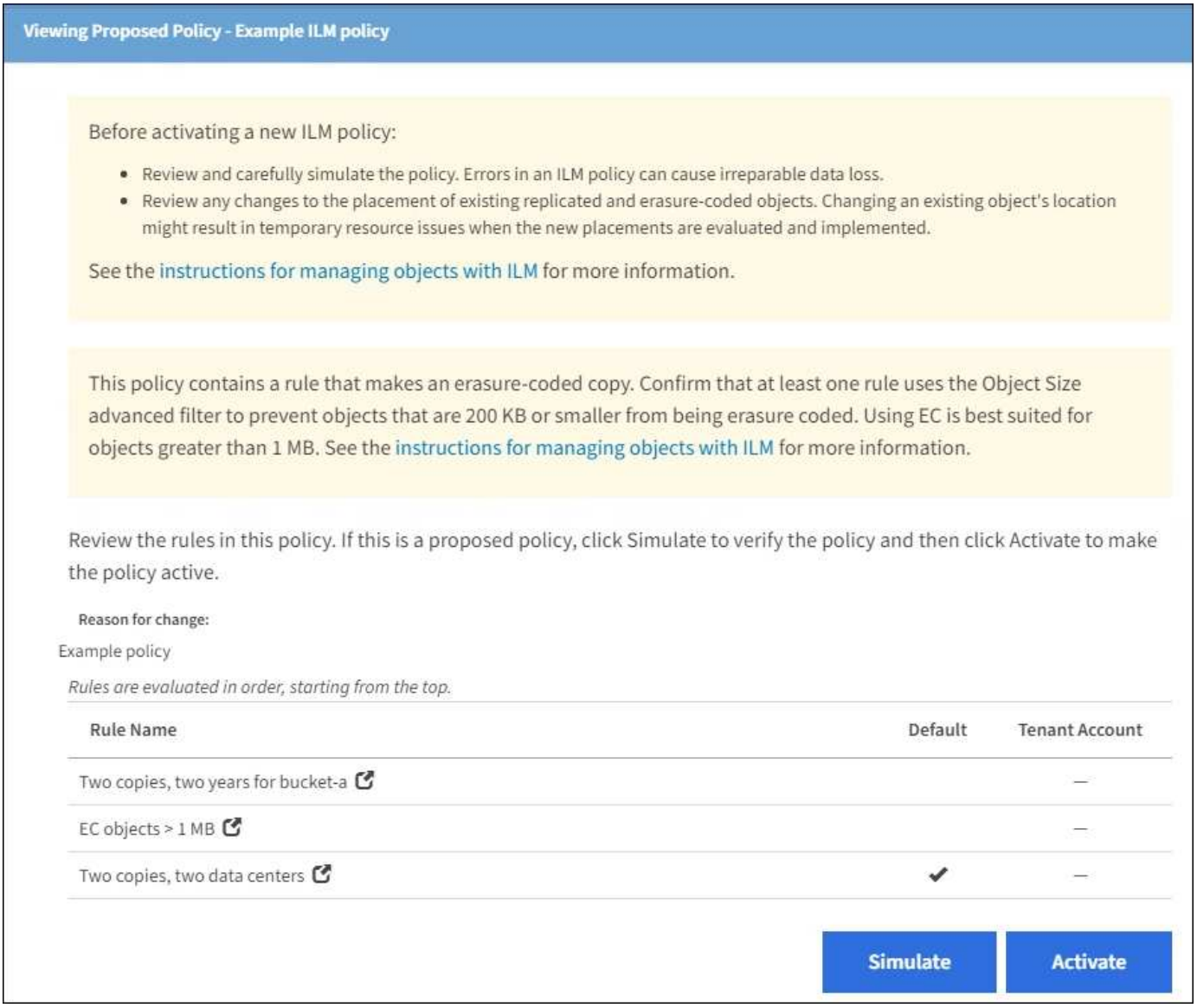


예 **1:** 제안된 **ILM** 정책을 시뮬레이션할 때 규칙을 확인합니다

이 예제에서는 제안된 정책을 시뮬레이션할 때 규칙을 확인하는 방법을 보여 줍니다.

이 예제에서 * 예제 ILM 정책 * 은 두 개의 버킷에 있는 인제스트된 오브젝트에 대해 시뮬레이션되고 있습니다. 이 정책은 다음과 같은 세 가지 규칙을 포함합니다.

- 첫 번째 규칙 * 2개 복사본, 버킷 - A * 의 경우 2년, 버킷 - a의 오브젝트에만 적용됩니다
- 두 번째 규칙인 * EC objects > 1MB * 는 1MB 이상의 객체에서 필터를 제외한 모든 버킷에 적용됩니다.
- 세 번째 규칙 * 두 개의 복사본, 두 개의 데이터 센터 * 가 기본 규칙입니다. 필터는 필터를 포함하지 않으며 비현재 참조 시간을 사용하지 않습니다.



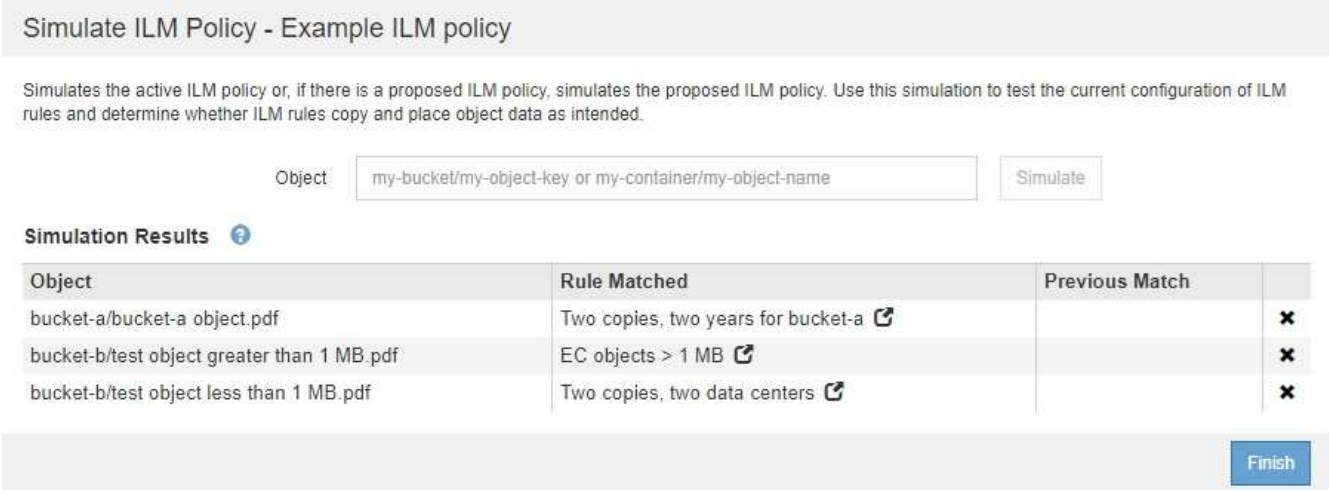
단계

1. 규칙을 추가하고 정책을 저장한 후 * Simulate * 를 선택합니다.

   ILM 정책 시뮬레이션 대화 상자가 나타납니다.

2. 오브젝트 * 필드에 테스트 오브젝트의 S3 버킷/오브젝트 키 또는 Swift 컨테이너/오브젝트 이름을 입력하고 * 시뮬레이션 * 을 선택합니다.

   Simulation 결과가 나타나고 정책의 어떤 규칙이 테스트한 각 개체와 일치하는지를 보여줍니다.



3. 각 객체가 올바른 규칙에 일치하는지 확인합니다.

   이 예에서

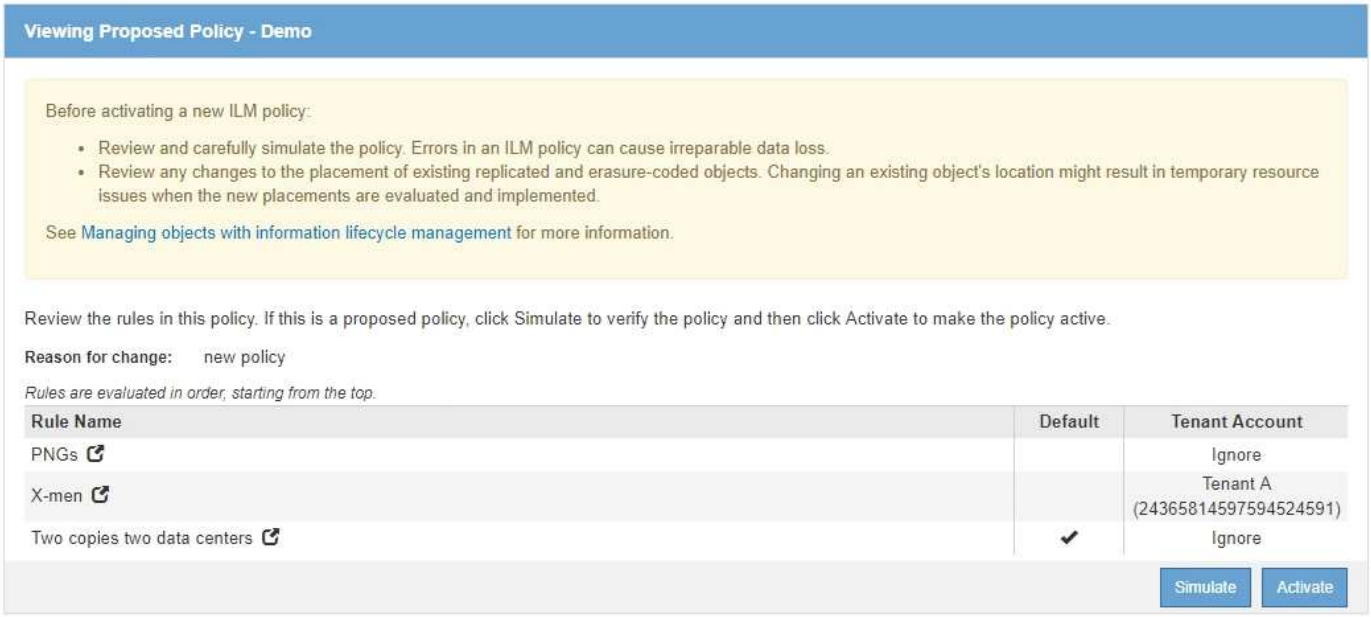
   a. bucket-A/bucket-a object.pdf는 bucket-A의 오브젝트를 필터링하는 첫 번째 규칙과 정확하게 일치했습니다.
   b. bucket-b/test object greater than 1 MB.pdf는 bucket-b에 들어 있어 첫 번째 규칙과 일치하지 않습니다. 대신 1MB보다 큰 객체를 필터링하는 두 번째 규칙에 의해 올바르게 일치되었습니다.
   c. bucket-b/test object less than 1 MB.pdf가 처음 두 개의 규칙에 있는 필터와 일치하지 않아 필터가 없는 기본 규칙에 따라 배치됩니다.

예 **2:** 제안된 **ILM** 정책을 시뮬레이션할 때 규칙 순서 바꾸기

이 예제에서는 정책을 시뮬레이션할 때 결과를 변경하기 위해 규칙의 순서를 변경하는 방법을 보여 줍니다.

이 예에서는 * Demo * 정책을 시뮬레이션하고 있습니다. 이 정책은 시리즈 = x-men 사용자 메타데이터가 있는 개체를 찾기 위해 다음과 같은 세 가지 규칙을 포함합니다.

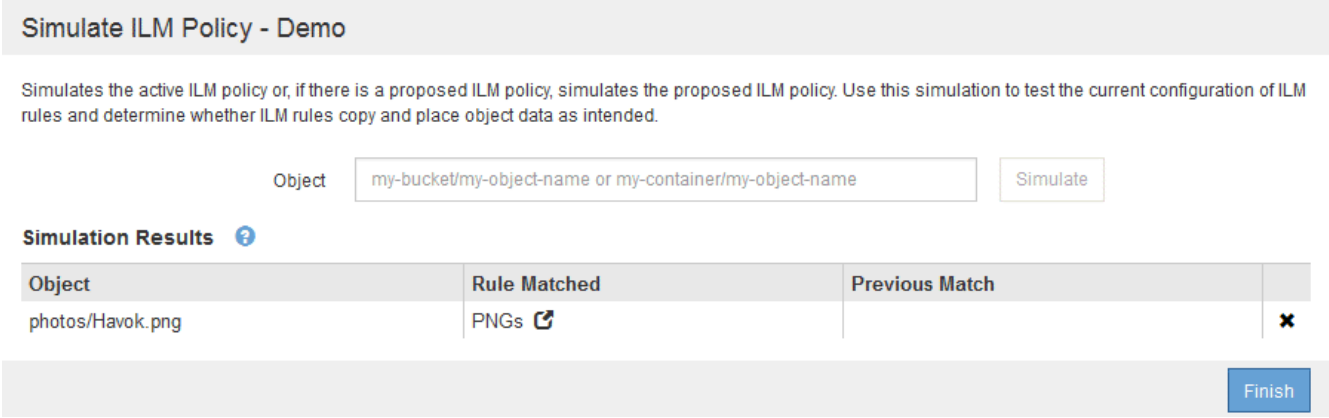
- 첫 번째 규칙인 * PNG * 는 '.png'로 끝나는 키 이름을 필터링합니다.
- 두 번째 규칙 * X-Men * 은 테넌트 A의 객체와 시리즈 = x-멘의 사용자 메타데이터에만 적용됩니다.
- 마지막 규칙인 * Two 는 두 데이터 센터 * 를 복사합니다. 이 규칙은 처음 두 규칙과 일치하지 않는 모든 개체와 일치합니다.



단계

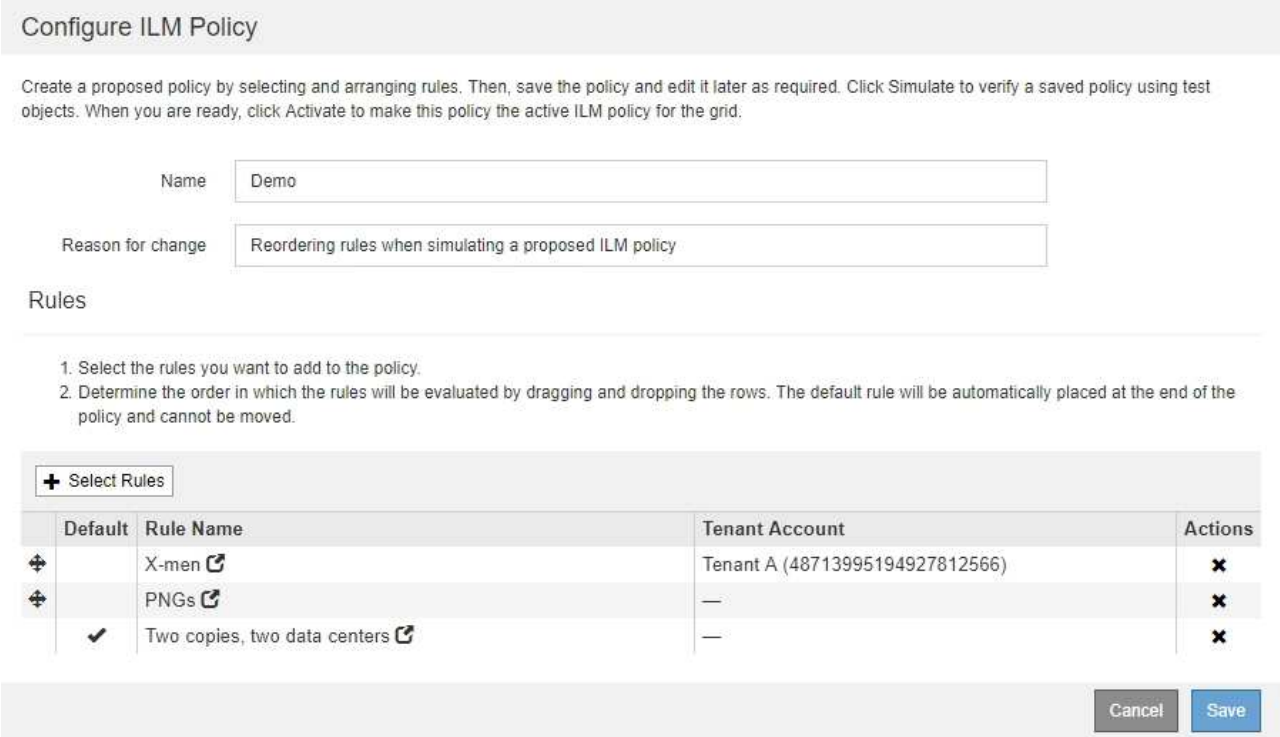
1. 규칙을 추가하고 정책을 저장한 후 * Simulate * 를 선택합니다.
2. 오브젝트 * 필드에 테스트 오브젝트의 S3 버킷/오브젝트 키 또는 Swift 컨테이너/오브젝트 이름을 입력하고 * 시뮬레이션 * 을 선택합니다.

   Simulation 결과가 나타나면서 'Havok.png' 객체가 * PNG * 규칙에 일치했음을 나타냅니다.



   그러나 하브록.png의 대상이 테스트한다는 규칙은 * X-MEN * 규칙이었습니다.

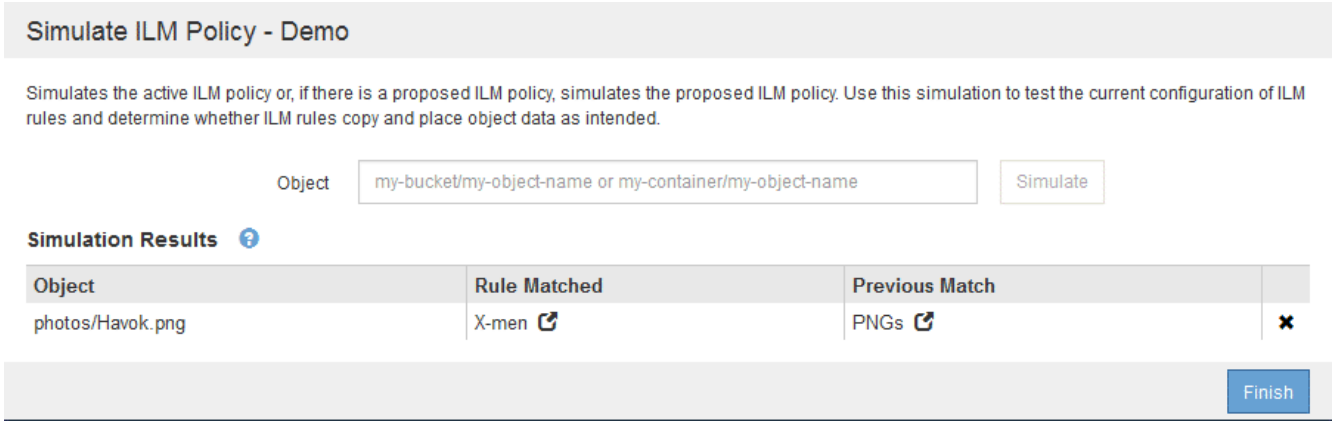
3. 문제를 해결하려면 규칙을 다시 정렬하십시오.
   a. ILM 정책 시뮬레이션 페이지를 닫으려면 * 마침 * 을 선택합니다.
   b. 정책을 편집하려면 * 편집 * 을 선택합니다.
   c. X-MEN * 규칙을 목록의 맨 위로 끕니다.



d. 저장 * 을 선택합니다.

4. 시뮬레이션 * 을 선택합니다.

이전에 테스트한 객체는 업데이트된 정책에 대해 재평가되고 새 시뮬레이션 결과가 표시됩니다. 이 예에서 Rule Matched 열은 'Havok.png' 객체가 예상대로 X-Men 메타데이터 규칙과 일치한다는 것을 보여줍니다. 이전 일치 열은 PNG 규칙이 이전 시뮬레이션에서 개체와 일치했음을 나타냅니다.



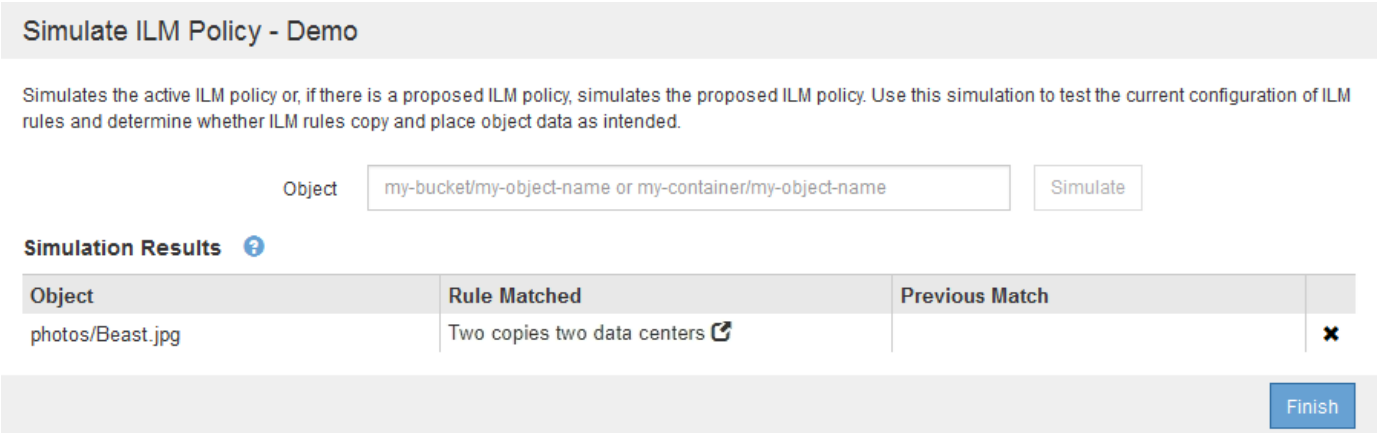
정책 구성 페이지에 있는 경우 테스트 개체의 이름을 다시 입력할 필요 없이 변경 후 정책을 다시 시뮬레이션할 수 있습니다.

예 **3:** 제안된 **ILM** 정책을 시뮬레이션할 때 규칙을 수정합니다

이 예제에서는 정책을 시뮬레이션하고 정책의 규칙을 정정하고 시뮬레이션을 계속하는 방법을 보여 줍니다.

이 예에서는 * Demo * 정책을 시뮬레이션하고 있습니다. 이 정책은 시리즈=X-MEN 사용자 메타데이터가 있는 객체를 찾는 데 목적이 있습니다. 그러나 Beast.jpg` 개체에 대해 이 정책을 시뮬레이션하는 동안 예기치 않은 결과가 발생했습니다. 이 개체는 X-Men 메타데이터 규칙을 일치시키는 대신 기본 규칙과 일치하며 두 개의 데이터 센터를

복제합니다.

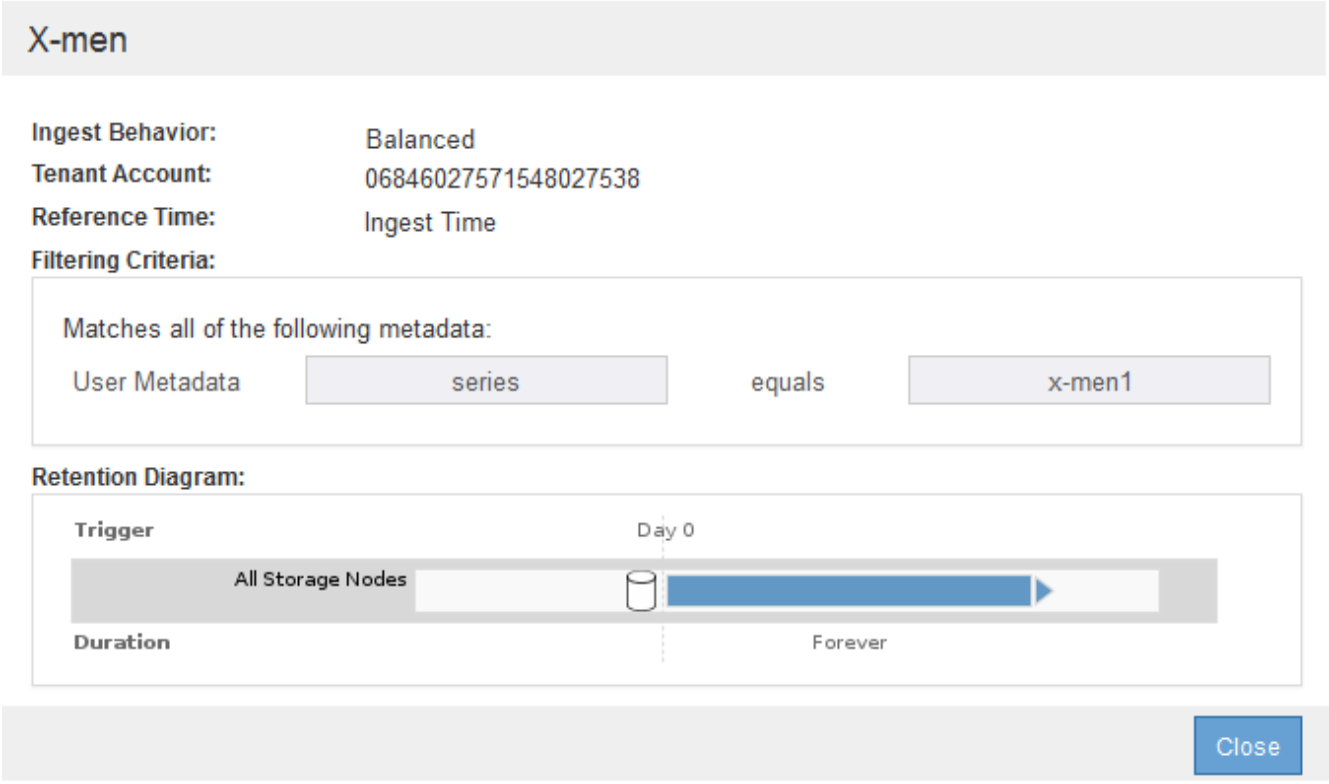


테스트 객체가 정책의 예상 규칙과 일치하지 않으면 정책의 각 규칙을 검사하고 오류를 수정해야 합니다.

단계

1. 정책의 각 규칙에 대해 규칙 이름 또는 자세한 정보 아이콘을 선택하여 규칙 설정을 확인합니다 규칙이 표시되는 대화 상자
2. 규칙의 테넌트 계정, 참조 시간 및 필터링 기준을 검토합니다.

   이 예제에서 X-MEN 규칙의 메타데이터에는 오류가 포함되어 있습니다. 메타데이터의 값은 "x-men" 대신 "x-men1"로 입력되었습니다.



3. 오류를 해결하려면 다음과 같이 규칙을 수정하십시오.

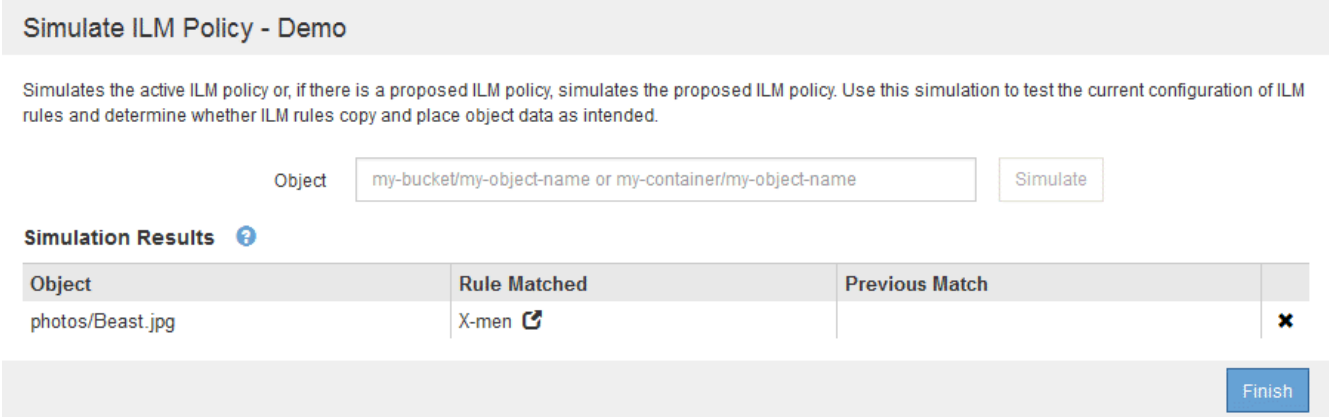
- 규칙이 제안된 정책의 일부인 경우 규칙을 복제하거나 정책에서 규칙을 제거한 다음 편집할 수 있습니다.
- 규칙이 활성 정책의 일부인 경우 규칙을 복제해야 합니다. 활성 정책에서 규칙을 편집하거나 제거할 수 없습니다.

옵션을 선택합니다	설명
규칙의 클론을 생성합니다	i. ILM * > * 규칙 * 을 선택합니다. ii. 잘못된 규칙을 선택하고 * Clone * 을 선택합니다. iii. 잘못된 정보를 변경하고 * Save * 를 선택합니다. iv. ILM * > * 정책 * 을 선택합니다. v. 제안된 정책을 선택하고 * Edit * 를 선택합니다. vi. 규칙 선택 * 을 선택합니다. vii. 새 규칙의 확인란을 선택하고 원래 규칙의 확인란을 선택 취소한 다음 * 적용 * 을 선택합니다. viii. 저장 * 을 선택합니다.
규칙을 편집합니다	i. 제안된 정책을 선택하고 * Edit * 를 선택합니다. ii. 삭제 아이콘을 선택합니다 ✖ 잘못된 규칙을 제거하려면 * 저장 * 을 선택합니다. iii. ILM * > * 규칙 * 을 선택합니다. iv. 잘못된 규칙을 선택하고 * 편집 * 을 선택합니다. v. 잘못된 정보를 변경하고 * Save * 를 선택합니다. vi. ILM * > * 정책 * 을 선택합니다. vii. 제안된 정책을 선택하고 * Edit * 를 선택합니다. viii. 수정된 규칙을 선택하고 * Apply * 를 선택한 다음 * Save * 를 선택합니다.

4. 시뮬레이션을 다시 수행합니다.

> ⓘ 규칙을 편집하기 위해 ILM 정책 페이지에서 탐색했기 때문에 이전에 시뮬레이션에 입력한 개체가 더 이상 표시되지 않습니다. 오브젝트의 이름을 다시 입력해야 합니다.

이 예에서 수정된 X-MEN 규칙은 이제 '시리즈=X-MEN' 사용자 메타데이터를 기반으로 하는 Beast.jpg` 객체와 일치합니다.



ILM 정책을 활성화합니다

ILM 규칙을 제안된 ILM 정책에 추가하고, 정책을 시뮬레이션하고, 정책이 예상대로 작동하는지 확인한 후에는 제안된 정책을 활성화할 준비가 된 것입니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- 제안된 ILM 정책을 저장하고 시뮬레이션했습니다.

> ILM 정책의 오류로 인해 복구할 수 없는 데이터 손실이 발생할 수 있습니다. 정책을 활성화하기 전에 정책을 주의 깊게 검토하고 시뮬레이션하여 의도한 대로 작동하도록 확인합니다.

> 새로운 ILM 정책을 활성화하면 StorageGRID은 이를 사용하여 기존 오브젝트 및 새로 수집된 오브젝트를 포함한 모든 오브젝트를 관리합니다. 새 ILM 정책을 활성화하기 전에 복제된 기존 오브젝트 및 삭제 코딩 오브젝트의 배치에 대한 변경 사항을 검토하십시오. 기존 오브젝트의 위치를 변경하면 새로운 배치가 평가되고 구현될 때 일시적인 리소스 문제가 발생할 수 있습니다.

이 작업에 대해

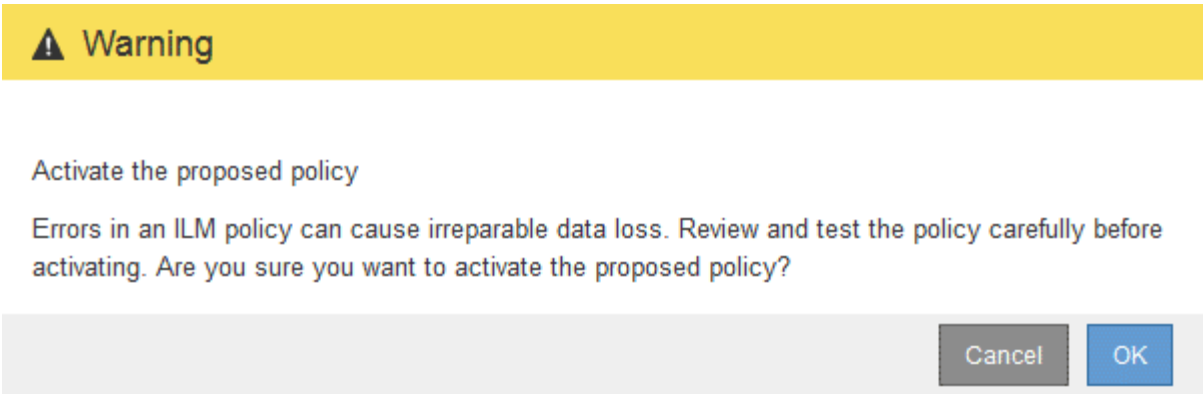
ILM 정책을 활성화하면 시스템은 새 정책을 모든 노드에 배포합니다. 그러나 새 활성 정책은 모든 그리드 노드가 새 정책을 받을 수 있을 때까지 실제로 적용되지 않을 수 있습니다. 경우에 따라 시스템이 그리드 객체가 실수로 제거되지 않도록 새 활성 정책을 구현하기를 기다립니다.

- 데이터 중복성 또는 내구성을 높이는 정책을 변경하는 경우 변경 사항이 즉시 적용됩니다. 예를 들어, 2개 복사본 규칙 대신 3개 복사본 규칙이 포함된 새 정책을 활성화하면 데이터 중복성이 증가하므로 해당 정책이 즉시 구현됩니다.
- 데이터 중복성이나 내구성이 저하될 수 있는 정책을 변경하면 모든 그리드 노드를 사용할 수 있을 때까지 이러한 변경 사항이 적용되지 않습니다. 예를 들어, 3개 복제본 규칙 대신 2개 복제본 규칙을 사용하는 새 정책을 활성화하면 새 정책이 "활성"으로 표시되지만 모든 노드가 온라인 상태가 되어 사용 가능할 때까지 적용되지 않습니다.

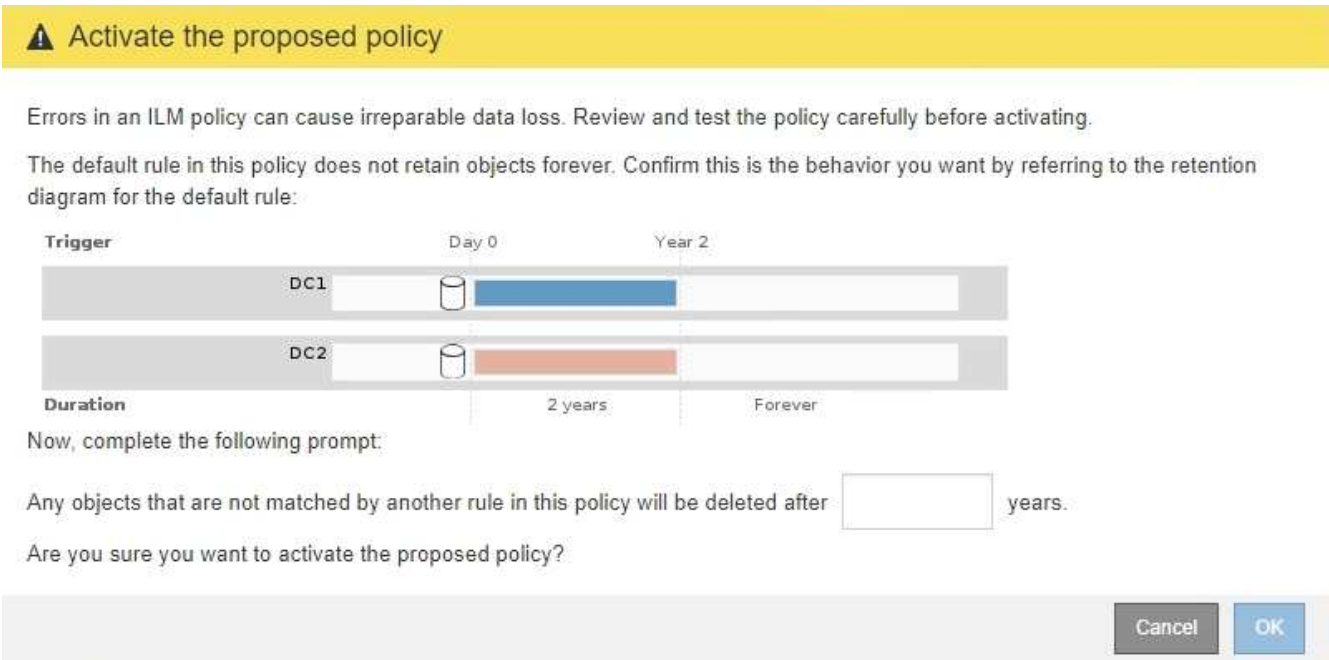
단계

1. 제안된 정책을 활성화할 준비가 되면 ILM 정책 페이지에서 정책을 선택하고 * 활성화 * 를 선택합니다.

   제안된 정책을 활성화할지 확인하는 경고 메시지가 표시됩니다.



정책에 대한 기본 규칙이 개체를 영구적으로 유지하지 않는 경우 경고 메시지에 프롬프트가 나타납니다. 이 예제에서 보존 다이어그램은 기본 규칙이 2년 후에 개체를 삭제하는 것을 보여 줍니다. 정책의 다른 규칙과 일치하지 않는 개체는 2년 후에 StorageGRID에서 제거됨을 인정하려면 텍스트 상자에 * 2 * 를 입력해야 합니다.

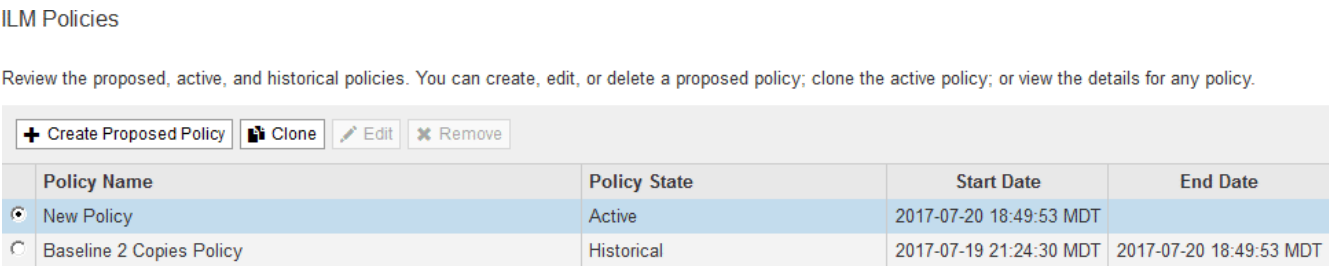


2. OK * 를 선택합니다.

결과

새 ILM 정책이 활성화된 경우:

- 정책은 ILM 정책 페이지의 표에 활성 정책 상태와 함께 표시됩니다. Start Date(시작 날짜) 항목은 정책이 활성화된 날짜 및 시간을 나타냅니다.



- 이전에 활성화된 정책이 정책 상태 기록 으로 표시됩니다. 시작 날짜 및 종료 날짜 항목은 정책이 활성화된 시기와

정책이 더 이상 적용되지 않는 시기를 나타냅니다.

관련 정보

예 6: ILM 정책 변경

개체 메타데이터 조회를 통해 **ILM** 정책을 확인합니다

ILM 정책을 활성화한 후 대표 테스트 개체를 StorageGRID 시스템으로 수집해야 합니다. 그런 다음 개체 메타데이터 조회를 수행하여 복사본이 의도한 대로 작성되고 올바른 위치에 배치되고 있는지 확인해야 합니다.

필요한 것

- 개체 식별자는 다음 중 하나일 수 있습니다.
  - * UUID *: 객체의 범용 고유 식별자입니다. UUID를 모두 대문자로 입력합니다.
  - * CBID *: StorageGRID 내에서 개체의 고유 식별자입니다. 감사 로그에서 개체의 CBID를 가져올 수 있습니다. CBID를 모두 대문자로 입력합니다.
  - * S3 버킷 및 오브젝트 키 *: S3 인터페이스를 통해 오브젝트를 수집하면 클라이언트 애플리케이션이 버킷과 오브젝트 키 조합을 사용하여 오브젝트를 저장하고 식별합니다. S3 버켓 버전이 있고 버킷과 오브젝트 키를 사용하여 S3 오브젝트의 특정 버전을 조회하려는 경우 * 버전 ID * 가 있습니다.
  - * Swift 컨테이너 및 오브젝트 이름 *: Swift 인터페이스를 통해 오브젝트가 수집되면 클라이언트 애플리케이션이 컨테이너 및 오브젝트 이름 조합을 사용하여 오브젝트를 저장하고 식별합니다.

단계

1. 오브젝트 수집:
2. ILM * > * 개체 메타데이터 조회 * 를 선택합니다.
3. 식별자 * 필드에 개체의 식별자를 입력합니다. UUID, CBID, S3 버킷/오브젝트 키 또는 Swift 컨테이너/오브젝트 이름을 입력할 수 있습니다.
4. 필요한 경우 오브젝트의 버전 ID를 입력합니다(S3만 해당).

5. Look Up * 을 선택합니다.

개체 메타데이터 조회 결과가 나타납니다. 이 페이지에는 다음 유형의 정보가 나열됩니다.

- 객체 ID(UUID), 객체 이름, 컨테이너 이름, 테넌트 계정 이름 또는 ID, 객체의 논리적 크기, 객체를 처음 생성한 날짜 및 시간, 객체를 마지막으로 수정한 날짜 및 시간을 비롯한 시스템 메타데이터
- 객체와 연결된 모든 사용자 메타데이터 키 값 쌍입니다.
- S3 오브젝트의 경우 오브젝트와 연결된 오브젝트 태그 키 값 쌍이 됩니다.
- 복제된 오브젝트 복사본의 경우 각 복제본의 현재 스토리지 위치입니다.
- 삭제 코딩 오브젝트 복사본의 경우 각 분절의 현재 스토리지 위치입니다.
- 클라우드 스토리지 풀의 오브젝트 복사본의 경우 외부 버킷의 이름 및 오브젝트의 고유 식별자를 비롯한 오브젝트의 위치가 포함됩니다.
- 분할된 오브젝트 및 다중 파트 오브젝트의 경우 세그먼트 식별자 및 데이터 크기를 포함한 오브젝트 세그먼트 목록입니다. 세그먼트가 100개를 초과하는 오브젝트의 경우 처음 100개의 세그먼트만 표시됩니다.
- 처리되지 않은 내부 스토리지 형식의 모든 오브젝트 메타데이터 이 원시 메타데이터에는 릴리즈부터 릴리즈까지 유지되지 않는 내부 시스템 메타데이터가 포함됩니다.

  다음 예는 2개의 복제된 복사본으로 저장된 S3 테스트 개체에 대한 오브젝트 메타데이터 조회 결과를 보여줍니다.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


6. 개체가 올바른 위치 또는 위치에 저장되어 있고 올바른 유형의 복사본인지 확인합니다.

> 감사 옵션이 활성화된 경우 ORLM 개체 규칙 충족 메시지에 대한 감사 로그를 모니터링할 수도 있습니다. ORLM 감사 메시지는 ILM 평가 프로세스의 상태에 대한 자세한 정보를 제공할 수 있지만, 개체 데이터의 배치 정확성 또는 ILM 정책의 완전성에 대한 정보는 제공할 수 없습니다. 직접 평가해야 합니다. 자세한 내용은 을 참조하십시오 감사 로그를 검토합니다.

관련 정보

- S3을 사용합니다
- Swift를 사용합니다

ILM 규칙 및 ILM 정책 작업

ILM 규칙 및 ILM 정책을 만든 후에는 스토리지 요구 사항이 변경됨에 따라 해당 구성을 수정하여 해당 규칙을 계속 사용할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

ILM 규칙을 삭제합니다

현재 ILM 규칙 목록을 관리할 수 있도록 유지하려면 사용하지 않을 수 있는 ILM 규칙을 모두 삭제하십시오.

ILM 규칙이 현재 활성 정책 또는 제안된 정책에서 사용 중인 경우에는 삭제할 수 없습니다. 정책을 사용하는 ILM 규칙을 삭제해야 하는 경우 먼저 다음 단계를 수행해야 합니다.

1. 활성 정책을 복제하거나 제안된 정책을 편집합니다.
2. 정책에서 ILM 규칙을 제거합니다.
3. 새 정책을 저장, 시뮬레이션 및 활성화하여 객체가 예상대로 보호되도록 합니다.

단계

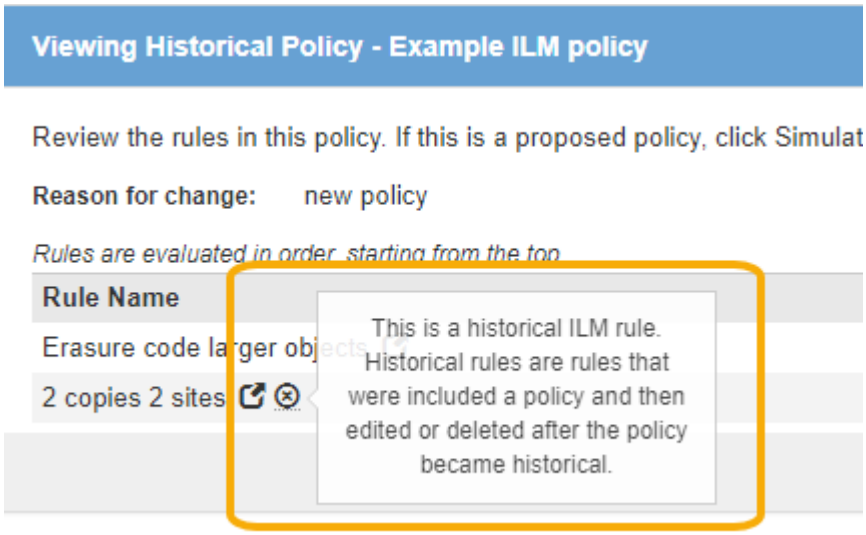
1. ILM * > * 규칙 * 을 선택합니다.
2. 제거할 규칙에 대한 테이블 항목을 검토합니다.

   활성 ILM 정책 또는 제안된 ILM 정책에서 규칙이 사용되지 않는지 확인합니다.

3. 제거하려는 규칙을 사용하지 않는 경우 라디오 버튼을 선택하고 * 제거 * 를 선택합니다.
4. ILM 규칙 삭제를 확인하려면 * OK * 를 선택합니다.

   ILM 규칙이 삭제됩니다.

내역 정책에 사용되는 규칙을 삭제하면 이(가) 됩니다 ⊗ 규칙을 볼 때 규칙에 대한 아이콘이 나타납니다. 이 아이콘은 규칙이 기록 규칙이 되었음을 나타냅니다.



ILM 규칙을 편집합니다

필터 또는 배치 지침을 변경하려면 ILM 규칙을 편집해야 할 수 있습니다.

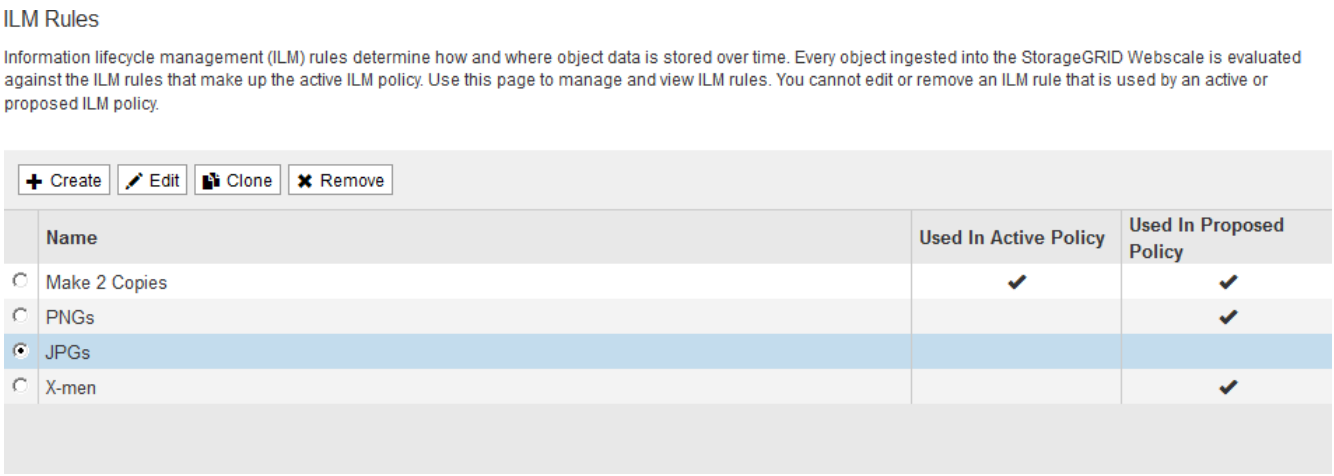
제안된 ILM 정책 또는 활성 ILM 정책에 사용되는 규칙은 편집할 수 없습니다. 대신 이러한 규칙을 클론 복제하고 클론 복제된 복사본을 필요한 사항으로 변경할 수 있습니다. 또한 StorageGRID 버전 10.3 이전에 생성된 재고 ILM 규칙(복사본 2개 만들기) 또는 ILM 규칙을 편집할 수 없습니다.

> 편집된 규칙을 활성 ILM 정책에 추가하기 전에 개체의 배치 지침을 변경하면 시스템에 부하가 증가할 수 있다는 점에 유의하십시오.

단계

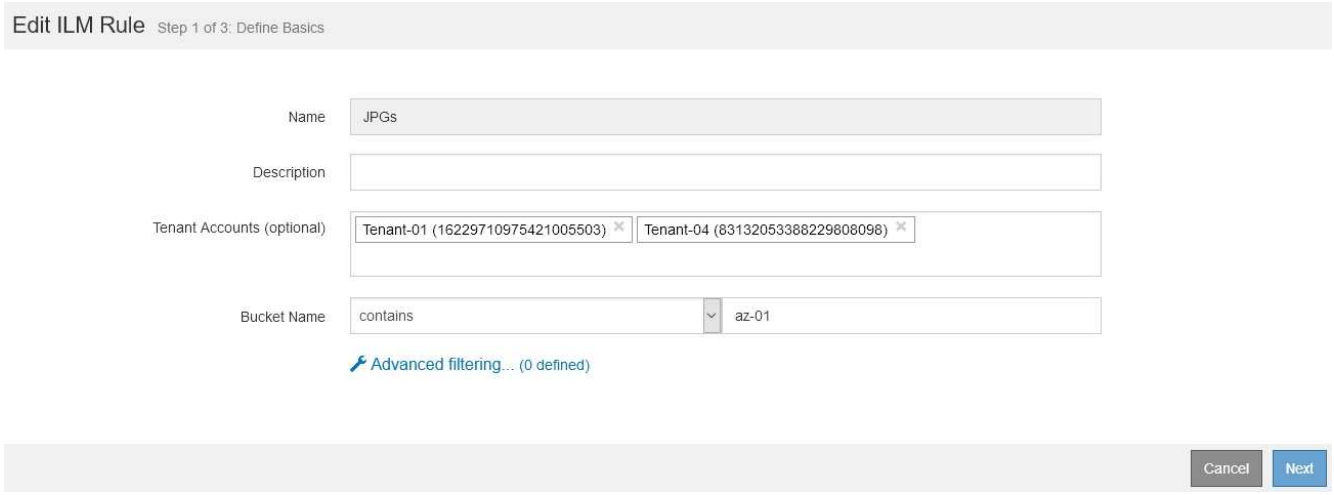
1. ILM * > * 규칙 * 을 선택합니다.

   ILM 규칙 페이지가 나타납니다. 이 페이지에는 사용 가능한 모든 규칙과 활성 정책 또는 제안된 정책에서 사용 중인 규칙이 표시됩니다.

2. 사용하지 않는 규칙을 선택하고 * 편집 * 을 선택합니다.

   ILM 규칙 편집 마법사가 열립니다.

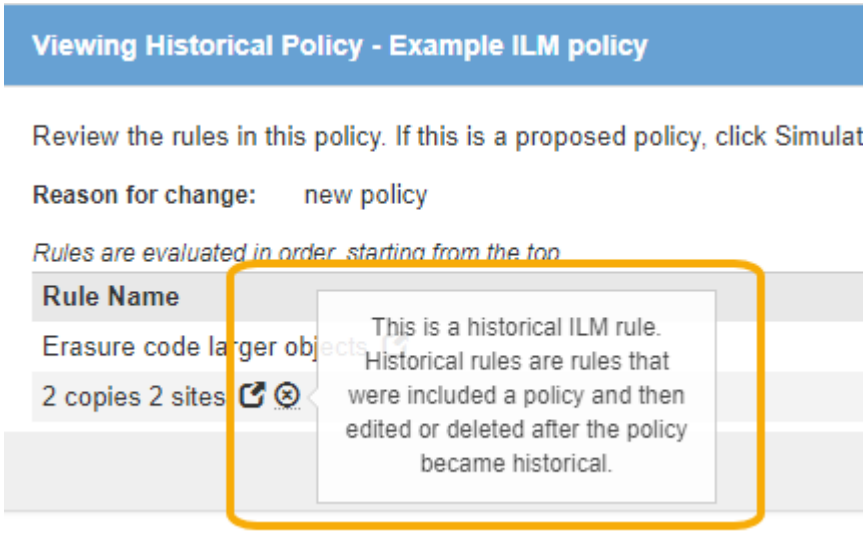
   

3. 에 대한 단계에 따라 ILM 규칙 편집 마법사의 페이지를 완료합니다 ILM 규칙 만들기 및 고급 필터 사용, 필요에 따라.

ILM 규칙을 편집할 때는 해당 이름을 변경할 수 없습니다.

4. 저장 * 을 선택합니다.

내역 정책에서 사용되는 규칙을 편집하는 경우, 은(는) 입니다 ⊗ 규칙을 볼 때 규칙에 대한 아이콘이 나타납니다. 이 아이콘은 규칙이 기록 규칙이 되었음을 나타냅니다.



ILM 규칙 클론 복제

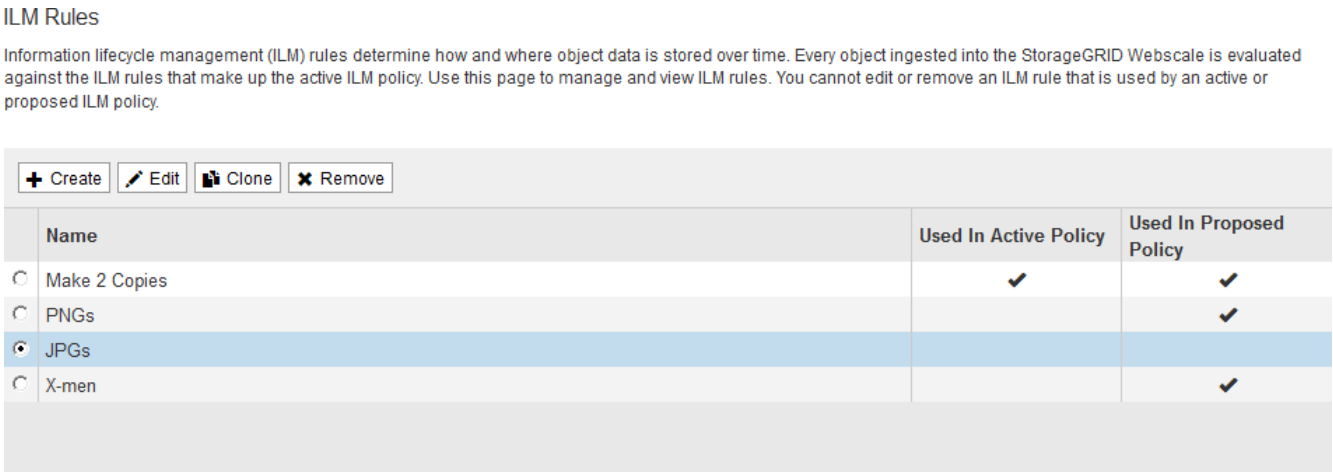
제안된 ILM 정책 또는 활성 ILM 정책에 사용되는 규칙은 편집할 수 없습니다. 대신 규칙을 클론 복제하고 클론 복제된 복사본을 필요한 변경 작업을 수행할 수 있습니다. 그런 다음 필요한 경우 제안된 정책에서 원래 규칙을 제거하고 수정된 버전으로 바꿀 수 있습니다. StorageGRID 버전 10.2 이하를 사용하여 ILM 규칙을 생성한 경우에는 해당 규칙을 복제할 수 없습니다.

활성 ILM 정책에 복제된 규칙을 추가하기 전에 개체의 배치 지침을 변경하면 시스템에 대한 로드가 증가할 수 있습니다.

단계

1. ILM * > * 규칙 * 을 선택합니다.

   ILM 규칙 페이지가 나타납니다.



2. 복제할 ILM 규칙을 선택하고 * Clone * 을 선택합니다.

   ILM 규칙 만들기 마법사가 열립니다.

3. ILM 규칙 편집 및 고급 필터 사용 단계에 따라 복제된 규칙을 업데이트합니다.

   ILM 규칙을 복제할 때 새 이름을 입력해야 합니다.

4. 저장 * 을 선택합니다.

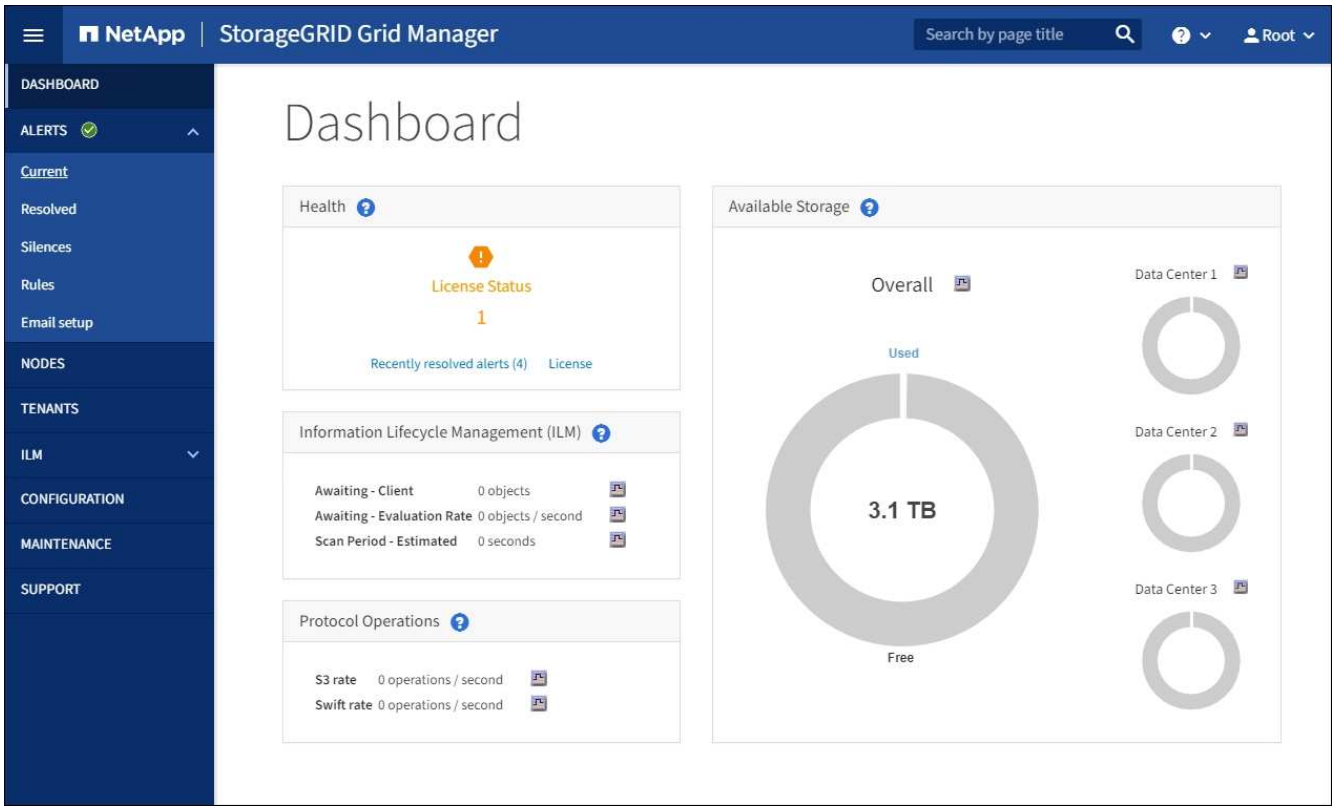
   새 ILM 규칙이 생성됩니다.

ILM 정책 활동 대기열을 봅니다

ILM 정책에 대해 평가할 대기열에 있는 개체의 수를 언제든지 볼 수 있습니다. ILM 처리 대기열을 모니터링하여 시스템 성능을 확인할 수 있습니다. 큐가 크면 시스템이 수집 속도를 따라가지 못하고, 클라이언트 애플리케이션의 로드가 너무 크거나, 일부 비정상적인 상태가 존재함을 나타낼 수 있습니다.

단계

1. 대시보드 * 를 선택합니다.



2. ILM(정보 수명 주기 관리) 섹션을 모니터링합니다.

   물음표를 선택할 수 있습니다 ? 이 섹션의 항목에 대한 설명을 봅니다.

ILM과 함께 S3 오브젝트 잠금을 사용합니다

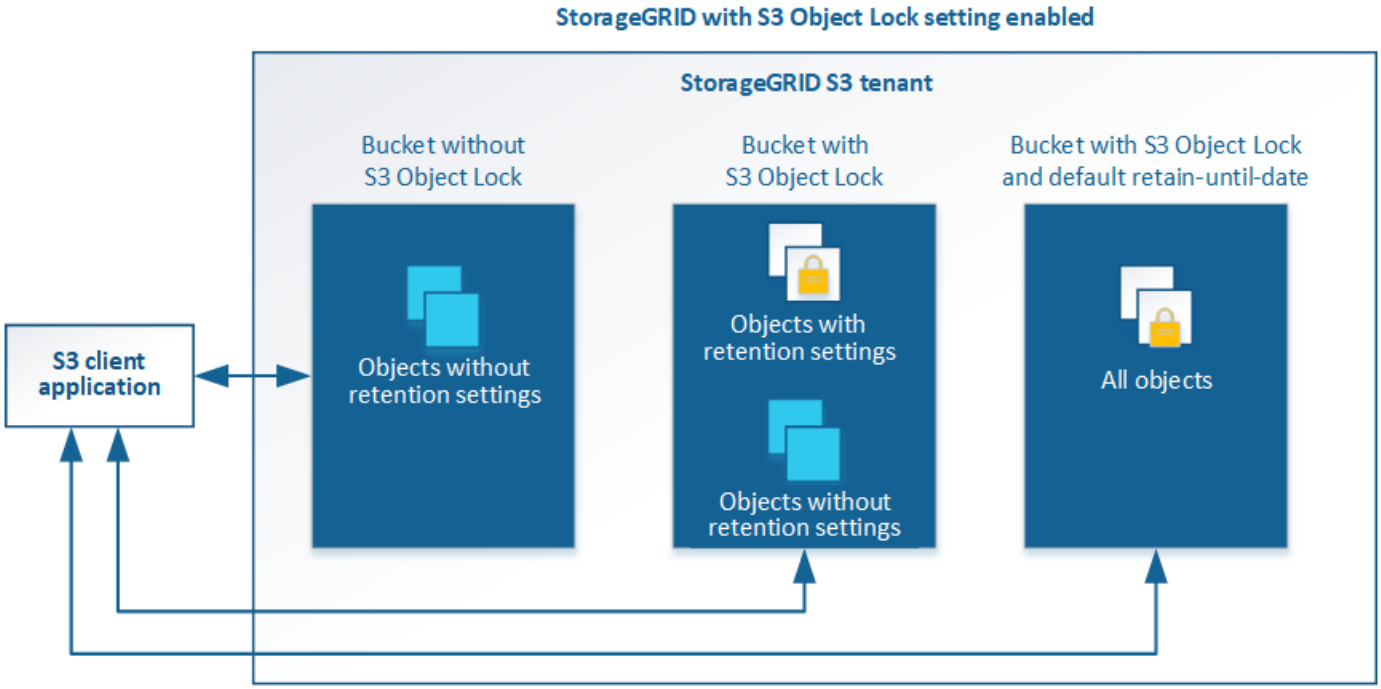
S3 오브젝트 잠금으로 오브젝트 관리

그리드 관리자는 StorageGRID 시스템에 S3 오브젝트 잠금을 설정하고 호환되는 ILM 정책을 구현하여 특정 S3 버킷의 오브젝트가 지정된 시간 동안 삭제 또는 덮어쓰지 않도록 할 수 있습니다.

S3 오브젝트 잠금이란 무엇입니까?

StorageGRID S3 오브젝트 잠금 기능은 Amazon S3(Amazon Simple Storage Service)의 S3 오브젝트 잠금과 동등한 오브젝트 보호 솔루션입니다.

그림에서 볼 수 있듯이 StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정을 사용하면 S3 테넌트 계정이 S3 오브젝트 잠금을 사용하거나 사용하지 않고 버킷을 생성할 수 있습니다. 버킷에 S3 오브젝트 잠금이 설정된 경우 S3 클라이언트 애플리케이션이 해당 버킷의 모든 오브젝트 버전에 대한 보존 설정을 선택적으로 지정할 수 있습니다. 오브젝트 버전에 S3 오브젝트 잠금으로 보호할 보존 설정이 지정되어 있어야 합니다. 또한 S3 오브젝트 잠금이 활성화된 각 버킷에는 선택적으로 기본 보존 모드 및 보존 기간이 있을 수 있으며, 이 기간은 객체가 고유한 보존 설정 없이 버킷에 추가되는 경우에 적용됩니다.



StorageGRID S3 오브젝트 잠금 기능은 Amazon S3 규정 준수 모드에 상응하는 단일 보존 모드를 제공합니다. 기본적으로 보호된 개체 버전은 사용자가 덮어쓰거나 삭제할 수 없습니다. StorageGRID S3 오브젝트 잠금 기능은 거버넌스 모드를 지원하지 않으며, 특별한 권한이 있는 사용자가 보존 설정을 무시하거나 보호된 오브젝트를 삭제할 수 없습니다.

버킷에 S3 오브젝트 잠금이 활성화된 경우 오브젝트를 생성하거나 업데이트할 때 S3 클라이언트 애플리케이션에서 다음 오브젝트 레벨 보존 설정 중 하나 또는 모두를 선택적으로 지정할 수 있습니다.

- * Retain-until-date *: 개체 버전의 Retain-until-date가 미래인 경우 개체를 검색할 수 있지만 수정하거나 삭제할 수 없습니다. 필요에 따라 오브젝트의 보존 기간(Retain-until-date)을 늘릴 수 있지만 이 날짜는 줄일 수 없습니다.
- * 법적 증거 자료 보관 *: 개체 버전에 법적 증거 자료 보관 기능을 적용하면 해당 개체가 즉시 잠깁니다. 예를 들어

조사 또는 법적 분쟁과 관련된 객체에 법적 보류를 지정해야 할 수 있습니다. 법적 보류는 만료 날짜가 없지만 명시적으로 제거될 때까지 유지됩니다. 법적 보류는 보존 기한 과 무관합니다.

개체 보존 설정에 대한 자세한 내용은 를 참조하십시오 S3 오브젝트 잠금을 사용합니다.

기본 버킷 고정 설정에 대한 자세한 내용은 을 참조하십시오 S3 오브젝트 잠금 기본 버킷 보존을 사용합니다.

S3 오브젝트 잠금을 레거시 규정 준수와 비교합니다

S3 오브젝트 잠금은 이전 StorageGRID 버전에서 사용할 수 있었던 규정 준수 기능을 대체합니다. S3 오브젝트 잠금 기능이 Amazon S3 요구 사항을 준수하므로, 이제 ""레거시 규정 준수""라고 하는 독점적인 StorageGRID 규정 준수 기능을 더 이상 사용하지 않습니다.

이전에 글로벌 규정 준수 설정을 활성화한 경우 글로벌 S3 오브젝트 잠금 설정이 자동으로 활성화됩니다. 테넌트 사용자는 더 이상 Compliance를 활성화한 상태로 새 버킷을 생성할 수 없지만, 필요에 따라 테넌트 사용자는 기존 레거시 준수 버킷을 계속 사용하고 관리할 수 있습니다. 여기에는 다음 작업이 포함됩니다.

- 레거시 규정 준수 기능이 활성화된 기존 버킷에 새 객체 인스팅
- 레거시 규정 준수를 활성화한 기존 버킷의 보존 기간 증가
- 레거시 규정 준수 기능이 활성화된 기존 버킷의 자동 삭제 설정을 변경합니다.
- 레거시 규정 준수 기능이 활성화된 기존 버킷에 법적 증거 자료 보관
- 법적 증거 자료 보관

을 참조하십시오 "NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법" 를 참조하십시오.

이전 버전의 StorageGRID에서 레거시 규정 준수 기능을 사용한 경우 다음 표를 참조하여 StorageGRID의 S3 오브젝트 잠금 기능과 어떻게 다른지 알아보십시오.

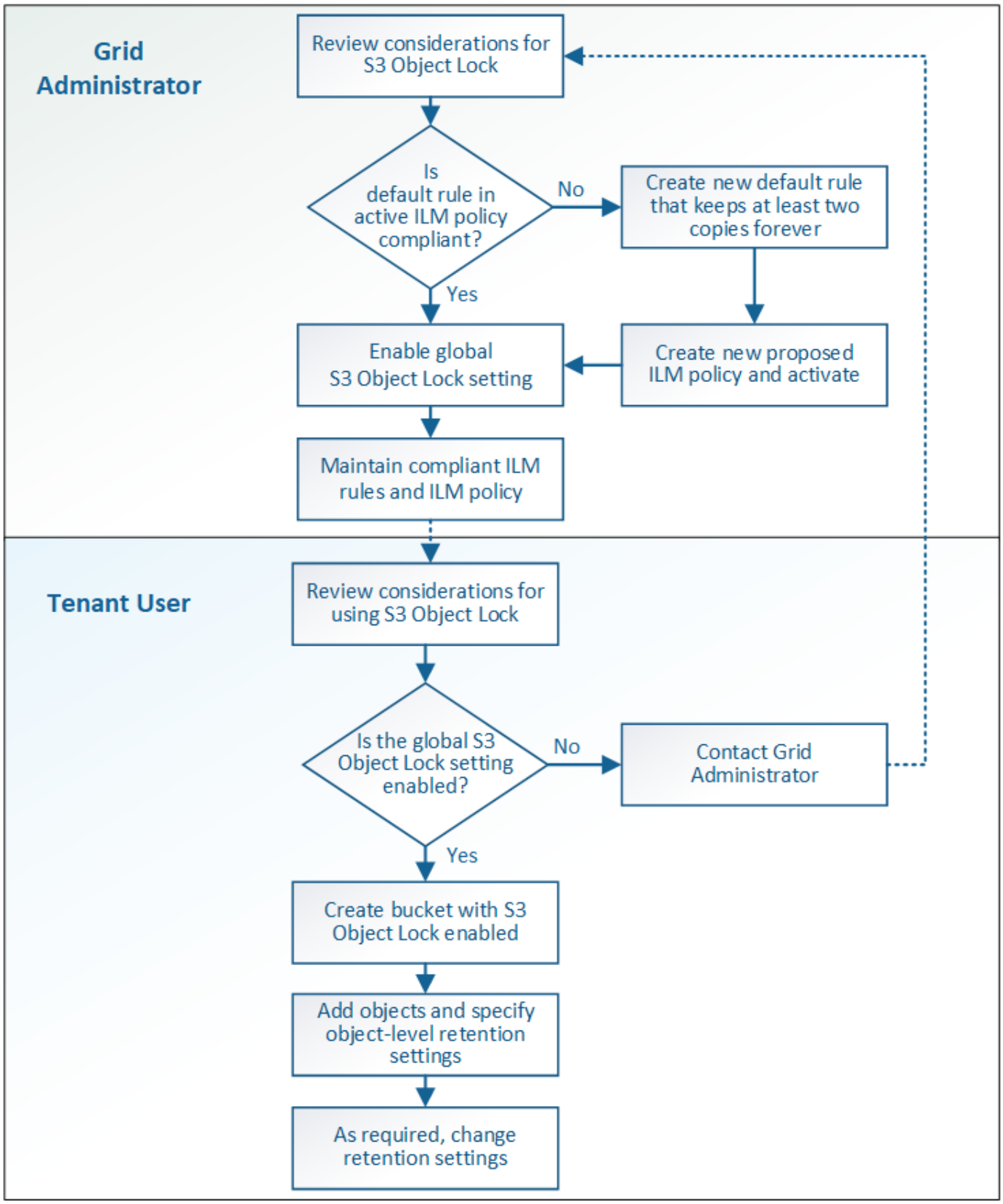
	S3 오브젝트 잠금(신규)	규정 준수(레거시)
이 기능은 전역적으로 어떻게 활성화됩니까?	그리드 관리자에서 * 구성 * > * 시스템 * > * S3 오브젝트 잠금 * 을 선택합니다.	더 이상 지원되지 않습니다. • 참고: * 이전 버전의 StorageGRID를 사용하여 글로벌 규정 준수 설정을 활성화한 경우 StorageGRID 11.6에서 S3 개체 잠금 설정이 활성화됩니다. StorageGRID를 계속 사용하여 기존 준수 버킷의 설정을 관리할 수 있지만 새로운 준수 버킷을 생성할 수는 없습니다.
버킷에 대한 기능은 어떻게 활성화됩니까?	사용자는 테넌트 관리자, 테넌트 관리 API 또는 S3 REST API를 사용하여 새 버킷을 생성할 때 S3 오브젝트 잠금을 활성화해야 합니다.	사용자는 더 이상 Compliance를 활성화한 상태로 새 버킷을 생성할 수 없지만 기존의 준수 버켓에 새 객체를 계속 추가할 수 있습니다.

	S3 오브젝트 잠금(신규)	규정 준수(레거시)
버킷 버전 관리가 지원됩니까?	예. 버킷에 대해 S3 오브젝트 잠금이 활성화된 경우 버킷 버전 관리가 필요하며 자동으로 활성화됩니다.	아니요 레거시 준수 기능은 버킷 버전 관리를 허용하지 않습니다.
개체 보존은 어떻게 설정됩니까?	사용자는 각 개체 버전에 대해 보존 종료 날짜를 설정할 수 있습니다.	사용자는 전체 버킷의 보존 기간을 설정해야 합니다. 보존 기간은 버킷의 모든 객체에 적용됩니다.
버킷에 보존 및 법적 보관에 대한 기본 설정이 있습니까?	예. S3 오브젝트 잠금이 설정된 StorageGRID 버킷은 수집 중에 지정된 자체 보존 설정이 없는 오브젝트 버전에 적용되는 기본 보존 기간을 가질 수 있습니다.	예
보존 기간을 변경할 수 있습니까?	개체 버전의 보존 기한 은 늘릴 수 있지만 줄일 수는 없습니다.	버킷의 보존 기간은 늘릴 수 있지만 줄일 수는 없습니다.
법적 보류가 통제되는 곳은 어디입니까?	사용자는 법적 증거 자료 보관 또는 버킷의 모든 개체 버전에 대한 법적 증거 자료 보관 장치를 들어 올릴 수 있습니다.	법적 구속이 버킷에 배치되어 버킷의 모든 물체에 영향을 미칩니다.
언제 오브젝트를 삭제할 수 있습니까?	개체가 법적 증거 자료 보관 중이 아닌 경우, 보존 기한 에 도달한 후에 개체 버전을 삭제할 수 있습니다.	버킷이 법적 증거 자료 보관 중이 아닌 경우, 보존 기간이 만료된 후에는 오브젝트를 삭제할 수 있습니다. 개체를 자동으로 또는 수동으로 삭제할 수 있습니다.
버킷 라이프사이클 구성이 지원됩니까?	예	아니요

S3 오브젝트 잠금 워크플로

그리드 관리자는 테넌트 사용자와 긴밀하게 협력하여 보존 요구 사항을 충족하는 방식으로 객체가 보호되도록 해야 합니다.

워크플로우 다이어그램은 S3 오브젝트 잠금을 사용하기 위한 상위 단계를 보여줍니다. 이러한 단계는 그리드 관리자 및 테넌트 사용자가 수행합니다.



그리드 관리 작업

워크플로우 다이어그램에 표시된 것처럼, 그리드 관리자는 S3 테넌트 사용자가 S3 오브젝트 잠금을 사용하기 전에 다음과 같은 두 가지 높은 수준의 작업을 수행해야 합니다.

1. 호환되는 ILM 규칙을 하나 이상 생성하고 해당 규칙을 활성 ILM 정책의 기본 규칙으로 설정합니다.
2. 전체 StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정을 활성화합니다.

테넌트 사용자 작업

전역 S3 오브젝트 잠금 설정이 활성화된 후 테넌트는 다음 작업을 수행할 수 있습니다.

1. S3 오브젝트 잠금이 활성화된 버킷을 생성합니다.
2. 버킷의 기본 보존 설정을 지정합니다. 버킷은 고유한 보존 설정을 지정하지 않는 버킷에 추가된 오브젝트에 적용됩니다.
3. 이러한 버킷에 오브젝트를 추가하고 오브젝트 레벨 보존 기간 및 법적 보존 설정을 지정합니다.
4. 필요에 따라 보존 기간을 업데이트하거나 개별 객체에 대한 법적 보류 설정을 변경합니다.

관련 정보

- 테넌트 계정을 사용합니다
- S3을 사용합니다
- S3 오브젝트 잠금 기본 버킷 보존을 사용합니다

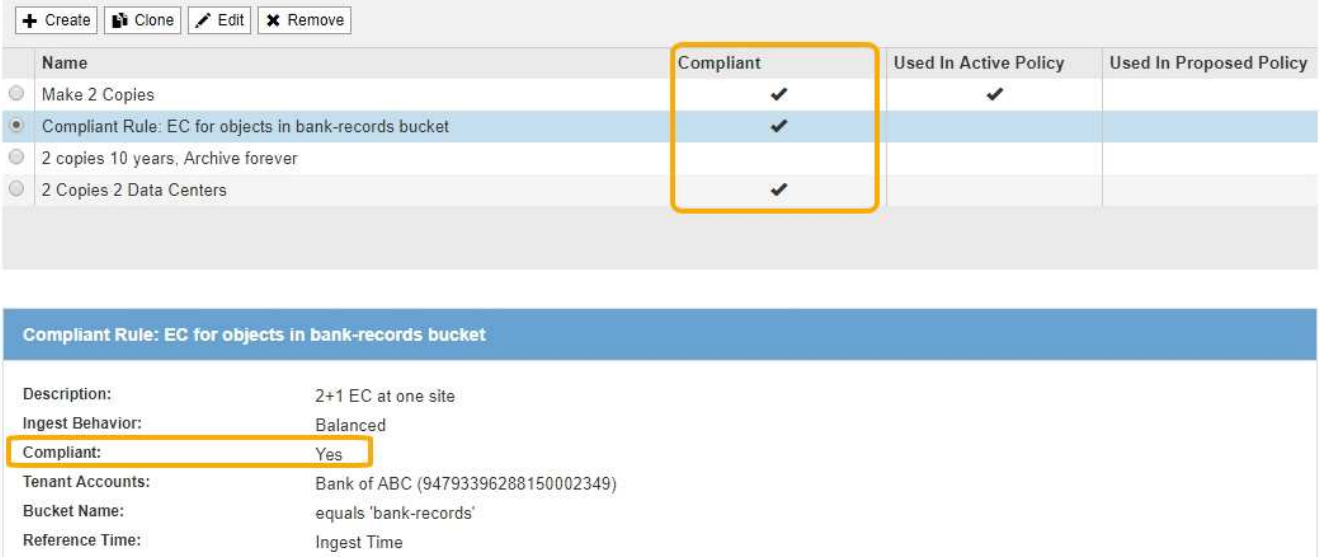
S3 오브젝트 잠금에 대한 요구사항

글로벌 S3 오브젝트 잠금 설정을 사용하기 위한 요구사항, 호환되는 ILM 규칙 및 ILM 정책을 만들기 위한 요구사항 및 StorageGRID가 S3 오브젝트 잠금을 사용하는 버킷과 오브젝트에 배치하는 제한을 검토해야 합니다.

전역 **S3** 오브젝트 잠금 설정 사용 요구 사항

- S3 테넌트가 S3 오브젝트 잠금이 활성화된 버킷을 생성하려면 먼저 그리드 관리자 또는 그리드 관리 API를 사용하여 글로벌 S3 오브젝트 잠금 설정을 활성화해야 합니다.
- 글로벌 S3 오브젝트 잠금 설정을 활성화하면 모든 S3 테넌트 계정에서 S3 오브젝트 잠금이 설정된 버킷을 생성할 수 있습니다.
- 전역 S3 오브젝트 잠금 설정을 활성화한 후에는 설정을 비활성화할 수 없습니다.
- 활성 ILM 정책의 기본 규칙이 호환(즉, 기본 규칙이 S3 오브젝트 잠금이 활성화된 버킷의 요구 사항을 준수해야 함)인 경우에만 전역 S3 오브젝트 잠금을 활성화할 수 있습니다.
- 전역 S3 개체 잠금 설정이 활성화된 경우 정책의 기본 규칙이 규정을 준수하지 않는 한 새로 제안된 ILM 정책을 생성하거나 기존의 제안된 ILM 정책을 활성화할 수 없습니다. 전역 S3 개체 잠금 설정이 활성화된 후 ILM 규칙 및 ILM 정책 페이지는 어떤 ILM 규칙이 준수되는지 나타냅니다.

  다음 예제에서 ILM 규칙 페이지에는 S3 오브젝트 잠금이 활성화된 버킷과 호환되는 세 가지 규칙이 나열되어 있습니다.

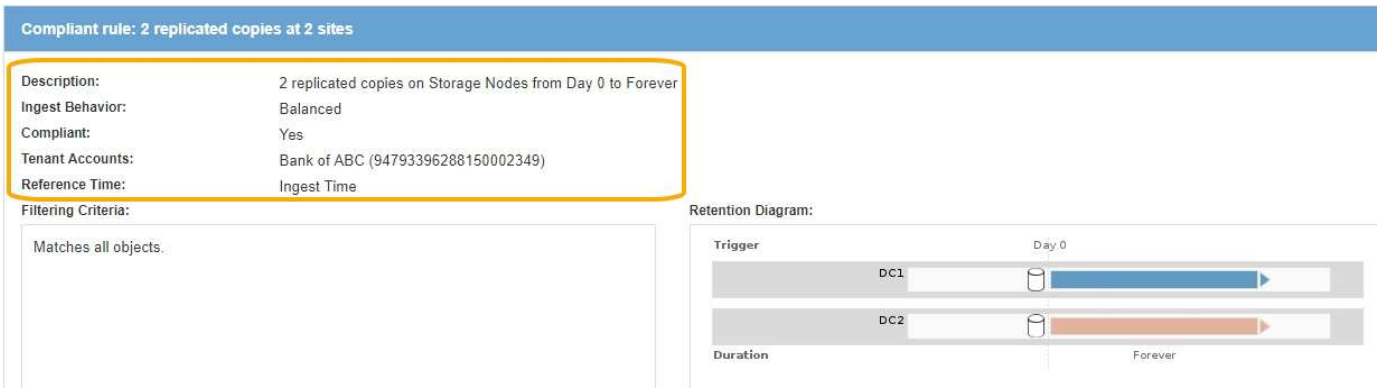


규정 준수 **ILM** 규칙 요구 사항

전역 S3 오브젝트 잠금 설정을 활성화하려면 활성 ILM 정책의 기본 규칙이 준수되는지 확인해야 합니다. 규정 준수 규칙은 S3 오브젝트 잠금이 활성화된 두 버킷의 요구 사항과 레거시 규정 준수가 활성화된 기존 버킷의 요구 사항을 모두 충족합니다.

- 복제된 오브젝트 복사본 2개 이상 또는 삭제 코딩 복사본 1개를 생성해야 합니다.
- 이러한 복제본은 배치 지침에서 각 행의 전체 기간 동안 스토리지 노드에 있어야 합니다.
- 오브젝트 복사본은 클라우드 스토리지 풀에 저장할 수 없습니다.
- 오브젝트 복사본은 아카이브 노드에 저장할 수 없습니다.
- 최소 한 줄의 배치 지침은 * Ingest Time * 을 기준 시간으로 사용하여 0일에 시작해야 합니다.
- 적어도 한 줄의 배치 지침은 영원히 있어야 합니다.

예를 들어 이 규칙은 S3 오브젝트 잠금이 설정된 버킷의 요구 사항을 충족합니다. 이 제품은 Ingest Time(0일)에서 ""Forever""로 복제된 오브젝트 복사본 2개를 저장합니다. 오브젝트는 두 데이터 센터의 스토리지 노드에 저장됩니다.



활성 및 제안된 **ILM** 정책에 대한 요구 사항

전역 S3 개체 잠금 설정이 활성화되면 활성 및 제안된 ILM 정책에 규정 준수 및 비준수 규칙이 모두 포함될 수 있습니다.

- 활성 또는 제안된 ILM 정책의 기본 규칙은 반드시 준수해야 합니다.

- 비준수 규칙은 S3 오브젝트 잠금이 활성화되지 않았거나 레거시 규정 준수 기능이 활성화되지 않은 버킷의 오브젝트에만 적용됩니다.
- 규정 준수 규칙은 모든 버킷의 오브젝트에 적용할 수 있습니다. 버킷에 대해 S3 오브젝트 잠금이나 레거시 규정 준수를 활성화할 필요는 없습니다.

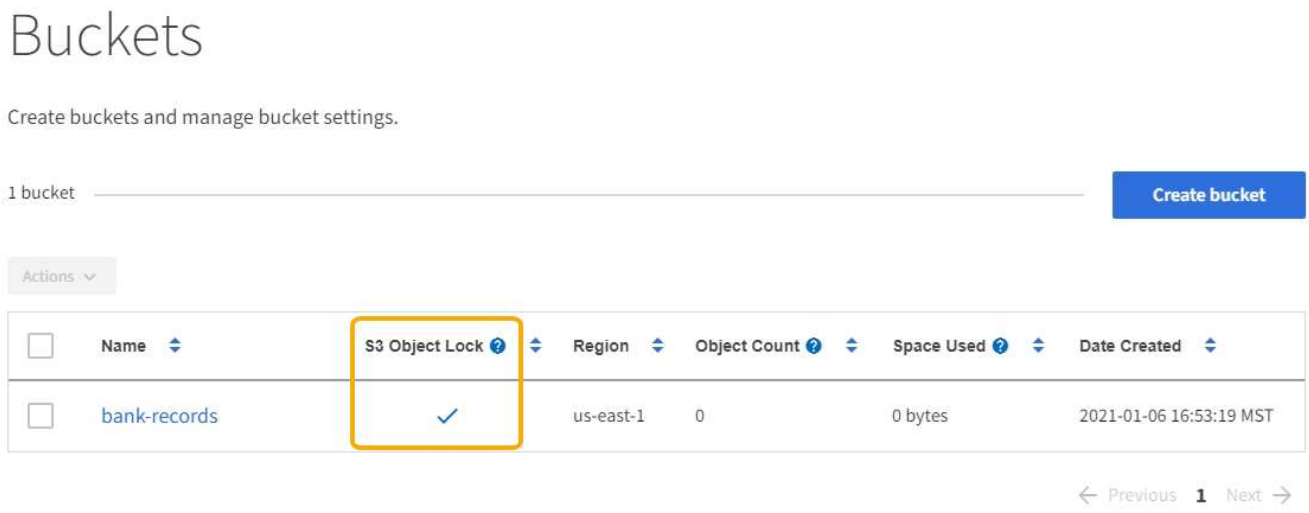
호환되는 ILM 정책에는 다음 세 가지 규칙이 포함될 수 있습니다.

1. S3 오브젝트 잠금이 설정된 특정 버킷에서 오브젝트의 삭제 코딩 복사본을 생성하는 규정 준수 규칙 EC 복사본은 0일째부터 영원까지 스토리지 노드에 저장됩니다.
2. 1년 동안 스토리지 노드에 복제된 오브젝트 복사본 2개를 생성한 다음 오브젝트 복사본 하나를 아카이브 노드로 이동하여 복사본을 영구히 저장하는 규정을 준수하지 않습니다. 이 규칙은 S3 오브젝트 잠금이나 레거시 규정 준수를 사용하지 않는 버킷에만 적용됩니다. 왜냐하면 단일 오브젝트 복사본만 영구 저장하고 아카이브 노드를 사용하기 때문입니다.
3. 스토리지 노드에 2개의 복제된 오브젝트 복사본을 만드는 기본 규정 준수 규칙입니다. 이 규칙은 처음 두 규칙에 의해 필터링되지 않은 버킷의 모든 오브젝트에 적용됩니다.

S3 오브젝트 잠금이 설정된 버킷의 요구 사항

- StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 테넌트 관리자, 테넌트 관리 API 또는 S3 REST API를 사용하여 S3 오브젝트 잠금이 활성화된 버킷을 생성할 수 있습니다.

  테넌트 관리자의 이 예에서는 S3 오브젝트 잠금이 설정된 버킷을 보여 줍니다.



- S3 오브젝트 잠금을 사용하려는 경우 버킷을 생성할 때 S3 오브젝트 잠금을 활성화해야 합니다. 기존 버킷에 대해 S3 오브젝트 잠금을 활성화할 수 없습니다.
- S3 오브젝트 잠금에서 버킷 버전 관리가 필요합니다. 버킷에 대해 S3 오브젝트 잠금이 활성화된 경우 StorageGRID는 해당 버킷의 버전 관리를 자동으로 활성화합니다.
- S3 오브젝트 잠금이 설정된 버킷을 생성한 후에는 해당 버켓에 대한 S3 오브젝트 잠금을 비활성화하거나 버전 관리를 일시 중단할 수 없습니다.
- 필요에 따라 버킷의 기본 보존을 구성할 수 있습니다. 개체 버전이 업로드되면 기본 보존 기간이 개체 버전에 적용됩니다. 객체 버전 업로드 요청에 보존 모드와 보존 기간을 지정하여 버킷 기본값을 재정의할 수 있습니다.
- S3 오브젝트 라이프사이클 버킷에 대해 버킷 라이프사이클 구성이 지원됩니다.
- S3 오브젝트 잠금이 설정된 버킷에는 CloudMirror 복제가 지원되지 않습니다.

S3 오브젝트 잠금이 설정된 버킷의 오브젝트 요구사항

- 오브젝트 버전을 보호하려면 S3 클라이언트 애플리케이션이 버킷 기본 보존을 구성하거나 각 업로드 요청에서 보존 설정을 지정해야 합니다.
- 개체 버전에 대한 보존 기간을 늘릴 수 있지만 이 값을 줄일 수는 없습니다.
- 법적 조치 또는 규제 조사가 보류 중인 경우 개체 버전에 법적 증거 자료를 두어 관련 정보를 보존할 수 있습니다. 개체 버전이 법적 증거 자료 보관 중인 경우, 해당 개체가 보존 기한 에 도달한 경우에도 StorageGRID에서 해당 개체를 삭제할 수 없습니다. 법적 증거 자료 보관 기간이 해제됨과 동시에, 보존 기한이 만료된 경우 개체 버전을 삭제할 수 있습니다.
- S3 오브젝트 잠금에는 버전 관리되는 버킷을 사용해야 합니다. 보존 설정은 개별 개체 버전에 적용됩니다. 개체 버전에는 보존 기한 및 법적 보류 설정이 둘 다 있을 수 있으며, 둘 중 하나만 설정할 수도 있고 둘 다 가질 수도 없습니다. 개체에 대한 보존 기한 또는 법적 보류 설정을 지정하면 요청에 지정된 버전만 보호됩니다. 이전 버전의 개체는 잠겨 있는 상태에서 새 버전의 개체를 만들 수 있습니다.

S3 오브젝트 잠금이 설정된 버킷의 오브젝트 라이프사이클

S3 오브젝트 잠금이 설정된 버킷에 저장된 각 오브젝트는 다음 3단계를 거칩니다.

1. * 오브젝트 수집 *
   - S3 오브젝트 잠금이 설정된 버킷에 오브젝트 버전을 추가할 경우 S3 클라이언트 애플리케이션이 기본 버킷 보존 설정을 사용하거나 선택적으로 오브젝트에 대한 보존 설정을 지정할 수 있습니다(보존 기한, 법적 보류 또는 둘 다). 그런 다음 StorageGRID에서는 해당 개체의 메타데이터를 생성하며 고유한 UUID(Object Identifier)와 수집 날짜 및 시간이 포함됩니다.
   - 보존 설정이 포함된 오브젝트 버전을 수집하면 해당 데이터와 S3 사용자 정의 메타데이터를 수정할 수 없습니다.
   - StorageGRID는 오브젝트 메타데이터를 오브젝트 데이터와 독립적으로 저장합니다. 이 기능은 각 사이트에서 모든 오브젝트 메타데이터의 복사본을 3개 유지 관리합니다.
2. * 개체 보존 *
   - 개체의 여러 복사본이 StorageGRID에 저장됩니다. 정확한 복제본 수와 유형 및 스토리지 위치는 활성 ILM 정책의 규정 준수 규칙에 따라 결정됩니다.
3. * 개체 삭제 *
   - 보존 기한 에 도달하면 개체를 삭제할 수 있습니다.
   - 법적 증거 자료 보관 중인 개체는 삭제할 수 없습니다.

관련 정보

- 테넌트 계정을 사용합니다
- S3을 사용합니다
- S3 오브젝트 잠금을 레거시 규정 준수와 비교합니다
- 예 7: S3 오브젝트 잠금에 대한 규정 준수 ILM 정책
- 감사 로그를 검토합니다
- S3 오브젝트 잠금 기본 버킷 보존을 사용합니다.

S3 오브젝트 잠금을 전역적으로 활성화합니다

오브젝트 데이터를 저장할 때 S3 테넌트 계정이 규정 요구사항을 준수해야 하는 경우 전체 StorageGRID 시스템에 대해 S3 오브젝트 잠금을 활성화해야 합니다. 글로벌 S3 오브젝트 잠금 설정을 활성화하면 모든 S3 테넌트 사용자가 S3 오브젝트 잠금을 통해 버킷과 오브젝트를 생성하고 관리할 수 있습니다.

필요한 것

- 루트 액세스 권한이 있습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- S3 오브젝트 잠금 워크플로우를 검토했으며 고려 사항을 이해해야 합니다.
- 활성 ILM 정책의 기본 규칙은 준수입니다.
  - 기본 ILM 규칙을 생성합니다
  - ILM 정책을 생성합니다

이 작업에 대해

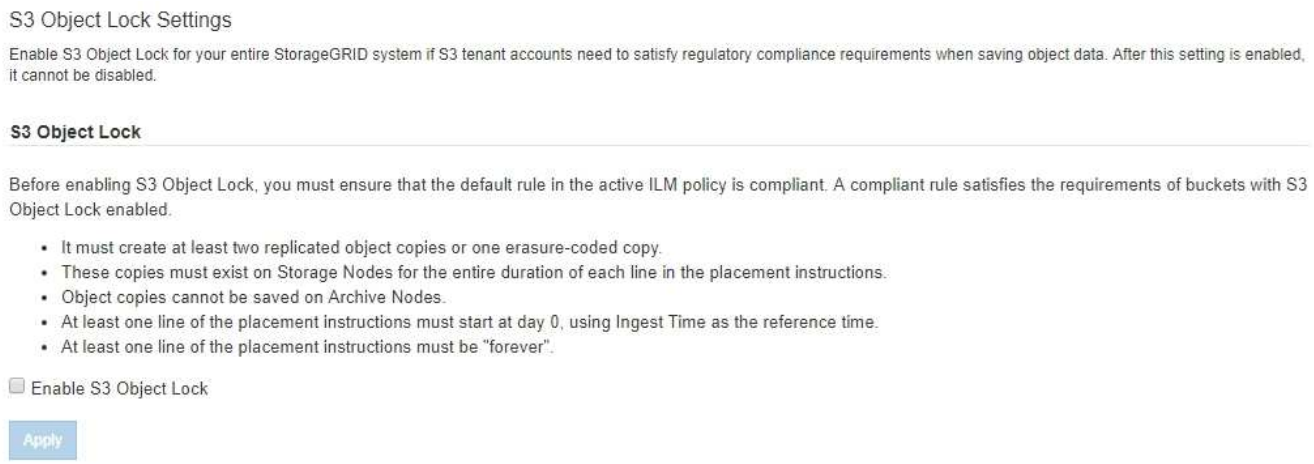
그리드 관리자는 글로벌 S3 오브젝트 잠금 설정을 활성화하여 테넌트 사용자가 S3 오브젝트 잠금이 활성화된 새 버킷을 생성할 수 있도록 해야 합니다. 이 설정을 활성화한 후에는 비활성화할 수 없습니다.

> 이전 버전의 StorageGRID를 사용하여 글로벌 규정 준수 설정을 활성화한 경우 StorageGRID 11.6에서 S3 개체 잠금 설정이 활성화됩니다. StorageGRID를 계속 사용하여 기존 준수 버킷의 설정을 관리할 수 있지만 새로운 준수 버킷을 생성할 수는 없습니다. 을 참조하십시오 "NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법".

단계

1. 구성 * > * 시스템 * > * S3 오브젝트 잠금 * 을 선택합니다.

   S3 오브젝트 잠금 설정 페이지가 나타납니다.

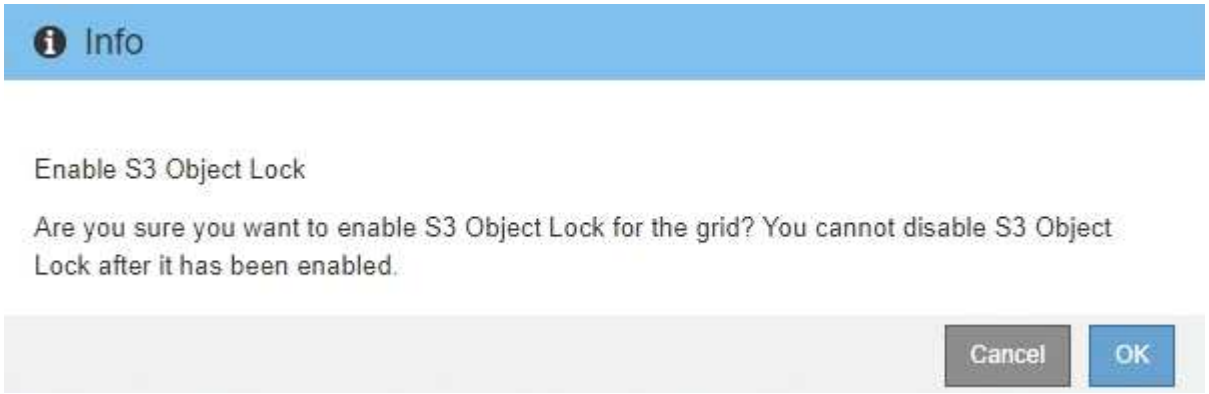


   이전 버전의 StorageGRID를 사용하여 글로벌 규정 준수 설정을 활성화한 경우 다음 참고 사항이 페이지에 포함됩니다.

The S3 Object Lock setting replaces the legacy Compliance setting. When this setting is enabled, tenant users can create buckets with S3 Object Lock enabled. Tenants who previously created buckets for the legacy Compliance feature can manage their existing buckets, but can no longer create new buckets with legacy Compliance enabled. See Managing objects with information lifecycle management for information.

2. S3 오브젝트 잠금 활성화 * 를 선택합니다.
3. Apply * 를 선택합니다.

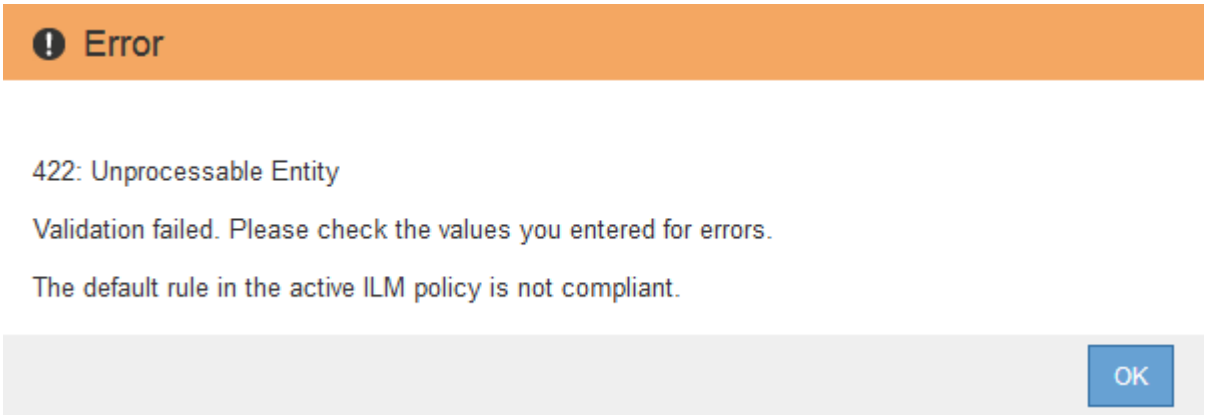
   S3 오브젝트 잠금을 사용하도록 설정한 후 해제할 수 없다는 확인 대화 상자가 나타납니다.



4. 전체 시스템에 대해 S3 오브젝트 잠금을 영구적으로 활성화하려면 * OK * 를 선택합니다.

   OK * 를 선택한 경우:

   - 활성 ILM 정책의 기본 규칙이 준수되면 S3 오브젝트 잠금이 전체 그리드에 대해 활성화되며 비활성화할 수 없습니다.
   - 기본 규칙이 규정을 준수하지 않으면 규정 준수 규칙을 기본 규칙으로 포함하는 새 ILM 정책을 만들고 활성화해야 함을 나타내는 오류가 나타납니다. OK * 를 선택하고 새 제안된 정책을 생성하고 시뮬레이션한 후 활성화합니다.



작업을 마친 후

전역 S3 오브젝트 잠금 설정을 활성화한 후 가 필요할 수 있습니다 기본 규칙을 만듭니다 준수해야 합니다 ILM 정책을 생성합니다 준수해야 합니다. 설정을 활성화한 후 ILM 정책에 준수 기본 규칙과 비준수 기본 규칙이 모두 선택적으로 포함될 수 있습니다. 예를 들어, S3 오브젝트 잠금이 활성화되지 않은 버킷의 오브젝트에 대한 필터가 없는 규정을 준수하지 않는 규칙을 사용할 수 있습니다.

관련 정보

- S3 오브젝트 잠금을 레거시 규정 준수와 비교합니다

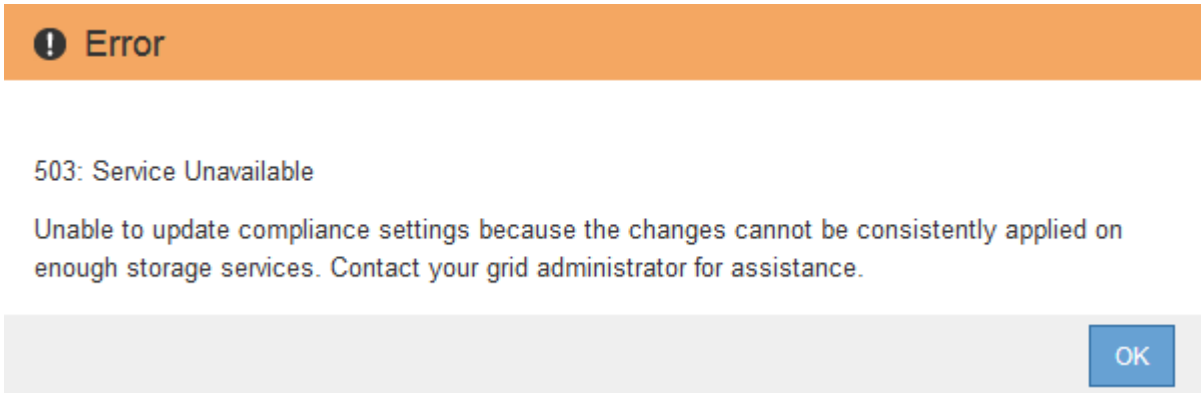
S3 오브젝트 잠금 또는 레거시 규정 준수 구성을 업데이트할 때 일관성 오류를 해결합니다

사이트의 데이터 센터 사이트 또는 여러 스토리지 노드를 사용할 수 없게 된 경우, S3 테넌트 사용자가 S3 오브젝트 잠금 또는 레거시 규정 준수 구성에 변경 사항을 적용할 수 있도록 도와야 할 수 있습니다.

S3 오브젝트 잠금(또는 레거시 규정 준수)이 설정된 버킷이 있는 테넌트 사용자는 특정 설정을 변경할 수 있습니다. 예를 들어, S3 오브젝트 잠금을 사용하는 테넌트 사용자는 오브젝트 버전을 법적 증거 자료 보관 상태로 두어야 할 수 있습니다.

테넌트 사용자가 S3 버킷 또는 오브젝트 버전에 대한 설정을 업데이트하면 StorageGRID는 그리드 전체에서 버킷 또는 오브젝트 메타데이터를 즉시 업데이트하려고 시도합니다. 데이터 센터 사이트 또는 여러 스토리지 노드를 사용할 수 없어 시스템에서 메타데이터를 업데이트할 수 없는 경우 오류 메시지가 표시됩니다. 주요 내용은 다음과 같습니다.

- 테넌트 관리자 사용자에게는 다음 오류 메시지가 표시됩니다.



- 테넌트 관리 API 사용자와 S3 API 사용자는 유사한 메시지 텍스트와 함께 503 서비스 사용 불가 응답 코드를 받습니다.

이 오류를 해결하려면 다음 단계를 수행하십시오.

1. 가능한 한 빨리 모든 스토리지 노드 또는 사이트를 다시 사용할 수 있도록 합니다.
2. 각 사이트에서 스토리지 노드를 충분히 사용할 수 없는 경우 기술 지원 부서에 문의하십시오. 기술 지원 담당자는 노드를 복구하도록 지원하고 변경 사항이 그리드 전체에 일관되게 적용되도록 할 수 있습니다.
3. 기본 문제가 해결되면 테넌트 사용자에게 구성 변경을 다시 시도하도록 알립니다.

관련 정보

- 테넌트 계정을 사용합니다
- S3을 사용합니다
- 복구 및 유지 관리

ILM 규칙 및 정책의 예

예 **1:** 오브젝트 스토리지에 대한 **ILM** 규칙 및 정책

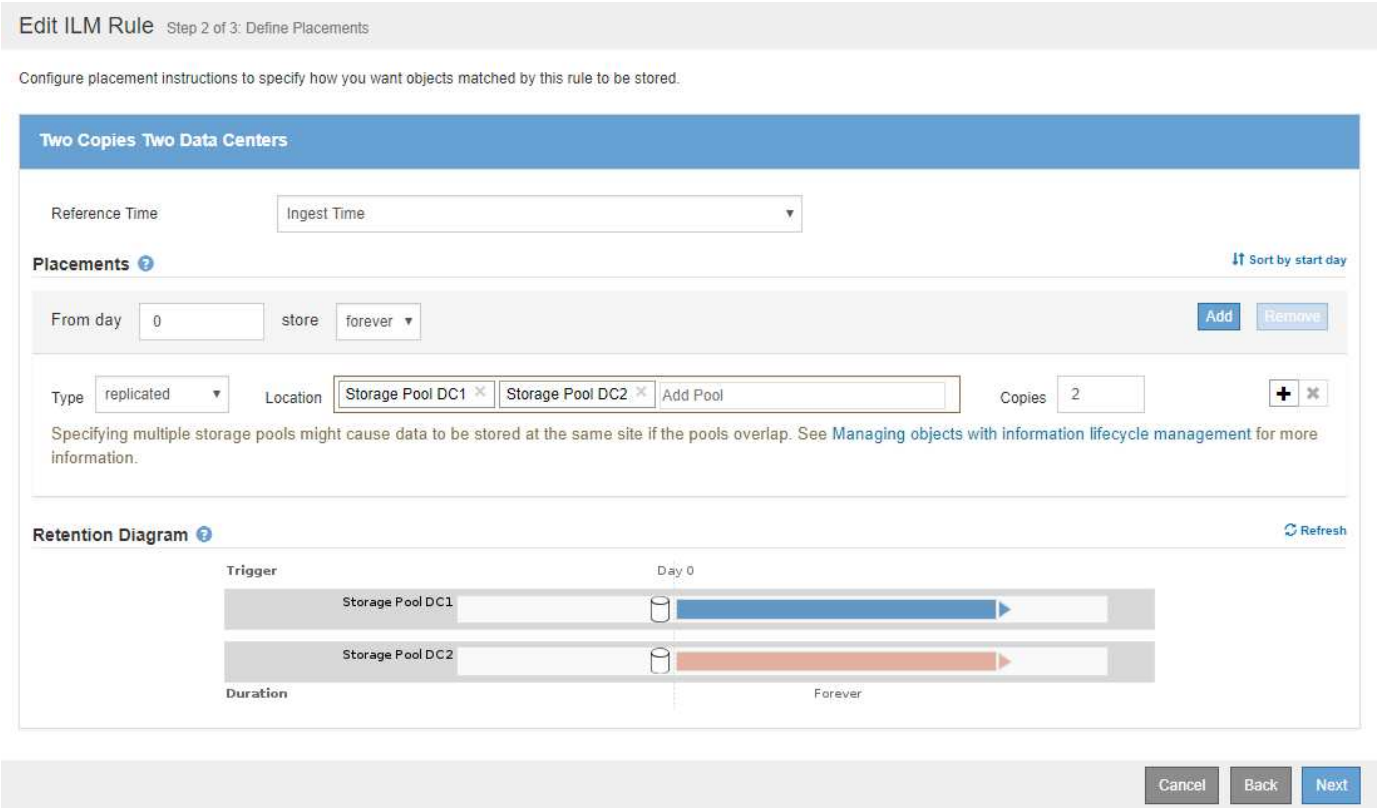
ILM 정책을 정의하여 개체 보호 및 보존 요구 사항을 충족할 때 다음 예제 규칙 및 정책을 출발점으로 사용할 수 있습니다.

> 다음 ILM 규칙 및 정책은 예일 뿐입니다. ILM 규칙을 구성하는 방법은 여러 가지가 있습니다. 새 정책을 활성화하기 전에 제안된 정책을 시뮬레이션하여 콘텐츠가 손실로부터 보호되도록 의도한 대로 동작하는지 확인합니다.

예를 들어 **ILM** 규칙 **1:** 개체 데이터를 두 데이터 센터에 복사

이 ILM 규칙 예에서는 오브젝트 데이터를 두 데이터 센터의 스토리지 풀로 복사합니다.

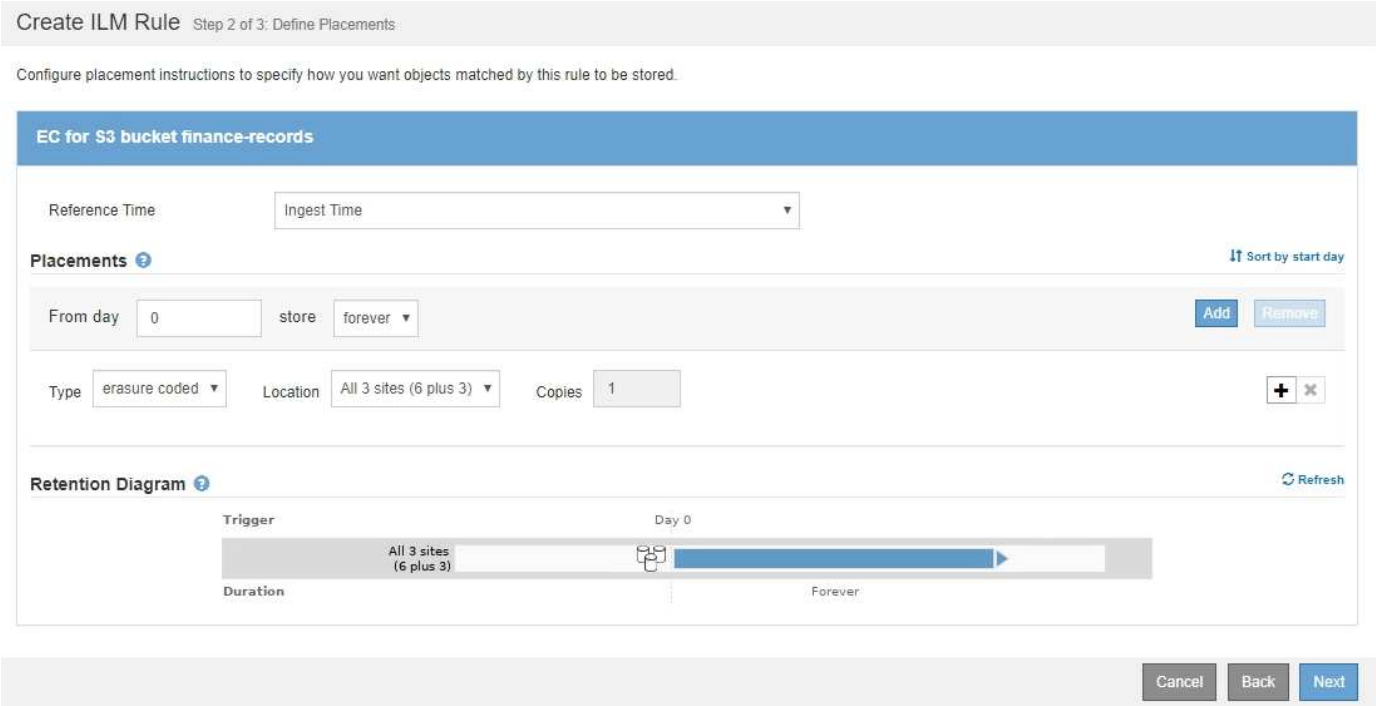
규칙 정의	예제 값
스토리지 풀	스토리지 풀 DC1과 스토리지 풀 DC2라는 두 개의 스토리지 풀이 서로 다른 데이터 센터에 있습니다.
규칙 이름	2개의 복사본 2개의 데이터 센터
참조 시간	수집 시간
콘텐츠 배치	0일째, 복제된 복사본 두 개를 영구 보관합니다. 하나는 스토리지 풀 DC1이고 다른 하나는 스토리지 풀 DC2에 있습니다.



예를 들어, **ILM** 규칙 **2:** 버킷 일치가 있는 삭제 코딩 프로필

이 ILM 규칙 예에서는 삭제 코딩 프로파일과 S3 버킷을 사용하여 오브젝트가 저장되는 위치 및 기간을 결정합니다.

규칙 정의	예제 값
삭제 코딩 프로필	• 3개의 데이터 센터에 걸쳐 단일 스토리지 풀(3개 사이트 모두) • 6+3 삭제 코딩 방법을 사용합니다
규칙 이름	S3 버킷 재무 기록용 EC
참조 시간	수집 시간
콘텐츠 배치	S3 버킷의 오브젝트(finance-records)의 경우 삭제 코딩 프로필에 지정된 풀에서 삭제 코딩 복사본을 하나 생성합니다. 이 복사본을 영구적으로 유지하십시오.

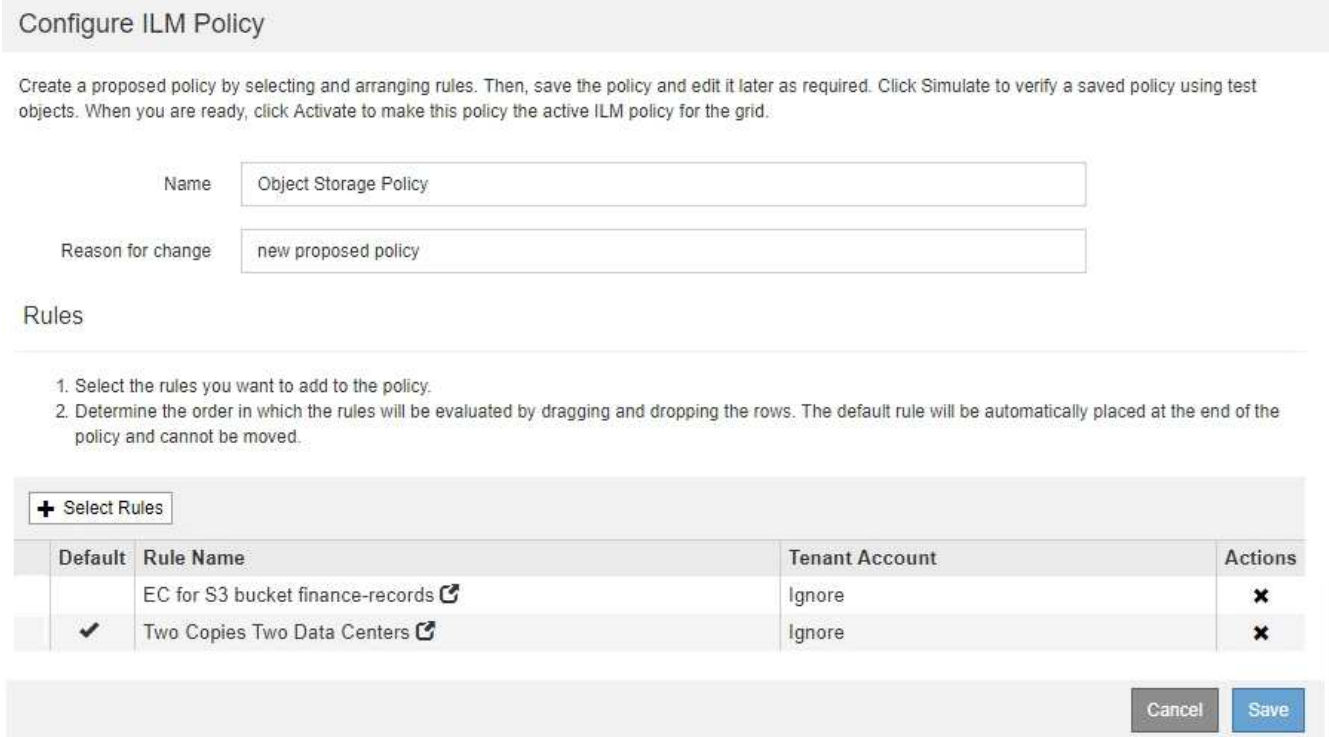


예 **1**의 **ILM** 정책

StorageGRID 시스템을 사용하면 정교하고 복잡한 ILM 정책을 설계할 수 있지만 실제로는 대부분의 ILM 정책이 간단합니다.

다중 사이트 토폴로지에 대한 일반적인 ILM 정책에는 다음과 같은 ILM 규칙이 포함될 수 있습니다.

- 수집 시 6+3 삭제 코딩을 사용하여 S3 버킷에 속하는 모든 오브젝트를 3개의 데이터 센터에 '금융 기록'이라고 합니다.
- 개체가 첫 번째 ILM 규칙과 일치하지 않으면 정책의 기본 ILM 규칙, 두 개의 복사본 두 개의 데이터 센터를 사용하여 해당 개체의 복사본을 두 데이터 센터 DC1과 DC2에 저장합니다.



예 **2: EC** 개체 크기 필터링에 대한 **ILM** 규칙 및 정책

다음 예제 규칙 및 정책을 시작점으로 사용하여 개체 크기를 기준으로 필터링하여 권장 EC 요구 사항을 충족하는 ILM 정책을 정의할 수 있습니다.

> 다음 ILM 규칙 및 정책은 예일 뿐입니다. ILM 규칙을 구성하는 방법은 여러 가지가 있습니다. 새 정책을 활성화하기 전에 제안된 정책을 시뮬레이션하여 콘텐츠가 손실로부터 보호되도록 의도한 대로 동작하는지 확인합니다.

예를 들어, **ILM** 규칙 **1: 1MB** 이상의 개체에 **EC**를 사용합니다

이 예에서는 ILM 규칙 삭제 코드 개체가 1MB 이상인 경우

> 삭제 코딩은 1MB 이상의 오브젝트에 가장 적합합니다. 매우 작은 삭제 코딩 조각을 관리해야 하는 오버헤드를 방지하기 위해 200KB 미만의 오브젝트에 삭제 코딩을 사용하지 마십시오.

규칙 정의	예제 값
규칙 이름	EC는 1MB 이상의 객체만 지원합니다
참조 시간	수집 시간
개체 크기에 대한 고급 필터링	개체 크기(MB)가 1보다 큽니다
콘텐츠 배치	3개의 사이트를 사용하여 2+1 삭제 코딩 복사본을 생성합니다

ILM 규칙 2(예: 복제된 복사본 2개)

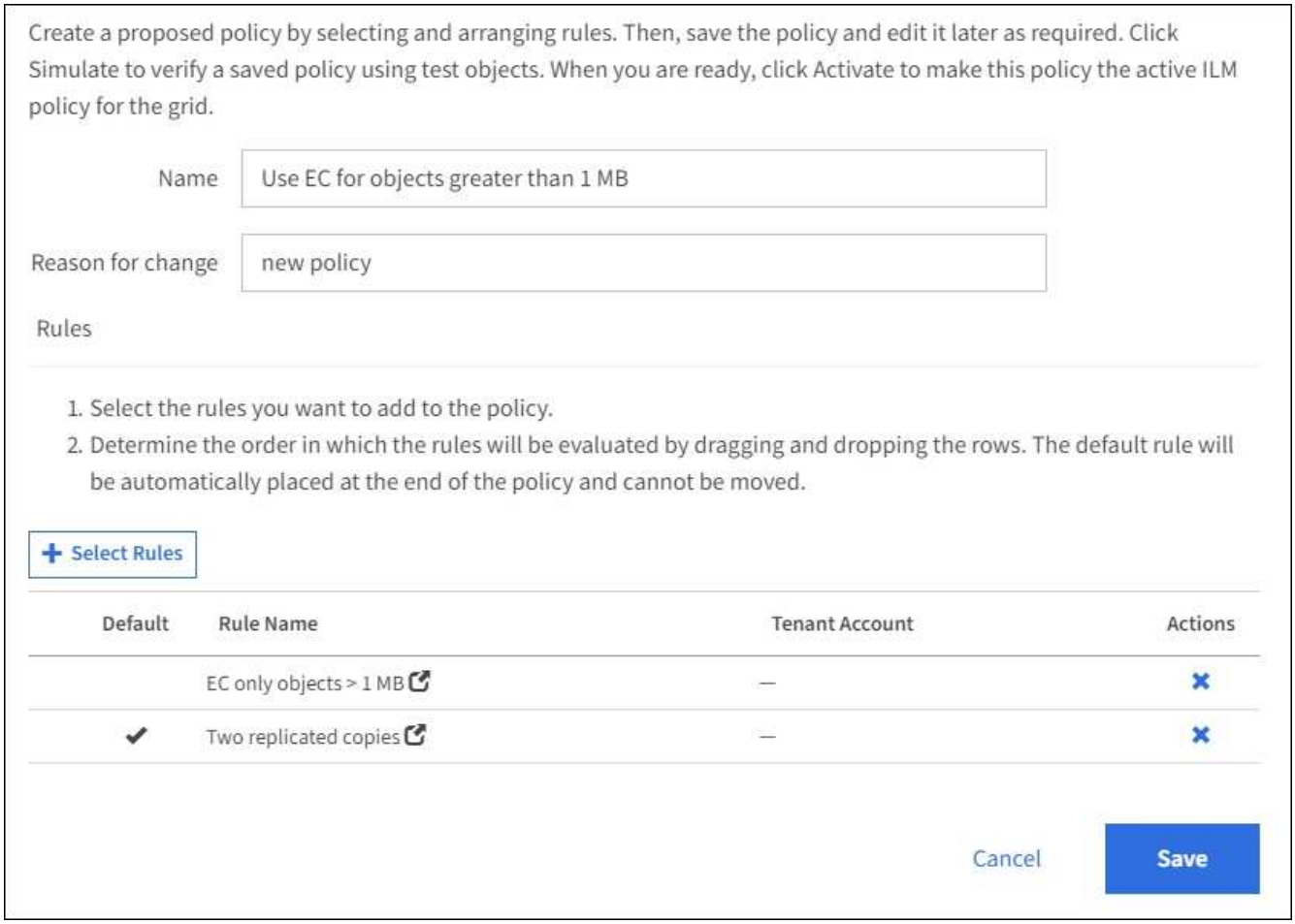
이 ILM 규칙은 복제된 복사본 두 개를 만들며 개체 크기별로 필터링하지 않습니다. 이 규칙은 정책의 기본 규칙입니다. 첫 번째 규칙은 1MB 이상의 모든 객체를 필터링하므로 이 규칙은 1MB 이하의 객체에만 적용됩니다.

규칙 정의	예제 값
규칙 이름	복제된 복사본 2개
참조 시간	수집 시간
개체 크기에 대한 고급 필터링	없음
콘텐츠 배치	복제된 복사본 2개를 생성하여 DC1과 DC2의 두 데이터 센터에 저장합니다

예 **2: 1MB**보다 큰 개체에 **EC**를 사용합니다

이 ILM 정책 예제에는 두 가지 ILM 규칙이 포함되어 있습니다.

- 첫 번째 규칙 삭제 시 1MB 이상의 모든 오브젝트를 코딩합니다.
- 두 번째(기본) ILM 규칙은 복제된 복사본 두 개를 생성합니다. 1MB 이상의 객체가 규칙 1에 의해 필터링되었기 때문에 규칙 2는 1MB 이하의 객체에만 적용됩니다.



예 **3:** 이미지 파일의 보호 향상을 위한 **ILM** 규칙 및 정책

다음 예제 규칙 및 정책을 사용하여 1MB 이상의 이미지가 삭제 코딩되고 두 개의 복사본이 더 작은 이미지로 만들어졌는지 확인할 수 있습니다.

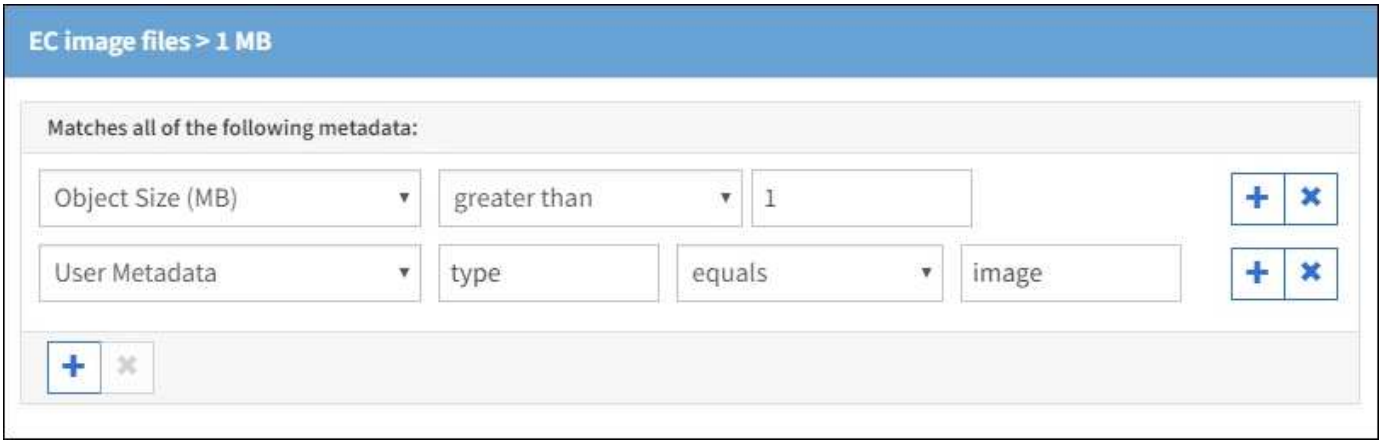
> 다음 ILM 규칙 및 정책은 예일 뿐입니다. ILM 규칙을 구성하는 방법은 여러 가지가 있습니다. 새 정책을 활성화하기 전에 제안된 정책을 시뮬레이션하여 콘텐츠가 손실로부터 보호되도록 의도한 대로 동작하는지 확인합니다.

예를 들어 **ILM** 규칙 **1: 1MB**보다 큰 이미지 파일에 **EC**를 사용합니다

이 ILM 규칙 예에서는 고급 필터링을 사용하여 1MB 이상의 모든 이미지 파일을 삭제합니다.

> 삭제 코딩은 1MB 이상의 오브젝트에 가장 적합합니다. 매우 작은 삭제 코딩 조각을 관리해야 하는 오버헤드를 방지하기 위해 200KB 미만의 오브젝트에 삭제 코딩을 사용하지 마십시오.

규칙 정의	예제 값
규칙 이름	EC 이미지 파일 > 1MB
참조 시간	수집 시간
개체 크기에 대한 고급 필터링	객체 크기(MB)가 1.0보다 큽니다
사용자 메타데이터에 대한 고급 필터링	사용자 메타데이터 유형은 이미지와 동일합니다
콘텐츠 배치	3개의 사이트를 사용하여 2+1 삭제 코딩 복사본을 생성합니다



이 규칙은 정책의 첫 번째 규칙으로 구성되므로 삭제 코딩 배치 지침은 1MB 이상인 이미지에만 적용됩니다.

예를 들어 **ILM** 규칙 **2:** 나머지 모든 이미지 파일에 대해 **2**개의 복제된 복사본을 만듭니다

이 ILM 규칙 예에서는 고급 필터링을 사용하여 더 작은 이미지 파일을 복제하도록 지정합니다. 정책의 첫 번째 규칙이 이미 1MB 이상의 이미지 파일과 일치했기 때문에 이 규칙은 1MB 이하의 이미지 파일에 적용됩니다.

규칙 정의	예제 값
규칙 이름	이미지 파일 2부
참조 시간	수집 시간
사용자 메타데이터에 대한 고급 필터링	사용자 메타데이터 유형은 이미지 파일과 동일합니다
콘텐츠 배치	2개의 스토리지 풀에 2개의 복제 복제본을 생성합니다

예를 들어, **ILM** 정책 **3:** 이미지 파일에 대한 보호 개선

이 ILM 정책 예제에는 다음 세 가지 규칙이 포함되어 있습니다.

- 첫 번째 규칙 삭제 시 1MB 이상의 모든 이미지 파일이 코딩됩니다.
- 두 번째 규칙은 나머지 이미지 파일(즉, 1MB 이하의 이미지)의 복사본을 두 개 만듭니다.
- 기본 규칙은 나머지 모든 개체(즉, 이미지가 아닌 파일)에 적용됩니다.

예 **4: S3** 버전 오브젝트에 대한 **ILM** 규칙 및 정책

버전 관리가 활성화된 S3 버킷을 사용하는 경우 * 비현재 시간 * 을 참조 시간으로 사용하는 ILM 정책에 규칙을 포함하여 비최신 오브젝트 버전을 관리할 수 있습니다.

이 예제에서 볼 수 있듯이 버전이 아닌 개체 버전에 대해 다른 배치 명령을 사용하여 버전이 지정된 개체에서 사용하는 스토리지의 양을 제어할 수 있습니다.

> 다음 ILM 규칙 및 정책은 예일 뿐입니다. ILM 규칙을 구성하는 방법은 여러 가지가 있습니다. 새 정책을 활성화하기 전에 제안된 정책을 시뮬레이션하여 콘텐츠가 손실로부터 보호되도록 의도한 대로 동작하는지 확인합니다.

> ILM 정책을 생성하여 비최신 개체 버전을 관리하는 경우 정책을 시뮬레이션하려면 개체 버전의 UUID 또는 CBID를 알고 있어야 합니다. 개체의 UUID 및 CBID를 찾으려면 개체가 현재 상태일 때 개체 메타데이터 조회를 사용합니다. 을 참조하십시오 개체 메타데이터 조회를 통해 ILM 정책을 확인합니다.

관련 정보

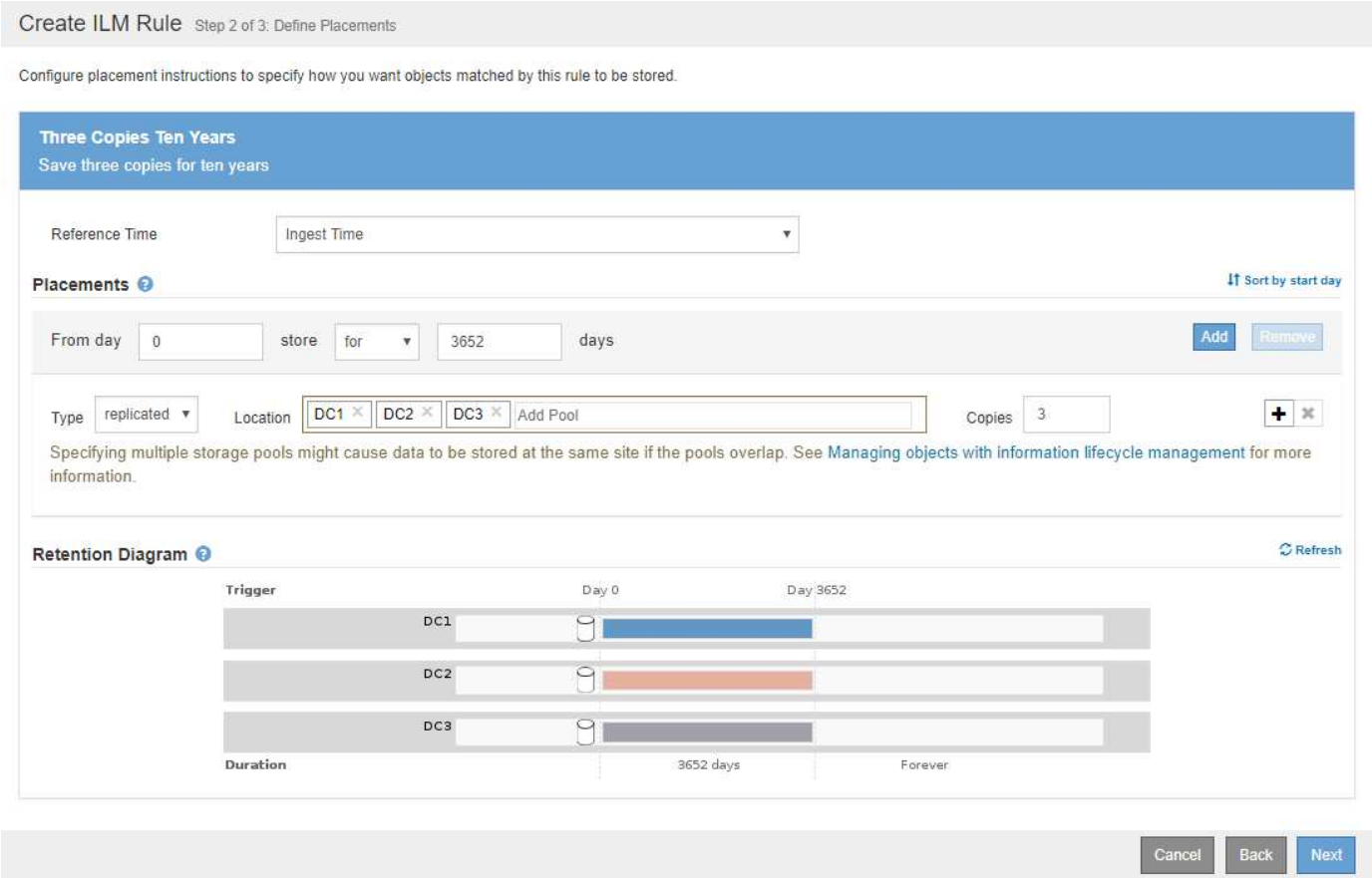
- 오브젝트 삭제 방법

예를 들어 **ILM** 규칙 **1: 10**년 동안 복사본 **3**개를 저장합니다

이 ILM 규칙은 10년 동안 3개의 데이터 센터에 각 개체의 복사본을 저장합니다.

이 규칙은 버전 적용 여부에 관계없이 모든 개체에 적용됩니다.

규칙 정의	예제 값
스토리지 풀	각각 서로 다른 데이터 센터에 있는 세 개의 스토리지 풀(DC1, DC2 및 DC3)입니다.
규칙 이름	10년 동안 3부
참조 시간	수집 시간
콘텐츠 배치	0일째, 복제된 복사본 3개를 10년(3,652일), DC1에 1개, DC2에 1개, DC3에 1개씩 보관합니다. 10년이 끝나면 개체의 복사본을 모두 삭제합니다.



예를 들어 **ILM** 규칙 **2: 2**년 동안 비최신 버전의 복사본 **2**개를 저장합니다

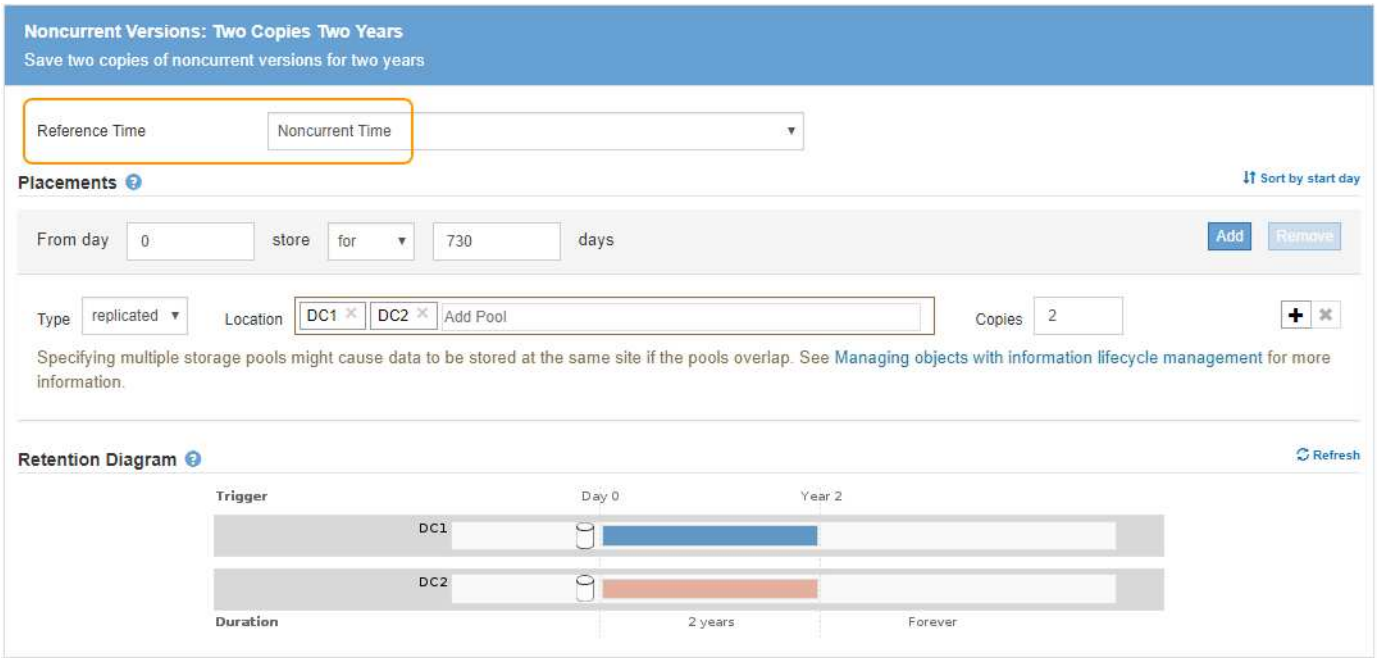
이 ILM 규칙 예에서는 2년 동안 S3 버전 오브젝트에서 2개의 복사본을 저장합니다.

ILM 규칙 1은 개체의 모든 버전에 적용되므로 다른 규칙을 만들어 현재 버전이 아닌 버전을 필터링해야 합니다. 이 규칙은 참조 시간에 * 비현재 시간 * 옵션을 사용합니다.

이 예제에서는 비최신 버전의 복사본 두 개만 저장되고 이 복사본은 2년 동안 저장됩니다.

규칙 정의	예제 값
스토리지 풀	각각 서로 다른 데이터 센터에 있는 두 개의 스토리지 풀(DC1 및 DC2)입니다.

규칙 정의	예제 값
규칙 이름	비최신 버전: 2부 2년
참조 시간	현재 시간이 아닙니다
콘텐츠 배치	현재 시간이 아닌 경우(즉, 개체 버전이 최신 버전이 아닌 버전이 되는 날부터 시작)에 대해 0일째 되는 경우, 2년(730일) 동안 DC1과 DC2에 있는 2개의 비현재 개체 버전의 복제된 복사본을 유지합니다. 2년이 끝나면 최신 버전이 아닌 버전을 삭제합니다.



ILM 정책(예: **4:S3** 버전 오브젝트

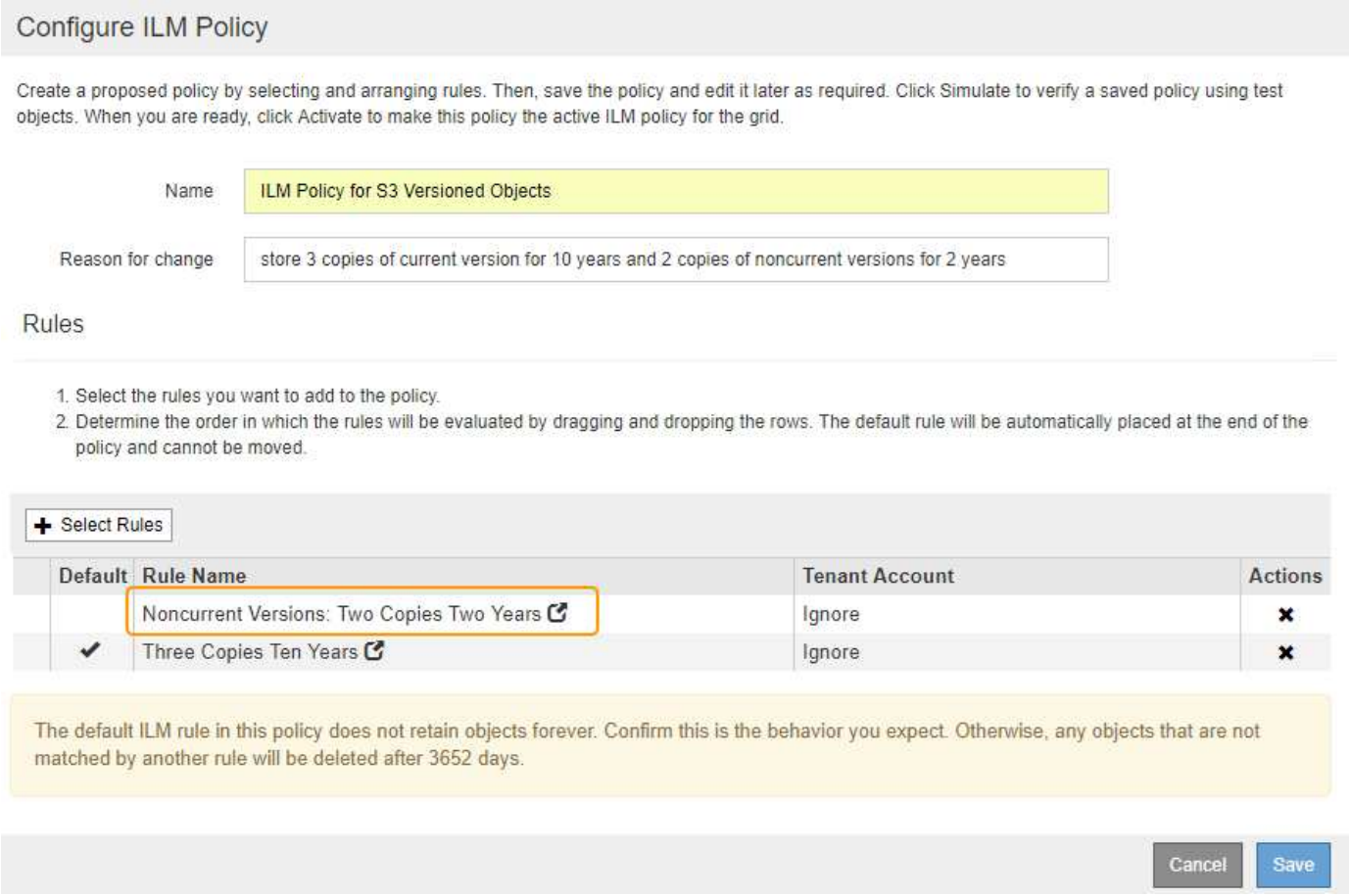
개체의 이전 버전을 현재 버전과 다르게 관리하려면 현재 개체 버전에 적용되는 규칙 전에 참조 시간으로 * 비현재 시간 * 을 사용하는 규칙이 ILM 정책에 나타나야 합니다.

S3 버전 개체에 대한 ILM 정책에는 다음과 같은 ILM 규칙이 포함될 수 있습니다.

- 버전이 최신 버전이 아닌 날부터 시작하여 각 개체의 이전(비최신) 버전을 2년 동안 유지합니다.

> 현재 개체 버전에 적용되는 규칙 앞의 정책에 현재 시간 이외의 규칙이 표시되어야 합니다. 그렇지 않으면 현재 개체 버전이 아닌 시간 규칙과 일치하지 않습니다.

- 수집 시 3개의 복제 복사본을 생성하고 3개 데이터 센터 각각에 하나의 복사본을 저장합니다. 10년 동안 현재 개체 버전의 복사본을 유지합니다.



예제 정책을 시뮬레이션할 때 테스트 개체는 다음과 같이 평가됩니다.

- 최신 버전이 아닌 개체 버전은 첫 번째 규칙에 따라 일치됩니다. 최신 버전이 아닌 개체 버전이 2년 이상이면 ILM을 통해 영구적으로 삭제됩니다(비최신 버전의 모든 복사본이 그리드에서 제거됨).

> 최신 버전이 아닌 개체 버전을 시뮬레이션하려면 해당 버전의 UUID 또는 CBID를 사용해야 합니다. 객체가 아직 남아 있는 동안 객체 메타데이터 조회를 사용하여 해당 UUID 및 CBID를 찾을 수 있습니다.

- 현재 개체 버전은 두 번째 규칙에 따라 일치됩니다. 현재 개체 버전이 10년 동안 저장된 경우 ILM 프로세스는 삭제 마커를 개체의 현재 버전으로 추가하고 이전 개체 버전을 ""비현재""로 만듭니다. 다음 번에 ILM 평가를 수행할 때 이 비최신 버전은 첫 번째 규칙에 따라 일치합니다. 따라서 DC3에서 복제본이 제거되고 DC1과 DC2에서 두 개의 복제본이 2년 더 저장됩니다.

예 **5:** 엄격한 수집 동작을 위한 **ILM** 규칙 및 정책

위치 필터 및 Strict 수집 동작을 규칙에서 사용하여 개체가 특정 데이터 센터 위치에 저장되지 않도록 할 수 있습니다.

이 예에서 파리에 본사를 둔 테넌트는 규제 문제로 인해 EU 외부에 일부 객체를 저장하지 않으려는 경우가 있습니다. 다른 테넌트 계정의 모든 객체를 포함하여 다른 객체는 파리 데이터 센터 또는 미국 데이터 센터에 저장할 수 있습니다.

다음 ILM 규칙 및 정책은 예일 뿐입니다. ILM 규칙을 구성하는 방법은 여러 가지가 있습니다. 새 정책을 활성화하기 전에 제안된 정책을 시뮬레이션하여 콘텐츠가 손실로부터 보호되도록 의도한 대로 동작하는지 확인합니다.

관련 정보

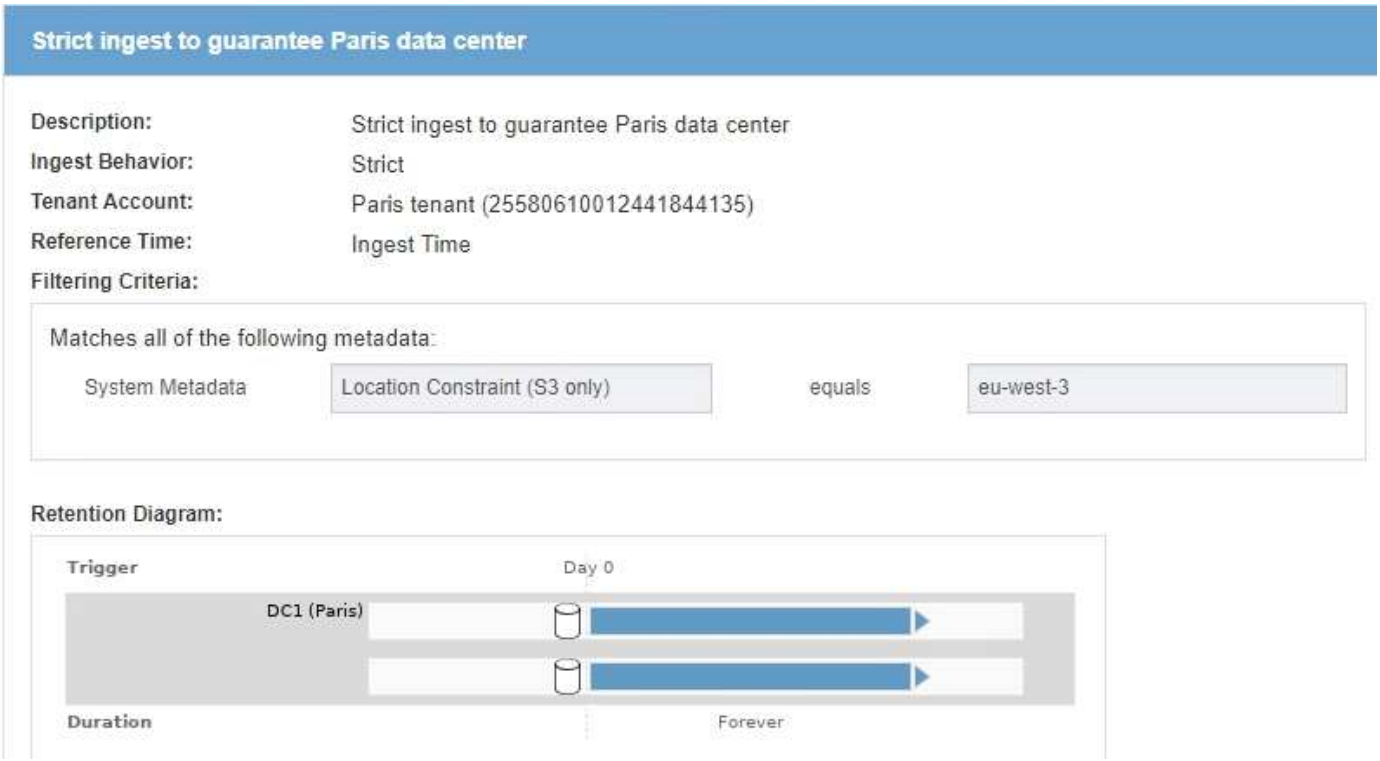
- 데이터 보호를 위한 수집 옵션
- 3단계 중 3단계: 수집 동작 정의

예를 들어 **ILM** 규칙 **1:** 파리 데이터 센터를 보장하기 위한 엄격한 수집

이 ILM 규칙은 엄격한 수집 동작을 사용하여 유럽-서부-3 지역(파리)으로 설정된 지역이 US 데이터 센터에 저장되지 않은 S3 버킷에 파리 기반 테넌트가 저장한 오브젝트를 보장합니다.

이 규칙은 파리 테넌트에 속하며 S3 버킷 영역이 EU-West-3(파리)로 설정된 오브젝트에 적용됩니다.

규칙 정의	예제 값
테넌트 계정	파리 테넌트
고급 필터링	위치 제약 조건은 EU-West-3과 동일합니다
스토리지 풀	DC1(파리)
규칙 이름	엄격한 인제스트로 파리 데이터 센터 보장
참조 시간	수집 시간
콘텐츠 배치	0일째, 복제된 복사본 2개를 DC1(파리)에 영구적으로 유지
수집 동작	엄격한 수집 시에는 항상 이 규칙의 배치를 사용하십시오. 파리 데이터 센터에 오브젝트 복사본 2개를 저장할 수 없는 경우 수집에 실패합니다.



ILM 규칙 **2(**예**: 5):** 다른 개체에 대한 균형 잡힌 수집

이 ILM 규칙 예에서는 균형 잡힌 수집 동작을 사용하여 첫 번째 규칙과 일치하지 않는 오브젝트에 대해 최적의 ILM 효율성을 제공합니다. 이 규칙에 일치하는 모든 오브젝트의 두 복사본이 저장됩니다. 하나는 미국 데이터 센터이고 다른 하나는 파리 데이터 센터에 저장됩니다. 규칙을 즉시 충족할 수 없는 경우 임시 사본은 사용 가능한 위치에 저장됩니다.

이 규칙은 모든 테넌트 및 영역에 속하는 객체에 적용됩니다.

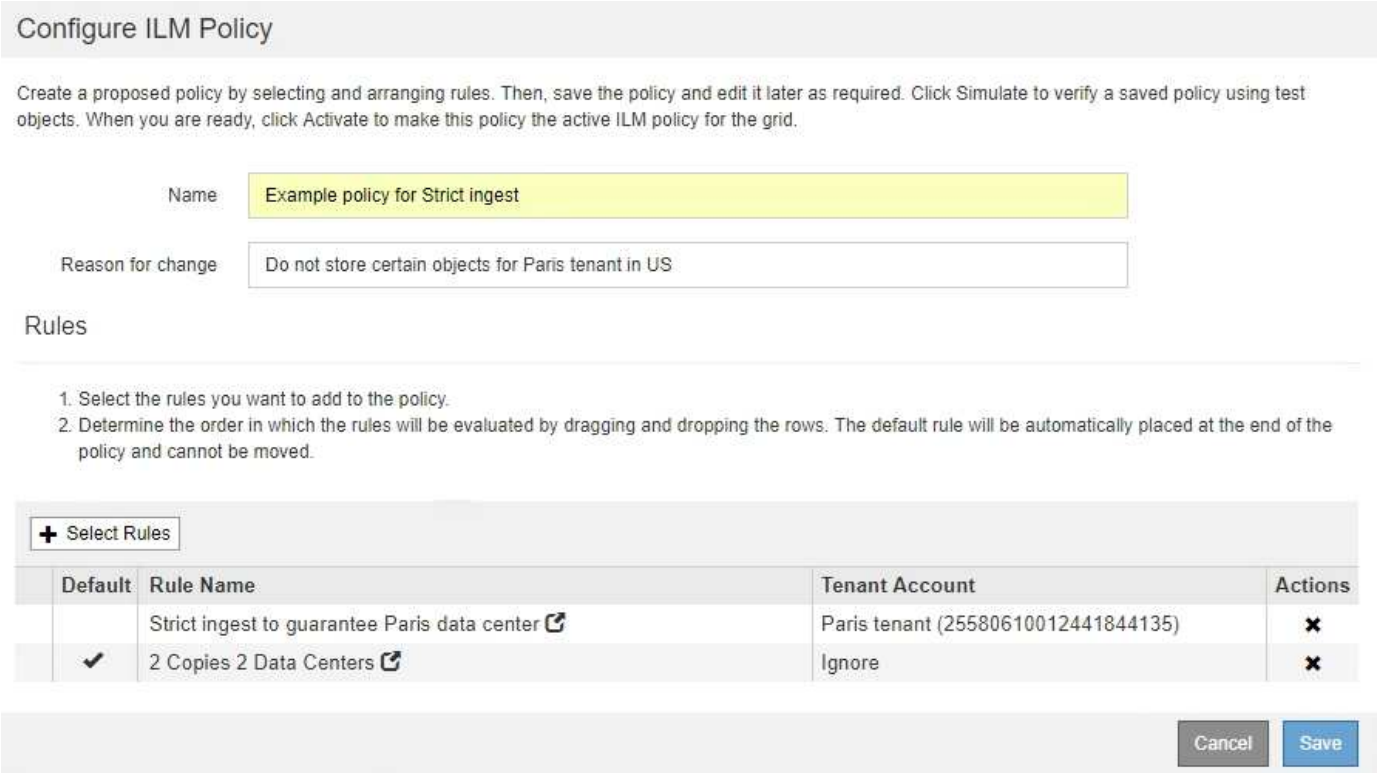
규칙 정의	예제 값
테넌트 계정	무시
고급 필터링	_ 지정 안 됨 _
스토리지 풀	DC1(파리) 및 DC2(미국)
규칙 이름	2 2개의 데이터 센터를 복사합니다
참조 시간	수집 시간
콘텐츠 배치	0일차의 경우 두 데이터 센터에 복제된 복사본 두 개를 영구적으로 유지합니다
수집 동작	균형. 이 규칙과 일치하는 개체는 가능한 경우 규칙의 배치 지침에 따라 배치됩니다. 그렇지 않으면 임시 사본이 사용 가능한 모든 위치에서 만들어집니다.

예 **5**의 **ILM** 정책**:** 수집 동작 결합

ILM 정책의 예에는 수집 동작이 서로 다른 두 규칙이 포함되어 있습니다.

두 가지 수집 동작을 사용하는 ILM 정책에는 다음과 같은 ILM 규칙이 포함될 수 있습니다.

- 파리 테넌트에 속해 있고 S3 버킷 영역이 파리 데이터 센터에서만 EU-West-3(파리)으로 설정된 오브젝트를 저장합니다. 파리 데이터 센터를 사용할 수 없는 경우 수집에 실패합니다.
- 미국 데이터 센터와 파리 데이터 센터에 있는 다른 모든 오브젝트(파리 테넌트에 속해 있지만 다른 버킷 지역이 있는 객체 포함)를 저장합니다. 배치 지침을 충족할 수 없는 경우 사용 가능한 위치에 임시 사본을 만듭니다.



예제 정책을 시뮬레이션할 때 테스트 개체는 다음과 같이 평가됩니다.

- 파리 테넌트에 속해 있고 S3 버킷 영역이 EU-West-3으로 설정된 모든 오브젝트는 첫 번째 규칙에 따라 일치하며 파리 데이터 센터에 저장됩니다. 첫 번째 규칙은 Strict 수집 을 사용하기 때문에 이러한 오브젝트는 미국 데이터 센터에 저장되지 않습니다. 파리 데이터 센터의 스토리지 노드를 사용할 수 없는 경우 수집에서 실패합니다.
- 다른 모든 오브젝트는 파리 테넌트에 속하며 S3 버킷 영역이 EU-West-3으로 설정되지 않은 오브젝트를 포함하여 두 번째 규칙에 따라 대응됩니다. 각 오브젝트의 한 복사본이 각 데이터 센터에 저장됩니다. 그러나 두 번째 규칙은 균형 잡힌 수집을 사용하므로 한 데이터 센터를 사용할 수 없는 경우 두 개의 중간 복사본이 사용 가능한 위치에 저장됩니다.

예 **6: ILM** 정책 변경

데이터 보호가 변경하거나 새 사이트를 추가하는 경우 새 ILM 정책을 만들고 활성화해야 할 수 있습니다.

정책을 변경하기 전에 ILM 배치 변경이 StorageGRID 시스템의 전반적인 성능에 일시적으로 어떤 영향을 미칠 수 있는지 이해해야 합니다.

이 예에서는 새 StorageGRID 사이트가 확장에 추가되었으며 새 사이트에 데이터를 저장하기 위해 활성 ILM 정책을 수정해야 합니다.

> 다음 ILM 규칙 및 정책은 예일 뿐입니다. ILM 규칙을 구성하는 방법은 여러 가지가 있습니다. 새 정책을 활성화하기 전에 제안된 정책을 시뮬레이션하여 콘텐츠가 손실로부터 보호되도록 의도한 대로 동작하는지 확인합니다.

ILM 정책을 변경하면 성능에 어떤 영향을 미칩니까

새로운 ILM 정책을 활성화할 때 StorageGRID 시스템의 성능은 일시적으로 영향을 받을 수 있습니다. 특히 새 정책의 배치 명령에 따라 많은 기존 오브젝트를 새 위치로 이동해야 하는 경우에 그렇습니다.

> 새로운 ILM 정책을 활성화하면 StorageGRID은 이를 사용하여 기존 오브젝트 및 새로 수집된 오브젝트를 포함한 모든 오브젝트를 관리합니다. 새 ILM 정책을 활성화하기 전에 복제된 기존 오브젝트 및 삭제 코딩 오브젝트의 배치에 대한 변경 사항을 검토하십시오. 기존 오브젝트의 위치를 변경하면 새로운 배치가 평가되고 구현될 때 일시적인 리소스 문제가 발생할 수 있습니다.

StorageGRID 성능에 일시적으로 영향을 미칠 수 있는 ILM 정책 변경 유형은 다음과 같습니다.

- 기존의 삭제 코딩 오브젝트에 다른 삭제 코딩 프로파일 적용

> StorageGRID는 각 삭제 코딩 프로필을 고유한 것으로 간주하며 새 프로필을 사용할 때 삭제 코딩 조각을 다시 사용하지 않습니다.

- 기존 오브젝트에 필요한 복사 유형을 변경합니다. 예를 들어, 복제된 오브젝트의 많은 비율을 삭제 코딩 오브젝트로 변환합니다.
- 기존 오브젝트의 복사본을 전혀 다른 위치로 이동(예: 많은 오브젝트를 Cloud Storage Pool 간에 이동 또는 원격 사이트 간에 이동)

관련 정보

ILM 정책을 생성합니다

활성 **ILM** 정책(예**: 6:** 두 사이트의 데이터 보호

이 예에서 활성 ILM 정책은 처음에 2개 사이트 StorageGRID 시스템용으로 설계되었고 두 가지 ILM 규칙을 사용합니다.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy | Clone | Edit | Remove

	Policy Name	Policy State	Start Date	End Date
◉	Data Protection for Two Sites	Active	2020-06-10 16:42:09 MDT	
○	Baseline 2 Copies Policy	Historical	2020-06-09 21:48:34 MDT	2020-06-10 16:42:09 MDT

Viewing Active Policy - Data Protection for Two Sites

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Data Protection for Two Sites

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
One-Site Erasure Coding for Tenant A		Tenant A (49752734300032812036)
Two-Site Replication for Other Tenants	✔	Ignore

Simulate | Activate

이 ILM 정책에서는 테넌트 A에 속하는 객체는 단일 사이트에서 2+1 삭제 코딩으로 보호되며, 다른 모든 테넌트에 속한 객체는 2개 복제본 복제를 사용하여 2개 사이트 간에 보호됩니다.

> 이 예제의 첫 번째 규칙은 고급 필터를 사용하여 작은 오브젝트에 삭제 코딩을 사용하지 않도록 합니다. 1MB 미만의 테넌트 A의 객체는 복제를 사용하는 두 번째 규칙에 의해 보호됩니다.

규칙 **1:** 테넌트 **A**에 대한 단일 사이트 삭제 코딩

규칙 정의	예제 값
규칙 이름	테넌트 A에 대한 1개 사이트 삭제 코딩
테넌트 계정	테넌트 A
스토리지 풀	데이터 센터 1
콘텐츠 배치	데이터 센터 1의 2+1 삭제 코딩은 0일째부터 영원까지

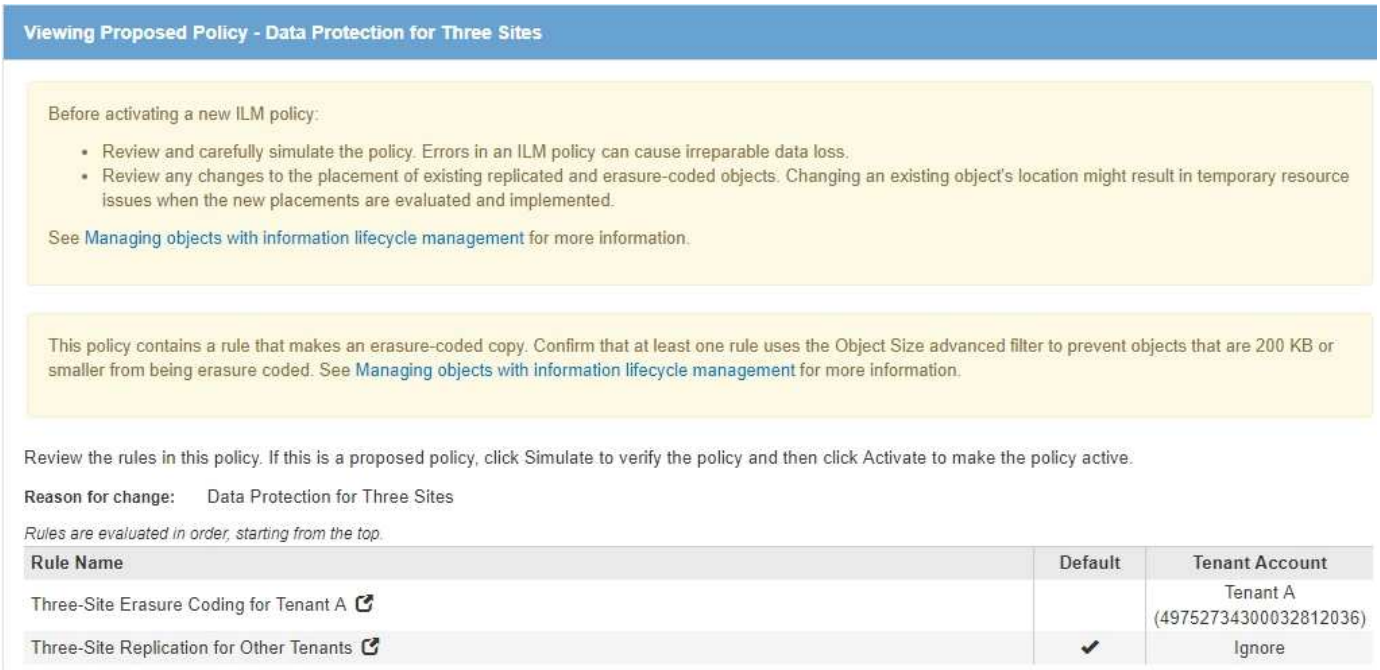
규칙 **2:** 다른 테넌트를 위한 **2**개 사이트 복제

규칙 정의	예제 값
규칙 이름	다른 테넌트를 위한 2개 사이트 복제
테넌트 계정	무시
스토리지 풀	데이터 센터 1 및 데이터 센터 2
콘텐츠 배치	0일째부터 영구 복제 복사본 2개: 데이터 센터 1에 복사본 1개, 데이터 센터 2에 복사본 1개

예를 들어, 제안된 **ILM** 정책 **6:** 세 사이트의 데이터 보호

이 예에서 ILM 정책은 3개 사이트 StorageGRID 시스템에 대해 업데이트됩니다.

확장을 수행하여 새 사이트를 추가한 후 그리드 관리자는 두 개의 새 스토리지 풀을 만들었습니다. 하나는 데이터 센터 3용 스토리지 풀이고 다른 하나는 세 개의 사이트를 모두 포함하는 스토리지 풀입니다(모든 스토리지 노드 기본 스토리지 풀과 동일하지 않음). 그런 다음 관리자는 두 가지 새로운 ILM 규칙 및 제안된 새 ILM 정책을 만들었습니다. 이 정책은 세 사이트 모두의 데이터를 보호하도록 설계되었습니다.



이 새로운 ILM 정책이 활성화되면 테넌트 A에 속하는 객체는 3개의 사이트에서 2+1 삭제 코딩으로 보호되며, 다른 테넌트(및 테넌트 A에 속하는 더 작은 객체)에 속하는 객체는 3개의 복제본 복제를 사용하여 3개의 사이트에 걸쳐 보호됩니다.

규칙 **1:** 테넌트 **A**의 **3**개 사이트 삭제 코딩

규칙 정의	예제 값
규칙 이름	테넌트 A의 3개 사이트 삭제 코딩
테넌트 계정	테넌트 A
스토리지 풀	3개 데이터 센터 모두(데이터 센터 1, 데이터 센터 2 및 데이터 센터 3 포함)
콘텐츠 배치	3개 데이터 센터 모두에서 2개 이상의 1 삭제 코딩: 0일째부터 영원까지

규칙 **2:** 다른 테넌트를 위한 **3**개 사이트 복제

규칙 정의	예제 값
규칙 이름	다른 테넌트를 위한 3개 사이트 복제
테넌트 계정	무시
스토리지 풀	데이터 센터 1, 데이터 센터 2 및 데이터 센터 3
콘텐츠 배치	0일째부터 영원히 복제되는 복사본 3개: 데이터 센터 1에 복사본 1개, 데이터 센터 2에 복사본 1개, 데이터 센터 3에 복사본 1개

새로 제안된 ILM 정책을 활성화하면 새 규칙 또는 업데이트된 규칙의 배치 지침에 따라 기존 개체를 새 위치로 이동하거나 기존 개체에 대한 새 개체 복사본을 만들 수 있습니다.

> ILM 정책의 오류로 인해 복구할 수 없는 데이터 손실이 발생할 수 있습니다. 정책을 활성화하기 전에 정책을 주의 깊게 검토하고 시뮬레이션하여 의도한 대로 작동하도록 확인합니다.

> 새로운 ILM 정책을 활성화하면 StorageGRID은 이를 사용하여 기존 오브젝트 및 새로 수집된 오브젝트를 포함한 모든 오브젝트를 관리합니다. 새 ILM 정책을 활성화하기 전에 복제된 기존 오브젝트 및 삭제 코딩 오브젝트의 배치에 대한 변경 사항을 검토하십시오. 기존 오브젝트의 위치를 변경하면 새로운 배치가 평가되고 구현될 때 일시적인 리소스 문제가 발생할 수 있습니다.

삭제 코딩 지침이 변경될 때 수행되는 작업

이 예에 대해 현재 활성화된 ILM 정책에서 테넌트 A에 속하는 객체는 Data Center 1에서 2+1 삭제 코딩을 사용하여 보호됩니다. 새로 제안된 ILM 정책에서는 테넌트 A에 속하는 객체는 데이터 센터 1, 2 및 3에서 2+1 삭제 코딩을 사용하여 보호됩니다.

새 ILM 정책이 활성화되면 다음 ILM 작업이 수행됩니다.

- 테넌트 A에 의해 수집된 새 객체는 두 개의 데이터 조각으로 분할되고 하나의 패리티 조각이 추가됩니다. 그런 다음 세 개의 각 단편이 다른 데이터 센터에 저장됩니다.
- 현재 진행 중인 ILM 스캔 프로세스 중에 테넌트 A에 속한 기존 객체가 다시 평가됩니다. ILM 배치 지침은 새로운 삭제 코딩 프로필을 사용하므로 완전히 새로운 삭제 코딩 조각이 생성되어 세 데이터 센터에 배포됩니다.

> 데이터 센터 1의 기존 2 + 1 조각은 재사용되지 않습니다. StorageGRID는 각 삭제 코딩 프로필을 고유한 것으로 간주하며 새 프로필을 사용할 때 삭제 코딩 조각을 다시 사용하지 않습니다.

복제 지침이 변경될 때 수행되는 작업

이 예에 대한 현재 활성 ILM 정책에서 다른 테넌트에 속한 개체는 데이터 센터 1 및 2의 스토리지 풀에 있는 두 개의 복제된 복사본을 사용하여 보호됩니다. 새로 제안된 ILM 정책에서는 다른 테넌트에 속한 객체는 데이터 센터 1, 2 및 3의 스토리지 풀에 있는 3개의 복제된 복사본을 사용하여 보호됩니다.

새 ILM 정책이 활성화되면 다음 ILM 작업이 수행됩니다.

- 테넌트 A 이외의 테넌트가 새 객체를 링하면 StorageGRID는 복제본 3개를 생성하고 각 데이터 센터에 복제본 1개를 저장합니다.
- 이러한 다른 테넌트에 속한 기존 객체는 지속적인 ILM 검색 프로세스 중에 재평가됩니다. 데이터 센터 1과 데이터 센터 2의 기존 오브젝트 복사본이 새로운 ILM 규칙의 복제 요구사항을 계속해서 충족하므로 StorageGRID은 데이터 센터 3용 개체의 새 복사본만 생성하면 됩니다.

이 정책 활성화의 성능 영향

이 예에서 제안된 ILM 정책이 활성화되면 이 StorageGRID 시스템의 전체 성능이 일시적으로 영향을 받습니다. 다른 테넌트의 기존 객체에 대해 테넌트 A의 기존 객체와 Data Center 3에 새로운 복제된 복제본에 대한 새로운 삭제 코딩 조각을 생성하는 데 일반 그리드 리소스 수준보다 높은 수준의 리소스가 필요합니다.

ILM 정책 변경으로 인해 클라이언트 읽기 및 쓰기 요청이 일시적으로 일반 지연 시간보다 길어질 수 있습니다. 그리드

전체에 배치 명령이 완전히 구현된 후 지연 시간은 정상 수준으로 돌아갑니다.

새 ILM 정책을 활성화할 때 리소스 문제를 방지하려면 많은 수의 기존 오브젝트의 위치를 변경할 수 있는 모든 규칙에서 Ingest Time 고급 필터를 사용할 수 있습니다. 기존 개체가 불필요하게 이동되지 않도록 새 정책이 적용되는 대략적인 시간과 같거나 큰 수집 시간을 설정합니다.

> ILM 정책 변경 이후 개체가 처리되는 속도를 늦추거나 높여야 하는 경우에는 기술 지원 부서에 문의하십시오.

예 **7: S3** 오브젝트 잠금에 대한 규정 준수 **ILM** 정책

이 예제에서 S3 오브젝트 잠금이 활성화된 버킷의 오브젝트에 대한 오브젝트 보호 및 보존 요구사항을 충족하기 위해 ILM 정책을 정의할 때 시작 지점으로 S3 버킷, ILM 규칙 및 ILM 정책을 사용할 수 있습니다.

> 이전 StorageGRID 릴리스에서 레거시 규정 준수 기능을 사용한 경우 이 예제를 사용하여 레거시 규정 준수 기능이 활성화된 기존 버킷을 관리할 수도 있습니다.

> 다음 ILM 규칙 및 정책은 예일 뿐입니다. ILM 규칙을 구성하는 방법은 여러 가지가 있습니다. 새 정책을 활성화하기 전에 제안된 정책을 시뮬레이션하여 콘텐츠가 손실로부터 보호되도록 의도한 대로 동작하는지 확인합니다.

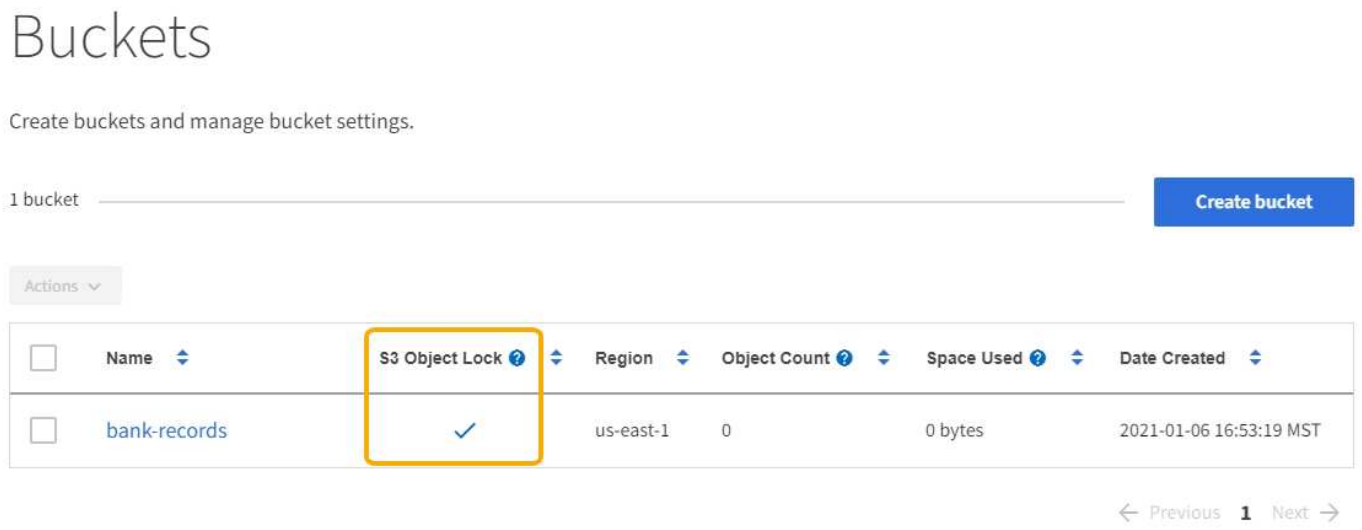
관련 정보

- S3 오브젝트 잠금으로 오브젝트 관리
- ILM 정책을 생성합니다

S3 오브젝트 잠금의 버킷 및 오브젝트 예

이 예에서는 ABC의 Bank라는 S3 테넌트 계정이 테넌트 관리자를 사용하여 중요한 은행 레코드를 저장할 수 있는 S3 Object Lock이 활성화된 버킷을 만들었습니다.

버킷 정의	예제 값
테넌트 계정 이름입니다	ABC 은행
버킷 이름	은행 - 레코드
버킷 영역	미국 - 동부 - 1(기본값)



은행 레코드 버킷에 추가되는 각 개체 및 개체 버전은 다음 값(최신 상태)과 법적 증거 자료 보관(Legal Hold) 설정을 사용합니다.

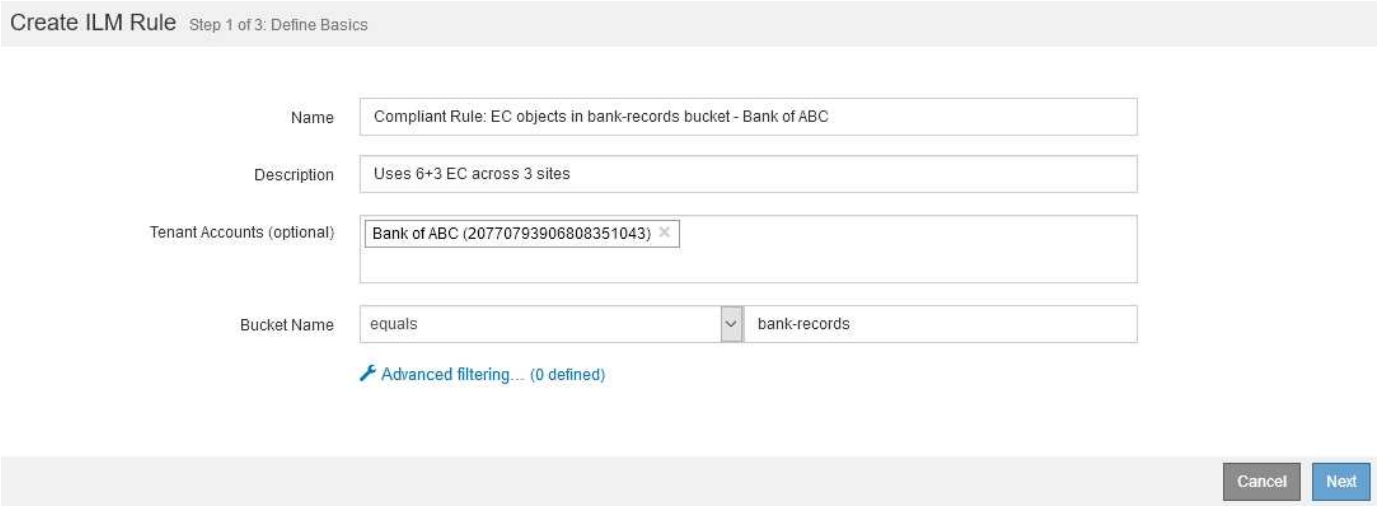
각 개체에 대한 설정입니다	예제 값
기일까지	"2030-12-30T23:59:59Z'(2030년 12월 30일) 각 개체 버전에는 고유한 '최신 상태' 설정이 있습니다. 이 설정은 늘릴 수 있지만 줄일 수는 없습니다.
법적 증거 자료 보관	"OFF'(효과 없음) 보존 기간 동안 언제든지 개체 버전에 대한 법적 지류를 설정하거나 인양할 수 있습니다. 개체가 법적 증거 자료 보관 중인 경우 보관 기한 에 도달하더라도 삭제할 수 없습니다.

S3 오브젝트 잠금에 대한 **ILM** 규칙 **1** 예**:** 버킷 일치가 있는 삭제 코딩 프로필

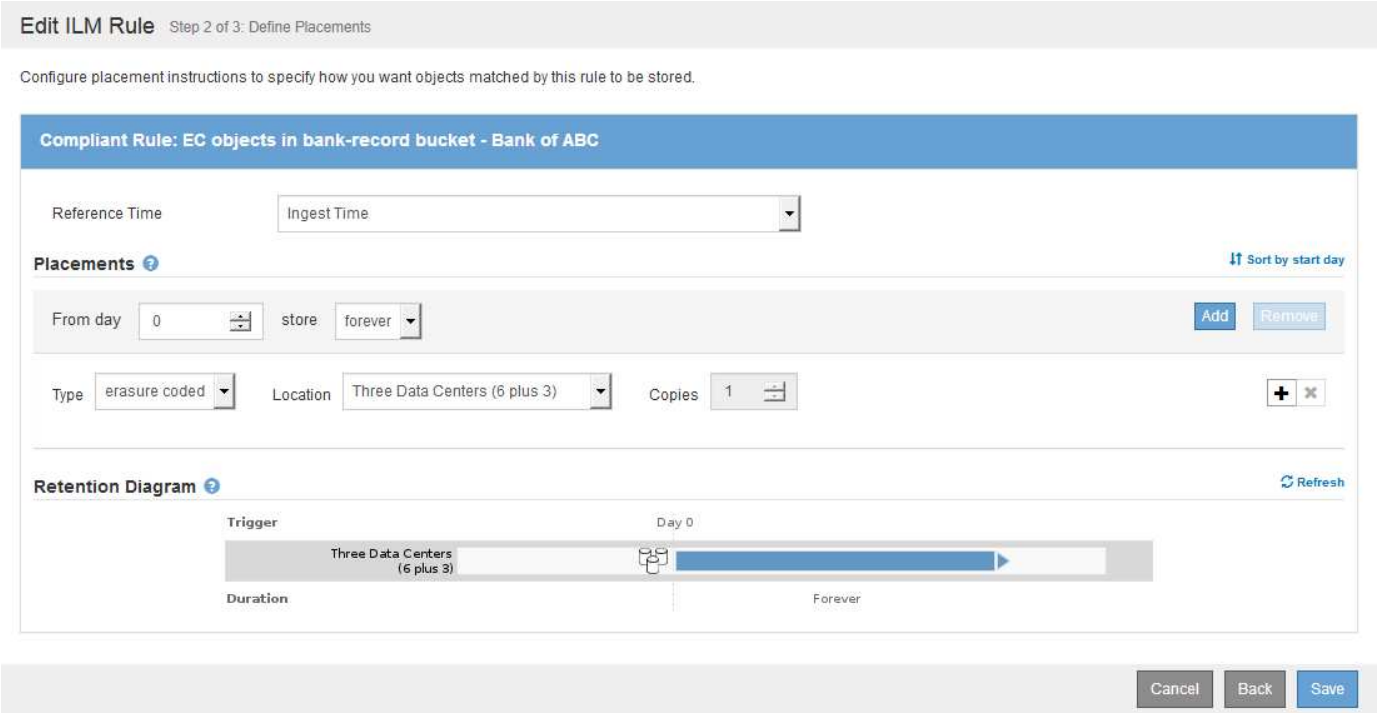
이 ILM 규칙 예는 Bank of ABC라는 S3 테넌트 계정에만 적용됩니다. 이 삭제 코딩은 '뱅크 레코드' 버킷의 모든 오브젝트를 일치시킨 다음 삭제 코딩을 사용하여 6개 + 3개의 삭제 코딩 프로필을 사용하여 3개의 데이터 센터 사이트에 있는 스토리지 노드에 오브젝트를 저장합니다. 이 규칙은 S3 오브젝트 잠금이 설정된 버킷의 요구 사항을 충족합니다. 즉, 삭제 코딩 복사본이 0일부터 영원까지 스토리지 노드에 보관되며, Ingest 시간을 참조 시간으로 사용합니다.

규칙 정의	예제 값
규칙 이름	규정 준수 규칙: 은행 레코드 버킷의 EC 오브젝트 - ABC 은행
테넌트 계정	ABC 은행
버킷 이름	은행기록

규칙 정의	예제 값
고급 필터링	개체 크기(MB)가 1보다 큽니다 • 참고: * 이 필터는 삭제 코딩이 1MB 이하의 오브젝트에 사용되지 않도록 합니다.



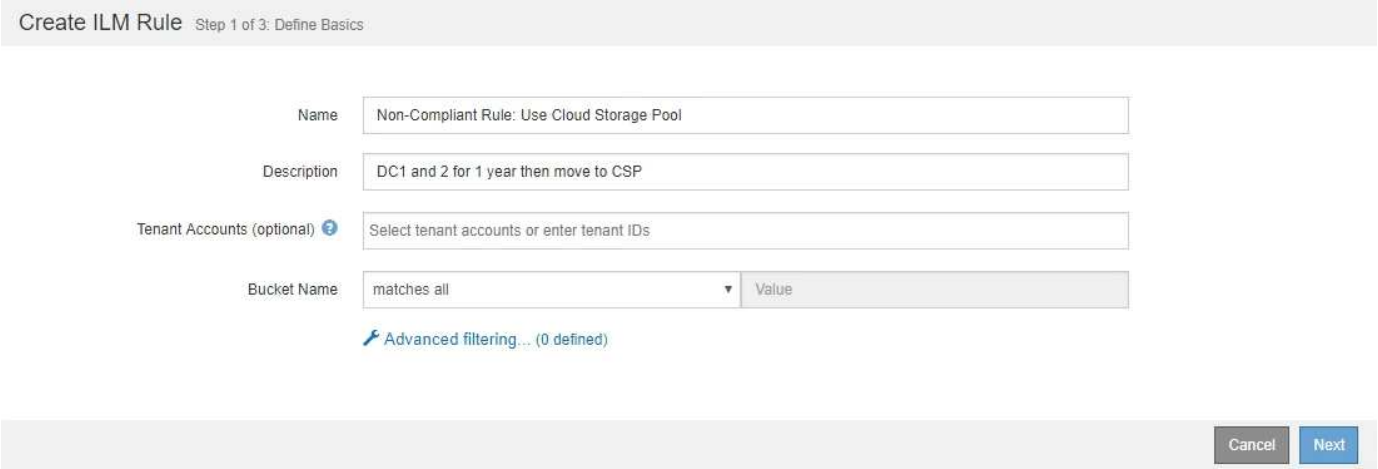
규칙 정의	예제 값
참조 시간	수집 시간
배치	0일째부터 영원히
삭제 코딩 프로필	• 3개의 데이터 센터 사이트에서 스토리지 노드에 삭제 코딩 복사본을 생성합니다 • 6+3 삭제 코딩 방법을 사용합니다



S3 오브젝트 잠금에 대한 **ILM** 규칙 **2** 예**:** 비준수 규칙

이 ILM 규칙은 처음에 두 개의 복제된 오브젝트 복사본을 스토리지 노드에 저장합니다. 1년이 지나면 Cloud Storage Pool에 하나의 복사본이 영구 저장됩니다. 이 규칙은 Cloud Storage Pool을 사용하기 때문에 S3 Object Lock이 설정된 버킷의 오브젝트에는 적용되지 않고 호환되지 않습니다.

규칙 정의	예제 값
규칙 이름	규정 위반 규칙: 클라우드 스토리지 풀 사용
테넌트 계정	지정되지 않음
버킷 이름	지정되지 않았지만 S3 오브젝트 잠금(또는 레거시 규정 준수 기능)이 활성화되지 않은 버킷에만 적용됩니다.
고급 필터링	지정되지 않음

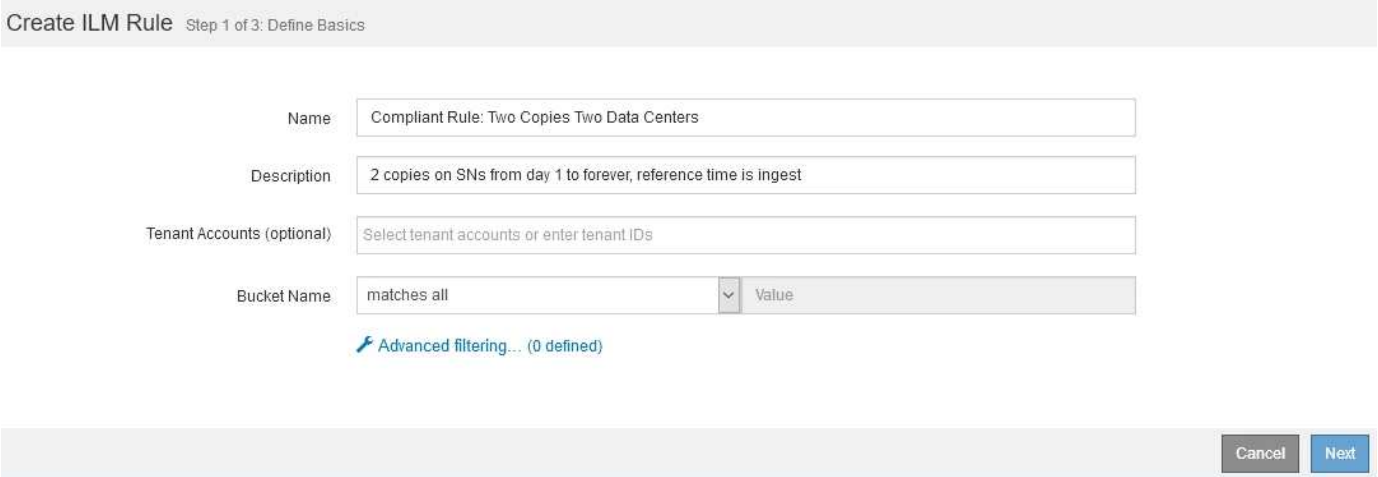


규칙 정의	예제 값
참조 시간	수집 시간
배치	• 0일째, 데이터 센터 1의 스토리지 노드에 복제된 복사본 2개를 유지하고 365일 동안 데이터 센터 2를 유지합니다 • 1년 후에는 복제된 복사본 하나를 Cloud Storage Pool에 영구 보관합니다

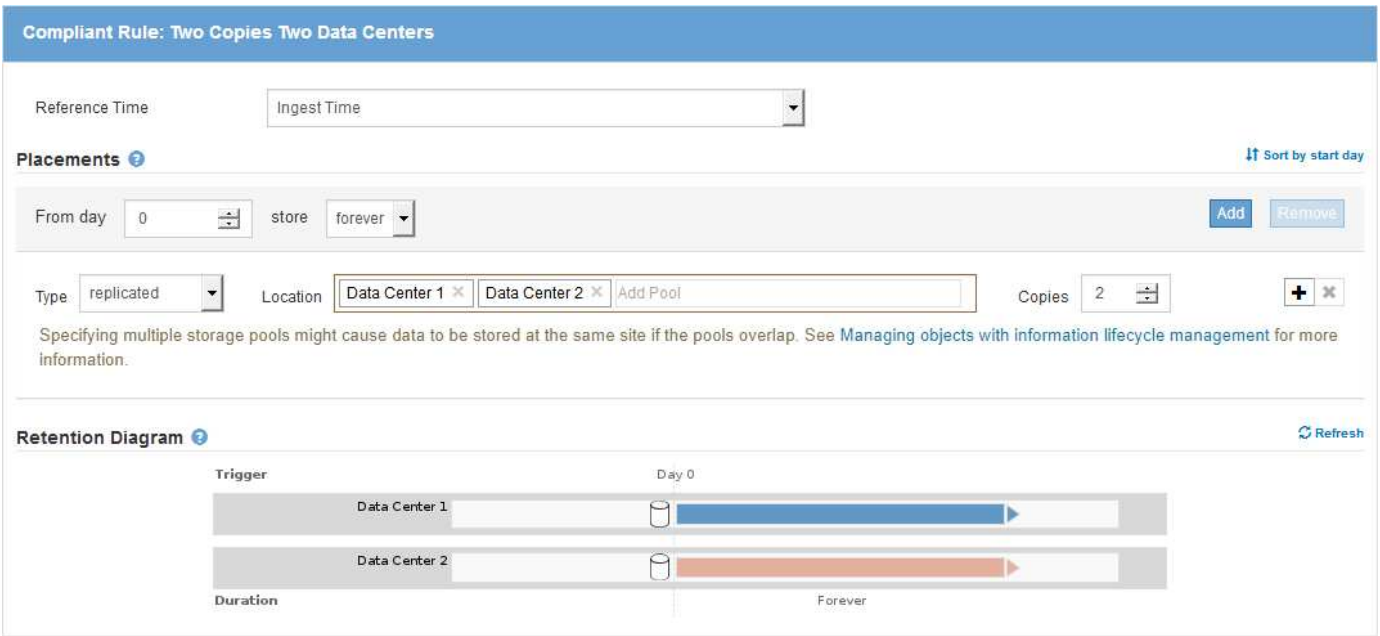
S3 오브젝트 잠금에 대한 **ILM** 규칙 **3** 예**:** 기본 규칙

이 ILM 규칙 예에서는 오브젝트 데이터를 두 데이터 센터의 스토리지 풀로 복사합니다. 이 규정 준수 규칙은 ILM 정책의 기본 규칙으로 설계되었습니다. 이 노드에는 필터가 포함되지 않으며, 비현재 참조 시간을 사용하지 않으며, S3 오브젝트 잠금이 설정된 버킷의 요구 사항을 충족합니다. 즉, Ingest를 참조 시간으로 사용하여 오브젝트 복사본 2개가 0부터 영원까지 스토리지 노드에 보관됩니다.

규칙 정의	예제 값
규칙 이름	기본 규정 준수 규칙: 복사본 2개 데이터 센터
테넌트 계정	지정되지 않음
버킷 이름	지정되지 않음
고급 필터링	지정되지 않음



규칙 정의	예제 값
참조 시간	수집 시간
배치	0일째부터 영구, 복제된 복사본 두 개 유지 - 하나는 데이터 센터 1의 스토리지 노드에, 다른 하나는 데이터 센터 2의 스토리지 노드에 있습니다.



S3 오브젝트 잠금에 대한 규정 준수 **ILM** 정책 예

S3 Object Lock이 설정된 버킷에 포함된 개체를 포함하여 시스템의 모든 개체를 효과적으로 보호하는 ILM 정책을 생성하려면 모든 개체의 스토리지 요구사항을 충족하는 ILM 규칙을 선택해야 합니다. 그런 다음 제안된 정책을 시뮬레이션하고 활성화해야 합니다.

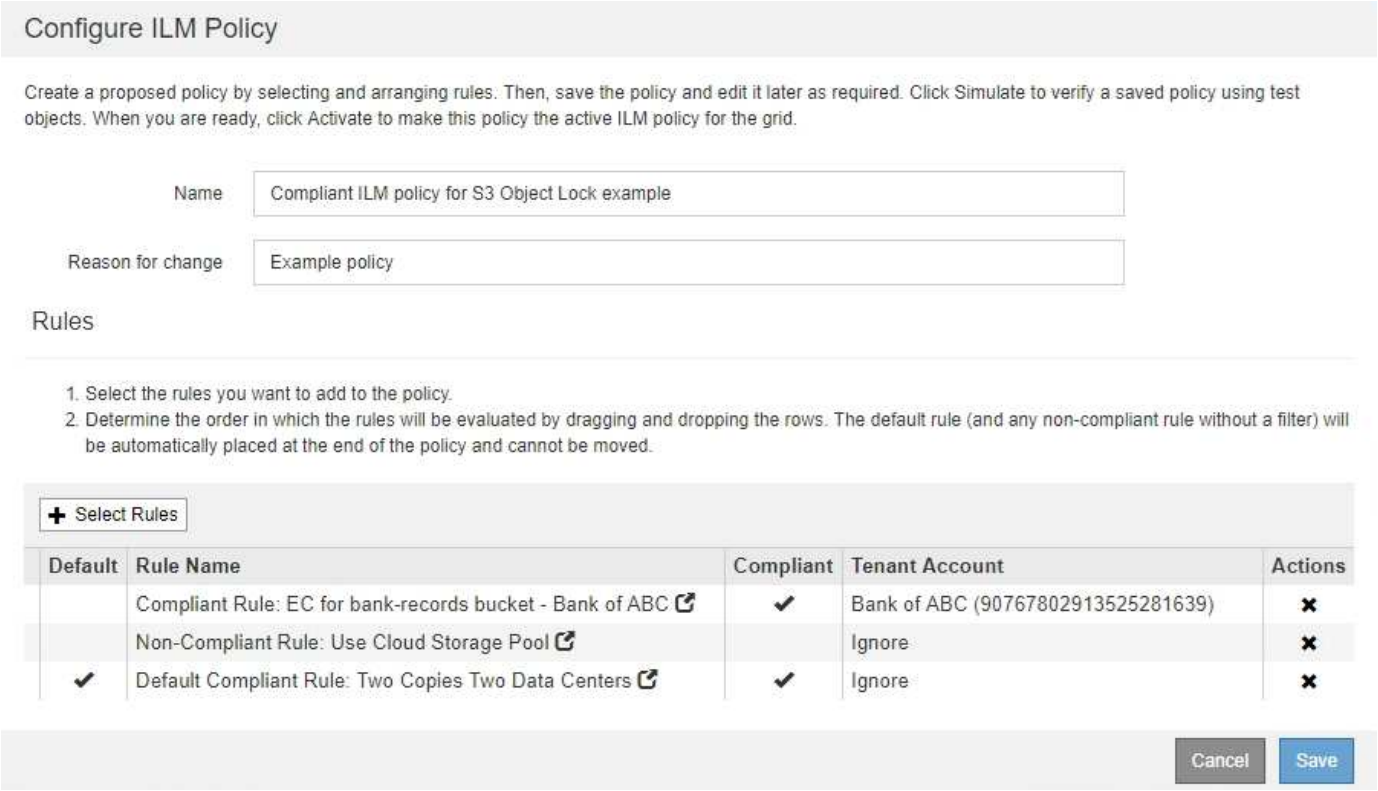
정책에 규칙을 추가합니다

이 예에서 ILM 정책에는 다음 순서로 세 가지 ILM 규칙이 포함되어 있습니다.

1. S3 오브젝트 잠금이 활성화된 특정 버킷에서 삭제 코딩을 사용하여 1MB 이상의 오브젝트를 보호하는 규정 준수

규칙입니다. 오브젝트는 0일부터 영원까지 스토리지 노드에 저장됩니다.

2. 1년 동안 스토리지 노드에 2개의 복제된 오브젝트 복사본을 생성한 다음 하나의 오브젝트 복사본을 클라우드 스토리지 풀로 영구적으로 이동하는 규정을 준수하지 않습니다. 이 규칙은 클라우드 스토리지 풀을 사용하기 때문에 S3 오브젝트 잠금이 설정된 버킷에는 적용되지 않습니다.
3. 스토리지 노드에 복제된 오브젝트 복사본 2개를 생성하는 기본 규정 준수 규칙입니다.



제안된 정책을 시뮬레이션합니다

제안된 정책에 규칙을 추가하고 기본 규정 준수 규칙을 선택하고 다른 규칙을 정렬한 후에는 S3 오브젝트 잠금이 활성화된 버킷과 다른 버킷에서 객체를 테스트하여 정책을 시뮬레이션해야 합니다. 예를 들어, 예제 정책을 시뮬레이션할 때 테스트 개체는 다음과 같이 평가됩니다.

- 첫 번째 규칙은 Bank of ABC Tenant의 버킷 뱅크 레코드에 1MB보다 큰 테스트 오브젝트만 일치시킵니다.
- 두 번째 규칙은 다른 모든 테넌트 계정에 대해 모든 비준수 버킷의 모든 오브젝트를 일치시킵니다.
- 기본 규칙은 다음 개체와 일치합니다.
  - BANK BANK BANK에서 객체 1MB 이하 - ABC 테넌트의 은행 레코드.
  - 다른 모든 테넌트 계정에 대해 S3 Object Lock이 활성화된 다른 버킷의 오브젝트

정책을 활성화합니다

새 정책이 예상대로 개체 데이터를 보호한다고 완전히 만족할 경우 이를 활성화할 수 있습니다.

시스템 강화

시스템 강화: 개요

시스템 강화는 StorageGRID 시스템에서 가능한 한 많은 보안 위험을 제거하는 프로세스입니다.

이 문서에서는 StorageGRID와 관련된 강화 지침에 대해 간략하게 설명합니다. 이 지침은 시스템 강화를 위한 업계 표준 모범 사례를 보완합니다. 예를 들어, 이 지침에서는 StorageGRID에 강력한 암호를 사용하고 HTTP 대신 HTTPS를 사용하고 가능한 경우 인증서 기반 인증을 활성화한다고 가정합니다.

StorageGRID를 설치 및 구성할 때 이 지침을 사용하여 정보 시스템의 기밀성, 무결성 및 가용성에 대해 규정된 모든 보안 목표를 충족할 수 있습니다.

StorageGRID은 _ NetApp 취약점 처리 정책 _ 을(를) 따릅니다. 보고된 취약점은 제품 보안 사고 대응 프로세스에 따라 확인 및 해결됩니다.

StorageGRID 시스템 강화를 위한 일반 고려 사항

StorageGRID 시스템을 강화하려면 다음 사항을 고려해야 합니다.

- 구현한 3개의 StorageGRID 네트워크는 무엇입니까? 모든 StorageGRID 시스템은 그리드 네트워크를 사용해야 하지만 관리자 네트워크, 클라이언트 네트워크 또는 둘 다를 사용할 수도 있습니다. 각 네트워크마다 서로 다른 보안 고려 사항이 있습니다.
- StorageGRID 시스템의 개별 노드에 사용하는 플랫폼 유형입니다. StorageGRID 노드는 VMware 가상 머신, Linux 호스트의 컨테이너 엔진 내부 또는 전용 하드웨어 어플라이언스에 구축할 수 있습니다. 각 플랫폼 유형에는 강화 모범 사례가 자체적으로 있습니다.
- 테넌트 계정의 신뢰성. 신뢰할 수 없는 테넌트 계정을 사용하는 서비스 공급자라면 신뢰할 수 있는 내부 테넌트만 사용하는 것과 보안 문제가 다릅니다.
- 조직의 보안 요구 사항 및 규약 뒤에 오는 것은 무엇입니까? 특정 규정 또는 기업 요구 사항을 준수해야 할 수 있습니다.

관련 정보

"취약점 처리 정책"

소프트웨어 업그레이드 강화 지침

공격을 방어하려면 StorageGRID 시스템 및 관련 서비스를 최신 상태로 유지해야 합니다.

StorageGRID 소프트웨어로 업그레이드합니다

가능하면 StorageGRID 소프트웨어를 최신 주요 릴리즈나 이전 주요 릴리즈로 업그레이드해야 합니다. StorageGRID를 최신 상태로 유지하면 알려진 취약점이 활성화되는 시간을 줄이고 전체 공격 노출 영역을 줄일 수 있습니다. 또한 최신 버전의 StorageGRID에는 이전 릴리즈에 포함되지 않은 보안 강화 기능이 포함되어 있는 경우가 많습니다.

핫픽스가 필요한 경우 NetApp은 가장 최근 릴리즈에 대한 업데이트를 만드는 데 우선 순위를 지정합니다. 일부 패치는 이전 릴리스와 호환되지 않을 수 있습니다.

최신 StorageGRID 릴리스 및 핫픽스를 다운로드하려면 StorageGRID 소프트웨어 다운로드 페이지로 이동하십시오. StorageGRID 소프트웨어 업그레이드에 대한 단계별 지침은 StorageGRID 업그레이드 지침을 참조하십시오. 핫픽스를 적용하는 방법은 복구 및 유지 관리 지침을 참조하십시오.

외부 서비스로 업그레이드

외부 서비스에는 StorageGRID에 간접적으로 영향을 주는 취약점이 있을 수 있습니다. StorageGRID가 의존하는 서비스를 최신 상태로 유지해야 합니다. 이러한 서비스에는 LDAP, KMS(또는 KMIP 서버), DNS 및 NTP가 포함됩니다.

NetApp 상호 운용성 매트릭스 툴을 사용하여 지원되는 버전 목록을 확인하십시오.

하이퍼바이저로 업그레이드

StorageGRID 노드가 VMware 또는 다른 하이퍼바이저에서 실행 중인 경우 하이퍼바이저 소프트웨어 및 펌웨어를 최신 상태로 유지해야 합니다.

NetApp 상호 운용성 매트릭스 툴을 사용하여 지원되는 버전 목록을 확인하십시오.

*** Linux** 노드로 업그레이드 *****

StorageGRID 노드가 Linux 호스트 플랫폼을 사용하는 경우 보안 업데이트 및 커널 업데이트가 호스트 OS에 적용되었는지 확인해야 합니다. 또한 이러한 업데이트를 사용할 수 있게 되면 취약한 하드웨어에 펌웨어 업데이트를 적용해야 합니다.

NetApp 상호 운용성 매트릭스 툴을 사용하여 지원되는 버전 목록을 확인하십시오.

관련 정보

"NetApp 다운로드: StorageGRID"

소프트웨어 업그레이드

복구 및 유지 관리

"NetApp 상호 운용성 매트릭스 툴"

StorageGRID 네트워크에 대한 강화 지침

StorageGRID 시스템은 그리드 노드당 최대 3개의 네트워크 인터페이스를 지원하므로 각 개별 그리드 노드에 대한 네트워킹을 보안 및 액세스 요구 사항에 맞게 구성할 수 있습니다.

그리드 네트워크 지침

모든 내부 StorageGRID 트래픽에 대해 그리드 네트워크를 구성해야 합니다. 모든 그리드 노드는 그리드 네트워크에 있으며 다른 모든 노드와 통신할 수 있어야 합니다.

그리드 네트워크를 구성할 때 다음 지침을 따르십시오.

- 네트워크가 인터넷에 있는 클라이언트와 같이 신뢰할 수 없는 클라이언트로부터 보호되는지 확인합니다.
- 가능한 경우 내부 트래픽에만 그리드 네트워크를 사용합니다. 관리 네트워크와 클라이언트 네트워크 모두 내부 서비스에 대한 외부 트래픽을 차단하는 추가 방화벽 제한이 있습니다. 외부 클라이언트 트래픽에 그리드 네트워크 사용이 지원되지만, 이러한 사용은 보호 계층의 수를 줄입니다.
- StorageGRID 구축이 여러 데이터 센터에 걸쳐 있는 경우, 내부 트래픽을 추가로 보호하기 위해 VPN(가상 사설망) 또는 이와 동등한 그리드 네트워크를 사용합니다.
- 일부 유지 관리 절차에서는 기본 관리 노드와 다른 모든 그리드 노드 사이의 포트 22에서 SSH(Secure Shell)

액세스가 필요합니다. 외부 방화벽을 사용하여 신뢰할 수 있는 클라이언트에 대한 SSH 액세스를 제한합니다.

관리 네트워크 지침

관리 네트워크는 일반적으로 관리 작업(Grid Manager 또는 SSH를 사용하는 신뢰할 수 있는 직원)과 LDAP, DNS, NTP 또는 KMS(또는 KMIP 서버)와 통신하는 데 사용됩니다. 그러나 StorageGRID에서는 이 사용을 내부적으로 적용하지 않습니다.

관리자 네트워크를 사용하는 경우 다음 지침을 따르십시오.

- 관리 네트워크의 모든 내부 트래픽 포트를 차단합니다. 해당 플랫폼의 설치 가이드에서 내부 포트 목록을 참조하십시오.
- 신뢰할 수 없는 클라이언트가 관리자 네트워크에 액세스할 수 있는 경우 외부 방화벽을 사용하여 관리자 네트워크의 StorageGRID에 대한 액세스를 차단합니다.

클라이언트 네트워크 지침

클라이언트 네트워크는 일반적으로 테넌트에 사용되며 CloudMirror 복제 서비스 또는 다른 플랫폼 서비스와 같은 외부 서비스와 통신하는 데 사용됩니다. 그러나 StorageGRID에서는 이 사용을 내부적으로 적용하지 않습니다.

클라이언트 네트워크를 사용하는 경우 다음 지침을 따르십시오.

- 클라이언트 네트워크의 모든 내부 트래픽 포트를 차단합니다. 해당 플랫폼의 설치 가이드에서 내부 포트 목록을 참조하십시오.
- 명시적으로 구성된 끝점에서만 인바운드 클라이언트 트래픽을 허용합니다. 을 참조하십시오 신뢰할 수 없는 클라이언트 네트워크 관리.

관련 정보

네트워킹 지침

그리드 프라이머

StorageGRID 관리

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

Ubuntu 또는 Debian을 설치합니다

VMware를 설치합니다

StorageGRID 노드에 대한 강화 지침

StorageGRID 노드는 VMware 가상 머신, Linux 호스트의 컨테이너 엔진 내부 또는 전용 하드웨어 어플라이언스에 구축할 수 있습니다. 각 플랫폼 유형과 각 노드 유형에는 강화 모범 사례가 포함되어 있습니다.

방화벽 구성

시스템 강화 프로세스의 일환으로 외부 방화벽 구성을 검토하고 트래픽이 IP 주소 및 해당 IP 주소가 반드시 필요한 포트에서만 허용되도록 수정해야 합니다.

StorageGRID는 자동으로 관리되는 내부 방화벽을 사용합니다. 이 내부 방화벽은 일부 일반적인 위협에 대한 추가 보호 계층을 제공하지만 외부 방화벽의 필요성을 제거하지 않습니다.

StorageGRID에서 사용하는 모든 내부 및 외부 포트 목록은 해당 플랫폼의 설치 가이드를 참조하십시오.

가상화, 컨테이너 및 공유 하드웨어

모든 StorageGRID 노드의 경우 신뢰할 수 없는 소프트웨어와 동일한 물리적 하드웨어에서 StorageGRID를 실행하지 마십시오. StorageGRID와 맬웨어가 모두 동일한 물리적 하드웨어에 존재할 경우 하이퍼바이저 보호를 통해 맬웨어가 StorageGRID로 보호되는 데이터에 액세스하지 못할 것이라고 가정하지 마십시오. 예를 들어 멜트다운 및 스펙터 공격은 최신 프로세서의 중요한 취약점을 악용하고 프로그램이 동일한 컴퓨터의 메모리에 있는 데이터를 훔칠 수 있도록 합니다.

사용하지 않는 서비스를 비활성화합니다

모든 StorageGRID 노드에 대해 사용하지 않는 서비스에 대한 액세스를 비활성화하거나 차단해야 합니다. 예를 들어 CIFS 또는 NFS에 대한 감사 공유에 대한 클라이언트 액세스를 구성하지 않을 경우 이러한 서비스에 대한 액세스를 차단하거나 해제합니다.

설치하는 동안 노드를 보호합니다

노드가 설치될 때 신뢰할 수 없는 사용자가 네트워크를 통해 StorageGRID 노드에 액세스하도록 허용하지 마십시오. 노드가 그리드에 가입될 때까지 완전히 보안되지 않습니다.

관리 노드에 대한 지침

관리 노드는 시스템 구성, 모니터링 및 로깅과 같은 관리 서비스를 제공합니다. 그리드 관리자 또는 테넌트 관리자에 로그인할 때 관리 노드에 연결됩니다.

다음 지침에 따라 StorageGRID 시스템의 관리 노드를 보호합니다.

- 인터넷에 있는 클라이언트와 같이 신뢰할 수 없는 클라이언트의 모든 관리 노드를 보호합니다. 신뢰할 수 없는 클라이언트가 그리드 네트워크, 관리 네트워크 또는 클라이언트 네트워크의 관리 노드에 액세스할 수 있는지 확인합니다.
- StorageGRID 그룹은 그리드 관리자 및 테넌트 관리자 기능에 대한 액세스를 제어합니다. 각 사용자 그룹에 역할에 필요한 최소 권한을 부여하고 읽기 전용 액세스 모드를 사용하여 사용자가 구성을 변경하지 못하도록 합니다.
- StorageGRID 로드 밸런서 끝점을 사용할 때는 신뢰할 수 없는 클라이언트 트래픽에 관리자 노드 대신 게이트웨이 노드를 사용합니다.
- 신뢰할 수 없는 테넌트가 있는 경우 테넌트 관리자 또는 테넌트 관리 API에 대한 직접 액세스 권한을 허용하지 마십시오. 대신 신뢰할 수 없는 테넌트가 테넌트 관리 API와 상호 작용하는 테넌트 포털 또는 외부 테넌트 관리 시스템을 사용하도록 합니다.
- 선택적으로 관리 프록시를 사용하여 관리 노드에서 NetApp 지원으로 AutoSupport 통신을 더 많이 제어할 수 있습니다. StorageGRID 관리 지침에 있는 관리자 프록시 생성 단계를 참조하십시오.
- 필요에 따라 제한된 8443 및 9443 포트를 사용하여 Grid Manager 및 Tenant Manager 통신을 분리합니다. 추가 보호를 위해 공유 포트 443을 차단하고 테넌트 요청을 포트 9443으로 제한합니다.
- 선택적으로 그리드 관리자 및 테넌트 사용자에 대해 별도의 관리 노드를 사용합니다.

자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

스토리지 노드 지침

스토리지 노드: 오브젝트 데이터 및 메타데이터를 관리하고 저장합니다. 다음 지침에 따라 StorageGRID 시스템의 스토리지 노드를 보호합니다.

- 신뢰할 수 없는 클라이언트가 스토리지 노드에 직접 연결하도록 허용하지 않습니다. 게이트웨이 노드 또는 타사 로드 밸런서가 제공하는 로드 밸런서 끝점을 사용합니다.
- 신뢰할 수 없는 테넌트에 대해 아웃바운드 서비스를 활성화하지 마십시오. 예를 들어, 신뢰할 수 없는 테넌트의 계정을 생성할 때 테넌트가 자신의 ID 소스를 사용하도록 허용하지 않고 플랫폼 서비스의 사용을 허용하지 않습니다. StorageGRID 관리 지침에 있는 테넌트 계정 생성 단계를 참조하십시오.
- 신뢰할 수 없는 클라이언트 트래픽에 타사 로드 밸런서를 사용합니다. 타사 로드 밸런싱은 더 많은 제어 기능과 공격에 대한 추가적인 보호 계층을 제공합니다.
- 필요한 경우 스토리지 프록시를 사용하여 스토리지 노드에서 외부 서비스로의 클라우드 스토리지 풀 및 플랫폼 서비스 통신을 보다 효과적으로 제어할 수 있습니다. StorageGRID 관리 지침에 있는 스토리지 프록시 생성 단계를 참조하십시오.
- 선택적으로 클라이언트 네트워크를 사용하여 외부 서비스에 연결합니다. 그런 다음 * 구성 * > * 네트워크 * > * 신뢰할 수 없는 클라이언트 네트워크 * 를 선택하고 스토리지 노드의 클라이언트 네트워크를 신뢰할 수 없음을 표시합니다. 스토리지 노드는 더 이상 클라이언트 네트워크에서 들어오는 트래픽을 허용하지 않지만 플랫폼 서비스에 대한 아웃바운드 요청은 계속 허용합니다.

게이트웨이 노드에 대한 지침

게이트웨이 노드는 클라이언트 애플리케이션이 StorageGRID에 연결하는 데 사용할 수 있는 선택적 로드 밸런싱 인터페이스를 제공합니다. 다음 지침에 따라 StorageGRID 시스템의 게이트웨이 노드를 보호합니다.

- 게이트웨이 노드에서 CLB 서비스를 사용하는 대신 로드 밸런서 끝점을 구성하고 사용합니다. StorageGRID 관리에 대한 지침은 로드 밸런싱 관리 단계를 참조하십시오.

  CLB 서비스는 더 이상 사용되지 않습니다.

- 신뢰할 수 없는 클라이언트 트래픽에 대해 클라이언트와 게이트웨이 노드 또는 스토리지 노드 간에 타사 로드 밸런서를 사용합니다. 타사 로드 밸런싱은 더 많은 제어 기능과 공격에 대한 추가적인 보호 계층을 제공합니다. 타사 로드 밸런서를 사용하는 경우에도 내부 로드 밸런서 엔드포인트를 통과하도록 네트워크 트래픽을 선택적으로 구성하거나 스토리지 노드로 직접 보내도록 구성할 수 있습니다.
- 부하 분산 엔드포인트를 사용하는 경우 선택적으로 클라이언트가 클라이언트 네트워크를 통해 접속하도록 합니다. 그런 다음 * 구성 * > * 네트워크 * > * 신뢰할 수 없는 클라이언트 네트워크 * 를 선택하고 게이트웨이 노드의 클라이언트 네트워크를 신뢰할 수 없음을 표시합니다. 게이트웨이 노드는 로드 밸런서 끝점으로 명시적으로 구성된 포트의 인바운드 트래픽만 허용합니다.

하드웨어 어플라이언스 노드에 대한 지침입니다

StorageGRID 하드웨어 어플라이언스는 StorageGRID 시스템에서 사용하도록 특별히 설계되었습니다. 일부 어플라이언스는 스토리지 노드로 사용할 수 있습니다. 다른 어플라이언스를 관리 노드 또는 게이트웨이 노드로 사용할 수 있습니다. 어플라이언스 노드를 소프트웨어 기반 노드와 결합하거나 완전히 엔지니어링된 모든 어플라이언스 그리드를 구축할 수 있습니다.

StorageGRID 시스템에서 하드웨어 어플라이언스 노드를 보호하려면 다음 지침을 따르십시오.

- 어플라이언스가 스토리지 컨트롤러 관리에 SANtricity System Manager를 사용하는 경우 신뢰할 수 없는 클라이언트가 네트워크를 통해 SANtricity System Manager에 액세스하지 못하도록 합니다.

- 어플라이언스에 BMC(베이스보드 관리 컨트롤러)가 있는 경우 BMC 관리 포트가 낮은 수준의 하드웨어 액세스를 허용한다는 점에 유의하십시오. BMC 관리 포트는 안전하고 신뢰할 수 있는 내부 관리 네트워크에만 연결합니다. 이러한 네트워크를 사용할 수 없는 경우 기술 지원 부서에서 BMC 연결을 요청하지 않는 한 BMC 관리 포트는 연결되지 않거나 차단된 상태로 둡니다.
- 어플라이언스가 IPMI(Intelligent Platform Management Interface) 표준을 사용하여 이더넷을 통한 컨트롤러 하드웨어의 원격 관리를 지원하는 경우 포트 623에서 신뢰할 수 없는 트래픽을 차단합니다.
- 어플라이언스의 스토리지 컨트롤러에 FDE 또는 FIPS 드라이브가 포함되어 있고 드라이브 보안 기능이 활성화된 경우 SANtricity를 사용하여 드라이브 보안 키를 구성하십시오.
- FDE 또는 FIPS 드라이브가 없는 어플라이언스의 경우 KMS(Key Management Server)를 사용하여 노드 암호화를 활성화합니다.

StorageGRID 하드웨어 어플라이언스의 설치 및 유지보수 지침을 참조하십시오.

관련 정보

- Red Hat Enterprise Linux 또는 CentOS를 설치합니다
- Ubuntu 또는 Debian을 설치합니다
- VMware를 설치합니다
- StorageGRID 관리
- 테넌트 계정을 사용합니다
- SG100 및 SG1000 서비스 어플라이언스
- SG5600 스토리지 어플라이언스
- SG5700 스토리지 어플라이언스
- SG6000 스토리지 어플라이언스

서버 인증서에 대한 강화 지침

설치 중에 생성된 기본 인증서를 사용자 지정 인증서로 교체해야 합니다.

많은 조직에서 StorageGRID 웹 액세스를 위한 자체 서명된 디지털 인증서가 정보 보안 정책을 준수하지 않습니다. 프로덕션 시스템에서는 StorageGRID 인증에 사용할 CA 서명 디지털 인증서를 설치해야 합니다.

특히 다음과 같은 기본 인증서 대신 사용자 지정 서버 인증서를 사용해야 합니다.

- * 관리 인터페이스 인증서 *: 그리드 관리자, 테넌트 관리자, 그리드 관리 API 및 테넌트 관리 API에 대한 액세스를 보호하는 데 사용됩니다.
- * S3 및 Swift API 인증서 *: S3 및 Swift 클라이언트 애플리케이션이 오브젝트 데이터를 업로드 및 다운로드하는 데 사용하는 스토리지 노드 및 게이트웨이 노드에 대한 액세스를 보호하는 데 사용됩니다.

> StorageGRID는 로드 밸런서 끝점에 사용되는 인증서를 별도로 관리합니다. 로드 밸런서 인증서를 구성하려면 StorageGRID 관리 지침 에서 로드 밸런서 엔드포인트를 구성하는 단계를 참조하십시오.

사용자 지정 서버 인증서를 사용하는 경우 다음 지침을 따르십시오.

- 인증서에는 StorageGRID의 DNS 항목과 일치하는 "*subjectAltName*"이(가) 있어야 합니다. 자세한 내용은 의 4.2.1.6 "대체 이름" 단원을 참조하십시오 "RFC 5280: PKIX 인증서 및 CRL 프로필".

- 가능한 경우 와일드카드 인증서를 사용하지 마십시오. 이 지침의 예외는 S3 가상 호스팅 스타일 엔드포인트에 대한 인증서이며, 버킷 이름을 미리 모르는 경우 와일드카드를 사용해야 합니다.
- 인증서에 와일드카드를 사용해야 하는 경우 위험을 줄이기 위해 추가 단계를 수행해야 합니다. '* .s3.example.com ' 와 같은 와일드카드 패턴을 사용하고 다른 응용 프로그램에는 '3.example.com' 접미사를 사용하지 마십시오. 이 패턴은 경로 스타일 S3 액세스(예: ddc1-s1.s3.example.com/mybucket`)에서도 사용할 수 있습니다.
- 인증서 만료 시간을 짧게(예: 2개월) 설정하고 그리드 관리 API를 사용하여 인증서 회전을 자동화합니다. 이것은 와일드카드 인증서에 특히 중요합니다.

또한 클라이언트는 StorageGRID과 통신할 때 엄격한 호스트 이름 확인을 사용해야 합니다.

기타 강화 지침

StorageGRID 네트워크 및 노드에 대한 강화 지침을 따르는 것 외에도 StorageGRID 시스템의 다른 영역에 대한 강화 지침을 따라야 합니다.

로그 및 감사 메시지

항상 안전한 방법으로 StorageGRID 로그 및 감사 메시지 출력을 보호합니다. StorageGRID 로그 및 감사 메시지는 지원 및 시스템 가용성의 관점에서 중요한 정보를 제공합니다. 또한 StorageGRID 로그 및 감사 메시지 출력에 포함된 정보와 세부 정보는 일반적으로 민감한 특성을 가지고 있습니다.

보안 이벤트를 외부 syslog 서버로 보내도록 StorageGRID를 구성합니다. syslog 내보내기를 사용하는 경우 전송 프로토콜에 대해 TLS 및 RELP/TLS를 선택합니다.

StorageGRID 로그에 대한 자세한 내용은 모니터링 및 문제 해결 지침을 참조하십시오. StorageGRID 감사 메시지에 대한 자세한 내용은 감사 메시지 지침을 참조하십시오.

NetApp AutoSupport를 참조하십시오

StorageGRID의 AutoSupport 기능을 사용하면 시스템 상태를 능동적으로 모니터링하고 메시지 및 세부 정보를 NetApp 기술 지원, 조직의 내부 지원 팀 또는 지원 파트너에게 자동으로 전송할 수 있습니다. 기본적으로 StorageGRID를 처음 구성하면 NetApp 기술 지원에 보내는 AutoSupport 메시지가 활성화됩니다.

AutoSupport 기능을 비활성화할 수 있습니다. 하지만 AutoSupport는 StorageGRID 시스템에서 문제가 발생할 경우 문제를 빠르게 식별하고 해결할 수 있도록 하므로 NetApp에서 이 기능을 사용하도록 권장합니다.

AutoSupport는 전송 프로토콜을 위해 HTTPS, HTTP 및 SMTP를 지원합니다. AutoSupport 메시지는 기본적으로 민감하므로 NetApp 지원에 AutoSupport 메시지를 보낼 때 HTTPS를 기본 전송 프로토콜로 사용하는 것이 좋습니다.

선택적으로 관리자 노드에서 NetApp 기술 지원으로 AutoSupport 통신을 더 많이 제어할 수 있도록 관리자 프록시를 구성할 수 있습니다. StorageGRID 관리 지침에 있는 관리자 프록시 생성 단계를 참조하십시오.

CORS(Cross-Origin Resource Sharing)

다른 도메인의 웹 애플리케이션에서 해당 버킷의 버킷 및 오브젝트에 액세스할 수 있도록 하려면 S3 버킷에 대해 CORS(Cross-Origin Resource Sharing)를 구성할 수 있습니다. 일반적으로 CORS가 필요한 경우가 아니면 활성화하지 마십시오. CORS가 필요한 경우 신뢰할 수 있는 오리진으로 제한합니다.

테넌트 계정 사용 지침에 있는 CORS(Cross-Origin Resource Sharing) 구성 단계를 참조하십시오.

외부 보안 장치

완벽한 강화 솔루션은 StorageGRID 외부의 보안 메커니즘을 해결해야 합니다. StorageGRID에 대한 액세스를 필터링하고 제한하는 데 추가 인프라 장치를 사용하는 것은 엄격한 보안 상태를 설정하고 유지하는 효과적인 방법입니다. 이러한 외부 보안 장치에는 방화벽, IPS(침입 방지 시스템) 및 기타 보안 장치가 포함됩니다.

신뢰할 수 없는 클라이언트 트래픽에는 타사 로드 밸런서가 권장됩니다. 타사 로드 밸런싱은 더 많은 제어 기능과 공격에 대한 추가적인 보호 계층을 제공합니다.

관련 정보

모니터링하고 문제를 해결합니다

감사 로그를 검토합니다

테넌트 계정을 사용합니다

StorageGRID 관리

FabricPool를 구성합니다

StorageGRID for FabricPool 구성: 개요

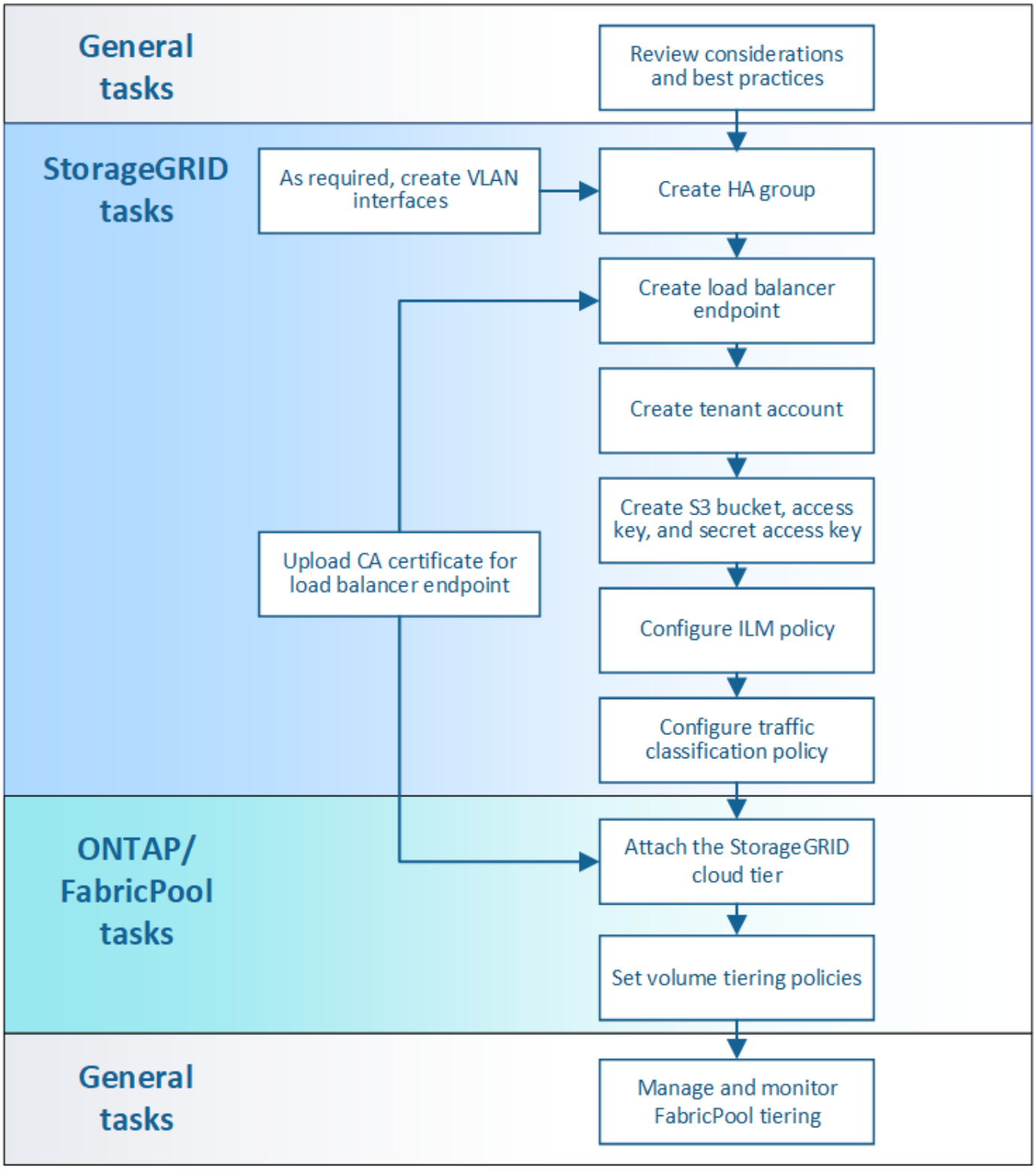
NetApp ONTAP 소프트웨어를 사용하는 경우 NetApp FabricPool를 사용하여 비활성 또는 콜드 데이터를 NetApp StorageGRID 오브젝트 스토리지 시스템에 계층화할 수 있습니다.

참조하십시오

다음 지침을 따르십시오.

- FabricPool에서 사용할 StorageGRID 오브젝트 스토리지 시스템 구성에 대한 개요를 제공합니다.
- StorageGRID를 FabricPool 클라우드 계층으로 연결할 때 ONTAP에 제공하는 정보를 얻는 방법에 대해 알아보십시오.
- StorageGRID ILM(정보 수명 주기 관리) 정책, StorageGRID 트래픽 분류 정책 및 FabricPool 워크로드에 대한 기타 StorageGRID 옵션을 구성하기 위한 모범 사례에 대해 알아보십시오.

구성 워크플로우



시작하기 전에

- 비활성 ONTAP 데이터를 StorageGRID에 계층화하는 데 사용할 FabricPool 볼륨 계층화 정책을 결정합니다.
- 스토리지 용량 및 성능 요구 사항을 충족하도록 StorageGRID 시스템 계획 및 설치
- 그리드 관리자 및 테넌트 관리자를 포함한 StorageGRID 시스템 소프트웨어에 익숙해질 수 있습니다.
- FabricPool 사용 및 구성에 대한 자세한 내용은 다음 추가 리소스를 검토하십시오.

- "TR-4598: ONTAP 9.9.1의 FabricPool 모범 사례"
- "ONTAP 9 설명서"

FabricPool란 무엇입니까**?**

FabricPool는 고성능 플래시 애그리게이트를 성능 계층으로 사용하고 오브젝트 저장소를 클라우드 계층으로 사용하는 ONTAP 하이브리드 스토리지 솔루션입니다. 데이터는 자주 액세스되는지 여부에 따라 운영 스토리지 미디어나 오브젝트 데이터 저장소에 저장됩니다. FabricPool 지원 애그리게이트를 사용하면 성능, 효율성 또는 보호 기능에 영향을 주지 않으면서 스토리지 비용을 절감할 수 있습니다.

아키텍처를 변경할 필요가 없으며 중앙 ONTAP 스토리지 시스템에서 데이터 및 애플리케이션 환경을 계속 관리할 수 있습니다.

StorageGRID란 무엇입니까**?**

StorageGRID는 파일 또는 블록 스토리지와 같은 다른 스토리지 아키텍처와 달리 데이터를 객체로 관리하는 스토리지 아키텍처입니다. 오브젝트는 버킷과 같은 단일 컨테이너 내부에 보관되며 다른 디렉토리 내의 디렉토리 내에 파일로 중첩되지 않습니다. 오브젝트 스토리지는 일반적으로 파일 또는 블록 스토리지보다 성능이 낮지만 확장성이 훨씬 더 높습니다. StorageGRID 버킷에는 페타바이트 단위의 데이터와 수십억 개의 오브젝트를 저장할 수 있습니다.

StorageGRID를 **FabricPool** 클라우드 계층으로 사용하는 이유

FabricPool는 ONTAP 데이터를 StorageGRID를 비롯한 여러 오브젝트 저장소 공급자에 계층화할 수 있습니다. 버킷 또는 컨테이너 레벨에서 지원되는 최대 IOPS(초당 입출력 작업 수)를 설정할 수 있는 퍼블릭 클라우드와 달리, StorageGRID 성능은 시스템의 노드 수에 따라 확장됩니다. StorageGRID를 FabricPool 클라우드 계층으로 사용하면 자체 프라이빗 클라우드에 콜드 데이터를 유지하여 데이터를 최적의 성능으로 완벽하게 제어할 수 있습니다.

또한 StorageGRID를 클라우드 계층으로 사용할 때는 FabricPool 라이센스가 필요하지 않습니다.

StorageGRID에서 여러 **ONTAP** 클러스터를 사용할 수 있습니까**?**

다음 지침은 StorageGRID를 단일 ONTAP 클러스터에 연결하는 방법을 설명합니다. 그러나 동일한 StorageGRID 시스템을 여러 ONTAP 클러스터에 연결할 수 있습니다.

여러 ONTAP 클러스터에서 단일 StorageGRID 시스템으로 데이터를 계층화하기 위한 유일한 요구사항은 각 클러스터에 다른 S3 버킷을 사용해야 한다는 것입니다. 요구 사항에 따라 모든 클러스터에 동일한 고가용성(HA) 그룹, 로드 밸런서 끝점 및 테넌트 계정을 사용하거나 각 클러스터에 대해 이러한 각 항목을 구성할 수 있습니다.

StorageGRID를 클라우드 계층으로 연결

StorageGRID를 클라우드 계층으로 연결하는 데 필요한 정보

StorageGRID를 FabricPool의 클라우드 계층으로 연결하려면 먼저 StorageGRID에서 몇 가지 구성 단계를 수행하고 특정 값을 얻어야 합니다.

이 작업에 대해

다음 표에는 StorageGRID을 FabricPool의 클라우드 계층으로 연결할 때 ONTAP에 제공해야 하는 정보가 나와 있습니다. 이 섹션의 항목에서는 StorageGRID 그리드 관리자 및 테넌트 관리자를 사용하여 필요한 정보를 얻는 방법을 설명합니다.

> 나열된 정확한 필드 이름과 ONTAP에 필요한 값을 입력하는 프로세스는 ONTAP CLI(스토리지 애그리게이트 오브젝트 저장소 구성 생성) 또는 ONTAP System Manager(* 스토리지 * > * 애그리게이트 및 디스크 * > * 클라우드 계층 *)를 사용하는지 여부에 따라 달라집니다.

자세한 내용은 다음을 참조하십시오.

- "TR-4598: ONTAP 9.9.1의 FabricPool 모범 사례"
- "ONTAP 9 설명서"

ONTAP 필드	설명
오브젝트 저장소 이름	고유하고 설명이 포함된 이름입니다. 예를 들어, 'storageGRID_Cloud_Tier'와 같습니다.
공급자 유형입니다	StorageGRID(ONTAP System Manager) 또는 SGWS(ONTAP CLI).
포트	FabricPool가 StorageGRID에 연결할 때 사용할 포트입니다. StorageGRID 로드 밸런서 끝점을 정의할 때 사용할 포트 번호를 결정합니다. FabricPool용 로드 밸런서 끝점을 만듭니다
서버 이름입니다	StorageGRID 로드 밸런서 끝점의 FQDN(정규화된 도메인 이름)입니다. 예를 들어, '3.storagegrid.company.com`. 다음 사항에 유의하십시오. • 여기에서 지정하는 도메인 이름은 StorageGRID 로드 밸런서 끝점에 대해 업로드하는 CA 인증서의 도메인 이름과 일치해야 합니다. • 이 도메인 이름의 DNS 레코드는 StorageGRID에 연결하는 데 사용할 각 IP 주소에 매핑되어야 합니다. StorageGRID IP 주소에 대해 DNS 서버를 구성합니다
컨테이너 이름입니다	이 ONTAP 클러스터에 사용할 StorageGRID 버킷의 이름입니다. 예를 들어, '배합통'을 예로 들 수 있습니다. 이 버킷을 테넌트 관리자에서 생성하거나 ONTAP 9.10 System Manager부터 FabricPool 설정 마법사를 사용하여 버킷을 생성할 수 있습니다. 다음 사항에 유의하십시오. • 구성을 생성한 후에는 버킷 이름을 변경할 수 없습니다. • 버킷은 버전 관리를 활성화할 수 없습니다. • 데이터를 StorageGRID에 계층화할 각 ONTAP 클러스터에 다른 버킷을 사용해야 합니다. S3 버킷을 생성하고 액세스 키를 얻습니다

ONTAP 필드	설명
액세스 키 및 비밀 암호	StorageGRID 테넌트 계정의 액세스 키 및 암호 액세스 키입니다. 이러한 값은 테넌트 관리자에서 생성합니다. S3 버킷을 생성하고 액세스 키를 얻습니다
SSL	활성화해야 합니다.
오브젝트 저장소 인증서	StorageGRID 로드 밸런서 끝점을 만들 때 업로드한 CA 인증서입니다. • 참고: * 중간 CA가 StorageGRID 인증서를 발급한 경우 중간 CA 인증서를 제공해야 합니다. StorageGRID 인증서가 루트 CA에서 직접 발급된 경우 루트 CA 인증서를 제공해야 합니다. FabricPool용 로드 밸런서 끝점을 만듭니다

작업을 마친 후

필요한 StorageGRID 정보를 얻은 후 ONTAP로 이동하여 StorageGRID를 클라우드 계층으로 추가하고, 클라우드 계층을 Aggregate로 추가한 다음 볼륨 계층화 정책을 설정할 수 있습니다.

로드 밸런싱에 대한 모범 사례

StorageGRID를 FabricPool 클라우드 계층으로 연결하기 전에 StorageGRID 그리드 관리자를 사용하여 하나 이상의 로드 밸런서 끝점을 구성해야 합니다.

로드 밸런싱이란 무엇입니까?

데이터가 FabricPool에서 StorageGRID 시스템으로 계층화되면 StorageGRID는 로드 밸런서를 사용하여 수집 및 검색 워크로드를 관리합니다. 로드 밸런싱은 여러 스토리지 노드에 FabricPool 워크로드를 분산하여 속도와 연결 용량을 극대화합니다.

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

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

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

> 게이트웨이 노드의 별도의 CLB(연결 로드 밸런서) 서비스는 더 이상 사용되지 않으며 FabricPool에서 더 이상 사용하지 않는 것이 좋습니다.

StorageGRID 로드 밸런싱에 대한 Best Practice

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

게이트웨이 노드 및 관리 노드가 수신 및 발신 FabricPool 요청에 사용할 포트를 정의하려면 StorageGRID 로드 밸런서 끝점을 구성해야 합니다.

로드 밸런서 끝점 인증서에 대한 Best Practice

FabricPool와 함께 사용할 로드 밸런서 끝점을 만들 때는 HTTPS를 프로토콜로 사용해야 합니다. TLS 암호화 없이 StorageGRID와 통신하는 것은 지원되지만 권장되지 않습니다

그런 다음 공개적으로 신뢰할 수 있는 인증서나 개인 인증 기관(CA)에서 서명한 인증서를 업로드하거나 자체 서명된 인증서를 생성할 수 있습니다. 이 인증서를 통해 ONTAP는 StorageGRID를 사용하여 인증할 수 있습니다.

가장 좋은 방법은 CA 서버 인증서를 사용하여 연결을 보호하는 것입니다. CA에서 서명한 인증서는 중단 없이 회전할 수 있습니다.

로드 밸런서 끝점에서 사용할 CA 인증서를 요청할 때는 인증서의 도메인 이름이 해당 로드 밸런서 끝점에 대해 ONTAP에 입력한 서버 이름과 일치하는지 확인합니다. 가능한 경우 와일드카드(*)를 사용하여 가상 호스트 스타일 URL을 허용합니다. 예를 들면 다음과 같습니다.

```
*.s3.storagegrid.company.com
```

StorageGRID를 FabricPool 클라우드 계층으로 추가하는 경우 루트 및 하위 CA(인증 기관) 인증서뿐만 아니라 ONTAP 클러스터에 동일한 인증서를 설치해야 합니다.

> StorageGRID는 여러 가지 목적으로 서버 인증서를 사용합니다. 로드 밸런서 서비스에 연결하는 경우 S3 및 Swift API 인증서를 선택적으로 사용할 수 있습니다.

로드 밸런싱 끝점의 서버 인증서에 대한 자세한 내용은 다음을 참조하십시오.

- 로드 밸런서 엔드포인트를 구성합니다
- 서버 인증서에 대한 강화 지침

고가용성 그룹에 대한 Best Practice

StorageGRID를 FabricPool 클라우드 계층으로 연결하기 전에 StorageGRID 그리드 관리자를 사용하여 고가용성(HA) 그룹을 구성해야 합니다.

고가용성(HA) 그룹이란 무엇입니까?

로드 밸런서 서비스를 항상 사용하여 FabricPool 데이터를 관리할 수 있도록 여러 관리 및 게이트웨이 노드의 네트워크 인터페이스를 고가용성(HA) 그룹이라고 하는 단일 엔터티로 그룹화할 수 있습니다. HA 그룹의 액티브 노드에 장애가 발생할 경우 그룹의 다른 노드가 워크로드를 계속 관리할 수 있습니다.

각 HA 그룹은 연결된 노드의 공유 서비스에 대한 고가용성 액세스를 제공합니다. 예를 들어, 게이트웨이 노드에만

있거나 관리 노드와 게이트웨이 노드 모두에 있는 인터페이스로 구성된 HA 그룹은 공유 로드 밸런서 서비스에 대한 고가용성 액세스를 제공합니다.

HA 그룹을 생성하려면 다음 일반 단계를 수행합니다.

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

> VLAN 인터페이스를 사용하여 FabricPool 트래픽을 분리하려는 경우 네트워크 관리자는 먼저 트렁크 인터페이스와 해당 VLAN을 구성해야 합니다. 각 VLAN은 숫자 ID 또는 태그로 식별됩니다. 예를 들어 네트워크에서 FabricPool 트래픽에 VLAN 100을 사용할 수 있습니다.

2. 그룹에 하나 이상의 가상 IP(VIP) 주소를 할당합니다. FabricPool와 같은 클라이언트 응용 프로그램은 이러한 VIP 주소를 사용하여 StorageGRID에 연결할 수 있습니다.
3. 기본 인터페이스로 사용할 인터페이스를 지정하고 백업 인터페이스의 우선 순위를 결정합니다. Primary 인터페이스는 장애가 발생하지 않는 한 Active 인터페이스입니다.

HA 그룹에 둘 이상의 인터페이스가 포함되어 있고 기본 인터페이스에 장애가 발생하면 VIP 주소가 우선 순위 순서대로 첫 번째 백업 인터페이스로 이동합니다. 이 인터페이스에 장애가 발생하면 VIP 주소가 다음 백업 인터페이스로 이동합니다. 이 장애 조치 프로세스는 일반적으로 몇 초 밖에 걸리지 않으며 클라이언트 응용 프로그램에 거의 영향을 주지 않고 정상적인 재시도 동작에 의존하여 작업을 계속할 수 있을 정도로 빠릅니다.

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

고가용성(**HA**) 그룹에 대한 모범 사례

FabricPool용 StorageGRID HA 그룹을 생성하는 모범 사례는 다음과 같이 워크로드에 따라 다릅니다.

- 운영 워크로드 데이터에 FabricPool를 사용할 계획이라면 데이터 검색이 중단되지 않도록 최소 2개의 로드 밸런싱 노드를 포함하는 HA 그룹을 생성해야 합니다.
- FabricPool 스냅샷 전용 볼륨 계층화 정책 또는 비 운영 로컬 성능 계층(예: 재해 복구 위치 또는 NetApp SnapMirror ® 대상)을 사용하려는 경우 하나의 노드만 사용하여 HA 그룹을 구성할 수 있습니다.

다음 지침은 Active-Backup HA에 대한 HA 그룹 설정(한 노드는 활성 상태이고 한 노드는 백업)에 대해 설명합니다. 그러나 DNS 라운드 로빈 또는 Active-Active HA를 사용하는 것이 좋습니다. 이러한 기타 HA 구성의 이점에 대한 자세한 내용은 를 참조하십시오 HA 그룹에 대한 구성 옵션.

StorageGRID IP 주소에 대해 **DNS** 서버를 구성합니다

고가용성 그룹 및 로드 밸런서 끝점을 구성한 후에는 ONTAP 시스템의 DNS(도메인 이름 시스템)에 StorageGRID 서버 이름(정규화된 도메인 이름)을 FabricPool가 연결에 사용할 IP 주소에 연결하는 레코드가 포함되어 있는지 확인해야 합니다.

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

- HA 그룹을 구성한 경우 FabricPool는 해당 HA 그룹의 가상 IP 주소에 연결됩니다.
- HA 그룹을 사용하지 않는 경우 FabricPool는 게이트웨이 노드 또는 관리 노드의 IP 주소를 사용하여 StorageGRID 로드 밸런서 서비스에 연결할 수 있습니다.

또한 DNS 레코드가 와일드카드 이름을 포함하여 필요한 모든 끝점 도메인 이름을 참조하는지 확인해야 합니다.

FabricPool에 대한 고가용성**(HA)** 그룹을 생성합니다

FabricPool와 함께 사용하도록 StorageGRID를 구성할 때 HA(고가용성) 그룹을 하나 이상 선택적으로 생성할 수 있습니다. HA 그룹은 관리 노드, 게이트웨이 노드 또는 둘 다에서 하나 이상의 네트워크 인터페이스로 구성됩니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.
- VLAN을 사용하려는 경우 VLAN 인터페이스를 만들었습니다. 을 참조하십시오 VLAN 인터페이스를 구성합니다.

이 작업에 대해

각 HA 그룹은 가상 IP 주소(VIP)를 사용하여 연결된 노드의 공유 서비스에 대한 고가용성 액세스를 제공합니다.

이 작업에 대한 자세한 내용은 을 참조하십시오 고가용성 그룹을 관리합니다.

단계

1. 구성 * > * 네트워크 * > * 고가용성 그룹 * 을 선택합니다.
2. Create * 를 선택합니다.
3. 고유한 이름과 설명을 입력합니다(선택 사항).
4. 이 HA 그룹에 추가할 인터페이스를 하나 이상 선택하십시오.

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

5. 이 HA 그룹에 대한 기본 인터페이스 및 백업 인터페이스를 확인합니다.

   행을 끌어 놓아서 * Priority order * 열의 값을 변경합니다.

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

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

6. CIDR 표기법 &#8212로 VIP 서브넷을 지정합니다. IPv4 주소 뒤에 슬래시와 서브넷 길이(0-32)를 입력합니다.

   네트워크 주소에는 호스트 비트가 설정되어 있지 않아야 합니다. 예를 들어, '192.16.0.0/22'가 있습니다.

7. 선택적으로, StorageGRID 액세스에 사용되는 ONTAP IP 주소가 StorageGRID VIP 주소와 동일한 서브넷에 없는 경우 StorageGRID VIP 로컬 게이트웨이 IP 주소를 입력합니다. 로컬 게이트웨이 IP 주소는 VIP 서브넷 내에 있어야 합니다.
8. HA 그룹에 대한 가상 IP 주소를 하나 이상 입력합니다. 최대 10개의 IP 주소를 추가할 수 있습니다. 모든 VIP는 VIP 서브넷 내에 있어야 합니다.

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

9. Create HA group * 을 선택한 다음 * Finish * 를 선택합니다.

FabricPool용 로드 밸런서 끝점을 만듭니다

FabricPool와 함께 사용하도록 StorageGRID를 구성할 때는 로드 밸런서 끝점을 구성하고 로드 밸런서 끝점 인증서를 업로드해야 합니다. 이 인증서는 ONTAP와 StorageGRID 간의 연결을 보호하는 데 사용됩니다.

필요한 것

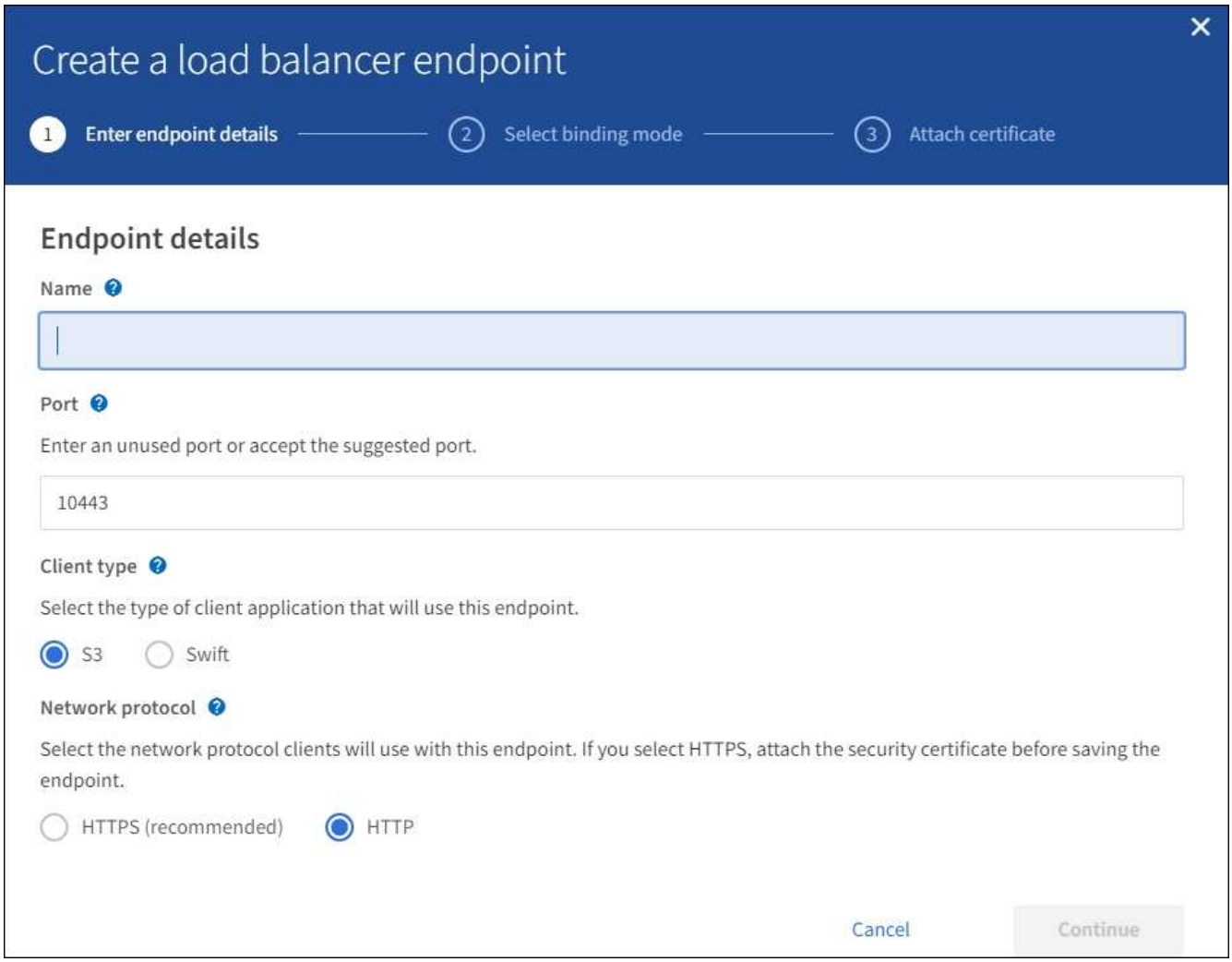
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.
- 다음 파일이 있습니다.
  - 서버 인증서: 사용자 지정 서버 인증서 파일입니다.
  - 서버 인증서 개인 키: 사용자 지정 서버 인증서 개인 키 파일입니다.
  - CA 번들: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 선택적 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.

이 작업에 대해

이 작업에 대한 자세한 내용은 을 참조하십시오 로드 밸런서 엔드포인트를 구성합니다.

단계

1. 구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 * 를 선택합니다.
2. Create * 를 선택합니다.



3. 끝점 세부 정보를 입력합니다.

필드에 입력합니다	설명
이름	끝점에 대한 설명 이름입니다
포트	로드 밸런싱에 사용할 StorageGRID 포트입니다. 이 필드의 기본값은 10433이지만 사용하지 않는 외부 포트는 입력할 수 있습니다. 80 또는 443을 입력하면 엔드포인트는 게이트웨이 노드에서만 구성됩니다. 이러한 포트는 관리 노드에 예약되기 때문입니다. • 참고: * 다른 그리드 서비스에서 사용하는 포트는 허용되지 않습니다. 를 참조하십시오네트워크 포트 참조. StorageGRID를 FabricPool 클라우드 계층으로 연결할 때 ONTAP에 동일한 포트 번호를 제공해야 합니다.
클라이언트 유형입니다	S3 * 를 선택합니다.

필드에 입력합니다	설명
네트워크 프로토콜	HTTPS * 를 선택합니다. • 참고 *: * HTTP * 사용은 지원되지만 권장되지 않습니다.

4. Continue * 를 선택합니다.
5. 바인딩 모드를 지정합니다.

   글로벌 * 설정(권장)을 사용하거나 이 끝점의 접근성을 다음 중 하나로 제한합니다.

   - 특정 노드의 특정 네트워크 인터페이스
   - 특정 HA(고가용성) 가상 IP 주소(VIP) 워크로드를 훨씬 더 높은 수준으로 격리해야 하는 경우에만 이 옵션을 사용하십시오.
6. Continue * 를 선택합니다.
7. 인증서 업로드 * (권장)를 선택한 다음 서버 인증서, 인증서 개인 키 및 선택적 CA 번들로 이동합니다.
8. Create * 를 선택합니다.

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

FabricPool에 대한 테넌트 계정을 생성합니다

FabricPool용 그리드 관리자에서 테넌트 계정을 만들어야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

테넌트 계정을 사용하면 클라이언트 애플리케이션이 StorageGRID에 객체를 저장하고 검색할 수 있습니다. 각 테넌트 계정에는 고유한 계정 ID, 인증된 그룹 및 사용자, 버킷 및 객체가 있습니다.

여러 ONTAP 클러스터에 동일한 테넌트 계정을 사용할 수 있습니다. 또는 필요에 따라 각 ONTAP 클러스터에 대한 전용 테넌트 계정을 생성할 수 있습니다.

> 이 지침에서는 Grid Manager에 대해 SSO(Single Sign-On)를 구성했다고 가정합니다. SSO가 활성화되지 않은 경우 를 사용합니다 테넌트 계정을 생성하기 위한 지침입니다 대신

단계

1. Tenants * 를 선택합니다.
2. Create * 를 선택합니다.
3. 표시 이름과 설명을 입력합니다.
4. S3 * 를 선택합니다.
5. 스토리지 할당량 * 필드는 비워 둡니다.

6. 플랫폼 서비스 사용을 활성화하려면 * 플랫폼 서비스 허용 * 을 선택합니다.

   플랫폼 서비스가 설정된 경우 테넌트는 외부 서비스에 액세스하는 CloudMirror 복제와 같은 기능을 사용할 수 있습니다.

7. 자체 ID 소스 사용 * 을 선택하지 마십시오.
8. S3 선택 허용 * 을 선택하지 마십시오.
9. 테넌트에 대한 초기 루트 액세스 권한을 가지려면 그리드 관리자에서 기존 통합 그룹을 선택합니다.
10. 테넌트 생성 * 을 선택합니다.

S3 버킷을 생성하고 액세스 키를 얻습니다

FabricPool 워크로드에 StorageGRID를 사용하기 전에 FabricPool 데이터용 S3 버킷을 생성해야 합니다. 또한 FabricPool에 사용할 테넌트 계정에 대한 액세스 키와 비밀 액세스 키를 얻어야 합니다.

필요한 것

- FabricPool 사용을 위해 테넌트 계정을 만들었습니다.

이 작업에 대해

다음 지침은 StorageGRID 테넌트 관리자를 사용하여 버킷을 생성하고 액세스 키를 얻는 방법을 설명합니다. 테넌트 관리 API 또는 StorageGRID S3 REST API를 사용하여 이러한 작업을 수행할 수도 있습니다. 또는 ONTAP 9.10을 사용하는 경우 대신 FabricPool 설정 마법사를 사용하여 버킷을 생성할 수 있습니다.

자세한 내용:

- 테넌트 계정을 사용합니다
- S3을 사용합니다

단계

1. 테넌트 관리자에 로그인합니다.

   다음 중 하나를 수행할 수 있습니다.

   - Grid Manager의 Tenant Accounts 페이지에서 테넌트의 * Sign In * 링크를 선택하고 자격 증명을 입력합니다.
   - 웹 브라우저에 테넌트 계정의 URL을 입력하고 자격 증명을 입력합니다.

2. FabricPool 데이터용 S3 버킷을 생성합니다.

   사용하려는 각 ONTAP 클러스터에 대해 고유한 버킷을 생성해야 합니다.

   a. 스토리지(S3) * > * 버킷 * 을 선택합니다.
   b. Create bucket * 을 선택합니다.
   c. FabricPool와 함께 사용할 StorageGRID 버킷의 이름을 입력합니다. 예를 들어, '배합통'을 예로 들 수 있습니다.

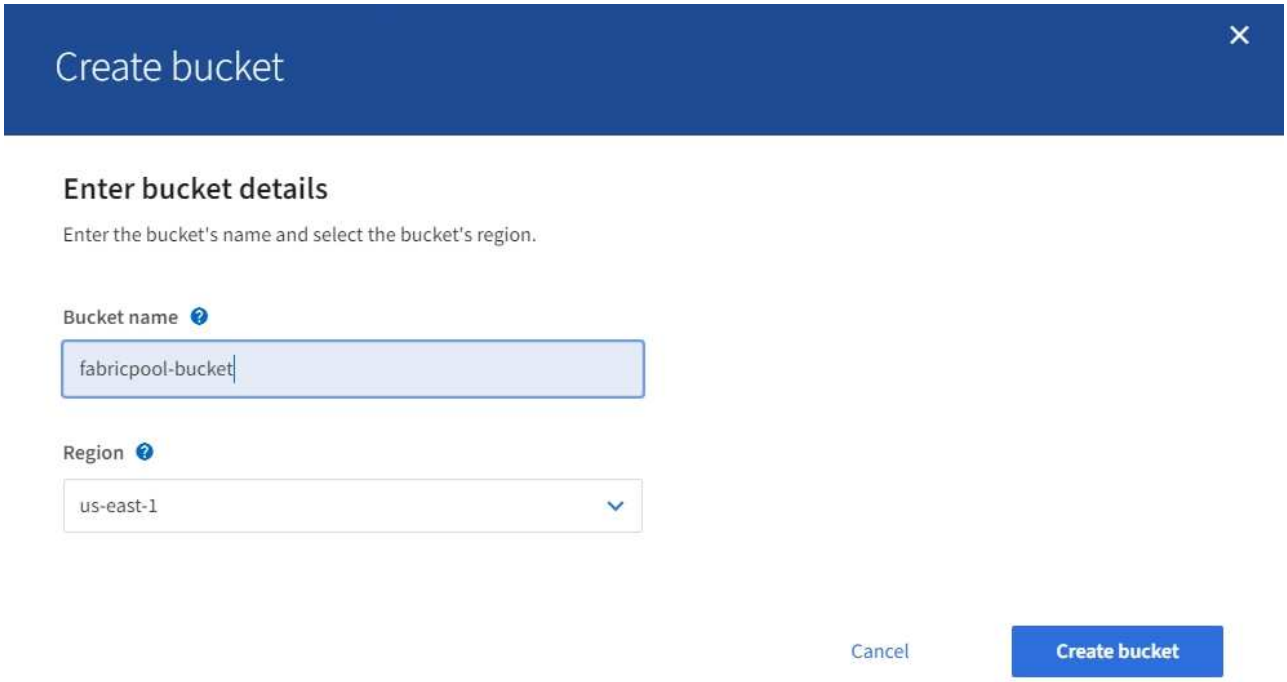
      ⓘ 버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

버킷 이름은 다음 규칙을 준수해야 합니다.

- 각 StorageGRID 시스템에서 고유해야 합니다(테넌트 계정에서만 고유한 것은 아님).
- DNS를 준수해야 합니다.
- 3자 이상 63자 이하여야 합니다.
- 인접한 레이블이 마침표로 구분된 하나 이상의 레이블일 수 있습니다. 각 레이블은 소문자 또는 숫자로 시작하고 끝나야 하며 소문자, 숫자 및 하이픈만 사용할 수 있습니다.
- 텍스트 형식의 IP 주소처럼 보이지 않아야 합니다.
- 가상 호스팅 스타일 요청에서 기간을 사용하지 않아야 합니다. 마침표는 서버 와일드카드 인증서 확인에 문제를 일으킬 수 있습니다.

d. 이 버킷의 영역을 선택합니다.

기본적으로 모든 버킷은 us-east-1 영역에 생성됩니다.



e. Create bucket * 을 선택합니다.

> FabricPool 버킷의 경우 권장되는 버킷 정합성 수준은 새 버킷의 기본 설정인 * 읽기 후 새 쓰기 * 입니다. 사용 가능 * 또는 기타 정합성 보장 레벨을 사용하기 위해 FabricPool 버킷을 편집하지 마십시오.

3. 액세스 키와 비밀 액세스 키를 생성합니다.

a. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.

b. Create key * 를 선택합니다.

c. Create access key * 를 선택합니다.

d. 액세스 키 ID와 비밀 액세스 키를 안전한 위치에 복사하거나 * Download.csv * 를 선택하여 액세스 키 ID와 비밀 액세스 키가 포함된 스프레드시트 파일을 저장합니다.

StorageGRID를 FabricPool 클라우드 계층으로 구성할 때 ONTAP에 이러한 값을 입력합니다.

> 나중에 새 액세스 키와 비밀 액세스 키를 생성하는 경우 ONTAP가 중단 없이 StorageGRID에 데이터를 저장하고 검색할 수 있도록 ONTAP에서 해당 값을 즉시 업데이트해야 합니다.

FabricPool 데이터에 StorageGRID 정보 수명 주기 관리 사용

FabricPool를 사용하여 데이터를 StorageGRID에 계층화하려는 경우 StorageGRID ILM(정보 수명 주기 관리) 규칙을 생성하기 위한 요구사항과 FabricPool 데이터를 관리하기 위한 ILM 정책을 이해해야 합니다. FabricPool 데이터에 적용되는 ILM 규칙이 중단되지 않도록 해야 합니다.

> FabricPool에는 StorageGRID ILM 규칙 또는 정책에 대한 지식이 없습니다. StorageGRID ILM 정책이 잘못 구성된 경우 데이터 손실이 발생할 수 있습니다. 을 참조하십시오 ILM을 사용하여 개체를 관리합니다 자세한 ILM 지침을 참조하십시오.

ILM 규칙 및 ILM 정책이 FabricPool 데이터 및 비즈니스 요구 사항에 적합한지 확인하려면 다음 지침을 검토하십시오. StorageGRID ILM을 이미 사용 중인 경우 이러한 지침을 충족하기 위해 활성 ILM 정책을 업데이트해야 할 수 있습니다.

- 복제 및 삭제 코딩 규칙을 조합하여 클라우드 계층 데이터를 보호할 수 있습니다.

  가장 권장되는 모범 사례는 비용 효율적인 데이터 보호를 위해 사이트 내에서 2+1 삭제 코딩을 사용하는 것입니다. 삭제 코딩은 더 많은 CPU를 사용하지만 복제에 비해 스토리지 용량이 훨씬 적습니다. 4+1 및 6+1 구성표는 2+1 구성표보다 적은 용량을 사용합니다. 그러나 그리드 확장 중에 스토리지 노드를 추가해야 하는 경우 4+1 및 6+1 구성표는 유연하지 않습니다. 자세한 내용은 을 참조하십시오 삭제 코딩 오브젝트를 위한 스토리지 용량을 추가합니다.

- FabricPool 데이터에 적용되는 각 규칙은 삭제 코딩을 사용하거나 적어도 두 개의 복제된 복사본을 만들어야 합니다.

  > 특정 기간 동안 복제된 복사본을 하나만 생성하는 ILM 규칙은 데이터가 영구적으로 손실될 위험이 있습니다. 복제된 객체 복제본이 하나만 있는 경우 스토리지 노드에 장애가 발생하거나 심각한 오류가 발생한 경우 해당 객체가 손실됩니다. 또한 업그레이드와 같은 유지보수 절차 중에는 개체에 대한 액세스가 일시적으로 중단됩니다.

- FabricPool 클라우드 계층 데이터가 만료되거나 삭제될 ILM 규칙을 사용하지 마십시오. 각 ILM 규칙의 보존 기간을 "Forever"로 설정하여 StorageGRID ILM에서 FabricPool 개체가 삭제되지 않도록 합니다.
- FabricPool 클라우드 계층 데이터를 버킷에서 다른 위치로 이동할 규칙을 만들지 마십시오. ILM 규칙을 사용하여 아카이브 노드를 사용하여 FabricPool 데이터를 테이프에 아카이빙하거나 클라우드 스토리지 풀을 사용하여 FabricPool 데이터를 다른 오브젝트 저장소로 이동할 수 없습니다.

  > FabricPool에서 클라우드 스토리지 풀 타겟의 객체를 검색하는 지연 시간이 추가되었기 때문에 클라우드 스토리지 풀을 사용할 수 없습니다.

- ONTAP 9.8부터 객체 태그를 생성하여 계층형 데이터를 쉽게 분류하고 정렬할 수 있습니다. 예를 들어, StorageGRID에 연결된 FabricPool 볼륨에만 태그를 설정할 수 있습니다. 그런 다음 StorageGRID에서 ILM 규칙을 만들 때 개체 태그 고급 필터를 사용하여 이 데이터를 선택하고 배치할 수 있습니다.

FabricPool 데이터에 대한 **ILM** 정책의 예

이 간단한 예제 정책을 자신의 ILM 규칙 및 정책의 시작 지점으로 사용합니다.

이 예제에서는 콜로라도주 덴버의 단일 데이터 센터에 4개의 스토리지 노드가 있는 StorageGRID 시스템에 대한 ILM 규칙 및 ILM 정책을 디자인한다고 가정합니다. 이 예의 FabricPool 데이터는 '배풀버킷'이라는 이름의 버킷을 사용합니다.

> 다음 ILM 규칙 및 정책은 예일 뿐입니다. ILM 규칙을 구성하는 방법은 여러 가지가 있습니다. 새 정책을 활성화하기 전에 제안된 정책을 시뮬레이션하여 콘텐츠가 손실로부터 보호되도록 의도한 대로 동작하는지 확인합니다. 자세한 내용은 을 참조하십시오 ILM을 사용하여 개체를 관리합니다.

단계

1. 이름이 * den * 인 스토리지 풀을 생성합니다. 덴버 사이트를 선택합니다.
2. 이름이 * 2와 1 * 인 삭제 코딩 프로필을 만듭니다. 2+1 삭제 코딩 체계와 * den * 스토리지 풀을 선택합니다.
3. 'fabricpool-bucket'의 데이터에만 적용되는 ILM 규칙을 생성합니다. 이 예제 규칙은 삭제 코딩 복사본을 만듭니다.

규칙 정의	예제 값
규칙 이름	FabricPool 데이터에 2개 이상의 삭제 코딩
버킷 이름	배합통 FabricPool 테넌트 계정에서도 필터링할 수 있습니다.
고급 필터링	객체 크기(MB)가 0.2 MB를 초과합니다. • 참고: * FabricPool는 4MB 객체만 쓰지만 이 규칙은 삭제 코딩을 사용하므로 객체 크기 필터를 추가해야 합니다.
참조 시간	수집 시간
배치	0일째부터 영원히
유형	삭제 코딩
위치	DEN(2 + 1)
수집 동작	균형

4. 첫 번째 규칙과 일치하지 않는 개체의 복제된 복사본 2개를 생성하는 ILM 규칙을 생성합니다. 기본 필터(테넌트 계정 또는 버킷 이름) 또는 고급 필터를 선택하지 마십시오.

규칙 정의	예제 값
규칙 이름	2개의 복제 복사본

규칙 정의	예제 값
버킷 이름	없음
고급 필터링	없음
참조 시간	수집 시간
배치	0일째부터 영원히
유형	복제됨
위치	수
사본	2
수집 동작	균형

5. 제안된 ILM 정책을 생성하고 두 규칙을 선택합니다. 복제 규칙에서는 필터를 사용하지 않으므로 정책의 기본(마지막) 규칙일 수 있습니다.
6. 테스트 오브젝트를 그리드에 수집.
7. 테스트 개체를 사용하여 정책을 시뮬레이션하여 동작을 확인합니다.
8. 정책을 활성화합니다.

이 정책이 활성화되면 StorageGRID는 다음과 같이 오브젝트 데이터를 배치합니다.

- 'fabricpool-bucket'의 FabricPool에서 계층화한 데이터는 2+1 삭제 코딩 방식을 사용하여 삭제 코딩됩니다. 데이터 조각 2개와 패리티 조각 1개가 서로 다른 스토리지 노드 3개에 배치됩니다.
- 다른 모든 버킷의 모든 객체가 복제됩니다. 두 개의 복제본이 생성되고 두 개의 서로 다른 스토리지 노드에 배치됩니다.
- 삭제 코딩 및 복제된 복사본은 S3 클라이언트에서 삭제할 때까지 StorageGRID에서 유지됩니다. StorageGRID ILM은 이러한 항목을 삭제하지 않습니다.

FabricPool에 대한 트래픽 분류 정책을 생성합니다

FabricPool 워크로드에 대한 서비스 품질을 최적화하기 위해 StorageGRID 트래픽 분류 정책을 선택적으로 설계할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.

이 작업에 대해

FabricPool에 대한 트래픽 분류 정책을 생성하는 모범 사례는 다음과 같이 워크로드에 따라 달라집니다.

- FabricPool 운영 워크로드 데이터를 StorageGRID에 계층화하려는 경우 FabricPool 워크로드의 대역폭 대부분은 확인해야 합니다. 트래픽 분류 정책을 생성하여 다른 모든 워크로드를 제한할 수 있습니다.

  > 일반적으로 FabricPool 읽기 작업은 쓰기 작업보다 우선 순위를 지정하는 것이 더 중요합니다.

  예를 들어, 다른 S3 클라이언트가 이 StorageGRID 시스템을 사용하는 경우 트래픽 분류 정책을 생성해야 합니다. 다른 버킷, 테넌트, IP 서브넷 또는 로드 밸런서 끝점에 대한 네트워크 트래픽을 제한할 수 있습니다.

- 일반적으로 FabricPool 워크로드에 대해 서비스 품질 제한을 적용하지 마십시오. 다른 워크로드만 제한하면 됩니다.
- 다른 워크로드에 대한 제한에는 이러한 워크로드의 동작이 고려되어야 합니다. 또한 그리드 크기 조정 및 기능과 예상되는 활용률에 따라 제한이 달라집니다.

자세한 내용: 트래픽 분류 정책을 관리합니다

단계

1. 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택합니다.
2. 이름과 설명을 입력합니다.
3. 일치 규칙 섹션에서 하나 이상의 규칙을 만듭니다.
   a. Create * 를 선택합니다.
   b. 끝점 * 을 선택하고 FabricPool에 대해 만든 로드 밸런서 끝점을 선택합니다.

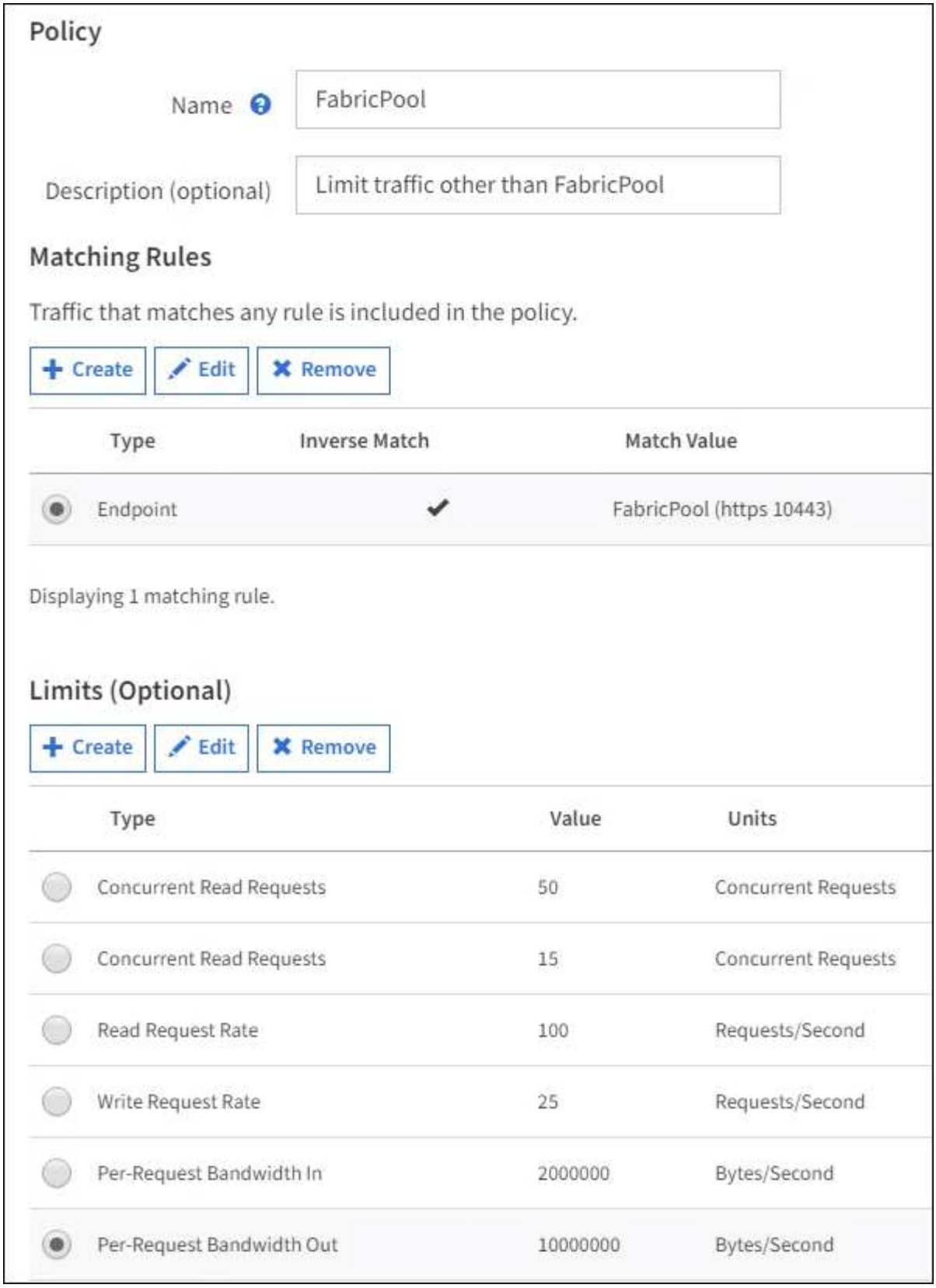
      FabricPool 테넌트 계정 또는 버킷을 선택할 수도 있습니다.

   c. 이 트래픽 정책이 다른 끝점의 트래픽을 제한하도록 하려면 * 역일치 * 를 선택합니다.
4. 필요에 따라 하나 이상의 제한을 만듭니다.

   > 트래픽 분류 정책에 대한 제한이 설정되어 있지 않더라도 트래픽 추세를 파악할 수 있도록 메트릭이 수집됩니다.

   a. Create * 를 선택합니다.
   b. 제한할 트래픽 유형과 적용할 제한을 선택합니다.

      이 예제 FabricPool 트래픽 분류 정책은 제한할 수 있는 네트워크 트래픽의 유형과 선택할 수 있는 값의 유형을 보여 줍니다. 실제 정책의 한도는 특정 요구사항에 따라 다릅니다.



5. 트래픽 분류 정책을 생성한 후 정책을 선택하고 * Metrics * 를 선택하여 정책이 트래픽을 예상대로 제한하고 있는지 확인합니다.

기타 **StorageGRID** 및 **FabricPool** 모범 사례

FabricPool와 함께 사용하도록 StorageGRID 시스템을 구성할 때는 데이터 저장 방식에 영향을 줄 수 있는 전역 옵션을 설정하지 않아야 합니다.

오브젝트 암호화

StorageGRID를 구성할 때 다른 StorageGRID 클라이언트에 데이터 암호화가 필요한 경우 선택적으로 글로벌 * 저장된 개체 암호화 * 설정을 활성화할 수 있습니다(* 구성 * > * 시스템 * > * 그리드 옵션 *). FabricPool에서 StorageGRID로 계층화된 데이터는 이미 암호화되므로 StorageGRID 설정을 활성화할 필요가 없습니다. 클라이언트측 암호화 키는 ONTAP의 소유입니다.

오브젝트 압축

StorageGRID를 구성할 때 전역 * 저장된 개체 압축 * 설정을 사용하지 마십시오(* 구성 * > * 시스템 * > * 그리드 옵션 *). FabricPool에서 StorageGRID로 계층화된 데이터는 이미 압축된 상태입니다. 저장된 개체 압축 * 을 사용하면 개체의 크기가 더 작아지지 않습니다.

정합성 보장 레벨

FabricPool 버킷의 경우 권장되는 버킷 정합성 수준은 새 버킷의 기본 설정인 * 읽기 후 새 쓰기 * 입니다. 사용 가능 * 또는 기타 정합성 보장 레벨을 사용하기 위해 FabricPool 버킷을 편집하지 마십시오.

FabricPool 계층화

StorageGRID 노드에서 NetApp ONTAP 시스템에서 할당된 스토리지를 사용하는 경우 볼륨에 FabricPool 계층화 정책이 활성화되어 있지 않은지 확인합니다. 예를 들어 StorageGRID 노드가 VMware 호스트에서 실행 중인 경우 StorageGRID 노드의 데이터 저장소를 백업하는 볼륨에 FabricPool 계층화 정책이 설정되어 있지 않은지 확인합니다. StorageGRID 노드와 함께 사용되는 볼륨에 대해 FabricPool 계층화를 사용하지 않도록 설정하면 문제 해결과 스토리지 작업이 간소화됩니다.

> FabricPool를 사용하여 StorageGRID 관련 데이터를 StorageGRID 자체로 계층화하지 마십시오. StorageGRID 데이터를 StorageGRID로 다시 계층화하면 문제 해결과 운영 복잡성이 늘어납니다.

StorageGRID를 사용합니다

테넌트 계정을 사용합니다

테넌트 계정 사용: 개요

테넌트 계정을 사용하면 S3(Simple Storage Service) REST API 또는 Swift REST API를 사용하여 StorageGRID 시스템에 오브젝트를 저장하고 검색할 수 있습니다.

테넌트 계정이란 무엇입니까?

각 테넌트 계정에는 자체 통합 또는 로컬 그룹, 사용자, S3 버킷 또는 Swift 컨테이너 및 객체가 있습니다.

필요한 경우 테넌트 계정을 사용하여 저장된 객체를 다른 엔터티로 분리할 수 있습니다. 예를 들어, 다음과 같은 사용 사례에서 여러 테넌트 계정을 사용할 수 있습니다.

- * 기업 활용 사례: * 기업 내에서 StorageGRID 시스템을 사용하는 경우 그리드의 객체 스토리지를 조직의 여러 부서에서 분리할 수 있습니다. 예를 들어 마케팅 부서, 고객 지원 부서, 인사 부서 등의 테넌트 계정이 있을 수 있습니다.

> S3 클라이언트 프로토콜을 사용하는 경우 S3 버킷 및 버킷 정책을 사용하여 엔터프라이즈의 부서 간에 오브젝트를 분리할 수도 있습니다. 별도의 테넌트 계정을 생성할 필요가 없습니다. 를 참조하십시오 S3 클라이언트 애플리케이션 구현 지침.

- * 서비스 공급자 사용 사례: * 서비스 공급자가 StorageGRID 시스템을 사용 중인 경우, 스토리지를 임대하는 다른 엔터티로 그리드의 개체 스토리지를 분리할 수 있습니다. 예를 들어 회사 A, 회사 B, 회사 C 등에 대한 테넌트 계정이 있을 수 있습니다.

테넌트 계정을 생성하는 방법

테넌트 계정은 에 의해 생성됩니다 그리드 관리자를 사용하는 StorageGRID 그리드 관리자. 테넌트 계정을 생성할 때 그리드 관리자는 다음 정보를 지정합니다.

- 테넌트의 표시 이름(테넌트의 계정 ID가 자동으로 할당되며 변경할 수 없음)
- 테넌트 계정에서 S3 또는 Swift를 사용할지 여부를 나타냅니다.
- S3 테넌트 계정의 경우: 테넌트 계정이 플랫폼 서비스를 사용하도록 허용되는지 여부 플랫폼 서비스를 사용할 수 있는 경우 그리드 사용을 지원하도록 구성해야 합니다.
- 필요한 경우 테넌트 계정의 스토리지 할당량 — 테넌트의 객체에 사용할 수 있는 최대 GB, 테라바이트 또는 PB입니다. 테넌트의 스토리지 할당량은 물리적 크기(디스크 크기)가 아닌 논리적 양(오브젝트 크기)을 나타냅니다.
- StorageGRID 시스템에 대해 ID 페더레이션이 설정된 경우 테넌트 계정을 구성할 수 있는 루트 액세스 권한이 있는 통합 그룹입니다.
- StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하지 않는 경우 테넌트 계정이 자체 ID 소스를 사용할지 또는 그리드의 ID 소스를 공유할지 여부 및 테넌트의 로컬 루트 사용자의 초기 암호를 공유할지 여부

또한, S3 테넌트 계정이 규정 요구 사항을 준수해야 하는 경우 그리드 관리자는 StorageGRID 시스템에 대해 S3 오브젝트 잠금 설정을 활성화할 수 있습니다. S3 오브젝트 잠금이 활성화된 경우 모든 S3 테넌트 계정에서 호환 버킷을 생성하고 관리할 수 있습니다.

S3 테넌트를 구성합니다

을(를) 마친 후 S3 테넌트 계정이 생성됩니다테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 통합을 설정하거나(ID 소스를 그리드와 공유하지 않는 경우) 로컬 그룹 및 사용자를 생성합니다
- S3 액세스 키 관리
- 규정 준수 버킷을 포함하여 S3 버킷 생성 및 관리
- 플랫폼 서비스 사용(활성화된 경우)
- 스토리지 사용량 모니터링

> 테넌트 관리자를 사용하여 S3 버킷을 생성 및 관리할 수 있지만 에는 가 있어야 합니다 S3 액세스 키를 사용하고 S3 REST API를 사용하여 오브젝트를 수집 및 관리합니다.

Swift 테넌트를 구성합니다

A 뒤에 Swift 테넌트 계정이 생성됩니다테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 통합을 설정하고(ID 소스를 그리드와 공유하지 않는 경우) 로컬 그룹 및 사용자를 만듭니다
- 스토리지 사용량 모니터링

> Swift 사용자는 테넌트 관리자에 액세스하려면 루트 액세스 권한이 있어야 합니다. 그러나 루트 액세스 권한에서는 사용자가 에 인증할 수 없습니다 Swift REST API 컨테이너 및 수집 개체 생성 사용자는 Swift REST API에 인증할 수 있는 Swift 관리자 권한이 있어야 합니다.

테넌트 관리자를 사용합니다

테넌트 관리자를 사용하면 StorageGRID 테넌트 계정의 모든 측면을 관리할 수 있습니다.

테넌트 관리자를 사용하여 테넌트 계정의 스토리지 사용량을 모니터링하고 ID 페더레이션을 통해 사용자를 관리하거나 로컬 그룹 및 사용자를 생성할 수 있습니다. S3 테넌트 계정의 경우 S3 키를 관리하고 S3 버킷을 관리하고 플랫폼 서비스를 구성할 수도 있습니다.

로그인 및 로그아웃 방법

테넌트 관리자에 로그인합니다

의 주소 표시줄에 테넌트에 대한 URL을 입력하여 테넌트 관리자에 액세스합니다 지원되는 웹 브라우저.

필요한 것

- 로그인 자격 증명이 있어야 합니다.
- 그리드 관리자가 제공한 대로 테넌트 관리자에 액세스하기 위한 URL이 있어야 합니다. URL은 다음 예 중 하나로 표시됩니다.

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

```
https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id
```

```
https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

URL은 항상 FQDN(정규화된 도메인 이름) 또는 관리 노드에 액세스하는 데 사용되는 IP 주소를 포함하며, 포트 번호, 20자리 테넌트 계정 ID 또는 둘 다를 선택적으로 포함할 수도 있습니다.

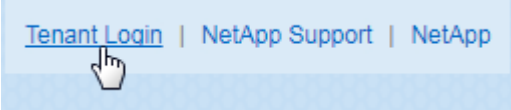
- URL에 테넌트의 20자리 계정 ID가 포함되지 않은 경우 이 계정 ID가 있어야 합니다.
- 을(를) 사용해야 합니다 지원되는 웹 브라우저.
- 웹 브라우저에서 쿠키를 활성화해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

단계

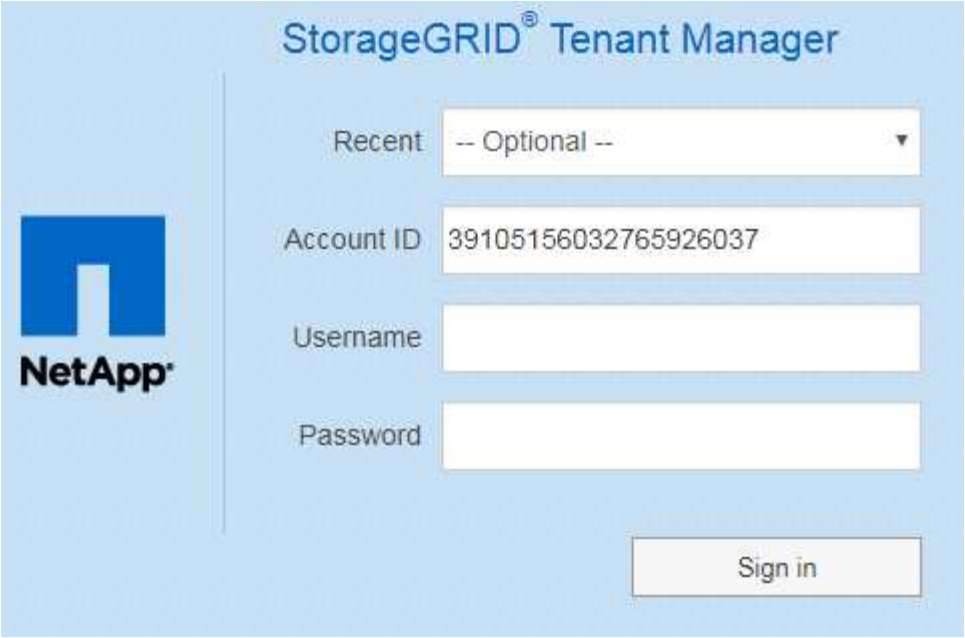
1. A를 시작합니다 지원되는 웹 브라우저.
2. 브라우저의 주소 표시줄에 Tenant Manager에 액세스하기 위한 URL을 입력합니다.
3. 보안 경고 메시지가 나타나면 브라우저의 설치 마법사를 사용하여 인증서를 설치합니다.
4. 테넌트 관리자에 로그인합니다.

   표시되는 로그인 화면은 입력한 URL과 조직에서 SSO(Single Sign-On)를 사용하고 있는지 여부에 따라 달라집니다. 다음 화면 중 하나가 표시됩니다.

   - Grid Manager 로그인 페이지 오른쪽 상단에서 * Tenant Login * 링크를 클릭합니다.

   - Tenant Manager 로그인 페이지. 아래와 같이 * Account ID * 필드가 이미 입력되어 있을 수 있습니다.



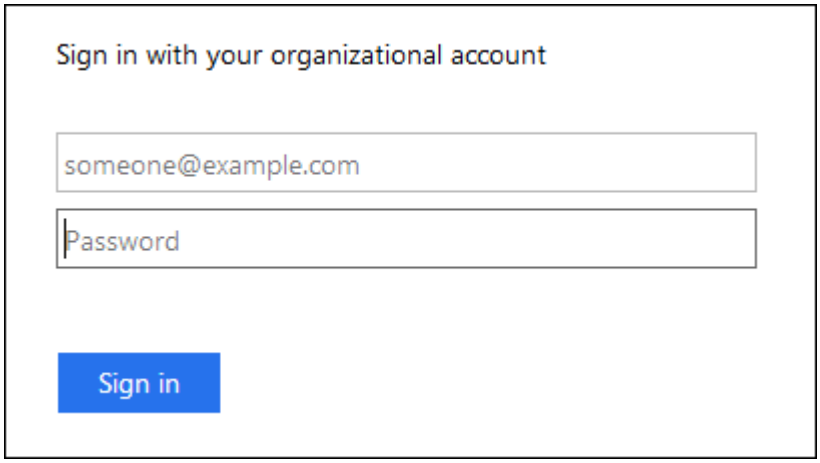
i. 테넌트의 20자리 계정 ID가 표시되지 않으면 최근 계정 목록에 테넌트 계정 이름이 나타날 경우 해당 계정 이름을 선택하거나 계정 ID를 입력합니다.

ii. 사용자 이름과 암호를 입력합니다.

iii. 로그인 * 을 클릭합니다.

Tenant Manager 대시보드가 나타납니다.

- SSO가 그리드에 활성화되어 있는 경우 조직의 SSO 페이지. 예를 들면 다음과 같습니다.



표준 SSO 자격 증명을 입력하고 * 로그인 * 을 클릭합니다.

- Tenant Manager SSO 로그인 페이지.

i. 테넌트의 20자리 계정 ID가 표시되지 않으면 최근 계정 목록에 테넌트 계정 이름이 나타날 경우 해당 계정 이름을 선택하거나 계정 ID를 입력합니다.

ii. 로그인 * 을 클릭합니다.

iii. 조직의 SSO 로그인 페이지에서 표준 SSO 자격 증명을 사용하여 로그인합니다.

Tenant Manager 대시보드가 나타납니다.

5. 다른 사람으로부터 초기 암호를 받은 경우 암호를 변경하여 계정을 보호하십시오. 사용자 이름 _ * > * 암호 변경 * 을 선택합니다.

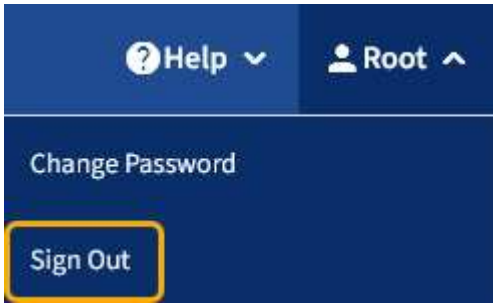
> StorageGRID 시스템에 SSO가 설정되어 있으면 테넌트 관리자에서 암호를 변경할 수 없습니다.

테넌트 관리자에서 로그아웃합니다

테넌트 관리자 작업을 마치면 로그아웃하여 권한이 없는 사용자가 StorageGRID 시스템에 액세스할 수 없도록 해야 합니다. 브라우저를 닫아도 브라우저 쿠키 설정에 따라 시스템에서 로그아웃되지 않을 수 있습니다.

단계

1. 사용자 인터페이스의 오른쪽 위 모서리에서 사용자 이름 드롭다운을 찾습니다.



2. 사용자 이름을 선택한 다음 * 로그아웃 * 을 선택합니다.

   - SSO가 사용되지 않는 경우:

     관리자 노드에서 로그아웃되었습니다. Tenant Manager 로그인 페이지가 표시됩니다.

> 두 개 이상의 관리 노드에 로그인한 경우 각 노드에서 로그아웃해야 합니다.

- SSO가 활성화된 경우:

  액세스 중인 모든 관리 노드에서 로그아웃되었습니다. StorageGRID 로그인 페이지가 표시됩니다. 방금 액세스한 테넌트 계정의 이름이 * 최근 계정 * 드롭다운에 기본값으로 나열되고 테넌트의 * 계정 ID * 가 표시됩니다.

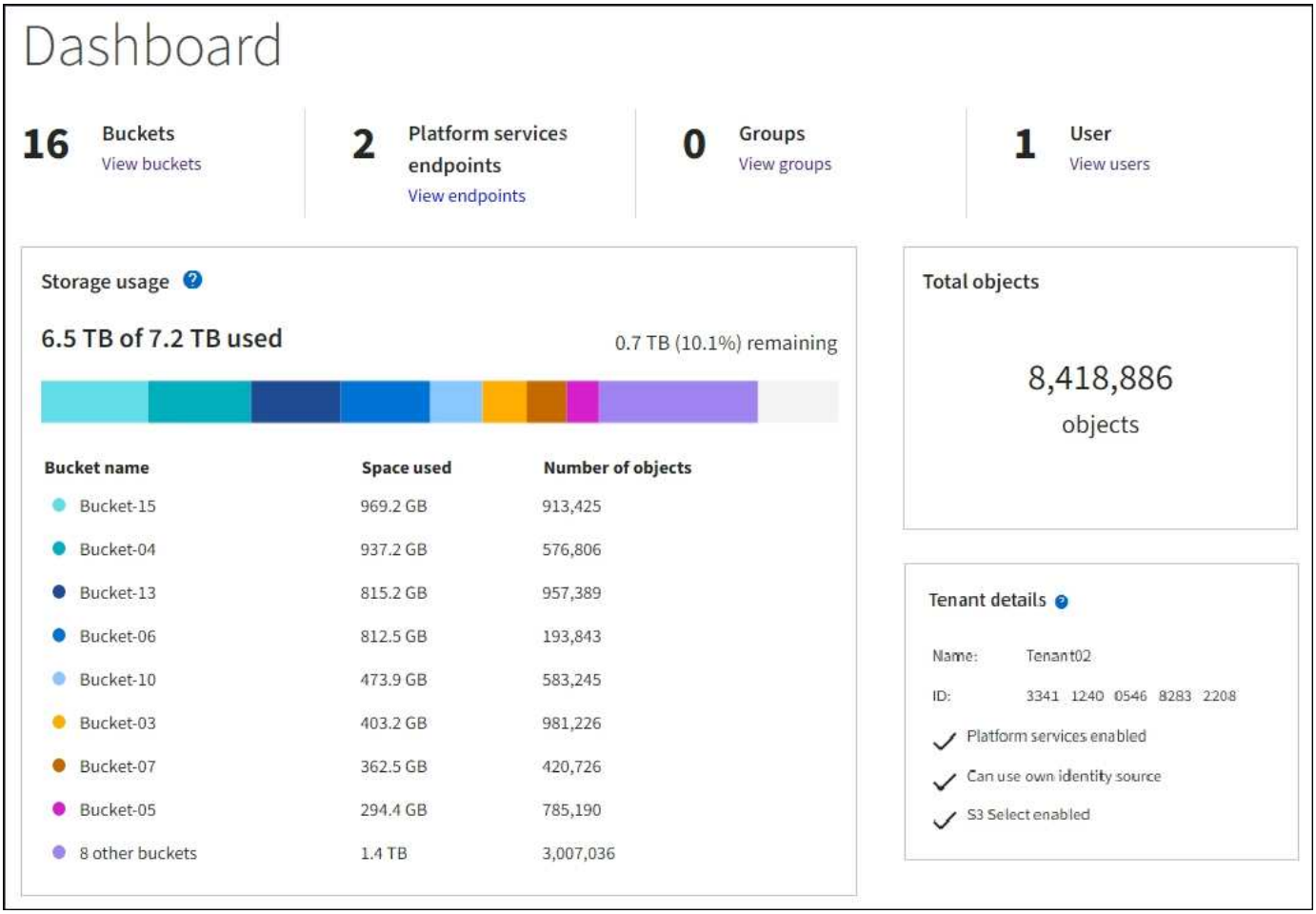
> SSO가 활성화되어 있고 Grid Manager에도 로그인한 경우, Grid Manager에서 로그아웃하여 SSO를 로그아웃해야 합니다.

테넌트 관리자 대시보드 이해

테넌트 관리자 대시보드에서는 테넌트 계정의 구성과 테넌트의 버킷(S3) 또는 컨테이너(Swift)에 있는 객체가 사용하는 공간의 양을 개괄적으로 보여 줍니다. 테넌트에 할당량이 있는 경우 대시보드에는 사용된 할당량의 양과 남아 있는 양이 표시됩니다. 테넌트 계정과 관련된 오류가 있는 경우 대시보드 에 오류가 표시됩니다.

> 사용된 공간 값은 추정값입니다. 이러한 추정치는 베스트 타이밍, 네트워크 연결 및 노드 상태의 영향을 받습니다.

객체가 업로드되면 대시보드는 다음 예제와 같습니다.



테넌트 계정 요약

대시보드 상단에는 다음 정보가 포함되어 있습니다.

- 구성된 버킷 또는 컨테이너, 그룹 및 사용자 수
- 구성된 플랫폼 서비스 엔드포인트의 수입니다

링크를 선택하여 세부 정보를 볼 수 있습니다.

대시보드의 오른쪽에는 다음과 같은 정보가 포함되어 있습니다.

- 테넌트의 총 객체 수입니다.

  S3 계정의 경우 오브젝트가 수집되지 않고 루트 액세스 권한이 있는 경우 총 오브젝트 수 대신 시작 지침이 나타납니다.

- 테넌트 계정 이름 및 ID와 테넌트가 사용할 수 있는지 여부를 포함한 테넌트 세부 정보입니다 플랫폼 서비스, 고유한 ID 소스입니다, 또는 S3 를 선택합니다 (설정된 권한만 나열됩니다).

스토리지 및 할당량 사용

Storage usage(저장소 사용) 패널에는 다음과 같은 정보가 포함되어 있습니다.

- 테넌트에 대한 객체 데이터의 양입니다.

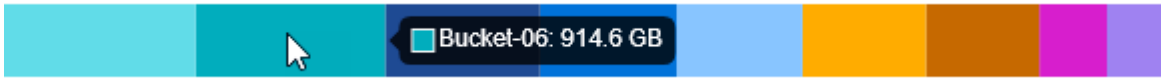
  > 이 값은 업로드된 총 오브젝트 데이터 양을 나타내며 해당 오브젝트 및 해당 메타데이터의 복사본을 저장하는 데 사용되는 공간을 나타내지 않습니다.

- 할당량이 설정된 경우 개체 데이터에 사용할 수 있는 총 공간과 남은 공간의 양과 백분율이 표시됩니다. 할당량은 섭취 가능한 오브젝트 데이터의 양을 제한합니다.

  > 할당량 활용도는 내부 추정치에 기반하며 경우에 따라 초과될 수 있습니다. 예를 들어, 테넌트가 객체를 업로드하기 시작할 때 StorageGRID는 할당량을 확인하고 테넌트가 할당량을 초과할 경우 새 베스트(ingest)를 거부합니다. 그러나 StorageGRID에서는 할당량이 초과되었는지 확인할 때 현재 업로드 크기를 고려하지 않습니다. 개체를 삭제하면 할당량 활용률이 다시 계산될 때까지 테넌트가 일시적으로 새 개체를 업로드하지 못할 수 있습니다. 할당량 사용률 계산에는 10분 이상이 소요될 수 있습니다.

- 가장 큰 버킷 또는 컨테이너의 상대적 크기를 나타내는 막대 차트.

  차트 세그먼트 위에 커서를 놓으면 해당 버킷이나 컨테이너에서 소비한 전체 공간을 볼 수 있습니다.



- 막대 도표에 대응하려면 총 오브젝트 데이터 양과 각 버킷 또는 컨테이너의 오브젝트 수를 포함하여 가장 큰 버킷 또는 컨테이너의 목록입니다.

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

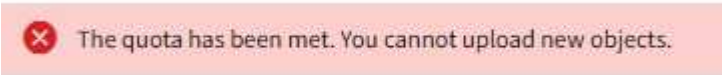
테넌트에 9개 이상의 버킷이나 컨테이너가 있는 경우 다른 모든 버킷이나 컨테이너는 목록 하단의 단일 항목으로 결합됩니다.

할당량 사용 알림을 표시합니다

그리드 관리자에서 할당량 사용 알림이 활성화된 경우 할당량이 낮거나 초과되면 다음과 같이 테넌트 관리자에 표시됩니다.

테넌트 할당량의 90% 이상이 사용된 경우 * Tenant quota usage high * 경고가 트리거됩니다. 자세한 내용은 StorageGRID 모니터링 및 문제 해결 설명서의 경고 참조를 참조하십시오.

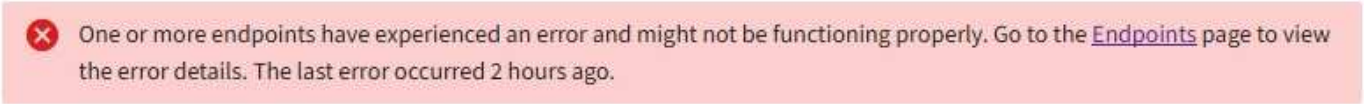
할당량을 초과하면 새 객체를 업로드할 수 없습니다.



추가 세부 정보를 보고 알림에 대한 규칙 및 알림을 관리하려면 StorageGRID 모니터링 및 문제 해결 지침을 참조하십시오.

끝점 오류

Grid Manager를 사용하여 플랫폼 서비스에 사용할 하나 이상의 엔드포인트를 구성한 경우 지난 7일 이내에 엔드포인트 오류가 발생한 경우 Tenant Manager 대시보드에 경고가 표시됩니다.



끝점 오류에 대한 세부 정보를 보려면 끝점 을 선택하여 끝점 페이지를 표시합니다.

관련 정보

플랫폼 서비스 끝점 오류 문제 해결

모니터링하고 문제를 해결합니다

테넌트 관리 **API**

테넌트 관리 **API** 이해

테넌트 관리자 사용자 인터페이스 대신 테넌트 관리 REST API를 사용하여 시스템 관리 작업을 수행할 수 있습니다. 예를 들어, API를 사용하여 작업을 자동화하거나 사용자와 같은 여러 엔터티를 더 빠르게 생성할 수 있습니다.

테넌트 관리 API:

- Swagger 오픈 소스 API 플랫폼을 사용합니다. Swagger는 개발자와 개발자가 아닌 사용자가 API와 상호 작용할 수 있는 직관적인 사용자 인터페이스를 제공합니다. Swagger 사용자 인터페이스는 각 API 작동에 대한 전체 세부 정보와 문서를 제공합니다.
- 사용 무중단 업그레이드를 지원하는 버전 관리.

테넌트 관리 API에 대한 Swagger 문서에 액세스하려면 다음을 수행합니다.

단계

1. 테넌트 관리자에 로그인합니다.
2. 테넌트 관리자 상단에서 도움말 아이콘을 선택하고 * API Documentation * 을 선택합니다.

API 작업

테넌트 관리 API는 사용 가능한 API 작업을 다음 섹션으로 구성합니다.

- * 계정 * — 스토리지 사용 정보를 가져오는 것을 포함하여 현재 테넌트 계정의 작업입니다.
- * auth * — 사용자 세션 인증을 수행하기 위한 작업.

  Tenant Management API는 Bearer Token Authentication Scheme을 지원합니다. 테넌트 로그인의 경우 인증 요청의 JSON 본문에 사용자 이름, 암호 및 accountId를 입력합니다(즉, 'POST/API/v3/authorize'). 사용자가 성공적으로 인증되면 보안 토큰이 반환됩니다. 이 토큰은 후속 API 요청 헤더("Authorization: Bearer token")에 제공되어야 합니다.

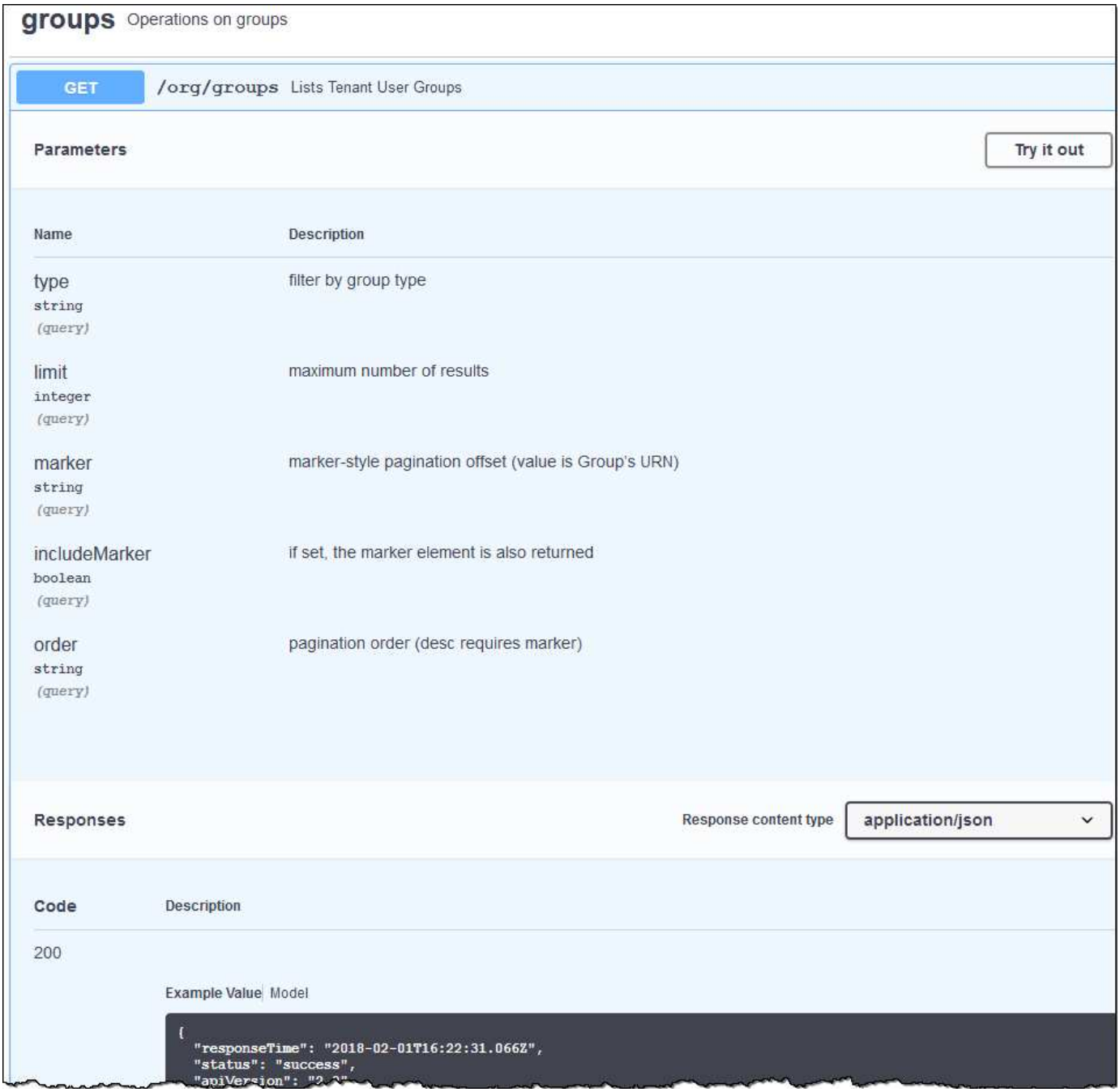
  인증 보안 개선에 대한 자세한 내용은 을 참조하십시오 사이트 간 요청 위조 방지.

  > StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 인증을 위해 다른 단계를 수행해야 합니다. 를 참조하십시오 Grid Management API 사용 지침.

- * config * — 제품 릴리스 및 테넌트 관리 API 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 API의 주요 버전을 나열할 수 있습니다.
- * 컨테이너 * — S3 버킷 또는 Swift 컨테이너에서 다음과 같은 작업을 수행합니다.
- S3 *
  - 버킷 생성(S3 오브젝트 잠금이 활성화된 상태 및 활성화되지 않은 상태)
  - 버킷 기본 보존 수정(S3 오브젝트 잠금이 활성화된 버킷의 경우)
  - 객체에 대해 수행되는 작업에 대한 정합성 제어를 설정합니다
  - 버킷의 CORS 구성을 생성, 업데이트 및 삭제합니다
  - 객체에 대한 마지막 액세스 시간 업데이트를 설정 및 해제합니다
  - CloudMirror 복제, 알림 및 검색 통합(메타데이터 알림)을 비롯한 플랫폼 서비스에 대한 구성 설정 관리
  - 빈 버킷을 삭제합니다
- Swift *: 컨테이너에 사용되는 정합성 수준을 설정합니다
- * deactivated - features * — 비활성화된 기능을 보기 위한 작업.
- * 끝점 * — 끝점을 관리하는 작업. 엔드포인트는 S3 버킷이 StorageGRID CloudMirror 복제, 알림 또는 검색 통합에 외부 서비스를 사용할 수 있도록 합니다.
- * 그룹 * — 로컬 테넌트 그룹을 관리하고 외부 ID 소스에서 통합 테넌트 그룹을 검색하는 작업입니다.
- * identity-source * — 외부 ID 소스를 구성하고 통합 그룹 및 사용자 정보를 수동으로 동기화하는 작업.
- * 지역 * — StorageGRID 시스템에 대해 구성된 지역을 결정하는 작업.
- * S3 * — 테넌트 사용자를 위한 S3 액세스 키를 관리하는 운영
- * S3-오브젝트 잠금 * — 글로벌 S3 오브젝트 잠금 설정에서 운영, 규정 준수 지원에 사용됩니다.
- * 사용자 * — 테넌트 사용자를 보고 관리하는 작업.

작업 세부 정보

각 API 작업을 확장하면 HTTP 동작, 끝점 URL, 필수 또는 선택적 매개 변수 목록, 요청 본문(필요한 경우) 예제 및 가능한 응답을 볼 수 있습니다.



API 요청을 발행합니다

> API Docs 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

단계

1. 요청 세부 정보를 보려면 HTTP 작업을 선택합니다.
2. 요청에 그룹 또는 사용자 ID와 같은 추가 매개 변수가 필요한지 확인합니다. 그런 다음 이 값을 구합니다. 필요한 정보를 얻기 위해 먼저 다른 API 요청을 발급해야 할 수도 있습니다.
3. 예제 요청 본문을 수정해야 하는지 확인합니다. 이 경우 * Model * 을 선택하여 각 필드의 요구 사항을 확인할 수 있습니다.

4. 체험하기 * 를 선택합니다.
5. 필요한 매개 변수를 제공하거나 요청 본문을 필요에 따라 수정합니다.
6. Execute * 를 선택합니다.
7. 응답 코드를 검토하여 요청이 성공했는지 확인합니다.

테넌트 관리 **API** 버전 관리

테넌트 관리 API는 버전 관리를 사용하여 무중단 업그레이드를 지원합니다.

예를 들어 이 요청 URL은 API의 버전 3을 지정합니다.

```
https://hostname_or_ip_address/api/v3/authorize
```

테넌트 관리 API의 주요 버전은 이전 버전과 * _호환되지 않는 _ * 변경 사항이 있을 때 충돌합니다. 테넌트 관리 API의 부 버전은 * _ 이(가) 이전 버전과 호환된다는 변경 사항이 있을 때 충돌합니다. 호환 가능한 변경 사항에는 새 끝점 또는 새 속성 추가가 포함됩니다. 다음 예제에서는 변경 유형에 따라 API 버전을 충돌하는 방법을 보여 줍니다.

API 변경 유형입니다	이전 버전	새 버전
이전 버전과 호환 가능합니다	2.1	2.2
이전 버전과 호환되지 않습니다	2.1	3.0

StorageGRID 소프트웨어를 처음 설치하면 가장 최신 버전의 테넌트 관리 API만 활성화됩니다. 그러나 StorageGRID를 새 기능 릴리즈로 업그레이드하면 하나 이상의 StorageGRID 기능 릴리즈에 대한 이전 API 버전에 계속 액세스할 수 있습니다.

오래된 요청은 다음과 같은 방법으로 더 이상 사용되지 않는 것으로 표시됩니다.

- 응답 헤더가 "DEPRECATED:TRUE"입니다.
- JSON 응답 본문에는 "DEPRECATED"가 포함됩니다. TRUE

현재 릴리즈에서 지원되는 **API** 버전을 확인합니다

다음 API 요청을 사용하여 지원되는 API 주요 버전 목록을 반환합니다.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

요청에 대한 **API** 버전을 지정합니다

PATH 파라미터('/api/v3')나 header('api-Version:3')를 이용하여 API 버전을 지정할 수 있다. 두 값을 모두 제공하면 헤더 값이 경로 값을 재정의합니다.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

사이트 간 요청 위조**(CSRF)**로부터 보호

CSRF 토큰을 사용하여 쿠키를 사용하는 인증을 강화하면 StorageGRID에 대한 CSRF(사이트 간 요청 위조) 공격으로부터 보호할 수 있습니다. Grid Manager 및 Tenant Manager는 이 보안 기능을 자동으로 활성화합니다. 다른 API 클라이언트는 로그인할 때 활성화 여부를 선택할 수 있습니다.

HTTP 양식 POST와 같이 다른 사이트에 대한 요청을 트리거할 수 있는 공격자는 로그인한 사용자의 쿠키를 사용하여 특정 요청을 만들 수 있습니다.

StorageGRID는 CSRF 토큰을 사용하여 CSRF 공격으로부터 보호합니다. 활성화된 경우 특정 쿠키의 내용은 특정 헤더 또는 특정 POST 본문 매개 변수의 내용과 일치해야 합니다.

이 기능을 활성화하려면 인증 중에 csrfToken 매개 변수를 true로 설정하십시오. 기본값은 false 입니다.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

true이면 Grid Manager에 로그인할 때 임의의 값으로 GridCsrfToken 쿠키가 설정되고 테넌트 관리자에 로그인할 때

임의의 값으로 AccountCsrfToken 쿠키가 설정됩니다.

쿠키가 있는 경우 시스템 상태(POST, PUT, 패치, 삭제)를 수정할 수 있는 모든 요청에 다음 중 하나가 포함되어야 합니다.

- CSRF 토큰 쿠키의 값으로 설정된 헤더의 X-CSRF-Token 헤더입니다.
- 폼 인코딩된 본문을 허용하는 끝점의 경우 "csrfToken" 형식 인코딩된 요청 본문 매개 변수입니다.

CSRF 보호를 구성하려면 를 사용합니다 Grid Management API를 참조하십시오 또는 테넌트 관리 API.

> CSRF 토큰 쿠키 세트를 가진 요청은 또한 JSON 요청 본문을 CSRF 공격에 대한 추가 보호로서 기대하는 모든 요청에 대해 ""Content-Type:application/json"" 헤더를 적용합니다.

시스템 액세스를 관리합니다

ID 페더레이션을 사용합니다

ID 페더레이션을 사용하면 테넌트 그룹 및 사용자를 더 빠르게 설정할 수 있으며, 테넌트 사용자는 익숙한 자격 증명을 사용하여 테넌트 계정에 로그인할 수 있습니다.

테넌트 관리자에 대한 **ID** 페더레이션을 구성합니다

테넌트 그룹 및 사용자를 Active Directory, Azure Active Directory(Azure AD), OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 관리하도록 하려면 테넌트 관리자에 대한 ID 페더레이션을 구성할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.
- Active Directory, Azure AD, OpenLDAP 또는 Oracle Directory Server를 ID 공급자로 사용하고 있습니다.

  > 목록에 없는 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의하십시오.

- OpenLDAP를 사용하려면 OpenLDAP 서버를 구성해야 합니다. 을 참조하십시오 OpenLDAP 서버 구성 지침.
- LDAP 서버와의 통신에 TLS(Transport Layer Security)를 사용하려는 경우 ID 공급자는 TLS 1.2 또는 1.3을 사용해야 합니다. 을 참조하십시오 발신 TLS 연결에 지원되는 암호.

이 작업에 대해

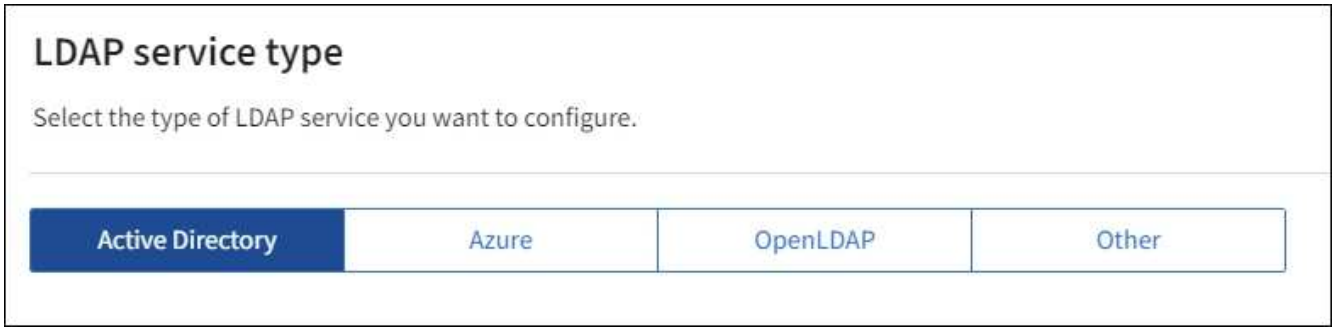
테넌트의 ID 페더레이션 서비스를 구성할 수 있는지 여부는 테넌트 계정 설정 방법에 따라 달라집니다. 테넌트가 Grid Manager용으로 구성된 ID 페더레이션 서비스를 공유할 수 있습니다. ID 페더레이션 페이지에 액세스할 때 이 메시지가 표시되면 이 테넌트에 대해 별도의 통합 ID 소스를 구성할 수 없습니다.

> This tenant account uses the LDAP server that is configured for the Grid Manager.
> Contact the grid administrator for information or to change this setting.

구성을 입력합니다

단계

1. 액세스 관리 * > * ID 페더레이션 * 을 선택합니다.
2. ID 페더레이션 사용 * 을 선택합니다.
3. LDAP 서비스 유형 섹션에서 구성할 LDAP 서비스 유형을 선택합니다.



Oracle Directory Server를 사용하는 LDAP 서버의 값을 구성하려면 * 기타 * 를 선택합니다.

4. 기타 * 를 선택한 경우 LDAP 속성 섹션의 필드를 작성합니다. 그렇지 않으면 다음 단계로 이동합니다.
   - * 사용자 고유 이름 *: LDAP 사용자의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 Active Directory의 경우 'AMAccountName', OpenLDAP의 경우 'uid'와 같습니다. Oracle Directory Server를 구성하는 경우 "uid"를 입력합니다.
   - * 사용자 UUID *: LDAP 사용자의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 Active Directory의 경우 objectGUID, OpenLDAP의 경우 entryUUID와 같습니다. Oracle Directory Server를 구성하는 경우 "n스uniqueid"를 입력합니다. 지정된 속성에 대한 각 사용자의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.
   - * 그룹 고유 이름 *: LDAP 그룹의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 Active Directory의 경우 'AMAccountName', OpenLDAP의 경우 'cn'과 같습니다. Oracle Directory Server를 구성하는 경우 cn을 입력합니다.
   - * 그룹 UUID *: LDAP 그룹의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 Active Directory의 경우 objectGUID, OpenLDAP의 경우 entryUUID와 같습니다. Oracle Directory Server를 구성하는 경우 "n스uniqueid"를 입력합니다. 지정된 속성에 대한 각 그룹의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.
5. 모든 LDAP 서비스 유형에 대해 LDAP 서버 구성 섹션에 필요한 LDAP 서버 및 네트워크 연결 정보를 입력합니다.
   - * 호스트 이름 *: LDAP 서버의 FQDN(정규화된 도메인 이름) 또는 IP 주소입니다.
   - * 포트 *: LDAP 서버에 연결하는 데 사용되는 포트입니다.

     STARTTLS의 기본 포트는 389이고 LDAPS의 기본 포트는 636입니다. 그러나 방화벽이 올바르게 구성된 경우 모든 포트를 사용할 수 있습니다.

   - * 사용자 이름 *: LDAP 서버에 연결할 사용자의 DN(고유 이름)의 전체 경로입니다.

     Active Directory의 경우 아래쪽 로그온 이름 또는 사용자 기본 이름을 지정할 수도 있습니다.

     지정된 사용자는 그룹 및 사용자를 나열하고 다음 속성에 액세스할 수 있는 권한이 있어야 합니다.

     - '사계정 이름' 또는 'uid'
     - objectGUID, entryUUID, n스uniqueid

        - 'cn'입니다
        - 'emberOf' 또는 'isMemberOf'
        - Active Directory *: objectSid, primaryGroupID, userAccountControl, userPrincipalName
        - * Azure *:'accountEnabled' 및 'userPrincipalName'
    - * 암호 *: 사용자 이름과 연결된 암호입니다.
    - * Group Base DN *: 그룹을 검색할 LDAP 하위 트리에 대한 DN(고유 이름)의 전체 경로입니다. Active Directory 예제(아래)에서 고유 이름이 기본 DN(DC=StorageGrid, DC=example, DC=com)과 관련된 모든 그룹을 통합 그룹으로 사용할 수 있습니다.

      > 그룹 고유 이름 * 값은 * 그룹 기본 DN * 내에서 고유해야 합니다.

    - * 사용자 기본 DN *: 사용자를 검색할 LDAP 하위 트리의 고유 이름(DN)의 전체 경로입니다.

      > 사용자 고유 이름 * 값은 * 사용자 기본 DN * 내에서 고유해야 합니다.

    - * 사용자 이름 형식 바인딩 * (선택 사항): 패턴을 자동으로 확인할 수 없는 경우 StorageGRID에서 기본 사용자 이름 패턴을 사용해야 합니다.

      StorageGRID가 서비스 계정에 바인딩할 수 없는 경우 사용자가 로그인할 수 있으므로 * 사용자 이름 형식 바인딩 * 을 제공하는 것이 좋습니다.

      다음 패턴 중 하나를 입력합니다.

        - * UserPrincipalName 패턴(Active Directory 및 Azure) *: '[UserName]@*example*.com'
        - * 하위 수준 로그온 이름 패턴(Active Directory 및 Azure) *: `*example*\[사용자 이름]'
        - * 고유 이름 패턴 *:'CN=[UserName],CN=Users,DC=*Example*,DC=com'

          [UserName] * 을 서면 그대로 포함합니다.

6. TLS(전송 계층 보안) 섹션에서 보안 설정을 선택합니다.
    - * STARTTLS 사용 *: STARTTLS를 사용하여 LDAP 서버와의 통신 보안을 설정합니다. 이 옵션은 Active Directory, OpenLDAP 또는 기타 에 대해 권장되지만 Azure에서는 지원되지 않습니다.
    - * LDAPS * 사용: LDAPS(LDAP over SSL) 옵션은 TLS를 사용하여 LDAP 서버에 연결합니다. Azure의 경우 이 옵션을 선택해야 합니다.
    - * TLS * 사용 안 함: StorageGRID 시스템과 LDAP 서버 간의 네트워크 트래픽은 보호되지 않습니다. 이 옵션은 Azure에서 지원되지 않습니다.

      > Active Directory 서버가 LDAP 서명을 적용하는 경우 * TLS 사용 안 함 * 옵션을 사용할 수 없습니다. STARTTLS 또는 LDAPS를 사용해야 합니다.

7. STARTTLS 또는 LDAPS를 선택한 경우 연결 보안에 사용되는 인증서를 선택합니다.
    - * 운영 체제 CA 인증서 사용 *: 운영 체제에 설치된 기본 그리드 CA 인증서를 사용하여 연결을 보호합니다.
    - * 사용자 지정 CA 인증서 사용 *: 사용자 지정 보안 인증서를 사용합니다.

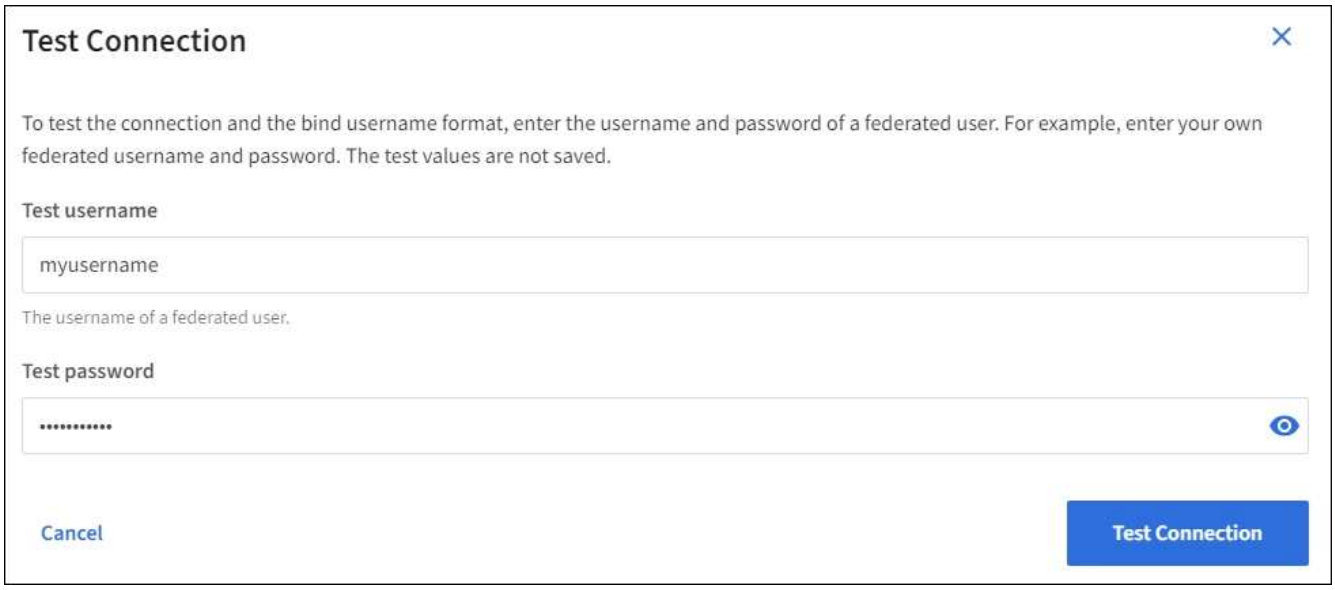
      이 설정을 선택한 경우 사용자 지정 보안 인증서를 복사하여 CA 인증서 텍스트 상자에 붙여 넣습니다.

연결을 테스트하고 구성을 저장합니다

모든 값을 입력한 후 구성을 저장하기 전에 연결을 테스트해야 합니다. StorageGRID는 LDAP 서버에 대한 연결 설정과 바인딩 사용자 이름 형식(제공한 경우)을 확인합니다.

1. Test connection * 을 선택합니다.
2. 바인딩 사용자 이름 형식을 제공하지 않은 경우:
   - 연결 설정이 유효하면 "Test connection successful(연결 테스트 성공)" 메시지가 나타납니다. Save * 를 선택하여 설정을 저장합니다.
   - 연결 설정이 잘못된 경우 ""테스트 연결을 설정할 수 없습니다"" 메시지가 나타납니다. 닫기 * 를 선택합니다. 그런 다음 문제를 해결하고 연결을 다시 테스트합니다.
3. 바인딩 사용자 이름 형식을 제공한 경우 유효한 통합 사용자의 사용자 이름과 암호를 입력합니다.

   예를 들어 사용자 이름과 암호를 입력합니다. @ 또는 / 같은 특수 문자를 사용자 이름에 포함하지 마십시오.



   - 연결 설정이 유효하면 "Test connection successful(연결 테스트 성공)" 메시지가 나타납니다. Save * 를 선택하여 설정을 저장합니다.
   - 연결 설정, 바인딩 사용자 이름 형식 또는 테스트 사용자 이름과 암호가 올바르지 않으면 오류 메시지가 나타납니다. 모든 문제를 해결하고 연결을 다시 테스트합니다.

ID 소스와 강제로 동기화합니다

StorageGRID 시스템은 ID 소스에서 페더레이션 그룹과 사용자를 정기적으로 동기화합니다. 사용자 권한을 최대한 빨리 설정하거나 제한하려는 경우 동기화를 강제로 시작할 수 있습니다.

단계

1. ID 페더레이션 페이지로 이동합니다.
2. 페이지 맨 위에서 * 서버 동기화 * 를 선택합니다.

   동기화 프로세스는 환경에 따라 다소 시간이 걸릴 수 있습니다.

ID 소스에서 페더레이션 그룹과 사용자를 동기화하는 데 문제가 있는 경우 * ID 페더레이션 동기화 실패 * 경고가 트리거됩니다.

ID 페더레이션을 비활성화합니다

그룹 및 사용자에 대한 ID 페더레이션을 일시적으로 또는 영구적으로 비활성화할 수 있습니다. ID 페더레이션을 사용하지 않도록 설정하면 StorageGRID와 ID 소스 간에 통신이 이루어지지 않습니다. 그러나 구성한 설정은 그대로 유지되므로 나중에 ID 페더레이션을 쉽게 다시 사용할 수 있습니다.

이 작업에 대해

ID 페더레이션을 사용하지 않도록 설정하기 전에 다음 사항을 확인해야 합니다.

- 페더레이션 사용자는 로그인할 수 없습니다.
- 현재 로그인한 페더레이션 사용자는 세션이 만료될 때까지 StorageGRID 시스템에 대한 액세스 권한을 유지하지만 세션이 만료된 후에는 로그인할 수 없습니다.
- StorageGRID 시스템과 ID 소스 간의 동기화는 수행되지 않으며 동기화되지 않은 계정에 대해 알림 또는 경보가 발생하지 않습니다.
- SSO(Single Sign-On)가 * Enabled * 또는 * Sandbox Mode * 로 설정된 경우 * Enable identity federation *(ID 페더레이션 사용 *) 확인란이 비활성화됩니다. ID 페더레이션을 비활성화하려면 Single Sign-On 페이지의 SSO 상태가 * 사용 안 함 * 이어야 합니다. 을 참조하십시오 SSO(Single Sign-On)를 비활성화합니다.

단계

1. ID 페더레이션 페이지로 이동합니다.
2. ID 페더레이션 사용 * 확인란의 선택을 취소합니다.

OpenLDAP 서버 구성 지침

OpenLDAP 서버를 ID 페더레이션에 사용하려면 OpenLDAP 서버에서 특정 설정을 구성해야 합니다.

ActiveDirectory 또는 Azure가 아닌 ID 소스의 경우 StorageGRID는 외부에서 비활성화된 사용자에 대한 S3 액세스를 자동으로 차단하지 않습니다. S3 액세스를 차단하려면 사용자의 S3 키를 삭제하고 모든 그룹에서 사용자를 제거합니다.

MemberOf 및 구체화 오버레이

MemberOf 및 구체화 오버레이를 활성화해야 합니다. 자세한 내용은 의 역방향 그룹 구성원 유지 관리 지침을 참조하십시오http://www.openldap.org/doc/admin24/index.html["OpenLDAP 설명서: 버전 2.4 관리자 가이드"^].

인덱싱

지정된 인덱스 키워드를 사용하여 다음 OpenLDAP 속성을 구성해야 합니다.

- olcDbIndex:objectClass eq
- "olcDbIndex:uid eq,pres,sub'
- 올크DbIndex=cn eq,pres,sub
- olcDbIndex: entryUUID eq

또한 최적의 성능을 위해 사용자 이름 도움말에 언급된 필드를 인덱싱해야 합니다.

에서 역방향 그룹 구성원 유지 관리에 대한 정보를
참조하십시오http://www.openldap.org/doc/admin24/index.html["OpenLDAP 설명서: 버전 2.4 관리자 가이드"^].

그룹을 관리합니다

S3 테넌트에 대한 그룹을 생성합니다

통합 그룹을 가져오거나 로컬 그룹을 생성하여 S3 사용자 그룹에 대한 권한을 관리할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.
- 통합 그룹을 가져오려는 경우 ID 페더레이션을 구성하고 통합 그룹이 이미 구성된 ID 소스에 있습니다.

S3에 대한 자세한 내용은 을 참조하십시오 S3을 사용합니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.

2. Create group * 을 선택합니다.
3. 로컬 그룹을 생성하려면 * Local group * 탭을 선택하고, 이전에 구성된 ID 소스에서 그룹을 가져오려면 * Federated group * 탭을 선택합니다.

   StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하는 경우 로컬 그룹에 속한 사용자는 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있지만 테넌트 관리자에 로그인할 수 없습니다.

4. 그룹의 이름을 입력합니다.

- * 로컬 그룹 *: 표시 이름과 고유 이름을 모두 입력합니다. 나중에 표시 이름을 편집할 수 있습니다.
- * 페더레이션 그룹 *: 고유한 이름을 입력합니다. Active Directory의 경우 고유한 이름은 'AMAccountName' 속성과 관련된 이름입니다. OpenLDAP의 경우 고유 이름은 "uid" 특성과 관련된 이름입니다.

5. Continue * 를 선택합니다.
6. 액세스 모드를 선택합니다. 사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.
   - * 읽기-쓰기 * (기본값): 사용자는 테넌트 관리자에 로그인하여 테넌트 구성을 관리할 수 있습니다.
   - * 읽기 전용 *: 사용자는 설정 및 기능만 볼 수 있습니다. 테넌트 관리자 또는 테넌트 관리 API에서 작업을 변경하거나 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 암호를 변경할 수 있습니다.
7. 이 그룹에 대한 그룹 권한을 선택합니다.

   테넌트 관리 권한에 대한 정보를 참조하십시오.

8. Continue * 를 선택합니다.
9. 그룹 정책을 선택하여 이 그룹의 구성원이 가질 S3 액세스 권한을 결정합니다.
   - * S3 액세스 없음 *: 기본값. 이 그룹의 사용자는 버킷 정책을 통해 액세스가 부여되지 않는 한 S3 리소스에 액세스할 수 없습니다. 이 옵션을 선택하면 루트 사용자만 기본적으로 S3 리소스에 액세스할 수 있습니다.
   - * 읽기 전용 액세스 *: 이 그룹의 사용자는 S3 리소스에 대한 읽기 전용 액세스 권한을 가집니다. 예를 들어 이 그룹의 사용자는 개체를 나열하고 개체 데이터, 메타데이터 및 태그를 읽을 수 있습니다. 이 옵션을 선택하면 읽기 전용 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
   - * 전체 액세스 *: 이 그룹의 사용자는 버킷을 포함하여 S3 리소스에 대한 모든 액세스 권한을 가집니다. 이 옵션을 선택하면 전체 액세스 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
   - * 사용자 정의 *: 그룹의 사용자에게는 텍스트 상자에 지정한 사용 권한이 부여됩니다. 언어 구문 및 예제를 비롯한 그룹 정책에 대한 자세한 내용은 S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.
10. 사용자 정의 * 를 선택한 경우 그룹 정책을 입력합니다. 각 그룹 정책은 크기 제한이 5,120바이트입니다. 올바른 JSON 형식 문자열을 입력해야 합니다.

    이 예제에서 그룹 구성원은 지정된 버킷의 사용자 이름(키 접두사)과 일치하는 폴더만 나열하고 액세스할 수 있습니다. 이러한 폴더의 개인 정보를 확인할 때는 다른 그룹 정책 및 버킷 정책의 액세스 권한을 고려해야 합니다.

11. 통합 그룹을 생성하는지 또는 로컬 그룹을 생성하는지에 따라 표시되는 버튼을 선택합니다.

    - 통합 그룹: * 그룹 생성 *
    - 로컬 그룹: * 계속 *

    로컬 그룹을 만드는 경우 * Continue * 를 선택하면 4단계(사용자 추가)가 나타납니다. 이 단계는 통합 그룹에 대해서는 나타나지 않습니다.

12. 그룹에 추가할 각 사용자에 대한 확인란을 선택한 다음 * 그룹 생성 * 을 선택합니다.

    필요에 따라 사용자를 추가하지 않고 그룹을 저장할 수 있습니다. 나중에 그룹에 사용자를 추가하거나 새 사용자를 추가할 때 그룹을 선택할 수 있습니다.

13. 마침 * 을 선택합니다.

    생성한 그룹이 그룹 목록에 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

Swift 테넌트의 그룹을 생성합니다

통합 그룹을 가져오거나 로컬 그룹을 생성하여 Swift 테넌트 계정에 대한 액세스 권한을 관리할 수 있습니다. 하나 이상의 그룹에 Swift 관리자 권한이 있어야 합니다. 이 권한은 Swift 테넌트 계정의 컨테이너 및 개체를 관리하는 데 필요합니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

- 통합 그룹을 가져오려는 경우 ID 페더레이션을 구성하고 통합 그룹이 이미 구성된 ID 소스에 있습니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.

2. Create group * 을 선택합니다.
3. 로컬 그룹을 생성하려면 * Local group * 탭을 선택하고, 이전에 구성된 ID 소스에서 그룹을 가져오려면 * Federated group * 탭을 선택합니다.

   StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하는 경우 로컬 그룹에 속한 사용자는 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있지만 테넌트 관리자에 로그인할 수 없습니다.

4. 그룹의 이름을 입력합니다.
   - * 로컬 그룹 *: 표시 이름과 고유 이름을 모두 입력합니다. 나중에 표시 이름을 편집할 수 있습니다.
   - * 페더레이션 그룹 *: 고유한 이름을 입력합니다. Active Directory의 경우 고유한 이름은 'AMAccountName' 속성과 관련된 이름입니다. OpenLDAP의 경우 고유 이름은 "uid" 특성과 관련된 이름입니다.
5. Continue * 를 선택합니다.
6. 액세스 모드를 선택합니다. 사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.
   - * 읽기-쓰기 * (기본값): 사용자는 테넌트 관리자에 로그인하여 테넌트 구성을 관리할 수 있습니다.
   - * 읽기 전용 *: 사용자는 설정 및 기능만 볼 수 있습니다. 테넌트 관리자 또는 테넌트 관리 API에서 작업을 변경하거나 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 암호를 변경할 수 있습니다.
7. 그룹 권한을 설정합니다.
   - 사용자가 테넌트 관리자 또는 테넌트 관리 API에 로그인해야 하는 경우 * Root Access * 확인란을 선택합니다. (기본값)
   - 사용자가 테넌트 관리자 또는 테넌트 관리 API에 액세스할 필요가 없는 경우 * Root Access * (루트 액세스 *) 확인란의 선택을 취소합니다. 예를 들어, 테넌트에 액세스할 필요가 없는 응용 프로그램의 확인란을 선택

취소합니다. 그런 다음 이러한 사용자가 컨테이너 및 개체를 관리할 수 있도록 * Swift 관리자 * 권한을 할당합니다.

8. Continue * 를 선택합니다.
9. 사용자가 Swift REST API를 사용할 수 있어야 하는 경우 * Swift administrator * 확인란을 선택합니다.

   Swift 사용자는 테넌트 관리자에 액세스하려면 루트 액세스 권한이 있어야 합니다. 그러나 루트 액세스 권한은 사용자가 Swift REST API에 인증하여 컨테이너를 생성하고 객체를 수집하는 것을 허용하지 않습니다. 사용자는 Swift REST API에 인증할 수 있는 Swift 관리자 권한이 있어야 합니다.

10. 통합 그룹을 생성하는지 또는 로컬 그룹을 생성하는지에 따라 표시되는 버튼을 선택합니다.
    - 통합 그룹: * 그룹 생성 *
    - 로컬 그룹: * 계속 *

      로컬 그룹을 만드는 경우 * Continue * 를 선택하면 4단계(사용자 추가)가 나타납니다. 이 단계는 통합 그룹에 대해서는 나타나지 않습니다.

11. 그룹에 추가할 각 사용자에 대한 확인란을 선택한 다음 * 그룹 생성 * 을 선택합니다.

    필요에 따라 사용자를 추가하지 않고 그룹을 저장할 수 있습니다. 나중에 그룹에 사용자를 추가하거나 새 사용자를 만들 때 그룹을 선택할 수 있습니다.

12. 마침 * 을 선택합니다.

    생성한 그룹이 그룹 목록에 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

테넌트 관리 권한

Swift를 사용합니다

테넌트 관리 권한

테넌트 그룹을 생성하기 전에 해당 그룹에 할당할 권한을 고려하십시오. 테넌트 관리 권한은 사용자가 테넌트 관리자 또는 테넌트 관리 API를 사용하여 수행할 수 있는 작업을 결정합니다. 사용자는 하나 이상의 그룹에 속할 수 있습니다. 사용자가 여러 그룹에 속한 경우 권한은 누적됩니다.

테넌트 관리자에 로그인하거나 테넌트 관리 API를 사용하려면 사용자가 하나 이상의 권한이 있는 그룹에 속해야 합니다. 로그인할 수 있는 모든 사용자는 다음 작업을 수행할 수 있습니다.

- 대시보드 보기
- 자신의 암호 변경(로컬 사용자의 경우)

모든 권한에 대해 그룹의 액세스 모드 설정은 사용자가 설정을 변경하고 작업을 수행할 수 있는지 또는 관련 설정과 기능만 볼 수 있는지 여부를 결정합니다.

> 사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.

그룹에 다음 권한을 할당할 수 있습니다. S3 테넌트와 Swift 테넌트는 다른 그룹 권한을 가집니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

권한	설명
루트 액세스	테넌트 관리자 및 테넌트 관리 API에 대한 전체 액세스를 제공합니다. • 참고: * Swift 사용자는 테넌트 계정에 로그인하려면 루트 액세스 권한이 있어야 합니다.
관리자	Swift 테넌트만 해당. 이 테넌트 계정에 대한 Swift 컨테이너 및 객체에 대한 전체 액세스를 제공합니다 • 참고: * Swift 사용자는 Swift REST API를 사용하여 모든 작업을 수행하려면 Swift 관리자 권한이 있어야 합니다.
자신의 S3 자격 증명을 관리합니다	S3 테넌트만 해당. 사용자가 자신의 S3 액세스 키를 생성하고 제거할 수 있습니다. 이 권한이 없는 사용자는 * storage(S3) * > * My S3 access keys * 메뉴 옵션을 볼 수 없습니다.
모든 버킷 관리	• S3 테넌트: 사용자가 테넌트 관리자 및 테넌트 관리 API를 사용하여 S3 버킷을 생성 및 삭제하고 S3 버킷 또는 그룹 정책에 관계없이 테넌트 계정의 모든 S3 버킷을 관리할 수 있습니다. 이 권한이 없는 사용자는 * Bucket * 메뉴 옵션을 볼 수 없습니다. • Swift 테넌트: Swift 사용자가 테넌트 관리 API를 사용하여 Swift 컨테이너의 정합성 수준을 제어할 수 있습니다. • 참고: * 테넌트 관리 API에서 Swift 그룹에만 모든 버킷 관리 권한을 할당할 수 있습니다. 테넌트 관리자를 사용하여 Swift 그룹에 이 권한을 할당할 수 없습니다.
엔드포인트 관리	S3 테넌트만 해당. 테넌트 관리자 또는 테넌트 관리 API를 사용하여 StorageGRID 플랫폼 서비스의 대상으로 사용되는 엔드포인트를 생성하거나 편집할 수 있습니다. 이 권한이 없는 사용자는 * 플랫폼 서비스 끝점 * 메뉴 옵션을 볼 수 없습니다.

관련 정보

S3을 사용합니다

Swift를 사용합니다

그룹 세부 정보를 보고 편집합니다

그룹의 세부 정보를 볼 때 그룹의 표시 이름, 사용 권한, 정책 및 그룹에 속한 사용자를 변경할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 세부 정보를 보거나 편집할 그룹의 이름을 선택합니다.

   또는 * Actions * > * View group details * 를 선택할 수 있습니다.

   그룹 세부 정보 페이지가 나타납니다. 다음 예에서는 S3 그룹 세부 정보 페이지를 보여 줍니다.

Groups > Applications

Overview

Display name:	**Applications**
Unique name:	**group/Applications**
Type:	**Local**
Access mode:	**Read-write**
Permissions:	**Root Access**
S3 Policy:	**None**
Number of users in this group:	**0**

Group permissions | S3 group policy | Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

(●) Read-write ( ) Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

[x] **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

[x] **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

[x] **Manage Endpoints**

Allows users to configure endpoints for platform services.

[x] **Manage Your Own S3 Credentials**

Allows users to create and delete their own S3 access keys.

Save changes

3. 필요에 따라 그룹 설정을 변경합니다.

> 변경 내용을 저장하려면 각 섹션을 변경한 후 * 변경 사항 저장 * 을 선택합니다. 변경 내용이 저장되면 페이지의 오른쪽 상단에 확인 메시지가 나타납니다.

   a. 선택적으로 표시 이름 또는 편집 아이콘을 선택합니다 표시 이름을 업데이트합니다.

      그룹의 고유한 이름은 변경할 수 없습니다. 통합 그룹의 표시 이름은 편집할 수 없습니다.

   b. 필요에 따라 사용 권한을 업데이트합니다.

   c. 그룹 정책의 경우 S3 또는 Swift 테넌트를 적절하게 변경합니다.

      - S3 테넌트의 그룹을 편집하는 경우 선택적으로 다른 S3 그룹 정책을 선택합니다. 사용자 지정 S3 정책을 선택한 경우 필요에 따라 JSON 문자열을 업데이트합니다.
      - Swift 테넌트의 그룹을 편집하는 경우, 필요에 따라 * Swift 관리자 * 확인란을 선택하거나 선택 취소합니다.

        Swift 관리자 권한에 대한 자세한 내용은 Swift 테넌트에 대한 그룹 생성 지침을 참조하십시오.

   d. 필요에 따라 사용자를 추가 또는 제거합니다.

4. 변경한 각 섹션에 대해 * 변경 사항 저장 * 을 선택했는지 확인합니다.

   캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

S3 테넌트용 그룹을 생성합니다

Swift 테넌트용 그룹을 생성합니다

로컬 그룹에 사용자를 추가합니다

필요에 따라 로컬 그룹에 사용자를 추가할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 사용자를 추가할 로컬 그룹의 이름을 선택합니다.

   또는 * Actions * > * View group details * 를 선택할 수 있습니다.

   그룹 세부 정보 페이지가 나타납니다.

Groups > Applications

Overview

Display name:	**Applications**
Unique name:	**group/Applications**
Type:	**Local**
Access mode:	**Read-write**
Permissions:	**Root Access**
S3 Policy:	**None**
Number of users in this group:	**0**

Group permissions | S3 group policy | Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

(●) Read-write ( ) Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

[x] **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

[x] **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

[x] **Manage Endpoints**

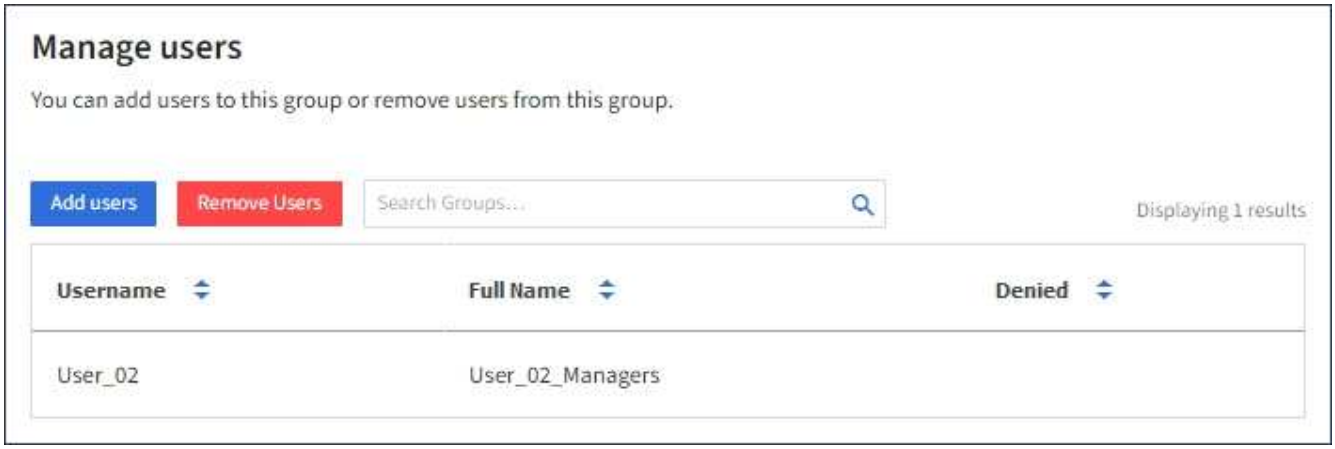
Allows users to configure endpoints for platform services.

[x] **Manage Your Own S3 Credentials**

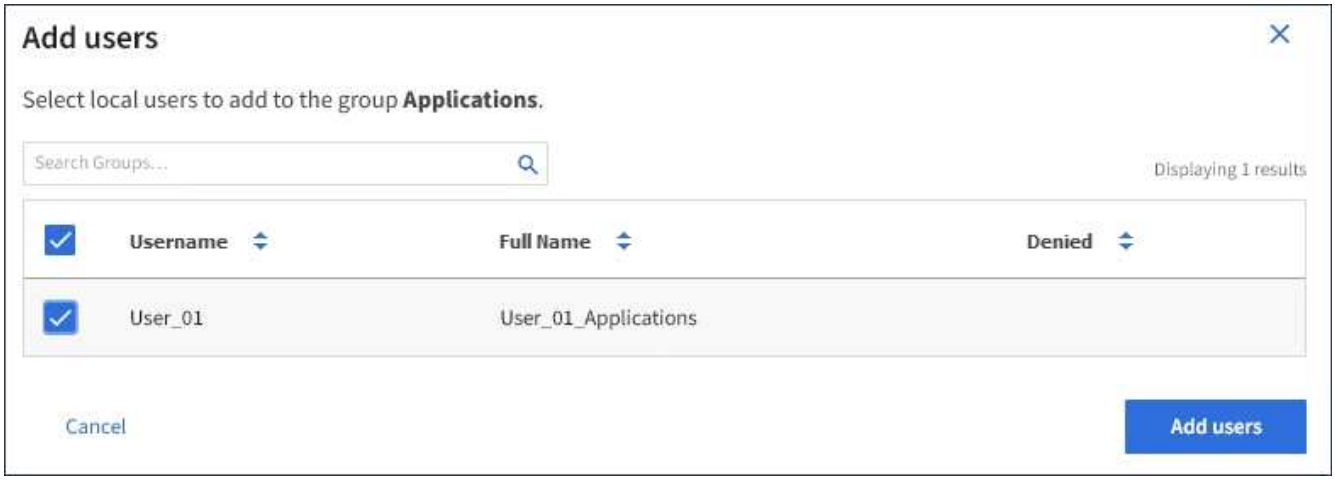
Allows users to create and delete their own S3 access keys.

Save changes

3. 사용자 * 를 선택한 다음 * 사용자 추가 * 를 선택합니다.



4. 그룹에 추가할 사용자를 선택한 다음 * 사용자 추가 * 를 선택합니다.



페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

그룹 이름을 편집합니다

그룹의 표시 이름을 편집할 수 있습니다. 그룹의 고유한 이름은 편집할 수 없습니다.

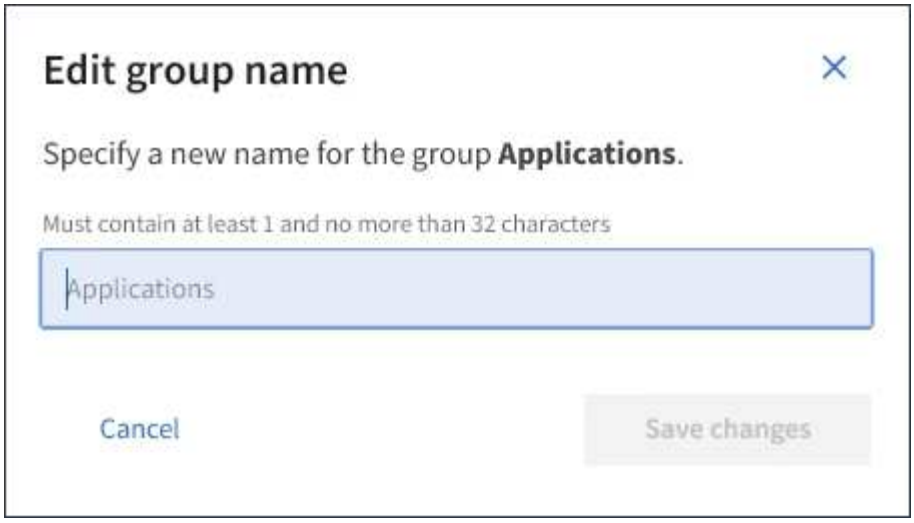
필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 표시 이름을 편집할 그룹의 확인란을 선택합니다.
3. Actions * > * Edit group name * 을 선택합니다.

   Edit group name(그룹 이름 편집) 대화 상자가 나타납니다.



4. 로컬 그룹을 편집하는 경우 필요에 따라 표시 이름을 업데이트합니다.

   그룹의 고유한 이름은 변경할 수 없습니다. 통합 그룹의 표시 이름은 편집할 수 없습니다.

5. 변경 내용 저장 * 을 선택합니다.

   페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

그룹이 중복되었습니다

기존 그룹을 복제하면 새 그룹을 더 빠르게 만들 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 복제할 그룹의 확인란을 선택합니다.
3. Duplicate group * 을 선택합니다. 그룹 만들기에 대한 자세한 내용은 에 대한 그룹 만들기 지침을 참조하십시오 S3 테넌트 또는 을(를) 선택합니다 Swift 테넌트입니다.
4. 로컬 그룹을 생성하려면 * Local group * 탭을 선택하고, 이전에 구성된 ID 소스에서 그룹을 가져오려면 * Federated group * 탭을 선택합니다.

   StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 로컬 그룹에 속하는 사용자는 클라이언트 애플리케이션을 사용하여 테넌트의 리소스를 관리할 수 있지만 테넌트 관리자에 로그인할 수 없습니다. 그룹 권한에 따라 다릅니다.

5. 그룹의 이름을 입력합니다.
   - * 로컬 그룹 *: 표시 이름과 고유 이름을 모두 입력합니다. 나중에 표시 이름을 편집할 수 있습니다.
   - * 페더레이션 그룹 *: 고유한 이름을 입력합니다. Active Directory의 경우 고유한 이름은 'AMAccountName' 속성과 관련된 이름입니다. OpenLDAP의 경우 고유 이름은 "uid" 특성과 관련된 이름입니다.

6. Continue * 를 선택합니다.
7. 필요에 따라 이 그룹에 대한 권한을 수정합니다.
8. Continue * 를 선택합니다.
9. 필요에 따라 S3 테넌트에 대한 그룹을 복제할 경우 * S3 정책 추가 * 라디오 버튼에서 다른 정책을 선택할 수도 있습니다. 사용자 지정 정책을 선택한 경우 필요에 따라 JSON 문자열을 업데이트합니다.
10. Create group * 을 선택합니다.

그룹을 삭제합니다

시스템에서 그룹을 삭제할 수 있습니다. 해당 그룹에만 속하는 사용자는 더 이상 테넌트 관리자에 로그인하거나 테넌트 계정을 사용할 수 없습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.

2. 삭제할 그룹의 확인란을 선택합니다.
3. Actions * > * Delete group * 을 선택합니다.

   확인 메시지가 나타납니다.

4. 확인 메시지에 표시된 그룹을 삭제하려면 * Delete group * 을 선택합니다.

   페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

로컬 사용자를 관리합니다

로컬 사용자를 만들고 로컬 그룹에 할당하여 사용자가 액세스할 수 있는 기능을 결정할 수 있습니다. Tenant Manager에는 ""root""라는 이름의 미리 정의된 로컬 사용자가 한 명 있습니다. 로컬 사용자를 추가 및 제거할 수는 있지만 루트 사용자는 제거할 수 없습니다.

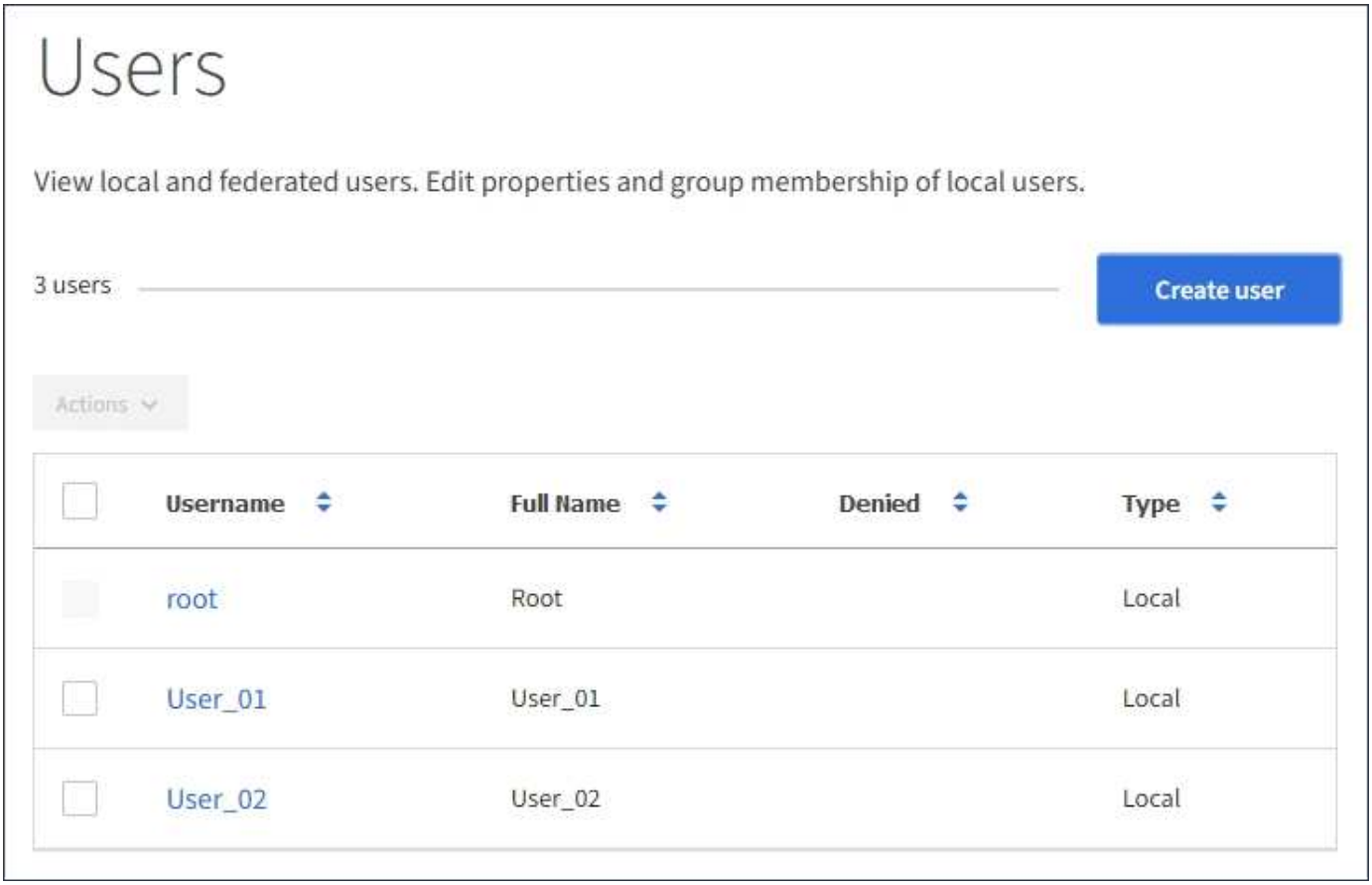
필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있는 읽기-쓰기 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.

> StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 그룹 사용 권한에 따라 S3 또는 Swift 클라이언트 애플리케이션을 사용하여 테넌트의 리소스에 액세스할 수 있지만 로컬 사용자는 테넌트 관리자 또는 테넌트 관리 API에 로그인할 수 없습니다.

사용자 페이지에 액세스합니다

액세스 관리 * > * 사용자 * 를 선택합니다.



로컬 사용자를 생성합니다

로컬 사용자를 만들고 하나 이상의 로컬 그룹에 할당하여 액세스 권한을 제어할 수 있습니다.

그룹에 속하지 않은 S3 사용자는 관리 권한이나 S3 그룹 정책이 적용되지 않습니다. 이러한 사용자는 버킷 정책을 통해 S3 버킷 액세스가 부여될 수 있습니다.

그룹에 속하지 않는 Swift 사용자는 관리 권한이나 Swift 컨테이너 액세스 권한이 없습니다.

단계

1. 사용자 생성 * 을 선택합니다.
2. 다음 필드를 작성합니다.
   - * 전체 이름 *: 이 사용자의 전체 이름(예: 사용자의 이름 및 성 또는 응용 프로그램 이름)입니다.
   - * 사용자 이름 *: 이 사용자가 로그인하는 데 사용할 이름입니다. 사용자 이름은 고유해야 하며 변경할 수 없습니다.
   - * 암호 * : 사용자가 로그인할 때 사용하는 암호입니다.
   - * 암호 확인 *: 암호 필드에 입력한 것과 동일한 암호를 입력합니다.
   - * 액세스 거부 *: * 예 * 를 선택하면 사용자가 하나 이상의 그룹에 속해 있더라도 이 사용자는 테넌트 계정에 로그인할 수 없습니다.

     예를 들어 이 기능을 사용하여 사용자의 로그인 기능을 일시적으로 중단할 수 있습니다.
3. Continue * 를 선택합니다.
4. 사용자를 하나 이상의 로컬 그룹에 할당합니다.

   그룹에 속하지 않은 사용자에게는 관리 권한이 없습니다. 권한은 누적됩니다. 사용자는 자신이 속한 모든 그룹에 대한 모든 권한을 갖게 됩니다.
5. 사용자 생성 * 을 선택합니다.

   캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

사용자 세부 정보를 편집합니다

사용자의 세부 정보를 편집할 때 사용자의 전체 이름과 암호를 변경하고, 사용자를 다른 그룹에 추가하고, 사용자가 테넌트에 액세스하지 못하도록 할 수 있습니다.

단계

1. 사용자 목록에서 세부 정보를 보거나 편집할 사용자의 이름을 선택합니다.

   또는 사용자의 확인란을 선택한 다음 * Actions * > * View user details * 를 선택합니다.
2. 필요에 따라 사용자 설정을 변경합니다.
   a. 필요에 따라 전체 이름 또는 편집 아이콘을 선택하여 사용자의 전체 이름을 변경합니다 개요 섹션.

      사용자 이름은 변경할 수 없습니다.
   b. 암호 * 탭에서 필요에 따라 사용자 암호를 변경합니다.
   c. Access * 탭에서 사용자가 로그인(* 아니요 * 선택)하거나 사용자가 필요에 따라 로그인하지 못하도록 합니다(* 예 * 선택).
   d. 그룹 * 탭에서 사용자를 그룹에 추가하거나 필요에 따라 그룹에서 사용자를 제거합니다.
   e. 각 섹션에 필요한 경우 * 변경 사항 저장 * 을 선택합니다.

캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

로컬 사용자가 중복되었습니다

로컬 사용자를 복제하면 새 사용자를 보다 빠르게 만들 수 있습니다.

단계

1. 사용자 목록에서 복제할 사용자를 선택합니다.
2. 사용자 복제 * 를 선택합니다.
3. 새 사용자에 대해 다음 필드를 수정합니다.
   - * 전체 이름 *: 이 사용자의 전체 이름(예: 사용자의 이름 및 성 또는 응용 프로그램 이름)입니다.
   - * 사용자 이름 *: 이 사용자가 로그인하는 데 사용할 이름입니다. 사용자 이름은 고유해야 하며 변경할 수 없습니다.
   - * 암호 * : 사용자가 로그인할 때 사용하는 암호입니다.
   - * 암호 확인 *: 암호 필드에 입력한 것과 동일한 암호를 입력합니다.
   - * 액세스 거부 *: * 예 * 를 선택하면 사용자가 하나 이상의 그룹에 속해 있더라도 이 사용자는 테넌트 계정에 로그인할 수 없습니다.

     예를 들어 이 기능을 사용하여 사용자의 로그인 기능을 일시적으로 중단할 수 있습니다.
4. Continue * 를 선택합니다.
5. 하나 이상의 로컬 그룹을 선택합니다.

   그룹에 속하지 않은 사용자에게는 관리 권한이 없습니다. 권한은 누적됩니다. 사용자는 자신이 속한 모든 그룹에 대한 모든 권한을 갖게 됩니다.
6. 사용자 생성 * 을 선택합니다.

   캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

로컬 사용자를 삭제합니다

StorageGRID 테넌트 계정에 더 이상 액세스할 필요가 없는 로컬 사용자를 영구적으로 삭제할 수 있습니다.

테넌트 관리자를 사용하여 로컬 사용자는 삭제할 수 있지만 페더레이션 사용자는 삭제할 수 없습니다. 통합 사용자를 삭제하려면 통합 ID 소스를 사용해야 합니다.

단계

1. 사용자 목록에서 삭제할 로컬 사용자의 확인란을 선택합니다.
2. Actions * > * Delete user * 를 선택합니다.
3. 확인 대화 상자에서 * 사용자 삭제 * 를 선택하여 시스템에서 사용자를 삭제할 것인지 확인합니다.

   캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

S3 테넌트 계정 관리

S3 액세스 키를 관리합니다

S3 테넌트 계정의 각 사용자는 StorageGRID 시스템에 오브젝트를 저장하고 검색하기 위한 액세스 키가 있어야 합니다. 액세스 키는 액세스 키 ID와 비밀 액세스 키로 구성됩니다.

이 작업에 대해

S3 액세스 키는 다음과 같이 관리할 수 있습니다.

- 자신의 S3 자격 증명 관리 * 권한이 있는 사용자는 자신의 S3 액세스 키를 생성하거나 제거할 수 있습니다.
- 루트 액세스* 권한이 있는 사용자는 S3 루트 계정 및 다른 모든 사용자의 액세스 키를 관리할 수 있습니다. 루트 액세스 키는 버킷 정책에 의해 명시적으로 비활성화되지 않는 한 테넌트의 모든 버킷과 객체에 대한 전체 액세스를 제공합니다.

StorageGRID는 서명 버전 2 및 서명 버전 4 인증을 지원합니다. 버킷 정책에 의해 명시적으로 활성화되지 않은 경우 교차 계정 액세스가 허용되지 않습니다.

자체 S3 액세스 키를 생성합니다

S3 테넌트를 사용 중이며 적절한 권한이 있는 경우 자체 S3 액세스 키를 생성할 수 있습니다. S3 테넌트 계정의 버킷 및 오브젝트에 액세스하려면 액세스 키가 있어야 합니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 자신의 S3 자격 증명 관리 권한이 있어야 합니다. 을 참조하십시오 테넌트 관리 권한.

이 작업에 대해

하나 이상의 S3 액세스 키를 생성하여 테넌트 계정의 버킷을 생성하고 관리할 수 있습니다. 새 액세스 키를 생성한 후 새 액세스 키 ID와 비밀 액세스 키로 응용 프로그램을 업데이트합니다. 보안을 위해 필요한 것보다 더 많은 키를 생성하지 말고 사용하지 않는 키를 삭제하십시오. 하나의 키만 있고 만료되려고 하는 경우 이전 키가 만료되기 전에 새 키를 만든 다음 이전 키를 삭제합니다.

각 키에는 특정 만료 시간 또는 만료 기간이 있을 수 있습니다. 만료 시간에 대한 다음 지침을 따르십시오.

- 키의 만료 시간을 설정하여 특정 기간에 대한 액세스를 제한합니다. 만료 시간을 짧게 설정하면 액세스 키 ID 및 비밀 액세스 키가 실수로 노출되었을 경우 위험을 줄일 수 있습니다. 만료된 키는 자동으로 제거됩니다.
- 환경의 보안 위험이 낮으며 정기적으로 새 키를 만들 필요가 없는 경우 키에 대한 만료 시간을 설정할 필요가 없습니다. 나중에 새 키를 만들려면 이전 키를 수동으로 삭제합니다.

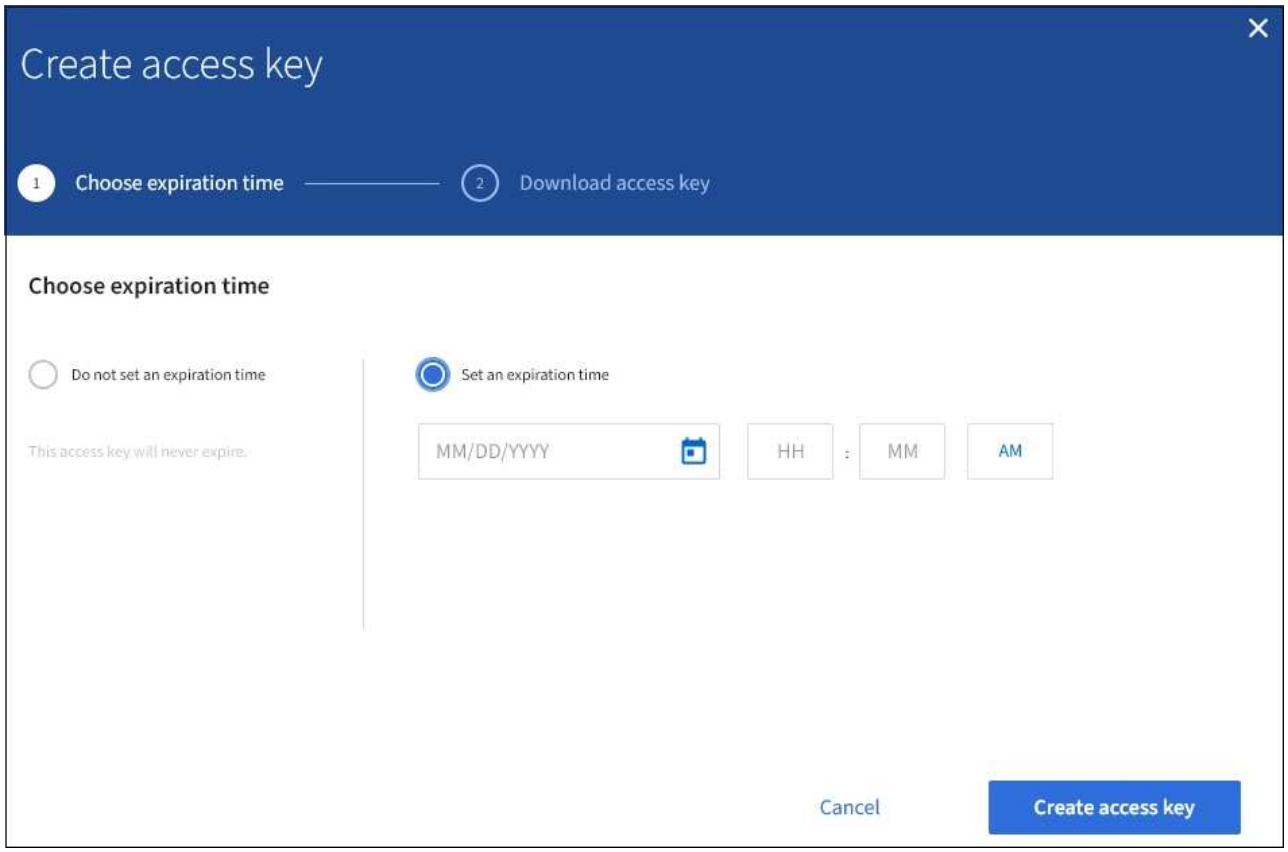
> 계정에 속한 S3 버킷 및 오브젝트는 테넌트 관리자에 계정에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.

   내 액세스 키 페이지가 나타나고 기존 액세스 키가 나열됩니다.

2. Create key * 를 선택합니다.
3. 다음 중 하나를 수행합니다.
   - 만료 시간을 설정하지 않음 * 을 선택하여 만료되지 않는 키를 생성합니다. (기본값)
   - 만료 시간 설정 * 을 선택하고 만료 날짜 및 시간을 설정합니다.

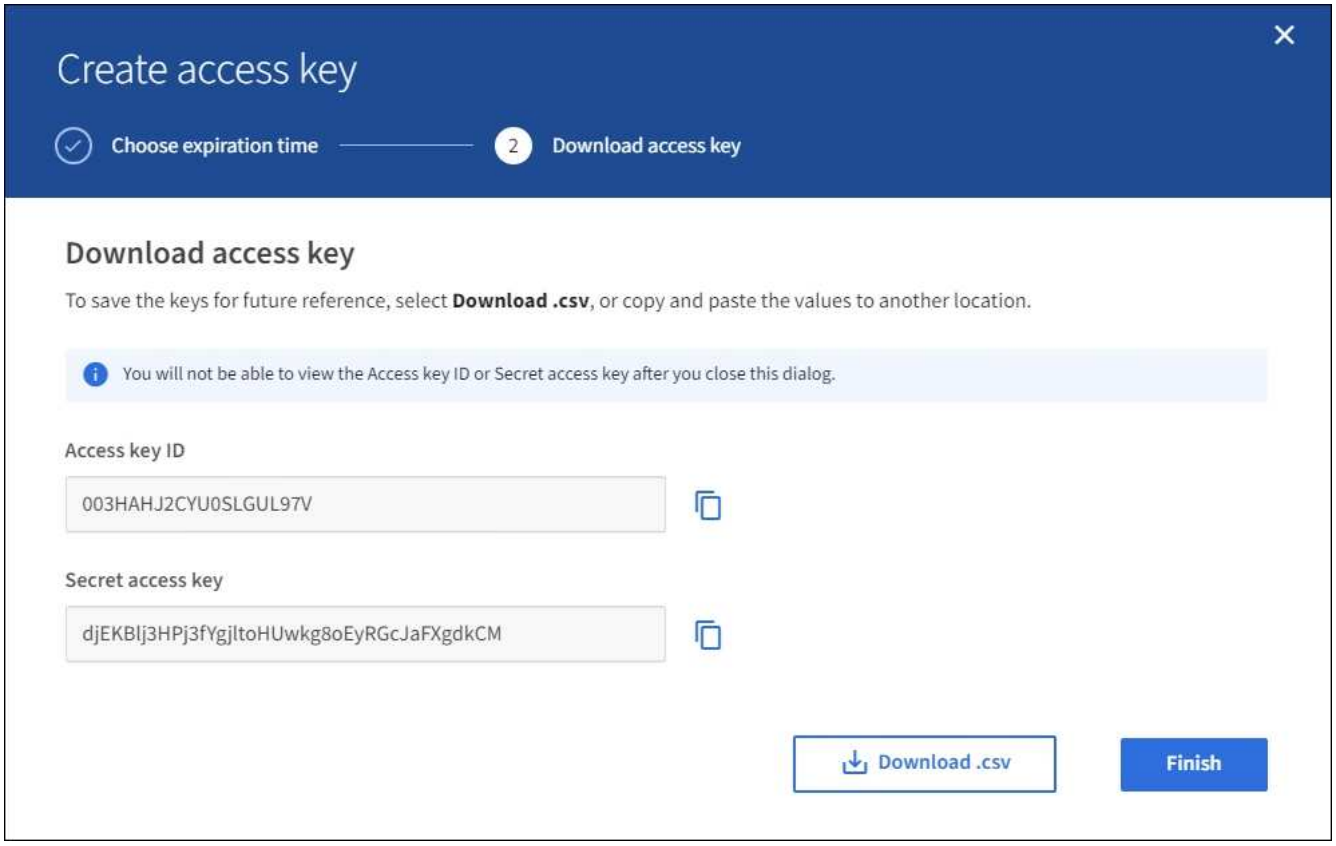


4. Create access key * 를 선택합니다.

   액세스 키 ID 및 비밀 액세스 키가 나열된 다운로드 액세스 키 대화 상자가 나타납니다.

5. 액세스 키 ID와 비밀 액세스 키를 안전한 위치에 복사하거나 * Download.csv * 를 선택하여 액세스 키 ID와 비밀 액세스 키가 포함된 스프레드시트 파일을 저장합니다.

   이 정보를 복사하거나 다운로드할 때까지 이 대화 상자를 닫지 마십시오. 대화 상자를 닫은 후에는 키를 복사하거나 다운로드할 수 없습니다.



6. 마침 * 을 선택합니다.

   새 키가 내 액세스 키 페이지에 나열됩니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

S3 액세스 키를 봅니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 S3 액세스 키 목록을 볼 수 있습니다. 만료 시간을 기준으로 목록을 정렬할 수 있으므로 곧 만료되는 키를 확인할 수 있습니다. 필요에 따라 새 키를 만들거나 더 이상 사용하지 않는 키를 삭제할 수 있습니다.

필요한 것

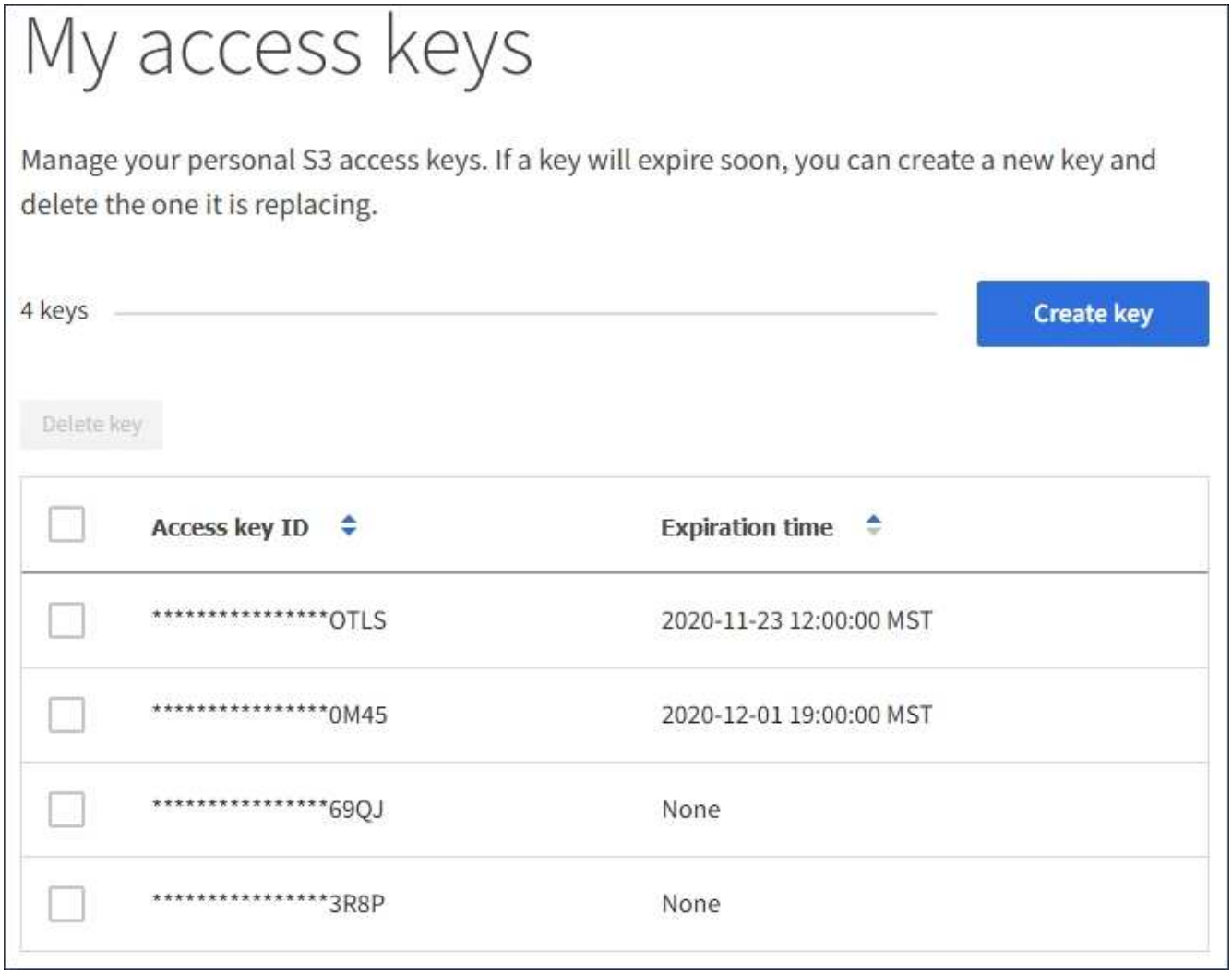
- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 자신의 S3 자격 증명 관리 권한이 있어야 합니다.

> 계정에 속한 S3 버킷 및 오브젝트는 테넌트 관리자에 계정에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.

   내 액세스 키 페이지가 나타나고 기존 액세스 키가 나열됩니다.



2. 키를 * Expiration Time * 또는 * Access key ID * 로 정렬합니다.
3. 필요에 따라 새 키를 만들고 더 이상 사용하지 않는 키를 수동으로 삭제합니다.

   기존 키가 만료되기 전에 새 키를 만들면 계정의 개체에 대한 액세스 권한을 일시적으로 잃지 않고 새 키를 사용할 수 있습니다.

   만료된 키는 자동으로 제거됩니다.

관련 정보

자체 S3 액세스 키를 생성합니다

자체 S3 액세스 키를 삭제합니다

자체 **S3** 액세스 키를 삭제합니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 자신의 S3 액세스 키를 삭제할 수 있습니다. 액세스 키가 삭제된 후에는 더 이상 테넌트 계정의 객체와 버킷에 액세스할 수 없습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

- 자신의 S3 자격 증명 관리 권한이 있어야 합니다. 을 참조하십시오 테넌트 관리 권한.

> 계정에 속한 S3 버킷 및 오브젝트는 테넌트 관리자에 계정에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

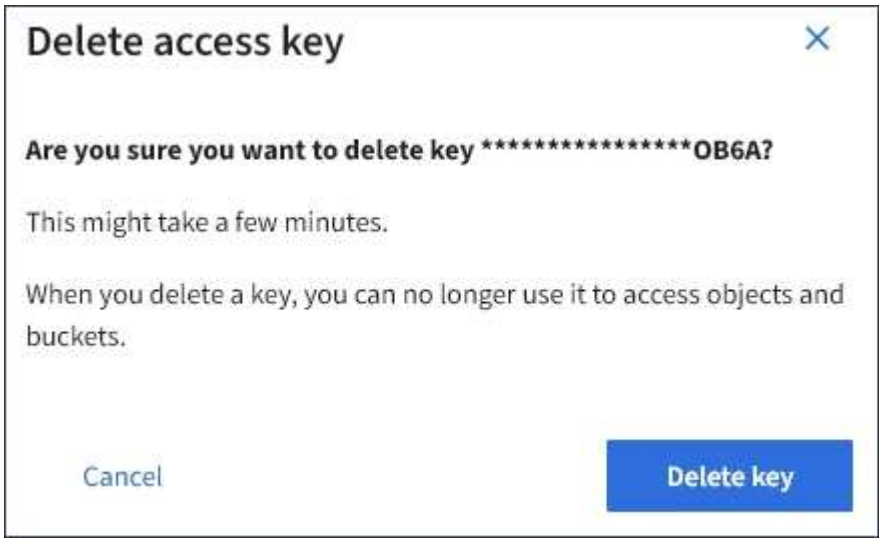
단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.

   내 액세스 키 페이지가 나타나고 기존 액세스 키가 나열됩니다.

2. 제거할 각 액세스 키에 대한 확인란을 선택합니다.
3. Delete key * 를 선택합니다.

   확인 대화 상자가 나타납니다.



4. Delete key * 를 선택합니다.

   페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

다른 사용자의 **S3** 액세스 키를 생성합니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 버킷 및 오브젝트에 액세스해야 하는 애플리케이션 같은 다른 사용자를 위한 S3 액세스 키를 생성할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있어야 합니다.

이 작업에 대해

하나 이상의 다른 사용자를 위한 S3 액세스 키를 생성하여 해당 테넌트 계정에 대한 버킷을 생성하고 관리할 수 있습니다. 새 액세스 키를 생성한 후 새 액세스 키 ID와 비밀 액세스 키로 응용 프로그램을 업데이트합니다. 보안을 위해

사용자 요구 사항보다 많은 키를 생성하지 말고 사용하지 않는 키를 삭제하십시오. 하나의 키만 있고 만료되려고 하는 경우 이전 키가 만료되기 전에 새 키를 만든 다음 이전 키를 삭제합니다.

각 키에는 특정 만료 시간 또는 만료 기간이 있을 수 있습니다. 만료 시간에 대한 다음 지침을 따르십시오.

- 키의 만료 시간을 설정하여 사용자의 액세스를 특정 기간으로 제한합니다. 만료 시간을 짧게 설정하면 액세스 키 ID 및 비밀 액세스 키가 실수로 노출될 경우 위험을 줄일 수 있습니다. 만료된 키는 자동으로 제거됩니다.
- 환경의 보안 위험이 낮으며 주기적으로 새 키를 만들 필요가 없는 경우 키의 만료 시간을 설정할 필요가 없습니다. 나중에 새 키를 만들려면 이전 키를 수동으로 삭제합니다.

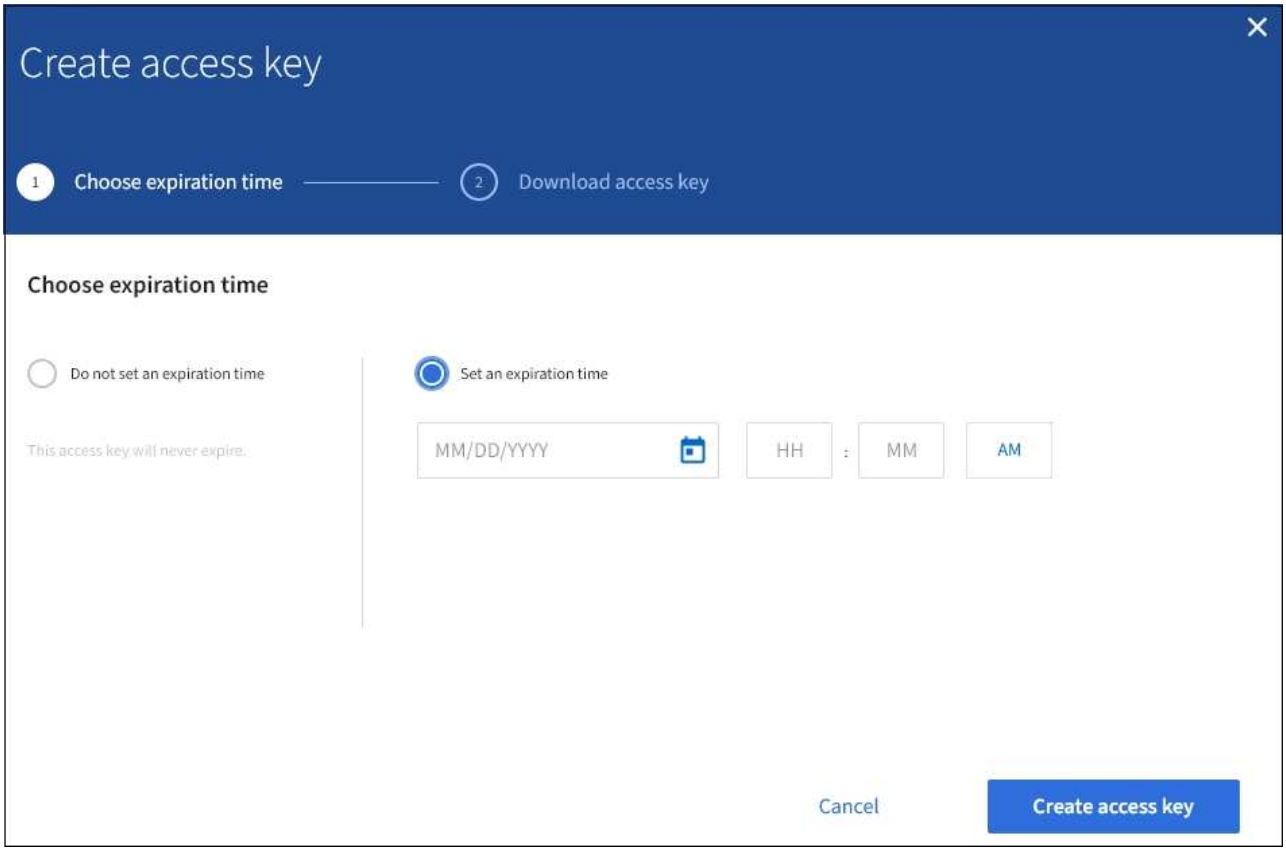
> 사용자에게 속한 S3 버킷 및 오브젝트는 테넌트 관리자에서 해당 사용자에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.
2. S3 액세스 키를 관리할 사용자를 선택합니다.

   사용자 세부 정보 페이지가 나타납니다.

3. 액세스 키 * 를 선택한 다음 * 키 만들기 * 를 선택합니다.
4. 다음 중 하나를 수행합니다.
   - 만료 시간을 설정하지 않음 * 을 선택하여 만료되지 않는 키를 생성합니다. (기본값)
   - 만료 시간 설정 * 을 선택하고 만료 날짜 및 시간을 설정합니다.

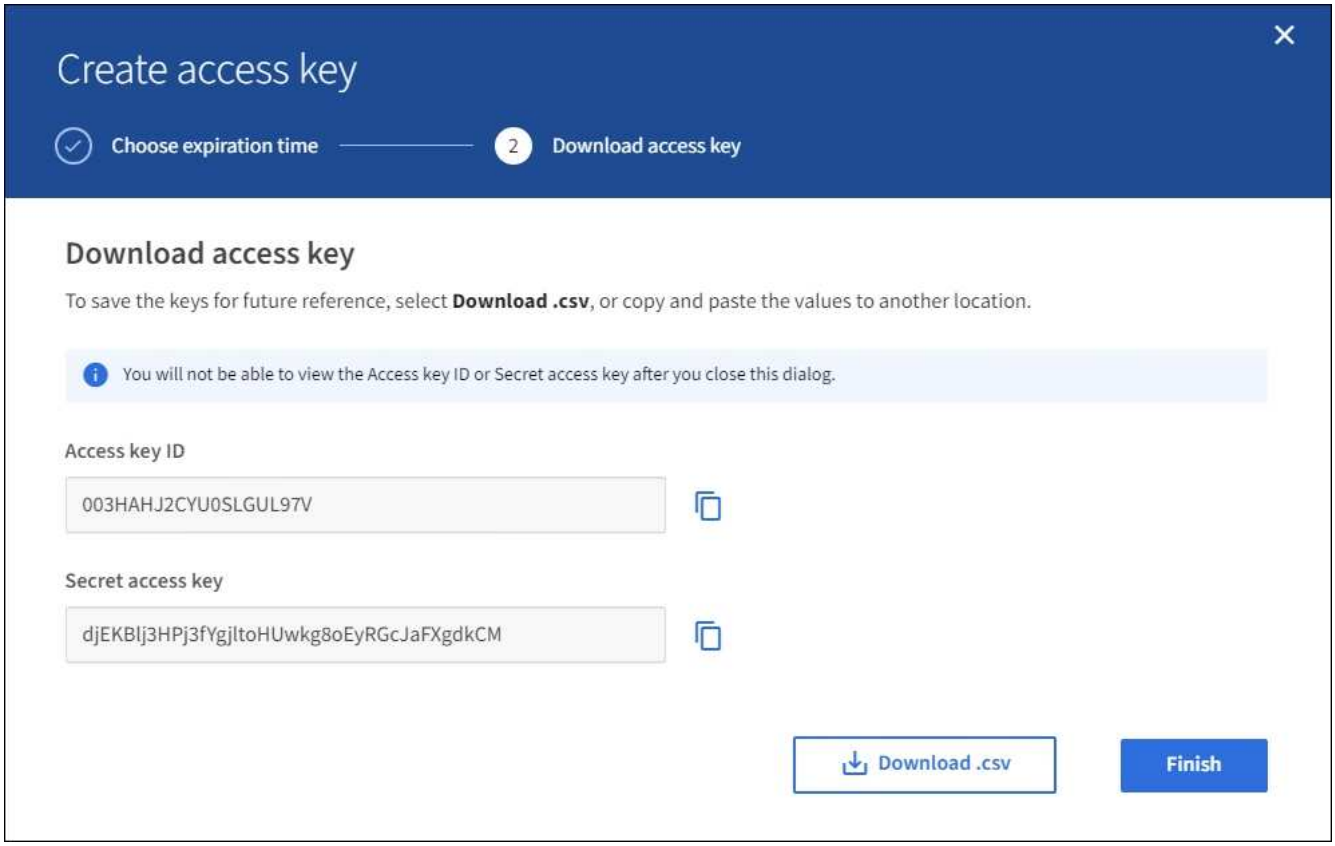


5. Create access key * 를 선택합니다.

   액세스 키 ID 및 비밀 액세스 키가 나열된 다운로드 액세스 키 대화 상자가 나타납니다.

6. 액세스 키 ID와 비밀 액세스 키를 안전한 위치에 복사하거나 * Download.csv * 를 선택하여 액세스 키 ID와 비밀 액세스 키가 포함된 스프레드시트 파일을 저장합니다.

   > 이 정보를 복사하거나 다운로드할 때까지 이 대화 상자를 닫지 마십시오. 대화 상자를 닫은 후에는 키를 복사하거나 다운로드할 수 없습니다.



7. 마침 * 을 선택합니다.

   새 키가 사용자 세부 정보 페이지의 액세스 키 탭에 나열됩니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

관련 정보

테넌트 관리 권한

다른 사용자의 **S3** 액세스 키를 봅니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 다른 사용자의 S3 액세스 키를 볼 수 있습니다. 만료 시간을 기준으로 목록을 정렬하면 곧 만료되는 키를 확인할 수 있습니다. 필요에 따라 새 키를 생성하고 더 이상 사용하지 않는 키를 삭제할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

- 루트 액세스 권한이 있어야 합니다.

> 사용자에게 속한 S3 버킷 및 오브젝트는 테넌트 관리자에서 해당 사용자에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

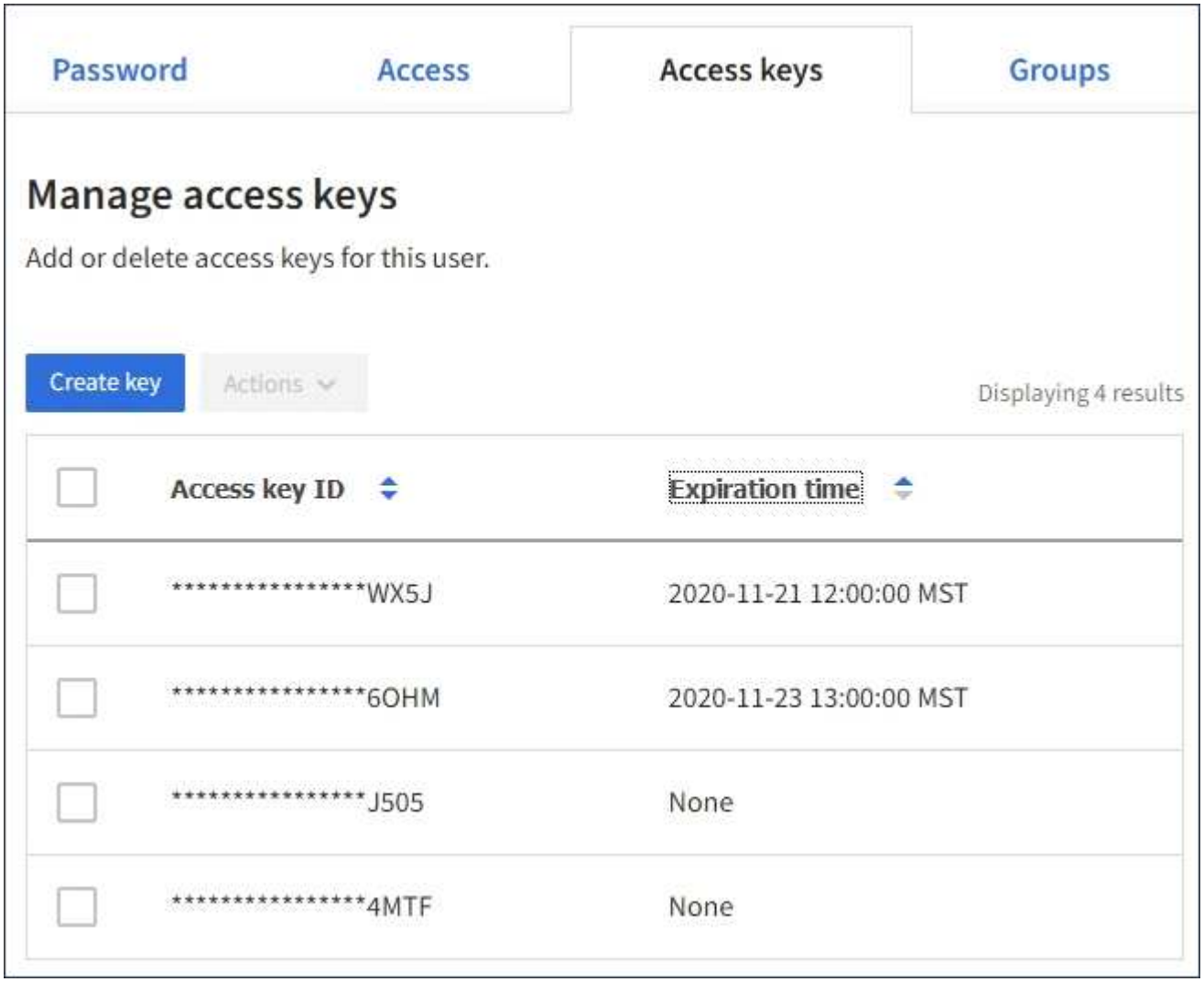
1. 액세스 관리 * > * 사용자 * 를 선택합니다.

   사용자 페이지가 나타나고 기존 사용자가 나열됩니다.

2. S3 액세스 키를 보려는 사용자를 선택합니다.

   사용자 세부 정보 페이지가 나타납니다.

3. 액세스 키 * 를 선택합니다.



4. 키를 * Expiration Time * 또는 * Access key ID * 로 정렬합니다.
5. 필요에 따라 새 키를 생성하고 에서 더 이상 사용하지 않는 키를 수동으로 삭제합니다.

기존 키가 만료되기 전에 새 키를 만들면 사용자는 계정의 개체에 대한 액세스 권한을 일시적으로 잃지 않고 새 키를 사용할 수 있습니다.

만료된 키는 자동으로 제거됩니다.

관련 정보

다른 사용자의 S3 액세스 키를 생성합니다

다른 사용자의 S3 액세스 키를 삭제합니다

다른 사용자의 **S3** 액세스 키를 삭제합니다

S3 테넌트를 사용하는 경우 적절한 권한이 있으면 다른 사용자의 S3 액세스 키를 삭제할 수 있습니다. 액세스 키가 삭제된 후에는 더 이상 테넌트 계정의 객체와 버킷에 액세스할 수 없습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있어야 합니다. 을 참조하십시오 테넌트 관리 권한.

> 사용자에게 속한 S3 버킷 및 오브젝트는 테넌트 관리자에서 해당 사용자에 대해 표시된 액세스 키 ID 및 비밀 액세스 키를 사용하여 액세스할 수 있습니다. 이러한 이유로 액세스 키를 암호로 보호해야 합니다. 액세스 키를 정기적으로 회전하고, 계정에서 사용되지 않는 키를 제거하며, 다른 사용자와 공유하지 마십시오.

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.

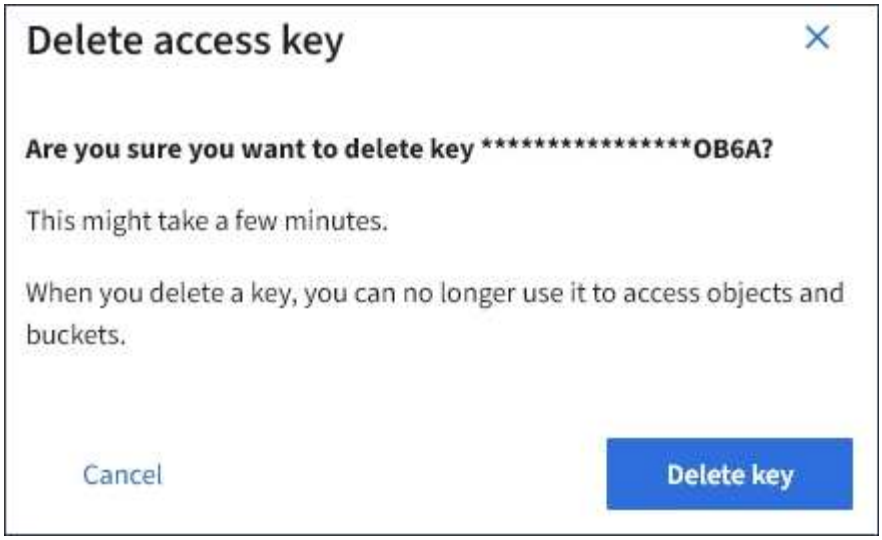
   사용자 페이지가 나타나고 기존 사용자가 나열됩니다.

2. S3 액세스 키를 관리할 사용자를 선택합니다.

   사용자 세부 정보 페이지가 나타납니다.

3. 액세스 키 * 를 선택한 다음 삭제할 각 액세스 키에 대한 확인란을 선택합니다.
4. Actions * > * Delete Selected key * 를 선택합니다.

   확인 대화 상자가 나타납니다.



5. Delete key * 를 선택합니다.

   페이지의 오른쪽 상단에 확인 메시지가 나타납니다. 캐시 때문에 변경사항을 적용하려면 15분이 소요될 수 있습니다.

S3 버킷을 관리합니다

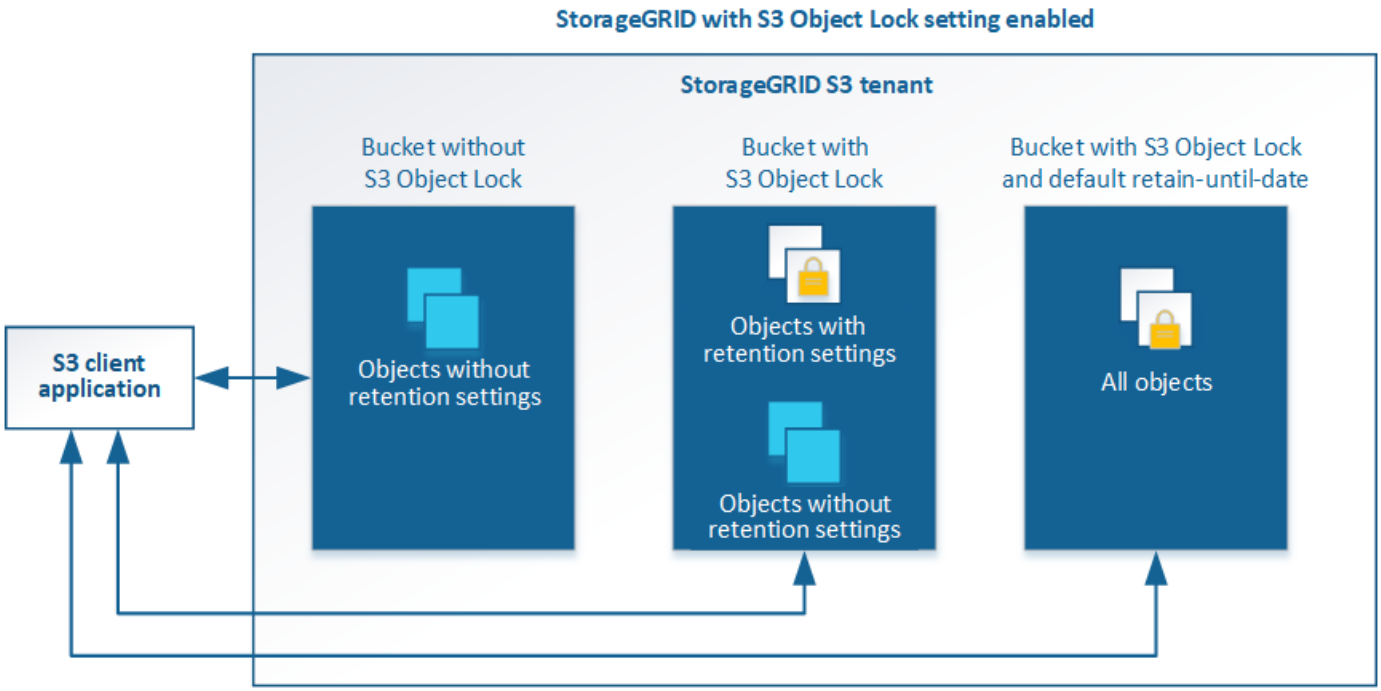
테넌트에 S3 오브젝트 잠금을 사용합니다

오브젝트가 보존 규정 요구사항을 충족해야 하는 경우 StorageGRID의 S3 오브젝트 잠금 기능을 사용할 수 있습니다.

S3 오브젝트 잠금이란 무엇입니까?

StorageGRID S3 오브젝트 잠금 기능은 Amazon S3(Amazon Simple Storage Service)의 S3 오브젝트 잠금과 동등한 오브젝트 보호 솔루션입니다.

그림에서 볼 수 있듯이 StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정을 사용하면 S3 테넌트 계정이 S3 오브젝트 잠금을 사용하거나 사용하지 않고 버킷을 생성할 수 있습니다. 버킷에 S3 오브젝트 잠금이 설정된 경우 S3 클라이언트 애플리케이션이 해당 버킷의 모든 오브젝트 버전에 대한 보존 설정을 선택적으로 지정할 수 있습니다. 오브젝트 버전에 S3 오브젝트 잠금으로 보호할 보존 설정이 지정되어 있어야 합니다.



StorageGRID S3 오브젝트 잠금 기능은 Amazon S3 규정 준수 모드에 상응하는 단일 보존 모드를 제공합니다. 기본적으로 보호된 개체 버전은 사용자가 덮어쓰거나 삭제할 수 없습니다. StorageGRID S3 오브젝트 잠금 기능은 거버넌스 모드를 지원하지 않으며, 특별한 권한이 있는 사용자가 보존 설정을 무시하거나 보호된 오브젝트를 삭제할 수 없습니다.

버킷에 S3 오브젝트 잠금이 활성화된 경우 오브젝트를 생성하거나 업데이트할 때 S3 클라이언트 애플리케이션에서 다음 오브젝트 레벨 보존 설정 중 하나 또는 모두를 선택적으로 지정할 수 있습니다.

- * Retain-until-date *: 개체 버전의 Retain-until-date가 미래인 경우 개체를 검색할 수 있지만 수정하거나 삭제할 수 없습니다. 필요에 따라 오브젝트의 보존 기간(Retain-until-date)을 늘릴 수 있지만 이 날짜는 줄일 수 없습니다.
- * 법적 증거 자료 보관 *: 개체 버전에 법적 증거 자료 보관 기능을 적용하면 해당 개체가 즉시 잠깁니다. 예를 들어 조사 또는 법적 분쟁과 관련된 객체에 법적 보류를 지정해야 할 수 있습니다. 법적 보류는 만료 날짜가 없지만 명시적으로 제거될 때까지 유지됩니다. 법적 보류는 보존 기한 과 무관합니다.

또한 가능합니다 버킷의 기본 보존 모드 및 기본 보존 기간을 지정합니다. 고유한 보존 설정을 지정하지 않는 버킷에 추가된 각 오브젝트에 적용됩니다.

이러한 설정에 대한 자세한 내용은 을 참조하십시오 S3 오브젝트 잠금을 사용합니다.

레거시 준수 버킷을 관리합니다

S3 오브젝트 잠금 기능은 이전 StorageGRID 버전에서 사용할 수 있었던 규정 준수 기능을 대체합니다. 이전 버전의 StorageGRID를 사용하여 준수 버킷을 생성한 경우 이러한 버켓의 설정을 계속 관리할 수 있지만, 더 이상 새로운 준수 버킷을 생성할 수 없습니다. 자세한 내용은 NetApp 기술 자료 문서를 참조하십시오.

"NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

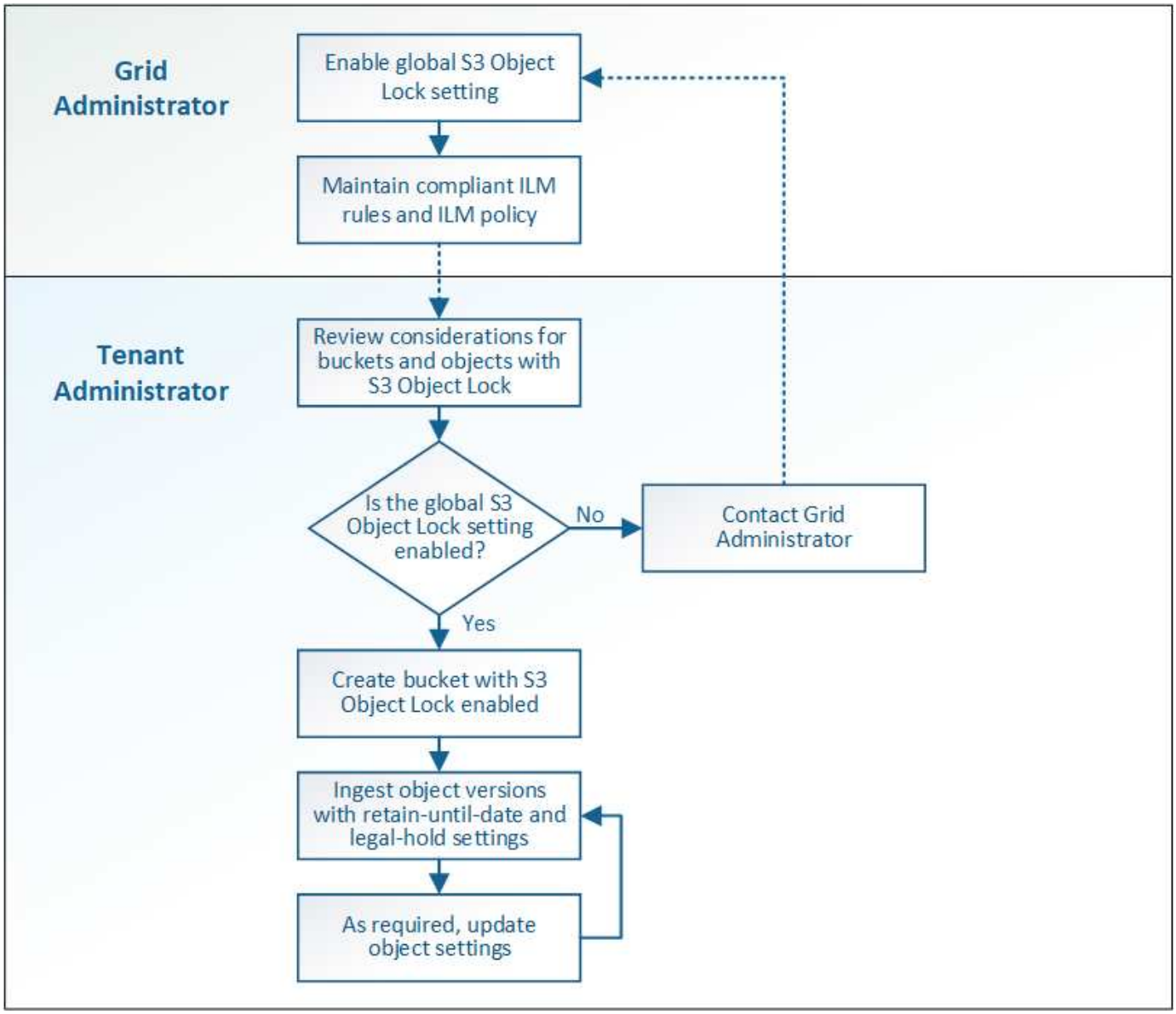
S3 오브젝트 잠금 워크플로

워크플로우 다이어그램은 StorageGRID에서 S3 오브젝트 잠금 기능을 사용하기 위한 상위 단계를 보여줍니다.

S3 오브젝트 잠금이 설정된 버킷을 생성하려면 그리드 관리자가 전체 StorageGRID 시스템에 대해 글로벌 S3

오브젝트 잠금 설정을 활성화해야 합니다. 또한 그리드 관리자는 을 확인해야 합니다 ILM(정보 수명 주기 관리) 정책 은(는) ""준수""입니다. S3 오브젝트 잠금이 활성화된 버킷의 요구 사항을 충족해야 합니다. 자세한 내용은 그리드 관리자에게 문의하거나 정보 수명 주기 관리를 사용하여 개체를 관리하는 지침을 참조하십시오.

글로벌 S3 오브젝트 잠금 설정을 활성화한 후 S3 오브젝트 잠금이 설정된 버킷을 생성할 수 있습니다. 그런 다음 S3 클라이언트 애플리케이션을 사용하여 필요에 따라 각 오브젝트 버전에 대한 보존 설정을 지정할 수 있습니다.



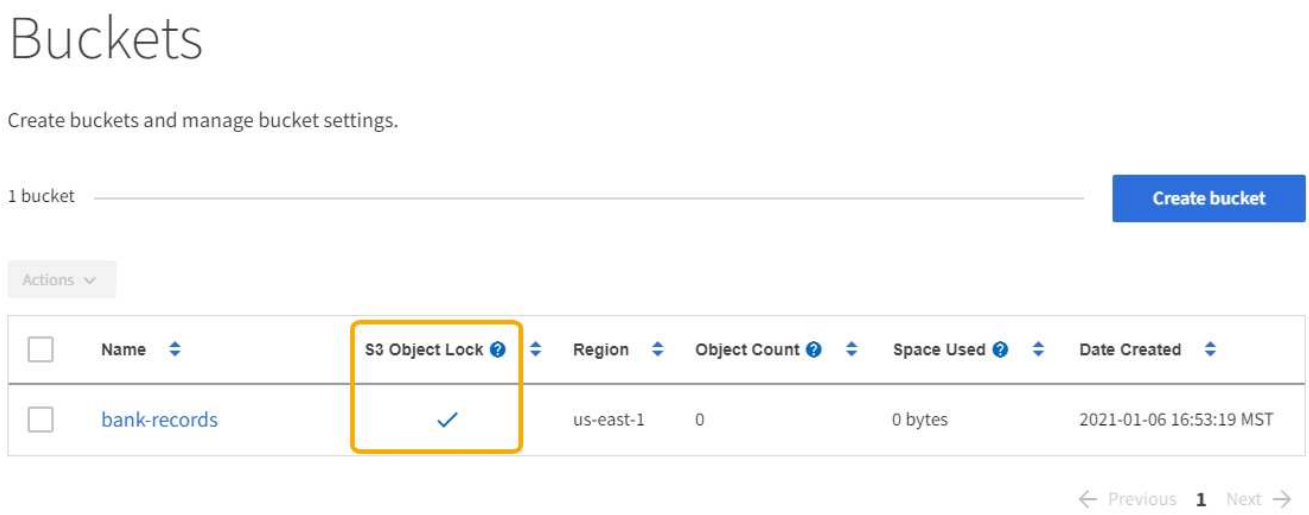
S3 오브젝트 잠금에 대한 요구사항

버킷에 대해 S3 오브젝트 잠금을 설정하기 전에 S3 오브젝트 잠금 버킷 및 오브젝트에 대한 요구사항과 S3 오브젝트 잠금이 활성화된 버킷에 포함된 오브젝트의 수명 주기를 검토하십시오.

S3 오브젝트 잠금이 설정된 버킷의 요구 사항

- StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 테넌트 관리자, 테넌트 관리 API 또는 S3 REST API를 사용하여 S3 오브젝트 잠금이 활성화된 버킷을 생성할 수 있습니다.

  테넌트 관리자의 이 예에서는 S3 오브젝트 잠금이 설정된 버킷을 보여 줍니다.



- S3 오브젝트 잠금을 사용하려는 경우 버킷을 생성할 때 S3 오브젝트 잠금을 활성화해야 합니다. 기존 버킷에 대해 S3 오브젝트 잠금을 활성화할 수 없습니다.
- S3 오브젝트 잠금에서 버킷 버전 관리가 필요합니다. 버킷에 대해 S3 오브젝트 잠금이 활성화된 경우 StorageGRID는 해당 버킷의 버전 관리를 자동으로 활성화합니다.
- S3 오브젝트 잠금이 설정된 버킷을 생성한 후에는 해당 버켓에 대한 S3 오브젝트 잠금을 비활성화하거나 버전 관리를 일시 중단할 수 없습니다.
- 필요에 따라 버킷의 기본 보존을 구성할 수 있습니다. 개체 버전이 업로드되면 기본 보존 기간이 개체 버전에 적용됩니다. 객체 버전 업로드 요청에 보존 모드와 보존 기간을 지정하여 버킷 기본값을 재정의할 수 있습니다.
- S3 오브젝트 라이프사이클 버킷에 대해 버킷 라이프사이클 구성이 지원됩니다.
- S3 오브젝트 잠금이 설정된 버킷에는 CloudMirror 복제가 지원되지 않습니다.

S3 오브젝트 잠금이 설정된 버킷의 오브젝트 요구사항

- 오브젝트 버전을 보호하려면 S3 클라이언트 애플리케이션이 버킷 기본 보존을 구성하거나 각 업로드 요청에서 보존 설정을 지정해야 합니다.
- 개체 버전에 대한 보존 기간을 늘릴 수 있지만 이 값을 줄일 수는 없습니다.
- 법적 조치 또는 규제 조사가 보류 중인 경우 개체 버전에 법적 증거 자료를 두어 관련 정보를 보존할 수 있습니다. 개체 버전이 법적 증거 자료 보관 중인 경우, 해당 개체가 보존 기한 에 도달한 경우에도 StorageGRID에서 해당 개체를 삭제할 수 없습니다. 법적 증거 자료 보관 기간이 해제됨과 동시에, 보존 기한이 만료된 경우 개체 버전을 삭제할 수 있습니다.
- S3 오브젝트 잠금에는 버전 관리되는 버킷을 사용해야 합니다. 보존 설정은 개별 개체 버전에 적용됩니다. 개체 버전에는 보존 기한 및 법적 보류 설정이 둘 다 있을 수 있으며, 둘 중 하나만 설정할 수도 있고 둘 다 가질 수도 없습니다. 개체에 대한 보존 기한 또는 법적 보류 설정을 지정하면 요청에 지정된 버전만 보호됩니다. 이전 버전의 개체는 잠겨 있는 상태에서 새 버전의 개체를 만들 수 있습니다.

S3 오브젝트 잠금이 설정된 버킷의 오브젝트 라이프사이클

S3 오브젝트 잠금이 설정된 버킷에 저장된 각 오브젝트는 다음 3단계를 거칩니다.

1. * 오브젝트 수집 *
    - S3 오브젝트 잠금이 설정된 버킷에 오브젝트 버전을 추가할 경우 S3 클라이언트 애플리케이션이 오브젝트에 대한 보존 설정을 선택적으로 지정할 수 있습니다(보존 기한, 법적 보류 또는 둘 다). 그런 다음

StorageGRID에서는 해당 개체의 메타데이터를 생성하며 고유한 UUID(Object Identifier)와 수집 날짜 및 시간이 포함됩니다.

- 보존 설정이 포함된 오브젝트 버전을 수집하면 해당 데이터와 S3 사용자 정의 메타데이터를 수정할 수 없습니다.
- StorageGRID는 오브젝트 메타데이터를 오브젝트 데이터와 독립적으로 저장합니다. 이 기능은 각 사이트에서 모든 오브젝트 메타데이터의 복사본을 3개 유지 관리합니다.

2. * 개체 보존 *
   - 개체의 여러 복사본이 StorageGRID에 저장됩니다. 정확한 복제본 수와 유형 및 스토리지 위치는 활성 ILM 정책의 규정 준수 규칙에 따라 결정됩니다.
3. * 개체 삭제 *
   - 보존 기한 에 도달하면 개체를 삭제할 수 있습니다.
   - 법적 증거 자료 보관 중인 개체는 삭제할 수 없습니다.

S3 버킷을 생성합니다

테넌트 관리자를 사용하여 오브젝트 데이터용 S3 버킷을 생성할 수 있습니다. 버킷을 생성할 때 버킷의 이름과 영역을 지정해야 합니다. StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 버킷에 대해 S3 오브젝트 잠금을 선택적으로 활성화할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해 있습니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

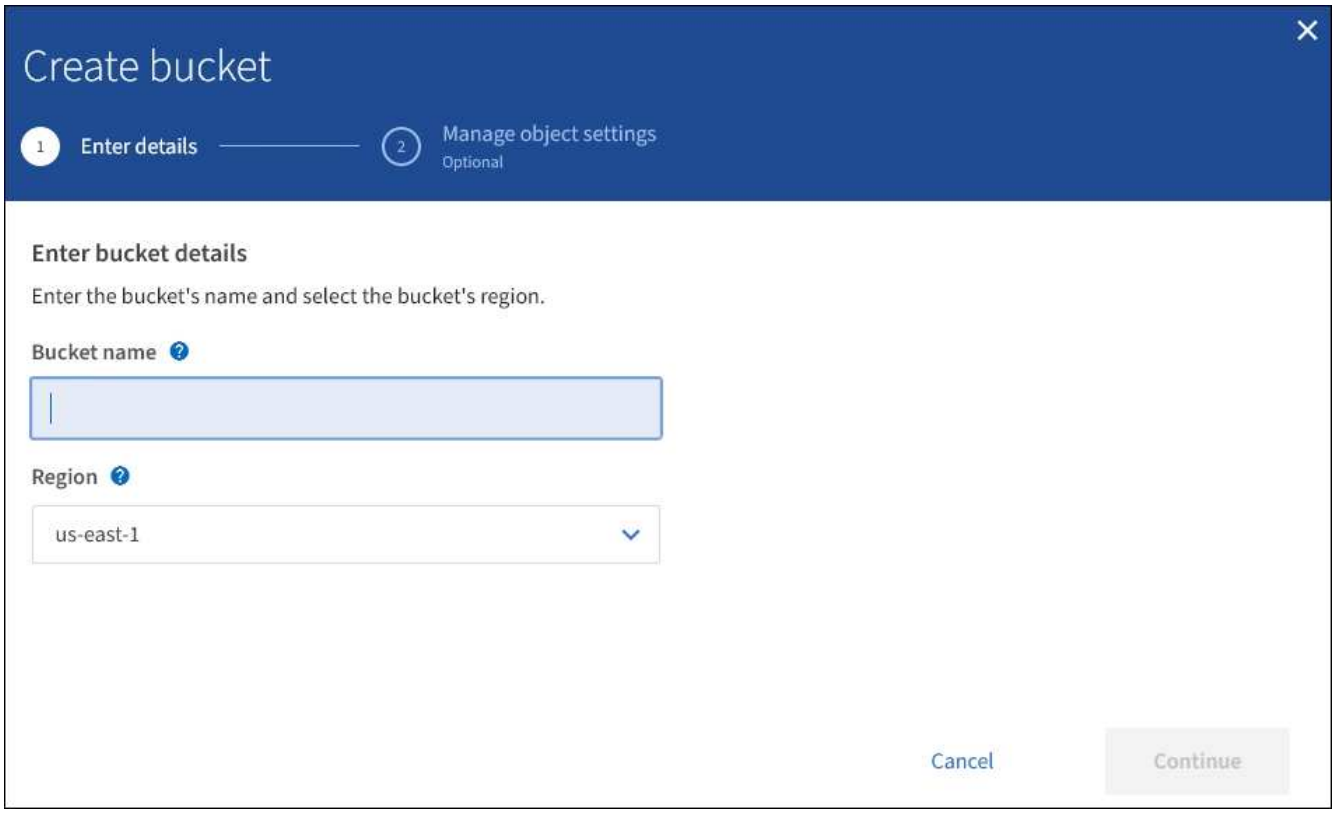
> 에서 버킷 또는 오브젝트의 S3 오브젝트 잠금 속성을 설정하거나 수정하는 권한을 부여할 수 있습니다 버킷 정책 또는 그룹 정책.

- S3 오브젝트 잠금을 사용하여 버킷을 생성하려는 경우 StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정을 활성화하고 S3 오브젝트 잠금 버킷 및 오브젝트에 대한 요구사항을 검토했습니다.

  S3 오브젝트 잠금을 사용합니다

단계

1. 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. Create bucket * 을 선택합니다.



3. 버킷의 고유한 이름을 입력하십시오.

> 버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

버킷 이름은 다음 규칙을 준수해야 합니다.

- 각 StorageGRID 시스템에서 고유해야 합니다(테넌트 계정에서만 고유한 것은 아님).
- DNS를 준수해야 합니다.
- 3자 이상 63자 이하여야 합니다.
- 각 레이블은 소문자 또는 숫자로 시작하고 끝나야 하며 소문자, 숫자 및 하이픈만 사용할 수 있습니다.
- 가상 호스팅 스타일 요청에서 기간을 사용하지 않아야 합니다. 마침표는 서버 와일드카드 인증서 확인에 문제를 일으킬 수 있습니다.

> 자세한 내용은 를 참조하십시오 "버킷 명명 규칙에 대한 AWS(Amazon Web Services) 문서입니다".

4. 이 버킷의 영역을 선택합니다.

StorageGRID 관리자가 사용 가능한 영역을 관리합니다. 버킷 영역은 오브젝트에 적용되는 데이터 보호 정책에 영향을 미칠 수 있습니다. 기본적으로 모든 버킷은 us-east-1 영역에 생성됩니다.

> 버킷을 생성한 후에는 지역을 변경할 수 없습니다.

5. Continue * 를 선택합니다.
6. 필요한 경우 버킷에 대한 오브젝트 버전 관리를 활성화합니다.

이 버킷에 각 오브젝트의 모든 버전을 저장하려면 오브젝트 버전 관리를 활성화하십시오. 그런 다음 필요에 따라 개체의 이전 버전을 검색할 수 있습니다.

7. S3 오브젝트 잠금 섹션이 나타나면 버킷에 대해 S3 오브젝트 잠금을 선택적으로 활성화합니다.

   > 버킷을 생성한 후에는 S3 오브젝트 잠금을 설정하거나 해제할 수 없습니다.

   S3 오브젝트 잠금 섹션은 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우에만 나타납니다.

   S3 클라이언트 애플리케이션이 버킷에 추가된 오브젝트에 대한 보관 종료 날짜 및 법적 보류 설정을 지정하려면 먼저 버킷에 대해 S3 오브젝트 잠금을 활성화해야 합니다.

   버킷에 대해 S3 오브젝트 잠금을 설정하면 버킷 버전 관리가 자동으로 활성화됩니다. 또한 가능합니다 버킷의 기본 보존 모드 및 기본 보존 기간을 지정합니다 고유한 보존 설정을 지정하지 않는 버킷에 수집된 각 개체에 적용됩니다.

8. Create bucket * 을 선택합니다.

   버킷이 생성되어 버킷 페이지의 테이블에 추가됩니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

테넌트 관리 API 이해

S3을 사용합니다

S3 버킷 세부 정보를 봅니다

테넌트 계정에서 버킷 및 버킷 설정 목록을 볼 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

단계

1. 스토리지(S3) * > * 버킷 * 을 선택합니다.

   Bucket 페이지가 나타나고 테넌트 계정에 대한 모든 버킷이 나열됩니다.

2. 각 버킷에 대한 정보를 검토합니다.

   필요에 따라 모든 열을 기준으로 정보를 정렬하거나 목록 앞뒤에 페이지를 표시할 수 있습니다.

   - 이름: 변경할 수 없는 버킷의 고유 이름입니다.
   - S3 오브젝트 잠금: 이 버킷에 대해 S3 오브젝트 잠금이 설정되었는지 여부.

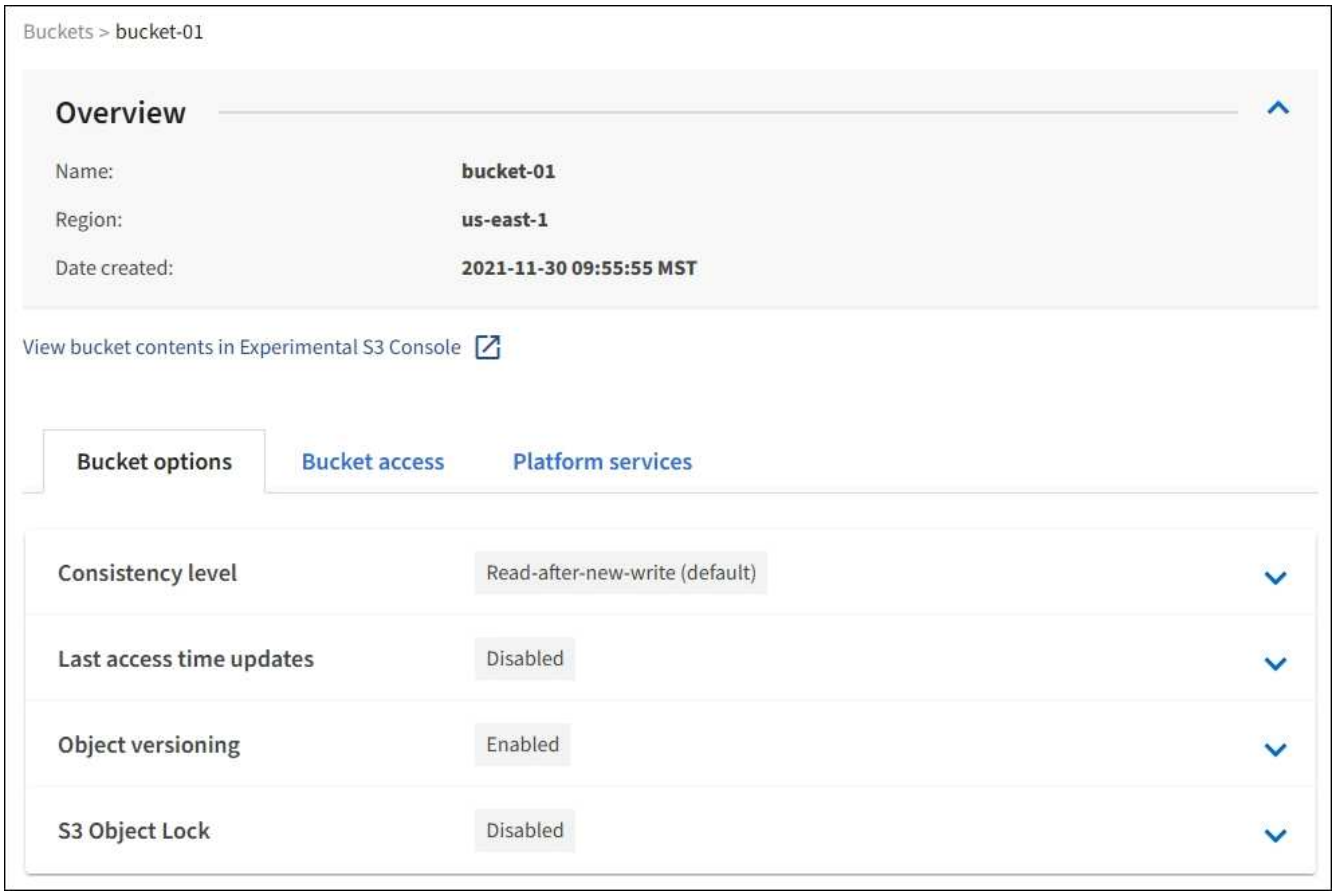
     전역 S3 오브젝트 잠금 설정이 비활성화된 경우 이 열은 표시되지 않습니다. 또한 이 열에는 레거시 준수 버킷에 대한 정보도 표시됩니다.

   - 지역: 변경할 수 없는 버킷의 영역입니다.
   - 개체 수: 이 버킷의 오브젝트 수입니다.
   - 사용된 공간: 이 버킷에 있는 모든 오브젝트의 논리적 크기입니다. 논리적 크기에는 복제 또는 삭제 코딩 복사본 또는 오브젝트 메타데이터에 필요한 실제 공간이 포함되지 않습니다.
   - 만든 날짜: 버킷을 만든 날짜 및 시간입니다.

   > 표시된 개체 수와 사용된 공간 값은 추정값입니다. 이러한 추정치는 베스트 타이밍, 네트워크 연결 및 노드 상태의 영향을 받습니다. 버킷에 버전 관리가 활성화된 경우 삭제된 개체 버전은 오브젝트 수에 포함됩니다.

3. 버킷의 설정을 보고 관리하려면 버킷 이름을 선택합니다.

   버킷 세부 정보 페이지에서는 버킷 옵션, 버킷 액세스 및 에 대한 설정을 보고 편집할 수 있습니다 플랫폼 서비스.



정합성 보장 수준을 변경합니다

S3 테넌트를 사용하는 경우 테넌트 관리자 또는 테넌트 관리 API를 사용하여 S3 버킷의 오브젝트에 대해 수행된 작업의 정합성 제어를 변경할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다. 을 참조하십시오 테넌트 관리 권한.

이 작업에 대해

정합성 보장 레벨은 오브젝트의 가용성과 서로 다른 스토리지 노드 및 사이트에서 이러한 오브젝트의 일관성 간의 균형을 제공합니다. 일반적으로 버킷에 대해 * Read-After-new-write * 정합성 수준을 사용해야 합니다.

새 쓰기 후 읽기 * 정합성 보장 레벨이 클라이언트 애플리케이션의 요구 사항을 충족하지 않는 경우 버킷 정합성 수준을 설정하거나 을 사용하여 정합성 보장 레벨을 변경할 수 있습니다 `Consistency-Control` 머리글. 를 클릭합니다 `Consistency-Control` 헤더는 버킷 정합성 레벨을 오버라이드합니다.

> 버킷의 정합성 수준을 변경하면 변경 후 수집된 객체만 수정된 레벨에 맞게 보장됩니다.

단계

1. 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. 목록에서 버킷 이름을 선택합니다.

버킷 세부 정보 페이지가 나타납니다.

3. 버킷 옵션 * > * 정합성 보장 레벨 * 을 선택합니다.
4. 이 버킷의 오브젝트에 대해 수행된 작업의 정합성 수준을 선택합니다.
   - * 모두 *: 최고 수준의 일관성을 제공합니다. 모든 노드가 데이터를 즉시 수신하거나 요청이 실패합니다.
   - * 강력한 글로벌 *: 모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
   - * 강력한 사이트 *: 사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
   - * Read-After-new-write * (기본값): 새 객체에 대해 읽기-쓰기 후 정합성을 보장하고 객체 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 필요에 따라 만 사용하십시오(예: 거의 읽지 않는 로그 값이 포함된 버킷의 경우 또는 존재하지 않는 키의 헤드 또는 GET 작업의 경우). S3 FabricPool 버킷은 지원되지 않습니다.
5. 변경 내용 저장 * 을 선택합니다.

마지막 액세스 시간 업데이트를 사용하거나 사용하지 않도록 설정합니다

그리드 관리자가 StorageGRID 시스템에 대한 ILM(정보 수명 주기 관리) 규칙을 만들 때 오브젝트의 마지막 액세스 시간을 사용하여 해당 오브젝트를 다른 스토리지 위치로 이동할지 여부를 결정하도록 선택적으로 지정할 수 있습니다. S3 테넌트를 사용하는 경우 S3 버킷의 오브젝트에 대한 마지막 액세스 시간 업데이트를 활성화하여 이러한 규칙을 활용할 수 있습니다.

이 지침은 배치 지침에서 * Last Access Time * 옵션을 사용하는 ILM 규칙을 하나 이상 포함하는 StorageGRID 시스템에만 적용됩니다. StorageGRID 시스템에 이러한 규칙이 포함되어 있지 않으면 이 지침을 무시할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다. 을 참조하십시오 테넌트 관리 권한.
- 마지막 액세스 시간 * 은 ILM 규칙에 대한 * 참조 시간 * 배치 명령에 사용할 수 있는 옵션 중 하나입니다. 규칙의 참조 시간을 마지막 액세스 시간으로 설정하면 그리드 관리자는 해당 개체를 마지막으로 검색한 시기(읽기 또는 보기)에 따라 특정 저장소 위치에 개체가 배치되도록 지정할 수 있습니다.

예를 들어, 최근에 본 오브젝트를 더 빠른 스토리지에 유지하기 위해 그리드 관리자는 다음을 지정하는 ILM 규칙을 생성할 수 있습니다.

- 지난 달 동안 검색된 객체는 로컬 스토리지 노드에 남아 있어야 합니다.
- 지난 달에 검색되지 않은 객체는 오프 사이트 위치로 이동해야 합니다.

> 정보 수명 주기 관리를 사용하여 개체를 관리하는 방법에 대한 지침을 참조하십시오.

기본적으로 마지막 액세스 시간에 대한 업데이트는 사용되지 않습니다. StorageGRID 시스템에 * Last Access Time * 옵션을 사용하는 ILM 규칙이 포함되어 있고 이 옵션이 이 버킷의 오브젝트에 적용되도록 하려면 해당 규칙에 지정된 S3 버킷에 대한 마지막 액세스 시간에 대한 업데이트를 활성화해야 합니다.

개체가 검색될 때 마지막 액세스 시간을 업데이트하면 특히 작은 개체의 StorageGRID 성능이 저하될 수 있습니다.

StorageGRID는 객체가 검색될 때마다 다음 추가 단계를 수행해야 하므로 마지막 액세스 시간 업데이트 시 성능 영향이 발생합니다.

- 객체를 새 타임스탬프로 업데이트합니다
- ILM 대기열에 개체를 추가하여 현재 ILM 규칙 및 정책에 대해 다시 평가할 수 있습니다

이 표에는 마지막 액세스 시간이 비활성화되거나 활성화될 때 버킷의 모든 오브젝트에 적용되는 동작이 요약되어 있습니다.

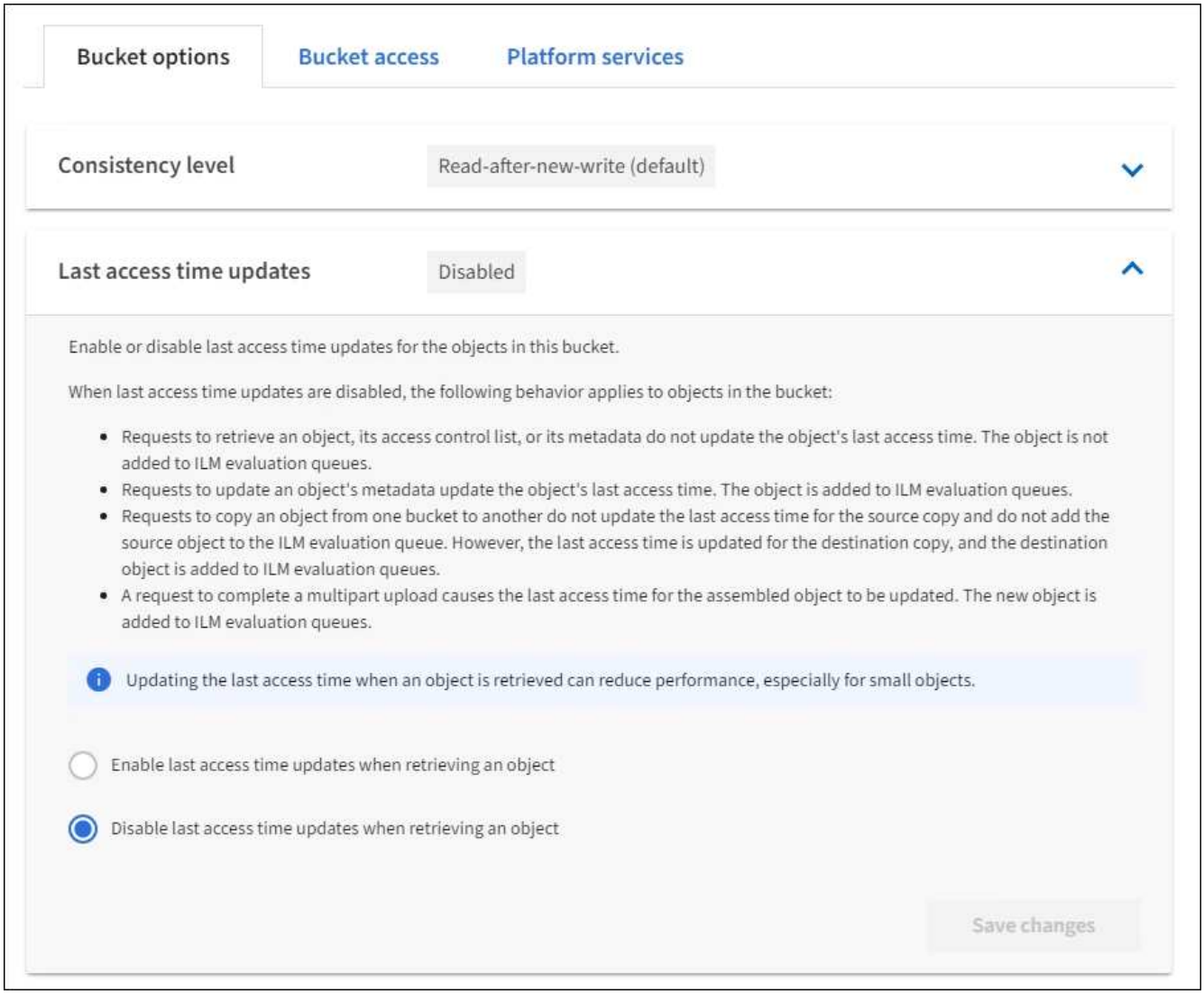
요청 유형입니다	마지막 액세스 시간이 비활성화된 경우의 동작(기본값)		마지막 액세스 시간이 설정된 경우의 동작	
	마지막 액세스 시간이 업데이트되었습니까?	ILM 평가 대기열에 객체가 추가되었습니까?	마지막 액세스 시간이 업데이트되었습니까?	ILM 평가 대기열에 객체가 추가되었습니까?
개체, 해당 액세스 제어 목록 또는 해당 메타데이터를 검색하는 요청입니다	아니요	아니요	예	예
개체의 메타데이터를 업데이트하도록 요청합니다	예	예	예	예
한 버킷에서 다른 버킷으로 오브젝트 복사 요청	• 아니요, 소스 복제본입니다 • 예, 대상 복사본에 대해 입니다	• 아니요, 소스 복제본입니다 • 예, 대상 복사본에 대해 입니다	• 예. 소스 복제본에 대해 가능합니다 • 예, 대상 복사본에 대해 입니다	• 예. 소스 복제본에 대해 가능합니다 • 예, 대상 복사본에 대해 입니다
여러 부분 업로드를 완료하도록 요청합니다	예. 조립된 개체에 대해 가능합니다	예. 조립된 개체에 대해 가능합니다	예. 조립된 개체에 대해 가능합니다	예. 조립된 개체에 대해 가능합니다

단계

1. 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. 목록에서 버킷 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

3. Bucket options * > * Last access time updates * 를 선택합니다.
4. 마지막 액세스 시간 업데이트를 활성화하거나 비활성화하려면 해당 라디오 버튼을 선택합니다.



5. 변경 내용 저장 * 을 선택합니다.

관련 정보

테넌트 관리 권한

ILM을 사용하여 개체를 관리합니다

버킷의 오브젝트 버전 관리를 변경합니다

S3 테넌트를 사용하는 경우 테넌트 관리자 또는 테넌트 관리 API를 사용하여 S3 버킷의 버전 관리 상태를 변경할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해 있습니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

  테넌트 관리 권한

이 작업에 대해

버킷에 대한 오브젝트 버전 관리를 설정하거나 일시 중지할 수 있습니다. 버켓에 대한 버전 관리를 활성화한 후에는 버전이 지정되지 않은 상태로 돌아갈 수 없습니다. 그러나 버킷의 버전 관리를 일시 중단할 수 있습니다.

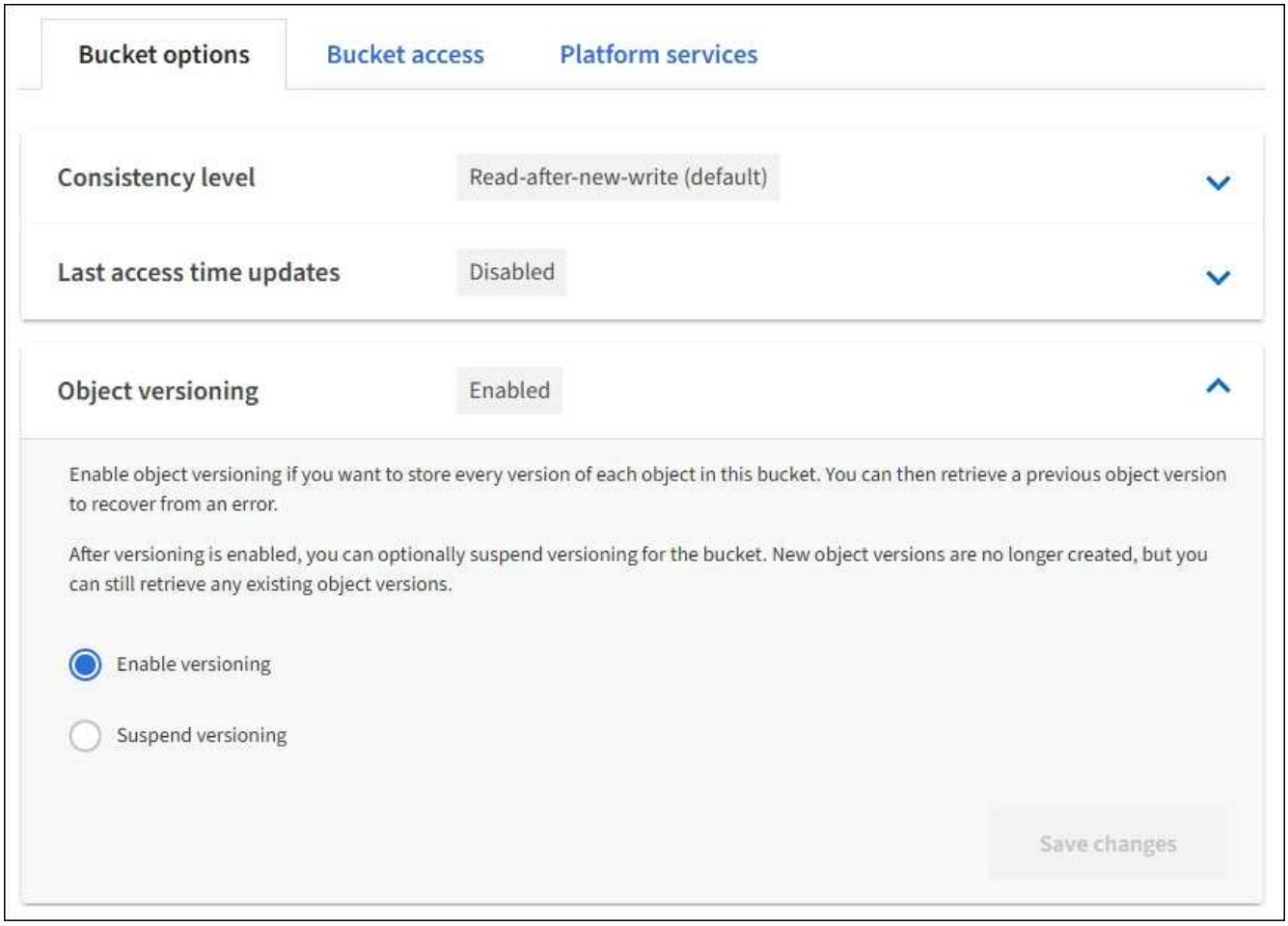
- 사용 안 함: 버전 관리가 활성화되지 않았습니다
- 사용: 버전 관리가 활성화됩니다
- 일시 중단됨: 버전 관리가 이전에 활성화되었으며 일시 중단되었습니다

S3 오브젝트 버전 관리

S3 버전 오브젝트 ILM 규칙 및 정책(예 4)

단계

1. 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. 목록에서 버킷 이름을 선택합니다.
3. 버킷 옵션 * > * 오브젝트 버전 관리 * 를 선택합니다.



4. 이 버킷의 오브젝트에 대한 버전 관리 상태를 선택합니다.

> S3 오브젝트 잠금 또는 레거시 규정 준수를 활성화하면 * 오브젝트 버전 관리 * 옵션이 비활성화됩니다.

옵션을 선택합니다	설명
버전 관리를 활성화합니다	이 버킷에 각 오브젝트의 모든 버전을 저장하려면 오브젝트 버전 관리를 활성화하십시오. 그런 다음 필요에 따라 개체의 이전 버전을 검색할 수 있습니다. 버킷에 이미 있던 객체는 사용자가 수정할 때 버전이 적용됩니다.
버전 관리를 일시 중단합니다	새 개체 버전을 더 이상 만들지 않으려면 개체 버전 관리를 일시 중단합니다. 기존 개체 버전을 검색할 수 있습니다.

5. 변경 내용 저장 * 을 선택합니다.

CORS(Cross-Origin Resource Sharing) 구성

다른 도메인의 웹 애플리케이션에서 해당 버킷의 버킷 및 오브젝트에 액세스할 수 있도록 하려면 S3 버킷에 대해 CORS(Cross-Origin Resource Sharing)를 구성할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

이 작업에 대해

CORS(Cross-Origin Resource Sharing)는 한 도메인의 클라이언트 웹 애플리케이션이 다른 도메인의 리소스에 액세스할 수 있도록 하는 보안 메커니즘입니다. 예를 들어, 그래픽을 저장하기 위해 "이미지"라는 S3 버킷을 사용한다고 가정합니다. 영상물통용 CORS를 구성하여 해당 버켓의 영상을 웹사이트 http://www.example.com` 에 표시할 수 있습니다.

단계

1. 텍스트 편집기를 사용하여 CORS를 활성화하는 데 필요한 XML을 만듭니다.

   이 예에서는 S3 버킷에 대해 CORS를 활성화하는 데 사용되는 XML을 보여 줍니다. 이 XML을 사용하면 모든 도메인이 버킷에 GET 요청을 보낼 수 있지만 "http://www.example.com` 도메인에서만 POST 및 삭제 요청을 보낼 수 있습니다. 모든 요청 헤더가 허용됩니다.

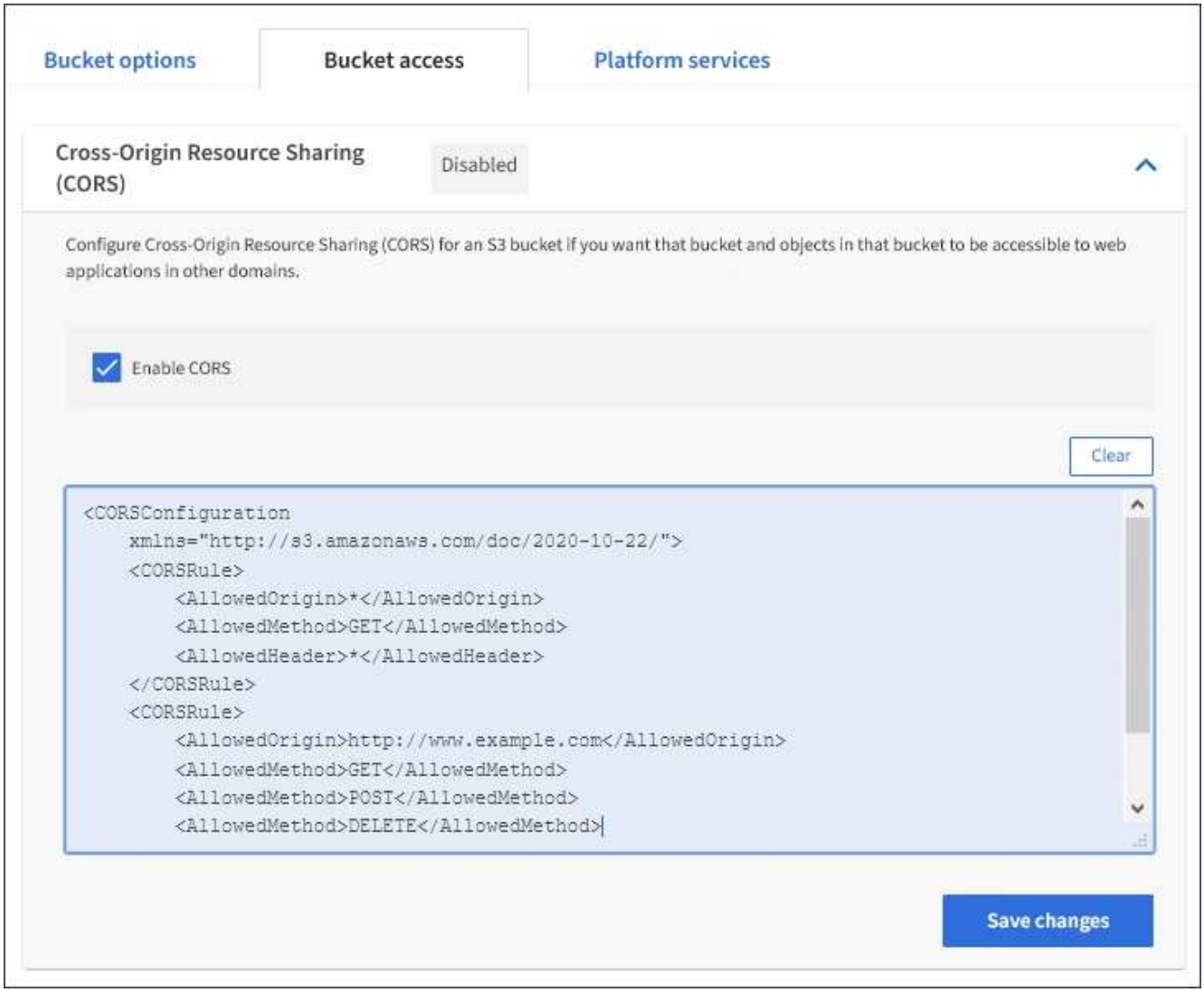
```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

CORS 구성 XML에 대한 자세한 내용은 을 참조하십시오 "AWS(Amazon Web Services) 문서: Amazon Simple Storage Service 개발자 가이드 를 참조하십시오".

2. 테넌트 관리자에서 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
3. 목록에서 버킷 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

4. Bucket access * > * Cross-Origin Resource Sharing (CORS) * 를 선택합니다.
5. CORS * 활성화 확인란을 선택합니다.
6. 텍스트 상자에 CORS 구성 XML을 붙여 넣고 * 변경 내용 저장 * 을 선택합니다.



7. 버킷의 CORS 설정을 수정하려면 텍스트 상자에서 CORS 구성 XML을 업데이트하거나 다시 시작하려면 * Clear * 를 선택하십시오. 그런 다음 * 변경 사항 저장 * 을 선택합니다.
8. 버킷에 대한 CORS를 비활성화하려면 * CORS * 활성화 확인란의 선택을 취소한 다음 * 변경 사항 저장 * 을 선택합니다.

S3 버킷을 삭제합니다

테넌트 관리자를 사용하여 비어 있는 하나 이상의 S3 버킷을 삭제할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다. 을 참조하십시오 테넌트 관리 권한.
- 삭제할 버킷이 비어 있습니다.

이 작업에 대해

다음 지침은 Tenant Manager를 사용하여 S3 버킷을 삭제하는 방법을 설명합니다. 를 사용하여 S3 버킷을 삭제할 수도 있습니다 테넌트 관리 API 또는 을 누릅니다 S3 REST API.

오브젝트 또는 비최신 오브젝트 버전이 포함된 S3 버킷을 삭제할 수 없습니다. S3 버전 오브젝트를 삭제하는 방법에 대한 자세한 내용은 를 참조하십시오 정보 수명 주기 관리를 사용하여 개체를 관리하기 위한 지침.

단계

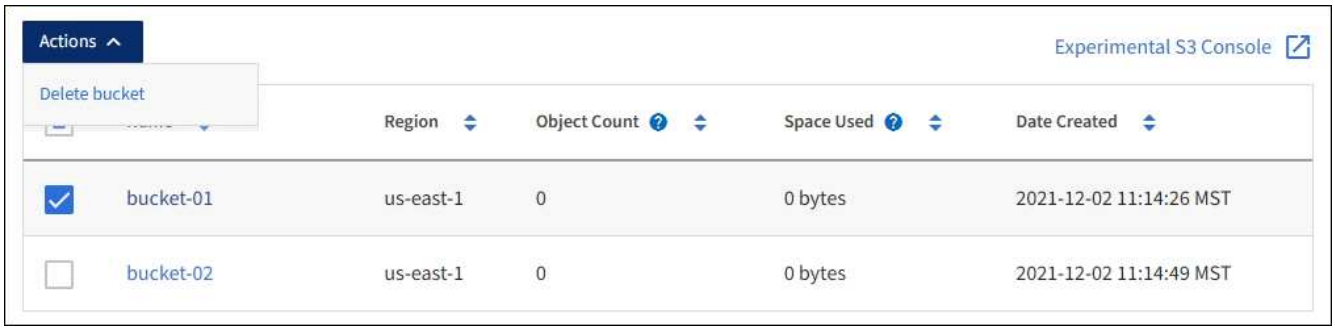
1. 스토리지(S3) * > * 버킷 * 을 선택합니다.

   Bucket 페이지가 나타나고 기존의 모든 S3 버킷을 표시합니다.

2. 삭제할 빈 버킷의 확인란을 선택합니다. 한 번에 둘 이상의 버킷을 선택할 수 있습니다.

   작업 메뉴가 활성화됩니다.

3. 작업 메뉴에서 * 버킷 삭제 * (또는 둘 이상을 선택한 경우 * 버킷 삭제 *)를 선택합니다.



4. 확인 대화 상자가 나타나면 * 예 * 를 선택하여 선택한 모든 버킷을 삭제합니다.

   StorageGRID는 각 버킷이 비어 있음을 확인한 다음 각 버킷을 삭제합니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.

   버킷이 비어 있지 않으면 오류 메시지가 나타납니다. 버킷을 삭제하려면 먼저 모든 오브젝트를 삭제해야 합니다.

Experimental S3 Console을 사용합니다

S3 콘솔을 사용하여 S3 버킷의 오브젝트를 볼 수 있습니다.

S3 콘솔을 사용하여 다음을 수행할 수도 있습니다.

- 개체, 개체 버전 및 폴더를 추가하고 삭제합니다
- 개체 이름을 바꿉니다
- 버킷 및 폴더 간에 오브젝트를 이동 및 복사합니다
- 오브젝트 태그 관리
- 개체 메타데이터를 봅니다
- 객체를 다운로드합니다

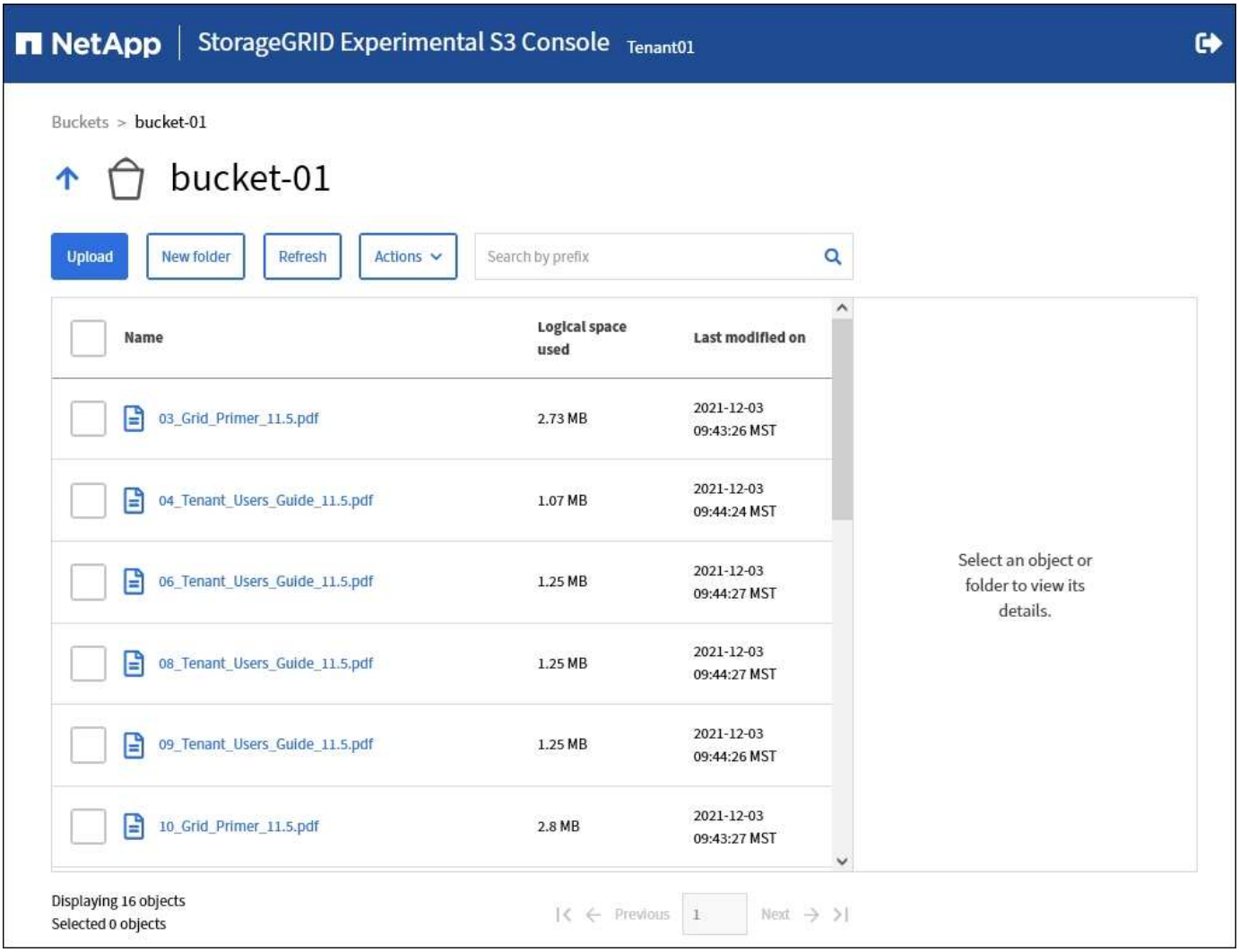
> S3 콘솔이 완전히 테스트되지 않았으며 "Experimental(실험)"으로 표시됩니다. 대량의 오브젝트 관리 또는 운영 환경에서 사용하기 위한 것이 아닙니다. 테넌트는 새로운 ILM 정책을 시뮬레이션하기 위해 개체를 업로드할 때, 수집 문제 해결 또는 개념 증명 또는 비운영 그리드를 사용하는 경우와 같이 소수의 개체에 대한 기능을 수행할 때만 S3 콘솔을 사용해야 합니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 자신의 S3 자격 증명 관리 권한이 있습니다.
- 버킷을 만들었습니다.
- 사용자의 액세스 키 ID와 비밀 액세스 키를 알고 있습니다. 필요한 경우 이 정보가 포함된 '.csv' 파일을 사용할 수 있습니다. 를 참조하십시오 액세스 키 생성에 대한 지침.

단계

1. Bucket * 을 선택합니다.
2. 를 선택합니다 Experimental S3 Console . 버킷 세부 정보 페이지에서 이 링크에 액세스할 수도 있습니다.
3. Experimental S3 Console 로그인 페이지에서 액세스 키 ID 및 비밀 액세스 키를 필드에 붙여 넣습니다. 그렇지 않으면 * 업로드 액세스 키 * 를 선택하고 '.csv' 파일을 선택합니다.
4. 로그인 * 을 선택합니다.
5. 필요에 따라 오브젝트 관리



S3 플랫폼 서비스 관리

플랫폼 서비스란 무엇입니까?

StorageGRID 플랫폼 서비스는 하이브리드 클라우드 전략을 구현하는 데 도움이 될 수 있습니다.

테넌트 계정에 플랫폼 서비스를 사용할 수 있는 경우 모든 S3 버킷에 대해 다음 서비스를 구성할 수 있습니다.

- * CloudMirror 복제 * StorageGRID CloudMirror 복제 서비스입니다 StorageGRID 버킷에서 지정된 외부 대상으로 특정 오브젝트를 미러링하는 데 사용됩니다.

  예를 들어, CloudMirror 복제를 사용하여 특정 고객 레코드를 Amazon S3에 미러링한 다음 AWS 서비스를 활용하여 데이터에 대한 분석을 수행할 수 있습니다.

  > 소스 버킷에 S3 오브젝트 잠금이 설정된 경우 CloudMirror 복제가 지원되지 않습니다.

- * 알림 *: 버킷당 이벤트 알림 지정된 외부 SNS(Amazon Simple Notification Service ™)에 객체에 대해 수행된 특정 작업에 대한 알림을 보내는 데 사용됩니다.

  예를 들어, 버킷에 추가된 각 오브젝트에 대해 관리자에게 경고가 전송되도록 구성할 수 있습니다. 여기서 객체는

중요한 시스템 이벤트와 연결된 로그 파일을 나타냅니다.

> S3 오브젝트 잠금이 활성화된 버킷에서 이벤트 알림을 구성할 수 있지만 오브젝트의 S3 오브젝트 잠금 메타데이터(마지막 보존 날짜 및 법적 보류 상태 포함)는 알림 메시지에 포함되지 않습니다.

- * 통합 서비스 검색 * 검색 통합 서비스 외부 서비스를 사용하여 메타데이터를 검색하거나 분석할 수 있는 지정된 Elasticsearch 인덱스에 S3 개체 메타데이터를 전송하는 데 사용됩니다.

  예를 들어, S3 오브젝트 메타데이터를 원격 Elasticsearch 서비스로 전송하도록 버킷을 구성할 수 있습니다. 그런 다음 Elasticsearch를 사용하여 버킷에 대한 검색을 수행하고 객체 메타데이터에 있는 패턴에 대한 정교한 분석을 수행할 수 있습니다.

> S3 오브젝트 잠금이 활성화된 버킷에서 Elasticsearch 통합을 구성할 수 있지만 오브젝트의 S3 오브젝트 잠금 메타데이터(보존 기한 및 법적 보류 상태 포함)는 알림 메시지에 포함되지 않습니다.

플랫폼 서비스의 대상 위치는 일반적으로 StorageGRID 구축과 외부적이기 때문에 플랫폼 서비스는 데이터에 대한 외부 스토리지 리소스, 알림 서비스 및 검색 또는 분석 서비스를 사용하여 얻을 수 있는 성능과 유연성을 제공합니다.

단일 S3 버킷에 대해 모든 플랫폼 서비스 조합을 구성할 수 있습니다. 예를 들어, StorageGRID S3 버킷에서 CloudMirror 서비스 및 알림을 모두 구성하여 특정 오브젝트를 Amazon Simple Storage Service에 미러링하고 이러한 각 오브젝트에 대한 알림을 타사 모니터링 애플리케이션에 전송하여 AWS 비용을 추적할 수 있도록 할 수 있습니다.

> 그리드 관리자 또는 그리드 관리 API를 사용하여 StorageGRID 관리자가 각 테넌트 계정에 대해 플랫폼 서비스 사용을 활성화해야 합니다.

플랫폼 서비스 구성 방법

플랫폼 서비스는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성한 외부 엔드포인트와 통신합니다. 각 엔드포인트는 StorageGRID S3 버킷, Amazon 웹 서비스 버킷, SNS(Simple Notification Service) 주제 또는 로컬, AWS 또는 기타 위치에서 호스팅되는 Elasticsearch 클러스터와 같은 외부 대상을 나타냅니다.

끝점을 만든 후 버킷에 XML 구성을 추가하여 버킷에 대한 플랫폼 서비스를 활성화할 수 있습니다. XML 구성은 버킷이 작업해야 하는 오브젝트, 버킷이 취해야 하는 조치 및 버킷이 서비스에 사용해야 하는 엔드포인트를 식별합니다.

구성할 각 플랫폼 서비스에 대해 별도의 XML 구성을 추가해야 합니다. 예를 들면 다음과 같습니다.

1. 키가 '/images'로 시작하는 모든 오브젝트를 Amazon S3 버킷에 복제하려면 소스 버킷에 복제 구성을 추가해야 합니다.
2. 이러한 객체가 버킷에 저장될 때 알림을 보내려면 알림 구성을 추가해야 합니다.
3. 마지막으로 이러한 개체의 메타데이터를 인덱싱하려면 검색 통합을 구현하는 데 사용되는 메타데이터 알림 구성을 추가해야 합니다.

구성 XML의 형식은 StorageGRID 플랫폼 서비스를 구현하는 데 사용되는 S3 REST API를 통해 제어됩니다.

플랫폼 서비스	**S3 REST API**
CloudMirror 복제	• 버킷 복제를 가져옵니다 • 버킷 복제를 배치합니다

플랫폼 서비스	**S3 REST API**
알림	• 버킷 알림을 받습니다 • 버킷 통지를 보냅니다
검색 통합	• Bucket 메타데이터 알림 구성 가져오기 • Put Bucket 메타데이터 알림 구성 이러한 작업은 StorageGRID에 맞게 맞춤형으로 제공됩니다.

StorageGRID에서 이러한 API를 구축하는 방법에 대한 자세한 내용은 S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

관련 정보

플랫폼 서비스 사용에 대한 고려 사항

S3을 사용합니다

CloudMirror 복제 서비스

StorageGRID가 버킷에 추가된 지정된 오브젝트를 하나 이상의 대상 버킷에 복제하도록 하려면 S3 버킷에 대해 CloudMirror 복제를 활성화할 수 있습니다.

CloudMirror 복제는 그리드의 활성 ILM 정책과 독립적으로 작동합니다. CloudMirror 서비스는 소스 버킷에 저장된 객체를 복제하여 가능한 한 빨리 대상 버킷에 제공합니다. 오브젝트 수집의 성공 시 복제된 오브젝트 제공이 트리거됩니다.

기존 버킷에 대해 CloudMirror 복제를 설정하면 해당 버킷에 추가된 새 객체만 복제됩니다. 버킷의 기존 객체는 복제되지 않습니다. 기존 오브젝트의 복제를 강제로 수행하려면 오브젝트 복사를 수행하여 기존 오브젝트의 메타데이터를 업데이트할 수 있습니다.

> CloudMirror 복제를 사용하여 오브젝트를 AWS S3 대상으로 복사하는 경우 Amazon S3는 각 PUT 요청 헤더 내의 사용자 정의 메타데이터 크기를 2KB로 제한합니다. 객체에 2KB보다 큰 사용자 정의 메타데이터가 있는 경우 해당 객체가 복제되지 않습니다.

StorageGRID에서는 단일 버킷의 오브젝트를 여러 개의 대상 버킷으로 복제할 수 있습니다. 이렇게 하려면 복제 구성 XML에서 각 규칙의 대상을 지정합니다. 객체를 둘 이상의 버킷에 동시에 복제할 수 없습니다.

또한 버전 관리되거나 버전이 지정되지 않은 버킷에서 CloudMirror 복제를 구성하고 버전 관리되거나 버전이 지정되지 않은 버킷을 대상으로 지정할 수 있습니다. 버전 및 비버전 버킷의 모든 조합을 사용할 수 있습니다. 예를 들어 버전이 지정되지 않은 소스 버킷의 대상으로 버전 관리가 지정된 버킷을 지정하거나 그 반대로 지정할 수 있습니다. 버전이 지정되지 않은 버킷 간에 복제할 수도 있습니다.

CloudMirror 복제 서비스의 삭제 동작은 Amazon S3에서 제공하는 CRR(Cross Region Replication) 서비스의 삭제 동작과 같습니다. 소스 버킷에서 객체를 삭제해도 대상에서 복제된 객체는 삭제되지 않습니다. 소스 및 대상 버킷의 버전이 모두 지정된 경우 삭제 마커가 복제됩니다. 대상 버킷의 버전이 지정되지 않은 경우 소스 버킷에서 오브젝트를 삭제해도 삭제 마커가 대상 버킷에 복제되거나 대상 오브젝트가 삭제되지 않습니다.

객체가 대상 버킷에 복제되면 StorageGRID는 객체를 "replicas"로 표시합니다. 대상 StorageGRID 버킷은 복제본으로

표시된 객체를 다시 복제하지 않으므로 실수로 인한 복제 루프로부터 보호됩니다. 이 복제 마크는 StorageGRID 내부에 있으며 Amazon S3 버킷을 대상으로 사용할 때 AWS CRR을 활용하는 것을 방지하지 않습니다.

> 복제본을 표시하는 데 사용되는 사용자 지정 헤더는 X-NTAP-sg-replica입니다. 이 표시는 계단식 미러를 방지합니다. StorageGRID는 두 그리드 간의 양방향 CloudMirror를 지원합니다.

대상 버킷의 이벤트의 고유성과 순서는 보장되지 않습니다. 전송 성공을 보장하기 위해 수행된 작업의 결과로 소스 객체의 동일한 복제본이 두 개 이상 대상에 제공될 수 있습니다. 드물지만 둘 이상의 서로 다른 StorageGRID 사이트에서 동일한 객체가 동시에 업데이트되는 경우 대상 버킷의 작업 순서가 소스 버킷의 이벤트 순서와 일치하지 않을 수 있습니다.

CloudMirror 복제는 일반적으로 외부 S3 버킷을 대상으로 사용하도록 구성됩니다. 그러나 다른 StorageGRID 배포나 S3 호환 서비스를 사용하도록 복제를 구성할 수도 있습니다.

버킷에 대한 알림을 이해합니다

StorageGRID에서 지정된 이벤트에 대한 알림을 대상 SNS(Amazon Simple Notification Service)로 보내도록 하려면 S3 버킷에 대한 이벤트 알림을 활성화할 수 있습니다.

가능합니다 이벤트 알림을 구성합니다 알림 구성 XML을 소스 버킷과 연결합니다. 알림 구성 XML은 버킷 알림을 구성하기 위한 S3 규칙을 따르고, 엔드포인트의 URN으로 지정된 대상 SNS 항목을 따릅니다.

이벤트 알림은 알림 구성에 지정된 대로 소스 버킷에서 생성되며 대상으로 전달됩니다. 개체와 관련된 이벤트가 성공하면 해당 이벤트에 대한 알림이 생성되고 배달 대기 상태가 됩니다.

알림의 고유성과 순서는 보장되지 않습니다. 전송 성공을 보장하기 위해 수행된 작업의 결과로 하나 이상의 이벤트 알림이 대상에 전달될 수 있습니다. 그리고 납품이 비동기식이기 때문에, 특히 서로 다른 StorageGRID 사이트에서 발생하는 작업의 경우, 대상에서 알림의 시간 순서가 소스 버킷의 이벤트 순서와 일치한다고 보장할 수 없습니다. 이벤트 메시지에서 '시퀀스' 키를 사용하여 Amazon S3 문서에 설명된 대로 특정 객체에 대한 이벤트 순서를 결정할 수 있습니다.

지원되는 알림 및 메시지

StorageGRID 이벤트 알림은 Amazon S3 API를 따르며 다음과 같은 제한 사항이 적용됩니다.

- 다음 이벤트 유형에 대한 알림을 구성할 수 없습니다. 이러한 이벤트 유형은 * 지원되지 않습니다 *.
  - '3: RedundancyLostObject'를 선택합니다
  - '3:ObjectRestore:완료됨'
- StorageGRID에서 보낸 이벤트 알림은 표에 나와 있는 것처럼 일부 키를 포함하지 않고 다른 키에 대해 특정 값을 사용한다는 점을 제외하고 표준 JSON 형식을 사용합니다.

키 이름	**StorageGRID** 값
이벤트 소스	전쟁포로 S3
awsRegion	포함되지 않음
X-amz-id-2	포함되지 않음

키 이름	**StorageGRID** 값
ARN	"urn:SGWs:S3::bucket_name'

검색 통합 서비스를 이해합니다

오브젝트 메타데이터에 외부 검색 및 데이터 분석 서비스를 사용하려는 경우 S3 버킷에 대한 검색 통합을 활성화할 수 있습니다.

검색 통합 서비스는 오브젝트 또는 해당 메타데이터가 업데이트될 때마다 자동으로 그리고 비동기적으로 S3 오브젝트 메타데이터를 대상 끝점에 보내는 사용자 지정 StorageGRID 서비스입니다. 그런 다음 대상 서비스에서 제공하는 정교한 검색, 데이터 분석, 시각화 또는 머신 러닝 도구를 사용하여 오브젝트 데이터를 검색, 분석 및 분석할 수 있습니다.

버전 관리되거나 버전이 지정되지 않은 모든 버킷에 대해 검색 통합 서비스를 활성화할 수 있습니다. 검색 통합은 메타데이터 알림 구성 XML을 작업할 개체 및 개체 메타데이터에 대한 대상을 지정하는 버킷과 연결하여 구성됩니다.

알림은 버킷 이름, 오브젝트 이름 및 버전 ID(있는 경우)로 명명된 JSON 문서의 형식으로 생성됩니다. 각 메타데이터 알림에는 개체의 모든 태그 및 사용자 메타데이터 외에도 개체에 대한 표준 시스템 메타데이터 세트가 포함되어 있습니다.

> 태그 및 사용자 메타데이터의 경우 StorageGRID는 날짜 및 숫자를 Elasticsearch에 문자열 또는 S3 이벤트 알림으로 전달합니다. 이러한 문자열을 날짜 또는 숫자로 해석하도록 Elasticsearch를 구성하려면 동적 필드 매핑 및 날짜 형식 매핑에 대한 Elasticsearch 지침을 따르십시오. 검색 통합 서비스를 구성하기 전에 인덱스에서 동적 필드 매핑을 활성화해야 합니다. 문서가 인덱싱된 후에는 인덱스에서 문서의 필드 형식을 편집할 수 없습니다.

알림은 다음과 같은 경우에 생성되고 전송 대기 상태가 됩니다.

- 객체가 생성됩니다.
- 그리드의 ILM 정책 작업으로 인해 오브젝트가 삭제된 경우를 포함하여 오브젝트가 삭제됩니다.
- 오브젝트 메타데이터 또는 태그가 추가, 업데이트 또는 삭제됩니다. 메타데이터 및 태그의 전체 집합은 항상 변경된 값뿐만 아니라 업데이트 시 전송됩니다.

메타데이터 알림 구성 XML을 버킷에 추가하면 생성한 새 개체 및 데이터, 사용자 메타데이터 또는 태그를 업데이트하여 수정하는 모든 개체에 대한 알림이 전송됩니다. 그러나 버킷에 이미 있는 객체에 대해서는 알림이 전송되지 않습니다. 버킷의 모든 오브젝트에 대한 오브젝트 메타데이터가 대상으로 전송되도록 하려면 다음 중 하나를 수행해야 합니다.

- 버킷을 생성한 후 개체를 추가하기 전에 즉시 검색 통합 서비스를 구성합니다.
- 메타데이터 알림 메시지가 대상으로 전송되도록 버킷에 이미 있는 모든 객체에 대해 작업을 수행합니다.

StorageGRID 검색 통합 서비스는 Elasticsearch 클러스터를 대상으로 지원합니다. 다른 플랫폼 서비스와 마찬가지로 대상은 서비스의 구성 XML에서 URN이 사용되는 끝점에서 지정됩니다. 를 사용합니다 "NetApp 상호 운용성 매트릭스 툴" 지원되는 Elasticsearch 버전을 확인합니다.

관련 정보

검색 통합을 위한 구성 XML

메타데이터 알림에 포함된 개체 메타데이터입니다

JSON이 검색 통합 서비스에 의해 생성되었습니다

검색 통합 서비스를 구성합니다

플랫폼 서비스 사용에 대한 고려 사항

플랫폼 서비스를 구현하기 전에 이러한 서비스를 사용하기 위한 권장 사항 및 고려 사항을 검토하십시오.

S3에 대한 자세한 내용은 을 참조하십시오 S3을 사용합니다.

플랫폼 서비스 사용에 대한 고려 사항

고려 사항	세부 정보
대상 엔드포인트 모니터링	각 대상 끝점의 가용성을 모니터링해야 합니다. 대상 끝점에 대한 연결이 오랜 시간 동안 손실되고 요청의 백로그가 많은 경우 StorageGRID에 대한 추가 클라이언트 요청(예: PUT 요청)이 실패합니다. 엔드포인트에 연결할 수 있게 되면 실패한 요청을 다시 시도해야 합니다.
대상 끝점 임계치 조절	요청이 전송되는 속도가 대상 엔드포인트에서 요청을 수신할 수 있는 속도를 초과하는 경우 StorageGRID 소프트웨어는 버킷에 대한 수신 S3 요청을 스로틀할 수 있습니다. 임계치 조절은 대상 끝점으로 보내려고 기다리는 요청의 백로그가 있는 경우에만 발생합니다. 단, 들어오는 S3 요청의 실행 시간이 더 오래 걸린다는 점을 알 수 있습니다. 속도가 현저히 느린 성능을 감지하기 시작하는 경우 수집 속도를 줄이거나 용량이 더 큰 엔드포인트를 사용해야 합니다. 요청 백로그가 계속 증가하는 경우 PUT 요청과 같은 클라이언트 S3 작업이 결국 실패합니다. CloudMirror 요청은 일반적으로 검색 통합 또는 이벤트 알림 요청보다 더 많은 데이터 전송을 포함하므로 대상 엔드포인트의 성능에 영향을 받을 가능성이 더 높습니다.
주문 보증	StorageGRID은 사이트 내의 개체에 대한 작업을 주문할 수 있도록 보장합니다. 객체에 대한 모든 작업이 동일한 사이트 내에 있는 한 최종 객체 상태(복제의 경우)는 항상 StorageGRID의 상태와 동일합니다. StorageGRID는 StorageGRID 사이트 전체에서 작업이 수행되는 경우 요청을 주문하기 위해 최선의 노력을 다하고 있습니다. 예를 들어 처음에 사이트 A에 오브젝트를 작성한 다음 나중에 사이트 B에서 동일한 오브젝트를 덮어쓰는 경우 CloudMirror에서 대상 버킷에 복제한 최종 오브젝트는 새로운 오브젝트일 수 없습니다.
ILM 기반 오브젝트 삭제	AWS CRR 및 SNS 서비스의 삭제 동작과 일치하도록 StorageGRID ILM 규칙 때문에 소스 버킷의 객체가 삭제될 때 CloudMirror 및 이벤트 알림 요청이 전송되지 않습니다. 예를 들어 ILM 규칙이 14일 후에 개체를 삭제하는 경우 CloudMirror 또는 이벤트 알림 요청이 전송되지 않습니다. 반면, 검색 통합 요청은 ILM로 인해 객체가 삭제될 때 전송됩니다.

고려 사항	세부 정보
복제 상태입니다	StorageGRID는 X-amz-replication-status 헤더를 지원하지 않습니다.
개체 크기	CloudMirror 복제 서비스를 통해 대상 버킷에 복제할 수 있는 개체의 최대 크기는 5TiB이며, 이는 maximum_supported_object 크기와 같습니다. • 참고 *: 단일 PUT 오브젝트 작업에 대한 maximum_recommended_size는 5GiB(5,368,709,120바이트)입니다. 5GiB보다 큰 객체가 있는 경우 대신 멀티파트 업로드를 사용합니다.
버킷 버전 관리 및 버전 ID	StorageGRID의 소스 S3 버킷에서 버전 관리가 활성화된 경우 대상 버킷의 버전 관리도 활성화해야 합니다. 버전 관리를 사용할 때는 S3 프로토콜의 제한으로 인해 대상 버킷에서 오브젝트 버전 순서가 CloudMirror 서비스에 의해 보장되지 않는 것이 가장 좋습니다. • 참고 *: StorageGRID의 소스 버킷에 대한 버전 ID는 대상 버킷의 버전 ID와 관련이 없습니다.
개체 버전에 태그 달기	CloudMirror 서비스는 S3 프로토콜의 제한으로 인해 버전 ID를 제공하는 Put Object 태그 지정 또는 Delete Object 태그 지정 요청을 복제하지 않습니다. 소스 및 대상의 버전 ID는 관련이 없으므로 특정 버전 ID에 대한 태그 업데이트를 복제할 수 없습니다. 반면 CloudMirror 서비스는 Put Object 태그 지정 요청을 복제하거나 버전 ID를 지정하지 않는 Object 태그 지정 요청을 삭제합니다. 이러한 요청은 최신 키의 태그(또는 버킷의 버전이 지정된 경우 최신 버전)를 업데이트합니다. 태그가 있는 일반 베스트(업데이트 태그 지정 안 함)도 복제됩니다.
멀티파트 업로드 및 'ETag' 값	여러 부분 업로드를 사용하여 업로드한 개체를 미러링할 때 CloudMirror 서비스는 해당 파트를 보존하지 않습니다. 따라서 대칭 복사된 오브젝트의 ETag 값은 원래 오브젝트의 ETag 값과 다릅니다.
SSE-C로 암호화된 오브젝트(고객이 제공한 키를 사용한 서버측 암호화)	CloudMirror 서비스는 SSE-C로 암호화된 객체를 지원하지 않습니다 CloudMirror 복제를 위해 소스 버킷으로 객체를 수집하려고 하고 요청에 SSE-C 요청 헤더가 포함된 경우 작업이 실패합니다.
S3 오브젝트 잠금이 활성화된 버킷	CloudMirror 복제에 대한 대상 S3 버킷에서 S3 Object Lock이 활성화된 경우 버킷 복제(Put Bucket 복제)를 구성하려고 하면 AccessDenied 오류가 발생하고 실패합니다.

플랫폼 서비스 끝점을 구성합니다

버킷에 대한 플랫폼 서비스를 구성하려면 먼저 플랫폼 서비스의 대상으로 하나 이상의 엔드포인트를 구성해야 합니다.

플랫폼 서비스에 대한 액세스는 StorageGRID 관리자가 테넌트 단위로 사용하도록 설정합니다. 플랫폼 서비스 끝점을 만들거나 사용하려면 스토리지 노드가 외부 끝점 리소스에 액세스할 수 있도록 네트워킹이 구성된 그리드에서 끝점 관리

또는 루트 액세스 권한이 있는 테넌트 사용자여야 합니다. 자세한 내용은 StorageGRID 관리자에게 문의하십시오.

플랫폼 서비스 엔드포인트란 무엇입니까?

플랫폼 서비스 끝점을 만들 때 StorageGRID가 외부 대상에 액세스하는 데 필요한 정보를 지정합니다.

예를 들어, StorageGRID 버킷에서 AWS S3 버킷으로 오브젝트를 복제하려는 경우 StorageGRID에서 AWS의 대상 버킷에 액세스하는 데 필요한 정보와 자격 증명이 포함된 플랫폼 서비스 엔드포인트를 생성할 수 있습니다.

각 플랫폼 서비스 유형에는 고유한 엔드포인트가 필요하므로 사용하려는 각 플랫폼 서비스에 대해 하나 이상의 엔드포인트를 구성해야 합니다. 플랫폼 서비스 끝점을 정의한 후 서비스를 활성화하는 데 사용되는 구성 XML에서 끝점의 URN을 대상으로 사용합니다.

둘 이상의 소스 버킷에 대해 목적지와 동일한 끝점을 사용할 수 있습니다. 예를 들어, 여러 버킷에서 검색을 수행할 수 있도록 여러 소스 버킷을 구성하여 동일한 검색 통합 엔드포인트로 오브젝트 메타데이터를 보낼 수 있습니다. 또한 소스 버킷을 구성하여 둘 이상의 엔드포인트를 대상으로 사용할 수 있습니다. 이를 통해 하나의 SNS 항목에 개체 생성 알림을 보내고 개체 삭제에 대한 알림을 두 번째 SNS 항목으로 보내는 등의 작업을 수행할 수 있습니다.

CloudMirror 복제용 엔드포인트

StorageGRID는 S3 버킷을 나타내는 복제 엔드포인트를 지원합니다. 이러한 버킷은 Amazon Web Services, 동일한 또는 원격 StorageGRID 구축 또는 다른 서비스에서 호스팅될 수 있습니다.

알림의 끝점입니다

StorageGRID는 SNS(Simple Notification Service) 엔드포인트를 지원합니다. SQS(Simple Queue Service) 또는 AWS Lambda 엔드포인트는 지원되지 않습니다.

검색 통합 서비스의 끝점입니다

StorageGRID는 Elasticsearch 클러스터를 나타내는 검색 통합 끝점을 지원합니다. 이러한 Elasticsearch 클러스터는 로컬 데이터 센터에 있거나 AWS 클라우드 또는 다른 곳에서 호스팅될 수 있습니다.

검색 통합 끝점은 특정 Elasticsearch 인덱스 및 유형을 참조합니다. StorageGRID에서 끝점을 만들기 전에 Elasticsearch에서 인덱스를 만들어야 합니다. 그렇지 않으면 끝점 생성이 실패합니다. 끝점을 만들기 전에 형식을 만들 필요가 없습니다. StorageGRID는 개체 메타데이터를 끝점으로 보낼 때 필요한 경우 형식을 만듭니다.

관련 정보

StorageGRID 관리

플랫폼 서비스 끝점에 URN을 지정합니다

플랫폼 서비스 끝점을 만들 때는 고유한 URN(리소스 이름)을 지정해야 합니다. 플랫폼 서비스에 대한 구성 XML을 만들 때 URN을 사용하여 끝점을 참조합니다. 각 끝점의 URN은 고유해야 합니다.

StorageGRID에서는 플랫폼 서비스 엔드포인트를 만들 때 이를 검증합니다. 플랫폼 서비스 끝점을 만들기 전에 끝점에 지정된 리소스가 있고 해당 리소스에 도달할 수 있는지 확인합니다.

urn 요소

플랫폼 서비스 끝점의 URN은 다음과 같이 "arn:AWS" 또는 "urn:mysite"로 시작해야 합니다.

- AWS(Amazon Web Services)에서 호스팅되는 서비스의 경우 'arn:AWS'를 사용합니다.
- 서비스가 GCP(Google Cloud Platform)에서 호스팅되는 경우 "arn:AWS"를 사용하십시오.
- 서비스가 로컬로 호스트되는 경우 urn:mysite를 사용합니다

예를 들어, StorageGRID에서 호스팅되는 CloudMirror 엔드포인트에 대해 URN을 지정하는 경우 URN은 "urn:SGWs"로 시작할 수 있습니다.

URN의 다음 요소는 다음과 같이 플랫폼 서비스의 유형을 지정합니다.

서비스	유형
CloudMirror 복제	S3
알림	SNS
검색 통합	ES

예를 들어, StorageGRID에서 호스팅되는 CloudMirror 엔드포인트에 대해 URN을 계속 지정하려면 's3'을 추가하여 urn:SGWs:s3'을 가져옵니다.

URN의 마지막 요소는 대상 URI에서 특정 대상 리소스를 식별합니다.

서비스	특정 리소스
CloudMirror 복제	버킷 이름
알림	SNS-주제-이름
검색 통합	domain-name/index-name/type-name'입니다 • 참고: * Elasticsearch 클러스터가 자동으로 인덱스를 만들도록 * 구성되지 * 인 경우 끝점을 만들기 전에 수동으로 인덱스를 만들어야 합니다.

AWS 및 **GCP**에서 호스팅되는 서비스의 여관

AWS 및 GCP 엔터티의 경우 URN은 유효한 AWS ARN입니다. 예를 들면 다음과 같습니다.

- CloudMirror 복제:

```
arn:aws:s3:::bucket-name
```

- 알림:

```
arn:aws:sns:region:account-id:topic-name
```

- 검색 통합:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> AWS 검색 통합 엔드포인트의 경우 domain-name에는 여기에 나와 있는 리터럴 문자열 domain/"이 포함되어야 합니다.

현지 호스팅 서비스를 위한 여관

클라우드 서비스 대신 로컬로 호스팅된 서비스를 사용하는 경우 URN에 필요한 요소가 세 번째 및 최종 위치에 포함되어 있는 한 유효하고 고유한 URN을 만드는 방식으로 URN을 지정할 수 있습니다. 선택 사항으로 표시된 요소를 비워 두거나 자원을 식별하고 URN을 고유하게 만드는 데 도움이 되도록 원하는 방식으로 지정할 수 있습니다. 예를 들면 다음과 같습니다.

- CloudMirror 복제:

```
urn:mysite:s3:optional:optional:bucket-name
```

  StorageGRID에서 호스팅되는 CloudMirror 엔드포인트의 경우 "urn:SGW"로 시작하는 유효한 URN을 지정할 수 있습니다.

```
urn:sgws:s3:optional:optional:bucket-name
```

- 알림:

```
urn:mysite:sns:optional:optional:sns-topic-name
```

- 검색 통합:

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```

> 로컬에서 호스팅되는 검색 통합 끝점의 경우 끝점의 URN이 고유하면 domain-name 요소는 모든 문자열이 될 수 있습니다.

플랫폼 서비스 끝점을 만듭니다

플랫폼 서비스를 사용하려면 먼저 올바른 유형의 끝점을 하나 이상 만들어야 합니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 사용하도록 설정해야 합니다.

- 끝점 관리 권한이 있는 사용자 그룹에 속해야 합니다.
- 플랫폼 서비스 끝점에서 참조하는 리소스가 생성되어야 합니다.
  - CloudMirror 복제: S3 버킷
  - 이벤트 알림: SNS 항목
  - 검색 알림: 대상 클러스터가 인덱스를 자동으로 생성하도록 구성되지 않은 경우 Elasticsearch index입니다.
- 대상 리소스에 대한 정보가 있어야 합니다.
  - URI(Uniform Resource Identifier)의 호스트 및 포트

    > StorageGRID 시스템에서 호스팅되는 버킷을 CloudMirror 복제의 엔드포인트로 사용하려면 그리드 관리자에게 문의하여 입력해야 하는 값을 확인하십시오.

  - 고유 리소스 이름(URN)

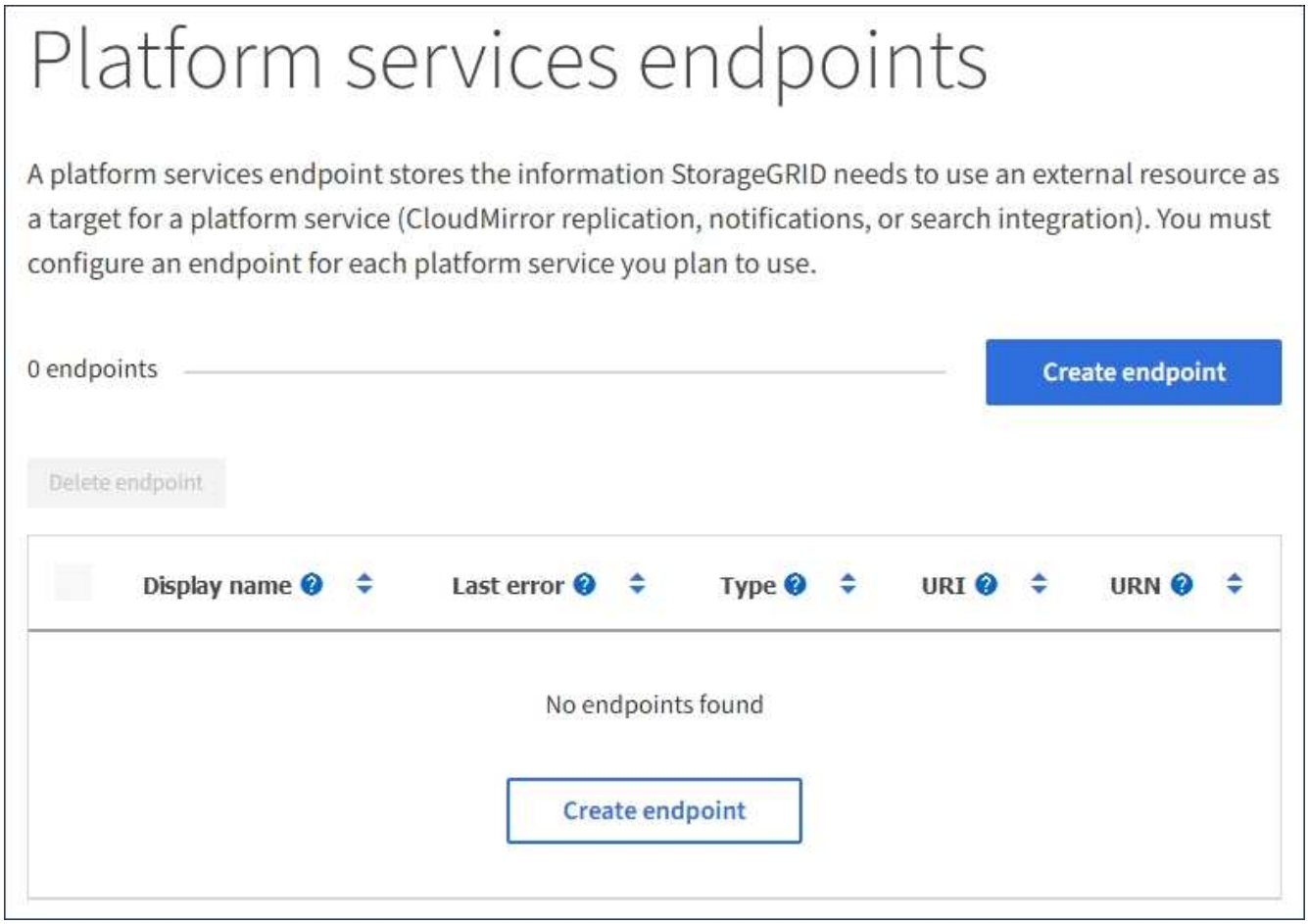
    플랫폼 서비스 끝점에 URN을 지정합니다

  - 인증 자격 증명(필요한 경우):
    - 액세스 키: 액세스 키 ID 및 비밀 액세스 키
    - 기본 HTTP: 사용자 이름 및 암호
    - CAP(C2S Access Portal): 임시 자격 증명 URL, 서버 및 클라이언트 인증서, 클라이언트 키 및 선택적 클라이언트 개인 키 암호.
  - 보안 인증서(사용자 지정 CA 인증서를 사용하는 경우)

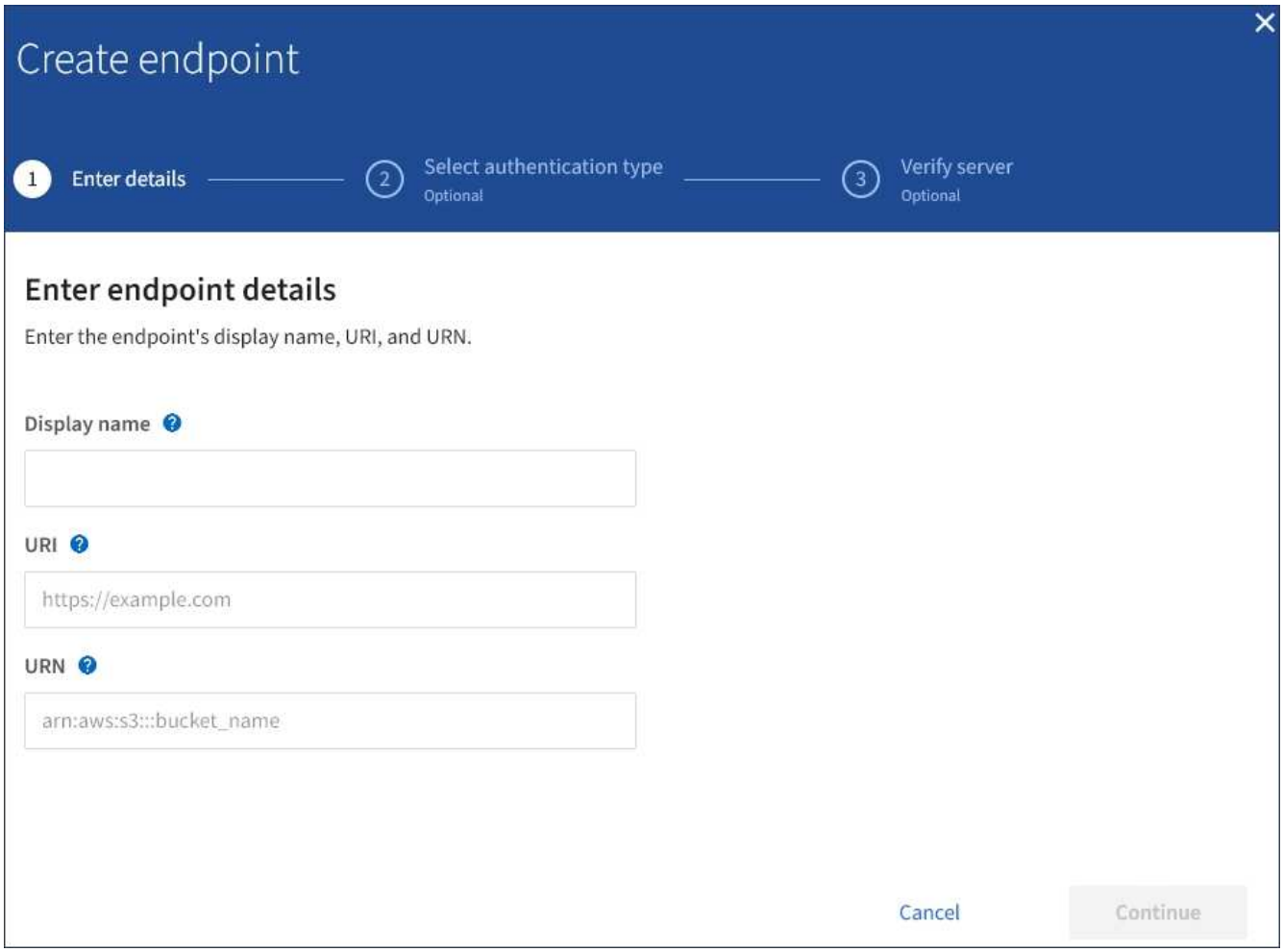
단계

1. 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 * 를 선택합니다.

   플랫폼 서비스 끝점 페이지가 나타납니다.



2. 끝점 만들기 * 를 선택합니다.



3. 표시 이름을 입력하여 끝점과 그 용도를 간략하게 설명합니다.

   끝점이 지원하는 플랫폼 서비스 유형은 끝점 페이지에 나열될 때 끝점 이름 옆에 표시됩니다. 따라서 이름에 해당 정보를 포함할 필요가 없습니다.

4. URI * 필드에서 끝점의 고유 URI(Resource Identifier)를 지정합니다.

   다음 형식 중 하나를 사용합니다.

```
https://host:port
http://host:port
```

   포트를 지정하지 않으면 포트 443이 HTTPS URI에 사용되고 포트 80은 HTTP URI에 사용됩니다.

   예를 들어 StorageGRID에서 호스팅되는 버킷의 URI는 다음과 같습니다.

```
https://s3.example.com:10443
```

   이 예에서 '3.example.com'는 StorageGRID HA(High Availability) 그룹의 가상 IP(VIP)에 대한 DNS 항목을 나타내고, '10443'은 로드 밸런서 끝점에 정의된 포트를 나타냅니다.

가능하면 단일 장애 지점을 피하기 위해 로드 밸런싱 노드의 HA 그룹에 연결해야 합니다.

마찬가지로 AWS에서 호스팅되는 버킷의 URI는 다음과 같습니다.

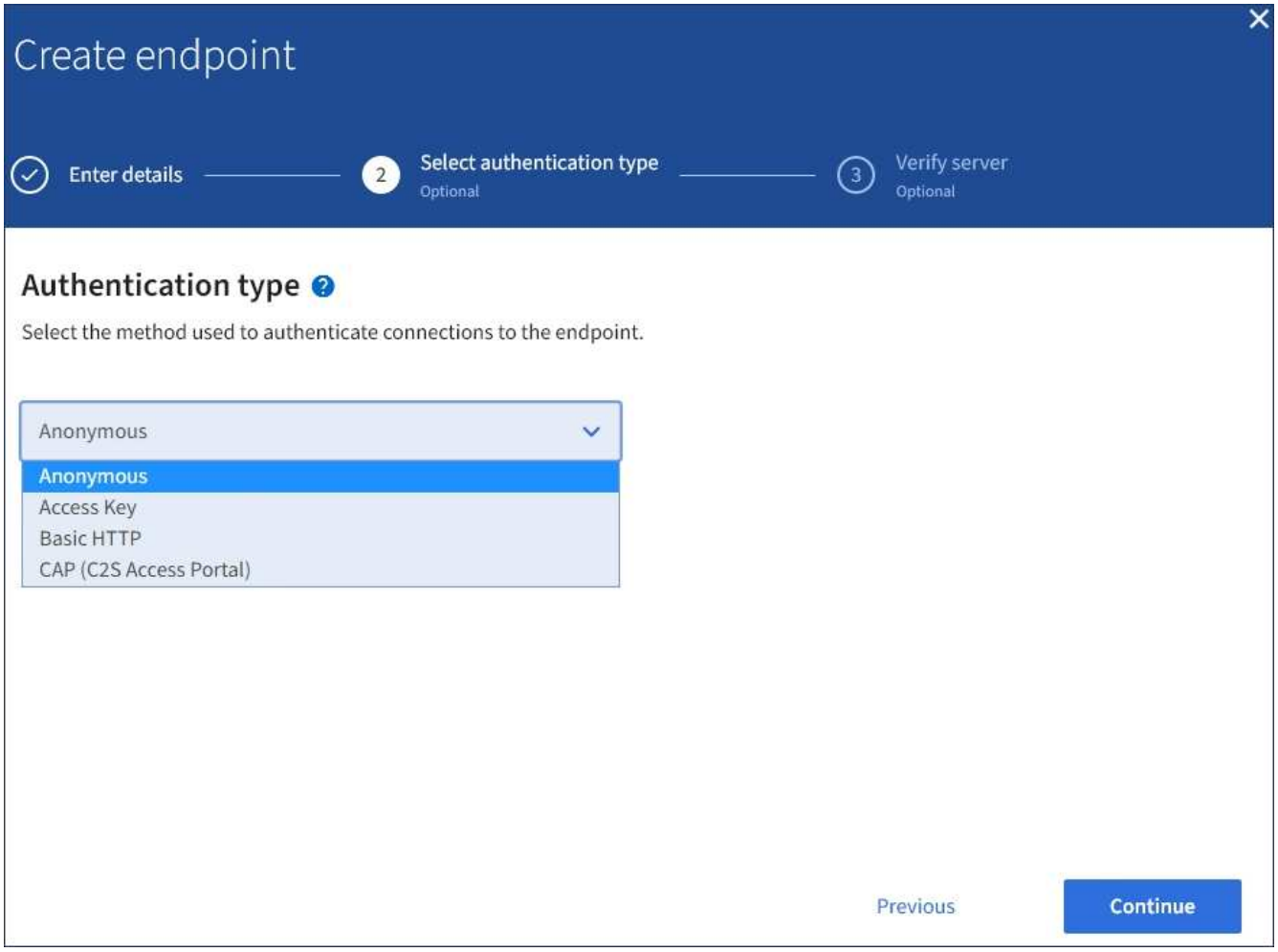
```
https://s3-aws-region.amazonaws.com
```

엔드포인트가 CloudMirror 복제 서비스에 사용되는 경우 버킷 이름을 URI에 포함하지 마십시오. 버킷 이름을 * URN * 필드에 포함시킵니다.

5. 끝점에 대한 고유 URN(리소스 이름)을 입력합니다.

   끝점이 생성된 후에는 끝점의 URN을 변경할 수 없습니다.

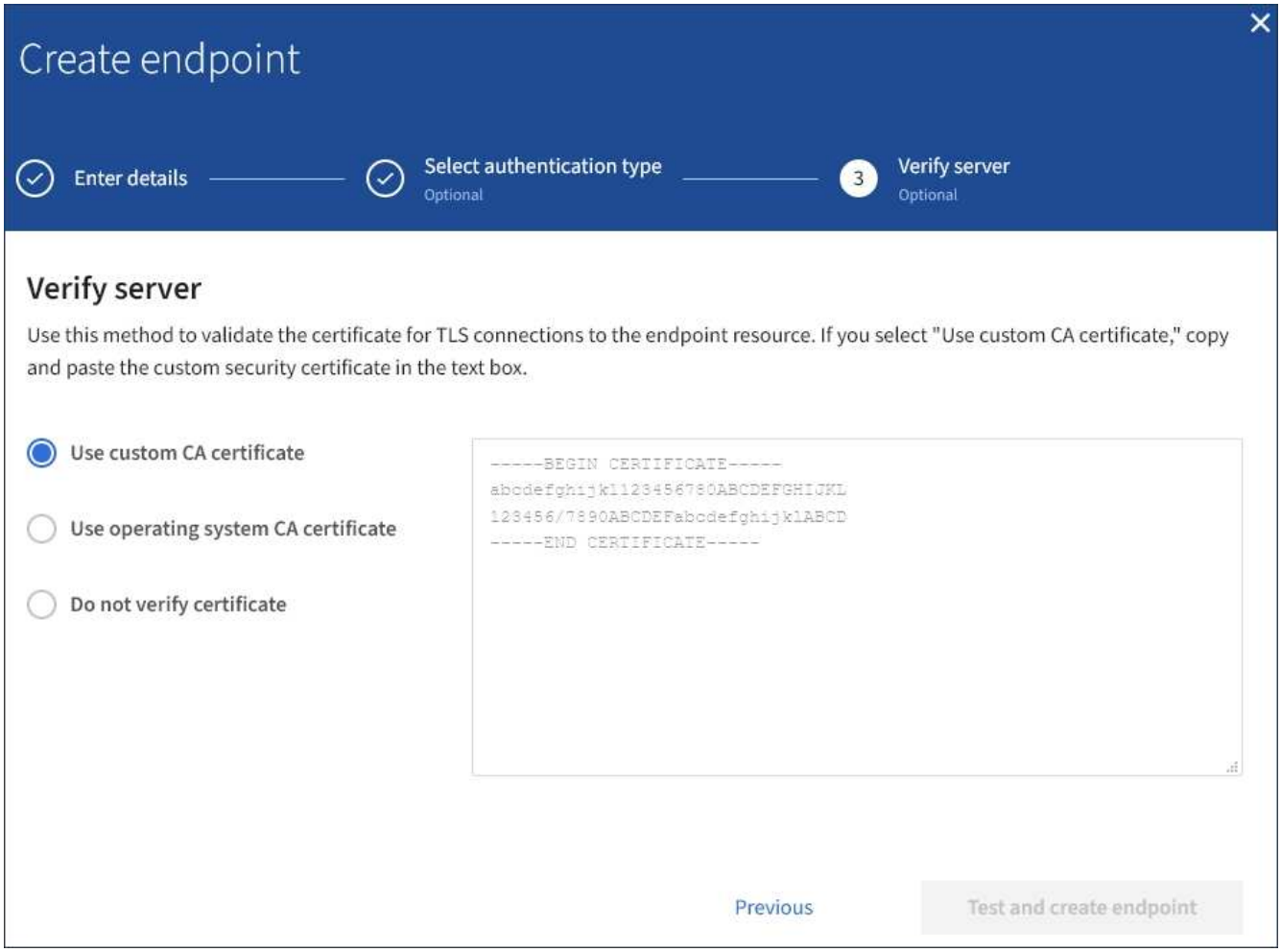
6. Continue * 를 선택합니다.
7. 인증 유형 * 의 값을 선택한 다음 필요한 자격 증명을 입력하거나 업로드합니다.



제공하는 자격 증명에 대상 리소스에 대한 쓰기 권한이 있어야 합니다.

인증 유형입니다	설명	자격 증명
익명	대상에 대한 익명 액세스를 제공합니다. 보안이 비활성화된 끝점에서만 작동합니다.	인증이 없습니다.
액세스 키	AWS 스타일 자격 증명을 사용하여 대상과의 연결을 인증합니다.	• 액세스 키 ID입니다 • 비밀 액세스 키
기본 HTTP	사용자 이름과 암호를 사용하여 대상에 대한 연결을 인증합니다.	• 사용자 이름 • 암호
CAP(C2S 액세스 포털)	인증서 및 키를 사용하여 대상에 대한 연결을 인증합니다.	• 임시 자격 증명 URL입니다 • 서버 CA 인증서(PEM 파일 업로드) • 클라이언트 인증서(PEM 파일 업로드) • 클라이언트 개인 키(PEM 파일 업로드, OpenSSL 암호화 형식 또는 암호화되지 않은 개인 키 형식) • 클라이언트 개인 키 암호 구문(선택 사항)

8. Continue * 를 선택합니다.
9. 끝점에 대한 TLS 연결을 확인하는 방법을 선택하려면 * 서버 확인 * 에 대한 라디오 버튼을 선택합니다.



인증서 확인 유형입니다	설명
사용자 지정 CA 인증서를 사용합니다	사용자 지정 보안 인증서를 사용합니다. 이 설정을 선택한 경우 사용자 지정 보안 인증서를 복사하여 * CA 인증서 * 텍스트 상자에 붙여 넣습니다.
운영 체제 CA 인증서를 사용합니다	운영 체제에 설치된 기본 그리드 CA 인증서를 사용하여 연결을 보호합니다.
인증서를 확인하지 않습니다	TLS 연결에 사용되는 인증서가 검증되지 않았습니다. 이 옵션은 안전하지 않습니다.

10. 테스트를 선택하고 끝점 * 을 작성합니다.
    - 지정된 자격 증명을 사용하여 끝점에 도달할 수 있으면 성공 메시지가 나타납니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.
    - 끝점 유효성 검사에 실패하면 오류 메시지가 나타납니다. 오류를 수정하기 위해 끝점을 수정해야 하는 경우 * 끝점 세부 정보로 돌아가기 * 를 선택하고 정보를 업데이트합니다. 그런 다음 * 테스트 를 선택하고 끝점 * 을 만듭니다.

> 테넌트 계정에 플랫폼 서비스가 활성화되어 있지 않으면 엔드포인트 생성이 실패합니다. StorageGRID 관리자에게 문의하십시오.

끝점을 구성한 후 URN을 사용하여 플랫폼 서비스를 구성할 수 있습니다.

관련 정보

플랫폼 서비스 끝점에 URN을 지정합니다

CloudMirror 복제를 구성합니다

이벤트 알림을 구성합니다

검색 통합 서비스를 구성합니다

플랫폼 서비스 끝점에 대한 연결을 테스트합니다

플랫폼 서비스에 대한 연결이 변경된 경우 끝점에 대한 연결을 테스트하여 대상 리소스가 있는지 그리고 지정한 자격 증명을 사용하여 해당 리소스에 연결할 수 있는지 확인할 수 있습니다.

필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 끝점 관리 권한이 있는 사용자 그룹에 속해야 합니다.

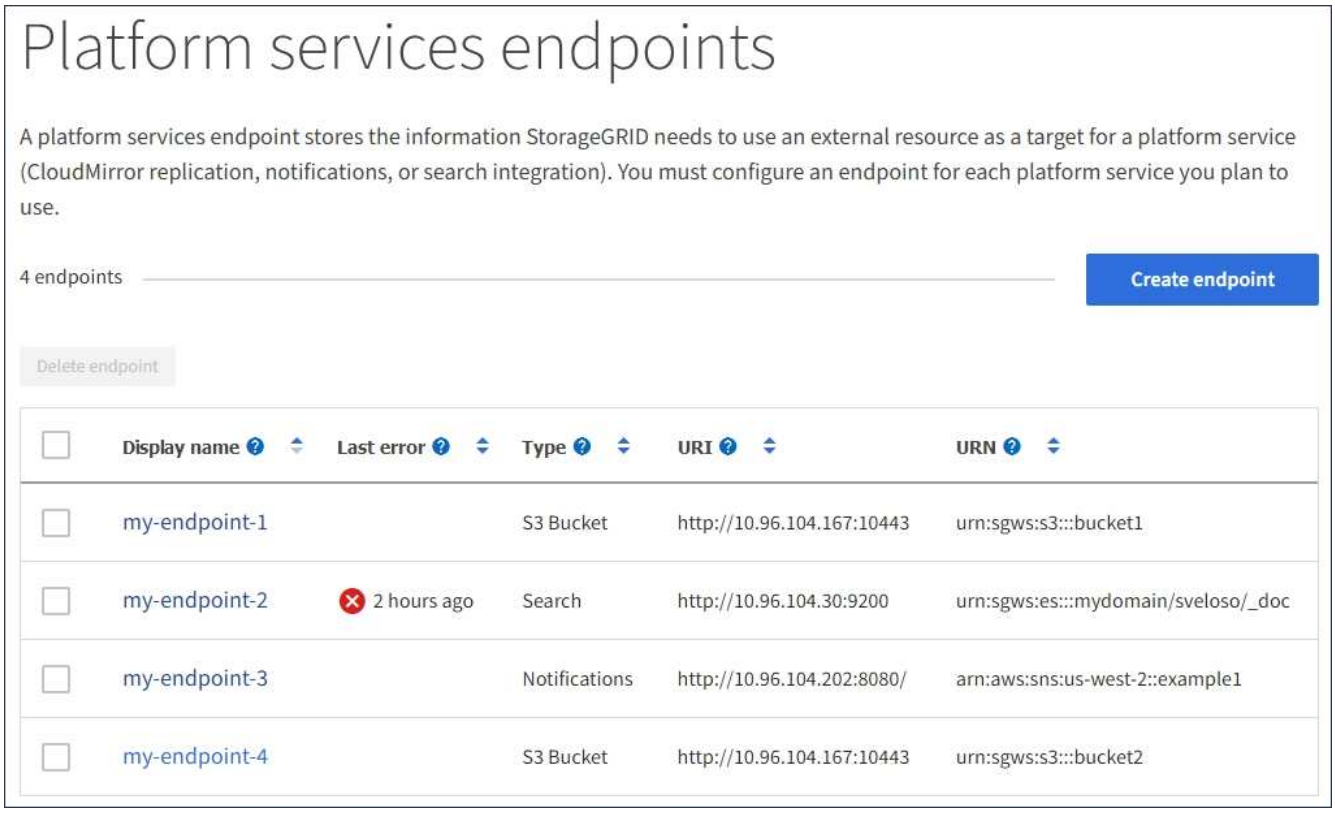
이 작업에 대해

StorageGRID는 자격 증명에 올바른 권한이 있는지 확인하지 않습니다.

단계

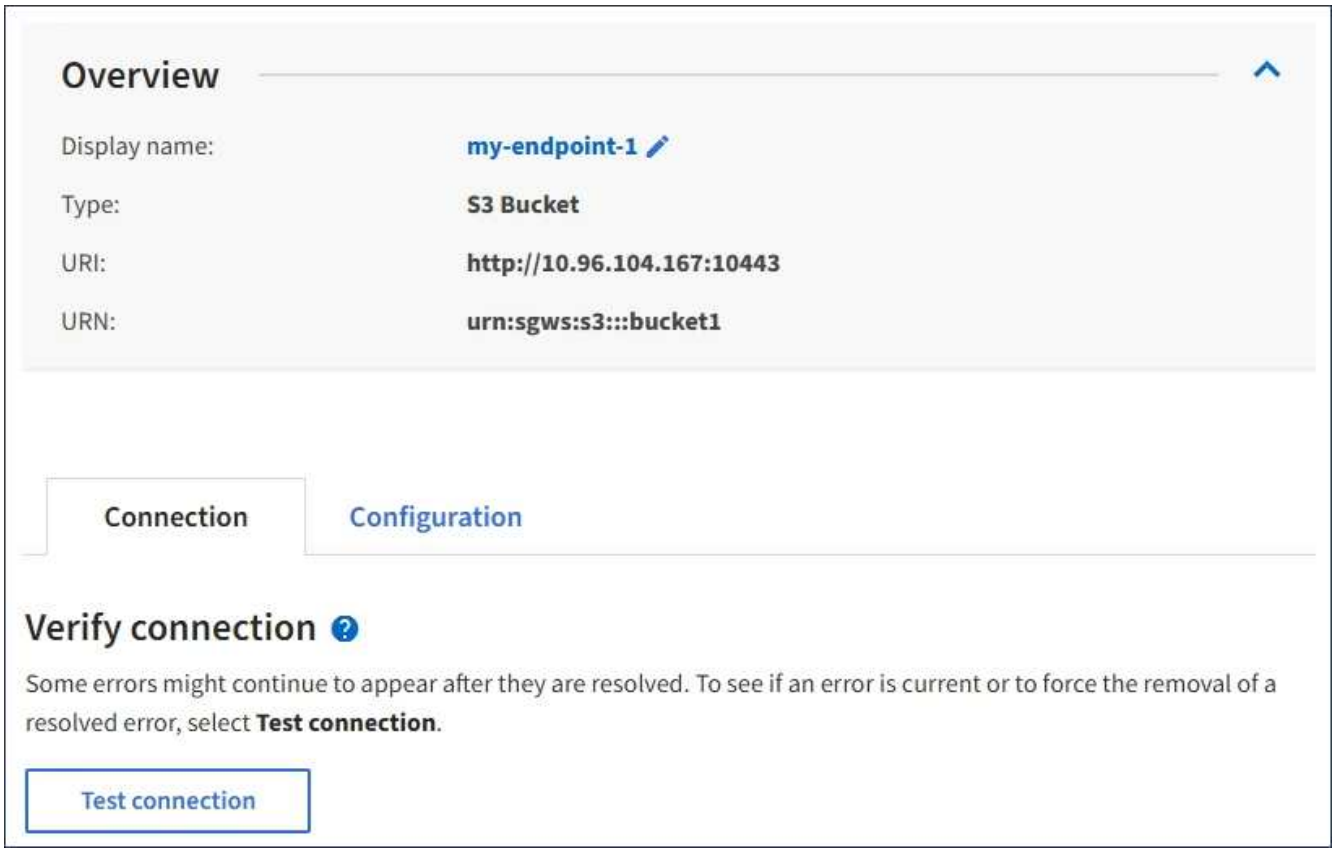
1. 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 * 를 선택합니다.

   플랫폼 서비스 끝점 페이지가 나타나고 이미 구성된 플랫폼 서비스 끝점 목록이 표시됩니다.



2. 연결을 테스트할 끝점을 선택합니다.

   끝점 세부 정보 페이지가 나타납니다.



3. Test connection * 을 선택합니다.
   - 지정된 자격 증명을 사용하여 끝점에 도달할 수 있으면 성공 메시지가 나타납니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.
   - 끝점 유효성 검사에 실패하면 오류 메시지가 나타납니다. 오류를 정정하기 위해 끝점을 수정해야 하는 경우 * 구성 * 을 선택하고 정보를 업데이트합니다. 그런 다음 * 테스트 및 변경 내용 저장 * 을 선택합니다.

플랫폼 서비스 끝점을 편집합니다

플랫폼 서비스 끝점의 구성을 편집하여 이름, URI 또는 기타 세부 정보를 변경할 수 있습니다. 예를 들어 만료된 자격 증명을 업데이트하거나 대체 작동을 위한 백업 Elasticsearch 인덱스를 가리키도록 URI를 변경해야 할 수 있습니다. 플랫폼 서비스 끝점의 URN은 변경할 수 없습니다.

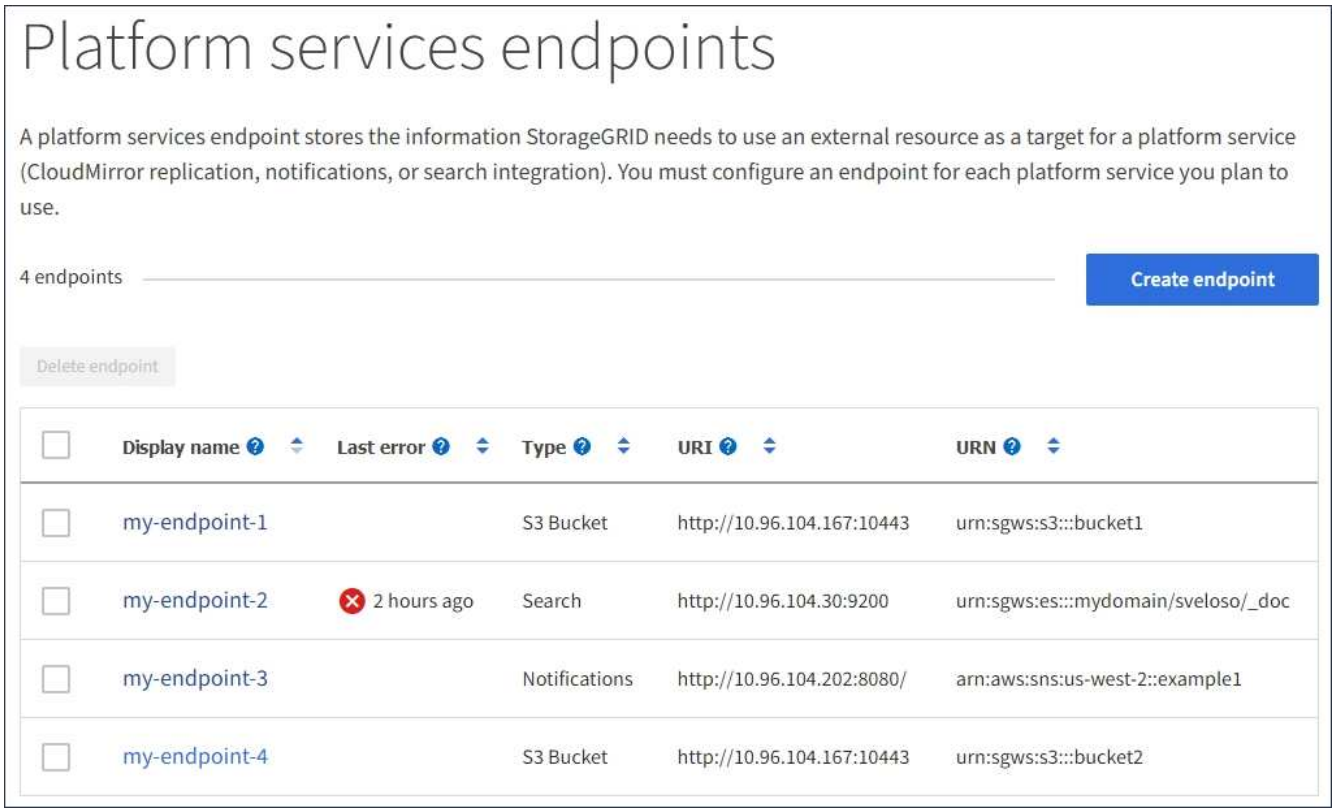
필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 끝점 관리 권한이 있는 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.

단계

1. 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 * 를 선택합니다.

   플랫폼 서비스 끝점 페이지가 나타나고 이미 구성된 플랫폼 서비스 끝점 목록이 표시됩니다.



2. 편집할 끝점을 선택합니다.

   끝점 세부 정보 페이지가 나타납니다.

3. Configuration * 을 선택합니다.

Overview

Display name: my-endpoint-3

Type: Notifications

URI: http://10.96.104.202:8080/

URN: arn:aws:sns:us-west-2::example1

Connection | Configuration

Edit configuration

Endpoint details

URI

http://10.96.104.202:8080/

URN

arn:aws:sns:us-west-2::example1

Authentication type

Basic HTTP

Username

testme

Password

••••••••

Edit password

Verify server

- Use custom CA certificate
- Use operating system CA certificate
- Do not verify certificate

```
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
```

Test and save changes

4. 필요에 따라 끝점의 구성을 변경합니다.

> 끝점이 생성된 후에는 끝점의 URN을 변경할 수 없습니다.

   a. 끝점의 표시 이름을 변경하려면 편집 아이콘을 선택합니다 .
   b. 필요에 따라 URI를 변경합니다.
   c. 필요에 따라 인증 유형을 변경합니다.
      - 액세스 키 인증의 경우 * S3 키 편집 * 을 선택하고 새 액세스 키 ID 및 비밀 액세스 키를 붙여 넣어 필요에 따라 키를 변경합니다. 변경 사항을 취소하려면 * S3 키 편집 되돌리기 * 를 선택합니다.
      - 기본 HTTP 인증의 경우 필요에 따라 사용자 이름을 변경합니다. 필요에 따라 * 암호 편집 * 을 선택하고 새 암호를 입력하여 암호를 변경합니다. 변경 사항을 취소해야 하는 경우 * 암호 편집 되돌리기 * 를 선택합니다.
      - CAP(C2S Access Portal) 인증의 경우 임시 자격 증명 URL 또는 선택적 클라이언트 개인 키 암호를 변경하고 필요에 따라 새 인증서 및 키 파일을 업로드합니다.

        > 클라이언트 개인 키는 OpenSSL 암호화 형식 또는 암호화되지 않은 개인 키 형식이어야 합니다.

   d. 필요에 따라 서버 확인 방법을 변경합니다.
5. Test(테스트)를 선택하고 변경 내용을 저장합니다 *.
   - 지정된 자격 증명을 사용하여 끝점에 도달할 수 있으면 성공 메시지가 나타납니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 확인합니다.
   - 끝점 유효성 검사에 실패하면 오류 메시지가 나타납니다. 끝점을 수정하여 오류를 수정한 다음 * 테스트 및 변경 내용 저장 * 을 선택합니다.

플랫폼 서비스 끝점을 삭제합니다

연결된 플랫폼 서비스를 더 이상 사용하지 않으려면 끝점을 삭제할 수 있습니다.

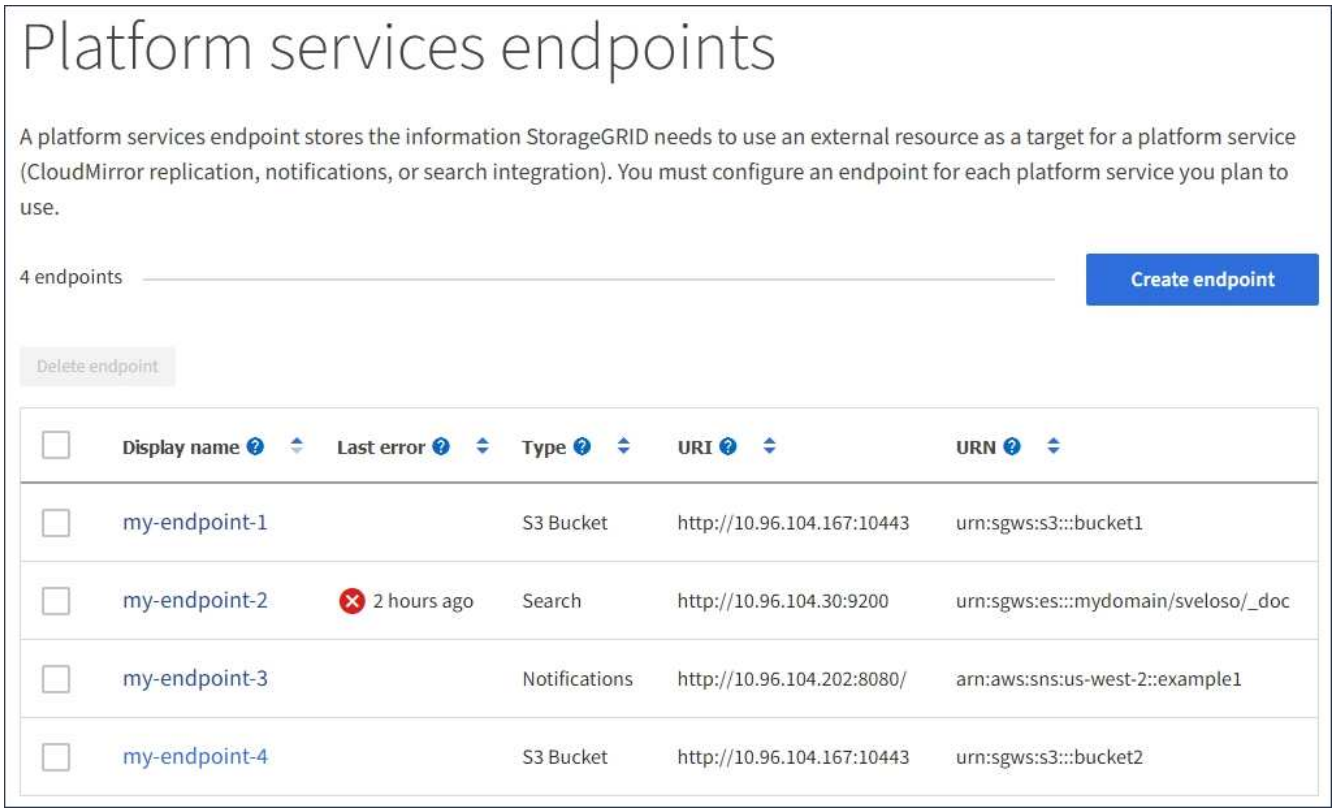
필요한 것

- 를 사용하여 테넌트 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 끝점 관리 * 권한이 있는 사용자 그룹에 속해야 합니다. 을 참조하십시오 테넌트 관리 권한.

단계

1. 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 * 를 선택합니다.

   플랫폼 서비스 끝점 페이지가 나타나고 이미 구성된 플랫폼 서비스 끝점 목록이 표시됩니다.

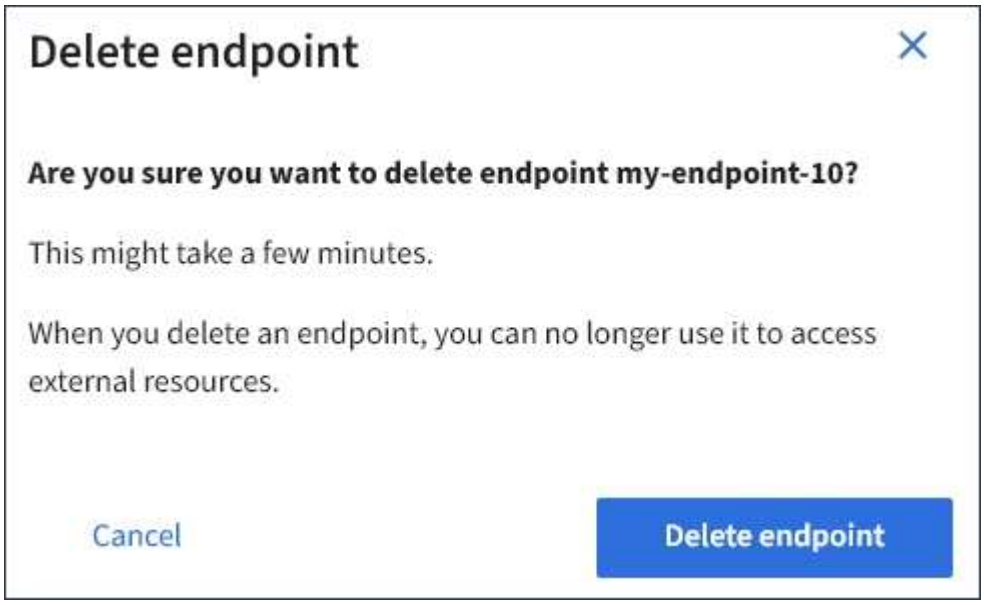


2. 삭제할 각 끝점의 확인란을 선택합니다.

> 사용 중인 플랫폼 서비스 끝점을 삭제하면 해당 끝점을 사용하는 모든 버킷에 대해 연결된 플랫폼 서비스가 비활성화됩니다. 아직 완료되지 않은 요청은 삭제됩니다. 삭제된 URN을 더 이상 참조하지 않도록 버킷 구성을 변경할 때까지 새 요청은 계속 생성됩니다. StorageGRID는 이러한 요청을 복구할 수 없는 오류로 보고합니다.

3. 작업 * > * 끝점 삭제 * 를 선택합니다.

   확인 메시지가 나타납니다.



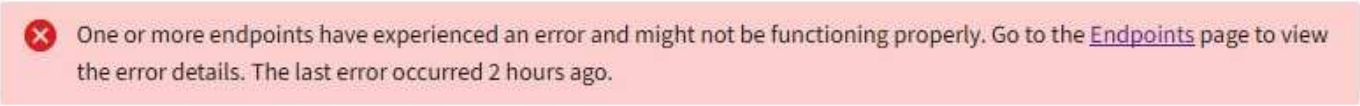
4. 끝점 삭제 * 를 선택합니다.

플랫폼 서비스 끝점 오류 문제 해결

StorageGRID가 플랫폼 서비스 끝점과 통신하려고 할 때 오류가 발생하면 대시보드에 메시지가 표시됩니다. 플랫폼 서비스 끝점 페이지에서 마지막 오류 열은 오류가 발생한 시간을 나타냅니다. 끝점의 자격 증명과 연결된 권한이 올바르지 않으면 오류가 표시되지 않습니다.

오류가 발생했는지 확인합니다

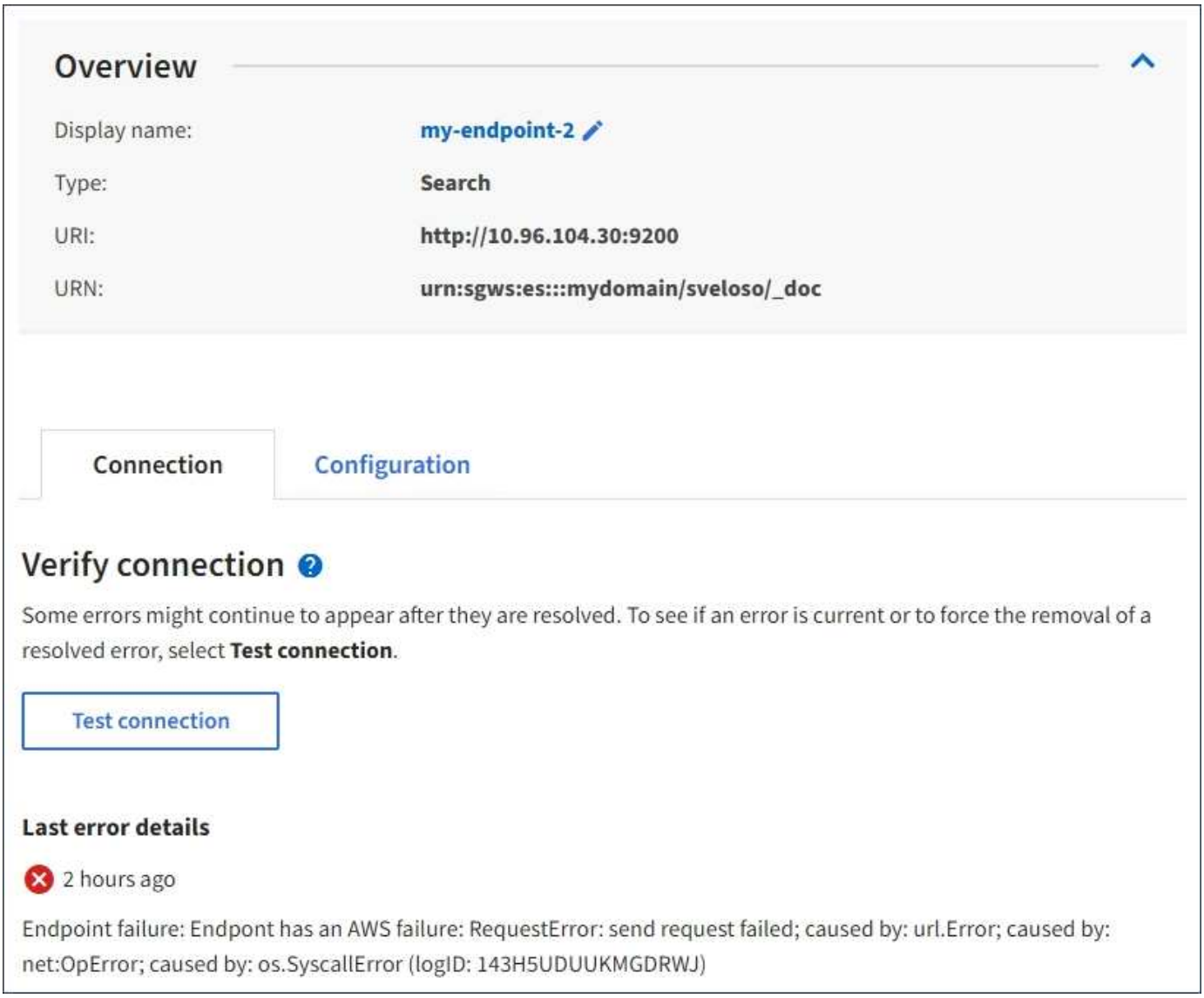
지난 7일 이내에 플랫폼 서비스 끝점 오류가 발생한 경우 테넌트 관리자 대시보드에 경고 메시지가 표시됩니다. 플랫폼 서비스 끝점 페이지로 이동하여 오류에 대한 자세한 정보를 볼 수 있습니다.



대시보드에 나타나는 동일한 오류가 플랫폼 서비스 끝점 페이지 맨 위에도 나타납니다. 자세한 오류 메시지를 보려면:

단계

1. 끝점 목록에서 오류가 있는 끝점을 선택합니다.
2. 끝점 세부 정보 페이지에서 * 연결 * 을 선택합니다. 이 탭은 끝점에 대한 가장 최근 오류만 표시하고 오류가 발생한 시간을 표시합니다. 빨간색 X 아이콘이 포함된 오류 지난 7일 이내에 발생했습니다.



오류가 여전히 최신 상태인지 확인합니다

일부 오류는 해결된 후에도 * 마지막 오류 * 열에 계속 표시될 수 있습니다. 오류가 현재 오류인지 확인하거나 테이블에서 해결된 오류를 강제로 제거하려면 다음과 같이 하십시오.

단계

1. 끝점을 선택합니다.

   끝점 세부 정보 페이지가 나타납니다.

2. 연결 * > * 연결 테스트 * 를 선택합니다.

연결 테스트 * 를 선택하면 StorageGRID가 플랫폼 서비스 끝점이 있는지, 그리고 현재 자격 증명으로 연결할 수 있는지 검증합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

끝점 오류를 해결합니다

끝점 세부 정보 페이지의 * 마지막 오류 * 메시지를 사용하여 오류의 원인을 확인할 수 있습니다. 일부 오류에서는 문제를 해결하기 위해 끝점을 편집해야 할 수 있습니다. 예를 들어, 올바른 액세스 권한이 없거나 액세스 키가 만료되어

StorageGRID가 대상 S3 버킷을 액세스할 수 없는 경우 클라우드미러링 오류가 발생할 수 있습니다. 이 메시지는 ""끝점 자격 증명이나 대상 액세스 업데이트 필요""이며 세부 정보는 ""AccessDenied"" 또는 ""InvalidAccessKeyId""입니다.

오류를 해결하기 위해 끝점을 편집해야 하는 경우 * 테스트 및 변경 내용 저장 * 을 선택하면 StorageGRID가 업데이트된 끝점을 검증하고 현재 자격 증명으로 연결할 수 있는지 확인합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

단계

1. 끝점을 선택합니다.
2. 끝점 세부 정보 페이지에서 * 구성 * 을 선택합니다.
3. 필요에 따라 끝점 설정을 편집합니다.
4. 연결 * > * 연결 테스트 * 를 선택합니다.

권한이 부족한 끝점 자격 증명

StorageGRID에서 플랫폼 서비스 끝점의 유효성을 검사할 때 끝점의 자격 증명을 사용하여 대상 리소스에 연결할 수 있는지 확인하고 기본적인 사용 권한 검사를 수행합니다. 그러나 StorageGRID는 특정 플랫폼 서비스 작업에 필요한 모든 사용 권한의 유효성을 검사하지 않습니다. 따라서 플랫폼 서비스("403 사용 금지" 등)를 사용할 때 오류가 발생하면 끝점의 자격 증명과 관련된 권한을 확인하십시오.

추가 플랫폼 서비스 문제 해결

플랫폼 서비스 문제 해결에 대한 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

StorageGRID 관리

관련 정보

플랫폼 서비스 끝점을 만듭니다

플랫폼 서비스 끝점에 대한 연결을 테스트합니다

플랫폼 서비스 끝점을 편집합니다

CloudMirror 복제를 구성합니다

를 클릭합니다 CloudMirror 복제 서비스 는 세 가지 StorageGRID 플랫폼 서비스 중 하나입니다. CloudMirror 복제를 사용하여 오브젝트를 외부 S3 버킷에 자동으로 복제할 수 있습니다.

필요한 것

- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 사용하도록 설정해야 합니다.
- 복제 소스로 사용할 버킷을 이미 생성해야 합니다.
- CloudMirror 복제의 대상으로 사용하려는 엔드포인트가 이미 있어야 하며 URN이 있어야 합니다.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이 권한을 사용하여 테넌트 계정의 모든 S3 버킷에 대한 설정을 관리할 수 있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업에 대해

CloudMirror 복제는 소스 버킷에서 엔드포인트에 지정된 대상 버킷으로 객체를 복제합니다. 버킷에 대해 CloudMirror 복제를 설정하려면 유효한 버킷 복제 구성 XML을 생성하고 적용해야 합니다. 복제 구성 XML은 각 대상에 대해 S3 버킷 엔드포인트의 URN을 사용해야 합니다.

> S3 오브젝트 잠금이 활성화된 소스 또는 대상 버킷에는 복제가 지원되지 않습니다.

버킷 복제 및 구성 방법에 대한 일반적인 정보는 교차 지역 복제(CRR)에 대한 Amazon Simple Storage Service(S3) 설명서를 참조하십시오. StorageGRID에서 S3 버킷 복제 구성 API를 구현하는 방법에 대한 자세한 내용은 를 참조하십시오 S3 클라이언트 애플리케이션 구현 지침.

객체가 포함된 버킷에서 CloudMirror 복제를 활성화하면 버킷에 추가된 새 객체가 복제되지만 버킷의 기존 객체는 복제되지 않습니다. 복제를 트리거하려면 기존 객체를 업데이트해야 합니다.

복제 구성 XML에서 스토리지 클래스를 지정하는 경우 StorageGRID는 대상 S3 끝점에 대해 작업을 수행할 때 해당 클래스를 사용합니다. 대상 끝점은 지정된 저장소 클래스도 지원해야 합니다. 대상 시스템 공급업체에서 제공하는 권장 사항을 따르십시오.

단계

1. 소스 버킷에 대한 복제 지원:

   텍스트 편집기를 사용하여 S3 복제 API에 지정된 대로 복제를 활성화하는 데 필요한 복제 구성 XML을 생성합니다. XML을 구성할 때:

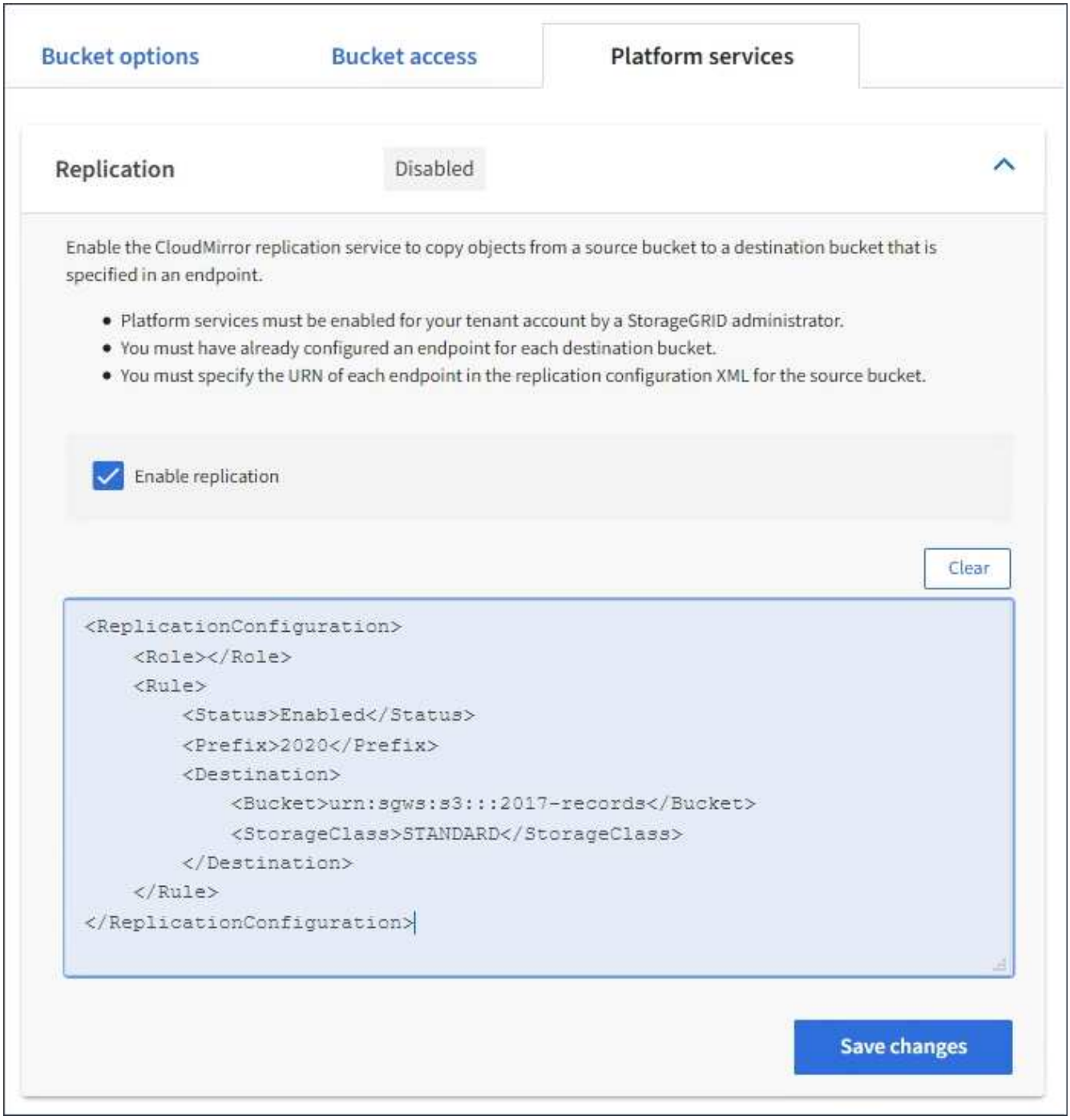
   - StorageGRID는 복제 구성의 V1만 지원합니다. 즉, StorageGRID는 규칙에 대해 'Filter' 요소의 사용을 지원하지 않으며 개체 버전 삭제에 대해서는 V1 규약을 따릅니다. 자세한 내용은 복제 구성에 대한 Amazon 설명서를 참조하십시오.
   - S3 버킷 엔드포인트의 URN을 대상으로 사용합니다.
   - 필요한 경우 "<StorageClass>" 요소를 추가하고 다음 중 하나를 지정합니다.
     - 'Standard': 기본 스토리지 클래스. 객체를 업로드할 때 스토리지 클래스를 지정하지 않으면 '표준' 스토리지 클래스가 사용됩니다.
     - S tandard_IA: (Standard - Infrequent Access) 액세스 빈도가 낮지만 필요한 경우 빠른 액세스가 필요한 데이터에 이 스토리지 클래스를 사용합니다.
     - Reduced_redundancy: standard 스토리지 클래스보다 중복성이 적은 비위험, 재현 가능한 데이터에 이 스토리지 클래스를 사용합니다.
   - 구성 XML에서 Role을 지정하면 무시됩니다. 이 값은 StorageGRID에서 사용되지 않습니다.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. 테넌트 관리자에서 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

4. 플랫폼 서비스 * > * 복제 * 를 선택합니다.
5. 복제 사용 * 확인란을 선택합니다.
6. 복제 구성 XML을 텍스트 상자에 붙여 넣고 * 변경 내용 저장 * 을 선택합니다.



> 그리드 관리자 또는 그리드 관리 API를 사용하여 StorageGRID 관리자가 각 테넌트 계정에 대해 플랫폼 서비스를 활성화해야 합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 복제가 올바르게 구성되었는지 확인합니다.
   a. 복제 구성에 지정된 대로 복제 요구 사항을 충족하는 객체를 소스 버킷에 추가합니다.

      앞서 설명한 예에서는 접두사 "2020"과 일치하는 객체가 복제됩니다.

   b. 객체가 대상 버킷에 복제되었는지 확인합니다.

      오브젝트 크기가 작은 경우 복제가 빠르게 수행됩니다.

관련 정보

S3을 사용합니다

플랫폼 서비스 끝점을 만듭니다

이벤트 알림을 구성합니다

알림 서비스는 세 가지 StorageGRID 플랫폼 서비스 중 하나입니다. 버킷에 대한 알림을 활성화하여 지정된 이벤트에 대한 정보를 AWS SNS(Simple Notification Service ™)를 지원하는 대상 서비스로 전송할 수 있습니다.

필요한 것

- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 사용하도록 설정해야 합니다.
- 알림 소스로 사용하려면 이미 버킷을 만들어야 합니다.
- 이벤트 알림 대상으로 사용하려는 엔드포인트가 이미 있어야 하며 URN이 있어야 합니다.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이 권한을 사용하여 테넌트 계정의 모든 S3 버킷에 대한 설정을 관리할 수 있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업에 대해

이벤트 알림을 구성한 후 소스 버킷의 개체에 대해 지정된 이벤트가 발생할 때마다 알림이 생성되어 대상 끝점으로 사용되는 SNS(Simple Notification Service) 항목으로 전송됩니다. 버킷에 대한 알림을 활성화하려면 유효한 알림 구성 XML을 생성하고 적용해야 합니다. 알림 구성 XML은 각 대상에 대해 이벤트 알림 끝점의 URN을 사용해야 합니다.

이벤트 알림 및 구성 방법에 대한 일반 정보는 아마존 문서를 참조하십시오. StorageGRID에서 S3 버킷 알림 구성 API를 구현하는 방법에 대한 자세한 내용은 S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

객체가 포함된 버킷에 대해 이벤트 알림을 활성화하면 알림 구성이 저장된 후 수행되는 작업에 대해서만 알림이 전송됩니다.

단계

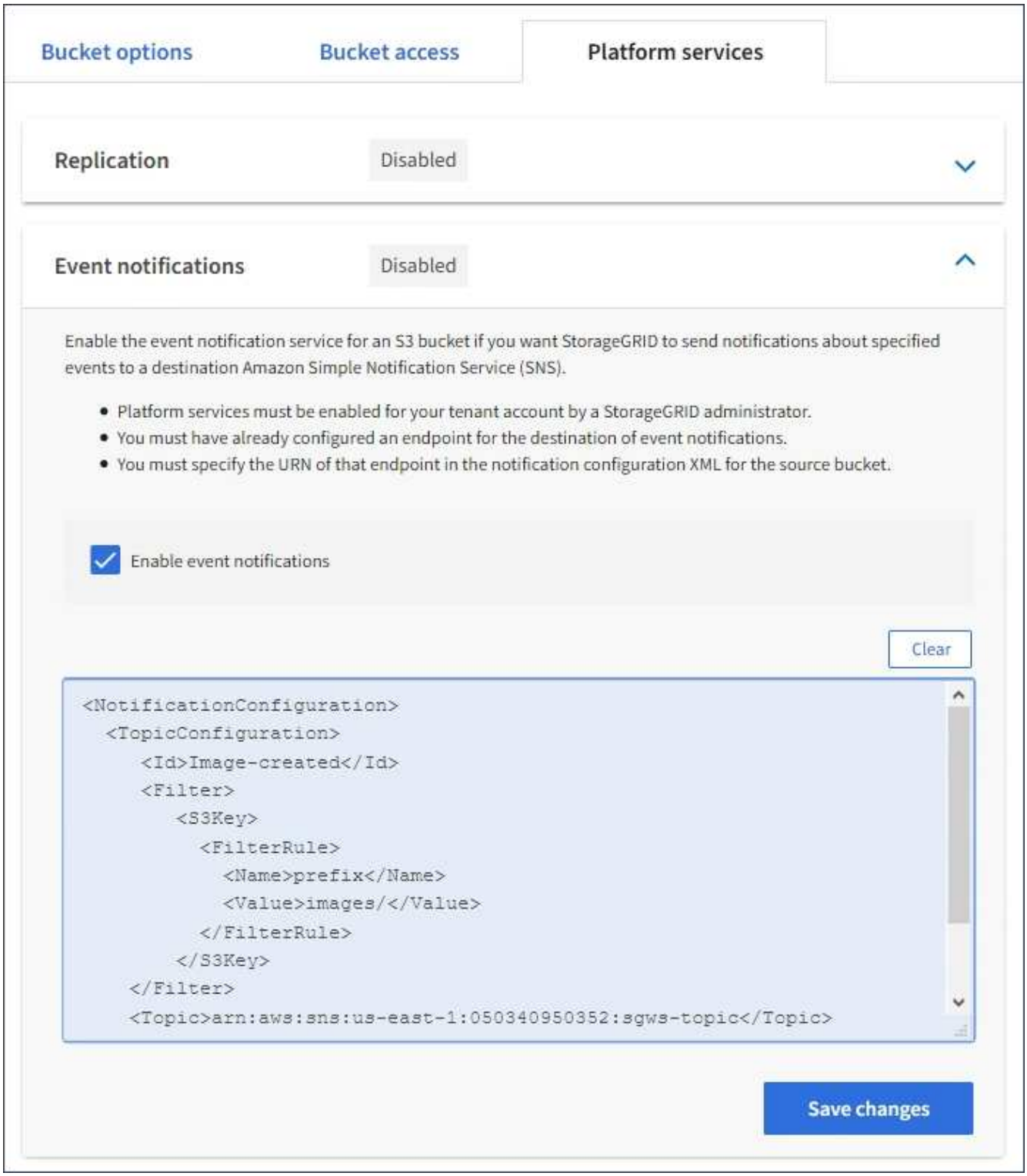
1. 소스 버킷에 대한 알림 활성화:
    - 텍스트 편집기를 사용하여 S3 알림 API에 지정된 대로 이벤트 알림을 활성화하는 데 필요한 알림 구성 XML을 생성합니다.
    - XML을 구성할 때는 이벤트 알림 끝점의 URN을 대상 항목으로 사용합니다.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. 테넌트 관리자에서 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

4. 플랫폼 서비스 * > * 이벤트 알림 * 을 선택합니다.
5. 이벤트 알림 사용 * 확인란을 선택합니다.
6. 알림 구성 XML을 텍스트 상자에 붙여 넣고 * 변경 내용 저장 * 을 선택합니다.



> 그리드 관리자 또는 그리드 관리 API를 사용하여 StorageGRID 관리자가 각 테넌트 계정에 대해 플랫폼 서비스를 활성화해야 합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 이벤트 알림이 올바르게 구성되었는지 확인합니다.

   a. 구성 XML에 구성된 알림을 트리거하기 위한 요구 사항을 충족하는 소스 버킷의 객체에 대한 작업을 수행합니다.

이 예제에서는 "images/" 접두사로 객체를 만들 때마다 이벤트 알림이 전송됩니다.

b. 알림이 대상 SNS 항목으로 전달되었는지 확인합니다.

예를 들어 대상 주제가 AWS SNS(Simple Notification Service)에 호스팅된 경우, 알림 전송 시 이메일을 보내도록 서비스를 구성할 수 있습니다.


```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"1111111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"1111111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```


대상 항목에서 알림이 수신되면 StorageGRID 알림에 대한 소스 버킷을 성공적으로 구성한 것입니다.

관련 정보

버킷에 대한 알림을 이해합니다

S3을 사용합니다

플랫폼 서비스 끝점을 만듭니다

검색 통합 서비스를 사용합니다

검색 통합 서비스는 세 가지 StorageGRID 플랫폼 서비스 중 하나입니다. 오브젝트 생성, 삭제 또는 해당 메타데이터 또는 태그가 업데이트될 때마다 대상 검색 인덱스에 오브젝트 메타데이터를 전송하도록 이 서비스를 활성화할 수 있습니다.

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

> 검색 통합 서비스로 인해 개체 메타데이터가 대상으로 전송되기 때문에 해당 구성 XML을 _ 메타데이터 알림 구성 xml _ 이라고 합니다. 이 구성 XML은 이벤트 알림을 설정하는 데 사용되는 _notification 구성 xml_과 다릅니다.

를 참조하십시오 S3 클라이언트 애플리케이션 구현 지침 다음 사용자 지정 StorageGRID S3 REST API 작업에 대한 자세한 내용은 다음을 참조하십시오.

- 버킷 메타데이터 알림 구성 요청을 삭제합니다
- 버킷 메타데이터 알림 구성 요청을 가져옵니다
- PUT 버킷 메타데이터 알림 구성 요청

관련 정보

검색 통합을 위한 구성 XML

메타데이터 알림에 포함된 개체 메타데이터입니다

JSON이 검색 통합 서비스에 의해 생성되었습니다

검색 통합 서비스를 구성합니다

S3을 사용합니다

검색 통합을 위한 구성 **XML**

검색 통합 서비스는 "<MetadataNotificationConfiguration>" 및 "</MetadataNotificationConfiguration>" 태그에 포함된 규칙 집합을 사용하여 구성됩니다. 각 규칙은 규칙이 적용되는 오브젝트와 StorageGRID가 해당 오브젝트의 메타데이터를 보내야 하는 대상을 지정합니다.

개체 이름의 접두어를 기준으로 개체를 필터링할 수 있습니다. 예를 들어, 접두어 '이미지'가 있는 객체에 대한 메타데이터를 한 대상으로, 접두어 '비디오'가 있는 객체에 대한 메타데이터를 다른 대상으로 전송할 수 있습니다. 중복되는 접두사가 있는 구성은 유효하지 않으며 제출될 때 거부됩니다. 예를 들어 접두사 test를 가진 개체에 대해 하나의 규칙과 접두사 test2 를 가진 개체에 대한 두 번째 규칙을 포함하는 구성은 허용되지 않습니다.

검색 통합 서비스를 위해 생성된 StorageGRID 엔드포인트의 URN을 사용하여 대상을 지정해야 합니다. 이러한 엔드포인트는 Elasticsearch 클러스터에 정의된 인덱스 및 유형을 나타냅니다.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

이 표에서는 메타데이터 알림 구성 XML의 요소에 대해 설명합니다.

이름	설명	필수 요소입니다
MetadataNotificationConfiguration을 참조하십시오	메타데이터 알림의 개체 및 대상을 지정하는 데 사용되는 규칙의 컨테이너 태그입니다. 하나 이상의 규칙 요소가 포함되어 있습니다.	예
규칙	메타데이터를 지정된 인덱스에 추가해야 하는 개체를 식별하는 규칙의 컨테이너 태그입니다. 접두사가 겹치는 규칙은 거부됩니다. MetadataNotificationConfiguration 요소에 포함되어 있습니다.	예
ID입니다	규칙의 고유 식별자입니다. Rule 요소에 포함되어 있습니다.	아니요
상태	상태는 '활성화' 또는 '비활성화'가 될 수 있습니다. 비활성화된 규칙에 대해 어떠한 작업도 수행되지 않습니다. Rule 요소에 포함되어 있습니다.	예

이름	설명	필수 요소입니다
접두어	접두사와 일치하는 개체는 규칙의 영향을 받으며 해당 메타데이터는 지정된 대상으로 전송됩니다. 모든 오브젝트를 일치시키려면 빈 접두사를 지정합니다. Rule 요소에 포함되어 있습니다.	예
목적지	규칙의 대상에 대한 컨테이너 태그입니다. Rule 요소에 포함되어 있습니다.	예
urn	객체 메타데이터가 전송되는 대상의 urn입니다. 다음 속성을 가진 StorageGRID 끝점의 URN이어야 합니다. • 세 번째 요소는 'es'여야 합니다. • URN은 메타데이터가 저장된 인덱스 및 형식으로 domain-name/myindex/MyType 형식으로 끝나야 합니다. 엔드포인트는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성됩니다. 다음과 같은 형식을 취합니다. • "arn:aws:region:account-ID:domain/mydomain/myindex/MyType" • 'urn:mysite:es:::mydomain/myindex/MyType' 구성 XML을 제출하기 전에 끝점을 구성해야 합니다. 그렇지 않으면 404 오류로 인해 구성이 실패합니다. urn은 Destination 요소에 포함됩니다.	예

샘플 메타데이터 알림 구성 XML을 사용하여 고유한 XML을 구성하는 방법을 배웁니다.

모든 개체에 적용되는 메타데이터 알림 구성입니다

이 예제에서 모든 오브젝트의 오브젝트 메타데이터는 동일한 대상으로 전송됩니다.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

두 가지 규칙을 사용하여 메타데이터 알림 구성

이 예에서는 접두사 /images와 일치하는 객체의 객체 메타데이터가 한 대상으로 전송되고 접두사 /videos와 일치하는 객체의 객체 메타데이터는 두 번째 대상으로 전송됩니다.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

관련 정보

S3을 사용합니다

메타데이터 알림에 포함된 개체 메타데이터입니다

JSON이 검색 통합 서비스에 의해 생성되었습니다

검색 통합 서비스를 구성합니다

검색 통합 서비스는 개체가 생성, 삭제 또는 해당 메타데이터 또는 태그가 업데이트될 때마다 대상 검색 인덱스에 개체 메타데이터를 보냅니다.

필요한 것

- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 사용하도록 설정해야 합니다.
- 인덱싱할 콘텐츠가 있는 S3 버킷을 이미 생성해야 합니다.
- 검색 통합 서비스의 대상으로 사용하려는 끝점이 이미 있어야 하며 URN이 있어야 합니다.
- 모든 버킷 관리 또는 루트 액세스 권한이 있는 사용자 그룹에 속해야 합니다. 이 권한을 사용하여 테넌트 계정의 모든 S3 버킷에 대한 설정을 관리할 수 있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업에 대해

소스 버킷에 대한 검색 통합 서비스를 구성한 후 객체를 만들거나 객체의 메타데이터 또는 태그를 업데이트하면 대상 엔드포인트로 객체 메타데이터가 전송됩니다. 이미 객체가 포함된 버킷에 대해 검색 통합 서비스를 활성화하면 기존 객체에 대한 메타데이터 알림이 자동으로 전송되지 않습니다. 이러한 기존 개체를 업데이트하여 대상 검색 인덱스에 해당 메타데이터가 추가되도록 해야 합니다.

단계

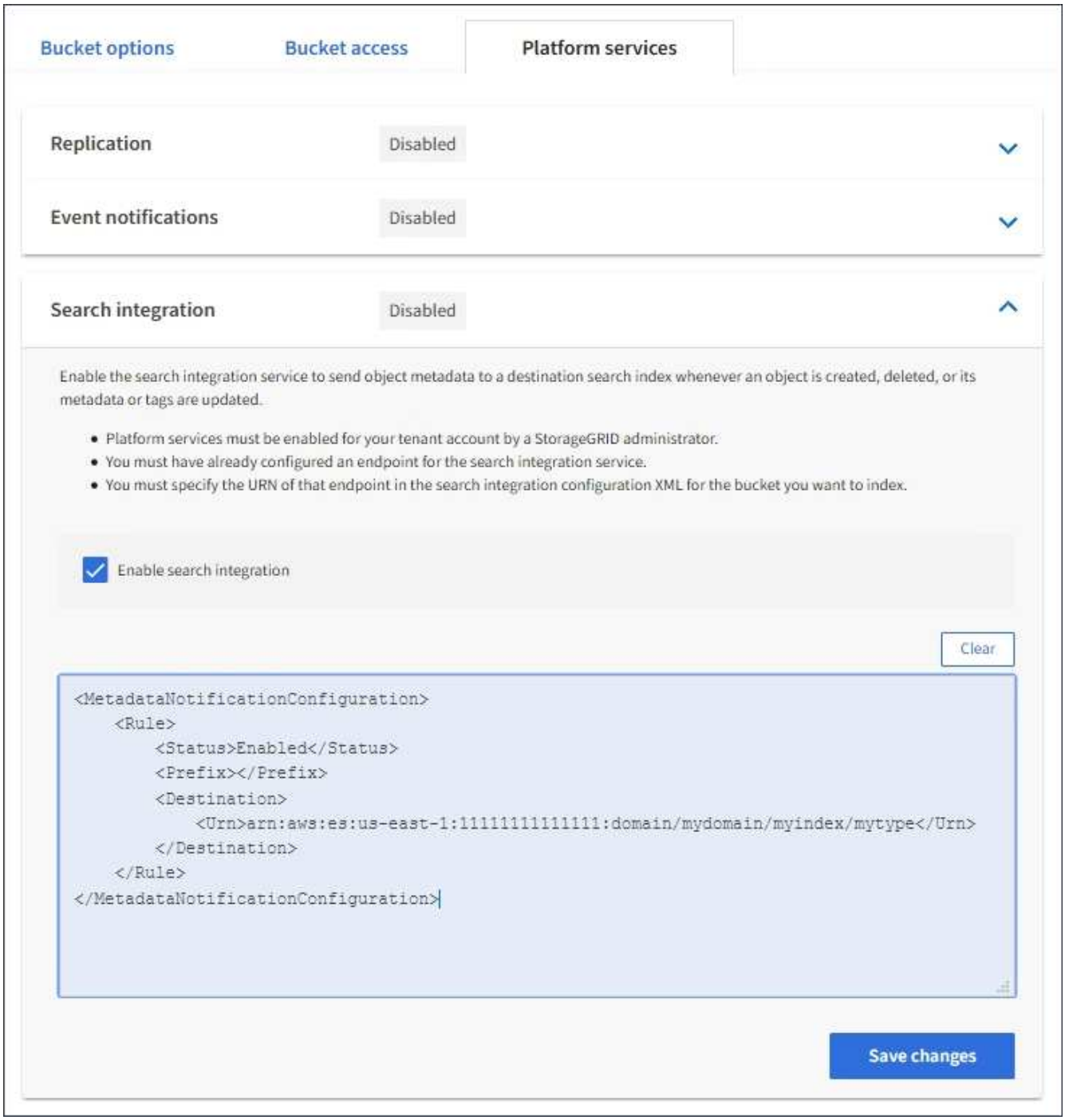
1. 텍스트 편집기를 사용하여 검색 통합을 활성화하는 데 필요한 메타데이터 알림 XML을 만듭니다.
   - 검색 통합을 위한 구성 XML에 대한 정보를 참조하십시오.
   - XML을 구성할 때는 검색 통합 끝점의 URN을 대상으로 사용합니다.

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. 테넌트 관리자에서 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
3. 소스 버킷의 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

4. 플랫폼 서비스 * > * 통합 검색 * 을 선택합니다
5. 검색 통합 사용 * 확인란을 선택합니다.
6. 메타데이터 알림 구성을 텍스트 상자에 붙여 넣고 * 변경 내용 저장 * 을 선택합니다.



> 그리드 관리자 또는 관리 API를 사용하여 StorageGRID 관리자가 각 테넌트 계정에 대해 플랫폼 서비스를 활성화해야 합니다. 구성 XML을 저장할 때 오류가 발생하면 StorageGRID 관리자에게 문의하십시오.

7. 검색 통합 서비스가 올바르게 구성되었는지 확인합니다.
   a. 구성 XML에 지정된 대로 메타데이터 알림을 트리거하기 위한 요구 사항을 충족하는 객체를 소스 버킷에 추가합니다.

      앞의 예제에서 버킷에 추가된 모든 오브젝트는 메타데이터 알림을 트리거합니다.

   b. 개체의 메타데이터와 태그가 포함된 JSON 문서가 끝점에 지정된 검색 인덱스에 추가되었는지 확인합니다.

작업을 마친 후

필요에 따라 다음 방법 중 하나를 사용하여 버킷에 대한 검색 통합을 비활성화할 수 있습니다.

- 스토리지(S3) * > * 버킷 * 을 선택하고 * 검색 통합 활성화 * 확인란의 선택을 취소합니다.
- S3 API를 직접 사용하는 경우 Delete Bucket 메타데이터 알림 요청을 사용합니다. S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

관련 정보

검색 통합 서비스를 이해합니다

검색 통합을 위한 구성 XML

S3을 사용합니다

플랫폼 서비스 끝점을 만듭니다

JSON이 검색 통합 서비스에 의해 생성되었습니다

버킷에 대한 검색 통합 서비스를 활성화하면 개체 메타데이터 또는 태그를 추가, 업데이트 또는 삭제할 때마다 JSON 문서가 생성되어 대상 끝점으로 전송됩니다.

이 예에서는 'test'라는 버킷에 'gws/tagging.txt' 키가 있는 객체가 생성될 때 생성될 수 있는 JSON의 예를 보여 줍니다. 시험용 버킷은 버전 관리가 되지 않아 rionId 태그가 비어 있습니다.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

메타데이터 알림에 포함된 개체 메타데이터입니다

이 표에는 검색 통합이 활성화된 경우 대상 끝점으로 전송되는 JSON 문서에 포함된 모든 필드가 나열됩니다.

문서 이름에는 버킷 이름, 오브젝트 이름 및 버전 ID(있는 경우)가 포함됩니다.

유형	항목 이름 및 설명입니다
버킷 및 오브젝트 정보	버켓 이름
키 : 개체 키 이름	거장된 버킷을 가진 개체의 개체 버전
'리기온': '우동-1'과 같은 버켓 지역	시스템 메타데이터
'크기': HTTP 클라이언트에 표시되는 개체 크기(바이트)입니다	'mD5': 객체 해시
사용자 메타데이터	metadata: 객체에 대한 모든 사용자 메타데이터를 키 값 쌍으로 사용합니다 키: 값
태그	"태그": 오브젝트에 대해 정의된 모든 오브젝트 태그는 키 값 쌍으로 제공됩니다 키: 값

태그 및 사용자 메타데이터의 경우 StorageGRID는 날짜 및 숫자를 Elasticsearch에 문자열 또는 S3 이벤트 알림으로 전달합니다. 이러한 문자열을 날짜 또는 숫자로 해석하도록 Elasticsearch를 구성하려면 동적 필드 매핑 및 날짜 형식 매핑에 대한 Elasticsearch 지침을 따르십시오. 검색 통합 서비스를 구성하기 전에 인덱스에서 동적 필드 매핑을 활성화해야 합니다. 문서가 인덱싱된 후에는 인덱스에서 문서의 필드 형식을 편집할 수 없습니다.

S3을 사용합니다

S3:개요를 사용합니다

StorageGRID는 REST(Representational State Transfer) 웹 서비스 세트로 구현되는 S3(Simple Storage Service) API를 지원합니다. S3 REST API를 지원하므로 StorageGRID 시스템을 사용하는 사내 오브젝트 스토리지와 S3 웹 서비스를 위해 개발된 서비스 지향 애플리케이션을 연결할 수 있습니다. 따라서 클라이언트 애플리케이션의 현재 S3 REST API 호출 사용에 대한 변경이 최소화됩니다.

S3 REST API 지원으로 변경

S3 REST API에 대한 StorageGRID 시스템의 지원 변경사항을 알고 있어야 합니다.

놓습니다	설명
11.6	• 객체 가져오기 및 헤드 객체 요청에 'PARTNUMBER' 요청 매개 변수 사용 지원 추가 • S3 오브젝트 잠금의 버킷 레벨에서 기본 보존 모드 및 기본 보존 기간에 대한 지원이 추가되었습니다. • 객체에 대해 허용 가능한 보존 기간 범위를 설정하기 위해 '객체 잠금 잔여 보존 기간' 정책 조건 키에 대한 지원이 추가되었습니다. • 단일 PUT 오브젝트 작업의 maximum_recommended_size가 이제 5GiB(5,368,709,120바이트)입니다. 5GiB보다 큰 객체가 있는 경우 대신 멀티파트 업로드를 사용합니다. ⓘ StorageGRID 11.6에서 단일 PUT 객체 작업에 대한 Maximum_supported_size는 5TiB로 유지됩니다(5,497,558,138,880 바이트). 그러나 5GiB를 초과하는 개체를 업로드하려고 하면 * S3 PUT 오브젝트 크기가 너무 큼 * 경고가 트리거됩니다.
11.5	• 버킷 암호화 관리에 대한 지원이 추가되었습니다. • S3 오브젝트 잠금 및 더 이상 사용되지 않는 레거시 규정 준수 요청에 대한 지원 추가 • 버전이 있는 버킷에서 여러 오브젝트 삭제 사용에 대한 지원이 추가되었습니다. • Content-MD5 요청 헤더가 올바르게 지원됩니다.
11.4	• 버킷 태그 삭제, 버킷 태그 지정 가져오기 및 버킷 태그 지정을 위한 지원이 추가되었습니다. 비용 할당 태그는 지원되지 않습니다. • StorageGRID 11.4에서 만든 버킷의 경우 성능 모범 사례에 맞게 개체 키 이름을 제한하는 것이 더 이상 필요하지 않습니다. • '3:ObjectRestore:Post' 이벤트 유형에 대한 버킷 알림 지원이 추가되었습니다. • 이제 여러 파트에 대한 AWS 크기 제한이 적용됩니다. 멀티파트 업로드의 각 파트는 5MiB에서 5GiB 사이여야 합니다. 마지막 부분은 5MiB보다 작을 수 있습니다. • TLS 1.3에 대한 지원 및 지원되는 TLS 암호 제품군의 업데이트된 목록이 추가되었습니다. • CLB 서비스는 더 이상 사용되지 않습니다.
11.3	• 고객이 제공한 키(SSE-C)를 사용하여 오브젝트 데이터의 서버측 암호화에 대한 지원이 추가되었습니다. • Bucket 수명주기 작업(만료 작업에만 해당) 및 "x-amz-expiration" 응답 헤더에 대한 삭제, 가져오기 및 PUT 지원이 추가되었습니다. • 수집 시 동기식 배치를 사용하는 ILM 규칙의 영향을 설명하기 위해 PUT 개체, Put Object-Copy 및 MultiPart Upload가 업데이트되었습니다. • 지원되는 TLS 암호 그룹 목록이 업데이트되었습니다. TLS 1.1 암호가 더 이상 지원되지 않습니다.

놓습니다	설명
11.2	클라우드 스토리지 풀과 함께 사용할 POST 오브젝트 복원에 대한 지원이 추가되었습니다. 그룹 및 버킷 정책에서 ARN, 정책 조건 키 및 정책 변수에 대해 AWS 구문 사용을 지원합니다. StorageGRID 구문을 사용하는 기존 그룹 및 버킷 정책은 계속 지원됩니다. • 참고: * 사용자 지정 StorageGRID 기능에 사용되는 것을 포함하여 다른 구성 JSON/XML에서 ARN/URN을 사용하는 것은 변경되지 않았습니다.
11.1	CORS(Cross-Origin Resource Sharing), 그리드 노드에 대한 S3 클라이언트 연결을 위한 HTTP 및 버킷의 규정 준수 설정에 대한 지원이 추가되었습니다.
11.0	버킷에 대한 플랫폼 서비스(CloudMirror 복제, 알림 및 Elasticsearch 검색 통합) 구성 지원 추가 또한 버킷에 대한 객체 태그 지정 위치 제약 조건 및 사용 가능한 정합성 제어 설정에 대한 지원이 추가되었습니다.
10.4	버전 관리, 끝점 도메인 이름 페이지 업데이트, 정책, 정책 예제 및 PutOverwriteObject 권한에 대한 ILM 검색 변경 사항에 대한 지원이 추가되었습니다.
10.3	버전 관리 지원 추가.
10.2	그룹 및 버킷 액세스 정책 및 다중 파트 복제본(업로드 부분 복사)에 대한 지원이 추가되었습니다.
10.1	멀티파트 업로드, 가상 호스팅 스타일 요청 및 v4 인증에 대한 지원이 추가되었습니다.
10.0	StorageGRID 시스템에서 S3 REST API의 초기 지원. 현재 지원되는 _Simple Storage Service API Reference_는 2006-03-01입니다.

지원되는 버전

StorageGRID는 다음과 같은 S3 및 HTTP 버전을 지원합니다.

항목	버전
S3 사양	_Simple Storage Service API Reference_2006-03-01
HTTP	1.1 HTTP에 대한 자세한 내용은 HTTP/1.1(RFC 7230-35)을 참조하십시오. • 참고 *: StorageGRID는 HTTP/1.1 파이프라이닝을 지원하지 않습니다.

관련 정보

"IETF RFC 2616:HTTP/1.1(Hypertext Transfer Protocol)"

"AWS(Amazon Web Services) 문서: Amazon Simple Storage Service API Reference 를 참조하십시오"

StorageGRID 플랫폼 서비스 지원

StorageGRID 플랫폼 서비스를 사용하면 StorageGRID 테넌트 계정에서 원격 S3 버킷, SNS(Simple Notification Service) 엔드포인트 또는 Elasticsearch 클러스터와 같은 외부 서비스를 활용하여 그리드에 의해 제공되는 서비스를 확장할 수 있습니다.

다음 표에는 사용 가능한 플랫폼 서비스와 이를 구성하는 데 사용되는 S3 API가 요약되어 있습니다.

플랫폼 서비스	목적	**S3 API**를 사용하여 서비스를 구성합니다
CloudMirror 복제	소스 StorageGRID 버킷에서 구성된 원격 S3 버킷으로 오브젝트를 복제합니다.	버킷 복제를 배치합니다
알림	소스 StorageGRID 버킷의 이벤트에 대한 알림을 구성된 SNS(Simple Notification Service) 엔드포인트로 보냅니다.	버킷 통지를 보냅니다
검색 통합	StorageGRID 버킷에 저장된 객체에 대한 객체 메타데이터를 구성된 Elasticsearch 인덱스로 전송합니다.	Bucket 메타데이터 알림을 배치합니다 • 참고: * 이것은 StorageGRID 사용자 정의 S3 API입니다.

그리드 관리자는 테넌트 계정에 대해 플랫폼 서비스를 사용하도록 설정해야 사용할 수 있습니다. 그런 다음 테넌트 관리자는 테넌트 계정의 원격 서비스를 나타내는 끝점을 만들어야 합니다. 서비스를 구성하려면 이 단계가 필요합니다.

플랫폼 서비스 사용을 위한 권장 사항

플랫폼 서비스를 사용하기 전에 다음 권장 사항을 숙지해야 합니다.

- CloudMirror 복제, 알림 및 검색 통합이 필요한 S3 요청을 가진 활성 테넌트 100개 이상을 허용하지 않는 것이 좋습니다. 활성 테넌트가 100개 이상인 경우 S3 클라이언트 성능이 저하될 수 있습니다.
- StorageGRID 시스템의 S3 버켓에서 버전 관리 및 CloudMirror 복제를 모두 사용하는 경우, 대상 엔드포인트에 S3 버킷 버전 관리도 활성화할 것을 권장합니다. 이를 통해 CloudMirror 복제가 엔드포인트에 비슷한 개체 버전을 생성할 수 있습니다.
- 소스 버킷에 S3 오브젝트 잠금이 설정된 경우 CloudMirror 복제가 지원되지 않습니다.
- 대상 버킷에 레거시 규정 준수 기능이 설정된 경우 CloudMirror 복제가 실패하고 AccessDenied 오류가 표시됩니다.

관련 정보

테넌트 계정을 사용합니다

StorageGRID 관리

버킷 작업

PUT 버킷 메타데이터 알림 구성 요청

테넌트 계정 및 연결을 구성합니다

클라이언트 응용 프로그램에서 연결을 허용하도록 StorageGRID를 구성하려면 하나 이상의 테넌트 계정을 만들고 연결을 설정해야 합니다.

S3 테넌트 계정 생성 및 구성

S3 API 클라이언트가 StorageGRID에 오브젝트를 저장하고 검색할 수 있으려면 먼저 S3 테넌트 계정이 필요합니다. 각 테넌트 계정에는 고유한 계정 ID, 그룹 및 사용자, 컨테이너 및 객체가 있습니다.

S3 테넌트 계정은 StorageGRID 그리드 관리자가 그리드 관리자 또는 그리드 관리 API를 사용하여 생성합니다. S3 테넌트 계정을 생성할 때 그리드 관리자는 다음 정보를 지정합니다.

- 테넌트의 표시 이름(테넌트의 계정 ID가 자동으로 할당되며 변경할 수 없음)
- 테넌트 계정이 플랫폼 서비스를 사용하도록 허용되는지 여부 플랫폼 서비스를 사용할 수 있는 경우 그리드 사용을 지원하도록 구성해야 합니다.
- 필요한 경우 테넌트 계정의 스토리지 할당량 — 테넌트의 객체에 사용할 수 있는 최대 GB, 테라바이트 또는 PB입니다. 테넌트의 스토리지 할당량은 물리적 크기(디스크 크기)가 아닌 논리적 양(오브젝트 크기)을 나타냅니다.
- StorageGRID 시스템에 대해 ID 페더레이션이 설정된 경우 테넌트 계정을 구성할 수 있는 루트 액세스 권한이 있는 통합 그룹입니다.
- StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하지 않는 경우 테넌트 계정이 자체 ID 소스를 사용할지 또는 그리드의 ID 소스를 공유할지 여부 및 테넌트의 로컬 루트 사용자의 초기 암호를 공유할지 여부

S3 테넌트 계정이 생성된 후 테넌트 사용자는 테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 소스를 그리드와 공유하지 않는 경우 ID 페더레이션을 설정하고 로컬 그룹 및 사용자를 만듭니다
- S3 액세스 키를 관리합니다
- S3 오브젝트 잠금이 설정된 버킷을 포함하여 S3 버킷을 생성하고 관리합니다
- 플랫폼 서비스 사용(활성화된 경우)
- 스토리지 사용량을 모니터링합니다

> S3 테넌트 사용자는 테넌트 관리자를 사용하여 S3 버킷을 생성 및 관리할 수 있지만, S3 액세스 키를 가지고 S3 REST API를 사용하여 오브젝트를 수집 및 관리해야 합니다.

관련 정보

StorageGRID 관리

테넌트 계정을 사용합니다

클라이언트 연결 구성 방법

그리드 관리자는 S3 클라이언트가 StorageGRID에 연결하여 데이터를 저장 및 검색하는 방법에 영향을 주는 구성을 선택합니다. 연결에 필요한 특정 정보는 선택한 구성에 따라 다릅니다.

클라이언트 응용 프로그램은 다음 중 하나를 연결하여 개체를 저장하거나 검색할 수 있습니다.

- 관리 노드 또는 게이트웨이 노드의 부하 분산 서비스 또는 선택적으로 관리 노드 또는 게이트웨이 노드의 고가용성(HA) 그룹의 가상 IP 주소입니다
- 게이트웨이 노드의 CLB 서비스 또는 게이트웨이 노드의 고가용성 그룹의 가상 IP 주소(선택 사항)입니다

> CLB 서비스는 더 이상 사용되지 않습니다. StorageGRID 11.3 릴리스 전에 구성된 클라이언트는 게이트웨이 노드에서 CLB 서비스를 계속 사용할 수 있습니다. 로드 밸런싱을 제공하기 위해 StorageGRID에 의존하는 다른 모든 클라이언트 애플리케이션은 로드 밸런서 서비스를 사용하여 연결해야 합니다.

- 외부 로드 밸런서가 있거나 없는 스토리지 노드

StorageGRID를 구성할 때 그리드 관리자는 그리드 관리자 또는 그리드 관리 API를 사용하여 다음 단계를 수행할 수 있습니다. 이 모든 단계는 선택 사항입니다.

1. 로드 밸런서 서비스의 끝점을 구성합니다.

   로드 밸런서 서비스를 사용하려면 끝점을 구성해야 합니다. 관리 노드 또는 게이트웨이 노드의 부하 분산 서비스는 들어오는 네트워크 연결을 클라이언트 애플리케이션에서 스토리지 노드로 분산합니다. 로드 밸런서 끝점을 만들 때 StorageGRID 관리자는 포트 번호, 엔드포인트가 HTTP 또는 HTTPS 연결을 수락하는지 여부, 엔드포인트를 사용할 클라이언트 유형(S3 또는 Swift) 및 HTTPS 연결에 사용할 인증서(해당하는 경우)를 지정합니다.

2. 신뢰할 수 없는 클라이언트 네트워크를 구성합니다.

   StorageGRID 관리자가 노드의 클라이언트 네트워크를 신뢰할 수 없도록 구성하는 경우 노드는 로드 밸런서 끝점으로 명시적으로 구성된 포트의 클라이언트 네트워크에서 인바운드 연결만 허용합니다.

3. 고가용성 그룹을 구성합니다.

   관리자가 HA 그룹을 생성하면 여러 관리 노드 또는 게이트웨이 노드의 네트워크 인터페이스가 액티브-백업 구성에 배치됩니다. HA 그룹의 가상 IP 주소를 사용하여 클라이언트 연결이 이루어집니다.

각 옵션에 대한 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

관련 정보

StorageGRID 관리

요약**:** 클라이언트 연결을 위한 **IP** 주소 및 포트

클라이언트 애플리케이션은 그리드 노드의 IP 주소와 해당 노드의 서비스 포트 번호를 사용하여 StorageGRID에 접속합니다. HA(고가용성) 그룹이 구성되어 있는 경우 클라이언트 애플리케이션은 HA 그룹의 가상 IP 주소를 사용하여 연결할 수 있습니다.

클라이언트 연결을 만드는 데 필요한 정보입니다

이 표에는 클라이언트가 StorageGRID에 연결할 수 있는 다양한 방법과 각 연결 유형에 사용되는 IP 주소 및 포트가 요약되어 있습니다. 자세한 내용은 StorageGRID 관리자에게 문의하거나 StorageGRID 관리 지침 에서 그리드 관리자에서 이 정보를 찾는 방법에 대한 설명을 참조하십시오.

연결 위치	클라이언트가 연결하는 서비스입니다	**IP** 주소입니다	포트
HA 그룹	로드 밸런서	HA 그룹의 가상 IP 주소입니다	• 로드 밸런서 엔드포인트 포트
HA 그룹	CLB 참고:** CLB 서비스는 더 이상 사용되지 않습니다.	HA 그룹의 가상 IP 주소입니다	기본 S3 포트: • HTTPS: 8082 • HTTP: 8084
관리자 노드	로드 밸런서	관리 노드의 IP 주소입니다	• 로드 밸런서 엔드포인트 포트
게이트웨이 노드	로드 밸런서	게이트웨이 노드의 IP 주소입니다	• 로드 밸런서 엔드포인트 포트
게이트웨이 노드	CLB 참고:** CLB 서비스는 더 이상 사용되지 않습니다.	게이트웨이 노드의 IP 주소입니다 • 참고:** 기본적으로 CLB 및 LDR에 대한 HTTP 포트는 사용되지 않습니다.	기본 S3 포트: • HTTPS: 8082 • HTTP: 8084
스토리지 노드	LDR	스토리지 노드의 IP 주소입니다	기본 S3 포트: • HTTPS: 18082 • HTTP: 18084

예

S3 클라이언트를 게이트웨이 노드 HA 그룹의 로드 밸런서 끝점에 연결하려면 아래와 같이 구조화된 URL을 사용합니다.

- "https://*VIP-of-HA-group*:_LB-endpoint-port_`

예를 들어 HA 그룹의 가상 IP 주소가 192.0.2.5이고 S3 로드 밸런서 끝점의 포트 번호가 10443인 경우 S3 클라이언트는 다음 URL을 사용하여 StorageGRID에 연결할 수 있습니다.

- "https://192.0.2.5:10443`

클라이언트가 StorageGRID에 연결하는 데 사용하는 IP 주소에 대한 DNS 이름을 구성할 수 있습니다. 로컬 네트워크 관리자에게 문의하십시오.

관련 정보

StorageGRID 관리

HTTPS 또는 **HTTP** 연결을 사용하도록 결정합니다

로드 밸런서 끝점을 사용하여 클라이언트 연결을 만들 때는 해당 끝점에 지정된 프로토콜(HTTP 또는 HTTPS)을 사용하여 연결해야 합니다. 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 대한 클라이언트 연결에 HTTP를 사용하려면 해당 사용을 설정해야 합니다.

기본적으로 클라이언트 응용 프로그램이 게이트웨이 노드의 스토리지 노드 또는 CLB 서비스에 연결할 때는 모든 연결에 암호화된 HTTPS를 사용해야 합니다. 선택적으로 Grid Manager에서 * HTTP Connection * 그리드 사용 옵션을 선택하여 보안성이 떨어지는 HTTP 연결을 활성화할 수 있습니다. 예를 들어, 클라이언트 애플리케이션은 비운영 환경에서 스토리지 노드에 대한 접속을 테스트할 때 HTTP를 사용할 수 있습니다.

> 요청은 암호화되지 않은 상태로 전송되므로 프로덕션 그리드에 대해 HTTP를 설정할 때는 주의해야 합니다.

> CLB 서비스는 더 이상 사용되지 않습니다.

HTTP 연결 사용 * 옵션을 선택한 경우 클라이언트는 HTTPS에 사용하는 것과 다른 HTTP 포트를 사용해야 합니다. StorageGRID 관리 지침을 참조하십시오.

관련 정보

StorageGRID 관리

활성, 유휴 및 동시 HTTP 연결의 이점

S3 요청에 대한 끝점 도메인 이름입니다

클라이언트 요청에 S3 도메인 이름을 사용하려면 StorageGRID 관리자가 S3 경로 스타일 및 S3 가상 호스팅 스타일 요청에서 S3 도메인 이름을 사용하는 연결을 허용하도록 시스템을 구성해야 합니다.

이 작업에 대해

S3 가상 호스팅 스타일 요청을 사용하려면 그리드 관리자가 다음 작업을 수행해야 합니다.

- 그리드 관리자를 사용하여 StorageGRID 시스템에 S3 끝점 도메인 이름을 추가합니다.
- 클라이언트가 StorageGRID에 대한 HTTPS 연결에 사용하는 인증서가 클라이언트에 필요한 모든 도메인 이름에 서명되었는지 확인합니다.

  예를 들어, 끝점이 '3.company.com` 인 경우 그리드 관리자는 HTTPS 연결에 사용되는 인증서에 '3.company.com` 끝점 및 끝점 와일드카드 주체 대체 이름(SAN):' * .s3.company.com` 가 포함되어 있는지 확인해야 합니다.

- 필요한 와일드카드 레코드를 포함하여 끝점 도메인 이름과 일치하는 DNS 레코드를 포함하도록 클라이언트에서 사용하는 DNS 서버를 구성합니다.

클라이언트가 로드 밸런서 서비스를 사용하여 연결하는 경우 그리드 관리자가 구성하는 인증서는 클라이언트가 사용하는 로드 밸런서 끝점에 대한 인증서입니다.

> 각 로드 밸런서 끝점마다 고유한 인증서가 있으며 각 끝점이 서로 다른 끝점 도메인 이름을 인식하도록 구성할 수 있습니다.

클라이언트가 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 연결하는 경우 그리드 관리자가 구성하는 인증서는

그리드에 사용되는 단일 사용자 지정 서버 인증서입니다.

> CLB 서비스는 더 이상 사용되지 않습니다.

자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

이러한 단계를 완료한 후에는 가상 호스팅 스타일 요청(예: ' bucket.s3.company.com`)을 사용할 수 있습니다.

관련 정보

StorageGRID 관리

REST API에 대한 보안을 구성합니다

S3 REST API 구성을 테스트합니다

AWS CLI(Amazon Web Services Command Line Interface)를 사용하여 시스템에 대한 연결을 테스트하고 시스템에 개체를 읽고 쓸 수 있는지 확인할 수 있습니다.

필요한 것

- 에서 AWS CLI를 다운로드하여 설치했습니다 "aws.amazon.com/cli".
- StorageGRID 시스템에서 S3 테넌트 계정을 생성했습니다.

단계

1. StorageGRID 시스템에서 생성한 계정을 사용하도록 Amazon 웹 서비스 설정을 구성합니다.
   a. 구성 모드 'AWS configure'로 진입한다
   b. 생성한 계정의 AWS 액세스 키 ID를 입력합니다.
   c. 생성한 계정의 AWS Secret Access 키를 입력합니다.
   d. 사용할 기본 영역을 입력합니다(예: us-east-1).
   e. 사용할 기본 출력 형식을 입력하거나 * Enter * 를 눌러 JSON을 선택합니다.
2. 버킷을 만듭니다.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

   버킷이 성공적으로 생성되면 다음 예와 같이 버킷의 위치가 반환됩니다.

```
"Location": "/testbucket"
```

1. 개체를 업로드합니다.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

객체가 성공적으로 업로드되면 객체 데이터의 해시인 Etag가 반환됩니다.

2. 버킷의 내용을 나열하여 객체가 업로드되었는지 확인합니다.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

3. 개체를 삭제합니다.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

4. 버킷을 삭제합니다.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

StorageGRID에서 **S3 REST API**를 구현하는 방법

클라이언트 애플리케이션은 S3 REST API 호출을 사용하여 StorageGRID에 연결하여 버킷을 생성, 삭제 및 수정할 수 있을 뿐만 아니라 오브젝트를 저장 및 검색할 수 있습니다.

클라이언트 요청 충돌

동일한 키에 쓰는 두 클라이언트 등의 충돌하는 클라이언트 요청은 "최신 성공" 기준으로 해결됩니다.

"Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 합니다.

일관성 제어

일관성 제어는 애플리케이션의 요구에 따라 오브젝트의 가용성과 서로 다른 스토리지 노드 및 사이트 전체에서 오브젝트의 일관성 간의 균형을 제공합니다.

기본적으로 StorageGRID는 새로 생성된 개체에 대해 쓰기 후 읽기 일관성을 보장합니다. 성공적으로 완료된 PUT를 팔로우하면 새로 작성된 데이터를 읽을 수 있습니다. 기존 오브젝트, 메타데이터 업데이트 및 삭제를 덮어쓰는 것은 결국 일관성이 유지됩니다. 덮어쓰기는 일반적으로 전파되는 데 몇 초 또는 몇 분이 걸리지만 최대 15일이 소요될 수 있습니다.

오브젝트 작업을 다른 정합성 보장 레벨에서 수행하려는 경우 각 버킷 또는 각 API 작업에 대해 정합성 제어를 지정할 수 있습니다.

일관성 제어

정합성 보장 제어는 StorageGRID에서 객체를 추적하는 데 사용하는 메타데이터가 노드 간에 분산되므로 클라이언트 요청에 대한 객체의 가용성에 영향을 줍니다.

버킷 또는 API 작업에 대한 정합성 제어를 다음 값 중 하나로 설정할 수 있습니다.

- * ALL *: 모든 노드가 즉시 데이터를 수신하거나 요청이 실패합니다.
- * strong-global *: 모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
- * strong-site *: 사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
- * read-after-new-write *: (기본값)는 새 객체에 대한 읽기 후 쓰기 정합성을 보장하고 객체 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 필요에 따라 만 사용하십시오(예: 거의 읽지 않는 로그 값이 포함된 버킷의 경우 또는 존재하지 않는 키의 헤드 또는 GET 작업의 경우). S3 FabricPool 버킷은 지원되지 않습니다.

"새 쓰기 후"와 "사용 가능한" 일관성 제어 기능을 사용합니다

HEAD 또는 GET 연산에서 "read-after-new-write" 정합성 제어를 사용하면 StorageGRID는 다음과 같이 여러 단계로 조회를 수행합니다.

- 먼저 낮은 일관성을 사용하여 오브젝트를 찾습니다.
- 이 조회에 실패하면 강력한 글로벌 동작에 해당하는 일관성 수준에 도달할 때까지 조회가 다음 일관성 수준에서 반복됩니다.

헤드 또는 GET 연산에서 "READ-After-NEW-WRITE" 일관성 컨트롤을 사용하지만 개체가 없으면 개체 조회는 항상 강력한 글로벌 동작의 일관성 수준에 도달합니다. 이 정합성 보장 수준에서는 각 사이트에서 개체 메타데이터의 여러 복사본을 사용할 수 있어야 하므로 같은 사이트에 있는 둘 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 많이 발생할 수 있습니다.

Amazon S3와 유사한 일관성 보증이 필요하지 않으면 일관성 제어를 ""사용 가능""으로 설정하여 헤드 및 GET 작업에 대한 이러한 오류를 방지할 수 있습니다. 헤드 또는 GET 작업에서 "사용 가능한" 정합성 제어를 사용할 경우 StorageGRID는 최종 일관성만 제공합니다. 일관성 수준을 높일 때 실패한 작업을 다시 시도하지 않으므로 오브젝트 메타데이터의 여러 복사본을 사용할 필요가 없습니다.

API 작업에 대한 정합성 제어를 지정합니다

개별 API 작업의 정합성 제어를 설정하려면 작업에 대해 정합성 보장 제어가 지원되어야 하며 요청 헤더에 정합성 제어를 지정해야 합니다. 이 예제에서는 개체 가져오기 작업을 위해 일관성 컨트롤을 "문자열 사이트"로 설정합니다.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

> 개체 넣기 작업과 개체 가져오기 작업 모두에 대해 동일한 일관성 컨트롤을 사용해야 합니다.

버킷의 정합성 제어를 지정합니다

버킷의 일관성 제어를 설정하려면 StorageGRID PUT 버킷 정합성 보장 요청 및 GET 버킷 정합성 보장 요청을 사용할 수 있습니다. 또는 테넌트 관리자 또는 테넌트 관리 API를 사용할 수 있습니다.

버킷의 정합성 제어 기능을 설정할 때는 다음 사항에 유의하십시오.

- 버킷의 일관성 제어를 설정하면 버킷의 오브젝트 또는 버킷 구성에 대해 수행된 S3 작업에 사용되는 일관성 제어가 결정됩니다. 버킷 자체의 작동에는 영향을 미치지 않습니다.
- 개별 API 작업의 정합성 제어는 버킷의 정합성 제어를 재정의합니다.
- 일반적으로 버킷은 기본 일관성 제어인 "read-after-new-write"를 사용해야 합니다. 요청이 올바르게 작동하지 않는 경우 가능한 경우 응용 프로그램 클라이언트 동작을 변경합니다. 또는 클라이언트가 각 API 요청에 대한 정합성 제어를 지정하도록 구성합니다. 버킷 레벨에서만 정합성 제어를 최후의 수단으로 설정하십시오.

일관성 제어 및 **ILM** 규칙이 상호 작용하여 데이터 보호에 영향을 미치는 방식

일관성 제어와 ILM 규칙 모두 오브젝트의 보호 방법에 영향을 미칩니다. 이러한 설정은 상호 작용할 수 있습니다.

예를 들어, 개체가 저장될 때 사용되는 일관성 컨트롤은 오브젝트 메타데이터의 초기 배치에 영향을 미치는 반면 ILM 규칙에 대해 선택된 수집 동작은 오브젝트 복사본의 초기 배치에 영향을 줍니다. StorageGRID에서는 클라이언트 요청을 이행하기 위해 오브젝트의 메타데이터와 해당 데이터에 모두 액세스해야 하므로 일관성 수준과 수집 동작에 적합한 보호 수준을 선택하면 초기 데이터 보호 수준을 높이고 시스템 응답을 더욱 정확하게 예측할 수 있습니다.

ILM 규칙에 대해 다음과 같은 수집 동작을 사용할 수 있습니다.

- * Strict * : ILM 규칙에 지정된 모든 사본은 클라이언트에 반환되기 전에 만들어야 합니다.
- * 균형 *: StorageGRID는 수집 시 ILM 규칙에 지정된 모든 복제본을 생성하려고 합니다. 그렇지 않을 경우 중간 복사본이 만들어지고 클라이언트에 성공적으로 반환됩니다. ILM 규칙에 지정된 복사본은 가능한 경우 만들어집니다.
- * 이중 커밋*: StorageGRID는 즉시 개체의 임시 복사본을 만들고 클라이언트에 성공을 반환합니다. ILM 규칙에 지정된 복사본은 가능한 경우 만들어집니다.

> ILM 규칙에 대한 수집 동작을 선택하기 전에 에서 이러한 설정에 대한 전체 설명을 읽어보십시오 ILM을 사용하여 개체를 관리합니다.

일관성 제어 및 **ILM** 규칙이 상호 작용하는 방법의 예

다음 ILM 규칙 및 다음 일관성 수준 설정이 있는 두 사이트 그리드가 있다고 가정합니다.

- * ILM 규칙 *: 로컬 사이트와 원격 사이트에 각각 하나씩, 두 개의 오브젝트 복사본을 만듭니다. Strict 수집 동작이 선택됩니다.
- * Consistency level *: "trong-global"(개체 메타데이터가 모든 사이트에 즉시 배포됩니다.)

클라이언트가 오브젝트를 그리드에 저장할 때 StorageGRID는 오브젝트 복사본을 둘 다 만들고 메타데이터를 두 사이트에 분산한 다음 클라이언트에 성공을 반환합니다.

수집 성공 메시지가 표시된 시점에 객체가 손실로부터 완벽하게 보호됩니다. 예를 들어, 수집 직후 로컬 사이트가

손실되면 오브젝트 데이터와 오브젝트 메타데이터의 복사본이 원격 사이트에 계속 존재합니다. 개체를 완전히 검색할 수 있습니다.

대신 동일한 ILM 규칙 및 "'strong-site' 정합성 보장 수준을 사용한 경우 객체 데이터가 원격 사이트에 복제되었지만 객체 메타데이터가 그 위치에 배포되기 전에 클라이언트에 성공 메시지가 표시될 수 있습니다. 이 경우 오브젝트 메타데이터의 보호 수준이 오브젝트 데이터의 보호 수준과 일치하지 않습니다. 수집 후 곧바로 로컬 사이트가 손실되면 오브젝트 메타데이터가 손실됩니다. 객체를 검색할 수 없습니다.

일관성 수준과 ILM 규칙 간의 상호 관계는 복잡할 수 있습니다. 도움이 필요한 경우 NetApp에 문의하십시오.

관련 정보

버킷 정합성 보장 요청 가져오기

버킷 정합성 보장 요청을 배치합니다

StorageGRID ILM 규칙이 개체를 관리하는 방법

그리드 관리자는 정보 라이프사이클 관리(ILM) 규칙을 생성하여 S3 REST API 클라이언트 애플리케이션에서 StorageGRID 시스템으로 수집된 오브젝트 데이터를 관리합니다. 그런 다음 이러한 규칙을 ILM 정책에 추가하여 시간 경과에 따라 오브젝트 데이터가 저장되는 방법 및 위치를 결정합니다.

ILM 설정은 개체의 다음 측면을 결정합니다.

- * 지역 *

  StorageGRID 시스템(스토리지 풀) 또는 클라우드 스토리지 풀 내에서 오브젝트 데이터의 위치입니다.

- * 스토리지 등급 *

  오브젝트 데이터를 저장하는 데 사용되는 스토리지의 유형(예: 플래시 또는 회전식 디스크)

- * 손실 방지 *

  복제, 삭제 코딩 또는 두 가지 유형의 복사본을 만들 수와 복사본 유형을 지정합니다.

- * 보존 *

  오브젝트의 데이터 관리 방식, 저장 위치 및 데이터 손실을 보호하는 방법에 대한 시간이 지나면서 변동합니다.

- * 수집 중 보호 *

  수집 중에 오브젝트 데이터를 보호하는 데 사용되는 방법: 동기 배치(Ingest 동작에 대한 균형 또는 엄격 옵션 사용) 또는 중간 복사본 만들기(이중 커밋 옵션 사용).

ILM 규칙을 사용하여 개체를 필터링 및 선택할 수 있습니다. S3을 사용하여 수집된 개체의 경우 ILM 규칙을 통해 다음 메타데이터를 기반으로 개체를 필터링할 수 있습니다.

- 테넌트 계정
- 버킷 이름

- 수집 시간
- 키
- 마지막 액세스 시간입니다

> 기본적으로 마지막 액세스 시간에 대한 업데이트는 모든 S3 버킷에 대해 비활성화됩니다. StorageGRID 시스템에 마지막 액세스 시간 옵션을 사용하는 ILM 규칙이 포함된 경우 해당 규칙에 지정된 S3 버킷의 마지막 액세스 시간에 대한 업데이트를 활성화해야 합니다. Tenant Manager의 [버킷 최종 액세스 시간] 요청, [S3 * > * Bucket * > * [마지막 액세스 시간 구성] * 확인란을 사용하거나 Tenant Management API를 사용하여 마지막 액세스 시간 업데이트를 활성화할 수 있습니다. 마지막 액세스 시간 업데이트를 설정할 때는 특히 작은 오브젝트가 있는 시스템에서 StorageGRID 성능이 저하될 수 있다는 점에 유의하십시오.

- 위치 제약 조건
- 개체 크기
- 사용자 메타데이터
- 개체 태그

ILM에 대한 자세한 내용은 정보 수명 주기 관리를 통해 개체 관리 지침을 참조하십시오.

관련 정보

테넌트 계정을 사용합니다

ILM을 사용하여 개체를 관리합니다

버킷 최종 액세스 시간 요청

오브젝트 버전 관리

버전 관리를 사용하면 개체의 여러 버전을 유지하여 실수에 의한 개체 삭제로부터 보호하고 이전 버전의 개체를 검색하고 복원할 수 있습니다.

StorageGRID 시스템은 대부분의 기능을 지원하는 버전 관리를 구현하지만 몇 가지 제한 사항이 있습니다. StorageGRID는 각 오브젝트의 버전을 최대 1,000개까지 지원합니다.

오브젝트 버전 관리를 StorageGRID ILM(정보 라이프사이클 관리) 또는 S3 버킷 라이프사이클 구성과 결합할 수 있습니다. 버킷에 대해 이 기능을 설정하려면 각 버킷에 대해 버전 관리를 명시적으로 활성화해야 합니다. 버킷의 각 오브젝트에는 StorageGRID 시스템에서 생성되는 버전 ID가 할당됩니다.

MFA(다중 요소 인증) 삭제 사용은 지원되지 않습니다.

> 버전 관리는 StorageGRID 버전 10.3 이상으로 생성된 버킷에서만 사용할 수 있습니다.

ILM 및 버전 관리

ILM 정책은 개체의 각 버전에 적용됩니다. ILM 스캔 프로세스는 모든 개체를 지속적으로 스캔하고 현재 ILM 정책에 대해 다시 평가합니다. ILM 정책에 대한 모든 변경 사항은 이전에 수집된 모든 개체에 적용됩니다. 여기에는 버전 관리가 활성화된 경우 이전에 수집된 버전이 포함됩니다. ILM 스캐닝은 이전에 수집된 개체에 새로운 ILM 변경 사항을 적용합니다.

버전 관리가 활성화된 버킷의 S3 오브젝트에서 버전 관리를 지원하므로 비현재 시간을 참조 시간으로 사용하는 ILM 규칙을 생성할 수 있습니다. 개체가 업데이트되면 이전 버전은 업데이트되지 않습니다. 비현재 시간 필터를 사용하면 이전 버전의 오브젝트에 대한 스토리지 영향을 줄이는 정책을 생성할 수 있습니다.

> 다중 파트 업로드 작업을 사용하여 새 버전의 개체를 업로드할 때 개체의 원래 버전에 대한 비현재 시간은 다중 파트 업로드가 완료될 때가 아닌 새 버전에 대해 다중 파트 업로드가 생성된 시점을 반영합니다. 제한된 경우 원래 버전의 비현재 시간이 현재 버전의 시간보다 몇 시간 또는 며칠 빨라질 수 있습니다.

S3 버전 오브젝트에 대한 ILM 정책 예제를 보려면 정보 수명 주기 관리로 오브젝트를 관리하는 지침을 참조하십시오.

관련 정보

ILM을 사용하여 개체를 관리합니다

S3 REST API 구현을 위한 권장사항

StorageGRID와 함께 사용할 S3 REST API를 구현할 때는 다음 권장 사항을 따라야 합니다.

존재하지 않는 객체에 대한 헤드 권장 사항

응용 프로그램에서 개체가 실제로 존재하지 않을 것으로 예상되는 경로에 개체가 있는지 정기적으로 확인하는 경우 ""사용 가능한"" 일관성 제어를 사용해야 합니다. 예를 들어, 응용 프로그램이 해당 위치에 배치되기 전에 위치를 지정할 경우 ""사용 가능"" 정합성 제어를 사용해야 합니다.

그렇지 않으면 헤드 작업에서 개체를 찾지 못할 경우 하나 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다.

PUT Bucket 정합성 보장 요청을 사용하여 각 버킷에 대해 ""사용 가능" 정합성 제어를 설정하거나 개별 API 작업에 대한 요청 헤더에서 정합성 제어를 지정할 수 있습니다.

개체 키에 대한 권장 사항

StorageGRID 11.4 이상에서 생성된 버킷의 경우 성능 모범 사례에 맞게 오브젝트 키 이름을 제한하는 것은 더 이상 필요하지 않습니다. 예를 들어, 이제 개체 키 이름의 처음 4개 문자에 임의의 값을 사용할 수 있습니다.

StorageGRID 11.4 이전 릴리스에서 생성된 버킷의 경우 객체 키 이름에 대한 다음 권장 사항을 계속 따르십시오.

- 개체 키의 처음 네 문자로 임의 값을 사용하면 안 됩니다. 이는 이전 AWS에서 권장하는 키 접두사와 다릅니다. 대신 "이미지"와 같은 비무작위, 고유하지 않은 접두사를 사용해야 합니다.
- 이전 AWS 권장 사항에 따라 키 접두사에 임의의 고유 문자를 사용하려면 객체 키에 디렉토리 이름을 접두사로 지정해야 합니다. 즉, 다음 형식을 사용합니다.

  ```
  mybucket/mydir/f8e3-image3132.jpg
  ```

  이 형식 대신:

  ```
  mybucket/f8e3-image3132.jpg
  ```

저장된 오브젝트 압축 * 옵션을 선택한 경우(* 구성 * > * 시스템 * > * 그리드 옵션 *) S3 클라이언트 응용 프로그램은 바이트 범위를 지정하는 오브젝트 가져오기 작업을 수행하지 않아야 합니다. 이러한 ""범위 읽기"" 작업은 StorageGRID가 요청된 바이트에 액세스하기 위해 개체의 압축을 효과적으로 해제해야 하기 때문에 비효율적입니다. 매우 큰 개체에서 작은 바이트 범위를 요청하는 Get Object 작업은 특히 비효율적입니다. 예를 들어, 50GB의 압축 개체에서 10MB 범위를 읽는 것은 매우 비효율적입니다.

압축된 개체에서 범위를 읽으면 클라이언트 요청이 시간 초과될 수 있습니다.

> 개체를 압축해야 하고 클라이언트 응용 프로그램에서 범위 읽기를 사용해야 하는 경우 응용 프로그램의 읽기 시간 초과를 늘리십시오.

관련 정보

- 일관성 제어
- 버킷 정합성 보장 요청을 배치합니다
- StorageGRID 관리

S3 REST API에서 지원되는 작업 및 제한 사항

StorageGRID 시스템은 대부분의 작업을 지원하고 몇 가지 제한 사항이 있는 간단한 스토리지 서비스 API(API 버전 2006-03-01)를 구현합니다. S3 REST API 클라이언트 애플리케이션을 통합할 때 구현 세부 정보를 이해해야 합니다.

StorageGRID 시스템은 가상 호스팅 방식의 요청과 경로 스타일 요청을 모두 지원합니다.

날짜 처리

S3 REST API의 StorageGRID 구현은 유효한 HTTP 날짜 형식만 지원합니다.

StorageGRID 시스템은 날짜 값을 허용하는 모든 헤더에 대해 유효한 HTTP 날짜 형식만 지원합니다. 날짜의 시간 부분은 그리니치 표준시(GMT) 형식 또는 표준 시간대 오프셋 없이 UTC(국제 표준시) 형식으로 지정할 수 있습니다(+0000을 지정해야 함). 요청에 "x-amz-date" 헤더를 포함하면 날짜 요청 헤더에 지정된 모든 값이 무시됩니다. AWS 서명 버전 4를 사용할 때는 날짜 헤더가 지원되지 않으므로 서명된 요청에 "x-amz-date" 헤더가 있어야 합니다.

공통 요청 헤더

StorageGRID 시스템은 에 의해 정의된 공통 요청 헤더를 지원합니다 "AWS(Amazon Web Services) 문서: Amazon Simple Storage Service API Reference 를 참조하십시오"한 가지 예외가 있습니다.

요청 헤더	구축
권한 부여	AWS Signature 버전 2에 대한 전체 지원 다음 경우를 제외하고 AWS Signature 버전 4 지원: • 요청 본문에 대한 SHA256 값이 계산되지 않습니다. 사용자가 제출한 값은 X-amz-content-SHA256 헤더용으로 'unsigned-payload' 값이 제공된 것처럼 유효성 검사 없이 허용됩니다.
X-amz-security-token	구현되지 않았습니다. 'XNotImplemented'를 반환합니다.

공통 응답 헤더

StorageGRID 시스템은 한 가지 예외를 제외하고 _Simple Storage Service API Reference_에 의해 정의된 모든 공통 응답 헤더를 지원합니다.

응답 헤더	구축
X-amz-id-2	사용 안 합니다

요청을 인증합니다

StorageGRID 시스템은 S3 API를 사용하여 오브젝트에 대한 인증된 액세스와 익명 액세스를 모두 지원합니다.

S3 API는 S3 API 요청을 인증하는 데 서명 버전 2 및 서명 버전 4를 지원합니다.

인증된 요청은 액세스 키 ID 및 비밀 액세스 키를 사용하여 서명해야 합니다.

StorageGRID 시스템은 HTTP '권한 부여' 헤더와 쿼리 매개 변수 사용 등 두 가지 인증 방법을 지원합니다.

HTTP 인증 헤더를 사용합니다

HTTP '권한 부여' 헤더는 버킷 정책에서 허용하는 익명 요청을 제외한 모든 S3 API 작업에서 사용됩니다. '권한 부여' 헤더에는 요청을 인증하는 데 필요한 모든 서명 정보가 들어 있습니다.

쿼리 매개 변수를 사용합니다

쿼리 매개 변수를 사용하여 URL에 인증 정보를 추가할 수 있습니다. 이를 URL 사전 서명 이라고 하며, 이 URL을 사용하여 특정 리소스에 대한 임시 액세스 권한을 부여할 수 있습니다. 미리 지정된 URL을 가진 사용자는 리소스에 액세스하기 위해 비밀 액세스 키를 알 필요가 없습니다. 이 키를 사용하면 타사에 리소스에 대한 제한된 액세스를 제공할 수 있습니다.

서비스에 대한 작업

StorageGRID 시스템은 서비스에 대해 다음 작업을 지원합니다.

작동	구축
서비스 받기	모든 Amazon S3 REST API 동작으로 구현됩니다.
스토리지 사용량을 가져옵니다	Get Storage Usage 요청은 계정이 사용하는 총 스토리지 양과 계정과 연결된 각 버킷에 대해 알려줍니다. 이 작업은 경로에 /을 추가하고 사용자 지정 쿼리 매개 변수("?x-ntap-sg-usage")를 추가하는 서비스에 대한 작업입니다.
옵션 /	클라이언트 애플리케이션은 스토리지 노드의 S3 인증 자격 증명을 제공하지 않고 스토리지 노드의 S3 포트에 대한 "옵션/" 요청을 발행하여 스토리지 노드의 사용 가능 여부를 결정할 수 있습니다. 이 요청을 사용하여 모니터링을 수행하거나, 외부 로드 밸런서가 스토리지 노드가 다운된 시점을 식별하도록 할 수 있습니다.

관련 정보

스토리지 사용 요청 가져오기

버킷 작업

StorageGRID 시스템은 각 S3 테넌트 계정에 대해 최대 1,000개의 버킷을 지원합니다.

버킷 이름 제한은 AWS US 표준 지역 제한을 따르지만, S3 가상 호스팅 스타일 요청을 지원하려면 이러한 제한을 DNS 명명 규칙으로 제한해야 합니다.

"AWS(Amazon Web Services) 문서: 버킷 제한 및 제한 사항"

S3 API 엔드포인트 도메인 이름을 구성합니다

버킷 가져오기(개체 나열) 및 버킷 버전 가져오기 작업은 StorageGRID 정합성 보장 제어를 지원합니다.

개별 버킷에 대해 마지막 액세스 시간에 대한 업데이트가 설정되었는지 여부를 확인할 수 있습니다.

다음 표에서는 StorageGRID에서 S3 REST API 버킷 작업을 구축하는 방법을 설명합니다. 이러한 작업을 수행하려면 계정에 필요한 액세스 자격 증명을 제공해야 합니다.

작동	구축
버킷 삭제	모든 Amazon S3 REST API 동작으로 구현됩니다.
버킷 CORS를 삭제합니다	이 작업은 버킷에 대한 CORS 구성을 삭제합니다.
Bucket 암호화를 삭제합니다	이 작업은 버킷에서 기본 암호화를 삭제합니다. 암호화된 기존 개체는 암호화된 상태로 유지되지만 버킷에 추가된 새 개체는 암호화되지 않습니다.
버킷 수명 주기를 삭제합니다	이 작업은 버킷에서 라이프사이클 구성을 삭제합니다.

작동	구축
버킷 정책을 삭제합니다	이 작업은 버킷에 연결된 정책을 삭제합니다.
버킷 복제를 삭제합니다	이 작업은 버킷에 연결된 복제 구성을 삭제합니다.
버킷 태그 지정을 삭제합니다	이 작업은 "태그 지정" 하위 리소스를 사용하여 버킷에서 모든 태그를 제거합니다.
버킷(목록 오브젝트), 버전 1 및 버전 2를 가져옵니다	이 작업은 버킷에 있는 오브젝트의 일부 또는 전체(최대 1,000개)를 반환합니다. 객체에 대한 스토리지 클래스는 객체가 REDucted_redundancy 스토리지 클래스 옵션으로 인제스트된 경우에도 두 값 중 하나를 가질 수 있습니다. • 객체가 스토리지 노드로 구성된 스토리지 풀에 저장되었음을 나타내는 'Standard'입니다. • Glacier는 해당 객체가 Cloud Storage Pool에서 지정한 외부 버킷으로 이동되었음을 나타냅니다. 버킷에 동일한 접두사가 있는 삭제된 키의 수가 많은 경우, 응답에는 키가 포함되지 않은 몇 가지 CommonPrefixes가 포함될 수 있습니다.
버킷 ACL 가져오기	이 작업은 양수 응답 및 버킷 소유자의 ID, DisplayName 및 권한을 반환하며, 이는 소유자가 버킷에 대한 모든 액세스 권한을 가지고 있음을 나타냅니다.
버킷 CORS를 가져옵니다	이 작업은 버킷에 대한 'CORS' 구성을 반환합니다.
버킷 암호화 가져오기	이 작업은 버킷의 기본 암호화 구성을 반환합니다.
버킷 수명 주기 가져오기	이 작업은 버킷의 수명 주기 구성을 반환합니다.
버킷 위치를 가져옵니다	이 작업은 Put Bucket 요청에서 "LocationConstraint" 요소를 사용하여 설정된 영역을 반환합니다. 버켓 지역이 us-east-1인 경우 해당 지역에 대해 빈 문자열이 반환됩니다.
버킷 알림을 받습니다	이 작업은 버킷에 연결된 알림 구성을 반환합니다.
버킷 객체 버전을 가져옵니다	버킷에 대한 읽기 액세스 기능을 사용하면 하위 리소스의 이 작업에서는 버킷에 있는 모든 개체 버전의 메타데이터를 나열합니다.
버킷 정책 가져오기	이 작업은 버킷에 연결된 정책을 반환합니다.
버킷 복제를 가져옵니다	이 작업은 버킷에 연결된 복제 구성을 반환합니다.
버킷 태그 지정을 가져옵니다	이 작업은 "태그 지정" 하위 리소스를 사용하여 버킷에 대한 모든 태그를 반환합니다.

작동	구축
버킷 버전 관리 가져오기	이를 위해 장난 서브리소스를 사용해 버켓의 버전 상태를 반환한다. • *blank*: 버전 관리가 활성화된 적이 없습니다(버킷을 ""버전 없음""). • 사용: 버전 관리가 활성화됩니다 • 일시 중단됨: 버전 관리가 이전에 활성화되었으며 일시 중단되었습니다
개체 잠금 구성을 가져옵니다	이 작업은 버킷 기본 보존 모드 및 기본 보존 기간(구성된 경우)을 반환합니다. 을 참조하십시오 개체 잠금 구성을 가져옵니다 을 참조하십시오.
헤드 버킷	이 작업은 버킷이 있는지 그리고 버킷에 액세스할 권한이 있는지 여부를 결정합니다. 이 작업은 다음을 반환합니다. • X-NTAP-sg-bucket-id: UUID 형식의 버킷 UUID • X-NTAP-sg-trace-id: 연관된 요청의 고유 추적 ID.

작동	구축
버킷 을 놓습니다	이 작업은 새 버킷을 생성합니다. 버킷을 만들면 버켓 소유자가 됩니다. • 버킷 이름은 다음 규칙을 준수해야 합니다. ◦ 각 StorageGRID 시스템에서 고유해야 합니다(테넌트 계정에서만 고유한 것은 아님). ◦ DNS를 준수해야 합니다. ◦ 3자 이상 63자 이하여야 합니다. ◦ 인접한 레이블이 마침표로 구분된 하나 이상의 레이블일 수 있습니다. 각 레이블은 소문자 또는 숫자로 시작하고 끝나야 하며 소문자, 숫자 및 하이픈만 사용할 수 있습니다. ◦ 텍스트 형식의 IP 주소처럼 보이지 않아야 합니다. ◦ 가상 호스팅 스타일 요청에서 기간을 사용하지 않아야 합니다. 마침표는 서버 와일드카드 인증서 확인에 문제를 일으킬 수 있습니다. • 기본적으로 버킷은 us-east-1 영역에 생성되지만 요청 본문의 LocationConstraint 요청 요소를 사용하여 다른 영역을 지정할 수 있습니다. "LocationConstraint" 요소를 사용할 때는 Grid Manager 또는 Grid Management API를 사용하여 정의된 영역의 정확한 이름을 지정해야 합니다. 사용할 지역 이름을 모르는 경우 시스템 관리자에게 문의하십시오. • 참고 *: PUT 버킷 요청이 StorageGRID에 정의되지 않은 지역을 사용하는 경우 오류가 발생합니다. • 'x-amz-bucket-object-lock-enabled' 요청 헤더를 포함시켜 S3 오브젝트 잠금이 활성화된 버킷을 생성할 수 있습니다. 을 참조하십시오 S3 오브젝트 잠금을 사용합니다. 버킷을 생성할 때 S3 오브젝트 잠금을 활성화해야 합니다. 버킷을 생성한 후에는 S3 오브젝트 잠금을 추가하거나 비활성화할 수 없습니다. S3 오브젝트 잠금에는 버킷 버전 관리가 필요하며, 이 버전은 버킷을 생성할 때 자동으로 활성화됩니다.
버킷 CORS를 넣습니다	이 작업은 버킷이 오리진 간 요청을 처리할 수 있도록 버킷에 대한 CORS 구성을 설정합니다. CORS(Cross-origin Resource Sharing)는 한 도메인의 클라이언트 웹 애플리케이션이 다른 도메인의 리소스에 액세스할 수 있도록 하는 보안 메커니즘입니다. 예를 들어, 그래픽을 저장하기 위해 "images"라는 S3 버킷을 사용한다고 가정합니다. 'images' bucket에 대한 CORS 설정을 통해 해당 bucket의 이미지를 웹사이트(+ http://www.example.com+`) 에 표시할 수 있습니다.
Bucket 암호화를 적용합니다	이 작업은 기존 버킷의 기본 암호화 상태를 설정합니다. 버킷 수준 암호화가 활성화된 경우 버킷에 추가된 모든 새 오브젝트는 암호화됩니다. StorageGRID는 StorageGRID 관리 키로 서버 측 암호화를 지원합니다. 서버쪽 암호화 설정 규칙을 지정할 때 SEAlgorithm 매개변수를 AES256으로 설정하고 KMSMasterKeyID 매개변수를 사용하지 마십시오. 객체 업로드 요청이 이미 암호화를 지정한 경우(즉, 요청에 "x-amz-server-side-encryption- *" 요청 헤더가 포함된 경우) 버킷 기본 암호화 구성이 무시됩니다.

작동	구축
버킷 수명 주기를 놓습니다	이 작업은 버킷에 대한 새 수명 주기 구성을 생성하거나 기존 수명 주기 구성을 대체합니다. StorageGRID는 수명 주기 구성에서 최대 1,000개의 수명 주기 규칙을 지원합니다. 각 규칙에는 다음 XML 요소가 포함될 수 있습니다. • 만료(일, 날짜) • NoncurrentVersionExpiration(NoncurrentDays) • 필터(접두사, 태그) • 상태 • ID입니다 StorageGRID는 다음 작업을 지원하지 않습니다. • AbortIncompleteMultipartUpload를 중단합니다 • ExpiredObjectDeleteMarker 를 참조하십시오 • 전환 버킷 수명 주기의 만료 작업이 ILM 배치 명령과 상호 작용하는 방법을 이해하려면 정보 수명 주기 관리를 통해 개체를 관리하기 위한 지침에서 ""ILM이 개체의 수명 내내 작동하는 방식""을 참조하십시오. • 참고 *: 버킷 수명 주기 구성은 S3 오브젝트 잠금이 활성화된 버킷과 함께 사용할 수 있지만 레거시 준수 버킷에서는 버킷 수명 주기 구성이 지원되지 않습니다.

작동	구축
버킷 통지를 보냅니다	이 작업은 요청 본문에 포함된 알림 구성 XML을 사용하여 버킷에 대한 알림을 구성합니다. 다음과 같은 구현 세부 사항에 유의해야 합니다. • StorageGRID는 SNS(Simple Notification Service) 항목을 대상으로 지원합니다. SQS(Simple Queue Service) 또는 Amazon Lambda 엔드포인트는 지원되지 않습니다. • 알림 대상은 StorageGRID 엔드포인트의 URN으로 지정해야 합니다. 테넌트 관리자 또는 테넌트 관리 API를 사용하여 엔드포인트를 생성할 수 있습니다. 알림 설정을 성공적으로 하려면 끝점이 있어야 합니다. 끝점이 없으면 400개의 잘못된 요청 오류가 InvalidArgument 코드와 함께 반환됩니다. • 다음 이벤트 유형에 대한 알림을 구성할 수 없습니다. 이러한 이벤트 유형은 * 지원되지 않습니다 *. ◦ '3: RedundancyLostObject'를 선택합니다 ◦ '3:ObjectRestore:완료됨' • StorageGRID에서 보낸 이벤트 알림은 다음 목록과 같이 일부 키를 포함하지 않고 다른 키에 대해 특정 값을 사용한다는 점을 제외하고 표준 JSON 형식을 사용합니다. • * eventSource * 를 선택합니다 전쟁포로 S3 • * awsRegion * 포함되지 않음 • x-amz-id-2 * 포함되지 않음 • * 표시 * "urn:SGWs:S3::bucket_name'
버킷 정책을 적용합니다	이 작업은 버킷에 연결된 정책을 설정합니다.

작동	구축

버킷 복제를 배치합니다	이 작업은 요청 본문에 제공된 복제 구성 XML을 사용하여 버킷에 대한 StorageGRID CloudMirror 복제를 구성합니다. CloudMirror 복제의 경우 다음과 같은 구축 세부 정보를 알고 있어야 합니다.
	
	• StorageGRID는 복제 구성의 V1만 지원합니다. 즉, StorageGRID는 규칙에 대해 'Filter' 요소의 사용을 지원하지 않으며 개체 버전 삭제에 대해서는 V1 규약을 따릅니다. 자세한 내용은 를 참조하십시오 "복제 구성에 대한 Amazon S3 문서".
	• 버킷 복제는 버전 관리되거나 버전이 지정되지 않은 버킷에서 구성할 수 있습니다.
	• 복제 구성 XML의 각 규칙에서 다른 대상 버킷을 지정할 수 있습니다. 소스 버킷은 둘 이상의 대상 버킷에 복제할 수 있습니다.
	• 대상 버킷은 테넌트 관리자 또는 테넌트 관리 API에 지정된 StorageGRID 엔드포인트의 URN으로 지정해야 합니다.
	
	복제 구성이 성공하려면 엔드포인트가 있어야 합니다. 종점이 존재하지 않으면 400개의 불량 요청으로 실패한다. "복제 정책을 저장할 수 없습니다. 지정한 끝점 URN이 없습니다:_URN_.
	
	• 구성 XML에서 역할 을 지정할 필요는 없습니다. 이 값은 StorageGRID에서 사용되지 않으며 제출될 경우 무시됩니다.
	• 구성 XML에서 스토리지 클래스를 생략하면 StorageGRID에서는 기본적으로 '표준' 스토리지 클래스를 사용합니다.
	• 소스 버킷에서 객체를 삭제하거나 소스 버킷 자체를 삭제하는 경우 지역 간 복제 동작은 다음과 같습니다.
	  ◦ 복제되기 전에 오브젝트 또는 버킷을 삭제하면 객체/버킷이 복제되지 않으므로 사용자에게 통보되지 않습니다.
	  ◦ 복제된 후 오브젝트 또는 버킷을 삭제하면 StorageGRID는 지역 간 복제 V1에 대한 표준 Amazon S3 삭제 동작을 따릅니다.

Bucket 태그 달기	이 작업은 "태그 지정" 하위 리소스를 사용하여 버킷에 대한 태그 집합을 추가하거나 업데이트합니다. 버킷 태그를 추가할 때 다음과 같은 제한 사항을 숙지하십시오. • StorageGRID 및 Amazon S3 모두 각 버킷당 최대 50개의 태그를 지원합니다. • 버킷과 연결된 태그에는 고유한 태그 키가 있어야 합니다. 태그 키의 길이는 최대 128자의 유니코드 문자일 수 있습니다. • 태그 값의 길이는 최대 256자의 유니코드 문자일 수 있습니다. • 키와 값은 대/소문자를 구분합니다.
버킷 버전 관리	이 구현은 재세팅된 서브리소스를 사용하여 기존 버킷의 버전 관리 상태를 설정합니다. 다음 값 중 하나를 사용하여 버전 관리 상태를 설정할 수 있습니다. • Enabled(사용): 버킷의 오브젝트에 대한 버전 관리를 활성화합니다. 버킷에 추가된 모든 오브젝트는 고유한 버전 ID를 받습니다. • Suspended(일시 중지됨): 버킷의 오브젝트에 대한 버전 관리를 비활성화합니다. 버킷에 추가된 모든 오브젝트는 버전 ID "null"을 받습니다.

작동	구축
개체 잠금 구성을 배치합니다	이 작업은 버킷 기본 보존 모드 및 기본 보존 기간을 구성하거나 제거합니다. 기본 보존 기간이 수정되면 기존 개체 버전의 보존 기한은 그대로 유지되며 새 기본 보존 기간을 사용하여 다시 계산되지 않습니다. 을 참조하십시오 개체 잠금 구성을 배치합니다 을 참조하십시오.

관련 정보

일관성 제어

버킷 최종 액세스 시간 요청 가져오기

버킷 및 그룹 액세스 정책

S3 작업이 감사 로그에서 추적되었습니다

ILM을 사용하여 개체를 관리합니다

테넌트 계정을 사용합니다

S3 라이프사이클 구성을 생성합니다

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

이 섹션의 간단한 예는 S3 라이프사이클 구성에서 특정 S3 버킷에서 특정 객체가 삭제(만료)되는 시기를 제어하는 방법을 보여줍니다. 이 섹션의 예제는 설명을 위한 것입니다. S3 라이프사이클 구성 생성에 대한 자세한 내용은 를 참조하십시오 "Amazon Simple Storage Service 개발자 가이드: 개체 수명 주기 관리". StorageGRID는 만료 작업만 지원하며 전환 작업은 지원하지 않습니다.

문서 수정 상태 설정은 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.

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
- ID입니다

버킷에 라이프사이클 구성을 적용하는 경우 버킷의 라이프사이클 설정은 항상 StorageGRID ILM 설정을 재정의합니다. StorageGRID는 ILM이 아닌 버킷의 만료 설정을 사용하여 특정 개체의 삭제 또는 유지 여부를 결정합니다.

따라서 ILM 규칙의 배치 지침이 개체에 계속 적용되더라도 그리드에서 개체를 제거할 수 있습니다. 또는 개체에 대한 ILM 배치 지침이 만료된 후에도 개체가 그리드에 남아 있을 수 있습니다. 자세한 내용은 을 참조하십시오 ILM이 개체 수명 전반에 걸쳐 작동하는 방식.

> 버킷 수명 주기 구성은 S3 오브젝트 잠금이 활성화된 버킷과 함께 사용할 수 있지만 버킷 수명 주기 구성은 레거시 준수 버킷에서 지원되지 않습니다.

StorageGRID는 다음 버킷 작업을 사용하여 라이프사이클 구성을 관리합니다.

- 버킷 수명 주기를 삭제합니다
- 버킷 수명 주기 가져오기
- 버킷 수명 주기를 놓습니다

문서 수정 상태 설정 작성

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 1은 접두사 categy1과 일치하고 key2 값이 tag2 인 객체에만 적용됩니다. Expiration 매개변수는 필터와 일치하는 객체가 2020년 8월 22일 자정에 만료되도록 지정합니다.
2. 규칙 2는 접두사 'category2'/ 와 일치하는 객체에만 적용됩니다. Expiration 매개 변수는 필터와 일치하는 객체가 수집되고 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 3은 접두사 'category3'/ 와 일치하는 객체에만 적용됩니다. Expiration 매개 변수는 일치하는 객체의 비최신 버전이 비최신 상태가 된 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 작성한 후 PUT Bucket 수명주기 요청을 실행하여 이를 버킷에 적용합니다.

이 요청은 예제 파일의 수명 주기 구성을 'testbucket'이라는 이름의 버킷의 개체에 적용합니다.

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

라이프사이클 구성이 버킷에 성공적으로 적용되었는지 확인하려면 Get Bucket 수명주기 요청을 실행합니다. 예를 들면 다음과 같습니다.

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

성공적으로 응답하면 방금 적용한 문서 수정 상태 설정이 나열됩니다.

버킷 수명 주기 만료가 객체에 적용되는지 확인합니다

Put Object, Head Object 또는 Get Object 요청을 실행할 때 수명 주기 구성의 만료 규칙이 특정 개체에 적용되는지 확인할 수 있습니다. 규칙이 적용될 경우 응답에는 개체 만료 시기 및 일치하는 만료 규칙을 나타내는 Expiration 매개변수가 포함됩니다.

> 버킷 라이프사이클이 ILM을 무시하기 때문에 표시된 '만료 날짜'는 객체가 삭제될 실제 날짜입니다. 자세한 내용은 을 참조하십시오 개체 보존이 결정되는 방식.

예를 들어, 이 PUT 오브젝트 요청은 2020년 6월 22일에 발행되었으며 'testbucket' 버킷에 오브젝트를 배치했습니다.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

성공 응답은 개체가 100일(2020년 10월 1일) 내에 만료되고 라이프사이클 구성의 규칙 2와 일치함을 나타냅니다.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

예를 들어, 이 head Object 요청은 testbucket 버킷에서 동일한 객체에 대한 메타데이터를 가져오는 데 사용되었습니다.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

성공 응답에는 개체의 메타데이터가 포함되며 개체가 100일 후에 만료되고 규칙 2와 일치함을 나타냅니다.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

S3 오브젝트 잠금 기본 버킷 보존을 사용합니다

버킷에 S3 오브젝트 잠금이 활성화된 경우 버킷에 추가된 각 오브젝트에 적용되는 기본 보존 모드와 기본 보존 기간을 지정할 수 있습니다.

- 버킷 생성 중에 버킷에 대해 S3 오브젝트 잠금을 설정하거나 해제할 수 있습니다.
- 버킷에 대해 S3 오브젝트 잠금이 활성화된 경우 버킷의 기본 보존을 구성할 수 있습니다.
- 기본 보존 구성은 다음을 지정합니다.
  - 기본 보존 모드: StorageGRID는 "규정 준수" 모드만 지원합니다.
  - 기본 보존 기간(일 또는 년).

개체 잠금 구성을 가져옵니다

객체 잠금 구성 가져오기 요청을 사용하면 버킷에 대해 객체 잠금이 설정되어 있는지 확인하고, 활성화된 경우 버킷에 대해 기본 보존 모드 및 보존 기간이 구성되어 있는지 확인할 수 있습니다.

새로운 오브젝트 버전이 버킷에 수집되면 "x-amz-object-lock-mode"가 지정되지 않은 경우 기본 보존 모드가 적용됩니다. x-amz-object-lock-retain-until-date를 지정하지 않으면 기본 보존 기간을 사용하여 Retain-until-date를 계산합니다.

이 작업을 완료하려면 S3:GetBucketObjectLockConfiguration 권한이 있거나 계정 루트여야 합니다.

요청 예

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization string
Authorization: authorization string
```

응답 예

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

개체 잠금 구성을 배치합니다

객체 잠금 구성 요청을 사용하면 객체 잠금이 활성화된 버킷의 기본 보존 모드 및 기본 보존 기간을 수정할 수 있습니다. 이전에 구성한 기본 보존 설정을 제거할 수도 있습니다.

새로운 오브젝트 버전이 버킷에 수집되면 "x-amz-object-lock-mode"가 지정되지 않은 경우 기본 보존 모드가 적용됩니다. x-amz-object-lock-retain-until-date를 지정하지 않으면 기본 보존 기간을 사용하여 Retain-until-date를 계산합니다.

오브젝트 버전을 수집한 후 기본 보존 기간을 수정하면 오브젝트 버전의 보존 기한은 그대로 유지되고 새 기본 보존 기간을 사용하여 다시 계산되지 않습니다.

이 작업을 완료하려면 S3:PutBucketObjectLockConfiguration 권한이 있거나 계정 루트여야 합니다.

PUT 요청에는 Content-MD5 요청 헤더를 지정해야 합니다.

요청 예

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization string
Authorization: authorization string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

버킷에 대한 사용자 지정 작업

StorageGRID 시스템은 S3 REST API에 추가되고 시스템에 고유한 맞춤형 버킷 작업을 지원합니다.

다음 표에는 StorageGRID에서 지원하는 사용자 지정 버킷 작업이 나열되어 있습니다.

작동	설명	를 참조하십시오
버킷 일관성 확보	특정 버킷에 적용되는 정합성 보장 레벨을 반환합니다.	버킷 정합성 보장 요청 가져오기
버킷 일관성을 유지합니다	특정 버킷에 적용되는 정합성 수준을 설정합니다.	버킷 정합성 보장 요청을 배치합니다
버킷 최종 액세스 시간 가져오기	특정 버킷에 대해 마지막 액세스 시간 업데이트를 사용할 수 있는지 여부를 반환합니다.	버킷 최종 액세스 시간 요청 가져오기
버킷 최종 접근 시간	특정 버킷에 대한 마지막 액세스 시간 업데이트를 활성화하거나 비활성화할 수 있습니다.	버킷 최종 액세스 시간 요청

작동	설명	를 참조하십시오
버킷 메타데이터 알림 구성을 삭제합니다	특정 버킷과 연결된 메타데이터 알림 구성 XML을 삭제합니다.	버킷 메타데이터 알림 구성 요청을 삭제합니다
Bucket 메타데이터 알림 구성 가져오기	특정 버킷과 연결된 메타데이터 알림 구성 XML을 반환합니다.	버킷 메타데이터 알림 구성 요청을 가져옵니다
Put Bucket 메타데이터 알림 구성	버킷에 대한 메타데이터 알림 서비스를 구성합니다.	PUT 버킷 메타데이터 알림 구성 요청
준수 설정이 적용된 버킷을 배치합니다	더 이상 사용되지 않으며 지원되지 않음: Compliance를 사용하는 새 버킷을 더 이상 생성할 수 없습니다.	사용되지 않음: 준수 설정이 포함된 Bucket을 넣습니다
버킷 규정 준수	더 이상 사용되지 않지만 지원됨: 기존 레거시 준수 버킷에 대해 현재 적용되는 규정 준수 설정을 반환합니다.	사용되지 않음: 버킷 준수 요청 가져오기
버킷 규정 준수	사용되지 않지만 지원됨: 기존 레거시 준수 버킷의 준수 설정을 수정할 수 있습니다.	폐기됨: 버킷 준수 요청을 넣으십시오

관련 정보

감사 로그에서 S3 작업을 추적했습니다

객체에 대한 작업

이 섹션에서는 StorageGRID 시스템이 객체에 대해 S3 REST API 작업을 구축하는 방법에 대해 설명합니다.

다음 조건은 모든 개체 작업에 적용됩니다.

- StorageGRID 일관성 제어 는 다음과 같은 경우를 제외하고 모든 개체 작업에서 지원됩니다.
  - 객체 ACL을 가져옵니다
  - '옵션 /'
  - 개체를 법적 증거 자료 보관
  - 개체 보존
  - 개체 내용 을 선택합니다
- 동일한 키에 쓰는 두 클라이언트 등의 충돌하는 클라이언트 요청은 "최신 성공" 기준으로 해결됩니다. "Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 합니다.
- StorageGRID 버킷의 모든 오브젝트는 익명 사용자 또는 다른 계정에서 만든 오브젝트를 포함하여 버킷 소유자가 소유합니다.

- Swift를 통해 StorageGRID 시스템으로 수집된 데이터 오브젝트는 S3를 통해 액세스할 수 없습니다.

다음 표에서는 StorageGRID에서 S3 REST API 오브젝트 작업을 구현하는 방법을 설명합니다.

작동	구축
개체 삭제	멀티팩터 인증(MFA)과 응답 헤더 X-amz-MFA는 지원되지 않습니다. 오브젝트 삭제 요청을 처리할 때 StorageGRID는 저장된 모든 위치에서 오브젝트의 모든 복사본을 즉시 제거하려고 시도합니다. 성공하면 StorageGRID는 즉시 클라이언트에 응답을 반환합니다. 위치를 일시적으로 사용할 수 없기 때문에 30초 이내에 모든 복사본을 제거할 수 없는 경우 StorageGRID는 제거할 복사본을 대기시킨 다음 클라이언트에 성공 여부를 표시합니다. • 버전 관리 * 특정 버전을 제거하려면 요청자가 버킷 소유자여야 하며 rrionId 하위 리소스를 사용해야 합니다. 이 하위 리소스를 사용하면 버전이 영구적으로 삭제됩니다. 만약 rionId가 삭제 표식에 해당하면 응답 헤더 x-amz-delete-marker가 TRUE로 설정된다. • 버전 지원 버킷에서 rionId 하위 리소스 없이 개체를 삭제하면 삭제 표식이 생성됩니다. 삭제 마커의 rionId는 x-amz-version-id 응답 헤더를 사용하여 반환되고 x-amz-delete-marker 응답 헤더는 TRUE로 설정됩니다. • 버전 일시 중지된 버킷에서 rionId ' 하위 리소스 없이 개체를 삭제하면 기존 'null' 버전 또는 'null' 삭제 표식이 영구적으로 삭제되고 새 'null' 삭제 표식이 생성됩니다. x-amz-DELETE-MARKER 응답 헤더가 TRUE로 설정된 상태로 반환됩니다. • 참고 *: 경우에 따라 객체에 대해 여러 개의 삭제 마커가 존재할 수 있습니다.
여러 개체를 삭제합니다	멀티팩터 인증(MFA)과 응답 헤더 X-amz-MFA는 지원되지 않습니다. 동일한 요청 메시지에서 여러 객체를 삭제할 수 있습니다.
개체 태그 지정 삭제	"태그 지정" 하위 리소스를 사용하여 개체에서 모든 태그를 제거합니다. 모든 Amazon S3 REST API 동작으로 구현됩니다. • 버전 관리 * 요청에 rionId 쿼리 매개 변수가 지정되지 않은 경우 버전 지정된 버킷에 있는 개체의 최신 버전에서 모든 태그가 삭제됩니다. 객체의 현재 버전이 삭제 표식이면 x-amz-delete-marker 응답 헤더가 true로 설정된 상태로 "MethodNotAllowed" 상태가 반환됩니다.
객체 가져오기	객체 가져오기

작동	구축
객체 ACL을 가져옵니다	계정에 필요한 액세스 자격 증명이 제공된 경우 이 작업은 개체 소유자의 ID, DisplayName 및 사용 권한과 함께 긍정적인 응답을 반환합니다. 이는 소유자가 개체에 대한 모든 액세스 권한을 가지고 있음을 나타냅니다.
객체 법적 증거 자료 보관	S3 오브젝트 잠금을 사용합니다
개체 보존 가져오기	S3 오브젝트 잠금을 사용합니다
객체 태그 지정 가져오기	"태그 지정" 하위 리소스를 사용하여 개체에 대한 모든 태그를 반환합니다. 모든 Amazon S3 REST API 동작으로 구현됩니다 • 버전 관리 * 요청에 rionId 쿼리 매개 변수가 지정되지 않은 경우 이 작업은 최신 버전의 개체에서 버전 관리되는 버킷으로 모든 태그를 반환합니다. 객체의 현재 버전이 삭제 표식이면 x-amz-delete-marker 응답 헤더가 true로 설정된 상태로 "MethodNotAllowed" 상태가 반환됩니다.
헤드 개체	헤드 개체
사후 개체 복원	사후 개체 복원
개체 를 넣습니다	개체 를 넣습니다
개체 - 복사 를 선택합니다	개체 - 복사 를 선택합니다
개체를 법적 증거 자료 보관	S3 오브젝트 잠금을 사용합니다
개체 보존	S3 오브젝트 잠금을 사용합니다

작동	구축
개체 태그 지정	태그 지정 하위 리소스를 사용하여 기존 개체에 태그 집합을 추가합니다. 모든 Amazon S3 REST API 동작으로 구현됩니다 • 개체 태그 제한 * 새 개체를 업로드할 때 태그를 추가하거나 기존 개체에 태그를 추가할 수 있습니다. StorageGRID 및 Amazon S3 모두 각 오브젝트에 대해 최대 10개의 태그를 지원합니다. 개체와 관련된 태그에는 고유한 태그 키가 있어야 합니다. 태그 키의 길이는 최대 128자의 유니코드 문자이고 태그 값의 길이는 최대 256자의 유니코드 문자일 수 있습니다. 키와 값은 대/소문자를 구분합니다. • 태그 업데이트 및 수집 동작 * 오브젝트 태그 지정을 사용하여 개체의 태그를 업데이트하는 경우 StorageGRID에서는 개체를 다시 수집하지 않습니다. 즉, 일치하는 ILM 규칙에 지정된 Ingest 동작 옵션이 사용되지 않습니다. ILM이 정상적인 백그라운드 ILM 프로세스에 의해 다시 평가될 때 업데이트로 인해 트리거되는 개체 배치에 대한 모든 변경 사항이 발생합니다. 즉, ILM 규칙이 수집 동작에 Strict 옵션을 사용하는 경우 필요한 개체 배치를 만들 수 없는 경우(예: 새로 필요한 위치를 사용할 수 없음) 작업이 수행되지 않습니다. 업데이트된 오브젝트는 필요한 배치가 가능할 때까지 현재 위치를 유지합니다. • 충돌 해결 * 동일한 키에 쓰는 두 클라이언트 등의 충돌하는 클라이언트 요청은 "최신 성공" 기준으로 해결됩니다. "Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 합니다. • 버전 관리 * 요청에 rionId 쿼리 매개 변수가 지정되지 않은 경우 작업에서 버전 관리되는 버킷의 가장 최신 버전의 개체에 태그를 추가합니다. 객체의 현재 버전이 삭제 표식이면 x-amz-delete-marker 응답 헤더가 true로 설정된 상태로 "MethodNotAllowed" 상태가 반환됩니다.

관련 정보

S3 작업이 감사 로그에서 추적되었습니다

S3 오브젝트 잠금을 사용합니다

StorageGRID 시스템에서 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 S3 오브젝트 잠금이 설정된 버킷을 생성한 다음 각 버킷의 기본 보존 기간 또는 해당 버킷에 추가한 각 오브젝트 버전에 대한 특정 보관 기간 및 법적 증거 보관 설정을 지정할 수 있습니다.

S3 오브젝트 잠금을 사용하면 고정된 시간 또는 무기한으로 오브젝트를 삭제 또는 덮어쓰는 것을 방지하기 위해 오브젝트 레벨 설정을 지정할 수 있습니다.

StorageGRID S3 오브젝트 잠금 기능은 Amazon S3 규정 준수 모드에 상응하는 단일 보존 모드를 제공합니다. 기본적으로 보호된 개체 버전은 사용자가 덮어쓰거나 삭제할 수 없습니다. StorageGRID S3 오브젝트 잠금 기능은 거버넌스 모드를 지원하지 않으며, 특별한 권한이 있는 사용자가 보존 설정을 무시하거나 보호된 오브젝트를 삭제할 수 없습니다.

버킷에 대해 **S3** 오브젝트 잠금을 설정합니다

StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 각 버킷을 생성할 때 선택적으로 S3 오브젝트 잠금을 활성화할 수 있습니다. 다음 방법 중 하나를 사용할 수 있습니다.

- 테넌트 관리자를 사용하여 버킷을 생성합니다.

  테넌트 계정을 사용합니다

- X-amz-bucket-object-lock-enabled 요청 헤더로 PUT Bucket 요청을 이용하여 bucket을 생성한다.

  버킷 작업

버킷이 생성된 후에는 S3 오브젝트 잠금을 추가하거나 비활성화할 수 없습니다. S3 오브젝트 잠금에는 버킷 버전 관리가 필요하며, 이 버전은 버킷을 생성할 때 자동으로 활성화됩니다.

S3 오브젝트 잠금이 활성화된 버킷에는 S3 오브젝트 잠금 설정이 있는 오브젝트와 없는 오브젝트의 조합이 포함될 수 있습니다. StorageGRID는 S3 오브젝트 잠금 버킷의 오브젝트에 대한 기본 보존 기간을 지원하며 오브젝트 잠금 구성 버킷 작업을 지원합니다. '3:object-lock-remaining-days' 정책 조건 키는 객체에 대해 허용되는 최소 및 최대 보존 기간을 설정합니다.

버킷에 **S3** 오브젝트 잠금이 설정되었는지 확인

S3 오브젝트 잠금이 활성화되어 있는지 확인하려면 를 사용합니다 개체 잠금 구성을 가져옵니다 요청하십시오.

S3 오브젝트 잠금 설정으로 오브젝트를 생성합니다

S3 오브젝트 잠금이 활성화된 버킷에 오브젝트 버전을 추가할 때 S3 오브젝트 잠금 설정을 지정하려면 오브젝트 넣기, 오브젝트 복사 넣기 또는 다중 파트 업로드 요청을 시작합니다. 다음 요청 헤더를 사용하십시오.

> 버킷을 생성할 때 S3 오브젝트 잠금을 활성화해야 합니다. 버킷을 생성한 후에는 S3 오브젝트 잠금을 추가하거나 비활성화할 수 없습니다.

- 'x-amz-object-lock-mode'로, 반드시 준수(대소문자 구분)되어야 합니다.

  > x-amz-object-lock-mode를 지정할 경우 x-amz-object-lock-retain-until-date를 지정해야 합니다.

- 'X-amz-object-lock-retain-until-date'
  - 유지 종료 날짜 값은 2020-08-10T21:46:00Z 형식이어야 합니다. 소수 자릿수는 허용되지만 소수점 이하 자릿수는 3자리만 유지됩니다(밀리초 단위). 다른 ISO 8601 형식은 허용되지 않습니다.
  - 보존 종료 날짜는 미래여야 합니다.
- X-amz-object-lock-legal-hold

  법적 증거 자료 보관(대소문자 구분)이 켜져 있는 경우, 해당 물체는 법적 증거 자료 보관 하에 배치됩니다. 법적 증거 자료 보관 기능이 꺼져 있는 경우 법적 증거 자료 보관 작업이 없습니다. 다른 값을 사용하면 400개의 잘못된

요청(InvalidArgument) 오류가 발생합니다.

이러한 요청 헤더를 사용하는 경우 다음과 같은 제한 사항에 유의하십시오.

- "x-amz-object-lock- *" 요청 헤더가 Put Object 요청에 있는 경우 Content-MD5" 요청 헤더가 필요합니다. 개체 복사 또는 멀티파트 업로드를 시작하려면 Content-MD5가 필요하지 않습니다.
- 버킷에 S3 오브젝트 잠금이 활성화되어 있지 않고 "x-amz-object-lock- *" 요청 헤더가 있는 경우 400개의 잘못된 요청(InvalidRequest) 오류가 반환됩니다.
- Put Object 요청은 AWS 동작에 맞춰 "x-amz-storage-class:reduced_redundancy"를 사용할 수 있도록 지원합니다. 하지만 오브젝트가 S3 오브젝트 잠금이 설정된 버킷으로 수집되면 StorageGRID는 항상 이중 커밋 수집을 수행합니다.
- 이후 GET 또는 HEAD 객체 버전 응답에는 헤더 "x-amz-OBJECT-LOCK-MODE", "x-amz-OBJECT-REGATE-DATE" 및 "x-amz-OBJECT-LOCK-REGAL-HOLD"가 포함되며, 구성된 경우 요청 송신자가 올바른 '3:GET *' 권한을 가지고 있는 경우 이에 해당합니다.
- 이후 개체 버전 삭제 또는 개체 버전 삭제 요청은 보존 기한 이전이거나 법적 보류가 켜져 있는 경우 실패합니다.

S3 오브젝트 잠금 설정을 업데이트합니다

기존 개체 버전에 대한 법적 증거 자료 보관 또는 보존 설정을 업데이트해야 하는 경우 다음 개체 하위 리소스 작업을 수행할 수 있습니다.

- '개체 법적 증거 자료 보관'

  새 법적 증거 자료 보관 값이 켜져 있으면 해당 개체는 법적 증거 자료 보관 아래에 배치됩니다. 법적 증거 자료 보관 가치가 없는 경우 법적 구속이 해제됩니다.

- '개체 보존'을 선택합니다
  - 모드 값은 규정 준수(대/소문자 구분)여야 합니다.
  - 유지 종료 날짜 값은 2020-08-10T21:46:00Z 형식이어야 합니다. 소수 자릿수는 허용되지만 소수점 이하 자릿수는 3자리만 유지됩니다(밀리초 단위). 다른 ISO 8601 형식은 허용되지 않습니다.
  - 개체 버전에 기존 보존 기한이 있는 경우 개체 버전을 늘릴 수만 있습니다. 새 값은 미래여야 합니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

테넌트 계정을 사용합니다

개체 를 넣습니다

개체 - 복사 를 선택합니다

멀티파트 업로드를 시작합니다

오브젝트 버전 관리

"Amazon Simple Storage Service 사용자 가이드: S3 Object Lock 사용"

StorageGRID는 에 대해 다음 AWS S3 Select 절, 데이터 유형 및 연산자를 지원합니다 SelectObjectContent 명령.

> 목록에 없는 항목은 지원되지 않습니다.

구문은 을 참조하십시오 SelectObjectContent 를 선택합니다. S3 Select에 대한 자세한 내용은 를 참조하십시오 "S3 Select용 AWS 문서".

S3 Select가 활성화된 테넌트 계정만 SelectObjectContent 쿼리를 실행할 수 있습니다. 를 참조하십시오 S3 Select 사용에 대한 고려 사항 및 요구 사항.

절을 참조하십시오

- 목록을 선택합니다
- FROM 절입니다
- WHERE 절
- Limit 절

데이터 유형

- 불입니다
- 정수
- 문자열
- 부동
- 십진수, 숫자
- 타임 스탬프입니다

연산자

논리 연산자

- 및
- 아닙니다
- 또는

비교 연산자

- 를 누릅니다
- 를 누릅니다
- lt;=.(&L
- GT;=.(&T
- =

- =
- 를 누릅니다
- !=
- 사이
- 인치

패턴 일치 연산자

- 좋아요
- _
- %

단일 작업자

- NULL입니다
- NULL이 아닙니다

수학 연산자

- 를 누릅니다
- -
- *
- /
- %

StorageGRID는 AWS S3 Select 운영자 우선권을 따릅니다.

집계 함수

- 평균()
- 개수(*)
- 최대()
- 최소()
- 합계()

조건부 함수

- 케이스
- 합체
- 노LIF

변환 함수

- 캐스트(지원되는 데이터 형식용)

날짜 함수

- date_add
- Date_DIFF(날짜/시간
- 압축 풀기
- to_string(대상 문자열)
- 를 _TIMESTAMP로 설정합니다
- UTCNOW

문자열 함수

- char_length, character_length
- 낮음
- 부분 문자열
- 잘라내기
- 위쪽

서버측 암호화를 사용합니다

서버측 암호화를 통해 유휴 개체 데이터를 보호할 수 있습니다. StorageGRID는 개체를 쓸 때 데이터를 암호화하고 개체에 액세스할 때 데이터를 해독합니다.

서버측 암호화를 사용하려면 암호화 키가 관리되는 방식에 따라 상호 배타적인 두 가지 옵션 중 하나를 선택할 수 있습니다.

- * SSE(StorageGRID 관리 키를 사용한 서버 측 암호화) *: S3 요청을 발행하여 오브젝트를 저장할 때 StorageGRID는 고유 키를 사용하여 오브젝트를 암호화합니다. S3 요청을 통해 오브젝트를 검색할 때 StorageGRID는 저장된 키를 사용하여 오브젝트를 해독합니다.
- * SSE-C(고객이 제공한 키를 사용한 서버측 암호화) *: S3 요청을 발행하여 오브젝트를 저장할 때 사용자는 자신만의 암호화 키를 제공합니다. 오브젝트를 검색할 때 요청의 일부로 동일한 암호화 키를 제공합니다. 두 암호화 키가 일치하면 해당 개체는 해독되고 개체 데이터는 반환됩니다.

  StorageGRID는 모든 개체 암호화 및 암호 해독 작업을 관리하지만 사용자가 제공하는 암호화 키를 관리해야 합니다.

  > 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다.

  > 개체가 SSE 또는 SSE-C로 암호화된 경우 버킷 수준 또는 그리드 수준 암호화 설정은 무시됩니다.

SSE를 사용합니다

StorageGRID에서 관리하는 고유 키를 사용하여 개체를 암호화하려면 다음 요청 헤더를 사용합니다.

'X-amz-서버측-암호화'

SSE 요청 헤더는 다음 오브젝트 작업에서 지원됩니다.

- 개체 를 넣습니다
- 개체 - 복사 를 선택합니다
- 멀티파트 업로드를 시작합니다

SSE-C를 사용합니다

관리하는 고유 키로 개체를 암호화하려면 다음 세 가지 요청 헤더를 사용합니다.

요청 헤더	설명
"x-amz-server-sidesidebencryptionsever-customer-algorithm"입니다	암호화 알고리즘을 지정합니다. 헤더 값은 AES256이어야 합니다.
"x-amz-server-sideebencryptionsever-customer-key"	개체를 암호화하거나 해독하는 데 사용할 암호화 키를 지정합니다. 키의 값은 256비트 base64로 인코딩되어야 합니다.
"X-amz-server-sidemidebencryptionsever-customer-key-md5'	RFC 1321에 따라 암호화 키의 MD5 다이제스트를 지정합니다. RFC 1321은 암호화 키가 오류 없이 전송되도록 하는 데 사용됩니다. MD5 다이제스트 값은 base64로 인코딩된 128비트여야 합니다.

SSE-C 요청 헤더는 다음 개체 작업에서 지원됩니다.

- 객체 가져오기
- 헤드 개체
- 개체 를 넣습니다
- 개체 - 복사 를 선택합니다
- 멀티파트 업로드를 시작합니다
- 부품 업로드
- 업로드 부품 - 복사

고객이 제공한 키**(SSE-C)**와 함께 서버측 암호화 사용 시 고려 사항

SSE-C를 사용하기 전에 다음 사항을 고려하십시오.

- https를 사용해야 합니다.

> StorageGRID는 SSE-C를 사용할 때 http를 통해 이루어진 요청을 거부합니다 보안을 위해 실수로 http를 사용하여 보낸 모든 키가 손상되지 않도록 고려해야 합니다. 키를 폐기하고 필요에 따라 회전합니다.

- 응답의 ETag는 객체 데이터의 MD5가 아닙니다.
- 암호화 키를 개체에 매핑하는 작업을 관리해야 합니다. StorageGRID는 암호화 키를 저장하지 않습니다. 각 개체에 대해 제공하는 암호화 키를 추적할 책임은 사용자에게 있습니다.
- 버킷을 버전 관리가 활성화된 경우 각 오브젝트 버전에는 고유한 암호화 키가 있어야 합니다. 각 개체 버전에 사용되는 암호화 키를 추적할 책임은 사용자에게 있습니다.
- 클라이언트 측에서 암호화 키를 관리하기 때문에 클라이언트 측에서 키 회전과 같은 추가 보호 수단을 관리해야 합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다.

- CloudMirror 복제가 버킷에 대해 구성된 경우 SSE-C 객체를 수집할 수 없습니다. 수집 작업이 실패합니다.

관련 정보

객체 가져오기

헤드 개체

개체 를 넣습니다

개체 - 복사 를 선택합니다

멀티파트 업로드를 시작합니다

부품 업로드

업로드 부품 - 복사

"Amazon S3 개발자 가이드: 고객 제공 암호화 키(SSE-C)를 사용하여 서버측 암호화를 사용하여 데이터 보호"

객체 가져오기

S3 오브젝트 가져오기 요청을 사용하여 S3 버킷에서 오브젝트를 검색할 수 있습니다.

개체 및 다중 파트 개체를 가져옵니다

'PARTNUMBER' 요청 파라미터를 사용하면 멀티파트 또는 분할된 개체의 특정 부분을 검색할 수 있습니다. X-amz-MP-parts-count 응답 요소는 개체의 부품 수를 나타냅니다.

분할/다중 파트 개체와 비분할/비다중 파트 개체 모두에 대해 'PARTNUMBER'를 1로 설정할 수 있지만, "x-amz-MP-parts-count" 응답 요소는 분할된 또는 다중 파트 개체에 대해서만 반환됩니다.

고객이 제공한 암호화 키**(SSE-C)**를 사용하여 서버측 암호화를 위한 요청 헤더

사용자가 제공한 고유 키로 개체를 암호화한 경우 머리글 3개를 모두 사용합니다.

- X-amz-서버측-암호화-고객-알고리즘: AES256 지정.
- 'x-amz-서버측-암호화-고객-키': 오브젝트의 암호화 키를 지정합니다.
- X-amz-서버측-암호화-고객-키-MD5: 오브젝트의 암호화 키에 대한 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.

사용자 메타데이터의 **UTF-8** 문자

StorageGRID는 사용자 정의 메타데이터에서 이스케이프된 UTF-8 문자를 구문 분석하거나 해석하지 않습니다. 사용자 정의 메타데이터에서 이스케이프된 UTF-8 문자가 있는 개체에 대한 요청을 가져오십시오. 키 이름이나 값에 인쇄할 수 없는 문자가 포함되어 있으면 "x-amz-missing-meta" 헤더가 반환되지 않습니다.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않으며 'XNotImplemented'를 반환합니다.

- X-amz-웹사이트-리디렉션-위치

버전 관리

rrionId 서브리소스를 지정하지 않으면 가장 최근 버전의 객체가 버전 관리되는 버킷에 페치됩니다. 객체의 현재 버전이 삭제 표식이면 x-amz-DELETE-MARKER 응답 헤더가 TRUE로 설정된 상태로 "Not Found" 상태가 반환됩니다.

Get Object for Cloud Storage Pool 개체의 동작

개체가 클라우드 스토리지 풀에 저장된 경우(정보 수명 주기 관리를 통해 개체 관리 지침 참조) 오브젝트 가져오기 요청의 동작은 개체의 상태에 따라 달라집니다. 자세한 내용은 " 헤드 개체 "를 참조하십시오.

> 객체가 클라우드 스토리지 풀에 저장되고 오브젝트 복사본이 하나 이상 그리드에 존재하는 경우, 객체 가져오기 요청은 클라우드 스토리지 풀에서 데이터를 검색하기 전에 그리드에서 데이터를 검색하려고 시도합니다.

개체의 상태입니다	**Get Object**의 동작입니다
StorageGRID로 수집되었지만 아직 ILM에 의해 평가되지 않은 오브젝트 또는 기존 스토리지 풀에 저장된 오브젝트 또는 삭제 코딩 사용	200OK 개체의 복사본이 검색됩니다.
Cloud Storage Pool의 개체이지만 아직 검색할 수 없는 상태로 전환되지 않았습니다	200OK 개체의 복사본이 검색됩니다.
개체가 검색할 수 없는 상태로 전환되었습니다	403 금지됨, InvalidObjectState 개체를 검색 가능한 상태로 복원하려면 POST 개체 복원 요청을 사용합니다.

개체의 상태입니다	**Get Object**의 동작입니다
복구할 수 없는 상태에서 복원 중인 개체입니다	403 금지됨, InvalidObjectState POST 개체 복원 요청이 완료될 때까지 기다립니다.
객체가 클라우드 스토리지 풀에 완전히 복구되었습니다	200OK 개체의 복사본이 검색됩니다.

클라우드 스토리지 풀에서 다중 또는 분할 오브젝트

여러 부분 개체를 업로드했거나 StorageGRID가 큰 개체를 세그먼트로 분할한 경우 StorageGRID는 개체의 부분 또는 세그먼트의 하위 집합을 샘플링하여 클라우드 저장소 풀에서 개체를 사용할 수 있는지 여부를 결정합니다. 일부 개체의 일부가 이미 검색 불가능한 상태로 전환되었거나 개체의 일부가 아직 복원되지 않은 경우 Get Object 요청이 '200 OK'를 잘못 반환할 수도 있습니다.

다음과 같은 경우:

- Get Object 요청이 일부 데이터를 반환하지만 전송 도중에 중지될 수 있습니다.
- 이후 개체 가져오기 요청이 403 사용 금지 를 반환할 수 있습니다.

관련 정보

서버측 암호화를 사용합니다

ILM을 사용하여 개체를 관리합니다

사후 개체 복원

S3 작업이 감사 로그에서 추적되었습니다

헤드 개체

S3 헤드 오브젝트 요청을 사용하여 오브젝트 자체를 반환하지 않고 오브젝트에서 메타데이터를 검색할 수 있습니다. 객체가 클라우드 스토리지 풀에 저장된 경우 헤드 객체를 사용하여 객체의 전환 상태를 확인할 수 있습니다.

헤드 개체 및 다중 파트 개체

'PARTNUMBER' 요청 파라미터를 사용하면 멀티파트 또는 분할된 개체의 특정 부분에 대한 메타데이터를 검색할 수 있습니다. X-amz-MP-parts-count 응답 요소는 개체의 부품 수를 나타냅니다.

분할/다중 파트 개체와 비분할/비다중 파트 개체 모두에 대해 'PARTNUMBER'를 1로 설정할 수 있지만, "x-amz-MP-parts-count" 응답 요소는 분할된 또는 다중 파트 개체에 대해서만 반환됩니다.

고객이 제공한 암호화 키**(SSE-C)**를 사용하여 서버측 암호화를 위한 요청 헤더

사용자가 제공한 고유 키로 개체를 암호화한 경우 이 헤더 3개를 모두 사용합니다.

- X-amz-서버측-암호화-고객-알고리즘: AES256 지정.

- 'x-amz-서버측-암호화-고객-키': 오브젝트의 암호화 키를 지정합니다.
- X-amz-서버측-암호화-고객-키-MD5: 오브젝트의 암호화 키에 대한 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.

사용자 메타데이터의 **UTF-8** 문자

StorageGRID는 사용자 정의 메타데이터에서 이스케이프된 UTF-8 문자를 구문 분석하거나 해석하지 않습니다. 사용자 정의 메타데이터에서 이스케이프된 UTF-8 문자가 있는 개체에 대한 헤드 요청은 키 이름이나 값에 인쇄할 수 없는 문자가 포함된 경우 "x-amz-missing-meta" 헤더를 반환하지 않습니다.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않으며 'XNotImplemented'를 반환합니다.

- X-amz-웹사이트-리디렉션-위치

클라우드 스토리지 풀 객체에 대한 응답 헤더입니다

객체가 클라우드 스토리지 풀에 저장된 경우(정보 수명 주기 관리를 통해 객체 관리 지침 참조) 다음 응답 헤더가 반환됩니다.

- X-amz-STERAGE-CLASS:빙하
- X-amz-restore

응답 헤더는 클라우드 스토리지 풀로 이동되는 오브젝트의 상태에 대한 정보를 제공하며, 선택적으로 검색할 수 없는 상태로 전환된 후 복구됩니다.

개체의 상태입니다	헤드 객체에 대한 응답
StorageGRID로 수집되었지만 아직 ILM에 의해 평가되지 않은 오브젝트 또는 기존 스토리지 풀에 저장된 오브젝트 또는 삭제 코딩 사용	200 OK (특별한 응답 헤더는 반환되지 않음)
Cloud Storage Pool의 개체이지만 아직 검색할 수 없는 상태로 전환되지 않았습니다	200OK X-amz-STERAGE-CLASS:빙하 "x-amz-restore:ongoing-request="false", expiry-date="sat, 23 JULY 20 2030 00:00:00:00 GMT" 객체가 검색 불가능한 상태로 전환되기 전까지 만료 날짜 값은 향후 일정 원거리 시간으로 설정됩니다. 정확한 전환 시간은 StorageGRID 시스템에 의해 제어되지 않습니다.

개체의 상태입니다	헤드 객체에 대한 응답
개체가 검색할 수 없는 상태로 전환되었지만 하나 이상의 복사본이 그리드에 있습니다	200OK X-amz-STERAGE-CLASS:빙하 "x-amz-restore:ongoing-request="false", expiry-date="sat, 23 JULY 20 2030 00:00:00:00 GMT" 만료 날짜 값은 앞으로 어느 정도 먼 시간으로 설정됩니다. • 참고 *: 그리드의 복사본을 사용할 수 없는 경우(예: 스토리지 노드가 다운된 경우), 객체를 성공적으로 검색하기 전에 POST 객체 복원 요청을 발행하여 클라우드 스토리지 풀에서 복제본을 복원해야 합니다.
개체가 검색할 수 없는 상태로 전환되었으며 그리드에 복사본이 없습니다	200OK X-amz-STERAGE-CLASS:빙하
복구할 수 없는 상태에서 복원 중인 개체입니다	200OK X-amz-STERAGE-CLASS:빙하 "x-amz-restore:진행 중인-request="true"'
객체가 클라우드 스토리지 풀에 완전히 복구되었습니다	200OK X-amz-STERAGE-CLASS:빙하 "x-amz-restore:ongoing-request="false", expiry-date="sat, 23 July 20 2018 00:00:00:00 GMT" '만료 날짜'는 Cloud Storage Pool의 객체가 검색 불가능한 상태로 반환되는 시점을 나타냅니다.

Cloud Storage Pool에서 다중 또는 분할 오브젝트 지원

여러 부분 개체를 업로드했거나 StorageGRID가 큰 개체를 세그먼트로 분할한 경우 StorageGRID는 개체의 부분 또는 세그먼트의 하위 집합을 샘플링하여 클라우드 저장소 풀에서 개체를 사용할 수 있는지 여부를 결정합니다. 일부 개체의 일부가 이미 검색 불가능 상태로 전환되었거나 개체의 일부가 아직 복원되지 않은 경우 헤드 객체 요청이 "x-amz-restore:ongoing-request="false""를 잘못 반환할 수 있습니다.

버전 관리

rrionId 서브리소스를 지정하지 않으면 가장 최근 버전의 객체가 버전 관리되는 버킷에 페치됩니다. 객체의 현재 버전이 삭제 표식이면 x-amz-DELETE-MARKER 응답 헤더가 TRUE로 설정된 상태로 "Not Found" 상태가 반환됩니다.

관련 정보

서버측 암호화를 사용합니다

ILM을 사용하여 개체를 관리합니다

사후 개체 복원

S3 작업이 감사 로그에서 추적되었습니다

사후 개체 복원

S3 POST 오브젝트 복원 요청을 사용하여 클라우드 스토리지 풀에 저장된 오브젝트를 복원할 수 있습니다.

지원되는 요청 유형입니다

StorageGRID는 개체 복원을 위한 POST 개체 복원 요청만 지원합니다. 복원의 선택 유형을 지원하지 않습니다. SELECT 요청은 'XNotImplemented'를 반환합니다.

버전 관리

필요한 경우 rionId를 지정하여 버전이 있는 버킷에서 개체의 특정 버전을 복원합니다. rionId를 지정하지 않으면 객체의 최신 버전이 복원됩니다

클라우드 스토리지 풀 객체에 대한 **POST** 객체 복구의 동작

개체가 클라우드 스토리지 풀에 저장된 경우(정보 수명 주기 관리를 통해 개체 관리 지침 참조) POST 개체 복원 요청은 개체의 상태에 따라 다음과 같은 동작을 수행합니다. 자세한 내용은 " 헤드 개체 "를 참조하십시오.

> 객체가 클라우드 스토리지 풀에 저장되어 있고 하나 이상의 오브젝트 복제본도 그리드에 있는 경우 POST 객체 복원 요청을 실행하여 객체를 복원할 필요가 없습니다. 대신 Get Object 요청을 사용하여 로컬 복사본을 직접 검색할 수 있습니다.

개체의 상태입니다	**POST** 개체 복원 동작
StorageGRID로 수집되었지만 ILM에서 아직 평가되지 않은 오브젝트 또는 클라우드 스토리지 풀에 없는 오브젝트	403 금지됨, InvalidObjectState
Cloud Storage Pool의 개체이지만 아직 검색할 수 없는 상태로 전환되지 않았습니다	200 OK 어떤 변경도 없다. • 참고 *: 객체가 검색 불가능한 상태로 전환되기 전에는 해당 '만료 날짜'를 변경할 수 없습니다.

개체의 상태입니다	**POST** 개체 복원 동작
개체가 검색할 수 없는 상태로 전환되었습니다	'202 수락됨'은 요청 본문에 지정된 일 동안 검색할 수 있는 객체 복사본을 클라우드 스토리지 풀에 복원합니다. 이 기간이 끝나면 객체는 복구할 수 없는 상태로 돌아갑니다. 선택적으로 "계층" 요청 요소를 사용하여 복원 작업이 완료될 때까지 걸리는 시간("신속", "표준" 또는 "대량")을 결정합니다. '계층'을 지정하지 않으면 '표준' 계층이 사용됩니다. • 주의 *: 오브젝트가 S3 Glacier Deep Archive로 전환되었거나 Cloud Storage Pool이 Azure Blob Storage를 사용하는 경우 "빠른" 계층을 사용하여 복원할 수 없습니다. 다음 오류는 403 사용 금지, InvalidTier로 반환됩니다. 검색 옵션은 이 저장소 클래스에서 지원되지 않습니다.
복구할 수 없는 상태에서 복원 중인 개체입니다	409갈등대, RestoreAlreadyInProgress
객체가 클라우드 스토리지 풀에 완전히 복구되었습니다	200OK • 참고: * 개체가 검색 가능한 상태로 복원되면, POST 개체 복원 요청을 새 값으로 다시 발행하여 '만료 날짜'를 변경할 수 있습니다. 복원 날짜는 요청 시간을 기준으로 업데이트됩니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

헤드 개체

S3 작업이 감사 로그에서 추적되었습니다

개체 를 넣습니다

S3 PUT 오브젝트 요청을 사용하여 오브젝트를 버킷에 추가할 수 있습니다.

충돌 해결

동일한 키에 쓰는 두 클라이언트 등의 충돌하는 클라이언트 요청은 "최신 성공" 기준으로 해결됩니다. "Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 합니다.

개체 크기

단일 PUT 오브젝트 작업의 maximum_recommended_size는 5GiB(5,368,709,120바이트)입니다. 5GiB보다 큰 객체가 있는 경우 대신 멀티파트 업로드를 사용합니다.

> StorageGRID 11.6에서 단일 PUT 객체 작업에 대한 Maximum_supported_size는 5TiB(5,497,558,138,880바이트)입니다. 그러나 5GiB를 초과하는 개체를 업로드하려고 하면 * S3 PUT 오브젝트 크기가 너무 큼 * 경고가 트리거됩니다.

사용자 메타데이터 크기입니다

Amazon S3는 각 PUT 요청 헤더 내의 사용자 정의 메타데이터 크기를 2KB로 제한합니다. StorageGRID는 사용자 메타데이터를 24KiB로 제한합니다. 사용자 정의 메타데이터의 크기는 각 키와 값의 UTF-8 인코딩에서 바이트 수의 합계를 구하여 측정됩니다.

사용자 메타데이터의 **UTF-8** 문자

요청에 사용자 정의 메타데이터의 키 이름이나 값에 UTF-8 값이 포함되어 있으면 StorageGRID 동작이 정의되지 않습니다.

StorageGRID는 사용자 정의 메타데이터의 키 이름이나 값에 포함된 이스케이프된 UTF-8 문자를 구문 분석하거나 해석하지 않습니다. 이스케이프된 UTF-8 문자는 ASCII 문자로 처리됩니다.

- 사용자 정의 메타데이터에 이스케이프된 UTF-8 문자가 포함된 경우 Put, Put Object-Copy, Get 및 head 요청이 성공합니다.
- StorageGRID는 키 이름 또는 값의 해석된 값에 인쇄할 수 없는 문자가 포함된 경우 "x-amz-missing-meta" 헤더를 반환하지 않습니다.

개체 태그 제한

새 개체를 업로드할 때 태그를 추가하거나 기존 개체에 태그를 추가할 수 있습니다. StorageGRID 및 Amazon S3 모두 각 오브젝트에 대해 최대 10개의 태그를 지원합니다. 개체와 관련된 태그에는 고유한 태그 키가 있어야 합니다. 태그 키의 길이는 최대 128자의 유니코드 문자이고 태그 값의 길이는 최대 256자의 유니코드 문자일 수 있습니다. 키와 값은 대/소문자를 구분합니다.

개체 소유권

StorageGRID에서는 소유자가 아닌 계정 또는 익명 사용자가 만든 개체를 포함하여 모든 개체가 버킷 소유자 계정에 의해 소유됩니다.

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- 캐시-컨트롤
- 'Content-Disposition'
- 콘텐츠 인코딩

  Content-Encoding의 torageGRID에 대해 AWS-chunched를 지정하면 다음 항목을 확인할 수 없습니다.

  - StorageGRID는 청크 데이터에 대해 청크 서명을 확인하지 않습니다.
  - StorageGRID는 오브젝트에 대해 사용자가 "x-amz-decoded-content-length"를 제공하는 값을 확인하지 않습니다.
- 컨텐츠-언어

- 콘텐츠 길이
- 내용-MD5
- 콘텐츠 유형
- '만료'
- 전송 인코딩

  AWS-chunched 페이로드 서명도 사용되는 경우 청크된 전송 인코딩이 지원됩니다.

- x-amz-meta- 뒤에 사용자 정의 메타데이터를 포함하는 이름-값 쌍이 있습니다.

  사용자 정의 메타데이터에 대한 이름 값 쌍을 지정할 때 다음 일반 형식을 사용합니다.

```
x-amz-meta-name: value
```

  ILM 규칙의 참조 시간으로 * 사용자 정의 작성 시간 * 옵션을 사용하려면 객체를 만들 때 기록하는 메타데이터의 이름으로 "creation-time"을 사용해야 합니다. 예를 들면 다음과 같습니다.

```
x-amz-meta-creation-time: 1443399726
```

  창조시간 값은 1970년 1월 1일 이후 초 단위로 평가된다.

  ILM 규칙은 참조 시간에 * 사용자 정의 작성 시간 * 과 수집 동작에 대한 균형 또는 엄격 옵션을 모두 사용할 수 없습니다. ILM 규칙을 만들면 오류가 반환됩니다.

- X-amz-태깅
- S3 오브젝트 잠금 요청 헤더
  - 'X-amz-object-lock-mode
  - 'X-amz-object-lock-retain-until-date'
  - X-amz-object-lock-legal-hold

    이러한 헤더 없이 요청이 이루어지면 버킷 기본 보존 설정을 사용하여 개체 버전 보존 기간을 계산합니다.

  S3 오브젝트 잠금을 사용합니다

- SSE 요청 헤더:
  - 'X-amz-서버측-암호화'
  - X-amz-서버측-암호화-고객-키-MD5
  - 'X-amz-서버측-암호화-고객-키'
  - 'X-amz-서버측-암호화-고객-알고리즘'

    을 참조하십시오 서버측 암호화에 대한 요청 헤더

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

- X-amz-ACL 요청 헤더는 지원되지 않습니다.
- X-amz-website-redirect-location 요청 헤더는 지원되지 않으며 XNotImplemented를 반환합니다.

스토리지 클래스 옵션

X-amz-STERAGE-CLASS 요청 헤더는 지원된다. 'x-amz-storage-class'에 대해 제출된 가치는 수집 중에 StorageGRID가 오브젝트 데이터를 보호하는 방식에 영향을 주며, ILM에 의해 결정되는 StorageGRID 시스템에 저장된 개체의 영구 복사본의 수가 아닙니다.

수집된 개체와 일치하는 ILM 규칙이 Ingest 동작에 Strict 옵션을 사용하는 경우 "x-amz-storage-class" 헤더는 영향을 주지 않습니다.

X-amz-storage-class에 사용할 수 있는 값은 다음과 같다.

- '표준'(기본값)
  - * 이중 커밋 *: ILM 규칙이 Ingest 동작에 대한 이중 커밋 옵션을 지정하는 경우, 개체가 수집되는 즉시 해당 개체의 두 번째 복사본이 생성되어 다른 스토리지 노드(이중 커밋)에 배포됩니다. ILM을 평가할 때 StorageGRID는 이러한 초기 중간 복사본이 규칙의 배치 지침을 충족하는지 여부를 결정합니다. 그렇지 않으면 새 오브젝트 복사본을 다른 위치에 만들어야 하고 초기 중간 복사본을 삭제해야 할 수 있습니다.
  - * 균형 *: ILM 규칙이 균형 옵션을 지정하고 StorageGRID이 규칙에 지정된 모든 복사본을 즉시 만들 수 없는 경우 StorageGRID은 다른 스토리지 노드에 두 개의 임시 복사본을 만듭니다.

    StorageGRID에서 ILM 규칙(동기 배치)에 지정된 모든 오브젝트 복사본을 즉시 생성할 수 있으면 'x-amz-storage-class' 헤더가 효과가 없습니다.
- Reduced_redundancy를 선택합니다
  - * 이중 커밋 *: ILM 규칙이 Ingest 동작에 대한 이중 커밋 옵션을 지정하는 경우 StorageGRID는 오브젝트가 수집될 때(단일 커밋) 단일 임시 복사본을 만듭니다.
  - * 균형 *: ILM 규칙이 균형 옵션을 지정하는 경우 StorageGRID은 시스템에서 규칙에 지정된 모든 사본을 즉시 만들 수 없는 경우에만 단일 중간 복사본을 만듭니다. StorageGRID에서 동기 배치를 수행할 수 있는 경우 이 머리글은 영향을 주지 않습니다. Reduced_redundancy 옵션은 개체와 일치하는 ILM 규칙이 복제된 단일 복사본을 만들 때 가장 적합합니다. 이 경우 'REDED_READITORY'를 사용하면 모든 수집 작업에 대해 불필요한 오브젝트 복사본을 생성하고 삭제할 필요가 없습니다.

  다른 상황에서는 reducted_redundancy 옵션을 사용하지 않는 것이 좋습니다. REDED_READITAINEY는 수집 중에 오브젝트 데이터가 손실될 위험을 증가시킵니다. 예를 들어, ILM 평가가 발생하기 전에 실패한 스토리지 노드에 단일 복사본이 처음 저장되는 경우 데이터가 손실될 수 있습니다.

- 주의 *: 한 번에 하나의 복제 사본만 있으면 데이터가 영구적으로 손실될 위험이 있습니다. 복제된 객체 복제본이 하나만 있는 경우 스토리지 노드에 장애가 발생하거나 심각한 오류가 발생한 경우 해당 객체가 손실됩니다. 또한 업그레이드와 같은 유지보수 절차 중에는 개체에 대한 액세스가 일시적으로 중단됩니다.

reducted_redundancy를 지정하면 개체를 처음 인제스트할 때 생성되는 복제본 수만 영향을 받습니다. 활성 ILM 정책에 따라 개체를 평가할 때 개체의 복사본 수에 영향을 주지 않으며 StorageGRID 시스템에서 낮은 수준의 중복성에 데이터가 저장되지 않습니다.

- 참고 *: S3 오브젝트 잠금이 활성화된 버킷으로 오브젝트를 인스팅하는 경우, reducted_redundancy 옵션이

무시됩니다. 개체를 레거시 준수 버킷으로 인스팅하는 경우 REDED_REPREADITORIAL' 옵션은 오류를 반환합니다. StorageGRID은 규정 준수 요구 사항이 충족될 수 있도록 항상 이중 커밋 수집을 수행합니다.

서버측 암호화에 대한 요청 헤더

다음 요청 헤더를 사용하여 서버측 암호화를 사용하여 개체를 암호화할 수 있습니다. SSE 및 SSE-C 옵션은 상호 배타적입니다.

- * SSE *: StorageGRID에서 관리하는 고유 키를 사용하여 오브젝트를 암호화하려면 다음 헤더를 사용하십시오.
  - 'X-amz-서버측-암호화'
- * SSE-C *: 사용자가 제공 및 관리하는 고유 키로 객체를 암호화하려면 이 헤더 세 개를 모두 사용합니다.
  - X-amz-서버측-암호화-고객-알고리즘: AES256 지정.
  - 'X-amz-서버측-암호화-고객 키': 새 오브젝트의 암호화 키를 지정합니다.
  - X-amz-서버측-암호화-고객-키-MD5: 새 개체의 암호화 키에 대해 MD5 다이제스트를 지정합니다.
- 주의: * 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.
- 참고: * 개체가 SSE 또는 SSE-C로 암호화된 경우 버킷 수준 또는 그리드 수준 암호화 설정은 무시됩니다.

버전 관리

버켓에 대한 버전 관리가 활성화된 경우 저장할 개체의 버전에 대해 고유한 rionId가 자동으로 생성됩니다. 이 인상파 ID는 X-amz-version-id 응답 헤더를 사용하여 응답에서도 반환됩니다.

버전 관리가 일시 중단된 경우 개체 버전은 null rionId로 저장되며, null 버전이 이미 있는 경우에는 덮어쓰게 됩니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

버킷 작업

S3 작업이 감사 로그에서 추적되었습니다

서버측 암호화를 사용합니다

클라이언트 연결 구성 방법

개체 - 복사 를 선택합니다

S3 PUT 오브젝트 복사 요청을 사용하여 S3에 이미 저장된 오브젝트 복사본을 생성할 수 있습니다. Put Object - Copy 작업은 GET 및 PUT를 수행하는 작업과 동일합니다.

충돌 해결

동일한 키에 쓰는 두 클라이언트 등의 충돌하는 클라이언트 요청은 "최신 성공" 기준으로 해결됩니다. "Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 합니다.

개체 크기

단일 PUT 오브젝트 작업의 maximum_recommended_size는 5GiB(5,368,709,120바이트)입니다. 5GiB보다 큰 객체가 있는 경우 대신 멀티파트 업로드를 사용합니다.

> StorageGRID 11.6에서 단일 PUT 객체 작업에 대한 Maximum_supported_size는 5TiB(5,497,558,138,880바이트)입니다. 그러나 5GiB를 초과하는 개체를 업로드하려고 하면 * S3 PUT 오브젝트 크기가 너무 큼 * 경고가 트리거됩니다.

사용자 메타데이터의 **UTF-8** 문자

요청에 사용자 정의 메타데이터의 키 이름이나 값에 UTF-8 값이 포함되어 있으면 StorageGRID 동작이 정의되지 않습니다.

StorageGRID는 사용자 정의 메타데이터의 키 이름이나 값에 포함된 이스케이프된 UTF-8 문자를 구문 분석하거나 해석하지 않습니다. 이스케이프된 UTF-8 문자는 ASCII 문자로 처리됩니다.

- 사용자 정의 메타데이터에 이스케이프된 UTF-8 문자가 포함된 경우 요청이 성공합니다.
- StorageGRID는 키 이름 또는 값의 해석된 값에 인쇄할 수 없는 문자가 포함된 경우 "x-amz-missing-meta" 헤더를 반환하지 않습니다.

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- 콘텐츠 유형
- X-amz-copy 소스
- X-amz-copy-source-if-match
- X-amz-copy-source-if-none-match
- X-amz-copy-source-if-수정되지 않음-since
- X-amz-copy-source-if-modified-since
- x-amz-meta- 뒤에 사용자 정의 메타데이터를 포함하는 이름-값 쌍이 있습니다
- 'x-amz-metadata-directive': 기본값은 'copy'로, 객체와 관련 메타데이터를 복사할 수 있습니다.

  오브젝트를 복사할 때 기존 메타데이터를 덮어쓰거나 오브젝트 메타데이터를 업데이트하도록 "replace"를 지정할 수 있습니다.

- X-amz-스토리지 클래스
- 'x-amz-tagging-directive': 기본값은 'copy'로, 객체와 모든 태그를 복사할 수 있습니다.

  개체를 복사할 때 기존 태그를 덮어쓰거나 태그를 업데이트하려면 "다시 배치"를 지정할 수 있습니다.

- S3 오브젝트 잠금 요청 헤더:
  - 'X-amz-object-lock-mode
  - 'X-amz-object-lock-retain-until-date'
  - X-amz-object-lock-legal-hold

이러한 헤더 없이 요청이 이루어지면 버킷 기본 보존 설정을 사용하여 개체 버전 보존 기간을 계산합니다.

S3 오브젝트 잠금을 사용합니다

- SSE 요청 헤더:
  - "x-amz-copy-sourcestevids-server-sideencryptionsever-customer-algorithm"입니다
  - X-amz-copy-sources.\xserver-side-encryption-customer-key
  - "X-amz-copy-sourcestifs-server-side-encryption-customer-key-md5'
  - 'X-amz-서버측-암호화'
  - X-amz-서버측-암호화-고객-키-MD5
  - 'X-amz-서버측-암호화-고객-키'
  - 'X-amz-서버측-암호화-고객-알고리즘'

  을 참조하십시오 서버측 암호화에 대한 요청 헤더

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

- 캐시-컨트롤
- 'Content-Disposition'
- 콘텐츠 인코딩
- 컨텐츠-언어
- '만료'
- X-amz-웹사이트-리디렉션-위치

스토리지 클래스 옵션

"x-amz-storage-class" 요청 헤더가 지원되며 일치하는 ILM 규칙에서 이중 커밋 또는 밸런스의 수집 동작을 지정하는 경우 StorageGRID에서 생성되는 개체 복사본 수에 영향을 줍니다.

- '표준'입니다

  (기본값) ILM 규칙이 이중 커밋 옵션을 사용하거나 균형 옵션이 중간 복사본 생성으로 돌아올 때 이중 커밋 수집 작업을 지정합니다.

- Reduced_redundancy를 선택합니다

  ILM 규칙이 이중 커밋 옵션을 사용하거나 균형 옵션이 중간 복사본 생성으로 돌아올 때 단일 커밋 수집 작업을 지정합니다.

> S3 오브젝트 잠금이 활성화된 버킷으로 오브젝트를 인스팅하는 경우 REDED_REPREADITORY' 옵션이 무시됩니다. 개체를 레거시 준수 버킷으로 인스팅하는 경우 REDED_REPREADITORIAL' 옵션은 오류를 반환합니다. StorageGRID은 규정 준수 요구 사항이 충족될 수 있도록 항상 이중 커밋 수집을 수행합니다.

Put Object - Copy에서 **x-amz-copy-source** 사용

x-amz-copy-source 헤더에 지정된 소스 버킷과 키가 대상 버킷 및 키와 다른 경우 소스 객체 데이터의 복제본이 대상에 기록됩니다.

소스와 대상이 일치하고 "x-amz-metadata-directive" 헤더가 replace"로 지정된 경우 해당 요청의 메타데이터 값으로 오브젝트의 메타데이터가 업데이트됩니다. 이 경우 StorageGRID는 오브젝트를 다시 수집하지 않습니다. 여기에는 두 가지 중요한 결과가 있습니다.

- Put Object-Copy를 사용하여 기존 개체를 현재 위치에서 암호화하거나 기존 개체의 암호화를 변경할 수 없습니다. X-amz-서버측-암호화 헤더나 x-amz-서버측-암호화-고객-알고리즘 헤더를 제공하면 StorageGRID는 요청을 거부하고 XNotImplemented를 반환합니다.
- 일치하는 ILM 규칙에 지정된 Ingest 동작 옵션은 사용되지 않습니다. ILM이 정상적인 백그라운드 ILM 프로세스에 의해 다시 평가될 때 업데이트로 인해 트리거되는 개체 배치에 대한 모든 변경 사항이 발생합니다.

  즉, ILM 규칙이 수집 동작에 Strict 옵션을 사용하는 경우 필요한 개체 배치를 만들 수 없는 경우(예: 새로 필요한 위치를 사용할 수 없음) 작업이 수행되지 않습니다. 업데이트된 오브젝트는 필요한 배치가 가능할 때까지 현재 위치를 유지합니다.

서버측 암호화에 대한 요청 헤더

서버 측 암호화를 사용하는 경우 소스 개체가 암호화되었는지 여부 및 대상 개체를 암호화할 계획인지에 따라 요청 헤더가 제공됩니다.

- 소스 객체가 SSE-C(customer-provided key)를 사용하여 암호화된 경우, 객체를 해독한 다음 복사할 수 있도록 객체 복사 요청(Put Object-Copy request)에 다음 세 개의 헤더를 포함해야 합니다.
  - X-amz-copy-sourcesources. ever-sideboretationsencryptionsever-customer-algorithm은 AES256을 지정합니다.
  - 'x-amz-copy-sourcesources.x.server-side-encryption-customer-key'는 소스 객체를 만들 때 제공한 암호화 키를 지정합니다.
  - "x-amz-copy-sourcesourcesifx-server-side-encryption-customer-key-md5': 소스 개체를 만들 때 제공한 MD5 다이제스트를 지정합니다.
- 제공 및 관리하는 고유 키를 사용하여 대상 개체(복사본)를 암호화하려면 다음 세 개의 머리글을 포함합니다.
  - X-amz-서버측-암호화-고객-알고리즘: AES256 지정.
  - 'X-amz-서버측-암호화-고객-키': 대상 객체에 대한 새 암호화 키를 지정합니다.
  - X-amz-서버측-암호화-고객-키-MD5: 새 암호화 키의 MD5 다이제스트를 지정합니다.
- 주의: * 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.
- SSE(StorageGRID)에서 관리되는 고유 키로 대상 객체(사본)를 암호화하려면 객체 복사 요청(Put Object-Copy request)에 이 헤더를 포함시킵니다.
  - 'X-amz-서버측-암호화'

참고: * 오브젝트의 '서버측 암호화' 값은 업데이트할 수 없습니다. 대신 X-amz-metadata-directive:replace를 사용하여 새로운 서버 측 암호화 값으로 복사본을 만듭니다.

버전 관리

소스 버킷의 버전이 있는 경우 "x-amz-copy-source" 헤더를 사용하여 객체의 최신 버전을 복사할 수 있습니다. 개체의 특정 버전을 복사하려면 rionId 하위 리소스를 사용하여 복사할 버전을 명시적으로 지정해야 합니다. 목적지 버킷의 버전 관리가 되면 생성된 버전은 'x-amz-version-id' 응답 헤더로 반환됩니다. 대상 버킷의 버전 관리가 일시 중단된 경우 x-amz-version-id는 "null" 값을 반환합니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

서버측 암호화를 사용합니다

S3 작업이 감사 로그에서 추적되었습니다

개체 를 넣습니다

SelectObjectContent 를 선택합니다

S3 SelectObjectContent 요청을 사용하여 간단한 SQL 문을 기반으로 S3 개체의 내용을 필터링할 수 있습니다.

자세한 내용은 를 참조하십시오 "SelectObjectContent에 대한 AWS 문서".

필요한 것

- 테넌트 계정에 S3 Select 권한이 있습니다.
- 쿼리할 객체에 대한 '3:GetObject' 권한이 있습니다.
- 쿼리할 객체가 CSV 형식이거나 CSV 형식 파일이 포함된 GZIP 또는 BZIP2 압축 파일입니다.
- SQL 식의 최대 길이는 256KB입니다.
- 입력 또는 결과에 있는 모든 레코드의 최대 길이는 1MiB입니다.

요청 구문 예

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

SQL 쿼리의 예

이 쿼리는 시/도 이름, 2010년 인구, 2015년 예상 인구, 미국 인구 조사 데이터의 변경 비율을 가져옵니다. 파일에 있는 상태가 아닌 레코드는 무시됩니다.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

질의할 파일의 처음 몇 줄인 'sub-EST2020_all.csv'는 다음과 같습니다.

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

AWS-CLI 사용 예

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

출력 파일의 처음 몇 줄인 changes.csv는 다음과 같습니다.

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

멀티파트 업로드 작업

이 섹션에서는 StorageGRID가 멀티파트 업로드 작업을 지원하는 방법에 대해 설명합니다.

다음 조건 및 참고 사항은 모든 다중 파트 업로드 작업에 적용됩니다.

- 해당 버킷에 대한 다중 파트 업로드 나열 쿼리 결과는 불완전한 결과를 반환할 수 있으므로 단일 버킷에 대한 동시 다중 파트 업로드 1,000개를 초과할 수 없습니다.
- StorageGRID는 여러 파트에 대해 AWS 크기 제한을 적용합니다. S3 클라이언트는 다음 지침을 따라야 합니다.
  - 멀티파트 업로드의 각 파트는 5MiB(5,242,880바이트)와 5GiB(5,368,709,120바이트) 사이여야 합니다.
  - 마지막 부분은 5MiB(5,242,880바이트)보다 작을 수 있습니다.
  - 일반적으로 파트 크기는 가능한 한 커야합니다. 예를 들어, 100GiB 개체의 경우 5GiB의 파트 크기를 사용합니다. 각 파트는 고유한 개체로 간주되므로 큰 파트 크기를 사용하면 StorageGRID 메타데이터 오버헤드가 줄어듭니다.
  - 5GiB보다 작은 오브젝트의 경우 대신 비다중 파트 업로드를 사용하는 것이 좋습니다.
- ILM 규칙이 Strict 또는 Balanced 수집 동작을 사용하는 경우 ILM은 다중 파트 개체의 각 부분을 인제스트할 때 계산되고 다중 파트 업로드가 완료될 때 전체 개체에 대해 평가됩니다. 이 사항이 개체 및 파트 배치에 미치는 영향에 대해 알고 있어야 합니다.
  - S3 멀티파트 업로드가 진행 중인 동안 ILM이 변경되면 멀티파트 업로드가 완료될 때 개체의 일부 부분이 현재 ILM 요구 사항을 충족하지 못할 수 있습니다. 올바르게 배치되지 않은 모든 부품은 ILM 재평가를 위해 대기 중이며 나중에 올바른 위치로 이동됩니다.
  - 파트에 대한 ILM을 평가할 때 StorageGRID은 개체의 크기가 아닌 파트 크기를 필터링합니다. 즉, 개체의 일부를 개체의 ILM 요구 사항을 전체가 충족하지 않는 위치에 저장할 수 있습니다. 예를 들어, 규칙이 모든 오브젝트 10GB 이상이 DC1에 저장되는 반면 모든 작은 오브젝트는 DC2에 저장되는 것으로 지정하는 경우 10개 부분 멀티파트 업로드의 각 1GB 부분은 DC2에 저장됩니다. 개체에 대한 ILM을 전체적으로 평가할 때 개체의 모든 부분이 DC1로 이동합니다.
- 모든 멀티파트 업로드 작업은 StorageGRID 정합성 제어를 지원합니다.
- 필요한 경우 다중 파트 업로드와 함께 서버측 암호화를 사용할 수 있습니다. SSE(StorageGRID 관리 키가 있는 서버쪽 암호화)를 사용하려면 '다중 파트 업로드 시작' 요청에만 'x-amz-서버측-암호화' 요청 헤더가 포함됩니다. SSE-C(고객이 제공한 키와 함께 서버측 암호화)를 사용하려면 다중 파트 업로드 시작 요청 및 각 후속 업로드 파트 요청에서 동일한 세 가지 암호화 키 요청 헤더를 지정합니다.

작동	구축
다중 파트 업로드 나열	을 참조하십시오 다중 파트 업로드 나열
멀티파트 업로드를 시작합니다	을 참조하십시오 멀티파트 업로드를 시작합니다

작동	구축
부품 업로드	을 참조하십시오 부품 업로드
업로드 부품 - 복사	을 참조하십시오 업로드 부품 - 복사
멀티파트 업로드를 완료합니다	을 참조하십시오 멀티파트 업로드를 완료합니다
멀티파트 업로드를 중단합니다	모든 Amazon S3 REST API 동작으로 구현됩니다
파트 목록	모든 Amazon S3 REST API 동작으로 구현됩니다

관련 정보

- 일관성 제어
- 서버측 암호화를 사용합니다

다중 파트 업로드 나열

다중 파트 업로드 나열 작업은 버킷에 대해 진행 중인 다중 파트 업로드를 나열합니다.

지원되는 요청 매개 변수는 다음과 같습니다.

- 인코딩 형식
- 최대 업로드
- 키-마커
- 접두사
- 업로드-ID-마커

기한도자 요청 매개변수는 지원되지 않습니다.

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. 전체 다중 파트 업로드 작업이 수행되는 경우, 즉 개체가 작성되는 시점(해당되는 경우 버전)입니다.

멀티파트 업로드를 시작합니다

다중 파트 업로드 시작 작업은 개체에 대한 다중 파트 업로드를 시작하고 업로드 ID를 반환합니다.

X-amz-STERAGE-CLASS 요청 헤더는 지원된다. 'x-amz-storage-class'에 대해 제출된 가치는 수집 중에 StorageGRID가 오브젝트 데이터를 보호하는 방식에 영향을 주며, ILM에 의해 결정되는 StorageGRID 시스템에 저장된 개체의 영구 복사본의 수가 아닙니다.

수집된 개체와 일치하는 ILM 규칙이 Ingest 동작에 Strict 옵션을 사용하는 경우 "x-amz-storage-class" 헤더는 영향을

주지 않습니다.

X-amz-storage-class에 사용할 수 있는 값은 다음과 같다.

- '표준'(기본값)
  - * 이중 커밋 *: ILM 규칙이 Ingest 동작에 대한 이중 커밋 옵션을 지정하는 경우, 개체가 수집되는 즉시 해당 개체의 두 번째 복사본이 생성되어 다른 스토리지 노드(이중 커밋)에 배포됩니다. ILM을 평가할 때 StorageGRID는 이러한 초기 중간 복사본이 규칙의 배치 지침을 충족하는지 여부를 결정합니다. 그렇지 않으면 새 오브젝트 복사본을 다른 위치에 만들어야 하고 초기 중간 복사본을 삭제해야 할 수 있습니다.
  - * 균형 *: ILM 규칙이 균형 옵션을 지정하고 StorageGRID이 규칙에 지정된 모든 복사본을 즉시 만들 수 없는 경우 StorageGRID은 다른 스토리지 노드에 두 개의 임시 복사본을 만듭니다.

    StorageGRID에서 ILM 규칙(동기 배치)에 지정된 모든 오브젝트 복사본을 즉시 생성할 수 있으면 'x-amz-storage-class' 헤더가 효과가 없습니다.

- Reduced_redundancy를 선택합니다
  - * 이중 커밋 *: ILM 규칙이 Ingest 동작에 대한 이중 커밋 옵션을 지정하는 경우 StorageGRID는 오브젝트가 수집될 때(단일 커밋) 단일 임시 복사본을 만듭니다.
  - * 균형 *: ILM 규칙이 균형 옵션을 지정하는 경우 StorageGRID은 시스템에서 규칙에 지정된 모든 사본을 즉시 만들 수 없는 경우에만 단일 중간 복사본을 만듭니다. StorageGRID에서 동기 배치를 수행할 수 있는 경우 이 머리글은 영향을 주지 않습니다. Reduced_redundancy 옵션은 개체와 일치하는 ILM 규칙이 복제된 단일 복사본을 만들 때 가장 적합합니다. 이 경우 'REDED_READITORY'를 사용하면 모든 수집 작업에 대해 불필요한 오브젝트 복사본을 생성하고 삭제할 필요가 없습니다.

  다른 상황에서는 reducted_redundancy 옵션을 사용하지 않는 것이 좋습니다. REDED_READITAINEY는 수집 중에 오브젝트 데이터가 손실될 위험을 증가시킵니다. 예를 들어, ILM 평가가 발생하기 전에 실패한 스토리지 노드에 단일 복사본이 처음 저장되는 경우 데이터가 손실될 수 있습니다.

- 주의 *: 한 번에 하나의 복제 사본만 있으면 데이터가 영구적으로 손실될 위험이 있습니다. 복제된 객체 복제본이 하나만 있는 경우 스토리지 노드에 장애가 발생하거나 심각한 오류가 발생한 경우 해당 객체가 손실됩니다. 또한 업그레이드와 같은 유지보수 절차 중에는 개체에 대한 액세스가 일시적으로 중단됩니다.

reducted_redundancy를 지정하면 개체를 처음 인제스트할 때 생성되는 복제본 수만 영향을 받습니다. 활성 ILM 정책에 따라 개체를 평가할 때 개체의 복사본 수에 영향을 주지 않으며 StorageGRID 시스템에서 낮은 수준의 중복성에 데이터가 저장되지 않습니다.

- 참고 *: S3 오브젝트 잠금이 활성화된 버킷으로 오브젝트를 인스팅하는 경우, reducted_redundancy 옵션이 무시됩니다. 개체를 레거시 준수 버킷으로 인스팅하는 경우 REDED_REPREADITORIAL' 옵션은 오류를 반환합니다. StorageGRID은 규정 준수 요구 사항이 충족될 수 있도록 항상 이중 커밋 수집을 수행합니다.

지원되는 요청 헤더는 다음과 같습니다.

- 콘텐츠 유형
- x-amz-meta- 뒤에 사용자 정의 메타데이터를 포함하는 이름-값 쌍이 있습니다

  사용자 정의 메타데이터에 대한 이름 값 쌍을 지정할 때 다음 일반 형식을 사용합니다.

  ```
  x-amz-meta-_name_: `value`
  ```

ILM 규칙의 참조 시간으로 * 사용자 정의 작성 시간 * 옵션을 사용하려면 객체를 만들 때 기록하는 메타데이터의 이름으로 "creation-time"을 사용해야 합니다. 예를 들면 다음과 같습니다.

```
x-amz-meta-creation-time: 1443399726
```

창조시간 값은 1970년 1월 1일 이후 초 단위로 평가된다.

> 레거시 규정 준수 기능이 설정된 버킷에 객체를 추가하는 경우 사용자 정의 메타데이터로 '생성 시간'을 추가할 수 없습니다. 오류가 반환됩니다.

- S3 오브젝트 잠금 요청 헤더:
  - 'X-amz-object-lock-mode
  - 'X-amz-object-lock-retain-until-date'
  - X-amz-object-lock-legal-hold

    이러한 헤더 없이 요청이 이루어지면 버킷 기본 보존 설정을 사용하여 개체 버전 보존 기간을 계산합니다.

  S3 오브젝트 잠금 사용

- SSE 요청 헤더:
  - 'X-amz-서버측-암호화'
  - X-amz-서버측-암호화-고객-키-MD5
  - 'X-amz-서버측-암호화-고객-키'
  - 'X-amz-서버측-암호화-고객-알고리즘'

    서버측 암호화에 대한 요청 헤더

> StorageGRID에서 UTF-8 문자를 처리하는 방법에 대한 자세한 내용은 Put Object 설명서를 참조하십시오.

서버측 암호화에 대한 요청 헤더

다음 요청 헤더를 사용하여 서버측 암호화를 사용하여 다중 파트 개체를 암호화할 수 있습니다. SSE 및 SSE-C 옵션은 상호 배타적입니다.

- * SSE *: StorageGRID에서 관리하는 고유 키로 객체를 암호화하려면 다중 파트 업로드 시작 요청에서 다음 헤더를 사용하십시오. 업로드 부품 요청에 이 헤더를 지정하지 마십시오.
  - 'X-amz-서버측-암호화'
- * SSE-C *: 사용자가 제공 및 관리하는 고유 키를 사용하여 개체를 암호화하려는 경우 다중 파트 업로드 시작 요청(및 각 후속 업로드 파트 요청)에서 이 헤더 세 개를 모두 사용합니다.
  - X-amz-서버측-암호화-고객-알고리즘: AES256 지정.
  - 'X-amz-서버측-암호화-고객 키': 새 오브젝트의 암호화 키를 지정합니다.

  - X-amz-서버측-암호화-고객-키-MD5: 새 개체의 암호화 키에 대해 MD5 다이제스트를 지정합니다.
- 주의: * 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않으며 'XNotImplemented'를 반환합니다

- X-amz-웹사이트-리디렉션-위치

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. MultiPart Upload 작업이 완료되면 개체가 만들어지고 버전이 적용됩니다(해당하는 경우).

관련 정보

ILM을 사용하여 개체를 관리합니다

서버측 암호화를 사용합니다

개체 를 넣습니다

부품 업로드

파트 업로드 작업은 개체에 대해 여러 부분으로 업로드되는 파트를 업로드합니다.

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- 콘텐츠 길이
- 내용-MD5

서버측 암호화에 대한 요청 헤더

다중 파트 업로드 시작 요청에 대해 SSE-C 암호화를 지정한 경우 각 업로드 파트 요청에 다음 요청 헤더를 포함해야 합니다.

- X-amz-서버측-암호화-고객-알고리즘: AES256 지정.
- 'x-amz-서버측-암호화-고객 키': '멀티파트 업로드 시작' 요청에서 제공한 암호화 키와 동일한 암호화 키를 지정합니다.
- "X-amz-서버측-암호화-고객-키-MD5': '멀티파트 업로드 시작' 요청에서 제공한 것과 동일한 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. MultiPart Upload 작업이 완료되면 개체가 만들어지고 버전이 적용됩니다(해당하는 경우).

관련 정보

서버측 암호화를 사용합니다

업로드 부품 - 복사

파트 업로드 - 복사 작업은 기존 개체의 데이터를 데이터 소스로 복사하여 개체의 일부를 업로드합니다.

Part-Copy 업로드 작업은 모든 Amazon S3 REST API 동작으로 구현됩니다.

이 요청은 StorageGRID 시스템 내에서 'x-amz-copy-source-range'에 지정된 객체 데이터를 읽고 씁니다.

지원되는 요청 헤더는 다음과 같습니다.

- X-amz-copy-source-if-match
- X-amz-copy-source-if-none-match
- X-amz-copy-source-if-수정되지 않음-since
- X-amz-copy-source-if-modified-since

서버측 암호화에 대한 요청 헤더

다중 파트 업로드 시작 요청에 대해 SSE-C 암호화를 지정한 경우 각 업로드 파트 - 복사 요청에 다음 요청 헤더를 포함해야 합니다.

- X-amz-서버측-암호화-고객-알고리즘: AES256 지정.
- 'x-amz-서버측-암호화-고객 키': '멀티파트 업로드 시작' 요청에서 제공한 암호화 키와 동일한 암호화 키를 지정합니다.
- "X-amz-서버측-암호화-고객-키-MD5': '멀티파트 업로드 시작' 요청에서 제공한 것과 동일한 MD5 다이제스트를 지정합니다.

소스 객체가 SSE-C(customer-provided key)를 사용하여 암호화된 경우, 객체가 해독되고 복사될 수 있도록 업로드 파트 - 복사 요청에 다음 세 개의 헤더를 포함해야 합니다.

- 'x-amz-copy-sourcesources. ever-sideboretationsencryptionsever-customer-algorithm': AES256 지정.
- 'x-amz-copy-sourcesources.x.server-side-encryption-customer-key': 소스 객체를 만들 때 제공한 암호화 키를 지정합니다.
- "x-amz-copy-sourcesourcesifx-server-side-encryption-customer-key-md5': 소스 개체를 만들 때 제공한 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 오브젝트 데이터를 보호하기 전에 "'서버측 암호화 사용'의 고려 사항을 검토하십시오.

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. MultiPart Upload 작업이 완료되면 개체가 만들어지고 버전이 적용됩니다(해당하는 경우).

멀티파트 업로드를 완료합니다

전체 다중 파트 업로드 작업은 이전에 업로드한 파트를 조립하여 개체의 여러 부분 업로드를 완료합니다.

충돌 해결

동일한 키에 쓰는 두 클라이언트 등의 충돌하는 클라이언트 요청은 "최신 성공" 기준으로 해결됩니다. "Latest-WINS" 평가 시기는 S3 클라이언트가 작업을 시작할 때가 아니라 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 합니다.

요청 헤더

"x-amz-storage-class" 요청 헤더가 지원되며 일치하는 ILM 규칙에서 이중 커밋 또는 밸런스의 수집 동작을 지정하는 경우 StorageGRID에서 생성되는 개체 복사본 수에 영향을 줍니다.

- '표준'입니다

  (기본값) ILM 규칙이 이중 커밋 옵션을 사용하거나 균형 옵션이 중간 복사본 생성으로 돌아올 때 이중 커밋 수집 작업을 지정합니다.

- Reduced_redundancy를 선택합니다

  ILM 규칙이 이중 커밋 옵션을 사용하거나 균형 옵션이 중간 복사본 생성으로 돌아올 때 단일 커밋 수집 작업을 지정합니다.

  > S3 오브젝트 잠금이 활성화된 버킷으로 오브젝트를 인스팅하는 경우 REDED_REPREADITORY' 옵션이 무시됩니다. 개체를 레거시 준수 버킷으로 인스팅하는 경우 REDED_REPREADITORIAL' 옵션은 오류를 반환합니다. StorageGRID은 규정 준수 요구 사항이 충족될 수 있도록 항상 이중 커밋 수집을 수행합니다.

> 15일 이내에 여러 부분 업로드가 완료되지 않으면 작업이 비활성으로 표시되고 모든 관련 데이터가 시스템에서 삭제됩니다.

> 반환된 "ETag" 값은 MD5 데이터 합계가 아니라 다중 파트 오브젝트에 대한 "ETag" 값의 Amazon S3 API 구현을 따릅니다.

버전 관리

이 작업은 여러 부분 업로드를 완료합니다. 버켓에 대해 버전 관리가 활성화된 경우 다중 파트 업로드가 완료되면 개체 버전이 생성됩니다.

버켓에 대한 버전 관리가 활성화된 경우 저장할 개체의 버전에 대해 고유한 rionId가 자동으로 생성됩니다. 이 인상파 ID는 X-amz-version-id 응답 헤더를 사용하여 응답에서도 반환됩니다.

버전 관리가 일시 중단된 경우 개체 버전은 null rionId로 저장되며, null 버전이 이미 있는 경우에는 덮어쓰게 됩니다.

> 버켓에 대해 버전 관리가 활성화된 경우, 같은 개체 키에서 동시 다중 파트 업로드가 완료된 경우에도 다중 파트 업로드를 완료하면 항상 새 버전이 생성됩니다. 버켓에 대해 버전 관리를 사용하지 않으면 다중 파트 업로드를 시작한 다음 다른 다중 파트 업로드를 시작하여 동일한 개체 키에서 먼저 완료할 수 있습니다. 비버전 버킷에서는 마지막으로 완료한 다중 파트 업로드가 우선 적용됩니다.

복제, 알림 또는 메타데이터 알림에 실패했습니다

플랫폼 서비스에 대해 다중 파트 업로드가 발생하는 버킷이 구성된 경우 연결된 복제 또는 알림 작업이 실패한 경우에도 다중 파트 업로드가 성공합니다.

이 경우 SMTT(Grid Manager on Total Events)에서 경보가 발생합니다. 마지막 이벤트 메시지는 알림이 실패한 마지막 객체에 대해 "버킷 이름 오브젝트 키에 대한 알림을 게시하지 못했습니다"라고 표시됩니다. (이 메시지를 보려면 * nodes * > **Storage Node* * > * Events * 를 선택합니다. 테이블 상단의 마지막 이벤트 보기) 이벤트 메시지는 '/var/local/log/bycast-err.log'에도 나열됩니다.

테넌트는 개체의 메타데이터 또는 태그를 업데이트하여 실패한 복제 또는 알림을 트리거할 수 있습니다. 테넌트는 불필요한 변경을 방지하기 위해 기존 값을 다시 제출할 수 있습니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

오류 응답

StorageGRID 시스템은 적용되는 모든 표준 S3 REST API 오류 응답을 지원합니다. 또한 StorageGRID 구현에는 여러 개의 사용자 지정 응답이 추가됩니다.

지원되는 **S3 API** 오류 코드입니다

이름	**HTTP** 상태입니다
액세스가 거부되었습니다	403 사용 금지
배다이제스트	400 잘못된 요청
BuckketAlreadyExists를 참조하십시오	409 충돌
BuckketNotEmpty	409 충돌
IncompleteBody	400 잘못된 요청
내부 오류입니다	500 내부 서버 오류입니다
InvalidAccessKeyId 입니다	403 사용 금지
InvalidArgument 를 선택합니다	400 잘못된 요청

이름	**HTTP** 상태입니다
InvalidBuckName입니다	400 잘못된 요청
InvalidBuckketState입니다	409 충돌
InvalidDigest 를 선택합니다	400 잘못된 요청
InvalidEncryptionAlgorithmError 가 발생합니다	400 잘못된 요청
InvalidPart 를 선택합니다	400 잘못된 요청
InvalidPartOrder를 선택합니다	400 잘못된 요청
InvalidRange 를 선택합니다	416 요청된 범위가 충분하지 않습니다
InvalidRequest 입니다	400 잘못된 요청
InvalidStorageClass 의 값을 반환합니다	400 잘못된 요청
InvalidTag 를 선택합니다	400 잘못된 요청
InvalidURI입니다	400 잘못된 요청
키투롱	400 잘못된 요청
MalformedXML을 참조하십시오	400 잘못된 요청
MetadataTooLarge를 참조하십시오	400 잘못된 요청
MethodNotAllowed 를 참조하십시오	405 메서드를 사용할 수 없습니다
MissingContentLength를 참조하십시오	411 길이 필요
MissingRequestBodyError가 발생합니다	400 잘못된 요청
MissingSecurityHeader 를 참조하십시오	400 잘못된 요청
NoSuchBucket	404를 찾을 수 없습니다
NoSuchKey를 클릭합니다	404를 찾을 수 없습니다
NoSuchUpload 를 클릭합니다	404를 찾을 수 없습니다

이름	**HTTP** 상태입니다
구현되지 않았습니다	501 구현되지 않음
NoSuchBuckketPolicy를 참조하십시오	404를 찾을 수 없습니다
ObjectLockConfigurationNotFoundError 가 발생합니다	404를 찾을 수 없습니다
사전 조건에 실패했습니다	412 전제 조건 실패
RequestTimeTooSkewed 를 참조하십시오	403 사용 금지
서비스를 사용할 수 없습니다	503 서비스를 사용할 수 없습니다
SignatureDoesNotMatch 를 참조하십시오	403 사용 금지
투만이버킷	400 잘못된 요청
UserKeyMustBeSpecified 를 선택합니다	400 잘못된 요청

StorageGRID 사용자 지정 오류 코드

이름	설명	**HTTP** 상태입니다
XBuckketLifecycleNotAllowed를 참조하십시오	버킷 수명 주기 구성은 레거시 준수 버킷에서 허용되지 않습니다	400 잘못된 요청
XBuckketPolicyParseException 을 참조하십시오	수신된 버킷 정책 JSON을 구문 분석하지 못했습니다.	400 잘못된 요청
XComplianceConflictt	레거시 준수 설정으로 인해 작업이 거부되었습니다.	403 사용 금지
XComplianceRedundancyForbidden을 선택합니다	레거시 준수 버킷에서는 감소된 중복성이 허용되지 않습니다	400 잘못된 요청
XMaxBuckketPolicyLengthExceeded 를 참조하십시오	정책이 허용되는 최대 버킷 정책 길이를 초과합니다.	400 잘못된 요청
XMissingInternalRequestHeader를 참조하십시오	내부 요청의 헤더가 누락되었습니다.	400 잘못된 요청
XNoSuchBuckketCompliance	지정된 버킷에 레거시 준법 기능이 설정되어 있지 않습니다.	404를 찾을 수 없습니다

이름	설명	HTTP 상태입니다
XNotAcceptable(X 허용 가능)	요청에 충족되지 않은 하나 이상의 수락 헤더가 있습니다.	406 허용되지 않습니다
XNotImplemented(XNotImplemented)	제공한 요청은 구현되지 않은 기능을 의미합니다.	501 구현되지 않음

StorageGRID S3 REST API 작업

StorageGRID 시스템별 S3 REST API에 작업이 추가됩니다.

- 버킷 정합성 보장 요청 가져오기

  Get Bucket 정합성 보장 요청을 사용하면 특정 버킷에 적용되는 정합성 보장 수준을 확인할 수 있습니다.

- 버킷 정합성 보장 요청을 배치합니다

  PUT 버킷 정합성 보장 요청을 사용하면 버킷에서 수행된 작업에 적용할 정합성 수준을 지정할 수 있습니다.

- 버킷 최종 액세스 시간 요청 가져오기

  [버킷 최종 액세스 시간 가져오기(Get Bucket Last Access Time) 요청 을 사용하면 개별 버킷에 대해 마지막 액세스 시간 업데이트가 활성화되거나 비활성화되었는지 확인할 수 있습니다.

- 버킷 최종 액세스 시간 요청

  Put Bucket Last Access Time 요청을 사용하면 개별 버킷에 대한 마지막 액세스 시간 업데이트를 활성화하거나 비활성화할 수 있습니다. 마지막 액세스 시간 업데이트를 비활성화하면 성능이 향상되고 버전 10.3.0 이상으로 생성된 모든 버킷의 기본 설정이 됩니다.

- 버킷 메타데이터 알림 구성 요청을 삭제합니다

  Delete Bucket 메타데이터 알림 구성 요청을 사용하면 구성 XML을 삭제하여 개별 버킷에 대한 검색 통합 서비스를 비활성화할 수 있습니다.

- 버킷 메타데이터 알림 구성 요청을 가져옵니다

  Get Bucket 메타데이터 알림 구성 요청을 사용하면 개별 버킷에 대한 검색 통합을 구성하는 데 사용되는 구성 XML을 검색할 수 있습니다.

- PUT 버킷 메타데이터 알림 구성 요청

  Put Bucket 메타데이터 알림 구성 요청을 사용하면 개별 버킷에 대한 검색 통합 서비스를 활성화할 수 있습니다. 요청 본문에 제공하는 메타데이터 알림 구성 XML은 대상 검색 인덱스에 메타데이터가 전송되는 개체를 지정합니다.

- 스토리지 사용 요청 가져오기

  Get Storage Usage 요청은 계정이 사용하는 총 스토리지 양과 계정과 연결된 각 버킷에 대해 알려줍니다.

- 레거시 규정 준수에 대한 더 이상 사용되지 않는 버킷 요청

StorageGRID S3 REST API를 사용하여 레거시 규정 준수 기능을 사용하여 생성된 버킷을 관리해야 할 수 있습니다.

버킷 정합성 보장 요청 가져오기

Get Bucket 정합성 보장 요청을 사용하면 특정 버킷에 적용되는 정합성 보장 수준을 확인할 수 있습니다.

기본 정합성 보장 컨트롤은 새로 생성된 객체에 대해 읽기/쓰기 작업을 보장하도록 설정됩니다.

이 작업을 완료하려면 S3:GetBucketConsistency 권한이 있거나 계정 루트가 됩니다.

요청 예

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

응답

응답 XML에서 "<Consistency>"는 다음 값 중 하나를 반환합니다.

일관성 제어	설명
모두	모든 노드가 데이터를 즉시 수신하거나 요청이 실패합니다.
강함 - 글로벌	모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 정합성을 보장합니다.
강력한 사이트	사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
읽기-후-새로-쓰기	(기본값) 새 객체에 대한 읽기 후 쓰기 정합성을 보장하고 객체 업데이트에 대한 최종 일관성을 제공합니다. 고가용성 및 데이터 보호 보장 제공 Amazon S3 일관성 보장과 가장 비슷합니다. • 참고: * 응용 프로그램이 존재하지 않는 개체에 대한 헤드 요청을 사용하는 경우 하나 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다. 이러한 오류를 방지하려면 Amazon S3와 유사한 일관성 보장이 필요하지 않는 한 일관성 제어를 ""사용 가능""으로 설정합니다.

일관성 제어	설명
사용 가능(헤드 작업의 최종 일관성)	"새 쓰기 후 다시 쓰기" 정합성 수준과 동일하게 동작하지만 헤드 작업에 대한 최종 정합성 보장만 제공합니다. 스토리지 노드를 사용할 수 없는 경우 "새 쓰기 후"보다 헤드 작업에 더 높은 가용성을 제공합니다. 헤드 작업에 대한 Amazon S3 정합성 보장과 다릅니다.

응답 예

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

관련 정보

일관성 제어

버킷 정합성 보장 요청을 배치합니다

PUT 버킷 정합성 보장 요청을 사용하면 버킷에서 수행된 작업에 적용할 정합성 수준을 지정할 수 있습니다.

기본 정합성 보장 컨트롤은 새로 생성된 객체에 대해 읽기/쓰기 작업을 보장하도록 설정됩니다.

이 작업을 완료하려면 S3:PutBucketConsistency 권한이 있거나 계정 루트가 됩니다.

요청하십시오

"x-ntap-sg-consistency" 매개 변수는 다음 값 중 하나를 포함해야 합니다.

일관성 제어	설명
모두	모든 노드가 데이터를 즉시 수신하거나 요청이 실패합니다.
강함 - 글로벌	모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 정합성을 보장합니다.

일관성 제어	설명
강력한 사이트	사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
읽기-후-새로-쓰기	(기본값) 새 객체에 대한 읽기 후 쓰기 정합성을 보장하고 객체 업데이트에 대한 최종 일관성을 제공합니다. 고가용성 및 데이터 보호 보장 제공 Amazon S3 일관성 보장과 가장 비슷합니다. • 참고: * 응용 프로그램이 존재하지 않는 개체에 대한 헤드 요청을 사용하는 경우 하나 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다. 이러한 오류를 방지하려면 Amazon S3와 유사한 일관성 보장이 필요하지 않는 한 일관성 제어를 ""사용 가능""으로 설정합니다.
사용 가능(헤드 작업의 최종 일관성)	"새 쓰기 후 다시 쓰기" 정합성 수준과 동일하게 동작하지만 헤드 작업에 대한 최종 정합성 보장만 제공합니다. 스토리지 노드를 사용할 수 없는 경우 "새 쓰기 후"보다 헤드 작업에 더 높은 가용성을 제공합니다. 헤드 작업에 대한 Amazon S3 정합성 보장과 다릅니다.

- 참고: * 일반적으로 "새 쓰기 후" 정합성 보장 제어 값을 사용해야 합니다. 요청이 올바르게 작동하지 않는 경우 가능한 경우 응용 프로그램 클라이언트 동작을 변경합니다. 또는 클라이언트가 각 API 요청에 대한 정합성 제어를 지정하도록 구성합니다. 버킷 레벨에서만 정합성 제어를 최후의 수단으로 설정하십시오.

요청 예

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

관련 정보

일관성 제어

버킷 최종 액세스 시간 요청 가져오기

[버킷 최종 액세스 시간 가져오기(Get Bucket Last Access Time) 요청 을 사용하면 개별 버킷에 대해 마지막 액세스 시간 업데이트가 활성화되거나 비활성화되었는지 확인할 수 있습니다.

이 작업을 완료하려면 S3:GetBucketLastAccessTime 권한이 있거나 계정 루트가 됩니다.

요청 예

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

응답 예

이 예에서는 버킷에 대해 마지막 액세스 시간 업데이트가 활성화되어 있음을 보여 줍니다.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

버킷 최종 액세스 시간 요청

Put Bucket Last Access Time 요청을 사용하면 개별 버킷에 대한 마지막 액세스 시간 업데이트를 활성화하거나 비활성화할 수 있습니다. 마지막 액세스 시간 업데이트를 비활성화하면 성능이 향상되고 버전 10.3.0 이상으로 생성된 모든 버킷의 기본 설정이 됩니다.

이 작업을 완료하려면 버킷에 대한 S3:PutBucketLastAccessTime 권한이 있거나 계정 루트가 됩니다.

> StorageGRID 버전 10.3부터는 모든 새 버킷에 대해 마지막 액세스 시간에 대한 업데이트가 기본적으로 비활성화됩니다. 이전 버전의 StorageGRID를 사용하여 만든 버킷이 있고 새 기본 동작과 일치시키려면 이전의 각 버킷에 대해 마지막 액세스 시간 업데이트를 명시적으로 비활성화해야 합니다. 테넌트 관리자의 Put Bucket Last Access Time 요청, * S3 * > * Bucket * > * Change Last Access Setting * 확인란 또는 테넌트 관리 API를 사용하여 마지막 액세스 시간에 대한 업데이트를 활성화하거나 비활성화할 수 있습니다.

버킷에 대해 마지막 액세스 시간 업데이트가 비활성화된 경우 버킷의 작업에 다음 동작이 적용됩니다.

- 객체 가져오기, 객체 ACL 가져오기, 객체 태그 지정 가져오기 및 헤드 객체 요청은 마지막 액세스 시간을 업데이트하지 않습니다. ILM(정보 수명 주기 관리) 평가를 위해 객체가 대기열에 추가되지 않습니다.
- Put Object - 메타데이터만 업데이트하는 객체 태그 지정 요청을 복사하고 배치하면 마지막 액세스 시간도 업데이트됩니다. ILM 평가를 위해 오브젝트가 대기열에 추가됩니다.
- 소스 버킷에 대해 마지막 액세스 시간에 대한 업데이트를 사용할 수 없는 경우 객체 복사 요청을 소스 버킷의 마지막 액세스 시간을 업데이트하지 않습니다. 복사된 객체는 소스 버킷에 대한 ILM 평가를 위해 대기열에 추가되지 않습니다. 그러나 대상의 경우, 개체 복사 요청은 항상 마지막 액세스 시간을 업데이트합니다. ILM 평가를 위해

개체의 복사본이 대기열에 추가됩니다.

- 완료 다중 파트 업로드 요청 마지막 액세스 시간 업데이트 완료된 객체가 ILM 평가를 위해 대기열에 추가됩니다.

예를 요청하십시오

이 예제에서는 버킷의 마지막 액세스 시간을 설정합니다.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

이 예제에서는 버킷의 마지막 액세스 시간을 비활성화합니다.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

관련 정보

테넌트 계정을 사용합니다

버킷 메타데이터 알림 구성 요청을 삭제합니다

Delete Bucket 메타데이터 알림 구성 요청을 사용하면 구성 XML을 삭제하여 개별 버킷에 대한 검색 통합 서비스를 비활성화할 수 있습니다.

이 작업을 완료하려면 버킷에 대한 S3:DeleteBucketMetadataNotification 권한 또는 계정 루트 권한이 있어야 합니다.

요청 예

이 예제에서는 버킷에 대한 검색 통합 서비스를 비활성화하는 방법을 보여 줍니다.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

버킷 메타데이터 알림 구성 요청을 가져옵니다

Get Bucket 메타데이터 알림 구성 요청을 사용하면 개별 버킷에 대한 검색 통합을 구성하는 데 사용되는 구성 XML을 검색할 수 있습니다.

이 작업을 완료하려면 S3:GetBuckMetadataNotification 권한 또는 계정 루트 권한이 있어야 합니다.

요청 예

이 요청은 bucket이라는 이름의 버킷에 대한 메타데이터 알림 구성을 검색합니다.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

응답

응답 본문에는 버킷에 대한 메타데이터 알림 구성이 포함됩니다. 메타데이터 알림 구성을 사용하면 버킷이 검색 통합을 위해 구성되는 방식을 결정할 수 있습니다. 즉, 인덱싱된 개체와 해당 개체 메타데이터가 전송되는 끝점을 확인할 수 있습니다.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

각 메타데이터 알림 구성에는 하나 이상의 규칙이 포함됩니다. 각 규칙은 적용되는 오브젝트와 StorageGRID가 오브젝트 메타데이터를 보내야 하는 대상을 지정합니다. 대상은 StorageGRID 끝점의 URN을 사용하여 지정해야 합니다.

이름	설명	필수 요소입니다
MetadataNotificationConfiguration을 참조하십시오	메타데이터 알림의 개체 및 대상을 지정하는 데 사용되는 규칙의 컨테이너 태그입니다. 하나 이상의 규칙 요소가 포함되어 있습니다.	예

이름	설명	필수 요소입니다
규칙	메타데이터를 지정된 인덱스에 추가해야 하는 개체를 식별하는 규칙의 컨테이너 태그입니다. 접두사가 겹치는 규칙은 거부됩니다. MetadataNotificationConfiguration 요소에 포함되어 있습니다.	예
ID입니다	규칙의 고유 식별자입니다. Rule 요소에 포함되어 있습니다.	아니요
상태	상태는 '활성화' 또는 '비활성화'가 될 수 있습니다. 비활성화된 규칙에 대해 어떠한 작업도 수행되지 않습니다. Rule 요소에 포함되어 있습니다.	예
접두어	접두사와 일치하는 개체는 규칙의 영향을 받으며 해당 메타데이터는 지정된 대상으로 전송됩니다. 모든 오브젝트를 일치시키려면 빈 접두사를 지정합니다. Rule 요소에 포함되어 있습니다.	예
목적지	규칙의 대상에 대한 컨테이너 태그입니다. Rule 요소에 포함되어 있습니다.	예

이름	설명	필수 요소입니다
urn	객체 메타데이터가 전송되는 대상의 urn입니다. 다음 속성을 가진 StorageGRID 끝점의 URN이어야 합니다. • 세 번째 요소는 'es'여야 합니다. • URN은 메타데이터가 저장된 인덱스 및 형식으로 domain-name/myindex/MyType 형식으로 끝나야 합니다. 엔드포인트는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성됩니다. 다음과 같은 형식을 취합니다. • 'arn:AWS:es:_region:account-ID_:domain/mydomain/myindex/MyType' • 'urn:mysite:es:::mydomain/myindex/MyType' 구성 XML을 제출하기 전에 끝점을 구성해야 합니다. 그렇지 않으면 404 오류로 인해 구성이 실패합니다. urn은 Destination 요소에 포함됩니다.	예

응답 예

"<MetadataNotificationConfiguration></MetadataNotificationConfiguration>" 태그 사이에 포함된 XML은 버킷에 대한 검색 통합 끝점과의 통합이 어떻게 구성되어 있는지 보여줍니다. 이 예에서 객체 메타데이터는 'Current'라는 Elasticsearch 인덱스로 전송되고 있으며 'rest코드'라는 AWS 도메인에서 호스팅되는 '2017'이라는 유형으로 전송됩니다.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

관련 정보

테넌트 계정을 사용합니다

PUT 버킷 메타데이터 알림 구성 요청

Put Bucket 메타데이터 알림 구성 요청을 사용하면 개별 버킷에 대한 검색 통합 서비스를 활성화할 수 있습니다. 요청 본문에 제공하는 메타데이터 알림 구성 XML은 대상 검색 인덱스에 메타데이터가 전송되는 개체를 지정합니다.

이 작업을 완료하려면 버킷에 대한 PutBucketMetadataNotification 권한 또는 계정 루트 권한이 있어야 합니다.

요청하십시오

요청 본문에는 메타데이터 알림 구성이 포함되어야 합니다. 각 메타데이터 알림 구성에는 하나 이상의 규칙이 포함됩니다. 각 규칙은 적용되는 오브젝트와 StorageGRID가 오브젝트 메타데이터를 보내야 하는 대상을 지정합니다.

개체 이름의 접두어를 기준으로 개체를 필터링할 수 있습니다. 예를 들어, 접두어 '/images'가 있는 객체의 메타데이터를 한 대상에 전송하고 접두어 '/videos'가 있는 객체를 다른 대상으로 전송할 수 있습니다.

중복되는 접두사가 있는 구성은 유효하지 않으며 제출될 때 거부됩니다. 예를 들어 접두사 test를 가진 개체에 대해 하나의 규칙을 포함하고 test2 접두사가 있는 개체에 대해 두 번째 규칙을 포함하는 구성은 허용되지 않습니다.

대상은 StorageGRID 끝점의 URN을 사용하여 지정해야 합니다. 메타데이터 알림 설정이 제출되거나 요청이 '400 Bad Request'로 실패하는 경우 단말 장치가 존재해야 한다. "메타데이터 알림(검색) 정책을 저장할 수 없습니다. 지정한 끝점 URN이 없습니다:_URN_.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

이 표에서는 메타데이터 알림 구성 XML의 요소에 대해 설명합니다.

이름	설명	필수 요소입니다
MetadataNotificationConfiguration을 참조하십시오	메타데이터 알림의 개체 및 대상을 지정하는 데 사용되는 규칙의 컨테이너 태그입니다. 하나 이상의 규칙 요소가 포함되어 있습니다.	예
규칙	메타데이터를 지정된 인덱스에 추가해야 하는 개체를 식별하는 규칙의 컨테이너 태그입니다. 접두사가 겹치는 규칙은 거부됩니다. MetadataNotificationConfiguration 요소에 포함되어 있습니다.	예
ID입니다	규칙의 고유 식별자입니다. Rule 요소에 포함되어 있습니다.	아니요
상태	상태는 '활성화' 또는 '비활성화'가 될 수 있습니다. 비활성화된 규칙에 대해 어떠한 작업도 수행되지 않습니다. Rule 요소에 포함되어 있습니다.	예

이름	설명	필수 요소입니다
접두어	접두사와 일치하는 개체는 규칙의 영향을 받으며 해당 메타데이터는 지정된 대상으로 전송됩니다. 모든 오브젝트를 일치시키려면 빈 접두사를 지정합니다. Rule 요소에 포함되어 있습니다.	예
목적지	규칙의 대상에 대한 컨테이너 태그입니다. Rule 요소에 포함되어 있습니다.	예
urn	객체 메타데이터가 전송되는 대상의 urn입니다. 다음 속성을 가진 StorageGRID 끝점의 URN이어야 합니다. • 세 번째 요소는 'es'여야 합니다. • URN은 메타데이터가 저장된 인덱스 및 형식으로 domain-name/myindex/MyType 형식으로 끝나야 합니다. 엔드포인트는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성됩니다. 다음과 같은 형식을 취합니다. • "arn:aws:region:account-ID:domain/mydomain/myindex/MyType" • 'urn:mysite:es:::mydomain/myindex/MyType' 구성 XML을 제출하기 전에 끝점을 구성해야 합니다. 그렇지 않으면 404 오류로 인해 구성이 실패합니다. urn은 Destination 요소에 포함됩니다.	예

예를 요청하십시오

이 예제에서는 버킷에 대한 검색 통합을 활성화하는 방법을 보여 줍니다. 이 예제에서 모든 오브젝트의 오브젝트 메타데이터는 동일한 대상으로 전송됩니다.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

이 예에서는 접두사 /images와 일치하는 객체의 객체 메타데이터가 한 대상으로 전송되고 접두사 /videos와 일치하는 객체의 객체 메타데이터는 두 번째 대상으로 전송됩니다.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

JSON이 검색 통합 서비스에 의해 생성되었습니다

버킷에 대한 검색 통합 서비스를 활성화하면 개체 메타데이터 또는 태그를 추가, 업데이트 또는 삭제할 때마다 JSON 문서가 생성되어 대상 끝점으로 전송됩니다.

이 예에서는 'test'라는 버킷에 'gws/tagging.txt' 키가 있는 객체가 생성될 때 생성될 수 있는 JSON의 예를 보여 줍니다. 시험용 버킷은 버전 관리가 되지 않아 rionId 태그가 비어 있습니다.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

메타데이터 알림에 포함된 개체 메타데이터입니다

이 표에는 검색 통합이 활성화된 경우 대상 끝점으로 전송되는 JSON 문서에 포함된 모든 필드가 나열됩니다.

문서 이름에는 버킷 이름, 오브젝트 이름 및 버전 ID(있는 경우)가 포함됩니다.

유형	항목 이름	설명
버킷 및 오브젝트 정보	버킷	버킷의 이름입니다
버킷 및 오브젝트 정보	키	개체 키 이름입니다
버킷 및 오브젝트 정보	버전 ID	오브젝트 버전, 버전 버킷 내 오브젝트
버킷 및 오브젝트 정보	지역	우동동-1 등 버킷 지역
시스템 메타데이터	크기	HTTP 클라이언트에 표시되는 개체 크기(바이트)입니다
시스템 메타데이터	MD5	개체 해시

유형	항목 이름	설명
사용자 메타데이터	메타데이터 '*key:value*'	객체에 대한 모든 사용자 메타데이터를 키 값 쌍으로 사용합니다
태그	태그 `*key:value*'	개체에 대해 정의된 모든 개체 태그를 키 값 쌍으로 사용합니다

- 참고: * 태그 및 사용자 메타데이터의 경우 StorageGRID는 날짜 및 숫자를 Elasticsearch에 문자열로 전달하거나 S3 이벤트 알림으로 전달합니다. 이러한 문자열을 날짜 또는 숫자로 해석하도록 Elasticsearch를 구성하려면 동적 필드 매핑 및 날짜 형식 매핑에 대한 Elasticsearch 지침을 따르십시오. 검색 통합 서비스를 구성하기 전에 인덱스에서 동적 필드 매핑을 활성화해야 합니다. 문서가 인덱싱된 후에는 인덱스에서 문서의 필드 형식을 편집할 수 없습니다.

관련 정보

테넌트 계정을 사용합니다

스토리지 사용 요청 가져오기

Get Storage Usage 요청은 계정이 사용하는 총 스토리지 양과 계정과 연결된 각 버킷에 대해 알려줍니다.

어카운트 및 해당 버킷에 사용되는 스토리지의 양은 'x-ntap-sg-usage' 쿼리 매개 변수를 사용하는 수정된 Get Service 요청을 통해 얻을 수 있습니다. 시스템에서 처리하는 PUT 및 삭제 요청과는 별도로 버킷 스토리지 사용량을 추적합니다. 특히 시스템이 과부하 상태인 경우, 사용 값이 요청 처리를 기준으로 예상 값과 일치하기 전에 약간의 지연이 있을 수 있습니다.

기본적으로 StorageGRID는 강력한 글로벌 일관성을 사용하여 사용 정보 검색을 시도합니다. 강력한 글로벌 일관성을 달성할 수 없는 경우 StorageGRID는 강력한 사이트 일관성으로 사용 정보를 검색합니다.

이 작업을 완료하려면 S3:ListAllMyBucket 권한이 있거나 계정 루트 권한이 있어야 합니다.

요청 예

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

응답 예

이 예에서는 두 버킷에 4개의 오브젝트와 12바이트의 데이터가 있는 계정을 보여 줍니다. 각 버킷에는 2개의 오브젝트와 6바이트의 데이터가 포함되어 있습니다.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

버전 관리

저장된 모든 개체 버전은 응답에서 ObjectCount 및 DataBytes 값에 기여합니다. 삭제 표식이 ObjectCount 합계에 추가되지 않습니다.

관련 정보

일관성 제어

레거시 규정 준수를 위한 더 이상 사용되지 않는 버킷 요청

StorageGRID S3 REST API를 사용하여 레거시 규정 준수 기능을 사용하여 생성된 버킷을 관리해야 할 수 있습니다.

규정 준수 기능이 사용되지 않습니다

이전 StorageGRID 버전에서 사용할 수 있었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 오브젝트 잠금으로 대체되었습니다.

이전에 글로벌 규정 준수 설정을 활성화한 경우 StorageGRID 11.6에서 전역 S3 개체 잠금 설정이 활성화됩니다. Compliance를 사용하도록 설정한 상태에서 새 버킷을 더 이상 생성할 수 없지만, 필요에 따라 StorageGRID S3 REST

API를 사용하여 기존의 규정을 준수하는 버킷을 관리할 수 있습니다.

- S3 오브젝트 잠금을 사용합니다
- ILM을 사용하여 개체를 관리합니다
- "NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

더 이상 사용되지 않는 규정 준수 요청:

- 폐기됨 - 규정 준수를 위해 버킷 요청을 수정합니다

  SGCompliance XML 요소는 사용되지 않습니다. 이전 버전에서는 이 StorageGRID 사용자 정의 요소를 PUT 버킷 요청의 선택적 XML 요청 본문에 포함하여 준수 버킷을 생성할 수 있었습니다.

- 사용되지 않음 - 버킷 준수 요청 가져오기

  Get Bucket 준수 요청은 더 이상 사용되지 않습니다. 그러나 이 요청을 계속 사용하여 기존 레거시 준수 버킷에 현재 적용되는 준수 설정을 확인할 수 있습니다.

- 폐기됨 - 버킷 준수 요청을 넣으십시오

  PUT 버킷 준수 요청은 더 이상 사용되지 않습니다. 그러나 이 요청을 계속 사용하여 기존 레거시 준수 버킷의 준수 설정을 수정할 수 있습니다. 예를 들어, 기존 버킷을 법적 보존 상태로 놓거나 보존 기간을 늘릴 수 있습니다.

사용되지 않음: 규정 준수를 위해 버킷 요청 수정을 배치합니다

SGCompliance XML 요소는 사용되지 않습니다. 이전 버전에서는 이 StorageGRID 사용자 정의 요소를 PUT 버킷 요청의 선택적 XML 요청 본문에 포함하여 준수 버킷을 생성할 수 있었습니다.

> 이전 StorageGRID 버전에서 사용할 수 있었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 오브젝트 잠금으로 대체되었습니다.

S3 오브젝트 잠금을 사용합니다

ILM을 사용하여 개체를 관리합니다

"NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

Compliance가 설정된 새 버킷을 더 이상 생성할 수 없습니다. 새 준수 버킷을 생성하기 위해 준수 준수를 위해 Put Bucket 요청 수정을 사용하려는 경우 다음 오류 메시지가 반환됩니다.

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

관련 정보

ILM을 사용하여 개체를 관리합니다

테넌트 계정을 사용합니다

사용되지 않음: 버킷 준수 요청 가져오기

Get Bucket 준수 요청은 더 이상 사용되지 않습니다. 그러나 이 요청을 계속 사용하여 기존 레거시 준수 버킷에 현재 적용되는 준수 설정을 확인할 수 있습니다.

> 이전 StorageGRID 버전에서 사용할 수 있었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 오브젝트 잠금으로 대체되었습니다.

S3 오브젝트 잠금을 사용합니다

ILM을 사용하여 개체를 관리합니다

"NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

이 작업을 완료하려면 S3:GetBucketCompliance 권한이 있거나 계정 루트가 됩니다.

요청 예

이 예제 요청을 사용하여 'mybucket'이라는 이름의 버킷에 대한 준수 설정을 확인할 수 있습니다.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

응답 예

응답 XML에서 "<SGCompliance>"는 버킷에 적용되는 준수 설정을 나열합니다. 이 예제 응답에서는 오브젝트를 그리드에 인제스트하는 시점을 시작으로 각 오브젝트를 1년(525,600분)동안 보존할 버킷의 규정 준수 설정을 보여줍니다. 현재 이 버킷에 대한 법적 보류가 없습니다. 각 개체는 1년 후에 자동으로 삭제됩니다.

```
HTTP/1.1 200 OK
Date: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

이름	설명
RetenionPeriodMinutes(주기적 지연 시간)	이 버킷에 추가된 객체의 보존 기간(분)입니다. 보존 기간은 객체가 그리드에 수집될 때 시작됩니다.
LegalHold	• 참: 이 버킷은 현재 법적 증거 자료 보관 중입니다. 이 버킷의 오브젝트는 보존 기간이 만료된 경우에도 법적 보류가 해제될 때까지 삭제할 수 없습니다. • 거짓: 이 버킷은 현재 법적 증거 자료 보관 중이 아닙니다. 이 버킷의 오브젝트는 보존 기간이 만료되면 삭제할 수 있습니다.
자동 삭제	• 참: 버킷이 법적 보존 상태에 있지 않는 한, 보존 기간이 만료되면 이 버킷의 객체가 자동으로 삭제됩니다. • False: 보존 기간이 만료되면 이 버킷의 객체가 자동으로 삭제되지 않습니다. 이러한 개체를 삭제하려면 해당 개체를 수동으로 삭제해야 합니다.

오류 응답

버킷을 규정에 맞게 만들지 않은 경우 응답에 대한 HTTP 상태 코드는 XNoSuchBuckketCompliance의 S3 오류 코드와 함께 404를 찾을 수 없습니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

테넌트 계정을 사용합니다

폐기됨: 버킷 준수 요청을 넣으십시오

PUT 버킷 준수 요청은 더 이상 사용되지 않습니다. 그러나 이 요청을 계속 사용하여 기존 레거시 준수 버킷의 준수 설정을 수정할 수 있습니다. 예를 들어, 기존 버킷을 법적 보존 상태로 놓거나 보존 기간을 늘릴 수 있습니다.

> 이전 StorageGRID 버전에서 사용할 수 있었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 오브젝트 잠금으로 대체되었습니다.

S3 오브젝트 잠금을 사용합니다

ILM을 사용하여 개체를 관리합니다

"NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

이 작업을 완료하려면 S3:PutBucketCompliance 권한 또는 계정 루트 권한이 있어야 합니다.

PUT 버킷 준수 요청을 발행할 때 준수 설정의 모든 필드에 값을 지정해야 합니다.

요청 예

이 예제 요청은 'mybucket'이라는 이름의 버킷에 대한 준수 설정을 수정합니다. 이 예에서는 객체가 그리드에 인제된 후 1년이 아닌 2년(1,051,200분) 동안 mybucket의 객체가 보존됩니다. 이 버킷에는 법적 구속이 없습니다. 각 개체는 2년 후에 자동으로 삭제됩니다.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

이름	설명
RetenionPeriodMinutes(주기적 지연 시간)	이 버킷에 추가된 객체의 보존 기간(분)입니다. 보존 기간은 객체가 그리드에 수집될 때 시작됩니다. • 주의: * RetenitionPeriodMinutes에 새 값을 지정할 때는 버킷의 현재 보존 기간과 같거나 큰 값을 지정해야 합니다. 버킷의 보존 기간이 설정된 후에는 해당 값을 줄일 수 없으며 증가만 가능합니다.
LegalHold	• 참: 이 버킷은 현재 법적 증거 자료 보관 중입니다. 이 버킷의 오브젝트는 보존 기간이 만료된 경우에도 법적 보류가 해제될 때까지 삭제할 수 없습니다. • 거짓: 이 버킷은 현재 법적 증거 자료 보관 중이 아닙니다. 이 버킷의 오브젝트는 보존 기간이 만료되면 삭제할 수 있습니다.
자동 삭제	• 참: 버킷이 법적 보존 상태에 있지 않는 한, 보존 기간이 만료되면 이 버킷의 객체가 자동으로 삭제됩니다. • False: 보존 기간이 만료되면 이 버킷의 객체가 자동으로 삭제되지 않습니다. 이러한 개체를 삭제하려면 해당 개체를 수동으로 삭제해야 합니다.

규정 준수 설정을 위한 정합성 보장 레벨

PUT 버킷 준수 요청으로 S3 버킷의 준수 설정을 업데이트하면 StorageGRID는 그리드 전체에서 버킷의 메타데이터를 업데이트하려고 시도합니다. 기본적으로 StorageGRID는 * strong-global * 일관성 수준을 사용하여 버킷 메타데이터를 포함하는 모든 데이터 센터 사이트와 모든 스토리지 노드가 변경된 규정 준수 설정에 대해 읽기-쓰기 후 일관성을

유지하도록 보장합니다.

데이터 센터 사이트 또는 사이트의 여러 스토리지 노드를 사용할 수 없어 StorageGRID가 * 강력한 글로벌 * 정합성 수준을 달성할 수 없는 경우 응답에 대한 HTTP 상태 코드는 503 서비스를 사용할 수 없습니다

이 응답을 받으면 그리드 관리자에게 문의하여 필요한 스토리지 서비스를 가능한 빨리 사용할 수 있도록 해야 합니다. 그리드 관리자가 각 사이트에서 충분한 스토리지 노드를 사용할 수 없는 경우, 기술 지원 부서에서 * strong-site * 정합성 보장 수준을 강제로 진행하여 실패한 요청을 다시 시도하도록 할 수 있습니다.

> 기술 지원 부서의 지시가 있는 경우를 제외하고, 이 레벨을 사용할 경우 발생할 수 있는 결과를 이해하지 않는 한 * 강력한 사이트 * 일관성 수준을 강제로 버킷 규정 준수를 강제하지 마십시오.

정합성 보장 수준을 * strong-site * 로 축소하면 StorageGRID는 업데이트된 규정 준수 설정이 사이트 내의 클라이언트 요청에 대해서만 읽기/쓰기 후 일관성을 갖게 됩니다. 즉, 모든 사이트 및 스토리지 노드를 사용할 수 있을 때까지 StorageGRID 시스템에 이 버킷에 대한 여러 개의 일관되지 않은 설정이 일시적으로 있을 수 있습니다. 설정이 일치하지 않으면 예기치 않거나 원치 않는 동작이 발생할 수 있습니다. 예를 들어, 버킷을 법적 증거 자료 보관 아래에 놓고 정합성 보장 수준을 낮추면 버킷의 이전 규정 준수 설정(즉, 법적 증거 자료 보관)이 일부 데이터 센터 사이트에서 계속 적용될 수 있습니다. 따라서 보존 기간이 만료되면 사용자나 자동 삭제(활성화된 경우)에 의해 법적 보류라고 생각하는 개체가 삭제될 수 있습니다.

strong-site * 정합성 보장 수준을 강제로 사용하려면 PUT Bucket 준수 요청을 다시 발행하고 다음과 같이 "Consistency-Control" HTTP 요청 헤더를 포함시킵니다.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

오류 응답

- 버킷이 규정을 준수하도록 생성되지 않은 경우 응답에 대한 HTTP 상태 코드는 404를 찾을 수 없습니다.
- 요청의 RetenitionPeriodMinutes가 버킷의 현재 보존 기간보다 짧으면 HTTP 상태 코드는 400개의 잘못된 요청입니다.

관련 정보

사용되지 않음: 규정 준수를 위해 버킷 요청 수정을 배치합니다

테넌트 계정을 사용합니다

ILM을 사용하여 개체를 관리합니다

버킷 및 그룹 액세스 정책

StorageGRID은 AWS(Amazon Web Services) 정책 언어를 사용하여 S3 테넌트가 해당 버킷 및 오브젝트 내의 버킷에 대한 액세스를 제어할 수 있도록 합니다. StorageGRID 시스템은 S3 REST API 정책 언어의 하위 집합을 구현합니다. S3 API에 대한 액세스 정책은 JSON으로 기록됩니다.

액세스 정책 개요

StorageGRID에서 지원하는 액세스 정책에는 두 가지 유형이 있습니다.

- * 버킷 정책 * - 버킷 정책 가져오기, 버킷 정책 적용 및 버킷 정책 삭제 S3 API 작업을 사용하여 구성됩니다. 버킷 정책은 버킷에 첨부되므로 버킷 소유자 계정 또는 버킷에 대한 다른 계정 및 버킷에 있는 오브젝트에 대한 사용자의 액세스를 제어하도록 구성됩니다. 버킷 정책은 하나의 버킷과 여러 그룹에만 적용됩니다.
- 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성된 * 그룹 정책 * 입니다. 그룹 정책은 계정의 그룹에 연결되므로 해당 그룹이 해당 계정이 소유한 특정 리소스에 액세스할 수 있도록 구성됩니다. 그룹 정책은 하나의 그룹에만 적용되고 여러 버킷에 적용될 수 있습니다.

StorageGRID 버킷 및 그룹 정책은 아마존에서 정의한 특정 문법을 따릅니다. 각 정책 안에는 정책 문의 배열이 들어 있으며 각 문에는 다음 요소가 포함되어 있습니다.

- 정책 ID(SID)(선택 사항)
- 효과
- Principal/NotPrincipal입니다
- 리소스/NotResource입니다
- 작업/NotAction
- 조건(선택 사항)

정책 문은 이 구조를 사용하여 권한을 지정합니다. pert <effect> <principal>이(가) <condition>이(가) 적용될 때 <Resource>에서 <Action>을(를) 수행하도록 허용/거부합니다.

각 정책 요소는 특정 함수에 사용됩니다.

요소	설명
SID	SID 요소는 선택 사항입니다. SID는 사용자에 대한 설명으로만 제공됩니다. StorageGRID 시스템에서 저장하지만 해석되지 않습니다.
효과	Effect 요소를 사용하여 지정된 작업의 허용 여부를 설정합니다. 지원되는 작업 요소 키워드를 사용하여 버킷 또는 오브젝트에 대해 허용(또는 거부)하는 작업을 식별해야 합니다.
Principal/NotPrincipal입니다	사용자, 그룹 및 계정이 특정 리소스에 액세스하고 특정 작업을 수행하도록 허용할 수 있습니다. 요청에 S3 서명이 포함되지 않은 경우 와일드카드 문자(*)를 보안 주체에 지정하여 익명 액세스가 허용됩니다. 기본적으로 계정 루트만 해당 계정이 소유한 리소스에 액세스할 수 있습니다. 버킷 정책에서 Principal 요소만 지정하면 됩니다. 그룹 정책의 경우 정책이 연결된 그룹이 암시적 Principal 요소입니다.
리소스/NotResource입니다	Resource 요소는 버킷 및 오브젝트를 식별합니다. ARN(Amazon Resource Name)을 사용하여 리소스를 식별하는 버킷 및 객체에 대한 권한을 허용하거나 거부할 수 있습니다.

요소	설명
작업/NotAction	Action 및 Effect 요소는 권한의 두 구성 요소입니다. 그룹이 리소스를 요청하면 리소스에 대한 액세스가 부여되거나 거부됩니다. 명시적으로 권한을 할당하지 않는 한 액세스가 거부되지만 명시적 DENY를 사용하여 다른 정책이 부여한 권한을 재정의할 수 있습니다.
조건	Condition 요소는 선택 요소입니다. 조건을 사용하면 식을 만들어 정책을 적용해야 하는 시기를 결정할 수 있습니다.

Action 요소에서 와일드카드 문자(*)를 사용하여 모든 작업이나 작업의 하위 집합을 지정할 수 있습니다. 예를 들어 이 작업은 S3:GetObject , S3:PutObject 및 S3:DeleteObject 와 같은 사용 권한을 일치시킵니다.

```
s3:*Object
```

Resource 요소에서 와일드카드 문자(\ **)** 및 **(?)**를 사용할 수 있습니다**.** 별표**(**)가 0개 이상의 문자와 일치하면 물음표 (?)가 모든 단일 문자와 일치합니다.

Principal 요소에서 모든 사용자에게 권한을 부여하는 익명 액세스를 설정하는 경우를 제외하고 와일드카드 문자는 지원되지 않습니다. 예를 들어 와일드카드(*)를 Principal 값으로 설정합니다.

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

다음 예제에서는 Effect , Principal , Action 및 Resource 요소를 사용합니다. 이 예제는 "Allow" 효과를 사용하여 Principals, 관리 그룹 "federated-group/admin" 및 재무 그룹 "federated-group/finance"에 mbucket이라는 버킷에 대해 Action'3:ListBucket"을 수행할 수 있는 권한 및 해당 버킷 내의 모든 개체에 대해 Action'3:GetObject'를 제공하는 전체 버킷 정책 설명을 보여줍니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

버킷 정책은 크기 제한이 20,480바이트이고 그룹 정책은 크기 제한이 5,120바이트입니다.

관련 정보

테넌트 계정을 사용합니다

정책에 대한 정합성 보장 제어 설정입니다

기본적으로 그룹 정책에 대한 모든 업데이트는 최종적으로 일치합니다. 그룹 정책이 일관되면 정책 캐싱 때문에 변경 내용이 적용되는 데 15분 정도 더 걸릴 수 있습니다. 기본적으로 버킷 정책에 대한 모든 업데이트도 최종적으로 일치합니다.

필요에 따라 버킷 정책 업데이트의 일관성 보장을 변경할 수 있습니다. 예를 들어, 보안상의 이유로 버킷 정책을 최대한 빨리 변경할 수 있습니다.

이 경우 Put Bucket 정책 요청에서 정합성 보장 제어 헤더를 설정하거나 Put Bucket 정합성 보장 요청을 사용할 수 있습니다. 이 요청에 대한 정합성 제어를 변경할 때는 읽기 후 쓰기 정합성을 보장하는 * All * 값을 사용해야 합니다. Put Bucket 정합성 보장 요청의 헤더에 다른 정합성 보장 제어 값을 지정하면 요청이 거부됩니다. Put Bucket 정책 요청에 대해 다른 값을 지정하면 값이 무시됩니다. 버킷 정책이 일관되면 정책 캐싱으로 인해 변경 사항이 적용되는 데 8초가 더 걸릴 수 있습니다.

> 정합성 수준을 * All * 로 설정하면 새 버킷 정책이 더 빨리 발효되도록 하려면 작업이 완료되면 버킷 수준 제어를 원래 값으로 다시 설정해야 합니다. 그렇지 않으면 이후의 모든 버킷 요청은 * All * 설정을 사용합니다.

정책 설명에 **ARN**을 사용합니다

정책 문에서 ARN은 Principal 및 Resource 요소에서 사용됩니다.

- 이 구문을 사용하여 S3 리소스 ARN을 지정합니다.

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- 이 구문을 사용하여 ID 리소스 ARN(사용자 및 그룹)을 지정합니다.

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

기타 고려 사항:

- 별표(*)를 와일드카드로 사용하여 개체 키 안에 0개 이상의 문자를 일치시킬 수 있습니다.
- 개체 키에 지정할 수 있는 국제 문자는 JSON UTF-8 또는 JSON\u 이스케이프 시퀀스를 사용하여 인코딩해야 합니다. 퍼센트 인코딩은 지원되지 않습니다.

  "RFC 2141 URN 구문"

  Put Bucket 정책 작업의 HTTP 요청 본문은 charset=UTF-8로 인코딩되어야 합니다.

정책에서 리소스를 지정합니다

정책 문에서 Resource 요소를 사용하여 사용 권한이 허용되거나 거부되는 버킷 또는 개체를 지정할 수 있습니다.

- 각 정책 문에는 Resource 요소가 필요합니다. 정책에서 리소스는 '리소스' 또는 'NotResource'(제외)로 표시됩니다.
- S3 리소스 ARN을 사용하여 리소스를 지정합니다. 예를 들면 다음과 같습니다.

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- 개체 키 내에서 정책 변수를 사용할 수도 있습니다. 예를 들면 다음과 같습니다.

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- 리소스 값은 그룹 정책이 생성될 때 아직 존재하지 않는 버킷을 지정할 수 있습니다.

관련 정보

정책에 변수를 지정합니다

정책에 보안 주체를 지정합니다

Principal 요소를 사용하여 policy 문에 의해 리소스에 대한 액세스가 허용/거부된 사용자, 그룹 또는 테넌트 계정을 식별합니다.

- 버킷 정책의 각 정책 선언에는 Principal 요소가 포함되어야 합니다. 그룹 정책의 정책 설명은 그룹이 보안 주체로 인식되기 때문에 Principal 요소가 필요하지 않습니다.
- 정책에서 교장은 제외에 대해 "Principal" 또는 "NotPrincipal" 요소로 표시됩니다.
- 계정 기반 ID는 ID 또는 ARN을 사용하여 지정해야 합니다.

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- 이 예에서는 계정 루트 및 계정의 모든 사용자를 포함하는 테넌트 계정 ID 27233906934684427525를 사용합니다.

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

- 계정 루트만 지정할 수 있습니다.

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 특정 페더레이션 사용자("Alex")를 지정할 수 있습니다.

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

- 특정 통합 그룹("관리자")을 지정할 수 있습니다.

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

- 익명 보안 주체를 지정할 수 있습니다.

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

- 모호함을 방지하려면 사용자 이름 대신 사용자 UUID를 사용할 수 있습니다.

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

예를 들어, 알렉스가 퇴사하고 사용자 이름 알렉스가 삭제되었다고 가정해 봅시다. 새 알렉스가 조직에 가입하여 동일한 '알렉스' 사용자 이름을 할당하면 새 사용자는 원래 사용자에게 부여된 권한을 의도치 않게 상속할 수 있습니다.

- Principal 값은 버킷 정책이 생성될 때 아직 존재하지 않는 그룹/사용자 이름을 지정할 수 있습니다.

정책에서 사용 권한을 지정합니다

정책에서 Action 요소는 리소스에 대한 권한을 허용/거부하는 데 사용됩니다. 정책에서 지정할 수 있는 사용 권한 집합이 있으며, 이러한 권한은 "작업" 또는 "NotAction" 요소로 표시됩니다. 각 요소는 특정 S3 REST API 작업에 매핑됩니다.

이 표에는 버킷에 적용되는 사용 권한과 객체에 적용되는 사용 권한이 나열되어 있습니다.

Amazon S3는 이제 PUT 및 DELETE Bucket 복제 작업 모두에 S3:PutReplicationConfiguration 권한을 사용합니다. StorageGRID는 원래 Amazon S3 사양과 일치하는 각 작업에 대해 별도의 권한을 사용합니다.

기존 값을 덮어쓰는 데 PUT를 사용할 때 삭제가 수행됩니다.

버킷에 적용되는 권한

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:생성 버킷	버킷 을 놓습니다	
S3:삭제 버킷	버킷 삭제	
S3:DeleteBucketMetadataNotification	버킷 메타데이터 알림 구성을 삭제합니다	예
S3:삭제 BucketPolicy	버킷 정책을 삭제합니다	
S3:DeleteReplicationConfiguration	버킷 복제를 삭제합니다	예, PUT 및 DELETE에 대한 별도의 권한 *
S3:GetBuckketAcl	버킷 ACL 가져오기	
S3:GetBucketCompliance	버킷 규정 준수 가져오기(더 이상 사용되지 않음)	예
S3:GetBuckketConsistency	버킷 일관성 확보	예

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:GetBuckketCORS	버킷 CORS를 가져옵니다	
S3:GetEncryptionConfiguration	버킷 암호화 가져오기	
S3:GetBucketLastAccessTime	버킷 최종 액세스 시간 가져오기	예
S3:GetBucketLocation	버킷 위치를 가져옵니다	
S3:GetBuckMetadataNotification 을 참조하십시오	Bucket 메타데이터 알림 구성 가져오기	예
S3:GetBucketNotification 을 참조하십시오	버킷 알림을 받습니다	
S3:GetBuckketObjectLockConfiguration	개체 잠금 구성을 가져옵니다	
S3:GetBuckketPolicy를 참조하십시오	버킷 정책 가져오기	
S3:GetBucketTagging	버킷 태그 지정을 가져옵니다	
S3:GetBucketVersioning	버킷 버전 관리 가져오기	
S3:GetLifecycleConfiguration	버킷 수명 주기 가져오기	
S3:GetReplicationConfiguration	버킷 복제를 가져옵니다	
S3:ListAllMyBucket	• 서비스 받기 • 스토리지 사용량을 가져옵니다	예, 스토리지 사용량 가져오에 대해 가능합니다
S3:목록 버킷	• 버킷 가져오기(객체 나열) • 헤드 버킷 • 사후 개체 복원	
S3:ListBuckketMultipartUploads	• 다중 파트 업로드 나열 • 사후 개체 복원	
S3:목록 BuckketVersions	버킷 버전 가져오기	
S3: PutBucketCompliance	버킷 규정 준수(폐기됨)	예

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3: PutBucketConsistency	버킷 일관성을 유지합니다	예
S3: PutBucketCORS	• 버킷 CORS† 삭제 • 버킷 CORS를 넣습니다	
S3:PutEncryptionConfiguration	• Bucket 암호화를 삭제합니다 • Bucket 암호화를 적용합니다	
S3:PutBucketLastAccessTime	버킷 최종 접근 시간	예
S3:PutBucketMetadataNotification	Put Bucket 메타데이터 알림 구성	예
S3: PutBucketNotification	버킷 통지를 보냅니다	
S3:PutBucketObjectLockConfiguration	• "x-amz-bucket-object-lock-enabled: true" 요청 헤더가 있는 Bucket을 배치합니다(또한 S3:CreateBucket 권한이 필요함). • 개체 잠금 구성을 배치합니다	
S3: PutBucketPolicy	버킷 정책을 적용합니다	
S3: PutBucketTagging	• 버킷 태그 표시 삭제† • Bucket 태그 달기	
S3: PutBucketVersioning	버킷 버전 관리	
S3: PutLifecycleConfiguration	• 버킷 수명 주기 삭제† • 버킷 수명 주기를 놓습니다	
S3:PutReplicationConfiguration	버킷 복제를 배치합니다	예, PUT 및 DELETE에 대한 별도의 권한 *

객체에 적용되는 권한

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:중단멀티업로드입니다	• 멀티파트 업로드를 중단합니다 • 사후 개체 복원	

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:DeleteObject 를 선택합니다	• 개체 삭제 • 여러 개체를 삭제합니다 • 사후 개체 복원	
S3:삭제 ObjectTagging	개체 태그 지정을 삭제합니다	
S3:DeleteObjectVersionTagging	개체 태그 지정 삭제(개체의 특정 버전)	
S3:DeleteObjectVersion	개체 삭제(개체의 특정 버전)	
S3:GetObject	• 객체 가져오기 • 헤드 개체 • 사후 개체 복원 • 개체 내용 을 선택합니다	
S3:GetObjectAcl	객체 ACL을 가져옵니다	
S3:GetObjectLegalHold	객체 법적 증거 자료 보관	
S3:GetObjectRetention	개체 보존 가져오기	
S3:GetObjectTagging	개체 태그 지정을 가져옵니다	
S3:GetObjectVersionTagging	개체 태그 지정 가져오기(개체의 특정 버전)	
S3:GetObjectVersion	개체 가져오기(개체의 특정 버전)	
S3:ListMultipartUploadParts(S3:ListMultimpartUploadParts) 를	부품 나열, POST 개체 복원	
S3:PutObject	• 개체 를 넣습니다 • 개체 - 복사 를 선택합니다 • 사후 개체 복원 • 멀티파트 업로드를 시작합니다 • 멀티파트 업로드를 완료합니다 • 부품 업로드 • 업로드 부품 - 복사	

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:PutObjectLegalHold	개체를 법적 증거 자료 보관	
S3:PutObjectRetention	개체 보존	
S3:PutObjectTagging	개체 태깅을 넣습니다	
S3:PutObjectVersionTagging	개체 태그 지정(개체의 특정 버전)	
S3:PutOverwriteObject	• 개체 를 넣습니다 • 개체 - 복사 를 선택합니다 • 개체 태그 지정 • 개체 태그 지정 삭제 • 멀티파트 업로드를 완료합니다	예
S3:RestoreObject	사후 개체 복원	

PutOverwriteObject 권한을 사용합니다

S3:PutOverwriteObject 권한은 개체를 만들거나 업데이트하는 작업에 적용되는 사용자 지정 StorageGRID 권한입니다. 이 사용 권한의 설정에 따라 클라이언트가 개체의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태그 지정을 덮어쓸 수 있는지 여부가 결정됩니다.

이 권한에 사용할 수 있는 설정은 다음과 같습니다.

- * 허용 *: 클라이언트가 개체를 덮어쓸 수 있습니다. 기본 설정입니다.
- * 거부 *: 클라이언트가 개체를 덮어쓸 수 없습니다. Deny 로 설정된 경우 PutOverwriteObject 권한은 다음과 같이 작동합니다.
  - 기존 객체가 같은 경로에 있는 경우:
    - 오브젝트의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태깅을 덮어쓸 수 없습니다.
    - 진행 중인 모든 수집 작업이 취소되고 오류가 반환됩니다.
    - S3 버전 관리가 활성화된 경우 거부 설정을 사용하면 개체 태그 지정 또는 개체 삭제 태그 지정 작업에서 개체 및 현재 버전이 아닌 개체의 TagSet을 수정할 수 없습니다.
  - 기존 개체를 찾을 수 없으면 이 권한은 적용되지 않습니다.
- 이 권한이 없으면 Allow가 설정된 것과 효과가 같습니다.

> 현재 S3 정책이 덮어쓰기를 허용하고 PutOverwriteObject 권한이 Deny 로 설정된 경우 클라이언트는 개체의 데이터, 사용자 정의 메타데이터 또는 개체 태그를 덮어쓸 수 없습니다. 또한, * 클라이언트 수정 방지 * 확인란이 선택된 경우(* 구성 * > * 시스템 * > * 그리드 옵션 *) 해당 설정은 PutOverwriteObject 권한 설정을 재정의합니다.

관련 정보

정책에서 조건을 지정합니다

조건은 정책이 적용되는 시점을 정의합니다. 조건은 연산자 및 키 값 쌍으로 구성됩니다.

조건은 평가에 키 값 쌍을 사용합니다. 조건 요소에는 여러 조건이 포함될 수 있으며 각 조건에는 여러 키 값 쌍이 포함될 수 있습니다. 조건 블럭은 다음 형식을 사용합니다:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

다음 예제에서 IPAddress 조건은 SOURCEIP 조건 키를 사용합니다.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

지원되는 조건 연산자

조건 연산자는 다음과 같이 분류됩니다.

- 문자열
- 숫자
- 부울
- IP 주소입니다
- Null 확인

조건 연산자	설명
StringEquals	정확한 일치(대/소문자 구분)를 기반으로 문자열 값과 키를 비교합니다.
StringNotEquals	키를 부정 일치(대/소문자 구분)를 기반으로 문자열 값과 비교합니다.
StringEqualsIgnoreCase 를 참조하십시오	정확한 일치를 기준으로 문자열 값과 키를 비교합니다(대/소문자 무시).

조건 연산자	설명
StringNotEqualsIgnoreCase 를 참조하십시오	Negated matching (대소문자 무시)을 기준으로 문자열 값과 키를 비교합니다.
StringLike 를 선택합니다	정확한 일치(대/소문자 구분)를 기반으로 문자열 값과 키를 비교합니다. 및 * 를 포함할 수 있습니까? 와일드카드 문자.
StringNotLike 를 참조하십시오	키를 부정 일치(대/소문자 구분)를 기반으로 문자열 값과 비교합니다. 및 * 를 포함할 수 있습니까? 와일드카드 문자.
NumericEquals	정확한 일치를 기준으로 키를 숫자 값과 비교합니다.
NumericNotEquals	키를 부정 일치를 기준으로 숫자 값과 비교합니다.
NumericGreaterThan	키를 ""보다 큼"" 일치를 기준으로 숫자 값과 비교합니다.
NumericGreaterThanEquals	키를 ""크거나 같음"" 일치를 기준으로 숫자 값과 비교합니다.
NumericLessThan	""보다 작음" 일치를 기준으로 키를 숫자 값과 비교합니다.
NumericLessThanEquals	키를 ""보다 작음 또는 같음" 일치를 기준으로 숫자 값과 비교합니다.
불입니다	"true 또는 false" 일치를 기준으로 키를 부울 값과 비교합니다.
IP 주소	키를 IP 주소 또는 IP 주소 범위와 비교합니다.
NotIpAddress 를 참조하십시오	부정 일치를 기준으로 IP 주소 또는 IP 주소 범위와 키를 비교합니다.
null입니다	현재 요청 컨텍스트에 조건 키가 있는지 확인합니다.

지원되는 조건 키

범주	적용 가능한 조건 키	설명
IP 연산자	AWS: SOURCEIP	요청이 전송된 IP 주소와 비교합니다. 버킷 또는 오브젝트 작업에 사용할 수 있습니다. • 참고: * S3 요청이 관리 노드 및 게이트웨이 노드의 로드 밸런서 서비스를 통해 전송된 경우 로드 밸런서 서비스의 IP 주소 업스트림과 비교됩니다. • 참고 *: 타사, 비투명 로드 밸런서가 사용되는 경우 이 로드 밸런서의 IP 주소와 비교합니다. X-Forwarded-For 헤더는 유효성을 확인할 수 없기 때문에 무시됩니다.
리소스/ID입니다	AWS: 사용자 이름	요청이 전송된 보낸 사람의 사용자 이름과 비교합니다. 버킷 또는 오브젝트 작업에 사용할 수 있습니다.
S3:ListBucket 및 S3: ListBuckketVersions 권한	S3: 구분 기호	버킷 가져오기 또는 버킷 오브젝트 버전 가져오기 요청에 지정된 구분 기호 매개변수와 비교합니다.
S3:ListBucket 및 S3: ListBuckketVersions 권한	S3: 최대 키	버킷 가져오기 또는 버킷 객체 버전 가져오기 요청에 지정된 최대 키 매개변수와 비교합니다.
S3:ListBucket 및 S3: ListBuckketVersions 권한	S3: 접두어	Get Bucket 또는 Get Bucket Object Versions 요청에 지정된 접두사 매개변수와 비교합니다.
S3:PutObject	S3: 오브젝트 잠금 장치 - 남은 보존 기간(일)	'x-amz-object-lock-retain-until-date' 요청 헤더에 지정된 보존 기한 또는 버킷 기본 보존 기간(bucket default retention period)에서 계산된 보존 기한(retain-until-date)과 비교하여 이러한 값이 다음 요청에 대해 허용 가능한 범위 내에 있는지 확인합니다. • 개체 를 넣습니다 • 개체 - 복사 를 선택합니다 • 멀티파트 업로드를 시작합니다

범주	적용 가능한 조건 키	설명
S3:PutObjectRetention	S3: 오브젝트 잠금 장치 - 남은 보존 기간(일)	허용 범위 내에 있는지 확인하기 위해 Put Object Retention 요청에 지정된 Retain-until-date와 비교합니다.

정책에 변수를 지정합니다

정책의 변수를 사용하여 사용 가능한 정책 정보를 채울 수 있습니다. 'Resource' 요소와 'Condition' 요소의 문자열 비교에 정책 변수를 사용할 수 있습니다.

이 예제에서 변수 "${AWS:UserName}"은(는) Resource 요소의 일부입니다.

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

이 예제에서 변수 "${AWS:username}"은 조건 블록의 조건 값의 일부입니다.

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

변수	설명
'${AWS:SOURCEIP}'	SOURCEIP 키를 제공된 변수로 사용합니다.
'${AWS:username}'	제공된 변수로 사용자 이름 키를 사용합니다.
'${s3:prefix}'	서비스별 prefix key를 제공된 variable 로 사용한다.
'${S3:max-keys}'	서비스별 최대 키 키를 제공된 변수로 사용합니다.
'${ *}'	특수 문자. 문자를 리터럴 * 문자로 사용합니다.
"${?}"	특수 문자. 문자를 리터럴로 사용합니까? 문자.
"${$}"	특수 문자. 문자를 리터럴 $ 문자로 사용합니다.

특별한 처리가 필요한 정책을 생성합니다

때로는 정책에 따라 보안이 위험하거나 계정 루트 사용자를 잠그는 등 지속적인 작업에 위험한 사용 권한을 부여할 수 있습니다. StorageGRID S3 REST API 구현은 Amazon보다 정책 검증 중에 덜 제한적이지만 정책 평가 중에도

동일하게 엄격합니다.

정책 설명입니다	정책 유형입니다	아마존 행동	**StorageGRID** 동작
루트 계정에 대한 모든 권한을 스스로 거부합니다	버킷	유효하고 적용되지만 루트 사용자 계정은 모든 S3 버킷 정책 작업에 대한 권한을 보유합니다	동일합니다
사용자/그룹에 대한 모든 권한을 스스로 거부합니다	그룹	유효하고 시행되었습니다	동일합니다
외부 계정 그룹에 모든 권한을 허용합니다	버킷	주체가 잘못되었습니다	유효하지만 모든 S3 버킷 정책 작업에 대한 권한은 정책에서 허용하는 경우 405 메서드 허용되지 않음 오류를 반환합니다
외부 계정 루트 또는 사용자에게 모든 권한을 허용합니다	버킷	유효하지만 모든 S3 버킷 정책 작업에 대한 권한은 정책에서 허용하는 경우 405 메서드 허용되지 않음 오류를 반환합니다	동일합니다
모든 사용자에게 모든 작업에 대한 사용 권한을 허용합니다	버킷	유효하지만 모든 S3 버킷 정책 작업에 대한 사용 권한이 외국 계정 루트 및 사용자에 대해 405 메서드 허용 안 됨 오류를 반환합니다	동일합니다
모든 작업에 대한 모든 사용자의 권한을 거부합니다	버킷	유효하고 적용되지만 루트 사용자 계정은 모든 S3 버킷 정책 작업에 대한 권한을 보유합니다	동일합니다
보안 주체는 존재하지 않는 사용자 또는 그룹입니다	버킷	주체가 잘못되었습니다	유효합니다
리소스가 존재하지 않는 S3 버킷입니다	그룹	유효합니다	동일합니다
보안 주체는 로컬 그룹입니다	버킷	주체가 잘못되었습니다	유효합니다

정책 설명입니다	정책 유형입니다	아마존 행동	**StorageGRID** 동작
정책은 개체를 넣을 수 있는 비소유자 계정(익명 계정 포함) 권한을 부여합니다	버킷	유효합니다. 객체는 생성자 계정이 소유하며 버킷 정책은 적용되지 않습니다. 생성자 계정은 개체 ACL을 사용하여 개체에 대한 액세스 권한을 부여해야 합니다.	유효합니다. 오브젝트는 버킷 소유자 계정이 소유합니다. 버킷 정책이 적용됩니다.

WORM(Write-Once-Read-Many) 보호

WORM(Write-Once-Read-Many) 버킷을 생성하여 데이터, 사용자 정의 오브젝트 메타데이터 및 S3 오브젝트 태깅을 보호할 수 있습니다. 새 객체를 생성하고 기존 컨텐츠를 덮어쓰거나 삭제하지 못하도록 WORM 버킷을 구성합니다. 여기에 설명된 방법 중 하나를 사용합니다.

덮어쓰기가 항상 거부되도록 하려면 다음을 수행할 수 있습니다.

- Grid Manager에서 * 구성 * > * 시스템 * > * 그리드 옵션 * 으로 이동하여 * 클라이언트 수정 방지 * 확인란을 선택합니다.
- 다음 규칙 및 S3 정책을 적용합니다.
  - S3 정책에 PutOverwriteObject 거부 작업을 추가합니다.
  - DeleteObject 거부 작업을 S3 정책에 추가합니다.
  - S3 정책에 오브젝트 허용(Put Object Allow) 작업을 추가합니다.

> S3 정책에서 DeleteObject 를 deny 로 설정해도 ""30일 후 0개 복사본""과 같은 규칙이 있을 때 ILM이 개체를 삭제하는 것을 차단하지 않습니다.

> 이러한 규칙과 정책이 모두 적용되더라도 동시 쓰기를 방지하지 않습니다(상황 A 참조). 순차적 완료된 덮어쓰기를 방지합니다(상황 B 참조).

- 상황 A *: 동시 쓰기(보호 안 됨)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

- 상황 B *: 순차적 완료된 덮어쓰기(방지됨)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

관련 정보

ILM을 사용하여 개체를 관리합니다

특별한 처리가 필요한 정책을 생성합니다

StorageGRID ILM 규칙이 개체를 관리하는 방법

S3 그룹 정책의 예

S3 정책 예

이 섹션의 예를 사용하여 버킷 및 그룹에 대한 StorageGRID 액세스 정책을 구축합니다.

S3 버킷 정책의 예

버킷 정책은 정책이 연결된 버킷에 대한 액세스 권한을 지정합니다. 버킷 정책은 S3 PutBucketPolicy API를 사용하여 구성됩니다.

다음 명령에 따라 AWS CLI를 사용하여 버킷 정책을 구성할 수 있습니다.

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

예: 모든 사용자가 버킷에 읽기 전용 액세스를 허용합니다

이 예제에서는 anonymous 를 비롯한 모든 사람이 버킷에 있는 오브젝트를 나열하고 버킷에 있는 모든 오브젝트에 대해 오브젝트 가져오기 작업을 수행할 수 있습니다. 다른 모든 작업은 거부됩니다. 이 정책은 계정 루트 외에는 버킷에 쓸 수 있는 권한이 없으므로 특히 유용하지 않을 수 있습니다.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

예: 한 계정의 모든 사용자가 완전히 액세스할 수 있도록 허용하고 다른 계정의 모든 사용자는 버킷에 읽기 전용으로 액세스할 수 있습니다

이 예제에서는 지정된 계정의 모든 사용자가 버킷에 완전히 액세스할 수 있지만, 지정된 다른 계정의 모든 사용자는 '공유/' 개체 키 접두사로 시작하는 버킷의 개체에 대해 버킷을 나열하고 GetObject 작업을 수행할 수만 있습니다.

> StorageGRID에서 비소유자 계정(익명 계정 포함)으로 생성된 객체는 버킷 소유자 계정이 소유합니다. 버킷 정책은 이러한 오브젝트에 적용됩니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

예: 모든 사용자가 버킷에 대한 읽기 전용 액세스 및 지정된 그룹에 의한 전체 액세스 허용

이 예에서는 anonymous를 비롯한 모든 사용자가 버킷을 나열하고 버킷의 모든 오브젝트에 대해 오브젝트 가져오기 작업을 수행할 수 있지만 지정된 계정의 MMarketing 그룹에 속한 사용자만 전체 액세스가 허용됩니다.

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

예: 클라이언트가 **IP** 범위에 있는 경우 모든 사용자가 버킷에 대한 읽기 및 쓰기 액세스를 허용합니다

이 예제에서는 요청이 지정된 IP 범위(54.240.143.0 ~ 54.240.143.255, 54.240.143.188 제외)에서 발생한 경우 anonymous를 포함한 모든 사람이 버킷을 나열하고 버킷의 모든 오브젝트에 대해 오브젝트 작업을 수행할 수 있습니다. 다른 모든 작업이 거부되고 IP 범위를 벗어난 모든 요청이 거부됩니다.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

예: 지정된 통합 사용자가 단독으로 버킷을 완전히 액세스할 수 있도록 허용합니다

이 예에서는 페더레이션 사용자 Alex가 'examplebucket' 버킷과 그 객체에 대한 전체 액세스를 허용합니다. "root"를 포함한 다른 모든 사용자는 모든 작업을 명시적으로 거부합니다. 그러나 "root"는 PUT/GET/DeleteBucketPolicy에 대한 권한이 거부되지 않습니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::9539088723000255820 2:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::9539088723000255820 2:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

예: **PutOverwriteObject** 권한

이 예제에서 PutOverwriteObject 및 DeleteObject 에 대한 Deny 효과를 사용하면 개체의 데이터, 사용자 정의 메타데이터 및 S3 개체 태그를 덮어쓰거나 삭제할 수 없습니다.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

관련 정보

버킷 작업

S3 그룹 정책의 예

그룹 정책은 정책이 연결된 그룹에 대한 액세스 권한을 지정합니다. 이 정책에는 주체가 없는 것은 암묵적인 것이기 때문입니다. 그룹 정책은 테넌트 관리자 또는 API를 사용하여 구성됩니다.

예: 테넌트 관리자를 사용하여 그룹 정책을 설정합니다

테넌트 관리자를 사용하여 그룹을 추가 또는 편집할 때 이 그룹의 S3 액세스 권한 구성원이 가질 그룹 정책을 생성하는

방법을 다음과 같이 선택할 수 있습니다.

- * S3 액세스 없음 *: 기본 옵션. 이 그룹의 사용자는 버킷 정책을 통해 액세스가 부여되지 않는 한 S3 리소스에 액세스할 수 없습니다. 이 옵션을 선택하면 루트 사용자만 기본적으로 S3 리소스에 액세스할 수 있습니다.
- * 읽기 전용 액세스 *: 이 그룹의 사용자는 S3 리소스에 대한 읽기 전용 액세스 권한을 가집니다. 예를 들어 이 그룹의 사용자는 개체를 나열하고 개체 데이터, 메타데이터 및 태그를 읽을 수 있습니다. 이 옵션을 선택하면 읽기 전용 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
- * 전체 액세스 *: 이 그룹의 사용자는 버킷을 포함하여 S3 리소스에 대한 모든 액세스 권한을 가집니다. 이 옵션을 선택하면 전체 액세스 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열은 편집할 수 없습니다.
- * 사용자 정의 *: 그룹의 사용자에게는 텍스트 상자에 지정한 사용 권한이 부여됩니다.

  이 예제에서 그룹의 구성원은 지정된 버킷의 특정 폴더(키 접두사)를 나열하고 액세스할 수만 있습니다.

예**:** 모든 버킷에 대한 그룹 전체 액세스 허용

이 예에서 그룹의 모든 구성원은 버킷 정책에 의해 명시적으로 거부되지 않는 한 테넌트 계정이 소유한 모든 버킷에 대해 전체 액세스가 허용됩니다.

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

예: 모든 버킷에 대한 그룹 읽기 전용 액세스를 허용합니다

이 예제에서 그룹의 모든 구성원은 버킷 정책에 의해 명시적으로 거부되지 않는 한 S3 리소스에 대해 읽기 전용 액세스 권한을 갖습니다. 예를 들어 이 그룹의 사용자는 개체를 나열하고 개체 데이터, 메타데이터 및 태그를 읽을 수 있습니다.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

예: 그룹 구성원이 버킷의 "" 폴더에만 완전히 액세스할 수 있도록 허용합니다

이 예제에서 그룹의 구성원은 지정된 버킷의 특정 폴더(키 접두사)를 나열하고 액세스할 수만 있습니다. 이러한 폴더의 개인 정보를 확인할 때는 다른 그룹 정책 및 버킷 정책의 액세스 권한을 고려해야 합니다.

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

관련 정보

테넌트 계정을 사용합니다

REST API에 대한 보안을 구성합니다

REST API에 대해 구현된 보안 조치를 검토하고 시스템 보안 방법을 이해해야 합니다.

StorageGRID에서 REST API에 대한 보안을 제공하는 방법

StorageGRID 시스템이 REST API에 대한 보안, 인증 및 권한 부여를 구현하는 방법을 이해해야 합니다.

StorageGRID는 다음과 같은 보안 조치를 사용합니다.

- 로드 밸런서 끝점에 HTTPS가 구성되어 있는 경우 로드 밸런서 서비스와의 클라이언트 통신은 HTTPS를 사용합니다.

  로드 밸런서 끝점을 구성할 때 HTTP를 선택적으로 활성화할 수 있습니다. 예를 들어, 테스트 또는 기타 비운영 목적으로 HTTP를 사용할 수 있습니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

- 기본적으로 StorageGRID는 게이트웨이 노드에서 스토리지 노드 및 CLB 서비스와의 클라이언트 통신에 HTTPS를 사용합니다.

  이러한 연결에 대해 HTTP를 선택적으로 활성화할 수 있습니다. 예를 들어, 테스트 또는 기타 비운영 목적으로 HTTP를 사용할 수 있습니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

CLB 서비스는 더 이상 사용되지 않습니다.

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

보안 인증서 및 클라이언트 응용 프로그램

클라이언트는 게이트웨이 노드 또는 관리 노드의 로드 밸런서 서비스, 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 직접 연결할 수 있습니다.

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

- 클라이언트 응용 프로그램이 로드 밸런서 서비스에 연결되면 연결을 만드는 데 사용되는 특정 로드 밸런서 끝점에 대해 구성된 인증서를 사용합니다. 각 끝점마다 고유한 인증서가 있습니다. 이 인증서는 그리드 관리자가 업로드한 사용자 지정 서버 인증서이거나, 끝점 구성 시 그리드 관리자가 StorageGRID에서 생성한 인증서입니다.
- 클라이언트 응용 프로그램이 게이트웨이 노드의 스토리지 노드 또는 CLB 서비스에 직접 연결할 때 StorageGRID 시스템이 설치될 때 스토리지 노드에 대해 생성된 시스템 생성 서버 인증서(시스템 인증 기관이 서명)를 사용합니다. 또는 그리드 관리자가 그리드에 제공하는 단일 사용자 정의 서버 인증서입니다.

클라이언트가 TLS 연결을 설정하는 데 사용하는 인증서를 신뢰하도록 구성해야 합니다.

로드 밸런서 끝점 구성에 대한 정보와 TLS 연결에 대한 단일 사용자 지정 서버 인증서를 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 직접 추가하는 방법에 대한 지침은 StorageGRID 관리 지침을 참조하십시오.

요약

다음 표에서는 S3 및 Swift REST API에서 보안 문제가 구현되는 방식을 보여 줍니다.

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

관련 정보

StorageGRID 관리

TLS 라이브러리에 대해 지원되는 해시 및 암호화 알고리즘

StorageGRID 시스템은 TLS(전송 계층 보안) 세션을 설정할 때 클라이언트 응용 프로그램에서 사용할 수 있는 제한된 암호화 그룹 세트를 지원합니다.

지원되는 **TLS** 버전입니다

StorageGRID는 TLS 1.2 및 TLS 1.3을 지원합니다.

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

지원되는 암호 그룹

TLS 버전입니다	암호화 그룹의 **IANA** 이름입니다
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
1.2	TLS_ECDHE_RSA_WITH_CHACH20_POLY1305_SHA256
1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
1.3	TLS_CHACH20_POLY1305_SHA256
1.3	TLS_AES_128_GCM_SHA256

더 이상 사용되지 않는 암호화 그룹

다음 암호화 그룹은 더 이상 사용되지 않습니다. 이러한 암호화에 대한 지원은 이후 릴리스에서 제거됩니다.

IANA 이름입니다
TLS_RSA_with_AES_128_GCM_SHA256
TLS_RSA_WITED_AES_256_GCM_SHA384

관련 정보

클라이언트 연결 구성 방법

운영 모니터링 및 감사

전체 그리드 또는 특정 노드에 대한 트랜잭션 추세를 확인하여 클라이언트 작업의 워크로드 및 효율성을 모니터링할 수 있습니다. 감사 메시지를 사용하여 클라이언트 작업 및 트랜잭션을 모니터링할 수 있습니다.

오브젝트 수집 및 검색 속도와 오브젝트 수, 쿼리, 검증을 위한 메트릭을 모니터링할 수 있습니다. 클라이언트 응용 프로그램이 StorageGRID 시스템에서 개체를 읽고, 쓰고, 수정하는 데 성공한 시도 및 실패한 시도 횟수를 볼 수 있습니다.

단계

1. 를 사용하여 Grid Manager에 로그인합니다 지원되는 웹 브라우저.
2. Dashboard에서 Protocol Operations 섹션을 찾습니다.

   이 섹션에서는 StorageGRID 시스템에서 수행하는 클라이언트 작업의 수를 요약합니다. 프로토콜 속도는 최근 2분 동안의 평균값입니다.

3. 노드 * 를 선택합니다.
4. 노드 홈 페이지(배포 수준)에서 * 로드 밸런서 * 탭을 클릭합니다.

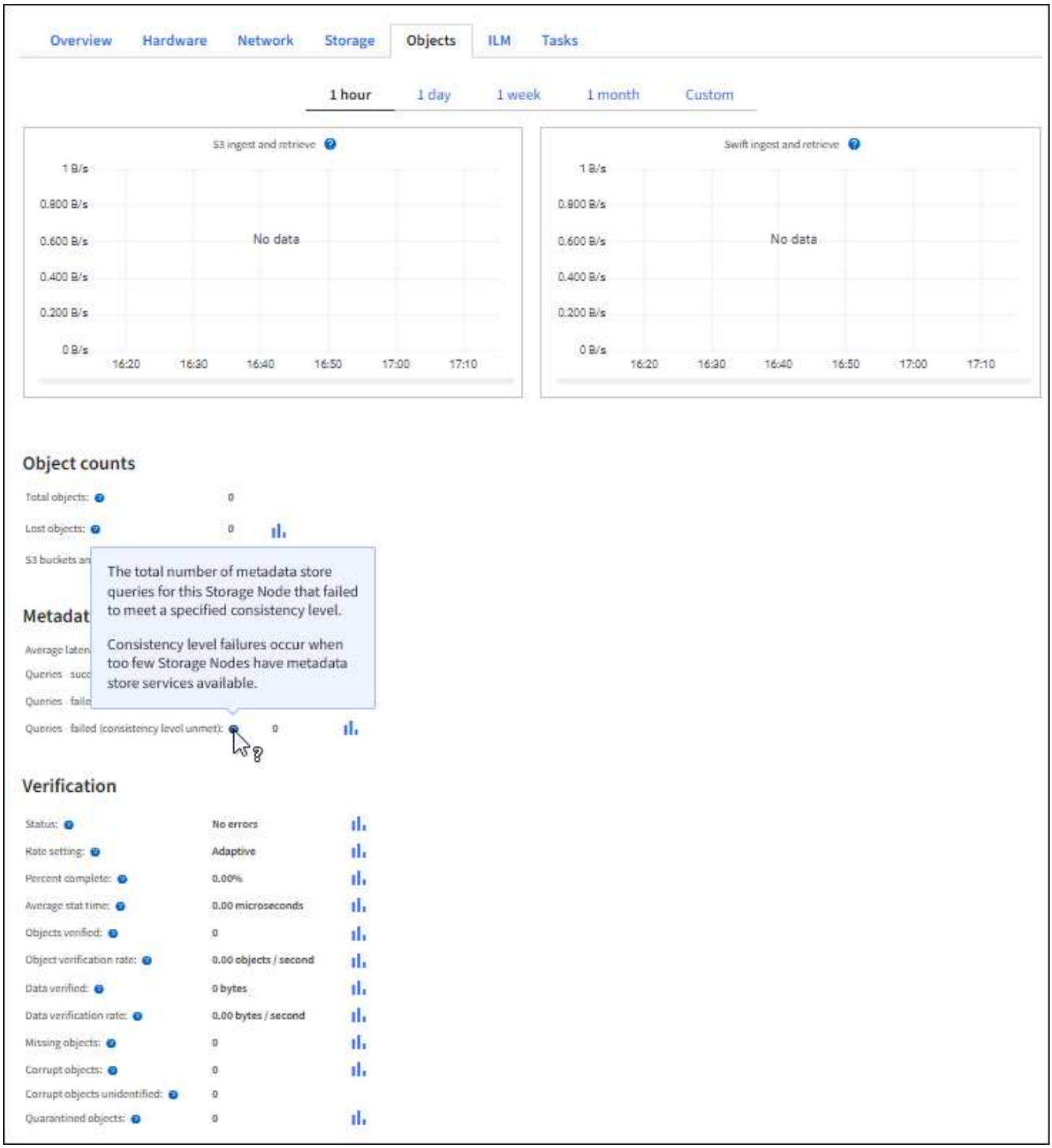
   차트에는 그리드 내의 로드 밸런서 끝점에 대한 모든 클라이언트 트래픽에 대한 추세가 표시됩니다. 시간 간격(시간, 일, 주, 월 또는 년)을 선택할 수 있습니다. 또는 사용자 지정 간격을 적용할 수 있습니다.

5. 노드 홈 페이지(배포 수준)에서 * 개체 * 탭을 클릭합니다.

   이 차트에는 전체 StorageGRID 시스템의 수집 및 검색 속도가 초당 바이트 및 총 바이트 단위로 표시됩니다. 시간 간격(시간, 일, 주, 월 또는 년)을 선택할 수 있습니다. 또는 사용자 지정 간격을 적용할 수 있습니다.

6. 특정 스토리지 노드에 대한 정보를 보려면 왼쪽의 목록에서 노드를 선택하고 * Objects * 탭을 클릭합니다.

   이 차트에는 이 스토리지 노드의 객체 수집 및 검색 속도가 나와 있습니다. 이 탭에는 개체 수, 쿼리 및 검증에 대한 메트릭도 포함되어 있습니다. 레이블을 클릭하여 이러한 메트릭의 정의를 볼 수 있습니다.



7. 더 자세한 내용을 원하는 경우:
   a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
   b. site_ * > * Overview * > * Main * 을 선택합니다.

      API 작업 섹션에는 전체 그리드에 대한 요약 정보가 표시됩니다.

   c. 스토리지 노드 * > * LDR * > **CLIENT APPLICATION* * > * Overview * > * Main * 을 선택합니다

      작업 섹션에는 선택한 스토리지 노드에 대한 요약 정보가 표시됩니다.

감사 로그 액세스 및 검토

감사 메시지는 StorageGRID 서비스에서 생성되고 텍스트 로그 파일에 저장됩니다. 감사 로그의 API 관련 감사 메시지는 시스템의 상태를 평가하는 데 도움이 되는 중요한 보안, 운영 및 성능 모니터링 데이터를 제공합니다.

필요한 것

- 특정 액세스 권한이 있습니다.
- "passwords.txt" 파일이 있습니다.
- 관리 노드의 IP 주소를 알고 있습니다.

이 작업에 대해

활성 감사 로그 파일은 AUDIT.LOG라는 이름으로 관리 노드에 저장됩니다.

하루에 한 번 활성 audit.log 파일이 저장되고 새 감사.로그 파일이 시작됩니다. 저장된 파일의 이름은 저장 시기를 나타냅니다('*yyyy-mm-dd.txt*' 형식).

하루 후에는 원래 날짜를 유지하는 형식(*yyyy-mm-dd.txt.gz*)으로 저장된 파일이 압축되고 이름이 변경됩니다.

이 예에서는 액티브 'audit.log' 파일, 전날 파일('2018-04-15.txt') 및 전날 압축 파일('2018-04-14.txt.gz')을 보여줍니다.

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

단계

1. 관리자 노드에 로그인:
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
2. 감사 로그 파일이 포함된 디렉토리로 이동합니다.

   ```
   cd /var/local/audit/export
   ```

3. 필요에 따라 현재 또는 저장된 감사 로그 파일을 봅니다.

감사 로그에서 **S3** 작업을 추적했습니다

StorageGRID 감사 로그에서 여러 버킷 작업 및 오브젝트 작업을 추적합니다.

감사 로그에서 버킷 작업을 추적했습니다

- 버킷 삭제
- 버킷 태그 지정을 삭제합니다

- 여러 개체를 삭제합니다
- 버킷 가져오기(객체 나열)
- 버킷 객체 버전을 가져옵니다
- 버킷 태그 지정을 가져옵니다
- 헤드 버킷
- 버킷 을 놓습니다
- 버킷 규정 준수
- Bucket 태그 달기
- 버킷 버전 관리

감사 로그에서 추적된 객체 작업입니다

- 멀티파트 업로드를 완료합니다
- 파트 업로드(ILM 규칙이 Strict 또는 Balanced 수집 동작을 사용하는 경우)
- Upload Part-Copy (ILM 규칙이 Strict 또는 Balanced 수집 동작을 사용하는 경우)
- 개체 삭제
- 객체 가져오기
- 헤드 개체
- 사후 개체 복원
- 개체 를 넣습니다
- 개체 - 복사 를 선택합니다

관련 정보

버킷 작업

객체에 대한 작업

활성, 유휴 및 동시 **HTTP** 연결의 이점

HTTP 연결을 구성하는 방법은 StorageGRID 시스템의 성능에 영향을 줄 수 있습니다. 구성은 HTTP 연결이 활성 상태인지 유휴 상태인지 또는 여러 개의 동시 연결이 있는지 여부에 따라 달라집니다.

다음과 같은 유형의 HTTP 연결에 대한 성능 이점을 확인할 수 있습니다.

- 유휴 HTTP 연결
- 활성 HTTP 연결
- 동시 HTTP 연결

유휴 **HTTP** 연결을 열어 두면 얻을 수 있는 이점

클라이언트 응용 프로그램이 열려 있는 연결을 통해 후속 트랜잭션을 수행할 수 있도록 클라이언트 응용 프로그램이 유휴 상태인 경우에도 HTTP 연결을 열어 두어야 합니다. 시스템 측정 및 통합 경험을 바탕으로 유휴 HTTP 연결을 최대 10분 동안 열어 두어야 합니다. StorageGRID는 열려 있고 10분 이상 유휴 상태로 유지되는 HTTP 연결을 자동으로 닫을 수 있습니다.

개방 및 유휴 HTTP 연결은 다음과 같은 이점을 제공합니다.

- StorageGRID 시스템이 HTTP 트랜잭션을 수행해야 한다고 결정하는 시간부터 StorageGRID 시스템이 트랜잭션을 수행할 수 있는 시간까지 지연 시간을 줄였습니다

  지연 시간 감소는 특히 TCP/IP 및 TLS 연결을 설정하는 데 필요한 시간의 주요 장점입니다.

- 이전에 수행된 전송을 사용하여 TCP/IP 저속 시작 알고리즘을 프라이밍하여 데이터 전송 속도를 높였습니다
- 클라이언트 응용 프로그램과 StorageGRID 시스템 간의 연결을 중단하는 여러 가지 장애 조건에 대한 즉각적인 알림

유휴 연결을 유지하는 기간을 결정하는 것은 기존 연결과 관련된 느린 시작의 이점과 내부 시스템 리소스에 대한 연결의 이상적인 할당을 절충하는 것입니다.

활성 **HTTP** 연결의 이점

스토리지 노드 또는 게이트웨이 노드의 CLB 서비스(더 이상 사용되지 않음)에 직접 연결하는 경우 HTTP 연결이 지속적으로 트랜잭션을 수행하더라도 활성 HTTP 연결 기간을 최대 10분으로 제한해야 합니다.

연결을 열어 두어야 하는 최대 기간을 결정하는 것은 연결 지속성의 이점과 내부 시스템 리소스에 대한 연결을 이상적으로 할당하는 것입니다.

클라이언트가 스토리지 노드 또는 CLB 서비스에 접속할 경우 활성 HTTP 연결을 제한하면 다음과 같은 이점이 있습니다.

- StorageGRID 시스템 전체에서 최적의 로드 밸런싱을 지원합니다.

  CLB 서비스를 사용할 때는 오래 지속되는 TCP/IP 연결을 방지하여 StorageGRID 시스템 전체의 로드 밸런싱을 최적화해야 합니다. HTTP 연결을 다시 설정하고 재조정할 수 있도록 클라이언트 응용 프로그램을 구성하여 각 HTTP 연결 기간을 추적하고 설정된 시간 후에 HTTP 연결을 닫아야 합니다.

  CLB 서비스는 클라이언트 응용 프로그램이 HTTP 연결을 설정할 때 StorageGRID 시스템 전체의 로드 균형을 조정합니다. 시간이 지남에 따라 로드 밸런싱 요구 사항이 변경됨에 따라 HTTP 연결이 더 이상 최적화되지 않을 수 있습니다. 시스템은 클라이언트 애플리케이션이 각 트랜잭션에 대해 별도의 HTTP 연결을 설정할 때 최상의 로드 밸런싱을 수행하지만, 이 경우 영구 연결과 관련된 훨씬 더 가치 있는 이득을 얻을 수 없습니다.

  ⓘ CLB 서비스는 더 이상 사용되지 않습니다.

- 클라이언트 응용 프로그램이 사용 가능한 공간이 있는 LDR 서비스로 HTTP 트랜잭션을 보낼 수 있도록 합니다.
- 유지보수 절차를 시작할 수 있습니다.

일부 유지 관리 절차는 진행 중인 모든 HTTP 연결이 완료된 후에만 시작됩니다.

부하 분산 서비스에 대한 클라이언트 연결의 경우 일부 유지 관리 절차를 즉시 시작할 수 있도록 개방 연결 기간을 제한하는 것이 유용할 수 있습니다. 클라이언트 연결 기간이 제한되지 않으면 활성 연결이 자동으로 종료되는 데 몇 분이 걸릴 수 있습니다.

동시 **HTTP** 연결의 이점

병렬 처리를 허용하도록 StorageGRID 시스템에 대한 여러 TCP/IP 연결을 열린 상태로 유지하여 성능을 향상시켜야 합니다. 최적의 병렬 연결 수는 다양한 요인에 따라 달라집니다.

동시 HTTP 연결은 다음과 같은 이점을 제공합니다.

- 지연 시간 단축

  다른 트랜잭션이 완료될 때까지 기다리지 않고 즉시 트랜잭션을 시작할 수 있습니다.

- 처리량 향상

  StorageGRID 시스템은 병렬 트랜잭션을 수행하고 총 트랜잭션 처리량을 늘릴 수 있습니다.

클라이언트 응용 프로그램은 여러 HTTP 연결을 설정해야 합니다. 클라이언트 응용 프로그램은 트랜잭션을 수행해야 하는 경우 트랜잭션을 현재 처리하지 않는 설정된 연결을 선택하여 즉시 사용할 수 있습니다.

각 StorageGRID 시스템의 토폴로지에는 성능이 저하되기 전에 동시 트랜잭션 및 연결에 대해 서로 다른 최대 처리량이 있습니다. 최대 처리량은 컴퓨팅 리소스, 네트워크 리소스, 스토리지 리소스, WAN 링크 등의 요인에 따라 달라집니다. StorageGRID 시스템에서 지원하는 서버 및 서비스 수와 애플리케이션 수도 고려해야 합니다.

StorageGRID 시스템은 종종 여러 클라이언트 애플리케이션을 지원합니다. 클라이언트 응용 프로그램에서 사용하는 최대 동시 연결 수를 결정할 때 이 점에 유의해야 합니다. 클라이언트 응용 프로그램이 StorageGRID 시스템에 대한 연결을 설정하는 여러 소프트웨어 엔터티로 구성된 경우 엔터티에 대한 모든 연결을 추가해야 합니다. 다음과 같은 경우 최대 동시 연결 수를 조정해야 할 수 있습니다.

- StorageGRID 시스템의 토폴로지는 시스템에서 지원할 수 있는 최대 동시 트랜잭션 및 연결 수에 영향을 줍니다.
- 대역폭이 제한된 네트워크에서 StorageGRID 시스템과 상호 작용하는 클라이언트 응용 프로그램은 개별 트랜잭션이 적절한 시간 내에 완료되도록 동시성 정도를 줄여야 할 수 있습니다.
- 많은 클라이언트 응용 프로그램이 StorageGRID 시스템을 공유하는 경우 시스템의 제한을 초과하지 않도록 동시성 정도를 줄여야 할 수 있습니다.

읽기 및 쓰기 작업을 위한 **HTTP** 연결 풀 분리

읽기 및 쓰기 작업에 별도의 HTTP 연결 풀을 사용하고 각 풀에 사용할 풀 수를 제어할 수 있습니다. 별도의 HTTP 연결 풀을 통해 트랜잭션을 보다 효율적으로 제어하고 로드 밸런싱을 수행할 수 있습니다.

클라이언트 애플리케이션은 검색 가능(읽기) 또는 저장 가능(쓰기) 부하를 생성할 수 있습니다. 읽기 및 쓰기 트랜잭션을 위한 별도의 HTTP 연결 풀을 사용하여 읽기 또는 쓰기 트랜잭션에 사용할 각 풀의 양을 조정할 수 있습니다.

Swift를 사용합니다

Swift:개요 를 사용합니다

클라이언트 애플리케이션은 OpenStack Swift API를 사용하여 StorageGRID 시스템과 상호 작용할 수 있습니다.

StorageGRID는 다음과 같은 특정 버전의 Swift 및 HTTP를 지원합니다.

항목	버전
SwiFT 사양	2015년 11월 기준 OpenStack Swift Object Storage API v1
HTTP	1.1 HTTP에 대한 자세한 내용은 HTTP/1.1(RFC 7230-35)을 참조하십시오. • 참고 *: StorageGRID는 HTTP/1.1 파이프라이닝을 지원하지 않습니다.

관련 정보

"OpenStack: 오브젝트 스토리지 API"

StorageGRID의 **Swift API** 지원 기록

Swift REST API에 대한 StorageGRID 시스템의 지원 변경 사항을 숙지해야 합니다.

놓습니다	설명
11.6	편집상의 사소한 변경.
11.5	약한 일관성 제어 기능이 제거되었습니다. 대신 사용 가능한 정합성 보장 레벨이 사용됩니다.
11.4	TLS 1.3에 대한 지원 및 지원되는 TLS 암호 제품군의 업데이트된 목록이 추가되었습니다. CLB는 사용되지 않습니다. ILM과 정합성 보장 설정 간의 상호 관계에 대한 설명이 추가되었습니다.
11.3	수집 시 동기식 배치를 사용하는 ILM 규칙(Ingest 동작에 대한 균형 및 엄격 옵션)의 영향을 설명하기 위해 PUT 오브젝트 작업이 업데이트되었습니다. 로드 밸런서 끝점 또는 고가용성 그룹을 사용하는 클라이언트 연결에 대한 설명이 추가되었습니다. 지원되는 TLS 암호 그룹 목록이 업데이트되었습니다. TLS 1.1 암호가 더 이상 지원되지 않습니다.

놓습니다	설명
11.2	문서에 대한 사소한 편집 변경.
11.1	그리드 노드에 대한 Swift 클라이언트 연결에 HTTP 사용 지원이 추가되었습니다. 일관성 제어의 정의를 업데이트했습니다.
11.0	각 테넌트 계정에 대해 1,000개의 컨테이너에 대한 지원이 추가되었습니다.
10.3	문서의 관리 업데이트 및 수정. 사용자 지정 서버 인증서를 구성하기 위한 섹션이 제거되었습니다.
10.2	StorageGRID 시스템에서 Swift API의 초기 지원 현재 지원되는 버전은 OpenStack Swift Object Storage API v1 입니다.

StorageGRID가 **Swift REST API**를 구현하는 방법

클라이언트 애플리케이션은 Swift REST API 호출을 사용하여 스토리지 노드 및 게이트웨이 노드에 연결하여 컨테이너를 생성하고 오브젝트를 저장 및 검색할 수 있습니다. 이를 통해 OpenStack Swift용으로 개발된 서비스 중심 애플리케이션을 StorageGRID 시스템에서 제공하는 사내 오브젝트 스토리지에 연결할 수 있습니다.

Swift 오브젝트 관리

Swift 객체가 StorageGRID 시스템에서 수집되면 시스템의 활성 ILM 정책에 있는 ILM(정보 수명 주기 관리) 규칙에 의해 관리됩니다. ILM 규칙 및 정책은 StorageGRID이 오브젝트 데이터 복사본을 만들고 배포하는 방법과 시간이 지남에 따라 이러한 복사본을 관리하는 방법을 결정합니다. 예를 들어, ILM 규칙은 특정 Swift 컨테이너의 개체에 적용될 수 있으며 특정 기간 동안 여러 개체 복사본을 여러 데이터 센터에 저장하도록 지정할 수 있습니다.

그리드의 ILM 규칙 및 정책이 Swift 테넌트 계정의 개체에 어떤 영향을 미치는지 알아야 하는 경우 StorageGRID 관리자에게 문의하십시오.

클라이언트 요청 충돌

동일한 키에 쓰는 두 클라이언트 등의 충돌하는 클라이언트 요청은 "최신 성공" 기준으로 해결됩니다. "최신" 평가 시기는 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 하며, Swift 클라이언트가 작업을 시작하는 시점이 아닙니다.

일관성 보장 및 제어

기본적으로 StorageGRID는 새로 생성된 객체에 대해 읽기 후 쓰기 정합성을 보장하고 객체 업데이트 및 헤드 작업에 대한 최종 일관성을 제공합니다. 성공적으로 완료된 PUT를 팔로우하면 새로 작성된 데이터를 읽을 수 있습니다. 기존 오브젝트, 메타데이터 업데이트 및 삭제를 덮어쓰는 것은 결국 일관성이 유지됩니다. 덮어쓰기는 일반적으로 전파되는 데 몇 초 또는 몇 분이 걸리지만 최대 15일이 소요될 수 있습니다.

또한 StorageGRID를 사용하면 컨테이너 단위로 일관성을 제어할 수 있습니다. 애플리케이션의 필요에 따라 일관성 제어를 변경하여 오브젝트의 가용성과 서로 다른 스토리지 노드 및 사이트 전체에서 오브젝트의 일관성 간의 균형을

유지할 수 있습니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

컨테이너 일관성 요청 가져오기

컨테이너 일관성 요청

Swift REST API 구축을 위한 권장 사항

StorageGRID와 함께 사용할 Swift REST API를 구현할 때는 다음 권장 사항을 따라야 합니다.

존재하지 않는 객체에 대한 헤드 권장 사항

응용 프로그램에서 개체가 실제로 존재하지 않을 것으로 예상되는 경로에 개체가 있는지 정기적으로 확인하는 경우 ""사용 가능한"" 일관성 제어를 사용해야 합니다. 예를 들어, 애플리케이션에서 해당 위치에 대한 PUT 작업을 수행하기 전에 헤드 작업을 수행하는 경우 ""사용 가능" 정합성 제어를 사용해야 합니다.

그렇지 않으면 헤드 작업에서 개체를 찾지 못할 경우 하나 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다.

Put container consistency request를 사용하여 각 컨테이너에 대해 ""사용 가능"" 정합성 제어를 설정할 수 있습니다.

오브젝트 이름에 대한 권장사항

StorageGRID 11.4 이상에서 생성된 컨테이너의 경우 성능 모범 사례에 맞게 개체 이름을 제한할 필요가 없습니다. 예를 들어, 이제 개체 이름의 처음 4개 문자에 임의의 값을 사용할 수 있습니다.

StorageGRID 11.4 이전 릴리즈에서 만든 컨테이너의 경우 개체 이름에 대한 다음 권장 사항을 계속 따릅니다.

- 개체 이름의 처음 네 문자로 임의 값을 사용하면 안 됩니다. 이는 이전 AWS에서 권장하는 이름 접두사와 다릅니다. 대신 "이미지"와 같은 비무작위, 고유하지 않은 접두사를 사용해야 합니다.
- 이전 AWS 권장 사항에 따라 이름 접두사에 랜덤 및 고유 문자를 사용하려면 오브젝트 이름에 디렉토리 이름을 접두사로 붙여야 합니다. 즉, 다음 형식을 사용합니다.

  ```
  mycontainer/mydir/f8e3-image3132.jpg
  ```

  이 형식 대신:

  ```
  mycontainer/f8e3-image3132.jpg
  ```

""범위 읽기" 권장 사항

저장된 객체 압축 * 옵션을 선택한 경우(* 구성 * > * 시스템 * > * 그리드 옵션 *) Swift 클라이언트 응용 프로그램은 바이트 범위를 지정하는 객체 가져오기 작업을 수행하지 않아야 합니다. 이러한 ""범위 읽기"" 작업은 StorageGRID가 요청된 바이트에 액세스하기 위해 개체의 압축을 효과적으로 해제해야 하기 때문에 비효율적입니다. 매우 큰 개체에서 작은 바이트 범위를 요청하는 Get Object 작업은 특히 비효율적입니다. 예를 들어, 50GB의 압축 개체에서 10MB

범위를 읽는 것은 매우 비효율적입니다.

압축된 개체에서 범위를 읽으면 클라이언트 요청이 시간 초과될 수 있습니다.

> 개체를 압축해야 하고 클라이언트 응용 프로그램에서 범위 읽기를 사용해야 하는 경우 응용 프로그램의 읽기 시간 초과를 늘리십시오.

관련 정보

컨테이너 일관성 요청 가져오기

컨테이너 일관성 요청

StorageGRID 관리

테넌트 계정 및 연결을 구성합니다

클라이언트 응용 프로그램에서 연결을 허용하도록 StorageGRID를 구성하려면 하나 이상의 테넌트 계정을 만들고 연결을 설정해야 합니다.

Swift 테넌트 계정을 생성하고 구성합니다

Swift API 클라이언트가 StorageGRID에 객체를 저장하고 검색하기 전에 Swift 테넌트 계정이 필요합니다. 각 테넌트 계정에는 고유한 계정 ID, 그룹 및 사용자, 컨테이너 및 객체가 있습니다.

Swift 테넌트 계정은 그리드 관리자 또는 그리드 관리 API를 사용하여 StorageGRID 그리드 관리자가 만듭니다.

Swift 테넌트 계정을 생성할 때 그리드 관리자는 다음 정보를 지정합니다.

- 테넌트의 표시 이름(테넌트의 계정 ID가 자동으로 할당되며 변경할 수 없음)
- 필요한 경우 테넌트 계정의 스토리지 할당량 — 테넌트의 객체에 사용할 수 있는 최대 GB, 테라바이트 또는 PB입니다. 테넌트의 스토리지 할당량은 물리적 크기(디스크 크기)가 아닌 논리적 양(오브젝트 크기)을 나타냅니다.
- StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하지 않는 경우 테넌트 계정이 자체 ID 소스를 사용할지 또는 그리드의 ID 소스를 공유할지 여부 및 테넌트의 로컬 루트 사용자의 초기 암호를 공유할지 여부
- SSO가 설정된 경우 테넌트 계정을 구성할 수 있는 루트 액세스 권한이 있는 통합 그룹이 있습니다.

Swift 테넌트 계정이 생성된 후 루트 액세스 권한이 있는 사용자는 테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 통합을 설정하고(ID 소스를 그리드와 공유하지 않는 경우) 로컬 그룹 및 사용자를 만듭니다
- 스토리지 사용량 모니터링

> Swift 사용자는 테넌트 관리자에 액세스하려면 루트 액세스 권한이 있어야 합니다. 그러나 루트 액세스 권한은 사용자가 Swift REST API에 인증하여 컨테이너를 생성하고 객체를 수집하는 것을 허용하지 않습니다. 사용자는 Swift REST API에 인증할 수 있는 Swift 관리자 권한이 있어야 합니다.

관련 정보

StorageGRID 관리

테넌트 계정을 사용합니다

지원되는 Swift API 엔드포인트

클라이언트 연결 구성 방법

그리드 관리자는 Swift 클라이언트가 StorageGRID에 연결하여 데이터를 저장 및 검색하는 방법에 영향을 주는 구성을 선택합니다. 연결에 필요한 특정 정보는 선택한 구성에 따라 다릅니다.

클라이언트 응용 프로그램은 다음 중 하나를 연결하여 개체를 저장하거나 검색할 수 있습니다.

- 관리 노드 또는 게이트웨이 노드의 부하 분산 서비스 또는 선택적으로 관리 노드 또는 게이트웨이 노드의 고가용성(HA) 그룹의 가상 IP 주소입니다
- 게이트웨이 노드의 CLB 서비스 또는 게이트웨이 노드의 고가용성 그룹의 가상 IP 주소(선택 사항)입니다

> CLB 서비스는 더 이상 사용되지 않습니다. StorageGRID 11.3 릴리스 전에 구성된 클라이언트는 게이트웨이 노드에서 CLB 서비스를 계속 사용할 수 있습니다. 로드 밸런싱을 제공하기 위해 StorageGRID에 의존하는 다른 모든 클라이언트 애플리케이션은 로드 밸런서 서비스를 사용하여 연결해야 합니다.

- 외부 로드 밸런서가 있거나 없는 스토리지 노드

StorageGRID를 구성할 때 그리드 관리자는 그리드 관리자 또는 그리드 관리 API를 사용하여 다음 단계를 수행할 수 있습니다. 이 모든 단계는 선택 사항입니다.

1. 로드 밸런서 서비스의 끝점을 구성합니다.

   로드 밸런서 서비스를 사용하려면 끝점을 구성해야 합니다. 관리 노드 또는 게이트웨이 노드의 부하 분산 서비스는 들어오는 네트워크 연결을 클라이언트 애플리케이션에서 스토리지 노드로 분산합니다. 로드 밸런서 끝점을 만들 때 StorageGRID 관리자는 포트 번호, 엔드포인트가 HTTP 또는 HTTPS 연결을 수락하는지 여부, 엔드포인트를 사용할 클라이언트 유형(S3 또는 Swift) 및 HTTPS 연결에 사용할 인증서(해당하는 경우)를 지정합니다.

2. 신뢰할 수 없는 클라이언트 네트워크를 구성합니다.

   StorageGRID 관리자가 노드의 클라이언트 네트워크를 신뢰할 수 없도록 구성하는 경우 노드는 로드 밸런서 끝점으로 명시적으로 구성된 포트의 클라이언트 네트워크에서 인바운드 연결만 허용합니다.

3. 고가용성 그룹을 구성합니다.

   관리자가 HA 그룹을 생성하면 여러 관리 노드 또는 게이트웨이 노드의 네트워크 인터페이스가 액티브-백업 구성에 배치됩니다. HA 그룹의 가상 IP 주소를 사용하여 클라이언트 연결이 이루어집니다.

각 옵션에 대한 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

요약: 클라이언트 연결을 위한 **IP** 주소 및 포트

클라이언트 애플리케이션은 그리드 노드의 IP 주소와 해당 노드의 서비스 포트 번호를 사용하여 StorageGRID에 접속합니다. HA(고가용성) 그룹이 구성되어 있는 경우 클라이언트 애플리케이션은 HA 그룹의 가상 IP 주소를 사용하여 연결할 수 있습니다.

클라이언트 연결을 만드는 데 필요한 정보입니다

이 표에는 클라이언트가 StorageGRID에 연결할 수 있는 다양한 방법과 각 연결 유형에 사용되는 IP 주소 및 포트가 요약되어 있습니다. 자세한 내용은 StorageGRID 관리자에게 문의하거나 StorageGRID 관리 지침 에서 그리드 관리자에서 이 정보를 찾는 방법에 대한 설명을 참조하십시오.

연결 위치	클라이언트가 연결하는 서비스입니다	**IP** 주소입니다	포트
HA 그룹	로드 밸런서	HA 그룹의 가상 IP 주소입니다	• 로드 밸런서 엔드포인트 포트
HA 그룹	CLB • 참고: * CLB 서비스는 더 이상 사용되지 않습니다.	HA 그룹의 가상 IP 주소입니다	기본 Swift 포트: • HTTPS: 8083 • HTTP: 8085
관리자 노드	로드 밸런서	관리 노드의 IP 주소입니다	• 로드 밸런서 엔드포인트 포트
게이트웨이 노드	로드 밸런서	게이트웨이 노드의 IP 주소입니다	• 로드 밸런서 엔드포인트 포트
게이트웨이 노드	CLB • 참고: * CLB 서비스는 더 이상 사용되지 않습니다.	게이트웨이 노드의 IP 주소입니다 • 참고: * 기본적으로 CLB 및 LDR용 HTTP 포트는 사용되지 않습니다.	기본 Swift 포트: • HTTPS: 8083 • HTTP: 8085
스토리지 노드	LDR	스토리지 노드의 IP 주소입니다	기본 Swift 포트: • HTTPS: 18083 • HTTP: 18085

예

Swift 클라이언트를 게이트웨이 노드 HA 그룹의 로드 밸런서 끝점에 연결하려면 아래와 같이 구조화된 URL을 사용합니다.

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

예를 들어 HA 그룹의 가상 IP 주소가 192.0.2.6이고 Swift 로드 밸런서 끝점의 포트 번호가 10444인 경우 Swift 클라이언트는 다음 URL을 사용하여 StorageGRID에 연결할 수 있습니다.

- 'https://192.0.2.6:10444`

클라이언트가 StorageGRID에 연결하는 데 사용하는 IP 주소에 대한 DNS 이름을 구성할 수 있습니다. 로컬 네트워크 관리자에게 문의하십시오.

HTTPS 또는 HTTP 연결을 사용하도록 결정합니다

로드 밸런서 끝점을 사용하여 클라이언트 연결을 만들 때는 해당 끝점에 지정된 프로토콜(HTTP 또는 HTTPS)을 사용하여 연결해야 합니다. 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 대한 클라이언트 연결에 HTTP를 사용하려면 해당 사용을 설정해야 합니다.

기본적으로 클라이언트 응용 프로그램이 게이트웨이 노드의 스토리지 노드 또는 CLB 서비스에 연결할 때는 모든 연결에 암호화된 HTTPS를 사용해야 합니다. 선택적으로 Grid Manager에서 * HTTP Connection * 그리드 사용 옵션을 선택하여 보안성이 떨어지는 HTTP 연결을 활성화할 수 있습니다. 예를 들어, 클라이언트 애플리케이션은 비운영 환경에서 스토리지 노드에 대한 접속을 테스트할 때 HTTP를 사용할 수 있습니다.

> 요청은 암호화되지 않은 상태로 전송되므로 프로덕션 그리드에 대해 HTTP를 설정할 때는 주의해야 합니다.

> CLB 서비스는 더 이상 사용되지 않습니다.

HTTP 연결 사용 * 옵션을 선택한 경우 클라이언트는 HTTPS에 사용하는 것과 다른 HTTP 포트를 사용해야 합니다. StorageGRID 관리 지침을 참조하십시오.

관련 정보

StorageGRID 관리

Swift API 구성에서 연결을 테스트합니다

Swift CLI를 사용하여 StorageGRID 시스템에 대한 연결을 테스트하고 시스템에 개체를 읽고 쓸 수 있는지 확인할 수 있습니다.

필요한 것

- Swift 명령줄 클라이언트인 python-swifftclient를 다운로드하여 설치해야 합니다.

  "SwiftStack:python-swiftclient"

- StorageGRID 시스템에 Swift 테넌트 계정이 있어야 합니다.

이 작업에 대해

보안을 구성하지 않은 경우 각 명령에 '--insecure' 플래그를 추가해야 합니다.

단계

1. StorageGRID Swift 배포에 대한 정보 URL 쿼리:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

   이는 Swift 배포가 제대로 작동하는지 테스트하는 데 충분합니다. 객체를 저장하여 계정 구성을 추가로 테스트하려면 추가 단계를 계속 진행합니다.

2. 컨테이너에 개체 넣기:

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. 컨테이너를 내려 개체를 확인합니다.

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. 개체 삭제:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. 컨테이너를 삭제합니다.

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

관련 정보

Swift 테넌트 계정을 생성하고 구성합니다

REST API에 대한 보안을 구성합니다

Swift REST API가 작업을 지원했습니다

StorageGRID 시스템은 OpenStack Swift API에서 대부분의 작업을 지원합니다. Swift REST

API 클라이언트를 StorageGRID와 통합하기 전에 계정, 컨테이너 및 오브젝트 작업에 대한 구현 세부 정보를 검토하십시오.

StorageGRID에서 지원되는 작업입니다

다음과 같은 Swift API 작업이 지원됩니다.

- 계정 작업
- 컨테이너 작업
- 오브젝트 작업

모든 작업에 대한 공통 응답 헤더입니다

StorageGRID 시스템은 OpenStack Swift 오브젝트 스토리지 API v1에 정의된 대로 지원되는 작업에 대해 모든 공통 헤더를 구현합니다.

관련 정보

"OpenStack: 오브젝트 스토리지 API"

지원되는 **Swift API** 엔드포인트

StorageGRID는 정보 URL, 인증 URL 및 스토리지 URL과 같은 Swift API 엔드포인트를 지원합니다.

정보 **URL**

/info 경로가 있는 Swift 기본 URL에 GET 요청을 실행하여 StorageGRID Swift 구현의 기능 및 제한 사항을 확인할 수 있습니다.

' https://*FQDN* | _ Node IP: Swift Port_/info/'

요청 시:

- '*FQDN*'은 정규화된 도메인 이름입니다.
- '*Node IP*'는 StorageGRID 네트워크의 스토리지 노드 또는 게이트웨이 노드에 대한 IP 주소입니다.
- '*Swift Port*'는 스토리지 노드 또는 게이트웨이 노드의 Swift API 연결에 사용되는 포트 번호입니다.

예를 들어 다음 정보 URL은 IP 주소가 10.99.106.103이고 포트 18083을 사용하는 스토리지 노드에서 정보를 요청합니다.

'https://10.99.106.103:18083/info/`

응답에는 JSON 사전으로서 Swift 구현의 기능이 포함됩니다. 클라이언트 도구는 JSON 응답을 구문 분석하여 구현 기능을 결정하고 후속 스토리지 작업의 제약 조건으로 사용할 수 있습니다.

Swift의 StorageGRID 구현을 통해 정보 URL에 대한 인증되지 않은 액세스가 가능합니다.

인증 URL

클라이언트는 Swift 인증 URL을 사용하여 테넌트 계정 사용자로 인증할 수 있습니다.

' https://*FQDN* | _ Node IP: Swift Port_/auth/v1.0/'

다음과 같이 X-Auth-User와 X-Auth-Key 요청 헤더의 매개 변수로 테넌트 계정 ID, 사용자 이름 및 암호를 제공해야 합니다.

'X-Auth-User:_Tenant_Account_ID: Username _'

'X-Auth-Key:_Password_'

요청 헤더에서:

- `*Tenant_Account_ID*'는 Swift 테넌트가 생성될 때 StorageGRID에서 할당한 계정 ID입니다. 테넌트 관리자 로그인 페이지에서 사용되는 것과 동일한 테넌트 계정 ID입니다.
- '*Username*'은 테넌트 관리자에서 생성된 테넌트 사용자의 이름입니다. 이 사용자는 Swift 관리자 권한이 있는 그룹에 속해야 합니다. 테넌트의 루트 사용자는 Swift REST API를 사용하도록 구성할 수 없습니다.

  테넌트 계정에 대해 ID 페더레이션을 사용하도록 설정한 경우 LDAP 서버에서 연결된 사용자의 사용자 이름과 암호를 입력합니다. 또는 LDAP 사용자의 도메인 이름을 제공합니다. 예를 들면 다음과 같습니다.

  'X-Auth-User:_Tenant_Account_ID: 사용자 이름@Domain_Name_'

- '*Password*'는 테넌트 사용자의 암호입니다. 사용자 암호는 테넌트 관리자에서 생성 및 관리됩니다.

인증 요청에 대한 응답은 다음과 같이 스토리지 URL 및 인증 토큰을 반환합니다.

'X-Storage-URL: https://FQDN |Node_IP:Swift_Port/v1/Tenant_Account_ID'

'X-Auth-Token:_token_'

'X-Storage-Token:_token_'

기본적으로 토큰은 생성 후 24시간 동안 유효합니다.

특정 테넌트 계정에 대해 토큰이 생성됩니다. 한 계정에 대해 유효한 토큰이 사용자에게 다른 계정에 액세스할 수 있는 권한을 부여하지 않습니다.

스토리지 URL입니다

클라이언트 애플리케이션은 Swift REST API 호출을 실행하여 게이트웨이 노드 또는 스토리지 노드에 대해 지원되는 계정, 컨테이너 및 오브젝트 작업을 수행할 수 있습니다. 저장소 요청은 인증 응답에서 반환된 저장소 URL로 처리됩니다. 또한 요청에는 인증 요청에서 반환된 X-Auth-Token 헤더 및 값이 포함되어야 합니다.

'https://FQDN |*IP:Swift_Port*/v1/*Tenant_Account_ID*'

'[*/container*][*/object*]'

'X-Auth-Token:_token_'

사용 통계를 포함하는 일부 스토리지 응답 헤더는 최근에 수정된 개체의 정확한 숫자를 반영하지 않을 수 있습니다. 이

머리글에 정확한 숫자가 표시되려면 몇 분 정도 걸릴 수 있습니다.

계정 및 컨테이너 작업에 대한 다음 응답 머리글은 사용 통계를 포함하는 응답의 예입니다.

- X-Account-Bytes-Used
- X-Account-Object-Count'입니다
- X-Container-Bytes-Used(X-Container-Bytes-Used)
- X-Container-Object-Count

관련 정보

테넌트 계정 및 연결을 구성합니다

계정 작업

컨테이너 작업

오브젝트 작업

계정 작업

다음 Swift API 작업은 어카운트에 대해 수행됩니다.

계정을 가져옵니다

이 작업은 계정 및 계정 사용 통계와 연결된 컨테이너 목록을 검색합니다.

다음 요청 매개 변수가 필요합니다.

- '계정'입니다

다음 요청 헤더가 필요합니다.

- X-Auth-Token

다음과 같은 지원되는 요청 쿼리 매개 변수는 선택 사항입니다.

- "암월터"
- 'End_marker'입니다
- 형식
- 제한
- '마커'
- 접두사

계정이 발견되어 컨테이너가 없거나 컨테이너 목록이 비어 있는 경우 "HTTP/1.1 204 컨텐츠 없음" 응답이 있는 다음 헤더가 성공적으로 실행되면 "HTTP/1.1 200 OK" 응답이 반환됩니다. 계정이 발견되어 컨테이너 목록이 비어 있지 않은 경우 "HTTP/1.1 200 OK" 응답이 반환됩니다.

- '수용 범위'

- 콘텐츠 길이
- 콘텐츠 유형
- 다
- X-Account-Bytes-Used
- X-계정-컨테이너-카운트
- X-Account-Object-Count'입니다
- X-타임스탬프
- X-Trans-ID

머리 계정

이 작업은 Swift 계정에서 계정 정보 및 통계를 검색합니다.

다음 요청 매개 변수가 필요합니다.

- '계정'입니다

다음 요청 헤더가 필요합니다.

- X-Auth-Token

성공적으로 실행하면 ""HTTP/1.1 204 컨텐츠 없음" 응답이 있는 다음 헤더가 반환됩니다.

- '수용 범위'
- 콘텐츠 길이
- 다
- X-Account-Bytes-Used
- X-계정-컨테이너-카운트
- X-Account-Object-Count'입니다
- X-타임스탬프
- X-Trans-ID

관련 정보

운영 모니터링 및 감사

컨테이너 작업

StorageGRID는 Swift 계정당 최대 1,000개의 컨테이너를 지원합니다. 컨테이너에서 다음과 같은 Swift API 작업이 수행됩니다.

컨테이너를 삭제합니다

이 작업을 수행하면 StorageGRID 시스템의 Swift 계정에서 빈 컨테이너가 제거됩니다.

다음 요청 매개 변수가 필요합니다.

- '계정'입니다
- 컨테이너

다음 요청 헤더가 필요합니다.

- X-Auth-Token

성공적으로 실행하면 "HTTP/1.1 204 컨텐츠 없음" 응답이 있는 다음 헤더가 반환됩니다.

- 콘텐츠 길이
- 콘텐츠 유형
- 다
- X-Trans-ID

컨테이너를 가져옵니다

이 작업은 StorageGRID 시스템의 컨테이너 통계 및 메타데이터와 함께 컨테이너와 연결된 개체 목록을 검색합니다.

다음 요청 매개 변수가 필요합니다.

- '계정'입니다
- 컨테이너

다음 요청 헤더가 필요합니다.

- X-Auth-Token

다음과 같은 지원되는 요청 쿼리 매개 변수는 선택 사항입니다.

- "암월터"
- 'End_marker'입니다
- 형식
- 제한
- '마커'
- "경로"
- 접두사

성공적으로 실행하면 "HTTP/1.1 200 Success" 또는 "HTTP/1.1 204 No Content" 응답으로 다음 헤더가 반환됩니다.

- '수용 범위'
- 콘텐츠 길이
- 콘텐츠 유형
- 다
- X-Container-Bytes-Used(X-Container-Bytes-Used)

- X-Container-Object-Count
- X-타임스탬프
- X-Trans-ID

헤드 컨테이너

이 작업은 StorageGRID 시스템에서 컨테이너 통계 및 메타데이터를 검색합니다.

다음 요청 매개 변수가 필요합니다.

- '계정'입니다
- 컨테이너

다음 요청 헤더가 필요합니다.

- X-Auth-Token

성공적으로 실행하면 "HTTP/1.1 204 컨텐츠 없음" 응답이 있는 다음 헤더가 반환됩니다.

- '수용 범위'
- 콘텐츠 길이
- 다
- X-Container-Bytes-Used(X-Container-Bytes-Used)
- X-Container-Object-Count
- X-타임스탬프
- X-Trans-ID

용기를 놓습니다

이 작업은 StorageGRID 시스템의 계정에 대한 컨테이너를 만듭니다.

다음 요청 매개 변수가 필요합니다.

- '계정'입니다
- 컨테이너

다음 요청 헤더가 필요합니다.

- X-Auth-Token

성공적으로 실행하면 "HTTP/1.1 201 Created" 또는 "HTTP/1.1 202 Accepted"(컨테이너가 이미 이 계정에 있는 경우) 응답으로 다음 헤더가 반환됩니다.

- 콘텐츠 길이
- 다
- X-타임스탬프

- X-Trans-ID

컨테이너 이름은 StorageGRID 네임스페이스에서 고유해야 합니다. 컨테이너가 다른 계정 아래에 있는 경우 "HTTP/1.1 409 충돌"이라는 헤더가 반환됩니다.

관련 정보

운영 모니터링 및 감사

오브젝트 작업

객체에 대해 다음과 같은 Swift API 작업이 수행됩니다.

개체를 삭제합니다

이 작업은 StorageGRID 시스템에서 개체의 콘텐츠 및 메타데이터를 삭제합니다.

다음 요청 매개 변수가 필요합니다.

- '계정'입니다
- 컨테이너
- '개체'

다음 요청 헤더가 필요합니다.

- X-Auth-Token

성공적으로 실행하면 HTTP/1.1 204 No Content 응답이 있는 다음 응답 헤더가 반환됩니다.

- 콘텐츠 길이
- 콘텐츠 유형
- 다
- X-Trans-ID

오브젝트 삭제 요청을 처리할 때 StorageGRID는 저장된 모든 위치에서 오브젝트의 모든 복사본을 즉시 제거하려고 시도합니다. 성공하면 StorageGRID는 즉시 클라이언트에 응답을 반환합니다. 위치를 일시적으로 사용할 수 없기 때문에 30초 이내에 모든 복사본을 제거할 수 없는 경우 StorageGRID는 제거할 복사본을 대기시킨 다음 클라이언트에 성공 여부를 표시합니다.

개체 삭제 방법에 대한 자세한 내용은 정보 수명 주기 관리를 사용하여 개체 관리 지침을 참조하십시오.

객체를 가져옵니다

이 작업은 개체 콘텐츠를 검색하고 StorageGRID 시스템에서 개체 메타데이터를 가져옵니다.

다음 요청 매개 변수가 필요합니다.

- '계정'입니다
- 컨테이너
- '개체'

다음 요청 헤더가 필요합니다.

- X-Auth-Token

다음 요청 헤더는 선택 사항입니다.

- 인코딩 수락
- IF-MATCH
- If-Modified-Since
- "If-None-Match"
- "수정되지 않은 경우 - 이후"
- "범위"

성공적으로 실행하면 HTTP/1.1 200 OK 응답이 있는 다음 헤더가 반환됩니다.

- '수용 범위'
- Content-Disposition은 Content-Disposition 메타데이터가 설정된 경우에만 반환됩니다
- Content-Encoding은 Content-Encoding 메타데이터가 설정된 경우에만 반환됩니다
- 콘텐츠 길이
- 콘텐츠 유형
- 다
- 'ETag'
- 마지막 수정일
- X-타임스탬프
- X-Trans-ID

머리 물체

이 작업은 StorageGRID 시스템에서 수집된 개체의 메타데이터 및 속성을 검색합니다.

다음 요청 매개 변수가 필요합니다.

- '계정'입니다
- 컨테이너
- '개체'

다음 요청 헤더가 필요합니다.

- X-Auth-Token

성공적으로 실행하면 "HTTP/1.1 200 OK" 응답과 함께 다음 헤더가 반환됩니다.

- '수용 범위'
- Content-Disposition은 Content-Disposition 메타데이터가 설정된 경우에만 반환됩니다

- Content-Encoding은 Content-Encoding 메타데이터가 설정된 경우에만 반환됩니다
- 콘텐츠 길이
- 콘텐츠 유형
- 다
- 'ETag'
- 마지막 수정일
- X-타임스탬프
- X-Trans-ID

개체를 넣습니다

이 작업을 실행하면 새 개체가 데이터와 메타데이터로 만들어지거나 기존 개체를 StorageGRID 시스템의 데이터 및 메타데이터로 바꿉니다.

StorageGRID는 최대 5TiB(5,497,558,138,880바이트)의 오브젝트를 지원합니다.

> 동일한 키에 쓰는 두 클라이언트 등의 충돌하는 클라이언트 요청은 "최신 성공" 기준으로 해결됩니다. "최신" 평가 시기는 StorageGRID 시스템이 지정된 요청을 완료하는 시점을 기준으로 하며, Swift 클라이언트가 작업을 시작하는 시점이 아닙니다.

다음 요청 매개 변수가 필요합니다.

- '계정'입니다
- 컨테이너
- '개체'

다음 요청 헤더가 필요합니다.

- X-Auth-Token

다음 요청 헤더는 선택 사항입니다.

- 'Content-Disposition'
- 콘텐츠 인코딩

  개체에 적용되는 ILM 규칙이 크기에 따라 개체를 필터링하고 수집 시 동기식 배치(Ingest 동작에 대한 균형 또는 엄격 옵션)를 사용하는 경우 청크된 "콘텐츠 인코딩"을 사용하지 마십시오.

- 전송 인코딩

  개체에 적용되는 ILM 규칙이 크기에 따라 개체를 필터링하고 수집 시 동기식 배치(Ingest 동작에 대한 균형 또는 엄격 옵션)를 사용하는 경우 압축 또는 청크된 "전송 인코딩"을 사용하지 마십시오.

- 콘텐츠 길이

  ILM 규칙이 크기를 기준으로 오브젝트를 필터링하고 수집 시 동기 배치를 사용하는 경우 'Content-Length'를 지정해야 합니다.

> Content-Encoding, Transfer-Encoding, Content-Length에 대한 지침을 따르지 않을 경우 StorageGRID는 개체 크기를 결정하고 ILM 규칙을 적용하기 전에 개체를 저장해야 합니다. 다시 말해, StorageGRID은 수집 중인 오브젝트의 중간 복사본을 기본적으로 생성해야 합니다. 즉, StorageGRID는 Ingest 동작에 대해 이중 커밋 옵션을 사용해야 합니다.

동기 배치 및 ILM 규칙에 대한 자세한 내용은 정보 수명 주기 관리를 통해 개체 관리 지침을 참조하십시오.

- 콘텐츠 유형
- 'ETag'
- 'X-Object-Meta-<name\>'(객체 관련 메타데이터)

  ILM 규칙의 참조 시간으로 * 사용자 정의 작성 시간 * 옵션을 사용하려면 값을 사용자 정의 헤더("X-Object-Meta-Creation-Time")에 저장해야 합니다. 예를 들면 다음과 같습니다.

  ```
  X-Object-Meta-Creation-Time: 1443399726
  ```

  이 필드는 1970년 1월 1일 이후 초 단위로 평가됩니다.

- X-Storage-Class: reduced_redundancy가 있습니다

  수집된 개체와 일치하는 ILM 규칙이 이중 커밋 또는 균형 설정의 수집 동작을 지정하는 경우 이 헤더는 StorageGRID에서 만드는 개체 복사본 수에 영향을 줍니다.

  - * 이중 커밋 *: ILM 규칙이 Ingest 동작에 대한 이중 커밋 옵션을 지정하는 경우 StorageGRID는 오브젝트가 수집될 때(단일 커밋) 단일 임시 복사본을 만듭니다.
  - * 균형 *: ILM 규칙이 균형 옵션을 지정하는 경우 StorageGRID은 시스템에서 규칙에 지정된 모든 사본을 즉시 만들 수 없는 경우에만 단일 중간 복사본을 만듭니다. StorageGRID에서 동기 배치를 수행할 수 있는 경우 이 머리글은 영향을 주지 않습니다.

    reducted_redundancy' 헤더는 개체와 일치하는 ILM 규칙이 복제된 단일 복사본을 만들 때 가장 적합합니다. 이 경우 'REDED_READITORY'를 사용하면 모든 수집 작업에 대해 불필요한 오브젝트 복사본을 생성하고 삭제할 필요가 없습니다.

    다른 상황에서는 수집 중에 오브젝트 데이터가 손실될 위험이 있기 때문에 reducted_redundancy" 헤더를 사용하지 않는 것이 좋습니다. 예를 들어, ILM 평가가 발생하기 전에 실패한 스토리지 노드에 단일 복사본이 처음 저장되는 경우 데이터가 손실될 수 있습니다.

    > 복제된 복사본이 항상 하나만 있으면 데이터가 영구적으로 손실될 위험이 있습니다. 복제된 객체 복제본이 하나만 있는 경우 스토리지 노드에 장애가 발생하거나 심각한 오류가 발생한 경우 해당 객체가 손실됩니다. 또한 업그레이드와 같은 유지보수 절차 중에는 개체에 대한 액세스가 일시적으로 중단됩니다.

  reducted_redundancy를 지정하면 개체를 처음 인제스트할 때 생성되는 복사본 수에만 영향을 줍니다. 활성 ILM 정책에 따라 개체를 평가할 때 개체의 복사본 수에 영향을 주지 않으며 StorageGRID 시스템의 낮은 수준의 중복성에 데이터가 저장되지 않습니다.

성공적으로 실행하면 "HTTP/1.1 201 created" 응답으로 다음 헤더가 반환됩니다.

- 콘텐츠 길이
- 콘텐츠 유형
- 다
- 'ETag'
- 마지막 수정일
- X-Trans-ID

관련 정보

ILM을 사용하여 개체를 관리합니다

운영 모니터링 및 감사

옵션 요청

옵션 요청은 개별 Swift 서비스의 사용 가능 여부를 확인합니다. 옵션 요청은 URL에 지정된 스토리지 노드 또는 게이트웨이 노드에 의해 처리됩니다.

옵션 방법입니다

예를 들어, 클라이언트 애플리케이션은 스토리지 노드의 Swift 인증 자격 증명을 제공하지 않고 스토리지 노드의 Swift 포트에 대한 옵션 요청을 발급하여 스토리지 노드를 사용할 수 있는지 여부를 확인할 수 있습니다. 이 요청을 사용하여 스토리지 노드가 다운된 시점을 모니터링하거나 외부 로드 밸런서가 식별하도록 할 수 있습니다.

info URL 또는 저장소 URL과 함께 사용할 경우 options 메서드는 지정된 URL에 대해 지원되는 동사 목록(예: head, get, options 및 put)을 반환합니다. 옵션 방법은 인증 URL과 함께 사용할 수 없습니다.

다음 요청 매개 변수가 필요합니다.

- '계정'입니다

다음 요청 매개 변수는 선택 사항입니다.

- 컨테이너
- '개체'

성공적으로 실행하면 HTTP/1.1 204 컨텐츠 없음 응답이 있는 다음 헤더가 반환됩니다. 스토리지 URL에 대한 옵션 요청에는 타겟이 없을 필요가 없습니다.

- "Allow"(지정된 URL에 대해 지원되는 동사 목록, 예: head, get, options, 및 PUT)
- 콘텐츠 길이
- 콘텐츠 유형
- 다
- X-Trans-ID

관련 정보

지원되는 Swift API 엔드포인트

Swift API 작업에 대한 오류 응답

가능한 오류 응답을 이해하면 작업 문제를 해결하는 데 도움이 됩니다.

작업 중에 오류가 발생하면 다음 HTTP 상태 코드가 반환될 수 있습니다.

SWIFT 오류 이름	**HTTP** 상태입니다
AccountNameTooLong, ContainerNameTooLong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameTooLong, MetadataValueTooBig, MissingSecurityHeader, ObjectNameTooLong, TooManyContainers, TooManyMetadataItems, TotalMetadataTooLarge입니다	400 잘못된 요청
액세스가 거부되었습니다	403 사용 금지
ContainerNotEmpty , ContainerAlreadyExists	409 충돌
내부 오류입니다	500 내부 서버 오류입니다
InvalidRange 를 선택합니다	416 요청된 범위가 충분하지 않습니다
MethodNotAllowed 를 참조하십시오	405 메서드를 사용할 수 없습니다
MissingContentLength를 참조하십시오	411 길이 필요
지원되지 않습니다	404를 찾을 수 없습니다
구현되지 않았습니다	501 구현되지 않음
사전 조건에 실패했습니다	412 전제 조건 실패
리소스 NotFound 를 참조하십시오	404를 찾을 수 없습니다
권한이 없습니다	401 승인되지 않음
UnprocessableEntity입니다	422 처리할 수 없는 엔터티

StorageGRID Swift REST API 작업

StorageGRID 시스템별 Swift REST API에 작업이 추가됩니다.

컨테이너 일관성 요청 가져오기

정합성 보장 레벨은 오브젝트의 가용성과 서로 다른 스토리지 노드 및 사이트에서 이러한 오브젝트의 일관성 간의 균형을 제공합니다. 컨테이너 일관성 가져오기 요청을 사용하면 특정 컨테이너에 적용되는 일관성 수준을 확인할 수 있습니다.

요청하십시오

HTTP 헤더를 요청합니다	설명
X-Auth-Token	요청에 사용할 계정의 Swift 인증 토큰을 지정합니다.
'x-ntap-sg-consistency'	요청 유형을 지정합니다. 여기서 true는 컨테이너 일관성을 얻고 false는 컨테이너를 가져옵니다.
호스트	요청이 전달되는 호스트 이름입니다.

요청 예

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

응답

응답 **HTTP** 헤더	설명
다	응답의 날짜 및 시간입니다.
'연결'을 선택합니다	서버에 대한 연결이 열려 있는지 또는 닫혀 있는지 여부
X-Trans-ID	요청에 대한 고유한 트랜잭션 식별자입니다.
콘텐츠 길이	응답 바디의 길이.

응답 **HTTP** 헤더	설명
'x-ntap-sg-consistency'	컨테이너에 적용되는 정합성 보장 제어 레벨입니다. 지원되는 값은 다음과 같습니다. • * ALL *: 모든 노드가 데이터를 즉시 수신하거나 요청이 실패합니다. • * strong-global *: 모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다. • * strong-site *: 사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다. • * read-after-new-write *: 새 객체에 대한 읽기 후 쓰기 정합성을 보장하고 객체 업데이트에 대한 최종 일관성을 제공합니다. 고가용성 및 데이터 보호 보장 제공 • 참고 *: 응용 프로그램이 존재하지 않는 개체에 대한 헤드 요청을 사용하는 경우 하나 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다. 이러한 오류를 방지하려면 "사용 가능" 수준을 사용하십시오. • * Available * (헤드 작업의 최종 일관성): "read-after-new-write" 정합성 수준과 동일하게 동작하지만 헤드 작업에 대한 최종 정합성 보장만 제공합니다. 스토리지 노드를 사용할 수 없는 경우 "새 쓰기 후"보다 헤드 작업에 더 높은 가용성을 제공합니다.

응답 예

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

관련 정보

테넌트 계정을 사용합니다

컨테이너 일관성 요청

저장 컨테이너 일관성 요청을 사용하면 컨테이너에서 수행된 작업에 적용할 일관성 수준을 지정할 수 있습니다. 기본적으로 새 컨테이너는 "새 쓰기 후 다시 쓰기" 일관성 수준을 사용하여 생성됩니다.

요청하십시오

HTTP 헤더를 요청합니다	설명
X-Auth-Token	요청에 사용할 계정의 Swift 인증 토큰입니다.
'x-ntap-sg-consistency'	컨테이너의 작업에 적용할 일관성 제어 수준입니다. 지원되는 값은 다음과 같습니다. • * ALL *: 모든 노드가 데이터를 즉시 수신하거나 요청이 실패합니다. • * strong-global *: 모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다. • * strong-site *: 사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다. • * read-after-new-write *: 새 객체에 대한 읽기 후 쓰기 정합성을 보장하고 객체 업데이트에 대한 최종 일관성을 제공합니다. 고가용성 및 데이터 보호 보장 제공 • 참고 *: 응용 프로그램이 존재하지 않는 개체에 대한 헤드 요청을 사용하는 경우 하나 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다. 이러한 오류를 방지하려면 "사용 가능" 수준을 사용하십시오. • * Available * (헤드 작업의 최종 일관성): "read-after-new-write" 정합성 수준과 동일하게 동작하지만 헤드 작업에 대한 최종 정합성 보장만 제공합니다. 스토리지 노드를 사용할 수 없는 경우 "새 쓰기 후"보다 헤드 작업에 더 높은 가용성을 제공합니다.
호스트	요청이 전달되는 호스트 이름입니다.

일관성 제어 및 **ILM** 규칙이 상호 작용하여 데이터 보호에 영향을 미치는 방식

일관성 제어와 ILM 규칙 모두 오브젝트의 보호 방법에 영향을 미칩니다. 이러한 설정은 상호 작용할 수 있습니다.

예를 들어, 개체가 저장될 때 사용되는 일관성 컨트롤은 오브젝트 메타데이터의 초기 배치에 영향을 미치는 반면 ILM 규칙에 대해 선택된 수집 동작은 오브젝트 복사본의 초기 배치에 영향을 줍니다. StorageGRID에서는 클라이언트 요청을 이행하기 위해 오브젝트의 메타데이터와 해당 데이터에 모두 액세스해야 하므로 일관성 수준과 수집 동작에 적합한 보호 수준을 선택하면 초기 데이터 보호 수준을 높이고 시스템 응답을 더욱 정확하게 예측할 수 있습니다.

ILM 규칙에 대해 다음과 같은 수집 동작을 사용할 수 있습니다.

- * Strict * : ILM 규칙에 지정된 모든 사본은 클라이언트에 반환되기 전에 만들어야 합니다.
- * 균형 *: StorageGRID는 수집 시 ILM 규칙에 지정된 모든 복제본을 생성하려고 합니다. 그렇지 않을 경우 중간 복사본이 만들어지고 클라이언트에 성공적으로 반환됩니다. ILM 규칙에 지정된 복사본은 가능한 경우 만들어집니다.
- * 이중 커밋*: StorageGRID는 즉시 개체의 임시 복사본을 만들고 클라이언트에 성공을 반환합니다. ILM 규칙에 지정된 복사본은 가능한 경우 만들어집니다.

ILM 규칙의 수집 동작을 선택하기 전에 정보 수명 주기 관리를 통해 개체를 관리하기 위한 지침에서 이러한 설정에 대한 전체 설명을 읽어보십시오.

일관성 제어 및 **ILM** 규칙이 상호 작용하는 방법의 예

다음 ILM 규칙 및 다음 일관성 수준 설정이 있는 두 사이트 그리드가 있다고 가정합니다.

- * ILM 규칙 *: 로컬 사이트와 원격 사이트에 각각 하나씩, 두 개의 오브젝트 복사본을 만듭니다. Strict 수집 동작이 선택됩니다.
- * Consistency level *: "trong-global"(개체 메타데이터가 모든 사이트에 즉시 배포됩니다.)

클라이언트가 오브젝트를 그리드에 저장할 때 StorageGRID는 오브젝트 복사본을 둘 다 만들고 메타데이터를 두 사이트에 분산한 다음 클라이언트에 성공을 반환합니다.

수집 성공 메시지가 표시된 시점에 객체가 손실로부터 완벽하게 보호됩니다. 예를 들어, 수집 직후 로컬 사이트가 손실되면 오브젝트 데이터와 오브젝트 메타데이터의 복사본이 원격 사이트에 계속 존재합니다. 개체를 완전히 검색할 수 있습니다.

대신 동일한 ILM 규칙 및 "'strong-site' 정합성 보장 수준을 사용한 경우 객체 데이터가 원격 사이트에 복제되었지만 객체 메타데이터가 그 위치에 배포되기 전에 클라이언트에 성공 메시지가 표시될 수 있습니다. 이 경우 오브젝트 메타데이터의 보호 수준이 오브젝트 데이터의 보호 수준과 일치하지 않습니다. 수집 후 곧바로 로컬 사이트가 손실되면 오브젝트 메타데이터가 손실됩니다. 객체를 검색할 수 없습니다.

일관성 수준과 ILM 규칙 간의 상호 관계는 복잡할 수 있습니다. 도움이 필요한 경우 NetApp에 문의하십시오.

요청 예

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

응답

응답 **HTTP** 헤더	설명
다	응답의 날짜 및 시간입니다.
'연결'을 선택합니다	서버에 대한 연결이 열려 있는지 또는 닫혀 있는지 여부
X-Trans-ID	요청에 대한 고유한 트랜잭션 식별자입니다.
콘텐츠 길이	응답 바디의 길이.

응답 예

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

관련 정보

테넌트 계정을 사용합니다

REST API에 대한 보안을 구성합니다

REST API에 대해 구현된 보안 조치를 검토하고 시스템 보안 방법을 이해해야 합니다.

StorageGRID에서 REST API에 대한 보안을 제공하는 방법

StorageGRID 시스템이 REST API에 대한 보안, 인증 및 권한 부여를 구현하는 방법을 이해해야 합니다.

StorageGRID는 다음과 같은 보안 조치를 사용합니다.

- 로드 밸런서 끝점에 HTTPS가 구성되어 있는 경우 로드 밸런서 서비스와의 클라이언트 통신은 HTTPS를 사용합니다.

  로드 밸런서 끝점을 구성할 때 HTTP를 선택적으로 활성화할 수 있습니다. 예를 들어, 테스트 또는 기타 비운영 목적으로 HTTP를 사용할 수 있습니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

- 기본적으로 StorageGRID는 게이트웨이 노드에서 스토리지 노드 및 CLB 서비스와의 클라이언트 통신에 HTTPS를 사용합니다.

  이러한 연결에 대해 HTTP를 선택적으로 활성화할 수 있습니다. 예를 들어, 테스트 또는 기타 비운영 목적으로 HTTP를 사용할 수 있습니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

  > CLB 서비스는 더 이상 사용되지 않습니다.

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

보안 인증서 및 클라이언트 응용 프로그램

클라이언트는 게이트웨이 노드 또는 관리 노드의 부하 분산 서비스, 스토리지 노드 또는 게이트웨이 노드의 더 이상 사용되지 않는 CLB 서비스에 직접 연결할 수 있습니다.

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

- 클라이언트 응용 프로그램이 로드 밸런서 서비스에 연결되면 연결을 만드는 데 사용되는 특정 로드 밸런서 끝점에 대해 구성된 인증서를 사용합니다. 각 끝점마다 고유한 인증서가 있습니다. 이 인증서는 그리드 관리자가 업로드한

사용자 지정 서버 인증서이거나, 끝점 구성 시 그리드 관리자가 StorageGRID에서 생성한 인증서입니다.

- 클라이언트 응용 프로그램이 게이트웨이 노드의 스토리지 노드 또는 CLB 서비스에 직접 연결할 때 StorageGRID 시스템이 설치될 때 스토리지 노드에 대해 생성된 시스템 생성 서버 인증서(시스템 인증 기관이 서명)를 사용합니다. 또는 그리드 관리자가 그리드에 제공하는 단일 사용자 정의 서버 인증서입니다.

클라이언트가 TLS 연결을 설정하는 데 사용하는 인증서를 신뢰하도록 구성해야 합니다.

로드 밸런서 끝점 구성에 대한 정보와 TLS 연결에 대한 단일 사용자 지정 서버 인증서를 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 직접 추가하는 방법에 대한 지침은 StorageGRID 관리 지침을 참조하십시오.

요약

다음 표에서는 S3 및 Swift REST API에서 보안 문제가 구현되는 방식을 보여 줍니다.

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

관련 정보

StorageGRID 관리

TLS 라이브러리에 대해 지원되는 해시 및 암호화 알고리즘

StorageGRID 시스템은 TLS(전송 계층 보안) 세션을 설정할 때 클라이언트 응용 프로그램에서 사용할 수 있는 제한된 암호화 그룹 세트를 지원합니다.

지원되는 **TLS** 버전입니다

StorageGRID는 TLS 1.2 및 TLS 1.3을 지원합니다.

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

지원되는 암호 그룹

TLS 버전입니다	암호화 그룹의 **IANA** 이름입니다
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS 버전입니다	암호화 그룹의 **IANA** 이름입니다
TLS_ECDHE_RSA_WITH_CHACH20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
TLS_CHACH20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

더 이상 사용되지 않는 암호화 그룹

다음 암호화 그룹은 더 이상 사용되지 않습니다. 이러한 암호화에 대한 지원은 이후 릴리스에서 제거됩니다.

IANA 이름입니다
TLS_RSA_with_AES_128_GCM_SHA256
TLS_RSA_WITED_AES_256_GCM_SHA384

관련 정보

테넌트 계정 및 연결을 구성합니다

운영 모니터링 및 감사

전체 그리드 또는 특정 노드에 대한 트랜잭션 추세를 확인하여 클라이언트 작업의 워크로드 및 효율성을 모니터링할 수 있습니다. 감사 메시지를 사용하여 클라이언트 작업 및 트랜잭션을 모니터링할 수 있습니다.

오브젝트 수집 및 검색 속도 모니터링

오브젝트 수집 및 검색 속도와 오브젝트 수, 쿼리, 검증을 위한 메트릭을 모니터링할 수 있습니다. 클라이언트 응용 프로그램이 StorageGRID 시스템에서 개체를 읽고, 쓰고, 수정하는 데 성공한 시도 및 실패한 시도 횟수를 볼 수 있습니다.

단계

1. 를 사용하여 Grid Manager에 로그인합니다 지원되는 웹 브라우저.
2. Dashboard에서 Protocol Operations 섹션을 찾습니다.

   이 섹션에서는 StorageGRID 시스템에서 수행하는 클라이언트 작업의 수를 요약합니다. 프로토콜 속도는 최근 2분 동안의 평균값입니다.

3. 노드 * 를 선택합니다.
4. 노드 홈 페이지(배포 수준)에서 * 로드 밸런서 * 탭을 클릭합니다.

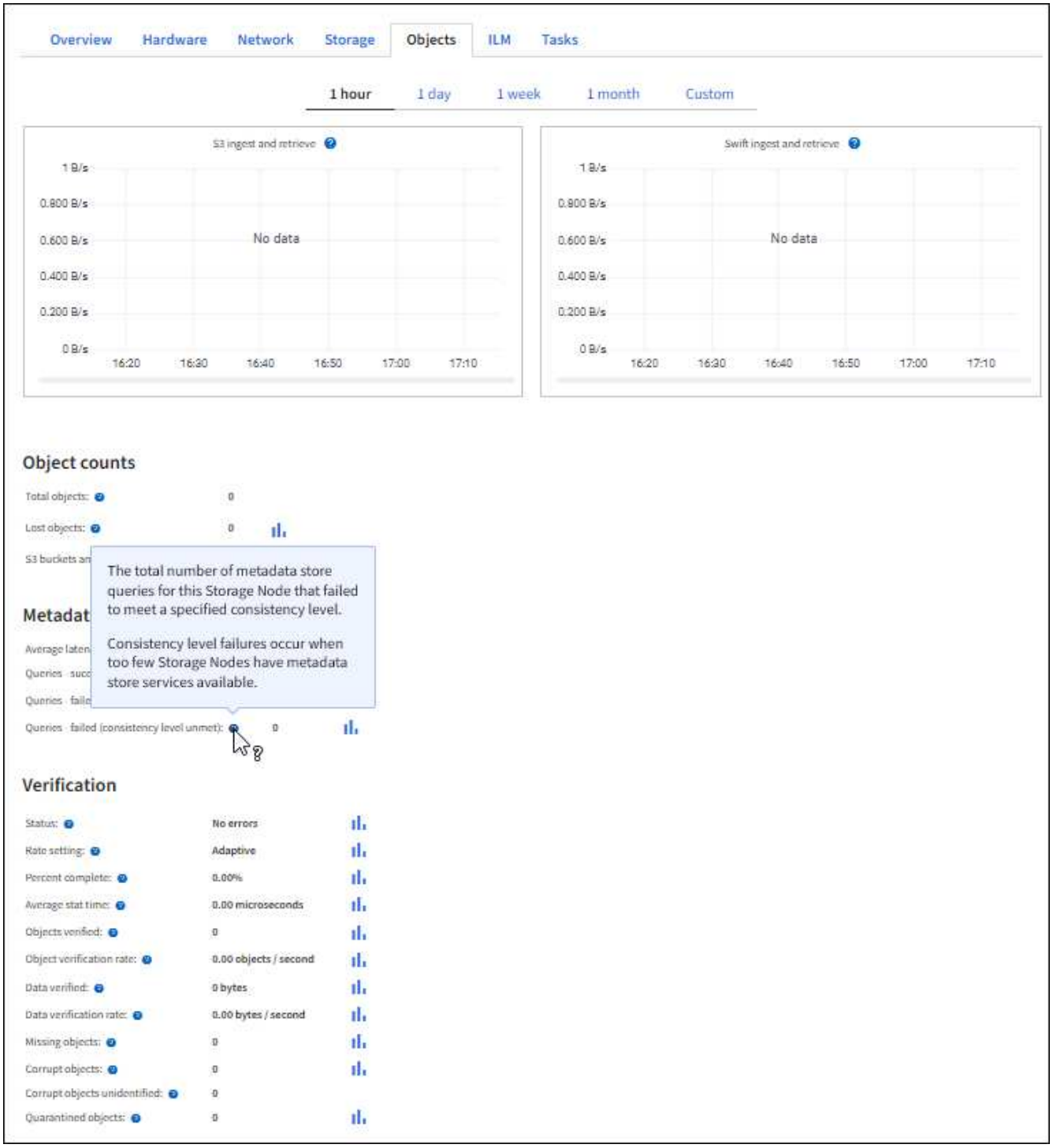
   차트에는 그리드 내의 로드 밸런서 끝점에 대한 모든 클라이언트 트래픽에 대한 추세가 표시됩니다. 시간 간격(시간, 일, 주, 월 또는 년)을 선택할 수 있습니다. 또는 사용자 지정 간격을 적용할 수 있습니다.

5. 노드 홈 페이지(배포 수준)에서 * 개체 * 탭을 클릭합니다.

   이 차트에는 전체 StorageGRID 시스템의 수집 및 검색 속도가 초당 바이트 및 총 바이트 단위로 표시됩니다. 시간 간격(시간, 일, 주, 월 또는 년)을 선택할 수 있습니다. 또는 사용자 지정 간격을 적용할 수 있습니다.

6. 특정 스토리지 노드에 대한 정보를 보려면 왼쪽의 목록에서 노드를 선택하고 * Objects * 탭을 클릭합니다.

   이 차트에는 이 스토리지 노드의 객체 수집 및 검색 속도가 나와 있습니다. 이 탭에는 개체 수, 쿼리 및 검증에 대한 메트릭도 포함되어 있습니다. 레이블을 클릭하여 이러한 메트릭의 정의를 볼 수 있습니다.



7. 더 자세한 내용을 원하는 경우:

a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.

b. site_ * > * Overview * > * Main * 을 선택합니다.

   API 작업 섹션에는 전체 그리드에 대한 요약 정보가 표시됩니다.

c. 스토리지 노드 * > * LDR * > **CLIENT APPLICATION* * > * Overview * > * Main * 을 선택합니다

   작업 섹션에는 선택한 스토리지 노드에 대한 요약 정보가 표시됩니다.

감사 로그 액세스 및 검토

감사 메시지는 StorageGRID 서비스에서 생성되고 텍스트 로그 파일에 저장됩니다. 감사 로그의 API 관련 감사 메시지는 시스템의 상태를 평가하는 데 도움이 되는 중요한 보안, 운영 및 성능 모니터링 데이터를 제공합니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.
- 관리 노드의 IP 주소를 알아야 합니다.

이 작업에 대해

활성 감사 로그 파일은 AUDIT.LOG라는 이름으로 관리 노드에 저장됩니다.

하루에 한 번 활성 audit.log 파일이 저장되고 새 audit.log 파일이 시작됩니다. 저장된 파일의 이름은 저장 시기를 yyyy-mm-dd.txt 형식으로 나타냅니다.

하루 후에는 원래 날짜를 유지하는 형식(yyyy-mm-dd.txt.gz)으로 저장된 파일이 압축되고 이름이 변경됩니다.

이 예에서는 활성 audit.log 파일, 이전 날짜의 파일(2018-04-15.txt) 및 이전 날짜의 압축 파일('2018-04-14.txt.gz')을 보여 줍니다.

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

단계

1. 관리자 노드에 로그인:

   a. 'ssh_admin@primary_Admin_Node_IP_' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

2. 감사 로그 파일이 들어 있는 디렉터리('cd/var/local/audit/export')로 이동합니다

3. 필요에 따라 현재 또는 저장된 감사 로그 파일을 봅니다.

관련 정보

감사 로그를 검토합니다

성공한 모든 스토리지 삭제, 가져오기, 헤드, POST 및 PUT 작업은 StorageGRID 감사 로그에서 추적됩니다. 실패는 기록되지 않으며 정보, 인증 또는 옵션 요청도 기록되지 않습니다.

다음 Swift 작업에 대해 추적되는 정보에 대한 자세한 내용은 _감사 메시지 이해_를 참조하십시오.

계정 작업

- 계정을 가져옵니다
- 머리 계정

컨테이너 작업

- 컨테이너를 삭제합니다
- 컨테이너를 가져옵니다
- 헤드 컨테이너
- 용기를 놓습니다

오브젝트 작업

- 개체를 삭제합니다
- 객체를 가져옵니다
- 머리 물체
- 개체를 넣습니다

관련 정보

감사 로그를 검토합니다

계정 작업

컨테이너 작업

오브젝트 작업

StorageGRID 모니터링 및 유지 관리

모니터링하고 문제를 해결합니다

모니터링 및 문제 해결: 개요

이 지침을 사용하여 StorageGRID 시스템을 모니터링하고 발생할 수 있는 문제를 평가하고 해결합니다.

참조하십시오

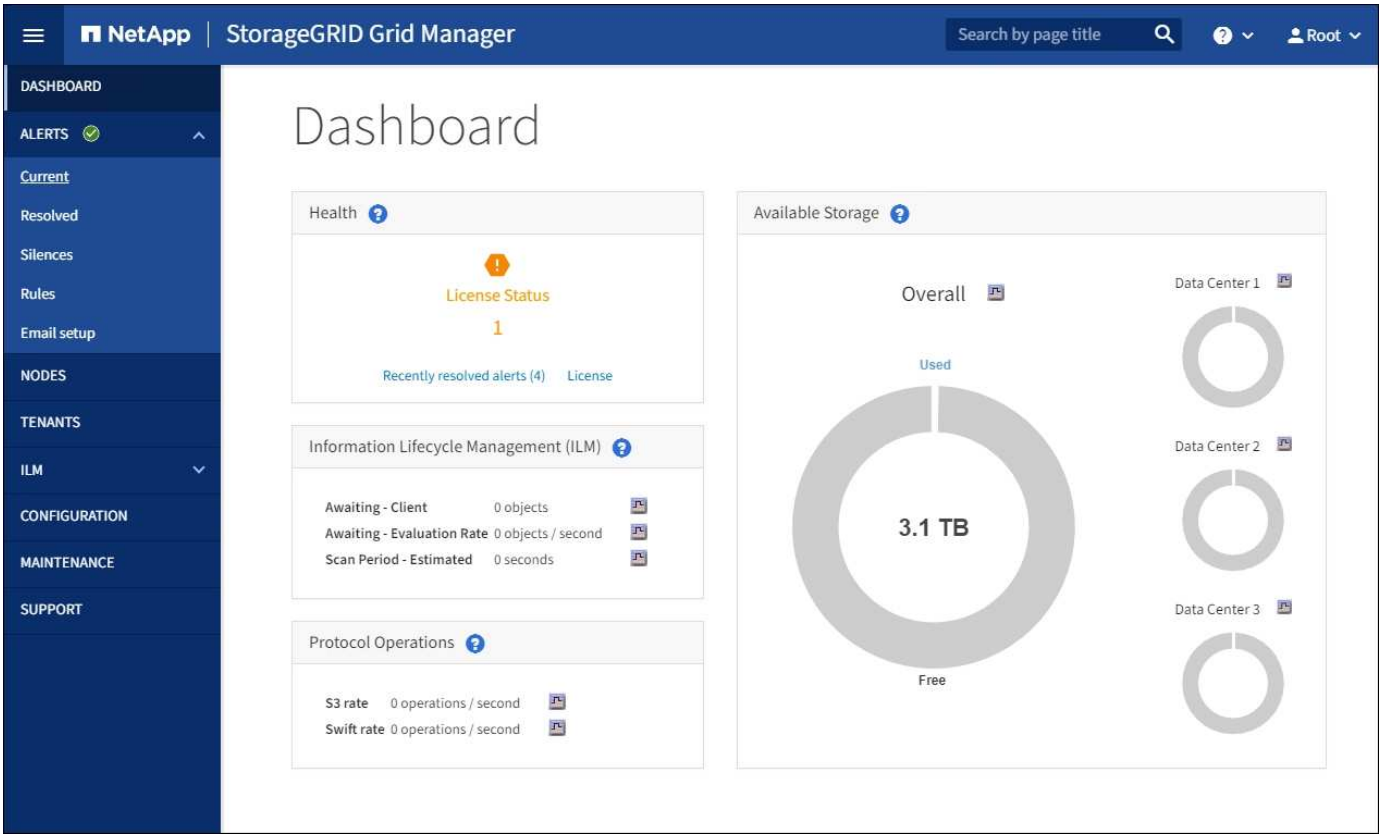
다음 지침은 그리드 관리자를 사용하여 StorageGRID 시스템을 모니터링하는 방법에 대해 설명합니다. 정기적으로 모니터링해야 하는 정보, 경고 및 기존 경보를 관리하는 방법, 모니터링을 위해 SNMP를 사용하는 방법, 메트릭 및 진단을 비롯한 추가 StorageGRID 데이터를 얻는 방법에 대해 알아봅니다.

또한 StorageGRID 시스템의 문제를 해결하는 방법과 모든 시스템 경고, 기존 경보 및 로그 파일에 대해 설명합니다.

StorageGRID 시스템을 설치한 후 이 시스템을 모니터링 및 지원할 경우 다음 지침을 따르십시오.

대시보드 보기

그리드 관리자에 처음 로그인할 때 대시보드를 사용하여 시스템 활동을 한 눈에 모니터링할 수 있습니다. 대시보드에는 시스템 상태, 사용 메트릭, 운영 추세 및 차트에 대한 정보가 포함되어 있습니다.



검색 필드

머리글 표시줄의 * 검색 * 필드를 사용하면 그리드 관리자 내의 특정 페이지 또는 사이드바 항목으로 빠르게 이동할 수 있습니다. 예를 들어, 키 * 를 입력하여 키 관리 서버 페이지에 액세스할 수 있습니다.

상태 패널

설명	추가 세부 정보를 봅니다	자세한 정보
에는 시스템 상태가 요약되어 있습니다. 녹색 확인 표시는 현재 경고가 없고 모든 그리드 노드가 연결되었음을 의미합니다. 다른 아이콘은 현재 경고 또는 연결이 끊긴 노드가 하나 이상 있음을 의미합니다.	다음 링크 중 하나 이상이 표시될 수 있습니다. • * Grid details *: 노드 연결이 끊어진 경우 나타납니다(연결 상태를 알 수 없음 또는 관리상 중단). 링크를 클릭하거나 파란색 또는 회색 아이콘을 클릭하여 영향을 받는 노드를 확인합니다. • * 현재 경고 *: 현재 활성화된 경고가 있는 경우 표시됩니다. 링크를 클릭하거나 * Critical *, * Major * 또는 * Minor * 를 클릭하여 * alerts * > * Current * 페이지에 대한 세부 정보를 확인합니다. • 최근 해결된 경고 *: 지난 주에 트리거된 경고가 이제 해결된 경우 표시됩니다. 링크를 클릭하면 * alerts * > * Resolved * 페이지에서 자세한 내용을 볼 수 있습니다. • * 레거시 알람 *: 현재 활성화된 알람(레거시 시스템)이 있는 경우 나타납니다. 링크를 클릭하면 * 지원 * > * 알람(레거시) * > * 현재 알람 * 페이지에 대한 세부 정보를 볼 수 있습니다. • * 라이센스 *: 이 StorageGRID 시스템에 대한 소프트웨어 라이센스에 문제가 있는 경우 나타납니다. 링크를 클릭하면 * 유지보수 * > * 시스템 * > * 라이센스 * 페이지에 대한 세부 정보를 볼 수 있습니다.	• 노드 연결 상태를 모니터링합니다 • 현재 경고를 봅니다 • 해결된 경고를 봅니다 • 레거시 알람을 봅니다 • StorageGRID 관리

Available Storage(사용 가능한 스토리지**)** 패널

설명	추가 세부 정보를 봅니다	자세한 정보
아카이브 미디어를 제외한 전체 그리드에 사용 가능한 스토리지 용량과 사용된 스토리지 용량을 표시합니다. 전체 차트에는 그리드 전체 합계가 표시됩니다. 다중 사이트 그리드인 경우 각 데이터 센터 사이트에 대해 추가 차트가 나타납니다. 이 정보를 사용하여 사용된 스토리지를 사용 가능한 스토리지와 비교할 수 있습니다. 다중 사이트 그리드가 있는 경우 더 많은 스토리지를 사용하고 있는 사이트를 확인할 수 있습니다.	• 용량을 보려면 차트의 사용 가능 용량 및 사용된 용량 섹션 위에 커서를 놓습니다. • 날짜 범위에 대한 용량 추세를 보려면 차트 아이콘을 클릭합니다 전체 그리드 또는 데이터 센터 사이트의 경우 • 자세한 내용을 보려면 * nodes * 를 선택하십시오. 그런 다음 전체 그리드, 전체 사이트 또는 단일 스토리지 노드에 대한 스토리지 탭을 확인합니다.	• Storage 탭을 봅니다 • 스토리지 용량을 모니터링합니다

ILM(정보 수명 주기 관리) 패널

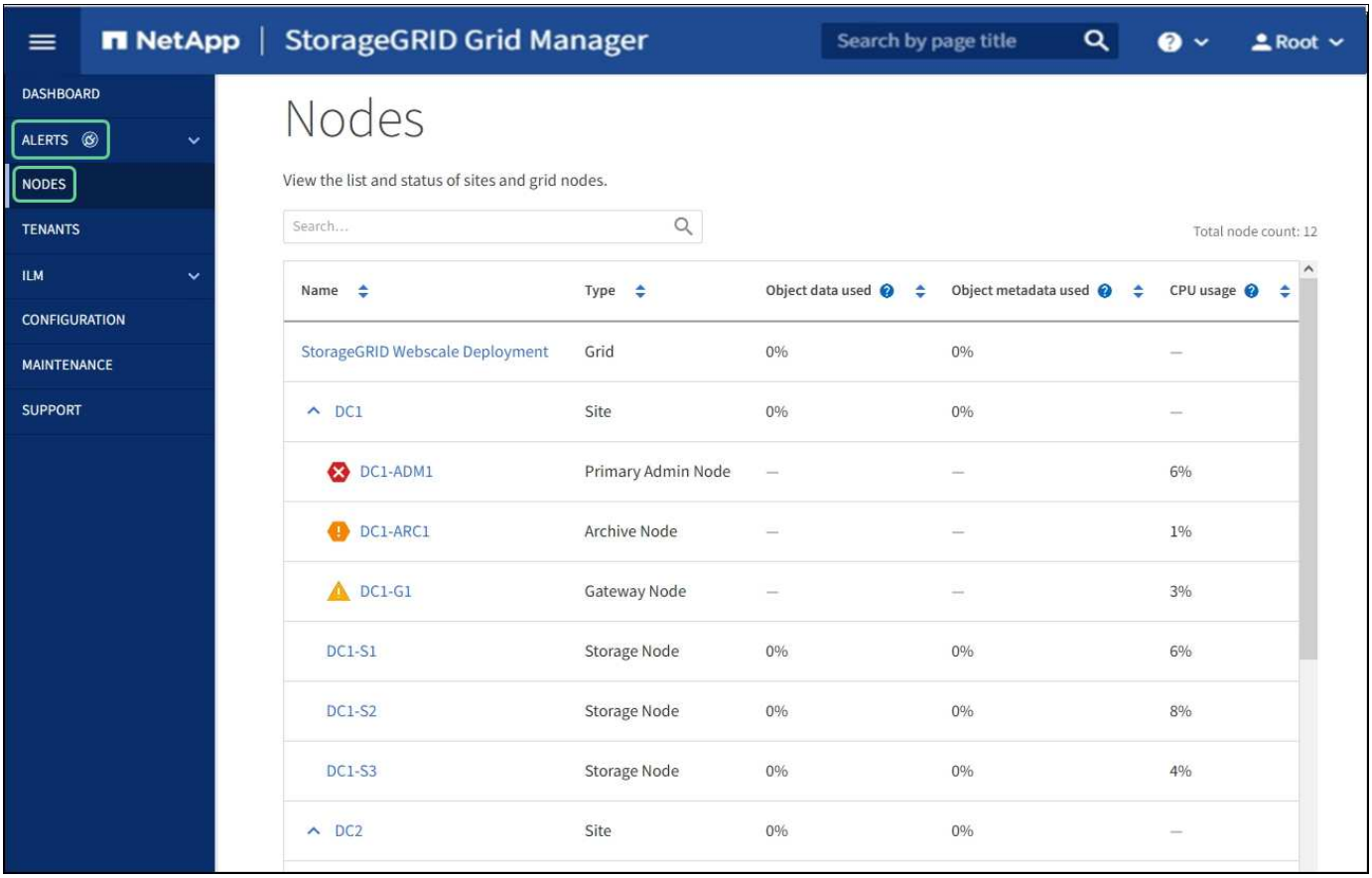
설명	추가 세부 정보를 봅니다	자세한 정보
시스템의 현재 ILM 작업 및 ILM 대기열을 표시합니다. 이 정보를 사용하여 시스템의 워크로드를 모니터링할 수 있습니다. • * Awaiting-Client *: 클라이언트 작업에서 ILM 평가를 기다리는 총 오브젝트 수(예: 수집). • * Awaiting - Evaluation Rate *: 그리드의 ILM 정책에 따라 객체가 평가되는 현재 속도입니다. • * Scan Period - Estimated *(스캔 기간 - 추정 *): 모든 개체의 전체 ILM 스캔을 완료하는 데 걸리는 예상 시간입니다. * 참고: * 전체 스캔은 ILM이 모든 개체에 적용되었다고 보장하지 않습니다.	• 자세한 내용을 보려면 * nodes * 를 선택하십시오. 그런 다음 전체 그리드, 전체 사이트 또는 단일 스토리지 노드에 대한 ILM 탭을 확인합니다. • 기존 ILM 규칙을 보려면 * ILM * > * 규칙 * 을 선택합니다. • 기존 ILM 정책을 보려면 * ILM * > * 정책 * 을 선택합니다.	• ILM 탭을 봅니다 • StorageGRID 관리.

Protocol Operations(프로토콜 작업) 패널

설명	추가 세부 정보를 봅니다	자세한 정보
시스템에서 수행하는 프로토콜 관련 작업(S3 및 Swift)의 수를 표시합니다. 이 정보를 사용하여 시스템의 워크로드와 효율성을 모니터링할 수 있습니다. 프로토콜 속도는 최근 2분 동안의 평균값입니다.	• 자세한 내용을 보려면 * nodes * 를 선택하십시오. 그런 다음 전체 그리드, 전체 사이트 또는 단일 스토리지 노드에 대한 객체 탭을 봅니다. • 날짜 범위에 대한 추세를 보려면 차트 아이콘을 클릭합니다 S3 또는 Swift 프로토콜 속도의 오른쪽에 있습니다.	• 개체 탭을 봅니다 • S3을 사용합니다 • Swift를 사용합니다

노드 페이지를 봅니다

대시보드에서 제공하는 것보다 StorageGRID 시스템에 대한 자세한 정보가 필요한 경우 노드 페이지를 사용하여 전체 그리드, 그리드의 각 사이트 및 사이트의 각 노드에 대한 메트릭을 볼 수 있습니다.



노드 테이블에는 StorageGRID 시스템의 모든 사이트 및 노드가 나열됩니다. 각 노드에 대한 요약 정보가 표시됩니다. 노드에 활성 경고가 있는 경우 노드 이름 옆에 아이콘이 표시됩니다. 노드가 연결되어 있고 활성 경고가 없는 경우 아이콘이 표시되지 않습니다.

연결 상태 아이콘

- * 연결되지 않음 - 알 수 없음 * : 알 수 없는 이유로 노드가 그리드에 연결되어 있지 않습니다. 예를 들어, 노드 간 네트워크 연결이 끊어지거나 전원이 꺼졌습니다. 노드 * 와 통신할 수 없음 알림도 트리거될 수 있습니다. 다른 알림도 활성 상태일 수 있습니다. 이 상황은 즉각적인 주의가 필요합니다.

  > 관리되는 종료 작업 중에 노드가 알 수 없음으로 나타날 수 있습니다. 이러한 경우 알 수 없음 상태를 무시할 수 있습니다.

- * 연결되지 않음 - 관리 중단 * : 노드가 예상 이유로 그리드에 연결되어 있지 않습니다. 예를 들어, 노드의 노드 또는 서비스가 정상적으로 종료되었거나 노드가 재부팅 중이거나 소프트웨어가 업그레이드 중입니다. 하나 이상의 경고가 활성 상태일 수도 있습니다.

노드가 그리드에서 분리되면 기본 경고가 있을 수 있지만 ""연결되지 않음" 아이콘만 나타납니다. 노드의 활성 알림을 보려면 노드를 선택합니다.

경고 아이콘

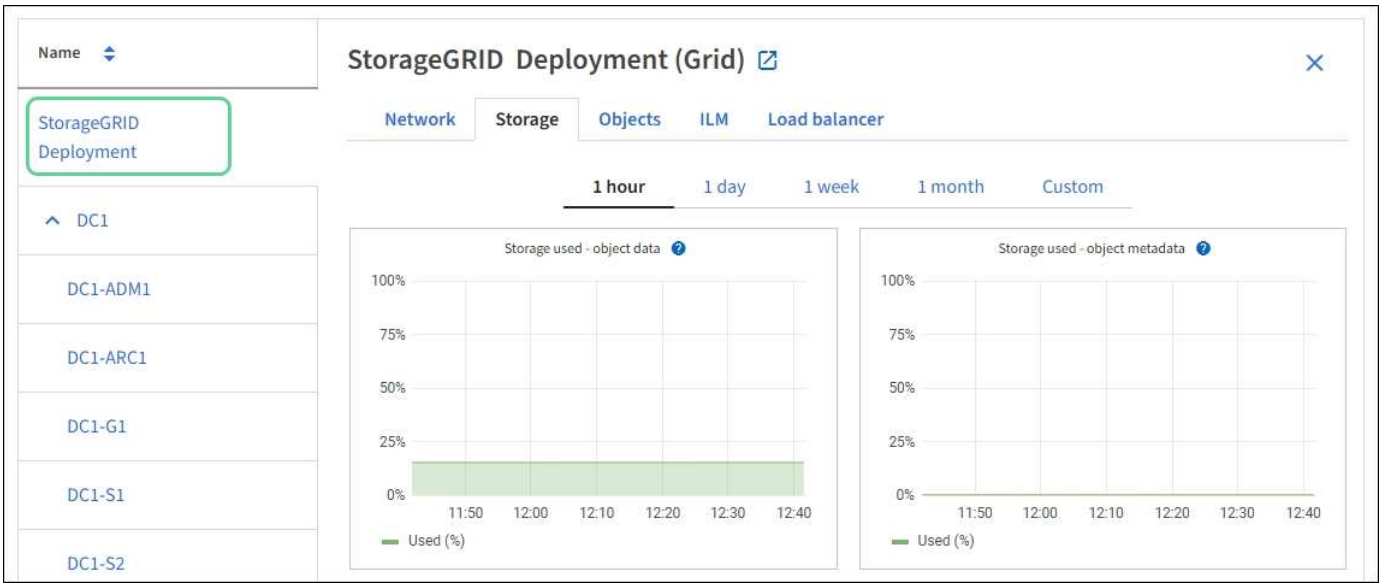
노드에 대한 활성 경고가 있는 경우 노드 이름 옆에 다음 아이콘 중 하나가 표시됩니다.

- * 심각 * : StorageGRID 노드나 서비스의 정상적인 작동을 중지해 온 비정상적인 조건이 존재합니다. 기본 문제를 즉시 해결해야 합니다. 문제가 해결되지 않으면 서비스가 중단되거나 데이터가 손실될 수 있습니다.
- * 주 * : 현재 작업에 영향을 미치거나 위험 경고에 대한 임계값에 근접한 비정상적인 상태가 존재합니다. StorageGRID 노드나 서비스의 정상 작동을 비정상적인 상태로 중지하지 않도록 주요 경고를 조사하고 모든 기본 문제를 해결해야 합니다.
- * 보조 * : 시스템이 정상적으로 작동하지만 시스템이 계속 작동할 경우 시스템 기능에 영향을 줄 수 있는 비정상적인 상태가 존재합니다. 보다 심각한 문제를 초래하지 않도록 자체적으로 명확하지 않은 사소한 경고를 모니터링하고 해결해야 합니다.

시스템, 사이트 또는 노드에 대한 세부 정보 보기

사용 가능한 정보를 보려면 다음과 같이 그리드, 사이트 또는 노드의 이름을 선택합니다.

- 전체 StorageGRID 시스템에 대한 통계 요약을 보려면 그리드 이름을 선택합니다.
- 특정 데이터 센터 사이트를 선택하면 해당 사이트의 모든 노드에 대한 통계 요약을 볼 수 있습니다.
- 특정 노드를 선택하여 해당 노드에 대한 세부 정보를 봅니다.



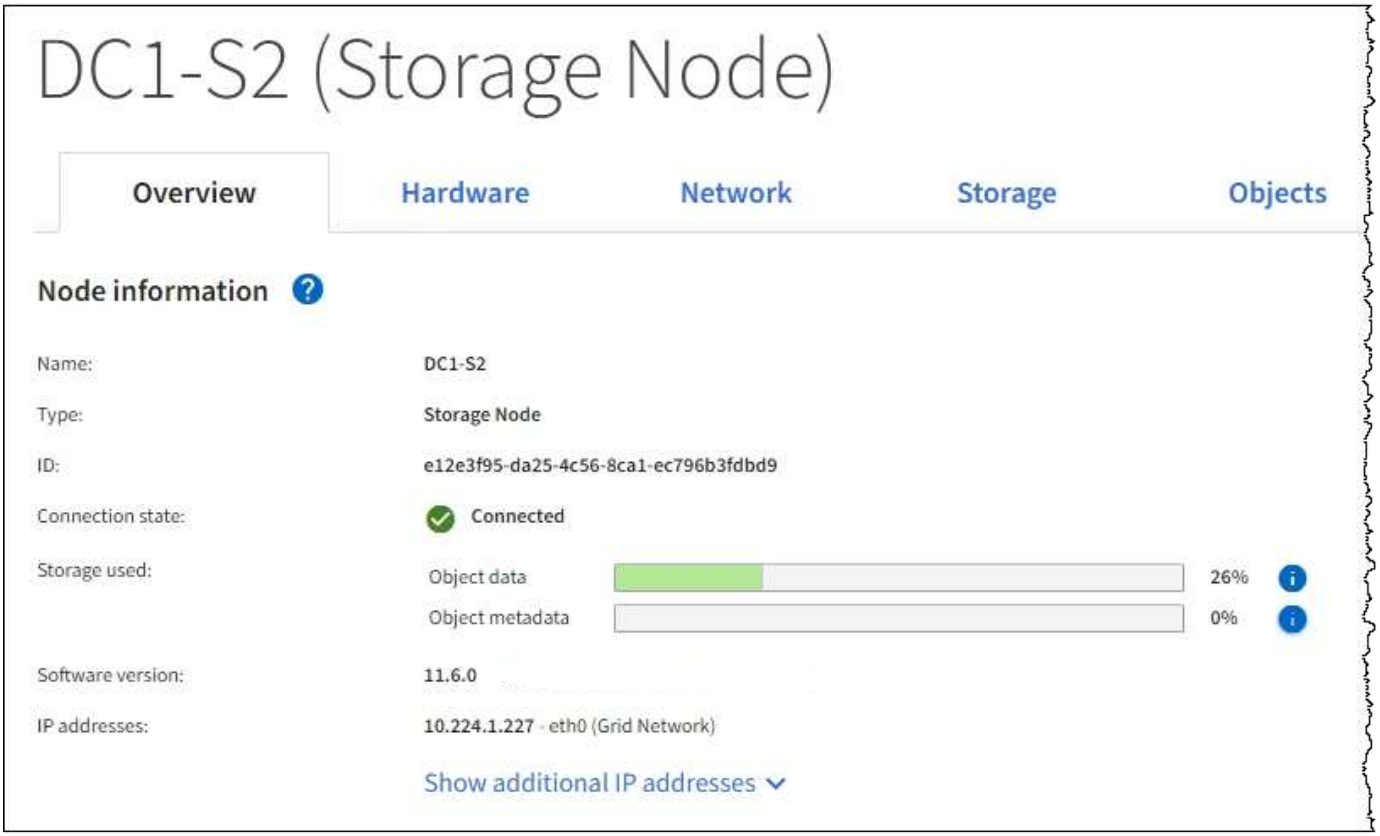
개요 탭을 봅니다

개요 탭은 각 노드에 대한 기본 정보를 제공합니다. 또한 현재 노드에 영향을 주는 모든 알림도 표시됩니다.

개요 탭은 모든 노드에 대해 표시됩니다.

노드 정보

개요 탭의 노드 정보 섹션에는 그리드 노드에 대한 기본 정보가 나열됩니다.



노드에 대한 개요 정보는 다음과 같습니다.

- * Name *: 노드에 할당되고 Grid Manager에 표시되는 호스트 이름입니다.
- * 유형 *: 노드 유형 - 관리 노드, 기본 관리 노드, 스토리지 노드, 게이트웨이 노드 또는 아카이브 노드.
- * ID *: UUID라고도 하는 노드의 고유 식별자입니다.
- * 연결 상태 *: 세 가지 상태 중 하나입니다. 가장 심각한 상태의 아이콘이 표시됩니다.
  - 알 수 없음 * : 알 수 없는 이유로 노드가 그리드에 연결되어 있지 않습니다. 예를 들어, 노드 간 네트워크 연결이 끊어지거나 전원이 꺼졌습니다. 노드 * 와 통신할 수 없음 알림도 트리거될 수 있습니다. 다른 알림도 활성 상태일 수 있습니다. 이 상황은 즉각적인 주의가 필요합니다.

    관리되는 종료 작업 중에 노드가 알 수 없음으로 나타날 수 있습니다. 이러한 경우 알 수 없음 상태를 무시할 수 있습니다.

  - * 관리 아래 * : 노드가 예상 이유로 그리드에 연결되어 있지 않습니다. 예를 들어, 노드의 노드 또는 서비스가 정상적으로 종료되었거나 노드가 재부팅 중이거나 소프트웨어가 업그레이드 중입니다. 하나 이상의 경고가 활성 상태일 수도 있습니다.
  - * 연결됨 * : 노드가 그리드에 연결되어 있습니다.
- * 사용된 스토리지 *: 스토리지 노드에만 해당
  - * 오브젝트 데이터 *: 스토리지 노드에서 사용된 오브젝트 데이터에 대한 총 사용 가능 공간의 비율입니다.
  - * 오브젝트 메타데이터 *: 스토리지 노드에서 사용된 오브젝트 메타데이터에 대해 허용되는 총 공간의 비율입니다.
- 소프트웨어 버전 *: 노드에 설치된 StorageGRID 버전입니다.
- * HA 그룹 *: 관리 노드 및 게이트웨이 노드에만 해당. 노드의 네트워크 인터페이스가 고가용성 그룹에 포함되어 있고 해당 인터페이스가 기본 인터페이스인지 여부를 나타냅니다.
- * IP 주소 *: 노드의 IP 주소 노드의 IPv4 및 IPv6 주소 및 인터페이스 매핑을 보려면 * 추가 IP 주소 표시 * 를 클릭합니다.

경고

Overview(개요) 탭의 Alerts(경고) 섹션에는 이 노드에 현재 영향을 미치고 있는 모든 알림이 소거되지 않은 것으로 표시됩니다. 추가 세부 정보 및 권장 조치를 보려면 알림 이름을 클릭하십시오.

관련 정보

노드 연결 상태를 모니터링합니다

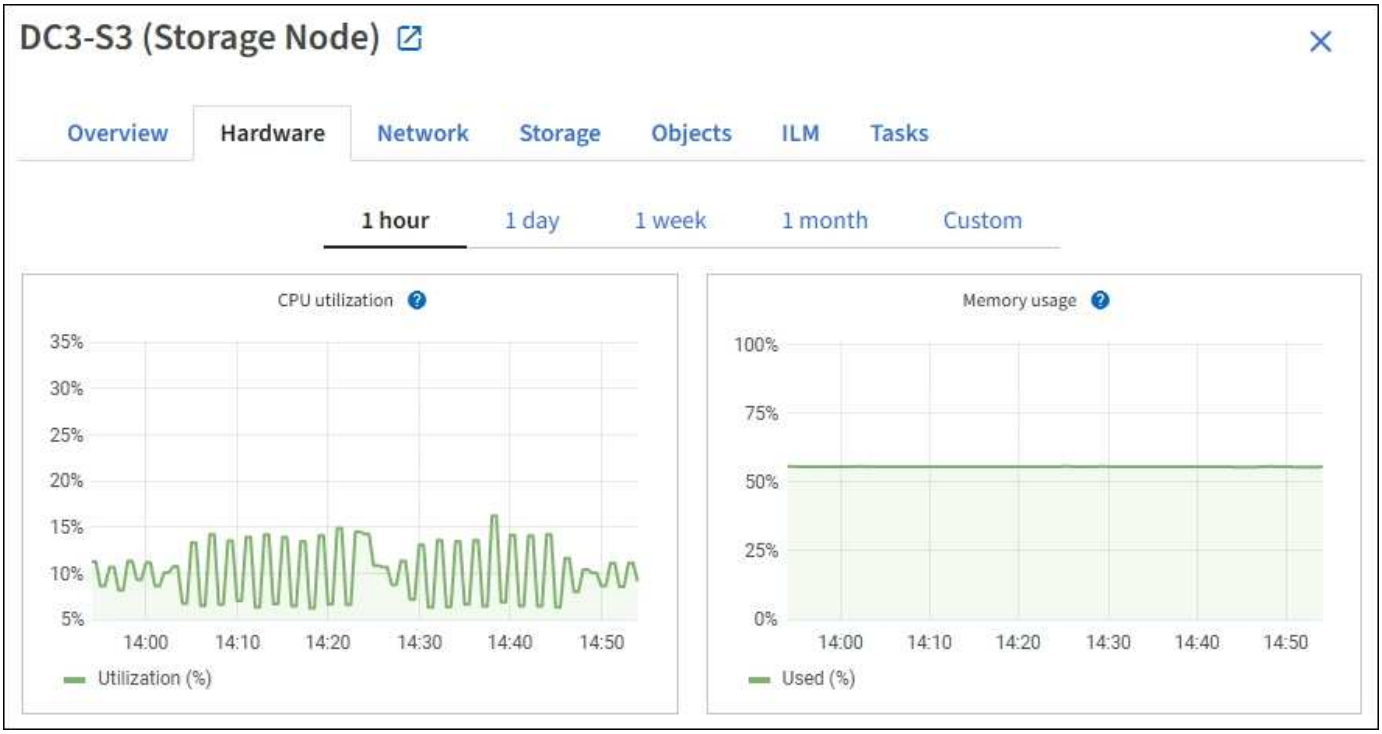
현재 경고를 봅니다

특정 경고를 봅니다

하드웨어 탭을 봅니다

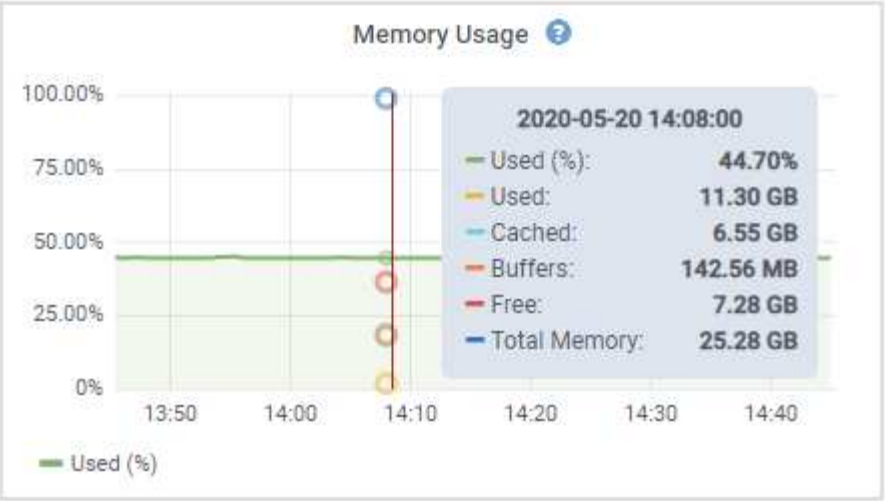
하드웨어 탭에는 각 노드의 CPU 사용률 및 메모리 사용량, 어플라이언스에 대한 추가 하드웨어 정보가 표시됩니다.

모든 노드에 대해 하드웨어 탭이 표시됩니다.



다른 시간 간격을 표시하려면 차트 또는 그래프 위에 있는 컨트롤 중 하나를 선택합니다. 1시간, 1일, 1주 또는 1개월 간격으로 사용 가능한 정보를 표시할 수 있습니다. 날짜 및 시간 범위를 지정할 수 있는 사용자 지정 간격을 설정할 수도 있습니다.

CPU 사용률 및 메모리 사용량에 대한 세부 정보를 보려면 커서를 각 그래프 위에 놓습니다.



노드가 어플라이언스 노드인 경우 이 탭에는 어플라이언스 하드웨어에 대한 자세한 정보가 있는 섹션도 포함되어 있습니다.

어플라이언스 스토리지 노드에 대한 정보를 봅니다

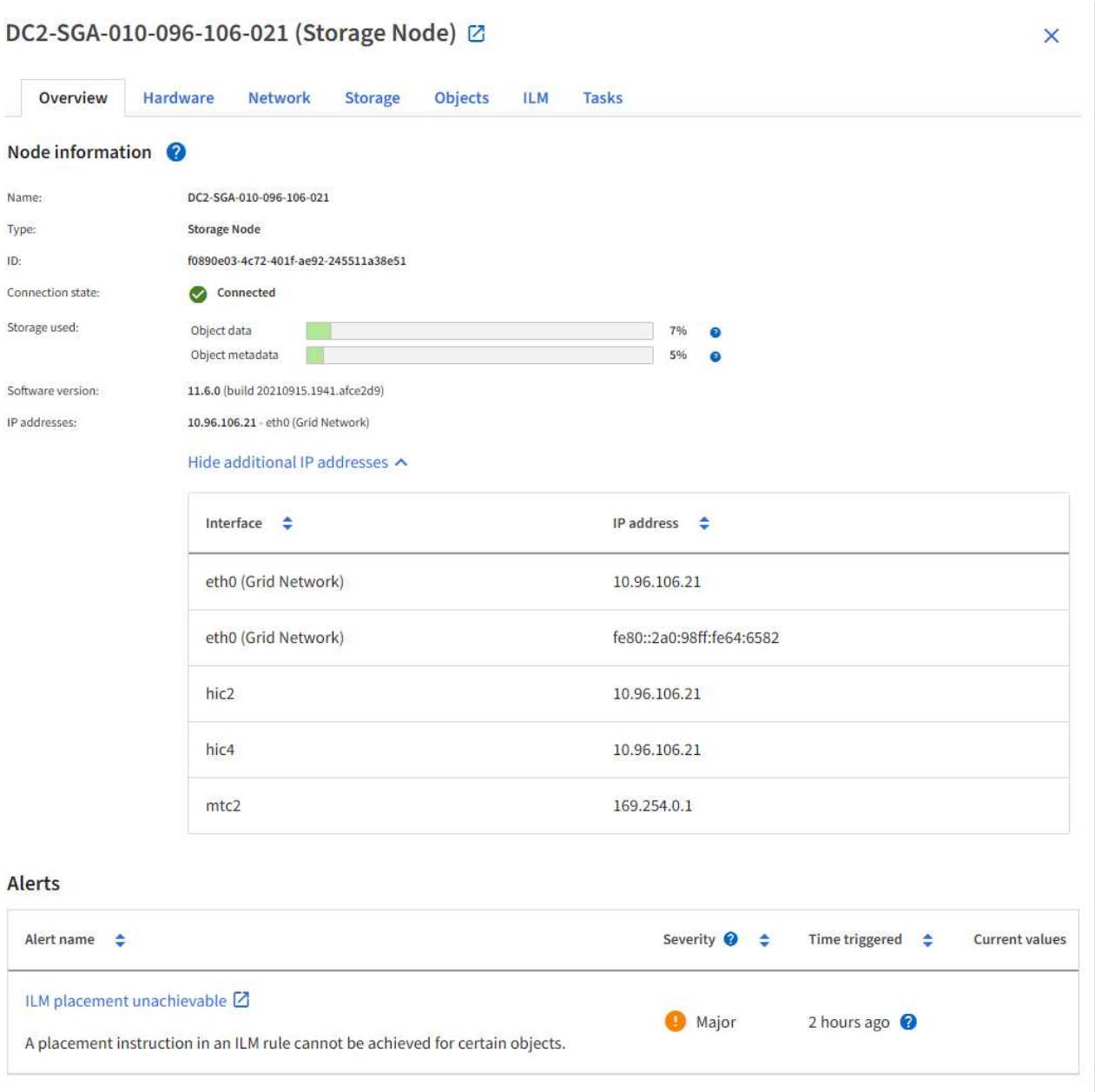
노드 페이지에는 서비스 상태에 대한 정보와 각 어플라이언스 스토리지 노드의 모든 컴퓨팅, 디스크 디바이스 및 네트워크 리소스에 대한 정보가 나열됩니다. 또한 메모리, 스토리지 하드웨어, 컨트롤러 펌웨어 버전, 네트워크 리소스, 네트워크 인터페이스, 네트워크 주소, 데이터 수신 및 전송

단계

1. 노드 페이지에서 어플라이언스 스토리지 노드를 선택합니다.
2. 개요 * 를 선택합니다.

   개요 탭의 노드 정보 섹션에는 노드의 이름, 유형, ID 및 연결 상태와 같은 노드에 대한 요약 정보가 표시됩니다. IP 주소 목록에는 다음과 같이 각 주소에 대한 인터페이스 이름이 포함됩니다.

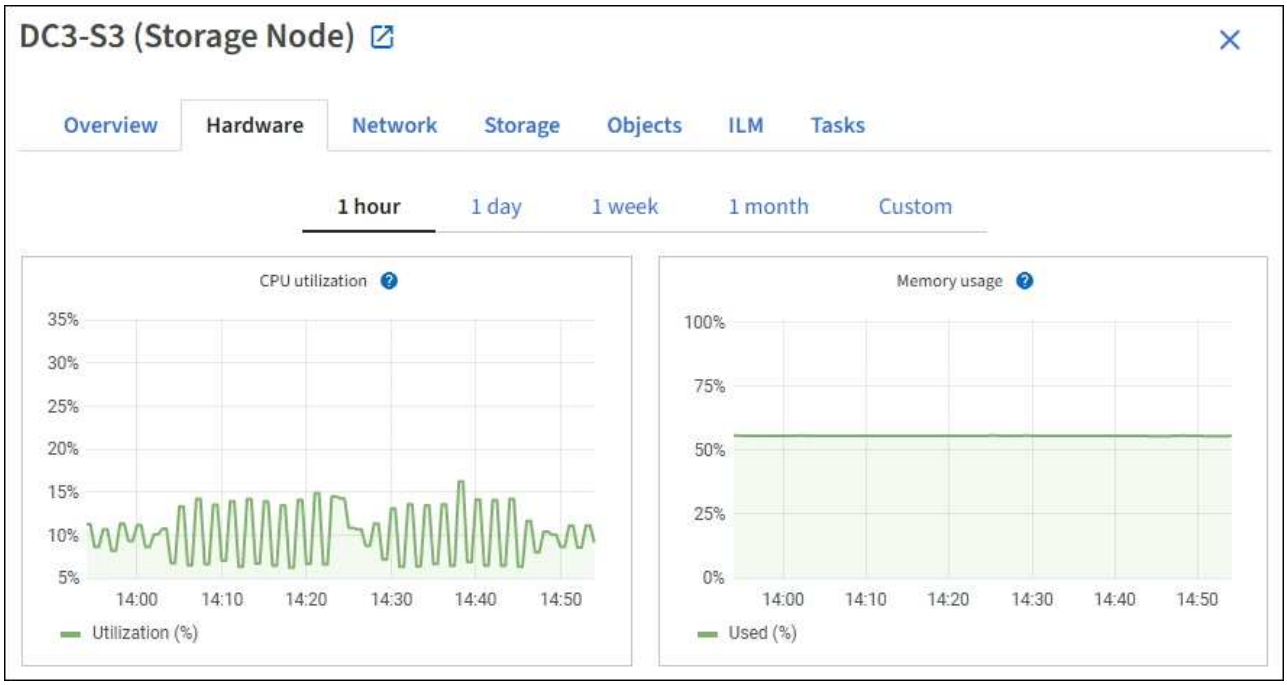
   - * eth *: 그리드 네트워크, 관리자 네트워크 또는 클라이언트 네트워크.
   - * hic *: 어플라이언스에 있는 물리적 10GbE, 25 또는 100GbE 포트 중 하나입니다. 이러한 포트는 함께 연결되어 StorageGRID 그리드 네트워크(eth0) 및 클라이언트 네트워크(eth2)에 연결할 수 있습니다.
   - * MTC *: 어플라이언스에 있는 물리적 1GbE 포트 중 하나입니다. 하나 이상의 MTC 인터페이스가 StorageGRID 관리 네트워크 인터페이스(eth1)를 형성하도록 연결됩니다. 다른 MTC 인터페이스를 데이터 센터 내 기술자의 임시 로컬 연결에 사용할 수 있도록 둘 수 있습니다.



개요 탭의 경고 섹션에는 노드에 대한 활성 경고가 표시됩니다.

3. 어플라이언스에 대한 자세한 내용을 보려면 * 하드웨어 * 를 선택하십시오.

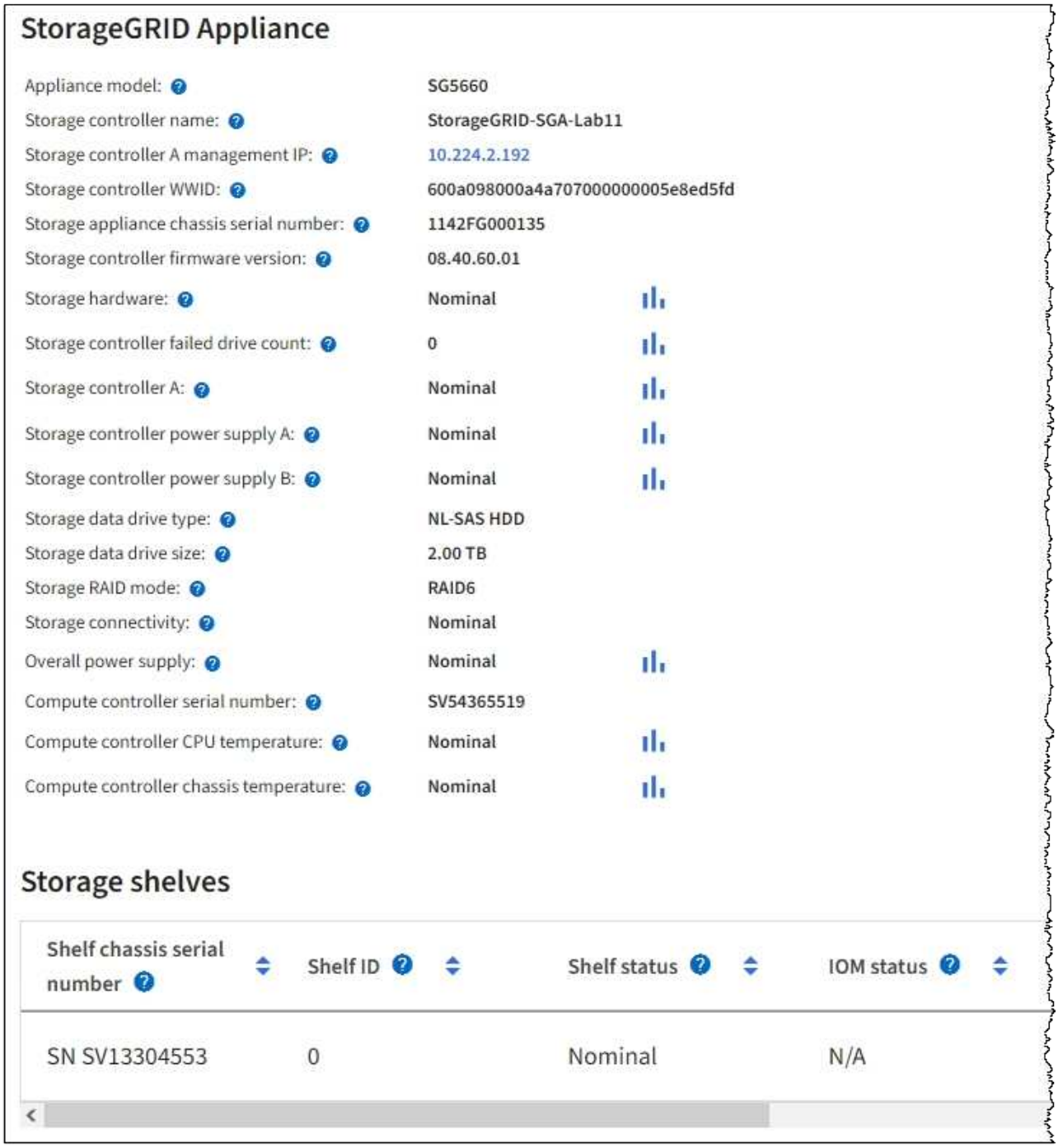
   a. CPU Utilization(CPU 사용률) 및 Memory(메모리) 그래프를 보고 시간에 따른 CPU 및 메모리 사용량 비율을 확인합니다. 다른 시간 간격을 표시하려면 차트 또는 그래프 위에 있는 컨트롤 중 하나를 선택합니다. 1시간, 1일, 1주 또는 1개월 간격으로 사용 가능한 정보를 표시할 수 있습니다. 날짜 및 시간 범위를 지정할 수 있는 사용자 지정 간격을 설정할 수도 있습니다.



b. 아래로 스크롤하여 제품의 구성 요소 표를 봅니다. 이 표에는 어플라이언스의 모델 이름, 컨트롤러 이름, 일련 번호 및 IP 주소, 각 구성요소의 상태와 같은 정보가 포함되어 있습니다.

> 컴퓨팅 컨트롤러 BMC IP 및 컴퓨팅 하드웨어와 같은 일부 필드는 해당 기능이 있는 어플라이언스에 대해서만 나타납니다.

스토리지 쉘프의 구성요소 및 설치 시 확장 쉘프가 어플라이언스 테이블 아래의 개별 테이블에 표시됩니다.



Appliance 테이블의 필드	설명
어플라이언스 모델	이 StorageGRID 어플라이언스의 모델 번호는 SANtricity 소프트웨어에 나와 있습니다.
스토리지 컨트롤러 이름입니다	SANtricity 소프트웨어에 표시된 이 StorageGRID 어플라이언스의 이름입니다.
스토리지 컨트롤러 A 관리 IP	스토리지 컨트롤러 A의 관리 포트 1에 대한 IP 주소입니다 이 IP를 사용하여 SANtricity 소프트웨어에 액세스하여 스토리지 문제를 해결할 수 있습니다.

Appliance 테이블의 필드	설명
스토리지 컨트롤러 B 관리 IP	스토리지 컨트롤러 B의 관리 포트 1에 대한 IP 주소입니다 이 IP를 사용하여 SANtricity 소프트웨어에 액세스하여 스토리지 문제를 해결할 수 있습니다. 일부 어플라이언스 모델에는 스토리지 컨트롤러 B가 없습니다
스토리지 컨트롤러 WWID입니다	SANtricity 소프트웨어에 표시된 스토리지 컨트롤러의 전 세계적 식별자입니다.
스토리지 어플라이언스 섀시 일련 번호입니다	어플라이언스의 섀시 일련 번호입니다.
스토리지 컨트롤러 펌웨어 버전입니다	이 어플라이언스에 대한 스토리지 컨트롤러의 펌웨어 버전입니다.
스토리지 하드웨어	스토리지 컨트롤러 하드웨어의 전체 상태입니다. SANtricity System Manager에서 스토리지 하드웨어에 대한 Needs Attention(주의 필요) 상태를 보고하는 경우 StorageGRID 시스템도 이 값을 보고합니다. 상태가 "'주의 필요'인 경우 먼저 SANtricity 소프트웨어를 사용하여 스토리지 컨트롤러를 확인하십시오. 그런 다음 컴퓨팅 컨트롤러에 적용되는 다른 경보가 없는지 확인합니다.
스토리지 컨트롤러의 드라이브 수가 실패했습니다	최적화되지 않은 드라이브 수입니다.
스토리지 컨트롤러 A	스토리지 컨트롤러 A의 상태입니다
스토리지 컨트롤러 B	스토리지 컨트롤러 B의 상태입니다 일부 어플라이언스 모델에는 스토리지 컨트롤러 B가 없습니다
스토리지 컨트롤러 전원 공급 장치 A	스토리지 컨트롤러의 전원 공급 장치 A의 상태입니다.
스토리지 컨트롤러 전원 공급 장치 B	스토리지 컨트롤러의 전원 공급 장치 B의 상태입니다.
스토리지 데이터 드라이브 유형입니다	HDD(하드 디스크 드라이브) 또는 SSD(Solid State Drive)와 같은 어플라이언스의 드라이브 유형입니다.
스토리지 데이터 드라이브 크기입니다	하나의 데이터 드라이브의 유효 크기입니다. • 참고 *: 확장 쉘프가 있는 노드의 경우 를 사용하십시오 각 쉘프의 데이터 드라이브 크기입니다 대신 유효 드라이브 크기는 쉘프마다 다를 수 있습니다.
스토리지 RAID 모드	어플라이언스에 대해 구성된 RAID 모드입니다.

Appliance 테이블의 필드	설명
스토리지 연결	스토리지 접속 상태입니다.
전체 전원 공급 장치	어플라이언스에 대한 모든 전원 공급 장치의 상태입니다.
컨트롤러 BMC IP를 계산합니다	컴퓨팅 컨트롤러에 있는 BMC(베이스보드 관리 컨트롤러) 포트의 IP 주소입니다. 이 IP를 사용하여 BMC 인터페이스에 연결하여 어플라이언스 하드웨어를 모니터링하고 진단합니다. BMC가 포함되지 않은 어플라이언스 모델에는 이 필드가 표시되지 않습니다.
컴퓨팅 컨트롤러 일련 번호입니다	컴퓨팅 컨트롤러의 일련 번호입니다.
컴퓨팅 하드웨어	컴퓨팅 컨트롤러 하드웨어의 상태입니다. 별도의 컴퓨팅 하드웨어와 스토리지 하드웨어가 없는 어플라이언스 모델에는 이 필드가 표시되지 않습니다.
컨트롤러 CPU 온도를 계산합니다	컴퓨팅 컨트롤러의 CPU의 온도 상태입니다.
컨트롤러 섀시 온도를 계산합니다	컴퓨팅 컨트롤러의 온도 상태입니다.

+

열을 클릭합니다	설명
쉘프 섀시 일련 번호입니다	스토리지 쉘프 섀시의 일련 번호입니다.
쉘프 ID입니다	스토리지 쉘프의 숫자 식별자입니다. • 99:스토리지 컨트롤러 쉘프 • 0:첫 번째 확장 쉘프 • 1초 확장 쉘프 ◦ 참고: * 확장 선반은 SG6060 및 SG6060X에만 적용됩니다.
쉘프 상태입니다	스토리지 쉘프의 전체 상태입니다.
IOM 상태	확장 셸프의 입출력 모듈(IOM)의 상태입니다. 해당 없음 - 확장 쉘프가 아닌 경우.
전원 공급 장치 상태입니다	스토리지 쉘프의 전원 공급 장치의 전체 상태입니다.
문서함 상태입니다	스토리지 쉘프에 있는 드로어의 상태입니다. 해당 없음 - 선반에 서랍이 없는 경우

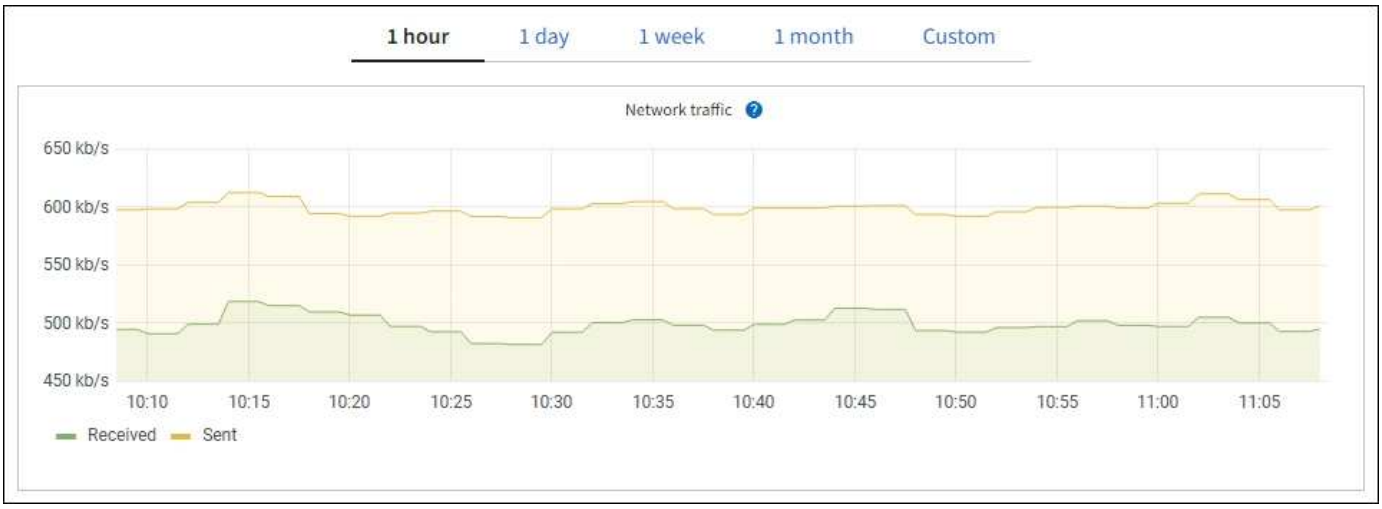
열을 클릭합니다	설명
팬 상태입니다	스토리지 쉘프에 있는 냉각 팬의 전체 상태입니다.
드라이브 슬롯	스토리지 쉘프의 총 드라이브 슬롯 수입니다.
데이터 드라이브	스토리지 쉘프의 드라이브 수로, 데이터 스토리지에 사용됩니다.
데이터 드라이브 크기	스토리지 쉘프에 있는 데이터 드라이브 1개의 유효 크기입니다.
캐시 드라이브	캐시로 사용되는 스토리지 쉘프의 드라이브 수입니다.
캐시 드라이브 크기입니다	스토리지 쉘프에서 가장 작은 캐시 드라이브의 크기입니다. 일반적으로 캐시 드라이브는 모두 크기가 같습니다.
구성 상태입니다	스토리지 셸프의 구성 상태입니다.

4. 모든 스테이터스가 ""명목""인지 확인합니다.

   상태가 "공칭"가 아닌 경우 현재 경고를 검토하십시오. SANtricity 시스템 관리자를 사용하여 이러한 하드웨어 값 중 일부에 대해 자세히 알아볼 수도 있습니다. 제품 설치 및 유지 관리 지침을 참조하십시오.

5. 각 네트워크에 대한 정보를 보려면 * Network * 를 선택하십시오.

네트워크 트래픽 그래프는 전체 네트워크 트래픽에 대한 요약을 제공합니다.



1. 네트워크 인터페이스 섹션을 검토합니다.

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

네트워크 인터페이스 테이블의 * Speed * 열에 있는 값을 사용하여 어플라이언스의 10/25-GbE 네트워크 포트가 액티브/백업 모드 또는 LACP 모드를 사용하도록 구성되었는지 확인하십시오.

표에 표시된 값은 4개의 링크가 모두 사용된다고 가정합니다.

링크 모드	본드 모드	개별 **HIC** 링크 속도**(hic1, hic2, hic3, hic4)**	예상 그리드/클라이언트 네트워크 속도**(eth0, eth2)**
집계	LACP	25	100
고정	LACP	25	50
고정	Active/Backup(활성/백업)	25	25
집계	LACP	10	40
고정	LACP	10	20
고정	Active/Backup(활성/백업)	10	10

10/25-GbE 포트 구성에 대한 자세한 내용은 어플라이언스의 설치 및 유지보수 지침을 참조하십시오.

2. 네트워크 통신 섹션을 검토합니다.

   Receive 및 Transmit 테이블은 각 네트워크를 통해 수신 및 전송된 바이트 및 패킷의 수와 기타 수신 및 전송 메트릭을 보여줍니다.

Network communication

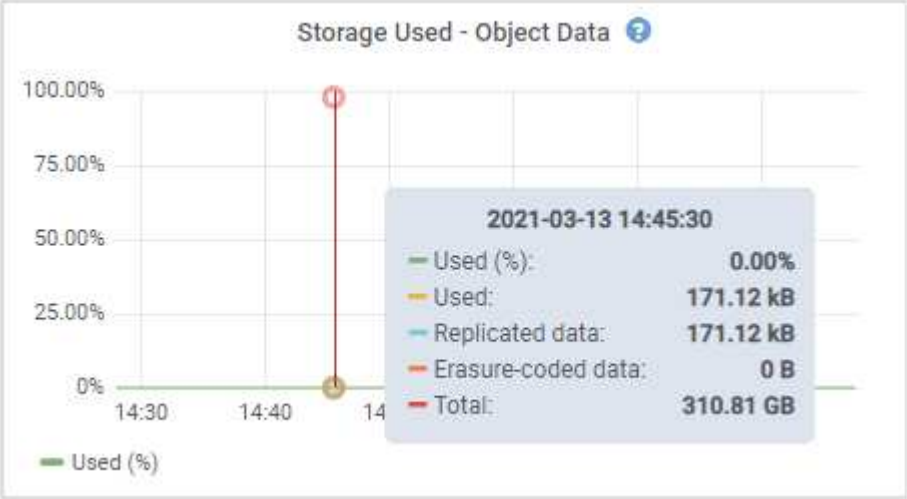
Receive

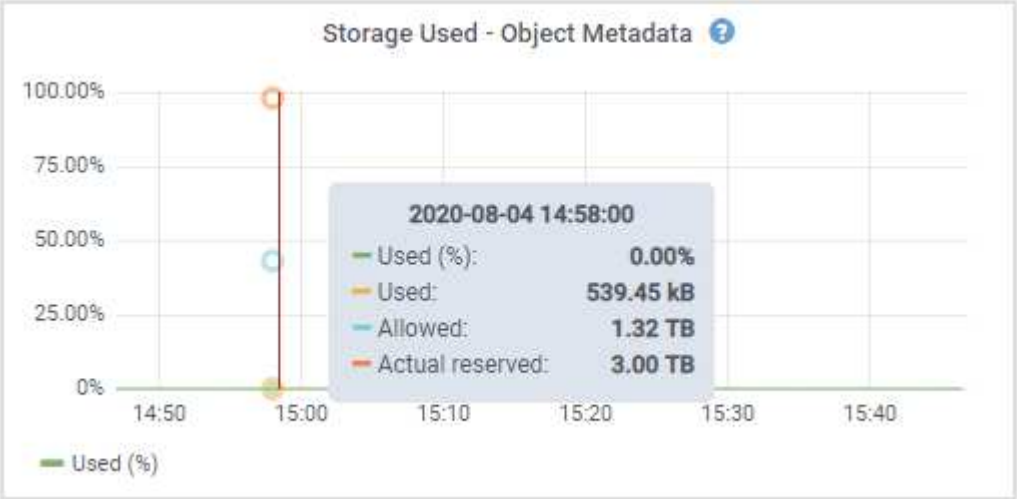
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

3. 스토리지 * 를 선택하면 객체 데이터 및 객체 메타데이터에 대해 시간에 따른 스토리지 사용율과 디스크 디바이스, 볼륨 및 객체 저장소에 대한 정보를 보여주는 그래프를 볼 수 있습니다.





a. 아래로 스크롤하여 각 볼륨 및 오브젝트 저장소에서 사용 가능한 스토리지 양을 확인합니다.

각 디스크의 전 세계 이름은 SANtricity 소프트웨어(어플라이언스의 스토리지 컨트롤러에 연결된 관리 소프트웨어)의 표준 볼륨 속성을 볼 때 나타나는 볼륨 WWID(World-Wide Identifier)와 일치합니다.

볼륨 마운트 지점과 관련된 디스크 읽기 및 쓰기 통계를 해석하려면 디스크 장치 테이블의 * 이름 * 열에 표시된 이름(즉, *sdc*, *SDD*, *SDE* 등)의 첫 번째 부분이 볼륨 테이블의 * 장치 * 열에 표시된 값과 일치합니다.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

관련 정보

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG5600 스토리지 어플라이언스

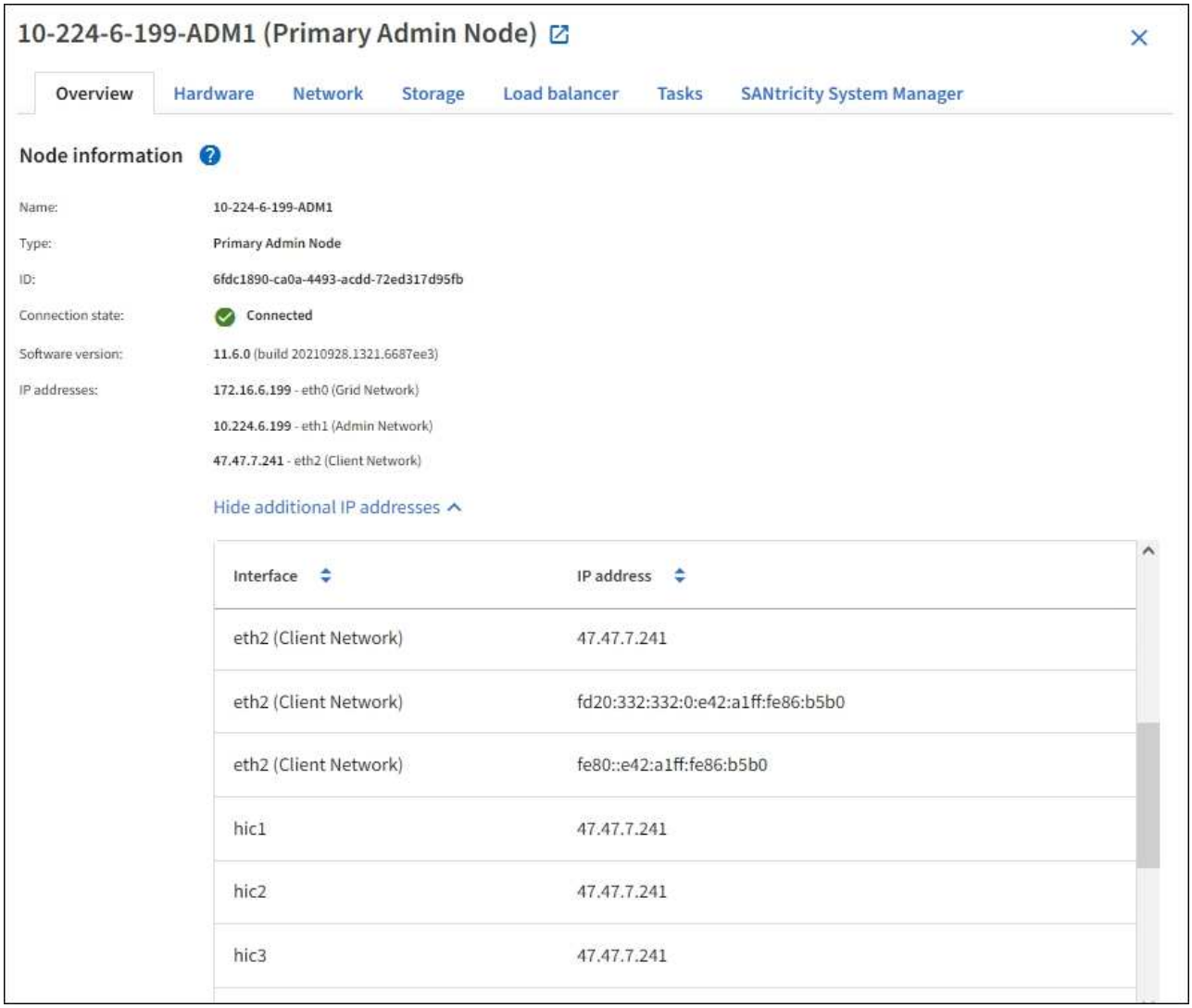
노드 페이지에는 서비스 상태에 대한 정보와 관리 노드 또는 게이트웨이 노드로 사용되는 각 서비스 어플라이언스에 대한 모든 컴퓨팅, 디스크 디바이스 및 네트워크 리소스에 대한 정보가 나열됩니다. 또한 메모리, 스토리지 하드웨어, 네트워크 리소스, 네트워크 인터페이스, 네트워크 주소, 데이터를 수신하고 전송합니다.

단계

1. 노드 페이지에서 어플라이언스 관리 노드 또는 어플라이언스 게이트웨이 노드를 선택합니다.
2. 개요 * 를 선택합니다.

   개요 탭의 노드 정보 섹션에는 노드의 이름, 유형, ID 및 연결 상태와 같은 노드에 대한 요약 정보가 표시됩니다. IP 주소 목록에는 다음과 같이 각 주소에 대한 인터페이스 이름이 포함됩니다.

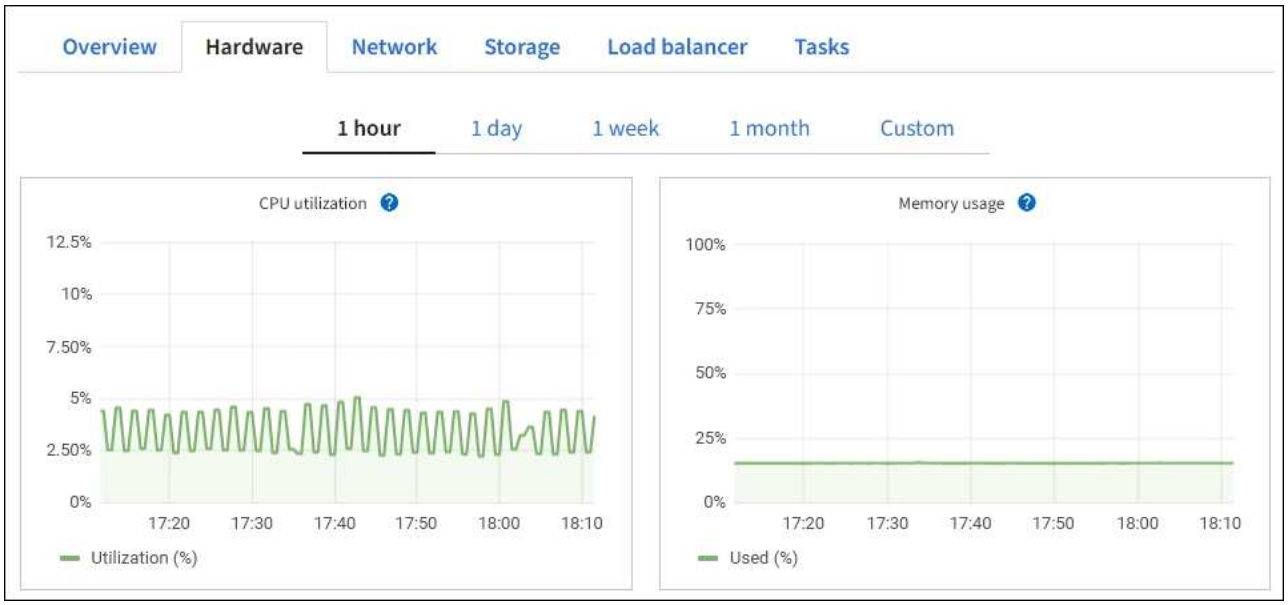
   - * adllb * 및 * adlli *: 관리 네트워크 인터페이스에 활성/백업 본딩을 사용하는 경우에 표시됩니다
   - * eth *: 그리드 네트워크, 관리자 네트워크 또는 클라이언트 네트워크.
   - * hic *: 어플라이언스에 있는 물리적 10GbE, 25 또는 100GbE 포트 중 하나입니다. 이러한 포트는 함께 연결되어 StorageGRID 그리드 네트워크(eth0) 및 클라이언트 네트워크(eth2)에 연결할 수 있습니다.
   - * MTC *: 어플라이언스에 있는 물리적 1GbE 포트 중 하나입니다. 하나 이상의 MTC 인터페이스가 관리 네트워크 인터페이스(eth1)를 형성하도록 연결됩니다. 다른 MTC 인터페이스를 데이터 센터 내 기술자의 임시 로컬 연결에 사용할 수 있도록 둘 수 있습니다.



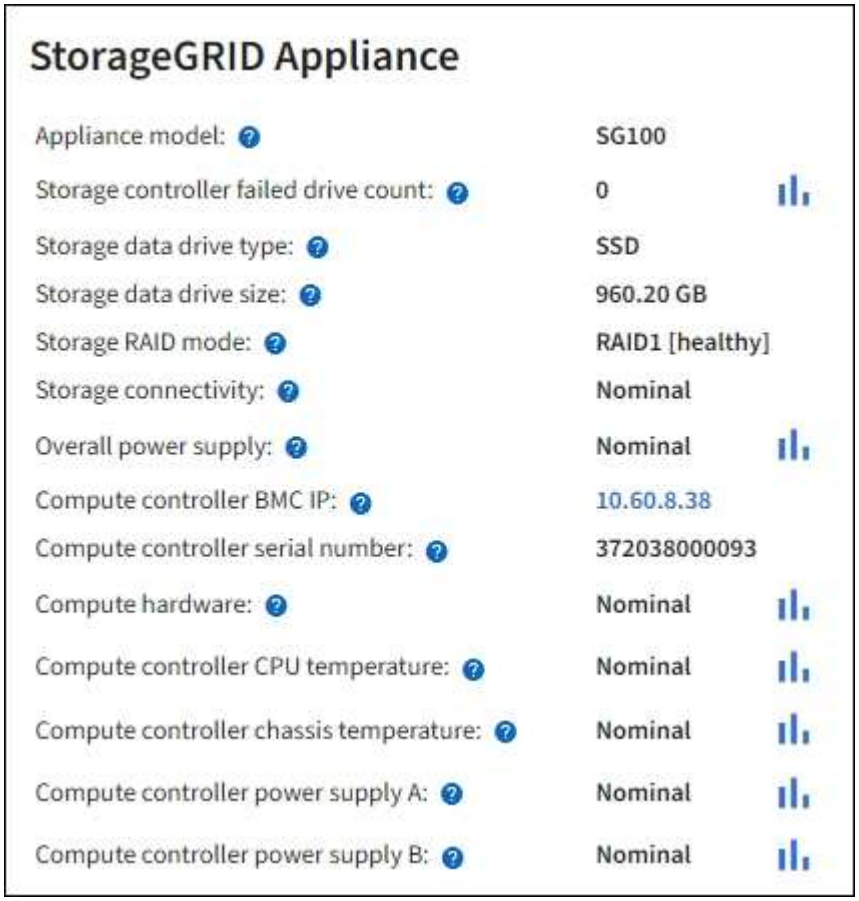
개요 탭의 경고 섹션에는 노드에 대한 활성 경고가 표시됩니다.

3. 어플라이언스에 대한 자세한 내용을 보려면 * 하드웨어 * 를 선택하십시오.

   a. CPU Utilization(CPU 사용률) 및 Memory(메모리) 그래프를 보고 시간에 따른 CPU 및 메모리 사용량 비율을 확인합니다. 다른 시간 간격을 표시하려면 차트 또는 그래프 위에 있는 컨트롤 중 하나를 선택합니다. 1시간, 1일, 1주 또는 1개월 간격으로 사용 가능한 정보를 표시할 수 있습니다. 날짜 및 시간 범위를 지정할 수 있는 사용자 지정 간격을 설정할 수도 있습니다.



b. 아래로 스크롤하여 제품의 구성 요소 표를 봅니다. 이 표에는 모델 이름, 일련 번호, 컨트롤러 펌웨어 버전 및 각 구성 요소의 상태와 같은 정보가 포함되어 있습니다.



Appliance 테이블의 필드	설명
어플라이언스 모델	이 StorageGRID 어플라이언스의 모델 번호입니다.

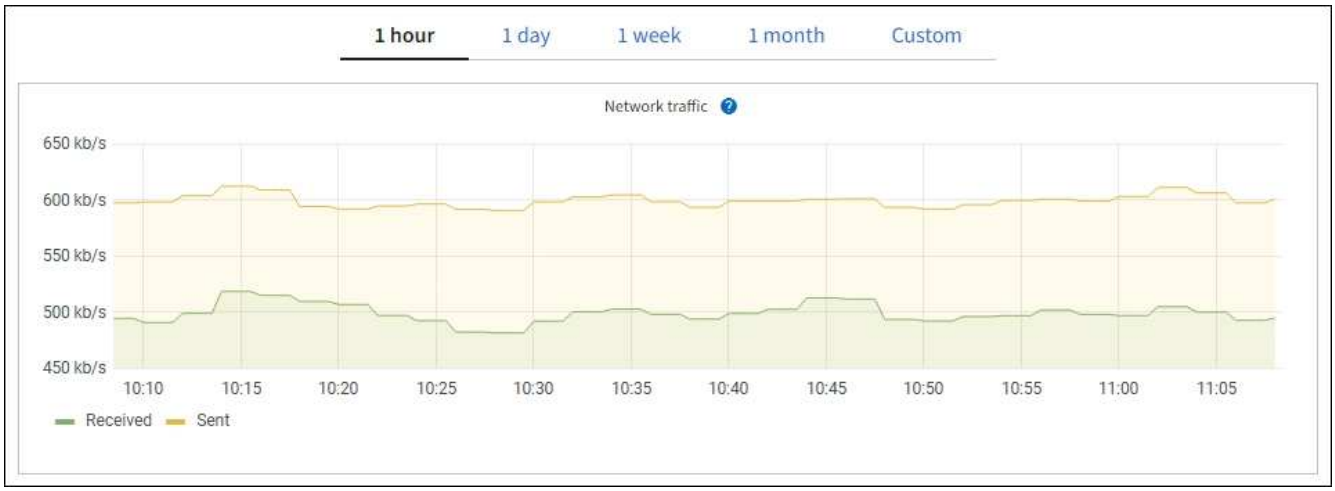
Appliance 테이블의 필드	설명
스토리지 컨트롤러의 드라이브 수가 실패했습니다	최적화되지 않은 드라이브 수입니다.
스토리지 데이터 드라이브 유형입니다	HDD(하드 디스크 드라이브) 또는 SSD(Solid State Drive)와 같은 어플라이언스의 드라이브 유형입니다.
스토리지 데이터 드라이브 크기입니다	하나의 데이터 드라이브의 유효 크기입니다.
스토리지 RAID 모드	어플라이언스의 RAID 모드입니다.
전체 전원 공급 장치	어플라이언스에 있는 모든 전원 공급 장치의 상태입니다.
컨트롤러 BMC IP를 계산합니다	컴퓨팅 컨트롤러에 있는 BMC(베이스보드 관리 컨트롤러) 포트의 IP 주소입니다. 이 IP를 사용하여 BMC 인터페이스에 연결하여 어플라이언스 하드웨어를 모니터링하고 진단할 수 있습니다. BMC가 포함되지 않은 어플라이언스 모델에는 이 필드가 표시되지 않습니다.
컴퓨팅 컨트롤러 일련 번호입니다	컴퓨팅 컨트롤러의 일련 번호입니다.
컴퓨팅 하드웨어	컴퓨팅 컨트롤러 하드웨어의 상태입니다.
컨트롤러 CPU 온도를 계산합니다	컴퓨팅 컨트롤러의 CPU의 온도 상태입니다.
컨트롤러 섀시 온도를 계산합니다	컴퓨팅 컨트롤러의 온도 상태입니다.

a. 모든 스테이터스가 ""명목""인지 확인합니다.

   상태가 "공칭"가 아닌 경우 현재 경고를 검토하십시오.

4. 각 네트워크에 대한 정보를 보려면 * Network * 를 선택하십시오.

   네트워크 트래픽 그래프는 전체 네트워크 트래픽에 대한 요약을 제공합니다.



a. 네트워크 인터페이스 섹션을 검토합니다.

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
eth1	B4:A9:FC:71:68:36	Gigabit	Full	Off	Up
eth2	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
hic1	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic2	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic3	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic4	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
mtc1	B4:A9:FC:71:68:36	Gigabit	Full	On	Up
mtc2	B4:A9:FC:71:68:35	Gigabit	Full	On	Up

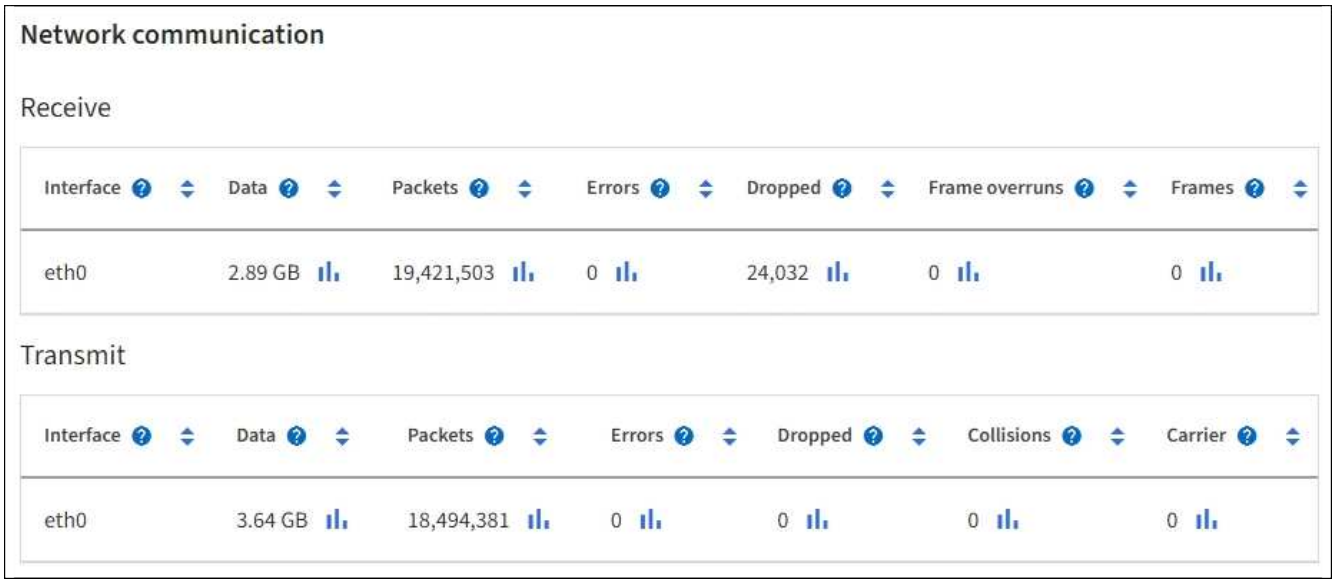
네트워크 인터페이스 테이블의 * Speed * 열에 있는 값을 사용하여 어플라이언스의 40개/100GbE 네트워크 포트 4개가 액티브/백업 모드 또는 LACP 모드를 사용하도록 구성되었는지 확인하십시오.

표에 표시된 값은 4개의 링크가 모두 사용된다고 가정합니다.

링크 모드	본드 모드	개별 **HIC** 링크 속도**(hic1, hic2, hic3, hic4)**	예상 그리드/클라이언트 네트워크 속도**(eth0, eth2)**
집계	LACP	100	400
고정	LACP	100	200
고정	Active/Backup(활성/백업)	100	100
집계	LACP	40	160
고정	LACP	40	80
고정	Active/Backup(활성/백업)	40	40

b. 네트워크 통신 섹션을 검토합니다.

Receive 및 Transmit 테이블은 각 네트워크에서 수신 및 전송된 바이트 및 패킷의 수와 기타 수신 및 전송 메트릭을 보여줍니다.



Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

5. 서비스 어플라이언스의 디스크 장치 및 볼륨에 대한 정보를 보려면 * Storage * 를 선택합니다.

DO-REF-DC1-GW1 (Gateway Node)

Overview | Hardware | Network | Storage | Load balancer | Tasks

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.02%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.03%	0 bytes/s	6 KB/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.63 GB	Unknown

관련 정보

SG100 및 SG1000 서비스 어플라이언스

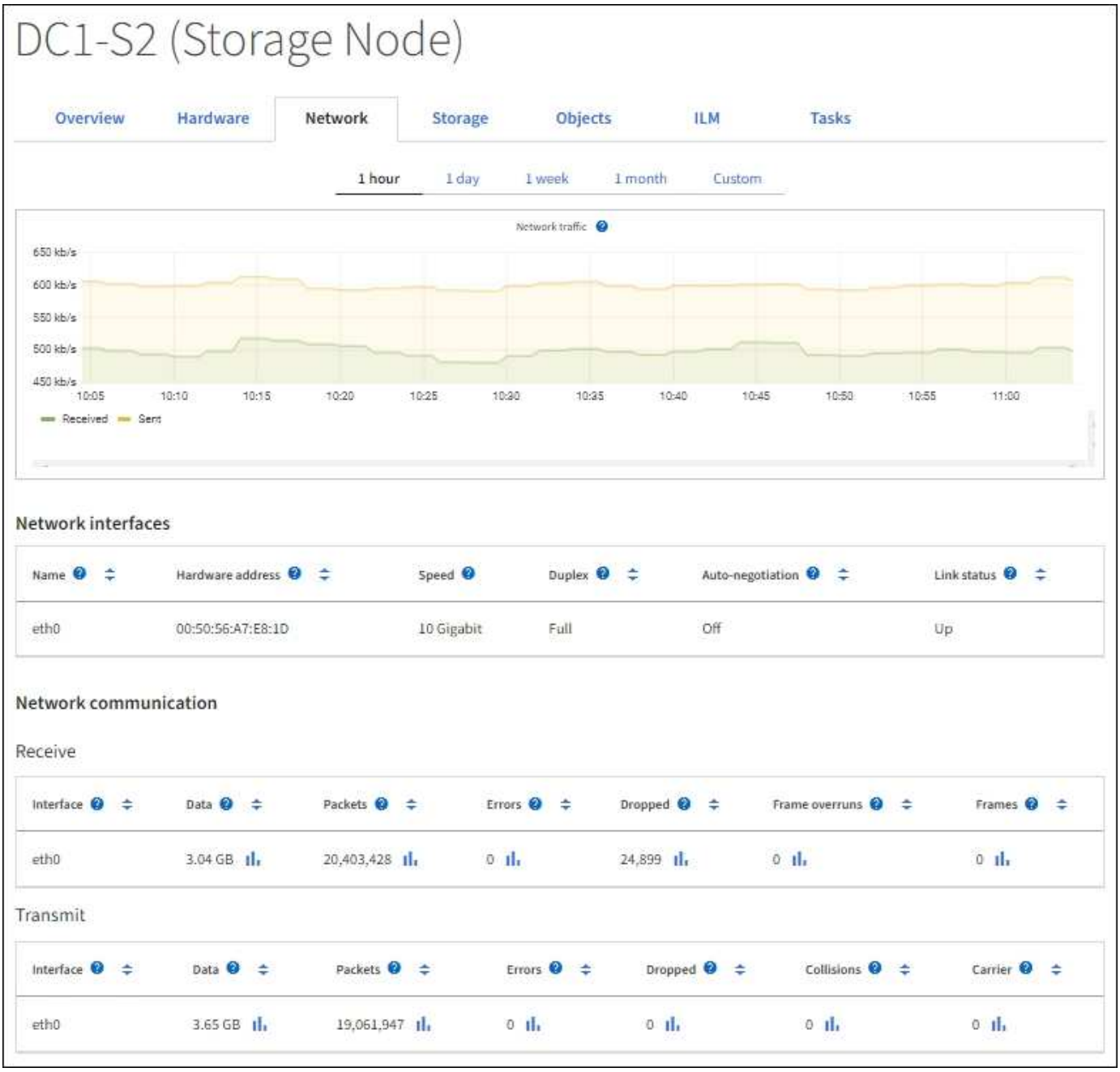
네트워크 탭을 봅니다

네트워크 탭은 노드, 사이트 또는 그리드의 모든 네트워크 인터페이스를 통해 수신 및 전송된 네트워크 트래픽을 보여주는 그래프를 표시합니다.

네트워크 탭은 모든 노드, 각 사이트 및 전체 그리드에 대해 표시됩니다.

다른 시간 간격을 표시하려면 차트 또는 그래프 위에 있는 컨트롤 중 하나를 선택합니다. 1시간, 1일, 1주 또는 1개월 간격으로 사용 가능한 정보를 표시할 수 있습니다. 날짜 및 시간 범위를 지정할 수 있는 사용자 지정 간격을 설정할 수도 있습니다.

노드의 경우 네트워크 인터페이스 표에 각 노드의 물리적 네트워크 포트에 대한 정보가 나와 있습니다. Network communications(네트워크 통신) 표에는 각 노드의 수신 및 전송 작업과 드라이버에서 보고된 고장 카운터에 대한 세부 정보가 나와 있습니다.



관련 정보

네트워크 연결 및 성능을 모니터링합니다

Storage 탭을 봅니다

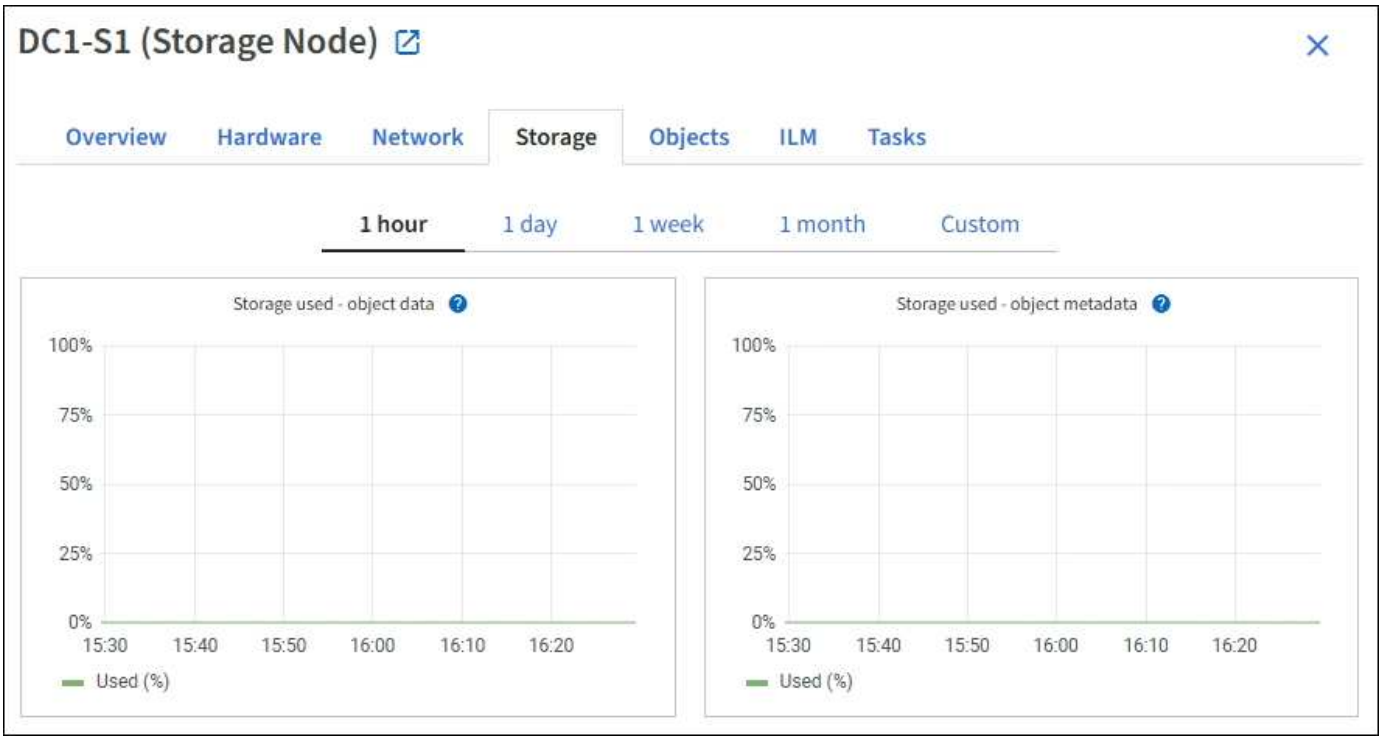
스토리지 탭에는 스토리지 가용성 및 기타 스토리지 메트릭이 요약되어 있습니다.

스토리지 탭은 모든 노드, 각 사이트 및 전체 그리드에 대해 표시됩니다.

스토리지 사용 그래프

스토리지 노드, 각 사이트 및 전체 그리드의 경우 스토리지 탭에는 시간 경과에 따라 오브젝트 데이터 및 오브젝트 메타데이터에 사용된 스토리지 양이 표시된 그래프가 포함됩니다.

사이트 또는 그리드의 총 값에는 오프라인 노드와 같이 최소 5분 동안 보고된 메트릭이 없는 노드가 포함되지 않습니다.



디스크 디바이스, 볼륨 및 객체는 테이블을 저장합니다

모든 노드의 경우 Storage 탭에는 노드의 디스크 디바이스 및 볼륨에 대한 세부 정보가 포함되어 있습니다. 스토리지 노드의 경우 오브젝트 저장소 테이블은 각 스토리지 볼륨에 대한 정보를 제공합니다.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

관련 정보

스토리지 용량을 모니터링합니다

작업 탭을 사용하여 그리드 노드를 재부팅합니다

작업 탭에서는 선택한 노드를 재부팅할 수 있습니다. 모든 노드에 대해 작업 탭이 표시됩니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다.

- 프로비저닝 암호가 있습니다.

이 작업에 대해

작업 탭을 사용하여 노드를 재부팅할 수 있습니다. 어플라이언스 노드의 경우 작업 탭을 사용하여 어플라이언스를 유지 관리 모드로 전환할 수도 있습니다.

- 작업 탭에서 그리드 노드를 재부팅하면 타겟 노드에 재부팅 명령이 실행됩니다. 노드를 재부팅하면 노드가 종료되고 다시 시작됩니다. 모든 서비스가 자동으로 다시 시작됩니다.

  스토리지 노드를 재부팅하려는 경우 다음 사항에 유의하십시오.

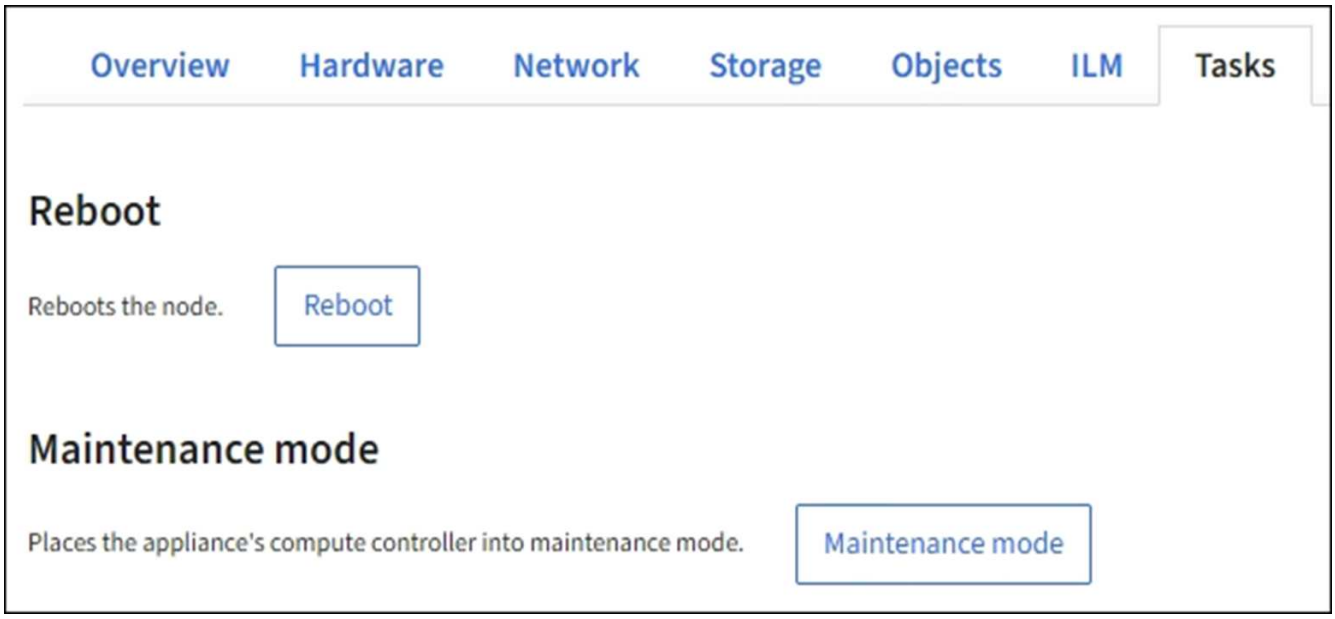
  - ILM 규칙이 이중 커밋의 수집 동작을 지정하거나 규칙이 Balanced 를 지정하며 필요한 모든 복사본을 즉시 생성할 수 없는 경우, StorageGRID는 새로 수집된 개체를 즉시 동일한 사이트의 두 스토리지 노드에 커밋하고 나중에 ILM을 평가합니다. 특정 사이트에서 두 개 이상의 스토리지 노드를 재부팅하려는 경우 재부팅 기간 동안 이러한 개체에 액세스하지 못할 수 있습니다.
  - 스토리지 노드가 재부팅되는 동안 모든 개체에 액세스할 수 있도록 노드를 재부팅하기 전에 약 1시간 동안 사이트에서 객체 인제스트를 중지하십시오.

- 링크 구성 변경 또는 스토리지 컨트롤러 교체와 같은 특정 절차를 수행하려면 StorageGRID 어플라이언스를 유지보수 모드로 전환해야 할 수 있습니다. 자세한 지침은 어플라이언스에 대한 하드웨어 설치 및 유지 관리 지침을 참조하십시오.

> StorageGRID 어플라이언스를 유지보수 모드로 전환하면 원격 액세스가 불가능한 경우가 드물게 있습니다.

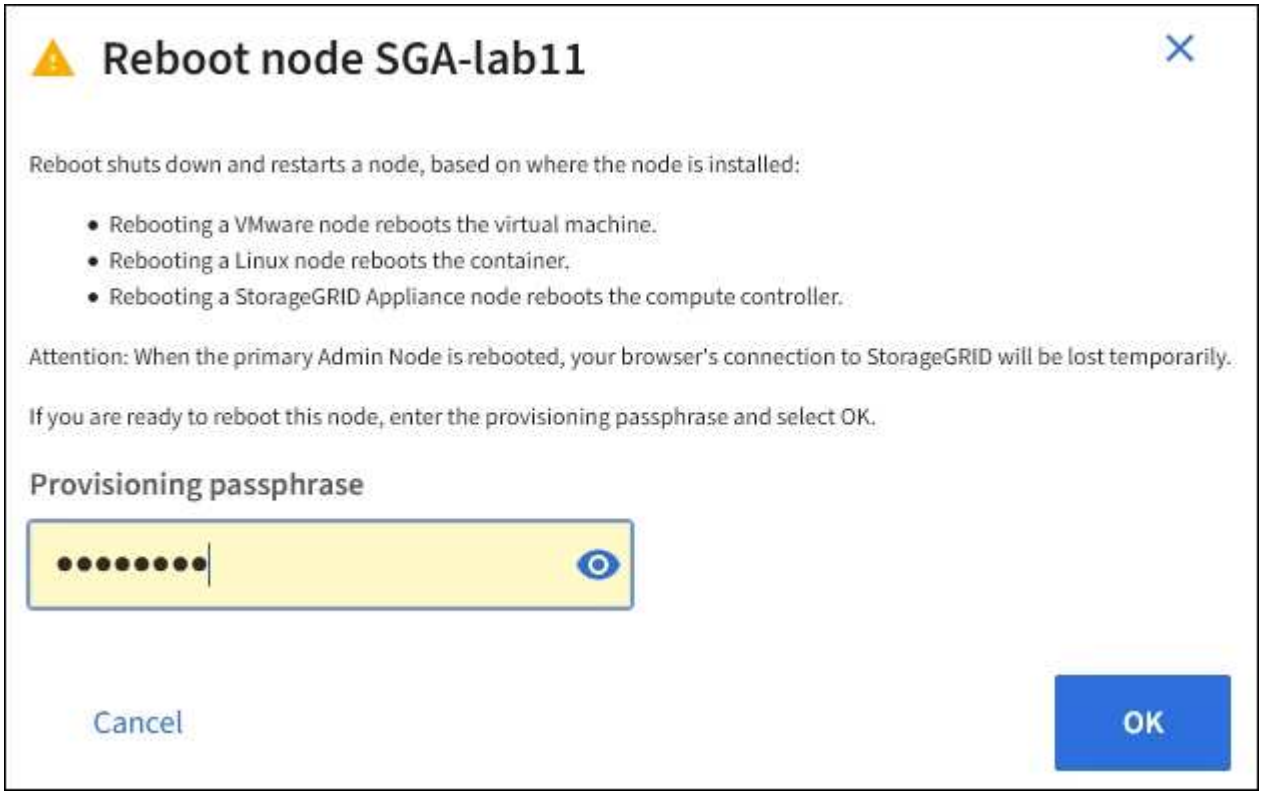
단계

1. 노드 * 를 선택합니다.
2. 재부팅할 그리드 노드를 선택합니다.
3. 작업 * 탭을 선택합니다.



4. 재부팅 * 을 선택합니다.

확인 대화 상자가 나타납니다.



> 기본 관리 노드를 재부팅할 경우 서비스가 중지되면 브라우저에서 Grid Manager에 대한 연결이 일시적으로 끊겼다는 확인 대화 상자가 나타납니다.

5. 프로비저닝 암호를 입력하고 * OK * 를 클릭합니다.
6. 노드가 재부팅될 때까지 기다립니다.

   서비스가 종료되는 데 약간의 시간이 걸릴 수 있습니다.

   노드가 재부팅되면 * Nodes * 페이지 왼쪽에 회색 아이콘(관리자 아래)이 나타납니다. 모든 서비스가 다시 시작되고 노드가 그리드에 성공적으로 연결되면 * Nodes * 페이지에 정상 상태(노드 이름 왼쪽에 아이콘이 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.

관련 정보

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG5600 스토리지 어플라이언스

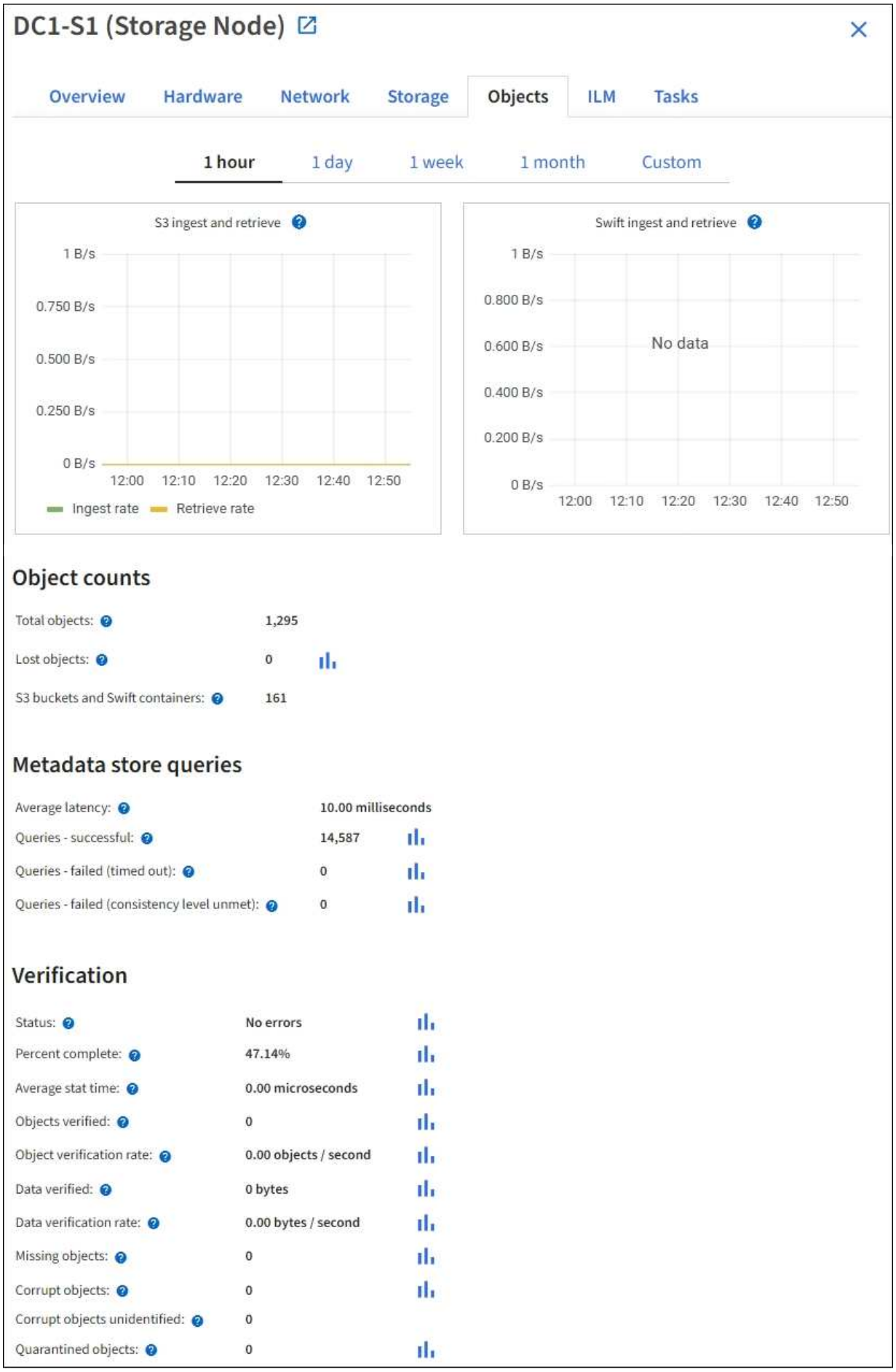
SG100 및 SG1000 서비스 어플라이언스

개체 탭을 봅니다

개체 탭은 에 대한 정보를 제공합니다 S3 및 스위프트 수집 및 검색 속도:

객체 탭은 각 스토리지 노드, 각 사이트 및 전체 그리드에 대해 표시됩니다. 스토리지 노드의 경우 오브젝트 탭에서는

메타데이터 쿼리 및 백그라운드 검증에 대한 개체 수와 정보도 제공합니다.

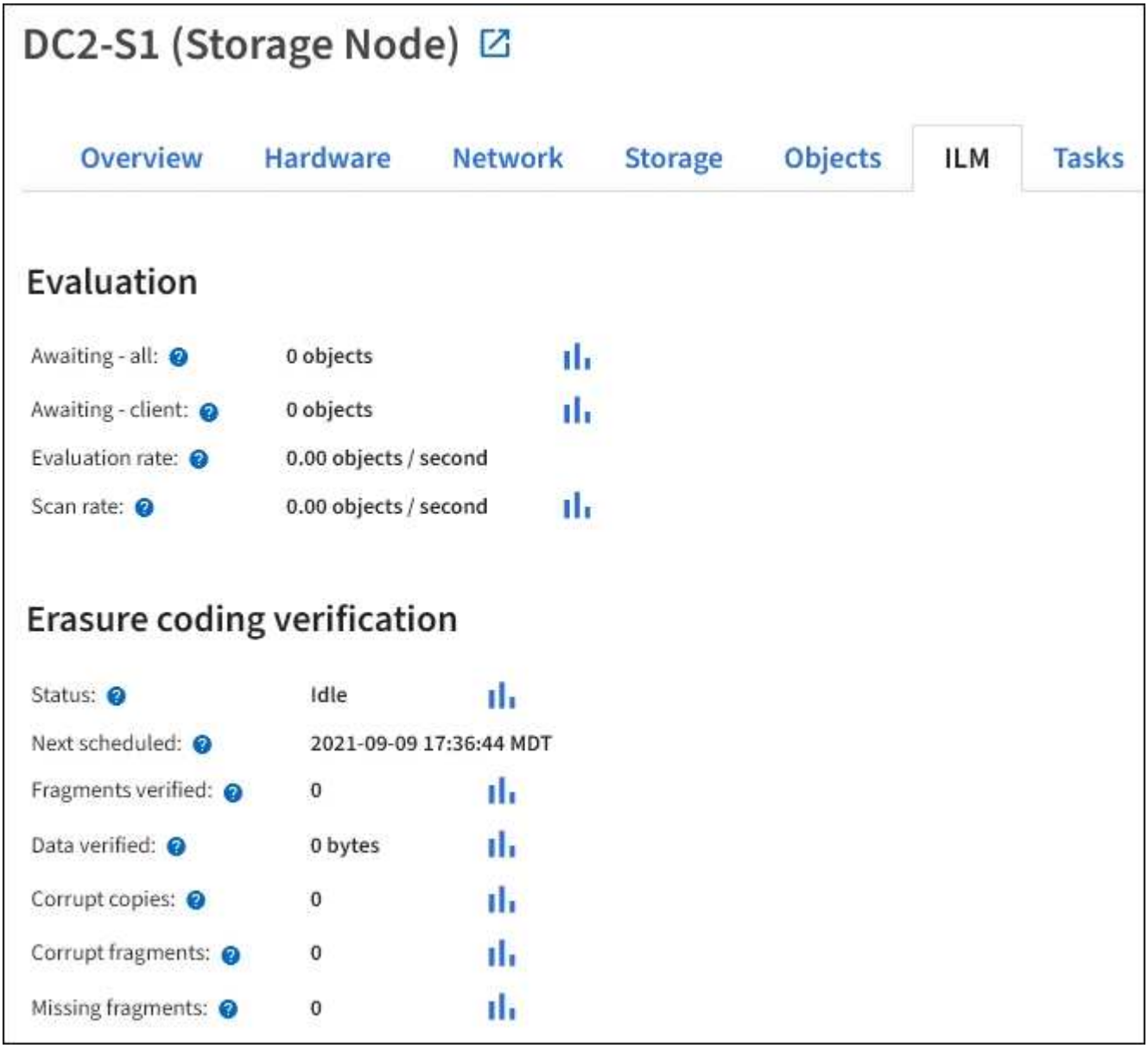

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
Average stat time: 0.00 microseconds
Objects verified: 0
Object verification rate: 0.00 objects / second
Data verified: 0 bytes
Data verification rate: 0.00 bytes / second
Missing objects: 0
Corrupt objects: 0
Corrupt objects unidentified: 0
Quarantined objects: 0

ILM 탭을 봅니다

ILM 탭은 ILM(정보 수명 주기 관리) 작업에 대한 정보를 제공합니다.

ILM 탭은 각 스토리지 노드, 각 사이트 및 전체 그리드에 대해 표시됩니다. 각 사이트 및 그리드에 대해 ILM 탭에는 시간 경과에 따른 ILM 대기열 그래프가 표시됩니다. 그리드의 경우 이 탭은 모든 개체의 전체 ILM 스캔을 완료하는 데 필요한 예상 시간을 제공합니다.

스토리지 노드의 경우 ILM 탭에서 삭제 코딩 개체에 대한 ILM 평가 및 백그라운드 검증에 대한 세부 정보를 제공합니다.



관련 정보

정보 수명 주기 관리를 모니터링합니다

StorageGRID 관리

부하 분산 탭을 봅니다

로드 밸런서 탭에는 로드 밸런서 서비스 작업과 관련된 성능 및 진단 그래프가 포함되어 있습니다.

부하 분산 탭은 관리 노드 및 게이트웨이 노드, 각 사이트 및 전체 그리드에 대해 표시됩니다. 각 사이트에 대해 부하 분산 탭은 해당 사이트의 모든 노드에 대한 통계를 집계한 요약을 제공합니다. 전체 그리드에서 로드 밸런서 탭은 모든 사이트에 대한 통계를 집계한 요약을 제공합니다.

로드 밸런서 서비스를 통해 실행되는 입출력이 없거나 로드 밸런서가 구성되지 않은 경우 그래프에 ""데이터 없음"이 표시됩니다.

교통 정보 요청

이 그래프는 로드 밸런서 끝점과 요청을 하는 클라이언트 간에 전송되는 데이터 처리량의 3분 이동 평균을 초당 비트 수로 제공합니다.

> 이 값은 각 요청이 완료될 때 업데이트됩니다. 따라서 이 값은 낮은 요청 속도에서의 실시간 처리량 또는 매우 오래 지속되는 요청과 다를 수 있습니다. 네트워크 탭을 보면 현재 네트워크 동작을 보다 사실적으로 볼 수 있습니다.

수신 요청율입니다

이 그래프는 초당 새 요청 수(GET, PUT, HEAD, DELETE)에 대한 3분의 이동 평균을 요청 유형(GET, PUT, HEAD, DELETE)별로 제공합니다. 이 값은 새 요청의 헤더가 검증되면 업데이트됩니다.

평균 요청 기간(오류 없음)

이 그래프는 요청 유형(GET, PUT, HEAD, DELETE)별로 분류되는 요청 지속 시간의 3분 이동 평균을 제공합니다. 각 요청 기간은 부하 분산 서비스에서 요청 헤더를 구문 분석할 때 시작되어 완전한 응답 본문이 클라이언트로 반환될 때 종료됩니다.

오류 응답 속도

이 그래프는 오류 응답 코드로 분할된 초당 클라이언트에 반환되는 오류 응답 수의 3분 이동 평균을 제공합니다.

관련 정보

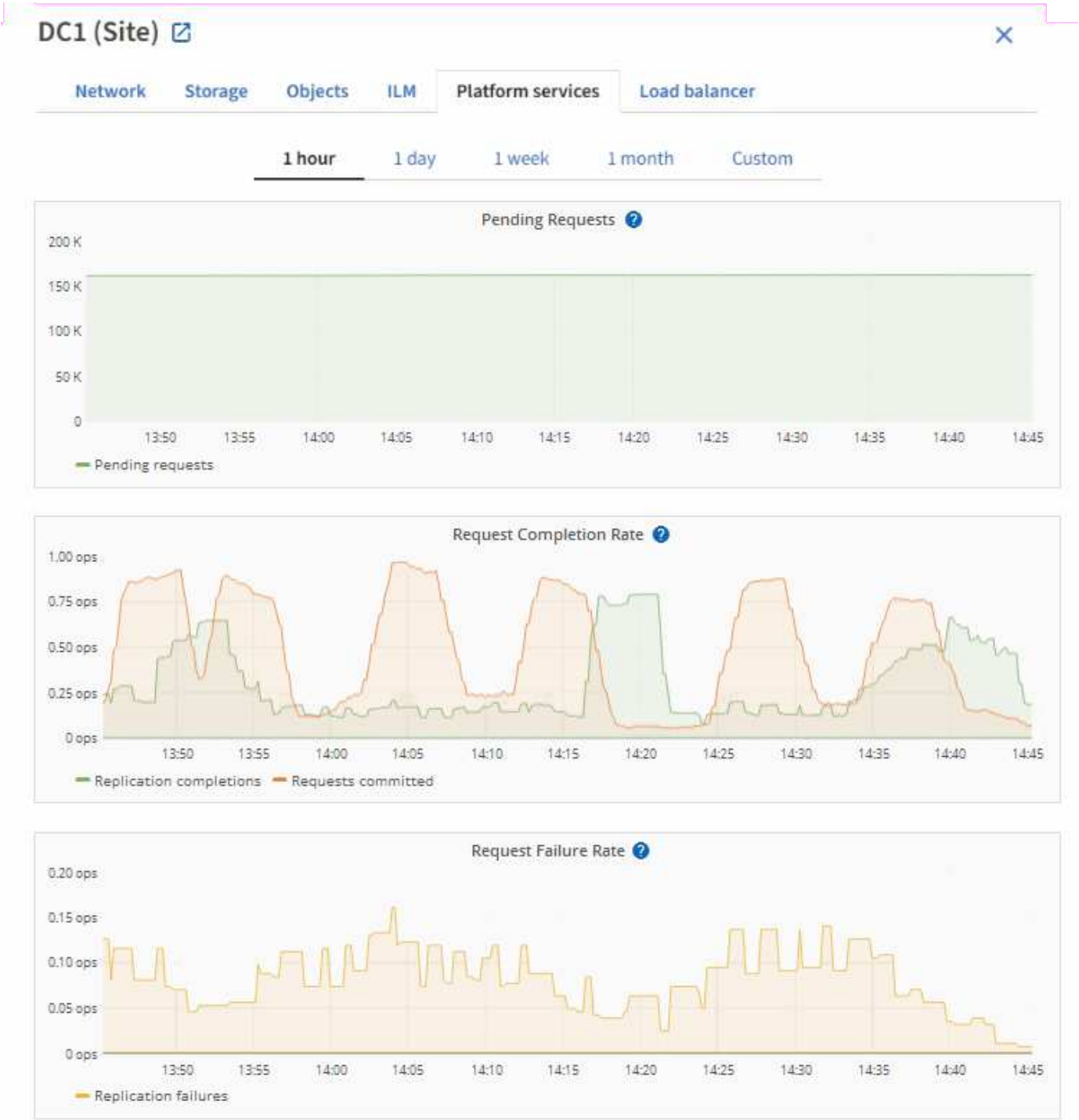
로드 밸런싱 작업을 모니터링합니다

StorageGRID 관리

플랫폼 서비스 탭을 봅니다

플랫폼 서비스 탭은 사이트의 S3 플랫폼 서비스 작업에 대한 정보를 제공합니다.

플랫폼 서비스 탭이 각 사이트에 표시됩니다. 이 탭은 CloudMirror 복제 및 검색 통합 서비스와 같은 S3 플랫폼 서비스에 대한 정보를 제공합니다. 이 탭의 그래프에는 보류 중인 요청 수, 요청 완료율, 요청 실패율 등의 메트릭이 표시됩니다.



문제 해결 정보를 포함한 S3 플랫폼 서비스에 대한 자세한 내용은 를 참조하십시오 StorageGRID 관리 지침.

SANtricity 시스템 관리자 탭을 봅니다

SANtricity 시스템 관리자 탭을 사용하면 스토리지 어플라이언스의 관리 포트를 구성하거나 연결하지 않고도 SANtricity 시스템 관리자에 액세스할 수 있습니다. 이 탭을 사용하여 하드웨어 진단 및 환경 정보와 드라이브 관련 문제를 검토할 수 있습니다.

스토리지 어플라이언스 노드에 대해 SANtricity System Manager 탭이 표시됩니다.

SANtricity 시스템 관리자를 사용하여 다음을 수행할 수 있습니다.

- 스토리지 어레이 레벨 성능, I/O 지연 시간, 스토리지 컨트롤러 CPU 활용률, 처리량과 같은 성능 데이터를 봅니다
- 하드웨어 구성 요소 상태를 확인합니다
- 진단 데이터 보기 및 E-Series AutoSupport 구성과 같은 지원 기능을 수행합니다

> SANtricity System Manager를 사용하여 E-Series AutoSupport의 프록시를 구성하려면 StorageGRID 관리 의 지침을 참조하십시오.

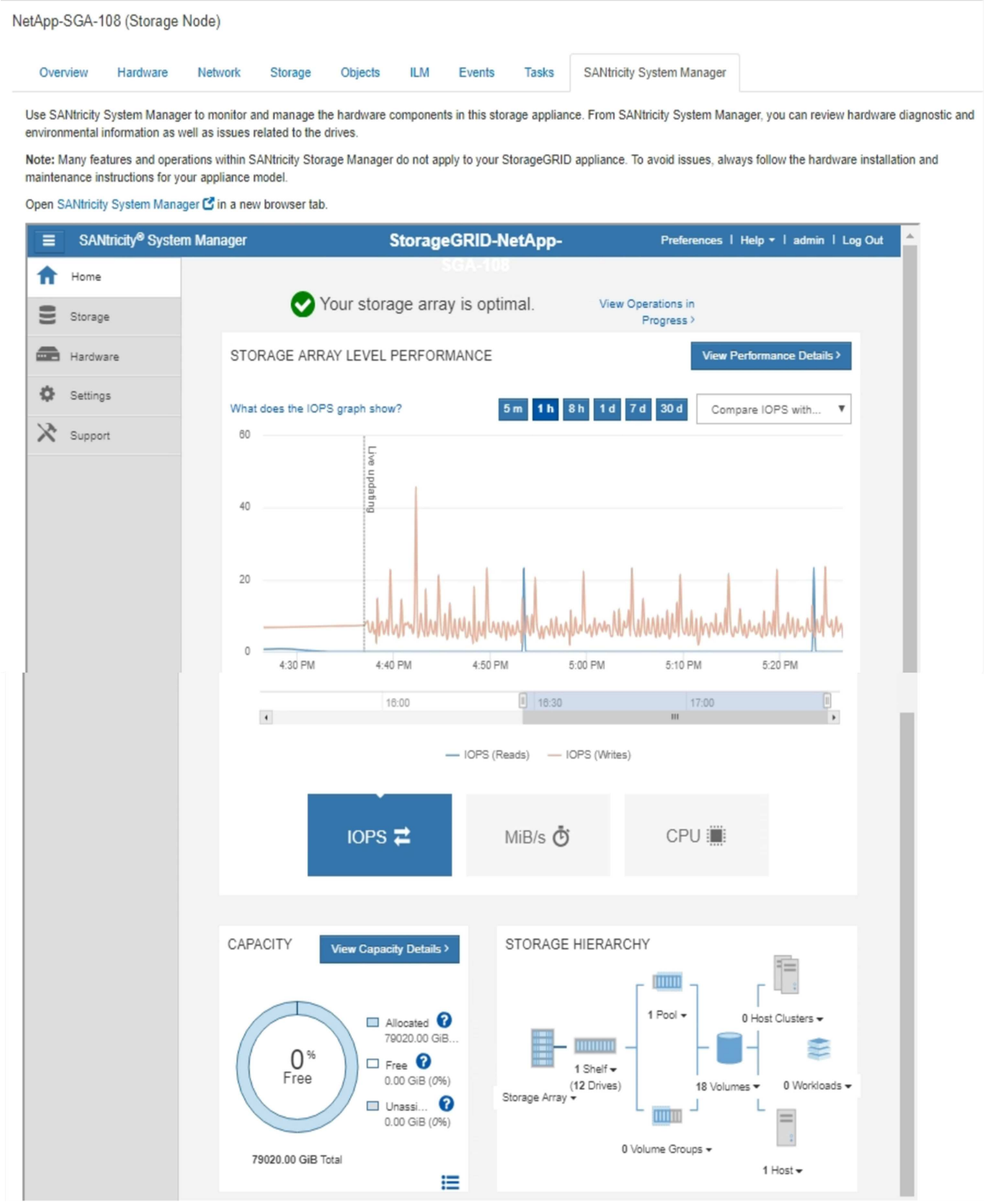
StorageGRID 관리

그리드 관리자를 통해 SANtricity 시스템 관리자에 액세스하려면 스토리지 어플라이언스 관리자 권한이나 루트 액세스 권한이 있어야 합니다.

> 그리드 관리자를 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 펌웨어 8.70(11.70) 이상이 있어야 합니다.

> 그리드 관리자에서 SANtricity 시스템 관리자에 액세스하는 것은 일반적으로 어플라이언스 하드웨어를 모니터링하고 E-Series AutoSupport를 구성하는 것만을 의미합니다. 펌웨어 업그레이드와 같은 SANtricity System Manager 내의 많은 기능과 작업은 StorageGRID 어플라이언스 모니터링에는 적용되지 않습니다. 문제를 방지하려면 항상 어플라이언스에 대한 하드웨어 설치 및 유지 관리 지침을 따르십시오.

이 탭에는 SANtricity 시스템 관리자의 홈 페이지가 표시됩니다.



SANtricity 시스템 관리자 링크를 사용하여 새 브라우저 창에서 SANtricity 시스템 관리자를 열어 보다 쉽게 볼 수 있습니다.

스토리지 시스템 레벨 성능 및 용량 사용량에 대한 세부 정보를 보려면 각 그래프 위에 커서를 놓습니다.

SANtricity 시스템 관리자 탭에서 액세스할 수 있는 정보를 보는 방법에 대한 자세한 내용은 를 참조하십시오 "NetApp E-Series 및 SANtricity 문서".

정기적으로 모니터링해야 하는 정보

StorageGRID는 오류가 발생하거나 노드 또는 사이트를 사용할 수 없는 경우에도 계속 작동하도록 설계된 내결함성 분산 스토리지 시스템입니다. 시스템 상태, 워크로드 및 사용 통계를 사전에 모니터링하여 잠재적인 문제가 그리드의 효율성 또는 가용성에 영향을 미치기 전에 이를 해결하기 위해 조치를 취해야 합니다.

사용량이 많은 시스템에서는 많은 양의 정보가 생성됩니다. 이 섹션에서는 지속적인 모니터링을 위한 가장 중요한 정보에 대한 지침을 제공합니다.

모니터링할 대상	주파수
를 클릭합니다 시스템 상태 데이터 그리드 관리자 대시보드에 표시됩니다. 이전 날부터 변경된 내용이 있으면 확인합니다.	매일
어느 것을 기준으로 레이팅 스토리지 노드 오브젝트 및 메타데이터 용량 사용 중입니다	매주
정보 수명 주기 관리 작업	매주
네트워크 연결 및 성능	매주
노드 레벨 리소스	매주
테넌트 작업	매주
외부 아카이브 스토리지 시스템의 용량입니다	매주
로드 밸런싱 작업	초기 설정 후 및 구성 변경 후
소프트웨어 핫픽스 및 소프트웨어 업그레이드 가용성	매월

시스템 상태를 모니터링합니다

StorageGRID 시스템의 전반적인 상태를 매일 모니터링해야 합니다.

이 작업에 대해

StorageGRID 시스템은 내결함성이 있으며 그리드의 일부를 사용할 수 없는 경우에도 계속 작동할 수 있습니다. StorageGRID 시스템에서 발생할 수 있는 문제의 첫 번째 징후는 경보 또는 경보(레거시 시스템)일 가능성이 높으며 시스템 작동에 문제가 있는 것은 아닙니다. 시스템 상태에 주의를 기울일 경우 운영 또는 그리드 효율성에 영향을 미치기 전에 사소한 문제를 감지하는 데 도움이 됩니다.

Grid Manager 대시보드의 상태 패널에서는 시스템에 영향을 줄 수 있는 문제에 대한 요약을 제공합니다. 대시보드에 표시되는 모든 문제를 조사해야 합니다.

알림이 트리거되는 즉시 알림을 받으려면 알림에 대한 e-메일 알림을 설정하거나 SNMP 트랩을 구성할 수 있습니다.

단계

1. Grid Manager에 로그인하여 대시보드를 봅니다.
2. Health(상태) 패널에서 정보를 검토합니다.

문제가 발생하면 추가 세부 정보를 볼 수 있는 링크가 나타납니다.

링크	를 나타냅니다
그리드 세부 정보	연결이 끊어진 노드가 있으면 나타납니다(연결 상태 알 수 없음 또는 관리 중단). 링크를 클릭하거나 파란색 또는 회색 아이콘을 클릭하여 영향을 받는 노드를 확인합니다.
현재 경고	현재 활성화된 알림이 있는 경우 나타납니다. 링크를 클릭하거나 * Critical *, * Major * 또는 * Minor * 를 클릭하여 * alerts * > * Current * 페이지에 대한 세부 정보를 확인합니다.
최근에 해결된 경고	지난 주에 트리거된 알림이 이제 해결된 경우 나타납니다. 링크를 클릭하면 * alerts * > * Resolved * 페이지에서 자세한 내용을 볼 수 있습니다.
라이센스	이 StorageGRID 시스템의 소프트웨어 라이센스에 문제가 있는 경우 나타납니다. 링크를 클릭하면 * 유지보수 * > * 시스템 * > * 라이센스 * 페이지에 대한 세부 정보를 볼 수 있습니다.

관련 정보

- StorageGRID 관리
- 알림에 대한 이메일 알림을 설정합니다
- SNMP 모니터링을 사용합니다

노드 연결 상태를 모니터링합니다

하나 이상의 노드가 그리드에서 분리되면 중요한 StorageGRID 작업이 영향을 받을 수

있습니다. 노드 연결 상태를 모니터링하고 문제를 즉시 해결해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

이 작업에 대해

노드는 다음 세 가지 연결 상태 중 하나일 수 있습니다.

- * 연결되지 않음 - 알 수 없음 * : 알 수 없는 이유로 노드가 그리드에 연결되어 있지 않습니다. 예를 들어, 노드 간 네트워크 연결이 끊어지거나 전원이 꺼졌습니다. 노드 * 와 통신할 수 없음 알림도 트리거될 수 있습니다. 다른 알림도 활성 상태일 수 있습니다. 이 상황은 즉각적인 주의가 필요합니다.

  > 관리되는 종료 작업 중에 노드가 알 수 없음으로 나타날 수 있습니다. 이러한 경우 알 수 없음 상태를 무시할 수 있습니다.

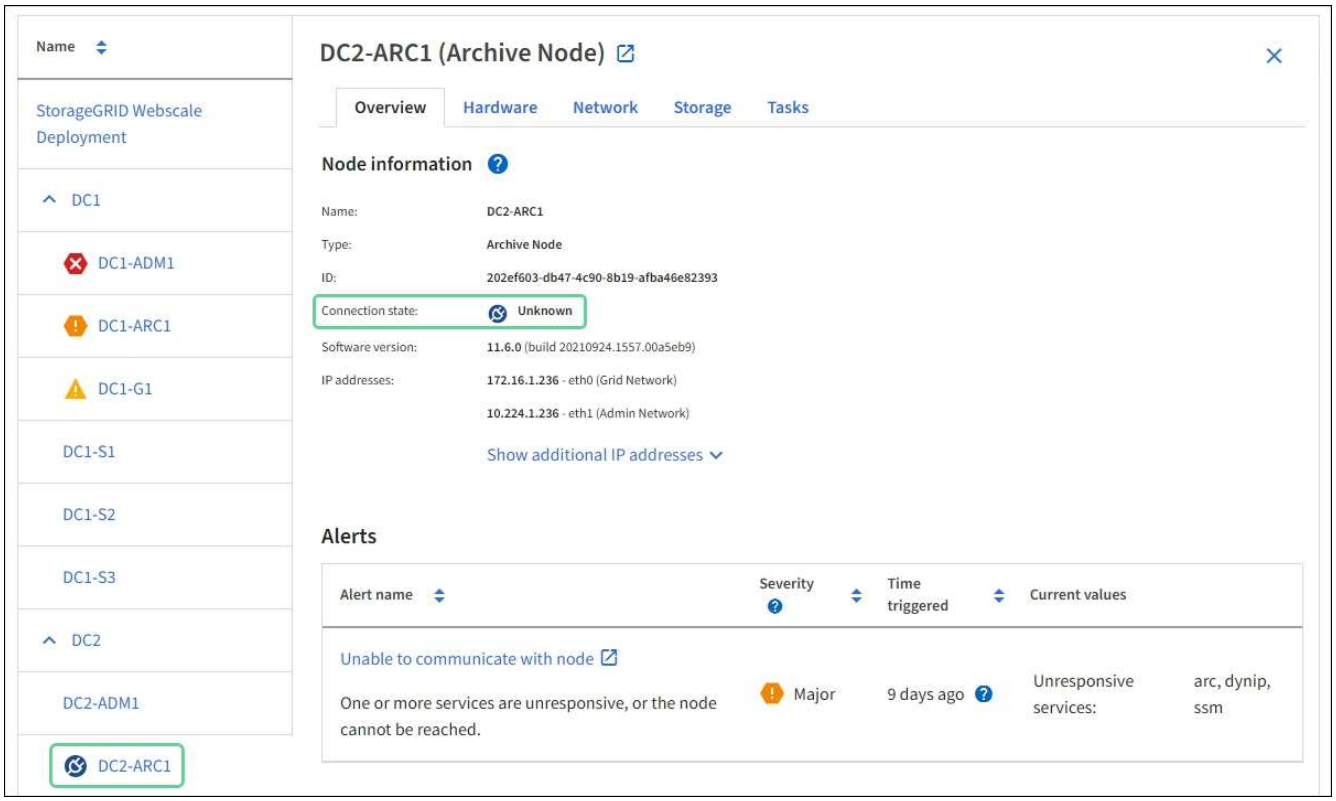
- * 연결되지 않음 - 관리 중단 * : 노드가 예상 이유로 그리드에 연결되어 있지 않습니다. 예를 들어, 노드의 노드 또는 서비스가 정상적으로 종료되었거나 노드가 재부팅 중이거나 소프트웨어가 업그레이드 중입니다. 하나 이상의 경고가 활성 상태일 수도 있습니다.
- * 연결됨 * : 노드가 그리드에 연결되어 있습니다.

단계

1. 대시보드의 상태 패널에 파란색 또는 회색 아이콘이 나타나면 아이콘을 클릭하거나 * Grid details * 를 클릭합니다. (파란색 또는 회색 아이콘과 * Grid details * 링크는 그리드에서 하나 이상의 노드가 분리된 경우에만 나타납니다.)

   노드 트리의 첫 번째 파란색 노드에 대한 개요 페이지가 나타납니다. 파란색 노드가 없으면 트리의 첫 번째 회색 노드에 대한 개요 페이지가 나타납니다.

   이 예에서는 DC1-S3라는 스토리지 노드에 파란색 아이콘이 있습니다. 노드 정보 패널의 * 연결 상태 * 는 * 알 수 없음 * 이고 * 노드 * 와 통신할 수 없음 경고가 활성화됩니다. 이 알림은 하나 이상의 서비스가 응답하지 않거나 노드에 연결할 수 없음을 나타냅니다.



2. 노드에 파란색 아이콘이 있는 경우 다음 단계를 수행하십시오.
   a. 표에서 각 경고를 선택하고 권장 조치를 따릅니다.

      예를 들어, 노드의 호스트를 중지하거나 다시 시작한 서비스를 다시 시작해야 할 수 있습니다.

   b. 노드를 다시 온라인 상태로 전환할 수 없는 경우 기술 지원 팀에 문의하십시오.
3. 노드에 회색 아이콘이 있는 경우 다음 단계를 수행합니다.

   회색 노드는 유지보수 절차 중에 예상되며 하나 이상의 경고와 연결될 수 있습니다. 이 문제의 근원적 근거를 토대로 이러한 "관리적 중단" 노드는 대개 아무런 개입 없이 온라인 상태로 돌아갑니다.

   a. Alerts 섹션을 검토하고 이 노드에 영향을 주는 알림이 있는지 확인합니다.
   b. 하나 이상의 경고가 활성화된 경우 표에서 각 경고를 선택하고 권장 조치를 따릅니다.
   c. 노드를 다시 온라인 상태로 전환할 수 없는 경우 기술 지원 팀에 문의하십시오.

관련 정보

경고 참조

복구 및 유지 관리

현재 경고를 봅니다

경고가 트리거되면 경고 아이콘이 대시보드에 표시됩니다. 노드 페이지의 노드에 대한 알림 아이콘도 표시됩니다. 경고가 소거되지 않은 경우 이메일 알림도 전송될 수 있습니다.

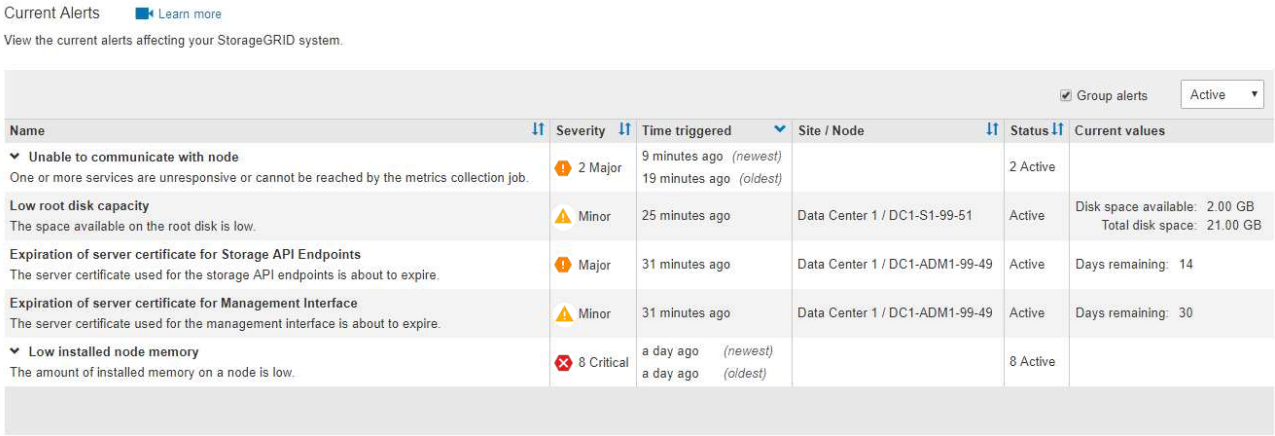
필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 선택적으로 비디오를 시청했습니다. "비디오: 경고 개요".

단계

1. 하나 이상의 경고가 활성화된 경우 다음 중 하나를 수행합니다.
   - 대시보드의 상태 패널에서 경고 아이콘을 클릭하거나 * 현재 경고 * 를 클릭합니다. (경고 아이콘과 * 현재 경고 * 링크는 현재 하나 이상의 경고가 활성화된 경우에만 나타납니다.)
   - alerts * > * current * 를 선택합니다.

     현재 경고 페이지가 나타납니다. 현재 StorageGRID 시스템에 영향을 주는 모든 알림이 나열됩니다.



     기본적으로 경고는 다음과 같이 표시됩니다.

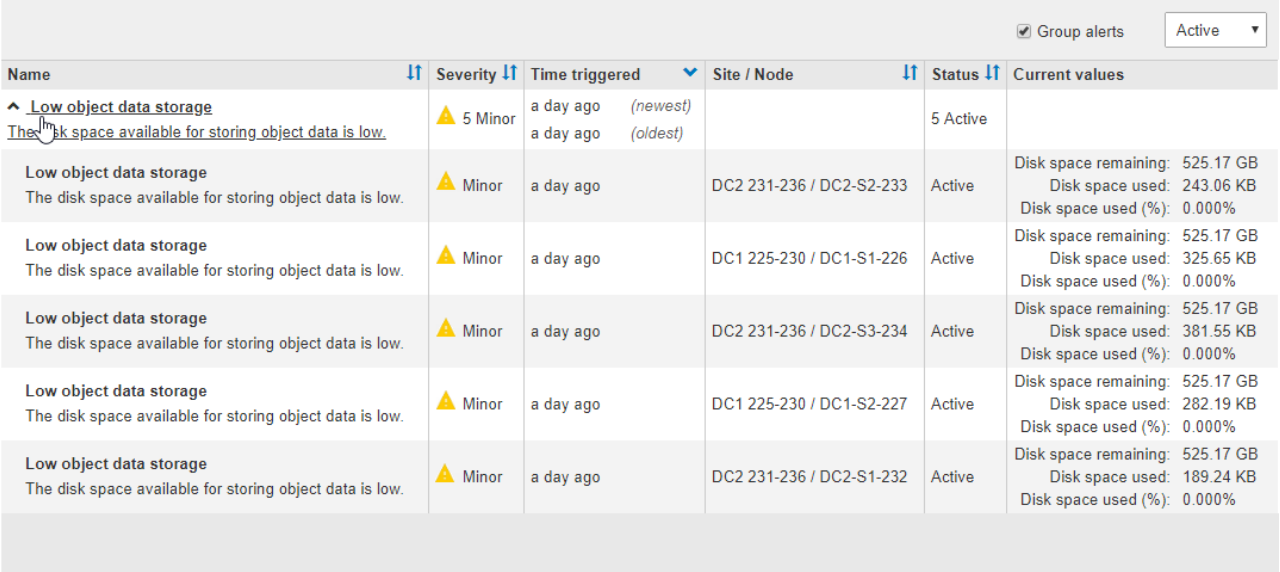
   - 가장 최근에 트리거된 경고가 먼저 표시됩니다.
   - 동일한 유형의 여러 알림이 그룹으로 표시됩니다.
   - 해제된 알림은 표시되지 않습니다.
   - 특정 노드의 특정 경고에 대해 둘 이상의 심각도에 대한 임계값에 도달하면 가장 심각한 알림만 표시됩니다. 즉, Minor, Major 및 Critical 심각도에 대한 경고 임계값에 도달하면 Critical 경고만 표시됩니다.

현재 경고 페이지는 2분마다 새로 고쳐집니다.

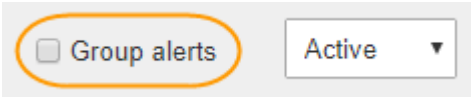
2. 표의 정보를 검토합니다.

열 머리글	설명
이름	알림의 이름과 설명입니다.
심각도입니다	알림의 심각도입니다. 여러 개의 경고가 그룹화되면 제목 행에 각 심각도에 대해 발생한 해당 경고의 인스턴스 수가 표시됩니다. • * 심각 * : StorageGRID 노드나 서비스의 정상적인 작동을 중지해 온 비정상적인 조건이 존재합니다. 기본 문제를 즉시 해결해야 합니다. 문제가 해결되지 않으면 서비스가 중단되거나 데이터가 손실될 수 있습니다. • * 주 * : 현재 작업에 영향을 미치거나 위험 경고에 대한 임계값에 근접한 비정상적인 상태가 존재합니다. StorageGRID 노드나 서비스의 정상 작동을 비정상적인 상태로 중지하지 않도록 주요 경고를 조사하고 모든 기본 문제를 해결해야 합니다. • * 보조 * : 시스템이 정상적으로 작동하지만 시스템이 계속 작동할 경우 시스템 기능에 영향을 줄 수 있는 비정상적인 상태가 존재합니다. 보다 심각한 문제를 초래하지 않도록 자체적으로 명확하지 않은 사소한 경고를 모니터링하고 해결해야 합니다.
시간 트리거됨	알림이 트리거된 지 얼마 전입니다. 여러 개의 경고가 그룹화되면 제목 행에 경고의 가장 최근 인스턴스(/최신형)와 가장 오래된 인스턴스(*oldest*)에 대한 시간이 표시됩니다.
사이트/노드	알림이 발생하는 사이트 및 노드의 이름입니다. 여러 개의 알림이 그룹화되면 사이트 및 노드 이름이 제목 행에 표시되지 않습니다.
상태	경고가 활성 상태인지 또는 해제되었는지 여부 여러 개의 경고가 그룹화되고 드롭다운에서 * All alerts * 를 선택하면 제목 행에 해당 경고의 활성 인스턴스 수와 해제된 인스턴스 수가 표시됩니다.
현재 값	알림이 트리거된 메트릭의 현재 값입니다. 일부 경고의 경우 경고를 이해하고 조사하는 데 도움이 되는 추가 값이 표시됩니다. 예를 들어 * Low object data storage * 알림에 표시되는 값에는 사용된 디스크 공간의 비율, 총 디스크 공간 및 사용된 디스크 공간의 양이 포함됩니다. • 참고: * 여러 개의 경고가 그룹화되어 있으면 제목 행에 현재 값이 표시되지 않습니다.

3. 알림 그룹을 확장하고 축소하려면:
   - 그룹에 개별 경고를 표시하려면 아래쪽 캐럿을 클릭합니다 ⌄ 제목에서 그룹 이름을 클릭합니다.
   - 그룹의 개별 경고를 숨기려면 위쪽 캐럿을 클릭합니다 ⌃ 제목에서 그룹 이름을 클릭합니다.



4. 경고 그룹 대신 개별 경고를 표시하려면 테이블 상단의 * Group alerts * (그룹 알림 *) 확인란을 선택 취소합니다.



5. 경고 또는 경고 그룹을 정렬하려면 위/아래 화살표를 클릭합니다 ⇅ 각 열 머리글에서.
   - Group alerts * 를 선택하면 각 그룹 내의 알림 그룹과 개별 경고가 모두 정렬됩니다. 예를 들어 특정 경고의 가장 최근 인스턴스를 찾기 위해 * 시간 트리거 * 를 기준으로 그룹의 경고를 정렬할 수 있습니다.
   - Group alerts * 를 선택 취소하면 전체 경고 목록이 정렬됩니다. 예를 들어, 특정 노드에 영향을 주는 모든 경고를 보기 위해 * 노드/사이트 * 별로 모든 경고를 정렬할 수 있습니다.
6. 상태를 기준으로 경고를 필터링하려면 테이블 상단의 드롭다운 메뉴를 사용합니다.

   - 모든 현재 경고를 보려면 * All alerts * (모든 경고 *)를 선택합니다(활성 및 해제 경고 모두).
   - 활성 상태인 현재 경고만 보려면 * Active * 를 선택합니다.
   - 해제된 현재 경고만 보려면 * Silenced * 를 선택합니다. 을 참조하십시오 알림 메시지를 해제합니다.
7. 특정 경고에 대한 세부 정보를 보려면 테이블에서 경고를 선택합니다.

   경고에 대한 대화 상자가 나타납니다. 을 참조하십시오 특정 경고를 봅니다.

해결된 경고를 봅니다

해결된 알림의 기록을 검색하고 볼 수 있습니다.

필요한 것

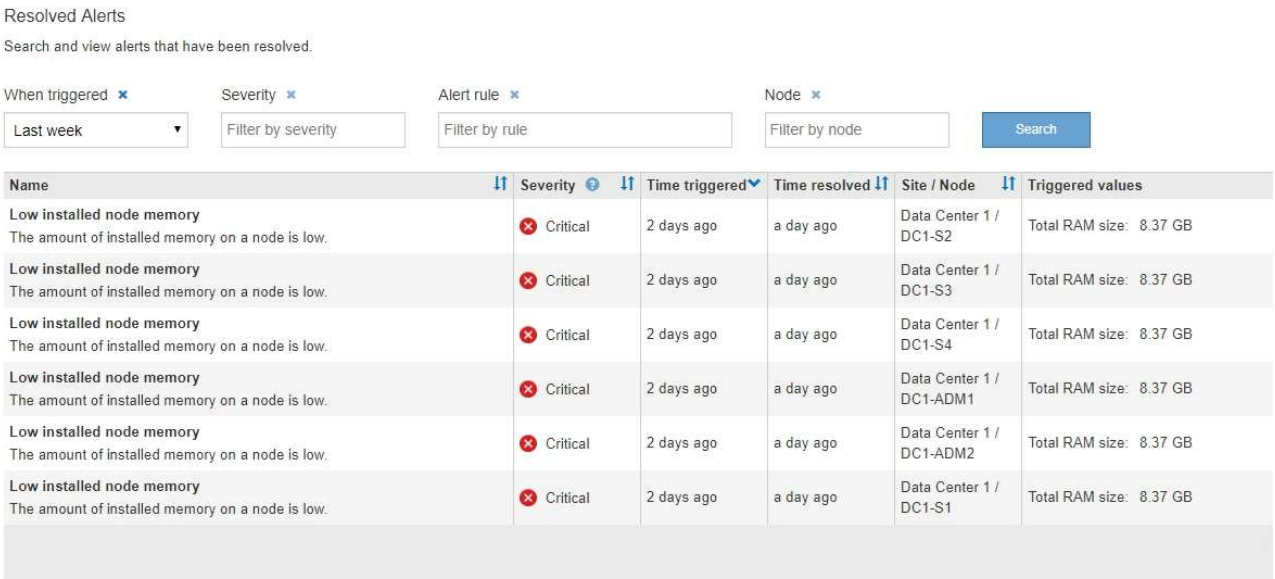
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

단계

1. 해결된 알림을 보려면 다음 중 하나를 수행합니다.
   - 대시보드의 상태 패널에서 * Recently Resolved alerts * 를 클릭합니다.

     최근 해결된 경고 * 링크는 지난 주 동안 하나 이상의 경고가 트리거되어 현재 해결된 경우에만 나타납니다.

   - alerts * > * Resolved * 를 선택합니다. 해결된 경고 페이지가 나타납니다. 기본적으로 지난 주에 트리거된 해결된 알림이 표시되고 가장 최근에 트리거된 알림이 먼저 표시됩니다. 이 페이지의 경고는 이전에 현재 알림 페이지 또는 이메일 알림에 표시되었습니다.



2. 표의 정보를 검토합니다.

열 머리글	설명
이름	알림의 이름과 설명입니다.

열 머리글	설명
심각도입니다	알림의 심각도입니다. • * 심각 * : StorageGRID 노드나 서비스의 정상적인 작동을 중지해 온 비정상적인 조건이 존재합니다. 기본 문제를 즉시 해결해야 합니다. 문제가 해결되지 않으면 서비스가 중단되거나 데이터가 손실될 수 있습니다. • * 주 * : 현재 작업에 영향을 미치거나 위험 경고에 대한 임계값에 근접한 비정상적인 상태가 존재합니다. StorageGRID 노드나 서비스의 정상 작동을 비정상적인 상태로 중지하지 않도록 주요 경고를 조사하고 모든 기본 문제를 해결해야 합니다. • * 보조 * : 시스템이 정상적으로 작동하지만 시스템이 계속 작동할 경우 시스템 기능에 영향을 줄 수 있는 비정상적인 상태가 존재합니다. 보다 심각한 문제를 초래하지 않도록 자체적으로 명확하지 않은 사소한 경고를 모니터링하고 해결해야 합니다.
시간 트리거됨	알림이 트리거된 지 얼마 전입니다.
시간이 해결되었습니다	알림이 해결된 지 얼마 전입니다.
사이트/노드	알림이 발생한 사이트 및 노드의 이름입니다.
트리거된 값	알림이 트리거된 메트릭 값입니다. 일부 경고의 경우 경고를 이해하고 조사하는 데 도움이 되는 추가 값이 표시됩니다. 예를 들어 * Low object data storage * 알림에 표시되는 값에는 사용된 디스크 공간의 비율, 총 디스크 공간 및 사용된 디스크 공간의 양이 포함됩니다.

3. 해결된 알림의 전체 목록을 정렬하려면 위쪽/아래쪽 화살표를 클릭합니다 ⇅ 각 열 머리글에서.

   예를 들어, 특정 노드에 영향을 미치는 경고를 보려면 * 사이트/노드 * 별로 해결된 경고를 정렬할 수 있습니다.

4. 필요에 따라 테이블 상단의 드롭다운 메뉴를 사용하여 해결된 경고 목록을 필터링합니다.
   a. 트리거된 시간 * 드롭다운 메뉴에서 기간을 선택하여 트리거된 기간에 따라 해결된 경고를 표시합니다.

      다음 기간 내에 트리거된 알림을 검색할 수 있습니다.

      - 지난 시간
      - 마지막 날
      - 지난 주(기본 보기)
      - 지난 달

    - 모든 기간
    - 사용자 지정(기간의 시작 날짜와 종료 날짜를 지정할 수 있음)

  b. 심각도* 드롭다운 메뉴에서 하나 이상의 심각도를 선택하여 특정 심각도에 대한 해결된 경고를 필터링합니다.

  c. 경고 규칙 * 드롭다운 메뉴에서 하나 이상의 기본 또는 사용자 지정 경고 규칙을 선택하여 특정 경고 규칙과 관련된 해결된 경고를 필터링합니다.

  d. 노드 * 드롭다운 메뉴에서 하나 이상의 노드를 선택하여 특정 노드와 관련된 해결된 경고를 필터링합니다.

  e. 검색 * 을 클릭합니다.

5. 해결된 특정 경고에 대한 세부 정보를 보려면 테이블에서 경고를 선택합니다.

   경고에 대한 대화 상자가 나타납니다. 을 참조하십시오 특정 경고를 봅니다.

특정 경고를 봅니다

현재 StorageGRID 시스템에 영향을 미치는 알림 또는 해결된 알림에 대한 자세한 정보를 볼 수 있습니다. 세부 정보에는 권장 수정 조치, 알림이 트리거된 시간, 이 경고와 관련된 메트릭의 현재 값이 포함됩니다.

필요에 따라 할 수 있습니다 현재 경고를 해제합니다 또는 알림 규칙을 업데이트합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

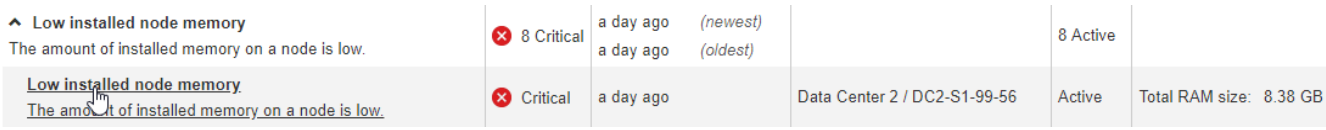
단계

1. 현재 또는 해결된 알림을 표시할지 여부에 따라 다음 중 하나를 수행합니다.

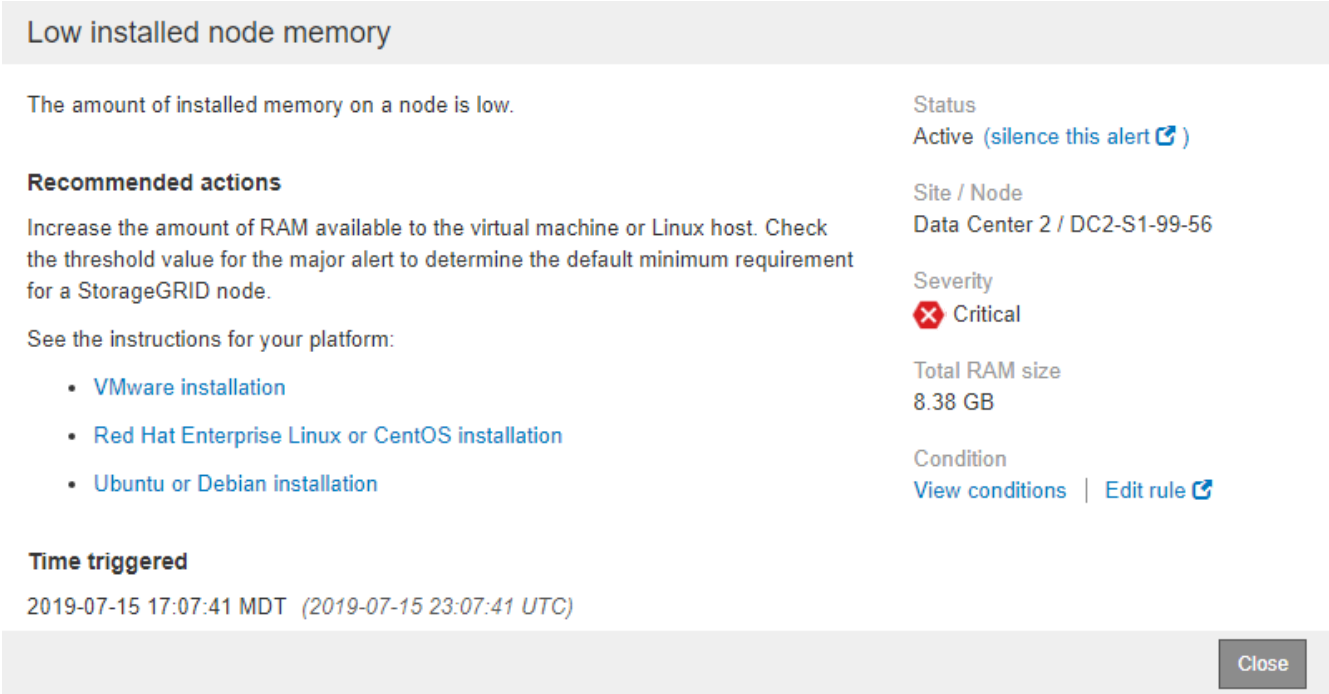
열 머리글	설명
현재 경고	• 대시보드의 상태 패널에서 * Current alerts * 링크를 클릭합니다. 이 링크는 현재 하나 이상의 경고가 활성화된 경우에만 나타납니다. 현재 경고가 없거나 모든 현재 경고가 해제된 경우 이 링크가 표시되지 않습니다. • alerts * > * current * 를 선택합니다. • nodes * 페이지에서 경고 아이콘이 있는 노드의 * Overview * 탭을 선택합니다. 그런 다음 알림 섹션에서 알림 이름을 클릭합니다.
해결된 경고	• 대시보드의 상태 패널에서 * Recently Resolved alerts * 링크를 클릭합니다. (이 링크는 지난 주 동안 하나 이상의 경고가 트리거되어 현재 해결된 경우에만 나타납니다. 지난 주에 트리거되어 해결된 알림이 없으면 이 링크가 표시되지 않습니다.) • alerts * > * Resolved * 를 선택합니다.

2. 필요에 따라 알림 그룹을 확장한 다음 확인할 알림을 선택합니다.

   알림 그룹의 제목이 아닌 알림을 선택합니다.



선택한 알림에 대한 세부 정보를 제공하는 대화 상자가 나타납니다.



3. 경고 세부 정보를 검토합니다.

정보	설명
제목 _	알림의 이름입니다.
_첫 번째 단락 _	알림에 대한 설명입니다.
권장 조치	이 알림에 대한 권장 조치입니다.
시간 트리거됨	현지 시간 및 UTC에서 알림이 트리거된 날짜 및 시간입니다.
시간이 해결되었습니다	해결된 알림의 경우 현지 시간 및 UTC에서 알림이 해결된 날짜 및 시간입니다.
상태	알림의 상태: 활성, 해제 또는 해결됨
사이트/노드	알림의 영향을 받는 사이트 및 노드의 이름입니다.

정보	설명
심각도입니다	알림의 심각도입니다. • * 심각 * : StorageGRID 노드나 서비스의 정상적인 작동을 중지해 온 비정상적인 조건이 존재합니다. 기본 문제를 즉시 해결해야 합니다. 문제가 해결되지 않으면 서비스가 중단되거나 데이터가 손실될 수 있습니다. • * 주 * : 현재 작업에 영향을 미치거나 위험 경고에 대한 임계값에 근접한 비정상적인 상태가 존재합니다. StorageGRID 노드나 서비스의 정상 작동을 비정상적인 상태로 중지하지 않도록 주요 경고를 조사하고 모든 기본 문제를 해결해야 합니다. • * 보조 * : 시스템이 정상적으로 작동하지만 시스템이 계속 작동할 경우 시스템 기능에 영향을 줄 수 있는 비정상적인 상태가 존재합니다. 보다 심각한 문제를 초래하지 않도록 자체적으로 명확하지 않은 사소한 경고를 모니터링하고 해결해야 합니다.
_데이터 값 _	이 알림에 대한 메트릭의 현재 값입니다. 일부 경고의 경우 경고를 이해하고 조사하는 데 도움이 되는 추가 값이 표시됩니다. 예를 들어, * Low Metadata Storage * 경고에 대해 표시되는 값에는 사용된 디스크 공간의 비율, 총 디스크 공간 및 사용된 디스크 공간의 양이 포함됩니다.

4. 선택적으로 * 이 경고 해제 * 를 클릭하여 이 경고가 트리거되도록 한 경고 규칙을 해제합니다.

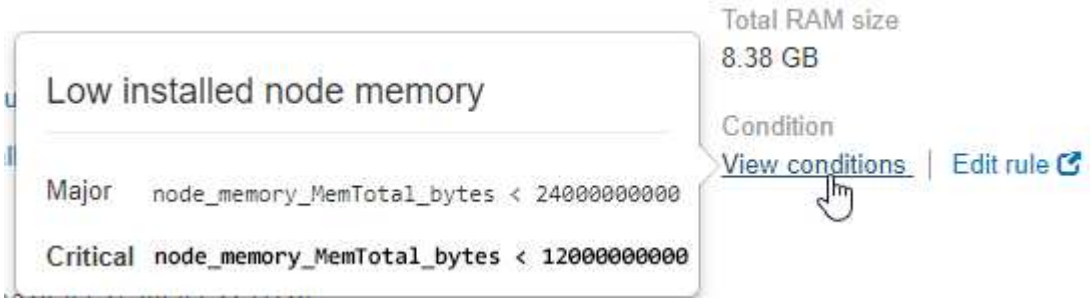
   알림 규칙을 해제하려면 알림 관리 또는 루트 액세스 권한이 있어야 합니다.

   > 경고 규칙을 해제할 때는 주의하십시오. 경고 규칙이 해제된 경우 중요한 작업이 완료되지 못하도록 하기 전까지는 기본 문제를 감지하지 못할 수 있습니다.

5. 알림 규칙의 현재 조건을 보려면:

   a. 경고 세부 정보에서 * 조건 보기 * 를 클릭합니다.

      정의된 각 심각도에 대한 Prometheus 표현식이 나열된 팝업이 나타납니다.



   a. 팝업을 닫으려면 팝업 외부의 아무 곳이나 클릭합니다.

6. 필요에 따라 * 규칙 편집 * 을 클릭하여 이 경고가 트리거되도록 한 경고 규칙을 편집합니다.

   알림 규칙을 편집하려면 알림 관리 또는 루트 액세스 권한이 있어야 합니다.

알림 규칙을 편집하기로 결정할 때는 주의해야 합니다. 트리거 값을 변경하는 경우 중요한 작업이 완료되지 못할 때까지 기본 문제를 감지하지 못할 수 있습니다.

7. 경고 세부 정보를 닫으려면 * 닫기 * 를 클릭합니다.

레거시 알람을 봅니다

알람(레거시 시스템)은 시스템 속성이 알람 임계값에 도달할 때 트리거됩니다. Current Alarms(현재 알람) 페이지에서 현재 활성화된 알람을 볼 수 있습니다.

기존 알람 시스템은 계속 지원되지만, 알림 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

단계

1. 지원 * > * 알람(레거시) * > * 현재 알람 * 을 선택합니다.

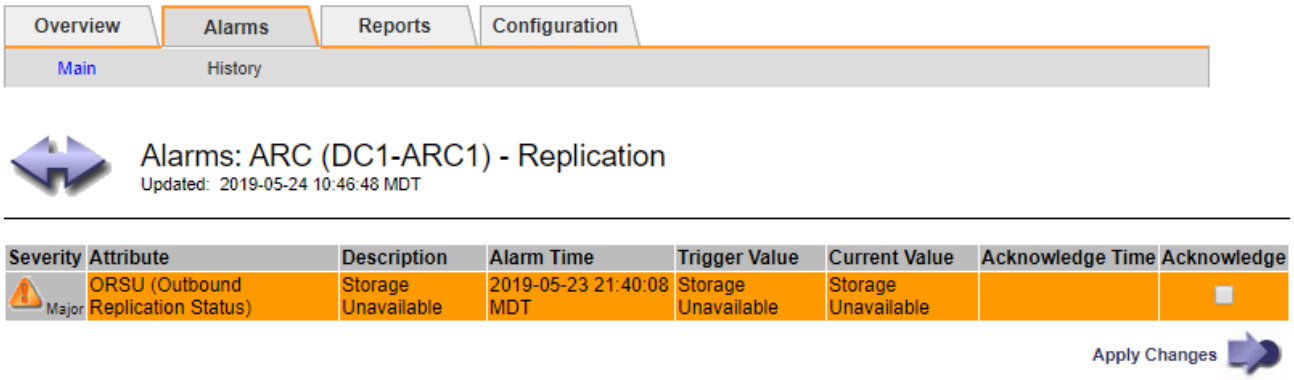
알람 아이콘은 각 알람의 심각도를 다음과 같이 나타냅니다.

아이콘을 클릭합니다	색상	알람 심각도입니다	의미
	노란색	주의	노드가 그리드에 연결되어 있지만 정상적인 작동에 영향을 주지 않는 비정상적인 상태가 존재합니다.
	연한 주황색	경미합니다	노드가 그리드에 연결되어 있지만 향후 운영에 영향을 미칠 수 있는 비정상적인 조건이 존재합니다. 에스컬레이션을 방지하려면 조사해야 합니다.
	진한 주황색	전공	노드가 그리드에 연결되어 있지만 현재 작업에 영향을 미치는 비정상적인 상태가 존재합니다. 에스컬레이션을 방지하려면 즉각적인 주의가 필요합니다.

아이콘을 클릭합니다	색상	알람 심각도입니다	의미
✕	빨간색	심각	노드가 그리드에 연결되었지만 정상 작동을 중지한 비정상적인 조건이 존재합니다. 문제를 즉시 해결해야 합니다.

2. 알람이 트리거된 속성에 대해 알아보려면 테이블에서 속성 이름을 마우스 오른쪽 버튼으로 클릭합니다.
3. 알람에 대한 추가 세부 정보를 보려면 표에서 서비스 이름을 클릭합니다.

   선택한 서비스에 대한 경보 탭이 나타납니다(* 지원 * > * 도구 * > * 그리드 토폴로지 * > *그리드 노드 _ * > *_서비스 * > * 경보 *).



4. 현재 알람의 개수를 지우려면 다음을 수행할 수도 있습니다.
   - 알람을 확인합니다. 확인된 알람은 다음 심각도 수준에서 트리거되거나 해결되었다가 다시 발생하지 않는 한 기존 알람의 개수에 더 이상 포함되지 않습니다.
   - 특정 기본 알람 또는 전체 시스템에 대한 전체 사용자 정의 알람을 비활성화하여 다시 트리거되지 않도록 합니다.

관련 정보

알람 기준(레거시 시스템)

현재 알람 확인(레거시 시스템)

알람 비활성화(기존 시스템)

스토리지 용량을 모니터링합니다

사용 가능한 총 공간을 모니터링하여 StorageGRID 시스템에 오브젝트 또는 오브젝트 메타데이터의 스토리지 공간이 부족하지 않은지 확인합니다.

StorageGRID는 오브젝트 데이터와 오브젝트 메타데이터를 별도로 저장하며 오브젝트 메타데이터를 포함하는 분산된 Cassandra 데이터베이스에 대한 특정 양의 공간을 예약합니다. 오브젝트 및 오브젝트 메타데이터에 사용되는 총 공간의 양과 각 오브젝트에 사용되는 공간 추세를 모니터링합니다. 따라서 노드를 추가하기 전에 미리 계획하고 서비스 중단을 방지할 수 있습니다.

가능합니다 스토리지 용량 정보를 봅니다 전체 그리드, 각 사이트 및 StorageGRID 시스템의 각 스토리지 노드에 대해

전체 그리드에 대한 스토리지 용량을 모니터링합니다

그리드의 전체 스토리지 용량을 모니터링하여 오브젝트 데이터 및 오브젝트 메타데이터에 대한 충분한 여유 공간이 유지되도록 해야 합니다. 시간이 지남에 따라 스토리지 용량이 변경되는 방식을 이해하면 그리드의 가용 스토리지 용량이 소비되기 전에 스토리지 노드 또는 스토리지 볼륨을 추가할 계획을 세울 수 있습니다.

필요한 것

를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

이 작업에 대해

Grid Manager의 대시보드를 사용하면 전체 그리드와 각 데이터 센터에 대해 사용 가능한 스토리지 양을 신속하게 평가할 수 있습니다. 노드 페이지에서는 오브젝트 데이터 및 오브젝트 메타데이터에 대한 자세한 값을 제공합니다.

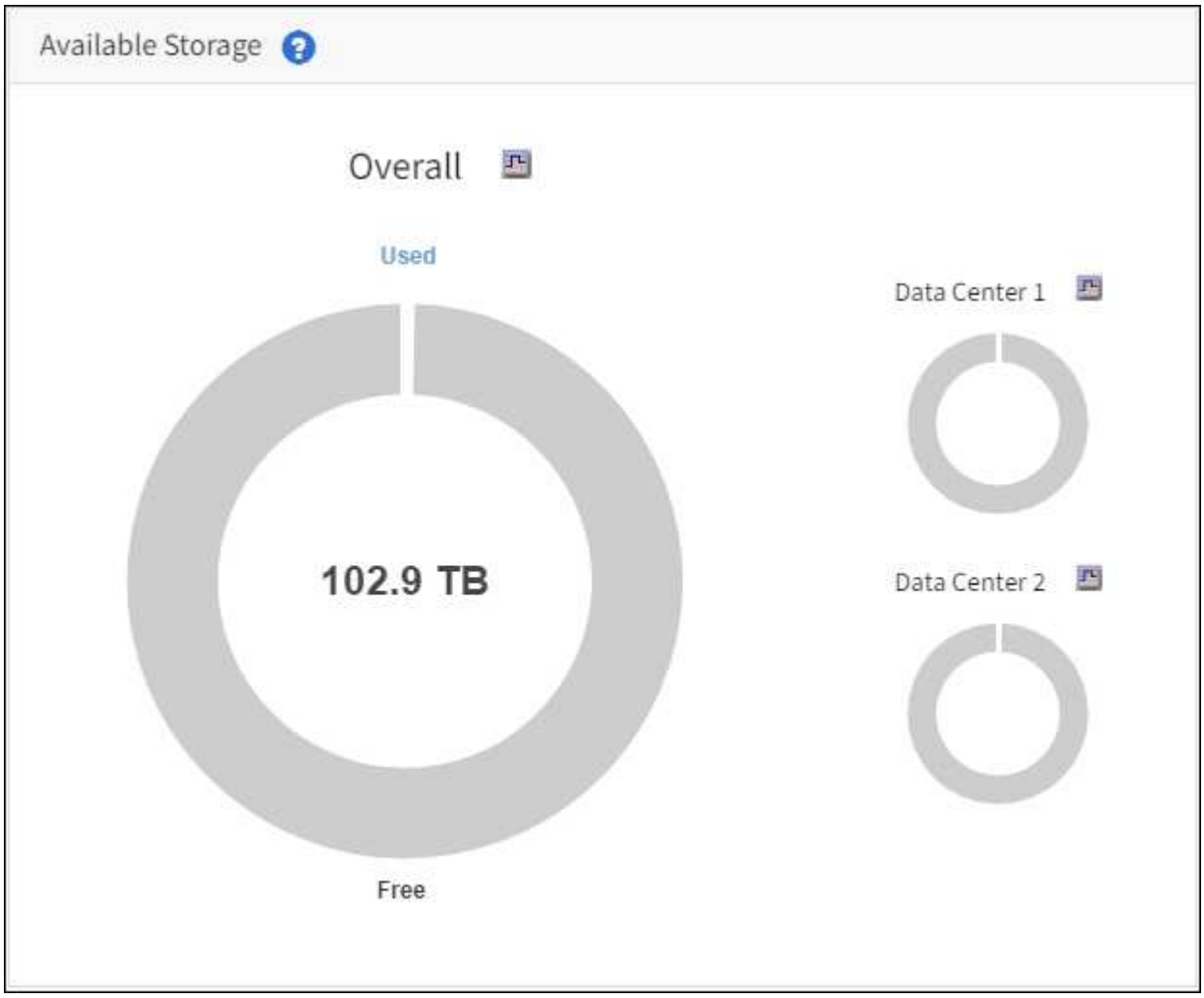
단계

1. 전체 그리드 및 각 데이터 센터에 사용할 수 있는 스토리지 양을 평가합니다.

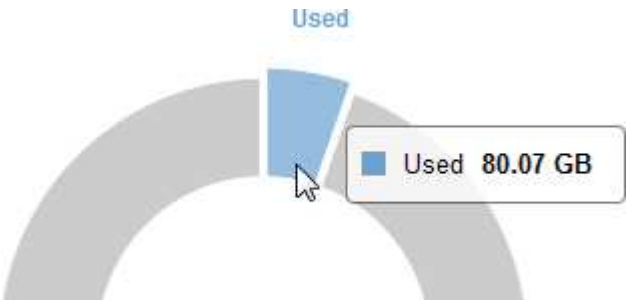
   a. 대시보드 * 를 선택합니다.

   b. Available Storage(사용 가능한 스토리지) 패널에서 사용 가능한 스토리지 용량과 사용된 스토리지 용량의 전체 요약을 확인합니다.

   요약에는 아카이브 미디어가 포함되지 않습니다.



a. 차트의 Free(여유) 또는 Used Capacity(사용된 용량) 섹션 위에 커서를 놓으면 사용 가능한 공간 또는 사용된 공간을 정확하게 확인할 수 있습니다.



b. 다중 사이트 그리드의 경우 각 데이터 센터에 대한 차트를 검토하십시오.

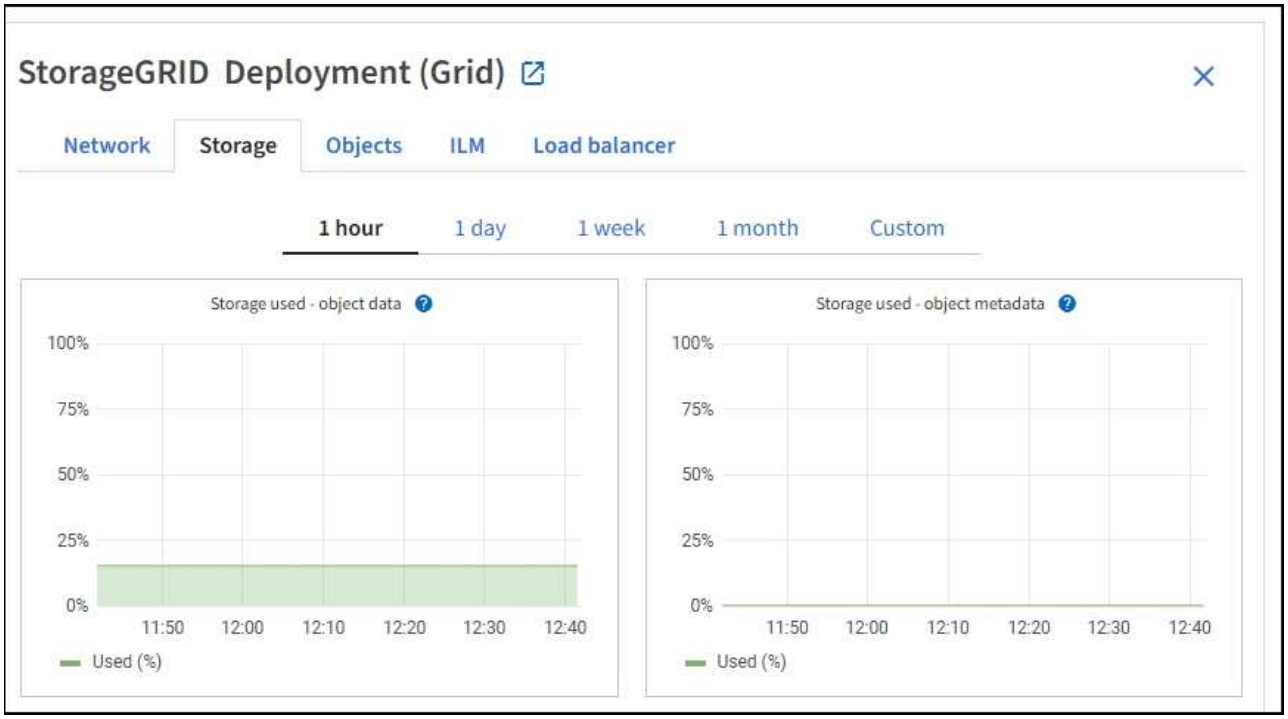
c. 차트 아이콘을 클릭합니다 전체 차트 또는 개별 데이터 센터에 대해 시간별 용량 사용을 보여주는 그래프를 표시합니다.

사용된 스토리지 용량(%)과 을 비교한 그래프입니다 시간이 나타납니다.

2. 사용된 스토리지 양과 오브젝트 데이터 및 오브젝트 메타데이터에 사용 가능한 스토리지 양을 확인합니다.

a. 노드 * 를 선택합니다.

b. **GRID* * > * 스토리지 * 를 선택합니다.



c. 커서를 * Storage Used-object data * 및 * Storage Used-object metadata * 차트 위에 올려 놓으면 전체 그리드에 사용 가능한 객체 스토리지 및 객체 메타데이터 스토리지가 얼마나 되는지, 그리고 시간이 지남에 따라 얼마나 사용되었는지 확인할 수 있습니다.

> 사이트 또는 그리드의 총 값에는 오프라인 노드와 같이 최소 5분 동안 보고된 메트릭이 없는 노드가 포함되지 않습니다.

3. 그리드의 가용 스토리지 용량이 소비되기 전에 스토리지 노드 또는 스토리지 볼륨을 추가하기 위해 확장을 수행할 계획을 수립합니다.

   확장 시기를 계획할 때 추가 스토리지를 조달 및 설치하는 데 걸리는 시간을 고려하십시오.

   > ILM 정책에서 삭제 코딩을 사용하는 경우 기존 스토리지 노드의 비율이 약 70%일 때 확장을 수행하여 추가해야 할 노드 수를 줄일 수 있습니다.

   스토리지 확장 계획에 대한 자세한 내용은 를 참조하십시오 StorageGRID 확장 지침.

각 스토리지 노드의 스토리지 용량을 모니터링합니다

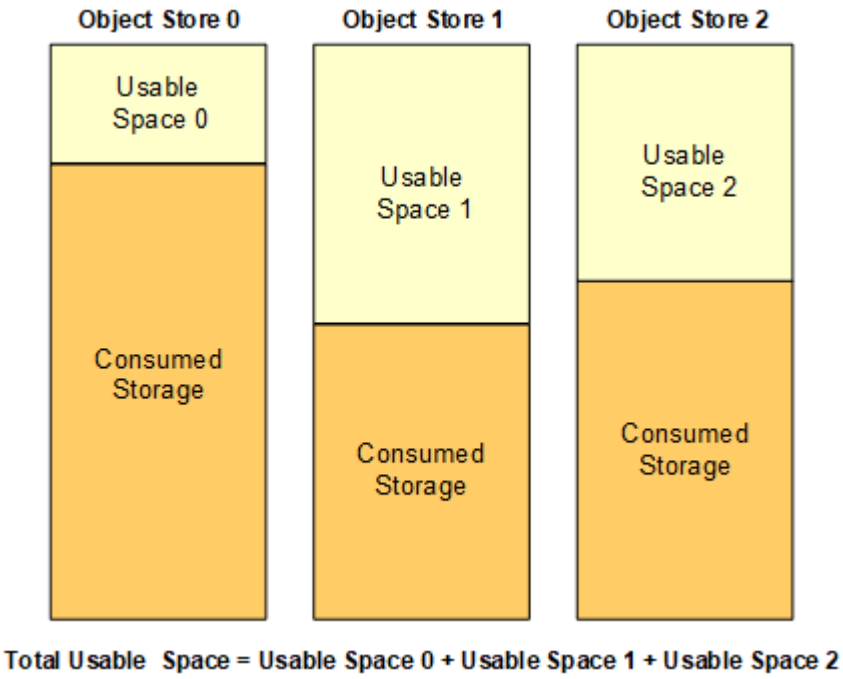
각 스토리지 노드의 총 사용 가능 공간을 모니터링하여 노드에 새 객체 데이터를 위한 충분한 공간이 있는지 확인합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

이 작업에 대해

사용 가능한 공간 은 오브젝트를 저장할 수 있는 저장 공간의 양입니다. 스토리지 노드의 사용 가능한 총 공간은 노드 내의 모든 오브젝트 저장소에 사용 가능한 공간을 추가하여 계산합니다.



단계

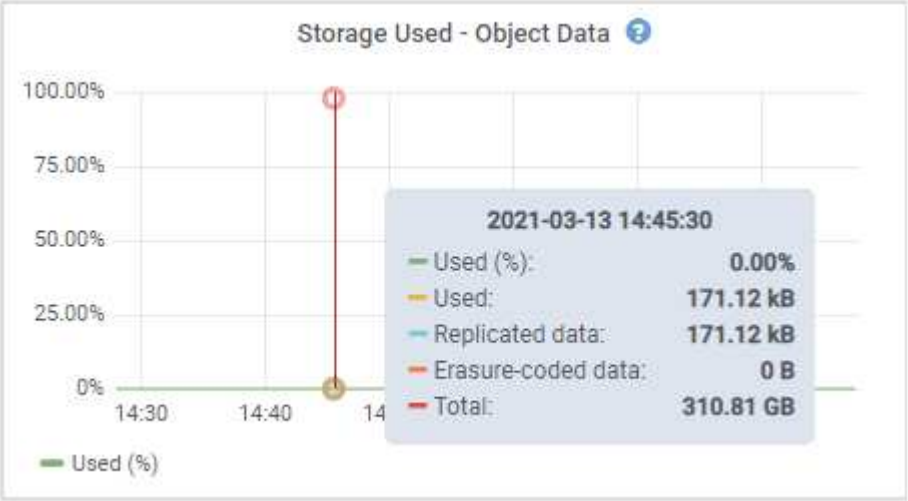
1. nodes * > **Storage Node* * > * Storage * 를 선택합니다.

   노드에 대한 그래프와 표가 나타납니다.

2. 커서를 Storage Used-object 데이터 그래프 위에 놓습니다.

   다음 값이 표시됩니다.

- * 사용됨(%) *: 오브젝트 데이터에 사용된 총 사용 가능 공간의 비율입니다.
- * 사용됨 *: 오브젝트 데이터에 사용된 총 사용 가능 공간의 양입니다.
- * 복제된 데이터 *: 이 노드, 사이트 또는 그리드에 복제된 객체 데이터의 양을 추정하는 것입니다.
- * 삭제 코딩 데이터 *: 이 노드, 사이트 또는 그리드에 삭제 코딩 처리된 오브젝트 데이터의 양을 예측합니다.
- * 총 *: 이 노드, 사이트 또는 그리드에서 사용 가능한 총 공간입니다. 사용된 값은 'toragegrid_storage_Utilization_data_bytes' 메트릭입니다.



3. 그래프 아래에 있는 Volumes and Object Stores(볼륨 및 오브젝트 저장소) 표에서 사용 가능한 값을 검토합니다.

이러한 값의 그래프를 보려면 차트 아이콘을 클릭합니다 를 클릭합니다.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

4. 시간에 따른 값을 모니터링하여 사용 가능한 스토리지 공간이 사용되는 속도를 예측합니다.
5. 정상적인 시스템 운영을 유지하려면 사용 가능한 공간이 소비되기 전에 스토리지 노드를 추가하고, 스토리지 볼륨을 추가하거나, 오브젝트 데이터를 아카이빙합니다.

   확장 시기를 계획할 때 추가 스토리지를 조달 및 설치하는 데 걸리는 시간을 고려하십시오.

   > ILM 정책에서 삭제 코딩을 사용하는 경우 기존 스토리지 노드의 비율이 약 70%일 때 확장을 수행하여 추가해야 할 노드 수를 줄일 수 있습니다.

   스토리지 확장 계획에 대한 자세한 내용은 를 참조하십시오 StorageGRID 확장 지침.

   를 클릭합니다 * 낮은 오브젝트 데이터 스토리지 * 스토리지 노드에 오브젝트 데이터를 저장하기 위한 공간이 부족할

때 경고가 트리거됩니다.

각 스토리지 노드의 객체 메타데이터 용량을 모니터링합니다

각 스토리지 노드의 메타데이터 사용량을 모니터링하여 필수 데이터베이스 작업에 사용할 수 있는 충분한 공간을 확보합니다. 오브젝트 메타데이터가 허용된 메타데이터 공간의 100%를 초과하기 전에 각 사이트에 새 스토리지 노드를 추가해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.

이 작업에 대해

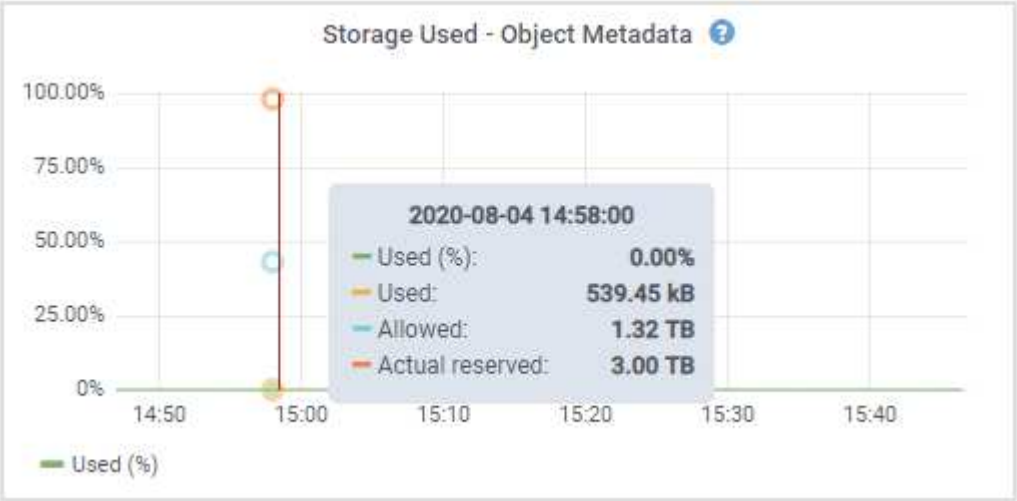
StorageGRID는 이중화를 제공하고 오브젝트 메타데이터를 손실로부터 보호하기 위해 각 사이트에 3개의 오브젝트 메타데이터 복사본을 유지합니다. 이 세 복제본은 각 스토리지 노드의 스토리지 볼륨 0에 있는 메타데이터에 예약된 공간을 사용하여 각 사이트의 모든 스토리지 노드에 균등하게 분산됩니다.

경우에 따라 그리드의 오브젝트 메타데이터 용량이 오브젝트 스토리지 용량보다 더 빠르게 소비될 수 있습니다. 예를 들어, 일반적으로 많은 수의 작은 오브젝트를 수집하는 경우 충분한 오브젝트 스토리지 용량이 남아 있더라도 메타데이터 용량을 늘리려면 스토리지 노드를 추가해야 할 수 있습니다.

메타데이터 사용량을 늘릴 수 있는 요인으로는 사용자 메타데이터 및 태그의 크기와 수량, 여러 부분 업로드의 총 부품 수, ILM 스토리지 위치의 변경 빈도 등이 있습니다.

단계

1. nodes * > **Storage Node* * > * Storage * 를 선택합니다.
2. 커서를 Storage Used-object 메타데이터 그래프 위에 놓으면 특정 시간의 값을 볼 수 있습니다.



값	설명	**Prometheus** 메트릭입니다
사용됨(%)	이 스토리지 노드에서 사용된 허용된 메타데이터 공간의 비율입니다.	'toragegrid_storage_Utilization_metadata_bytes/StorageGRID_storage_Utilization_metadata_Allowed_bytes'

값	설명	**Prometheus** 메트릭입니다
사용됨	이 스토리지 노드에서 사용된 허용되는 메타데이터 공간의 바이트	'toragegrid_storage_Utilization_metadata_bytes'
허용됨	이 스토리지 노드의 객체 메타데이터에 허용되는 공간입니다. 이 값이 각 스토리지 노드에 대해 어떻게 결정되는지 알아보려면 를 참조하십시오 StorageGRID 관리 지침.	'toragegrid_storage_Utilization_metadata_allowed_bytes'
실제 예약입니다	이 스토리지 노드의 메타데이터에 예약된 실제 공간입니다. 필수 메타데이터 작업에 필요한 공간 및 허용된 공간이 포함됩니다. 각 스토리지 노드에 대해 이 값이 계산되는 방법에 대한 자세한 내용은 를 참조하십시오 StorageGRID 관리 지침.	_Metric은 향후 릴리즈에서 추가될 예정입니다. _

> 사이트 또는 그리드의 총 값에는 오프라인 노드와 같이 최소 5분 동안 메트릭을 보고하지 않은 노드가 포함되지 않습니다.

3. Used(%) * 값이 70% 이상인 경우 각 사이트에 스토리지 노드를 추가하여 StorageGRID 시스템을 확장합니다.

> 사용된 값(%) * 값이 특정 임계값에 도달하면 * Low metadata storage * 경고가 트리거됩니다. 오브젝트 메타데이터에서 허용되는 공간의 100% 이상을 사용하는 경우 바람직하지 않은 결과가 발생할 수 있습니다.

새 노드를 추가하면 시스템에서 사이트 내의 모든 스토리지 노드에서 개체 메타데이터를 자동으로 재조정합니다. 를 참조하십시오 StorageGRID 시스템 확장을 위한 지침.

정보 수명 주기 관리를 모니터링합니다

ILM(정보 수명 주기 관리) 시스템은 그리드에 저장된 모든 개체에 대한 데이터 관리 기능을 제공합니다. ILM 작업을 모니터링하여 그리드에서 현재 로드를 처리할 수 있는지 또는 더 많은 리소스가 필요한지 여부를 이해해야 합니다.

필요한 것

를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

이 작업에 대해

StorageGRID 시스템은 활성 ILM 정책을 적용하여 객체를 관리합니다. ILM 정책 및 관련 ILM 규칙은 복사되는 복사본 수, 생성되는 복사본 유형, 복사본 배치 위치 및 각 복사본이 유지되는 시간을 결정합니다.

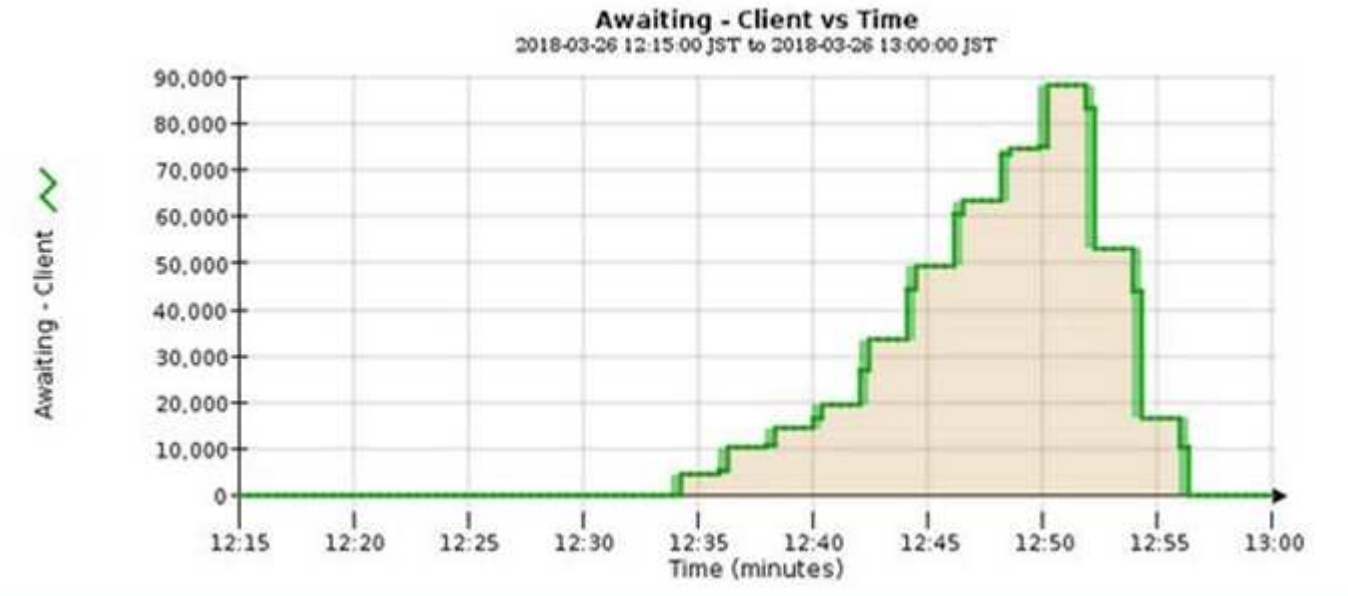
오브젝트 수집 및 기타 오브젝트 관련 활동이 StorageGRID에서 ILM을 평가할 수 있는 속도를 초과할 수 있으므로 시스템에서 ILM 배치 지침을 거의 실시간으로 이행할 수 없는 개체를 대기열에 추가할 수 있습니다. Awaiting-Client 속성을 차트로 표시하여 StorageGRID가 클라이언트 작업을 지원하는지 여부를 모니터링할 수 있습니다.

이 속성을 차트로 작성하려면 다음과 같이 하십시오.

1. Grid Manager에 로그인합니다.

2. 대시보드에서 ILM(정보 수명 주기 관리) 패널에서 * Awaiting-Client * 항목을 찾습니다.
3. 차트 아이콘을 클릭합니다 .

이 예제 차트는 ILM 평가를 기다리는 개체 수가 일시적으로 지속 불가능한 방식으로 증가했다가 결국 감소하는 상황을 보여 줍니다. 이러한 경향은 ILM이 거의 실시간으로 임시 이행되지 않았음을 나타냅니다.



대기 중 - 클라이언트 차트에서 일시적인 스파이크가 예상됩니다. 하지만 차트에 표시된 값이 계속 증가하고 감소되지 않는 경우 그리드에서 효율적으로 작동하기 위해 더 많은 리소스가 필요합니다. 즉, 더 많은 스토리지 노드 또는 ILM 정책이 원격 위치에 개체를 배치하는 경우 더 많은 네트워크 대역폭 이 필요합니다.

nodes * 페이지를 사용하여 ILM 대기열을 추가로 조사할 수 있습니다.

단계

1. 노드 * 를 선택합니다.
2. *GRID NAME* * > * ILM * 을 선택합니다.
3. ILM 대기열 그래프 위로 커서를 이동하면 특정 시점에 다음 속성의 값을 볼 수 있습니다.
   - * 대기 중인 오브젝트(클라이언트 작업에서) *: 클라이언트 작업(예: 수집)으로 인해 ILM 평가를 대기 중인 총 오브젝트 수
   - * 대기 중인 개체(모든 작업에서) *: ILM 평가를 대기 중인 총 개체 수.
   - * 스캔 속도(개체/초) *: 그리드의 개체가 스캔되어 ILM을 위해 대기 중인 속도입니다.
   - * 평가 속도(개체/초) *: 그리드의 ILM 정책에 따라 개체를 평가하는 현재 속도입니다.
4. ILM 대기열 섹션에서 다음 속성을 확인합니다.

> ILM 대기열 섹션은 그리드에만 포함됩니다. 이 정보는 사이트 또는 스토리지 노드의 ILM 탭에 표시되지 않습니다.

   - * Scan Period - Estimated *(스캔 기간 - 추정 *): 모든 개체의 전체 ILM 스캔을 완료하는 데 걸리는 예상 시간입니다.

> 전체 스캔은 ILM이 모든 개체에 적용되었다고 보장하지 않습니다.

- * 복구 시도 *: 복제된 데이터에 대한 총 객체 복구 작업 수입니다. 이 수는 스토리지 노드가 고위험 객체를 복구하려고 할 때마다 증가합니다. 그리드가 사용 중인 경우 위험이 높은 ILM 수리의 우선 순위가 지정됩니다.

> 복구 후 복제에 실패한 경우 동일한 객체 복구가 다시 증가할 수 있습니다.

이러한 속성은 스토리지 노드 볼륨 복구 진행률을 모니터링할 때 유용할 수 있습니다. 시도된 수리 횟수가 증가하고 전체 스캔이 완료된 경우 수리가 완료된 것일 수 있습니다.

네트워크 연결 및 성능을 모니터링합니다

그리드 노드는 그리드가 작동하도록 서로 통신할 수 있어야 합니다. 노드와 사이트 간의 네트워크 무결성과 사이트 간의 네트워크 대역폭은 효율적인 운영에 매우 중요합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

네트워크 연결 및 대역폭은 정보 라이프사이클 관리(ILM)가 사이트 간에 복제된 개체를 복사하거나 사이트 손실 보호를 제공하는 체계를 사용하여 삭제 코딩 오브젝트를 저장할 때 특히 중요합니다. 사이트 간 네트워크를 사용할 수 없거나, 네트워크 지연 시간이 너무 길거나, 네트워크 대역폭이 충분하지 않은 경우 일부 ILM 규칙으로 인해 원하는 위치에 개체를 배치할 수 없을 수 있습니다. 이로 인해 수집 실패(ILM 규칙에 대해 Strict 수집 옵션을 선택한 경우)가 발생하거나 수집 성능 및 ILM 백로그가 저하될 수 있습니다.

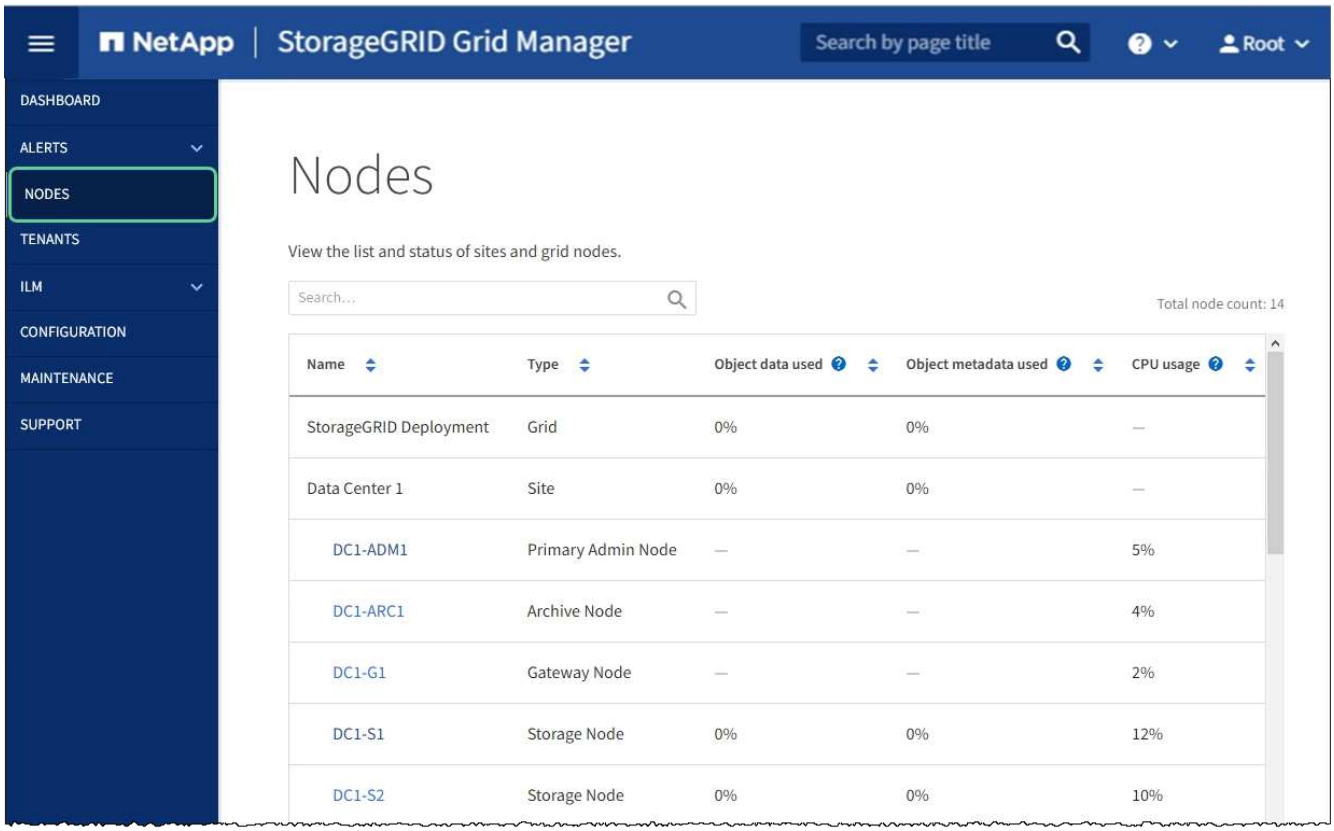
Grid Manager를 사용하여 연결 및 네트워크 성능을 모니터링할 수 있으므로 모든 문제를 즉시 해결할 수 있습니다.

또한 특정 테넌트, 버킷, 서브넷 또는 로드 밸런서 엔드포인트와 관련된 트래픽을 모니터링하고 제한하는 네트워크 트래픽 분류 정책을 만드는 것을 고려하십시오. 를 참조하십시오 StorageGRID 관리 지침.

단계

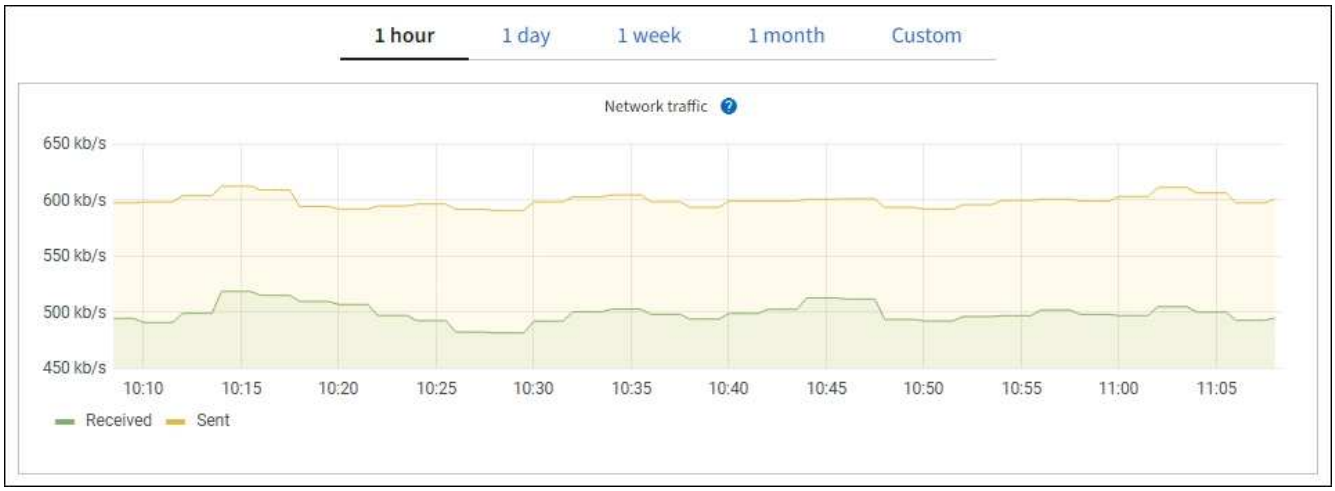
1. 노드 * 를 선택합니다.

   노드 페이지가 나타납니다. 그리드의 각 노드는 테이블 형식으로 나열됩니다.

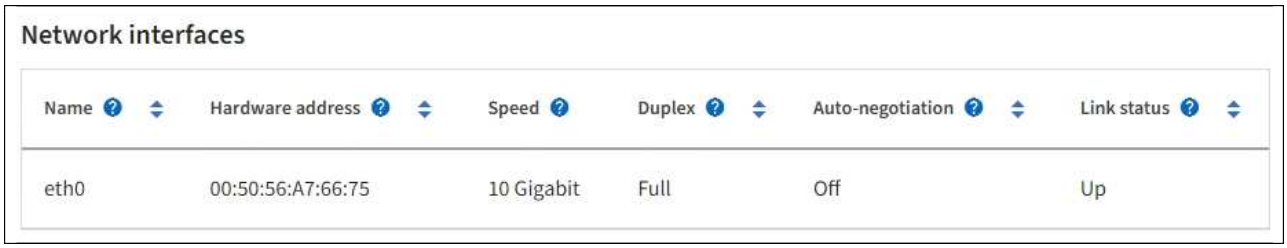


2. 그리드 이름, 특정 데이터 센터 사이트 또는 그리드 노드를 선택한 다음 * 네트워크 * 탭을 선택합니다.

   네트워크 트래픽 그래프는 그리드의 전체 네트워크 트래픽, 데이터 센터 사이트 또는 노드에 대한 요약 정보를 제공합니다.



   a. 그리드 노드를 선택한 경우 아래로 스크롤하여 페이지의 * 네트워크 인터페이스 * 섹션을 검토합니다.



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

b. 그리드 노드의 경우 아래로 스크롤하여 페이지의 * 네트워크 통신 * 섹션을 검토합니다.

Receive 및 Transmit 테이블은 각 네트워크에서 수신 및 전송된 바이트 및 패킷의 수와 기타 수신 및 전송 메트릭을 보여줍니다.

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

3. 트래픽 분류 정책과 관련된 메트릭을 사용하여 네트워크 트래픽을 모니터링합니다.

a. 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택합니다.

트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create | Edit | Remove | Metrics

	Name	Description	ID
○	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
◉	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

b. 정책과 연결된 네트워킹 메트릭을 보여주는 그래프를 보려면 정책 왼쪽의 라디오 버튼을 선택한 다음 * Metrics * 를 클릭합니다.

c. 그래프를 검토하여 정책과 관련된 네트워크 트래픽을 파악합니다.

트래픽 분류 정책이 네트워크 트래픽을 제한하도록 설계된 경우 트래픽이 얼마나 자주 제한되는지 분석하고 정책이 계속해서 요구 사항을 충족하는지 결정합니다. 때때로 필요에 따라 각 트래픽 분류 정책을 조정합니다.

트래픽 분류 정책을 생성, 편집 또는 삭제하려면 를 참조하십시오 StorageGRID 관리 지침.

관련 정보

네트워크 탭을 봅니다

노드 연결 상태를 모니터링합니다

노드 레벨 리소스를 모니터링합니다

개별 그리드 노드를 모니터링하여 리소스 활용도 수준을 확인해야 합니다.

필요한 것

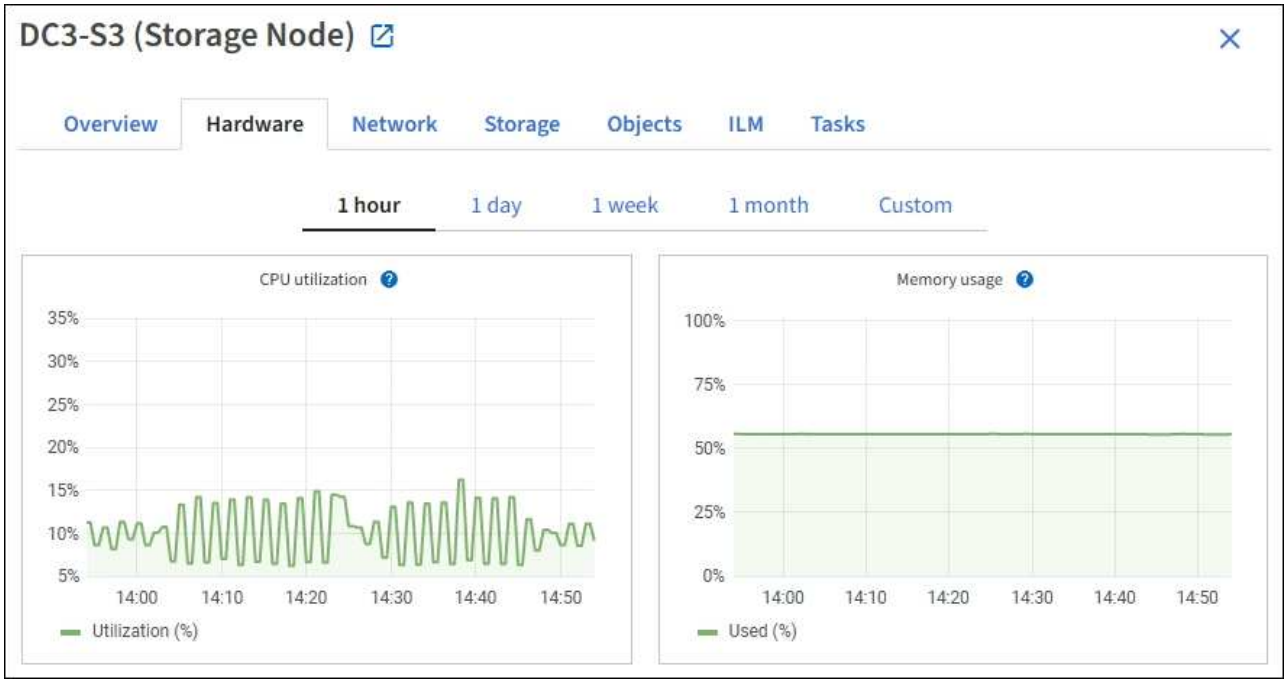
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

이 작업에 대해

노드가 지속적으로 과부하 상태가 되면 효율적인 작업에 더 많은 노드가 필요할 수 있습니다.

단계

1. 그리드 노드의 하드웨어 활용도에 대한 정보를 보려면 다음을 수행합니다.
   a. nodes * 페이지에서 노드를 선택합니다.
   b. Hardware * 탭을 선택하여 CPU 사용률 및 메모리 사용량 그래프를 표시합니다.



   c. 다른 시간 간격을 표시하려면 차트 또는 그래프 위에 있는 컨트롤 중 하나를 선택합니다. 1시간, 1일, 1주 또는 1개월 간격으로 사용 가능한 정보를 표시할 수 있습니다. 날짜 및 시간 범위를 지정할 수 있는 사용자 지정 간격을 설정할 수도 있습니다.
   d. 노드가 스토리지 어플라이언스 또는 서비스 어플라이언스에서 호스팅되는 경우 아래로 스크롤하여 구성 요소 테이블을 확인합니다. 모든 부품의 상태는 ""공칭""이어야 합니다. 다른 상태가 있는 구성 요소를 조사합니다.

관련 정보

어플라이언스 스토리지 노드에 대한 정보를 봅니다

어플라이언스 관리 노드 및 게이트웨이 노드에 대한 정보를 봅니다

테넌트 작업을 모니터링합니다

모든 클라이언트 작업이 테넌트 계정과 연결되어 있습니다. 그리드 관리자를 사용하여 테넌트의

스토리지 사용 또는 네트워크 트래픽을 모니터링하거나 감사 로그 또는 Grafana 대시보드를 사용하여 테넌트가 StorageGRID를 사용하는 방법에 대한 자세한 정보를 수집할 수 있습니다.

필요한 것

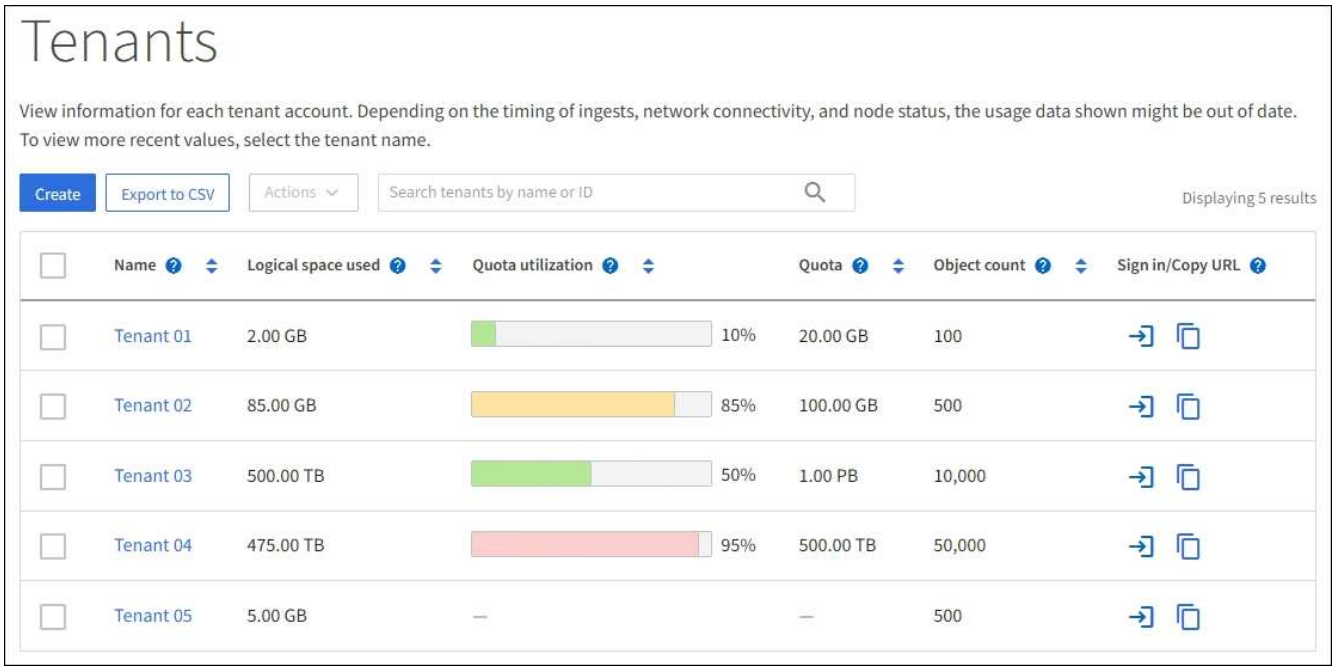
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 또는 관리자 권한이 있습니다.

> 이 작업에 대해
>
> 사용된 공간 값은 추정값입니다. 이러한 추정치는 베스트 타이밍, 네트워크 연결 및 노드 상태의 영향을 받습니다.

단계

1. 모든 테넌트가 사용하는 스토리지 양을 검토하려면 * Tenants * 를 선택합니다.

   사용된 논리적 공간, 할당량 사용률, 할당량 및 객체 수가 각 테넌트에 대해 나열됩니다. 할당량이 테넌트에 대해 설정되지 않은 경우 할당량 사용률과 할당량 필드에는 대시(—)가 포함됩니다.



   로그인 링크를 선택하여 테넌트 계정에 로그인할 수 있습니다 테이블의 * 로그인/URL 복사 * 열에 있습니다.

   URL 복사 링크를 선택하여 테넌트의 로그인 페이지에 대한 URL을 복사할 수 있습니다 테이블의 * 로그인/URL 복사 * 열에 있습니다.

2. 필요한 경우 * CSV로 내보내기 * 를 선택하여 모든 테넌트의 사용 값이 포함된 .csv 파일을 보고 내보냅니다.

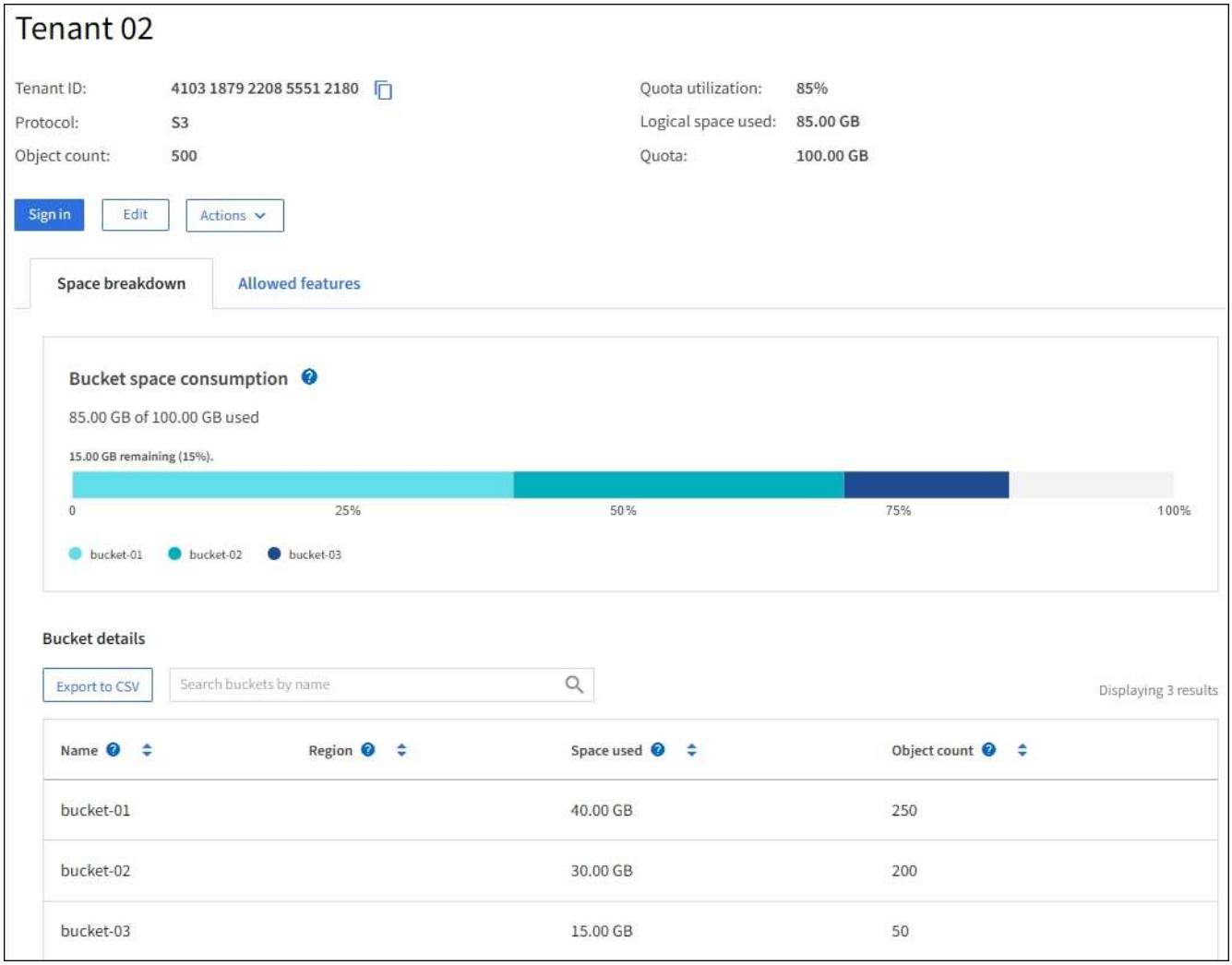
   '.csv' 파일을 열거나 저장하라는 메시지가 표시됩니다.

   CSV 파일의 내용은 다음 예제와 같습니다.

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

스프레드시트 응용 프로그램에서 .csv 파일을 열거나 자동화 시 사용할 수 있습니다.

3. 사용 차트를 비롯한 특정 테넌트의 세부 정보를 보려면 테넌트 페이지에서 테넌트 계정 이름을 선택합니다.



- * 테넌트 개요 *

  테넌트의 개요 영역에는 개체 수, 할당량 사용률, 사용된 논리적 공간 및 할당량 설정에 대한 값이 포함되어 있습니다.

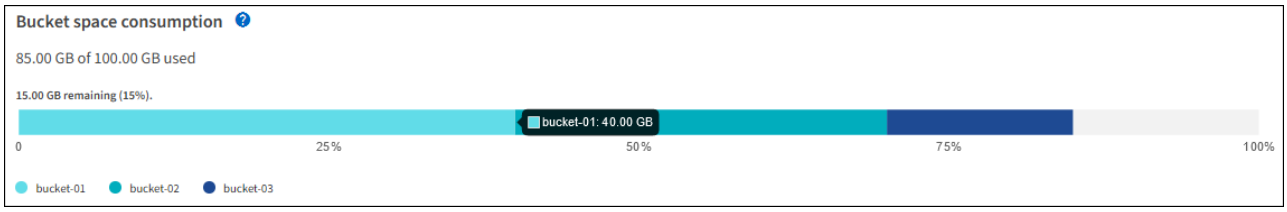
- * 공간 분석 — 공간 소비 *

  공간 분석 탭에는 버킷(S3) 또는 컨테이너(Swift)의 총 공간 소비에 대한 값과 각 버킷 또는 컨테이너에 사용된 공간 및 오브젝트 수가 포함됩니다.

  이 테넌트에 대해 할당량이 설정된 경우 사용된 할당량과 남은 할당량이 텍스트로 표시됩니다(예: 사용된 100GB의 85.00GB). 할당량이 설정되어 있지 않으면 테넌트에 무제한 할당량이 있고 텍스트에 사용된 공간(예:

85.00GB 사용됨)만 포함됩니다. 막대 차트는 각 버킷 또는 컨테이너의 할당량 백분율을 보여 줍니다. 테넌트가 스토리지 할당량을 1% 이상 초과하고 1GB 이상 초과한 경우 총 할당량과 초과 금액이 차트에 표시됩니다.

막대 차트 위에 커서를 놓으면 각 버킷이나 컨테이너에서 사용하는 저장소를 볼 수 있습니다. 사용 가능한 공간 세그먼트 위에 커서를 놓으면 남은 스토리지 할당량 크기를 확인할 수 있습니다.



> 할당량 활용도는 내부 추정치에 기반하며 경우에 따라 초과될 수 있습니다. 예를 들어, 테넌트가 객체를 업로드하기 시작할 때 StorageGRID는 할당량을 확인하고 테넌트가 할당량을 초과할 경우 새 베스트(ingest)를 거부합니다. 그러나 StorageGRID에서는 할당량이 초과되었는지 확인할 때 현재 업로드 크기를 고려하지 않습니다. 개체를 삭제하면 할당량 활용률이 다시 계산될 때까지 테넌트가 일시적으로 새 개체를 업로드하지 못할 수 있습니다. 할당량 사용률 계산에는 10분 이상이 소요될 수 있습니다.

> 테넌트의 할당량 활용도는 테넌트가 StorageGRID에 업로드한 총 객체 데이터 양(논리적 크기)을 나타냅니다. 할당량 활용은 해당 객체와 해당 메타데이터(물리적 크기)의 복사본을 저장하는 데 사용되는 공간을 나타내지 않습니다.

> 테넌트 할당량 사용량 높음 * 알림을 설정하여 테넌트가 할당량을 사용하고 있는지 확인할 수 있습니다. 활성화된 경우 테넌트가 할당량의 90%를 사용한 경우 이 경고가 트리거됩니다. 자세한 내용은 알림 참조 를 참조하십시오.

- * 공간 분석 — 버킷 또는 컨테이너 세부 정보 *

  Bucket details * (S3) 또는 * Container details * (Swift) 테이블에는 테넌트의 버킷 또는 컨테이너가 나열됩니다. 사용된 공간 은 버킷 또는 컨테이너에 있는 오브젝트 데이터의 총 양입니다. 이 값은 ILM 복사본 및 개체 메타데이터에 필요한 스토리지 공간을 나타내지 않습니다.

4. 필요에 따라 * CSV로 내보내기 * 를 선택하여 각 버킷 또는 컨테이너의 사용량 값이 포함된 .csv 파일을 보고 내보냅니다.

   개별 S3 테넌트의 .csv 파일 내용은 다음 예제와 같습니다.

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

   스프레드시트 응용 프로그램에서 .csv 파일을 열거나 자동화 시 사용할 수 있습니다.

5. 테넌트를 위한 트래픽 분류 정책이 마련되어 있는 경우 해당 테넌트의 네트워크 트래픽을 검토하십시오.

   a. 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택합니다.

      트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create | Edit | Remove | Metrics

	Name	Description	ID
○	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
◉	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

a. 정책 목록을 검토하여 특정 테넌트에 적용되는 정책을 식별합니다.

b. 정책과 관련된 메트릭을 보려면 정책 왼쪽의 라디오 버튼을 선택한 다음 * Metrics * 를 클릭합니다.

c. 그래프를 분석하여 정책에 따라 트래픽이 제한되는 빈도와 정책을 조정해야 하는지 여부를 결정합니다.

트래픽 분류 정책을 생성, 편집 또는 삭제하려면 StorageGRID 관리 지침을 참조하십시오.

6. 필요에 따라 감사 로그를 사용하여 테넌트의 활동을 보다 세부적으로 모니터링할 수 있습니다.

예를 들어 다음과 같은 유형의 정보를 모니터링할 수 있습니다.

- Put, Get 또는 Delete 같은 특정 클라이언트 작업입니다
- 개체 크기
- 개체에 적용된 ILM 규칙
- 클라이언트 요청의 소스 IP입니다

감사 로그는 선택한 로그 분석 도구를 사용하여 분석할 수 있는 텍스트 파일에 기록됩니다. 이를 통해 클라이언트 활동을 더 잘 이해하거나 정교한 차지백 및 청구 모델을 구현할 수 있습니다.

자세한 내용은 감사 메시지 이해를 위한 지침을 참조하십시오.

7. 선택적으로 Prometheus 메트릭을 사용하여 테넌트 활동을 보고합니다.

- Grid Manager에서 * 지원 * > * 도구 * > * 메트릭 * 을 선택합니다. S3 개요와 같은 기존 대시보드를 사용하여 클라이언트 작업을 검토할 수 있습니다.

> ⓘ 메트릭 페이지에서 사용할 수 있는 도구는 주로 기술 지원 부서에서 사용하도록 설계되었습니다. 이러한 도구 내의 일부 기능 및 메뉴 항목은 의도적으로 작동하지 않습니다.

- Grid Manager 상단에서 도움말 아이콘을 선택하고 * API Documentation * 을 선택합니다. Grid Management API의 Metrics(메트릭) 섹션에 있는 메트릭을 사용하여 테넌트 활동에 대한 사용자 지정 알림 규칙 및 대시보드를 생성할 수 있습니다.

관련 정보

경고 참조

감사 로그를 검토합니다

StorageGRID 관리

지원 메트릭을 검토합니다

아카이빙 용량을 모니터링합니다

StorageGRID 시스템을 통해서는 외부 아카이브 스토리지 시스템의 용량을 직접 모니터링할 수 없습니다. 그러나 아카이브 노드가 아카이브 대상으로 개체 데이터를 전송할 수 있는지 여부를 모니터링할 수 있습니다. 이는 아카이브 미디어의 확장이 필요함을 나타낼 수 있습니다.

필요한 것

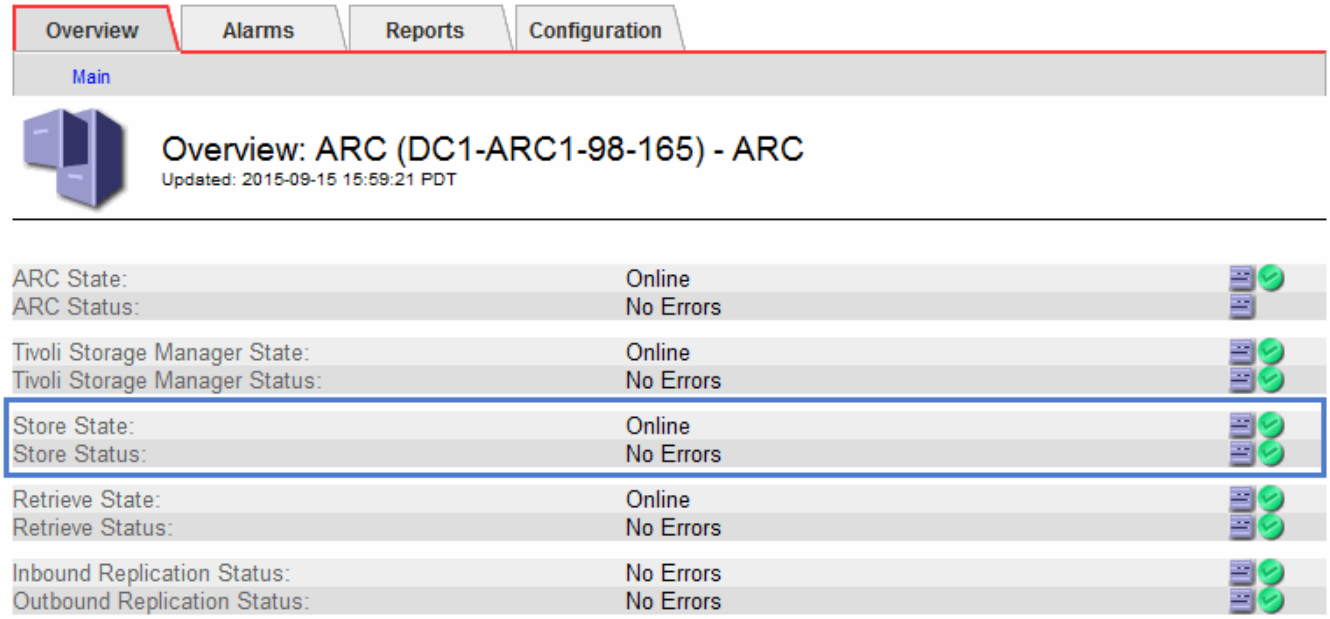
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

Store 구성 요소를 모니터링하여 아카이브 노드가 대상 아카이브 스토리지 시스템으로 객체 데이터를 전송할 수 있는지 확인할 수 있습니다. ARVF(Store Failures) 경보는 대상 아카이브 스토리지 시스템의 용량이 한도에 도달하여 더 이상 오브젝트 데이터를 수용할 수 없음을 나타낼 수도 있습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node_*>* ARC **> Overview** > Main*을 선택합니다.
3. Store State 및 Store Status 속성을 확인하여 Store 구성 요소가 Online with No Errors 인지 확인합니다.



오프라인 저장소 구성 요소 또는 오류가 있는 구성 요소는 대상 아카이브 스토리지 시스템이 용량에 도달하여 더 이상 오브젝트 데이터를 수용할 수 없음을 나타낼 수 있습니다.

로드 밸런싱 작업을 모니터링합니다

로드 밸런서를 사용하여 StorageGRID에 대한 클라이언트 연결을 관리하는 경우 시스템을 처음 구성한 후 또는 구성을 변경하거나 확장을 수행한 후에 로드 밸런싱 작업을 모니터링해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

관리 노드 또는 게이트웨이 노드에서 로드 밸런서 서비스, 외부 타사 로드 밸런서 또는 게이트웨이 노드의 CLB 서비스를 사용하여 여러 스토리지 노드에 클라이언트 요청을 분산할 수 있습니다.

> CLB 서비스는 더 이상 사용되지 않습니다.

로드 밸런싱을 구성한 후에는 오브젝트 수집 및 검색 작업이 스토리지 노드 간에 균등하게 분산되는지 확인해야 합니다. 균등하게 분산된 요청은 StorageGRID가 로드 중인 클라이언트 요청에 계속 응답하도록 하며 클라이언트 성능을 유지하는 데 도움이 됩니다.

액티브-백업 모드에서 게이트웨이 노드 또는 관리 노드의 고가용성(HA) 그룹을 구성한 경우 그룹의 노드 중 하나만 클라이언트 요청을 능동적으로 분배합니다.

StorageGRID 관리 지침에 있는 클라이언트 연결 구성 섹션을 참조하십시오.

단계

1. S3 또는 Swift 클라이언트가 로드 밸런서 서비스를 사용하여 연결하는 경우 관리 노드 또는 게이트웨이 노드가 예상대로 트래픽을 적극적으로 분산하는지 확인합니다.
   a. 노드 * 를 선택합니다.
   b. 게이트웨이 노드 또는 관리자 노드를 선택합니다.
   c. Overview * 탭에서 노드 인터페이스가 HA 그룹에 있는지, 노드 인터페이스가 Master 역할을 하는지 확인합니다.

      Master 역할과 HA 그룹에 속하지 않는 노드를 가진 노드는 요청을 클라이언트에 능동적으로 분산해야 합니다.

   d. 클라이언트 요청을 활발하게 분산해야 하는 각 노드에 대해 * 로드 밸런서 * 탭을 선택합니다.
   e. 지난 주 로드 밸런서 요청 트래픽 차트를 검토하여 노드가 요청을 적극적으로 배포했는지 확인합니다.

      액티브-백업 HA 그룹의 노드는 수시로 백업 역할을 수행할 수 있습니다. 이 시간 동안 노드는 클라이언트 요청을 배포하지 않습니다.

   f. 지난 주 로드 밸런서 수신 요청 속도 차트를 검토하여 노드의 객체 처리량을 검토합니다.
   g. StorageGRID 시스템의 각 관리 노드 또는 게이트웨이 노드에 대해 이 단계를 반복합니다.
   h. 필요에 따라 트래픽 분류 정책을 사용하여 부하 분산 서비스가 제공하는 트래픽에 대한 보다 자세한 분석을 볼 수 있습니다.
2. S3 또는 Swift 클라이언트가 CLB 서비스를 사용하여 연결된 경우(더 이상 사용되지 않음) 다음 검사를 수행합니다.
   a. 노드 * 를 선택합니다.
   b. 게이트웨이 노드를 선택합니다.
   c. Overview * 탭에서 노드 인터페이스가 HA 그룹에 있는지, 노드 인터페이스가 Master 역할을 하는지 확인합니다.

      Master 역할과 HA 그룹에 속하지 않는 노드를 가진 노드는 요청을 클라이언트에 능동적으로 분산해야 합니다.

d. 클라이언트 요청을 활발하게 분산해야 하는 각 게이트웨이 노드에 대해 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.

e. **Gateway Node* * > * CLB * > * HTTP * > * Overview * > * Main * 을 선택합니다.

f. 들어오는 세션 수 * 를 검토하여 게이트웨이 노드가 요청을 능동적으로 처리하는지 확인합니다.

3. 이러한 요청이 스토리지 노드에 고르게 분산되는지 확인합니다.

a. 스토리지 노드 * > * LDR * > * HTTP * 를 선택합니다.

b. 현재 설정된 수신 세션 수 * 를 검토합니다.

c. 그리드의 각 스토리지 노드에 대해 이 과정을 반복합니다.

세션 수는 모든 스토리지 노드에서 거의 같아야 합니다.

관련 정보

StorageGRID 관리

부하 분산 탭을 봅니다

필요한 경우 핫픽스 또는 업그레이드 소프트웨어를 적용합니다

핫픽스나 새 버전의 StorageGRID 소프트웨어를 사용할 수 있는 경우 업데이트가 시스템에 적합한지 평가하고 필요한 경우 설치해야 합니다.

이 작업에 대해

StorageGRID 핫픽스에는 기능 또는 패치 릴리스 외부에서 사용할 수 있는 소프트웨어 변경 사항이 포함되어 있습니다. 동일한 변경 사항이 향후 릴리스에 포함됩니다.

단계

1. StorageGRID용 NetApp 다운로드 페이지로 이동합니다.

"NetApp 다운로드: StorageGRID"

2. 다운로드할 수 있는 업데이트 목록을 보려면 * 유형/버전 선택 * 필드의 아래쪽 화살표를 선택하십시오.

- * StorageGRID 소프트웨어 버전 *: 11._x. y _
- StorageGRID 핫픽스 *:11.*x.x.y.z*

3. 업데이트에 포함된 변경 사항을 검토합니다.

a. 풀다운 메뉴에서 버전을 선택하고 * Go * 를 클릭합니다.

b. NetApp 계정의 사용자 이름과 암호를 사용하여 로그인합니다.

c. 최종 사용자 사용권 계약을 읽고 확인란을 선택한 다음 * 동의 및 계속 * 을 선택합니다.

선택한 버전의 다운로드 페이지가 나타납니다.

4. 소프트웨어 버전 또는 핫픽스에 포함된 변경 사항에 대해 알아봅니다.

- 새 소프트웨어 버전은 StorageGRID 업그레이드 설명서의 ""새로운 기능" 항목을 참조하십시오.
- 핫픽스의 경우 README 파일을 다운로드하여 핫픽스에 포함된 변경 사항을 요약하십시오.

5. 소프트웨어 업데이트가 필요한 경우 계속하기 전에 지침을 찾습니다.
    - 새 소프트웨어 버전의 경우 StorageGRID 업그레이드 지침을 주의하여 따르십시오.
    - 핫픽스의 경우 복구 및 유지 관리 지침에 있는 핫픽스 절차를 찾습니다
        - 관련 정보 *

소프트웨어 업그레이드

복구 및 유지 관리

경고 및 알람을 관리합니다

경보 및 경보 관리: 개요

StorageGRID 경고 시스템은 주의가 필요한 운영 문제를 알려주도록 설계되었습니다. 기존 경보 시스템은 더 이상 사용되지 않습니다.

경고 시스템

경고 시스템은 StorageGRID 시스템에서 발생할 수 있는 문제를 모니터링하는 기본 도구로 설계되었습니다. 경고 시스템은 문제 감지, 평가 및 해결을 위한 사용이 간편한 인터페이스를 제공합니다.

알림은 알림 규칙 조건이 true로 평가될 때 특정 심각도 수준에서 트리거됩니다. 경고가 트리거되면 다음 작업이 수행됩니다.

- 그리드 관리자의 대시보드에 경고 심각도 아이콘이 표시되고 현재 경고의 수가 증가합니다.
- 이 알림은 * nodes * 요약 페이지와 * nodes * > **node* * > * Overview * 탭에 표시됩니다.
- SMTP 서버를 구성하고 수신자에 대한 이메일 주소를 제공한 경우 이메일 알림이 전송됩니다.
- StorageGRID SNMP 에이전트를 구성한 경우 SNMP(Simple Network Management Protocol) 알림이 전송됩니다.

레거시 알람 시스템

경고와 마찬가지로, 속성은 정의된 임계값에 도달할 때 특정 심각도 수준에서 트리거됩니다. 그러나 알림과 달리, 많은 알람은 사용자가 안전하게 무시할 수 있는 이벤트에 대해 트리거되며, 이로 인해 e-메일 또는 SNMP 알림이 과도하게 많아질 수 있습니다.

> 알람 시스템은 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다. 기존 경보를 계속 사용하는 경우 가능한 한 빨리 경보 시스템으로 완전히 전환해야 합니다.

알람이 트리거되면 다음과 같은 동작이 발생합니다.

- 알람이 * support * > * Alarms (Legacy) * > * Current alarms * 페이지에 나타납니다.
- SMTP 서버를 구성하고 하나 이상의 메일 그룹을 구성한 경우 이메일 알림이 전송됩니다.
- StorageGRID SNMP 에이전트를 구성한 경우 SNMP 알림이 전송될 수 있습니다. (모든 알람 또는 알람 심각도에 대해 SNMP 알림이 전송되지 않습니다.)

알림 시스템과 기존 경보 시스템은 서로 유사점이 많지만, 알림 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

유사한 작업을 수행하는 방법은 다음 표를 참조하십시오.

	경고	알람(레거시 시스템)
어떤 경보 또는 경보가 활성 상태인지 어떻게 알 수 있습니까?	• 대시보드에서 * Current alerts * 링크를 선택합니다. • nodes * > * Overview * 페이지에서 경고를 선택합니다. • alerts * > * current * 를 선택합니다. 현재 경고를 봅니다	지원 * > * 알람(레거시) * > * 현재 알람 * 을 선택합니다. 알람 관리(기존 시스템)
경보 또는 경보가 트리거되는 원인은 무엇입니까?	알림은 알림 규칙의 Prometheus 식이 특정 트리거 조건 및 기간에 대해 true로 평가될 때 트리거됩니다. 경고 규칙을 봅니다	StorageGRID 속성이 임계값에 도달하면 알람이 트리거됩니다. 알람 관리(기존 시스템)
경고 또는 알람이 트리거된 경우 기본 문제를 어떻게 해결합니까?	경고에 대한 권장 조치는 이메일 알림에 포함되며 Grid Manager의 Alerts 페이지에서 사용할 수 있습니다. 필요한 경우 StorageGRID 설명서에 추가 정보가 제공됩니다. 경고 참조	속성 이름을 선택하여 알람에 대해 자세히 알아보거나 StorageGRID 설명서에서 경보 코드를 검색할 수 있습니다. 알람 기준(레거시 시스템)
해결된 경고 또는 알람 목록은 어디에서 확인할 수 있습니까?	alerts * > * Resolved * 를 선택합니다. 해결된 경고를 봅니다	지원 * > * 알람(레거시) * > * 내역 알람 * 을 선택합니다. 알람 관리(기존 시스템)
설정 관리 위치	알림 * > * 규칙 * 을 선택합니다. 알림을 관리합니다	지원 * 을 선택합니다. 그런 다음 메뉴의 * Alarms (Legacy) * (알람(레거시) *) 섹션에 있는 옵션을 사용합니다. 알람 관리(기존 시스템)

	경고	알람(레거시 시스템)
어떤 사용자 그룹 권한이 필요합니까?	• Grid Manager에 로그인할 수 있는 모든 사용자는 현재 및 해결된 경고를 볼 수 있습니다. • 알림 차단, 알림 알림 및 알림 규칙을 관리하려면 알림 관리 권한이 있어야 합니다. StorageGRID 관리	• Grid Manager에 로그인할 수 있는 모든 사용자는 레거시 알람을 볼 수 있습니다. • 알람을 승인하려면 알람 확인 권한이 있어야 합니다. • 글로벌 경보 및 이메일 알림을 관리하려면 그리드 토폴로지 페이지 구성 및 기타 그리드 구성 권한이 모두 있어야 합니다. StorageGRID 관리
이메일 알림은 어떻게 관리합니까?	알림 * > * 이메일 설정 * 을 선택합니다. • 참고: * 알람과 알림은 독립 시스템이므로 알람 및 AutoSupport 알림에 사용되는 이메일 설정은 알림 용도로 사용되지 않습니다. 그러나 모든 알림에 동일한 메일 서버를 사용할 수 있습니다. 알림에 대한 이메일 알림을 설정합니다	지원 * > * 알람(레거시) * > * 레거시 이메일 설정 * 을 선택합니다. 알람 관리(기존 시스템)
SNMP 알림을 관리하려면 어떻게 해야 합니까?	구성 * > * 모니터링 * > * SNMP 에이전트 * 를 선택합니다. SNMP 모니터링을 사용합니다	구성 * > * 모니터링 * > * SNMP 에이전트 * 를 선택합니다. SNMP 모니터링을 사용합니다 • 참고 *: SNMP 알림은 모든 알람 또는 알람 심각도에 대해 전송되지 않습니다. SNMP 알림을 생성하는 알람(레거시 시스템)
알림을 받는 사람을 어떻게 제어합니까?	1. 알림 * > * 이메일 설정 * 을 선택합니다. 2. 받는 사람* 섹션에서 경고가 발생할 때 전자 메일을 받을 각 전자 메일 목록의 전자 메일 주소를 입력합니다. 알림에 대한 이메일 알림을 설정합니다	1. 지원 * > * 알람(레거시) * > * 레거시 이메일 설정 * 을 선택합니다. 2. 메일 그룹 만들기. 3. 알림 * 을 선택합니다. 4. 메일 그룹을 선택합니다. 알람 관리(기존 시스템)

	경고	알람(레거시 시스템)
알림을 보내는 관리 노드는 무엇입니까?	단일 관리 노드("선호 발신자"). StorageGRID 관리	단일 관리 노드("선호 발신자"). StorageGRID 관리
일부 알림을 표시하지 않으려면 어떻게 해야 합니까?	1. alerts * > * silences * 를 선택합니다. 2. 무음 설정할 경고 규칙을 선택합니다. 3. 무음 시간을 지정합니다. 4. 무음 설정할 경고의 심각도를 선택합니다. 5. 전체 그리드, 단일 사이트 또는 단일 노드에 무음을 적용하려면 선택합니다. ◦ 참고 *: SNMP 에이전트를 사용하도록 설정한 경우, SNMP 트랩을 표시하지 않고 알려줍니다. 알림 메시지를 해제합니다	1. 지원 * > * 알람(레거시) * > * 레거시 이메일 설정 * 을 선택합니다. 2. 알림 * 을 선택합니다. 3. 메일링 목록을 선택하고 * 기능 억제 * 를 선택합니다. 알람 관리(기존 시스템)
모든 알림을 표시하지 않으려면 어떻게 해야 합니까?	alerts * > * silences * 를 선택한 후 * all rules * 를 선택합니다. • 참고 *: SNMP 에이전트를 사용하도록 설정한 경우, SNMP 트랩을 표시하지 않고 알려줍니다. 알림 메시지를 해제합니다	1. 구성 * > * 시스템 * > * 디스플레이 옵션 * 을 선택합니다. 2. 알림 모두 표시 안 함 * 확인란을 선택합니다. ◦ 참고 *: e-메일 알림을 시스템 전체에 표시하지 않으면 이벤트 트리거된 AutoSupport e-메일도 표시되지 않습니다. 알람 관리(기존 시스템)
조건 및 트리거를 사용자 지정하려면 어떻게 해야 합니까?	1. 알림 * > * 규칙 * 을 선택합니다. 2. 편집할 기본 규칙을 선택하거나 * 사용자 지정 규칙 만들기 * 를 선택합니다. 알림 규칙을 편집합니다 사용자 지정 알림 규칙을 생성합니다	1. 지원 * > * 알람(레거시) * > * 전체 알람 * 을 선택합니다. 2. 기본 알람을 재정의하거나 기본 알람이 없는 속성을 모니터링하려면 글로벌 사용자 정의 알람을 생성합니다. 알람 관리(기존 시스템)

	경고	알람(레거시 시스템)
개별 경보 또는 경보를 비활성화하려면 어떻게 해야 합니까?	1. 알림 * > * 규칙 * 을 선택합니다. 2. 규칙을 선택하고 * 규칙 편집 * 을 선택합니다. 3. 사용 * 확인란의 선택을 취소합니다. 경고 규칙을 비활성화합니다	1. 지원 * > * 알람(레거시) * > * 전체 알람 * 을 선택합니다. 2. 규칙을 선택하고 편집 아이콘을 선택합니다. 3. 사용 * 확인란의 선택을 취소합니다. 알람 관리(기존 시스템)

알림을 관리합니다

알림 관리: 개요

경고를 통해 StorageGRID 시스템 내의 다양한 이벤트 및 조건을 모니터링할 수 있습니다. 사용자 지정 알림을 생성하고, 기본 경고를 편집 또는 비활성화하고, 경고에 대한 이메일 알림을 설정하고, 알림 해제를 통해 알림을 관리할 수 있습니다.

StorageGRID 알림에 대해 알아봅니다

이 경고 시스템은 StorageGRID 작동 중에 발생할 수 있는 문제를 감지, 평가 및 해결하기 위한 사용이 간편한 인터페이스를 제공합니다.

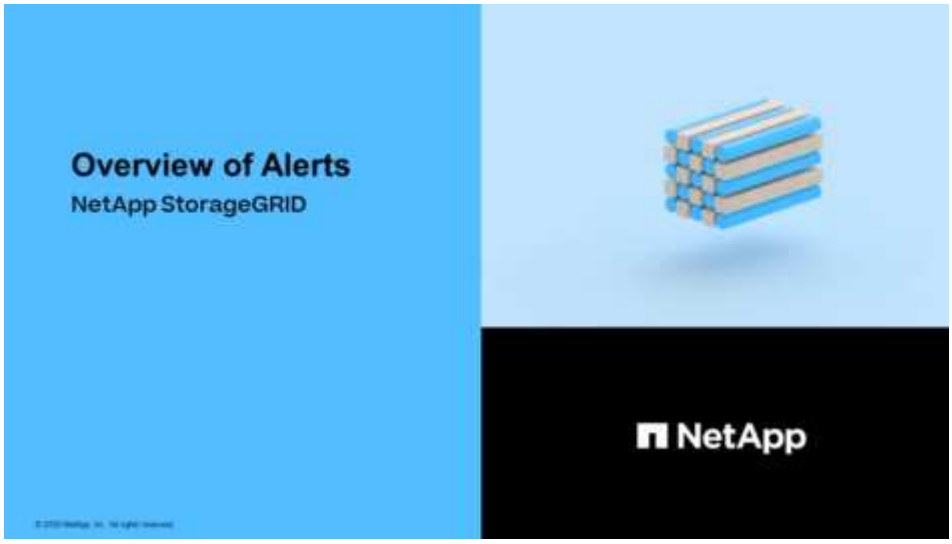
- 알림 시스템은 시스템에서 실행 가능한 문제에 초점을 맞춥니다. 경고는 안전하게 무시할 수 있는 이벤트가 아니라 즉각적인 주의가 필요한 이벤트에 대해 트리거됩니다.
- 현재 경고 페이지에서는 현재 문제를 볼 수 있는 사용자 친화적인 인터페이스를 제공합니다. 개별 알림 및 알림 그룹을 기준으로 목록을 정렬할 수 있습니다. 예를 들어 모든 알림을 노드/사이트별로 정렬하여 특정 노드에 영향을 미치는 알림을 확인할 수 있습니다. 또는 특정 알림의 가장 최근 인스턴스를 찾기 위해 트리거된 시간을 기준으로 그룹의 알림을 정렬할 수 있습니다.
- 해결된 경고 페이지는 현재 경고 페이지와 유사한 정보를 제공하지만, 경고가 트리거된 시기 및 해결된 시점을 포함하여 해결된 경고의 기록을 검색하고 볼 수 있습니다.
- 동일한 유형의 여러 알림이 하나의 이메일로 그룹화되어 알림 수가 줄어듭니다. 또한 동일한 유형의 여러 알림이 경고 페이지에 그룹으로 표시됩니다. 알림 그룹을 확장하고 축소하여 개별 알림을 표시하거나 숨길 수 있습니다. 예를 들어, 여러 노드에서 * 노드 * 경고와 거의 동시에 통신할 수 없다고 보고하면 하나의 이메일만 전송되고 알림은 경고 페이지에 그룹으로 표시됩니다.
- 알림은 직관적인 이름과 설명을 사용하여 문제를 빠르게 파악할 수 있도록 도와줍니다. 알림 알림에는 영향을 받는 노드 및 사이트에 대한 세부 정보, 알림 심각도, 알림 규칙이 트리거된 시간, 경고와 관련된 메트릭의 현재 값이 포함됩니다.
- 경고 이메일 알림 및 현재 경고 및 해결된 경고 페이지의 경고 목록은 경고 해결을 위한 권장 조치를 제공합니다. 이러한 권장 조치에는 보다 자세한 문제 해결 절차를 쉽게 찾아 액세스할 수 있도록 StorageGRID 문서 센터로 직접 연결되는 링크가 포함되어 있습니다.
- 하나 이상의 심각도 수준에서 알림에 대한 알림을 일시적으로 억제해야 하는 경우 지정된 기간 및 전체 그리드, 단일 사이트 또는 단일 노드에 대해 특정 알림 규칙을 쉽게 해제할 수 있습니다. 또한 소프트웨어 업그레이드와 같은 계획된 유지 관리 절차 중에 모든 경고 규칙을 해제할 수 있습니다.
- 필요에 따라 기본 경고 규칙을 편집할 수 있습니다. 경고 규칙을 완전히 비활성화하거나 트리거 조건 및 기간을 변경할 수 있습니다.

- 사용자 정의 경고 규칙을 생성하여 자신의 상황과 관련된 특정 조건을 타겟팅하고 자신만의 권장 조치를 제공할 수 있습니다. 사용자 지정 알림의 조건을 정의하려면 Grid Management API의 Metrics 섹션에서 사용할 수 있는 Prometheus 메트릭을 사용하여 표현식을 생성합니다.

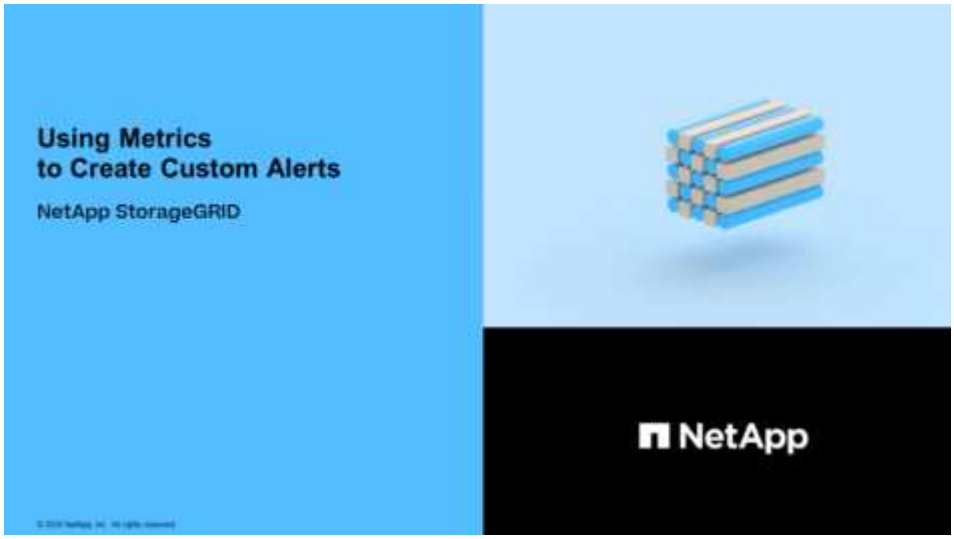
자세한 정보

자세한 내용은 다음 비디오를 참조하십시오.

- "비디오: 경고 개요"



- "비디오: 메트릭을 사용하여 사용자 지정 경고 생성"



경고 규칙을 봅니다

경고 규칙은 트리거되는 조건을 정의합니다 특정 경고. StorageGRID에는 기본 경고 규칙 집합이 포함되어 있으며, 이 규칙 집합을 그대로 사용하거나 수정하거나 사용자 지정 경고 규칙을 만들 수 있습니다.

모든 기본 및 사용자 지정 알림 규칙 목록을 보고 각 알림을 트리거할 조건을 확인하고 경고가 비활성화되었는지 여부를 확인할 수 있습니다.

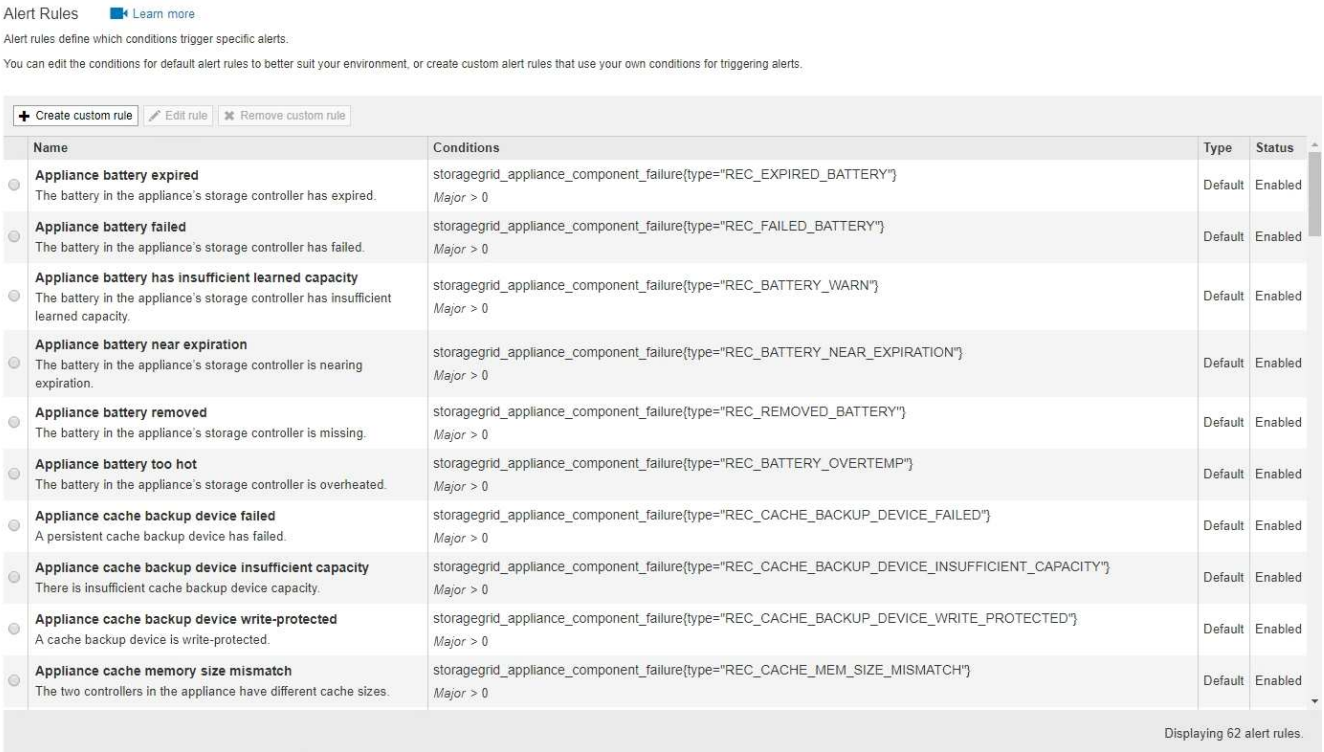
필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 알림 관리 또는 루트 액세스 권한이 있습니다.
- 선택적으로 비디오를 시청했습니다. "비디오: 경고 개요"

단계

1. 알림 * > * 규칙 * 을 선택합니다.

   경고 규칙 페이지가 나타납니다.



Alert Rules Learn more

Alert rules define which conditions trigger specific alerts.

You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

+ Create custom rule | Edit rule | Remove custom rule

Name	Conditions	Type	Status
Appliance battery expired The battery in the appliance's storage controller has expired.	storagegrid_appliance_component_failure{type="REC_EXPIRED_BATTERY"} *Major* > 0	Default	Enabled
Appliance battery failed The battery in the appliance's storage controller has failed.	storagegrid_appliance_component_failure{type="REC_FAILED_BATTERY"} *Major* > 0	Default	Enabled
Appliance battery has insufficient learned capacity The battery in the appliance's storage controller has insufficient learned capacity.	storagegrid_appliance_component_failure{type="REC_BATTERY_WARN"} *Major* > 0	Default	Enabled
Appliance battery near expiration The battery in the appliance's storage controller is nearing expiration.	storagegrid_appliance_component_failure{type="REC_BATTERY_NEAR_EXPIRATION"} *Major* > 0	Default	Enabled
Appliance battery removed The battery in the appliance's storage controller is missing.	storagegrid_appliance_component_failure{type="REC_REMOVED_BATTERY"} *Major* > 0	Default	Enabled
Appliance battery too hot The battery in the appliance's storage controller is overheated.	storagegrid_appliance_component_failure{type="REC_BATTERY_OVERTEMP"} *Major* > 0	Default	Enabled
Appliance cache backup device failed A persistent cache backup device has failed.	storagegrid_appliance_component_failure{type="REC_CACHE_BACKUP_DEVICE_FAILED"} *Major* > 0	Default	Enabled
Appliance cache backup device insufficient capacity There is insufficient cache backup device capacity.	storagegrid_appliance_component_failure{type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY"} *Major* > 0	Default	Enabled
Appliance cache backup device write-protected A cache backup device is write-protected.	storagegrid_appliance_component_failure{type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED"} *Major* > 0	Default	Enabled
Appliance cache memory size mismatch The two controllers in the appliance have different cache sizes.	storagegrid_appliance_component_failure{type="REC_CACHE_MEM_SIZE_MISMATCH"} *Major* > 0	Default	Enabled

Displaying 62 alert rules.

2. 경고 규칙 표의 정보를 검토합니다.

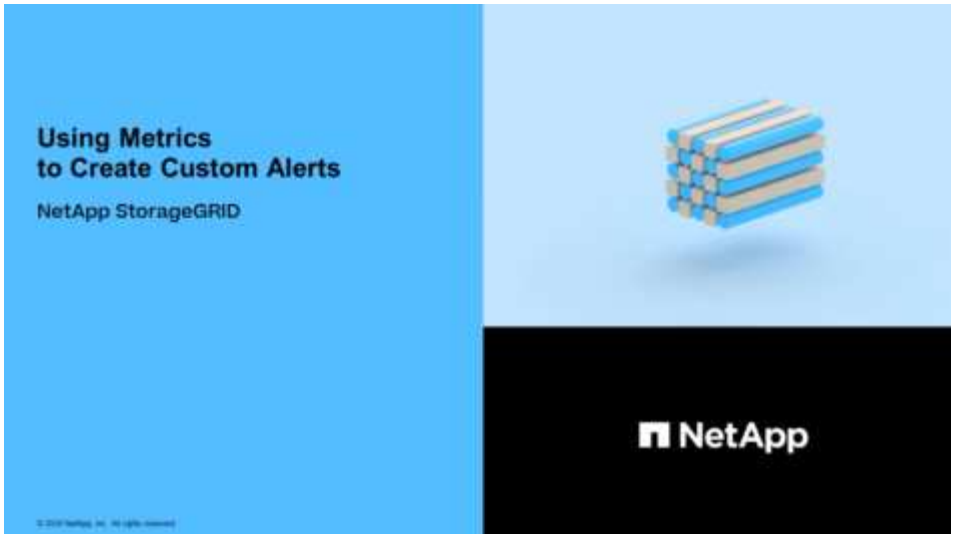
열 머리글	설명
이름	알림 규칙의 고유한 이름 및 설명입니다. 사용자 지정 경고 규칙이 먼저 나열되고 그 뒤에 기본 경고 규칙이 나열됩니다. 알림 규칙 이름은 이메일 알림의 제목입니다.
조건	이 알림이 트리거되는 시기를 결정하는 Prometheus 식입니다. 알림은 다음 심각도 수준 중 하나 이상으로 트리거될 수 있지만 각 심각도에 대한 조건은 필요하지 않습니다. • * 심각 * : StorageGRID 노드나 서비스의 정상적인 작동을 중지해 온 비정상적인 조건이 존재합니다. 기본 문제를 즉시 해결해야 합니다. 문제가 해결되지 않으면 서비스가 중단되거나 데이터가 손실될 수 있습니다. • * 주 * : 현재 작업에 영향을 미치거나 위험 경고에 대한 임계값에 근접한 비정상적인 상태가 존재합니다. StorageGRID 노드나 서비스의 정상 작동을 비정상적인 상태로 중지하지 않도록 주요 경고를 조사하고 모든 기본 문제를 해결해야 합니다. • * 보조 * : 시스템이 정상적으로 작동하지만 시스템이 계속 작동할 경우 시스템 기능에 영향을 줄 수 있는 비정상적인 상태가 존재합니다. 보다 심각한 문제를 초래하지 않도록 자체적으로 명확하지 않은 사소한 경고를 모니터링하고 해결해야 합니다.
유형	알림 규칙의 유형: • * 기본값 *: 시스템과 함께 제공되는 경고 규칙입니다. 기본 알림 규칙을 비활성화하거나 기본 알림 규칙의 조건 및 기간을 편집할 수 있습니다. 기본 알림 규칙은 제거할 수 없습니다. • * 기본값**: 편집된 조건 또는 기간이 포함된 기본 경고 규칙입니다. 필요에 따라 수정된 조건을 원래 기본값으로 쉽게 되돌릴 수 있습니다. • * 사용자 정의 *: 사용자가 만든 알림 규칙입니다. 사용자 지정 경고 규칙을 비활성화, 편집 및 제거할 수 있습니다.
상태	이 경고 규칙의 현재 활성화 또는 비활성화 여부를 나타냅니다. 비활성화된 경고 규칙의 조건은 평가되지 않으므로 경고가 트리거되지 않습니다.

사용자 지정 알림 규칙을 생성합니다

사용자 지정 알림 규칙을 만들어 알림을 트리거할 자체 조건을 정의할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저
- 알림 관리 또는 루트 액세스 권한이 있습니다
- 에 익숙합니다 일반적으로 사용되는 Prometheus 메트릭입니다
- 을(를) 이해합니다 "Prometheus 쿼리의 구문"
- 선택적으로 비디오를 시청했습니다. "비디오: 메트릭을 사용하여 사용자 지정 경고 생성"



이 작업에 대해

StorageGRID에서는 사용자 지정 경고의 유효성을 검사하지 않습니다. 사용자 지정 알림 규칙을 만들려면 다음 일반 지침을 따릅니다.

- 기본 알림 규칙의 조건을 확인하고 사용자 지정 알림 규칙의 예로 사용합니다.
- 경고 규칙에 대해 둘 이상의 조건을 정의하는 경우 모든 조건에 동일한 식을 사용합니다. 그런 다음 각 조건에 대한 임계값을 변경합니다.
- 각 조건에서 오타 및 논리 오류가 있는지 주의 깊게 확인합니다.
- Grid Management API에 나열된 메트릭만 사용하십시오.
- Grid Management API를 사용하여 표현식을 테스트할 때 "성공" 응답은 단순히 빈 응답 본체일 수 있습니다(경고가 트리거되지 않음). 알림이 실제로 트리거되었는지 확인하려면 임계값을 현재 참인 것으로 예상되는 값으로 일시적으로 설정할 수 있습니다.

  예를 들어 'node_memory_MemTotal_bytes<24000000000' 식을 테스트하려면 먼저 'node_memory_MemTotal_bytes>=0'을 실행하고 예상 결과를 확인합니다(모든 노드가 값을 반환함). 그런 다음 연산자 및 임계값을 다시 원하는 값으로 변경하고 다시 실행합니다. 이 식에 대한 현재 경고가 없음을 나타내는 결과가 없습니다.

- 알림이 예상대로 트리거되었음을 확인한 경우를 제외하고 사용자 지정 알림이 작동 중인 것으로 가정하지 마십시오.

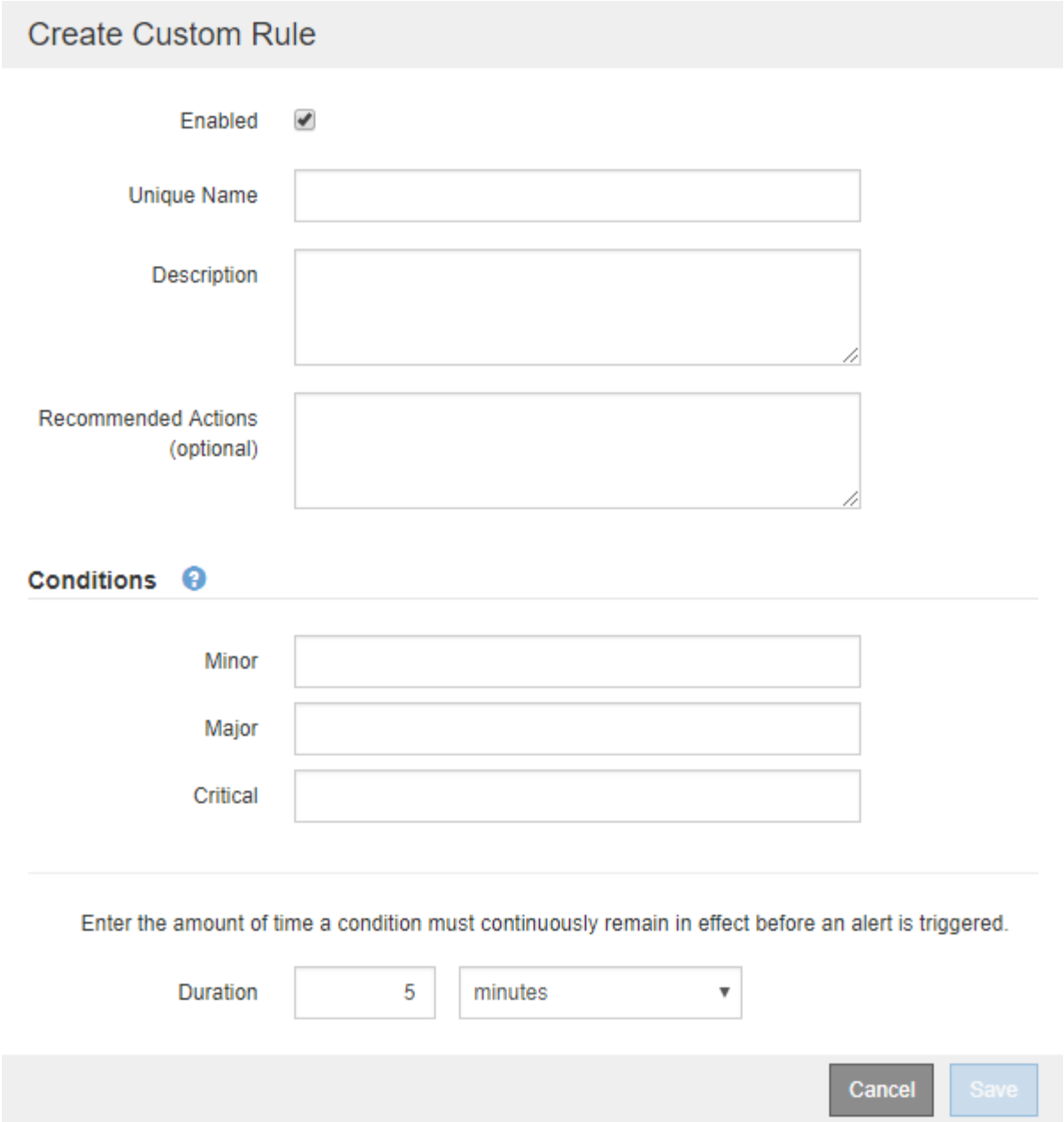
단계

1. 알림 * > * 규칙 * 을 선택합니다.

   경고 규칙 페이지가 나타납니다.

2. 사용자 지정 규칙 만들기 * 를 선택합니다.

   사용자 지정 규칙 만들기 대화 상자가 나타납니다.



3. 이 경고 규칙이 현재 활성화되어 있는지 여부를 확인하려면 * Enabled * (활성화 *) 확인란을 선택하거나 선택을 취소합니다.

   경고 규칙을 비활성화하면 해당 식이 계산되지 않고 경고가 트리거되지 않습니다.

4. 다음 정보를 입력합니다.

필드에 입력합니다	설명
고유 이름	이 규칙의 고유 이름입니다. 알림 규칙 이름은 알림 페이지에 표시되며 이메일 알림의 제목이기도 합니다. 알림 규칙의 이름은 1자에서 64자 사이여야 합니다.

필드에 입력합니다	설명
설명	발생한 문제에 대한 설명입니다. 설명은 경고 페이지와 이메일 알림에 표시되는 경고 메시지입니다. 알림 규칙에 대한 설명은 1자에서 128자 사이여야 합니다.
권장 조치	이 경고가 트리거될 때 수행할 권장 조치를 선택할 수도 있습니다. 권장 작업을 일반 텍스트로 입력합니다(서식 코드 없음). 경고 규칙에 권장되는 작업은 0자에서 1,024자 사이여야 합니다.

5. 조건 섹션에 하나 이상의 알림 심각도 수준에 대한 Prometheus 식을 입력합니다.

   기본 표현식은 대개 다음과 같습니다.

   '[metric][operator][value]'

   식은 임의의 길이일 수 있지만 사용자 인터페이스의 한 줄에 표시됩니다. 적어도 하나의 식이 필요합니다.

   이 식을 사용하면 노드에 설치된 RAM의 양이 24,000,000,000바이트(24GB) 미만인 경우 경고가 트리거됩니다.

   'node_memory_MemTotal_bytes<24000000000'

   사용 가능한 메트릭을 확인하고 Prometheus 식을 테스트하려면 도움말 아이콘을 선택합니다 ? 그리드 관리 API의 메트릭 섹션 링크를 따라 이동합니다.

6. [기간*] 필드에 경고가 트리거되기 전에 조건이 계속 유효해야 하는 시간을 입력하고 시간 단위를 선택합니다.

   조건이 참일 때 경고를 즉시 트리거하려면 * 0 * 을 입력합니다. 이 값을 늘려 일시적 조건이 경고를 트리거하지 않도록 합니다.

   기본값은 5분입니다.

7. 저장 * 을 선택합니다.

   대화 상자가 닫히고 새 사용자 지정 경고 규칙이 경고 규칙 테이블에 나타납니다.

알림 규칙을 편집합니다

알림 규칙을 편집하여 트리거 조건을 변경할 수 있습니다. 사용자 지정 알림 규칙의 경우 규칙 이름, 설명 및 권장 작업을 업데이트할 수도 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 알림 관리 또는 루트 액세스 권한이 있습니다.

이 작업에 대해

기본 경고 규칙을 편집할 때 Minor, Major 및 Critical 경고의 조건 및 기간을 변경할 수 있습니다. 사용자 지정 알림 규칙을 편집할 때 규칙의 이름, 설명 및 권장 작업을 편집할 수도 있습니다.

알림 규칙을 편집하기로 결정할 때는 주의해야 합니다. 트리거 값을 변경하는 경우 중요한 작업이 완료되지 못할 때까지 기본 문제를 감지하지 못할 수 있습니다.

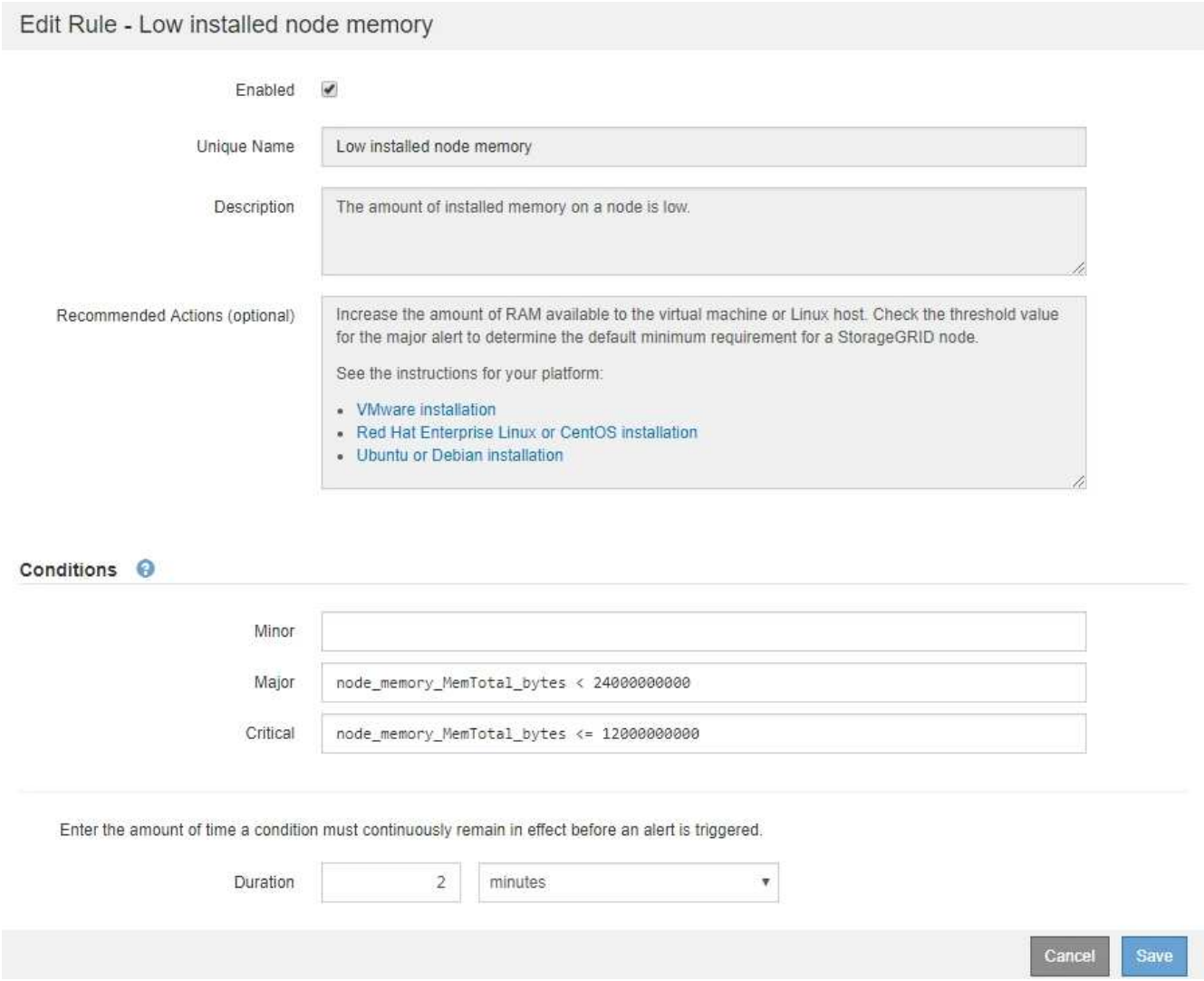
단계

1. 알림 * > * 규칙 * 을 선택합니다.

   경고 규칙 페이지가 나타납니다.

2. 편집하려는 경고 규칙에 대한 라디오 버튼을 선택합니다.
3. 규칙 편집 * 을 선택합니다.

   규칙 편집 대화 상자가 나타납니다. 이 예제에서는 기본 경고 규칙을 보여 줍니다. 고유 이름, 설명 및 권장 조치 필드는 사용할 수 없으며 편집할 수 없습니다.



4. 이 경고 규칙이 현재 활성화되어 있는지 여부를 확인하려면 * Enabled * (활성화 *) 확인란을 선택하거나 선택을 취소합니다.

   경고 규칙을 비활성화하면 해당 식이 계산되지 않고 경고가 트리거되지 않습니다.

현재 알림에 대한 알림 규칙을 사용하지 않도록 설정한 경우 알림이 더 이상 활성 알림으로 나타나지 않을 때까지 몇 분 정도 기다려야 합니다.

일반적으로 기본 알림 규칙을 사용하지 않는 것이 좋습니다. 경고 규칙을 비활성화하면 중요한 작업이 완료되지 못할 때까지 기본 문제를 감지하지 못할 수 있습니다.

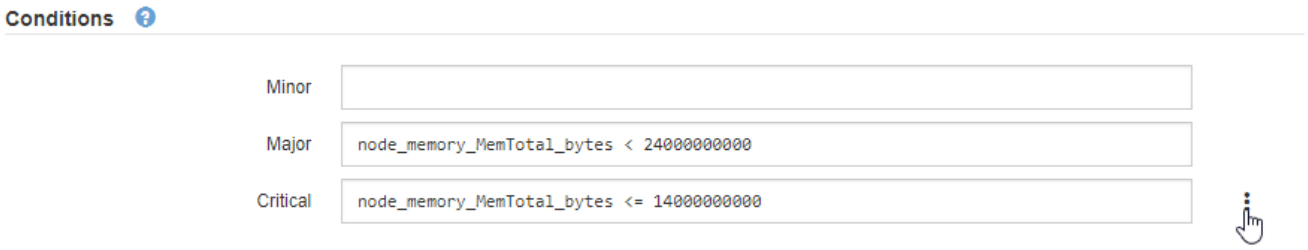
5. 사용자 지정 알림 규칙의 경우 필요에 따라 다음 정보를 업데이트합니다.

기본 경고 규칙에 대해서는 이 정보를 편집할 수 없습니다.

필드에 입력합니다	설명
고유 이름	이 규칙의 고유 이름입니다. 알림 규칙 이름은 알림 페이지에 표시되며 이메일 알림의 제목이기도 합니다. 알림 규칙의 이름은 1자에서 64자 사이여야 합니다.
설명	발생한 문제에 대한 설명입니다. 설명은 경고 페이지와 이메일 알림에 표시되는 경고 메시지입니다. 알림 규칙에 대한 설명은 1자에서 128자 사이여야 합니다.
권장 조치	이 경고가 트리거될 때 수행할 권장 조치를 선택할 수도 있습니다. 권장 작업을 일반 텍스트로 입력합니다(서식 코드 없음). 경고 규칙에 권장되는 작업은 0자에서 1,024자 사이여야 합니다.

6. 조건 섹션에서 하나 이상의 알림 심각도 수준에 대한 Prometheus 식을 입력하거나 업데이트합니다.

편집된 기본 경고 규칙의 조건을 원래 값으로 복원하려면 수정된 조건의 오른쪽에 있는 세 개의 점을 선택합니다.



현재 알림에 대한 조건을 업데이트하면 이전 조건이 해결될 때까지 변경 내용이 적용되지 않을 수 있습니다. 다음에 규칙의 조건 중 하나가 충족되면 해당 알림에 업데이트된 값이 반영됩니다.

기본 표현식은 대개 다음과 같습니다.

'[metric][operator][value]'

식은 임의의 길이일 수 있지만 사용자 인터페이스의 한 줄에 표시됩니다. 적어도 하나의 식이 필요합니다.

이 식을 사용하면 노드에 설치된 RAM의 양이 24,000,000,000바이트(24GB) 미만인 경우 경고가 트리거됩니다.

'node_memory_MemTotal_bytes<24000000000'

7. [기간*] 필드에 경고가 트리거되기 전에 조건이 계속 유효해야 하는 시간을 입력하고 시간 단위를 선택합니다.

   조건이 참일 때 경고를 즉시 트리거하려면 * 0 * 을 입력합니다. 이 값을 늘려 일시적 조건이 경고를 트리거하지 않도록 합니다.

   기본값은 5분입니다.

8. 저장 * 을 선택합니다.

   기본 경고 규칙을 편집한 경우 유형 열에 * 기본값** 이 나타납니다. 기본 또는 사용자 지정 경고 규칙을 비활성화하면 * 상태 * 열에 * 사용 안 함 * 이 나타납니다.

경고 규칙을 비활성화합니다

기본 또는 사용자 지정 알림 규칙에 대해 활성화/비활성화 상태를 변경할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 알림 관리 또는 루트 액세스 권한이 있습니다.

이 작업에 대해

경고 규칙을 비활성화하면 해당 식이 계산되지 않고 경고가 트리거되지 않습니다.

> 일반적으로 기본 알림 규칙을 사용하지 않는 것이 좋습니다. 경고 규칙을 비활성화하면 중요한 작업이 완료되지 못할 때까지 기본 문제를 감지하지 못할 수 있습니다.

단계

1. 알림 * > * 규칙 * 을 선택합니다.

   경고 규칙 페이지가 나타납니다.

2. 비활성화 또는 활성화할 경고 규칙의 라디오 버튼을 선택합니다.
3. 규칙 편집 * 을 선택합니다.

   규칙 편집 대화 상자가 나타납니다.

4. 이 경고 규칙이 현재 활성화되어 있는지 여부를 확인하려면 * Enabled * (활성화 *) 확인란을 선택하거나 선택을 취소합니다.

   경고 규칙을 비활성화하면 해당 식이 계산되지 않고 경고가 트리거되지 않습니다.

   > 현재 알림에 대한 알림 규칙을 사용하지 않도록 설정한 경우 알림이 더 이상 활성 알림으로 표시되지 않을 때까지 몇 분 정도 기다려야 합니다.

5. 저장 * 을 선택합니다.
   - 상태 * 열에 * 사용 안 함 * 이 나타납니다.

사용자 지정 알림 규칙을 더 이상 사용하지 않으려는 경우 제거할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 알림 관리 또는 루트 액세스 권한이 있습니다.

단계

1. 알림 * > * 규칙 * 을 선택합니다.

   경고 규칙 페이지가 나타납니다.

2. 제거할 사용자 지정 알림 규칙의 라디오 버튼을 선택합니다.

   기본 알림 규칙은 제거할 수 없습니다.

3. 사용자 지정 규칙 제거 * 를 선택합니다.

   확인 대화 상자가 나타납니다.

4. 경고 규칙을 제거하려면 * OK * 를 선택합니다.

   알림의 활성 인스턴스는 10분 이내에 해결됩니다.

경고 알림을 관리합니다

경고에 대한 **SNMP** 알림을 설정합니다

경고가 발생할 때 StorageGRID에서 SNMP 알림을 보내도록 하려면 StorageGRID SNMP 에이전트를 활성화하고 하나 이상의 트랩 대상을 구성해야 합니다.

그리드 관리자의 * 구성 * > * 모니터링 * > * SNMP 에이전트 * 옵션을 사용하거나 그리드 관리 API의 SNMP 끝점을 사용하여 StorageGRID SNMP 에이전트를 활성화 및 구성할 수 있습니다. SNMP 에이전트는 SNMP 프로토콜의 세 가지 버전을 모두 지원합니다.

SNMP 에이전트를 구성하는 방법에 대한 자세한 내용은 을 참조하십시오 SNMP 모니터링을 사용합니다.

StorageGRID SNMP 에이전트를 구성한 후 두 가지 유형의 이벤트 기반 알림을 보낼 수 있습니다.

- 트랩은 관리 시스템에서 확인이 필요하지 않은 SNMP 에이전트가 보낸 알림입니다. 트랩은 알림이 트리거되는 등 StorageGRID 내에 발생한 사항을 관리 시스템에 알리는 역할을 합니다. 트랩은 SNMP의 세 가지 버전에서 모두 지원됩니다.
- 는 트랩과 유사하지만 관리 시스템에서 확인을 필요로 합니다. SNMP 에이전트가 일정 시간 내에 승인을 받지 못하면 승인을 받거나 최대 재시도 값에 도달할 때까지 알림을 다시 보냅니다. SNMPv2c 및 SNMPv3에서 알림이 지원됩니다.

기본 또는 사용자 지정 경고가 심각도 수준에서 트리거되면 트랩 및 알림 알림이 전송됩니다. 경고에 대한 SNMP 알림을 표시하지 않으려면 경고에 대한 무음을 구성해야 합니다. 을 참조하십시오 알림 메시지를 해제합니다.

경고 알림은 선호하는 송신자가 되도록 구성된 관리 노드에서 보냅니다. 기본적으로 기본 관리 노드가 선택됩니다. 를 참조하십시오 StorageGRID 관리 지침.

> 특정 알람(기존 시스템)이 지정된 심각도 수준 이상으로 트리거될 때도 트랩 및 알림 알림이 전송되지만, 모든 알람 또는 모든 알람 심각도에 대해 SNMP 알림이 전송되지 않습니다. 을 참조하십시오 SNMP 알림을 생성하는 알람(레거시 시스템).

알림에 대한 이메일 알림을 설정합니다

경고가 발생할 때 이메일 알림을 보내려면 SMTP 서버에 대한 정보를 제공해야 합니다. 알림 메시지를 받는 사람의 전자 메일 주소도 입력해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 알림 관리 또는 루트 액세스 권한이 있습니다.

이 작업에 대해

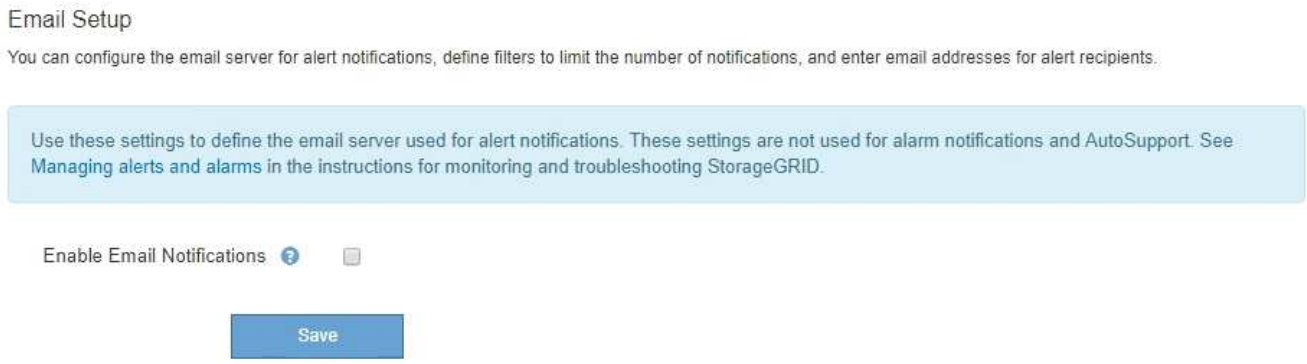
알람과 경고는 독립적인 시스템이므로 경고 알림에 사용되는 이메일 설정은 알람 알림 및 AutoSupport 메시지에 사용되지 않습니다. 그러나 모든 알림에 동일한 이메일 서버를 사용할 수 있습니다.

StorageGRID 배포에 여러 관리 노드가 포함된 경우 알림 알림을 보내는 기본 설정 관리자 노드를 선택할 수 있습니다. 알람 알림 및 AutoSupport 메시지에도 동일한 "선호 발신자"가 사용됩니다. 기본적으로 기본 관리 노드가 선택됩니다. 자세한 내용은 를 참조하십시오 StorageGRID 관리 지침.

단계

1. 알림 * > * 이메일 설정 * 을 선택합니다.

   이메일 설정 페이지가 나타납니다.



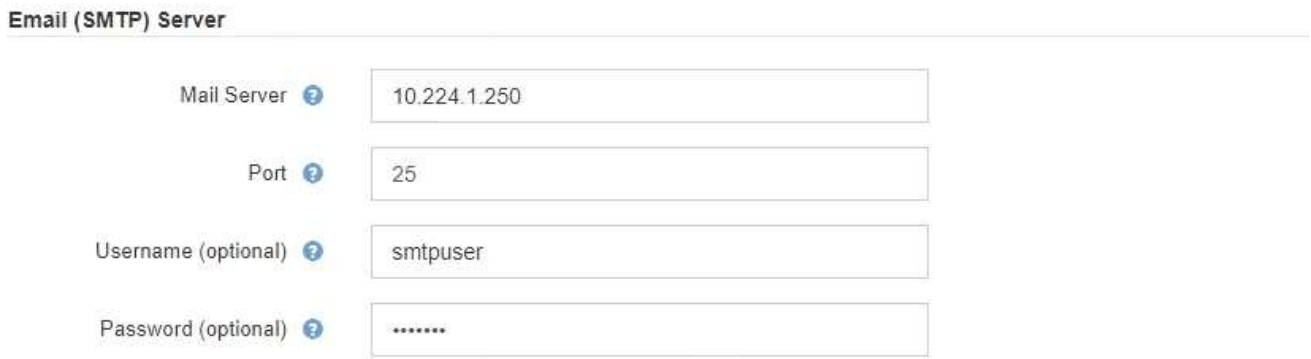
2. 알림이 구성된 임계값에 도달할 때 알림 이메일을 보내도록 하려면 * 이메일 알림 활성화 * 확인란을 선택합니다.

   이메일(SMTP) 서버, 전송 계층 보안(TLS), 이메일 주소 및 필터 섹션이 나타납니다.

3. 이메일(SMTP) 서버 섹션에서 StorageGRID가 SMTP 서버에 액세스하는 데 필요한 정보를 입력합니다.

   SMTP 서버에 인증이 필요한 경우 사용자 이름과 암호를 모두 제공해야 합니다.

필드에 입력합니다	를 입력합니다
메일 서버	SMTP 서버의 FQDN(정규화된 도메인 이름) 또는 IP 주소입니다.
포트	SMTP 서버에 액세스하는 데 사용되는 포트입니다. 1에서 65535 사이여야 합니다.
사용자 이름(선택 사항)	SMTP 서버에 인증이 필요한 경우 인증할 사용자 이름을 입력합니다.
암호(선택 사항)	SMTP 서버에 인증이 필요한 경우 인증할 암호를 입력합니다.



4. 전자 메일 주소 섹션에서 보낸 사람 및 각 받는 사람에 대한 전자 메일 주소를 입력합니다.

   a. 보낸 사람 e-메일 주소 * 에 대해 알림 알림의 보낸 사람 주소로 사용할 유효한 e-메일 주소를 지정합니다.

      예를 들면, 'toragegrid-alerts@example.com'입니다

   b. 받는 사람 섹션에서 경고가 발생할 때 전자 메일을 받아야 하는 각 전자 메일 목록의 전자 메일 주소를 입력합니다.

      더하기 아이콘을 선택합니다 ✚ 받는 사람을 추가합니다.

5. SMTP 서버와의 통신에 TLS(전송 계층 보안)가 필요한 경우 TLS(전송 계층 보안) 섹션에서 * TLS * 필요 를 선택합니다.

   a. CA 인증서* 필드에 SMTP 서버 ID를 확인하는 데 사용할 CA 인증서를 제공합니다.

      내용을 복사하여 이 필드에 붙여넣거나 * 찾아보기 * 를 선택하고 파일을 선택할 수 있습니다.

      각 중간 발급 CA(인증 기관)의 인증서가 포함된 단일 파일을 제공해야 합니다. 파일에는 인증서 체인 순서에

연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.

b. SMTP 전자 메일 서버에서 인증을 위해 클라이언트 인증서를 제공하도록 전자 메일 보낸 사람이 필요한 경우 * 클라이언트 인증서 보내기 * 확인란을 선택합니다.

c. 클라이언트 인증서 * 필드에 SMTP 서버로 보낼 PEM 인코딩된 클라이언트 인증서를 입력합니다.

   내용을 복사하여 이 필드에 붙여넣거나 * 찾아보기 * 를 선택하고 파일을 선택할 수 있습니다.

d. 개인 키 * 필드에 암호화되지 않은 PEM 인코딩으로 클라이언트 인증서에 대한 개인 키를 입력합니다.

   내용을 복사하여 이 필드에 붙여넣거나 * 찾아보기 * 를 선택하고 파일을 선택할 수 있습니다.

   이메일 설정을 편집해야 하는 경우 연필 아이콘을 선택하여 이 필드를 업데이트합니다.

Transport Layer Security (TLS)

Require TLS ☑

CA Certificate

```
-----BEGIN CERTIFICATE-----
1234567890abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
-----END CERTIFICATE-----
```

Browse

Send Client Certificate ☑

Client Certificate

```
-----BEGIN CERTIFICATE-----
1234567890abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
-----END CERTIFICATE-----
```

Browse

Private Key

```
-----BEGIN PRIVATE KEY-----
1234567890abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
-----BEGIN PRIVATE KEY-----
```

Browse

6. 특정 경고에 대한 규칙이 해제된 경우를 제외하고 필터 섹션에서 이메일 알림을 발생시킬 알림 심각도 수준을 선택합니다.

심각도입니다	설명
경미, 중대, 중대	경고 규칙에 대한 하위, 주 또는 위험 조건이 충족되면 이메일 알림이 전송됩니다.
주요, 중요	경고 규칙에 대한 중요 또는 위험 조건이 충족되면 이메일 알림이 전송됩니다. 알림 메시지는 사소한 알림에 대해서는 전송되지 않습니다.
중요 전용	경고 규칙에 대한 위험 조건이 충족된 경우에만 이메일 알림이 전송됩니다. Minor 또는 Major 알림에 대한 알림은 전송되지 않습니다.

7. 이메일 설정을 테스트할 준비가 되면 다음 단계를 수행하십시오.
   a. 테스트 이메일 전송 * 을 선택합니다.

      테스트 이메일이 전송되었음을 나타내는 확인 메시지가 나타납니다.

   b. 모든 이메일 수신인의 확인란을 선택하고 테스트 이메일이 수신되었는지 확인합니다.

      > 몇 분 이내에 이메일을 받지 못했거나 * 이메일 알림 실패 * 경고가 트리거된 경우 설정을 확인하고 다시 시도하십시오.

   c. 다른 관리 노드에 로그인하고 테스트 이메일을 보내 모든 사이트의 연결을 확인합니다.

      > 알림 알림을 테스트할 때는 모든 관리 노드에 로그인하여 연결을 확인해야 합니다. 이는 모든 관리 노드가 테스트 이메일을 보내는 알람 알림 및 AutoSupport 메시지를 테스트하는 것과는 다릅니다.

8. 저장 * 을 선택합니다.

   테스트 이메일을 전송해도 설정이 저장되지 않습니다. 저장 * 을 선택해야 합니다.

   이메일 설정이 저장됩니다.

알림 e-메일 알림에 포함된 정보입니다

SMTP 이메일 서버를 구성한 후에는 경고 규칙이 무음으로 표시되지 않는 한 경고가 트리거될 때 지정된 수신자에게 이메일 알림이 전송됩니다. 을 참조하십시오 알림 메시지를 해제합니다.

이메일 알림에는 다음 정보가 포함됩니다.

NetApp StorageGRID

Low object data storage (6 alerts) (1)

The space available for storing object data is low. (2)

Recommended actions (3)

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

Node	DC1-S1-226
Site	DC1 225-230
Severity	Minor
Time triggered	Fri Jun 28 14:43:27 UTC 2019
Job	storagegrid
Service	ldr

(4)

DC1-S2-227

Node	DC1-S2-227
Site	DC1 225-230
Severity	Minor
Time triggered	Fri Jun 28 14:43:27 UTC 2019
Job	storagegrid
Service	ldr

Sent from: DC1-ADM1-225 (5)

속성 표시기	설명
1	알림의 이름, 이 알림의 활성 인스턴스 수 순으로 표시됩니다.
2	알림에 대한 설명입니다.
3	경고에 대해 권장되는 모든 작업
4	영향을 받는 노드 및 사이트, 알림 심각도, 경고 규칙이 트리거된 UTC 시간, 영향을 받는 작업 및 서비스 이름 등 알림의 각 활성 인스턴스에 대한 세부 정보입니다.
5	알림을 보낸 관리 노드의 호스트 이름입니다.

알림을 그룹화하는 방법

알림이 트리거될 때 과도한 수의 이메일 알림이 전송되지 않도록 하기 위해 StorageGRID는 동일한 알림에 여러 개의 알림을 그룹화하려고 시도합니다.

StorageGRID가 이메일 알림에서 여러 경고를 그룹화하는 방법의 예는 다음 표를 참조하십시오.

동작	예
각 알림 알림은 이름이 같은 알림에만 적용됩니다. 이름이 다른 두 개의 알림이 동시에 트리거되면 두 개의 이메일 알림이 전송됩니다.	• 경고 A는 두 노드에서 동시에 트리거됩니다. 하나의 알림만 전송됩니다. • 노드 1에서 경고 A가 트리거되고, 노드 2에서 경고 B가 동시에 트리거됩니다. 각 알림에 대해 하나씩 두 개의 알림이 전송됩니다.
특정 노드의 특정 경고에 대해 둘 이상의 심각도에 대한 임계값에 도달하면 가장 심각한 경고에 대해서만 알림이 전송됩니다.	• 경고 A가 트리거되고 Minor, Major 및 Critical 경고 임계값에 도달합니다. 긴급 경고에 대해 하나의 알림이 전송됩니다.
알림이 처음 트리거되면 StorageGRID는 2분 후에 알림을 보냅니다. 같은 이름의 다른 알림이 이 시간 동안 트리거되면 StorageGRID는 초기 알림에서 모든 경고를 그룹화합니다	1. 알림 A는 노드 1의 오전 8시에 트리거됩니다. 알림이 전송되지 않습니다. 2. 알림 A는 노드 2의 08:01에 트리거됩니다. 알림이 전송되지 않습니다. 3. 08:02에 알림의 두 인스턴스를 모두 보고하라는 알림이 전송됩니다.
같은 이름의 다른 알림이 트리거되면 StorageGRID는 10분 후에 새 알림을 보냅니다. 새 알림은 이전에 보고되었더라도 모든 활성 경고(해제되지 않은 현재 경고)를 보고합니다.	1. 알림 A는 노드 1의 오전 8시에 트리거됩니다. 통지는 08:02에 전송됩니다. 2. 알림 A는 노드 2의 오전 8시 5분에 트리거됩니다. 두 번째 통지는 08:15(10분 후)에 전송됩니다. 두 노드가 모두 보고됩니다.
동일한 이름의 현재 알림이 여러 개 있고 이 경고 중 하나가 해결된 경우, 경고가 해결된 노드에서 다시 발생하면 새 알림이 전송되지 않습니다.	1. 노드 1에 대해 경고 A가 트리거됩니다. 알림이 전송됩니다. 2. 노드 2에 대해 경고 A가 트리거됩니다. 두 번째 알림이 전송됩니다. 3. 노드 2에 대해 경고 A가 해결되었지만 노드 1에 대해 활성 상태로 유지됩니다. 4. 노드 2에 대해 경고 A가 다시 트리거됩니다. 노드 1에 대한 알림이 아직 활성 상태이므로 새 알림이 전송되지 않습니다.
StorageGRID는 모든 경고 인스턴스가 해결되거나 경고 규칙이 해제될 때까지 7일마다 이메일 알림을 계속 전송합니다.	1. 3월 8일에 노드 1에 대해 경고 A가 트리거됩니다. 알림이 전송됩니다. 2. 경고 A가 해결되지 않거나 소거되지 않았습니다. 추가 통지는 3월 15일, 3월 22일, 3월 29일 등으로 발송됩니다.

경고 **e**-메일 알림 문제를 해결합니다

이메일 알림 실패 * 알림이 트리거되거나 테스트 알림 이메일 알림을 받을 수 없는 경우 다음 단계를 따라 문제를 해결하십시오.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 알림 관리 또는 루트 액세스 권한이 있습니다.

단계

1. 설정을 확인합니다.
   a. 알림 * > * 이메일 설정 * 을 선택합니다.
   b. 이메일(SMTP) 서버 설정이 올바른지 확인합니다.
   c. 받는 사람에 대해 유효한 전자 메일 주소를 지정했는지 확인합니다.
2. 스팸 필터를 확인하고 이메일이 정크 폴더로 전송되지 않았는지 확인합니다.
3. 이메일 관리자에게 문의하여 보낸 사람 주소의 이메일이 차단되지 않았는지 확인하십시오.
4. 관리 노드에 대한 로그 파일을 수집한 다음 기술 지원 부서에 문의하십시오.

   기술 지원 부서에서는 로그의 정보를 사용하여 무엇이 잘못되었는지 확인할 수 있습니다. 예를 들어, 지정한 서버에 연결할 때 prometheus.log 파일에 오류가 표시될 수 있습니다.

   을 참조하십시오 로그 파일 및 시스템 데이터를 수집합니다.

알림 메시지를 해제합니다

선택적으로, 알림 알림을 일시적으로 표시하지 않도록 Silence를 구성할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 알림 관리 또는 루트 액세스 권한이 있습니다.

이 작업에 대해

전체 그리드, 단일 사이트 또는 단일 노드 및 하나 이상의 심각도에 대한 경고 규칙을 해제할 수 있습니다. 각 무정지는 단일 경고 규칙 또는 모든 경고 규칙에 대한 모든 알림을 표시하지 않습니다.

SNMP 에이전트를 사용하도록 설정한 경우, 이 옵션을 해제해도 SNMP 트랩이 억제되고 에 알립니다.

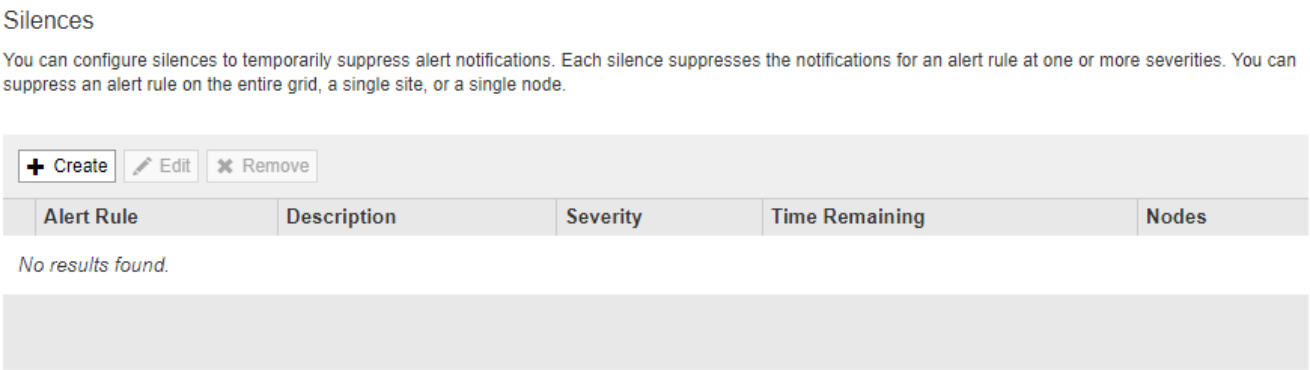
> 경고 규칙을 해제할 때는 주의하십시오. 경고를 음소거하면 중요한 작업이 완료되지 못하게 될 때까지 기본 문제를 감지하지 못할 수 있습니다.

> 알람과 알림은 독립 시스템이므로 이 기능을 사용하여 알람 알림을 억제할 수 없습니다.

단계

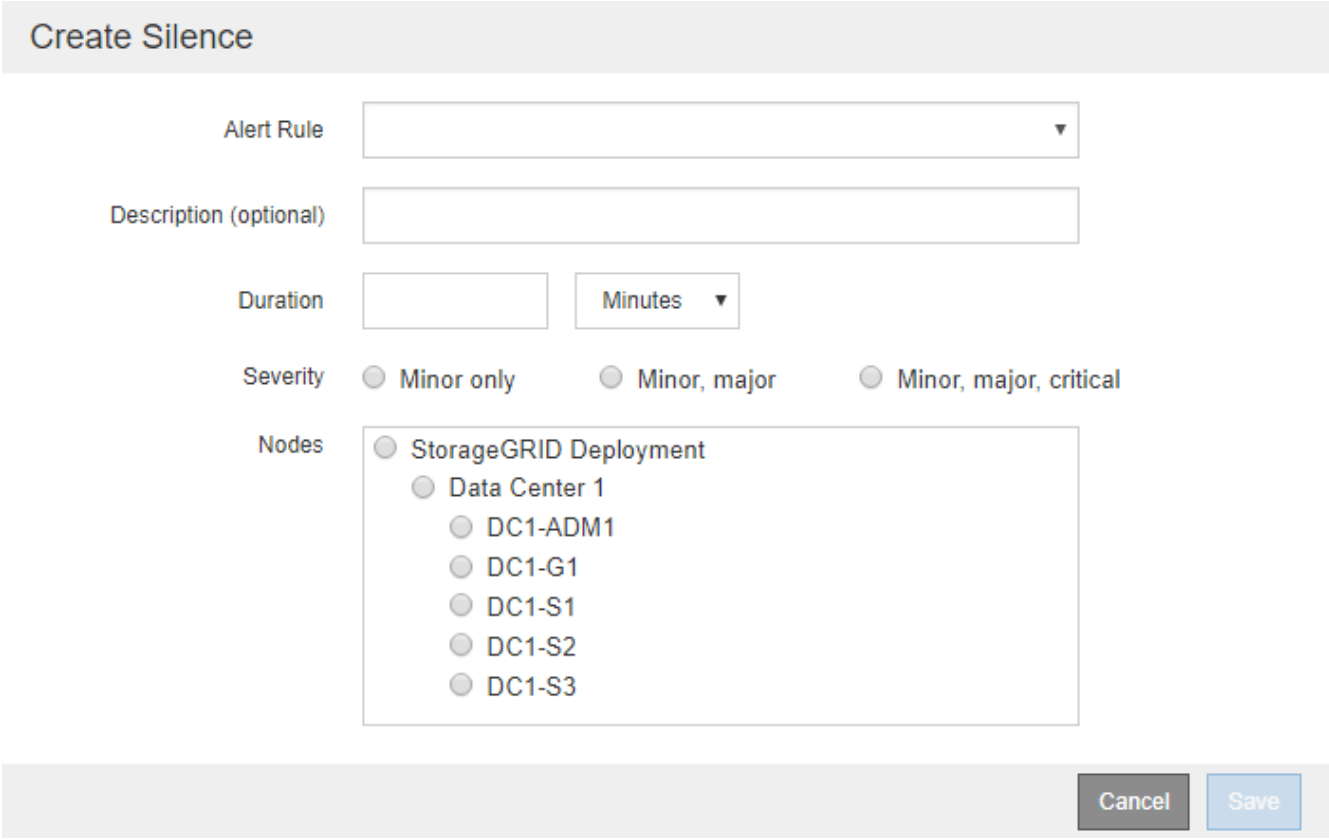
1. alerts * > * silences * 를 선택합니다.

   Silence 페이지가 나타납니다.



2. Create * 를 선택합니다.

   Create Silence 대화상자가 나타납니다.



3. 다음 정보를 선택하거나 입력합니다.

필드에 입력합니다	설명
경고 규칙	무음 설정할 알림 규칙의 이름입니다. 알림 규칙이 비활성화된 경우에도 기본 또는 사용자 지정 알림 규칙을 선택할 수 있습니다. • 참고: * 이 대화 상자에 지정된 기준을 사용하여 모든 경고 규칙을 해제하려면 * 모든 규칙 * 을 선택합니다.
설명	선택적으로 무음 에 대한 설명입니다. 예를 들어, 이 침묵의 목적을 설명하십시오.

필드에 입력합니다	설명
기간	몇 분, 몇 시간 또는 며칠 내에 이 침묵이 얼마나 오랫동안 지속되기를 바라는지. 5분에서 1,825일(5년)까지 침묵이 적용됩니다. • 참고: * 알림 규칙을 장시간 사용하지 않아야 합니다. 경고 규칙이 해제된 경우 중요한 작업이 완료되지 못하도록 하기 전까지는 기본 문제를 감지하지 못할 수 있습니다. 그러나, * 서비스 어플라이언스 링크 다운 * 알림 및 * 스토리지 어플라이언스 링크 다운 * 경고와 같이 특정 의도적 구성에 의해 경고가 트리거되는 경우, 확장된 무음을 사용해야 할 수도 있습니다.
심각도입니다	어떤 경고 심각도 또는 심각도를 소거해야 하는지 확인합니다. 선택한 심각도 중 하나에서 경고가 트리거되면 알림이 전송되지 않습니다.
노드	이 무정적을 적용할 노드나 노드입니다. 전체 그리드, 단일 사이트 또는 단일 노드에 대한 알림 규칙이나 모든 규칙을 억제할 수 있습니다. 전체 그리드를 선택하면 모든 사이트와 모든 노드에 무음(Silence)이 적용됩니다. 사이트를 선택하면 해당 사이트의 노드에만 무음 이 적용됩니다. • 참고: * 각 무음 시 둘 이상의 노드 또는 둘 이상의 사이트를 선택할 수 없습니다. 둘 이상의 노드 또는 둘 이상의 사이트에서 한 번에 동일한 알림 규칙을 억제하려면 추가 비누를 만들어야 합니다.

4. 저장 * 을 선택합니다.
5. 만료되기 전에 무음을 수정하거나 종료하려면 무음을 편집하거나 제거할 수 있습니다.

옵션을 선택합니다	설명
무음을 편집합니다	a. alerts * > * silences * 를 선택합니다. b. 테이블에서 편집하려는 무음(Silence)에 대한 라디오 버튼을 선택합니다. c. 편집 * 을 선택합니다. d. 설명, 남은 시간, 선택한 심각도 또는 영향을 받는 노드를 변경합니다. e. 저장 * 을 선택합니다.
정적을 제거합니다	a. alerts * > * silences * 를 선택합니다. b. 테이블에서 제거할 무음(Silence)에 대한 라디오 버튼을 선택합니다. c. 제거 * 를 선택합니다. d. 이 무음을 제거할 것인지 확인하려면 * OK * 를 선택하십시오. ◦ 참고 *: 이제 이 경고가 트리거될 때 알림이 전송됩니다(다른 무음으로 인해 억제되지 않는 경우). 이 경고가 현재 트리거된 경우 이메일 또는 SNMP 알림을 보내고 경고 페이지를 업데이트하는 데 몇 분 정도 걸릴 수 있습니다.

관련 정보

- SNMP 에이전트를 구성합니다

StorageGRID 알람 시스템은 정상 작동 중에 가끔 발생하는 문제 지점을 식별하는 데 사용되는 레거시 시스템입니다.

> 기존 알람 시스템은 계속 지원되지만, 알림 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

알람 등급(레거시 시스템)

레거시 알람은 상호 배타적인 두 가지 알람 클래스 중 하나에 속할 수 있습니다.

- 기본 알람은 각 StorageGRID 시스템과 함께 제공되며 수정할 수 없습니다. 그러나 기본 알람을 비활성화하거나 글로벌 사용자 정의 알람을 정의하여 재정의할 수 있습니다.
- 글로벌 사용자 정의 알람은 StorageGRID 시스템에서 지정된 유형의 모든 서비스의 상태를 모니터링합니다. 글로벌 사용자 정의 알람을 생성하여 기본 알람을 재정의할 수 있습니다. 새 글로벌 사용자 지정 알람을 만들 수도 있습니다. 이 기능은 StorageGRID 시스템의 사용자 지정 조건을 모니터링하는 데 유용합니다.

알람 트리거 논리(레거시 시스템)

StorageGRID 속성이 알람 클래스(기본값 또는 글로벌 사용자 정의)와 알람 심각도 수준의 조합에 대해 TRUE로 평가되는 임계값에 도달하면 레거시 알람이 트리거됩니다.

아이콘을 클릭합니다	색상	알람 심각도입니다	의미
	노란색	주의	노드가 그리드에 연결되어 있지만 정상적인 작동에 영향을 주지 않는 비정상적인 상태가 존재합니다.
	연한 주황색	경미합니다	노드가 그리드에 연결되어 있지만 향후 운영에 영향을 미칠 수 있는 비정상적인 조건이 존재합니다. 에스컬레이션을 방지하려면 조사해야 합니다.
	진한 주황색	전공	노드가 그리드에 연결되어 있지만 현재 작업에 영향을 미치는 비정상적인 상태가 존재합니다. 에스컬레이션을 방지하려면 즉각적인 주의가 필요합니다.
	빨간색	심각	노드가 그리드에 연결되었지만 정상 작동을 중지한 비정상적인 조건이 존재합니다. 문제를 즉시 해결해야 합니다.

알람 심각도 및 해당 임계값은 모든 숫자 특성에 대해 설정할 수 있습니다. 각 관리 노드의 NMS 서비스는 현재 속성 값을 구성된 임계값에 대해 지속적으로 모니터링합니다. 알람이 트리거되면 지정된 모든 직원에게 알림이 전송됩니다.

Normal(정상)의 심각도 수준은 알람을 트리거하지 않습니다.

속성 값은 해당 속성에 대해 정의된 활성화된 경보 목록에 대해 평가됩니다. 다음 순서로 알람 목록을 확인하여 속성에 대해 정의되고 활성화된 알람이 있는 첫 번째 알람 클래스를 찾습니다.

1. Critical에서 Notice 까지 알람 심각도를 갖는 Global Custom 알람

2. Critical에서 Notice 까지 알람 심각도를 갖는 기본 알람.

상위 알람 클래스에서 해당 속성에 대해 활성화된 알람이 발견된 후 NMS 서비스는 해당 클래스 내에서만 평가합니다. NMS 서비스는 다른 낮은 우선 순위 클래스에 대해 평가되지 않습니다. 즉, 속성에 대해 활성화된 글로벌 사용자 정의 경보가 있는 경우 NMS 서비스는 글로벌 사용자 정의 알람에 대해서만 특성 값을 평가합니다. 기본 알람은 평가되지 않습니다. 따라서 속성에 대해 활성화된 기본 알람은 알람을 트리거하는 데 필요한 기준을 충족할 수 있지만 동일한 속성에 대해 지정된 기준을 충족하지 않는 Global Custom 알람이 활성화되었기 때문에 트리거되지 않습니다. 알람이 트리거되지 않고 알림이 전송되지 않습니다.

알람 트리거링 예

이 예제를 사용하여 전역 사용자 정의 알람과 기본 알람이 트리거되는 방식을 이해할 수 있습니다.

다음 예제에서 속성에 글로벌 사용자 정의 알람과 기본 알람이 정의되어 있고 다음 표에 나와 있는 것처럼 활성화되어 있습니다.

	글로벌 사용자 지정 알람 임계값 (활성화됨)	기본 알람 임계값(활성화됨)
주의	>= 1500	>= 1000
경미합니다	>= 15,000	>= 1000
전공	>= 150,000	>= 250,000입니다

속성 값이 1000일 때 평가되면 알람이 트리거되지 않고 알림이 전송되지 않습니다.

전체 사용자 정의 알람이 기본 알람보다 우선합니다. 1000의 값이 글로벌 사용자 지정 알람의 심각도 수준의 임계값에 도달하지 않습니다. 그 결과, 알람 레벨이 정상으로 평가됩니다.

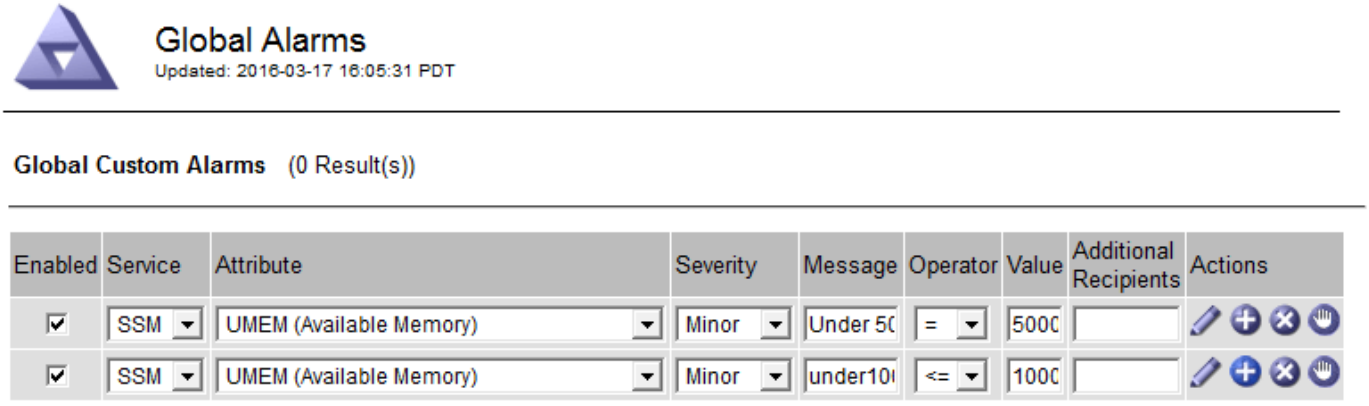
위 시나리오 이후 Global Custom(전체 사용자 정의) 경보가 비활성화되면 아무 것도 변경되지 않습니다. 새 알람 레벨이 트리거되기 전에 속성 값을 재평가해야 합니다.

전역 사용자 정의 경보를 비활성화한 상태에서 특성 값을 재평가하면 기본 알람의 임계값에 대해 속성 값이 평가됩니다. 알람 수준은 알림 수준 경보를 트리거하고 지정된 직원에게 이메일 알림을 보냅니다.

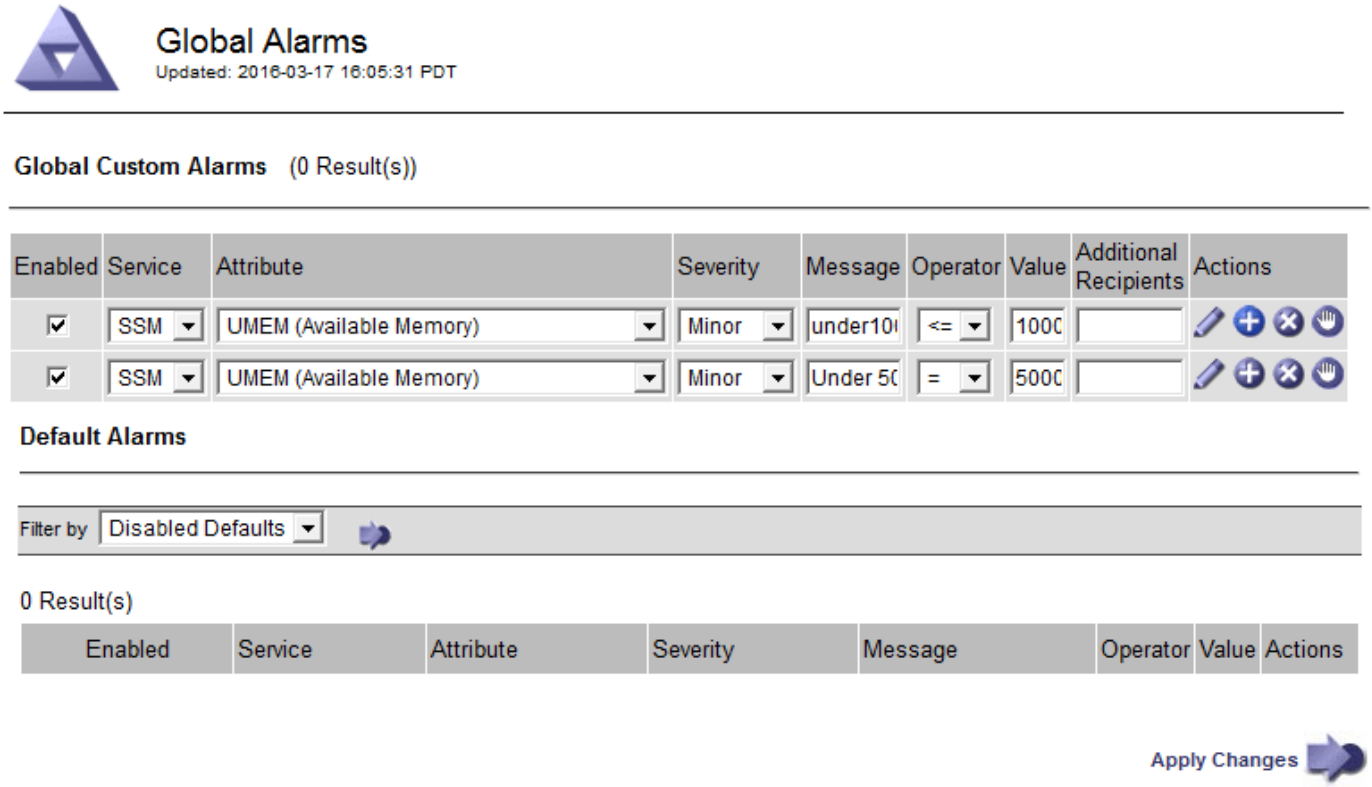
동일한 심각도의 경보

동일한 속성에 대해 두 개의 글로벌 사용자 정의 알람이 동일한 심각도를 갖는 경우, 알람은 ""하향식" 우선 순위로 평가됩니다.

예를 들어, UMEM이 50MB로 떨어지면 첫 번째 경보가 트리거되지만(=50000000) 그 아래에 있는 알람은 트리거되지 않습니다(<=100000000).



순서가 반대로 바뀌면 UMEM이 100MB로 떨어지면 첫 번째 알람(<=100000000)이 트리거되지만 그 아래에 있는 알람(= 50000000)은 트리거되지 않습니다.



알림

알림은 서비스의 알람 발생 또는 상태 변경을 보고합니다. 알람 알림은 e-메일 또는 SNMP를 통해 보낼 수 있습니다.

알람 임계값에 도달할 때 여러 알람 및 알림이 전송되지 않도록 하려면 해당 속성의 현재 알람 심각도에 대해 알람 심각도를 확인합니다. 변경 사항이 없으면 추가 작업이 수행되지 않습니다. 즉, NMS 서비스가 시스템을 계속 모니터링함에 따라 알람을 발생시키고 속성에 대한 알람 조건을 처음으로 인식한 경우에만 알림을 전송합니다. 속성에 대한 새 값 임계값에 도달하여 감지되면 알람 심각도가 변경되고 새 알림이 전송됩니다. 조건이 정상 수준으로 되돌아오면 알람이 해제됩니다.

알람 상태 알림에 표시되는 트리거 값은 소수점 셋째 자리까지 반올림됩니다. 따라서 특성 값 1.9999는 임계값이 (<) 2.0 미만인 알람을 트리거하지만 알람 알림은 트리거 값을 2.0으로 표시합니다.

새로운 서비스

새 그리드 노드 또는 사이트를 추가하여 새 서비스를 추가하면 기본 알람과 글로벌 사용자 지정 경보가 상속됩니다.

알람 및 표

표에 표시된 알람 속성은 시스템 수준에서 비활성화할 수 있습니다. 테이블의 개별 행에 대해서는 알람을 비활성화할 수 없습니다.

예를 들어 다음 표에는 사용 가능한 두 가지 중요 항목(VMFI) 경보가 나와 있습니다. (* 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 * *Storage Node* * > * SSM * > * Resources * 를 선택합니다.)

Critical level VMFI alarm이 triggering 되지 않도록 VMFI alarm을 disable 할 수 있다(현재 Critical alarm이 모두 green로 테이블에 나타남). 그러나 하나의 VMFI 알람이 위험 수준 알람으로 표시되고 다른 하나는 녹색으로 유지되도록 테이블 행에서 단일 알람을 비활성화할 수는 없습니다.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	sda1	Online	10.6 GB	7.46 GB	655,360	559,263	Enabled
/var/local	sda3	Online	63.4 GB	59.4 GB	3,932,160	3,931,842	Unknown
/var/local/rangedb/0	sdb	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled
/var/local/rangedb/1	sdc	Online	53.4 GB	53.4 GB	52,428,800	52,427,848	Enabled
/var/local/rangedb/2	sdd	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled

현재 알람 확인(레거시 시스템)

레거시 알람은 시스템 속성이 알람 임계값에 도달할 때 트리거됩니다. 또는 레거시 알람 목록을 줄이거나 지우려면 알람을 확인할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 알람 확인 권한이 있어야 합니다.

이 작업에 대해

기존 알람 시스템은 계속 지원되기 때문에 새 알람이 발생할 때마다 현재 알람 페이지의 기존 알람 목록이 증가합니다. 일반적으로 경보를 무시하거나(경고를 통해 시스템을 더 잘 볼 수 있으므로) 알람을 확인할 수 있습니다.

> 필요에 따라 알림 시스템으로 완전히 전환한 경우 각 기존 알람을 비활성화하여 기존 알람의 개수에 추가되지 않도록 할 수 있습니다.

경보를 승인하면 알람이 다음 심각도 수준에서 트리거되거나 해결되었다가 다시 발생하지 않는 한 그리드 관리자의 현재 알람 페이지에 더 이상 표시되지 않습니다.

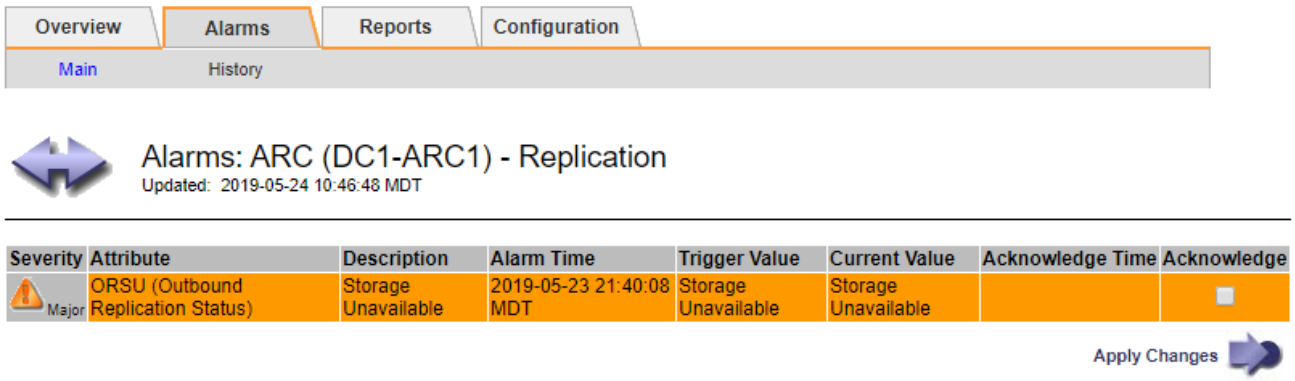
> 기존 알람 시스템은 계속 지원되지만, 알림 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

단계

1. 지원 * > * 알람(레거시) * > * 현재 알람 * 을 선택합니다.

2. 테이블에서 서비스 이름을 선택합니다.

   선택한 서비스에 대한 경보 탭이 나타납니다(* 지원 * > * 도구 * > * 그리드 토폴로지 * > *그리드 노드 _ * > *_서비스 * > * 경보 *).



3. 알람의 * 확인 * 확인란을 선택하고 * 변경 사항 적용 * 을 클릭합니다.

   대시보드 또는 현재 알람 페이지에 알람이 더 이상 나타나지 않습니다.

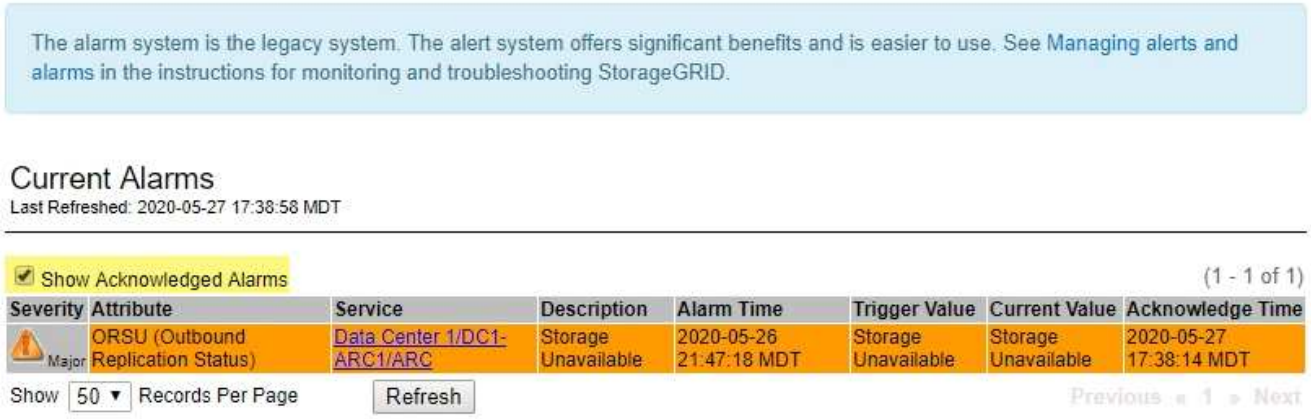
   > 알람을 확인하면 승인이 다른 관리 노드로 복사되지 않습니다. 이러한 이유로 다른 관리 노드에서 대시보드를 보는 경우 활성 경보를 계속 볼 수 있습니다.

4. 필요한 경우 확인된 알람을 봅니다.

   a. 지원 * > * 알람(레거시) * > * 현재 알람 * 을 선택합니다.

   b. Show Acknowledged Alarms * 를 선택합니다.

      확인된 알람이 표시됩니다.



기본 알람 보기(레거시 시스템)

모든 기본 레거시 알람 목록을 볼 수 있습니다.

필요한 것

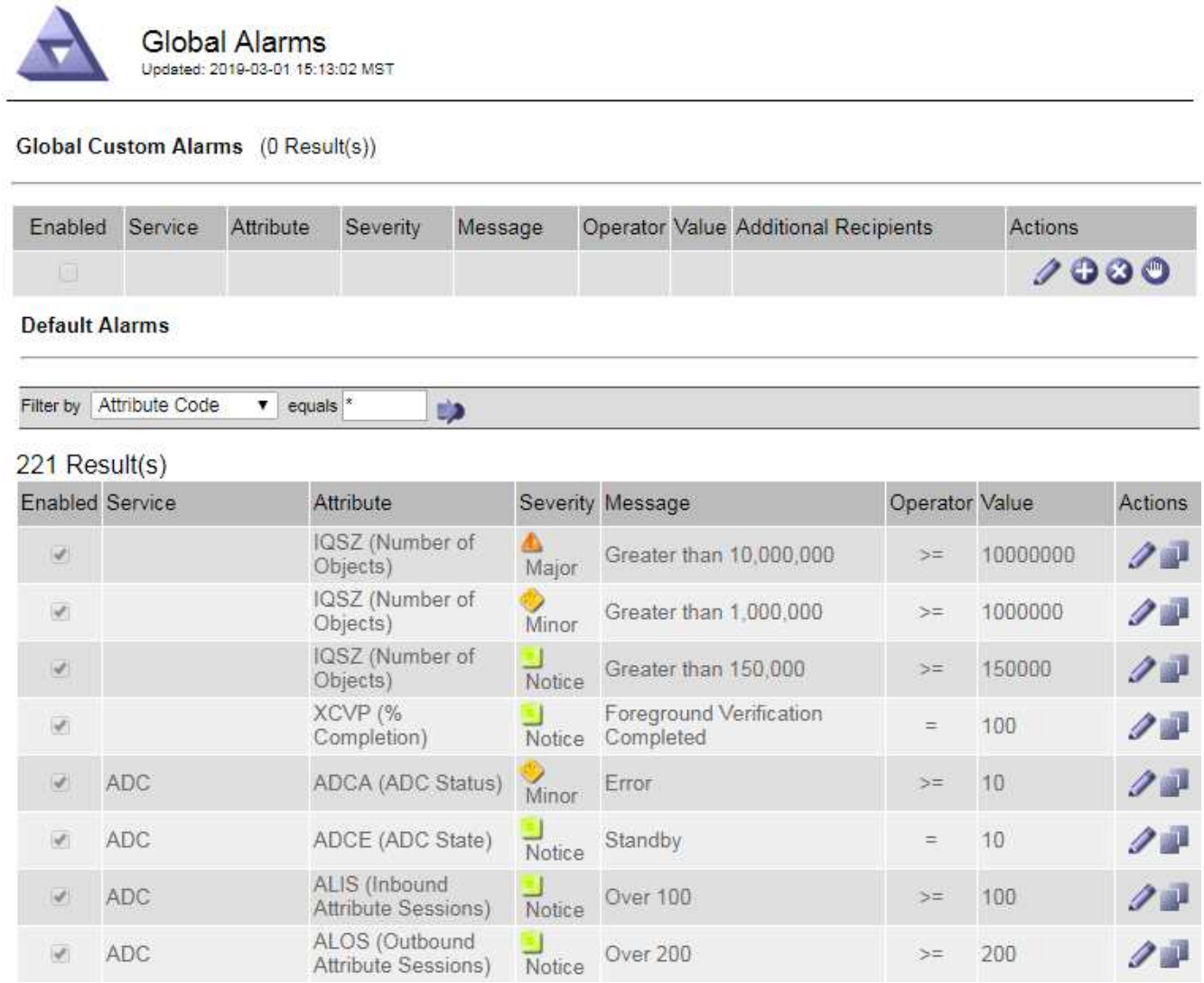
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

> 기존 알람 시스템은 계속 지원되지만, 알림 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

단계

1. 지원 * > * 알람(레거시) * > * 전체 알람 * 을 선택합니다.
2. 필터 기준 으로 * 특성 코드 * 또는 * 특성 이름 * 을 선택합니다.
3. 등에서는 별표(*)를 입력합니다
4. 화살표를 클릭합니다 또는 * Enter * 를 누릅니다.

   모든 기본 알람이 나열됩니다.



과거 알람 및 알람 빈도 검토(레거시 시스템)

문제를 해결할 때 레거시 알람이 이전에 트리거된 빈도를 검토할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

> 기존 알람 시스템은 계속 지원되지만, 알림 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

단계

1. 다음 단계에 따라 일정 기간 동안 트리거된 모든 알람 목록을 가져옵니다.
   a. 지원 * > * 알람(레거시) * > * 내역 알람 * 을 선택합니다.
   b. 다음 중 하나를 수행합니다.
      - 기간 중 하나를 클릭합니다.
      - 사용자 지정 범위를 입력하고 * 사용자 지정 쿼리 * 를 클릭합니다.

2. 다음 단계에 따라 특정 속성에 대해 알람이 트리거되는 빈도를 확인합니다.
   a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
   b. grid node_ * > **service* 또는 *component* * > * Alarms * > * History * 를 선택합니다.
   c. 목록에서 속성을 선택합니다.
   d. 다음 중 하나를 수행합니다.
      - 기간 중 하나를 클릭합니다.
      - 사용자 지정 범위를 입력하고 * 사용자 지정 쿼리 * 를 클릭합니다.

      알람은 시간순으로 역순으로 나열됩니다.
   e. 경보 기록 요청 양식으로 돌아가려면 * 기록 * 을 클릭합니다.

전체 사용자 정의 알람 생성(레거시 시스템)

특정 모니터링 요구 사항을 해결하기 위해 기존 시스템에 대해 글로벌 사용자 지정 알람을 사용했을 수 있습니다. 글로벌 사용자 정의 알람에는 기본 알람을 재정의하는 알람 수준이 있거나 기본 알람이 없는 속성을 모니터링할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

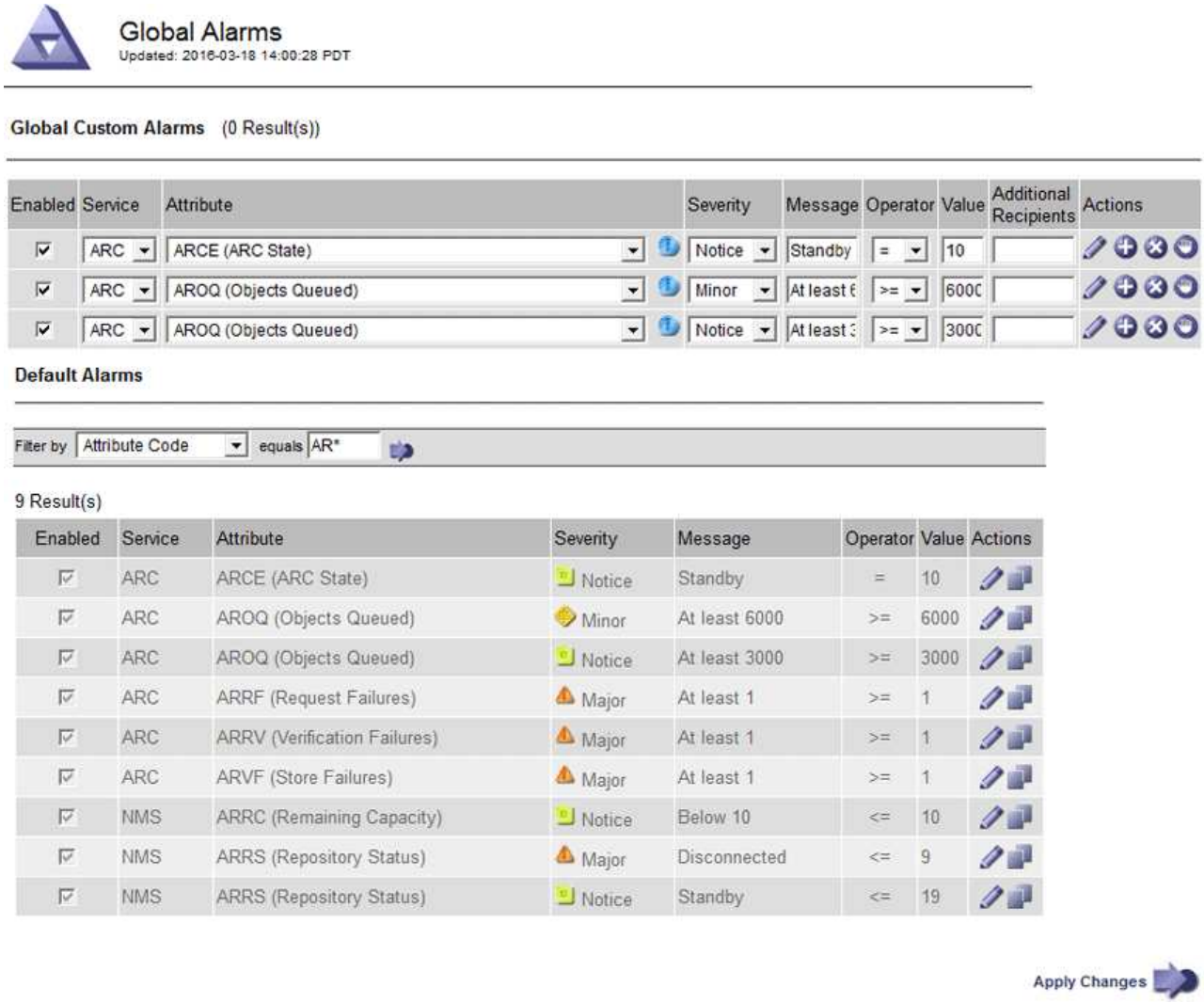
> 기존 알람 시스템은 계속 지원되지만, 알림 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

전체 사용자 정의 알람은 기본 알람보다 우선합니다. 반드시 필요한 경우가 아니면 기본 알람 값을 변경해서는 안 됩니다. 기본 알람을 변경하면 알람을 트리거할 수 있는 문제가 은폐될 위험이 있습니다.

> 알람 설정을 변경할 때는 매우 주의해야 합니다. 예를 들어, 알람의 임계값을 증가해도 기본 문제를 감지하지 못할 수 있습니다. 알람 설정을 변경하기 전에 기술 지원 부서의 변경 사항에 대해 논의하십시오.

단계

1. 지원 * > * 알람(레거시) * > * 전체 알람 * 을 선택합니다.
2. Global Custom Alarms(전체 사용자 정의 알람) 테이블에 새 행을 추가합니다.
   - 새 알람을 추가하려면 * Edit * (편집 *)를 클릭합니다 (첫 번째 항목인 경우) 또는 * Insert * (삽입 *)를 선택합니다.



- 기본 알람을 수정하려면 기본 알람을 검색합니다.
  i. 필터 기준 아래에서 * 특성 코드 * 또는 * 특성 이름 * 을 선택합니다.
  ii. 검색 문자열을 입력합니다.

  4개의 문자를 지정하거나 와일드카드(예: a??? 또는 AB **).** 별표**(**)는 여러 문자를 나타내고 물음표(?)는 단일 문자를 나타냅니다.

  iii. 화살표를 클릭합니다 또는 * Enter * 를 누릅니다.
  iv. 결과 목록에서 * 복사 * 를 클릭합니다 수정할 알람 옆에 있습니다.

  Default alarm(기본 알람)이 Global Custom alarms(전체 사용자 정의 알람) 테이블에 복사됩니다.

3. 전역 사용자 정의 알람 설정을 필요에 따라 변경합니다.

제목	설명
활성화됨	확인란을 선택하거나 선택 취소하여 알람을 활성화 또는 비활성화합니다.

제목	설명
속성	선택한 서비스 또는 구성 요소에 적용 가능한 모든 속성 목록에서 모니터링 중인 특성의 이름과 코드를 선택합니다. 속성에 대한 정보를 표시하려면 * 정보 * 를 클릭합니다 속성 이름 옆에 있습니다.
심각도입니다	알람 레벨을 나타내는 아이콘과 텍스트
메시지	알람이 발생한 이유(연결 끊김, 저장 공간 10% 미만 등)
운영자	값 임계값에 대해 현재 속성 값을 테스트하는 연산자: • = 같음 • > 보다 큼 • 보다 작음 • >= 보다 크거나 같음 • = 보다 작거나 같음 • ≠ 같지 않음
값	운용자를 사용하여 속성의 실제 값을 기준으로 테스트하는 데 사용되는 알람의 임계값입니다. 항목은 단일 번호, 콜론(1:3)으로 지정된 숫자 범위 또는 숫자와 범위의 쉼표로 구분된 목록이 될 수 있습니다.
추가 받는 사람	알람이 트리거될 때 알림을 받을 e-메일 주소의 추가 목록입니다. 이것은 * 알람 * > * 이메일 설정 * 페이지에 구성된 메일링 리스트와 함께 사용됩니다. 목록은 쉼표로 구분됩니다. • 참고: * 메일링 목록을 사용하려면 SMTP 서버를 설정해야 합니다. 메일 그룹을 추가하기 전에 SMTP가 구성되어 있는지 확인합니다. 사용자 정의 알람에 대한 알림은 전체 사용자 정의 또는 기본 알람의 알림을 재정의할 수 있습니다.
작업	컨트롤 버튼: 행을 편집합니다 를 누릅니다 행을 삽입합니다 를 누릅니다 행을 삭제합니다 를 누릅니다 행을 위 또는 아래로 끌어서 놓습니다 를 누릅니다 행을 복사합니다

4. 변경 내용 적용 * 을 클릭합니다.

알람 비활성화(기존 시스템)

레거시 알람 시스템의 알람은 기본적으로 활성화되어 있지만 필요하지 않은 알람은 비활성화할 수 있습니다. 새 경보 시스템으로 완전히 전환한 후 기존 경보를 비활성화할 수도 있습니다.

> 기존 알람 시스템은 계속 지원되지만, 알림 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

기본 알람 비활성화(레거시 시스템)

전체 시스템에 대해 레거시 기본 알람 중 하나를 비활성화할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

현재 알람이 트리거된 속성에 대해 알람을 비활성화해도 현재 알람은 지워지지 않습니다. 다음 번에 속성이 알람 임계값을 넘어가면 알람이 비활성화되거나 트리거된 알람을 지울 수 있습니다.

> 새 경보 시스템으로 완전히 전환할 때까지 기존 경보를 비활성화하지 마십시오. 그렇지 않으면 중요한 작업이 완료되지 못할 때까지 근본적인 문제를 감지하지 못할 수 있습니다.

단계

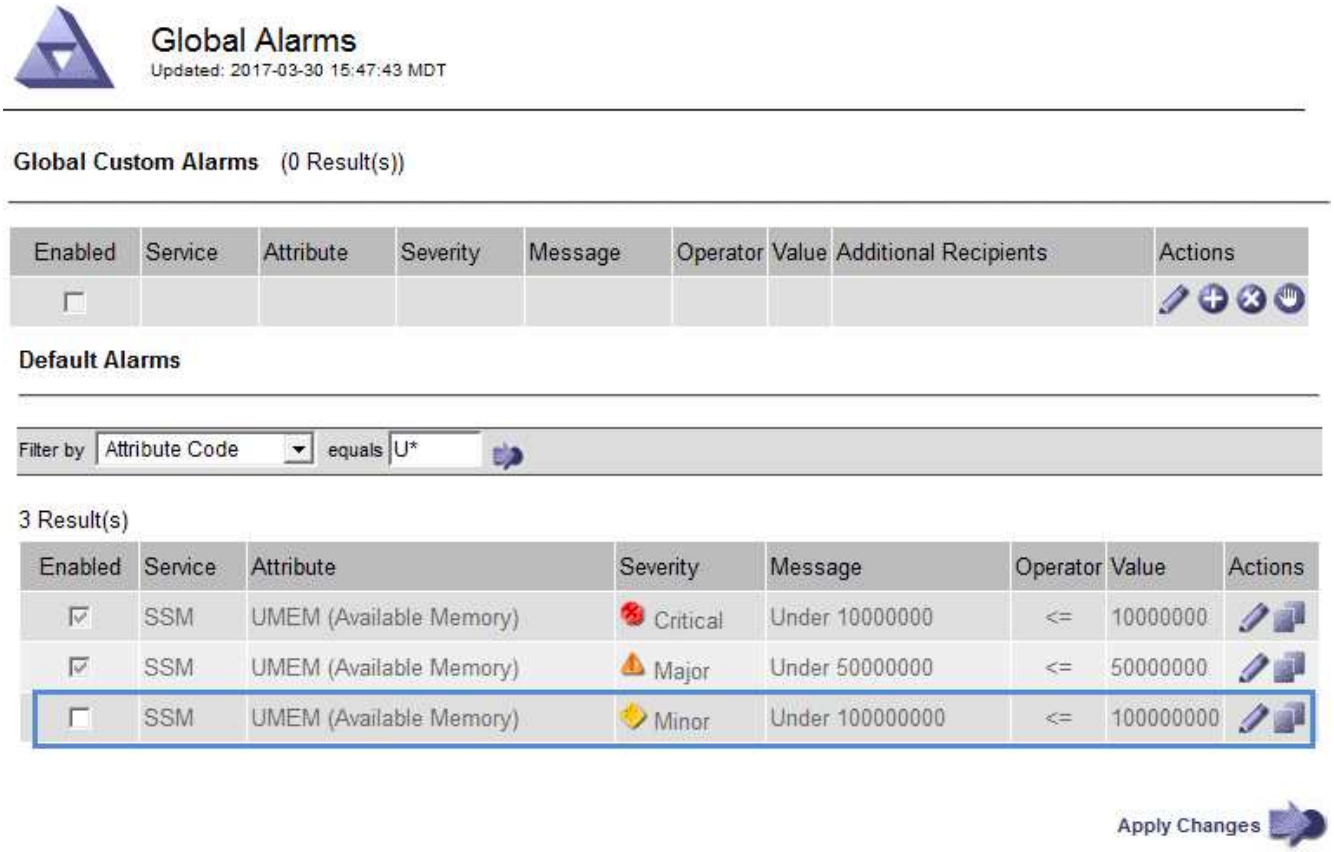
1. 지원 * > * 알람(레거시) * > * 전체 알람 * 을 선택합니다.
2. 기본 알람을 검색하여 비활성화합니다.
   a. 기본 알람 섹션에서 * Filter by * > * Attribute Code * 또는 * Attribute Name * 을 선택합니다.
   b. 검색 문자열을 입력합니다.

      4개의 문자를 지정하거나 와일드카드(예: a??? 또는 AB **).** 별표()는 여러 문자를 나타내고 물음표(?)는 단일 문자를 나타냅니다.

   c. 화살표를 클릭합니다 또는 * Enter * 를 누릅니다.

      > Disabled Defaults * 를 선택하면 현재 비활성화된 모든 기본 알람 목록이 표시됩니다.

3. 검색 결과 테이블에서 편집 아이콘을 클릭합니다 비활성화하려는 알람의 경우.



선택한 알람의 * Enabled * (활성화 *) 확인란이 활성화됩니다.

4. 사용 * 확인란의 선택을 취소합니다.
5. 변경 내용 적용 * 을 클릭합니다.

   기본 알람은 비활성화됩니다.

전체 사용자 정의 알람 비활성화(레거시 시스템)

전체 시스템에 대해 레거시 글로벌 사용자 정의 알람을 비활성화할 수 있습니다.

필요한 것

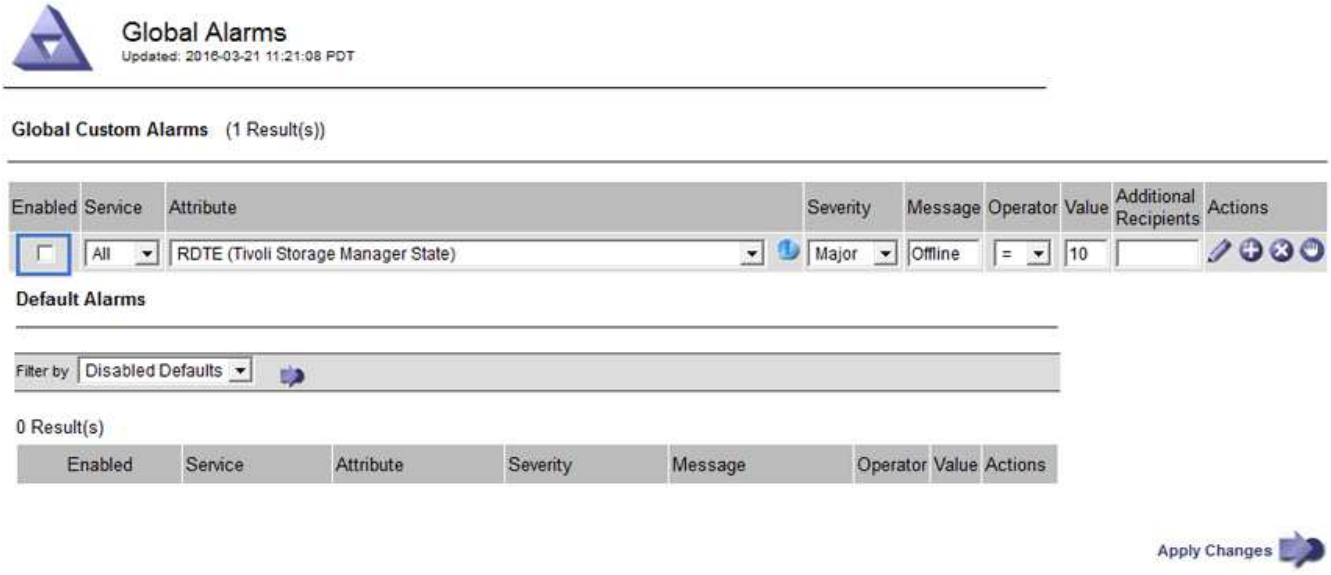
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

현재 알람이 트리거된 속성에 대해 알람을 비활성화해도 현재 알람은 지워지지 않습니다. 다음 번에 속성이 알람 임계값을 넘어가면 알람이 비활성화되거나 트리거된 알람을 지울 수 있습니다.

단계

1. 지원 * > * 알람(레거시) * > * 전체 알람 * 을 선택합니다.
2. 글로벌 사용자 정의 알람 표에서 * 편집 * 을 클릭합니다 비활성화할 알람 옆에 있습니다.
3. 사용 * 확인란의 선택을 취소합니다.



4. 변경 내용 적용 * 을 클릭합니다.

   전체 사용자 정의 알람이 비활성화됩니다.

트리거된 알람 지우기(레거시 시스템)

레거시 알람이 트리거되면 이를 확인하는 대신 지울 수 있습니다.

필요한 것

- 비밀번호 .txt 파일이 있어야 합니다.

현재 알람이 트리거된 속성에 대해 알람을 비활성화해도 알람이 지워지지 않습니다. 다음 번에 특성이 변경되면 알람이 비활성화됩니다. 알람을 확인하거나 속성 값이 변경될 때까지 기다리지 않고 즉시 알람을 소거하려는 경우(알람 상태가 변경되는 경우) 트리거된 알람을 지울 수 있습니다. 이 기능은 값이 자주 변경되지 않는 속성(예: 상태 속성)에 대해 즉시 경보를 지우려는 경우에 유용할 수 있습니다.

1. 알람을 비활성화합니다.
2. 기본 관리자 노드에 로그인합니다.
   a. '*ssh admin@primary_Admin_Node_IP*' 명령을 입력합니다
   b. 비밀번호 .txt 파일에 나열된 비밀번호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
3. NMS 서비스 'Service NMS restart'를 다시 시작한다
4. Admin Node에서 로그아웃: exit

   알람이 해제됩니다.

알람 알림 구성(기존 시스템)

StorageGRID 시스템은 자동으로 및 이메일을 보낼 수 있습니다 SNMP 알림 알람이 트리거되거나 서비스 상태가 변경되는 경우

기본적으로 알람 이메일 알림은 전송되지 않습니다. e-메일 알림의 경우 e-메일 서버를 구성하고 e-메일 수신자를 지정해야 합니다. SNMP 알림의 경우 SNMP 에이전트를 구성해야 합니다.

알람 알림 유형(기존 시스템)

레거시 알람이 트리거되면 StorageGRID 시스템은 심각도 레벨과 서비스 상태의 두 가지 유형의 알람 알림을 전송합니다.

심각도 수준 알림

선택한 심각도 수준에서 기존 알람이 트리거되면 알람 e-메일 알림이 전송됩니다.

- 주의
- 경미합니다
- 전공
- 심각

메일 그룹은 선택한 심각도에 대한 알람과 관련된 모든 알림을 수신합니다. 알람이 알람 수준을 벗어날 경우(해제 중 또는 다른 알람 심각도 수준 입력) 알림도 전송됩니다.

서비스 상태 알림

서비스(예: LDR 서비스 또는 NMS 서비스)가 선택한 서비스 상태로 진입하고 선택한 서비스 상태를 벗어날 때 서비스 상태 알림이 전송됩니다. 서비스 상태 알림은 서비스가 다음 서비스 상태 중 하나를 시작하거나 벗어날 때 전송됩니다.

- 알 수 없음
- 관리상의 이유로 다운되었습니다

메일 그룹은 선택한 상태의 변경과 관련된 모든 알림을 받습니다.

경보에 대한 이메일 서버 설정 구성(레거시 시스템)

레거시 경보가 트리거될 때 StorageGRID에서 이메일 알림을 보내도록 하려면 SMTP 메일 서버 설정을 지정해야 합니다. StorageGRID 시스템은 이메일만 전송하며 이메일을 수신할 수 없습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

이 설정을 사용하여 레거시 알람 이메일 알림 및 AutoSupport 이메일 메시지에 사용되는 SMTP 서버를 정의합니다. 이러한 설정은 경고 알림에 사용되지 않습니다.

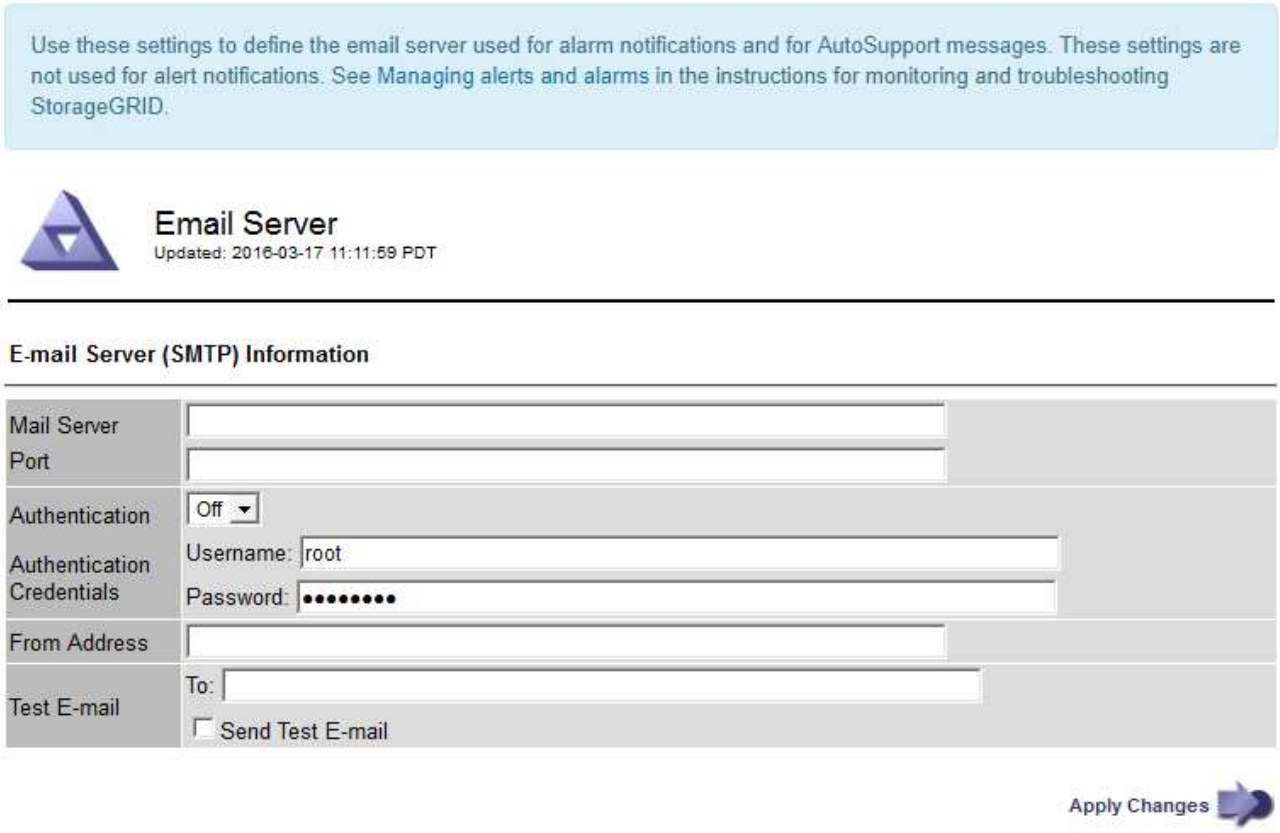
AutoSupport 메시지의 프로토콜로 SMTP를 사용하는 경우 이미 SMTP 메일 서버를 구성했을 수 있습니다. 알람 이메일 알림에 동일한 SMTP 서버가 사용되므로 이 절차를 건너뛸 수 있습니다. 를 참조하십시오 StorageGRID 관리 지침.

SMTP는 이메일을 보내는 데 지원되는 유일한 프로토콜입니다.

단계

1. 지원 * > * 알람(레거시) * > * 레거시 이메일 설정 * 을 선택합니다.
2. 이메일 메뉴에서 * 서버 * 를 선택합니다.

   이메일 서버 페이지가 나타납니다. 이 페이지는 AutoSupport 메시지에 대한 전자 메일 서버를 구성하는 데도 사용됩니다.



3. 다음 SMTP 메일 서버 설정을 추가합니다.

항목	설명
메일 서버	SMTP 메일 서버의 IP 주소입니다. 관리 노드에서 이전에 DNS 설정을 구성한 경우 IP 주소 대신 호스트 이름을 입력할 수 있습니다.
포트	SMTP 메일 서버에 액세스하기 위한 포트 번호입니다.
인증	SMTP 메일 서버의 인증을 허용합니다. 기본적으로 인증은 Off입니다.

항목	설명
인증 자격 증명	SMTP 메일 서버의 사용자 이름 및 암호입니다. 인증이 켜짐으로 설정된 경우 SMTP 메일 서버에 액세스하기 위한 사용자 이름과 암호를 제공해야 합니다.

4. 보내는 사람 주소 * 에 SMTP 서버가 보내는 전자 메일 주소로 인식할 유효한 전자 메일 주소를 입력합니다. 이 주소는 이메일 메시지를 보낸 공식 이메일 주소입니다.
5. 필요에 따라 SMTP 메일 서버 설정이 올바른지 확인하기 위해 테스트 이메일을 보냅니다.
   a. Test E-mail * > * 받는 사람 * 상자에 액세스할 수 있는 주소를 하나 이상 추가합니다.

      단일 이메일 주소 또는 쉼표로 구분된 이메일 주소 목록을 입력할 수 있습니다. NMS 서비스는 테스트 이메일을 보낼 때 성공 또는 실패를 확인하지 않으므로 테스트 수신자의 받은 편지함을 확인할 수 있어야 합니다.

   b. 테스트 이메일 전송 * 을 선택합니다.
6. 변경 내용 적용 * 을 클릭합니다.

   SMTP 메일 서버 설정이 저장됩니다. 테스트 이메일에 대한 정보를 입력한 경우 해당 이메일이 전송됩니다. 테스트 이메일은 즉시 메일 서버로 전송되며 알림 대기열을 통해 전송되지 않습니다. 여러 관리 노드가 있는 시스템에서 각 관리 노드는 이메일을 보냅니다. 테스트 이메일을 받으면 SMTP 메일 서버 설정이 올바르고 NMS 서비스가 메일 서버에 성공적으로 연결되었음을 확인합니다. NMS 서비스와 메일 서버 간의 연결 문제가 사소한 심각도 수준에서 레거시 분(NMS 알림 상태) 알람을 트리거합니다.

알람 이메일 템플릿 생성(기존 시스템)

이메일 템플릿을 사용하여 레거시 알람 이메일 알림의 머리글, 바닥글 및 제목 줄을 사용자 지정할 수 있습니다. 이메일 템플릿을 사용하여 동일한 본문 텍스트를 포함하는 고유한 알림을 다른 메일 그룹에 보낼 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

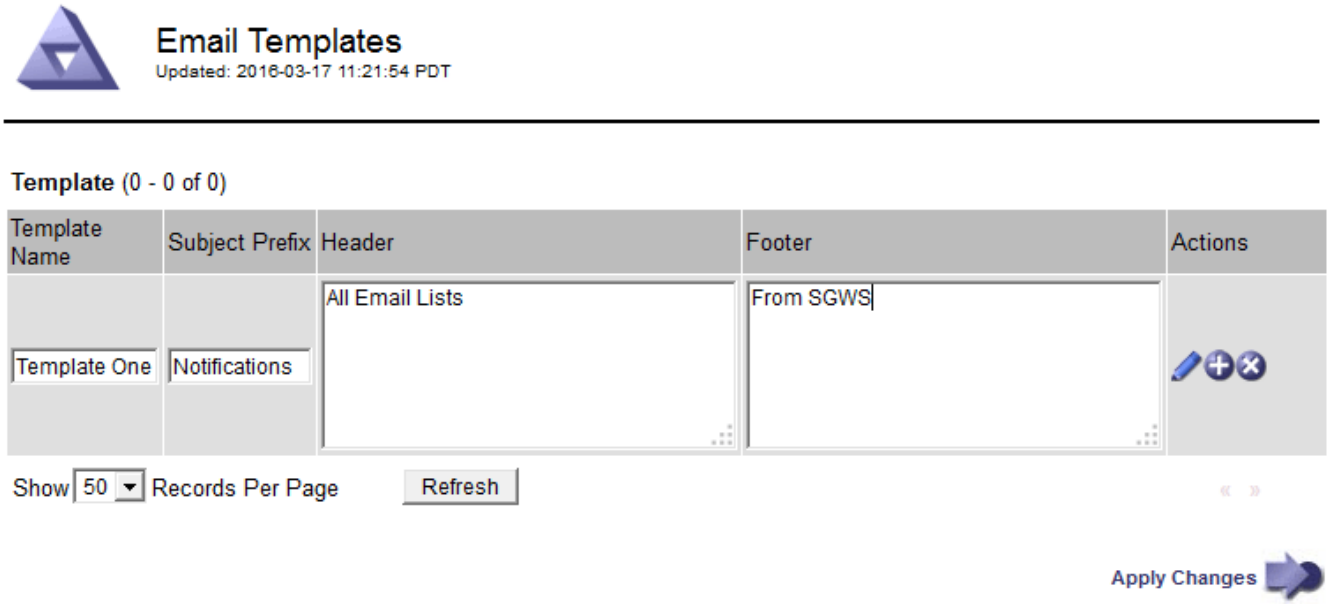
이 작업에 대해

이 설정을 사용하여 레거시 알람 알림에 사용되는 이메일 템플릿을 정의합니다. 이러한 설정은 경고 알림에 사용되지 않습니다.

메일링 리스트마다 다른 연락처 정보가 필요할 수 있습니다. 템플릿에는 이메일 메시지의 본문 텍스트가 포함되지 않습니다.

단계

1. 지원 * > * 알람(레거시) * > * 레거시 이메일 설정 * 을 선택합니다.
2. 이메일 메뉴에서 * 템플릿 * 을 선택합니다.
3. 편집 * 을 클릭합니다 (또는 * Insert * (삽입 *)를 클릭합니다 첫 번째 템플릿이 아닌 경우).



4. 새 행에 다음을 추가합니다.

항목	설명
템플릿 이름	템플릿을 식별하는 데 사용되는 고유한 이름입니다. 템플릿 이름은 복제할 수 없습니다.
제목 접두어	선택 사항. 이메일의 제목 줄 앞에 표시되는 접두사입니다. 접두사를 사용하여 이메일 필터를 쉽게 구성하고 알림을 구성할 수 있습니다.
머리글	선택 사항. 전자 메일 메시지 본문의 시작 부분에 나타나는 머리글 텍스트입니다. 머리글 텍스트를 사용하여 전자 메일 메시지의 내용을 회사 이름 및 주소 등의 정보로 미리 표시할 수 있습니다.
바닥글	선택 사항. 전자 메일 메시지 본문 끝에 나타나는 바닥글 텍스트입니다. 바닥글 텍스트는 연락처 전화 번호 또는 웹 사이트 링크와 같은 미리 알림 정보가 있는 전자 메일 메시지를 닫는 데 사용할 수 있습니다.

5. 변경 내용 적용 * 을 클릭합니다.

   알림에 대한 새 템플릿이 추가됩니다.

알람 알림에 대한 메일 그룹 생성(레거시 시스템)

메일링 목록을 사용하면 레거시 알람이 트리거되거나 서비스 상태가 변경될 때 수신자에게 알릴 수 있습니다. 알람 이메일 알림을 전송하려면 하나 이상의 메일 그룹을 생성해야 합니다. 단일 수신인에게 알림을 보내려면 하나의 이메일 주소로 메일 그룹을 만듭니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

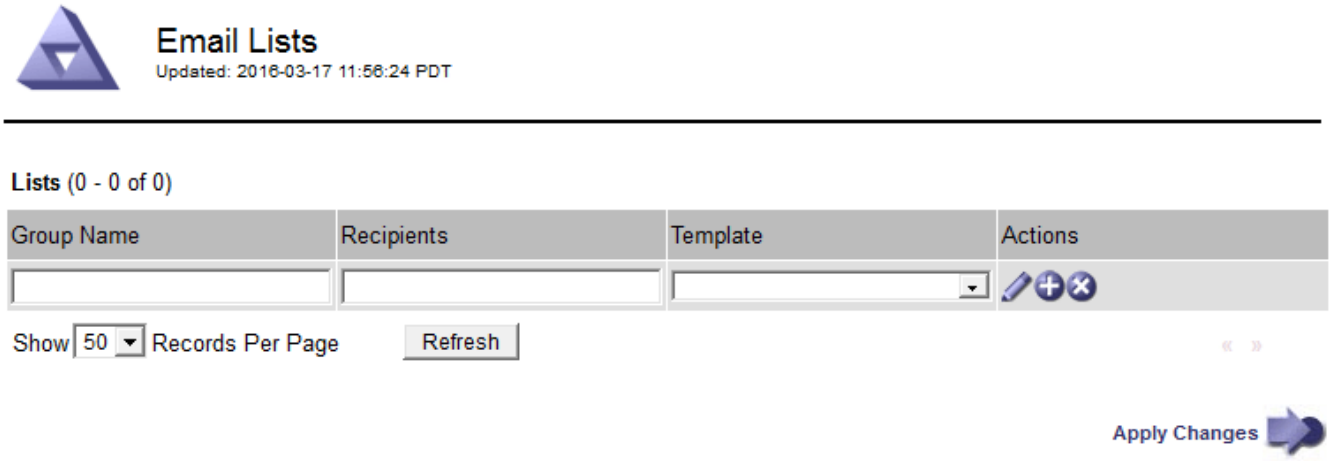
- 메일 그룹에 대한 전자 메일 서식 파일(사용자 지정 머리글, 바닥글 및 제목 줄)을 지정하려면 해당 서식 파일을 이미 만들어야 합니다.

이 작업에 대해

이 설정을 사용하여 레거시 알람 이메일 알림에 사용되는 메일 그룹을 정의합니다. 이러한 설정은 경고 알림에 사용되지 않습니다.

단계

1. 지원 * > * 알람(레거시) * > * 레거시 이메일 설정 * 을 선택합니다.
2. 이메일 메뉴에서 * 목록 * 을 선택합니다.
3. 편집 * 을 클릭합니다 (또는 * Insert * (삽입 *)를 클릭합니다 첫 번째 메일링 리스트가 아닌 경우).



4. 새 행에 다음을 추가합니다.

항목	설명
그룹 이름	메일 그룹을 식별하는 데 사용되는 고유한 이름입니다. 메일 그룹 이름은 복제할 수 없습니다. • 참고: * 메일 그룹의 이름을 변경하면 변경 내용이 메일 그룹 이름을 사용하는 다른 위치로 전달되지 않습니다. 새 메일 그룹 이름을 사용하려면 구성된 모든 알림을 수동으로 업데이트해야 합니다.
받는 사람	단일 이메일 주소, 이전에 구성된 메일링 목록 또는 알림을 보낼 이메일 주소 및 메일링 목록의 쉼표로 구분된 목록. • 참고: * 이메일 주소가 여러 메일 그룹에 속한 경우 알림 트리거 이벤트가 발생할 때 하나의 이메일 알림만 전송됩니다.
템플릿	필요에 따라 이 메일 그룹의 모든 수신자에게 보내는 알림에 고유한 머리글, 바닥글 및 제목 줄을 추가할 이메일 템플릿을 선택합니다.

5. 변경 내용 적용 * 을 클릭합니다.

   새 메일 그룹이 만들어집니다.

알람에 대한 이메일 알림 구성(기존 시스템)

기존 경보 시스템에 대한 이메일 알림을 수신하려면 수신자가 메일 그룹의 구성원이어야 하며 해당 목록을 알림 페이지에 추가해야 합니다. 알림은 심각도 수준이 지정된 알람이 트리거되거나 서비스 상태가 변경될 경우에만 수신자에게 이메일을 보내도록 구성됩니다. 따라서 수신자는 수신해야 하는 알림만 수신합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.
- 이메일 목록을 구성해야 합니다.

이 작업에 대해

레거시 경보에 대한 알림을 구성하려면 이 설정을 사용합니다. 이러한 설정은 경고 알림에 사용되지 않습니다.

이메일 주소(또는 목록)가 여러 메일 그룹에 속한 경우 알림 트리거 이벤트가 발생할 때 하나의 이메일 알림만 전송됩니다. 예를 들어 조직 내의 한 관리자 그룹이 심각도에 관계없이 모든 알람에 대한 알림을 받도록 구성할 수 있습니다. 다른 그룹에는 심각도가 심각 인 알람에 대해서만 알림이 필요할 수 있습니다. 두 목록 모두에 속할 수 있습니다. 위험 알람이 트리거되면 하나의 알림만 수신됩니다.

단계

1. 지원 * > * 알람(레거시) * > * 레거시 이메일 설정 * 을 선택합니다.
2. 이메일 메뉴에서 * 알림 * 을 선택합니다.
3. 편집 * 을 클릭합니다 (또는 * Insert * (삽입 *)를 클릭합니다 첫 번째 알림이 아닌 경우).
4. 전자 메일 목록에서 메일 그룹을 선택합니다.
5. 하나 이상의 알람 심각도 수준 및 서비스 상태를 선택합니다.
6. 변경 내용 적용 * 을 클릭합니다.

   선택한 알람 심각도 수준 또는 서비스 상태의 알람이 트리거되거나 변경되면 알림이 메일 목록으로 전송됩니다.

메일 그룹에 대한 알람 알림 기능 억제(레거시 시스템)

더 이상 우편 발송 목록에서 경보에 대한 알림을 받지 않으려면 메일 그룹에 대한 알람 알림을 표시하지 않을 수 있습니다. 예를 들어, 알림 e-메일 알림을 사용하도록 전환한 후 기존 경보에 대한 알림을 표시하지 않을 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

레거시 알람 시스템에 대한 이메일 알림을 표시하지 않으려면 이 설정을 사용합니다. 이러한 설정은 경고 이메일 알림에는 적용되지 않습니다.

> 기존 알람 시스템은 계속 지원되지만, 알림 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

단계

1. 지원 * > * 알람(레거시) * > * 레거시 이메일 설정 * 을 선택합니다.

2. 이메일 메뉴에서 * 알림 * 을 선택합니다.
3. 편집 * 을 클릭합니다 알림을 표시하지 않을 메일링 목록 옆에 있습니다.
4. 표시 안 함에서 억제할 메일 그룹 옆에 있는 확인란을 선택하거나 열 맨 위에 있는 * 표시 안 함 * 을 선택하여 모든 메일 그룹을 숨깁니다.
5. 변경 내용 적용 * 을 클릭합니다.

   기존 알람 알림은 선택한 메일링 목록에 대해 억제됩니다.

e-메일 알림을 시스템 전체에 표시하지 않습니다

StorageGRID 시스템에서 기존 경보 및 이벤트 트리거 AutoSupport 메시지에 대한 이메일 알림을 보내는 기능을 차단할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

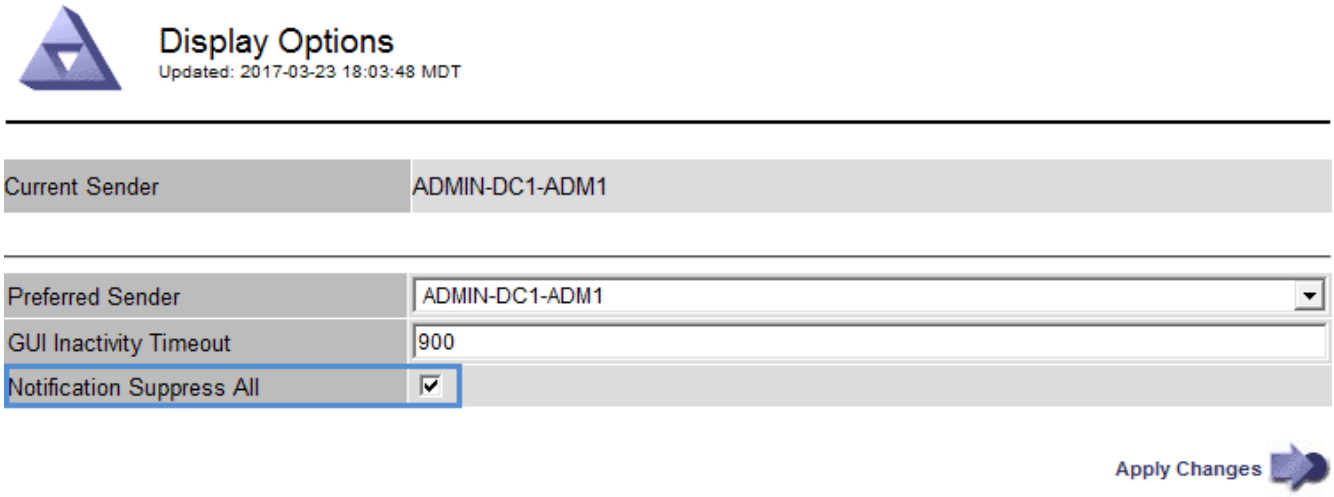
이 작업에 대해

레거시 알람 및 이벤트 트리거 AutoSupport 메시지에 대한 이메일 알림을 표시하지 않으려면 이 옵션을 사용합니다.

> 이 옵션은 알림 e-메일 알림을 표시하지 않습니다. 또한 매주 또는 사용자가 트리거한 AutoSupport 메시지도 표시하지 않습니다.

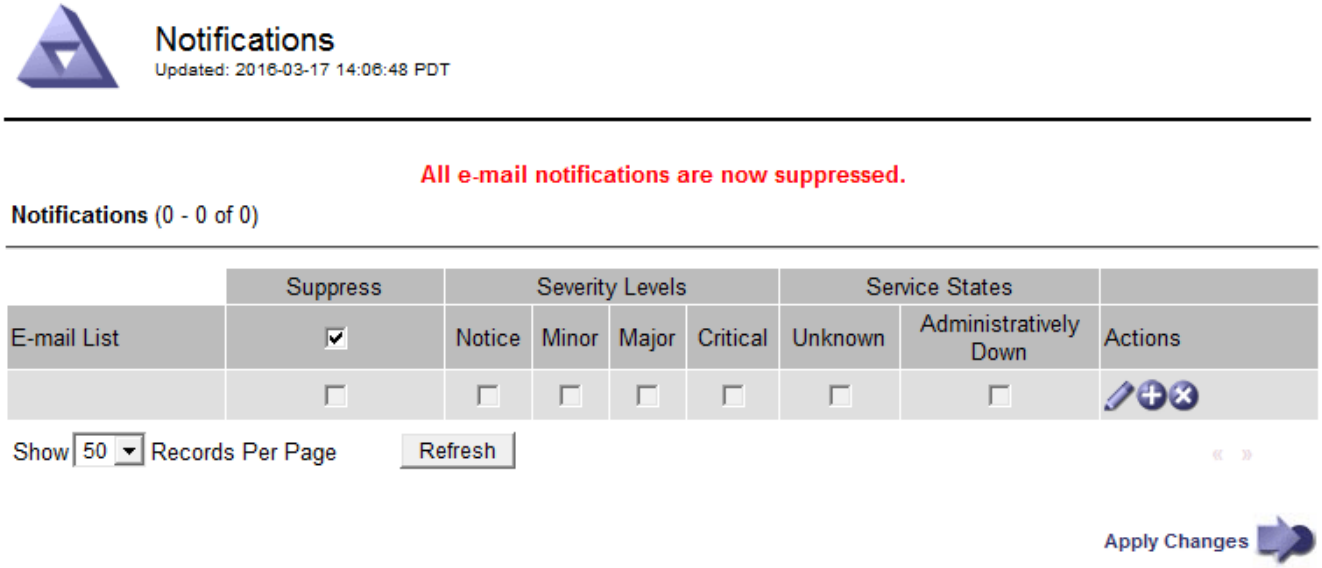
단계

1. 구성 * > * 시스템 설정 * > * 디스플레이 옵션 * 을 선택합니다.
2. 표시 옵션 메뉴에서 * 옵션 * 을 선택합니다.
3. 알림 모두 억제 * 를 선택합니다.



4. 변경 내용 적용 * 을 클릭합니다.

   알림 페이지(* 구성 * > * 알림 *)에 다음 메시지가 표시됩니다.



감사 메시지 및 로그 대상을 구성합니다

감사 메시지와 로그는 시스템 활동 및 보안 이벤트를 기록하고, 모니터링 및 문제 해결에 필수적인 도구입니다. 감사 수준을 조정하여 기록된 감사 메시지의 유형과 수를 늘리거나 줄일 수 있습니다. 선택적으로 감사 메시지를 읽고 쓸 클라이언트에 포함할 HTTP 요청 헤더를 정의할 수 있습니다. 외부 syslog 서버를 구성하고 감사 정보의 대상을 변경할 수도 있습니다.

감사 메시지에 대한 자세한 내용은 을 참조하십시오 감사 로그를 검토합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다.

이 작업에 대해

모든 StorageGRID 노드는 감사 메시지와 로그를 생성하여 시스템 활동 및 이벤트를 추적합니다. 기본적으로 감사 정보는 관리 노드의 감사 로그로 전송됩니다. 감사 레벨을 조정하여 감사 로그에 기록되는 감사 메시지의 유형과 수를 늘리거나 줄일 수 있습니다. 필요에 따라 원격 syslog 서버로 전송되거나 수동 수집을 위해 원래 노드에 임시로 저장되도록 감사 정보를 구성할 수 있습니다.

감사 로그에서 감사 메시지 수준을 변경합니다

감사 로그에서 다음 메시지 범주에 대해 서로 다른 감사 수준을 설정할 수 있습니다.

감사 범주	설명
시스템	기본적으로 이 수준은 보통 으로 설정됩니다. 을 참조하십시오 시스템 감사 메시지.
스토리지	기본적으로 이 수준은 오류 로 설정됩니다. 을 참조하십시오 오브젝트 스토리지 감사 메시지.
관리	기본적으로 이 수준은 보통 으로 설정됩니다. 을 참조하십시오 관리 감사 메시지입니다.

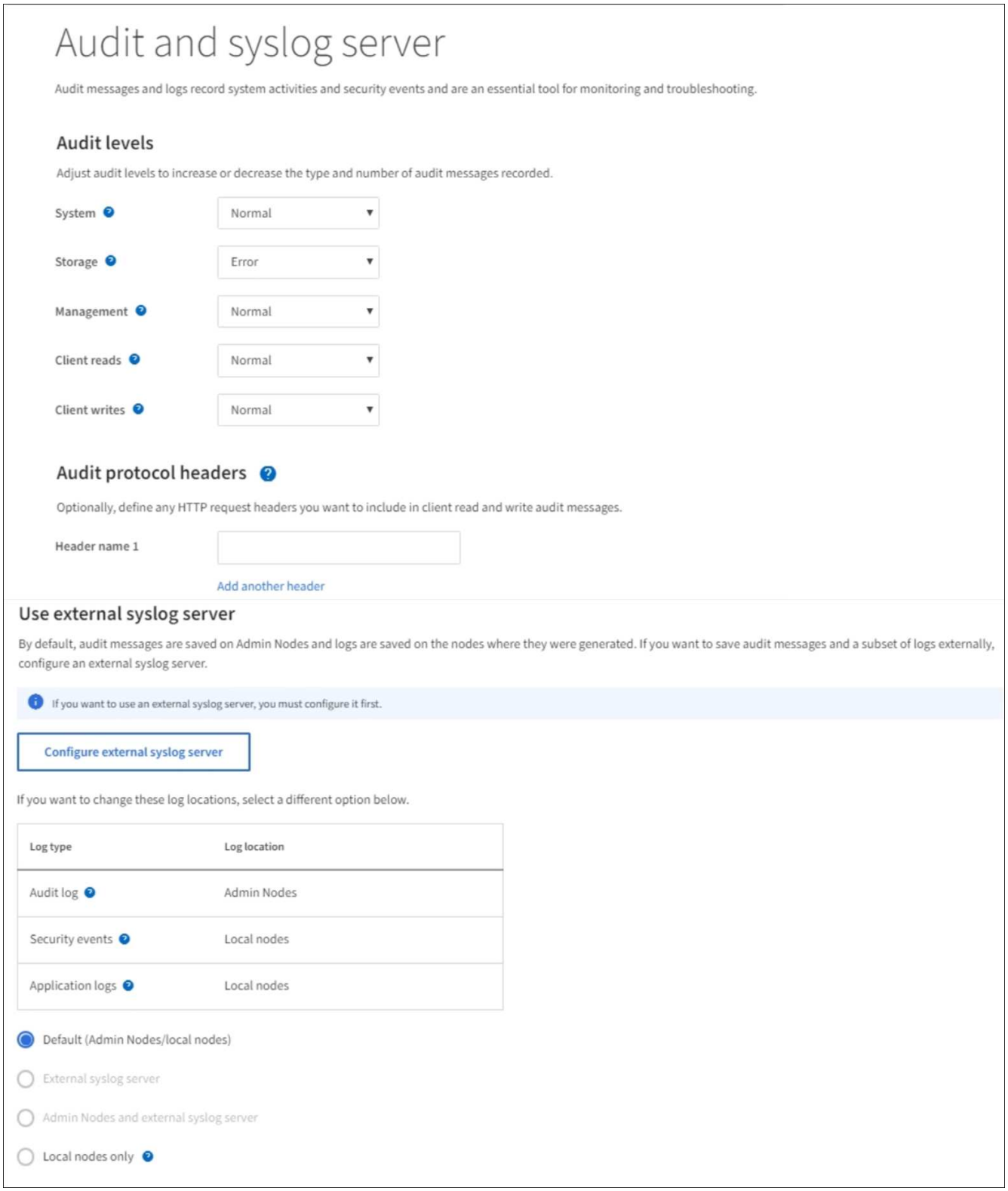
감사 범주	설명
클라이언트 읽기	기본적으로 이 수준은 보통 으로 설정됩니다. 을 참조하십시오 클라이언트가 감사 메시지를 읽습니다.
클라이언트 쓰기	기본적으로 이 수준은 보통 으로 설정됩니다. 을 참조하십시오 클라이언트가 감사 메시지를 기록합니다.

이 기본값은 버전 10.3 이상을 사용하여 StorageGRID를 처음 설치한 경우에 적용됩니다. 이전 버전의 StorageGRID에서 업그레이드한 경우 모든 범주의 기본값은 보통으로 설정됩니다.

업그레이드 중에는 감사 수준 구성이 즉시 적용되지 않습니다.

단계

1. 구성 * > * 모니터링 * > * 감사 및 syslog 서버 * 를 선택합니다.



2. 각 감사 메시지 범주에 대해 드롭다운 목록에서 감사 수준을 선택합니다.

감사 수준	설명
꺼짐	범주의 감사 메시지가 기록되지 않습니다.

감사 수준	설명
오류	오류 메시지만 기록됩니다. 결과 코드가 "성공"하지 않은 감사 메시지입니다(SUCS).
정상	표준 트랜잭션 메시지가 기록됩니다. — 범주에 대한 이 지침에 나열된 메시지입니다.
디버그	사용되지 않음. 이 수준은 일반 감사 수준과 동일하게 작동합니다.

특정 수준에 포함되는 메시지에는 더 높은 수준으로 기록되는 메시지가 포함됩니다. 예를 들어 일반 수준에는 모든 오류 메시지가 포함됩니다.

3. 선택적으로 * 감사 프로토콜 헤더 * 에서 클라이언트 읽기 및 쓰기 감사 메시지에 포함할 HTTP 요청 헤더를 정의합니다. 0개 이상의 문자를 일치시키려면 별표(\ *)를 와일드카드로 사용하십시오. 이스케이프 시퀀스(\ *)를 사용하여 리터럴 별표를 일치시킵니다.

   감사 프로토콜 헤더는 S3 및 Swift 요청에만 적용됩니다.

4. 필요한 경우 추가 헤더를 만들려면 * 다른 헤더 추가 * 를 선택합니다.

   HTTP 헤더가 요청에서 검색되면 HTRH 필드 아래의 감사 메시지에 포함됩니다.

   감사 프로토콜 요청 헤더는 * 클라이언트 읽기 * 또는 * 클라이언트 쓰기 * 에 대한 감사 수준이 * 꺼짐 * 이 아닌 경우에만 기록됩니다.

5. 저장 * 을 선택합니다

   구성이 성공적으로 저장되었음을 나타내는 녹색 배너가 표시됩니다.

외부 **syslog** 서버를 사용합니다

감사 정보를 원격으로 저장하려면 외부 syslog 서버를 구성할 수 있습니다.

- 감사 정보를 외부 syslog 서버에 저장하려면 로 이동합니다 외부 syslog 서버를 구성합니다.
- 외부 syslog 서버를 사용하지 않는 경우 로 이동합니다 감사 정보 대상을 선택합니다.

감사 정보 대상을 선택합니다

감사 로그, 보안 이벤트 로그 및 응용 프로그램 로그를 보낼 위치를 지정할 수 있습니다.

일부 대상은 외부 syslog 서버를 사용하는 경우에만 사용할 수 있습니다. 을 참조하십시오 외부 syslog 서버를 구성합니다 외부 syslog 서버를 구성하려면 다음을 수행합니다.

StorageGRID 소프트웨어 로그에 대한 자세한 내용은 을 참조하십시오 StorageGRID 소프트웨어 로그.

1. 감사 및 syslog 서버 페이지의 나열된 옵션 중에서 감사 정보의 대상을 선택합니다.

옵션을 선택합니다	설명
기본값(관리자 노드/로컬 노드)	감사 메시지는 관리 노드의 감사 로그("audit.log")로 전송되고 보안 이벤트 로그 및 응용 프로그램 로그는 생성된 노드("로컬 노드"라고도 함)에 저장됩니다.
외부 syslog 서버	감사 정보는 외부 syslog 서버로 전송되고 로컬 노드에 저장됩니다. 전송되는 정보의 유형은 외부 syslog 서버를 구성한 방식에 따라 다릅니다. 이 옵션은 외부 syslog 서버를 구성한 후에만 활성화됩니다.
관리 노드 및 외부 syslog 서버	감사 메시지는 Admin Node의 Audit Log("audit.log")로 전송되며, Audit 정보는 외부 syslog 서버로 전송되어 Local Node에 저장된다. 전송되는 정보의 유형은 외부 syslog 서버를 구성한 방식에 따라 다릅니다. 이 옵션은 외부 syslog 서버를 구성한 후에만 활성화됩니다.
로컬 노드만 해당	관리자 노드 또는 원격 syslog 서버로 감사 정보가 전송되지 않습니다. 감사 정보는 감사 정보를 생성한 노드에만 저장됩니다. • 참고 *: StorageGRID는 공간을 확보하기 위해 주기적으로 이러한 로컬 로그를 제거합니다. 노드의 로그 파일이 1GB에 도달하면 기존 파일이 저장되고 새 로그 파일이 시작됩니다. 로그의 회전 제한은 21개 파일입니다. 22버전의 로그 파일이 만들어지면 가장 오래된 로그 파일이 삭제됩니다. 평균적으로 약 20GB의 로그 데이터가 각 노드에 저장됩니다.

모든 로컬 노드에서 생성된 감사 정보는 '/var/local/log/localaudit.log'에 저장됩니다

1. 저장 * 을 선택합니다.

다음과 같은 경고 메시지가 나타납니다.

로그 대상을 변경하시겠습니까?

1. [확인]을 선택하여 감사 정보의 대상을 변경할지 확인합니다.

   감사 구성이 성공적으로 저장되었음을 알리는 녹색 배너가 나타납니다.

   새 로그가 선택한 대상으로 전송됩니다. 기존 로그는 현재 위치에 남아 있습니다.

관련 정보

외부 syslog 서버에 대한 고려 사항

StorageGRID 관리

외부 syslog 서버의 문제를 해결합니다

외부 **syslog** 서버를 사용합니다

외부 **syslog** 서버에 대한 고려 사항

다음 지침에 따라 필요한 외부 syslog 서버의 크기를 추정합니다.

외부 **syslog** 서버란 무엇입니까**?**

외부 syslog 서버는 단일 위치에서 시스템 감사 정보를 수집하는 데 사용할 수 있는 StorageGRID 외부의 서버입니다. 외부 syslog 서버를 사용하면 감사 정보의 대상을 구성하여 관리 노드의 네트워크 트래픽을 줄이고 정보를 보다 효율적으로 관리할 수 있습니다. 외부 syslog 서버로 보낼 수 있는 감사 정보의 유형은 다음과 같습니다.

- 정상적인 시스템 작동 중에 생성된 감사 메시지를 포함하는 감사 로그
- 로그인 및 루트 에스컬레이션과 같은 보안 관련 이벤트입니다
- 발생한 문제를 해결하기 위해 지원 케이스를 열어야 하는 경우 요청될 수 있는 응용 프로그램 로그

외부 **syslog** 서버의 크기를 예측하는 방법

일반적으로, 그리드는 초당 S3 작업 또는 초당 바이트 수로 정의되는 필요한 처리량을 달성하도록 크기가 조정됩니다. 예를 들어, 그리드에서 1,000개의 초당 S3 작업, 즉 2,000개의 오브젝트 검색 및 검색을 처리해야 하는 요구사항이 있을 수 있습니다. 그리드의 데이터 요구 사항에 따라 외부 syslog 서버의 크기를 지정해야 합니다.

이 섹션에서는 외부 syslog 서버가 처리할 수 있어야 하는 다양한 유형의 로그 메시지 속도 및 평균 크기를 예측하는 데 도움이 되는 몇 가지 발견적 공식을 제공합니다. 이는 그리드의 알려진 성능 특성 또는 원하는 성능 특성(초당 S3 작업 수)을 기준으로 합니다.

계산 공식에서 초당 **S3** 작업을 사용합니다

그리드의 크기가 초당 바이트 수로 표시된 처리량인 경우 이 사이징을 초당 S3 작업으로 변환하여 추정 공식을 사용해야 합니다. 그리드 처리량을 변환하려면 먼저 평균 개체 크기를 확인해야 합니다. 이 크기는 기존 감사 로그 및 메트릭의 정보(있는 경우)를 사용하거나 StorageGRID를 사용할 애플리케이션에 대한 지식을 사용하여 확인할 수 있습니다. 예를 들어, 그리드의 크기가 2,000 MB/s의 처리량을 달성할 수 있도록 조정되었고 평균 오브젝트 크기가 2MB인 경우, 그리드는 초당 1,000 S3 작업(2,000MB/2MB)을 처리할 수 있도록 크기가 조정되었습니다.

> 다음 섹션의 외부 syslog 서버 크기 조정 공식은 최악의 경우를 추정하는 대신 일반적인 대/소문자 추정치를 제공합니다. 구성 및 워크로드에 따라 syslog 메시지 또는 syslog 데이터 볼륨이 수식에 따라 예측되는 것보다 높거나 낮을 수 있습니다. 수식은 지침으로만 사용됩니다.

감사 로그의 계산 공식

그리드에서 지원해야 하는 초당 S3 작업 수 이외의 S3 작업 부하에 대한 정보가 없는 경우 외부 syslog 서버가 다음 공식을 사용하여 처리해야 하는 감사 로그 볼륨을 예측할 수 있습니다. 감사 수준을 기본값으로 설정했다고 가정합니다(오류 로 설정된 스토리지를 제외한 모든 범주는 보통 으로 설정됨).

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

예를 들어, 그리드가 초당 1,000개의 S3 작업용으로 사이징된 경우 외부 syslog 서버는 초당 2,000개의 syslog 메시지를 지원하도록 크기를 조정해야 하며 초당 1.6MB의 속도로 감사 로그 데이터를 수신(일반적으로 저장)할 수

있어야 합니다.

당신이 당신의 업무량에 대해 더 알고 있다면, 더 정확한 예측들이 가능합니다. 감사 로그의 경우 가장 중요한 추가 변수는 S3 작업이 놓이는 비율(대)입니다 다음 S3 필드의 평균 크기(바이트)와 평균 크기(표에 사용된 4자 약어는 감사 로그 필드 이름입니다).

코드	필드에 입력합니다	설명
SACC	S3 테넌트 계정 이름(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 이름입니다. 익명 요청에 대해 비어 있습니다.
SBAC	S3 테넌트 계정 이름(버킷 소유자)	버킷 소유자의 테넌트 계정 이름입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
S3BK	S3 버킷	S3 버킷 이름입니다.
S3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷의 작업에는 이 필드가 포함되지 않습니다.

P를 사용하여 S3 작업 중 위치, 0 ≤ P ≤ 1(100% put 워크로드, P=1 및 100% get 워크로드, P=0)의 비율을 표시하겠습니다.

K를 사용하여 S3 계정 이름, S3 버킷 및 S3 키의 평균 크기를 나타내보겠습니다. S3 계정 이름이 항상 -s3-계정(13바이트)이고, 버킷에는 /my/application/bucket-12345(28바이트)와 같은 고정 길이 이름이 있고, 오브젝트에는 5733a5d7-f069-411f-8fbd-13247494c69c(36바이트)와 같은 고정 길이 키가 있다고 가정해 보겠습니다. 그런 다음 K 값은 90(13+13+28+36)입니다.

P와 K의 값을 결정할 수 있는 경우 감사 수준을 기본값으로 설정했다는 가정 하에 외부 syslog 서버가 처리해야 하는 감사 로그 볼륨을 다음 공식을 사용하여 추정할 수 있습니다(스토리지를 제외한 모든 범주는 Normal로 설정됨). 오류 로 설정된 경우):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

예를 들어, 그리드가 초당 1,000개의 S3 작업용으로 사이징된 경우, 작업 부하의 크기는 50%이고 S3 계정 이름, 버킷 이름은 개체 이름의 평균 90바이트는 외부 syslog 서버가 초당 1,500개의 syslog 메시지를 지원하도록 사이징되어야 하며, 일반적으로 초당 약 1MB의 속도로 감사 로그 데이터를 수신(및 저장)할 수 있어야 합니다.

기본 감사 수준이 아닌 감사 수준에 대한 계산 공식

감사 로그에 제공된 수식에서는 기본 감사 수준 설정(오류 로 설정된 스토리지를 제외한 모든 범주가 보통으로 설정됨)을 사용한다고 가정합니다. 기본값이 아닌 감사 수준 설정에 대한 감사 메시지의 비율 및 평균 크기를 추정하는 자세한 공식은 사용할 수 없습니다. 그러나 다음 표를 사용하여 요율을 대략적으로 추정할 수 있습니다. 감사 로그에 제공된 평균 크기 수식을 사용할 수 있지만 "추가" 감사 메시지는 평균적으로 기본 감사 메시지보다 작기 때문에 과대 평가로 이어질 수 있습니다.

조건	수식
복제: 감사 수준 모두 디버그 또는 정상 으로 설정됩니다	감사 로그 속도 = S3 작업 속도 8개
삭제 코딩: 모두 디버그 또는 정상 으로 설정된 감사 수준	기본 설정과 동일한 수식을 사용합니다

보안 이벤트의 계산 공식

보안 이벤트는 S3 운영과 관련이 없으며 일반적으로 최소한의 로그 및 데이터 볼륨을 생성합니다. 이러한 이유로 추정 공식은 제공되지 않습니다.

응용 프로그램 로그의 계산 공식

그리드에서 지원해야 하는 초당 S3 작업 수 이외의 S3 작업 부하에 대한 정보가 없는 경우 외부 syslog 서버에서 다음 공식을 사용하여 처리해야 하는 애플리케이션 로그 볼륨을 예측할 수 있습니다.

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

예를 들어, 그리드가 초당 1,000개의 S3 작업용으로 사이징된 경우 외부 syslog 서버는 초당 3,300개의 애플리케이션 로그를 지원할 수 있도록 사이징되어야 하고 초당 약 1.2MB의 속도로 애플리케이션 로그 데이터를 수신 및 저장할 수 있어야 합니다.

당신이 당신의 업무량에 대해 더 알고 있다면, 더 정확한 예측들이 가능합니다. 애플리케이션 로그의 경우 가장 중요한 추가 변수는 데이터 보호 전략(복제 및 삭제 코딩), 위치(vs 다음 S3 필드의 평균 크기(바이트)와 평균 크기(표에 사용되는 4자 약어는 감사 로그 필드 이름입니다).

코드	필드에 입력합니다	설명
SACC	S3 테넌트 계정 이름(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 이름입니다. 익명 요청에 대해 비어 있습니다.
SBAC	S3 테넌트 계정 이름(버킷 소유자)	버킷 소유자의 테넌트 계정 이름입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
S3BK	S3 버킷	S3 버킷 이름입니다.
S3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷의 작업에는 이 필드가 포함되지 않습니다.

크기 예측의 예

이 섹션에서는 다음과 같은 데이터 보호 방법을 사용하여 그리드에 대한 예측 공식을 사용하는 방법의 예를 설명합니다.

- 복제
- 삭제 코딩

데이터 보호를 위해 복제를 사용하는 경우

P는 S3 작업의 비율을, 여기서 0 ≤ P ≤ 1(100% put 워크로드의 경우 P=1, 100% get 워크로드의 경우 P=0)을 나타냅니다.

K는 S3 계정 이름, S3 버킷 및 S3 키의 평균 크기를 나타냅니다. S3 계정 이름이 항상 -s3-계정(13바이트)이고, 버킷에는 /my/application/bucket-12345(28바이트)와 같은 고정 길이 이름이 있고, 오브젝트에는 5733a5d7-f069-411f-8fbd-13247494c69c(36바이트)와 같은 고정 길이 키가 있다고 가정해 보겠습니다. 그런 다음 K의 값은 90(13+13+28+36)입니다.

P와 K의 값을 확인할 수 있는 경우, 외부 syslog 서버가 다음 공식을 사용하여 처리할 수 있어야 하는 애플리케이션 로그 볼륨을 예측할 수 있습니다.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

예를 들어, 그리드가 초당 1,000개의 S3 작업에 맞게 사이징된 경우 작업 부하가 50%이고 S3 계정 이름, 버킷 이름 및 오브젝트 이름이 평균 90바이트인 경우, 외부 syslog 서버는 초당 1800개의 애플리케이션 로그를 지원하도록 크기여야 합니다. 그리고 애플리케이션 데이터를 초당 0.5MB의 속도로 수신(일반적으로 저장)할 것입니다.

데이터 보호를 위해 삭제 코딩을 사용하는 경우

P는 S3 작업의 비율을, 여기서 0 ≤ P ≤ 1(100% put 워크로드의 경우 P=1, 100% get 워크로드의 경우 P=0)을 나타냅니다.

K는 S3 계정 이름, S3 버킷 및 S3 키의 평균 크기를 나타냅니다. S3 계정 이름이 항상 -s3-계정(13바이트)이고, 버킷에는 /my/application/bucket-12345(28바이트)와 같은 고정 길이 이름이 있고, 오브젝트에는 5733a5d7-f069-411f-8fbd-13247494c69c(36바이트)와 같은 고정 길이 키가 있다고 가정해 보겠습니다. 그런 다음 K의 값은 90(13+13+28+36)입니다.

P와 K의 값을 확인할 수 있는 경우, 외부 syslog 서버가 다음 공식을 사용하여 처리할 수 있어야 하는 애플리케이션 로그 볼륨을 예측할 수 있습니다.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

예를 들어, 그리드가 초당 1,000개의 S3 작업에 맞게 사이징된 경우, 작업 부하가 50%이고 S3 계정 이름, 버킷 이름, 객체 이름 평균 90바이트에서 외부 syslog 서버는 초당 2,250개의 애플리케이션 로그를 지원하도록 크기를 조정해야 하며, 초당 0.6MB의 속도로 애플리케이션 데이터를 수신(일반적으로 저장)할 수 있어야 합니다.

감사 메시지 수준 및 외부 syslog 서버 구성에 대한 자세한 내용은 다음을 참조하십시오.

- 외부 syslog 서버를 구성합니다

- 감사 메시지 및 로그 대상을 구성합니다

외부 **syslog** 서버를 구성합니다

감사 로그, 응용 프로그램 로그 및 보안 이벤트 로그를 그리드 외부의 위치에 저장하려면 다음 절차를 사용하여 외부 syslog 서버를 구성합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 로그 파일을 수신하고 저장할 용량이 있는 syslog 서버가 있습니다. 자세한 내용은 을 참조하십시오 외부 syslog 서버에 대한 고려 사항.
- TLS 또는 RELP/TLS를 사용하려는 경우 올바른 서버 및 클라이언트 인증을 보유하고 있습니다.

이 작업에 대해

외부 syslog 서버로 감사 정보를 보내려면 먼저 외부 서버를 구성해야 합니다.

감사 정보를 외부 syslog 서버로 전송하면 다음을 수행할 수 있습니다.

- 감사 메시지, 응용 프로그램 로그 및 보안 이벤트와 같은 감사 정보를 보다 효율적으로 수집 및 관리합니다
- 관리 노드를 거치지 않고도 감사 정보가 다양한 스토리지 노드에서 외부 syslog 서버로 직접 전송되므로 관리 노드의 네트워크 트래픽을 줄일 수 있습니다

> 외부 syslog 서버로 로그를 전송할 때 메시지 끝에서 8192바이트보다 큰 단일 로그가 잘려서 외부 syslog 서버 구현의 일반적인 제한 사항을 따릅니다.

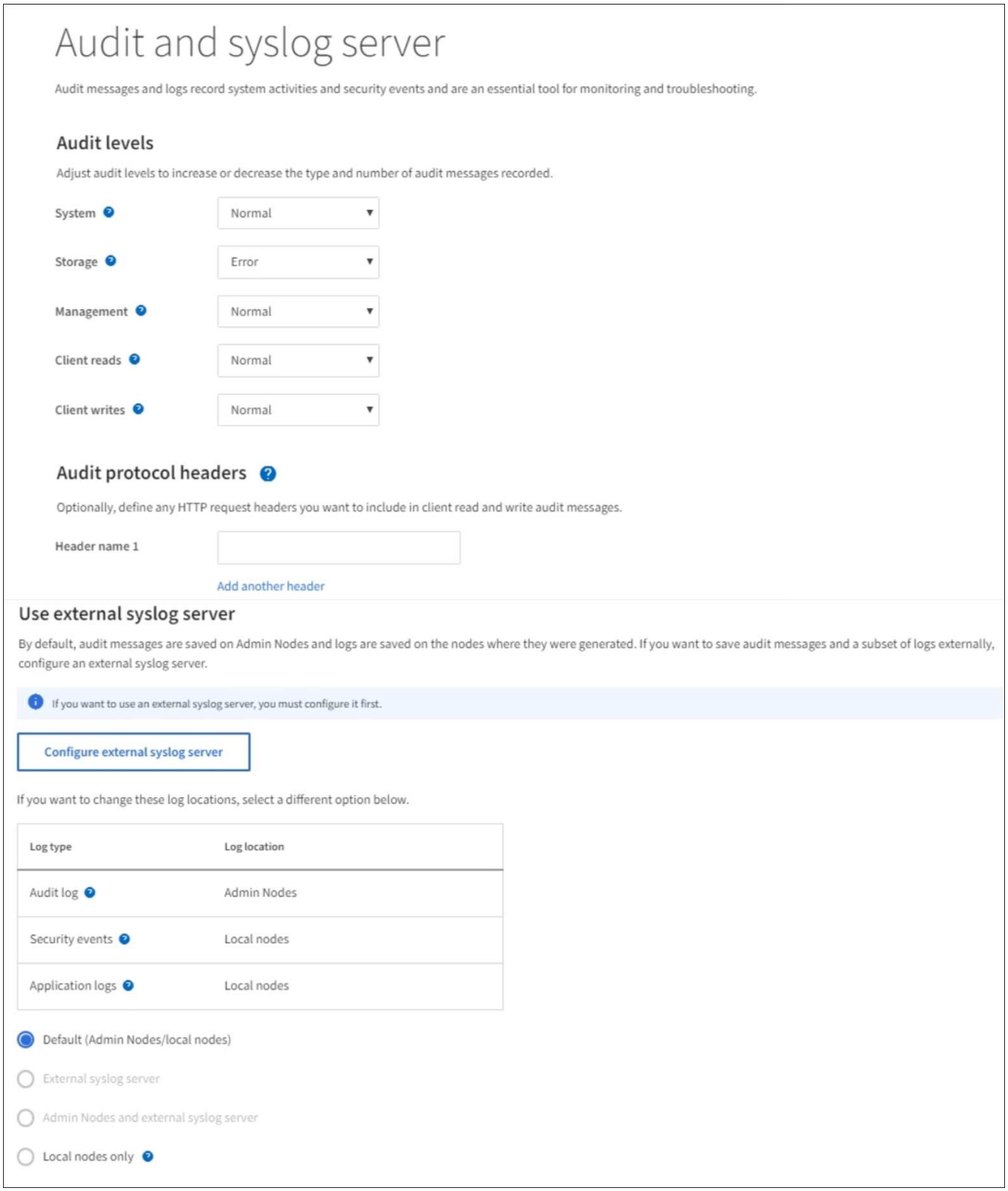
> 외부 syslog 서버에 장애가 발생할 경우 전체 데이터 복구 옵션을 최대화하려면 각 노드에서 최대 20GB의 감사 레코드 로컬 로그(localaudit.log)가 유지됩니다.

> 이 절차에서 사용할 수 있는 구성 옵션이 요구 사항을 충족할 만큼 유연하지 않은 경우 전용 API '감사 대상' 끝점을 사용하여 추가 구성 옵션을 적용할 수 있습니다. 예를 들어, 서로 다른 노드 그룹에 서로 다른 syslog 서버를 사용할 수 있습니다.

syslog 서버 구성 마법사에 액세스합니다

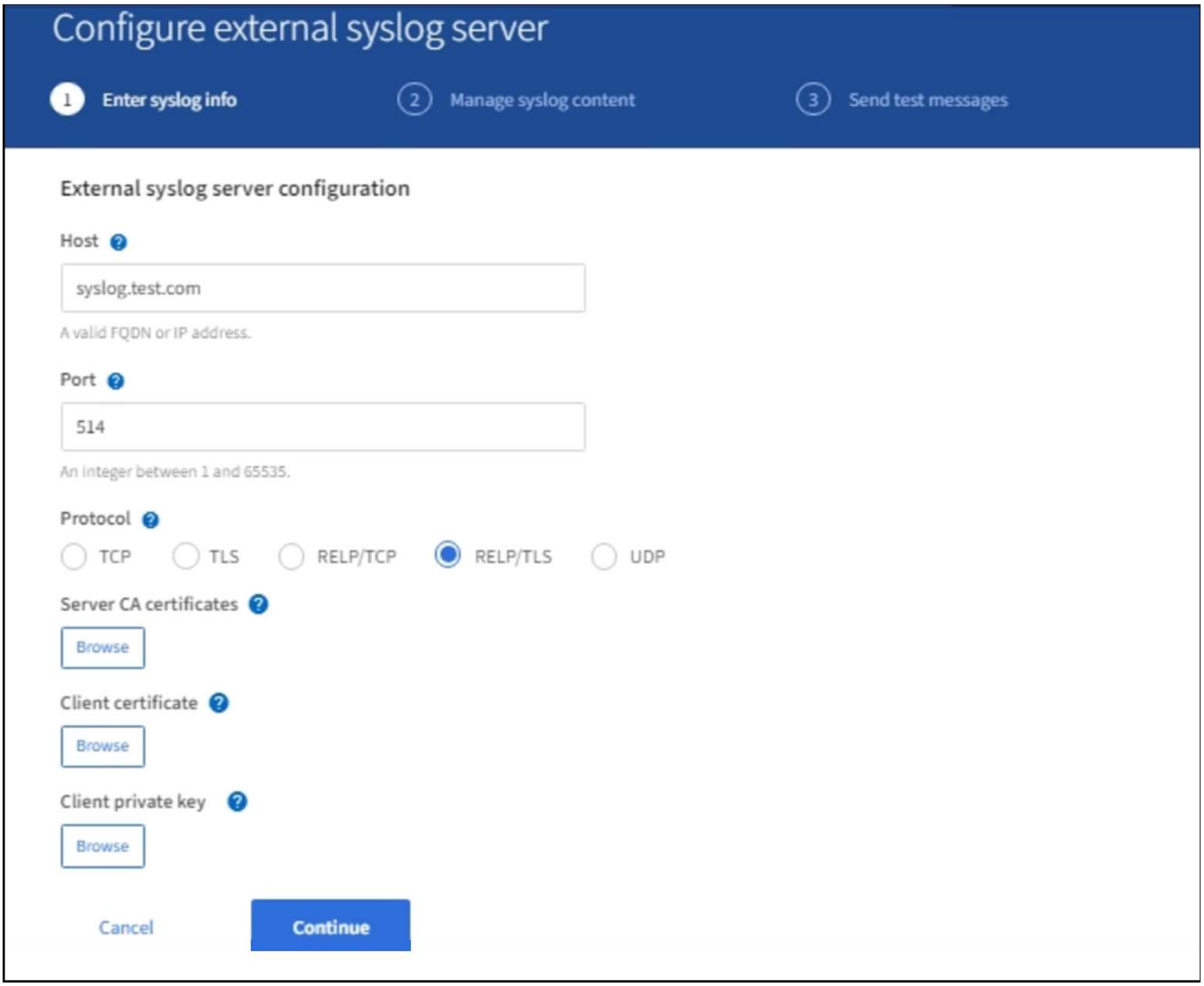
단계

1. 구성 * > * 모니터링 * > * 감사 및 syslog 서버 * 를 선택합니다.



2. 감사 및 syslog 서버 페이지에서 * 외부 syslog 서버 구성 * 을 선택합니다. 이전에 외부 syslog 서버를 구성한 경우 * 외부 syslog 서버 편집 * 을 선택합니다.

syslog 정보를 입력합니다



1. 호스트 * 필드에 외부 syslog 서버에 대한 유효한 정규화된 도메인 이름 또는 IPv4 또는 IPv6 주소를 입력합니다.
2. 외부 syslog 서버의 대상 포트를 입력합니다(1과 65535 사이의 정수여야 함). 기본 포트는 514입니다.
3. 외부 syslog 서버로 감사 정보를 보내는 데 사용되는 프로토콜을 선택합니다.

   TLS 또는 RELP/TLS를 사용하는 것이 좋습니다. 이러한 옵션 중 하나를 사용하려면 서버 인증서를 업로드해야 합니다.

   인증서를 사용하면 그리드와 외부 syslog 서버 간의 연결을 보호할 수 있습니다. 자세한 내용은 을 참조하십시오 StorageGRID 보안 인증서를 사용합니다.

   모든 프로토콜 옵션에는 외부 syslog 서버에 대한 지원 및 구성이 필요합니다. 외부 syslog 서버와 호환되는 옵션을 선택해야 합니다.

   > 신뢰할 수 있는 이벤트 로깅 프로토콜(RELP)은 syslog 프로토콜의 기능을 확장하여 이벤트 메시지를 안정적으로 제공합니다. RELP를 사용하면 외부 syslog 서버를 다시 시작해야 하는 경우 감사 정보의 손실을 방지할 수 있습니다.

4. Continue * 를 선택합니다.

5. * TLS * 또는 * RELP/TLS * 를 선택한 경우 다음 인증서를 업로드하십시오.

   - * 서버 CA 인증서 *: 외부 syslog 서버를 확인하기 위한 하나 이상의 트러스트된 CA 인증서(PEM 인코딩). 이 인수를 생략하면 기본 Grid CA 인증서가 사용됩니다. 여기에 업로드하는 파일은 CA 번들이 될 수 있습니다.
   - * 클라이언트 인증서 *: 외부 syslog 서버(PEM 인코딩)에 대한 인증을 위한 클라이언트 인증서입니다.
   - * 클라이언트 개인 키 *: 클라이언트 인증서에 대한 개인 키(PEM 인코딩).

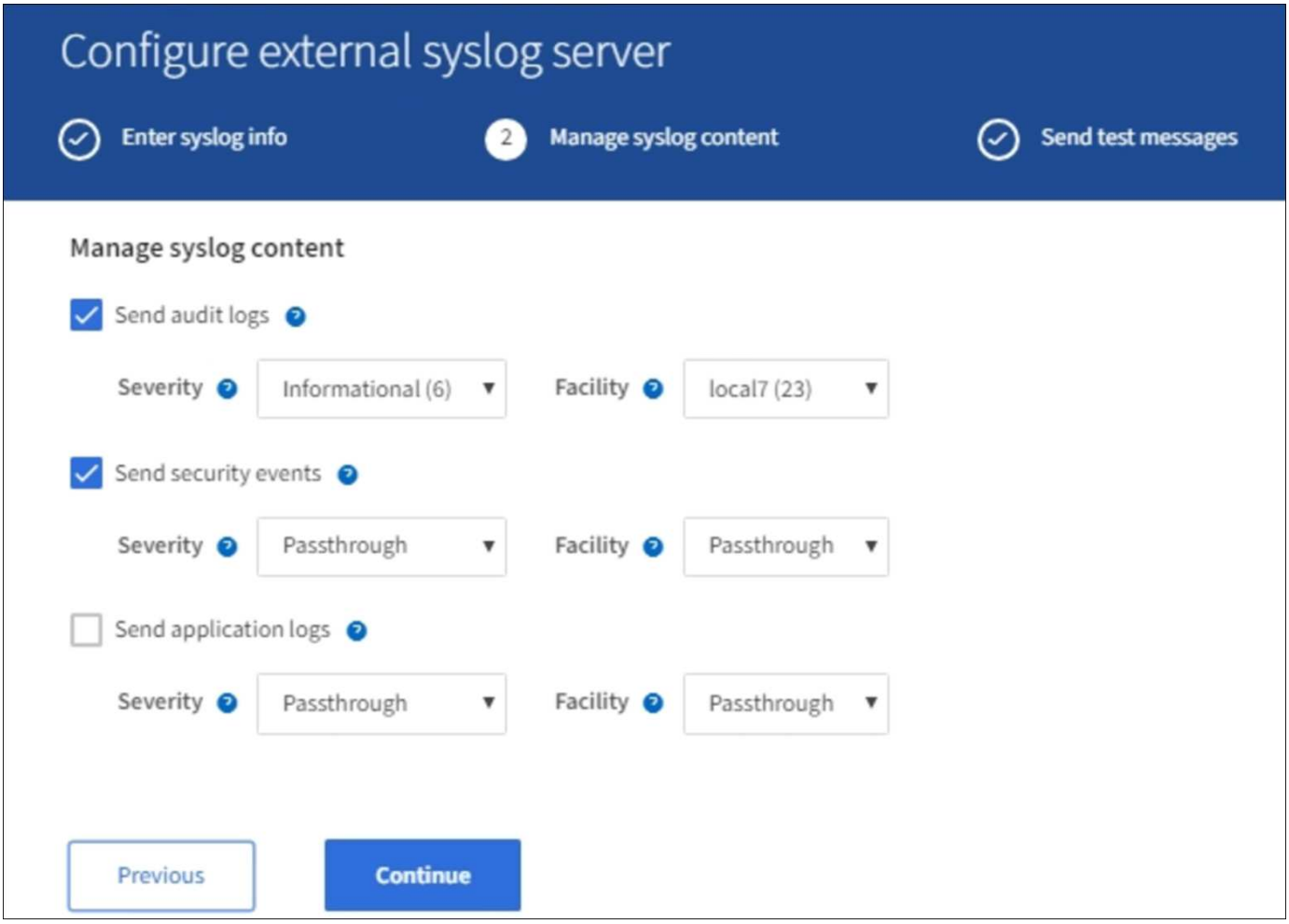
   > 클라이언트 인증서를 사용하는 경우 클라이언트 개인 키도 사용해야 합니다. 암호화된 개인 키를 제공하는 경우 암호문도 제공해야 합니다. 키와 암호를 저장해야 하므로 암호화된 개인 키를 사용하면 보안 상의 큰 이점이 없습니다. 사용 가능한 경우 암호화되지 않은 개인 키를 사용하는 것이 좋습니다.

   i. 사용할 인증서 또는 키를 * 찾아보기 * 를 선택합니다.
   ii. 인증서 파일 또는 키 파일을 선택합니다.
   iii. 파일을 업로드하려면 * 열기 * 를 선택합니다.

   인증서 또는 키 파일 이름 옆에 녹색 확인 표시가 나타나 성공적으로 업로드되었음을 알려줍니다.

6. Continue * 를 선택합니다.

syslog 콘텐츠를 관리합니다



1. 외부 syslog 서버로 보낼 감사 정보의 각 유형을 선택합니다.
   - * 감사 로그 전송 *: StorageGRID 이벤트 및 시스템 활동
   - * 보안 이벤트 전송 *: 권한이 없는 사용자가 로그인을 시도하거나 사용자가 루트로 로그인하는 등의 보안 이벤트입니다
   - * 응용 프로그램 로그 전송 *: 문제 해결에 유용한 로그 파일:
     - bycast-err.log
     - bycast.log
     - jaeger.log
     - nms.log (관리자 노드 전용)
     - prometheus.log
     - raft.log
     - hagroups.log
2. 드롭다운 메뉴를 사용하여 보내려는 감사 정보 범주에 대한 심각도 및 기능(메시지 유형)을 선택합니다.

   심각도 및 설비에 대해 * 통과 * 를 선택하면 원격 syslog 서버로 전송되는 정보는 노드에 로컬로 로그온할 때와 동일한 심각도와 기능을 받습니다. 시설 및 심각도를 설정하면 더욱 쉽게 분석할 수 있도록 로그를 사용자 지정 가능한 방식으로 집계하는 데 도움이 됩니다.

   > StorageGRID 소프트웨어 로그에 대한 자세한 내용은 을 참조하십시오 StorageGRID 소프트웨어 로그.

   a. 심각도 * 의 경우 * 통과 * 를 선택하여 외부 syslog에 전송되는 각 메시지의 심각도 값이 로컬 syslog와 동일하게 되도록 합니다.

      감사 로그의 경우 * 통과 * 를 선택하면 '정보'가 심각합니다.

      보안 이벤트의 경우 * 통과 * 를 선택하면 노드의 Linux 배포에서 심각도 값이 생성됩니다.

      응용 프로그램 로그의 경우 * 통과 * 를 선택하면 문제의 내용에 따라 심각도가 '정보'와 '알림'에 따라 다릅니다. 예를 들어 NTP 서버를 추가하고 HA 그룹을 구성하면 '정보' 값이 제공되지만 SSM 또는 RSM 서비스를 의도적으로 중지하는 경우 '알림'이 표시됩니다.

   b. 통과 연결 값을 사용하지 않으려면 0에서 7 사이의 심각도 값을 선택합니다.

      선택한 값은 이 유형의 모든 메시지에 적용됩니다. 심각도가 고정 값으로 재정의되면 서로 다른 심각도에 대한 정보가 손실됩니다.

심각도입니다	설명
0	비상: 시스템을 사용할 수 없습니다
1	경고: 즉시 조치를 취해야 합니다
2	심각: 심각 상태

심각도입니다	설명
3	오류: 오류 조건
4	경고: 경고 조건
5	주의사항: 정상이지만 중대한 조건
6	정보: 정보 메시지
7	디버그: 디버그 레벨 메시지

c. Facility * 의 경우 * PassThrough * 를 선택하여 외부 syslog로 전송되는 각 메시지가 로컬 syslog와 동일한 설비 값을 가지도록 합니다.

감사 로그의 경우 * 통과 * 를 선택하면 외부 syslog 서버로 전송된 기능이 'local7'입니다.

보안 이벤트의 경우 * PassThrough * 를 선택하면 시설 값이 노드의 Linux 배포판에 의해 생성됩니다.

응용 프로그램 로그의 경우 * 통과 * 를 선택하면 외부 syslog 서버로 전송된 응용 프로그램 로그의 항목 값은 다음과 같습니다.

응용 프로그램 로그	통과 연결 값입니다
bycast.log	사용자 또는 데몬
bycast-err.log	사용자, 데몬, local3 또는 local4
jaeger.log	로컬2
nms.log	로컬3
prometheus.log	로컬4
raft.log	로컬5
hagroups.log	로컬6

d. 통과 연결 값을 사용하지 않으려면 0에서 23 사이의 설비 값을 선택합니다.

선택한 값은 이 유형의 모든 메시지에 적용됩니다. 고정 값으로 시설을 재정의하면 다른 시설에 대한 정보가 손실됩니다.

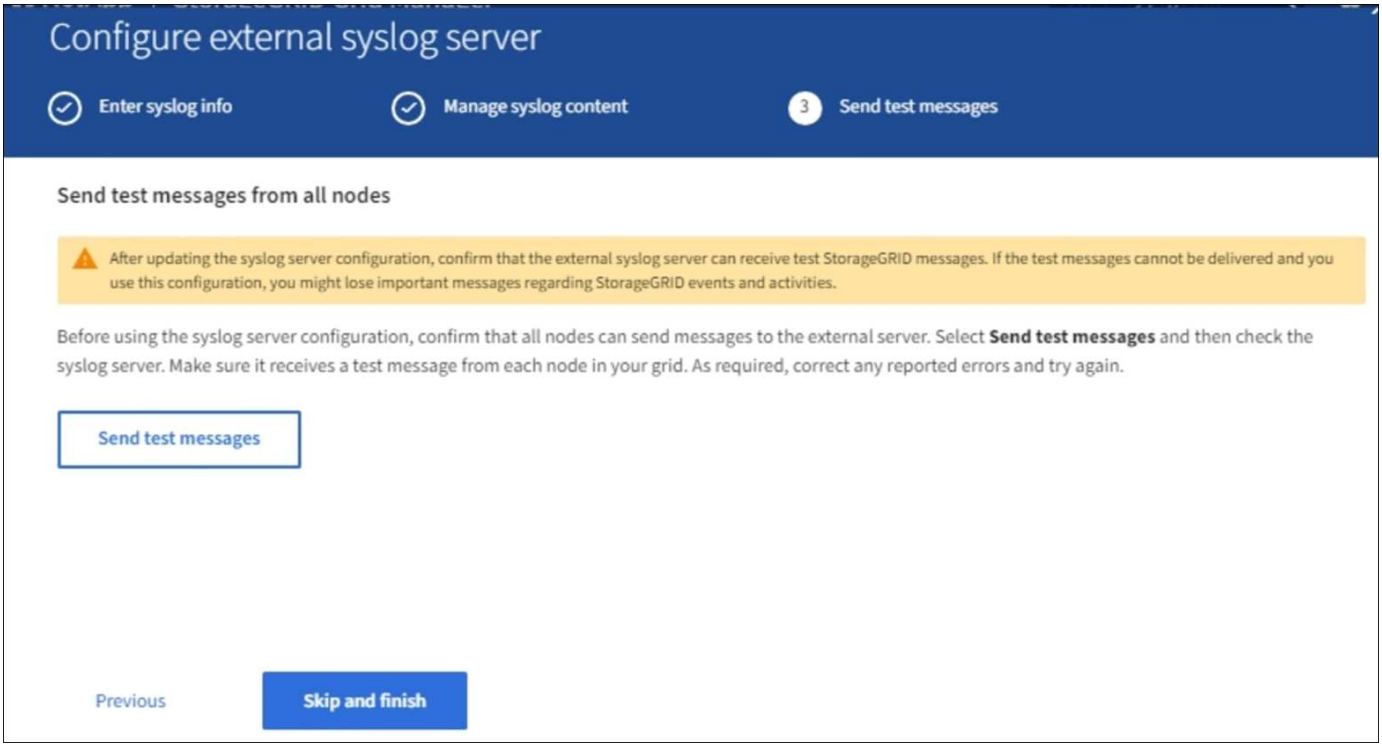
있습니다	설명
0	Kern(커널 메시지)

있습니다	설명
1	사용자(사용자 수준 메시지)
2	메일
3	데몬(시스템 데몬)
4	인증(보안/인증 메시지)
5	syslog(syslogd에 의해 내부적으로 생성된 메시지)
6	LPR(라인 프린터 하위 시스템)
7	뉴스(네트워크 뉴스 서브시스템)
8	UUCP
9	cron(클록 데몬)
10	보안(보안/인증 메시지)
11	FTP
12	NTP
13	Logaudit(로그 감사)
14	Logalert(로그 경고)
15	클록(클록 데몬)
16	로컬0
17	로컬1
18	로컬2
19	로컬3
20	로컬4
21	로컬5

있습니다	설명
22	로컬6
23	로컬7

3. Continue * 를 선택합니다.

테스트 메시지를 보냅니다



외부 syslog 서버를 사용하기 전에 그리드의 모든 노드가 외부 syslog 서버로 테스트 메시지를 보내도록 요청해야 합니다. 외부 syslog 서버로 데이터를 전송하기 전에 이러한 테스트 메시지를 사용하여 전체 로그 수집 인프라의 유효성을 확인해야 합니다.

> 외부 syslog 서버가 그리드의 각 노드로부터 테스트 메시지를 수신하고 메시지가 예상대로 처리되었음을 확인하기 전까지는 외부 syslog 서버 구성을 사용하지 마십시오.

1. 테스트 메시지를 보내지 않고 외부 syslog 서버가 제대로 구성되어 있고 그리드의 모든 노드에서 감사 정보를 받을 수 있는 경우 * Skip and finish * 를 선택합니다.

   구성이 성공적으로 저장되었음을 나타내는 녹색 배너가 나타납니다.

2. 그렇지 않으면 * 테스트 메시지 전송 * 을 선택합니다.

   테스트를 중지할 때까지 테스트 결과가 페이지에 계속 표시됩니다. 테스트가 진행되는 동안 감사 메시지는 이전에 구성된 대상으로 계속 전송됩니다.

3. 오류가 발생하면 오류를 수정하고 * 테스트 메시지 보내기 * 를 다시 선택합니다. 을 참조하십시오 외부 syslog 서버 문제 해결 오류를 해결하는 데 도움이 됩니다.

4. 모든 노드가 테스트를 통과했음을 나타내는 녹색 배너가 나타날 때까지 기다립니다.
5. syslog 서버를 확인하여 테스트 메시지가 예상대로 수신 및 처리되는지 확인합니다.

> UDP를 사용하는 경우 전체 로그 수집 인프라를 확인합니다. UDP 프로토콜은 다른 프로토콜처럼 엄격한 오류 감지를 허용하지 않습니다.

6. Stop and finish * 를 선택합니다.

   감사 및 syslog 서버 * 페이지로 돌아갑니다. syslog 서버 구성이 성공적으로 저장되었음을 알리는 녹색 배너가 나타납니다.

> 외부 syslog 서버를 포함하는 대상을 선택할 때까지 StorageGRID 감사 정보가 외부 syslog 서버로 전송되지 않습니다.

감사 정보 대상을 선택합니다

보안 이벤트 로그, 응용 프로그램 로그 및 감사 메시지 로그를 보낼 위치를 지정할 수 있습니다.

> StorageGRID 소프트웨어 로그에 대한 자세한 내용은 을 참조하십시오 StorageGRID 소프트웨어 로그.

1. 감사 및 syslog 서버 페이지의 나열된 옵션 중에서 감사 정보의 대상을 선택합니다.

옵션을 선택합니다	설명
기본값(관리자 노드/로컬 노드)	감사 메시지는 관리 노드의 감사 로그("audit.log")로 전송되고 보안 이벤트 로그 및 응용 프로그램 로그는 생성된 노드("로컬 노드"라고도 함)에 저장됩니다.
외부 syslog 서버	감사 정보는 외부 syslog 서버로 전송되고 로컬 노드에 저장됩니다. 전송되는 정보의 유형은 외부 syslog 서버를 구성한 방식에 따라 다릅니다. 이 옵션은 외부 syslog 서버를 구성한 후에만 활성화됩니다.
관리 노드 및 외부 syslog 서버	감사 메시지는 Admin Node의 Audit Log("audit.log")로 전송되며, Audit 정보는 외부 syslog 서버로 전송되어 Local Node에 저장된다. 전송되는 정보의 유형은 외부 syslog 서버를 구성한 방식에 따라 다릅니다. 이 옵션은 외부 syslog 서버를 구성한 후에만 활성화됩니다.
로컬 노드만 해당	관리자 노드 또는 원격 syslog 서버로 감사 정보가 전송되지 않습니다. 감사 정보는 감사 정보를 생성한 노드에만 저장됩니다. • 참고 *: StorageGRID는 공간을 확보하기 위해 주기적으로 이러한 로컬 로그를 제거합니다. 노드의 로그 파일이 1GB에 도달하면 기존 파일이 저장되고 새 로그 파일이 시작됩니다. 로그의 회전 제한은 21개 파일입니다. 22버전의 로그 파일이 만들어지면 가장 오래된 로그 파일이 삭제됩니다. 평균적으로 약 20GB의 로그 데이터가 각 노드에 저장됩니다.

> 모든 로컬 노드에서 생성된 감사 정보는 '/var/local/log/localaudit.log'에 저장됩니다

1. 저장 * 을 선택합니다. 그런 다음 확인을 선택하여 로그 대상에 대한 변경 사항을 적용합니다.
2. 외부 syslog 서버 * 또는 * 관리 노드 및 외부 syslog 서버 * 를 감사 정보 대상으로 선택한 경우 추가 경고가 나타납니다. 경고 텍스트를 검토합니다.

> 외부 syslog 서버가 테스트 StorageGRID 메시지를 수신할 수 있는지 확인해야 합니다.

1. [확인]을 선택하여 감사 정보의 대상을 변경할지 확인합니다.

   감사 구성이 성공적으로 저장되었음을 알리는 녹색 배너가 나타납니다.

   새 로그가 선택한 대상으로 전송됩니다. 기존 로그는 현재 위치에 남아 있습니다.

관련 정보

감사 메시지 개요

감사 메시지 및 로그 대상을 구성합니다

시스템 감사 메시지

오브젝트 스토리지 감사 메시지

관리 감사 메시지입니다

클라이언트가 감사 메시지를 읽습니다

StorageGRID 관리

SNMP 모니터링을 사용합니다

SNMP(Simple Network Management Protocol)를 사용하여 StorageGRID를 모니터링하려면 StorageGRID에 포함된 SNMP 에이전트를 구성해야 합니다.

- SNMP 에이전트를 구성합니다
- SNMP 에이전트를 업데이트합니다

제공합니다

각 StorageGRID 노드는 MIB(Management Information Base)를 제공하는 SNMP 에이전트 또는 데몬을 실행합니다. StorageGRID MIB에는 알림 및 알람에 대한 테이블 및 알림 정의가 포함되어 있습니다. MIB에는 각 노드의 플랫폼 및 모델 번호와 같은 시스템 설명 정보도 포함되어 있습니다. 각 StorageGRID 노드는 MIB-II 객체의 하위 세트도 지원합니다.

처음에는 모든 노드에서 SNMP가 사용되지 않습니다. SNMP 에이전트를 구성할 때 모든 StorageGRID 노드는 동일한 구성을 받습니다.

StorageGRID SNMP 에이전트는 세 가지 버전의 SNMP 프로토콜을 모두 지원합니다. 쿼리에 대한 읽기 전용 MIB 액세스를 제공하며 관리 시스템에 두 가지 유형의 이벤트 기반 알림을 보낼 수 있습니다.

- * 트랩 * 은 관리 시스템에서 확인이 필요하지 않은 SNMP 에이전트가 보낸 알림입니다. 트랩은 알림이 트리거되는 등 StorageGRID 내에 발생한 사항을 관리 시스템에 알리는 역할을 합니다.

  트랩은 SNMP의 세 가지 버전에서 모두 지원됩니다.

- * 알림 * 은 트랩과 유사하지만 관리 시스템에서 확인을 요구합니다. SNMP 에이전트가 일정 시간 내에 승인을 받지 못하면 승인을 받거나 최대 재시도 값에 도달할 때까지 알림을 다시 보냅니다.

  SNMPv2c 및 SNMPv3에서 알림이 지원됩니다.

다음과 같은 경우 트랩 및 알림 알림이 전송됩니다.

- 기본 또는 사용자 지정 알림은 모든 심각도 수준에서 트리거됩니다. 경고에 대한 SNMP 알림을 표시하지 않으려면 경고에 대한 무음을 구성해야 합니다. 경고 알림은 선호하는 송신자가 되도록 구성된 관리 노드에서 보냅니다.

  각 알림은 알림의 심각도 수준, activeMinorAlert, activeMajorAlert 및 activeCriticalAlert 중 하나를 기준으로 세 가지 트랩 유형 중 하나에 매핑됩니다. 이러한 트랩을 트리거할 수 있는 경고에 대한 설명은 을 참조하십시오 경고 참조.

- 특정 알람(기존 시스템)은 지정된 심각도 수준 이상에서 트리거됩니다.

  ⓘ 모든 알람 또는 알람 심각도에 대해 SNMP 알림이 전송되지 않습니다.

SNMP 버전 지원

이 표에는 각 SNMP 버전에서 지원되는 항목에 대한 자세한 요약 정보가 나와 있습니다.

	SNMPv1	**SNMPv2c**입니다	**SNMPv3**
쿼리	읽기 전용 MIB 쿼리	읽기 전용 MIB 쿼리	읽기 전용 MIB 쿼리
쿼리 인증	커뮤니티 문자열	커뮤니티 문자열	USM(사용자 기반 보안 모델) 사용자
알림	트랩만	함정 및 통보	함정 및 통보
알림 인증	각 트랩 대상에 대한 기본 트랩 커뮤니티 또는 사용자 지정 커뮤니티 문자열입니다	각 트랩 대상에 대한 기본 트랩 커뮤니티 또는 사용자 지정 커뮤니티 문자열입니다	각 트랩 대상에 대한 USM 사용자입니다

제한 사항

- StorageGRID는 읽기 전용 MIB 액세스를 지원합니다. 읽기-쓰기 액세스는 지원되지 않습니다.
- 그리드의 모든 노드는 동일한 구성을 받습니다.
- SNMPv3: StorageGRID는 전송 지원 모드(TSM)를 지원하지 않습니다.
- SNMPv3: 지원되는 유일한 인증 프로토콜은 SHA(HMAC-SHA-96)입니다.
- SNMPv3: 지원되는 유일한 개인 정보 보호 프로토콜은 AES입니다.

MIB에 액세스합니다

StorageGRID 노드의 다음 위치에서 MIB 정의 파일에 액세스할 수 있습니다.

'/usr/share/snmp/mibs/netapp-StorageGrid-mib.txt'

관련 정보

- 경고 참조
- 알람 기준(레거시 시스템)
- SNMP 알림을 생성하는 알람(레거시 시스템)
- 알림 메시지를 해제합니다

SNMP 에이전트를 구성합니다

읽기 전용 MIB 액세스 및 알림에 타사 SNMP 관리 시스템을 사용하려는 경우 StorageGRID SNMP 에이전트를 구성할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.

이 작업에 대해

StorageGRID SNMP 에이전트는 세 가지 버전의 SNMP 프로토콜을 모두 지원합니다. 하나 이상의 버전에 대해 에이전트를 구성할 수 있습니다.

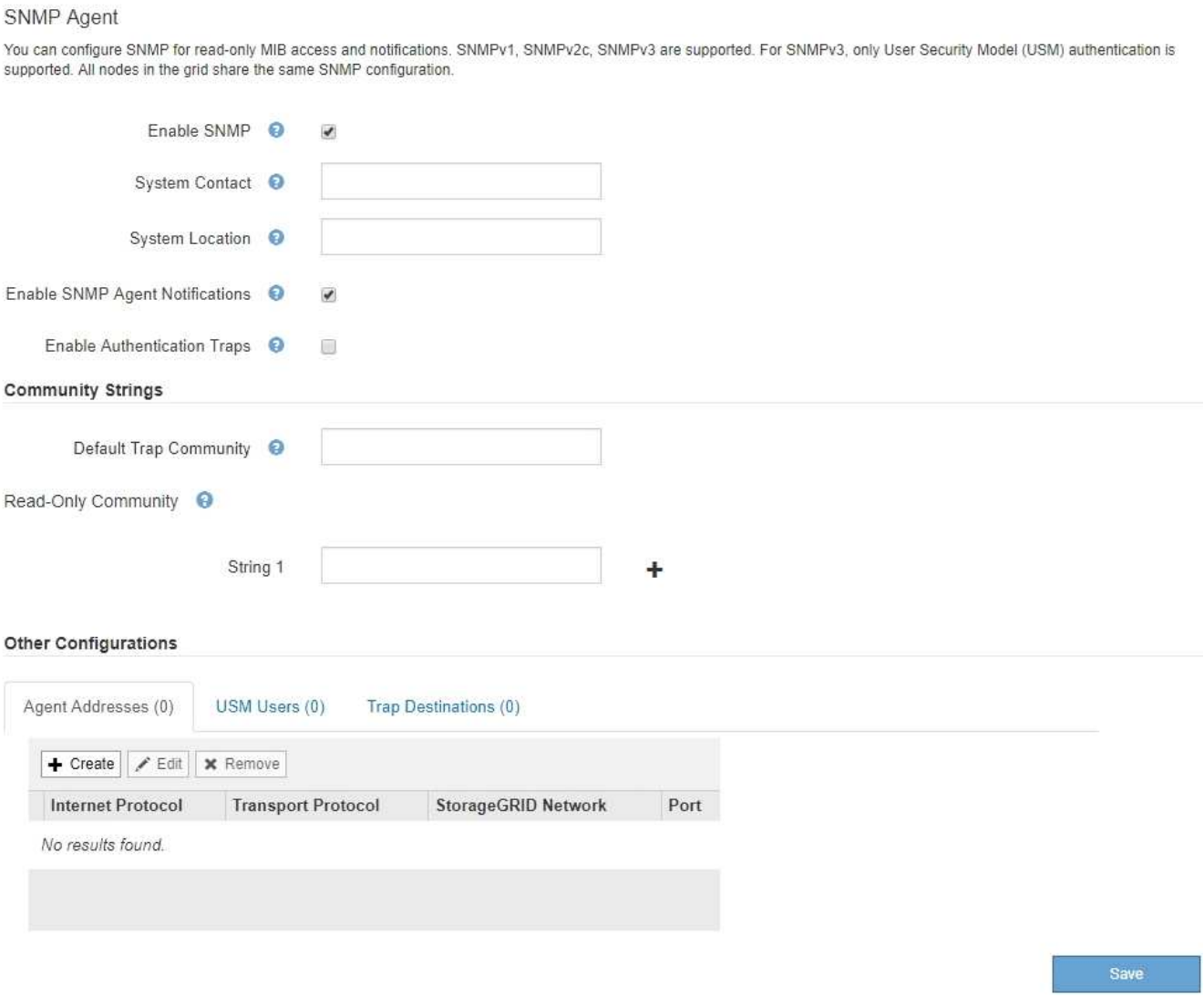
단계

1. 구성 * > * 모니터링 * > * SNMP 에이전트 * 를 선택합니다.

   SNMP Agent 페이지가 나타납니다.

2. 모든 그리드 노드에서 SNMP 에이전트를 활성화하려면 * SNMP * 활성화 확인란을 선택합니다.

   SNMP 에이전트를 구성하는 필드가 나타납니다.



3. 시스템 연락처 * 필드에 sysContact에 대한 SNMP 메시지에 StorageGRID를 제공할 값을 입력합니다.

   일반적으로 시스템 담당자는 이메일 주소입니다. 제공하는 값은 StorageGRID 시스템의 모든 노드에 적용됩니다. 시스템 연락처 * 는 최대 255자까지 입력할 수 있습니다.

4. 시스템 위치 * 필드에 sysLocation에 대한 SNMP 메시지에 StorageGRID를 제공할 값을 입력합니다.

   시스템 위치는 StorageGRID 시스템의 위치를 식별하는 데 유용한 모든 정보가 될 수 있습니다. 예를 들어 시설의 주소를 사용할 수 있습니다. 제공하는 값은 StorageGRID 시스템의 모든 노드에 적용됩니다. * 시스템 위치 * 는 최대 255자까지 입력할 수 있습니다.

5. StorageGRID SNMP 에이전트가 트랩을 전송하고 알림을 보내도록 하려면 * SNMP 에이전트 알림 사용 * 확인란을 선택한 상태로 유지합니다.

   이 확인란의 선택을 취소하면 SNMP 에이전트는 읽기 전용 MIB 액세스를 지원하지만 SNMP 알림은 보내지 않습니다.

6. StorageGRID SNMP 에이전트가 잘못 인증된 프로토콜 메시지를 수신할 경우 인증 트랩을 보내도록 하려면 * 인증 트랩 사용 * 확인란을 선택합니다.

7. SNMPv1 또는 SNMPv2c를 사용하는 경우 커뮤니티 문자열 섹션을 완료합니다.

이 섹션의 필드는 SNMPv1 또는 SNMPv2c에서 커뮤니티 기반 인증에 사용됩니다. 이 필드는 SNMPv3에는 적용되지 않습니다.

a. 기본 트랩 커뮤니티 * 필드에 트랩 대상에 사용할 기본 커뮤니티 문자열을 입력합니다(선택 사항).

   필요한 경우 다른 커뮤니티 문자열을 제공할 수 있습니다(""사용자 지정") 특정 트랩 대상을 정의합니다.

   - 기본 트랩 커뮤니티 * 는 최대 32자이고 공백 문자를 포함할 수 없습니다.

b. 읽기 전용 커뮤니티*의 경우 IPv4 및 IPv6 에이전트 주소에서 읽기 전용 MIB 액세스를 허용하도록 하나 이상의 커뮤니티 문자열을 입력합니다. 더하기 기호를 클릭합니다 + 여러 문자열을 추가합니다.

   관리 시스템이 StorageGRID MIB를 쿼리하면 커뮤니티 문자열을 보냅니다. 커뮤니티 문자열이 여기에 지정된 값 중 하나와 일치하면 SNMP 에이전트는 관리 시스템에 응답을 보냅니다.

   각 커뮤니티 문자열은 최대 32자이고 공백 문자를 포함할 수 없습니다. 최대 5개의 문자열이 허용됩니다.

   > StorageGRID 시스템의 보안을 보장하기 위해 커뮤니티 문자열로 ""public""을 사용하지 마십시오. 커뮤니티 문자열을 입력하지 않으면 SNMP 에이전트는 StorageGRID 시스템의 그리드 ID를 커뮤니티 문자열로 사용합니다.

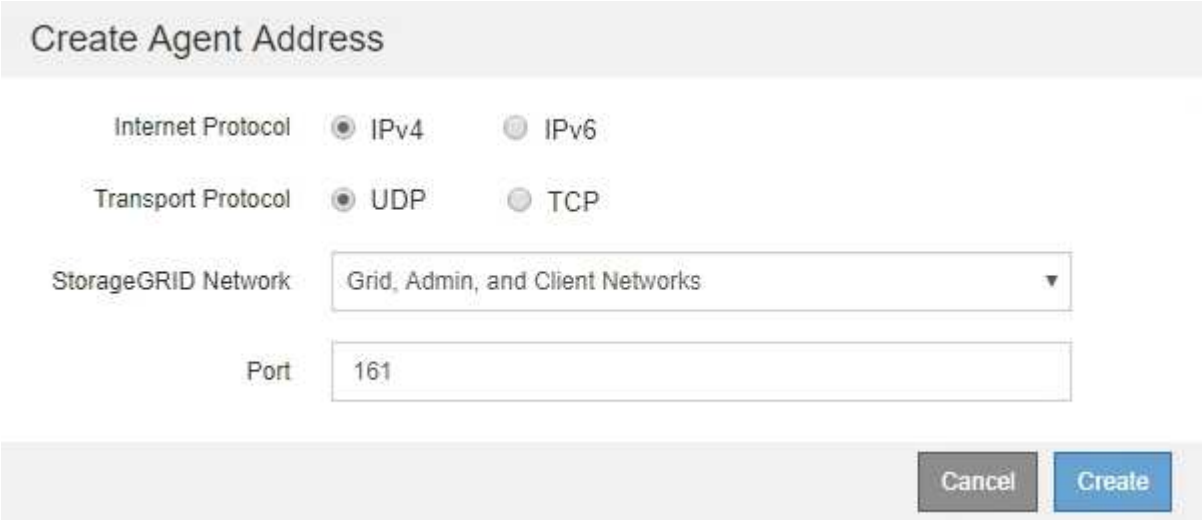
8. 필요에 따라 기타 구성 섹션에서 상담원 주소 탭을 선택합니다.

   이 탭을 사용하여 하나 이상의 ""수신 주소""를 지정하십시오. SNMP 에이전트가 쿼리를 받을 수 있는 StorageGRID 주소입니다. 각 에이전트 주소에는 인터넷 프로토콜, 전송 프로토콜, StorageGRID 네트워크 및 포트(옵션)가 포함됩니다.

   에이전트 주소를 구성하지 않으면 기본 수신 주소는 모든 StorageGRID 네트워크에서 UDP 포트 161입니다.

   a. Create * 를 클릭합니다.

      상담원 주소 작성 대화 상자가 나타납니다.



   b. 인터넷 프로토콜 * 의 경우 이 주소가 IPv4와 IPv6을 사용할지 여부를 선택합니다.

      기본적으로 SNMP는 IPv4를 사용합니다.

c. 전송 프로토콜 * 의 경우 이 주소가 UDP 또는 TCP를 사용할지 여부를 선택합니다.

기본적으로 SNMP는 UDP를 사용합니다.

d. StorageGRID 네트워크 * 필드에서 쿼리를 수신할 StorageGRID 네트워크를 선택합니다.

- 그리드, 관리자 및 클라이언트 네트워크:StorageGRID는 세 네트워크 모두에서 SNMP 쿼리를 수신해야 합니다.
- 그리드 네트워크
- 관리자 네트워크
- 클라이언트 네트워크

> StorageGRID와 클라이언트 통신이 안전하게 유지되도록 하려면 클라이언트 네트워크에 대한 에이전트 주소를 만들지 않아야 합니다.

e. Port* 필드에 SNMP 에이전트가 수신 대기해야 하는 포트 번호를 입력합니다(선택 사항).

SNMP 에이전트의 기본 UDP 포트는 161이지만 사용하지 않는 포트 번호를 입력할 수 있습니다.

> SNMP 에이전트를 저장하면 StorageGRID에서 내부 방화벽에 있는 에이전트 주소 포트를 자동으로 엽니다. 모든 외부 방화벽이 이러한 포트에 대한 액세스를 허용하는지 확인해야 합니다.

f. Create * 를 클릭합니다.

상담원 주소가 생성되어 테이블에 추가됩니다.

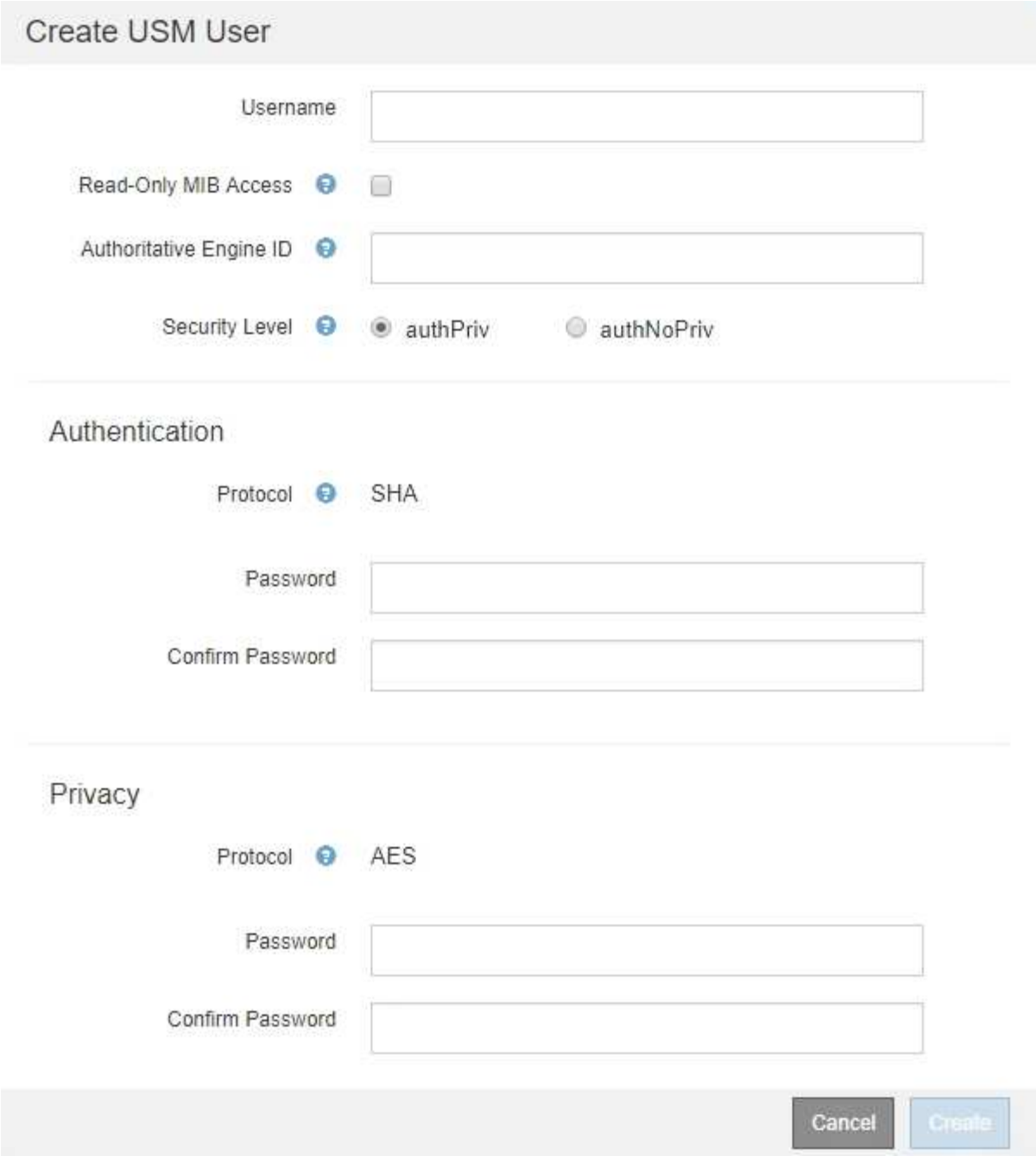
9. SNMPv3을 사용하는 경우 기타 구성 섹션에서 USM 사용자 탭을 선택합니다.

이 탭을 사용하여 MIB를 쿼리하거나 트랩 및 알림을 받을 권한이 있는 USM 사용자를 정의합니다.

> SNMPv1 또는 SNMPv2c만 사용하는 경우에는 이 단계가 적용되지 않습니다.

a. Create * 를 클릭합니다.

USM 사용자 생성 대화 상자가 나타납니다.



b. 이 USM 사용자에 대한 고유한 * 사용자 이름 * 을 입력합니다.

   사용자 이름은 최대 32자이며 공백 문자를 포함할 수 없습니다. 사용자가 생성된 후에는 사용자 이름을 변경할 수 없습니다.

c. 이 사용자가 MIB에 대한 읽기 전용 액세스를 가지고 있어야 하는 경우 * 읽기 전용 MIB 액세스 * 확인란을 선택합니다.

   읽기 전용 MIB 액세스 * 를 선택하면 * Authoritative Engine ID * 필드가 비활성화됩니다.

   > 읽기 전용 MIB 액세스가 있는 USM 사용자는 엔진 ID를 가질 수 없습니다.

d. 이 사용자를 알림 대상에서 사용할 경우 이 사용자에 대한 * Authoritative Engine ID * 를 입력합니다.

> SNMPv3 알림 대상에는 엔진 ID가 있는 사용자가 있어야 합니다. SNMPv3 트랩 대상에는 엔진 ID를 가진 사용자가 있을 수 없습니다.

신뢰할 수 있는 엔진 ID는 5바이트에서 32바이트까지 16진수로 지정할 수 있습니다.

e. USM 사용자의 보안 수준을 선택합니다.

- * auth암호화 *: 이 사용자는 인증 및 개인 정보 보호(암호화)와 통신합니다. 인증 프로토콜 및 암호와 개인 정보 보호 프로토콜 및 암호를 지정해야 합니다.
- * authNo암호화 *: 이 사용자는 개인 정보 보호 없이 인증과 통신합니다(암호화 없음). 인증 프로토콜과 암호를 지정해야 합니다.

f. 이 사용자가 인증에 사용할 암호를 입력하고 확인합니다.

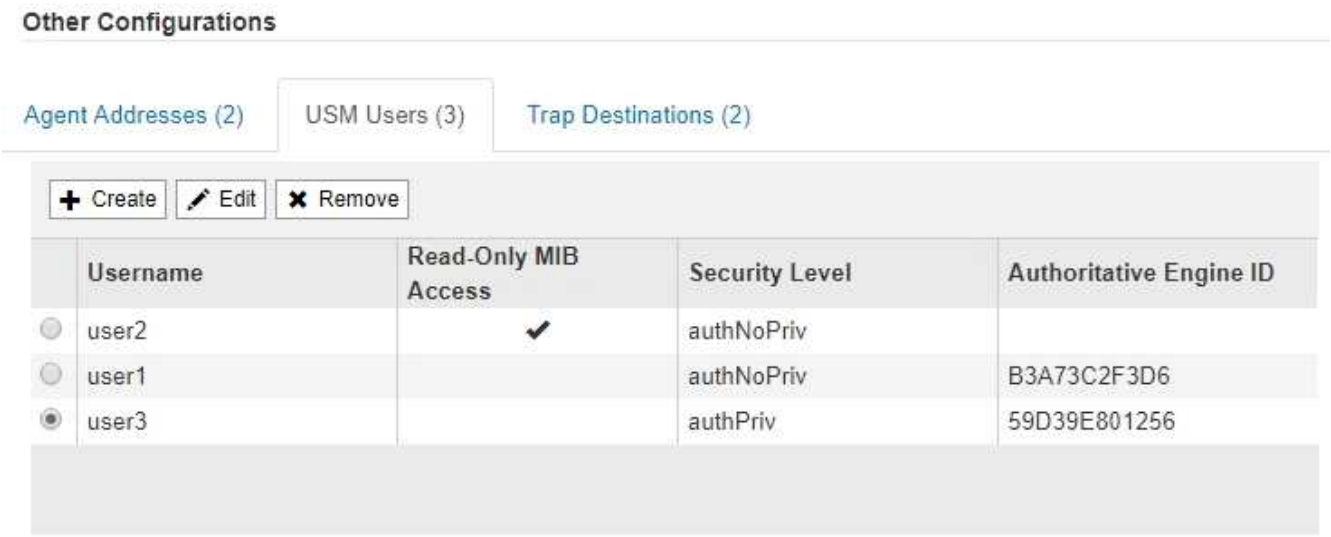
> 지원되는 유일한 인증 프로토콜은 SHA(HMAC-SHA-96)입니다.

g. auth암호화 * 를 선택한 경우 이 사용자가 개인 정보 보호에 사용할 암호를 입력하고 확인합니다.

> 지원되는 개인 정보 보호 프로토콜은 AES 뿐입니다.

h. Create * 를 클릭합니다.

USM 사용자가 생성되어 테이블에 추가됩니다.

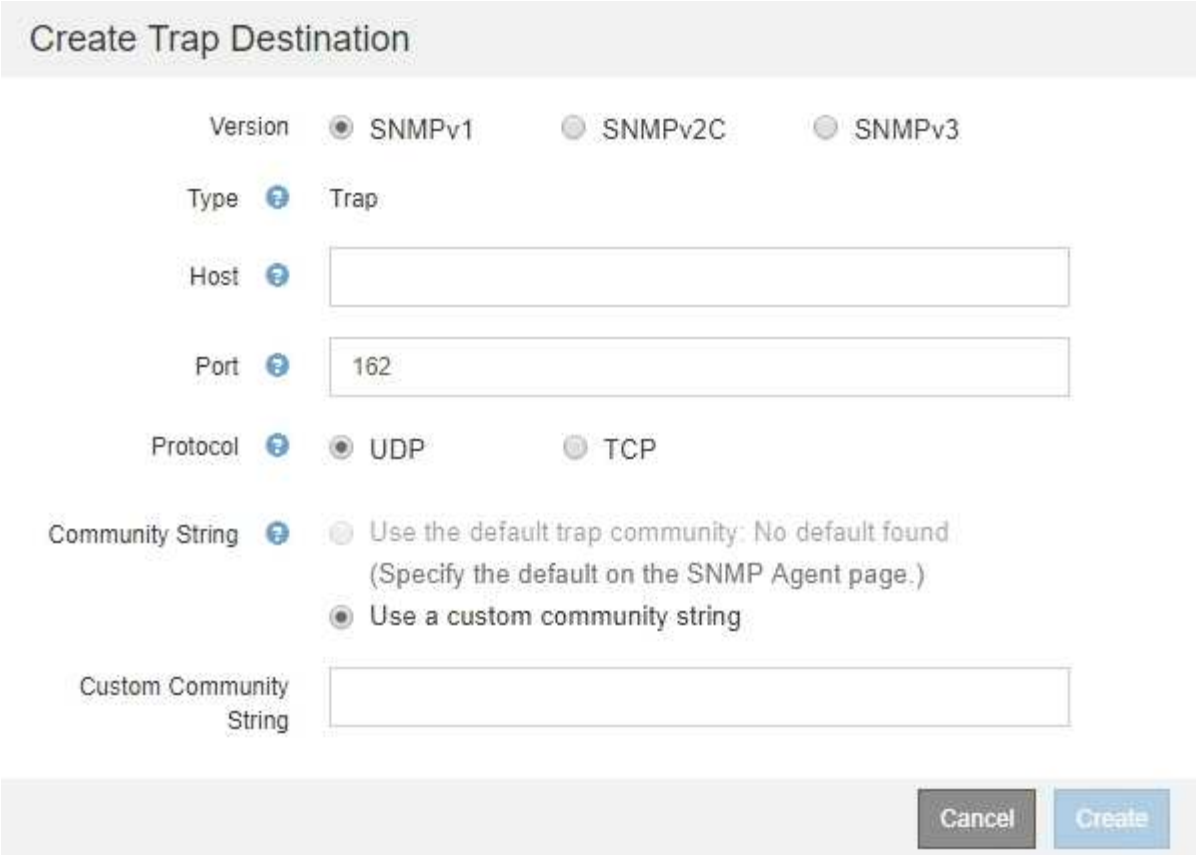


10. 기타 구성 섹션에서 트랩 대상 탭을 선택합니다.

트랩 대상 탭에서는 StorageGRID 트랩 또는 알림 알림에 대한 하나 이상의 대상을 정의할 수 있습니다. SNMP 에이전트를 활성화하고 * 저장 * 을 클릭하면 StorageGRID가 정의된 각 대상으로 알림을 보내기 시작합니다. 알림 및 알람이 트리거되면 알림이 전송됩니다. 지원되는 MIB-II 엔티티에 대해서도 표준 알림이 전송됩니다(예: ifdown 및 coldstart).

a. Create * 를 클릭합니다.

Create Trap Destination 대화상자가 나타납니다.



b. 버전 * 필드에서 이 알림에 사용할 SNMP 버전을 선택합니다.

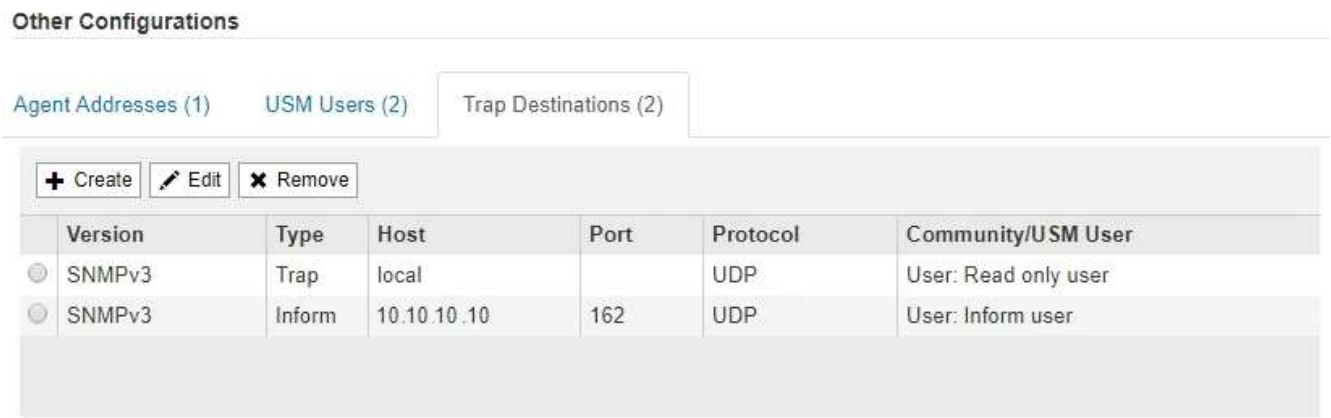
c. 선택한 버전에 따라 양식을 작성합니다

버전	이 정보를 지정하십시오
SNMPv1	• 참고: * SNMPv1의 경우 SNMP 에이전트는 트랩만 보낼 수 있습니다. 알림이 지원되지 않습니다. i. Host * 필드에 트랩을 수신할 IPv4 또는 IPv6 주소(또는 FQDN)를 입력합니다. ii. 포트*의 경우 다른 값을 사용해야 하는 경우가 아니면 기본값(162)을 사용합니다. (162는 SNMP 트랩의 표준 포트입니다.) iii. 프로토콜 * 의 경우 기본값(UDP)을 사용합니다. TCP도 지원됩니다. (UDP는 표준 SNMP 트랩 프로토콜입니다.) iv. SNMP 에이전트 페이지에 지정된 경우 기본 트랩 커뮤니티를 사용하거나 이 트랩 대상에 대한 사용자 지정 커뮤니티 문자열을 입력합니다. 사용자 지정 커뮤니티 문자열은 최대 32자이며 공백을 포함할 수 없습니다.

버전	이 정보를 지정하십시오
SNMPv2c입니다	i. 대상이 트랩에 사용되는지 아니면 정보를 제공할 것인지 선택합니다. ii. Host * 필드에 트랩을 수신할 IPv4 또는 IPv6 주소(또는 FQDN)를 입력합니다. iii. 포트*의 경우 다른 값을 사용해야 하는 경우가 아니면 기본값(162)을 사용합니다. (162는 SNMP 트랩의 표준 포트입니다.) iv. 프로토콜 * 의 경우 기본값(UDP)을 사용합니다. TCP도 지원됩니다. (UDP는 표준 SNMP 트랩 프로토콜입니다.) v. SNMP 에이전트 페이지에 지정된 경우 기본 트랩 커뮤니티를 사용하거나 이 트랩 대상에 대한 사용자 지정 커뮤니티 문자열을 입력합니다. 사용자 지정 커뮤니티 문자열은 최대 32자이며 공백을 포함할 수 없습니다.
SNMPv3	i. 대상이 트랩에 사용되는지 아니면 정보를 제공할 것인지 선택합니다. ii. Host * 필드에 트랩을 수신할 IPv4 또는 IPv6 주소(또는 FQDN)를 입력합니다. iii. 포트*의 경우 다른 값을 사용해야 하는 경우가 아니면 기본값(162)을 사용합니다. (162는 SNMP 트랩의 표준 포트입니다.) iv. 프로토콜 * 의 경우 기본값(UDP)을 사용합니다. TCP도 지원됩니다. (UDP는 표준 SNMP 트랩 프로토콜입니다.) v. 인증에 사용할 USM 사용자를 선택합니다. ◦ Trap * 을 선택하면 권한 있는 엔진 ID가 없는 USM 사용자만 표시됩니다. ◦ 알림 * 을 선택하면 권한 있는 엔진 ID가 있는 USM 사용자만 표시됩니다.

d. Create * 를 클릭합니다.

   트랩 대상이 생성되어 테이블에 추가됩니다.



11. SNMP 에이전트 구성을 완료하면 * Save * 를 클릭합니다

    새 SNMP 에이전트 구성이 활성화됩니다.

관련 정보

알림 메시지를 해제합니다

SNMP 에이전트를 업데이트합니다

SNMP 알림을 비활성화하거나 커뮤니티 문자열을 업데이트하거나 에이전트 주소, USM 사용자 및 트랩 대상을 추가 또는 제거할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있어야 합니다.

이 작업에 대해

를 업데이트할 때마다 SNMP 에이전트 구성각 탭에서 변경한 내용을 적용하려면 SNMP 에이전트 페이지 하단의 * Save * 를 클릭해야 합니다.

단계

1. 구성 * > * 모니터링 * > * SNMP 에이전트 * 를 선택합니다.

   SNMP Agent 페이지가 나타납니다.

2. 모든 그리드 노드에서 SNMP 에이전트를 비활성화하려면 * SNMP * 활성화 확인란의 선택을 취소하고 * 저장 * 을 클릭합니다.

   SNMP 에이전트는 모든 그리드 노드에 대해 비활성화됩니다. 나중에 에이전트를 다시 활성화하면 이전의 모든 SNMP 구성 설정이 유지됩니다.

3. 선택적으로 * 시스템 연락처 * 및 * 시스템 위치 * 에 대해 입력한 값을 업데이트합니다.
4. StorageGRID SNMP 에이전트가 트랩을 전송하고 알림을 보내지 않도록 하려면 선택적으로 * SNMP 에이전트 알림 사용 * 확인란을 선택 취소합니다.

   이 확인란의 선택을 취소하면 SNMP 에이전트는 읽기 전용 MIB 액세스를 지원하지만 SNMP 알림은 보내지 않습니다.

5. StorageGRID SNMP 에이전트가 부적절하게 인증된 프로토콜 메시지를 받을 때 더 이상 인증 트랩을 보내지 않도록 하려면 [인증 트랩 사용] * 확인란을 선택 취소합니다.
6. SNMPv1 또는 SNMPv2c를 사용하는 경우 선택적으로 커뮤니티 문자열 섹션을 업데이트합니다.

   이 섹션의 필드는 SNMPv1 또는 SNMPv2c에서 커뮤니티 기반 인증에 사용됩니다. 이 필드는 SNMPv3에는 적용되지 않습니다.

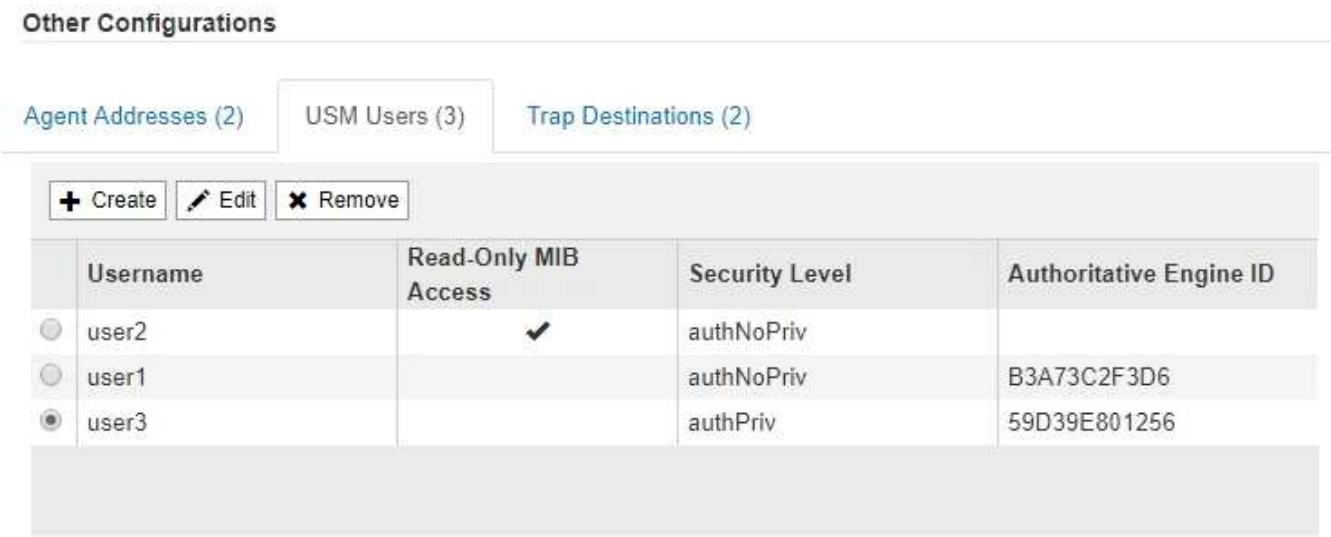
   > 기본 커뮤니티 문자열을 제거하려면 먼저 모든 트랩 대상에 사용자 지정 커뮤니티 문자열을 사용해야 합니다.

7. 상담원 주소를 업데이트하려면 기타 구성 섹션에서 상담원 주소 탭을 선택합니다.

   이 탭을 사용하여 하나 이상의 ""수신 주소""를 지정하십시오. SNMP 에이전트가 쿼리를 받을 수 있는 StorageGRID 주소입니다. 각 에이전트 주소에는 인터넷 프로토콜, 전송 프로토콜, StorageGRID 네트워크 및 포트가 포함됩니다.

   a. 상담원 주소를 추가하려면 * 생성 * 을 클릭합니다. 그런 다음 SNMP 에이전트 구성 지침에 있는 에이전트 주소 단계를 참조하십시오.
   b. 상담원 주소를 편집하려면 주소의 라디오 버튼을 선택하고 * 편집 * 을 클릭합니다. 그런 다음 SNMP 에이전트 구성 지침에 있는 에이전트 주소 단계를 참조하십시오.
   c. 상담원 주소를 제거하려면 주소의 라디오 버튼을 선택하고 * 제거 * 를 클릭합니다. 그런 다음 * 확인 * 을 클릭하여 이 주소를 제거할 것인지 확인합니다.
   d. 변경 사항을 커밋하려면 SNMP 에이전트 페이지 맨 아래에 있는 * Save * 를 클릭합니다.

8. USM 사용자를 업데이트하려면 기타 구성 섹션에서 USM 사용자 탭을 선택합니다.



이 탭을 사용하여 MIB를 쿼리하거나 트랩 및 알림을 받을 권한이 있는 USM 사용자를 정의합니다.

a. USM 사용자를 추가하려면 * Create * 를 클릭합니다. 그런 다음 SNMP 에이전트를 구성하는 지침은 USM 사용자에 대한 단계를 참조하십시오.

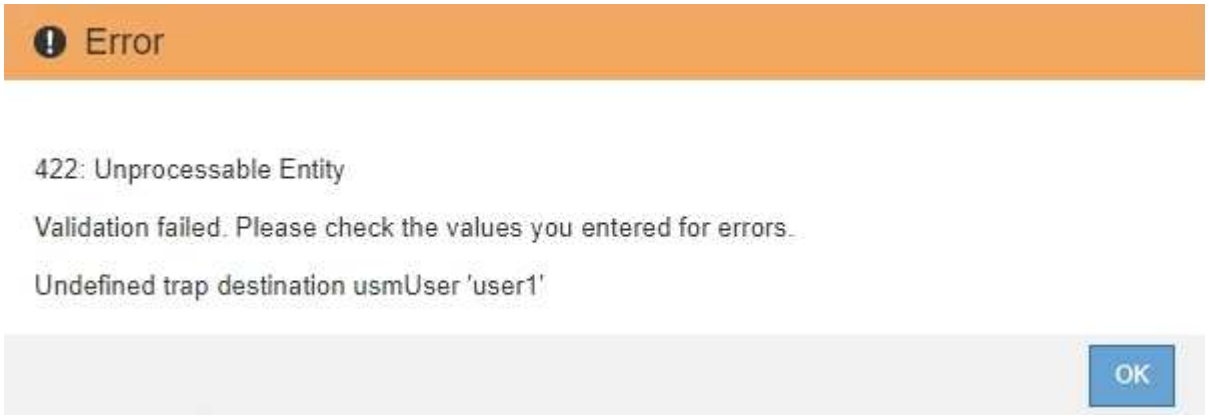
b. USM 사용자를 편집하려면 해당 사용자의 라디오 버튼을 선택하고 * Edit * 를 클릭합니다. 그런 다음 SNMP 에이전트를 구성하는 지침은 USM 사용자에 대한 단계를 참조하십시오.

   기존 USM 사용자의 사용자 이름은 변경할 수 없습니다. 사용자 이름을 변경해야 하는 경우 사용자를 제거하고 새 사용자 이름을 만들어야 합니다.

   > 사용자의 신뢰할 수 있는 엔진 ID를 추가 또는 제거하고 해당 사용자가 현재 대상에 대해 선택된 경우 단계에 설명된 대로 대상을 편집하거나 제거해야 합니다 SNMP 트랩 대상입니다. 그렇지 않으면 SNMP 에이전트 구성을 저장할 때 유효성 검사 오류가 발생합니다.

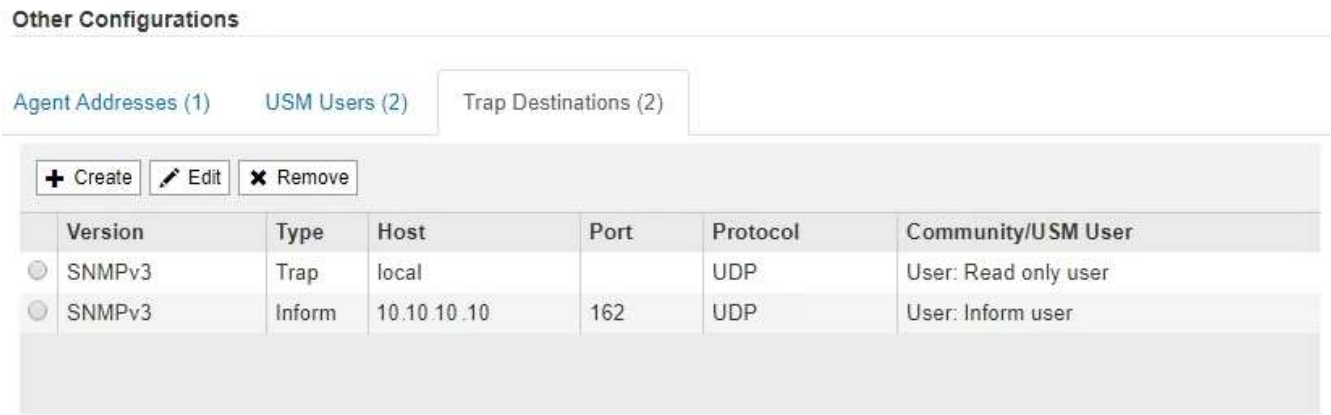
c. USM 사용자를 제거하려면 해당 사용자의 라디오 버튼을 선택하고 * Remove * 를 클릭합니다. 그런 다음 * 확인 * 을 클릭하여 이 사용자를 제거할 것인지 확인합니다.

   > 제거한 사용자가 현재 트랩 대상에 대해 선택된 경우 단계에 설명된 대로 대상을 편집하거나 제거해야 합니다 SNMP 트랩 대상입니다. 그렇지 않으면 SNMP 에이전트 구성을 저장할 때 유효성 검사 오류가 발생합니다.



a. 변경 사항을 커밋하려면 SNMP 에이전트 페이지 맨 아래에 있는 * Save * 를 클릭합니다.

9. 트랩 대상을 업데이트하려면 기타 구성 섹션에서 트랩 대상 탭을 선택합니다.



트랩 대상 탭에서는 StorageGRID 트랩 또는 알림 알림에 대한 하나 이상의 대상을 정의할 수 있습니다. SNMP 에이전트를 활성화하고 * 저장 * 을 클릭하면 StorageGRID가 정의된 각 대상으로 알림을 보내기 시작합니다. 알림 및 알람이 트리거되면 알림이 전송됩니다. 지원되는 MIB-II 엔티티에 대해서도 표준 알림이 전송됩니다(예: ifdown 및 coldstart).

a. 트랩 대상을 추가하려면 * Create * 를 클릭합니다. 그런 다음 SNMP 에이전트 구성 지침에 있는 트랩 대상 단계를 참조하십시오.

b. 트랩 대상을 편집하려면 사용자의 라디오 버튼을 선택하고 * Edit * 를 클릭합니다. 그런 다음 SNMP 에이전트 구성 지침에 있는 트랩 대상 단계를 참조하십시오.

c. 트랩 대상을 제거하려면 대상의 라디오 단추를 선택하고 * 제거 * 를 클릭합니다. 그런 다음 * 확인 * 을 클릭하여 이 대상을 제거할 것인지 확인합니다.

d. 변경 사항을 커밋하려면 SNMP 에이전트 페이지 맨 아래에 있는 * Save * 를 클릭합니다.

10. SNMP 에이전트 구성을 업데이트했으면 * Save * 를 클릭합니다.

추가 **StorageGRID** 데이터를 수집합니다

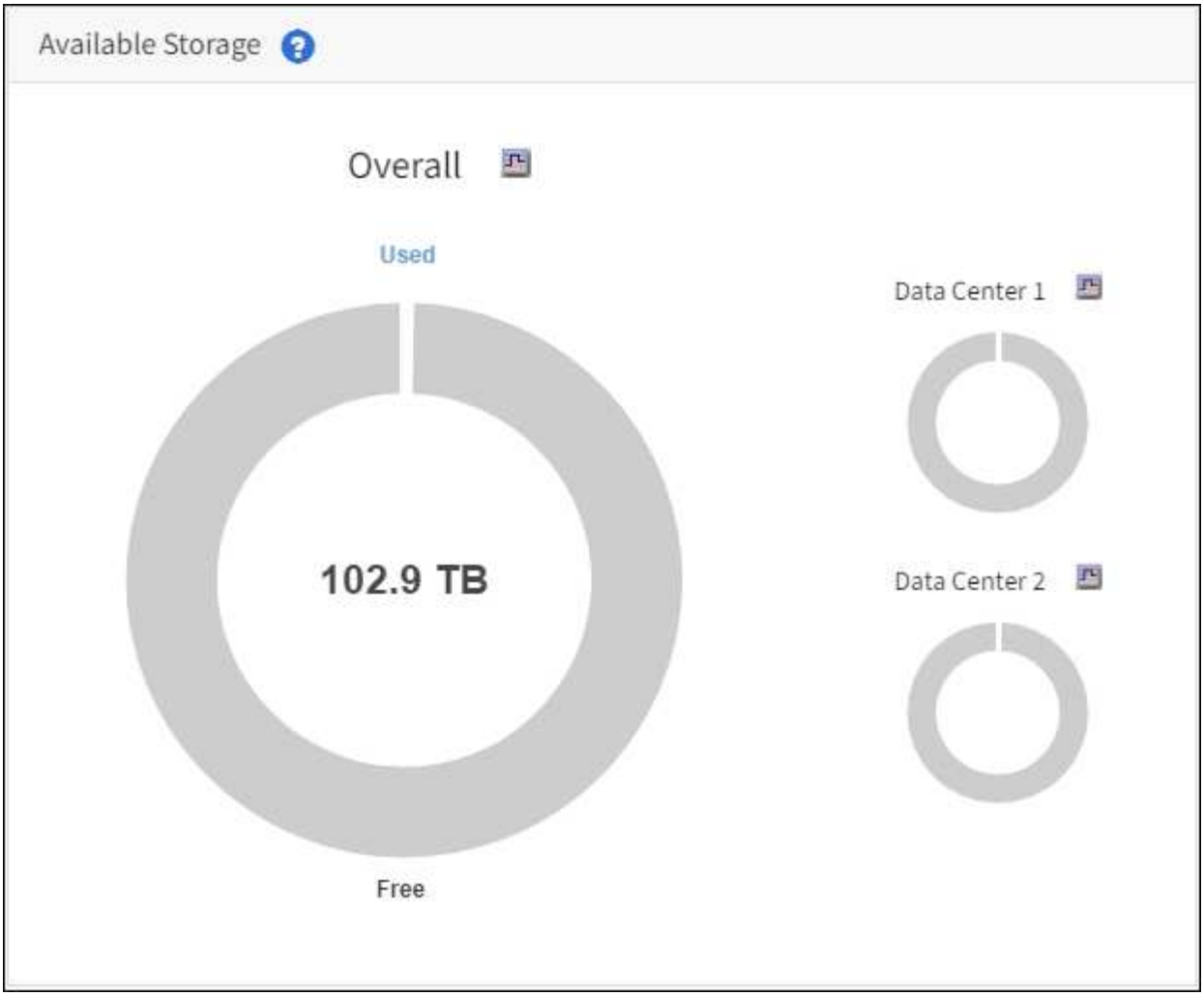
차트와 그래프를 사용합니다

차트와 보고서를 사용하여 StorageGRID 시스템의 상태를 모니터링하고 문제를 해결할 수 있습니다. Grid Manager에서 사용할 수 있는 차트 및 보고서 유형에는 도넛형 차트(대시보드에만 해당), 그래프 및 텍스트 보고서가 있습니다.

차트 종류

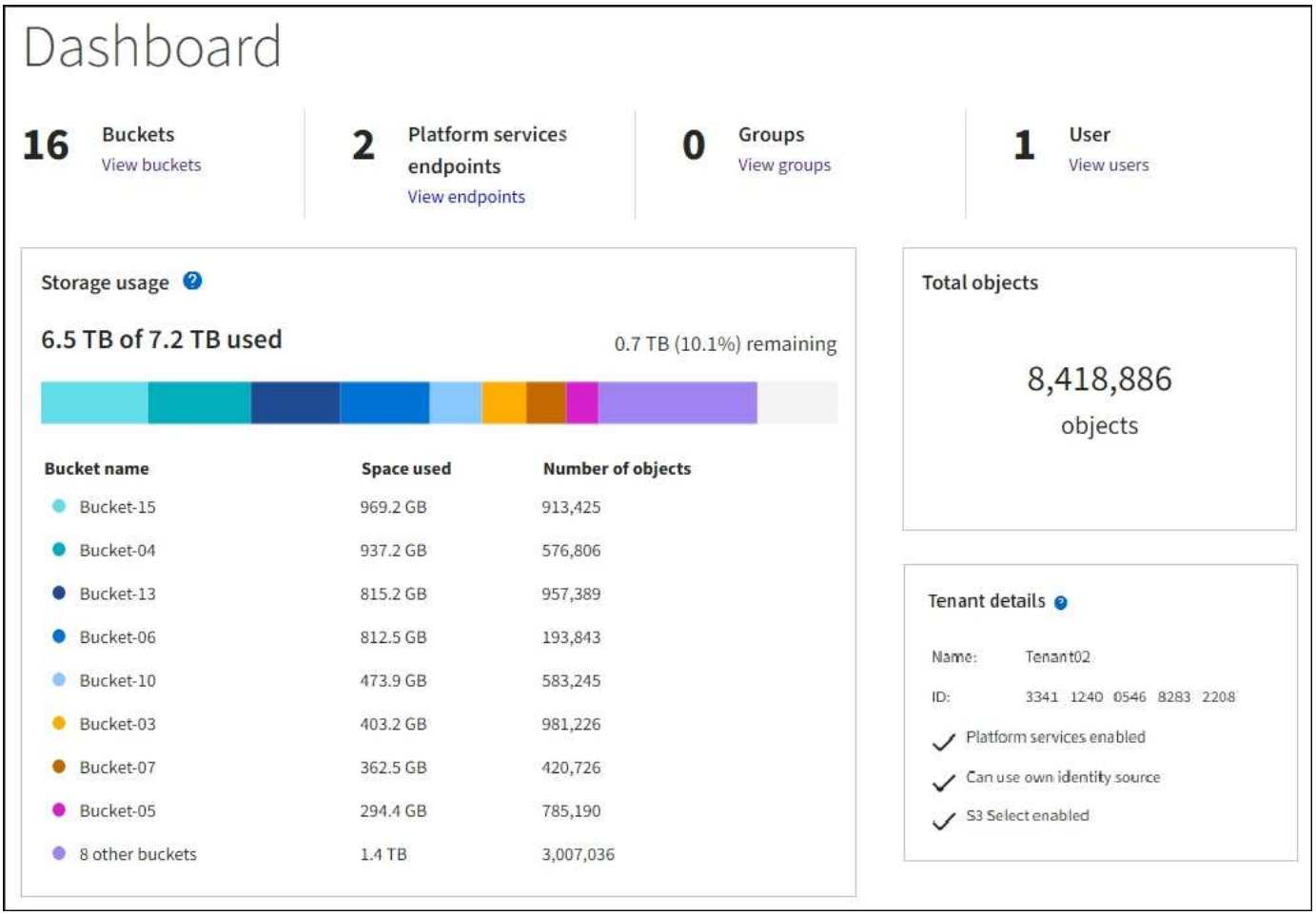
차트와 그래프에는 특정 StorageGRID 메트릭 및 특성의 값이 요약되어 있습니다.

Grid Manager 대시보드에는 그리드 및 각 사이트에 사용할 수 있는 스토리지를 요약하는 도넛형 차트가 포함되어 있습니다.



테넌트 관리자 대시보드의 스토리지 사용 패널에 다음이 표시됩니다.

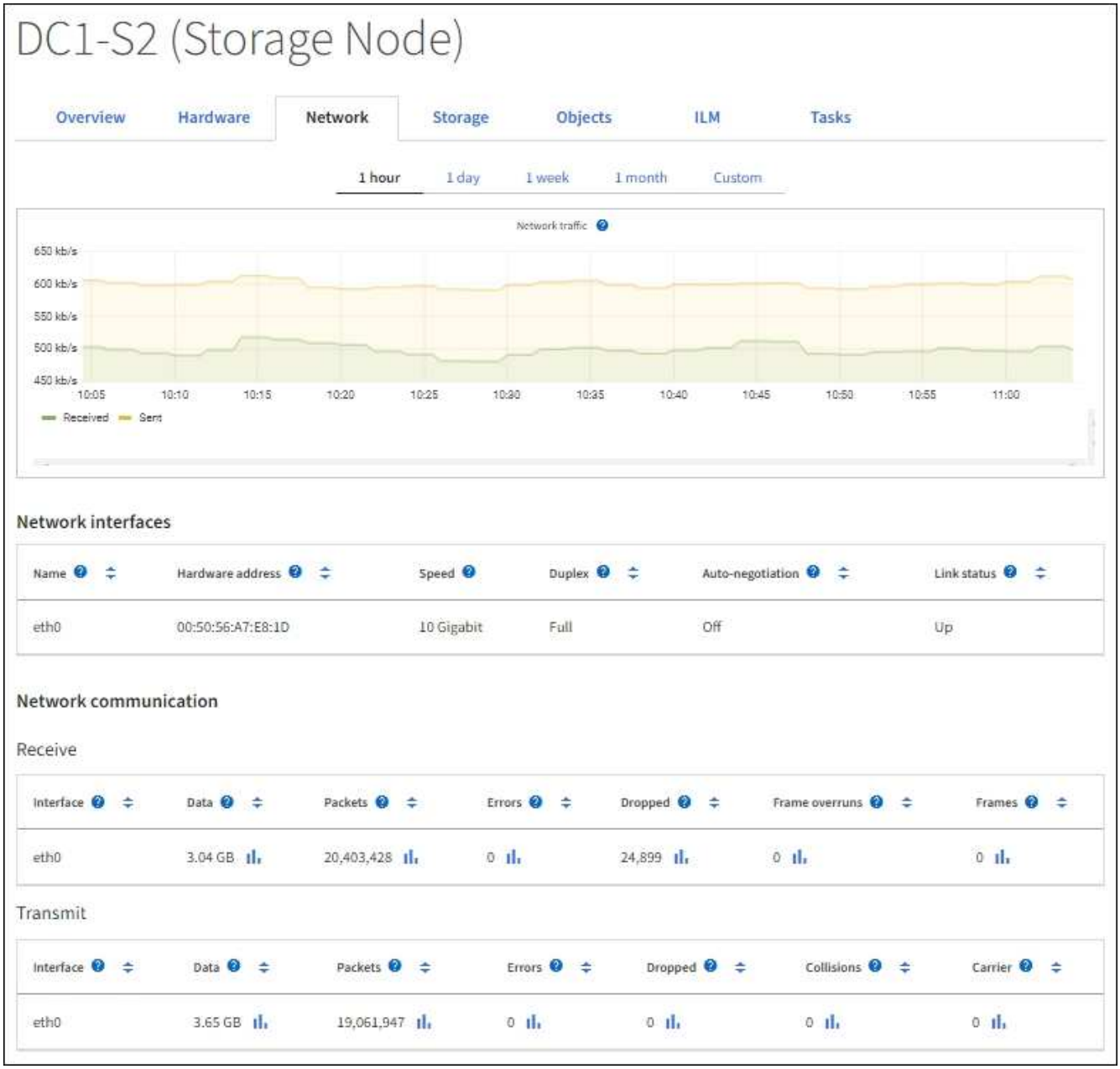
- 테넌트를 위해 가장 큰 버킷(S3) 또는 컨테이너(Swift)의 목록입니다
- 가장 큰 버킷 또는 컨테이너의 상대적 크기를 나타내는 막대 차트
- 사용된 총 공간 및 할당량이 설정된 경우 남은 공간의 양과 백분율이 표시됩니다



또한 노드 페이지 및 * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지에서 StorageGRID 메트릭 및 속성이 시간에 따라 변경되는 방식을 보여 주는 그래프입니다.

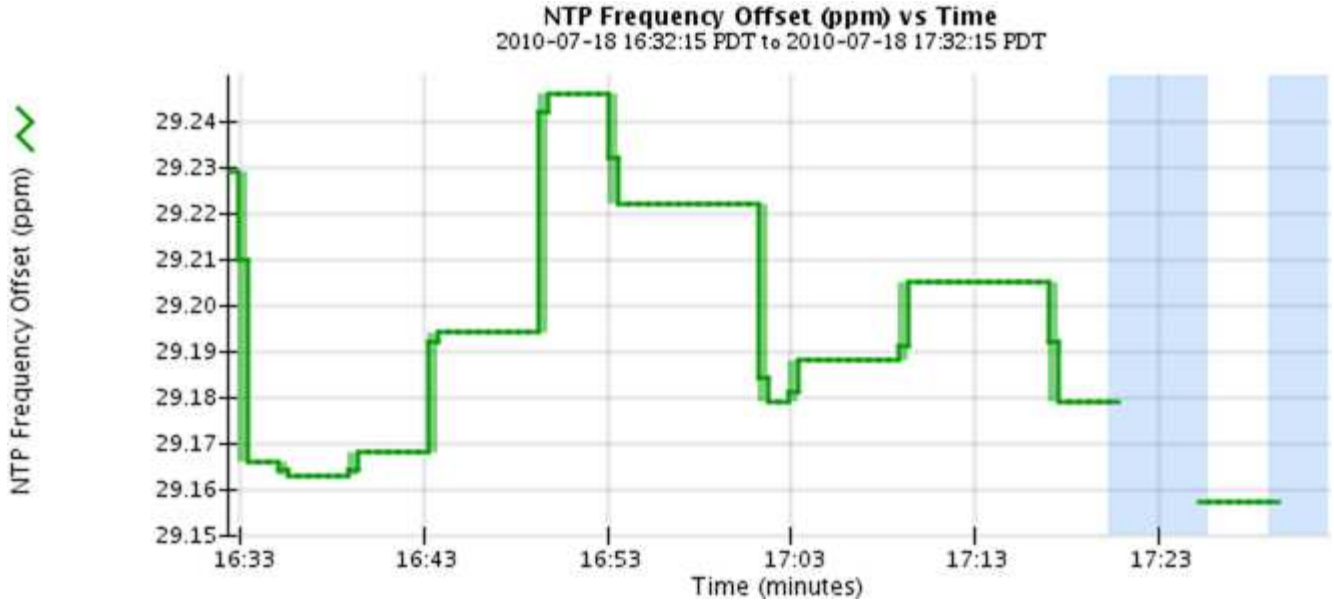
그래프에는 네 가지 유형이 있습니다.

- * Grafana 차트 *: 노드 페이지에 표시된 Grafana 차트는 시간의 경과에 따라 Prometheus 메트릭의 값을 플롯하는 데 사용됩니다. 예를 들어, 스토리지 노드의 * 노드 * > * 네트워크 * 탭에는 네트워크 트래픽에 대한 Grafana 차트가 들어 있습니다.

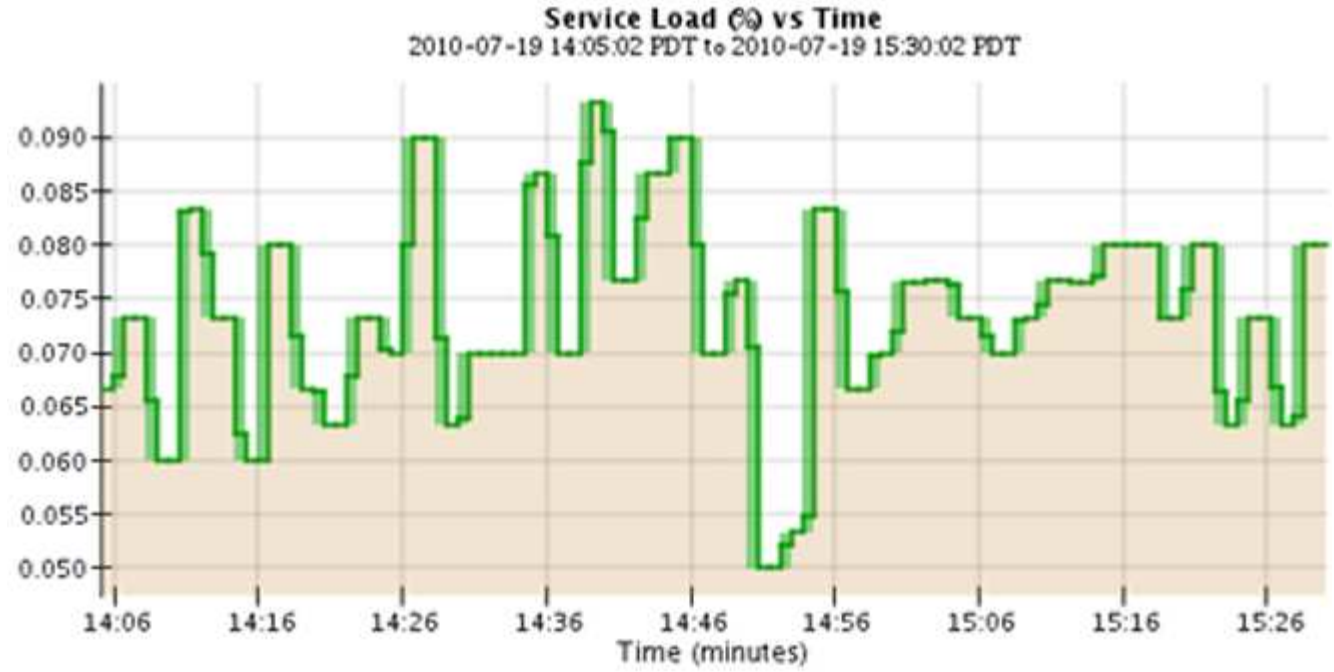


Grafana 차트는 * 지원 * > * 도구 * > * 메트릭 * 페이지에서 사용할 수 있는 사전 구성된 대시보드에도 포함되어 있습니다.

- * 선 그래프 *: 노드 페이지 및 * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지에서 사용할 수 있습니다(차트 아이콘 선택) 데이터 값 다음에), 선 그래프는 단위 값이 있는 StorageGRID 속성 값(예: NTP 주파수 오프셋, ppm)을 플롯하는 데 사용됩니다. 값의 변경 내용은 시간 경과에 따른 정규 데이터 간격(빈)으로 표시됩니다.

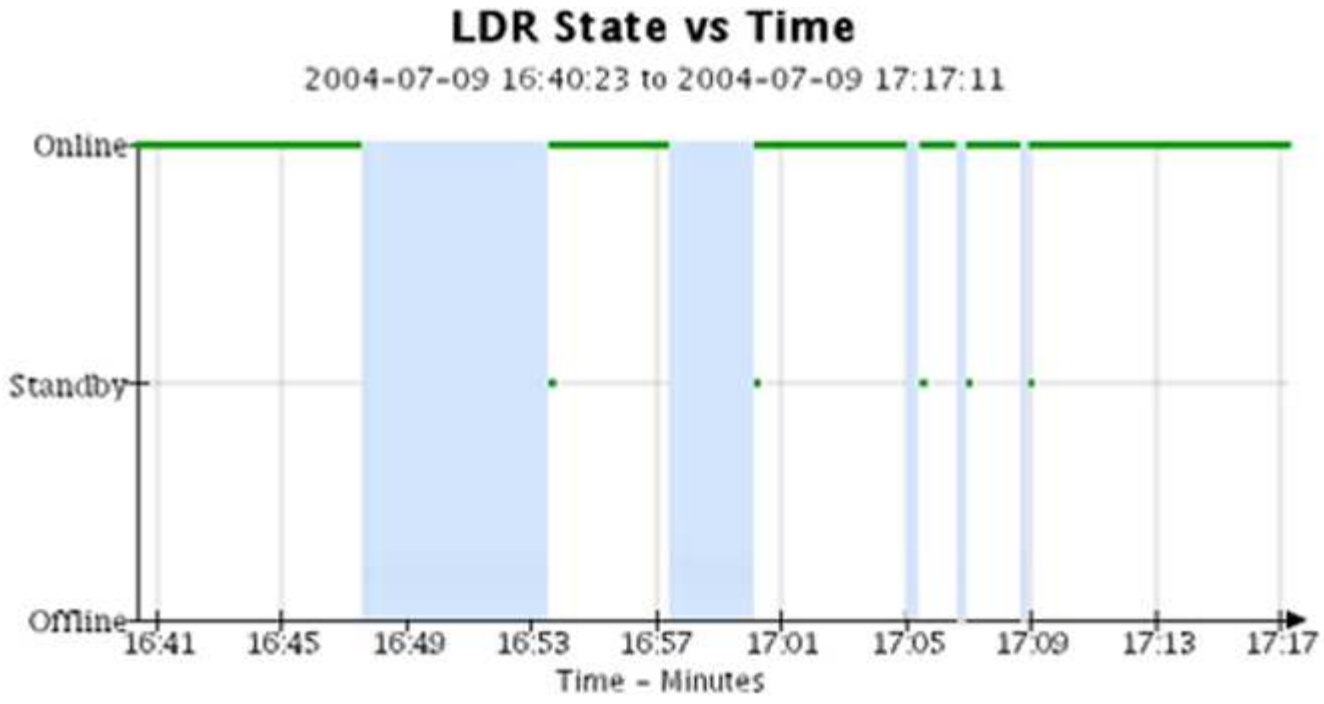


- * 영역 그래프 *: 노드 페이지 및 * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지에서 사용할 수 있습니다(차트 아이콘을 선택합니다) 데이터 값 다음에) 영역 그래프는 개체 수 또는 서비스 하중 값과 같은 용적 특성 수량을 플롯하는 데 사용됩니다. 영역 그래프는 선 그래프와 비슷하지만 선 아래에 밝은 갈색 음영을 포함합니다. 값의 변경 내용은 시간 경과에 따른 정규 데이터 간격(빈)으로 표시됩니다.



- 일부 그래프는 다른 유형의 차트 아이콘으로 표시됩니다 다른 형식을 사용합니다.

- * 상태 그래프 *: * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지에서 사용할 수 있습니다(차트 아이콘 선택) 데이터 값 다음에) 상태 그래프는 온라인, 대기 또는 오프라인일 수 있는 서비스 상태와 같은 고유한 상태를 나타내는 속성 값을 플롯하는 데 사용됩니다. 상태 그래프는 선 그래프와 유사하지만 전이는 불연속입니다. 즉, 값이 한 상태 값에서 다른 상태 값으로 이동합니다.



관련 정보

노드 페이지를 봅니다

그리드 토폴로지 트리를 봅니다

지원 메트릭을 검토합니다

차트 범례

차트를 그리는 데 사용되는 선과 색상은 특정한 의미를 갖습니다.

샘플	의미
	보고된 속성 값은 진한 녹색 선으로 표시됩니다.
	어두운 녹색 선 주변의 밝은 녹색 음영은 해당 시간 범위의 실제 값이 가변적이며 빠른 플로팅의 경우 "비닝"이 되었음을 나타냅니다. 어두운 선은 가중 평균을 나타냅니다. 녹색으로 표시된 범위는 입력 용지함 내의 최대 및 최소 값을 나타냅니다. 밝은 갈색 음영은 체적 데이터를 나타내는 영역 그래프에 사용됩니다.
	빈 영역(표시된 데이터 없음)은 속성 값을 사용할 수 없음을 나타냅니다. 배경은 속성을 보고하는 서비스의 상태에 따라 파란색, 회색 또는 회색과 파란색이 혼합되어 있을 수 있습니다.
	연한 파란색 음영은 해당 시점의 속성 값 중 일부 또는 모두가 결정되지 않았음을 나타냅니다. 서비스가 알 수 없는 상태이기 때문에 특성이 값을 보고하지 않았습니다.
	회색 음영은 속성을 보고하는 서비스가 관리상 중단되었기 때문에 해당 시점의 일부 또는 모든 속성 값을 알 수 없음을 나타냅니다.
	회색 음영과 파란색 음영이 혼합되어 있으면 해당 시점의 일부 속성 값이 불확정(서비스가 알 수 없는 상태였기 때문)인 반면, 속성을 보고하는 서비스가 관리상 다운되었기 때문에 다른 속성 값은 알 수 없습니다.

차트와 그래프를 표시합니다

노드 페이지에는 스토리지 용량 및 처리량과 같은 속성을 모니터링하기 위해 정기적으로 액세스해야 하는 차트와 그래프가 포함되어 있습니다. 경우에 따라, 특히 기술 지원 작업을 할 때 * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지를 사용하여 추가 차트에 액세스할 수 있습니다.

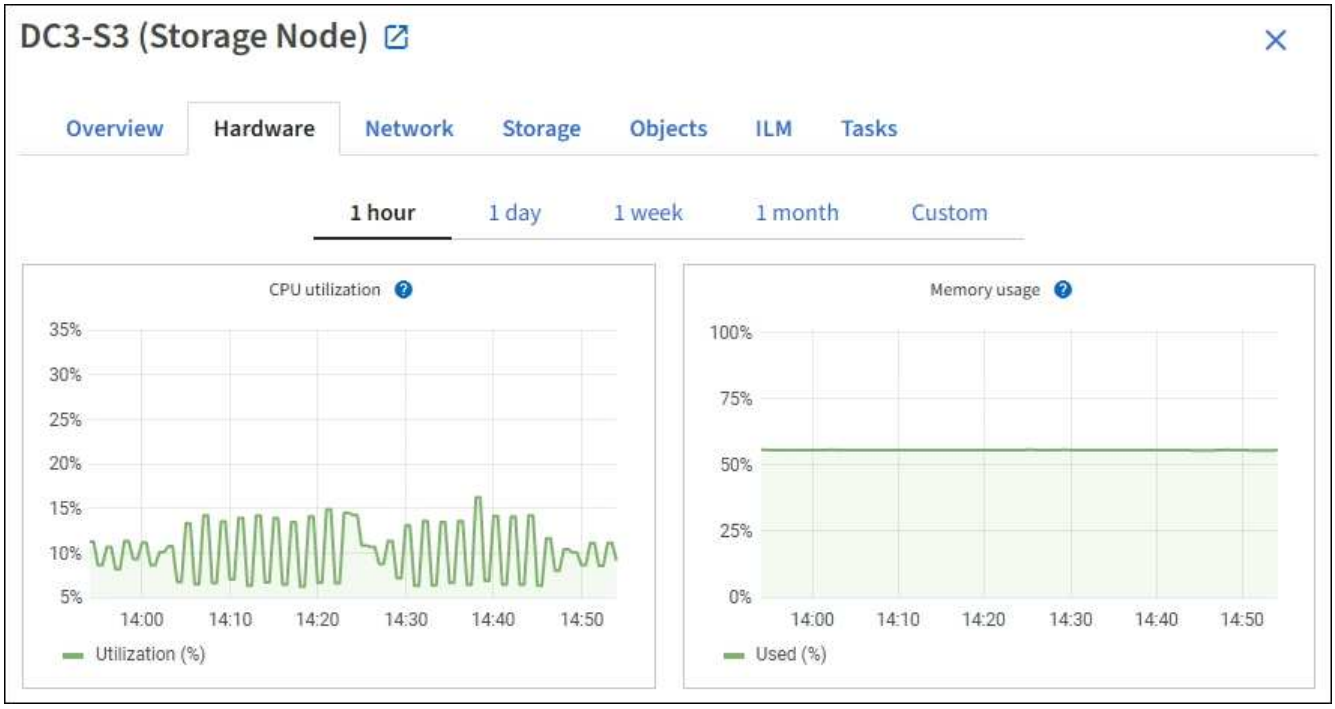
필요한 것

를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

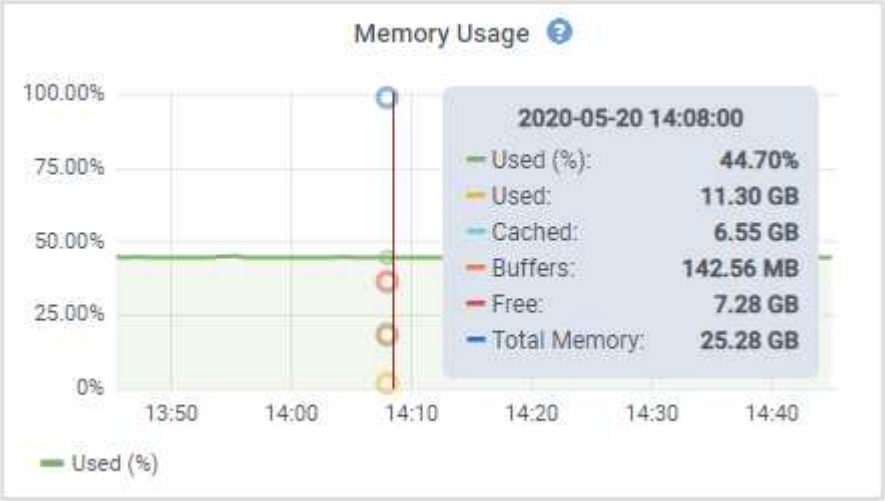
단계

1. 노드 * 를 선택합니다. 그런 다음 노드, 사이트 또는 전체 그리드를 선택합니다.
2. 정보를 보려는 탭을 선택합니다.

일부 탭에는 한 개 이상의 Grafana 차트가 포함되어 있으며, 이 차트는 시간의 경과에 따른 Prometheus 메트릭의 값을 플롯하는 데 사용됩니다. 예를 들어, 노드의 * 노드 * > * 하드웨어 * 탭에는 두 개의 Grafana 차트가 들어 있습니다.



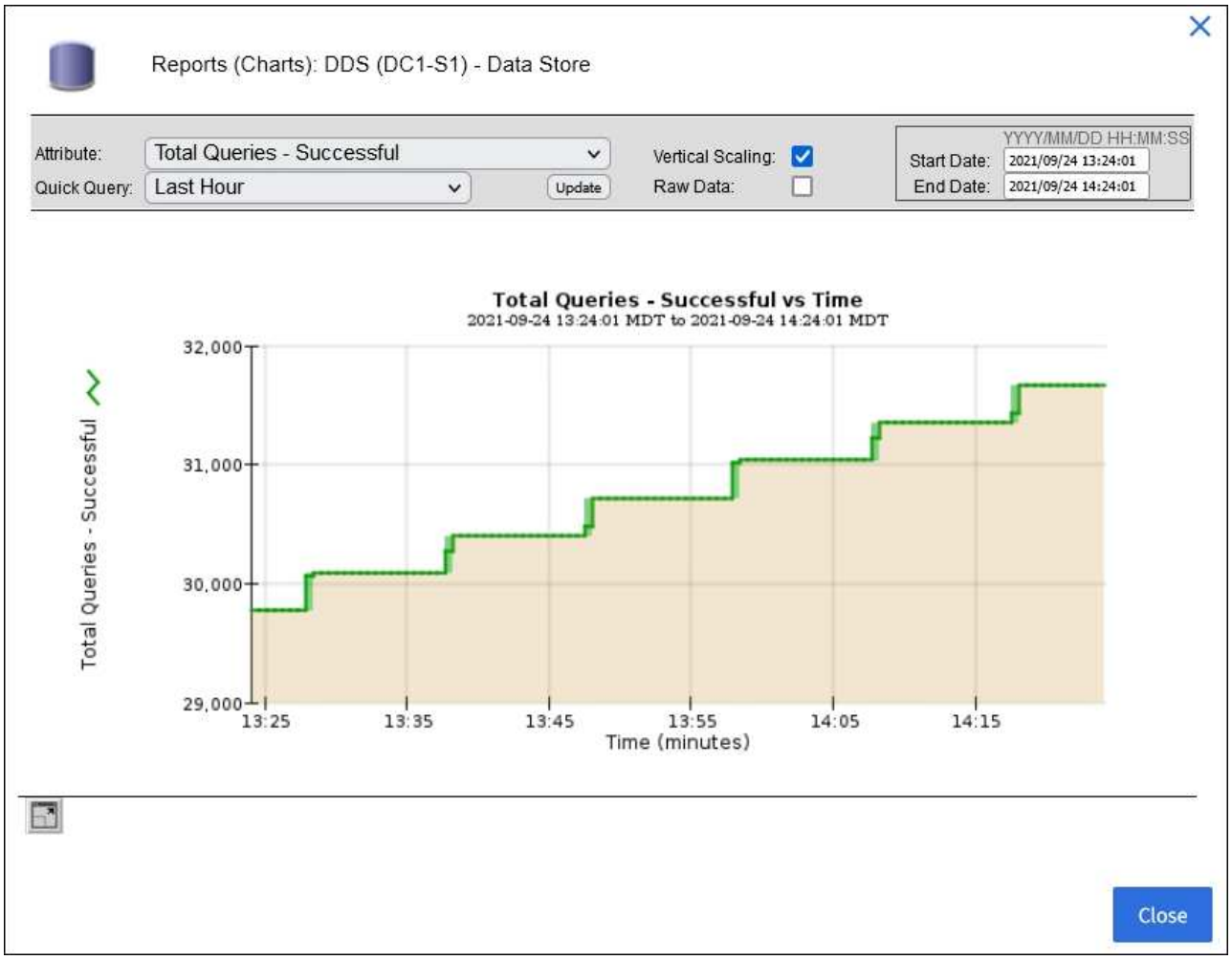
3. 원하는 경우 차트 위에 커서를 올려 놓으면 특정 시점에 대한 보다 자세한 값을 볼 수 있습니다.

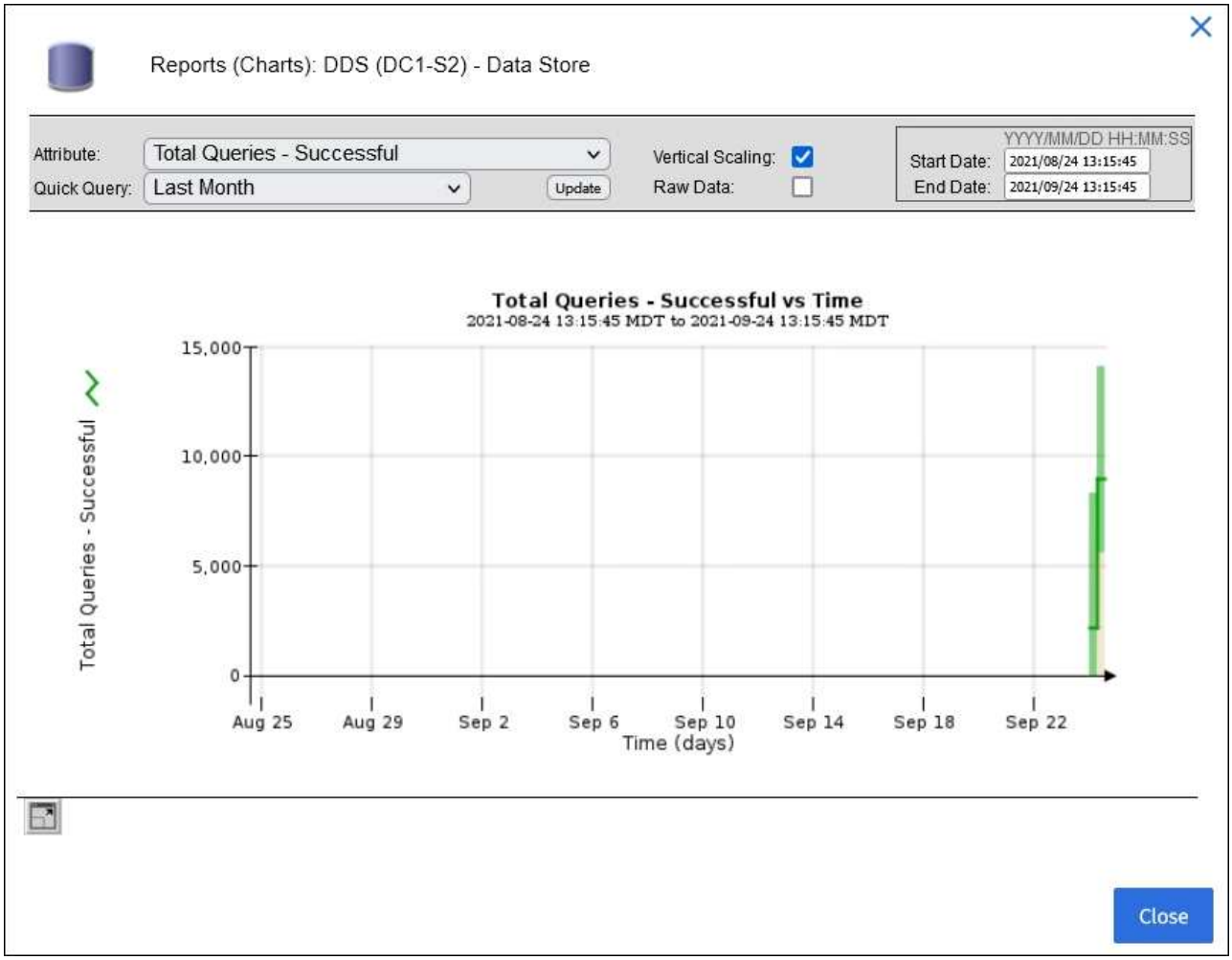


4. 필요에 따라 특정 특성 또는 메트릭에 대한 차트를 표시할 수 있습니다. 노드 페이지의 표에서 차트 아이콘을 선택합니다 속성 이름의 오른쪽에 있습니다.

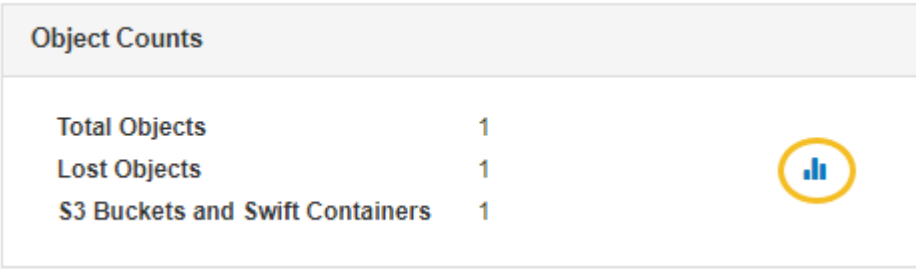
> 일부 메트릭 및 특성에는 차트를 사용할 수 없습니다.

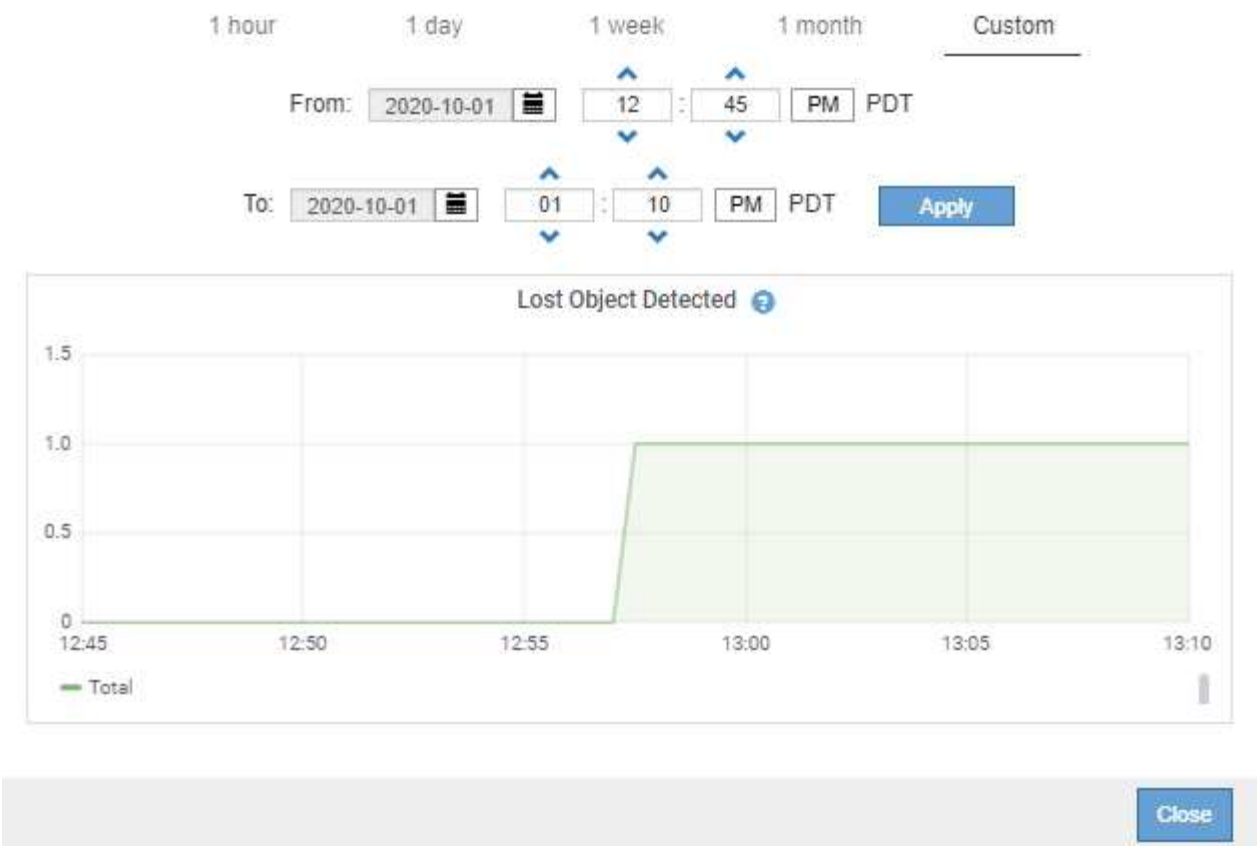
- 예 1 *: 스토리지 노드의 객체 탭에서 차트 아이콘을 선택할 수 있습니다 스토리지 노드에 대한 성공한 메타데이터 저장소 쿼리의 총 수를 확인합니다.


Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close

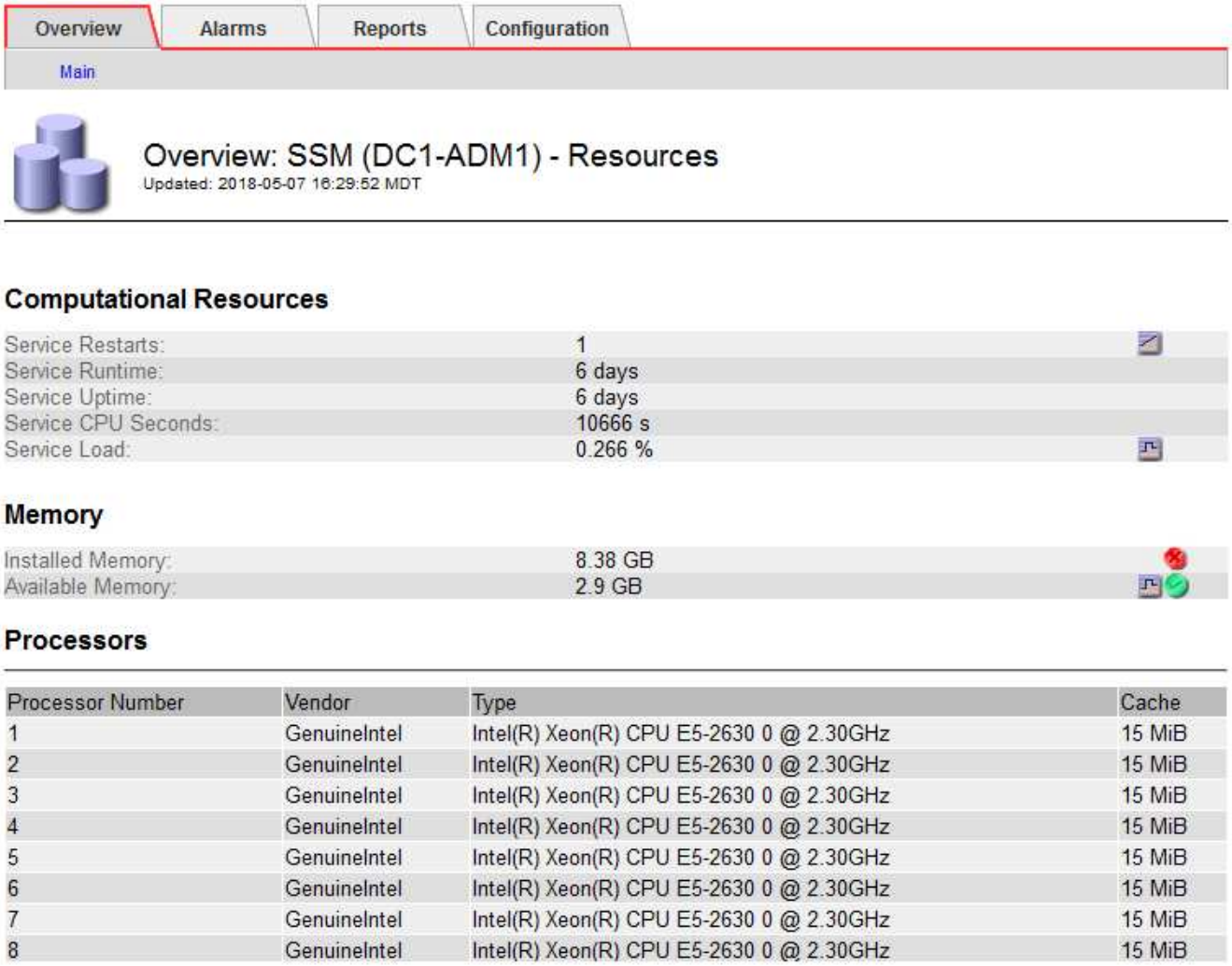


- 예 2 *: 스토리지 노드의 객체 탭에서 차트 아이콘을 선택할 수 있습니다 Grafana 로 시간 경과에 따라 감지된 오브젝트의 수에 대한 그래프 를 봅니다.





5. 노드 페이지에 표시되지 않은 속성에 대한 차트를 표시하려면 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
6. grid node_ * > * *component* 또는 *service* * > * Overview * > * Main * 을 선택합니다.



7. 차트 아이콘을 선택합니다 속성 옆에 있습니다.

   그러면 * Reports * > * Charts * 페이지가 자동으로 변경됩니다. 차트는 지난 하루 동안의 특성 데이터를 표시합니다.

차트를 생성합니다

차트는 특성 데이터 값의 그래픽 표현을 표시합니다. 데이터 센터 사이트, 그리드 노드, 구성 요소 또는 서비스에 대해 보고할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. grid node_ * > * *component* 또는 *service* * > * Reports * > * Charts * 를 선택합니다.
3. 특성 * 드롭다운 목록에서 보고할 특성을 선택합니다.
4. Y축을 0에서 시작하려면 * 수직 배율 * 확인란을 선택 취소합니다.

5. 값을 전체 정밀도로 표시하려면 * Raw Data * 확인란을 선택하거나 값을 최대 3개의 소수 자릿수(예: 비율로 보고된 속성)로 반올림하려면 * Raw Data * 확인란을 선택 취소합니다.
6. 빠른 쿼리 * 드롭다운 목록에서 보고할 기간을 선택합니다.

   사용자 지정 쿼리 옵션을 선택하여 특정 시간 범위를 선택합니다.

   잠시 후에 차트가 나타납니다. 긴 시간 범위의 표 형성을 위해 몇 분 정도 기다립니다.

7. 사용자 지정 쿼리를 선택한 경우 * 시작 날짜 * 와 * 종료 날짜 * 를 입력하여 차트의 기간을 사용자 지정합니다.

   현지 시간에 '*YYYY/MM/DDHH:MM:SS*' 형식을 사용합니다. 형식과 일치시키려면 맨 앞에 0이 있어야 합니다. 예를 들어, 2017/4/6 7:30:00은 검증에 실패합니다. 올바른 형식은 2017/04/06 07:30:00입니다.

8. Update * 를 선택합니다.

   차트가 몇 초 후에 생성됩니다. 긴 시간 범위의 표 형성을 위해 몇 분 정도 기다립니다. 쿼리에 대해 설정된 시간에 따라 원시 텍스트 보고서 또는 집계 텍스트 보고서가 표시됩니다.

텍스트 보고서를 사용합니다

텍스트 보고서는 NMS 서비스에서 처리한 속성 데이터 값의 텍스트 표현을 표시합니다. 보고하는 기간에 따라 두 가지 유형의 보고서가 생성됩니다. 즉, 주 미만의 기간에 대한 원시 텍스트 보고서와 주 이상의 기간에 대한 텍스트 보고서를 집계합니다.

원시 텍스트 보고서

원시 텍스트 보고서는 선택한 속성에 대한 세부 정보를 표시합니다.

- 수신 시간: NMS 서비스에서 특성 데이터의 샘플 값을 처리한 현지 날짜 및 시간입니다.
- 샘플 시간: 소스에서 특성 값이 샘플링되거나 변경된 로컬 날짜 및 시간입니다.
- 값: 샘플 시간의 특성 값입니다.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

텍스트 보고서를 집계합니다

집계 텍스트 보고서는 원시 텍스트 보고서보다 더 긴 기간(일반적으로 1주일) 동안의 데이터를 표시합니다. 각 항목은 NMS 서비스가 시간에 따라 여러 특성 값(특성 값의 집계)을 집계에서 파생된 평균, 최대 및 최소값을 포함하는 단일 항목으로 요약한 결과입니다.

각 항목에는 다음 정보가 표시됩니다.

- 집계 시간: NMS 서비스가 변경된 속성 값 집합을 집계(수집)한 마지막 로컬 날짜 및 시간입니다.
- 평균 값: 집계된 기간 동안의 특성 값의 평균입니다.
- 최소값: 집계된 기간 동안의 최소값입니다.
- 최대값: 집계된 기간의 최대 값입니다.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

텍스트 보고서를 생성합니다

텍스트 보고서는 NMS 서비스에서 처리한 속성 데이터 값의 텍스트 표현을 표시합니다. 데이터 센터 사이트, 그리드 노드, 구성 요소 또는 서비스에 대해 보고할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

지속적으로 변경해야 하는 특성 데이터의 경우 NMS 서비스(소스에서)가 정기적으로 이 특성 데이터를 샘플링합니다. 자주 변경되지 않는 특성 데이터(예: 상태 또는 상태 변경 등의 이벤트 기반 데이터)의 경우 값이 변경되면 특성 값이 NMS 서비스로 전송됩니다.

표시되는 보고서 유형은 구성된 기간에 따라 다릅니다. 기본적으로 집계 텍스트 보고서는 1주 이상의 기간 동안 생성됩니다.

회색 텍스트는 서비스가 샘플링되는 동안 관리적으로 중단되었음을 나타냅니다. 파란색 텍스트는 서비스가 알 수 없는 상태임을 나타냅니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. grid node_ * > * *component* 또는 *service* * > * Reports * > * Text * 를 선택합니다.
3. 특성 * 드롭다운 목록에서 보고할 특성을 선택합니다.
4. 페이지당 결과 수 * 드롭다운 목록에서 페이지당 결과 수를 선택합니다.
5. 값을 최대 3자리(예: 비율로 보고된 속성)로 반올림하려면 * 원시 데이터 * 확인란의 선택을 취소합니다.
6. 빠른 쿼리 * 드롭다운 목록에서 보고할 기간을 선택합니다.

   사용자 지정 쿼리 옵션을 선택하여 특정 시간 범위를 선택합니다.

   잠시 후에 보고서가 나타납니다. 긴 시간 범위의 표 형성을 위해 몇 분 정도 기다립니다.

7. 사용자 지정 쿼리를 선택한 경우 * 시작일 * 및 * 종료일 * 을 입력하여 보고할 기간을 사용자 지정해야 합니다.

   현지 시간에 YYYY/MM/DDHH:MM:SS 형식을 사용합니다. 형식과 일치시키려면 맨 앞에 0이 있어야 합니다. 예를 들어, 2017/4/6 7:30:00은 검증에 실패합니다. 올바른 형식은 2017/04/06 07:30:00입니다.

8. Update * 를 클릭합니다.

   몇 분 후에 텍스트 보고서가 생성됩니다. 긴 시간 범위의 표 형성을 위해 몇 분 정도 기다립니다. 쿼리에 대해 설정된 시간에 따라 원시 텍스트 보고서 또는 집계 텍스트 보고서가 표시됩니다.

텍스트 보고서를 내보냅니다

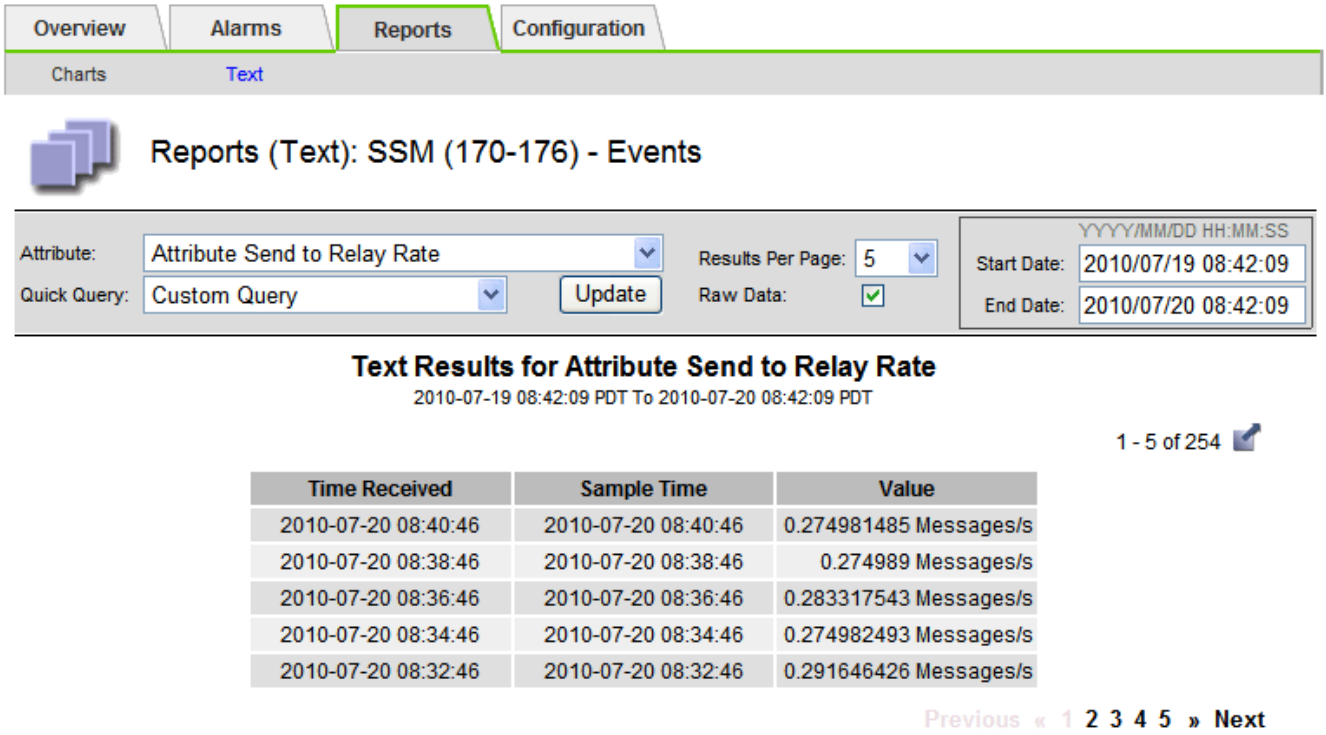
내보낸 텍스트 보고서는 데이터를 선택하고 복사할 수 있는 새 브라우저 탭을 엽니다.

이 작업에 대해

그런 다음 복사한 데이터를 새 문서(예: 스프레드시트)에 저장하고 StorageGRID 시스템의 성능을 분석하는 데 사용할 수 있습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. 텍스트 보고서를 만듭니다.
3. 내보내기 * 를 클릭합니다.



   보고서를 표시하는 Export Text Report(텍스트 보고서 내보내기) 창이 열립니다.

```
Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U
```

4. 텍스트 보고서 내보내기 창의 내용을 선택하고 복사합니다.

   이제 이 데이터를 스프레드시트와 같은 타사 문서에 붙여넣을 수 있습니다.

PUT 모니터링 및 성능 확보

개체 저장소 및 검색 등의 특정 작업의 성능을 모니터링하여 추가 조사가 필요할 수 있는 변경 내용을 식별할 수 있습니다.

이 작업에 대해

PUT 및 GET 성능을 모니터링하려면 워크스테이션에서 직접 또는 오픈 소스 S3tester 애플리케이션을 사용하여 S3 및 Swift 명령을 실행할 수 있습니다. 이러한 방법을 사용하면 클라이언트 응용 프로그램 문제 또는 외부 네트워크 문제 등 StorageGRID 외부의 요인에 관계없이 성능을 평가할 수 있습니다.

PUT 및 GET 작업을 수행할 때 다음 지침을 따르십시오.

- 일반적으로 그리드에 수집한 오브젝트와 비슷한 오브젝트 크기를 사용합니다.
- 로컬 및 원격 사이트 모두에서 작업 수행

에 메시지가 있습니다 감사 로그 특정 작업을 실행하는 데 필요한 총 시간을 나타냅니다. 예를 들어, S3 GET 요청에 대한 총 처리 시간을 결정하려면 SGET 감사 메시지에서 TIME 속성 값을 검토할 수 있습니다. 감사 메시지에서 다음 작업에 대한 시간 속성을 찾을 수도 있습니다.

- * S3 *: 삭제, 가져오기, 헤드, 메타데이터 업데이트됨, POST, 를 누릅니다
- * Swift *: 삭제, 가져오기, 헤드, PUT

결과를 분석할 때 요청을 충족하는 데 필요한 평균 시간과 달성할 수 있는 전체 처리량을 확인하십시오. 동일한 테스트를 정기적으로 반복하고 결과를 기록하여 조사가 필요할 수 있는 추세를 파악할 수 있습니다.

- 가능합니다 "github에서 S3tester를 다운로드합니다".

개체 검증 작업을 모니터링합니다

StorageGRID 시스템은 스토리지 노드에서 오브젝트 데이터의 무결성을 검사하여 손상된 오브젝트와 누락된 오브젝트가 모두 있는지 확인할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.

이 작업에 대해

2개 검증 프로세스 함께 협력하여 데이터 무결성 보장:

- * 백그라운드 검증 * 이 자동으로 실행되어 개체 데이터의 정확성을 지속적으로 확인합니다.

  백그라운드 검증 기능은 모든 스토리지 노드를 자동으로 지속적으로 검사하여 복제된/삭제 코딩 오브젝트 데이터의 손상된 복사본이 있는지 확인합니다. 문제가 발견되면 StorageGRID 시스템은 시스템에 저장된 사본에서 손상된 개체 데이터를 자동으로 교체하려고 시도합니다. 백그라운드 검증이 아카이브 노드 또는 클라우드 스토리지 풀의 객체에서 실행되지 않습니다.

  > 시스템에서 자동으로 수정할 수 없는 손상된 개체를 감지하면 * Unidentified corrupt object detected * 경고가 트리거됩니다.

- * 개체 존재 여부 검사 * 는 개체 데이터의 존재 여부를 보다 빠르게 확인하기 위해 사용자에 의해 트리거될 수 있습니다(정확성은 아님).

  오브젝트 존재 여부는 스토리지 노드에 예상되는 모든 오브젝트 복제 복사본과 삭제 코딩 조각이 있는지 확인합니다. 개체 존재 확인 기능은 특히 최근 하드웨어 문제로 인해 데이터 무결성이 영향을 받을 수 있는 경우 스토리지 디바이스의 무결성을 확인하는 방법을 제공합니다.

백그라운드 검증과 개체 존재 확인 결과를 정기적으로 검토해야 합니다. 손상되었거나 누락된 객체 데이터의 인스턴스를 즉시 조사하여 근본 원인을 파악합니다.

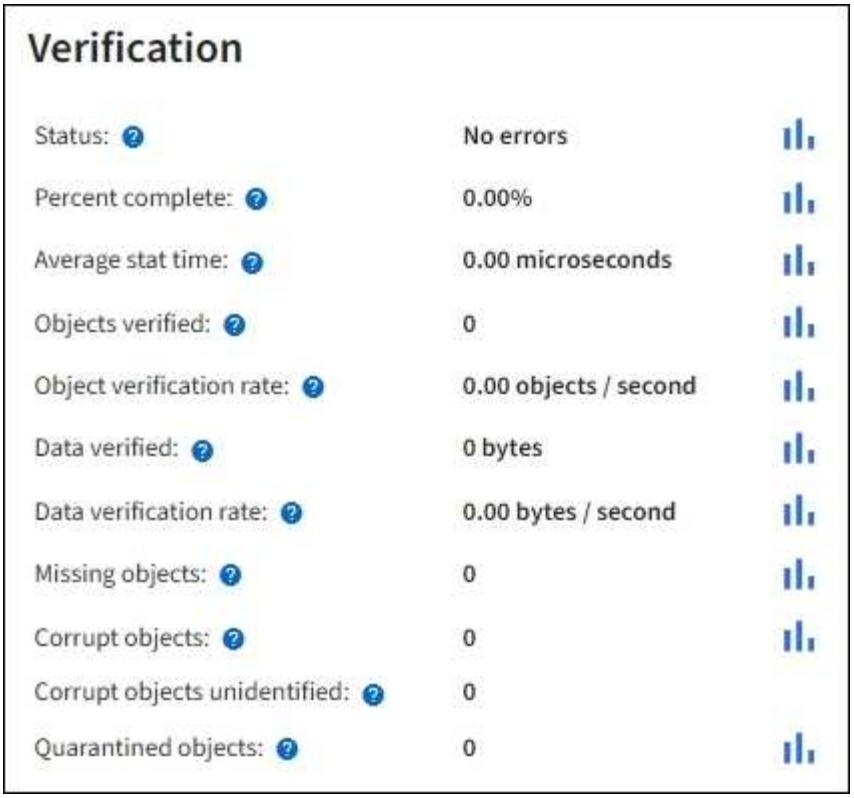
단계

1. 배경 검증에서 얻은 결과를 검토합니다.

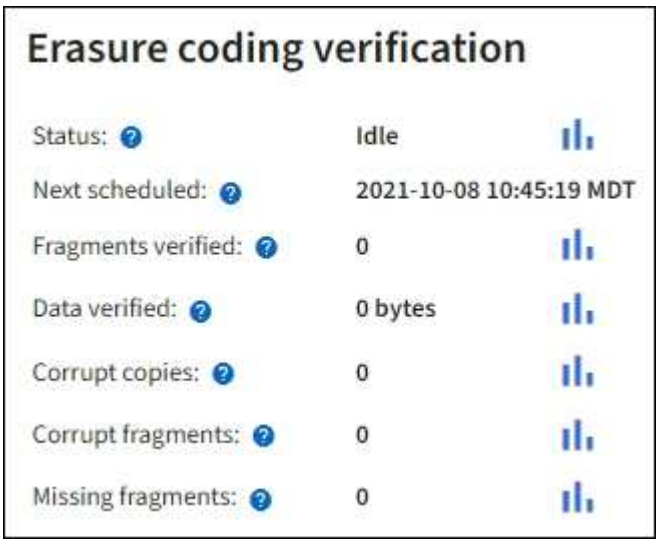
   a. 노드 * > *스토리지 노드 * > * 오브젝트 * 를 선택합니다.

   b. 확인 결과를 확인합니다.

      - 복제된 오브젝트 데이터 검증을 확인하려면 검증 섹션에서 특성을 확인하십시오.

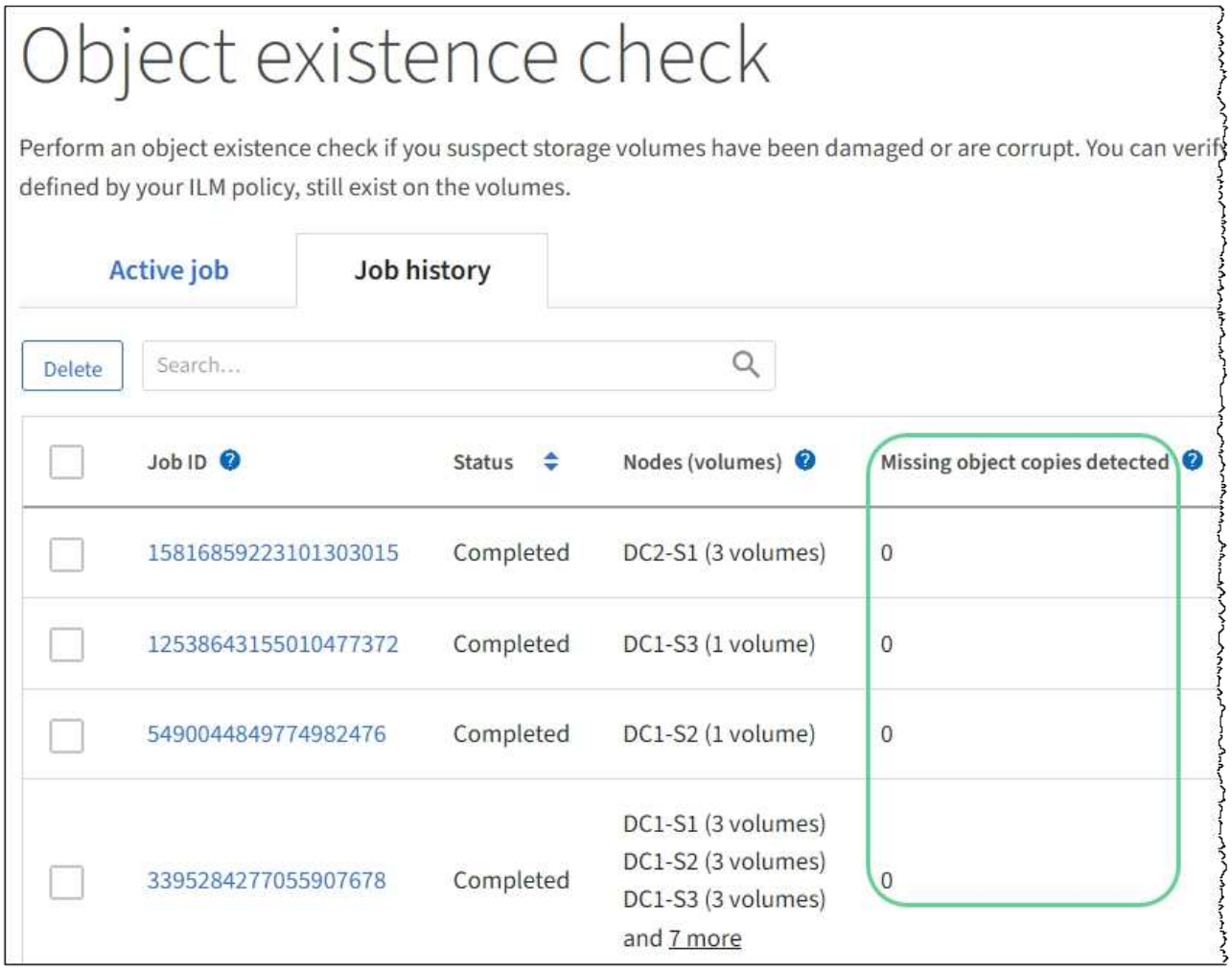


- 삭제 코딩 조각 검증을 확인하려면 * *Storage Node* * > * ILM * 을 선택하고 삭제 코딩 검증 섹션에서 속성을 확인하십시오.



물음표를 선택합니다 ? 속성 이름 옆에 도움말 텍스트를 표시합니다.

2. 개체 존재 확인 작업의 결과를 검토합니다.
   a. 유지보수 * > * 개체 존재 확인 * > * 작업 내역 * 을 선택합니다.
   b. 누락된 개체 복사본 감지 열을 스캔합니다. 작업이 100개 이상의 누락된 오브젝트 복제본과 를 생성하는 경우 개체 손실 경고 이(가) 트리거되었습니다. 기술 지원 부서에 문의하십시오.



이벤트를 모니터링합니다

syslog 서버에 기록된 이벤트를 추적하기 위해 만든 사용자 지정 이벤트를 포함하여 그리드 노드에서 감지한 이벤트를 모니터링할 수 있습니다. 가장 최근의 이벤트에 대한 자세한 내용은 그리드 관리자에 표시된 마지막 이벤트 메시지를 참조하십시오.

이벤트 메시지는 '/var/local/log/bycast-err.log' 로그 파일에도 나열됩니다. 를 참조하십시오 로그 파일 참조.

SMTT(Total events) 알람은 네트워크 문제, 정전 또는 업그레이드와 같은 문제로 인해 반복적으로 발생할 수 있습니다. 이 섹션에서는 이러한 알람이 발생한 이유를 보다 잘 이해할 수 있도록 이벤트 조사에 대한 정보를 제공합니다. 알려진 문제로 인해 이벤트가 발생한 경우 이벤트 카운터를 다시 설정하는 것이 안전합니다.

단계

1. 각 그리드 노드에 대한 시스템 이벤트를 검토합니다.
   a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
   b. site_ * > **GRID node* * > * SSM * > * Events * > * Overview * > * Main * 을 선택합니다.
2. 이전 이벤트 메시지의 목록을 생성하여 이전에 발생한 문제를 격리할 수 있습니다.
   a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
   b. site_ * > **GRID node* * > * SSM * > * Events * > * Reports * 를 선택합니다.

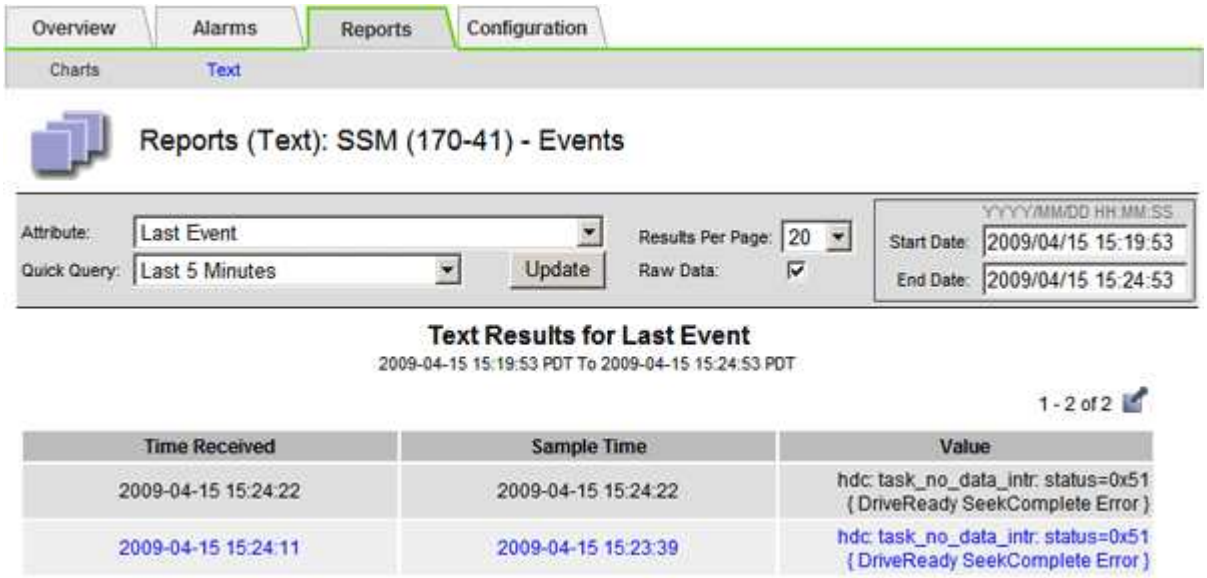
c. 텍스트 * 를 선택합니다.

Last Event * 속성은 에 표시되지 않습니다 차트 보기. 보기:

d. 속성 * 을 * 마지막 이벤트 * 로 변경합니다.

e. 필요에 따라 * 빠른 쿼리 * 의 기간을 선택합니다.

f. Update * 를 선택합니다.



사용자 지정 **syslog** 이벤트를 생성합니다

사용자 지정 이벤트를 사용하면 syslog 서버에 기록된 모든 커널, 데몬, 오류 및 중요한 수준 사용자 이벤트를 추적할 수 있습니다. 사용자 지정 이벤트는 시스템 로그 메시지(네트워크 보안 이벤트 및 하드웨어 장애)의 발생을 모니터링하는 데 유용할 수 있습니다.

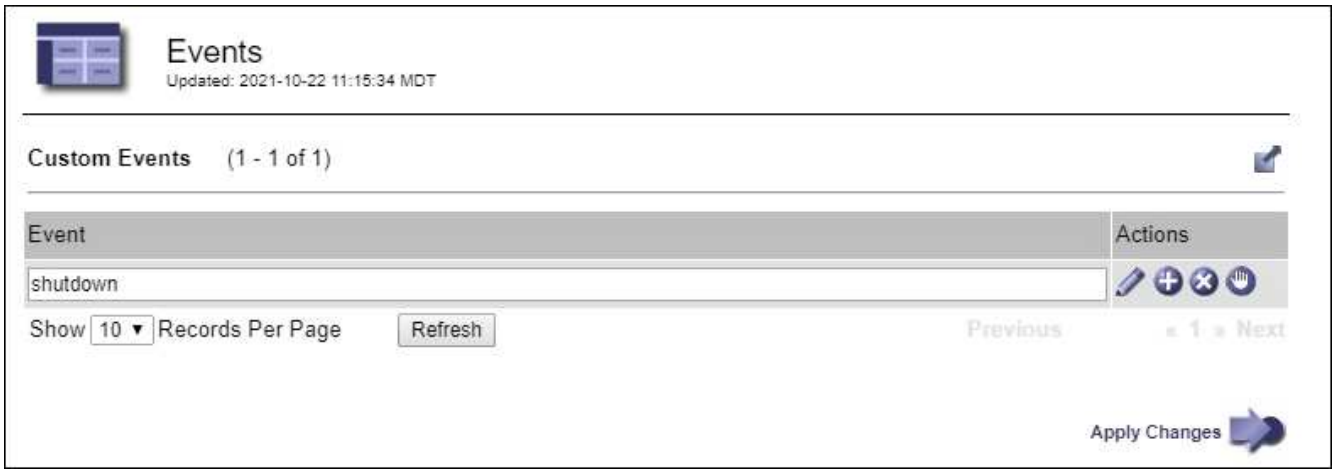
이 작업에 대해

반복되는 문제를 모니터링하려면 사용자 지정 이벤트를 만드는 것이 좋습니다. 사용자 지정 이벤트에는 다음 고려 사항이 적용됩니다.

- 사용자 지정 이벤트가 생성되면 이벤트가 발생할 때마다 모니터링됩니다.
- '/var/local/log/messages' 파일의 키워드를 기반으로 사용자 지정 이벤트를 만들려면 해당 파일의 로그가 다음 중 어떤 것이어야 합니다.
  - 커널에 의해 생성됩니다
  - 오류 또는 위험 수준에서 데몬 또는 사용자 프로그램에 의해 생성됩니다
- 참고: * 위에 명시된 요구 사항을 충족하지 않는 한, '/var/local/log/messages' 파일의 모든 항목이 일치되는 것은 아닙니다.

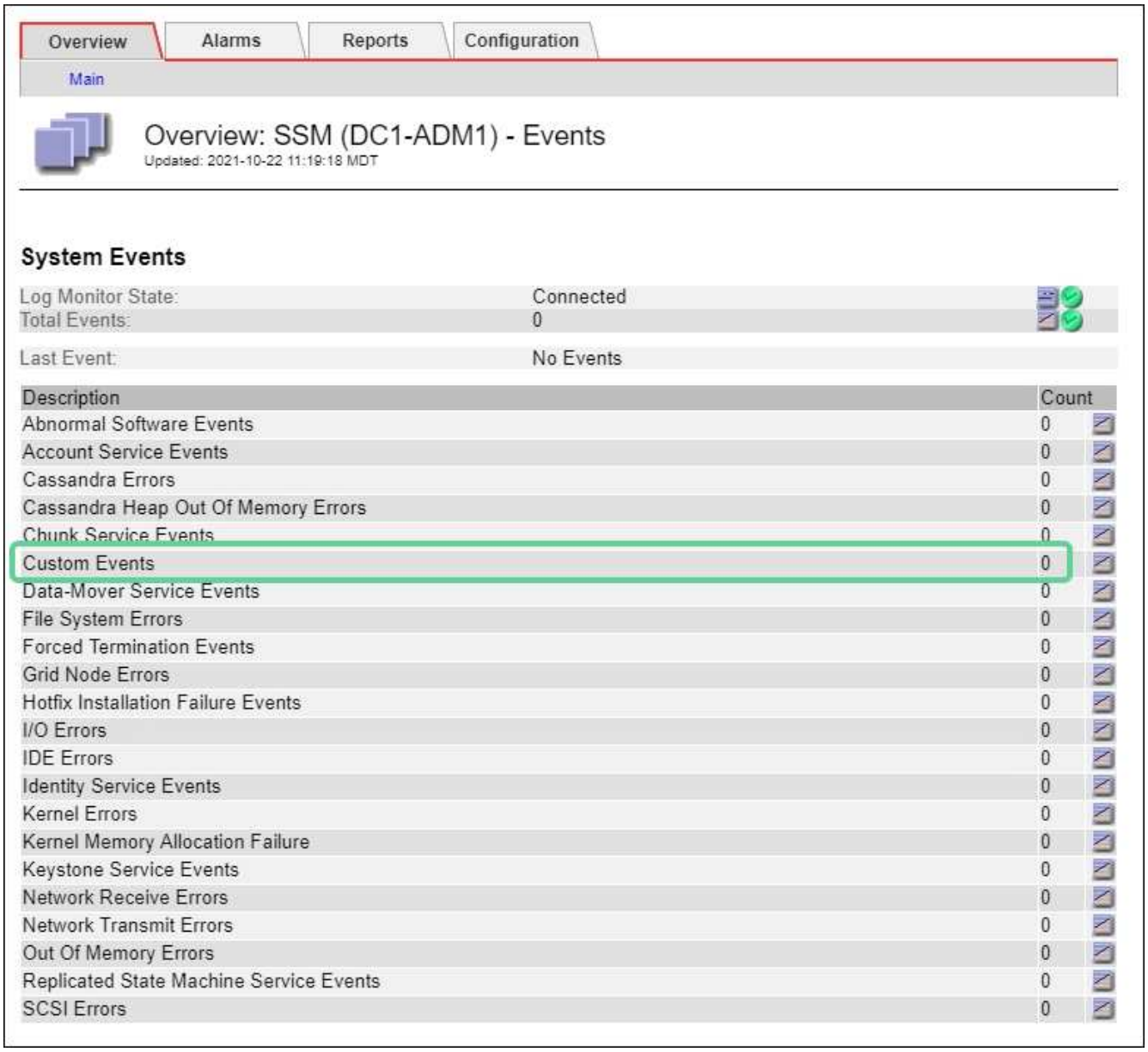
단계

1. 지원 * > * 알람(레거시) * > * 사용자 정의 이벤트 * 를 선택합니다.
2. 편집 * 을 클릭합니다 (또는 * Insert * (삽입 *)를 클릭합니다 첫 번째 이벤트가 아닌 경우).
3. shutdown 과 같은 사용자 지정 이벤트 문자열을 입력합니다



4. Apply Changes * 를 선택합니다.
5. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
6. grid node_ * > * ssm * > * Events * 를 선택합니다.
7. Events 테이블에서 Custom Events 항목을 찾아 * Count * 에 대한 값을 모니터링합니다.

   개수가 증가하면 모니터링 중인 사용자 지정 이벤트가 해당 그리드 노드에서 트리거됩니다.



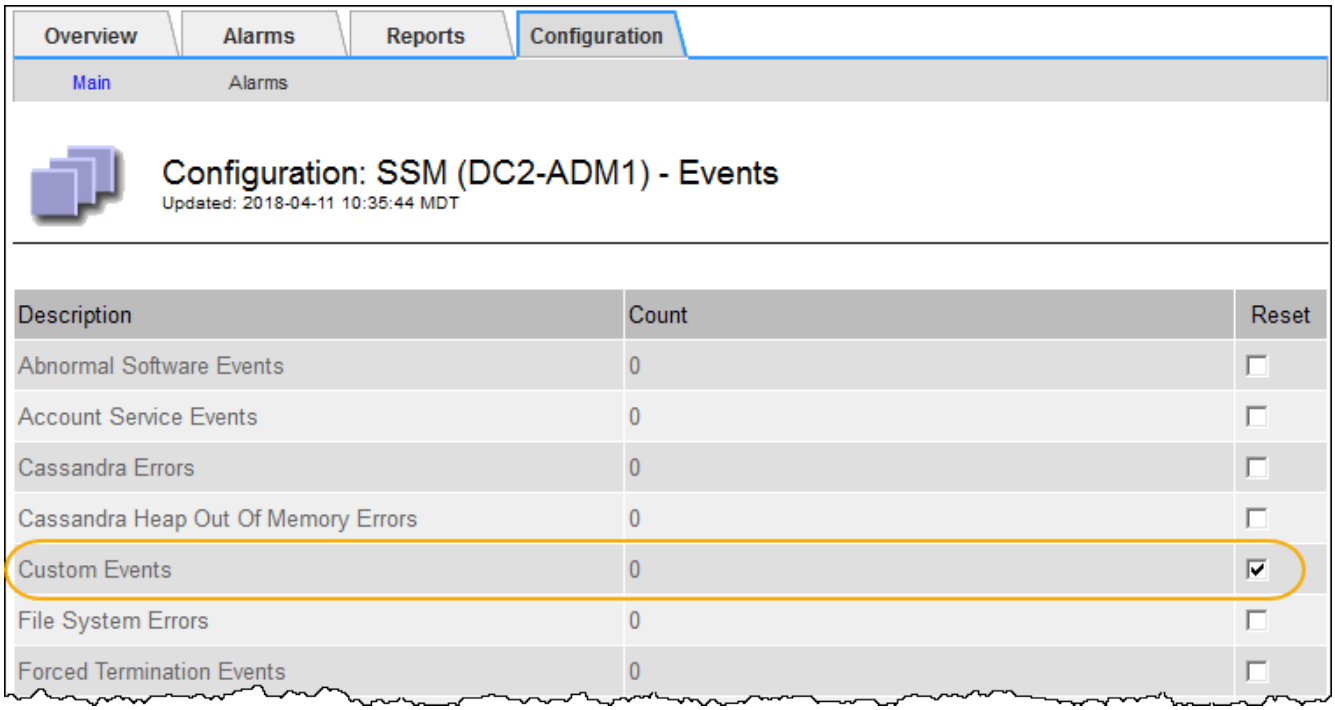
사용자 지정 이벤트 수를 **0**으로 재설정합니다

사용자 지정 이벤트에 대해서만 카운터를 재설정하려면 지원 메뉴의 그리드 토폴로지 페이지를 사용해야 합니다.

이 작업에 대해

카운터를 재설정하면 다음 이벤트에 의해 알람이 트리거됩니다. 반면, 알람을 확인할 때 해당 알람은 다음 임계값 수준에 도달한 경우에만 다시 트리거됩니다.

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. grid node_ * > * ssm * > * Events * > * Configuration * > * Main * 을 선택합니다.
3. 사용자 지정 이벤트의 * 재설정 * 확인란을 선택합니다.



4. Apply Changes * 를 선택합니다.

감사 메시지를 검토합니다

감사 메시지를 통해 StorageGRID 시스템의 세부 작업을 보다 잘 이해할 수 있습니다. 감사 로그를 사용하여 문제를 해결하고 성능을 평가할 수 있습니다.

정상적인 시스템 작동 중에 모든 StorageGRID 서비스는 다음과 같이 감사 메시지를 생성합니다.

- 시스템 감사 메시지는 감사 시스템 자체, 그리드 노드 상태, 시스템 전체 작업 및 서비스 백업 작업과 관련되어 있습니다.
- 오브젝트 스토리지 감사 메시지는 오브젝트 스토리지 및 검색, 그리드 노드에서 그리드 노드 전송, 확인을 포함하여 StorageGRID 내의 오브젝트 스토리지 및 관리와 관련되어 있습니다.
- S3 또는 Swift 클라이언트 애플리케이션이 오브젝트 생성, 수정 또는 검색을 요청할 때 클라이언트 읽기 및 쓰기 감사 메시지가 기록됩니다.
- 관리 감사 메시지는 관리 API에 사용자 요청을 기록합니다.

각 관리 노드는 감사 메시지를 텍스트 파일에 저장합니다. 감사 공유에는 활성 파일(audit.log)과 이전 일로부터의 압축된 감사 로그가 포함됩니다. 그리드의 각 노드는 노드에서 생성된 감사 정보의 복사본도 저장합니다.

감사 로그에 쉽게 액세스할 수 있도록 NFS 및 CIFS에 대한 감사 공유에 대한 클라이언트 액세스를 구성할 수 있습니다(CIFS는 더 이상 사용되지 않음). 관리자 노드의 명령줄에서 직접 감사 로그 파일에 액세스할 수도 있습니다.

선택적으로 감사 로그의 대상을 변경하고 감사 정보를 외부 syslog 서버로 보낼 수 있습니다. 외부 syslog 서버가 구성되면 감사 레코드의 로컬 로그가 계속 생성되고 저장됩니다. 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다.

감사 로그 파일, 감사 메시지 형식, 감사 메시지 유형 및 감사 메시지 분석에 사용할 수 있는 도구에 대한 자세한 내용은 감사 메시지 지침을 참조하십시오. 감사 클라이언트 액세스를 구성하는 방법에 대한 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

관련 정보

감사 로그를 검토합니다

StorageGRID 관리

로그 파일 및 시스템 데이터를 수집합니다

그리드 관리자를 사용하여 StorageGRID 시스템에 대한 로그 파일 및 시스템 데이터(구성 데이터 포함)를 검색할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.

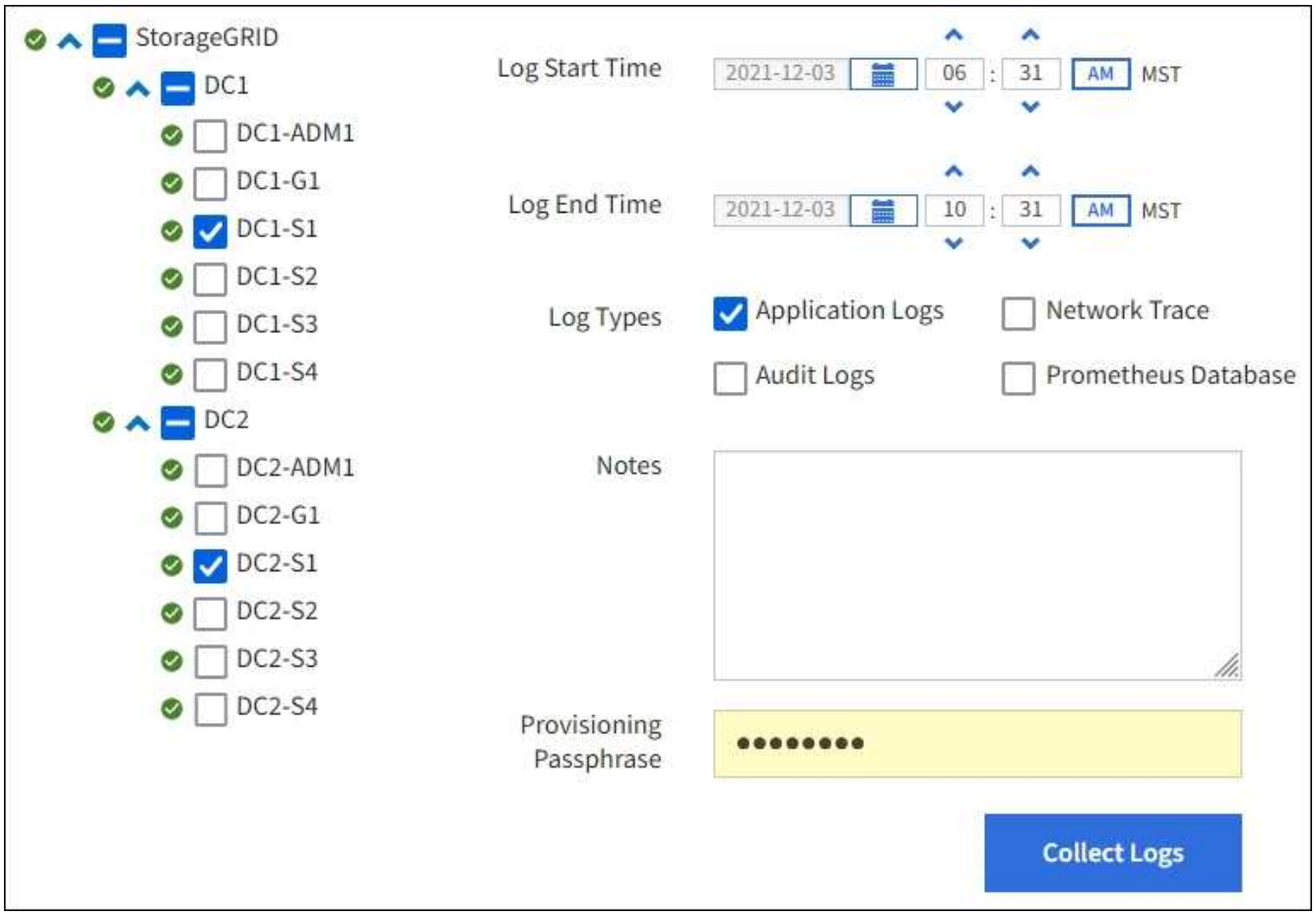
이 작업에 대해

그리드 관리자를 사용하여 수집할 수 있습니다 로그 파일선택한 기간 동안 그리드 노드의 시스템 데이터 및 구성 데이터 데이터는 .tar.gz 파일에 수집 및 보관되며, 이 파일은 로컬 컴퓨터로 다운로드할 수 있습니다.

선택적으로 감사 로그의 대상을 변경하고 감사 정보를 외부 syslog 서버로 보낼 수 있습니다. 외부 syslog 서버가 구성되면 감사 레코드의 로컬 로그가 계속 생성되고 저장됩니다. 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다.

단계

1. 지원 * > * 도구 * > * 로그 * 를 선택합니다.



2. 로그 파일을 수집할 그리드 노드를 선택합니다.

   필요에 따라 전체 그리드 또는 전체 데이터 센터 사이트에 대한 로그 파일을 수집할 수 있습니다.

3. 시작 시간 * 과 * 종료 시간 * 을 선택하여 로그 파일에 포함할 데이터의 시간 범위를 설정합니다.

   매우 긴 기간을 선택하거나 큰 그리드의 모든 노드에서 로그를 수집할 경우 로그 아카이브가 너무 커서 노드에 저장할 수 없거나 너무 커서 기본 관리 노드에 다운로드할 수 없습니다. 이 경우 더 작은 데이터 집합으로 로그 수집을 다시 시작해야 합니다.

4. 수집할 로그 유형을 선택합니다.
   - * 응용 프로그램 로그 *: 기술 지원 부서에서 문제 해결을 위해 가장 자주 사용하는 응용 프로그램별 로그. 수집된 로그는 사용 가능한 애플리케이션 로그의 하위 집합입니다.
   - * 감사 로그 *: 정상적인 시스템 작동 중에 생성된 감사 메시지를 포함하는 로그.
   - * 네트워크 추적*: 네트워크 디버깅에 사용되는 로그.
   - * Prometheus Database *: 모든 노드의 서비스에서 시계열 메트릭입니다.
5. 필요한 경우 * Notes * 텍스트 상자에 수집하고 있는 로그 파일에 대한 메모를 입력합니다.

   이러한 메모를 사용하여 로그 파일을 수집하라는 메시지가 표시되는 문제에 대한 기술 지원 정보를 제공할 수 있습니다. 참고는 로그 파일 컬렉션에 대한 기타 정보와 함께 "info.txt"라는 파일에 추가됩니다. info.txt 파일은 로그 파일 아카이브 패키지에 저장됩니다.

6. Provisioning Passphrase * 텍스트 상자에 StorageGRID 시스템의 프로비저닝 암호를 입력합니다.

7. 로그 수집 * 을 선택합니다.

   새 요청을 제출하면 이전 로그 파일 모음이 삭제됩니다.

   로그 페이지를 사용하여 각 그리드 노드에 대한 로그 파일 수집 진행률을 모니터링할 수 있습니다.

   로그 크기에 대한 오류 메시지가 표시되면 더 짧은 기간 또는 더 적은 수의 노드에 대해 로그를 수집해 보십시오.

8. 로그 파일 수집이 완료되면 * Download * 를 선택합니다.

   tar.gz_file에는 로그 수집이 성공한 모든 그리드 노드의 모든 로그 파일이 포함되어 있습니다. combined_.tar.gz_file 안에는 각 그리드 노드에 대해 하나의 로그 파일 아카이브가 있습니다.

작업을 마친 후

필요한 경우 나중에 로그 파일 아카이브 패키지를 다시 다운로드할 수 있습니다.

선택적으로 * Delete * 를 선택하여 로그 파일 아카이브 패키지를 제거하고 디스크 공간을 확보할 수 있습니다. 다음 번에 로그 파일을 수집할 때 현재 로그 파일 아카이브 패키지가 자동으로 제거됩니다.

AutoSupport 메시지를 수동으로 트리거합니다

StorageGRID 시스템 관련 문제 해결에 대한 기술 지원을 받으려면 AutoSupport 메시지를 수동으로 전송할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 또는 기타 그리드 구성 권한이 있어야 합니다.

단계

1. 지원 * > * 도구 * > * AutoSupport * 를 선택합니다.

   AutoSupport 페이지가 나타나고 * 설정 * 탭이 선택됩니다.

2. Send User-triggered AutoSupport * 를 선택합니다.

   StorageGRID는 기술 지원 부서에 AutoSupport 메시지를 보내려고 시도합니다. 시도가 성공하면 * Results * 탭의 * Most Recent Result * 및 * Last Successful Time * 값이 업데이트됩니다. 문제가 있는 경우 * 가장 최근의 결과 * 값이 "실패"로 업데이트되고 StorageGRID는 AutoSupport 메시지를 다시 전송하지 않습니다.

   > 사용자 트리거 AutoSupport 메시지를 보낸 후 1분 후 브라우저에서 AutoSupport 페이지를 새로 고쳐 가장 최근 결과에 액세스합니다.

관련 정보

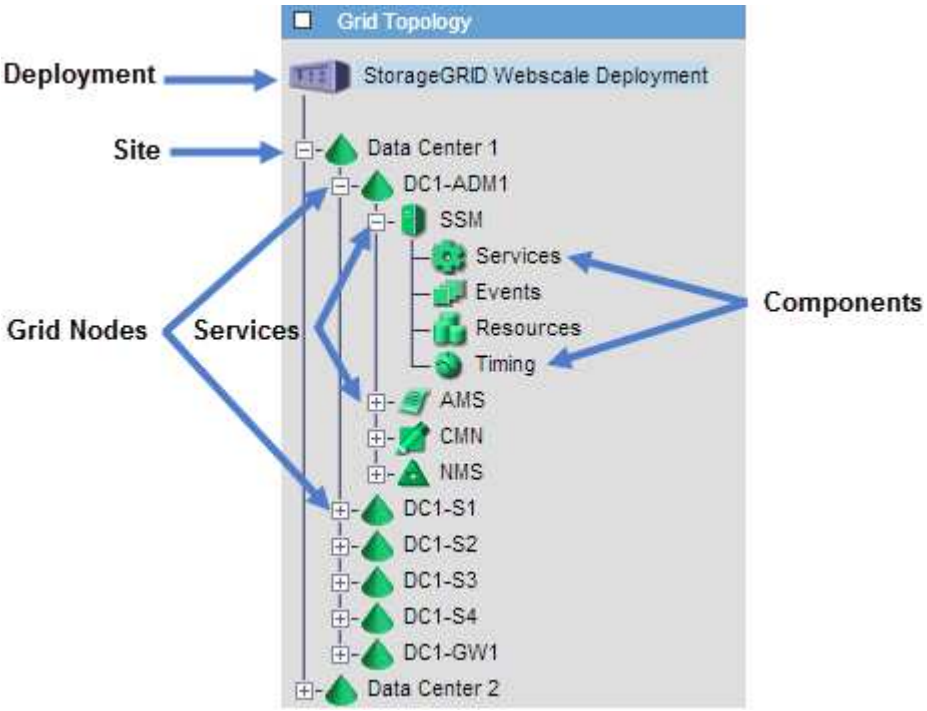
경보에 대한 이메일 서버 설정 구성(레거시 시스템)

그리드 토폴로지 트리를 봅니다

그리드 토폴로지 트리를 사용하면 사이트, 그리드 노드, 서비스 및 구성 요소를 비롯한

StorageGRID 시스템 요소에 대한 자세한 정보에 액세스할 수 있습니다. 대부분의 경우, 문서에 지시된 경우 또는 기술 지원 부서의 작업 시에만 그리드 토폴로지 트리에 액세스해야 합니다.

그리드 토폴로지 트리에 액세스하려면 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.



그리드 토폴로지 트리를 확장하거나 축소하려면 을 클릭합니다 ⊞ 또는 ⊟ 사이트, 노드 또는 서비스 수준에서 선택합니다. 전체 사이트 또는 각 노드의 모든 항목을 확장하거나 축소하려면 * <Ctrl> * 키를 누른 상태에서 클릭합니다.

지원 메트릭을 검토합니다

문제를 해결할 때 기술 지원 팀과 협력하여 StorageGRID 시스템에 대한 자세한 메트릭 및 차트를 검토할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

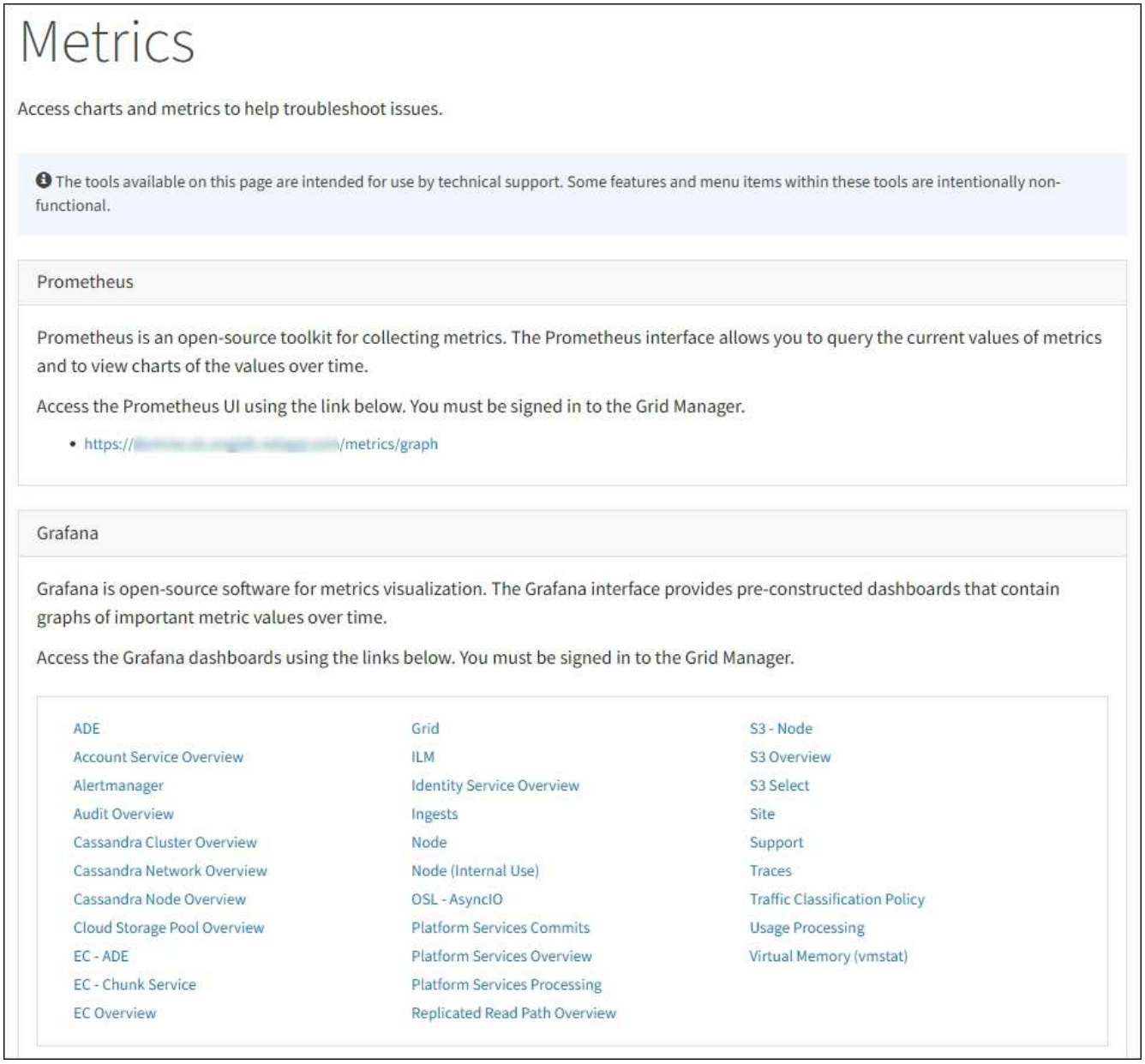
메트릭 페이지에서는 Prometheus 및 Grafana 사용자 인터페이스에 액세스할 수 있습니다. Prometheus는 메트릭 수집을 위한 오픈 소스 소프트웨어입니다. Grafana는 메트릭 시각화를 위한 오픈 소스 소프트웨어입니다.

> 메트릭 페이지에서 사용할 수 있는 도구는 기술 지원 부서에서 사용하기 위한 것입니다. 이러한 도구 내의 일부 기능 및 메뉴 항목은 의도적으로 작동하지 않으며 변경될 수 있습니다. 의 목록을 참조하십시오 일반적으로 사용되는 Prometheus 메트릭입니다.

단계

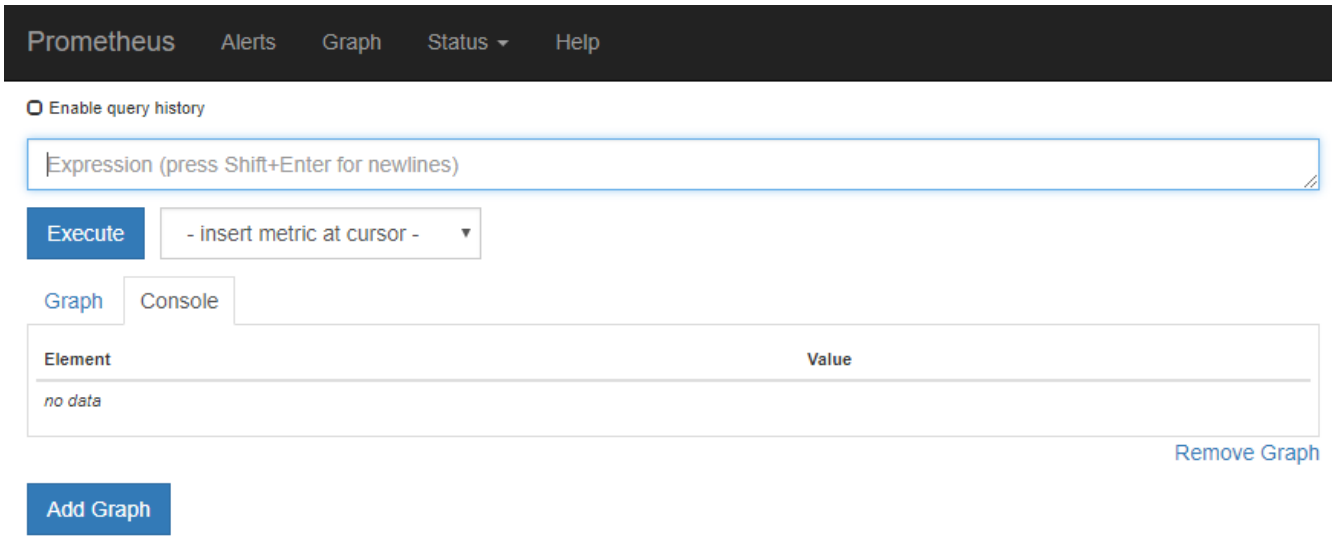
1. 기술 지원의 지시에 따라 * 지원 * > * 도구 * > * 메트릭 * 을 선택합니다.

   Metrics(메트릭) 페이지의 예는 다음과 같습니다.



2. StorageGRID 메트릭의 현재 값을 쿼리하고 시간에 따른 값의 그래프를 보려면 Prometheus 섹션에서 링크를 클릭합니다.

   Prometheus 인터페이스가 나타납니다. 이 인터페이스를 사용하여 사용 가능한 StorageGRID 메트릭에 대한 쿼리를 실행하고 시간에 따른 StorageGRID 메트릭을 그래프로 작성할 수 있습니다.



> 이름에 _private_이 포함된 메트릭은 내부 전용이며 StorageGRID 릴리스 간에 예고 없이 변경될 수 있습니다.

3. 시간에 따른 StorageGRID 메트릭 그래프가 포함된 미리 작성된 대시보드에 액세스하려면 Grafana 섹션의 링크를 클릭하십시오.

   선택한 링크에 대한 Grafana 인터페이스가 나타납니다.

진단 유틸리티를 실행합니다

문제를 해결할 때 기술 지원 부서의 도움을 받을 수 있습니다. StorageGRID 시스템에서 진단 프로그램을 실행하고 결과를 검토할 수 있습니다.

- 지원 메트릭을 검토합니다
- 일반적으로 사용되는 Prometheus 메트릭입니다

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있습니다.

이 작업에 대해

진단 페이지는 그리드의 현재 상태에 대한 진단 검사 집합을 수행합니다. 각 진단 점검에는 다음 세 가지 상태 중 하나가 있을 수 있습니다.

- * 정상 *: 모든 값이 정상 범위 내에 있습니다.
- * 주의 *: 하나 이상의 값이 정상 범위를 벗어났습니다.
- * 주의 *: 하나 이상의 값이 정상 범위를 크게 벗어났습니다.

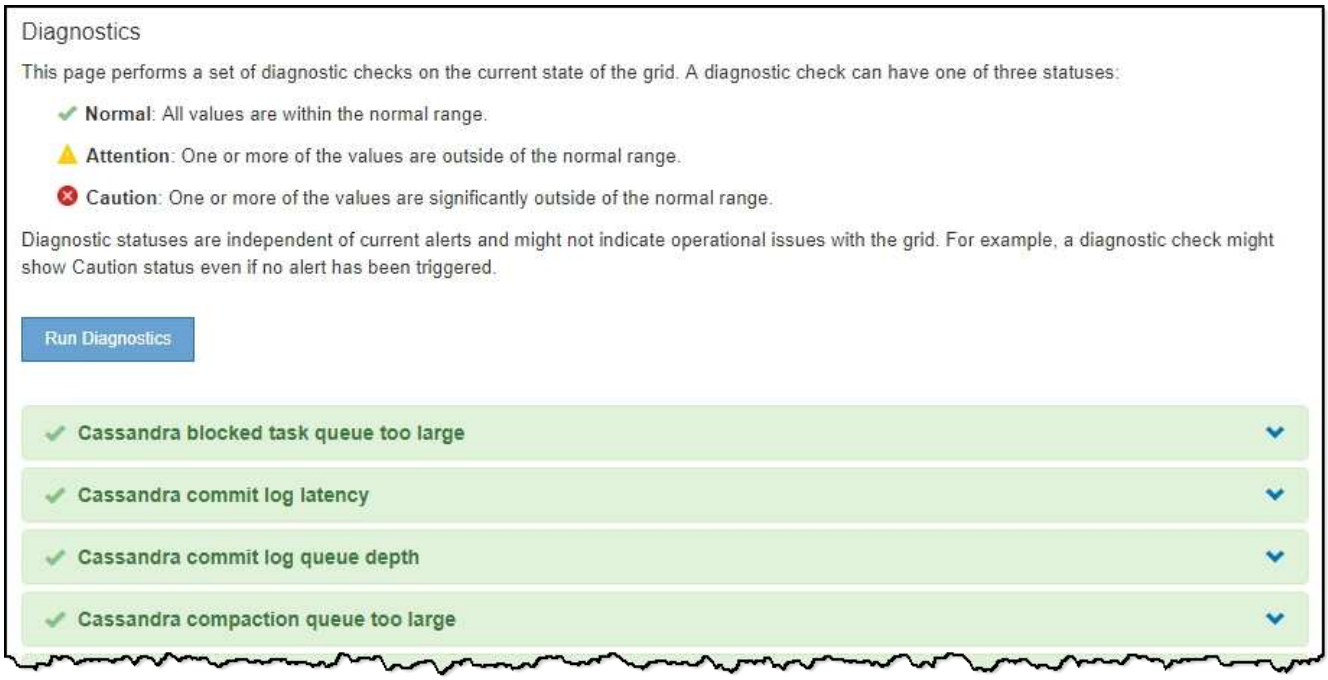
진단 상태는 현재 알림과 독립적이며, 그리드에 작동 문제를 나타내지 않을 수 있습니다. 예를 들어, 경고가 트리거되지 않았더라도 진단 점검에 주의 상태가 표시될 수 있습니다.

단계

1. 지원 * > * 도구 * > * 진단 * 을 선택합니다.

   진단 페이지가 나타나고 각 진단 점검의 결과가 나열됩니다. 결과는 심각도(주의, 주의 및 정상)별로 정렬됩니다. 각 심각도 내에서는 결과가 알파벳순으로 정렬됩니다.

   이 예에서 모든 진단 유틸리티는 정상 상태입니다.



2. 특정 진단에 대한 자세한 내용을 보려면 행의 아무 곳이나 클릭합니다.

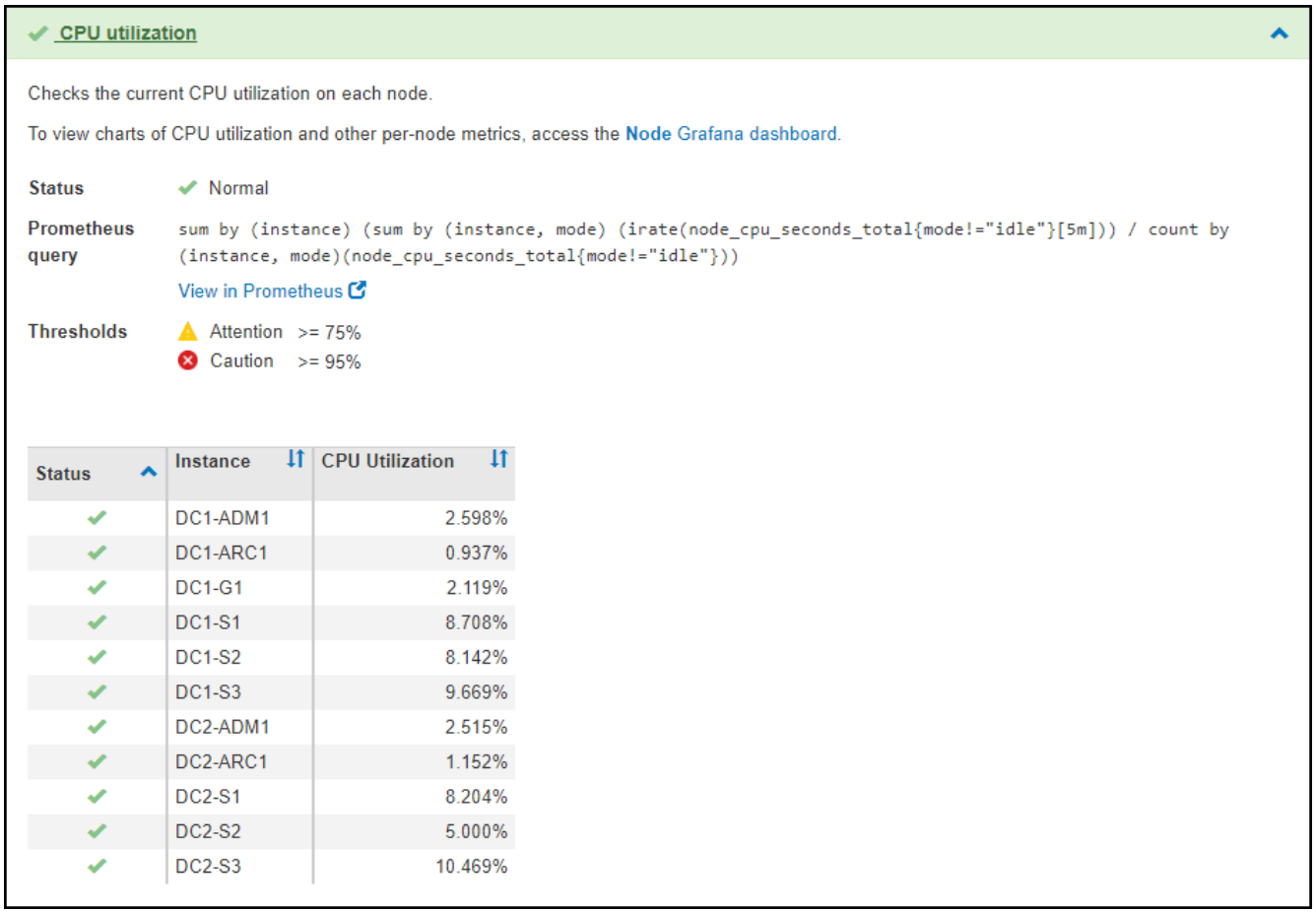
   진단 및 현재 결과에 대한 세부 정보가 나타납니다. 다음 세부 정보가 나열됩니다.

   - * 상태 *: 이 진단의 현재 상태: 정상, 주의 또는 주의.
   - * Prometheus query *: 진단용으로 사용된 경우 상태 값을 생성하는 데 사용된 Prometheus 식입니다. (Prometheus 표현식은 일부 진단에는 사용되지 않습니다.)
   - * 임계값 *: 진단에 사용할 수 있는 경우 각 비정상적인 진단 상태에 대한 시스템 정의 임계값입니다. (일부 진단 유틸리티에는 임계값이 사용되지 않습니다.)

     이러한 임계값은 변경할 수 없습니다.

   - * 상태 값 *: StorageGRID 시스템 전체에서 진단 상태 및 값을 보여주는 표. 이 예에서는 StorageGRID

시스템의 모든 노드에 대한 현재 CPU 활용률이 표시됩니다. 모든 노드 값이 주의 및 주의 임계값 미만이므로 진단의 전체 상태는 정상입니다.



Status	Instance	CPU Utilization
✔	DC1-ADM1	2.598%
✔	DC1-ARC1	0.937%
✔	DC1-G1	2.119%
✔	DC1-S1	8.708%
✔	DC1-S2	8.142%
✔	DC1-S3	9.669%
✔	DC2-ADM1	2.515%
✔	DC2-ARC1	1.152%
✔	DC2-S1	8.204%
✔	DC2-S2	5.000%
✔	DC2-S3	10.469%

3. * 선택 사항 *: 이 진단과 관련된 Grafana 차트를 보려면 * Grafana 대시보드 * 링크를 클릭하십시오.

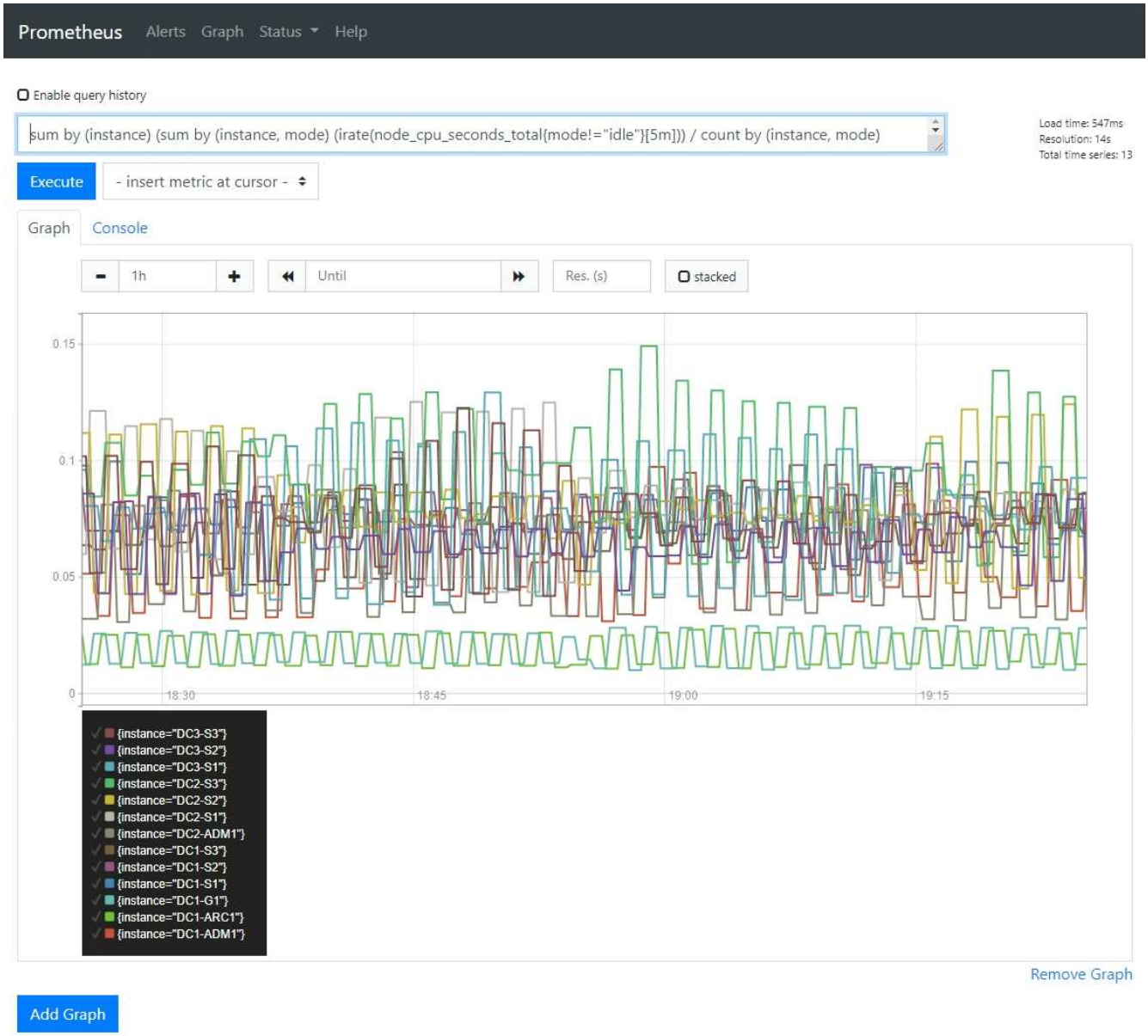
   이 링크는 일부 진단 유틸리티에는 표시되지 않습니다.

   관련 Grafana 대시보드가 나타납니다. 이 예에서 노드 대시보드는 이 노드에 대한 CPU 사용률 및 해당 노드에 대한 다른 Grafana 차트를 보여 줍니다.

   > 지원 * > * 도구 * > * 메트릭 * 페이지의 Grafana 섹션에서 사전 구성된 Grafana 대시보드에 액세스할 수도 있습니다.

4. * 선택 사항 *: Prometheus 표현식의 차트를 보려면 * Prometheus * 에서 보기 를 클릭합니다.

   진단에서 사용되는 표현식의 Prometheus 그래프가 나타납니다.



맞춤형 모니터링 애플리케이션을 생성합니다

그리드 관리 API에서 사용할 수 있는 StorageGRID 메트릭을 사용하여 맞춤형 모니터링 애플리케이션과 대시보드를 구축할 수 있습니다.

그리드 관리자의 기존 페이지에 표시되지 않은 메트릭을 모니터링하거나 StorageGRID용 사용자 지정 대시보드를 만들려는 경우 그리드 관리 API를 사용하여 StorageGRID 메트릭을 쿼리할 수 있습니다.

Grafana와 같은 외부 모니터링 툴을 사용하여 Prometheus 메트릭에 직접 액세스할 수도 있습니다. 외부 도구를 사용하려면 StorageGRID에서 보안을 위해 도구를 인증할 수 있도록 관리 클라이언트 인증서를 업로드하거나 생성해야 합니다. 를 참조하십시오 StorageGRID 관리 지침.

사용 가능한 메트릭의 전체 목록을 포함하여 메트릭 API 작업을 보려면 Grid Manager로 이동하십시오. 페이지 상단에서 도움말 아이콘을 선택하고 * API Documentation * > * metrics * 를 선택합니다.

metrics Operations on metrics

GET	/grid/metric-labels/{label}/values	Lists the values for a metric label
GET	/grid/metric-names	Lists all available metric names
GET	/grid/metric-query	Performs an instant metric query at a single point in time
GET	/grid/metric-query-range	Performs a metric query over a range of time

사용자 지정 모니터링 응용 프로그램을 구현하는 방법에 대한 자세한 내용은 이 설명서의 범위를 벗어납니다.

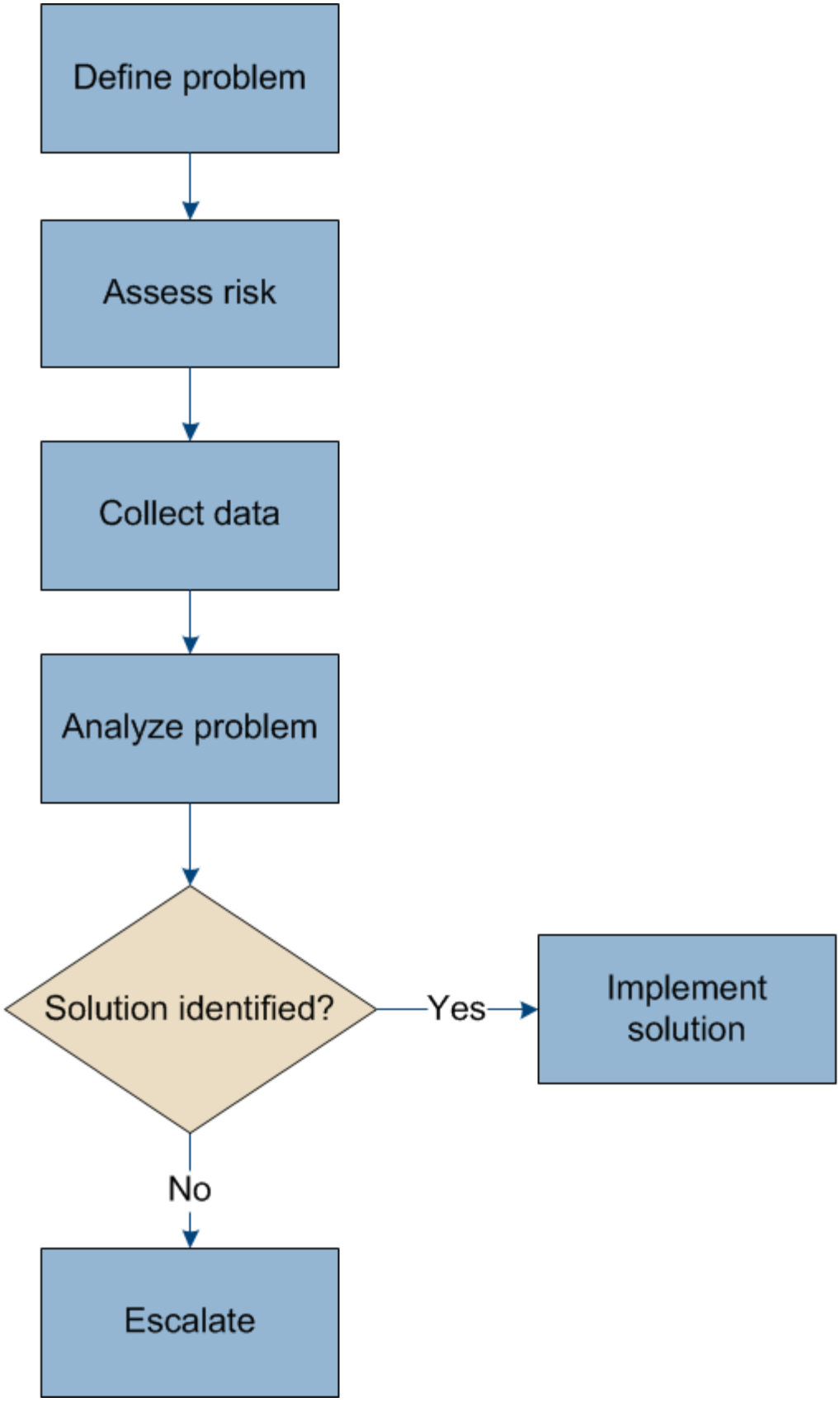
StorageGRID 시스템 문제를 해결합니다

StorageGRID 시스템 문제를 해결합니다

StorageGRID 시스템을 사용할 때 문제가 발생하는 경우 이 섹션의 팁과 지침을 참조하여 문제를 확인하고 해결하십시오.

문제 확인 개요

에 문제가 있는 경우 StorageGRID 시스템 관리, 이 그림에 설명된 프로세스를 사용하여 문제를 식별하고 분석할 수 있습니다. 대부분의 경우 직접 문제를 해결할 수 있지만 일부 문제는 기술 지원 부서에 에스컬레이션해야 할 수 있습니다.



문제를 정의합니다

문제를 해결하기 위한 첫 번째 단계는 문제를 명확하게 정의하는 것입니다.

이 표에서는 문제를 정의하기 위해 수집할 수 있는 정보 유형의 예를 제공합니다.

질문	샘플 응답
StorageGRID 시스템의 기능은 무엇입니까? 또는 작동하지 않습니다. 증상은 무엇입니까?	클라이언트 애플리케이션이 객체를 StorageGRID로 인제스트할 수 없다고 보고합니다.
문제가 언제 시작되었습니까?	오브젝트 수집은 2020년 1월 8일 약 14:50에 처음 거부되었습니다.
문제를 처음 알게 된 방법은 무엇입니까?	클라이언트 응용 프로그램에 의해 통지됩니다. 알림 e-메일 알림도 받았습니다.
문제가 지속적으로 발생합니까, 아니면 가끔만 발생합니까?	문제가 지속되고 있습니다.
문제가 정기적으로 발생하면 어떤 단계를 통해 문제가 발생하는지 확인합니다	클라이언트에서 오브젝트를 수집하려고 할 때마다 문제가 발생합니다.
문제가 간헐적으로 발생하는 경우 언제 발생합니까? 알고 있는 각 사고의 시간을 기록합니다.	문제가 간헐적으로 발생하지 않습니다.
이전에 이 문제를 본 적이 있습니까? 과거에 이 문제가 얼마나 자주 있었습니까?	이 문제를 처음 본 것입니다.

시스템에 미치는 위험과 영향을 평가합니다

문제를 정의한 후 StorageGRID 시스템에 미치는 위험과 영향을 평가합니다. 예를 들어, 중요한 경고가 있다고 해서 시스템에서 핵심 서비스를 제공하지 않는 것은 아닙니다.

이 표에는 시스템 운영에 대한 예제 문제의 영향이 요약되어 있습니다.

질문	샘플 응답
StorageGRID 시스템에서 콘텐츠를 수집할 수 있습니까?	아니요
클라이언트 응용 프로그램이 콘텐츠를 검색할 수 있습니까?	일부 개체는 검색할 수 있고 다른 개체는 검색할 수 없습니다.
데이터가 위험에 노출되어 있습니까?	아니요
비즈니스를 수행하는 능력이 심각하게 영향을 받습니까?	예. 클라이언트 응용 프로그램은 StorageGRID 시스템에 개체를 저장할 수 없고 데이터를 일관되게 검색할 수 없기 때문입니다.

데이터 수집

문제를 정의하고 위험 및 영향을 평가한 후 분석을 위해 데이터를 수집합니다. 수집하는 데 가장 유용한 데이터 유형은 문제의 특성에 따라 다릅니다.

수집할 데이터의 유형입니다	이 데이터를 수집하는 이유	지침
최근 변경 사항의 시간 표시 막대를 만듭니다	StorageGRID 시스템, 구성 또는 환경을 변경하면 새로운 동작이 발생할 수 있습니다.	• 최근 변경 내용의 시간 표시 막대를 만듭니다
경고 및 알람을 검토합니다	경고와 알람은 문제의 근본 원인에 대한 중요한 단서를 제공하여 문제의 근본 원인을 신속하게 파악하는 데 도움이 됩니다. 현재 경고 및 알람 목록을 검토하여 StorageGRID가 문제의 근본 원인을 식별하는지 확인합니다. 이전에 트리거된 알림 및 알람을 검토하여 추가적인 통찰력을 얻을 수 있습니다.	• 현재 경고를 봅니다 • 레거시 알람을 봅니다 • 해결된 경고를 봅니다 • 과거 알람 및 알람 빈도 검토(레거시 시스템)
이벤트를 모니터링합니다	이벤트에는 네트워크 오류와 같은 오류를 포함하여 노드에 대한 시스템 오류 또는 장애 이벤트가 포함됩니다. 이벤트를 모니터링하여 문제에 대해 자세히 알아보거나 문제 해결에 도움을 받으십시오.	• 이벤트를 모니터링합니다
차트 및 텍스트 보고서를 사용하여 추세를 식별합니다	동향은 문제가 처음 나타난 시기에 대한 중요한 단서가 될 수 있으며, 상황이 얼마나 빠르게 변화하는지 이해하는 데 도움이 될 수 있습니다.	• 차트와 그래프를 사용합니다 • 텍스트 보고서를 사용합니다
기준 설정	다양한 운영 값의 일반 수준에 대한 정보를 수집합니다. 이러한 기준 값과 이러한 기준선에서 벗어난 값들은 유용한 단서를 제공할 수 있습니다.	• 기준 설정
수집 및 검색 테스트 수행	수집 및 검색과 관련된 성능 문제를 해결하려면 워크스테이션을 사용하여 오브젝트를 저장하고 검색합니다. 클라이언트 응용 프로그램을 사용할 때 표시되는 결과와 결과를 비교합니다.	• PUT 모니터링 및 성능 확보
감사 메시지를 검토합니다	감사 메시지를 검토하여 StorageGRID 작업에 대해 자세히 설명합니다. 감사 메시지의 세부 정보는 성능 문제를 비롯한 다양한 유형의 문제를 해결하는 데 유용할 수 있습니다.	• 감사 메시지를 검토합니다

수집할 데이터의 유형입니다	이 데이터를 수집하는 이유	지침
오브젝트 위치 및 스토리지 무결성을 점검하십시오	스토리지에 문제가 있는 경우 오브젝트가 원하는 위치에 배치되었는지 확인합니다. 스토리지 노드에서 객체 데이터의 무결성을 점검하십시오.	• 개체 검증 작업을 모니터링합니다 • 객체 데이터 위치를 확인합니다 • 개체 무결성을 확인합니다
기술 지원을 위한 데이터 수집	기술 지원 부서에서 문제 해결을 위해 데이터를 수집하거나 특정 정보를 검토하도록 요청할 수 있습니다.	• 로그 파일 및 시스템 데이터를 수집합니다 • AutoSupport 메시지를 수동으로 트리거합니다 • 지원 메트릭을 검토합니다

최근 변경 내용의 타임라인을 만듭니다

문제가 발생하면 최근에 변경된 내용과 변경된 시기를 고려해야 합니다.

- StorageGRID 시스템, 구성 또는 환경을 변경하면 새로운 동작이 발생할 수 있습니다.
- 변경 일정을 사용하면 어떤 변경 사항이 문제에 대해 어떤 영향을 미칠 수 있는지, 그리고 각 변경이 개발에 어떤 영향을 미쳤는지 파악할 수 있습니다.

각 변경이 발생한 시기 및 변경에 대한 관련 세부 정보, 변경이 진행 중인 동안 발생한 다른 작업에 대한 정보가 포함된 시스템의 최근 변경 사항 테이블을 만듭니다.

변경 시간	변경 유형	세부 정보
예를 들면 다음과 같습니다. • 노드 복구를 언제 시작했습니까? • 소프트웨어 업그레이드가 언제 완료되었습니까? • 프로세스를 중단했습니까?	무슨 일이 있었죠? 무엇을 했습니까?	변경에 관한 모든 관련 세부 사항을 문서화합니다. 예를 들면 다음과 같습니다. • 네트워크 변경에 대한 세부 정보. • 설치된 핫픽스가 무엇입니까? • 클라이언트 워크로드가 어떻게 변경되었는지 나타냅니다. 동시에 두 개 이상의 변경이 발생했는지 확인하십시오. 예를 들어, 업그레이드가 진행되는 동안 변경된 사항은 무엇입니까?

최근 주요 변경 사항의 예

다음은 잠재적으로 중요한 변경 사항의 몇 가지 예입니다.

- StorageGRID 시스템이 최근에 설치, 확장 또는 복구되었습니까?
- 최근에 시스템을 업그레이드했습니까? 핫픽스가 적용되었습니까?
- 최근에 수리 또는 변경된 하드웨어가 있습니까?
- ILM 정책이 업데이트되었습니까?
- 클라이언트 워크로드가 변경되었습니까?
- 클라이언트 응용 프로그램 또는 해당 동작이 변경되었습니까?
- 로드 밸런서를 변경했거나 관리 노드 또는 게이트웨이 노드의 고가용성 그룹을 추가 또는 제거했습니까?
- 완료하는 데 시간이 오래 걸릴 수 있는 작업이 시작되었습니까? 예를 들면 다음과 같습니다.
  - 장애가 발생한 스토리지 노드 복구
  - 스토리지 노드 사용 중지
- 테넌트 추가 또는 LDAP 구성 변경과 같은 사용자 인증이 변경되었습니까?
- 데이터 마이그레이션이 진행됩니까?
- 플랫폼 서비스가 최근에 활성화 또는 변경되었습니까?
- 최근에 규정 준수를 활성화했습니까?
- Cloud Storage Pool이 추가 또는 제거되었습니까?
- 스토리지 압축 또는 암호화에 대한 변경 사항이 있습니까?
- 네트워크 인프라에 변화가 있었습니까? 예를 들어 VLAN, 라우터 또는 DNS가 있습니다.
- NTP 소스를 변경했습니까?
- 그리드, 관리자 또는 클라이언트 네트워크 인터페이스가 변경되었습니까?
- 아카이브 노드에 대한 구성 변경 사항이 있습니까?
- StorageGRID 시스템 또는 환경에 다른 변경 사항이 있습니까?

초기 계획을 설정합니다

다양한 운영 값의 일반 레벨을 기록하여 시스템의 기준을 설정할 수 있습니다. 향후 현재 값을 이러한 기준선과 비교하여 비정상 값을 감지하고 해결할 수 있습니다.

속성	값	얻는 방법
평균 스토리지 소비량	GB 사용량/일 소비 비율/일	그리드 관리자로 이동합니다. 노드 페이지에서 전체 그리드 또는 사이트를 선택하고 스토리지 탭으로 이동합니다. Storage Used - Object Data 차트에서 라인이 상당히 안정적인 기간을 찾습니다. 차트 위에 커서를 올려 놓으면 매일 얼마나 많은 스토리지가 사용되는지를 추정할 수 있습니다 전체 시스템 또는 특정 데이터 센터에 대해 이 정보를 수집할 수 있습니다.
평균 메타데이터 사용	GB 사용량/일 소비 비율/일	그리드 관리자로 이동합니다. 노드 페이지에서 전체 그리드 또는 사이트를 선택하고 스토리지 탭으로 이동합니다. 사용된 스토리지 - 객체 메타데이터 차트에서 라인이 상당히 안정적인 기간을 찾습니다. 차트 위에 커서를 올려 놓으면 매일 메타데이터 스토리지가 얼마나 소모되는지를 추정할 수 있습니다 전체 시스템 또는 특정 데이터 센터에 대해 이 정보를 수집할 수 있습니다.
S3/Swift 작업의 속도입니다	작업/초	Grid Manager에서 대시보드로 이동합니다. 프로토콜 작업 섹션에서 S3 속도 및 Swift 속도의 값을 확인합니다. 특정 사이트 또는 노드에 대한 수집 및 검색 속도 및 카운트를 보려면 * 노드 * > * _ 사이트 또는 스토리지 노드 _ * > * 개체 * 를 선택합니다. S3 또는 Swift에 대한 Ingest 및 Retrieve 차트 위에 커서를 놓습니다.
S3/Swift 작업에 실패했습니다	운영	지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. API Operations 섹션의 Overview 탭에서 S3 Operations - Failed 또는 Swift Operations - Failed 값을 확인합니다.

속성	값	얻는 방법
ILM 평가 비율	개체/초	노드 페이지에서 **GRID* * > * ILM * 을 선택합니다. ILM 대기열 차트에서 라인이 상당히 안정적인 기간을 찾습니다. 차트 위에 커서를 올려 놓으면 시스템의 * 평가 비율 * 에 대한 기준값이 추정됩니다.
ILM 스캔 속도	개체/초	nodes * > **grid* * > * ILM * 을 선택합니다. ILM 대기열 차트에서 라인이 상당히 안정적인 기간을 찾습니다. 차트 위에 커서를 올려 놓으면 * 시스템의 * 스캔 속도 * 에 대한 기준값이 추정됩니다.
클라이언트 작업에서 대기 중인 객체입니다	개체/초	nodes * > **grid* * > * ILM * 을 선택합니다. ILM 대기열 차트에서 라인이 상당히 안정적인 기간을 찾습니다. 커서를 차트 위에 올려 놓으면 * 클라이언트 작업에서 대기열에 있는 객체 * 에 대한 기준 값이 추정됩니다.
평균 쿼리 지연 시간입니다	밀리초	노드 * > *스토리지 노드 * > * 오브젝트 * 를 선택합니다. 쿼리 테이블에서 평균 지연 시간 값을 확인합니다.

데이터 분석

수집한 정보를 사용하여 문제의 원인과 잠재적인 해결책을 파악합니다.

분석은 문제에 따라 다르지만 일반적으로 다음과 같습니다.

- 알람을 사용하여 장애 지점 및 병목 지점을 찾습니다.
- 알람 기록 및 차트를 사용하여 문제 기록을 재구성합니다.
- 차트를 사용하여 이상 징후를 찾고 문제 상황을 정상 작동과 비교합니다.

에스컬레이션 정보 체크리스트

직접 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오. 기술 지원에 문의하기 전에 문제 해결을 위해 다음 표에 나열된 정보를 수집하십시오.

✔	항목	참고
	문제 설명	문제 증상은 무엇입니까? 문제가 언제 시작되었습니까? 일관성 또는 간헐적으로 발생합니까? 간헐적으로 발생하는 경우 몇 번 발생했습니까? 문제를 정의합니다
	영향 평가	문제의 심각성은 무엇입니까? 클라이언트 애플리케이션에 미치는 영향은 무엇입니까? • 이전에 클라이언트가 성공적으로 연결되었습니까? • 클라이언트가 데이터를 수집, 검색 및 삭제할 수 있습니까?
	StorageGRID 시스템 ID입니다	유지 관리 * > * 시스템 * > * 라이센스 * 를 선택합니다. StorageGRID 시스템 ID는 현재 라이센스의 일부로 표시됩니다.
	소프트웨어 버전	그리드 관리자 상단에서 도움말 아이콘을 선택하고 * 정보 * 를 선택하여 StorageGRID 버전을 확인합니다.
	맞춤화	StorageGRID 시스템의 구성 방법을 요약합니다. 예를 들어 다음을 나열합니다. • 그리드에서 스토리지 압축, 스토리지 암호화 또는 규정 준수를 사용합니까? • ILM이 복제된 또는 삭제 코딩 오브젝트를 만들어집니까? ILM이 사이트 중복을 보장합니까? ILM 규칙이 Strict, Balanced 또는 Dual Commit 수집 동작을 사용합니까?
	로그 파일 및 시스템 데이터	시스템에 대한 로그 파일 및 시스템 데이터를 수집합니다. 지원 * > * 도구 * > * 로그 * 를 선택합니다. 전체 그리드 또는 선택한 노드에 대한 로그를 수집할 수 있습니다. 선택한 노드에 대해서만 로그를 수집하는 경우 ADC 서비스가 있는 스토리지 노드를 하나 이상 포함해야 합니다. (사이트의 처음 세 개의 스토리지 노드에는 ADC 서비스가 포함됩니다.) 로그 파일 및 시스템 데이터를 수집합니다

✔	항목	참고
	기준선 정보	수집 작업, 검색 작업 및 스토리지 사용에 대한 기본 정보를 수집합니다. 기준 설정
	최근 변경 시간 표시 막대	시스템 또는 해당 환경의 최근 변경 사항을 요약하는 일정을 만듭니다. 최근 변경 내용의 시간 표시 막대를 만듭니다
	문제를 진단하기 위한 노력 이력	문제를 직접 진단하거나 해결하기 위한 단계를 수행한 경우 수행한 단계와 결과를 기록해야 합니다.

오브젝트 및 스토리지 문제를 해결합니다

객체 데이터 위치를 확인합니다

문제에 따라 오브젝트 데이터가 저장되는 위치를 확인할 수 있습니다. 예를 들어, ILM 정책이 예상대로 수행되고 있고 대상 데이터가 원하는 위치에 저장되어 있는지 확인해야 할 수 있습니다.

필요한 것

- 다음 중 하나의 개체 식별자가 있어야 합니다.
  - * UUID *: 객체의 범용 고유 식별자입니다. UUID를 모두 대문자로 입력합니다.
  - * CBID *: StorageGRID 내에서 개체의 고유 식별자입니다. 감사 로그에서 개체의 CBID를 가져올 수 있습니다. CBID를 모두 대문자로 입력합니다.
  - * S3 버킷 및 오브젝트 키 *: S3 인터페이스를 통해 오브젝트를 수집하면 클라이언트 애플리케이션이 버킷과 오브젝트 키 조합을 사용하여 오브젝트를 저장하고 식별합니다.
  - * Swift 컨테이너 및 오브젝트 이름 *: Swift 인터페이스를 통해 오브젝트가 수집되면 클라이언트 애플리케이션이 컨테이너 및 오브젝트 이름 조합을 사용하여 오브젝트를 저장하고 식별합니다.

단계

1. ILM * > * 개체 메타데이터 조회 * 를 선택합니다.
2. 식별자 * 필드에 개체의 식별자를 입력합니다.

   UUID, CBID, S3 버킷/오브젝트 키 또는 Swift 컨테이너/오브젝트 이름을 입력할 수 있습니다.

3. 개체의 특정 버전을 조회하려면 버전 ID(선택 사항)를 입력합니다.

4. Look Up * 을 선택합니다.

   개체 메타데이터 조회 결과가 나타납니다. 이 페이지에는 다음 유형의 정보가 나열됩니다.

   - 객체 ID(UUID), 버전 ID(선택 사항), 객체 이름, 컨테이너 이름, 테넌트 계정 이름 또는 ID, 객체의 논리적 크기, 객체를 처음 생성한 날짜 및 시간, 객체를 마지막으로 수정한 날짜 및 시간을 비롯한 시스템 메타데이터
   - 객체와 연결된 모든 사용자 메타데이터 키 값 쌍입니다.
   - S3 오브젝트의 경우 오브젝트와 연결된 오브젝트 태그 키 값 쌍이 됩니다.
   - 복제된 오브젝트 복사본의 경우 각 복제본의 현재 스토리지 위치입니다.
   - 삭제 코딩 오브젝트 복사본의 경우 각 분절의 현재 스토리지 위치입니다.
   - 클라우드 스토리지 풀의 오브젝트 복사본의 경우 외부 버킷의 이름 및 오브젝트의 고유 식별자를 비롯한 오브젝트의 위치가 포함됩니다.
   - 분할된 오브젝트 및 다중 파트 오브젝트의 경우 세그먼트 식별자 및 데이터 크기를 포함한 오브젝트 세그먼트 목록입니다. 세그먼트가 100개를 초과하는 오브젝트의 경우 처음 100개의 세그먼트만 표시됩니다.
   - 처리되지 않은 내부 스토리지 형식의 모든 오브젝트 메타데이터 이 원시 메타데이터에는 릴리즈부터 릴리즈까지 유지되지 않는 내부 시스템 메타데이터가 포함됩니다.

     다음 예는 2개의 복제된 복사본으로 저장된 S3 테스트 개체에 대한 오브젝트 메타데이터 조회 결과를 보여줍니다.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


관련 정보

ILM을 사용하여 개체를 관리합니다

S3을 사용합니다

Swift를 사용합니다

오브젝트 저장소(스토리지 볼륨) 장애가 발생했습니다

스토리지 노드의 기본 스토리지는 오브젝트 저장소로 나뉩니다. 오브젝트 저장소는 스토리지 볼륨이라고도 합니다.

각 스토리지 노드에 대한 오브젝트 저장소 정보를 볼 수 있습니다. 오브젝트 저장소는 * 노드 * > *스토리지 노드 * > * 스토리지 * 페이지 하단에 표시됩니다.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

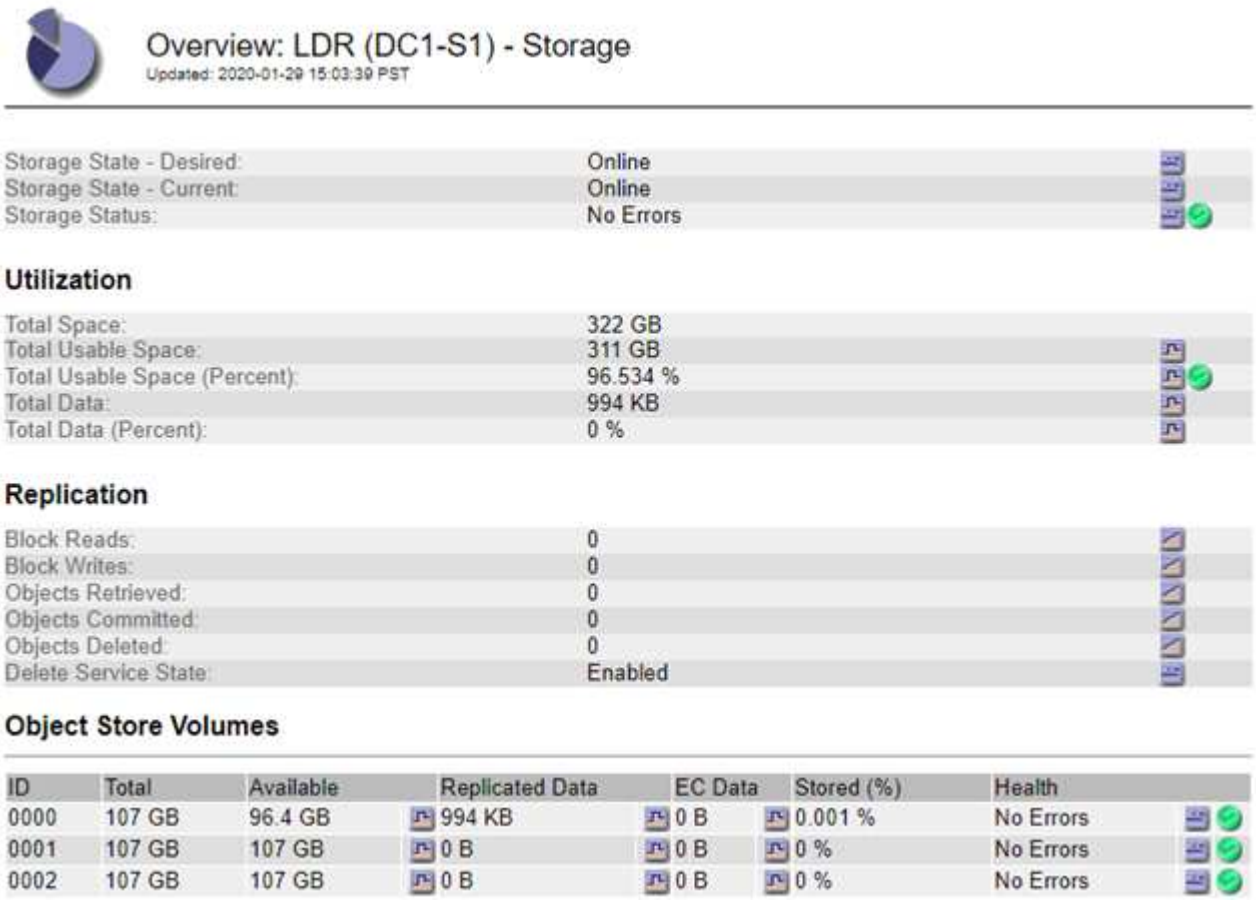
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

각 스토리지 노드에 대한 자세한 내용을 보려면 다음 단계를 수행하십시오.

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. site_ * > **Storage Node* * > * LDR * > * Storage * > * Overview * > * Main * 을 선택합니다.



장애의 특성에 따라 스토리지 볼륨의 장애가 스토리지 상태 또는 오브젝트 저장소 상태에 대한 알람에 반영될 수 있습니다. 스토리지 볼륨에 장애가 발생하면 장애가 발생한 스토리지 볼륨을 복구하여 스토리지 노드를 최대한 빨리 전체 기능으로 복원해야 합니다. 필요한 경우 * 구성 * 탭으로 이동하여 스토리지 노드를 읽기 전용 상태로 배치하여 StorageGRID 시스템이 서버의 전체 복구를 준비하는 동안 데이터 검색에 사용할 수 있도록 합니다.

관련 정보

복구 및 유지 관리

개체 무결성을 확인합니다

StorageGRID 시스템은 스토리지 노드에서 오브젝트 데이터의 무결성을 확인하여 손상되거나 누락된 오브젝트가 없는지 확인합니다.

검증 프로세스에는 두 가지가 있습니다. 백그라운드 검증 및 개체 존재 확인(이전의 포그라운드 검증)입니다. 이 두 구성 모두 함께 작동하여 데이터 무결성을 보장합니다. 백그라운드 검증이 자동으로 실행되고 개체 데이터의 정확성을 지속적으로 확인합니다. 개체의 존재 여부를 보다 빠르게 확인하기 위해 사용자가 개체 존재 여부를 확인할 수 있습니다(정확성은 아님).

백그라운드 검증이란 무엇입니까?

백그라운드 검증 프로세스는 스토리지 노드에서 손상된 오브젝트 데이터 복사본을 자동으로 지속적으로 검사하고 발견한 문제를 자동으로 복구합니다.

백그라운드 검증 에서는 다음과 같이 복제된 오브젝트와 삭제 코딩 오브젝트의 무결성을 검사합니다.

- * 복제된 객체 *: 백그라운드 검증 프로세스에서 손상된 복제된 객체가 발견되면 손상된 복제본이 해당 위치에서 제거되고 스토리지 노드의 다른 곳에서 격리됩니다. 그런 다음 손상되지 않은 새 복사본이 생성되어 활성 ILM 정책을 충족하도록 배치됩니다. 새 복제본이 원래 복제본에 사용된 스토리지 노드에 배치되지 않을 수 있습니다.

> 손상된 개체 데이터가 시스템에서 삭제되지 않고 격리되므로 계속 액세스할 수 있습니다. 격리된 객체 데이터에 액세스하는 방법에 대한 자세한 내용은 기술 지원 팀에 문의하십시오.

- * 삭제 코딩 오브젝트 *: 백그라운드 검증 프로세스에서 삭제 코딩 오브젝트의 조각이 손상된 것을 감지하면 StorageGRID는 나머지 데이터 및 패리티 조각을 사용하여 동일한 스토리지 노드에 누락된 조각을 자동으로 재구축하려고 시도합니다. 손상된 조각을 다시 만들 수 없는 경우 개체의 다른 복사본을 가져오려고 시도합니다. 가져오기가 성공하면 삭제 코딩 개체의 대체 복사본을 만들기 위해 ILM 평가가 수행됩니다.

  백그라운드 검증 프로세스는 스토리지 노드의 객체만 확인합니다. 아카이브 노드 또는 클라우드 스토리지 풀에서 객체를 확인하지 않습니다. 백그라운드 검증을 받으려면 객체가 4일 이상이어야 합니다.

백그라운드 검증은 일반적인 시스템 활동을 방해하지 않도록 설계된 연속 속도로 실행됩니다. 백그라운드 검증을 중지할 수 없습니다. 그러나 문제가 의심될 경우 백그라운드 검증 속도를 높여 스토리지 노드의 내용을 더 빠르게 확인할 수 있습니다.

백그라운드 검증과 관련된 경고 및 알람(레거시

손상된 개체가 시스템에서 자동으로 수정할 수 없는 것을 감지하면(손상으로 인해 개체가 식별되지 않음) * 식별되지 않은 손상된 개체가 감지됨 * 경고가 트리거됩니다.

다른 복사본을 찾을 수 없기 때문에 백그라운드 검증이 손상된 개체를 대체할 수 없는 경우 * Objects Lost * 경고가 트리거됩니다.

백그라운드 검증 비율을 변경합니다

데이터 무결성에 대한 우려가 있는 경우 백그라운드 검증이 스토리지 노드에서 복제된 오브젝트 데이터를 검사하는 속도를 변경할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

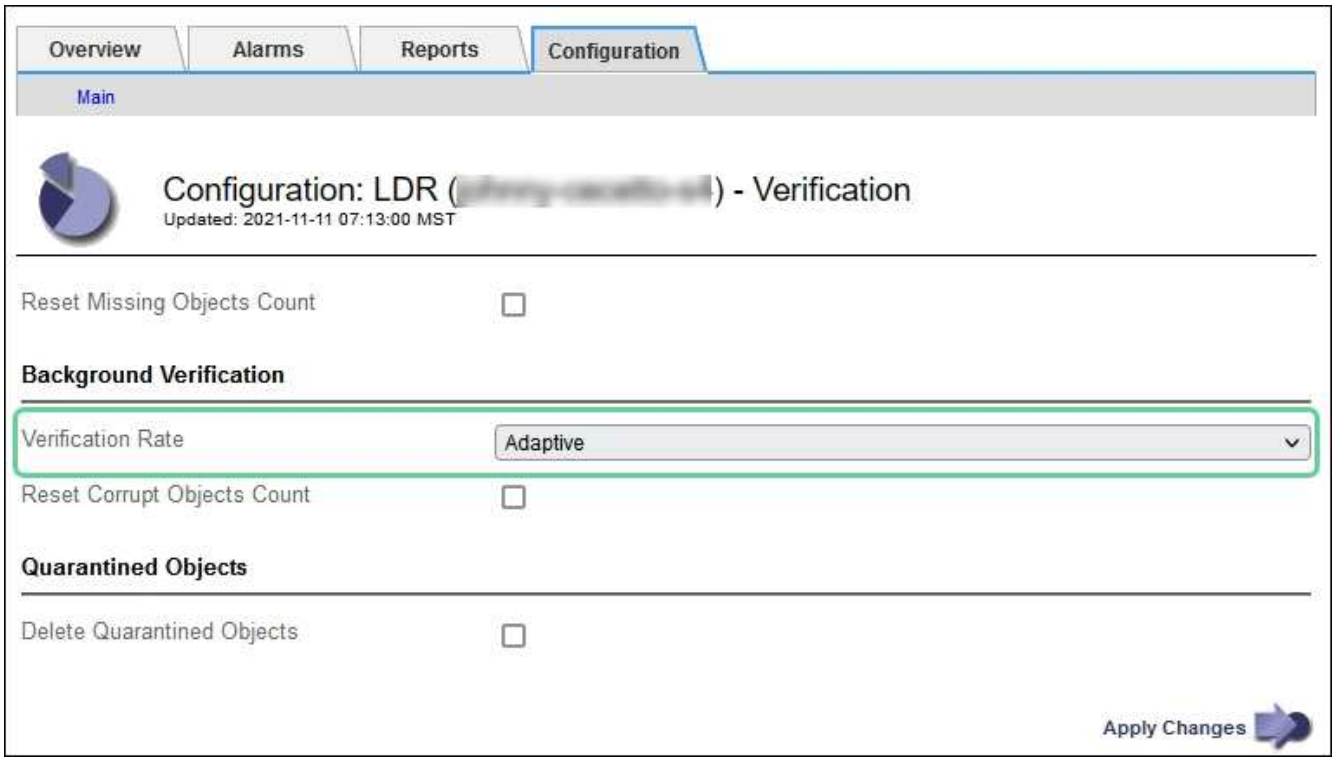
스토리지 노드에서 백그라운드 검증을 위한 검증 비율을 변경할 수 있습니다.

- 적응: 기본 설정. 이 작업은 최대 4MB/s 또는 10개의 오브젝트/s(둘 중 먼저 초과되는 값)에서 확인하도록 설계되었습니다.
- 높음: 일반적인 시스템 작업을 느리게 할 수 있는 속도로 스토리지 검증이 빠르게 진행됩니다.

하드웨어 또는 소프트웨어 오류로 인해 오브젝트 데이터가 손상되었을 수 있다고 의심되는 경우에만 높은 확인 속도를 사용하십시오. 우선 순위가 높은 백그라운드 검증이 완료되면 검증 속도가 자동으로 적응(Adaptive)으로 재설정됩니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. 스토리지 노드 * > * LDR * > * 검증 * 을 선택합니다.
3. Configuration * > * Main * 을 선택합니다.
4. LDR * > * 검증 * > * 구성 * > * 주 * 로 이동합니다.
5. Background Verification(배경 검증) 아래에서 * Verification Rate(검증 비율) * > * High(높음) * 또는 * Verification Rate(검증 비율) * > * Adaptive * 를 선택합니다.



> Verification Rate(확인 속도)를 High(높음)로 설정하면 통지 수준에서 VPRI(검증 비율) 레거시 경보가 트리거됩니다.

6. 변경 내용 적용 * 을 클릭합니다.
7. 복제된 객체에 대한 백그라운드 검증 결과를 모니터링합니다.
   a. 노드 * > *스토리지 노드 * > * 개체 * 로 이동합니다.
   b. 확인 섹션에서 * 손상된 개체 * 및 * 식별되지 않은 개체 * 에 대한 값을 모니터링합니다.

      백그라운드 확인이 손상된 복제된 개체 데이터를 찾으면 * 손상된 개체 * 메트릭이 증가하고 StorageGRID는 다음과 같이 데이터에서 개체 식별자를 추출하려고 시도합니다.

      - 개체 식별자를 추출할 수 있는 경우 StorageGRID는 개체 데이터의 새 복사본을 자동으로 만듭니다. 활성 ILM 정책을 충족하는 StorageGRID 시스템의 모든 위치에서 새 복사본을 만들 수 있습니다.
      - 개체 식별자가 손상되어 추출할 수 없는 경우 * 손상된 개체 식별되지 않음 * 메트릭이 증가하고 * 식별되지 않은 손상된 개체 감지됨 * 경고가 트리거됩니다.

c. 손상된 복제된 개체 데이터가 발견되면 기술 지원 부서에 문의하여 손상의 근본 원인을 확인하십시오.

8. 삭제 코딩 개체에 대한 백그라운드 검증 결과를 모니터링합니다.

   백그라운드 검증이 삭제 코딩 오브젝트 데이터의 손상된 조각을 찾으면 손상된 조각 감지됨 속성이 증가합니다. StorageGRID는 동일한 스토리지 노드에 손상된 부분을 재생성하여 복구합니다.

   a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
   b. 스토리지 노드 * > * LDR * > * 삭제 코딩 * 을 선택합니다.
   c. Verification Results 테이블에서 손상된 조각 감지(ECCD) 속성을 모니터링합니다.

9. 손상된 개체가 StorageGRID 시스템에 의해 자동으로 복구된 후 손상된 개체의 수를 재설정합니다.
   a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
   b. 스토리지 노드 * > * LDR * > * 검증 * > * 구성 * 을 선택합니다.
   c. 손상된 개체 수 재설정 * 을 선택합니다.
   d. 변경 내용 적용 * 을 클릭합니다.

10. 격리된 객체가 필요하지 않은 것으로 확신하면 삭제할 수 있습니다.

   개체 손실 * 경고 또는 손실된(개체 손실) 레거시 경보가 트리거된 경우 기술 지원 부서에서 격리된 개체에 액세스하여 기본 문제를 디버깅하거나 데이터 복구를 시도할 수 있습니다.

   a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
   b. 스토리지 노드 * > * LDR * > * 검증 * > * 구성 * 을 선택합니다.
   c. 격리된 개체 삭제 * 를 선택합니다.
   d. Apply Changes * 를 선택합니다.

개체 존재 확인이란 무엇입니까**?**

오브젝트 존재 여부는 스토리지 노드에 예상되는 모든 오브젝트 복제 복사본과 삭제 코딩 조각이 있는지 확인합니다. 개체 존재 확인은 개체 데이터 자체를 확인하지 않습니다(백그라운드 검증에서 확인). 대신 스토리지 디바이스의 무결성을 확인하는 방법을 제공합니다. 특히 최근 하드웨어 문제로 인해 데이터 무결성이 영향을 받을 수 있는 경우 더욱 그렇습니다.

자동으로 발생하는 백그라운드 확인과는 달리 개체 존재 확인 작업을 수동으로 시작해야 합니다.

오브젝트 존재 확인 은 StorageGRID에 저장된 모든 오브젝트의 메타데이터를 읽고 복제 오브젝트 복사본과 삭제 코딩 오브젝트 조각의 존재 여부를 확인합니다. 누락된 데이터는 다음과 같이 처리됩니다.

- * 복제된 복사본 *: 복제된 개체 데이터의 복사본이 누락된 경우 StorageGRID는 자동으로 시스템의 다른 위치에 저장된 복사본에서 복사본을 교체하려고 시도합니다. 스토리지 노드는 ILM 평가를 통해 기존 복사본을 실행합니다. 그러면 다른 복사본이 없기 때문에 현재 ILM 정책이 이 개체에 대해 더 이상 충족되지 않는 것으로 결정됩니다. 시스템의 활성 ILM 정책을 충족하기 위해 새 복사본이 생성되고 배치됩니다. 이 새 사본은 누락된 사본이 저장된 동일한 위치에 배치되지 않을 수 있습니다.
- * 삭제 코딩 단편 *: 삭제 코딩 오브젝트의 조각이 누락된 경우 StorageGRID는 나머지 조각을 사용하여 동일한 스토리지 노드에 누락된 조각을 자동으로 재구축합니다. 누락된 조각을 다시 생성할 수 없는 경우(너무 많은 조각이 손실되었기 때문에) ILM은 오브젝트의 다른 복사본을 찾으려고 시도합니다. 이 복사본은 새로운 삭제 코딩 조각을 생성하는 데 사용할 수 있습니다.

개체 존재 확인 실행

한 번에 하나의 개체 존재 확인 작업을 만들고 실행할 수 있습니다. 작업을 생성할 때 확인할 스토리지 노드 및 볼륨을 선택합니다. 작업의 정합성 제어도 선택합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 확인할 스토리지 노드가 온라인 상태인지 확인했습니다. 노드 테이블을 보려면 * nodes * 를 선택합니다. 확인할 노드의 노드 이름 옆에 알림 아이콘이 나타나지 않는지 확인합니다.
- 확인할 노드에서 다음 절차가 * 실행되지 않음 * 인지 확인했습니다.
  - 스토리지 노드를 추가하기 위한 그리드 확장
  - 스토리지 노드 서비스 해제
  - 장애가 발생한 스토리지 볼륨 복구
  - 장애가 발생한 시스템 드라이브로 스토리지 노드 복구
  - EC 재조정
  - 어플라이언스 노드 클론

개체 존재 여부 검사는 이러한 절차가 진행 중인 동안에는 유용한 정보를 제공하지 않습니다.

이 작업에 대해

오브젝트 존재 확인 작업은 그리드의 오브젝트 수, 선택한 스토리지 노드 및 볼륨 및 선택한 일관성 제어에 따라 완료하는 데 며칠 또는 몇 주가 걸릴 수 있습니다. 한 번에 하나의 작업만 실행할 수 있지만 여러 스토리지 노드와 볼륨을 동시에 선택할 수 있습니다.

단계

1. 유지보수 * > * 작업 * > * 개체 존재 확인 * 을 선택합니다.
2. 작업 생성 * 을 선택합니다. 개체 존재 확인 작업 생성 마법사가 나타납니다.
3. 확인할 볼륨이 포함된 노드를 선택합니다. 모든 온라인 노드를 선택하려면 열 머리글에서 * 노드 이름 * 확인란을 선택합니다.

   노드 이름 또는 사이트별로 검색할 수 있습니다.

   그리드에 연결되지 않은 노드는 선택할 수 없습니다.

4. Continue * 를 선택합니다.
5. 목록의 각 노드에 대해 하나 이상의 볼륨을 선택합니다. 스토리지 볼륨 번호 또는 노드 이름을 사용하여 볼륨을 검색할 수 있습니다.

   선택한 각 노드의 모든 볼륨을 선택하려면 열 머리글에서 * 스토리지 볼륨 * 확인란을 선택합니다.

6. Continue * 를 선택합니다.
7. 작업의 정합성 제어를 선택합니다.

   일관성 컨트롤은 개체 존재 여부를 확인하는 데 사용되는 개체 메타데이터의 복사본 수를 결정합니다.

- * 강력한 사이트 *: 단일 사이트에 메타데이터 복사본 2개
- * 강력한 글로벌 *: 각 사이트에 메타데이터 복사본 2개
- * 모두 * (기본값): 각 사이트에 있는 세 개의 메타데이터 복사본 모두

  일관성 제어에 대한 자세한 내용은 마법사의 설명을 참조하십시오.

8. Continue * 를 선택합니다.
9. 선택 항목을 검토하고 확인합니다. 이전 * 을 선택하여 마법사의 이전 단계로 이동하여 선택 사항을 업데이트할 수 있습니다.

   개체 존재 확인 작업이 생성되고 다음 중 하나가 발생할 때까지 실행됩니다.

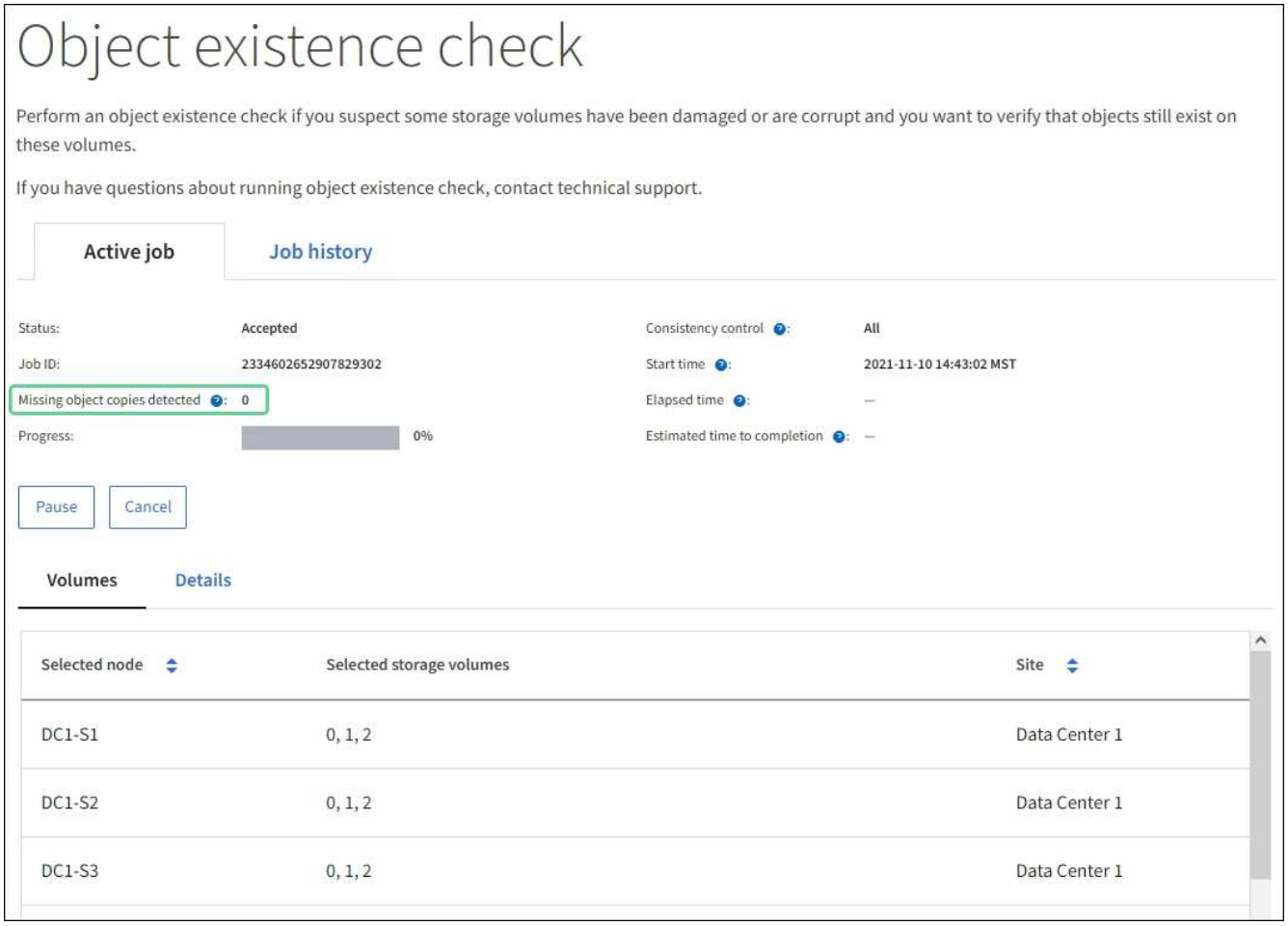
   - 작업이 완료됩니다.
   - 작업을 일시 중지하거나 취소합니다. 일시 중지한 작업은 다시 시작할 수 있지만 취소한 작업은 다시 시작할 수 없습니다.
   - 작업이 멈춥니다. Object existence check has Stallered * 경고가 트리거됩니다. 경고에 지정된 수정 조치를 따릅니다.
   - 작업이 실패합니다. 개체 존재 확인 실패 * 경고가 트리거됩니다. 경고에 지정된 수정 조치를 따릅니다.
   - '서비스를 사용할 수 없음' 또는 '내부 서버 오류' 메시지가 나타납니다. 1분 후 페이지를 새로 고쳐 작업을 계속 모니터링합니다.

   > 필요한 경우 개체 존재 확인 페이지에서 벗어나 작업을 계속 모니터링하기 위해 돌아갈 수 있습니다.

10. 작업이 실행될 때 * 활성 작업 * 탭을 보고 감지된 누락된 오브젝트 복사본의 값을 기록합니다.

    이 값은 하나 이상의 누락된 조각이 있는 복제된 오브젝트 및 삭제 코딩 오브젝트의 누락된 총 수를 나타냅니다.

    감지된 누락된 객체 복제본 수가 100개를 초과하는 경우 스토리지 노드의 스토리지에 문제가 있을 수 있습니다.



11. 작업이 완료된 후 필요한 추가 작업을 수행합니다.
    - 감지된 누락된 개체 복사본이 0이면 문제를 찾을 수 없습니다. 별도의 조치가 필요하지 않습니다.
    - 감지된 누락된 개체 사본이 0보다 크고 * Objects Lost * 경고가 트리거되지 않은 경우 누락된 모든 복사본은 시스템에서 복구되었습니다. 향후 개체 복사본에 대한 손상을 방지하기 위해 하드웨어 문제가 해결되었는지 확인합니다.
    - 감지된 누락된 개체 사본이 0보다 크고 * 개체 손실 * 경고가 트리거되면 데이터 무결성이 영향을 받을 수 있습니다. 기술 지원 부서에 문의하십시오.
    - grep를 사용하여 LLST 감사 메시지 "grep LLST audit_file_name"을 추출하면 손실된 개체 복사본을 조사할 수 있습니다.

      이 절차는 의 절차와 유사합니다 분실된 물체를 조사 중입니다개체 사본의 경우 OLST 대신 "LLL ST"를 검색합니다.

12. 작업에 대한 강력한 사이트 또는 강력한 글로벌 일관성 제어를 선택한 경우 메타데이터 일관성을 위해 약 3주를 기다린 다음 동일한 볼륨에서 작업을 다시 실행합니다.

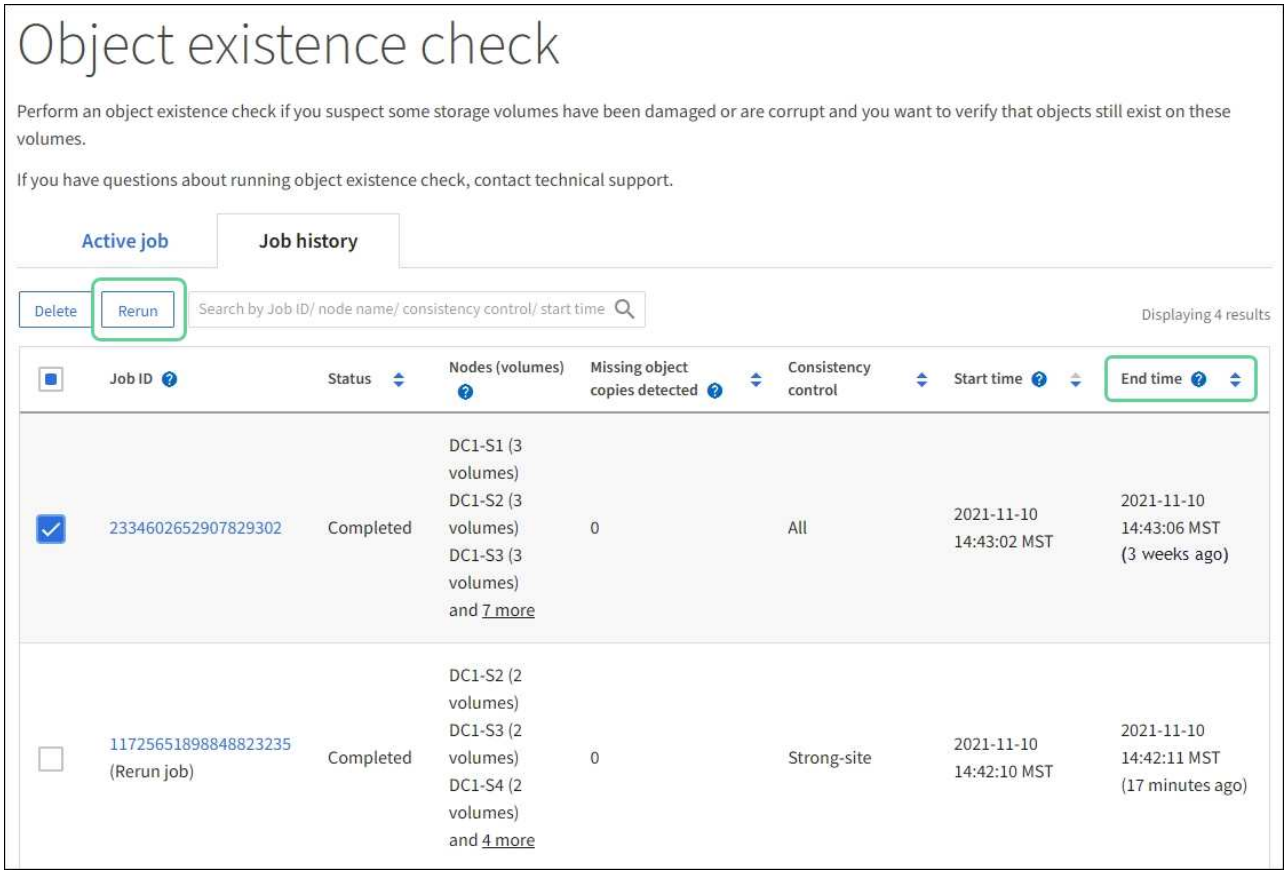
    StorageGRID가 작업에 포함된 노드와 볼륨의 메타데이터 일관성을 달성할 시간이 있는 경우, 작업을 다시 실행하면 잘못 보고된 누락된 오브젝트 복사본을 지우거나 누락된 경우 추가 오브젝트 복사본을 확인할 수 있습니다.

    a. 유지보수 * > * 개체 존재 확인 * > * 작업 내역 * 을 선택합니다.
    b. 재실행할 준비가 된 작업을 확인합니다.

i. 3주 전에 실행된 작업을 판별하려면 * 종료 시간 * 열을 확인하십시오.

ii. 이러한 작업의 경우 정합성 보장 제어 열에서 강력한 사이트 또는 강력한 글로벌 사이트를 검사합니다.

c. 재실행할 각 작업에 대한 확인란을 선택한 다음 * 재실행 * 을 선택합니다.



d. 작업 재실행 마법사에서 선택한 노드와 볼륨 및 정합성 제어를 검토합니다.

e. 작업을 다시 실행할 준비가 되면 * 재실행 * 을 선택합니다.

활성 작업 탭이 나타납니다. 선택한 모든 작업은 강력한 사이트의 일관성 제어에서 하나의 작업으로 다시 실행됩니다. 세부 정보 섹션의 * 관련 작업 * 필드에 원래 작업의 작업 ID가 나열됩니다.

작업을 마친 후

데이터 무결성에 대한 우려가 있는 경우 * 지원 * > * 도구 * > * 그리드 토폴로지 * > * _사이트 _ * > * _ 스토리지 노드 _ * > * LDR * > * 검증 * > * 구성 * > * 주 * 로 이동하여 배경 검증 비율을 높이십시오. 백그라운드 검사는 저장된 모든 개체 데이터의 정확성을 확인하고 발견된 문제를 모두 복구합니다. 가능한 한 빨리 잠재적 문제를 찾아 수리하면 데이터 손실의 위험이 감소합니다.

분실하거나 누락된 오브젝트 데이터 문제를 해결합니다

클라이언트 애플리케이션의 읽기 요청, 복제된 오브젝트 데이터의 백그라운드 검증, ILM 재평가, 스토리지 노드 복구 중 오브젝트 데이터 복원을 비롯한 여러 가지 이유로 오브젝트를 검색할 수 있습니다.

StorageGRID 시스템은 개체의 메타데이터에 있는 위치 정보를 사용하여 개체를 검색할 위치를 결정합니다. 개체의 복사본을 예상 위치에 찾을 수 없는 경우, ILM 정책에 개체 복사본을 둘 이상 만드는 규칙이 포함되어 있다고 가정하여 시스템이 시스템의 다른 위치에서 개체의 다른 복사본을 가져오려고 시도합니다.

이 검색이 성공하면 StorageGRID 시스템은 누락된 객체 복사본을 대체합니다. 그렇지 않으면 다음과 같이 * Objects Lost * 경고가 트리거됩니다.

- 복제된 복사본의 경우 다른 복사본을 검색할 수 없으면 개체가 손실된 것으로 간주되고 경고가 트리거됩니다.
- 삭제 코딩 사본의 경우, 예상 위치에서 복사본을 검색할 수 없는 경우 손상된 복사본 감지(ECOR) 속성은 다른 위치에서 복사본을 검색하기 전에 1씩 증가합니다. 다른 복사본을 찾을 수 없으면 경고가 트리거됩니다.

모든 * Objects Lost * 경고를 즉시 조사하여 손실의 근본 원인을 파악하고 객체가 여전히 오프라인 상태이거나 현재 사용할 수 없는 스토리지 노드 또는 아카이브 노드에 있는지 확인해야 합니다.

복사본 없이 오브젝트 데이터를 손실할 경우 복구 솔루션이 없습니다. 그러나 손실된 개체를 다시 설정하여 손실된 개체를 새로 마스킹하지 못하도록 해야 합니다.

관련 정보

손실된 개체를 조사합니다

분실 및 누락된 개체 수를 재설정합니다

손실된 개체를 조사합니다

Objects Lost * 경고가 트리거되면 즉시 조사해야 합니다. 영향을 받는 개체에 대한 정보를 수집하고 기술 지원 부서에 문의하십시오.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.

이 작업에 대해

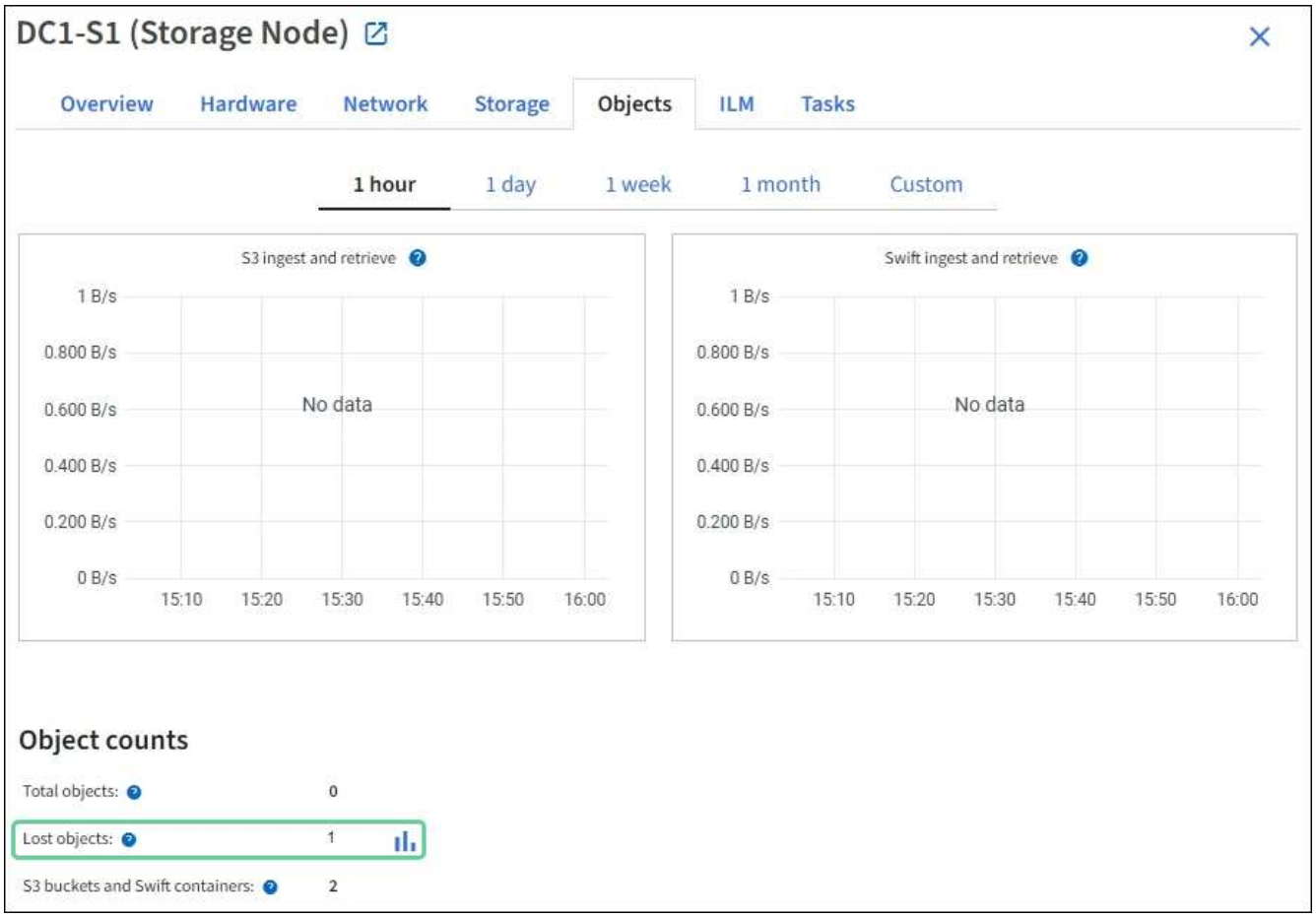
Objects Lost * 알림은 StorageGRID가 그리드에 개체의 복사본이 없다고 판단함을 나타냅니다. 데이터가 영구적으로 손실되었을 수 있습니다.

손실된 개체 경고를 즉시 조사합니다. 추가 데이터 손실을 방지하기 위해 조치를 취해야 할 수 있습니다. 경우에 따라 프롬프트 작업을 수행하면 손실된 개체를 복원할 수 있습니다.

단계

1. 노드 * 를 선택합니다.
2. 스토리지 노드 * > * 오브젝트 * 를 선택합니다.
3. 개체 수 표에 표시된 손실된 개체의 수를 검토합니다.

   이 숫자는 그리드 노드가 전체 StorageGRID 시스템에서 누락된 것으로 감지한 총 오브젝트 수를 나타냅니다. 값은 LDR 및 DDS 서비스 내에서 데이터 저장소 구성 요소의 손실된 개체 카운터의 합계입니다.



4. 관리 노드에서 감사 로그에 액세스하여 * Objects Lost * 경고를 트리거한 개체의 고유 식별자(UUID)를 확인합니다.
   a. 그리드 노드에 로그인합니다.
      i. ssh admin@grid_node_ip' 명령을 입력한다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다. 루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
   b. 감사 로그가 있는 디렉토리로 변경합니다. "cd /var/local/audit/export/"를 입력합니다
   c. grep를 사용하여 OLST(Object Lost) 감사 메시지를 추출합니다. 'grep OLST AUDIT_FILE_NAME'을 입력합니다
   d. 메시지에 포함된 UUID 값을 확인합니다.

```
>Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. "ObjectByUUID" 명령을 사용하여 ID(UUID)로 개체를 찾은 다음 데이터가 위험에 처하는지 확인합니다.

   a. LDR 콘솔에 액세스하려면 localhost 1402에 Telnet을 사용합니다.

   b. '/proc/OBRP/ObjectByUUID UUID UUID UUID_value'를 입력합니다

   이 첫 번째 예에서는 UUID 926026C4-00A4-449B-AC72-BCCA72DD1311이 있는 개체에 두 개의 위치가 나열되어 있습니다.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
```

```
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```


두 번째 예에서는 UUID 926026C4-00A4-449B-AC72-BCCA72DD1311이 있는 개체에 위치가 나열되지 않습니다.

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}
```

a. /proc/OBRP/ObjectByUUID의 출력을 검토하고 적절한 작업을 수행합니다.

메타데이터	결론
개체를 찾을 수 없음("오류":"")	개체를 찾을 수 없으면 "error":" 메시지가 반환됩니다. 개체를 찾을 수 없는 경우 * Objects Lost * 의 개수를 다시 설정하여 경고를 지울 수 있습니다. 개체가 없다는 것은 개체가 의도적으로 삭제되었음을 나타냅니다.
위치 > 0	출력에 표시된 위치가 있으면 * Objects Lost * 경고가 거짓 양수가 될 수 있습니다. 객체가 존재하는지 확인합니다. 출력에 나열된 노드 ID 및 파일 경로를 사용하여 개체 파일이 나열된 위치에 있는지 확인합니다. (의 절차 잠재적으로 손실된 개체를 검색합니다 노드 ID를 사용하여 올바른 스토리지 노드를 찾는 방법은 에 나와 있습니다.) 개체가 있는 경우 * Objects Lost * 의 개수를 다시 설정하여 경고를 지울 수 있습니다.
위치 = 0	출력에 나열된 위치가 없으면 개체가 누락될 수 있습니다. 시도할 수 있습니다 개체를 검색하고 복원합니다 직접 문의하거나 기술 지원 부서에 문의할 수 있습니다. 기술 지원 부서에서 진행 중인 스토리지 복구 절차가 있는지 확인하도록 요청할 수 있습니다. 즉, 모든 스토리지 노드에서 _repair-data_command가 실행되었으며 복구가 아직 진행 중입니까? 에 대한 정보를 참조하십시오 오브젝트 데이터를 스토리지 볼륨에 복원 중입니다.

관련 정보

감사 로그를 검토합니다

잠재적으로 손실된 개체를 검색하여 복원합니다

개체 손실(손실) 경보와 * 개체 손실 * 경고를 트리거하고 잠재적으로 분실된 것으로 식별된 개체를 찾아서 복원할 수 있습니다.

필요한 것

- "손실된 객체 조사"에서 식별된 대로 손실된 객체의 UUID가 있어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.

이 작업에 대해

이 절차에 따라 그리드의 다른 위치에서 손실된 개체의 복제된 복사본을 찾을 수 있습니다. 대부분의 경우 손실된 개체를 찾을 수 없습니다. 그러나 경우에 따라 즉각적인 조치를 취할 경우 손실된 복제 개체를 찾아 복원할 수 있습니다.

> 이 절차에 대한 지원은 기술 지원 부서에 문의하십시오.

단계

1. 관리 노드에서 감사 로그에서 가능한 객체 위치를 검색합니다.
   a. 그리드 노드에 로그인합니다.
      i. ssh admin@grid_node_ip' 명령을 입력한다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다. 루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
   b. 감사 로그가 있는 디렉토리로 변경합니다: 'cd /var/local/audit/export/'
   c. grep를 사용하여 잠재적으로 손실된 개체와 관련된 감사 메시지를 추출하고 출력 파일로 보냅니다. ' grep uuid-valueaudit_file_name > output_file_name ' 을 입력합니다

      예를 들면 다음과 같습니다.

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      messages_about_lost_object.txt
      ```

   d. grep를 사용하여 이 출력 파일에서 LLST(Location Lost) 감사 메시지를 추출합니다. 'grep LLST output_file_name'을 입력합니다

      예를 들면 다음과 같습니다.

      ```
      Admin: # grep LLST messages_about_lost_objects.txt
      ```

      LLST 감사 메시지는 이 샘플 메시지와 같습니다.

      ```
      [AUDT:\[NOID\(UI32\):12448208\][CBIL(UI64):0x38186FE53E3C49A5]
      [UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
      [PCLD\(CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
      [TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):
      1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
      SM]
      [ATID(UI64):7086871083190743409]]
      ```

   e. LLST 메시지에서 PCLD 필드와 noid 필드를 찾습니다.

      PCLD 값이 있는 경우 누락된 복제 객체 복사본에 대한 디스크의 전체 경로입니다. noid 값은 개체의 복사본을 찾을 수 있는 LDR의 노드 ID입니다.

      개체 위치를 찾으면 개체를 복원할 수 있습니다.

   f. 이 LDR 노드 ID의 스토리지 노드를 찾습니다.

      노드 ID를 사용하여 스토리지 노드를 찾는 방법에는 두 가지가 있습니다.

- Grid Manager에서 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 *데이터 센터 * > *스토리지 노드 * > * LDR * 을 선택합니다. LDR 노드 ID는 Node Information 테이블에 있습니다. 이 LDR을 호스팅하는 스토리지 노드를 찾을 때까지 각 스토리지 노드에 대한 정보를 검토하십시오.
- 그리드에 대한 복구 패키지를 다운로드하고 압축을 풉니다. 해당 패키지에 _\docs_directory가 있습니다. index.html 파일을 열면 서버 요약에 모든 그리드 노드의 모든 노드 ID가 표시됩니다.

2. 감사 메시지에 표시된 스토리지 노드에 객체가 있는지 확인합니다.
   a. 그리드 노드에 로그인합니다.
      i. ssh admin@grid_node_ip' 명령을 입력한다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

1. 개체의 파일 경로가 있는지 확인합니다.

객체의 파일 경로에 LLST 감사 메시지의 PCLD 값을 사용한다.

예를 들어 다음을 입력합니다.

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

- 참고 *: 특수 문자를 이스케이프하려면 항상 명령에서 개체 파일 경로를 작은따옴표로 묶어야 합니다.
- 개체 경로를 찾을 수 없으면 개체가 손실되어 이 절차를 사용하여 복원할 수 없습니다. 기술 지원 부서에 문의하십시오.
- 개체 경로가 발견되면 단계를 계속 진행합니다 개체를 StorageGRID 로 복원합니다. 검색된 객체를 다시 StorageGRID로 복원할 수 있습니다.
  a. 개체 경로가 발견되면 개체를 StorageGRID에 복원해 보십시오.
     i. 동일한 스토리지 노드에서 StorageGRID에서 관리할 수 있도록 객체 파일의 소유권을 변경합니다. 'chown LDR-user: bycast 'file_path_of_object"를 입력합니다
     ii. LDR 콘솔에 액세스하려면 localhost 1402에 Telnet을 사용합니다. telnet 0 1402 를 입력한다
     iii. 'cd/proc/Stor'를 입력합니다
     iv. 'Object_found' file_path_of_object"를 입력합니다

     예를 들어 다음을 입력합니다.

```
Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

+
"Object_found" 명령을 실행하면 오브젝트 위치를 그리드에 알린다. 또한 활성 ILM 정책을 트리거하여 정책에 지정된 대로 추가 복사본을 만듭니다.

- 참고 *: 객체를 찾은 스토리지 노드가 오프라인인 경우 온라인 상태인 스토리지 노드에 객체를 복사할 수 있습니다. 객체를 온라인 스토리지 노드의 /var/local/rangedb 디렉토리에 배치합니다. 그런 다음 객체의 파일 경로를 사용하여 'Object_found' 명령을 실행합니다.
  - 개체를 복원할 수 없으면 "Object_found" 명령이 실패합니다. 기술 지원 부서에 문의하십시오.
  - 개체가 StorageGRID로 복원되면 성공 메시지가 나타납니다. 예를 들면 다음과 같습니다.

```
ade 12448208: /proc/STOR > Object_Found
'/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
```

단계를 계속 진행합니다 새 위치가 생성되었는지 확인합니다

i. 객체가 StorageGRID에 성공적으로 복구되었으면 새 위치가 생성되었는지 확인합니다.

A. 'cd/proc/OBRP'를 입력한다

B. 'ObjectByUUID_value'를 입력합니다

다음 예에서는 UUID 926026C4-00A4-449B-AC72-BCCA72DD1311이 있는 개체의 위치가 두 가지임을 보여 줍니다.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
```

```
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```


1. LDR 콘솔에서 로그아웃합니다. 'exit'로 진입합니다
   a. 관리 노드에서 이 객체에 대한 ORLM 감사 메시지에 대한 감사 로그를 검색하여 ILM(정보 수명 주기 관리)이 필요에 따라 복제본을 배치했는지 확인합니다.
2. 그리드 노드에 로그인합니다.
   a. ssh admin@grid_node_ip' 명령을 입력한다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다. 루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
3. 감사 로그가 있는 디렉토리로 변경합니다: 'cd /var/local/audit/export/'
4. grep를 사용하여 개체와 관련된 감사 메시지를 출력 파일에 추출합니다. ' grep uuid-valueaudit_file_name >

output_file_name ' 을 입력합니다

예를 들면 다음과 같습니다.

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_restored_object.txt
```

5. grep를 사용하여 이 출력 파일에서 ORLM(Object Rules MET) 감사 메시지를 추출합니다. 'grep ORLM output_file_name'을 입력합니다

   예를 들면 다음과 같습니다.

```
Admin: # grep ORLM messages_about_restored_object.txt
```

   ORLM 감사 메시지는 이 샘플 메시지와 같습니다.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

6. 감사 메시지에서 Locs 필드를 찾습니다.

   있는 경우 Locs의 CLDI 값은 노드 ID 및 객체 복제본이 생성된 볼륨 ID입니다. 이 메시지는 ILM이 적용되었으며 그리드의 두 위치에서 두 개의 개체 복사본이 생성되었음을 나타냅니다. . 그리드 관리자에서 손실된 개체의 수를 재설정합니다.

관련 정보

손실된 개체를 조사합니다

분실 및 누락된 개체 수를 재설정합니다

감사 로그를 검토합니다

분실 및 누락된 개체 수를 재설정합니다

StorageGRID 시스템을 조사하고 기록된 손실된 개체가 모두 영구적으로 손실되거나 잘못된 알람인지 확인한 후 손실된 개체 속성의 값을 0으로 다시 설정할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

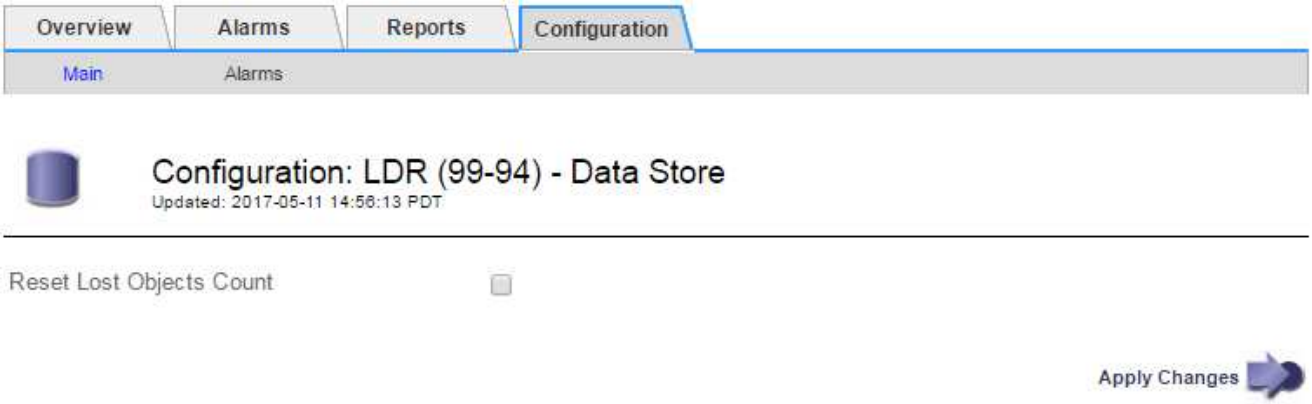
다음 페이지 중 하나에서 Lost Objects 카운터를 재설정할 수 있습니다.

- * 지원 * > * 도구 * > * 그리드 토폴로지 * > *사이트 * > * 스토리지 노드 * > * LDR * > * 데이터 저장소 * > * 개요 * > * 주 *
- * 지원 * > * 툴 * > * 그리드 토폴로지 * > * *Site* * > * *Storage Node* * > * DDS * > * 데이터 저장소 * > * 개요 * > * Main *

다음 지침은 * LDR * > * 데이터 저장소 * 페이지에서 카운터를 재설정하는 방법을 보여줍니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Objects Lost * 알림 또는 손실 경보가 있는 스토리지 노드에 대해 **Site* * > **Storage Node* * > * LDR * > * Data Store * > * Configuration * 을 선택합니다.
3. 손실된 개체 수 재설정 * 을 선택합니다.



4. 변경 내용 적용 * 을 클릭합니다.

   Lost Objects 속성은 0으로 재설정되고 * Objects Lost * 알림과 손실된 알람 지우기는 몇 분 정도 걸릴 수 있습니다.

5. 필요에 따라 손실된 개체를 식별하는 과정에서 증가했을 수 있는 다른 관련 특성 값을 재설정합니다.

   a. Site_ * > * *Storage Node* * > * LDR * > * 삭제 코딩 * > * 구성 * 을 선택합니다.
   b. Reset Reads Failure Count * 및 * Reset Corrupt Copies Detected Count * 를 선택합니다.
   c. 변경 내용 적용 * 을 클릭합니다.
   d. Site_ * > **Storage Node* * > * LDR * > * Verification * > * Configuration * 을 선택합니다.
   e. 누락된 개체 수 재설정 * 및 * 손상된 개체 수 재설정 * 을 선택합니다.
   f. 격리된 객체가 필요하지 않은 것으로 확신하면 * 격리된 객체 삭제 * 를 선택할 수 있습니다.

      백그라운드 검증이 손상된 복제된 객체 복사본을 식별하면 격리된 객체가 생성됩니다. 대부분의 경우 StorageGRID는 손상된 개체를 자동으로 대체하므로 격리된 개체를 삭제하는 것이 안전합니다. 그러나 * Objects Lost * 경고 또는 분실 경보가 트리거되면 기술 지원 부서에서 격리된 개체에 액세스하려고 할 수

있습니다.

g. 변경 내용 적용 * 을 클릭합니다.

[변경 내용 적용]을 클릭한 후 속성을 다시 설정하는 데 몇 분 정도 걸릴 수 있습니다.

오브젝트 부족 데이터 스토리지 경고 문제를 해결합니다

Low object data storage * 알림은 각 스토리지 노드에 오브젝트 데이터를 저장하는 데 사용할 수 있는 공간의 양을 모니터링합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

스토리지 노드에서 복제 및 삭제 코딩 오브젝트 데이터의 총 양이 경고 규칙에 구성된 조건 중 하나를 충족할 경우 * Low object data storage * 경고가 트리거됩니다.

기본적으로 이 조건이 true로 평가되면 주 경고가 트리거됩니다.

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

이 경우:

- 'toragegrid_storage_Utilization_data_bytes'는 스토리지 노드에 대해 복제되고 삭제 코딩된 오브젝트 데이터의 총 크기를 추정하는 것입니다.
- 'toragegrid_storage_Utilization_usable_space_bytes'는 스토리지 노드에 남아 있는 객체 스토리지 공간의 총 양입니다.

Major 또는 Minor * Low object data storage * 경고가 트리거되면 가능한 한 빨리 확장 절차를 수행해야 합니다.

단계

1. alerts * > * current * 를 선택합니다.

   경고 페이지가 나타납니다.

2. 알림 표에서 * Low object data storage * 알림 그룹을 확장하고 필요한 경우 보려는 경고를 선택합니다.

   알림 그룹의 제목이 아닌 알림을 선택합니다.

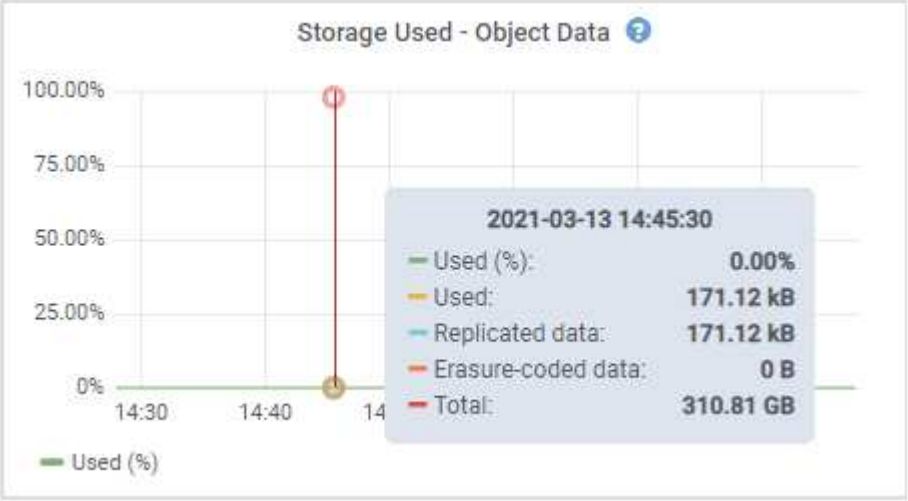
3. 대화 상자에서 세부 정보를 검토하고 다음 사항을 확인합니다.
   - 시간 트리거됨
   - 사이트 및 노드의 이름입니다

- 이 알림에 대한 메트릭의 현재 값입니다

4. nodes * > **Storage Node* 또는 *Site* * > * Storage * 를 선택합니다.
5. 커서를 Storage Used - Object Data 그래프 위에 놓습니다.

   다음 값이 표시됩니다.

   - * 사용됨(%) *: 오브젝트 데이터에 사용된 총 사용 가능 공간의 비율입니다.
   - * 사용됨 *: 오브젝트 데이터에 사용된 총 사용 가능 공간의 양입니다.
   - * 복제된 데이터 *: 이 노드, 사이트 또는 그리드에 복제된 객체 데이터의 양을 추정하는 것입니다.
   - * 삭제 코딩 데이터 *: 이 노드, 사이트 또는 그리드에 삭제 코딩 처리된 오브젝트 데이터의 양을 예측합니다.
   - * 총 *: 이 노드, 사이트 또는 그리드에서 사용 가능한 총 공간입니다. 사용된 값은 'toragegrid_storage_Utilization_data_bytes' 메트릭입니다.



6. 그래프 위에서 시간 컨트롤을 선택하여 다른 기간에 대한 스토리지 사용량을 표시합니다.

   시간이 지남에 따라 스토리지를 사용하는 것을 보면 알림이 트리거되기 전과 후에 사용된 스토리지의 양을 파악하고 노드의 남은 공간이 가득 차는 데 걸리는 시간을 예측하는 데 도움이 됩니다.

7. 가능한 한 빨리 확장 절차를 수행하여 스토리지 용량을 추가합니다.

   기존 스토리지 노드에 스토리지 볼륨(LUN)을 추가하거나 새 스토리지 노드를 추가할 수 있습니다.

   > 전체 스토리지 노드를 관리하려면 StorageGRID 관리 지침을 참조하십시오.

관련 정보

SSTS(Storage Status) 경보 문제를 해결합니다

그리드를 확장합니다

StorageGRID 관리

스토리지 볼륨 워터마크에 사용자 지정 값을 사용하는 경우 * 읽기 전용 로우 워터마크 재정의 * 알림을 확인해야 할 수 있습니다. 가능한 경우 최적화된 값을 사용하도록 시스템을 업데이트해야 합니다.

이전 버전에서는 세 가지가 있었습니다 스토리지 볼륨 워터마크입니다 전역 설정 — 모든 스토리지 노드의 모든 스토리지 볼륨에 동일한 값이 적용되었습니다. StorageGRID 11.6부터 소프트웨어는 스토리지 노드의 크기와 볼륨의 상대적 용량을 기준으로 각 스토리지 볼륨에 대해 이러한 워터마크를 최적화할 수 있습니다.

StorageGRID 11.6으로 업그레이드하면 다음 중 하나가 적용되지 않는 한 최적화된 읽기 전용 및 읽기-쓰기 워터마크가 모든 스토리지 볼륨에 자동으로 적용됩니다.

- 시스템의 용량이 거의 다 되었으며, 최적화된 워터마크가 적용된 경우 새 데이터를 사용할 수 없습니다. 이 경우 StorageGRID는 워터마크 설정을 변경하지 않습니다.
- 이전에 스토리지 볼륨 워터마크를 사용자 지정 값으로 설정했습니다. StorageGRID는 사용자 지정 워터마크 설정을 최적화된 값으로 재정의하지 않습니다. 그러나 스토리지 볼륨 소프트 읽기 전용 배경무늬의 사용자 지정 값이 너무 작은 경우 StorageGRID에서 * 낮은 읽기 전용 배경무늬 무시 * 알림을 트리거할 수 있습니다.

경고를 이해합니다

스토리지 볼륨 워터마크에 사용자 지정 값을 사용하는 경우 하나 이상의 스토리지 노드에 대해 * 읽기 전용 로우 워터마크 재정의 * 알림이 트리거될 수 있습니다.

알림의 각 인스턴스는 * 스토리지 볼륨 소프트 읽기 전용 워터마크 * 의 사용자 지정 값이 해당 스토리지 노드에 대해 최적화된 최소값보다 작음을 나타냅니다. 사용자 지정 설정을 계속 사용하는 경우 스토리지 노드가 읽기 전용 상태로 안전하게 전환되기 전에 공간이 매우 부족할 수 있습니다. 노드가 용량에 도달하면 일부 스토리지 볼륨을 액세스할 수 없게 되거나 자동으로 마운트 해제될 수 있습니다.

예를 들어, 이전에 * 스토리지 볼륨 소프트 읽기 전용 워터마크 * 를 5GB로 설정했다고 가정합니다. 이제 StorageGRID가 스토리지 노드 A의 4개 스토리지 볼륨에 대해 다음과 같은 최적화된 값을 계산했다고 가정합니다.

볼륨 0	12GB
볼륨 1	12GB
볼륨 2	11GB
볼륨 3	15GB

사용자 지정 워터마크(5GB)가 해당 노드의 모든 볼륨(11GB)에 대해 최적화된 최소값보다 작기 때문에 스토리지 노드 A에 대해 * 낮은 읽기 전용 워터마크 재정의 * 알림이 트리거됩니다. 사용자 지정 설정을 계속 사용하는 경우 노드가 공간이 매우 부족해서 읽기 전용 상태로 안전하게 전환될 수 있습니다.

경고를 해결합니다

하나 이상의 * 낮은 읽기 전용 배경무늬 무시 * 알림이 트리거된 경우 다음 단계를 따르십시오. 현재 사용자 지정 워터마크 설정을 사용하고 있고 경고가 트리거되지 않았더라도 최적화된 설정을 사용하려는 경우에도 이 지침을 사용할 수 있습니다.

필요한 것

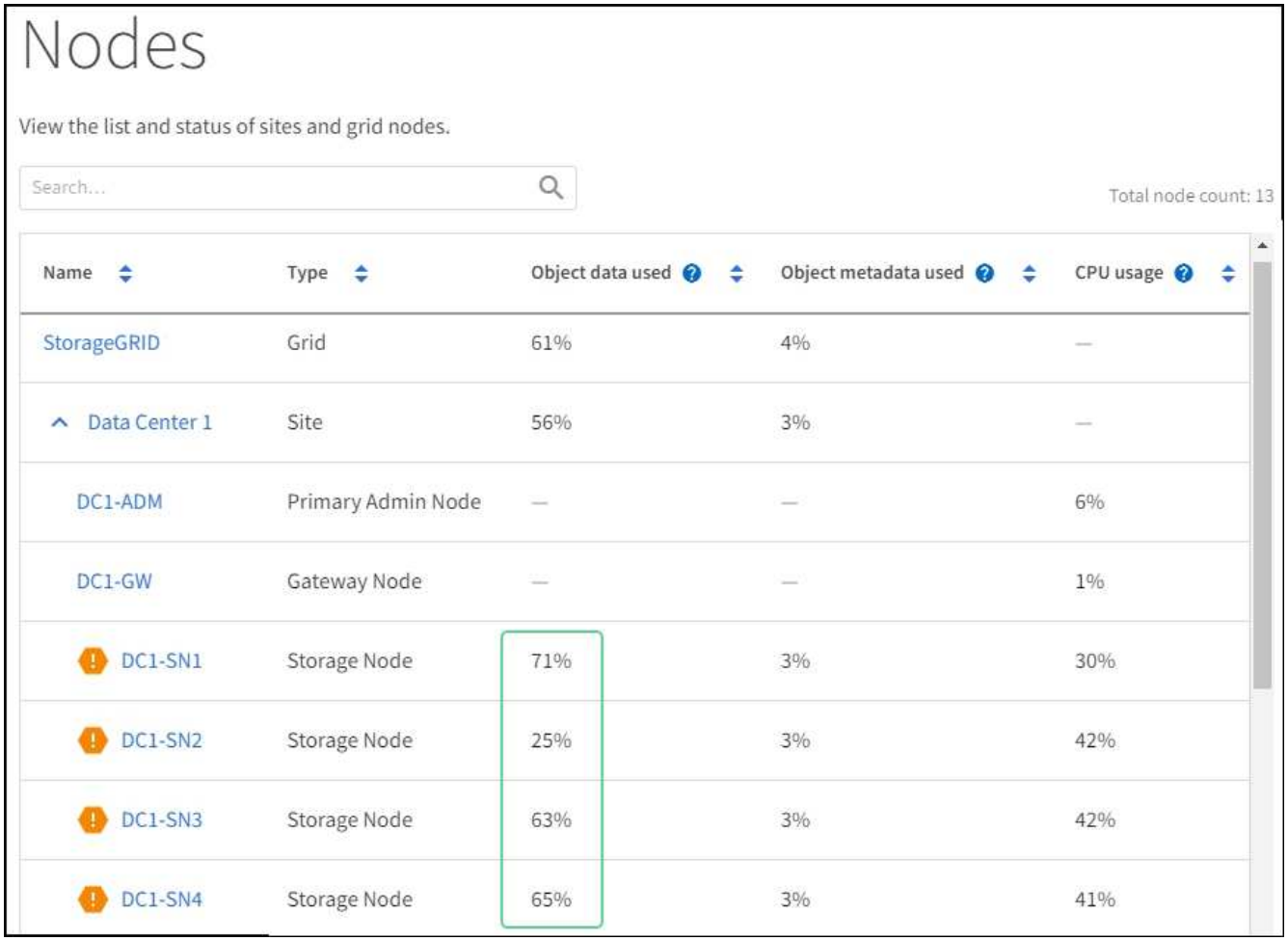
- StorageGRID 11.6으로의 업그레이드를 완료했습니다.
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 루트 액세스 권한이 있습니다.

이 작업에 대해

사용자 지정 배경무늬 설정을 새 배경무늬 재정의로 업데이트하여 * 낮은 읽기 전용 배경무늬 무시 * 알림을 확인할 수 있습니다. 그러나 하나 이상의 스토리지 노드가 거의 꽉 찼거나 특별한 ILM 요구 사항이 있는 경우 먼저 최적화된 스토리지 워터마크를 확인하고 해당 스토리지 노드를 사용하기에 안전한지 확인해야 합니다.

전체 그리드에 대한 객체 데이터 사용량을 평가합니다

1. 노드 * 를 선택합니다.
2. 그리드의 각 사이트에 대해 노드 목록을 확장합니다.
3. 모든 사이트의 각 스토리지 노드에 대해 * 사용된 객체 데이터 * 열에 표시된 백분율 값을 검토합니다.



4. 스토리지 노드 중 거의 꽉 참(예: 모든 * 사용된 객체 데이터 * 값이 80% 미만인 경우)이 없는 경우 재정의 설정을 사용할 수 있습니다. 로 이동합니다 최적화된 워터마크를 사용합니다.

> 이 일반 규칙에는 몇 가지 예외가 있습니다. 예를 들어 ILM 규칙이 Strict 수집 동작을 사용하거나 특정 스토리지 풀이 거의 꽉 찬 경우 먼저 의 단계를 수행해야 합니다 최적화된 스토리지 워터마크를 봅니다 및 최적화된 워터마크를 사용할 수 있는지 확인합니다.

5. 하나 이상의 스토리지 노드가 거의 꽉 찬 경우 의 단계를 수행합니다 최적화된 스토리지 워터마크를 봅니다 및 최적화된 워터마크를 사용할 수 있는지 확인합니다.

최적화된 스토리지 워터마크를 봅니다

StorageGRID는 두 개의 Prometheus 메트릭을 사용하여 * 스토리지 볼륨 소프트 읽기 전용 워터마크 * 에 대해 계산된 최적화 값을 표시합니다. 그리드의 각 스토리지 노드에 대해 최적화된 최소 및 최대 값을 볼 수 있습니다.

1. 지원 * > * 도구 * > * 메트릭 * 을 선택합니다.
2. Prometheus 섹션에서 Prometheus 사용자 인터페이스에 액세스할 링크를 선택합니다.
3. 권장되는 최소 소프트 읽기 전용 워터마크를 보려면 다음 Prometheus 메트릭을 입력하고 * Execute * 를 선택합니다.

   'toragegrid_storage_volume_minimum_optimized_soft_readonly_watermark'

   마지막 열에는 각 스토리지 노드의 모든 스토리지 볼륨에 대해 소프트 읽기 전용 워터마크의 최적화된 최소값이 표시됩니다. 이 값이 * 스토리지 볼륨 소프트 읽기 전용 워터마크 * 에 대한 사용자 정의 설정보다 크면 * 읽기 전용 로우 워터마크 재정의 * 알림이 스토리지 노드에 대해 트리거됩니다.

4. 권장되는 최대 소프트 읽기 전용 워터마크를 보려면 다음 Prometheus 메트릭을 입력하고 * Execute * 를 선택합니다.

   'toragegrid_storage_volume_maximum_optimized_soft_readonly_watermark'

   마지막 열에는 각 스토리지 노드의 모든 스토리지 볼륨에 대해 소프트 읽기 전용 워터마크의 최대 최적화 값이 표시됩니다.

5. 각 스토리지 노드에 대해 최적화된 최대 값을 기록합니다.

최적화된 워터마크를 사용할 수 있는지 확인합니다

1. 노드 * 를 선택합니다.
2. 각 온라인 스토리지 노드에 대해 다음 단계를 반복합니다.
   a. 스토리지 노드 * > * 스토리지 * 를 선택합니다.
   b. Object Stores(오브젝트 저장소) 테이블까지 아래로 스크롤합니다.
   c. 각 오브젝트 저장소(볼륨)의 * 사용 가능 * 값을 해당 스토리지 노드에 대해 기록해 둔 최대 최적화 워터마크와 비교합니다.
3. 모든 온라인 스토리지 노드에서 하나 이상의 볼륨에 해당 노드에 대해 최적화된 최대 워터마크보다 사용 가능한 공간이 더 많은 경우 로 이동합니다 최적화된 워터마크를 사용합니다 최적화된 워터마크를 사용하기 시작합니다.

   그렇지 않으면 그리드를 확장합니다 빨리. 기존 노드에 스토리지 볼륨을 추가하거나 새 스토리지 노드를 추가합니다. 그런 다음 로 이동합니다 최적화된 워터마크를 사용합니다 배경무늬 설정을 업데이트합니다.

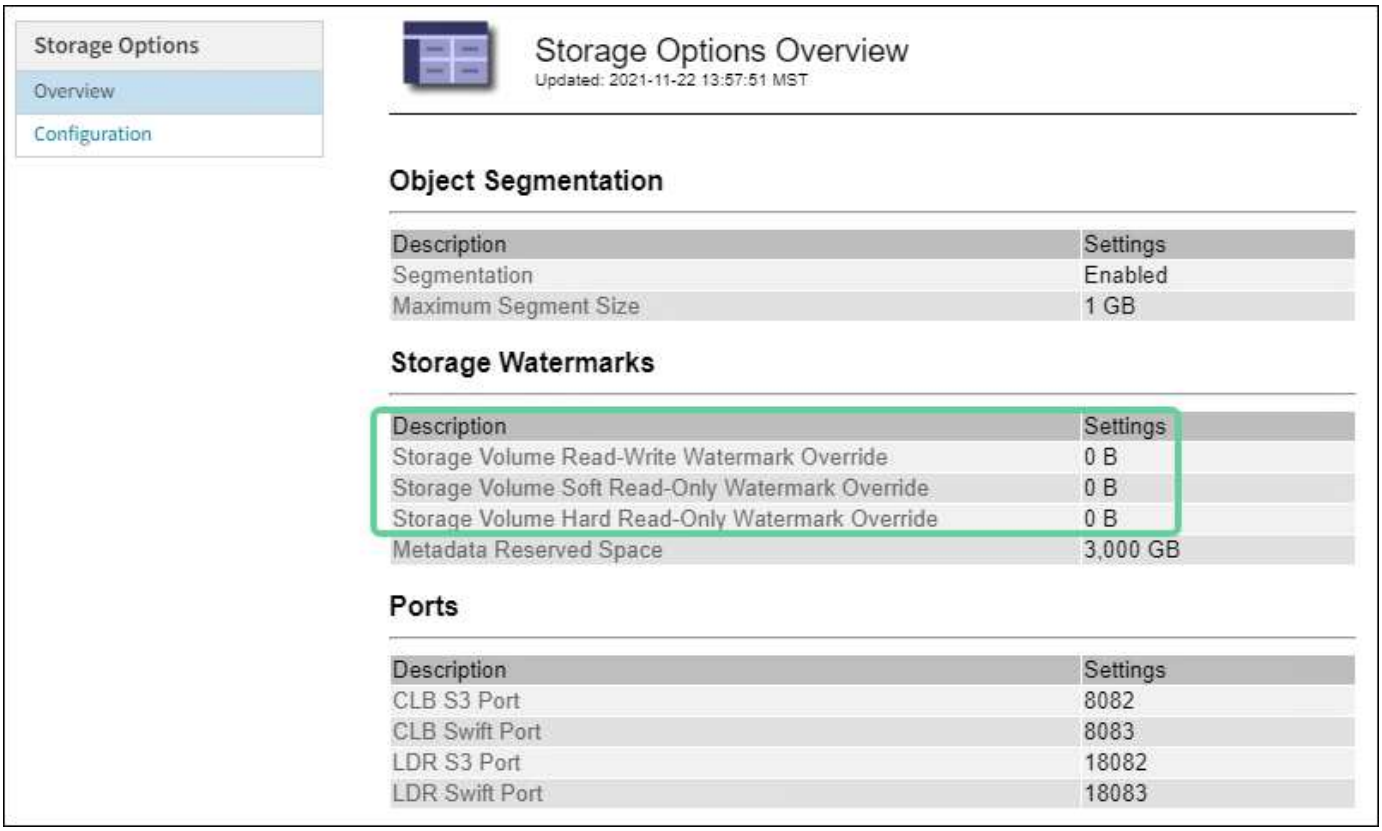
4. 스토리지 볼륨 워터마크에 대해 사용자 지정 값을 계속 사용해야 하는 경우 침묵 또는 사용 안 함 낮은 읽기 전용 배경무늬 무시 * 알림.

> 모든 스토리지 노드의 모든 스토리지 볼륨에 동일한 사용자 지정 워터마크 값이 적용됩니다. 스토리지 볼륨 워터마크에 권장되는 값보다 작은 값을 사용하면 노드가 용량에 도달하면 일부 스토리지 볼륨을 자동으로 마운트 해제된 상태로 액세스할 수 없게 될 수 있습니다.

최적화된 워터마크를 사용합니다

1. 구성 * > * 시스템 * > * 스토리지 옵션 * 으로 이동합니다.
2. Storage Options 메뉴에서 * Configuration * 을 선택합니다.
3. 세 개의 배경무늬 덮어쓰기가 모두 0으로 변경됩니다.
4. Apply Changes * 를 선택합니다.

스토리지 노드의 크기와 볼륨의 상대적 용량에 따라 최적화된 스토리지 볼륨 워터마크 설정이 각 스토리지 볼륨에 적용됩니다.



SSTS(Storage Status) 경보 문제를 해결합니다

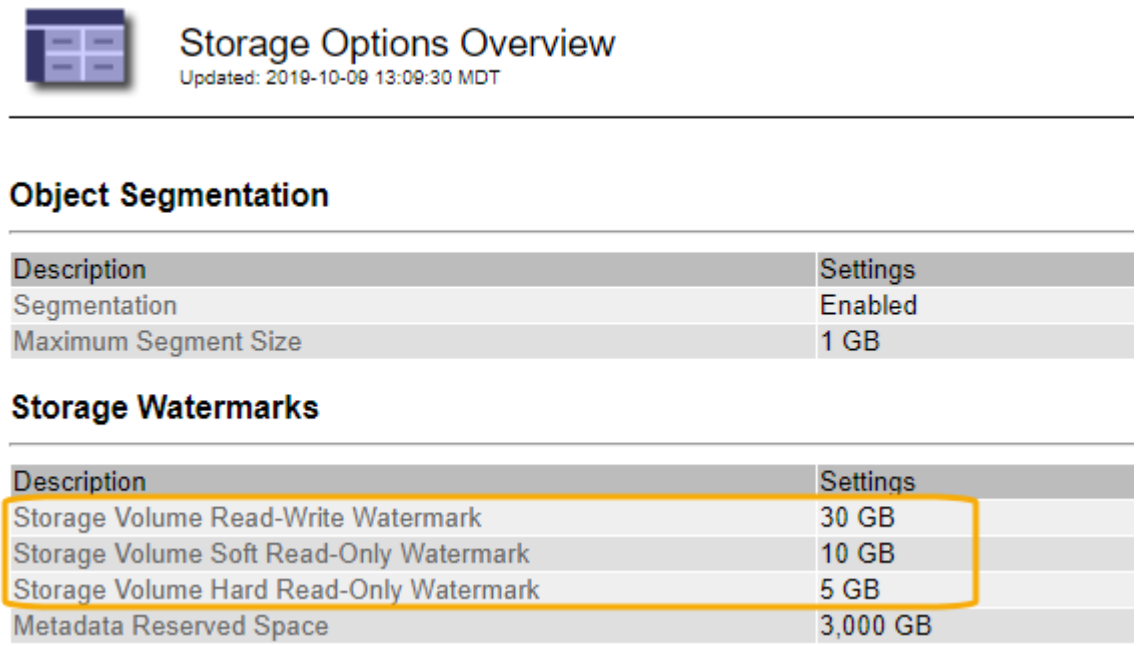
스토리지 노드에 객체 저장을 위한 여유 공간이 부족한 경우 SSTS(Storage Status) 경보가 트리거됩니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

SSTS(Storage Status) 알람은 스토리지 노드의 모든 볼륨에서 사용 가능한 공간의 양이 스토리지 볼륨 소프트 읽기 전용 배경무늬(* configuration * > * System * > * Storage options *)의 값 아래로 떨어지면 알림 레벨에서 트리거됩니다.



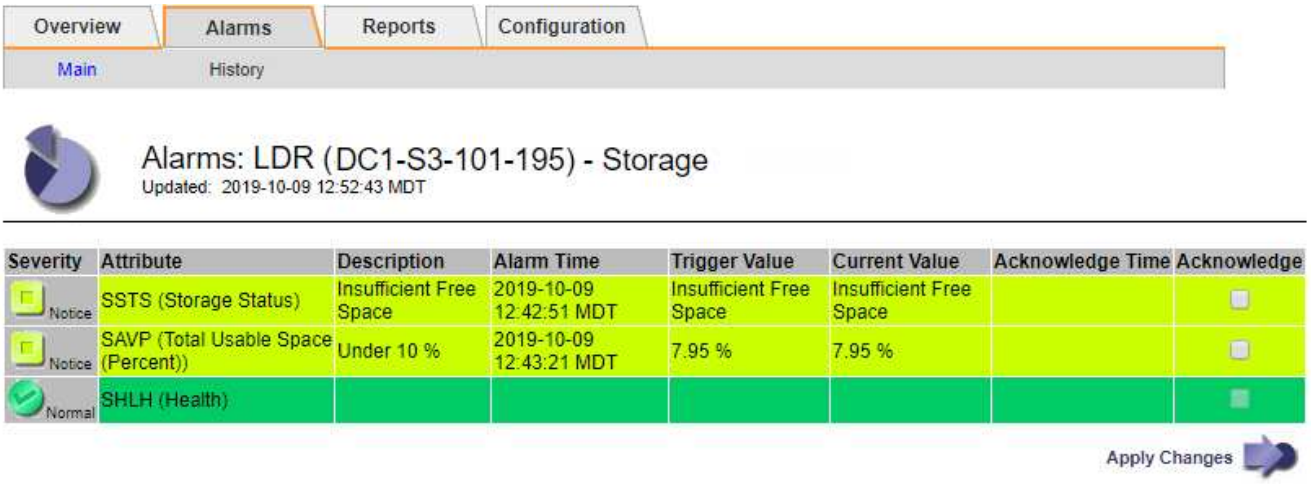
예를 들어 스토리지 볼륨 소프트 읽기 전용 워터마크가 기본값인 10GB로 설정되어 있다고 가정합니다. 스토리지 노드의 각 스토리지 볼륨에 사용 가능한 공간이 10GB 미만인 경우 SSTS 알람이 트리거됩니다. 볼륨에 사용 가능한 공간이 10GB 이상인 경우 알람이 트리거되지 않습니다.

SSTS 알람이 트리거된 경우 다음 단계에 따라 문제를 보다 잘 이해할 수 있습니다.

단계

1. 지원 * > * 알람(레거시) * > * 현재 알람 * 을 선택합니다.
2. Service(서비스) 열에서 SSTS 알람과 관련된 데이터 센터, 노드 및 서비스를 선택합니다.

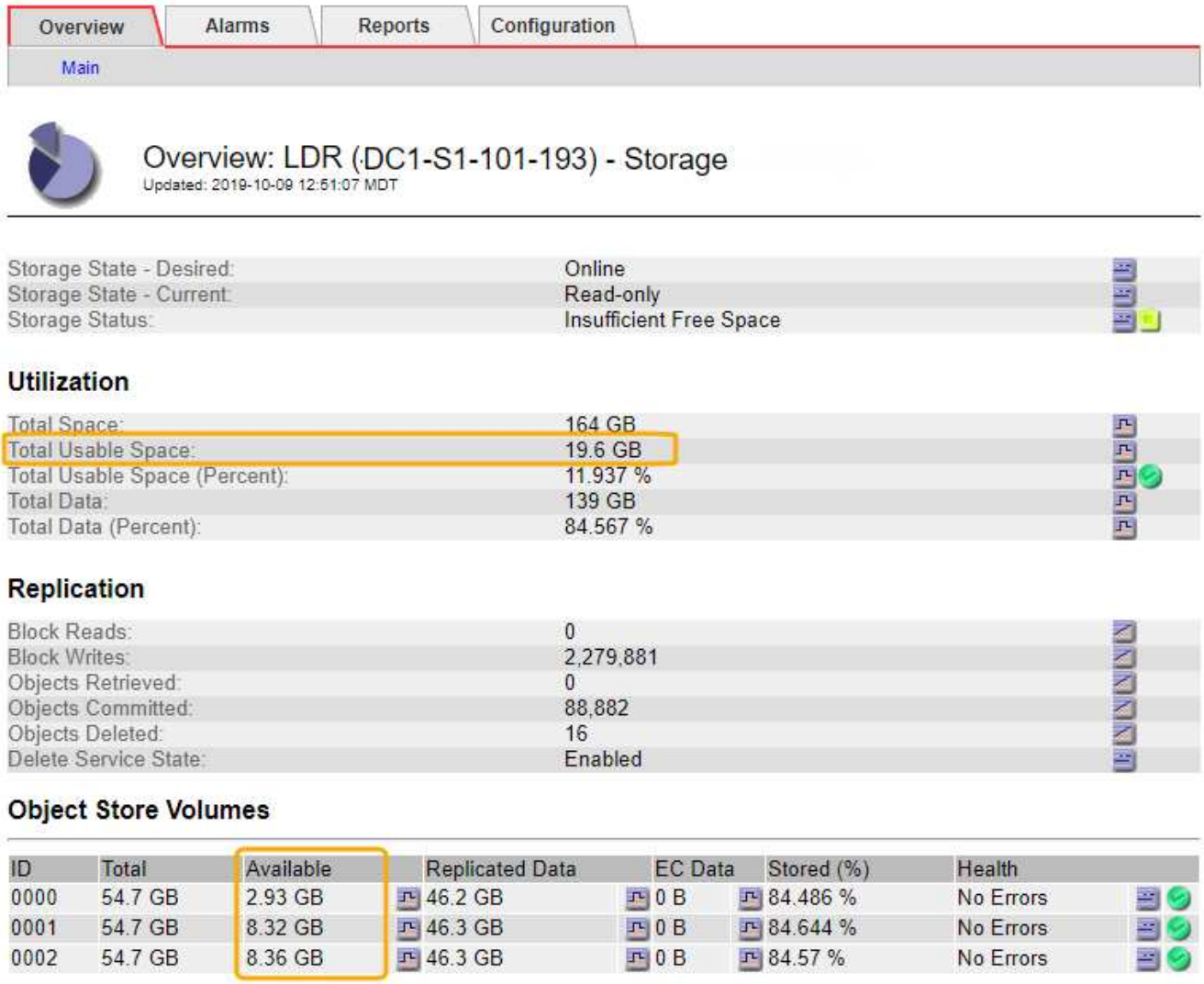
   그리드 토폴로지 페이지가 나타납니다. Alarms(알람) 탭에는 선택한 노드와 서비스에 대한 활성 알람이 표시됩니다.



   이 예에서는 SSTS(Storage Status) 알람과 SAVP(Total Usable Space(Percent)) 알람이 모두 Notice 레벨에서 트리거되었습니다.

> 일반적으로 SSTS 알람과 SAVP 알람은 거의 동시에 트리거되지만 두 알람이 트리거되는지 여부는 배경무늬 설정(GB)과 SAVP 알람 설정(백분율)에 따라 달라집니다.

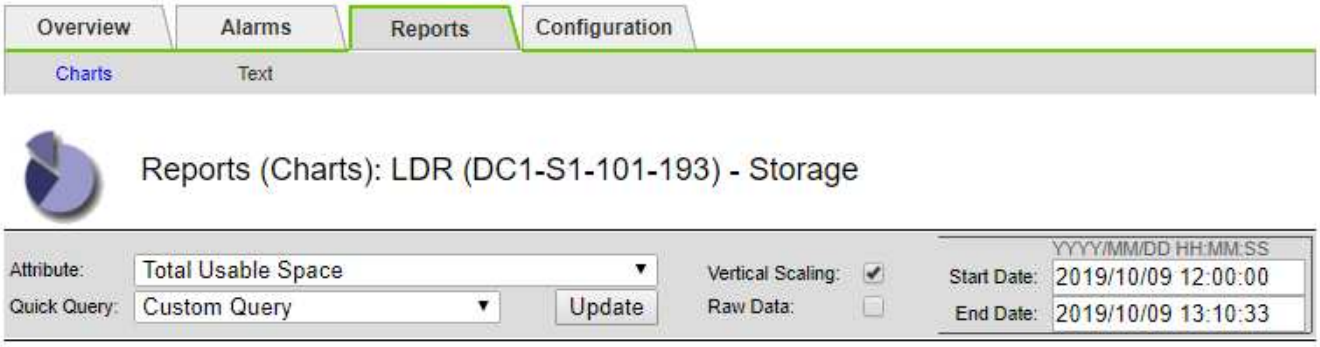
3. 실제로 사용 가능한 공간을 확인하려면 * LDR * > * 스토리지 * > * 개요 * 를 선택하고 총 사용 가능한 공간(STAS) 속성을 찾습니다.

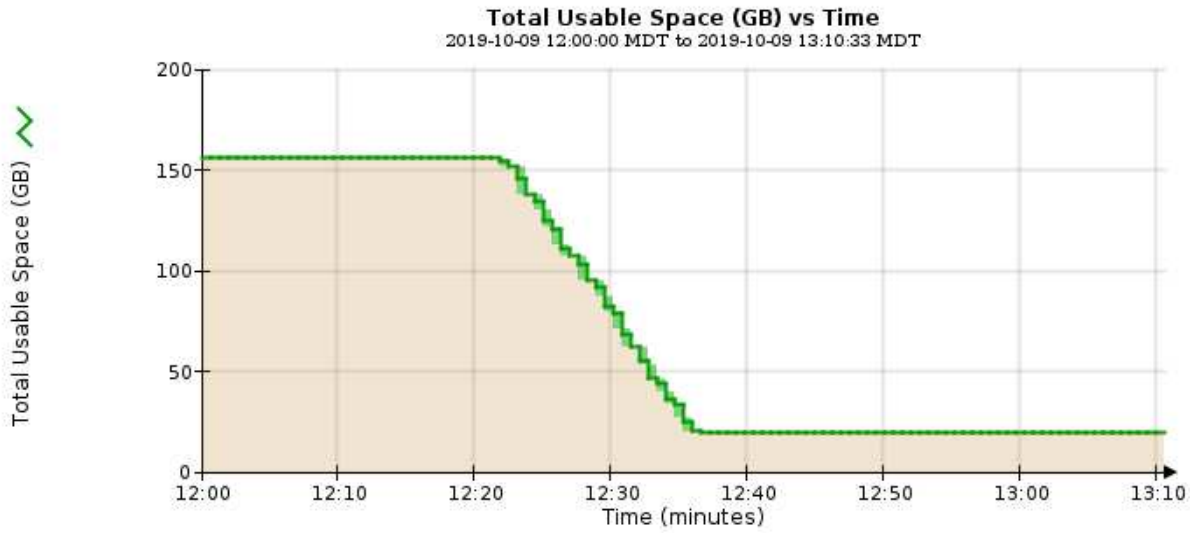


이 예에서는 이 스토리지 노드의 164GB 공간 중 19.6GB만 사용할 수 있습니다. 총 값은 세 개의 오브젝트 저장소 볼륨에 대해 * 사용 가능한 * 값의 합계입니다. 세 개의 스토리지 볼륨 각각이 사용 가능한 공간이 10GB보다 작기 때문에 SSTS 알람이 트리거되었습니다.

4. 시간이 지남에 따라 스토리지가 어떻게 사용되었는지 이해하려면 * Reports * 탭을 선택하고 지난 몇 시간 동안 총 사용 가능한 공간을 플롯합니다.

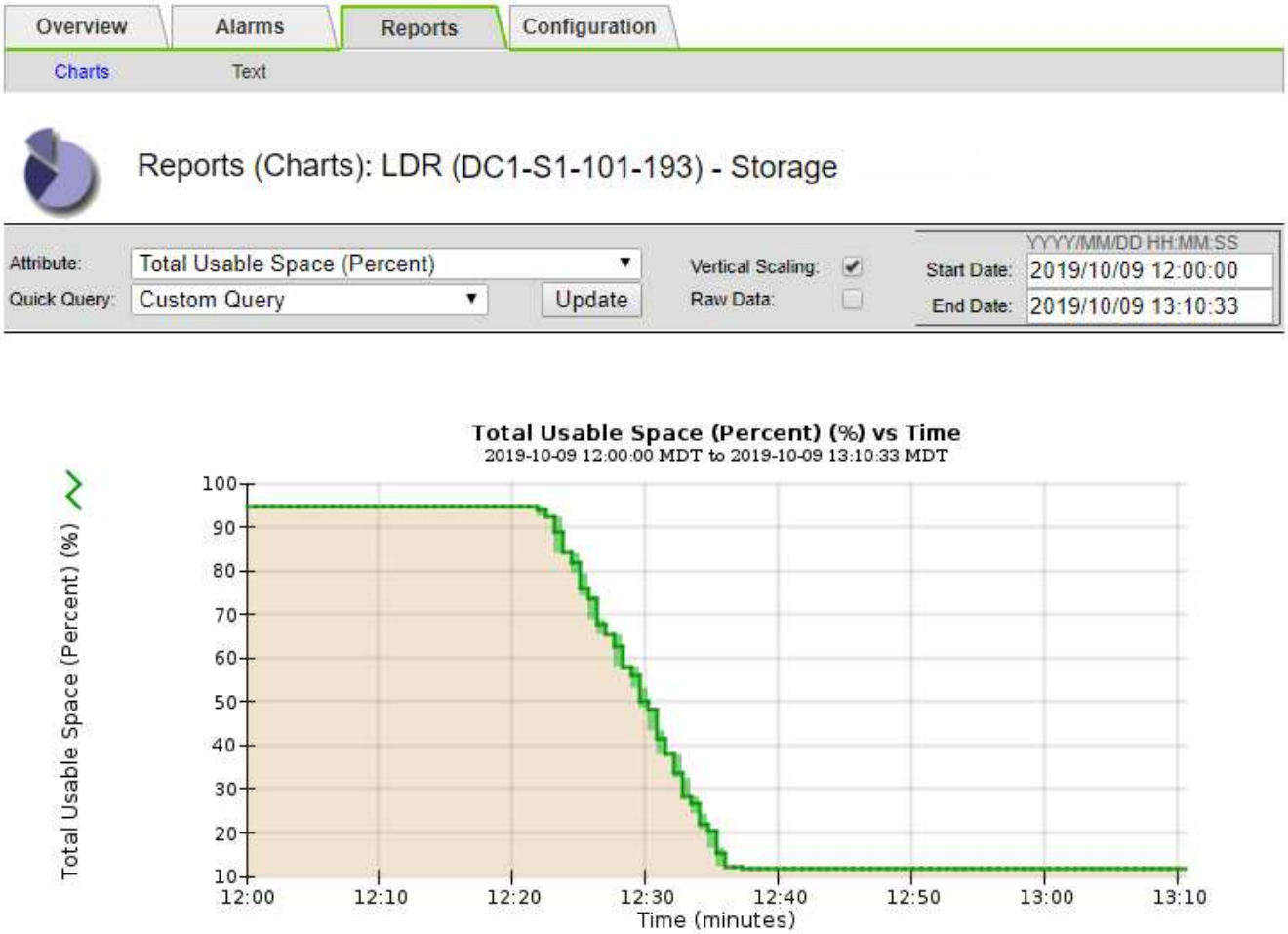
   이 예에서는 총 가용 공간이 12:00에 약 155GB에서 12:35에 20GB로 감소했으며, 이는 SSTS 알람이 트리거된 시간에 해당합니다.





5. 스토리지가 전체 용량의 백분율 단위로 어떻게 사용되는지 이해하려면 최근 몇 시간 동안의 총 사용 가능 공간(%)을 플롯합니다.

   이 예에서 사용 가능한 총 공간은 95%에서 약 10%로 거의 동시에 떨어졌습니다.



6. 필요에 따라 를 통해 스토리지 용량을 추가합니다 StorageGRID 시스템 확장.

   전체 스토리지 노드를 관리하는 방법에 대한 절차는 를 참조하십시오 StorageGRID 관리 지침.

플랫폼 서비스 메시지 전달 문제 해결(**SMTT** 알람)

플랫폼 서비스 메시지가 데이터를 수용할 수 없는 대상으로 전달될 경우 그리드 관리자에서 SMTT(Total Events) 경보가 트리거됩니다.

이 작업에 대해

예를 들어 연결된 복제 또는 알림 메시지를 구성된 엔드포인트로 전달할 수 없더라도 S3 멀티파트 업로드에 성공할 수 있습니다. 또는 메타데이터가 너무 긴 경우 CloudMirror 복제에 대한 메시지를 배달하지 못할 수 있습니다.

SMTT 알람에는 알림이 실패한 마지막 객체에 대해 '*bucket-name object key* 에 대한 알림을 게시하지 못했습니다 .'라는 마지막 이벤트 메시지가 포함됩니다.

이벤트 메시지는 '/var/local/log/bycast-err.log' 로그 파일에도 나열됩니다. 를 참조하십시오 로그 파일 참조.

플랫폼 서비스 문제 해결에 대한 자세한 내용은 를 참조하십시오 StorageGRID 관리 지침. 필요한 경우도 있습니다 테넌트 관리자에서 테넌트에 액세스합니다 플랫폼 서비스 오류를 디버깅하려면

단계

1. 경보를 보려면 * nodes * > **site* * > **GRID node* * > * Events * 를 선택합니다.

2. 테이블 상단의 마지막 이벤트 보기

   이벤트 메시지는 '/var/local/log/bycast-err.log'에도 나열됩니다.

3. SMTT 알람 내용물에 제공된 지침을 따라 문제를 해결하십시오.
4. Reset event counts * 를 선택합니다.
5. 플랫폼 서비스 메시지가 전달되지 않은 객체를 테넌트에 알립니다.
6. 테넌트에게 개체의 메타데이터 또는 태그를 업데이트하여 실패한 복제 또는 알림을 트리거하도록 지시합니다.

메타데이터 문제를 해결합니다

여러 작업을 수행하여 메타데이터 문제의 원인을 확인할 수 있습니다.

메타데이터 부족 스토리지 경고 문제를 해결합니다

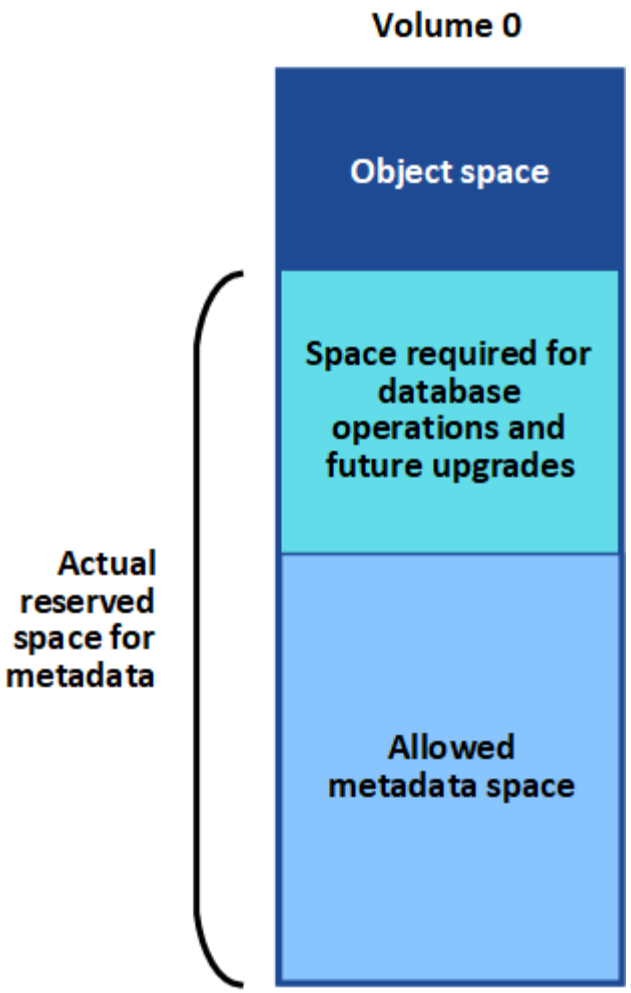
메타데이터 스토리지 부족 * 경고가 트리거되면 새 스토리지 노드를 추가해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

이 작업에 대해

StorageGRID는 각 스토리지 노드의 볼륨 0에 개체 메타데이터를 위한 일정한 양의 공간을 예약합니다. 이 공간을 실제 예약 공간이라고 하며, 여기에는 오브젝트 메타데이터(허용되는 메타데이터 공간)에 허용되는 공간과 컴팩션 및 복구처럼 필수 데이터베이스 작업에 필요한 공간으로 세분화됩니다. 허용되는 메타데이터 공간은 전체 오브젝트 용량을 관리합니다.



오브젝트 메타데이터가 메타데이터에 허용된 공간의 100% 이상을 소비하면 데이터베이스 작업이 효율적으로 실행되지 않고 오류가 발생합니다.

가능합니다 각 스토리지 노드의 객체 메타데이터 용량을 모니터링합니다 오류가 발생하기 전에 미리 예측하고 수정할 수 있도록 도와줍니다.

StorageGRID는 다음 Prometheus 메트릭을 사용하여 허용되는 메타데이터 공간의 전체 용량을 측정합니다.

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

이 Prometheus 표현식이 특정 임계값에 도달하면 * Low metadata storage * 경고가 트리거됩니다.

- * Minor * : 객체 메타데이터가 허용된 메타데이터 공간의 70% 이상을 사용하고 있습니다. 가능한 빨리 새 스토리지 노드를 추가해야 합니다.
- * Major *: 오브젝트 메타데이터는 허용된 메타데이터 공간을 90% 이상 사용합니다. 새 스토리지 노드를 즉시 추가해야 합니다.

> 오브젝트 메타데이터가 허용된 메타데이터 공간의 90% 이상을 사용하는 경우 대시보드에 경고가 표시됩니다. 이 경고가 나타나면 새 스토리지 노드를 즉시 추가해야 합니다. 오브젝트 메타데이터에서 허용되는 공간의 100% 이상을 사용하도록 허용해서는 안 됩니다.

- * Critical *: 오브젝트 메타데이터는 허용된 메타데이터 공간을 100% 이상 사용하며 필수 데이터베이스 작업에 필요한 공간을 사용하기 시작합니다. 새 오브젝트 수집을 중지해야 하며 새 스토리지 노드를 즉시 추가해야 합니다.

다음 예제에서 오브젝트 메타데이터는 허용되는 메타데이터 공간의 100% 이상을 사용합니다. 이는 비효율적인 데이터베이스 작업 및 오류를 초래할 수 있는 심각한 상황입니다.

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

Node	% Used	Used	Allowed
DC1-S2-227	104.51%	6.73 GB	6.44 GB
DC1-S3-228	104.36%	6.72 GB	6.44 GB
DC2-S2-233	104.20%	6.71 GB	6.44 GB
DC1-S1-226	104.20%	6.71 GB	6.44 GB
DC2-S3-234	103.43%	6.66 GB	6.44 GB

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.

> 볼륨 0의 크기가 Metadata Reserved Space Storage Option(예: 비운영 환경)보다 작은 경우 * Low Metadata Storage * 알림에 대한 계산이 부정확할 수 있습니다.

단계

1. alerts * > * current * 를 선택합니다.
2. 경고 표에서 * Low metadata storage * 알림 그룹을 확장하고 필요한 경우 보려는 특정 경고를 선택합니다.
3. 경고 대화 상자에서 세부 정보를 검토합니다.
4. Major 또는 Critical * Low Metadata Storage * 알림이 트리거된 경우 확장을 수행하여 스토리지 노드를 즉시 추가합니다.

> StorageGRID는 모든 오브젝트 메타데이터의 전체 복사본을 각 사이트에 유지하므로 전체 그리드의 메타데이터 용량은 가장 작은 사이트의 메타데이터 용량에 의해 제한됩니다. 한 사이트에 메타데이터 용량을 추가해야 하는 경우에도 필요합니다 다른 사이트를 확장합니다 동일한 수의 스토리지 노드 기준

확장을 수행한 후 StorageGRID는 기존 오브젝트 메타데이터를 새 노드로 재분산하여 그리드의 전체 메타데이터 용량을 늘립니다. 사용자 작업이 필요하지 않습니다. Low metadata storage * 알림이 지워집니다.

서비스: 상태 - **Cassandra(SVST)** 알람 문제를 해결합니다

서비스: 상태 - Cassandra(SVST) 알람은 스토리지 노드에 대한 Cassandra 데이터베이스를 재구성해야 할 수 있음을 나타냅니다. Cassandra는 StorageGRID의 메타데이터 저장소로 사용됩니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.

이 작업에 대해

Cassandra가 15일 이상 중지(예: 스토리지 노드 전원이 꺼져 있는 경우)인 경우, 노드가 다시 온라인 상태가 될 때 Cassandra가 시작되지 않습니다. 영향을 받는 DDS 서비스를 위해 Cassandra 데이터베이스를 재구축해야 합니다.

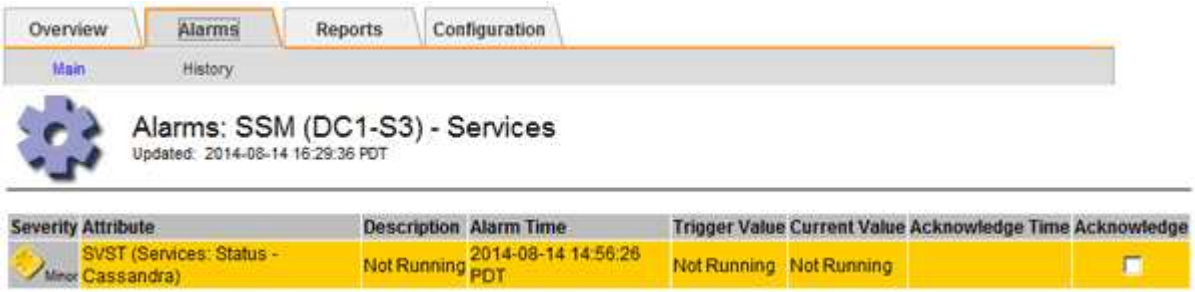
가능합니다 진단 유틸리티를 실행합니다 그리드의 현재 상태에 대한 추가 정보를 얻습니다.

Cassandra 데이터베이스 서비스가 15일 이상 중단된 경우, 기술 지원 팀에 문의 하여 다음 단계를 진행하지 마십시오.

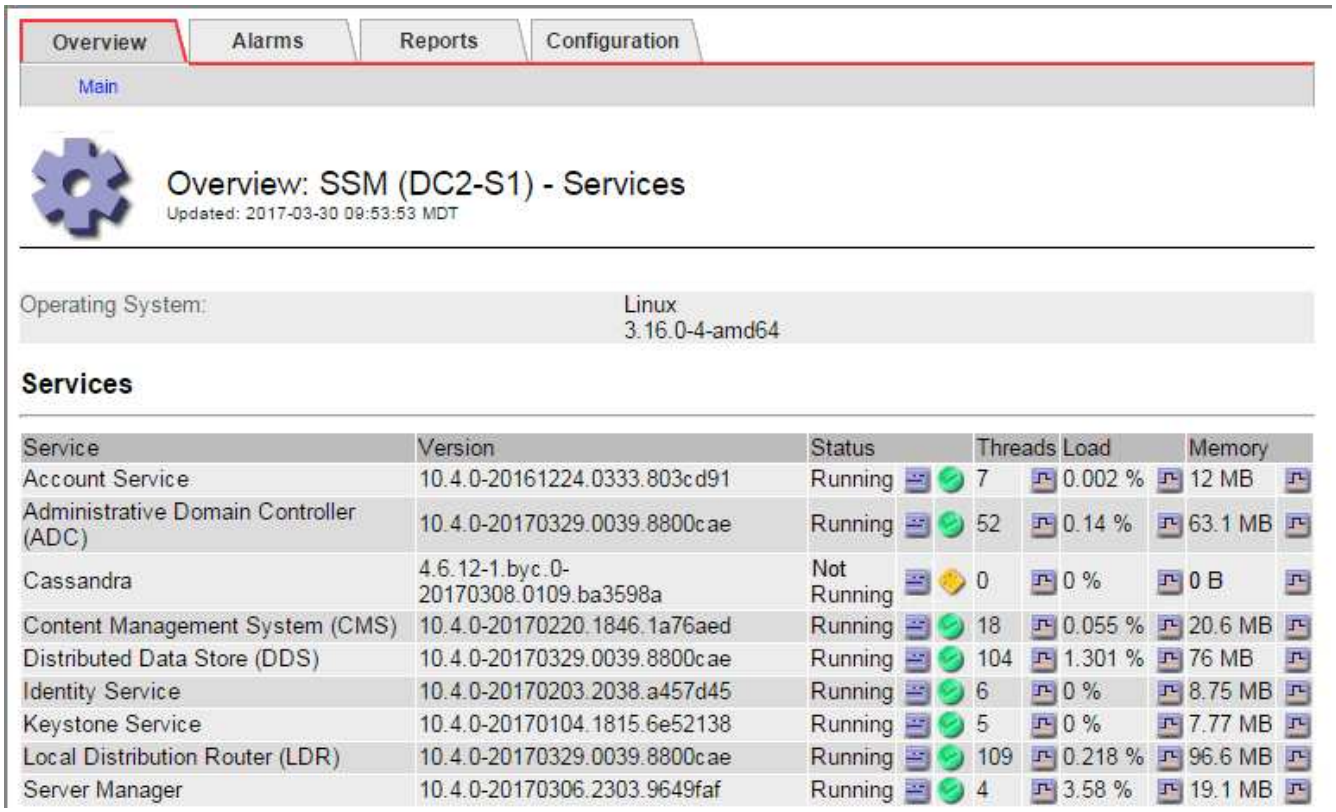
단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. 경보를 표시하려면 **Site* * > **Storage Node* * > * SSM * > * Services * > * Alarms * > * Main * 을 선택합니다.

   이 예에서는 SVST 알람이 트리거되었음을 보여 줍니다.



   SSM 서비스 기본 페이지에는 Cassandra가 실행되고 있지 않습니다.



3. 스토리지 노드에서 Cassandra를 다시 시작합니다.
   a. 그리드 노드에 로그인합니다.
      i. ssh admin@grid_node_ip' 명령을 입력한다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다

iv. "passwords.txt" 파일에 나열된 암호를 입력합니다. 루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

b. '/etc/init.d/cassandra status'를 입력합니다

c. Cassandra가 실행되고 있지 않으면 '/etc/init.d/cassandra restart'를 다시 시작합니다

4. Cassandra가 다시 시작되지 않으면 Cassandra가 얼마 동안 중단되었는지 확인합니다. Cassandra가 15일 이상 중단된 경우 Cassandra 데이터베이스를 재구성해야 합니다.

> Cassandra 데이터베이스 서비스가 두 개 이상 중단된 경우 기술 지원 팀에 문의 하여 다음 단계를 진행하지 마십시오.

Cassandra의 가동 중지 시간은 차트를 작성하거나 servermanager.log 파일을 검토하여 확인할 수 있습니다.

5. Cassandra 차트 만들기:

a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **Site* * > **Storage Node* * > * SSM * > * Services * > * Reports * > * Charts * 를 선택합니다.

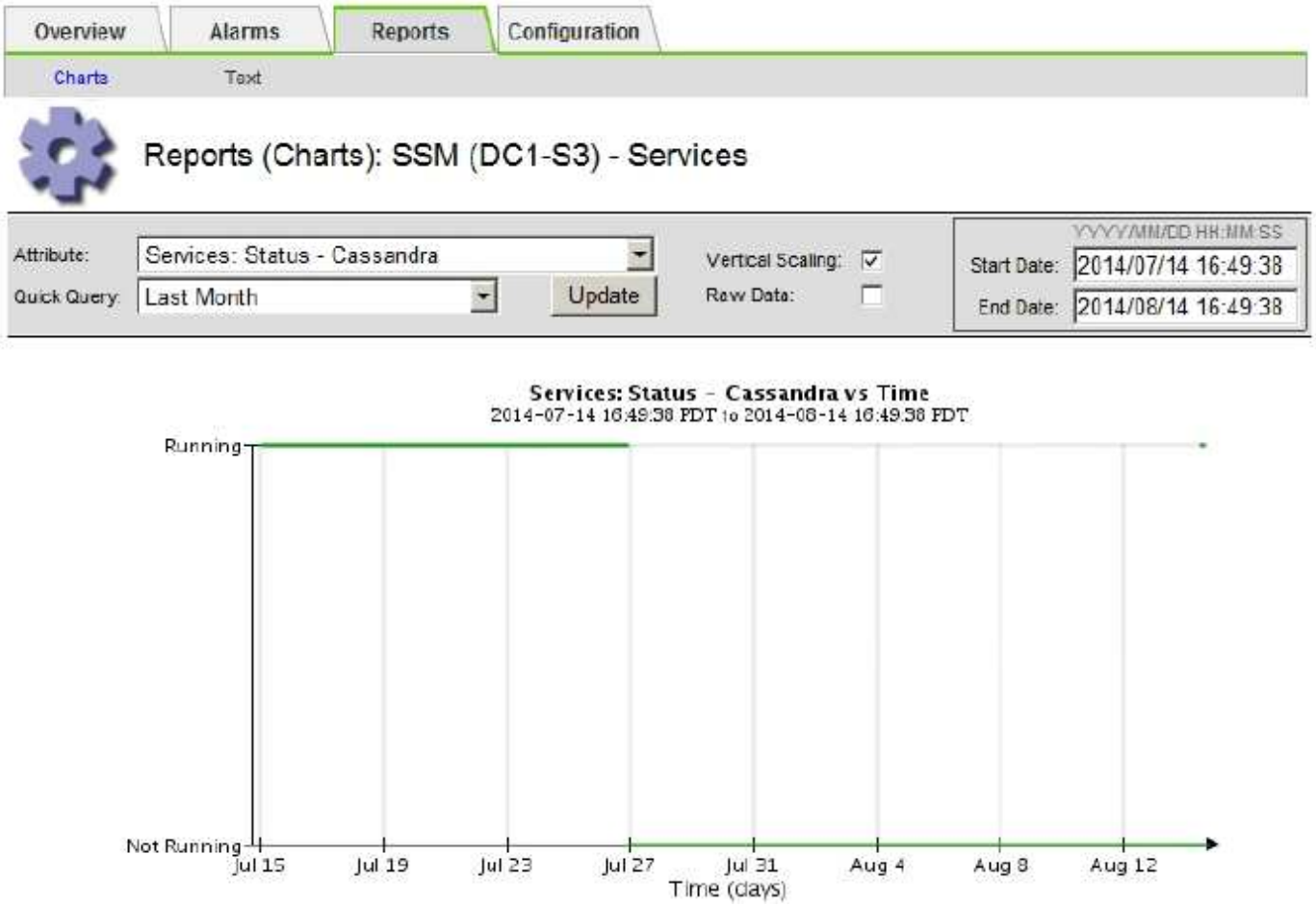
b. Attribute * > * Service:Status-Cassandra * 를 선택합니다.

c. 시작 날짜 * 에 대해 현재 날짜 16일 이전의 날짜를 입력합니다. 종료 날짜 * 에 현재 날짜를 입력합니다.

d. Update * 를 클릭합니다.

e. 차트에 Cassandra가 15일 이상 다운된 것으로 표시되면 Cassandra 데이터베이스를 재구축합니다.

다음 차트 예제에서는 Cassandra가 최소 17일 동안 중단되었음을 보여 줍니다.



1. 스토리지 노드에서 servermanager.log 파일을 검토하려면 다음을 수행합니다.

   a. 그리드 노드에 로그인합니다.

      i. ssh admin@grid_node_ip' 명령을 입력한다

      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      iii. 루트로 전환하려면 다음 명령을 입력합니다

      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다. 루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

   b. 'cat/var/local/log/ServerManager.log'를 입력합니다

      servermanager.log 파일의 내용이 표시됩니다.

      Cassandra가 15일 이상 중단된 경우 servermanager.log 파일에 다음 메시지가 표시됩니다.

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

   a. 이 메시지의 타임스탬프가 단계의 지침에 따라 Cassandra를 다시 시작하려고 시도한 시간인지 확인합니다 스토리지 노드에서 Cassandra를 다시 시작합니다.

      Cassandra에는 여러 항목이 있을 수 있으며, 가장 최근 항목을 찾아야 합니다.

   b. Cassandra가 15일 이상 중단된 경우 Cassandra 데이터베이스를 재구성해야 합니다.

      자세한 내용은 을 참조하십시오 스토리지 노드를 15일 이상 복구합니다.

   c. Cassandra를 재구축한 후 경보가 지워지지 않으면 기술 지원 부서에 문의하십시오.

Cassandra 메모리 부족 오류(SMTT 알람) 문제 해결

Cassandra 데이터베이스에 메모리 부족 오류가 발생하면 SMTT(Total Events) 경보가 발생합니다. 이 오류가 발생하면 기술 지원 부서에 문의하여 문제를 해결하십시오.

이 작업에 대해

Cassandra 데이터베이스에 대해 메모리 부족 오류가 발생하면 힙 덤프가 생성되고, SMTT(Total Events) 경보가 트리거되고, Cassandra 힙 Out of Memory Errors 카운트가 1씩 증가합니다.

단계

1. 이벤트를 보려면 * 지원 * > * 도구 * > * 그리드 토폴로지 * > * 구성 * 을 선택합니다.
2. Cassandra 힙 Out of Memory Errors 카운트가 1 이상인지 확인합니다.

   가능합니다 진단 유틸리티를 실행합니다 그리드의 현재 상태에 대한 추가 정보를 얻습니다.

3. '/var/local/core/'로 이동하여 "Cassandra.hprof' 파일을 압축하고 기술 지원 부서에 보냅니다.
4. Cassandra.hprof 파일을 백업하고 "/var/local/core/directory"에서 삭제합니다.

이 파일은 24GB까지 커질 수 있으므로 이 파일을 제거하여 공간을 확보해야 합니다.

5. 문제가 해결된 후 Cassandra 힙 Out of Memory Errors 카운트에 대한 * Reset * 확인란을 선택합니다. 그런 다음 * 변경 사항 적용 * 을 선택합니다.

> 이벤트 수를 재설정하려면 그리드 토폴로지 페이지 구성 권한이 있어야 합니다.

인증서 오류 문제 해결

웹 브라우저, S3 또는 Swift 클라이언트 또는 외부 모니터링 도구를 사용하여 StorageGRID에 연결하려고 할 때 보안 또는 인증서 문제가 발생하는 경우 인증서를 확인해야 합니다.

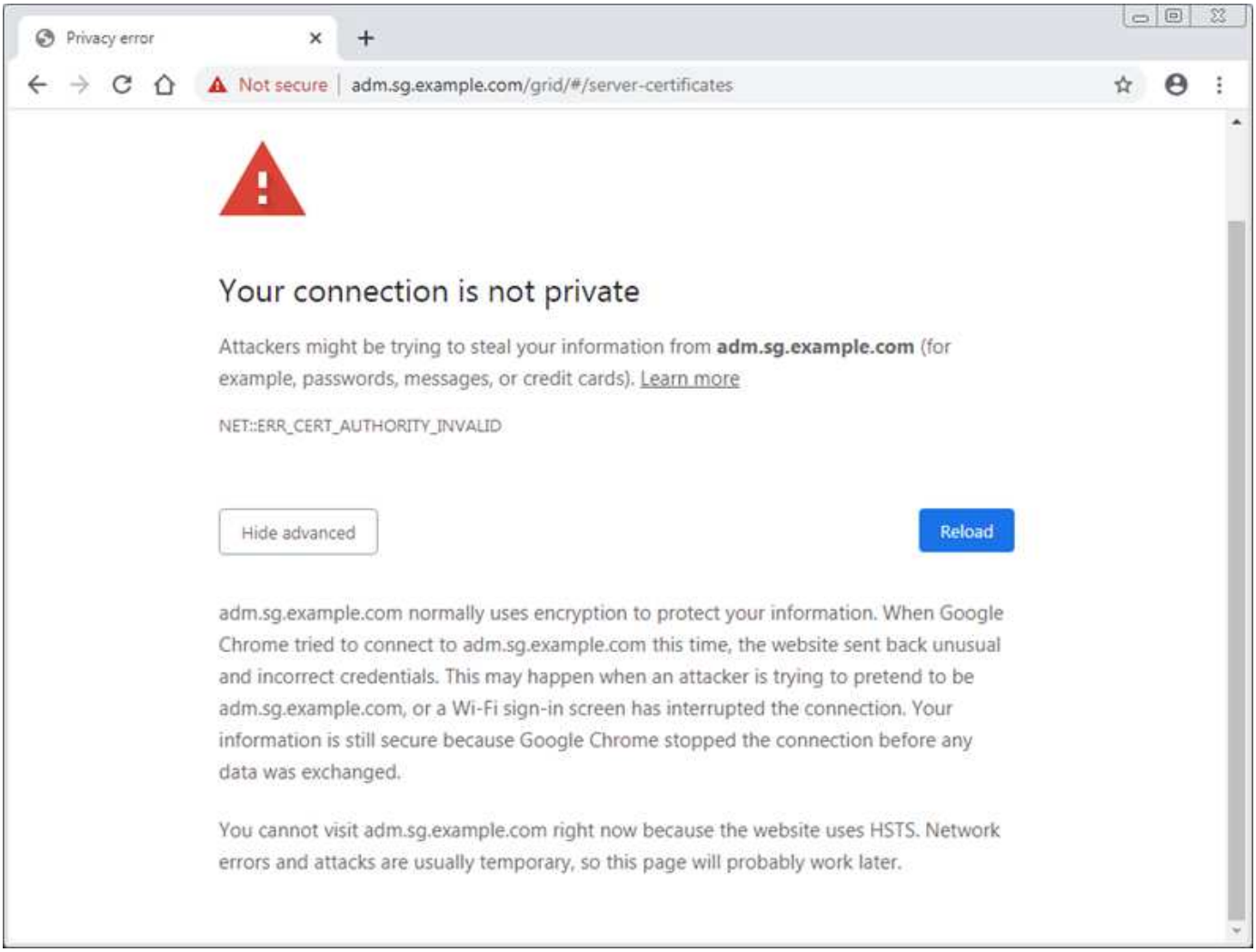
이 작업에 대해

그리드 관리자, 그리드 관리 API, 테넌트 관리자 또는 테넌트 관리 API를 사용하여 StorageGRID에 연결하려고 하면 인증서 오류로 인해 문제가 발생할 수 있습니다. S3, Swift 클라이언트 또는 외부 모니터링 도구에 연결하려고 할 때도 인증서 오류가 발생할 수 있습니다.

IP 주소 대신 도메인 이름을 사용하여 Grid Manager 또는 Tenant Manager에 액세스하는 경우, 다음 중 하나가 발생할 경우 브라우저에 인증서 오류가 표시되지 않고 무시하도록 옵션이 표시되지 않습니다.

- 사용자 지정 관리 인터페이스 인증서가 만료됩니다.
- 사용자 지정 관리 인터페이스 인증서에서 기본 서버 인증서로 되돌립니다.

다음 예에서는 사용자 지정 관리 인터페이스 인증서가 만료된 경우 인증서 오류를 보여 줍니다.



실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 서버 인증서가 곧 만료될 때 * Management Interface * 용 서버 인증서 만료 알림이 트리거됩니다.

외부 Prometheus 통합에 클라이언트 인증서를 사용하는 경우 StorageGRID 관리 인터페이스 인증서 또는 클라이언트 인증서로 인해 인증서 오류가 발생할 수 있습니다. 인증서 페이지에 구성된 * 클라이언트 인증서 만료 * 경고는 클라이언트 인증서가 곧 만료될 때 트리거됩니다.

단계

만료된 인증서에 대한 경고 알림을 받은 경우 인증서 세부 정보에 액세스합니다. 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 적절한 인증서 탭을 선택합니다.

1. 인증서의 유효 기간을 확인합니다. + 일부 웹 브라우저 및 S3 또는 Swift 클라이언트는 398일이 넘는 유효 기간이 있는 인증서를 수락하지 않습니다.
2. 인증서가 만료되었거나 곧 만료될 예정이면 새 인증서를 업로드하거나 생성합니다.
   - 서버 인증서의 경우 의 단계를 참조하십시오 Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성.
   - 클라이언트 인증서의 경우 의 단계를 참조하십시오 클라이언트 인증서 구성.
3. 서버 인증서 오류의 경우 다음 옵션 중 하나 또는 모두를 시도해 보십시오.
   - 인증서의 SAN(Subject Alternative Name)이 채워지고 SAN이 연결 중인 노드의 IP 주소 또는 호스트 이름과 일치하는지 확인합니다.

- 도메인 이름을 사용하여 StorageGRID에 연결하려는 경우:
  i. 연결 오류를 무시하고 Grid Manager에 액세스하려면 도메인 이름 대신 관리 노드의 IP 주소를 입력합니다.
  ii. 그리드 관리자에서 * 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 적절한 인증서 탭을 선택합니다 새 사용자 지정 인증서를 설치하거나 기본 인증서를 계속 사용합니다.
  iii. StorageGRID 관리에 대한 지침은 의 단계를 참조하십시오 Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성.

관리 노드 및 사용자 인터페이스 문제를 해결합니다

관리 노드 및 StorageGRID 사용자 인터페이스와 관련된 문제의 원인을 파악하는 데 도움이 되는 몇 가지 작업을 수행할 수 있습니다.

로그인 오류 문제 해결

StorageGRID 관리 노드에 로그인할 때 오류가 발생하는 경우 ID 페더레이션 구성, 네트워킹 또는 하드웨어 문제, 관리 노드 서비스 문제 또는 연결된 스토리지 노드의 Cassandra 데이터베이스 관련 문제가 시스템에 발생할 수 있습니다.

필요한 것

- "passwords.txt" 파일이 있어야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

관리 노드에 로그인하려고 할 때 다음 오류 메시지가 나타나면 다음 문제 해결 지침을 사용하십시오.

- "이 계정에 대한 귀하의 자격 증명이 유효하지 않습니다. 다시 시도하십시오
- "서비스 시작 대기 중…
- '내부 서버 오류. 서버에 오류가 발생하여 요청을 완료할 수 없습니다. 다시 시도하십시오. 문제가 지속되면 기술 지원 부서에 문의하십시오
- 서버와 통신할 수 없습니다. 페이지를 다시 로드하는 중…

단계

1. 10분 정도 기다린 후 다시 로그인하세요.

   오류가 자동으로 해결되지 않으면 다음 단계로 이동합니다.

2. StorageGRID 시스템에 둘 이상의 관리 노드가 있는 경우 다른 관리 노드에서 그리드 관리자에 로그인을 시도하십시오.
   - 로그인할 수 있는 경우 * 대시보드 *, * 노드 *, * 알림 * 및 * 지원 * 옵션을 사용하여 오류의 원인을 확인할 수 있습니다.
   - 관리자 노드가 하나뿐이거나 여전히 로그인할 수 없는 경우 다음 단계로 이동합니다.
3. 노드의 하드웨어가 오프라인인지 확인합니다.
4. StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 StorageGRID 관리 지침에 따라 SSO(Single Sign-On) 구성 단계를 참조하십시오.

   문제를 해결하려면 단일 관리 노드에 대해 SSO를 일시적으로 비활성화하고 다시 활성화해야 할 수 있습니다.

SSO가 활성화된 경우 제한된 포트를 사용하여 로그인할 수 없습니다. 포트 443을 사용해야 합니다.

5. 사용 중인 계정이 통합 사용자에 속하는지 확인합니다.

   통합 사용자 계정이 작동하지 않는 경우 그리드 관리자에 root 와 같은 로컬 사용자로 로그인합니다.

   - 로컬 사용자가 로그인할 수 있는 경우:
     i. 표시된 알람을 검토합니다.
     ii. 구성 * > * 액세스 제어 * > * ID 페더레이션 * 을 선택합니다.
     iii. LDAP 서버에 대한 연결 설정을 확인하려면 * 연결 테스트 * 를 클릭합니다.
     iv. 테스트에 실패한 경우 구성 오류를 해결합니다.
   - 로컬 사용자가 로그인할 수 없고 자격 증명이 올바르다는 확신이 있으면 다음 단계로 이동합니다.

6. SSH(Secure Shell)를 사용하여 관리자 노드에 로그인합니다.
   a. ssh admin@Admin_Node_IP' 명령어를 입력한다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

7. 그리드 노드에서 실행 중인 모든 서비스의 상태를 'toragegrid-status'로 봅니다

   NMS, mi, nginx 및 관리 API 서비스가 모두 실행 중인지 확인합니다.

   서비스 상태가 변경되면 출력이 즉시 업데이트됩니다.

```
$ storagegrid-status
Host Name                       99-211
IP Address                      10.96.99.211
Operating System Kernel         4.19.0         Verified
Operating System Environment    Debian 10.1    Verified
StorageGRID Webscale Release    11.4.0         Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                 5.5.9999+default Running
Network Monitoring              11.4.0         Running
Time Synchronization            1:4.2.8p10+dfsg Running
ams                             11.4.0         Running
cmn                             11.4.0         Running
nms                             11.4.0         Running
ssm                             11.4.0         Running
mi                              11.4.0         Running
dynip                           11.4.0         Running
nginx                           1.10.3         Running
tomcat                          9.0.27         Running
grafana                         6.4.3          Running
mgmt api                        11.4.0         Running
prometheus                      11.4.0         Running
persistence                     11.4.0         Running
ade exporter                    11.4.0         Running
alertmanager                    11.4.0         Running
attrDownPurge                   11.4.0         Running
attrDownSamp1                   11.4.0         Running
attrDownSamp2                   11.4.0         Running
node exporter                   0.17.0+ds      Running
sg snmp agent                   11.4.0         Running
```

8. nginx-GW 서비스가 `#service nginx-GW status'를 실행 중인지 확인한다
9. 로그 수집에 lumberjack을 사용합니다. 로그 수집: "#/usr/local/sbin/lumberjack.rb"

   이전에 실패한 인증이 발생한 경우 — start 및 - end lumberjack 스크립트 옵션을 사용하여 적절한 시간 범위를 지정할 수 있습니다. 이러한 옵션에 대한 자세한 내용은 lumberjack-h를 사용하십시오.

   터미널에 대한 출력은 로그 아카이브가 복사된 위치를 나타냅니다.

10. 다음 로그를 검토합니다.
    - '/var/local/log/bycast.log'
    - '/var/local/log/bycast-err.log'
    - '/var/local/log/NMS.log'
    - '*/ commands.txt'

11. 관리 노드에서 문제를 식별할 수 없는 경우 다음 명령 중 하나를 실행하여 사이트에서 ADC 서비스를 실행하는 세 개의 스토리지 노드의 IP 주소를 확인합니다. 일반적으로 사이트에 설치된 처음 세 개의 스토리지 노드입니다.

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

관리 노드는 인증 프로세스 중에 ADC 서비스를 사용합니다.

12. 관리 노드에서 확인한 IP 주소를 사용하여 각 ADC 스토리지 노드에 로그인합니다.
    a. ssh admin@grid_node_ip' 명령을 입력한다
    b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
    c. 루트로 전환하려면 다음 명령을 입력합니다
    d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

    루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

13. 그리드 노드에서 실행 중인 모든 서비스의 상태를 'toragegrid-status'로 봅니다

    idnt, acct, nginx 및 cassandra 서비스가 모두 실행 중인지 확인합니다.

14. 단계를 반복합니다 로그를 수집하려면 Lumberjack을 사용합니다 및 로그를 검토합니다 스토리지 노드의 로그를 검토합니다.
15. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

    기술 지원 팀에 수집한 로그를 제공합니다. 도 참조하십시오 로그 파일 참조.

사용자 인터페이스 문제를 해결합니다

새 버전의 StorageGRID 소프트웨어로 업그레이드한 후 그리드 관리자 또는 테넌트 관리자에 문제가 발생할 수 있습니다.

웹 인터페이스가 예상대로 응답하지 않습니다

StorageGRID 소프트웨어를 업그레이드한 후 그리드 관리자 또는 테넌트 관리자가 예상대로 응답하지 않을 수 있습니다.

웹 인터페이스에 문제가 있는 경우:

- 를 사용하고 있는지 확인합니다 지원되는 웹 브라우저.

  StorageGRID 11.5에 대한 브라우저 지원이 변경되었습니다. 지원되는 버전을 사용하고 있는지 확인합니다.

- 웹 브라우저 캐시를 지웁니다.

캐시를 지우면 이전 버전의 StorageGRID 소프트웨어에서 사용된 오래된 리소스가 제거되고 사용자 인터페이스가 다시 올바르게 작동할 수 있습니다. 자세한 내용은 웹 브라우저 설명서를 참조하십시오.

사용할 수 없는 관리자 노드의 상태를 확인합니다

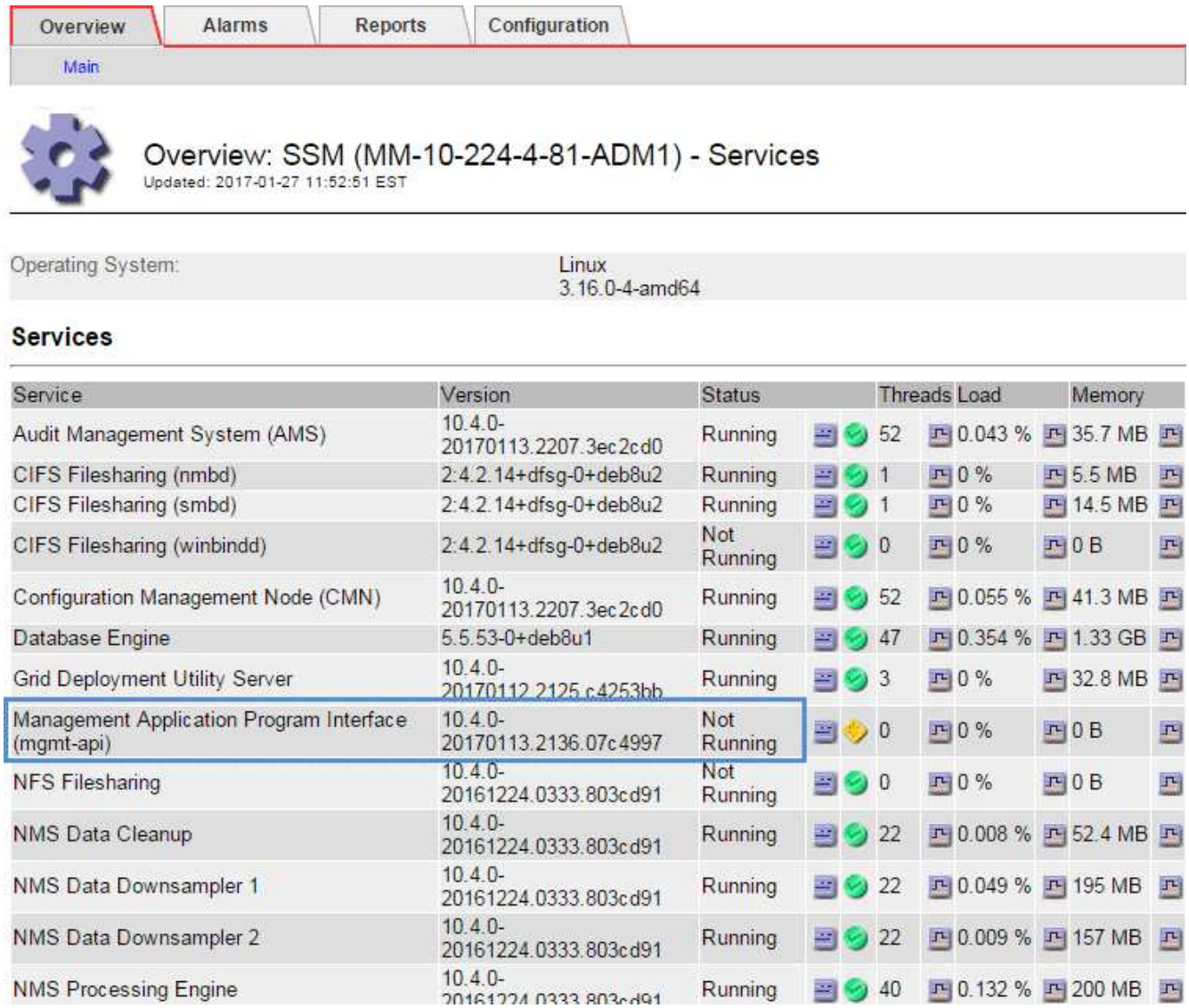
StorageGRID 시스템에 여러 관리 노드가 포함된 경우 다른 관리 노드를 사용하여 사용할 수 없는 관리 노드의 상태를 확인할 수 있습니다.

필요한 것

특정 액세스 권한이 있어야 합니다.

단계

1. 사용 가능한 관리 노드에서 를 사용하여 그리드 관리자에 로그인합니다 지원되는 웹 브라우저.
2. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
3. 사이트 * > * 사용할 수 없는 관리자 노드 _ * > * SSM * > * 서비스 * > * 개요 * > * 주 * 를 선택합니다.
4. Not Running 상태이고 파란색으로 표시될 수 있는 서비스를 찾습니다.



5. 알람이 트리거되었는지 확인합니다.

6. 적절한 조치를 통해 문제를 해결합니다.

관련 정보

StorageGRID 관리

네트워크, 하드웨어 및 플랫폼 문제를 해결합니다

StorageGRID 네트워크, 하드웨어 및 플랫폼 문제와 관련된 문제의 원인을 파악하는 데 도움이 되는 몇 가지 작업을 수행할 수 있습니다.

'''422:처리할 수 없는 엔티티''' 오류를 해결합니다

422:처리할 수 없는 엔터티는 여러 상황에서 발생할 수 있습니다. 오류 메시지를 확인하여 문제의 원인을 파악합니다.

나열된 오류 메시지 중 하나가 표시되면 권장 조치를 취하십시오.

오류 메시지	근본 원인 및 수정 조치

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	이 메시지는 Windows AD(Active Directory)를 사용하여 ID 페더레이션을 구성할 때 TLS(Transport Layer Security)에 대해 TLS * 사용 안 함 옵션을 선택한 경우에 발생할 수 있습니다.
	
	LDAP 서명을 적용하는 AD 서버에서는 * TLS 사용 안 함 * 옵션을 사용할 수 없습니다. STARTTLS* 사용 옵션 또는 TLS에 대한 * LDAPS* 사용 옵션을 선택해야 합니다.

오류 메시지	근본 원인 및 수정 조치

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	이 메시지는 지원되지 않는 암호화를 사용하여 StorageGRID에서 페더레이션 또는 클라우드 스토리지 풀을 식별하는 데 사용되는 외부 시스템으로 TLS(전송 계층 보안) 연결을 하려고 할 때 나타납니다.
	
	외부 시스템에서 제공하는 Cipherer를 확인한다. 시스템은 StorageGRID 관리 지침에 나와 있는 것처럼 발신 TLS 연결에 대해 StorageGRID에서 지원하는 암호 중 하나를 사용해야 합니다.

관련 정보

StorageGRID 관리

그리드 네트워크 **MTU** 불일치 경고를 해결합니다

그리드 네트워크 인터페이스(eth0)에 대한 최대 전송 단위(MTU) 설정이 그리드의 노드 간에 상당히 다를 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다.

이 작업에 대해

MTU 설정의 차이는 일부(전기는 아님) eth0 네트워크가 점보 프레임에 맞게 구성되었다는 것을 나타낼 수 있습니다. MTU 크기가 1000보다 크면 네트워크 성능 문제가 발생할 수 있습니다.

단계

1. 모든 노드의 eth0에 대한 MTU 설정을 나열합니다.
   - Grid Manager에 제공된 쿼리를 사용합니다.
   - "*primary Admin Node IP address*/metrics/graph"로 이동하여 "node_network_mtu_bytes{interface='eth0'}" 쿼리를 입력합니다
2. 모든 노드의 그리드 네트워크 인터페이스(eth0)와 동일한지 확인하기 위해 필요에 따라 MTU 설정을 수정합니다.
   - 어플라이언스 노드의 경우 어플라이언스의 설치 및 유지보수 지침을 참조하십시오.
   - Linux 및 VMware 기반 노드의 경우 '/usr/sbin/change-ip.py [-h] [-n node] MTU network [network...]' 명령을 사용합니다
     - 예 *:'change-ip.py-n node 1500 grid admin'
     - 참고 *: Linux 기반 노드에서 컨테이너에 있는 네트워크에 대해 원하는 MTU 값이 호스트 인터페이스에 이미 구성된 값을 초과하는 경우, 먼저 원하는 MTU 값을 사용하도록 호스트 인터페이스를 구성해야 합니다. 그런 다음 change-ip.py 스크립트를 사용하여 컨테이너에 있는 네트워크의 MTU 값을 변경합니다.

   Linux 또는 VMware 기반 노드에서 MTU를 수정하려면 다음 인수를 사용하십시오.

위치 인수	설명
'mtu'입니다	설정할 MTU입니다. 1280 ~ 9216 범위에 있어야 합니다.
네트워크	MTU를 적용할 네트워크입니다. 다음 네트워크 유형 중 하나 이상을 포함합니다. • 그리드 • 관리자 • 클라이언트

+

선택적 인수입니다	설명
'-h,-help'	도움말 메시지를 표시하고 종료합니다.
'-n node, -node node'	노드. 기본값은 로컬 노드입니다.

관련 정보

SG100 및 SG1000 서비스 어플라이언스

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG5600 스토리지 어플라이언스

NRER(Network Receive Error) 경보 문제를 해결합니다

네트워크 수신 오류(NRER) 경보는 StorageGRID와 네트워크 하드웨어 간의 연결 문제로 인해 발생할 수 있습니다. 경우에 따라 NRER 오류는 수동 개입 없이 해결할 수 있습니다. 오류가 지워지지 않으면 권장 조치를 취하십시오.

이 작업에 대해

NRER 경보는 StorageGRID에 연결되는 네트워크 하드웨어의 다음과 같은 문제로 인해 발생할 수 있습니다.

- 정방향 오류 수정(FEC)이 필요하며 사용되지 않습니다
- 스위치 포트와 NIC MTU가 일치하지 않습니다
- 높은 링크 오류율
- NIC 링 버퍼 오버런

단계

1. 네트워크 구성 시 NRER 알람의 모든 잠재적 원인에 대한 문제 해결 단계를 따르십시오.
    - FEC 불일치로 인해 오류가 발생한 경우 다음 단계를 수행하십시오.

- 참고 *: 이러한 단계는 StorageGRID 장비의 FEC 불일치로 인한 NRER 오류에만 적용됩니다.
  i. StorageGRID 어플라이언스에 연결된 스위치에 있는 포트의 FEC 상태를 확인합니다.
  ii. 제품에서 스위치로 연결되는 케이블의 물리적 무결성을 점검하십시오.
  iii. NRER 경보를 해결하기 위해 FEC 설정을 변경하려면 먼저 StorageGRID 어플라이언스 설치 프로그램의 링크 구성 페이지에서 어플라이언스가 * AUTO * 모드로 구성되어 있는지 확인하십시오 (어플라이언스 설치 및 유지 관리 지침 참조). 그런 다음 스위치 포트의 FEC 설정을 변경합니다. 가능한 경우 StorageGRID 어플라이언스 포트가 FEC 설정을 일치하도록 조정합니다.

     (StorageGRID 어플라이언스에서 FEC 설정을 구성할 수 없습니다. 대신 어플라이언스는 연결된 스위치 포트에서 FEC 설정을 검색하고 미러링하려고 합니다. 링크가 25GbE 또는 100GbE의 네트워크 속도로 강제 적용되는 경우 스위치와 NIC가 일반적인 FEC 설정을 협상하지 못할 수 있습니다. 일반 FEC 설정이 없으면 네트워크는 "no-FEC" 모드로 되돌아갑니다. FEC를 사용하지 않으면 전기 노이즈로 인해 발생한 오류가 연결에 더 취약합니다.)

- 참고 *: StorageGRID 어플라이언스는 FEC뿐만 아니라 FC(Firecode) 및 RS(Reed Solomon) FEC도 지원합니다.

◦ 스위치 포트 및 NIC MTU 불일치로 인해 오류가 발생한 경우 노드에 구성된 MTU 크기가 스위치 포트의 MTU 설정과 동일한지 확인합니다.

  노드에 구성된 MTU 크기가 노드가 연결된 스위치 포트의 설정보다 작을 수 있습니다. StorageGRID 노드가 MTU보다 큰 이더넷 프레임을 수신하는 경우, 이 구성에서 NRER 알람이 보고될 수 있습니다. 이러한 상황이 발생하는 것으로 판단될 경우 전체 MTU 목표 또는 요구 사항에 따라 스위치 포트의 MTU를 StorageGRID 네트워크 인터페이스 MTU와 일치하도록 변경하거나 StorageGRID 네트워크 인터페이스의 MTU를 스위치 포트에 맞게 변경합니다.

  > 최상의 네트워크 성능을 얻으려면 모든 노드를 그리드 네트워크 인터페이스에서 유사한 MTU 값으로 구성해야 합니다. 개별 노드의 그리드 네트워크에 대한 MTU 설정에 상당한 차이가 있을 경우 * Grid Network MTU mismatch * 경고가 트리거됩니다. MTU 값은 모든 네트워크 유형에 대해 같을 필요는 없습니다.

  > MTU 설정을 변경하려면 어플라이언스의 설치 및 유지보수 설명서를 참조하십시오.

◦ 링크 오류율이 높아 오류가 발생한 경우 다음 단계를 수행하십시오.
  i. FEC가 아직 활성화되지 않은 경우 FEC를 활성화합니다.
  ii. 네트워크 케이블 연결 품질이 양호하며 손상되었거나 잘못 연결되지 않았는지 확인합니다.
  iii. 케이블이 문제가 아닌 경우 기술 지원 부서에 문의하십시오.

  > 전기 소음이 많은 환경에서 높은 오류율을 느낄 수 있습니다.

◦ 오류가 NIC 링 버퍼 오버런인 경우 기술 지원 부서에 문의하십시오.

  링 버퍼는 StorageGRID 시스템이 과부하되어 적시에 네트워크 이벤트를 처리할 수 없을 때 오버런될 수 있습니다.

2. 기본 문제를 해결한 후 오류 카운터를 재설정합니다.
   a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.

b. site_ * > **GRID node* * > * SSM * > * Resources * > * Configuration * > * Main * 을 선택합니다.

c. 수신 오류 수 재설정 * 을 선택하고 * 변경 내용 적용 * 을 클릭합니다.

관련 정보

Grid Network MTU 불일치 알림 문제를 해결합니다

알람 기준(레거시 시스템)

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG5600 스토리지 어플라이언스

SG100 및 SG1000 서비스 어플라이언스

시간 동기화 오류 문제 해결

시간 동기화와 관련된 문제가 그리드에 나타날 수 있습니다.

시간 동기화 문제가 발생하면 각각 Stratum 3 이상의 참조를 제공하는 외부 NTP 소스를 4개 이상 지정했으며 모든 외부 NTP 소스가 정상적으로 작동하고 StorageGRID 노드에서 액세스할 수 있는지 확인합니다.

> 프로덕션 수준 StorageGRID 설치에 외부 NTP 소스를 지정할 때 Windows Server 2016 이전 버전의 Windows에서는 Windows 시간(W32Time) 서비스를 사용하지 마십시오. 이전 버전의 Windows의 시간 서비스는 정확하지 않으며 StorageGRID와 같은 고정밀 환경에서 사용하기 위해 Microsoft에서 지원되지 않습니다.

관련 정보

복구 및 유지 관리

Linux: 네트워크 연결 문제

Linux 호스트에서 호스팅되는 StorageGRID 그리드 노드의 네트워크 연결 문제가 발생할 수 있습니다.

MAC 주소 복제

경우에 따라 MAC 주소 클로닝을 사용하여 네트워크 문제를 해결할 수 있습니다. 가상 호스트를 사용하는 경우 노드 구성 파일에서 각 네트워크의 MAC 주소 클로닝 키 값을 "참"으로 설정합니다. 이 설정으로 인해 StorageGRID 컨테이너의 MAC 주소가 호스트의 MAC 주소를 사용하게 됩니다. 노드 구성 파일을 만들려면 해당 플랫폼의 설치 가이드에 있는 지침을 참조하십시오.

> Linux 호스트 OS에서 사용할 별도의 가상 네트워크 인터페이스를 생성합니다. Linux 호스트 OS 및 StorageGRID 컨테이너에 동일한 네트워크 인터페이스를 사용하면 하이퍼바이저에서 Promiscuous 모드가 활성화되지 않은 경우 호스트 OS에 연결할 수 없게 될 수 있습니다.

MAC 클로닝 활성화에 대한 자세한 내용은 해당 플랫폼 설치 안내서의 지침을 참조하십시오.

무차별 모드

MAC 주소 클로닝을 사용하지 않고 모든 인터페이스가 하이퍼바이저에 의해 할당된 것이 아닌 MAC 주소에 대한 데이터를 수신 및 전송하도록 허용하는 경우, 가상 스위치 및 포트 그룹 수준의 보안 속성이 Promiscuous Mode, MAC Address 변경 및 Forged 전송에 대해 * Accept * 로 설정되어 있는지 확인합니다. 가상 스위치에 설정된 값은 포트 그룹 수준의 값으로 재정의할 수 있으므로 두 위치에서 설정이 동일한지 확인합니다.

관련 정보

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

Ubuntu 또는 Debian을 설치합니다

리눅스: 노드 상태가 ""고아""입니다.

고립된 상태의 Linux 노드는 대개 StorageGRID 서비스나 노드의 컨테이너를 제어하는 StorageGRID 노드 데몬이 예기치 않게 종료되었음을 나타냅니다.

이 작업에 대해

Linux 노드가 분리된 상태에 있다고 보고하는 경우 다음을 수행해야 합니다.

- 로그에서 오류 및 메시지를 확인합니다.
- 노드를 다시 시작하려고 합니다.
- 필요한 경우 컨테이너 엔진 명령을 사용하여 기존 노드 컨테이너를 중지합니다.
- 노드를 다시 시작합니다.

단계

1. 서비스 데몬과 분리된 노드에 대한 로그에서 예기치 않은 종료에 대한 명백한 오류 또는 메시지를 확인합니다.
2. 호스트에 루트로 로그인하거나 sudo 권한이 있는 계정을 사용합니다.
3. '$sudo StorageGRID node start node-name' 명령을 실행하여 노드를 다시 시작합니다

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   노드가 분리된 경우 응답은 입니다

   ```
   Not starting ORPHANED node DC1-S1-172-16-1-172
   ```

4. Linux에서 컨테이너 엔진 및 모든 제어 StorageGRID 노드 프로세스를 중지합니다. 예를 들어, "SUDO docker stop-time secondscontainer-name"이 있습니다

   '초'의 경우 컨테이너가 중지될 때까지 대기하는 시간(일반적으로 15분 이하)을 입력합니다. 예를 들면 다음과 같습니다.

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. StorageGRID node start node-name 노드를 다시 시작합니다

```
storagegrid node start DC1-S1-172-16-1-172
```

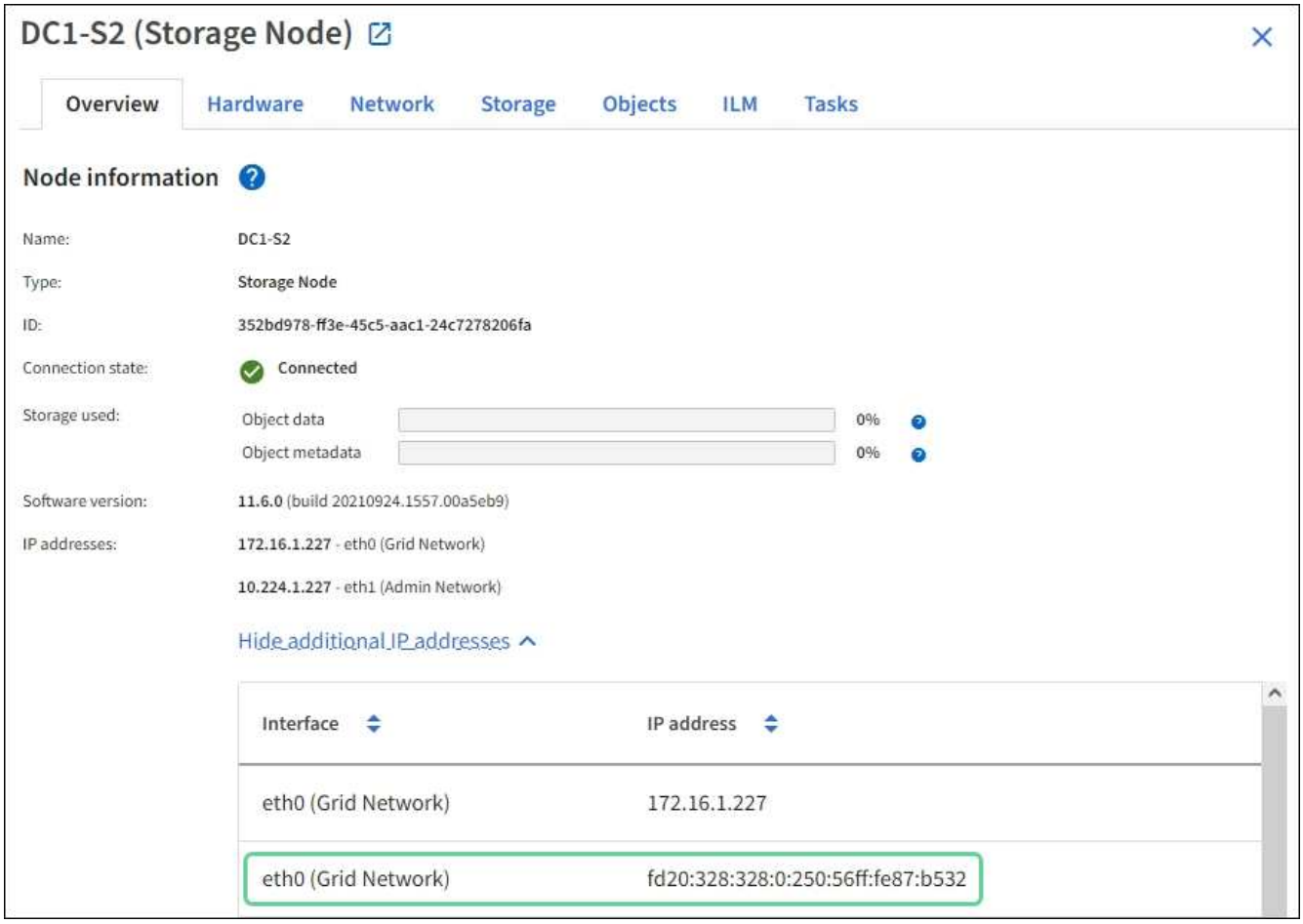
Linux: IPv6 지원 문제 해결

Linux 호스트에 StorageGRID 노드를 설치한 경우 커널에서 IPv6 지원을 활성화해야 하며, IPv6 주소가 예상대로 노드 컨테이너에 할당되지 않은 것을 확인할 수 있습니다.

이 작업에 대해

Grid Manager의 다음 위치에서 그리드 노드에 할당된 IPv6 주소를 볼 수 있습니다.

- nodes * 를 선택하고 노드를 선택합니다. 그런 다음 개요 탭에서 * IP 주소 * 옆에 * 더 보기 * 를 선택합니다.



- 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **NODE* * > * SSM * > * Resources * 를 선택합니다. IPv6 주소가 할당된 경우 * 네트워크 주소 * 섹션의 IPv4 주소 아래에 나열됩니다.

IPv6 주소가 표시되지 않고 노드가 Linux 호스트에 설치된 경우 다음 단계에 따라 커널에서 IPv6 지원을 활성화합니다.

단계

1. 호스트에 루트로 로그인하거나 sudo 권한이 있는 계정을 사용합니다.
2. 'sysctl net.ipv6.conf.all.disable_ipv6' 명령을 실행합니다

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

결과는 0이어야 합니다.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

> 결과가 0이 아니면 운영 체제 설명서에서 'sysctl' 설정을 변경합니다. 그런 다음 계속하기 전에 값을 0으로 변경합니다.

3. StorageGRID node container: 'StorageGRID node enter node-name'을 입력합니다
4. 'sysctl net.ipv6.conf.all.disable_ipv6' 명령을 실행합니다

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

결과는 1이어야 합니다.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

> 결과가 1이 아닌 경우 이 절차는 적용되지 않습니다. 기술 지원 부서에 문의하십시오.

5. 컨테이너 'exit'를 종료합니다

```
root@DC1-S1:~ # exit
```

6. 루트로 '/var/lib/StorageGrid/settings/sysctl.d/net.conf' 파일을 편집합니다.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. 다음 두 줄을 찾아 주석 태그를 제거합니다. 그런 다음 파일을 저장하고 닫습니다.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. 다음 명령을 실행하여 StorageGRID 컨테이너를 다시 시작합니다.

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

외부 **syslog** 서버의 문제를 해결합니다

다음 표에서는 외부 syslog 서버 오류 메시지에 대해 설명하고 수정 조치를 나열합니다.

오류 메시지	설명 및 권장 조치
호스트 이름을 확인할 수 없습니다	syslog 서버에 대해 입력한 FQDN을 IP 주소로 확인할 수 없습니다. 1. 입력한 호스트 이름을 확인하십시오. IP 주소를 입력한 경우 W.X.Y.Z("점분리 십진수") 표기법으로 유효한 IP 주소인지 확인합니다. 2. DNS 서버가 올바르게 구성되었는지 확인합니다. 3. 각 노드가 DNS 서버의 IP 주소에 액세스할 수 있는지 확인합니다.
연결이 거부되었습니다	syslog 서버에 대한 TCP 또는 TLS 연결이 거부되었습니다. 호스트의 TCP 또는 TLS 포트에서 수신 대기 중인 서비스가 없거나 방화벽이 액세스를 차단하고 있을 수 있습니다. 1. syslog 서버에 대해 올바른 FQDN 또는 IP 주소, 포트 및 프로토콜을 입력했는지 확인합니다. 2. syslog 서비스의 호스트가 지정된 포트에서 수신 대기하는 syslog 데몬을 실행 중인지 확인합니다. 3. 방화벽이 노드에서 syslog 서버의 IP 및 포트로의 TCP/TLS 연결에 대한 액세스를 차단하지 않는지 확인합니다.
네트워크에 연결할 수 없습니다	syslog 서버가 직접 연결된 서브넷에 없습니다. 라우터가 ICMP 오류 메시지를 반환하여 나열된 노드의 테스트 메시지를 syslog 서버로 전달할 수 없음을 나타냅니다. 1. syslog 서버에 대한 올바른 FQDN 또는 IP 주소를 입력했는지 확인합니다. 2. 나열된 각 노드에 대해 그리드 네트워크 서브넷 목록, 관리 네트워크 서브넷 목록 및 클라이언트 네트워크 게이트웨이를 확인합니다. 트래픽이 예상 네트워크 인터페이스 및 게이트웨이(Grid, Admin 또는 Client)를 통해 syslog 서버로 라우팅되도록 구성되었는지 확인합니다.

오류 메시지	설명 및 권장 조치
호스트에 연결할 수 없습니다	syslog 서버는 직접 연결된 서브넷(그리드, 관리 또는 클라이언트 IP 주소에 대해 나열된 노드에서 사용하는 서브넷)에 있습니다. 노드가 테스트 메시지를 보내려고 시도했지만 syslog 서버의 MAC 주소에 대한 ARP 요청에 대한 응답을 수신하지 못했습니다. 1. syslog 서버에 대한 올바른 FQDN 또는 IP 주소를 입력했는지 확인합니다. 2. syslog 서비스를 실행 중인 호스트가 작동 중인지 확인합니다.
연결 시간이 초과되었습니다	TCP/TLS 연결을 시도했지만 오랫동안 syslog 서버로부터 응답이 수신되지 않았습니다. 라우팅 구성이 잘못되거나 방화벽이 응답을 보내지 않고 트래픽을 떨어뜨릴 수 있습니다(공통 구성). 1. syslog 서버에 대한 올바른 FQDN 또는 IP 주소를 입력했는지 확인합니다. 2. 나열된 각 노드에 대해 그리드 네트워크 서브넷 목록, 관리 네트워크 서브넷 목록 및 클라이언트 네트워크 게이트웨이를 확인합니다. syslog 서버에 도달할 것으로 예상되는 네트워크 인터페이스 및 게이트웨이(Grid, Admin 또는 Client)를 통해 트래픽을 syslog 서버로 라우팅하도록 구성되었는지 확인합니다. 3. 방화벽이 syslog 서버의 IP 및 포트에 나열된 노드에서 TCP/TLS 연결에 대한 액세스를 차단하지 않는지 확인합니다.

파트너가 연결을 닫았습니다	syslog 서버에 대한 TCP 연결이 성공적으로 설정되었지만 나중에 종료되었습니다. 그 이유는 다음과 같습니다.
	
	• syslog 서버가 다시 시작되었거나 재부팅되었을 수 있습니다.
	• 노드와 syslog 서버의 TCP/TLS 설정이 다를 수 있습니다.
	• 중간 방화벽이 유휴 TCP 연결을 닫는 중일 수 있습니다.
	• syslog 서버 포트에서 수신 대기하는 비 syslog 서버가 연결을 닫았을 수 있습니다.
	  a. syslog 서버에 대해 올바른 FQDN 또는 IP 주소, 포트 및 프로토콜을 입력했는지 확인합니다.
	  b. TLS를 사용하는 경우 syslog 서버가 TLS도 사용하고 있는지 확인합니다. TCP를 사용하는 경우 syslog 서버가 TCP도 사용하고 있는지 확인합니다.
	  c. 유휴 TCP 연결을 종료하도록 중간 방화벽이 구성되어 있지 않은지 확인합니다.

오류 메시지	설명 및 권장 조치
TLS 인증서 오류입니다	syslog 서버로부터 받은 서버 인증서가 제공된 CA 인증서 번들 및 클라이언트 인증서와 호환되지 않습니다. 1. CA 인증서 번들 및 클라이언트 인증서(있는 경우)가 syslog 서버의 서버 인증서와 호환되는지 확인합니다. 2. syslog 서버의 서버 인증서 ID에 예상 IP 또는 FQDN 값이 포함되어 있는지 확인합니다.
전달이 일시 중단되었습니다	syslog 레코드가 더 이상 syslog 서버로 전달되지 않으며 StorageGRID에서 이유를 감지할 수 없습니다. 이 오류와 함께 제공된 디버깅 로그를 검토하여 근본 원인을 확인합니다.
TLS 세션이 종료되었습니다	syslog 서버가 TLS 세션을 종료했으며 StorageGRID에서 이유를 감지할 수 없습니다. 1. 이 오류와 함께 제공된 디버깅 로그를 검토하여 근본 원인을 확인합니다. 2. syslog 서버에 대해 올바른 FQDN 또는 IP 주소, 포트 및 프로토콜을 입력했는지 확인합니다. 3. TLS를 사용하는 경우 syslog 서버가 TLS도 사용하고 있는지 확인합니다. TCP를 사용하는 경우 syslog 서버가 TCP도 사용하고 있는지 확인합니다. 4. CA 인증서 번들 및 클라이언트 인증서(있는 경우)가 syslog 서버의 서버 인증서와 호환되는지 확인합니다. 5. syslog 서버의 서버 인증서 ID에 예상 IP 또는 FQDN 값이 포함되어 있는지 확인합니다.
결과 쿼리에 실패했습니다	syslog 서버 구성 및 테스트에 사용된 관리자 노드가 나열된 노드에서 테스트 결과를 요청할 수 없습니다. 하나 이상의 노드가 다운되었을 수 있습니다. 1. 표준 문제 해결 단계를 수행하여 노드가 온라인 상태이고 모든 예상 서비스가 실행 중인지 확인합니다. 2. 나열된 노드에서 오류 서비스를 다시 시작합니다.

경고 참조

다음 표에는 모든 기본 StorageGRID 경고가 나와 있습니다. 필요에 따라 시스템 관리 방식에 맞게 사용자 지정 경고 규칙을 만들 수 있습니다.

에 대한 정보를 참조하십시오 일반적으로 사용되는 Prometheus 메트릭입니다 이러한 알림 중 일부에 사용된 메트릭에 대해 알아봅니다.

경고 이름입니다	설명 및 권장 조치

어플라이언스 배터리가 만료되었습니다	제품의 저장소 컨트롤러 배터리가 만료되었습니다.
	
	1. 배터리를 교체합니다. 전지 분리 및 교체 단계는 저장 컨트롤러 교체 절차에 포함되어 있습니다. 스토리지 어플라이언스에 대한 지침을 참조하십시오.
	  ◦ SG5600 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스
	2. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.

어플라이언스 배터리 고장	제품의 저장소 컨트롤러 에 있는 배터리가 실패했습니다.
	
	1. 배터리를 교체합니다. 전지 분리 및 교체 단계는 저장 컨트롤러 교체 절차에 포함되어 있습니다. 스토리지 어플라이언스에 대한 지침을 참조하십시오.
	  ◦ SG5600 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스
	2. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.

어플라이언스 배터리가 학습된 용량이 부족합니다	제품의 저장 장치 컨트롤러의 배터리가 학습된 용량이 부족합니다.
	
	1. 배터리를 교체합니다. 전지 분리 및 교체 단계는 저장 컨트롤러 교체 절차에 포함되어 있습니다. 스토리지 어플라이언스에 대한 지침을 참조하십시오.
	  ◦ SG5600 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스
	2. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.

어플라이언스 배터리 수명이 거의 다 되었습니다	어플라이언스 저장소 컨트롤러의 배터리 수명이 거의 다했습니다.
	
	1. 배터리를 곧 교체하십시오. 전지 분리 및 교체 단계는 저장 컨트롤러 교체 절차에 포함되어 있습니다. 스토리지 어플라이언스에 대한 지침을 참조하십시오.
	  ◦ SG5600 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스
	2. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.

경고 이름입니다	설명 및 권장 조치

제품 배터리가 제거되었습니다	제품의 저장 컨트롤러에 배터리가 없습니다.
	
	1. 배터리를 장착하십시오. 전지 분리 및 교체 단계는 저장 컨트롤러 교체 절차에 포함되어 있습니다. 스토리지 어플라이언스에 대한 지침을 참조하십시오.
	  ◦ SG5600 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스
	2. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.

제품 배터리가 너무 뜨겁습니다	제품 보관 컨트롤러의 배터리가 과열되었습니다. 1. 이 노드에 영향을 주는 다른 경고가 있는지 확인합니다. 이 경고는 다른 경고를 해결할 때 해결될 수 있습니다. 2. 팬 또는 HVAC 장애와 같은 온도 상승의 가능한 원인을 조사하십시오. 3. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.

어플라이언스 BMC 통신 오류입니다	베이스보드 관리 컨트롤러(BMC)와의 통신이 끊어졌습니다.
	
	1. BMC가 정상적으로 작동하는지 확인합니다. nodes * 를 선택한 다음 어플라이언스 노드의 * Hardware * 탭을 선택합니다. Compute Controller BMC IP 필드를 찾아 해당 IP로 이동합니다.
	2. 노드를 유지보수 모드로 전환한 다음 어플라이언스 전원을 껐다가 다시 켜서 BMC 통신을 복구해 보십시오. 사용 중인 제품의 지침을 참조하십시오.
	  ◦ SG100 및 SG1000 서비스 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스
	3. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.

어플라이언스 캐시 백업 디바이스에 장애가 발생했습니다	영구 캐시 백업 디바이스가 실패했습니다. 1. 이 노드에 영향을 주는 다른 경고가 있는지 확인합니다. 이 경고는 다른 경고를 해결할 때 해결될 수 있습니다. 2. 기술 지원 부서에 문의하십시오.
어플라이언스 캐시 백업 디바이스의 용량이 부족합니다	캐시 백업 디바이스 용량이 부족합니다. 기술 지원 부서에 문의하십시오.
어플라이언스 캐시 백업 디바이스 쓰기 방지	캐시 백업 디바이스가 쓰기 금지되어 있습니다. 기술 지원 부서에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
어플라이언스 캐시 메모리 크기가 일치하지 않습니다	어플라이언스의 두 컨트롤러는 캐시 크기가 다릅니다. 기술 지원 부서에 문의하십시오.

어플라이언스의 컴퓨팅 컨트롤러 섀시 온도가 너무 높습니다	StorageGRID 어플라이언스의 컴퓨팅 컨트롤러 온도가 공칭 임계값을 초과했습니다.
	
	1. 하드웨어 구성 요소의 과열 상태를 점검하고 권장 조치를 따르십시오.
	  ◦ SG100, SG1000 또는 SG6000을 사용하는 경우 BMC를 사용하십시오.
	  ◦ SG5600 또는 SG5700을 사용하는 경우 SANtricity 시스템 관리자를 사용하십시오.
	2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오.
	  ◦ SG100 및 SG1000 서비스 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG5600 스토리지 어플라이언스

어플라이언스의 컴퓨팅 컨트롤러 CPU 온도가 너무 높습니다	StorageGRID 어플라이언스의 컴퓨팅 컨트롤러에 있는 CPU 온도가 공칭 임계값을 초과했습니다.
	
	1. 하드웨어 구성 요소의 과열 상태를 점검하고 권장 조치를 따르십시오.
	  ◦ SG100, SG1000 또는 SG6000을 사용하는 경우 BMC를 사용하십시오.
	  ◦ SG5600 또는 SG5700을 사용하는 경우 SANtricity 시스템 관리자를 사용하십시오.
	2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오.
	  ◦ SG100 및 SG1000 서비스 어플라이언스
	  ◦ SG5600 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스

경고 이름입니다	설명 및 권장 조치

어플라이언스 컴퓨팅 컨트롤러에 주의가 필요합니다	StorageGRID 어플라이언스의 컴퓨팅 컨트롤러에서 하드웨어 장애가 감지되었습니다.
	
	1. 하드웨어 구성 요소에 오류가 있는지 확인하고 권장 조치를 따르십시오.
	  ◦ SG100, SG1000 또는 SG6000을 사용하는 경우 BMC를 사용하십시오.
	  ◦ SG5600 또는 SG5700을 사용하는 경우 SANtricity 시스템 관리자를 사용하십시오.
	2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오.
	  ◦ SG100 및 SG1000 서비스 어플라이언스
	  ◦ SG5600 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스

어플라이언스 컴퓨팅 컨트롤러 전원 공급 장치 A에 문제가 있습니다	컴퓨팅 컨트롤러의 전원 공급 장치 A에 문제가 있습니다. 이 경고는 전원 공급 장치에 문제가 있거나 전원을 공급하는 데 문제가 있음을 나타낼 수 있습니다.
	
	1. 하드웨어 구성 요소에 오류가 있는지 확인하고 권장 조치를 따르십시오.
	  ◦ SG100, SG1000 또는 SG6000을 사용하는 경우 BMC를 사용하십시오.
	  ◦ SG5600 또는 SG5700을 사용하는 경우 SANtricity 시스템 관리자를 사용하십시오.
	2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오.
	  ◦ SG100 및 SG1000 서비스 어플라이언스
	  ◦ SG5600 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스

경고 이름입니다	설명 및 권장 조치
어플라이언스 컴퓨팅 컨트롤러 전원 공급 장치 B에 문제가 있습니다	컴퓨팅 컨트롤러의 전원 공급 장치 B에 문제가 있습니다. 이 알림은 전원 공급 장치에 오류가 발생했거나 전원을 공급하는 데 문제가 있음을 나타낼 수 있습니다. 1. 하드웨어 구성 요소에 오류가 있는지 확인하고 권장 조치를 따르십시오. ◦ SG100, SG1000 또는 SG6000을 사용하는 경우 BMC를 사용하십시오. ◦ SG5600 또는 SG5700을 사용하는 경우 SANtricity 시스템 관리자를 사용하십시오. 2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오. ◦ SG100 및 SG1000 서비스 어플라이언스 ◦ SG5600 스토리지 어플라이언스 ◦ SG5700 스토리지 어플라이언스 ◦ SG6000 스토리지 어플라이언스
어플라이언스 컴퓨팅 하드웨어 모니터 서비스가 중단되었습니다	스토리지 하드웨어 상태를 모니터링하는 서비스가 데이터 보고를 중지했습니다. 1. Base-OS에서 eos-system-status 서비스의 상태를 확인한다. 2. 서비스가 중지되었거나 오류 상태인 경우 서비스를 다시 시작합니다. 3. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.

경고 이름입니다	설명 및 권장 조치

어플라이언스 Fibre Channel 장애가 감지되었습니다	어플라이언스 스토리지 컨트롤러와 컴퓨팅 컨트롤러 간에 파이버 채널 링크 문제가 감지되었습니다.
	
	이 알림은 어플라이언스에서 스토리지와 컴퓨팅 컨트롤러 간의 파이버 채널 연결에 문제가 있음을 나타낼 수 있습니다.
	
	1. 하드웨어 구성 요소에서 오류를 확인합니다(* nodes * > **appliance node* * > * Hardware *). 구성 요소의 상태가 ""공칭""가 아닌 경우 다음 조치를 취하십시오.
	  a. 컨트롤러 간 파이버 채널 케이블이 완전히 연결되어 있는지 확인합니다.
	  b. Fibre Channel 케이블이 과도하게 구부러져 있지 않은지 확인합니다.
	  c. SFP+ 모듈이 올바르게 장착되었는지 확인합니다.
	  ▪ 참고: * 이 문제가 지속되면 StorageGRID 시스템에서 문제가 있는 연결을 자동으로 오프라인 상태로 전환할 수 있습니다.
	2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오.
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스

어플라이언스 Fibre Channel HBA 포트 오류입니다	Fibre Channel HBA 포트에 장애가 발생했거나 장애가 발생했습니다. 기술 지원 부서에 문의하십시오.

어플라이언스 플래시 캐시 드라이브가 최적이 아닙니다	SSD 캐시에 사용되는 드라이브가 최적화되지 않았습니다.
	
	1. SSD 캐시 드라이브를 교체합니다. 사용 중인 제품의 지침을 참조하십시오.
	  ◦ SG5600 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스
	2. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.

어플라이언스 상호 연결/배터리 캐니스터가 제거되었습니다	상호 연결/배터리 캐니스터가 없습니다.
	
	1. 배터리를 교체합니다. 전지 분리 및 교체 단계는 저장 컨트롤러 교체 절차에 포함되어 있습니다. 스토리지 어플라이언스 지침을 참조하십시오.
	  ◦ SG5600 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG6000 스토리지 어플라이언스
	2. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
어플라이언스 LACP 포트가 누락되었습니다	StorageGRID 어플라이언스의 포트가 LACP 결합에 사용되고 있지 않습니다. 1. 스위치의 구성을 확인하십시오. 인터페이스가 올바른 Link Aggregation 그룹에 구성되어 있는지 확인합니다. 2. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.
어플라이언스의 전체 전원 공급 장치 성능이 저하되었습니다	StorageGRID 제품의 전원이 권장 작동 전압을 벗어나 있습니다. 1. 전원 공급 장치 A 및 B의 상태를 점검하여 어떤 전원 공급 장치가 비정상적으로 작동하는지 확인하고 권장 조치를 따르십시오. ◦ SG100, SG1000 또는 SG6000을 사용하는 경우 BMC를 사용하십시오. ◦ SG5600 또는 SG5700을 사용하는 경우 SANtricity 시스템 관리자를 사용하십시오. 2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오. ◦ SG6000 스토리지 어플라이언스 ◦ SG5700 스토리지 어플라이언스 ◦ SG5600 스토리지 어플라이언스 ◦ SG100 및 SG1000 서비스 어플라이언스
어플라이언스 스토리지 컨트롤러 A에 장애가 발생했습니다	StorageGRID 어플라이언스의 스토리지 컨트롤러 A에 장애가 발생했습니다. 1. SANtricity 시스템 관리자를 사용하여 하드웨어 구성 요소를 확인하고 권장 조치를 수행하십시오. 2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오. ◦ SG6000 스토리지 어플라이언스 ◦ SG5700 스토리지 어플라이언스 ◦ SG5600 스토리지 어플라이언스
어플라이언스 스토리지 컨트롤러 B에 장애가 발생했습니다	StorageGRID 어플라이언스의 스토리지 컨트롤러 B에 장애가 발생했습니다. 1. SANtricity 시스템 관리자를 사용하여 하드웨어 구성 요소를 확인하고 권장 조치를 수행하십시오. 2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오. ◦ SG6000 스토리지 어플라이언스 ◦ SG5700 스토리지 어플라이언스 ◦ SG5600 스토리지 어플라이언스

경고 이름입니다	설명 및 권장 조치

어플라이언스 스토리지 컨트롤러 드라이브 오류입니다	StorageGRID 어플라이언스에 있는 하나 이상의 드라이브가 실패했거나 최적이 아닙니다.
	
	1. SANtricity 시스템 관리자를 사용하여 하드웨어 구성 요소를 확인하고 권장 조치를 수행하십시오.
	2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오.
	  ◦ SG6000 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG5600 스토리지 어플라이언스

어플라이언스 스토리지 컨트롤러 하드웨어 문제입니다	SANtricity 소프트웨어가 StorageGRID 어플라이언스의 구성 요소에 대해 "주의 필요"를 보고하고 있습니다.
	
	1. SANtricity 시스템 관리자를 사용하여 하드웨어 구성 요소를 확인하고 권장 조치를 수행하십시오.
	2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오.
	  ◦ SG6000 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG5600 스토리지 어플라이언스

어플라이언스 스토리지 컨트롤러 전원 공급 장치 A 고장	StorageGRID 제품의 전원 공급 장치 A가 권장 작동 전압을 벗어나고 있습니다.
	
	1. SANtricity 시스템 관리자를 사용하여 하드웨어 구성 요소를 확인하고 권장 조치를 수행하십시오.
	2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오.
	  ◦ SG6000 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG5600 스토리지 어플라이언스

경고 이름입니다	설명 및 권장 조치
어플라이언스 스토리지 컨트롤러 전원 공급 장치 B 오류입니다	StorageGRID 제품의 전원 공급 장치 B가 권장 작동 전압을 벗어나 있습니다. 1. SANtricity 시스템 관리자를 사용하여 하드웨어 구성 요소를 확인하고 권장 조치를 수행하십시오. 2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오. ◦ SG6000 스토리지 어플라이언스 ◦ SG5700 스토리지 어플라이언스 ◦ SG5600 스토리지 어플라이언스
어플라이언스 스토리지 하드웨어 모니터 서비스가 중단되었습니다	스토리지 하드웨어 상태를 모니터링하는 서비스가 데이터 보고를 중지했습니다. 1. Base-OS에서 eos-system-status 서비스의 상태를 확인한다. 2. 서비스가 중지되었거나 오류 상태인 경우 서비스를 다시 시작합니다. 3. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.
어플라이언스 스토리지 쉘프 성능이 저하되었습니다	스토리지 어플라이언스의 스토리지 쉘프에 있는 구성 요소 중 하나의 상태가 성능 저하입니다. 1. SANtricity 시스템 관리자를 사용하여 하드웨어 구성 요소를 확인하고 권장 조치를 수행하십시오. 2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오. ◦ SG6000 스토리지 어플라이언스 ◦ SG5700 스토리지 어플라이언스 ◦ SG5600 스토리지 어플라이언스
제품 온도가 초과되었습니다	제품 보관 컨트롤러의 공칭 또는 최대 온도를 초과했습니다. 1. 이 노드에 영향을 주는 다른 경고가 있는지 확인합니다. 이 경고는 다른 경고를 해결할 때 해결될 수 있습니다. 2. 팬 또는 HVAC 장애와 같은 온도 상승의 가능한 원인을 조사하십시오. 3. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.
제품 온도 센서가 제거되었습니다	온도 센서가 제거되었습니다. 기술 지원 부서에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
Cassandra 자동 콤팩터 오류입니다	Cassandra 자동 콤팩터에 오류가 발생했습니다. Cassandra 자동 압축 프로그램은 모든 스토리지 노드에 있으며, 과도한 워크로드를 덮어쓰기 및 삭제할 수 있도록 Cassandra 데이터베이스 크기를 관리합니다. 이 상태가 지속되는 동안 특정 워크로드에서 예기치 않게 높은 메타데이터 소비가 발생합니다. 1. 이 노드에 영향을 주는 다른 경고가 있는지 확인합니다. 이 경고는 다른 경고를 해결할 때 해결될 수 있습니다. 2. 기술 지원 부서에 문의하십시오.
감사 로그가 인메모리 대기열에 추가되고 있습니다	노드가 로컬 syslog 서버로 로그를 전송할 수 없고 인메모리 큐가 가득 찬 경우 1. rsyslog 서비스가 노드에서 실행되고 있는지 확인합니다. 2. 필요한 경우 'service rsyslog restart' 명령을 사용하여 노드에서 rsyslog 서비스를 다시 시작합니다. 3. rsyslog 서비스를 다시 시작할 수 없고 감사 메시지를 관리 노드에 저장하지 않은 경우 기술 지원 부서에 문의하십시오. 이 상태가 수정되지 않으면 감사 로그가 손실됩니다.
Cassandra 자동 콤팩터 메트릭이 최신 상태가 아닙니다	Cassandra 자동 콤팩터를 설명하는 메트릭이 최신 상태가 아닙니다. Cassandra 자동 압축 프로그램은 모든 스토리지 노드에 있으며, 과도한 워크로드를 덮어쓰기 및 삭제할 수 있도록 Cassandra 데이터베이스 크기를 관리합니다. 이 알림이 지속되는 동안 특정 워크로드에서 예기치 않게 높은 메타데이터 소비가 발생합니다. 1. 이 노드에 영향을 주는 다른 경고가 있는지 확인합니다. 이 경고는 다른 경고를 해결할 때 해결될 수 있습니다. 2. 기술 지원 부서에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
Cassandra 통신 오류입니다	Cassandra 서비스를 실행하는 노드는 서로 통신하는 데 문제가 있습니다. 이 알림은 노드 간 통신을 방해하는 것이 있음을 나타냅니다. 네트워크 문제가 있거나 하나 이상의 스토리지 노드에서 Cassandra 서비스가 다운되었을 수 있습니다. 1. 하나 이상의 스토리지 노드에 영향을 주는 다른 경고가 있는지 확인합니다. 이 경고는 다른 경고를 해결할 때 해결될 수 있습니다. 2. 하나 이상의 스토리지 노드에 영향을 줄 수 있는 네트워크 문제를 확인합니다. 3. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 4. 시스템의 각 스토리지 노드에 대해 * SSM * > * Services * 를 선택합니다. Cassandra 서비스의 상태가 "실행 중"인지 확인합니다. 5. Cassandra가 실행되고 있지 않으면 의 단계를 따릅니다 서비스를 시작하거나 다시 시작하는 중입니다. 6. Cassandra 서비스의 모든 인스턴스가 실행되고 있고 경고가 해결되지 않으면 기술 지원 부서에 문의하십시오.
Cassandra 압축 과부하입니다	Cassandra 컴팩션 프로세스가 과부하 상태입니다. 컴팩션 프로세스가 과부하되면 읽기 성능이 저하되고 RAM이 사용될 수 있습니다. Cassandra 서비스가 응답하지 않거나 충돌될 수도 있습니다. 1. 에 대한 단계를 수행하여 Cassandra 서비스를 다시 시작합니다 서비스를 다시 시작하는 중입니다. 2. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.
Cassandra 복구 메트릭이 최신 상태가 아닙니다	Cassandra 복구 작업을 설명하는 메트릭이 최신 상태가 아닙니다. 이 조건이 48시간 이상 지속되는 경우 버킷 리스팅과 같은 클라이언트 쿼리에 삭제된 데이터가 표시될 수 있습니다. 1. 노드를 재부팅합니다. Grid Manager에서 * nodes * 로 이동하여 노드를 선택하고 Tasks 탭을 선택합니다. 2. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
Cassandra 복구 진행률이 느립니다	Cassandra 데이터베이스 복구 진행률이 느립니다. 데이터베이스 복구 속도가 느리면 Cassandra 데이터 일관성 작업이 지연됩니다. 이 조건이 48시간 이상 지속되는 경우 버킷 리스팅과 같은 클라이언트 쿼리에 삭제된 데이터가 표시될 수 있습니다. 1. 모든 스토리지 노드가 온라인 상태이고 네트워킹 관련 경고가 없는지 확인합니다. 2. 이 경고를 최대 2일간 모니터링하여 문제가 자체적으로 해결되는지 확인합니다. 3. 데이터베이스 복구가 계속 느리게 진행될 경우 기술 지원 부서에 문의하십시오.
Cassandra 복구 서비스를 사용할 수 없습니다	Cassandra 복구 서비스를 사용할 수 없습니다. Cassandra 복구 서비스는 모든 스토리지 노드에 있으며 Cassandra 데이터베이스에 대한 중요 복구 기능을 제공합니다. 이 조건이 48시간 이상 지속되는 경우 버킷 리스팅과 같은 클라이언트 쿼리에 삭제된 데이터가 표시될 수 있습니다. 1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 2. 시스템의 각 스토리지 노드에 대해 * SSM * > * Services * 를 선택합니다. Cassandra Refaper 서비스의 상태가 "Running"인지 확인합니다. 3. Cassandra Reaper가 실행되고 있지 않으면 의 단계를 따릅니다 서비스를 시작하거나 다시 시작하는 중입니다. 4. Cassandra Refaper 서비스의 모든 인스턴스가 실행 중이고 경고가 해결되지 않으면 기술 지원 부서에 문의하십시오.
Cassandra 테이블 손상	Cassandra가 테이블 손상을 감지했습니다. 테이블 손상이 감지되면 Cassandra가 자동으로 다시 시작됩니다. 기술 지원 부서에 문의하십시오.
클라우드 스토리지 풀 연결 오류입니다	클라우드 스토리지 풀의 상태 점검에서 하나 이상의 새 오류가 감지되었습니다. 1. 스토리지 풀 페이지의 클라우드 스토리지 풀 섹션으로 이동합니다. 2. 마지막 오류 열을 확인하여 오류가 있는 클라우드 스토리지 풀을 확인합니다. 3. 의 지침을 참조하십시오 정보 수명 주기 관리로 개체 관리.

경고 이름입니다	설명 및 권장 조치
DHCP 리스가 만료되었습니다	네트워크 인터페이스의 DHCP 리스가 만료되었습니다. DHCP 리스가 만료된 경우 권장 조치를 따르십시오. 1. 영향을 받는 인터페이스에서 이 노드와 DHCP 서버 사이에 연결이 있는지 확인합니다. 2. DHCP 서버의 영향을 받는 서브넷에 할당할 수 있는 IP 주소가 있는지 확인합니다. 3. DHCP 서버에 구성된 IP 주소에 대한 영구 예약이 있는지 확인합니다. 또는 StorageGRID IP 변경 도구를 사용하여 DHCP 주소 풀 외부에서 고정 IP 주소를 할당합니다. 를 참조하십시오 복구 및 유지 관리 지침.
DHCP 임대가 곧 만료됩니다	네트워크 인터페이스의 DHCP 임대가 곧 만료됩니다. DHCP 임대가 만료되지 않도록 하려면 권장 조치를 따르십시오. 1. 영향을 받는 인터페이스에서 이 노드와 DHCP 서버 사이에 연결이 있는지 확인합니다. 2. DHCP 서버의 영향을 받는 서브넷에 할당할 수 있는 IP 주소가 있는지 확인합니다. 3. DHCP 서버에 구성된 IP 주소에 대한 영구 예약이 있는지 확인합니다. 또는 StorageGRID IP 변경 도구를 사용하여 DHCP 주소 풀 외부에서 고정 IP 주소를 할당합니다. 를 참조하십시오 복구 및 유지 관리 지침.
DHCP 서버를 사용할 수 없습니다	DHCP 서버를 사용할 수 없습니다. StorageGRID 노드가 DHCP 서버에 연결할 수 없습니다. 노드의 IP 주소에 대한 DHCP 리스를 확인할 수 없습니다. 1. 영향을 받는 인터페이스에서 이 노드와 DHCP 서버 사이에 연결이 있는지 확인합니다. 2. DHCP 서버의 영향을 받는 서브넷에 할당할 수 있는 IP 주소가 있는지 확인합니다. 3. DHCP 서버에 구성된 IP 주소에 대한 영구 예약이 있는지 확인합니다. 또는 StorageGRID IP 변경 도구를 사용하여 DHCP 주소 풀 외부에서 고정 IP 주소를 할당합니다. 를 참조하십시오 복구 및 유지 관리 지침.

경고 이름입니다	설명 및 권장 조치
디스크 I/O가 매우 느립니다	매우 느린 디스크 I/O는 StorageGRID 성능에 영향을 미칠 수 있습니다. 1. 문제가 스토리지 어플라이언스 노드와 관련된 경우 SANtricity System Manager를 사용하여 드라이브 오류, 예상 오류가 있는 드라이브 또는 진행 중인 드라이브 수리를 확인합니다. 또한 어플라이언스 컴퓨팅 및 스토리지 컨트롤러 간의 파이버 채널 또는 SAS 링크 상태를 확인하여 링크가 다운되었는지 또는 과도한 오류 비율을 표시하는지 확인합니다. 2. 이 노드의 볼륨을 호스팅하는 스토리지 시스템을 검사하여 느린 I/O의 근본 원인을 확인하고 수정합니다 3. 이 경고가 지속되면 기술 지원 팀에 문의하십시오. ◦ 참고: * 영향 받는 노드는 서비스를 사용하지 않도록 설정하고 자체적으로 재부팅하여 전체 그리드 성능에 영향을 미치지 않도록 할 수 있습니다. 기본 상태가 해제되고 이러한 노드가 정상적인 I/O 성능을 감지하면 전체 서비스로 자동으로 돌아갑니다.
EC 재조정 실패	스토리지 노드 간에 삭제 코딩 데이터의 균형을 재조정하는 작업이 실패했거나 사용자가 일시 중지했습니다. 1. 재조정되는 사이트의 모든 스토리지 노드가 온라인 상태이고 사용 가능한지 확인합니다. 2. 재조정된 사이트에서 볼륨 장애가 발생하지 않도록 하십시오. 복구 작업을 실행할 수 있도록 EC 재조정 작업이 있는 경우 작업을 종료합니다. "밸런스-데이터 종료—작업 ID<ID>' 3. 재조정되고 있는 사이트에서 서비스 오류가 없는지 확인합니다. 서비스가 실행되고 있지 않으면 복구 및 유지 관리 지침의 서비스 시작 또는 재시작 단계를 따르십시오. 4. 문제를 해결한 후 기본 관리 노드에서 다음 명령을 실행하여 작업을 다시 시작합니다. ``re balance-data start—job-id<ID>' 5. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
EC 복구 실패	삭제 코딩 데이터에 대한 복구 작업이 실패했거나 중지되었습니다. 1. 장애가 발생한 스토리지 노드 또는 볼륨을 대신 사용할 수 있는 스토리지 노드 또는 볼륨이 있는지 확인합니다. 2. 활성 ILM 정책을 충족할 수 있는 충분한 스토리지 노드가 있는지 확인합니다. 3. 네트워크 연결 문제가 없는지 확인합니다. 4. 문제를 해결한 후 기본 관리 노드에서 다음 명령을 실행하여 작업을 다시 시작합니다. ``repair-data start-ec-node-repair—repair-id<ID>' 5. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.
EC 복구가 중단되었습니다	삭제 코딩 데이터에 대한 복구 작업이 중단되었습니다. 1. 장애가 발생한 스토리지 노드 또는 볼륨을 대신 사용할 수 있는 스토리지 노드 또는 볼륨이 있는지 확인합니다. 2. 네트워크 연결 문제가 없는지 확인합니다. 3. 문제를 해결한 후 경고가 해결되었는지 확인합니다. 복구 진행 상황에 대한 자세한 보고서를 보려면 기본 관리 노드에서 다음 명령을 실행합니다. ``repair-data show-ec-repair-status—repair-id<ID>' 4. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
이메일 알림 실패	알림에 대한 이메일 알림을 보낼 수 없습니다. 이 알림은 알림 e-메일 알림이 실패하거나 테스트 e-메일(* alerts*>* Email setup* 페이지에서 보냄)을 전달할 수 없을 때 트리거됩니다. 1. 경고의 * 사이트/노드 * 열에 나열된 관리 노드에서 그리드 관리자에 로그인합니다. 2. 알림 * > * 이메일 설정 * 페이지로 이동하여 설정을 확인하고 필요한 경우 변경하십시오. 3. 테스트 이메일 보내기 * 를 클릭하고 테스트 수신자의 받은 편지함에서 이메일을 확인합니다. 테스트 이메일을 보낼 수 없는 경우 이 경고의 새 인스턴스가 트리거될 수 있습니다. 4. 테스트 이메일을 보낼 수 없는 경우 이메일 서버가 온라인 상태인지 확인합니다. 5. 서버가 작동하는 경우 * 지원 * > * 도구 * > * 로그 * 를 선택하고 관리 노드에 대한 로그를 수집합니다. 경고 시간 15분 전후의 기간을 지정합니다. 6. 다운로드한 아카이브를 추출하고 'Prometheus.log'(_/GID<gid><time_stamp>/<site_node>/<time_stamp>/metrics/Prometheus.log)의 내용을 검토합니다. 7. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.
인증서 페이지에 구성된 클라이언트 인증서 만료	인증서 페이지에 구성된 하나 이상의 클라이언트 인증서가 곧 만료됩니다. 1. 그리드 관리자에서 * 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 클라이언트 * 탭을 선택합니다. 2. 곧 만료될 인증서를 선택합니다. 3. 새 인증서 첨부 * 를 선택합니다 새 인증서를 업로드하거나 생성합니다. 4. 곧 만료되는 각 인증서에 대해 이 단계를 반복합니다.
로드 밸런서 끝점 인증서 만료	하나 이상의 로드 밸런서 끝점 인증서가 곧 만료됩니다. 1. 구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 * 를 선택합니다. 2. 곧 만료될 인증서가 있는 끝점을 선택합니다. 3. 새 인증서를 업로드하거나 생성하려면 * 끝점 편집 * 을 선택합니다. 4. 인증서가 만료되었거나 곧 만료될 각 끝점에 대해 이 단계를 반복합니다. 로드 밸런서 끝점 관리에 대한 자세한 내용은 을 참조하십시오 StorageGRID 관리 지침.

경고 이름입니다	설명 및 권장 조치
관리 인터페이스에 대한 서버 인증서 만료	관리 인터페이스에 사용되는 서버 인증서가 곧 만료됩니다. 1. 구성 * > * 보안 * > * 인증서 * 를 선택합니다. 2. 글로벌 * 탭에서 * 관리 인터페이스 인증서 * 를 선택합니다. 3. 새 관리 인터페이스 인증서를 업로드합니다.
S3 및 Swift API에 대한 글로벌 서버 인증서 만료	스토리지 API 엔드포인트를 액세스하는 데 사용되는 서버 인증서가 곧 만료됩니다. 1. 구성 * > * 보안 * > * 인증서 * 를 선택합니다. 2. 글로벌 * 탭에서 * S3 및 Swift API 인증서 * 를 선택합니다. 3. 새 S3 및 Swift API 인증서를 업로드합니다.
외부 syslog CA 인증서 만료	외부 syslog 서버 인증서에 서명하는 데 사용되는 CA(인증 기관) 인증서가 곧 만료됩니다. 1. 외부 syslog 서버의 CA 인증서를 업데이트합니다. 2. 업데이트된 CA 인증서의 복사본을 가져옵니다. 3. Grid Manager에서 * 구성 * > * 모니터링 * > * 감사 및 syslog 서버 * 로 이동합니다. 4. Edit external syslog server * 를 선택합니다. 5. 새 인증서를 업로드하려면 * 찾아보기 * 를 선택합니다. 6. 구성 마법사를 완료하여 새 인증서와 키를 저장합니다.
외부 syslog 클라이언트 인증서 만료	외부 syslog 서버에 대한 클라이언트 인증서가 곧 만료됩니다. 1. Grid Manager에서 * 구성 * > * 모니터링 * > * 감사 및 syslog 서버 * 로 이동합니다. 2. Edit external syslog server * 를 선택합니다. 3. 새 인증서를 업로드하려면 * 찾아보기 * 를 선택합니다. 4. 새 개인 키를 업로드하려면 * 찾아보기 * 를 선택합니다. 5. 구성 마법사를 완료하여 새 인증서와 키를 저장합니다.
외부 syslog 서버 인증서 만료	외부 syslog 서버가 제공하는 서버 인증서가 곧 만료됩니다. 1. 외부 syslog 서버의 서버 인증서를 업데이트합니다. 2. 이전에 Grid Manager API를 사용하여 인증서 유효성 검사를 위한 서버 인증서를 제공한 경우 API를 사용하여 업데이트된 서버 인증서를 업로드합니다.

경고 이름입니다	설명 및 권장 조치
외부 syslog 서버 전달 오류입니다	노드가 외부 syslog 서버로 로그를 전달할 수 없습니다. 1. Grid Manager에서 * 구성 * > * 모니터링 * > * 감사 및 syslog 서버 * 로 이동합니다. 2. Edit external syslog server * 를 선택합니다. 3. 테스트 메시지 보내기 * 를 선택할 수 있을 때까지 구성 마법사를 진행합니다. 4. 외부 syslog 서버로 로그를 전달할 수 없는 이유를 확인하려면 * 테스트 메시지 전송 * 을 선택합니다. 5. 보고된 모든 문제를 해결합니다.
그리드 네트워크 MTU가 일치하지 않습니다	그리드 네트워크 인터페이스(eth0)에 대한 MTU(Maximum Transmission Unit) 설정은 그리드의 노드 간에 상당히 다릅니다. MTU 설정의 차이는 일부(전기는 아님) eth0 네트워크가 점보 프레임에 맞게 구성되었다는 것을 나타낼 수 있습니다. MTU 크기가 1000보다 크면 네트워크 성능 문제가 발생할 수 있습니다. 에서 Grid Network MTU mismatch 알림에 대한 지침을 참조하십시오 네트워크, 하드웨어 및 플랫폼 문제를 해결합니다.
높은 Java 힙 사용	Java 힙 공간의 높은 비율이 사용되고 있습니다. Java 힙이 가득 차면 메타데이터 서비스를 사용할 수 없게 되고 클라이언트 요청이 실패할 수 있습니다. 1. 대시보드에서 ILM 활동을 검토합니다. ILM 워크로드가 감소하면 이 알림이 단독으로 해결될 수 있습니다. 2. 이 노드에 영향을 주는 다른 경고가 있는지 확인합니다. 이 경고는 다른 경고를 해결할 때 해결될 수 있습니다. 3. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.
메타데이터 쿼리를 위한 높은 지연 시간	Cassandra 메타데이터 쿼리의 평균 시간이 너무 깁니다. 쿼리 대기 시간의 증가는 디스크 교체, 갑작스런 잉조수 증가 등의 워크로드 변경, 노드와 사이트 간 통신 문제 등의 네트워크 변경 등으로 인해 발생할 수 있습니다. 1. 쿼리 대기 시간이 증가하는 시간 동안 하드웨어, 워크로드 또는 네트워크가 변경되었는지 확인합니다. 2. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
ID 페더레이션 동기화 실패	ID 소스에서 페더레이션 그룹과 사용자를 동기화할 수 없습니다. 1. 구성된 LDAP 서버가 온라인 상태이고 사용 가능한지 확인합니다. 2. ID 페더레이션 페이지에서 설정을 검토합니다. 모든 값이 최신인지 확인합니다. 을 참조하십시오 ID 페더레이션을 사용합니다 StorageGRID 관리 지침 3. Test Connection * 을 클릭하여 LDAP 서버 설정을 확인합니다. 4. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.
테넌트의 ID 페더레이션 동기화 실패	테넌트가 구성한 ID 소스에서 페더레이션 그룹과 사용자를 동기화할 수 없습니다. 1. 테넌트 관리자에 로그인합니다. 2. 테넌트가 구성한 LDAP 서버가 온라인 상태이고 사용 가능한지 확인합니다. 3. ID 페더레이션 페이지에서 설정을 검토합니다. 모든 값이 최신인지 확인합니다. 을 참조하십시오 ID 페더레이션을 사용합니다 테넌트 계정 사용 지침 4. Test Connection * 을 클릭하여 LDAP 서버 설정을 확인합니다. 5. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.
ILM 배치를 달성 할 수 없습니다	ILM 규칙의 배치 지침은 특정 개체에 대해 달성할 수 없습니다. 이 알림은 배치 명령에 필요한 노드를 사용할 수 없거나 ILM 규칙이 잘못 구성되었음을 나타냅니다. 예를 들어 규칙이 스토리지 노드보다 더 많은 복제 복사본을 지정할 수 있습니다. 1. 모든 노드가 온라인 상태인지 확인합니다. 2. 모든 노드가 온라인 상태인 경우 활성 ILM 정책을 사용하는 모든 ILM 규칙의 배치 지침을 검토하십시오. 모든 개체에 대한 올바른 지침이 있는지 확인합니다. 를 참조하십시오 정보 수명 주기 관리를 사용하여 개체를 관리하기 위한 지침. 3. 필요에 따라 규칙 설정을 업데이트하고 새 정책을 활성화합니다. ◦ 참고: * 알림이 지워지려면 최대 1일이 걸릴 수 있습니다. 4. 문제가 지속되면 기술 지원 팀에 문의하십시오. ◦ 참고: * 이 알림은 업그레이드 중에 나타날 수 있으며 업그레이드가 성공적으로 완료된 후 1일 동안 지속될 수 있습니다. 업그레이드로 인해 이 알림이 트리거되면 알림이 자체적으로 삭제됩니다.

경고 이름입니다	설명 및 권장 조치
ILM 스캔 기간이 너무 깁니다	ILM을 스캔, 평가 및 적용하는 데 필요한 시간이 너무 깁니다. 모든 개체에 대한 전체 ILM 스캔을 완료하는 데 걸리는 예상 시간이 너무 긴 경우(* 대시보드의 * 스캔 기간 - 예상 * 참조) 활성 ILM 정책이 새로 수집된 개체에 적용되지 않을 수 있습니다. ILM 정책 변경 사항이 기존 개체에 적용되지 않을 수 있습니다. 1. 이 노드에 영향을 주는 다른 경고가 있는지 확인합니다. 이 경고는 다른 경고를 해결할 때 해결될 수 있습니다. 2. 모든 스토리지 노드가 온라인 상태인지 확인합니다. 3. 클라이언트 트래픽의 양을 일시적으로 줄입니다. 예를 들어 그리드 관리자에서 * 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택하고 대역폭 또는 요청 수를 제한하는 정책을 만듭니다. 4. 디스크 I/O 또는 CPU가 과부하 상태인 경우 로드를 줄이거나 리소스를 늘리십시오. 5. 필요한 경우 ILM 규칙을 업데이트하여 동기 배치(StorageGRID 11.3 이후에 생성된 규칙의 기본값)를 사용합니다. 6. 이 경고가 지속되면 기술 지원 팀에 문의하십시오. StorageGRID 관리
ILM 스캔 속도가 낮습니다	ILM 스캔 속도는 초당 100개 미만으로 설정됩니다. 이 알림은 시스템의 ILM 스캔 속도를 초당 100개 미만으로 변경했음을 나타냅니다(기본값: 400개 개체/초). 활성 ILM 정책이 새로 수집된 개체에 적용되지 않을 수 있습니다. ILM 정책에 대한 이후의 변경 사항은 기존 개체에 적용되지 않습니다. 1. 지속적인 지원 조사의 일환으로 ILM 스캔 속도가 일시적으로 변경되었는지 확인합니다. 2. 기술 지원 부서에 문의하십시오. ⓘ 기술 지원 부서에 문의하지 않고 ILM 스캔 속도를 변경하지 마십시오.

경고 이름입니다	설명 및 권장 조치
KMS CA 인증서 만료	KMS(키 관리 서버) 인증서에 서명하는 데 사용되는 CA(인증 기관) 인증서가 곧 만료됩니다. 1. KMS 소프트웨어를 사용하여 키 관리 서버에 대한 CA 인증서를 업데이트합니다. 2. Grid Manager에서 * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다. 3. 인증서 상태 경고가 있는 KMS를 선택합니다. 4. 편집 * 을 선택합니다. 5. 2단계(서버 인증서 업로드)로 이동하려면 * 다음 * 을 선택합니다. 6. 새 인증서를 업로드하려면 * 찾아보기 * 를 선택합니다. 7. 저장 * 을 선택합니다. StorageGRID 관리
KMS 클라이언트 인증서 만료	키 관리 서버의 클라이언트 인증서가 곧 만료됩니다. 1. Grid Manager에서 * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다. 2. 인증서 상태 경고가 있는 KMS를 선택합니다. 3. 편집 * 을 선택합니다. 4. 다음 * 을 선택하여 3단계(클라이언트 인증서 업로드)로 이동합니다. 5. 새 인증서를 업로드하려면 * 찾아보기 * 를 선택합니다. 6. 새 개인 키를 업로드하려면 * 찾아보기 * 를 선택합니다. 7. 저장 * 을 선택합니다. StorageGRID 관리
KMS 구성을 로드하지 못했습니다	키 관리 서버에 대한 구성이 있지만 로드하지 못했습니다. 1. 이 노드에 영향을 주는 다른 경고가 있는지 확인합니다. 이 경고는 다른 경고를 해결할 때 해결될 수 있습니다. 2. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
KMS 연결 오류입니다	어플라이언스 노드가 사이트의 키 관리 서버에 연결할 수 없습니다. 1. Grid Manager에서 * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다. 2. 포트 및 호스트 이름 항목이 올바른지 확인합니다. 3. 서버 인증서, 클라이언트 인증서 및 클라이언트 인증서 개인 키가 올바르고 만료되지 않았는지 확인합니다. 4. 어플라이언스 노드가 지정된 KMS와 통신할 수 있도록 방화벽 설정이 허용되는지 확인합니다. 5. 네트워킹 또는 DNS 문제를 모두 해결합니다. 6. 도움이 필요하거나 이 경고가 계속 표시되면 기술 지원 팀에 문의하십시오.
KMS 암호화 키 이름을 찾을 수 없습니다	구성된 키 관리 서버에 제공된 이름과 일치하는 암호화 키가 없습니다. 1. 사이트에 할당된 KMS가 암호화 키 및 이전 버전에 대해 올바른 이름을 사용하고 있는지 확인합니다. 2. 도움이 필요하거나 이 경고가 계속 표시되면 기술 지원 팀에 문의하십시오.
KMS 암호화 키 회전이 실패했습니다	모든 어플라이언스 볼륨이 해독되었지만 하나 이상의 볼륨이 최신 키로 회전할 수 없습니다. 기술 지원 부서에 문의하십시오.
KMS가 구성되지 않았습니다	이 사이트에 대한 키 관리 서버가 없습니다. 1. Grid Manager에서 * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다. 2. 이 사이트에 대해 KMS를 추가하거나 기본 KMS를 추가합니다. StorageGRID 관리
킬로미터 키가 어플라이언스 볼륨을 해독하지 못했습니다	노드 암호화가 활성화된 어플라이언스에서 하나 이상의 볼륨을 현재 KMS 키로 해독할 수 없습니다. 1. 이 노드에 영향을 주는 다른 경고가 있는지 확인합니다. 이 경고는 다른 경고를 해결할 때 해결될 수 있습니다. 2. KMS(키 관리 서버)에 암호화 키 및 이전 키 버전이 구성되어 있는지 확인합니다. 3. 도움이 필요하거나 이 경고가 계속 표시되면 기술 지원 팀에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
KMS 서버 인증서 만료	KMS(키 관리 서버)에서 사용하는 서버 인증서가 곧 만료됩니다. 1. KMS 소프트웨어를 사용하여 키 관리 서버에 대한 서버 인증서를 업데이트합니다. 2. 도움이 필요하거나 이 경고가 계속 표시되면 기술 지원 팀에 문의하십시오. StorageGRID 관리
대규모 감사 대기열	감사 메시지의 디스크 대기열이 가득 찼습니다. 1. 시스템의 로드 점검 — 트랜잭션 수가 상당히 많은 경우 시간이 지남에 따라 경고가 자동으로 해결되고 경고를 무시할 수 있습니다. 2. 경고가 지속되고 심각도가 증가하면 대기열 크기의 차트를 참조하십시오. 시간이 경과하거나 며칠 동안 꾸준히 증가하는 경우 감사 로드가 시스템의 감사 용량을 초과할 가능성이 높습니다. 3. 클라이언트 쓰기 및 클라이언트 읽기에 대한 감사 수준을 오류 또는 끄기로 변경하여 클라이언트 작업 속도를 줄이거나 기록된 감사 메시지 수를 줄이십시오(* 구성 * > * 모니터링 * > * 감사 및 syslog 서버 *). 감사 로그를 검토합니다
레거시 CLB 로드 밸런서 활동이 감지되었습니다	일부 클라이언트는 기본 S3 및 Swift API 인증서를 사용하여 더 이상 사용되지 않는 CLB 로드 밸런서 서비스에 연결할 수 있습니다. 1. 향후 업그레이드를 간소화하려면 * 인증서 * 페이지의 * 글로벌 * 탭에 사용자 정의 S3 및 Swift API 인증서를 설치하십시오. 그런 다음 레거시 CLB에 연결하는 모든 S3 또는 Swift 클라이언트에 새 인증서가 있는지 확인합니다. 2. 하나 이상의 로드 밸런서 끝점을 만듭니다. 그런 다음 기존의 모든 S3 및 Swift 클라이언트를 이러한 엔드포인트로 연결합니다. 클라이언트 포트를 다시 매핑해야 하는 경우 기술 지원 부서에 문의하십시오. 포트 스캔을 비롯한 다른 작업으로 인해 이 경고가 발생할 수 있습니다. 더 이상 사용되지 않는 CLB 서비스가 현재 사용 중인지 확인하려면 'toragegrid_private_clb_http_connection_설정됨_successful' Prometheus 메트릭을 참조하십시오. CLB 서비스를 더 이상 사용하지 않는 경우 필요에 따라 이 경고 규칙을 해제하거나 비활성화하십시오.

경고 이름입니다	설명 및 권장 조치
로그가 디스크 대기열에 추가되고 있습니다	노드가 외부 syslog 서버로 로그를 전달할 수 없고 디스크 내 대기열이 가득 찬 경우 1. Grid Manager에서 * 구성 * > * 모니터링 * > * 감사 및 syslog 서버 * 로 이동합니다. 2. Edit external syslog server * 를 선택합니다. 3. 테스트 메시지 보내기 * 를 선택할 수 있을 때까지 구성 마법사를 진행합니다. 4. 외부 syslog 서버로 로그를 전달할 수 없는 이유를 확인하려면 * 테스트 메시지 전송 * 을 선택합니다. 5. 보고된 모든 문제를 해결합니다.
감사 로그 디스크 용량이 낮습니다	감사 로그에 사용할 수 있는 공간이 부족합니다. 1. 이 경고를 모니터링하여 문제가 자체적으로 해결되고 디스크 공간을 다시 사용할 수 있는지 확인합니다. 2. 사용 가능한 공간이 계속 줄어지면 기술 지원 부서에 문의하십시오.
사용 가능한 노드 메모리가 부족합니다	노드에서 사용할 수 있는 RAM 용량이 부족합니다. 사용 가능한 RAM이 낮으면 작업 부하가 변경되거나 하나 이상의 노드에서 메모리 누수가 발생한 것일 수 있습니다. 1. 이 경고를 모니터링하여 문제가 자체적으로 해결되는지 확인합니다. 2. 사용 가능한 메모리가 주요 경고 임계값 아래로 떨어지면 기술 지원 부서에 문의하십시오.
스토리지 풀의 사용 가능한 공간이 부족합니다	스토리지 풀에 오브젝트 데이터를 저장하는 데 사용할 수 있는 공간이 부족합니다. 1. ILM * > * 스토리지 풀 * 을 선택합니다. 2. 알림에 나열된 스토리지 풀을 선택하고 * View details * 를 선택합니다. 3. 추가 스토리지 용량이 필요한 위치를 확인합니다. 스토리지 풀의 각 사이트에 스토리지 노드를 추가하거나 하나 이상의 기존 스토리지 노드에 스토리지 볼륨(LUN)을 추가할 수 있습니다. 4. 스토리지 용량을 늘리려면 확장 절차를 수행하십시오. 그리드를 확장합니다

경고 이름입니다	설명 및 권장 조치
설치된 노드 메모리가 부족합니다	노드에 설치된 메모리 양이 부족합니다. 가상 머신 또는 Linux 호스트에서 사용할 수 있는 RAM의 양을 늘립니다. StorageGRID 노드의 기본 최소 요구 사항을 확인하려면 주 경고의 임계값을 확인합니다. 플랫폼에 대한 설치 지침을 참조하십시오. • Red Hat Enterprise Linux 또는 CentOS를 설치합니다 • Ubuntu 또는 Debian을 설치합니다 • VMware를 설치합니다

낮은 메타데이터 스토리지	오브젝트 메타데이터를 저장하는 데 사용할 수 있는 공간이 부족합니다.
	
	• 긴급 경보 *
	  1. 개체 인제스트를 중지합니다.
	  2. 확장 절차에서 스토리지 노드를 즉시 추가합니다.
	• 주요 경고 *
	
	확장 절차에서 스토리지 노드를 즉시 추가합니다.
	
	• 보조 알림 *
	  1. 오브젝트 메타데이터 공간이 사용되는 속도를 모니터링합니다. nodes * > **Storage Node* * > * Storage * 를 선택하고 Storage Used - Object Metadata 그래프를 봅니다.
	  2. 에 스토리지 노드를 추가합니다 확장 절차 빨리.
	
	새 스토리지 노드가 추가되면 시스템이 모든 스토리지 노드에서 개체 메타데이터를 자동으로 재조정하며 경보가 지워집니다.
	
	에서 메타데이터 저장 부족 경고에 대한 지침을 참조하십시오 메타데이터 문제를 해결합니다.

낮은 메트릭 디스크 용량	메트릭 데이터베이스에 사용할 수 있는 공간이 부족합니다. 1. 이 경고를 모니터링하여 문제가 자체적으로 해결되고 디스크 공간을 다시 사용할 수 있는지 확인합니다. 2. 사용 가능한 공간이 계속 줄어지면 기술 지원 부서에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
오브젝트 데이터 스토리지가 부족합니다	오브젝트 데이터를 저장하는 데 사용할 수 있는 공간이 부족합니다. 확장 절차를 수행합니다. 기존 스토리지 노드에 스토리지 볼륨(LUN)을 추가하거나 새 스토리지 노드를 추가할 수 있습니다. 오브젝트 부족 데이터 스토리지 경고 문제를 해결합니다 그리드를 확장합니다
읽기 전용 로우 워터마크가 무시됩니다	스토리지 볼륨 소프트 읽기 전용 워터마크 재정의는 스토리지 노드에 대해 최적화된 최소 워터마크보다 작습니다. 이 경고를 해결하는 방법을 알아보려면 로 이동하십시오 낮은 읽기 전용 배경무늬 재정의 알림 문제 해결.
루트 디스크 용량이 부족합니다	루트 디스크에 사용할 수 있는 공간이 부족합니다. 1. 이 경고를 모니터링하여 문제가 자체적으로 해결되고 디스크 공간을 다시 사용할 수 있는지 확인합니다. 2. 사용 가능한 공간이 계속 줄어지면 기술 지원 부서에 문의하십시오.
시스템 데이터 용량이 부족합니다	'/var/local' 파일 시스템에서 StorageGRID 시스템 데이터에 사용할 수 있는 공간이 부족합니다. 1. 이 경고를 모니터링하여 문제가 자체적으로 해결되고 디스크 공간을 다시 사용할 수 있는지 확인합니다. 2. 사용 가능한 공간이 계속 줄어지면 기술 지원 부서에 문의하십시오.
tmp 디렉토리 여유 공간이 부족합니다	/tmp 디렉토리에 사용 가능한 공간이 부족합니다. 1. 이 경고를 모니터링하여 문제가 자체적으로 해결되고 디스크 공간을 다시 사용할 수 있는지 확인합니다. 2. 사용 가능한 공간이 계속 줄어지면 기술 지원 부서에 문의하십시오.
노드 네트워크 연결 오류입니다	노드 간에 데이터를 전송하는 동안 오류가 발생했습니다. 네트워크 연결 오류는 수동 개입 없이 해결할 수 있습니다. 오류가 해결되지 않으면 기술 지원 부서에 문의하십시오. 에서 NRER(Network Receive Error) 경보에 대한 지침을 참조하십시오 네트워크, 하드웨어 및 플랫폼 문제를 해결합니다.

경고 이름입니다	설명 및 권장 조치
노드 네트워크 수신 프레임 오류입니다	노드에서 수신한 네트워크 프레임의 비율이 높은 경우 오류가 발생했습니다. 이 알림은 이더넷 연결 양쪽 끝에서 케이블 불량 또는 트랜시버 오류 등의 하드웨어 문제를 나타낼 수 있습니다. 1. 어플라이언스를 사용하는 경우 각 SFP+ 또는 SFP28 트랜시버 및 케이블을 한 번에 하나씩 교체하여 경고가 사라지는지 확인하십시오. 2. 이 경고가 지속되면 기술 지원 팀에 문의하십시오.
노드가 NTP 서버와 동기화되지 않았습니다	노드 시간이 NTP(네트워크 시간 프로토콜) 서버와 동기화되지 않습니다. 1. Stratum 3 이상의 참조를 제공하는 외부 NTP 서버를 4개 이상 지정했는지 확인합니다. 2. 모든 NTP 서버가 정상적으로 작동하는지 확인합니다. 3. NTP 서버에 대한 연결을 확인합니다. 방화벽에 의해 차단되지 않았는지 확인합니다.
NTP 서버로 잠겨 있지 않은 노드입니다	노드가 네트워크 시간 프로토콜(NTP) 서버에 잠기지 않았습니다. 1. Stratum 3 이상의 참조를 제공하는 외부 NTP 서버를 4개 이상 지정했는지 확인합니다. 2. 모든 NTP 서버가 정상적으로 작동하는지 확인합니다. 3. NTP 서버에 대한 연결을 확인합니다. 방화벽에 의해 차단되지 않았는지 확인합니다.
비어플라이언스 노드 네트워크가 다운되었습니다	하나 이상의 네트워크 장치가 다운되었거나 연결이 끊어졌습니다. 이 알림은 가상 머신 또는 Linux 호스트에 설치된 노드의 네트워크 인터페이스(eth)에 액세스할 수 없음을 나타냅니다. 기술 지원 부서에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
개체 존재 여부를 확인하지 못했습니다	개체 존재 확인 작업이 실패했습니다. 1. 유지보수 > 개체 존재 확인 * 을 선택합니다. 2. 오류 메시지를 확인합니다. 적절한 수정 조치를 수행합니다. ◦ 시작 실패 *, * 연결 끊김 *, * 알 수 없는 오류 * a. 작업에 포함된 스토리지 노드 및 볼륨이 온라인 상태이고 사용 가능한지 확인합니다. b. 스토리지 노드에 서비스 또는 볼륨 장애가 없는지 확인합니다. 서비스가 실행되고 있지 않으면 서비스를 시작하거나 다시 시작합니다. 를 참조하십시오 복구 및 유지 관리 지침. c. 선택한 일관성 제어가 충족될 수 있는지 확인합니다. d. 문제를 해결한 후 * Retry *(재시도 *)를 선택합니다. 마지막 유효한 상태에서 작업이 재개됩니다. ◦ 볼륨의 중요한 스토리지 오류 * a. 장애가 발생한 볼륨을 복구합니다. 를 참조하십시오 복구 및 유지 관리 지침. b. 재시도 * 를 선택합니다. c. 작업이 완료된 후 노드의 나머지 볼륨에 대해 다른 작업을 생성하여 추가 오류를 확인합니다. 3. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.
개체 존재 검사가 중단되었습니다	개체 존재 확인 작업이 중단되었습니다. 개체 존재 확인 작업을 계속할 수 없습니다. 작업에 포함된 하나 이상의 스토리지 노드 또는 볼륨이 오프라인 상태이거나 응답하지 않거나, 너무 많은 노드가 다운되었거나 사용할 수 없기 때문에 선택한 정합성 제어를 더 이상 충족할 수 없습니다. 1. 확인 중인 모든 스토리지 노드 및 볼륨이 온라인 상태이고 사용 가능한지 확인합니다(* 노드 * 선택). 2. 현재 코디네이터 노드가 선택한 정합성 제어를 사용하여 객체 메타데이터를 읽을 수 있도록 충분한 스토리지 노드가 온라인 상태이고 사용 가능한지 확인합니다. 필요한 경우 서비스를 시작하거나 다시 시작합니다. 를 참조하십시오 복구 및 유지 관리 지침. 1단계와 2단계를 해결하면 작업이 꺼진 위치에서 자동으로 시작됩니다. 3. 선택한 정합성 보장 제어가 충족되지 않으면 작업을 취소하고 더 낮은 정합성 제어를 사용하여 다른 작업을 시작합니다. 4. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
객체가 손실되었습니다	그리드에서 하나 이상의 오브젝트가 손실되었습니다. 이 알림은 데이터가 영구적으로 손실되었으며 검색할 수 없음을 나타낼 수 있습니다. 1. 이 경고를 즉시 조사하십시오. 추가 데이터 손실을 방지하기 위해 조치를 취해야 할 수 있습니다. 프롬프트 작업을 수행하는 경우 손실된 개체를 복원할 수도 있습니다. 분실하거나 누락된 오브젝트 데이터 문제를 해결합니다 2. 기본 문제가 해결되면 카운터를 재설정합니다. a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. b. 경고를 발생시킨 스토리지 노드의 경우 **site* * > **GRID node* * > * LDR * > * Data Store * > * Configuration * > * Main * 을 선택합니다. c. 손실된 개체 수 재설정 * 을 선택하고 * 변경 내용 적용 * 을 클릭합니다.
플랫폼 서비스를 사용할 수 없습니다	RSM 서비스가 실행 중이거나 사이트에서 사용 가능한 스토리지 노드가 너무 적습니다. 영향을 받는 사이트에서 RSM 서비스가 있는 스토리지 노드 중 대부분이 실행 중이고 오류가 없는 상태인지 확인합니다. 의 "플랫폼 서비스 문제 해결"을 참조하십시오 StorageGRID 관리 지침.
S3 PUT 오브젝트 크기가 너무 큽니다	S3 클라이언트가 S3 크기 제한을 초과하는 Put Object 작업을 수행하려고 합니다. 1. 알림 세부 정보에 표시된 테넌트 ID를 사용하여 테넌트 계정을 식별합니다. 2. 지원 * > * 도구 * > * 로그 * 로 이동하여 경고 세부 정보에 표시된 스토리지 노드에 대한 애플리케이션 로그를 수집합니다. 경고 시간 15분 전후의 기간을 지정합니다. 3. 다운로드한 아카이브를 추출하고 'bycast.log'('/GID <grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log')의 위치로 이동합니다. 4. bycast.log의 내용을 검색하여 method=put을 찾은 다음 clientIP 필드를 보고 S3 클라이언트의 IP 주소를 확인합니다. 5. 모든 클라이언트 사용자에게 최대 Put Object 크기가 5GiB임을 알립니다. 6. 5GiB보다 큰 개체에 대해 멀티파트 업로드를 사용합니다.

경고 이름입니다	설명 및 권장 조치
관리 네트워크 포트 1에서 서비스 어플라이언스 링크가 다운되었습니다	어플라이언스의 관리 네트워크 포트 1이 다운되었거나 연결이 해제되었습니다. 1. 관리 네트워크 포트 1에 대한 케이블 및 물리적 연결을 확인합니다. 2. 모든 연결 문제를 해결합니다. 어플라이언스 하드웨어의 설치 및 유지 관리 지침을 참조하십시오. 3. 이 포트가 의도적으로 연결이 끊어진 경우 이 규칙을 비활성화하십시오. Grid Manager에서 * alerts * > * rules * 를 선택하고 규칙을 선택한 다음 * Edit rule * 을 클릭합니다. 그런 다음 * 사용 * 확인란의 선택을 취소합니다. ◦ SG100 및 SG1000 서비스 어플라이언스 ◦ 경고 규칙을 비활성화합니다
관리 네트워크(또는 클라이언트 네트워크)에서 서비스 어플라이언스 링크가 다운되었습니다.	관리 네트워크(eth1) 또는 클라이언트 네트워크(eth2)에 대한 어플라이언스 인터페이스가 다운되거나 연결이 끊겼습니다. 1. StorageGRID 네트워크에 대한 케이블, SFP 및 물리적 연결을 확인합니다. 2. 모든 연결 문제를 해결합니다. 어플라이언스 하드웨어의 설치 및 유지 관리 지침을 참조하십시오. 3. 이 포트가 의도적으로 연결이 끊어진 경우 이 규칙을 비활성화하십시오. Grid Manager에서 * alerts * > * rules * 를 선택하고 규칙을 선택한 다음 * Edit rule * 을 클릭합니다. 그런 다음 * 사용 * 확인란의 선택을 취소합니다. ◦ SG100 및 SG1000 서비스 어플라이언스 ◦ 경고 규칙을 비활성화합니다
네트워크 포트 1, 2, 3 또는 4에서 서비스 어플라이언스 링크가 다운되었습니다	어플라이언스의 네트워크 포트 1, 2, 3 또는 4가 다운되었거나 연결이 해제되었습니다. 1. StorageGRID 네트워크에 대한 케이블, SFP 및 물리적 연결을 확인합니다. 2. 모든 연결 문제를 해결합니다. 어플라이언스 하드웨어의 설치 및 유지 관리 지침을 참조하십시오. 3. 이 포트가 의도적으로 연결이 끊어진 경우 이 규칙을 비활성화하십시오. Grid Manager에서 * alerts * > * rules * 를 선택하고 규칙을 선택한 다음 * Edit rule * 을 클릭합니다. 그런 다음 * 사용 * 확인란의 선택을 취소합니다. ◦ SG100 및 SG1000 서비스 어플라이언스 ◦ 경고 규칙을 비활성화합니다

경고 이름입니다	설명 및 권장 조치
서비스 어플라이언스의 스토리지 연결이 저하되었습니다	서비스 어플라이언스의 두 SSD 중 하나에 장애가 발생했거나 다른 SSD와 동기화되지 않았습니다. 어플라이언스 기능은 영향을 받지 않지만 문제를 즉시 해결해야 합니다. 두 드라이브 모두에 장애가 발생할 경우 어플라이언스가 더 이상 작동하지 않습니다. 1. Grid Manager에서 * nodes * > ***_services appliance_**를 선택한 다음 Hardware * 탭을 선택합니다. 2. Storage RAID Mode * 필드에서 메시지를 검토합니다. 3. 메시지에 재동기화 작업의 진행률이 표시되면 작업이 완료될 때까지 기다린 다음 알림이 해결되었는지 확인합니다. 재동기화 메시지는 SSD가 최근에 교체되었거나 다른 이유로 재동기화 중임을 의미합니다. 4. SSD 중 하나에 오류가 발생했음을 나타내는 메시지가 표시되면 가능한 한 빨리 장애가 발생한 드라이브를 교체합니다. 서비스 어플라이언스에서 드라이브를 교체하는 방법에 대한 지침은 SG100 및 SG1000 어플라이언스 설치 및 유지 관리 가이드를 참조하십시오. SG100 및 SG1000 서비스 어플라이언스
관리 네트워크 포트 1에서 스토리지 어플라이언스 링크가 다운되었습니다	어플라이언스의 관리 네트워크 포트 1이 다운되었거나 연결이 해제되었습니다. 1. 관리 네트워크 포트 1에 대한 케이블 및 물리적 연결을 확인합니다. 2. 모든 연결 문제를 해결합니다. 어플라이언스 하드웨어의 설치 및 유지 관리 지침을 참조하십시오. 3. 이 포트가 의도적으로 연결이 끊어진 경우 이 규칙을 비활성화하십시오. Grid Manager에서 * alerts * > * rules * 를 선택하고 규칙을 선택한 다음 * Edit rule * 을 클릭합니다. 그런 다음 * 사용 * 확인란의 선택을 취소합니다. ◦ SG6000 스토리지 어플라이언스 ◦ SG5700 스토리지 어플라이언스 ◦ SG5600 스토리지 어플라이언스 ◦ 경고 규칙을 비활성화합니다

경고 이름입니다	설명 및 권장 조치
관리 네트워크(또는 클라이언트 네트워크)에서 스토리지 어플라이언스 링크가 다운되었습니다.	관리 네트워크(eth1) 또는 클라이언트 네트워크(eth2)에 대한 어플라이언스 인터페이스가 다운되거나 연결이 끊겼습니다. 1. StorageGRID 네트워크에 대한 케이블, SFP 및 물리적 연결을 확인합니다. 2. 모든 연결 문제를 해결합니다. 어플라이언스 하드웨어의 설치 및 유지 관리 지침을 참조하십시오. 3. 이 포트가 의도적으로 연결이 끊어진 경우 이 규칙을 비활성화하십시오. Grid Manager에서 * alerts * > * rules * 를 선택하고 규칙을 선택한 다음 * Edit rule * 을 클릭합니다. 그런 다음 * 사용 * 확인란의 선택을 취소합니다. ◦ SG6000 스토리지 어플라이언스 ◦ SG5700 스토리지 어플라이언스 ◦ SG5600 스토리지 어플라이언스 ◦ 경고 규칙을 비활성화합니다
네트워크 포트 1, 2, 3 또는 4에서 스토리지 어플라이언스 링크가 다운되었습니다	어플라이언스의 네트워크 포트 1, 2, 3 또는 4가 다운되었거나 연결이 해제되었습니다. 1. StorageGRID 네트워크에 대한 케이블, SFP 및 물리적 연결을 확인합니다. 2. 모든 연결 문제를 해결합니다. 어플라이언스 하드웨어의 설치 및 유지 관리 지침을 참조하십시오. 3. 이 포트가 의도적으로 연결이 끊어진 경우 이 규칙을 비활성화하십시오. Grid Manager에서 * alerts * > * rules * 를 선택하고 규칙을 선택한 다음 * Edit rule * 을 클릭합니다. 그런 다음 * 사용 * 확인란의 선택을 취소합니다. ◦ SG6000 스토리지 어플라이언스 ◦ SG5700 스토리지 어플라이언스 ◦ SG5600 스토리지 어플라이언스 ◦ 경고 규칙을 비활성화합니다

경고 이름입니다	설명 및 권장 조치
스토리지 어플라이언스 스토리지 연결이 저하되었습니다	컴퓨팅 컨트롤러와 스토리지 컨트롤러 사이에 하나 이상의 연결에 문제가 있습니다. 1. 포트 표시등을 확인하려면 제품으로 이동하십시오. 2. 포트의 표시등이 꺼져 있는 경우 케이블이 제대로 연결되어 있는지 확인합니다. 필요한 경우 케이블을 교체합니다. 3. 최대 5분 동안 기다립니다. ◦ 참고: * 두 번째 케이블을 교체해야 하는 경우 최소 5분 동안 케이블을 분리하지 마십시오. 그렇지 않으면 루트 볼륨이 읽기 전용이 되어 하드웨어를 다시 시작해야 할 수 있습니다. 4. Grid Manager에서 * nodes * 를 선택합니다. 그런 다음 문제가 있는 노드의 Hardware 탭을 선택합니다. 경고 상태가 해결되었는지 확인합니다.

스토리지 디바이스를 액세스할 수 없습니다	스토리지 디바이스를 액세스할 수 없습니다.
	
	이 알림은 기본 스토리지 디바이스의 문제로 인해 볼륨을 마운트하거나 액세스할 수 없음을 나타냅니다.
	
	1. 노드에 사용된 모든 스토리지 디바이스의 상태를 확인합니다.
	  ◦ 노드가 가상 머신 또는 Linux 호스트에 설치된 경우 운영 체제의 지침에 따라 하드웨어 진단을 실행하거나 파일 시스템 검사를 수행합니다.
	  ▪ Red Hat Enterprise Linux 또는 CentOS를 설치합니다
	  ▪ Ubuntu 또는 Debian을 설치합니다
	  ▪ VMware를 설치합니다
	  ◦ SG100, SG1000 또는 SG6000 어플라이언스에 노드가 설치된 경우 BMC를 사용하십시오.
	  ◦ 노드가 SG5600 또는 SG5700 어플라이언스에 설치된 경우 SANtricity 시스템 관리자를 사용하십시오.
	2. 필요한 경우 구성 요소를 교체합니다. 사용 중인 제품의 지침을 참조하십시오.
	  ◦ SG6000 스토리지 어플라이언스
	  ◦ SG5700 스토리지 어플라이언스
	  ◦ SG5600 스토리지 어플라이언스

경고 이름입니다	설명 및 권장 조치

테넌트 할당량 사용량이 높습니다	테넌트 할당량 공간의 높은 비율이 사용되고 있습니다. 테넌트가 할당량을 초과하면 새 베스트 일스트가 거부됩니다.
	
	• 참고: * 이 경고 규칙은 많은 알림을 생성할 수 있으므로 기본적으로 비활성화되어 있습니다.
	  1. Grid Manager에서 * Tenants * 를 선택합니다.
	  2. 할당량 사용량 * 을 기준으로 테이블을 정렬합니다.
	  3. 할당량 활용률이 100%에 가까운 테넌트를 선택합니다.
	  4. 다음 중 하나 또는 모두를 수행합니다.
	  ▪ 테넌트에 대한 저장소 할당량을 늘리려면 * 편집 * 을 선택합니다.
	  ▪ 할당량의 활용도가 높다고 테넌트에 알립니다.

노드와 통신할 수 없습니다	하나 이상의 서비스가 응답하지 않거나 노드에 연결할 수 없습니다. 이 알림은 알 수 없는 이유로 노드의 연결이 끊겼음을 나타냅니다. 예를 들어, 노드의 서비스가 중지되거나 전원 장애 또는 예기치 않은 정전으로 인해 노드의 네트워크 연결이 끊겼을 수 있습니다. 이 경고를 모니터링하여 문제가 자체적으로 해결되는지 확인합니다. 문제가 지속되는 경우: 1. 이 노드에 영향을 주는 다른 경고가 있는지 확인합니다. 이 경고는 다른 경고를 해결할 때 해결될 수 있습니다. 2. 이 노드의 모든 서비스가 실행 중인지 확인합니다. 서비스가 중지된 경우 서비스를 시작해 보십시오. 를 참조하십시오 복구 및 유지 관리 지침. 3. 노드의 호스트 전원이 켜져 있는지 확인합니다. 그렇지 않으면 호스트를 시작합니다. ◦ 참고: * 둘 이상의 호스트가 꺼져 있는 경우 를 참조하십시오 복구 및 유지 관리 지침. 4. 이 노드와 관리자 노드 사이에 네트워크 연결 문제가 있는지 확인합니다. 5. 경고를 해결할 수 없는 경우 기술 지원 팀에 문의하십시오.
예기치 않은 노드 재부팅	지난 24시간 동안 노드가 예기치 않게 재부팅되었습니다. 1. 이 경고를 모니터링합니다. 24시간이 지나면 경고가 지워집니다. 그러나 노드가 다시 예기치 않게 재부팅되면 이 경고가 다시 발생합니다. 2. 경고를 해결할 수 없는 경우 하드웨어 오류가 발생할 수 있습니다. 기술 지원 부서에 문의하십시오.

경고 이름입니다	설명 및 권장 조치
알 수 없는 손상된 개체가 감지되었습니다	복제된 오브젝트로 식별되지 않는 파일이 복제된 오브젝트 스토리지에 있습니다. 1. 스토리지 노드의 기본 스토리지에 문제가 있는지 확인합니다. 예를 들어, 하드웨어 진단을 실행하거나 파일 시스템 검사를 수행합니다. 2. 스토리지 문제를 해결한 후 개체 존재 확인 실행 ILM 정책에 정의된 복제된 복사본이 없는지 확인합니다. 3. 이 경고를 모니터링합니다. 이 알림은 24시간 후에 해결되지만 문제가 해결되지 않으면 다시 트리거됩니다. 4. 경고를 해결할 수 없는 경우 기술 지원 팀에 문의하십시오.

일반적으로 사용되는 **Prometheus** 메트릭입니다

관리 노드의 Prometheus 서비스는 모든 노드의 서비스에서 시계열 메트릭을 수집합니다. Prometheus는 1,000개 이상의 메트릭을 수집하지만 가장 중요한 StorageGRID 작업을 모니터링하려면 상대적으로 적은 수의 수치가 필요합니다.

메트릭은 Prometheus 데이터에 예약된 공간이 가득 찰 때까지 각 관리 노드에 저장됩니다. '/var/local/mysql_ibdata/' 볼륨이 용량에 도달하면 가장 오래된 메트릭이 먼저 삭제됩니다.

전체 메트릭 목록을 얻으려면 Grid Management API를 사용하십시오.

1. Grid Manager 상단에서 도움말 아이콘을 선택하고 * API Documentation * 을 선택합니다.
2. 메트릭 * 작업을 찾습니다.
3. Get/Grid/metric-names 동작을 수행한다.
4. 결과를 다운로드합니다.

다음 표에는 가장 일반적으로 사용되는 Prometheus 메트릭이 나열되어 있습니다. 이 목록을 참조하여 기본 알림 규칙의 조건을 보다 잘 이해하거나 사용자 지정 알림 규칙의 조건을 구성할 수 있습니다.

> 이름에 _private_이 포함된 메트릭은 내부 전용이며 StorageGRID 릴리스 간에 예고 없이 변경될 수 있습니다.

Prometheus 메트릭입니다	설명
alertmanager_notifications_failed_total	실패한 총 경고 알림 수입니다.
node_filesystem_AVAIL_bytes를 나타냅니다	루트가 아닌 사용자가 사용할 수 있는 파일 시스템 공간의 크기(바이트)입니다.
node_memory_MemAvailable_bytes입니다	메모리 정보 필드 MemAvailable_Bytes
node_network_carrier 를 선택합니다	/sys/class/net/<iface>의 캐리어 값입니다.

Prometheus 메트릭입니다	설명
node_network_Receive_errs_total	네트워크 장치 통계 Receive_errs입니다.
node_network_transmit_errs_total	네트워크 디바이스 통계 transmit_errs
StorageGRID_관리_다운	노드가 예상 이유로 그리드에 연결되어 있지 않습니다. 예를 들어, 노드의 노드 또는 서비스가 정상적으로 종료되었거나 노드가 재부팅 중이거나 소프트웨어가 업그레이드 중입니다.
StorageGRID_appliance_compute_controller_hardware_status입니다	어플라이언스에서 컴퓨팅 컨트롤러 하드웨어의 상태입니다.
StorageGRID_appliance_failed_disks입니다	어플라이언스의 스토리지 컨트롤러의 경우 최적화되지 않은 드라이브의 수입니다.
StorageGRID_어플라이언스_스토리지_컨트롤러_하드웨어_상태입니다	어플라이언스에 있는 스토리지 컨트롤러 하드웨어의 전체 상태입니다.
StorageGRID_content_버킷 및_컨테이너	이 스토리지 노드에서 알려진 S3 버킷 및 Swift 컨테이너의 총 수입니다.
StorageGRID_content_objects	이 스토리지 노드에서 알려진 S3 및 Swift 데이터 오브젝트의 총 수 Count는 S3 또는 Swift를 통해 시스템과 상호 작용하는 클라이언트 애플리케이션에서 생성한 데이터 오브젝트에만 유효합니다.
StorageGRID_content_objects_lost	이 서비스가 StorageGRID 시스템에서 누락된 것으로 감지한 총 오브젝트 수입니다. 손실 원인을 파악하고 복구가 가능한지 여부를 판단하기 위한 조치를 취해야 합니다. 분실하거나 누락된 오브젝트 데이터 문제를 해결합니다
StorageGRID_http_sessions_incoming_attempted입니다	스토리지 노드에 대해 시도된 총 HTTP 세션 수입니다.
StorageGRID_http_sessions_incoming_currently_설정됨	스토리지 노드에서 현재 활성(열린) 상태의 HTTP 세션 수입니다.
StorageGRID_http_sessions_incoming_failed 를 참조하십시오	조작된 HTTP 요청 또는 작업 처리 중 오류로 인해 성공적으로 완료되지 못한 총 HTTP 세션 수입니다.
StorageGRID_http_sessions_incoming_successful입니다	성공적으로 완료된 총 HTTP 세션 수입니다.

Prometheus 메트릭입니다	설명
StorageGRID_ILM_waiting_background_objects	이 노드의 총 개체 수가 스캔에서 ILM 평가를 대기 중입니다.
StorageGRID_ILM_클라이언트_평가_개체_초당_대기 중	이 노드의 ILM 정책에 따라 객체가 평가되는 현재 속도입니다.
StorageGRID_ILM_클라이언트_개체 대기 중	클라이언트 작업(예: 수집)에서 ILM 평가를 대기 중인 이 노드의 총 오브젝트 수
StorageGRID_ILM_TOTAL_OBJECURS_TOTAL_OB	ILM 평가를 대기 중인 총 개체 수입니다.
StorageGRID_ILM_스캔_개체_초당_입니다	이 노드가 소유한 오브젝트가 스캔되어 ILM을 위해 대기되는 속도입니다.
StorageGRID_ILM_SCAN_PERIOD_Estimated_minutes입니다	이 노드에서 전체 ILM 스캔을 완료하는 데 걸리는 예상 시간입니다. • 참고: * 전체 스캔은 ILM이 이 노드가 소유한 모든 개체에 적용되었다고 보장하지 않습니다.
StorageGRID_load_balancer_endpoint_cert_expiry_time	epoch 이후 초 단위의 로드 밸런서 끝점 인증서 만료 시간.
StorageGRID_metadata_query_average_latency_milliseconds	이 서비스를 통해 메타데이터 저장소에 대해 쿼리를 실행하는 데 필요한 평균 시간입니다.
StorageGRID_NETWORK_Received_Bytes를 나타냅니다	설치 후 수신된 총 데이터 양입니다.
StorageGRID_NETWORK_TAINED_BATED	설치 후 전송된 총 데이터 양입니다.
StorageGRID_노드_CPU_활용률_백분율	이 서비스에서 현재 사용 중인 사용 가능한 CPU 시간의 백분율입니다. 서비스 사용 중인 상태를 나타냅니다. 사용 가능한 CPU 시간은 서버의 CPU 수에 따라 다릅니다.
StorageGRID_NTP_선택됨_시간_소스_오프셋_밀리초	선택한 시간 소스에서 제공하는 시간의 체계적 오프셋. 시간 소스에 도달하는 지연 시간이 시간 소스가 NTP 클라이언트에 도달하는 데 필요한 시간과 같지 않으면 오프셋이 발생합니다.
StorageGRID_NTP_잠김	노드가 네트워크 시간 프로토콜(NTP) 서버에 잠기지 않았습니다.
StorageGRID_S3_데이터_전송_바이트_수집되었습니다	속성이 마지막으로 재설정된 이후 S3 클라이언트에서 이 스토리지 노드로 수집된 총 데이터 양입니다.

Prometheus 메트릭입니다	설명
StorageGRID_S3_데이터_전송_바이트_검색됨	속성이 마지막으로 재설정된 이후 이 스토리지 노드에서 S3 클라이언트가 검색한 총 데이터 양입니다.
StorageGRID_S3_작업_에 실패했습니다	S3 승인 실패로 인해 발생한 작업을 제외한 총 S3 작업 실패 횟수(HTTP 상태 코드 4xx 및 5xx).
StorageGRID_S3_운영_성공	성공한 S3 작업의 총 수(HTTP 상태 코드 2xx).
StorageGRID_S3_운영_권한이 없습니다	인증 실패로 인한 총 실패한 S3 작업 수.
StorageGRID_servercertificate_management_interface_cert_expiry_days입니다	관리 인터페이스 인증서가 만료되기 전의 일 수입니다.
StorageGRID_servercertificate_storage_api_endpoints_cert_expiry_days를 지정합니다	객체 스토리지 API 인증서가 만료되기 전의 일 수입니다.
StorageGRID_SERVICE_CPU_초	설치 후 이 서비스에서 CPU를 사용한 누적 시간입니다.
StorageGRID_SERVICE_MEMORY_USAGE_Bytes	이 서비스에서 현재 사용 중인 메모리(RAM)의 양입니다. 이 값은 Linux 상위 유틸리티가 RES로 표시하는 값과 동일합니다.
StorageGRID_SERVICE_NETWORK_Received_Bytes를 나타냅니다	설치 후 이 서비스에서 수신한 총 데이터 양입니다.
StorageGRID_SERVICE_NETWORK_TAINED_BATED	이 서비스에서 보낸 총 데이터 양입니다.
StorageGRID_Service_Restarts	서비스가 다시 시작된 총 횟수입니다.
StorageGRID_SERVICE_RUNTIME_초	설치 후 서비스가 실행된 총 시간입니다.
StorageGRID_SERVICE_Uptime_초	서비스가 마지막으로 다시 시작된 이후 실행된 총 시간입니다.
StorageGRID_스토리지_상태_현재	스토리지 서비스의 현재 상태입니다. 속성 값은 다음과 같습니다. • 10 = 오프라인 • 15 = 유지 보수 • 20 = 읽기 전용 • 30 = 온라인

Prometheus 메트릭입니다	설명
StorageGRID_스토리지_상태입니다	스토리지 서비스의 현재 상태입니다. 속성 값은 다음과 같습니다. • 0 = 오류 없음 • 10 = 전환 중 • 20 = 사용 가능한 공간이 부족합니다 • 30 = 볼륨을 사용할 수 없습니다 • 40 = 오류
StorageGRID_스토리지_활용률_바이트	스토리지 노드에서 복제 및 삭제 코딩 오브젝트 데이터의 총 크기에 대한 추정치입니다.
StorageGRID_스토리지_활용률_메타데이터_허용됨_바이트	객체 메타데이터에 허용되는 각 스토리지 노드의 볼륨 0의 총 공간입니다. 이 값은 항상 노드의 메타데이터에 예약된 실제 공간보다 작습니다. 왜냐하면 예약된 공간의 일부는 필수 데이터베이스 작업(예: 컴팩션 및 복구) 및 향후 하드웨어 및 소프트웨어 업그레이드에 필요하기 때문입니다. 오브젝트 메타데이터에 허용되는 공간은 전체 오브젝트 용량을 제어합니다.
StorageGRID_스토리지_활용률_메타데이터_바이트	스토리지 볼륨 0의 오브젝트 메타데이터 크기(바이트)입니다.
StorageGRID_스토리지_활용률_총_공간_바이트	모든 오브젝트 저장소에 할당된 총 스토리지 공간입니다.
StorageGRID_스토리지_활용률_가용_공간_바이트	남은 총 오브젝트 스토리지 공간 크기입니다. 스토리지 노드의 모든 오브젝트 저장소에 사용할 수 있는 공간을 합산하여 계산합니다.
StorageGRID_Swift_데이터_전송_바이트_수집되었습니다	속성을 마지막으로 재설정한 이후 Swift 클라이언트에서 이 스토리지 노드로 수집된 총 데이터 양입니다.
StorageGRID_SwiFT_DATA_transfers_bytes_검색됨	속성이 마지막으로 재설정된 이후 이 스토리지 노드에서 Swift 클라이언트가 검색한 총 데이터 양입니다.
StorageGRID_SwiFT_operations_failed 를 참조하십시오	Swift 인증 실패에 의해 발생한 것을 제외한 Swift 작업의 총 실패 수(HTTP 상태 코드 4xx 및 5xx).
StorageGRID_Swift_operations_successful입니다	성공적인 Swift 작업의 총 수(HTTP 상태 코드 2xx).
StorageGRID_SwiFT_operations_unauthorized를 지정합니다	인증 실패로 인해 실패한 Swift 작업의 총 수(HTTP 상태 코드 401, 403, 405).

Prometheus 메트릭입니다	설명
StorageGRID_tenant_usage_data_bytes를 나타냅니다	테넌트의 모든 객체의 논리적 크기입니다.
StorageGRID_tenant_usage_object_count	테넌트의 객체 수입니다.
StorageGRID_tenant_usage_quota_bytes를 나타냅니다	테넌트 객체에 사용할 수 있는 최대 논리 공간 크기입니다. 할당량 메트릭을 제공하지 않으면 무제한 공간을 사용할 수 있습니다.

알람 기준(레거시 시스템)

다음 표에는 레거시 기본 경보가 모두 나열되어 있습니다. 알람이 트리거되면 이 표에서 알람 코드를 조회하여 권장 조치를 찾을 수 있습니다.

> 기존 알람 시스템은 계속 지원되지만, 알림 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

코드	이름	서비스	권장 조치
ABRL	사용 가능한 특성 릴레이	BDC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	속성 릴레이 서비스를 실행하는 서비스(ADC 서비스)에 대한 연결을 가능한 한 빨리 복원합니다. 연결된 특성 릴레이가 없는 경우 그리드 노드는 NMS 서비스에 특성 값을 보고할 수 없습니다. 따라서 NMS 서비스는 더 이상 서비스의 상태를 모니터링하거나 서비스의 속성을 업데이트할 수 없습니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
ACMS	사용 가능한 메타데이터 서비스	BARC, BLDR, BCMN	LDR 또는 ARC 서비스가 DDS 서비스에 대한 연결을 끊으면 경보가 발생합니다. 이 경우 수집 또는 검색 트랜잭션을 처리할 수 없습니다. DDS 서비스를 사용할 수 없게 되는 것이 일시적인 문제일 경우 트랜잭션이 지연될 수 있습니다. DDS 서비스에 대한 연결을 확인 및 복원하여 이 경보를 지우고 서비스를 전체 기능으로 되돌립니다.

코드	이름	서비스	권장 조치
행동합니다	Cloud Tiering Service 상태	호	타겟 클라우드 계층화의 유형이 S3(Simple Storage Service)인 아카이브 노드에만 사용할 수 있습니다. 아카이브 노드의 ACTS 속성이 읽기 전용 설정 또는 읽기-쓰기 비활성 으로 설정된 경우 속성을 읽기-쓰기 사용 으로 설정해야 합니다. 인증 실패로 인해 주요 경보가 트리거되는 경우 대상 버킷과 연결된 자격 증명을 확인하고 필요한 경우 값을 업데이트합니다. 다른 이유로 인해 주요 경보가 발생하는 경우 기술 지원 부서에 문의하십시오.
고급	ADC 상태	ADC	알람이 트리거되면 * support * > * Tools * > * Grid topology * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * ADC * > * Overview * > * Main * 및 * ADC * > * Alarms * > * Main * 을 선택하여 알람 원인을 확인합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
고급	ADC 상태	ADC	ADC 상태 값이 Standby(대기) 인 경우 서비스 모니터링을 계속하고 문제가 지속되면 기술 지원 부서에 문의하십시오. ADC 상태 값이 오프라인이면 서비스를 다시 시작합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
아ITE	상태 검색	BARC	타겟 유형이 TSM(Tivoli Storage Manager)인 아카이브 노드에만 사용할 수 있습니다. Retrieve State 값이 Target을 기다리는 경우 TSM 미들웨어 서버를 확인하고 올바르게 작동하는지 확인합니다. 아카이브 노드가 StorageGRID 시스템에 방금 추가된 경우 대상 외부 아카이브 스토리지 시스템에 대한 아카이브 노드의 연결이 올바르게 구성되어 있는지 확인합니다. 아카이브 검색 상태 값이 오프라인인 경우 상태를 온라인으로 업데이트해 봅니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * ARC * > * Retrieve * > * Configuration * > * Main * 을 선택하고 * Archive Retrieve State * > * Online * 을 선택한 다음 * Apply Changes * 를 클릭합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.

코드	이름	서비스	권장 조치
AITU	상태 검색	BARC	검색 상태 값이 대상 오류인 경우 대상 외부 아카이브 스토리지 시스템에서 오류를 확인하십시오. Archive Retrieve Status 값이 Session Lost인 경우 대상이 지정된 외부 아카이브 스토리지 시스템이 온라인 상태이고 올바르게 작동하는지 확인합니다. 대상과의 네트워크 연결을 확인합니다. 아카이브 검색 상태 값이 알 수 없는 오류인 경우 기술 지원 부서에 문의하십시오.
ALIS	인바운드 속성 세션	ADC	속성 릴레이의 인바운드 속성 세션 수가 너무 커지면 StorageGRID 시스템이 균형을 잃어 있음을 나타낼 수 있습니다. 정상적인 조건에서 특성 세션은 ADC 서비스 간에 균등하게 분산되어야 합니다. 불균형은 성능 문제를 야기할 수 있습니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
알로스	아웃바운드 속성 세션	ADC	ADC 서비스는 많은 속성 세션을 가지고 있으며 과부하가 되고 있습니다. 이 경보가 트리거되면 기술 지원 부서에 문의하십시오.
알로	연결할 수 없는 속성 리포지토리	ADC	NMS 서비스와의 네트워크 연결을 확인하여 서비스가 속성 리포지토리에 연결할 수 있는지 확인합니다. 이 경보가 트리거되고 네트워크 연결이 양호한 경우 기술 지원 부서에 문의하십시오.

코드	이름	서비스	권장 조치
AMQS	감사 메시지가 대기 중입니다	BDC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	감사 메시지를 즉시 감사 릴레이 또는 리포지토리로 전달할 수 없는 경우 메시지는 디스크 대기열에 저장됩니다. 디스크 대기열이 가득 차면 중단이 발생할 수 있습니다. 가동 중단을 방지하기 위해 적시에 응답할 수 있도록 디스크 대기열의 메시지 수가 다음 임계값에 도달하면 AMQS 알람이 트리거됩니다. • 주의사항: 100,000개 이상의 메시지 • Minor(최소): 최소 500,000개의 메시지 • Major: 최소 2,000,000개의 메시지 • 위험: 최소 5,000,000개의 메시지 AMQS 알람이 트리거되면 시스템의 부하를 점검합니다. 트랜잭션이 상당히 많이 발생한 경우 알람이 시간 경과에 따라 자동으로 해결되어야 합니다. 이 경우 알람을 무시할 수 있습니다. 경보가 지속되고 심각도가 증가하면 대기열 크기의 차트를 보십시오. 시간이 경과하거나 며칠 동안 꾸준히 증가하는 경우 감사 로드가 시스템의 감사 용량을 초과할 가능성이 높습니다. 감사 수준을 오류 또는 끄기로 변경하여 클라이언트 작업 속도를 줄이거나 기록된 감사 메시지 수를 줄입니다. 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다.
AOTE	Store State(상태 저장)	BARC	타겟 유형이 TSM(Tivoli Storage Manager)인 아카이브 노드에만 사용할 수 있습니다. Store State 값이 Target을 기다리는 경우, 외부 아카이브 스토리지 시스템을 확인하고 올바르게 작동하는지 확인합니다. 아카이브 노드가 StorageGRID 시스템에 방금 추가된 경우 대상 외부 아카이브 스토리지 시스템에 대한 아카이브 노드의 연결이 올바르게 구성되어 있는지 확인합니다. Store State 값이 Offline 인 경우 Store Status 값을 확인합니다. Store State(매장 상태)를 다시 Online(온라인)으로 이동하기 전에 문제를 해결하십시오.

코드	이름	서비스	권장 조치
AOTU	저장 상태	BARC	Store Status 값이 Session Lost인 경우 외부 아카이브 스토리지 시스템이 연결되어 있고 온라인 상태인지 확인합니다. Target Error 값이 있는 경우 외부 아카이브 스토리지 시스템에서 오류를 확인합니다. 스토어 상태 값이 알 수 없는 오류인 경우 기술 지원 부서에 문의하십시오.
APMS	스토리지 다중 경로 연결	SSM	다중 경로 상태 알람이 "Dedgeded"로 표시되는 경우(* 지원 * > * 도구 * > * 그리드 토폴로지 * 선택) * *site* * > * *GRID NODE* * > * SSM * > * Events * 선택) 다음을 수행합니다. 1. 표시등이 표시되지 않는 케이블을 연결하거나 교체합니다. 2. 1-5분 정도 기다립니다. 첫 번째 케이블을 연결한 후 5분 이상 다른 케이블을 뽑지 마십시오. 너무 일찍 플러그를 뽑으면 루트 볼륨이 읽기 전용으로 되어 하드웨어를 다시 시작해야 할 수 있습니다. 3. SSM * > * Resources * 페이지로 돌아가 스토리지 하드웨어 섹션에서 "Ded그레이드" 다중 경로 상태가 ""공칭""로 변경되었는지 확인합니다.
ARCE	호 상태	호	ARC 서비스는 모든 ARC 구성 요소(복제, 저장, 검색, 대상)가 시작될 때까지 대기 상태를 가집니다. 그런 다음 온라인으로 전환됩니다. ARC 상태 값이 Standby(대기)에서 Online(온라인)으로 전환되지 않는 경우 ARC 구성 요소의 상태를 확인합니다. ARC 상태 값이 오프라인이면 서비스를 다시 시작합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
AROQ	개체가 대기 중입니다	호	이 경보는 대상 외부 아카이브 스토리지 시스템의 문제로 인해 이동식 저장 장치가 느리게 실행되거나 여러 개의 읽기 오류가 발생한 경우에 발생할 수 있습니다. 외부 아카이브 스토리지 시스템에서 오류가 있는지 확인하고 제대로 작동하는지 확인합니다. 경우에 따라 데이터 요청 비율이 높기 때문에 이 오류가 발생할 수 있습니다. 시스템 활동이 감소함에 따라 대기 중인 개체의 수를 모니터링합니다.

코드	이름	서비스	권장 조치
ARRF	요청 실패	호	대상 외부 아카이브 스토리지 시스템에서 검색에 실패하면 아카이브 노드는 일시적인 문제로 인해 장애가 발생할 수 있으므로 검색을 다시 시도합니다. 그러나 개체 데이터가 손상되었거나 영구적으로 사용할 수 없는 것으로 표시된 경우에는 검색이 실패하지 않습니다. 대신 아카이브 노드는 검색을 계속 재시도하며 요청 실패 값은 계속 증가합니다. 이 경보는 요청된 데이터를 보관하는 저장 미디어가 손상되었음을 나타낼 수 있습니다. 문제를 더 자세히 진단하려면 외부 아카이브 스토리지 시스템을 확인하십시오. 객체 데이터가 더 이상 아카이브에 없는 것으로 판단될 경우 객체를 StorageGRID 시스템에서 제거해야 합니다. 자세한 내용은 기술 지원 부서에 문의하십시오. 이 알람을 트리거한 문제가 해결되면 실패 수를 재설정합니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * ARC * > * Retrieve * > * Configuration * > * Main * 을 선택하고 * Reset Request Failure Count * 를 선택한 후 * Apply Changes * 를 클릭합니다.
ARRV	확인 실패	호	이 문제를 진단하고 해결하려면 기술 지원 부서에 문의하십시오. 이 알람을 트리거한 문제가 해결되면 실패 수를 재설정합니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * ARC * > * Retrieve * > * Configuration * > * Main * 을 선택하고 * Reset Verification Failure Count * 를 선택한 후 * Apply Changes * 를 클릭합니다.
ARVF	저장 실패	호	이 경보는 대상 외부 아카이브 스토리지 시스템의 오류로 인해 발생할 수 있습니다. 외부 아카이브 스토리지 시스템에서 오류가 있는지 확인하고 제대로 작동하는지 확인합니다. 이 알람을 트리거한 문제가 해결되면 실패 수를 재설정합니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * ARC * > * Retrieve * > * Configuration * > * Main * 을 선택하고 * Reset Store Failure Count * 를 선택한 다음 * Apply Changes * 를 클릭합니다.

코드	이름	서비스	권장 조치
ASXP	공유 감사	AMS	Audit Shares의 값이 Unknown인 경우 알람이 발생합니다. 이 경보는 관리 노드의 설치 또는 구성에 문제가 있음을 나타낼 수 있습니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
8월	AMS 상태	AMS	AMS Status 값이 DB Connectivity Error인 경우 GRID 노드를 다시 시작한다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
자동	AMS 상태	AMS	AMS 상태 값이 Standby(대기) 인 경우 StorageGRID 시스템 모니터링을 계속합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오. AMS 상태 값이 오프라인이면 서비스를 다시 시작합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
AUXS	감사 내보내기 상태	AMS	알람이 트리거되면 기본 문제를 해결한 다음 AMS 서비스를 다시 시작합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
BADD	스토리지 컨트롤러 오류 드라이브 수	SSM	이 경보는 StorageGRID 어플라이언스에 있는 하나 이상의 드라이브가 고장났거나 최적 상태가 아닐 때 발생합니다. 필요에 따라 드라이브를 교체하십시오.
BASF	사용 가능한 개체 식별자	CMN	StorageGRID 시스템이 프로비저닝되면 CMN 서비스에 고정된 수의 오브젝트 식별자가 할당됩니다. 이 경보는 StorageGRID 시스템이 개체 식별자의 공급을 배가하기 시작할 때 트리거됩니다. 더 많은 식별자를 할당하려면 기술 지원 부서에 문의하십시오.

코드	이름	서비스	권장 조치
중저음	식별자 블록 할당 상태	CMN	기본적으로 ADC 쿼럼에 도달할 수 없기 때문에 개체 식별자를 할당할 수 없을 때 경보가 트리거됩니다. CMN 서비스에 대한 식별자 블록 할당을 수행하려면 ADC 서비스의 쿼럼(50% + 1)이 온라인 및 연결되어야 합니다. 쿼럼을 사용할 수 없는 경우 CMN 서비스는 ADC 쿼럼이 다시 설정될 때까지 새 식별자 블록을 할당할 수 없습니다. ADC 쿼럼이 손실된 경우 일반적으로 StorageGRID 시스템에 즉각적인 영향을 주지 않습니다(클라이언트는 콘텐츠를 수집하고 검색할 수 있음). 약 한 달 동안 ID가 그리드의 다른 위치에 캐시되기 때문입니다. 그러나 이러한 상황이 계속되면 StorageGRID 시스템이 새 콘텐츠를 수집하는 기능을 잃게 됩니다. 알람이 트리거되면 ADC quorum이 손실된 이유(예: 네트워크 또는 스토리지 노드 장애)를 조사하여 수정 조치를 취합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
BRDT	컴퓨팅 컨트롤러 섀시 온도	SSM	StorageGRID 어플라이언스의 컴퓨팅 컨트롤러 온도가 공칭 임계값을 초과할 경우 알람이 트리거됩니다. 하드웨어 구성 요소 및 환경 문제가 과열되었는지 확인합니다. 필요한 경우 구성 요소를 교체합니다.
BTOF	오프셋	BDC, BLDR, BNMS, BMS, BCLB, BCMN, BARC	서비스 시간(초)이 운영 체제 시간과 크게 다를 경우 알람이 트리거됩니다. 정상적인 상황에서는 서비스가 자체적으로 재동기화되어야 합니다. 서비스 시간이 운영 체제 시간에서 너무 멀리 떨어져 있는 경우 시스템 작동에 영향을 줄 수 있습니다. StorageGRID 시스템의 시간 소스가 올바른지 확인합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
BTSE	시계 상태	BDC, BLDR, BNMS, BMS, BCLB, BCMN, BARC	서비스 시간이 운영 체제에서 추적한 시간과 동기화되지 않으면 경보가 발생합니다. 정상적인 상황에서는 서비스가 자체적으로 재동기화되어야 합니다. 시간이 운영 체제 시간에서 너무 멀리 떨어져 있는 경우 시스템 작동에 영향을 줄 수 있습니다. StorageGRID 시스템의 시간 소스가 올바른지 확인합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.

코드	이름	서비스	권장 조치
CAHP	Java 힙 사용량 백분율	DDS	Java가 시스템이 제대로 작동할 수 있도록 충분한 힙 공간을 허용하는 속도로 가비지 수집을 수행할 수 없는 경우 알람이 트리거됩니다. 이 경보는 DDS 메타데이터 저장소에 대해 시스템 전체에서 사용 가능한 리소스를 초과하는 사용자 작업 부하를 나타낼 수 있습니다. 대시보드에서 ILM 활동을 확인하거나 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택한 다음 *사이트 * > * *GRID* 노드 * > * DDS * > * 리소스 * > * 개요 * > * 주 * 를 선택합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
CAIH	사용 가능한 Ingest 대상 수입니다	CLB	이 알람은 사용되지 않습니다.
캐나다	사용 가능한 대상 수	CLB	이 경보는 사용 가능한 LDR 서비스의 기본 문제가 해결되면 해제됩니다. LDR 서비스의 HTTP 구성 요소가 온라인 상태이고 정상적으로 실행되고 있는지 확인합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
카사	데이터 저장소 상태	DDS	Cassandra 메타데이터 저장소를 사용할 수 없게 되면 알람이 발생합니다. Cassandra 상태 확인: 1. 스토리지 노드에서 admin과 Su로 로그인하여 Passwords.txt 파일에 나열된 암호를 사용하여 root로 로그인합니다. 2. 'Service cassandra status'를 입력합니다 3. Cassandra가 실행되고 있지 않으면 'Service cassandra restart(서비스 카사드라 다시 시작)'를 다시 시작합니다 이 경보는 또한 스토리지 노드의 메타데이터 저장소(Cassandra 데이터베이스)를 재구축해야 함을 나타낼 수 있습니다. 에서 서비스:상태-Cassandra(SVST) 알람 문제 해결에 대한 정보를 참조하십시오 메타데이터 문제를 해결합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
케이스	데이터 저장소 상태	DDS	이 경보는 설치 또는 확장 중에 새 데이터 저장소가 그리드에 가입되고 있음을 나타내기 위해 트리거됩니다.

코드	이름	서비스	권장 조치
CCES를 참조하십시오	수신 세션 - 설정됨	CLB	이 경보는 게이트웨이 노드에서 현재 활성(개방) 상태인 HTTP 세션이 20,000개 이상인 경우 트리거됩니다. 클라이언트에 연결이 너무 많은 경우 연결 오류가 발생할 수 있습니다. 작업 부하를 줄여야 합니다.
CCNA	컴퓨팅 하드웨어	SSM	이 경보는 StorageGRID 어플라이언스의 컴퓨팅 컨트롤러 하드웨어 상태에 주의가 필요한 경우에 발생합니다.
CDLP	사용된 메타데이터 공간(퍼센트)	DDS	이 경보는 CEMS(Metadata Effective Space)가 70% 차(Minor 알람), 90% 차(Major 알람) 및 100% 차(Critical 알람)에 도달할 때 트리거됩니다. 이 경보가 90% 임계값에 도달하면 그리드 관리자의 대시보드에 경고가 나타납니다. 가능한 빨리 확장 절차를 수행하여 새 스토리지 노드를 추가해야 합니다. 을 참조하십시오 그리드를 확장합니다. 이 경보가 100% 임계값에 도달하면 객체 인제스트를 중지하고 스토리지 노드를 즉시 추가해야 합니다. Cassandra에는 컴팩션 및 복원과 같은 중요 작업을 수행하려면 일정 양의 공간이 필요합니다. 오브젝트 메타데이터에서 허용되는 공간의 100% 이상을 사용하는 경우 이러한 작업이 영향을 받습니다. 원치 않는 결과가 발생할 수 있습니다. • 참고 *: 스토리지 노드를 추가할 수 없는 경우 기술 지원 부서에 문의하십시오. 새 스토리지 노드가 추가되면 시스템이 모든 스토리지 노드에서 개체 메타데이터를 자동으로 재조정하며 경보가 지워집니다. 에서 메타데이터 부족 스토리지 알림 문제 해결에 대한 정보도 참조하십시오 메타데이터 문제를 해결합니다.
CLBA	CLB 상태	CLB	알람이 트리거되면 * support * > * Tools * > * Grid topology * 를 선택한 다음 **site* * > * *GRID node* * > * CLB * > * Overview * > * Main * 및 * CLB * > * Alarms * > * Main * 을 선택하여 알람 원인을 확인하고 문제를 해결하십시오. 문제가 지속되면 기술 지원 팀에 문의하십시오.

코드	이름	서비스	권장 조치
CLBE	CLB 상태	CLB	CLB 상태 값이 Standby(대기) 인 경우, 상황을 계속 모니터링하고 문제가 지속되면 기술 지원 부서에 문의하십시오. 상태가 오프라인이고 알려진 서버 하드웨어 문제(예: 서버 연결이 끊어짐)가 없거나 예약된 가동 중지 시간이 없는 경우 서비스를 다시 시작합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
CMNA	CMN 상태	CMN	CMN 상태 값이 오류인 경우 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택한 다음 *사이트 _ * > * _*GRID NODE* * > * CMN * > * 개요 * > * 메인 * 및 * CMN * > * 알람 * > * 메인 * 을 선택하여 오류의 원인을 확인하고 문제를 해결하십시오. CMN이 전환될 때 기본 관리 노드의 하드웨어 새로 고침 중에 알람이 트리거되고 CMN 상태 값이 온라인 CMN이 아닙니다(이전 CMN 상태 값은 대기 상태이고 새 값은 온라인). 문제가 지속되면 기술 지원 팀에 문의하십시오.
CPRC	남은 용량	NMS	남은 용량(NMS 데이터베이스에서 열 수 있는 사용 가능한 연결 수)이 구성된 알람 심각도 미만으로 떨어지면 알람이 트리거됩니다. 알람이 트리거되면 기술 지원 팀에 문의하십시오.
CPSA	컴퓨팅 컨트롤러 전원 공급 장치 A	SSM	StorageGRID 어플라이언스의 컴퓨팅 컨트롤러에 전원 공급 장치 A에 문제가 있는 경우 알람이 트리거됩니다. 필요한 경우 구성 요소를 교체합니다.
cPSB	컴퓨팅 컨트롤러 전원 공급 장치 B	SSM	StorageGRID 어플라이언스의 컴퓨팅 컨트롤러에 전원 공급 장치 B에 문제가 있는 경우 알람이 트리거됩니다. 필요한 경우 구성 요소를 교체합니다.
CPUT	컴퓨팅 컨트롤러 CPU 온도	SSM	StorageGRID 어플라이언스의 컴퓨팅 컨트롤러에 있는 CPU 온도가 공칭 임계값을 초과하면 경보가 발생합니다. 스토리지 노드가 StorageGRID 어플라이언스인 경우 StorageGRID 시스템에서 컨트롤러에 주의가 필요함을 나타냅니다. 하드웨어 구성 요소 및 환경 문제가 과열되었는지 확인합니다. 필요한 경우 구성 요소를 교체합니다.

코드	이름	서비스	권장 조치
NST	DNS 상태	SSM	설치가 완료되면 SSM 서비스에서 NST 알람이 트리거됩니다. DNS를 구성하고 새 서버 정보가 모든 그리드 노드에 도달하면 알람이 취소됩니다.
ECCD	손상된 조각이 감지되었습니다	LDR	백그라운드 검증 프로세스에서 손상된 삭제 코딩 조각이 감지되면 경보가 트리거됩니다. 손상된 조각이 발견되면 조각을 재생성하려고 시도합니다. 손상된 조각을 재설정하고 손실된 속성을 0으로 복사하며, 이를 모니터링하여 카운트 다시 증가 여부를 확인합니다. 카운트가 상향 이동되면 스토리지 노드의 기본 스토리지에 문제가 있을 수 있습니다. 삭제 코딩 오브젝트 데이터의 사본은 손실되거나 손상된 조각의 수가 삭제 코드의 내결함성을 손상할 때까지 누락된 것으로 간주하지 않습니다. 따라서 손상된 조각을 가지고 계속 오브젝트를 검색할 수 있습니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
ECST	확인 상태	LDR	이 경보는 이 스토리지 노드에서 암호화된 오브젝트 삭제 데이터에 대한 백그라운드 검증 프로세스의 현재 상태를 나타냅니다. 백그라운드 검증 프로세스에 오류가 있는 경우 주요 경보가 트리거됩니다.
부품 번호	파일 설명자를 엽니다	BDC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	FOPN은 최대 활동 중에 크기가 커질 수 있습니다. 활동이 느린 기간 동안 감소하지 않으면 기술 지원 부서에 문의하십시오.
HSTE	HTTP 상태	흑백	HSTU에 대한 권장 조치를 참조하십시오.

코드	이름	서비스	권장 조치
HSTU	HTTP 상태	흑백	HSTE 및 HSTU는 S3, Swift 및 기타 내부 StorageGRID 트래픽을 포함한 모든 LDR 트래픽에 대한 HTTP 프로토콜과 관련되어 있습니다. 경보는 다음 상황 중 하나가 발생했음을 나타냅니다. • HTTP 프로토콜이 수동으로 오프라인 상태로 전환되었습니다. • 자동 시작 HTTP 특성이 비활성화되었습니다. • LDR 서비스가 종료되는 중입니다. 자동 시작 HTTP 속성은 기본적으로 활성화되어 있습니다. 이 설정을 변경하면 다시 시작한 후에 HTTP가 오프라인 상태로 유지될 수 있습니다. 필요한 경우 LDR 서비스가 다시 시작될 때까지 기다립니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 *스토리지 노드 * > * LDR * > * 구성 * 을 선택합니다. HTTP 프로토콜이 오프라인인 경우 온라인 상태로 전환합니다. HTTP 자동 시작 속성이 활성화되어 있는지 확인합니다. HTTP 프로토콜이 오프라인 상태로 유지되면 기술 지원 부서에 문의하십시오.
HTAS	HTTP를 자동으로 시작합니다	LDR	시작 시 HTTP 서비스를 자동으로 시작할지 여부를 지정합니다. 사용자 지정 구성 옵션입니다.
IRSU	인바운드 복제 상태	BLDR, BARC	인바운드 복제가 비활성화되었음을 알리는 경보가 표시됩니다. 구성 설정 확인: * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * LDR * > * Replication * > * Configuration * > * Main * 을 선택합니다.
라타	평균 지연 시간	NMS	연결 문제를 확인합니다. 시스템 활동을 점검하여 시스템 활동이 증가하는지 확인하십시오. 시스템 활동이 증가하면 특성 데이터 활동이 증가합니다. 이렇게 활동이 증가하면 특성 데이터 처리가 지연됩니다. 이는 정상적인 시스템 활동일 수 있으며 하위 작업이 될 수 있습니다. 여러 개의 알람을 점검합니다. 평균 지연 시간 증가는 트리거된 알람의 과다한 수로 나타날 수 있습니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.

코드	이름	서비스	권장 조치
LDRE	LDR 상태	LDR	LDR 상태 값이 대기 인 경우, 상태를 계속 모니터링하고 문제가 지속되면 기술 지원 부서에 문의하십시오. LDR 상태 값이 오프라인인 경우 서비스를 다시 시작합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
분실	손실된 개체	DDS, LDR	StorageGRID 시스템이 시스템 내의 모든 위치에서 요청된 개체의 복사본을 검색하지 못할 때 트리거됩니다. 손실(개체 손실) 경보가 트리거되기 전에 시스템은 시스템의 다른 위치에서 누락된 개체를 검색하고 교체하려고 시도합니다. 손실된 개체는 데이터 손실을 나타냅니다. 손실된 개체 속성은 DDS 서비스가 ILM 정책을 충족하기 위해 의도적으로 컨텐츠를 퍼지하지 않고 객체의 위치 수가 0으로 떨어질 때마다 증가합니다. 분실(객체 손실) 알람을 즉시 조사하십시오. 문제가 지속되면 기술 지원 팀에 문의하십시오. 분실하거나 누락된 오브젝트 데이터 문제를 해결합니다
MCEP	관리 인터페이스 인증서 만료	CMN	관리 인터페이스에 액세스하는 데 사용되는 인증서가 곧 만료될 때 트리거됩니다. 1. 그리드 관리자에서 * 구성 * > * 보안 * > * 인증서 * 를 선택합니다. 2. 글로벌 * 탭에서 * 관리 인터페이스 인증서 * 를 선택합니다. 3. 새 관리 인터페이스 인증서를 업로드합니다.
마인큐	이메일 알림 대기 중	NMS	NMS 서비스를 호스팅하는 서버 및 외부 메일 서버의 네트워크 연결을 확인합니다. 또한 이메일 서버 구성이 올바른지 확인하십시오. 경보에 대한 이메일 서버 설정 구성(레거시 시스템)
분	이메일 알림 상태	BNMS	NMS 서비스가 메일 서버에 연결할 수 없는 경우 보조 경보가 발생합니다. NMS 서비스를 호스팅하는 서버 및 외부 메일 서버의 네트워크 연결을 확인합니다. 또한 이메일 서버 구성이 올바른지 확인하십시오. 경보에 대한 이메일 서버 설정 구성(레거시 시스템)

코드	이름	서비스	권장 조치
놓칠 수 있습니다	NMS 인터페이스 엔진 상태	BNMS	관리 노드의 NMS 인터페이스 엔진이 시스템에서 인터페이스 컨텐츠를 수집하고 생성하는 경우 알람이 트리거됩니다. 서버 관리자 를 선택하여 서버 개별 응용 프로그램이 다운되었는지 확인합니다.
Nang	네트워크 자동 협상 설정	SSM	네트워크 어댑터 구성을 확인합니다. 이 설정은 네트워크 라우터 및 스위치의 기본 설정과 일치해야 합니다. 잘못된 설정은 시스템 성능에 심각한 영향을 줄 수 있습니다.
NDUP	네트워크 이중 모드 설정	SSM	네트워크 어댑터 구성을 확인합니다. 이 설정은 네트워크 라우터 및 스위치의 기본 설정과 일치해야 합니다. 잘못된 설정은 시스템 성능에 심각한 영향을 줄 수 있습니다.
NLNK	네트워크 링크 감지	SSM	포트와 스위치에서 네트워크 케이블 연결을 확인합니다. 네트워크 라우터, 스위치 및 어댑터 구성을 확인합니다. 서버를 다시 시작합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
NRER	수신 오류	SSM	NRER 알람의 원인은 다음과 같습니다. • 정방향 오류 수정(FEC)이 일치하지 않습니다 • 스위치 포트와 NIC MTU가 일치하지 않습니다 • 높은 링크 오류율 • NIC 링 버퍼 오버런 에서 NRER(Network Receive Error) 경보 문제 해결에 대한 정보를 참조하십시오 네트워크, 하드웨어 및 플랫폼 문제를 해결합니다.
NRLY	사용 가능한 감사 릴레이	BDC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	감사 릴레이가 ADC 서비스에 연결되어 있지 않으면 감사 이벤트를 보고할 수 없습니다. 연결이 복원될 때까지 사용자가 대기하며 사용할 수 없습니다. ADC 서비스에 대한 연결을 가능한 한 빨리 복원합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.

코드	이름	서비스	권장 조치
NSCA	NMS 상태	NMS	NMS Status 값이 DB Connectivity Error인 경우 서비스를 다시 시작합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
NSCE	NMS 상태	NMS	NMS 상태 값이 Standby(대기) 인 경우 모니터링을 계속하고 문제가 지속되면 기술 지원 부서에 문의하십시오. NMS 상태 값이 오프라인인 경우 서비스를 다시 시작합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
NSPD	속도	SSM	이 문제는 네트워크 연결 또는 드라이버 호환성 문제로 인해 발생할 수 있습니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
NTBR	사용 가능한 테이블스페이스	NMS	알람이 트리거되면 데이터베이스 사용량이 얼마나 빠르게 변경되었는지 확인합니다. 시간이 지남에 따라 점진적으로 변경되는 것이 아니라 갑작스런 드롭은 오류 상태를 나타냅니다. 문제가 지속되면 기술 지원 팀에 문의하십시오. 알람 임계값을 조정하면 추가 스토리지를 할당해야 할 때 사전 예방적으로 관리할 수 있습니다. 사용 가능한 공간이 하한 임계값에 도달하면(알람 임계값 참조) 기술 지원 부서에 문의하여 데이터베이스 할당을 변경합니다.
네터	전송 오류	SSM	이러한 오류는 수동으로 다시 설정하지 않고 지울 수 있습니다. 이 옵션을 선택하지 않으면 네트워크 하드웨어를 확인하십시오. 어댑터 하드웨어 및 드라이버가 네트워크 라우터 및 스위치와 작동하도록 올바르게 설치 및 구성되었는지 확인합니다. 기본 문제가 해결되면 카운터를 재설정합니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * SSM * > * Resources * > * Configuration * > * Main * 을 선택하고 * Reset Transmit Error Count * 를 선택한 다음 * Apply Changes * 를 클릭합니다.
NTFQ	NTP 주파수 오프셋	SSM	주파수 오프셋이 구성된 임계값을 초과하는 경우 로컬 클럭에 하드웨어 문제가 있을 수 있습니다. 문제가 지속되면 기술 지원 팀에 문의하여 교체를 요청하십시오.

코드	이름	서비스	권장 조치
NTLK	NTP 잠금	SSM	NTP 데몬이 외부 시간 소스에 잠기지 않은 경우 지정된 외부 시간 소스, 해당 가용성 및 안정성에 대한 네트워크 연결을 확인합니다.
NTOF	NTP 시간 오프셋	SSM	시간 오프셋이 구성된 임계값을 초과하는 경우 로컬 시계의 발진기에 하드웨어 문제가 있을 수 있습니다. 문제가 지속되면 기술 지원 팀에 문의하여 교체를 요청하십시오.
NTSJ	선택한 시간 소스 지터	SSM	이 값은 로컬 서버의 NTP가 참조로 사용하는 시간 소스의 안정성 및 안정성을 나타냅니다. 알람이 트리거되면 시간 소스의 발진기에 결함이 있거나 시간 소스에 대한 WAN 링크에 문제가 있음을 나타낼 수 있습니다.
NTSU	NTP 상태	SSM	NTP 상태 값이 실행되고 있지 않으면 기술 지원 부서에 문의하십시오.
OPST	전체 전원 상태	SSM	StorageGRID 제품의 전원이 권장 작동 전압과 차이가 나는 경우 알람이 트리거됩니다. 전원 공급 장치 A 또는 B의 상태를 점검하여 어떤 전원 공급 장치가 비정상적으로 작동하는지 확인합니다. 필요한 경우 전원 공급 장치를 교체합니다.
합니다	개체를 격리했습니다	LDR	StorageGRID 시스템에서 개체를 자동으로 복원한 후에는 격리된 개체를 격리 디렉터리에서 제거할 수 있습니다. 1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 2. site * > * Storage Node * > * LDR * > * Verification * > * Configuration * > * Main * 을 선택합니다. 3. 격리된 개체 삭제 * 를 선택합니다. 4. 변경 내용 적용 * 을 클릭합니다. 격리된 객체가 제거되고 개수가 0으로 재설정됩니다.

코드	이름	서비스	권장 조치
ORSU	아웃바운드 복제 상태입니다	BLDR, BARC	알람은 아웃바운드 복제가 가능하지 않음을 나타냅니다. 스토리지는 객체를 검색할 수 없는 상태입니다. 아웃바운드 복제를 수동으로 비활성화하면 경보가 트리거됩니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * LDR * > * Replication * > * Configuration * 을 선택합니다. LDR 서비스를 복제할 수 없는 경우 알람이 트리거됩니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * LDR * > * Storage * 를 선택합니다.
OSLF	쉘프 상태	SSM	스토리지 어플라이언스의 스토리지 쉘프에 있는 구성 요소 중 하나의 상태가 저하되면 알람이 트리거됩니다. 스토리지 쉘프 구성 요소에는 IOM, 팬, 전원 공급 장치 및 드라이브 드로어가 포함됩니다. 이 경보가 발생하면 어플라이언스에 대한 유지 관리 지침을 참조하십시오.
PMEM	서비스 메모리 사용량(%)	BDC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Y% RAM 이상의 값을 가질 수 있습니다. 여기서 Y는 서버에서 사용 중인 메모리의 백분율을 나타냅니다. 80% 미만의 수치는 정상입니다. 90% 이상이 문제로 간주됩니다. 단일 서비스에 대한 메모리 사용량이 높은 경우 상황을 모니터링하고 조사합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
PSA	전원 공급 장치 A 상태	SSM	StorageGRID 제품의 전원 공급 장치 A가 권장 작동 전압과 차이가 나는 경우 알람이 트리거됩니다. 필요한 경우 전원 공급 장치 A를 교체합니다
PSBS	전원 공급 장치 B 상태	SSM	StorageGRID 제품의 전원 공급 장치 B가 권장 작동 전압과 차이가 나는 경우 알람이 트리거됩니다. 필요한 경우 전원 공급 장치 B를 교체합니다

코드	이름	서비스	권장 조치
RDTE	Tivoli Storage Manager 상태입니다	BARC	타겟 유형이 TSM(Tivoli Storage Manager)인 아카이브 노드에만 사용할 수 있습니다. Tivoli Storage Manager State의 값이 Offline인 경우 Tivoli Storage Manager Status를 확인하여 문제를 해결하십시오. 구성 요소를 다시 온라인 상태로 전환합니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * ARC * > * Target * > * Configuration * > * Main * 을 선택하고 * Tivoli Storage Manager State * > * Online * 을 선택한 다음 * Apply Changes * 를 클릭합니다.
RDTU	Tivoli Storage Manager 상태입니다	BARC	타겟 유형이 TSM(Tivoli Storage Manager)인 아카이브 노드에만 사용할 수 있습니다. Tivoli Storage Manager Status의 값이 Configuration Error 이고 아카이브 노드가 StorageGRID 시스템에 방금 추가된 경우 TSM 미들웨어 서버가 올바르게 구성되어 있는지 확인하십시오. Tivoli Storage Manager Status의 값이 Connection Failure 또는 Connection Failure인 경우, 재시도 시 TSM 미들웨어 서버의 네트워크 구성과 TSM 미들웨어 서버와 StorageGRID 시스템 간의 네트워크 연결을 확인하십시오. Tivoli Storage Manager Status의 값이 Authentication Failure 또는 Authentication Failure인 경우 Reconnecting인 경우 StorageGRID 시스템은 TSM 미들웨어 서버에 연결할 수 있지만 연결을 인증할 수 없습니다. TSM 미들웨어 서버가 올바른 사용자, 암호 및 권한으로 구성되어 있는지 확인하고 서비스를 다시 시작합니다. Tivoli Storage Manager Status의 값이 Session Failure인 경우, 설정된 세션이 예기치 않게 손실되었습니다. TSM 미들웨어 서버와 StorageGRID 시스템 간의 네트워크 연결을 확인합니다. 미들웨어 서버에 오류가 있는지 확인합니다. Tivoli Storage Manager Status의 값이 Unknown Error인 경우 기술 지원 부서에 문의하십시오.

코드	이름	서비스	권장 조치
RIRF	인바운드 복제 — 실패	BLDR, BARC	인바운드 복제 — 장애가 발생한 알람은 로드가 높거나 일시적인 네트워크 중단 기간 동안 발생할 수 있습니다. 시스템 활동이 감소하면 이 경보가 해제됩니다. 실패한 복제 수가 계속 증가하는 경우 네트워크 문제를 찾아 소스 및 대상 LDR 및 ARC 서비스가 온라인 상태이고 사용 가능한지 확인합니다. 개수를 재설정하려면 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택한 다음 *사이트 * > * *GRID* 노드 * > * LDR * > * 복제 * > * 구성 * > * 주 * 를 선택합니다. Reset Inbound Replication Failure Count * 를 선택하고 * Apply Changes * 를 클릭합니다.
RIRQ	인바운드 복제 — 대기 중	BLDR, BARC	알람은 부하가 높거나 일시적인 네트워크 중단 기간 동안 발생할 수 있습니다. 시스템 활동이 감소하면 이 경보가 해제됩니다. 대기 중인 복제 수가 계속 증가하는 경우 네트워크 문제를 찾아 소스 및 대상 LDR 및 ARC 서비스가 온라인 상태이고 사용 가능한지 확인합니다.
RORQ	아웃바운드 복제 — 대기열에 있습니다	BLDR, BARC	아웃바운드 복제 큐에는 ILM 규칙 및 클라이언트가 요청한 객체를 충족하기 위해 복제되는 객체 데이터가 포함되어 있습니다. 시스템 과부하로 인해 알람이 발생할 수 있다. 시스템 활동이 감소하면 경보가 해제되는지 확인할 때까지 기다립니다. 알람이 다시 발생하면 스토리지 노드를 추가하여 용량을 추가합니다.
SAVP	총 사용 가능한 공간(%)	LDR	사용 가능한 공간이 낮은 임계값에 도달하면 StorageGRID 시스템을 확장하거나 아카이브 노드를 통해 아카이브할 객체 데이터를 이동하는 옵션이 포함됩니다.
CA	상태	CMN	활성 그리드 작업의 상태 값이 오류인 경우 그리드 작업 메시지를 찾습니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * CMN * > * Grid Tasks * > * Overview * > * Main * 을 선택합니다. 그리드 작업 메시지는 오류에 대한 정보를 표시합니다(예: ""노드 12130011에서 검사 실패"). 문제를 조사하고 해결한 후 그리드 작업을 다시 시작합니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * CMN * > * Grid Tasks * > * Configuration * > * Main * 을 선택하고 * Actions * > * Run * 을 선택합니다. 중단 중인 그리드 작업의 상태 값이 오류인 경우 그리드 작업 중단을 다시 시도하십시오. 문제가 지속되면 기술 지원 팀에 문의하십시오.

코드	이름	서비스	권장 조치
SCEP	스토리지 API 서비스 엔드포인트 인증서 만료	CMN	스토리지 API 엔드포인트를 액세스하는 데 사용되는 인증서가 곧 만료될 때 트리거됩니다. 1. 구성 * > * 보안 * > * 인증서 * 를 선택합니다. 2. 글로벌 * 탭에서 * S3 및 Swift API 인증서 * 를 선택합니다. 3. 새 S3 및 Swift API 인증서를 업로드합니다.
SCHR	상태	CMN	내역 그리드 작업의 상태 값이 중단된 경우 이유를 조사하고 필요한 경우 작업을 다시 실행합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
SCSA	스토리지 컨트롤러 A	SSM	StorageGRID 어플라이언스에서 스토리지 컨트롤러 A에 문제가 있는 경우 알람이 트리거됩니다. 필요한 경우 구성 요소를 교체합니다.
SCSB	스토리지 컨트롤러 B	SSM	StorageGRID 어플라이언스에서 스토리지 컨트롤러 B에 문제가 있는 경우 알람이 트리거됩니다. 필요한 경우 구성 요소를 교체합니다. 일부 어플라이언스 모델에는 스토리지 컨트롤러 B가 없습니다
SHLH	상태	LDR	오브젝트 저장소의 상태 값이 오류인 경우 다음을 확인하고 수정하십시오. • 마운트하는 볼륨에 문제가 있습니다 • 파일 시스템 오류입니다
SLSA	CPU 로드 평균	SSM	값이 클수록 시스템이 더 많이 사용됩니다. CPU Load Average(CPU 로드 평균)가 높은 값으로 지속될 경우 시스템의 트랜잭션 수를 조사하여 해당 시점에 로드가 과부하인지 여부를 확인해야 합니다. CPU 로드 평균의 차트를 봅니다. * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * SSM * > * Resources * > * Reports * > * Charts * 를 선택합니다. 시스템의 로드가 무겁지 않고 문제가 지속되면 기술 지원 부서에 문의하십시오.

코드	이름	서비스	권장 조치
SMST	로그 모니터 상태	SSM	로그 모니터 상태 값이 지속적으로 연결되지 않은 경우 기술 지원 부서에 문의하십시오.
SMTT	총 이벤트	SSM	Total Events 값이 0보다 큰 경우, 원인이 될 수 있는 알려진 이벤트(예: 네트워크 장애)가 있는지 확인합니다. 이러한 오류가 지워지지 않은 경우(즉, 카운트가 0으로 재설정됨) 전체 이벤트 알람이 트리거될 수 있습니다. 문제가 해결되면 카운터를 재설정하여 경보를 지웁니다. nodes * > **site* * > **GRID node* * > * Events * > * Reset event counts * 를 선택합니다. 이벤트 수를 재설정하려면 그리드 토폴로지 페이지 구성 권한이 있어야 합니다. 총 이벤트 수가 0이거나 숫자가 증가하고 문제가 지속되면 기술 지원 팀에 문의하십시오.
SNST	상태	CMN	알람은 그리드 작업 번들을 저장하는 데 문제가 있음을 나타냅니다. Status 값이 Checkpoint Error 또는 Quorum Not reached인 경우, ADC 서비스 대부분이 StorageGRID 시스템에 연결되어 있는지 확인한 다음(50% + 1) 몇 분 정도 기다립니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
SOSS	스토리지 운영 체제 상태입니다	SSM	SANtricity 소프트웨어에서 StorageGRID 어플라이언스의 구성 요소에 ""주의 필요"" 문제가 있는 경우 알람이 트리거됩니다. 노드 * 를 선택합니다. 그런 다음 * 어플라이언스 스토리지 노드 * > * 하드웨어 * 를 선택합니다. 각 구성 요소의 상태를 보려면 아래로 스크롤합니다. SANtricity 소프트웨어에서 다른 어플라이언스 구성 요소를 확인하여 문제를 격리합니다.
SSMA	SSM 상태	SSM	SSM Status 값이 Error인 경우 * support * > * Tools * > * Grid topology * 를 선택한 후 **site* * > * *GRID node* * > * SSM * > * Overview * > * Main * 및 * SSM * > * Overview * > * Alarms * 를 선택하여 알람 원인을 파악합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.

코드	이름	서비스	권장 조치
SSME	SSM 상태	SSM	SSM 상태 값이 Standby(대기) 인 경우 모니터링을 계속하고 문제가 지속되면 기술 지원 부서에 문의하십시오. SSM State 값이 Offline 인 경우 서비스를 다시 시작한다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
SSTS	저장소 상태	흑백	스토리지 상태 값이 가용 공간이 부족하면 스토리지 노드에 사용 가능한 스토리지가 더 이상 없으며 데이터 베스트 데이터가 사용 가능한 다른 스토리지 노드로 리디렉션됩니다. 검색 요청은 이 그리드 노드에서 계속 전달될 수 있습니다. 추가 스토리지를 추가해야 합니다. 최종 사용자 기능에는 영향을 미치지 않지만 추가 스토리지가 추가될 때까지 경보가 지속됩니다. 저장소 상태 값이 볼륨을 사용할 수 없는 경우 저장소 일부를 사용할 수 없습니다. 이러한 볼륨에서의 저장 및 검색은 불가능합니다. 자세한 내용은 볼륨 상태를 확인하십시오. * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택하십시오. 그런 다음 **site* * > **GRID node* * > * LDR * > * Storage * > * Overview * > * Main * 을 선택합니다. 볼륨의 상태는 오브젝트 저장소 아래에 나열됩니다. 스토리지 상태 값이 오류 인 경우 기술 지원 부서에 문의하십시오. SSTS(Storage Status) 경보 문제를 해결합니다

코드	이름	서비스	권장 조치
SVST	상태	SSM	이 알람은 실행되지 않는 서비스와 관련된 다른 알람이 해결되면 해제됩니다. 소스 서비스 경보를 추적하여 작업을 복구합니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * SSM * > * Services * > * Overview * > * Main * 을 선택합니다. 서비스 상태가 Not Running 으로 표시되면 서비스 상태가 Administratively Down 으로 표시됩니다. 서비스 상태는 다음과 같은 이유로 Not Running(실행되지 않음) 으로 표시될 수 있습니다. • 서비스가 수동으로 중지되었습니다('/etc/init.d/<service\> stop'). • MySQL 데이터베이스에 문제가 있으며 Server Manager가 MI 서비스를 종료합니다. • 그리드 노드가 추가되었지만 시작되지 않았습니다. • 설치 중에 그리드 노드가 아직 관리 노드에 연결되지 않았습니다. 서비스가 실행 중이 아닌 것으로 표시되면 서비스를 다시 시작합니다('/etc/init.d/<service\> restart'). 이 경보는 또한 스토리지 노드의 메타데이터 저장소(Cassandra 데이터베이스)를 재구축해야 함을 나타낼 수 있습니다. 문제가 지속되면 기술 지원 팀에 문의하십시오. 서비스: 상태 - Cassandra(SVST) 알람 문제를 해결합니다
TMEM	메모리를 설치했습니다	SSM	설치된 메모리 용량이 24GiB 미만인 노드를 실행하면 성능 문제와 시스템 불안정으로 이어질 수 있습니다. 시스템에 설치된 메모리 양을 24GiB 이상으로 늘려야 합니다.
TPOP	보류 중인 작업	ADC	메시지 큐는 ADC 서비스가 과부하되었음을 나타낼 수 있습니다. StorageGRID 시스템에 연결할 수 있는 ADC 서비스가 너무 적습니다. 대규모 배포에서는 ADC 서비스에 컴퓨팅 리소스를 추가해야 하거나 시스템에 추가 ADC 서비스가 필요할 수 있습니다.
메모리	사용 가능한 메모리	SSM	사용 가능한 RAM이 부족한 경우 이것이 하드웨어 문제인지 소프트웨어 문제인지 확인합니다. 하드웨어 문제가 아니거나 사용 가능한 메모리가 50MB(기본 알람 임계값) 미만인 경우 기술 지원 부서에 문의하십시오.

코드	이름	서비스	권장 조치
VMFI	사용 가능한 항목	SSM	이는 추가 보관이 필요함을 나타냅니다. 기술 지원 부서에 문의하십시오.
VMFR	사용 가능한 공간	SSM	사용 가능한 공간 값이 너무 낮으면(알람 임계값 참조), 로그 파일의 비율이 초과되었는지 또는 디스크 공간이 너무 많은 개체(알람 임계값 참조)를 축소 또는 삭제해야 하는지 여부를 조사해야 합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.
VMST	상태	SSM	마운트된 볼륨의 상태 값이 알 수 없는 경우 알람이 트리거됩니다. Unknown 또는 Offline 값은 기본 스토리지 디바이스의 문제로 인해 볼륨을 마운트하거나 액세스할 수 없음을 나타낼 수 있습니다.
VPRI	검증 우선 순위	BLDR, BARC	기본적으로 검증 우선 순위 값은 적응 입니다. Verification Priority(확인 우선 순위)가 High(높음)로 설정된 경우, 스토리지 확인 시 서비스의 정상적인 작동이 느려질 수 있기 때문에 알람이 트리거됩니다.
VSTU	개체 검증 상태	흑백	지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **site* * > **GRID node* * > * LDR * > * Storage * > * Overview * > * Main * 을 선택합니다. 운영 체제에서 블록 장치 또는 파일 시스템 오류의 징후를 확인합니다. 개체 검증 상태 값이 알 수 없는 오류인 경우 일반적으로 저장소 확인 작업이 저장된 콘텐츠에 액세스하지 못하게 하는 낮은 수준의 파일 시스템 또는 하드웨어 문제(I/O 오류)를 나타냅니다. 기술 지원 부서에 문의하십시오.
XMS	연결할 수 없는 감사 저장소	BDC, BARC, BCLB, BCMN, BLDR, BNMS	관리 노드를 호스팅하는 서버에 대한 네트워크 연결을 확인합니다. 문제가 지속되면 기술 지원 팀에 문의하십시오.

SNMP 알림을 생성하는 알람**(**레거시 시스템**)**

다음 표에는 SNMP 알림을 생성하는 기존 경보가 나열되어 있습니다. 경고와 달리 모든 알람에서 SNMP 알림이 생성되는 것은 아닙니다. 나열된 알람만 SNMP 알림을 생성하고, 표시된 심각도 이상에서만 알림을 생성합니다.

기존 알람 시스템은 계속 지원되지만, 알림 시스템은 상당한 이점을 제공하며 사용이 간편합니다.

코드	이름	심각도입니다
ACMS	사용 가능한 메타데이터 서비스	심각
아ITE	상태 검색	경미합니다
AITU	상태 검색	전공
AMQS	감사 메시지가 대기 중입니다	주의
AOTE	Store State(상태 저장)	경미합니다
AOTU	저장 상태	전공
AROQ	개체가 대기 중입니다	경미합니다
ARRF	요청 실패	전공
ARRV	확인 실패	전공
ARVF	저장 실패	전공
ASXP	공유 감사	경미합니다
8월	AMS 상태	경미합니다
AUXS	감사 내보내기 상태	경미합니다
BTOF	오프셋	주의
CAHP	Java 힙 사용량 백분율	전공
캐나다	사용 가능한 대상 수	주의
카사	데이터 저장소 상태	전공
CDLP	사용된 메타데이터 공간(퍼센트)	전공
CLBE	CLB 상태	심각
NST	DNS 상태	심각
ECST	확인 상태	전공

코드	이름	심각도입니다
HSTE	HTTP 상태	전공
HTAS	HTTP를 자동으로 시작합니다	주의
분실	손실된 개체	전공
마인큐	이메일 알림 대기 중	주의
분	이메일 알림 상태	경미합니다
Nang	네트워크 자동 협상 설정	주의
NDUP	네트워크 이중 모드 설정	경미합니다
NLNK	네트워크 링크 감지	경미합니다
NRER	수신 오류	주의
NSPD	속도	주의
네터	전송 오류	주의
NTFQ	NTP 주파수 오프셋	경미합니다
NTLK	NTP 잠금	경미합니다
NTOF	NTP 시간 오프셋	경미합니다
NTSJ	선택한 시간 소스 지터	경미합니다
NTSU	NTP 상태	전공
OPST	전체 전원 상태	전공
ORSU	아웃바운드 복제 상태입니다	주의
PSA	전원 공급 장치 A 상태	전공
PSBS	전원 공급 장치 B 상태	전공
RDTE	Tivoli Storage Manager 상태입니다	주의

코드	이름	심각도입니다
RDTU	Tivoli Storage Manager 상태입니다	전공
SAVP	총 사용 가능한 공간(%)	주의
SHLH	상태	주의
SLSA	CPU 로드 평균	주의
SMTT	총 이벤트	주의
SNST	상태	
SOSS	스토리지 운영 체제 상태입니다	주의
SSTS	저장소 상태	주의
SVST	상태	주의
TMEM	메모리를 설치했습니다	경미합니다
메모리	사용 가능한 메모리	경미합니다
VMST	상태	경미합니다
VPRI	검증 우선 순위	주의
VSTU	개체 검증 상태	주의

로그 파일 참조

StorageGRID는 이벤트, 진단 메시지 및 오류 상태를 캡처하는 데 사용되는 로그를 제공합니다. 문제 해결을 지원하기 위해 로그 파일을 수집하여 기술 지원 부서에 전달하라는 요청을 받을 수 있습니다.

로그는 다음과 같이 분류됩니다.

- StorageGRID 소프트웨어 로그
- 배포 및 유지 관리 로그
- 타사 소프트웨어에 대한 로그입니다
- bycast.log 정보

각 로그 유형에 대해 제공되는 세부 정보는 참조용으로만 제공됩니다. 로그는 기술 지원 부서에서 제공하는 고급 문제 해결을 위한 것입니다. 감사 로그 및 응용 프로그램 로그 파일을 사용하여 문제 기록을 재구성하는 고급 기술은 이 지침의 범위를 벗어납니다.

로그에 액세스하려면 하나 이상의 노드에서 로그 파일 및 시스템 데이터를 단일 로그 파일 아카이브로 수집할 수 있습니다(* 지원 * > * 도구 * > * 로그 *). 또는 운영 관리 노드를 사용할 수 없거나 특정 노드에 연결할 수 없는 경우 다음과 같이 각 그리드 노드에 대한 개별 로그 파일에 액세스할 수 있습니다.

1. ssh admin@grid_node_ip' 명령을 입력한다
2. "passwords.txt" 파일에 나열된 암호를 입력합니다.
3. 루트로 전환하려면 다음 명령을 입력합니다
4. "passwords.txt" 파일에 나열된 암호를 입력합니다.

StorageGRID 로그 파일 아카이브에는 각 범주에 대해 설명된 로그와 메트릭 및 디버그 명령 출력이 포함된 추가 파일이 포함됩니다.

보관 위치	설명
감사	정상적인 시스템 작동 중에 생성된 감사 메시지입니다.
기본 OS 로그	StorageGRID 이미지 버전을 포함한 기본 운영 체제 정보
번들	글로벌 구성 정보(번들)
Cassandra 를 클릭합니다	Cassandra 데이터베이스 정보 및 리퍼 복구 로그.
EC	현재 노드에 대한 VCSs 정보 및 프로필 ID별 EC 그룹 정보
그리드	디버그(bycast.log)와 스베르매니저 로그를 포함한 일반 그리드 로그입니다.
grid.xml	모든 노드에서 공유되는 그리드 구성 파일입니다.
해그루	고가용성 그룹 메트릭 및 로그
설치합니다	'두서버' 및 설치 로그.
lumberjack.log	로그 수집과 관련된 디버그 메시지입니다.
람다 - 중재인	S3 Select 프록시 요청과 관련된 로그입니다.
메트릭	Grafana, Jaeger, 노드 수출자 및 Prometheus에 대한 서비스 로그.
오류	Miscd 액세스 및 오류 로그.

보관 위치	설명
MySQL	MariaDB 데이터베이스 구성 및 관련 로그.
결과	네트워킹 관련 스크립트 및 Dynip 서비스에서 생성된 로그입니다.
Nginx	부하 분산 장치 구성 파일 및 로그 그리드 관리자 및 테넌트 관리자 트래픽 로그도 포함됩니다.
Nginx-GW	부하 분산 장치 구성 파일 및 로그
NTP	NTP 구성 파일 및 로그
OS	서비스 PID를 포함한 노드 및 그리드 상태 파일
기타	다른 폴더에 수집되지 않은 '/var/local/log' 아래의 로그 파일.
성능	CPU, 네트워킹 및 디스크 I/O에 대한 성능 정보
Prometheus - 데이터	로그 컬렉션에 Prometheus 데이터가 포함된 경우 현재 Prometheus 메트릭입니다.
프로비저닝	그리드 프로비저닝 프로세스와 관련된 로그입니다.
래프트	플랫폼 서비스에 사용되는 RAFT 클러스터의 로그입니다.
SNMP를 선택합니다	SNMP 에이전트 구성 및 알람 허용/거부 목록은 SNMP 알림을 보내는 데 사용됩니다.
소켓 - 데이터	네트워크 디버그용 소켓 데이터
system-commands.txt	StorageGRID 컨테이너 명령의 출력 네트워킹 및 디스크 사용과 같은 시스템 정보를 포함합니다.

관련 정보

로그 파일 및 시스템 데이터를 수집합니다

StorageGRID 소프트웨어 로그

StorageGRID 로그를 사용하여 문제를 해결할 수 있습니다.

로그를 외부 syslog 서버로 전송하거나 'bycast.log', 'NMS.log' 등의 감사 정보 대상을 변경하려면 를 참조하십시오 감사 메시지 및 로그 대상을 구성합니다.

일반 **StorageGRID** 로그

파일 이름입니다	참고	에 있습니다
'/var/local/log/bycast.log'	기본 StorageGRID 문제 해결 파일입니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **Site* * > **Node* * > * SSM * > * Events * 를 선택합니다.	모든 노드
'/var/local/log/bycast-err.log'	bycast.log의 하위 집합(severity error 및 critical 메시지)이 포함되어 있습니다. 중요 메시지도 시스템에 표시됩니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 **Site* * > **Node* * > * SSM * > * Events * 를 선택합니다.	모든 노드
'/var/local/core/'	프로그램이 비정상적으로 종료될 경우 생성된 코어 덤프 파일이 포함되어 있습니다. 가능한 원인으로는 어설션 실패, 위반 또는 스레드 시간 초과가 있습니다. 일반적으로 어플라이언스 노드에 "/var/local/core/kexec_cmd' 파일이 있으며 오류를 나타내지 않습니다.	모든 노드

서버 관리자 로그

파일 이름입니다	참고	에 있습니다
'/var/local/log/ServerManager.log'	서버에서 실행 중인 Server Manager 응용 프로그램의 로그 파일입니다.	모든 노드
'/var/local/log/GridstatBackend.errlog'	Server Manager GUI 백엔드 애플리케이션에 대한 로그 파일입니다.	모든 노드
'/var/local/log/gridstat.errlog'	서버 관리자 GUI에 대한 로그 파일입니다.	모든 노드

StorageGRID 서비스에 대한 로그입니다

파일 이름입니다	참고	에 있습니다
'/var/local/log/acct.errlog'		ADC 서비스를 실행하는 스토리지 노드

파일 이름입니다	참고	에 있습니다
'/var/local/log/ADC.errlog'	해당 서비스의 표준 오류(stderr) 스트림을 포함합니다. 서비스당 하나의 로그 파일이 있습니다. 서비스에 문제가 없는 경우 이러한 파일은 일반적으로 비어 있습니다.	ADC 서비스를 실행하는 스토리지 노드
'/var/local/log/AMS.errlog'		관리자 노드
'/var/local/log/arc.errlog'		아카이브 노드
'/var/local/log/cassandra/system.log'	새 스토리지 노드를 추가할 때 문제가 발생하거나 작업 중단 시 사용할 수 있는 메타데이터 저장소(Cassandra 데이터베이스)에 대한 정보입니다.	스토리지 노드
'/var/local/log/cassandra-reaper.log'	Cassandra Reaper 서비스: Cassandra 데이터베이스 데이터의 복구를 수행합니다.	스토리지 노드
'/var/local/log/cassandra-reaper.errlog'	Cassandra Refaper 서비스에 대한 오류 정보입니다.	스토리지 노드
'/var/local/log/chunk.errlog'		스토리지 노드
'/var/local/log/clb.errlog'	CLB 서비스에 대한 오류 정보 • 참고: * CLB 서비스는 더 이상 사용되지 않습니다.	게이트웨이 노드
'/var/local/log/CMN.errlog'		관리자 노드
'/var/local/log/CMS.errlog'	이 로그 파일은 이전 버전의 StorageGRID에서 업그레이드된 시스템에 있을 수 있습니다. 기존 정보가 포함되어 있습니다.	스토리지 노드
'/var/local/log/cts.errlog'	이 로그 파일은 타겟 유형이 * Cloud Tiering - Simple Storage Service(S3) * 인 경우에만 생성됩니다	아카이브 노드
'/var/local/log/dS.errlog'		스토리지 노드
'/var/local/log/DMV.errlog'		스토리지 노드

파일 이름입니다	참고	에 있습니다
'/var/local/log/dynip * '	동적 IP 변경을 위해 그리드를 모니터링하고 로컬 구성을 업데이트하는 dynip 서비스와 관련된 로그를 포함합니다.	모든 노드
'/var/local/log/fraftana.log'	Grafana 서비스와 연관된 로그로, Grid Manager에서 메트릭 시각화에 사용됩니다.	관리자 노드
'/var/local/log/hagroups.log'	고가용성 그룹과 연결된 로그입니다.	관리 노드 및 게이트웨이 노드
'/var/local/log/hagroups_events.log'	백업에서 마스터로 전환 또는 오류와 같은 상태 변경을 추적합니다.	관리 노드 및 게이트웨이 노드
'/var/local/log/idnt.errlog'		ADC 서비스를 실행하는 스토리지 노드
'/var/local/log/Jaeger.log'	추적 수집에 사용되는 Jaeger 서비스와 연관된 로그입니다.	모든 노드
'/var/local/log/kstn.errlog'		ADC 서비스를 실행하는 스토리지 노드
'/var/local/log/lambda * '	S3 Select 서비스에 대한 로그를 포함합니다.	관리자 및 게이트웨이 노드 특정 관리자 및 게이트웨이 노드에만 이 로그가 포함됩니다. 를 참조하십시오 S3 관리자 및 게이트웨이 노드에 대한 요구 사항 및 제한 사항을 선택합니다.
'/var/local/log/LDR.errlog'		스토리지 노드
'/var/local/log/miscd/ *.log'	MISCd 서비스(정보 서비스 제어 데몬)에 대한 로그를 포함합니다. 이 로그는 다른 노드의 서비스를 쿼리 및 관리하고 다른 노드에서 실행 중인 서비스 상태를 쿼리하는 등 노드의 환경 구성을 관리하는 인터페이스를 제공합니다.	모든 노드

파일 이름입니다	참고	에 있습니다
'/var/local/log/nginx/ *.log'	HTTPS API를 통해 다른 노드의 서비스와 통신할 수 있도록 다양한 그리드 서비스(예: Prometheus 및 Dynip)에 대한 인증 및 보안 통신 메커니즘 역할을 하는 nginx 서비스에 대한 로그를 포함합니다.	모든 노드
'/var/local/log/nginx-GW/ *.log'	관리 노드의 제한된 관리 포트 및 클라이언트에서 스토리지 노드로의 S3 및 Swift 트래픽의 로드 밸런싱을 제공하는 로드 밸런서 서비스에 대한 로그가 포함됩니다.	관리 노드 및 게이트웨이 노드
'/var/local/log/persistence *'	재부팅 시 유지되어야 하는 루트 디스크의 파일을 관리하는 Persistence 서비스에 대한 로그를 포함합니다.	모든 노드
'/var/local/log/Prometheus.log'	모든 노드에 대해 노드 수출자 서비스 로그 및 ade-Exporter 메트릭 서비스 로그를 포함합니다. 관리 노드의 경우 Prometheus 및 Alert Manager 서비스에 대한 로그도 포함됩니다.	모든 노드
'/var/local/log/raft.log'입니다	RAFT 프로토콜에 대해 RSM 서비스에서 사용하는 라이브러리의 출력을 포함합니다.	RSM 서비스가 있는 스토리지 노드
'/var/local/log/rms.errlog'	S3 플랫폼 서비스에 사용되는 RSM(Replicated State Machine Service) 서비스에 대한 로그를 포함합니다.	RSM 서비스가 있는 스토리지 노드
'/var/local/log/ssm.errlog'		모든 노드
'/var/local/log/update-s3vs-domain.log'	S3 가상 호스팅 도메인 이름 구성에 대한 업데이트 처리 관련 로그가 들어 있습니다. S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.	관리자 및 게이트웨이 노드
'/var/local/log/update-snmp-firewall. *	SNMP를 위해 관리되는 방화벽 포트와 관련된 로그를 포함합니다.	모든 노드
'/var/local/log/update-sysll.log'	시스템 syslog 구성에 대한 변경 사항과 관련된 로그를 포함합니다.	모든 노드

파일 이름입니다	참고	에 있습니다
'/var/local/log/update-traffic-classes.log'	트래픽 분류자 구성 변경과 관련된 로그를 포함합니다.	관리자 및 게이트웨이 노드
'/var/local/log/update-utcn.log'	이 노드의 신뢰할 수 없는 클라이언트 네트워크 모드와 관련된 로그를 포함합니다.	모든 노드

NMS 로그

파일 이름입니다	참고	에 있습니다
'/var/local/log/NMS.log'	• Grid Manager 및 테넌트 관리자의 알림을 캡처합니다. • 알람 처리, e-메일 알림, 구성 변경 등 NMS 서비스 작업과 관련된 이벤트를 캡처합니다. • 시스템에서 변경한 구성 변경으로 인한 XML 번들 업데이트를 포함합니다. • 하루에 한 번 수행된 속성 다운샘플링과 관련된 오류 메시지가 포함되어 있습니다. • Java 웹 서버 오류 메시지(예: 페이지 생성 오류 및 HTTP 상태 500 오류)가 포함되어 있습니다.	관리자 노드
'/var/local/log/NMS.errlog'	MySQL 데이터베이스 업그레이드와 관련된 오류 메시지가 포함되어 있습니다. 해당 서비스의 표준 오류(stderr) 스트림을 포함합니다. 서비스당 하나의 로그 파일이 있습니다. 서비스에 문제가 없는 경우 이러한 파일은 일반적으로 비어 있습니다.	관리자 노드
'/var/local/log/NMS.requestlog'입니다	관리 API에서 내부 StorageGRID 서비스로 나가는 연결에 대한 정보를 포함합니다.	관리자 노드

관련 정보

bycast.log 정보

S3을 사용합니다

배포 및 유지 관리 로그

배포 및 유지 관리 로그를 사용하여 문제를 해결할 수 있습니다.

파일 이름입니다	참고	에 있습니다
'/var/local/log/install.log'입니다	소프트웨어 설치 중에 생성됩니다. 설치 이벤트 기록을 포함합니다.	모든 노드
'/var/local/log/expansion-progress.log'	확장 작업 중에 생성됩니다. 확장 이벤트의 레코드를 포함합니다.	스토리지 노드
'/var/local/log/gdu-server.log'	GDU 서비스에 의해 생성됩니다. 기본 관리 노드에서 관리하는 프로비저닝 및 유지 보수 절차와 관련된 이벤트를 포함합니다.	기본 관리자 노드
'/var/local/log/send_admin_hw.log'	설치 중에 생성됩니다. 기본 관리 노드와의 노드 통신과 관련된 디버깅 정보를 포함합니다.	모든 노드
'/var/local/log/upgrade.log'	소프트웨어 업그레이드 중에 생성됩니다. 소프트웨어 업데이트 이벤트 기록을 포함합니다.	모든 노드

타사 소프트웨어에 대한 로그입니다

타사 소프트웨어 로그를 사용하여 문제를 해결할 수 있습니다.

범주	파일 이름입니다	참고	에 있습니다
아카이빙	/var/local/log/dsierror.log 를 참조하십시오	TSM 클라이언트 API에 대한 오류 정보입니다.	아카이브 노드
MySQL	/var/local/log/mysql.err/var/local/log/mysql-slow.log	MySQL에서 생성된 로그 파일. mysql.err 파일은 데이터베이스 오류와 시작 및 종료 등의 이벤트를 캡처합니다. mysql-slow.log 파일(slow query log)은 실행에 10초 이상 걸린 SQL 문을 캡처합니다.	관리자 노드
운영 체제	/var/local/log/messages입니다	이 디렉토리에는 운영 체제에 대한 로그 파일이 포함되어 있습니다. 이러한 로그에 포함된 오류도 그리드 관리자에 표시됩니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 * Topology * > **Site* * > **Node* * > * SSM * > * Events * 를 선택합니다.	모든 노드

범주	파일 이름입니다	참고	에 있습니다
NTP	/var/local/log/ntp.log /var/lib/ntp/var/log/ntpstats/	'/var/local/log/ntp.log'에는 NTP 오류 메시지에 대한 로그 파일이 포함되어 있습니다. '/var/lib/ntp/var/log/ntpstats/' 디렉토리에는 NTP 타이밍 통계가 포함됩니다. 'loostats'는 루프 필터 통계 정보를 기록합니다. 피에르통계(peerstats)는 피어 통계 정보를 기록합니다.	모든 노드
삼바	/var/local/log/samba/	Samba 로그 디렉토리에는 각 Samba 프로세스(SMB, NMB 및 winbind)와 모든 클라이언트 호스트 이름/IP에 대한 로그 파일이 포함됩니다.	관리자 노드가 CIFS를 통해 감사 공유를 내보내도록 구성되었습니다

bycast.log 정보

파일 '/var/local/log/bycast.log'는 StorageGRID 소프트웨어의 주요 문제 해결 파일입니다. 모든 그리드 노드에 대한 bycast.log 파일이 있다. 이 파일에는 해당 그리드 노드와 관련된 메시지가 들어 있습니다.

'/var/local/log/bycast-err.log' 파일은 bycast.log의 하위 집합입니다. 여기에는 심각도 오류 메시지와 중요 메시지가 포함됩니다.

선택적으로 감사 로그의 대상을 변경하고 감사 정보를 외부 syslog 서버로 보낼 수 있습니다. 외부 syslog 서버가 구성되면 감사 레코드의 로컬 로그가 계속 생성되고 저장됩니다. 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다.

bycast.log 파일 회전

bycast.log 파일이 1GB에 도달하면 기존 파일이 저장되고 새 로그 파일이 시작됩니다.

저장된 파일의 이름이 bycast.log.1로 바뀌고 새 파일의 이름이 bycast.log로 지정됩니다. 새로운 bycast.log가 1GB에 도달하면 bycast.log.1이 이름이 바뀌어 bycast.log.2.gz가 되고 bycast.log.1로 이름이 변경됩니다.

bycast.log의 회전 제한은 21개 파일입니다. bycast.log의 22버전을 만들면 가장 오래된 파일이 삭제됩니다.

bycast-err.log의 회전 제한은 7개 파일입니다.

> 로그 파일이 압축되어 있는 경우 로그 파일이 기록된 동일한 위치에 압축을 풀면 안 됩니다. 같은 위치로 파일 압축을 해제하면 로그 회전 스크립트가 방해를 받을 수 있습니다.

선택적으로 감사 로그의 대상을 변경하고 감사 정보를 외부 syslog 서버로 보낼 수 있습니다. 외부 syslog 서버가 구성되면 감사 레코드의 로컬 로그가 계속 생성되고 저장됩니다. 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다.

관련 정보

bycast.log 의 메시지

bycast.log의 메시지는 ADE(Asynchronous Distributed Environment)에서 작성한다. ade는 각 그리드 노드의 서비스에서 사용되는 런타임 환경입니다.

ADE 메시지 예:

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

ade 메시지에는 다음 정보가 포함됩니다.

메시지 세그먼트	예제 값
노드 ID입니다	12455685
ade 프로세스 ID	0357819531
모듈 이름입니다	SVM
메시지 식별자입니다	EVHR
UTC 시스템 시간입니다	2019-05-05T27T17:10:29.784677(YYYY-MM-DDTHH:MM:SS.uuuuuu)
심각도 수준	오류
내부 추적 번호	0906
메시지	SVMR: 볼륨 3에 대한 상태 점검에 'Tout' 이유가 있습니다.

bycast.log 의 메시지 심각도

bycast.log의 메시지는 심각도 수준이 할당됩니다.

예를 들면 다음과 같습니다.

- * 공지 * — 기록해야 하는 이벤트가 발생했습니다. 대부분의 로그 메시지는 이 수준에 있습니다.
- * 경고 * — 예상치 못한 조건이 발생했습니다.
- * 오류 * — 작업에 영향을 주는 중대한 오류가 발생했습니다.
- * 심각 * — 정상 작동을 멈춘 비정상적인 조건이 발생했습니다. 기저 질환을 즉시 해결해야 합니다. 중요 메시지는 그리드 관리자에도 표시됩니다. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 * 사이트 * > * 노드 * > * SSM * > * 이벤트 * 를 선택합니다.

에 오류 코드가 있습니다 `bycast.log`

bycast.log의 대부분의 오류 메시지에 오류 코드가 포함되어 있습니다.

다음 표는 bycast.log의 일반적인 비숫자 코드를 열거합니다. 숫자가 아닌 코드의 정확한 의미는 보고되는 컨텍스트에 따라 달라집니다.

오류 코드	의미
SUCS	오류가 없습니다
GERR	알 수 없음
CANC	취소됨
ABRT	중단되었습니다
출력	시간 초과
송장	유효하지 않습니다
NFND	찾을 수 없습니다
서버	버전
구성	구성
실패	실패했습니다
ICPL	완료되지 않았습니다
완료	완료
SUNV	서비스를 사용할 수 없습니다

다음 표에는 bycast.log의 숫자 오류 코드가 나와 있습니다.

오류 번호	오류 코드	의미
001	EPERM	작업이 허용되지 않습니다
002	이비인후과	해당 파일 또는 디렉토리가 없습니다
003	ESRCH	그러한 프로세스가 없습니다

오류 번호	오류 코드	의미
004	EINTR	시스템 호출이 중단되었습니다
005	EIO	I/O 오류
006	ENXIO	해당 장치 또는 주소가 없습니다
007	E2BIG	인수 목록이 너무 깁니다
008	ENOEXEC	exec 형식 오류입니다
009	EBADF	파일 번호가 잘못되었습니다
010	ECHILD	하위 프로세스가 없습니다
011	EAGAIN	다시 시도하십시오
012	ENOMEM	메모리가 부족합니다
013	EACCES를 참조하십시오	권한이 거부되었습니다
014	기본값	주소가 잘못되었습니다
015	ENOTBLK	블록 장치가 필요합니다
016	EBUSY(확장	장치 또는 리소스가 사용 중입니다
017	EEXIST	파일이 있습니다
018	예	장치 간 링크
019	ENODEV	해당 장치가 없습니다
020	ENOTDIR	디렉토리가 아닙니다
021	EISDIR	는 디렉토리입니다
022	EINVAL	인수가 잘못되었습니다
023	ENFILE	파일 테이블 오버플로
024	EMFILE	열려 있는 파일이 너무 많습니다

오류 번호	오류 코드	의미
025	ENOTTY	타자가 아닙니다
026	ETXTBSY	텍스트 파일이 사용 중입니다
027	EFBIG	파일이 너무 큽니다
028	ENOSPC	장치에 남은 공간이 없습니다
029)를 참조하십시오	ESPIPE	잘못된 탐색
030	EROFS	읽기 전용 파일 시스템입니다
031	EMLINK	링크가 너무 많습니다
032	EPIPE	파이프 파손
033	에돔	함수 도메인에서 수학 인수를 제외합니다
034	ERANGE	수학 결과를 표현할 수 없습니다
035	EDEADLK	리소스 교착 상태가 발생합니다
036	ENAMETOOLING	파일 이름이 너무 깁니다
037	ENOLCK	사용 가능한 레코드 잠금이 없습니다
038	ENOSYS	기능이 구현되지 않았습니다
039	ENOTEMPTY	디렉토리가 비어 있지 않습니다
040	ELOOP	너무 많은 심볼 링크가 발견되었습니다
041		
042	ENOMSG	원하는 유형의 메시지가 없습니다
043	EIDRM	식별자가 제거되었습니다
044	ECHRNG	채널 번호가 범위를 벗어났습니다

오류 번호	오류 코드	의미
045	EL2NSYNC	레벨 2가 동기화되지 않았습니다
046	EL3HLT	레벨 3이 정지되었습니다
047	EL3RST	레벨 3 재설정
048	ELNNG	링크 번호가 범위를 벗어났습니다
049	EUNATCH	프로토콜 드라이버가 연결되지 않았습니다
050	ENOCSI	사용 가능한 CSI 구조가 없습니다
051	EL2HLT	레벨 2가 정지되었습니다
052	EBADE	잘못된 교환입니다
053)를 참조하십시오	EBADR	요청 설명자가 잘못되었습니다
054)를 참조하십시오	엑블	Exchange가 가득 찼습니다
055	에노ANO	양극 없음
056)를 참조하십시오	EBADRQC	잘못된 요청 코드입니다
057)를 참조하십시오	EBADDSLT	슬롯이 잘못되었습니다
058		
059	EBFONT(2박	잘못된 글꼴 파일 형식입니다
060	ENOSTR	장치가 스트림이 아닙니다
061	데이터	사용 가능한 데이터가 없습니다
062	eTIME	타이머가 만료되었습니다
063	ENOSR	스트림 리소스가 없습니다

오류 번호	오류 코드	의미
064	ENONET	컴퓨터가 네트워크에 없습니다
065	ENOPKG	패키지가 설치되지 않았습니다
066	EREMOTE	객체가 원격입니다
067	ENOLINK	링크가 분리되었습니다
068)을 참조하십시오	EADV	오류 알림
069)를 참조하십시오	ESRMNT	Srmount 오류입니다
070	eComm	전송 시 통신 오류가 발생했습니다
071	EPROTO(EPROTO	프로토콜 오류입니다
072	EMULTIHOP	멀티홉을 시도했습니다
073	EDOTDOT	RFS 특정 오류입니다
074	EBADMSG	데이터 메시지가 아닙니다
075	EOVERFLOW	값이 정의된 데이터 형식에 비해 너무 큽니다
076	ENOTUNIQ	이름이 네트워크에서 고유하지 않습니다
077	EBADFD	파일 설명자가 잘못된 상태입니다
078)을 참조하십시오	EREMCHG	원격 주소가 변경되었습니다
079	ElibACC	필요한 공유 라이브러리에 액세스할 수 없습니다
080	온라인 서비스	손상된 공유 라이브러리에 액세스 중입니다
081	엘리브SCN	
082를 참조하십시오	엘리브맥스	너무 많은 공유 라이브러리에서 연결을 시도하는 중입니다

오류 번호	오류 코드	의미
083	ELIBEXEC	공유 라이브러리를 직접 실행할 수 없습니다
084	에일세큐	잘못된 바이트 시퀀스입니다
085	ERESTART	중단된 시스템 통화를 다시 시작해야 합니다
086	테스트 IPE	스트림 파이프 오류입니다
087	EUSERS	사용자가 너무 많습니다
088	ENOTSOCK	비소켓에서 소켓 작동
089)를 참조하십시오	EDESTADDREQ	대상 주소가 필요합니다
090	EMSGSIZE	메시지가 너무 깁니다
091	EPROTOTYPE	소켓 프로토콜 유형이 잘못되었습니다
092)를 참조하십시오	ENOPROTOOPT	프로토콜을 사용할 수 없습니다
093)를 참조하십시오	EPROTONOSUPPORT를 참조하십시오	지원되지 않는 프로토콜입니다
094를 참조하십시오	ESOCKTNOSUPPORT	지원되지 않는 소켓 유형입니다
095	EOPNOTSUPP	전송 엔드포인트에서 지원되지 않는 작업입니다
096를 참조하십시오	EPFNOSUPPORT	프로토콜 제품군이 지원되지 않습니다
097	EAFNOSUPPORT를 참조하십시오	프로토콜에서 지원되지 않는 주소 제품군입니다
098	EADDRINUSE	이미 사용 중인 주소입니다
099	EADDRNOTAVAIL	요청된 주소를 할당할 수 없습니다
100	ENETDOWN	네트워크가 다운되었습니다
101	ENETUNREACH를 참조하십시오	네트워크에 연결할 수 없습니다

오류 번호	오류 코드	의미
102	네테세트	재설정으로 인해 네트워크 연결이 끊어졌습니다
103	연결\nECONNABORTED	소프트웨어에서 연결이 중단되었습니다
104	ECONNRESET	피어에 의해 연결이 재설정되었습니다
105	ENOBUFS	사용 가능한 버퍼 공간이 없습니다
106	EISCONN	전송 엔드포인트가 이미 연결되어 있습니다
107	ENOTCONN	전송 엔드포인트가 연결되지 않았습니다
108	ESHUTDOWN	전송 엔드포인트 종료 후 전송할 수 없습니다
109	이토마이닉스	참조가 너무 많습니다: 연결할 수 없습니다
110	이테크진	연결 시간이 초과되었습니다
111	ECONNEREFUSED	연결이 거부되었습니다
112	EHOSTDOWN	호스트가 다운되었습니다
113	EHOSTUNREACH를 선택합니다	호스트에 대한 경로가 없습니다
114	EALREADY	작업이 이미 진행 중입니다
115	설치	작업이 진행 중입니다
116		
117	유럽 연합	구조를 청소해야 합니다
118	ENOTAM	XENIX 명명된 형식 파일이 아닙니다
119	에나비IL	XENIX 세마포는 사용할 수 없습니다
120	EISNAM	명명된 형식 파일입니다
121	EREMOTEIO	원격 I/O 오류입니다
122	EDQUOT	할당량이 초과되었습니다

오류 번호	오류 코드	의미
123을 선택합니다	ENOMEDIUM	미디어를 찾을 수 없습니다
124를 참조하십시오	EMEDIUMTYPE	잘못된 매체 유형입니다
125	ECANCELED	작업이 취소되었습니다
126을 참조하십시오	ENOKEY	필수 키를 사용할 수 없습니다
127로 표시됩니다	에케예피레드	키가 만료되었습니다
128	EKEYREVOKED	키가 취소되었습니다
129	EKEYREJECTED	서비스가 키를 거부했습니다
130	EOWNERDEAD	확실한 돌연변이: 주인이 죽었다
131	복구불가	강력한 뮤텍스의 경우: 상태를 복구할 수 없습니다

그리드를 확장합니다

그리드 확장: 개요

다음 지침을 사용하여 시스템 운영을 중단하지 않고 StorageGRID 시스템의 용량 또는 기능을 확장할 수 있습니다.

참조하십시오

다음 지침은 스토리지 노드에 스토리지 볼륨을 추가하기 위해 StorageGRID 확장을 수행하는 방법, 기존 사이트에 새 그리드 노드 또는 전체 새 사이트에 대해 설명합니다.

이 지침은 StorageGRID 시스템을 설치한 후 구성 및 지원하는 기술 담당자를 위한 것입니다.

확장 절차 개요

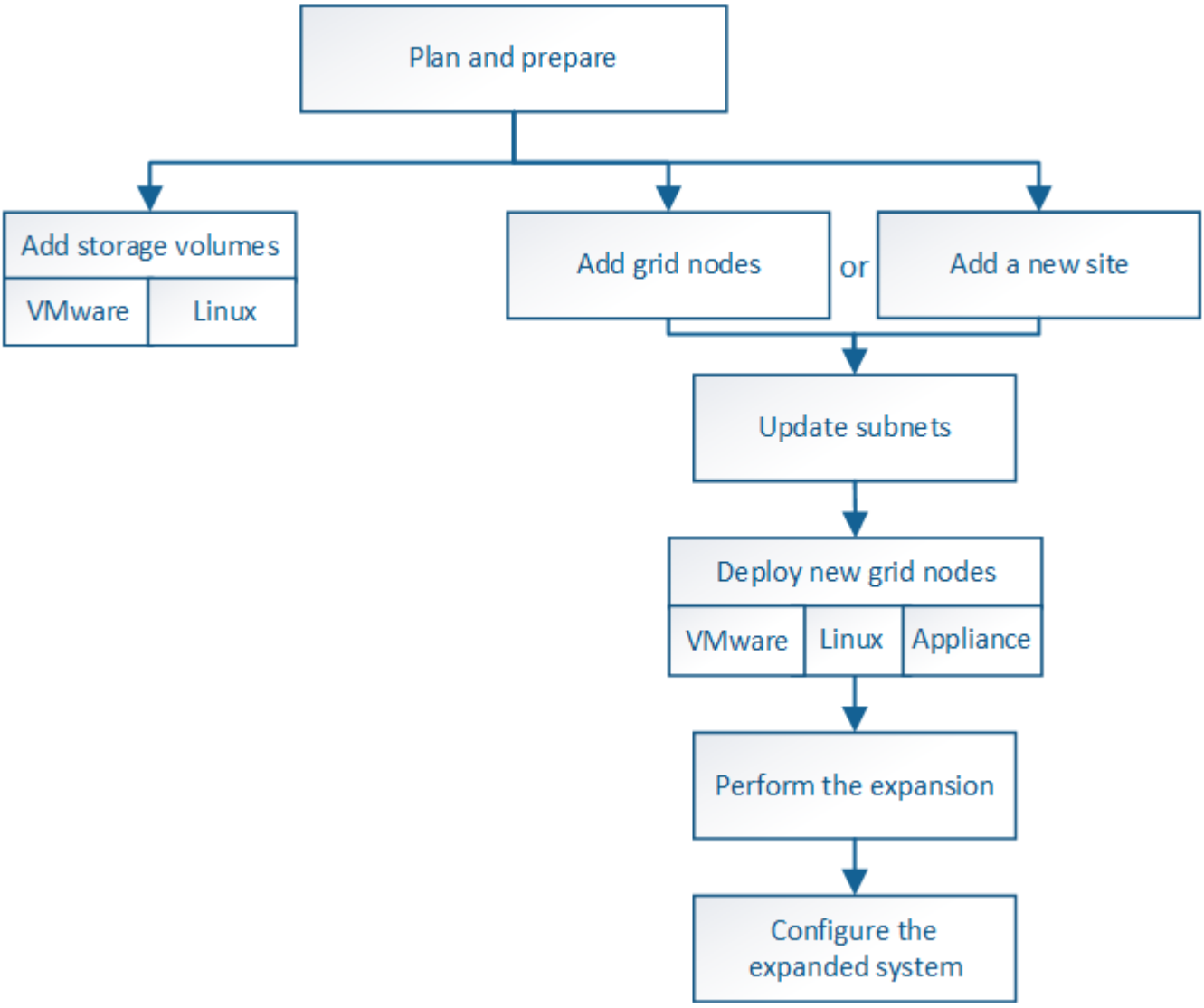
확장을 수행하는 이유는 추가해야 하는 각 유형의 새 노드 수와 새 노드의 위치를 결정합니다. 예를 들어 스토리지 용량을 늘리거나, 메타데이터 용량을 추가하거나, 중복성 또는 새로운 기능을 추가하기 위해 확장을 수행하는 경우에는 노드 요구 사항이 다릅니다.

워크플로우 다이어그램에 표시된 것처럼 스토리지 노드를 추가하거나 기존 사이트에 새 노드를 추가하거나 새 사이트를 추가하는지에 따라 확장을 수행하는 단계가 달라집니다. 어떤 경우든 현재 시스템의 운영을 중단하지 않고 확장을 수행할 수 있습니다.

노드를 추가하는 단계는 StorageGRID 어플라이언스를 추가하거나 VMware 또는 Linux를 실행하는 호스트를

추가하는지에 따라서도 달라집니다.

> "'Linux'는 Red Hat ® Enterprise Linux ®, Ubuntu ®, CentOS 또는 Debian ® 배포를 의미합니다. 를 사용합니다 "NetApp 상호 운용성 매트릭스 툴(IMT)" 를 클릭하여 지원되는 버전 목록을 가져옵니다.



StorageGRID 확장 계획

스토리지 용량을 추가합니다

오브젝트 용량 추가 지침

기존 스토리지 노드에 스토리지 볼륨을 추가하거나 기존 사이트에 새 스토리지 노드를 추가하여 StorageGRID 시스템의 오브젝트 스토리지 용량을 확장할 수 있습니다. ILM(정보 수명 주기 관리) 정책의 요구 사항을 충족하는 방법으로 스토리지 용량을 추가해야 합니다.

스토리지 볼륨 추가 지침

기존 스토리지 노드에 스토리지 볼륨을 추가하기 전에 다음 지침 및 제한 사항을 검토하십시오.

- 현재 ILM 규칙을 검토하여 복제된 또는 삭제 코딩 개체에 사용할 수 있는 스토리지를 늘리기 위해 스토리지 볼륨을 어디에 언제 추가해야 하는지 결정해야 합니다. 의 지침을 참조하십시오 정보 수명 주기 관리로 개체 관리.
- 오브젝트 메타데이터는 볼륨 0에만 저장되기 때문에 스토리지 볼륨을 추가하여 시스템의 메타데이터 용량을 늘릴 수 없습니다.
- 각 소프트웨어 기반 스토리지 노드는 최대 16개의 스토리지 볼륨을 지원할 수 있습니다. 그 이상으로 용량을 추가해야 하는 경우 새 스토리지 노드를 추가해야 합니다.
- 각 SG6060 또는 SG6060X 어플라이언스에 하나 또는 두 개의 확장 셸프를 추가할 수 있습니다. 각 확장 셸프마다 16개의 스토리지 볼륨이 추가됩니다. SG6060 및 SG6060X는 두 확장 셸프를 모두 설치하여 각각 총 48개의 스토리지 볼륨을 지원할 수 있습니다.
- 다른 스토리지 어플라이언스에는 스토리지 볼륨을 추가할 수 없습니다.
- 기존 스토리지 볼륨의 크기는 늘릴 수 없습니다.
- 시스템 업그레이드, 복구 작업 또는 다른 확장을 수행하는 동시에 스토리지 노드를 추가할 수 없습니다.

스토리지 볼륨을 추가하고 ILM 정책을 충족하기 위해 확장해야 하는 스토리지 노드를 결정한 후에는 사용 중인 스토리지 노드 유형에 대한 지침을 따르십시오.

- SG6060 또는 SG6060X 스토리지 어플라이언스에 하나 또는 두 개의 확장 셸프를 추가하려면 로 이동합니다 배포된 SG6060 또는 SG6060X에 확장 셸프를 추가합니다.
- 소프트웨어 기반 노드의 경우 의 지침을 따릅니다스토리지 노드에 스토리지 볼륨을 추가하는 중입니다.

스토리지 노드 추가 지침

기존 사이트에 스토리지 노드를 추가하기 전에 다음 지침 및 제한 사항을 검토하십시오.

- 현재 ILM 규칙을 검토하여 복제된 또는 삭제 코딩 개체에 사용할 수 있는 스토리지를 늘리기 위해 스토리지 노드를 추가할 위치 및 시기를 결정해야 합니다. 의 지침을 참조하십시오 정보 수명 주기 관리로 개체 관리.
- 단일 확장 절차에서 스토리지 노드를 10개 이상 추가할 수 없습니다.
- 단일 확장 절차에서 여러 사이트에 스토리지 노드를 추가할 수 있습니다.
- 단일 확장 절차에서 스토리지 노드 및 다른 유형의 노드를 추가할 수 있습니다.
- 확장 절차를 시작하기 전에 복구의 일부로 수행된 모든 데이터 복구 작업이 완료되었는지 확인해야 합니다. 을 참조하십시오 데이터 복구 작업을 확인합니다.
- 확장을 수행하기 전이나 후에 스토리지 노드를 제거해야 하는 경우 단일 서비스 해제 노드 절차에서 10개 이상의 스토리지 노드를 서비스 해제할 수 없습니다.

스토리지 노드의 **ADC** 서비스에 대한 지침

확장을 구성할 때 각 새 스토리지 노드에 관리 도메인 컨트롤러(ADC) 서비스를 포함할지 여부를 선택해야 합니다. ADC 서비스는 그리드 서비스의 위치 및 가용성을 추적합니다.

- StorageGRID 시스템에는 가 필요합니다 ADC 서비스 쿼럼입니다 항상 각 사이트에서 사용할 수 있습니다.
- 각 사이트에 적어도 3개의 스토리지 노드가 ADC 서비스를 포함해야 합니다.
- ADC 서비스를 모든 스토리지 노드에 추가하는 것은 권장되지 않습니다. 너무 많은 ADC 서비스를 포함시키면 노드 간 통신 증가로 인해 속도가 느려지게 될 수 있습니다.
- 단일 그리드에는 ADC 서비스가 있는 48개 이상의 스토리지 노드가 있을 수 없습니다. 이는 각 사이트에 3개의 ADC 서비스를 제공하는 16개 사이트와 동일합니다.

- 일반적으로 새 노드에 대해 * ADC 서비스 * 설정을 선택할 때 * 자동 * 을 선택해야 합니다. 새 노드가 ADC 서비스를 포함하는 다른 스토리지 노드를 교체할 경우에만 * 예 * 를 선택합니다. 너무 적은 ADC 서비스가 남아 있는 경우 스토리지 노드를 해제할 수 없으므로 이전 서비스를 제거하기 전에 새 ADC 서비스를 사용할 수 있습니다.
- ADC 서비스를 배포한 후에는 노드에 추가할 수 없습니다.

복제된 객체에 대한 스토리지 용량을 추가합니다

배포에 대한 ILM(정보 수명 주기 관리) 정책에 개체의 복제된 복사본을 만드는 규칙이 포함된 경우 추가할 스토리지 양과 새 스토리지 볼륨 또는 스토리지 노드를 추가할 위치를 고려해야 합니다.

추가 스토리지 추가 위치에 대한 지침은 복제된 복사본을 생성하는 ILM 규칙을 검토하십시오. ILM 규칙이 두 개 이상의 오브젝트 복사본을 만드는 경우 오브젝트 복사본이 만들어지는 각 위치에 스토리지를 추가할 계획입니다. 간단한 예를 들어, 각 사이트에 하나의 오브젝트 복사본을 만드는 2개 사이트 그리드와 ILM 규칙이 있는 경우 각 사이트에 스토리지를 추가하여 그리드의 전체 오브젝트 용량을 늘려야 합니다. 의 지침을 참조하십시오 정보 수명 주기 관리로 개체 관리.

성능을 위해 사이트 간에 스토리지 용량과 컴퓨팅 성능을 균형 있게 유지해야 합니다. 따라서 이 예에서는 각 사이트에 동일한 수의 스토리지 노드를 추가하거나 각 사이트에 추가 스토리지 볼륨을 추가해야 합니다.

버킷 이름 등의 기준에 따라 오브젝트를 다른 위치에 배치하는 규칙 또는 시간에 따라 오브젝트 위치를 변경하는 규칙을 포함하는 보다 복잡한 ILM 정책을 가진 경우 확장에 필요한 스토리지의 위치 분석은 비슷하지만 더 복잡합니다.

전체 스토리지 용량이 얼마나 빨리 소비되는지를 차트를 통해 확장에 추가할 스토리지의 양과 추가 스토리지 공간이 언제 필요한지 파악할 수 있습니다. 의 지침에 설명된 대로 Grid Manager를 사용하여 스토리지 용량을 모니터링하고 차트를 작성할 수 있습니다 StorageGRID 모니터링 및 문제 해결.

확장 시기를 계획할 때 추가 스토리지를 조달 및 설치하는 데 얼마나 오래 걸릴 수 있는지 고려하십시오.

삭제 코딩 오브젝트를 위한 스토리지 용량을 추가합니다

ILM 정책에 삭제 코딩 복사본을 만드는 규칙이 포함된 경우 새 스토리지를 추가할 위치와 새 스토리지를 추가할 시기를 계획해야 합니다. 추가하는 스토리지의 양과 추가 시점에 따라 그리드의 가용 스토리지 용량이 영향을 받을 수 있습니다.

스토리지 확장을 계획하는 첫 번째 단계는 삭제 코딩 오브젝트를 생성하는 ILM 정책의 규칙을 검토하는 것입니다. StorageGRID는 모든 삭제 코딩 오브젝트에 대해 _k+m_fagment를 생성하고 각 조각을 다른 스토리지 노드에 저장하기 때문에 확장 후 새로운 삭제 코딩 데이터를 위한 공간이 최소한 _k+m_개 이상 있어야 합니다. 삭제 코딩 프로파일이 사이트 손실 방지 기능을 제공하는 경우 각 사이트에 스토리지를 추가해야 합니다. 을 참조하십시오 ILM을 사용하여 개체를 관리합니다.

추가해야 하는 노드 수도 확장을 수행할 때 기존 노드의 전체 수에 따라 달라집니다.

삭제 코딩 오브젝트를 위한 스토리지 용량을 추가하는 일반 권장 사항입니다

자세한 계산을 방지하려면 기존 스토리지 노드가 70% 용량에 도달할 때 사이트당 두 개의 스토리지 노드를 추가할 수 있습니다.

이 일반적인 권장사항은 단일 사이트 그리드 및 삭제 코딩이 사이트 손실을 보호하는 그리드에 대한 광범위한 삭제 코딩 체계에서 합리적인 결과를 제공합니다.

이 권장사항으로 이어지는 요인을 더 잘 이해하거나 사이트에 대한 보다 정확한 계획을 개발하려면 다음 섹션을 검토하십시오. 현재 상황에 맞는 맞춤형 권장사항을 보려면 NetApp 어카운트 담당자에게 문의하십시오.

삭제 코딩 오브젝트에 추가할 확장 스토리지 노드의 수를 계산합니다

삭제 코딩 오브젝트를 저장하는 배포 방법을 최적화하려면 다음과 같은 여러 요소를 고려해야 합니다.

- 삭제 코딩 방법을 사용하고 있습니다
- 각 사이트의 노드 수 및 각 노드의 사용 가능한 공간 크기를 포함하여 삭제 코딩에 사용되는 스토리지 풀의 특성
- 그리드가 이전에 확장되었는지 여부(스토리지 노드당 사용 가능한 공간의 양이 모든 노드에서 거의 동일하지 않을 수 있음)
- ILM 규칙이 복제된 개체와 삭제 코딩 개체를 모두 만들었는지 여부와 같은 ILM 정책의 정확한 특성

다음 예에서는 삭제 코딩 구조, 스토리지 풀의 노드 수, 각 노드의 사용 가능한 공간 크기를 이해하는 데 도움이 될 수 있습니다.

이와 유사한 고려 사항은 복제된 데이터와 삭제 코딩 데이터를 모두 저장하는 ILM 정책의 계산과 이전에 확장된 그리드에 대한 계산에도 영향을 줍니다.

> 이 섹션의 예는 StorageGRID 시스템에 스토리지 용량을 추가하는 모범 사례를 보여줍니다. 권장되는 노드 수를 추가할 수 없는 경우 삭제 코딩 오브젝트를 추가로 저장할 수 있도록 EC 균형 조정 절차를 실행해야 할 수 있습니다. 을 참조하십시오 삭제 코딩 데이터의 균형을 재조정합니다.

예 **1: 2+1** 삭제 코딩을 사용하는 단일 사이트 그리드를 확장합니다

이 예제에서는 세 개의 스토리지 노드만 포함하는 단순 그리드를 확장하는 방법을 보여 줍니다.

> 이 예제에서는 세 개의 스토리지 노드만 사용하여 작업을 간단하게 합니다. 그러나 세 개의 스토리지 노드만 사용하는 것은 권장되지 않습니다. 실제 운영 그리드는 이중화를 위해 최소 *k*+*m*+1 스토리지 노드를 사용해야 합니다. 이 경우 스토리지 노드 4개(2+1+1)가 됩니다.

다음 사항을 가정합니다.

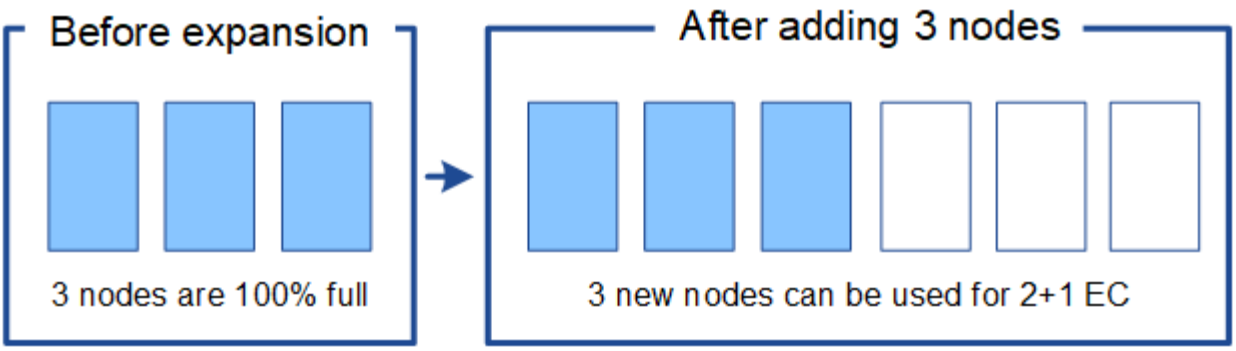
- 모든 데이터는 2+1 삭제 코딩 체계를 사용하여 저장됩니다. 2+1 삭제 코딩 체계를 사용하면 모든 오브젝트는 3개의 조각으로 저장되며 각 단편은 다른 스토리지 노드에 저장됩니다.
- 스토리지 노드 3개가 있는 사이트가 1개 있습니다. 각 스토리지 노드의 총 용량은 100TB입니다.
- 새로운 100TB 스토리지 노드를 추가하여 확장할 수 있습니다.
- 따라서 이전 노드와 새 노드에서 삭제 코딩 데이터의 균형을 최종적으로 조정하려고 합니다.

확장을 수행할 때 스토리지 노드의 전체 성능을 기준으로 다양한 옵션이 제공됩니다.

- * 기존 노드가 100% 찰 경우 100TB 스토리지 노드 3개 추가 *

  이 예에서는 기존 노드가 100% 찼습니다. 사용 가능한 용량이 없기 때문에 2+1 삭제 코딩을 계속하려면 노드 3개를 즉시 추가해야 합니다.

  확장이 완료된 후 오브젝트를 삭제 코딩하면 모든 조각이 새 노드에 배치됩니다.

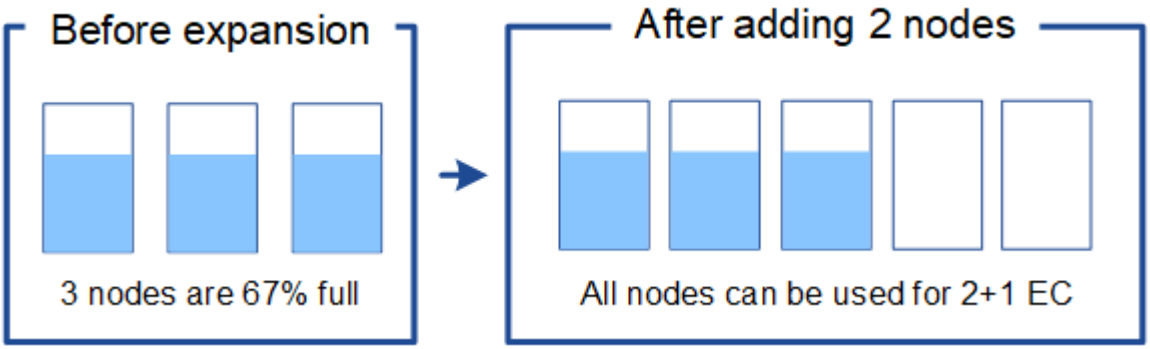


> 이 확장에서는 _k+m_nodes가 추가됩니다. 이중화를 위해 4개의 노드를 추가하는 것이 좋습니다. 기존 노드가 100% 차 있을 때 _k+m_확장 스토리지 노드만 추가하면 모든 새 오브젝트가 확장 노드에 저장됩니다. 새로운 노드 중 하나를 일시적으로 사용할 수 없게 되는 경우에도 StorageGRID는 ILM 요구 사항을 충족할 수 없습니다.

- * 기존 스토리지 노드가 67% 찰 때 100TB 스토리지 노드 2개 추가 *

  이 예에서는 기존 노드가 67% 찼습니다. 기존 노드에 100TB의 여유 용량이 있기 때문에(노드당 33TB) 지금 확장을 수행하는 경우에만 노드 2개만 추가하면 됩니다.

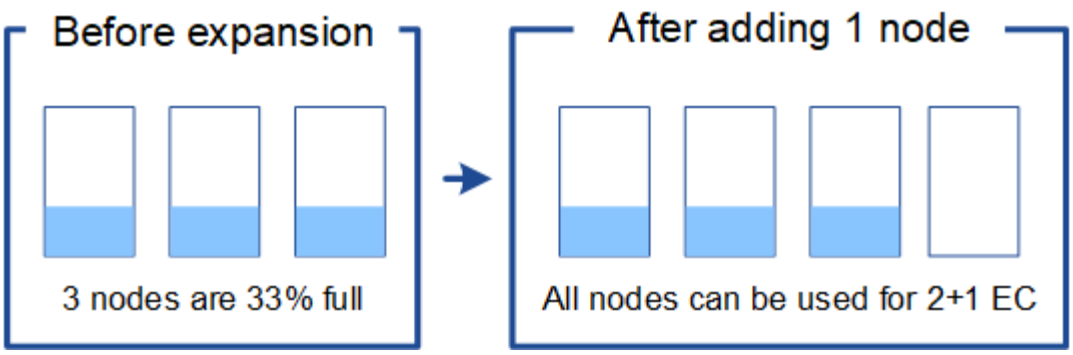
  200TB의 용량을 추가하면 2+1 삭제 코딩을 계속할 수 있으며, 결국 모든 노드에서 삭제 코딩 데이터의 균형을 유지할 수 있습니다.



- * 기존 스토리지 노드가 33% 찰 경우 100TB 스토리지 노드 1개 추가 *

  이 예에서는 기존 노드가 33% 찼습니다. 기존 노드에 200TB의 여유 용량(노드당 67TB)이 있으므로 지금 확장을 수행하는 경우에만 노드를 추가하면 됩니다.

  100TB의 용량을 추가하면 2+1 삭제 코딩을 계속할 수 있으며, 결국 모든 노드에서 삭제 코딩 데이터의 균형을 유지할 수 있습니다.



예 **2: 6+3** 삭제 코딩을 사용하는 **3**개 사이트 그리드를 확장합니다

이 예에서는 여러 조각으로 이루어진 삭제 코딩 체계를 갖춘 다중 사이트 그리드에 대한 확장 계획을 개발하는 방법을 보여 줍니다. 이러한 예들의 차이에도 불구하고 권장 확장 계획은 매우 유사합니다.

다음 사항을 가정합니다.

- 모든 데이터는 6+3 삭제 코딩 체계를 사용하여 저장됩니다. 6+3 삭제 코딩 체계를 사용하면 모든 오브젝트는 9 조각으로 저장되며 각 단편은 다른 스토리지 노드에 저장됩니다.
- 3개의 사이트가 있고 각 사이트에는 4개의 스토리지 노드(총 12개 노드)가 있습니다. 각 노드의 총 용량은 100TB입니다.
- 새로운 100TB 스토리지 노드를 추가하여 확장할 수 있습니다.
- 따라서 이전 노드와 새 노드에서 삭제 코딩 데이터의 균형을 최종적으로 조정하려고 합니다.

확장을 수행할 때 스토리지 노드의 전체 성능을 기준으로 다양한 옵션이 제공됩니다.

- * 기존 노드가 100% 꽉 찬 경우 사이트당 3개씩 총 9개의 100TB 스토리지 노드를 추가합니다. *

  이 예에서는 기존 노드 12개가 100% 찼습니다. 사용 가능한 용량이 없으므로 6개 이상의 3 삭제 코딩을 계속하려면 9개 노드(900TB의 추가 용량)를 즉시 추가해야 합니다.

  확장이 완료된 후 오브젝트를 삭제 코딩하면 모든 조각이 새 노드에 배치됩니다.

  > 이 확장에서는 _k+m_nodes가 추가됩니다. 이중화를 위해 12개 노드(사이트당 4개)를 추가하는 것이 좋습니다. 기존 노드가 100% 차 있을 때 _k+m_확장 스토리지 노드만 추가하면 모든 새 오브젝트가 확장 노드에 저장됩니다. 새로운 노드 중 하나를 일시적으로 사용할 수 없게 되는 경우에도 StorageGRID는 ILM 요구 사항을 충족할 수 없습니다.

- * 기존 노드가 75% 차 있는 경우 사이트당 2개의 100TB 스토리지 노드 6개 추가 *

  이 예에서는 기존 노드 12개가 75% 찼습니다. 300TB의 여유 용량(노드당 25TB)이 있으므로 지금 확장을 수행하는 경우에는 6개의 노드만 추가하면 됩니다. 세 사이트 각각에 두 개의 노드를 추가합니다.

  600TB의 스토리지 용량을 추가하면 6개 이상의 3 삭제 코딩을 계속할 수 있으며, 결국 모든 노드에서 삭제 코딩 데이터의 균형을 맞출 수 있습니다.

- * 기존 노드가 50% 찰 경우 사이트당 하나씩 100TB 스토리지 노드 3개를 추가합니다. *

  이 예에서는 기존 노드 12개가 50% 찼습니다. 사용 가능한 용량이 600TB(노드당 50TB)이므로 지금 확장을

수행하는 경우에만 노드를 3개만 추가하면 됩니다. 세 사이트 각각에 하나의 노드를 추가합니다.

300TB의 스토리지 용량을 추가하면 6+3 삭제 코딩을 계속할 수 있으며, 결국 모든 노드에서 삭제 코딩 데이터의 균형을 맞출 수 있습니다.

삭제 코딩 데이터의 재조정에 대한 고려사항

스토리지 노드 추가를 위해 확장을 수행하는 경우 ILM 정책에 코드 데이터를 삭제할 수 있는 하나 이상의 ILM 규칙이 포함된 경우 확장이 완료된 후 EC 균형 조정 절차를 수행해야 할 수 있습니다.

예를 들어, 사용 중인 삭제 코딩 체계에 권장되는 스토리지 노드 수를 추가할 수 없는 경우, 삭제 코딩 오브젝트를 추가로 저장할 수 있도록 EC 재조정 절차를 실행해야 할 수 있습니다.

이러한 고려 사항을 검토한 후 확장을 수행한 다음 로 이동합니다 스토리지 노드를 추가한 후 삭제 코딩 데이터의 균형을 재조정합니다 절차를 실행합니다.

EC 재조정 이란 무엇입니까**?**

EC 재조정은 스토리지 노드 확장 후 필요할 수 있는 StorageGRID 절차입니다. 이 절차는 기본 관리 노드에서 명령줄 스크립트로 실행됩니다. EC 균형 조정 절차를 실행하면 StorageGRID는 삭제 코딩 조각을 사이트의 기존 스토리지 노드와 새로 확장된 스토리지 노드 간에 재배포합니다.

EC 재조정 절차:

- 삭제 코딩 오브젝트 데이터만 이동합니다. 복제된 오브젝트 데이터는 이동하지 않습니다.
- 사이트 내에서 데이터를 재배포합니다. 사이트 간에 데이터를 이동하지 않습니다.
- 사이트의 모든 스토리지 노드 간에 데이터를 재배포합니다. 스토리지 볼륨 내에서 데이터를 재배포하지 않습니다.
- 에서는 삭제 코딩 데이터를 이동할 위치를 결정할 때 각 스토리지 노드에서 복제된 데이터 사용을 고려하지 않습니다

EC 재조정 절차가 완료되면 다음을 수행합니다.

- 삭제 코딩 데이터는 사용 가능한 공간이 적은 스토리지 노드에서 사용 가능한 공간이 더 많은 스토리지 노드로 이동됩니다.
- EC 균형 조정 절차가 복제된 오브젝트 복사본을 이동하지 않으므로 사용된 값(%)이 스토리지 노드 간에 서로 다를 수 있습니다.
- 삭제 코딩 오브젝트의 데이터 보호는 변경되지 않습니다.

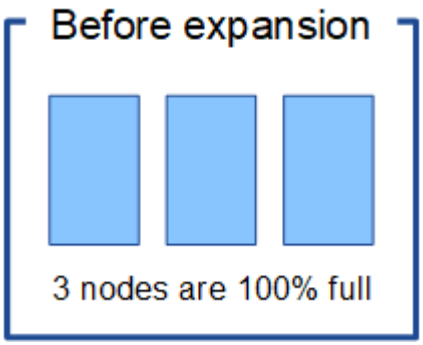
EC 재조정 절차가 실행 중이면 ILM 작업 및 S3 및 Swift 클라이언트 작업의 성능에 영향을 줄 수 있습니다. 따라서 이 절차는 제한된 경우에만 수행해야 합니다.

EC 균형 조정을 수행하지 않는 경우

EC 균형 조정을 수행할 필요가 없는 경우를 예로 들면 다음과 같습니다.

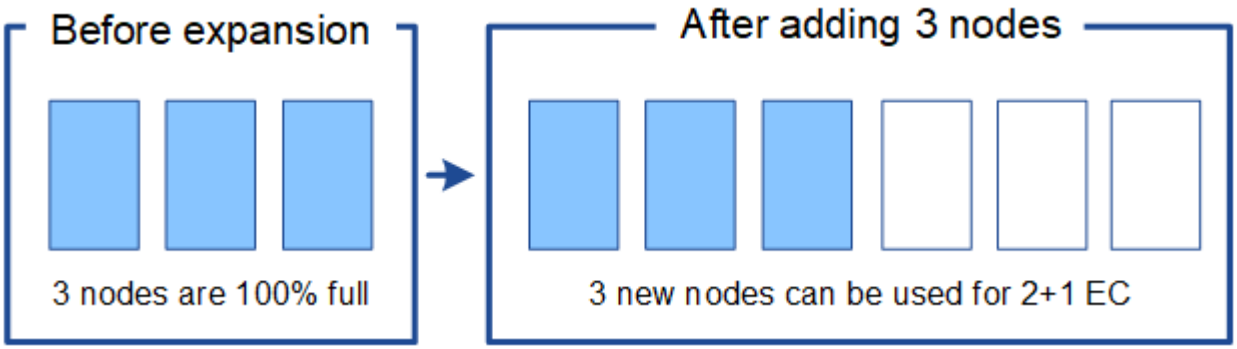
- StorageGRID는 단일 사이트에서 실행 중이며 3개의 스토리지 노드가 있습니다.
- ILM 정책은 1.0MB보다 큰 모든 개체에 대해 2+1 삭제 코딩 규칙을 사용하고 더 작은 개체에 대해서는 2-복사 복제 규칙을 사용합니다.

- 모든 스토리지 노드가 완전히 꽉 차서 주요 심각도 수준에서 * 낮은 오브젝트 스토리지 * 경고가 트리거되었습니다. 권장되는 작업은 스토리지 노드를 추가하기 위한 확장 절차를 수행하는 것입니다.



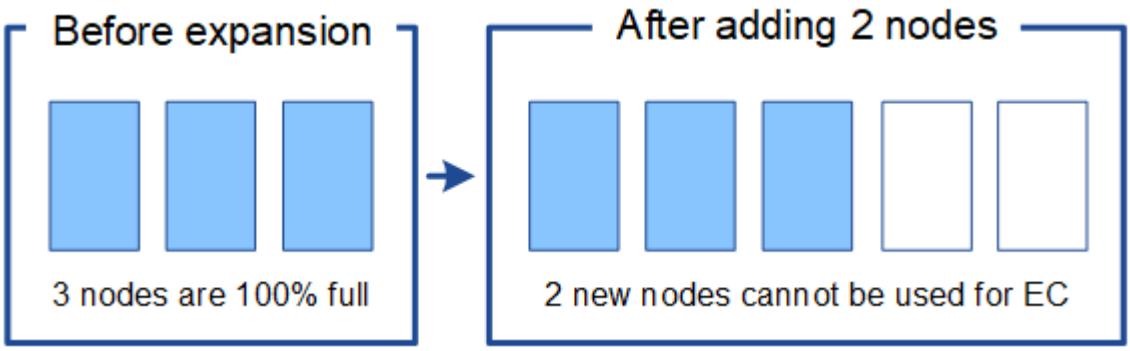
이 예제에서 사이트를 확장하려면 새 스토리지 노드를 3개 이상 추가하는 것이 좋습니다. StorageGRID에서는 2+1 삭제 코딩용 스토리지 노드 3개가 필요하므로 두 데이터 단편을 서로 다른 노드에 하나의 패리티 분편을 배치할 수 있습니다.

3개의 스토리지 노드를 추가한 후에도 원래 스토리지 노드가 꽉 찬 상태로 유지되지만, 새 노드의 2+1 삭제 코딩 체계로 오브젝트를 계속 인제스트할 수 있습니다. 이 경우에는 EC 재조정 절차를 실행하지 않는 것이 좋습니다. 절차를 실행하면 성능이 일시적으로 저하되어 클라이언트 작업에 영향을 줄 수 있습니다.



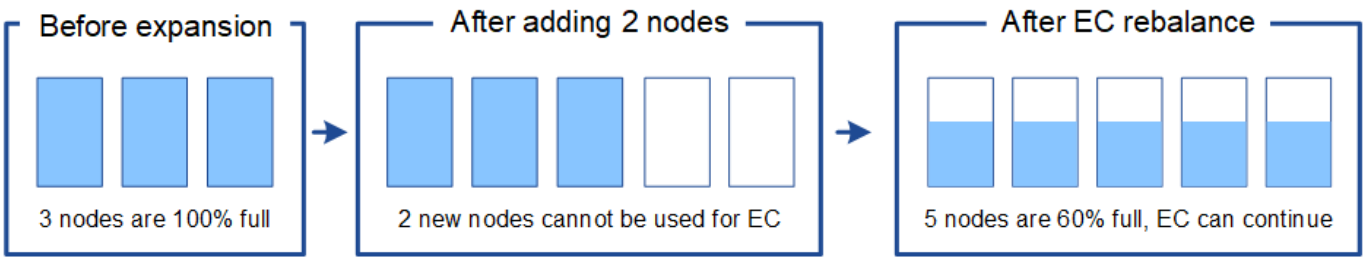
EC 균형 조정을 수행하는 시기

EC 균형 조정 절차를 수행해야 하는 경우를 예로 들어 보겠습니다. 하지만 두 개의 스토리지 노드만 추가할 수 있다고 가정합니다. 2+1 삭제 코딩에 3개 이상의 스토리지 노드가 필요하므로 새 노드를 삭제 코딩 데이터에 사용할 수 없습니다.



이 문제를 해결하고 새 스토리지 노드를 사용하려면 EC 재조정 절차를 실행할 수 있습니다. 이 절차를 실행하면 StorageGRID는 사이트의 모든 스토리지 노드 간에 삭제 코딩 데이터 및 패리티 조각을 재배포합니다. 이 예에서 EC

균형 조정 절차가 완료되면 5개 노드 모두가 60%에 불과하며, 모든 스토리지 노드의 2+1 삭제 코딩 체계로 오브젝트를 계속 인제스트할 수 있습니다.



EC 재조정 요구 사항

일반적으로 EC 재조정 절차는 제한된 경우에만 실행해야 합니다. 특히, 다음 사항이 모두 참인 경우에만 EC 재조정을 수행해야 합니다.

- 오브젝트 데이터에 삭제 코딩을 사용합니다.
- 사이트의 하나 이상의 스토리지 노드에 대해 * Low Object Storage * 알림이 트리거되어 노드가 80% 이상 꽉 찼음을 나타냅니다.
- 사용 중인 삭제 코딩 구성표에 권장되는 새 스토리지 노드 수를 추가할 수 없습니다. 을 참조하십시오 삭제 코딩 오브젝트를 위한 스토리지 용량을 추가합니다.
- S3 및 Swift 클라이언트는 EC 균형 조정 절차가 실행되는 동안 쓰기 및 읽기 작업 성능이 낮은 것을 허용할 수 있습니다.

EC 재조정 절차가 다른 유지 관리 작업과 상호 작용하는 방식

EC 재조정 절차를 실행하는 동시에 특정 유지보수 절차를 수행할 수 없습니다.

절차를 참조하십시오	**EC** 재조정 절차 중에 허용됩니까**?**
EC 재조정 절차 추가	아니요 한 번에 하나의 EC 재조정 절차만 실행할 수 있습니다.
서비스 해제 절차 EC 데이터 복구 작업	아니요 • EC 재조정 절차가 실행되는 동안에는 파기 절차 또는 EC 데이터 복구를 시작할 수 없습니다. • 스토리지 노드 서비스 해제 절차 또는 EC 데이터 복구가 실행 중인 동안에는 EC 재조정 절차를 시작할 수 없습니다.
확장 절차	아니요 확장 시 새 스토리지 노드를 추가해야 하는 경우 모든 새 노드를 추가할 때까지 EC 균형 조정 절차를 실행해야 합니다. 새 스토리지 노드를 추가할 때 EC 균형 조정 절차가 진행 중이면 데이터가 해당 노드로 이동되지 않습니다.

절차를 참조하십시오	**EC** 재조정 절차 중에 허용됩니까**?**
업그레이드 절차	아니요 StorageGRID 소프트웨어를 업그레이드해야 하는 경우 EC 재조정 절차를 실행하기 전이나 후에 업그레이드 절차를 수행해야 합니다. 필요에 따라 EC 재조정 절차를 종료하여 소프트웨어 업그레이드를 수행할 수 있습니다.
어플라이언스 노드 클론 절차	아니요 어플라이언스 스토리지 노드를 복제해야 하는 경우 새 노드를 추가할 때까지 EC 재조정 절차를 실행할 때까지 기다려야 합니다. 새 스토리지 노드를 추가할 때 EC 균형 조정 절차가 진행 중이면 데이터가 해당 노드로 이동되지 않습니다.
핫픽스 절차	예. EC 재조정 절차가 실행되는 동안 StorageGRID 핫픽스를 적용할 수 있습니다.
기타 유지보수 절차	아니요 다른 유지보수 절차를 실행하기 전에 EC 재조정 절차를 종료해야 합니다.

EC 재조정 절차가 **ILM**과 상호 작용하는 방법

EC 재조정 절차가 실행되는 동안 기존 삭제 코딩 오브젝트의 위치를 변경할 수 있는 ILM을 변경하지 마십시오. 예를 들어 다른 삭제 코딩 프로필을 가진 ILM 규칙을 사용하지 마십시오. 이러한 ILM을 변경해야 하는 경우 EC 재조정 절차를 중단해야 합니다.

메타데이터 용량을 추가합니다

개체 메타데이터에 적절한 공간을 사용할 수 있도록 하려면 확장 절차를 수행하여 각 사이트에 새 스토리지 노드를 추가해야 할 수 있습니다.

StorageGRID는 각 스토리지 노드의 볼륨 0에 개체 메타데이터를 위한 공간을 예약합니다. 모든 오브젝트 메타데이터의 사본 3개가 각 사이트에서 유지 관리되므로 모든 스토리지 노드에 균등하게 분산됩니다.

Grid Manager를 사용하여 스토리지 노드의 메타데이터 용량을 모니터링하고 메타데이터 용량이 사용되는 속도를 예측할 수 있습니다. 또한 사용된 메타데이터 공간이 특정 임계값에 도달하면 스토리지 노드에 대해 * Low Metadata Storage * 경고가 트리거됩니다.

그리드의 오브젝트 메타데이터 용량은 그리드 사용 방식에 따라 오브젝트 스토리지 용량보다 더 빠르게 소비될 수 있습니다. 예를 들어, 일반적으로 많은 수의 작은 오브젝트를 수집하거나 오브젝트에 대량의 사용자 메타데이터 또는 태그를 추가하는 경우 오브젝트 스토리지 용량이 충분한 경우에도 메타데이터 용량을 늘리려면 스토리지 노드를 추가해야 할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- 오브젝트 메타데이터 스토리지 관리

- 각 스토리지 노드의 객체 메타데이터 용량을 모니터링합니다

메타데이터 용량 확장 지침

스토리지 노드를 추가하여 메타데이터 용량을 증가시키기 전에 다음 지침 및 제한 사항을 검토하십시오.

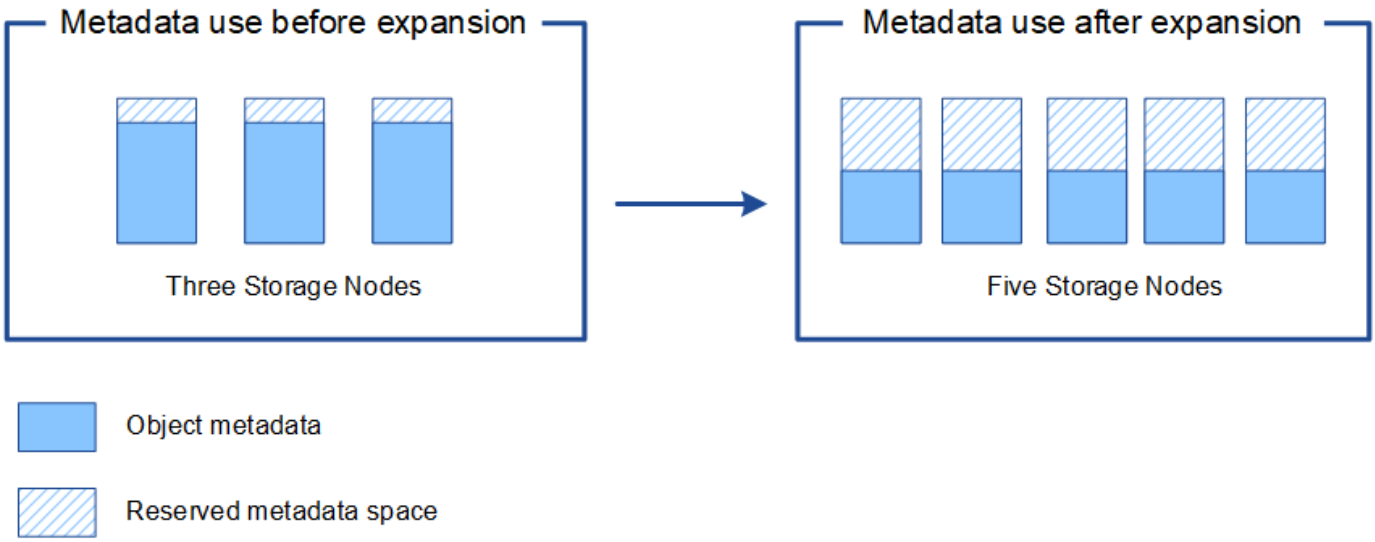
- 오브젝트 스토리지 용량이 충분하다면 오브젝트 메타데이터에 사용 가능한 공간이 많을수록 StorageGRID 시스템에 저장할 수 있는 오브젝트 수가 증가합니다.
- 각 사이트에 하나 이상의 스토리지 노드를 추가하여 그리드의 메타데이터 용량을 늘릴 수 있습니다.
- 지정된 스토리지 노드의 개체 메타데이터에 예약된 실제 공간은 메타데이터 예약된 공간 스토리지 옵션(시스템 전체 설정), 노드에 할당된 RAM 크기 및 노드 볼륨 0의 크기에 따라 달라집니다. 의 지침을 참조하십시오 StorageGRID 관리.
- 메타데이터가 볼륨 0에만 저장되므로 스토리지 볼륨을 기존 스토리지 노드에 추가하여 메타데이터 용량을 늘릴 수 없습니다.
- 새 사이트를 추가하여 메타데이터 용량을 늘릴 수 없습니다.
- StorageGRID는 모든 사이트에 모든 오브젝트 메타데이터의 복사본을 3개 보관합니다. 따라서 시스템의 메타데이터 용량은 가장 작은 사이트의 메타데이터 용량에 의해 제한됩니다.
- 메타데이터 용량을 추가할 때는 각 사이트에 동일한 수의 스토리지 노드를 추가해야 합니다.

스토리지 노드를 추가할 때 메타데이터가 재배포되는 방식

확장 시 스토리지 노드를 추가하면 StorageGRID는 기존 오브젝트 메타데이터를 각 사이트의 새 노드로 재분배하여 그리드의 전체 메타데이터 용량을 늘립니다. 사용자 작업이 필요하지 않습니다.

다음 그림에서는 확장에서 스토리지 노드를 추가할 때 StorageGRID가 개체 메타데이터를 재배포하는 방법을 보여줍니다. 그림의 왼쪽은 확장 전에 세 개의 스토리지 노드의 볼륨 0을 나타냅니다. 메타데이터는 각 노드의 사용 가능한 메타데이터 공간의 상대적으로 큰 부분을 소비하며 * Low metadata storage * 알림이 트리거되었습니다.

그림의 오른쪽에는 사이트에 두 개의 스토리지 노드가 추가된 후 기존 메타데이터가 재분배되는 방법이 나와 있습니다. 각 노드의 메타데이터 양이 감소하고 * Low Metadata Storage * 알림이 더 이상 트리거되지 않으며 메타데이터에 사용 가능한 공간이 증가했습니다.



그리드 노드를 추가하여 시스템에 기능을 추가합니다

기존 사이트에 새 그리드 노드를 추가하여 StorageGRID 시스템에 중복성 또는 추가 기능을 추가할 수 있습니다.

예를 들어 게이트웨이 노드의 고가용성 그룹 생성을 지원하기 위해 게이트웨이 노드를 추가하거나 원격 사이트에 관리 노드를 추가하여 로컬 노드를 사용한 모니터링을 허용할 수 있습니다.

다음 노드 유형 중 하나 이상을 단일 확장 작업에서 하나 이상의 기존 사이트에 추가할 수 있습니다.

- 운영 관리자 노드가 아닌 노드
- 스토리지 노드
- 게이트웨이 노드
- 아카이브 노드

그리드 노드 추가를 준비하는 경우 다음 제한 사항을 유의하십시오.

- 기본 관리 노드는 초기 설치 중에 배포됩니다. 확장 중에는 운영 관리자 노드를 추가할 수 없습니다.
- 스토리지 노드 및 다른 유형의 노드를 동일한 확장에서 추가할 수 있습니다.
- 스토리지 노드를 추가할 때는 새 노드의 수와 위치를 신중하게 계획해야 합니다. 을 참조하십시오 오브젝트 용량 추가 지침.
- 아카이브 노드를 추가하는 경우 각 아카이브 노드는 TSM(Tivoli Storage Manager) 미들웨어를 통해 테이프만 지원합니다.
- 신뢰할 수 없는 클라이언트 네트워크 페이지에서 * 새 노드 클라이언트 네트워크 기본값 * 옵션이 * 신뢰할 수 없음 * 으로 설정된 경우 클라이언트 네트워크를 사용하여 확장 노드에 연결하는 클라이언트 응용 프로그램은 로드 밸런서 엔드포인트 포트(* 구성 * > * 네트워크 * > * 신뢰할 수 없는 클라이언트 네트워크 *)를 사용하여 연결해야 합니다. 의 지침을 참조하십시오 StorageGRID 관리 새 노드의 설정을 변경하고 로드 밸런서 엔드포인트를 구성합니다.

새 사이트를 추가합니다

새 사이트를 추가하여 StorageGRID 시스템을 확장할 수 있습니다.

사이트 추가 지침

사이트를 추가하기 전에 다음 요구 사항 및 제한 사항을 검토하십시오.

- 확장 작업당 하나의 사이트만 추가할 수 있습니다.
- 동일한 확장의 일부로 기존 사이트에 그리드 노드를 추가할 수 없습니다.
- 모든 사이트에는 3개 이상의 스토리지 노드가 포함되어야 합니다.
- 새 사이트를 추가해도 저장할 수 있는 개체 수는 자동으로 늘어지지 않습니다. 그리드의 총 오브젝트 용량은 사용 가능한 스토리지 양, ILM 정책 및 각 사이트의 메타데이터 용량에 따라 달라집니다.
- 새 사이트를 사이징할 때는 충분한 메타데이터 용량이 포함되어야 합니다.

  StorageGRID는 모든 사이트에 모든 오브젝트 메타데이터의 복사본을 보관합니다. 새 사이트를 추가할 때는 기존 오브젝트 메타데이터에 충분한 메타데이터 용량과 성장을 위한 충분한 메타데이터 용량이 포함되어야 합니다.

자세한 내용은 다음을 참조하십시오.

  - 오브젝트 메타데이터 스토리지 관리
  - 각 스토리지 노드의 객체 메타데이터 용량을 모니터링합니다

- 사이트 간에 사용 가능한 네트워크 대역폭과 네트워크 대기 시간 수준을 고려해야 합니다. 모든 오브젝트가 수집된 사이트에만 저장되어 있더라도 사이트 간에 메타데이터 업데이트가 지속적으로 복제됩니다.
- 확장 중에 StorageGRID 시스템이 계속 작동하므로 확장 절차를 시작하기 전에 ILM 규칙을 검토해야 합니다. 확장 절차가 완료될 때까지 오브젝트 복사본이 새 사이트에 저장되지 않도록 해야 합니다.

  예를 들어 확장을 시작하기 전에 규칙에 기본 스토리지 풀(모든 스토리지 노드)이 사용되고 있는지 확인합니다. 이러한 경우 기존 스토리지 노드가 포함된 새 스토리지 풀을 생성하고 ILM 규칙을 업데이트하여 새 스토리지 풀을 사용해야 합니다. 그렇지 않으면 해당 사이트의 첫 번째 노드가 활성 상태가 되는 즉시 새 사이트에 개체가 복사됩니다.

  새 사이트를 추가할 때 ILM을 변경하는 방법에 대한 자세한 내용은 의 지침에 있는 ILM 정책 변경 예제를 참조하십시오 ILM을 사용하여 개체 관리.

필요한 자료를 수집합니다

확장 작업을 수행하기 전에 자료를 수집하고 새 하드웨어 및 네트워크를 설치하고 구성합니다.

항목	참고
StorageGRID 설치 아카이브	새 그리드 노드 또는 새 사이트를 추가하는 경우 StorageGRID 설치 아카이브를 다운로드하여 추출해야 합니다. 그리드에서 현재 실행 중인 버전과 동일한 버전을 사용해야 합니다. 자세한 내용은 의 지침을 참조하십시오 StorageGRID 설치 파일 다운로드 및 추출. • 참고: * 기존 스토리지 노드에 새 스토리지 볼륨을 추가하거나 새 StorageGRID 어플라이언스를 설치할 경우 파일을 다운로드할 필요가 없습니다.
서비스 노트북	서비스 랩톱의 특징은 다음과 같습니다. • 네트워크 포트 • SSH 클라이언트(예: PuTTY) • 지원되는 웹 브라우저
"passwords.txt" 파일	명령줄에서 그리드 노드에 액세스하는 데 필요한 암호를 포함합니다. 복구 패키지에 포함되어 있습니다.
프로비저닝 암호	StorageGRID 시스템을 처음 설치할 때 암호가 생성되고 문서화됩니다. 프로비저닝 암호문은 passwords.txt 파일에 없습니다.

항목	참고

StorageGRID 설명서	• StorageGRID 관리
	• 릴리스 정보
	• 플랫폼에 대한 설치 지침
	  ◦ Red Hat Enterprise Linux 또는 CentOS를 설치합니다
	  ◦ Ubuntu 또는 Debian을 설치합니다
	  ◦ VMware를 설치합니다

현재 사용 중인 플랫폼에 대한 설명서입니다	지원되는 버전은 를 참조하십시오 "상호 운용성 매트릭스".

StorageGRID 설치 파일을 다운로드하고 압축을 풉니다

([다운로드 및 추출-설치 파일])

새 그리드 노드 또는 새 사이트를 추가하려면 먼저 적절한 StorageGRID 설치 아카이브를 다운로드하고 파일을 추출해야 합니다.

이 작업에 대해

현재 그리드에서 실행 중인 StorageGRID 버전을 사용하여 확장 작업을 수행해야 합니다.

단계

1. StorageGRID용 NetApp 다운로드 페이지로 이동합니다.

   "NetApp 다운로드: StorageGRID"

2. 그리드에서 현재 실행 중인 StorageGRID 버전을 선택합니다.
3. NetApp 계정의 사용자 이름과 암호를 사용하여 로그인합니다.
4. 최종 사용자 사용권 계약을 읽고 확인란을 선택한 다음 * 동의 및 계속 * 을 선택합니다.
5. 다운로드 페이지의 * StorageGRID * 설치 열에서 해당 플랫폼의 ".tgz" 또는 ".zip" 파일을 선택합니다.

   설치 아카이브 파일에 표시된 버전이 현재 설치된 소프트웨어 버전과 일치해야 합니다.

   서비스 랩톱에서 Windows를 실행 중인 경우 '.zip' 파일을 사용합니다.

플랫폼	설치 아카이브
Red Hat Enterprise Linux 또는 CentOS	'S torageGRID-Webscale-*version*-RPM-*UniqueID*.zip"S torageGRID-Webscale-*version*-RPM-*UniqueID*.tgz'
Ubuntu 또는 Debian 또는 어플라이언스	'storageGRID-Webscale-*version*-deb-*UniqueID*.zip"storageGRID-Webscale-*version*-deb-*UniqueID*.tgz'
VMware	'S torageGRID-Webscale-*version*-vmware-*UniqueID*.zip"S torageGRID-Webscale-*version*-vmware-*UniqueID*.tgz'

플랫폼	설치 아카이브
OpenStack 및 기타 하이퍼바이저	OpenStack에서 기존 구축을 확장하려면 위에 나열된 지원되는 Linux 배포 중 하나를 실행하는 가상 시스템을 구축하고 Linux에 대한 적절한 지침을 따라야 합니다.

6. 아카이브 파일을 다운로드하고 압축을 풉니다.
7. 플랫폼에 적합한 단계에 따라 플랫폼, 계획된 그리드 토폴로지 및 StorageGRID 시스템을 확장하는 방법에 따라 필요한 파일을 선택합니다.

   각 플랫폼의 단계에 나열된 경로는 아카이브 파일에 의해 설치된 최상위 디렉토리를 기준으로 합니다.

8. Red Hat Enterprise Linux 또는 CentOS 시스템을 확장하는 경우 해당 파일을 선택합니다.

경로 및 파일 이름입니다	설명
	StorageGRID 다운로드 파일에 포함된 모든 파일을 설명하는 텍스트 파일입니다.
	제품에 대한 지원 권한을 제공하지 않는 무료 라이센스입니다.
	RHEL 또는 CentOS 호스트에 StorageGRID 노드 이미지를 설치하기 위한 rpm 패키지입니다.
	RHEL 또는 CentOS 호스트에 StorageGRID 호스트 서비스를 설치하기 위한 rpm 패키지입니다.
배포 스크립팅 도구	설명
	StorageGRID 시스템 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
	StorageGRID 어플라이언스 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
/rpms/configure -StorageGrid.sample.json	"configure-StorageGrid.py" 스크립트와 함께 사용할 구성 파일의 예
	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/rpms/configure -StorageGrid.blank.json을 지정합니다	configure-StorageGrid.py 스크립트와 함께 사용할 빈 구성 파일입니다.

경로 및 파일 이름입니다	설명
	StorageGRID 컨테이너 배포를 위한 RHEL 또는 CentOS 호스트 구성을 위한 Ansible 역할 및 플레이북의 예 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.
/rpms/Extras/API-schemas	StorageGRID에 대한 API 스키마입니다. • 참고 *: 업그레이드를 수행하기 전에 이러한 스키마를 사용하여 StorageGRID 관리 API를 사용하도록 작성한 코드가 업그레이드 호환성 테스트를 위한 비프로덕션 StorageGRID 환경이 없는 경우 새 StorageGRID 릴리스와 호환되는지 확인할 수 있습니다.

1. Ubuntu 또는 Debian 시스템을 확장하는 경우 적절한 파일을 선택합니다.

경로 및 파일 이름입니다	설명
	StorageGRID 다운로드 파일에 포함된 모든 파일을 설명하는 텍스트 파일입니다.
/debs/NLF000000.txt 를 참조하십시오	테스트 및 개념 증명 배포에 사용할 수 있는 비프로덕션 NetApp 라이센스 파일.
/debs/storagegrid-webscale-images-version-SHA.deb 를 참조하십시오	StorageGRID 노드 이미지를 Ubuntu 또는 Debian 호스트에 설치하기 위한 DEB 패키지.
/debs/storagegrid-webscale-images-version-SHA.deb.md5 를 참조하십시오	파일 '/debs/storagegrid-webscale-images-version-SHA.deb` 에 대한 MD5 체크섬입니다.
/debs/storagegrid-webscale-service-version-SHA.deb 를 참조하십시오	Ubuntu 또는 Debian 호스트에 StorageGRID 호스트 서비스를 설치하기 위한 DEB 패키지.
배포 스크립팅 도구	설명
/debs/configure-storagegrid.py 를 참조하십시오	StorageGRID 시스템 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
/debs/configure-sga.py 를 참조하십시오	StorageGRID 어플라이언스 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
/debs/storagegrid-ssoauth.py 를 참조하십시오	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제

경로 및 파일 이름입니다	설명
/debs/configure -StorageGrid.sample.json 을 참조하십시오	"configure-StorageGrid.py" 스크립트와 함께 사용할 구성 파일의 예
/debs/configure -StorageGrid.blank.json 을 참조하십시오	configure-StorageGrid.py 스크립트와 함께 사용할 빈 구성 파일입니다.
	StorageGRID 컨테이너 배포를 위한 Ubuntu 또는 Debian 호스트 구성을 위한 Ansible 역할 및 플레이북 예 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.
/debs/Extras/API-schemas	StorageGRID에 대한 API 스키마입니다. • 참고 *: 업그레이드를 수행하기 전에 이러한 스키마를 사용하여 StorageGRID 관리 API를 사용하도록 작성한 코드가 업그레이드 호환성 테스트를 위한 비프로덕션 StorageGRID 환경이 없는 경우 새 StorageGRID 릴리스와 호환되는지 확인할 수 있습니다.

1. VMware 시스템을 확장하는 경우 해당 파일을 선택합니다.

경로 및 파일 이름입니다	설명
	StorageGRID 다운로드 파일에 포함된 모든 파일을 설명하는 텍스트 파일입니다.
	제품에 대한 지원 권한을 제공하지 않는 무료 라이센스입니다.
	그리드 노드 가상 머신을 생성하기 위한 템플릿으로 사용되는 가상 머신 디스크 파일입니다.
	기본 관리 노드를 배포하기 위한 오픈 가상화 형식 템플릿 파일(".ovf") 및 매니페스트 파일(".mf")입니다.
	비기본 관리 노드를 배포하기 위한 템플릿 파일(".ovf")과 매니페스트 파일(".mf")입니다.
/vSphere/vSphere-archive.ovf./vSphere/vSphere-archive.mf	아카이브 노드 배포를 위한 템플릿 파일(".ovf")과 매니페스트 파일(".mf")입니다.
	게이트웨이 노드를 배포하기 위한 템플릿 파일(".ovf")과 매니페스트 파일(".mf")입니다.

경로 및 파일 이름입니다	설명
	가상 머신 기반 스토리지 노드 구축을 위한 템플릿 파일('.ovf') 및 매니페스트 파일('.mf')입니다.
배포 스크립팅 도구	설명
	가상 그리드 노드의 배포를 자동화하는 데 사용되는 Bash 쉘 스크립트입니다.
	'deploy-vsphere-ovftool.sh' 스크립트와 함께 사용할 구성 파일의 예.
	StorageGRID 시스템 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
	StorageGRID 어플라이언스 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/vSphere/configure -StorageGrid.sample.json을 참조하십시오	"configure-StorageGrid.py" 스크립트와 함께 사용할 구성 파일의 예
/vSphere/configure -StorageGrid.blank.json 을 참조하십시오	configure-StorageGrid.py 스크립트와 함께 사용할 빈 구성 파일입니다.
/vSphere/Extras/API-schemas	StorageGRID에 대한 API 스키마입니다. • 참고 *: 업그레이드를 수행하기 전에 이러한 스키마를 사용하여 StorageGRID 관리 API를 사용하도록 작성한 코드가 업그레이드 호환성 테스트를 위한 비프로덕션 StorageGRID 환경이 없는 경우 새 StorageGRID 릴리스와 호환되는지 확인할 수 있습니다.

1. StorageGRID 어플라이언스 기반 시스템을 확장하는 경우 해당 파일을 선택합니다.

경로 및 파일 이름입니다	설명
/debs/storagegrid-webscale-images-version-SHA.deb 를 참조하십시오	어플라이언스에 StorageGRID 노드 이미지를 설치하기 위한 DEB 패키지.

경로 및 파일 이름입니다	설명
/debs/storagegrid-webscale-images-version-SHA.deb.md5 를 참조하십시오	업로드 후 패키지가 손상되지 않았는지 확인하기 위해 StorageGRID 어플라이언스 설치 프로그램에서 사용하는 DEB 설치 패키지의 체크섬입니다.

> 어플라이언스 설치의 경우, 이러한 파일은 네트워크 트래픽을 방지해야 하는 경우에만 필요합니다. 어플라이언스는 기본 관리 노드에서 필요한 파일을 다운로드할 수 있습니다.

하드웨어 및 네트워킹을 확인합니다

StorageGRID 시스템 확장을 시작하기 전에 다음 사항을 확인하십시오.

- 새 그리드 노드 또는 새 사이트를 지원하는 데 필요한 하드웨어가 설치 및 구성되었습니다.
- 모든 새 노드에는 기존 노드와 새 노드 모두에 대한 양방향 통신 경로가 있습니다(그리드 네트워크에 대한 요구 사항).
- 기본 관리 노드는 StorageGRID 시스템을 호스트하기 위한 모든 확장 서버와 통신할 수 있습니다.
- 새 노드의 그리드 네트워크 IP 주소가 이전에 사용되지 않은 서브넷에 있는 경우 이미 있는 것입니다 새 서브넷을 추가했습니다 Grid Network 서브넷 목록으로 이동합니다. 그렇지 않으면 확장을 취소하고 새 서브넷을 추가한 다음 절차를 다시 시작해야 합니다.
- 그리드 네트워크에서 그리드 노드 간 또는 StorageGRID 사이트 간에 NAT(네트워크 주소 변환)를 사용하지 않습니다. Grid Network에 전용 IPv4 주소를 사용하는 경우, 이러한 주소는 모든 사이트의 모든 그리드 노드에서 직접 라우팅할 수 있어야 합니다. NAT를 사용하여 공용 네트워크 세그먼트에서 그리드 네트워크를 연결하는 것은 그리드의 모든 노드에 투명한 터널링 애플리케이션을 사용하는 경우에만 지원됩니다. 즉, 그리드 노드는 공용 IP 주소를 알 필요가 없습니다.

  이 NAT 제한은 그리드 노드 및 그리드 네트워크에 특정합니다. 필요한 경우 게이트웨이 노드에 대한 공용 IP 주소를 제공하는 등 외부 클라이언트와 그리드 노드 간에 NAT를 사용할 수 있습니다.

스토리지 볼륨을 추가합니다

스토리지 노드에 스토리지 볼륨을 추가합니다

스토리지 볼륨을 추가하여 스토리지 볼륨이 16개 이하인 스토리지 노드의 스토리지 용량을 확장할 수 있습니다. 복제 또는 삭제 코딩 복사본에 대한 ILM 요구 사항을 충족하려면 스토리지 볼륨을 두 개 이상의 스토리지 노드에 추가해야 할 수 있습니다.

필요한 것

스토리지 볼륨을 추가하기 전에 을 검토하십시오 오브젝트 용량 추가 지침 ILM 정책의 요구 사항을 충족하기 위해 볼륨을 추가할 위치를 알고 있어야 합니다.

> 이 지침은 소프트웨어 기반 스토리지 노드에만 적용됩니다. 을 참조하십시오 배포된 SG6060 또는 SG6060X에 확장 셸프를 추가합니다 확장 셸프를 설치하여 스토리지 볼륨을 SG6060 또는 SG6060X에 추가하는 방법에 대해 알아봅니다. 다른 어플라이언스 스토리지 노드는 확장할 수 없습니다.

이 작업에 대해

스토리지 노드의 기본 스토리지는 여러 스토리지 볼륨으로 나뉩니다. 스토리지 볼륨은 StorageGRID 시스템에서 포맷되고 객체를 저장하도록 마운트된 블록 기반 스토리지 디바이스입니다. 각 스토리지 노드는 그리드 관리자에서 _object store_라고 하는 최대 16개의 스토리지 볼륨을 지원할 수 있습니다.

> 오브젝트 메타데이터는 항상 오브젝트 저장소 0에 저장됩니다.

각 오브젝트 저장소는 해당 ID에 해당하는 볼륨에 마운트됩니다. 예를 들어, ID가 0000인 오브젝트 저장소는 '/var/local/rangedb/0' 마운트 지점에 해당합니다.

새 스토리지 볼륨을 추가하기 전에 Grid Manager를 사용하여 각 스토리지 노드의 현재 객체 저장소와 해당 마운트 지점을 확인합니다. 스토리지 볼륨을 추가할 때 이 정보를 사용할 수 있습니다.

단계

1. 노드 * > **site* * > **Storage Node* * > * Storage * 를 선택합니다.
2. 아래로 스크롤하여 각 볼륨 및 오브젝트 저장소에서 사용 가능한 스토리지 양을 확인합니다.

   어플라이언스 스토리지 노드의 경우 각 디스크의 전 세계 이름이 SANtricity 소프트웨어(어플라이언스의 스토리지 컨트롤러에 연결된 관리 소프트웨어)에서 표준 볼륨 속성을 볼 때 표시되는 볼륨 WWID(World-Wide Identifier)와 일치합니다.

   볼륨 마운트 지점과 관련된 디스크 읽기 및 쓰기 통계를 해석하려면 디스크 장치 테이블의 * 이름 * 열에 표시된 이름(즉, *sdc*, *SDD*, *SDE* 등)의 첫 번째 부분이 볼륨 테이블의 * 장치 * 열에 표시된 값과 일치합니다.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

3. 플랫폼에 대한 지침에 따라 스토리지 노드에 새 스토리지 볼륨을 추가합니다.
    - VMware: 스토리지 노드에 스토리지 볼륨을 추가합니다
    - Linux: 스토리지 노드에 직접 연결 또는 SAN 볼륨을 추가합니다

VMware: 스토리지 노드에 스토리지 볼륨을 추가합니다

스토리지 노드에 16개 미만의 스토리지 볼륨이 포함된 경우 VMware vSphere를 사용하여 볼륨을 추가하여 용량을 늘릴 수 있습니다.

필요한 것

- VMware 배포용 StorageGRID 설치 지침을 액세스할 수 있습니다.
    - VMware를 설치합니다
- "passwords.txt" 파일이 있습니다.
- 특정 액세스 권한이 있습니다.

> 소프트웨어 업그레이드, 복구 절차 또는 다른 확장 절차가 활성화되어 있는 동안에는 스토리지 노드를 스토리지 노드에 추가하지 마십시오.

이 작업에 대해

스토리지 볼륨을 추가할 때 잠시 동안 스토리지 노드를 사용할 수 없습니다. 클라이언트 대상 그리드 서비스에 영향을 주지 않도록 한 번에 하나의 스토리지 노드에서 이 절차를 수행해야 합니다.

단계

1. 필요한 경우 새 스토리지 하드웨어를 설치하고 새 VMware 데이터 저장소를 생성합니다.
2. 스토리지로 사용할 하나 이상의 하드 디스크를 가상 머신에 추가합니다(오브젝트 저장소).
    a. VMware vSphere Client를 엽니다.
    b. 가상 시스템 설정을 편집하여 하나 이상의 추가 하드 디스크를 추가합니다.

    하드 디스크는 일반적으로 VMDK(Virtual Machine Disk)로 구성됩니다. VMDK는 일반적으로 더 많이 사용되며 관리가 더 쉽지만 RDM은 더 큰 개체 크기(예: 100MB 이상)를 사용하는 워크로드에 더 나은 성능을 제공할 수 있습니다. 가상 머신에 하드 디스크를 추가하는 방법에 대한 자세한 내용은 VMware vSphere 설명서를 참조하십시오.

3. VMware vSphere Client에서 * Restart Guest OS * 옵션을 사용하거나 가상 머신에 대한 ssh 세션에 "SUDO reboot" 명령을 입력하여 가상 머신을 다시 시작합니다

    > 가상 컴퓨터를 다시 시작하기 위해 * Power Off * 또는 * Reset * 을 사용하지 마십시오.

4. 스토리지 노드에서 사용할 새 스토리지를 구성합니다.
    a. 그리드 노드에 로그인합니다.
        i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
        ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
        iii. 루트로 전환하려면 다음 명령을 입력합니다

iv. "passwords.txt" 파일에 나열된 암호를 입력합니다. 루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

b. 새 스토리지 볼륨 구성:

'SUDO ADD_Rangedbs.rb'

이 스크립트는 새 스토리지 볼륨을 찾아 포맷하라는 메시지를 표시합니다.

a. y * 를 입력하여 서식을 적용합니다.

b. 이전에 포맷된 볼륨이 있는 경우 다시 포맷할지 여부를 결정합니다.

- 다시 포맷하려면 * y * 를 입력합니다.
- 포맷을 건너뛰려면 * n * 을 입력합니다.

c. 스토리지 서비스를 중지하려면 * y * 를 입력합니다.

스토리지 서비스가 중지되고 'setup_rangedbs.sh' 스크립트가 자동으로 실행됩니다. 볼륨을 레인저로 사용할 준비가 되면 서비스가 다시 시작됩니다.

5. 서비스가 올바르게 시작되는지 점검한다.

a. 서버에 있는 모든 서비스의 상태 목록을 봅니다.

'SUDO StorageGrid - status'

상태가 자동으로 업데이트됩니다.

a. 모든 서비스가 실행 중이거나 검증될 때까지 기다립니다.

b. 상태 화면을 종료합니다.

'Ctrl+C'

6. 스토리지 노드가 온라인 상태인지 확인합니다.

a. 를 사용하여 Grid Manager에 로그인합니다 지원되는 웹 브라우저.

b. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.

c. site_ * > **Storage Node* * > * LDR * > * Storage * 를 선택합니다.

d. Configuration * 탭을 선택한 다음 * Main * 탭을 선택합니다.

e. 스토리지 상태 - 원하는 * 드롭다운 목록이 읽기 전용 또는 오프라인으로 설정된 경우 * 온라인 * 을 선택합니다.

f. Apply Changes * 를 선택합니다.

7. 새 오브젝트 저장소를 보려면 다음을 수행합니다.

a. 노드 * > **site* * > **Storage Node* * > * Storage * 를 선택합니다.

b. Object Stores * 표에서 세부 정보를 봅니다.

결과

스토리지 노드의 확장된 용량을 사용하여 오브젝트 데이터를 저장할 수 있습니다.

Linux: 스토리지 노드에 직접 연결 또는 **SAN** 볼륨을 추가합니다

스토리지 노드에 스토리지 볼륨이 16개 미만인 경우 새 블록 스토리지 디바이스를 추가하고, Linux 호스트에 표시하고, 스토리지 노드에 사용되는 StorageGRID 구성 파일에 새 블록 디바이스 매핑을 추가하여 용량을 늘릴 수 있습니다.

필요한 것

- Linux 플랫폼용 StorageGRID 설치 지침을 액세스할 수 있습니다.
  - Red Hat Enterprise Linux 또는 CentOS를 설치합니다
  - Ubuntu 또는 Debian을 설치합니다
- "passwords.txt" 파일이 있습니다.
- 특정 액세스 권한이 있습니다.

> 소프트웨어 업그레이드, 복구 절차 또는 다른 확장 절차가 활성화되어 있는 동안에는 스토리지 노드를 스토리지 노드에 추가하지 마십시오.

이 작업에 대해

스토리지 볼륨을 추가할 때 잠시 동안 스토리지 노드를 사용할 수 없습니다. 클라이언트 대상 그리드 서비스에 영향을 주지 않도록 한 번에 하나의 스토리지 노드에서 이 절차를 수행해야 합니다.

단계

1. 새 스토리지 하드웨어를 설치합니다.

   자세한 내용은 해당 하드웨어 공급업체에서 제공하는 설명서를 참조하십시오.

2. 원하는 크기의 새 블록 스토리지 볼륨을 생성합니다.
   - 새 디스크 드라이브를 연결하고 필요에 따라 RAID 컨트롤러 구성을 업데이트하거나 공유 스토리지 어레이에 새 SAN LUN을 할당하고 Linux 호스트가 액세스할 수 있도록 허용합니다.
   - 기존 스토리지 노드의 스토리지 볼륨에 사용한 것과 동일한 영구 명명 체계를 사용합니다.
   - StorageGRID 노드 마이그레이션 기능을 사용하는 경우 이 스토리지 노드의 마이그레이션 대상인 다른 Linux 호스트에 새 볼륨을 표시합니다. 자세한 내용은 Linux 플랫폼용 StorageGRID 설치 지침을 참조하십시오.
3. 스토리지 노드를 지원하는 Linux 호스트에 루트 또는 sudo 권한이 있는 계정으로 로그인합니다.
4. 새 스토리지 볼륨이 Linux 호스트에 표시되는지 확인합니다.

   장치를 다시 검색해야 할 수도 있습니다.

5. 다음 명령을 실행하여 스토리지 노드를 일시적으로 해제합니다.

   'SUDO StorageGRID node stop <node-name>'

6. vim 또는 pico와 같은 텍스트 편집기를 사용하여 "/etc/StorageGrid/nodes/<node-name>.conf"에서 찾을 수 있는 스토리지 노드의 노드 구성 파일을 편집합니다.
7. 기존 오브젝트 스토리지 블록 디바이스 매핑이 포함된 노드 구성 파일의 섹션을 찾습니다.

   이 예에서 Block_device_RANGEDB_00 과 Block_device_RANGEDB_03 사이의 블록_device_RANGEDB_00은 기존 객체 스토리지 블록 디바이스 매핑입니다.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. 이 스토리지 노드에 대해 추가한 블록 스토리지 볼륨에 해당하는 새 오브젝트 스토리지 블록 디바이스 매핑을 추가합니다.

   다음 'BLOCK_DEVICE_RANGEDB_nn'에서 시작해야 합니다. 간격을 두지 마십시오.

   - 위의 예제를 토대로 블록_디바이스_RANGEDB_04'에서 시작합니다.
   - 아래 예에서는 Block_device_RANGEDB_07 노드에 Block_device_RANGEDB_04 라는 4개의 새 블록 스토리지 볼륨이 추가되었습니다.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. 다음 명령을 실행하여 스토리지 노드의 노드 구성 파일에 대한 변경 내용을 검증합니다.

   'SUDO StorageGRID node validate <node-name>'

다음 단계로 진행하기 전에 오류 또는 경고를 모두 해결하십시오.

> 다음과 같은 오류가 발생하면 노드 구성 파일이 '<purpose>'에 사용되는 블록 디바이스를 Linux 파일 시스템의 지정된 '<path-name>'에 매핑하려고 시도하고 있음을 의미합니다. 그러나 해당 위치에 유효한 블록 장치 특수 파일(또는 블록 장치 특수 파일에 대한 소프트링크)이 없습니다.
>
> ```
> Checking configuration file for node <node-name>…
> ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
> <path-name> is not a valid block device
> ```
>
> 올바른 '<path-name>'을(를) 입력했는지 확인하십시오.

10. 다음 명령을 실행하여 새 블록 디바이스 매핑이 있는 노드를 다시 시작합니다.

    'SUDO StorageGRID node start <node-name>'

11. "passwords.txt" 파일에 나열된 암호를 사용하여 스토리지 노드에 admin으로 로그인합니다.
12. 서비스가 올바르게 시작되는지 점검한다.
    a. 서버에 있는 모든 서비스의 상태 목록을 봅니다. + sudo StorageGrid - status

       상태가 자동으로 업데이트됩니다.

    b. 모든 서비스가 실행 중이거나 검증될 때까지 기다립니다.
    c. 상태 화면을 종료합니다.

       'Ctrl+C'

13. 스토리지 노드에서 사용할 새 스토리지를 구성합니다.
    a. 새 스토리지 볼륨 구성:

       'SUDO ADD_Rangedbs.rb'

    이 스크립트는 새 스토리지 볼륨을 찾아 포맷하라는 메시지를 표시합니다.

    a. 스토리지 볼륨을 포맷하려면 * y * 를 입력합니다.
    b. 이전에 포맷된 볼륨이 있는 경우 다시 포맷할지 여부를 결정합니다.
       - 다시 포맷하려면 * y * 를 입력합니다.
       - 포맷을 건너뛰려면 * n * 을 입력합니다.
    c. 스토리지 서비스를 중지하려면 * y * 를 입력합니다.

       스토리지 서비스가 중지되고 'setup_rangedbs.sh' 스크립트가 자동으로 실행됩니다. 볼륨을 레인저로 사용할 준비가 되면 서비스가 다시 시작됩니다.

14. 서비스가 올바르게 시작되는지 점검한다.
    a. 서버에 있는 모든 서비스의 상태 목록을 봅니다.

'SUDO StorageGrid - status'

상태가 자동으로 업데이트됩니다.

a. 모든 서비스가 실행 중이거나 검증될 때까지 기다립니다.
b. 상태 화면을 종료합니다.

'Ctrl+C'

15. 스토리지 노드가 온라인 상태인지 확인합니다.
    a. 를 사용하여 Grid Manager에 로그인합니다 지원되는 웹 브라우저.
    b. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
    c. site_ * > **Storage Node* * > * LDR * > * Storage * 를 선택합니다.
    d. Configuration * 탭을 선택한 다음 * Main * 탭을 선택합니다.
    e. 스토리지 상태 - 원하는 * 드롭다운 목록이 읽기 전용 또는 오프라인으로 설정된 경우 * 온라인 * 을 선택합니다.
    f. 변경 내용 적용 * 을 클릭합니다.
16. 새 오브젝트 저장소를 보려면 다음을 수행합니다.
    a. 노드 * > **site* * > **Storage Node* * > * Storage * 를 선택합니다.
    b. Object Stores * 표에서 세부 정보를 봅니다.

결과

이제 스토리지 노드의 확장된 용량을 사용하여 오브젝트 데이터를 저장할 수 있습니다.

그리드 노드 또는 사이트를 추가합니다

기존 사이트에 그리드 노드를 추가하거나 새 사이트를 추가합니다

다음 절차에 따라 그리드 노드를 기존 사이트에 추가하거나 새 사이트를 추가할 수 있지만 두 가지 유형의 확장을 동시에 수행할 수는 없습니다.

필요한 것

- 루트 액세스 또는 유지 관리 권한이 있습니다.
- 그리드의 모든 기존 노드가 모든 사이트에서 실행 및 실행됩니다.
- 이전의 모든 확장, 업그레이드, 사용 중단 또는 복구 절차가 완료되었습니다.

> 다른 확장, 업그레이드, 복구 또는 활성 서비스 해제 절차가 진행 중인 동안에는 확장을 시작할 수 없습니다. 그러나 필요한 경우 서비스 해제 절차를 일시 중지하여 확장을 시작할 수 있습니다.

단계

1. 그리드 네트워크에 대한 서브넷을 업데이트합니다.
2. 새 그리드 노드를 배포합니다.
3. 확장을 수행합니다.

그리드 네트워크에 대한 서브넷을 업데이트합니다

확장 시 그리드 노드 또는 새 사이트를 추가할 때 그리드 네트워크에 서브넷을 업데이트하거나 추가해야 할 수 있습니다.

StorageGRID는 그리드 네트워크(eth0)의 그리드 노드 간에 통신하는 데 사용되는 네트워크 서브넷 목록을 유지합니다. 이러한 항목에는 StorageGRID 시스템의 각 사이트에서 그리드 네트워크에 사용되는 서브넷과 그리드 네트워크 게이트웨이를 통해 액세스되는 NTP, DNS, LDAP 또는 기타 외부 서버에 사용되는 서브넷이 포함됩니다.

필요한 것

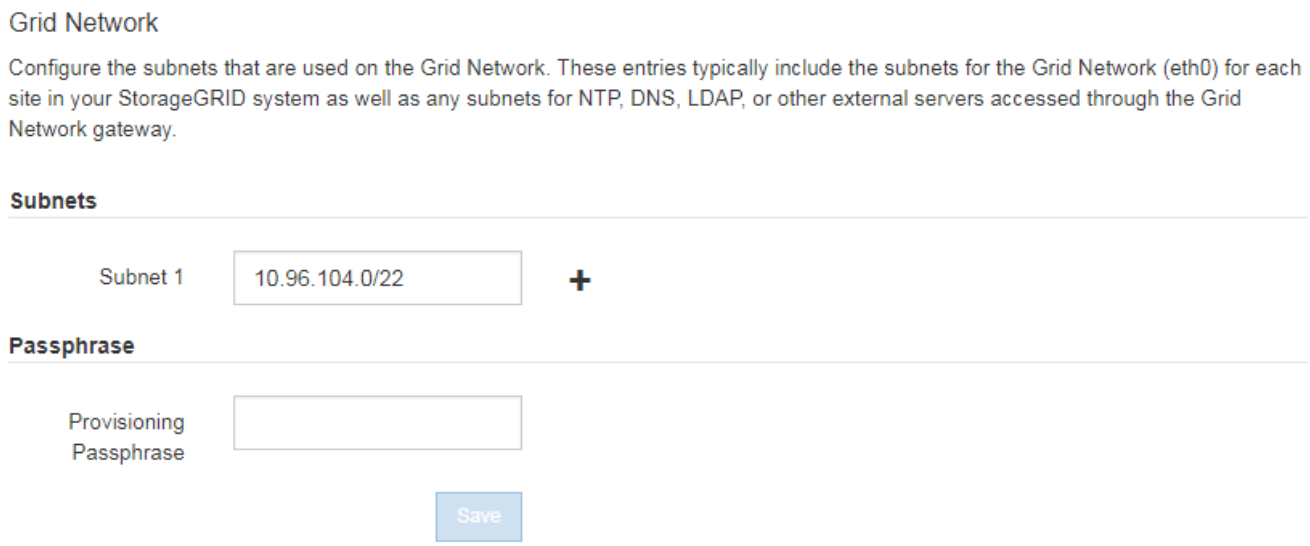
- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 프로비저닝 암호가 있습니다.
- 구성할 서브넷의 네트워크 주소(CIDR 표기법)가 있습니다.

이 작업에 대해

새 노드의 그리드 네트워크 IP 주소가 이전에 사용되지 않은 서브넷에 있는 경우 확장을 시작하기 전에 그리드 네트워크 서브넷 목록에 새 서브넷을 추가해야 합니다. 그렇지 않으면 확장을 취소하고 새 서브넷을 추가한 다음 절차를 다시 시작해야 합니다.

단계

1. 유지보수 * > * 네트워크 * > * 그리드 네트워크 * 를 선택합니다.



2. 서브넷 목록에서 더하기 기호를 선택하여 CIDR 표기법으로 새 서브넷을 추가합니다.

   예를 들어 10.96.104.0/22를 입력합니다.

3. 프로비저닝 암호를 입력하고 * Save * 를 선택합니다.

   지정한 서브넷은 StorageGRID 시스템에 대해 자동으로 구성됩니다.

확장 시 새 그리드 노드를 구축하는 단계는 그리드를 처음 설치할 때 사용한 단계와 동일합니다. 확장을 수행하려면 먼저 모든 새 그리드 노드를 배포해야 합니다.

그리드를 확장하면 추가하는 노드가 기존 노드 유형과 일치하지 않아도 됩니다. VMware 노드, Linux 컨테이너 기반 노드 또는 어플라이언스 노드를 추가할 수 있습니다.

VMware: 그리드 노드를 구축합니다

확장에 추가할 각 VMware 노드에 대해 VMware vSphere에 가상 머신을 구축해야 합니다.

단계

1. 새 노드를 가상 머신으로 구축합니다 하나 이상의 StorageGRID 네트워크에 연결합니다.

   노드를 배포할 때 선택적으로 노드 포트를 재매핑하거나 CPU 또는 메모리 설정을 늘릴 수 있습니다.

2. 새 VMware 노드를 모두 구축한 후 확장 절차를 수행합니다.

Linux: 그리드 노드 배포

그리드 노드는 새 Linux 호스트 또는 기존 Linux 호스트에 배포할 수 있습니다. 그리드에 추가하려는 StorageGRID 노드의 CPU, RAM 및 스토리지 요구 사항을 지원하기 위해 추가 Linux 호스트가 필요한 경우 호스트를 처음 설치할 때와 동일한 방법으로 준비합니다. 그런 다음 설치 중에 그리드 노드를 구축하는 것과 동일한 방식으로 확장 노드를 배포합니다.

필요한 것

- 사용 중인 Linux 버전에 대한 StorageGRID 설치 지침이 있으며 하드웨어 및 스토리지 요구 사항을 검토했습니다.
  - Red Hat Enterprise Linux 또는 CentOS를 설치합니다
  - Ubuntu 또는 Debian을 설치합니다
- 기존 호스트에 새 그리드 노드를 배포하려는 경우 기존 호스트에 추가 노드에 대한 CPU, RAM 및 스토리지 용량이 충분한지 확인했습니다.
- 장애 도메인을 최소화할 계획이 있습니다. 예를 들어, 단일 물리적 호스트에 모든 게이트웨이 노드를 배포해서는 안 됩니다.

> 운영 구축 시 단일 물리적 호스트 또는 가상 호스트에서 스토리지 노드를 두 개 이상 실행하지 마십시오. 각 스토리지 노드에 대해 전용 호스트를 사용하면 격리된 장애 도메인이 제공됩니다.

- StorageGRID 노드에서 NetApp ONTAP 시스템에서 할당된 스토리지를 사용하는 경우 볼륨에 FabricPool 계층화 정책이 활성화되어 있지 않은지 확인합니다. StorageGRID 노드와 함께 사용되는 볼륨에 대해 FabricPool 계층화를 사용하지 않도록 설정하면 문제 해결과 스토리지 작업이 간소화됩니다.

단계

1. 새 호스트를 추가하는 경우 StorageGRID 노드 구축을 위한 설치 지침에 액세스합니다.
2. 새 호스트를 구축하려면 호스트 준비 지침을 따르십시오.
3. 노드 구성 파일을 생성하고 StorageGRID 구성을 검증하려면 그리드 노드 배포 지침을 따르십시오.
4. 새 Linux 호스트에 노드를 추가하는 경우 StorageGRID 호스트 서비스를 시작합니다.

5. 기존 Linux 호스트에 노드를 추가하는 경우 StorageGRID 호스트 서비스 CLI를 사용하여 새 노드를 시작합니다. "'SUDO StorageGRID node start[<node name\>]"

작업을 마친 후

새 그리드 노드를 모두 구축한 후에는 을(를) 사용할 수 있습니다 확장을 수행합니다.

어플라이언스: 스토리지, 게이트웨이 또는 비 기본 관리 노드 배포

어플라이언스 노드에 StorageGRID 소프트웨어를 설치하려면 어플라이언스에 포함된 StorageGRID 어플라이언스 설치 프로그램을 사용합니다. 확장 시 각 스토리지 어플라이언스는 단일 스토리지 노드로 작동하며, 각 서비스 어플라이언스는 단일 게이트웨이 노드 또는 비기본 관리 노드로 작동합니다. 모든 어플라이언스는 그리드 네트워크, 관리 네트워크 및 클라이언트 네트워크에 연결할 수 있습니다.

필요한 것

- 이 제품은 랙 또는 캐비닛에 설치되었고 네트워크에 연결되어 있으며 전원이 켜져 있습니다.
- StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스 설치 및 유지 관리 지침의 모든 ""하드웨어 구성" 단계를 완료했습니다.
  - SG100 및 SG1000 서비스 어플라이언스
  - 하드웨어 구성(SG5600)
  - 하드웨어 구성(SG5700)
  - 하드웨어 구성(SG6000)

  어플라이언스 하드웨어 구성에는 StorageGRID 연결(네트워크 링크 및 IP 주소)을 구성하는 데 필요한 단계와 노드 암호화 활성화, RAID 모드 변경 및 네트워크 포트 재매핑을 위한 선택적 단계가 포함됩니다.
- StorageGRID 어플라이언스 설치 프로그램의 IP 구성 페이지에 나열된 모든 그리드 네트워크 서브넷은 기본 관리 노드의 그리드 네트워크 서브넷 목록에 정의되어 있습니다.
- 교체 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램 펌웨어는 현재 그리드에서 실행 중인 StorageGRID 소프트웨어 버전과 호환됩니다. 예를 들어, StorageGRID 어플라이언스 설치 프로그램의 버전 3.6은 StorageGRID 버전 11.6과 호환됩니다. (버전이 호환되지 않는 경우 StorageGRID 어플라이언스 설치 프로그램 펌웨어를 업그레이드해야 합니다.)
- 에 서비스 랩톱이 있습니다 지원되는 웹 브라우저.
- 어플라이언스의 컴퓨팅 컨트롤러에 할당된 IP 주소 중 하나를 알고 있습니다. 연결된 모든 StorageGRID 네트워크에 대해 IP 주소를 사용할 수 있습니다.

이 작업에 대해

어플라이언스 노드에 StorageGRID를 설치하는 과정은 다음과 같습니다.

- 기본 관리 노드의 IP 주소와 어플라이언스 노드의 이름을 지정하거나 확인합니다.
- 설치를 시작하고 볼륨이 구성되고 소프트웨어가 설치될 때까지 기다립니다.

  어플라이언스 설치 작업이 중간에 중지되면 설치가 일시 중지됩니다. 설치를 다시 시작하려면 그리드 관리자에 로그인하고 모든 그리드 노드를 승인하고 StorageGRID 설치 프로세스를 완료합니다.

> 한 번에 여러 어플라이언스 노드를 구축해야 하는 경우 'configure-sGA.py' 어플라이언스 설치 스크립트를 사용하여 설치 프로세스를 자동화할 수 있습니다.

단계

1. 브라우저를 열고 어플라이언스의 컴퓨팅 컨트롤러에 대한 IP 주소 중 하나를 입력합니다.

   "https://*Controller_IP*:8443`

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. Primary Admin Node* 연결 섹션에서 기본 관리 노드의 IP 주소를 지정해야 하는지 여부를 확인합니다.

   이전에 이 데이터 센터에 다른 노드를 설치한 경우 StorageGRID 어플라이언스 설치 관리자는 기본 관리 노드 또는 admin_IP가 구성된 다른 그리드 노드가 동일한 서브넷에 있다고 가정하여 이 IP 주소를 자동으로 검색할 수 있습니다.

3. 이 IP 주소가 표시되지 않거나 변경해야 하는 경우 주소를 지정합니다.

옵션을 선택합니다	설명
수동 IP 입력	a. 관리자 노드 검색 사용 * 확인란의 선택을 취소합니다. b. IP 주소를 수동으로 입력합니다. c. 저장 * 을 클릭합니다. d. 새 IP 주소가 준비될 때까지 연결 상태를 기다립니다.
연결된 모든 운영 관리 노드의 자동 검색	a. 관리자 노드 검색 사용 * 확인란을 선택합니다. b. 검색된 IP 주소 목록이 표시될 때까지 기다립니다. c. 이 어플라이언스 스토리지 노드를 구축할 그리드의 기본 관리 노드를 선택합니다. d. 저장 * 을 클릭합니다. e. 새 IP 주소가 준비될 때까지 연결 상태를 기다립니다.

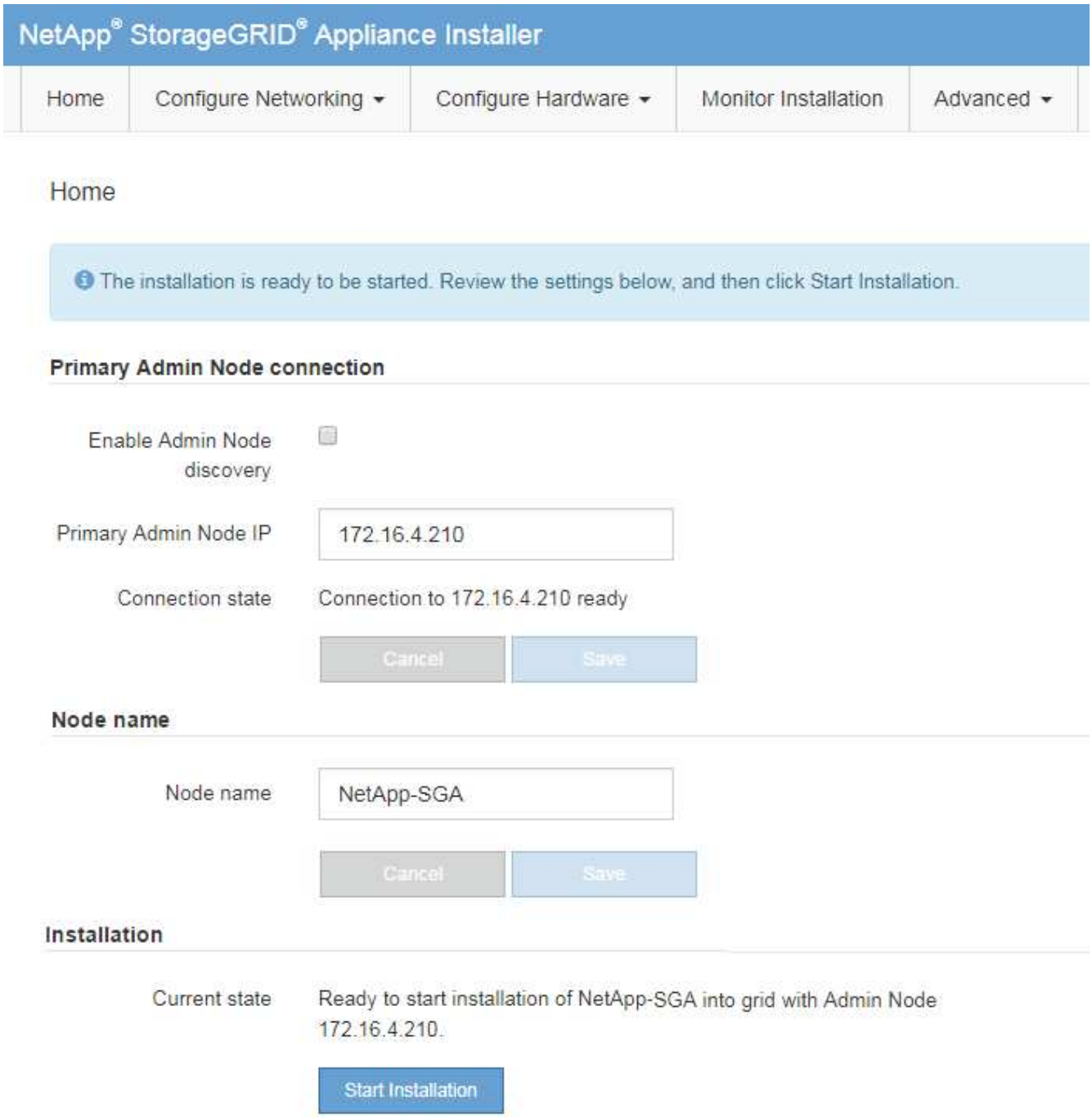
4. 노드 이름 * 필드에 이 어플라이언스 노드에 사용할 이름을 입력하고 * 저장 * 을 선택합니다.

   노드 이름은 StorageGRID 시스템의 이 어플라이언스 노드에 할당됩니다. 그리드 관리자의 노드 페이지(개요 탭)에 표시됩니다. 필요한 경우 노드를 승인할 때 이름을 변경할 수 있습니다.

5. 설치 * 섹션에서 현재 상태가 "'기본 Admin Node_admin_IP_'을(를) 사용하여_node name_을(를) 그리드에 설치할 준비가 되었으며 * 설치 시작 * 버튼이 활성화되어 있는지 확인합니다.

   설치 시작 * 버튼이 활성화되지 않은 경우 네트워크 구성 또는 포트 설정을 변경해야 할 수 있습니다. 자세한 내용은 제품의 설치 및 유지보수 지침을 참조하십시오.

6. StorageGRID 어플라이언스 설치 관리자 홈 페이지에서 * 설치 시작 * 을 선택합니다.



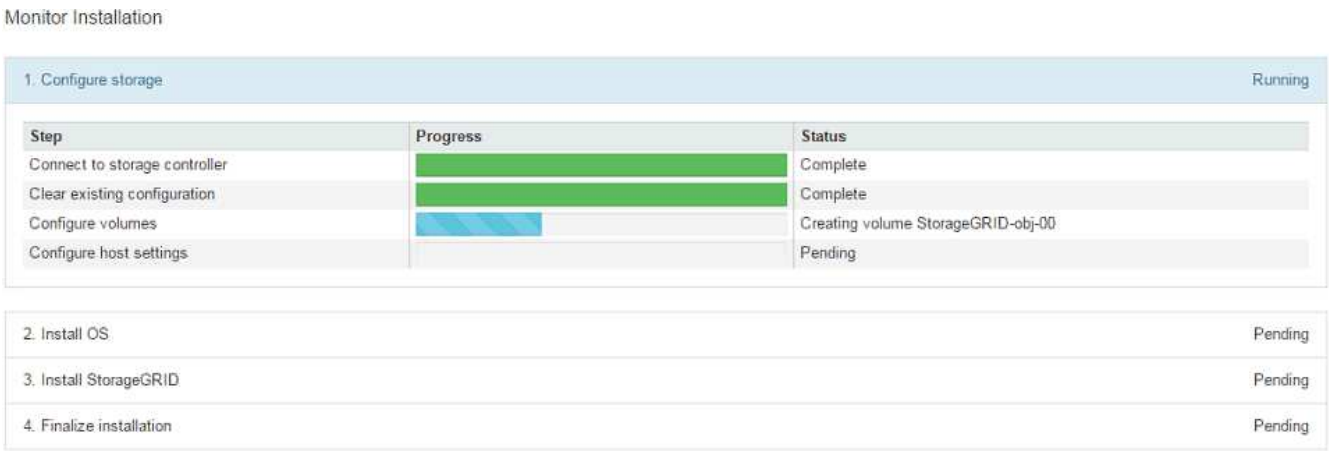
현재 상태가 ""설치 진행 중""으로 변경되고 모니터 설치 페이지가 표시됩니다.

7. 확장에 여러 어플라이언스 노드가 포함된 경우 각 어플라이언스에 대해 이전 단계를 반복합니다.

> 여러 어플라이언스 스토리지 노드를 한 번에 배포해야 하는 경우 configure-sga.py 어플라이언스 설치 스크립트를 사용하여 설치 프로세스를 자동화할 수 있습니다.

8. 모니터 설치 페이지에 수동으로 액세스해야 하는 경우 메뉴 모음에서 * 모니터 설치 * 를 선택합니다.

   Monitor Installation(모니터 설치) 페이지에 설치 진행률이 표시됩니다.



파란색 상태 표시줄은 현재 진행 중인 작업을 나타냅니다. 녹색 상태 표시줄은 성공적으로 완료된 작업을 나타냅니다.

> 설치 프로그램은 이전 설치에서 완료된 작업이 다시 실행되지 않도록 합니다. 설치를 다시 실행할 경우 다시 실행할 필요가 없는 작업은 녹색 상태 표시줄과 "중단" 상태로 표시됩니다.

9. 처음 두 설치 단계의 진행 상황을 검토합니다.
   - 1. 어플라이언스 구성 *

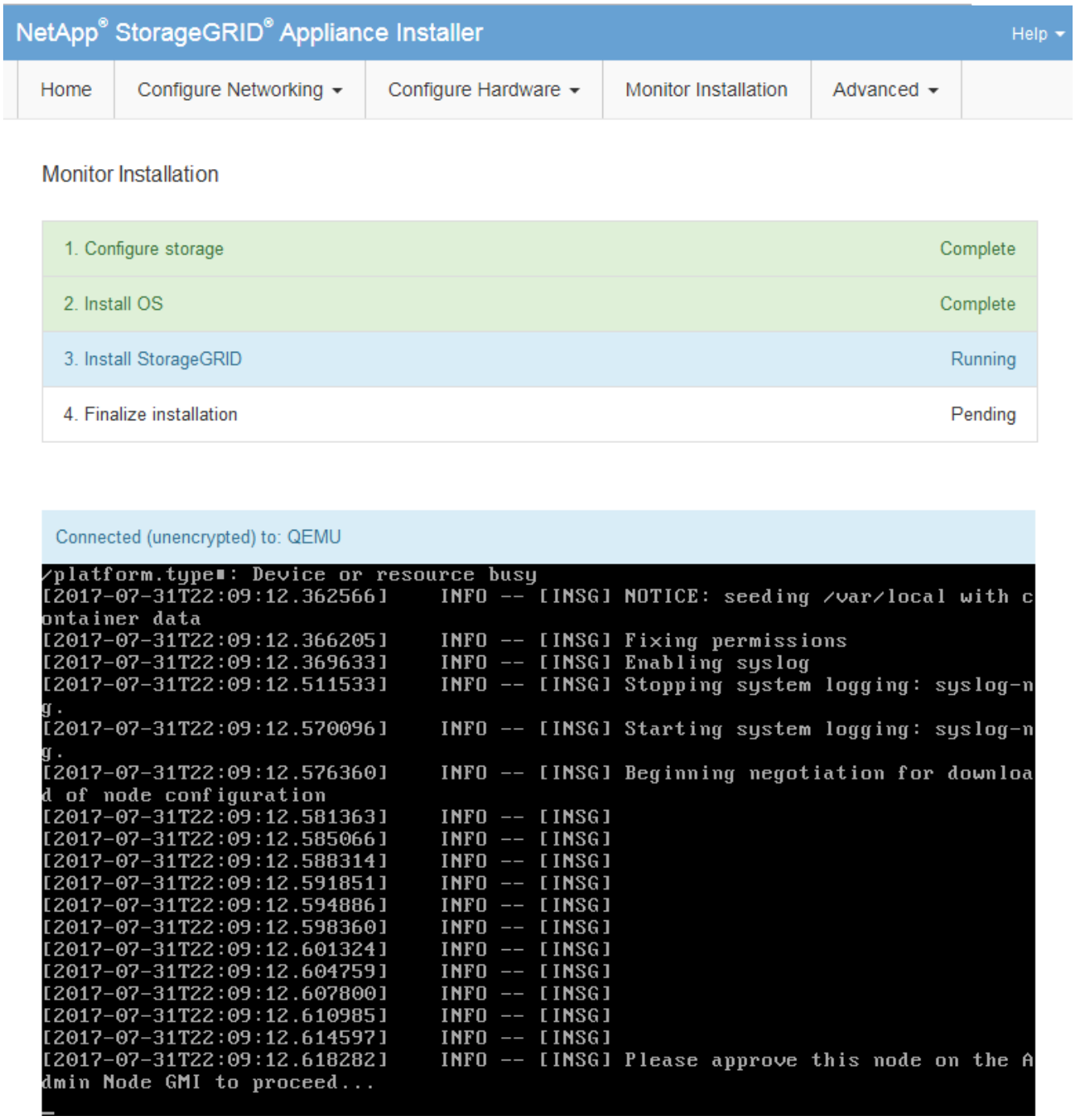
     이 단계에서 다음 프로세스 중 하나가 발생합니다.

     - 스토리지 어플라이언스의 경우 설치 프로그램이 스토리지 컨트롤러에 연결하고, 기존 구성을 지우고, SANtricity 소프트웨어와 통신하여 볼륨을 구성하고, 호스트 설정을 구성합니다.
     - 서비스 어플라이언스의 경우 설치 프로그램이 컴퓨팅 컨트롤러의 드라이브에서 기존 구성을 지우고 호스트 설정을 구성합니다.
   - 2. OS * 를 설치합니다

   이 단계에서 설치 프로그램은 StorageGRID의 기본 운영 체제 이미지를 어플라이언스에 복사합니다.

10. 그리드 관리자를 사용하여 노드를 승인하라는 메시지가 콘솔 창에 나타날 때까지 설치 진행 상태를 계속 모니터링합니다.

> 이 확장에서 추가한 모든 노드가 승인을 받을 준비가 될 때까지 기다린 다음 그리드 관리자로 이동하여 노드를 승인합니다.



확장을 수행합니다

확장을 수행하면 새 그리드 노드가 기존 StorageGRID 배포에 추가됩니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 프로비저닝 암호가 있습니다.
- 이 확장에서 추가되는 모든 그리드 노드를 배포했습니다.

- 스토리지 노드를 추가하는 경우 복구의 일부로 수행된 모든 데이터 복구 작업이 완료되었음을 확인했습니다. 을 참조하십시오 데이터 복구 작업을 확인합니다.
- 새 사이트를 추가하는 경우 확장 절차를 시작하기 전에 ILM 규칙을 검토 및 업데이트하여 확장이 완료될 때까지 개체 복사본이 새 사이트에 저장되지 않도록 해야 합니다. 예를 들어 규칙이 기본 스토리지 풀(모든 스토리지 노드)을 사용하는 경우 기존 스토리지 노드만 포함하는 새 스토리지 풀을 생성하고 ILM 규칙을 업데이트하여 새 스토리지 풀을 사용해야 합니다. 그렇지 않으면 해당 사이트의 첫 번째 노드가 활성 상태가 되는 즉시 새 사이트에 개체가 복사됩니다. 의 지침을 참조하십시오 ILM을 사용하여 개체 관리.

이 작업에 대해

확장을 수행하는 단계에는 다음 단계가 포함됩니다.

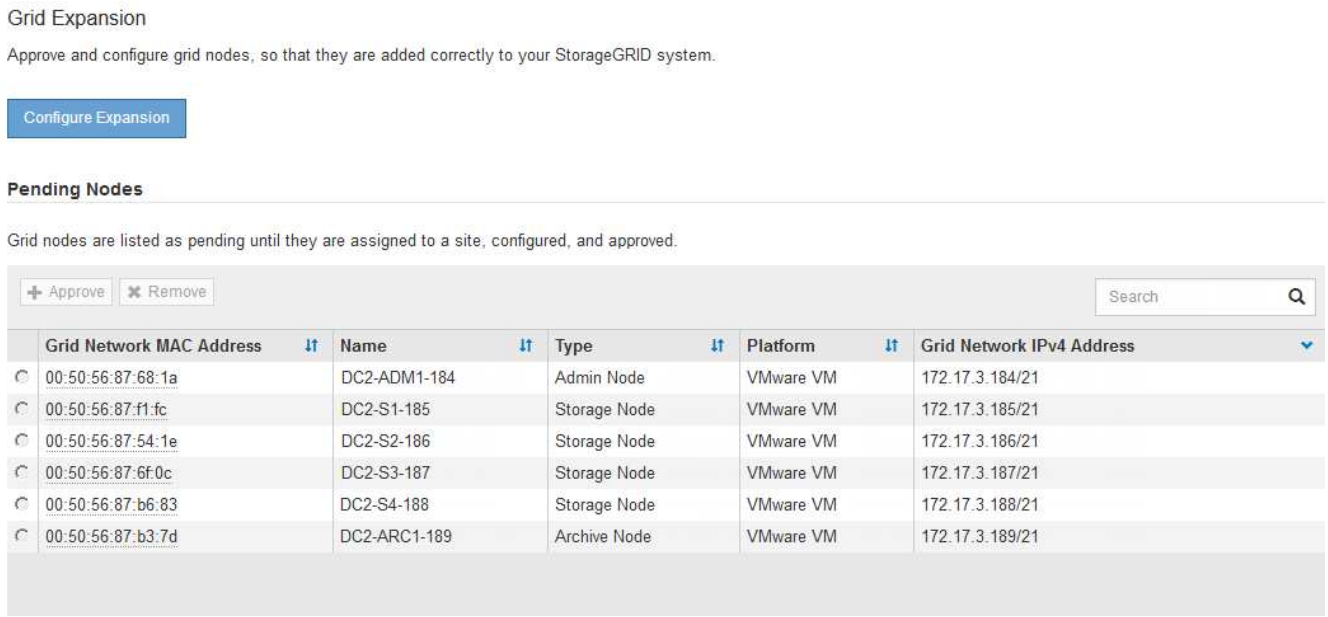
1. 새 그리드 노드를 추가할지 새 사이트를 추가할지 지정하고 추가할 그리드 노드를 승인하여 확장을 구성합니다.
2. 확장을 시작합니다.
3. 확장 프로세스가 실행되는 동안 새 복구 패키지 파일을 다운로드합니다.
4. 자동으로 실행되는 그리드 구성 단계의 상태를 모니터링합니다. 단계 집합은 추가할 그리드 노드의 유형과 새 사이트를 추가하는지 여부에 따라 달라집니다.

> 일부 단계는 큰 그리드에서 실행하는 데 상당한 시간이 걸릴 수 있습니다. 예를 들어 Cassandra를 새 스토리지 노드로 스트리밍하는 데 Cassandra 데이터베이스가 비어 있는 경우 몇 분 밖에 걸리지 않습니다. 하지만 Cassandra 데이터베이스에 많은 양의 개체 메타데이터가 있는 경우, 이 단계에서는 몇 시간 이상이 걸릴 수 있습니다. "Cassandra 클러스터 확장" 또는 "Cassandra 및 스트리밍 데이터 시작" 단계에서 스토리지 노드를 재부팅하지 마십시오.

단계

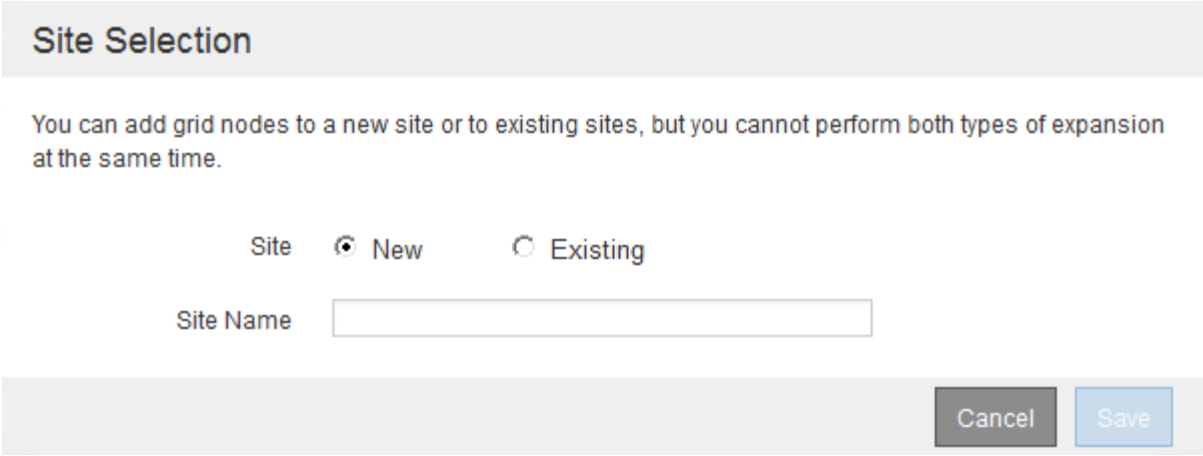
1. 유지보수 * > * 작업 * > * 확장 * 을 선택합니다.

   그리드 확장 페이지가 나타납니다. 보류 중인 노드 섹션에는 추가할 준비가 된 모든 노드가 나열됩니다.



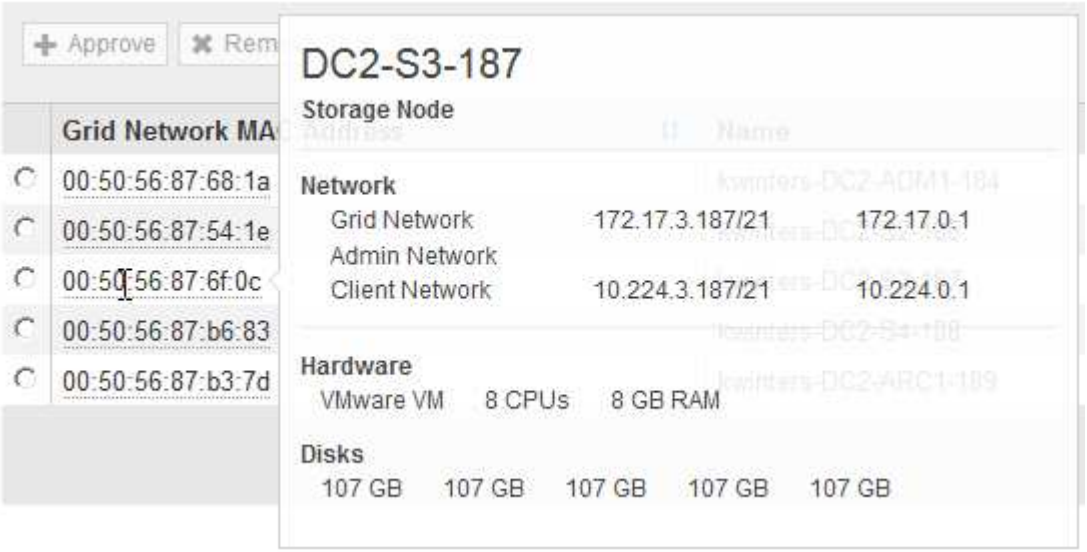
2. Configure Expansion * 을 선택합니다.

   사이트 선택 대화 상자가 나타납니다.



3. 시작할 확장 유형을 선택합니다.
   - 새 사이트를 추가하는 경우 * New * 를 선택하고 새 사이트의 이름을 입력합니다.
   - 기존 사이트에 그리드 노드를 추가하는 경우 * 기존 * 를 선택합니다.
4. 저장 * 을 선택합니다.
5. Pending Nodes * 목록을 검토하고 배포한 모든 그리드 노드가 표시되는지 확인합니다.

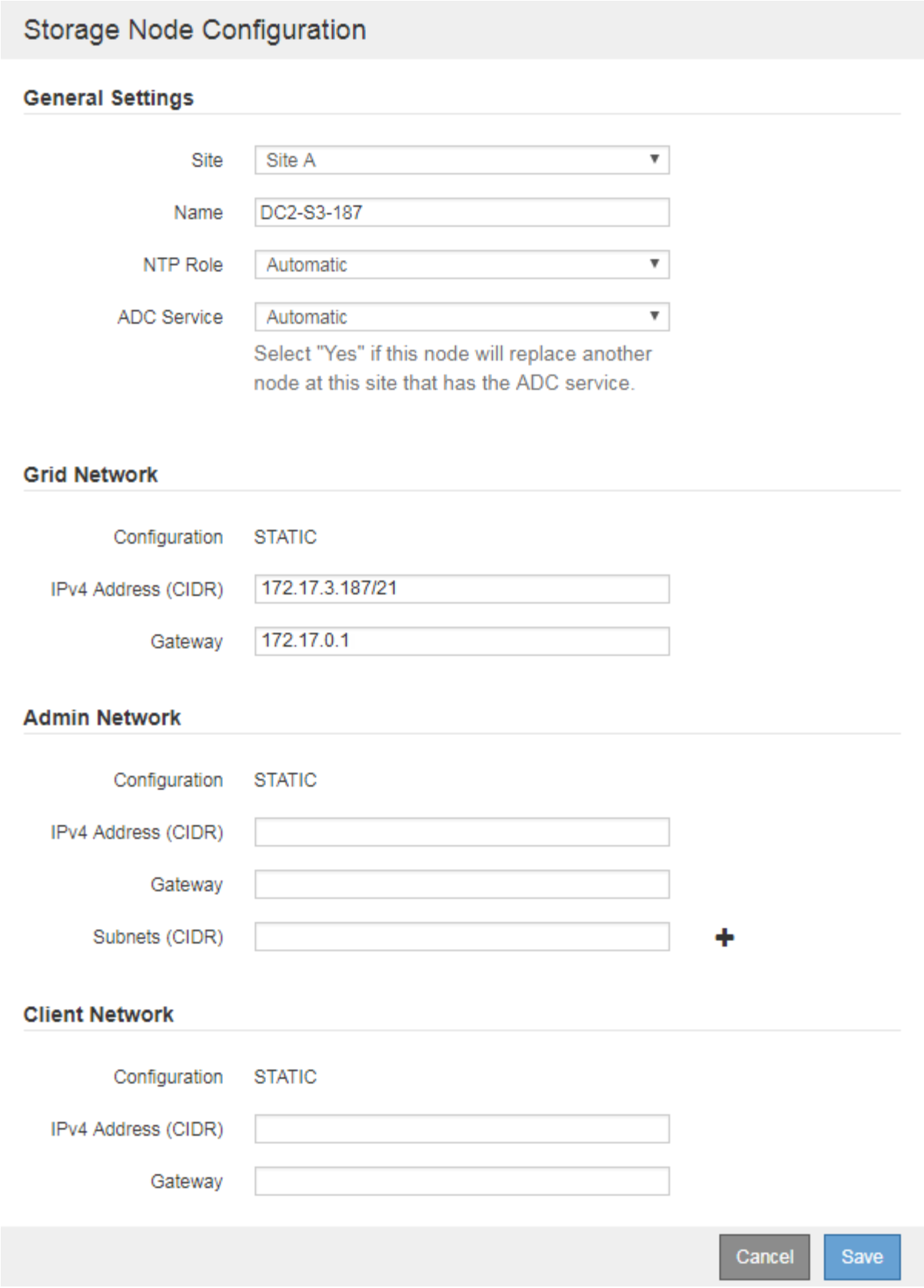
   필요한 경우 노드의 * Grid Network MAC Address * 에 커서를 올려 놓으면 해당 노드에 대한 세부 정보를 볼 수 있습니다.



> 그리드 노드가 누락된 경우 성공적으로 배포되었는지 확인합니다.

6. 보류 중인 노드 목록에서 이 확장에 대한 그리드 노드를 승인합니다.
   a. 승인하려는 첫 번째 보류 중인 그리드 노드 옆에 있는 라디오 버튼을 선택합니다.
   b. Approve * 를 선택합니다.

      그리드 노드 구성 양식이 나타납니다.



c. 필요에 따라 일반 설정을 수정합니다.

- * Site *: 그리드 노드가 연결될 사이트의 이름입니다. 여러 노드를 추가하는 경우 각 노드에 대해 올바른 사이트를 선택해야 합니다. 새 사이트를 추가하는 경우 모든 노드가 새 사이트에 추가됩니다.

- * 이름 *: 노드에 할당될 호스트 이름 및 그리드 관리자에 표시될 이름입니다.
- * NTP 역할 *: 그리드 노드의 NTP(Network Time Protocol) 역할입니다. 옵션은 * 자동 *, * 기본 * 및 * 클라이언트 * 입니다. Automatic * 을 선택하면 기본 역할이 관리 노드, ADC 서비스가 있는 스토리지 노드, 게이트웨이 노드 및 비정적 IP 주소가 있는 모든 그리드 노드에 할당됩니다. 다른 모든 그리드 노드에는 클라이언트 역할이 할당됩니다.

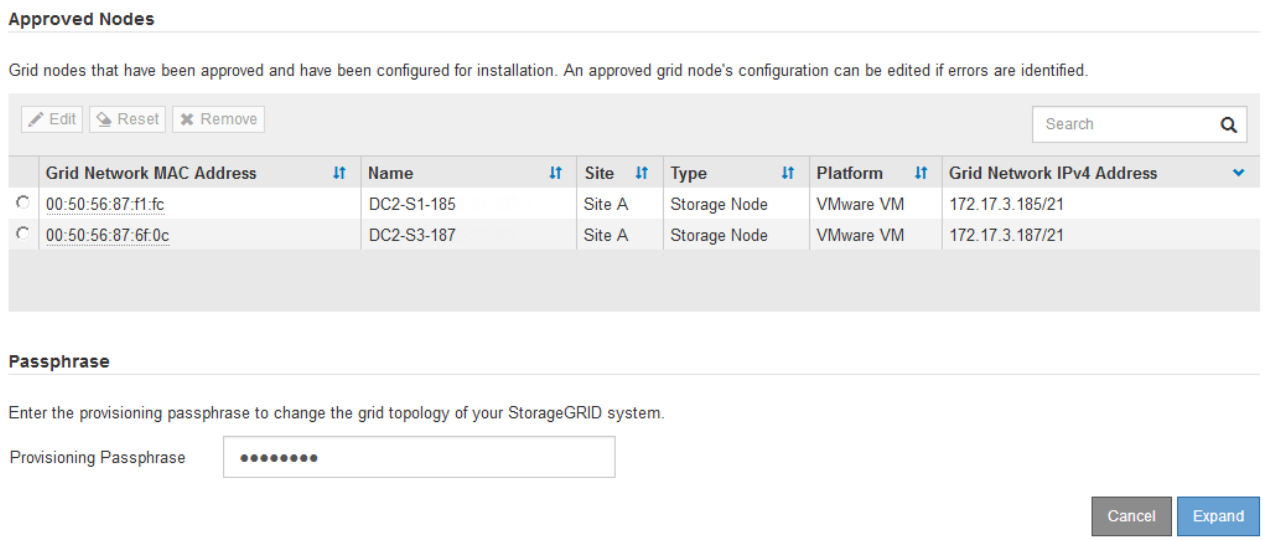
> 각 사이트에서 최소 2개의 노드에 기본 NTP 역할을 할당합니다. 이를 통해 외부 타이밍 소스에 대한 중복 시스템 액세스를 제공합니다.

- * ADC 서비스 * (스토리지 노드 전용): 이 스토리지 노드가 관리 도메인 컨트롤러(ADC) 서비스를 실행할지 여부를 나타냅니다. ADC 서비스는 그리드 서비스의 위치 및 가용성을 추적합니다. 각 사이트에 적어도 3개의 스토리지 노드가 ADC 서비스를 포함해야 합니다. ADC 서비스를 배포한 후에는 노드에 추가할 수 없습니다.
  - 스토리지 노드를 교체하기 위해 이 노드를 추가하는 경우 교체할 노드에 ADC 서비스가 포함된 경우 * 예 * 를 선택합니다. 너무 적은 ADC 서비스가 남아 있는 경우 스토리지 노드를 해제할 수 없으므로 이전 서비스를 제거하기 전에 새 ADC 서비스를 사용할 수 있습니다.
  - 그렇지 않으면 * Automatic * 을 선택하여 시스템이 이 노드에 ADC 서비스가 필요한지 여부를 결정합니다. ADC 쿼럼에 대해 알아보십시오 여기.

d. 필요에 따라 그리드 네트워크, 관리자 네트워크 및 클라이언트 네트워크에 대한 설정을 수정합니다.
   - * IPv4 주소(CIDR) *: 네트워크 인터페이스의 CIDR 네트워크 주소입니다. 예: 172.16.10.100/24
   - * 게이트웨이 *: 그리드 노드의 기본 게이트웨이입니다. 예: 172.16.10.1
   - * 서브넷(CIDR) *: 관리 네트워크에 대한 하나 이상의 하위 네트워크.

e. 저장 * 을 선택합니다.

승인된 그리드 노드는 승인된 노드 목록으로 이동합니다.



- 승인된 그리드 노드의 속성을 수정하려면 해당 라디오 버튼을 선택하고 * Edit * 를 선택합니다.
- 승인된 그리드 노드를 다시 Pending Nodes 목록으로 이동하려면 해당 라디오 버튼을 선택하고 * Reset * 을 선택합니다.
- 승인된 그리드 노드를 영구적으로 제거하려면 노드 전원을 끕니다. 그런 다음 해당 라디오 버튼을 선택하고 * 제거 * 를 선택합니다.

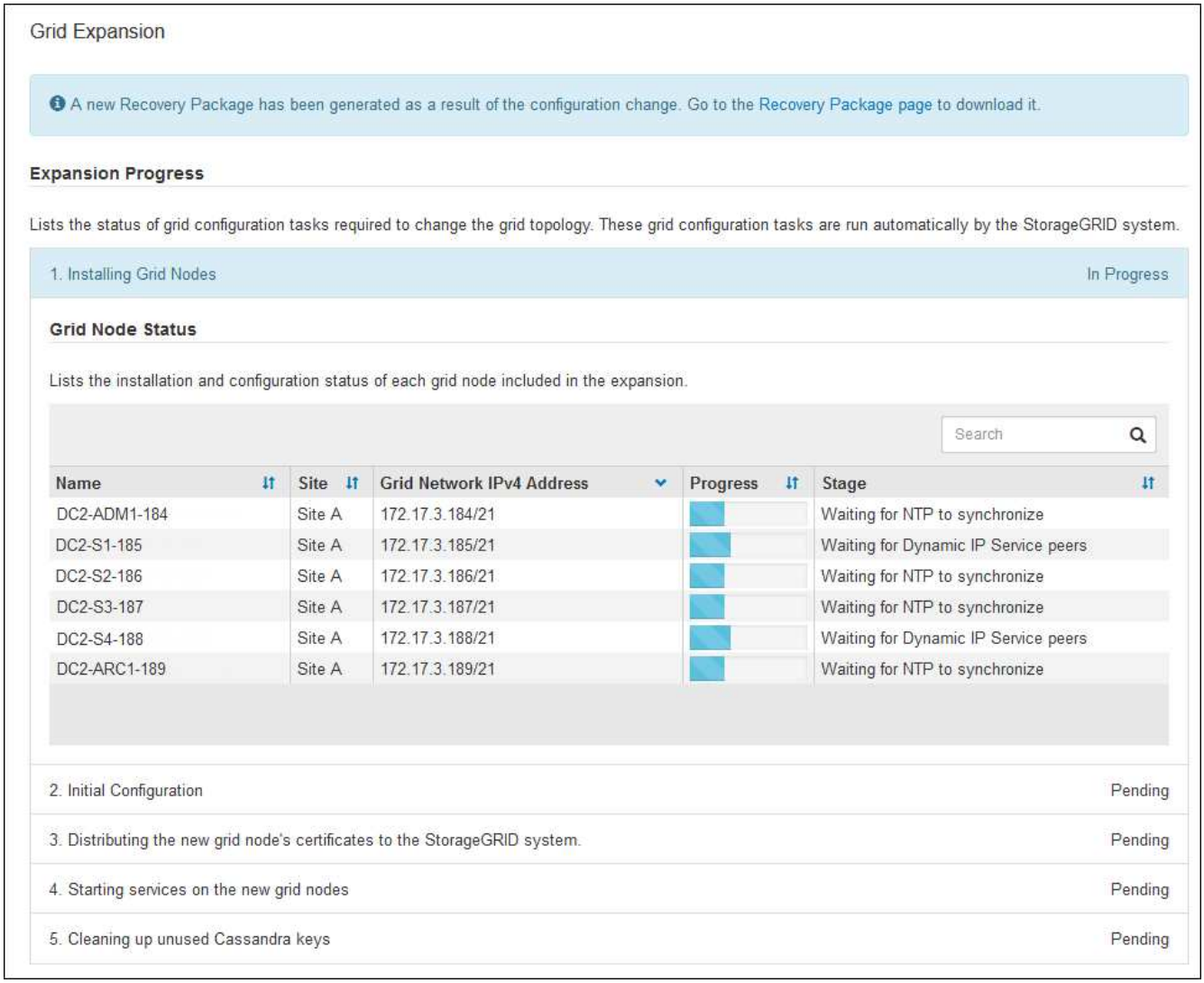
f. 승인하려는 보류 중인 각 그리드 노드에 대해 이 단계를 반복합니다.

> 가능한 경우 보류 중인 모든 그리드 노트를 승인하고 단일 확장을 수행해야 합니다. 여러 개의 소규모 확장을 수행하는 경우 더 많은 시간이 필요합니다.

7. 모든 그리드 노드를 승인하면 * Provisioning Passphrase * 를 입력하고 * Expand * 를 선택합니다.

   몇 분 후 이 페이지가 업데이트되어 확장 절차의 상태가 표시됩니다. 개별 그리드 노드에 영향을 미치는 작업이 진행 중인 경우 그리드 노드 상태 섹션에는 각 그리드 노드에 대한 현재 상태가 나열됩니다.

> 이 프로세스 동안 어플라이언스의 경우 StorageGRID 어플라이언스 설치 프로그램이 3단계에서 4단계로 이동하는 설치 완료 를 보여줍니다. 4단계가 완료되면 컨트롤러가 재부팅됩니다.



> 사이트 확장에는 새 사이트에 대한 Cassandra를 구성하는 추가 작업이 포함됩니다.

8. 복구 패키지 다운로드 * 링크가 나타나면 즉시 복구 패키지 파일을 다운로드합니다.

   StorageGRID 시스템에 그리드 토폴로지를 변경한 후 가능한 한 빨리 복구 패키지 파일의 업데이트된 복사본을 다운로드해야 합니다. 복구 패키지 파일을 사용하면 오류가 발생할 경우 시스템을 복원할 수 있습니다.

a. 다운로드 링크를 선택합니다.

b. 프로비저닝 암호를 입력하고 * 다운로드 시작 * 을 선택합니다.

c. 다운로드가 완료되면 '.zip' 파일을 열고 GPT-backup 디렉토리와 _ saed.zip 파일이 포함되어 있는지 확인합니다. 그런 다음 '_then.zip' 파일의 압축을 풀고 '/GID*_REV*' 디렉토리로 이동한 다음 'passwords.txt' 파일을 열 수 있는지 확인합니다.

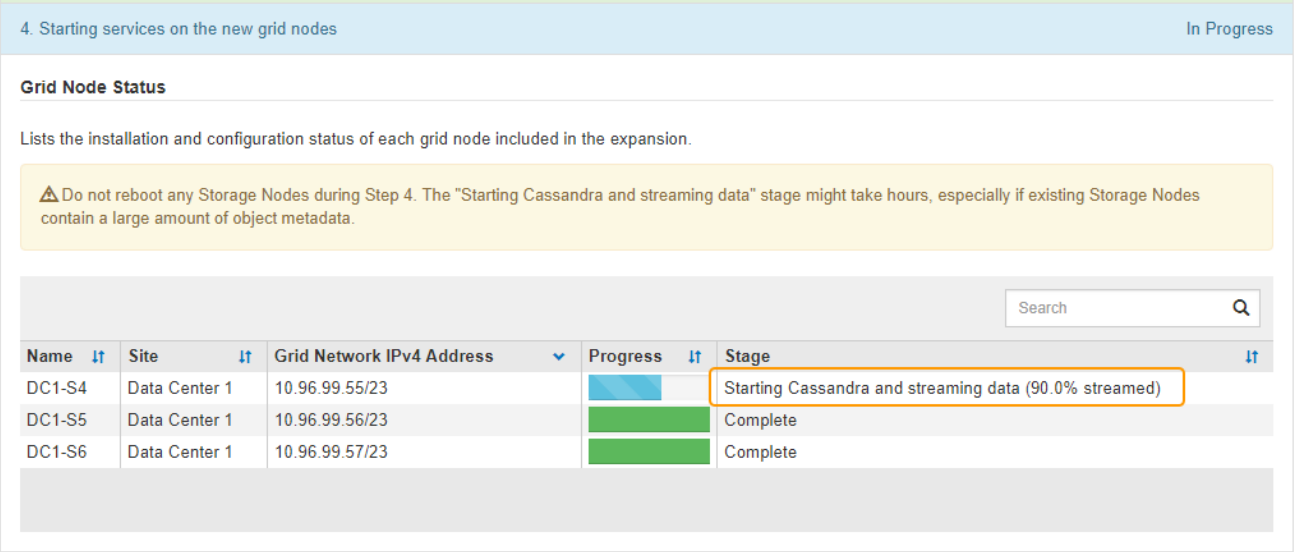
d. 다운로드한 복구 패키지 파일(.zip)을 두 개의 안전한 별도의 위치에 복사합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

9. 기존 사이트에 스토리지 노드를 추가하거나 새 사이트를 추가하는 방법에 대한 지침을 따릅니다.

기존 사이트에 스토리지 노드를 추가합니다

기존 사이트에 하나 이상의 스토리지 노드를 추가하는 경우 상태 메시지에 표시된 비율을 검토하여 "Cassandra 시작 및 데이터 스트리밍" 단계의 진행 상황을 모니터링합니다.



이 백분율은 Cassandra 스트리밍 작업이 완료된 정도를 추정합니다. 이 수치는 사용 가능한 Cassandra 데이터의 총 양과 이미 새 노드에 기록된 데이터를 기준으로 합니다.

> "Cassandra 클러스터 확장" 또는 "Cassandra 시작 및 데이터 스트리밍" 단계 중에 스토리지 노드를 재부팅하지 마십시오. 이러한 단계는 각 새 스토리지 노드에 대해 완료하는 데 몇 시간이 걸릴 수 있습니다. 특히 기존 스토리지 노드에 많은 양의 객체 메타데이터가 포함된 경우 더욱 그렇습니다.

새 사이트를 추가합니다

새 사이트를 추가하는 경우 'NOdetool status'를 사용하여 Cassandra 스트리밍 진행 상황을 모니터링하고 'Cassandra 클러스터 확장' 단계에서 새 사이트에 메타데이터가 얼마나 복사되었는지 확인합니다. 새 사이트의 총 데이터 로드는 현재 사이트의 총 데이터 로드 중 약 20% 이내여야 합니다.

> "Cassandra 클러스터 확장" 또는 "Cassandra 시작 및 데이터 스트리밍" 단계 중에 스토리지 노드를 재부팅하지 마십시오. 이러한 단계는 각 새 스토리지 노드에 대해 완료하는 데 몇 시간이 걸릴 수 있습니다. 특히 기존 스토리지 노드에 많은 양의 객체 메타데이터가 포함된 경우 더욱 그렇습니다.

1. 모든 작업이 완료될 때까지 확장을 계속 모니터링한 후 * 확장 구성 * 버튼이 다시 나타납니다.

작업을 마친 후

추가한 그리드 노드의 유형에 따라 추가 통합 및 구성 단계를 수행해야 합니다. 을 참조하십시오 확장 후 구성 단계.

확장된 시스템을 구성합니다

확장 후 구성 단계

확장을 완료한 후에는 추가 통합 및 구성 단계를 수행해야 합니다.

이 작업에 대해

확장 시 추가하는 그리드 노드에 대해 아래 나열된 구성 작업을 완료해야 합니다. 시스템 설치 및 관리 시 선택한 옵션과 확장 중에 추가된 그리드 노드를 구성하는 방법에 따라 일부 작업은 선택 사항일 수 있습니다.

단계

1. 스토리지 노드를 추가한 경우 다음 구성 작업을 완료합니다.
   a. ILM 규칙에 사용된 스토리지 풀을 검토하여 새 스토리지가 사용되는지 확인합니다. 을 참조하십시오 ILM을 사용하여 개체를 관리합니다.
      - 사이트를 추가한 경우 사이트의 스토리지 풀을 생성하고 ILM 규칙을 업데이트하여 새 스토리지 풀을 사용합니다.
      - 기존 사이트에 스토리지 노드를 추가한 경우 새 노드가 올바른 스토리지 등급을 사용하는지 확인합니다.

      > 기본적으로 새 스토리지 노드는 모든 스토리지 노드 스토리지 등급에 할당되며 사이트에 해당 등급을 사용하는 스토리지 풀에 추가됩니다. 새 노드에서 사용자 지정 스토리지 등급을 사용하려면 해당 노드를 수동으로 사용자 지정 등급(* ILM * > * 스토리지 등급 *)에 할당해야 합니다.

   b. 스토리지 노드가 객체를 인스팅하고 있는지 확인합니다. 을 참조하십시오 스토리지 노드가 활성 상태인지 확인합니다.
   c. 삭제 코딩 데이터의 균형을 재조정합니다(권장 스토리지 노드 수를 추가할 수 없는 경우에만). 을 참조하십시오스토리지 노드를 추가한 후 삭제 코딩 데이터의 균형을 재조정합니다.
2. 게이트웨이 노드를 추가한 경우 다음 구성 작업을 완료합니다.
   - 클라이언트 연결에 고가용성(HA) 그룹을 사용하는 경우 필요에 따라 게이트웨이 노드를 HA 그룹에 추가합니다. 구성 * > * 네트워크 * > * 고가용성 그룹 * 을 선택하여 기존 HA 그룹 목록을 검토하고 새 노드를 추가합니다. 을 참조하십시오 StorageGRID 관리.
3. 관리 노드를 추가한 경우 다음 구성 작업을 완료합니다.
   a. StorageGRID 시스템에 SSO(Single Sign-On)가 활성화된 경우 새 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 만듭니다. 이 신뢰할 수 있는 상대 트러스트를 만들 때까지 노드에 로그인할 수 없습니다. 을 참조하십시오Single Sign-On 구성.
   b. 관리 노드에서 로드 밸런서 서비스를 사용하려는 경우 필요에 따라 새 관리 노드를 HA 그룹에 추가합니다. 기존 HA 그룹 목록을 검토하고 새 노드를 추가하려면 * configuration * * * Network * * High Availability groups * 를 선택합니다. 을 참조하십시오 StorageGRID 관리.
   c. 필요에 따라 각 관리 노드에서 속성과 감사 정보를 일관되게 유지하려면 운영 관리 노드에서 확장 관리 노드로 관리 노드 데이터베이스를 복사합니다. 을 참조하십시오 관리 노드 데이터베이스를 복사합니다.
   d. 필요에 따라 각 관리 노드에서 기간별 메트릭을 일관되게 유지하려면 Prometheus 데이터베이스를 기본 관리 노드에서 확장 관리 노드로 복사합니다. 을 참조하십시오 Prometheus 메트릭을 복사합니다.
   e. 필요에 따라 각 관리 노드에서 기록 로그 정보를 일관되게 유지하려면 기존 감사 로그를 기본 관리 노드에서 확장 관리 노드로 복사합니다. 을 참조하십시오 감사 로그를 복사합니다.
   f. 필요한 경우 NFS 또는 CIFS 파일 공유를 통해 감사 목적으로 시스템에 대한 액세스를 구성합니다. 을 참조하십시오 StorageGRID 관리.

   > CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

g. 필요에 따라 알림에 대한 기본 설정 보낸 사람을 변경합니다. 확장 관리 노드를 기본 설정 보낸 사람으로 지정할 수 있습니다. 그렇지 않으면 기본 설정 송신자로 구성된 기존 관리 노드가 AutoSupport 메시지, SNMP 알림, 경고 이메일 및 알람 이메일(레거시 시스템)을 비롯한 알림을 계속 전송합니다. 을 참조하십시오 StorageGRID 관리.

4. 아카이브 노드를 추가한 경우 다음 구성 작업을 완료합니다.

   a. 대상 외부 아카이브 스토리지 시스템에 대한 아카이브 노드의 연결을 구성합니다. 확장을 완료하면 * ARC * > * Target * 구성 요소를 통해 연결 정보를 구성할 때까지 아카이브 노드는 알람 상태가 됩니다. 을 참조하십시오 StorageGRID 관리.

   b. ILM 정책을 업데이트하여 새 아카이브 노드를 통해 개체 데이터를 아카이빙합니다. 을 참조하십시오 ILM을 사용하여 개체를 관리합니다.

   c. 아카이브 노드로부터 개체 데이터 검색의 속도와 효율성을 모니터링하는 데 사용되는 속성에 대한 사용자 지정 알람을 구성합니다. 을 참조하십시오 StorageGRID 관리.

5. 신뢰할 수 없는 클라이언트 네트워크로 확장 노드가 추가되었는지 확인하거나 노드의 클라이언트 네트워크가 신뢰할 수 없는 것인지 변경하려면 * 구성 * > * 네트워크 * > * 신뢰할 수 없는 클라이언트 네트워크 * 로 이동하십시오.

   확장 노드의 클라이언트 네트워크를 신뢰할 수 없는 경우 로드 밸런서 끝점을 사용하여 클라이언트 네트워크의 노드에 연결해야 합니다. 을 참조하십시오 StorageGRID 관리.

6. DNS(Domain Name System)를 구성합니다.

   각 그리드 노드에 대해 DNS 설정을 별도로 지정한 경우 새 노드에 대해 노드별 DNS 설정을 사용자 지정해야 합니다. 을 참조하십시오 단일 그리드 노드에 대한 DNS 구성을 수정합니다.

   가장 좋은 방법은 각 사이트에서 로컬로 액세스할 수 있는 일부 DNS 서버를 그리드 전체 DNS 서버 목록에 포함하는 것입니다. 새 사이트를 추가한 경우 사이트에 대한 새 DNS 서버를 그리드 전체 DNS 구성에 추가합니다.

   > DNS 서버에 2-6개의 IPv4 주소를 제공합니다. 네트워크 연결 시 각 사이트에서 로컬로 액세스할 수 있는 DNS 서버를 선택해야 합니다. 이는 Is착륙한 사이트가 계속해서 DNS 서비스에 액세스할 수 있도록 하기 위한 것입니다. 그리드 전체 DNS 서버 목록을 구성한 후 각 노드에 대해 DNS 서버 목록을 추가로 사용자 지정할 수 있습니다. 자세한 내용은 을 참조하십시오 단일 그리드 노드에 대한 DNS 구성을 수정합니다…

7. 새 사이트를 추가한 경우 해당 사이트에서 NTP(Network Time Protocol) 서버에 액세스할 수 있는지 확인합니다. 을 참조하십시오 NTP 서버를 구성합니다.

   > 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.

스토리지 노드가 활성 상태인지 확인합니다

새 스토리지 노드를 추가하는 확장 작업이 완료되면 StorageGRID 시스템은 자동으로 새 스토리지 노드를 사용하여 시작해야 합니다. StorageGRID 시스템을 사용하여 새 스토리지 노드가 활성 상태인지 확인해야 합니다.

단계

1. 를 사용하여 Grid Manager에 로그인합니다 지원되는 웹 브라우저.
2. nodes * > **Expansion Storage Node* * > * Storage * 를 선택합니다.
3. 커서를 * Storage Used - Object Data * 그래프 위로 이동하면 * Used * 의 값이 표시됩니다. * 는 객체 데이터에 사용된 총 가용 공간의 양입니다.
4. 그래프 오른쪽으로 커서를 이동하면 * Used * 의 값이 증가하는지 확인합니다.

관리 노드 데이터베이스를 복사합니다

확장 절차를 통해 관리 노드를 추가할 때 필요에 따라 기본 관리 노드에서 새 관리 노드로 데이터베이스를 복사할 수 있습니다. 데이터베이스를 복사하면 속성, 알림 및 알림에 대한 기간별 정보를 유지할 수 있습니다.

필요한 것

- 관리자 노드를 추가하는 데 필요한 확장 단계를 완료했습니다.
- "passwords.txt" 파일이 있습니다.
- 프로비저닝 암호가 있습니다.

이 작업에 대해

StorageGRID 소프트웨어 활성화 프로세스는 확장 관리 노드에서 NMS 서비스에 대한 빈 데이터베이스를 생성합니다. 확장 관리 노드에서 NMS 서비스가 시작되면 현재 시스템에 포함되어 있거나 나중에 추가된 서버 및 서비스에 대한 정보가 기록됩니다. 이 관리 노드 데이터베이스에는 다음 정보가 포함되어 있습니다.

- 알림 기록
- 알람 기록
- 내역 특성 데이터 - * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지에서 사용 가능한 차트 및 텍스트 보고서에 사용됩니다

노드 간에 관리 노드 데이터베이스가 일관성을 유지하도록 기본 관리 노드에서 확장 관리 노드로 데이터베이스를 복사할 수 있습니다.

> 기본 관리 노드(*_source Admin Node*)에서 확장 관리 노드로 데이터베이스를 복사하는 데 최대 몇 시간이 걸릴 수 있습니다. 이 기간 동안 그리드 관리자에 액세스할 수 없습니다.

데이터베이스를 복사하기 전에 기본 관리 노드와 확장 관리 노드 모두에서 MI 서비스 및 관리 API 서비스를 중지하려면 다음 단계를 사용합니다.

단계

1. 기본 관리 노드에서 다음 단계를 완료합니다.
   a. 관리자 노드에 로그인합니다.
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

b. recover-access-points 명령을 실행합니다

c. 프로비저닝 암호를 입력합니다.

d. MI 서비스 'Service mi stop'을 중지합니다

e. 관리 응용 프로그램 인터페이스(mgmt-API) 서비스 'service mgmt-api stop'을 중지합니다

2. 확장 관리 노드에서 다음 단계를 완료합니다.

   a. 확장 관리 노드에 로그인합니다.

      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      iii. 루트로 전환하려면 다음 명령을 입력합니다

      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   b. MI 서비스 'Service mi stop'을 중지합니다

   c. 관리 API 서비스 'service mgmt-api stop'을 중지합니다

   d. SSH 에이전트에 SSH 개인 키를 추가합니다. ssh-add를 입력합니다

   e. "passwords.txt" 파일에 나열된 SSH 액세스 암호를 입력합니다.

   f. 소스 관리 노드에서 확장 관리 노드('/usr/local/mi/bin/mi-clone-db.sh_Source_Admin_Node_IP_')로 데이터베이스를 복사합니다

   g. 메시지가 표시되면 확장 관리 노드의 MI 데이터베이스를 덮어쓸지 확인합니다.

      데이터베이스와 해당 내역 데이터는 확장 관리 노드에 복사됩니다. 복사 작업이 완료되면 스크립트가 확장 관리 노드를 시작합니다.

   h. 다른 서버에 대한 암호 없는 액세스가 더 이상 필요하지 않으면 SSH 에이전트에서 개인 키를 제거합니다. ssh-add-D를 입력합니다

3. Primary Admin Node:'Service ServerManager start'에서 서비스를 다시 시작합니다

Prometheus 메트릭을 복사합니다

새 관리 노드를 추가한 후 선택적으로 Prometheus에서 관리하는 기간별 메트릭을 운영 관리 노드에서 새 관리 노드로 복사할 수 있습니다. 메트릭을 복사하면 관리 노드 간에 기간별 메트릭이 일관되게 유지됩니다.

필요한 것

- 새 관리 노드가 설치되고 실행 중입니다.
- "passwords.txt" 파일이 있습니다.
- 프로비저닝 암호가 있습니다.

이 작업에 대해

관리 노드를 추가하면 소프트웨어 설치 과정에서 새 Prometheus 데이터베이스가 생성됩니다. 기본 관리 노드(*source* 관리 노드)에서 새 관리 노드로 Prometheus 데이터베이스를 복사하여 노드 간에 기간별 메트릭을 일관되게 유지할 수 있습니다.

Prometheus 데이터베이스를 복사하는 데 1시간 이상이 걸릴 수 있습니다. 소스 관리 노드에서 서비스가 중지되는 동안에는 일부 Grid Manager 기능을 사용할 수 없습니다.

단계

1. 소스 관리 노드에 로그인합니다.
   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.
2. Source Admin Node에서 Prometheus 서비스 'Service Prometheus stop'을 중지합니다
3. 새 관리 노드에서 다음 단계를 완료합니다.
   a. 새 관리자 노드에 로그인합니다.
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   b. 프로메테우스 서비스 '프로메테우스 서비스'를 중단하십시오
   c. SSH 에이전트에 SSH 개인 키를 추가합니다. ssh-add를 입력합니다
   d. "passwords.txt" 파일에 나열된 SSH 액세스 암호를 입력합니다.
   e. 소스 관리 노드에서 새 관리 노드로 Prometheus 데이터베이스를 복사합니다: "/usr/local/Prometheus/bin/prometheus-clone-db.sh_Source_Admin_Node_IP_"
   f. 메시지가 표시되면 * Enter * 를 눌러 새 관리 노드에서 새 Prometheus 데이터베이스를 파기할지 확인합니다.

      원래 Prometheus 데이터베이스와 해당 기록 데이터가 새 관리 노드에 복사됩니다. 복사 작업이 완료되면 스크립트가 새 관리 노드를 시작합니다. 다음 상태가 나타납니다.

   다타바제 복제서비스 시작

   a. 다른 서버에 대한 암호 없는 액세스가 더 이상 필요하지 않으면 SSH 에이전트에서 개인 키를 제거합니다. 입력:

      '시-애드-D'

4. 소스 관리 노드에서 Prometheus 서비스를 다시 시작합니다.

   'Prometheus 서비스 시작

감사 로그를 복사합니다

확장 절차를 통해 새 관리 노드를 추가하면 AMS 서비스는 시스템에 연결된 후에 발생하는 이벤트 및 동작만 기록합니다. 필요에 따라 이전에 설치된 관리 노드에서 새 확장 관리 노드로 감사 로그를 복사하여 나머지 StorageGRID 시스템과 동기화할 수 있습니다.

필요한 것

- 관리자 노드를 추가하는 데 필요한 확장 단계를 완료했습니다.
- "passwords.txt" 파일이 있습니다.

이 작업에 대해

새 관리 노드에서 기록 감사 메시지를 사용하려면 감사 로그 파일을 기존 관리 노드에서 확장 관리 노드로 수동으로 복사해야 합니다.

> 기본적으로 감사 정보는 관리 노드의 감사 로그로 전송됩니다. 다음 중 하나가 적용되는 경우 이 단계를 건너뛸 수 있습니다.
>
> - 외부 syslog 서버를 구성했으며 이제 감사 로그가 관리 노드 대신 syslog 서버로 전송됩니다.
> - 감사 메시지를 생성한 로컬 노드에만 저장하도록 명시적으로 지정했습니다.
>
> 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다 를 참조하십시오.

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh_admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
2. AMS 서비스를 중지하여 새 파일인 'Service AMS stop'을 생성하지 않도록 합니다
3. "audit.log" 파일의 이름을 변경하여 복사할 확장 관리 노드의 파일을 덮어쓰지 않도록 합니다.

   "cd /var/local/audit/export" + "ls-l" + mv audit.log_new_name_.txt"
4. 모든 감사 로그 파일을 확장 관리 노드에 복사:

   S CP-p * *IP_address*:/var/local/audit/export
5. '/root/.ssh/id_rsa'에 대한 암호를 묻는 메시지가 나타나면 "passwords.txt" 파일에 나열된 운영 관리자 노드의 SSH 액세스 암호를 입력합니다.
6. 원래 'audit.log' 파일 복구:

   mv *new_name*.txt audit.log'입니다
7. AMS 서비스를 시작합니다.

   '서비스 AMS 시작
8. 서버에서 로그아웃합니다.

   종료

9. 확장 관리 노드에 로그인합니다.
   a. 'ssh admin@*expansion_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

10. 감사 로그 파일에 대한 사용자 및 그룹 설정을 업데이트합니다.

    'cd /var/local/audit/export' + 'chown AMS-user:bycast *'

11. 서버에서 로그아웃합니다.

    종료

스토리지 노드를 추가한 후 삭제 코딩 데이터의 균형을 재조정합니다

경우에 따라 새 스토리지 노드를 추가한 후 삭제 코딩 데이터의 균형을 재조정해야 할 수 있습니다.

필요한 것

- 새 스토리지 노드를 추가하는 확장 단계를 완료했습니다.
- 을(를) 검토했습니다 삭제 코딩 데이터의 재조정에 대한 고려사항.

> 사이트에서 하나 이상의 스토리지 노드에 대해 * Low Object Storage * 알림이 트리거되어 권장되는 수의 새 스토리지 노드를 추가할 수 없는 경우에만 이 절차를 수행하십시오.

- 복제된 오브젝트 데이터는 이 절차에 의해 이동되지 않으며 EC 재조정 절차에서는 삭제 코딩 데이터를 이동할 위치를 결정할 때 각 스토리지 노드에서 복제된 데이터 사용을 고려하지 않는다는 점을 이해합니다.
- "passwords.txt" 파일이 있습니다.

이 작업에 대해

EC 재조정 절차가 실행 중이면 ILM 작업 및 S3 및 Swift 클라이언트 작업의 성능에 영향을 줄 수 있습니다. 따라서 이 절차는 제한된 경우에만 수행해야 합니다.

> EC 재조정 절차는 많은 양의 스토리지를 임시로 예약합니다. 스토리지 알림이 트리거될 수 있지만 재조정이 완료되면 문제가 해결됩니다. 예약 저장 공간이 충분하지 않으면 EC 재조정 절차가 실패합니다. EC 재조정 절차가 완료되면 절차가 실패했는지 여부에 관계없이 스토리지 예약이 해제됩니다.

> EC 재조정 절차 중에 완료하는 데 24시간 이상이 필요한 경우 S3 및 Swift API 작업으로 오브젝트(또는 오브젝트 부분)가 업로드되지 않을 수 있습니다. 해당 ILM 규칙이 수집 시 Strict 또는 Balanced 배치를 사용하는 경우 장기 PUT 작업이 실패합니다. 다음 오류가 보고됩니다.
>
> '500 내부 서버 오류'

단계

1. 재조정할 사이트의 현재 오브젝트 스토리지 세부 정보를 검토합니다.
   a. 노드 * 를 선택합니다.
   b. 사이트에서 첫 번째 스토리지 노드를 선택합니다.
   c. Storage * 탭을 선택합니다.
   d. Storage Used-Object Data 차트 위에 커서를 올려 놓으면 스토리지 노드에서 복제된 데이터의 현재 양과 삭제 코딩 데이터를 확인할 수 있습니다.
   e. 사이트에서 다른 스토리지 노드를 보려면 다음 단계를 반복합니다.
2. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
3. 다음 명령을 입력합니다.

   rebalance-data start—site "*site-name*""

   ""*site-name*""에 새 스토리지 노드를 추가한 첫 번째 사이트를 지정합니다. 인용문에는 사인을 묶습니다.

   EC 재조정 절차가 시작되고 작업 ID가 반환됩니다.
4. 작업 ID를 복사합니다.
5. EC 재조정 절차의 상태를 모니터링합니다.
   - 단일 EC 재조정 절차의 상태를 보려면

     rebalance-data status—job-id_job-id_'

     '*job-id*'의 경우 절차를 시작할 때 반환된 ID를 지정합니다.
   - 현재 EC 재조정 절차 및 이전에 완료된 절차의 상태를 보려면

     rebalance-data status

     > rebalance-data 명령에 대한 도움말을 보려면 다음을 수행합니다.
     >
     > rebalance-data-help를 선택합니다
   - 현재 작업의 예상 완료 시간과 완료 비율을 보려면 * 지원 * > * 도구 * > * 메트릭 * 을 선택합니다. 그런 다음 Grafana 섹션에서 * EC 개요 * 를 선택합니다. Grid EC Job Ec Job Estimated Time to Completion * 및 * Grid EC Job Percentage Completed * 대시보드를 확인합니다.
6. 반환된 상태에 따라 추가 단계를 수행합니다.

- 상태가 '진행 중'인 경우 EC 재조정 작업이 계속 실행되고 있는 것입니다. 절차가 완료될 때까지 주기적으로 모니터링해야 합니다.
- 상태가 "실패"인 경우 를 수행합니다 실패 단계.
- 상태가 '성공'이면 를 수행합니다 성공 단계.

7. EC 균형 조정 절차에서 너무 많은 로드가 생성되는 경우(예: 수집 작업이 영향을 받음) 절차를 일시 중지하십시오.

   rebalance-data pause—job-id_job-id_'

8. EC 재조정 절차를 종료해야 하는 경우(예: StorageGRID 소프트웨어 업그레이드 수행) 다음을 입력합니다.

   rebalance-data terminate—job-id_job-id_'를 선택합니다

   > EC 재조정 절차를 종료할 때 이미 이동된 데이터 조각은 새 위치에 그대로 남아 있습니다. 데이터가 원래 위치로 다시 이동되지 않습니다.

9. EC rebalance procedure의 상태가 'Failure'인 경우, 다음 단계를 따른다.
   a. 사이트의 모든 스토리지 노드가 그리드에 연결되어 있는지 확인합니다.
   b. 이러한 스토리지 노드에 영향을 줄 수 있는 알림을 확인하고 해결합니다.

      특정 경고에 대한 자세한 내용은 모니터링 및 문제 해결 지침을 참조하십시오.

   c. EC 재조정 절차(+ rebalance-data start–-job-id_job-id_')를 다시 시작합니다
   d. EC 재조정 절차의 상태가 여전히 "실패"인 경우 기술 지원 부서에 문의하십시오.

10. [[rebalance_success] ([재조정_성공]) EC 재조정 절차의 상태가 '성공'(선택 사항)인 경우 오브젝트 스토리지 검토 사이트에 대한 업데이트된 세부 정보를 봅니다.

    이제 삭제 코딩 데이터가 사이트의 스토리지 노드 간에 더 균형 있게 균형 있게 조정되어야 합니다.

11. 둘 이상의 사이트에서 삭제 코딩을 사용하는 경우 영향을 받는 다른 모든 사이트에 대해 이 절차를 실행합니다.

기술 지원 부서에 문의하십시오

그리드 확장 프로세스 중에 해결할 수 없는 오류가 발생하거나 그리드 작업이 실패하면 기술 지원 부서에 문의하십시오.

이 작업에 대해

기술 지원 부서에 문의할 때는 발생한 오류의 문제를 해결하는 데 도움이 되는 필수 로그 파일을 제공해야 합니다.

단계

1. 장애가 발생한 확장 노드에 연결:

   a. "ssh-p 8022 admin@*grid_node_ip*' 명령을 입력한다

   > 포트 8022는 기본 OS의 SSH 포트이고, 포트 22는 StorageGRID를 실행하는 컨테이너 엔진의 SSH 포트입니다.

b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

c. 루트로 전환하려면 다음 명령을 입력합니다

d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

루트로 로그인하면 프롬프트는 '$'에서 '#'로 바뀝니다.

2. 설치에 도달한 단계에 따라 그리드 노드에서 사용할 수 있는 다음 로그를 검색합니다.

플랫폼	로그
VMware	• '/var/log/daemon.log'입니다 • '/var/log/StorageGrid/daemon.log'입니다 • "/var/log/StorageGrid/nodes/<node-name>.log"를 입력합니다
리눅스	• '/var/log/StorageGrid/daemon.log'입니다 • `/etc/StorageGrid/nodes/<node-name>.conf'(실패한 각 노드에 대해) • "/var/log/StorageGrid/nodes/<node-name>.log"(실패한 각 노드에 대해)

복구 및 유지 관리

복구 및 유지 관리: 개요

다음 지침에 따라 StorageGRID 시스템을 유지보수하고 장애로부터 복구합니다.

참조하십시오

이 지침에서는 소프트웨어 핫픽스 적용, 그리드 노드 복구, 장애가 발생한 사이트 복구, 그리드 노드 또는 전체 사이트 파기, 네트워크 유지보수 수행, 호스트 레벨 및 미들웨어 유지보수 절차 수행, 그리드 노드 절차 수행 방법에 대해 설명합니다.

> 이 지침에서 "'Linux'는 Red Hat ® Enterprise Linux ®, Ubuntu ®, CentOS 또는 Debian ® 배포를 의미합니다. 를 사용합니다 "NetApp 상호 운용성 매트릭스 툴" 를 클릭하여 지원되는 버전 목록을 가져옵니다.

시작하기 전에

- StorageGRID 시스템에 대한 폭넓은 지식을 갖추고 있습니다.
- StorageGRID 시스템의 토폴로지를 검토했으며 그리드 구성을 이해했습니다.
- 당신은 모든 지침을 정확하게 따르고 모든 경고에 주의를 기울여야 한다는 것을 이해합니다.
- 설명되지 않은 유지보수 절차는 지원되지 않거나 서비스 계약이 필요하다는 것을 알고 있습니다.

어플라이언스에 대한 유지보수 절차

하드웨어 절차는 StorageGRID 어플라이언스의 설치 및 유지보수 지침을 참조하십시오.

- SG100 및 SG1000 서비스 어플라이언스
- SG6000 스토리지 어플라이언스
- SG5700 스토리지 어플라이언스
- SG5600 스토리지 어플라이언스

복구 패키지를 다운로드합니다

복구 패키지 파일을 사용하면 오류가 발생할 경우 StorageGRID 시스템을 복원할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 프로비저닝 암호가 있어야 합니다.
- 특정 액세스 권한이 있어야 합니다.

그리드 토폴로지를 StorageGRID 시스템으로 변경하거나 소프트웨어를 업그레이드하기 전에 현재 복구 패키지 파일을 다운로드합니다. 그런 다음 그리드 토폴로지를 변경한 후 또는 소프트웨어를 업그레이드한 후 복구 패키지의 새 복사본을 다운로드합니다.

단계

1. 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
2. 프로비저닝 암호를 입력하고 * 다운로드 시작 * 을 선택합니다.

   다운로드가 즉시 시작됩니다.

3. 다운로드가 완료되면 다음을 수행합니다.
   a. '.zip' 파일을 엽니다.
   b. GPT 백업 디렉토리와 내부 '.zip' 파일이 포함되어 있는지 확인합니다.
   c. 안쪽 '.zip' 파일의 압축을 풉니다.
   d. 비밀번호.txt 파일을 열 수 있는지 확인합니다.
4. 다운로드한 복구 패키지 파일('.zip')을 두 개의 안전하고 서로 다른 위치에 복사합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

관련 정보

StorageGRID 관리

StorageGRID 핫픽스 절차

기능 릴리즈 간에 소프트웨어 문제가 발견되어 해결된 경우 StorageGRID 시스템에 핫픽스를

적용해야 할 수 있습니다.

StorageGRID 핫픽스에는 기능 또는 패치 릴리스 외부에서 사용할 수 있는 소프트웨어 변경 사항이 포함되어 있습니다. 동일한 변경 사항이 향후 릴리스에 포함됩니다. 또한 각 핫픽스 릴리스에는 기능 또는 패치 릴리스 내의 모든 이전 핫픽스의 롤업도 포함되어 있습니다.

핫픽스 적용 시 고려 사항

핫픽스를 적용하면 StorageGRID 시스템의 노드에 일련의 누적 소프트웨어 업데이트가 적용됩니다.

다른 유지보수 절차가 실행 중인 경우에는 StorageGRID 핫픽스를 적용할 수 없습니다. 예를 들어 서비스 해제, 확장 또는 복구 절차가 실행 중인 동안에는 핫픽스를 적용할 수 없습니다.

> 노드 또는 사이트 서비스 해제 절차가 일시 중지된 경우 핫픽스를 안전하게 적용할 수 있습니다. 또한 StorageGRID 업그레이드 절차의 마지막 단계에서 핫픽스를 적용할 수도 있습니다. 자세한 내용은 StorageGRID 소프트웨어 업그레이드 지침을 참조하십시오.

Grid Manager에서 핫픽스를 업로드하면 핫픽스가 기본 관리 노드에 자동으로 적용됩니다. 그런 다음 StorageGRID 시스템의 나머지 노드에 대한 핫픽스 응용 프로그램을 승인할 수 있습니다.

핫픽스가 하나 이상의 노드에 적용되지 않으면 핫픽스 진행률 표의 세부 정보 열에 실패 이유가 나타납니다. 실패의 원인이 된 모든 문제를 해결한 다음 전체 프로세스를 다시 시도해야 합니다. 이전에 성공한 핫픽스 응용 프로그램이 있는 노드는 후속 응용 프로그램에서 건너뜁니다. 모든 노드가 업데이트될 때까지 필요한 만큼 핫픽스 프로세스를 다시 시도할 수 있습니다. 응용 프로그램을 완료하려면 모든 그리드 노드에 핫픽스를 성공적으로 설치해야 합니다.

그리드 노드는 새 핫픽스 버전으로 업데이트되지만 핫픽스의 실제 변경 사항은 특정 노드 유형의 특정 서비스에만 영향을 줄 수 있습니다. 예를 들어 핫픽스는 스토리지 노드의 LDR 서비스에만 영향을 줄 수 있습니다.

복구 및 확장에 핫픽스 적용 방식

핫픽스가 그리드에 적용된 후 기본 관리 노드는 복구 작업에 의해 복원되거나 확장에 추가된 노드에 동일한 핫픽스 버전을 자동으로 설치합니다.

그러나 기본 관리 노드를 복구해야 하는 경우 올바른 StorageGRID 릴리스를 수동으로 설치한 다음 핫픽스를 적용해야 합니다. 기본 관리 노드의 최종 StorageGRID 버전은 그리드의 다른 노드의 버전과 일치해야 합니다.

다음 예에서는 기본 관리자 노드를 복구할 때 핫픽스를 적용하는 방법을 보여 줍니다.

1. 그리드가 최신 핫픽스와 함께 StorageGRID 11._A.B_version을 실행 중인 것으로 가정합니다. 그리드 버전(grid version)은 11입니다.
2. 기본 관리 노드에 장애가 발생합니다.
3. StorageGRID 11._A.B_를 사용하여 기본 관리 노드를 재구축하고 복구 절차를 수행합니다.

   > 그리드 버전과 일치하도록 노드를 배포할 때 부 릴리즈를 사용할 수 있습니다. 주 릴리스를 먼저 배포할 필요는 없습니다.

4. 그런 다음 핫 픽스 11._A.B.y_를 기본 관리 노드에 적용합니다.

관련 정보

대체 운영 관리자 노드를 구성합니다

핫픽스를 계획하고 준비합니다

StorageGRID 시스템에 대한 중단을 최소화하기 위해 핫픽스를 적용하기 전에 계획을 세워야 합니다.

단계

- 핫픽스를 적용할 때 시스템이 영향을 받는 방식
- 핫픽스에 필요한 자료 얻기
- 핫픽스 파일을 다운로드하는 중입니다
- 핫픽스를 적용하기 전에 시스템 상태를 확인합니다

핫픽스를 적용할 때 시스템이 영향을 받는 방식

핫픽스를 적용할 때 StorageGRID 시스템이 어떤 영향을 받는지 알아야 합니다.

클라이언트 애플리케이션은 단기간 동안 중단될 수 있습니다

StorageGRID 시스템은 핫픽스 프로세스를 통해 클라이언트 애플리케이션에서 데이터를 수집하고 검색할 수 있습니다. 하지만 핫픽스가 해당 노드에서 서비스를 다시 시작해야 하는 경우 개별 게이트웨이 노드 또는 스토리지 노드에 대한 클라이언트 연결이 일시적으로 중단될 수 있습니다. 핫픽스 프로세스가 완료되고 개별 노드에서 서비스가 다시 시작된 후 연결이 복원됩니다.

짧은 기간 동안 연결이 끊어지지 않는 경우 핫픽스를 적용하기 위해 다운타임을 예약해야 할 수 있습니다. 선택적 승인을 사용하여 특정 노드가 업데이트되는 시기를 예약할 수 있습니다.

> 여러 게이트웨이 및 고가용성(HA) 그룹을 사용하여 핫픽스 프로세스 중에 자동 페일오버를 제공할 수 있습니다. 의 지침을 참조하십시오 고가용성 그룹 구성.

경고 및 **SNMP** 알림이 트리거될 수 있습니다

서비스가 다시 시작되고 StorageGRID 시스템이 혼합 버전 환경으로 작동 중일 때(이전 버전을 실행하는 일부 그리드 노드와 이후 버전으로 업그레이드된 일부 그리드 노드) 알림 및 SNMP 알림이 트리거될 수 있습니다. 일반적으로 이러한 경고 및 알림은 핫픽스가 완료되면 지워집니다.

구성 변경이 제한됩니다

StorageGRID에 핫픽스를 적용할 경우:

- 핫픽스가 모든 노드에 적용될 때까지 그리드 구성 변경(예: 그리드 네트워크 서브넷 지정 또는 보류 중인 그리드 노드 승인)을 수행하지 마십시오.
- 핫픽스가 모든 노드에 적용될 때까지 ILM 구성을 업데이트하지 마십시오.

핫픽스에 필요한 자료를 얻습니다

핫픽스를 적용하기 전에 필요한 모든 자료를 확보해야 합니다.

항목	참고
StorageGRID 핫픽스 파일	StorageGRID 핫픽스 파일을 다운로드해야 합니다.
• 네트워크 포트 • 지원되는 웹 브라우저 • SSH 클라이언트(예: PuTTY)	
복구 패키지(".zip") 파일	핫픽스를 적용하기 전에 최신 복구 패키지 파일을 다운로드합니다 핫픽스 중에 문제가 발생하는 경우 핫픽스를 적용한 후 복구 패키지 파일의 새 복사본을 다운로드하여 안전한 위치에 저장합니다. 업데이트된 복구 패키지 파일을 사용하면 오류가 발생할 경우 시스템을 복원할 수 있습니다.
Passwords.txt 파일	선택 사항이며 SSH 클라이언트를 사용하여 핫픽스를 수동으로 적용하는 경우에만 사용됩니다. 복구 패키지 .zip의 일부인 해당 패키지에 passwords.txt 파일이 포함되어 있습니다.
프로비저닝 암호	StorageGRID 시스템을 처음 설치할 때 암호가 생성되고 문서화됩니다. 프로비저닝 암호는 passwords.txt 파일에 나열되지 않습니다.
관련 문서	핫픽스 "readme.txt" 파일. 이 파일은 핫픽스 다운로드 페이지에 포함되어 있습니다. 핫픽스를 적용하기 전에 반드시 "다시 보기" 파일을 주의 깊게 검토하십시오.

관련 정보

핫픽스 파일을 다운로드합니다

핫픽스 파일을 다운로드합니다

핫픽스를 적용하려면 먼저 핫픽스 파일을 다운로드해야 합니다.

단계

1. StorageGRID용 NetApp 다운로드 페이지로 이동합니다.

   "NetApp 다운로드: StorageGRID"

2. 다운로드할 수 있는 핫픽스 목록을 보려면 * Available Software * (사용 가능한 소프트웨어 *) 아래의 아래쪽 화살표를 선택합니다.

   핫픽스 파일 버전은 11.4__.x.y_ 형식입니다.

3. 업데이트에 포함된 변경 사항을 검토합니다.

   기본 관리 노드를 방금 복구한 경우 핫픽스를 적용해야 하는 경우 다른 그리드 노드에 설치된 것과 동일한 핫픽스 버전을 선택합니다.

a. 다운로드할 핫픽스 버전을 선택하고 * GO * 를 선택합니다.

b. NetApp 계정의 사용자 이름과 암호를 사용하여 로그인합니다.

c. 최종 사용자 사용권 계약을 읽고 동의합니다.

   선택한 버전의 다운로드 페이지가 나타납니다.

d. 핫픽스 "readme.txt" 파일을 다운로드하여 핫픽스에 포함된 변경 내용의 요약을 봅니다.

4. 핫픽스의 다운로드 버튼을 선택하고 파일을 저장합니다.

   > 이 파일의 이름은 변경하지 마십시오.

   > macOS 장치를 사용하는 경우 핫픽스 파일이 자동으로 '.txt' 파일로 저장될 수 있습니다. 이 경우 확장자가 .txt인 파일 이름을 변경하지 않고 이름을 변경해야 합니다.

5. 다운로드할 위치를 선택하고 * 저장 * 을 선택합니다.

관련 정보

대체 운영 관리자 노드를 구성합니다

핫픽스를 적용하기 전에 시스템 상태를 확인하십시오

핫픽스가 시스템에 적용되었는지 확인해야 합니다.

1. 를 사용하여 Grid Manager에 로그인합니다 지원되는 웹 브라우저.
2. 가능한 경우 시스템이 정상적으로 실행되고 있고 모든 그리드 노드가 그리드에 연결되어 있는지 확인합니다.

   연결된 노드에는 녹색 확인 표시가 있습니다 노드 페이지에서

3. 가능한 경우 현재 경고를 확인하고 해결합니다.

   특정 경고에 대한 자세한 내용은 StorageGRID 모니터링 및 문제 해결 지침을 참조하십시오.

4. 업그레이드, 복구, 확장 또는 서비스 해제 절차와 같은 다른 유지보수 절차가 진행되고 있지 않은지 확인합니다.

   핫픽스를 적용하기 전에 활성 유지 관리 절차가 완료될 때까지 기다려야 합니다.

   다른 유지보수 절차가 실행 중인 경우에는 StorageGRID 핫픽스를 적용할 수 없습니다. 예를 들어 서비스 해제, 확장 또는 복구 절차가 실행 중인 동안에는 핫픽스를 적용할 수 없습니다.

   > 노드 또는 사이트 서비스 해제 절차가 일시 중지된 경우 핫픽스를 안전하게 적용할 수 있습니다. 또한 StorageGRID 업그레이드 절차의 마지막 단계에서 핫픽스를 적용할 수도 있습니다. 자세한 내용은 StorageGRID 소프트웨어 업그레이드 지침을 참조하십시오.

관련 정보

모니터링하고 문제를 해결합니다

스토리지 노드에 대한 서비스 해제 프로세스를 일시 중지하고 다시 시작합니다

핫픽스를 적용합니다

핫픽스는 먼저 기본 관리자 노드에 자동으로 적용됩니다. 그런 다음 모든 노드가 동일한 소프트웨어 버전을 실행할 때까지 다른 그리드 노드에 대한 핫픽스 응용 프로그램을 승인해야 합니다. 개별 그리드 노드, 그리드 노드 그룹 또는 모든 그리드 노드를 승인하도록 선택하여 승인 순서를 사용자 지정할 수 있습니다.

필요한 것

- 고려 사항을 검토하고 의 단계를 완료했습니다 핫픽스를 계획하고 준비합니다.
- 프로비저닝 암호가 있습니다.
- 루트 액세스 또는 유지 관리 권한이 있습니다.

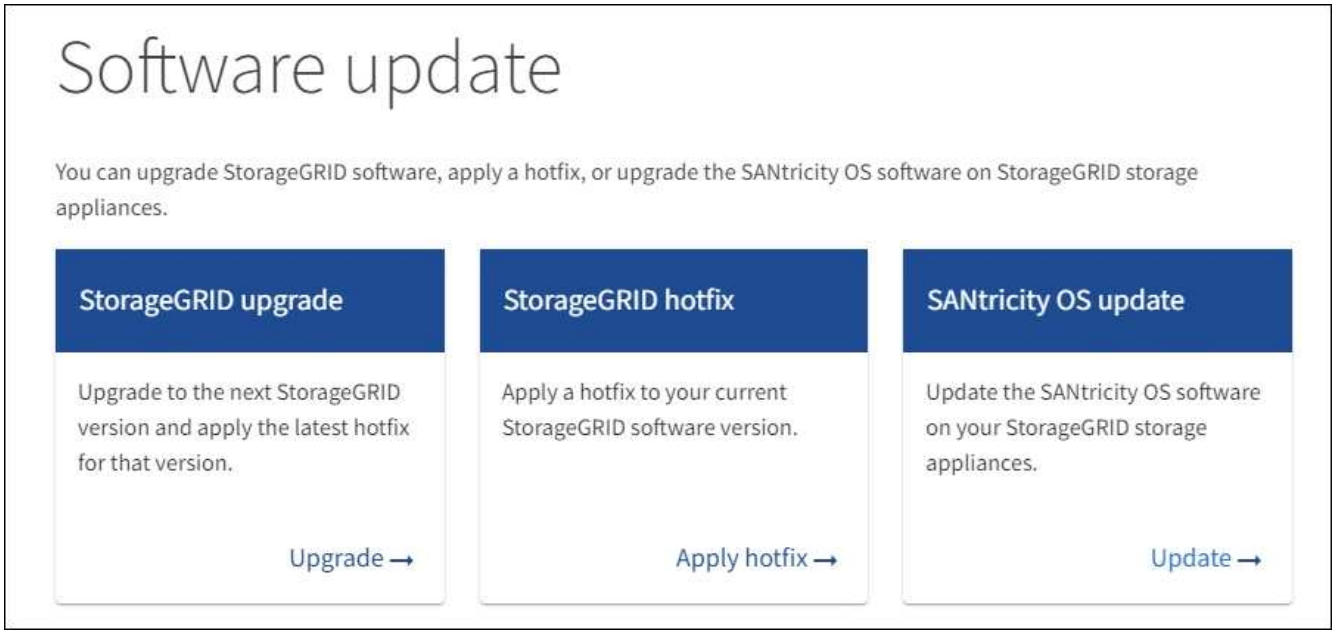
이 작업에 대해

- 노드에 핫픽스 적용을 지연할 수 있지만 모든 노드에 핫픽스를 적용할 때까지 핫픽스 프로세스는 완료되지 않습니다.
- 핫픽스 프로세스를 완료할 때까지 StorageGRID 소프트웨어 업그레이드 또는 SANtricity OS 업그레이드를 수행할 수 없습니다.

단계

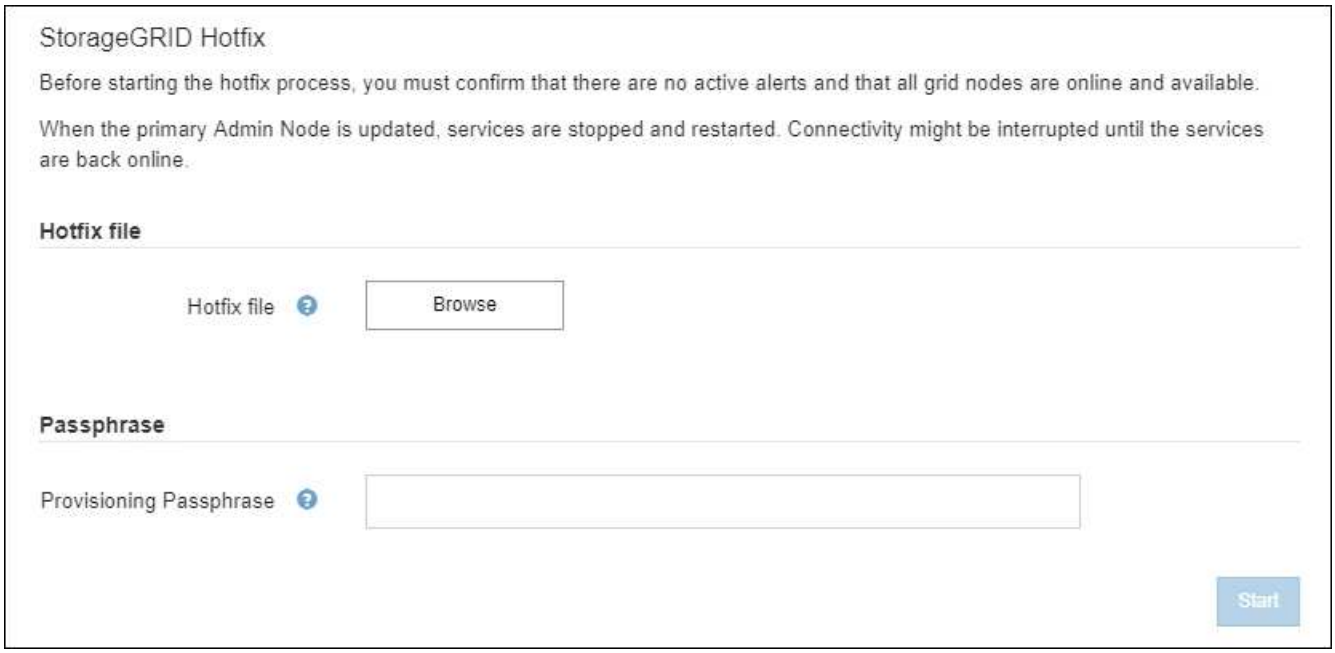
1. 를 사용하여 Grid Manager에 로그인합니다 지원되는 웹 브라우저.
2. 유지보수 * > * 시스템 * > * 소프트웨어 업데이트 * 를 선택합니다.

   소프트웨어 업데이트 페이지가 나타납니다.



3. 핫픽스 적용 * 을 선택합니다.

   StorageGRID 핫픽스 페이지가 나타납니다.



4. NetApp Support 사이트에서 다운로드한 핫픽스 파일을 선택합니다.

   a. 찾아보기 * 를 선택합니다.

   b. 파일을 찾아 선택합니다.

      'hotfix-install -*version*'

   c. 열기 * 를 선택합니다.

      파일이 업로드됩니다. 업로드가 완료되면 파일 이름이 세부 정보 필드에 표시됩니다.

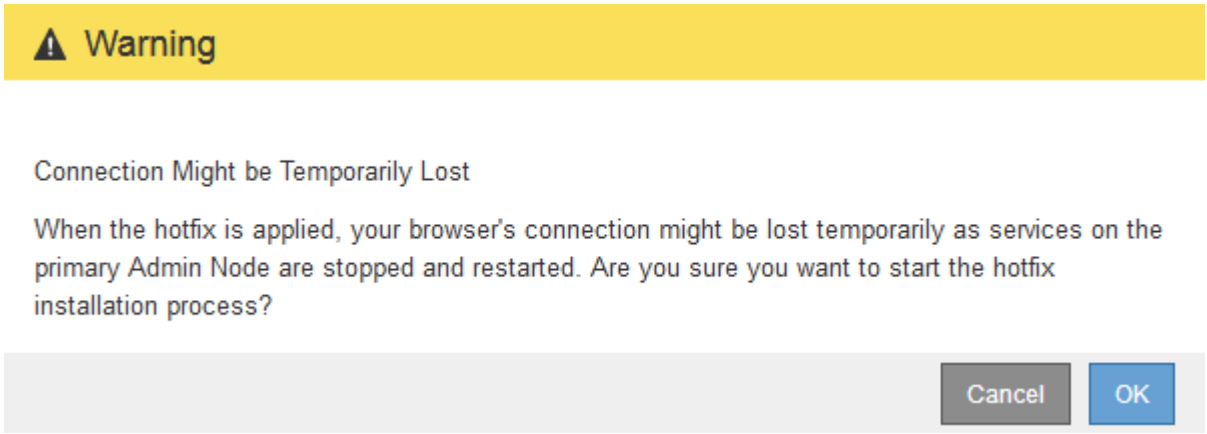
      ⓘ 파일 이름은 확인 프로세스의 일부이므로 변경하지 마십시오.

5. 텍스트 상자에 프로비저닝 암호를 입력합니다.

   시작 * 버튼이 활성화됩니다.

6. 시작 * 을 선택합니다.

   기본 관리 노드의 서비스가 다시 시작됨에 따라 브라우저의 연결이 일시적으로 끊길 수 있다는 경고가 나타납니다.



7. 기본 관리자 노드에 핫픽스 적용을 시작하려면 * 확인 * 을 선택합니다.

   핫픽스 시작 시:

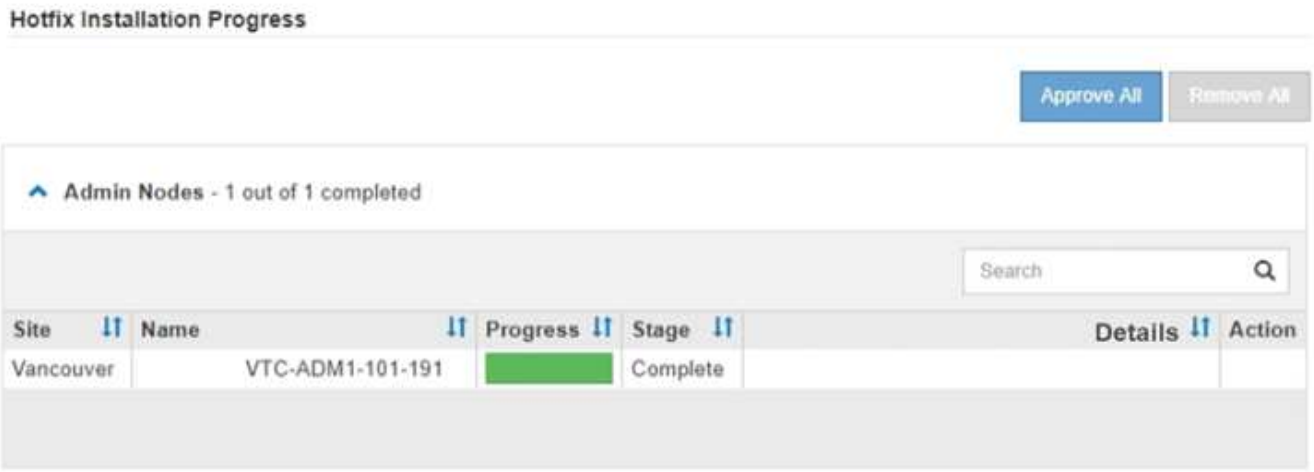
   a. 핫픽스 검증이 실행됩니다.

      > 오류가 보고되면 이를 해결한 후 핫픽스 파일을 다시 업로드하고 * 시작 * 을 다시 선택하십시오.

   b. 핫픽스 설치 진행률 표가 나타납니다. 이 표에는 그리드의 모든 노드와 각 노드에 대한 핫픽스 설치의 현재 단계가 나와 있습니다. 테이블의 노드는 다음과 같이 유형별로 그룹화됩니다.

      - 관리자 노드
      - 게이트웨이 노드
      - 스토리지 노드
      - 아카이브 노드

      > 진행 표시줄이 완성되면 기본 관리 노드가 ""완료" 스테이지와 함께 먼저 표시됩니다.



8. 선택적으로 * Site *, * Name *, * Progress *, * Stage * 또는 * Details * 를 기준으로 각 그룹의 노드 목록을 오름차순 또는 내림차순으로 정렬합니다. 또는 * 검색 * 상자에 용어를 입력하여 특정 노드를 검색합니다.
9. 업데이트할 준비가 된 그리드 노드를 승인합니다. 동일한 유형의 승인된 노드는 한 번에 하나씩 업그레이드됩니다.

   > 노드를 업데이트할 준비가 되었는지 확신할 수 없는 경우에는 노드에 대한 핫픽스를 승인하지 마십시오. 핫픽스가 그리드 노드에 적용되면 해당 노드의 일부 서비스가 다시 시작될 수 있습니다. 이러한 작업은 노드와 통신하는 클라이언트에 대해 서비스 중단을 일으킬 수 있습니다.

   - 하나 이상의 개별 노드를 핫픽스 대기열에 추가하려면 * Approve * 단추를 하나 이상 선택합니다.
   - 각 그룹 내에서 * 모두 승인 * 버튼을 선택하여 동일한 유형의 모든 노드를 핫픽스 대기열에 추가합니다. 검색 * 상자에 검색 조건을 입력한 경우 * 모두 승인 * 버튼은 검색 기준에 의해 선택된 모든 노드에 적용됩니다.

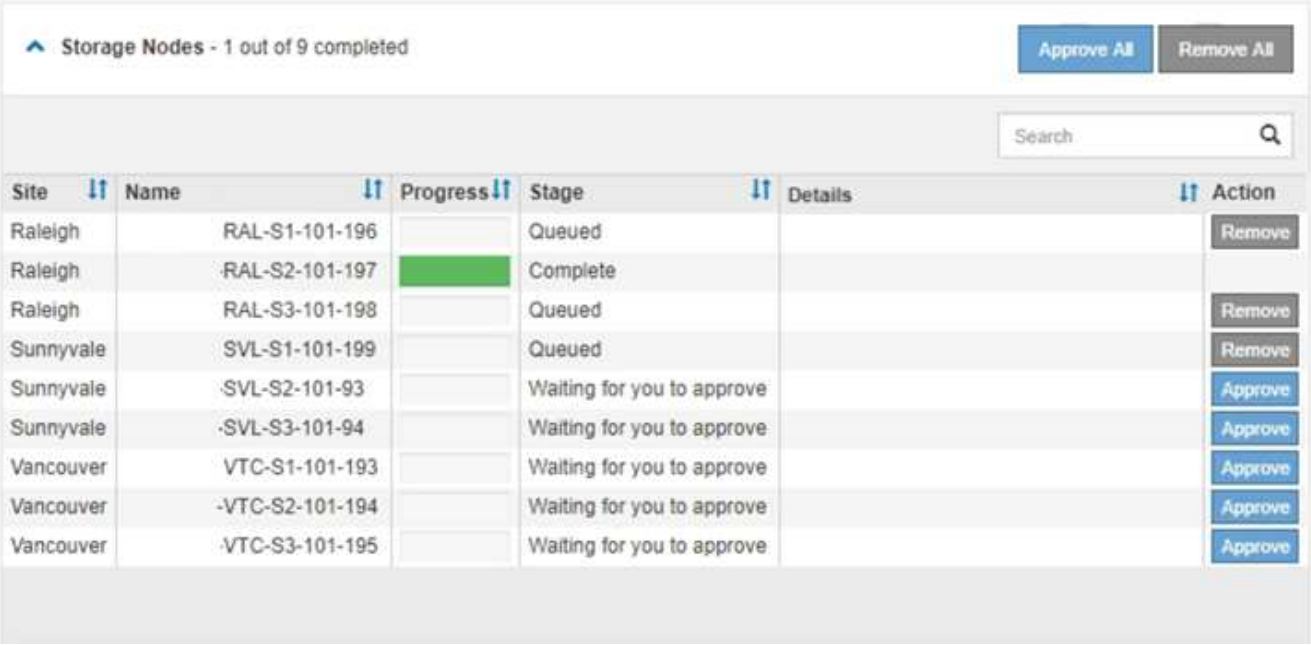
> 페이지 상단의 * Approve All * (모두 승인) 버튼을 클릭하면 페이지에 나열된 모든 노드가 승인되고, 테이블 그룹 상단의 * Approve All * (모두 승인) 버튼을 누르면 해당 그룹의 모든 노드만 승인됩니다. 노드 업그레이드 순서가 중요한 경우 노드 또는 노드 그룹을 한 번에 하나씩 승인하고 다음 노드를 승인하기 전에 각 노드에서 업그레이드가 완료될 때까지 기다립니다.

- 페이지 맨 위에 있는 최상위 * 모두 승인 * 단추를 선택하여 그리드의 모든 노드를 핫픽스 대기열에 추가합니다.

> 다른 소프트웨어 업데이트를 시작하려면 StorageGRID 핫픽스를 작성해야 합니다. 핫픽스를 완료할 수 없으면 기술 지원 부서에 문의하십시오.

- 핫픽스 큐에서 노드 또는 모든 노드를 제거하려면 * 제거 * 또는 * 모두 제거 * 를 선택합니다.

  스테이지가 ""대기 중"" 이상으로 진행되면 * 제거 * 버튼이 숨겨지고 더 이상 핫픽스 프로세스에서 노드를 제거할 수 없습니다.



10. 핫픽스가 승인된 각 그리드 노드에 적용될 때까지 기다립니다.

    핫픽스가 모든 노드에 성공적으로 설치되면 핫픽스 설치 진행률 테이블이 닫힙니다. 녹색 배너는 핫픽스가 완료된 날짜와 시간을 표시합니다.

11. 핫픽스를 노드에 적용할 수 없는 경우 각 노드에 대한 오류를 검토하고 문제를 해결한 다음 이 단계를 반복합니다.

    핫픽스가 모든 노드에 성공적으로 적용될 때까지 절차가 완료되지 않습니다. 핫픽스 프로세스가 완료될 때까지 필요한 만큼 안전하게 다시 시도할 수 있습니다.

관련 정보

StorageGRID 관리

모니터링하고 문제를 해결합니다

그리드 노드 복구 절차

그리드 노드에 장애가 발생할 경우 장애가 발생한 물리적 또는 가상 서버를 교체하고, StorageGRID 소프트웨어를 재설치하고, 복구 가능한 데이터를 복구하여 복구할 수 있습니다.

하드웨어, 가상화, 운영 체제 또는 소프트웨어 장애로 인해 노드가 작동 불능 또는 불안정해질 경우 그리드 노드에 장애가 발생할 수 있습니다. 그리드 노드를 복구해야 하는 필요성을 유발할 수 있는 장애 유형에는 여러 가지가 있습니다.

그리드 노드를 복구하는 단계는 그리드 노드가 호스팅되는 플랫폼 및 그리드 노드 유형에 따라 다릅니다. 각 유형의 그리드 노드에는 정확히 따라야 하는 특정 복구 절차가 있습니다.

일반적으로 장애가 발생한 그리드 노드의 데이터를 가능한 한 보존하고, 장애가 발생한 노드를 복구 또는 교체하고, Grid Manager를 사용하여 교체 노드를 구성하고, 노드의 데이터를 복구하려고 합니다.

> 전체 StorageGRID 사이트에 장애가 발생한 경우 기술 지원 팀에 문의하십시오. 기술 지원 부서는 고객과 협력하여 복구되는 데이터의 양을 극대화하고 비즈니스 목표를 충족하는 사이트 복구 계획을 개발하고 실행합니다.

관련 정보

기술 지원 부서에서 사이트 복구를 수행하는 방법

그리드 노드 복구에 대한 경고 및 고려 사항

그리드 노드에 장애가 발생할 경우 가능한 한 빨리 복구해야 합니다. 시작하기 전에 노드 복구에 대한 모든 경고 및 고려 사항을 검토해야 합니다.

> StorageGRID는 서로 작동하는 여러 노드로 구성된 분산 시스템입니다. 디스크 스냅샷을 사용하여 그리드 노드를 복구하지 마십시오. 대신 각 노드 유형에 대한 복구 및 유지보수 절차를 참조하십시오.

장애가 발생한 그리드 노드를 가능한 한 빨리 복구하는 데에는 다음과 같은 이유가 있습니다.

- 장애가 발생한 그리드 노드는 시스템 및 개체 데이터의 중복을 감소시켜 다른 노드에 장애가 발생할 경우 영구적인 데이터 손실 위험에 노출될 수 있습니다.
- 장애가 발생한 그리드 노드는 일상적인 작업의 효율성에 영향을 미칠 수 있습니다.
- 장애가 발생한 그리드 노드는 시스템 작업을 모니터링하는 기능을 줄일 수 있습니다.
- 엄격한 ILM 규칙이 적용된 경우 그리드 노드에 장애가 발생하면 500개의 내부 서버 오류가 발생할 수 있습니다.
- 그리드 노드가 즉시 복구되지 않으면 복구 시간이 증가할 수 있습니다. 예를 들어, 복구가 완료되기 전에 지워야 하는 대기열이 있을 수 있습니다.

복구 중인 특정 유형의 그리드 노드에 대해 항상 복구 절차를 따르십시오. 복구 절차는 운영 또는 비운영 관리 노드, 게이트웨이 노드, 아카이브 노드, 어플라이언스 노드 및 스토리지 노드에 따라 다릅니다.

그리드 노드 복구 사전 조건

그리드 노드를 복구할 때는 다음 조건이 모두 적용됩니다.

- 장애가 발생한 물리적 또는 가상 하드웨어가 교체되고 구성되었습니다.

- 교체 어플라이언스의 StorageGRID 어플라이언스 설치 관리자 버전은 StorageGRID 어플라이언스 설치 관리자 버전 확인 및 업그레이드를 위한 하드웨어 설치 및 유지 보수에 설명된 대로 StorageGRID 시스템의 소프트웨어 버전과 일치합니다.
  - SG100 및 SG1000 서비스 어플라이언스
  - SG5600 스토리지 어플라이언스
  - SG5700 스토리지 어플라이언스
  - SG6000 스토리지 어플라이언스
- 운영 관리 노드 이외의 그리드 노드를 복구하는 경우 복구되는 그리드 노드와 운영 관리 노드 사이에 연결이 있습니다.

둘 이상의 그리드 노드를 호스팅하는 서버가 실패한 경우 노드 복구 순서

둘 이상의 그리드 노드를 호스팅하는 서버에 장애가 발생할 경우 노드를 순서에 관계없이 복구할 수 있습니다. 그러나 장애가 발생한 서버가 운영 관리 노드를 호스팅하는 경우에는 먼저 해당 노드를 복구해야 합니다. 운영 관리 노드를 먼저 복구하면 다른 노드 복구가 운영 관리 노드에 접속하기 위해 대기할 때 중지되지 않습니다.

복구된 노드의 **IP** 주소입니다

현재 다른 노드에 할당된 IP 주소를 사용하여 노드를 복구하려고 시도하지 마십시오. 새 노드를 구축할 때는 장애가 발생한 노드의 현재 IP 주소 또는 사용되지 않는 IP 주소를 사용합니다.

새 IP 주소를 사용하여 새 노드를 구축한 다음 노드를 복구하는 경우 복구된 노드에 새 IP 주소가 계속 사용됩니다. 원래 IP 주소로 되돌리려면 복구가 완료된 후 IP 변경 도구를 사용합니다.

그리드 노드 복구를 위해 필요한 자료를 수집합니다

유지보수 절차를 수행하기 전에 장애가 발생한 그리드 노드를 복구하는 데 필요한 자료가 있는지 확인해야 합니다.

항목	참고
StorageGRID 설치 아카이브	그리드 노드를 복구해야 하는 경우 를 수행해야 합니다 StorageGRID 설치 파일을 다운로드합니다 있습니다. • 참고: * 스토리지 노드에서 장애가 발생한 스토리지 볼륨을 복구하는 경우에는 파일을 다운로드할 필요가 없습니다.
서비스 노트북	서비스 랩톱의 구성 요소는 다음과 같습니다. • 네트워크 포트 • SSH 클라이언트(예: PuTTY) • 지원되는 웹 브라우저

항목	참고
복구 패키지 '.zip' 파일	가장 최근의 복구 패키지 파일 .zip의 사본을 구해자 복구-패키지-*id-revision*.zip으로 준비합니다 시스템이 수정될 때마다 .zip 파일의 내용이 업데이트됩니다. 이러한 변경 작업을 수행한 후 가장 최신 버전의 복구 패키지를 안전한 위치에 저장하도록 지정됩니다. 그리드 장애로부터 복구하려면 최신 복제본을 사용합니다. 기본 관리 노드가 정상적으로 작동하는 경우 그리드 관리자에서 복구 패키지를 다운로드할 수 있습니다. 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다. 그리드 관리자에 액세스할 수 없는 경우 ADC 서비스가 포함된 일부 스토리지 노드에서 복구 패키지의 암호화된 사본을 찾을 수 있습니다. 각 스토리지 노드에서 복구 패키지의 이 위치를 확인합니다. '/var/local/install/SGWS-recovery-package -*grid-id-revision*.zip.gg' 복구 패키지는 개정 번호가 가장 높은 복구 패키지를 사용합니다.
"passwords.txt" 파일	명령줄에서 그리드 노드에 액세스하는 데 필요한 암호를 포함합니다. 복구 패키지에 포함되어 있습니다.
프로비저닝 암호	StorageGRID 시스템을 처음 설치할 때 암호가 생성되고 문서화됩니다. 프로비저닝 암호문은 passwords.txt 파일에 없습니다.
현재 사용 중인 플랫폼에 대한 설명서입니다	플랫폼 공급업체의 웹 사이트에서 설명서를 참조하십시오. 현재 지원되는 플랫폼 버전은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

StorageGRID 설치 파일을 다운로드하고 압축을 풉니다

소프트웨어가 아닌 경우 소프트웨어를 다운로드하고 파일의 압축을 풉니다 스토리지 노드에서 장애가 발생한 스토리지 볼륨 복구.

그리드에서 현재 실행 중인 StorageGRID 버전을 사용해야 합니다.

단계

1. 현재 설치된 소프트웨어 버전을 확인합니다. 그리드 관리자 상단에서 도움말 아이콘을 선택하고 * 정보 * 를 선택합니다.
2. 로 이동합니다 "StorageGRID용 NetApp 다운로드 페이지".
3. 그리드에서 현재 실행 중인 StorageGRID 버전을 선택합니다.

   StorageGRID 소프트웨어 버전은 11.x.y 형식으로 되어 있습니다.

4. NetApp 계정의 사용자 이름과 암호를 사용하여 로그인합니다.
5. 최종 사용자 사용권 계약을 읽고 확인란을 선택한 다음 * 동의 및 계속 * 을 선택합니다.
6. 다운로드 페이지의 * StorageGRID * 설치 열에서 해당 플랫폼의 ".tgz" 또는 ".zip" 파일을 선택합니다.

설치 아카이브 파일에 표시된 버전이 현재 설치된 소프트웨어 버전과 일치해야 합니다.

Windows를 실행 중인 경우 '.zip' 파일을 사용합니다.

플랫폼	설치 아카이브
Red Hat Enterprise Linux 또는 CentOS	'S torageGRID-Webscale-*version*-RPM-*UniqueID*.zip"S torageGRID-Webscale-*version*-RPM-*UniqueID*.tgz'
Ubuntu 또는 Debian 또는 어플라이언스	'storageGRID-Webscale-*version*-deb-*UniqueID*.zip"storageGRID-Webscale-*version*-deb-*UniqueID*.tgz'
VMware	'S torageGRID-Webscale-*version*-vmware-*UniqueID*.zip"S torageGRID-Webscale-*version*-vmware-*UniqueID*.tgz'

7. 아카이브 파일을 다운로드하고 압축을 풉니다.
8. 플랫폼에 적합한 단계에 따라 필요한 파일과 복구해야 할 그리드 노드를 기반으로 선택하십시오.

   각 플랫폼의 단계에 나열된 경로는 아카이브 파일에 의해 설치된 최상위 디렉토리를 기준으로 합니다.

9. 를 복구하는 경우 Red Hat Enterprise Linux 또는 CentOS 시스템에서 해당 파일을 선택합니다.

경로 및 파일 이름입니다	설명
	StorageGRID 다운로드 파일에 포함된 모든 파일을 설명하는 텍스트 파일입니다.
	제품에 대한 지원 권한을 제공하지 않는 무료 라이센스입니다.
	RHEL 또는 CentOS 호스트에 StorageGRID 노드 이미지를 설치하기 위한 rpm 패키지입니다.
	RHEL 또는 CentOS 호스트에 StorageGRID 호스트 서비스를 설치하기 위한 rpm 패키지입니다.
배포 스크립팅 도구	설명
	StorageGRID 시스템 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
	StorageGRID 어플라이언스 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
/rpms/configure -StorageGrid.sample.json	"configure-StorageGrid.py" 스크립트와 함께 사용할 구성 파일의 예

경로 및 파일 이름입니다	설명
	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/rpms/configure -StorageGrid.blank.json을 지정합니다	configure-StorageGrid.py 스크립트와 함께 사용할 빈 구성 파일입니다.
	StorageGRID 컨테이너 배포를 위한 RHEL 또는 CentOS 호스트 구성을 위한 Ansible 역할 및 플레이북의 예 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.
/rpms/Extras/API-schemas	StorageGRID에 대한 API 스키마입니다. • 참고 *: 업그레이드를 수행하기 전에 이러한 스키마를 사용하여 StorageGRID 관리 API를 사용하도록 작성한 코드가 업그레이드 호환성 테스트를 위한 비프로덕션 StorageGRID 환경이 없는 경우 새 StorageGRID 릴리스와 호환되는지 확인할 수 있습니다.

1. 를 복구하는 경우 Ubuntu 또는 Debian 시스템에서 해당 파일을 선택합니다.

경로 및 파일 이름입니다	설명
	StorageGRID 다운로드 파일에 포함된 모든 파일을 설명하는 텍스트 파일입니다.
/debs/NLF000000.txt 를 참조하십시오	테스트 및 개념 증명 배포에 사용할 수 있는 비프로덕션 NetApp 라이센스 파일.
/debs/storagegrid-webscale-images-version-SHA.deb 를 참조하십시오	StorageGRID 노드 이미지를 Ubuntu 또는 Debian 호스트에 설치하기 위한 DEB 패키지.
/debs/storagegrid-webscale-images-version-SHA.deb.md5 를 참조하십시오	파일 '/debs/storagegrid-webscale-images-version-SHA.deb` 에 대한 MD5 체크섬입니다.
/debs/storagegrid-webscale-service-version-SHA.deb 를 참조하십시오	Ubuntu 또는 Debian 호스트에 StorageGRID 호스트 서비스를 설치하기 위한 DEB 패키지.
배포 스크립팅 도구	설명
/debs/configure-storagegrid.py 를 참조하십시오	StorageGRID 시스템 구성을 자동화하는 데 사용되는 Python 스크립트입니다.

경로 및 파일 이름입니다	설명
/debs/configure-sga.py 를 참조하십시오	StorageGRID 어플라이언스 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
/debs/storagegrid-ssoauth.py 를 참조하십시오	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/debs/configure -StorageGrid.sample.json 을 참조하십시오	"configure-StorageGrid.py" 스크립트와 함께 사용할 구성 파일의 예
/debs/configure -StorageGrid.blank.json 을 참조하십시오	configure-StorageGrid.py 스크립트와 함께 사용할 빈 구성 파일입니다.
	StorageGRID 컨테이너 배포를 위한 Ubuntu 또는 Debian 호스트 구성을 위한 Ansible 역할 및 플레이북 예 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.
/debs/Extras/API-schemas	StorageGRID에 대한 API 스키마입니다. • 참고 *: 업그레이드를 수행하기 전에 이러한 스키마를 사용하여 StorageGRID 관리 API를 사용하도록 작성한 코드가 업그레이드 호환성 테스트를 위한 비프로덕션 StorageGRID 환경이 없는 경우 새 StorageGRID 릴리스와 호환되는지 확인할 수 있습니다.

1. 를 복구하는 경우 VMware 시스템에서 해당 파일을 선택합니다.

경로 및 파일 이름입니다	설명
	StorageGRID 다운로드 파일에 포함된 모든 파일을 설명하는 텍스트 파일입니다.
	제품에 대한 지원 권한을 제공하지 않는 무료 라이센스입니다.
	그리드 노드 가상 머신을 생성하기 위한 템플릿으로 사용되는 가상 머신 디스크 파일입니다.
	기본 관리 노드를 배포하기 위한 오픈 가상화 형식 템플릿 파일(".ovf") 및 매니페스트 파일(".mf")입니다.
	비기본 관리 노드를 배포하기 위한 템플릿 파일(".ovf")과 매니페스트 파일(".mf")입니다.

경로 및 파일 이름입니다	설명
/vSphere/vSphere-archive.ovf./vSphere/vSphere-archive.mf	아카이브 노드 배포를 위한 템플릿 파일(".ovf")과 매니페스트 파일(".mf")입니다.
	게이트웨이 노드를 배포하기 위한 템플릿 파일(".ovf")과 매니페스트 파일(".mf")입니다.
	가상 머신 기반 스토리지 노드 구축을 위한 템플릿 파일('.ovf') 및 매니페스트 파일('.mf')입니다.
배포 스크립팅 도구	설명
	가상 그리드 노드의 배포를 자동화하는 데 사용되는 Bash 쉘 스크립트입니다.
	'deploy-vsphere-ovftool.sh' 스크립트와 함께 사용할 구성 파일의 예.
	StorageGRID 시스템 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
	StorageGRID 어플라이언스 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/vSphere/configure -StorageGrid.sample.json을 참조하십시오	"configure-StorageGrid.py" 스크립트와 함께 사용할 구성 파일의 예
/vSphere/configure -StorageGrid.blank.json 을 참조하십시오	configure-StorageGrid.py 스크립트와 함께 사용할 빈 구성 파일입니다.
/vSphere/Extras/API-schemas	StorageGRID에 대한 API 스키마입니다. • 참고 *: 업그레이드를 수행하기 전에 이러한 스키마를 사용하여 StorageGRID 관리 API를 사용하도록 작성한 코드가 업그레이드 호환성 테스트를 위한 비프로덕션 StorageGRID 환경이 없는 경우 새 StorageGRID 릴리스와 호환되는지 확인할 수 있습니다.

1. StorageGRID 어플라이언스 기반 시스템을 복구하는 경우 적절한 파일을 선택합니다.

경로 및 파일 이름입니다	설명
/debs/storagegrid-webscale-images-version-SHA.deb 를 참조하십시오	어플라이언스에 StorageGRID 노드 이미지를 설치하기 위한 DEB 패키지.
/debs/storagegrid-webscale-images-version-SHA.deb.md5 를 참조하십시오	업로드 후 패키지가 손상되지 않았는지 확인하기 위해 StorageGRID 어플라이언스 설치 프로그램에서 사용하는 DEB 설치 패키지의 체크섬입니다.

> 어플라이언스 설치의 경우, 이러한 파일은 네트워크 트래픽을 방지해야 하는 경우에만 필요합니다. 어플라이언스는 기본 관리 노드에서 필요한 파일을 다운로드할 수 있습니다.

노드 복구 절차를 선택합니다

실패한 노드 유형에 대해 올바른 복구 절차를 선택해야 합니다.

그리드 노드	복구 절차
둘 이상의 스토리지 노드	기술 지원 부서에 문의하십시오. 둘 이상의 스토리지 노드에 장애가 발생한 경우 기술 지원 부서에서 복구를 지원하여 데이터 손실을 초래하는 데이터베이스 불일치를 방지해야 합니다. 사이트 복구 절차가 필요할 수 있습니다. 기술 지원 부서에서 사이트 복구를 수행하는 방법
단일 스토리지 노드	스토리지 노드 복구 절차는 장애 유형과 기간에 따라 다릅니다. 스토리지 노드 장애 복구
관리자 노드	관리 노드 절차는 기본 관리 노드 또는 비 기본 관리 노드 복구 여부에 따라 달라집니다. 관리자 노드 오류에서 복구
게이트웨이 노드	게이트웨이 노드에서 복구.
아카이브 노드	아카이브 노드 장애에서 복구.

> 둘 이상의 그리드 노드를 호스팅하는 서버에 장애가 발생할 경우 노드를 순서에 관계없이 복구할 수 있습니다. 그러나 장애가 발생한 서버가 운영 관리 노드를 호스팅하는 경우에는 먼저 해당 노드를 복구해야 합니다. 운영 관리 노드를 먼저 복구하면 다른 노드 복구가 운영 관리 노드에 접속하기 위해 대기할 때 중지되지 않습니다.

스토리지 노드 장애 복구

장애가 발생한 스토리지 노드를 복구하는 절차는 장애 유형과 장애가 발생한 스토리지 노드 유형에 따라 다릅니다.

이 표를 사용하여 장애가 발생한 스토리지 노드에 대한 복구 절차를 선택합니다.

문제	조치	참고
• 둘 이상의 스토리지 노드에 장애가 발생했습니다. • 스토리지 노드 장애 또는 복구 후 15일 이내에 두 번째 스토리지 노드에 장애가 발생했습니다. 다른 스토리지 노드의 복구가 진행 중인 동안 스토리지 노드에 장애가 발생한 경우를 포함합니다.	기술 지원 부서에 문의해야 합니다.	장애가 발생한 모든 스토리지 노드가 동일한 사이트에 있는 경우 사이트 복구 절차를 수행해야 할 수 있습니다. 기술 지원 부서에서 고객의 상황을 평가하고 복구 계획을 개발합니다. 기술 지원 부서에서 사이트 복구를 수행하는 방법 둘 이상의 스토리지 노드(또는 15일 이내에 둘 이상의 스토리지 노드)를 복구하는 경우 Cassandra 데이터베이스의 무결성에 영향을 주어 데이터가 손실될 수 있습니다. 기술 지원 부서에서는 보조 스토리지 노드의 복구를 시작하는 것이 안전한 시기를 결정할 수 있습니다. • 참고 *: 한 사이트에서 ADC 서비스를 포함하는 스토리지 노드가 두 개 이상 장애가 발생하면 해당 사이트에 대한 보류 중인 플랫폼 서비스 요청이 손실됩니다.
스토리지 노드가 15일 이상 오프라인 상태입니다.	스토리지 노드를 15일 이상 복구합니다	Cassandra 데이터베이스 무결성을 보장하기 위해 이 절차가 필요합니다.
어플라이언스 스토리지 노드에 장애가 발생했습니다.	어플라이언스 스토리지 노드를 복구합니다	어플라이언스 스토리지 노드의 복구 절차는 모든 장애 시 동일합니다.
하나 이상의 스토리지 볼륨에 오류가 발생했지만 시스템 드라이브가 손상되지 않았습니다	시스템 드라이브가 손상되지 않은 스토리지 볼륨 장애로부터 복구합니다	이 절차는 소프트웨어 기반 스토리지 노드에 사용됩니다.
시스템 드라이브에 오류가 발생했습니다.	시스템 드라이브 오류에서 복구합니다	노드 교체 절차는 구축 플랫폼과 스토리지 볼륨의 장애 여부에도 따라 달라집니다.

일부 StorageGRID 복구 절차에서는 리퍼를 사용하여 Cassandra 수리를 처리합니다. 관련 또는 필수 서비스가 시작되는 즉시 수리가 자동으로 이루어집니다. "리퍼" 또는 "'Cassandra 수리'라는 스크립트 출력을 볼 수 있습니다. 복구가 실패했다는 오류 메시지가 나타나면 오류 메시지에 표시된 명령을 실행합니다.

단일 스토리지 노드가 오프라인이고 다른 스토리지 노드에 15일 이상 연결되지 않은 경우 노드에서 Cassandra를 재구성해야 합니다.

필요한 것

- 스토리지 노드 사용 중지가 진행 중이 아니거나 노드 사용 중단 절차를 일시 중지했습니다. (Grid Manager에서 * 유지보수 * > * 작업 * > * 서비스 해제 * 를 선택합니다.)
- 확장이 진행 중이 아닌 것을 확인했습니다. (Grid Manager에서 * 유지보수 * > * 작업 * > * 확장 * 을 선택합니다.)

이 작업에 대해

스토리지 노드에는 개체 메타데이터가 포함된 Cassandra 데이터베이스가 있습니다. 스토리지 노드가 15일 이상 다른 스토리지 노드와 통신할 수 없는 경우 StorageGRID는 노드의 Cassandra 데이터베이스가 오래된 것으로 가정합니다. Cassandra가 다른 스토리지 노드의 정보를 사용하여 재구축될 때까지 스토리지 노드를 그리드에 다시 연결할 수 없습니다.

단일 스토리지 노드가 다운된 경우에만 Cassandra를 재구축하려면 다음 절차를 따르십시오. 추가 스토리지 노드가 오프라인이거나 Cassandra가 지난 15일 이내에 다른 스토리지 노드에 재구축된 경우 기술 지원 부서에 문의하십시오. 예를 들어, Cassandra는 실패한 스토리지 볼륨을 복구하거나 장애가 발생한 스토리지 노드를 복구하는 절차의 일부로 재구성되었을 수 있습니다.

> 둘 이상의 스토리지 노드에 장애가 있거나 오프라인 상태인 경우 기술 지원 부서에 문의하십시오. 다음 복구 절차를 수행하지 마십시오. 데이터가 손실될 수 있습니다.

> 스토리지 노드 장애 또는 복구 후 15일 이내에 두 번째 스토리지 노드 오류인 경우 기술 지원 부서에 문의하십시오. 다음 복구 절차를 수행하지 마십시오. 데이터가 손실될 수 있습니다.

> 한 사이트에 둘 이상의 스토리지 노드에 장애가 발생한 경우 사이트 복구 절차가 필요할 수 있습니다. 기술 지원 부서에 문의하십시오.

기술 지원 부서에서 사이트 복구를 수행하는 방법

단계

1. 필요한 경우 복구해야 할 스토리지 노드의 전원을 켭니다.
2. 그리드 노드에 로그인합니다.
   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트는 "$"에서 "#"로 바뀝니다

> 그리드 노드에 로그인할 수 없는 경우 시스템 디스크가 손상되지 않았을 수 있습니다. 의 절차로 이동합니다 시스템 드라이브 장애 복구.

1. 스토리지 노드에서 다음 검사를 수행합니다.

a. 이 명령을 'NOdetool status'로 발행한다

   출력은 "연결 거부"여야 합니다

b. Grid Manager에서 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.

c. 사이트 * > * 스토리지 노드 * > * SSM * > * 서비스 * 를 선택합니다. Cassandra 서비스에 Not Running(실행되지 않음) 이 표시되는지 확인합니다.

d. 스토리지 노드 * > * SSM * > * 리소스 * 를 선택합니다. 볼륨 섹션에 오류 상태가 없는지 확인합니다.

e. 'grep-i Cassandra/var/local/log/ServerManager.log' 명령을 실행합니다

   출력에 다음 메시지가 표시됩니다.

```
Cassandra not started because it has been offline for more than 15 day
grace period - rebuild Cassandra
```

2. 이 명령을 실행하고 스크립트 출력('check-cassandra-rebuild')을 모니터링합니다
   - 스토리지 서비스가 실행 중인 경우 서비스를 중지하라는 메시지가 표시됩니다. 입력: * y *
   - 스크립트의 경고를 검토합니다. 해당 사항이 없는 경우 Cassandra를 다시 빌드할지 확인합니다. 입력: * y *

> 일부 StorageGRID 복구 절차에서는 리퍼를 사용하여 Cassandra 수리를 처리합니다. 관련 또는 필수 서비스가 시작되는 즉시 수리가 자동으로 이루어집니다. "리퍼" 또는 "'Cassandra 수리'라는 스크립트 출력을 볼 수 있습니다. 복구가 실패했다는 오류 메시지가 나타나면 오류 메시지에 표시된 명령을 실행합니다.

3. 재생성이 완료된 후 다음 검사를 수행합니다.

   a. Grid Manager에서 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.

   b. 사이트 _ * > * 복구된 스토리지 노드 * > * SSM * > * 서비스 * 를 선택합니다.

   c. 모든 서비스가 실행 중인지 확인합니다.

   d. DDS * > * Data Store * 를 선택합니다.

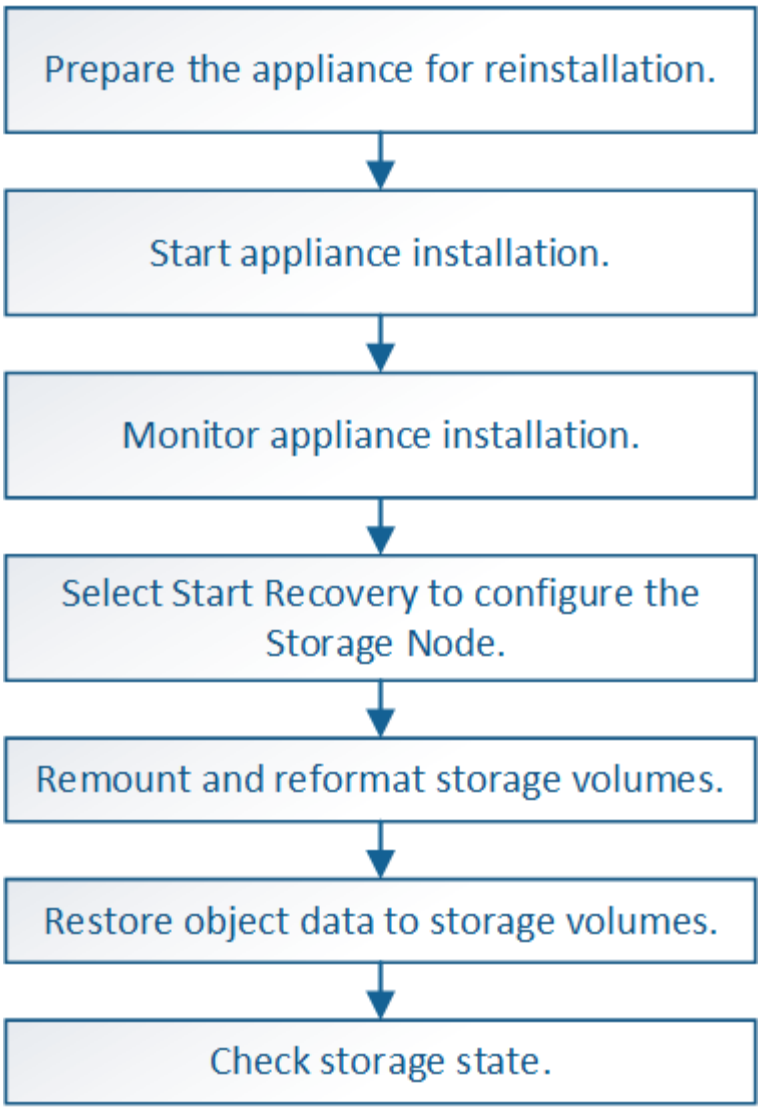
   e. Data Store Status * 가 "Up"이고 * Data Store State * 가 "Normal"인지 확인합니다.

어플라이언스 스토리지 노드를 복구합니다

장애가 발생한 StorageGRID 어플라이언스 스토리지 노드를 복구하는 절차는 시스템 드라이브 손실 또는 스토리지 볼륨 손실에서 복구하든 동일합니다.

이 작업에 대해

어플라이언스를 준비하고 소프트웨어를 재설치하고, 그리드에 다시 참가하도록 노드를 구성하고, 스토리지를 다시 포맷하고, 객체 데이터를 복원해야 합니다.



둘 이상의 스토리지 노드에 장애가 있거나 오프라인 상태인 경우 기술 지원 부서에 문의하십시오. 다음 복구 절차를 수행하지 마십시오. 데이터가 손실될 수 있습니다.

스토리지 노드 장애 또는 복구 후 15일 이내에 두 번째 스토리지 노드 오류인 경우 기술 지원 부서에 문의하십시오. 15일 이내에 두 개 이상의 스토리지 노드에서 Cassandra를 재구축하면 데이터가 손실될 수 있습니다.

한 사이트에 둘 이상의 스토리지 노드에 장애가 발생한 경우 사이트 복구 절차가 필요할 수 있습니다. 기술 지원 부서에 문의하십시오.

기술 지원 부서에서 사이트 복구를 수행하는 방법

ILM 규칙이 복제된 복사본을 하나만 저장하도록 구성되어 있고 해당 복사본이 실패한 스토리지 볼륨에 있으면 개체를 복구할 수 없습니다.

복구 중 서비스:상태-Cassandra(SVST) 경보가 발생하는 경우, Cassandra를 재작성하여 모니터링 및 문제 해결 지침을 참조하여 알람에서 복구합니다. Cassandra가 재구축된 후에는 경보가 지워집니다. 알람이 소거되지 않으면 기술 지원 부서에 문의하십시오.

컨트롤러 교체 또는 SANtricity OS 재설치 지침과 같은 하드웨어 유지보수 절차는 스토리지 어플라이언스의 설치 및 유지보수 지침을 참조하십시오.

관련 정보

모니터링하고 문제를 해결합니다

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

SG5600 스토리지 어플라이언스

어플라이언스 스토리지 노드의 재설치를 준비합니다

어플라이언스 스토리지 노드를 복구할 때는 먼저 StorageGRID 소프트웨어 재설치를 위한 어플라이언스를 준비해야 합니다.

1. 장애가 발생한 스토리지 노드에 로그인:

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. StorageGRID 소프트웨어 설치를 위해 어플라이언스 스토리지 노드를 준비합니다. '제왕절개술'

3. 계속하라는 메시지가 나타나면 y를 입력합니다

   어플라이언스가 재부팅되고 SSH 세션이 종료됩니다. StorageGRID 어플라이언스 설치 프로그램을 사용할 수 있게 되기까지 일반적으로 5분이 걸리지만 경우에 따라 최대 30분까지 기다려야 할 수도 있습니다.

   StorageGRID 어플라이언스 스토리지 노드가 재설정되고 스토리지 노드의 데이터에 더 이상 액세스할 수 없습니다. 원래 설치 프로세스 중에 구성된 IP 주소는 그대로 유지되지만 절차가 완료되면 이를 확인하는 것이 좋습니다.

   'Sareinstall' 명령을 실행하면 StorageGRID로 프로비저닝된 모든 계정, 암호 및 SSH 키가 제거되고 새 호스트 키가 생성됩니다.

StorageGRID 어플라이언스 설치를 시작합니다

어플라이언스 스토리지 노드에 StorageGRID를 설치하려면 어플라이언스에 포함된 StorageGRID 어플라이언스 설치 프로그램을 사용합니다.

필요한 것

- 이 어플라이언스는 랙에 설치되어 있고 네트워크에 연결되어 있으며 전원이 켜져 있습니다.
- 네트워크 링크 및 IP 주소는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스에 대해 구성되었습니다.

- StorageGRID 그리드에 대한 기본 관리 노드의 IP 주소를 알고 있습니다.
- StorageGRID 어플라이언스 설치 프로그램의 IP 구성 페이지에 나열된 모든 그리드 네트워크 서브넷은 기본 관리 노드의 그리드 네트워크 서브넷 목록에 정의되어 있습니다.
- 스토리지 어플라이언스에 대한 설치 및 유지 관리 지침에 따라 이러한 필수 작업을 완료했습니다.
  - SG5600 스토리지 어플라이언스
  - SG5700 스토리지 어플라이언스
  - SG6000 스토리지 어플라이언스
- 을(를) 사용하고 있습니다 지원되는 웹 브라우저.
- 어플라이언스의 컴퓨팅 컨트롤러에 할당된 IP 주소 중 하나를 알고 있습니다. 관리 네트워크(컨트롤러의 관리 포트 1), 그리드 네트워크 또는 클라이언트 네트워크의 IP 주소를 사용할 수 있습니다.

이 작업에 대해

어플라이언스 스토리지 노드에 StorageGRID를 설치하려면 다음을 따르십시오.

- 기본 관리 노드의 IP 주소와 노드 이름을 지정하거나 확인합니다.
- 설치를 시작하고 볼륨이 구성되고 소프트웨어가 설치될 때까지 기다립니다.
- 프로세스가 중간에 진행되면 설치가 일시 중지됩니다. 설치를 다시 시작하려면 그리드 관리자에 로그인하고 장애가 발생한 노드의 대체 노드로 보류 중인 스토리지 노드를 구성해야 합니다.
- 노드를 구성한 후에는 어플라이언스 설치 프로세스가 완료되고 어플라이언스가 재부팅됩니다.

단계

1. 브라우저를 열고 어플라이언스에서 컴퓨팅 컨트롤러의 IP 주소 중 하나를 입력합니다.

   (https://Controller_IP:8443`)

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 기본 관리 노드 연결 섹션에서 기본 관리 노드의 IP 주소를 지정해야 하는지 여부를 확인합니다.

   StorageGRID 어플라이언스 설치 관리자는 기본 관리 노드 또는 admin_IP가 구성된 다른 그리드 노드가 동일한 서브넷에 있다고 가정하여 이 IP 주소를 자동으로 검색할 수 있습니다.

3. 이 IP 주소가 표시되지 않거나 변경해야 하는 경우 주소를 지정합니다.

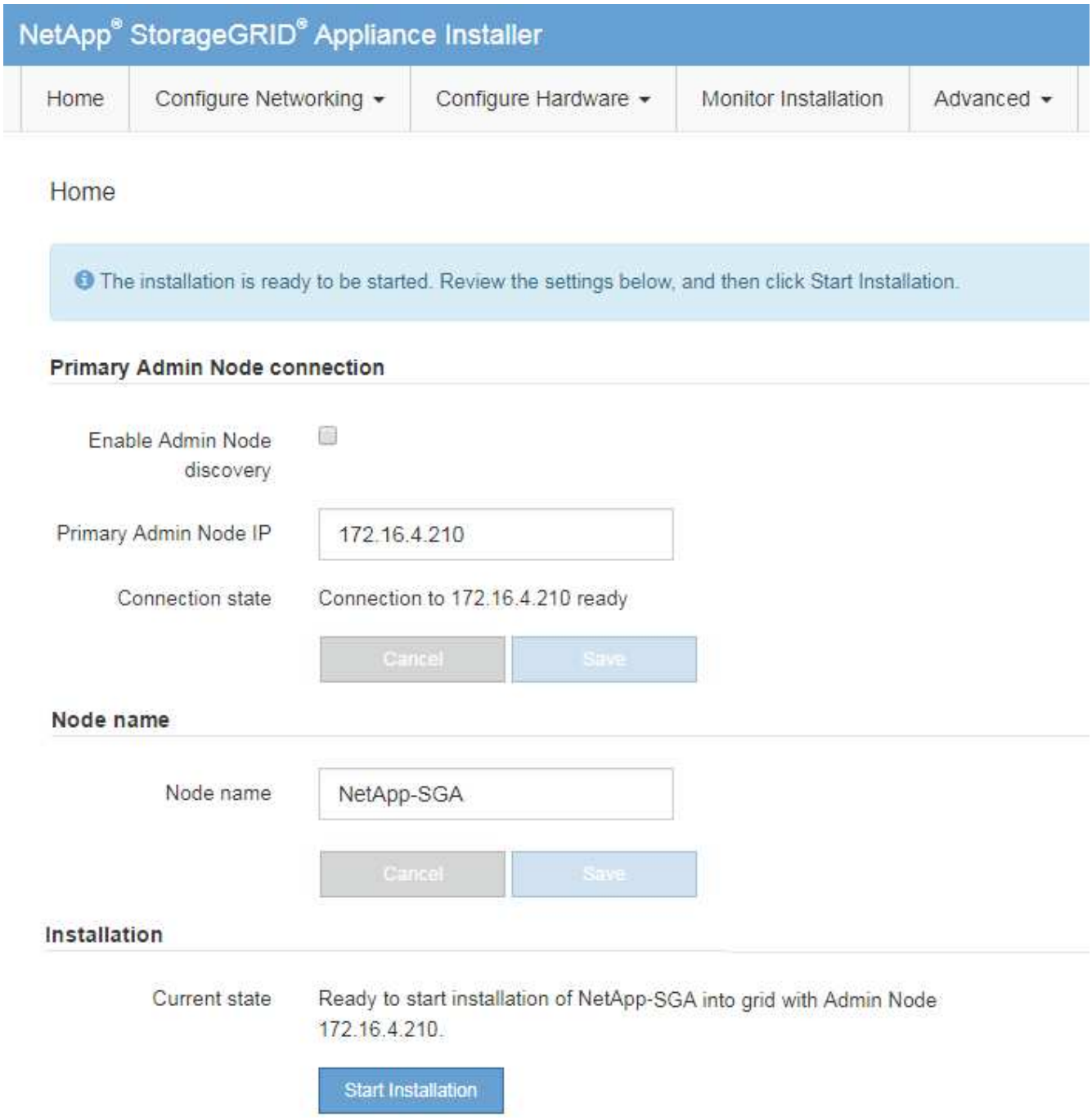
옵션을 선택합니다	단계
수동 IP 입력	a. 관리자 노드 검색 사용 * 확인란의 선택을 취소합니다. b. IP 주소를 수동으로 입력합니다. c. 저장 * 을 클릭합니다. d. 새 IP 주소의 연결 상태가 "다시 준비"가 될 때까지 기다립니다.

옵션을 선택합니다	단계
연결된 모든 운영 관리 노드의 자동 검색	a. 관리자 노드 검색 사용 * 확인란을 선택합니다. b. 검색된 IP 주소 목록에서 이 어플라이언스 스토리지 노드를 구축할 그리드의 기본 관리 노드를 선택합니다. c. 저장 * 을 클릭합니다. d. 새 IP 주소의 연결 상태가 "다시 준비"가 될 때까지 기다립니다.

4. Node Name * 필드에 복구 중인 노드에 사용된 이름과 동일한 이름을 입력하고 * Save * 를 클릭합니다.
5. 설치 섹션에서 현재 상태가 ""운영 관리 노드 admin_IP를 사용하여 노드 이름을 그리드에 설치 시작 준비 완료"이고 * 설치 시작 * 버튼이 활성화되어 있는지 확인합니다.

   설치 시작 * 버튼이 활성화되지 않은 경우 네트워크 구성 또는 포트 설정을 변경해야 할 수 있습니다. 자세한 내용은 제품의 설치 및 유지보수 지침을 참조하십시오.

6. StorageGRID 어플라이언스 설치 관리자 홈 페이지에서 * 설치 시작 * 을 클릭합니다.



현재 상태가 ""설치 진행 중""으로 변경되고 모니터 설치 페이지가 표시됩니다.

> 모니터 설치 페이지에 수동으로 액세스해야 하는 경우 메뉴 모음에서 * 모니터 설치 * 를 클릭합니다.

관련 정보

SG100 및 SG1000 서비스 어플라이언스

SG6000 스토리지 어플라이언스

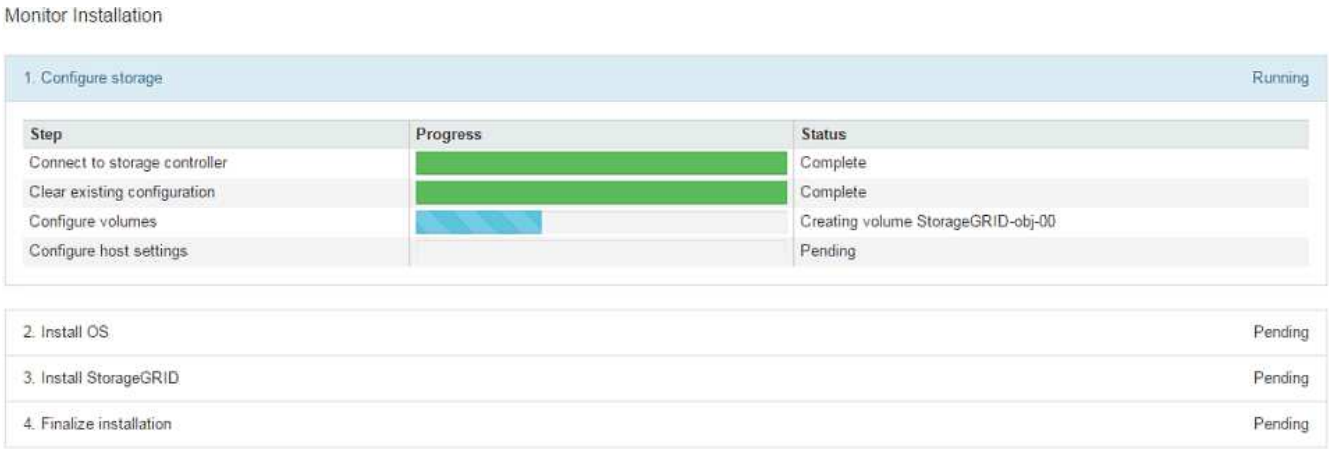
SG5700 스토리지 어플라이언스

SG5600 스토리지 어플라이언스

StorageGRID 어플라이언스 설치 프로그램은 설치가 완료될 때까지 상태를 제공합니다. 소프트웨어 설치가 완료되면 어플라이언스가 재부팅됩니다.

1. 설치 진행률을 모니터링하려면 메뉴 표시줄에서 * 모니터 설치 * 를 클릭합니다.

   Monitor Installation(모니터 설치) 페이지에 설치 진행률이 표시됩니다.

   파란색 상태 표시줄은 현재 진행 중인 작업을 나타냅니다. 녹색 상태 표시줄은 성공적으로 완료된 작업을 나타냅니다.

   > 설치 프로그램은 이전 설치에서 완료된 작업이 다시 실행되지 않도록 합니다. 설치를 다시 실행할 경우 다시 실행할 필요가 없는 작업은 녹색 상태 표시줄과 "중단" 상태로 표시됩니다.

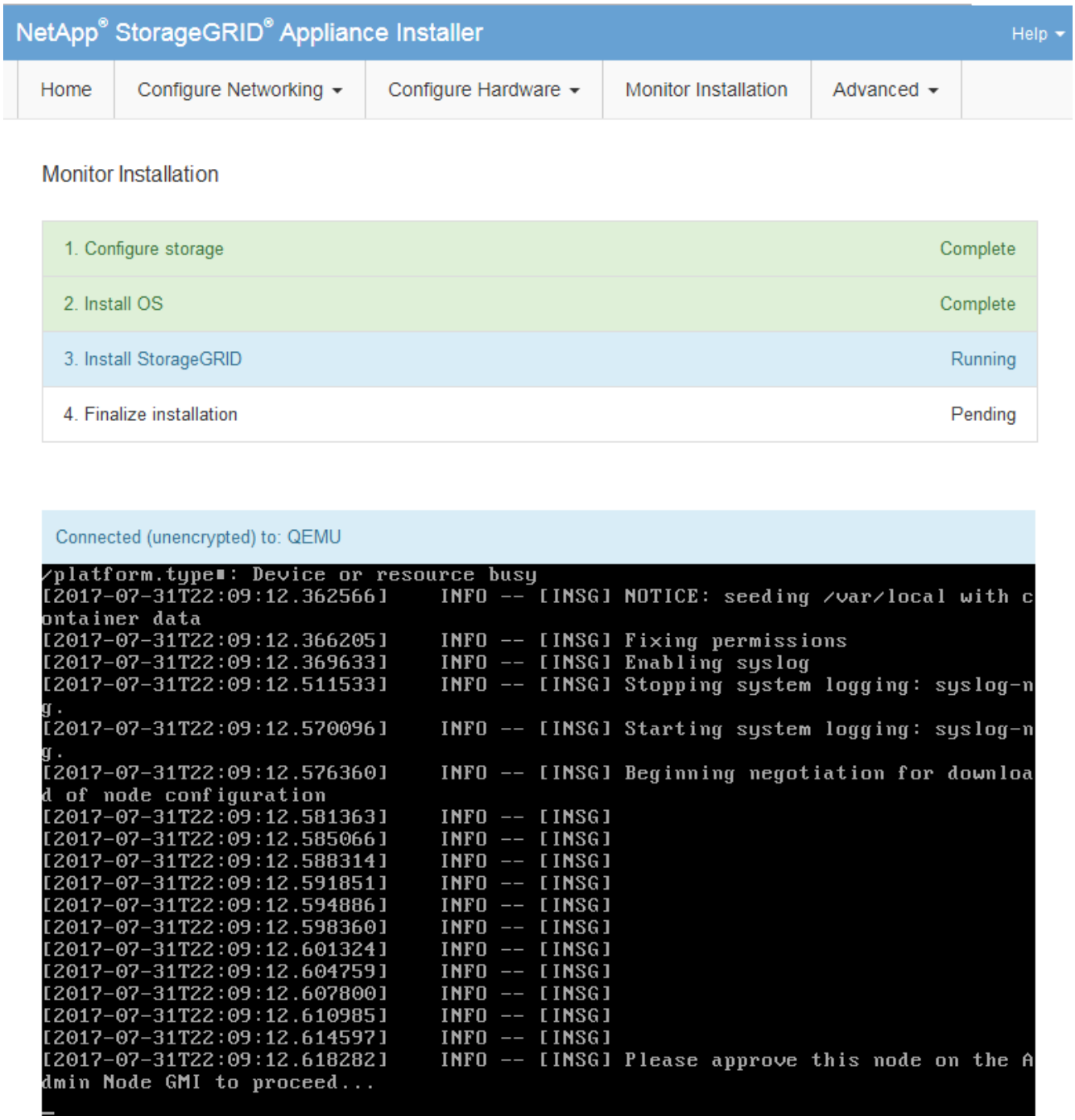
2. 처음 두 설치 단계의 진행 상황을 검토합니다.
   - * 1. 스토리지 구성 *

     이 단계에서 설치 관리자는 스토리지 컨트롤러에 연결하고, 기존 구성을 지우고, SANtricity 소프트웨어와 통신하여 볼륨을 구성하고, 호스트 설정을 구성합니다.

   - * 2. OS * 를 설치합니다

     이 단계에서 설치 프로그램은 StorageGRID의 기본 운영 체제 이미지를 어플라이언스에 복사합니다.

3. StorageGRID* 설치 단계가 일시 중지되고 그리드 관리자를 사용하여 관리 노드에서 이 노드를 승인하라는 메시지가 포함된 콘솔에 표시될 때까지 설치 진행 상태를 계속 모니터링합니다.



4. 어플라이언스 스토리지 노드를 구성하는 절차로 이동합니다.

Start Recovery(복구 시작**)** 를 선택하여 어플라이언스 스토리지 노드를 구성합니다

장애가 발생한 노드의 대체품으로 어플라이언스 스토리지 노드를 구성하려면 그리드 관리자에서 복구 시작을 선택해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.

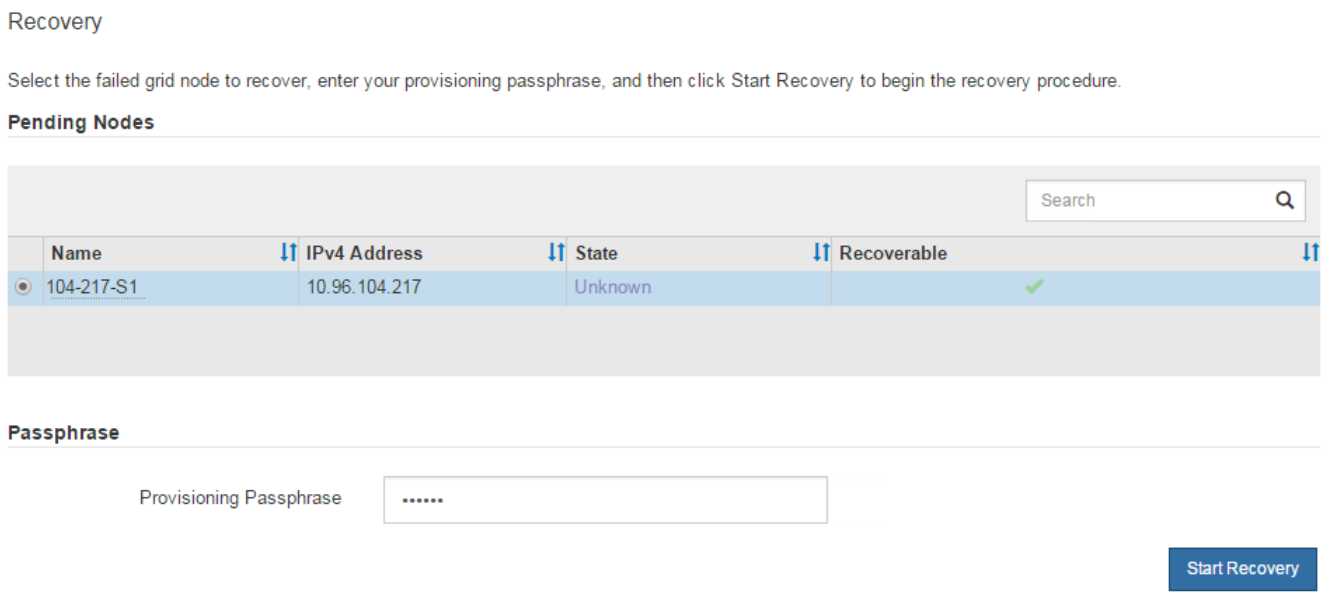
- 복구 어플라이언스 스토리지 노드를 구축해야 합니다.
- 삭제 코딩 데이터에 대한 복구 작업의 시작 날짜를 알아야 합니다.
- 스토리지 노드가 지난 15일 이내에 재구축되지 않은 것을 확인해야 합니다.

단계

1. Grid Manager에서 * 유지보수 * > * 작업 * > * 복구 * 를 선택합니다.
2. Pending Nodes 목록에서 복구할 그리드 노드를 선택합니다.

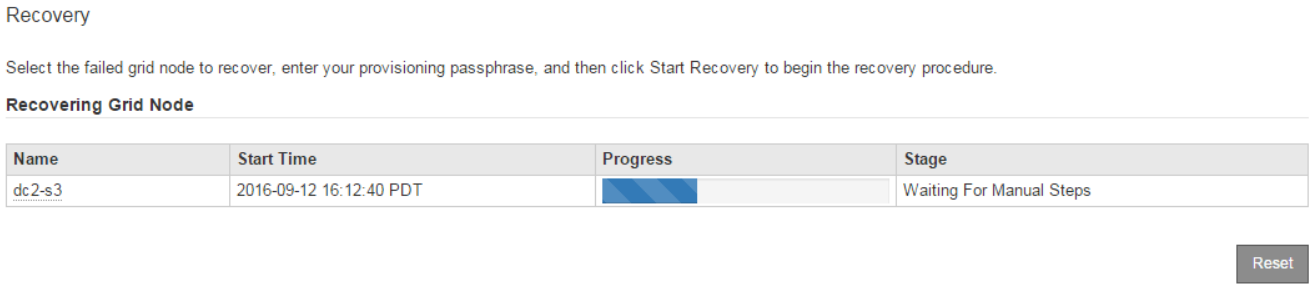
   노드가 실패한 후 목록에 나타나지만 다시 설치되고 복구 준비가 될 때까지 노드를 선택할 수 없습니다.

3. Provisioning Passphrase * 를 입력합니다.
4. 복구 시작 * 을 클릭합니다.

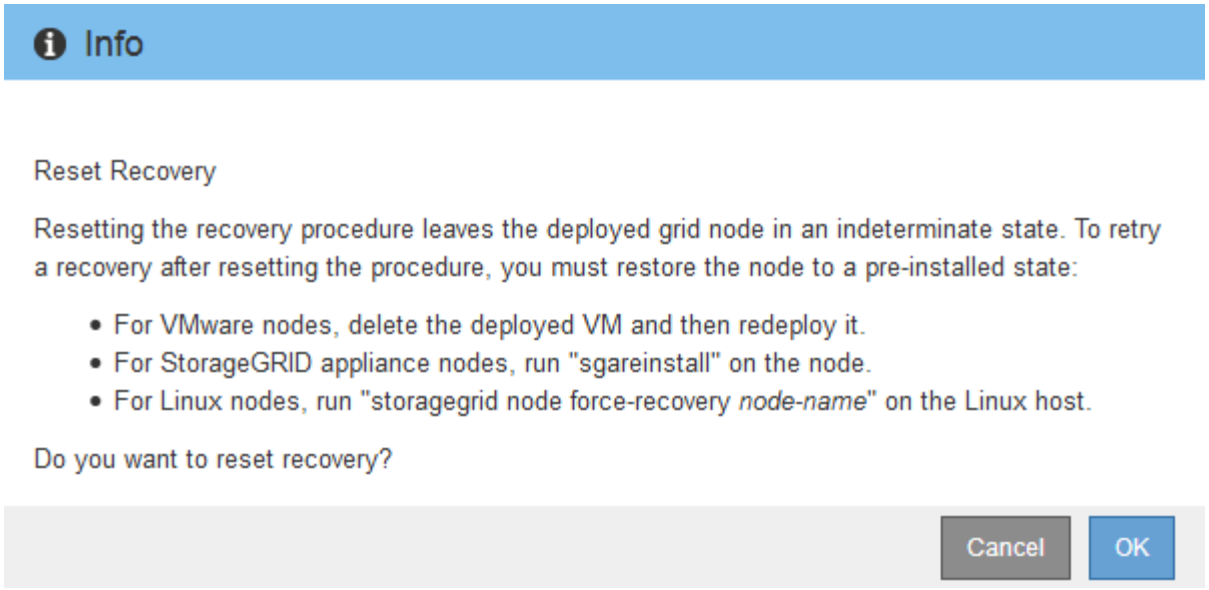


5. 복구 그리드 노드 테이블에서 복구 진행률을 모니터링합니다.

   그리드 노드가 ""수동 단계 대기 중" 단계에 도달하면 다음 항목으로 이동하여 어플라이언스 스토리지 볼륨을 다시 마운트하고 다시 포맷하는 수동 단계를 수행합니다.



> 복구 중에 언제든지 * Reset * (재설정 *)을 클릭하여 새 복구를 시작할 수 있습니다. 프로시저를 재설정하면 노드가 결정되지 않은 상태로 남아 있음을 나타내는 정보 대화 상자가 나타납니다.



절차를 재설정한 후 복구를 재시도하려면 노드에 '설치'를 실행하여 어플라이언스 노드를 사전 설치 상태로 복원해야 합니다.

어플라이언스 스토리지 볼륨을 다시 마운트하고 다시 포맷합니다**("**수동 단계**").**

보존된 스토리지 볼륨을 다시 마운트하고 장애가 발생한 스토리지 볼륨을 다시 포맷하려면 두 개의 스크립트를 수동으로 실행해야 합니다. 첫 번째 스크립트는 StorageGRID 스토리지 볼륨으로 올바르게 포맷된 볼륨을 다시 마운트합니다. 두 번째 스크립트는 마운트 해제된 볼륨을 다시 포맷하고 필요한 경우 Cassandra 데이터베이스를 재구축하며 서비스를 시작합니다.

필요한 것

- 장애가 발생한 스토리지 볼륨의 하드웨어를 교체하도록 이미 교체했습니다.

  'n-다시 마운트-볼륨' 스크립트를 실행하면 오류가 발생한 추가 스토리지 볼륨을 식별하는 데 도움이 될 수 있습니다.

- 스토리지 노드 사용 중지가 진행 중이 아니거나 노드 사용 중단 절차를 일시 중지했습니다. (Grid Manager에서 * 유지보수 * > * 작업 * > * 서비스 해제 * 를 선택합니다.)
- 확장이 진행 중이 아닌 것을 확인했습니다. (Grid Manager에서 * 유지보수 * > * 작업 * > * 확장 * 을 선택합니다.)

> 두 개 이상의 스토리지 노드가 오프라인이거나 이 그리드의 스토리지 노드가 최근 15일 내에 재구축된 경우 기술 지원 부서에 문의하십시오. sn-recovery-postinstall.sh 스크립트를 실행하지 마십시오. 2개 이상의 스토리지 노드에서 Cassandra를 상호 간에 15일 이내에 재구축하면 데이터가 손실될 수 있습니다.

이 작업에 대해

이 절차를 완료하려면 다음과 같은 고급 작업을 수행해야 합니다.

- 복구된 스토리지 노드에 로그인합니다.
- 'n-다시 마운트-볼륨' 스크립트를 실행하여 적절하게 포맷된 스토리지 볼륨을 다시 마운트합니다. 이 스크립트가 실행되면 다음 작업을 수행합니다.
  - 각 스토리지 볼륨을 마운트 및 마운트 해제하고 XFS 저널을 재생합니다.

- XFS 파일 일관성 검사를 수행합니다.
- 파일 시스템의 정합성이 보장되면 스토리지 볼륨이 제대로 포맷된 StorageGRID 스토리지 볼륨인지 확인합니다.
- 저장소 볼륨이 제대로 포맷된 경우 저장소 볼륨을 다시 마운트합니다. 볼륨의 기존 데이터는 그대로 유지됩니다.

- 스크립트 출력을 검토하고 문제를 해결합니다.
- 'sn-recovery-postinstall.sh' 스크립트를 실행합니다. 이 스크립트가 실행되면 다음 작업을 수행합니다.

> 복구 중에 스토리지 노드를 재부팅하지 말고, 실패한 스토리지 볼륨을 다시 포맷하고 객체 메타데이터를 복구하기 위해 'sn-recovery-postinstall.sh'(4단계)를 실행하십시오. 'sn-recovery-postinstall.sh'가 완료되기 전에 스토리지 노드를 재부팅하면 서비스를 시작할 때 오류가 발생하여 StorageGRID 어플라이언스 노드가 유지보수 모드를 종료합니다.

  - 'n-remount-volumes' 스크립트가 마운트할 수 없거나 잘못 포맷된 스토리지 볼륨을 다시 포맷합니다.

> 저장소 볼륨이 다시 포맷되면 해당 볼륨의 모든 데이터가 손실됩니다. ILM 규칙이 두 개 이상의 개체 복사본을 저장하도록 구성되었다고 가정하여 그리드의 다른 위치에서 개체 데이터를 복원하려면 추가 절차를 수행해야 합니다.

  - 필요한 경우 노드에서 Cassandra 데이터베이스를 재구축합니다.
  - 스토리지 노드에서 서비스를 시작합니다.

단계

1. 복구된 스토리지 노드에 로그인:
   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 첫 번째 스크립트를 실행하여 적절하게 포맷된 스토리지 볼륨을 다시 마운트합니다.

> 모든 스토리지 볼륨이 새 볼륨이고 포맷해야 하거나 모든 스토리지 볼륨이 실패한 경우 이 단계를 건너뛰고 두 번째 스크립트를 실행하여 마운트 해제된 모든 스토리지 볼륨을 다시 포맷할 수 있습니다.

   a. 'n-다시 마운트-볼륨' 스크립트를 실행합니다

      이 스크립트는 데이터가 포함된 스토리지 볼륨에서 실행되는 데 몇 시간이 걸릴 수 있습니다.

   b. 스크립트가 실행되면 출력을 검토하고 프롬프트에 응답합니다.

> 필요에 따라 'tail-f' 명령을 사용하여 스크립트 로그 파일의 내용을 모니터링할 수 있습니다('/var/local/log/sn-다시 마운트-volumes.log"). 로그 파일에는 명령줄 출력보다 자세한 정보가 들어 있습니다.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
```

```
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

예제 출력에서 한 스토리지 볼륨이 성공적으로 다시 마운트되었으며 세 개의 스토리지 볼륨에 오류가 발생했습니다.

- '/dev/sdb'는 XFS 파일 시스템 일관성 검사를 통과하고 유효한 볼륨 구조를 가지고 있으므로 성공적으로 다시 마운트되었습니다. 스크립트에 의해 다시 마운트된 디바이스의 데이터는 보존됩니다.
- 스토리지 볼륨이 새 볼륨이거나 손상되었기 때문에 '/dev/sdc'가 XFS 파일 시스템 일관성 검사에 실패했습니다.
- 디스크가 초기화되지 않았거나 디스크의 수퍼블록이 손상되어 '/dev/SDD'를 마운트할 수 없습니다. 스크립트가 스토리지 볼륨을 마운트할 수 없는 경우 파일 시스템 정합성 검사를 실행할 것인지 묻는 메시지가 표시됩니다.
  - 스토리지 볼륨이 새 디스크에 연결되어 있는 경우 프롬프트에 * N * 으로 응답합니다. 새 디스크에서 파일 시스템을 확인할 필요가 없습니다.
  - 스토리지 볼륨이 기존 디스크에 연결되어 있는 경우 프롬프트에 * Y * 로 응답합니다. 파일 시스템 검사 결과를 사용하여 손상의 원인을 확인할 수 있습니다. 결과는 '/var/local/log/sn-res마운트-volumes.log' 로그 파일에 저장됩니다.
- '/dev/SDE'는 XFS 파일 시스템 일관성 검사를 통과하고 유효한 볼륨 구조를 가지고 있지만 volid 파일의 LDR 노드 ID가 이 스토리지 노드의 ID(맨 위에 표시된 구성된 LDR noid)와 일치하지 않습니다. 이 메시지는 이 볼륨이 다른 스토리지 노드에 속함을 나타냅니다.

3. 스크립트 출력을 검토하고 문제를 해결합니다.

> 스토리지 볼륨이 XFS 파일 시스템 일관성 검사에 실패했거나 마운트할 수 없는 경우 출력에서 오류 메시지를 자세히 검토합니다. 이러한 볼륨에 대해 'sn-recovery-postinstall.sh' 스크립트를 실행하면 어떤 영향이 있는지 이해해야 합니다.

   a. 결과에 예상한 모든 볼륨에 대한 항목이 포함되어 있는지 확인합니다. 목록에 볼륨이 없으면 스크립트를 다시 실행합니다.

   b. 마운트된 모든 디바이스에 대한 메시지를 검토합니다. 스토리지 볼륨이 이 스토리지 노드에 속해 있지 않음을 나타내는 오류가 없는지 확인합니다.

      이 예제에서 /dev/SDE의 출력에는 다음 오류 메시지가 포함됩니다.

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> 스토리지 볼륨이 다른 스토리지 노드에 속하는 것으로 보고되면 기술 지원 부서에 문의하십시오. 'sn-recovery-postinstall.sh' 스크립트를 실행하면 스토리지 볼륨이 다시 포맷되어 데이터가 손실될 수 있습니다.

   c. 스토리지 디바이스를 마운트할 수 없는 경우 디바이스 이름을 기록해 두고 디바이스를 복구하거나 교체합니다.

> 마운트할 수 없는 스토리지 디바이스를 복구하거나 교체해야 합니다.

      디바이스 이름을 사용하여 볼륨 ID를 조회합니다. 볼륨 ID는 'repair-data' 스크립트를 실행하여 객체 데이터를 볼륨에 복원할 때 입력해야 합니다(다음 절차).

   d. UNMOUNTABLE 장치를 모두 복구하거나 교체한 후 'n-remount-volumes' 스크립트를 다시 실행하여 다시 마운트할 수 있는 모든 스토리지 볼륨이 다시 마운트되었는지 확인합니다.

> 스토리지 볼륨을 마운트할 수 없거나 잘못 포맷한 경우 다음 단계를 계속 수행하면 볼륨의 모든 데이터와 볼륨이 삭제됩니다. 오브젝트 데이터의 복사본이 2개인 경우 다음 절차(오브젝트 데이터 복원)를 완료할 때까지 복사본 하나가 유지됩니다.

> 실패한 스토리지 볼륨에 남아 있는 데이터를 그리드의 다른 위치에서 재구축할 수 없다고 판단되는 경우(예: ILM 정책에서 하나의 복제본만 만드는 규칙을 사용하거나 여러 노드에서 볼륨이 실패한 경우) 'sn-recovery-postinstall.sh' 스크립트를 실행하지 마십시오. 대신 기술 지원 부서에 문의하여 데이터 복구 방법을 확인하십시오.

4. sn-recovery-postinstall.sh 스크립트: sn-recovery-postinstall.sh를 실행합니다

   이 스크립트는 마운트할 수 없거나 잘못 포맷된 스토리지 볼륨을 다시 포맷하고, 필요한 경우 노드에서 Cassandra 데이터베이스를 재구축하고, 스토리지 노드에서 서비스를 시작합니다.

   다음 사항에 유의하십시오.

   - 스크립트를 실행하는 데 몇 시간이 걸릴 수 있습니다.

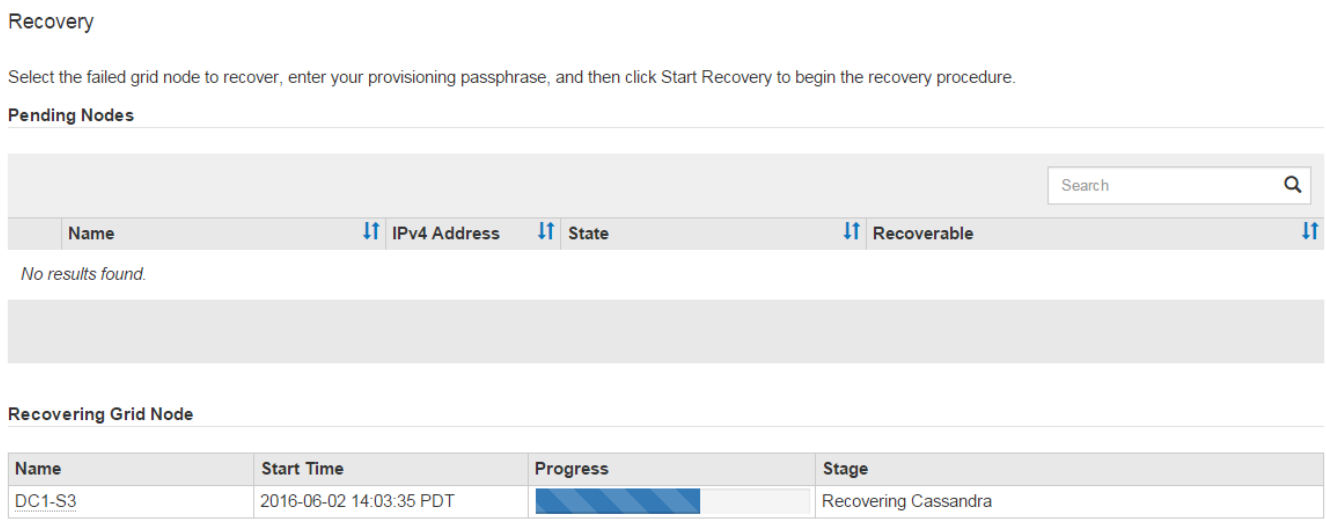
- 일반적으로 스크립트가 실행되는 동안에는 SSH 세션만 남겨야 합니다.
- SSH 세션이 활성화되어 있는 동안에는 * Ctrl + C * 를 누르지 마십시오.
- 네트워크 중단이 발생하여 SSH 세션을 종료하는 경우 스크립트는 백그라운드에서 실행되지만 복구 페이지에서 진행률을 볼 수 있습니다.
- 스토리지 노드가 RSM 서비스를 사용하는 경우 노드 서비스가 다시 시작됨에 따라 스크립트가 5분 동안 정지되는 것처럼 보일 수 있습니다. RSM 서비스가 처음 부팅될 때마다 5분 정도 지연될 수 있습니다.

> RSM 서비스는 ADC 서비스를 포함하는 스토리지 노드에 있습니다.

> 일부 StorageGRID 복구 절차에서는 리퍼를 사용하여 Cassandra 수리를 처리합니다. 관련 또는 필수 서비스가 시작되는 즉시 수리가 자동으로 이루어집니다. "리퍼" 또는 "'Cassandra 수리'라는 스크립트 출력을 볼 수 있습니다. 복구가 실패했다는 오류 메시지가 나타나면 오류 메시지에 표시된 명령을 실행합니다.

5. 'sn-recovery-postinstall.sh' 스크립트가 실행되면 Grid Manager에서 복구 페이지를 모니터링합니다.

   복구 페이지의 진행률 표시줄과 단계 열은 'sn-recovery-postinstall.sh' 스크립트의 상위 상태를 제공합니다.



'sn-recovery-postinstall.sh' 스크립트가 노드에서 서비스를 시작한 후 다음 절차에 설명된 대로 스크립트로 포맷된 모든 스토리지 볼륨에 객체 데이터를 복원할 수 있습니다.

관련 정보

스토리지 노드 시스템 드라이브 복구에 대한 경고를 검토합니다

어플라이언스의 스토리지 볼륨에 오브젝트 데이터를 복원합니다

어플라이언스의 스토리지 볼륨에 오브젝트 데이터를 복원합니다

어플라이언스 스토리지 노드의 스토리지 볼륨을 복구한 후 스토리지 노드에 장애가 발생할 때 손실된 객체 데이터를 복구할 수 있습니다.

필요한 것

- 복구된 스토리지 노드의 접속 상태가 * 연결됨 * 으로 확인되어야 합니다 Grid Manager의 * nodes * > * Overview * (노드 * > * 개요 *) 탭에서 선택합니다.

이 작업에 대해

그리드의 ILM 규칙이 구성되어 있어 오브젝트 복사본을 사용할 수 있다고 가정할 때 다른 스토리지 노드, 아카이브 노드 또는 클라우드 스토리지 풀에서 오브젝트 데이터를 복원할 수 있습니다.

다음 사항에 유의하십시오.

- ILM 규칙이 한 개의 복제된 복사본만 저장하도록 구성되었고 해당 복사본이 실패한 스토리지 볼륨에 존재하면 개체를 복구할 수 없습니다.
- 개체의 나머지 복사본만 클라우드 스토리지 풀에 있는 경우 StorageGRID은 오브젝트 데이터를 복원하기 위해 클라우드 스토리지 풀 엔드포인트에 여러 요청을 실행해야 합니다. 이 절차를 수행하기 전에 기술 지원 부서에 문의하여 복구 시간 프레임 및 관련 비용을 추정하십시오.
- 개체의 나머지 복사본만 아카이브 노드에 있는 경우 아카이브 노드에서 개체 데이터가 검색됩니다. 아카이브 노드에서 스토리지 노드로 오브젝트 데이터를 복원하는 것은 외부 아카이브 스토리지 시스템에서 검색 지연 시간 때문에 다른 스토리지 노드에서 복사본을 복원하는 것보다 시간이 더 오래 걸립니다.

에 대해 `repair-data` 스크립트

객체 데이터를 복원하려면 "repair-data" 스크립트를 실행합니다. 이 스크립트는 개체 데이터 복원 프로세스를 시작하고 ILM 스캔 작업을 통해 ILM 규칙이 충족되는지 확인합니다.

아래에서 * 복제된 데이터 * 또는 * 삭제 코딩(EC) 데이터 * 를 선택하여 복제된 데이터 또는 삭제 코딩 데이터 복원 여부에 따라 리페어 데이터(repair-data) 스크립트에 대한 다양한 옵션을 알아보십시오. 두 유형의 데이터를 모두 복원해야 하는 경우 두 명령 집합을 모두 실행해야 합니다.

> repair-data 스크립트에 대한 자세한 내용은 기본 Admin Node의 명령줄에 repair-data—help를 입력하십시오.

복제된 데이터

전체 노드를 복구해야 하는지 또는 노드의 특정 볼륨만 복구해야 하는지 여부에 따라 두 가지 명령을 사용하여 복제된 데이터를 복원할 수 있습니다.

'repair-data start-replicated-node-repair'를 선택합니다

Repair-data start-replicated-volume-repair를 선택합니다

다음 명령을 사용하여 복제된 데이터의 복구를 추적할 수 있습니다.

REpair-data show-replicated-repair-status'를 참조하십시오

> StorageGRID 11.6의 기술 미리 보기에는 '복제된-수리-상태' 옵션이 제공됩니다. 이 기능은 개발 중이며 반환된 값이 잘못되었거나 지연될 수 있습니다. 수리가 완료되었는지 확인하려면 에 설명된 대로 * Awaiting – All *, * repair attemptated (XRPA) * 및 * Scan Period — Estimated (XSCM) * 를 사용합니다 수리 모니터링.

삭제 코딩**(EC)** 데이터

전체 노드를 복구해야 하는지 또는 노드의 특정 볼륨만 복구해야 하는지 여부에 따라 두 가지 명령을 사용하여 삭제 코딩 데이터를 복원할 수 있습니다.

Repair-data start-ec-node-repair를 선택합니다

Repair-data start-ec-volume-repair를 선택합니다

일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

다음 명령을 사용하여 삭제 코딩 데이터의 복구를 추적할 수 있습니다.

Repair-data show-ec-repair-status'를 참조하십시오

> EC 복구 작업은 일시적으로 많은 양의 저장 공간을 예약합니다. 스토리지 알림이 트리거될 수 있지만 복구가 완료되면 문제가 해결됩니다. 예약 저장 공간이 충분하지 않으면 EC 복구 작업이 실패합니다. 작업 실패 또는 성공 여부에 관계없이 EC 복구 작업이 완료되면 저장소 예약이 해제됩니다.

스토리지 노드의 호스트 이름을 찾습니다

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 복구된 스토리지 볼륨에 대한 스토리지 노드의 호스트 이름을 찾으려면 '/etc/hosts' 파일을 사용합니다. 그리드의 모든 노드 목록을 보려면 cat /etc/hosts를 입력한다.

모든 볼륨이 실패한 경우 데이터를 복구합니다

모든 스토리지 볼륨에 장애가 발생한 경우 전체 노드를 복구합니다. 복제된 데이터 *, * 삭제 코딩(EC) 데이터 * 또는 둘 다에 대한 지침을 따르십시오. 복제된 데이터, 삭제 코딩(EC) 데이터 또는 둘 모두를 사용하는지 여부에 따라 달라집니다.

일부 볼륨만 장애가 발생한 경우 로 이동합니다 일부 볼륨만 장애가 발생한 경우 데이터를 복구합니다.

> 둘 이상의 노드에 대해 동시에 '데이터 다시 페어링' 작업을 실행할 수 없습니다. 여러 노드를 복구하려면 기술 지원 팀에 문의하십시오.

복제된 데이터

그리드에 복제된 데이터가 포함된 경우, '- nodes' 옵션과 함께 'repair-data start-replicated-node-repair' 명령을 사용하여 전체 스토리지 노드를 복구하십시오.

이 명령은 SG-DC-SN3이라는 스토리지 노드에서 복제된 데이터를 복구합니다.

REpair-data start-replicated-node-repair — nodes SG-DC-SN3'으로 표시됩니다

> 개체 데이터가 복원되면 StorageGRID 시스템에서 복제된 개체 데이터를 찾을 수 없을 경우 * 개체 손실 * 경고가 트리거됩니다. 시스템 전체의 스토리지 노드에서 경고가 트리거될 수 있습니다. 손실의 원인과 복구가 가능한지 확인해야 합니다. 을 참조하십시오 모니터링하고 문제를 해결합니다.

삭제 코딩**(EC)** 데이터

그리드에 삭제 코딩 데이터가 포함된 경우, '- nodes' 옵션과 함께 'repair-data start-EC-node-repair' 명령을 사용하여 전체 스토리지 노드를 복구하십시오.

이 명령은 이름이 SG-DC-SN3인 스토리지 노드에서 삭제 코딩 데이터를 복구합니다.

REpair-data start-ec-node-repair—nodes SG-DC-SN3'을 선택합니다

이 작업은 이 REpair_DATA 작업을 식별하는 고유한 REpair ID를 반환합니다. 이 재쌍 ID를 사용하여 REpair_DATA 작업의 진행 상황과 결과를 추적할 수 있습니다. 복구 프로세스가 완료되어도 다른 피드백이 반환되지 않습니다.

> 일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

일부 볼륨만 장애가 발생한 경우 데이터를 복구합니다

일부 볼륨만 장애가 발생한 경우 영향을 받는 볼륨을 복구합니다. 복제된 데이터 *, * 삭제 코딩(EC) 데이터 * 또는 둘 다에 대한 지침을 따르십시오. 복제된 데이터, 삭제 코딩(EC) 데이터 또는 둘 모두를 사용하는지 여부에 따라 달라집니다.

모든 볼륨이 실패한 경우 로 이동합니다 모든 볼륨이 실패한 경우 데이터를 복구합니다.

볼륨 ID를 16진수로 입력합니다. 예를 들어 0000은 첫 번째 볼륨이고 000F는 16번째 볼륨입니다. 하나의 볼륨, 하나의 볼륨 범위 또는 시퀀스에 없는 여러 볼륨을 지정할 수 있습니다.

모든 볼륨은 동일한 스토리지 노드에 있어야 합니다. 둘 이상의 스토리지 노드에 대한 볼륨을 복원해야 하는 경우 기술 지원 부서에 문의하십시오.

복제된 데이터

그리드에 복제된 데이터가 포함된 경우 '--nodes' 옵션과 함께 'start-replicated-volume-repair' 명령을 사용하여 노드를 식별합니다. 그런 다음 다음 아래 예와 같이 '--volumes' 또는 '- volume-range' 옵션을 추가합니다.

- 단일 볼륨 *: 이 명령은 복제된 데이터를 SG-DC-SN3이라는 스토리지 노드의 볼륨 '0002'로 복원합니다.

REpair-data start-replicated-volume-repair—nodes SG-DC-SN3—volum0002"를 참조하십시오

- 볼륨 범위 *: 이 명령은 SG-DC-SN3이라는 스토리지 노드의 "0003" ~ "0009" 범위의 모든 볼륨에 복제된 데이터를 복원합니다.

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

- 다중 볼륨 시퀀스 없음 *: 이 명령은 SG-DC-SN3이라는 스토리지 노드의 볼륨 '0001', '0005' 및 '0008'으로 복제된 데이터를 복원합니다.

REpair-data start-replicated-volume-repair—nodes SG-DC-SN3—volumes 0001,0005,0008'

> 개체 데이터가 복원되면 StorageGRID 시스템에서 복제된 개체 데이터를 찾을 수 없을 경우 * 개체 손실 * 경고가 트리거됩니다. 시스템 전체의 스토리지 노드에서 경고가 트리거될 수 있습니다. 손실의 원인과 복구가 가능한지 확인해야 합니다. StorageGRID 모니터링 및 문제 해결에 대한 지침을 참조하십시오.

삭제 코딩**(EC)** 데이터

그리드에 삭제 코딩 데이터가 포함된 경우 '- nodes' 옵션과 함께 'start-ec-volume-repair' 명령을 사용하여 노드를 식별하십시오. 그런 다음 다음 아래 예와 같이 '--volumes' 또는 '- volume-range' 옵션을 추가합니다.

- 단일 볼륨 *: 이 명령은 SG-DC-SN3이라는 스토리지 노드의 볼륨 '0007'에 삭제 코딩 데이터를 복원합니다.

REpair-data start-ec-volume-repair—nodes SG-DC-SN3—volumes 0007'을 참조하십시오

- 볼륨 범위 *: 이 명령은 삭제 코딩 데이터를 SG-DC-SN3이라는 스토리지 노드의 "0004" ~ "0006" 범위에 있는 모든 볼륨에 복원합니다.

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

- Multiple volumes not in a sequence *: 이 명령은 SG-DC-SN3이라는 스토리지 노드의 볼륨 '000A', '000C' 및 '000E'로 삭제 코딩 데이터를 복원합니다.

REpair-data start-EC-volume-repair—nodes SG-DC-SN3—volumes 000A, 000C, 000E

repair-data는 이 repair_data 작업을 식별하는 고유한 repair ID를 반환합니다. 이 재쌍 ID를 사용하여 REpair_DATA 작업의 진행 상황과 결과를 추적할 수 있습니다. 복구 프로세스가 완료되어도 다른 피드백이 반환되지 않습니다.

> 일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

수리 모니터링

복제된 데이터 *, * 삭제 코딩(EC) 데이터 * 또는 둘 모두를 사용하는지 여부에 따라 복구 작업의 상태를 모니터링합니다.

복제된 데이터

- 수리가 완료되었는지 확인하려면:
  a. 노드 * > * _ 복구되는 스토리지 노드 _ * > * ILM * 을 선택합니다.
  b. 평가 섹션의 속성을 검토합니다. 복구가 완료되면 * Awaiting-all * 속성이 0 개체를 나타냅니다.
- 수리를 더 자세히 모니터링하려면:
  a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
  b. 복구되는 **GRID* * > *_Storage Node _ * > * LDR * > * Data Store * 를 선택합니다.
  c. 복제된 수리가 완료된 경우 다음 특성을 조합하여 가능한 한 결정합니다.

    Cassandra의 일관성이 없을 수 있으며, 복구 실패를 추적하지 않습니다.

    - * 시도된 복구(XRPA) **:** 이 속성을 사용하여 복제된 복구 진행률을 추적합니다**.** 이 속성은 스토리지 노드가 고위험 객체를 복구하려고 할 때마다 증가합니다**.** 이 속성이 현재 스캔 기간**(** Scan Period — Estimated* 속성 제공)보다 더 긴 기간 동안 증가하지 않으면 ILM 스캐닝에서 모든 노드에서 복구해야 할 고위험 개체를 찾지 못한 것입니다.

      고위험 개체는 완전히 손실될 위험이 있는 개체입니다. ILM 구성을 충족하지 않는 개체는 포함되지 않습니다.

    - * 스캔 기간 — 예상(XSCM) *: 이 속성을 사용하여 이전에 수집된 개체에 정책 변경이 적용되는 시점을 추정합니다. 복구 시도 * 속성이 현재 스캔 기간보다 긴 기간 동안 증가하지 않으면 복제된 수리가 수행될 수 있습니다. 스캔 기간은 변경될 수 있습니다. 스캔 기간 — 예상(XSCM) * 속성은 전체 그리드에 적용되며 모든 노드 스캔 기간의 최대값입니다. 그리드에 대한 * Scan Period — Estimated * 속성 기록을 조회하여 적절한 기간을 결정할 수 있습니다.
- 필요에 따라 복제된 복구에 대한 예상 완료율을 얻으려면 repair-data 명령에 'show-replicated-repair-status' 옵션을 추가합니다.

  REpair-data show-replicated-repair-status'를 참조하십시오

  StorageGRID 11.6의 기술 미리 보기에는 '복제된-수리-상태' 옵션이 제공됩니다. 이 기능은 개발 중이며 반환된 값이 잘못되었거나 지연될 수 있습니다. 수리가 완료되었는지 확인하려면 에 설명된 대로 * Awaiting – All *, * repair attemptated (XRPA) * 및 * Scan Period — Estimated (XSCM) * 를 사용합니다 수리 모니터링.

삭제 코딩**(EC)** 데이터

삭제 코딩 데이터의 복구를 모니터링하고 실패한 요청을 다시 시도하려면 다음을 수행하십시오.

1. 삭제 코딩 데이터 복구 상태를 확인합니다.
   - 현재 작업의 예상 완료 시간과 완료 비율을 보려면 * 지원 * > * 도구 * > * 메트릭 * 을 선택합니다. 그런 다음 Grafana 섹션에서 * EC 개요 * 를 선택합니다. Grid EC Job Ec Job Estimated Time to Completion * 및 * Grid EC Job Percentage Completed * 대시보드를 확인합니다.
   - 특정 repair-data 작업의 상태를 확인하려면 다음 명령을 사용합니다.

     REpair-data show -ec-repair-status—repair-id repair ID'를 참조하십시오

- 이 명령을 사용하여 모든 수리를 나열합니다.

  Repair-data show-ec-repair-status'를 참조하십시오

이 출력에는 현재 실행 중인 모든 수리에 대한 "재쌍 ID"를 포함한 정보가 나열됩니다.

2. 출력에 복구 작업이 실패한 것으로 표시되면 '--repair-id' 옵션을 사용하여 복구를 다시 시도합니다.

   이 명령은 복구 ID 6949309319275667690을 사용하여 장애가 발생한 노드 복구를 재시도합니다.

   REpair-data start-ec-node-repair—repair-id 6949309319275667690

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 볼륨 복구를 재시도합니다.

   REpair-data start-ec-volume-repair—repair-id 6949309319275667690

어플라이언스 스토리지 노드를 복구한 후 스토리지 상태를 확인합니다

어플라이언스 스토리지 노드를 복구한 후에는 어플라이언스 스토리지 노드의 원하는 상태가 온라인으로 설정되어 있는지 확인하고 스토리지 노드 서버를 다시 시작할 때마다 기본적으로 온라인 상태가 되도록 해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 스토리지 노드가 복구되고 데이터 복구가 완료되었습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. 복구된 스토리지 노드 * > * LDR * > * 스토리지 * > * 스토리지 상태 — 원하는 * 및 * 스토리지 상태 — 현재 * 값을 확인합니다.

   두 속성의 값은 온라인이어야 합니다.

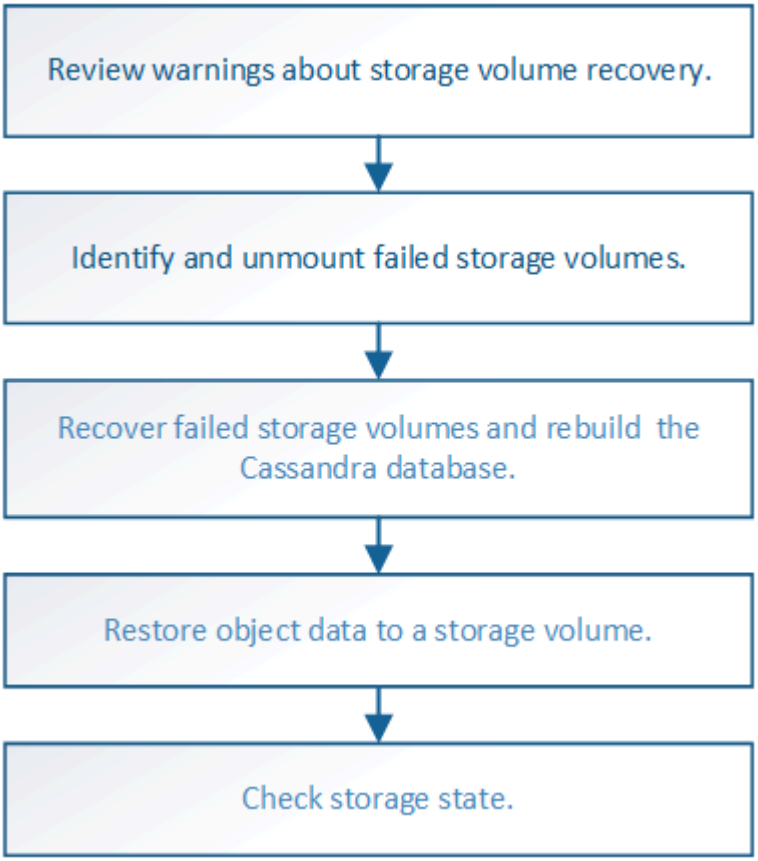
3. 원하는 스토리지 상태가 읽기 전용으로 설정되어 있으면 다음 단계를 수행하십시오.
   a. Configuration * 탭을 클릭합니다.
   b. Storage State — Desired * 드롭다운 목록에서 * Online * 을 선택합니다.
   c. 변경 내용 적용 * 을 클릭합니다.
   d. Overview * 탭을 클릭하고 * Storage State — Desired * 및 * Storage State — Current * 의 값이 Online으로 업데이트되었는지 확인합니다.

시스템 드라이브가 손상되지 않은 스토리지 볼륨 장애로부터 복구합니다

스토리지 노드의 하나 이상의 스토리지 볼륨이 실패했지만 시스템 드라이브가 손상되지 않은 소프트웨어 기반 스토리지 노드를 복구하려면 일련의 작업을 완료해야 합니다. 스토리지 볼륨만 장애가 발생한 경우에도 StorageGRID 시스템에서 스토리지 노드를 계속 사용할 수 있습니다.

이 작업에 대해

이 복구 절차는 소프트웨어 기반 스토리지 노드에만 적용됩니다. 어플라이언스 스토리지 노드에서 스토리지 볼륨이 실패한 경우 ""어플라이언스 스토리지 노드 복구" 절차를 사용하십시오.



관련 정보

어플라이언스 스토리지 노드를 복구합니다

스토리지 볼륨 복구에 대한 경고를 검토합니다

스토리지 노드에 대해 장애가 발생한 스토리지 볼륨을 복구하기 전에 다음 경고를 검토해야 합니다.

스토리지 노드의 스토리지 볼륨(또는 범위)은 볼륨 ID라고 하는 16진수 번호로 식별됩니다. 예를 들어 0000은 첫 번째 볼륨이고 000F는 16번째 볼륨입니다. 각 스토리지 노드의 첫 번째 오브젝트 저장소(볼륨 0)는 오브젝트 메타데이터 및 Cassandra 데이터베이스 작업에 최대 4TB의 공간을 사용하며, 해당 볼륨의 나머지 공간은 오브젝트 데이터에 사용됩니다. 다른 모든 스토리지 볼륨은 오브젝트 데이터에만 사용됩니다.

볼륨 0에 장애가 발생하여 복구해야 하는 경우, Cassandra 데이터베이스가 볼륨 복구 절차의 일부로 재구축될 수 있습니다. Cassandra는 다음과 같은 경우에도 재구축됩니다.

- 스토리지 노드는 15일 이상 오프라인 상태가 된 후 다시 온라인 상태로 전환됩니다.
- 시스템 드라이브 및 하나 이상의 스토리지 볼륨이 실패하고 복구됩니다.

Cassandra가 재구성되면 시스템은 다른 스토리지 노드의 정보를 사용합니다. 너무 많은 스토리지 노드가 오프라인인 경우 일부 Cassandra 데이터를 사용하지 못할 수 있습니다. Cassandra가 최근에 다시 빌드된 경우, Cassandra 데이터가 그리드 전체에서 아직 일관되지 않을 수 있습니다. Cassandra가 너무 많은 스토리지 노드가 오프라인이거나

둘 이상의 스토리지 노드가 서로 15일 이내에 재구축된 경우 데이터 손실이 발생할 수 있습니다.

> 둘 이상의 스토리지 노드에 장애가 있거나 오프라인 상태인 경우 기술 지원 부서에 문의하십시오. 다음 복구 절차를 수행하지 마십시오. 데이터가 손실될 수 있습니다.

> 스토리지 노드 장애 또는 복구 후 15일 이내에 두 번째 스토리지 노드 오류인 경우 기술 지원 부서에 문의하십시오. 15일 이내에 두 개 이상의 스토리지 노드에서 Cassandra를 재구축하면 데이터가 손실될 수 있습니다.

> 한 사이트에 둘 이상의 스토리지 노드에 장애가 발생한 경우 사이트 복구 절차가 필요할 수 있습니다. 기술 지원 부서에 문의하십시오.

기술 지원 부서에서 사이트 복구를 수행하는 방법

> ILM 규칙이 복제된 복사본을 하나만 저장하도록 구성되어 있고 해당 복사본이 실패한 스토리지 볼륨에 있으면 개체를 복구할 수 없습니다.

> 복구 중 서비스:상태-Cassandra(SVST) 경보가 발생하는 경우, Cassandra를 재작성하여 모니터링 및 문제 해결 지침을 참조하여 알람에서 복구합니다. Cassandra가 재구축된 후에는 경보가 지워집니다. 알람이 소거되지 않으면 기술 지원 부서에 문의하십시오.

관련 정보

모니터링하고 문제를 해결합니다

그리드 노드 복구에 대한 경고 및 고려 사항

장애가 발생한 스토리지 볼륨을 식별하고 마운트 해제합니다

장애가 발생한 스토리지 볼륨으로 스토리지 노드를 복구할 때는 장애가 발생한 볼륨을 식별하고 마운트 해제해야 합니다. 복구 절차의 일부로 장애가 발생한 스토리지 볼륨만 다시 포맷되었는지 확인해야 합니다.

필요한 것

를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

이 작업에 대해

장애가 발생한 스토리지 볼륨은 가능한 한 빨리 복구해야 합니다.

복구 프로세스의 첫 번째 단계는 분리되었거나, 마운트 해제되어야 하거나, I/O 오류가 있는 볼륨을 검색하는 것입니다. 오류가 발생한 볼륨이 여전히 연결되어 있지만 임의로 손상된 파일 시스템이 있는 경우 시스템에서 디스크의 사용되지 않거나 할당되지 않은 부분에 있는 손상을 감지하지 못할 수 있습니다.

> 디스크 추가 또는 다시 연결, 노드 중지, 노드 시작 또는 재부팅과 같은 수동 단계를 수행하여 볼륨을 복구하려면 이 절차를 완료해야 합니다. 그렇지 않으면 reformat_storage_block_devices.rb' 스크립트를 실행할 때 스크립트가 중단되거나 실패하는 파일 시스템 오류가 발생할 수 있습니다.

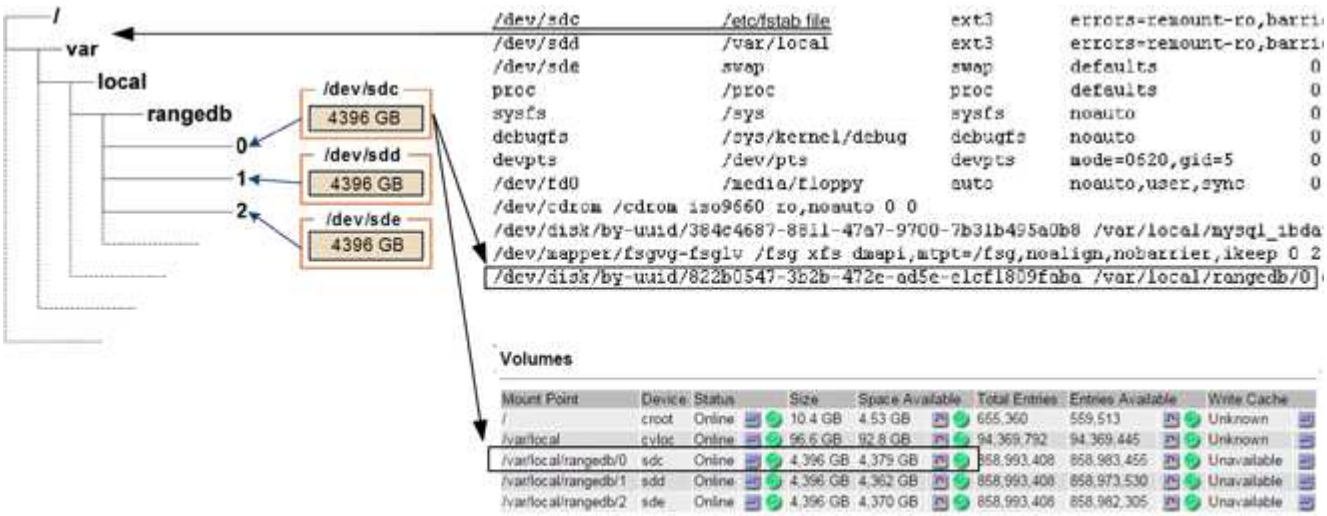
> Reboot 명령을 실행하기 전에 하드웨어를 복구하고 디스크를 올바르게 연결합니다.

> 장애가 발생한 스토리지 볼륨을 신중하게 식별합니다. 이 정보를 사용하여 재포맷해야 하는 볼륨을 확인할 수 있습니다. 볼륨이 다시 포맷되면 볼륨의 데이터를 복구할 수 없습니다.

장애가 발생한 스토리지 볼륨을 올바르게 복구하려면 실패한 스토리지 볼륨의 디바이스 이름과 해당 볼륨 ID를 모두 알아야 합니다.

설치 시 각 스토리지 디바이스에 파일 시스템 UUID(Universal Unique Identifier)가 할당되고 할당된 파일 시스템 UUID를 사용하여 스토리지 노드의 rangedb 디렉토리에 마운트됩니다. 파일 시스템 UUID와 rangedb 디렉토리는 '/etc/fstab' 파일에 나열되어 있습니다. 디바이스 이름, rangedb 디렉토리 및 마운트된 볼륨의 크기가 Grid Manager에 표시됩니다.

다음 예에서는 /dev/disk/by-uuuuid/822b0547-3b2b-472e-ad5e-ad5e-e1cf1809faba 등의 디바이스 이름을 사용하여 디바이스 '/var/local/rangedb/0'에 볼륨 크기가 4TB인 디바이스 '/var/local/rangedb/0'에 마운트됩니다.



단계

1. 다음 단계를 수행하여 장애가 발생한 스토리지 볼륨 및 해당 디바이스 이름을 기록합니다.

   a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.

   b. site * > * failed Storage Node * > * LDR * > * Storage * > * Overview * > * Main * 을 선택하고 알람이 있는 객체 저장소를 찾습니다.

   Object Stores

ID	Total	Available	Stored Data	Stored (%)	Health
0000	96.6 GB	96.6 GB	823 KB	0.001 %	Error
0001	107 GB	107 GB	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 %	No Errors

   c. site * > * failed Storage Node * > * SSM * > * Resources * > * Overview * > * Main * 을 선택합니다. 이전 단계에서 확인한 실패한 각 스토리지 볼륨의 마운트 지점 및 볼륨 크기를 확인합니다.

      오브젝트 저장소는 16진수로 번호가 매겨집니다. 예를 들어 0000은 첫 번째 볼륨이고 000F는 16번째 볼륨입니다. 이 예에서 ID가 0000인 오브젝트 저장소는 디바이스 이름이 sdc이고 크기가 107GB인 '/var/local/rangedb/0'에 해당합니다.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	croot	Online	10.4 GB	4.17 GB	655,360	554,806	Unknown
/var/local	cvloc	Online	96.6 GB	96.1 GB	94,369,792	94,369,423	Unknown
/var/local/rangedb/0	sdc	Online	107 GB	107 GB	104,857,600	104,856,202	Enabled
/var/local/rangedb/1	sdd	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled
/var/local/rangedb/2	sde	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled

2. 장애가 발생한 스토리지 노드에 로그인:

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

3. 다음 스크립트를 실행하여 스토리지 서비스를 중지하고 실패한 스토리지 볼륨을 마운트 해제합니다.

   'sn-unmount-volume object_store_ID'입니다

   object_store_ID는 실패한 스토리지 볼륨의 ID이다. 예를 들어, ID가 0000인 오브젝트 저장소의 명령에 "0"을 지정합니다.

4. 메시지가 표시되면 * y * 를 눌러 스토리지 노드의 스토리지 서비스를 중지합니다.

   > 스토리지 서비스가 이미 중지된 경우에는 메시지가 표시되지 않습니다. Cassandra 서비스는 볼륨 0에만 중지됩니다.

```
root@Storage-180:~ # sn-unmount-volume 0
Storage services (ldr, chunk, dds, cassandra) are not down.
Storage services must be stopped before running this script.
Stop storage services [y/N]? y
Shutting down storage services.
Storage services stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

   몇 초 후 스토리지 서비스가 중지되고 볼륨이 마운트 해제됩니다. 프로세스의 각 단계를 나타내는 메시지가 나타납니다. 마지막 메시지는 볼륨이 마운트 해제되었음을 나타냅니다.

장애가 발생한 스토리지 볼륨을 복구하고 **Cassandra** 데이터베이스를 재구축합니다

장애가 발생한 스토리지 볼륨에서 스토리지를 다시 포맷하고 다시 마운트하는 스크립트를 실행하고, 시스템에서 필요하다고 판단할 경우 스토리지 노드에서 Cassandra 데이터베이스를

재구성해야 합니다.

- "passwords.txt" 파일이 있어야 합니다.
- 서버의 시스템 드라이브가 손상되지 않아야 합니다.
- 실패의 원인을 식별해야 하며, 필요한 경우 교체 스토리지 하드웨어를 이미 구입한 상태여야 합니다.
- 교체 스토리지의 총 크기는 원본과 같아야 합니다.
- 스토리지 노드 사용 중지가 진행 중이 아니거나 노드 사용 중단 절차를 일시 중지했습니다. (Grid Manager에서 * 유지보수 * > * 작업 * > * 서비스 해제 * 를 선택합니다.)
- 확장이 진행 중이 아닌 것을 확인했습니다. (Grid Manager에서 * 유지보수 * > * 작업 * > * 확장 * 을 선택합니다.)
- 있습니다 스토리지 볼륨 복구에 대한 경고를 검토했습니다.

a. 필요에 따라 이전에 확인 및 마운트 해제한 실패한 스토리지 볼륨과 연결된 장애가 발생한 물리적 또는 가상 스토리지를 교체하십시오.

   스토리지를 교체한 후 운영 체제에서 인식되지만 볼륨을 다시 마운트하지 않도록 다시 스캔하거나 재부팅해야 합니다. 이후 단계에서 스토리지가 다시 마운트되고 '/etc/fstab'에 추가됩니다.

b. 장애가 발생한 스토리지 노드에 로그인:

   i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

   ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   iii. 루트로 전환하려면 다음 명령을 입력합니다

   iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

c. 텍스트 편집기(vi 또는 vim)를 사용하여 '/etc/fstab' 파일에서 실패한 볼륨을 삭제한 다음 파일을 저장합니다.

   > '/etc/fstab' 파일에서 실패한 볼륨을 주석으로 처리하지 않습니다. 복구 프로세스에서는 fstab 파일의 모든 행이 마운트된 파일 시스템과 일치하는지 확인하므로 fstab에서 볼륨을 삭제해야 합니다.

d. 장애가 발생한 스토리지 볼륨을 다시 포맷하고 필요한 경우 Cassandra 데이터베이스를 재구축합니다. rformat_storage_block_devices.rb를 입력합니다

   - 스토리지 서비스가 실행 중인 경우 서비스를 중지하라는 메시지가 표시됩니다. 입력: * y *
   - 필요한 경우 Cassandra 데이터베이스를 재구축하라는 메시지가 표시됩니다.
     - 경고를 검토합니다. 적용되는 데이터베이스가 없는 경우 Cassandra 데이터베이스를 재구축합니다. 입력: * y *
     - 둘 이상의 스토리지 노드가 오프라인이거나 지난 15일 동안 다른 스토리지 노드가 재구축된 경우 입력: * n *

       스크립트는 Cassandra를 다시 빌드하지 않고 종료됩니다. 기술 지원 부서에 문의하십시오.
   - 스토리지 노드의 각 rangedb 드라이브에 대해 "Reformat the rangedb drive_<name>_(device_<major number>:<minor number>_)? [y/n]?", 다음 응답 중 하나를 입력합니다.

- 오류가 있는 드라이브를 다시 포맷하려면 * y * 를 누릅니다. 이렇게 하면 스토리지 볼륨이 다시 포맷되고 다시 포맷된 스토리지 볼륨이 '/etc/fstab' 파일에 추가됩니다.
- * n * 드라이브에 오류가 없고 다시 포맷하지 않으려는 경우.

> n * 을 선택하면 스크립트가 종료됩니다. 드라이브를 마운트하거나(드라이브의 데이터가 보존되어야 하고 드라이브가 잘못 마운트 해제된 경우) 드라이브를 제거하십시오. 그런 다음 reformat_storage_block_devices.rb' 명령을 다시 실행합니다.

> 일부 StorageGRID 복구 절차에서는 리퍼를 사용하여 Cassandra 수리를 처리합니다. 관련 또는 필수 서비스가 시작되는 즉시 수리가 자동으로 이루어집니다. "리퍼" 또는 "'Cassandra 수리'라는 스크립트 출력을 볼 수 있습니다. 복구가 실패했다는 오류 메시지가 나타나면 오류 메시지에 표시된 명령을 실행합니다.

다음 예제 출력에서 드라이브 '/dev/sdf'를 다시 포맷해야 하며 Cassandra는 재구축할 필요가 없습니다.

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Storage services must be stopped before running this script.
Stop storage services [y/N]? **y**
Shutting down storage services.
Storage services stopped.
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? **y**
Successfully formatted /dev/sdf with UUID c817f87f-f989-4a21-8f03-
b6f42180063f
Skipping in use device /dev/sdg
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12075630
Cassandra does not need rebuilding.
Starting services.

Reformatting done.  Now do manual steps to
restore copies of data.
```

시스템 드라이브가 손상되지 않은 스토리지 볼륨에 개체 데이터를 복원합니다

시스템 드라이브가 손상되지 않은 스토리지 노드에서 스토리지 볼륨을 복구한 후에는 스토리지 볼륨 장애 시 손실된 개체 데이터를 복구할 수 있습니다.

필요한 것

- 복구된 스토리지 노드의 접속 상태가 * 연결됨 * 으로 확인되어야 합니다 Grid Manager의 * nodes * > * Overview * (노드 * > * 개요 *) 탭에서 선택합니다.

이 작업에 대해

그리드의 ILM 규칙이 구성되어 있어 오브젝트 복사본을 사용할 수 있다고 가정할 때 다른 스토리지 노드, 아카이브 노드 또는 클라우드 스토리지 풀에서 오브젝트 데이터를 복원할 수 있습니다.

다음 사항에 유의하십시오.

- ILM 규칙이 한 개의 복제된 복사본만 저장하도록 구성되었고 해당 복사본이 실패한 스토리지 볼륨에 존재하면 개체를 복구할 수 없습니다.
- 개체의 나머지 복사본만 클라우드 스토리지 풀에 있는 경우 StorageGRID은 오브젝트 데이터를 복원하기 위해 클라우드 스토리지 풀 엔드포인트에 여러 요청을 실행해야 합니다. 이 절차를 수행하기 전에 기술 지원 부서에 문의하여 복구 시간 프레임 및 관련 비용을 추정하십시오.
- 개체의 나머지 복사본만 아카이브 노드에 있는 경우 아카이브 노드에서 개체 데이터가 검색됩니다. 아카이브 노드에서 스토리지 노드로 오브젝트 데이터를 복원하는 것은 외부 아카이브 스토리지 시스템에서 검색 지연 시간 때문에 다른 스토리지 노드에서 복사본을 복원하는 것보다 시간이 더 오래 걸립니다.

에 대해 `repair-data` 스크립트

객체 데이터를 복원하려면 "repair-data" 스크립트를 실행합니다. 이 스크립트는 개체 데이터 복원 프로세스를 시작하고 ILM 스캔 작업을 통해 ILM 규칙이 충족되는지 확인합니다.

아래에서 * 복제된 데이터 * 또는 * 삭제 코딩(EC) 데이터 * 를 선택하여 복제된 데이터 또는 삭제 코딩 데이터 복원 여부에 따라 리페어 데이터(repair-data) 스크립트에 대한 다양한 옵션을 알아보십시오. 두 유형의 데이터를 모두 복원해야 하는 경우 두 명령 집합을 모두 실행해야 합니다.

repair-data 스크립트에 대한 자세한 내용은 기본 Admin Node의 명령줄에 repair-data—help를 입력하십시오.

복제된 데이터

전체 노드를 복구해야 하는지 또는 노드의 특정 볼륨만 복구해야 하는지 여부에 따라 두 가지 명령을 사용하여 복제된 데이터를 복원할 수 있습니다.

'repair-data start-replicated-node-repair'를 선택합니다

Repair-data start-replicated-volume-repair를 선택합니다

다음 명령을 사용하여 복제된 데이터의 복구를 추적할 수 있습니다.

REpair-data show-replicated-repair-status'를 참조하십시오

> StorageGRID 11.6의 기술 미리 보기에는 '복제된-수리-상태' 옵션이 제공됩니다. 이 기능은 개발 중이며 반환된 값이 잘못되었거나 지연될 수 있습니다. 수리가 완료되었는지 확인하려면 에 설명된 대로 * Awaiting – All *, * repair attemptated (XRPA) * 및 * Scan Period — Estimated (XSCM) * 를 사용합니다 수리 모니터링.

삭제 코딩**(EC)** 데이터

전체 노드를 복구해야 하는지 또는 노드의 특정 볼륨만 복구해야 하는지 여부에 따라 두 가지 명령을 사용하여 삭제 코딩 데이터를 복원할 수 있습니다.

Repair-data start-ec-node-repair를 선택합니다

Repair-data start-ec-volume-repair를 선택합니다

일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

다음 명령을 사용하여 삭제 코딩 데이터의 복구를 추적할 수 있습니다.

Repair-data show-ec-repair-status'를 참조하십시오

> EC 복구 작업은 일시적으로 많은 양의 저장 공간을 예약합니다. 스토리지 알림이 트리거될 수 있지만 복구가 완료되면 문제가 해결됩니다. 예약 저장 공간이 충분하지 않으면 EC 복구 작업이 실패합니다. 작업 실패 또는 성공 여부에 관계없이 EC 복구 작업이 완료되면 저장소 예약이 해제됩니다.

스토리지 노드의 호스트 이름을 찾습니다

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 복구된 스토리지 볼륨에 대한 스토리지 노드의 호스트 이름을 찾으려면 '/etc/hosts' 파일을 사용합니다. 그리드의 모든 노드 목록을 보려면 cat /etc/hosts를 입력한다.

모든 볼륨이 실패한 경우 데이터를 복구합니다

모든 스토리지 볼륨에 장애가 발생한 경우 전체 노드를 복구합니다. 복제된 데이터 *, * 삭제 코딩(EC) 데이터 * 또는 둘 다에 대한 지침을 따르십시오. 복제된 데이터, 삭제 코딩(EC) 데이터 또는 둘 모두를 사용하는지 여부에 따라 달라집니다.

일부 볼륨만 장애가 발생한 경우 로 이동합니다 일부 볼륨만 장애가 발생한 경우 데이터를 복구합니다.

> 둘 이상의 노드에 대해 동시에 '데이터 다시 페어링' 작업을 실행할 수 없습니다. 여러 노드를 복구하려면 기술 지원 팀에 문의하십시오.

복제된 데이터

그리드에 복제된 데이터가 포함된 경우, '- nodes' 옵션과 함께 'repair-data start-replicated-node-repair' 명령을 사용하여 전체 스토리지 노드를 복구하십시오.

이 명령은 SG-DC-SN3이라는 스토리지 노드에서 복제된 데이터를 복구합니다.

REpair-data start-replicated-node-repair — nodes SG-DC-SN3'으로 표시됩니다

> 개체 데이터가 복원되면 StorageGRID 시스템에서 복제된 개체 데이터를 찾을 수 없을 경우 * 개체 손실 * 경고가 트리거됩니다. 시스템 전체의 스토리지 노드에서 경고가 트리거될 수 있습니다. 손실의 원인과 복구가 가능한지 확인해야 합니다. 을 참조하십시오 모니터링하고 문제를 해결합니다.

삭제 코딩**(EC)** 데이터

그리드에 삭제 코딩 데이터가 포함된 경우, '- nodes' 옵션과 함께 'repair-data start-EC-node-repair' 명령을 사용하여 전체 스토리지 노드를 복구하십시오.

이 명령은 이름이 SG-DC-SN3인 스토리지 노드에서 삭제 코딩 데이터를 복구합니다.

REpair-data start-ec-node-repair—nodes SG-DC-SN3'을 선택합니다

이 작업은 이 REpair_DATA 작업을 식별하는 고유한 REpair ID를 반환합니다. 이 재쌍 ID를 사용하여 REpair_DATA 작업의 진행 상황과 결과를 추적할 수 있습니다. 복구 프로세스가 완료되어도 다른 피드백이 반환되지 않습니다.

> 일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

일부 볼륨만 장애가 발생한 경우 데이터를 복구합니다

일부 볼륨만 장애가 발생한 경우 영향을 받는 볼륨을 복구합니다. 복제된 데이터 *, * 삭제 코딩(EC) 데이터 * 또는 둘 다에 대한 지침을 따르십시오. 복제된 데이터, 삭제 코딩(EC) 데이터 또는 둘 모두를 사용하는지 여부에 따라 달라집니다.

모든 볼륨이 실패한 경우 로 이동합니다 모든 볼륨이 실패한 경우 데이터를 복구합니다.

볼륨 ID를 16진수로 입력합니다. 예를 들어 0000은 첫 번째 볼륨이고 000F는 16번째 볼륨입니다. 하나의 볼륨, 하나의 볼륨 범위 또는 시퀀스에 없는 여러 볼륨을 지정할 수 있습니다.

모든 볼륨은 동일한 스토리지 노드에 있어야 합니다. 둘 이상의 스토리지 노드에 대한 볼륨을 복원해야 하는 경우 기술 지원 부서에 문의하십시오.

복제된 데이터

그리드에 복제된 데이터가 포함된 경우 '--nodes' 옵션과 함께 'start-replicated-volume-repair' 명령을 사용하여 노드를 식별합니다. 그런 다음 다음 아래 예와 같이 '--volumes' 또는 '- volume-range' 옵션을 추가합니다.

- 단일 볼륨 *: 이 명령은 복제된 데이터를 SG-DC-SN3이라는 스토리지 노드의 볼륨 '0002'로 복원합니다.

REpair-data start-replicated-volume-repair—nodes SG-DC-SN3—volum0002"를 참조하십시오

- 볼륨 범위 *: 이 명령은 SG-DC-SN3이라는 스토리지 노드의 "0003" ~ "0009" 범위의 모든 볼륨에 복제된 데이터를 복원합니다.

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

- 다중 볼륨 시퀀스 없음 *: 이 명령은 SG-DC-SN3이라는 스토리지 노드의 볼륨 '0001', '0005' 및 '0008'으로 복제된 데이터를 복원합니다.

REpair-data start-replicated-volume-repair—nodes SG-DC-SN3—volumes 0001,0005,0008'

> 개체 데이터가 복원되면 StorageGRID 시스템에서 복제된 개체 데이터를 찾을 수 없을 경우 * 개체 손실 * 경고가 트리거됩니다. 시스템 전체의 스토리지 노드에서 경고가 트리거될 수 있습니다. 손실의 원인과 복구가 가능한지 확인해야 합니다. StorageGRID 모니터링 및 문제 해결에 대한 지침을 참조하십시오.

삭제 코딩**(EC)** 데이터

그리드에 삭제 코딩 데이터가 포함된 경우 '- nodes' 옵션과 함께 'start-ec-volume-repair' 명령을 사용하여 노드를 식별하십시오. 그런 다음 다음 아래 예와 같이 '--volumes' 또는 '- volume-range' 옵션을 추가합니다.

- 단일 볼륨 *: 이 명령은 SG-DC-SN3이라는 스토리지 노드의 볼륨 '0007'에 삭제 코딩 데이터를 복원합니다.

REpair-data start-ec-volume-repair—nodes SG-DC-SN3—volumes 0007'을 참조하십시오

- 볼륨 범위 *: 이 명령은 삭제 코딩 데이터를 SG-DC-SN3이라는 스토리지 노드의 "0004" ~ "0006" 범위에 있는 모든 볼륨에 복원합니다.

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

- Multiple volumes not in a sequence *: 이 명령은 SG-DC-SN3이라는 스토리지 노드의 볼륨 '000A', '000C' 및 '000E'로 삭제 코딩 데이터를 복원합니다.

REpair-data start-EC-volume-repair—nodes SG-DC-SN3—volumes 000A, 000C, 000E

repair-data는 이 repair_data 작업을 식별하는 고유한 repair ID를 반환합니다. 이 재쌍 ID를 사용하여 REpair_DATA 작업의 진행 상황과 결과를 추적할 수 있습니다. 복구 프로세스가 완료되어도 다른 피드백이 반환되지 않습니다.

> 일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

수리 모니터링

복제된 데이터 *, * 삭제 코딩(EC) 데이터 * 또는 둘 모두를 사용하는지 여부에 따라 복구 작업의 상태를 모니터링합니다.

복제된 데이터

- 수리가 완료되었는지 확인하려면:
  a. 노드 * > * _ 복구되는 스토리지 노드 _ * > * ILM * 을 선택합니다.
  b. 평가 섹션의 속성을 검토합니다. 복구가 완료되면 * Awaiting-all * 속성이 0 개체를 나타냅니다.
- 수리를 더 자세히 모니터링하려면:
  a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
  b. 복구되는 **GRID* * > *_Storage Node _ * > * LDR * > * Data Store * 를 선택합니다.
  c. 복제된 수리가 완료된 경우 다음 특성을 조합하여 가능한 한 결정합니다.

    Cassandra의 일관성이 없을 수 있으며, 복구 실패를 추적하지 않습니다.

    - * 시도된 복구(XRPA) **:** 이 속성을 사용하여 복제된 복구 진행률을 추적합니다**.** 이 속성은 스토리지 노드가 고위험 객체를 복구하려고 할 때마다 증가합니다**.** 이 속성이 현재 스캔 기간**(** Scan Period — Estimated* 속성 제공)보다 더 긴 기간 동안 증가하지 않으면 ILM 스캐닝에서 모든 노드에서 복구해야 할 고위험 개체를 찾지 못한 것입니다.

      고위험 개체는 완전히 손실될 위험이 있는 개체입니다. ILM 구성을 충족하지 않는 개체는 포함되지 않습니다.

    - * 스캔 기간 — 예상(XSCM) *: 이 속성을 사용하여 이전에 수집된 개체에 정책 변경이 적용되는 시점을 추정합니다. 복구 시도 * 속성이 현재 스캔 기간보다 긴 기간 동안 증가하지 않으면 복제된 수리가 수행될 수 있습니다. 스캔 기간은 변경될 수 있습니다. 스캔 기간 — 예상(XSCM) * 속성은 전체 그리드에 적용되며 모든 노드 스캔 기간의 최대값입니다. 그리드에 대한 * Scan Period — Estimated * 속성 기록을 조회하여 적절한 기간을 결정할 수 있습니다.
- 필요에 따라 복제된 복구에 대한 예상 완료율을 얻으려면 repair-data 명령에 'show-replicated-repair-status' 옵션을 추가합니다.

  REpair-data show-replicated-repair-status'를 참조하십시오

  StorageGRID 11.6의 기술 미리 보기에는 '복제된-수리-상태' 옵션이 제공됩니다. 이 기능은 개발 중이며 반환된 값이 잘못되었거나 지연될 수 있습니다. 수리가 완료되었는지 확인하려면 에 설명된 대로 * Awaiting – All *, * repair attemptated (XRPA) * 및 * Scan Period — Estimated (XSCM) * 를 사용합니다 수리 모니터링.

삭제 코딩**(EC)** 데이터

삭제 코딩 데이터의 복구를 모니터링하고 실패한 요청을 다시 시도하려면 다음을 수행하십시오.

1. 삭제 코딩 데이터 복구 상태를 확인합니다.
   - 현재 작업의 예상 완료 시간과 완료 비율을 보려면 * 지원 * > * 도구 * > * 메트릭 * 을 선택합니다. 그런 다음 Grafana 섹션에서 * EC 개요 * 를 선택합니다. Grid EC Job Ec Job Estimated Time to Completion * 및 * Grid EC Job Percentage Completed * 대시보드를 확인합니다.
   - 특정 repair-data 작업의 상태를 확인하려면 다음 명령을 사용합니다.

     REpair-data show -ec-repair-status—repair-id repair ID'를 참조하십시오

- 이 명령을 사용하여 모든 수리를 나열합니다.

  Repair-data show-ec-repair-status'를 참조하십시오

이 출력에는 현재 실행 중인 모든 수리에 대한 "재쌍 ID"를 포함한 정보가 나열됩니다.

2. 출력에 복구 작업이 실패한 것으로 표시되면 '--repair-id' 옵션을 사용하여 복구를 다시 시도합니다.

   이 명령은 복구 ID 6949309319275667690을 사용하여 장애가 발생한 노드 복구를 재시도합니다.

   REpair-data start-ec-node-repair—repair-id 6949309319275667690

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 볼륨 복구를 재시도합니다.

   REpair-data start-ec-volume-repair—repair-id 6949309319275667690

스토리지 볼륨을 복구한 후 스토리지 상태를 확인하십시오

스토리지 볼륨을 복구한 후에는 스토리지 노드의 원하는 상태가 온라인으로 설정되어 있는지 확인하고 스토리지 노드 서버가 다시 시작될 때마다 기본적으로 상태가 온라인 상태인지 확인해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 스토리지 노드가 복구되고 데이터 복구가 완료되었습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. 복구된 스토리지 노드 * > * LDR * > * 스토리지 * > * 스토리지 상태 — 원하는 * 및 * 스토리지 상태 — 현재 * 값을 확인합니다.

   두 속성의 값은 온라인이어야 합니다.

3. 원하는 스토리지 상태가 읽기 전용으로 설정되어 있으면 다음 단계를 수행하십시오.
   a. Configuration * 탭을 클릭합니다.
   b. Storage State — Desired * 드롭다운 목록에서 * Online * 을 선택합니다.
   c. 변경 내용 적용 * 을 클릭합니다.
   d. Overview * 탭을 클릭하고 * Storage State — Desired * 및 * Storage State — Current * 의 값이 Online으로 업데이트되었는지 확인합니다.

시스템 드라이브 오류에서 복구합니다

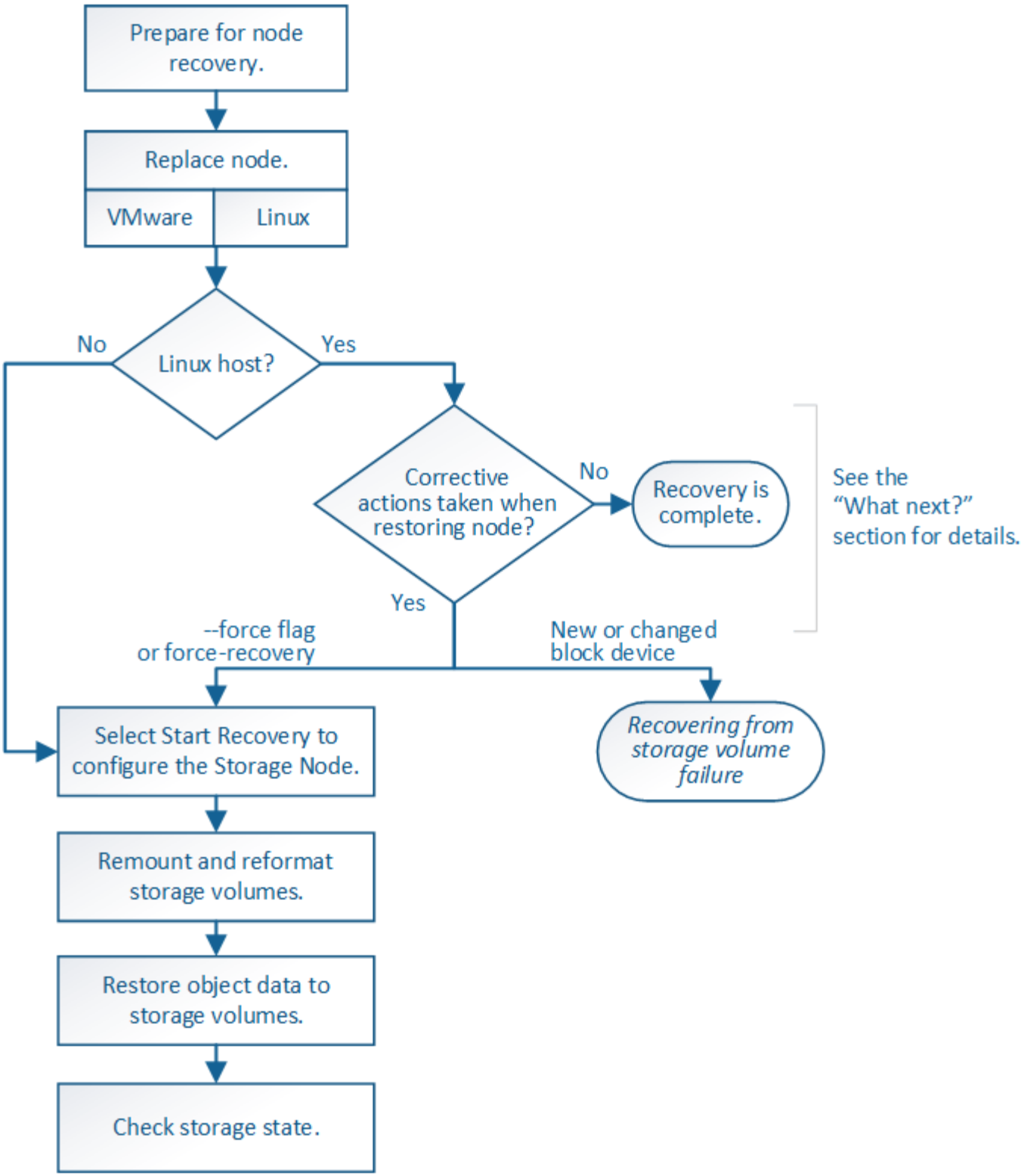
소프트웨어 기반 스토리지 노드의 시스템 드라이브에 장애가 발생한 경우 StorageGRID 시스템에서 스토리지 노드를 사용할 수 없습니다. 시스템 드라이브 장애 시 복구하려면 특정 작업 세트를 완료해야 합니다.

이 작업에 대해

소프트웨어 기반 스토리지 노드의 시스템 드라이브 장애를 복구하려면 다음 절차를 따르십시오. 이 절차에는 스토리지 볼륨도 실패하거나 다시 마운트할 수 없는 경우 따라야 할 단계가 포함되어 있습니다.

> 이 절차는 소프트웨어 기반 스토리지 노드에만 적용됩니다. 어플라이언스 스토리지 노드를 복구하려면 다른 절차를 따라야 합니다.

어플라이언스 스토리지 노드를 복구합니다



스토리지 노드 시스템 드라이브 복구에 대한 경고를 검토합니다

스토리지 노드의 장애가 발생한 시스템 드라이브를 복구하기 전에 다음 경고를 검토해야 합니다.

스토리지 노드에는 개체 메타데이터가 포함된 Cassandra 데이터베이스가 있습니다. Cassandra 데이터베이스는 다음과 같은 환경에서 재구축됩니다.

- 스토리지 노드는 15일 이상 오프라인 상태가 된 후 다시 온라인 상태로 전환됩니다.

- 스토리지 볼륨이 실패하여 복구되었습니다.
- 시스템 드라이브 및 하나 이상의 스토리지 볼륨이 실패하고 복구됩니다.

Cassandra가 재구성되면 시스템은 다른 스토리지 노드의 정보를 사용합니다. 너무 많은 스토리지 노드가 오프라인인 경우 일부 Cassandra 데이터를 사용하지 못할 수 있습니다. Cassandra가 최근에 다시 빌드된 경우, Cassandra 데이터가 그리드 전체에서 아직 일관되지 않을 수 있습니다. Cassandra가 너무 많은 스토리지 노드가 오프라인이거나 둘 이상의 스토리지 노드가 서로 15일 이내에 재구축된 경우 데이터 손실이 발생할 수 있습니다.

> 둘 이상의 스토리지 노드에 장애가 있거나 오프라인 상태인 경우 기술 지원 부서에 문의하십시오. 다음 복구 절차를 수행하지 마십시오. 데이터가 손실될 수 있습니다.

> 스토리지 노드 장애 또는 복구 후 15일 이내에 두 번째 스토리지 노드 오류인 경우 기술 지원 부서에 문의하십시오. 15일 이내에 두 개 이상의 스토리지 노드에서 Cassandra를 재구축하면 데이터가 손실될 수 있습니다.

> 한 사이트에 둘 이상의 스토리지 노드에 장애가 발생한 경우 사이트 복구 절차가 필요할 수 있습니다. 기술 지원 부서에 문의하십시오.

기술 지원 부서에서 사이트 복구를 수행하는 방법

> 이 스토리지 노드가 읽기 전용 유지 보수 모드에 있으면 스토리지 볼륨이 장애가 발생한 다른 스토리지 노드에서 객체를 검색할 수 있습니다. 장애가 발생한 스토리지 노드를 복구하기 전에 스토리지 노드의 볼륨을 장애가 발생한 스토리지 볼륨으로 복구합니다. 시스템 드라이브가 손상되지 않은 스토리지 볼륨의 손실로부터 복구하는 지침은 를 참조하십시오.

> ILM 규칙이 복제된 복사본을 하나만 저장하도록 구성되어 있고 해당 복사본이 실패한 스토리지 볼륨에 있으면 개체를 복구할 수 없습니다.

> 복구 중 서비스:상태-Cassandra(SVST) 경보가 발생하는 경우, Cassandra를 재작성하여 모니터링 및 문제 해결 지침을 참조하여 알람에서 복구합니다. Cassandra가 재구축된 후에는 경보가 지워집니다. 알람이 소거되지 않으면 기술 지원 부서에 문의하십시오.

관련 정보

모니터링하고 문제를 해결합니다

그리드 노드 복구에 대한 경고 및 고려 사항

시스템 드라이브가 손상되지 않은 스토리지 볼륨 장애로부터 복구합니다

스토리지 노드를 교체합니다

시스템 드라이브에 오류가 발생한 경우 먼저 스토리지 노드를 교체해야 합니다.

플랫폼에 대한 노드 교체 절차를 선택해야 합니다. 노드를 교체하는 단계는 모든 유형의 그리드 노드에 대해 동일합니다.

> 이 절차는 소프트웨어 기반 스토리지 노드에만 적용됩니다. 어플라이언스 스토리지 노드를 복구하려면 다른 절차를 따라야 합니다.

어플라이언스 스토리지 노드를 복구합니다

- Linux: * 시스템 드라이브 고장 여부를 잘 모르는 경우 지침에 따라 노드를 교체하여 필요한 복구 단계를 결정합니다.

플랫폼	절차를 참조하십시오
VMware	VMware 노드를 교체합니다
리눅스	Linux 노드를 교체합니다
더 적합하였습니다	NetApp에서 제공하는 OpenStack용 가상 머신 디스크 파일 및 스크립트는 더 이상 복구 작업을 지원하지 않습니다. OpenStack 배포에서 실행 중인 노드를 복구해야 하는 경우 Linux 운영 체제용 파일을 다운로드하십시오. 그런 다음 Linux 노드 교체 절차를 따릅니다.

복구 시작 을 선택하여 스토리지 노드를 구성합니다

스토리지 노드를 교체한 후 그리드 관리자에서 복구 시작 을 선택하여 장애가 발생한 노드의 대체 노드로 새 노드를 구성해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.
- 교체 노드를 구축하고 구성해야 합니다.
- 삭제 코딩 데이터에 대한 복구 작업의 시작 날짜를 알아야 합니다.
- 스토리지 노드가 지난 15일 이내에 재구축되지 않은 것을 확인해야 합니다.

이 작업에 대해

스토리지 노드가 Linux 호스트에 컨테이너로 설치되어 있는 경우 다음 중 하나가 참인 경우에만 이 단계를 수행해야 합니다.

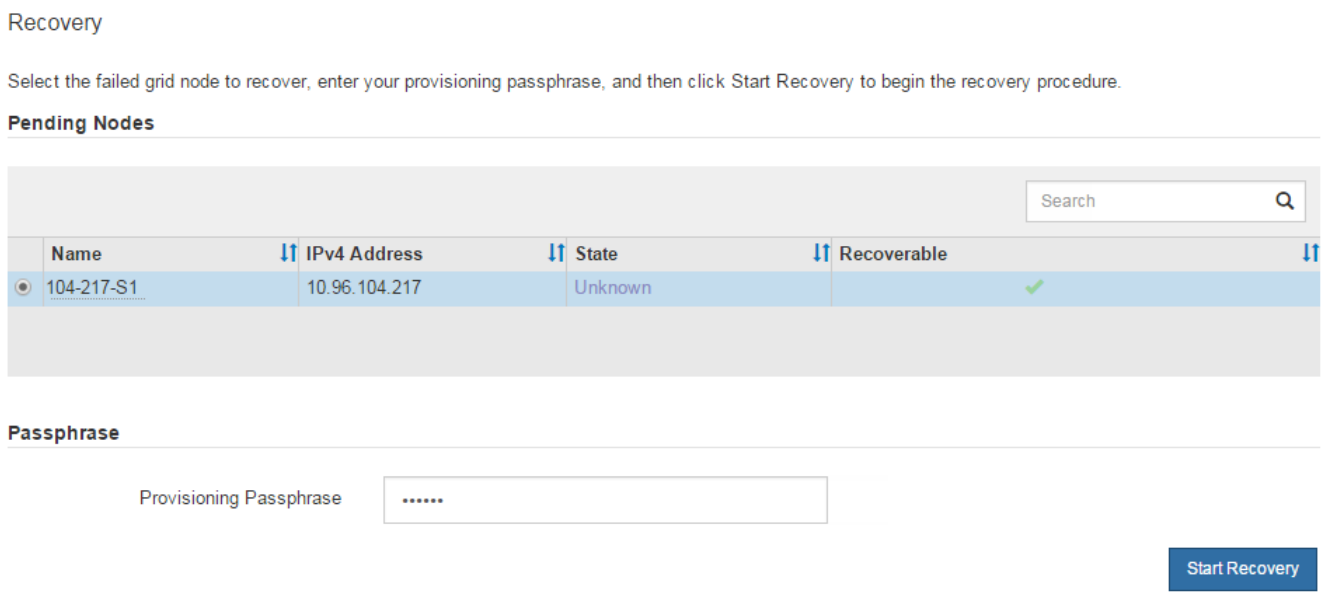
- 노드를 가져오려면 '--force' 플래그를 사용하거나 StorageGRID node force-recovery_node-name_'을(를) 실행했습니다
- 전체 노드를 다시 설치하거나 /var/local을 복원해야 했습니다.

단계

1. Grid Manager에서 * 유지보수 * > * 작업 * > * 복구 * 를 선택합니다.
2. Pending Nodes 목록에서 복구할 그리드 노드를 선택합니다.

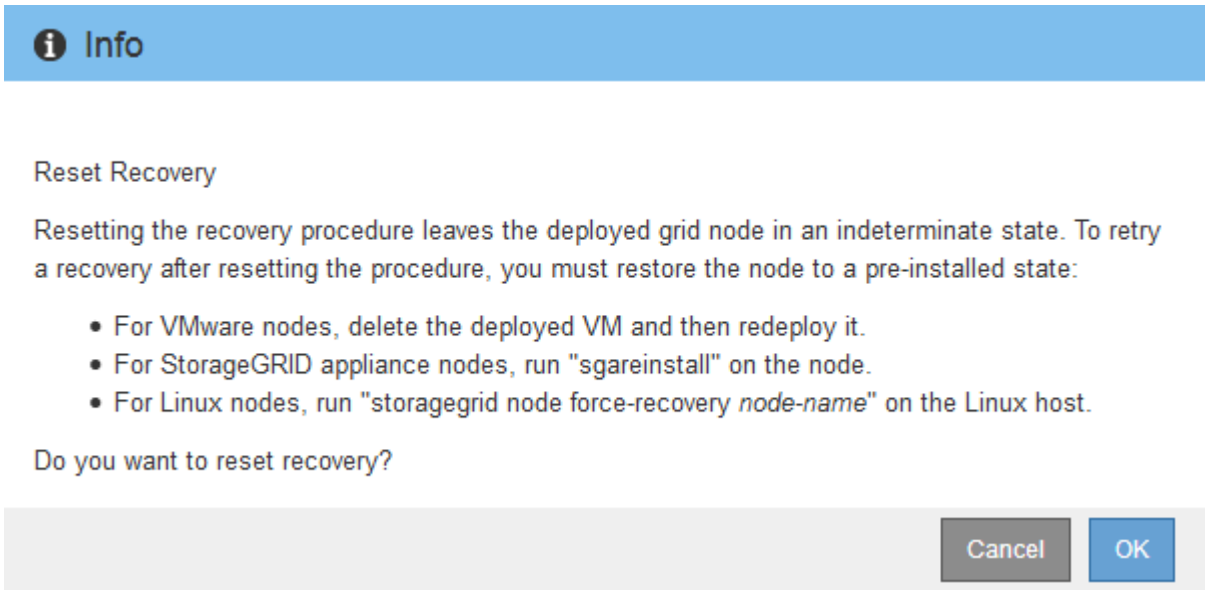
   노드가 실패한 후 목록에 나타나지만 다시 설치되고 복구 준비가 될 때까지 노드를 선택할 수 없습니다.

3. Provisioning Passphrase * 를 입력합니다.
4. 복구 시작 * 을 클릭합니다.



5. 복구 그리드 노드 테이블에서 복구 진행률을 모니터링합니다.

> 복구 절차가 실행되는 동안 * Reset * 을 클릭하여 새 복구를 시작할 수 있습니다. 프로시저를 재설정하면 노드가 결정되지 않은 상태로 남아 있음을 나타내는 정보 대화 상자가 나타납니다.



절차를 재설정한 후 복구를 재시도하려면 다음과 같이 노드를 사전 설치된 상태로 복원해야 합니다.

- * VMware *: 배포된 가상 그리드 노드를 삭제합니다. 그런 다음 복구를 다시 시작할 준비가 되면 노드를 다시 배포합니다.
- Linux*: Linux 호스트에서 'StorageGRID node force-recovery_node-name_' 명령을 실행하여 노드를 다시 시작합니다

6. 스토리지 노드가 ""수동 단계 대기 중" 단계에 도달하면 복구 절차의 다음 작업으로 이동하여 스토리지 볼륨을 다시 마운트하고 다시 포맷합니다.

관련 정보

스토리지 볼륨을 다시 마운트하고 다시 포맷합니다**("수동 단계").**

보존된 스토리지 볼륨을 다시 마운트하고 장애가 발생한 스토리지 볼륨을 다시 포맷하려면 두 개의 스크립트를 수동으로 실행해야 합니다. 첫 번째 스크립트는 StorageGRID 스토리지 볼륨으로 올바르게 포맷된 볼륨을 다시 마운트합니다. 두 번째 스크립트는 마운트 해제된 볼륨을 다시 포맷하고 필요한 경우 Cassandra를 재구축하며 서비스를 시작합니다.

필요한 것

- 장애가 발생한 스토리지 볼륨의 하드웨어를 교체하도록 이미 교체했습니다.

  'n-다시 마운트-볼륨' 스크립트를 실행하면 오류가 발생한 추가 스토리지 볼륨을 식별하는 데 도움이 될 수 있습니다.

- 스토리지 노드 사용 중지가 진행 중이 아니거나 노드 사용 중단 절차를 일시 중지했습니다. (Grid Manager에서 * 유지보수 * > * 작업 * > * 서비스 해제 * 를 선택합니다.)
- 확장이 진행 중이 아닌 것을 확인했습니다. (Grid Manager에서 * 유지보수 * > * 작업 * > * 확장 * 을 선택합니다.)
- 있습니다 스토리지 노드 시스템 드라이브 복구에 대한 경고를 검토했습니다.

> 두 개 이상의 스토리지 노드가 오프라인이거나 이 그리드의 스토리지 노드가 최근 15일 내에 재구축된 경우 기술 지원 부서에 문의하십시오. sn-recovery-postinstall.sh 스크립트를 실행하지 마십시오. 2개 이상의 스토리지 노드에서 Cassandra를 상호 간에 15일 이내에 재구축하면 데이터가 손실될 수 있습니다.

이 작업에 대해

이 절차를 완료하려면 다음과 같은 고급 작업을 수행해야 합니다.

- 복구된 스토리지 노드에 로그인합니다.
- 'n-다시 마운트-볼륨' 스크립트를 실행하여 적절하게 포맷된 스토리지 볼륨을 다시 마운트합니다. 이 스크립트가 실행되면 다음 작업을 수행합니다.
  - 각 스토리지 볼륨을 마운트 및 마운트 해제하고 XFS 저널을 재생합니다.
  - XFS 파일 일관성 검사를 수행합니다.
  - 파일 시스템의 정합성이 보장되면 스토리지 볼륨이 제대로 포맷된 StorageGRID 스토리지 볼륨인지 확인합니다.
  - 저장소 볼륨이 제대로 포맷된 경우 저장소 볼륨을 다시 마운트합니다. 볼륨의 기존 데이터는 그대로 유지됩니다.
- 스크립트 출력을 검토하고 문제를 해결합니다.
- 'sn-recovery-postinstall.sh' 스크립트를 실행합니다. 이 스크립트가 실행되면 다음 작업을 수행합니다.

> 실행 전에 복구 중에 스토리지 노드를 재부팅하지 마십시오 `sn-recovery-postinstall.sh` 장애가 발생한 스토리지 볼륨을 다시 포맷하고 객체 메타데이터를 복원합니다. 전에 스토리지 노드를 재부팅합니다 `sn-recovery-postinstall.sh` 완료로 인해 서비스를 시작하려고 하는 서비스에 오류가 발생하여 StorageGRID 어플라이언스 노드가 유지보수 모드를 종료합니다. 의 단계를 참조하십시오 설치 후 스크립트.

  - 'n-remount-volumes' 스크립트가 마운트할 수 없거나 잘못 포맷된 스토리지 볼륨을 다시 포맷합니다.

> 저장소 볼륨이 다시 포맷되면 해당 볼륨의 모든 데이터가 손실됩니다. ILM 규칙이 두 개 이상의 개체 복사본을 저장하도록 구성되었다고 가정하여 그리드의 다른 위치에서 개체 데이터를 복원하려면 추가 절차를 수행해야 합니다.

- 필요한 경우 노드에서 Cassandra 데이터베이스를 재구축합니다.
- 스토리지 노드에서 서비스를 시작합니다.

단계

1. 복구된 스토리지 노드에 로그인:

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 첫 번째 스크립트를 실행하여 적절하게 포맷된 스토리지 볼륨을 다시 마운트합니다.

   > 모든 스토리지 볼륨이 새 볼륨이고 포맷해야 하거나 모든 스토리지 볼륨이 실패한 경우 이 단계를 건너뛰고 두 번째 스크립트를 실행하여 마운트 해제된 모든 스토리지 볼륨을 다시 포맷할 수 있습니다.

   a. 'n-다시 마운트-볼륨' 스크립트를 실행합니다

      이 스크립트는 데이터가 포함된 스토리지 볼륨에서 실행되는 데 몇 시간이 걸릴 수 있습니다.

   b. 스크립트가 실행되면 출력을 검토하고 프롬프트에 응답합니다.

      > 필요에 따라 'tail-f' 명령을 사용하여 스크립트 로그 파일의 내용을 모니터링할 수 있습니다('/var/local/log/sn-다시 마운트-volumes.log"). 로그 파일에는 명령줄 출력보다 자세한 정보가 들어 있습니다.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully
```

```
====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
```

```
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

예제 출력에서 한 스토리지 볼륨이 성공적으로 다시 마운트되었으며 세 개의 스토리지 볼륨에 오류가 발생했습니다.

- '/dev/sdb'는 XFS 파일 시스템 일관성 검사를 통과하고 유효한 볼륨 구조를 가지고 있으므로 성공적으로 다시 마운트되었습니다. 스크립트에 의해 다시 마운트된 디바이스의 데이터는 보존됩니다.
- 스토리지 볼륨이 새 볼륨이거나 손상되었기 때문에 '/dev/sdc'가 XFS 파일 시스템 일관성 검사에 실패했습니다.
- 디스크가 초기화되지 않았거나 디스크의 수퍼블록이 손상되어 '/dev/SDD'를 마운트할 수 없습니다. 스크립트가 스토리지 볼륨을 마운트할 수 없는 경우 파일 시스템 정합성 검사를 실행할 것인지 묻는 메시지가 표시됩니다.
  - 스토리지 볼륨이 새 디스크에 연결되어 있는 경우 프롬프트에 * N * 으로 응답합니다. 새 디스크에서 파일 시스템을 확인할 필요가 없습니다.
  - 스토리지 볼륨이 기존 디스크에 연결되어 있는 경우 프롬프트에 * Y * 로 응답합니다. 파일 시스템 검사 결과를 사용하여 손상의 원인을 확인할 수 있습니다. 결과는 '/var/local/log/sn-res마운트-volumes.log' 로그 파일에 저장됩니다.
- '/dev/SDE'는 XFS 파일 시스템 일관성 검사를 통과하고 유효한 볼륨 구조를 가지고 있지만 volid 파일의 LDR 노드 ID가 이 스토리지 노드의 ID(맨 위에 표시된 구성된 LDR noid)와 일치하지 않습니다. 이 메시지는 이 볼륨이 다른 스토리지 노드에 속함을 나타냅니다.

3. 스크립트 출력을 검토하고 문제를 해결합니다.

> 스토리지 볼륨이 XFS 파일 시스템 일관성 검사에 실패했거나 마운트할 수 없는 경우 출력에서 오류 메시지를 자세히 검토합니다. 이러한 볼륨에 대해 'sn-recovery-postinstall.sh' 스크립트를 실행하면 어떤 영향이 있는지 이해해야 합니다.

   a. 결과에 예상한 모든 볼륨에 대한 항목이 포함되어 있는지 확인합니다. 목록에 볼륨이 없으면 스크립트를 다시 실행합니다.

   b. 마운트된 모든 디바이스에 대한 메시지를 검토합니다. 스토리지 볼륨이 이 스토리지 노드에 속해 있지 않음을 나타내는 오류가 없는지 확인합니다.

      이 예에서 '/dev/SDE'의 출력에는 다음 오류 메시지가 포함됩니다.

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> 스토리지 볼륨이 다른 스토리지 노드에 속하는 것으로 보고되면 기술 지원 부서에 문의하십시오. 'sn-recovery-postinstall.sh' 스크립트를 실행하면 스토리지 볼륨이 다시 포맷되어 데이터가 손실될 수 있습니다.

   c. 스토리지 디바이스를 마운트할 수 없는 경우 디바이스 이름을 기록해 두고 디바이스를 복구하거나 교체합니다.

> 마운트할 수 없는 스토리지 디바이스를 복구하거나 교체해야 합니다.

      디바이스 이름을 사용하여 볼륨 ID를 조회합니다. 볼륨 ID는 'repair-data' 스크립트를 실행하여 객체 데이터를 볼륨에 복원할 때 입력해야 합니다(다음 절차).

   d. UNMOUNTABLE 장치를 모두 복구하거나 교체한 후 'n-remount-volumes' 스크립트를 다시 실행하여 다시 마운트할 수 있는 모든 스토리지 볼륨이 다시 마운트되었는지 확인합니다.

> 스토리지 볼륨을 마운트할 수 없거나 잘못 포맷한 경우 다음 단계를 계속 수행하면 볼륨의 모든 데이터와 볼륨이 삭제됩니다. 오브젝트 데이터의 복사본이 2개인 경우 다음 절차(오브젝트 데이터 복원)를 완료할 때까지 복사본 하나가 유지됩니다.

> 실패한 스토리지 볼륨에 남아 있는 데이터를 그리드의 다른 위치에서 재구축할 수 없다고 판단되는 경우(예: ILM 정책에서 하나의 복제본만 만드는 규칙을 사용하거나 여러 노드에서 볼륨이 실패한 경우) 'sn-recovery-postinstall.sh' 스크립트를 실행하지 마십시오. 대신 기술 지원 부서에 문의하여 데이터 복구 방법을 확인하십시오.

4. sn-recovery-postinstall.sh 스크립트: sn-recovery-postinstall.sh를 실행합니다

   이 스크립트는 마운트할 수 없거나 잘못 포맷된 스토리지 볼륨을 다시 포맷하고, 필요한 경우 노드에서 Cassandra 데이터베이스를 재구축하고, 스토리지 노드에서 서비스를 시작합니다.

   다음 사항에 유의하십시오.

   - 스크립트를 실행하는 데 몇 시간이 걸릴 수 있습니다.

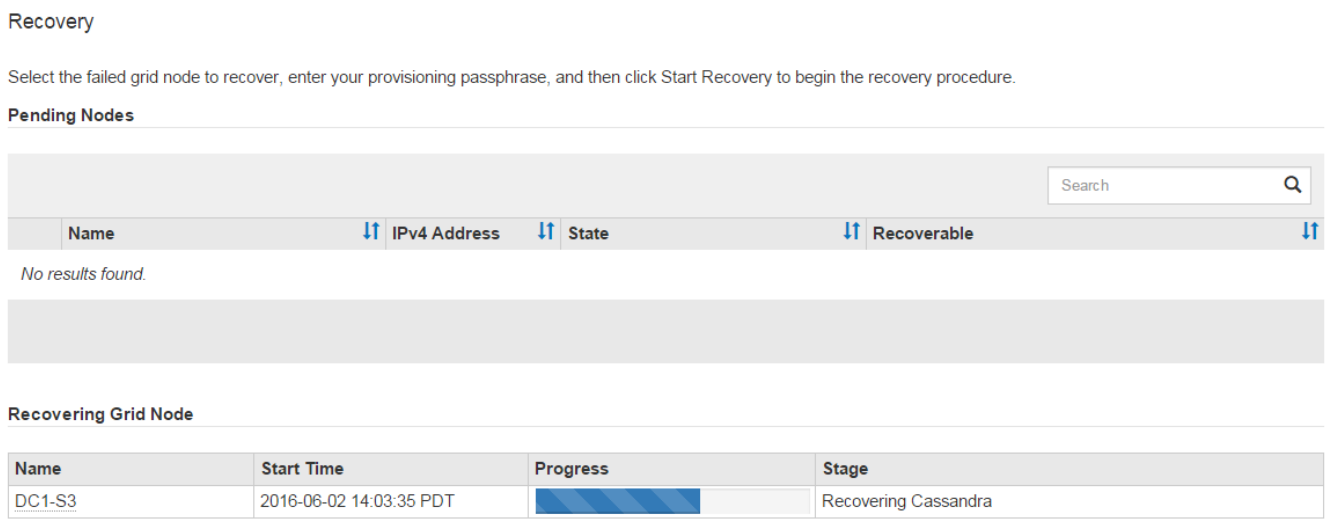
- 일반적으로 스크립트가 실행되는 동안에는 SSH 세션만 남겨야 합니다.
- SSH 세션이 활성화되어 있는 동안에는 * Ctrl + C * 를 누르지 마십시오.
- 네트워크 중단이 발생하여 SSH 세션을 종료하는 경우 스크립트는 백그라운드에서 실행되지만 복구 페이지에서 진행률을 볼 수 있습니다.
- 스토리지 노드가 RSM 서비스를 사용하는 경우 노드 서비스가 다시 시작됨에 따라 스크립트가 5분 동안 정지되는 것처럼 보일 수 있습니다. RSM 서비스가 처음 부팅될 때마다 5분 정도 지연될 수 있습니다.

> RSM 서비스는 ADC 서비스를 포함하는 스토리지 노드에 있습니다.

> 일부 StorageGRID 복구 절차에서는 리퍼를 사용하여 Cassandra 수리를 처리합니다. 관련 또는 필수 서비스가 시작되는 즉시 수리가 자동으로 이루어집니다. "리퍼" 또는 "'Cassandra 수리'라는 스크립트 출력을 볼 수 있습니다. 복구가 실패했다는 오류 메시지가 나타나면 오류 메시지에 표시된 명령을 실행합니다.

5. 을(를) 로 설정합니다 `sn-recovery-postinstall.sh` 스크립트가 실행되면 Grid Manager에서 복구 페이지를 모니터링합니다.

   복구 페이지의 진행률 표시줄과 단계 열은 'sn-recovery-postinstall.sh' 스크립트의 상위 상태를 제공합니다.



'sn-recovery-postinstall.sh' 스크립트가 노드에서 서비스를 시작한 후 해당 절차에 설명된 대로 스크립트로 포맷된 모든 스토리지 볼륨에 객체 데이터를 복원할 수 있습니다.

관련 정보

스토리지 노드 시스템 드라이브 복구에 대한 경고를 검토합니다

필요한 경우 오브젝트 데이터를 스토리지 볼륨으로 복구합니다

필요한 경우 오브젝트 데이터를 스토리지 볼륨으로 복구합니다

하나 이상의 실패한 스토리지 볼륨을 다시 포맷하기 위해 'sn-recovery-postinstall.sh' 스크립트가 필요한 경우 다른 스토리지 노드 및 아카이브 노드에서 포맷된 스토리지 볼륨으로 객체 데이터를 복원해야 합니다. 하나 이상의 스토리지 볼륨을 다시 포맷하지 않으면 이러한 단계가 필요하지 않습니다.

필요한 것

- 복구된 스토리지 노드의 접속 상태가 * 연결됨 * 으로 확인되어야 합니다 Grid Manager의 * nodes * > * Overview * (노드 * > * 개요 *) 탭에서 선택합니다.

이 작업에 대해

그리드의 ILM 규칙이 구성되어 있어 오브젝트 복사본을 사용할 수 있다고 가정할 때 다른 스토리지 노드, 아카이브 노드 또는 클라우드 스토리지 풀에서 오브젝트 데이터를 복원할 수 있습니다.

다음 사항에 유의하십시오.

- ILM 규칙이 한 개의 복제된 복사본만 저장하도록 구성되었고 해당 복사본이 실패한 스토리지 볼륨에 존재하면 개체를 복구할 수 없습니다.
- 개체의 나머지 복사본만 클라우드 스토리지 풀에 있는 경우 StorageGRID은 오브젝트 데이터를 복원하기 위해 클라우드 스토리지 풀 엔드포인트에 여러 요청을 실행해야 합니다. 이 절차를 수행하기 전에 기술 지원 부서에 문의하여 복구 시간 프레임 및 관련 비용을 추정하십시오.
- 개체의 나머지 복사본만 아카이브 노드에 있는 경우 아카이브 노드에서 개체 데이터가 검색됩니다. 아카이브 노드에서 스토리지 노드로 오브젝트 데이터를 복원하는 것은 외부 아카이브 스토리지 시스템에서 검색 지연 시간 때문에 다른 스토리지 노드에서 복사본을 복원하는 것보다 시간이 더 오래 걸립니다.

에 대해 `repair-data` 스크립트

객체 데이터를 복원하려면 "repair-data" 스크립트를 실행합니다. 이 스크립트는 개체 데이터 복원 프로세스를 시작하고 ILM 스캔 작업을 통해 ILM 규칙이 충족되는지 확인합니다.

아래에서 * 복제된 데이터 * 또는 * 삭제 코딩(EC) 데이터 * 를 선택하여 복제된 데이터 또는 삭제 코딩 데이터 복원 여부에 따라 리페어 데이터(repair-data) 스크립트에 대한 다양한 옵션을 알아보십시오. 두 유형의 데이터를 모두 복원해야 하는 경우 두 명령 집합을 모두 실행해야 합니다.

repair-data 스크립트에 대한 자세한 내용은 기본 Admin Node의 명령줄에 repair-data—help를 입력하십시오.

복제된 데이터

전체 노드를 복구해야 하는지 또는 노드의 특정 볼륨만 복구해야 하는지 여부에 따라 두 가지 명령을 사용하여 복제된 데이터를 복원할 수 있습니다.

'repair-data start-replicated-node-repair'를 선택합니다

Repair-data start-replicated-volume-repair를 선택합니다

다음 명령을 사용하여 복제된 데이터의 복구를 추적할 수 있습니다.

REpair-data show-replicated-repair-status'를 참조하십시오

> StorageGRID 11.6의 기술 미리 보기에는 '복제된-수리-상태' 옵션이 제공됩니다. 이 기능은 개발 중이며 반환된 값이 잘못되었거나 지연될 수 있습니다. 수리가 완료되었는지 확인하려면 에 설명된 대로 * Awaiting – All *, * repair attemptated (XRPA) * 및 * Scan Period — Estimated (XSCM) * 를 사용합니다 수리 모니터링.

삭제 코딩**(EC)** 데이터

전체 노드를 복구해야 하는지 또는 노드의 특정 볼륨만 복구해야 하는지 여부에 따라 두 가지 명령을 사용하여 삭제 코딩 데이터를 복원할 수 있습니다.

Repair-data start-ec-node-repair를 선택합니다

Repair-data start-ec-volume-repair를 선택합니다

일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

다음 명령을 사용하여 삭제 코딩 데이터의 복구를 추적할 수 있습니다.

Repair-data show-ec-repair-status'를 참조하십시오

> EC 복구 작업은 일시적으로 많은 양의 저장 공간을 예약합니다. 스토리지 알림이 트리거될 수 있지만 복구가 완료되면 문제가 해결됩니다. 예약 저장 공간이 충분하지 않으면 EC 복구 작업이 실패합니다. 작업 실패 또는 성공 여부에 관계없이 EC 복구 작업이 완료되면 저장소 예약이 해제됩니다.

스토리지 노드의 호스트 이름을 찾습니다

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 복구된 스토리지 볼륨에 대한 스토리지 노드의 호스트 이름을 찾으려면 '/etc/hosts' 파일을 사용합니다. 그리드의 모든 노드 목록을 보려면 cat /etc/hosts를 입력한다.

모든 볼륨이 실패한 경우 데이터를 복구합니다

모든 스토리지 볼륨에 장애가 발생한 경우 전체 노드를 복구합니다. 복제된 데이터 *, * 삭제 코딩(EC) 데이터 * 또는 둘 다에 대한 지침을 따르십시오. 복제된 데이터, 삭제 코딩(EC) 데이터 또는 둘 모두를 사용하는지 여부에 따라 달라집니다.

일부 볼륨만 장애가 발생한 경우 로 이동합니다 일부 볼륨만 장애가 발생한 경우 데이터를 복구합니다.

> 둘 이상의 노드에 대해 동시에 '데이터 다시 페어링' 작업을 실행할 수 없습니다. 여러 노드를 복구하려면 기술 지원 팀에 문의하십시오.

복제된 데이터

그리드에 복제된 데이터가 포함된 경우, '- nodes' 옵션과 함께 'repair-data start-replicated-node-repair' 명령을 사용하여 전체 스토리지 노드를 복구하십시오.

이 명령은 SG-DC-SN3이라는 스토리지 노드에서 복제된 데이터를 복구합니다.

REpair-data start-replicated-node-repair — nodes SG-DC-SN3'으로 표시됩니다

> 개체 데이터가 복원되면 StorageGRID 시스템에서 복제된 개체 데이터를 찾을 수 없을 경우 * 개체 손실 * 경고가 트리거됩니다. 시스템 전체의 스토리지 노드에서 경고가 트리거될 수 있습니다. 손실의 원인과 복구가 가능한지 확인해야 합니다. 을 참조하십시오 모니터링하고 문제를 해결합니다.

삭제 코딩**(EC)** 데이터

그리드에 삭제 코딩 데이터가 포함된 경우, '- nodes' 옵션과 함께 'repair-data start-EC-node-repair' 명령을 사용하여 전체 스토리지 노드를 복구하십시오.

이 명령은 이름이 SG-DC-SN3인 스토리지 노드에서 삭제 코딩 데이터를 복구합니다.

REpair-data start-ec-node-repair—nodes SG-DC-SN3'을 선택합니다

이 작업은 이 REpair_DATA 작업을 식별하는 고유한 REpair ID를 반환합니다. 이 재쌍 ID를 사용하여 REpair_DATA 작업의 진행 상황과 결과를 추적할 수 있습니다. 복구 프로세스가 완료되어도 다른 피드백이 반환되지 않습니다.

> 일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

일부 볼륨만 장애가 발생한 경우 데이터를 복구합니다

일부 볼륨만 장애가 발생한 경우 영향을 받는 볼륨을 복구합니다. 복제된 데이터 *, * 삭제 코딩(EC) 데이터 * 또는 둘 다에 대한 지침을 따르십시오. 복제된 데이터, 삭제 코딩(EC) 데이터 또는 둘 모두를 사용하는지 여부에 따라 달라집니다.

모든 볼륨이 실패한 경우 로 이동합니다 모든 볼륨이 실패한 경우 데이터를 복구합니다.

볼륨 ID를 16진수로 입력합니다. 예를 들어 0000은 첫 번째 볼륨이고 000F는 16번째 볼륨입니다. 하나의 볼륨, 하나의 볼륨 범위 또는 시퀀스에 없는 여러 볼륨을 지정할 수 있습니다.

모든 볼륨은 동일한 스토리지 노드에 있어야 합니다. 둘 이상의 스토리지 노드에 대한 볼륨을 복원해야 하는 경우 기술 지원 부서에 문의하십시오.

복제된 데이터

그리드에 복제된 데이터가 포함된 경우 '--nodes' 옵션과 함께 'start-replicated-volume-repair' 명령을 사용하여 노드를 식별합니다. 그런 다음 다음 아래 예와 같이 '--volumes' 또는 '- volume-range' 옵션을 추가합니다.

- 단일 볼륨 *: 이 명령은 복제된 데이터를 SG-DC-SN3이라는 스토리지 노드의 볼륨 '0002'로 복원합니다.

REpair-data start-replicated-volume-repair—nodes SG-DC-SN3—volum0002"를 참조하십시오

- 볼륨 범위 *: 이 명령은 SG-DC-SN3이라는 스토리지 노드의 "0003" ~ "0009" 범위의 모든 볼륨에 복제된 데이터를 복원합니다.

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

- 다중 볼륨 시퀀스 없음 *: 이 명령은 SG-DC-SN3이라는 스토리지 노드의 볼륨 '0001', '0005' 및 '0008'으로 복제된 데이터를 복원합니다.

REpair-data start-replicated-volume-repair—nodes SG-DC-SN3—volumes 0001,0005,0008'

> 개체 데이터가 복원되면 StorageGRID 시스템에서 복제된 개체 데이터를 찾을 수 없을 경우 * 개체 손실 * 경고가 트리거됩니다. 시스템 전체의 스토리지 노드에서 경고가 트리거될 수 있습니다. 손실의 원인과 복구가 가능한지 확인해야 합니다. StorageGRID 모니터링 및 문제 해결에 대한 지침을 참조하십시오.

삭제 코딩**(EC)** 데이터

그리드에 삭제 코딩 데이터가 포함된 경우 '- nodes' 옵션과 함께 'start-ec-volume-repair' 명령을 사용하여 노드를 식별하십시오. 그런 다음 다음 아래 예와 같이 '--volumes' 또는 '- volume-range' 옵션을 추가합니다.

- 단일 볼륨 *: 이 명령은 SG-DC-SN3이라는 스토리지 노드의 볼륨 '0007'에 삭제 코딩 데이터를 복원합니다.

REpair-data start-ec-volume-repair—nodes SG-DC-SN3—volumes 0007'을 참조하십시오

- 볼륨 범위 *: 이 명령은 삭제 코딩 데이터를 SG-DC-SN3이라는 스토리지 노드의 "0004" ~ "0006" 범위에 있는 모든 볼륨에 복원합니다.

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

- Multiple volumes not in a sequence *: 이 명령은 SG-DC-SN3이라는 스토리지 노드의 볼륨 '000A', '000C' 및 '000E'로 삭제 코딩 데이터를 복원합니다.

REpair-data start-EC-volume-repair—nodes SG-DC-SN3—volumes 000A, 000C, 000E

repair-data는 이 repair_data 작업을 식별하는 고유한 repair ID를 반환합니다. 이 재쌍 ID를 사용하여 REpair_DATA 작업의 진행 상황과 결과를 추적할 수 있습니다. 복구 프로세스가 완료되어도 다른 피드백이 반환되지 않습니다.

> 일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

수리 모니터링

복제된 데이터 *, * 삭제 코딩(EC) 데이터 * 또는 둘 모두를 사용하는지 여부에 따라 복구 작업의 상태를 모니터링합니다.

복제된 데이터

- 수리가 완료되었는지 확인하려면:
  a. 노드 * > * _ 복구되는 스토리지 노드 _ * > * ILM * 을 선택합니다.
  b. 평가 섹션의 속성을 검토합니다. 복구가 완료되면 * Awaiting-all * 속성이 0 개체를 나타냅니다.
- 수리를 더 자세히 모니터링하려면:
  a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
  b. 복구되는 **GRID* * > *_Storage Node _ * > * LDR * > * Data Store * 를 선택합니다.
  c. 복제된 수리가 완료된 경우 다음 특성을 조합하여 가능한 한 결정합니다.

    Cassandra의 일관성이 없을 수 있으며, 복구 실패를 추적하지 않습니다.

    - * 시도된 복구(XRPA) **:** 이 속성을 사용하여 복제된 복구 진행률을 추적합니다**.** 이 속성은 스토리지 노드가 고위험 객체를 복구하려고 할 때마다 증가합니다**.** 이 속성이 현재 스캔 기간**(** Scan Period — Estimated* 속성 제공)보다 더 긴 기간 동안 증가하지 않으면 ILM 스캐닝에서 모든 노드에서 복구해야 할 고위험 개체를 찾지 못한 것입니다.

      고위험 개체는 완전히 손실될 위험이 있는 개체입니다. ILM 구성을 충족하지 않는 개체는 포함되지 않습니다.

    - * 스캔 기간 — 예상(XSCM) *: 이 속성을 사용하여 이전에 수집된 개체에 정책 변경이 적용되는 시점을 추정합니다. 복구 시도 * 속성이 현재 스캔 기간보다 긴 기간 동안 증가하지 않으면 복제된 수리가 수행될 수 있습니다. 스캔 기간은 변경될 수 있습니다. 스캔 기간 — 예상(XSCM) * 속성은 전체 그리드에 적용되며 모든 노드 스캔 기간의 최대값입니다. 그리드에 대한 * Scan Period — Estimated * 속성 기록을 조회하여 적절한 기간을 결정할 수 있습니다.
- 필요에 따라 복제된 복구에 대한 예상 완료율을 얻으려면 repair-data 명령에 'show-replicated-repair-status' 옵션을 추가합니다.

  REpair-data show-replicated-repair-status'를 참조하십시오

  StorageGRID 11.6의 기술 미리 보기에는 '복제된-수리-상태' 옵션이 제공됩니다. 이 기능은 개발 중이며 반환된 값이 잘못되었거나 지연될 수 있습니다. 수리가 완료되었는지 확인하려면 에 설명된 대로 * Awaiting – All *, * repair attemptated (XRPA) * 및 * Scan Period — Estimated (XSCM) * 를 사용합니다 수리 모니터링.

삭제 코딩**(EC)** 데이터

삭제 코딩 데이터의 복구를 모니터링하고 실패한 요청을 다시 시도하려면 다음을 수행하십시오.

1. 삭제 코딩 데이터 복구 상태를 확인합니다.
   - 현재 작업의 예상 완료 시간과 완료 비율을 보려면 * 지원 * > * 도구 * > * 메트릭 * 을 선택합니다. 그런 다음 Grafana 섹션에서 * EC 개요 * 를 선택합니다. Grid EC Job Ec Job Estimated Time to Completion * 및 * Grid EC Job Percentage Completed * 대시보드를 확인합니다.
   - 특정 repair-data 작업의 상태를 확인하려면 다음 명령을 사용합니다.

     REpair-data show -ec-repair-status—repair-id repair ID'를 참조하십시오

- 이 명령을 사용하여 모든 수리를 나열합니다.

  Repair-data show-ec-repair-status'를 참조하십시오

이 출력에는 현재 실행 중인 모든 수리에 대한 "재쌍 ID"를 포함한 정보가 나열됩니다.

2. 출력에 복구 작업이 실패한 것으로 표시되면 '--repair-id' 옵션을 사용하여 복구를 다시 시도합니다.

   이 명령은 복구 ID 6949309319275667690을 사용하여 장애가 발생한 노드 복구를 재시도합니다.

   REpair-data start-ec-node-repair—repair-id 6949309319275667690

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 볼륨 복구를 재시도합니다.

   REpair-data start-ec-volume-repair—repair-id 6949309319275667690

스토리지 노드 시스템 드라이브를 복구한 후 스토리지 상태를 확인합니다

스토리지 노드에 대한 시스템 드라이브를 복구한 후에는 스토리지 노드의 원하는 상태가 온라인으로 설정되어 있는지 확인하고 스토리지 노드 서버가 다시 시작될 때마다 기본적으로 상태가 온라인 상태인지 확인해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 스토리지 노드가 복구되고 데이터 복구가 완료되었습니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. 복구된 스토리지 노드 * > * LDR * > * 스토리지 * > * 스토리지 상태 — 원하는 * 및 * 스토리지 상태 — 현재 * 값을 확인합니다.

   두 속성의 값은 온라인이어야 합니다.

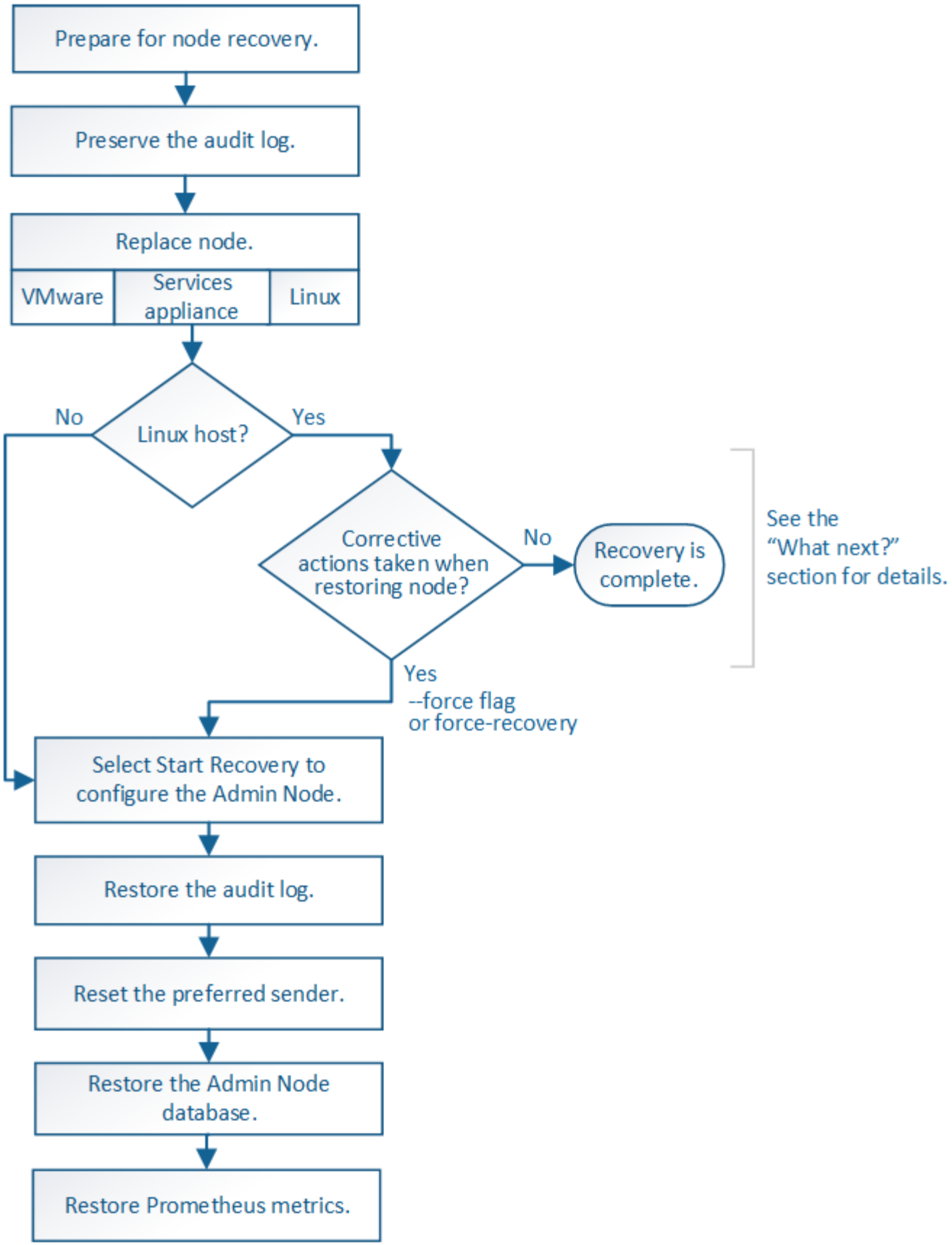
3. 원하는 스토리지 상태가 읽기 전용으로 설정되어 있으면 다음 단계를 수행하십시오.
   a. Configuration * 탭을 클릭합니다.
   b. Storage State — Desired * 드롭다운 목록에서 * Online * 을 선택합니다.
   c. 변경 내용 적용 * 을 클릭합니다.
   d. Overview * 탭을 클릭하고 * Storage State — Desired * 및 * Storage State — Current * 의 값이 Online으로 업데이트되었는지 확인합니다.

관리자 노드 오류에서 복구

관리 노드의 복구 프로세스는 기본 관리 노드인지 또는 비기본 관리 노드인지에 따라 달라집니다.

이 작업에 대해

기본 또는 비기본 관리 노드를 복구하는 높은 수준의 단계는 동일하지만 단계의 세부 사항은 다릅니다.



복구 중인 관리 노드에 대해 항상 올바른 복구 절차를 따르십시오. 절차는 높은 수준에서 동일하지만 세부 사항은 다릅니다.

관련 정보

SG100 및 SG1000 서비스 어플라이언스

선택

- 운영 관리 노드 오류에서 복구
- 운영 관리자 노드가 아닌 노드에서 복구합니다

운영 관리 노드 오류에서 복구

기본 관리 노드 오류에서 복구하려면 특정 작업 세트를 완료해야 합니다. 기본 관리 노드는 그리드에 대한 CMN(Configuration Management Node) 서비스를 호스팅합니다.

이 작업에 대해

장애가 발생한 운영 관리자 노드는 즉시 교체해야 합니다. 기본 관리 노드의 CMN(구성 관리 노드) 서비스는 그리드에 대한 객체 식별자 블록을 발행합니다. 이러한 식별자는 인제스트될 때 오브젝트에 할당됩니다. 사용 가능한 식별자가 없으면 새 개체를 인제스트할 수 없습니다. 약 한 달 동안 ID가 그리드에 캐시되기 때문에 CMN을 사용할 수 없는 동안 객체 인제스트를 계속할 수 있습니다. 그러나 캐시된 식별자를 모두 사용한 후에는 새 개체를 추가할 수 없습니다.

> 장애가 발생한 1차 관리 노드를 약 1개월 이내에 복구하거나 교체해야 합니다. 그렇지 않으면 그리드에 새 객체를 수집하는 기능이 손실될 수 있습니다. 정확한 기간은 개체 수집 속도에 따라 다릅니다. 그리드에 대한 기간을 더 정확하게 평가하려면 기술 지원 부서에 문의하십시오.

실패한 기본 관리 노드에서 감사 로그를 복사합니다

실패한 기본 관리 노드에서 감사 로그를 복사할 수 있는 경우 감사 로그를 보존하여 시스템 활동 및 사용에 대한 그리드의 기록을 유지해야 합니다. 유지 감사 로그를 실행 및 실행한 후 복구된 기본 관리 노드에 복원할 수 있습니다.

이 절차에서는 실패한 관리 노드의 감사 로그 파일을 별도의 그리드 노드의 임시 위치로 복사합니다. 이렇게 보존된 감사 로그를 대체 관리 노드에 복사할 수 있습니다. 감사 로그는 새 관리 노드에 자동으로 복사되지 않습니다.

실패 유형에 따라 실패한 관리 노드에서 감사 로그를 복사하지 못할 수 있습니다. 배포에 하나의 관리 노드만 있는 경우 복구된 관리 노드는 새 빈 파일의 감사 로그에 이벤트를 기록하기 시작하고 이전에 기록된 데이터가 손실됩니다. 배포에 둘 이상의 관리 노드가 포함된 경우 다른 관리 노드에서 감사 로그를 복구할 수 있습니다.

> 이제 실패한 관리 노드에서 감사 로그에 액세스할 수 없는 경우 호스트 복구 후 나중에 감사 로그에 액세스할 수 있습니다.

1. 가능한 경우 실패한 관리 노드에 로그인합니다. 그렇지 않으면 기본 관리자 노드 또는 다른 관리자 노드(있는 경우)에 로그인합니다.
   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
2. 새 로그 파일('Service AMS stop')을 만들지 못하도록 AMS 서비스를 중지합니다

3. audit.log 파일을 복구된 관리 노드에 복사할 때 기존 파일을 덮어쓰지 않도록 파일 이름을 바꿉니다.

   audit.log 이름을 yyyy-mm-dd.txt.1과 같이 번호가 지정된 고유한 파일 이름으로 바꿉니다. 예를 들어 audit.log 파일의 이름을 2015-10-25.txt.1""cd/var/local/audit/export""ls-l" mv audit.log 2015-10-25.txt.1로 변경할 수 있습니다

4. AMS service:'service AMS start'를 다시 시작한다
5. 모든 감사 로그 파일을 별도의 그리드 노드의 임시 위치에 복사할 디렉토리를 만듭니다. 'ssh admin@_grid_node_ip_mkdir -p /var/local/tmp/saved-audit-logs'

   메시지가 표시되면 admin의 암호를 입력합니다.

6. 모든 감사 로그 파일:'scp -p * admin@*GRID_node_ip*:/var/local/tmp/saved-audit-logs'를 복사합니다

   메시지가 표시되면 admin의 암호를 입력합니다.

7. root: exit로 로그아웃

기본 관리 노드를 교체합니다

기본 관리 노드를 복구하려면 먼저 물리적 또는 가상 하드웨어를 교체해야 합니다.

장애가 발생한 운영 관리 노드를 동일한 플랫폼에서 실행되는 운영 관리 노드로 교체하거나, VMware 또는 Linux 호스트에서 실행되는 운영 관리 노드를 서비스 어플라이언스에서 호스팅되는 운영 관리 노드로 교체할 수 있습니다.

노드에 대해 선택한 대체 플랫폼과 일치하는 절차를 사용하십시오. 모든 노드 유형에 적합한 노드 교체 절차를 완료하면 해당 절차를 통해 운영 관리자 노드 복구를 위한 다음 단계로 이동합니다.

교체용 플랫폼	절차를 참조하십시오
VMware	VMware 노드를 교체합니다
리눅스	Linux 노드를 교체합니다
SG100 및 SG1000 서비스 어플라이언스	서비스 어플라이언스를 교체하십시오
더 적합하였습니다	NetApp에서 제공하는 OpenStack용 가상 머신 디스크 파일 및 스크립트는 더 이상 복구 작업을 지원하지 않습니다. OpenStack 배포에서 실행 중인 노드를 복구해야 하는 경우 Linux 운영 체제용 파일을 다운로드하십시오. 그런 다음 Linux 노드 교체 절차를 따릅니다.

대체 운영 관리자 노드를 구성합니다

교체 노드는 StorageGRID 시스템의 기본 관리 노드로 구성해야 합니다.

필요한 것

- 가상 시스템에서 호스팅되는 운영 관리 노드의 경우 가상 머신을 구축, 전원 켜기 및 초기화해야 합니다.
- 서비스 어플라이언스에서 호스팅되는 운영 관리 노드의 경우 어플라이언스를 교체하고 소프트웨어를 설치했습니다.

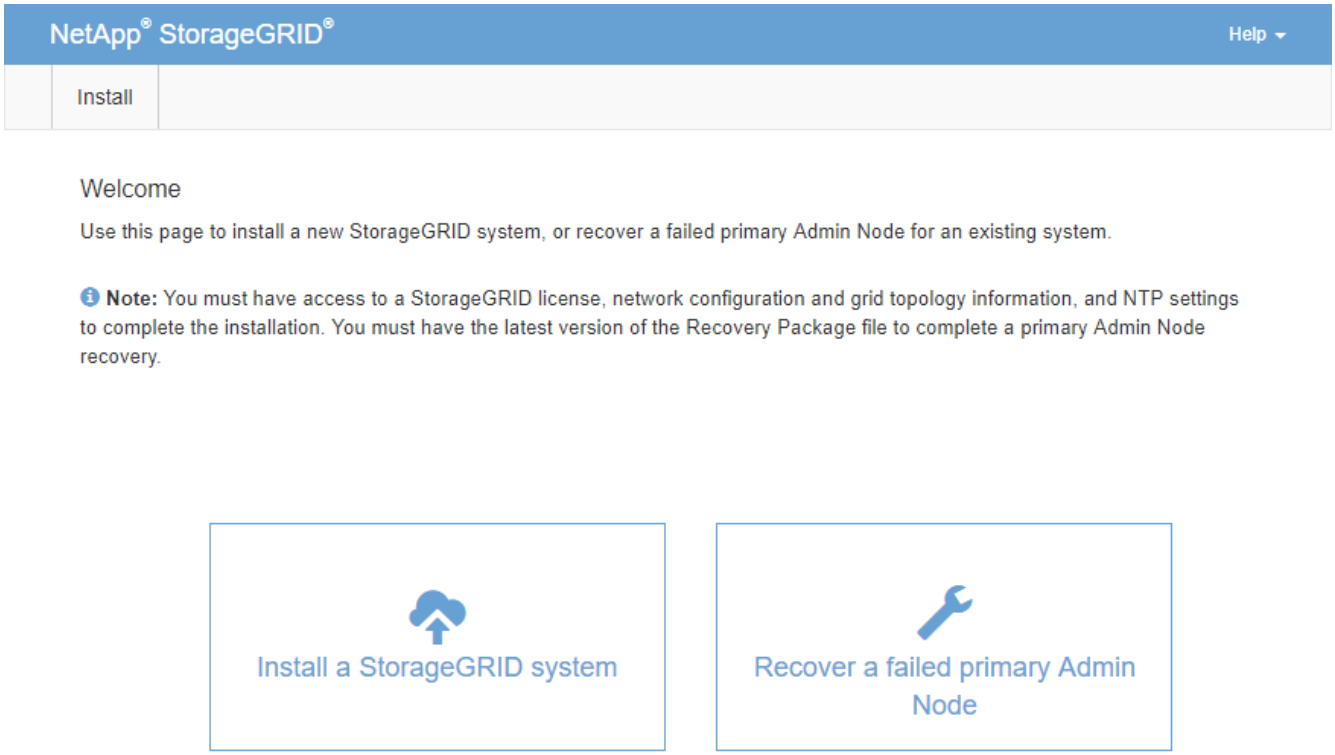
사용 중인 제품의 설치 안내서를 참조하십시오.

SG100 및 SG1000 서비스 어플라이언스

- 복구 패키지 파일의 최신 백업이 있어야 합니다('SUW-RECOVERY-PACKAGE-*id-revision*.zip').
- 프로비저닝 암호가 있어야 합니다.

단계

1. 웹 브라우저를 열고 'https://primary_admin_node_ip` 이동하십시오.



2. 실패한 운영 관리자 노드 복구 * 를 클릭합니다.
3. 복구 패키지의 최신 백업 업로드:
   a. 찾아보기 * 를 클릭합니다.
   b. StorageGRID 시스템에 대한 최신 복구 패키지 파일을 찾아 * 열기 * 를 클릭합니다.
4. 프로비저닝 암호를 입력합니다.
5. 복구 시작 * 을 클릭합니다.

   복구 프로세스가 시작됩니다. 필요한 서비스가 시작되면서 몇 분 동안 Grid Manager를 사용할 수 없게 될 수 있습니다. 복구가 완료되면 로그인 페이지가 표시됩니다.

6. StorageGRID 시스템에 SSO(Single Sign-On)가 설정되어 있고 복구된 관리자 노드에 대한 기반 당사자 트러스트가 기본 관리 인터페이스 인증서를 사용하도록 구성된 경우 AD FS(Active Directory Federation Services)에서 노드의 기반 당사자 트러스트를 업데이트(또는 삭제 및 다시 생성)합니다. 관리 노드 복구 프로세스 중에 생성된 새 기본 서버 인증서를 사용합니다.

> 신뢰할 수 있는 상대 신뢰를 구성하려면 StorageGRID 관리 지침을 참조하십시오. 기본 서버 인증서에 액세스하려면 관리 노드의 명령 셸에 로그인합니다. '/var/local/mgmt-api' 디렉토리로 이동하여 'server.crt' 파일을 선택한다.

7. 핫픽스를 적용해야 하는지 확인합니다.
   a. 를 사용하여 Grid Manager에 로그인합니다 지원되는 웹 브라우저.
   b. 노드 * 를 선택합니다.
   c. 왼쪽 목록에서 기본 관리 노드를 선택합니다.
   d. 개요 탭의 * 소프트웨어 버전 * 필드에 표시된 버전을 확인합니다.
   e. 다른 그리드 노드를 선택합니다.
   f. 개요 탭의 * 소프트웨어 버전 * 필드에 표시된 버전을 확인합니다.
      - 소프트웨어 버전* 필드에 표시된 버전이 같으면 핫픽스를 적용할 필요가 없습니다.
      - 소프트웨어 버전* 필드에 표시된 버전이 다른 경우 핫픽스를 적용하여 복구된 기본 관리 노드를 동일한 버전으로 업데이트해야 합니다.

관련 정보

StorageGRID 관리

StorageGRID 핫픽스 절차

복구된 운영 관리자 노드에서 감사 로그를 복구합니다

실패한 기본 관리 노드에서 감사 로그를 보존할 수 있는 경우 복구 중인 기본 관리 노드에 복사할 수 있습니다.

- 복구된 관리자 노드를 설치하고 실행해야 합니다.
- 원래 관리 노드에 장애가 발생한 후 감사 로그를 다른 위치로 복사해야 합니다.

관리자 노드에 장애가 발생하면 해당 관리 노드에 저장된 감사 로그가 손실될 수 있습니다. 실패한 관리 노드에서 감사 로그를 복사한 다음 이러한 감사 로그를 복구된 관리 노드로 복원하여 손실로부터 데이터를 보존할 수 있습니다. 오류에 따라 실패한 관리 노드에서 감사 로그를 복사하지 못할 수 있습니다. 이 경우 배포에 둘 이상의 관리 노드가 있는 경우 감사 로그가 모든 관리 노드에 복제되므로 다른 관리 노드에서 감사 로그를 복구할 수 있습니다.

관리자 노드가 하나뿐이고 실패한 노드에서 감사 로그를 복사할 수 없는 경우 복구된 관리자 노드가 새 설치인 것처럼 감사 로그에 이벤트 기록을 시작합니다.

로깅 기능을 복원하려면 가능한 한 빨리 관리자 노드를 복구해야 합니다.

> 기본적으로 감사 정보는 관리 노드의 감사 로그로 전송됩니다. 다음 중 하나가 적용되는 경우 이 단계를 건너뛸 수 있습니다.
>
> - 외부 syslog 서버를 구성했으며 이제 감사 로그가 관리 노드 대신 syslog 서버로 전송됩니다.
> - 감사 메시지를 생성한 로컬 노드에만 저장하도록 명시적으로 지정했습니다.
>
> 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다 를 참조하십시오.

단계

1. 복구된 관리자 노드에 로그인합니다.

   a. ssh admin@recovery_Admin_Node_IP 명령을 입력한다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인한 후 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 어떤 감사 파일이 보존되어 있는지 'cd/var/local/audit/export'를 확인한다

3. 보존된 감사 로그 파일을 복구된 관리 노드에 복사합니다. 'scp admin@*grid_node_ip*:/var/local/tmp/saved-audit-logs/YYYY *.

   메시지가 표시되면 admin의 암호를 입력합니다.

4. 보안을 위해 장애가 발생한 그리드 노드에서 복구된 관리 노드에 성공적으로 복사되었는지 확인한 후 감사 로그를 삭제합니다.

5. 복구된 Admin Node에서 감사 로그 파일의 사용자 및 그룹 설정을 업데이트합니다: "chown AMS-user: bycast *"

6. root: exit로 로그아웃

또한 감사 공유에 대한 기존 클라이언트 액세스도 복원해야 합니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

관련 정보

StorageGRID 관리

복구된 기본 관리자 노드에서 기본 보낸 사람을 재설정합니다

복구 중인 운영 관리 노드가 현재 경고 알림, 알람 알림 및 AutoSupport 메시지의 기본 설정 송신자로 설정된 경우 이 설정을 재구성해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.
- 복구된 관리자 노드를 설치하고 실행해야 합니다.

단계

1. 구성 * > * 시스템 * > * 디스플레이 옵션 * 을 선택합니다.

2. Preferred Sender * (기본 설정 보낸 사람) 드롭다운 목록에서 복구된 관리자 노드를 선택합니다.

3. 변경 내용 적용 * 을 클릭합니다.

관련 정보

StorageGRID 관리

장애가 발생한 운영 관리 노드에 대한 속성, 경보 및 경고에 대한 기록 정보를 유지하려면 관리 노드 데이터베이스를 복원할 수 있습니다. StorageGRID 시스템에 다른 관리 노드가 포함된 경우에만 이 데이터베이스를 복원할 수 있습니다.

- 복구된 관리자 노드를 설치하고 실행해야 합니다.
- StorageGRID 시스템에는 적어도 두 개의 관리 노드가 포함되어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.

관리 노드에 장애가 발생하면 해당 관리 노드 데이터베이스에 저장된 기록 정보가 손실됩니다. 이 데이터베이스에는 다음 정보가 포함되어 있습니다.

- 알림 기록
- 알람 기록
- 내역 특성 데이터 - * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지에서 사용 가능한 차트 및 텍스트 보고서에 사용됩니다.

관리 노드를 복구할 때 소프트웨어 설치 프로세스에서는 복구된 노드에 빈 관리 노드 데이터베이스를 생성합니다. 그러나 새 데이터베이스에는 현재 시스템에 포함되어 있거나 나중에 추가된 서버 및 서비스에 대한 정보만 포함됩니다.

기본 관리 노드를 복원했고 StorageGRID 시스템에 다른 관리 노드가 있는 경우, 비 기본 관리 노드(*source* 관리 노드)에서 복구된 기본 관리 노드로 관리 노드 데이터베이스를 복사하여 기록 정보를 복원할 수 있습니다. 시스템에 기본 관리 노드만 있는 경우 관리 노드 데이터베이스를 복원할 수 없습니다.

> 관리 노드 데이터베이스를 복사하는 데 몇 시간이 걸릴 수 있습니다. 소스 관리 노드에서 서비스가 중지되는 동안에는 일부 Grid Manager 기능을 사용할 수 없습니다.

1. 소스 관리 노드에 로그인합니다.
   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.
2. 소스 관리 노드에서 MI 서비스 'service mi stop'을 중지합니다
3. 소스 관리 노드에서 관리 응용 프로그램 인터페이스(mgmt-API) 서비스인 'Service mgmt-API stop'을 중지합니다
4. 복구된 관리자 노드에서 다음 단계를 완료합니다.
   a. 복구된 관리자 노드에 로그인합니다.
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

b. MI 서비스 'Service mi stop'을 중지합니다

c. 관리 API 서비스 'service mgmt-api stop'을 중지합니다

d. SSH 에이전트에 SSH 개인 키를 추가합니다. ssh-add를 입력합니다

e. "passwords.txt" 파일에 나열된 SSH 액세스 암호를 입력합니다.

f. 원본 관리 노드에서 복구된 관리 노드로 데이터베이스를 복사합니다: "/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP"

g. 메시지가 표시되면 복구된 관리 노드의 MI 데이터베이스를 덮어쓸지 확인합니다.

   데이터베이스와 해당 기록 데이터가 복구된 관리 노드에 복사됩니다. 복사 작업이 완료되면 스크립트는 복구된 관리자 노드를 시작합니다.

h. 다른 서버에 대한 암호 없는 액세스가 더 이상 필요하지 않으면 SSH 에이전트에서 개인 키를 제거합니다. ssh-add-D를 입력합니다

5. Source Admin Node:'Service ServerManager start'에서 서비스를 다시 시작합니다

기본 관리 노드를 복구할 때 **Prometheus** 메트릭을 복원합니다

선택적으로, 장애가 발생한 운영 관리 노드에서 Prometheus가 유지 관리하는 기간별 메트릭을 유지할 수 있습니다. Prometheus 메트릭은 StorageGRID 시스템에 다른 관리 노드가 포함된 경우에만 복원할 수 있습니다.

- 복구된 관리자 노드를 설치하고 실행해야 합니다.
- StorageGRID 시스템에는 적어도 두 개의 관리 노드가 포함되어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.

관리 노드에 장애가 발생하면 관리 노드의 Prometheus 데이터베이스에 유지되는 메트릭이 손실됩니다. 관리 노드를 복구하면 소프트웨어 설치 프로세스에서 새 Prometheus 데이터베이스를 생성합니다. 복구된 관리 노드가 시작된 후 StorageGRID 시스템의 새 설치를 수행한 것처럼 메트릭을 기록합니다.

기본 관리 노드를 복원했고 StorageGRID 시스템에 다른 관리 노드가 있는 경우, 비 기본 관리 노드(*source* 관리 노드)에서 복구된 기본 관리 노드로 Prometheus 데이터베이스를 복사하여 기간별 메트릭을 복원할 수 있습니다. 시스템에 기본 관리 노드만 있는 경우 Prometheus 데이터베이스를 복원할 수 없습니다.

> Prometheus 데이터베이스를 복사하는 데 1시간 이상이 걸릴 수 있습니다. 소스 관리 노드에서 서비스가 중지되는 동안에는 일부 Grid Manager 기능을 사용할 수 없습니다.

1. 소스 관리 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

2. Source Admin Node에서 Prometheus 서비스 'Service Prometheus stop'을 중지합니다

3. 복구된 관리자 노드에서 다음 단계를 완료합니다.

   a. 복구된 관리자 노드에 로그인합니다.

      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      iii. 루트로 전환하려면 다음 명령을 입력합니다

      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   b. 프로메테우스 서비스 '프로메테우스 서비스'를 중단하십시오

   c. SSH 에이전트에 SSH 개인 키를 추가합니다. ssh-add를 입력합니다

   d. "passwords.txt" 파일에 나열된 SSH 액세스 암호를 입력합니다.

   e. 소스 관리 노드에서 복구된 관리 노드로 Prometheus 데이터베이스를 복사합니다: "/usr/local/Prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP"

   f. 메시지가 표시되면 * Enter * 를 눌러 복구된 관리 노드에서 새 Prometheus 데이터베이스를 파기할지 확인합니다.

      원래 Prometheus 데이터베이스와 해당 기록 데이터가 복구된 관리 노드에 복사됩니다. 복사 작업이 완료되면 스크립트는 복구된 관리자 노드를 시작합니다. 다음 상태가 나타납니다.

   데이터베이스가 복제되어 서비스를 시작하는 중입니다

   a. 다른 서버에 대한 암호 없는 액세스가 더 이상 필요하지 않으면 SSH 에이전트에서 개인 키를 제거합니다. ssh-add-D를 입력합니다

4. Source Admin Node에서 Prometheus 서비스를 다시 시작하고, Service Prometheus start를 한다

운영 관리자 노드가 아닌 노드에서 복구합니다

운영 관리자 노드가 아닌 노드에서 복구하려면 다음 작업을 완료해야 합니다. 하나의 관리 노드는 CMN(Configuration Management Node) 서비스를 호스팅하며 기본 관리 노드라고 합니다. 여러 개의 관리 노드를 사용할 수 있지만 각 StorageGRID 시스템에는 하나의 기본 관리 노드만 포함됩니다. 다른 모든 관리 노드는 비 기본 관리 노드입니다.

관련 정보

SG100 및 SG1000 서비스 어플라이언스

실패한 비기본 관리 노드에서 감사 로그를 복사합니다

실패한 관리 노드에서 감사 로그를 복사할 수 있는 경우 해당 감사 로그를 보존하여 시스템 활동 및 사용에 대한 그리드의 기록을 유지해야 합니다. 감사 로그를 실행 및 실행한 후 복구된 비 기본 관리 노드로 복원할 수 있습니다.

이 절차에서는 실패한 관리 노드의 감사 로그 파일을 별도의 그리드 노드의 임시 위치로 복사합니다. 이렇게 보존된 감사 로그를 대체 관리 노드에 복사할 수 있습니다. 감사 로그는 새 관리 노드에 자동으로 복사되지 않습니다.

실패 유형에 따라 실패한 관리 노드에서 감사 로그를 복사하지 못할 수 있습니다. 배포에 하나의 관리 노드만 있는 경우 복구된 관리 노드는 새 빈 파일의 감사 로그에 이벤트를 기록하기 시작하고 이전에 기록된 데이터가 손실됩니다. 배포에

둘 이상의 관리 노드가 포함된 경우 다른 관리 노드에서 감사 로그를 복구할 수 있습니다.

> 이제 실패한 관리 노드에서 감사 로그에 액세스할 수 없는 경우 호스트 복구 후 나중에 감사 로그에 액세스할 수 있습니다.

1. 가능한 경우 실패한 관리 노드에 로그인합니다. 그렇지 않으면 기본 관리자 노드 또는 다른 관리자 노드(있는 경우)에 로그인합니다.
   a. ssh admin@grid_node_ip' 명령을 입력한다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
2. 새 로그 파일('Service AMS stop')을 만들지 못하도록 AMS 서비스를 중지합니다
3. audit.log 파일을 복구된 관리 노드에 복사할 때 기존 파일을 덮어쓰지 않도록 파일 이름을 바꿉니다.

   audit.log 이름을 yyyy-mm-dd.txt.1과 같이 번호가 지정된 고유한 파일 이름으로 바꿉니다. 예를 들어 audit.log 파일의 이름을 2015-10-25.txt.1""cd/var/local/audit/export""ls-l" mv audit.log 2015-10-25.txt.1로 변경할 수 있습니다
4. AMS service:'service AMS start'를 다시 시작한다
5. 모든 감사 로그 파일을 별도의 그리드 노드의 임시 위치에 복사할 디렉터리를 만듭니다. ssh admin@grid_node_ip mkdir -p /var/local/tmp/saved-audit-logs

   메시지가 표시되면 admin의 암호를 입력합니다.
6. 모든 감사 로그 파일 복사:'scp -p * admin@grid_node_ip:/var/local/tmp/saved-audit-logs'

   메시지가 표시되면 admin의 암호를 입력합니다.
7. root: exit로 로그아웃

운영 관리자 노드가 아닌 노드를 교체합니다

운영 관리자 노드가 아닌 노드를 복구하려면 먼저 물리적 또는 가상 하드웨어를 교체해야 합니다.

장애가 발생한 비 운영 관리 노드를 동일한 플랫폼에서 실행되는 비 운영 관리 노드로 대체하거나, VMware 또는 Linux 호스트에서 실행되는 비 운영 관리 노드를 서비스 어플라이언스에서 호스팅되는 비 운영 관리 노드로 교체할 수 있습니다.

노드에 대해 선택한 대체 플랫폼과 일치하는 절차를 사용하십시오. 모든 노드 유형에 적합한 노드 교체 절차를 완료하면 해당 절차를 통해 비 기본 관리 노드 복구를 위한 다음 단계로 이동합니다.

교체용 플랫폼	절차를 참조하십시오
VMware	VMware 노드를 교체합니다

교체용 플랫폼	절차를 참조하십시오
리눅스	Linux 노드를 교체합니다
SG100 및 SG1000 서비스 어플라이언스	서비스 어플라이언스를 교체하십시오
더 적합하였습니다	NetApp에서 제공하는 OpenStack용 가상 머신 디스크 파일 및 스크립트는 더 이상 복구 작업을 지원하지 않습니다. OpenStack 배포에서 실행 중인 노드를 복구해야 하는 경우 Linux 운영 체제용 파일을 다운로드하십시오. 그런 다음 Linux 노드 교체 절차를 따릅니다.

복구 시작 을 선택하여 비 기본 관리 노드를 구성합니다

비기본 관리 노드를 교체한 후 그리드 관리자에서 복구 시작 을 선택하여 새 노드를 장애가 발생한 노드에 대한 교체품으로 구성해야 합니다.

필요한 것

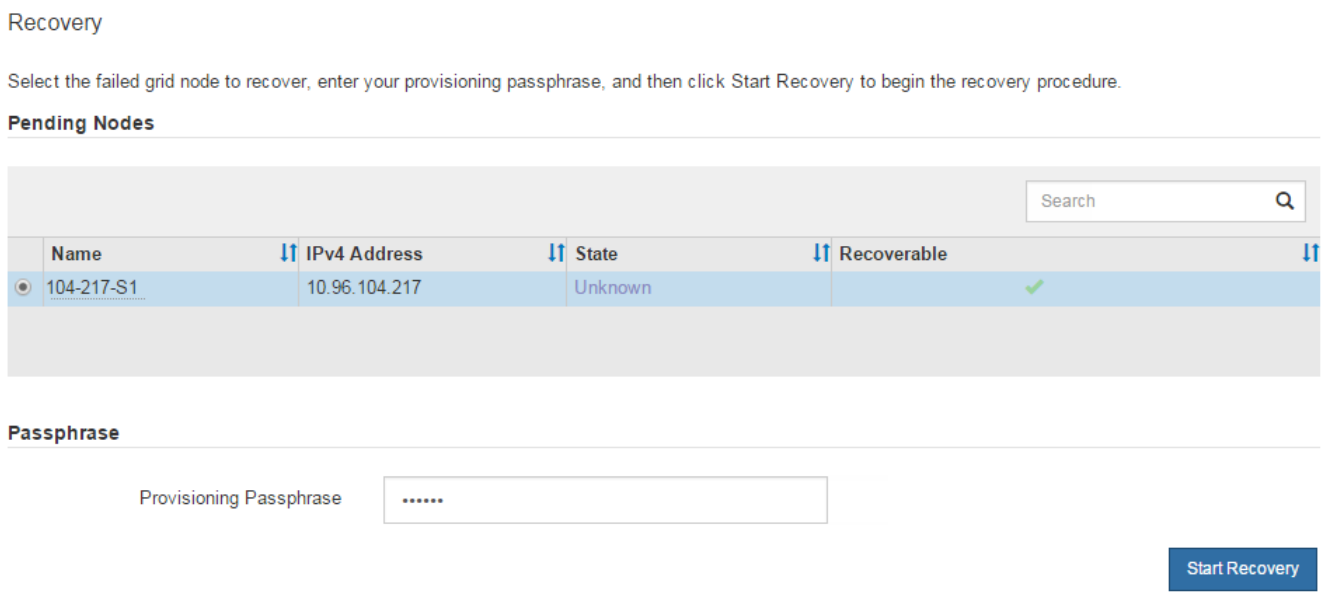
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.
- 교체 노드를 구축하고 구성해야 합니다.

단계

1. Grid Manager에서 * 유지보수 * > * 작업 * > * 복구 * 를 선택합니다.
2. Pending Nodes 목록에서 복구할 그리드 노드를 선택합니다.

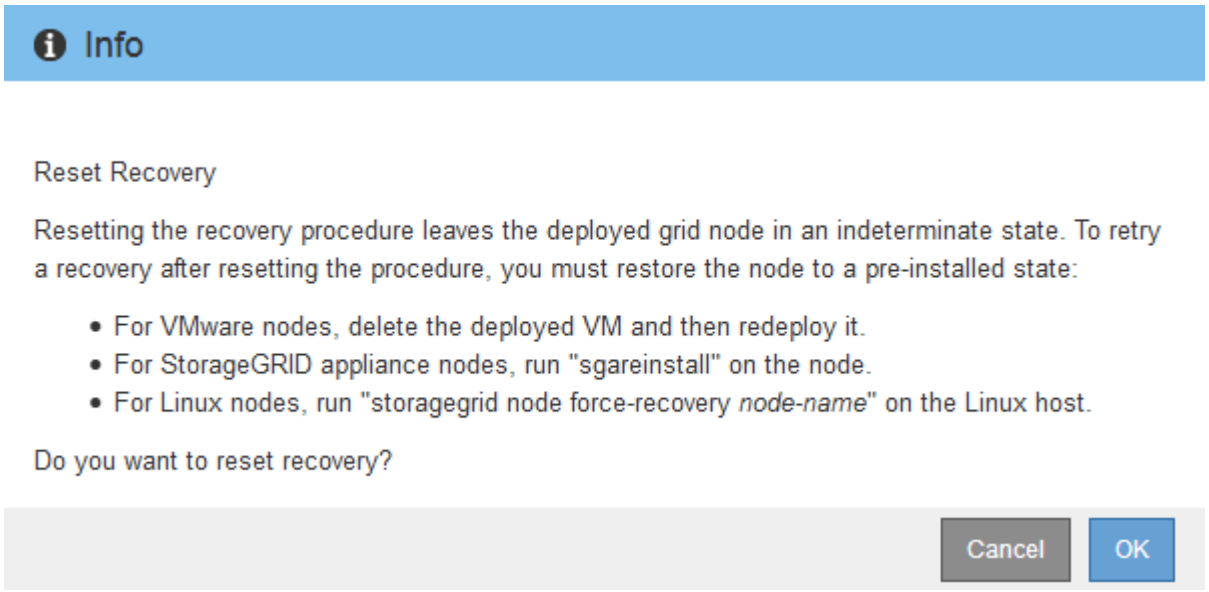
   노드가 실패한 후 목록에 나타나지만 다시 설치되고 복구 준비가 될 때까지 노드를 선택할 수 없습니다.

3. Provisioning Passphrase * 를 입력합니다.
4. 복구 시작 * 을 클릭합니다.



5. 복구 그리드 노드 테이블에서 복구 진행률을 모니터링합니다.

> 복구 절차가 실행되는 동안 * Reset * 을 클릭하여 새 복구를 시작할 수 있습니다. 프로시저를 재설정하면 노드가 결정되지 않은 상태로 남아 있음을 나타내는 정보 대화 상자가 나타납니다.



절차를 재설정한 후 복구를 재시도하려면 다음과 같이 노드를 사전 설치된 상태로 복원해야 합니다.

- * VMware *: 배포된 가상 그리드 노드를 삭제합니다. 그런 다음 복구를 다시 시작할 준비가 되면 노드를 다시 배포합니다.
- Linux*: Linux 호스트에서 'StorageGRID node force-recovery_node-name_' 명령을 실행하여 노드를 다시 시작합니다
- * 어플라이언스*: 절차를 재설정한 후 복구를 재시도하려면 노드에서 '설치'를 실행하여 어플라이언스 노드를 사전 설치 상태로 복원해야 합니다.

6. StorageGRID 시스템에 SSO(Single Sign-On)가 설정되어 있고 복구된 관리자 노드에 대한 기반 당사자 트러스트가 기본 관리 인터페이스 인증서를 사용하도록 구성된 경우 AD FS(Active Directory Federation

Services)에서 노드의 기반 당사자 트러스트를 업데이트(또는 삭제 및 다시 생성)합니다. 관리 노드 복구 프로세스 중에 생성된 새 기본 서버 인증서를 사용합니다.

> 신뢰할 수 있는 상대 신뢰를 구성하려면 StorageGRID 관리 지침을 참조하십시오. 기본 서버 인증서에 액세스하려면 관리 노드의 명령 셸에 로그인합니다. '/var/local/mgmt-api' 디렉토리로 이동하여 'server.crt' 파일을 선택한다.

관련 정보

StorageGRID 관리

어플라이언스 재설치 준비(플랫폼 교체만 해당)

복구된 비 기본 관리자 노드에서 감사 로그를 복구합니다

실패한 비 기본 관리 노드에서 감사 로그를 보존할 수 있으므로 기록 감사 로그 정보를 보존할 수 있다면 복구 중인 비 기본 관리 노드에 복사할 수 있습니다.

- 복구된 관리자 노드를 설치하고 실행해야 합니다.
- 원래 관리 노드에 장애가 발생한 후 감사 로그를 다른 위치로 복사해야 합니다.

관리자 노드에 장애가 발생하면 해당 관리 노드에 저장된 감사 로그가 손실될 수 있습니다. 실패한 관리 노드에서 감사 로그를 복사한 다음 이러한 감사 로그를 복구된 관리 노드로 복원하여 손실로부터 데이터를 보존할 수 있습니다. 오류에 따라 실패한 관리 노드에서 감사 로그를 복사하지 못할 수 있습니다. 이 경우 배포에 둘 이상의 관리 노드가 있는 경우 감사 로그가 모든 관리 노드에 복제되므로 다른 관리 노드에서 감사 로그를 복구할 수 있습니다.

관리자 노드가 하나뿐이고 실패한 노드에서 감사 로그를 복사할 수 없는 경우 복구된 관리자 노드가 새 설치인 것처럼 감사 로그에 이벤트 기록을 시작합니다.

로깅 기능을 복원하려면 가능한 한 빨리 관리자 노드를 복구해야 합니다.

> 기본적으로 감사 정보는 관리 노드의 감사 로그로 전송됩니다. 다음 중 하나가 적용되는 경우 이 단계를 건너뛸 수 있습니다.
>
> - 외부 syslog 서버를 구성했으며 이제 감사 로그가 관리 노드 대신 syslog 서버로 전송됩니다.
> - 감사 메시지를 생성한 로컬 노드에만 저장하도록 명시적으로 지정했습니다.
>
> 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다 를 참조하십시오.

단계

1. 복구된 관리자 노드에 로그인합니다.

   a. 다음 명령을 입력합니다: + ssh admin@recovery_Admin_Node_IP'

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인한 후 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 어떤 감사 파일이 보존되었는지 확인합니다.

   'cd /var/local/audit/export'

3. 보존된 감사 로그 파일을 복구된 관리 노드에 복사합니다.

   'CP admin@grid_node_ip:/var/local/tmp/saved-audit-logs/YYYY *'

   메시지가 표시되면 admin의 암호를 입력합니다.

4. 보안을 위해 장애가 발생한 그리드 노드에서 복구된 관리 노드에 성공적으로 복사되었는지 확인한 후 감사 로그를 삭제합니다.
5. 복구된 관리 노드에서 감사 로그 파일의 사용자 및 그룹 설정을 업데이트합니다.

   'chown AMS-user: bycast *'

6. root: exit로 로그아웃

또한 감사 공유에 대한 기존 클라이언트 액세스도 복원해야 합니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

관련 정보

StorageGRID 관리

복구된 비 기본 관리 노드에서 기본 보낸 사람을 재설정합니다

복구 중인 비 운영 관리 노드가 현재 경고 알림, 알람 알림 및 AutoSupport 메시지의 기본 설정 송신자로 설정된 경우 StorageGRID 시스템에서 이 설정을 다시 구성해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 특정 액세스 권한이 있어야 합니다.
- 복구된 관리자 노드를 설치하고 실행해야 합니다.

단계

1. 구성 * > * 시스템 * > * 디스플레이 옵션 * 을 선택합니다.
2. Preferred Sender * (기본 설정 보낸 사람) 드롭다운 목록에서 복구된 관리자 노드를 선택합니다.
3. 변경 내용 적용 * 을 클릭합니다.

관련 정보

StorageGRID 관리

비운영 관리자 노드를 복구할 때 관리 노드 데이터베이스를 복원합니다

장애가 발생한 비 운영 관리 노드에 대한 속성, 경보 및 경고에 대한 기록 정보를 보존하려면 기본 관리 노드에서 관리 노드 데이터베이스를 복원할 수 있습니다.

- 복구된 관리자 노드를 설치하고 실행해야 합니다.

- StorageGRID 시스템에는 적어도 두 개의 관리 노드가 포함되어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.

관리 노드에 장애가 발생하면 해당 관리 노드 데이터베이스에 저장된 기록 정보가 손실됩니다. 이 데이터베이스에는 다음 정보가 포함되어 있습니다.

- 알림 기록
- 알람 기록
- 내역 특성 데이터 - * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지에서 사용 가능한 차트 및 텍스트 보고서에 사용됩니다.

관리 노드를 복구할 때 소프트웨어 설치 프로세스에서는 복구된 노드에 빈 관리 노드 데이터베이스를 생성합니다. 그러나 새 데이터베이스에는 현재 시스템에 포함되어 있거나 나중에 추가된 서버 및 서비스에 대한 정보만 포함됩니다.

운영 관리자 노드가 아닌 노드를 복원한 경우 운영 관리 노드(*source Admin Node*)에서 복구된 노드로 관리 노드 데이터베이스를 복사하여 기록 정보를 복원할 수 있습니다.

> 관리 노드 데이터베이스를 복사하는 데 몇 시간이 걸릴 수 있습니다. 일부 Grid Manager 기능은 소스 노드에서 서비스가 중지되는 동안 사용할 수 없습니다.

1. 소스 관리 노드에 로그인합니다.
   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.
2. 소스 관리 노드에서 다음 명령을 실행합니다. 그런 다음 메시지가 표시되면 프로비저닝 암호를 입력합니다. 재액세스 포인트
3. 소스 관리 노드에서 MI 서비스 'service mi stop'을 중지합니다
4. 소스 관리 노드에서 관리 응용 프로그램 인터페이스(mgmt-API) 서비스인 'Service mgmt-API stop'을 중지합니다
5. 복구된 관리자 노드에서 다음 단계를 완료합니다.
   a. 복구된 관리자 노드에 로그인합니다.
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다
      iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   b. MI 서비스 'Service mi stop'을 중지합니다
   c. 관리 API 서비스 'service mgmt-api stop'을 중지합니다
   d. SSH 에이전트에 SSH 개인 키를 추가합니다. ssh-add를 입력합니다
   e. "passwords.txt" 파일에 나열된 SSH 액세스 암호를 입력합니다.

f. 원본 관리 노드에서 복구된 관리 노드로 데이터베이스를 복사합니다: "/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP"

g. 메시지가 표시되면 복구된 관리 노드의 MI 데이터베이스를 덮어쓸지 확인합니다.

   데이터베이스와 해당 기록 데이터가 복구된 관리 노드에 복사됩니다. 복사 작업이 완료되면 스크립트는 복구된 관리자 노드를 시작합니다.

h. 다른 서버에 대한 암호 없는 액세스가 더 이상 필요하지 않으면 SSH 에이전트에서 개인 키를 제거합니다. ssh-add-D를 입력합니다

6. Source Admin Node:'Service ServerManager start'에서 서비스를 다시 시작합니다

비운영 관리자 노드를 복구할 때 **Prometheus** 메트릭을 복원합니다

선택적으로, 장애가 발생한 비 운영 관리 노드에서 Prometheus가 유지 관리하는 기간별 메트릭을 유지할 수 있습니다.

- 복구된 관리자 노드를 설치하고 실행해야 합니다.
- StorageGRID 시스템에는 적어도 두 개의 관리 노드가 포함되어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.

관리 노드에 장애가 발생하면 관리 노드의 Prometheus 데이터베이스에 유지되는 메트릭이 손실됩니다. 관리 노드를 복구하면 소프트웨어 설치 프로세스에서 새 Prometheus 데이터베이스를 생성합니다. 복구된 관리 노드가 시작된 후 StorageGRID 시스템의 새 설치를 수행한 것처럼 메트릭을 기록합니다.

운영 관리자 노드가 아닌 노드를 복원한 경우 기본 관리 노드(*source Admin Node*)에서 복구된 관리 노드로 Prometheus 데이터베이스를 복사하여 기간별 메트릭을 복원할 수 있습니다.

> Prometheus 데이터베이스를 복사하는 데 1시간 이상이 걸릴 수 있습니다. 소스 관리 노드에서 서비스가 중지되는 동안에는 일부 Grid Manager 기능을 사용할 수 없습니다.

1. 소스 관리 노드에 로그인합니다.
   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.
2. Source Admin Node에서 Prometheus 서비스 'Service Prometheus stop'을 중지합니다
3. 복구된 관리자 노드에서 다음 단계를 완료합니다.
   a. 복구된 관리자 노드에 로그인합니다.
      i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
      ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
      iii. 루트로 전환하려면 다음 명령을 입력합니다

iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.

b. 프로메테우스 서비스 '프로메테우스 서비스'를 중단하십시오

c. SSH 에이전트에 SSH 개인 키를 추가합니다. ssh-add를 입력합니다

d. "passwords.txt" 파일에 나열된 SSH 액세스 암호를 입력합니다.

e. 소스 관리 노드에서 복구된 관리 노드로 Prometheus 데이터베이스를 복사합니다: "/usr/local/Prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP"

f. 메시지가 표시되면 * Enter * 를 눌러 복구된 관리 노드에서 새 Prometheus 데이터베이스를 파기할지 확인합니다.

   원래 Prometheus 데이터베이스와 해당 기록 데이터가 복구된 관리 노드에 복사됩니다. 복사 작업이 완료되면 스크립트는 복구된 관리자 노드를 시작합니다. 다음 상태가 나타납니다.

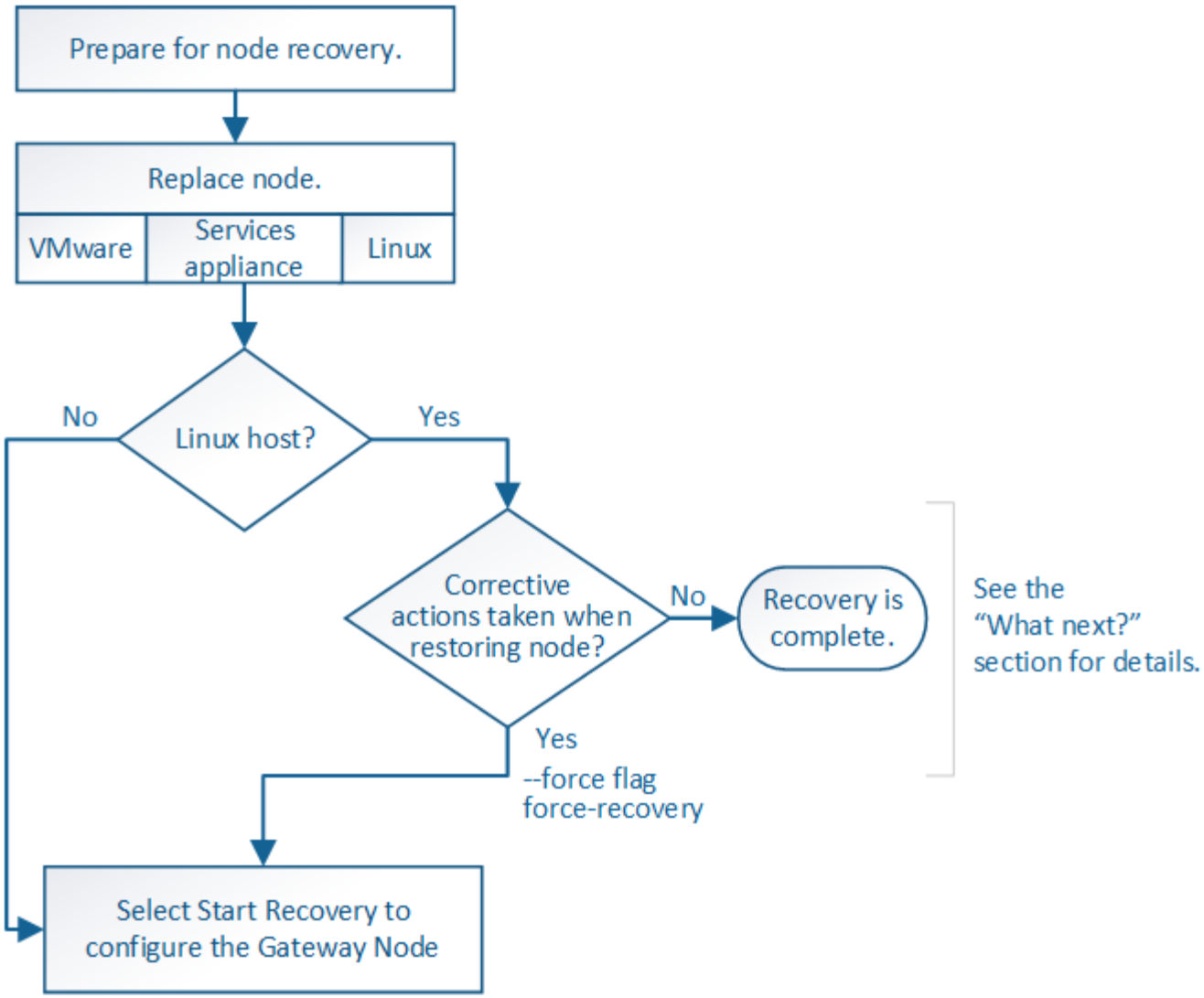
데이터베이스가 복제되어 서비스를 시작하는 중입니다

a. 다른 서버에 대한 암호 없는 액세스가 더 이상 필요하지 않으면 SSH 에이전트에서 개인 키를 제거합니다. ssh-add-D를 입력합니다

4. Source Admin Node에서 Prometheus 서비스를 다시 시작하고, Service Prometheus start를 한다

게이트웨이 노드에서 복구

게이트웨이 노드 장애를 복구하려면 일련의 작업을 정확히 완료해야 합니다.



관련 정보

SG100 및 SG1000 서비스 어플라이언스

게이트웨이 노드를 교체합니다

장애가 발생한 게이트웨이 노드를 동일한 물리적 또는 가상 하드웨어에서 실행되는 게이트웨이 노드로 대체하거나, VMware 또는 Linux 호스트에서 실행되는 게이트웨이 노드를 서비스 어플라이언스에서 호스팅되는 게이트웨이 노드로 교체할 수 있습니다.

따라야 하는 노드 교체 절차는 교체 노드에서 사용할 플랫폼에 따라 다릅니다. 모든 노드 유형에 적합한 노드 교체 절차를 완료하면 게이트웨이 노드 복구를 위한 다음 단계로 이동합니다.

교체용 플랫폼	절차를 참조하십시오
VMware	VMware 노드를 교체합니다
리눅스	Linux 노드를 교체합니다

교체용 플랫폼	절차를 참조하십시오
SG100 및 SG1000 서비스 어플라이언스	서비스 어플라이언스를 교체하십시오
더 적합하였습니다	NetApp에서 제공하는 OpenStack용 가상 머신 디스크 파일 및 스크립트는 더 이상 복구 작업을 지원하지 않습니다. OpenStack 배포에서 실행 중인 노드를 복구해야 하는 경우 Linux 운영 체제용 파일을 다운로드하십시오. 그런 다음 Linux 노드 교체 절차를 따릅니다.

Start Recovery(복구 시작**)** 를 선택하여 게이트웨이 노드를 구성합니다

게이트웨이 노드를 교체한 후 그리드 관리자에서 복구 시작 을 선택하여 새 노드를 장애가 발생한 노드에 대한 교체품으로 구성해야 합니다.

필요한 것

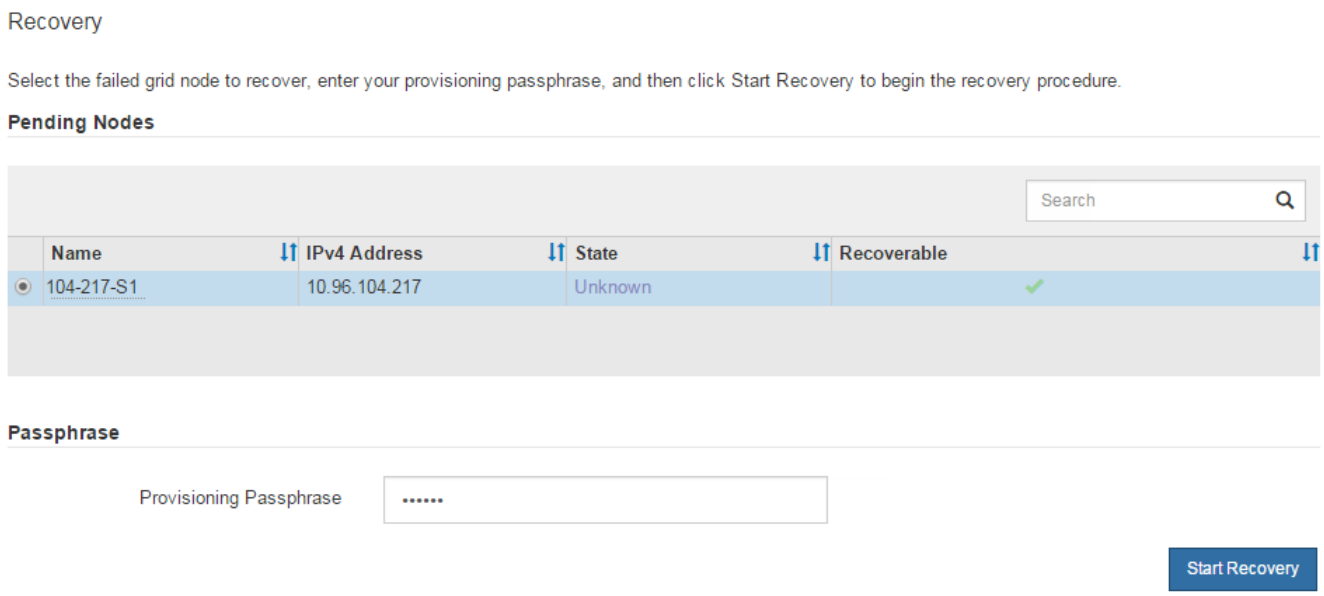
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.
- 교체 노드를 구축하고 구성해야 합니다.

단계

1. Grid Manager에서 * 유지보수 * > * 작업 * > * 복구 * 를 선택합니다.
2. Pending Nodes 목록에서 복구할 그리드 노드를 선택합니다.

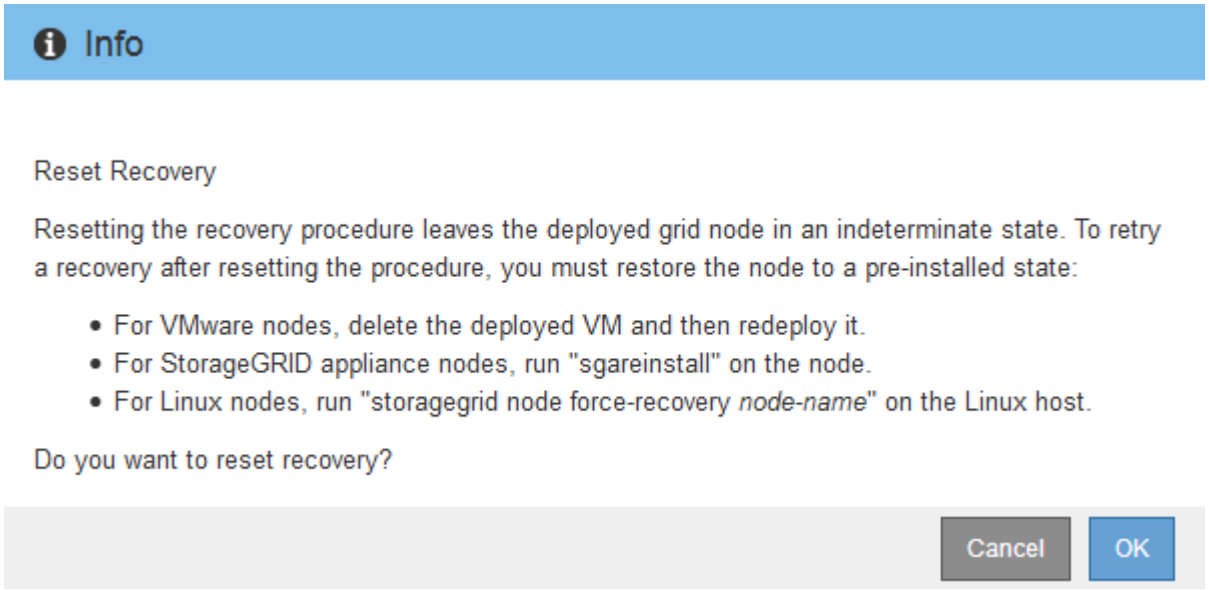
   노드가 실패한 후 목록에 나타나지만 다시 설치되고 복구 준비가 될 때까지 노드를 선택할 수 없습니다.

3. Provisioning Passphrase * 를 입력합니다.
4. 복구 시작 * 을 클릭합니다.



5. 복구 그리드 노드 테이블에서 복구 진행률을 모니터링합니다.

> 복구 절차가 실행되는 동안 * Reset * 을 클릭하여 새 복구를 시작할 수 있습니다. 프로시저를 재설정하면 노드가 결정되지 않은 상태로 남아 있음을 나타내는 정보 대화 상자가 나타납니다.



절차를 재설정한 후 복구를 재시도하려면 다음과 같이 노드를 사전 설치된 상태로 복원해야 합니다.

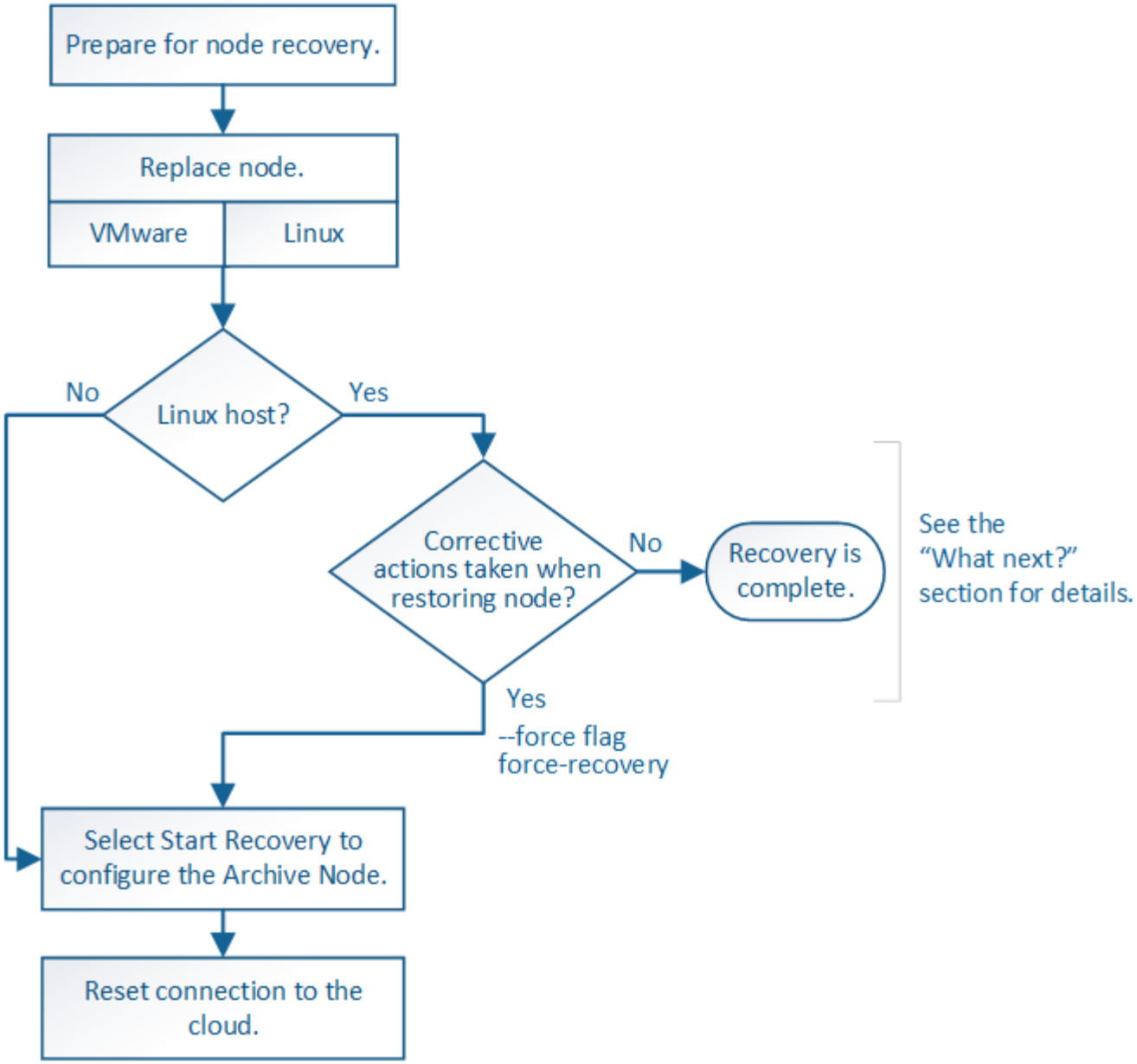
- * VMware *: 배포된 가상 그리드 노드를 삭제합니다. 그런 다음 복구를 다시 시작할 준비가 되면 노드를 다시 배포합니다.
- Linux*: Linux 호스트에서 'StorageGRID node force-recovery_node-name_' 명령을 실행하여 노드를 다시 시작합니다
- * 어플라이언스*: 절차를 재설정한 후 복구를 재시도하려면 노드에서 '설치'를 실행하여 어플라이언스 노드를 사전 설치 상태로 복원해야 합니다.

관련 정보

어플라이언스 재설치 준비(플랫폼 교체만 해당)

아카이브 노드 장애에서 복구

아카이브 노드 장애를 복구하려면 정확한 작업 시퀀스를 완료해야 합니다.



이 작업에 대해

아카이브 노드 복구는 다음 문제의 영향을 받습니다.

- ILM 정책이 단일 복사본을 복제하도록 구성된 경우

  개체의 단일 복사본을 만들기 위해 구성된 StorageGRID 시스템에서 아카이브 노드 장애가 발생하면 복구할 수 없는 데이터 손실이 발생할 수 있습니다. 오류가 발생하면 이러한 모든 개체가 손실되지만 StorageGRID 시스템을 ""정리""하고 데이터베이스에서 손실된 개체 정보를 제거하려면 복구 절차를 수행해야 합니다.

- 스토리지 노드 복구 중에 아카이브 노드 장애가 발생하는 경우

  스토리지 노드 복구의 일부로 대량 검색을 처리하는 동안 아카이브 노드에서 장애가 발생하면 아카이브 노드에서 검색된 모든 오브젝트 데이터가 스토리지 노드로 복원되도록 객체 데이터의 복제본을 처음부터 스토리지 노드로 복구하려면 이 절차를 반복해야 합니다.

아카이브 노드를 복구하려면 먼저 노드를 교체해야 합니다.

플랫폼에 대한 노드 교체 절차를 선택해야 합니다. 노드를 교체하는 단계는 모든 유형의 그리드 노드에 대해 동일합니다.

플랫폼	절차를 참조하십시오
VMware	VMware 노드를 교체합니다
리눅스	Linux 노드를 교체합니다
더 적합하였습니다	NetApp에서 제공하는 OpenStack용 가상 머신 디스크 파일 및 스크립트는 더 이상 복구 작업을 지원하지 않습니다. OpenStack 배포에서 실행 중인 노드를 복구해야 하는 경우 Linux 운영 체제용 파일을 다운로드하십시오. 그런 다음 Linux 노드 교체 절차를 따릅니다.

복구 시작 을 선택하여 아카이브 노드를 구성합니다

아카이브 노드를 교체한 후 그리드 관리자에서 복구 시작 을 선택하여 새 노드를 장애가 발생한 노드에 대한 교체품으로 구성해야 합니다.

필요한 것

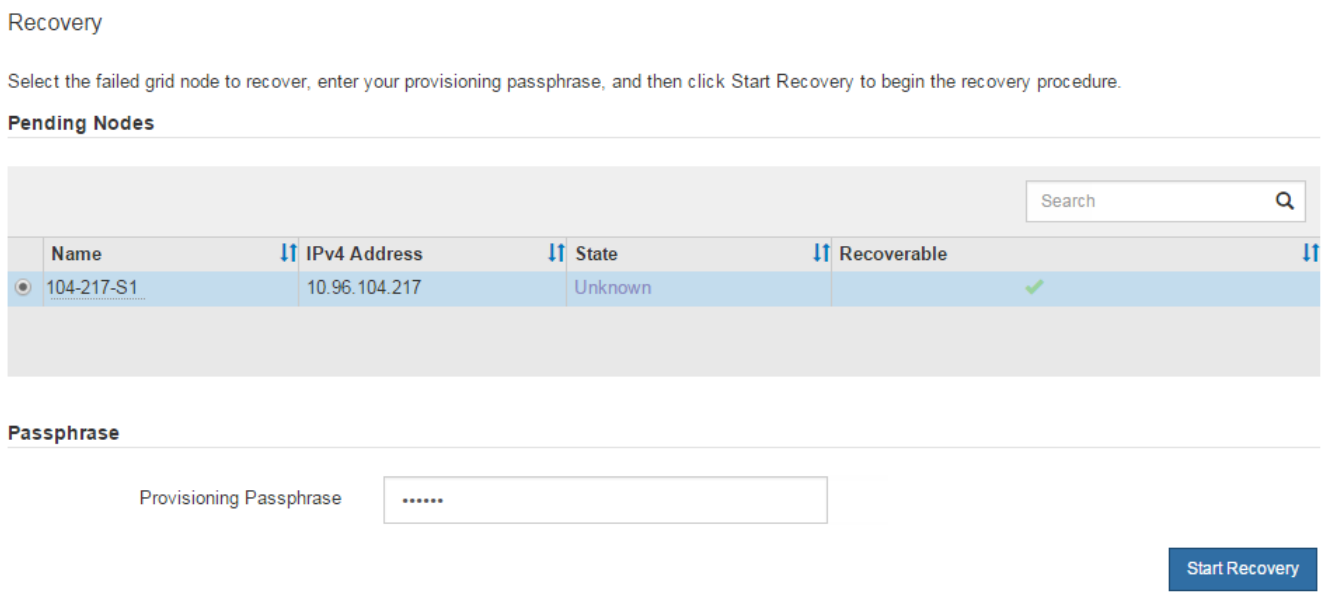
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.
- 교체 노드를 구축하고 구성해야 합니다.

단계

1. Grid Manager에서 * 유지보수 * > * 작업 * > * 복구 * 를 선택합니다.
2. Pending Nodes 목록에서 복구할 그리드 노드를 선택합니다.

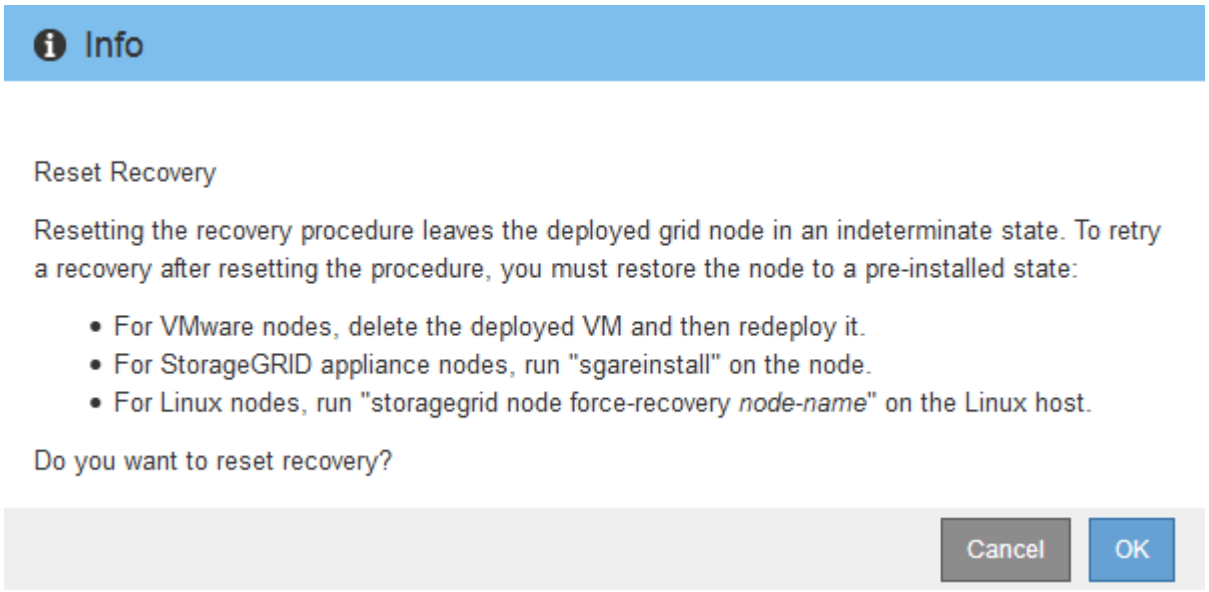
   노드가 실패한 후 목록에 나타나지만 다시 설치되고 복구 준비가 될 때까지 노드를 선택할 수 없습니다.

3. Provisioning Passphrase * 를 입력합니다.
4. 복구 시작 * 을 클릭합니다.



5. 복구 그리드 노드 테이블에서 복구 진행률을 모니터링합니다.

> 복구 절차가 실행되는 동안 * Reset * 을 클릭하여 새 복구를 시작할 수 있습니다. 프로시저를 재설정하면 노드가 결정되지 않은 상태로 남아 있음을 나타내는 정보 대화 상자가 나타납니다.



절차를 재설정한 후 복구를 재시도하려면 다음과 같이 노드를 사전 설치된 상태로 복원해야 합니다.

- * VMware *: 배포된 가상 그리드 노드를 삭제합니다. 그런 다음 복구를 다시 시작할 준비가 되면 노드를 다시 배포합니다.
- Linux*: Linux 호스트에서 'StorageGRID node force-recovery_node-name_' 명령을 실행하여 노드를 다시 시작합니다

클라우드에 아카이브 노드 연결을 재설정합니다

S3 API를 통해 클라우드를 대상으로 하는 아카이브 노드를 복구한 후 연결을 재설정하려면 구성 설정을 수정해야 합니다. 보관 노드가 객체 데이터를 검색할 수 없는 경우 아웃바운드 복제

상태(ORSU) 경보가 트리거됩니다.

> 아카이브 노드가 TSM 미들웨어를 통해 외부 스토리지에 연결되면 노드가 자동으로 재설정되므로 다시 구성할 필요가 없습니다.

필요한 것

를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node * > * ARC * > * Target * 을 선택합니다.
3. 잘못된 값을 입력하여 * 액세스 키 * 필드를 편집하고 * 변경 내용 적용 * 을 클릭합니다.
4. 올바른 값을 입력하여 * 액세스 키 * 필드를 편집하고 * 변경 내용 적용 * 을 클릭합니다.

모든 그리드 노드 유형**: VMware** 노드 교체

VMware에서 호스팅되어 장애가 발생한 StorageGRID 노드를 복구할 때는 장애가 발생한 노드를 제거하고 복구 노드를 구축해야 합니다.

필요한 것

가상 머신을 복구할 수 없으며 교체해야 합니다.

이 작업에 대해

먼저 VMware vSphere Web Client를 사용하여 장애가 발생한 그리드 노드와 연결된 가상 머신을 제거합니다. 그런 다음 새 가상 시스템을 구축할 수 있습니다.

이 절차는 그리드 노드 복구 프로세스의 한 단계일 뿐입니다. 노드 제거 및 구축 절차는 관리 노드, 스토리지 노드, 게이트웨이 노드 및 아카이브 노드를 비롯한 모든 VMware 노드에서 동일합니다.

단계

1. VMware vSphere Web Client에 로그인합니다.
2. 장애가 발생한 그리드 노드 가상 시스템으로 이동합니다.
3. 복구 노드를 구축하는 데 필요한 모든 정보를 기록해 둡니다.
   a. 가상 컴퓨터를 마우스 오른쪽 단추로 클릭하고 * 설정 편집 * 탭을 선택한 다음 사용 중인 설정을 확인합니다.
   b. 그리드 노드 네트워크 설정을 보고 기록하려면 * vApp Options * 탭을 선택합니다.
4. 장애가 발생한 그리드 노드가 스토리지 노드인 경우 데이터 저장에 사용되는 가상 하드 디스크가 손상되지 않았는지 확인하고 복구된 그리드 노드에 다시 연결할 수 있도록 보존합니다.
5. 가상 머신의 전원을 끕니다.
6. 가상 머신을 삭제하려면 * Actions * > * All vCenter Actions * > * Delete from Disk * 를 선택합니다.
7. 새 가상 시스템을 교체 노드로 구축하고 하나 이상의 StorageGRID 네트워크에 연결합니다.

   노드를 배포할 때 선택적으로 노드 포트를 재매핑하거나 CPU 또는 메모리 설정을 늘릴 수 있습니다.

> 새 노드를 구축한 후 스토리지 요구 사항에 따라 새 가상 디스크를 추가하거나, 이전에 제거한 장애가 발생한 그리드 노드에서 보존된 가상 하드 디스크를 다시 연결하거나, 둘 다 다시 연결할 수 있습니다.

지침:

VMware를 설치합니다 > StorageGRID 노드를 가상 머신으로 구축

8. 복구할 노드 유형에 따라 노드 복구 절차를 완료합니다.

노드 유형입니다	로 이동합니다
기본 관리자 노드	대체 운영 관리자 노드를 구성합니다
운영 관리자 노드가 아닌 노드	복구 시작 을 선택하여 비 기본 관리 노드를 구성합니다
게이트웨이 노드	Start Recovery(복구 시작) 를 선택하여 게이트웨이 노드를 구성합니다
스토리지 노드	복구 시작 을 선택하여 스토리지 노드를 구성합니다
아카이브 노드	복구 시작 을 선택하여 아카이브 노드를 구성합니다

모든 그리드 노드 유형**: Linux** 노드 교체

장애가 발생하여 하나 이상의 새로운 물리적 또는 가상 호스트를 구축해야 하거나 기존 호스트에 Linux를 재설치해야 하는 경우 그리드 노드를 복구하기 전에 대체 호스트를 구축 및 구성해야 합니다. 이 절차는 모든 유형의 그리드 노드에 대한 그리드 노드 복구 프로세스의 한 단계입니다.

"'Linux'는 Red Hat ® Enterprise Linux ®, Ubuntu ®, CentOS 또는 Debian ® 배포를 의미합니다. NetApp 상호 운용성 매트릭스 툴을 사용하여 지원되는 버전 목록을 확인하십시오.

이 절차는 소프트웨어 기반 스토리지 노드, 운영 또는 비운영 관리 노드, 게이트웨이 노드 또는 아카이브 노드 복구 프로세스의 한 단계로만 수행됩니다. 복구 중인 그리드 노드의 유형에 관계없이 단계가 동일합니다.

물리적 또는 가상 Linux 호스트에서 둘 이상의 그리드 노드가 호스팅되는 경우, 순서에 관계없이 그리드 노드를 복구할 수 있습니다. 그러나 운영 관리자 노드가 있는 경우 먼저 복구하면 다른 그리드 노드의 복구가 운영 관리자 노드에 연락하여 복구를 등록하려고 할 때 지연되는 것을 방지할 수 있습니다.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

새 **Linux** 호스트를 배포합니다

몇 가지 예외가 있을 경우 초기 설치 프로세스 중에 했던 것처럼 새 호스트를 준비합니다.

물리적 또는 가상 Linux 호스트를 새로 배포하거나 다시 설치하려면 Linux 운영 체제에 대한 StorageGRID 설치 지침에 따라 호스트를 준비하는 절차를 따르십시오.

이 절차에는 다음 작업을 수행하는 단계가 포함됩니다.

1. Linux를 설치합니다.
2. 호스트 네트워크를 구성합니다.
3. 호스트 스토리지를 구성합니다.
4. 컨테이너 엔진을 장착하십시오.
5. StorageGRID 호스트 서비스를 설치합니다.

> 설치 지침에서 ""StorageGRID 호스트 서비스 설치"" 작업을 완료한 후 중지합니다. "구축 그리드 노드" 작업을 시작하지 마십시오.

이 단계를 수행할 때 다음 중요 지침을 참고하십시오.

- 원래 호스트에서 사용한 것과 동일한 호스트 인터페이스 이름을 사용해야 합니다.
- 공유 스토리지를 사용하여 StorageGRID 노드를 지원하거나 의 디스크 드라이브 또는 SSD 중 일부 또는 전부를 장애 노드에서 교체 노드로 이동한 경우 원래 호스트에 있던 것과 동일한 스토리지 매핑을 다시 설정해야 합니다. 예를 들어, 설치 지침에서 권장하는 대로 '/etc/multipath.conf'에서 WWID와 별칭을 사용한 경우 교체 호스트의 '/etc/multipath.conf'에서 동일한 별칭/WWID 쌍을 사용해야 합니다.
- StorageGRID 노드에서 NetApp ONTAP 시스템에서 할당된 스토리지를 사용하는 경우 볼륨에 FabricPool 계층화 정책이 활성화되어 있지 않은지 확인합니다. StorageGRID 노드와 함께 사용되는 볼륨에 대해 FabricPool 계층화를 사용하지 않도록 설정하면 문제 해결과 스토리지 작업이 간소화됩니다.

> FabricPool를 사용하여 StorageGRID 관련 데이터를 StorageGRID 자체로 계층화하지 마십시오. StorageGRID 데이터를 StorageGRID로 다시 계층화하면 문제 해결과 운영 복잡성이 늘어납니다.

관련 정보

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

Ubuntu 또는 Debian을 설치합니다

그리드 노드를 호스트에 복구합니다

장애가 발생한 그리드 노드를 새 Linux 호스트로 복구하려면 적절한 명령을 사용하여 노드 구성 파일을 복구합니다.

새로 설치할 때 호스트에 설치할 각 그리드 노드에 대한 노드 구성 파일을 만듭니다. 그리드 노드를 대체 호스트로 복원할 때 장애가 발생한 모든 그리드 노드에 대한 노드 구성 파일을 복구하거나 교체합니다.

이전 호스트에서 보존한 블록 스토리지 볼륨이 있는 경우 추가 복구 절차를 수행해야 할 수 있습니다. 이 섹션의 명령을 사용하면 필요한 추가 절차를 결정할 수 있습니다.

단계

- 그리드 노드 복원 및 검증
- StorageGRID 호스트 서비스를 시작합니다
- 정상적으로 시작하지 못한 노드를 복구합니다

장애가 발생한 그리드 노드에 대해 그리드 구성 파일을 복원한 다음 그리드 구성 파일의 유효성을 검사하고 오류를 해결해야 합니다.

이 작업에 대해

이전 호스트의 장애로 인해 '/var/local' 볼륨이 손실되지 않은 경우 호스트에 있어야 하는 모든 그리드 노드를 가져올 수 있습니다. 예를 들어, Linux 운영 체제의 StorageGRID 설치 지침에 설명된 대로 StorageGRID 시스템 데이터 볼륨에 공유 스토리지를 사용한 경우 '/var/local' 볼륨이 계속 존재할 수 있습니다. 노드를 가져오면 해당 노드 구성 파일이 호스트에 복구됩니다.

누락된 노드를 가져올 수 없는 경우 그리드 구성 파일을 다시 생성해야 합니다.

그런 다음 그리드 구성 파일을 확인하고 StorageGRID를 다시 시작하기 전에 발생할 수 있는 네트워킹 또는 스토리지 문제를 해결해야 합니다. 노드에 대한 구성 파일을 다시 생성할 때 복구 중인 노드에 사용된 교체 노드에 대해 동일한 이름을 사용해야 합니다.

노드의 '/var/local' 볼륨 위치에 대한 자세한 내용은 설치 지침을 참조하십시오.

단계

1. 복구된 호스트의 명령줄에 현재 구성된 모든 StorageGRID 그리드 노드('SUDO StorageGRID node list')를 나열합니다

   그리드 노드가 구성되어 있지 않으면 출력이 없습니다. 일부 그리드 노드가 구성된 경우 다음과 같은 형식으로 출력이 예상됩니다.

   ```
   Name                Metadata-Volume
   ==================================================================
   dc1-adm1            /dev/mapper/sgws-adm1-var-local
   dc1-gw1             /dev/mapper/sgws-gw1-var-local
   dc1-sn1             /dev/mapper/sgws-sn1-var-local
   dc1-arc1            /dev/mapper/sgws-arc1-var-local
   ```

   호스트에서 구성해야 하는 일부 또는 모든 그리드 노드가 목록에 없는 경우 누락된 그리드 노드를 복원해야 합니다.

2. '/var/local' 볼륨이 있는 그리드 노드를 가져오려면:

   a. 가져올 각 노드에 대해 "SUDO StorageGRID node import node -var-local-volume-path'를 실행합니다

      StorageGRID node import 명령은 대상 노드가 마지막으로 실행된 호스트에서 완전히 종료된 경우에만 성공한다. 그렇지 않으면 다음과 유사한 오류가 발생합니다.

      "이 노드(*node-name*)는 다른 호스트(UUID host-uuuid)가 소유한 것으로 보입니다.

   수입은 안전하다고 확신한다면 -force 플래그를 사용하세요

   a. 다른 호스트가 소유하는 노드에 대한 오류가 표시되는 경우 '--force' 플래그를 사용하여 명령을 다시 실행하여 가져오기를 완료합니다. "SUDO StorageGRID --force node import node -var-local-volume-path'

'--force' 플래그를 사용하여 가져온 모든 노드는 에 설명된 대로 그리드에 다시 참가하기 전에 추가 복구 단계가 필요합니다 다음 단계: 필요한 경우 추가 복구 단계를 수행합니다.

3. '/var/local' 볼륨이 없는 그리드 노드의 경우 노드의 구성 파일을 다시 생성하여 호스트에 복구합니다.

   설치 지침에 있는 "'노드 구성 파일 작성'의 지침을 따르십시오.

   노드에 대한 구성 파일을 다시 생성할 때 복구 중인 노드에 사용된 교체 노드에 대해 동일한 이름을 사용해야 합니다. Linux 배포의 경우 구성 파일 이름에 노드 이름이 포함되어 있는지 확인합니다. 가능하면 동일한 네트워크 인터페이스, 블록 장치 매핑 및 IP 주소를 사용해야 합니다. 이러한 관행은 복구 중에 노드로 복사해야 하는 데이터 양을 최소화하여 복구 속도가 크게 향상되도록 합니다(경우에 따라 몇 주가 아닌 몇 분).

   노드에 대한 구성 파일을 다시 생성할 때 "BLOCK_DEVICE_"로 시작하는 구성 변수의 값으로 새 블록 디바이스(StorageGRID 노드에서 이전에 사용하지 않은 디바이스)를 사용하는 경우 의 모든 지침을 따라야 합니다 누락된 블록 장치 오류를 수정합니다.

4. 복구된 호스트에서 다음 명령을 실행하여 모든 StorageGRID 노드를 나열합니다.

   'SUDO StorageGRID node list

5. StorageGRID 노드 목록 출력에 이름이 표시된 각 그리드 노드에 대한 노드 구성 파일의 유효성을 검사합니다.

   'SUDO StorageGRID node validate_node-name_'

   StorageGRID 호스트 서비스를 시작하기 전에 오류 또는 경고를 해결해야 합니다. 다음 섹션에서는 복구 중에 특별한 의미가 있을 수 있는 오류에 대해 자세히 설명합니다.

관련 정보

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

Ubuntu 또는 Debian을 설치합니다

누락된 네트워크 인터페이스 오류를 수정합니다

누락된 네트워크 인터페이스 오류를 수정합니다

호스트 네트워크가 올바르게 구성되지 않았거나 이름의 철자가 틀린 경우 StorageGRID가 '/etc/StorageGrid/nodes/*node-name*.conf' 파일에 지정된 매핑을 확인할 때 오류가 발생합니다.

이 패턴과 일치하는 오류 또는 경고가 나타날 수 있습니다.

node_node-name_…에 대한 구성 파일 '/etc/StorageGrid/nodes/*node-name*.conf'를 확인하는 중입니다 'ERROR:_NODE-NAME_:GRID_NETWORK_TARGET=*HOST-INTERFACE-NAME*""*NODE-NAME*: Interface'*HOST-INTERFACE-NAME*'이(가) 없습니다.

그리드 네트워크, 관리 네트워크 또는 클라이언트 네트워크에 대한 오류가 보고될 수 있습니다. 이 오류는 '/etc/StorageGrid/nodes/*node-name*.conf' 파일이 표시된 StorageGRID 네트워크를 '*host-interface-name*'이라는 호스트 인터페이스에 매핑하지만 현재 호스트에 해당 이름의 인터페이스가 없음을 의미합니다.

이 오류가 발생하면 의 단계를 완료했는지 확인합니다 새 Linux 호스트를 배포합니다. 원래 호스트에서 사용된 모든 호스트 인터페이스에 동일한 이름을 사용합니다.

노드 구성 파일과 일치하도록 호스트 인터페이스의 이름을 지정할 수 없는 경우 노드 구성 파일을 편집하고 GRID_NETWORK_TARGET, ADMIN_NETWORK_TARGET 또는 CLIENT_NETWORK_TARGET의 값을 변경하여 기존 호스트 인터페이스와 일치시킬 수 있습니다.

호스트 인터페이스가 적절한 물리적 네트워크 포트 또는 VLAN에 대한 액세스를 제공하고 인터페이스가 Bond 또는 Bridge 장치를 직접 참조하지 않는지 확인합니다. 호스트의 연결 디바이스 위에 VLAN(또는 기타 가상 인터페이스)을 구성하거나 브리지 및 가상 이더넷(veth) 쌍을 사용해야 합니다.

누락된 블록 장치 오류를 수정합니다

시스템은 복구된 각 노드가 유효한 블록 디바이스 특수 파일 또는 블록 디바이스 특수 파일에 대한 유효한 소프트링크에 매핑되는지 확인합니다. StorageGRID가 '/etc/StorageGrid/nodes/*node-name*.conf' 파일에서 잘못된 매핑을 찾으면 누락된 블록 디바이스 오류가 표시됩니다.

이 패턴과 일치하는 오류가 발생하는 경우:

"node_node-name_…에 대한 구성 파일 /etc/StorageGrid/nodes/*node-name*.conf 확인 중. "error:_node-name_: block_device_purpose=*path-name*""*node-name*:_path-name_not exist.

즉, '/etc/StorageGrid/nodes/*node-name*.conf'는 Linux 파일 시스템에서 지정된 경로 이름에 사용하도록 _node-name_에 사용되는 블록 디바이스를 매핑하지만 해당 위치에 유효한 블록 디바이스 특수 파일 또는 블록 디바이스 특수 파일에 대한 소프트링크가 없음을 의미합니다.

의 단계를 완료했는지 확인합니다 새 Linux 호스트를 배포합니다. 원래 호스트에서 사용된 것과 동일한 영구 디바이스 이름을 모든 블록 디바이스에 사용합니다.

누락된 블록 디바이스 특수 파일을 복구하거나 다시 생성할 수 없는 경우 적절한 크기 및 스토리지 범주의 새 블록 디바이스를 할당하고 노드 구성 파일을 편집하여 새 블록 디바이스 특수 파일을 가리키도록 block_device_purpose 값을 변경할 수 있습니다.

Linux 운영 체제 설치 지침의 "스토리지 요구 사항" 섹션에 있는 표에서 적절한 크기와 스토리지 범주를 확인하십시오. 블록 디바이스 교체를 진행하기 전에 ""호스트 스토리지 구성""의 권장 사항을 검토하십시오.

> 장애가 발생한 호스트에서 원래 블록 디바이스가 손실되었기 때문에 "BLOCK_DEVICE_"로 시작하는 구성 파일 변수에 대해 새 블록 스토리지 디바이스를 제공해야 하는 경우 추가 복구 절차를 시도하기 전에 새 블록 디바이스의 포맷이 해제되었는지 확인하십시오. 공유 스토리지를 사용 중이고 새 볼륨을 생성한 경우 새 블록 디바이스의 포맷이 해제됩니다. 확실하지 않은 경우 새 블록 스토리지 디바이스 특수 파일에 대해 다음 명령을 실행합니다.

주의:

새 블록 스토리지 디바이스에 대해서만 다음 명령을 실행합니다. 블록 스토리지에 복구 중인 노드에 대한 유효한 데이터가 계속 포함되어 있다고 생각되면 디바이스의 모든 데이터가 손실되므로 이 명령을 실행하지 마십시오.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

관련 정보

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

Ubuntu 또는 Debian을 설치합니다

StorageGRID 호스트 서비스를 시작합니다

StorageGRID 노드를 시작하고 호스트를 재부팅한 후 다시 시작하려면 StorageGRID 호스트 서비스를 설정하고 시작해야 합니다.

1. 각 호스트에서 다음 명령을 실행합니다.

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. 다음 명령을 실행하여 구축이 진행되고 있는지 확인합니다.

   'SUDO StorageGRID NODE STATUS_NODE-NAME_'

   실행 안 됨 또는 중지됨 상태를 반환하는 노드에 대해 다음 명령을 실행합니다.

   'SUDO StorageGRID NODE START_NODE-NAME_'

3. 이전에 StorageGRID 호스트 서비스를 설정 및 시작한 경우(또는 서비스가 활성화 및 시작되었는지 확실하지 않은 경우) 다음 명령을 실행합니다.

```
sudo systemctl reload-or-restart storagegrid
```

정상적으로 시작하지 못한 노드를 복구합니다

StorageGRID 노드가 그리드에 정상적으로 다시 참가하지 않고 복구 가능으로 표시되지 않으면 손상된 것일 수 있습니다. 노드를 복구 모드로 강제 전환할 수 있습니다.

노드를 복구 모드로 전환하려면 다음을 수행합니다.

'SUDO StorageGRID node force-recovery_node-name_'

> 이 명령을 실행하기 전에 노드의 네트워크 구성이 올바른지 확인하십시오. 잘못된 네트워크 인터페이스 매핑이나 잘못된 그리드 네트워크 IP 주소 또는 게이트웨이로 인해 그리드에 다시 연결되지 않았을 수 있습니다.

> 'StorageGRID node force-recovery_node-name_' 명령어를 실행한 후, _node-name_에 대해 추가 복구 단계를 수행해야 합니다.

관련 정보

다음 단계: 필요한 경우 추가 복구 단계를 수행합니다

교체 호스트에서 StorageGRID 노드를 실행하기 위해 수행한 작업에 따라 각 노드에 대해 추가 복구 단계를 수행해야 할 수도 있습니다.

노드 복구는 Linux 호스트를 교체하거나 장애가 발생한 그리드 노드를 새 호스트로 복구하는 동안 수정 조치를 취할 필요가 없는 경우에 완료됩니다.

수정 조치 및 다음 단계

노드 교체 중에 다음 수정 조치 중 하나를 수행해야 할 수 있습니다.

- 노드를 가져오려면 '--force' 플래그를 사용해야 했습니다.
- 모든 "<목적>"에서 "block_device_<purpose>" 구성 파일 변수의 값은 호스트 장애 전에 했던 것과 동일한 데이터가 포함되지 않은 블록 디바이스를 나타냅니다.
- 노드에 대해 StorageGRID node force-recovery_node-name _ 을(를) 실행했습니다.
- 새 차단 장치를 추가했습니다.

이러한 수정 조치 * 중 * 하나를 수행한 경우 추가 복구 단계를 수행해야 합니다.

복구 유형입니다	다음 단계
기본 관리자 노드	대체 운영 관리자 노드를 구성합니다
운영 관리자 노드가 아닌 노드	복구 시작 을 선택하여 비 기본 관리 노드를 구성합니다
게이트웨이 노드	Start Recovery(복구 시작) 를 선택하여 게이트웨이 노드를 구성합니다
아카이브 노드	복구 시작 을 선택하여 아카이브 노드를 구성합니다
스토리지 노드(소프트웨어 기반): • 노드를 가져오기 위해 '--force' 플래그를 사용하거나 StorageGRID node force-recovery_node-name_'을(를) 실행한 경우 • 전체 노드를 다시 설치해야 하거나 /var/local을 복원해야 하는 경우	복구 시작 을 선택하여 스토리지 노드를 구성합니다
스토리지 노드(소프트웨어 기반): • 새 차단 장치를 추가한 경우 • 어떤 "<목적>"에 대해서도 "block_device_<목적>" 구성 파일 변수의 값은 호스트 장애 전에 했던 것과 동일한 데이터가 포함되지 않은 블록 디바이스를 의미합니다.	시스템 드라이브가 손상되지 않은 스토리지 볼륨 장애로부터 복구합니다

장애가 발생한 노드를 서비스 어플라이언스로 교체합니다

SG100 또는 SG1000 서비스 어플라이언스를 사용하여 장애가 발생한 게이트웨이 노드, 장애가 발생한 비 기본 관리 노드 또는 VMware, Linux 호스트 또는 서비스 어플라이언스에서 호스팅되는 실패한 운영 관리 노드를 복구할 수 있습니다. 이 절차는 그리드 노드 복구 절차의 한 단계입니다.

필요한 것

- 다음 상황 중 하나가 사실임을 확인해야 합니다.
  - 노드를 호스팅하는 가상 머신을 복구할 수 없습니다.
  - 그리드 노드의 물리적 또는 가상 Linux 호스트에 장애가 발생하여 교체해야 합니다.
  - 그리드 노드를 호스팅하는 서비스 어플라이언스를 교체해야 합니다.
- StorageGRID 어플라이언스 설치 관리자 버전 확인 및 업그레이드를 위한 하드웨어 설치 및 유지 보수에 설명된 대로 서비스 어플라이언스의 StorageGRID 어플라이언스 설치 관리자 버전이 StorageGRID 시스템의 소프트웨어 버전과 일치하는지 확인해야 합니다.

  SG100 및 SG1000 서비스 어플라이언스

> SG100과 SG1000 서비스 어플라이언스를 같은 사이트에 배포하지 마십시오. 성능을 예측할 수 없습니다.

이 작업에 대해

다음과 같은 경우 SG100 또는 SG1000 서비스 어플라이언스를 사용하여 장애가 발생한 그리드 노드를 복구할 수 있습니다.

- 장애가 발생한 노드가 VMware 또는 Linux에서 호스팅됨(플랫폼 변경)
- 장애가 발생한 노드가 서비스 어플라이언스에서 호스팅됨(플랫폼 교체)

서비스 어플라이언스 설치(플랫폼 변경 전용)

VMware 또는 Linux 호스트에서 호스팅되는 장애가 발생한 그리드 노드를 복구하는 중에 교체 노드에 SG100 또는 SG1000 서비스 어플라이언스를 사용하는 경우, 먼저 장애가 발생한 노드와 동일한 노드 이름을 사용하여 새 어플라이언스 하드웨어를 설치해야 합니다.

장애가 발생한 노드에 대한 다음 정보가 있어야 합니다.

- * 노드 이름 *: 서비스 어플라이언스는 장애가 발생한 노드와 동일한 노드 이름을 사용하여 설치해야 합니다.
- * IP 주소 *: 서비스 어플라이언스에 장애가 발생한 노드와 동일한 IP 주소를 할당할 수 있습니다. 이는 기본 설정 옵션이며, 각 네트워크에서 사용되지 않은 새 IP 주소를 선택할 수 있습니다.

VMware 또는 Linux에서 호스팅되어 서비스 어플라이언스에서 호스팅되는 노드로 대체되는 장애가 발생한 노드를 복구하는 경우에만 이 절차를 수행하십시오.

1. 새 SG100 또는 SG1000 서비스 어플라이언스 설치 지침을 따르십시오.
2. 노드 이름을 묻는 메시지가 표시되면 장애가 발생한 노드의 노드 이름을 사용합니다.

관련 정보

SG100 및 SG1000 서비스 어플라이언스

재설치 준비를 위한 어플라이언스 재설치 준비(플랫폼 교체만 해당)

서비스 어플라이언스에서 호스팅되는 그리드 노드를 복구할 때는 먼저 StorageGRID 소프트웨어 재설치를 위한 어플라이언스를 준비해야 합니다.

서비스 어플라이언스에서 호스팅되는 장애가 발생한 노드를 교체하는 경우에만 이 절차를 수행합니다. 장애가 발생한 노드가 원래 VMware 또는 Linux 호스트에서 호스팅되는 경우 이 단계를 수행하지 마십시오.

1. 장애가 발생한 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. StorageGRID 소프트웨어 설치를 위해 어플라이언스를 준비합니다. '설치'를 입력합니다

3. 계속하라는 메시지가 나타나면 y를 입력합니다

   어플라이언스가 재부팅되고 SSH 세션이 종료됩니다. StorageGRID 어플라이언스 설치 프로그램을 사용할 수 있게 되기까지 일반적으로 5분이 걸리지만 경우에 따라 최대 30분까지 기다려야 할 수도 있습니다.

   서비스 어플라이언스가 재설정되고 그리드 노드의 데이터에 더 이상 액세스할 수 없습니다. 원래 설치 프로세스 중에 구성된 IP 주소는 그대로 유지되지만 절차가 완료되면 이를 확인하는 것이 좋습니다.

   'Sareinstall' 명령을 실행하면 StorageGRID로 프로비저닝된 모든 계정, 암호 및 SSH 키가 제거되고 새 호스트 키가 생성됩니다.

서비스 어플라이언스에서 소프트웨어 설치를 시작합니다

SG100 또는 SG1000 서비스 어플라이언스에 게이트웨이 노드 또는 관리 노드를 설치하려면 어플라이언스에 포함된 StorageGRID 어플라이언스 설치 프로그램을 사용합니다.

필요한 것

- 어플라이언스는 랙에 설치하고 네트워크에 연결한 후 전원을 켜야 합니다.
- StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스에 대해 네트워크 링크 및 IP 주소를 구성해야 합니다.
- 게이트웨이 노드 또는 비 기본 관리 노드를 설치하는 경우 StorageGRID 그리드에 대한 기본 관리 노드의 IP 주소를 알 수 있습니다.
- StorageGRID 어플라이언스 설치 프로그램의 IP 구성 페이지에 나열된 모든 그리드 네트워크 서브넷은 기본 관리 노드의 그리드 네트워크 서브넷 목록에 정의되어 있어야 합니다.

이러한 필수 작업을 완료하기 위한 지침은 SG100 또는 SG1000 서비스 어플라이언스의 설치 및 유지보수 지침을 참조하십시오.

- 을(를) 사용해야 합니다 지원되는 웹 브라우저.
- 어플라이언스에 할당된 IP 주소 중 하나를 알아야 합니다. 관리 네트워크, 그리드 네트워크 또는 클라이언트 네트워크의 IP 주소를 사용할 수 있습니다.
- 기본 관리자 노드를 설치하는 경우 이 버전의 StorageGRID에 대한 Ubuntu 또는 Debian 설치 파일을 사용할 수 있습니다.

> 최신 버전의 StorageGRID 소프트웨어는 제조 과정에서 서비스 어플라이언스에 사전 로드되어 있습니다. 사전 로드된 소프트웨어 버전이 StorageGRID 배포에서 사용 중인 버전과 일치하면 설치 파일이 필요하지 않습니다.

이 작업에 대해

SG100 또는 SG1000 서비스 어플라이언스에 StorageGRID 소프트웨어를 설치하려면:

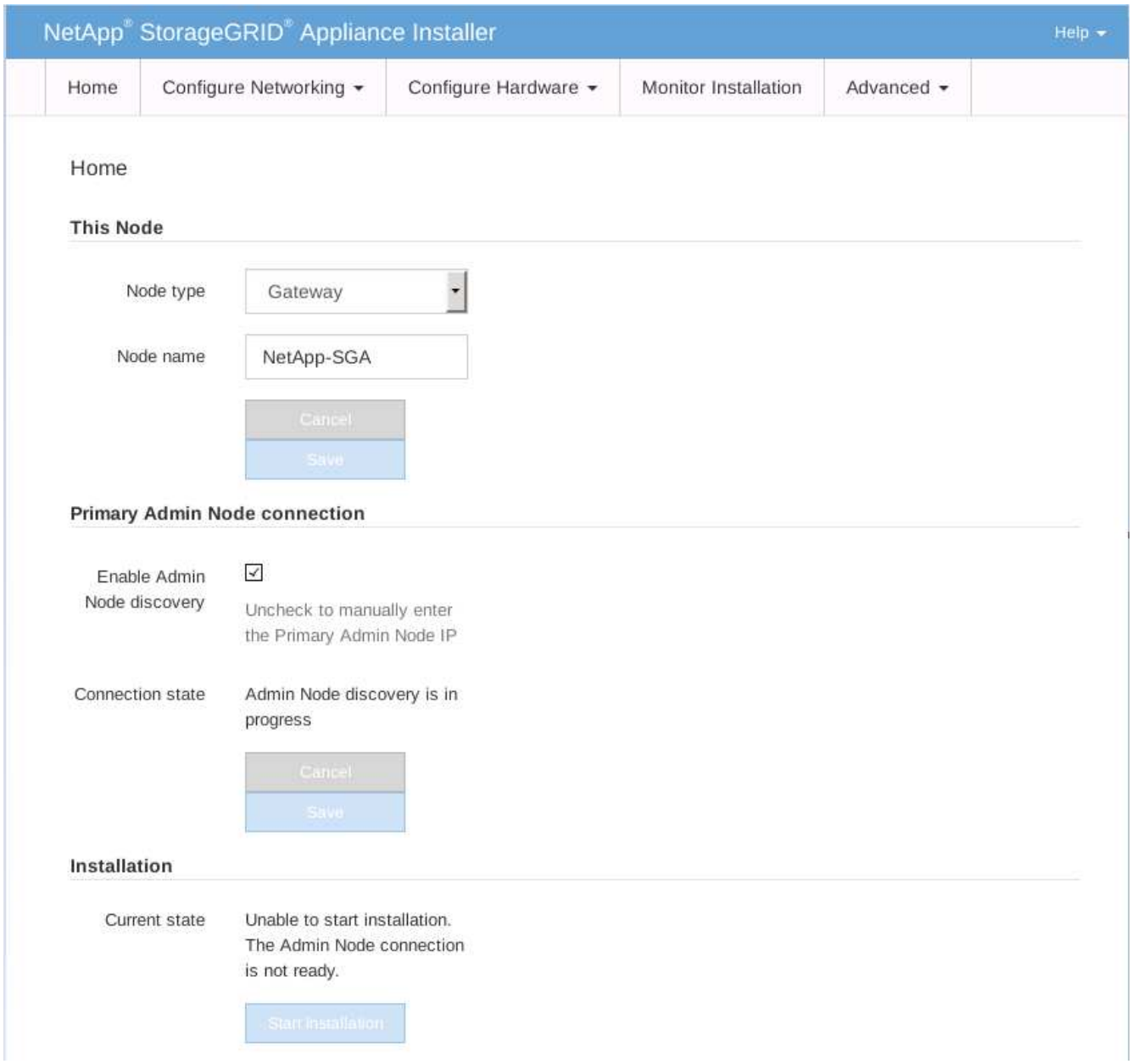
- 기본 관리 노드의 경우 노드 이름을 지정한 다음 적절한 소프트웨어 패키지를 업로드합니다(필요한 경우).
- 비 기본 관리 노드 또는 게이트웨이 노드의 경우 기본 관리 노드의 IP 주소와 노드 이름을 지정하거나 확인합니다.
- 설치를 시작하고 볼륨이 구성되고 소프트웨어가 설치될 때까지 기다립니다.
- 프로세스가 중간에 진행되면 설치가 일시 중지됩니다. 설치를 다시 시작하려면 그리드 관리자에 로그인하고 보류 중인 노드를 장애 발생 노드의 대체용으로 구성해야 합니다.
- 노드를 구성한 후에는 어플라이언스 설치 프로세스가 완료되고 어플라이언스가 재부팅됩니다.

단계

1. 브라우저를 열고 SG100 또는 SG1000 서비스 어플라이언스의 IP 주소 중 하나를 입력합니다.

   (https://Controller_IP:8443`)

   StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.



2. 기본 관리 노드를 설치하려면:

   a. 이 노드 섹션의 * 노드 유형 * 에서 * 기본 관리자 * 를 선택합니다.

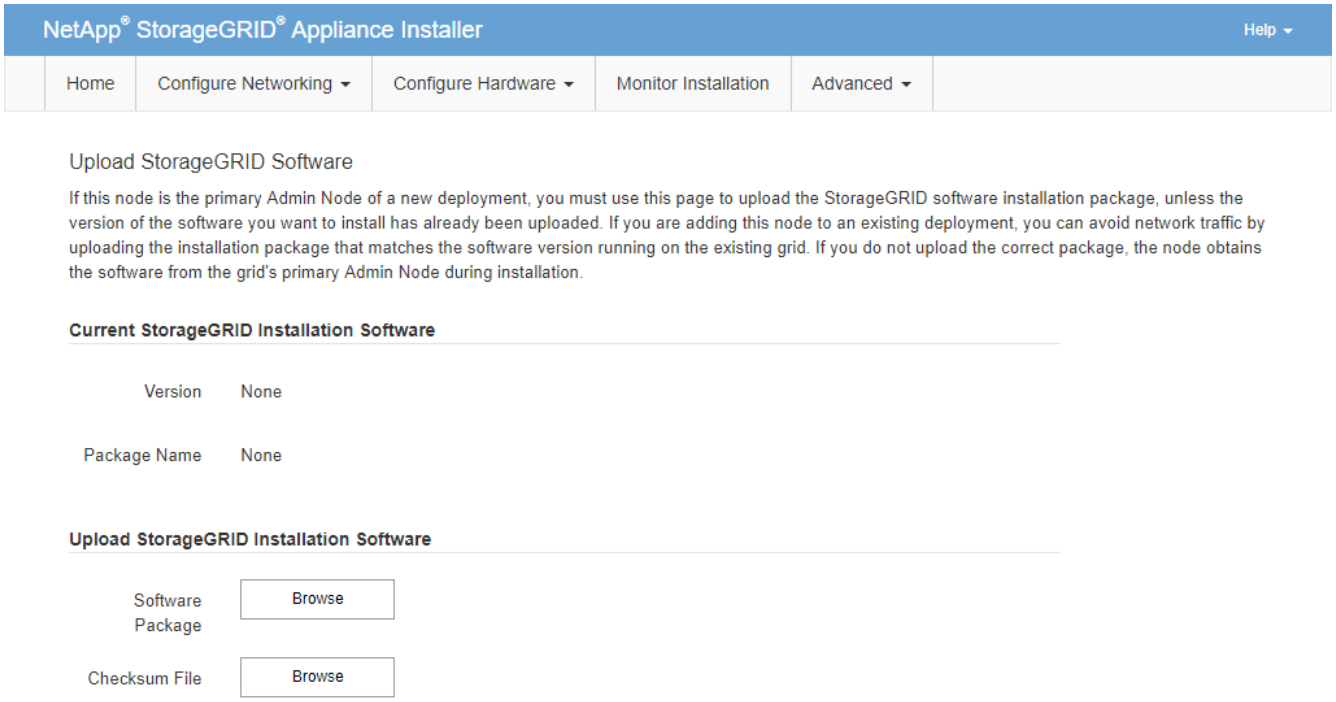
   b. Node Name * 필드에 복구 중인 노드에 사용된 이름과 동일한 이름을 입력하고 * Save * 를 클릭합니다.

   c. 설치 섹션에서 현재 상태에 나열된 소프트웨어 버전을 확인합니다

      설치 준비가 완료된 소프트웨어 버전이 올바른 경우 로 건너뜁니다 설치 단계.

   d. 다른 버전의 소프트웨어를 업로드하려면 * 고급 * 메뉴에서 * StorageGRID 소프트웨어 업로드 * 를 선택합니다.

      StorageGRID 소프트웨어 업로드 페이지가 나타납니다.



a. StorageGRID 소프트웨어용 * 소프트웨어 패키지 * 및 * 체크섬 파일 * 을 업로드하려면 * 찾아보기 * 를 클릭합니다.

   파일을 선택하면 파일이 자동으로 업로드됩니다.

b. StorageGRID 어플라이언스 설치 관리자 홈 페이지로 돌아가려면 * 홈 * 을 클릭합니다.

3. 게이트웨이 노드 또는 비 기본 관리 노드를 설치하려면:

a. 복원하는 노드 유형에 따라 이 노드 섹션에서 * 노드 유형 * 에 대해 * 게이트웨이 * 또는 * 비기본 관리자 * 를 선택합니다.

b. Node Name * 필드에 복구 중인 노드에 사용된 이름과 동일한 이름을 입력하고 * Save * 를 클릭합니다.

c. 기본 관리 노드 연결 섹션에서 기본 관리 노드의 IP 주소를 지정해야 하는지 여부를 확인합니다.

   StorageGRID 어플라이언스 설치 관리자는 기본 관리 노드 또는 admin_IP가 구성된 다른 그리드 노드가 동일한 서브넷에 있다고 가정하여 이 IP 주소를 자동으로 검색할 수 있습니다.

d. 이 IP 주소가 표시되지 않거나 변경해야 하는 경우 주소를 지정합니다.

옵션을 선택합니다	설명
수동 IP 입력	a. 관리자 노드 검색 사용 * 확인란의 선택을 취소합니다. b. IP 주소를 수동으로 입력합니다. c. 저장 * 을 클릭합니다. d. 새 IP 주소의 연결 상태가 "다시 준비"가 될 때까지 기다립니다.

옵션을 선택합니다	설명
연결된 모든 운영 관리 노드의 자동 검색	a. 관리자 노드 검색 사용 * 확인란을 선택합니다. b. 검색된 IP 주소 목록에서 이 서비스 어플라이언스를 배포할 그리드의 기본 관리 노드를 선택합니다. c. 저장 * 을 클릭합니다. d. 새 IP 주소의 연결 상태가 "다시 준비"가 될 때까지 기다립니다.

4. 설치 섹션에서 현재 상태가 노드 이름 설치를 시작할 준비가 되었으며 * 설치 시작 * 버튼이 활성화되었는지 확인합니다.

   설치 시작 * 버튼이 활성화되지 않은 경우 네트워크 구성 또는 포트 설정을 변경해야 할 수 있습니다. 자세한 내용은 제품의 설치 및 유지보수 지침을 참조하십시오.

5. StorageGRID 어플라이언스 설치 관리자 홈 페이지에서 * 설치 시작 * 을 클릭합니다.

   현재 상태가 ""설치 진행 중""으로 변경되고 모니터 설치 페이지가 표시됩니다.

   > 모니터 설치 페이지에 수동으로 액세스해야 하는 경우 메뉴 모음에서 * 모니터 설치 * 를 클릭합니다.

관련 정보

SG100 및 SG1000 서비스 어플라이언스

서비스 어플라이언스 설치를 모니터링합니다

StorageGRID 어플라이언스 설치 프로그램은 설치가 완료될 때까지 상태를 제공합니다. 소프트웨어 설치가 완료되면 어플라이언스가 재부팅됩니다.

1. 설치 진행률을 모니터링하려면 메뉴 표시줄에서 * 모니터 설치 * 를 클릭합니다.

   Monitor Installation(모니터 설치) 페이지에 설치 진행률이 표시됩니다.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Running

Step	Progress	Status
Obtain installer binaries		Complete
Configure installer		Complete
Install OS		Installer VM running

3. Install StorageGRID	Pending
4. Finalize installation	Pending

파란색 상태 표시줄은 현재 진행 중인 작업을 나타냅니다. 녹색 상태 표시줄은 성공적으로 완료된 작업을 나타냅니다.

> 설치 프로그램은 이전 설치에서 완료된 작업이 다시 실행되지 않도록 합니다. 설치를 다시 실행할 경우 다시 실행할 필요가 없는 작업은 녹색 상태 표시줄과 "중단" 상태로 표시됩니다.

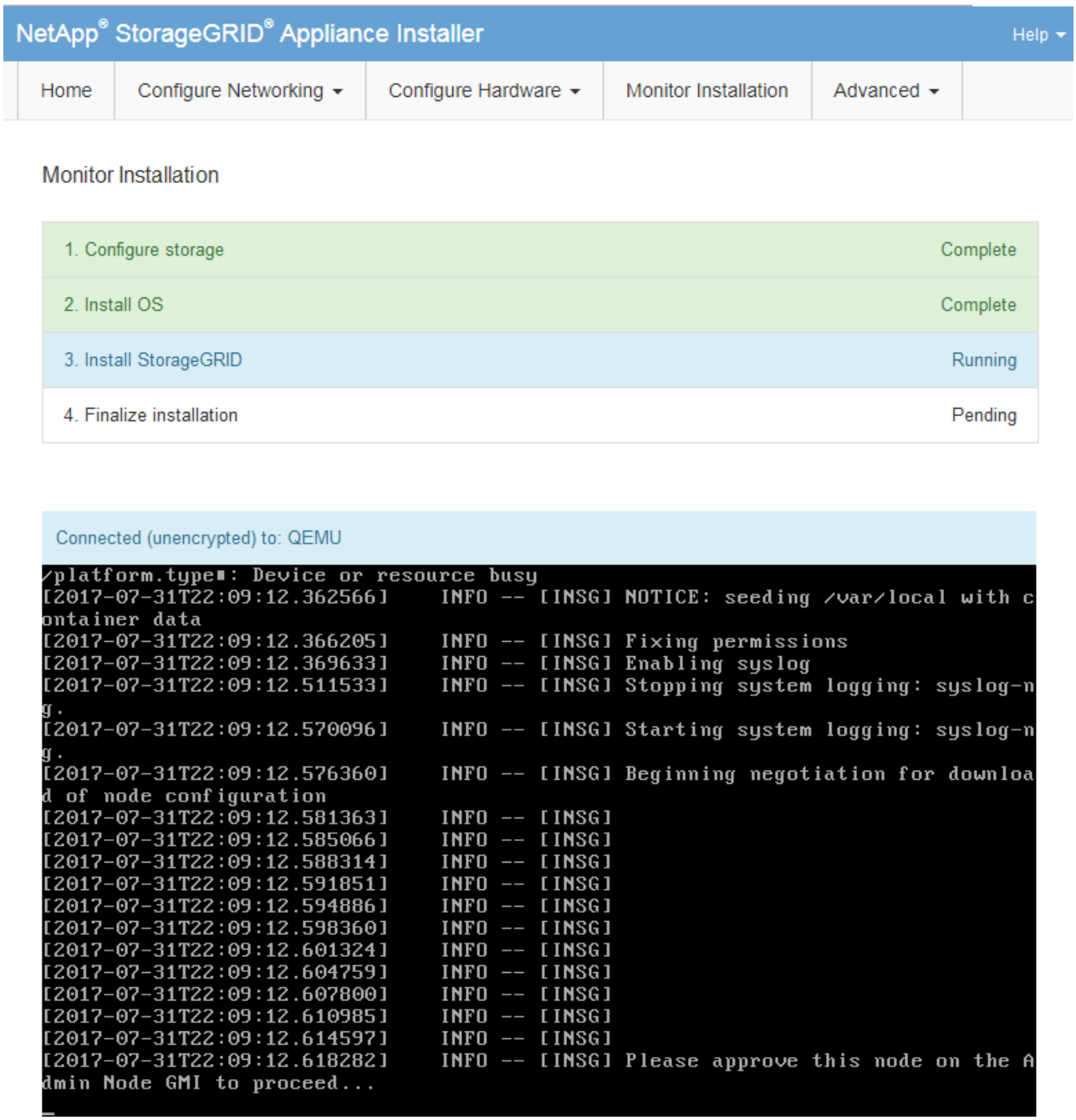
2. 처음 두 설치 단계의 진행 상황을 검토합니다.
   - * 1. 스토리지 구성 *

     이 단계에서 설치 관리자는 드라이브에서 기존 구성을 지우고 호스트 설정을 구성합니다.

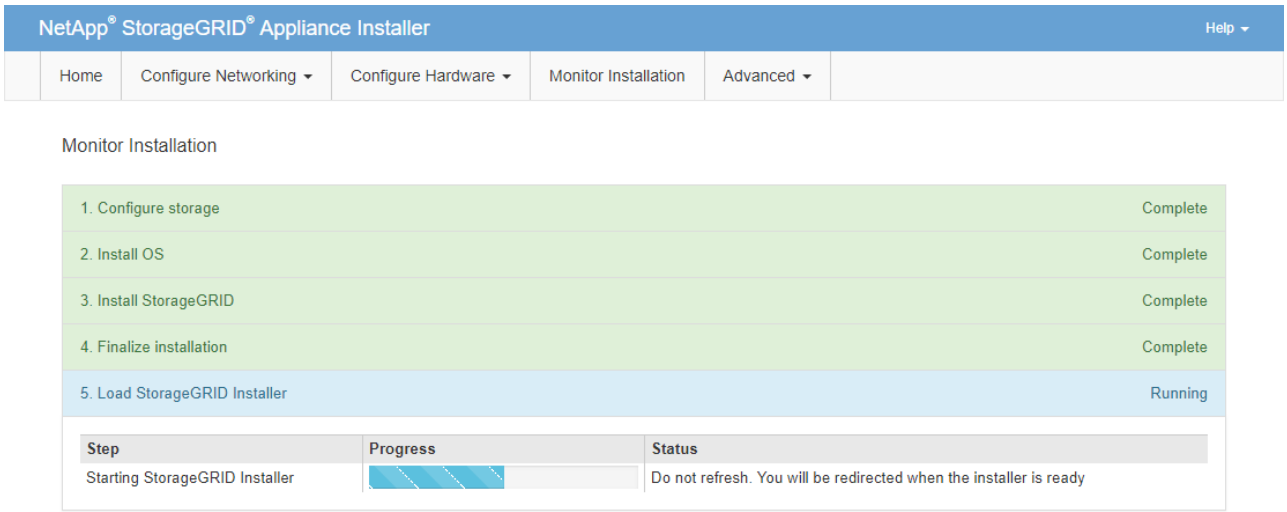
   - * 2. OS * 를 설치합니다

     이 단계에서 설치 관리자는 기본 관리 노드에서 기본 관리 노드로 StorageGRID의 기본 운영 체제 이미지를 복사하거나 기본 관리 노드의 설치 패키지에서 기본 운영 체제를 설치합니다.

3. 다음 중 하나가 발생할 때까지 설치 진행 상태를 계속 모니터링합니다.
   - 어플라이언스 게이트웨이 노드 또는 비기본 어플라이언스 관리 노드의 경우 * StorageGRID * 설치 단계가 일시 중지되고 그리드 관리자를 사용하여 관리 노드에서 이 노드를 승인하라는 메시지가 포함된 콘솔에 나타납니다.



- 어플라이언스 기본 관리 노드의 경우 다섯 번째 단계(StorageGRID 설치 프로그램 로드)가 나타납니다. 5단계가 10분 이상 진행 중인 경우 페이지를 수동으로 새로 고칩니다.



4. 복구 중인 어플라이언스 그리드 노드 유형에 대한 복구 프로세스의 다음 단계로 이동합니다.

복구 유형입니다	참조하십시오
게이트웨이 노드	Start Recovery(복구 시작) 를 선택하여 게이트웨이 노드를 구성합니다
운영 관리자 노드가 아닌 노드	복구 시작 을 선택하여 비 기본 관리 노드를 구성합니다
기본 관리자 노드	대체 운영 관리자 노드를 구성합니다

기술 지원 부서에서 사이트 복구를 수행하는 방법

전체 StorageGRID 사이트에 장애가 발생하거나 여러 스토리지 노드에 장애가 발생할 경우 기술 지원 부서에 문의해야 합니다. 기술 지원 부서에서는 상황을 평가하고 복구 계획을 개발한 다음 비즈니스 목표를 충족하는 방법으로 장애가 발생한 노드나 사이트를 복구하고 복구 시간을 최적화하며 불필요한 데이터 손실을 예방할 수 있습니다.

> 사이트 복구는 기술 지원 부서에서 수행할 수 있습니다.

StorageGRID 시스템은 다양한 장애에 대한 복원력을 갖추고 있으므로 수많은 복구 및 유지 관리 절차를 직접 수행할 수 있습니다. 그러나 구체적인 단계는 상황에 특정한 요인에 따라 달라지기 때문에 간단한 일반화된 사이트 복구 절차를 만드는 것은 어렵습니다. 예를 들면 다음과 같습니다.

- * 비즈니스 목표 *: StorageGRID 사이트가 완전히 손실된 후에는 비즈니스 목표를 가장 잘 달성할 수 있는 방법을 평가해야 합니다. 예를 들어 손실된 사이트를 제자리에서 다시 빌드하시겠습니까? 새 위치에서 손실된 StorageGRID 사이트를 대체하시겠습니까? 고객의 모든 상황은 다르고 복구 계획은 고객의 우선순위를 고려하여 설계되어야 합니다.
- * 정확한 장애 특성 *: 사이트 복구를 시작하기 전에 장애가 발생한 사이트의 노드가 온전한지 또는 스토리지 노드에 복구 가능한 객체가 포함되어 있는지 확인하는 것이 중요합니다. 유효한 데이터가 포함된 노드 또는 스토리지 볼륨을 재구축할 경우 불필요한 데이터 손실이 발생할 수 있습니다.
- * 활성 ILM 정책 *: 그리드의 개체 복사본 수, 유형 및 위치는 활성 ILM 정책에 의해 제어됩니다. ILM 정책의 구체적인 내용은 복구 가능한 데이터의 양과 복구에 필요한 특정 기술에 영향을 줄 수 있습니다.

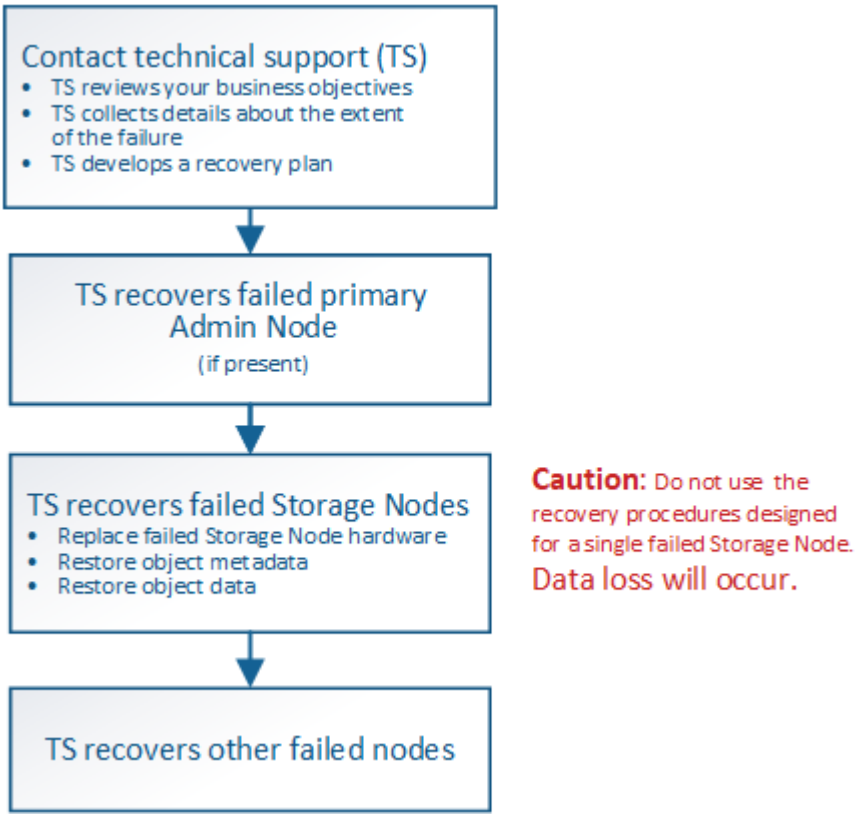
사이트에 개체의 복사본만 포함되어 있고 사이트가 손실되면 개체가 손실됩니다.

- * 버킷(또는 컨테이너) 일관성 *: 버킷(또는 컨테이너)에 적용되는 정합성 수준은 오브젝트 수집이 성공했음을 클라이언트에 알려주기 전에 StorageGRID가 오브젝트 메타데이터를 모든 노드와 사이트에 완전히 복제하는지 여부에 영향을 미칩니다. 정합성 보장 레벨에서 최종 일관성이 허용되는 경우 사이트 장애 시 일부 객체 메타데이터가 손실되었을 수 있습니다. 이는 복구 가능한 데이터의 양과 복구 절차의 세부 정보에 영향을 줄 수 있습니다.
- * 최근 변경 내역 *: 복구 절차의 세부 정보는 장애 발생 시 진행 중인 유지보수 절차가 있는지 또는 ILM 정책에 최근 변경 사항이 있었는지 여부에 따라 영향을 받을 수 있습니다. 기술 지원 부서에서는 사이트 복구를 시작하기 전에 그리드의 최근 내역과 현재 상황을 평가해야 합니다.

사이트 복구 개요

다음은 기술 지원 부서에서 장애가 발생한 사이트를 복구하는 데 사용하는 프로세스에 대한 일반적인 개요입니다.

사이트 복구는 기술 지원 부서에서 수행할 수 있습니다.



1. 기술 지원 부서에 문의하십시오.

   기술 지원 부서는 오류에 대한 세부 평가를 수행하고 귀사와 협력하여 비즈니스 목표를 검토합니다. 이 정보를 기반으로 기술 지원 부서에서는 귀사의 상황에 맞는 복구 계획을 개발합니다.

2. 기술 지원 부서에서는 운영 관리자 노드가 실패한 경우 이를 복구합니다.
3. 기술 지원은 다음 개요를 따라 모든 스토리지 노드를 복구합니다.

   a. 필요에 따라 스토리지 노드 하드웨어 또는 가상 머신을 교체합니다.

b. 개체 메타데이터를 장애가 발생한 사이트로 복원합니다.

c. 객체 데이터를 복구된 스토리지 노드로 복구합니다.

> 장애가 발생한 단일 스토리지 노드에 대한 복구 절차를 사용하면 데이터가 손실됩니다.

> 전체 사이트에 장애가 발생하면 객체 및 객체 메타데이터를 성공적으로 복구하려면 특수 명령이 필요합니다.

4. 기술 지원은 장애가 발생한 다른 노드를 복구합니다.

   개체 메타데이터 및 데이터가 복구된 후 표준 절차를 사용하여 장애가 발생한 게이트웨이 노드, 비기본 관리 노드 또는 아카이브 노드를 복구할 수 있습니다.

관련 정보

사이트 파기

서비스 해제 절차

서비스 해제 절차를 수행하여 그리드 노드 또는 전체 사이트를 StorageGRID 시스템에서 영구적으로 제거할 수 있습니다.

그리드 노드 또는 사이트를 제거하려면 다음 서비스 해제 절차 중 하나를 수행합니다.

- 하나 이상의 사이트에 있을 수 있는 하나 이상의 노드를 제거하려면 * 노드 파기 * 를 수행합니다. 제거하는 노드는 온라인 상태일 수 있으며 StorageGRID 시스템에 연결되어 있을 수도 있고 오프라인일 수도 있고 연결이 끊어질 수도 있습니다.
- 연결된 사이트 파기 * 를 수행하여 모든 노드가 StorageGRID에 연결된 사이트를 제거합니다.
- 연결이 끊긴 사이트 서비스 해제 * 를 수행하여 모든 노드가 StorageGRID에서 분리된 사이트를 제거합니다.

> 연결이 끊긴 사이트 파기 작업을 수행하기 전에 NetApp 계정 담당자에게 문의하십시오. NetApp은 서비스 해제 사이트 마법사의 모든 단계를 활성화하기 전에 요구사항을 검토합니다. 연결이 끊긴 사이트 서비스 해제를 시도해서는 안 됩니다. 사이트를 복구하거나 사이트에서 오브젝트 데이터를 복구할 수 있다고 생각되면 사이트 서비스 해제를 시도해서는 안 됩니다.

사이트에 연결된( ) 및 연결되지 않은 노드(또는), 모든 오프라인 노드를 다시 온라인 상태로 전환해야 합니다.

> 두 번째 유지보수 절차를 수행해야 하는 경우 를 수행할 수 있습니다 스토리지 노드를 제거하는 동안 서비스 해제 절차를 일시 중지합니다. ILM 평가 또는 삭제 코딩 데이터 사용 중단 단계에 도달한 경우에만 * 일시 중지 * 버튼이 활성화됩니다. 그러나 ILM 평가(데이터 마이그레이션)는 백그라운드에서 계속 실행됩니다. 두 번째 유지 보수 절차가 완료되면 서비스 해제를 재개할 수 있습니다.

관련 정보

그리드 노드 해제

사이트 파기

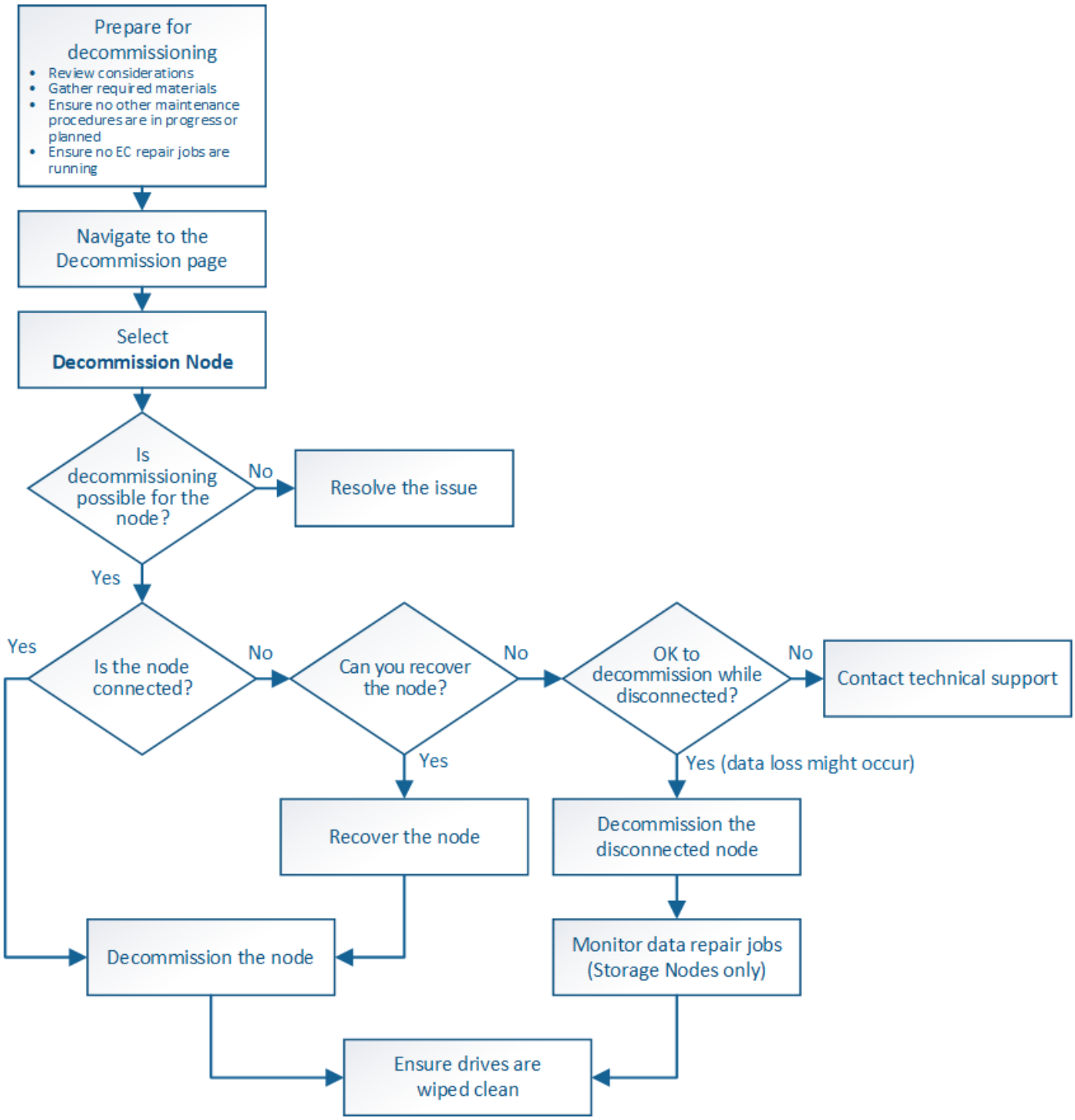
노드 사용 중지 절차를 사용하여 하나 이상의 사이트에서 하나 이상의 스토리지 노드, 게이트웨이 노드 또는 비 운영 관리 노드를 제거할 수 있습니다. 운영 관리자 노드 또는 아카이브 노드는 해제할 수 없습니다.

일반적으로 그리드 노드는 StorageGRID 시스템에 연결되어 있고 모든 노드가 정상 상태인 경우에만 그리드 노드의 서비스를 해제해야 합니다(* 노드 * 페이지 및 * 서비스 해제 노드 * 페이지에 녹색 아이콘이 있음). 그러나 필요한 경우 연결이 끊어진 그리드 노드를 해제할 수 있습니다. 연결이 끊긴 노드를 제거하기 전에 해당 프로세스의 영향과 제한을 이해해야 합니다.

다음 중 하나가 참인 경우 노드 해제 절차를 사용하십시오.

- 시스템에 더 큰 스토리지 노드를 추가했으며 객체를 보존하면서 하나 이상의 더 작은 스토리지 노드를 제거하려는 경우
- 필요한 총 스토리지 용량이 줄어듭니다.
- 더 이상 게이트웨이 노드가 필요하지 않습니다.
- 더 이상 비 기본 관리 노드가 필요하지 않습니다.
- 그리드에는 복구하거나 다시 온라인으로 전환할 수 없는 연결 해제된 노드가 포함되어 있습니다.

흐름도는 그리드 노드의 폐기에 대한 상위 단계를 보여줍니다.



그리드 노드의 해제에 대비합니다

그리드 노드를 제거할 때의 고려 사항을 검토하고 삭제 코딩 데이터에 대해 활성화된 복구 작업이 없는지 확인해야 합니다.

그리드 노드 해제에 대한 고려 사항

이 절차를 시작하여 하나 이상의 노드를 폐기하기 전에 각 노드 유형을 제거할 때의 영향을 이해해야 합니다. 노드가 성공적으로 해제되면 해당 서비스가 비활성화되고 노드가 자동으로 종료됩니다.

노드를 사용 중단할 수 없는 경우 StorageGRID이 잘못된 상태로 유지됩니다. 다음 규칙이 적용됩니다.

- 운영 관리자 노드의 해제는 불가능합니다.
- 아카이브 노드는 해제할 수 없습니다.
- 네트워크 인터페이스 중 하나가 고가용성(HA) 그룹에 속한 경우에는 관리 노드 또는 게이트웨이 노드를 해제할 수 없습니다.
- 스토리지 노드를 제거하면 ADC 쿼럼에 영향을 줄 수 있습니다.
- 활성 ILM 정책에 필요한 스토리지 노드는 해제할 수 없습니다.
- 단일 서비스 해제 노드 절차에서 10개 이상의 스토리지 노드를 서비스 해제할 수 없습니다.
- 그리드에 연결이 끊긴 노드(상태가 알 수 없거나 관리상 중단된 노드)가 포함된 경우 연결된 노드의 서비스를 해제할 수 없습니다. 먼저 연결이 끊긴 노드를 서비스 해제하거나 복구해야 합니다.
- 그리드에 연결이 끊어진 노드가 여러 개 포함된 경우, 소프트웨어를 동시에 모두 해제해야 예기치 않은 결과가 발생할 가능성이 높아집니다.
- 연결이 끊긴 노드를 제거할 수 없는 경우(예: ADC 쿼럼에 필요한 스토리지 노드) 연결이 끊긴 다른 노드는 제거할 수 없습니다.
- 이전 제품을 새 제품으로 교체하려면 다음을 고려하십시오 어플라이언스 노드 클론 생성 확장을 위해 기존 노드를 폐기하거나 새 노드를 추가하는 대신

> 서비스 해제 절차에서 지시할 때까지 그리드 노드의 가상 머신 또는 기타 리소스를 제거하지 마십시오.

관리 노드 또는 게이트웨이 노드 파기 고려 사항

관리 노드 또는 게이트웨이 노드를 해제하기 전에 다음 고려 사항을 검토하십시오.

- 서비스 해제 절차를 수행하려면 일부 시스템 리소스에 대한 독점적 액세스가 필요하므로 다른 유지보수 절차가 실행되고 있지 않은지 확인해야 합니다.
- 운영 관리자 노드의 해제는 불가능합니다.
- 네트워크 인터페이스 중 하나가 고가용성(HA) 그룹에 속한 경우에는 관리 노드 또는 게이트웨이 노드를 해제할 수 없습니다. 먼저 HA 그룹에서 네트워크 인터페이스를 제거해야 합니다. StorageGRID 관리 지침을 참조하십시오.
- 필요한 경우 게이트웨이 노드 또는 관리 노드를 폐기하는 동안 ILM 정책을 안전하게 변경할 수 있습니다.
- StorageGRID 시스템에 대해 관리자 노드를 사용 중지하고 SSO(Single Sign-On)를 사용하는 경우 AD FS(Active Directory Federation Services)에서 노드의 기반 당사자 신뢰를 제거해야 합니다.

관련 정보

StorageGRID 관리

스토리지 노드 파기 관련 고려 사항

스토리지 노드를 폐기하려는 경우 StorageGRID이 해당 노드에서 오브젝트 데이터 및 메타데이터를 관리하는 방법을 이해해야 합니다.

스토리지 노드를 사용 중단할 때는 다음과 같은 고려 사항 및 제한 사항이 적용됩니다.

- 시스템은 항상 ADC 쿼럼과 활성 ILM 정책을 포함하여 운영 요구 사항을 충족할 수 있는 충분한 스토리지 노드를

포함해야 합니다. 이러한 제한을 충족하려면 기존 스토리지 노드를 폐기하기 전에 확장 작업에서 새 스토리지 노드를 추가해야 할 수 있습니다.

- 스토리지 노드를 서비스 해제할 때 스토리지 노드의 연결이 끊어지면 시스템은 연결된 스토리지 노드의 데이터를 사용하여 데이터를 재구성해야 합니다. 이렇게 하면 데이터가 손실될 수 있습니다.
- 스토리지 노드를 제거할 때 대량의 객체 데이터를 네트워크를 통해 전송해야 합니다. 이러한 전송은 정상적인 시스템 작동에 영향을 주지 않지만 StorageGRID 시스템에서 사용하는 총 네트워크 대역폭에 영향을 줄 수 있습니다.
- 스토리지 노드 사용 중단과 관련된 작업은 일반 시스템 작업과 관련된 작업보다 우선 순위가 낮습니다. 즉, 서비스 해제는 정상적인 StorageGRID 시스템 작동을 방해하지 않으며 시스템 비활성 기간 동안 예약할 필요가 없습니다. 디커미셔닝 작업은 백그라운드에서 수행되므로 프로세스가 완료되는 데 걸리는 시간을 추정하기가 어렵습니다. 일반적으로 시스템이 정숙하거나 한 번에 하나의 스토리지 노드만 제거하는 경우 서비스 해제가 더 빠르게 완료됩니다.
- 스토리지 노드의 서비스를 해제하는 데 며칠 또는 몇 주가 걸릴 수 있습니다. 이에 따라 이 절차를 계획하십시오. 서비스 해제 프로세스는 시스템 운영에 영향을 주지 않도록 설계되었지만 다른 절차는 제한할 수 있습니다. 일반적으로 그리드 노드를 제거하기 전에 계획된 시스템 업그레이드 또는 확장을 수행해야 합니다.
- 특정 단계에서 스토리지 노드를 포함하는 서비스 해제 절차를 일시 중지하여 필요한 경우 다른 유지 보수 절차를 실행하고 작업이 완료되면 재개할 수 있습니다.
- 서비스 해제 작업이 실행 중인 경우에는 그리드 노드에서 데이터 복구 작업을 실행할 수 없습니다.
- 스토리지 노드를 사용 중단하는 동안에는 ILM 정책을 변경하지 않아야 합니다.
- 스토리지 노드를 제거하면 노드의 데이터가 다른 그리드 노드로 마이그레이션되지만 이 데이터는 사용 중지된 그리드 노드에서 완전히 제거되지 않습니다. 데이터를 영구적으로 안전하게 제거하려면 서비스 해제 절차가 완료된 후 사용 중지된 그리드 노드의 드라이브를 지어야 합니다.
- 스토리지 노드를 서비스 해제할 때 다음과 같은 경고 및 경보가 발생할 수 있으며 관련 e-메일 및 SNMP 알림을 받을 수 있습니다.
  - * 노드 * 경고와 통신할 수 없습니다. 이 알림은 ADC 서비스를 포함하는 스토리지 노드를 서비스 해제할 때 트리거됩니다. 서비스 해제 작업이 완료되면 경고가 해결됩니다.
  - VSTU(Object Verification Status) 알람. 이 알림 레벨 알람은 서비스 해제 프로세스 중에 스토리지 노드가 유지보수 모드로 전환됨을 나타냅니다.
  - Casa(Data Store Status) 알람. 이 주요 레벨 알람은 서비스가 중지되었기 때문에 Cassandra 데이터베이스가 작동 중지되었음을 나타냅니다.

관련 정보

필요한 경우 오브젝트 데이터를 스토리지 볼륨으로 복구합니다

ADC 쿼럼을 이해합니다

사용 중지 후에도 너무 적은 ADC(관리 도메인 컨트롤러) 서비스가 남아 있는 경우 데이터 센터 사이트에서 특정 스토리지 노드의 사용을 중지하지 못할 수 있습니다. 일부 스토리지 노드에서 찾을 수 있는 이 서비스는 그리드 토폴로지 정보를 유지하고 그리드에 구성 서비스를 제공합니다. StorageGRID 시스템은 각 사이트에서 항상 사용할 수 있는 ADC 서비스 쿼럼을 필요로 합니다.

노드를 제거하면 ADC 쿼럼이 더 이상 충족되지 않는 경우 스토리지 노드를 해제할 수 없습니다. 사용 중단 중에 ADC 쿼럼을 만족시키려면 각 데이터 센터 사이트의 최소 3개의 스토리지 노드에 ADC 서비스가 있어야 합니다. 데이터 센터 사이트에 ADC 서비스가 있는 스토리지 노드가 3개 이상 있는 경우 사용 중단 후 해당 노드 중 단순한 대부분을 사용할 수 있어야 합니다(0.5 * "*ADC*가 있는 스토리지 노드") + 1).

예를 들어 데이터 센터 사이트에 현재 ADC 서비스가 있는 6개의 스토리지 노드가 있고 3개의 스토리지 노드를 폐기하려는 경우를 가정해 보겠습니다. ADC quorum 요구 사항으로 인해 다음과 같이 2개의 서비스 해제 절차를 완료해야 합니다.

- 첫 번째 서비스 해제 절차에서는 ADC 서비스가 있는 스토리지 노드 4개를 사용할 수 있는지 확인해야 합니다((0.5 * 6) + 1). 즉, 처음에 2개의 스토리지 노드만 서비스 해제할 수 있습니다.
- 두 번째 서비스 해제 절차에서 세 번째 스토리지 노드를 제거할 수 있습니다. ADC 쿼럼은 이제 세 개의 ADC 서비스만 사용할 수 있어야 하므로((0.5 * 4) + 1) 세 번째 스토리지 노드를 제거할 수 있습니다.

스토리지 노드를 해제해야 하지만 ADC 쿼럼 요구 사항으로 인해 해제할 수 없는 경우 확장에서 새 스토리지 노드를 추가하고 ADC 서비스를 사용하도록 지정해야 합니다. 그런 다음 기존 스토리지 노드를 서비스 해제할 수 있습니다.

관련 정보

그리드를 확장합니다

ILM 정책 및 스토리지 구성을 검토합니다

스토리지 노드의 서비스를 해제할 계획인 경우 서비스 해제 프로세스를 시작하기 전에 StorageGRID 시스템의 ILM 정책을 검토해야 합니다.

서비스 해제 중에 모든 오브젝트 데이터가 사용 중지된 스토리지 노드에서 다른 스토리지 노드로 마이그레이션됩니다.

> 사용 중인 ILM 정책은 _ 사용 중지 중 _ 사용 후 _ 이(가) 사용됩니다. 서비스 해제를 시작하기 전과 서비스 해제가 완료된 후에 이 정책이 데이터 요구사항을 충족해야 합니다.

활성 ILM 정책의 규칙을 검토하여 StorageGRID 시스템이 스토리지 노드의 해체를 수용할 수 있는 올바른 유형과 올바른 위치에 있는 충분한 용량을 계속 유지할 수 있도록 해야 합니다.

다음 사항을 고려하십시오.

- ILM 규칙 충족을 위해 ILM 평가 서비스가 오브젝트 데이터를 복사할 수 있습니까?
- 서비스 해제 중에 사이트를 일시적으로 사용할 수 없게 되면 어떻게 됩니까? 다른 위치에서 추가 사본을 만들 수 있습니까?
- 서비스 해제 프로세스는 콘텐츠의 최종 배포에 어떤 영향을 미칩니까? 에 설명된 대로 스토리지 노드 통합이전 스토리지 노드를 폐기하기 전에 새 스토리지 노드를 추가해야 합니다. 더 작은 스토리지 노드를 해체한 후 더 큰 교체 스토리지 노드를 추가하면 기존 스토리지 노드의 용량이 거의 근접할 수 있고 새 스토리지 노드의 컨텐츠가 거의 없을 수 있습니다. 새 오브젝트 데이터에 대한 대부분의 쓰기 작업은 새 스토리지 노드로 보내되므로 시스템 작업의 전반적인 효율성이 감소합니다.
- 시스템이 항상 활성 ILM 정책을 충족할 수 있는 충분한 스토리지 노드를 포함합니까?

> 만족하지 못하는 ILM 정책은 백로그 및 알람을 발생시키고 StorageGRID 시스템의 작동을 중지할 수 있습니다.

해체 프로세스로 인해 발생하는 제안된 토폴로지가 표에 나열된 요소를 평가하여 ILM 정책을 충족하는지 확인합니다.

평가할 영역	참고
사용 가능한 용량입니다	StorageGRID 시스템에 저장된 모든 오브젝트 데이터를 수용할 수 있는 스토리지 용량이 충분해야 하며, 사용 중단할 스토리지 노드에 현재 저장된 오브젝트 데이터의 영구 복사본을 포함합니까? 사용 중단 완료 후 적절한 시간 간격 동안 저장된 오브젝트 데이터의 예상 증가를 처리할 수 있는 용량이 충분합니까?
저장 위치	StorageGRID 시스템 전체에 충분한 용량이 남아 있는 경우, StorageGRID 시스템의 비즈니스 규칙을 충족하는 데 적합한 위치에 용량이 있습니까?
스토리지 유형입니다	해체 완료 후 적절한 유형의 스토리지가 충분합니까? 예를 들어, ILM 규칙에 따라 콘텐츠가 오래되면 스토리지 유형 간에 이동되도록 지정할 수 있습니다. 이 경우 StorageGRID 시스템의 최종 구성에서 적절한 유형의 스토리지를 충분히 사용할 수 있는지 확인해야 합니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

그리드를 확장합니다

연결이 끊긴 스토리지 노드의 서비스 해제

스토리지 노드의 접속이 해제된 상태에서 스토리지 노드의 서비스를 해제할 경우 발생할 수 있는 상황을 파악해야 합니다(상태는 알 수 없음 또는 관리상 중단).

그리드에서 연결이 끊긴 스토리지 노드를 폐기하는 경우 StorageGRID는 다른 스토리지 노드의 데이터를 사용하여 연결이 끊긴 노드에 있던 오브젝트 데이터 및 메타데이터를 재구성합니다. 서비스 해제 프로세스가 끝나면 데이터 복구 작업을 자동으로 시작합니다.

분리된 스토리지 노드를 폐기하기 전에 다음 사항에 유의하십시오.

- 연결이 끊어진 노드를 온라인 상태로 만들거나 복구할 수 없는 경우가 아니면 이 노드를 사용 중단해서는 안 됩니다.

> 노드에서 오브젝트 데이터를 복구할 수 있다고 생각되면 이 절차를 수행하지 마십시오. 대신 기술 지원 부서에 문의하여 노드 복구가 가능한지 확인하십시오.

- 연결이 끊긴 스토리지 노드에 개체의 복사본만 포함되어 있는 경우 노드를 서비스 해제할 때 해당 개체가 손실됩니다. 데이터 복구 작업은 현재 연결된 스토리지 노드에 하나 이상의 복제된 복사본 또는 충분한 삭제 코딩 조각이 있는 경우에만 오브젝트를 재구성 및 복구할 수 있습니다.
- 연결이 끊긴 스토리지 노드를 폐기하면 서비스 해제 절차가 비교적 빠르게 완료됩니다. 그러나 데이터 복구 작업을 실행하는 데 며칠 또는 몇 주가 걸릴 수 있으며 서비스 해제 절차를 통해 모니터링되지 않습니다. 이러한 작업을 수동으로 모니터링하고 필요에 따라 다시 시작해야 합니다. 을 참조하십시오 데이터 복구 작업을 확인합니다.
- 연결이 끊긴 스토리지 노드를 한 번에 두 개 이상 폐기하는 경우 데이터가 손실될 수 있습니다. 오브젝트 데이터, 메타데이터 또는 삭제 코딩 단편의 복사본이 너무 적은 경우에도 데이터를 재구성하지 못할 수 있습니다.

> 복구할 수 없는 스토리지 노드가 두 개 이상 연결되어 있는 경우 기술 지원 부서에 문의하여 최상의 조치 방법을 확인하십시오.

스토리지 노드 통합

스토리지 노드를 통합하여 스토리지 용량을 늘리면서 사이트 또는 구축의 스토리지 노드 수를 줄일 수 있습니다.

스토리지 노드를 통합할 때 StorageGRID 시스템을 확장하여 용량이 큰 새 스토리지 노드를 추가한 다음 용량이 작은 기존 스토리지 노드의 사용을 해제합니다. 서비스 해제 절차 중에 오브젝트는 이전 스토리지 노드에서 새 스토리지 노드로 마이그레이션됩니다.

> 구형 어플라이언스 및 소형 어플라이언스를 새로운 모델 또는 더 큰 용량 어플라이언스로 통합하는 경우 일대다 교체를 수행하지 않을 경우 노드 클론 기능 또는 노드 클론 복제 절차와 서비스 해제 절차를 사용하는 경우가 많습니다.

예를 들어, 용량이 큰 새 스토리지 노드 2개를 추가하여 세 개의 이전 스토리지 노드를 교체할 수 있습니다. 먼저 확장 절차를 사용하여 2개의 더 큰 새 스토리지 노드를 추가한 다음 서비스 해제 절차를 사용하여 이전의 3개의 더 작은 용량 스토리지 노드를 제거할 수 있습니다.

기존 스토리지 노드를 제거하기 전에 새 용량을 추가하면 StorageGRID 시스템 전체에서 데이터의 균형 잡힌 배포가 보장됩니다. 또한 기존 스토리지 노드가 스토리지 워터마크 수준 이상으로 푸시될 가능성을 줄일 수 있습니다.

관련 정보

그리드를 확장합니다

여러 스토리지 노드의 서비스 해제

둘 이상의 스토리지 노드를 제거해야 하는 경우 순차적으로 또는 병렬로 서비스 해제할 수 있습니다.

- 스토리지 노드를 순차적으로 서비스 해제하는 경우 다음 스토리지 노드의 서비스 해제를 시작하기 전에 첫 번째 스토리지 노드가 서비스 해제를 완료할 때까지 기다려야 합니다.
- 스토리지 노드를 병렬로 폐기하는 경우 스토리지 노드는 사용 중단 중인 모든 스토리지 노드에 대한 서비스 해제 작업을 동시에 처리합니다. 이로 인해 파일의 모든 영구 사본이 "읽기 전용"으로 표시되어 이 기능이 활성화된 그리드의 삭제를 일시적으로 비활성화할 수 있습니다.

데이터 복구 작업을 확인합니다

그리드 노드를 폐기하기 전에 활성화된 데이터 복구 작업이 없는지 확인해야 합니다. 수리가 실패한 경우 서비스를 다시 시작하고 서비스 해제 절차를 수행하기 전에 수리가 완료될 수 있도록 해야 합니다.

연결이 끊긴 스토리지 노드의 서비스를 해제해야 하는 경우 서비스 해제 절차가 완료된 후 데이터 복구 작업이 성공적으로 완료되도록 이러한 단계를 완료해야 합니다. 제거된 노드에 있었던 삭제 코딩 조각이 성공적으로 복구되었는지 확인해야 합니다.

이 단계는 삭제 코딩 오브젝트가 있는 시스템에만 적용됩니다.

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

c. 루트로 전환하려면 다음 명령을 입력합니다

d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

2. Repair-data show-ec-repair-status'라는 복구 실행 여부를 확인한다

   - 데이터 복구 작업을 실행하지 않은 경우 출력은 "작업을 찾을 수 없음"입니다. 복구 작업을 다시 시작할 필요가 없습니다.
   - 데이터 복구 작업이 이전에 실행되었거나 현재 실행 중인 경우 출력에 복구에 대한 정보가 나열됩니다. 각 수리마다 고유한 수리 ID가 있습니다. 다음 단계로 이동합니다.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time End Time State Est/Affected Bytes Repaired
Retry Repair
==========================================================================
===========
949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359 0
Yes
949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359 0
Yes
949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359 0
Yes
```

3. 모든 수리의 상태가 '성공'이면 수리 작업을 다시 시작할 필요가 없습니다.

4. 복구 상태가 "실패"인 경우 해당 복구를 다시 시작해야 합니다.

   a. 출력에서 실패한 복구에 대한 수리 ID를 얻습니다.

   b. repair-data start-ec-node-repair' 명령을 실행합니다.

      '--repair-id' 옵션을 사용하여 복구 ID를 지정합니다. 예를 들어 복구 ID 949292를 사용하여 복구를 다시 시도하려는 경우 이 명령을 실행합니다. repair-data start-ec-node-repair—repair-id 949292

   c. 모든 수리에 대한 상태가 '성공'이 될 때까지 EC 데이터 수리 상태를 계속 추적합니다.

필요한 자료를 수집합니다

그리드 노드 해제를 수행하기 전에 다음 정보를 얻어야 합니다.

항목	참고
복구 패키지 '.zip' 파일	반드시 해야 합니다 최신 복구 패키지를 다운로드합니다 zip 파일('S Ws-recovery-package -*id-revision*.zip'). 장애가 발생할 경우 복구 패키지 파일을 사용하여 시스템을 복원할 수 있습니다.
"passwords.txt" 파일	이 파일에는 명령줄에서 그리드 노드에 액세스하는 데 필요한 암호가 들어 있으며 복구 패키지에 포함되어 있습니다.
프로비저닝 암호	StorageGRID 시스템을 처음 설치할 때 암호가 생성되고 문서화됩니다. 프로비저닝 암호문은 passwords.txt 파일에 없습니다.
서비스 해제 전 StorageGRID 시스템의 토폴로지에 대한 설명입니다	가능한 경우 시스템의 현재 토폴로지를 설명하는 문서를 가져옵니다.

관련 정보

웹 브라우저 요구 사항

서비스 해제 노드 액세스 페이지입니다

Grid Manager에서 Decommission Nodes 페이지에 액세스하면 사용 중단될 수 있는 노드를 한눈에 볼 수 있습니다.

필요한 것

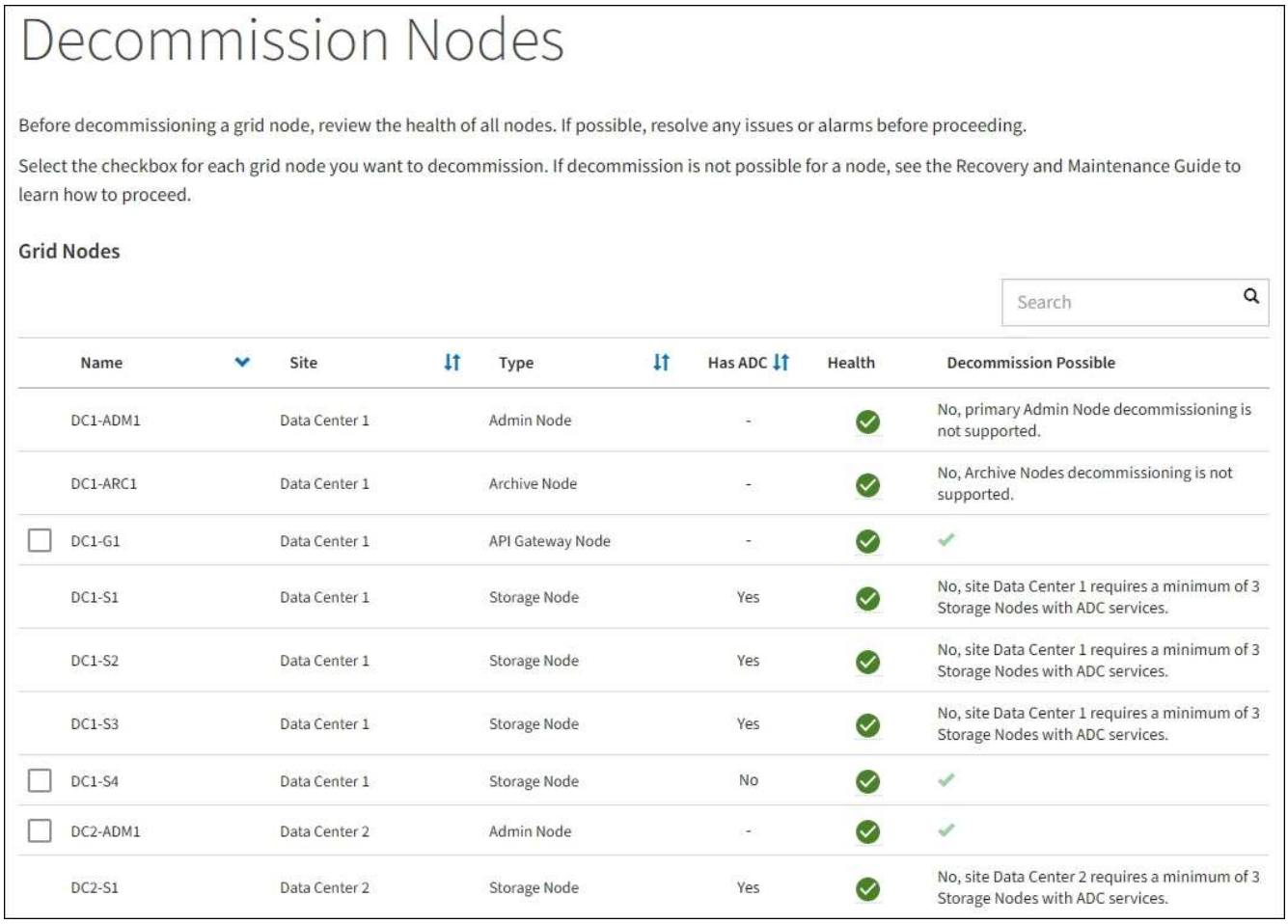
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.

단계

1. 유지 관리 * > * 작업 * > * 서비스 해제 * 를 선택합니다.
2. 서비스 해제 노드 * 를 선택합니다.

   서비스 해제 노드 페이지가 나타납니다. 이 페이지에서 다음을 수행할 수 있습니다.

   - 현재 사용 중단될 수 있는 그리드 노드를 결정합니다.
   - 모든 그리드 노드의 상태를 확인합니다
   - 목록을 오름차순 또는 내림차순으로 * 이름 *, * 사이트 *, * 유형 * 또는 * ADC * 를 기준으로 정렬합니다.
   - 검색어를 입력하여 특정 노드를 빠르게 찾을 수 있습니다. 예를 들어 이 페이지에는 두 데이터 센터의 그리드 노드가 표시됩니다. 서비스 해제 가능 열은 게이트웨이 노드, 5개의 스토리지 노드 중 하나 및 비운영 관리 노드를 서비스 해제할 수 있음을 나타냅니다.



3. 서비스 해제하려는 각 노드에 대해 * 서비스 해제 가능 * 열을 검토합니다.

   그리드 노드를 해체할 수 있는 경우 이 열에는 녹색 확인 표시가 있고 맨 왼쪽 열에는 확인란이 포함됩니다. 노드를 해체할 수 없는 경우 이 열에 이 문제가 설명되어 있습니다. 노드가 해체될 수 없는 두 가지 이상의 이유가 있는 경우 가장 중요한 이유가 표시됩니다.

사용 중지 가능한 이유	설명	해결 단계
아니요. 노드 유형 서비스 해제는 지원되지 않습니다.	운영 관리자 노드 또는 아카이브 노드는 해제할 수 없습니다.	없음.

사용 중지 가능한 이유	설명	해결 단계
아니요. 그리드 노드가 하나 이상 연결되어 있지 않습니다. • 참고: * 이 메시지는 연결된 그리드 노드에만 표시됩니다.	그리드 노드의 연결이 끊어진 경우에는 연결된 그리드 노드를 해제할 수 없습니다. 상태 * 열에는 연결이 끊긴 그리드 노드에 대한 다음 아이콘 중 하나가 포함됩니다. • (회색): 관리상 중단 • (파란색): 알 수 없음	로 이동합니다 서비스 해제 절차 선택 항목이 나열된 단계입니다.
아니요. 하나 이상의 필수 노드가 현재 연결 해제되어 있으며 복구해야 합니다. • 참고: * 이 메시지는 연결이 끊긴 그리드 노드에만 표시됩니다.	하나 이상의 필수 노드도 연결 해제된 경우(예: ADC 쿼럼에 필요한 스토리지 노드) 연결이 해제된 그리드 노드를 해제할 수 없습니다.	a. 연결이 끊긴 모든 노드에 대해 서비스 해제 가능 메시지를 검토합니다. b. 필요한 경우 사용 해제할 수 없는 노드를 결정합니다. ◦ 필요한 노드의 상태가 관리상 중단된 경우 노드를 다시 온라인 상태로 전환합니다. ◦ 필요한 노드의 상태가 Unknown 인 경우 노드 복구 절차를 수행하여 필요한 노드를 복구합니다.
아니요, HA 그룹의 구성원:_x_. 이 노드를 사용 해제하려면 먼저 모든 HA 그룹에서 제거해야 합니다.	노드 인터페이스가 고가용성(HA) 그룹에 속한 경우에는 관리 노드 또는 게이트웨이 노드를 해제할 수 없습니다.	HA 그룹을 편집하여 노드의 인터페이스를 제거하거나 전체 HA 그룹을 제거합니다. StorageGRID 관리 지침을 참조하십시오.
아니요. site_x_에는 ADC 서비스를 포함하는 최소 _n_개의 스토리지 노드가 필요합니다.	• 스토리지 노드만 해당. * ADC 쿼럼 요구 사항을 지원하기 위해 사이트에 충분한 노드가 남아 있으면 스토리지 노드를 해제할 수 없습니다.	확장을 수행합니다. 사이트에 새 스토리지 노드를 추가하고 ADC 서비스를 사용하도록 지정합니다. ADC 정수에 대한 정보를 참조하십시오.

사용 중지 가능한 이유	설명	해결 단계
아니요. 하나 이상의 삭제 코딩 프로파일에 적어도 _n_개의 스토리지 노드가 필요합니다. ILM 규칙에서 프로파일을 사용하지 않는 경우 비활성화할 수 있습니다.	• 스토리지 노드 전용. * 기존 삭제 코딩 프로파일에 대해 충분한 노드가 남아 있지 않으면 스토리지 노드를 해제할 수 없습니다. 예를 들어, 4+2 삭제 코딩에 대해 삭제 코딩 프로필이 있는 경우 최소 6개의 스토리지 노드를 유지해야 합니다.	영향을 받는 각 삭제 코딩 프로필에 대해 프로필을 사용하는 방법에 따라 다음 단계 중 하나를 수행합니다. • * 활성 ILM 정책에 사용됨 *: 확장을 수행합니다. 삭제 코딩을 계속할 수 있도록 새 스토리지 노드를 추가합니다. StorageGRID 확장 지침을 참조하십시오. • * ILM 규칙에 사용되지만 활성 ILM 정책에는 사용되지 않음 *: 규칙을 편집 또는 삭제한 다음 삭제 코딩 프로필을 비활성화합니다. • * ILM 규칙에서 사용되지 않음 *: 삭제 코딩 프로필을 비활성화합니다. ◦ 참고: * 삭제 코딩 프로파일을 비활성화하려고 하면 오류 메시지가 나타나고 오브젝트 데이터는 여전히 프로파일과 연결됩니다. 비활성화 프로세스를 다시 시도하기 전에 몇 주를 기다려야 할 수 있습니다. 정보 수명 주기 관리를 사용하여 개체를 관리하기 위한 지침에서 삭제 코딩 프로필 비활성화에 대해 알아보십시오.

4. [[서비스 해제_절차_선택]] 노드에 대해 서비스 해제가 가능한 경우 수행해야 할 절차를 결정합니다.

그리드에 다음 사항이 포함되어 있는 경우:	이동...
연결이 끊긴 모든 그리드 노드	연결이 끊긴 그리드 노드의 서비스 해제
연결된 그리드 노드만	연결된 그리드 노드 해제

관련 정보

데이터 복구 작업을 확인합니다

ADC 쿼럼을 이해합니다

ILM을 사용하여 개체를 관리합니다

그리드를 확장합니다

StorageGRID 관리

연결이 끊긴 그리드 노드의 서비스 해제

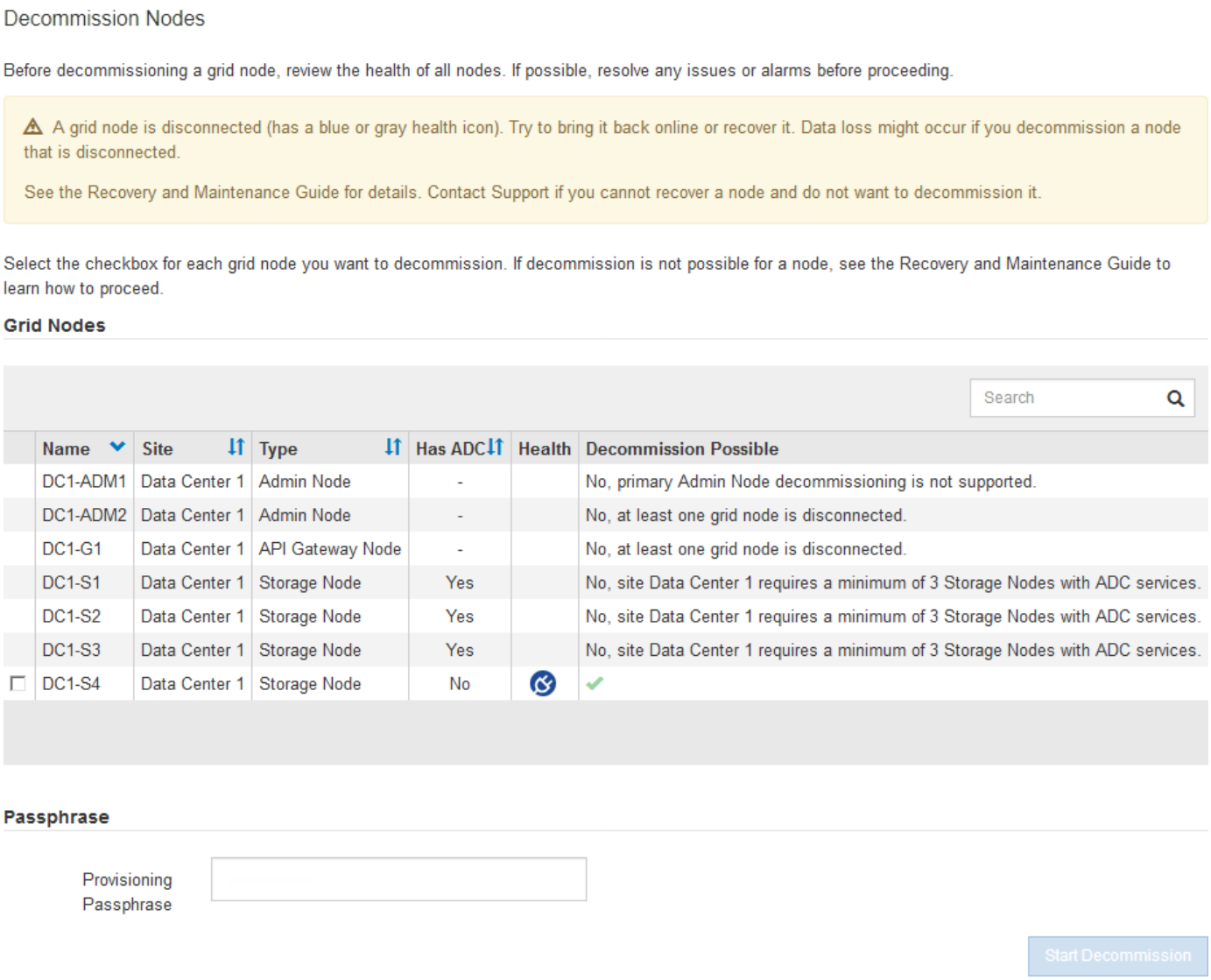
현재 그리드에 연결되어 있지 않은 노드(상태가 알 수 없거나 관리상 중단된 노드)를 해제해야 할 수 있습니다.

필요한 것

- 귀하는 및 의 요구사항을 이해합니다 그리드 노드 폐기에 대한 고려 사항.
- 모든 필수 항목을 확보했습니다.
- 활성화된 데이터 복구 작업이 없도록 했습니다. 을 참조하십시오 데이터 복구 작업을 확인합니다.
- 스토리지 노드 복구가 그리드의 어느 곳에서든 진행되고 있지 않음을 확인했습니다. 있는 경우 복구 과정에서 Cassandra 재구축이 완료될 때까지 기다려야 합니다. 그런 다음 해체 작업을 진행할 수 있습니다.
- 노드 서비스 해제 절차가 일시 중지되지 않는 한 노드 서비스 해제 절차가 실행되는 동안 다른 유지 보수 절차가 실행되지 않도록 했습니다.
- 서비스 해제하려는 연결이 끊긴 노드 또는 노드에 대한 * 서비스 해제 가능 * 열에 녹색 확인 표시가 포함됩니다.
- 프로비저닝 암호가 있어야 합니다.

이 작업에 대해

상태 * 열에서 알 수 없음(파란색) 또는 관리 다운(회색) 아이콘을 찾아 연결이 끊긴 노드를 식별할 수 있습니다. 이 예에서는 DC1-S4라는 스토리지 노드의 연결이 끊어지고 다른 모든 노드가 연결됩니다.



분리된 노드를 폐기하기 전에 다음 사항에 유의하십시오.

- 이 절차는 주로 연결이 끊긴 단일 노드를 제거하기 위한 것입니다. 그리드에 연결이 끊어진 노드가 여러 개 포함된 경우, 소프트웨어를 동시에 모두 해제해야 예기치 않은 결과가 발생할 가능성이 높아집니다.

> 연결이 끊긴 여러 개의 그리드 노드를 한 번에 해제할 때는 특히 연결이 끊긴 여러 스토리지 노드를 선택하는 경우 특히 주의해야 합니다.

- 연결이 끊긴 노드를 제거할 수 없는 경우(예: ADC 쿼럼에 필요한 스토리지 노드) 연결이 끊긴 다른 노드는 제거할 수 없습니다.

연결이 끊긴 * 스토리지 노드 * 를 해제하기 전에 다음 사항에 유의하십시오

- 연결 해제된 스토리지 노드를 온라인 상태로 만들거나 복구할 수 없는 경우가 아니라면 이 스토리지 노드를 서비스 해제해서는 안 됩니다.

> 노드에서 개체 데이터를 복구할 수 있다고 생각되면 이 절차를 수행하지 마십시오. 대신 기술 지원 부서에 문의하여 노드 복구가 가능한지 확인하십시오.

- 연결이 끊긴 스토리지 노드를 두 개 이상 폐기하는 경우 데이터가 손실될 수 있습니다. 오브젝트 복사본, 삭제 코딩 조각 또는 오브젝트 메타데이터가 충분하지 않은 경우 시스템에서 데이터를 재구성하지 못할 수 있습니다.

> 복구할 수 없는 스토리지 노드가 두 개 이상 연결되어 있는 경우 기술 지원 부서에 문의하여 최상의 조치 방법을 확인하십시오.

- 연결이 끊긴 스토리지 노드를 폐기하는 경우 StorageGRID는 서비스 해제 프로세스가 끝날 때 데이터 복구 작업을 시작합니다. 이러한 작업은 연결이 끊긴 노드에 저장된 개체 데이터 및 메타데이터를 재구성하려고 시도합니다.
- 연결이 끊긴 스토리지 노드를 폐기하면 서비스 해제 절차가 비교적 빠르게 완료됩니다. 그러나 데이터 복구 작업을 실행하는 데 며칠 또는 몇 주가 걸릴 수 있으며 서비스 해제 절차를 통해 모니터링되지 않습니다. 이러한 작업을 수동으로 모니터링하고 필요에 따라 다시 시작해야 합니다. 을 참조하십시오 데이터 복구 작업을 확인합니다.
- 개체의 복사본만 포함된 연결이 끊긴 스토리지 노드를 폐기하면 개체가 손실됩니다. 데이터 복구 작업은 현재 연결된 스토리지 노드에 하나 이상의 복제된 복사본 또는 충분한 삭제 코딩 조각이 있는 경우에만 오브젝트를 재구성 및 복구할 수 있습니다.

연결되지 않은 * 관리 노드 * 또는 * 게이트웨이 노드 * 를 해제하기 전에 다음 사항을 확인하십시오.

- 연결이 끊긴 관리 노드를 서비스 해제할 경우 해당 노드에서 감사 로그가 손실되지만 이러한 로그는 기본 관리 노드에도 존재해야 합니다.
- 연결이 끊어진 상태에서 게이트웨이 노드를 안전하게 해제할 수 있습니다.

단계

1. 연결이 끊긴 그리드 노드를 다시 온라인 상태로 만들거나 복구해 봅니다.

   지침은 복구 절차를 참조하십시오.

2. 연결이 끊긴 그리드 노드를 복구할 수 없고 연결이 끊긴 동안 노드 사용을 해제하려면 해당 노드에 대한 확인란을 선택합니다.

   > 그리드에 연결이 끊어진 노드가 여러 개 포함된 경우, 소프트웨어를 동시에 모두 해제해야 예기치 않은 결과가 발생할 가능성이 높아집니다.

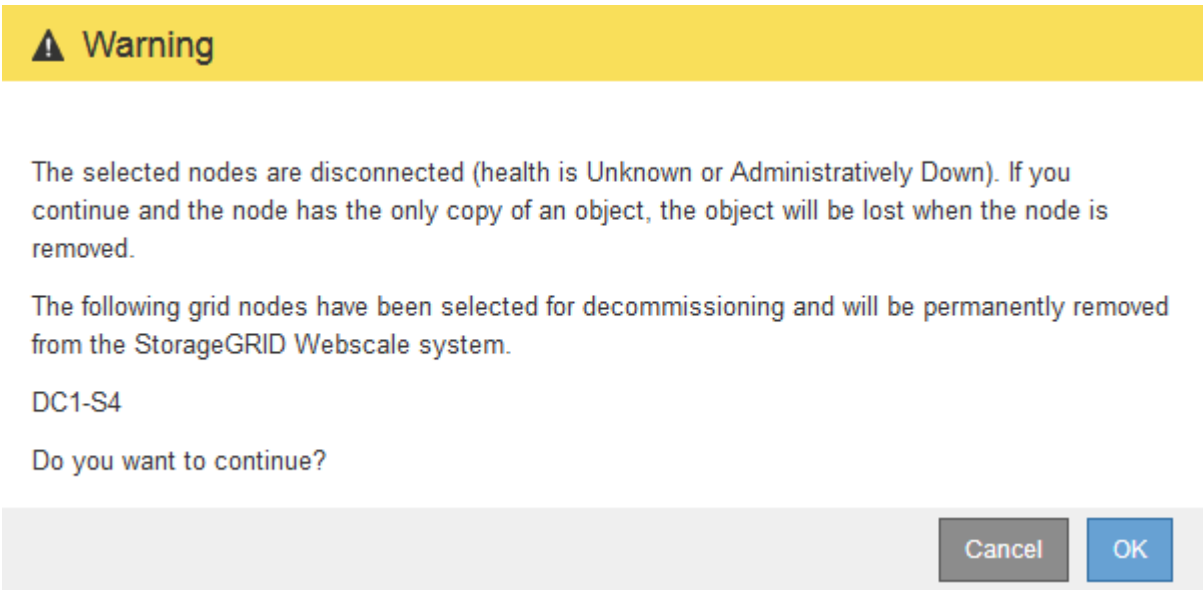
> 연결이 끊긴 여러 스토리지 노드를 선택하는 경우, 한 번에 둘 이상의 그리드 노드 해제를 선택할 때는 특히 주의해야 합니다. 복구할 수 없는 스토리지 노드가 두 개 이상 연결되어 있는 경우 기술 지원 부서에 문의하여 최상의 조치 방법을 확인하십시오.

3. 프로비저닝 암호를 입력합니다.

   서비스 해제 시작 * 버튼이 활성화됩니다.

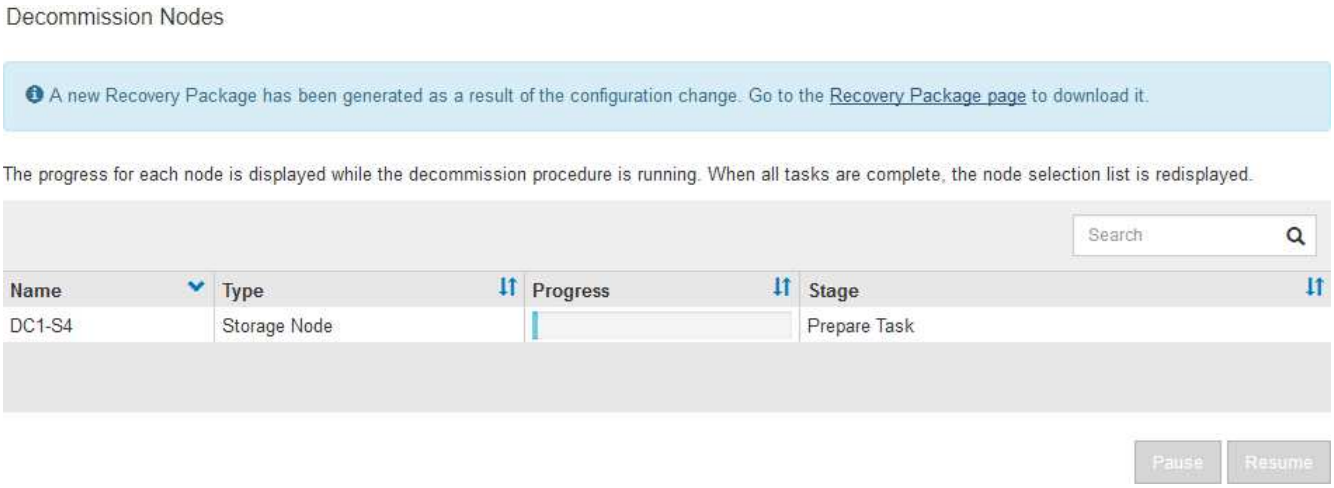
4. 서비스 해제 시작 * 을 클릭합니다.

   연결이 끊긴 노드를 선택했으며 노드에 개체의 복사본만 있는 경우 개체 데이터가 손실된다는 경고가 나타납니다.



5. 노드 목록을 검토하고 * OK * 를 클릭합니다.

   서비스 해제 절차가 시작되고 각 노드에 대한 진행률이 표시됩니다. 절차 중에 그리드 구성 변경을 포함하는 새 복구 패키지가 생성됩니다.



6. 새 복구 패키지를 사용할 수 있게 되면 링크를 클릭하거나 * 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택하여 복구 패키지 페이지에 액세스합니다. 그런 다음 .zip 파일을 다운로드합니다.

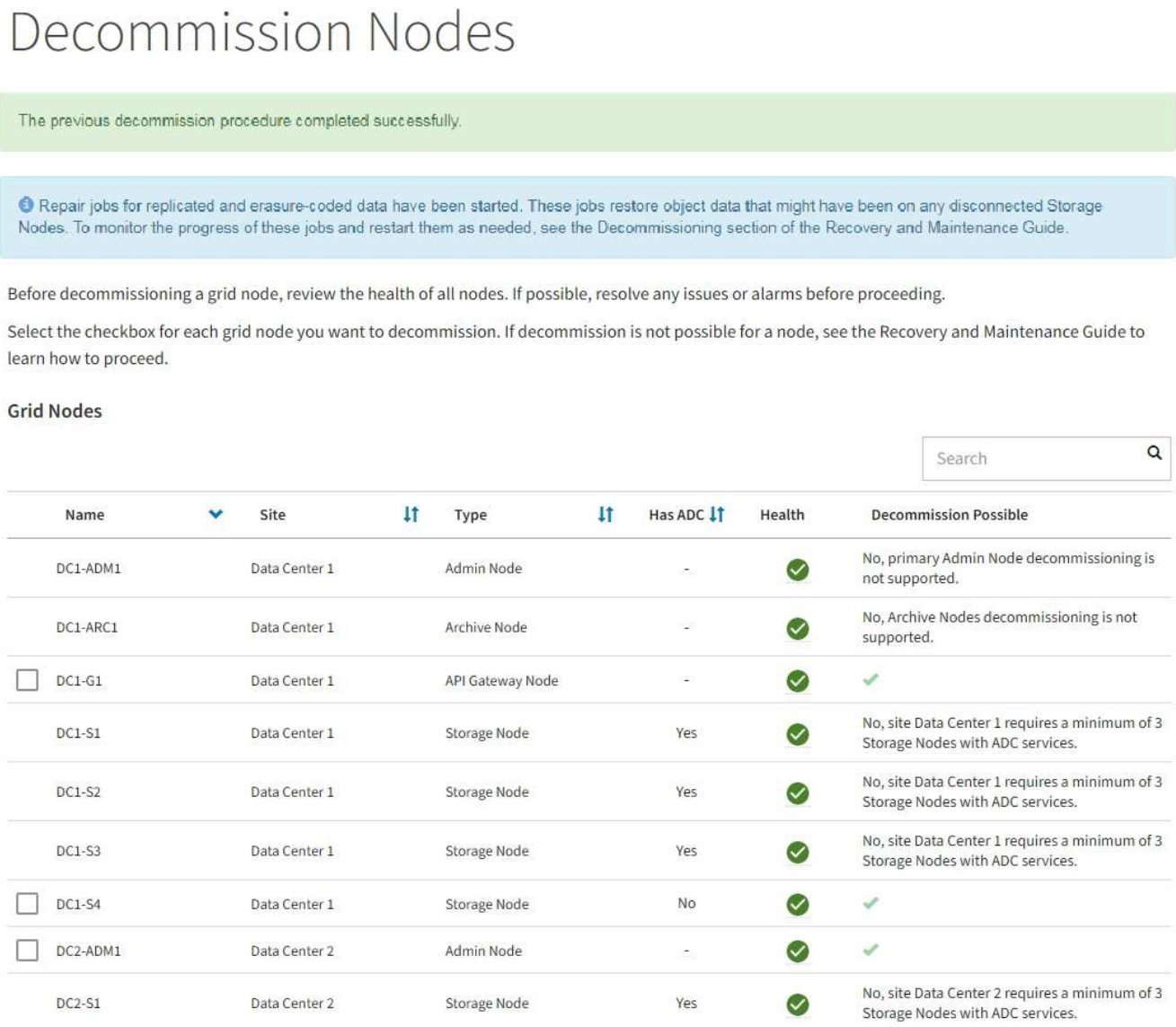
의 지침을 참조하십시오 복구 패키지 다운로드 중.

> 서비스 해제 절차 중에 문제가 발생할 경우 그리드를 복구할 수 있도록 가능한 한 빨리 복구 패키지를 다운로드하십시오.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

7. 서비스 해제 페이지를 주기적으로 모니터링하여 선택한 모든 노드가 성공적으로 폐기되었는지 확인합니다.

   스토리지 노드의 사용을 해제하는 데 며칠 또는 몇 주가 걸릴 수 있습니다. 모든 작업이 완료되면 노드 선택 목록이 성공 메시지와 함께 다시 표시됩니다. 분리된 스토리지 노드를 폐기한 경우 복구 작업이 시작되었다는 정보 메시지가 표시됩니다.



8. 서비스 해제 절차의 일부로 노드가 자동으로 종료된 후 나머지 가상 머신 또는 사용 중지된 노드와 관련된 기타 리소스를 제거합니다.

> 노드가 자동으로 종료될 때까지 이 단계를 수행하지 마십시오.

9. 스토리지 노드를 폐기하는 경우 서비스 해제 프로세스 중에 자동으로 시작되는 * 복제된 데이터 * 및 * 삭제 코딩(EC) 데이터 * 복구 작업의 상태를 모니터링합니다.

복제된 데이터

- 수리가 완료되었는지 확인하려면:
  a. 노드 * > * _ 복구되는 스토리지 노드 _ * > * ILM * 을 선택합니다.
  b. 평가 섹션의 속성을 검토합니다. 복구가 완료되면 * Awaiting-all * 속성이 0 개체를 나타냅니다.
- 수리를 더 자세히 모니터링하려면:
  a. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
  b. 복구되는 **GRID* * > *_Storage Node _ * > * LDR * > * Data Store * 를 선택합니다.
  c. 복제된 수리가 완료된 경우 다음 특성을 조합하여 가능한 한 결정합니다.

    Cassandra의 일관성이 없을 수 있으며, 복구 실패를 추적하지 않습니다.

    - * 시도된 복구(XRPA) **:** 이 속성을 사용하여 복제된 복구 진행률을 추적합니다**.** 이 속성은 스토리지 노드가 고위험 객체를 복구하려고 할 때마다 증가합니다**.** 이 속성이 현재 스캔 기간**(** Scan Period — Estimated* 속성 제공)보다 더 긴 기간 동안 증가하지 않으면 ILM 스캐닝에서 모든 노드에서 복구해야 할 고위험 개체를 찾지 못한 것입니다.

      고위험 개체는 완전히 손실될 위험이 있는 개체입니다. ILM 구성을 충족하지 않는 개체는 포함되지 않습니다.

    - * 스캔 기간 — 예상(XSCM) *: 이 속성을 사용하여 이전에 수집된 개체에 정책 변경이 적용되는 시점을 추정합니다. 복구 시도 * 속성이 현재 스캔 기간보다 긴 기간 동안 증가하지 않으면 복제된 수리가 수행될 수 있습니다. 스캔 기간은 변경될 수 있습니다. 스캔 기간 — 예상(XSCM) * 속성은 전체 그리드에 적용되며 모든 노드 스캔 기간의 최대값입니다. 그리드에 대한 * Scan Period — Estimated * 속성 기록을 조회하여 적절한 기간을 결정할 수 있습니다.
- 필요에 따라 복제된 복구에 대한 예상 완료율을 얻으려면 repair-data 명령에 'show-replicated-repair-status' 옵션을 추가합니다.

  REpair-data show-replicated-repair-status'를 참조하십시오

  StorageGRID 11.6의 기술 미리 보기에는 '복제된-수리-상태' 옵션이 제공됩니다. 이 기능은 개발 중이며 반환된 값이 잘못되었거나 지연될 수 있습니다. 수리가 완료되었는지 확인하려면 에 설명된 대로 * Awaiting – All *, * repair attemptated (XRPA) * 및 * Scan Period — Estimated (XSCM) * 를 사용합니다 수리 모니터링.

삭제 코딩**(EC)** 데이터

삭제 코딩 데이터의 복구를 모니터링하고 실패한 요청을 다시 시도하려면 다음을 수행하십시오.

1. 삭제 코딩 데이터 복구 상태를 확인합니다.
   - 현재 작업의 예상 완료 시간과 완료 비율을 보려면 * 지원 * > * 도구 * > * 메트릭 * 을 선택합니다. 그런 다음 Grafana 섹션에서 * EC 개요 * 를 선택합니다. Grid EC Job Ec Job Estimated Time to Completion * 및 * Grid EC Job Percentage Completed * 대시보드를 확인합니다.
   - 특정 repair-data 작업의 상태를 확인하려면 다음 명령을 사용합니다.

     REpair-data show -ec-repair-status—repair-id repair ID'를 참조하십시오

- 이 명령을 사용하여 모든 수리를 나열합니다.

  Repair-data show-ec-repair-status'를 참조하십시오

이 출력에는 현재 실행 중인 모든 수리에 대한 "재쌍 ID"를 포함한 정보가 나열됩니다.

2. 출력에 복구 작업이 실패한 것으로 표시되면 '--repair-id' 옵션을 사용하여 복구를 다시 시도합니다.

   이 명령은 복구 ID 6949309319275667690을 사용하여 장애가 발생한 노드 복구를 재시도합니다.

   REpair-data start-ec-node-repair—repair-id 6949309319275667690

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 볼륨 복구를 재시도합니다.

   REpair-data start-ec-volume-repair—repair-id 6949309319275667690

작업을 마친 후

연결이 끊긴 노드를 폐기하고 모든 데이터 복구 작업이 완료되는 즉시 연결된 모든 그리드 노드를 필요에 따라 해제할 수 있습니다.

그런 다음 서비스 해제 절차를 완료한 후 다음 단계를 완료합니다.

- 해체된 그리드 노드의 드라이브가 깨끗하게 지워졌는지 확인합니다. 상용 데이터 삭제 도구 또는 서비스를 사용하여 드라이브에서 데이터를 영구적으로 안전하게 제거합니다.
- 어플라이언스 노드를 폐기했고 어플라이언스의 데이터가 노드 암호화를 사용하여 보호된 경우 StorageGRID 어플라이언스 설치 프로그램을 사용하여 키 관리 서버 구성을 지웁니다(KMS 지우기). 다른 그리드에 어플라이언스를 추가하려면 KMS 구성을 지워야 합니다.
  - SG100 및 SG1000 서비스 어플라이언스
  - SG5600 스토리지 어플라이언스
  - SG5700 스토리지 어플라이언스
  - SG6000 스토리지 어플라이언스

관련 정보

그리드 노드 복구 절차

연결된 그리드 노드 해제

그리드에 연결된 노드를 사용 중지하고 영구적으로 제거할 수 있습니다.

- 요구사항과 을 이해해야 합니다 그리드 노드 폐기에 대한 고려 사항.
- 필요한 모든 자료를 수집해야 합니다.
- 활성화된 데이터 복구 작업이 없도록 해야 합니다.
- 스토리지 노드 복구가 그리드의 어느 곳에서든 진행 중이 아닌 것을 확인해야 합니다. 있는 경우 복구 과정에서 Cassandra 재구축이 완료될 때까지 기다려야 합니다. 그런 다음 해체 작업을 진행할 수 있습니다.
- 노드 서비스 해제 절차가 일시 중지되지 않는 한 노드 서비스 해제 절차가 실행되는 동안 다른 유지 보수 절차가 실행되지 않도록 해야 합니다.

- 프로비저닝 암호가 있어야 합니다.
- 그리드 노드가 연결되어 있습니다.
- 서비스 해제하려는 노드에 대한 * 서비스 해제 가능 * 열에 녹색 확인 표시가 있어야 합니다.
- 모든 그리드 노드에는 정상(녹색) 상태가 있어야 합니다 . 상태 * 열에 이러한 아이콘 중 하나가 표시되면 문제를 해결해야 합니다.

아이콘을 클릭합니다	색상	심각도입니다
	노란색	주의
	연한 주황색	경미합니다
	진한 주황색	전공
	빨간색	심각

- 이전에 분리된 스토리지 노드를 폐기한 경우 데이터 복구 작업이 모두 성공적으로 완료된 것입니다. 을 참조하십시오 데이터 복구 작업을 확인합니다.

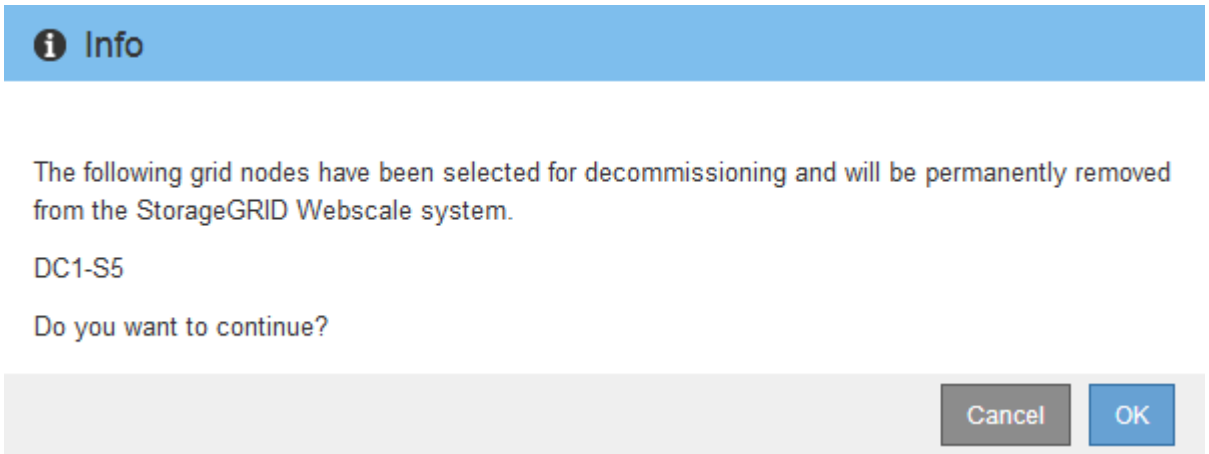
> 이 절차에서 지시될 때까지 그리드 노드의 가상 머신 또는 기타 리소스를 제거하지 마십시오.

1. 서비스 해제 노드 페이지에서 서비스 해제할 각 그리드 노드에 대한 확인란을 선택합니다.
2. 프로비저닝 암호를 입력합니다.

   서비스 해제 시작 * 버튼이 활성화됩니다.

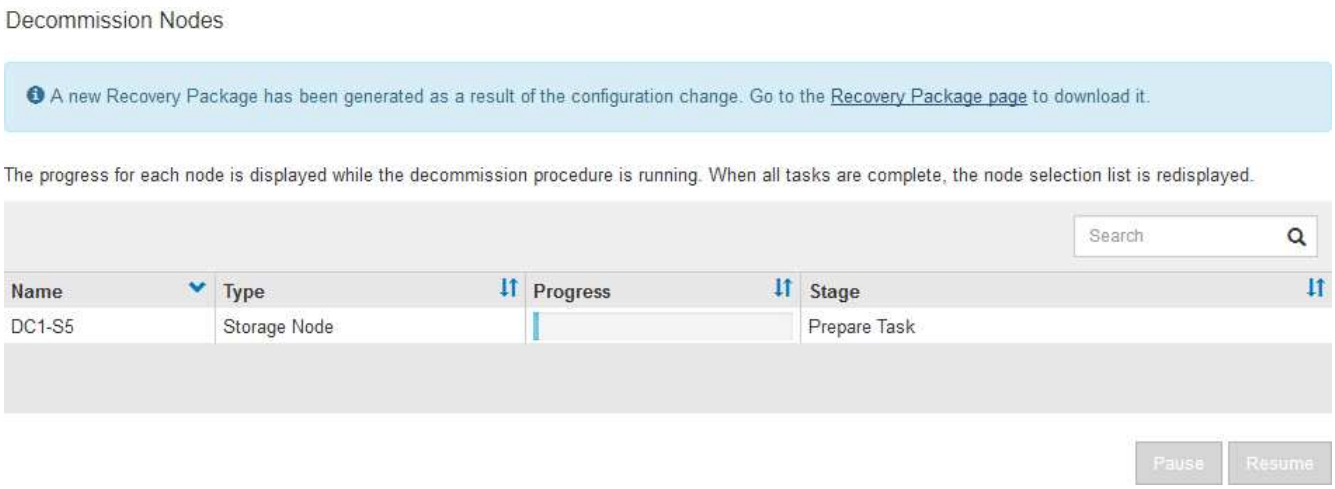
3. 서비스 해제 시작 * 을 클릭합니다.

   확인 대화 상자가 나타납니다.



4. 선택한 노드 목록을 검토하고 * OK * 를 클릭합니다.

노드 서비스 해제 절차가 시작되고 각 노드에 대한 진행률이 표시됩니다. 절차 중에 그리드 구성 변경 사항을 표시하기 위해 새 복구 패키지가 생성됩니다.



> 서비스 해제 절차가 시작된 후에는 스토리지 노드를 오프라인 상태로 전환하지 마십시오. 상태를 변경하면 일부 콘텐츠가 다른 위치에 복사되지 않을 수 있습니다.

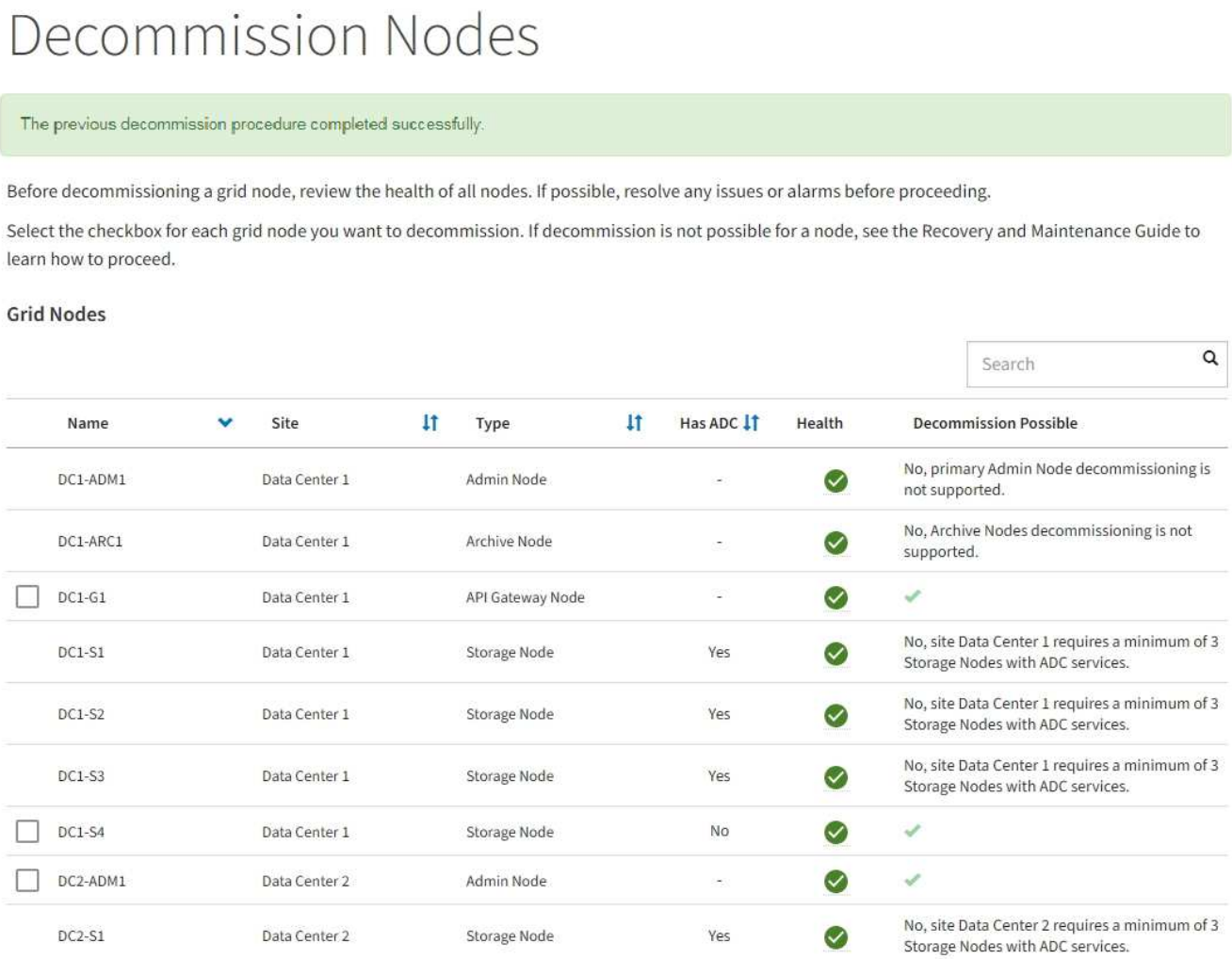
5. 새 복구 패키지를 사용할 수 있게 되면 링크를 클릭하거나 * 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택하여 복구 패키지 페이지에 액세스합니다. 그런 다음 .zip 파일을 다운로드합니다.

   의 지침을 참조하십시오 복구 패키지 다운로드 중.

   > 서비스 해제 절차 중에 문제가 발생할 경우 그리드를 복구할 수 있도록 가능한 한 빨리 복구 패키지를 다운로드하십시오.

6. 서비스 해제 노드 페이지를 주기적으로 모니터링하여 선택한 모든 노드가 성공적으로 폐기되었는지 확인합니다.

   스토리지 노드의 사용을 해제하는 데 며칠 또는 몇 주가 걸릴 수 있습니다. 모든 작업이 완료되면 노드 선택 목록이 성공 메시지와 함께 다시 표시됩니다.



7. 플랫폼에 맞는 적절한 단계를 따릅니다. 예를 들면 다음과 같습니다.
   - Linux *: 설치 중에 생성한 노드 구성 파일을 삭제하고 볼륨을 분리할 수 있습니다.
   - * VMware *: vCenter "Delete from Disk" 옵션을 사용하여 가상 머신을 삭제할 수 있습니다. 또한 가상 머신과 독립적인 데이터 디스크를 삭제해야 할 수도 있습니다.
   - **StorageGRID** 어플라이언스: 어플라이언스 노드는 StorageGRID 어플라이언스 설치 프로그램에 액세스할 수 있는 배포되지 않은 상태로 자동으로 돌아갑니다. 제품의 전원을 끄거나 다른 StorageGRID 시스템에 추가할 수 있습니다.

노드 사용 중단 절차를 완료한 후 다음 단계를 완료합니다.

- 해체된 그리드 노드의 드라이브가 깨끗하게 지워졌는지 확인합니다. 상용 데이터 삭제 도구 또는 서비스를 사용하여 드라이브에서 데이터를 영구적으로 안전하게 제거합니다.
- 어플라이언스 노드를 폐기했고 어플라이언스의 데이터가 노드 암호화를 사용하여 보호된 경우 StorageGRID 어플라이언스 설치 프로그램을 사용하여 키 관리 서버 구성을 지웁니다(KMS 지우기). 다른 격자에서 제품을 사용하려면 KMS 구성을 지워야 합니다.

  SG100 및 SG1000 서비스 어플라이언스

  SG5600 스토리지 어플라이언스

  SG5700 스토리지 어플라이언스

SG6000 스토리지 어플라이언스

관련 정보

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

스토리지 노드에 대한 서비스 해제 프로세스를 일시 중지하고 다시 시작합니다

두 번째 유지 보수 절차를 수행해야 하는 경우 특정 단계에서 스토리지 노드에 대한 서비스 해제 절차를 일시 중지할 수 있습니다. 다른 절차가 완료된 후 서비스 해제를 재개할 수 있습니다.

> ILM 평가 또는 삭제 코딩 데이터 사용 중단 단계에 도달한 경우에만 * 일시 중지 * 버튼이 활성화됩니다. 그러나 ILM 평가(데이터 마이그레이션)는 백그라운드에서 계속 실행됩니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.

단계

1. 유지 관리 * > * 작업 * > * 서비스 해제 * 를 선택합니다.

   서비스 해제 페이지가 나타납니다.

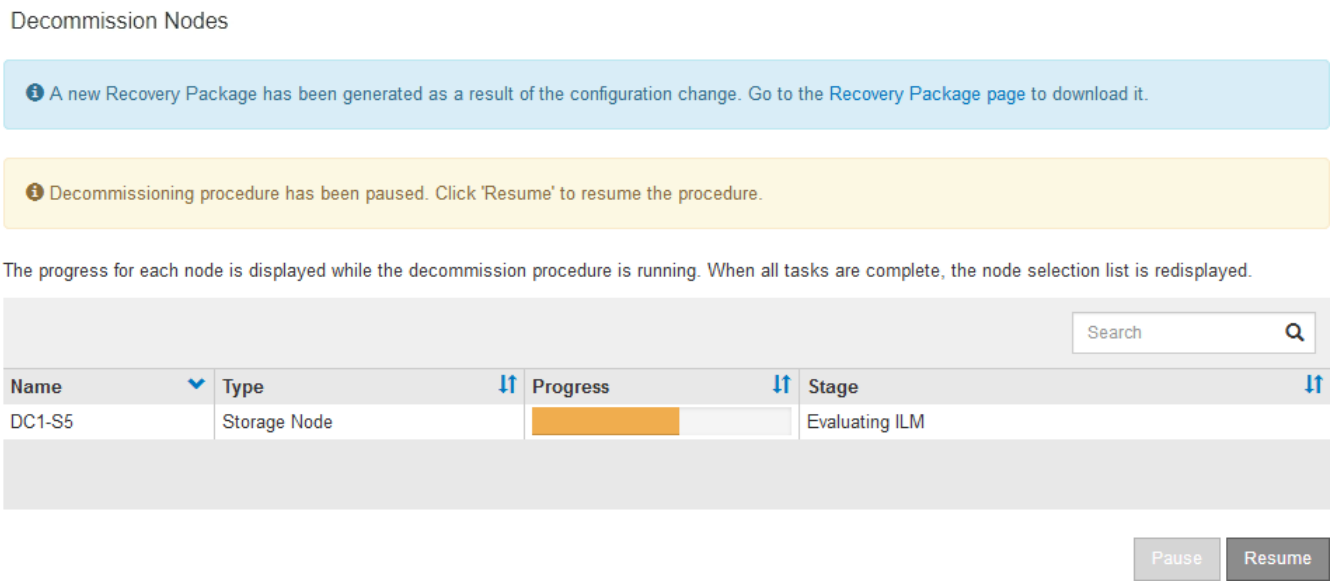
2. 서비스 해제 노드 * 를 선택합니다.

   서비스 해제 노드 페이지가 나타납니다. 서비스 해제 절차가 다음 단계 중 하나에 도달하면 * Pause * (일시 중지 *) 버튼이 활성화됩니다.

   - ILM 평가 중
   - 삭제 코딩 데이터 해제

3. 절차를 일시 중지하려면 * Pause * 를 선택합니다.

   현재 단계가 일시 중지되고 * Resume * 버튼이 활성화됩니다.



4. 다른 유지보수 절차가 완료된 후 서비스 해제를 진행하려면 * Resume * 을 선택하십시오.

노드 사용 중단 문제 해결

오류로 인해 노드 서비스 해제 절차가 중지되는 경우 특정 단계를 수행하여 문제를 해결할 수 있습니다.

필요한 것

를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

이 작업에 대해

사용 중단 중인 그리드 노드를 종료하면 그리드 노드가 다시 시작될 때까지 작업이 중지됩니다. 그리드 노드는 온라인이어야 합니다.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. 그리드 토폴로지 트리에서 각 스토리지 노드 항목을 확장하고 DDS 및 LDR 서비스가 모두 온라인 상태인지 확인합니다.

   스토리지 노드 폐기를 수행하려면 온라인 노드/사이트 서비스 해제 시작 시 모든 노드와 서비스가 정상 상태가 되어야 합니다.

3. 활성 그리드 작업을 보려면 * 기본 관리자 노드 * > * CMN * > * 그리드 작업 * > * 개요 * 를 선택합니다.
4. 서비스 해제 그리드 작업의 상태를 확인합니다.

   a. 해체 그리드 작업의 상태가 그리드 작업 번들을 저장하는 데 문제가 있으면 * 기본 관리 노드 * > * CMN * > * 이벤트 * > * 개요 * 를 선택합니다
   b. 사용 가능한 감사 릴레이 수를 확인합니다.

      사용 가능한 감사 릴레이 속성이 하나 이상인 경우 CMN 서비스는 하나 이상의 ADC 서비스에 연결됩니다. ADC 서비스는 감사 릴레이 역할을 합니다.

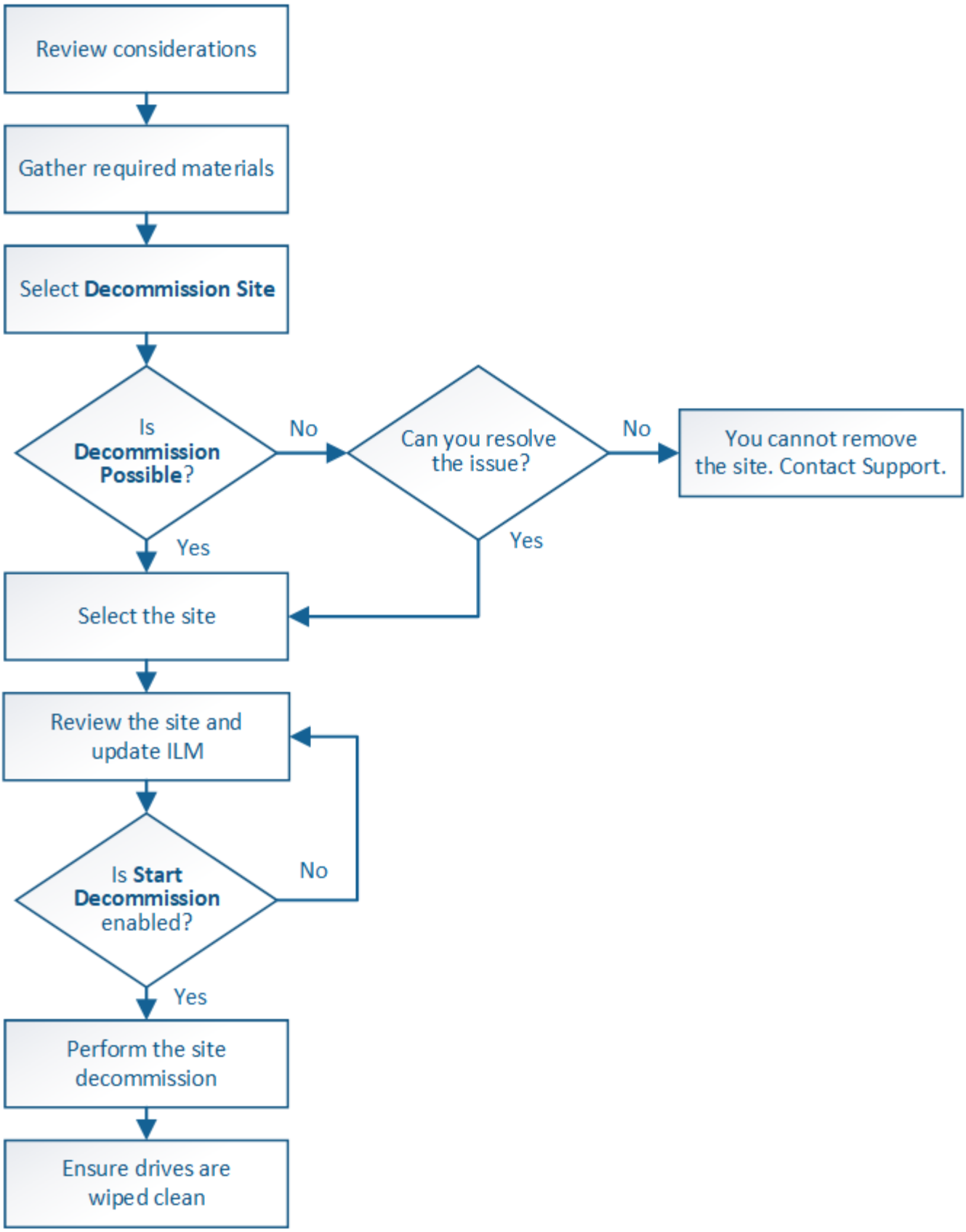
   CMN 서비스는 하나 이상의 ADC 서비스에 연결되어 있어야 하며 그리드 작업이 폐기 단계 간에 이동하고 완료될 수 있도록 StorageGRID 시스템의 ADC 서비스 중 과반수(50% + 1)를 사용할 수 있어야 합니다.

   a. CMN 서비스가 충분한 ADC 서비스에 연결되어 있지 않으면 스토리지 노드가 온라인 상태인지 확인하고 기본 관리 노드와 스토리지 노드 간의 네트워크 연결을 확인합니다.

사이트 파기

StorageGRID 시스템에서 데이터 센터 사이트를 제거해야 할 수 있습니다. 사이트를 제거하려면 사이트를 해제해야 합니다.

흐름도는 사이트 해체를 위한 상위 단계를 보여줍니다.



사이트 제거 고려 사항

사이트 서비스 해제 절차를 사용하여 사이트를 제거하기 전에 고려 사항을 검토해야 합니다.

사이트 서비스 해제 시 수행되는 작업

사이트를 서비스 해제할 경우 StorageGRID는 사이트의 모든 노드를 영구적으로 제거하고 StorageGRID 시스템에서 사이트 자체를 제거합니다.

사이트 서비스 해제 절차가 완료되면 다음을 수행합니다.

- 더 이상 StorageGRID를 사용하여 사이트의 사이트 또는 노드를 보거나 액세스할 수 없습니다.
- 더 이상 사이트를 참조하는 스토리지 풀 또는 삭제 코딩 프로필을 사용할 수 없습니다. StorageGRID에서 사이트의 압축을 풀 경우 해당 스토리지 풀이 자동으로 제거되고 이러한 삭제 코딩 프로필이 비활성화됩니다.

연결된 사이트와 분리된 사이트 파기 절차의 차이점

사이트 서비스 해제 절차를 사용하여 모든 노드가 StorageGRID에 연결된 사이트(연결된 사이트 서비스 해제라고 함)를 제거하거나 모든 노드가 StorageGRID에서 분리된 사이트(연결이 끊긴 사이트 서비스 해제라고 함)를 제거할 수 있습니다. 시작하기 전에 이러한 절차 간의 차이점을 이해해야 합니다.

> 사이트에 연결된( ) 및 연결되지 않은 노드(또는), 모든 오프라인 노드를 다시 온라인 상태로 전환해야 합니다.

- 연결된 사이트 파기를 사용하면 StorageGRID 시스템에서 운영 사이트를 제거할 수 있습니다. 예를 들어, 연결된 사이트 파기를 수행하여 더 이상 필요하지 않은 사이트를 제거할 수 있습니다.
- StorageGRID에서 연결된 사이트를 제거하면 ILM을 사용하여 사이트의 개체 데이터를 관리합니다. 연결된 사이트 서비스 해제를 시작하려면 먼저 모든 ILM 규칙에서 사이트를 제거하고 새 ILM 정책을 활성화해야 합니다. ILM 프로세스를 통해 개체 데이터를 마이그레이션하고 사이트 제거를 위한 내부 프로세스를 동시에 수행할 수 있지만, 실제 서비스 해제 절차를 시작하기 전에 ILM 단계를 완료할 수 있는 것이 가장 좋습니다.
- 연결이 끊어진 사이트 파기를 사용하면 장애가 발생한 사이트를 StorageGRID 시스템에서 제거할 수 있습니다. 예를 들어, 분리된 사이트 파기를 수행하여 화재나 홍수로 인해 파괴된 사이트를 제거할 수 있습니다.

  StorageGRID가 연결이 끊긴 사이트를 제거하면 모든 노드를 복구할 수 없다고 간주되어 데이터 보존을 시도하지 않습니다. 그러나 연결이 끊긴 사이트 해제를 시작하려면 먼저 모든 ILM 규칙에서 사이트를 제거하고 새 ILM 정책을 활성화해야 합니다.

  > 연결이 끊긴 사이트 서비스 해제 절차를 수행하기 전에 NetApp 어카운트 담당자에게 문의하십시오. NetApp은 서비스 해제 사이트 마법사의 모든 단계를 활성화하기 전에 요구사항을 검토합니다. 연결이 끊긴 사이트 서비스 해제를 시도해서는 안 됩니다. 사이트를 복구하거나 사이트에서 오브젝트 데이터를 복구할 수 있다고 생각되면 사이트 서비스 해제를 시도해서는 안 됩니다.

연결된 사이트 또는 분리된 사이트 제거에 대한 일반 요구 사항

연결 또는 분리된 사이트를 제거하기 전에 다음 요구 사항을 숙지해야 합니다.

- 기본 관리 노드를 포함하는 사이트는 서비스 해제할 수 없습니다.
- 보관 노드를 포함하는 사이트는 해제할 수 없습니다.
- HA(고가용성) 그룹에 속한 인터페이스가 있는 노드는 사이트 서비스를 해제할 수 없습니다. 노드의 인터페이스를 제거하거나 전체 HA 그룹을 제거하려면 HA 그룹을 편집해야 합니다.
- 연결된( ) 및 연결 끊김(또는) 노드.

- 다른 사이트의 노드 연결이 끊어진 경우 사이트 서비스를 해제할 수 없습니다(또는)를 클릭합니다.
- EC 노드 복구 작업이 진행 중인 경우에는 사이트 서비스 해제 절차를 시작할 수 없습니다. 을 참조하십시오 데이터 복구 작업을 확인합니다 삭제 코딩 데이터의 복구를 추적합니다.
- 사이트 서비스 해제 절차가 실행되는 동안 다음을 수행합니다.
  - 폐기되는 사이트를 참조하는 ILM 규칙을 생성할 수 없습니다. 사이트를 참조하기 위해 기존 ILM 규칙을 편집할 수도 없습니다.
  - 확장 또는 업그레이드와 같은 다른 유지보수 절차는 수행할 수 없습니다.

    연결된 사이트의 서비스 해제 중에 다른 유지보수 절차를 수행해야 하는 경우 다음을 수행할 수 있습니다 스토리지 노드를 제거하는 동안 절차를 일시 중지합니다. ILM 평가 또는 삭제 코딩 데이터 사용 중단 단계에 도달한 경우에만 * 일시 중지 * 버튼이 활성화됩니다. 그러나 ILM 평가(데이터 마이그레이션)는 백그라운드에서 계속 실행됩니다. 두 번째 유지 보수 절차가 완료되면 서비스 해제를 재개할 수 있습니다.

  - 사이트 서비스 해제 절차를 시작한 후 노드를 복구해야 하는 경우 지원 팀에 문의해야 합니다.
- 한 번에 두 개 이상의 사이트를 해제할 수 없습니다.
- 사이트에 하나 이상의 관리 노드가 포함되어 있고 StorageGRID 시스템에 대해 SSO(Single Sign-On)가 활성화되어 있는 경우 AD FS(Active Directory Federation Services)에서 사이트에 대한 모든 신뢰할 수 있는 상대 트러스트를 제거해야 합니다.

ILM(정보 수명 주기 관리)에 대한 요구 사항

사이트를 제거하는 과정에서 ILM 구성을 업데이트해야 합니다. 서비스 해제 사이트 마법사는 다음을 보장하기 위한 여러 필수 단계를 안내합니다.

- 활성 ILM 정책에 의해 사이트가 참조되지 않습니다. 새 ILM 규칙을 사용하여 새 ILM 정책을 만들고 활성화해야 합니다.
- 제안된 ILM 정책이 없습니다. 제안된 정책이 있는 경우 삭제해야 합니다.
- 활성 또는 제안된 정책에서 이러한 규칙이 사용되지 않는 경우에도 ILM 규칙이 사이트를 참조하지 않습니다. 사이트를 참조하는 모든 규칙을 삭제하거나 편집해야 합니다.

StorageGRID에서 사이트의 압축을 풀 경우 해당 사이트를 참조하는 사용되지 않는 삭제 코딩 프로필이 자동으로 비활성화되고, 해당 사이트를 참조하는 사용되지 않은 스토리지 풀이 자동으로 삭제됩니다. 시스템 기본 모든 스토리지 노드 스토리지 풀은 모든 사이트를 사용하므로 제거됩니다.

사이트를 제거하기 전에 새 ILM 규칙을 생성하고 새 ILM 정책을 활성화해야 할 수 있습니다. 이러한 지침에서는 ILM의 작동 방식과 스토리지 풀 생성, 삭제 코딩 프로필, ILM 규칙 및 ILM 정책 시뮬레이션 및 활성화에 대해 잘 알고 있다고 가정합니다. 정보 수명 주기 관리를 사용하여 개체를 관리하는 방법에 대한 지침을 참조하십시오.

ILM을 사용하여 개체를 관리합니다

연결된 사이트의 개체 데이터에 대한 고려 사항

연결된 사이트 파기를 수행하는 경우 새 ILM 규칙 및 새 ILM 정책을 생성할 때 사이트에서 기존 오브젝트 데이터를 사용하여 수행할 작업을 결정해야 합니다. 다음 중 하나 또는 모두를 수행할 수 있습니다.

- 선택한 사이트에서 눈금의 다른 사이트 하나 이상으로 개체 데이터를 이동합니다.
- 데이터 이동의 예 *: 서니베일에 새 사이트를 추가했기 때문에 Raleigh에서 사이트의 운영을 중단한다고 가정합니다. 이 예제에서는 모든 개체 데이터를 이전 사이트에서 새 사이트로 이동하려고 합니다. ILM 규칙 및 ILM 정책을 업데이트하기 전에 두 사이트 모두에서 용량을 검토해야 합니다. Saleigh 사이트의 오브젝트 데이터를 수용할 수 있는 충분한 용량이 Sunnyvale 사이트에 있는지, 그리고 향후 성장을 위해 적절한 용량이 Sunnyvale에 남아 있는지 확인해야 합니다.

> 적절한 용량을 사용하려면 이 절차를 수행하기 전에 스토리지 볼륨 또는 스토리지 노드를 기존 사이트에 추가하거나 새 사이트를 추가해야 할 수 있습니다. StorageGRID 시스템 확장 지침을 참조하십시오.

- 선택한 사이트에서 개체 복사본을 삭제합니다.
- 데이터 삭제 예 *: 현재 3개 복사본 ILM 규칙을 사용하여 3개 사이트 간에 오브젝트 데이터를 복제한다고 가정합니다. 사이트를 폐기하기 전에 2개 복사본 ILM 규칙을 생성하여 단 2개의 사이트에 데이터를 저장할 수 있습니다. 2-copy 규칙을 사용하는 새로운 ILM 정책을 활성화하면 StorageGRID은 해당 복사본이 더 이상 ILM 요구사항을 충족하지 않기 때문에 세 번째 사이트에서 삭제됩니다. 그러나 개체 데이터는 계속 보호되고 나머지 두 사이트의 용량은 동일하게 유지됩니다.

> 사이트 제거를 수용하기 위해 단일 복사본 ILM 규칙을 만들지 마십시오. 특정 기간 동안 복제된 복사본을 하나만 생성하는 ILM 규칙은 데이터가 영구적으로 손실될 위험이 있습니다. 복제된 객체 복제본이 하나만 있는 경우 스토리지 노드에 장애가 발생하거나 심각한 오류가 발생한 경우 해당 객체가 손실됩니다. 또한 업그레이드와 같은 유지보수 절차 중에는 개체에 대한 액세스가 일시적으로 중단됩니다.

연결된 사이트 파기 추가 요구 사항

StorageGRID에서 연결된 사이트를 제거하려면 먼저 다음 사항을 확인해야 합니다.

- StorageGRID 시스템의 모든 노드에는 * 연결됨 * (의 연결 상태가 있어야 합니다). 그러나 노드에 활성 경고가 있을 수 있습니다.

> 하나 이상의 노드의 연결이 끊어진 경우 사이트 서비스 해제 마법사의 1-4단계를 완료할 수 있습니다. 그러나 모든 노드가 연결되어 있지 않으면 서비스 해제 프로세스를 시작하는 마법사의 5단계를 완료할 수 없습니다.

- 제거하려는 사이트에 로드 밸런싱에 사용되는 게이트웨이 노드 또는 관리 노드가 포함된 경우 확장 절차를 수행하여 다른 사이트에 이와 동등한 새 노드를 추가해야 할 수 있습니다. 사이트 서비스 해제 절차를 시작하기 전에 클라이언트가 교체 노드에 연결할 수 있는지 확인하십시오.
- 제거하려는 사이트에 고가용성(HA) 그룹에 있는 게이트웨이 노드 또는 관리 노드가 있는 경우 사이트 서비스 해제 마법사의 1-4단계를 완료할 수 있습니다. 그러나 모든 HA 그룹에서 이러한 노드를 제거할 때까지 서비스 해제 프로세스를 시작하는 마법사의 5단계를 완료할 수 없습니다. 기존 클라이언트가 사이트의 노드가 포함된 HA 그룹에 연결할 경우 사이트가 제거된 후에도 StorageGRID에 계속 연결할 수 있는지 확인해야 합니다.
- 제거할 사이트의 스토리지 노드에 클라이언트가 직접 연결하는 경우 사이트 서비스 해제 절차를 시작하기 전에 클라이언트가 다른 사이트의 스토리지 노드에 연결할 수 있는지 확인해야 합니다.
- 활성 ILM 정책의 변경으로 인해 이동할 개체 데이터를 수용할 수 있는 충분한 공간을 나머지 사이트에 제공해야 합니다. 경우에 따라 연결된 사이트의 서비스 해제를 완료하기 전에 스토리지 노드, 스토리지 볼륨 또는 새 사이트를 추가하여 StorageGRID 시스템을 확장해야 할 수도 있습니다.

- 서비스 해제 절차를 완료하려면 적절한 시간이 필요합니다. StorageGRID ILM 프로세스를 사이트에 대한 서비스 중단 전에 사이트의 오브젝트 데이터를 이동하거나 삭제하는 데 며칠, 몇 주 또는 몇 달이 걸릴 수 있습니다.

> 사이트에서 오브젝트 데이터를 이동하거나 삭제하는 경우 사이트의 데이터 양, 시스템의 로드, 네트워크 지연 시간, 필요한 ILM의 특성 등에 따라 며칠, 몇 주 또는 몇 개월이 걸릴 수 있습니다.

- 가능한 한 빨리 서비스 해제 사이트 마법사의 1-4단계를 완료해야 합니다. 서비스 해제 절차는 실제 서비스 해제 절차를 시작하기 전에 사이트에서 데이터를 이동할 수 있도록 허용하면 더 빠르고 운영 중단과 성능에 미치는 영향이 줄어듭니다(마법사의 5단계에서 * 서비스 해제 시작 * 선택).

연결이 끊긴 사이트 폐기에 대한 추가 요구 사항

StorageGRID에서 분리된 사이트를 제거하려면 먼저 다음을 확인해야 합니다.

- NetApp 어카운트 담당자에게 문의했습니다. NetApp은 서비스 해제 사이트 마법사의 모든 단계를 활성화하기 전에 요구사항을 검토합니다.

> 연결이 끊긴 사이트 서비스 해제를 시도해서는 안 됩니다. 이 경우 사이트를 복구하거나 사이트에서 오브젝트 데이터를 복구할 수 있다고 판단됩니다.

- 사이트의 모든 노드에는 다음 중 하나의 연결 상태가 있어야 합니다.
  - 알 수 없음 * ( ) : 알 수 없는 이유로 노드가 그리드에 연결되어 있지 않습니다. 예를 들어, 노드 간 네트워크 연결이 끊어지거나 전원이 꺼졌습니다.
  - * 관리 아래 * ( ) : 노드가 예상 이유로 그리드에 연결되어 있지 않습니다. 예를 들어, 노드의 노드 또는 서비스가 정상적으로 종료되었습니다.
- 다른 모든 사이트의 모든 노드에는 연결 상태 * 연결됨 * (이(가) 있어야 합니다). 그러나 이러한 다른 노드에는 활성 경고가 있을 수 있습니다.
- StorageGRID를 사용하여 사이트에 저장된 개체 데이터를 더 이상 보거나 검색할 수 없다는 점을 이해해야 합니다. StorageGRID에서 이 절차를 수행할 때 연결이 끊긴 사이트의 데이터를 보존하려고 시도하지 않습니다.

> ILM 규칙 및 정책이 단일 사이트의 손실로부터 보호되도록 설계된 경우 남아 있는 개체에 대한 복사본이 유지됩니다.

- 사이트에 개체의 복사본만 포함되어 있으면 개체가 손실되어 검색할 수 없다는 점을 이해해야 합니다.

사이트를 제거할 때의 정합성 보장 컨트롤에 대한 고려 사항

S3 버킷 또는 Swift 컨테이너의 일관성 수준에 따라 StorageGRID가 오브젝트 메타데이터를 모든 노드 및 사이트에 완전히 복제한 후 클라이언트에 오브젝트 수집이 성공했음을 알리는 것이 결정됩니다. 일관성 제어를 통해 오브젝트의 가용성과 서로 다른 스토리지 노드 및 사이트 전체에서 이러한 오브젝트의 일관성 간의 균형을 유지할 수 있습니다.

StorageGRID에서 사이트를 제거할 때는 제거할 사이트에 데이터가 기록되지 않도록 해야 합니다. 따라서 각 버킷 또는 컨테이너의 정합성 보장 레벨을 일시적으로 재정의합니다. 사이트 서비스 해제 프로세스를 시작한 후 StorageGRID에서는 강력한 사이트 정합성을 일시적으로 사용하여 개체 메타데이터가 사이트에 기록되지 않도록 합니다.

이 임시 재정의의 결과로, 사이트 서비스 해제 중에 발생하는 모든 클라이언트 쓰기, 업데이트 및 삭제 작업은 나머지

사이트에서 여러 노드를 사용할 수 없게 될 경우 실패할 수 있습니다.

관련 정보

기술 지원 부서에서 사이트 복구를 수행하는 방법

ILM을 사용하여 개체를 관리합니다

그리드를 확장합니다

필요한 자료를 수집합니다

사이트를 해체하기 전에 다음 자료를 확보해야 합니다.

항목	참고
복구 패키지 '.zip' 파일	가장 최근의 복구 패키지 .zip 파일('GW-recovery-package-id-revision.zip')을 다운로드해야 합니다. 장애가 발생할 경우 복구 패키지 파일을 사용하여 시스템을 복원할 수 있습니다.
"passwords.txt" 파일	이 파일에는 명령줄에서 그리드 노드에 액세스하는 데 필요한 암호가 들어 있으며 복구 패키지에 포함되어 있습니다.
프로비저닝 암호	StorageGRID 시스템을 처음 설치할 때 암호가 생성되고 문서화됩니다. 프로비저닝 암호문은 passwords.txt 파일에 없습니다.
서비스 해제 전 StorageGRID 시스템의 토폴로지에 대한 설명입니다	가능한 경우 시스템의 현재 토폴로지를 설명하는 문서를 가져옵니다.

관련 정보

웹 브라우저 요구 사항

복구 패키지를 다운로드합니다

1단계**:** 사이트를 선택합니다

사이트를 해제할 수 있는지 확인하려면 서비스 해제 사이트 마법사에 액세스하여 시작합니다.

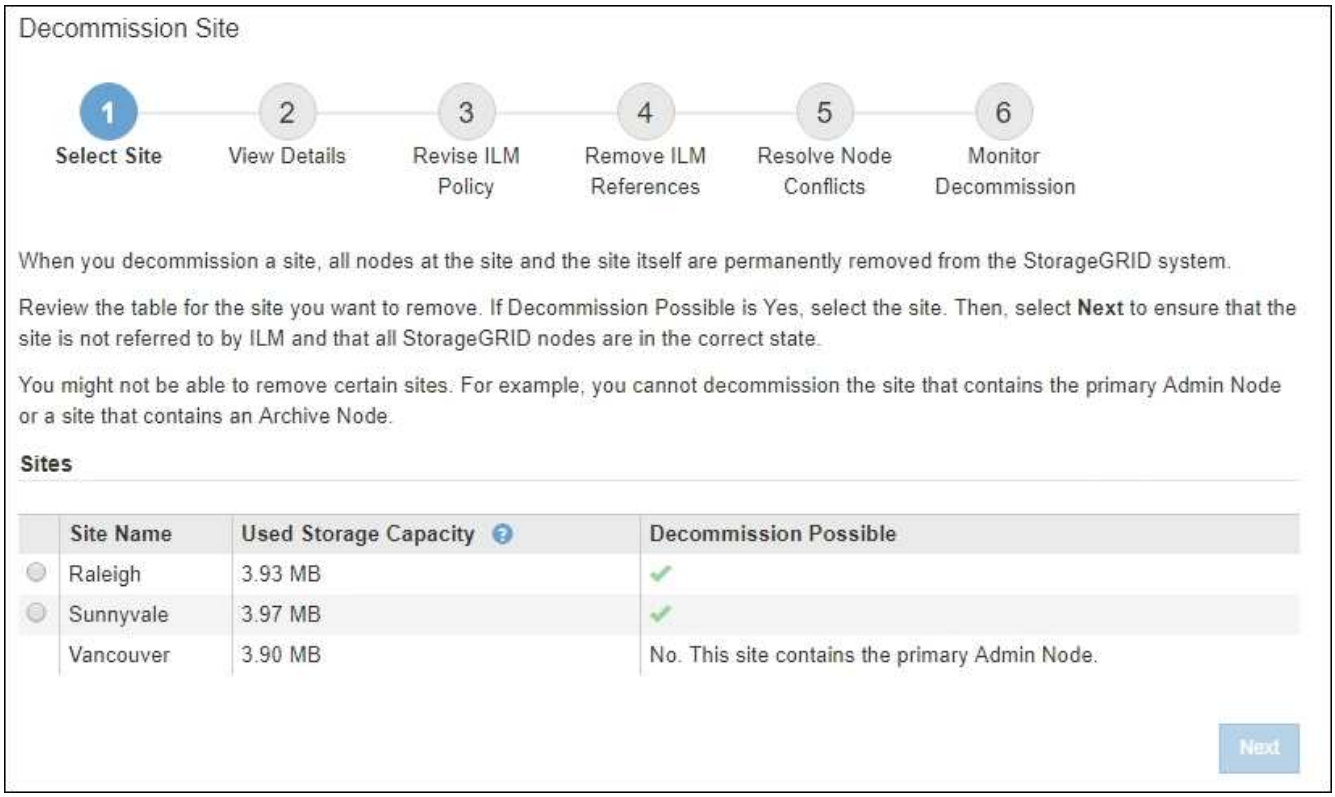
필요한 것

- 필요한 모든 자료를 확보해야 합니다.
- 사이트 제거 시 고려 사항을 검토해야 합니다.
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 루트 액세스 권한이나 유지 관리 및 ILM 권한이 있어야 합니다.

단계

1. 유지 관리 * > * 작업 * > * 서비스 해제 * 를 선택합니다.
2. 서비스 해제 사이트 * 를 선택합니다.

   사이트 서비스 해제 마법사의 1단계(사이트 선택)가 나타납니다. 이 단계는 StorageGRID 시스템에 있는 사이트의 알파벳 목록을 포함합니다.



3. Used Storage Capacity * 열의 값을 보고 각 사이트의 오브젝트 데이터에 현재 사용 중인 스토리지 용량을 확인합니다.

   사용된 스토리지 용량은 추정치입니다. 노드가 오프라인인 경우 사용된 스토리지 용량이 사이트에 대해 마지막으로 알려진 값입니다.

   - 연결된 사이트 서비스 해제의 경우 이 값은 이 사이트를 안전하게 서비스 해제하려면 먼저 다른 사이트로 이동하거나 ILM을 통해 삭제해야 하는 오브젝트 데이터의 양을 나타냅니다.
   - 연결이 끊긴 사이트 서비스 해제의 경우 이 값은 이 사이트를 서비스 해제할 때 시스템의 데이터 스토리지에 액세스할 수 없게 되는 양을 나타냅니다.

   ILM 정책을 통해 단일 사이트의 손실로부터 보호할 수 있다면 개체 데이터의 복사본이 나머지 사이트에 계속 존재해야 합니다.

4. [서비스 해제 가능성] * 열의 이유를 검토하여 현재 사용 중단될 수 있는 사이트를 확인합니다.

   사이트를 해체할 수 없는 이유가 두 가지 이상인 경우 가장 중요한 이유가 표시됩니다.

사용 중지 가능한 이유	설명	다음 단계
녹색 확인 표시( )	이 사이트의 서비스를 해제할 수 있습니다.	로 이동합니다 다음 단계.
아니요 이 사이트에는 기본 관리 노드가 포함되어 있습니다.	기본 관리자 노드가 포함된 사이트는 서비스 해제할 수 없습니다.	없음. 이 절차는 수행할 수 없습니다.
아니요 이 사이트에는 하나 이상의 아카이브 노드가 있습니다.	아카이브 노드가 포함된 사이트는 해제할 수 없습니다.	없음. 이 절차는 수행할 수 없습니다.
아니요 이 사이트의 모든 노드의 연결이 끊어졌습니다. NetApp 어카운트 담당자에게 문의하십시오.	사이트의 모든 노드가 연결되어 있지 않으면 연결된 사이트 서비스 해제를 수행할 수 없습니다( )를 클릭합니다.	연결이 끊긴 사이트 서비스 해제를 수행하려면 NetApp 계정 담당자에게 연락하여 해당 요구사항을 검토하고 나머지 서비스 해제 사이트 마법사를 활성화해야 합니다. • 중요 *: 사이트를 제거할 수 있도록 온라인 노드를 오프라인으로 전환하지 마십시오. 데이터가 손실됩니다.

이 예에서는 사이트가 3개인 StorageGRID 시스템을 보여 줍니다. 녹색 확인 표시( ) Raleigh 및 Sunnyvale 사이트의 경우 이러한 사이트의 서비스를 해제할 수 있음을 나타냅니다. 그러나 Vancouver 사이트에 기본 관리 노드가 포함되어 있으므로 서비스를 해제할 수 없습니다.

1. 서비스 해제가 가능한 경우 사이트의 라디오 버튼을 선택합니다.

   다음 * 버튼이 활성화됩니다.

2. 다음 * 을 선택합니다.

   2단계(세부 정보 보기)가 나타납니다.

2단계**:** 세부 정보 보기

서비스 해제 사이트 마법사의 2단계(세부 정보 보기)에서 사이트에 포함된 노드를 검토하고 각 스토리지 노드에서 사용된 공간의 양을 확인하고 그리드의 다른 사이트에서 사용 가능한 여유 공간의 양을 평가할 수 있습니다.

필요한 것

사이트를 해제하기 전에 사이트에 있는 개체 데이터의 양을 검토해야 합니다.

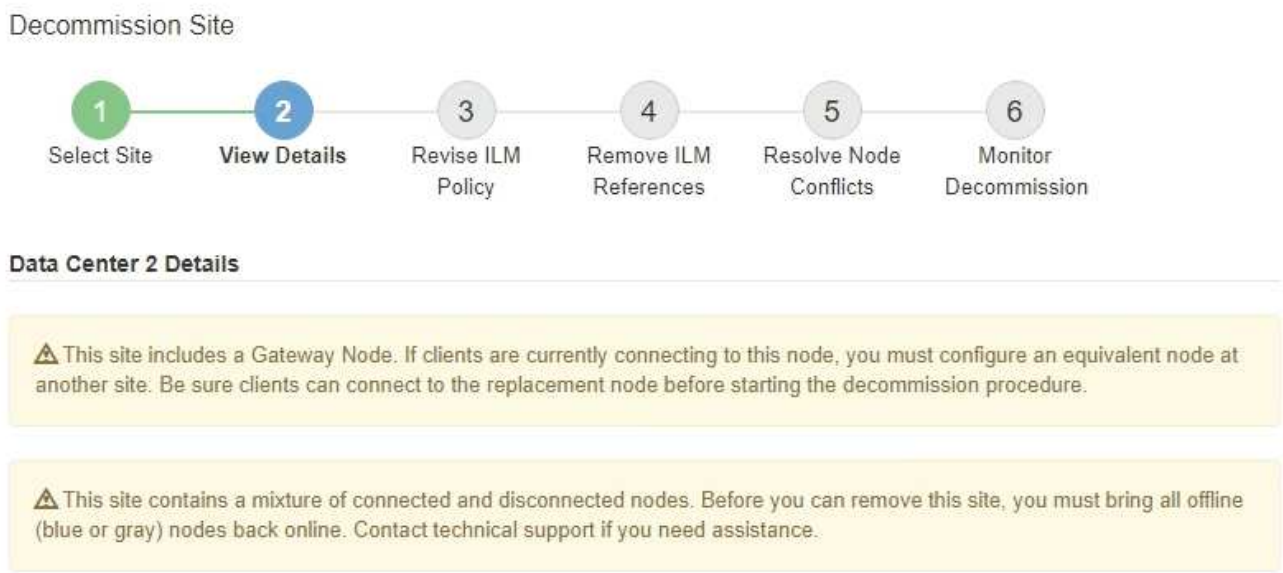
- 연결된 사이트 파기 작업을 수행하는 경우 ILM을 업데이트하기 전에 현재 사이트에 있는 개체 데이터의 양을 이해해야 합니다. 사이트 용량과 데이터 보호 요구사항에 따라 새로운 ILM 규칙을 생성하여 데이터를 다른 사이트로 이동하거나 사이트에서 오브젝트 데이터를 삭제할 수 있습니다.
- 가능한 경우 서비스 해제 절차를 시작하기 전에 필요한 스토리지 노드 확장을 수행합니다.
- 연결이 끊긴 사이트를 사용 중지하는 경우 사이트를 제거할 때 개체 데이터에 영구적으로 액세스할 수 없게 되는

양을 이해해야 합니다.

> 연결이 끊긴 사이트를 사용 중지하는 경우 ILM은 개체 데이터를 이동하거나 삭제할 수 없습니다. 사이트에 남아 있는 데이터는 모두 손실됩니다. 하지만 ILM 정책을 통해 단일 사이트의 손실로부터 보호할 수 있었던 경우 오브젝트 데이터 복사본은 나머지 사이트에 여전히 존재합니다.

단계

1. 2단계(세부 정보 보기)에서 제거하려는 사이트와 관련된 경고를 검토합니다.



   다음과 같은 경우 경고가 나타납니다.

   - 이 사이트에는 게이트웨이 노드가 포함되어 있습니다. S3 및 Swift 클라이언트가 현재 이 노드에 연결 중인 경우 다른 사이트에서 동일한 노드를 구성해야 합니다. 서비스 해제 절차를 계속하기 전에 클라이언트가 교체 노드에 연결할 수 있는지 확인하십시오.
   - 이 사이트에는 연결된( ) 및 연결되지 않은 노드(또는)를 클릭합니다. 이 사이트를 제거하려면 먼저 오프라인 노드를 모두 다시 온라인 상태로 전환해야 합니다.

2. 제거하려는 사이트에 대한 세부 정보를 검토합니다.

Decommission Site

1 Select Site — 2 View Details — 3 Revise ILM Policy — 4 Remove ILM References — 5 Resolve Node Conflicts — 6 Monitor Decommission

Raleigh Details

Number of Nodes: 3
Free Space: 475.38 GB
Used Space: 3.93 MB
Site Capacity: 475.38 GB

Node Name	Node Type	Connnection State	Details
RAL-S1-101-196	Storage Node	✔	1.30 MB used space
RAL-S2-101-197	Storage Node	✔	1.30 MB used space
RAL-S3-101-198	Storage Node	✔	1.34 MB used space

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB
Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space	Used Space	Site Capacity
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	**950.76 GB**	**7.87 MB**	**950.77 GB**

Previous Next

선택한 사이트에 대해 다음 정보가 포함됩니다.

- 노드 수
- 사이트에 있는 모든 스토리지 노드의 총 사용 공간, 사용 가능한 공간 및 용량입니다.
  - 연결된 사이트 서비스 해제의 경우 * Used Space * 값은 다른 사이트로 이동하거나 ILM을 통해 삭제해야 하는 개체 데이터의 양을 나타냅니다.
  - 연결이 끊어진 사이트의 경우 * Used Space * 값은 사이트를 제거할 때 액세스할 수 없는 개체 데이터의 양을 나타냅니다.
- 노드 이름, 유형 및 연결 상태:
  - (연결됨)
  - (관리자 다운)
  - (알 수 없음)
- 각 노드에 대한 세부 정보:
  - 각 스토리지 노드에 대해 오브젝트 데이터에 사용된 공간의 양입니다.

- 관리 노드 및 게이트웨이 노드의 경우 노드가 현재 고가용성(HA) 그룹에서 사용되고 있는지 여부를 나타냅니다. HA 그룹에서 사용되는 관리 노드 또는 게이트웨이 노드는 해제할 수 없습니다. 서비스 해제를 시작하려면 먼저 HA 그룹을 편집하여 사이트의 모든 노드를 제거해야 합니다. 또는 이 사이트의 노드만 포함하는 HA 그룹을 제거할 수 있습니다.

  StorageGRID 관리

3. 페이지의 다른 사이트에 대한 세부 정보 섹션에서 그리드의 다른 사이트에서 사용 가능한 공간을 평가합니다.

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB
Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space	Used Space	Site Capacity
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	**950.76 GB**	**7.87 MB**	**950.77 GB**

연결된 사이트를 사용 중지하고 ILM을 사용하여 선택한 사이트에서 오브젝트 데이터를 이동하려는 경우(삭제만 하는 것이 아니라) 다른 사이트의 용량이 이동된 데이터를 수용할 수 있을 만큼 충분한지, 그리고 향후 성장을 위해 적절한 용량이 남아 있는지 확인해야 합니다.

> 제거하려는 사이트의 * 사용된 공간 * 이 * 다른 사이트의 총 여유 공간 * 보다 큰 경우 경고가 나타납니다. 사이트를 제거한 후 적절한 스토리지 용량을 사용할 수 있도록 하려면 이 절차를 수행하기 전에 확장을 수행해야 할 수 있습니다.

4. 다음 * 을 선택합니다.

   3단계(ILM 정책 수정)가 나타납니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

3단계**: ILM** 정책 수정

서비스 해제 사이트 마법사의 3단계(ILM 정책 수정)에서 활성 ILM 정책에 의해 사이트가 참조되는지 확인할 수 있습니다.

필요한 것

ILM의 작동 방식에 대해 잘 알고 있으며 스토리지 풀 생성, 삭제 코딩 프로필, ILM 규칙 및 ILM 정책 시뮬레이션 및 활성화에 대해 잘 알고 있습니다.

ILM을 사용하여 개체를 관리합니다

이 작업에 대해

활성 ILM 정책의 ILM 규칙에 의해 해당 사이트를 참조하는 경우에는 StorageGRID에서 사이트를 해제할 수 없습니다.

현재 ILM 정책이 제거하려는 사이트를 참조하는 경우 특정 요구 사항을 충족하는 새 ILM 정책을 활성화해야 합니다.

특히 새로운 ILM 정책은 다음과 같습니다.

- 사이트를 참조하는 스토리지 풀을 사용할 수 없습니다.
- 사이트를 참조하는 삭제 코딩 프로필을 사용할 수 없습니다.
- 기본 * 모든 스토리지 노드 * 스토리지 풀 또는 기본 * 모든 사이트 * 사이트를 사용할 수 없습니다.
- Stock * Make 2 Copies * 규칙을 사용할 수 없습니다.
- 모든 오브젝트 데이터를 완벽하게 보호하도록 설계되어야 합니다.

> 사이트 제거를 수용하기 위해 단일 복사본 ILM 규칙을 만들지 마십시오. 특정 기간 동안 복제된 복사본을 하나만 생성하는 ILM 규칙은 데이터가 영구적으로 손실될 위험이 있습니다. 복제된 객체 복제본이 하나만 있는 경우 스토리지 노드에 장애가 발생하거나 심각한 오류가 발생한 경우 해당 객체가 손실됩니다. 또한 업그레이드와 같은 유지보수 절차 중에는 개체에 대한 액세스가 일시적으로 중단됩니다.

연결된 사이트 파기 _ 을(를) 수행하는 경우 StorageGRID에서 현재 제거하려는 사이트에 있는 오브젝트 데이터를 관리하는 방법을 고려해야 합니다. 데이터 보호 요구사항에 따라 새 규칙은 기존 오브젝트 데이터를 다른 사이트로 이동하거나 더 이상 필요하지 않은 추가 오브젝트 복사본을 삭제할 수 있습니다.

새로운 정책을 설계하는 데 도움이 필요한 경우 기술 지원 부서에 문의하십시오.

단계

1. 3단계(ILM 정책 수정)에서 활성 ILM 정책에 있는 ILM 규칙이 제거할 사이트를 참조하는지 확인합니다.

Decommission Site

1 Select Site — 2 View Details — 3 **Revise ILM Policy** — 4 Remove ILM References — 5 Resolve Node Conflicts — 6 Monitor Decommission

If your current ILM policy refers to the site, you must activate a new policy before you can go to the next step.

The new ILM policy:

- Cannot use a storage pool that refers to the site.
- Cannot use an Erasure Coding profile that refers to the site.
- Cannot use the default **All Storage Nodes** storage pool or the default **All Sites** site.
- Cannot use the **Make 2 Copies** rule.
- Must be designed to fully protect all object data after one site is removed.

Contact technical support if you need assistance in designing the new policy.

If you are performing a connected site decommission, StorageGRID will begin to remove object data from the site as soon as you activate the new ILM policy. Moving or deleting all object copies might take weeks, but you can safely start a site decommission while object data still exists at the site.

Rules Referring to Raleigh in the Active ILM Policy

The table lists the ILM rules in the active ILM policy that refer to the site.

- If no ILM rules are listed, the active ILM policy does not refer to the site. Select **Next** to go to Step 4 (Remove ILM References).
- If one or more ILM rules are listed, you must create and activate a new policy that does not use these rules.

Active Policy Name: Data Protection for Three Sites

The active ILM policy refers to Raleigh. Before you can remove this site, you must propose and activate a new policy.

Name	EC Profiles	Storage Pools
3 copies for S3 tenant	—	Raleigh storage pool
2 copy 2 sites for smaller objects	—	Raleigh storage pool
EC for larger objects	three site EC profile	All 3 Sites

Previous Next

2. 나열된 규칙이 없으면 * 다음 * 을 선택하여 4단계로 이동합니다(ILM 참조 제거).

   4단계: ILM 참조 제거

3. 하나 이상의 ILM 규칙이 표에 나열되어 있는 경우 * 활성 정책 이름 * 옆에 있는 링크를 선택합니다.

   ILM 정책 페이지가 새 브라우저 탭에 나타납니다. 이 탭을 사용하여 ILM을 업데이트하십시오. 서비스 해제 사이트 페이지는 기타 탭에 계속 열려 있습니다.

   a. 필요한 경우 * ILM * > * 스토리지 풀 * 을 선택하여 사이트를 참조하지 않는 하나 이상의 스토리지 풀을 생성합니다.

      자세한 내용은 정보 수명 주기 관리를 사용하여 개체를 관리하는 지침을 참조하십시오.

b. 삭제 코딩을 사용하려는 경우 * ILM * > * 삭제 코딩 * 을 선택하여 하나 이상의 삭제 코딩 프로파일을 만듭니다.

사이트를 참조하지 않는 스토리지 풀을 선택해야 합니다.

> 삭제 코딩 프로파일에서 * 모든 스토리지 노드 * 스토리지 풀을 사용하지 마십시오.

4. ILM * > * 규칙 * 을 선택하고 3단계(ILM 정책 수정)에 대해 표에 나열된 각 규칙을 복제합니다.

> 자세한 내용은 정보 수명 주기 관리를 사용하여 개체를 관리하는 지침을 참조하십시오.

a. 새 정책에서 이러한 규칙을 쉽게 선택할 수 있는 이름을 사용합니다.

b. 배치 지침을 업데이트합니다.

사이트를 참조하는 스토리지 풀 또는 삭제 코딩 프로필을 모두 제거하고 새 스토리지 풀 또는 삭제 코딩 프로파일로 교체합니다.

> 새 규칙에서 * 모든 스토리지 노드 * 스토리지 풀을 사용하지 마십시오.

5. ILM * > * 정책 * 을 선택하고 새 규칙을 사용하는 새 정책을 만듭니다.

> 자세한 내용은 정보 수명 주기 관리를 사용하여 개체를 관리하는 지침을 참조하십시오.

a. 활성 정책을 선택하고 * Clone * 을 선택합니다.

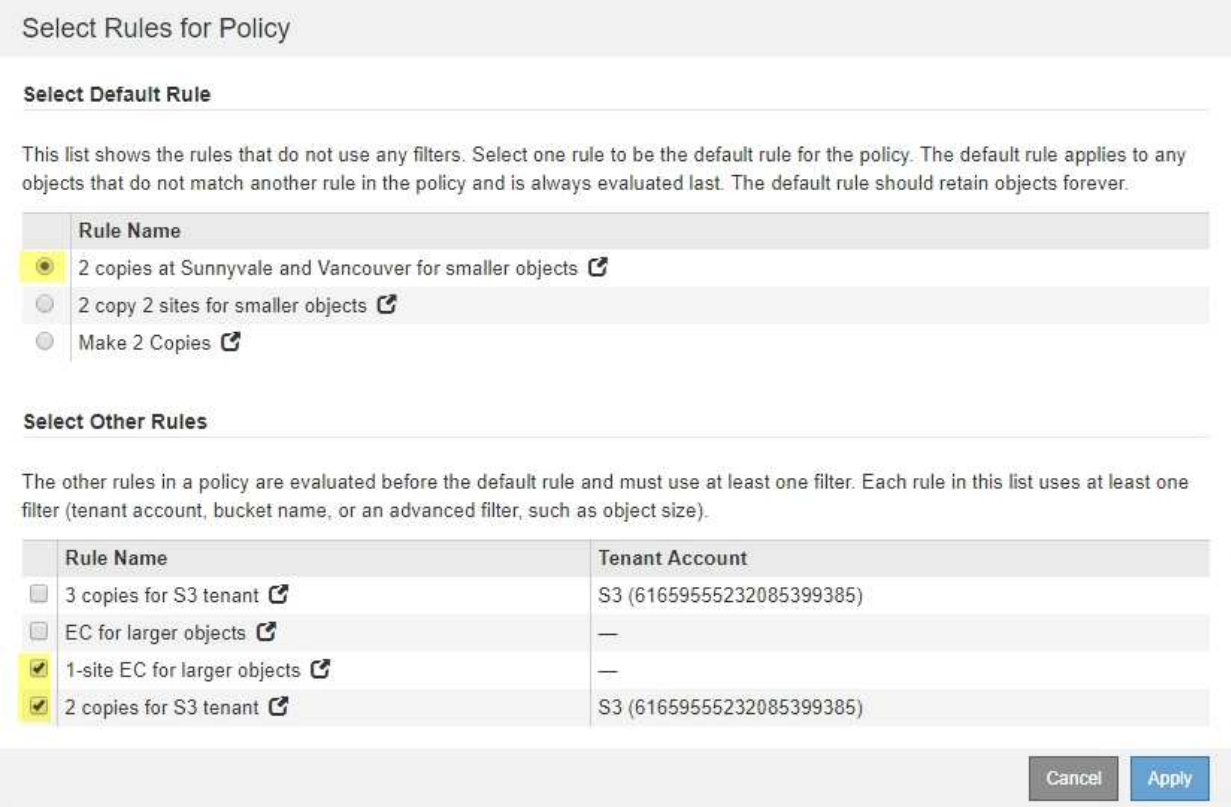
b. 정책 이름과 변경 이유를 지정합니다.

c. 클론 생성된 정책에 대한 규칙을 선택합니다.

- 서비스 해제 사이트 페이지의 3단계(ILM 정책 수정)에 대해 나열된 모든 규칙을 선택 취소합니다.
- 사이트를 참조하지 않는 기본 규칙을 선택합니다.

> 2개 복사본 만들기 * 규칙은 허용되지 않는 * 모든 스토리지 노드 * 스토리지 풀을 사용하므로 선택하지 마십시오.

- 작성한 다른 대체 규칙을 선택합니다. 이러한 규칙은 사이트를 참조해서는 안 됩니다.



d. Apply * 를 선택합니다.

e. 행을 끌어 놓아서 정책의 규칙 순서를 바꿉니다.

기본 규칙을 이동할 수 없습니다.

> ILM 규칙이 올바른 순서로 되어 있는지 확인해야 합니다. 정책이 활성화되면 위에서 시작하여 나열된 순서대로 새 개체와 기존 개체가 평가됩니다.

a. 제안된 정책을 저장합니다.

6. 테스트 개체를 수집하고 제안된 정책을 시뮬레이션하여 올바른 규칙이 적용되도록 합니다.

> ILM 정책의 오류로 인해 복구할 수 없는 데이터 손실이 발생할 수 있습니다. 정책을 활성화하기 전에 정책을 주의 깊게 검토하고 시뮬레이션하여 의도한 대로 작동하도록 확인합니다.

> 새로운 ILM 정책을 활성화하면 StorageGRID은 이를 사용하여 기존 오브젝트 및 새로 수집된 오브젝트를 포함한 모든 오브젝트를 관리합니다. 새 ILM 정책을 활성화하기 전에 복제된 기존 오브젝트 및 삭제 코딩 오브젝트의 배치에 대한 변경 사항을 검토하십시오. 기존 오브젝트의 위치를 변경하면 새로운 배치가 평가되고 구현될 때 일시적인 리소스 문제가 발생할 수 있습니다.

7. 새 정책을 활성화합니다.

연결된 사이트의 서비스 해제를 수행하는 경우 StorageGRID는 새 ILM 정책을 활성화하는 즉시 선택한 사이트에서 개체 데이터를 제거하기 시작합니다. 모든 오브젝트 복사본을 이동하거나 삭제하는 데 몇 주가 걸릴 수 있습니다. 사이트에 오브젝트 데이터가 아직 있는 동안 사이트의 폐기에 대한 안전한 사이트 폐기 시작 가능. 하지만 실제 서비스 해제 절차를 시작하기 전에 데이터를 사이트에서 이동할 수 있도록 하면 서비스 해제 절차가 더 빠르게 완료되고 운영 중단 및 성능에 미치는 영향이 줄어듭니다 (마법사 5단계에서 * 서비스 해제 시작 * 을 선택하여).

8. 3단계(ILM 정책 수정) * 로 돌아가서 새 활성 정책에 ILM 규칙이 없으면 사이트를 참조하고 * 다음 * 버튼이 활성화되어 있는지 확인합니다.

> 규칙이 나열된 경우 계속하기 전에 새 ILM 정책을 만들고 활성화해야 합니다.

9. 나열된 규칙이 없으면 * 다음 * 을 선택합니다.

   4단계(ILM 참조 제거)가 나타납니다.

4단계**: ILM** 참조 제거

서비스 해제 사이트 마법사의 4단계(ILM 참조 제거)에서 제안된 정책이 있는 경우 이를 제거하고 사이트를 참조하는 사용되지 않는 ILM 규칙을 삭제하거나 편집할 수 있습니다.

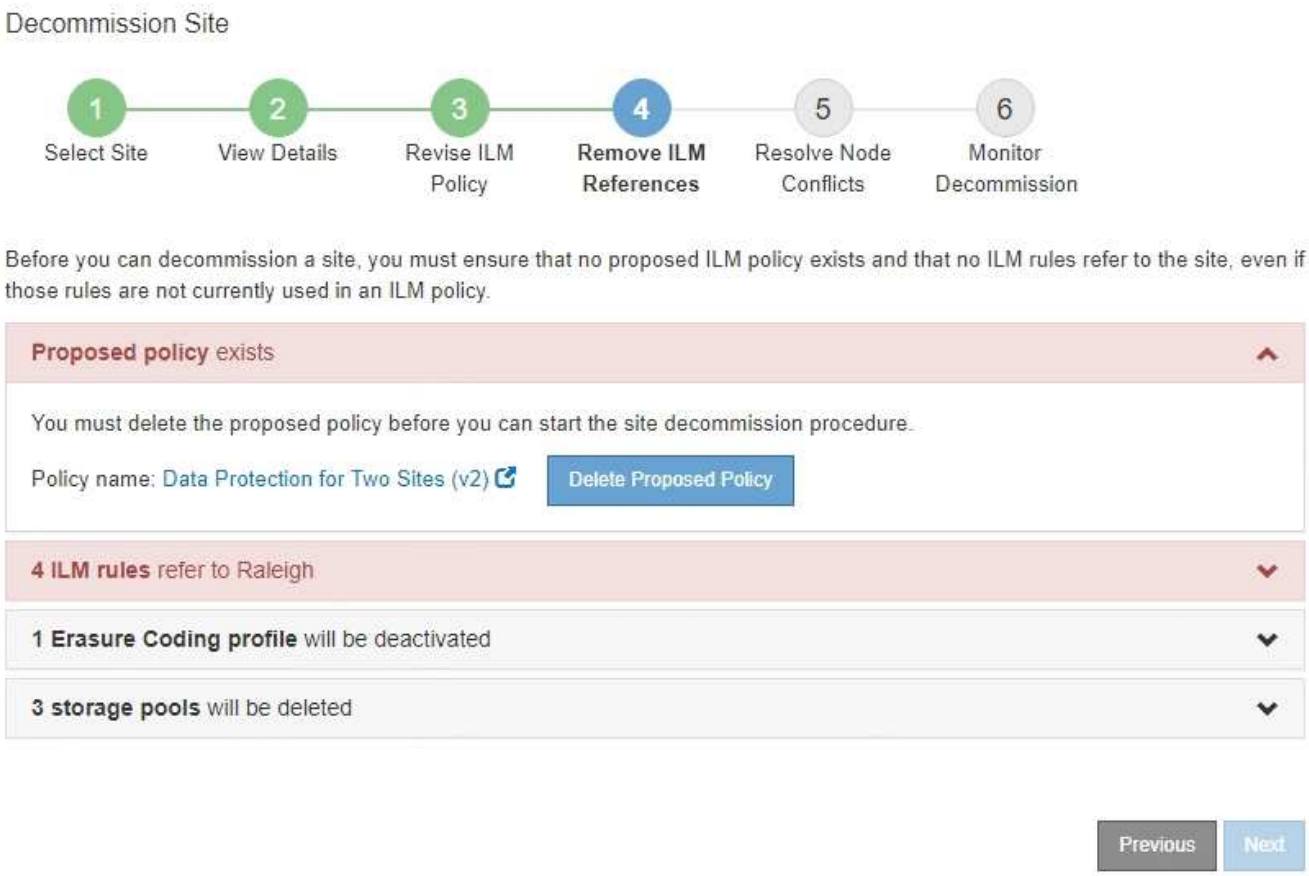
이 작업에 대해

다음과 같은 경우 사이트 서비스 해제 절차를 시작할 수 없습니다.

- 제안된 ILM 정책이 있습니다. 제안된 정책이 있는 경우 삭제해야 합니다.
- ILM 규칙은 ILM 정책에 사용되지 않는 경우에도 사이트를 참조합니다. 사이트를 참조하는 모든 규칙을 삭제하거나 편집해야 합니다.

단계

1. 제안된 정책이 나열된 경우 해당 정책을 제거합니다.



a. 제안된 정책 삭제 * 를 선택합니다.

b. 확인 대화 상자에서 * 확인 * 을 선택합니다.

2. 사용하지 않는 ILM 규칙이 사이트를 참조하는지 확인합니다.

Decommission Site

1 Select Site — 2 View Details — 3 Revise ILM Policy — **4 Remove ILM References** — 5 Resolve Node Conflicts — 6 Monitor Decommission

Before you can decommission a site, you must ensure that no proposed ILM policy exists and that no ILM rules refer to the site, even if those rules are not currently used in an ILM policy.

No proposed policy exists

4 ILM rules refer to Data Center 3

This table lists the unused ILM rules that still refer to the site. For each rule listed, you must do one of the following:

- Edit the rule to remove the Erasure Coding profile or storage pool from the placement instructions.
- Delete the rule.

Go to the ILM Rules page

Name	EC Profiles	Storage Pools	Delete
Make 2 Copies	—	All Storage Nodes	
3 copies for S3 tenant	—	Raleigh storage pool	
2 copies 2 sites for smaller objects	—	Raleigh storage pool	
EC larger objects	three site EC profile	All 3 Sites	

1 Erasure Coding profile will be deactivated

3 storage pools will be deleted

나열된 모든 ILM 규칙은 여전히 사이트를 참조하지만 정책에 사용되지 않습니다. 예제:

- STOCK * make 2 Copies * 규칙은 모든 사이트 사이트를 사용하는 시스템 기본값 * All Storage Nodes * 스토리지 풀을 사용합니다.
- S3 테넌트 * 의 사용되지 않은 * 3개 복사본은 * Raleigh * 스토리지 풀을 나타냅니다.
- 더 작은 객체를 위한 미사용 * 2 복제본 2 사이트는 * Raleigh * 스토리지 풀을 나타냅니다.
- 사용되지 않는 * EC 큰 개체 * 규칙은 * All 3 Sites * Erasure Coding 프로필의 Raleigh 사이트를 사용합니다.
- ILM 규칙이 나열되지 않으면 * 다음 * 을 선택하여 * 5단계(노드 충돌 해결) * 로 이동합니다.

5단계: 노드 충돌 해결(및 서비스 해제 시작)

> StorageGRID에서 사이트의 압축을 풀 경우 해당 사이트를 참조하는 사용되지 않는 삭제 코딩 프로필이 자동으로 비활성화되고, 해당 사이트를 참조하는 사용되지 않은 스토리지 풀이 자동으로 삭제됩니다. 시스템 기본 모든 스토리지 노드 스토리지 풀은 모든 사이트 사이트를 사용하므로 제거됩니다.

- 하나 이상의 ILM 규칙이 나열된 경우 다음 단계로 이동합니다.

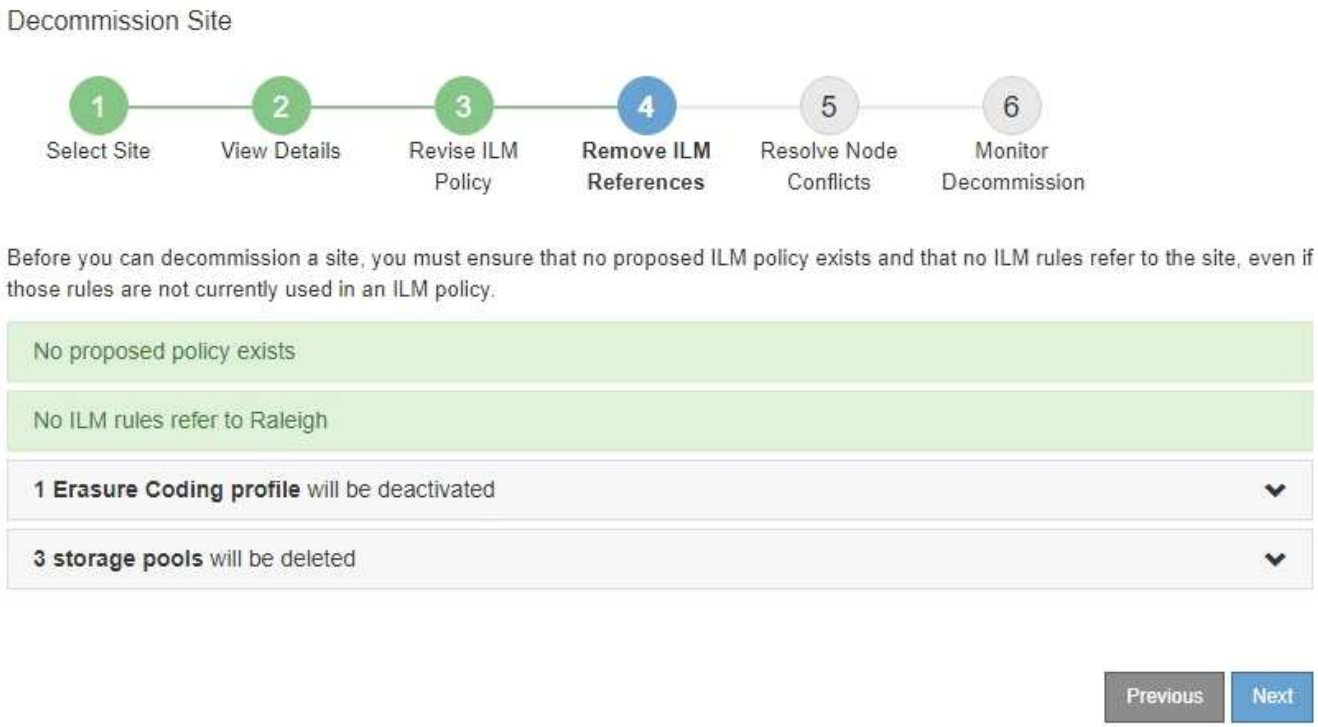
3. 사용하지 않는 각 규칙 편집 또는 삭제:
   - 규칙을 편집하려면 ILM 규칙 페이지로 이동하여 삭제 코딩 프로필 또는 사이트를 참조하는 스토리지 풀을 사용하는 모든 배치를 업데이트합니다. 그런 다음 * 4단계(ILM 참조 제거) * 로 돌아갑니다.

     ⓘ 자세한 내용은 정보 수명 주기 관리를 사용하여 개체를 관리하는 지침을 참조하십시오.

   - 규칙을 삭제하려면 휴지통 아이콘을 선택합니다 🗑 를 선택하고 * 확인 * 을 선택합니다.

     ⓘ 사이트 파기 전에 재고 * 복사본 2개 만들기 * 규칙을 삭제해야 합니다.

4. 제안된 ILM 정책이 존재하지 않는지, 사용되지 않는 ILM 규칙이 사이트를 참조하지 않는지, 그리고 * 다음 * 버튼이 활성화되어 있는지 확인합니다.



5. 다음 * 을 선택합니다.

   ⓘ 사이트를 제거하면 사이트를 참조하는 나머지 스토리지 풀 및 삭제 코딩 프로필이 무효화됩니다. StorageGRID에서 사이트의 압축을 풀 경우 해당 사이트를 참조하는 사용되지 않는 삭제 코딩 프로필이 자동으로 비활성화되고, 해당 사이트를 참조하는 사용되지 않은 스토리지 풀이 자동으로 삭제됩니다. 시스템 기본 모든 스토리지 노드 스토리지 풀은 모든 사이트 사이트를 사용하므로 제거됩니다.

   5단계(노드 충돌 해결)가 나타납니다.

5단계: 노드 충돌 해결(및 서비스 해제 시작)

서비스 해제 사이트 마법사의 5단계(노드 충돌 해결)에서 StorageGRID 시스템의 노드 연결이 끊겼는지 또는 선택한 사이트의 노드가 고가용성(HA) 그룹에 속해 있는지 확인할 수 있습니다. 노드 충돌이 해결된 후에는 이 페이지에서 서비스 해제 절차를 시작합니다.

다음과 같이 StorageGRID 시스템의 모든 노드가 올바른 상태인지 확인해야 합니다.

- StorageGRID 시스템의 모든 노드를 연결해야 합니다( )를 클릭합니다.

  연결이 끊긴 사이트 서비스 해제를 수행하는 경우 제거하려는 사이트의 모든 노드의 연결을 끊어야 하며 다른 모든 사이트의 모든 노드를 연결해야 합니다.

- 제거하려는 사이트에 HA(고가용성) 그룹에 속한 인터페이스가 있을 수 없습니다.

5단계(노드 충돌 해결)에 대해 노드가 나열된 경우 서비스 해제를 시작하기 전에 문제를 해결해야 합니다.

이 페이지에서 사이트 서비스 해제 절차를 시작하기 전에 다음 사항을 검토하십시오.

- 서비스 해제 절차를 완료하려면 적절한 시간이 필요합니다.

  사이트에서 오브젝트 데이터를 이동하거나 삭제하는 경우 사이트의 데이터 양, 시스템의 로드, 네트워크 지연 시간, 필요한 ILM의 특성 등에 따라 며칠, 몇 주 또는 몇 개월이 걸릴 수 있습니다.

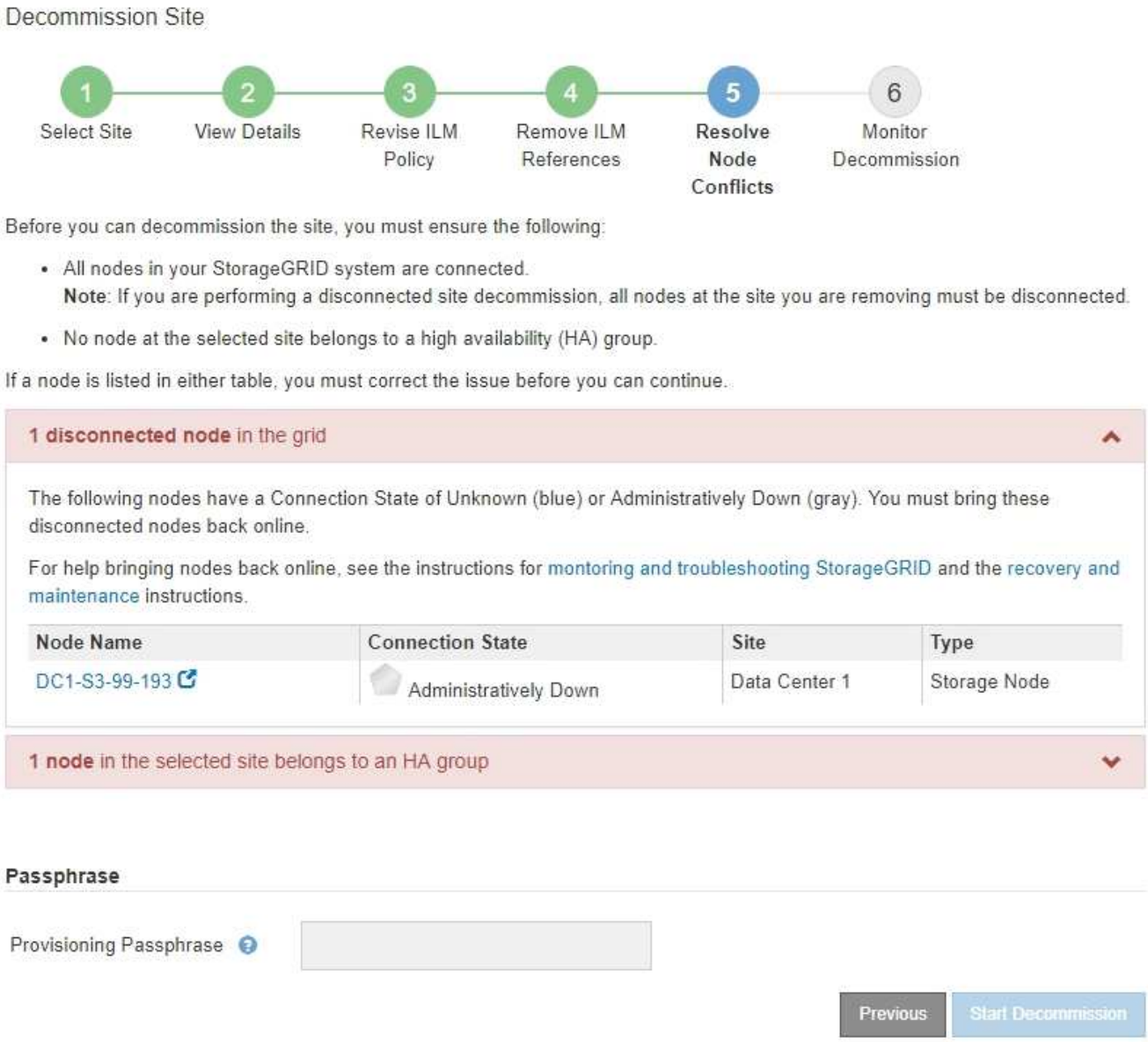
- 사이트 서비스 해제 절차가 실행되는 동안 다음을 수행합니다.
  - 폐기되는 사이트를 참조하는 ILM 규칙을 생성할 수 없습니다. 사이트를 참조하기 위해 기존 ILM 규칙을 편집할 수도 없습니다.
  - 확장 또는 업그레이드와 같은 다른 유지보수 절차는 수행할 수 없습니다.

    연결된 사이트의 서비스 해제 중에 다른 유지보수 절차를 수행해야 하는 경우 스토리지 노드가 제거되는 동안 절차를 일시 중지할 수 있습니다. "암호화된 데이터 삭제 및 중복 삭제" 단계에서는 * 일시 중지 * 버튼이 활성화됩니다.

  - 사이트 서비스 해제 절차를 시작한 후 노드를 복구해야 하는 경우 지원 팀에 문의해야 합니다.

단계

1. 5단계(노드 충돌 해결)의 연결되지 않은 노드 섹션을 검토하여 StorageGRID 시스템에 연결 상태가 알 수 없음( )인지 확인합니다) 또는 관리 중단( )를 클릭합니다.

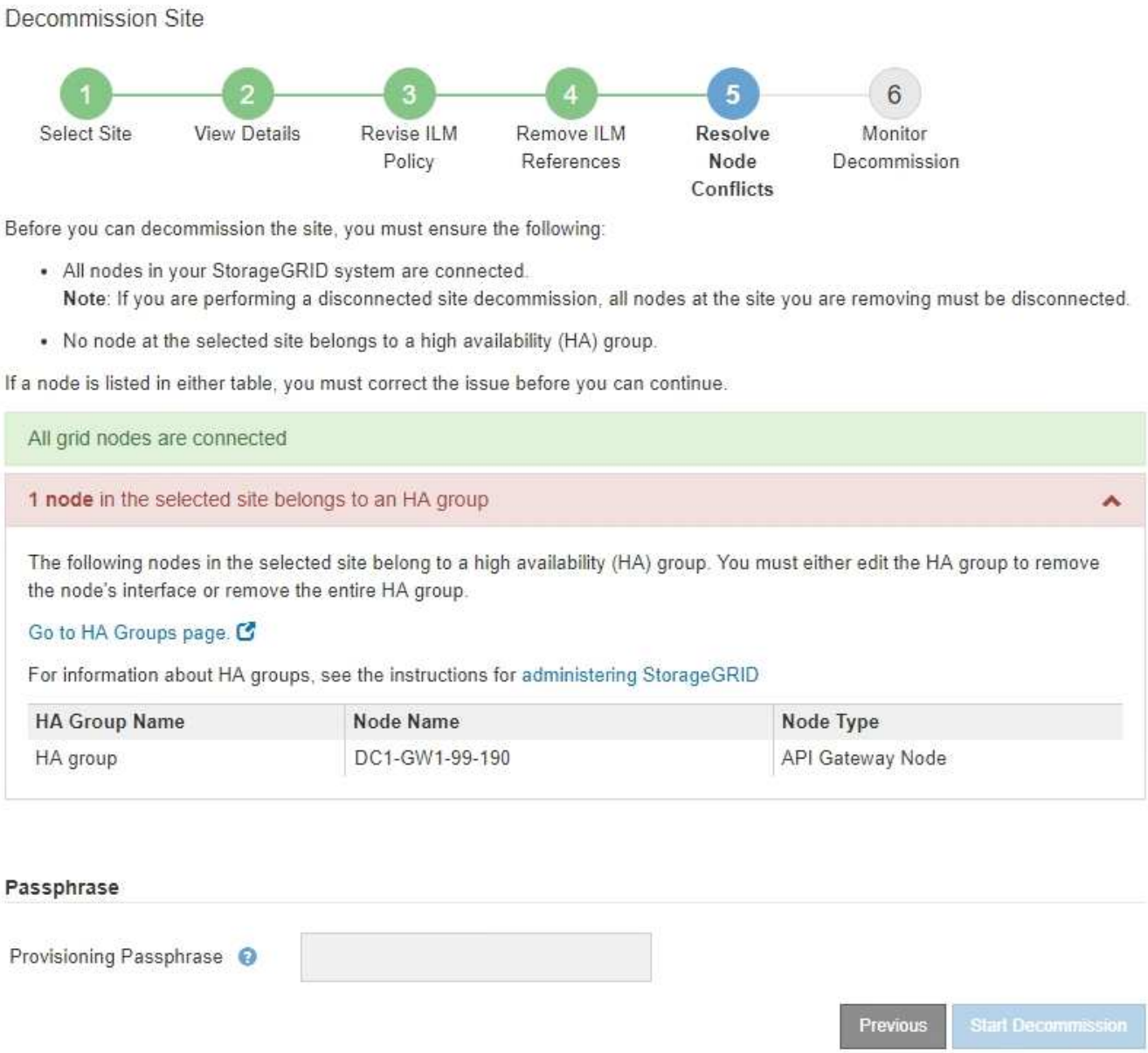


2. 노드의 연결이 끊어진 경우 다시 온라인 상태로 전환합니다.

   StorageGRID 및 그리드 노드 절차에 대한 모니터링 및 문제 해결 지침을 참조하십시오. 도움이 필요한 경우 기술 지원 부서에 문의하십시오.

3. 연결되지 않은 모든 노드가 다시 온라인 상태가 되면 5단계의 HA 그룹 섹션(노드 충돌 해결)을 검토하십시오.

   이 표에는 고가용성(HA) 그룹에 속한 선택한 사이트의 노드가 나열됩니다.

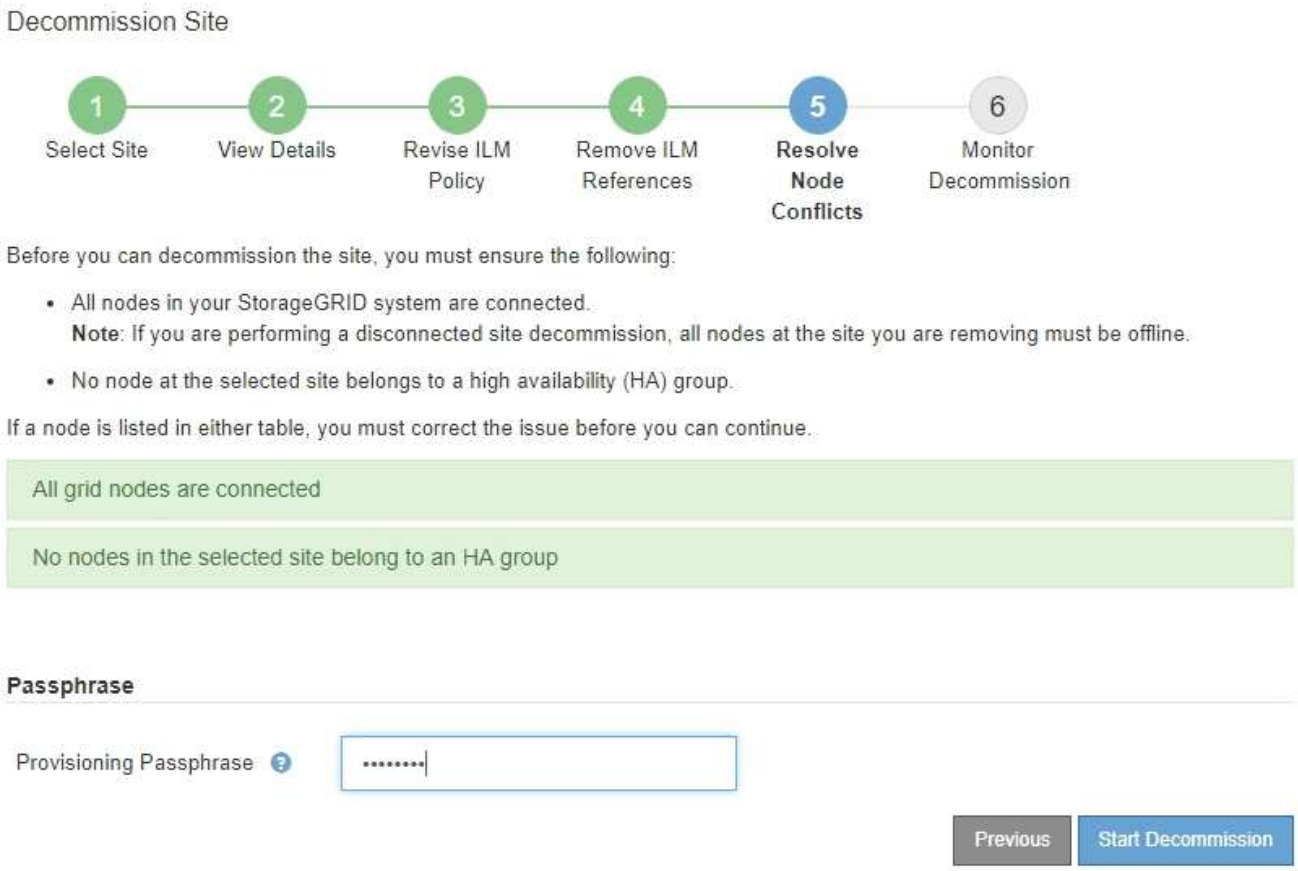


4. 노드가 나열된 경우 다음 중 하나를 수행합니다.
   - 영향을 받는 각 HA 그룹을 편집하여 노드 인터페이스를 제거합니다.
   - 이 사이트에서 노드만 포함하는 HA 그룹을 제거합니다. StorageGRID 관리 지침을 참조하십시오.

   모든 노드가 연결되어 있고 선택한 사이트의 노드가 HA 그룹에서 사용되지 않는 경우 * Provisioning Passphrase * 필드가 활성화됩니다.

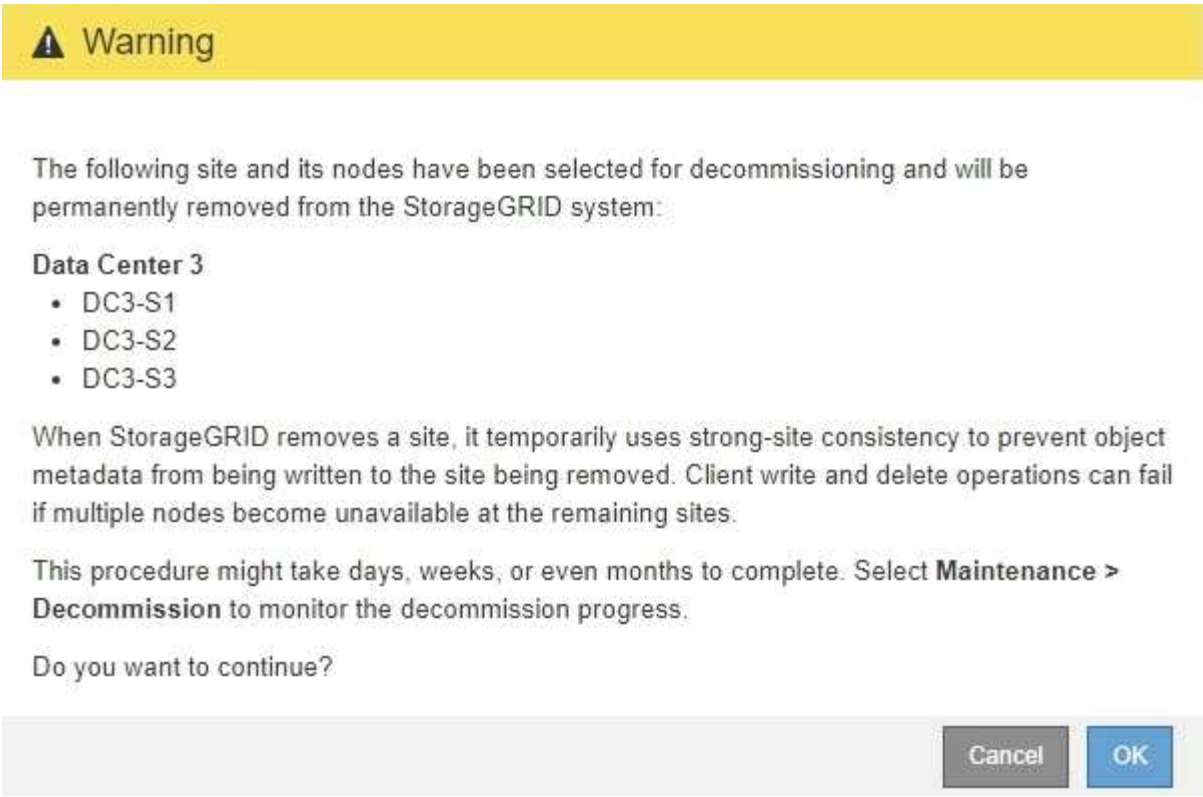
5. 프로비저닝 암호를 입력합니다.

   서비스 해제 시작 * 버튼이 활성화됩니다.



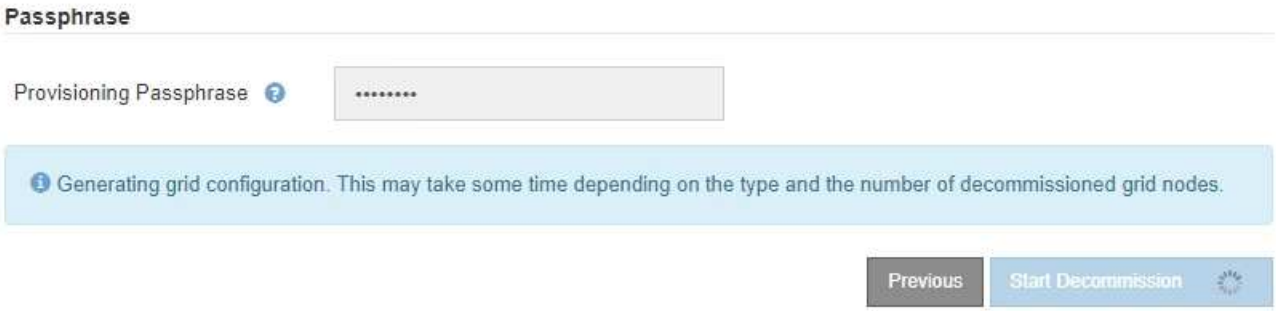
6. 사이트 서비스 해제 절차를 시작할 준비가 되면 * 서비스 해제 시작 * 을 선택합니다.

   경고는 제거할 사이트 및 노드를 나열합니다. 사이트를 완전히 제거하는 데 며칠, 몇 주 또는 몇 달이 걸릴 수 있습니다.



7. 경고를 검토합니다. 시작할 준비가 되었으면 * OK * 를 선택합니다.

   새 그리드 구성이 생성될 때 메시지가 나타납니다. 이 프로세스는 사용 중지된 그리드 노드의 유형과 수에 따라 다소 시간이 걸릴 수 있습니다.



   새 그리드 구성이 생성되면 6단계(서비스 해제 모니터링)가 나타납니다.

   파기가 완료될 때까지 * Previous * (이전 *) 버튼이 비활성화됩니다.

관련 정보

모니터링하고 문제를 해결합니다

그리드 노드 절차

StorageGRID 관리

서비스 해제 사이트 페이지 마법사의 6단계(서비스 해제 모니터링)에서 사이트가 제거될 때 진행 상황을 모니터링할 수 있습니다.

이 작업에 대해

StorageGRID에서 연결된 사이트를 제거하면 다음 순서로 노드가 제거됩니다.

1. 게이트웨이 노드
2. 관리자 노드
3. 스토리지 노드

StorageGRID에서 연결이 끊긴 사이트를 제거하면 다음 순서로 노드가 제거됩니다.

1. 게이트웨이 노드
2. 스토리지 노드
3. 관리자 노드

각 게이트웨이 노드 또는 관리 노드를 제거하는 데 몇 분 또는 1시간이 소요될 수 있지만 스토리지 노드는 며칠 또는 몇 주가 걸릴 수 있습니다.

단계

1. 새 복구 패키지가 생성되는 즉시 파일을 다운로드합니다.

> 서비스 해제 절차 중에 문제가 발생할 경우 그리드를 복구할 수 있도록 가능한 한 빨리 복구 패키지를 다운로드하십시오.

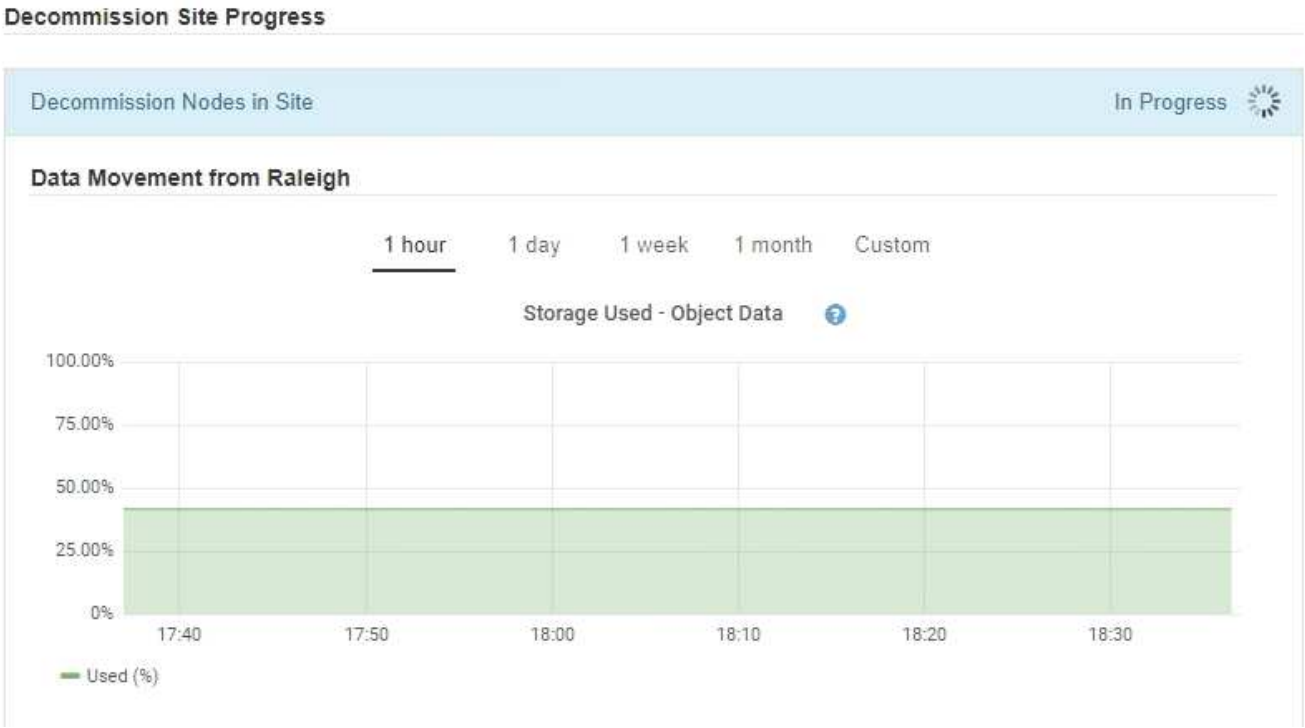
   a. 메시지에서 링크를 선택하거나 * 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
   b. '.zip' 파일을 다운로드합니다.

      의 지침을 참조하십시오 복구 패키지 다운로드 중.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

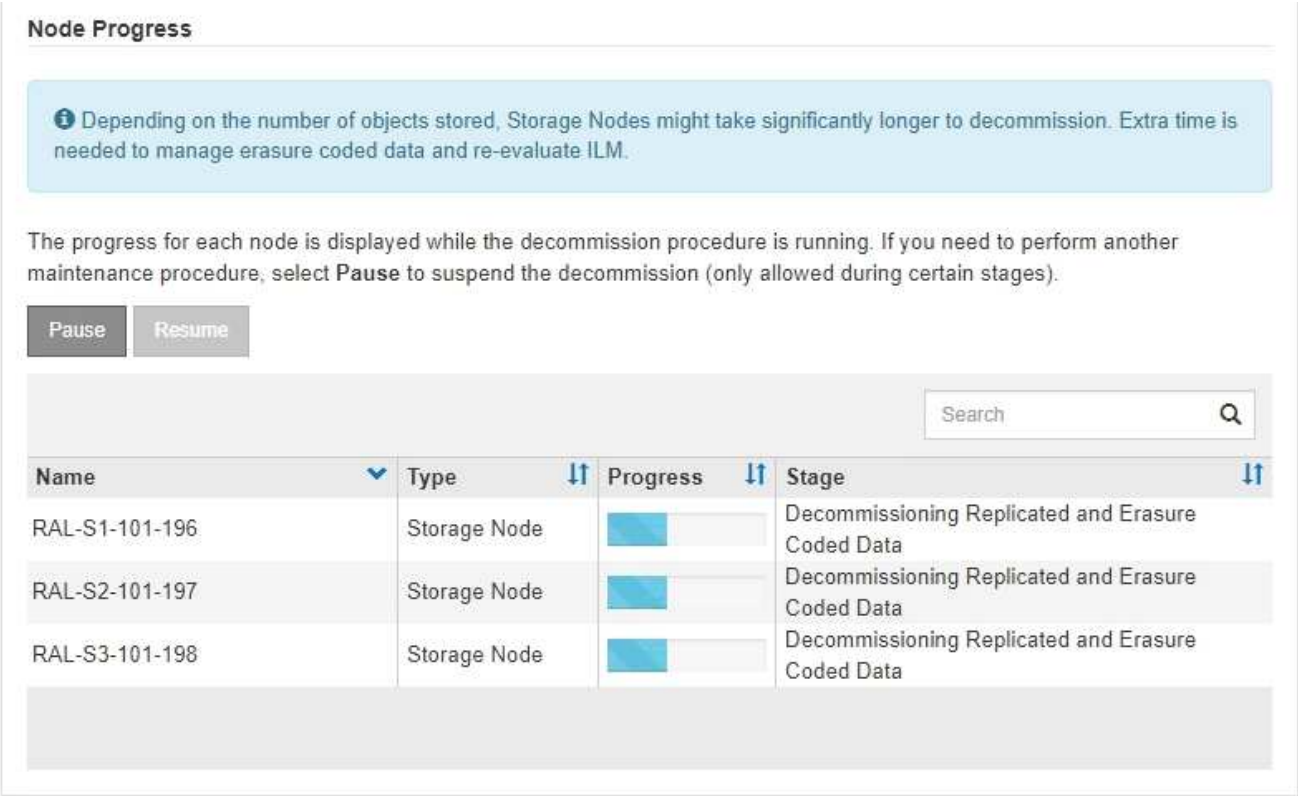
2. 데이터 이동 차트를 사용하여 이 사이트에서 다른 사이트로 개체 데이터의 이동을 모니터링합니다.

3단계에서 새로운 ILM 정책을 활성화했을 때 데이터 이동이 시작되었습니다(ILM 정책 수정). 서비스 해제 절차 중에 데이터 이동이 발생합니다.



3. 페이지의 노드 진행 섹션에서 노드가 제거될 때 서비스 해제 절차의 진행 상황을 모니터링합니다.

   스토리지 노드를 제거하면 각 노드가 일련의 단계를 거칩니다. 이러한 단계의 대부분은 신속하게 또는 심지어 눈에 띄지 않게 발생하지만 이동해야 할 데이터의 양에 따라 다른 단계가 완료될 때까지 며칠 또는 몇 주를 기다려야 할 수 있습니다. 삭제 코딩 데이터를 관리하고 ILM을 재평가하기 위해 추가 시간이 필요합니다.



연결된 사이트 서비스 해제의 진행률을 모니터링하는 경우 이 표를 참조하여 스토리지 노드의 서비스 해제 단계를 파악할 수 있습니다.

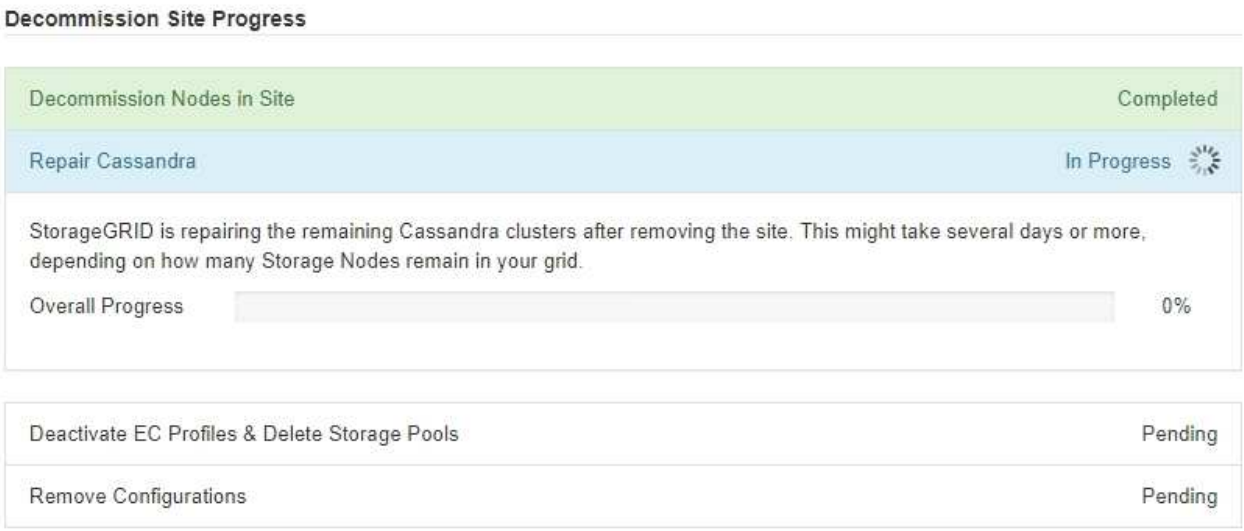
단계	예상 기간
보류 중	분 이하
잠금 대기	분
작업 준비	분 이하
LDR 사용 중지 표시	분
복제된 데이터 폐기 및 삭제 코딩 데이터	데이터 양을 기준으로 한 시간, 일 또는 주 • 참고 *: 다른 유지보수 활동을 수행해야 하는 경우 이 단계 동안 사이트 파기를 일시 중지할 수 있습니다.
LDR 설정 상태	분
감사 대기열 플러시	메시지 수 및 네트워크 대기 시간을 기준으로 분~시간
완료	분

연결이 끊긴 사이트 서비스 해제의 진행률을 모니터링하는 경우 이 표를 참조하여 스토리지 노드의 서비스 해제 단계를 파악할 수 있습니다.

단계	예상 기간
보류 중	분 이하
잠금 대기	분
작업 준비	분 이하
외부 서비스를 비활성화합니다	분
인증서 해지	분
노드 등록 취소	분
스토리지 등급 등록 취소	분
스토리지 그룹 제거	분

단계	예상 기간
도면요소 제거	분
완료	분

4. 모든 노드가 완료 단계에 도달한 후 나머지 사이트 서비스 해제 작업이 완료될 때까지 기다립니다.
   - Cassandra * 복구 단계 중, StorageGRID은 귀사의 그리드에 남아 있는 Cassandra 클러스터를 수정합니다. 그리드에 남아 있는 스토리지 노드 수에 따라 이러한 복구에는 며칠 이상이 걸릴 수 있습니다.

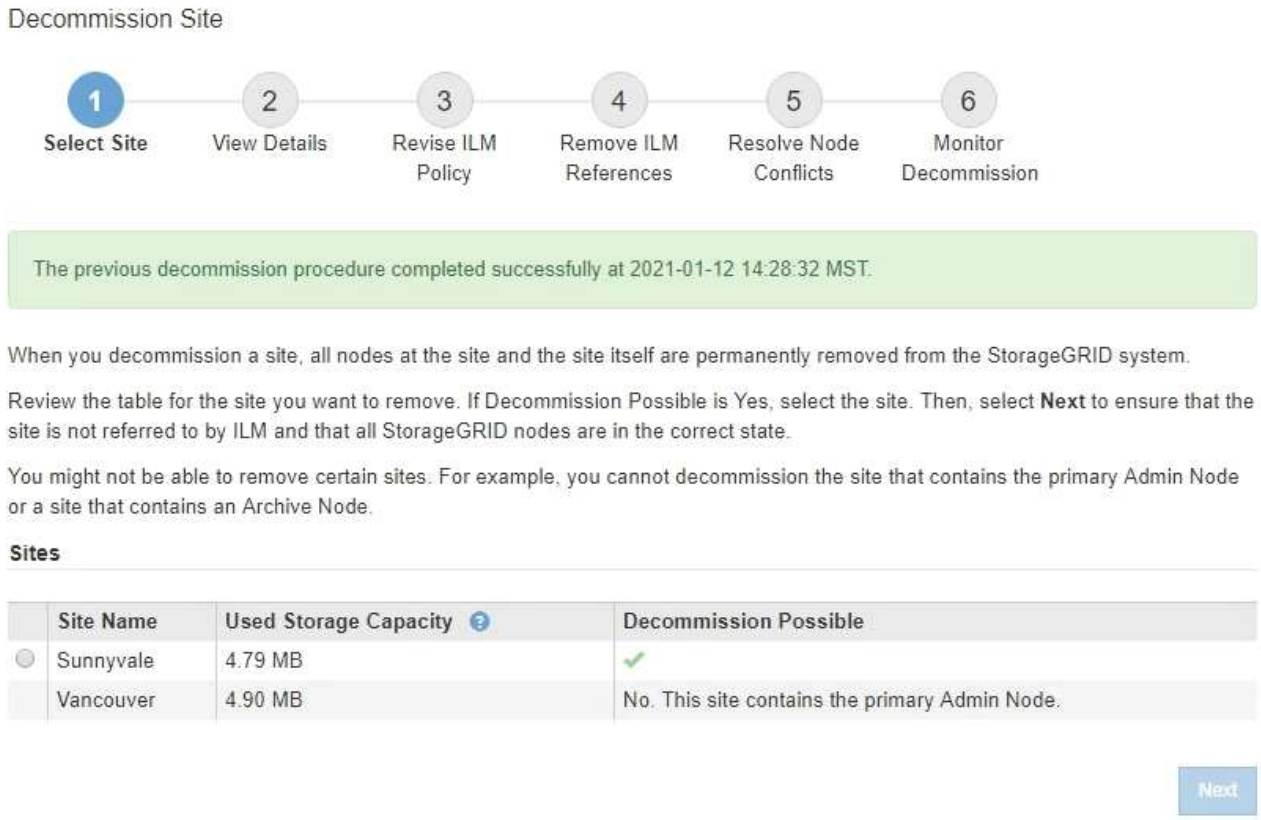


   - EC 프로파일 비활성화 및 스토리지 풀 삭제 * 단계에서 다음 ILM이 변경됩니다.
     - 사이트를 참조하는 모든 삭제 코딩 프로필은 비활성화됩니다.
     - 사이트를 참조하는 모든 스토리지 풀이 삭제됩니다.

> 시스템 기본 모든 스토리지 노드 스토리지 풀도 모든 사이트 사이트를 사용하므로 제거됩니다.

   - 마지막으로, * 구성 제거 * 단계에서 사이트 및 해당 노드에 대한 나머지 참조는 그리드의 나머지 부분에서 제거됩니다.

5. 서비스 해제 절차가 완료되면 서비스 해제 사이트 페이지에 성공 메시지가 표시되고 제거된 사이트가 더 이상 표시되지 않습니다.



작업을 마친 후

사이트 서비스 해제 절차를 완료한 후 다음 작업을 완료합니다.

- 해체된 사이트에 있는 모든 스토리지 노드의 드라이브가 깨끗하게 지워졌는지 확인합니다. 상용 데이터 삭제 도구 또는 서비스를 사용하여 드라이브에서 데이터를 영구적으로 안전하게 제거합니다.
- 사이트에 하나 이상의 관리 노드가 포함되어 있고 StorageGRID 시스템에 SSO(Single Sign-On)가 설정되어 있는 경우 AD FS(Active Directory Federation Services)에서 사이트에 대한 모든 신뢰할 수 있는 상대 트러스트를 제거합니다.
- 연결된 사이트 서비스 해제 절차의 일부로 노드의 전원이 자동으로 정상적으로 꺼진 후 연결된 가상 머신을 제거합니다.

네트워크 유지보수 절차

그리드 네트워크에 대한 서브넷을 업데이트합니다

StorageGRID는 그리드 네트워크(eth0)의 그리드 노드 간에 통신하는 데 사용되는 네트워크 서브넷 목록을 유지합니다. 이러한 항목에는 StorageGRID 시스템의 각 사이트에서 그리드 네트워크에 사용되는 서브넷과 그리드 네트워크 게이트웨이를 통해 액세스되는 NTP, DNS, LDAP 또는 기타 외부 서버에 사용되는 서브넷이 포함됩니다. 확장 시 그리드 노드 또는 새 사이트를 추가할 때 그리드 네트워크에 서브넷을 업데이트하거나 추가해야 할 수 있습니다.

필요한 것

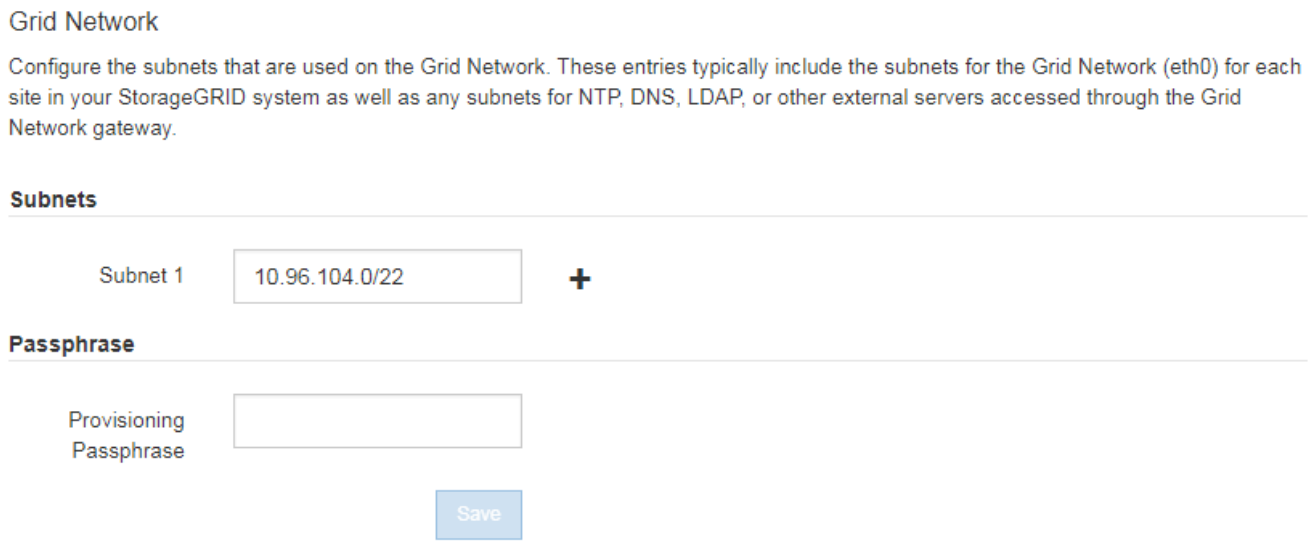
- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.
- 구성할 서브넷의 네트워크 주소(CIDR 표기법)가 있어야 합니다.

이 작업에 대해

새 서브넷 추가를 포함하는 확장 작업을 수행하는 경우 확장 절차를 시작하기 전에 새 그리드 서브넷을 추가해야 합니다.

단계

1. 유지보수 * > * 네트워크 * > * 그리드 네트워크 * 를 선택합니다.



2. 서브넷 목록에서 더하기 기호를 클릭하여 CIDR 표기법으로 새 서브넷을 추가합니다.

   예를 들어 10.96.104.0/22 를 입력합니다.

3. 프로비저닝 암호를 입력하고 * Save * 를 클릭합니다.

   지정한 서브넷은 StorageGRID 시스템에 대해 자동으로 구성됩니다.

4. Grid Manager에서 새 복구 패키지를 다운로드합니다.
   a. 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
   b. 프로비저닝 암호를 입력합니다.

IP 주소를 구성합니다

IP 변경 도구를 사용하여 그리드 노드에 대한 IP 주소를 구성하여 네트워크 구성을 수행할 수 있습니다.

그리드 배포 중에 처음 설정된 네트워킹 구성을 대부분 변경하려면 Change IP(IP 변경) 도구를 사용해야 합니다. 표준 Linux 네트워킹 명령 및 파일을 사용한 수동 변경 사항은 모든 StorageGRID 서비스에 전파되지 않을 수 있으며, 업그레이드, 재부팅 또는 노드 복구 절차 시에도 유지되지 않을 수 있습니다.

> 그리드의 모든 노드에 대한 그리드 네트워크 IP 주소를 변경하려면 을 사용합니다 그리드 전체의 변경 특수 절차.

> Grid Network Subnet List(그리드 네트워크 서브넷 목록)만 변경하는 경우 Grid Manager(그리드 관리자)를 사용하여 네트워크 구성을 추가하거나 변경합니다. 그렇지 않으면 네트워크 구성 문제로 인해 그리드 관리자에 액세스할 수 없거나 그리드 네트워크 라우팅 변경 및 기타 네트워크 변경을 동시에 수행하는 경우 IP 변경 도구를 사용합니다.

> IP 변경 절차는 중단 절차가 될 수 있습니다. 새 구성이 적용될 때까지 그리드의 부분을 사용할 수 없습니다.

- 이더넷 인터페이스 *

eth0에 할당된 IP 주소는 항상 그리드 노드의 그리드 네트워크 IP 주소입니다. eth1에 할당된 IP 주소는 항상 그리드 노드의 관리 네트워크 IP 주소입니다. eth2에 할당된 IP 주소는 항상 그리드 노드의 클라이언트 네트워크 IP 주소입니다.

StorageGRID 어플라이언스, eth0, eth1 및 eth2와 같은 일부 플랫폼에서는 종속 브리지 또는 물리적 또는 VLAN 인터페이스의 결합으로 구성된 통합 인터페이스일 수 있습니다. 이러한 플랫폼에서는 * SSM * > * Resources * 탭에 eth0, eth1 또는 eth2와 함께 다른 인터페이스에 할당된 Grid, Admin 및 Client Network IP 주소가 표시될 수 있습니다.

- DHCP *

배포 단계에서는 DHCP만 설정할 수 있습니다. 구성 중에는 DHCP를 설정할 수 없습니다. 그리드 노드의 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 변경하려면 IP 주소 변경 절차를 사용해야 합니다. IP 변경 도구를 사용하면 DHCP 주소가 정적이 됩니다.

- 고가용성(HA) 그룹 *
- 클라이언트 네트워크 인터페이스가 HA 그룹에 포함되어 있는 경우에는 해당 인터페이스의 클라이언트 네트워크 IP 주소를 HA 그룹에 구성된 서브넷 외부의 주소로 변경할 수 없습니다.
- 클라이언트 네트워크 IP 주소는 클라이언트 네트워크 인터페이스에 구성된 HA 그룹에 할당된 기존 가상 IP 주소의 값으로 변경할 수 없습니다.
- 그리드 네트워크 인터페이스가 HA 그룹에 포함되어 있는 경우에는 해당 인터페이스의 그리드 네트워크 IP 주소를 HA 그룹에 구성된 서브넷 외부의 주소로 변경할 수 없습니다.
- 그리드 네트워크 IP 주소는 그리드 네트워크 인터페이스에 구성된 HA 그룹에 할당된 기존 가상 IP 주소의 값으로 변경할 수 없습니다.

노드 네트워크 구성을 변경합니다

Change IP(IP 변경) 도구를 사용하여 하나 이상의 노드의 네트워크 구성을 변경할 수 있습니다. 그리드 네트워크의 구성을 변경하거나 관리자 또는 클라이언트 네트워크를 추가, 변경 또는 제거할 수 있습니다.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

이 작업에 대해

- Linux: * 그리드 노드를 관리 네트워크 또는 클라이언트 네트워크에 처음으로 추가하는 경우, 노드 구성 파일에서 admin_network_target 또는 client_network_target을 이전에 구성하지 않은 경우에는 지금 구성해야 합니다.

Linux 운영 체제에 대한 StorageGRID 설치 지침을 참조하십시오.

- 어플라이언스:* StorageGRID 초기 설치 중에 StorageGRID 어플라이언스 설치 프로그램에 클라이언트 또는 관리자 네트워크가 구성되어 있지 않으면 IP 변경 도구만 사용하여 네트워크를 추가할 수 없습니다. 먼저 해야 합니다 제품을 유지보수 모드로 두십시오링크를 구성하고 어플라이언스를 정상 작동 모드로 전환한 다음 IP 변경 도구를 사용하여 네트워크 구성을 수정합니다. 어플라이언스에 대한 설치 및 유지 관리 지침의 네트워크 링크 구성 절차를 참조하십시오.

네트워크에서 하나 이상의 노드에 대한 IP 주소, 서브넷 마스크, 게이트웨이 또는 MTU 값을 변경할 수 있습니다.

클라이언트 네트워크 또는 관리 네트워크에서 노드를 추가하거나 제거할 수도 있습니다.

- 노드에 해당 네트워크의 IP 주소/서브넷 마스크를 추가하여 노드를 클라이언트 네트워크 또는 관리 네트워크에 추가할 수 있습니다.
- 클라이언트 네트워크 또는 관리 네트워크에서 해당 네트워크의 노드에 대한 IP 주소/서브넷 마스크를 삭제하여 노드를 제거할 수 있습니다.

  그리드 네트워크에서 노드를 제거할 수 없습니다.

> IP 주소 교체는 허용되지 않습니다. 그리드 노드 간에 IP 주소를 교환해야 하는 경우 임시 중간 IP 주소를 사용해야 합니다.

> StorageGRID 시스템에 SSO(Single Sign-On)가 활성화되어 있고 관리자 노드의 IP 주소를 변경하는 경우, 관리자 노드의 IP 주소(권장 사항에 따라 정규화된 도메인 이름 대신)를 사용하여 구성된 모든 기반 당사자 트러스트가 무효화됩니다. 더 이상 노드에 로그인할 수 없습니다. IP 주소를 변경한 직후 새 IP 주소를 사용하여 AD FS(Active Directory Federation Services)에서 노드의 기반 당사자 신뢰를 업데이트하거나 다시 구성해야 합니다. StorageGRID 관리 지침을 참조하십시오.

> Change IP(IP 변경) 도구를 사용하여 네트워크를 변경하면 StorageGRID 어플라이언스의 설치 관리자 펌웨어로 전파됩니다. 이렇게 하면 어플라이언스에 StorageGRID 소프트웨어를 재설치하거나 어플라이언스를 유지 관리 모드로 설정한 경우 네트워킹 구성이 올바릅니다.

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
2. Change IP Tool을 시작하려면 'change-ip' 명령을 입력합니다
3. 프롬프트에 프로비저닝 암호를 입력합니다.

   기본 메뉴가 나타납니다.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
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:
```

4. 필요에 따라 * 1 * 을 선택하여 업데이트할 노드를 선택합니다. 그런 다음 다음 다음 다음 옵션 중 하나를 선택합니다.
   - * 1 *: 단일 노드 — 이름별로 선택합니다
   - * 2 *: 단일 노드 — 사이트별로 선택한 다음 이름별로 선택합니다
   - * 3 *: 단일 노드 — 현재 IP로 선택합니다
   - * 4 *: 사이트의 모든 노드
   - * 5 *: 그리드의 모든 노드
     - 참고: * 모든 노드를 업데이트하려면 "모두"가 선택된 상태로 유지되도록 하십시오.

   선택한 후 기본 메뉴가 나타나고 * Selected Nodes * 필드가 업데이트되어 선택 사항을 반영합니다. 이후의 모든 작업은 표시된 노드에서만 수행됩니다.

5. 메인 메뉴에서 옵션 * 2 * 를 선택하여 선택한 노드의 IP/마스크, 게이트웨이 및 MTU 정보를 편집합니다.
   a. 변경할 네트워크를 선택합니다.
      - * 1 *: 그리드 네트워크
      - * 2 *: 관리 네트워크
      - * 3 *: 클라이언트 네트워크
      - * 4 *: 모든 네트워크 선택 후 프롬프트에 노드 이름, 네트워크 이름(Grid, Admin 또는 Client), 데이터 유형(IP/마스크, 게이트웨이, 즉 MTU)와 현재 값을 입력합니다.

        DHCP 구성 인터페이스의 IP 주소, 접두사 길이, 게이트웨이 또는 MTU를 편집하면 인터페이스가 정적 인터페이스로 변경됩니다. DHCP에서 구성한 인터페이스를 변경하도록 선택하면 인터페이스가 static으로 변경됨을 알리는 경고가 표시됩니다.

      Fixed로 설정된 인터페이스는 편집할 수 없습니다.

   b. 새 값을 설정하려면 현재 값에 대해 표시된 형식으로 입력합니다.
   c. 현재 값을 변경하지 않고 그대로 두려면 * Enter * 를 누릅니다.
   d. 데이터 유형이 'IP/마스크'인 경우 * d * 또는 * 0.0.0.0/0 * 을 입력하여 노드에서 Admin 또는 Client Network를 삭제할 수 있습니다.
   e. 변경할 모든 노드를 편집한 후 * q * 를 입력하여 기본 메뉴로 돌아갑니다.

변경 내용은 지워지거나 적용될 때까지 유지됩니다.

6. 다음 옵션 중 하나를 선택하여 변경 사항을 검토합니다.
   - * 5 *: 변경된 항목만 표시하도록 격리된 출력의 편집 내용을 표시합니다. 변경 사항은 예제 출력에 표시된 대로 녹색(추가) 또는 빨간색(삭제)으로 강조 표시됩니다.

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
Press Enter to continue
```

   - * 6 *: 전체 구성을 표시하는 출력의 편집 내용을 표시합니다. 변경 사항은 녹색(추가) 또는 빨간색(삭제)으로 강조 표시됩니다.

> 특정 명령줄 인터페이스에서는 취소선 서식을 사용하여 추가 및 삭제를 표시할 수 있습니다. 올바른 표시는 필요한 VT100 이스케이프 시퀀스를 지원하는 터미널 클라이언트에 따라 다릅니다.

7. 옵션 * 7 * 을 선택하여 모든 변경 사항을 확인합니다.

   이 유효성 검사를 통해 그리드, 관리자 및 클라이언트 네트워크에 대한 규칙(예: 중복되는 서브넷 사용 안 됨)이 위반되지 않도록 합니다.

   이 예제에서는 유효성 검사에서 오류가 반환되었습니다.

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   이 예제에서는 유효성 검사가 통과되었습니다.

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

Press Enter to continue
```

8. 정품 확인이 완료되면 다음 옵션 중 하나를 선택합니다.
   - * 8 *: 적용되지 않은 변경 사항을 저장합니다.

     이 옵션을 사용하면 적용되지 않은 변경 내용을 유지하면서 IP 변경 도구를 종료하고 나중에 다시 시작할 수 있습니다.

   - * 10 *: 새 네트워크 구성을 적용합니다.
9. 옵션 * 10 * 을 선택한 경우 다음 옵션 중 하나를 선택합니다.
   - * 적용 *: 변경 사항을 즉시 적용하고 필요한 경우 각 노드를 자동으로 다시 시작합니다.

     새 네트워크 구성에 물리적 네트워크 변경이 필요하지 않은 경우 * apply * 를 선택하여 변경 사항을 즉시 적용할 수 있습니다. 필요한 경우 노드가 자동으로 재시작됩니다. 다시 시작해야 하는 노드가 표시됩니다.

   - * stage *: 다음에 노드를 수동으로 재시작할 때 변경 사항을 적용합니다.

     새 네트워크 구성을 작동하기 위해 물리적 또는 가상 네트워킹 구성을 변경해야 하는 경우 * stage * 옵션을 사용하고, 영향을 받는 노드를 종료하고, 필요한 물리적 네트워킹 변경을 수행하고, 영향을 받는 노드를 다시 시작해야 합니다. 이러한 네트워킹 변경을 먼저 수행하지 않고 * 적용 * 을 선택하면 변경 사항이 대개 실패합니다.

     > stage * 옵션을 사용하는 경우 중단을 최소화하려면 스테이징 후 가능한 한 빨리 노드를 다시 시작해야 합니다.

   - * 취소 *: 현재 네트워크를 변경하지 마십시오.

     제안된 변경에 따라 노드를 다시 시작해야 한다는 사실을 모르는 경우 변경 사항을 연기하여 사용자에게 미치는 영향을 최소화할 수 있습니다. 취소 * 를 선택하면 기본 메뉴로 돌아가고 변경 내용을 보존하여 나중에 적용할 수 있습니다.

     APPLY * 또는 * stage * 를 선택하면 새 네트워크 구성 파일이 생성되고, 프로비저닝이 수행되고, 노드가 새 작업 정보로 업데이트됩니다.

     프로비저닝 중, 업데이트 적용 시 출력에 상태가 표시됩니다.

     ```
     Generating new grid networking description file...

     Running provisioning...

     Updating grid network configuration on Name
     ```

변경 사항을 적용하거나 스테이징한 후에 그리드 구성 변경으로 인해 새 복구 패키지가 생성됩니다.

10. 스테이지 * 를 선택한 경우 프로비저닝이 완료된 후 다음 단계를 따르십시오.
    a. 필요한 물리적 또는 가상 네트워킹을 변경합니다.
        - 물리적 네트워킹 변경 *: 필요한 경우 노드를 안전하게 종료하면서 필요한 물리적 네트워킹을 변경합니다.
        - Linux*: 관리 네트워크 또는 클라이언트 네트워크에 처음 노드를 추가하는 경우 ""기존 노드에 인터페이스 추가"에 설명된 대로 인터페이스를 추가했는지 확인하십시오.
    b. 영향을 받는 노드를 다시 시작합니다.
11. 변경이 완료된 후 IP 변경 도구를 종료하려면 * 0 * 을 선택합니다.
12. Grid Manager에서 새 복구 패키지를 다운로드합니다.
    a. 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
    b. 프로비저닝 암호를 입력합니다.

관련 정보

Linux: 기존 노드에 인터페이스를 추가합니다

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

Ubuntu 또는 Debian을 설치합니다

SG100 및 SG1000 서비스 어플라이언스

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

StorageGRID 관리

IP 주소를 구성합니다

관리자 네트워크에서 서브넷 목록을 추가하거나 변경합니다

하나 이상의 노드의 관리 네트워크 서브넷 목록에서 서브넷을 추가, 삭제 또는 변경할 수 있습니다.

필요한 것

- "passwords.txt" 파일이 있어야 합니다.

관리자 네트워크 서브넷 목록에 있는 모든 노드에 서브넷을 추가, 삭제 또는 변경할 수 있습니다.

단계

1. 기본 관리자 노드에 로그인합니다.
    a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
    b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
    c. 루트로 전환하려면 다음 명령을 입력합니다
    d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. Change IP Tool을 시작하려면 'change-ip' 명령을 입력합니다
3. 프롬프트에 프로비저닝 암호를 입력합니다.

   기본 메뉴가 나타납니다.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
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:
```

4. 선택적으로, 작업이 수행되는 네트워크/노드를 제한합니다. 다음 중 하나를 선택합니다.
   - 작업을 수행할 특정 노드를 필터링하려면 * 1 * 을 선택하여 편집할 노드를 선택합니다. 다음 옵션 중 하나를 선택합니다.
     - * 1 *: 단일 노드(이름으로 선택)
     - * 2 *: 단일 노드(사이트별, 이름별로 선택)
     - * 3 *: 단일 노드(현재 IP로 선택)
     - * 4 *: 사이트의 모든 노드
     - * 5 *: 그리드의 모든 노드
     - * 0 *: 뒤로 가기
   - ""모두""가 선택된 상태로 유지되도록 허용합니다. 선택을 하면 기본 메뉴 화면이 나타납니다. 선택한 노드 필드에는 새 선택 항목이 반영되며 이제 선택한 모든 작업이 이 항목에 대해서만 수행됩니다.
5. 주 메뉴에서 관리 네트워크의 서브넷을 편집하는 옵션을 선택합니다(옵션 * 3 *).
6. 다음 중 하나를 선택합니다.
   - 'CIDR 추가' 명령을 입력하여 서브넷을 추가합니다
   - del CIDR 명령을 입력하여 서브넷을 삭제합니다
   - 'CIDR 설정' 명령을 입력하여 서브넷 목록을 설정합니다

     모든 명령에 대해 'CIDR, CIDR 추가' 형식을 사용하여 여러 주소를 입력할 수 있습니다

     예: 'add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16'

     ""위쪽 화살표""를 사용하여 이전에 입력한 값을 현재 입력 프롬프트로 불러와 필요한 경우 편집하여 필요한 입력 양을 줄일 수 있습니다.

아래 입력 예는 관리자 네트워크 서브넷 목록에 서브넷을 추가하는 것을 보여줍니다.

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
  10.0.0.0/8
  172.19.0.0/16
  172.21.0.0/16
  172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

7. 준비가 되면 * q * 를 입력하여 기본 메뉴 화면으로 돌아갑니다. 변경 내용은 지워지거나 적용될 때까지 유지됩니다.

> 2단계에서 "모든" 노드 선택 모드를 선택한 경우 * Enter * (* q * 제외)를 눌러 목록의 다음 노드로 이동합니다.

8. 다음 중 하나를 선택합니다.

   - 옵션 * 5 * 를 선택하여 변경된 항목만 표시하도록 격리된 출력의 편집 내용을 표시합니다. 변경 사항은 아래 예제 출력에 표시된 것처럼 녹색(추가) 또는 빨간색(삭제)으로 강조 표시됩니다.

```
================================================================================
Site: Data Center 1
================================================================================
DC1-ADM1-105-154 Admin  Subnets                          add 172.17.0.0/16
                                                         del 172.16.0.0/16
                                 [      172.14.0.0/16 ]
                                 [      172.15.0.0/16 ]
                                 [      172.17.0.0/16 ]
                                 [      172.19.0.0/16 ]
                                 [      172.20.0.0/16 ]
                                 [      172.21.0.0/16 ]
Press Enter to continue
```

   - 옵션 * 6 * 을 선택하여 전체 구성을 표시하는 출력에 편집 내용을 표시합니다. 변경 사항은 녹색(추가) 또는 빨간색(삭제)으로 강조 표시됩니다. * 참고: * 특정 터미널 에뮬레이터는 취소선 서식을 사용하여 추가 및 삭제를 표시할 수 있습니다.

     서브넷 목록을 변경하려고 하면 다음 메시지가 표시됩니다.

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that are not
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
are not reachable using default StorageGRID routing, but are
reachable using a different interface and gateway. Making and
applying changes to the subnet list will make all automatically
applied subnets persistent. If you do not want that to happen, delete
the unwanted subnets before applying changes. If you know that all
/32 subnets in the list were added intentionally, you can ignore this
caution.
```

특별히 NTP 및 DNS 서버 서브넷을 네트워크에 할당하지 않은 경우 StorageGRID는 연결에 대한 호스트 라우트(/32)를 자동으로 생성합니다. 예를 들어, DNS 또는 NTP 서버에 대한 아웃바운드 연결에 /16 또는 /24 경로를 사용하려면 자동으로 생성된 /32 경로를 삭제하고 원하는 경로를 추가해야 합니다. 자동으로 생성된 호스트 라우트를 삭제하지 않으면 서브넷 목록에 변경 사항을 적용한 후 유지됩니다.

> 자동으로 검색된 이러한 호스트 라우트를 사용할 수 있지만 일반적으로 연결을 위해 DNS 및 NTP 라우트를 수동으로 구성해야 합니다.

9. 미리 구성된 모든 변경 내용을 확인하려면 옵션 * 7 * 을 선택합니다.

   이러한 유효성 검사를 통해 그리드, 관리자 및 클라이언트 네트워크에 대한 규칙이 겹친 서브넷을 사용하는 등 준수되도록 합니다.

10. 선택적으로 옵션 * 8 * 을 선택하여 모든 단계별 변경 사항을 저장하고 나중에 다시 돌아와 변경을 계속합니다.

    이 옵션을 사용하면 적용되지 않은 변경 내용을 유지하면서 IP 변경 도구를 종료하고 나중에 다시 시작할 수 있습니다.

11. 다음 중 하나를 수행합니다.
    - 새 네트워크 구성을 저장하거나 적용하지 않고 모든 변경 사항을 지우려면 옵션 * 9 * 를 선택합니다.
    - 변경 사항을 적용하고 새 네트워크 구성을 프로비저닝할 준비가 되었으면 옵션 * 10 * 을 선택합니다. 프로비저닝 중에 출력은 다음 샘플 출력에 표시된 것처럼 업데이트가 적용될 때 상태를 표시합니다.

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

12. Grid Manager에서 새 복구 패키지를 다운로드합니다.
    a. 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
    b. 프로비저닝 암호를 입력합니다.

관련 정보

IP 주소를 구성합니다

그리드 네트워크에서 서브넷 목록을 추가하거나 변경합니다

IP 변경 도구를 사용하여 그리드 네트워크에 서브넷을 추가하거나 변경할 수 있습니다.

필요한 것

- "passwords.txt" 파일이 있어야 합니다.

그리드 네트워크 서브넷 목록에서 서브넷을 추가, 삭제 또는 변경할 수 있습니다. 변경 사항은 그리드의 모든 노드의 라우팅에 영향을 미칩니다.

> Grid Network Subnet List(그리드 네트워크 서브넷 목록)만 변경하는 경우 Grid Manager(그리드 관리자)를 사용하여 네트워크 구성을 추가하거나 변경합니다. 그렇지 않으면 네트워크 구성 문제로 인해 그리드 관리자에 액세스할 수 없거나 그리드 네트워크 라우팅 변경 및 기타 네트워크 변경을 동시에 수행하는 경우 IP 변경 도구를 사용합니다.

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
2. Change IP Tool을 시작하려면 'change-ip' 명령을 입력합니다
3. 프롬프트에 프로비저닝 암호를 입력합니다.

   기본 메뉴가 나타납니다.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
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:
```

4. 주 메뉴에서 그리드 네트워크의 서브넷을 편집하는 옵션을 선택합니다(옵션 * 4 *).

> 그리드 네트워크 서브넷 목록에 대한 변경 사항은 그리드 전체에 적용됩니다.

5. 다음 중 하나를 선택합니다.
   - 'CIDR 추가' 명령을 입력하여 서브넷을 추가합니다
   - del CIDR 명령을 입력하여 서브넷을 삭제합니다
   - 'CIDR 설정' 명령을 입력하여 서브넷 목록을 설정합니다

     > 모든 명령에 대해 'CIDR, CIDR 추가' 형식을 사용하여 여러 주소를 입력할 수 있습니다

     예: 'add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16'

     > ""위쪽 화살표""를 사용하여 이전에 입력한 값을 현재 입력 프롬프트로 불러와 필요한 경우 편집하여 필요한 입력 양을 줄일 수 있습니다.

     아래 입력 예는 그리드 네트워크 서브넷 목록의 설정 서브넷을 보여줍니다.

```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
  172.16.0.0/21
  172.17.0.0/21
  172.18.0.0/21
  192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

6. 준비가 되면 * q * 를 입력하여 기본 메뉴 화면으로 돌아갑니다. 변경 내용은 지워지거나 적용될 때까지 유지됩니다.
7. 다음 중 하나를 선택합니다.
   - 옵션 * 5 * 를 선택하여 변경된 항목만 표시하도록 격리된 출력의 편집 내용을 표시합니다. 변경 사항은 아래 예제 출력에 표시된 것처럼 녹색(추가) 또는 빨간색(삭제)으로 강조 표시됩니다.

```
==========================================================================
Grid Network Subnet List (GNSL)
==========================================================================
                                                      add 172.30.0.0/21
                                                      add 172.31.0.0/21
                                                      del 172.16.0.0/21
                                                      del 172.17.0.0/21
                                                      del 172.18.0.0/21
                                  [      172.30.0.0/21 ]
                                  [      172.31.0.0/21 ]
                                  [     192.168.0.0/21 ]
Press Enter to continue
```

- 옵션 * 6 * 을 선택하여 전체 구성을 표시하는 출력에 편집 내용을 표시합니다. 변경 사항은 녹색(추가) 또는 빨간색(삭제)으로 강조 표시됩니다.

  > 특정 명령줄 인터페이스에서는 취소선 서식을 사용하여 추가 및 삭제를 표시할 수 있습니다.

8. 미리 구성된 모든 변경 내용을 확인하려면 옵션 * 7 * 을 선택합니다.

   이러한 유효성 검사를 통해 그리드, 관리자 및 클라이언트 네트워크에 대한 규칙이 겹친 서브넷을 사용하는 등 준수되도록 합니다.

9. 선택적으로 옵션 * 8 * 을 선택하여 모든 단계별 변경 사항을 저장하고 나중에 다시 돌아와 변경을 계속합니다.

   이 옵션을 사용하면 적용되지 않은 변경 내용을 유지하면서 IP 변경 도구를 종료하고 나중에 다시 시작할 수 있습니다.

10. 다음 중 하나를 수행합니다.
    - 새 네트워크 구성을 저장하거나 적용하지 않고 모든 변경 사항을 지우려면 옵션 * 9 * 를 선택합니다.
    - 변경 사항을 적용하고 새 네트워크 구성을 프로비저닝할 준비가 되었으면 옵션 * 10 * 을 선택합니다. 프로비저닝 중에 출력은 다음 샘플 출력에 표시된 것처럼 업데이트가 적용될 때 상태를 표시합니다.

    ```
    Generating new grid networking description file...

    Running provisioning...

    Updating grid network configuration on Name
    ```

11. 그리드 네트워크를 변경할 때 * 10 * 옵션을 선택한 경우 다음 옵션 중 하나를 선택합니다.
    - * 적용 *: 변경 사항을 즉시 적용하고 필요한 경우 각 노드를 자동으로 다시 시작합니다.

      새 네트워크 구성이 외부 변경 없이 기존 네트워크 구성과 동시에 작동하는 경우 완전 자동화된 구성 변경을 위해 * 적용 * 옵션을 사용할 수 있습니다.

    - * stage *: 다음에 노드를 재시작할 때 변경 사항을 적용합니다.

      새 네트워크 구성을 작동하기 위해 물리적 또는 가상 네트워킹 구성을 변경해야 하는 경우 * stage * 옵션을 사용하고, 영향을 받는 노드를 종료하고, 필요한 물리적 네트워킹 변경을 수행하고, 영향을 받는 노드를 다시 시작해야 합니다.

      > stage * 옵션을 사용하는 경우 중단을 최소화하려면 스테이징 후 가능한 한 빨리 노드를 다시 시작해야 합니다.

    - * 취소 *: 현재 네트워크를 변경하지 마십시오.

      제안된 변경에 따라 노드를 다시 시작해야 한다는 사실을 모르는 경우 변경 사항을 연기하여 사용자에게 미치는 영향을 최소화할 수 있습니다. 취소 * 를 선택하면 기본 메뉴로 돌아가고 변경 내용을 보존하여 나중에 적용할 수 있습니다.

변경 사항을 적용하거나 스테이징한 후에 그리드 구성 변경으로 인해 새 복구 패키지가 생성됩니다.

12. 오류로 인해 구성을 중지할 경우 다음 옵션을 사용할 수 있습니다.
    - IP 변경 절차를 중단하고 기본 메뉴로 돌아가려면 * a * 를 입력합니다.
    - 실패한 작업을 다시 시도하려면 * r * 를 입력합니다.
    - 다음 작업을 계속하려면 * c * 를 입력합니다.

      나중에 기본 메뉴에서 옵션 * 10 * (변경 내용 적용)을 선택하여 실패한 작업을 다시 시도할 수 있습니다. 모든 작업이 성공적으로 완료될 때까지 IP 변경 절차가 완료되지 않습니다.

    - 노드를 재부팅하기 위해 수동으로 개입해야 하고(예: 노드 재부팅) 실패한 것으로 생각되는 작업이 실제로 성공적으로 완료되었다고 확신하는 경우 * f * 를 입력하여 성공한 것으로 표시하고 다음 작업으로 이동합니다.
13. Grid Manager에서 새 복구 패키지를 다운로드합니다.
    a. 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
    b. 프로비저닝 암호를 입력합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

관련 정보

IP 주소를 구성합니다

그리드의 모든 노드에 대한 **IP** 주소를 변경합니다

그리드의 모든 노드에 대해 그리드 네트워크 IP 주소를 변경해야 하는 경우 이 특수 절차를 따라야 합니다. 개별 노드를 변경하는 절차를 사용하여 그리드 전체 그리드 네트워크 IP를 변경할 수는 없습니다.

필요한 것

- "passwords.txt" 파일이 있어야 합니다.

그리드가 성공적으로 시작되도록 하려면 모든 변경을 한 번에 수행해야 합니다.

> 이 절차는 그리드 네트워크에만 적용됩니다. 이 절차를 사용하여 관리 또는 클라이언트 네트워크의 IP 주소를 변경할 수 없습니다.

한 사이트에서만 노드의 IP 주소 및 MTU를 변경하려면 를 따릅니다 노드 네트워크 구성을 변경합니다 지침.

단계

1. DNS 또는 NTP 변경 등 Change IP 도구 외부에서 변경해야 하는 변경 사항과 SSO(Single Sign-On) 구성 변경(사용되는 경우)을 미리 계획하십시오.

> 기존 NTP 서버가 새 IP 주소의 그리드에 액세스할 수 없는 경우 change-IP 절차를 수행하기 전에 새 NTP 서버를 추가하십시오.

> 기존 DNS 서버가 새 IP 주소의 그리드에 액세스할 수 없는 경우 change-IP 절차를 수행하기 전에 새 DNS 서버를 추가하십시오.

> StorageGRID 시스템에 SSO가 설정되어 있고 모든 기반 당사자 트러스트가 관리자 노드 IP 주소(권장되는 경우 정규화된 도메인 이름 대신)를 사용하여 구성된 경우 AD FS(Active Directory Federation Services)에서 이러한 기반 당사자 트러스트를 업데이트하거나 재구성할 준비를 해야 합니다. IP 주소를 변경한 직후 StorageGRID 관리 지침을 참조하십시오.

> 필요한 경우 새 IP 주소에 대한 새 서브넷을 추가합니다.

2. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.
3. Change IP Tool을 시작하려면 'change-ip' 명령을 입력합니다
4. 프롬프트에 프로비저닝 암호를 입력합니다.

   기본 메뉴가 나타납니다. 기본적으로 '선택한 노드' 필드는 '모두'로 설정됩니다.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
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:
```

5. 주 메뉴에서 * 2 * 를 선택하여 모든 노드에 대한 IP/서브넷 마스크, 게이트웨이 및 MTU 정보를 편집합니다.
   a. 그리드 네트워크를 변경하려면 * 1 * 을 선택합니다.

      선택한 후 프롬프트에 노드 이름, 그리드 네트워크 이름, 데이터 유형(IP/마스크, 게이트웨이 또는 MTU), 및 현재 값.

      DHCP 구성 인터페이스의 IP 주소, 접두사 길이, 게이트웨이 또는 MTU를 편집하면 인터페이스가 정적 인터페이스로 변경됩니다. DHCP로 구성된 각 인터페이스 앞에 경고가 표시됩니다.

   Fixed로 설정된 인터페이스는 편집할 수 없습니다.

   a. 새 값을 설정하려면 현재 값에 대해 표시된 형식으로 입력합니다.
   b. 변경할 모든 노드를 편집한 후 * q * 를 입력하여 기본 메뉴로 돌아갑니다.

변경 내용은 지워지거나 적용될 때까지 유지됩니다.

6. 다음 옵션 중 하나를 선택하여 변경 사항을 검토합니다.
   - * 5 *: 변경된 항목만 표시하도록 격리된 출력의 편집 내용을 표시합니다. 변경 사항은 예제 출력에 표시된 대로 녹색(추가) 또는 빨간색(삭제)으로 강조 표시됩니다.

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
Press Enter to continue
```

   - * 6 *: 전체 구성을 표시하는 출력의 편집 내용을 표시합니다. 변경 사항은 녹색(추가) 또는 빨간색(삭제)으로 강조 표시됩니다.

> ⓘ 특정 명령줄 인터페이스에서는 취소선 서식을 사용하여 추가 및 삭제를 표시할 수 있습니다. 올바른 표시는 필요한 VT100 이스케이프 시퀀스를 지원하는 터미널 클라이언트에 따라 다릅니다.

7. 옵션 * 7 * 을 선택하여 모든 변경 사항을 확인합니다.

   이 유효성 검사를 통해 그리드 네트워크에 대한 규칙이 겹친 서브넷을 사용하지 않는 등의 규칙을 위반하지 않도록 할 수 있습니다.

   이 예제에서는 유효성 검사에서 오류가 반환되었습니다.

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   이 예제에서는 유효성 검사가 통과되었습니다.

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

Press Enter to continue
```

8. 유효성 검사에 통과하면 * 10 * 을 선택하여 새 네트워크 구성을 적용합니다.
9. 다음에 노드를 다시 시작할 때 변경 사항을 적용하려면 * stage * 를 선택합니다.

> 스테이지 * 를 선택해야 합니다. 수동으로 또는 * stage * 대신 * apply * 를 선택하여 롤링 재시작을 수행하지 마십시오. 그리드가 성공적으로 시작되지 않습니다.

10. 변경이 완료되면 * 0 * 을 선택하여 IP 변경 도구를 종료합니다.
11. 모든 노드를 동시에 종료합니다.

> 모든 노드가 동시에 종료되도록 전체 그리드를 한 번에 종료해야 합니다.

12. 필요한 물리적 또는 가상 네트워킹을 변경합니다.
13. 모든 그리드 노드가 다운되었는지 확인합니다.
14. 모든 노드의 전원을 켭니다.
15. 그리드가 성공적으로 시작되면:
    a. 새 NTP 서버를 추가한 경우 이전 NTP 서버 값을 삭제합니다.
    b. 새 DNS 서버를 추가한 경우 이전 DNS 서버 값을 삭제합니다.
16. Grid Manager에서 새 복구 패키지를 다운로드합니다.
    a. 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
    b. 프로비저닝 암호를 입력합니다.

관련 정보

StorageGRID 관리

그리드 네트워크에서 서브넷 목록을 추가하거나 변경합니다

그리드 노드를 종료합니다

기존 노드에 인터페이스를 추가합니다

Linux: 기존 노드에 관리자 또는 클라이언트 인터페이스를 추가합니다

다음 단계를 수행하여 관리자 네트워크 또는 클라이언트 네트워크의 인터페이스를 Linux 노드에 설치합니다.

설치 중에 Linux 호스트의 노드 구성 파일에 admin_network_target 또는 client_network_target을 구성하지 않은 경우 이 절차를 사용하여 인터페이스를 추가합니다. 노드 구성 파일에 대한 자세한 내용은 Linux 운영 체제에 대한 지침을 참조하십시오.

- Red Hat Enterprise Linux 또는 CentOS를 설치합니다
- Ubuntu 또는 Debian을 설치합니다

노드 내부가 아닌 새 네트워크 할당이 필요한 노드를 호스팅하는 Linux 서버에서 이 절차를 수행합니다. 이 절차에서는 노드에만 인터페이스를 추가합니다. 다른 네트워크 매개 변수를 지정하려고 하면 유효성 검사 오류가 발생합니다.

주소 지정 정보를 제공하려면 IP 변경 도구를 사용해야 합니다. 을 참조하십시오 노드 네트워크 구성을 변경합니다.

단계

1. 노드를 호스팅하는 Linux 서버에 로그인합니다.
2. 노드 구성 파일('/etc/StorageGrid/nodes/*node-name*.conf)을 편집합니다.

   > 다른 네트워크 매개 변수를 지정하지 마십시오. 그렇지 않으면 유효성 검사 오류가 발생합니다.

   a. 새 네트워크 대상에 대한 항목을 추가합니다. 예를 들면 다음과 같습니다.

      'client_network_target=bond0.3206'

   b. 선택 사항: MAC 주소에 대한 항목을 추가합니다. 예를 들면 다음과 같습니다.

      'client_network_MAC=aa:57:61:07:ea:5c'

3. node validate 명령을 실행합니다.

   'SUDO StorageGRID node validate_node-name_'

4. 모든 유효성 검사 오류를 해결합니다.
5. 노드 다시 로드 명령을 실행합니다.

   'SUDO StorageGRID NODE RELOAD_NODE-NAME_'

Linux: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다

Linux 노드를 설치한 후 추가 트렁크 또는 액세스 인터페이스를 추가할 수 있습니다. 추가한 인터페이스는 VLAN 인터페이스 페이지와 HA 그룹 페이지에 표시됩니다.

필요한 것

- Linux 플랫폼에 StorageGRID를 설치하는 지침을 액세스할 수 있습니다.
  - Red Hat Enterprise Linux 또는 CentOS를 설치합니다
  - Ubuntu 또는 Debian을 설치합니다
- "passwords.txt" 파일이 있습니다.
- 특정 액세스 권한이 있습니다.

> 소프트웨어 업그레이드, 복구 절차 또는 확장 절차가 활성 상태인 동안에는 노드에 인터페이스를 추가하지 마십시오.

이 작업에 대해

노드를 설치한 후 Linux 노드에 하나 이상의 추가 인터페이스를 추가하려면 다음 단계를 수행하십시오. 예를 들어, 관리 또는 게이트웨이 노드에 트렁크 인터페이스를 추가하여 VLAN 인터페이스를 사용하여 다른 애플리케이션이나 테넌트에 속한 트래픽을 분리할 수 있습니다. 또는 고가용성(HA) 그룹에서 사용할 액세스 인터페이스를 추가할 수도 있습니다.

트렁크 인터페이스를 추가하는 경우 StorageGRID에서 VLAN 인터페이스를 구성해야 합니다. 액세스 인터페이스를 추가할 경우 인터페이스를 HA 그룹에 직접 추가할 수 있으며, VLAN 인터페이스를 구성할 필요가 없습니다.

인터페이스를 추가할 때 노드를 잠시 사용할 수 없습니다. 이 절차는 한 번에 하나의 노드에서 수행해야 합니다.

단계

1. 노드를 호스팅하는 Linux 서버에 로그인합니다.
2. vim 또는 pico와 같은 텍스트 편집기를 사용하여 노드 구성 파일을 편집합니다.

   '/etc/StorageGrid/nodes/*node-name*.conf'

3. 파일에 항목을 추가하여 이름을 지정하고 선택적으로 노드에 추가할 각 추가 인터페이스에 대한 설명을 지정합니다. 이 형식을 사용합니다.

   'interfaces_target_nnnn=*value*'

   nnnn_의 경우 추가하려는 각 "interfaces_target" 항목에 대해 고유 번호를 지정합니다.

   value_에 대해 베어 메탈 호스트의 물리적 인터페이스 이름을 지정합니다. 그런 다음 필요에 따라 쉼표를 추가하고 인터페이스에 대한 설명을 입력합니다. 이 설명은 VLAN 인터페이스 페이지와 HA 그룹 페이지에 표시됩니다.

   예를 들면 다음과 같습니다.

   interfaces_target_01=en256, 트렁크

   > 다른 네트워크 매개 변수를 지정하지 마십시오. 그렇지 않으면 유효성 검사 오류가 발생합니다.

4. 다음 명령을 실행하여 노드 구성 파일의 변경 내용을 검증합니다.

   'SUDO StorageGRID node validate_node-name_'

   다음 단계로 진행하기 전에 오류 또는 경고를 모두 해결하십시오.

5. 다음 명령을 실행하여 노드의 구성을 업데이트합니다.

   'SUDO StorageGRID NODE RELOAD_NODE-NAME_'

작업을 마친 후

- 하나 이상의 트렁크 인터페이스를 추가한 경우 로 이동합니다 VLAN 인터페이스를 구성합니다 각 새 상위 인터페이스에 대해 하나 이상의 VLAN 인터페이스를 구성하려면 다음을 수행합니다.
- 하나 이상의 액세스 인터페이스를 추가한 경우 로 이동합니다 고가용성 그룹을 구성합니다 새 인터페이스를 HA 그룹에 직접 추가합니다.

VMware: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다

노드가 설치된 후 VM 노드에 트렁크 또는 액세스 인터페이스를 추가할 수 있습니다. 추가한

인터페이스는 VLAN 인터페이스 페이지와 HA 그룹 페이지에 표시됩니다.

필요한 것

- VMware 플랫폼에 StorageGRID를 설치하는 방법에 대한 지침을 볼 수 있습니다.

VMware를 설치합니다

- StorageGRID 11.6을 구성했습니다.
- 관리 노드 및 게이트웨이 노드 VMware 가상 시스템이 있습니다.
- 그리드, 관리자 또는 클라이언트 네트워크로 사용되지 않는 네트워크 서브넷이 있습니다.
- "passwords.txt" 파일이 있습니다.
- 특정 액세스 권한이 있습니다.

> 소프트웨어 업그레이드, 복구 절차 또는 확장 절차가 활성 상태인 동안에는 노드에 인터페이스를 추가하지 마십시오.

이 작업에 대해

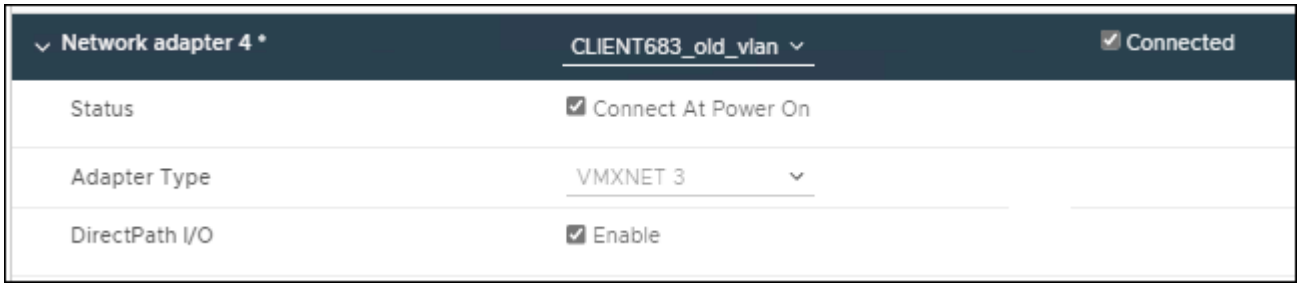
노드를 설치한 후 VMware 노드에 인터페이스를 하나 이상 추가하려면 다음 단계를 수행합니다. 예를 들어, 관리 또는 게이트웨이 노드에 트렁크 인터페이스를 추가하여 VLAN 인터페이스를 사용하여 다른 애플리케이션이나 테넌트에 속한 트래픽을 분리할 수 있습니다. 또는 고가용성(HA) 그룹에서 사용할 액세스 인터페이스를 추가할 수도 있습니다.

트렁크 인터페이스를 추가하는 경우 StorageGRID에서 VLAN 인터페이스를 구성해야 합니다. 액세스 인터페이스를 추가할 경우 인터페이스를 HA 그룹에 직접 추가할 수 있으며, VLAN 인터페이스를 구성할 필요가 없습니다.

인터페이스를 추가할 때 노드를 잠시 동안 사용할 수 없을 수도 있습니다.

단계

1. vCenter에서 관리 노드 및 게이트웨이 노드 VM에 새 네트워크 어댑터(VMXNET3 입력)를 추가합니다. Connected * 및 * Connect at Power On * 확인란을 선택합니다.



2. SSH를 사용하여 관리자 노드 또는 게이트웨이 노드에 로그인합니다.
3. IP LINK show를 사용하여 새로운 네트워크 인터페이스 ens256이 감지되는지 확인한다.

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT
group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

작업을 마친 후

- 하나 이상의 트렁크 인터페이스를 추가한 경우 로 이동합니다 VLAN 인터페이스를 구성합니다 각 새 상위 인터페이스에 대해 하나 이상의 VLAN 인터페이스를 구성하려면 다음을 수행합니다.
- 하나 이상의 액세스 인터페이스를 추가한 경우 로 이동합니다 고가용성 그룹을 구성합니다 새 인터페이스를 HA 그룹에 직접 추가합니다.

DNS 서버를 구성합니다

IP 주소 대신 FQDN(정규화된 도메인 이름) 호스트 이름을 사용할 수 있도록 DNS(도메인 이름 시스템) 서버를 추가, 제거 및 업데이트할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.
- 구성할 DNS 서버의 IP 주소가 있어야 합니다.

DNS 서버 정보를 지정하면 e-메일 또는 SNMP 알림 및 AutoSupport에 대한 IP 주소 대신 FQDN(정규화된 도메인 이름) 호스트 이름을 사용할 수 있습니다. DNS 서버를 두 개 이상 지정하는 것이 좋습니다.

> DNS 서버에 대해 2-6개의 IP 주소를 제공합니다. 일반적으로 네트워크 연결 시 각 사이트에서 로컬로 액세스할 수 있는 DNS 서버를 선택합니다. 이는 Is착륙한 사이트가 계속해서 DNS 서비스에 액세스할 수 있도록 하기 위한 것입니다. 그리드 전체 DNS 서버 목록을 구성한 후 를 사용할 수 있습니다 각 노드에 대해 DNS 서버 목록을 추가로 사용자 지정합니다.

DNS 서버 정보가 생략되거나 잘못 구성된 경우 각 그리드 노드의 SSM 서비스에서 NST 알람이 트리거됩니다. DNS가 올바르게 구성되고 새 서버 정보가 모든 그리드 노드에 도달하면 경보가 해제됩니다.

단계

1. 유지 관리 * > * 네트워크 * > * DNS 서버 * 를 선택합니다.
2. 서버 섹션에서 필요에 따라 업데이트를 추가하거나 DNS 서버 항목을 제거합니다.

   모범 사례는 사이트당 DNS 서버를 2개 이상 지정하는 것입니다. 최대 6개의 DNS 서버를 지정할 수 있습니다.

3. 저장 * 을 클릭합니다.

단일 그리드 노드에 대한 **DNS** 구성을 수정합니다

전체 배포에 대해 DNS(Domain Name System)를 전역적으로 구성하는 대신 스크립트를 실행하여 각 그리드 노드에 대해 DNS를 다르게 구성할 수 있습니다.

일반적으로 Grid Manager의 * 유지보수 * > * 네트워크 * > * DNS 서버 * 옵션을 사용하여 DNS 서버를 구성해야 합니다. 다른 그리드 노드에 다른 DNS 서버를 사용해야 하는 경우에만 다음 스크립트를 사용하십시오.

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

   e. SSH 에이전트에 SSH 개인 키를 추가합니다. ssh-add를 입력합니다
   f. "passwords.txt" 파일에 나열된 SSH 액세스 암호를 입력합니다.
2. 사용자 지정 DNS 구성인 'ssh_node_ip_address_'로 업데이트할 노드에 로그인합니다
3. DNS 설정 스크립트 'setup_resolv.rb.'를 실행합니다

   스크립트는 지원되는 명령 목록으로 응답합니다.

```
Tool to modify external name servers

available commands:
  add search <domain>
               add a specified domain to search list
               e.g.> add search netapp.com
  remove search <domain>
               remove a specified domain from list
               e.g.> remove search netapp.com
  add nameserver <ip>
               add a specified IP address to the name server list
               e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
               remove a specified IP address from list
               e.g.> remove nameserver 192.0.2.65
  remove nameserver all
               remove all nameservers from list
  save         write configuration to disk and quit
  abort        quit without saving changes
  help         display this help message


Current list of name servers:
    192.0.2.64
Name servers inherited from global DNS configuration:
    192.0.2.126
    192.0.2.127
Current list of search entries:
    netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
               [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

4. '<nameserver ip_address>' 네트워크에 도메인 이름 서비스를 제공하는 서버의 IPv4 주소를 추가합니다
5. 이름 서버를 추가하려면 '이름 서버 추가' 명령을 반복합니다.
6. 다른 명령을 묻는 메시지가 나타나면 지침을 따릅니다.
7. 변경 사항을 저장하고 '저장' 응용 프로그램을 종료합니다
8. 서버의 명령 셸을 닫습니다. 'exit'
9. 각 그리드 노드에 대해 의 단계를 반복합니다 노드에 로그인합니다 부터 까지 명령 셸을 닫습니다.
10. 다른 서버에 대한 암호 없는 액세스가 더 이상 필요하지 않으면 SSH 에이전트에서 개인 키를 제거합니다. ssh-add-D를 입력합니다

NTP 서버를 구성합니다

StorageGRID 시스템의 그리드 노드 간에 데이터가 정확하게 동기화되도록 NTP(네트워크 시간 프로토콜) 서버를 추가, 업데이트 또는 제거할 수 있습니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.
- 구성할 NTP 서버의 IPv4 주소가 있어야 합니다.

이 작업에 대해

StorageGRID 시스템은 NTP(네트워크 시간 프로토콜)를 사용하여 그리드의 모든 그리드 노드 간에 시간을 동기화합니다.

각 사이트에서 StorageGRID 시스템의 노드 2개 이상에 기본 NTP 역할이 할당됩니다. 이들은 최소 4개, 최대 6개의 외부 시간 소스와 상호 동기화됩니다. StorageGRID 시스템의 기본 NTP 노드가 아닌 모든 노드는 NTP 클라이언트로 작동하며 이러한 기본 NTP 노드와 동기화됩니다.

외부 NTP 서버는 이전에 기본 NTP 역할을 할당한 노드에 연결됩니다. 따라서 주 NTP 역할이 있는 노드를 두 개 이상 지정하는 것이 좋습니다.

> 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.

지정된 외부 NTP 서버는 NTP 프로토콜을 사용해야 합니다. 시간 드리프트와 관련된 문제를 방지하려면 Stratum 3 이상의 NTP 서버 참조를 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 Windows의 시간 서비스는 정확하지 않으며 StorageGRID와 같은 고정밀 환경에서 사용하기 위해 Microsoft에서 지원되지 않습니다.

"정확도가 높은 환경에 대한 Windows 시간 서비스를 구성하기 위한 경계를 지원합니다"

설치 중에 원래 지정한 NTP 서버의 안정성 또는 가용성에 문제가 발생하면 StorageGRID 시스템에서 서버를 추가하거나 기존 서버를 업데이트 또는 제거하여 사용하는 외부 NTP 소스 목록을 업데이트할 수 있습니다.

단계

1. 유지보수 * > * 네트워크 * > * NTP 서버 * 를 선택합니다.
2. Servers 섹션에서 필요에 따라 업데이트를 추가하거나 NTP 서버 항목을 제거합니다.

   NTP 서버는 4개 이상 포함해야 하며 최대 6개의 서버를 지정할 수 있습니다.

3. Provisioning Passphrase * 텍스트 상자에 StorageGRID 시스템의 프로비저닝 암호를 입력하고 * Save * 를 클릭합니다.

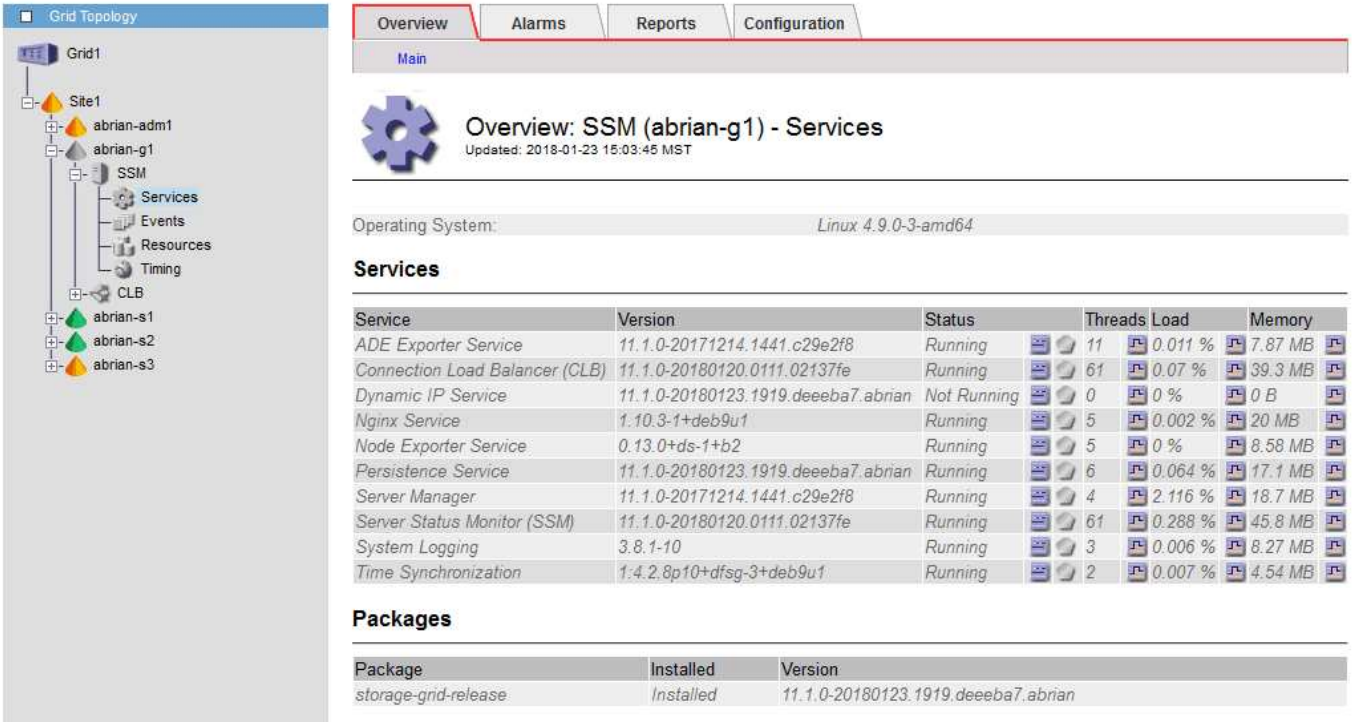
절차 상태가 페이지 상단에 표시됩니다. 구성 업데이트가 완료될 때까지 페이지가 비활성화됩니다.

> 새 NTP 서버를 저장한 후 모든 NTP 서버가 연결 테스트에 실패하면 계속 진행하지 마십시오. 기술 지원 부서에 문의하십시오.

격리된 노드의 네트워크 연결을 복구합니다

사이트 또는 그리드 전체 IP 주소 변경과 같은 특정 상황에서는 하나 이상의 노드 그룹이 나머지 그리드에 연결되지 않을 수 있습니다.

Grid Manager(* support*>* Tools*>* Grid topology*)에서 노드가 회색이거나, 실행 중이 아닌 다른 상태를 표시하는 서비스 중 많은 서비스가 있는 파란색 노드인 경우 노드 격리를 확인해야 합니다.



분리된 노드가 있을 경우 다음과 같은 결과가 발생할 수 있습니다.

- 여러 노드가 격리된 경우 에 로그인하거나 Grid Manager에 액세스하지 못할 수 있습니다.
- 여러 노드가 격리된 경우 테넌트 관리자의 대시보드에 표시되는 스토리지 사용량 및 할당량 값이 최신 상태가 아닐 수 있습니다. 네트워크 연결이 복원되면 합계가 업데이트됩니다.

격리 문제를 해결하려면 격자에서 격리된 각 격리된 노드나 그룹의 한 노드(기본 관리 노드를 포함하지 않는 서브넷의 모든 노드)에서 명령줄 유틸리티를 실행합니다. 이 유틸리티는 노드가 격자에서 격리되지 않은 노드의 IP 주소를 제공하여 격리된 노드 또는 노드 그룹이 전체 그리드에 다시 접속하도록 합니다.

> 네트워크에서 mDNS(multicast Domain Name System)를 사용하지 않도록 설정한 경우 격리된 각 노드에서 명령줄 유틸리티를 실행해야 할 수 있습니다.

1. 노드를 액세스하고 격리 메시지에 대해 '/var/local/log/dynip.log'를 확인합니다.

   예를 들면 다음과 같습니다.

```
[2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
no contact with other nodes.
If this warning persists, manual action may be required.
```

VMware 콘솔을 사용 중인 경우 노드를 격리할 수 있다는 메시지가 표시됩니다.

Linux 배포에서 격리 메시지는 "/var/log/StorageGrid/node/<nodename>.log" 파일에 나타납니다.

2. 격리 메시지가 반복되고 영구인 경우 다음 명령을 실행합니다.

   ' add_node_ip.py <address>'

   여기서 "<address>"는 그리드에 연결된 원격 노드의 IP 주소입니다.

```
# /usr/sbin/add_node_ip.py  10.224.4.210

Retrieving local host information
Validating remote node at address 10.224.4.210
Sending node IP hint for 10.224.4.210 to local node
Local node found on remote node. Update complete.
```

3. 이전에 격리된 각 노드에 대해 다음을 확인합니다.
   - 노드의 서비스가 시작되었습니다.
   - Dynamic IP Service의 상태는 'toragegrid-status' 명령어를 실행한 후 'Running' 상태가 된다.
   - Grid Topology(그리드 토폴로지) 트리에서 노드가 더 이상 나머지 그리드에서 연결 해제된 것으로 나타나지 않습니다.

> add_node_ip.py 명령을 실행해도 문제가 해결되지 않으면 해결해야 할 다른 네트워킹 문제가 있을 수 있습니다.

호스트 레벨 및 미들웨어 절차

일부 유지 보수 절차는 StorageGRID의 Linux 또는 VMware 배포에만 국한되거나 StorageGRID 솔루션의 다른 구성 요소에 한정됩니다.

Linux: 그리드 노드를 새 호스트로 마이그레이션

StorageGRID 노드를 한 Linux 호스트에서 다른 Linux 호스트로 마이그레이션하여 그리드의 기능 또는 가용성에 영향을 주지 않고 호스트 유지 관리(예: OS 패치 적용 및 재부팅)를 수행할 수 있습니다.

한 Linux 호스트("소스 호스트")에서 다른 Linux 호스트(""대상 호스트")로 하나 이상의 노드를 마이그레이션합니다. 타겟 호스트는 이전에 StorageGRID를 사용할 준비가 되어 있어야 합니다.

마이그레이션 지원을 포함하도록 StorageGRID 배포를 계획한 경우에만 이 절차를 사용할 수 있습니다.

그리드 노드를 새 호스트로 마이그레이션하려면 다음 두 조건이 모두 충족되어야 합니다.

- 공유 스토리지는 모든 노드별 스토리지 볼륨에 사용됩니다
- 네트워크 인터페이스는 호스트 간에 일관된 이름을 갖습니다

운영 구축 시 단일 호스트에서 스토리지 노드를 두 개 이상 실행하지 마십시오. 각 스토리지 노드에 대해 전용 호스트를 사용하면 격리된 장애 도메인이 제공됩니다.

관리 노드 또는 게이트웨이 노드와 같은 다른 유형의 노드를 동일한 호스트에 구축할 수 있습니다. 그러나 같은 유형의 여러 노드(예: 게이트웨이 노드 2개)가 있는 경우 같은 호스트에 모든 인스턴스를 설치하지 마십시오.

자세한 내용은 사용 중인 Linux 운영 체제에 대한 StorageGRID 설치 지침의 "노드 마이그레이션 요구 사항"을 참조하십시오.

관련 정보

새 Linux 호스트를 배포합니다

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

Ubuntu 또는 Debian을 설치합니다

Linux: 소스 호스트에서 노드를 내보냅니다

그리드 노드를 종료하고 소스 Linux 호스트에서 내보냅니다.

소스 Linux 호스트에서 다음 명령을 실행합니다.

1. 소스 호스트에서 현재 실행 중인 모든 노드의 상태를 가져옵니다.

   ```
   sudo storagegrid node status all
   ```

   이름 설정 - 상태 실행 상태

   DC1-ADM1 configured running'입니다

   'dC1-ARC1 구성됨'

   dC1-GW1이 실행 중'으로 구성되었습니다

   'dC1-S1 configured running'입니다

   dC1-S2 configured running(dC1-S2 러닝 구성)

   dC1-S3이 실행 중 상태로 구성되었습니다

2. 마이그레이션하려는 노드의 이름을 확인하고 해당 노드의 실행 상태가 '실행 중'인 경우 중지합니다.

```
sudo storagegrid node stop DC1-S3
```

'노드 DC1-S3'를 선택합니다

노드 종료를 위해 최대 630초간 기다리는 중입니다

3. 소스 호스트에서 노드를 내보냅니다.

```
sudo storagegrid node export DC1-S3
```

"노드 DC1-S3을 /dev/mapper/SGWs-dc1-s3-var-local로 내보내기를 마쳤습니다.

"StorageGRID node import/dev/mapper/SGWs-dc1-s3-var-local'을 사용합니다.

다시 가져오길 원해

4. 내보내기 명령의 출력에 제시된 가져오기 명령을 기록해 둡니다.

다음 단계에서 타겟 호스트에서 이 명령을 실행합니다.

Linux: 대상 호스트에서 노드 가져오기

소스 호스트에서 노드를 내보낸 후 타겟 Linux 호스트에서 노드를 가져오고 유효성을 검사합니다. 검증에서 노드가 소스 호스트와 동일한 블록 스토리지 및 네트워크 인터페이스 디바이스를 액세스할 수 있는지 확인합니다.

대상 Linux 호스트에서 다음 명령을 실행합니다.

1. 타겟 호스트에서 노드를 가져옵니다.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

/dev/mapper/SGWs-dc1-s3-var-local에서 노드 DC1-S3의 가져오기를 마쳤습니다

"StorageGRID node validate DC1-S3"를 실행해야 합니다

2. 새 호스트에서 노드 구성을 검증합니다.

```
sudo storagegrid node validate DC1-S3
```

'노드 DC1-S3의 존재 확인 중... Passed +()

'노드 DC1-S3에 대한 구성 파일 /etc/StorageGrid/nodes/DC1-s3.conf 확인 중... Passed +()

'고유 값의 중복 확인 중... Passed +()

3. 유효성 검사 오류가 발생하면 마이그레이션된 노드를 시작하기 전에 이를 해결하십시오.

   문제 해결 정보는 Linux 운영 체제의 StorageGRID 설치 지침을 참조하십시오.

관련 정보

Red Hat Enterprise Linux 또는 CentOS를 설치합니다

Ubuntu 또는 Debian을 설치합니다

Linux: 마이그레이션된 노드를 시작합니다

마이그레이션된 노드의 유효성을 검증한 후 타겟 Linux 호스트에서 명령을 실행하여 노드를 시작합니다.

단계

1. 새 호스트에서 노드를 시작합니다.

```
sudo storagegrid node start DC1-S3
Starting node DC1-S3
```

2. Grid Manager에서 노드의 상태가 녹색으로 표시되고 알람이 발생하지 않는지 확인합니다.

   > 노드 상태가 녹색인지 확인하면 마이그레이션된 노드가 완전히 다시 시작되고 그리드에 다시 조인됩니다. 상태가 녹색이 아닌 경우 둘 이상의 노드가 서비스 상태가 되지 않도록 추가 노드를 마이그레이션하지 마십시오.

   Grid Manager에 액세스할 수 없는 경우 10분 정도 기다린 후 다음 명령을 실행합니다.

   'SUDO StorageGRID NODE STATUS *NODE-NAME* *'

   마이그레이션된 노드에 '실행 중'의 실행 상태가 있는지 확인합니다.

TSM 미들웨어를 위한 아카이브 노드 유지 보수

아카이브 노드는 TSM 미들웨어 서버를 통해 테이프나 S3 API를 통해 클라우드로 대상을 겨냥하도록 구성할 수 있습니다. 구성 후에는 아카이브 노드의 타겟을 변경할 수 없습니다.

보관 노드를 호스팅하는 서버에 오류가 발생하면 서버를 교체하고 적절한 복구 절차를 따릅니다.

보관 저장 장치에 결함이 있습니다

아카이브 노드가 TSM(Tivoli Storage Manager)을 통해 액세스하는 아카이브 스토리지 디바이스에 장애가 있는 경우 아카이브 노드를 오프라인으로 전환하여 StorageGRID 시스템에 표시되는 알람 수를 제한합니다. 그런 다음 TSM 서버 또는 스토리지 디바이스의 관리 툴을 사용하거나 둘 모두를 사용하여 문제를 추가로 진단하고 해결할 수 있습니다.

대상 구성 요소를 오프라인으로 전환합니다

TSM 미들웨어 서버를 Archive Node에서 사용할 수 없게 될 수 있는 TSM 미들웨어 서버를 유지 관리하기 전에 Target 구성 요소를 오프라인으로 전환하여 TSM 미들웨어 서버를 사용할 수 없게 될 경우 트리거되는 알람 수를 제한합니다.

필요한 것

를 사용하여 그리드 관리자에 로그인해야 합니다 지원되는 웹 브라우저.

단계

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. Archive Node * > * ARC * > * Target * > * Configuration * > * Main * 을 선택합니다.
3. Tivoli Storage Manager State의 값을 * Offline * 으로 변경하고 * Apply Changes * 를 클릭합니다.
4. 유지 관리가 완료되면 Tivoli Storage Manager State의 값을 * Online * 으로 변경하고 * Apply Changes * 를 클릭합니다.

Tivoli Storage Manager 관리 툴

dsmadmc 툴은 아카이브 노드에 설치된 TSM 미들웨어 서버의 관리 콘솔입니다. 서버의 명령줄에 dsmadmc를 입력하여 도구에 액세스할 수 있습니다. ARC 서비스에 대해 구성된 것과 동일한 관리 사용자 이름과 암호를 사용하여 관리 콘솔에 로그인합니다.

dsmadmc에서 보다 읽기 쉬운 형식으로 상태 정보를 생성하기 위해 tsmquery.rb 스크립트를 만들었습니다. 아카이브 노드의 명령줄에 "/usr/local/arc/tsmquery.rb status"를 입력하여 이 스크립트를 실행할 수 있습니다

TSM 관리 콘솔 dsmadmc에 대한 자세한 내용은 _Tivoli Storage Manager for Linux: AdministratorNAC's Reference_를 참조하십시오.

개체를 영구적으로 사용할 수 없습니다

아카이브 노드가 TSM(Tivoli Storage Manager) 서버에서 객체를 요청하고 검색에 실패하면 아카이브 노드는 10초 간격으로 요청을 재시도합니다. 객체가 영구적으로 사용 불가능한 경우(예: 객체가 테이프에서 손상되었기 때문에) TSM API가 이를 아카이브 노드에 표시할 방법이 없으므로 아카이브 노드가 요청을 계속 재시도합니다.

이 상황이 발생하면 알람이 트리거되고 값이 계속 증가합니다. 경보를 보려면 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 * Archive Node * > * ARC * > * Retrieve * > * Request Failures * 를 선택합니다.

개체를 영구적으로 사용할 수 없는 경우 개체를 식별한 다음 절차에 설명된 대로 아카이브 노드의 요청을 수동으로 취소해야 합니다. 개체를 영구적으로 사용할 수 있는지 여부를 확인합니다.

개체를 일시적으로 사용할 수 없는 경우에도 검색이 실패할 수 있습니다. 이 경우 후속 검색 요청이 성공해야 합니다.

StorageGRID 시스템이 단일 오브젝트 복사본을 생성하는 ILM 규칙을 사용하도록 구성되어 있고 해당 복사본을 검색할 수 없으면 개체가 손실되어 복구할 수 없습니다. 그러나 이 절차에 따라 객체가 영구적으로 StorageGRID 시스템을 "정리"할 수 있는지, 아카이브 노드 요청을 취소하고, 손실된 객체에 대한 메타데이터를 제거할 수 있는지 확인해야 합니다.

개체를 영구적으로 사용할 수 있는지 여부를 확인합니다

TSM 관리 콘솔을 사용하여 요청을 수행하면 객체를 영구적으로 사용할 수 없는지 확인할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.
- 관리 노드의 IP 주소를 알아야 합니다.

이 작업에 대해

이 예제는 참고용으로만 제공됩니다. 이 절차는 사용할 수 없는 개체 또는 테이프 볼륨을 발생시킬 수 있는 모든 장애 조건을 식별하는 데 도움이 되지 않습니다. TSM 관리에 대한 자세한 내용은 TSM Server 설명서를 참조하십시오.

단계

1. 관리자 노드에 로그인:
   a. ssh admin@Admin_Node_IP' 명령어를 입력한다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
2. 아카이브 노드에서 검색할 수 없는 객체 식별:
   a. 감사 로그 파일이 포함된 디렉토리로 이동합니다: 'cd/var/local/audit/export'

      활성 감사 로그 파일의 이름은 audit.log입니다. 하루 한 번, 활성화된 'audit.log' 파일이 저장되고, 새로운 'audit.log' 파일이 시작된다. 저장된 파일의 이름은 저장 시기를 yyyy-mm-dd.txt 형식으로 나타냅니다. 하루 후에는 원래 날짜를 유지하는 형식(yyyy-mm-dd.txt.gz)으로 저장된 파일이 압축되고 이름이 변경됩니다.

   b. 관련 감사 로그 파일에서 보관된 개체를 검색할 수 없음을 나타내는 메시지를 검색합니다. 예를 들어, 'grep ARCE audit.log | less-n'을 입력합니다

      아카이브 노드에서 객체를 검색할 수 없는 경우 ARCE 감사 메시지(아카이브 객체 검색 종료)에 결과 필드에 Arun(아카이브 미들웨어를 사용할 수 없음) 또는 GERR(일반 오류)이 표시됩니다. 감사 로그의 다음 예제 줄은 CBID 498D8A1F681F05B3에 대한 결과 Arun로 ARCE 메시지가 종료되었음을 보여 줍니다.

      ```
      [AUDT:[CBID(UI64):0x498D8A1F681F05B3][VLID(UI64):□20091127][RSLT(FC32
      ):ARUN][AVER(UI32):7]
      [ATIM(UI64):1350613602969243][ATYP(FC32):ARCE][ANID(UI32):13959984][A
      MID(FC32):ARCI]
      [ATID(UI64):4560349751312520631]]
      ```

      자세한 내용은 감사 메시지 이해를 위한 지침을 참조하십시오.

   c. 요청 실패가 발생한 각 객체의 CBID를 기록합니다.

      TSM에서 아카이브 노드에 의해 저장된 객체를 식별하는 데 사용하는 다음과 같은 추가 정보를 기록할 수도 있습니다.

      - * 파일 공간 이름 *: 아카이브 노드 ID와 동일합니다. 아카이브 노드 ID를 찾으려면 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 * Archive Node * > * ARC * > * Target * > * Overview * 를 선택합니다.
      - * 상위 수준 이름 *: 아카이브 노드에서 객체에 할당한 볼륨 ID와 동일합니다. 볼륨 ID는 날짜 형식(예: 20091127)을 사용하여 아카이브 감사 메시지에 개체의 VLID로 기록됩니다.
      - * 낮은 수준 이름 *: StorageGRID 시스템에서 개체에 할당한 CBID와 같습니다.

d. 명령 셸에서 'exit'를 로그아웃합니다

3. TSM 서버에서 2단계에서 식별된 객체를 영구적으로 사용할 수 없는지 확인합니다.

   a. TSM 서버의 관리 콘솔인 dsmadmc에 로그인합니다

      ARC 서비스에 대해 구성된 관리 사용자 이름과 암호를 사용합니다. Grid Manager(그리드 관리자)에 사용자 이름과 암호를 입력합니다. (사용자 이름을 보려면 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 * Archive Node * > * ARC * > * Target * > * Configuration * 을 선택합니다.)

   b. 개체를 영구적으로 사용할 수 없는지 확인합니다.

      예를 들어 TSM 작업 로그에서 해당 객체에 대한 데이터 무결성 오류를 검색할 수 있습니다. 다음 예에서는 CBID가 498D8A1F681F05B3인 객체에 대한 지난 날의 활동 로그 검색을 보여줍니다.

```
> query actlog begindate=-1 search=276C14E94082CC69
12/21/2008 05:39:15 ANR0548W Retrieve or restore
failed for session 9139359 for node DEV-ARC-20 (Bycast ARC)
processing file space /19130020 4 for file /20081002/
498D8A1F681F05B3 stored as Archive - data
integrity error detected. (SESSION: 9139359)
>
```

      오류의 특성에 따라 TSM 작업 로그에 CBID가 기록되지 않을 수 있습니다. 요청 실패 시 로그에서 다른 TSM 오류를 검색해야 할 수 있습니다.

   c. 전체 테이프를 영구적으로 사용할 수 없는 경우 'query content TSM_Volume_Name' 볼륨에 저장된 모든 개체의 CBID를 식별합니다

      여기서 'TSM_Volume_Name'은 사용할 수 없는 테이프의 TSM 이름입니다. 다음은 이 명령의 출력 예입니다.

```
 > query content TSM-Volume-Name
Node Name     Type Filespace  FSID Client's Name for File Name
------------- ---- ---------- ---- ----------------------------
DEV-ARC-20    Arch /19130020  216  /20081201/ C1D172940E6C7E12
DEV-ARC-20    Arch /19130020  216  /20081201/ F1D7FBC2B4B0779E
```

      Client's Name for File Name'은 Archive Node 볼륨 ID(또는 TSM ""high level name") 다음에 객체의 CBID(또는 TSM ""low level name"")와 동일합니다. 즉, Client Name for File Name은 /Archive Node volume ID/CBID 형식을 사용합니다. 예제 출력의 첫 번째 줄에서는 '파일 이름에 대한 클라이언트 이름'이 '/20081201/C1D172940E6C7E12'입니다.

      파일 공간은 아카이브 노드의 노드 ID입니다.

   검색 요청을 취소하려면 볼륨에 저장된 각 개체의 CBID와 아카이브 노드의 노드 ID가 필요합니다.

4. 영구적으로 사용할 수 없는 각 개체에 대해 검색 요청을 취소하고 명령을 실행하여 StorageGRID 시스템에 개체 복사본이 손실되었음을 알립니다.

> ADE 콘솔을 주의하여 사용하십시오. 콘솔을 잘못 사용하면 시스템 작업을 중단하거나 데이터가 손상될 수 있습니다. 명령을 신중하게 입력하고 이 절차에 설명된 명령만 사용하십시오.

a. 아카이브 노드에 아직 로그인하지 않은 경우 다음과 같이 로그인합니다.
   i. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   ii. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   iii. 루트로 전환하려면 다음 명령을 입력합니다
   iv. "passwords.txt" 파일에 나열된 암호를 입력합니다.
b. ARC 서비스의 ADE 콘솔인 telnet localhost 1409 에 액세스합니다
c. 객체('/proc/brtr/cancel-c cbid')에 대한 요청을 취소합니다

   여기서 CBID는 TSM에서 검색할 수 없는 객체의 식별자입니다.

   테이프만 있는 경우 대량 검색 요청은 1개의 요청이 취소되었다는 메시지와 함께 취소됩니다. 시스템의 다른 곳에 개체 사본이 존재하면 개체 검색은 다른 모듈에 의해 처리되므로 메시지에 대한 응답은 "'0 request cancelled(0 request 취소됨)"입니다.

d. StorageGRID 시스템에 객체 사본이 손실되었으며 추가 복사본이 작성되어야 함을 알리는 명령을 발행합니다: "/proc/cMSI/Object_lost CBID node_ID"

   여기서 CBID는 TSM 서버에서 검색할 수 없는 객체의 식별자이며 node_ID는 검색이 실패한 아카이브 노드의 노드 ID입니다.

   손실된 각 개체 복사본에 대해 별도의 명령을 입력해야 합니다. CBID 범위를 입력하는 것은 지원되지 않습니다.

   대부분의 경우 StorageGRID 시스템은 시스템의 ILM 정책을 따르기 위해 즉시 오브젝트 데이터의 추가 복사본을 만들기 시작합니다.

   하지만 개체에 대한 ILM 규칙을 사용하여 복사본을 하나만 만들고 해당 복사본이 손실되면 개체를 복구할 수 없습니다. 이 경우 "Object_Lost" 명령을 실행하면 손실된 개체의 메타데이터가 StorageGRID 시스템에서 삭제됩니다.

   Object_lost 명령이 성공적으로 완료되면 다음과 같은 메시지가 반환됩니다.

```
CLOC_LOST_ANS returned result ‘SUCS’
```

+

> "/proc/cMSI/Object_lost" 명령은 아카이브 노드에 저장된 손실된 개체에 대해서만 유효합니다.

a. ADE 콘솔을 종료합니다. 'exit'
b. Archive Node(아카이브 노드)에서 로그아웃합니다: "exit(종료)"

5. StorageGRID 시스템에서 요청 실패 값을 재설정합니다.
   a. Archive Node * > * ARC * > * Retrieve * > * Configuration * 으로 이동하여 * Reset Request Failure Count * 를 선택합니다.

b. 변경 내용 적용 * 을 클릭합니다.

관련 정보

StorageGRID 관리

감사 로그를 검토합니다

VMware: 자동 재시작을 위해 가상 머신을 구성합니다

VMware vSphere Hypervisor를 다시 시작한 후 가상 머신을 다시 시작하지 않으면 가상 머신을 자동 다시 시작하도록 구성해야 할 수 있습니다.

그리드 노드를 복구하거나 다른 유지 보수 절차를 수행하는 동안 가상 시스템이 다시 시작되지 않는 경우 이 절차를 수행해야 합니다.

단계

1. VMware vSphere Client 트리에서 시작되지 않은 가상 머신을 선택합니다.
2. 가상 머신을 마우스 오른쪽 버튼으로 클릭하고 * Power On * 을 선택합니다.
3. 나중에 가상 머신을 자동으로 재시작하도록 VMware vSphere 하이퍼바이저를 구성합니다.

그리드 노드 절차

특정 그리드 노드에서 절차를 수행해야 할 수 있습니다. Grid Manager에서 이러한 절차 중 몇 가지를 수행할 수 있지만 대부분의 절차에서는 노드의 명령줄에서 Server Manager에 액세스해야 합니다.

서버 관리자는 모든 그리드 노드에서 실행되어 서비스의 시작 및 중지를 감독하고 서비스가 StorageGRID 시스템에 정상적으로 합류하고 탈퇴하도록 합니다. 또한 서버 관리자는 모든 그리드 노드의 서비스를 모니터링하고 장애를 보고하는 서비스를 자동으로 다시 시작합니다.

기술 지원 부서에서 지시하는 경우에만 서버 관리자에 액세스해야 합니다.

Server Manager를 완료한 후 현재 명령 셸 세션을 닫고 로그아웃해야 합니다. 'exit'로 진입합니다

서버 관리자 상태 및 버전을 봅니다

각 그리드 노드에 대해 해당 그리드 노드에서 실행 중인 서버 관리자의 현재 상태와 버전을 볼 수 있습니다. 또한 해당 그리드 노드에서 실행 중인 모든 서비스의 현재 상태를 얻을 수 있습니다.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

c. 루트로 전환하려면 다음 명령을 입력합니다

d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 그리드 노드에서 실행 중인 서버 관리자의 현재 상태(* service ServerManager status*)를 봅니다

   그리드 노드에서 실행 중인 Server Manager의 현재 상태가 보고됩니다(실행 여부). Server Manager의 상태가 Running인 경우, 마지막으로 시작된 이후 실행 중인 시간이 나열됩니다. 예를 들면 다음과 같습니다.

```
servermanager running for 1d, 13h, 0m, 30s
```

3. 그리드 노드에서 실행 중인 서버 관리자의 현재 버전(* service ServerManager version*)을 봅니다

   현재 버전이 나열됩니다. 예를 들면 다음과 같습니다.

```
11.1.0-20180425.1905.39c9493
```

4. 명령 쉘에서 로그아웃합니다: ' * exit * '

모든 서비스의 현재 상태를 봅니다

그리드 노드에서 실행 중인 모든 서비스의 현재 상태를 언제든지 볼 수 있습니다.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 그리드 노드에서 실행 중인 모든 서비스의 상태를 'toragegrid-status'로 봅니다

   예를 들어 기본 관리 노드의 출력은 AMS, CMN 및 NMS 서비스의 현재 상태를 실행 중으로 표시합니다. 이 출력은 서비스 상태가 변경되면 즉시 업데이트됩니다.

```
Host Name                      190-ADM1
IP Address
Operating System Kernel        4.9.0          Verified
Operating System Environment   Debian 9.4     Verified
StorageGRID Webscale Release   11.1.0         Verified
Networking                                    Verified
Storage Subsystem                             Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.1.0         Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.1.0         Running
cmn                            11.1.0         Running
nms                            11.1.0         Running
ssm                            11.1.0         Running
mi                             11.1.0         Running
dynip                          11.1.0         Running
nginx                          1.10.3         Running
tomcat                         8.5.14         Running
grafana                        4.2.0          Running
mgmt api                       11.1.0         Running
prometheus                     1.5.2+ds       Running
persistence                    11.1.0         Running
ade exporter                   11.1.0         Running
attrDownPurge                  11.1.0         Running
attrDownSamp1                  11.1.0         Running
attrDownSamp2                  11.1.0         Running
node exporter                  0.13.0+ds      Running
```

3. 명령줄로 돌아가 * Ctrl * + * C * 를 누릅니다.
4. 선택적으로 그리드 노드에서 실행 중인 모든 서비스에 대한 정적 보고서('/usr/local/ServerManager/reader.rb')를 봅니다

   이 보고서에는 계속 업데이트되는 보고서와 같은 정보가 포함되어 있지만 서비스 상태가 변경되면 업데이트되지 않습니다.

5. 명령 셸에서 'exit'를 로그아웃합니다

서버 관리자 및 모든 서비스를 시작합니다

서버 관리자를 시작해야 할 수도 있습니다. 그러면 그리드 노드에서 모든 서비스가 시작됩니다.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

이 작업에 대해

이미 실행 중인 그리드 노드에서 Server Manager를 시작하면 서버 관리자와 그리드 노드의 모든 서비스가 다시 시작됩니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. Server Manager 시작:'Service ServerManager 시작
3. 명령 셸에서 'exit'를 로그아웃합니다

서버 관리자 및 모든 서비스를 다시 시작합니다

서버 관리자와 그리드 노드에서 실행 중인 모든 서비스를 다시 시작해야 할 수 있습니다.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 서버 관리자 및 그리드 노드의 모든 서비스 'Service ServerManager restart'를 다시 시작합니다

   서버 관리자와 그리드 노드의 모든 서비스가 중지되었다가 다시 시작됩니다.

   > 'restart' 명령을 사용하는 것은 'top' 명령 다음에 'tart' 명령을 사용하는 것과 같습니다.

3. 명령 셸에서 'exit'를 로그아웃합니다

서버 관리자 및 모든 서비스를 중지합니다

Server Manager는 항상 실행되도록 되어 있지만 서버 관리자 및 그리드 노드에서 실행되는 모든 서비스를 중지해야 할 수 있습니다.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 서버 관리자와 그리드 노드에서 실행 중인 모든 서비스 'Service ServerManager stop'을 중지합니다

   서버 관리자와 그리드 노드에서 실행되는 모든 서비스가 정상적으로 종료됩니다. 서비스를 종료하는 데 최대 15분이 소요될 수 있습니다.

3. 명령 셸에서 'exit'를 로그아웃합니다

서비스의 현재 상태를 봅니다

그리드 노드에서 실행 중인 서비스의 현재 상태를 언제든지 볼 수 있습니다.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 그리드 노드에서 실행 중인 서비스의 현재 상태 보기: `* service_serviceName_status* 그리드 노드에서 실행 중인 요청된 서비스의 현재 상태가 보고됩니다(실행 중 또는 아님). 예를 들면 다음과 같습니다.

   ```
   cmn running for 1d, 14h, 21m, 2s
   ```

3. 명령 쉘에서 로그아웃합니다: ' * exit * '

서비스를 중지합니다

일부 유지 관리 절차에서는 그리드 노드의 다른 서비스를 계속 실행하는 동안 단일 서비스를 중지해야 합니다. 유지 관리 절차에 의해 지시된 경우에만 개별 서비스를 중지하십시오.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

이 작업에 대해

이러한 단계를 사용하여 서비스를 ""관리 중단""하면 서버 관리자가 서비스를 자동으로 다시 시작하지 않습니다. 단일 서비스를 수동으로 시작하거나 Server Manager를 다시 시작해야 합니다.

스토리지 노드에서 LDR 서비스를 중지해야 하는 경우 활성 연결이 있는 경우 서비스를 중지하는 데 시간이 걸릴 수 있습니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 개별 서비스 'service_serviceename_stop'을 중지합니다

   예를 들면 다음과 같습니다.

   ```
   service ldr stop
   ```

   서비스를 중지하는 데 최대 11분이 걸릴 수 있습니다.

3. 명령 셸에서 'exit'를 로그아웃합니다

관련 정보

서비스 강제 종료

제품을 유지보수 모드로 전환합니다

특정 유지보수 절차를 수행하기 전에 제품을 유지보수 모드로 전환해야 합니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다. 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

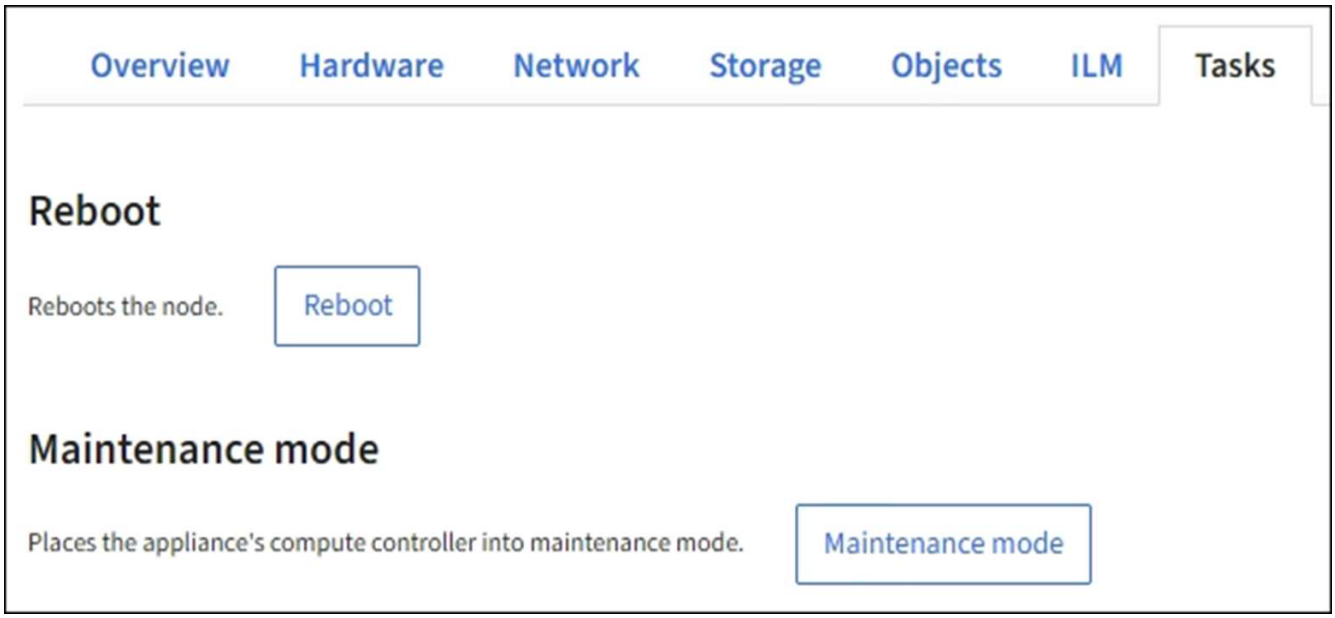
이 작업에 대해

StorageGRID 어플라이언스를 유지보수 모드로 전환하면 원격 액세스가 불가능한 경우가 드물게 있습니다.

유지보수 모드에서 StorageGRID 어플라이언스에 대한 admin 계정 암호 및 SSH 호스트 키는 어플라이언스가 서비스 중일 때와 동일하게 유지됩니다.

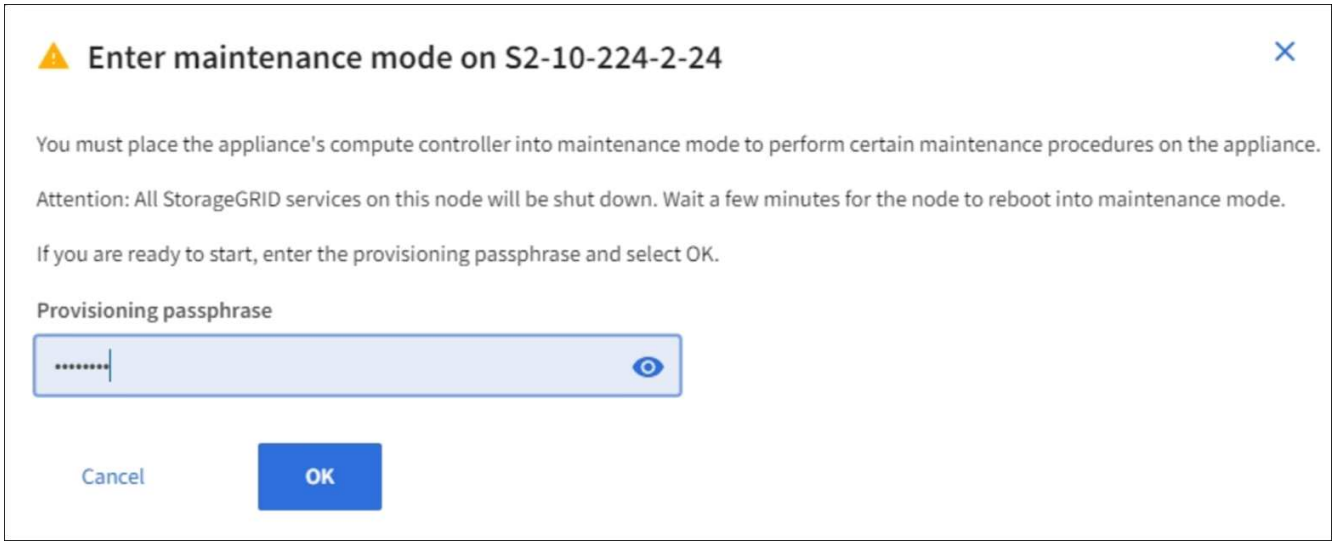
단계

1. Grid Manager에서 * nodes * 를 선택합니다.
2. 노드 페이지의 트리 뷰에서 어플라이언스 스토리지 노드를 선택합니다.
3. 작업 * 을 선택합니다.



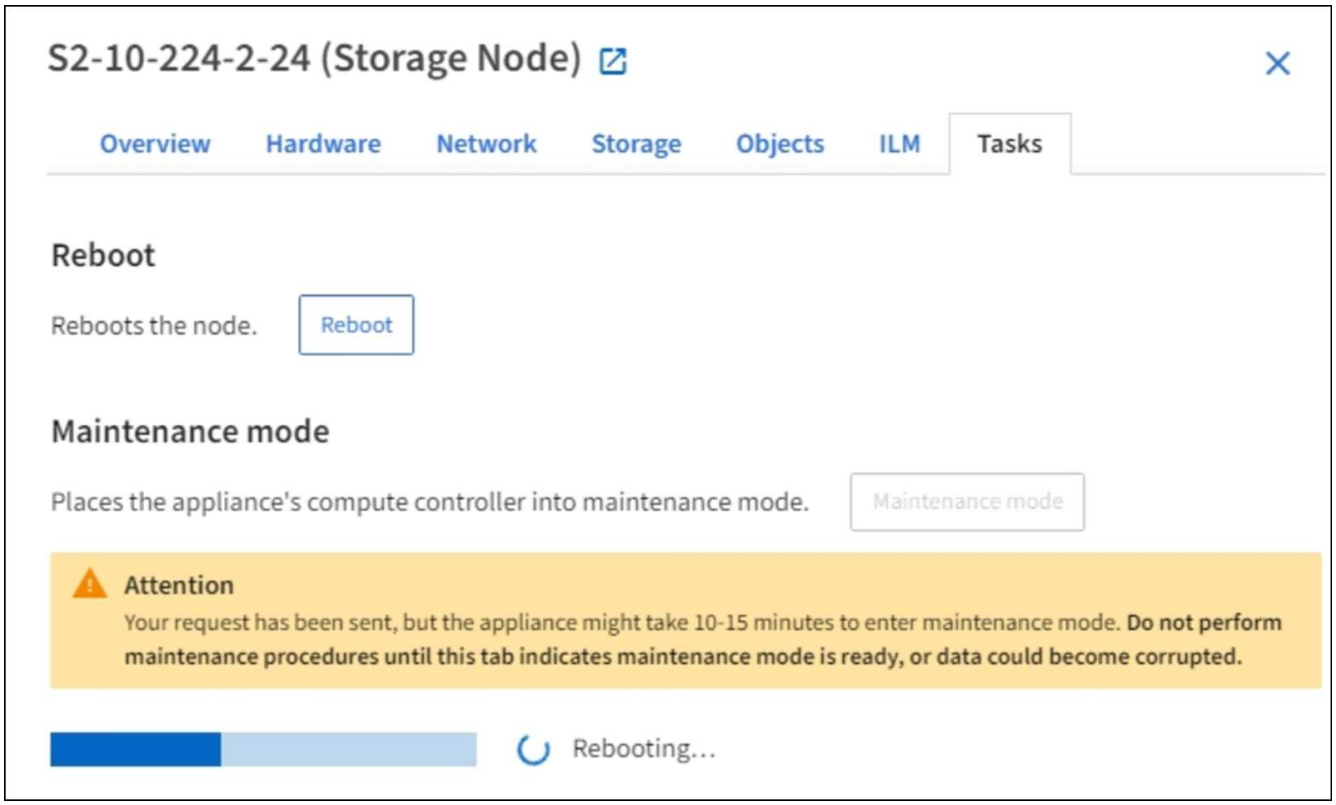
4. 유지보수 모드 * 를 선택합니다.

   확인 대화 상자가 나타납니다.

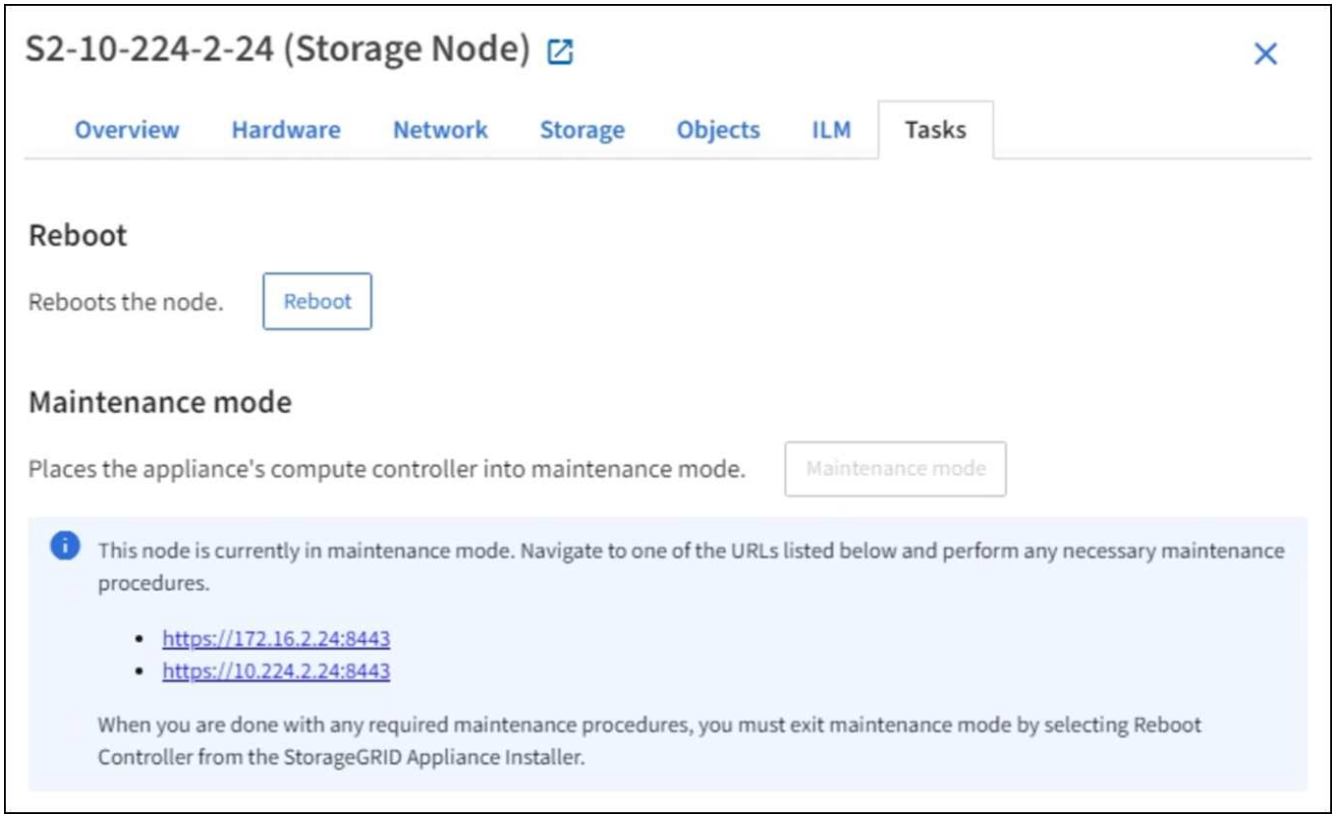


5. 프로비저닝 암호를 입력하고 * OK * 를 선택합니다.

   진행 표시줄과 "전송 요청", "StorageGRID 중지" 및 "재부팅"을 포함한 일련의 메시지는 어플라이언스가 유지보수 모드로 들어가기 위한 단계를 완료하고 있음을 나타냅니다.



어플라이언스가 유지보수 모드일 때 확인 메시지에 StorageGRID 어플라이언스 설치 프로그램에 액세스하는 데 사용할 수 있는 URL이 나열됩니다.



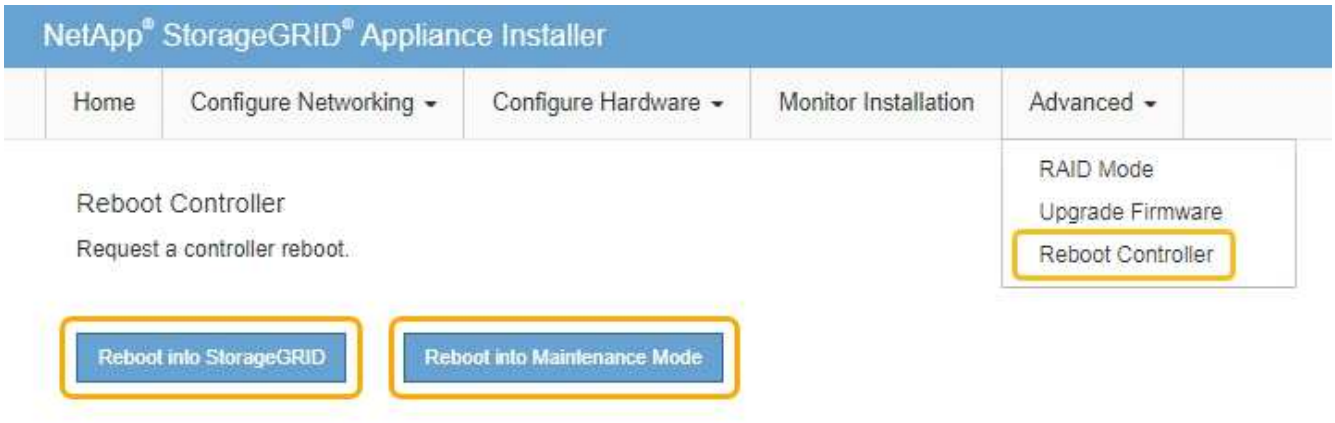
6. StorageGRID 어플라이언스 설치 프로그램에 액세스하려면 표시된 URL 중 하나를 찾습니다.

   가능한 경우 어플라이언스의 관리 네트워크 포트의 IP 주소가 포함된 URL을 사용하십시오.

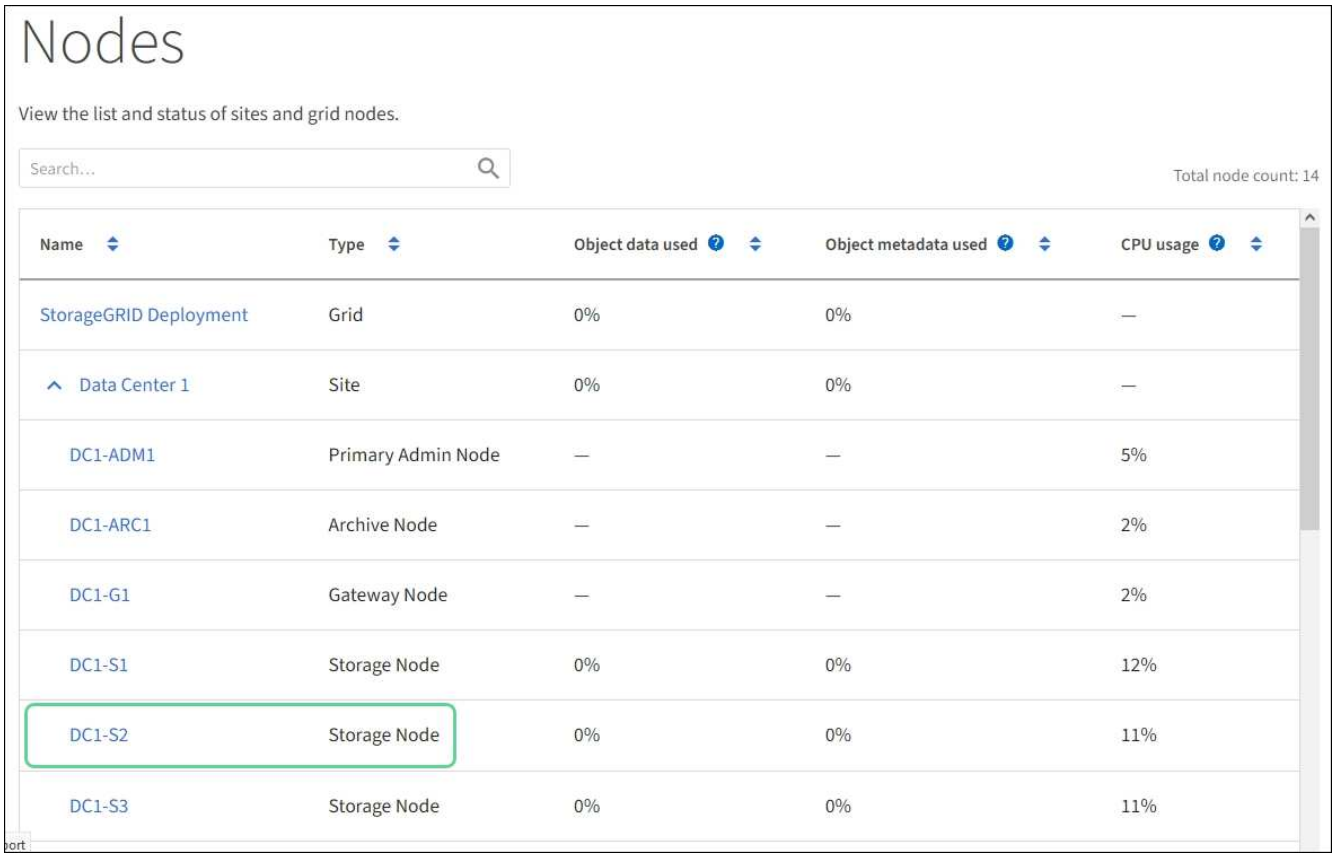
'https://169.254.0.1:8443` 액세스하려면 로컬 관리 포트에 직접 연결해야 합니다.

7. StorageGRID 어플라이언스 설치 프로그램에서 어플라이언스가 유지보수 모드인지 확인합니다.

8. 필요한 유지보수 작업을 수행합니다.
9. 유지보수 작업을 완료한 후 유지보수 모드를 종료하고 정상 노드 운영을 재개합니다. StorageGRID 어플라이언스 설치 프로그램에서 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * StorageGRID * 으로 재부팅 * 을 선택합니다.



어플라이언스가 재부팅되고 그리드에 다시 가입하는 데 최대 20분이 걸릴 수 있습니다. 재부팅이 완료되고 노드가 그리드에 다시 결합되었는지 확인하려면 Grid Manager로 돌아갑니다. 노드 * 페이지는 어플라이언스 노드에 대한 정상 상태(노드 이름 왼쪽에 아이콘이 없음)를 표시해야 합니다. 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.



서비스 강제 종료

서비스를 즉시 중지해야 하는 경우에는 강제 중지 명령을 사용할 수 있습니다.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 서비스를 수동으로 종료하도록 'service_serviceename_force-stop'

   예를 들면 다음과 같습니다.

   ```
   service ldr force-stop
   ```

   시스템은 30초 후에 서비스를 종료합니다.

3. 명령 셸에서 'exit'를 로그아웃합니다

서비스를 시작하거나 다시 시작합니다

중지된 서비스를 시작해야 하거나 서비스를 중지했다가 다시 시작해야 할 수 있습니다.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 서비스가 현재 실행 중인지 또는 중지되었는지 여부에 따라 실행할 명령을 결정합니다.

   - 서비스가 현재 중지된 경우 'start' 명령을 사용하여 서비스를 수동으로 시작합니다. 'service_serviceename_start'

     예를 들면 다음과 같습니다.

     ```
     service ldr start
     ```

   - 서비스가 현재 실행 중인 경우 restart 명령을 사용하여 서비스를 중지한 다음 다시 시작합니다. service_serviceename_restart

     예를 들면 다음과 같습니다.

   ```
   service ldr restart
   ```

   +

   > 'restart' 명령을 사용하는 것은 'top' 명령 다음에 'tart' 명령을 사용하는 것과 같습니다. 현재 서비스가 중지되어 있어도 다시 시작(restart)을 실행할 수 있습니다.

3. 명령 셸에서 'exit'를 로그아웃합니다

포트 재맵을 제거합니다

로드 밸런서 서비스에 대한 끝점을 구성하려는 경우 포트 재매핑의 매핑된-대상 포트로 이미 구성된 포트를 사용하려면 먼저 기존 포트 재매핑을 제거해야 합니다. 그렇지 않으면 끝점이

적용되지 않습니다. 노드의 모든 포트 매핑을 제거하려면 재매핑된 포트가 충돌하는 각 관리 노드와 게이트웨이 노드에서 스크립트를 실행해야 합니다.

> 이 작업에 대해
>
> 이 절차를 수행하면 모든 포트 재맵이 제거됩니다. 일부 재맵을 유지해야 하는 경우 기술 지원 부서에 문의하십시오.

로드 밸런서 엔드포인트를 구성하는 방법에 대한 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

> 포트 재매핑이 클라이언트 액세스를 제공하는 경우, 가능한 경우 로드 밸런서 끝점으로 구성된 다른 포트를 사용하도록 클라이언트를 다시 구성해야 서비스 손실을 방지할 수 있습니다. 그렇지 않으면 포트 매핑을 제거하면 클라이언트 액세스가 손실되므로 적절하게 예약해야 합니다.

> 베어 메탈 호스트에 컨테이너로 배포된 StorageGRID 시스템에서는 이 절차를 사용할 수 없습니다. 의 지침을 참조하십시오 베어 메탈 호스트에서 포트 리맵을 제거합니다.

단계

1. 노드에 로그인합니다.
   a. 'ssh-p 8022 admin@node_ip' 명령을 입력합니다

      포트 8022는 기본 OS의 SSH 포트이고, 포트 22는 StorageGRID를 실행하는 컨테이너 엔진의 SSH 포트입니다.

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. remove-port-remap.sh 스크립트를 실행합니다
3. 노드를 재부팅합니다.

   의 지침을 따릅니다 그리드 노드 재부팅.

4. 재매핑된 포트가 충돌하는 각 관리 노드와 게이트웨이 노드에서 이 단계를 반복합니다.

관련 정보

StorageGRID 관리

베어 메탈 호스트에서 포트 재맵을 제거합니다

로드 밸런서 서비스에 대한 끝점을 구성하려는 경우 포트 재매핑의 매핑된-대상 포트로 이미 구성된 포트를 사용하려면 먼저 기존 포트 재매핑을 제거해야 합니다. 그렇지 않으면 끝점이 적용되지 않습니다. 베어 메탈 호스트에서 StorageGRID를 실행 중인 경우 포트 재맵을 제거하는 일반 절차 대신 이 절차를 따르십시오. 충돌하는 재매핑된 포트가 있는 각 관리 노드와 게이트웨이 노드에 대한 노드 구성 파일을 편집하여 노드의 모든 포트를 제거하고 노드를 다시

시작해야 합니다.

> 이 작업에 대해
>
> 이 절차를 수행하면 모든 포트 재맵이 제거됩니다. 일부 재맵을 유지해야 하는 경우 기술 지원 부서에 문의하십시오.

로드 밸런서 엔드포인트를 구성하는 방법에 대한 자세한 내용은 StorageGRID 관리 지침을 참조하십시오.

> 노드를 다시 시작할 때 이 절차를 수행하면 서비스가 일시적으로 손실될 수 있습니다.

단계

1. 노드를 지원하는 호스트에 로그인합니다. 루트 또는 sudo 권한이 있는 계정으로 로그인합니다.
2. 'SUDO StorageGRID node stop_node -name_' 노드를 일시적으로 비활성화하려면 다음 명령을 실행합니다
3. vim 또는 pico와 같은 텍스트 편집기를 사용하여 노드의 노드 구성 파일을 편집합니다.

   노드 구성 파일은 '/etc/StorageGrid/nodes/*node-name*.conf'에서 찾을 수 있습니다.

4. 포트 재맵이 포함된 노드 구성 파일의 섹션을 찾습니다.

   다음 예제의 마지막 두 줄을 참조하십시오.

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = Interface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = Interface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = Interface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443
```

5. port_remap 및 port_remap_inbound 항목을 편집하여 포트 재맵을 제거합니다.

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. 다음 명령을 실행하여 노드의 노드 구성 파일에 대한 변경 사항을 확인합니다. "sudo StorageGRID node validate_node -name_'

   다음 단계로 진행하기 전에 오류 또는 경고를 모두 해결하십시오.

7. 'SUDO StorageGRID node start_node -name_' 포트를 재매핑하지 않고 노드를 재시작하려면 다음 명령을 실행합니다
8. "passwords.txt" 파일에 나열된 암호를 사용하여 노드에 admin으로 로그인합니다.
9. 서비스가 올바르게 시작되는지 확인합니다.
   a. 서버에 있는 모든 서비스의 상태 목록을 봅니다. 'SUDO StorageGrid-status'

      상태가 자동으로 업데이트됩니다.

b. 모든 서비스가 실행 중 또는 확인됨의 상태가 될 때까지 기다립니다.

c. 상태 화면을 종료합니다. Ctrl+C

10. 재매핑된 포트가 충돌하는 각 관리 노드와 게이트웨이 노드에서 이 단계를 반복합니다.

그리드 노드를 재부팅합니다

그리드 관리자 또는 노드의 명령 셸에서 그리드 노드를 재부팅할 수 있습니다.

이 작업에 대해

그리드 노드를 재부팅하면 노드가 종료되고 다시 시작됩니다. 모든 서비스가 자동으로 다시 시작됩니다.

스토리지 노드를 재부팅하려는 경우 다음 사항에 유의하십시오.

- ILM 규칙이 이중 커밋의 수집 동작을 지정하거나 규칙이 Balanced 를 지정하며 필요한 모든 복사본을 즉시 생성할 수 없는 경우, StorageGRID는 새로 수집된 개체를 즉시 동일한 사이트의 두 스토리지 노드에 커밋하고 나중에 ILM을 평가합니다. 특정 사이트에서 두 개 이상의 스토리지 노드를 재부팅하려는 경우 재부팅 기간 동안 이러한 개체에 액세스하지 못할 수 있습니다.
- 스토리지 노드가 재부팅되는 동안 모든 개체에 액세스할 수 있도록 노드를 재부팅하기 전에 약 1시간 동안 사이트에서 객체 인제스트를 중지하십시오.

관련 정보

StorageGRID 관리

Grid Manager에서 그리드 노드를 재부팅합니다

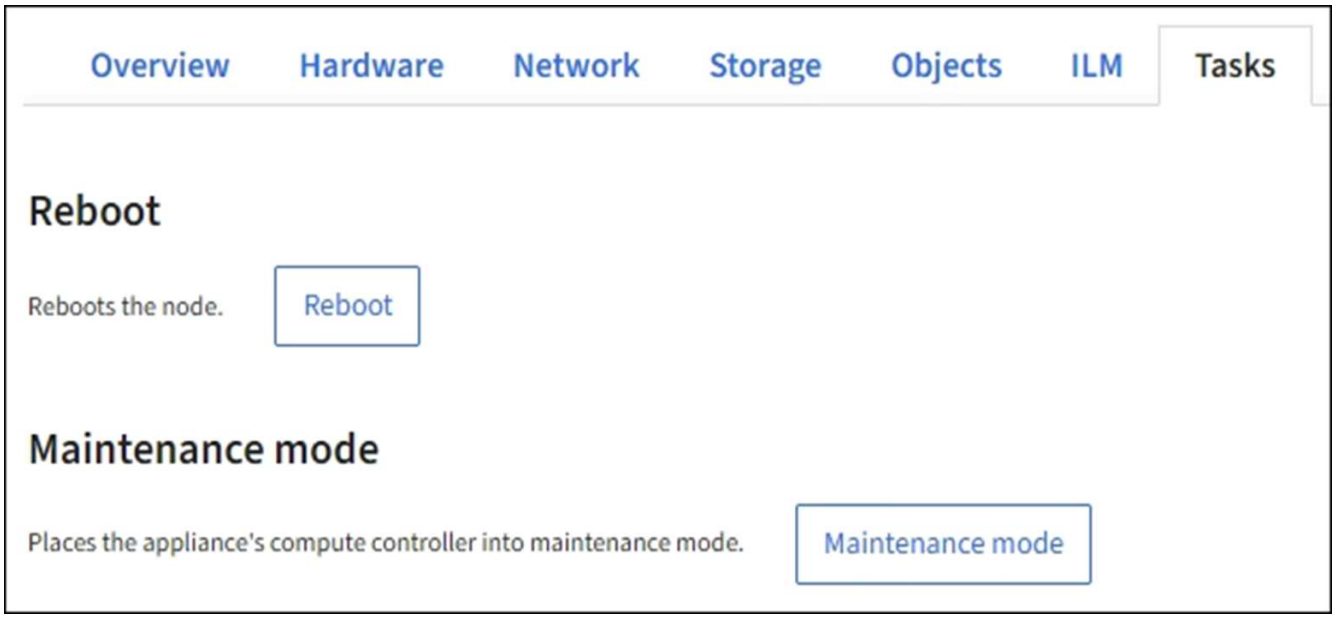
Grid Manager에서 그리드 노드를 재부팅하면 타겟 노드에 reboot 명령이 실행됩니다.

필요한 것

- 를 사용하여 그리드 관리자에 로그인했습니다 지원되는 웹 브라우저.
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 프로비저닝 암호가 있습니다.

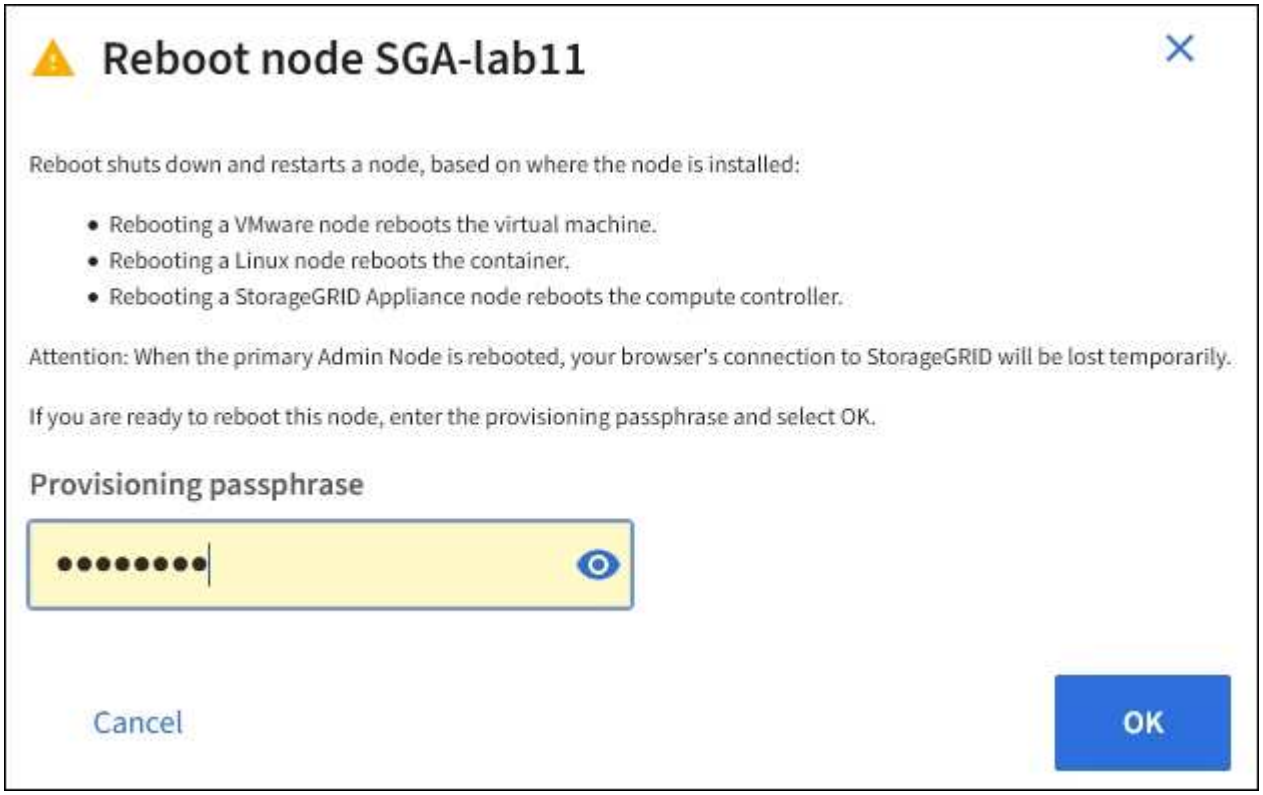
단계

1. 노드 * 를 선택합니다.
2. 재부팅할 그리드 노드를 선택합니다.
3. 작업 * 탭을 선택합니다.



4. 재부팅 * 을 선택합니다.

   확인 대화 상자가 나타납니다.



> 기본 관리 노드를 재부팅할 경우 서비스가 중지되면 브라우저에서 Grid Manager에 대한 연결이 일시적으로 끊겼다는 확인 대화 상자가 나타납니다.

5. 프로비저닝 암호를 입력하고 * OK * 를 클릭합니다.
6. 노드가 재부팅될 때까지 기다립니다.

   서비스가 종료되는 데 약간의 시간이 걸릴 수 있습니다.

노드가 재부팅되면 * Nodes * 페이지 왼쪽에 회색 아이콘(관리자 아래)이 나타납니다. 모든 서비스가 다시 시작되고 노드가 그리드에 성공적으로 연결되면 * Nodes * 페이지에 정상 상태(노드 이름 왼쪽에 아이콘이 없음)가 표시되어야 하며, 이는 활성화된 알림이 없고 노드가 그리드에 연결되었음을 나타냅니다.

명령 셸에서 그리드 노드를 재부팅합니다

재부팅 작업을 보다 자세히 모니터링해야 하거나 Grid Manager에 액세스할 수 없는 경우 GRID 노드에 로그인하여 명령 셸에서 Server Manager 재부팅 명령을 실행할 수 있습니다.

"passwords.txt" 파일이 있어야 합니다.

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 선택적으로, 서비스를 중지합니다: 'Service ServerManager stop'

   서비스를 중지하는 것은 선택 사항이지만 권장되는 단계입니다. 서비스를 종료하는 데 최대 15분이 걸릴 수 있으며, 다음 단계에서 노드를 재부팅하기 전에 시스템에 원격으로 로그인하여 종료 프로세스를 모니터링할 수 있습니다.

3. 그리드 노드를 다시 부팅한다

4. 명령 셸에서 'exit'를 로그아웃합니다

그리드 노드를 종료합니다

노드의 명령 셸에서 그리드 노드를 종료할 수 있습니다.

필요한 것

- "passwords.txt" 파일이 있어야 합니다.

이 작업에 대해

이 절차를 수행하기 전에 다음 사항을 검토하십시오.

- 일반적으로 중단을 방지하기 위해 노드를 한 번에 두 개 이상 종료해서는 안 됩니다.
- 설명서나 기술 지원 부서에서 명시적으로 지시하지 않는 한 유지보수 절차 중에 노드를 종료하지 마십시오.
- 종료 프로세스는 노드가 설치되는 위치를 기반으로 다음과 같이 진행됩니다.
  - VMware 노드를 종료하면 가상 머신이 종료됩니다.
  - Linux 노드를 종료하면 컨테이너가 종료됩니다.
  - StorageGRID 어플라이언스 노드를 종료하면 컴퓨팅 컨트롤러가 종료됩니다.
- 한 사이트에서 둘 이상의 스토리지 노드를 종료할 계획이면 노드를 종료하기 전에 해당 사이트에서 약 1시간 동안 객체 인제스트를 중지합니다.

ILM 규칙이 * 이중 커밋 * 수집 옵션을 사용하는 경우(또는 규칙이 * 균형 * 옵션을 사용하고 모든 필수 복사본을 즉시 생성할 수 없는 경우), StorageGRID는 새로 수집된 개체를 즉시 동일한 사이트의 두 스토리지 노드에 커밋하고 나중에 ILM을 평가합니다. 한 사이트에 둘 이상의 스토리지 노드가 종료된 경우 종료 기간 동안 새로 수집된 개체에 액세스하지 못할 수 있습니다. 사이트에서 사용 가능한 스토리지 노드가 너무 적은 경우에도 쓰기 작업이 실패할 수 있습니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 모든 서비스를 중지합니다: 'Service ServerManager stop'

   서비스를 종료하는 데 최대 15분이 걸릴 수 있으며, 종료 프로세스를 모니터링하기 위해 시스템에 원격으로 로그인하기를 원할 수 있습니다.

3. 노드가 VMware 가상 머신에서 실행 중이거나 어플라이언스 노드인 경우 shutdown -h now 명령을 실행합니다

   'Service ServerManager stop' 명령어의 결과에 상관없이 이 단계를 수행한다.

   > 어플라이언스 노드에서 '지금 종료' 명령을 실행한 후 어플라이언스를 껐다가 다시 시작해야 합니다.

   제품의 경우, 이 명령은 컨트롤러를 종료하지만 제품의 전원은 계속 켜져 있습니다. 다음 단계를 완료해야 합니다.

4. 어플라이언스 노드의 전원을 끄는 경우:
   - SG100 또는 SG1000 서비스 어플라이언스의 경우
     i. 제품의 전원을 끕니다.
     ii. 파란색 전원 LED가 꺼질 때까지 기다립니다.
   - SG6000 어플라이언스의 경우
     i. 스토리지 컨트롤러 후면의 녹색 캐시 활성 LED가 꺼질 때까지 기다립니다.

        캐싱된 데이터를 드라이브에 기록해야 하는 경우 이 LED가 켜집니다. 전원을 끄기 전에 이 LED가 꺼질 때까지 기다려야 합니다.

     ii. 제품의 전원을 끄고 파란색 전원 LED가 꺼질 때까지 기다리십시오.
   - SG5700 어플라이언스입니다
     i. 스토리지 컨트롤러 후면의 녹색 캐시 활성 LED가 꺼질 때까지 기다립니다.

        캐싱된 데이터를 드라이브에 기록해야 하는 경우 이 LED가 켜집니다. 전원을 끄기 전에 이 LED가 꺼질 때까지 기다려야 합니다.

ii. 제품의 전원을 끄고 모든 LED 및 7세그먼트 디스플레이 작동이 멈출 때까지 기다리십시오.

관련 정보

StorageGRID 관리

호스트 전원을 끕니다

호스트의 전원을 끄기 전에 해당 호스트의 모든 그리드 노드에서 서비스를 중지해야 합니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다

   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   c. 루트로 전환하려면 다음 명령을 입력합니다

   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 'Service ServerManager stop' 노드에서 실행 중인 모든 서비스를 중지합니다

   서비스를 종료하는 데 최대 15분이 걸릴 수 있으며, 종료 프로세스를 모니터링하기 위해 시스템에 원격으로 로그인하기를 원할 수 있습니다.

3. 호스트의 각 노드에 대해 1단계와 2단계를 반복합니다.

4. Linux 호스트가 있는 경우:

   a. 호스트 운영 체제에 로그인합니다.

   b. StorageGRID node stop 노드를 정지한다

   c. 호스트 운영 체제를 종료합니다.

5. 노드가 VMware 가상 머신에서 실행 중이거나 어플라이언스 노드인 경우 shutdown -h now 명령을 실행합니다

   'Service ServerManager stop' 명령어의 결과에 상관없이 이 단계를 수행한다.

   > 어플라이언스 노드에서 '지금 종료' 명령을 실행한 후 어플라이언스를 껐다가 다시 시작해야 합니다.

   제품의 경우, 이 명령은 컨트롤러를 종료하지만 제품의 전원은 계속 켜져 있습니다. 다음 단계를 완료해야 합니다.

6. 어플라이언스 노드의 전원을 끄는 경우:

   - SG100 또는 SG1000 서비스 어플라이언스의 경우

     i. 제품의 전원을 끕니다.

     ii. 파란색 전원 LED가 꺼질 때까지 기다립니다.

   - SG6000 어플라이언스의 경우

     i. 스토리지 컨트롤러 후면의 녹색 캐시 활성 LED가 꺼질 때까지 기다립니다.

     캐싱된 데이터를 드라이브에 기록해야 하는 경우 이 LED가 켜집니다. 전원을 끄기 전에 이 LED가 꺼질

때까지 기다려야 합니다.

ii. 제품의 전원을 끄고 파란색 전원 LED가 꺼질 때까지 기다리십시오.

- SG5700 어플라이언스입니다

i. 스토리지 컨트롤러 후면의 녹색 캐시 활성 LED가 꺼질 때까지 기다립니다.

캐싱된 데이터를 드라이브에 기록해야 하는 경우 이 LED가 켜집니다. 전원을 끄기 전에 이 LED가 꺼질 때까지 기다려야 합니다.

ii. 제품의 전원을 끄고 모든 LED 및 7세그먼트 디스플레이 작동이 멈출 때까지 기다리십시오.

7. 명령 셸에서 'exit'를 로그아웃합니다

관련 정보

SG100 및 SG1000 서비스 어플라이언스

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

그리드의 모든 노드를 끕니다

예를 들어 데이터 센터를 이동하는 경우 전체 StorageGRID 시스템을 종료해야 할 수 있습니다. 다음 단계에서는 제어 방식의 셧다운 및 시작을 수행하는 데 권장되는 순서에 대해 개략적으로 설명합니다.

사이트 또는 그리드의 모든 노드의 전원을 끌 경우 스토리지 노드가 오프라인 상태인 동안에는 수집된 개체에 액세스할 수 없습니다.

서비스를 중지하고 그리드 노드를 종료합니다

StorageGRID 시스템의 전원을 끄기 전에 각 그리드 노드에서 실행 중인 모든 서비스를 중지한 다음 모든 VMware 가상 머신, 컨테이너 엔진 및 StorageGRID 어플라이언스를 종료해야 합니다.

이 작업에 대해

먼저 관리 노드 및 API 게이트웨이 노드에서 서비스를 중지한 다음 스토리지 노드에서 서비스를 중지합니다.

이 접근 방식을 사용하면 기본 관리 노드를 사용하여 다른 그리드 노드의 상태를 가능한 한 오랫동안 모니터링할 수 있습니다.

> 단일 호스트에 둘 이상의 그리드 노드가 있는 경우 해당 호스트의 모든 노드를 중지할 때까지 호스트를 종료하지 마십시오. 호스트에 운영 관리 노드가 포함된 경우 해당 호스트를 마지막으로 종료합니다.

> 필요한 경우 를 사용할 수 있습니다 Linux 호스트 간에 노드를 마이그레이션합니다 그리드의 기능 또는 가용성에 영향을 주지 않고 호스트 유지 관리를 수행합니다.

단계

1. 모든 클라이언트 응용 프로그램이 그리드에 액세스하는 것을 중지합니다.

2. [[log_in_to_gn] 각 게이트웨이 노드에 로그인:
   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

      루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

3. 노드에서 실행 중인 모든 서비스를 중지합니다

   서비스를 종료하는 데 최대 15분이 걸릴 수 있으며, 종료 프로세스를 모니터링하기 위해 시스템에 원격으로 로그인하기를 원할 수 있습니다.

4. 앞의 두 단계를 반복하여 모든 스토리지 노드, 아카이브 노드 및 비 기본 관리 노드에서 서비스를 중지합니다.

   이러한 노드의 서비스는 순서에 관계없이 중지할 수 있습니다.

   > 어플라이언스 스토리지 노드에서 서비스를 중지하기 위해 'Service ServerManager stop' 명령을 실행하는 경우 어플라이언스를 껐다가 다시 시작해야 노드를 재시작할 수 있습니다.

5. 기본 관리 노드에 대해 의 단계를 반복합니다 노드에 로그인합니다 및 노드에서 모든 서비스를 중지하는 중입니다.
6. Linux 호스트에서 실행 중인 노드의 경우:
   a. 호스트 운영 체제에 로그인합니다.
   b. StorageGRID node stop 노드를 정지한다
   c. 호스트 운영 체제를 종료합니다.
7. VMware 가상 시스템 및 어플라이언스 스토리지 노드에서 실행 중인 노드의 경우 shutdown -h now 명령을 실행합니다

   'Service ServerManager stop' 명령어의 결과에 상관없이 이 단계를 수행한다.

   어플라이언스의 경우 이 명령은 컴퓨팅 컨트롤러를 종료하지만 어플라이언스 전원은 여전히 켜져 있습니다. 다음 단계를 완료해야 합니다.

8. 어플라이언스 노드가 있는 경우:
   - SG100 또는 SG1000 서비스 어플라이언스의 경우
     i. 제품의 전원을 끕니다.
     ii. 파란색 전원 LED가 꺼질 때까지 기다립니다.
   - SG6000 어플라이언스의 경우
     i. 스토리지 컨트롤러 후면의 녹색 캐시 활성 LED가 꺼질 때까지 기다립니다.

        캐싱된 데이터를 드라이브에 기록해야 하는 경우 이 LED가 켜집니다. 전원을 끄기 전에 이 LED가 꺼질 때까지 기다려야 합니다.

     ii. 제품의 전원을 끄고 파란색 전원 LED가 꺼질 때까지 기다리십시오.

- SG5700 어플라이언스입니다
  i. 스토리지 컨트롤러 후면의 녹색 캐시 활성 LED가 꺼질 때까지 기다립니다.

     캐싱된 데이터를 드라이브에 기록해야 하는 경우 이 LED가 켜집니다. 전원을 끄기 전에 이 LED가 꺼질 때까지 기다려야 합니다.

  ii. 제품의 전원을 끄고 모든 LED 및 7세그먼트 디스플레이 작동이 멈출 때까지 기다리십시오.

9. 필요한 경우 명령 셸에서 'exit'를 로그아웃합니다

   StorageGRID 그리드가 이제 종료되었습니다.

관련 정보

SG100 및 SG1000 서비스 어플라이언스

SG6000 스토리지 어플라이언스

SG5700 스토리지 어플라이언스

그리드 노드를 시작합니다

이 순서에 따라 시스템을 완전히 종료한 후 그리드 노드를 시작합니다.

> 무엇을 '필요로 할거야
>
> 전체 그리드가 15일 이상 종료된 경우 그리드 노드를 시작하기 전에 기술 지원 팀에 문의해야 합니다. Cassandra 데이터를 재구성하는 복구 절차를 시도하지 마십시오. 이렇게 하면 데이터가 손실될 수 있습니다.

이 작업에 대해

가능한 경우 다음과 같은 순서로 그리드 노드의 전원을 켭니다.

- 먼저 관리 노드에 전원을 적용합니다.
- 마지막으로 게이트웨이 노드에 전원을 공급합니다.

> 호스트에 다중 그리드 노드가 포함된 경우 호스트 전원을 켜면 노드가 자동으로 다시 온라인 상태가 됩니다.

단계

1. 운영 관리 노드 및 비 운영 관리 노드에 대한 호스트의 전원을 켭니다.

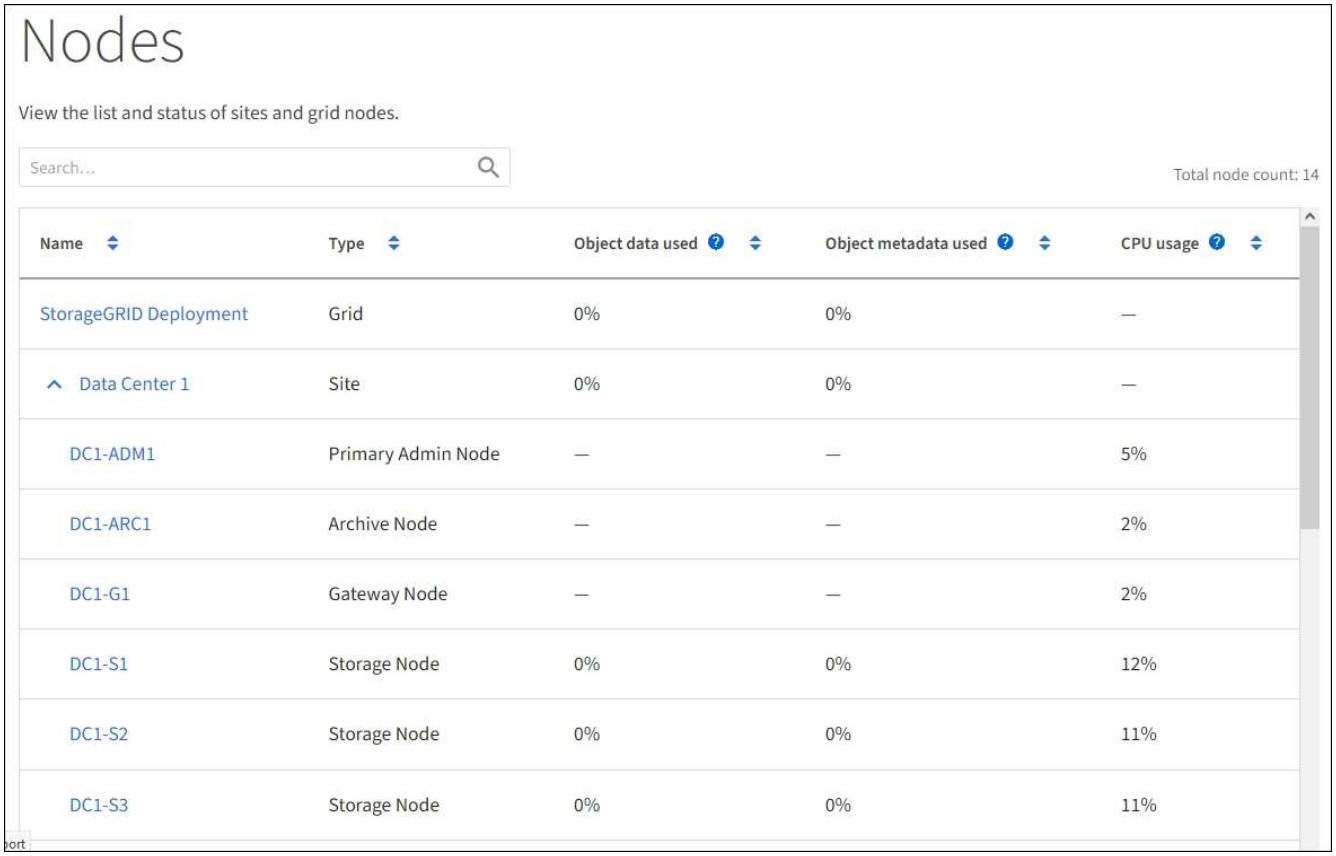
   > 스토리지 노드가 다시 시작될 때까지 관리 노드에 로그인할 수 없습니다.

2. 모든 아카이브 노드 및 스토리지 노드의 호스트 전원을 켭니다.

   이러한 노드의 전원은 순서에 상관없이 켤 수 있습니다.

3. 모든 게이트웨이 노드의 호스트 전원을 켭니다.
4. Grid Manager에 로그인합니다.

5. nodes * 를 선택하고 그리드 노드의 상태를 모니터링합니다. 노드 이름 옆에 알림 아이콘이 없는지 확인합니다.



DoNotStart 파일을 사용합니다

기술 지원 부서의 지시에 따라 다양한 유지 관리 또는 구성 절차를 수행하는 경우 DoNotStart 파일을 사용하여 Server Manager를 시작하거나 다시 시작할 때 서비스가 시작되지 않도록 해야 할 수 있습니다.

> 기술 지원 부서에서 지시한 경우에만 DoNotStart 파일을 추가하거나 제거해야 합니다.

서비스가 시작되지 않도록 하려면 시작할 수 없도록 하려는 서비스 디렉터리에 DoNotStart 파일을 배치합니다. 서버 관리자는 시작할 때 DoNotStart 파일을 찾습니다. 파일이 있으면 서비스(및 서비스에 종속된 모든 서비스)를 시작할 수 없습니다. DoNotStart 파일이 제거되면 이전에 중지된 서비스는 다음 서버 관리자를 시작하거나 다시 시작할 때 시작됩니다. DoNotStart 파일이 제거되면 서비스가 자동으로 시작되지 않습니다.

모든 서비스가 다시 시작되지 않도록 하는 가장 효율적인 방법은 NTP 서비스가 시작되지 않도록 하는 것입니다. 모든 서비스는 NTP 서비스에 종속되며 NTP 서비스가 실행되고 있지 않으면 실행할 수 없습니다.

서비스에 대한 **DoNotStart** 파일을 추가합니다

그리드 노드의 해당 서비스 디렉터리에 DoNotStart 파일을 추가하여 개별 서비스가 시작되지 않도록 할 수 있습니다.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. DoNotStart 파일 추가: 'touch/etc/sv/*service*/DoNotStart

   여기서 서비스는 시작할 수 없는 서비스의 이름입니다. 예를 들면, 다음과 같습니다.

   ```
   touch /etc/sv/ldr/DoNotStart
   ```

   DoNotStart 파일이 만들어집니다. 파일 콘텐츠가 필요하지 않습니다.

   서버 관리자 또는 그리드 노드가 다시 시작되면 서버 관리자가 다시 시작되지만 서비스는 다시 시작되지 않습니다.

3. 명령 셸에서 'exit'를 로그아웃합니다

서비스에 대한 **DoNotStart** 파일을 제거합니다

서비스 시작을 방해하는 DoNotStart 파일을 제거할 경우 해당 서비스를 시작해야 합니다.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 서비스 디렉터리 'rm/etc/sv/*service*/DoNotStart'에서 DoNotStart 파일을 제거합니다

   여기서 서비스는 서비스의 이름입니다. 예를 들면, 다음과 같습니다.

   ```
   rm /etc/sv/ldr/DoNotStart
   ```

3. 'service_serviceename_start' 서비스를 시작합니다

4. 명령 셸에서 'exit'를 로그아웃합니다

서버 관리자 문제를 해결합니다

Server Manager 로그 파일에 액세스합니다

Server Manager를 사용할 때 문제가 발생하면 로그 파일을 확인하십시오.

Server Manager와 관련된 오류 메시지는 서버 관리자 로그 파일("/var/local/log/ServerManager.log")에서 캡처됩니다

이 파일에서 장애와 관련된 오류 메시지를 확인하십시오. 필요한 경우 기술 지원 부서에 문제를 에스컬레이션합니다. 로그 파일을 기술 지원 부서에 전달하라는 메시지가 표시될 수 있습니다.

오류 상태의 서비스

서비스가 오류 상태로 전환되면 서비스를 다시 시작하십시오.

필요한 것

"passwords.txt" 파일이 있어야 합니다.

이 작업에 대해

Server Manager는 서비스를 모니터링하고 예기치 않게 중지된 서비스를 다시 시작합니다. 서비스에 오류가 발생하면 Server Manager가 서비스를 다시 시작합니다. 5분 내에 서비스 시작 시도가 세 번 실패하면 서비스가 오류 상태로 전환됩니다. 서버 관리자가 다시 시작하지 않습니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 'ssh admin@*grid_node_ip*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
   c. 루트로 전환하려면 다음 명령을 입력합니다
   d. "passwords.txt" 파일에 나열된 암호를 입력합니다.

   루트로 로그인하면 프롬프트가 '$'에서 '#'로 바뀝니다.

2. 서비스의 오류 상태 'service_serviceename_status'를 확인합니다

   예를 들면 다음과 같습니다.

   ```
   service ldr status
   ```

   서비스가 오류 상태인 경우 '_serviceName_in error state'라는 메시지가 반환됩니다. 예를 들면 다음과 같습니다.

   ```
   ldr in error state
   ```

   > 서비스 상태가 '비활성화'인 경우 의 지침을 참조하십시오 서비스에 대한 DoNotStart 파일 제거.

3. 'service_serviceename_restart' 서비스를 다시 시작하여 오류 상태를 제거하려고 시도합니다

   서비스가 다시 시작되지 않으면 기술 지원 부서에 문의하십시오.

4. 명령 셸에서 'exit'를 로그아웃합니다

어플라이언스 노드 클론 복제

StorageGRID에서 어플라이언스 노드를 클론 복제하여 새로운 설계 또는 향상된 기능의 어플라이언스를 사용할 수 있습니다. 클론 복제는 기존 노드의 모든 정보를 새 어플라이언스로 전송하고, 수행하기 쉬운 하드웨어 업그레이드 프로세스를 제공하며, 어플라이언스 교체를 위한 서비스 해제 및 확장 대안을 제공합니다.

어플라이언스 노드 클론 복제의 작동 방식

어플라이언스 노드 클론 복제를 사용하면 그리드에서 기존 어플라이언스 노드(소스)를 동일한 논리적 StorageGRID 사이트의 일부인 호환 어플라이언스(타겟)로 쉽게 교체할 수 있습니다. 이 프로세스는 모든 데이터를 새 어플라이언스에 전송하여 이전 어플라이언스 노드를 교체하고 이전 어플라이언스를 설치 전 상태로 둡니다.

어플라이언스 노드를 클론 복제해야 하는 이유

다음과 같은 경우에 어플라이언스 노드를 클론 복제할 수 있습니다.

- 수명이 다 된 제품은 교체하십시오.
- 기존 노드를 업그레이드하여 개선된 어플라이언스 기술을 활용하십시오.
- StorageGRID 시스템에서 스토리지 노드 수를 변경하지 않고 그리드 스토리지 용량을 늘립니다.
- RAID 모드를 DDP-8에서 DDP-16 또는 RAID-6으로 변경하는 것과 같은 스토리지 효율성을 향상시킵니다.
- 외부 키 관리 서버(KMS)를 사용할 수 있도록 노드 암호화를 효율적으로 구현합니다.

어떤 **StorageGRID** 네트워크가 사용됩니까**?**

클론 복제는 세 StorageGRID 네트워크 중 하나를 통해 소스 노드에서 타겟 어플라이언스로 직접 데이터를 전송합니다. 그리드 네트워크는 일반적으로 사용되지만 소스 어플라이언스가 이러한 네트워크에 연결되어 있는 경우 관리 네트워크 또는 클라이언트 네트워크를 사용할 수도 있습니다. StorageGRID 네트워크 성능 또는 데이터 가용성을 저하시키지 않으면서 최상의 데이터 전송 성능을 제공하는 트래픽 클론 생성에 사용할 네트워크를 선택하십시오.

교체 어플라이언스를 설치할 때 StorageGRID 연결 및 데이터 전송을 위한 임시 IP 주소를 지정해야 합니다. 교체 어플라이언스는 대체 어플라이언스와 동일한 네트워크에 속하므로 교체 어플라이언스에서 이러한 각 네트워크에 대한 임시 IP 주소를 지정해야 합니다.

대상 어플라이언스 호환성

교체 어플라이언스는 교체 중인 소스 노드와 유형이 같아야 하며 두 어플라이언스 모두 동일한 논리 StorageGRID 사이트의 일부여야 합니다.

- 교체 서비스 어플라이언스는 교체되는 관리 노드 또는 게이트웨이 노드와 다를 수 있습니다.
  - SG100 소스 노드 어플라이언스를 SG1000 서비스 대상 어플라이언스에 복제하여 관리자 노드 또는

게이트웨이 노드에 더 큰 기능을 제공할 수 있습니다.

  - SG1000 소스 노드 어플라이언스를 SG100 서비스 대상 어플라이언스에 복제하여 SG1000을 보다 까다로운 응용 프로그램에 재배포할 수 있습니다.

    예를 들어 SG1000 소스 노드 어플라이언스를 관리 노드로 사용하고 있고 이를 전용 로드 밸런싱 노드로 사용하려는 경우

  - SG1000 소스 노드 어플라이언스를 SG100 서비스 대상 어플라이언스로 교체하면 네트워크 포트의 최대 속도가 100GbE에서 25GbE로 줄어듭니다.
  - SG100 및 SG1000 어플라이언스의 네트워크 커넥터가 서로 다릅니다. 어플라이언스 유형을 변경하려면 케이블이나 SFP 모듈을 교체해야 할 수 있습니다.

- 교체 스토리지 어플라이언스의 용량은 교체할 스토리지 노드보다 크거나 같아야 합니다.

  - 타겟 스토리지 어플라이언스의 드라이브 수가 소스 노드와 동일한 경우 타겟 어플라이언스의 드라이브 용량이 TB여야 합니다.
  - 소스 노드에서 사용된 것과 동일한 RAID 모드를 타겟 노드에서 사용하려는 경우 또는 스토리지 효율성이 떨어지는 RAID 모드(예: RAID6에서 DDP로 전환)에서는 타겟 어플라이언스의 드라이브가 소스 어플라이언스의 드라이브보다 크거나(TB 단위) 해야 합니다.
  - SSD(Solid State Drive) 설치로 인해 타겟 스토리지 어플라이언스에 설치된 표준 드라이브 수가 소스 노드의 드라이브 수보다 적은 경우(TB) 타겟 어플라이언스에 있는 표준 드라이브의 전체 스토리지 용량 소스 스토리지 노드에 있는 모든 드라이브의 총 기능 드라이브 용량을 충족하거나 초과해야 합니다.

    예를 들어 60개의 드라이브를 사용하는 SG5660 소스 스토리지 노드 어플라이언스를 58개의 표준 드라이브를 사용하는 SG6060 또는 SG606060X 타겟 어플라이언스에 복제할 경우, 스토리지 용량을 유지하기 위해 클론 생성 전에 더 큰 드라이브를 SG6060 또는 SG6060X 타겟 어플라이언스에 설치해야 합니다. (타겟 어플라이언스에 SSD가 포함된 드라이브 슬롯 2개는 총 어플라이언스 스토리지 용량에 포함되지 않습니다.)

    하지만 60 드라이브 SG5660 소스 노드 어플라이언스가 SANtricity Dynamic Disk Pools DDP-8로 구성된 경우 DDP-16을 사용하여 58 드라이브 동일 크기 드라이브 SG6060 또는 SG606060X 타겟 어플라이언스를 구성하면 스토리지 효율성이 개선되어 SG6060 또는 SG606060X 어플라이언스가 유효한 클론 타겟이 될 수 있습니다.

Grid Manager의 * nodes * 페이지에서 소스 어플라이언스 노드의 현재 RAID 모드에 대한 정보를 볼 수 있습니다. 어플라이언스에 대한 * Storage * 탭을 선택합니다.

클론이 생성되지 않는 정보는 무엇입니까?

클론 생성 중에는 다음 어플라이언스 구성이 교체 어플라이언스로 전송되지 않습니다. 교체 어플라이언스의 초기 설정 중에 구성해야 합니다.

- BMC 인터페이스
- 네트워크 링크
- 노드 암호화 상태입니다
- SANtricity 시스템 관리자(스토리지 노드의 경우)
- RAID 모드(스토리지 노드의 경우)

클론 생성을 방해하는 문제는 무엇입니까?

클론 복제 중에 다음 문제가 발생하면 복제 프로세스가 중지되고 오류 메시지가 생성됩니다.

- 네트워크 구성이 잘못되었습니다
- 소스와 타겟 어플라이언스 간의 연결 부족
- 소스 및 타겟 어플라이언스가 호환되지 않습니다
- 스토리지 노드의 경우 용량이 부족한 대체 어플라이언스입니다

복제를 계속하려면 각 문제를 해결해야 합니다.

어플라이언스 노드 클론 생성을 위한 고려 사항 및 요구 사항

어플라이언스 노드를 클론 복제하기 전에 고려 사항 및 요구 사항을 이해해야 합니다.

교체 어플라이언스에 대한 하드웨어 요구 사항

교체 제품이 다음 기준을 충족하는지 확인하십시오.

- 소스 노드(어플라이언스 교체)와 타겟(새) 어플라이언스는 어플라이언스의 유형이 동일해야 합니다.
  - 관리 노드 어플라이언스 또는 게이트웨이 노드 어플라이언스를 새 서비스 어플라이언스에만 복제할 수 있습니다.
  - 스토리지 노드 어플라이언스는 새 스토리지 어플라이언스에만 복제할 수 있습니다.
- 관리 노드 또는 게이트웨이 노드 어플라이언스의 경우 소스 노드 어플라이언스 및 타겟 어플라이언스가 동일한 유형의 어플라이언스일 필요는 없지만 어플라이언스 유형을 변경하려면 케이블이나 SFP 모듈을 교체해야 할 수 있습니다.

  예를 들어 SG1000 노드 어플라이언스를 SG100으로 교체하거나 SG100 어플라이언스를 SG1000 어플라이언스로 교체할 수 있습니다.

- 스토리지 노드 어플라이언스의 경우 소스 노드 어플라이언스와 타겟 어플라이언스는 어플라이언스 유형이 같을 필요는 없지만 타겟 어플라이언스의 스토리지 용량은 소스 어플라이언스보다 커야 합니다.

  예를 들어 SG5600 노드 어플라이언스를 SG5700 또는 SG6000 어플라이언스로 교체할 수 있습니다.

StorageGRID 설치 시 특정 어플라이언스 노드를 클론 복제하기 위해 호환되는 교체 어플라이언스를 선택하는 데 도움이 필요하면 StorageGRID 영업 담당자에게 문의하십시오.

어플라이언스 노드의 클론을 생성할 준비를 합니다

어플라이언스 노드를 클론 복제하기 전에 다음 정보가 있어야 합니다.

- 초기 설치 중에 대상 어플라이언스와 함께 사용할 수 있도록 네트워크 관리자로부터 Grid Network에 대한 임시 IP 주소를 얻습니다. 소스 노드가 관리 네트워크 또는 클라이언트 네트워크에 속한 경우 이러한 네트워크에 대한 임시 IP 주소를 가져옵니다.

  임시 IP 주소는 일반적으로 클론 생성되는 소스 노드 어플라이언스와 동일한 서브넷에 있으며 클론 생성이 완료된 후에는 필요하지 않습니다. 클론 생성 연결을 설정하려면 소스 및 타겟 어플라이언스가 모두 StorageGRID의 기본 관리 노드에 연결되어야 합니다.

- StorageGRID 네트워크 성능 또는 데이터 가용성을 저하시키지 않으면서 최상의 데이터 전송 성능을 제공하는 데이터 전송 트래픽 복제에 사용할 네트워크를 결정합니다.

  클론 데이터 전송에 1GbE 관리자 네트워크를 사용하면 클론 생성 속도가 느려집니다.

- 타겟 어플라이언스에서 KMS(키 관리 서버)를 사용하여 노드 암호화를 사용할 것인지 확인하여 클론 생성 전에 초기 타겟 어플라이언스 설치 중에 노드 암호화를 활성화할 수 있도록 합니다. 어플라이언스 설치에 설명된 대로 소스 어플라이언스 노드에서 노드 암호화가 활성화되어 있는지 확인할 수 있습니다.

  소스 노드와 타겟 어플라이언스의 노드 암호화 설정이 다를 수 있습니다. 데이터 해독 및 암호화는 데이터 전송 중에 그리고 타겟 노드가 다시 시작되고 그리드에 조인될 때 자동으로 수행됩니다.

  - SG100 및 SG1000 서비스 어플라이언스
  - SG5600 스토리지 어플라이언스
  - SG5700 스토리지 어플라이언스
  - SG6000 스토리지 어플라이언스

- 타겟 어플라이언스의 RAID 모드를 기본 설정에서 변경해야 하는지 확인하여 클론 생성 전에 초기 타겟 어플라이언스 설치 중에 이 정보를 지정할 수 있습니다. Grid Manager의 * nodes * 페이지에서 소스 어플라이언스 노드의 현재 RAID 모드에 대한 정보를 볼 수 있습니다. 어플라이언스에 대한 * Storage * 탭을 선택합니다.

  소스 노드와 타겟 어플라이언스의 RAID 설정은 다를 수 있습니다.

- 노드 클론 생성 프로세스를 완료하는 데 충분한 시간을 확보하십시오. 운영 스토리지 노드에서 타겟 어플라이언스로 데이터를 전송하려면 며칠이 걸릴 수 있습니다. 비즈니스에 미치는 영향을 최소화할 수 있도록 한 번에 클론 복제 일정을 수립합니다.
- 한 번에 하나의 어플라이언스 노드만 복제해야 합니다. 클론 생성 시 다른 StorageGRID 유지 보수 기능을 동시에 수행할 수 없습니다.
- 어플라이언스 노드를 복제한 후에는 설치 전 상태로 반환된 소스 어플라이언스를 대상으로 사용하여 다른 호환 노드 어플라이언스를 복제할 수 있습니다.

클론 어플라이언스 노드

클론 생성 프로세스는 소스 노드(어플라이언스 교체)와 타겟(새) 어플라이언스 간에 데이터를 전송하는 데 며칠이 걸릴 수 있습니다.

필요한 것

- 호환 대상 어플라이언스를 캐비닛이나 랙에 설치하고, 모든 케이블을 연결하고, 전원을 공급했습니다.
- 교체 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램 버전이 StorageGRID 시스템의 소프트웨어 버전과 일치하는지 확인하고, 필요한 경우 StorageGRID 어플라이언스 설치 프로그램 펌웨어를 업그레이드합니다.
- StorageGRID 접속 구성, SANtricity 시스템 관리자(스토리지 어플라이언스 전용) 및 BMC 인터페이스를 포함하여 타겟 어플라이언스를 구성했습니다.
  - StorageGRID 연결을 구성할 때는 임시 IP 주소를 사용합니다.
  - 네트워크 링크를 구성할 때는 최종 링크 구성을 사용하십시오.

> 초기 타겟 어플라이언스 구성을 완료한 후 StorageGRID 어플라이언스 설치 프로그램을 열어 둡니다. 노드 클론 생성 프로세스를 시작하면 타겟 어플라이언스의 설치 관리자 페이지로 돌아갑니다.

- 대상 어플라이언스에 대한 노드 암호화를 선택적으로 활성화했습니다.
- 대상 어플라이언스에 대해 RAID 모드를 선택적으로 설정할 수 있습니다(스토리지 어플라이언스만 해당).
- 어플라이언스 노드 클론 생성을 위한 고려 사항 및 요구 사항

  SG100 및 SG1000 서비스 어플라이언스

  SG5600 스토리지 어플라이언스

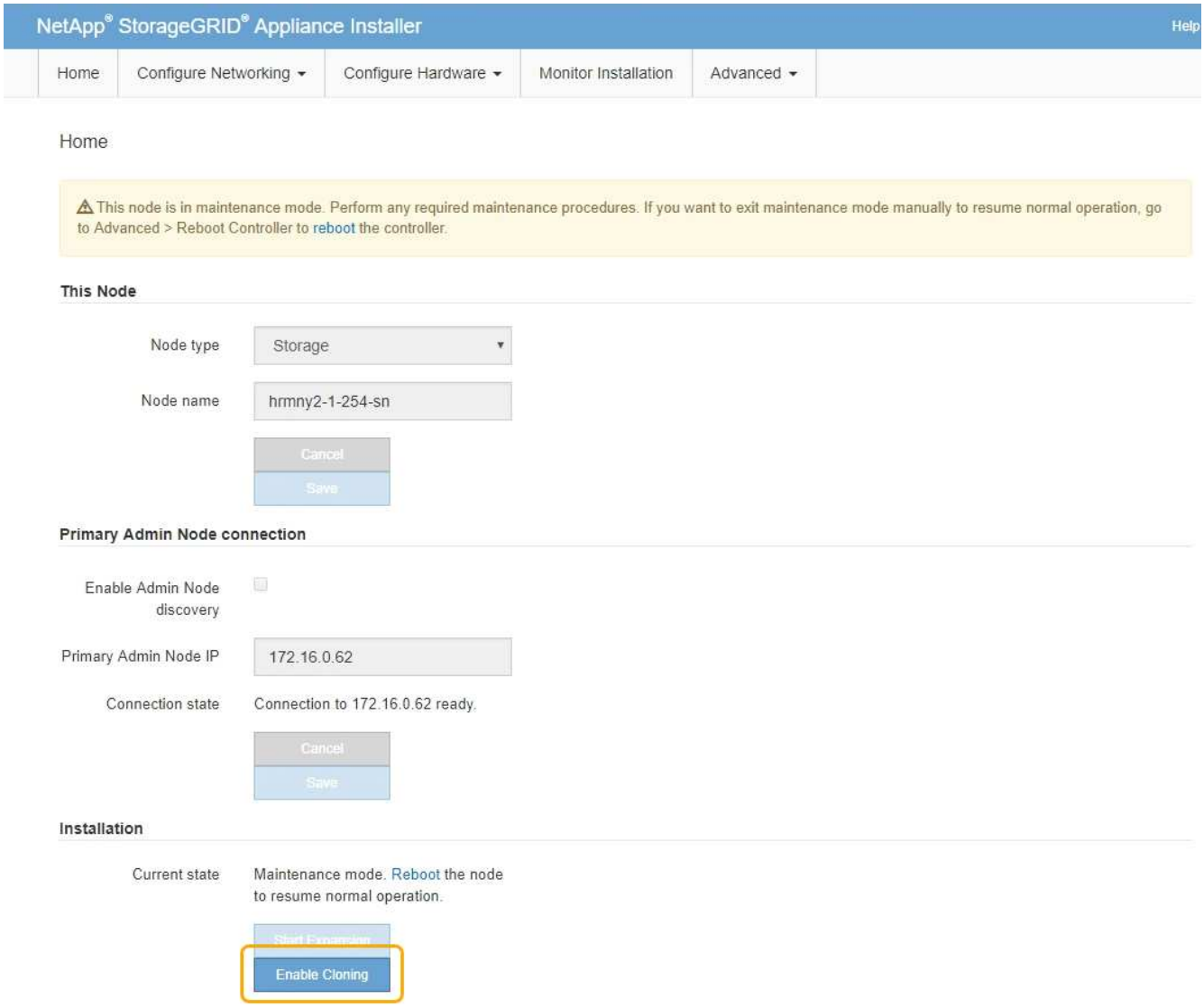
  SG5700 스토리지 어플라이언스

  SG6000 스토리지 어플라이언스

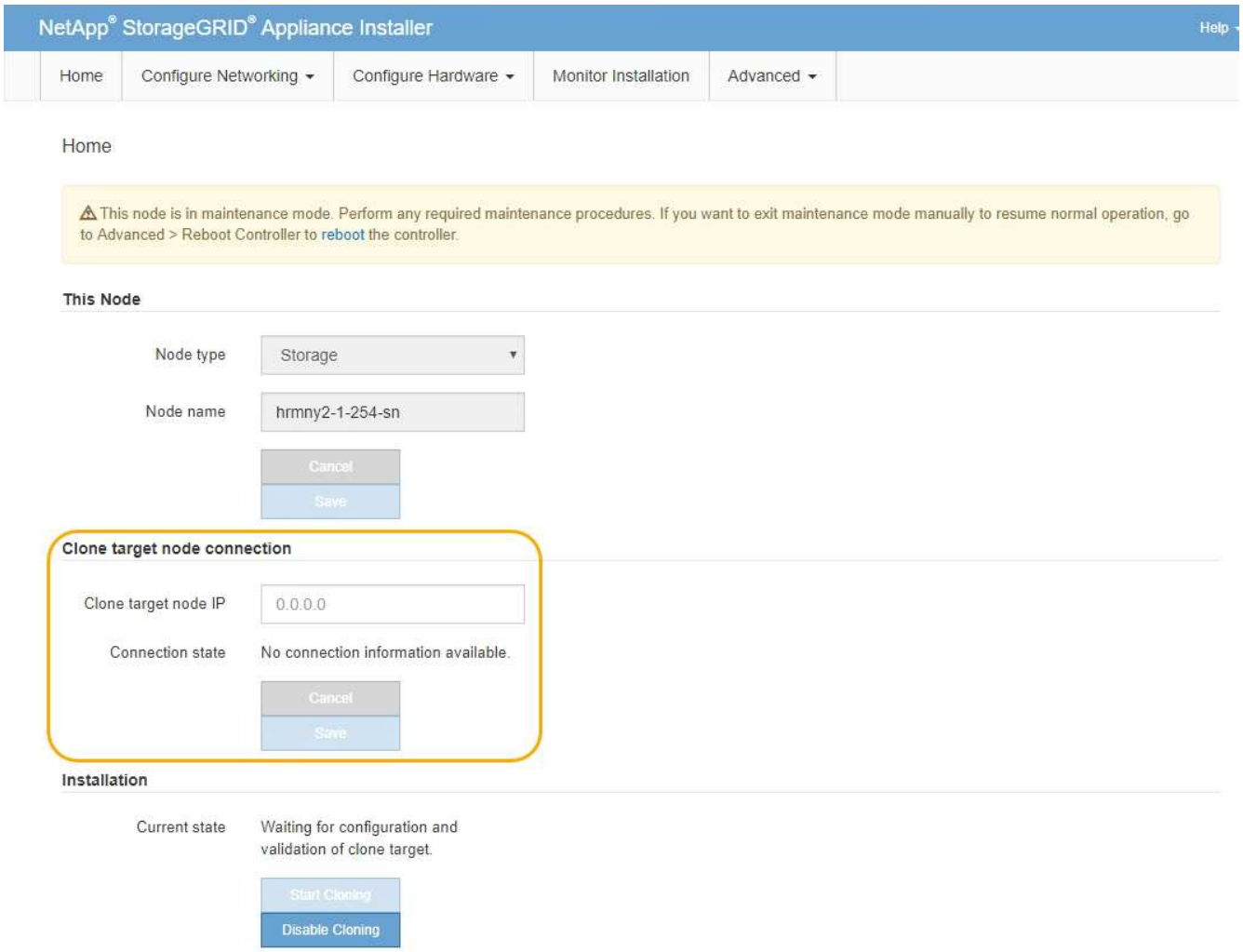
StorageGRID 네트워크 성능과 데이터 가용성을 유지하려면 한 번에 하나의 어플라이언스 노드만 복제해야 합니다.

단계

1. 클론 생성 중인 소스 노드를 유지보수 모드로 설정합니다.
2. 소스 노드의 StorageGRID 어플라이언스 설치 프로그램에서 홈 페이지의 설치 섹션에서 * 클론 생성 활성화 * 를 선택합니다.



운영 관리자 노드 연결 섹션이 클론 타겟 노드 연결 섹션으로 대체됩니다.

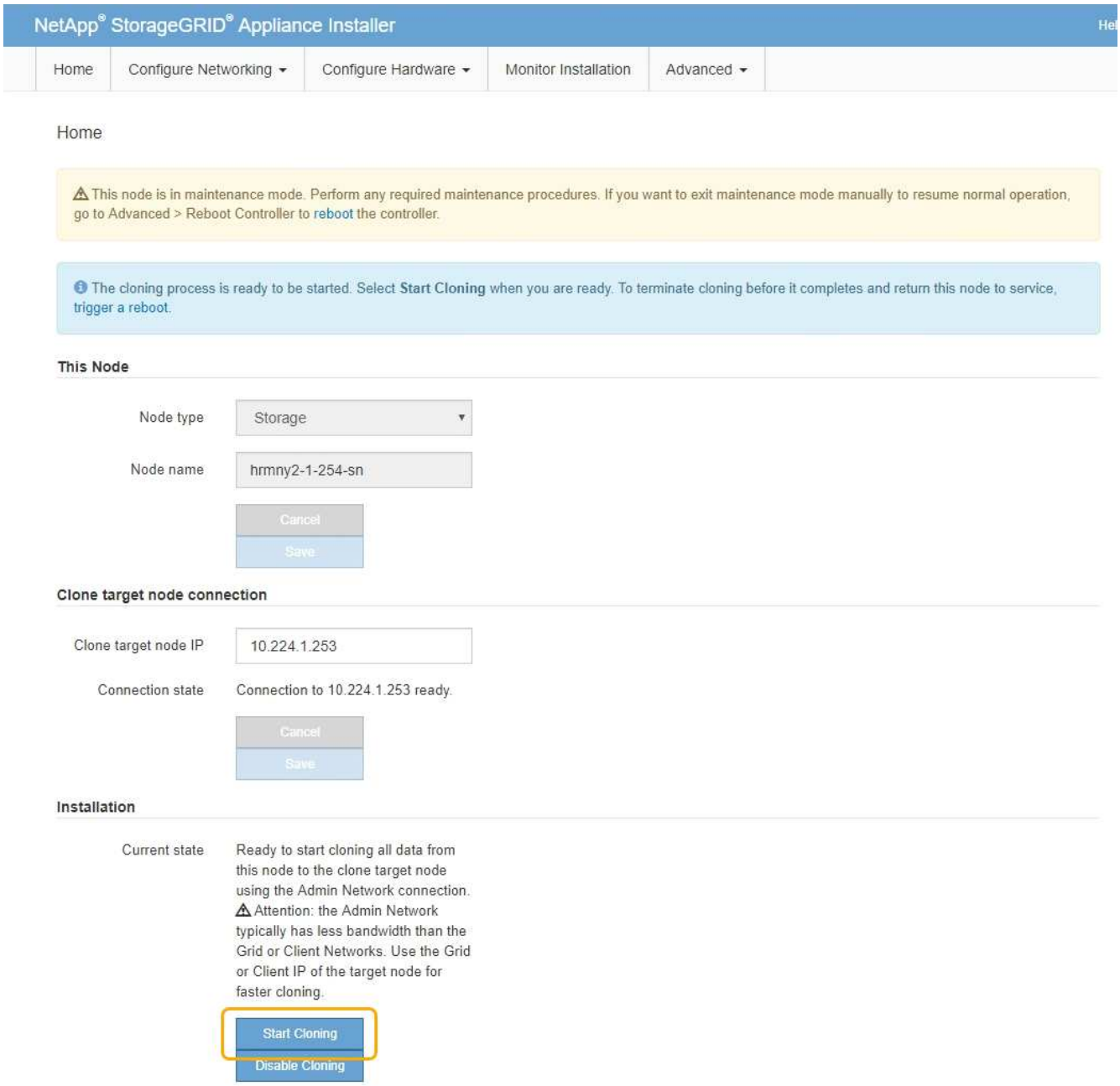


3. 클론 타겟 노드 IP * 의 경우 클론 데이터 전송 트래픽에 사용할 네트워크의 타겟 노드에 할당된 임시 IP 주소를 입력한 다음 * Save * 를 선택합니다.

   일반적으로 그리드 네트워크의 IP 주소를 입력하지만 클론 데이터 전송 트래픽에 다른 네트워크를 사용해야 하는 경우 해당 네트워크에 있는 대상 노드의 IP 주소를 입력합니다.

   > ⓘ 클론 데이터 전송에 1GbE 관리자 네트워크를 사용하면 클론 생성 속도가 느려집니다.

   타겟 어플라이언스를 구성 및 검증한 후 설치 섹션에서 소스 노드에서 * 클론 생성 시작 * 이 활성화됩니다.



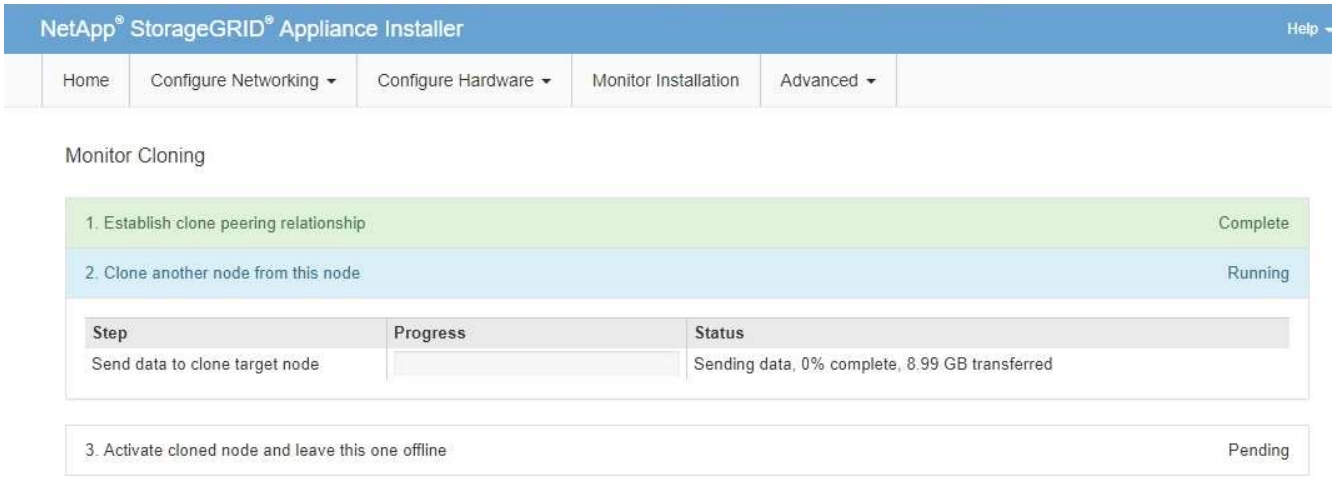
복제를 방해하는 문제가 있는 경우 * 클론 생성 시작 * 이 활성화되지 않으며 해결해야 하는 문제가 * 연결 상태 * 로 나열됩니다. 이러한 문제는 소스 노드와 타겟 어플라이언스의 StorageGRID 어플라이언스 설치 관리자 홈 페이지에 나열되어 있습니다. 한 번에 하나의 문제만 표시되고 상태가 변경되면 상태가 자동으로 업데이트됩니다. 클론 생성 시작 * 을 활성화하려면 모든 클론 생성 문제를 해결하십시오.

클론 생성 시작 * 이 활성화되면 * 현재 상태 * 는 트래픽을 복제하기 위해 선택된 StorageGRID 네트워크와 해당 네트워크 연결 사용에 대한 정보를 나타냅니다.

어플라이언스 노드 클론 생성을 위한 고려 사항 및 요구 사항

4. 소스 노드에서 * 클론 생성 시작 * 을 선택합니다.
5. 소스 또는 타겟 노드에서 StorageGRID 어플라이언스 설치 프로그램을 사용하여 클론 생성 진행률을 모니터링합니다.

   소스 노드와 타겟 노드의 StorageGRID 어플라이언스 설치 프로그램은 동일한 상태를 나타냅니다.



클론 생성 모니터링 페이지에서는 클론 생성 프로세스의 각 단계에 대한 자세한 진행 상황을 제공합니다.

- * 클론 피어링 관계 설정 * 은 클론 생성 설정 및 구성의 진행률을 표시합니다.
- * 이 노드에서 다른 노드 복제 * 는 데이터 전송 진행률을 표시합니다. (복제 프로세스의 이 부분을 완료하는 데 며칠이 걸릴 수 있습니다.)
- * 복제된 노드를 활성화하고 이 노드를 오프라인으로 둡니다. * 데이터 전송이 완료된 후 컨트롤을 대상 노드로 전송하고 소스 노드를 설치 전 상태로 설정하는 과정이 표시됩니다.

6. 클론 생성 프로세스를 종료하고 소스 노드를 서비스로 반환해야 하는 경우 소스 노드에서 StorageGRID 어플라이언스 설치 관리자 홈 페이지로 이동하여 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * StorageGRID * 으로 재부팅 * 을 선택합니다.

   클로닝 프로세스가 종료된 경우:

   - 소스 노드가 유지보수 모드를 종료하고 StorageGRID를 다시 연결합니다.
   - 타겟 노드는 사전 설치 상태로 유지됩니다. 소스 노드의 클론을 다시 시작하려면 1단계에서 클론 생성 프로세스를 다시 시작합니다.

클론 생성이 성공적으로 완료되면 다음을 수행합니다.

- 소스 및 타겟 노드가 IP 주소를 바꿉니다.
  - 이제 타겟 노드는 그리드, 관리 및 클라이언트 네트워크의 소스 노드에 원래 할당된 IP 주소를 사용합니다.
  - 이제 소스 노드는 타겟 노드에 처음 할당된 임시 IP 주소를 사용합니다.
- 타겟 노드가 유지보수 모드를 종료하고 StorageGRID를 결합하여 소스 노드를 대체합니다.
- 소스 어플라이언스는 이미 설치되어 있는 상태입니다 재설치를 준비했습니다.

> 어플라이언스가 그리드에 다시 연결되지 않으면 소스 노드의 StorageGRID 어플라이언스 설치 관리자 홈 페이지로 이동하여 * 고급 * > * 컨트롤러 재부팅 * 을 선택한 다음 * 유지 관리 모드로 재부팅 * 을 선택합니다. 소스 노드가 유지보수 모드로 재부팅된 후 노드 클론 복제 절차를 반복합니다.

타겟 노드에서 예기치 않은 문제가 발생하는 경우 사용자 데이터는 복구 옵션으로 소스 어플라이언스에 유지됩니다. 타겟 노드가 StorageGRID에 성공적으로 다시 결합되면 소스 어플라이언스의 사용자 데이터가 오래되어 더 이상 필요하지 않습니다. 필요한 경우 StorageGRID 지원 부서에 문의하여 소스 어플라이언스를 지우면 이 데이터가 삭제됩니다.

다음을 수행할 수 있습니다.

- 소스 어플라이언스를 추가 클론 생성 작업의 타겟으로 사용합니다. 추가 구성이 필요하지 않습니다. 이 어플라이언스에는 첫 번째 클론 타겟에 대해 원래 지정된 임시 IP 주소가 이미 할당되어 있습니다.
- 소스 어플라이언스를 새 어플라이언스 노드로 설치 및 설정합니다.
- 소스 제품을 StorageGRID에서 더 이상 사용하지 않을 경우 폐기하십시오.

감사 로그를 검토합니다

감사 로그 검토: 개요

이 지침에는 StorageGRID 감사 메시지 및 감사 로그의 구조 및 내용에 대한 정보가 포함되어 있습니다. 이 정보를 사용하여 시스템 활동의 감사 추적을 읽고 분석할 수 있습니다.

이 지침은 StorageGRID 시스템의 감사 메시지를 분석해야 하는 시스템 활동 및 사용 보고서를 작성하는 관리자를 위한 것입니다.

텍스트 로그 파일을 사용하려면 관리자 노드에서 구성된 감사 공유에 액세스할 수 있어야 합니다.

감사 메시지 수준 구성 및 외부 syslog 서버 사용에 대한 자세한 내용은 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다.

관련 정보

- StorageGRID 관리

감사 메시지 흐름 및 보존

모든 StorageGRID 서비스는 정상적인 시스템 작동 중에 감사 메시지를 생성합니다. 이러한 감사 메시지가 StorageGRID 시스템을 통해 어떻게 'audit.log' 파일로 이동하는지 이해해야 합니다.

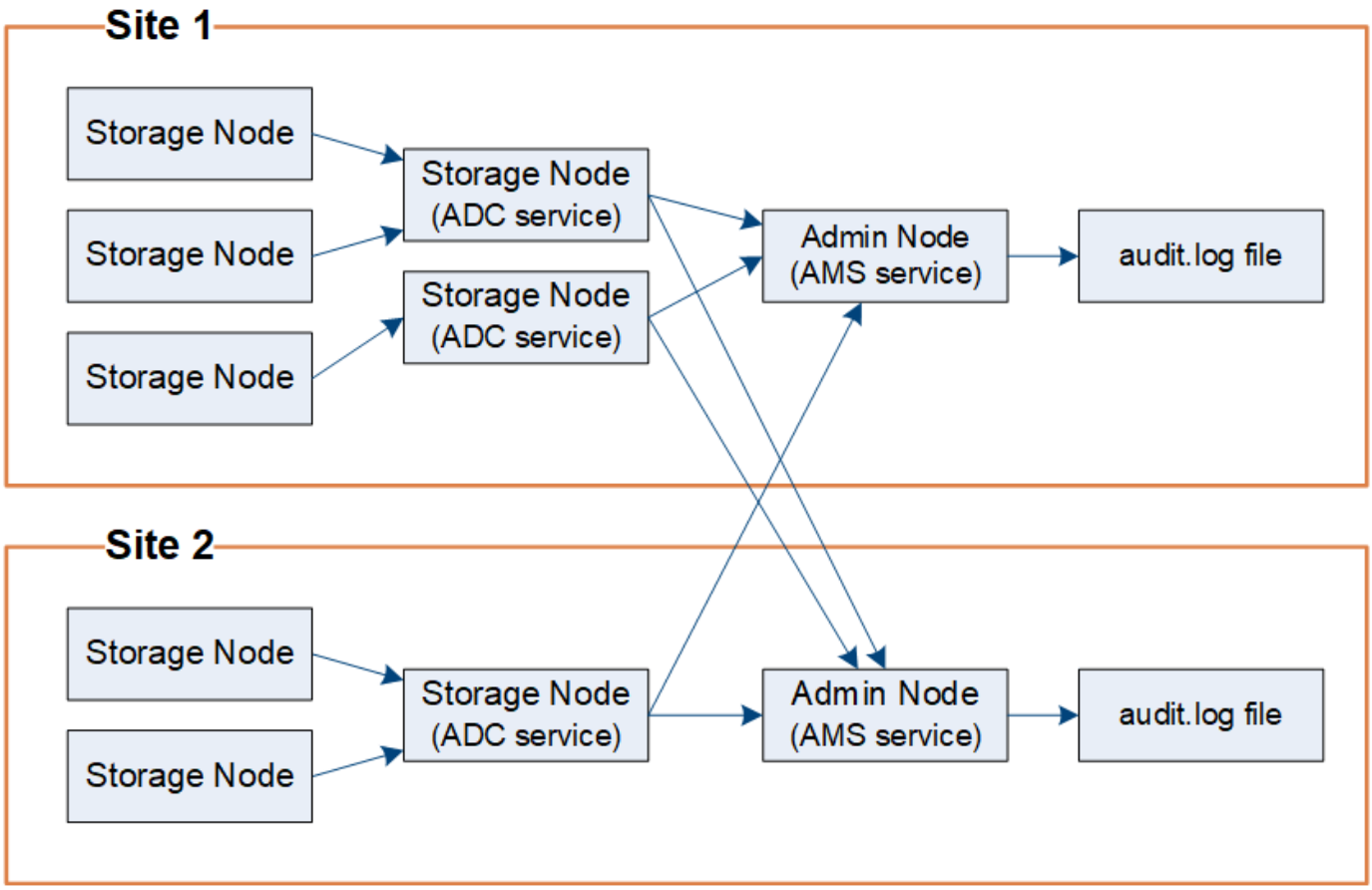
감사 메시지 흐름

감사 메시지는 관리 노드 및 ADC(관리 도메인 컨트롤러) 서비스가 있는 스토리지 노드에 의해 처리됩니다.

감사 메시지 흐름도에 표시된 대로 각 StorageGRID 노드는 데이터 센터 사이트의 ADC 서비스 중 하나에 감사 메시지를 보냅니다. ADC 서비스는 각 사이트에 설치된 처음 세 개의 스토리지 노드에 대해 자동으로 활성화됩니다.

그러면 각 ADC 서비스가 릴레이 역할을 하고 감사 메시지 모음을 StorageGRID 시스템의 모든 관리 노드로 전송하여 각 관리 노드에 시스템 활동의 전체 기록을 제공합니다.

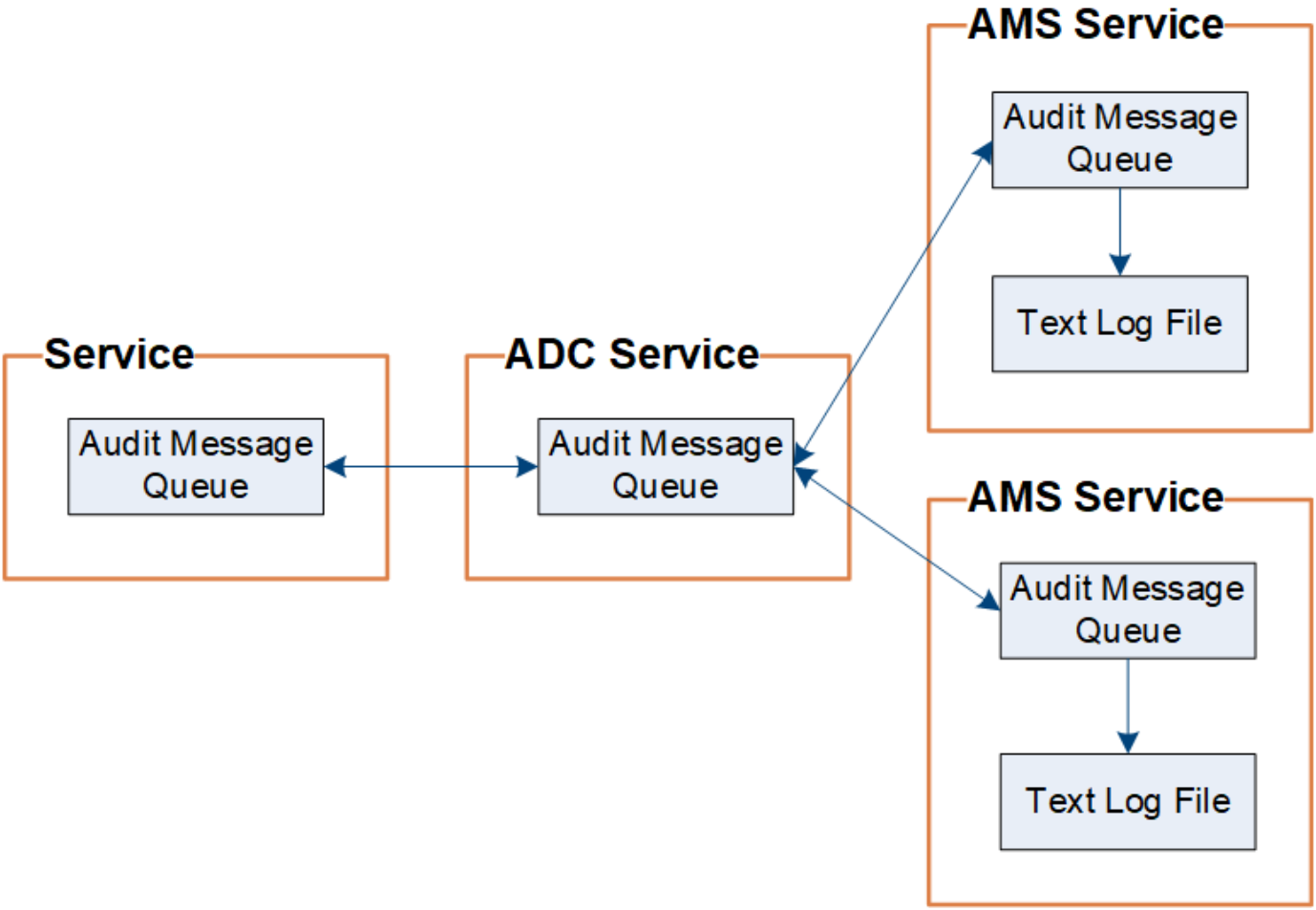
각 Admin Node는 텍스트 로그 파일에 감사 메시지를 저장하며, Active 로그 파일은 AUDIT.LOG로 명명된다.



감사 메시지 보존

StorageGRID는 복사 및 삭제 프로세스를 사용하여 감사 로그에 쓰기 전에 감사 메시지가 손실되지 않도록 합니다.

노드가 감사 메시지를 생성하거나 릴레이할 때 이 메시지는 그리드 노드의 시스템 디스크에 있는 감사 메시지 큐에 저장됩니다. 관리 노드의 '/var/local/audit/export' 디렉토리에 감사 로그 파일에 메시지가 기록될 때까지 메시지 복사본은 항상 감사 메시지 큐에 유지됩니다. 이렇게 하면 전송 중에 감사 메시지 손실을 방지할 수 있습니다.



네트워크 연결 문제 또는 감사 용량 부족으로 인해 감사 메시지 큐가 일시적으로 증가할 수 있습니다. 대기열이 늘어갈수록 각 노드의 '/var/local/' 디렉토리에서 사용 가능한 공간이 더 많이 사용됩니다. 문제가 지속되고 노드의 감사 메시지 디렉토리가 너무 가득 차면 개별 노드가 백로그 처리를 우선 순위에 따라 새 메시지에 일시적으로 사용할 수 없게 됩니다.

특히 다음과 같은 행동을 볼 수 있습니다.

- Admin Node에서 사용하는 '/var/local/audit/export' 디렉토리가 가득 차면 디렉토리가 더 이상 가득 차지 않을 때까지 Admin Node가 새 감사 메시지에 사용할 수 없는 것으로 플래그가 지정됩니다. S3 및 Swift 클라이언트 요청은 영향을 받지 않습니다. 감사 리포지토리에 연결할 수 없을 때 XAMS(Unreachable Audit Repositories) 경보가 트리거됩니다.
- ADC 서비스가 있는 스토리지 노드에서 사용하는 "/var/local/" 디렉토리가 92% 차면 디렉토리가 87%만 가득 찰 때까지 노드가 메시지를 감사할 수 없는 것으로 플래그가 지정됩니다. 다른 노드에 대한 S3 및 Swift 클라이언트 요청은 영향을 받지 않습니다. 감사 릴레이에 연결할 수 없는 경우 NRLY(사용 가능한 감사 릴레이) 경보가 트리거됩니다.

  ADC 서비스에 사용 가능한 스토리지 노드가 없는 경우 스토리지 노드는 감사 메시지를 '/var/local/log/localaudit.log' 파일에 로컬로 저장합니다.

- 스토리지 노드에서 사용하는 "/var/local/" 디렉토리가 85%가 되면 노드에서 S3 및 Swift 클라이언트 요청을 거부하고 503 서비스 사용 불가 를 시작합니다.

다음과 같은 유형의 문제로 인해 감사 메시지 큐가 크게 증가할 수 있습니다.

- ADC 서비스가 있는 관리 노드 또는 스토리지 노드의 정전. 시스템의 노드 중 하나가 다운되면 나머지 노드가 백로그될 수 있습니다.
- 시스템의 감사 용량을 초과하는 지속적인 활동률입니다.
- 감사 메시지와 무관한 이유로 ADC 스토리지 노드의 '/var/local/' 공간이 가득 찼습니다. 이 경우 노드에서 새 감사 메시지 수신을 중지하고 현재 백로그의 우선 순위를 지정하며, 이로 인해 다른 노드에 백로그가 발생할 수 있습니다.

AMQS(Large audit queue alert and Audit messages Queued)(대형 감사 대기열 경고 및 감사 메시지 대기 중

시간에 따라 감사 메시지 대기열의 크기를 모니터링할 수 있도록 스토리지 노드 대기열 또는 관리 노드 대기열의 메시지 수가 특정 임계값에 도달하면 * 대규모 감사 대기열 * 경고와 레거시 AMQS 경보가 트리거됩니다.

대규모 감사 대기열 * 경고 또는 레거시 AMQS 경보가 트리거되면 시스템에서 로드를 확인하여 시작합니다. — 최근 트랜잭션이 많이 발생한 경우, 경고 및 알람은 시간이 지남에 따라 해결되어야 하며 무시할 수 있습니다.

경고 또는 경보가 지속되고 심각도가 증가하면 대기열 크기의 차트를 참조하십시오. 시간이 경과하거나 며칠 동안 꾸준히 증가하는 경우 감사 로드가 시스템의 감사 용량을 초과할 가능성이 높습니다. 클라이언트 쓰기 및 클라이언트 읽기의 감사 수준을 오류 또는 끄기로 변경하여 클라이언트 작업 속도를 줄이거나 기록된 감사 메시지 수를 줄입니다. 참조"감사 메시지 및 로그 대상을 구성합니다있습니다."

중복된 메시지

StorageGRID 시스템은 네트워크 또는 노드 장애가 발생할 경우 보수적인 접근 방식을 사용합니다. 따라서 감사 로그에 중복된 메시지가 있을 수 있습니다.

감사 로그 파일에 액세스합니다

감사 공유는 활성 'audit.log' 파일과 압축된 감사 로그 파일을 포함합니다. 감사 로그에 쉽게 액세스할 수 있도록 NFS 및 CIFS에 대한 감사 공유에 대한 클라이언트 액세스를 구성할 수 있습니다(CIFS는 더 이상 사용되지 않음). 관리자 노드의 명령줄에서 직접 감사 로그 파일에 액세스할 수도 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.
- 관리 노드의 IP 주소를 알아야 합니다.

단계

1. 관리자 노드에 로그인:
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
2. 감사 로그 파일이 포함된 디렉토리로 이동합니다.

   'cd /var/local/audit/export'

3. 필요에 따라 현재 또는 저장된 감사 로그 파일을 봅니다.

관련 정보

로그 파일 회전을 감사합니다

감사 로그 파일은 관리 노드의 '/var/local/audit/export' 디렉토리에 저장됩니다. 활성 감사 로그 파일은 audit.log로 명명됩니다.

> 선택적으로 감사 로그의 대상을 변경하고 감사 정보를 외부 syslog 서버로 보낼 수 있습니다. 외부 syslog 서버가 구성되면 감사 레코드의 로컬 로그가 계속 생성되고 저장됩니다. 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다.

하루 한 번, 활성화된 'audit.log' 파일이 저장되고, 새로운 'audit.log' 파일이 시작된다. 저장된 파일의 이름은 저장 시기를 나타냅니다('*yyyy-mm-dd.txt*' 형식). 하루에 둘 이상의 감사 로그가 생성되는 경우 파일 이름에 숫자가 추가된 파일 저장 날짜가 사용됩니다(*yyyy-mm-dd.txt.n*). 예를 들어 2018년 4월 15일 생성된 첫 번째 및 두 번째 로그 파일은 2018-04-15.txt와 2018-04-15.txt.1입니다.

하루 후에는 원래 날짜를 유지하는 형식(*yyyy-mm-dd.txt.gz*)으로 저장된 파일이 압축되고 이름이 변경됩니다. 시간이 지남에 따라 이로 인해 관리 노드의 감사 로그에 할당된 스토리지가 소비됩니다. 스크립트는 감사 로그 공간 소비를 모니터링하고 필요에 따라 로그 파일을 삭제하여 '/var/local/audit/export' 디렉토리의 공간을 확보합니다. 감사 로그는 작성된 날짜를 기준으로 삭제되며 가장 오래된 로그가 먼저 삭제됩니다. 다음 파일에서 스크립트의 작업을 모니터링할 수 있습니다: '/var/local/log/manage-audit.log'.

이 예에서는 액티브 'audit.log' 파일, 전날 파일('2018-04-15.txt') 및 전날 압축 파일('2018-04-14.txt.gz')을 보여 줍니다.

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

감사 로그 파일 및 메시지 형식

감사 로그를 사용하여 시스템에 대한 정보를 수집하고 문제를 해결할 수 있습니다. 감사 로그 파일의 형식과 감사 메시지에 사용되는 일반 형식을 이해해야 합니다.

감사 로그 파일 형식

감사 로그 파일은 모든 관리 노드에서 찾을 수 있으며 개별 감사 메시지 모음을 포함합니다.

각 감사 메시지에는 다음이 포함됩니다.

- ISO 8601 형식의 감사 메시지(ATIM)를 트리거한 이벤트의 UTC(협정 세계시) 다음에 공백이 옵니다.

  '*YYYY-MM-DDTHH:MM:SS.UUUUUUU*'는 마이크로초입니다.

- 대괄호로 묶인 감사 메시지 자체가 AUDT로 시작하는 메시지입니다.

다음 예제에서는 감사 로그 파일에 포함된 세 가지 감사 메시지를 보여 줍니다(가독성을 위해 줄 바꿈이 추가됨). 이러한 메시지는 테넌트가 S3 버킷을 생성하고 이 버킷에 두 개의 오브젝트를 추가할 때 생성되었습니다.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

감사 로그 파일의 감사 메시지는 기본적으로 읽기 또는 해석하기가 쉽지 않습니다. 감사-설명 도구를 사용하면 감사 로그의 감사 메시지 요약을 간단하게 확인할 수 있습니다. '감사 합계' 도구를 사용하여 기록된 쓰기, 읽기 및 삭제 작업의 수와 이러한 작업에 소요된 시간을 요약할 수 있습니다.

관련 정보

감사 설명 도구를 사용합니다

감사 합계 도구를 사용합니다

감사-설명 도구를 사용하여 감사 로그의 감사 메시지를 읽기 쉬운 형식으로 변환할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.
- 기본 관리 노드의 IP 주소를 알아야 합니다.

이 작업에 대해

기본 관리 노드에서 사용할 수 있는 감사 설명 도구는 감사 로그에 감사 메시지를 간단히 요약해 줍니다.

> 감사-설명 도구는 주로 문제 해결 작업 중에 기술 지원 부서에서 사용하기 위한 것입니다. '감사 설명' 쿼리를 처리하면 StorageGRID 작업에 영향을 줄 수 있는 많은 CPU 성능이 소모될 수 있습니다.

이 예는 감사 설명 도구의 일반적인 출력을 보여줍니다. 이러한 4개의 SPUT 감사 메시지는 계정 ID 92484777768032262787 0이 있는 S3 테넌트가 S3 PUT 요청을 사용하여 "bucket1"이라는 이름의 버킷을 생성하고 해당 버킷에 3개의 오브젝트를 추가할 때 생성되었습니다.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

감사-설명 도구는 일반 감사 로그 또는 압축 감사 로그를 처리할 수 있습니다. 예를 들면 다음과 같습니다.

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

감사-설명 도구는 동시에 여러 파일을 처리할 수도 있습니다. 예를 들면 다음과 같습니다.

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

마지막으로, 감사-설명 도구는 파이프에서 입력을 받아 "grep" 명령이나 다른 방법을 사용하여 입력을 필터링하고 미리 처리할 수 있습니다. 예를 들면 다음과 같습니다.

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

감사 로그는 매우 크고 구문 분석 속도가 느릴 수 있으므로 전체 파일 대신 파트에 대해 보고 실행할 부분을 필터링하여 시간을 절약할 수 있습니다.

> 감사 설명 도구는 압축된 파일을 파이프 입력 파일로 받아들이지 않습니다. 압축된 파일을 처리하려면 파일 이름을 명령줄 인수로 제공하거나 "zcat" 도구를 사용하여 먼저 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

```
zcat audit.log.gz | audit-explain
```

사용 가능한 옵션을 보려면 도움말(-h) 옵션을 사용하십시오. 예를 들면 다음과 같습니다.

```
$ audit-explain -h
```

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
2. 다음 명령을 입력합니다. 여기서 '/var/local/audit/export/audit.log'는 분석할 파일의 이름과 위치를 나타냅니다.

   '$audit-exit/var/local/audit/export/audit.log'

   감사-설명 도구는 지정된 파일 또는 파일의 모든 메시지에 대해 사람이 읽을 수 있는 해석을 인쇄합니다.

   > 선 길이를 줄이고 가독성을 높이기 위해 타임스탬프가 기본적으로 표시되지 않습니다. 타임스탬프를 보려면 timestamp("-t") 옵션을 사용합니다.

관련 정보

SPUT: S3 PUT

감사 합계 도구를 사용합니다

'Audit-sum' 툴을 사용하면 감사 메시지 쓰기, 읽기, 헤드 및 삭제 횟수를 세고 각 작업 유형에 대한 최소, 최대 및 평균 시간(또는 크기)을 확인할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- "passwords.txt" 파일이 있어야 합니다.

- 기본 관리 노드의 IP 주소를 알아야 합니다.

이 작업에 대해

기본 관리 노드에서 사용할 수 있는 감사 합계 도구는 기록된 쓰기, 읽기 및 삭제 작업의 수와 이러한 작업이 소요된 시간을 요약합니다.

> 감사 합계 도구는 주로 문제 해결 작업 중에 기술 지원 부서에서 사용하도록 설계되었습니다. '감사 합계' 쿼리를 처리하면 많은 CPU 성능이 소모되어 StorageGRID 작업에 영향을 줄 수 있습니다.

이 예에서는 '감사 합계' 도구의 일반적인 출력을 보여 줍니다. 이 예에서는 프로토콜 작업이 얼마나 오래 걸렸는지 보여 줍니다.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                  1771398        0.011        1770.563
0.487
```

"감사 합계" 도구는 감사 로그에 다음 S3, Swift 및 ILM 감사 메시지의 수와 시간을 제공합니다.

코드	설명	을 참조하십시오
ARCT	클라우드 계층에서 아카이브 검색 - 계층	ARCT: 클라우드 계층에서 아카이브 검색
ASCT	Archive Store Cloud - Tier 를 선택합니다	ASCT: Archive Store Cloud - Tier(아카이브 저장소 클라우드 - 계층)
IDEL	ILM에서 삭제 시작: ILM이 개체 삭제 프로세스를 시작할 때 기록합니다.	IDEL: ILM 삭제 시작
SDEL	S3 삭제: 오브젝트 또는 버킷을 삭제하기 위해 트랜잭션을 성공적으로 기록합니다.	SDEL: S3 삭제
SGET	S3 GET: 성공적인 트랜잭션을 로그하여 객체를 검색하거나 버킷의 오브젝트를 나열합니다.	SGET: S3 GET

코드	설명	을 참조하십시오
셰어	S3 HEAD: 성공한 트랜잭션을 로그하여 오브젝트 또는 버킷의 존재 여부를 확인합니다.	Shea: S3 헤드
SPUT	S3 PUT: 새 오브젝트 또는 버킷을 생성하기 위한 성공적인 트랜잭션을 기록합니다.	SPUT: S3 PUT
WDEL	SwiFT DELETE(빠른 삭제): 성공한 트랜잭션을 로그하여 오브젝트 또는 컨테이너를 삭제합니다.	WDEL: Swift 삭제
윙입니다	SwiFT GET: 성공한 트랜잭션을 로그하여 객체를 검색하거나 컨테이너의 객체를 나열합니다.	wget: Swift get
WHEA	SwiFT HEAD: 성공한 트랜잭션을 로그하여 오브젝트 또는 컨테이너의 존재를 확인합니다.	WHEA: 스위프트 헤드
WPUT	SwiFT PUT: 새 개체 또는 컨테이너를 생성하기 위해 트랜잭션을 성공적으로 기록합니다.	WPUT: Swift Put

감사 합계 도구는 일반 감사 로그 또는 압축 감사 로그를 처리할 수 있습니다. 예를 들면 다음과 같습니다.

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

감사 합계 도구는 동시에 여러 파일을 처리할 수도 있습니다. 예를 들면 다음과 같습니다.

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

마지막으로, 감사 합계 도구는 파이프에서 입력을 받아 "grep" 명령이나 다른 방법을 사용하여 입력을 필터링하고 미리 처리할 수 있습니다. 예를 들면 다음과 같습니다.

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```

> 이 도구는 압축된 파일을 파이프된 입력으로 허용하지 않습니다. 압축된 파일을 처리하려면 파일 이름을 명령줄 인수로 제공하거나 "zcat" 도구를 사용하여 먼저 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

명령줄 옵션을 사용하여 객체에 대한 작업과 별도로 버킷 작업을 요약하거나 버킷 이름, 기간 또는 목표 유형별로 메시지 요약을 그룹화할 수 있습니다. 기본적으로 요약에는 최소, 최대 및 평균 작동 시간이 표시되지만 '크기(-s)' 옵션을 사용하여 개체 크기를 확인할 수 있습니다.

사용 가능한 옵션을 보려면 도움말(-h) 옵션을 사용하십시오. 예를 들면 다음과 같습니다.

```
$ audit-sum -h
```

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 'ssh admin@*primary_Admin_Node_IP*' 명령을 입력합니다
   b. "passwords.txt" 파일에 나열된 암호를 입력합니다.
2. 쓰기, 읽기, 헤드 및 삭제 작업과 관련된 모든 메시지를 분석하려면 다음 단계를 수행하십시오.
   a. 다음 명령을 입력합니다. 여기서 '/var/local/audit/export/audit.log'는 분석할 파일의 이름과 위치를 나타냅니다.

      ```
      $ audit-sum /var/local/audit/export/audit.log
      ```

      이 예에서는 '감사 합계' 도구의 일반적인 출력을 보여 줍니다. 이 예에서는 프로토콜 작업이 얼마나 오래 걸렸는지 보여 줍니다.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

이 예에서 SGET(S3 GET) 작업은 평균 1.13초 동안 가장 느리지만, SGET 및 SPUT(S3 PUT) 작업은 모두 1,770초 정도의 긴 최악의 경우를 나타냅니다.

b. 가장 느린 10개의 검색 작업을 표시하려면 grep 명령을 사용하여 SGET 메시지만 선택하고 긴 출력 옵션('-l')을 추가하여 객체 경로('grep SGET audit.log | audit-sum-l')를 포함시킵니다

   결과에 유형(오브젝트 또는 버킷) 및 경로가 포함되어 있어 이러한 특정 오브젝트와 관련된 다른 메시지에 대해 감사 로그를 작성할 수 있습니다.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== =============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
이 예제 출력에서 세 개의 가장 느린 S3 GET 요청은 크기가 약 5GB인 오브젝트에 대해 다른 오브젝트보다 훨씬 크다는 것을 알 수 있습니다. 크기가 크면 검색 시간이 느려질 수 있습니다.

3. 그리드에서 인제스트되고 검색되는 오브젝트 크기를 결정하려면 크기 옵션('-s')을 사용합니다.

```
audit-sum -s audit.log
```

```
  message group            count       min(MB)          max(MB)
average(MB)
  =============            =====     ========        ========
============
  IDEL                       274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

이 예에서 SPUT의 평균 개체 크기는 2.5MB 미만이지만 SGET의 평균 크기는 훨씬 큽니다. SPUT 메시지 수가 SGET 메시지 수보다 훨씬 많음을 나타내며, 이는 대부분의 개체가 검색되지 않음을 나타냅니다.

4. 어제 검색 속도가 느리는지 확인하려면:

   a. 적절한 감사 로그에 명령을 입력하고 GROUP-By-TIME 옵션('-GT')을 사용한 다음 기간(예: 15M, 1H, 10S)을 사용합니다.

```
grep SGET audit.log | audit-sum -gt 1H
```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

이러한 결과는 S3이 06:00에서 07:00 사이에 트래픽이 증가하는 것을 보여줍니다. 최대 시간과 평균 시간도 이 시기에 상당히 높으면서, 수가 증가할수록 점차 증가하지는 않았습니다. 이는 네트워크 또는 그리드의 요청 처리 능력 중 어느 곳보다 용량이 초과된 것을 의미합니다.

b. 어제 매시간 검색되는 개체의 크기를 확인하려면 명령에 size 옵션('-s')을 추가합니다.

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

이러한 결과는 전체 검색 트래픽이 최대값일 때 매우 큰 검색 결과가 발생했음을 나타냅니다.

c. 자세한 내용을 보려면 '감사 설명' 도구를 사용하여 해당 시간 동안 모든 SGET 작업을 검토하십시오.

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

grep 명령의 출력이 여러 줄로 예상되는 경우 "less" 명령을 추가하여 감사 로그 파일의 내용을 한 번에 한 페이지(한 화면)씩 표시합니다.

5. 버킷의 SPUT 작업이 개체에 대한 SPUT 작업보다 느리는지 확인하려면 다음을 수행합니다.

a. 먼저 오브젝트 및 버킷 작동을 위해 개별적으로 메시지를 그룹화하는 '-go' 옵션을 사용합니다.

```
grep SPUT sample.log | audit-sum -go
```

```
  message group            count     min(sec)        max(sec)
average(sec)
  =============            =====     ========        ========
============
  SPUT.bucket                  1        0.125           0.125
0.125
  SPUT.object                 12        0.025           1.019
0.236
```

결과는 버킷에 대한 SPUT 작업의 성능 특성이 객체에 대한 SPUT 작업과 다르다는 것을 보여줍니다.

b. 어떤 버킷이 가장 느린 SPUT 작업을 가지는지 확인하려면 버킷별로 메시지를 그룹화하는 '-GB' 옵션을 사용합니다.

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                   count     min(sec)        max(sec)
average(sec)
  =============                   =====     ========        ========
============
  SPUT.cho-non-versioning         71943        0.046        1770.563
1.571
  SPUT.cho-versioning             54277        0.047        1736.633
1.415
  SPUT.cho-west-region            80615        0.040          55.557
1.329
  SPUT.ldt002                   1564563        0.011          51.569
0.361
```

c. SPUT 객체 크기가 가장 큰 버킷을 결정하려면 '-GB'와 '-s' 옵션을 모두 사용합니다.

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

관련 정보

감사 설명 도구를 사용합니다

감사 메시지 형식

StorageGRID 시스템 내에서 교환되는 감사 메시지에는 모든 메시지에 공통되는 표준 정보 및 보고되는 이벤트 또는 활동을 설명하는 특정 콘텐츠가 포함됩니다.

감사-설명 및 감사-합계 도구가 제공하는 요약 정보가 부족한 경우 이 섹션을 참조하여 모든 감사 메시지의 일반적인 형식을 파악하십시오.

다음은 감사 로그 파일에 표시될 수 있는 감사 메시지의 예입니다.

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

각 감사 메시지에는 특성 요소의 문자열이 포함됩니다. 전체 문자열은 대괄호("[]")로 묶이고 문자열의 각 특성 요소에는 다음과 같은 특성이 있습니다.

- 괄호 '[]'로 묶습니다
- 감사 메시지를 나타내는 AUDT 문자열에 의해 도입되었습니다
- 앞 또는 뒤에 구분 기호(쉼표 또는 공백 없음)를 사용하지 않습니다
- 줄 바꿈 문자 '\n'에 의해 종료되었습니다

각 요소에는 특성 코드, 데이터 형식 및 다음 형식으로 보고된 값이 포함됩니다.

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

메시지의 특성 요소 수는 메시지의 이벤트 유형에 따라 달라집니다. 특성 요소는 특정 순서로 나열되지 않습니다.

다음 목록에서는 특성 요소에 대해 설명합니다.

- ATTR은 보고되는 특성에 대한 4자리 코드입니다. 모든 감사 메시지에 공통적으로 적용되는 일부 특성 및 이벤트별 특성이 있습니다.
- type은 UI64, FC32 등 값의 프로그래밍 데이터 형식의 4자리 식별자입니다. 형식은 괄호 '( )'로 묶습니다.
- 값 은 특성의 내용으로 일반적으로 숫자 또는 텍스트 값입니다. 값은 항상 콜론(':')을 따릅니다. CStr 데이터 형식의 값은 큰따옴표 " ""로 둘러싸입니다.

관련 정보

감사 설명 도구를 사용합니다

감사 합계 도구를 사용합니다

감사 메시지

감사 메시지의 공통 요소

데이터 유형

감사 메시지 예

데이터 유형

감사 메시지에 정보를 저장하는 데 사용되는 데이터 유형은 다양합니다.

유형	설명
UI32	부호 없는 긴 정수(32비트). 0에서 4,294,967,295 사이의 숫자를 저장할 수 있습니다.
UI64	부호 없는 이중 긴 정수(64비트). 0에서 18,446,744,073,709,551,615까지의 숫자를 저장할 수 있습니다.
FC32	4자 상수. 32비트 부호 없는 정수 값은 "ABCD"와 같은 4개의 ASCII 문자로 표시됩니다.
아이패드	IP 주소에 사용됩니다.

유형	설명
CStr(문자열)	UTF - 8 문자의 가변 길이 배열입니다. 문자는 다음과 같은 규약을 사용하여 이스케이프할 수 있습니다. • 백슬래시는 \\ 입니다. • 캐리지 리턴은\r입니다 • 큰따옴표는 \"지 않습니다. • 라인 피드(새 라인)는\n입니다 • 문자는 해당 16진수 등가물(\xHH 형식으로, 여기서 HH는 문자를 나타내는 16진수 값)로 대체할 수 있습니다.

이벤트 관련 데이터

감사 로그의 각 감사 메시지는 시스템 이벤트와 관련된 데이터를 기록합니다.

메시지 자체를 식별하는 열기 '[AUDT:]' 컨테이너에 이어 다음 속성 집합은 감사 메시지에서 설명하는 이벤트 또는 작업에 대한 정보를 제공합니다. 이러한 특성은 다음 예제에서 강조됩니다.

```
2018-12-05T08:24:45.921845 [AUDT: * \[RSLT\(FC32\):SUCS\] * \[TIME\(UI64\):11454\]
\[SAIP\(iPad\):"10.224.0.100"\]\[S3SStr\S31124562C642S562S564C6100C4S562S564CW5100C6100C6
100C4C4S564C4C4C4C4C4C4CW4S5100C4S562S564S564CW5100C4CW4S562S5100C4S5100C
4C4C4C4C4CW5100C4C4C4C4C6100C6100C6100CWs\S564C4C6100C4C4C4C4CWs\S564C4C4C4
CWs\S564CWs\S564C4C4S
```

이 예제에서 밑줄이 그어진 ATYP 요소는 메시지를 생성한 이벤트를 식별합니다. 이 예제 메시지에는 S3 헤드 요청에 의해 생성되었음을 나타내는 Shea 메시지 코드([ATYP(FC32):Shea])가 포함됩니다.

관련 정보

감사 메시지의 공통 요소

감사 메시지

감사 메시지의 공통 요소

모든 감사 메시지에는 공통 요소가 포함됩니다.

코드	유형	설명
있습니다	FC32	모듈 ID: 메시지를 생성한 모듈 ID의 4자리 식별자입니다. 이것은 감사 메시지가 생성된 코드 세그먼트를 나타냅니다.
ANID	UI32	노드 ID: 메시지를 생성한 서비스에 할당된 그리드 노드 ID입니다. 각 서비스는 StorageGRID 시스템을 구성하고 설치할 때 고유 식별자를 할당합니다. 이 ID는 변경할 수 없습니다.

코드	유형	설명
ASE	UI64	감사 세션 식별자: 이전 릴리즈에서는 이 요소는 서비스가 시작된 후 감사 시스템이 초기화된 시간을 나타냅니다. 이 시간 값은 운영 체제 Epoch(1970년 1월 1일 00:00:00 UTC) 이후 마이크로초 단위로 측정되었습니다. • 참고: * 이 요소는 사용되지 않으며 감사 메시지에 더 이상 나타나지 않습니다.
ASQN	UI64	시퀀스 수: 이전 릴리즈에서는 그리드 노드(ANID)에서 생성된 각 감사 메시지에 대해 이 카운터가 증가했으며 서비스 재시작 시 0으로 재설정됩니다. • 참고: * 이 요소는 사용되지 않으며 감사 메시지에 더 이상 나타나지 않습니다.
ATID	UI64	추적 ID: 단일 이벤트에 의해 트리거된 메시지 집합에서 공유하는 식별자입니다.
ATIM	UI64	Timestamp: 감사 메시지를 트리거한 이벤트가 생성된 시간으로, 운영 체제 Epoch(1970년 1월 1일 00:00:00 UTC) 이후 마이크로초 단위로 측정됩니다. 타임스탬프를 로컬 날짜 및 시간으로 변환하는 데 사용할 수 있는 대부분의 도구는 밀리초를 기반으로 합니다. 로깅된 타임스탬프의 반올림 또는 잘라내기가 필요할 수 있습니다. AUDIT.LOG 파일에서 감사 메시지 시작 부분에 나타나는 사람이 읽을 수 있는 시간은 ISO 8601 형식의 ATIM 속성입니다. 날짜 및 시간은 '*YYYY-MMDDTHH:MM:SS.UUUUUUU*'로 표시되며 여기서 T는 날짜 시간 세그먼트의 시작을 나타내는 리터럴 문자열 문자입니다. '*UUUUUU*'는 마이크로초입니다.
ATYP	FC32	이벤트 유형: 기록되는 이벤트의 4자리 식별자입니다. 이는 메시지의 "페이로드" 콘텐츠, 즉 포함된 속성을 제어합니다.
비버	UI32	버전: 감사 메시지의 버전입니다. StorageGRID 소프트웨어가 발전함에 따라 새로운 버전의 서비스에는 감사 보고에 새로운 기능이 포함될 수 있습니다. 이 필드를 사용하면 AMS 서비스의 이전 버전과의 호환성을 통해 이전 버전의 서비스에서 보낸 메시지를 처리할 수 있습니다.
RSLT	FC32	결과: 이벤트, 프로세스 또는 트랜잭션의 결과. 이 메시지와 관련이 없으면 메시지가 실수로 필터링되지 않도록 SUCS 대신 사용되지 않습니다.

감사 메시지 예

각 감사 메시지에서 자세한 정보를 찾을 수 있습니다. 모든 감사 메시지는 동일한 형식을 사용합니다.

다음은 감사 로그 파일에 나타날 수 있는 샘플 감사 메시지입니다.

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

감사 메시지에는 기록되는 이벤트에 대한 정보와 감사 메시지 자체에 대한 정보가 포함되어 있습니다.

감사 메시지에 의해 기록되는 이벤트를 식별하려면 ATYP 속성(아래에 강조 표시됨)을 찾습니다.

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP\(FC32\):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

ATYP 특성의 값은 SPUT입니다. SPUT는 오브젝트 인제스트를 버킷에 기록하는 S3 PUT 트랜잭션을 나타냅니다.

다음 감사 메시지는 객체가 연결된 버킷도 표시합니다.

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

PUT 이벤트가 발생한 시기를 확인하려면 감사 메시지 시작 부분에 UTC(Universal Coordinated Time) 타임스탬프를 기록합니다. 이 값은 감사 메시지 자체의 ATIM 속성:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM은 UNIX epoch 시작 이후 시간(단위: 마이크로초)을 기록합니다. 이 예에서 값 '1405631878959669'는 2014년 7월 17일 목요일 21:17:59 UTC로 변환됩니다.

관련 정보

SPUT: S3 PUT

감사 메시지의 공통 요소

감사 메시지 및 개체 수명 주기

감사 메시지는 개체가 수집되거나 검색되거나 삭제될 때마다 생성됩니다. API 관련(S3 또는 Swift) 감사 메시지를 찾아 감사 로그에서 이러한 트랜잭션을 식별할 수 있습니다.

감사 메시지는 각 프로토콜에 특정한 식별자를 통해 연결됩니다.

프로토콜	코드
S3 작업 연결	S3BK(S3 버킷) 및/또는 S3KY(S3 키)
Swift 작업 연결	WCON(Swift 컨테이너) 및/또는 WOBJ(Swift 오브젝트)
내부 작업 연결	CBID(객체의 내부 식별자)

감사 메시지 타이밍

그리드 노드 간 타이밍 차이, 개체 크기 및 네트워크 지연 등의 요인으로 인해 서로 다른 서비스에서 생성된 감사 메시지의 순서는 이 섹션의 예제에 표시된 순서와 다를 수 있습니다.

정보 수명 주기 관리 정책 구성

기본 ILM 정책(기본 2 복사본)을 사용하면 오브젝트 데이터가 총 2개 복사본에 대해 한 번 복사됩니다. ILM 정책에 2개 이상의 사본이 필요한 경우 각 추가 복사본에 대해 CBRE, CBSE 및 SCMT 메시지 집합이 추가로 제공됩니다. ILM 정책에 대한 자세한 내용은 정보 수명 주기 관리를 통해 개체 관리에 대한 정보를 참조하십시오.

아카이브 노드

아카이브 노드가 외부 아카이브 스토리지 시스템으로 개체 데이터를 전송할 때 생성되는 일련의 감사 메시지는 SCMT(Store Object Commit) 메시지가 없다는 점을 제외하고 스토리지 노드의 감사 메시지와 유사합니다. 그리고

ATCE(Archive Object Store Begin) 및 ASCE(Archive Object Store End) 메시지는 객체 데이터의 아카이빙된 각 사본에 대해 생성됩니다.

아카이브 노드가 외부 아카이브 스토리지 시스템에서 오브젝트 데이터를 검색할 때 생성되는 일련의 감사 메시지는 객체 데이터의 검색된 각 복제본에 대해 ARCB(Archive Object Retrieve Begin) 및 ARCE(Archive Object Retrieve End) 메시지가 생성된다는 점을 제외하고 스토리지 노드의 감사 메시지와 유사합니다.

아카이브 노드가 외부 아카이브 스토리지 시스템에서 오브젝트 데이터를 삭제할 때 생성되는 일련의 감사 메시지는 SREM(Object Store Remove) 메시지가 없고 각 삭제 요청에 대해 AREM(Archive Object Remove) 메시지가 있다는 점을 제외하고 스토리지 노드의 감사 메시지와 유사합니다.

관련 정보

ILM을 사용하여 개체를 관리합니다

오브젝트 수집 트랜잭션

API 관련(S3 또는 Swift) 감사 메시지를 찾아 감사 로그에서 클라이언트 수집 트랜잭션을 식별할 수 있습니다.

수집 트랜잭션 중에 생성된 모든 감사 메시지가 다음 표에 나와 있지 않습니다. 수집 트랜잭션을 추적하는 데 필요한 메시지만 포함됩니다.

S3 수집 감사 메시지

코드	이름	설명	트레이스	을 참조하십시오
SPUT	S3 PUT 트랜잭션	S3 PUT 수집 트랜잭션이 성공적으로 완료되었습니다.	CBID, S3BK, S3KY	SPUT: S3 PUT
ORLM	개체 규칙이 충족되었습니다	이 개체에 대한 ILM 정책이 충족되었습니다.	CBID	ORLM: 개체 규칙이 충족되었습니다

SWIFT 수집 감사 메시지

코드	이름	설명	트레이스	을 참조하십시오
WPUT	스위프트 PUT 트랜잭션	Swift Put 수집 트랜잭션이 성공적으로 완료되었습니다.	CBID, WCON, WOBJ	WPUT: Swift Put
ORLM	개체 규칙이 충족되었습니다	이 개체에 대한 ILM 정책이 충족되었습니다.	CBID	ORLM: 개체 규칙이 충족되었습니다

아래의 감사 메시지 시리즈는 S3 클라이언트가 스토리지 노드(LDR 서비스)에 개체를 인제스트할 때 감사 로그에 생성되고 저장되는 감사 메시지의 예입니다.

이 예에서 활성 ILM 정책에는 재고 ILM 규칙, Make 2 Copies가 포함됩니다.

> 아래 예에서는 트랜잭션 중에 생성된 모든 감사 메시지가 나와 있지 않습니다. S3 수집 트랜잭션(SPUT)과 관련된 항목만 나열됩니다.

이 예에서는 S3 버킷을 이전에 생성했다고 가정합니다.

SPUT: S3 PUT

SPUT 메시지는 특정 버킷에 오브젝트를 만들기 위해 S3 PUT 트랜잭션이 실행되었음을 나타내기 위해 생성됩니다.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: 개체 규칙이 충족되었습니다

ORLM 메시지는 이 개체에 대한 ILM 정책이 충족되었음을 나타냅니다. 메시지에는 객체의 CBID와 적용된 ILM 규칙 이름이 포함됩니다.

복제된 개체의 경우 Locs 필드에는 개체 위치의 LDR 노드 ID 및 볼륨 ID가 포함됩니다.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

삭제 코딩 오브젝트의 경우 삭제 코딩 프로필 ID와 삭제 코딩 그룹 ID가 Locs 필드에 포함됩니다

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

경로 필드에는 사용된 API에 따라 S3 버킷과 키 정보, Swift 컨테이너 및 오브젝트 정보가 포함됩니다.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

객체 삭제 트랜잭션입니다

API 관련(S3 및 Swift) 감사 메시지를 찾아 감사 로그에서 오브젝트 삭제 트랜잭션을 식별할 수 있습니다.

다음 표에는 삭제 트랜잭션 중에 생성된 모든 감사 메시지가 나와 있지 않습니다. 삭제 트랜잭션을 추적하는 데 필요한 메시지만 포함됩니다.

S3 감사 메시지 삭제

코드	이름	설명	트레이스	을 참조하십시오
SDEL	S3 삭제	버킷에서 오브젝트를 삭제하도록 요청했습니다.	CBID, S3KY	SDEL: S3 삭제

감사 메시지를 신속하게 삭제합니다

코드	이름	설명	트레이스	을 참조하십시오
WDEL	스위프트 삭제	컨테이너 또는 컨테이너에서 개체를 삭제하도록 요청했습니다.	CBID, WOBJ	WDEL: Swift 삭제

예: **S3** 오브젝트 삭제

S3 클라이언트가 스토리지 노드(LDR 서비스)에서 개체를 삭제하면 감사 메시지가 생성되고 감사 로그에 저장됩니다.

> 삭제 트랜잭션 중에 생성된 모든 감사 메시지가 아래 예제에 나와 있지 않습니다. S3 삭제 트랜잭션(SDEL)과 관련된 항목만 나열됩니다.

SDEL:S3 삭제

클라이언트가 LDR 서비스에 개체 삭제 요청을 보내면 개체 삭제가 시작됩니다. 메시지에는 오브젝트를 삭제할 버킷과 오브젝트를 식별하는 데 사용되는 오브젝트의 S3 키가 포함됩니다.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

객체 검색 트랜잭션입니다

API 관련(S3 및 Swift) 감사 메시지를 찾아 감사 로그에서 오브젝트 검색 트랜잭션을 식별할 수 있습니다.

다음 표에는 검색 트랜잭션 중에 생성된 모든 감사 메시지가 나와 있지 않습니다. 조회 트랜잭션을 추적하는 데 필요한 메시지만 포함됩니다.

S3 검색 감사 메시지

코드	이름	설명	트레이스	을 참조하십시오
SGET	S3 가져오기	버킷에서 오브젝트를 검색하도록 요청했습니다.	CBID, S3BK, S3KY	SGET: S3 GET

SWIFT 검색 감사 메시지

코드	이름	설명	트레이스	을 참조하십시오
윙입니다	신속한 지원	컨테이너에서 개체를 검색하도록 요청했습니다.	CBID, WCON, WOBJ	wget: Swift get

예: **S3** 오브젝트 검색

S3 클라이언트가 스토리지 노드(LDR 서비스)에서 오브젝트를 검색할 때 감사 메시지가 생성되고 감사 로그에 저장됩니다.

아래 예에서는 트랜잭션 중에 생성된 모든 감사 메시지가 나열되지 않습니다. S3 검색 트랜잭션(SGET)과 관련된 항목만 나열됩니다.

SGET: S3 GET

클라이언트가 LDR 서비스에 Get Object 요청을 보내면 개체 검색이 시작됩니다. 메시지에는 오브젝트를 검색할 버킷과 오브젝트를 식별하는 데 사용되는 오브젝트의 S3 키를 포함합니다.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

버킷 정책이 허용하는 경우 클라이언트는 익명으로 오브젝트를 검색하거나 다른 테넌트 계정이 소유한 버킷에서 오브젝트를 검색할 수 있습니다. 감사 메시지에는 이러한 익명 및 교차 계정 요청을 추적할 수 있도록 버킷 소유자의 테넌트 계정에 대한 정보가 포함되어 있습니다.

다음 예제 메시지에서 클라이언트는 소유하지 않은 버킷에 저장된 객체에 대한 객체 가져오기 요청을 보냅니다. SBAI 및 SBAC의 값은 버킷 소유자의 테넌트 계정 ID 및 이름을 기록합니다. 이 ID는 S3AI 및 SACC에 기록된 클라이언트의 테넌트 계정 ID 및 이름과 다릅니다.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

예: **S3** 오브젝트에서 선택합니다

S3 클라이언트가 개체에서 S3 Select 쿼리를 실행하면 감사 메시지가 생성되고 감사 로그에

저장됩니다.

아래 예에서는 트랜잭션 중에 생성된 모든 감사 메시지가 나열되지 않습니다. S3 선택 트랜잭션 (SelectObjectContent)과 관련된 항목만 나열됩니다.

각 쿼리는 S3 선택 요청의 승인(S3SR 필드는 "선택"으로 설정됨)을 수행하는 감사 메시지와 처리 중에 스토리지에서 데이터를 검색하는 후속 표준 가져오기 작업을 수행하는 두 개의 감사 메시지를 생성합니다.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

메타데이터 업데이트 메시지

감사 메시지는 S3 클라이언트가 오브젝트의 메타데이터를 업데이트할 때 생성됩니다.

S3 메타데이터 업데이트 감사 메시지

코드	이름	설명	트레이스	을 참조하십시오
SUPD	S3 메타데이터가 업데이트되었습니다	S3 클라이언트가 수집된 개체의 메타데이터를 업데이트할 때 생성됩니다.	CBID, S3KY, HTRH	SUPD:S3 메타데이터가 업데이트되었습니다

예: **S3** 메타데이터 업데이트

이 예에서는 기존 S3 오브젝트의 메타데이터를 업데이트하는 성공적인 트랜잭션을 보여 줍니다.

SUPD:S3 메타데이터 업데이트

S3 클라이언트는 S3 오브젝트(S3KY)에 대해 지정된 메타데이터('x-amz-meta-\ *')를 업데이트하도록 SUPD(Request)를 생성합니다. 이 예제에서는 요청 헤더가 감사 프로토콜 헤더로 구성되었으므로 HTRH 필드에 요청 헤더가 포함되어 있습니다(구성 > 모니터링 > 감사 및 **syslog** 서버).

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

관련 정보

감사 메시지 및 로그 대상을 구성합니다

감사 메시지

시스템에서 반환된 감사 메시지에 대한 자세한 설명은 다음 섹션에 나와 있습니다. 각 감사 메시지는 먼저 메시지가 나타내는 활동 클래스별로 관련 메시지를 그룹화하는 표에 나열됩니다.

이러한 그룹화는 감사되는 활동의 유형을 이해하고 원하는 유형의 감사 메시지 필터링을 선택하는 데 유용합니다.

감사 메시지는 4자리 코드별로 알파벳순으로 나열됩니다. 이 알파벳 목록을 사용하면 특정 메시지에 대한 정보를 찾을 수 있습니다.

이 장 전체에서 사용되는 4자 코드는 다음 샘플 메시지에 표시된 감사 메시지에 있는 ATYP 값입니다.

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

감사 메시지 수준 설정, 로그 대상 변경 및 감사 정보에 대한 외부 syslog 서버 사용에 대한 자세한 내용은 을 참조하십시오 감사 메시지 및 로그 대상을 구성합니다

감사 메시지 범주

감사 메시지가 그룹화되는 다양한 범주를 숙지해야 합니다. 이러한 그룹은 메시지가 나타내는 활동 클래스에 따라 구성됩니다.

시스템 감사 메시지

시스템 감사 범주에 속하는 감사 메시지에 익숙해야 합니다. 이러한 이벤트는 감사 시스템 자체, 그리드 노드 상태, 시스템 전체 작업(그리드 작업) 및 서비스 백업 작업과 관련된 이벤트로, 잠재적인 문제를 해결할 수 있습니다.

코드	메시지 제목 및 설명입니다	을 참조하십시오
ECMC	누락된 삭제 코딩 데이터 조각: 누락된 삭제 코딩 데이터 조각이 감지되었음을 나타냅니다.	ECMC: 삭제 코딩 데이터 조각이 없습니다
ECOC	손상된 삭제 코딩 데이터 조각: 손상된 삭제 코딩 데이터 조각이 감지되었음을 나타냅니다.	ECOC: 손상된 삭제 코딩 데이터 조각
ETAF	보안 인증 실패: 전송 계층 보안(TLS)을 사용한 연결 시도가 실패했습니다.	ETAF: 보안 인증 실패
GNRG	GNDS 등록: StorageGRID 시스템에서 자체적으로 갱신되거나 등록된 서비스.	GNRG: GNDS 등록

코드	메시지 제목 및 설명입니다	을 참조하십시오
GNUR	GNDS 등록 취소: StorageGRID 시스템에서 서비스 등록이 취소되었습니다.	GNUR:GNDS 등록 취소
GTED	그리드 작업 종료: CMN 서비스가 그리드 작업 처리를 완료했습니다.	GTED: 그리드 작업이 종료되었습니다
GTSt	그리드 작업 시작됨: CMN 서비스가 그리드 작업 처리를 시작했습니다.	GTSt: 그리드 작업이 시작되었습니다
GTSU	Grid Task Submitted(그리드 작업 제출됨): CMN 서비스로 GRID 작업이 제출되었습니다.	GTSU: 그리드 작업 제출됨
IDEL	ILM 시작 삭제: ILM이 개체 삭제 프로세스를 시작할 때 이 감사 메시지가 생성됩니다.	IDEL: ILM 삭제 시작
LKCU	덮어쓴 개체 정리. 이 감사 메시지는 덮어쓴 개체를 자동으로 제거하여 저장 공간을 확보할 때 생성됩니다.	LKCU: 덮어쓴 개체 정리
LLST	위치 손실: 이 감사 메시지는 위치가 손실될 때 생성됩니다.	LLST: 위치가 손실되었습니다
OLST	개체 손실: 요청된 개체를 StorageGRID 시스템 내에 찾을 수 없습니다.	OLST: 시스템에서 손실된 개체를 감지했습니다
ORLM	개체 규칙 충족: ILM 규칙에 지정된 대로 개체 데이터가 저장됩니다.	ORLM: 개체 규칙이 충족되었습니다
추가	보안 감사 비활성화: 감사 메시지 로깅이 꺼졌습니다.	추가: 보안 감사 비활성화
사드	보안 감사 활성화: 감사 메시지 로깅이 복원되었습니다.	Sade: 보안 감사 활성화
SVRF	오브젝트 저장소 확인 실패: 콘텐츠 블록이 확인 검사에 실패했습니다.	SVRF: Object Store Verify Fail(SVRF: 오브젝트 저장소 확인 실패)
SVRU	오브젝트 저장소 알 수 없음 확인: 오브젝트 저장소에서 예기치 않은 오브젝트 데이터가 감지되었습니다.	SVRU: Object Store Verify Unknown

코드	메시지 제목 및 설명입니다	을 참조하십시오
시스템	노드 중지: 종료가 요청되었습니다.	SYSD:노드 중지
시스템	노드 중지: 서비스가 정상 중지를 시작했습니다.	시스템:노드 중지 중
시스템	노드 시작: 서비스가 시작되었고 이전 종료의 특성이 메시지에 표시됩니다.	SYSU: 노드 시작
VLST	사용자가 시작한 볼륨 손실: '/proc/cMSI/Volume_lost' 명령이 실행되었습니다.	VLST: 사용자가 시작한 볼륨이 손실되었습니다

관련 정보

LKCU: 덮어쓴 개체 정리

오브젝트 스토리지 감사 메시지

따라서 오브젝트 스토리지 감사 범주에 속하는 감사 메시지를 잘 알고 있어야 합니다. 이러한 이벤트는 StorageGRID 시스템 내에서 개체의 스토리지 및 관리와 관련된 이벤트입니다. 여기에는 오브젝트 스토리지 및 검색, 그리드 노드에서 그리드 노드 전송, 검증도 포함됩니다.

코드	설명	을 참조하십시오
APCT	클라우드 계층에서 아카이브 제거: 아카이브된 오브젝트 데이터는 S3 API를 통해 StorageGRID에 연결되는 외부 아카이브 스토리지 시스템에서 삭제됩니다.	APCT: 클라우드-계층에서 아카이브 제거
ARCB	아카이브 오브젝트 검색 시작: ARC 서비스는 외부 아카이브 스토리지 시스템에서 오브젝트 데이터 검색을 시작합니다.	ARCB: 아카이브 객체 검색이 시작됩니다
ARCE	Archive Object Retrieve End(아카이브 객체 검색 종료): 외부 아카이브 스토리지 시스템에서 객체 데이터를 검색했으며 ARC 서비스가 검색 작업의 상태를 보고합니다.	ARCE: 아카이브 객체 검색 종료
ARCT	클라우드 계층에서 아카이브 검색: S3 API를 통해 StorageGRID에 연결되는 외부 아카이브 스토리지 시스템에서 아카이빙된 오브젝트 데이터를 검색합니다.	ARCT: 클라우드 계층에서 아카이브 검색

코드	설명	을 참조하십시오
합니다	아카이브 객체 제거: 외부 아카이브 스토리지 시스템에서 콘텐츠 블록이 성공적으로 삭제되었거나 삭제되지 않았습니다.	AREM: 아카이브 객체 제거
ASCE	Archive Object Store End(아카이브 오브젝트 저장소 종료): 컨텐츠 블록이 외부 아카이브 스토리지 시스템에 기록되고 ARC 서비스가 쓰기 작업의 상태를 보고합니다.	ASCE: 아카이브 객체 저장소 종료
ASCT	Archive Store Cloud-Tier: 오브젝트 데이터는 S3 API를 통해 StorageGRID에 연결되는 외부 아카이브 스토리지 시스템에 저장됩니다.	ASCT: Archive Store Cloud - Tier(아카이브 저장소 클라우드 - 계층)
ATCHE	아카이브 오브젝트 저장소 시작: 외부 아카이브 스토리지에 콘텐츠 블록 쓰기가 시작되었습니다.	ATCHE: 아카이브 오브젝트 저장소가 시작됩니다
AVCC	Archive Validate Cloud-Tier Configuration: 제공된 계정 및 버킷 설정이 성공적으로 검증되었는지 또는 확인되지 않았습니다.	AVCC: Archive Validate Cloud-Tier Configuration
카운터보어	Object Send End(개체 보내기 종료): 소스 엔터티가 그리드 노드 간 데이터 전송 작업을 완료했습니다.	CBSE: 객체 보내기 종료
CBRE	오브젝트 수신 종료: 대상 엔터티가 그리드 노드에서 그리드 노드 데이터 전송 작업을 완료했습니다.	CBRE: 객체 수신 종료
SCMT	오브젝트 저장소 커밋: 콘텐츠 블록이 완전히 저장되고 확인되었으므로 이제 요청할 수 있습니다.	SCMT: 오브젝트 저장소 커밋
SREM	오브젝트 저장소 제거: 콘텐츠 블록이 그리드 노드에서 삭제되었으며 더 이상 직접 요청할 수 없습니다.	SREM: 오브젝트 저장소 제거

클라이언트가 감사 메시지를 읽습니다

클라이언트 읽기 감사 메시지는 S3 또는 Swift 클라이언트 애플리케이션이 오브젝트 검색을 요청할 때 기록됩니다.

코드	설명	사용자	을 참조하십시오
SGET	S3 GET: 성공적인 트랜잭션을 로그하여 객체를 검색하거나 버킷의 오브젝트를 나열합니다. • 참고: * 트랜잭션이 하위 리소스에서 작동하는 경우 감사 메시지에는 S3SR 필드가 포함됩니다.	S3 클라이언트	SGET: S3 GET
셰어	S3 HEAD: 성공한 트랜잭션을 로그하여 오브젝트 또는 버킷의 존재 여부를 확인합니다.	S3 클라이언트	Shea: S3 헤드
윙입니다	SwiFT GET: 성공한 트랜잭션을 로그하여 객체를 검색하거나 컨테이너의 객체를 나열합니다.	SWIFT 클라이언트	wget: Swift get
WHEA	SwiFT HEAD: 성공한 트랜잭션을 로그하여 오브젝트 또는 컨테이너의 존재를 확인합니다.	SWIFT 클라이언트	WHEA: 스위프트 헤드

클라이언트가 감사 메시지를 기록합니다

S3 또는 Swift 클라이언트 애플리케이션이 오브젝트 생성 또는 수정을 요청할 때 클라이언트 쓰기 감사 메시지가 기록됩니다.

코드	설명	사용자	을 참조하십시오
OVWR	오브젝트 덮어쓰기: 트랜잭션을 로그하여 한 오브젝트를 다른 오브젝트로 덮어씁니다.	S3 클라이언트 SWIFT 클라이언트	OVWR: 개체 덮어쓰기

코드	설명	사용자	을 참조하십시오
SDEL	S3 삭제: 오브젝트 또는 버킷을 삭제하기 위해 트랜잭션을 성공적으로 기록합니다. • 참고: * 트랜잭션이 하위 리소스에서 작동하는 경우 감사 메시지에는 S3SR 필드가 포함됩니다.	S3 클라이언트	SDEL: S3 삭제
Spos	S3 POST: 성공적인 트랜잭션을 로그하여 AWS Glacier 스토리지에서 클라우드 스토리지 풀로 오브젝트를 복원합니다.	S3 클라이언트	Spos: S3 POST
SPUT	S3 PUT: 새 오브젝트 또는 버킷을 생성하기 위한 성공적인 트랜잭션을 기록합니다. • 참고: * 트랜잭션이 하위 리소스에서 작동하는 경우 감사 메시지에는 S3SR 필드가 포함됩니다.	S3 클라이언트	SPUT: S3 PUT
SUPD	S3 메타데이터 업데이트됨: 트랜잭션이 성공하여 기존 오브젝트 또는 버킷의 메타데이터를 업데이트합니다.	S3 클라이언트	SUPD:S3 메타데이터가 업데이트되었습니다
WDEL	SwiFT DELETE(빠른 삭제): 성공한 트랜잭션을 로그하여 오브젝트 또는 컨테이너를 삭제합니다.	SWIFT 클라이언트	WDEL: Swift 삭제
WPUT	SwiFT PUT: 새 개체 또는 컨테이너를 생성하기 위해 트랜잭션을 성공적으로 기록합니다.	SWIFT 클라이언트	WPUT: Swift Put

관리 감사 메시지입니다

관리 범주는 사용자 요청을 관리 API에 기록합니다.

코드	메시지 제목 및 설명입니다	을 참조하십시오
MGAU	관리 API 감사 메시지: 사용자 요청 로그입니다.	MGAU: 관리 감사 메시지

감사 메시지 참조

APCT: 클라우드-계층에서 아카이브 제거

이 메시지는 S3 API를 통해 StorageGRID에 연결되는 외부 아카이브 스토리지 시스템에서 아카이빙된 오브젝트 데이터를 삭제할 때 생성됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 ID입니다	삭제된 콘텐츠 블록의 고유 식별자입니다.
CSRZ	콘텐츠 크기	오브젝트의 크기(바이트)입니다. 항상 0을 반환합니다.
RSLT	결과 코드	성공(SUCS) 또는 백엔드에서 보고된 오류를 반환합니다.
SUID	스토리지 고유 식별자입니다	객체가 삭제된 클라우드 계층의 고유 식별자(UUID)입니다.

ARCB: 아카이브 객체 검색이 시작됩니다

이 메시지는 보관된 오브젝트 데이터 검색을 요청하고 검색 프로세스가 시작될 때 생성됩니다. 검색 요청은 즉시 처리되지만, 테이프와 같은 선형 미디어의 검색 효율성을 높이기 위해 재주문할 수 있습니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 ID입니다	외부 아카이브 스토리지 시스템에서 검색할 컨텐츠 블록의 고유 식별자입니다.
RSLT	결과	아카이브 검색 프로세스를 시작한 결과를 나타냅니다. 현재 정의된 값은 다음과 같습니다. SUCS: 콘텐츠 요청이 수신되어 검색 대기 중입니다.

이 감사 메시지는 아카이브 검색 시간을 표시합니다. 메시지를 해당 ARCE 종료 메시지와 일치하여 아카이브 검색 기간 및 작업 성공 여부를 결정할 수 있습니다.

ARCE: 아카이브 객체 검색 종료

이 메시지는 아카이브 노드가 외부 아카이브 스토리지 시스템에서 객체 데이터를 검색하려고 시도할 때 생성됩니다. 성공하면 요청된 개체 데이터가 아카이브 위치에서 완전히 읽혀져 성공적으로 확인되었음을 나타내는 메시지가 표시됩니다. 객체 데이터를 검색하여 확인한 후 요청 서비스로 전달합니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 ID입니다	외부 아카이브 스토리지 시스템에서 검색할 컨텐츠 블록의 고유 식별자입니다.
VLID	볼륨 식별자	데이터가 아카이빙된 볼륨의 식별자입니다. 콘텐츠의 아카이브 위치를 찾을 수 없으면 볼륨 ID가 0으로 반환됩니다.
RSLT	검색 결과	아카이브 검색 프로세스의 완료 상태: • SUCS: 성공했습니다 • VRFL: 실패(개체 검증 실패) • Arun: failed(실패)(외부 아카이브 스토리지 시스템을 사용할 수 없음) • CANC:실패(검색 작업 취소됨) • GERR: 실패(일반 오류)

이 메시지를 해당 ARCB 메시지와 일치시키는 것은 아카이브 검색을 수행하는 데 걸리는 시간을 나타낼 수 있습니다. 이 메시지는 검색이 성공했는지 여부를 나타내며, 오류가 발생한 경우 콘텐츠 블록 검색에 실패한 원인을 나타냅니다.

ARCT: 클라우드 계층에서 아카이브 검색

이 메시지는 S3 API를 통해 StorageGRID에 연결되는 외부 아카이브 스토리지 시스템에서 아카이빙된 오브젝트 데이터를 검색할 때 생성됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 ID입니다	검색된 콘텐츠 블록의 고유 식별자입니다.
CSRZ	콘텐츠 크기	오브젝트의 크기(바이트)입니다. 이 값은 성공적인 검색 시에만 정확합니다.

코드	필드에 입력합니다	설명
RSLT	결과 코드	성공(SUCS) 또는 백엔드에서 보고된 오류를 반환합니다.
SUID	스토리지 고유 식별자입니다	외부 아카이브 스토리지 시스템의 UUID(Unique Identifier)입니다.
시간	시간	요청의 총 처리 시간(마이크로초)입니다.

AREM: 아카이브 객체 제거

아카이브 객체 제거 감사 메시지는 컨텐츠 블록이 아카이브 노드에서 성공적으로 삭제되었거나 삭제되지 않았음을 나타냅니다. 결과가 성공적이면 아카이브 노드가 외부 아카이브 스토리지 시스템에 StorageGRID가 객체 위치를 해제했음을 알렸습니다. 객체가 외부 아카이브 스토리지 시스템에서 제거되었는지 여부는 시스템 유형과 해당 구성에 따라 달라집니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 ID입니다	외부 아카이브 미디어 시스템에서 검색할 컨텐츠 블록의 고유 식별자입니다.
VLID	볼륨 식별자	오브젝트 데이터가 아카이빙된 볼륨의 식별자입니다.
RSLT	결과	아카이브 제거 프로세스의 완료 상태: • SUCS: 성공했습니다 • Arun: failed(실패)(외부 아카이브 스토리지 시스템을 사용할 수 없음) • GERR: 실패(일반 오류)

ASCE: 아카이브 객체 저장소 종료

이 메시지는 외부 아카이브 스토리지 시스템에 콘텐츠 블록을 쓰는 작업이 종료되었음을 나타냅니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	외부 아카이브 스토리지 시스템에 저장된 콘텐츠 블록의 식별자입니다.

코드	필드에 입력합니다	설명
VLID	볼륨 식별자	객체 데이터가 기록되는 아카이브 볼륨의 고유 식별자입니다.
VREN	확인 활성화	컨텐츠 블록 검증 수행 여부를 나타낸다. 현재 정의된 값은 다음과 같습니다. • vena: 확인이 활성화되었습니다 • VDSA: 확인이 비활성화되었습니다
MCLS	관리 클래스	해당되는 경우 컨텐츠 블록이 할당되는 TSM 관리 클래스를 식별하는 문자열입니다.
RSLT	결과	아카이브 프로세스의 결과를 나타냅니다. 현재 정의된 값은 다음과 같습니다. • SUCS: 성공(아카이브 프로세스 성공) • OFFL: failed(보관 오프라인) • VRFL: 실패(객체 확인 실패) • Arun: failed(실패)(외부 아카이브 스토리지 시스템을 사용할 수 없음) • GERR: 실패(일반 오류)

이 감사 메시지는 지정된 콘텐츠 블록이 외부 아카이브 스토리지 시스템에 기록되었음을 의미합니다. 쓰기에 실패하면 장애 발생 위치에 대한 기본적인 문제 해결 정보를 제공합니다. 아카이브 실패에 대한 자세한 내용은 StorageGRID 시스템에서 아카이브 노드 속성을 검토하여 확인할 수 있습니다.

ASCT: Archive Store Cloud - Tier(아카이브 저장소 클라우드 **- 계층)**

이 메시지는 아카이브 오브젝트 데이터가 S3 API를 통해 StorageGRID에 연결되는 외부 아카이브 스토리지 시스템에 저장될 때 생성됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 ID입니다	검색된 콘텐츠 블록의 고유 식별자입니다.
CSRZ	콘텐츠 크기	오브젝트의 크기(바이트)입니다.

코드	필드에 입력합니다	설명
RSLT	결과 코드	성공(SUCS) 또는 백엔드에서 보고된 오류를 반환합니다.
SUID	스토리지 고유 식별자입니다	콘텐츠가 저장된 클라우드 계층의 UUID(Unique Identifier)입니다.
시간	시간	요청의 총 처리 시간(마이크로초)입니다.

ATCHE: 아카이브 오브젝트 저장소가 시작됩니다

이 메시지는 외부 아카이브 스토리지에 콘텐츠 블록을 쓰는 작업이 시작되었음을 나타냅니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 ID입니다	아카이빙할 컨텐츠 블록의 고유 식별자입니다.
VLID	볼륨 식별자	컨텐츠 블록이 기록되는 볼륨의 고유 식별자입니다. 작업이 실패하면 0의 볼륨 ID가 반환됩니다.
RSLT	결과	콘텐츠 블록의 전송 결과를 나타냅니다. 현재 정의된 값은 다음과 같습니다. • SUCS: 성공(콘텐츠 블록이 성공적으로 저장됨) • exis: ignored(콘텐츠 블록이 이미 저장됨) • ISFD: 실패(디스크 공간 부족) • ster:failed(CBID를 저장하는 동안 오류가 발생했습니다.) • OFFL: failed(보관 오프라인) • GERR: 실패(일반 오류)

AVCC: Archive Validate Cloud-Tier Configuration

이 메시지는 Cloud Tiering - S3(Simple Storage Service) 타겟 유형에 대해 구성 설정이 검증될 때 생성됩니다.

코드	필드에 입력합니다	설명
RSLT	결과 코드	성공(SUCS) 또는 백엔드에서 보고된 오류를 반환합니다.
SUID	스토리지 고유 식별자입니다	유효성을 검사할 외부 아카이브 스토리지 시스템과 연결된 UUID입니다.

CBRB: 객체 수신 시작

정상적인 시스템 작업 중에 데이터 액세스, 복제 및 보존에 따라 컨텐츠 블록이 서로 다른 노드 간에 지속적으로 전송됩니다. 한 노드에서 다른 노드로 콘텐츠 블록 전송이 시작되면 대상 엔터티가 이 메시지를 발행합니다.

코드	필드에 입력합니다	설명
CNID	연결 식별자	노드 간 세션/연결의 고유 식별자입니다.
CBID	콘텐츠 블록 식별자	전송 중인 컨텐츠 블록의 고유 식별자입니다.
CTDR	전송 방향	CBID 전송이 푸시 시작 또는 풀 초기화되었는지 여부를 나타냅니다. PUSH: 전송 작업이 전송 엔티티에 의해 요청되었습니다. Pull(풀): 수신 엔티티가 전송 작업을 요청했습니다.
CTSR	원본 요소	CBID 전송 소스(보낸 사람)의 노드 ID입니다.
CTDS	대상 요소	CBID 전송 대상(수신기)의 노드 ID입니다.
CTSS	시작 시퀀스 수	요청된 첫 번째 시퀀스 수를 나타냅니다. 성공한 경우 이 시퀀스 개수로 전송이 시작됩니다.
CTES	예상 종료 시퀀스 수입니다	요청된 마지막 시퀀스 수를 나타냅니다. 성공한 경우 이 시퀀스 카운트가 수신되면 전송이 완료된 것으로 간주됩니다.

코드	필드에 입력합니다	설명
RSLT	전송 시작 상태	전송이 시작된 시점의 상태: SUCS: 전송이 시작되었습니다.

이 감사 메시지는 컨텐츠 블록 식별자로 식별되는 단일 컨텐츠 부분에 대해 노드 간 데이터 전송 작업이 시작되었음을 의미합니다. 작업이 "시작 시퀀스 수"에서 "예상 종료 시퀀스 수"로 데이터를 요청합니다. 송신 및 수신 노드는 해당 노드 ID로 식별됩니다. 이 정보를 사용하여 시스템 데이터 흐름을 추적하고 스토리지 감사 메시지와 결합할 경우 복제본 수를 확인할 수 있습니다.

CBRE: 객체 수신 종료

한 노드에서 다른 노드로 콘텐츠 블록 전송이 완료되면 대상 엔터티가 이 메시지를 발행합니다.

코드	필드에 입력합니다	설명
CNID	연결 식별자	노드 간 세션/연결의 고유 식별자입니다.
CBID	콘텐츠 블록 식별자	전송 중인 컨텐츠 블록의 고유 식별자입니다.
CTDR	전송 방향	CBID 전송이 푸시 시작 또는 풀 초기화되었는지 여부를 나타냅니다. PUSH: 전송 작업이 전송 엔티티에 의해 요청되었습니다. Pull(풀): 수신 엔티티가 전송 작업을 요청했습니다.
CTSR	원본 요소	CBID 전송 소스(보낸 사람)의 노드 ID입니다.
CTDS	대상 요소	CBID 전송 대상(수신기)의 노드 ID입니다.
CTSS	시작 시퀀스 수	전송이 시작된 시퀀스 수를 나타냅니다.
CTAS	실제 종료 시퀀스 수입니다	성공적으로 전송된 마지막 시퀀스 수를 나타냅니다. 실제 End Sequence Count가 Start Sequence Count와 동일하고 Transfer Result가 성공하지 못한 경우 데이터가 교환되지 않았습니다.

코드	필드에 입력합니다	설명
RSLT	전송 결과	전송 작업의 결과(전송 요소의 관점에서): SUCS: 전송이 완료되었습니다. 요청된 모든 시퀀스 수가 전송되었습니다. CONL: 전송 중에 연결이 끊어졌습니다 CTMO: 설정 또는 전송 중 연결 시간이 초과되었습니다 UNRE: 대상 노드 ID에 연결할 수 없습니다 CRPT: 손상되거나 잘못된 데이터가 수신되어 전송이 종료됨(변조를 나타낼 수 있음)

이 감사 메시지는 노드 간 데이터 전송 작업이 완료되었음을 의미합니다. 전송 결과가 성공적이면 작업이 "시작 시퀀스 수"에서 "실제 종료 시퀀스 수"로 데이터를 전송합니다. 송신 및 수신 노드는 해당 노드 ID로 식별됩니다. 이 정보는 시스템 데이터 흐름을 추적하고 오류를 찾고, 도표하고, 분석하는 데 사용할 수 있습니다. 스토리지 감사 메시지와 함께 사용할 경우 복제본 수를 확인하는 데도 사용할 수 있습니다.

CBSB: 개체 보내기 시작

정상적인 시스템 작업 중에 데이터 액세스, 복제 및 보존에 따라 컨텐츠 블록이 서로 다른 노드 간에 지속적으로 전송됩니다. 한 노드에서 다른 노드로 콘텐츠 블록 전송이 시작되면 이 메시지는 소스 엔터티가 발행합니다.

코드	필드에 입력합니다	설명
CNID	연결 식별자	노드 간 세션/연결의 고유 식별자입니다.
CBID	콘텐츠 블록 식별자	전송 중인 컨텐츠 블록의 고유 식별자입니다.
CTDR	전송 방향	CBID 전송이 푸시 시작 또는 풀 초기화되었는지 여부를 나타냅니다. PUSH: 전송 작업이 전송 엔티티에 의해 요청되었습니다. Pull(풀): 수신 엔티티가 전송 작업을 요청했습니다.

코드	필드에 입력합니다	설명
CTSR	원본 요소	CBID 전송 소스(보낸 사람)의 노드 ID입니다.
CTDS	대상 요소	CBID 전송 대상(수신기)의 노드 ID입니다.
CTSS	시작 시퀀스 수	요청된 첫 번째 시퀀스 수를 나타냅니다. 성공한 경우 이 시퀀스 개수로 전송이 시작됩니다.
CTES	예상 종료 시퀀스 수입니다	요청된 마지막 시퀀스 수를 나타냅니다. 성공한 경우 이 시퀀스 카운트가 수신되면 전송이 완료된 것으로 간주됩니다.
RSLT	전송 시작 상태	전송이 시작된 시점의 상태: SUCS: 전송이 시작되었습니다.

이 감사 메시지는 컨텐츠 블록 식별자로 식별되는 단일 컨텐츠 부분에 대해 노드 간 데이터 전송 작업이 시작되었음을 의미합니다. 작업이 "시작 시퀀스 수"에서 "예상 종료 시퀀스 수"로 데이터를 요청합니다. 송신 및 수신 노드는 해당 노드 ID로 식별됩니다. 이 정보를 사용하여 시스템 데이터 흐름을 추적하고 스토리지 감사 메시지와 결합할 경우 복제본 수를 확인할 수 있습니다.

CBSE: 객체 보내기 종료

한 노드에서 다른 노드로 콘텐츠 블록 전송이 완료되면 소스 엔터티가 이 메시지를 발행합니다.

코드	필드에 입력합니다	설명
CNID	연결 식별자	노드 간 세션/연결의 고유 식별자입니다.
CBID	콘텐츠 블록 식별자	전송 중인 컨텐츠 블록의 고유 식별자입니다.
CTDR	전송 방향	CBID 전송이 푸시 시작 또는 풀 초기화되었는지 여부를 나타냅니다. PUSH: 전송 작업이 전송 엔티티에 의해 요청되었습니다. Pull(풀): 수신 엔티티가 전송 작업을 요청했습니다.

코드	필드에 입력합니다	설명
CTSR	원본 요소	CBID 전송 소스(보낸 사람)의 노드 ID입니다.
CTDS	대상 요소	CBID 전송 대상(수신기)의 노드 ID입니다.
CTSS	시작 시퀀스 수	전송이 시작된 시퀀스 수를 나타냅니다.
CTAS	실제 종료 시퀀스 수입니다	성공적으로 전송된 마지막 시퀀스 수를 나타냅니다. 실제 End Sequence Count가 Start Sequence Count와 동일하고 Transfer Result가 성공하지 못한 경우 데이터가 교환되지 않았습니다.
RSLT	전송 결과	전송 작업의 결과(전송 요소의 관점에서): SUCS: 전송이 성공적으로 완료되었습니다. 요청된 모든 시퀀스 수가 전송되었습니다. CONL: 전송 중에 연결이 끊어졌습니다 CTMO: 설정 또는 전송 중 연결 시간이 초과되었습니다 UNRE: 대상 노드 ID에 연결할 수 없습니다 CRPT: 손상되거나 잘못된 데이터가 수신되어 전송이 종료됨(변조를 나타낼 수 있음)

이 감사 메시지는 노드 간 데이터 전송 작업이 완료되었음을 의미합니다. 전송 결과가 성공적이면 작업이 "시작 시퀀스 수"에서 "실제 종료 시퀀스 수"로 데이터를 전송합니다. 송신 및 수신 노드는 해당 노드 ID로 식별됩니다. 이 정보는 시스템 데이터 흐름을 추적하고 오류를 찾고, 도표하고, 분석하는 데 사용할 수 있습니다. 스토리지 감사 메시지와 함께 사용할 경우 복제본 수를 확인하는 데도 사용할 수 있습니다.

ECMC: 삭제 코딩 데이터 조각이 없습니다

이 감사 메시지는 시스템에서 누락된 삭제 코딩 데이터 조각을 감지했음을 나타냅니다.

코드	필드에 입력합니다	설명
VCMC	VCS ID입니다	누락된 청크가 포함된 VCS의 이름입니다.
MCID	청크 ID입니다	누락된 삭제 코딩 조각의 식별자입니다.
RSLT	결과	이 필드에는 '없음' 값이 있습니다. RSLT는 필수 메시지 필드이지만 이 특정 메시지와 관련이 없습니다. 이 메시지가 필터링되지 않도록 'UCS' 대신 '없음'이 사용됩니다.

ECOC: 손상된 삭제 코딩 데이터 조각

이 감사 메시지는 시스템에서 손상된 삭제 코딩 데이터 조각을 감지했음을 나타냅니다.

코드	필드에 입력합니다	설명
VCCO	VCS ID입니다	손상된 청크가 포함된 VCS의 이름입니다.
VLID	볼륨 ID입니다	손상된 삭제 코딩 조각이 포함된 RangeDB 볼륨.
CCID	청크 ID입니다	손상된 삭제 코딩 조각의 식별자입니다.
RSLT	결과	이 필드에는 '없음' 값이 있습니다. RSLT는 필수 메시지 필드이지만 이 특정 메시지와 관련이 없습니다. 이 메시지가 필터링되지 않도록 'UCS' 대신 '없음'이 사용됩니다.

ETAF: 보안 인증 실패

이 메시지는 TLS(Transport Layer Security)를 사용한 연결 시도가 실패한 경우에 생성됩니다.

코드	필드에 입력합니다	설명
CNID	연결 식별자	인증에 실패한 TCP/IP 연결의 고유한 시스템 식별자입니다.
RUID	사용자 ID	원격 사용자의 ID를 나타내는 서비스 종속 식별자입니다.

코드	필드에 입력합니다	설명
RSLT	사유 코드	실패 이유: SCNI: 보안 연결 설정에 실패했습니다. CERM: 인증서가 누락되었습니다. 인증서: 인증서가 유효하지 않습니다. CERE: 인증서가 만료되었습니다. CERR: 인증서가 해지되었습니다. CSGN: 인증서 서명이 유효하지 않습니다. CSGU: 인증서 서명자를 알 수 없습니다. UCRM: 사용자 자격 증명이 누락되었습니다. UCRI: 사용자 자격 증명이 잘못되었습니다. UCRU: 사용자 자격 증명이 허용되지 않습니다. Tout: 인증 시간이 초과되었습니다.

TLS를 사용하는 보안 서비스에 연결이 설정되면 원격 엔터티의 자격 증명은 TLS 프로필과 서비스에 기본 제공되는 추가 로직을 사용하여 확인됩니다. 유효하지 않거나, 예기치 않거나, 허용되지 않는 인증서 또는 자격 증명으로 인해 이 인증에 실패하면 감사 메시지가 기록됩니다. 이렇게 하면 무단 액세스 시도 및 기타 보안 관련 연결 문제를 쿼리할 수 있습니다.

이 메시지는 원격 엔터티가 잘못된 구성을 가지거나 시스템에 유효하지 않거나 허용되지 않는 자격 증명을 제시하려고 할 때 발생할 수 있습니다. 시스템에 대한 무단 액세스 시도를 감지하기 위해 이 감사 메시지를 모니터링해야 합니다.

GNRG: GNDS 등록

CMN 서비스는 서비스가 StorageGRID 시스템에 자체 관련 정보를 업데이트하거나 등록할 때 이 감사 메시지를 생성합니다.

코드	필드에 입력합니다	설명
RSLT	결과	업데이트 요청의 결과: • SUCS: 성공했습니다 • SUNV: 서비스를 사용할 수 없습니다 • GERR: 기타 오류입니다
GNID입니다	노드 ID입니다	업데이트 요청을 시작한 서비스의 노드 ID입니다.
GNTP	장치 유형	그리드 노드의 디바이스 유형(예: LDR 서비스의 경우 BLDR)
GNDV	장치 모델 버전입니다	DMDL 번들에서 그리드 노드의 장치 모델 버전을 식별하는 문자열입니다.
GNGP	그룹	그리드 노드가 속한 그룹(링크 비용 및 서비스 쿼리 순위)
니아	IP 주소	그리드 노드의 IP 주소입니다.

이 메시지는 그리드 노드가 그리드 노드 번들의 해당 항목을 업데이트할 때마다 생성됩니다.

GNUR:GNDS 등록 취소

CMN 서비스는 StorageGRID 시스템에서 서비스에 대한 자체 정보가 등록되지 않은 경우 이 감사 메시지를 생성합니다.

코드	필드에 입력합니다	설명
RSLT	결과	업데이트 요청의 결과: • SUCS: 성공했습니다 • SUNV: 서비스를 사용할 수 없습니다 • GERR: 기타 오류입니다
GNID입니다	노드 ID입니다	업데이트 요청을 시작한 서비스의 노드 ID입니다.

GTED: 그리드 작업이 종료되었습니다

이 감사 메시지는 CMN 서비스가 지정된 그리드 작업 처리를 마치고 작업을 내역 테이블로 이동했음을 나타냅니다. 결과가 SUCS, ABRT 또는 Rolf인 경우 해당 Grid Task Started 감사

메시지가 표시됩니다. 다른 결과는 이 그리드 작업의 처리가 시작되지 않았음을 나타냅니다.

코드	필드에 입력합니다	설명
TSID	태스크 ID입니다	이 필드는 생성된 그리드 작업을 고유하게 식별하며 그리드 작업을 수명 주기 동안 관리할 수 있도록 합니다. • 참고: * 작업 ID는 그리드 작업이 생성될 때 할당되며, 전송 시간이 아닙니다. 지정된 그리드 작업을 여러 번 제출할 수 있으며, 이 경우 작업 ID 필드만으로는 제출됨, 시작됨 및 종료된 감사 메시지를 고유하게 연결할 수 없습니다.
RSLT	결과	그리드 작업의 최종 상태 결과: • SUCS: 그리드 작업이 성공적으로 완료되었습니다. • ABRT: 롤백 오류 없이 그리드 작업이 중단되었습니다. • Rolf: 그리드 작업이 중단되어 롤백 프로세스를 완료할 수 없습니다. • CANC: 그리드 작업을 시작하기 전에 사용자가 취소했습니다. • expr: 그리드 작업이 시작되기 전에 만료되었습니다. • IVLD: 그리드 작업이 잘못되었습니다. • 인증: 그리드 작업이 승인되지 않았습니다. • dupl: 그리드 작업이 중복으로 거부되었습니다.

GTSt: 그리드 작업이 시작되었습니다

이 감사 메시지는 CMN 서비스가 지정된 그리드 작업 처리를 시작했음을 나타냅니다. 감사 메시지는 내부 Grid Task Submission 서비스에서 시작하고 자동 활성화를 위해 선택된 그리드 작업에 대해 Grid Task Submitted 메시지 바로 다음에 표시됩니다. 보류 테이블에 제출된 그리드 작업의 경우 사용자가 그리드 작업을 시작할 때 이 메시지가 생성됩니다.

코드	필드에 입력합니다	설명
TSID	태스크 ID입니다	이 필드는 생성된 그리드 작업을 고유하게 식별하며 해당 수명 주기 동안 작업을 관리할 수 있도록 합니다. • 참고: * 작업 ID는 그리드 작업이 생성될 때 할당되며, 전송 시간이 아닙니다. 지정된 그리드 작업을 여러 번 제출할 수 있으며, 이 경우 작업 ID 필드만으로는 제출됨, 시작됨 및 종료된 감사 메시지를 고유하게 연결할 수 없습니다.
RSLT	결과	결과. 이 필드에는 하나의 값만 있습니다. • SUCS: 그리드 작업이 시작되었습니다.

GTSU: 그리드 작업 제출됨

이 감사 메시지는 그리드 작업이 CMN 서비스로 제출되었음을 나타냅니다.

코드	필드에 입력합니다	설명
TSID	태스크 ID입니다	생성된 그리드 작업을 고유하게 식별하고 해당 수명 주기 동안 작업을 관리할 수 있습니다. • 참고: * 작업 ID는 그리드 작업이 생성될 때 할당되며, 전송 시간이 아닙니다. 지정된 그리드 작업을 여러 번 제출할 수 있으며, 이 경우 작업 ID 필드만으로는 제출됨, 시작됨 및 종료된 감사 메시지를 고유하게 연결할 수 없습니다.
TTYP	태스크 유형	그리드 작업의 유형입니다.
버전	작업 버전	그리드 작업의 버전을 나타내는 숫자입니다.
TDSC	작업 설명	그리드 작업에 대한 사람이 읽을 수 있는 설명입니다.
귀리	타임스탬프 이후에 유효합니다	그리드 작업이 유효한 가장 빠른 시간(1970년 1월 1일부터 UNIX 시간으로 UInt64 마이크로초)입니다.

코드	필드에 입력합니다	설명
VBTS	타임스탬프 전에 유효합니다	그리드 작업이 유효한 최신 시간 (1970년 1월 1일 - UNIX 시간)입니다.
TsRC	출처	작업의 출처: • TXTB: 그리드 작업이 StorageGRID 시스템을 통해 서명된 텍스트 블록으로 제출되었습니다. • 그리드: 그리드 작업이 내부 그리드 작업 제출 서비스를 통해 제출되었습니다.
ACTV	활성화 유형	활성화 유형: • 자동: 그리드 작업이 자동 활성화를 위해 제출되었습니다. • PEND: 그리드 작업이 보류 중인 테이블에 제출되었습니다. TXTB 소스에 대한 유일한 가능성은 다음과 같은 것입니다.
RSLT	결과	제출 결과: • SUCS: 그리드 작업이 성공적으로 제출되었습니다. • 실패: 작업이 내역 테이블로 직접 이동되었습니다.

IDEL: ILM 삭제 시작

ILM이 개체 삭제 프로세스를 시작할 때 이 메시지가 생성됩니다.

IDEL 메시지는 다음 상황 중 하나에서 생성됩니다.

- * 규격 S3 버킷을 사용하는 오브젝트 *: ILM이 보존 기간이 만료되어(자동 삭제 설정이 활성화되고 법적 증거 자료 보관 기능이 꺼진 경우) 오브젝트를 자동 삭제하는 프로세스를 시작할 때 이 메시지가 생성됩니다.
- * 규정을 준수하지 않는 S3 버킷 또는 Swift 컨테이너 * 의 오브젝트 이 메시지는 ILM이 현재 개체에 적용되는 활성 ILM 정책의 배치 지침이 없으므로 개체 삭제 프로세스를 시작할 때 생성됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	객체의 CBID입니다.

코드	필드에 입력합니다	설명
CMPA	준수: 자동 삭제	규정 준수 S3 버킷에 있는 오브젝트에만 해당. 버킷을 법적 보관에 포함시키지 않는 한, 준수 객체가 보존 기간이 끝날 때 자동으로 삭제되어야 하는지 여부를 나타내는 0(false) 또는 1(true).
CMPL	규정 준수: 법적 증거 자료 보관	규정 준수 S3 버킷에 있는 오브젝트에만 해당. 버킷이 현재 법적 증거 자료 보관 중인지 여부를 나타내는 0(거짓) 또는 1(참)입니다.
CMPR	규정 준수: 보존 기간	규정 준수 S3 버킷에 있는 오브젝트에만 해당. 객체의 보존 기간(분)입니다.
CTME	규정 준수: 수집 시간	규정 준수 S3 버킷에 있는 오브젝트에만 해당. 개체의 수집 시간입니다. 이 값에 분 단위로 보존 기간을 추가하여 버킷에서 오브젝트를 삭제할 수 있는 시기를 결정할 수 있습니다.
DMRK	마커 버전 ID를 삭제합니다	버전이 있는 버킷에서 오브젝트를 삭제할 때 생성된 삭제 마커의 버전 ID입니다. 버킷의 작업에는 이 필드가 포함되지 않습니다.
CSRZ	콘텐츠 크기	오브젝트의 크기(바이트)입니다.
위치	위치	StorageGRID 시스템 내에서 오브젝트 데이터의 저장 위치입니다. 오브젝트에 위치가 없는 경우(예: 삭제된 경우) Locs 값은 ""입니다. CLEC: 삭제 코딩 오브젝트의 경우 삭제 코딩 프로필 ID와 오브젝트 데이터에 적용되는 삭제 코딩 그룹 ID입니다. CLDI: 복제된 개체의 경우 LDR 노드 ID 및 개체 위치의 볼륨 ID입니다. CLNL: 객체 데이터가 아카이빙된 경우 객체 위치의 ARC 노드 ID입니다.
경로	S3 버킷/키 또는 Swift 컨테이너 /오브젝트 ID	S3 버킷 이름 및 S3 키 이름 또는 Swift 컨테이너 이름 및 Swift 오브젝트 식별자.
RSLT	결과	ILM 작업의 결과. SUCS: ILM 작업이 성공했습니다.
규칙	규칙 레이블	• 보존 기간이 만료되어 호환 S3 버킷의 오브젝트가 자동으로 삭제되는 경우 이 필드는 비어 있습니다. • 현재 개체에 적용되는 배치 지침이 더 이상 없기 때문에 개체를 삭제하는 경우 이 필드에는 개체에 적용된 마지막 ILM 규칙의 사람이 읽을 수 있는 레이블이 표시됩니다.
SGRP	사이트(그룹)	개체가 있는 경우 지정된 사이트에서 해당 개체가 수집된 사이트가 아니라 해당 개체가 삭제되었습니다.

코드	필드에 입력합니다	설명
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
VSID 를 선택합니다	버전 ID	삭제된 개체의 특정 버전의 버전 ID입니다. 비버전 버킷의 버킷 및 오브젝트에 대한 작업에는 이 필드가 포함되지 않습니다.

LKCU: 덮어쓴 개체 정리

이 메시지는 StorageGRID가 이전에 정리 작업을 통해 스토리지 공간을 확보하는 데 필요한 덮어쓴 개체를 제거할 때 생성됩니다. S3 또는 Swift 클라이언트가 오브젝트를 이미 포함하고 있는 경로에 오브젝트를 쓸 때 오브젝트를 덮어쓰기합니다. 제거 프로세스는 백그라운드에서 자동으로 실행됩니다.

코드	필드에 입력합니다	설명
CSRZ	콘텐츠 크기	오브젝트의 크기(바이트)입니다.
LTYP	정리 유형입니다	내부 전용.
LUID	객체 UUID를 제거했습니다	제거된 개체의 식별자입니다.
경로	S3 버킷/키 또는 Swift 컨테이너 /오브젝트 ID	S3 버킷 이름 및 S3 키 이름 또는 Swift 컨테이너 이름 및 Swift 오브젝트 식별자.
SEGC	컨테이너 UUID	분할된 객체에 대한 컨테이너의 UUID입니다. 이 값은 개체가 분할된 경우에만 사용할 수 있습니다.
UUID입니다	범용 고유 식별자	아직 존재하는 개체의 식별자입니다. 이 값은 객체가 삭제되지 않은 경우에만 사용할 수 있습니다.

LLST: 위치가 손실되었습니다

이 메시지는 오브젝트 복사본(복제 또는 삭제 코딩)의 위치를 찾을 수 없을 때마다 생성됩니다.

코드	필드에 입력합니다	설명
CBIL	CBID	영향을 받는 CBID
귀도	소스 노드 ID입니다	위치가 손실된 노드 ID입니다.
UUID입니다	범용 고유 ID입니다	StorageGRID 시스템에서 영향을 받는 개체의 식별자입니다.

코드	필드에 입력합니다	설명
ECPR	삭제 코딩 프로필	삭제 코딩 오브젝트 데이터의 경우: 사용된 삭제 코딩 프로파일의 ID입니다.
LTYP	위치 유형	CLDI(온라인): 복제된 개체 데이터의 경우 CLEC(온라인): 삭제 코딩 오브젝트 데이터 CLNL(Nearline): 아카이빙된 복제 객체 데이터의 경우
PCLD	복제된 객체에 대한 경로입니다	손실된 개체 데이터의 디스크 위치에 대한 전체 경로입니다. LTYP에 CLDI 값(즉, 복제된 개체의 경우)이 있는 경우에만 반환됩니다. '/var/local/rangedb/2/p/13/13/00oJs6X%{h{U) SeUFxE@' 형식을 사용합니다
RSLT	결과	항상 없음. RSLT는 필수 메시지 필드이지만 이 메시지와 관련이 없습니다. 이 메시지가 필터링되지 않도록 SUCS 대신 사용되지 않습니다.
TsRC	트리거 소스	사용자: 사용자가 트리거했습니다 시스템: 시스템이 트리거되었습니다

MGAU: 관리 감사 메시지

관리 범주는 사용자 요청을 관리 API에 기록합니다. API에 대한 GET 또는 HEAD 요청이 아닌 모든 요청은 API에 대한 사용자 이름, IP 및 요청 유형을 사용하여 응답을 기록합니다.

코드	필드에 입력합니다	설명
MDIP	대상 IP 주소입니다	서버(대상) IP 주소입니다.
MDNA	도메인 이름	호스트 도메인 이름입니다.
MPAT	요청 경로	요청 경로입니다.
MPQP	쿼리 매개 변수를 요청합니다	요청에 대한 쿼리 매개 변수입니다.

코드	필드에 입력합니다	설명
MRBD	요청 본문	요청 본문의 내용 응답 본문이 기본적으로 기록되지만 응답 본문이 비어 있을 때 요청 본문이 특정 경우에 기록됩니다. 응답 본문에서 다음 정보를 사용할 수 없으므로 다음과 같은 POST 방법에 대한 요청 본문에서 가져옵니다. • POST authorize * 의 사용자 이름 및 계정 ID • POST/GRID/GRID-NETWORKS/UPDATE * 에 새로운 서브넷 구성 • POST/GRID/NTP-서버/업데이트 * 의 새로운 NTP 서버 • POST/GRID/SERVER/서비스 해제 * 에서 서비스 해제된 서버 ID • 참고: * 중요한 정보는 삭제(예: S3 액세스 키)되거나 별표로 가려집니다(예: 암호).
MRMD	요청 방법	HTTP 요청 방법: • 게시 • 를 누릅니다 • 삭제 • 패치
MRSC	응답 코드	응답 코드입니다.
MRSP	응답 바디	응답 내용(응답 본문)은 기본적으로 기록됩니다. • 참고: * 중요한 정보는 삭제(예: S3 액세스 키)되거나 별표로 가려집니다(예: 암호).
MSIP	소스 IP 주소입니다	클라이언트(소스) IP 주소입니다.
뮌헨	사용자 URN	요청을 보낸 사용자의 URN(Uniform Resource Name)입니다.

코드	필드에 입력합니다	설명
RSLT	결과	성공(SUCS) 또는 백엔드에서 보고된 오류를 반환합니다.

OLST: 시스템에서 손실된 개체를 감지했습니다

이 메시지는 DDS 서비스가 StorageGRID 시스템 내에서 개체의 복제본을 찾을 수 없을 때 생성됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	손실된 개체의 CBID입니다.
귀도	노드 ID입니다	가능한 경우 손실된 개체의 마지막 알려진 직접 또는 니어라인 위치입니다. 볼륨 정보를 사용할 수 없는 경우 볼륨 ID 없이 노드 ID만 가질 수 있습니다.
경로	S3 버킷/키 또는 Swift 컨테이너 /오브젝트 ID	사용 가능한 경우 S3 버킷 이름 및 S3 키 이름 또는 Swift 컨테이너 이름 및 Swift 오브젝트 ID입니다.
RSLT	결과	이 필드에 값이 없습니다. RSLT는 필수 메시지 필드이지만 이 메시지와 관련이 없습니다. 이 메시지가 필터링되지 않도록 SUCS 대신 사용되지 않습니다.
UUID입니다	범용 고유 ID입니다	StorageGRID 시스템 내의 손실된 개체의 식별자입니다.
볼리	볼륨 ID입니다	사용 가능한 경우 손실된 개체의 마지막 알려진 위치에 대한 스토리지 노드 또는 아카이브 노드의 볼륨 ID입니다.

ORLM: 개체 규칙이 충족되었습니다

이 메시지는 ILM 규칙에 지정된 대로 개체가 성공적으로 저장 및 복사될 때 생성됩니다.

> 정책의 다른 규칙에서 개체 크기 고급 필터를 사용하는 경우 객체가 기본 복사본 2개 만들기 규칙에 의해 성공적으로 저장되면 ORLM 메시지가 생성되지 않습니다.

코드	필드에 입력합니다	설명
BUID	버킷 헤더	버킷 ID 필드. 내부 작업에 사용됩니다. STAT가 PRGD인 경우에만 나타납니다.
CBID	콘텐츠 블록 식별자	객체의 CBID입니다.
CSRZ	콘텐츠 크기	오브젝트의 크기(바이트)입니다.
위치	위치	StorageGRID 시스템 내에서 오브젝트 데이터의 저장 위치입니다. 오브젝트에 위치가 없는 경우(예: 삭제된 경우) Locs 값은 ""입니다. CLEC: 삭제 코딩 오브젝트의 경우 삭제 코딩 프로필 ID와 오브젝트 데이터에 적용되는 삭제 코딩 그룹 ID입니다. CLDI: 복제된 개체의 경우 LDR 노드 ID 및 개체 위치의 볼륨 ID입니다. CLNL: 객체 데이터가 아카이빙된 경우 객체 위치의 ARC 노드 ID입니다.
경로	S3 버킷/키 또는 Swift 컨테이너/오브젝트 ID	S3 버킷 이름 및 S3 키 이름 또는 Swift 컨테이너 이름 및 Swift 오브젝트 식별자.
RSLT	결과	ILM 작업의 결과. SUCS: ILM 작업이 성공했습니다.
규칙	규칙 레이블	이 개체에 적용된 ILM 규칙에 지정된 사람이 읽을 수 있는 레이블입니다.
SEGC	컨테이너 UUID	분할된 객체에 대한 컨테이너의 UUID입니다. 이 값은 개체가 분할된 경우에만 사용할 수 있습니다.
SGCB	컨테이너 CBID	분할된 객체에 대한 컨테이너의 CBID입니다. 이 값은 세그먼트화된 개체와 여러 부분으로 구성된 개체에만 사용할 수 있습니다.

코드	필드에 입력합니다	설명
STAT	상태	ILM 작업의 상태입니다. 완료: 객체에 대한 ILM 작업이 완료되었습니다. DFER: 향후 ILM 재평가를 위해 객체가 표시되었습니다. PRGD: StorageGRID 시스템에서 객체가 삭제되었습니다. NLOC: 객체 데이터를 더 이상 StorageGRID 시스템에서 찾을 수 없습니다. 이 상태는 오브젝트 데이터의 모든 복사본이 누락 또는 손상되었음을 나타낼 수 있습니다.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.

ORLM 감사 메시지는 단일 객체에 대해 여러 번 발행될 수 있습니다. 예를 들어, 다음 이벤트 중 하나가 발생할 때마다 실행됩니다.

- 개체에 대한 ILM 규칙이 영구 충족됩니다.
- 개체에 대한 ILM 규칙이 이 Epoch에 충족되었습니다.
- ILM 규칙이 개체를 삭제했습니다.
- 백그라운드 검증 프로세스에서는 복제된 개체 데이터의 복사본이 손상되었음을 감지합니다. StorageGRID 시스템은 ILM 평가를 수행하여 손상된 개체를 교체합니다.

관련 정보

- 오브젝트 수집 트랜잭션
- 객체 삭제 트랜잭션입니다

OVWR: 개체 덮어쓰기

이 메시지는 외부(클라이언트 요청) 작업으로 인해 다른 개체에서 한 개체를 덮어쓸 때 생성됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자(신규)	새 개체의 CBID입니다.
CSRZ	이전 개체 크기	덮어쓰는 개체의 크기(바이트)입니다.
OCBD	콘텐츠 블록 식별자(이전)	이전 객체의 CBID입니다.

코드	필드에 입력합니다	설명
UUID입니다	범용 고유 ID(새로운 기능)	StorageGRID 시스템 내의 새 개체의 식별자입니다.
OUID	범용 고유 ID(이전)	StorageGRID 시스템 내의 이전 개체에 대한 식별자입니다.
경로	S3 또는 Swift 오브젝트 경로	이전 객체와 새 오브젝트 모두에 사용되는 S3 또는 Swift 오브젝트 경로입니다
RSLT	결과 코드	오브젝트 덮어쓰기 트랜잭션의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
SGRP	사이트(그룹)	덮어쓴 개체가 있는 경우 지정된 사이트에서 삭제된 개체는 덮어쓴 개체가 수집된 사이트가 아닙니다.

추가**:** 보안 감사 비활성화

이 메시지는 발신 서비스(노드 ID)가 감사 메시지 로깅을 해제했으며 감사 메시지가 더 이상 수집되거나 전달되지 않음을 나타냅니다.

코드	필드에 입력합니다	설명
AeTM	방법 사용	감사를 비활성화하는 데 사용되는 방법입니다.
아에이	사용자 이름	감사 로깅을 비활성화하기 위해 명령을 실행한 사용자 이름입니다.
RSLT	결과	이 필드에 값이 없습니다. RSLT는 필수 메시지 필드이지만 이 메시지와 관련이 없습니다. 이 메시지가 필터링되지 않도록 SUCS 대신 사용되지 않습니다.

이 메시지는 로깅이 이전에 활성화되었지만 이제 비활성화되었음을 나타냅니다. 일반적으로 대량 수집 중에만 사용되어 시스템 성능을 향상시킵니다. 대량 작업 후 감사가 복원(Sade)되고 감사를 해제하는 기능이 영구적으로 차단됩니다.

Sade: 보안 감사 활성화

이 메시지는 발신 서비스(노드 ID)가 감사 메시지 로깅을 복원했으며 감사 메시지가 다시 수집 및 전달되고 있음을 나타냅니다.

코드	필드에 입력합니다	설명
AeTM	방법 사용	감사를 활성화하는 데 사용되는 방법입니다.
아에이	사용자 이름	감사 로깅을 사용하도록 명령을 실행한 사용자 이름입니다.
RSLT	결과	이 필드에 값이 없습니다. RSLT는 필수 메시지 필드이지만 이 메시지와 관련이 없습니다. 이 메시지가 필터링되지 않도록 SUCS 대신 사용되지 않습니다.

이 메시지는 로깅이 이전에 비활성화(Sadd)되었지만 이제 복원되었음을 나타냅니다. 일반적으로 대량 수집 중에만 사용되어 시스템 성능을 향상시킵니다. 대량 작업이 완료된 후 감사가 복원되고 감사를 해제하는 기능이 영구적으로 차단됩니다.

SCMT: 오브젝트 저장소 커밋

그리드 콘텐츠는 커밋될 때까지(영구적으로 저장되었음을 의미) 사용 가능하거나 저장된 것으로 인식되지 않습니다. 영구적으로 저장된 콘텐츠는 디스크에 완전히 기록되었으며 관련 무결성 검사를 통과했습니다. 이 메시지는 콘텐츠 블록이 저장소에 커밋될 때 발행됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	영구 저장소에 커밋된 콘텐츠 블록의 고유 식별자입니다.
RSLT	결과 코드	객체가 디스크에 저장된 시점의 상태: SUCS: 객체가 성공적으로 저장되었습니다.

이 메시지는 지정된 콘텐츠 블록이 완전히 저장되고 확인되었으며 이제 요청될 수 있음을 의미합니다. 시스템 내의 데이터 흐름을 추적하는 데 사용할 수 있습니다.

SDEL: S3 삭제

S3 클라이언트가 삭제 트랜잭션을 실행할 때 지정된 오브젝트 또는 버킷을 제거하라는 요청이 발생합니다. 이 메시지는 트랜잭션이 성공하면 서버에서 발행됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	요청된 콘텐츠 블록의 고유 식별자입니다. CBID를 알 수 없는 경우 이 필드는 0으로 설정됩니다. 버킷의 작업에는 이 필드가 포함되지 않습니다.

코드	필드에 입력합니다	설명
CNCH	정합성 보장 제어 헤더	요청에 정합성 보장 - 제어 HTTP 요청 헤더(있는 경우)의 값입니다.
CNID	연결 식별자	TCP/IP 연결에 대한 고유한 시스템 식별자입니다.
CSRZ	콘텐츠 크기	삭제된 개체의 크기(바이트)입니다. 버킷의 작업에는 이 필드가 포함되지 않습니다.
DMRK	마커 버전 ID를 삭제합니다	버전이 있는 버킷에서 오브젝트를 삭제할 때 생성된 삭제 마커의 버전 ID입니다. 버킷의 작업에는 이 필드가 포함되지 않습니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. • 참고: * 요청에 X-Forwarded-For가 존재하고, X-Forwarded-For 값이 SAIP(Request sender IP address)(SAIP audit field)와 다른 경우 자동으로 포함된다.
MTME	마지막 수정 시간	객체가 마지막으로 수정된 시간을 나타내는 Unix 타임 스탬프(단위: 마이크로초)입니다.
RSLT	결과 코드	삭제 트랜잭션의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
S3AI	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 해시된 S3 액세스 키 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3BK	S3 버킷	S3 버킷 이름입니다.
S3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷의 작업에는 이 필드가 포함되지 않습니다.
S3SR	S3 하위 리소스	해당되는 경우, 작동 중인 버킷 또는 오브젝트 하위 자원.
SACC	S3 테넌트 계정 이름(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 이름입니다. 익명 요청에 대해 비어 있습니다.
SAIP	IP 주소(요청 발신자)	요청을 한 클라이언트 애플리케이션의 IP 주소입니다.

코드	필드에 입력합니다	설명
SBAC	S3 테넌트 계정 이름(버킷 소유자)	버킷 소유자의 테넌트 계정 이름입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
SBAI를 참조하십시오	S3 테넌트 계정 ID(버킷 소유자)	타겟 버킷의 소유자의 테넌트 계정 ID입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
SGRP	사이트(그룹)	개체가 있는 경우 지정된 사이트에서 해당 개체가 수집된 사이트가 아니라 해당 개체가 삭제되었습니다.
SUSR	S3 사용자 URN(요청 발신자)	테넌트 계정 ID 및 요청을 하는 사용자의 사용자 이름입니다. 사용자는 로컬 사용자 또는 LDAP 사용자일 수 있습니다. 예: 'urn:SGWs:identity::03393893651506583485:root 익명 요청에 대해 비어 있습니다.
시간	시간	요청의 총 처리 시간(마이크로초)입니다.
TLIP	신뢰할 수 있는 로드 밸런서 IP 주소	요청이 트러스트된 레이어 7 로드 밸런서에 의해 라우팅된 경우 로드 밸런서의 IP 주소입니다.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
VSID 를 선택합니다	버전 ID	삭제된 개체의 특정 버전의 버전 ID입니다. 비버전 버킷의 버킷 및 오브젝트에 대한 작업에는 이 필드가 포함되지 않습니다.

SGET: S3 GET

S3 클라이언트가 가져오기 트랜잭션을 실행할 때 오브젝트를 검색하거나 버킷에 있는 오브젝트를 나열하도록 요청이 이루어집니다. 이 메시지는 트랜잭션이 성공하면 서버에서 발행됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	요청된 콘텐츠 블록의 고유 식별자입니다. CBID를 알 수 없는 경우 이 필드는 0으로 설정됩니다. 버킷의 작업에는 이 필드가 포함되지 않습니다.
CNCH	정합성 보장 제어 헤더	요청에 정합성 보장 - 제어 HTTP 요청 헤더(있는 경우)의 값입니다.
CNID	연결 식별자	TCP/IP 연결에 대한 고유한 시스템 식별자입니다.

코드	필드에 입력합니다	설명
CSRZ	콘텐츠 크기	검색된 객체의 크기(바이트)입니다. 버킷의 작업에는 이 필드가 포함되지 않습니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. • 참고: * 요청에 X-Forwarded-For가 존재하고, X-Forwarded-For 값이 SAIP(Request sender IP address)(SAIP audit field)와 다른 경우 자동으로 포함된다.
벨이 울렸습니다	Range Read(범위 읽기)	범위 읽기 작업에만 해당됩니다. 이 요청에서 읽은 바이트 범위를 나타냅니다. 슬래시(/) 뒤의 값은 전체 오브젝트의 크기를 표시합니다.
RSLT	결과 코드	Get 트랜잭션의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
S3AI	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 해시된 S3 액세스 키 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3BK	S3 버킷	S3 버킷 이름입니다.
S3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷의 작업에는 이 필드가 포함되지 않습니다.
S3SR	S3 하위 리소스	해당되는 경우, 작동 중인 버킷 또는 오브젝트 하위 자원.
SACC	S3 테넌트 계정 이름(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 이름입니다. 익명 요청에 대해 비어 있습니다.
SAIP	IP 주소(요청 발신자)	요청을 한 클라이언트 애플리케이션의 IP 주소입니다.

코드	필드에 입력합니다	설명
SBAC	S3 테넌트 계정 이름(버킷 소유자)	버킷 소유자의 테넌트 계정 이름입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
SBAI를 참조하십시오	S3 테넌트 계정 ID(버킷 소유자)	타겟 버킷의 소유자의 테넌트 계정 ID입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
SUSR	S3 사용자 URN(요청 발신자)	테넌트 계정 ID 및 요청을 하는 사용자의 사용자 이름입니다. 사용자는 로컬 사용자 또는 LDAP 사용자일 수 있습니다. 예: 'urn:SGWs:identity::03393893651506583485:root 익명 요청에 대해 비어 있습니다.
시간	시간	요청의 총 처리 시간(마이크로초)입니다.
TLIP	신뢰할 수 있는 로드 밸런서 IP 주소	요청이 트러스트된 레이어 7 로드 밸런서에 의해 라우팅된 경우 로드 밸런서의 IP 주소입니다.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
VSID 를 선택합니다	버전 ID	요청된 개체의 특정 버전의 버전 ID입니다. 비버전 버킷의 버킷 및 오브젝트에 대한 작업에는 이 필드가 포함되지 않습니다.

Shea: S3 헤드

S3 클라이언트가 헤드 트랜잭션을 실행할 때 오브젝트 또는 버킷의 존재 여부를 확인하고 오브젝트에 대한 메타데이터를 검색하기 위한 요청이 발생합니다. 이 메시지는 트랜잭션이 성공하면 서버에서 발행됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	요청된 콘텐츠 블록의 고유 식별자입니다. CBID를 알 수 없는 경우 이 필드는 0으로 설정됩니다. 버킷의 작업에는 이 필드가 포함되지 않습니다.

코드	필드에 입력합니다	설명
CNID	연결 식별자	TCP/IP 연결에 대한 고유한 시스템 식별자입니다.
CSRZ	콘텐츠 크기	선택한 오브젝트의 크기(바이트)입니다. 버킷의 작업에는 이 필드가 포함되지 않습니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. • 참고: * 요청에 X-Forwarded-For가 존재하고, X-Forwarded-For 값이 SAIP(Request sender IP address)(SAIP audit field)와 다른 경우 자동으로 포함된다.
RSLT	결과 코드	Get 트랜잭션의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
S3AI	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 해시된 S3 액세스 키 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3BK	S3 버킷	S3 버킷 이름입니다.
S3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷의 작업에는 이 필드가 포함되지 않습니다.
SACC	S3 테넌트 계정 이름(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 이름입니다. 익명 요청에 대해 비어 있습니다.
SAIP	IP 주소(요청 발신자)	요청을 한 클라이언트 애플리케이션의 IP 주소입니다.
SBAC	S3 테넌트 계정 이름(버킷 소유자)	버킷 소유자의 테넌트 계정 이름입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.

코드	필드에 입력합니다	설명
SBAI를 참조하십시오	S3 테넌트 계정 ID(버킷 소유자)	타겟 버킷의 소유자의 테넌트 계정 ID입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
SUSR	S3 사용자 URN(요청 발신자)	테넌트 계정 ID 및 요청을 하는 사용자의 사용자 이름입니다. 사용자는 로컬 사용자 또는 LDAP 사용자일 수 있습니다. 예: 'urn:SGWs:identity::03393893651506583485:root 익명 요청에 대해 비어 있습니다.
시간	시간	요청의 총 처리 시간(마이크로초)입니다.
TLIP	신뢰할 수 있는 로드 밸런서 IP 주소	요청이 트러스트된 레이어 7 로드 밸런서에 의해 라우팅된 경우 로드 밸런서의 IP 주소입니다.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
VSID 를 선택합니다	버전 ID	요청된 개체의 특정 버전의 버전 ID입니다. 비버전 버킷의 버킷 및 오브젝트에 대한 작업에는 이 필드가 포함되지 않습니다.

Spos: S3 POST

S3 클라이언트가 POST 오브젝트 요청을 실행할 때 트랜잭션이 성공하면 서버에서 이 메시지를 발행합니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	요청된 콘텐츠 블록의 고유 식별자입니다. CBID를 알 수 없는 경우 이 필드는 0으로 설정됩니다.
CNCH	정합성 보장 제어 헤더	요청에 정합성 보장 - 제어 HTTP 요청 헤더(있는 경우)의 값입니다.
CNID	연결 식별자	TCP/IP 연결에 대한 고유한 시스템 식별자입니다.

코드	필드에 입력합니다	설명
CSRZ	콘텐츠 크기	검색된 객체의 크기(바이트)입니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. • 참고: * 요청에 X-Forwarded-For가 존재하고, X-Forwarded-For 값이 SAIP(Request sender IP address)(SAIP audit field)와 다른 경우 자동으로 포함된다.
RSLT	결과 코드	POST 개체 복원 요청의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
S3AI	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 해시된 S3 액세스 키 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3BK	S3 버킷	S3 버킷 이름입니다.
S3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷의 작업에는 이 필드가 포함되지 않습니다.
S3SR	S3 하위 리소스	해당되는 경우, 작동 중인 버킷 또는 오브젝트 하위 자원. S3 Select 작업의 경우 "선택"으로 설정합니다.
SACC	S3 테넌트 계정 이름(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 이름입니다. 익명 요청에 대해 비어 있습니다.
SAIP	IP 주소(요청 발신자)	요청을 한 클라이언트 애플리케이션의 IP 주소입니다.
SBAC	S3 테넌트 계정 이름(버킷 소유자)	버킷 소유자의 테넌트 계정 이름입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.

코드	필드에 입력합니다	설명
SBAI를 참조하십시오	S3 테넌트 계정 ID(버킷 소유자)	타겟 버킷의 소유자의 테넌트 계정 ID입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
SRCF	하위 리소스 구성	정보를 복원합니다.
SUSR	S3 사용자 URN(요청 발신자)	테넌트 계정 ID 및 요청을 하는 사용자의 사용자 이름입니다. 사용자는 로컬 사용자 또는 LDAP 사용자일 수 있습니다. 예: 'urn:SGWs:identity::03393893651506583485:root 익명 요청에 대해 비어 있습니다.
시간	시간	요청의 총 처리 시간(마이크로초)입니다.
TLIP	신뢰할 수 있는 로드 밸런서 IP 주소	요청이 트러스트된 레이어 7 로드 밸런서에 의해 라우팅된 경우 로드 밸런서의 IP 주소입니다.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
VSID 를 선택합니다	버전 ID	요청된 개체의 특정 버전의 버전 ID입니다. 비버전 버킷의 버킷 및 오브젝트에 대한 작업에는 이 필드가 포함되지 않습니다.

SPUT: S3 PUT

S3 클라이언트가 PUT 트랜잭션을 실행할 때 새 오브젝트 또는 버킷을 생성해야 합니다. 이 메시지는 트랜잭션이 성공하면 서버에서 발행됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	요청된 콘텐츠 블록의 고유 식별자입니다. CBID를 알 수 없는 경우 이 필드는 0으로 설정됩니다. 버킷의 작업에는 이 필드가 포함되지 않습니다.
CMPS	준수 설정	버킷 생성 시 사용된 준수 설정(Put Bucket 요청에 있는 경우)(처음 1024자로 잘림)

코드	필드에 입력합니다	설명
CNCH	정합성 보장 제어 헤더	요청에 정합성 보장 - 제어 HTTP 요청 헤더(있는 경우)의 값입니다.
CNID	연결 식별자	TCP/IP 연결에 대한 고유한 시스템 식별자입니다.
CSRZ	콘텐츠 크기	검색된 객체의 크기(바이트)입니다. 버킷의 작업에는 이 필드가 포함되지 않습니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. • 참고: * 요청에 X-Forwarded-For가 존재하고, X-Forwarded-For 값이 SAIP(Request sender IP address)(SAIP audit field)와 다른 경우 자동으로 포함된다.
LKEN	개체 잠금이 활성화되었습니다	PUT Bucket 요청시 요청헤더 X-amz-BUCKET-OBJECT-LOCK-ENABLED 값
LKLH	개체 잠금 법적 보류	PUT Object 요청에 요청 헤더 x-amz-object-lock-legal-hold의 값
LKMD	개체 잠금 보존 모드	PUT Object 요청에 요청 헤더 x-amz-object-lock-mode 값이 있는 경우
LKRU	개체 잠금 종료 날짜를 유지합니다	PUT Object 요청에 요청 헤더 "x-amz-object-lock-retain-until-date"의 값
MTME	마지막 수정 시간	객체가 마지막으로 수정된 시간을 나타내는 Unix 타임 스탬프(단위: 마이크로초)입니다.
RSLT	결과 코드	PUT 트랜잭션의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
S3AI	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.

코드	필드에 입력합니다	설명
S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 해시된 S3 액세스 키 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3BK	S3 버킷	S3 버킷 이름입니다.
S3KY	S3KY	버킷 이름을 제외한 S3 키 이름. 버킷의 작업에는 이 필드가 포함되지 않습니다.
S3SR	S3 하위 리소스	해당되는 경우, 작동 중인 버킷 또는 오브젝트 하위 자원.
SACC	S3 테넌트 계정 이름(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 이름입니다. 익명 요청에 대해 비어 있습니다.
SAIP	IP 주소(요청 발신자)	요청을 한 클라이언트 애플리케이션의 IP 주소입니다.
SBAC	S3 테넌트 계정 이름(버킷 소유자)	버킷 소유자의 테넌트 계정 이름입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
SBAI를 참조하십시오	S3 테넌트 계정 ID(버킷 소유자)	타겟 버킷의 소유자의 테넌트 계정 ID입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
SRCF	하위 리소스 구성	새 하위 리소스 구성(처음 1024자로 잘림)
SUSR	S3 사용자 URN(요청 발신자)	테넌트 계정 ID 및 요청을 하는 사용자의 사용자 이름입니다. 사용자는 로컬 사용자 또는 LDAP 사용자일 수 있습니다. 예: 'urn:SGWs:identity::03393893651506583485:root' 익명 요청에 대해 비어 있습니다.
시간	시간	요청의 총 처리 시간(마이크로초)입니다.

코드	필드에 입력합니다	설명
TLIP	신뢰할 수 있는 로드 밸런서 IP 주소	요청이 트러스트된 레이어 7 로드 밸런서에 의해 라우팅된 경우 로드 밸런서의 IP 주소입니다.
ULID	업로드 ID입니다	SPUT 메시지에만 포함되어 있어 다중 파트 업로드 작업을 완료할 수 있습니다. 모든 부품이 업로드 및 조립되었음을 나타냅니다.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
VSID 를 선택합니다	버전 ID	버전 관리되는 버킷에서 생성된 새 개체의 버전 ID입니다. 비버전 버킷의 버킷 및 오브젝트에 대한 작업에는 이 필드가 포함되지 않습니다.
VSST	버전 관리 상태	버킷의 새로운 버전 관리 상태입니다. "활성화됨" 또는 "일시 중단됨"의 두 가지 상태가 사용됩니다. 객체에 대한 작업에는 이 필드가 포함되지 않습니다.

SREM: 오브젝트 저장소 제거

이 메시지는 콘텐츠가 영구 저장소에서 제거되고 더 이상 일반 API를 통해 액세스할 수 없을 때 발행됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	영구 저장소에서 삭제된 콘텐츠 블록의 고유 식별자입니다.
RSLT	결과 코드	콘텐츠 제거 작업의 결과를 나타냅니다. 정의된 유일한 값은 다음과 같습니다. SUCS: 영구 스토리지에서 콘텐츠가 제거되었습니다

이 감사 메시지는 지정된 콘텐츠 블록이 노드에서 삭제되었으며 더 이상 직접 요청할 수 없음을 의미합니다. 이 메시지를 사용하여 시스템 내에서 삭제된 콘텐츠의 흐름을 추적할 수 있습니다.

SUPD:S3 메타데이터가 업데이트되었습니다

이 메시지는 S3 클라이언트가 수집된 개체의 메타데이터를 업데이트할 때 S3 API에서

생성됩니다. 메타데이터 업데이트에 성공하면 서버에서 이 메시지를 발행합니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	요청된 콘텐츠 블록의 고유 식별자입니다. CBID를 알 수 없는 경우 이 필드는 0으로 설정됩니다. 버킷의 작업에는 이 필드가 포함되지 않습니다.
CNCH	정합성 보장 제어 헤더	버킷의 준수 설정을 업데이트할 때 요청에 있는 경우 정합성 보장 제어 HTTP 요청 헤더의 값
CNID	연결 식별자	TCP/IP 연결에 대한 고유한 시스템 식별자입니다.
CSRZ	콘텐츠 크기	검색된 객체의 크기(바이트)입니다. 버킷의 작업에는 이 필드가 포함되지 않습니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. • 참고: * 요청에 X-Forwarded-For가 존재하고, X-Forwarded-For 값이 SAIP(Request sender IP address)(SAIP audit field)와 다른 경우 자동으로 포함된다.
RSLT	결과 코드	Get 트랜잭션의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
S3AI	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 해시된 S3 액세스 키 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3BK	S3 버킷	S3 버킷 이름입니다.
S3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷의 작업에는 이 필드가 포함되지 않습니다.

코드	필드에 입력합니다	설명
SACC	S3 테넌트 계정 이름(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 이름입니다. 익명 요청에 대해 비어 있습니다.
SAIP	IP 주소(요청 발신자)	요청을 한 클라이언트 애플리케이션의 IP 주소입니다.
SBAC	S3 테넌트 계정 이름(버킷 소유자)	버킷 소유자의 테넌트 계정 이름입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
SBAI를 참조하십시오	S3 테넌트 계정 ID(버킷 소유자)	타겟 버킷의 소유자의 테넌트 계정 ID입니다. 교차 계정 또는 익명 액세스를 식별하는 데 사용됩니다.
SUSR	S3 사용자 URN(요청 발신자)	테넌트 계정 ID 및 요청을 하는 사용자의 사용자 이름입니다. 사용자는 로컬 사용자 또는 LDAP 사용자일 수 있습니다. 예: 'urn:SGWs:identity::03393893651506583485:root 익명 요청에 대해 비어 있습니다.
시간	시간	요청의 총 처리 시간(마이크로초)입니다.
TLIP	신뢰할 수 있는 로드 밸런서 IP 주소	요청이 트러스트된 레이어 7 로드 밸런서에 의해 라우팅된 경우 로드 밸런서의 IP 주소입니다.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
VSID 를 선택합니다	버전 ID	메타데이터가 업데이트된 개체의 특정 버전의 버전 ID입니다. 비버전 버킷의 버킷 및 오브젝트에 대한 작업에는 이 필드가 포함되지 않습니다.

SVRF: Object Store Verify Fail(SVRF: 오브젝트 저장소 확인 실패**)**

이 메시지는 콘텐츠 블록이 확인 프로세스를 통과하지 못할 때마다 발행됩니다. 복제된 오브젝트 데이터를 디스크에서 읽거나 디스크에 쓸 때마다 여러 검증 및 무결성 검사가 수행되어 요청 사용자에게 전송된 데이터가 원래 시스템으로 수집된 데이터와 동일한지 확인합니다. 이러한 검사 중 하나라도 실패하면 시스템이 손상된 복제된 객체 데이터를 자동으로 격리하여 손상된 객체 데이터가 다시 검색되지 않도록 합니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	확인에 실패한 콘텐츠 블록의 고유 식별자입니다.
RSLT	결과 코드	확인 실패 유형: CRCF: CRC(Cyclic Redundancy Check)에 실패했습니다. HMAC: HMAC(해시 기반 메시지 인증 코드) 확인에 실패했습니다. EHSH: 예기치 않은 암호화된 콘텐츠 해시입니다. PHSH: 예기치 않은 원본 콘텐츠 해시입니다. SEQC: 디스크에 잘못된 데이터 시퀀스가 있습니다. PERR: 디스크 파일의 구조가 잘못되었습니다. DERR: 디스크 오류입니다. FNAM: 파일 이름이 잘못되었습니다.

- 참고: * 이 메시지는 면밀하게 모니터링되어야 합니다. 콘텐츠 확인 실패는 콘텐츠 변조 시도 또는 하드웨어 오류가 임박했음을 나타낼 수 있습니다.

메시지를 트리거한 작업을 확인하려면 모듈 ID(amid) 필드의 값을 참조하십시오. 예를 들어, SVFY 값은 메시지가 Storage Verifier 모듈에 의해 생성되었음을 나타냅니다. 즉, 백그라운드 검증 및 스토리지 는 메시지가 콘텐츠 검색에 의해 트리거되었음을 나타냅니다.

SVRU: Object Store Verify Unknown

LDR 서비스의 스토리지 구성 요소는 개체 저장소에서 복제된 개체 데이터의 모든 복사본을 지속적으로 검사합니다. 이 메시지는 객체 저장소에서 알 수 없거나 예상치 못한 복제된 객체 데이터 복제본이 발견되어 격리 디렉토리로 이동될 때 발행됩니다.

코드	필드에 입력합니다	설명
FPTH	파일 경로	예기치 않은 개체 복사의 파일 경로입니다.

코드	필드에 입력합니다	설명
RSLT	결과	이 필드에는 '없음' 값이 있습니다. RSLT는 필수 메시지 필드이지만 이 메시지와 관련이 없습니다. 이 메시지가 필터링되지 않도록 'UCS' 대신 '없음'이 사용됩니다.

- 참고: * SVRU: Object Store Verify Unknown audit 메시지는 면밀하게 모니터링되어야 합니다. 오브젝트 저장소에서 예기치 않은 오브젝트 데이터 복사본이 감지되었음을 의미합니다. 이러한 상황은 콘텐츠 조작 시도 또는 하드웨어 오류가 임박했음을 나타낼 수 있으므로 이러한 복사본이 생성된 방법을 즉시 조사해야 합니다.

SYSD:노드 중지

서비스가 정상적으로 중지되면 이 메시지가 생성되어 종료가 요청되었음을 나타냅니다. 일반적으로 이 메시지는 종료 전에 감사 메시지 대기열이 지워지지 않기 때문에 이후에 다시 시작한 후에만 전송됩니다. 서비스가 다시 시작되지 않은 경우 종료 시퀀스 시작 시 전송되는 SYST 메시지를 확인합니다.

코드	필드에 입력합니다	설명
RSLT	시스템 종료를 청소합니다	종료의 특성: SUCS: 시스템이 완전히 종료되었습니다.

이 메시지는 호스트 서버가 중지 중인지 여부를 나타내지 않으며 보고 서비스만 표시합니다. SYSD의 RSLT는 "비정상" 종료를 나타낼 수 없습니다. 왜냐하면 메시지는 "완전" 종료에서만 생성되기 때문입니다.

시스템**:**노드 중지 중

서비스가 정상적으로 중지되면 이 메시지가 생성되어 종료가 요청되었으며 서비스가 종료 시퀀스를 시작했음을 나타냅니다. SYSD와 달리 일반적으로 서비스를 다시 시작한 후 시스템을 사용하여 시스템 종료가 요청되었는지 확인할 수 있습니다.

코드	필드에 입력합니다	설명
RSLT	시스템 종료를 청소합니다	종료의 특성: SUCS: 시스템이 완전히 종료되었습니다.

이 메시지는 호스트 서버가 중지 중인지 여부를 나타내지 않으며 보고 서비스만 표시합니다. SYST 메시지의 RSLT 코드는 "비정상" 종료를 나타낼 수 없습니다. 왜냐하면 메시지는 "완전" 종료에서만 생성되기 때문입니다.

SYSU: 노드 시작

서비스가 다시 시작되면 이 메시지가 생성되어 이전 종료가 정상 종료(명령됨) 또는 불질서한

(예기치 않은) 상태임을 나타냅니다.

코드	필드에 입력합니다	설명
RSLT	시스템 종료를 청소합니다	종료의 특성: SUCS: 시스템이 완전히 종료되었습니다. DSDN: 시스템이 완전히 종료되지 않았습니다. VRGN: 서버 설치 후(또는 재설치) 처음으로 시스템이 시작되었습니다.

이 메시지는 호스트 서버가 시작되었는지 여부를 나타내지 않으며 보고 서비스만 표시합니다. 이 메시지는 다음과 같은 경우에 사용할 수 있습니다.

- 감사 추적에서 불연속성을 감지합니다.
- StorageGRID 시스템의 분산 특성으로 인해 이러한 오류가 마스킹될 수 있으므로 작업 중에 서비스가 실패하는지 확인합니다. 서버 관리자가 실패한 서비스를 자동으로 다시 시작합니다.

VLST: 사용자가 시작한 볼륨이 손실되었습니다

이 메시지는 '/proc/cMSI/Volume_lost' 명령어를 실행할 때마다 출력된다.

코드	필드에 입력합니다	설명
볼륨	볼륨 식별자 낮음	영향을 받는 볼륨 범위의 아래쪽 끝 또는 단일 볼륨입니다.
볼륨	볼륨 식별자 상부입니다	영향을 받는 볼륨 범위의 위쪽 끝입니다. 단일 볼륨의 경우 VOLL과 동일합니다.
귀도	소스 노드 ID입니다	위치가 손실된 노드 ID입니다.
LTYP	위치 유형	'CLDI'(온라인) 또는 'CLNL'(Nearline). 지정하지 않으면 기본적으로 'CLDI'가 사용됩니다.
RSLT	결과	항상 '없음'입니다. RSLT는 필수 메시지 필드이지만 이 메시지와 관련이 없습니다. 이 메시지가 필터링되지 않도록 'UCS' 대신 '없음'이 사용됩니다.

WDEL: Swift 삭제

Swift 클라이언트가 삭제 트랜잭션을 실행할 때 지정된 오브젝트 또는 컨테이너를 제거하라는 요청이 발생합니다. 이 메시지는 트랜잭션이 성공하면 서버에서 발행됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	요청된 콘텐츠 블록의 고유 식별자입니다. CBID를 알 수 없는 경우 이 필드는 0으로 설정됩니다. 컨테이너에 대한 작업에는 이 필드가 포함되지 않습니다.
CSRZ	콘텐츠 크기	삭제된 개체의 크기(바이트)입니다. 컨테이너에 대한 작업에는 이 필드가 포함되지 않습니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. • 참고: * 요청에 X-Forwarded-For가 존재하고, X-Forwarded-For 값이 SAIP(Request sender IP address)(SAIP audit field)와 다른 경우 자동으로 포함된다.
MTME	마지막 수정 시간	객체가 마지막으로 수정된 시간을 나타내는 Unix 타임 스탬프(단위: 마이크로초)입니다.
RSLT	결과 코드	삭제 트랜잭션의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
SAIP	요청 클라이언트의 IP 주소입니다	요청을 한 클라이언트 애플리케이션의 IP 주소입니다.
SGRP	사이트(그룹)	개체가 있는 경우 지정된 사이트에서 해당 개체가 수집된 사이트가 아니라 해당 개체가 삭제되었습니다.
시간	시간	요청의 총 처리 시간(마이크로초)입니다.
TLIP	신뢰할 수 있는 로드 밸런서 IP 주소	요청이 트러스트된 레이어 7 로드 밸런서에 의해 라우팅된 경우 로드 밸런서의 IP 주소입니다.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
WACC	SWIFT 계정 ID	StorageGRID 시스템에서 지정한 고유 계정 ID입니다.
WCON	SWIFT 컨테이너	Swift 컨테이너 이름입니다.
WOBJ	Swift 오브젝트	Swift 오브젝트 식별자입니다. 컨테이너에 대한 작업에는 이 필드가 포함되지 않습니다.

코드	필드에 입력합니다	설명
WUSR	SwiFT 계정 사용자	트랜잭션을 수행하는 클라이언트를 고유하게 식별하는 Swift 계정 사용자 이름입니다.

wget: Swift get

Swift 클라이언트가 가져오기 트랜잭션을 실행할 때 개체를 검색하거나 컨테이너의 개체를 나열하거나 계정의 컨테이너를 나열하도록 요청합니다. 이 메시지는 트랜잭션이 성공하면 서버에서 발행됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	요청된 콘텐츠 블록의 고유 식별자입니다. CBID를 알 수 없는 경우 이 필드는 0으로 설정됩니다. 계정 및 컨테이너에 대한 작업에는 이 필드가 포함되지 않습니다.
CSRZ	콘텐츠 크기	검색된 객체의 크기(바이트)입니다. 계정 및 컨테이너에 대한 작업에는 이 필드가 포함되지 않습니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. • 참고: * 요청에 X-Forwarded-For가 존재하고, X-Forwarded-For 값이 SAIP(Request sender IP address)(SAIP audit field)와 다른 경우 자동으로 포함된다.
RSLT	결과 코드	Get 트랜잭션의 결과. 결과는 항상 입니다 SUCS: 성공했습니다
SAIP	요청 클라이언트의 IP 주소입니다	요청을 한 클라이언트 애플리케이션의 IP 주소입니다.
시간	시간	요청의 총 처리 시간(마이크로초)입니다.
TLIP	신뢰할 수 있는 로드 밸런서 IP 주소	요청이 트러스트된 레이어 7 로드 밸런서에 의해 라우팅된 경우 로드 밸런서의 IP 주소입니다.

코드	필드에 입력합니다	설명
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
WACC	SWIFT 계정 ID	StorageGRID 시스템에서 지정한 고유 계정 ID입니다.
WCON	SWIFT 컨테이너	Swift 컨테이너 이름입니다. 계정 작업에는 이 필드가 포함되지 않습니다.
WOBJ	Swift 오브젝트	Swift 오브젝트 식별자입니다. 계정 및 컨테이너에 대한 작업에는 이 필드가 포함되지 않습니다.
WUSR	SwiFT 계정 사용자	트랜잭션을 수행하는 클라이언트를 고유하게 식별하는 Swift 계정 사용자 이름입니다.

WHEA: 스위프트 헤드

Swift 클라이언트가 헤드 트랜잭션을 실행할 때 계정, 컨테이너 또는 개체의 존재 여부를 확인하고 관련 메타데이터를 검색하도록 요청합니다. 이 메시지는 트랜잭션이 성공하면 서버에서 발행됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	요청된 콘텐츠 블록의 고유 식별자입니다. CBID를 알 수 없는 경우 이 필드는 0으로 설정됩니다. 계정 및 컨테이너에 대한 작업에는 이 필드가 포함되지 않습니다.
CSRZ	콘텐츠 크기	검색된 객체의 크기(바이트)입니다. 계정 및 컨테이너에 대한 작업에는 이 필드가 포함되지 않습니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. • 참고: * 요청에 X-Forwarded-For가 존재하고, X-Forwarded-For 값이 SAIP(Request sender IP address)(SAIP audit field)와 다른 경우 자동으로 포함된다.

코드	필드에 입력합니다	설명
RSLT	결과 코드	머리 거래의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
SAIP	요청 클라이언트의 IP 주소입니다	요청을 한 클라이언트 애플리케이션의 IP 주소입니다.
시간	시간	요청의 총 처리 시간(마이크로초)입니다.
TLIP	신뢰할 수 있는 로드 밸런서 IP 주소	요청이 트러스트된 레이어 7 로드 밸런서에 의해 라우팅된 경우 로드 밸런서의 IP 주소입니다.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
WACC	SWIFT 계정 ID	StorageGRID 시스템에서 지정한 고유 계정 ID입니다.
WCON	SWIFT 컨테이너	Swift 컨테이너 이름입니다. 계정 작업에는 이 필드가 포함되지 않습니다.
WOBJ	Swift 오브젝트	Swift 오브젝트 식별자입니다. 계정 및 컨테이너에 대한 작업에는 이 필드가 포함되지 않습니다.
WUSR	SwiFT 계정 사용자	트랜잭션을 수행하는 클라이언트를 고유하게 식별하는 Swift 계정 사용자 이름입니다.

WPUT: Swift Put

Swift 클라이언트가 PUT 트랜잭션을 실행할 때 새 오브젝트 또는 컨테이너를 만들도록 요청합니다. 이 메시지는 트랜잭션이 성공하면 서버에서 발행됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	요청된 콘텐츠 블록의 고유 식별자입니다. CBID를 알 수 없는 경우 이 필드는 0으로 설정됩니다. 컨테이너에 대한 작업에는 이 필드가 포함되지 않습니다.

코드	필드에 입력합니다	설명
CSRZ	콘텐츠 크기	검색된 객체의 크기(바이트)입니다. 컨테이너에 대한 작업에는 이 필드가 포함되지 않습니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. • 참고: * 요청에 X-Forwarded-For가 존재하고, X-Forwarded-For 값이 SAIP(Request sender IP address)(SAIP audit field)와 다른 경우 자동으로 포함된다.
MTME	마지막 수정 시간	객체가 마지막으로 수정된 시간을 나타내는 Unix 타임 스탬프(단위: 마이크로초)입니다.
RSLT	결과 코드	PUT 트랜잭션의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
SAIP	요청 클라이언트의 IP 주소입니다	요청을 한 클라이언트 애플리케이션의 IP 주소입니다.
시간	시간	요청의 총 처리 시간(마이크로초)입니다.
TLIP	신뢰할 수 있는 로드 밸런서 IP 주소	요청이 트러스트된 레이어 7 로드 밸런서에 의해 라우팅된 경우 로드 밸런서의 IP 주소입니다.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
WACC	SWIFT 계정 ID	StorageGRID 시스템에서 지정한 고유 계정 ID입니다.
WCON	SWIFT 컨테이너	Swift 컨테이너 이름입니다.
WOBJ	Swift 오브젝트	Swift 오브젝트 식별자입니다. 컨테이너에 대한 작업에는 이 필드가 포함되지 않습니다.

코드	필드에 입력합니다	설명
WUSR	SwiFT 계정 사용자	트랜잭션을 수행하는 클라이언트를 고유하게 식별하는 Swift 계정 사용자 이름입니다.

사용자 환경에서 **StorageGRID**를 활성화하는 방법

StorageGRID 환경에서 애플리케이션을 테스트하고 구현하는 방법을 알아보십시오.

로 이동합니다 "StorageGRID 지원" 이 사이트의 제품 설명서에서 확장하는 예제 및 요리책을 찾을 수 있는 DOC 사이트입니다. 또한 * StorageGRID-enable * 사이트에서는 StorageGRID를 평가하고 통합하는 몇 가지 단계를 설명합니다.

다음 정보가 포함되어 있습니다.

- 과거 및 현재 StorageGRID 릴리즈에서 검증된 타사 솔루션 목록
- 제품 기능 가이드. 예를 들어, 이 가이드에서는 클라우드 스토리지 풀을 생성하는 방법에 대한 자세한 정보를 제공합니다.
- 툴 및 애플리케이션 가이드
- S3 암호화, S3 오브젝트 잠금과 같은 StorageGRID 기능을 사용하기 위한 API 예

기타 버전의 NetApp StorageGRID 설명서

다른 NetApp StorageGRID 소프트웨어 릴리즈에 대한 문서는 다음을 참조하십시오.

- "StorageGRID 11.7 문서"
- "StorageGRID 11.5 문서"
- "StorageGRID 11.4 문서"
- "StorageGRID 11.3 문서"
- "StorageGRID 11.2 문서"

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/ECMLP2879263

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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