StorageGRID 11.9 설명서

StorageGRID 11.9

NetApp
November 08, 2024

목차

StorageGRID 11.9 설명서

StorageGRID 어플라이언스

StorageGRID 스토리지 및 서비스 어플라이언스를 설치, 구성 및 유지 관리하는 방법에 대해 알아보려면 를 "StorageGRID 어플라이언스 설명서" 참조하십시오.

릴리스 정보

해결된 문제 및 알려진 문제에 대한 릴리스 관련 정보를 얻습니다.

StorageGRID 11.9 릴리즈 노트가 포함된 NetApp 지원 사이트에 "PDF 파일을 보거나 다운로드합니다" 로그인합니다.

StorageGRID 시스템을 시작하십시오

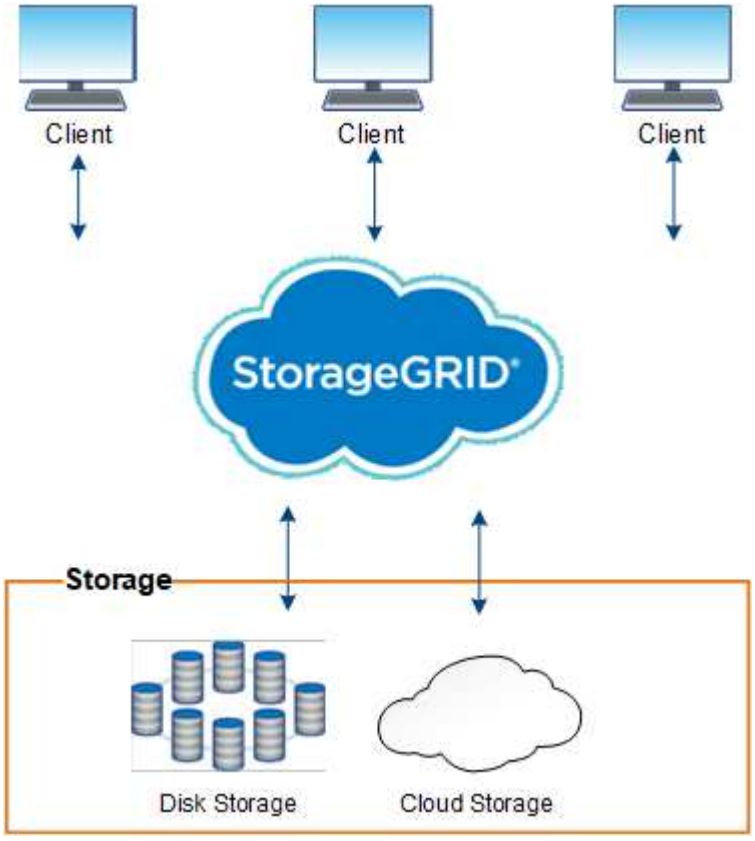
StorageGRID에 대해 자세히 알아보십시오

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.



아카이브 노드에 대한 지원이 제거되었습니다. S3 API를 통해 아카이브 노드에서 외부 아카이브 스토리지 시스템으로 오브젝트를 이동하는 것은 가 "ILM 클라우드 스토리지 풀"더 많은 기능을 제공하는 것으로 대체되었습니다.

StorageGRID의 이점

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

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

- 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. 오브젝트 수준에서 데이터 라이프사이클을 관리하는 ILM 규칙을 생성하여 데이터 인접성, 내구성, 성능, 비용, 사용자 정의 도움이 됩니다.
- 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 하이브리드 클라우드 구성에서 StorageGRID를 사용하고, 클라우드 스토리지 풀에 오브젝트를 저장하고, StorageGRID 플랫폼 서비스를 활용하고, ONTAP에서 NetApp FabricPool를 통해 StorageGRID로 데이터를 계층화합니다.

클라우드 스토리지 풀

클라우드 스토리지 풀을 사용하면 StorageGRID 시스템 외부에 오브젝트를 저장할 수 있습니다. 예를 들어, 자주 액세스하지 않는 오브젝트를 Microsoft Azure Blob 스토리지의 Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud 또는 Archive 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.

디스크 및 테이프 스토리지를 비롯한 타사 파트너 스토리지도 지원됩니다.

> 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 아마존 SNS(Simple Notification Service) 이벤트 수신을 지원하는 외부 엔드포인트로 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.

FabricPool를 사용한 ONTAP 데이터 계층화

FabricPool를 사용하여 데이터를 StorageGRID로 계층화하여 ONTAP 스토리지 비용을 절감할 수 있습니다. FabricPool를 사용하면 사내 또는 사외에서 데이터를 저비용 오브젝트 스토리지 계층으로 자동 계층화할 수 있습니다.

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

- "Cloud Storage Pool이란?"
- "플랫폼 서비스 관리"
- "FabricPool용 StorageGRID를 구성합니다"

StorageGRID 아키텍처 및 네트워크 토폴로지

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

를 "그리드 노드 유형에 대한 설명입니다"참조하십시오.

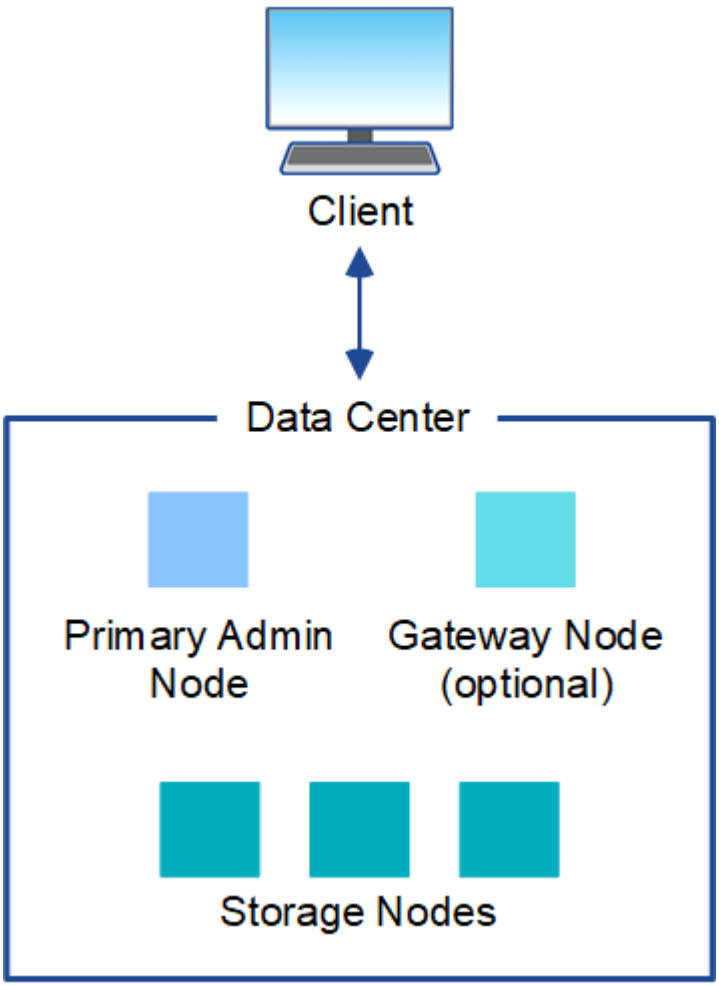
StorageGRID 네트워크 토폴로지, 요구 사항 및 그리드 통신에 대한 자세한 내용은 를 참조하십시오"네트워킹 지침".

구축 토폴로지

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

단일 사이트

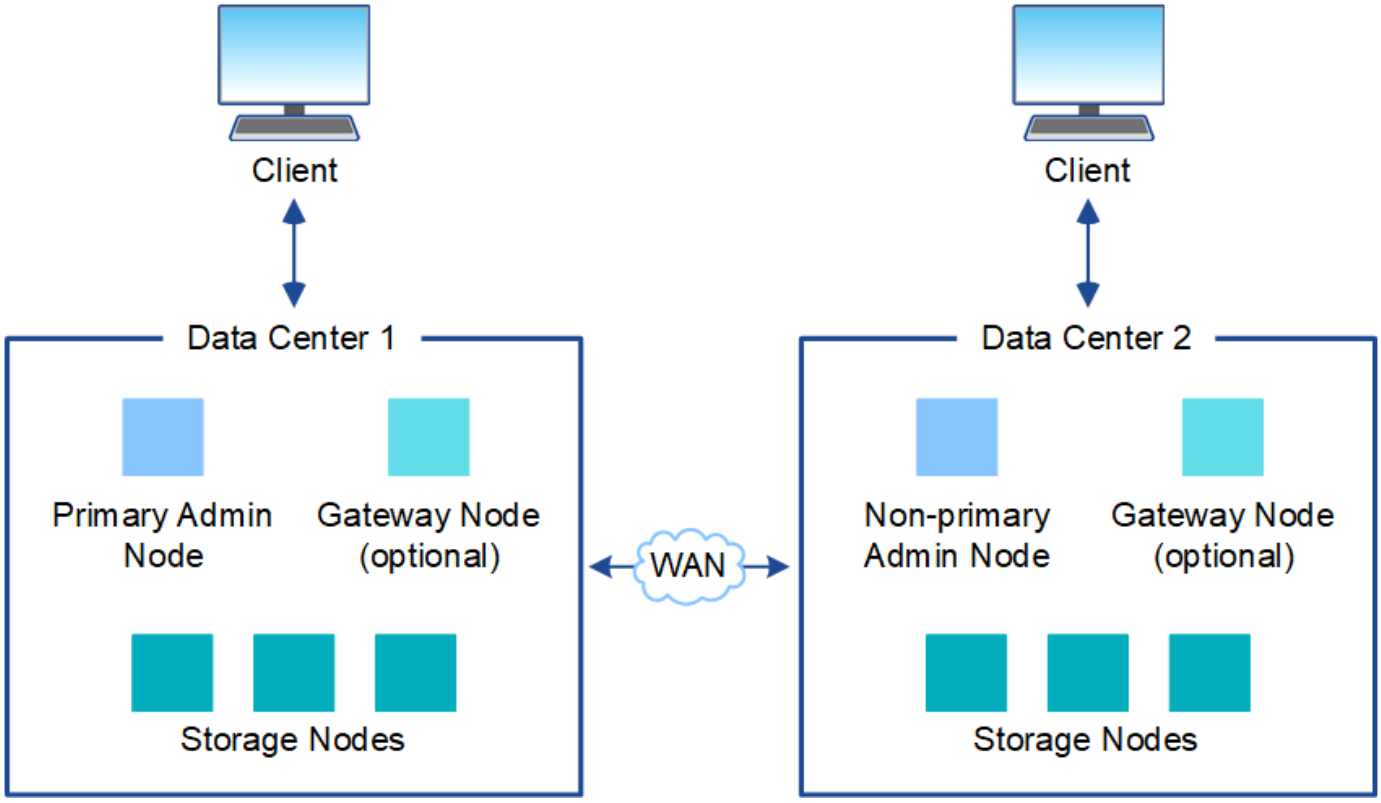
단일 사이트를 통한 배포에서는 StorageGRID 시스템의 인프라 및 운영이 중앙 집중화됩니다.



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.



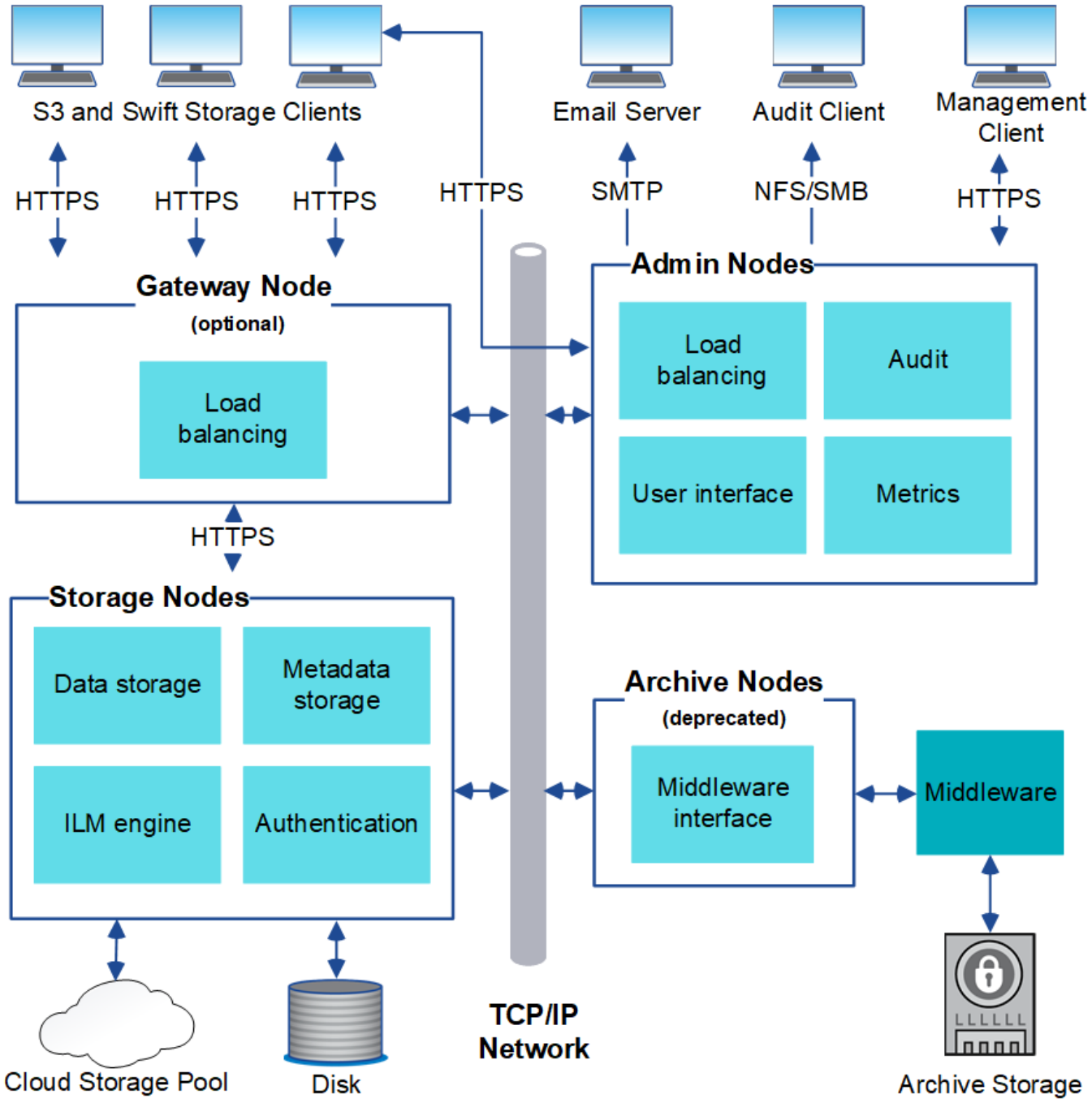
또한 단일 데이터 센터 내에 여러 개의 논리적 사이트가 존재하여 분산된 복제 및 삭제 코딩을 통해 가용성과 복원력을 높일 수 있습니다.

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

S3 클라이언트를 게이트웨이 노드 또는 관리자 노드에 연결하여 스토리지 노드에 대한 로드 밸런싱 인터페이스를 사용할 수 있습니다. 또는 S3 클라이언트를 HTTPS를 사용하여 스토리지 노드에 직접 연결할 수 있습니다.

오브젝트를 소프트웨어 또는 하드웨어 기반 스토리지 노드의 StorageGRID 내에 저장하거나 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.

그리드 노드의 유형

StorageGRID 시스템은 네 가지 유형의 그리드 노드를 사용합니다.

관리자 노드

시스템 구성, 모니터링 및 로깅 등의 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 클라이언트 트래픽의 로드 밸런싱을 수행할 수도 있습니다.

을 참조하십시오 "관리 노드란 무엇입니까?"

스토리지 노드

오브젝트 데이터 및 메타데이터를 관리 및 저장합니다. StorageGRID 시스템의 각 사이트에는 3개 이상의 스토리지 노드가 있어야 합니다.

을 참조하십시오 "스토리지 노드란?"

게이트웨이 노드(선택 사항)

클라이언트 애플리케이션이 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.

을 참조하십시오 "게이트웨이 노드란 무엇입니까?"

하드웨어 및 소프트웨어 노드

StorageGRID 노드는 StorageGRID 어플라이언스 노드로 구축하거나 소프트웨어 기반 노드로 구축할 수 있다.

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.

사용 가능한 어플라이언스에 대한 자세한 내용은 다음을 참조하십시오.

- "StorageGRID 어플라이언스 설명서"
- "NetApp Hardware Universe를 참조하십시오"

소프트웨어 기반 노드

소프트웨어 기반 그리드 노드는 VMware 가상 머신으로 구축하거나 Linux 호스트의 컨테이너 엔진 내에 구축할 수

있습니다.

- VMware vSphere의 VM(가상 머신): 를 참조하십시오."VMware에 StorageGRID를 설치합니다"
- Red Hat Enterprise Linux의 컨테이너 엔진 내부: 을 참조하십시오."Red Hat Enterprise Linux에 StorageGRID를 설치합니다"
- Ubuntu 또는 Debian의 컨테이너 엔진 내부: 를 참조하십시오"Ubuntu 또는 Debian에 StorageGRID를 설치합니다".

를 사용하여 "NetApp 상호 운용성 매트릭스 툴(IMT)" 지원되는 버전을 확인합니다.

새 소프트웨어 기반 스토리지 노드의 초기 설치 중에 에만 사용하도록 지정할 수 "메타데이터 저장"있습니다.

StorageGRID 서비스

다음은 StorageGRID 서비스의 전체 목록입니다.

서비스	설명	위치
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.	관리 노드 및 게이트웨이 노드의 로드 밸런서 서비스
ADC(관리 도메인 컨트롤러)	LDR 및 CMN 서비스의 토폴로지 정보 유지, 인증 서비스 제공 및 쿼리에 응답	각 사이트에서 ADC 서비스가 포함된 최소 3개의 스토리지 노드
AMS(감사 관리 시스템)	감사된 모든 시스템 이벤트 및 트랜잭션을 모니터링하고 텍스트 로그 파일에 기록합니다.	관리자 노드
Cassandra Refaper(Cassandra 성형기)	오브젝트 메타데이터를 자동으로 복구합니다.	스토리지 노드
청크 서비스	삭제 코딩 데이터 및 패리티 조각을 관리합니다.	스토리지 노드
CMN(구성 관리 노드)	시스템 전체 구성 및 그리드 작업 관리 각 그리드에는 하나의 CMN 서비스가 있습니다.	기본 관리자 노드
DDS(분산 데이터 저장소)	Cassandra 데이터베이스와 연결되어 개체 메타데이터를 관리합니다.	스토리지 노드
DMV(Data Mover)	데이터를 클라우드 엔드포인트로 이동합니다.	스토리지 노드
동적 IP(Dynip)	그리드를 모니터링하여 동적 IP 변경 사항을 모니터링하고 로컬 구성을 업데이트합니다.	모든 노드
그라파나	Grid Manager에서 메트릭 시각화에 사용됩니다.	관리자 노드

서비스	설명	위치
고가용성	High Availability Groups 페이지에 구성된 노드의 고가용성 가상 IP를 관리합니다. 이 서비스는 Keeepalived 서비스라고도 합니다.	관리자 및 게이트웨이 노드
ID(idnt)	LDAP 및 Active Directory에서 사용자 ID를 페더레이션합니다.	ADC 서비스를 사용하는 스토리지 노드입니다
람다 중재인	S3 Select SelectObjectContent 요청을 관리합니다.	모든 노드
로드 밸런서(nginx-GW)	클라이언트에서 스토리지 노드로의 S3 트래픽의 로드 밸런싱을 제공합니다. 부하 분산 서비스는 부하 분산 엔드포인트 구성 페이지를 통해 구성할 수 있습니다. 이 서비스는 nginx-GW 서비스라고도 합니다.	관리자 및 게이트웨이 노드
LDR(로컬 분배 라우터)	그리드 내의 컨텐츠 저장 및 전송을 관리합니다.	스토리지 노드
MISCd 정보 서비스 제어 데몬	다른 노드의 서비스를 쿼리 및 관리하고 다른 노드에서 실행 중인 서비스 상태를 쿼리하는 것과 같은 노드의 환경 구성을 관리하기 위한 인터페이스를 제공합니다.	모든 노드
Nginx	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.	모든 노드
Nginx-GW	로드 밸런서 서비스에 전원을 공급합니다.	관리자 및 게이트웨이 노드
NMS(네트워크 관리 시스템)	Grid Manager를 통해 표시되는 모니터링, 보고 및 구성 옵션을 강화합니다.	관리자 노드
지속성	재부팅 시 유지되어야 하는 루트 디스크의 파일을 관리합니다.	모든 노드
프로메테우스	모든 노드의 서비스에서 시계열 메트릭을 수집합니다.	관리자 노드
RSM(복제된 상태 시스템)	플랫폼 서비스 요청이 각 엔드포인트로 전송되도록 합니다.	ADC 서비스를 사용하는 스토리지 노드입니다
SSM(서버 상태 모니터)	하드웨어 조건을 모니터링하고 NMS 서비스에 보고합니다.	모든 그리드 노드에 인스턴스가 있습니다

서비스	설명	위치
추적 수집기	기술 지원 부서에서 사용할 정보를 수집하기 위해 추적 수집을 수행합니다. 추적 수집기 서비스는 오픈 소스 Jaeger 소프트웨어를 사용합니다.	관리자 노드

관리 노드란 무엇입니까?

관리 노드는 시스템 구성, 모니터링 및 로깅과 같은 관리 서비스를 제공합니다. 관리 노드를 사용하여 S3 클라이언트 트래픽의 로드 밸런싱을 수행할 수도 있습니다. 각 그리드에는 1개의 기본 관리 노드가 있어야 하며 이중화를 위해 여러 개의 비기본 관리 노드가 있을 수 있습니다.

운영 관리 노드와 비운영 관리 노드 간의 차이점

그리드 관리자 또는 테넌트 관리자에 로그인할 때 관리 노드에 연결됩니다. 모든 관리 노드에 연결할 수 있으며 각 관리 노드에는 StorageGRID 시스템의 유사한 보기가 표시됩니다. 하지만 기본 관리자 노드는 비기본 관리자 노드보다 더 많은 기능을 제공합니다. 예를 들어 대부분의 유지 관리 절차는 기본 관리 노드에서 수행해야 합니다.

이 표에는 기본 및 비기본 관리 노드의 기능이 요약되어 있습니다.

제공합니다	기본 관리자 노드	운영 관리자 노드가 아닌 노드
서비스가 포함됩니다AMS	예	예
서비스가 포함됩니다CMN	예	아니요
서비스가 포함됩니다NMS	예	예
서비스가 포함됩니다프로메테우스	예	예
서비스가 포함됩니다SSM	예	예
로드 밸런서및 고가용성 서비스가 포함됩니다	예	예
(mgmt-API) 지원관리 애플리케이션 프로그램 인터페이스	예	예
IP 주소 변경 및 NTP 서버 업데이트와 같은 모든 네트워크 관련 유지 관리 작업에 사용할 수 있습니다	예	아니요
스토리지 노드 확장 후 EC 재조정을 수행할 수 있습니다	예	아니요
볼륨 복원 절차에 사용할 수 있습니다	예	예
하나 이상의 노드에서 로그 파일과 시스템 데이터를 수집할 수 있습니다	예	아니요

제공합니다	기본 관리자 노드	운영 관리자 노드가 아닌 노드
알림, AutoSupport 패키지 및 SNMP 트랩을 보내고 알림을 보냅니다	예. 의 역할을 기본 보낸 사람합니다.	예. 대기 발신자의 역할을 합니다.

기본 보낸 사람 관리자 노드

StorageGRID 구축에 여러 관리자 노드가 포함된 경우 기본 관리자 노드가 경고 알림, AutoSupport 패키지, SNMP 트랩 및 알림을 보내는 기본 보낸 사람이 됩니다.

정상적인 시스템 작업에서 기본 설정 보낸 사람만이 알림을 보냅니다. 그러나 다른 모든 관리 노드는 기본 설정 발신자를 모니터링합니다. 문제가 감지되면 다른 관리 노드가 대기 보낸 사람 역할을 합니다.

다음과 같은 경우 여러 알림이 전송될 수 있습니다.

- 관리 노드가 서로 "표시"되는 경우 기본 설정 보낸 사람과 대기 보낸 사람 모두 알림 보내기를 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.

> AutoSupport 패키지를 테스트할 때 모든 관리 노드가 테스트를 보냅니다. 알림 알림을 테스트할 때는 모든 관리 노드에 로그인하여 연결을 확인해야 합니다.

관리 노드에 대한 기본 서비스

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

서비스	키 기능
감사 관리 시스템(AMS)	시스템 활동 및 이벤트를 추적합니다.
구성 관리 노드(CMN)	시스템 전체 구성을 관리합니다.
고가용성	관리 노드 및 게이트웨이 노드 그룹의 고가용성 가상 IP 주소를 관리합니다. • 참고: * 이 서비스는 게이트웨이 노드에서도 찾을 수 있습니다.
[[로드 밸런서]] 로드 밸런서	클라이언트에서 스토리지 노드로의 S3 트래픽의 로드 밸런싱을 제공합니다. • 참고: * 이 서비스는 게이트웨이 노드에서도 찾을 수 있습니다.
관리 응용 프로그램 인터페이스(mgmt-API)	Grid Management API 및 Tenant Management API의 요청을 처리합니다.
네트워크 관리 시스템(NMS)	그리드 관리자를 위한 기능을 제공합니다.

서비스	키 기능
프로메테우스	모든 노드의 서비스에서 시계열 메트릭을 수집 및 저장합니다.
서버 상태 모니터(SSM)	운영 체제 및 기본 하드웨어를 모니터링합니다.

스토리지 노드란**?**

스토리지 노드: 오브젝트 데이터 및 메타데이터를 관리하고 저장합니다. 스토리지 노드에는 디스크의 오브젝트 데이터와 메타데이터를 저장, 이동, 확인 및 검색하는 데 필요한 서비스와 프로세스가 포함됩니다.

StorageGRID 시스템의 각 사이트에는 3개 이상의 스토리지 노드가 있어야 합니다.

스토리지 노드 유형

설치 중에 설치할 스토리지 노드 유형을 선택할 수 있습니다. 이러한 유형은 소프트웨어 기반 스토리지 노드와 기능을 지원하는 어플라이언스 기반 스토리지 노드에 사용할 수 있습니다.

- 결합된 데이터 및 메타데이터 스토리지 노드
- 메타데이터 전용 스토리지 노드입니다
- 데이터 전용 스토리지 노드

다음과 같은 상황에서 스토리지 노드 유형을 선택할 수 있습니다.

- 스토리지 노드를 처음 설치할 때
- StorageGRID 시스템 확장 중에 스토리지 노드를 추가하는 경우

> 스토리지 노드 설치가 완료된 후에는 유형을 변경할 수 없습니다.

데이터 및 메타데이터 스토리지 노드**(**결합됨**)**

기본적으로 모든 새 스토리지 노드는 객체 데이터와 메타데이터를 모두 저장합니다. 이 유형의 스토리지 노드를 A_COMBINED_Storage Node라고 합니다.

메타데이터 전용 스토리지 노드입니다

그리드에 많은 수의 작은 오브젝트가 저장되는 경우 메타데이터에만 스토리지 노드를 사용하는 것이 적절할 수 있습니다. 전용 메타데이터 용량을 설치하면 많은 수의 작은 개체에 필요한 공간과 이러한 개체에 대한 메타데이터에 필요한 공간 사이의 균형이 향상됩니다. 또한 고성능 어플라이언스에 호스팅되는 메타데이터 전용 스토리지 노드도 성능을 높일 수 있습니다.

메타데이터 전용 노드를 설치할 때 그리드에는 데이터 저장을 위한 최소 노드 수도 있어야 합니다.

- 단일 사이트 그리드의 경우 최소 두 개의 결합된 스토리지 노드 또는 데이터 전용 스토리지 노드를 구성합니다.
- 다중 사이트 그리드의 경우 사이트 _ 당 하나 이상의 결합된 스토리지 노드 또는 데이터 전용 스토리지 노드를 구성합니다.

메타데이터 전용 스토리지 노드에는 가 포함되어 있고 S3 클라이언트 요청을 처리할 수 있지만 LDR 서비스StorageGRID 성능이 향상되지 않을 수 있습니다.

데이터 전용 스토리지 노드

스토리지 노드의 성능 특성이 다르면 데이터에만 스토리지 노드를 사용하는 것이 적절합니다. 예를 들어, 성능을 잠재적으로 높이기 위해 메타데이터 전용 고성능 스토리지 노드와 함께 사용하는 데이터 전용 고용량 회전식 디스크 스토리지 노드를 사용할 수 있습니다.

데이터 전용 노드를 설치할 때 그리드에는 다음이 포함되어야 합니다.

- 최소 2개의 결합된 스토리지 노드 또는 데이터 전용 스토리지 노드_per grid_
- 사이트 _ 당 하나 이상의 결합된 스토리지 노드 또는 데이터 전용 스토리지 노드 _
- 사이트 _ 당 최소 3개의 결합된 또는 메타데이터 전용 스토리지 노드

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.

서비스	키 기능
관리 도메인 컨트롤러(ADC)	토폴로지 및 그리드 전체의 구성 유지 • 참고 *: 데이터 전용 스토리지 노드는 ADC 서비스를 호스팅하지 않습니다. 세부 정보 ADC(관리 도메인 컨트롤러) 서비스는 그리드 노드와 상호 연결을 인증합니다. ADC 서비스는 한 사이트에서 최소 3개의 스토리지 노드에 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 사본을 보유하므로 모든 그리드 노드가 현재 구성 정보를 검색할 수 있습니다. 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 노드의 인증서를 캐시하여 ADC 서비스를 사용할 수 없는 경우에도 시스템이 알려진 그리드 노드에서 계속 작동할 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.
Cassandra 를 클릭합니다	오브젝트 메타데이터를 저장하고 보호합니다. • 참고 *: 데이터 전용 스토리지 노드는 Cassandra 서비스를 호스팅하지 않습니다.
Cassandra Refaper(Cassandra 성형기)	오브젝트 메타데이터를 자동으로 복구합니다. • 참고 *: 데이터 전용 스토리지 노드는 Cassandra Reaper 서비스를 호스팅하지 않습니다.
청크	삭제 코딩 데이터 및 패리티 조각을 관리합니다.
Data Mover(DMV)	데이터를 클라우드 스토리지 풀로 이동합니다.

서비스	키 기능
DDS(분산 데이터 저장소)	오브젝트 메타데이터 스토리지를 모니터링합니다. 세부 정보 각 스토리지 노드에는 DDS(Distributed Data Store) 서비스가 포함됩니다. 이 서비스는 Cassandra 데이터베이스와 연동되어 StorageGRID 시스템에 저장된 오브젝트 메타데이터에 대한 백그라운드 작업을 수행합니다. DDS 서비스는 StorageGRID 시스템에 수집된 총 개체 수와 시스템의 지원되는 각 인터페이스(S3)를 통해 수집된 총 개체 수를 추적합니다.
ID(idnt)	LDAP 및 Active Directory에서 사용자 ID를 페더레이션합니다.

서비스	키 기능
로컬 분배 라우터(LDR)	오브젝트 스토리지 프로토콜 요청을 처리하고 디스크의 오브젝트 데이터를 관리합니다. 세부 정보 각 *Combined*, *data-only* 및 *metadata-only* 스토리지 노드에는 LDR(Local Distribution Router) 서비스가 포함됩니다. 이 서비스는 데이터 저장, 라우팅 및 요청 처리를 비롯한 콘텐츠 전송 기능을 처리합니다. 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 • S3 프로토콜 인터페이스 LDR 서비스는 각 S3 오브젝트도 고유한 UUID에 매핑합니다. 오브젝트 저장소 LDR 서비스의 기본 데이터 스토리지는 고정된 수의 오브젝트 저장소(스토리지 볼륨이라고도 함)로 나뉩니다. 각 오브젝트 저장소는 별도의 마운트 지점입니다. 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. 개체 저장소의 용량이 가득 차면 나머지 개체 저장소는 스토리지 노드에 더 이상의 공간이 없을 때까지 계속 개체를 저장합니다. 메타데이터 보호 StorageGRID는 LDR 서비스와 상호 작용하는 Cassandra 데이터베이스에 개체 메타데이터를 저장합니다. 이중화를 보장하고 손실을 방지하기 위해 각 사이트에 오브젝트 메타데이터의 복사본 3개가 유지됩니다. 이 복제는 구성이 불가능하며 자동으로 수행됩니다. 자세한 내용은 을 참조하십시오 "오브젝트 메타데이터 스토리지 관리".

서비스	키 기능
복제된 상태 시스템(RSM)	S3 플랫폼 서비스 요청이 해당 엔드포인트로 전송되도록 합니다.
서버 상태 모니터(SSM)	운영 체제 및 기본 하드웨어를 모니터링합니다.

게이트웨이 노드란 무엇입니까**?**

게이트웨이 노드는 S3 클라이언트 애플리케이션이 StorageGRID에 연결하는 데 사용할 수 있는 전용 로드 밸런싱 인터페이스를 제공합니다. 로드 밸런싱은 여러 스토리지 노드에 워크로드를 분산하여 속도와 연결 용량을 극대화합니다. 게이트웨이 노드는 선택 사항입니다.

StorageGRID 로드 밸런서 서비스는 모든 관리 노드 및 모든 게이트웨이 노드에 제공됩니다. 클라이언트 요청에 대한 TLS(Transport Layer Security) 종료를 수행하고 요청을 검사하며 스토리지 노드에 대한 새로운 보안 연결을 설정합니다. 로드 밸런서 서비스는 클라이언트를 최적의 스토리지 노드로 원활하게 전달하므로 노드 장애나 전체 사이트에 장애가 발생하지 않습니다.

게이트웨이 및 관리 노드의 부하 분산 서비스에 액세스하는 데 들어오는 클라이언트 및 나가는 클라이언트 요청에 사용할 포트 및 네트워크 프로토콜(HTTPS 또는 HTTP)을 정의하도록 하나 이상의 부하 분산 단말 장치를 구성합니다. 또한 로드 밸런서 엔드포인트는 클라이언트 유형(S3), 바인딩 모드 및 허용되는 테넌트 또는 차단된 테넌트 목록을 정의합니다. 을 "로드 균형 조정에 대한 고려 사항"참조하십시오.

필요에 따라 여러 게이트웨이 노드와 관리 노드의 네트워크 인터페이스를 고가용성(HA) 그룹으로 그룹화할 수 있습니다. HA 그룹의 활성 인터페이스에 장애가 발생하면 백업 인터페이스에서 클라이언트 애플리케이션 워크로드를 관리할 수 있습니다. 을 "고가용성(HA) 그룹 관리"참조하십시오.

게이트웨이 노드에 대한 기본 서비스

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

서비스	키 기능
고가용성	관리 노드 및 게이트웨이 노드 그룹의 고가용성 가상 IP 주소를 관리합니다. • 참고: * 이 서비스는 관리 노드에서도 찾을 수 있습니다.
로드 밸런서	클라이언트에서 스토리지 노드까지 S3 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 노드란 무엇입니까**?**

아카이브 노드에 대한 지원이 제거되었습니다.

아카이브 노드에 대한 자세한 내용은 을 "아카이브 노드란 무엇입니까(StorageGRID 11.8 문서 사이트)"참조하십시오.

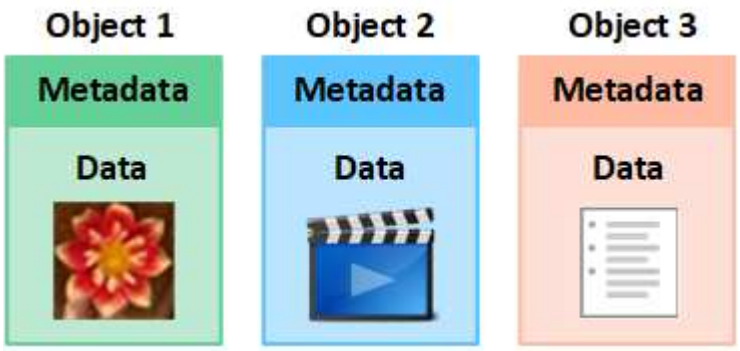
StorageGRID의 데이터 관리 방법

개체란 무엇입니까

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 데이터란?

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

오브젝트 메타데이터란?

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".

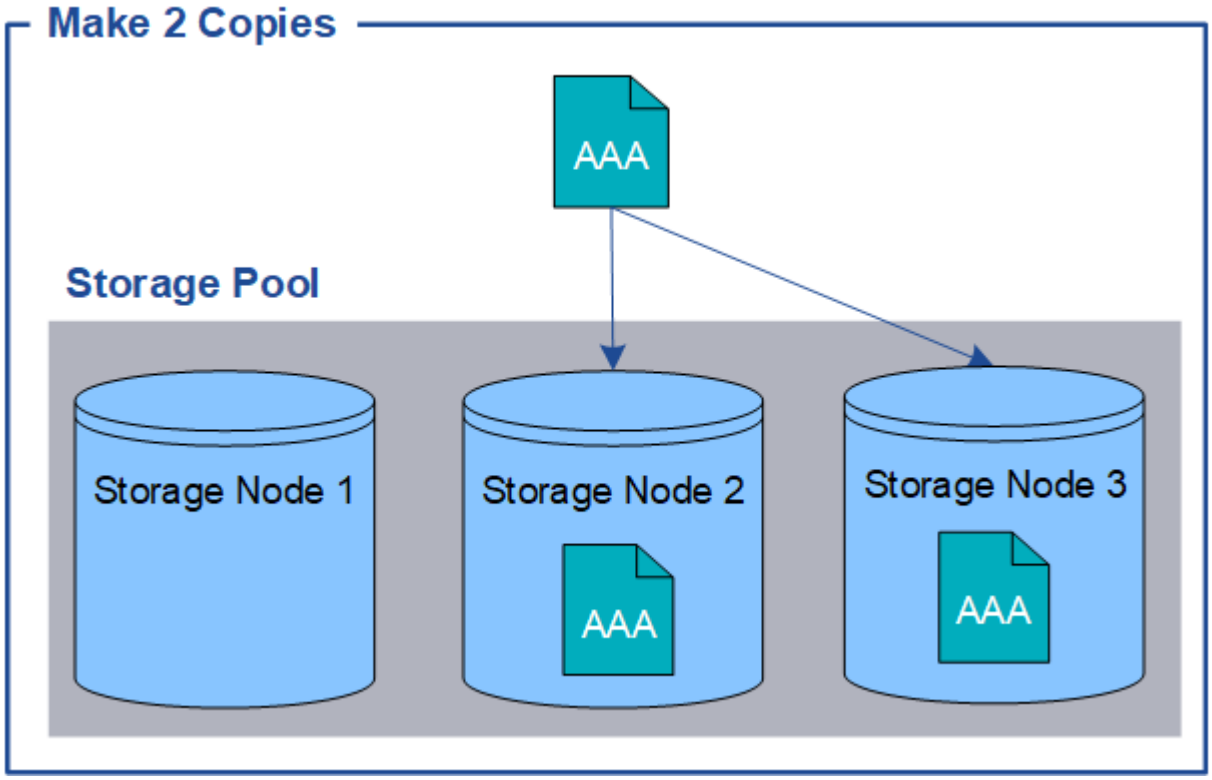
오브젝트 데이터는 어떻게 보호됩니까?

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

복제

StorageGRID가 복제된 복사본을 생성하도록 구성된 정보 라이프사이클 관리(ILM) 규칙과 일치하는 오브젝트가 있으면 시스템은 오브젝트 데이터의 정확한 복사본을 생성하고 이 복사본을 스토리지 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.

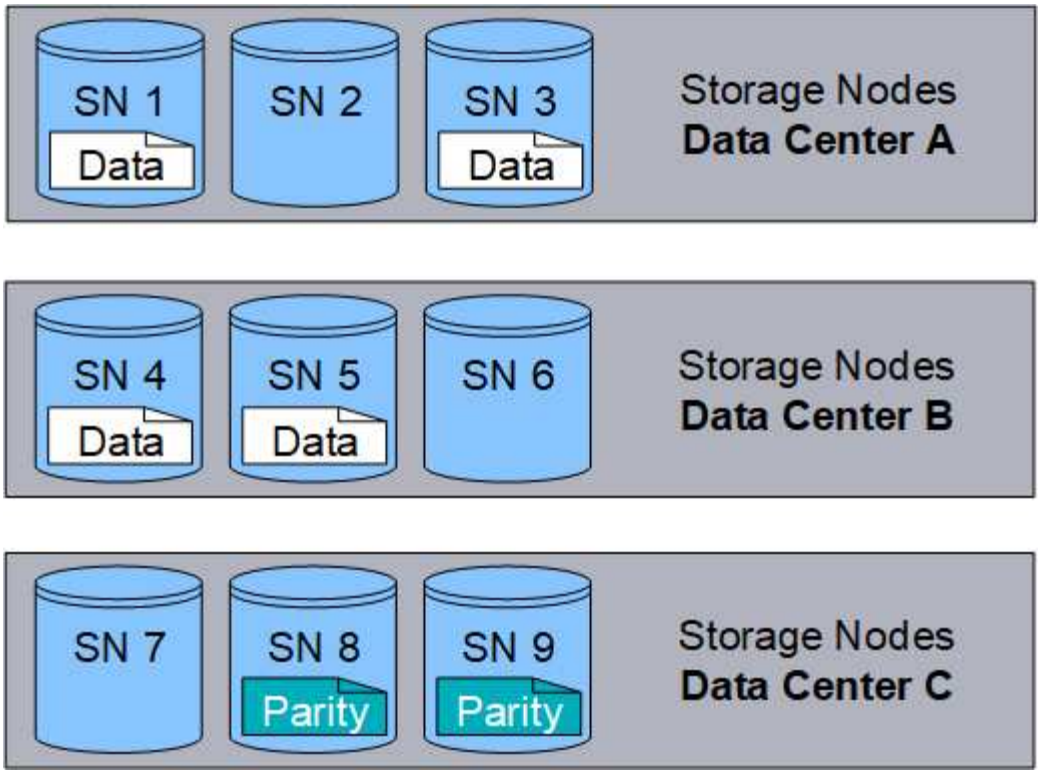
다음 예에서는 복제본 2개 만들기 규칙에 따라 각 객체의 복제된 복제본 2개가 스토리지 노드 3개가 포함된 스토리지 풀에 배치되도록 지정합니다.



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. 사용되는 삭제 코딩 체계는 ILM 규칙과 삭제 코딩 프로필에 따라 결정됩니다.

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"

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 StorageGRID 시스템에 개체를 저장하는 S3 클라이언트 응용 프로그램의 프로세스입니다. 이 단계에서 StorageGRID 시스템이 객체를 관리하기 시작합니다.
- * 복사 관리 *: 활성 ILM 정책의 ILM 규칙에 따라 StorageGRID에서 복제 및 삭제 코딩 복사본을 관리하는 프로세스입니다. 복사 관리 단계 중에 StorageGRID은 스토리지 노드 또는 클라우드 스토리지 풀에 지정된 수의 오브젝트 복사본을 생성하고 유지하여 오브젝트 데이터 손실을 보호합니다.
- * 검색 *: StorageGRID 시스템에 저장된 개체에 액세스하는 클라이언트 응용 프로그램의 프로세스입니다. 클라이언트는 스토리지 노드 또는 클라우드 스토리지 풀에서 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

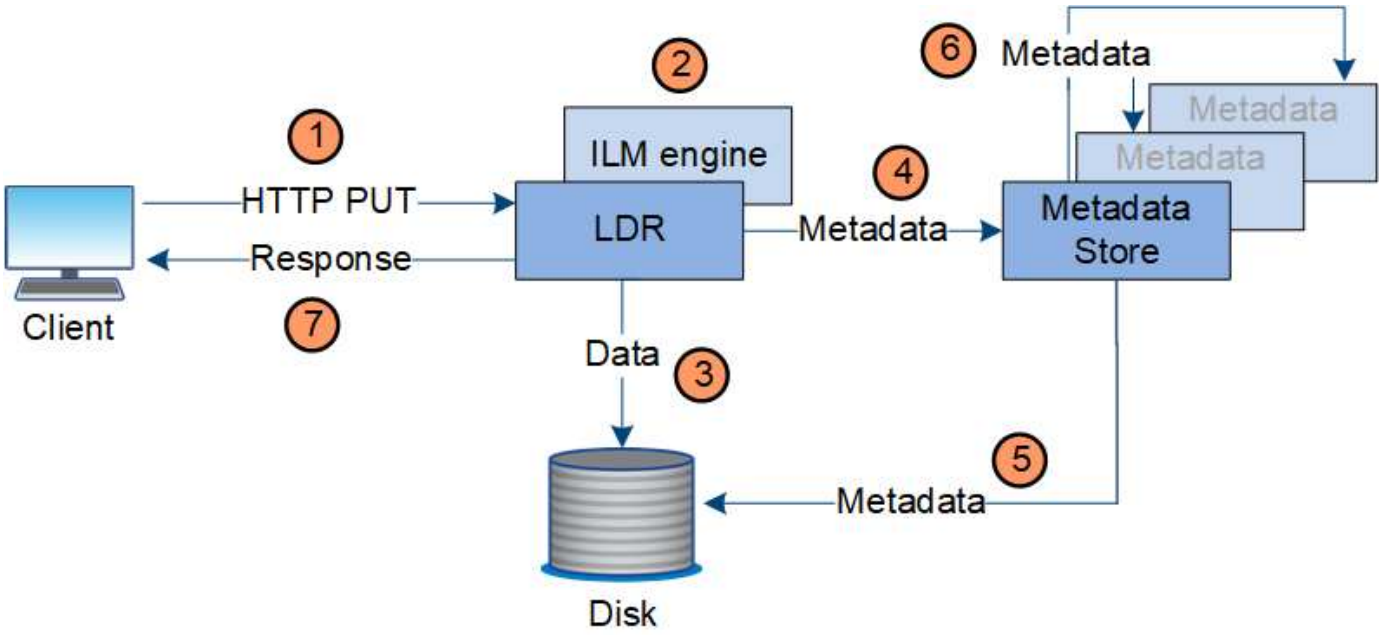
- "ILM을 사용하여 개체를 관리합니다"
- "정보 수명 주기 관리를 사용합니다"

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

오브젝트 데이터는 활성 ILM 정책 및 관련 ILM 규칙에 따라 관리됩니다. ILM 규칙은 복제된 복사본 또는 삭제 코딩 복사본을 만들어 오브젝트 데이터의 손실을 방지합니다.

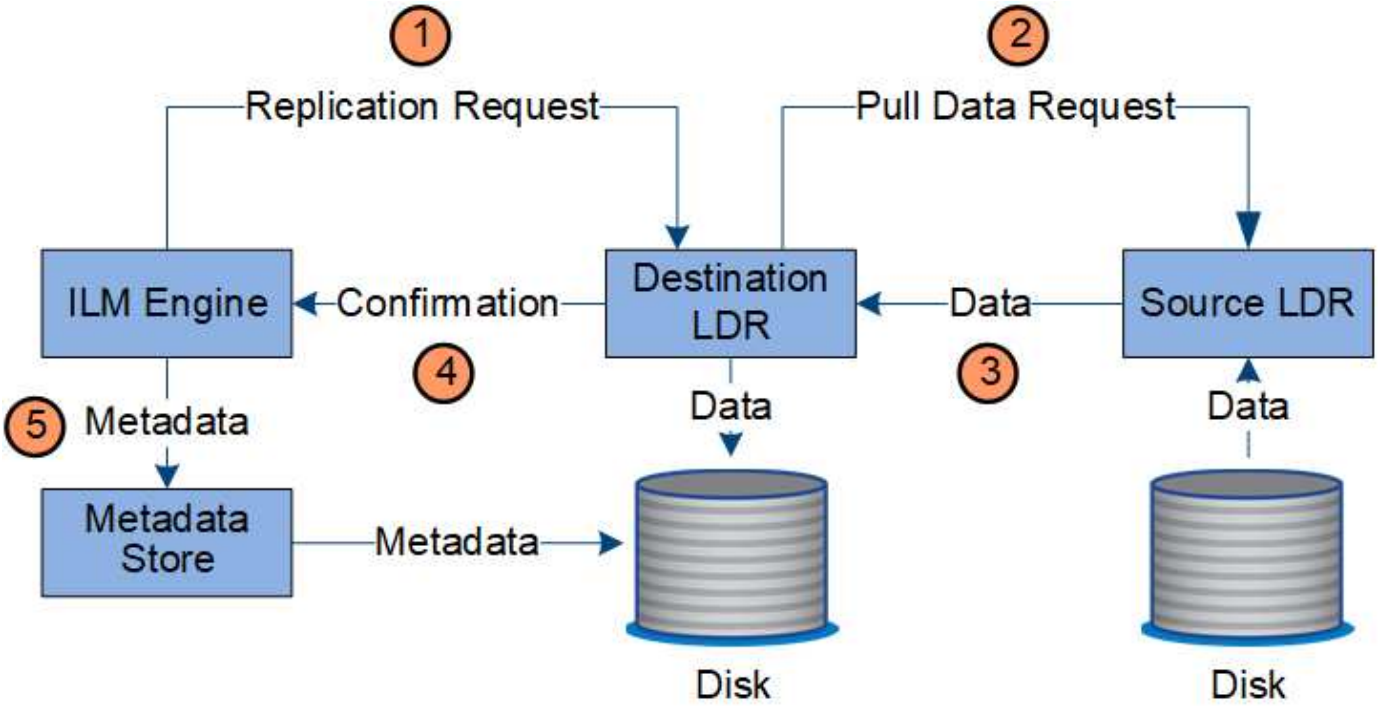
오브젝트 복사본의 다양한 유형 또는 위치는 오브젝트의 수명 동안 서로 다른 시간에 필요할 수 있습니다. ILM 규칙은 주기적으로 평가하여 개체가 필요에 따라 배치되도록 합니다.

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.

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

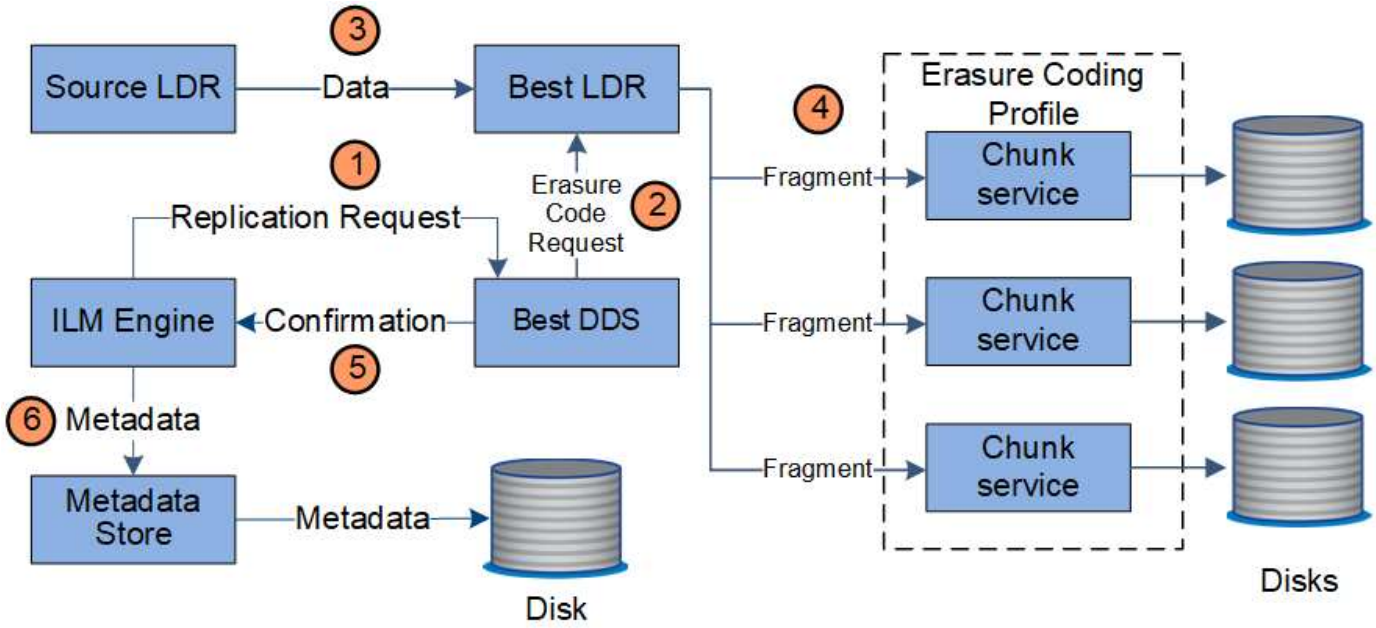


1. ILM 엔진은 ADC 서비스를 쿼리하여 ILM 규칙에 지정된 스토리지 풀 내에서 최상의 대상 LDR 서비스를 결정합니다. 그런 다음 LDR 서비스에 복제를 시작하는 명령을 보냅니다.
2. 대상 LDR 서비스는 ADC 서비스에 최상의 소스 위치를 쿼리합니다. 그런 다음 복제 요청을 소스 LDR 서비스로 보냅니다.
3. 소스 LDR 서비스는 대상 LDR 서비스에 복사본을 보냅니다.
4. 대상 LDR 서비스는 ILM 엔진에 개체 데이터가 저장되었음을 알립니다.
5. ILM 엔진은 메타데이터 저장소를 개체 위치 메타데이터로 업데이트합니다.

콘텐츠 보호: 삭제 코딩

ILM 규칙에 오브젝트 데이터의 삭제 코딩 복사본을 만드는 지침이 포함된 경우 해당 삭제 코딩 체계에서 오브젝트 데이터를 데이터 및 패리티 조각으로 분할하고 이러한 조각을 삭제 코딩 프로필에 구성된 스토리지 노드에 분산합니다.

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

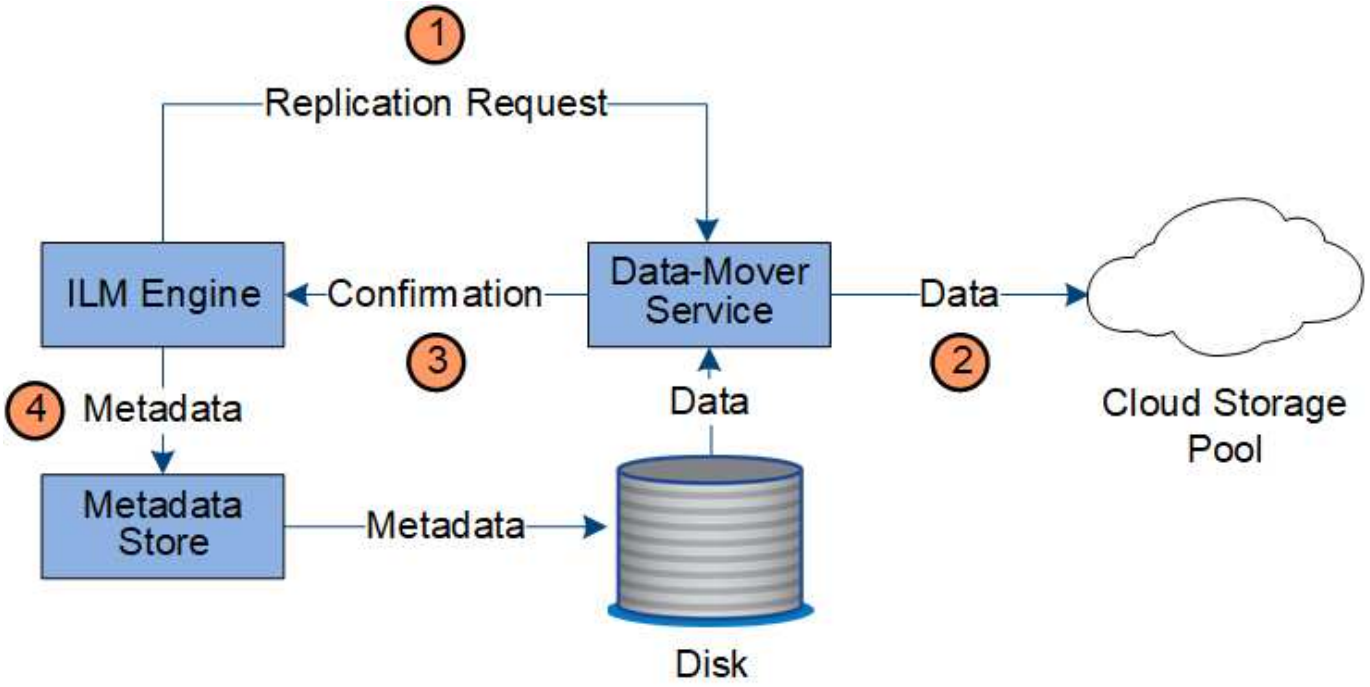


1. ILM 엔진은 ADC 서비스에 쿼리하여 삭제 코딩 작업을 가장 잘 수행할 수 있는 DDS 서비스를 결정합니다. 결정되면 ILM 엔진이 해당 서비스에 "시작" 요청을 보냅니다.
2. DDS 서비스는 LDR에 오브젝트 데이터를 삭제 코딩하도록 지시합니다.
3. 소스 LDR 서비스는 삭제 코딩을 위해 선택된 LDR 서비스에 복사본을 보냅니다.
4. 적절한 수의 패리티 및 데이터 조각을 생성한 후 LDR 서비스는 삭제 코딩 프로파일의 스토리지 풀을 구성하는 스토리지 노드(청크 서비스)에 이러한 조각을 분산합니다.
5. LDR 서비스는 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.

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



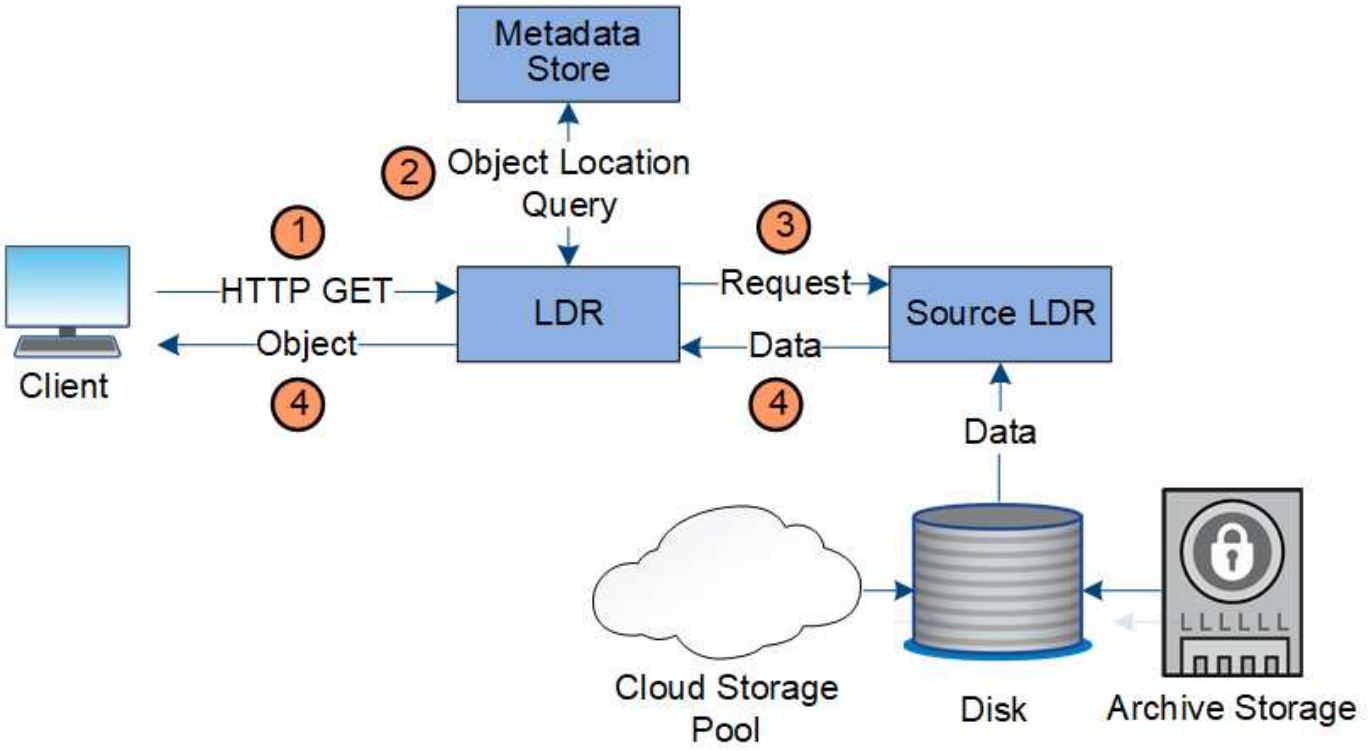
1. ILM 엔진은 Data Mover 서비스를 선택하여 Cloud Storage Pool에 복제합니다.
2. Data Mover 서비스는 객체 데이터를 클라우드 스토리지 풀로 보냅니다.
3. Data Mover 서비스는 ILM 엔진에 개체 데이터가 저장되었음을 알립니다.
4. ILM 엔진은 메타데이터 저장소를 개체 위치 메타데이터로 업데이트합니다.

데이터 흐름을 검색합니다

검색 작업은 StorageGRID 시스템과 클라이언트 간에 정의된 데이터 흐름으로 구성됩니다. 시스템은 특성을 사용하여 스토리지 노드 또는 필요한 경우 클라우드 스토리지 풀에서 객체 검색을 추적합니다.

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

> 오브젝트 복사본만 AWS Glacier 스토리지 또는 Azure Archive 계층에 있는 경우 클라이언트 애플리케이션은 S3 RestoreObject 요청을 발행하여 검색 가능한 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 설정된 버킷의 오브젝트는 ILM이 "영구"로 유지합니다. 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

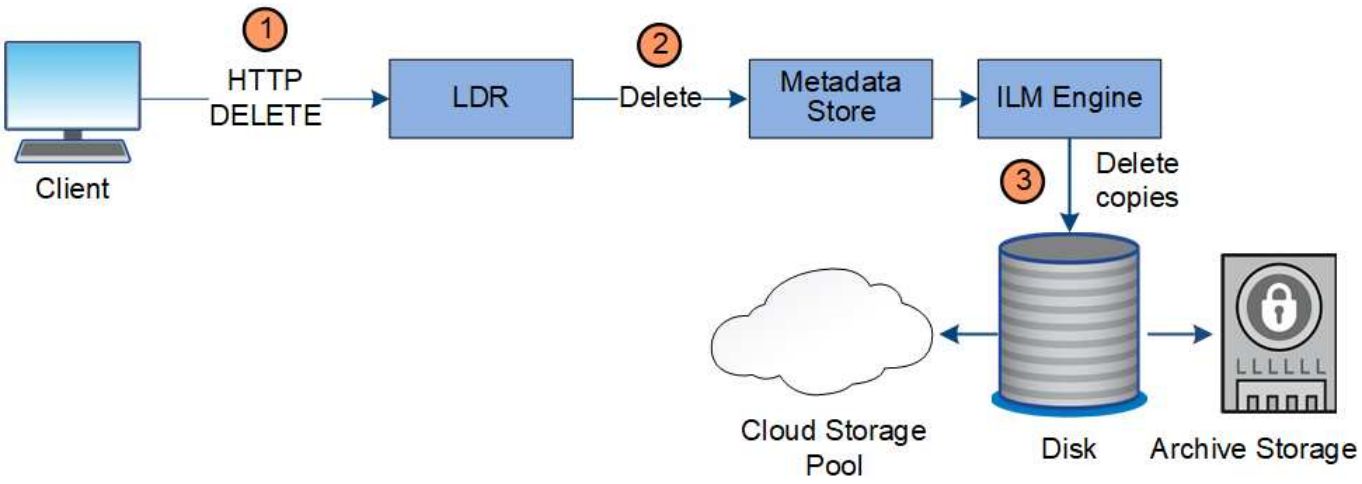
필요가 없습니다.

- * 클라이언트 삭제 요청 *: S3 클라이언트가 객체 삭제 요청을 실행할 수 있습니다. 클라이언트가 개체를 삭제하면 개체의 모든 복사본이 StorageGRID 시스템에서 제거됩니다.
- * 버킷에서 오브젝트 삭제 *: 테넌트 관리자 사용자는 이 옵션을 사용하여 StorageGRID 시스템에서 선택한 버킷에 있는 오브젝트 및 오브젝트 버전의 모든 복제본을 영구적으로 제거할 수 있습니다.
- * 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 라이프사이클이 구성된 경우 라이프사이클 만료 작업이 라이프사이클 필터와 일치하는 오브젝트에 대한 ILM 정책을 재정의합니다. 따라서 개체를 배치하기 위한 ILM 명령이 만료된 후에도 개체가 그리드에 유지될 수 있습니다.

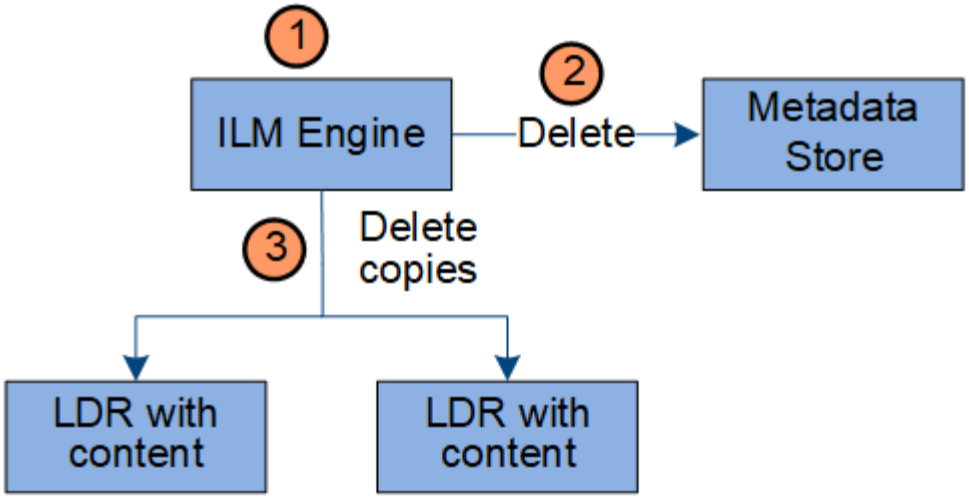
자세한 내용은 을 "오브젝트 삭제 방법" 참조하십시오.

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.

정보 수명 주기 관리

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

그리드에는 한 번에 하나의 활성 정책만 있습니다. 정책에는 여러 규칙이 포함될 수 있습니다.

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 또는 클라우드 스토리지 풀에 저장될 수 있습니다.
- 생성된 오브젝트 복사본의 유형입니다. 복사본을 복제하거나 삭제 코딩할 수 있습니다.
- 복제된 복사본의 경우 생성된 복사본 수입니다.
- 삭제 코딩 복사본의 경우 삭제 코딩 체계가 사용됩니다.
- 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.

ILM 규칙 예

예를 들어 ILM 규칙에서 다음을 지정할 수 있습니다.

- 테넌트 A에 속하는 객체에만 적용합니다
- 이러한 개체의 복제 복사본을 두 개 만들고 각 복사본을 다른 사이트에 저장합니다.
- 두 개의 복사본을 "영원히" 보존합니다. 즉, StorageGRID에서 자동으로 삭제하지 않습니다. 대신, StorageGRID는 이러한 객체가 클라이언트 삭제 요청에 의해 삭제되거나 버킷 수명 주기가 만료될 때까지 해당 객체를 유지합니다.
- 수집 동작에 균형 옵션을 사용합니다. 필요한 두 복제본을 모두 즉시 생성할 수 없는 경우 테넌트 A가 StorageGRID에 객체를 저장하는 즉시 2개 사이트 배치 명령이 적용됩니다.

  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 오브젝트의 배치, 기간 및 수집 동작을 제어합니다.

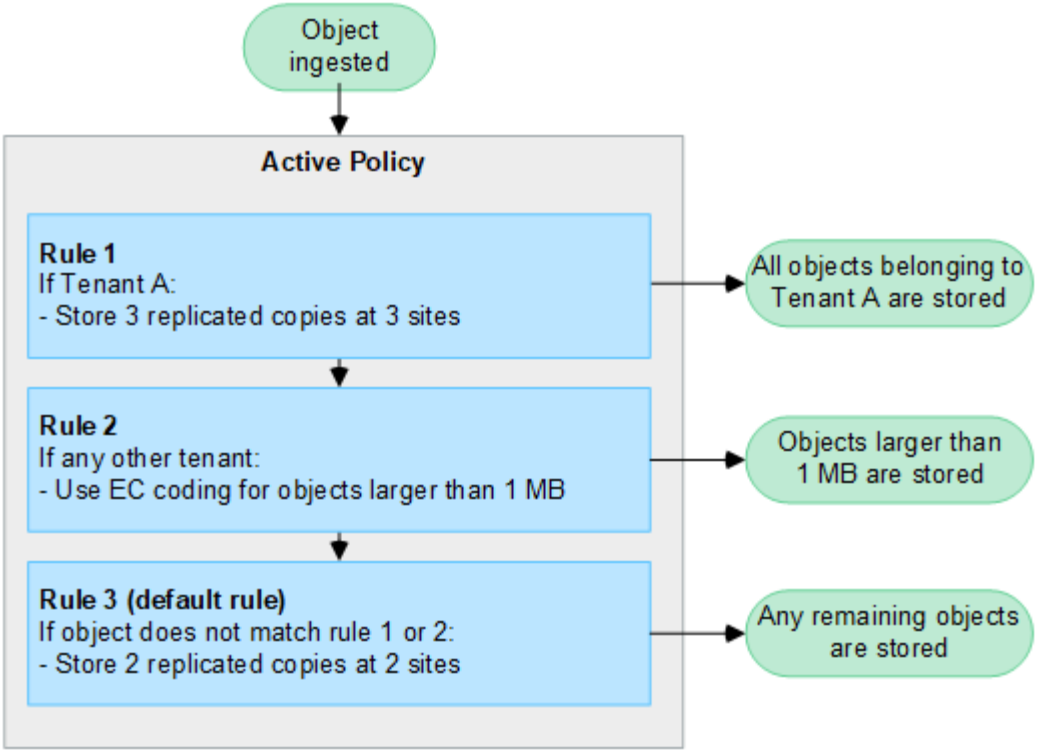
클라이언트가 개체를 StorageGRID에 저장하면 활성 정책에서 정렬된 ILM 규칙 집합에 대해 다음과 같이 개체가 평가됩니다.

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 일치가 이루어질 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

예를 들어 ILM 정책에 다음을 지정하는 세 가지 ILM 규칙이 포함될 수 있습니다.

- * 규칙 1: 테넌트 A * 에 대해 복제된 복사본
  - 테넌트 A에 속하는 모든 객체를 일치시킵니다
  - 이러한 객체를 3개의 사이트에 3개의 복제된 복제본으로 저장합니다.
  - 다른 테넌트에 속한 개체는 규칙 1에 의해 일치하지 않으므로 규칙 2에 대해 평가됩니다.
- * 규칙 2: 1MB * 이상의 개체에 대한 삭제 코딩
  - 다른 테넌트의 모든 객체를 일치하지만 1MB 이상인 경우에만 일치시킵니다. 이러한 큰 오브젝트는 3개의 사이트에서 6+3 삭제 코딩을 사용하여 저장됩니다.
  - 이(가) 1MB 이하의 객체와 일치하지 않으므로 이러한 오브젝트는 규칙 3에 대해 평가됩니다.
- * 규칙 3:2개 데이터 센터 2개 복사 * (기본값)
  - 정책의 마지막 기본 규칙입니다. 필터를 사용하지 않습니다.
  - 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"

StorageGRID를 살펴보십시오

Grid Manager를 살펴봅니다

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

Grid Manager는 각 릴리스와 함께 업데이트되며 이 페이지의 예제 스크린샷과 일치하지 않을 수 있습니다.

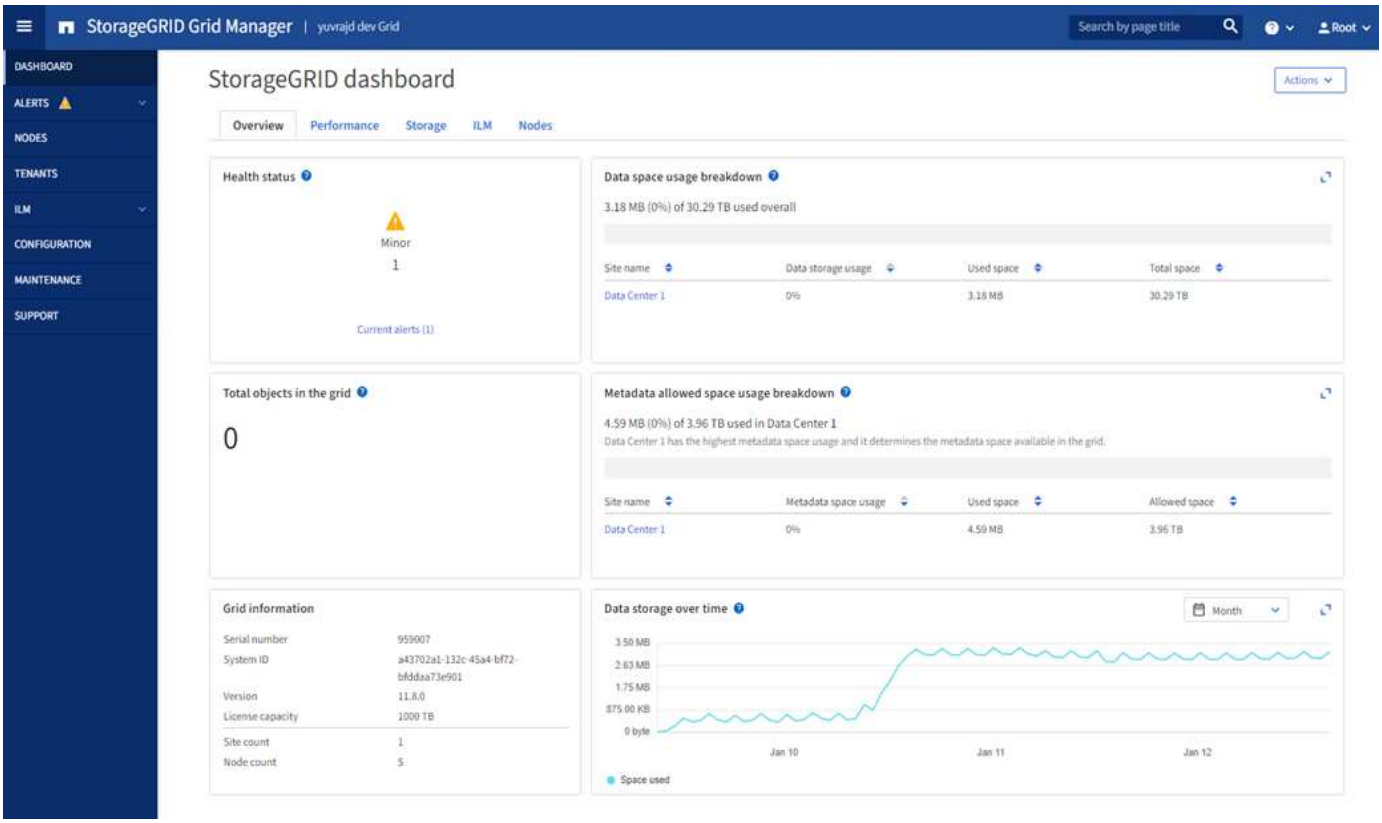
Grid Manager에 로그인하면 관리 노드에 연결됩니다. 각 StorageGRID 시스템에는 1개의 기본 관리 노드와 1차 관리자가 아닌 노드 수가 포함되어 있습니다. 모든 관리 노드에 연결할 수 있으며 각 관리 노드에는 StorageGRID 시스템의 유사한 보기가 표시됩니다.

을 사용하여 그리드 관리자에 액세스할 수 "지원되는 웹 브라우저"있습니다.

Grid Manager 대시보드

그리드 관리자에 처음 로그인할 때 대시보드를 사용하여 한 눈에 볼 수 "시스템 활동을 모니터링합니다"있습니다.

대시보드에는 시스템 상태 및 성능, 스토리지 사용, ILM 프로세스, S3 작업 및 그리드 노드의 정보가 포함되어 있습니다. 시스템을 효과적으로 모니터링하는 데 필요한 정보가 포함된 카드 모음에서 선택할 수 "대시보드를 구성합니다"있습니다.



각 카드에 표시된 정보에 대한 설명을 보려면 해당 카드의 도움말 아이콘을 선택하십시오.

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. 그리드 노드 및 테넌트 계정과 같은 항목의 이름별로 검색할 수도 있습니다.

도움말 메뉴

도움말 메뉴를 통해 다음 항목에 액세스할 수 있습니다.

- "FabricPool"및 "S3 설정" 마법사
- 현재 릴리즈에 대한 StorageGRID 문서 센터
- "API 설명서"
- 현재 설치되어 있는 StorageGRID 버전에 대한 정보입니다

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"알림을 관리합니다".

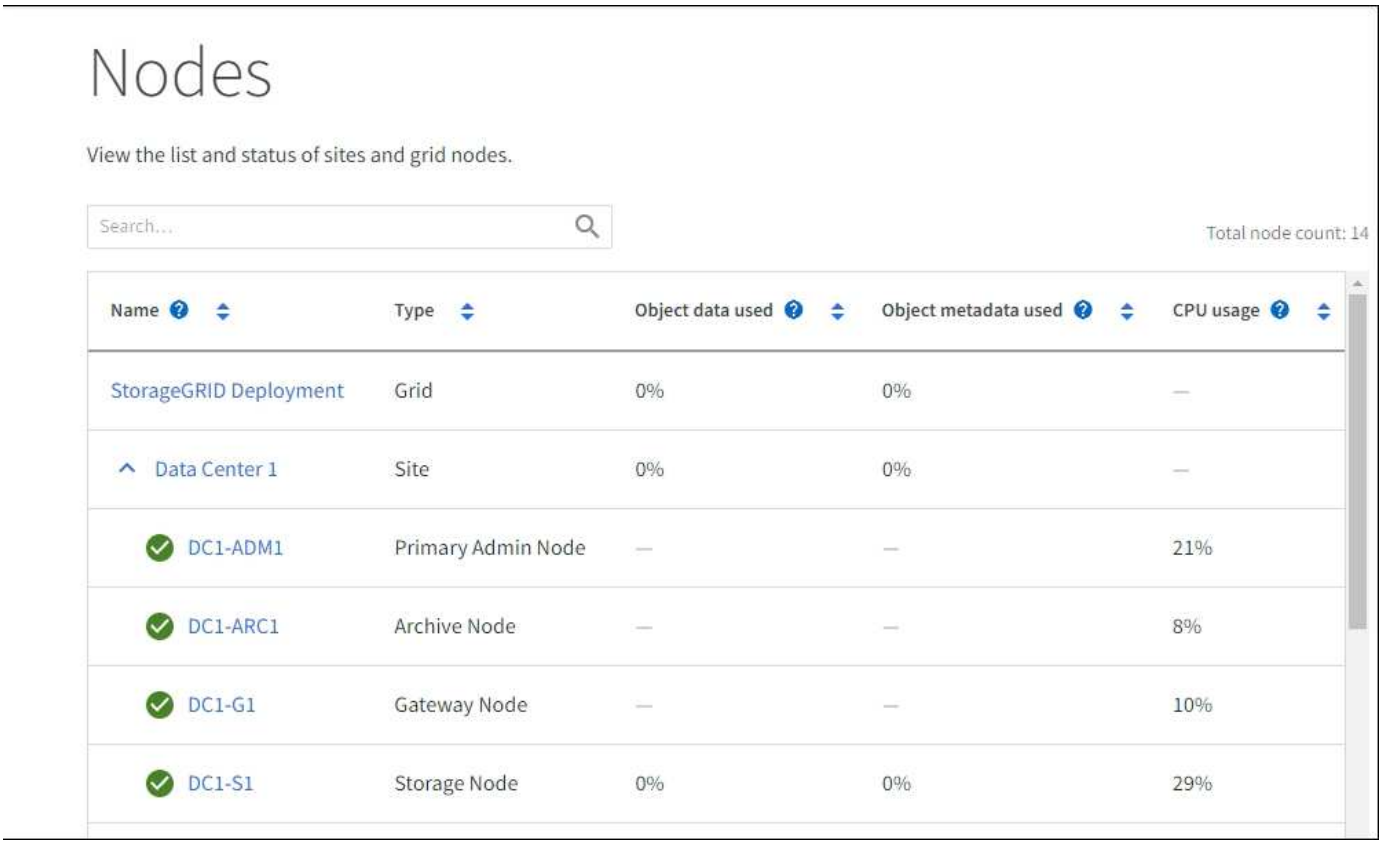
- 현재 경고를 검토합니다

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

노드 페이지

에는 "노드 페이지"전체 그리드, 그리드의 각 사이트 및 사이트의 각 노드에 대한 정보가 표시됩니다.

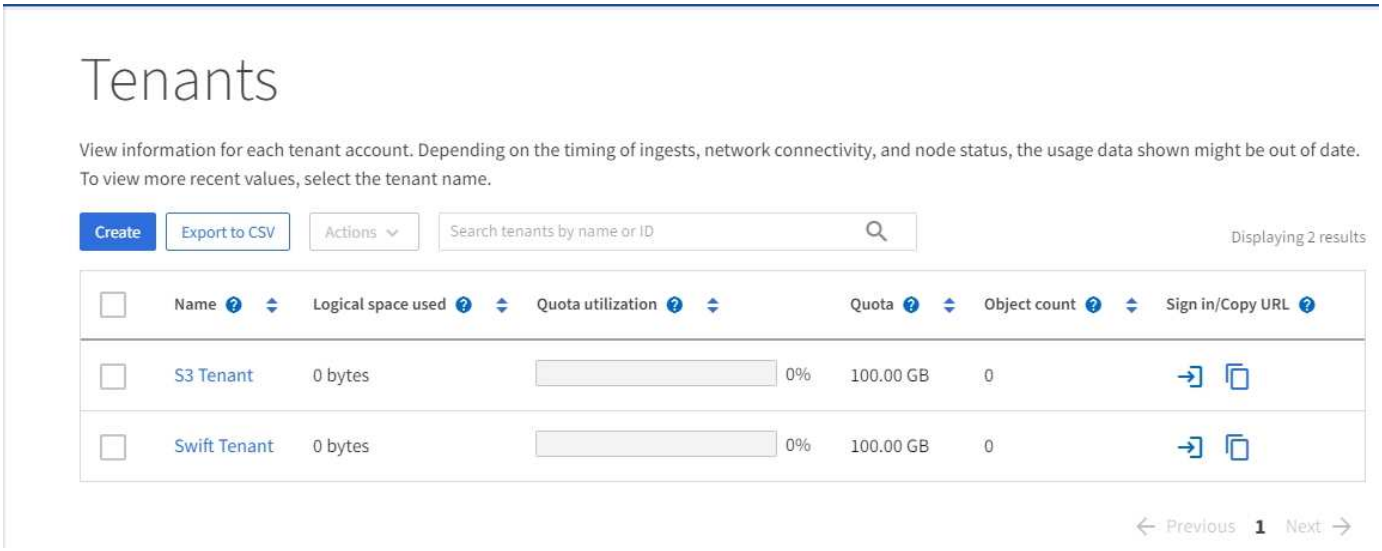
노드 홈 페이지에는 전체 그리드에 대한 결합된 메트릭이 표시됩니다. 특정 사이트 또는 노드에 대한 정보를 보려면 사이트 또는 노드를 선택합니다.



Tenants 페이지

를 "Tenants 페이지" 사용하면 "스토리지 테넌트 계정을 생성하고 모니터링합니다"StorageGRID 시스템을 사용할 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.



ILM 메뉴

을 "ILM 메뉴" 사용하여 데이터 내구성 및 가용성을 제어할 수 "정보 라이프사이클 관리(ILM) 규칙 및 정책을 구성합니다"있습니다. 개체 식별자를 입력하여 해당 개체의 메타데이터를 볼 수도 있습니다.

ILM 메뉴에서 ILM을 보고 관리할 수 있습니다.

- 규칙
- 정책
- 정책 태그
- 지원합니다
- 보관 등급
- 지역
- 개체 메타데이터 조회

구성 메뉴

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

네트워크 작업

네트워크 작업은 다음과 같습니다.

- "고가용성 그룹 관리"
- "로드 밸런서 엔드포인트 관리"
- "S3 엔드포인트 도메인 이름 구성 중"
- "트래픽 분류 정책 관리"
- "VLAN 인터페이스 구성"

보안 작업

보안 작업에는 다음이 포함됩니다.

- "보안 인증서 관리"
- "내부 방화벽 제어 관리"
- "키 관리 서버 구성"
- "TLS 및 SSH 정책""네트워크 및 개체 보안 옵션", 및 를 포함한 보안 설정 구성"인터페이스 보안 설정"
- 또는 에 대한 설정 구성 "스토리지 프록시""관리 프록시"

시스템 작업

시스템 작업은 다음과 같습니다.

- 를 사용하여 "그리드 통합"테넌트 계정 정보를 클론 복제하고 두 StorageGRID 시스템 간에 오브젝트 데이터를 복제합니다.
- 옵션을 활성화합니다(선택 사항)"저장된 객체를 압축합니다".
- "S3 오브젝트 잠금 관리"
- 및 등의 스토리지 옵션 이해"개체 분할""스토리지 볼륨 워터마크입니다"
- "삭제 코딩 프로필을 관리합니다"..

모니터링 작업

모니터링 작업에는 다음이 포함됩니다.

- "감사 메시지 및 로그 대상 구성"
- "SNMP 모니터링을 사용합니다"

액세스 제어 작업

액세스 제어 작업에는 다음이 포함됩니다.

- "관리 그룹 관리"
- "관리자 사용자 관리"
- "프로비저닝 암호"또는 변경 "노드 콘솔 암호"
- "ID 페더레이션 사용"
- "SSO 구성"

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.

- "서비스 해제 작업" 사용하지 않는 그리드 노드 및 사이트를 제거합니다
- "확장 작업" 새 그리드 노드 및 사이트를 추가합니다
- "그리드 노드 복구 절차" 장애가 발생한 노드를 교체하고 데이터를 복원합니다
- "절차 이름 바꾸기" 그리드, 사이트 및 노드의 표시 이름을 변경합니다
- "개체 존재 확인 작업" 개체 데이터의 존재 여부(정확도는 아님)를 확인합니다
- 를 "재부팅 롤링 중" 수행하여 여러 그리드 노드를 재시작합니다
- "볼륨 복원 작업"

시스템

수행할 수 있는 시스템 유지보수 작업은 다음과 같습니다.

- "StorageGRID 라이센스 정보 보기" 또는 "라이센스 정보를 업데이트하는 중입니다"
- 생성 및 다운로드 "복구 패키지"
- 선택한 어플라이언스에서 SANtricity OS 소프트웨어에 대한 소프트웨어 업그레이드, 핫픽스 및 업데이트를 포함한 StorageGRID 소프트웨어 업데이트 수행
  - "업그레이드 절차"
  - "핫픽스 절차"
  - "Grid Manager를 사용하여 SG6000 스토리지 컨트롤러에서 SANtricity OS를 업그레이드합니다"
  - "Grid Manager를 사용하여 SG5700 스토리지 컨트롤러에서 SANtricity OS를 업그레이드합니다"

네트워크

수행할 수 있는 네트워크 유지 보수 작업은 다음과 같습니다.

- "DNS 서버 구성"
- "그리드 네트워크 서브넷을 업데이트하는 중입니다"
- "NTP 서버 관리"

지원 메뉴

지원 메뉴는 기술 지원 부서에서 시스템을 분석하고 문제를 해결하는 데 도움이 되는 옵션을 제공합니다.

도구

지원 메뉴의 도구 섹션에서 다음을 수행할 수 있습니다.

- "AutoSupport를 구성합니다"
- "진단 유틸리티를 실행합니다" 그리드의 현재 상태
- "그리드 토폴로지 트리에 액세스합니다" 그리드 노드, 서비스 및 속성에 대한 자세한 정보를 보려면
- "로그 파일 및 시스템 데이터를 수집합니다"
- "지원 메트릭을 검토합니다"

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

알람(레거시)

기존 알람에 대한 정보는 이 버전의 설명서에서 제거되었습니다. 을 "경고 및 알람 관리(StorageGRID 11.8 설명서)"참조하십시오.

기타

지원 메뉴의 기타 섹션에서 다음을 수행할 수 있습니다.

- 관리 "링크 비용"
- "네트워크 관리 시스템(NMS)"항목을 봅니다
- 관리 "스토리지 워터마크"

테넌트 관리자를 탐색합니다

는 "테넌트 관리자"테넌트 사용자가 액세스하여 스토리지 계정을 구성, 관리 및 모니터링하는 브라우저 기반 그래픽 인터페이스입니다.

Tenant Manager는 각 릴리스에서 업데이트되며 이 페이지의 예제 스크린샷과 일치하지 않을 수 있습니다.

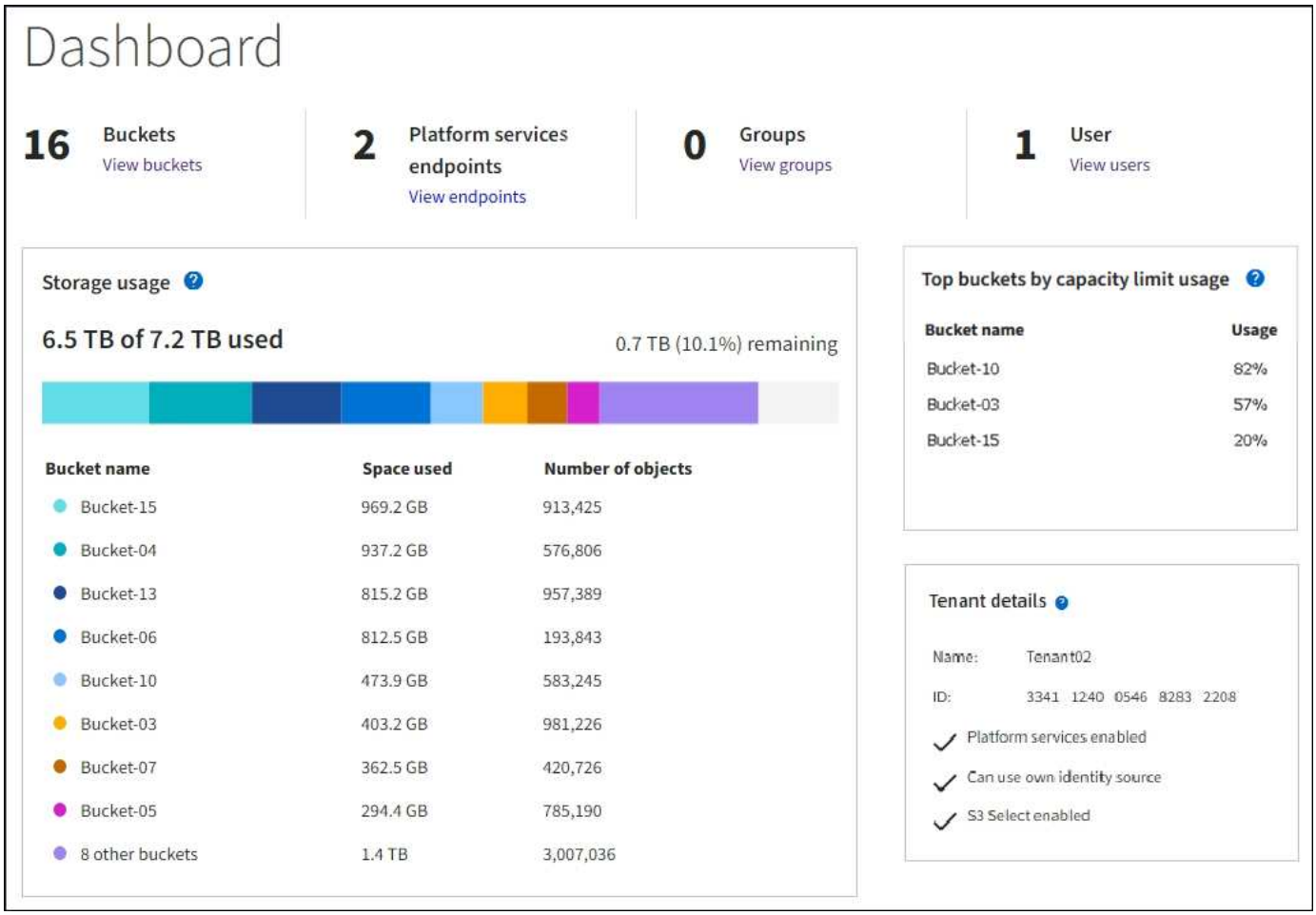
테넌트 사용자가 테넌트 관리자에 로그인하면 해당 사용자는 관리 노드에 연결됩니다.

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)**

스토리지 메뉴는 S3 테넌트 계정에만 제공됩니다. 이 메뉴를 통해 S3 사용자는 액세스 키를 관리하고, 버킷을 생성, 관리 및 삭제할 수 있으며, 플랫폼 서비스 끝점을 관리하고, 사용할 수 있는 모든 그리드 페더레이션 연결을 볼 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 자신의 버킷에 대해 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 값을 업데이트합니다
- 마지막 액세스 시간 업데이트를 설정 및 해제합니다
- 개체 버전 관리를 사용하거나 일시 중지합니다
- S3 오브젝트 잠금 기본 보존 업데이트
- CORS(Cross-Origin Resource Sharing) 구성
- 버킷의 모든 오브젝트를 삭제합니다
- 빈 버킷을 삭제합니다
- 버킷 오브젝트를 관리하려면 을 사용합니다"S3 콘솔"

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

- Amazon Simple Notification Service를 지원하는 대상 서비스로 보낼 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.

그리드 페더레이션 연결

그리드 관리자가 테넌트 계정에 대한 그리드 페더레이션 연결 사용을 설정한 경우 루트 액세스 권한이 있는 S3 테넌트 사용자는 연결 이름을 볼 수 있습니다. 또한 교차 그리드 복제가 활성화된 각 버킷의 버킷 세부 정보 페이지에 액세스합니다. 그리고 버킷 데이터가 연결의 다른 그리드에 복제되었을 때 발생하는 가장 최근의 오류를 확인합니다. 을 "그리드 페더레이션 연결을 봅니다"참조하십시오.

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.

네트워킹 지침

네트워킹 지침

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 아키텍처에 익숙해지십시오."StorageGRID에 대해 자세히 알아보십시오"

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

어플라이언스 노드를 설치합니다

- "어플라이언스 하드웨어를 설치합니다"

소프트웨어 기반 노드 설치

- "Red Hat Enterprise Linux에 StorageGRID를 설치합니다"
- "Ubuntu 또는 Debian에 StorageGRID를 설치합니다"
- "VMware에 StorageGRID를 설치합니다"

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(옵션), VLAN 네트워크(옵션)
클라이언트 트래픽	S3 클라이언트의 모든 오브젝트 스토리지 요청을 포함하여 외부 클라이언트 애플리케이션과 그리드 간에 이동하는 트래픽	클라이언트 네트워크(옵션), 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. "내부 그리드 노드 통신"및 을 "외부 통신"참조하십시오.

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)	윤리2

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

소프트웨어 기반 노드

- "Red Hat Enterprise Linux에 StorageGRID를 설치합니다"
- "Ubuntu 또는 Debian에 StorageGRID를 설치합니다"

- "VMware에 StorageGRID를 설치합니다"

어플라이언스 노드

- "SG6160 스토리지 어플라이언스"
- "SGF6112 스토리지 어플라이언스"
- "SG6000 스토리지 어플라이언스"
- "SG5800 스토리지 어플라이언스"
- "SG5700 스토리지 어플라이언스"
- "SG110 및 SG1100 서비스 어플라이언스"
- "SG100 및 SG1000 서비스 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 "고가용성 그룹을 관리합니다"참조하십시오.

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. 구성되면 S3와 같은 클라이언트 애플리케이션용 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. "방화벽 제어 관리"및 을 "로드 밸런서 엔드포인트를 구성합니다"참조하십시오.

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 노드가 StorageGRID 로드 밸런서 서비스에 대한 액세스와 그리드에 대한 S3 클라이언트 액세스를 제공합니다.
- 스토리지 노드: 이러한 노드가 S3 프로토콜과 클라우드 스토리지 풀 및 CloudMirror 복제 서비스에 대한 액세스를 제공합니다.
- 관리 노드: 테넌트 사용자가 관리 네트워크를 사용하지 않고 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 트렁크 인터페이스를 추가할 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 노드에 대한 클라이언트 또는 관리자 액세스에는 VLAN 인터페이스를 사용할 수 없습니다.

지침 및 지침은 을 "VLAN 인터페이스를 구성합니다"참조하십시오.

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

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.

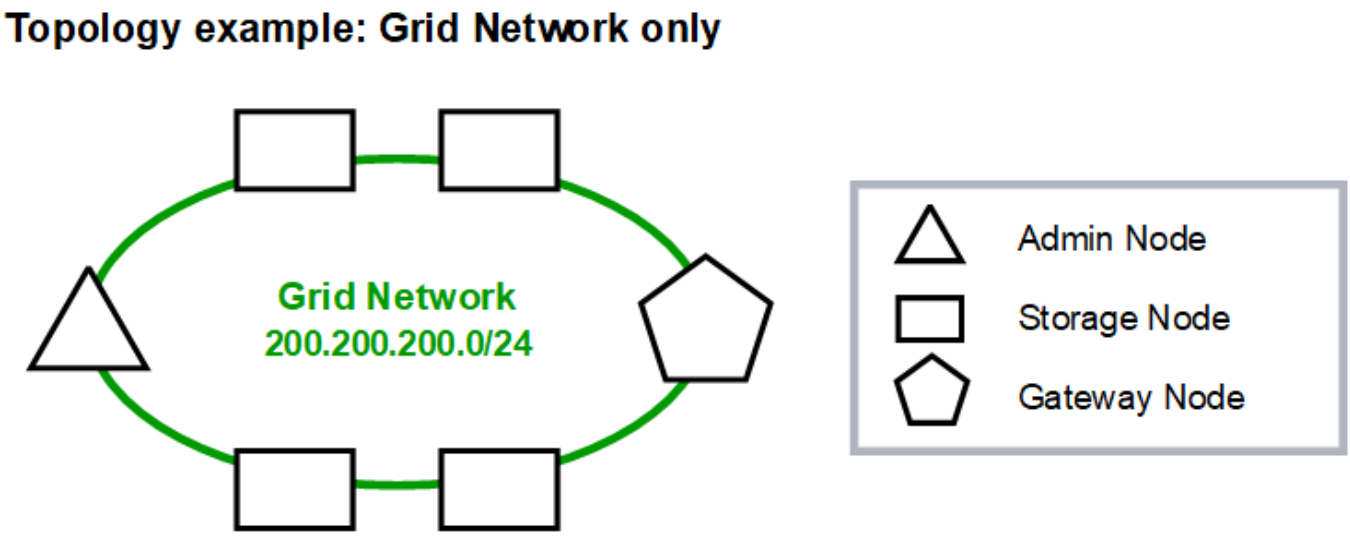
구성 중에 모든 그리드 네트워크 서브넷을 그리드 네트워크 서브넷 목록(GNSL)에 추가해야 합니다. 이 목록에는 모든

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 예에서는 S3 클라이언트 요청, 관리 및 유지보수 기능과 관련된 트래픽을 포함하여 모든 트래픽이 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

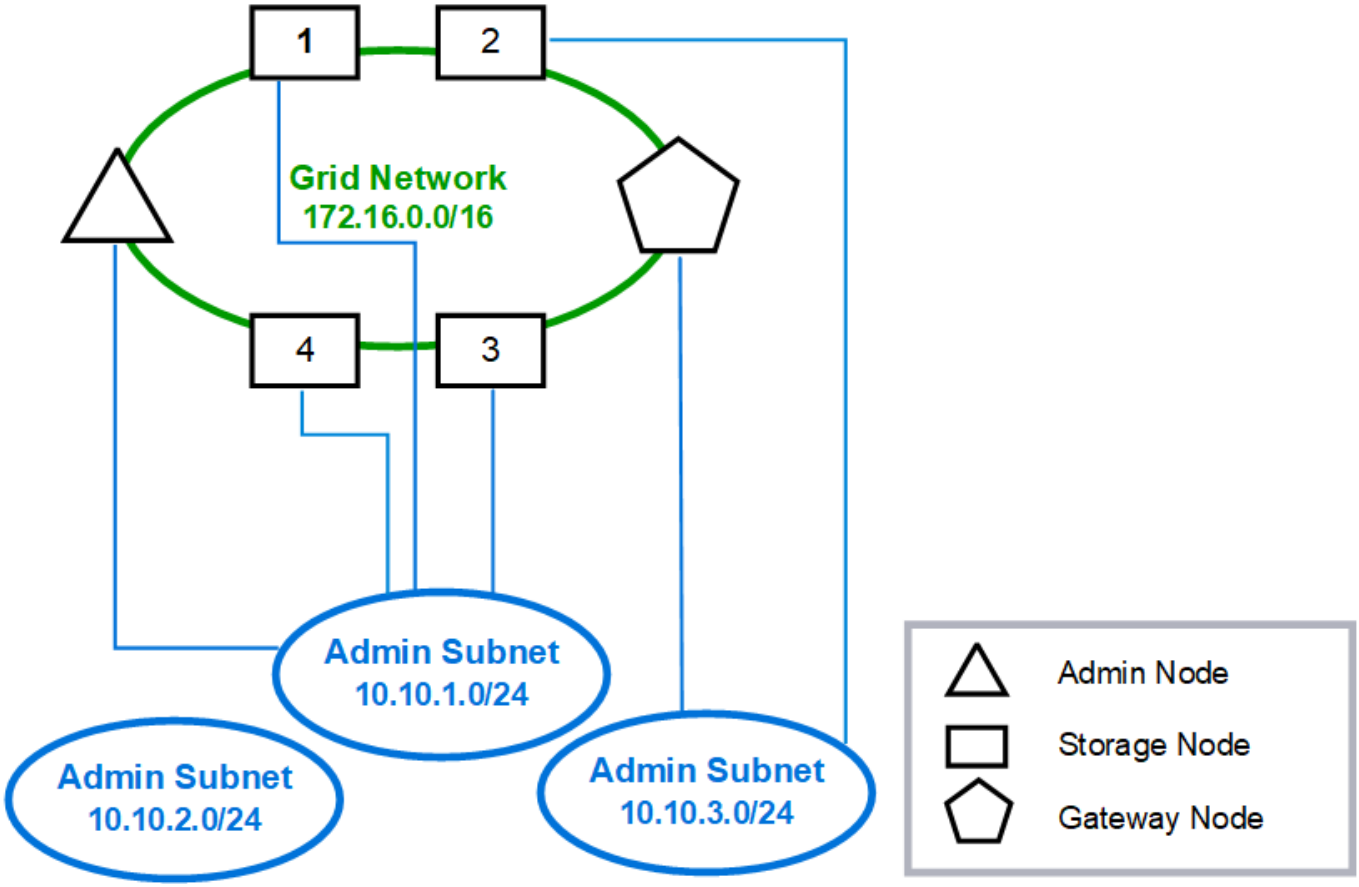
관리 네트워크 보유는 선택 사항입니다. 관리 네트워크 및 그리드 네트워크를 사용할 수 있는 한 가지 방법은 각 노드에 대해 라우팅 가능한 그리드 네트워크 및 경계 관리자 네트워크를 구성하는 것입니다.

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 클라이언트 요청 및 객체 관리와 관련된 트래픽에 사용되고 관리 기능은 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

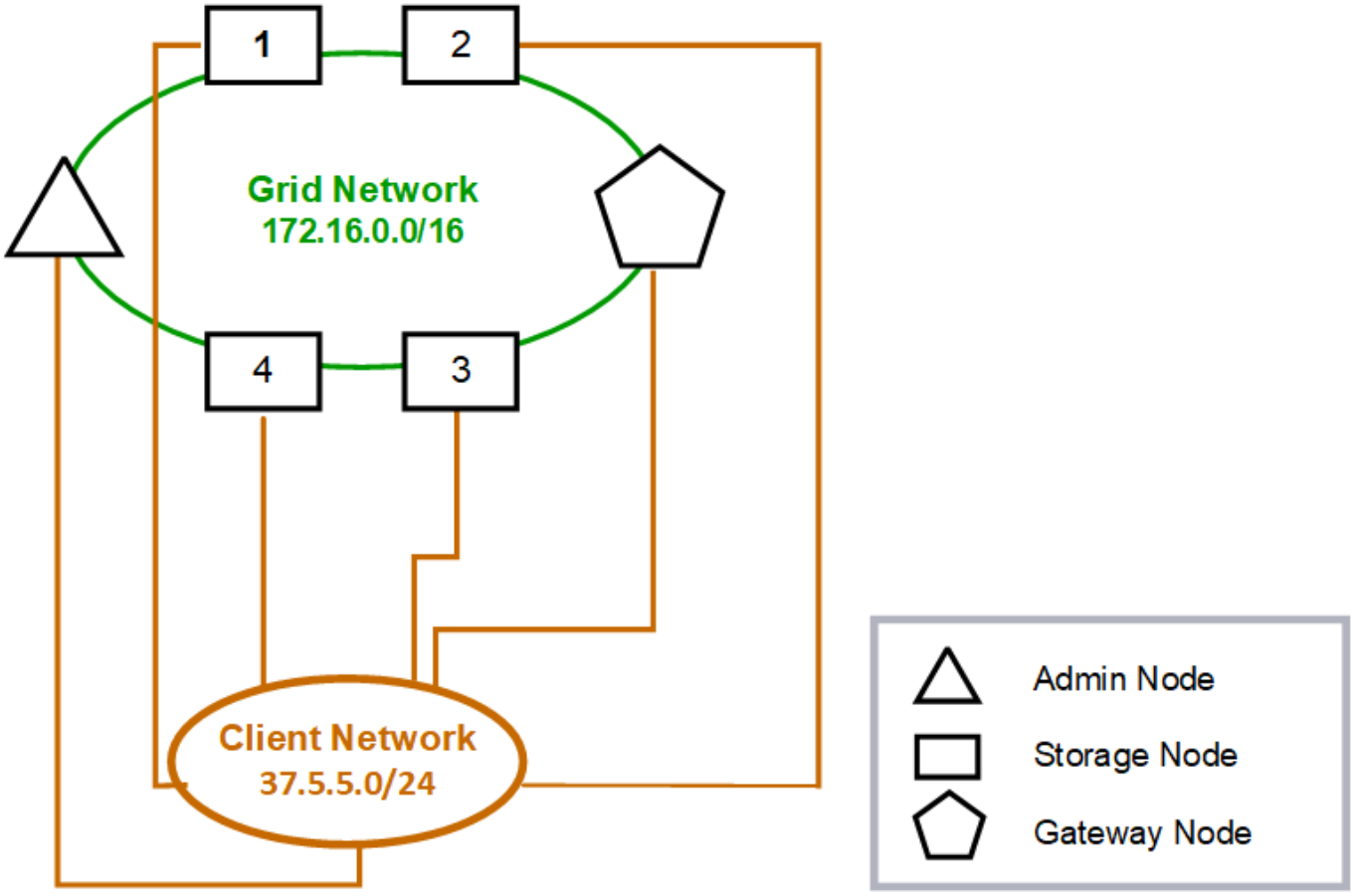
클라이언트 네트워크 보유는 선택 사항입니다. 클라이언트 네트워크를 사용하면 클라이언트 네트워크 트래픽(예: S3)을 그리드 내부 트래픽과 분리할 수 있으므로 그리드 네트워킹의 보안이 더욱 강화됩니다. 관리 네트워크가 구성되지 않은 경우 클라이언트 또는 그리드 네트워크에서 관리 트래픽을 처리할 수 있습니다.

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 클라이언트 요청 및 관리 기능에 사용되고 그리드 네트워크는 내부 객체 관리 작업에 사용됩니다.

Topology example: Grid and Client Networks



Provisioned

GNSL → 172.16.0.0/16

Nodes	Grid Network IP/mask	Client Network IP/mask	Client Network 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

관련 정보

"노드 네트워크 구성을 변경합니다"

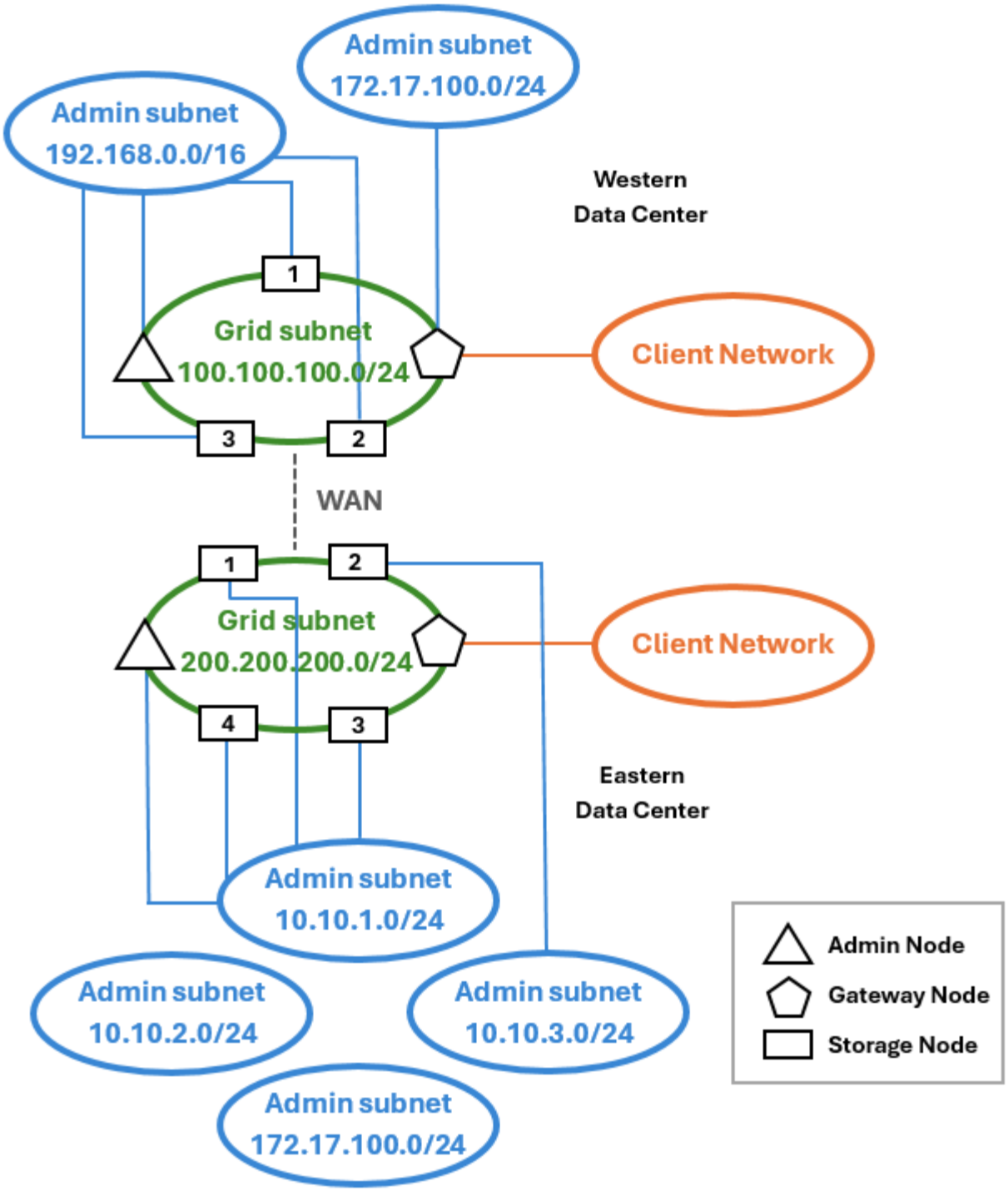
3개의 네트워크를 모두 위한 토폴로지

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 클라이언트 요청과 관련된 트래픽에 사용됩니다.

토폴로지 예: 그리드, 관리 및 클라이언트 네트워크



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 *: 관리 노드에서 또는 고객이 구성한 프록시로 아웃바운드 TCP 연결 `support.netapp.com`.
- * 외부 키 관리 서버 *: 노드 암호화가 활성화된 각 어플라이언스 노드에서 아웃바운드 TCP 연결.
- S3 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 서버에 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 설치 후 Change IP(IP 변경) 도구를 사용하여 이러한 네트워크를 구성할 수 있습니다(참조"IP 주소를 구성합니다").

S3 클라이언트 연결 및 SSH, Grid Manager 및 Tenant Manager 관리 연결만 VLAN 인터페이스를 통해 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.

실제 최소 WAN 대역폭 요구 사항은 클라이언트 작업 및 ILM 보호 체계에 따라 다릅니다. 최소 WAN 대역폭 요구 사항을 추정하는 데 도움이 필요한 경우 NetApp 프로페셔널 서비스 컨설턴트에게 문의하십시오.

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

"고가용성 그룹을 관리합니다"참조하십시오.

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)가 될 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 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 "로드 밸런서 엔드포인트를 구성합니다 "참조하십시오.
- 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.

관련 정보

"노드 네트워크 구성을 변경합니다"

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.

Bond 또는 Bridge 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.

또는 "Ubuntu 또는 Debian" 배포에 대한 설치 지침을 "Red Hat Enterprise Linux"참조하십시오.

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(노드 설치 전) *: "노드 구성 파일을 생성합니다"
  - * Ubuntu 또는 Debian (노드를 설치하기 전에) *: "노드 구성 파일을 생성합니다"
  - * RHEL, 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 LAN 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
	• 최소 LAN 대역폭 *	관리자	10Gbps
1Gbps	1Gbps	게이트웨이	10Gbps
1Gbps	10Gbps	스토리지	10Gbps

노드 유형입니다	네트워크 유형입니다		
1Gbps	10Gbps	아카이브	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)"
- "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

및 에 설명된 바와 같이 "테넌트를 위한 플랫폼 서비스 관리""플랫폼 서비스 관리"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 경로를 사용하는 경우 을 사용하여 인바운드 연결을 제한할 수 "신뢰할 수 없는 클라이언트 네트워크 기능입니다"있습니다.

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 "클라우드 스토리지 풀이란 무엇입니까"참조하십시오.

플랫폼 서비스 및 클라우드 스토리지 풀을 위한 포트입니다

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

- **80**: 로 시작하는 끝점 URI입니다 `http`
- **443**: 로 시작하는 끝점 URI입니다 `https`

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

투명하지 않은 프록시 서버를 사용하는 경우 인터넷의 끝점과 같은 외부 끝점으로 메시지를 보낼 수 있도록 허용해야 "스토리지 프록시 설정을 구성합니다"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.

제품의 포트 연결 모드에 대한 자세한 내용은 다음을 참조하십시오.

- "포트 본드 모드(SG6160)"
- "포트 본드 모드(SGF6112)"
- "포트 본드 모드(SG6000-CN 컨트롤러)"
- "포트 본드 모드(SG5800 컨트롤러)"
- "포트 결합 모드(E5500SG 컨트롤러)"
- "포트 본드 모드(SG110 및 SG1100)"
- "포트 본드 모드(SG100 및 SG1000)"

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 Grid Manager, Python 스크립트 또는 Installation API를 사용하여 그리드를 구성하고 등록된 노드를 승인할 수 `configure-storagegrid.py` 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").

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.

  > 그리드 네트워크 구성이 DHCP에 의해 변경될 때 노드가 재부팅되므로 DHCP 변경이 여러 노드에 동시에 영향을 미칠 경우 운영이 중단될 수 있습니다.

- 그리드 노드의 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 변경하려면 IP 변경 절차를 사용해야 합니다. 을 "IP 주소를 구성합니다"참조하십시오.
- 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

내부 그리드 노드 통신

StorageGRID 내부 방화벽을 사용하면 그리드 네트워크의 특정 포트에 연결할 수 있습니다. 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 가 구성된 경우에만 "고가용성 그룹"필요합니다.

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 Linux에 StorageGRID를 설치합니다"
- "Ubuntu 또는 Debian에 StorageGRID를 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 참조하십시오"VMware에 StorageGRID를 설치합니다".

어플라이언스 노드에 대한 지침

엔터프라이즈 네트워킹 정책에서 이러한 포트에 대한 액세스를 제한하는 경우 StorageGRID 어플라이언스 설치 프로그램을 사용하여 포트를 재매핑할 수 있습니다. 을 "옵션: 어플라이언스인 네트워크 포트를 재활용합니다 "참조하십시오.

StorageGRID 내부 포트

포트	**TCP** 또는 **UDP**입니다	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.
123	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.

포트	**TCP** 또는 **UDP**입니다	보낸 사람	를 선택합니다	세부 정보
1055	TCP	모든 노드	기본 관리자 노드	설치, 확장, 복구 및 기타 유지 보수 절차를 위한 내부 트래픽
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	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
1511	TCP	모든 노드	스토리지 노드	메타데이터 내부 트래픽.
7001	TCP	스토리지 노드	스토리지 노드	Cassandra TLS 노드 간 클러스터 통신.
7443	TCP	모든 노드	기본 관리자 노드	설치, 확장, 복구, 기타 유지보수 절차 및 오류 보고를 위한 내부 트래픽.
8011	TCP	모든 노드	기본 관리자 노드	설치, 확장, 복구 및 기타 유지 보수 절차를 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:

포트	**TCP** 또는 **UDP**입니다	보낸 사람	를 선택합니다	세부 정보
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	E-Series SANtricity System Manager에서 기본 관리자 노드로 AutoSupport 패키지를 전달하는 데 StorageGRID 어플라이언스에서 사용됩니다.
10342를 참조하십시오	TCP	모든 노드	기본 관리자 노드	설치, 확장, 복구 및 기타 유지 보수 절차를 위한 내부 트래픽
18000	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.
18086	TCP	모든 그리드 노드	모든 스토리지 노드	LDR 서비스와 관련된 내부 트래픽입니다.
18200	TCP	관리/스토리지 노드	스토리지 노드	클라이언트 요청에 대한 추가 통계입니다.

포트	**TCP** 또는 **UDP**입니다	보낸 사람	를 선택합니다	세부 정보
19000	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 정책이 포트 중 하나에 대한 액세스를 제한하는 경우 다음 중 하나를 수행할 수 있습니다.

- "부하 분산 장치 엔드포인트"사용자 정의 포트에 대한 액세스를 허용하는 데 사용됩니다.
- 노드를 구축할 때 포트를 다시 매핑합니다. 하지만 로드 밸런서 끝점을 다시 매핑하면 안 됩니다. StorageGRID 노드의 포트 재매핑에 대한 정보를 참조하십시오.
  - "Red Hat Enterprise Linux에서 StorageGRID에 대한 포트 재매핑 키"
  - "Ubuntu 또는 Debian에서 StorageGRID에 대한 포트 재매핑 키"
  - "VMware에서 StorageGRID에 대한 포트를 재매핑합니다"
  - "옵션: 어플라이언스인 네트워크 포트를 재활용합니다"

외부 통신에 사용되는 포트

다음 표는 노드로의 트래픽에 사용되는 포트를 보여줍니다.

이 목록에는 로 구성될 수 있는 포트가 "부하 분산 장치 엔드포인트"포함되어 있지 않습니다.

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 22 대신 포트 2022를 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	DNS에 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	AWS로 전송된 플랫폼 서비스 메시지 또는 HTTP를 사용하는 기타 외부 서비스에 사용됩니다. 테넌트는 끝점을 만들 때 기본 HTTP 포트 설정인 80을 재정의할 수 있습니다.
80	TCP	HTTP	스토리지 노드	설치하고	클라우드 스토리지 풀에서는 HTTP를 사용하는 AWS 타겟으로 전송된 요청을 풀링합니다. 그리드 관리자는 클라우드 스토리지 풀을 구성할 때 기본 HTTP 포트 설정 80을 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. • 참고: * NFS에 대한 지원은 더 이상 사용되지 않으며 향후 릴리스에서 제거될 예정입니다.
123	UDP입니다	NTP	기본 NTP 노드입니다	외부 NTP	네트워크 시간 프로토콜 서비스. 또한 주 NTP 소스로 선택된 노드는 외부 NTP 시간 소스와 클록 시간을 동기화합니다.

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 노드도 경고 데이터를 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. • 참고 *: Grid Manager 포트 443 또는 8443을 닫으면 사용자를 포함하여 차단된 포트에 현재 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다. 권한 있는 IP 주소를 구성하려면 를 "방화벽 제어를 구성합니다"참조하십시오.
443	TCP	HTTPS	관리자 노드	Active Directory를 클릭합니다	SSO(Single Sign-On)가 활성화된 경우 Active Directory에 연결하는 관리 노드에서 사용됩니다.

포트	**TCP** 또는 **UDP**입니다	프로토콜	보낸 사람	를 선택합니다	세부 정보
443	TCP	HTTPS	ADC가 있는 스토리지 노드	설치하고	AWS로 전송된 플랫폼 서비스 메시지 또는 HTTPS를 사용하는 기타 외부 서비스에 사용됩니다. 테넌트는 끝점을 만들 때 기본 HTTP 포트 설정인 443을 재정의할 수 있습니다.
443	TCP	HTTPS	스토리지 노드	설치하고	클라우드 스토리지 풀에서는 HTTPS를 사용하는 AWS 타겟으로 전송된 요청을 풀링합니다. 그리드 관리자는 클라우드 스토리지 풀을 구성할 때 기본 HTTPS 포트 설정 443을 재정의할 수 있습니다.
903	TCP	NFS 를 참조하십시오	NFS 클라이언트	관리자 노드	NFS 기반 감사 내보내기에 (`rpc.mountd`사용됨). • 참고: * 이 포트는 NFS 기반 감사 내보내기가 활성화된 경우에만 필요합니다. • 참고: * NFS에 대한 지원은 더 이상 사용되지 않으며 향후 릴리스에서 제거될 예정입니다.
2022년	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.
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. • 참고: * NFS에 대한 지원은 더 이상 사용되지 않으며 향후 릴리스에서 제거될 예정입니다.
5353	UDP입니다	mDNS	모든 노드	모든 노드	전체 그리드 IP 변경 및 설치, 확장 및 복구 중에 기본 관리 노드 검색에 사용되는 멀티캐스트 DNS(mDNS) 서비스를 제공합니다.
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.

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. • 참고 *: Grid Manager 포트 443 또는 8443을 닫으면 사용자를 포함하여 차단된 포트에 현재 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다. 권한 있는 IP 주소를 구성하려면 를 "방화벽 제어를 구성합니다"참조하십시오.
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.
9092	TCP	카프카	ADC가 있는 스토리지 노드	Kafka 클러스터	Kafka 클러스터로 전송되는 플랫폼 서비스 메시지에 사용됩니다. 테넌트는 엔드포인트를 생성할 때 기본 Kafka 포트 설정인 9092를 재정의할 수 있습니다.
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 연결됩니다.
18083	TCP	HTTPS	SWIFT 클라이언트	스토리지 노드	Swift 클라이언트 트래픽이 스토리지 노드(HTTPS)로 직접 연결됩니다.
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.

포트	**TCP** 또는 **UDP**입니다	프로토콜	보낸 사람	를 선택합니다	세부 정보
23000-23999 을 참조하십시오	TCP	HTTPS	그리드 간 복제를 위한 소스 그리드의 모든 노드	교차 그리드 복제를 위한 대상 그리드의 관리 노드 및 게이트웨이 노드	이 포트 범위는 그리드 페더레이션 연결용으로 예약되어 있습니다. 지정된 접속의 두 그리드는 동일한 포트를 사용합니다.

StorageGRID를 빠르게 시작합니다

모든 StorageGRID 시스템을 구성하고 사용하려면 다음 단계를 따르십시오.

데이터 학습, 계획 및 수집

NetApp 어카운트 담당자와 협력하여 새로운 StorageGRID 시스템의 옵션을 파악하고 계획을 수립합니다. 다음과 같은 질문을 고려하십시오.

- 처음에 그리고 나중에 어느 정도의 오브젝트 데이터를 저장할 것으로 예상하십니까?
- 얼마나 많은 사이트가 필요합니까?
- 각 사이트에 얼마나 많은 노드 유형이 필요합니까?
- 어떤 StorageGRID 네트워크를 사용하시겠습니까?
- 그리드를 사용해 객체를 저장하는 사람은 누구입니까? 어떤 애플리케이션을 사용합니까?
- 특별한 보안 또는 보관 요구 사항이 있습니까?
- 법률 또는 규정 요구 사항을 준수해야 합니까?

필요한 경우 NetApp 프로페셔널 서비스 컨설턴트와 함께 NetApp ConfigBuilder 툴에 액세스하여 새 시스템을 설치 및 구축할 때 사용할 구성 워크북을 작성합니다. 또한 이 도구를 사용하여 StorageGRID 어플라이언스 구성을 자동화할 수도 있습니다. 을 "어플라이언스 설치 및 구성 자동화"참조하십시오.

"StorageGRID에 대해 자세히 알아보십시오"및 을 "네트워킹 지침"검토합니다.

노드 설치

StorageGRID 시스템은 개별 하드웨어 기반 노드와 소프트웨어 기반 노드로 구성됩니다. 먼저 각 어플라이언스 노드에 대한 하드웨어를 설치하고 각 Linux 또는 VMware 호스트를 구성합니다.

설치를 완료하려면 각 어플라이언스 또는 소프트웨어 호스트에 StorageGRID 소프트웨어를 설치하고 노드를 그리드에 연결합니다. 이 단계에서는 NTP 및 DNS 서버에 대한 사이트 및 노드 이름, 서브넷 세부 정보 및 IP 주소를 제공합니다.

방법 알아보기:

- "어플라이언스 하드웨어를 설치합니다"

- "Red Hat Enterprise Linux에 StorageGRID를 설치합니다"
- "Ubuntu 또는 Debian에 StorageGRID를 설치합니다"
- "VMware에 StorageGRID를 설치합니다"

3 로그인하여 시스템 상태를 확인합니다

기본 관리 노드를 설치하는 즉시 그리드 관리자에 로그인할 수 있습니다. 여기에서 새 시스템의 일반적인 상태를 검토하고, AutoSupport 및 경고 이메일을 설정하고, S3 엔드포인트 도메인 이름을 설정할 수 있습니다.

방법 알아보기:

- "Grid Manager에 로그인합니다"
- "시스템 상태를 모니터링합니다"
- "AutoSupport를 구성합니다"
- "알림에 대한 이메일 알림을 설정합니다"
- "S3 끝점 도메인 이름을 구성합니다"

4 구성 및 관리

새 StorageGRID 시스템에 대해 수행해야 하는 구성 작업은 그리드 사용 방법에 따라 다릅니다. 최소한 시스템 액세스를 설정하고, FabricPool 및 S3 마법사를 사용하고, 다양한 스토리지 및 보안 설정을 관리합니다.

방법 알아보기:

- "StorageGRID 액세스를 제어합니다"
- "S3 설정 마법사를 사용합니다"
- "FabricPool 설정 마법사를 사용합니다"
- "보안 관리"
- "시스템 강화"

5 **ILM**을 설정합니다

하나 이상의 ILM 규칙으로 구성된 ILM(정보 수명 주기 관리) 정책을 구성하여 StorageGRID 시스템의 모든 개체에 대한 배치 및 기간을 제어할 수 있습니다. ILM 규칙은 StorageGRID에 오브젝트 데이터의 복사본을 만들고 배포하는 방법과 시간이 지남에 따라 이러한 복사본을 관리하는 방법을 지시합니다.

방법 알아보기: "ILM을 사용하여 개체를 관리합니다"

6 **StorageGRID**를 사용합니다

초기 구성이 완료된 후 StorageGRID 테넌트 계정은 S3 클라이언트 애플리케이션을 사용하여 오브젝트를 수집, 검색 및 삭제할 수 있습니다.

방법 알아보기:

- "테넌트 계정을 사용합니다"
- "S3 REST API를 사용합니다"

모니터링하고 문제 해결

시스템이 가동되어 실행 중인 경우 정기적으로 해당 작업을 모니터링하고 모든 경고를 문제 해결 및 해결해야 합니다. 또한 외부 syslog 서버를 구성하거나 SNMP 모니터링을 사용하거나 추가 데이터를 수집할 수도 있습니다.

방법 알아보기:

- "StorageGRID 모니터링"
- "StorageGRID 문제를 해결합니다"

확장, 유지 관리, 복구

노드 또는 사이트를 추가하여 시스템의 용량 또는 기능을 확장할 수 있습니다. 또한 다양한 유지보수 절차를 수행하여 장애를 복구하거나 StorageGRID 시스템을 최신 상태로 유지하고 효율적으로 수행할 수 있습니다.

방법 알아보기:

- "그리드를 확장합니다"
- "그리드를 유지합니다"
- "노드 복구"

StorageGRID 설치, 업그레이드 및 핫픽스

StorageGRID 어플라이언스

StorageGRID 스토리지 및 서비스 어플라이언스를 설치, 구성 및 유지 관리하는 방법에 대해 알아보려면 를 "StorageGRID 어플라이언스 설명서" 참조하십시오.

Red Hat Enterprise Linux에 StorageGRID를 설치합니다

Red Hat Enterprise Linux에 StorageGRID를 설치하기 위한 빠른 시작

RHEL(Red Hat Enterprise Linux) Linux StorageGRID 노드를 설치하려면 다음 단계를 따르십시오.

1 준비

- 에 대해 자세히 "StorageGRID 아키텍처 및 네트워크 토폴로지"알아보십시오.
- 에 대해 자세히 "StorageGRID 네트워킹"알아보십시오.
- 를 수집하고 "필요한 정보 및 자료"준비합니다.
- 필요한 를 "CPU 및 RAM"준비합니다.
- 에 대해 를 "스토리지 및 성능 요구사항"제공합니다.
- "Linux 서버를 준비합니다" 그러면 StorageGRID 노드가 호스팅됩니다.

2 구축

그리드 노드 구축 그리드 노드를 구축하면 StorageGRID 시스템의 일부로 생성되고 하나 이상의 네트워크에 연결됩니다.

- 1단계에서 준비한 호스트에 소프트웨어 기반 그리드 노드를 배포하려면 Linux 명령줄과 를 "노드 구성 파일 "사용합니다.
- StorageGRID 어플라이언스 노드를 배포하려면 를 "하드웨어 설치를 빠르게 시작합니다"따르십시오.

3 구성

모든 노드가 배포되면 Grid Manager를 사용하여 를 "그리드를 구성하고 설치를 완료합니다"수행합니다.

설치를 자동화합니다

StorageGRID 호스트 서비스 설치 및 그리드 노드 구성을 자동화하여 시간을 절약하고 일관성을 제공할 수 있습니다.

- Ansible, Puppet, Chef와 같은 표준 오케스트레이션 프레임워크를 사용하여 다음을 자동화합니다.
  - RHEL 설치

- 네트워킹 및 스토리지 구성
- 컨테이너 엔진 및 StorageGRID 호스트 서비스 설치
- 가상 그리드 노드 구축

을 "StorageGRID 호스트 서비스의 설치 및 구성을 자동화합니다"참조하십시오.

- 그리드 노드를 배포한 후 "StorageGRID 시스템의 구성을 자동화합니다"설치 아카이브에 제공된 Python 구성 스크립트를 사용합니다.
- "어플라이언스 그리드 노드의 설치 및 구성을 자동화합니다"
- StorageGRID 구축의 고급 개발자인 경우 를 사용하여 그리드 노드 설치를 "REST API 설치"자동화합니다.

Red Hat에서 설치 계획 및 준비

필요한 정보 및 자료

StorageGRID를 설치하기 전에 필요한 정보와 자료를 수집하고 준비합니다.

필수 정보입니다

네트워크 계획

각 StorageGRID 노드에 연결할 네트워크 StorageGRID는 트래픽 분리, 보안 및 관리의 편의를 위해 여러 네트워크를 지원합니다.

StorageGRID 를 "네트워킹 지침"참조하십시오.

네트워크 정보

각 그리드 노드에 할당할 IP 주소와 DNS 및 NTP 서버의 IP 주소입니다.

그리드 노드용 서버

구축할 StorageGRID 노드의 수와 유형을 지원하기에 충분한 리소스를 제공하는 물리적 서버 세트, 가상 서버 또는 둘 다 식별합니다.

> StorageGRID 설치에서 StorageGRID 어플라이언스(하드웨어) 스토리지 노드를 사용하지 않는 경우 BBWC(배터리 지원 쓰기 캐시)와 함께 하드웨어 RAID 스토리지를 사용해야 합니다. StorageGRID는 VSAN(Virtual Storage Area Network), 소프트웨어 RAID 또는 RAID 보호 사용을 지원하지 않습니다.

노드 마이그레이션(필요한 경우)

"노드 마이그레이션에 대한 요구사항"서비스 중단 없이 물리적 호스트에 대해 예약된 유지 관리를 수행하려는 경우을 이해합니다.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

필수 자료

NetApp StorageGRID 라이센스

디지털 서명된 유효한 NetApp 라이센스가 있어야 합니다.

테스트 및 개념 증명 그리드에 사용할 수 있는 비운영 라이센스가 StorageGRID 설치 아카이브에 포함되어 있습니다.

StorageGRID 설치 아카이브

"StorageGRID 설치 아카이브를 다운로드하고 파일 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"

StorageGRID 설치 파일을 다운로드하고 압축을 풉니다

StorageGRID 설치 아카이브를 다운로드하고 필요한 파일을 추출해야 합니다. 선택적으로 설치 패키지의 파일을 수동으로 확인할 수 있습니다.

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 "복구 및 유지 관리 지침의 핫픽스 절차"참조하십시오.

5. 최종 사용자 사용권 계약을 읽고 확인란을 선택한 다음 * 동의 및 계속 * 을 선택합니다.
6. StorageGRID 설치 * 열에서 Red Hat Enterprise Linux용 .tgz 또는 .zip 설치 아카이브를 선택합니다.

   `.zip`서비스 랩톱에서 Windows를 실행하는 경우 파일을 선택합니다.

7. 설치 아카이브를 저장합니다.
8. 설치 아카이브를 확인해야 하는 경우:

   a. StorageGRID 코드 서명 확인 패키지를 다운로드합니다. 이 패키지의 파일 이름은 StorageGRID 소프트웨어

버전의 형식을 `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` 사용합니다. `<version-number>`

b. 의 단계를 "설치 파일을 수동으로 확인합니다"따릅니다.

9. 설치 아카이브에서 파일 압축을 풉니다.
10. 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 호스트에 StorageGRID 노드 이미지를 설치하기 위한 rpm 패키지입니다.
	RHEL 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	스크립트와 함께 사용할 예제 구성 파일 `configure-storagegrid.py`
	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제 이 스크립트를 Ping 연합 통합에 사용할 수도 있습니다.
/rpms/configure -StorageGrid.blank.json을 지정합니다	스크립트와 함께 사용할 빈 구성 `configure-storagegrid.py` 파일입니다.

경로 및 파일 이름입니다	설명
	StorageGRID 컨테이너 배포를 위해 RHEL 호스트를 구성하기 위한 Ansible 역할 및 플레이북 예 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.
	Active Directory 또는 Ping 연방을 사용하여 SSO(Single Sign-On)를 사용하도록 설정한 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/rpms/StorageGrid-ssoauth-Azure.js	Azure와의 SSO 상호 작용을 수행하기 위해 Python 스크립트에 의해 호출되는 도우미 스크립트입니다. `storagegrid-ssoauth-azure.py`
/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.

설치 파일 수동 확인(선택 사항)

필요한 경우 StorageGRID 설치 아카이브의 파일을 수동으로 확인할 수 있습니다.

시작하기 전에

에서 "StorageGRID용 NetApp 다운로드 페이지" 가져온 "검증 패키지를 다운로드했습니다"것입니다.

단계

1. 검증 패키지에서 아티팩트를 추출합니다.

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. 이러한 아티팩트가 추출되었는지 확인합니다.
   - Leaf 인증서: `Leaf-Cert.pem`
   - 인증서 체인: `CA-Int-Cert.pem`
   - 타임 스탬프 응답 체인: `TS-Cert.pem`
   - 체크섬 파일: `sha256sum`
   - 체크섬 서명: `sha256sum.sig`
   - 타임 스탬프 응답 파일: `sha256sum.sig.tsr`
3. 체인을 사용하여 리프 인증서가 유효한지 확인합니다.
   - 예 *: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

- 예상 출력 *: `Leaf-Cert.pem: OK`

4. leaf 인증서가 만료되어 step_2_에 실패한 경우 파일을 사용하여 `tsr` 확인합니다.
   - 예 *: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`
   - 예상 출력 포함 *: `Verification: OK`
5. 리프 인증서에서 공용 키 파일을 만듭니다.
   - 예 *: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`
   - 예상 출력 *:_none_
6. 공개 키를 사용하여 `sha256sum` 에 대해 파일을 `sha256sum.sig` 확인합니다.
   - 예 *: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`
   - 예상 출력 *: `Verified OK`
7. `sha256sum`새로 생성된 체크섬을 기준으로 파일 내용을 확인합니다.
   - 예 *: `sha256sum -c sha256sum`

*예상 출력 * *<filename>*: OK:+는
<filename> 다운로드한 아카이브 파일의 이름입니다.

8. "나머지 단계를 완료합니다" 를 눌러 설치 아카이브에서 적절한 파일을 추출하고 선택합니다.

Red Hat Enterprise Linux에 대한 소프트웨어 요구 사항

가상 머신을 사용하여 모든 유형의 StorageGRID 노드를 호스팅할 수 있습니다. 각 그리드 노드에 대해 하나의 가상 머신이 필요합니다.

RHEL(Red Hat Enterprise Linux)에 StorageGRID를 설치하려면 일부 타사 소프트웨어 패키지를 설치해야 합니다. 지원되는 일부 Linux 배포판에는 기본적으로 이러한 패키지가 포함되어 있지 않습니다. StorageGRID 설치를 테스트하는 소프트웨어 패키지 버전에는 이 페이지에 나열된 버전이 포함됩니다.

이러한 패키지를 필요로 하는 Linux 배포 및 컨테이너 런타임 설치 옵션을 선택했는데 Linux 배포판에 의해 자동으로 설치되지 않은 경우, 해당 공급자 또는 Linux 배포판의 지원 공급업체에서 제공하는 경우 여기에 나열된 버전 중 하나를 설치하십시오. 그렇지 않으면 공급업체에서 제공하는 기본 패키지 버전을 사용하십시오.

모든 설치 옵션에는 Podman 또는 Docker가 필요합니다. 두 패키지를 모두 설치하지 마십시오. 설치 옵션에 필요한 패키지만 설치합니다.

> 소프트웨어 전용 배포를 위한 컨테이너 엔진으로 Docker에 대한 지원은 더 이상 사용되지 않습니다. Docker는 향후 릴리즈에서 다른 컨테이너 엔진으로 대체될 예정입니다.

Python 버전을 테스트했습니다

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38

- 3.6.9-1
- 3.7.3-1
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

Podman 버전을 테스트했습니다

- 3.2.3-0
- 3.4.4 + DS1
- 4.1.1-7
- 4.2.0-11
- 4.3.1+DS1-8+B1
- 4.4.1-8
- 4.4.1-12

Docker 버전을 테스트했습니다

Docker 지원은 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3 을 참조하십시오
- Docker-CE 23.0.6-1 을 참조하십시오
- Docker-CE 24.0.2-1 을 참조하십시오
- Docker-CE 24.0.4-1 을 참조하십시오
- Docker-CE 24.0.5-1 을 참조하십시오
- Docker-CE 24.0.7-1 을 참조하십시오
- 1.5-2 을 참조하십시오

CPU 및 **RAM** 요구 사항

StorageGRID 소프트웨어를 설치하기 전에 StorageGRID 시스템을 지원할 준비가 되도록 하드웨어를 확인 및 구성하십시오.

각 StorageGRID 노드에는 다음과 같은 최소 리소스가 필요합니다.

- CPU 코어: 노드당 8개
- RAM: 사용 가능한 총 RAM과 시스템에서 실행되는 비 StorageGRID 소프트웨어의 양에 따라 다릅니다

- 일반적으로 노드당 최소 24GB, 총 시스템 RAM보다 2 ~ 16GB 작습니다
- 각 테넌트당 최소 64GB의 버킷이 약 5,000개 있습니다

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 스토리지 관리, 메타데이터 예약 공간 설정 증가, CPU 및 메모리 사용량 모니터링에 대한 자세한 내용은"관리" "모니터링", 및 "업그레이드 중"StorageGRID에 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.

도 "요구사항을 충족해야 합니다"참조하십시오.

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 모두 공유 스토리지에 저장해야 합니다. 자세한 내용은 을 "노드 컨테이너 마이그레이션 요구사항"참조하십시오.

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 호스트의 요구 사항입니다

StorageGRID 노드가 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.

LUN 사용 목적	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

LUN 사용 목적	스토리지 범주입니다	**LUN** 수입니다	최소 크기/**LUN**
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 을 참조하십시오스토리지 노드의 스토리지 요구 사항.
스토리지 노드(메타데이터만)	오브젝트 메타데이터	1	4TB 자세한 내용은 을 스토리지 노드의 스토리지 요구 사항참조하십시오. • 참고 *: 메타데이터 전용 스토리지 노드에는 하나의 rangedb만 필요합니다.
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 레벨에 따라 S3 오브젝트 키 이름 등의 사용자 입력 크기, 그리고 보존해야 하는 감사 로그 데이터의 양을 위해 각 관리 노드에서 감사 로그 LUN의 크기를 늘려야 할 수도 있습니다. 일반적으로 그리드는 S3 작업당 약 1KB의 감사 데이터를 생성합니다. 즉, 200GB LUN이 2일에서 3일 동안 매일 7천만 개의 작업 또는 초당 800개의 작업을 지원하게 됩니다.

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 "그리드 노드 복구"각 노드 유형에 대한 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 _

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.

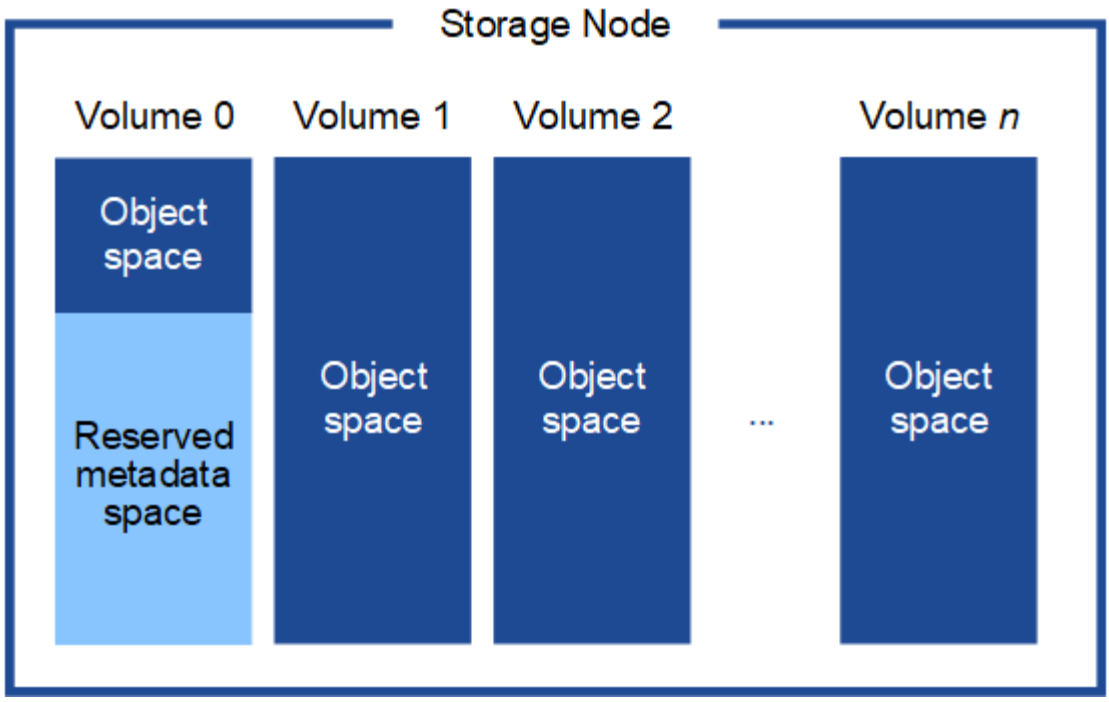
노드 유형입니다	**LUN** 사용 목적	**LUN** 수입니다	**LUN** 크기입니다
스토리지 노드	컨테이너 엔진 스토리지 풀입니다	1	300GB(100GB/노드)
스토리지 노드	`/var/local` 볼륨	1	90GB
스토리지 노드	오브젝트 데이터	3	12TB(4TB/LUN)
관리자 노드	`/var/local` 볼륨	1	90GB
관리자 노드	관리자 노드 감사 로그	1	200GB
관리자 노드	관리자 노드 테이블	1	200GB
게이트웨이 노드	`/var/local` 볼륨	1	90GB
• 합계 *		• 9 *	• 컨테이너 풀: * 300GB • 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.

메타데이터 전용 스토리지 노드가 있는 그리드를 설치할 경우 그리드에는 오브젝트 스토리지용 최소 노드 수도 있어야 합니다. 메타데이터 전용 스토리지 노드에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

- 단일 사이트 그리드의 경우 객체 및 메타데이터에 대해 2개 이상의 스토리지 노드가 구성됩니다.
- 다중 사이트 그리드의 경우 사이트당 하나 이상의 스토리지 노드가 객체 및 메타데이터에 대해 구성됩니다.

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 이하의 용량을 할당하면 스토리지 노드가 시작 시 스토리지 읽기 전용 상태로 전환되고 객체 메타데이터만 저장할 수 있습니다.

> ⓘ 볼륨 0에 500GB 미만의 용량을 할당할 경우(비운영 전용) 스토리지 볼륨 용량의 10%가 메타데이터용으로 예약됩니다.

- 새 시스템(StorageGRID 11.6 이상)을 설치하고 각 스토리지 노드에 128MB 이상의 RAM이 있는 경우 볼륨 0에 8TB 이상을 할당합니다. 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 을 "오브젝트 메타데이터 스토리지 관리"참조하십시오.

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 이동합니다. 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 "그리드 노드 종료"참조하십시오.

VMware Live Migration은 지원되지 않습니다

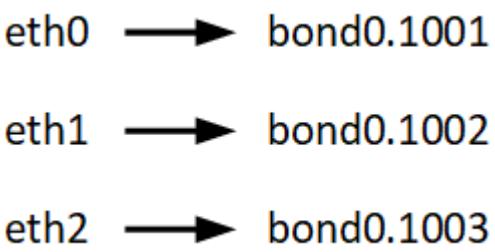
VMware VM에서 베어 메탈 설치를 수행할 때 OpenStack Live Migration 및 VMware Live vMotion을 사용하면 가상 머신 클록 시간이 증가하며 어떠한 유형의 그리드 노드에서도 지원되지 않습니다. 드물지만 잘못된 클럭 시간으로 인해 데이터 또는 구성 업데이트가 손실될 수 있습니다.

콜드 마이그레이션이 지원됩니다. 콜드 마이그레이션에서는 StorageGRID 노드를 호스트 간에 마이그레이션하기 전에 종료해야 합니다. 의 지침을 "그리드 노드 종료"참조하십시오.

일관된 네트워크 인터페이스 이름

한 호스트에서 다른 호스트로 노드를 이동하려면 StorageGRID 호스트 서비스가 노드가 현재 위치에 있는 외부 네트워크 연결을 새 위치에서 복제할 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 호스트 간에 일관된 네트워크 인터페이스 이름을 지정하는 방법은 여러 가지가 있습니다. 몇 가지 예는 를 참조하십시오."호스트 네트워크 구성"

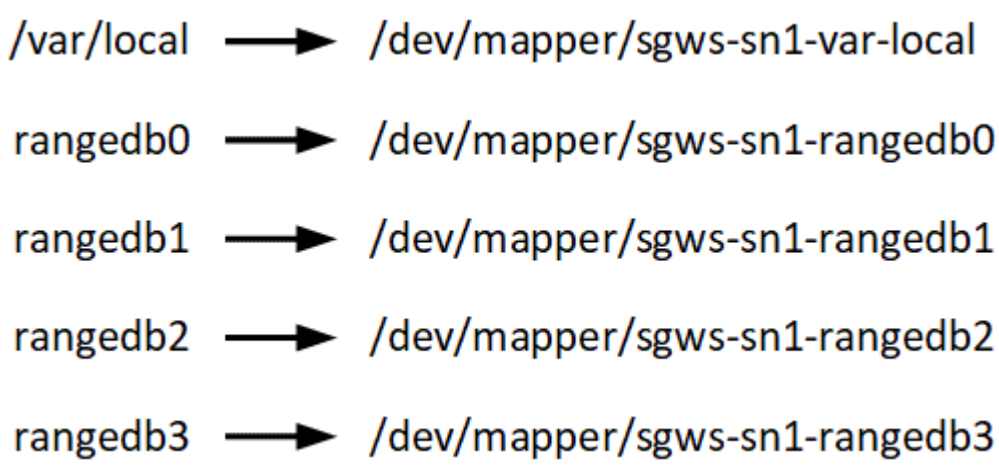
공유 스토리지

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 HostA에서 실행 중인 노드 컨테이너에서 소량의 영구 상태 데이터가 추출되고 해당 노드의 시스템 데이터 볼륨에 캐시됩니다. 그런 다음 HostA의 노드 컨테이너가 인스턴스화됩니다.
2. "노드 가져오기" 작업 중에 HostA에 적용된 동일한 네트워크 인터페이스와 블록 스토리지 매핑을 사용하는 HostB의 노드 컨테이너가 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 StorageGRID 스토리지 노드에 대한 블록 디바이스 매핑 솔루션 중 하나를 보여 줍니다. 이 경우 DM 다중 경로가 호스트에서 사용되고 별칭 필드는 모든 호스트에서 사용할 수 있는 일관되고 알기 쉬운 블록 디바이스 이름을 제공하기 위해 에 `/etc/multipath.conf` 사용되었습니다.



호스트 준비**(Red Hat)**

설치 중에 호스트 전체의 설정이 변경되는 방식

베어 메탈 시스템에서 StorageGRID는 호스트 전체 설정을 일부 변경합니다 `sysctl`.

다음과 같은 변경 사항이 적용됩니다.

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
```

```
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
```

```
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Linux를 설치합니다

모든 Red Hat Enterprise Linux 그리드 호스트에 StorageGRID를 설치해야 합니다. 지원되는 버전 목록은 NetApp 상호 운용성 매트릭스 툴을 참조하십시오.

시작하기 전에

운영 체제가 아래 나열된 StorageGRID의 최소 커널 버전 요구 사항을 충족하는지 확인합니다. 명령을 사용하여 `uname -r` 운영 체제의 커널 버전을 가져오거나 OS 공급업체에 문의하십시오.

Red Hat Enterprise Linux 버전	최소 커널 버전	커널 패키지 이름입니다
8.8(폐기됨)	4.18.0-477.10.1.el8_8.x86_64	커널 - 4.18.0-477.10.1.el8_8.x86_64
8.10	4.18.0-553.el8_10.x86_64	kernel-4.18.0-553.el8_10.x86_64
9.0(폐기됨)	5.14.0-70.22.1.el9_0.x86_64	커널 - 5.14.0-70.22.1.el9_0.x86_64
9.2(사용되지 않음)	5.14.0-284.11.1.el9_2.x86_64	커널 - 5.14.0-284.11.1.el9_2.x86_64

Red Hat Enterprise Linux 버전	최소 커널 버전	커널 패키지 이름입니다
9.4 를 참조하십시오	5.14.0-427.18.1.el9_4.x86_64	커널 - 5.14.0-427.18.1.el9_4.x86_64

단계

1. 배포자의 지침 또는 표준 절차에 따라 모든 물리적 또는 가상 그리드 호스트에 Linux를 설치합니다.

   > 표준 Linux 설치 프로그램을 사용하는 경우 사용 가능한 경우 "컴퓨팅 노드" 소프트웨어 구성을 선택하거나 "최소 설치" 기본 환경을 선택합니다. 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. 다음 명령을 실행합니다. `$ sudo swapoff --all`

   b. 설정을 유지하려면 에서 모든 스왑 항목을 `/etc/fstab` 제거합니다.

   > 스왑을 완전히 사용하지 않도록 설정하면 성능이 크게 저하될 수 있습니다.

호스트 네트워크 구성**(Red Hat Enterprise Linux)**

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.

시작하기 전에

- 를 검토했습니다."StorageGRID 네트워킹 지침"
- 에 대한 정보를 검토했습니다."노드 컨테이너 마이그레이션 요구사항"
- 가상 호스트를 사용하는 경우 호스트 네트워크를 구성하기 전에 를 읽은 MAC 주소 복제에 대한 고려 사항 및 권장 사항것입니다.

> 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.

> Bond 또는 Bridge 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 무작위로 생성된 주소이지만 노드 구성 키를 사용하여 주소를 설정한 경우 `_NETWORK_MAC` 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 클론 생성이 활성화되지 않음: `_CLONE_MAC` 노드 구성 파일의 키가 설정되지 않았거나 "false"로 설정되어 있지 않으면 호스트는 호스트 NIC MAC을 사용하고 컨테이너에 StorageGRID 생성 MAC을 갖게 됩니다. `_NETWORK_MAC` 키에 주소가 설정되어 있으면 `_NETWORK_MAC` 컨테이너에 키에 지정된 주소가 `_NETWORK_MAC` 지정됩니다. 이러한 키 구성을 위해서는 무차별 모드를 사용해야 합니다.
- MAC 클론 생성 활성화: 노드 구성 파일의 키가 "true"로 설정된 경우 `_CLONE_MAC` 컨테이너에서 호스트 NIC MAC을 사용하고, 키에 MAC이 지정되지 않은 경우 호스트는 StorageGRID에서 생성된 MAC을 사용합니다. `_NETWORK_MAC` 키에 주소가 설정된 경우 `_NETWORK_MAC` 호스트는 생성된 주소가 아닌 지정된 주소를 사용합니다. 이 키 구성에서 무차별 모드를 사용해서는 안 됩니다.

> ⓘ MAC 주소 클로닝을 사용하지 않고 하이퍼바이저에 의해 할당된 것이 아닌 MAC 주소에 대한 데이터를 모든 인터페이스에서 수신 및 전송하도록 허용하려면 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 복제를 활성화하려면 을 "노드 구성 파일 생성 지침"참조하십시오.

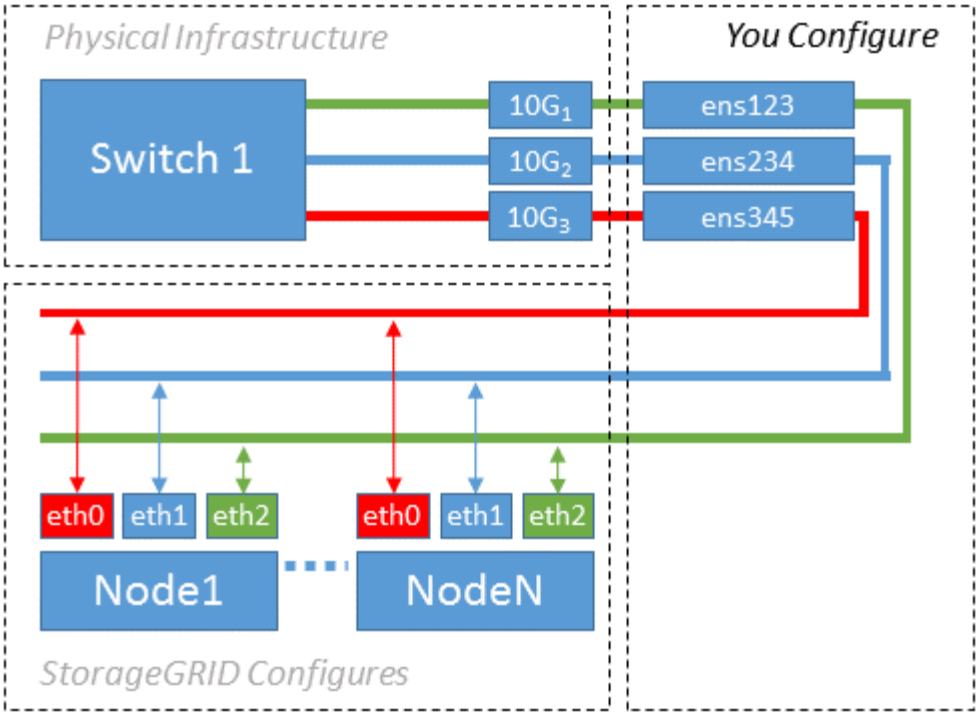
Mac 클론 복제의 예

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 `ensXYZ` 설치 또는 부팅 중에 또는 인터페이스가 핫 애드될 때 자동으로 인터페이스를 생성합니다. 부팅 후 인터페이스가 자동으로 실행되도록 설정하는 것 외에는 구성이 필요하지 않습니다. 나중에 구성 프로세스에서 올바른 매핑을 제공할 수 있도록 어떤 StorageGRID 네트워크(그리드, 관리자 또는 클라이언트)에 해당하는지 결정해야 `ensXYZ` 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

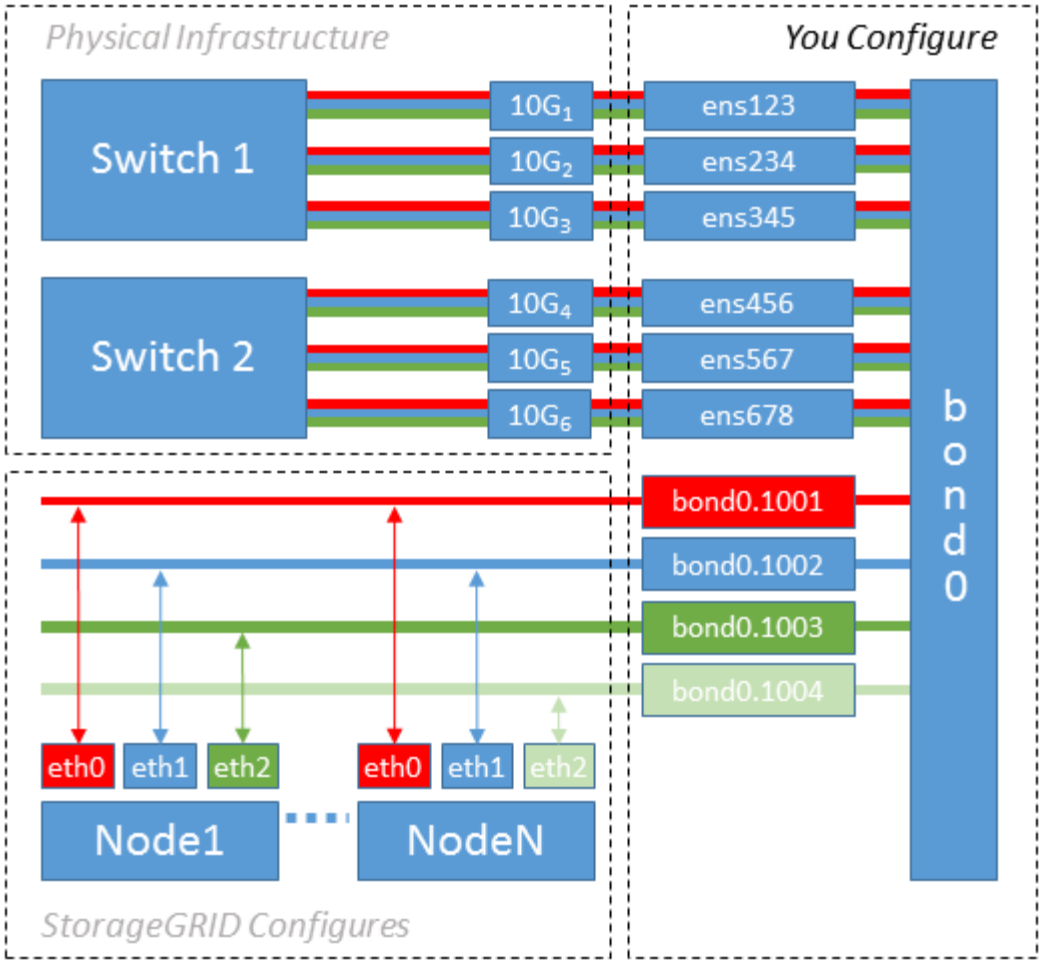
이 작업에 대해

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. `bond0`예를 들어,

2. 표준 VLAN 인터페이스 명명 규칙을 사용하여 이 연결을 관련 "물리적 장치"로 사용하는 VLAN 인터페이스를 `physdev-name.VLAN ID` 생성합니다.

   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.

시작하기 전에

이 과제를 수행하는 데 필요한 정보를 제공하는 다음 주제를 검토했습니다.

- "요구사항을 충족해야 합니다"
- "노드 컨테이너 마이그레이션 요구사항"

이 작업에 대해

블록 스토리지 볼륨(LUN)을 호스트에 할당할 때 "스토리지 요구 사항"의 표를 사용하여 다음을 확인합니다.

- 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.

메타데이터 전용 스토리지 노드에는 하나의 오브젝트 데이터 LUN만 필요합니다.

(/dev/sdb`볼륨 이름 목록을 작성할 때 "raw" 특수 장치 파일을 사용하지 마십시오. 이러한 파일은 호스트의 재부팅 시 변경될 수 있으며, 이는 시스템의 올바른 작동에 영향을 줍니다. iSCSI LUN 및 Device Mapper Multipathing을 사용하는 경우, 특히 SAN 토폴로지에 공유 스토리지에 대한 중복 네트워크 경로가 포함되어 있는 경우 디렉토리에서 다중 경로 별칭을 사용하는 `/dev/mapper 것이 좋습니다. 또는 영구 장치 이름에 대해 에서 시스템에서 만든 소프트링크를 사용할 수 /dev/disk/by-path/ 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 디바이스 매퍼 다중 경로 드라이버를 사용하는 경우 파일의 필드를 /etc/multipath.conf 사용할 수 alias 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
     }
     …
```

이러한 방식으로 별칭 필드를 사용하면 별칭이 호스트의 디렉토리에 블록 디바이스로 나타나므로 구성 또는 유지 관리 작업에서 블록 `/dev/mapper` 스토리지 볼륨을 지정해야 할 때마다 쉽게 검증된 친숙한 이름을 지정할 수 있습니다.

> StorageGRID 노드 마이그레이션을 지원하고 장치 매퍼 다중 경로를 사용하도록 공유 스토리지를 설정하는 경우 모든 공동 위치 호스트에 공통 을 생성하고 설치할 수 `/etc/multipath.conf` 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.

> 소프트웨어 전용 배포를 위한 컨테이너 엔진으로 Docker에 대한 지원은 더 이상 사용되지 않습니다. Docker는 향후 릴리즈에서 다른 컨테이너 엔진으로 대체될 예정입니다.

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.

> 소프트웨어 전용 배포를 위한 컨테이너 엔진으로 Docker에 대한 지원은 더 이상 사용되지 않습니다. Docker는 향후 릴리즈에서 다른 컨테이너 엔진으로 대체될 예정입니다.

이 작업에 대해

Docker 또는 Podman 스토리지 볼륨에 로컬 스토리지를 사용할 계획이고 Docker 및 `/var/lib/containers` Podman이 포함된 호스트 파티션에 사용 가능한 공간이 충분하다면 이 단계를 건너뛸 수 있습니다 `/var/lib/docker`.

> 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 Linux에서 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 RPM 패키지를 사용하여 StorageGRID 호스트 서비스를 설치합니다.

이 작업에 대해

다음 지침은 RPM 패키지에서 호스트 서비스를 설치하는 방법을 설명합니다. 또는 설치 아카이브에 포함된 DNF 리포지토리 메타데이터를 사용하여 RPM 패키지를 원격으로 설치할 수 있습니다. Linux 운영 체제에 대한 DNF 리포지토리 지침을 참조하십시오.

단계

1. 각 호스트에 StorageGRID RPM 패키지를 복사하거나 공유 스토리지에서 사용할 수 있도록 합니다.

   예를 들어, `/tmp` 다음 단계에서 예제 명령을 사용할 수 있도록 디렉토리에 배치합니다.

2. 각 호스트에 루트로 로그인하거나 sudo 권한이 있는 계정을 사용하여 다음 명령을 지정된 순서대로 실행합니다.

```
sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-version-SHA.rpm
```

```
sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-version-SHA.rpm
```

   먼저 이미지 패키지를 설치하고 서비스 패키지를 다시 설치해야 합니다.

   패키지를 이외의 디렉토리에 배치한 경우 `/tmp` 사용한 경로를 반영하도록 명령을 수정합니다.

Red Hat Enterprise Linux에서 StorageGRID 설치를 자동화합니다

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 작동합니다.
- 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 자동화하기 위한

선택적 Python 스크립트를 제공합니다. 이러한 스크립트를 직접 사용하거나 직접 개발한 그리드 배포 및 구성 도구의 사용 방법을 알아보기 위해 해당 스크립트를 검사할 수 "StorageGRID 설치 REST API"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. 이미 표준 오케스트레이션 프레임워크를 사용하여 RHEL을 설치 및 구성하는 경우 플레이북이나 레시피에 StorageGRID를 추가하는 것이 간단해야 합니다.

설치 아카이브와 함께 제공된 폴더에서 예제 Ansible 역할 및 플레이북을 `/extras` 참조하십시오. Ansible 플레이북에서는 역할이 호스트를 준비하고 타겟 서버에 StorageGRID를 설치하는 방법을 보여줍니다 `storagegrid`. 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.

Ansible 역할 및 플레이북 예

예제 Ansible 역할 및 플레이북은 폴더에 설치 아카이브와 함께 `/extras` 제공됩니다. Ansible 플레이북에서는 역할이 호스트를 준비하고 타겟 서버에 StorageGRID를 설치하는 방법을 보여줍니다 `storagegrid`. 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.

제공된 역할 예제의 설치 작업은 `storagegrid` 모듈을 사용하여 `ansible.builtin.dnf` 로컬 RPM 파일 또는 원격 Yum 리포지토리에서 설치를 수행합니다. 모듈을 사용할 수 없거나 지원되지 않는 경우 또는 `ansible.builtin.yum` 모듈을 사용하려면 다음 파일에서 적절한 Ansible 작업을 편집해야 할 수 있습니다 `yum`.

- `roles/storagegrid/tasks/rhel_install_from_repo.yml`
- `roles/storagegrid/tasks/rhel_install_from_local.yml`

StorageGRID의 구성을 자동화합니다

그리드 노드를 구축한 후 StorageGRID 시스템 구성을 자동화할 수 있습니다.

시작하기 전에

- 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 예제 구성 파일
configure -StorageGrid.blank.json을 지정합니다	스크립트에 사용할 빈 구성 파일입니다

- `configure-storagegrid.json`구성 파일을 만들었습니다. 이 파일을 작성하려면 예제 구성 파일(`configure-storagegrid.sample.json`)이나 빈 구성 파일을 수정할 수 (`configure-storagegrid.blank.json`있습니다.

이 작업에 대해

Python 스크립트와 `configure-storagegrid.json` 구성 파일을 사용하여 StorageGRID 시스템 구성을 자동화할 수 `configure-storagegrid.py` 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 `platform` 는 `debs`, `rpms` 또는 `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 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.

임의의 암호를 생성하도록 지정한 경우 파일을 열고 `Passwords.txt` StorageGRID 시스템에 액세스하는 데 필요한 암호를 찾습니다.

```
###################################################################
##### 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

"REST API 설치"

가상 그리드 노드 배포(Red Hat)

Red Hat Enterprise Linux 배포를 위한 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 노드에 사용되지 않습니다.

노드 구성 파일의 위치입니다

각 StorageGRID 노드의 구성 파일을 `/etc/storagegrid/nodes` 노드가 실행될 호스트의 디렉토리에 배치합니다. 예를 들어 HostA에서 관리자 노드 1개, 게이트웨이 노드 1개 및 스토리지 노드 1개를 실행하려면 HostA에 3개의 노드 구성 파일을 배치해야 `/etc/storagegrid/nodes` 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 파일 이름 지정

구성 파일의 이름이 중요합니다. 형식은 입니다 `node-name.conf`. 여기서 `node-name` 는 노드에 할당한 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.
- 확장자는 32자 이하여야 합니다 `.conf`

에서 이러한 명명 규칙을 따르지 않는 파일은 `/etc/storagegrid/nodes` 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 관리자 노드와 `dc2-sn3.conf` 데이터 센터 2의 세 번째 스토리지 노드에 을

사용할 수 `dc1-adm1.conf` 있습니다. 그러나 모든 노드 이름이 명명 규칙을 따른다 하더라도 원하는 스키마를 사용할 수 있습니다.

노드 구성 파일의 내용입니다

구성 파일에는 키/값 쌍이 포함되어 있으며 한 줄에 하나의 키와 하나의 값이 있습니다. 각 키/값 쌍에 대해 다음 규칙을 따르십시오.

- 키와 값은 등호(=)와 선택적 공백으로 구분해야 합니다.
- 키에는 공백이 포함될 수 없습니다.
- 값에는 포함된 공백이 포함될 수 있습니다.
- 선행 또는 후행 공백은 무시됩니다.

다음 표에서는 지원되는 모든 키의 값을 정의합니다. 각 키에는 다음 중 하나가 지정됩니다.

- * 필수 *: 모든 노드 또는 지정된 노드 유형에 필요합니다
- * 모범 사례 *: 선택 사항이지만 권장됨
- * 선택 사항 *: 모든 노드에 대해 선택 사항입니다

관리 네트워크 키

관리**_IP**

값	지정
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.	모범 사례

관리 네트워크 구성

값	지정
DHCP, 정적 또는 비활성	선택 사항

관리_네트워크**_ESL**

값	지정
쉼표로 구분된 서브넷 목록으로, 이 노드가 Admin Network 게이트웨이를 사용하여 통신해야 하는 CIDR 표기법을 사용합니다. 예: `172.16.0.0/21,172.17.0.0/21`	선택 사항

Admin_network_Gateway를 선택합니다

값	지정

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.
 	
예:
 	
`1.1.1.1`
 	
`10.224.4.81`
	가 지정된 경우 `ADMIN_NETWORK_ESL` 필수입니다. 그렇지 않으면 선택 사항입니다.

admin_network_ip을 선택합니다

값	지정

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_config = static 인 경우 필요합니다.
	
	그렇지 않으면 선택 사항입니다.

admin_network_MAC입니다

값	지정
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`	선택 사항

admin_network_mask를 선택합니다

값	지정

이 노드의 IPv4 넷마스크는 관리자 네트워크에서 설정합니다. admin_network_config = static 인 경우 이 키를 지정하고 다른 값에 대해서는 이 키를 지정하지 마십시오.
 	
예:
 	
`255.255.255.0`
 	
`255.255.248.0`
	admin_network_ip을 지정하고 admin_network_Config=static인 경우 필수입니다.
	
	그렇지 않으면 선택 사항입니다.

admin_network_mtu

값	지정

Admin Network의 이 노드에 대한 MTU(Maximum Transmission Unit)입니다. admin_network_Config=DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 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:
 	
`1500`
 	
`8192`
	선택 사항

admin_network_target 을 선택합니다

값	지정

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:
 	
`bond0.1002`
 	
`ens256`
	모범 사례

admin_network_target_type입니다

값	지정
인터페이스(이 값만 지원됩니다.)	선택 사항

admin_network_target_type_interface_clone_MAC

값	지정
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 복제의 고려 사항 및 권장 사항(Red Hat Enterprise Linux)" • "MAC 주소 복제에 대한 고려 사항 및 권장 사항(Ubuntu 또는 Debian)"	모범 사례

admin_role을 선택합니다

값	지정
Primary 또는 Non-Primary 이 키는 node_type=vm_Admin_Node인 경우에만 필요하며 다른 노드 유형에 대해서는 지정하지 않습니다.	node_type=vm_admin_Node인 경우 필요합니다 그렇지 않으면 선택 사항입니다.

장치 키를 차단합니다

Block_device_audit_logs

값	지정

이 노드가 감사 로그의 영구 저장에 사용할 블록 디바이스 특수 파일의 경로 및 이름입니다.
 	
예:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	node_type이 vm_admin_Node인 노드에 필요합니다. 다른 노드 유형에는 지정하지 마십시오.

Block_device_RANGEDB_nnn을 선택합니다

값	지정

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 않습니다.
 	
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`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	필수:
	
	BLOCK_DEVICE_RANGEDB_000
	
	선택 사항:
	
	BLOCK_DEVICE_RANGEDB_001
	
	BLOCK_DEVICE_RANGEDB_002 를 참조하십시오
	
	Block_device_RANGEDB_003 을 참조하십시오
	
	Block_device_RANGEDB_004 를 참조하십시오
	
	Block_device_RANGEDB_005 를 참조하십시오
	
	Block_device_RANGEDB_006
	
	Block_device_RANGEDB_007 을 참조하십시오
	
	Block_device_RANGEDB_008 을 참조하십시오
	
	Block_device_RANGEDB_009 를 참조하십시오
	
	Block_device_RANGEDB_010
	
	Block_device_RANGEDB_011 을 참조하십시오
	
	Block_device_RANGEDB_012 를 참조하십시오
	
	Block_device_RANGEDB_013
	
	Block_device_RANGEDB_014
	
	Block_device_RANGEDB_015 를 참조하십시오

BLOCK_DEVICE_Tables

값	지정

이 노드가 데이터베이스 테이블의 영구 저장에 사용할 블록 디바이스 특수 파일의 경로 및 이름입니다. 이 키는 node_type=vm_Admin_Node인 노드에만 필요합니다. 다른 노드 유형에 대해서는 지정하지 마십시오.
 	
예:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	필수 요소입니다

BLOCK_DEVICE_VAR_LOCAL

값	지정

이 노드가 영구 스토리지에 사용할 블록 디바이스 특수 파일의 경로 및 `/var/local` 이름입니다.
 	
예:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	필수 요소입니다

클라이언트 네트워크 키

client_network_Config

값	지정
DHCP, 정적 또는 비활성	선택 사항

CLIENT_NETWORK_GATEWAY

값	지정

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`
	선택 사항

client_network_ip

값	지정

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`
	client_network_Config=static 인 경우 필요합니다
	
	그렇지 않으면 선택 사항입니다.

client_network_MAC

값	지정
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`	선택 사항

client_network_mask.(클라이언트 네트워크 마스크

값	지정

클라이언트 네트워크의 이 노드에 대한 IPv4 넷마스크입니다.
 	
client_network_config = static 인 경우 이 키를 지정하고 다른 값에는 이 키를 지정하지 마십시오.
 	
예:
 	
`255.255.255.0`
 	
`255.255.248.0`
	client_network_ip을 지정하고 client_network_Config=static인 경우 필수입니다
	
	그렇지 않으면 선택 사항입니다.

client_network_mtu

값	지정

Client Network의 이 노드에 대한 MTU(Maximum Transmission Unit)입니다. client_network_Config = DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 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:
 	
`1500`
 	
`8192`
	선택 사항

client_network_target 을 선택합니다

값	지정

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:
 	
`bond0.1003`
 	
`ens423`
	모범 사례

CLIENT_NETWORK_TARGET_TYPE

값	지정
인터페이스(지원되는 값만 해당)	선택 사항

client_network_target_type_interface_clone_MAC

값	지정
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 복제의 고려 사항 및 권장 사항(Red Hat Enterprise Linux)" • "MAC 주소 복제에 대한 고려 사항 및 권장 사항(Ubuntu 또는 Debian)"	모범 사례

그리드 네트워크 키

GRID_NETWORK_CONFIG(그리드 네트워크 구성

값	지정
고정 또는 DHCP 지정하지 않으면 기본적으로 정적입니다.	모범 사례

GRID_NETWORK_Gateway를 참조하십시오

값	지정
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.	필수 요소입니다

GRID_NETWORK_IP입니다

값	지정

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_CONFIG = STATIC인 경우 필요합니다
	
	그렇지 않으면 선택 사항입니다.

GRID_NETWORK_MAC을 선택합니다

값	지정
컨테이너의 그리드 네트워크 인터페이스에 대한 MAC 주소입니다. 콜론으로 구분된 6쌍의 16진수 숫자이어야 합니다. 예: `b2:9c:02:c2:27:30`	선택 사항 생략할 경우 MAC 주소가 자동으로 생성됩니다.

GRID_NETWORK_MASK 를 참조하십시오

값	지정

그리드 네트워크에서 이 노드에 대한 IPv4 넷마스크입니다. GRID_NETWORK_CONFIG = STATIC인 경우 이 키를 지정하고 다른 값에는 이 키를 지정하지 마십시오.
 	
예:
 	
`255.255.255.0`
 	
`255.255.248.0`
	GRID_NETWORK_IP를 지정하고 GRID_NETWORK_CONFIG=STATIC인 경우에 필요합니다.
	
	그렇지 않으면 선택 사항입니다.

GRID_NETWORK_MTU 를 참조하십시오

값	지정

Grid Network의 이 노드에 대한 MTU(Maximum Transmission Unit)입니다. GRID_NETWORK_CONFIG=DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 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:
 	
`1500`
 	
`8192`
	선택 사항

GRID_NETWORK_TARGET

값	지정

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:
 	
`bond0.1001`
 	
`ens192`
	필수 요소입니다

GRID_NETWORK_TARGET_TYPE

값	지정
인터페이스(이 값만 지원됩니다.)	선택 사항

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

값	지정
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 복제의 고려 사항 및 권장 사항(Red Hat Enterprise Linux)" • "MAC 주소 복제에 대한 고려 사항 및 권장 사항(Ubuntu 또는 Debian)"	모범 사례

설치 암호 키(임시)

사용자 지정_임시_암호_해시

값	지정
기본 관리자 노드의 경우 설치 중에 StorageGRID 설치 API에 대한 기본 임시 암호를 설정합니다. • 참고 *: 기본 관리자 노드에서만 설치 암호를 설정합니다. 다른 노드 유형에 암호를 설정하려고 하면 노드 구성 파일의 유효성 검사가 실패합니다. 이 값을 설정해도 설치가 완료된 경우 아무런 영향이 없습니다. 이 키를 생략하면 기본적으로 임시 암호가 설정되지 않습니다. 또는 StorageGRID 설치 API를 사용하여 임시 암호를 설정할 수 있습니다. 8자 이상 32자 이하의 암호 형식을 가진 SHA-512 암호 `$6$<salt>$<password hash>` 해시여야 `crypt()` 합니다. 이 해시는 SHA-512 모드의 명령과 같은 CLI 툴을 사용하여 생성할 수 `openssl passwd` 있습니다.	모범 사례

인터페이스 키입니다

interface_target_nnnn입니다

값	지정
이 노드에 추가할 추가 인터페이스의 이름 및 선택적 설명입니다. 각 노드에 여러 개의 인터페이스를 추가할 수 있습니다. _nnnn_의 경우 추가할 각 interface_target 항목의 고유 번호를 지정합니다. 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: `INTERFACE_TARGET_0001=ens256, 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.	선택 사항

최대 **RAM** 키

최대 **RAM**

값	지정

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 "메타데이터 예약된 공간에 대한 설명입니다"참조하십시오.
 	
이 필드의 형식은 *numberunit*, WHERE *unit* b, k, m 또는 `g`입니다.
 	
예:
 	
`24g`
 	
`38654705664b`
 	
• 참고 *: 이 옵션을 사용하려면 메모리 cgroup에 대한 커널 지원을 활성화해야 합니다.
	선택 사항

노드 유형 키입니다

node_type입니다

값	지정
노드 유형: • VM_Admin_Node • VM_스토리지_노드 • VM_Archive_Node • VM_API_게이트웨이	필수 요소입니다

스토리지 유형

값	지정
스토리지 노드에 포함된 객체 유형을 정의합니다. 자세한 내용은 을 "스토리지 노드 유형"참조하십시오. 이 키는 node_type=vm_Storage_Node인 노드에만 필요하며 다른 노드 유형에 대해서는 지정하지 않습니다. 스토리지 유형: • 결합된 • 데이터 • 메타데이터 • 참고 *: storage_type이 지정되지 않은 경우 스토리지 노드 유형은 기본적으로 결합(데이터 및 메타데이터)으로 설정됩니다.	선택 사항

포트 재매핑 키

port_remap 을 참조하십시오

값	지정
노드에서 내부 그리드 노드 통신 또는 외부 통신을 위해 사용하는 모든 포트를 다시 매핑합니다. 엔터프라이즈 네트워킹 정책으로 StorageGRID에서 사용하는 하나 이상의 포트를 제한하는 경우 또는 에 설명된 대로 포트를 다시 매핑해야 "내부 그리드 노드 통신""외부 통신"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 다음과 같습니다 *network type/protocol/default port used by grid node/new port*. 여기서 *network type* 그리드, 관리자 또는 클라이언트이고 *protocol* TCP 또는 UDP입니다. 예: `PORT_REMAP = client/tcp/18082/443` 쉼표로 구분된 목록을 사용하여 여러 포트를 다시 매핑할 수도 있습니다. 예: `PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80`	선택 사항

port_remap_inbound 를 참조하십시오

값	지정
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 다음과 같습니다 *network type/protocol/remapped port/default port used by grid node*. 여기서 *network type* 그리드, 관리자 또는 클라이언트이고 *protocol* TCP 또는 UDP입니다. 예: `PORT_REMAP_INBOUND = grid/tcp/3022/22` 쉼표로 구분된 목록을 사용하여 여러 인바운드 포트를 다시 매핑할 수도 있습니다. 예: `PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22`	선택 사항

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 mDNS(multicast domain name system)를 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
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
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
```

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 에서 구성 파일을 만든 후에는 `/etc/storagegrid/nodes` 해당 파일의 내용을 확인해야 합니다.

구성 파일의 내용을 확인하려면 각 호스트에서 다음 명령을 실행합니다.

```
sudo storagegrid node validate all
```

파일이 올바른 경우, 예제에 표시된 대로 각 구성 파일에 대해 * Passed * 가 출력됩니다.

메타데이터 전용 노드에서 LUN을 하나만 사용하는 경우에는 무시해도 되는 경고 메시지가 표시될 수 있습니다.

```
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 명령의 또는 `--quiet` 옵션 `storagegrid`(예: `storagegrid --quiet…`)을 사용하여 이 출력을 표시하지 않을 수 있습니다 `-q`. 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
```

3. 노드가 "not running" 또는 "stopped" 상태를 반환하는 경우 다음 명령을 실행합니다.

```
sudo storagegrid node start node-name
```

4. 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(Red Hat)

그리드 관리자로 이동합니다

그리드 관리자를 사용하여 StorageGRID 시스템을 구성하는 데 필요한 모든 정보를 정의합니다.

시작하기 전에

기본 관리 노드를 구축하고 초기 시작 시퀀스를 완료해야 합니다.

단계

1. 웹 브라우저를 열고 다음으로 이동합니다.

   `https://primary_admin_node_ip`

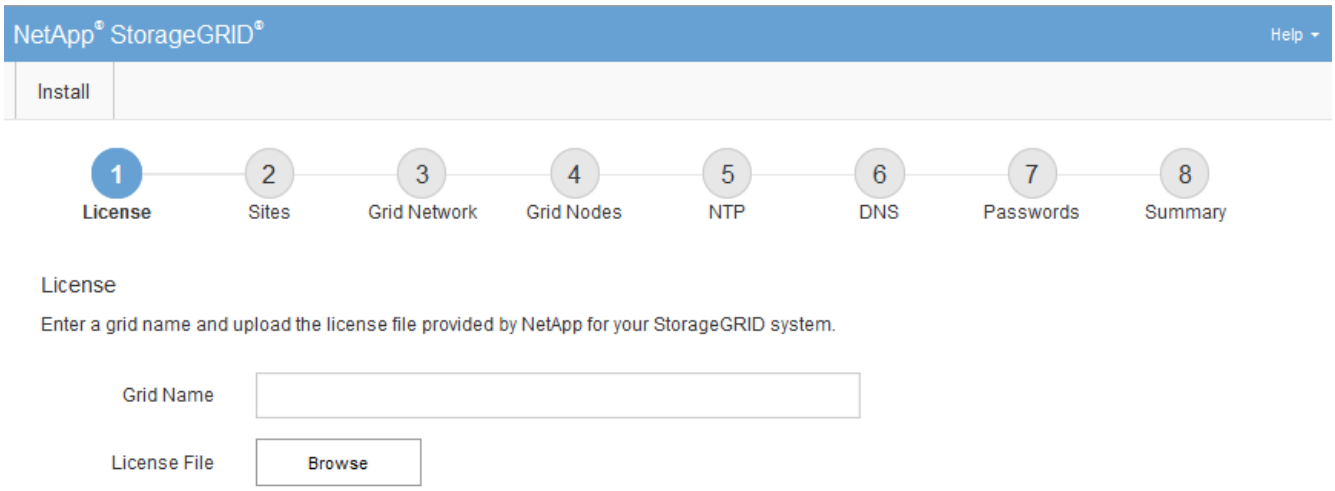
   또는 포트 8443에서 그리드 관리자에 액세스할 수 있습니다.

   `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. 필요에 따라 임시 설치 관리자 암호를 관리합니다.
   - 이러한 방법 중 하나를 사용하여 암호를 이미 설정한 경우 암호를 입력하여 계속 진행합니다.
     - 사용자가 이전에 설치 프로그램에 액세스하는 동안 암호를 설정했습니다
     - 암호가 에 있는 노드 구성 파일에서 자동으로 가져온 것입니다 `/etc/storagegrid/nodes/<node_name>.conf`
   - 암호를 설정하지 않은 경우 StorageGRID 설치 프로그램을 보호할 암호를 선택적으로 설정합니다.
3. StorageGRID 시스템 설치 * 를 선택합니다.

   StorageGRID 시스템을 구성하는 데 사용되는 페이지가 나타납니다.



StorageGRID 라이센스 정보를 지정합니다

StorageGRID 시스템의 이름을 지정하고 NetApp에서 제공하는 라이센스 파일을 업로드해야 합니다.

단계

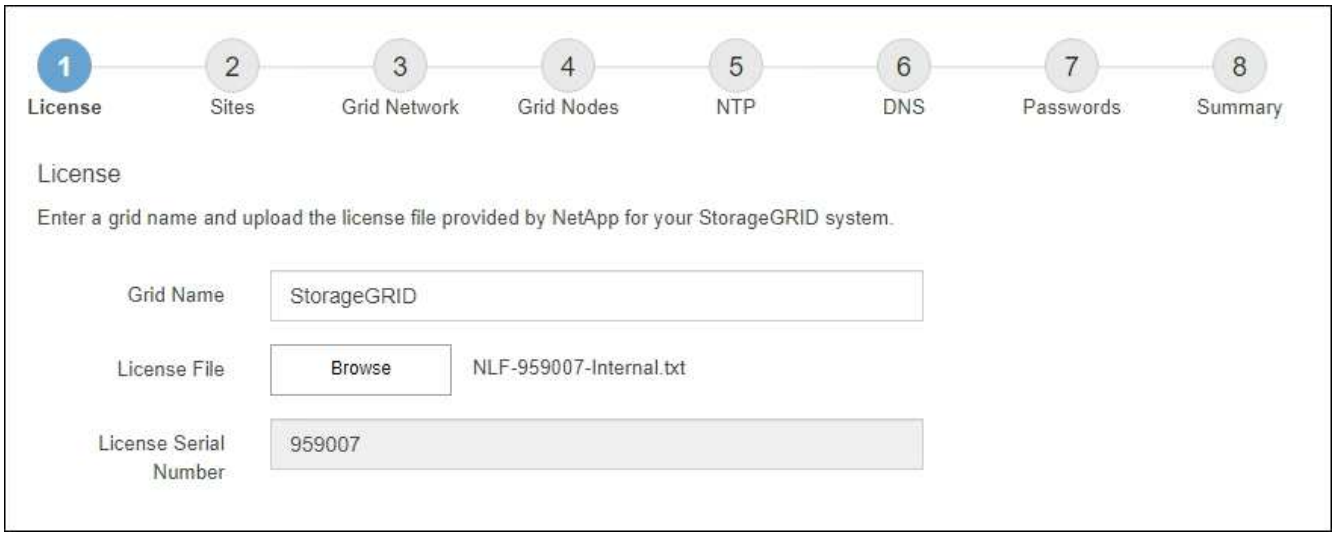
1. 라이센스 페이지의 * 그리드 이름 * 필드에 StorageGRID 시스템에 대한 의미 있는 이름을 입력합니다.

   설치 후, 이름이 Nodes 메뉴 맨 위에 표시됩니다.

2. 찾아보기 * 를 선택하고 NetApp 라이센스 파일을 찾은 (`NLF-*unique-id*.txt`다음 * 열기 * 를 선택합니다.

   라이센스 파일의 유효성이 검사되고 일련 번호가 표시됩니다.

   StorageGRID 설치 아카이브에는 제품에 대한 지원 권한이 없는 무료 라이센스가 포함되어 있습니다. 설치 후 지원을 제공하는 라이센스로 업데이트할 수 있습니다.



3. 다음 * 을 선택합니다.

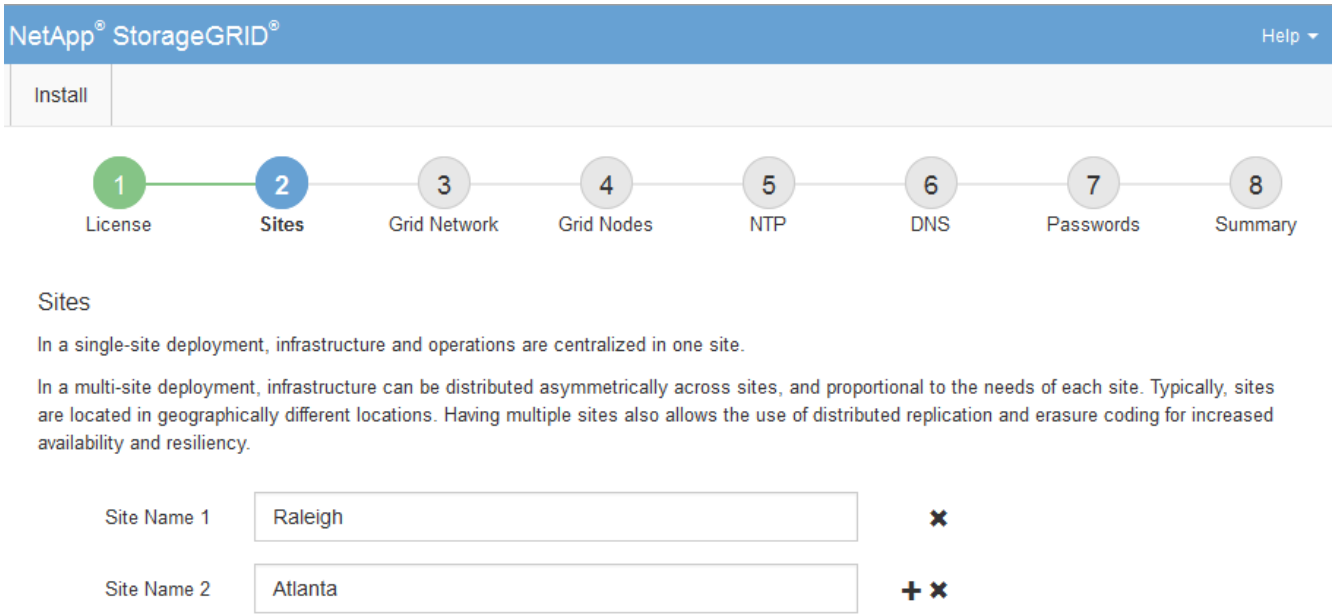
사이트를 추가합니다

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

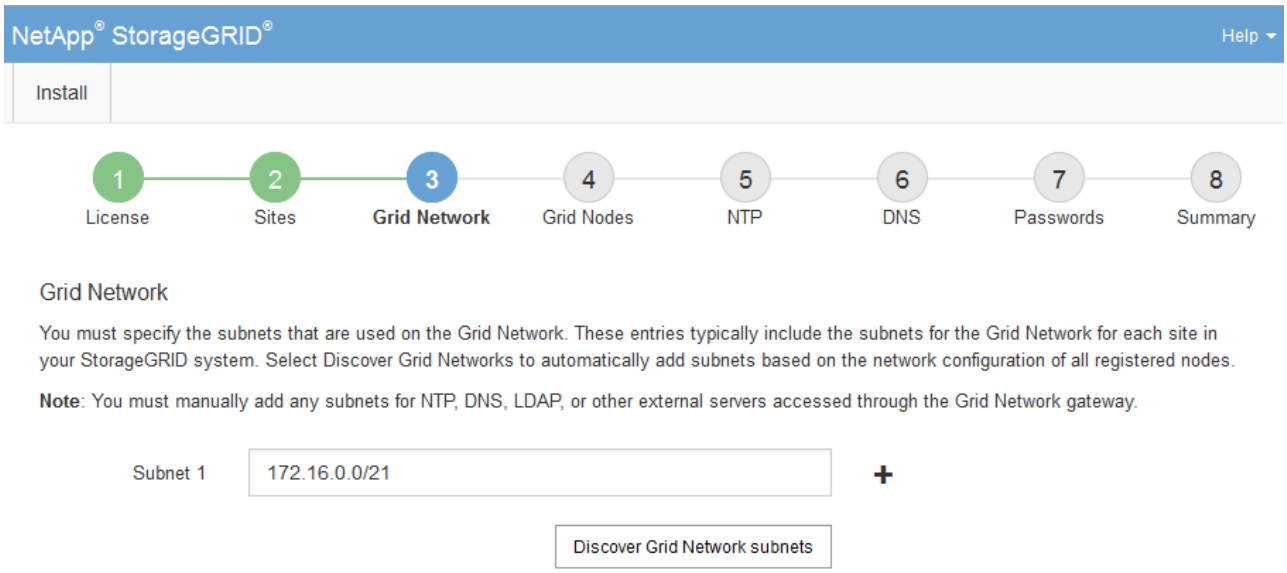
서브넷 항목에는 그리드 네트워크를 통해 연결할 수 있어야 하는 서브넷과 함께 StorageGRID 시스템의 각 사이트에 대한 그리드 네트워크의 서브넷이 포함됩니다.

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. 그리드 네트워크의 모든 사이트에 대해 모든 서브넷을 지정해야 합니다.
   - 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.

◦ 그리드 네트워크 게이트웨이를 통해 액세스하는 NTP, DNS, LDAP 또는 기타 외부 서버에 대해 서브넷을 수동으로 추가해야 합니다.



3. 다음 * 을 클릭합니다.

보류 중인 그리드 노드를 승인합니다

StorageGRID 시스템에 가입하려면 각 그리드 노드를 승인해야 합니다.

시작하기 전에

모든 가상 및 StorageGRID 어플라이언스 그리드 노드를 구축했습니다.

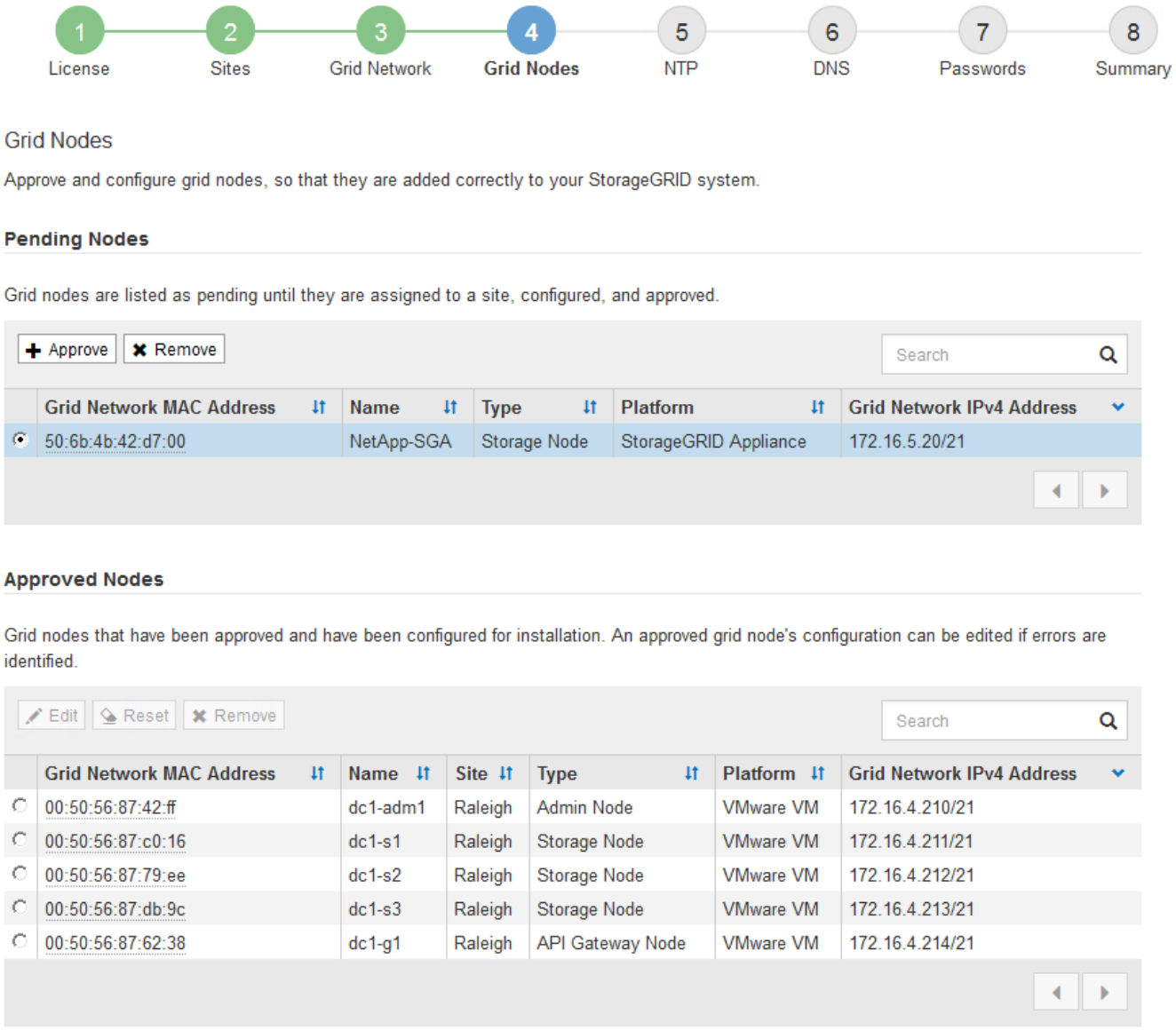
일부 노드를 나중에 설치하는 대신 모든 노드를 한 번 설치하는 것이 더 효율적입니다.

단계

1. Pending Nodes(보류 중인 노드) 목록을 검토하고 배포된 모든 그리드 노드가 표시되는지 확인합니다.

그리드 노드가 누락된 경우 그리드 노드가 성공적으로 배포되었으며 admin_IP에 대해 설정된 기본 관리 노드의 올바른 그리드 네트워크 IP가 있는지 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 노드에 대한 사이트의 시스템 이름입니다.
   - * 이름 *: 노드의 시스템 이름입니다. 기본적으로 노드를 구성할 때 지정한 이름이 지정됩니다.

     시스템 이름은 내부 StorageGRID 작업에 필요하며 설치를 완료한 후에는 변경할 수 없습니다. 그러나 설치 프로세스의 이 단계에서 필요에 따라 시스템 이름을 변경할 수 있습니다.

     - * 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.

- * 스토리지 유형 * (스토리지 노드에만 해당): 새 스토리지 노드가 데이터 전용, 메타데이터 전용 또는 둘 다에 대해서만 사용되도록 지정합니다. 옵션은 * 데이터 및 메타데이터 * ("결합"), * 데이터 전용 * 및 * 메타데이터만 * 입니다.

  이러한 노드 유형의 요구 사항에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

- * 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. 구성된 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. 구성된 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 제거합니다.

f. Pending Nodes 테이블에서 노드를 제거합니다.

g. 대기 중인 노드 목록에 노드가 다시 나타날 때까지 기다립니다.

h. 적절한 네트워크를 구성할 수 있는지 확인합니다. 어플라이언스 설치 프로그램의 IP 구성 페이지에서 제공한 정보로 이미 채워져야 합니다.

   자세한 내용은 해당 어플라이언스 모델의 설치 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. 구성된 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 제거합니다.

   f. Pending Nodes 테이블에서 노드를 제거합니다.

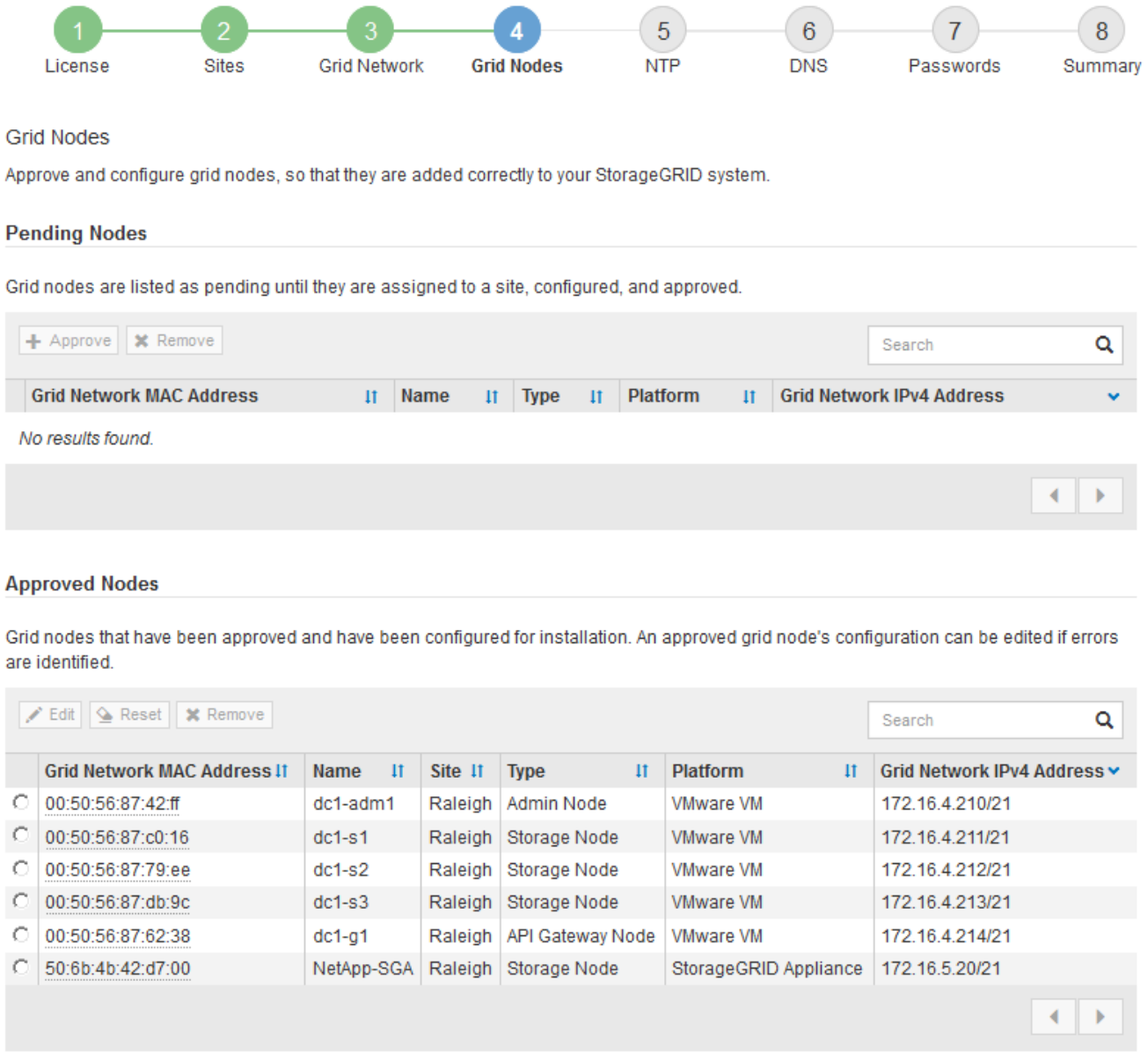
   g. 대기 중인 노드 목록에 노드가 다시 나타날 때까지 기다립니다.

   h. 적절한 네트워크를 구성할 수 있는지 확인합니다. 어플라이언스 설치 프로그램의 IP 구성 페이지에서 제공한 정보로 이미 채워져야 합니다.

      자세한 내용은 어플라이언스 설치 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.

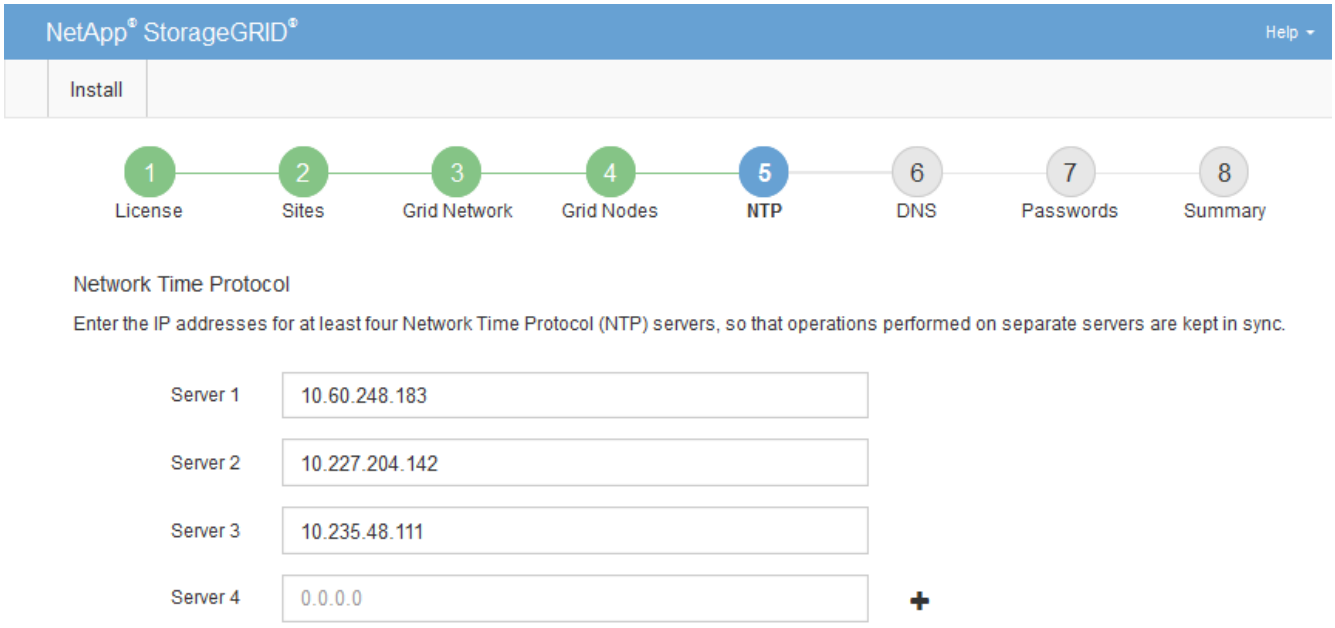
> 프로덕션 수준 StorageGRID 설치에 외부 NTP 소스를 지정할 때 Windows Server 2016 이전 버전의 Windows에서는 Windows 시간(W32Time) 서비스를 사용하지 마십시오. 이전 버전의 Windows의 시간 서비스는 정확하지 않으며 StorageGRID와 같은 고정밀 환경에서 사용하기 위해 Microsoft에서 지원되지 않습니다.
>
> "정확도가 높은 환경에 대한 Windows 시간 서비스를 구성하기 위한 경계를 지원합니다"

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.

DNS 서버 정보를 지정합니다

IP 주소 대신 호스트 이름을 사용하여 외부 서버에 액세스할 수 있도록 StorageGRID 시스템에 대한 DNS 정보를 지정해야 합니다.

이 작업에 대해

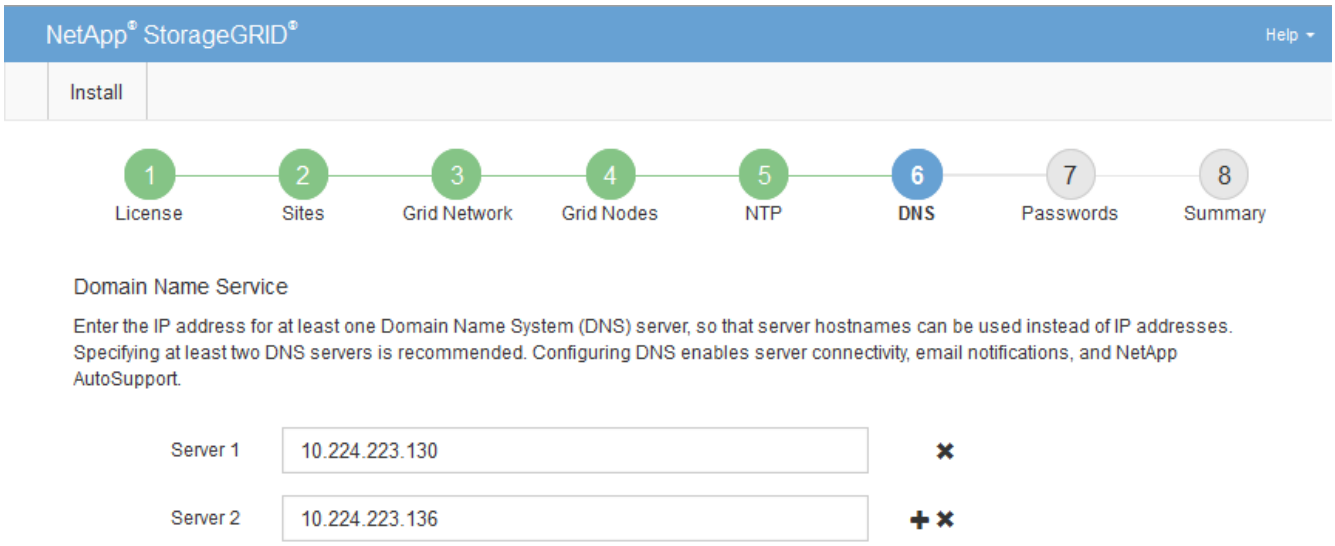
를 "DNS 서버 정보입니다" 지정하면 이메일 알림 및 AutoSupport에 IP 주소 대신 FQDN(정규화된 도메인 이름) 호스트 이름을 사용할 수 있습니다.

제대로 작동하려면 DNS 서버를 두 대 또는 세 대 지정합니다. 3개 이상을 지정하면 일부 플랫폼의 알려진 OS 제한 때문에 3개만 사용할 수 있습니다. 사용자 환경에 라우팅 제한이 있는 경우 개별 노드(일반적으로 사이트의 모든 노드)에서 최대 3개의 DNS 서버로 구성된 다른 세트를 사용할 수 "DNS 서버 목록을 사용자 지정합니다"있습니다.

가능한 경우 각 사이트에서 로컬로 액세스할 수 있는 DNS 서버를 사용하여 isfan 사이트가 외부 대상의 FQDN을 확인할 수 있도록 합니다.

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 `Passwords.txt` 복구 패키지의 파일에 저장됩니다.

단계

1. Provisioning Passphrase * 에서 StorageGRID 시스템의 그리드 토폴로지를 변경하는 데 필요한 프로비저닝

암호를 입력합니다.

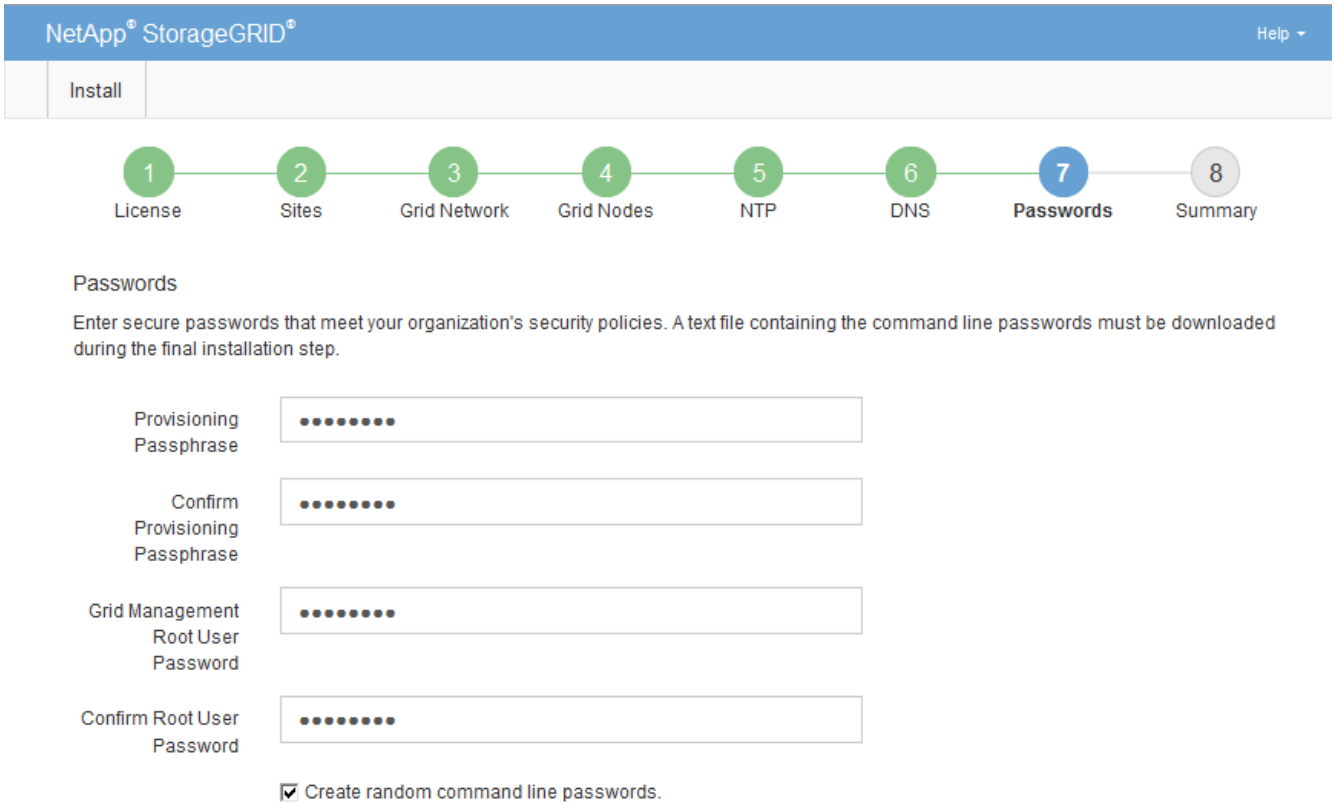
프로비저닝 암호를 안전한 장소에 보관합니다.

> 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. 그리드 관리 루트 사용자 암호 * 에 그리드 관리자에 "루트" 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. Clear * 임의의 명령줄 암호 만들기 * 기본 암호를 사용하여 "root" 또는 "admin" 계정을 사용하여 명령줄에서 그리드 노드에 액세스하려는 경우 데모 그리드에만 사용합니다.

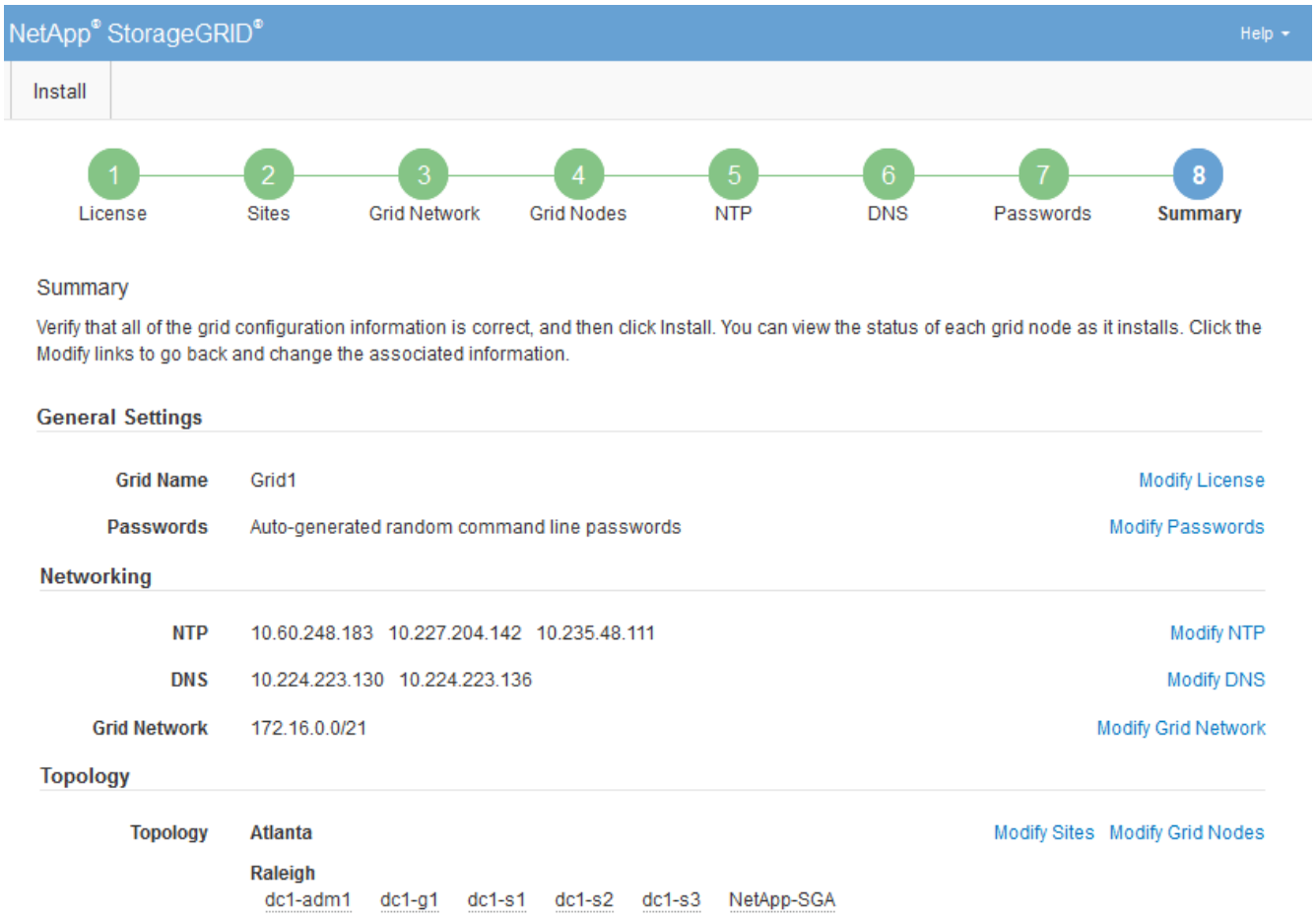
> 복구 패키지 파일을 다운로드하라는 메시지가 (`sgws-recovery-package-id-revision.zip`표시됩니다.) 요약 페이지에서 * 설치 * 를 클릭하면 됩니다. "이 파일을 다운로드합니다"설치를 완료해야 합니다. 시스템에 액세스하는 데 필요한 암호는 `Passwords.txt` 복구 패키지 파일에 포함된 파일에 저장됩니다.

6. 다음 * 을 클릭합니다.

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. 자세한 내용은 을 "네트워킹 지침" 참조하십시오.

4. 복구 패키지 다운로드 * 를 클릭합니다.

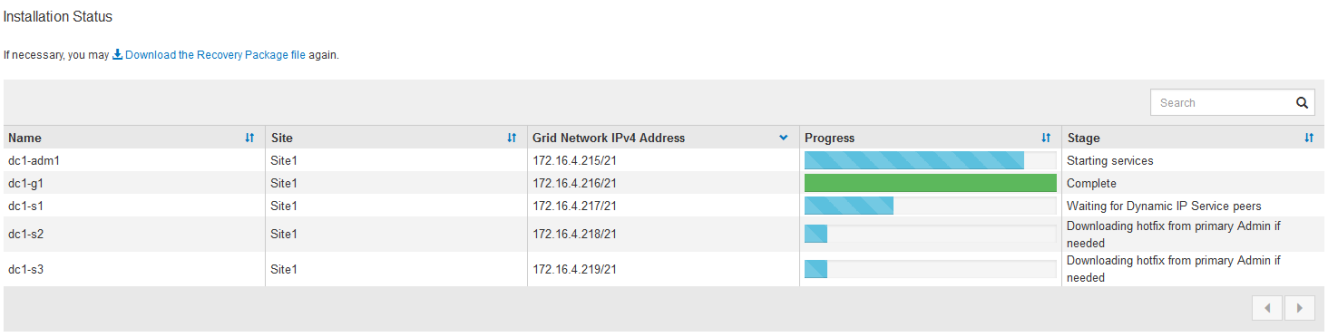
   그리드 토폴로지가 정의된 지점으로 설치가 진행되면 복구 패키지 파일을 다운로드하라는 메시지가 (`.zip`표시됩니다.) 이 파일의 내용에 성공적으로 액세스할 수 있는지 확인합니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 다운로드해야 합니다. 백그라운드에서 설치가 계속되지만 이 파일을 다운로드하여 확인할 때까지 설치를 완료하고 StorageGRID 시스템에 액세스할 수 없습니다.

5. 파일의 내용을 추출한 다음 안전하고 별도의 두 위치에 저장할 수 있는지 확인합니다 `.zip`.

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

6. 복구 패키지 파일 * 을 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.

  그리드 네트워크 구성이 DHCP에 의해 변경될 때 노드가 재부팅되므로 DHCP 변경이 여러 노드에 동시에 영향을 미칠 경우 운영이 중단될 수 있습니다.

- 그리드 노드의 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 변경하려면 IP 변경 절차를 사용해야 합니다. 을 "IP 주소를 구성합니다"참조하십시오.
- 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.

REST API 설치

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 데이터 형식에 대해 잘 알고 있다고 가정합니다.

API 문서 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.
- * Temporary-password * — 설치 중 mgmt-API를 보호하기 위한 임시 암호의 작동.

다음 단계로 넘어갑니다

설치를 완료한 후 필요한 통합 및 구성 작업을 수행합니다. 필요에 따라 옵션 작업을 수행할 수 있습니다.

필수 작업

- "테넌트 계정을 생성합니다" StorageGRID 시스템에 오브젝트를 저장하는 데 사용되는 S3 클라이언트 프로토콜의 경우
- "시스템 액세스를 제어합니다" 그룹 및 사용자 계정을 구성합니다. 선택적으로 Active Directory 또는 OpenLDAP와 같은 관리 그룹과 사용자를 가져올 수 "통합 ID 소스를 구성합니다"있습니다. 또는, 할 수 "로컬 그룹 및 사용자를 생성합니다"있습니다.
- 개체를 StorageGRID 시스템에 업로드하는 데 사용할 클라이언트 응용 프로그램을 통합하고 "S3 API를 사용합니다"테스트합니다.
- "ILM(정보 수명 주기 관리) 규칙 및 ILM 정책을 구성합니다" 를 사용하여 오브젝트 데이터를 보호하려고 합니다.
- 설치에 어플라이언스 스토리지 노드가 포함된 경우 SANtricity OS를 사용하여 다음 작업을 완료합니다.

◦ 각 StorageGRID 어플라이언스에 연결하십시오.

◦ AutoSupport 데이터가 수신되었는지 확인합니다.

을 "하드웨어를 설정합니다"참조하십시오.

- 을 검토하고 따라 "StorageGRID 시스템 강화 지침"보안 위험을 제거합니다.
- "시스템 경고에 대한 이메일 알림을 구성합니다"..

선택적 태스크입니다

- "그리드 노드 IP 주소를 업데이트합니다" 배포를 계획하고 복구 패키지를 생성한 이후에 변경된 경우
- "스토리지 암호화를 구성합니다"필요한 경우.
- "스토리지 압축을 구성합니다" 필요한 경우 저장된 개체의 크기를 줄입니다.
- "VLAN 인터페이스를 구성합니다" 필요한 경우 네트워크 트래픽을 격리하고 분할합니다.
- "고가용성 그룹을 구성합니다" 필요한 경우 Grid Manager, Tenant Manager 및 S3 클라이언트의 연결 가용성을 향상시킵니다.
- "로드 밸런서 엔드포인트를 구성합니다" 필요한 경우 S3 클라이언트 연결의 경우

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 관리자 노드에서 찾음)

호스트에서 다음 설치 로그 파일을 사용할 수 있습니다.

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

로그 파일에 액세스하는 방법에 대한 자세한 내용은 을 "로그 파일 및 시스템 데이터를 수집합니다"참조하십시오.

관련 정보

"StorageGRID 시스템 문제를 해결합니다"

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 Debian에 StorageGRID를 설치합니다

Ubuntu 또는 Debian에 StorageGRID를 설치하기 위한 빠른 시작

다음 상위 단계에 따라 Ubuntu 또는 Debian StorageGRID 노드를 설치합니다.

1 준비

- 에 대해 자세히 "StorageGRID 아키텍처 및 네트워크 토폴로지"알아보십시오.
- 에 대해 자세히 "StorageGRID 네트워킹"알아보십시오.
- 를 수집하고 "필요한 정보 및 자료"준비합니다.
- 필요한 를 "CPU 및 RAM"준비합니다.
- 에 대해 를 "스토리지 및 성능 요구사항"제공합니다.
- "Linux 서버를 준비합니다" 그러면 StorageGRID 노드가 호스팅됩니다.

2 구축

그리드 노드 구축 그리드 노드를 구축하면 StorageGRID 시스템의 일부로 생성되고 하나 이상의 네트워크에 연결됩니다.

- 1단계에서 준비한 호스트에 소프트웨어 기반 그리드 노드를 배포하려면 Linux 명령줄과 를 "노드 구성 파일 "사용합니다.
- StorageGRID 어플라이언스 노드를 배포하려면 를 "하드웨어 설치를 빠르게 시작합니다"따르십시오.

3 구성

모든 노드가 배포되면 Grid Manager를 사용하여 를 "그리드를 구성하고 설치를 완료합니다"수행합니다.

설치를 자동화합니다

StorageGRID 호스트 서비스 설치 및 그리드 노드 구성을 자동화하여 시간을 절약하고 일관성을 제공할 수 있습니다.

- Ansible, Puppet, Chef와 같은 표준 오케스트레이션 프레임워크를 사용하여 다음을 자동화합니다.
  - Ubuntu 또는 Debian 설치
  - 네트워킹 및 스토리지 구성
  - 컨테이너 엔진 및 StorageGRID 호스트 서비스 설치
  - 가상 그리드 노드 구축

  을 "StorageGRID 호스트 서비스의 설치 및 구성을 자동화합니다"참조하십시오.
- 그리드 노드를 배포한 후 "StorageGRID 시스템의 구성을 자동화합니다"설치 아카이브에 제공된 Python 구성 스크립트를 사용합니다.
- "어플라이언스 그리드 노드의 설치 및 구성을 자동화합니다"
- StorageGRID 구축의 고급 개발자인 경우 를 사용하여 그리드 노드 설치를 "REST API 설치"자동화합니다.

Ubuntu 또는 Debian에서 설치를 계획하고 준비합니다

필요한 정보 및 자료

StorageGRID를 설치하기 전에 필요한 정보와 자료를 수집하고 준비합니다.

필수 정보입니다

네트워크 계획

각 StorageGRID 노드에 연결할 네트워크 StorageGRID는 트래픽 분리, 보안 및 관리의 편의를 위해 여러 네트워크를 지원합니다.

StorageGRID 를 "네트워킹 지침"참조하십시오.

네트워크 정보

각 그리드 노드에 할당할 IP 주소와 DNS 및 NTP 서버의 IP 주소입니다.

그리드 노드용 서버

구축할 StorageGRID 노드의 수와 유형을 지원하기에 충분한 리소스를 제공하는 물리적 서버 세트, 가상 서버 또는 둘 다 식별합니다.

StorageGRID 설치에서 StorageGRID 어플라이언스(하드웨어) 스토리지 노드를 사용하지 않는 경우 BBWC(배터리 지원 쓰기 캐시)와 함께 하드웨어 RAID 스토리지를 사용해야 합니다. StorageGRID는 VSAN(Virtual Storage Area Network), 소프트웨어 RAID 또는 RAID 보호 사용을 지원하지 않습니다.

노드 마이그레이션(필요한 경우)

"노드 마이그레이션에 대한 요구사항"서비스 중단 없이 물리적 호스트에 대해 예약된 유지 관리를 수행하려는 경우을 이해합니다.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

필수 자료

NetApp StorageGRID 라이센스

디지털 서명된 유효한 NetApp 라이센스가 있어야 합니다.

테스트 및 개념 증명 그리드에 사용할 수 있는 비운영 라이센스가 StorageGRID 설치 아카이브에 포함되어 있습니다.

StorageGRID 설치 아카이브

"StorageGRID 설치 아카이브를 다운로드하고 파일 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"

StorageGRID 설치 파일을 다운로드하고 압축을 풉니다

StorageGRID 설치 아카이브를 다운로드하고 필요한 파일을 추출해야 합니다. 선택적으로 설치 패키지의 파일을 수동으로 확인할 수 있습니다.

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 Ubuntu 또는 Debian용 .tgz 또는 .zip 설치 아카이브를 선택합니다.

   `.zip`서비스 랩톱에서 Windows를 실행하는 경우 파일을 선택합니다.

7. 설치 아카이브를 저장합니다.
8. 설치 아카이브를 확인해야 하는 경우:

   a. StorageGRID 코드 서명 확인 패키지를 다운로드합니다. 이 패키지의 파일 이름은 StorageGRID 소프트웨어 버전의 형식을 `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` 사용합니다. `<version-number>`

   b. 의 단계를 "설치 파일을 수동으로 확인합니다"따릅니다.

9. 설치 아카이브에서 파일 압축을 풉니다.
10. 필요한 파일을 선택합니다.

    필요한 파일은 계획된 그리드 토폴로지와 StorageGRID 시스템 배포 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.
/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	파일의 MD5 체크섬 `/debs/storagegrid-webscale-images-version-SHA.deb`.
/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 이 스크립트를 Ping 연합 통합에 사용할 수도 있습니다.
/debs/configure -StorageGrid.sample.json 을 참조하십시오	스크립트와 함께 사용할 예제 구성 파일 `configure-storagegrid.py`
/debs/configure -StorageGrid.blank.json 을 참조하십시오	스크립트와 함께 사용할 빈 구성 `configure-storagegrid.py` 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.
	Active Directory 또는 Ping 연방을 사용하여 SSO(Single Sign-On)를 사용하도록 설정한 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/debs/StorageGrid-ssoauth-Azure.js를 입력합니다	Azure와의 SSO 상호 작용을 수행하기 위해 Python 스크립트에 의해 호출되는 도우미 스크립트입니다. `storagegrid-ssoauth-azure.py`
/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.

설치 파일 수동 확인(선택 사항)

필요한 경우 StorageGRID 설치 아카이브의 파일을 수동으로 확인할 수 있습니다.

시작하기 전에

에서 "StorageGRID용 NetApp 다운로드 페이지" 가져온 "검증 패키지를 다운로드했습니다"것입니다.

단계

1. 검증 패키지에서 아티팩트를 추출합니다.

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. 이러한 아티팩트가 추출되었는지 확인합니다.
   - Leaf 인증서: `Leaf-Cert.pem`
   - 인증서 체인: `CA-Int-Cert.pem`
   - 타임 스탬프 응답 체인: `TS-Cert.pem`
   - 체크섬 파일: `sha256sum`
   - 체크섬 서명: `sha256sum.sig`
   - 타임 스탬프 응답 파일: `sha256sum.sig.tsr`
3. 체인을 사용하여 리프 인증서가 유효한지 확인합니다.
   - 예 *: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`
   - 예상 출력 *: `Leaf-Cert.pem: OK`
4. leaf 인증서가 만료되어 step_2_에 실패한 경우 파일을 사용하여 `tsr` 확인합니다.
   - 예 *: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`
   - 예상 출력 포함 *: `Verification: OK`
5. 리프 인증서에서 공용 키 파일을 만듭니다.
   - 예 *: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`
   - 예상 출력 *:_none_
6. 공개 키를 사용하여 `sha256sum` 에 대해 파일을 `sha256sum.sig` 확인합니다.
   - 예 *: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`
   - 예상 출력 *: `Verified OK`
7. `sha256sum`새로 생성된 체크섬을 기준으로 파일 내용을 확인합니다.
   - 예 *: `sha256sum -c sha256sum`

   *예상 출력 * *<filename>*: OK:+는
   <filename> 다운로드한 아카이브 파일의 이름입니다.
8. "나머지 단계를 완료합니다" 를 눌러 적절한 설치 파일을 추출하고 선택합니다.

Ubuntu 및 **Debian**용 소프트웨어 요구 사항

가상 머신을 사용하여 모든 유형의 StorageGRID 노드를 호스팅할 수 있습니다. 각 그리드 노드에 대해 하나의 가상 머신이 필요합니다.

Ubuntu 또는 Debian에 StorageGRID를 설치하려면 타사 소프트웨어 패키지를 설치해야 합니다. 지원되는 일부 Linux 배포판에는 기본적으로 이러한 패키지가 포함되어 있지 않습니다. StorageGRID 설치를 테스트하는 소프트웨어 패키지 버전에는 이 페이지에 나열된 버전이 포함됩니다.

이러한 패키지를 필요로 하는 Linux 배포 및 컨테이너 런타임 설치 옵션을 선택했는데 Linux 배포판에 의해 자동으로 설치되지 않은 경우, 해당 공급자 또는 Linux 배포판의 지원 공급업체에서 제공하는 경우 여기에 나열된 버전 중 하나를 설치하십시오. 그렇지 않으면 공급업체에서 제공하는 기본 패키지 버전을 사용하십시오.

모든 설치 옵션에는 Podman 또는 Docker가 필요합니다. 두 패키지를 모두 설치하지 마십시오. 설치 옵션에 필요한 패키지만 설치합니다.

소프트웨어 전용 배포를 위한 컨테이너 엔진으로 Docker에 대한 지원은 더 이상 사용되지 않습니다. Docker는 향후 릴리즈에서 다른 컨테이너 엔진으로 대체될 예정입니다.

Python 버전을 테스트했습니다

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

Podman 버전을 테스트했습니다

- 3.2.3-0
- 3.4.4 + DS1
- 4.1.1-7
- 4.2.0-11
- 4.3.1+DS1-8+B1
- 4.4.1-8
- 4.4.1-12

Docker 버전을 테스트했습니다

Docker 지원은 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3 을 참조하십시오
- Docker-CE 23.0.6-1 을 참조하십시오
- Docker-CE 24.0.2-1 을 참조하십시오
- Docker-CE 24.0.4-1 을 참조하십시오

- Docker-CE 24.0.5-1 을 참조하십시오
- Docker-CE 24.0.7-1 을 참조하십시오
- 1.5-2 을 참조하십시오

CPU 및 **RAM** 요구 사항

StorageGRID 소프트웨어를 설치하기 전에 StorageGRID 시스템을 지원할 준비가 되도록 하드웨어를 확인 및 구성하십시오.

각 StorageGRID 노드에는 다음과 같은 최소 리소스가 필요합니다.

- CPU 코어: 노드당 8개
- RAM: 사용 가능한 총 RAM과 시스템에서 실행되는 비 StorageGRID 소프트웨어의 양에 따라 다릅니다
  - 일반적으로 노드당 최소 24GB, 총 시스템 RAM보다 2 ~ 16GB 작습니다
  - 각 테넌트당 최소 64GB의 버킷이 약 5,000개 있습니다

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 스토리지 관리, 메타데이터 예약 공간 설정 증가, CPU 및 메모리 사용량 모니터링에 대한 자세한 내용은"관리" "모니터링", 및 "업그레이드 중"StorageGRID에 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.

도 "요구사항을 충족해야 합니다"참조하십시오.

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 모두 공유 스토리지에 저장해야 합니다. 자세한 내용은 을 "노드 컨테이너 마이그레이션 요구사항"참조하십시오.

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 호스트의 요구 사항입니다

StorageGRID 노드가 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.

LUN 사용 목적	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 을 참조하십시오스토리지 노드의 스토리지 요구 사항.
스토리지 노드(메타데이터만)	오브젝트 메타데이터	1	4TB 자세한 내용은 을 스토리지 노드의 스토리지 요구 사항참조하십시오. • 참고 *: 메타데이터 전용 스토리지 노드에는 하나의 rangedb만 필요합니다.
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 레벨에 따라 S3 오브젝트 키 이름 등의 사용자 입력 크기, 그리고 보존해야 하는 감사 로그 데이터의 양을 위해 각 관리 노드에서 감사 로그 LUN의 크기를 늘려야 할 수도 있습니다. 일반적으로 그리드는 S3 작업당 약 1KB의 감사 데이터를 생성합니다. 즉, 200GB LUN이 2일에서 3일 동안 매일 7천만 개의 작업 또는 초당 800개의 작업을 지원하게 됩니다.

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 "그리드 노드 복구"각 노드 유형에 대한 절차를 참조하십시오.

노드 유형입니다	컨테이너 풀입니다	시스템 데이터	오브젝트 데이터
스토리지 노드	100GB	90GB	4,000GB

노드 유형입니다	컨테이너 풀입니다	시스템 데이터	오브젝트 데이터
관리자 노드	100GB	490GB(LUN 3개)	_해당 사항 없음 _
게이트웨이 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.

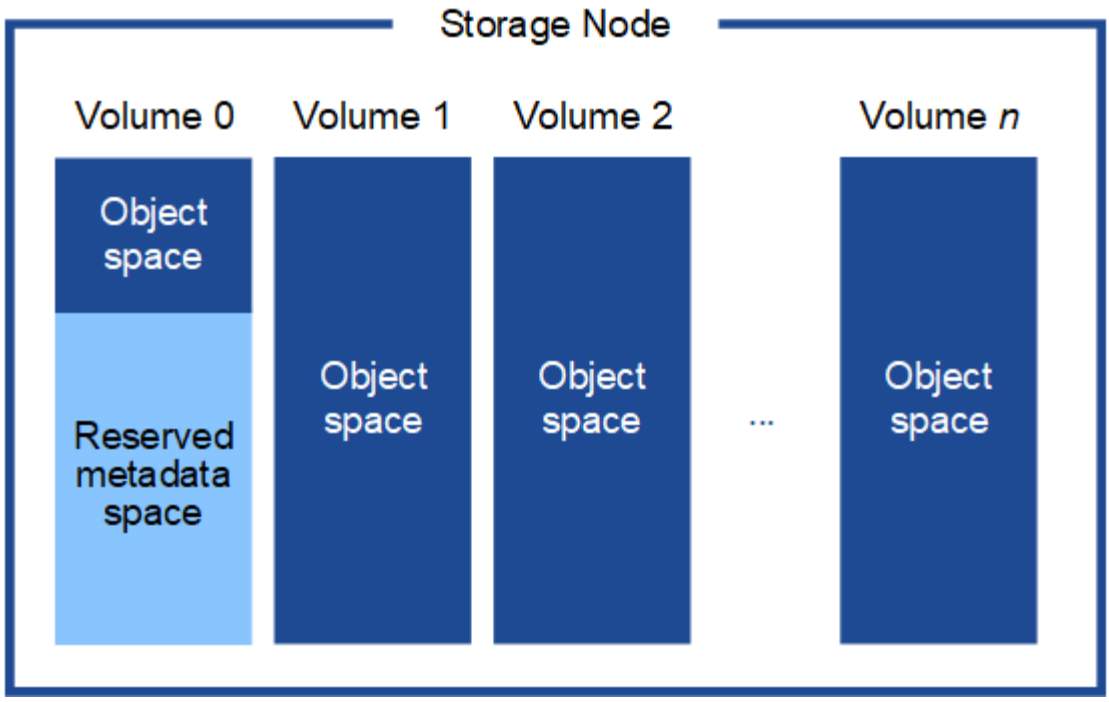
노드 유형입니다	**LUN** 사용 목적	**LUN** 수입니다	**LUN** 크기입니다
스토리지 노드	Docker 스토리지 풀	1	300GB(100GB/노드)
스토리지 노드	`/var/local` 볼륨	1	90GB
스토리지 노드	오브젝트 데이터	3	12TB(4TB/LUN)
관리자 노드	`/var/local` 볼륨	1	90GB
관리자 노드	관리자 노드 감사 로그	1	200GB
관리자 노드	관리자 노드 테이블	1	200GB
게이트웨이 노드	`/var/local` 볼륨	1	90GB
• 합계 *		• 9 *	• 컨테이너 풀: * 300GB • 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.

메타데이터 전용 스토리지 노드가 있는 그리드를 설치할 경우 그리드에는 오브젝트 스토리지용 최소 노드 수도 있어야 합니다. 메타데이터 전용 스토리지 노드에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

- 단일 사이트 그리드의 경우 객체 및 메타데이터에 대해 2개 이상의 스토리지 노드가 구성됩니다.
- 다중 사이트 그리드의 경우 사이트당 하나 이상의 스토리지 노드가 객체 및 메타데이터에 대해 구성됩니다.

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 이하의 용량을 할당하면 스토리지 노드가 시작 시 스토리지 읽기 전용 상태로 전환되고 객체 메타데이터만 저장할 수 있습니다.

> ⓘ 볼륨 0에 500GB 미만의 용량을 할당할 경우(비운영 전용) 스토리지 볼륨 용량의 10%가 메타데이터용으로 예약됩니다.

- 새 시스템(StorageGRID 11.6 이상)을 설치하고 각 스토리지 노드에 128MB 이상의 RAM이 있는 경우 볼륨 0에 8TB 이상을 할당합니다. 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 을 "오브젝트 메타데이터 스토리지 관리"참조하십시오.

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 이동합니다. 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 "그리드 노드 종료"참조하십시오.

VMware Live Migration은 지원되지 않습니다

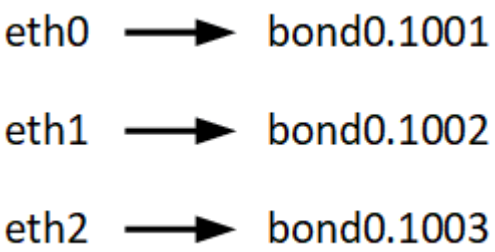
VMware VM에서 베어 메탈 설치를 수행할 때 OpenStack Live Migration 및 VMware Live vMotion을 사용하면 가상 머신 클록 시간이 증가하며 어떠한 유형의 그리드 노드에서도 지원되지 않습니다. 드물지만 잘못된 클럭 시간으로 인해 데이터 또는 구성 업데이트가 손실될 수 있습니다.

콜드 마이그레이션이 지원됩니다. 콜드 마이그레이션에서는 StorageGRID 노드를 호스트 간에 마이그레이션하기 전에 종료해야 합니다. 의 지침을 "그리드 노드 종료"참조하십시오.

일관된 네트워크 인터페이스 이름

한 호스트에서 다른 호스트로 노드를 이동하려면 StorageGRID 호스트 서비스가 노드가 현재 위치에 있는 외부 네트워크 연결을 새 위치에서 복제할 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 호스트 간에 일관된 네트워크 인터페이스 이름을 지정하는 방법은 여러 가지가 있습니다. 몇 가지 예는 를 참조하십시오."호스트 네트워크를 구성합니다"

공유 스토리지

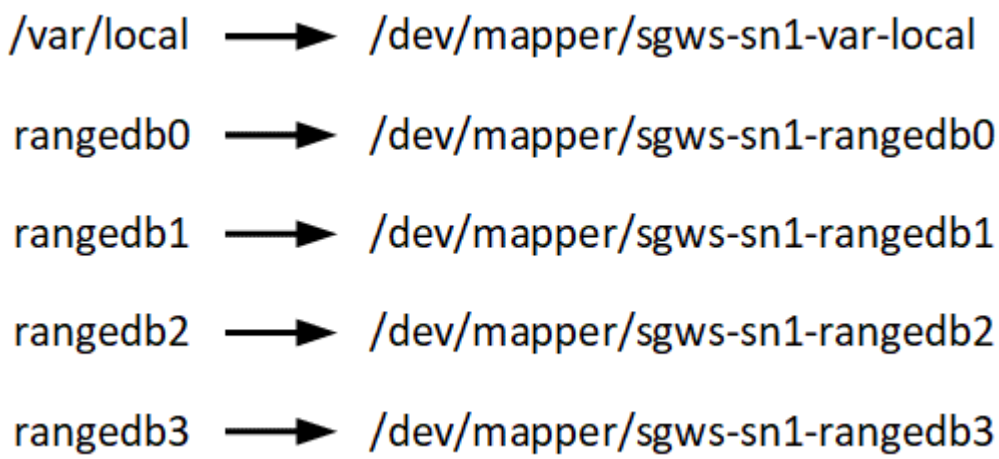
오버헤드가 낮은 노드를 신속하게 마이그레이션하기 위해 StorageGRID 노드 마이그레이션 기능은 노드 데이터를 물리적으로 이동하지 않습니다. 대신 노드 마이그레이션은 다음과 같이 한 쌍의 엑스포트 및 임포트 작업으로 수행됩니다.

단계

1. "노드 내보내기" 작업 중에 HostA에서 실행 중인 노드 컨테이너에서 소량의 영구 상태 데이터가 추출되고 해당 노드의 시스템 데이터 볼륨에 캐시됩니다. 그런 다음 HostA의 노드 컨테이너가 인스턴스화됩니다.
2. "노드 가져오기" 작업 중에 HostA에 적용된 동일한 네트워크 인터페이스와 블록 스토리지 매핑을 사용하는 HostB의 노드 컨테이너가 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 StorageGRID 스토리지 노드에 대한 블록 디바이스 매핑 솔루션 중 하나를 보여 줍니다. 이 경우 DM 다중 경로가 호스트에서 사용되고 별칭 필드는 모든 호스트에서 사용할 수 있는 일관되고 알기 쉬운 블록 디바이스 이름을 제공하기 위해 에 `/etc/multipath.conf` 사용되었습니다.



호스트 준비**(Ubuntu** 또는 **Debian)**

설치 중에 호스트 전체의 설정이 변경되는 방식

베어 메탈 시스템에서 StorageGRID는 호스트 전체 설정을 일부 변경합니다 `sysctl`.

다음과 같은 변경 사항이 적용됩니다.

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
```

```
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1
```

```
# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Linux를 설치합니다

모든 Ubuntu 또는 Debian GRID 호스트에 StorageGRID를 설치해야 합니다. 지원되는 버전 목록은 NetApp 상호 운용성 매트릭스 툴을 참조하십시오.

시작하기 전에

운영 체제가 아래 나열된 StorageGRID의 최소 커널 버전 요구 사항을 충족하는지 확인합니다. 명령을 사용하여 `uname -r` 운영 체제의 커널 버전을 가져오거나 OS 공급업체에 문의하십시오.

- 참고: * Ubuntu 버전 18.04 및 20.04에 대한 지원은 더 이상 사용되지 않으며 향후 릴리스에서 제거될 예정입니다.

Ubuntu 버전	최소 커널 버전	커널 패키지 이름입니다
18.04.6(사용되지 않음)	5.4.0-150 - 일반	linux-image-5.4.0-150-generic/bionic-updates, bionic-security, 현재 5.4.0-150.167-18.04.1
20.04.5(사용되지 않음)	5.4.0-131 - 일반	linux-image-5.4.0-131-generic/focal-updates, 현재 5.4.0-131.147

Ubuntu 버전	최소 커널 버전	커널 패키지 이름입니다
22.04.1	5.15.0-47 - 일반	linux-image-5.15.0-47-generic/jammy-updates, jammy-security, 현재 5.15.0-47.51
24.04	6.8.0-31 - 일반	linux-image-6.8.0-31-generic/noble, 현재 6.8.0-31.31

참고**:** 데비안 버전 11에 대한 지원은 더 이상 사용되지 않으며 향후 릴리스에서 제거될 예정입니다.

데비안 버전	최소 커널 버전	커널 패키지 이름입니다
11(폐기됨)	5.10.0-18-AMD64	Linux-image-5.10.0-18-AMD64/stable, 현재 5.10.150-1
12	6.1.0-9-AMD64	linux-image-6.1.0-9-amd64/stable, 현재 6.1.27-1

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 선택 취소 상태를 유지할 수 있습니다.

2. 모든 호스트가 Ubuntu 또는 Debian 패키지 리포지토리에 액세스할 수 있는지 확인합니다.
3. 스왑이 활성화된 경우:
   a. 다음 명령을 실행합니다. `$ sudo swapoff --all`
   b. 설정을 유지하려면 에서 모든 스왑 항목을 `/etc/fstab` 제거합니다.

> 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". 최신 Ubuntu 버전에서는 AppArmor를 완전히 비활성화할 수 없습니다.

  AppArmor를 비활성화하면 StorageGRID 로그 파일에 AppArmor가 활성화되었음을 나타내는 항목이 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.

시작하기 전에

- 를 검토했습니다."StorageGRID 네트워킹 지침"
- 에 대한 정보를 검토했습니다."노드 컨테이너 마이그레이션 요구사항"
- 가상 호스트를 사용하는 경우 호스트 네트워크를 구성하기 전에 를 읽은 MAC 주소 복제에 대한 고려 사항 및 권장 사항것입니다.

> 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.

> Bond 또는 Bridge 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 무작위로 생성된 주소이지만 노드 구성 키를 사용하여 주소를 설정한 경우 `_NETWORK_MAC` 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 클론 생성이 활성화되지 않음: `_CLONE_MAC` 노드 구성 파일의 키가 설정되지 않았거나 "false"로 설정되어 있지 않으면 호스트는 호스트 NIC MAC을 사용하고 컨테이너에 StorageGRID 생성 MAC을 갖게 됩니다. `_NETWORK_MAC` 키에 주소가 설정되어 있으면 `_NETWORK_MAC` 컨테이너에 키에 지정된 주소가 `_NETWORK_MAC` 지정됩니다. 이러한 키 구성을 위해서는 무차별 모드를 사용해야 합니다.
- MAC 클론 생성 활성화: 노드 구성 파일의 키가 "true"로 설정된 경우 `_CLONE_MAC` 컨테이너에서 호스트 NIC MAC을 사용하고, 키에 MAC이 지정되지 않은 경우 호스트는 StorageGRID에서 생성된 MAC을 사용합니다. `_NETWORK_MAC` 키에 주소가 설정된 경우 `_NETWORK_MAC` 호스트는 생성된 주소가 아닌 지정된 주소를 사용합니다. 이 키 구성에서 무차별 모드를 사용해서는 안 됩니다.

> MAC 주소 클로닝을 사용하지 않고 하이퍼바이저에 의해 할당된 것이 아닌 MAC 주소에 대한 데이터를 모든 인터페이스에서 수신 및 전송하도록 허용하려면 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 복제를 활성화하려면 을 "노드 구성 파일 생성 지침"참조하십시오.

Mac 클론 복제의 예

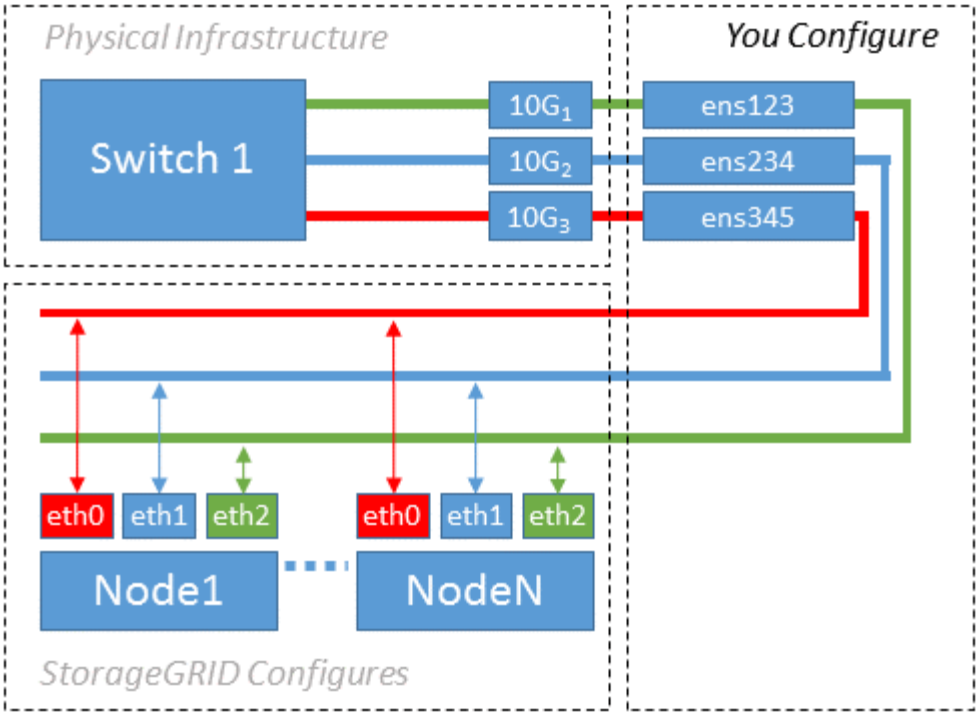
인터페이스 ens256의 경우 MAC 주소가 11:22:33:44:55:66이고 노드 구성 파일의 경우 다음 키가 있는 호스트에서 활성화된 MAC 클론 복제의 예:

- `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 NIC에 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

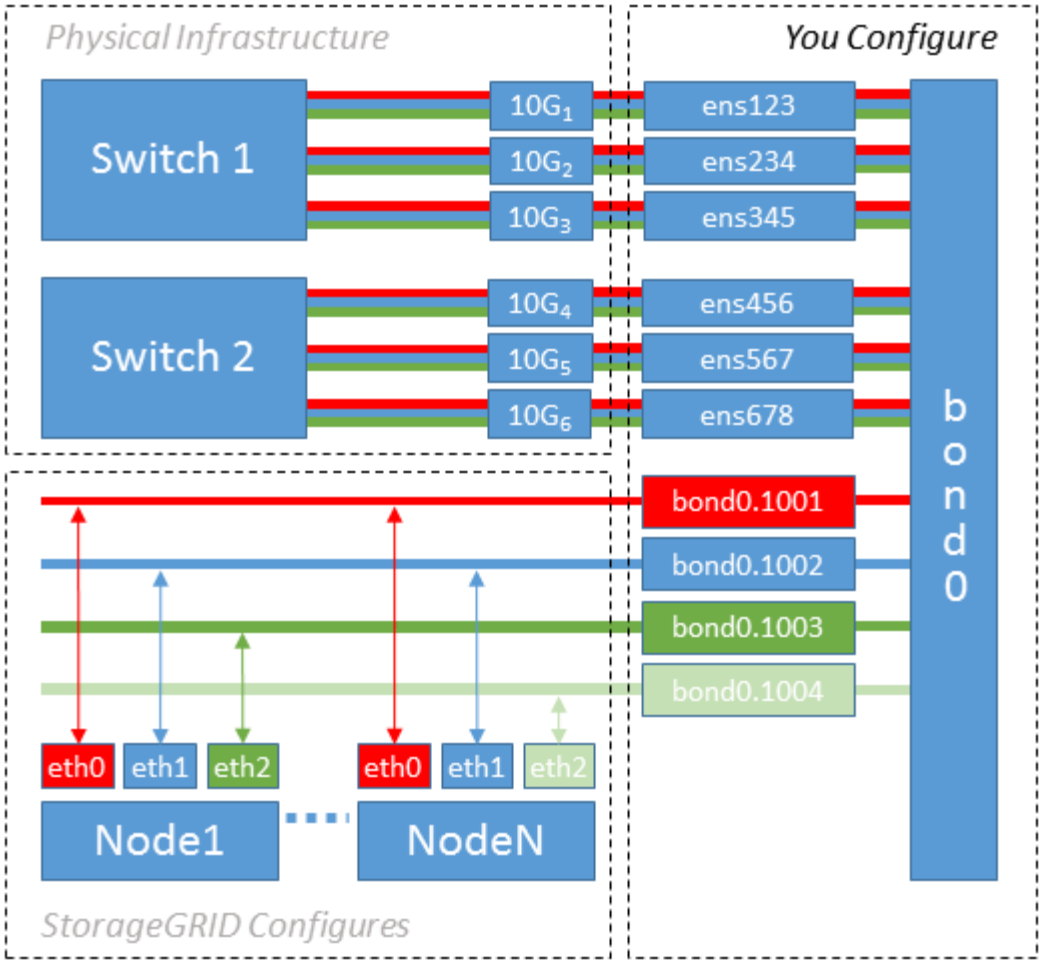
예제 2에서는 네트워크 인터페이스를 결합하거나 사용 중인 Linux 배포판에서 VLAN 인터페이스를 만드는 방법에 대해 잘 알고 있다고 가정합니다.

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 규칙을 사용하여 이 연결을 관련 "물리적 장치"로 사용하는 VLAN 인터페이스를 `physdev-name.VLAN ID` 생성합니다.

   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.

   이 호스트별 네트워킹 구성 체계에 대한 인터페이스 구성 파일 예가 제공됩니다.

관련 정보

"예 /etc/network/interfaces"

호스트 스토리지를 구성합니다

각 호스트에 블록 스토리지 볼륨을 할당해야 합니다.

시작하기 전에

이 과제를 수행하는 데 필요한 정보를 제공하는 다음 주제를 검토했습니다.

- "요구사항을 충족해야 합니다"
- "노드 컨테이너 마이그레이션 요구사항"

이 작업에 대해

블록 스토리지 볼륨(LUN)을 호스트에 할당할 때 "스토리지 요구 사항"의 표를 사용하여 다음을 확인합니다.

- 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.

메타데이터 전용 스토리지 노드에는 하나의 오브젝트 데이터 LUN만 필요합니다.

(/dev/sdb`볼륨 이름 목록을 작성할 때 "raw" 특수 장치 파일을 사용하지 마십시오. 이러한 파일은 호스트의 재부팅 시 변경될 수 있으며, 이는 시스템의 올바른 작동에 영향을 줍니다. iSCSI LUN 및 Device Mapper Multipathing을 사용하는 경우, 특히 SAN 토폴로지에 공유 스토리지에 대한 중복 네트워크 경로가 포함되어 있는 경우 디렉토리에서 다중 경로 별칭을 사용하는 `/dev/mapper 것이 좋습니다. 또는 영구 장치 이름에 대해 에서 시스템에서 만든 소프트링크를 사용할 수 /dev/disk/by-path/ 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 디바이스 매퍼 다중 경로 드라이버를 사용하는 경우 파일의 필드를 /etc/multipath.conf 사용할 수 alias 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
     }
     …
```

이러한 방식으로 별칭 필드를 사용하면 별칭이 호스트의 디렉토리에 블록 디바이스로 나타나므로 구성 또는 유지 관리 작업에서 블록 `/dev/mapper` 스토리지 볼륨을 지정해야 할 때마다 쉽게 검증된 친숙한 이름을 지정할 수 있습니다.

StorageGRID 노드 마이그레이션을 지원하고 장치 매퍼 다중 경로를 사용하도록 공유 스토리지를 설정하는 경우 모든 공동 위치 호스트에 공통 을 생성하고 설치할 수 `/etc/multipath.conf` 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.

> 소프트웨어 전용 배포를 위한 컨테이너 엔진으로 Docker에 대한 지원은 더 이상 사용되지 않습니다. Docker는 향후 릴리즈에서 다른 컨테이너 엔진으로 대체될 예정입니다.

관련 정보

- "요구사항을 충족해야 합니다"

- "노드 컨테이너 마이그레이션 요구사항"

컨테이너 엔진 저장소 볼륨을 구성합니다

컨테이너 엔진(Docker 또는 Podman)을 설치하기 전에 스토리지 볼륨을 포맷하고 마운트해야 할 수 있습니다.

> 소프트웨어 전용 배포를 위한 컨테이너 엔진으로 Docker에 대한 지원은 더 이상 사용되지 않습니다. Docker는 향후 릴리즈에서 다른 컨테이너 엔진으로 대체될 예정입니다.

이 작업에 대해

Docker 저장소 볼륨에 로컬 스토리지를 사용할 계획이고 이 포함된 호스트 파티션에 사용 가능한 공간이 충분하다면 이 단계를 건너뛸 수 있습니다 `/var/lib`.

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.

> 소프트웨어 전용 배포를 위한 컨테이너 엔진으로 Docker에 대한 지원은 더 이상 사용되지 않습니다. Docker는 향후 릴리즈에서 다른 컨테이너 엔진으로 대체될 예정입니다.

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

다음 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 합니다.

   예를 들어, `/tmp` 다음 단계에서 예제 명령을 사용할 수 있도록 디렉토리에 배치합니다.

2. 각 호스트에 루트로 로그인하거나 sudo 권한이 있는 계정을 사용하여 다음 명령을 실행합니다.

   먼저 패키지를 `service` 설치하고 패키지를 두 번째로 설치해야 `images` 합니다. 패키지를 이외의 디렉토리에 배치한 경우 `/tmp` 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. 이 `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` 명령을 실행할 때까지 명령이 실패합니다.

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 자동화하기 위한 선택적 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. 에서 StorageGRID 노드 구성 파일을 생성합니다 `/etc/storagegrid/nodes`
8. StorageGRID 노드 구성 파일의 유효성을 검사하는 중입니다
9. StorageGRID 호스트 서비스를 시작합니다

Ansible 역할 및 플레이북 예

예제 Ansible 역할 및 플레이북은 폴더에 설치 아카이브와 함께 `/extras` 제공됩니다. Ansible 플레이북에서는 역할이 호스트를 준비하고 타겟 서버에 StorageGRID를 설치하는 방법을 보여줍니다 `storagegrid`. 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.

StorageGRID의 구성을 자동화합니다

그리드 노드를 구축한 후 StorageGRID 시스템 구성을 자동화할 수 있습니다.

시작하기 전에

- 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 예제 구성 파일
configure -StorageGrid.blank.json을 지정합니다	스크립트에 사용할 빈 구성 파일입니다

- `configure-storagegrid.json`구성 파일을 만들었습니다. 이 파일을 작성하려면 예제 구성 파일(`configure-storagegrid.sample.json`)이나 빈 구성 파일을 수정할 수 (`configure-storagegrid.blank.json`있습니다.

이 작업에 대해

Python 스크립트와 `configure-storagegrid.json` 구성 파일을 사용하여 StorageGRID 시스템 구성을 자동화할 수 `configure-storagegrid.py` 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 `platform` 는 `debs`, `rpms` 또는 `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 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.

임의의 암호를 생성하도록 지정한 경우 파일을 열고 `Passwords.txt` StorageGRID 시스템에 액세스하는 데 필요한 암호를 찾습니다.

```
###################################################################
##### 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

"REST API 설치"

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 노드에 사용되지 않습니다.

노드 구성 파일의 위치입니다

각 StorageGRID 노드의 구성 파일을 `/etc/storagegrid/nodes` 노드가 실행될 호스트의 디렉토리에 배치합니다. 예를 들어 HostA에서 관리자 노드 1개, 게이트웨이 노드 1개 및 스토리지 노드 1개를 실행하려면 HostA에 3개의 노드 구성 파일을 배치해야 `/etc/storagegrid/nodes` 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 파일 이름 지정

구성 파일의 이름이 중요합니다. 형식은 입니다 `node-name.conf`. 여기서 `node-name` 는 노드에 할당한 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.
- 확장자는 32자 이하여야 합니다 `.conf`

에서 이러한 명명 규칙을 따르지 않는 파일은 `/etc/storagegrid/nodes` 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 관리자 노드와 `dc2-sn3.conf` 데이터 센터 2의 세 번째 스토리지 노드에 을 사용할 수 `dc1-adm1.conf` 있습니다. 그러나 모든 노드 이름이 명명 규칙을 따른다 하더라도 원하는 스키마를 사용할 수 있습니다.

노드 구성 파일의 내용입니다

구성 파일에는 키/값 쌍이 포함되어 있으며 한 줄에 하나의 키와 하나의 값이 있습니다. 각 키/값 쌍에 대해 다음 규칙을 따르십시오.

- 키와 값은 등호(=)와 선택적 공백으로 구분해야 합니다.
- 키에는 공백이 포함될 수 없습니다.
- 값에는 포함된 공백이 포함될 수 있습니다.
- 선행 또는 후행 공백은 무시됩니다.

다음 표에서는 지원되는 모든 키의 값을 정의합니다. 각 키에는 다음 중 하나가 지정됩니다.

- * 필수 *: 모든 노드 또는 지정된 노드 유형에 필요합니다
- * 모범 사례 *: 선택 사항이지만 권장됨
- * 선택 사항 *: 모든 노드에 대해 선택 사항입니다

관리 네트워크 키

관리_IP

값	지정
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.	모범 사례

관리 네트워크 구성

값	지정
DHCP, 정적 또는 비활성	선택 사항

관리_네트워크_**ESL**

값	지정
쉼표로 구분된 서브넷 목록으로, 이 노드가 Admin Network 게이트웨이를 사용하여 통신해야 하는 CIDR 표기법을 사용합니다. 예: `172.16.0.0/21,172.17.0.0/21`	선택 사항

Admin_network_Gateway를 선택합니다

값	지정

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.
 	
예:
 	
`1.1.1.1`
 	
`10.224.4.81`
	가 지정된 경우 `ADMIN_NETWORK_ESL` 필수입니다. 그렇지 않으면 선택 사항입니다.

admin_network_ip을 선택합니다

값	지정

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_config = static 인 경우 필요합니다.
	
	그렇지 않으면 선택 사항입니다.

admin_network_MAC입니다

값	지정
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`	선택 사항

admin_network_mask를 선택합니다

값	지정

이 노드의 IPv4 넷마스크는 관리자 네트워크에서 설정합니다. admin_network_config = static 인 경우 이 키를 지정하고 다른 값에 대해서는 이 키를 지정하지 마십시오.
 	
예:
 	
`255.255.255.0`
 	
`255.255.248.0`
	admin_network_ip을 지정하고 admin_network_Config=static인 경우 필수입니다.
	
	그렇지 않으면 선택 사항입니다.

admin_network_mtu

값	지정

Admin Network의 이 노드에 대한 MTU(Maximum Transmission Unit)입니다. admin_network_Config=DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 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:
 	
`1500`
 	
`8192`
	선택 사항

admin_network_target 을 선택합니다

값	지정

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:
 	
`bond0.1002`
 	
`ens256`
	모범 사례

admin_network_target_type입니다

값	지정
인터페이스(이 값만 지원됩니다.)	선택 사항

admin_network_target_type_interface_clone_MAC

값	지정
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 복제의 고려 사항 및 권장 사항(Red Hat Enterprise Linux)" • "MAC 주소 복제에 대한 고려 사항 및 권장 사항(Ubuntu 또는 Debian)"	모범 사례

admin_role을 선택합니다

값	지정
Primary 또는 Non-Primary 이 키는 node_type=vm_Admin_Node인 경우에만 필요하며 다른 노드 유형에 대해서는 지정하지 않습니다.	node_type=vm_admin_Node인 경우 필요합니다 그렇지 않으면 선택 사항입니다.

장치 키를 차단합니다

Block_device_audit_logs

값	지정

이 노드가 감사 로그의 영구 저장에 사용할 블록 디바이스 특수 파일의 경로 및 이름입니다.
 	
예:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	node_type이 vm_admin_Node인 노드에 필요합니다. 다른 노드 유형에는 지정하지 마십시오.

Block_device_RANGEDB_nnn을 선택합니다

값	지정

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 않습니다.
 	
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`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	필수:
	
	BLOCK_DEVICE_RANGEDB_000
	
	선택 사항:
	
	BLOCK_DEVICE_RANGEDB_001
	
	BLOCK_DEVICE_RANGEDB_002 를 참조하십시오
	
	Block_device_RANGEDB_003 을 참조하십시오
	
	Block_device_RANGEDB_004 를 참조하십시오
	
	Block_device_RANGEDB_005 를 참조하십시오
	
	Block_device_RANGEDB_006
	
	Block_device_RANGEDB_007 을 참조하십시오
	
	Block_device_RANGEDB_008 을 참조하십시오
	
	Block_device_RANGEDB_009 를 참조하십시오
	
	Block_device_RANGEDB_010
	
	Block_device_RANGEDB_011 을 참조하십시오
	
	Block_device_RANGEDB_012 를 참조하십시오
	
	Block_device_RANGEDB_013
	
	Block_device_RANGEDB_014
	
	Block_device_RANGEDB_015 를 참조하십시오

BLOCK_DEVICE_Tables

값	지정

이 노드가 데이터베이스 테이블의 영구 저장에 사용할 블록 디바이스 특수 파일의 경로 및 이름입니다. 이 키는 node_type=vm_Admin_Node인 노드에만 필요합니다. 다른 노드 유형에 대해서는 지정하지 마십시오.
 	
예:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	필수 요소입니다

BLOCK_DEVICE_VAR_LOCAL

값	지정

이 노드가 영구 스토리지에 사용할 블록 디바이스 특수 파일의 경로 및 `/var/local` 이름입니다.
 	
예:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	필수 요소입니다

클라이언트 네트워크 키

client_network_Config

값	지정
DHCP, 정적 또는 비활성	선택 사항

CLIENT_NETWORK_GATEWAY

값	지정

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`
	선택 사항

client_network_ip

값	지정

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`
	client_network_Config=static 인 경우 필요합니다
	
	그렇지 않으면 선택 사항입니다.

client_network_MAC

값	지정
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`	선택 사항

client_network_mask.(클라이언트 네트워크 마스크

값	지정

클라이언트 네트워크의 이 노드에 대한 IPv4 넷마스크입니다.
 	
client_network_config = static 인 경우 이 키를 지정하고 다른 값에는 이 키를 지정하지 마십시오.
 	
예:
 	
`255.255.255.0`
 	
`255.255.248.0`
	client_network_ip을 지정하고 client_network_Config=static인 경우 필수입니다
	
	그렇지 않으면 선택 사항입니다.

client_network_mtu

값	지정

Client Network의 이 노드에 대한 MTU(Maximum Transmission Unit)입니다. client_network_Config = DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 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:
 	
`1500`
 	
`8192`
	선택 사항

client_network_target 을 선택합니다

값	지정

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:
 	
`bond0.1003`
 	
`ens423`
	모범 사례

CLIENT_NETWORK_TARGET_TYPE

값	지정
인터페이스(지원되는 값만 해당)	선택 사항

client_network_target_type_interface_clone_MAC

값	지정
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 복제의 고려 사항 및 권장 사항(Red Hat Enterprise Linux)" • "MAC 주소 복제에 대한 고려 사항 및 권장 사항(Ubuntu 또는 Debian)"	모범 사례

그리드 네트워크 키

GRID_NETWORK_CONFIG(그리드 네트워크 구성

값	지정
고정 또는 DHCP 지정하지 않으면 기본적으로 정적입니다.	모범 사례

GRID_NETWORK_Gateway를 참조하십시오

값	지정
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.	필수 요소입니다

GRID_NETWORK_IP입니다

값	지정

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_CONFIG = STATIC인 경우 필요합니다
	
	그렇지 않으면 선택 사항입니다.

GRID_NETWORK_MAC을 선택합니다

값	지정
컨테이너의 그리드 네트워크 인터페이스에 대한 MAC 주소입니다. 콜론으로 구분된 6쌍의 16진수 숫자이어야 합니다. 예: `b2:9c:02:c2:27:30`	선택 사항 생략할 경우 MAC 주소가 자동으로 생성됩니다.

GRID_NETWORK_MASK 를 참조하십시오

값	지정

그리드 네트워크에서 이 노드에 대한 IPv4 넷마스크입니다. GRID_NETWORK_CONFIG = STATIC인 경우 이 키를 지정하고 다른 값에는 이 키를 지정하지 마십시오.
 	
예:
 	
`255.255.255.0`
 	
`255.255.248.0`
	GRID_NETWORK_IP를 지정하고 GRID_NETWORK_CONFIG=STATIC인 경우에 필요합니다.
	
	그렇지 않으면 선택 사항입니다.

GRID_NETWORK_MTU 를 참조하십시오

값	지정

Grid Network의 이 노드에 대한 MTU(Maximum Transmission Unit)입니다. GRID_NETWORK_CONFIG=DHCP인지 지정하지 마십시오. 지정된 경우 값은 1280에서 9216 사이여야 합니다. 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:
 	
`1500`
 	
`8192`
	선택 사항

GRID_NETWORK_TARGET

값	지정

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:
 	
`bond0.1001`
 	
`ens192`
	필수 요소입니다

GRID_NETWORK_TARGET_TYPE

값	지정
인터페이스(이 값만 지원됩니다.)	선택 사항

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

값	지정
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 복제의 고려 사항 및 권장 사항(Red Hat Enterprise Linux)" • "MAC 주소 복제에 대한 고려 사항 및 권장 사항(Ubuntu 또는 Debian)"	모범 사례

설치 암호 키(임시)

사용자 지정_임시_암호_해시

값	지정
기본 관리자 노드의 경우 설치 중에 StorageGRID 설치 API에 대한 기본 임시 암호를 설정합니다. • 참고 *: 기본 관리자 노드에서만 설치 암호를 설정합니다. 다른 노드 유형에 암호를 설정하려고 하면 노드 구성 파일의 유효성 검사가 실패합니다. 이 값을 설정해도 설치가 완료된 경우 아무런 영향이 없습니다. 이 키를 생략하면 기본적으로 임시 암호가 설정되지 않습니다. 또는 StorageGRID 설치 API를 사용하여 임시 암호를 설정할 수 있습니다. 8자 이상 32자 이하의 암호 형식을 가진 SHA-512 암호 `$6$<salt>$<password hash>` 해시여야 `crypt()` 합니다. 이 해시는 SHA-512 모드의 명령과 같은 CLI 툴을 사용하여 생성할 수 `openssl passwd` 있습니다.	모범 사례

인터페이스 키입니다

interface_target_nnnn입니다

값	지정
이 노드에 추가할 추가 인터페이스의 이름 및 선택적 설명입니다. 각 노드에 여러 개의 인터페이스를 추가할 수 있습니다. _nnnn_의 경우 추가할 각 interface_target 항목의 고유 번호를 지정합니다. 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: `INTERFACE_TARGET_0001=ens256, 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.	선택 사항

최대 **RAM** 키

최대 **RAM**

값	지정

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 "메타데이터 예약된 공간에 대한 설명입니다"참조하십시오.
 	
이 필드의 형식은 *numberunit*, WHERE *unit* `b`, `k`, `m` 또는 `g`입니다.
 	
예:
 	
`24g`
 	
`38654705664b`
 	
• 참고 *: 이 옵션을 사용하려면 메모리 cgroup에 대한 커널 지원을 활성화해야 합니다.
	선택 사항

노드 유형 키입니다

node_type입니다

값	지정
노드 유형: • VM_Admin_Node • VM_스토리지_노드 • VM_Archive_Node • VM_API_게이트웨이	필수 요소입니다

스토리지 유형

값	지정
스토리지 노드에 포함된 객체 유형을 정의합니다. 자세한 내용은 을 "스토리지 노드 유형"참조하십시오. 이 키는 node_type=vm_Storage_Node인 노드에만 필요하며 다른 노드 유형에 대해서는 지정하지 않습니다. 스토리지 유형: • 결합된 • 데이터 • 메타데이터 • 참고 *: storage_type이 지정되지 않은 경우 스토리지 노드 유형은 기본적으로 결합(데이터 및 메타데이터)으로 설정됩니다.	선택 사항

포트 재매핑 키

port_remap 을 참조하십시오

값	지정
노드에서 내부 그리드 노드 통신 또는 외부 통신을 위해 사용하는 모든 포트를 다시 매핑합니다. 엔터프라이즈 네트워킹 정책으로 StorageGRID에서 사용하는 하나 이상의 포트를 제한하는 경우 또는 에 설명된 대로 포트를 다시 매핑해야 "내부 그리드 노드 통신""외부 통신"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 다음과 같습니다 *network type/protocol/default port used by grid node/new port*. 여기서 *network type* 그리드, 관리자 또는 클라이언트이고 *protocol* TCP 또는 UDP입니다. 예: `PORT_REMAP = client/tcp/18082/443` 쉼표로 구분된 목록을 사용하여 여러 포트를 다시 매핑할 수도 있습니다. 예: `PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80`	선택 사항

port_remap_inbound 를 참조하십시오

값	지정
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 다음과 같습니다 *network type/protocol/remapped port/default port used by grid node*. 여기서 *network type* 그리드, 관리자 또는 클라이언트이고 *protocol* TCP 또는 UDP입니다. 예: `PORT_REMAP_INBOUND = grid/tcp/3022/22` 쉼표로 구분된 목록을 사용하여 여러 인바운드 포트를 다시 매핑할 수도 있습니다. 예: `PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22`	선택 사항

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 mDNS(multicast domain name system)를 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
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
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
```

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 에서 구성 파일을 만든 후에는 `/etc/storagegrid/nodes` 해당 파일의 내용을 확인해야 합니다.

구성 파일의 내용을 확인하려면 각 호스트에서 다음 명령을 실행합니다.

```
sudo storagegrid node validate all
```

파일이 올바른 경우, 예제에 표시된 대로 각 구성 파일에 대해 * Passed * 가 출력됩니다.

메타데이터 전용 노드에서 LUN을 하나만 사용하는 경우에는 무시해도 되는 경고 메시지가 표시될 수 있습니다.

```
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 명령의 또는 `--quiet` 옵션 `storagegrid`(예: `storagegrid --quiet…`)을 사용하여 이 출력을 표시하지 않을 수 있습니다 `-q`. 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
```

3. 노드가 "not running" 또는 "stopped" 상태를 반환하는 경우 다음 명령을 실행합니다.

```
sudo storagegrid node start node-name
```

4. 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.

시작하기 전에

기본 관리 노드를 구축하고 초기 시작 시퀀스를 완료해야 합니다.

단계

1. 웹 브라우저를 열고 다음으로 이동합니다.

   `https://primary_admin_node_ip`

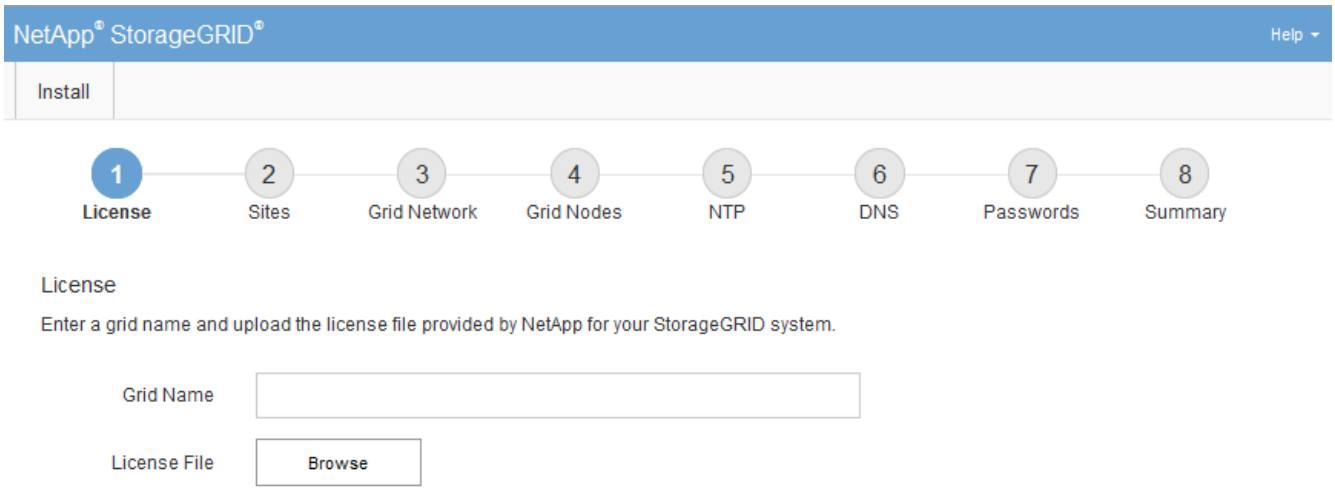
   또는 포트 8443에서 그리드 관리자에 액세스할 수 있습니다.

   `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. 필요에 따라 임시 설치 관리자 암호를 관리합니다.
   - 이러한 방법 중 하나를 사용하여 암호를 이미 설정한 경우 암호를 입력하여 계속 진행합니다.
     - 사용자가 이전에 설치 프로그램에 액세스하는 동안 암호를 설정했습니다
     - 암호가 에 있는 노드 구성 파일에서 자동으로 가져온 것입니다 `/etc/storagegrid/nodes/<node_name>.conf`
   - 암호를 설정하지 않은 경우 StorageGRID 설치 프로그램을 보호할 암호를 선택적으로 설정합니다.
3. StorageGRID 시스템 설치 * 를 선택합니다.

   StorageGRID 시스템을 구성하는 데 사용되는 페이지가 나타납니다.



StorageGRID 라이센스 정보를 지정합니다

StorageGRID 시스템의 이름을 지정하고 NetApp에서 제공하는 라이센스 파일을 업로드해야 합니다.

단계

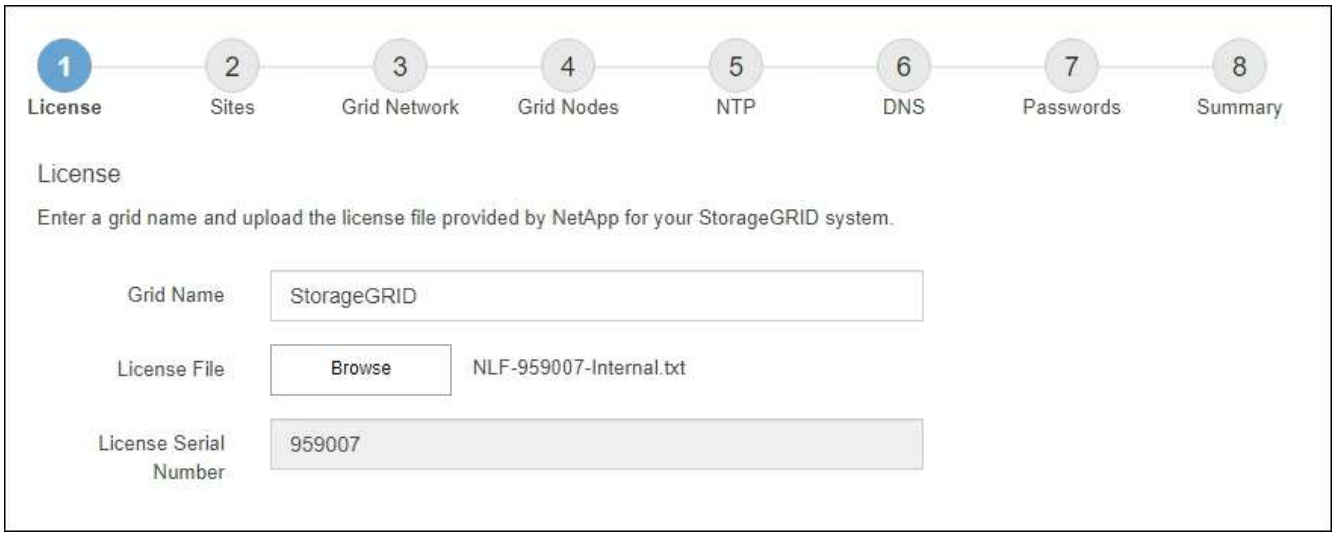
1. 라이센스 페이지의 * 그리드 이름 * 필드에 StorageGRID 시스템에 대한 의미 있는 이름을 입력합니다.

   설치 후, 이름이 Nodes 메뉴 맨 위에 표시됩니다.

2. 찾아보기 * 를 선택하고 NetApp 라이센스 파일을 찾은 (`NLF-*unique-id*.txt`다음 * 열기 * 를 선택합니다.

   라이센스 파일의 유효성이 검사되고 일련 번호가 표시됩니다.

   StorageGRID 설치 아카이브에는 제품에 대한 지원 권한이 없는 무료 라이센스가 포함되어 있습니다. 설치 후 지원을 제공하는 라이센스로 업데이트할 수 있습니다.



3. 다음 * 을 선택합니다.

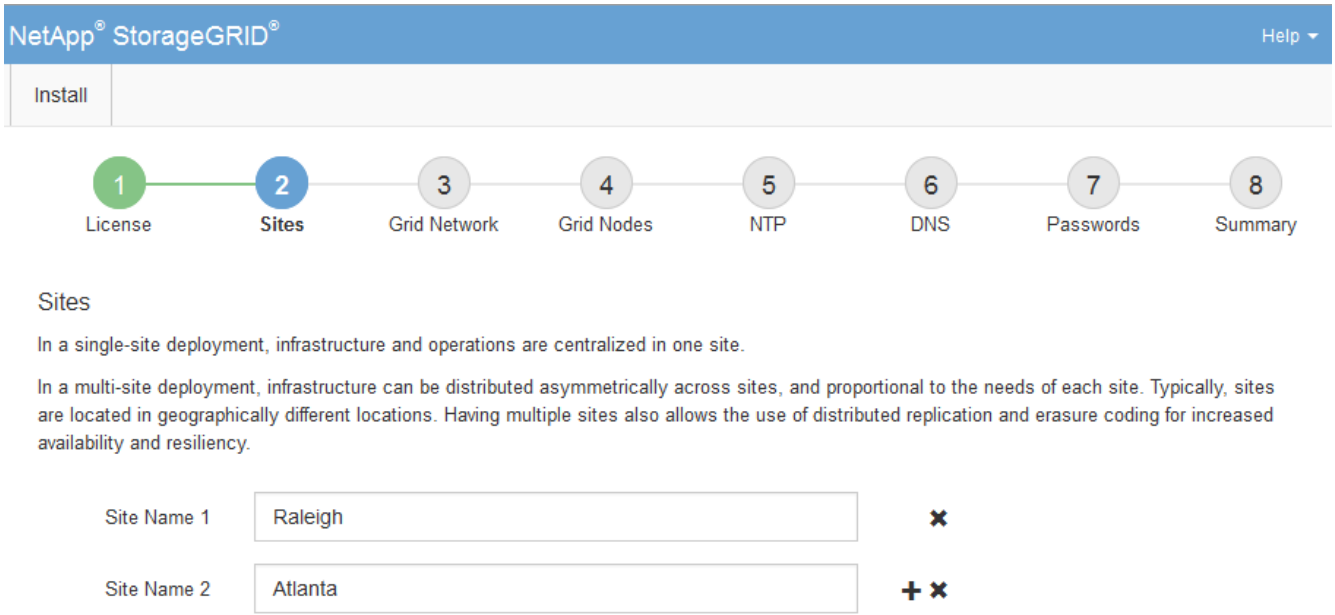
사이트를 추가합니다

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

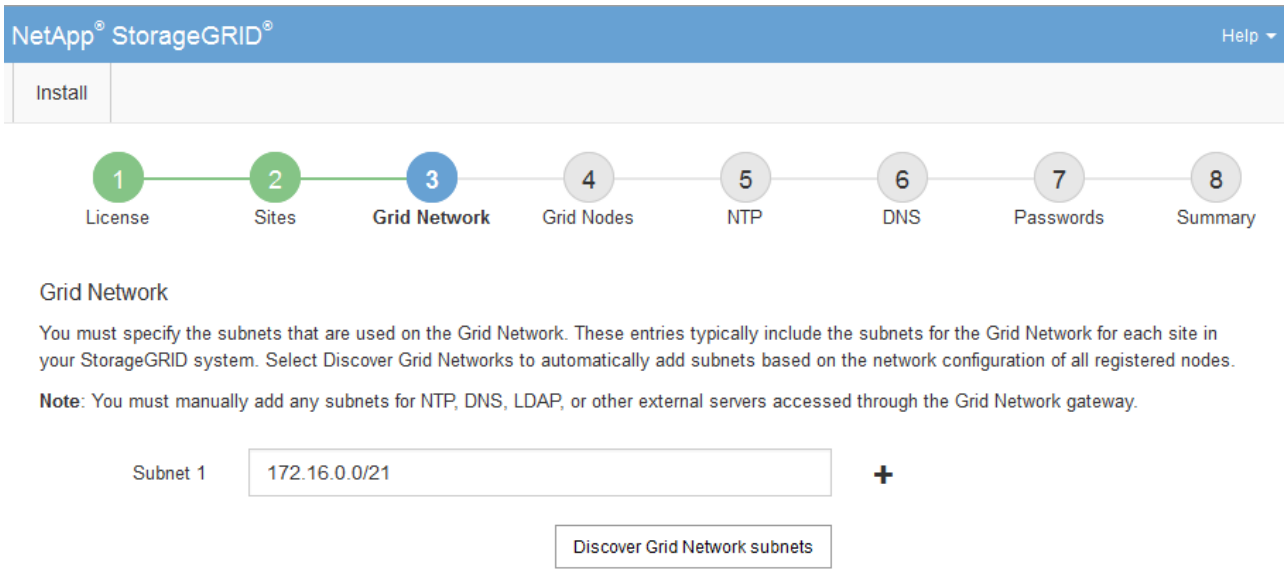
서브넷 항목에는 그리드 네트워크를 통해 연결할 수 있어야 하는 서브넷과 함께 StorageGRID 시스템의 각 사이트에 대한 그리드 네트워크의 서브넷이 포함됩니다.

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. 그리드 네트워크의 모든 사이트에 대해 모든 서브넷을 지정해야 합니다.
   - 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.

◦ 그리드 네트워크 게이트웨이를 통해 액세스하는 NTP, DNS, LDAP 또는 기타 외부 서버에 대해 서브넷을 수동으로 추가해야 합니다.



3. 다음 * 을 클릭합니다.

보류 중인 그리드 노드를 승인합니다

StorageGRID 시스템에 가입하려면 각 그리드 노드를 승인해야 합니다.

시작하기 전에

모든 가상 및 StorageGRID 어플라이언스 그리드 노드를 구축했습니다.

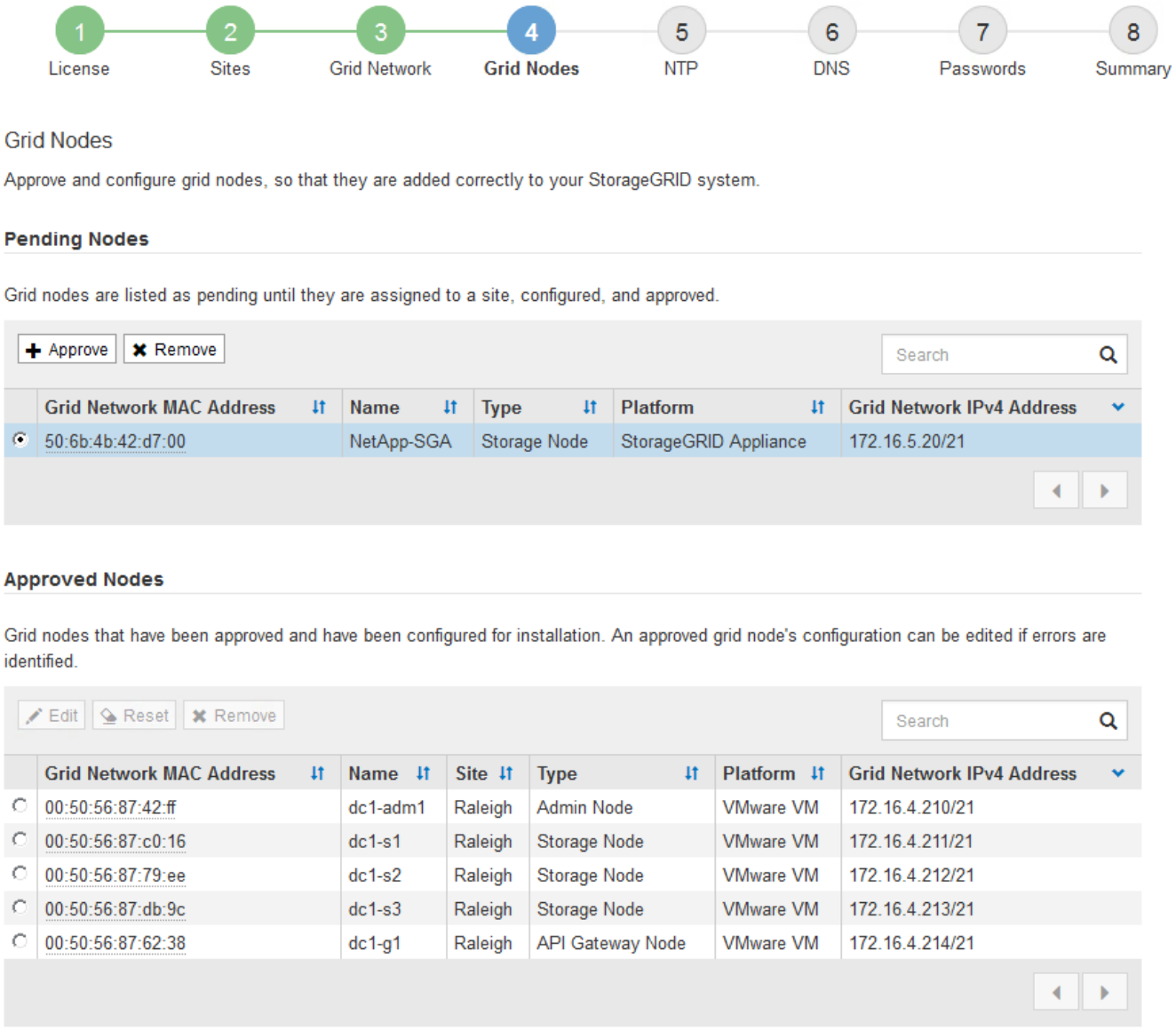
일부 노드를 나중에 설치하는 대신 모든 노드를 한 번 설치하는 것이 더 효율적입니다.

단계

1. Pending Nodes(보류 중인 노드) 목록을 검토하고 배포된 모든 그리드 노드가 표시되는지 확인합니다.

그리드 노드가 누락된 경우 그리드 노드가 성공적으로 배포되었으며 admin_IP에 대해 설정된 기본 관리 노드의 올바른 그리드 네트워크 IP가 있는지 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 노드에 대한 사이트의 시스템 이름입니다.
   - * 이름 *: 노드의 시스템 이름입니다. 기본적으로 노드를 구성할 때 지정한 이름이 지정됩니다.

     시스템 이름은 내부 StorageGRID 작업에 필요하며 설치를 완료한 후에는 변경할 수 없습니다. 그러나 설치 프로세스의 이 단계에서 필요에 따라 시스템 이름을 변경할 수 있습니다.

   - * 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.

- * 스토리지 유형 * (스토리지 노드에만 해당): 새 스토리지 노드가 데이터 전용, 메타데이터 전용 또는 둘 다에 대해서만 사용되도록 지정합니다. 옵션은 * 데이터 및 메타데이터 * ("결합"), * 데이터 전용 * 및 * 메타데이터만 * 입니다.

  이러한 노드 유형의 요구 사항에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

- * 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. 구성된 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. 구성된 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 제거합니다.

f. Pending Nodes 테이블에서 노드를 제거합니다.

g. 대기 중인 노드 목록에 노드가 다시 나타날 때까지 기다립니다.

h. 적절한 네트워크를 구성할 수 있는지 확인합니다. 어플라이언스 설치 프로그램의 IP 구성 페이지에서 제공한 정보로 이미 채워져야 합니다.

   자세한 내용은 를 "하드웨어 설치를 빠르게 시작합니다" 참조하여 제품에 대한 지침을 확인하십시오.

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. 구성된 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 제거합니다.

   f. Pending Nodes 테이블에서 노드를 제거합니다.

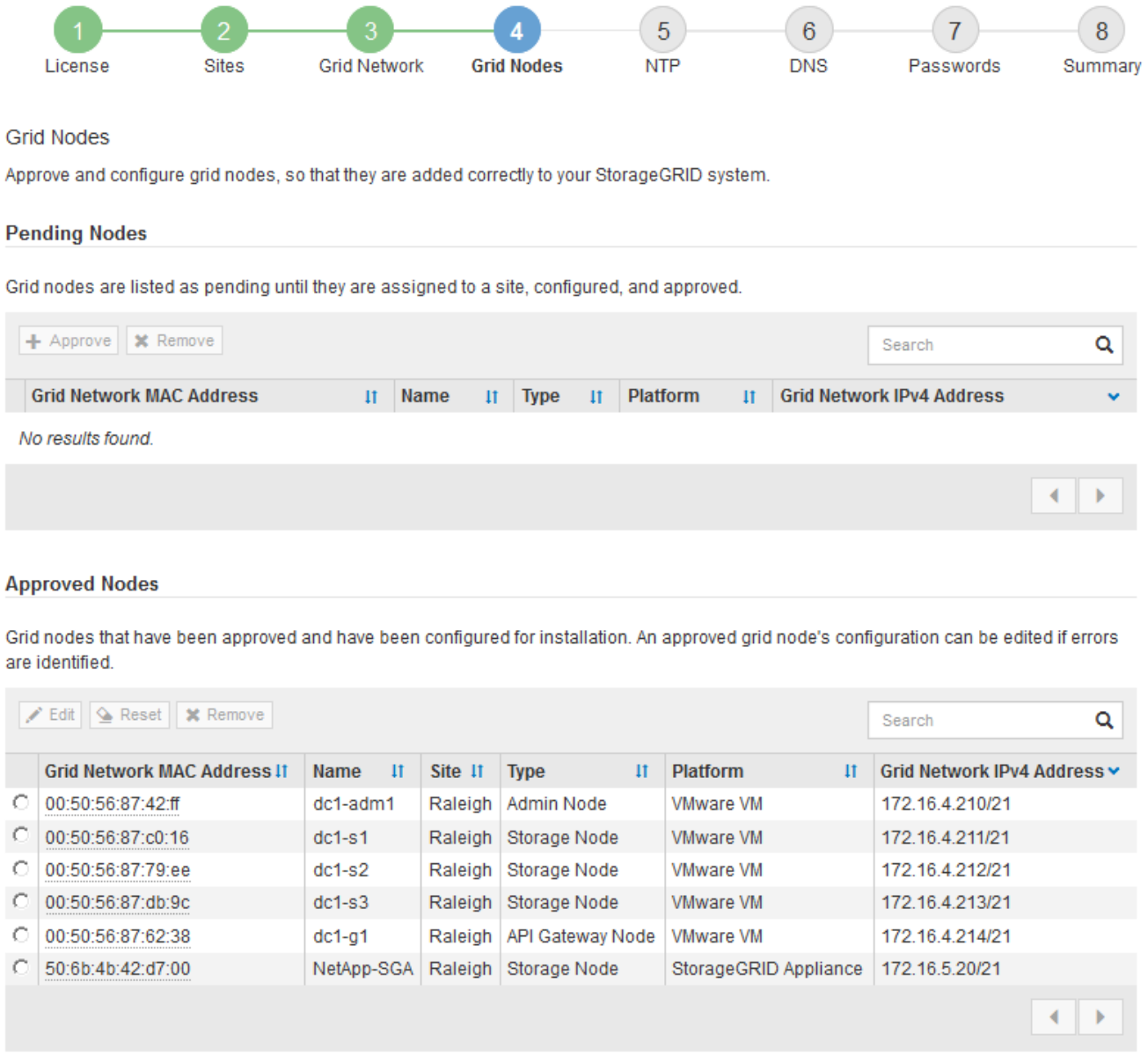
   g. 대기 중인 노드 목록에 노드가 다시 나타날 때까지 기다립니다.

   h. 적절한 네트워크를 구성할 수 있는지 확인합니다. 어플라이언스 설치 프로그램의 IP 구성 페이지에서 제공한 정보로 이미 채워져야 합니다.

      StorageGRID 어플라이언스를 설치하는 방법에 대한 자세한 내용은 를 "하드웨어 설치를 빠르게 시작합니다" 참조하여 해당 어플라이언스에 대한 지침을 확인하십시오.

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.

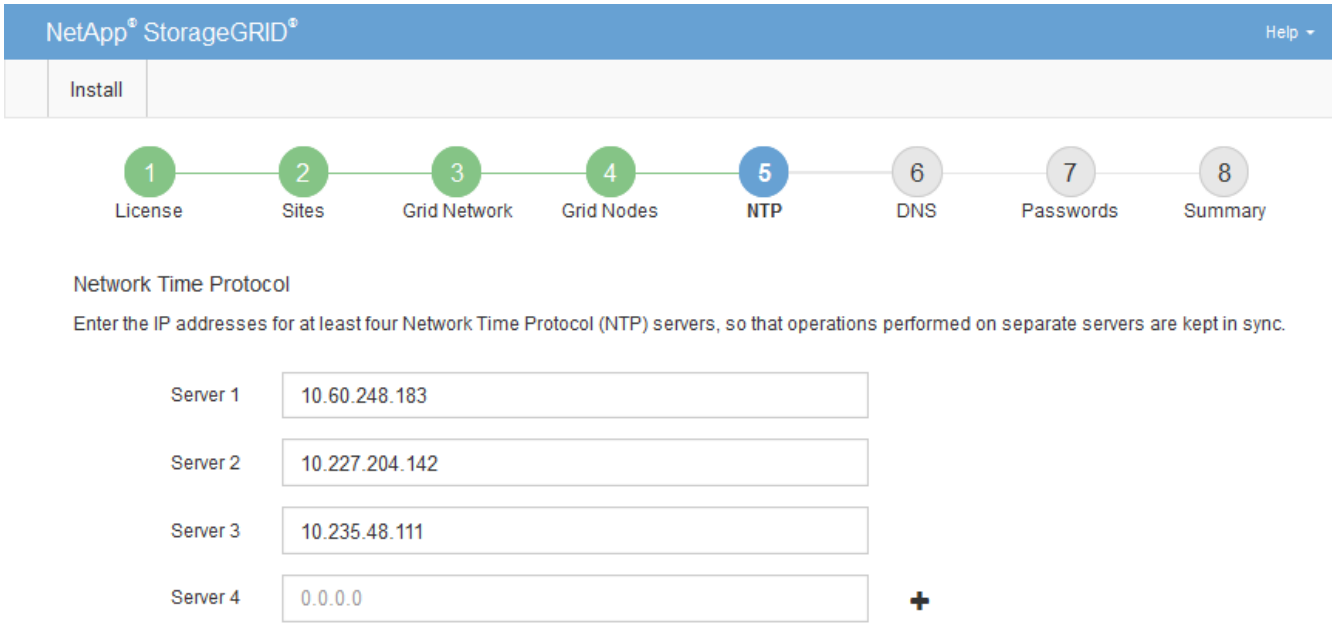
> 프로덕션 수준 StorageGRID 설치에 외부 NTP 소스를 지정할 때 Windows Server 2016 이전 버전의 Windows에서는 Windows 시간(W32Time) 서비스를 사용하지 마십시오. 이전 버전의 Windows의 시간 서비스는 정확하지 않으며 StorageGRID와 같은 고정밀 환경에서 사용하기 위해 Microsoft에서 지원되지 않습니다.
>
> "정확도가 높은 환경에 대한 Windows 시간 서비스를 구성하기 위한 경계를 지원합니다"

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"

DNS 서버 정보를 지정합니다

IP 주소 대신 호스트 이름을 사용하여 외부 서버에 액세스할 수 있도록 StorageGRID 시스템에 대한 DNS 정보를 지정해야 합니다.

이 작업에 대해

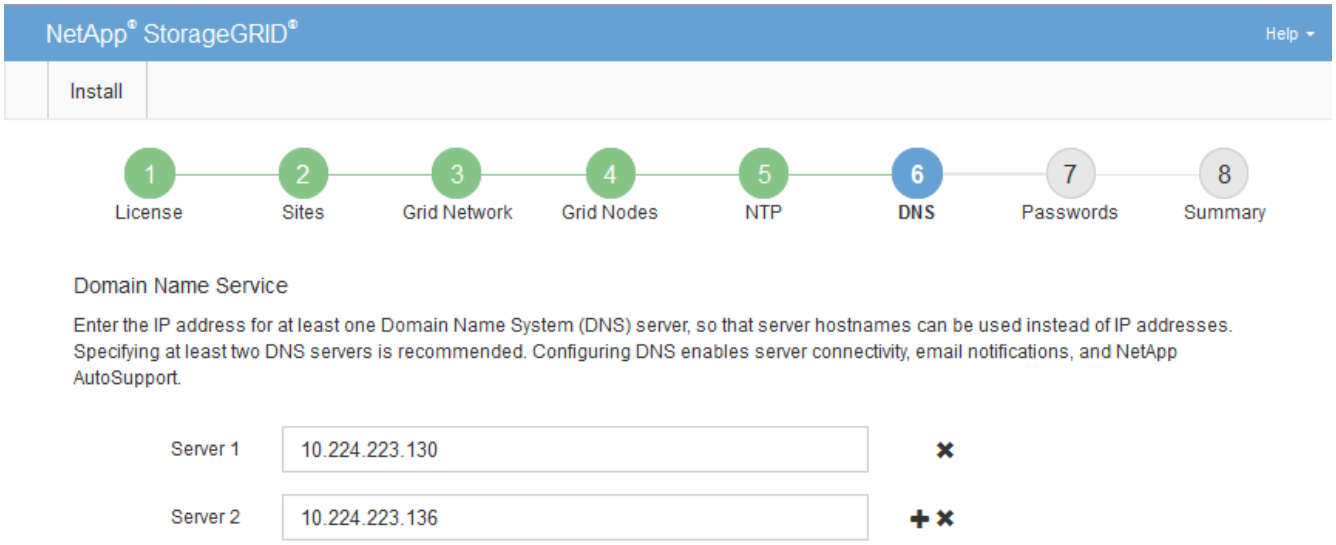
를 "DNS 서버 정보입니다" 지정하면 이메일 알림 및 AutoSupport에 IP 주소 대신 FQDN(정규화된 도메인 이름) 호스트 이름을 사용할 수 있습니다.

제대로 작동하려면 DNS 서버를 두 대 또는 세 대 지정합니다. 3개 이상을 지정하면 일부 플랫폼의 알려진 OS 제한 때문에 3개만 사용할 수 있습니다. 사용자 환경에 라우팅 제한이 있는 경우 개별 노드(일반적으로 사이트의 모든 노드)에서 최대 3개의 DNS 서버로 구성된 다른 세트를 사용할 수 "DNS 서버 목록을 사용자 지정합니다"있습니다.

가능한 경우 각 사이트에서 로컬로 액세스할 수 있는 DNS 서버를 사용하여 isfan 사이트가 외부 대상의 FQDN을 확인할 수 있도록 합니다.

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 `Passwords.txt` 복구 패키지의 파일에 저장됩니다.

단계

1. Provisioning Passphrase * 에서 StorageGRID 시스템의 그리드 토폴로지를 변경하는 데 필요한 프로비저닝 암호를 입력합니다.

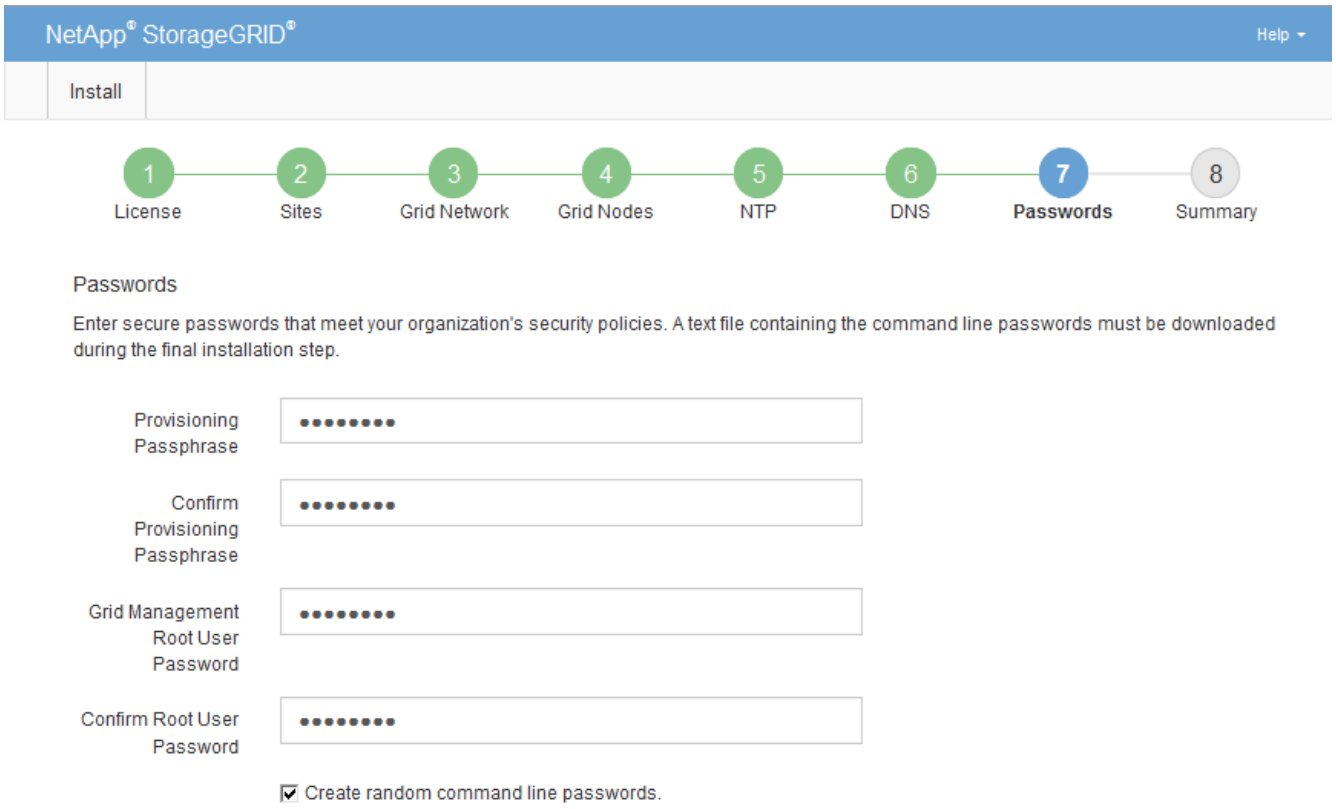
   프로비저닝 암호를 안전한 장소에 보관합니다.

   > 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. 그리드 관리 루트 사용자 암호 * 에 그리드 관리자에 "루트" 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. Clear * 임의의 명령줄 암호 만들기 * 기본 암호를 사용하여 "root" 또는 "admin" 계정을 사용하여 명령줄에서 그리드 노드에 액세스하려는 경우 데모 그리드에만 사용합니다.

   > 복구 패키지 파일을 다운로드하라는 메시지가 (`sgws-recovery-package-id-revision.zip`표시됩니다.) 요약 페이지에서 * 설치 * 를 클릭하면 됩니다. "이 파일을 다운로드합니다"설치를 완료해야 합니다. 시스템에 액세스하는 데 필요한 암호는 `Passwords.txt` 복구 패키지 파일에 포함된 파일에 저장됩니다.

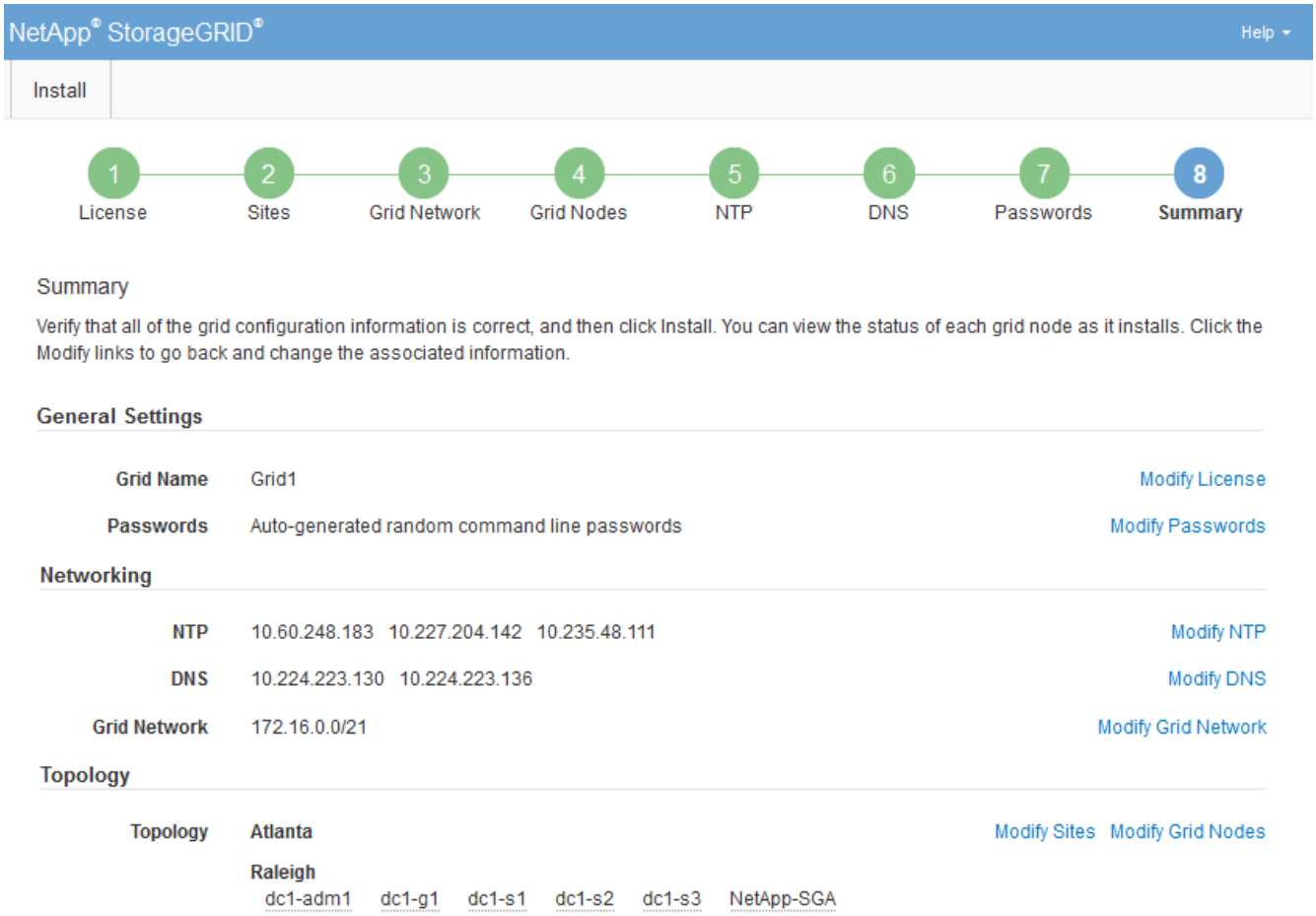
6. 다음 * 을 클릭합니다.

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. 자세한 내용은 을 "네트워킹 지침" 참조하십시오.

4. 복구 패키지 다운로드 * 를 클릭합니다.

그리드 토폴로지가 정의된 지점으로 설치가 진행되면 복구 패키지 파일을 다운로드하라는 메시지가 (`.zip`표시됩니다.) 이 파일의 내용에 성공적으로 액세스할 수 있는지 확인합니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 다운로드해야 합니다. 백그라운드에서 설치가 계속되지만 이 파일을 다운로드하여 확인할 때까지 설치를 완료하고 StorageGRID

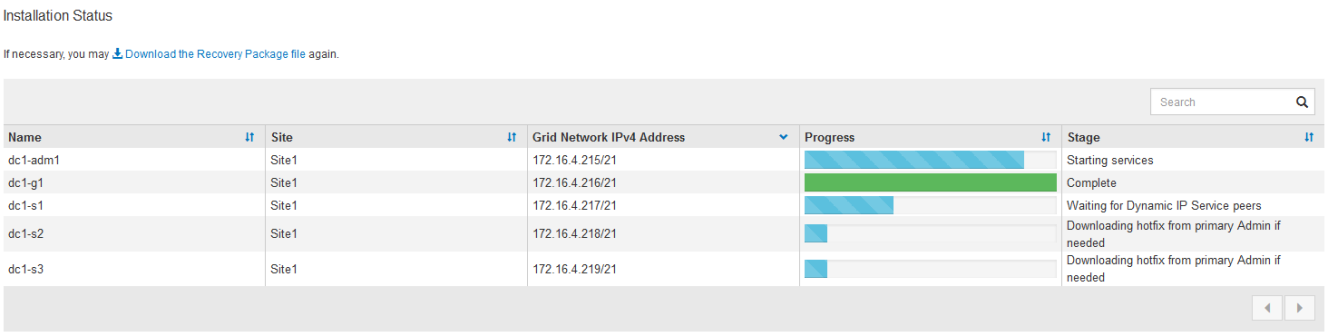
시스템에 액세스할 수 없습니다.

5. 파일의 내용을 추출한 다음 안전하고 별도의 두 위치에 저장할 수 있는지 확인합니다 `.zip`.

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

6. 복구 패키지 파일 * 을 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.

  그리드 네트워크 구성이 DHCP에 의해 변경될 때 노드가 재부팅되므로 DHCP 변경이 여러 노드에 동시에 영향을 미칠 경우 운영이 중단될 수 있습니다.

- 그리드 노드의 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 변경하려면 IP 변경 절차를 사용해야 합니다. 을 "IP 주소를 구성합니다"참조하십시오.
- 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.

REST API 설치

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 데이터 형식에 대해 잘 알고 있다고 가정합니다.

API 문서 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.
- * Temporary-password * — 설치 중 mgmt-API를 보호하기 위한 임시 암호의 작동.

관련 정보

"설치 자동화"

다음 단계로 넘어갑니다

설치를 완료한 후 필요한 통합 및 구성 작업을 수행합니다. 필요에 따라 옵션 작업을 수행할 수 있습니다.

필수 작업

- "테넌트 계정을 생성합니다" StorageGRID 시스템에 오브젝트를 저장하는 데 사용되는 S3 클라이언트 프로토콜의 경우
- "시스템 액세스를 제어합니다" 그룹 및 사용자 계정을 구성합니다. 선택적으로 Active Directory 또는 OpenLDAP와 같은 관리 그룹과 사용자를 가져올 수 "통합 ID 소스를 구성합니다"있습니다. 또는, 할 수 "로컬 그룹 및 사용자를 생성합니다"있습니다.
- 개체를 StorageGRID 시스템에 업로드하는 데 사용할 클라이언트 응용 프로그램을 통합하고 "S3 API를 사용합니다"테스트합니다.

- "ILM(정보 수명 주기 관리) 규칙 및 ILM 정책을 구성합니다" 를 사용하여 오브젝트 데이터를 보호하려고 합니다.
- 설치에 어플라이언스 스토리지 노드가 포함된 경우 SANtricity OS를 사용하여 다음 작업을 완료합니다.
  - 각 StorageGRID 어플라이언스에 연결하십시오.
  - AutoSupport 데이터가 수신되었는지 확인합니다.

  을 "하드웨어를 설정합니다"참조하십시오.
- 을 검토하고 따라 "StorageGRID 시스템 강화 지침"보안 위험을 제거합니다.
- "시스템 경고에 대한 이메일 알림을 구성합니다"..

선택적 태스크입니다

- "그리드 노드 IP 주소를 업데이트합니다" 배포를 계획하고 복구 패키지를 생성한 이후에 변경된 경우
- "스토리지 암호화를 구성합니다"필요한 경우.
- "스토리지 압축을 구성합니다" 필요한 경우 저장된 개체의 크기를 줄입니다.
- "VLAN 인터페이스를 구성합니다" 필요한 경우 네트워크 트래픽을 격리하고 분할합니다.
- "고가용성 그룹을 구성합니다" 필요한 경우 Grid Manager, Tenant Manager 및 S3 클라이언트의 연결 가용성을 향상시킵니다.
- "로드 밸런서 엔드포인트를 구성합니다" 필요한 경우 S3 클라이언트 연결의 경우

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 관리자 노드에서 찾음)

호스트에서 다음 설치 로그 파일을 사용할 수 있습니다.

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/<node-name>.log`

로그 파일에 액세스하는 방법에 대한 자세한 내용은 을 "로그 파일 및 시스템 데이터를 수집합니다"참조하십시오.

관련 정보

"StorageGRID 시스템 문제를 해결합니다"

예 /etc/network/interfaces

이 `/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
```

VMware에 StorageGRID를 설치합니다

VMware에 StorageGRID를 설치하기 위한 빠른 시작

다음 단계에 따라 VMware StorageGRID 노드를 설치합니다.

1 준비

- 에 대해 자세히 "StorageGRID 아키텍처 및 네트워크 토폴로지"알아보십시오.
- 에 대해 자세히 "StorageGRID 네트워킹"알아보십시오.
- 를 수집하고 "필요한 정보 및 자료"준비합니다.
- 설치 및 구성"VMware vSphere Hypervisor, vCenter 및 ESX 호스트"
- 필요한 를 "CPU 및 RAM"준비합니다.
- 에 대해 를 "스토리지 및 성능 요구사항"제공합니다.

2 구축

그리드 노드 구축 그리드 노드를 구축하면 StorageGRID 시스템의 일부로 생성되고 하나 이상의 네트워크에 연결됩니다.

- 1단계에서 준비한 서버에서 VMware vSphere Web Client, .vmdk 파일 및 .ovf 파일 템플릿 집합을 사용합니다 "소프트웨어 기반 노드를 가상 머신(VM)으로 구축".
- StorageGRID 어플라이언스 노드를 배포하려면 를 "하드웨어 설치를 빠르게 시작합니다"따르십시오.

3 구성

모든 노드가 배포되면 Grid Manager를 사용하여 를 "그리드를 구성하고 설치를 완료합니다"수행합니다.

설치를 자동화합니다

시간을 절약하고 일관성을 제공하기 위해 그리드 노드의 구축과 구성 및 StorageGRID 시스템 구성을 자동화할 수 있습니다.

- "VMware vSphere를 사용하여 그리드 노드 구축을 자동화합니다"..
- 그리드 노드를 배포한 후 "StorageGRID 시스템의 구성을 자동화합니다"설치 아카이브에 제공된 Python 구성 스크립트를 사용합니다.
- "어플라이언스 그리드 노드의 설치 및 구성을 자동화합니다"
- StorageGRID 구축의 고급 개발자인 경우 를 사용하여 그리드 노드 설치를 "REST API 설치"자동화합니다.

VMware에서의 설치 계획 및 준비

필요한 정보 및 자료

StorageGRID를 설치하기 전에 필요한 정보와 자료를 수집하고 준비합니다.

필수 정보입니다

네트워크 계획

각 StorageGRID 노드에 연결할 네트워크 StorageGRID는 트래픽 분리, 보안 및 관리의 편의를 위해 여러 네트워크를 지원합니다.

StorageGRID 를 "네트워킹 지침"참조하십시오.

네트워크 정보

각 그리드 노드에 할당할 IP 주소와 DNS 및 NTP 서버의 IP 주소입니다.

그리드 노드용 서버

구축할 StorageGRID 노드의 수와 유형을 지원하기에 충분한 리소스를 제공하는 물리적 서버 세트, 가상 서버 또는 둘 다 식별합니다.

StorageGRID 설치에서 StorageGRID 어플라이언스(하드웨어) 스토리지 노드를 사용하지 않는 경우 BBWC(배터리 지원 쓰기 캐시)와 함께 하드웨어 RAID 스토리지를 사용해야 합니다. StorageGRID는 VSAN(Virtual Storage Area Network), 소프트웨어 RAID 또는 RAID 보호 사용을 지원하지 않습니다.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

필수 자료

NetApp StorageGRID 라이센스

디지털 서명된 유효한 NetApp 라이센스가 있어야 합니다.

테스트 및 개념 증명 그리드에 사용할 수 있는 비운영 라이센스가 StorageGRID 설치 아카이브에 포함되어 있습니다.

StorageGRID 설치 아카이브

"StorageGRID 설치 아카이브를 다운로드하고 파일 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"

StorageGRID 설치 파일을 다운로드하고 압축을 풉니다

StorageGRID 설치 아카이브를 다운로드하고 파일을 추출해야 합니다. 선택적으로 설치 패키지의 파일을 수동으로 확인할 수 있습니다.

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 VMware용 .tgz 또는 .zip 설치 아카이브를 선택합니다.

   서비스 랩톱에서 Windows를 실행하는 경우 이 `.zip` 파일을 사용합니다.

7. 설치 아카이브를 저장합니다.
8. 설치 아카이브를 확인해야 하는 경우:

   a. StorageGRID 코드 서명 확인 패키지를 다운로드합니다. 이 패키지의 파일 이름은 StorageGRID 소프트웨어

버전의 형식을 `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` 사용합니다. `<version-number>`

b. 의 단계를 "설치 파일을 수동으로 확인합니다"따릅니다.

9. 설치 아카이브에서 파일 압축을 풉니다.
10. 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.
	Open Virtualization Format 템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 기본 관리자 노드를 배포할 수 있습니다.
	템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 비기본 관리 노드를 배포합니다.
	템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 게이트웨이 노드를 배포할 수 있습니다.
	템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 가상 머신 기반 스토리지 노드를 구축합니다.
배포 스크립팅 도구	설명
	가상 그리드 노드의 배포를 자동화하는 데 사용되는 Bash 쉘 스크립트입니다.
	스크립트와 함께 사용할 예제 구성 파일 `deploy-vsphere-ovftool.sh`
	StorageGRID 시스템 구성을 자동화하는 데 사용되는 Python 스크립트입니다.

경로 및 파일 이름입니다	설명
	StorageGRID 어플라이언스 구성을 자동화하는 데 사용되는 Python 스크립트입니다.
	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트의 예 이 스크립트를 Ping 연합 통합에 사용할 수도 있습니다.
/vSphere/configure -StorageGrid.sample.json을 참조하십시오	스크립트와 함께 사용할 예제 구성 파일 `configure-storagegrid.py`
/vSphere/configure -StorageGrid.blank.json 을 참조하십시오	스크립트와 함께 사용할 빈 구성 `configure-storagegrid.py` 파일입니다.
	Active Directory 또는 Ping 연방을 사용하여 SSO(Single Sign-On)를 사용하도록 설정한 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/vSphere/StorageGrid-ssoauth-Azure.js	Azure와의 SSO 상호 작용을 수행하기 위해 Python 스크립트에 의해 호출되는 도우미 스크립트입니다. `storagegrid-ssoauth-azure.py`
/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.

설치 파일 수동 확인(선택 사항)

필요한 경우 StorageGRID 설치 아카이브의 파일을 수동으로 확인할 수 있습니다.

시작하기 전에

에서 "StorageGRID용 NetApp 다운로드 페이지" 가져온 "검증 패키지를 다운로드했습니다"것입니다.

단계

1. 검증 패키지에서 아티팩트를 추출합니다.

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. 이러한 아티팩트가 추출되었는지 확인합니다.
   - Leaf 인증서: `Leaf-Cert.pem`

- 인증서 체인: `CA-Int-Cert.pem`
- 타임 스탬프 응답 체인: `TS-Cert.pem`
- 체크섬 파일: `sha256sum`
- 체크섬 서명: `sha256sum.sig`
- 타임 스탬프 응답 파일: `sha256sum.sig.tsr`

3. 체인을 사용하여 리프 인증서가 유효한지 확인합니다.
   - 예 *: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`
   - 예상 출력 *: `Leaf-Cert.pem: OK`
4. leaf 인증서가 만료되어 step_2_에 실패한 경우 파일을 사용하여 `tsr` 확인합니다.
   - 예 *: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`
   - 예상 출력 포함 *: `Verification: OK`
5. 리프 인증서에서 공용 키 파일을 만듭니다.
   - 예 *: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`
   - 예상 출력 *:_none_
6. 공개 키를 사용하여 `sha256sum` 에 대해 파일을 `sha256sum.sig` 확인합니다.
   - 예 *: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`
   - 예상 출력 *: `Verified OK`
7. `sha256sum`새로 생성된 체크섬을 기준으로 파일 내용을 확인합니다.
   - 예 *: `sha256sum -c sha256sum`

   *예상 출력 * *<filename>*: OK:+는
   <filename> 다운로드한 아카이브 파일의 이름입니다.
8. "나머지 단계를 완료합니다" 를 눌러 적절한 설치 파일을 추출하고 선택합니다.

VMware 소프트웨어 요구 사항

가상 머신을 사용하여 모든 유형의 StorageGRID 노드를 호스팅할 수 있습니다. 각 그리드 노드에 대해 하나의 가상 머신이 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 노드를 구축하기 전에 VMware vSphere 및 vCenter를 설치하고 구성해야 합니다.

지원되는 VMware vSphere Hypervisor 및 VMware vCenter Server 소프트웨어 버전은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

이러한 VMware 제품을 설치하는 데 필요한 단계는 VMware 설명서를 참조하십시오.

CPU 및 **RAM** 요구 사항

StorageGRID 소프트웨어를 설치하기 전에 StorageGRID 시스템을 지원할 준비가 되도록 하드웨어를 확인 및 구성하십시오.

각 StorageGRID 노드에는 다음과 같은 최소 리소스가 필요합니다.

- CPU 코어: 노드당 8개
- RAM: 사용 가능한 총 RAM과 시스템에서 실행되는 비 StorageGRID 소프트웨어의 양에 따라 다릅니다
  - 일반적으로 노드당 최소 24GB, 총 시스템 RAM보다 2 ~ 16GB 작습니다
  - 각 테넌트당 최소 64GB의 버킷이 약 5,000개 있습니다

VMware는 가상 머신당 하나의 노드를 지원합니다. StorageGRID 노드가 사용 가능한 물리적 RAM을 초과하지 않는지 확인합니다. 각 가상 머신은 StorageGRID를 실행하기 위한 전용이어야 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 스토리지 관리, 메타데이터 예약 공간 설정 증가, CPU 및 메모리 사용량 모니터링에 대한 자세한 내용은"관리" "모니터링", 및 "업그레이드 중"StorageGRID에 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.

도 "요구사항을 충족해야 합니다"참조하십시오.

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 머신에 대한 요구 사항

StorageGRID 노드를 NetApp ONTAP 시스템에서 할당된 스토리지가 있는 가상 머신으로 구축하는 경우 볼륨에 FabricPool 계층화 정책이 설정되어 있지 않은 것이 확인되었습니다. 예를 들어 StorageGRID 노드가 VMware 호스트에서 가상 머신으로 실행 중인 경우 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.

필요한 가상 머신의 수입니다

각 StorageGRID 사이트에는 최소 3개의 스토리지 노드가 필요합니다.

노드 유형별 스토리지 요구 사항

운영 환경에서 StorageGRID 노드의 가상 머신은 노드 유형에 따라 서로 다른 요구 사항을 충족해야 합니다.

> 디스크 스냅샷을 사용하여 그리드 노드를 복원할 수 없습니다. 대신 "그리드 노드 복구"각 노드 유형에 대한 절차를 참조하십시오.

노드 유형	스토리지
관리자 노드	OS용 100GB LUN 관리자 노드 테이블용 200GB LUN 관리자 노드 감사 로그용 200GB LUN

노드 유형	스토리지
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.
스토리지 노드(메타데이터만)	OS용 100GB LUN LUN 1개 LUN당 최소 크기: 4TB • 참고 *: 단일 LUN의 최대 크기는 없습니다. 초과 용량은 향후 사용을 위해 저장됩니다. • 참고 *: 메타데이터 전용 스토리지 노드에는 하나의 rangedb만 필요합니다.
게이트웨이 노드	OS용 100GB LUN

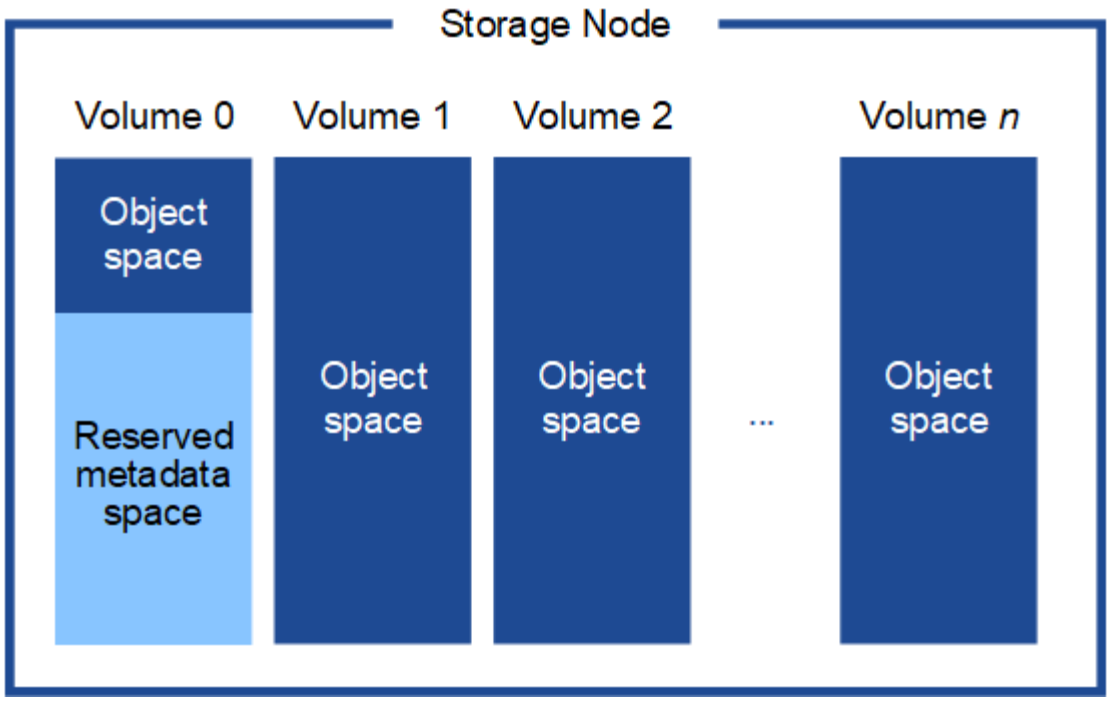
구성된 감사 레벨에 따라 S3 오브젝트 키 이름 등의 사용자 입력 크기, 그리고 보존해야 하는 감사 로그 데이터의 양을 위해 각 관리 노드에서 감사 로그 LUN의 크기를 늘려야 할 수도 있습니다. 일반적으로 그리드는 S3 작업당 약 1KB의 감사 데이터를 생성합니다. 즉, 200GB LUN이 2일에서 3일 동안 매일 7천만 개의 작업 또는 초당 800개의 작업을 지원하게 됩니다.

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.

메타데이터 전용 스토리지 노드가 있는 그리드를 설치할 경우 그리드에는 오브젝트 스토리지용 최소 노드 수도 있어야 합니다. 메타데이터 전용 스토리지 노드에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

- 단일 사이트 그리드의 경우 객체 및 메타데이터에 대해 2개 이상의 스토리지 노드가 구성됩니다.
- 다중 사이트 그리드의 경우 사이트당 하나 이상의 스토리지 노드가 객체 및 메타데이터에 대해 구성됩니다.

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 이하의 용량을 할당하면 스토리지 노드가 시작 시 스토리지 읽기 전용 상태로 전환되고 객체 메타데이터만 저장할 수 있습니다.

> ⓘ 볼륨 0에 500GB 미만의 용량을 할당할 경우(비운영 전용) 스토리지 볼륨 용량의 10%가 메타데이터용으로 예약됩니다.

- 새 시스템(StorageGRID 11.6 이상)을 설치하고 각 스토리지 노드에 128MB 이상의 RAM이 있는 경우 볼륨 0에 8TB 이상을 할당합니다. 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 을 "오브젝트 메타데이터 스토리지 관리"참조하십시오.

설치 자동화(VMware)

VMware OVF Tool을 사용하여 그리드 노드의 구축을 자동화할 수 있습니다. StorageGRID의 구성을 자동화할 수도 있습니다.

그리드 노드 구축을 자동화합니다

VMware OVF Tool을 사용하여 그리드 노드의 구축을 자동화합니다.

시작하기 전에

- Bash 3.2 이상이 설치된 Linux/Unix 시스템에 액세스할 수 있습니다.
- vCenter가 포함된 VMware vSphere를 사용하고 있습니다
- VMware OVF Tool 4.1이 설치되고 올바르게 구성되었습니다.
- OVF 툴을 사용하여 VMware vSphere에 액세스하기 위한 사용자 이름과 암호를 알고 있습니다
- OVF 파일에서 VM을 배포하고 전원을 켤 수 있는 충분한 권한과 VM에 연결할 추가 볼륨을 생성할 수 있는 권한이 있습니다. `ovftool`자세한 내용은 설명서를 참조하십시오.
- StorageGRID 가상 머신을 구축할 vSphere의 위치에 대한 VI(가상 인프라) URL을 알고 있습니다. 이 URL은 일반적으로 vApp 또는 리소스 풀이 됩니다. 예를 들면 다음과 같습니다.
  `vi://vcenter.example.com/vi/sgws`

  VMware 유틸리티를 사용하여 이 값을 확인할 수 `ovftool` 있습니다(자세한 내용은 설명서 참조 `ovftool`).

  vApp에 구축할 경우 가상 머신이 처음 시작될 때 자동으로 시작되지 않으며 수동으로 전원을 설정해야 합니다.

- 배포 구성 파일에 필요한 모든 정보를 수집했습니다. 자세한 내용은 을 "배포 환경에 대한 정보를 수집합니다 "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 및 `.mf` 파일과 동일한 폴더에 있어야 `.ovf` 합니다.
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Open Virtualization Format 템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 기본 관리자 노드를 배포할 수 있습니다.
vsphere - non-primary-admin.ovf vsphere - non-primary-admin.mf	템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 비기본 관리 노드를 배포합니다.

파일 이름	설명
vsphere-gateway.ovf vsphere-gateway.mf	템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 게이트웨이 노드를 배포할 수 있습니다.
vsphere-storage.ovf vsphere-storage.mf	템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 가상 머신 기반 스토리지 노드를 구축합니다.
deploy-vsphere-ovftool.sh	가상 그리드 노드의 배포를 자동화하는 데 사용되는 Bash 쉘 스크립트입니다.
deploy-vsphere-ovftool-sample.ini	스크립트와 함께 사용할 예제 구성 `deploy-vsphere-ovftool.sh` 파일입니다.

배포를 위한 구성 파일을 정의합니다

Bash 스크립트에서 사용하는 구성 파일에 StorageGRID용 가상 그리드 노드를 배포하는 데 필요한 정보를 지정합니다 `deploy-vsphere-ovftool.sh`. 예제 구성 파일을 수정하여 처음부터 새로 만들 필요가 없도록 할 수 있습니다.

단계

1. 예제 구성 파일의 복사본을 (`deploy-vsphere-ovftool.sample.ini`만듭니다. 새 파일을 `deploy-vsphere-ovftool.ini` 와 같은 디렉토리에 `deploy-vsphere-ovftool.sh` 저장합니다.
2. `deploy-vsphere-ovftool.ini`개방형:
3. VMware 가상 그리드 노드를 구축하는 데 필요한 모든 정보를 입력합니다.

   자세한 내용은 을 구성 파일 설정참조하십시오.

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'
```

  및 `--overwrite` 옵션을 사용하여 기존 가상 머신을 종료하고 교체할 수 `--powerOffTarget` 있습니다.

  > 노드를 서로 다른 데이터 저장소에 배포하고 전역이 아닌 각 노드에 대해 OVFTOOL_MOUMENT를 지정해야 합니다.

- * 소스 *: StorageGRID 가상 머신 템플릿의 경로(`.vmdk`) 파일 및 `.mf` 개별 그리드 노드의 파일과 `.ovf` 파일. 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 = STATIC
```

- * 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 = 9000
```

생략하면 1400이 사용됩니다.

점보 프레임을 사용하려면 MTU를 9000과 같은 점보 프레임에 적합한 값으로 설정합니다. 그렇지 않으면 기본값을 유지합니다.

> 네트워크의 MTU 값은 노드가 연결된 vSphere의 가상 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. 그리드 네트워크와 달리 모든 노드는 동일한 관리 네트워크에 연결할 필요가 없습니다. 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. 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. 그리드 네트워크와 달리 모든 노드는 동일한 클라이언트 네트워크에 연결할 필요가 없습니다. 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. 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 다음과 같습니다 *`network type/protocol/default port used by grid node/new port`*. 여기서 네트워크 유형은 그리드, 관리자 또는 클라이언트이고 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.

  쉼표로 구분된 목록을 사용하여 여러 포트를 다시 매핑할 수도 있습니다.

  예를 들면 다음과 같습니다.

```
PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80
```

- * 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 다음과 같습니다 *network type/protocol/_default port used by grid node /new port*. 여기서 네트워크 유형은 그리드, 관리자 또는 클라이언트이고 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.

  쉼표로 구분된 목록을 사용하여 여러 인바운드 포트를 다시 매핑할 수도 있습니다.

  예를 들면 다음과 같습니다.

```
PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22
```

- * Temporary_password_type *: 노드가 그리드에 합류하기 전에 VM 콘솔이나 StorageGRID 설치 API에 액세스하거나 SSH를 사용할 때 사용되는 임시 설치 암호의 유형입니다.

  모든 노드 또는 대부분의 노드가 동일한 유형의 임시 설치 암호를 사용하는 경우 전역 매개 변수 섹션에 형식을 지정합니다. 그런 다음 필요에 따라 개별 노드에 대해 다른 설정을 사용합니다. 예를 들어, * 사용자 정의 암호 사용 * 을 전역적으로 선택한 경우 * custom_temporary_password=<password> * 를 사용하여 각 노드의 암호를 설정할 수 있습니다.

- Temporary_password_type * 은 다음 중 하나일 수 있습니다.
  - * 노드 이름 사용 *: 노드 이름은 임시 설치 암호로 사용되며 VM 콘솔, StorageGRID 설치 API 및 SSH에 대한 액세스를 제공합니다.
  - * 비밀번호 비활성화 * : 임시 설치 비밀번호가 사용되지 않습니다. 설치 문제를 디버깅하기 위해 VM에 액세스해야 하는 경우 를 참조하십시오"설치 문제를 해결합니다".
  - * 사용자 정의 암호 사용 *: * custom_temporary_password=<password> * 에 제공된 값은 임시 설치 암호로 사용되며 VM 콘솔, StorageGRID 설치 API 및 SSH에 대한 액세스를 제공합니다.

    필요한 경우 * Temporary_password_type * 매개 변수를 생략하고 * custom_Temporary_password=<password> * 만 지정할 수 있습니다.

- *custom_Temporary_password=<password> * 선택 요소입니다. 설치 중에 VM 콘솔, StorageGRID 설치 API 및 SSH에 액세스할 때 사용할 임시 암호입니다. Temporary_password_type * 이 * 노드 이름 사용 * 또는 * 암호

비활성화 * 로 설정된 경우 무시됩니다.

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 또는 VM_API_Gateway_Node
- * STORAGE_TYPE *: 조합, 데이터 또는 메타데이터. 스토리지 노드의 이 선택적 매개 변수는 지정되지 않은 경우 기본적으로 Combined(데이터 및 메타데이터)로 설정됩니다. 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.
- * 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 "그리드 노드가 기본 관리자 노드를 검색하는 방법"참조하십시오.

  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
  TEMPORARY_PASSWORD_TYPE = Use custom password
  CUSTOM_TEMPORARY_PASSWORD = Passw0rd

  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 노드에 대한 다음 추가 설정은 선택 사항입니다.

- * disk *: 기본적으로 스토리지 노드에는 RangeDB 사용을 위해 3 개의 4TB 디스크가 할당됩니다. 디스크 매개 변수를 사용하여 이러한 설정을 늘릴 수 있습니다. 예를 들면 다음과 같습니다.

```
DISK = INSTANCES=16, CAPACITY=4096
```

- * STORAGE_TYPE *: 기본적으로 모든 새 스토리지 노드는 오브젝트 데이터와 메타데이터를 모두 저장하도록 구성되어 있습니다. storage_type 매개 변수를 사용하여 데이터나 메타데이터만 저장하도록 스토리지 노드 유형을 변경할 수 있습니다. 예를 들면 다음과 같습니다.

```
STORAGE_TYPE = data
```

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 노드의 배포를 자동화하기 위해 수정한 Bash 스크립트와 deploy-vsphere-ovftool.ini 구성 파일을 사용할 수 `deploy-vsphere-ovftool.sh` 있습니다.

시작하기 전에

사용자 환경에 대한 deploy-vsphere-ovftool.ini 구성 파일을 만들었습니다.

도움말 명령을 입력하여 Bash 스크립트에서 사용할 수 있는 도움말을 사용할 수 (`-h/--help`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 "Passed"이면 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.

시작하기 전에

- 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 예제 구성 파일
configure -StorageGrid.blank.json을 지정합니다	스크립트에 사용할 빈 구성 파일입니다

- `configure-storagegrid.json`구성 파일을 만들었습니다. 이 파일을 작성하려면 예제 구성 파일(`configure-storagegrid.sample.json`)이나 빈 구성 파일을 수정할 수 (`configure-storagegrid.blank.json`있습니다.

  Python 스크립트와 `configure-storagegrid.json` 그리드 구성 파일을 사용하여 StorageGRID 시스템의 구성을 자동화할 수 `configure-storagegrid.py` 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 `platform` 는 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.

임의의 암호를 생성하도록 지정한 경우 파일을 열고 `Passwords.txt` StorageGRID 시스템에 액세스하는 데 필요한 암호를 찾습니다.

```
###################################################################
##### 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"
- "REST API 설치"

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 노드 가상 머신에 대한 호스트, 데이터 저장소 및 네트워크 구성 정보입니다.

> 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.
- 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.
  - DHCP를 사용하는 경우 그리드 네트워크에 있는 기본 관리자 노드의 IP 주소입니다. 자세한 내용은 을 "그리드 노드가 기본 관리자 노드를 검색하는 방법" 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.
  - DHCP를 사용하는 경우 그리드 네트워크에 있는 기본 관리자 노드의 IP 주소입니다. 자세한 내용은 을 "그리드 노드가 기본 관리자 노드를 검색하는 방법" 참조하십시오.
- 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 "VLAN 인터페이스를 구성합니다"참조하십시오.
- 액세스 인터페이스를 추가할 경우 HA 그룹에 직접 추가해야 합니다. 을 "고가용성 그룹을 구성합니다"참조하십시오.

가상 스토리지 노드의 스토리지 볼륨

가상 머신 기반 스토리지 노드에 대한 다음 정보를 수집해야 합니다.

- 추가하려는 스토리지 볼륨(스토리지 LUN)의 수와 크기입니다. 을 참조하십시오."요구사항을 충족해야 합니다"

그리드 구성 정보

그리드를 구성하려면 정보를 수집해야 합니다.

- 그리드 사용권
- NTP(Network Time Protocol) 서버 IP 주소입니다
- DNS 서버 IP 주소입니다

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 mDNS(multicast domain name system)를 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.

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 를 참조하십시오. "어플라이언스 스토리지 노드 구축"

선택적으로 노드의 전원을 켜기 전에 노드 포트를 재매핑하거나 노드의 CPU 또는 메모리 설정을 늘릴 수 있습니다.

시작하기 전에

- "설치 계획 및 준비"소프트웨어, CPU 및 RAM, 스토리지 및 성능에 대한 요구 사항을 검토하고 이해했습니다.
- VMware vSphere 하이퍼바이저에 대해 잘 알고 있으며 이 환경에서 가상 머신을 구축한 경험이 있습니다.

> VMware 툴과 유사한 오픈 소스 구축 패키지인 이 `open-vm-tools` StorageGRID 가상 머신은 포함되어 있습니다. VMware Tools를 수동으로 설치할 필요가 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 있는 경우:

```
NetApp-SG-version-SHA.vmdk
```

- `.ovf`배포하려는 각 그리드 노드 유형에 대한 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-storage.ovf vsphere-storage.mf	스토리지 노드의 템플릿 파일 및 매니페스트 파일
vsphere-gateway.ovf vsphere-gateway.mf	게이트웨이 노드의 템플릿 파일 및 매니페스트 파일

- `.vdmk` `.ovf`, 및 `.mf` 파일은 모두 같은 디렉터리에 있습니다.
- 장애 도메인을 최소화할 계획이 있습니다. 예를 들어 단일 vSphere ESXi 호스트에 모든 게이트웨이 노드를 배포하면 안 됩니다.

운영 구축 환경에서는 단일 가상 머신에서 스토리지 노드를 두 개 이상 실행하지 마십시오. 허용할 수 없는 장애 도메인 문제가 발생할 경우 동일한 ESXi 호스트에서 여러 가상 머신을 실행하지 마십시오.

- 확장 또는 복구 작업의 일부로 노드를 구축하는 경우 또는 이 있는 "StorageGRID 시스템 확장을 위한 지침""복구 및 유지 관리 지침"것입니다.
- StorageGRID 노드를 NetApp ONTAP 시스템에서 할당된 스토리지가 있는 가상 머신으로 구축하는 경우 볼륨에 FabricPool 계층화 정책이 설정되어 있지 않은 것이 확인되었습니다. 예를 들어 StorageGRID 노드가 VMware 호스트에서 가상 머신으로 실행 중인 경우 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.

이 작업에 대해

이 지침에 따라 초기에 VMware 노드를 배포하거나, 확장 시 새 VMware 노드를 추가하거나, 복구 작업의 일부로 VMware 노드를 대체하십시오. 단계에 설명된 경우를 제외하고 노드 구축 절차는 관리 노드, 스토리지 노드 및 게이트웨이 노드를 포함한 모든 노드 유형에 대해 동일합니다.

새 StorageGRID 시스템을 설치하는 경우:

- 노드는 원하는 순서로 배포할 수 있습니다.
- 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 다른 모든 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
vsphere-primary-admin.ovf
vsphere-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 지침에 따라 스토리지 복구 단계입니다새 가상 디스크를 추가하거나, 오류가 발생한 그리드 노드에서 가상 하드 디스크를 다시 연결하거나, 둘 다 수행합니다.

   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 등의 일부 하이퍼바이저 매개 변수를 조정해야 할 수 `MaxAddressableSpaceTB` 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. + 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용됩니다. 그리드의 모든 노드, 모든 사이트와 서브넷에 걸쳐 연결을 제공합니다. 그리드 네트워크의 모든 노드는 다른 모든 노드와 통신할 수 있어야 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.
   - Admin 또는 Client 네트워크를 사용하는 경우 노드가 동일한 Admin 또는 Client 네트워크에 있을 필요가 없습니다.

7. 템플릿 사용자 정의 * 의 경우 필요한 StorageGRID 노드 속성을 구성합니다.

a. 노드 이름 * 을 입력합니다.

> 그리드 노드를 복구하는 경우 복구할 노드의 이름을 입력해야 합니다.

b. 임시 설치 암호를 지정하려면 * 임시 설치 암호 * 드롭다운을 사용하십시오. 그러면 새 노드가 그리드에 합류하기 전에 VM 콘솔이나 StorageGRID 설치 API에 액세스하거나 SSH를 사용할 수 있습니다.

> 임시 설치 암호는 노드 설치 중에만 사용됩니다. 노드가 그리드에 추가된 후 복구 패키지의 파일에"노드 콘솔 암호" 나열된 를 사용하여 액세스할 수 있습니다. `Passwords.txt`

- * 노드 이름 사용 *: * 노드 이름 * 필드에 입력한 값이 임시 설치 암호로 사용됩니다.
- * 사용자 정의 암호 사용 *: 사용자 정의 암호는 임시 설치 암호로 사용됩니다.
- * 비밀번호 비활성화 * : 임시 설치 비밀번호가 사용되지 않습니다. 설치 문제를 디버깅하기 위해 VM에 액세스해야 하는 경우 를 참조하십시오"설치 문제를 해결합니다".

c. 사용자 정의 암호 사용 * 을 선택한 경우 * 사용자 정의 암호 * 필드에 사용할 임시 설치 암호를 지정합니다.

d. 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.

e. 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 수행합니다.

엔터프라이즈 네트워킹 정책이 StorageGRID에서 사용하는 하나 이상의 포트에 대한 액세스를 제한하는 경우 포트를 다시 매핑해야 할 수 있습니다. StorageGRID에서 사용하는 포트는 를 "네트워킹 지침"참조하십시오.

> ⓘ 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. Set Value * 를 선택합니다.
       ii. 포트 매핑을 입력합니다.

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

       `<network type>` 그리드, 관리자 또는 클라이언트이며 `<protocol>` TCP 또는 UDP입니다.

       예를 들어 포트 22에서 포트 3022로 ssh 트래픽을 재매핑하려면 다음을 입력합니다.

```
client/tcp/22/3022
```

       쉼표로 구분된 목록을 사용하여 여러 포트를 다시 매핑할 수 있습니다.

예를 들면 다음과 같습니다.

```
client/tcp/18082/443, client/tcp/18083/80
```

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. Set Value * 를 선택합니다.

ii. 포트 매핑을 입력합니다.

`<network type>/<protocol>/<remapped inbound port>/<default inbound port used by grid node>`

`<network type>` 그리드, 관리자 또는 클라이언트이며 `<protocol>` TCP 또는 UDP입니다.

예를 들어, 포트 3022로 전송된 인바운드 SSH 트래픽을 그리드 노드가 포트 22에서 수신하도록 재매핑하려면 다음을 입력합니다.

```
client/tcp/3022/22
```

쉼표로 구분된 목록을 사용하여 여러 인바운드 포트를 다시 매핑할 수 있습니다.

예를 들면 다음과 같습니다.

```
grid/tcp/3022/22, admin/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.

시작하기 전에

기본 관리 노드를 구축하고 초기 시작 시퀀스를 완료해야 합니다.

단계

1. 웹 브라우저를 열고 다음으로 이동합니다.

   `https://primary_admin_node_ip`

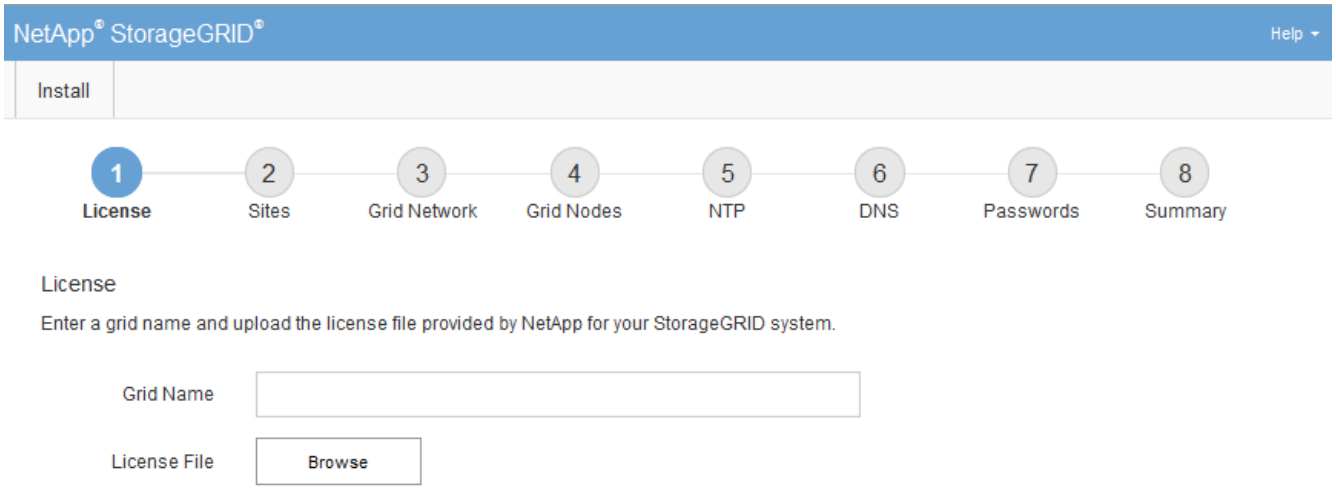
   또는 포트 8443에서 그리드 관리자에 액세스할 수 있습니다.

   `https://primary_admin_node_ip:8443`

   네트워크 구성에 따라 그리드 네트워크 또는 관리 네트워크의 기본 관리 노드 IP에 대한 IP 주소를 사용할 수 있습니다. 신뢰할 수 없는 인증서로 이동하려면 브라우저에서 보안/고급 옵션을 사용해야 할 수 있습니다.

2. 필요에 따라 임시 설치 관리자 암호를 관리합니다.
   - 이러한 방법 중 하나를 사용하여 암호를 이미 설정한 경우 암호를 입력하여 계속 진행합니다.
     - 사용자가 이전에 설치 프로그램에 액세스하는 동안 암호를 설정했습니다
     - SSH/콘솔 암호를 OVF 속성에서 자동으로 가져왔습니다
   - 암호를 설정하지 않은 경우 StorageGRID 설치 프로그램을 보호할 암호를 선택적으로 설정합니다.
3. StorageGRID 시스템 설치 * 를 선택합니다.

   StorageGRID 그리드를 구성하는 데 사용되는 페이지가 나타납니다.



StorageGRID 라이센스 정보를 지정합니다

StorageGRID 시스템의 이름을 지정하고 NetApp에서 제공하는 라이센스 파일을 업로드해야 합니다.

단계

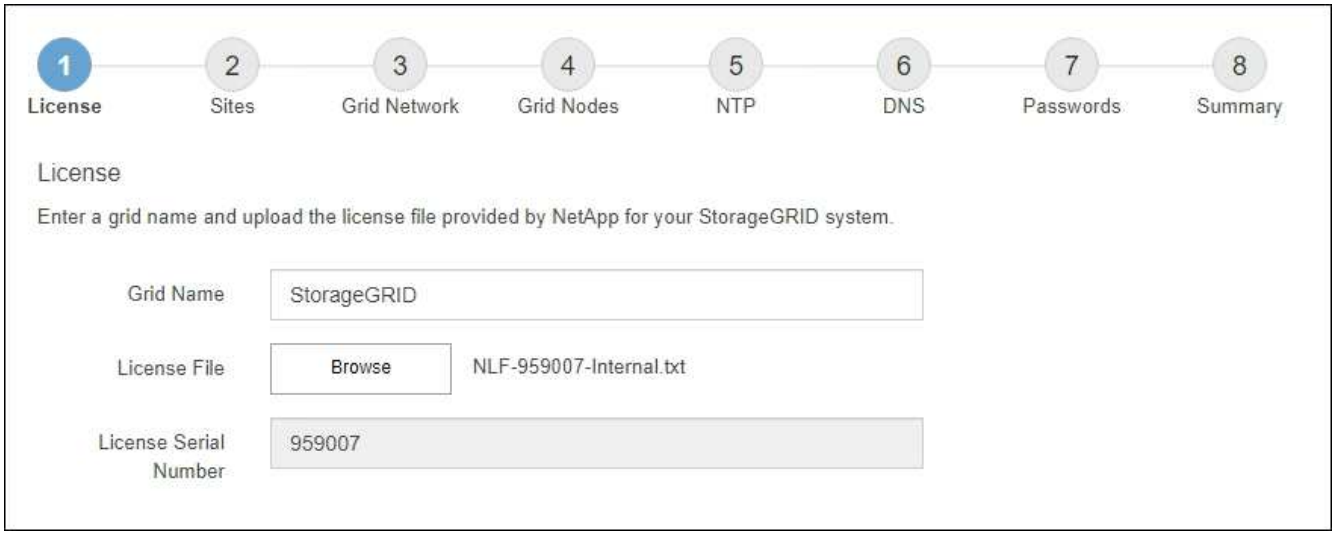
1. 라이센스 페이지의 * 그리드 이름 * 필드에 StorageGRID 시스템에 대한 의미 있는 이름을 입력합니다.

   설치 후, 이름이 Nodes 메뉴 맨 위에 표시됩니다.

2. 찾아보기 * 를 선택하고 NetApp 라이센스 파일을 찾은 (`NLF-*unique-id*.txt`다음 * 열기 * 를 선택합니다.

   라이센스 파일의 유효성이 검사되고 일련 번호가 표시됩니다.

   StorageGRID 설치 아카이브에는 제품에 대한 지원 권한이 없는 무료 라이센스가 포함되어 있습니다. 설치 후 지원을 제공하는 라이센스로 업데이트할 수 있습니다.



3. 다음 * 을 선택합니다.

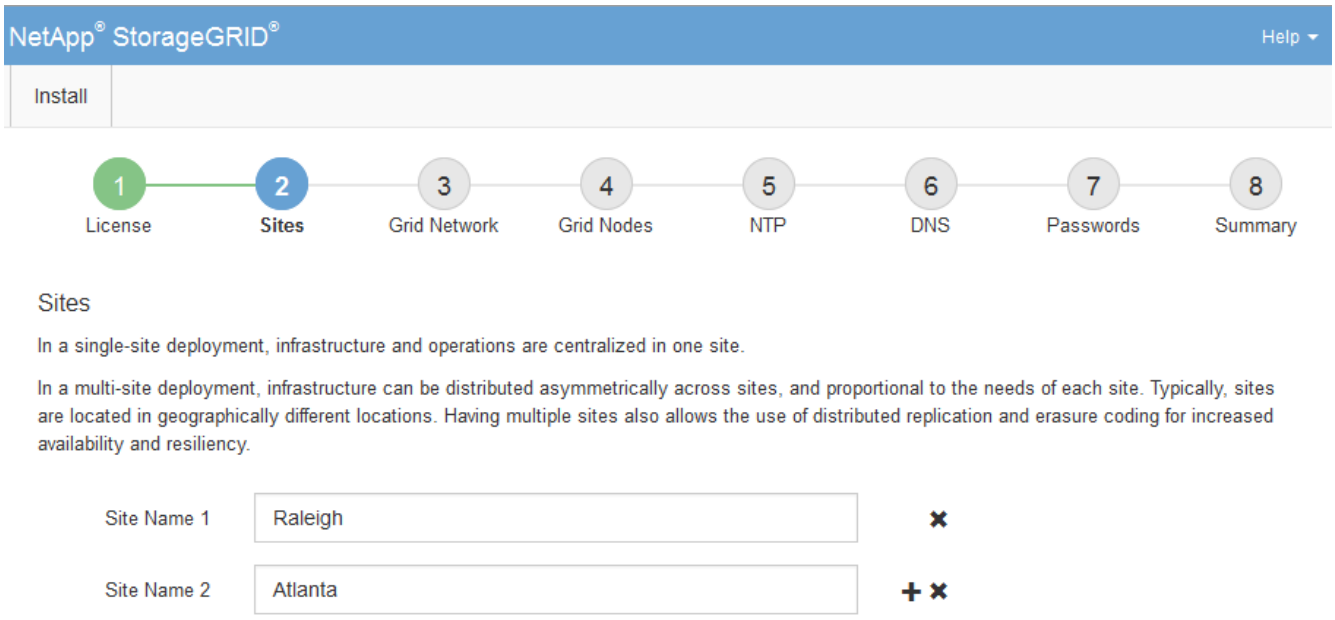
사이트를 추가합니다

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.

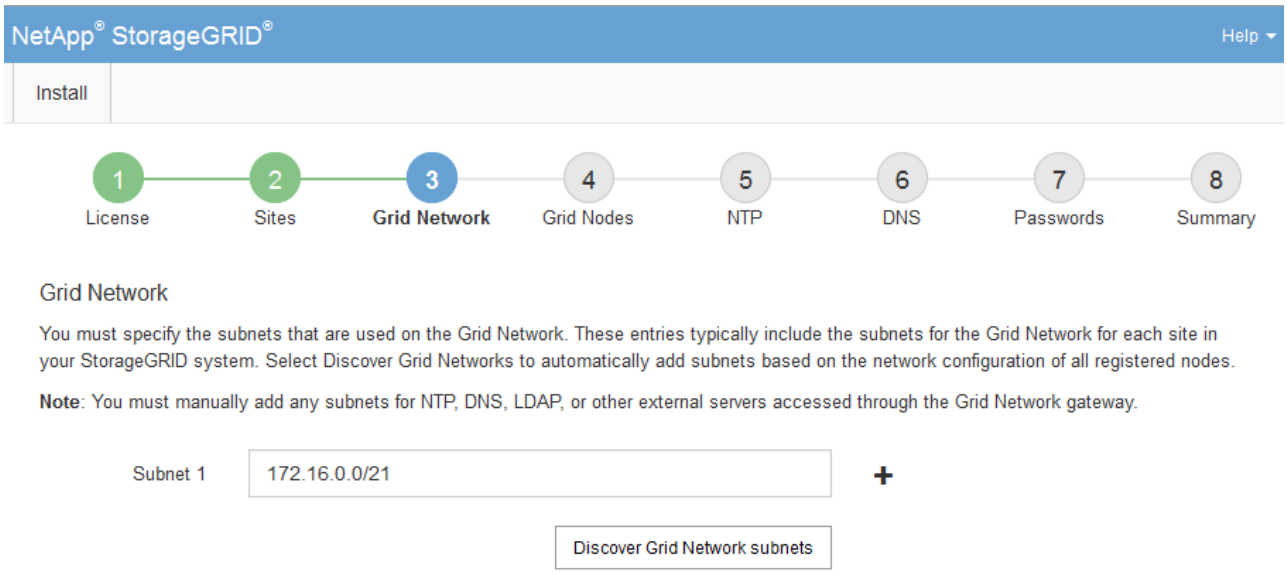
이 작업에 대해

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. 그리드 네트워크의 모든 사이트에 대해 모든 서브넷을 지정해야 합니다.
   - 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.
   - 그리드 네트워크 게이트웨이를 통해 액세스하는 NTP, DNS, LDAP 또는 기타 외부 서버에 대해 서브넷을 수동으로 추가해야 합니다.



3. 다음 * 을 클릭합니다.

보류 중인 그리드 노드를 승인합니다

StorageGRID 시스템에 가입하려면 각 그리드 노드를 승인해야 합니다.

시작하기 전에

모든 가상 및 StorageGRID 어플라이언스 그리드 노드를 구축했습니다.

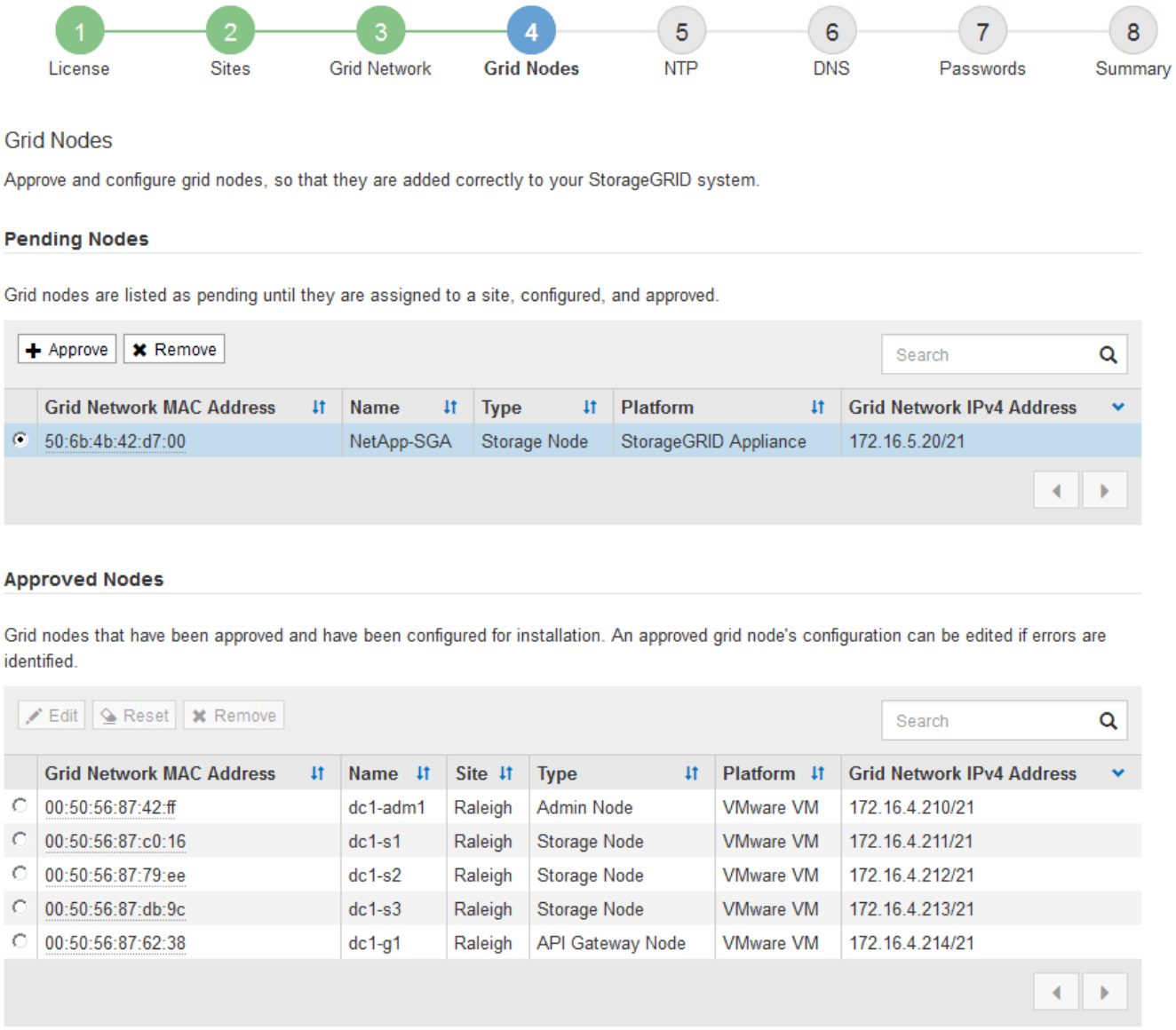
일부 노드를 나중에 설치하는 대신 모든 노드를 한 번 설치하는 것이 더 효율적입니다.

단계

1. Pending Nodes(보류 중인 노드) 목록을 검토하고 배포된 모든 그리드 노드가 표시되는지 확인합니다.

그리드 노드가 누락된 경우 그리드 노드가 성공적으로 배포되었으며 admin_IP에 대해 설정된 기본 관리 노드의 올바른 그리드 네트워크 IP가 있는지 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 노드에 대한 사이트의 시스템 이름입니다.
   - * 이름 *: 노드의 시스템 이름입니다. 기본적으로 노드를 구성할 때 지정한 이름이 지정됩니다.

     시스템 이름은 내부 StorageGRID 작업에 필요하며 설치를 완료한 후에는 변경할 수 없습니다. 그러나 설치 프로세스의 이 단계에서 필요에 따라 시스템 이름을 변경할 수 있습니다.

     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.

- * 스토리지 유형 * (스토리지 노드에만 해당): 새 스토리지 노드가 데이터 전용, 메타데이터 전용 또는 둘 다에 대해서만 사용되도록 지정합니다. 옵션은 * 데이터 및 메타데이터 * ("결합"), * 데이터 전용 * 및 * 메타데이터만 * 입니다.

  이러한 노드 유형의 요구 사항에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

- * 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. 구성된 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. 구성된 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 제거합니다.

f. Pending Nodes 테이블에서 노드를 제거합니다.

g. 대기 중인 노드 목록에 노드가 다시 나타날 때까지 기다립니다.

h. 적절한 네트워크를 구성할 수 있는지 확인합니다. 어플라이언스 설치 프로그램의 IP 구성 페이지에서 제공한 정보로 이미 채워져야 합니다.

   자세한 내용은 를 "하드웨어 설치를 빠르게 시작합니다" 참조하여 제품에 대한 지침을 확인하십시오.

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. 구성된 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 제거합니다.

   f. Pending Nodes 테이블에서 노드를 제거합니다.

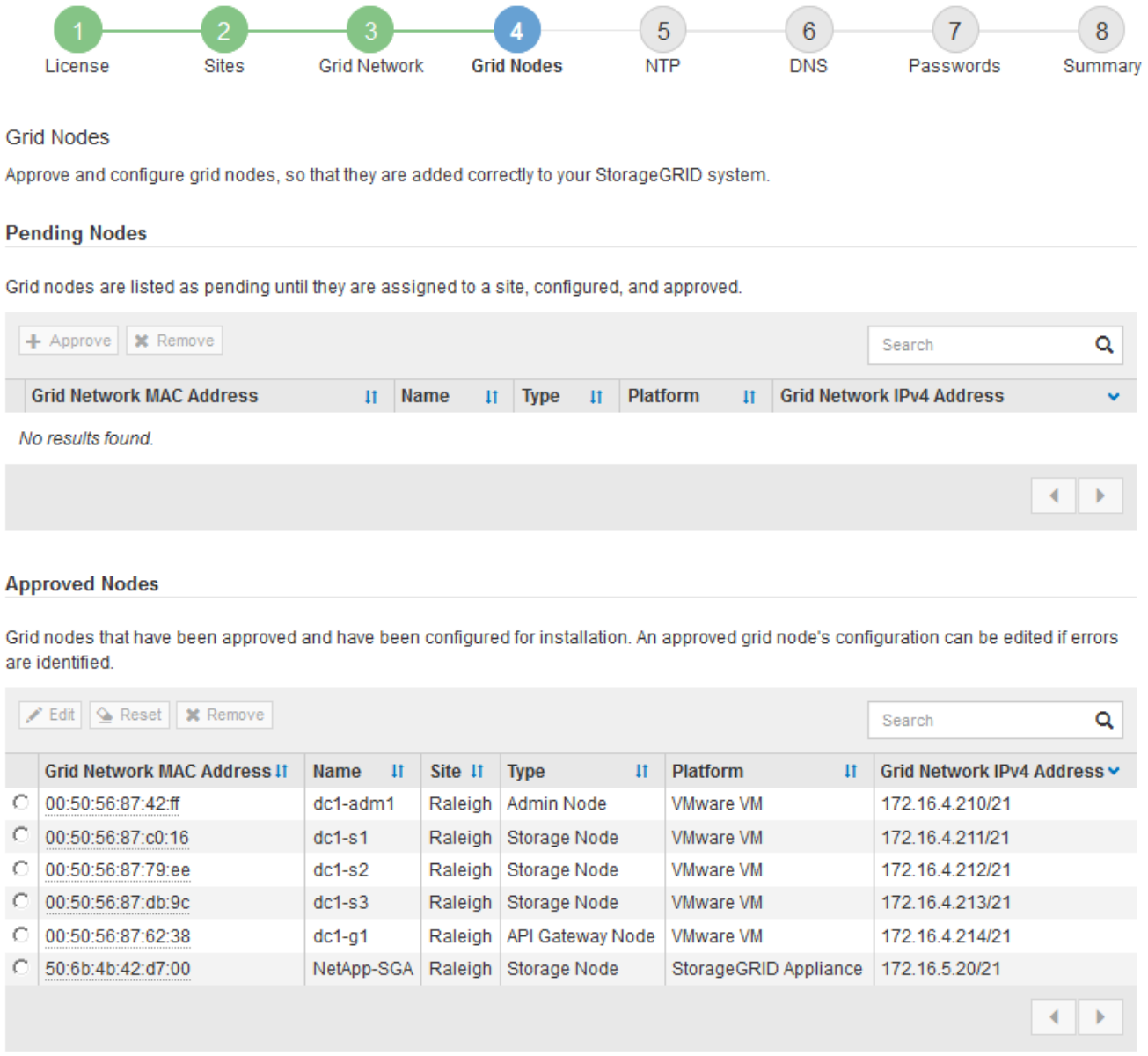
   g. 대기 중인 노드 목록에 노드가 다시 나타날 때까지 기다립니다.

   h. 적절한 네트워크를 구성할 수 있는지 확인합니다. 어플라이언스 설치 프로그램의 IP 구성 페이지에서 제공한 정보로 이미 채워져야 합니다.

      자세한 내용은 를 "하드웨어 설치를 빠르게 시작합니다" 참조하여 제품에 대한 지침을 확인하십시오.

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"

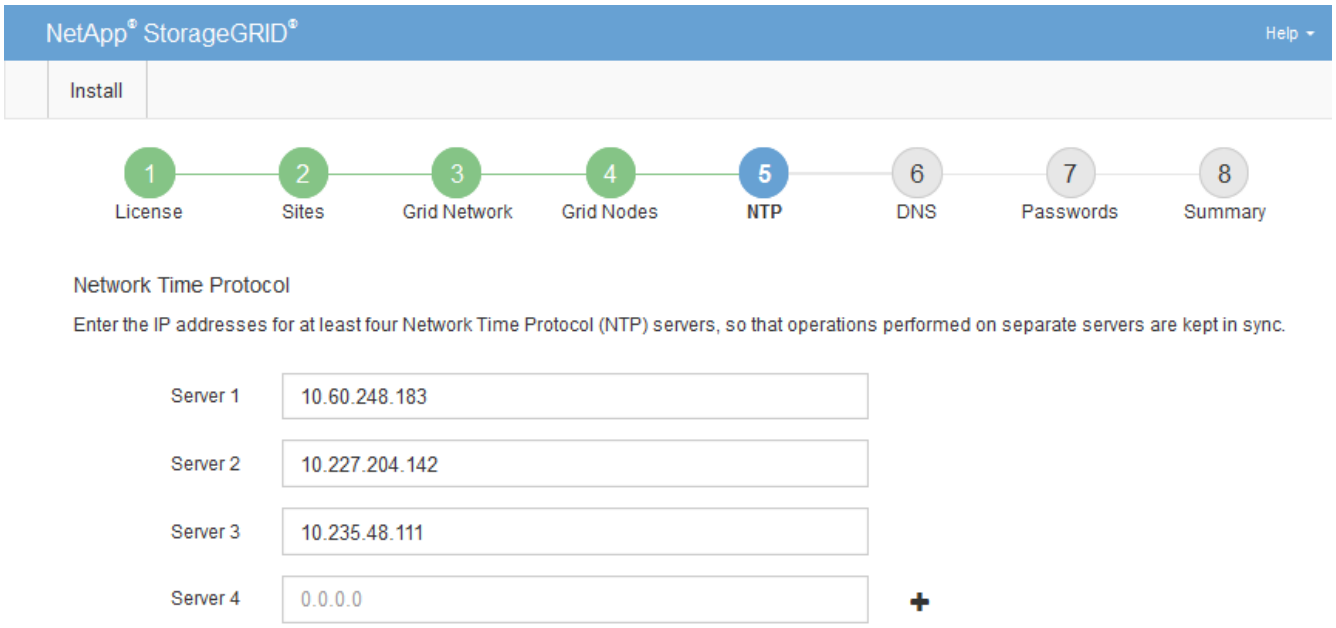
외부 NTP 서버는 이전에 기본 NTP 역할을 할당한 노드에서 사용됩니다.

> 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.

DNS 서버 정보를 지정합니다

IP 주소 대신 호스트 이름을 사용하여 외부 서버에 액세스할 수 있도록 StorageGRID 시스템에 대한 DNS 정보를 지정해야 합니다.

이 작업에 대해

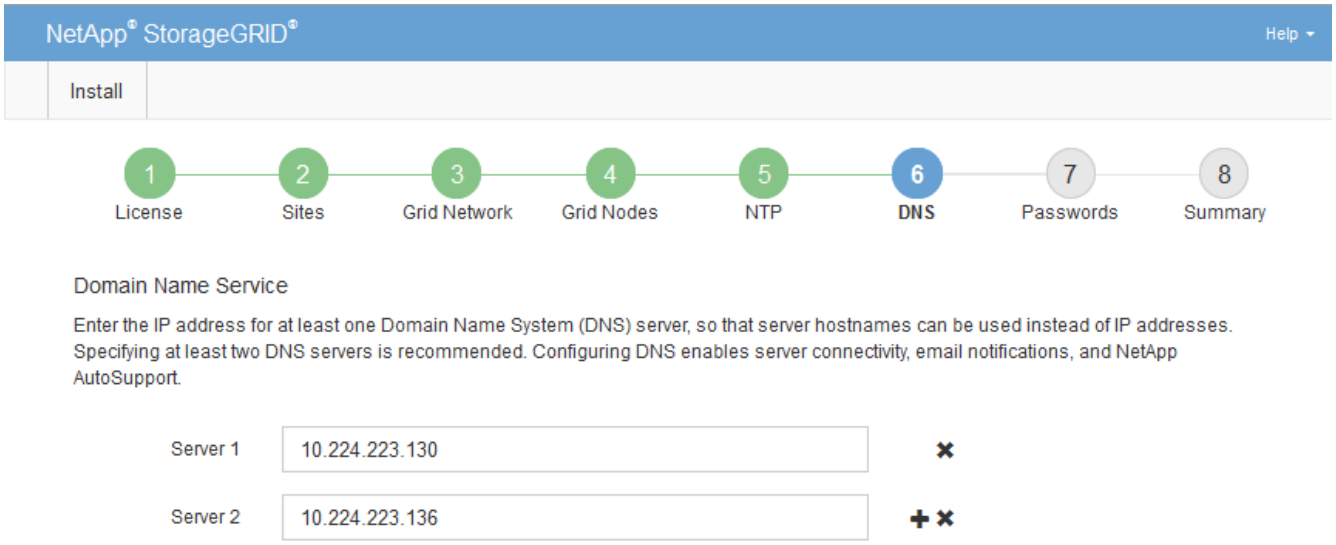
를 "DNS 서버 정보입니다" 지정하면 이메일 알림 및 AutoSupport에 IP 주소 대신 FQDN(정규화된 도메인 이름) 호스트 이름을 사용할 수 있습니다.

제대로 작동하려면 DNS 서버를 두 대 또는 세 대 지정합니다. 3개 이상을 지정하면 일부 플랫폼의 알려진 OS 제한 때문에 3개만 사용할 수 있습니다. 사용자 환경에 라우팅 제한이 있는 경우 개별 노드(일반적으로 사이트의 모든 노드)에서 최대 3개의 DNS 서버로 구성된 다른 세트를 사용할 수 "DNS 서버 목록을 사용자 지정합니다"있습니다.

가능한 경우 각 사이트에서 로컬로 액세스할 수 있는 DNS 서버를 사용하여 isfan 사이트가 외부 대상의 FQDN을 확인할 수 있도록 합니다.

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 `Passwords.txt` 복구 패키지의 파일에 저장됩니다.

단계

1. Provisioning Passphrase * 에서 StorageGRID 시스템의 그리드 토폴로지를 변경하는 데 필요한 프로비저닝 암호를 입력합니다.

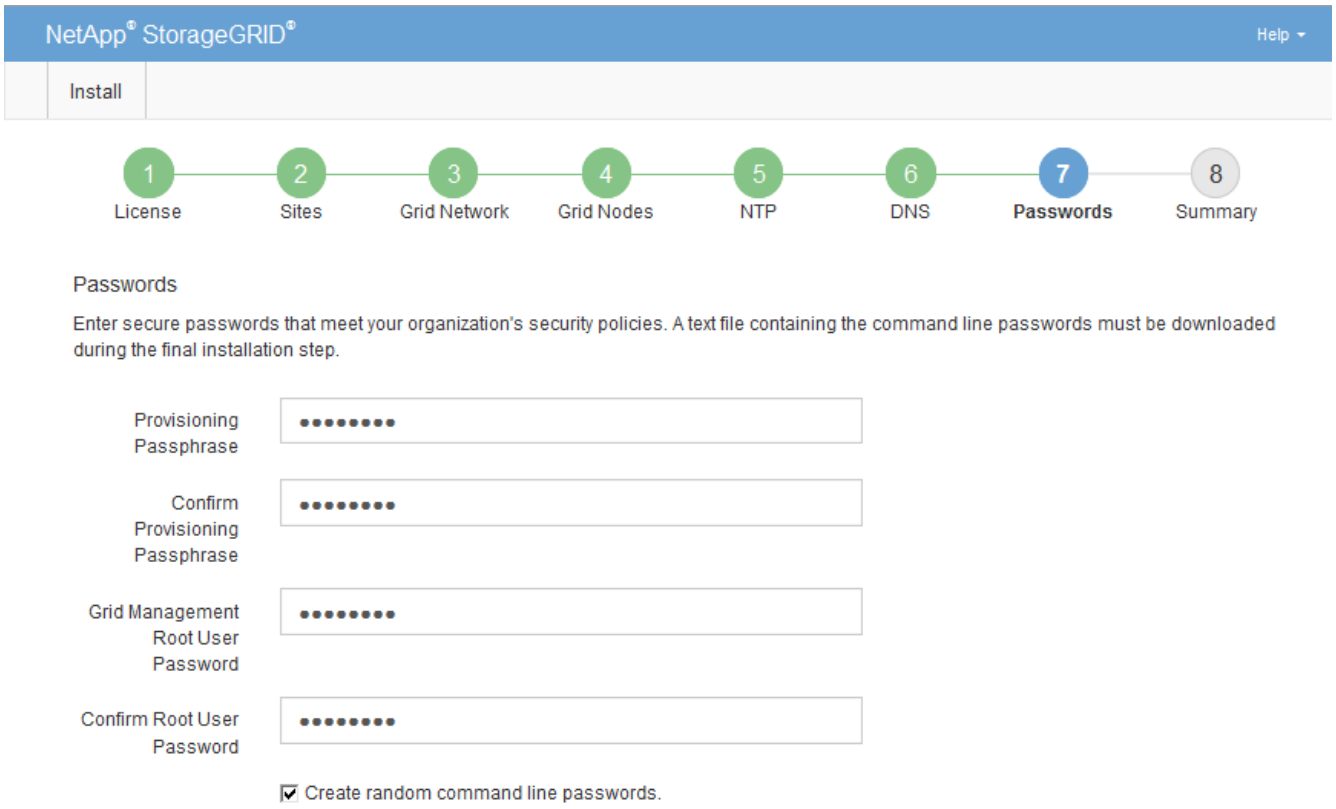
   프로비저닝 암호를 안전한 장소에 보관합니다.

   > 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. 그리드 관리 루트 사용자 암호 * 에 그리드 관리자에 "루트" 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. Clear * 임의의 명령줄 암호 만들기 * 기본 암호를 사용하여 "root" 또는 "admin" 계정을 사용하여 명령줄에서 그리드 노드에 액세스하려는 경우 데모 그리드에만 사용합니다.

   > 복구 패키지 파일을 다운로드하라는 메시지가 (`sgws-recovery-package-id-revision.zip`표시됩니다.) 요약 페이지에서 * 설치 * 를 클릭하면 됩니다. "이 파일을 다운로드합니다"설치를 완료해야 합니다. 시스템에 액세스하는 데 필요한 암호는 `Passwords.txt` 복구 패키지 파일에 포함된 파일에 저장됩니다.

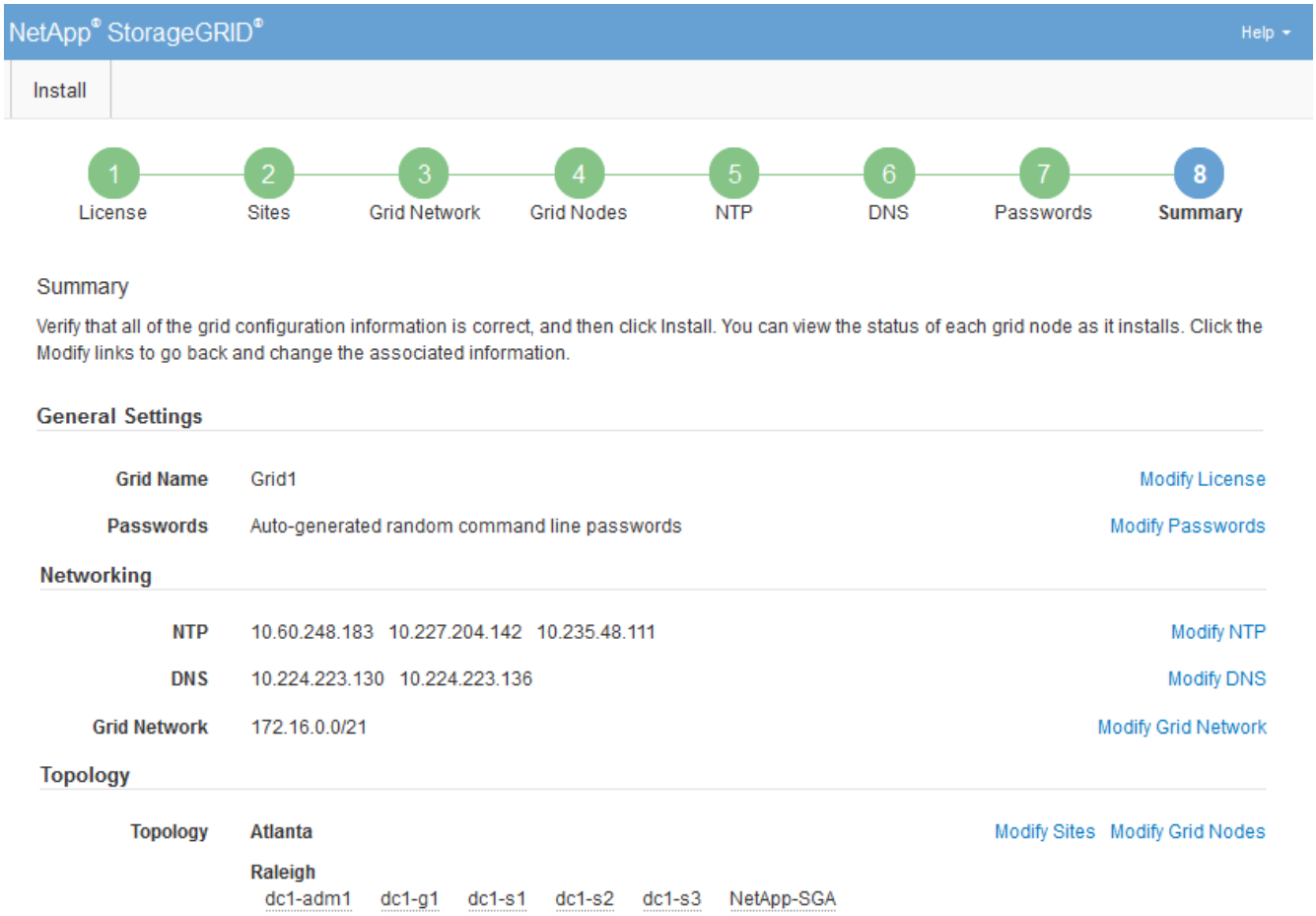
6. 다음 * 을 클릭합니다.

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. 자세한 내용은 을 "네트워킹 지침" 참조하십시오.

4. 복구 패키지 다운로드 * 를 클릭합니다.

그리드 토폴로지가 정의된 지점으로 설치가 진행되면 복구 패키지 파일을 다운로드하라는 메시지가 (`.zip`표시됩니다.) 이 파일의 내용에 성공적으로 액세스할 수 있는지 확인합니다. 하나 이상의 그리드 노드에 장애가 발생할 경우 StorageGRID 시스템을 복구할 수 있도록 복구 패키지 파일을 다운로드해야 합니다. 백그라운드에서 설치가 계속되지만 이 파일을 다운로드하여 확인할 때까지 설치를 완료하고 StorageGRID

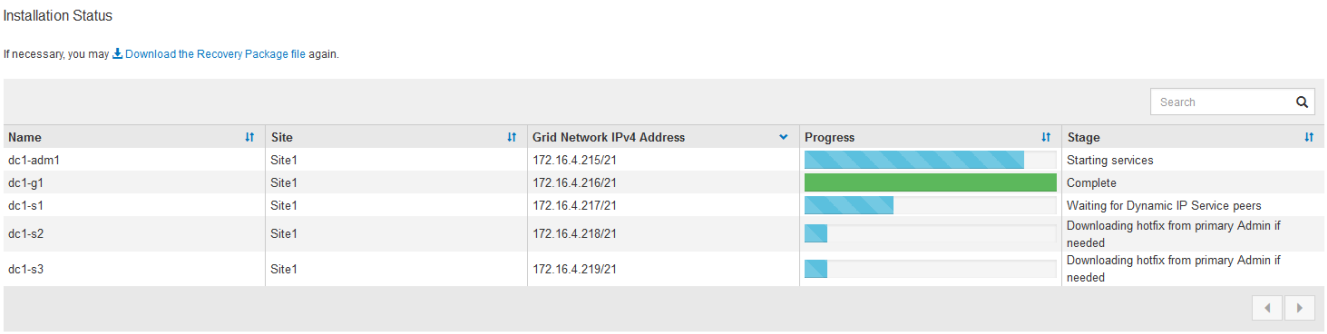
시스템에 액세스할 수 없습니다.

5. 파일의 내용을 추출한 다음 안전하고 별도의 두 위치에 저장할 수 있는지 확인합니다 `.zip`.

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

6. 복구 패키지 파일 * 을 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.

> 그리드 네트워크 구성이 DHCP에 의해 변경될 때 노드가 재부팅되므로 DHCP 변경이 여러 노드에 동시에 영향을 미칠 경우 운영이 중단될 수 있습니다.

- 그리드 노드의 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 변경하려면 IP 변경 절차를 사용해야 합니다. 을 "IP 주소를 구성합니다"참조하십시오.
- 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.

REST API 설치

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 데이터 형식에 대해 잘 알고 있다고 가정합니다.

API 문서 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.
- * Temporary-password * — 설치 중 mgmt-API를 보호하기 위한 임시 암호의 작동.

다음 단계로 넘어갑니다

설치를 완료한 후 필요한 통합 및 구성 작업을 수행합니다. 필요에 따라 옵션 작업을 수행할 수 있습니다.

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.

- "테넌트 계정을 생성합니다" StorageGRID 시스템에 오브젝트를 저장하는 데 사용되는 S3 클라이언트 프로토콜의 경우
- "시스템 액세스를 제어합니다" 그룹 및 사용자 계정을 구성합니다. 선택적으로 Active Directory 또는 OpenLDAP와 같은 관리 그룹과 사용자를 가져올 수 "통합 ID 소스를 구성합니다"있습니다. 또는, 할 수 "로컬 그룹 및 사용자를 생성합니다"있습니다.

- 개체를 StorageGRID 시스템에 업로드하는 데 사용할 클라이언트 응용 프로그램을 통합하고 "S3 API를 사용합니다"테스트합니다.
- "ILM(정보 수명 주기 관리) 규칙 및 ILM 정책을 구성합니다" 를 사용하여 오브젝트 데이터를 보호하려고 합니다.
- 설치에 어플라이언스 스토리지 노드가 포함된 경우 SANtricity OS를 사용하여 다음 작업을 완료합니다.
  - 각 StorageGRID 어플라이언스에 연결하십시오.
  - AutoSupport 데이터가 수신되었는지 확인합니다.

  을 "하드웨어를 설정합니다"참조하십시오.
- 을 검토하고 따라 "StorageGRID 시스템 강화 지침"보안 위험을 제거합니다.
- "시스템 경고에 대한 이메일 알림을 구성합니다"..

선택적 태스크입니다

- "그리드 노드 IP 주소를 업데이트합니다" 배포를 계획하고 복구 패키지를 생성한 이후에 변경된 경우
- "스토리지 암호화를 구성합니다"필요한 경우.
- "스토리지 압축을 구성합니다" 필요한 경우 저장된 개체의 크기를 줄입니다.
- "VLAN 인터페이스를 구성합니다" 필요한 경우 네트워크 트래픽을 격리하고 분할합니다.
- "고가용성 그룹을 구성합니다" 필요한 경우 Grid Manager, Tenant Manager 및 S3 클라이언트의 연결 가용성을 향상시킵니다.
- "로드 밸런서 엔드포인트를 구성합니다" 필요한 경우 S3 클라이언트 연결의 경우

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 관리자 노드에서 찾음)

관련 정보

로그 파일에 액세스하는 방법에 대한 자세한 내용은 을 "로그 파일 참조"참조하십시오.

추가 도움이 필요한 경우 에 "NetApp 지원"문의하십시오.

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.

임시 설치 암호가 비활성화되었습니다

VMware 노드를 구축할 때 필요한 경우 임시 설치 암호를 지정할 수 있습니다. VM 콘솔에 액세스하거나 새 노드가 그리드에 합류하기 전에 SSH를 사용하려면 이 암호가 있어야 합니다.

임시 설치 암호를 사용하지 않도록 선택한 경우 설치 문제를 디버깅하기 위한 추가 단계를 수행해야 합니다.

다음 중 하나를 수행할 수 있습니다.

- VM을 재배포하되 콘솔에 액세스하거나 SSH를 사용하여 설치 문제를 디버깅할 수 있도록 임시 설치 암호를 지정합니다.
- vCenter를 사용하여 암호를 설정합니다.
  a. VM의 전원을 끕니다.
  b. vm * 으로 이동하고 * Configure * 탭을 선택한 다음 * vApp Options * 를 선택합니다.
  c. 설정할 임시 설치 암호 유형 지정:
     - 사용자 지정 임시 암호를 설정하려면 * custom_temporary_password * 를 선택하십시오.
     - 노드 이름을 임시 암호로 사용하려면 * Temporary_password_type * 을 선택하십시오.
  d. Set Value * 를 선택합니다.
  e. 임시 암호를 설정합니다.
     - custom_Temporary_password * 를 사용자 정의 암호 값으로 변경합니다.
     - use node name * 값으로 * Temporary_password_type * 을 업데이트합니다.
  f. VM을 다시 시작하여 새 암호를 적용합니다.

StorageGRID 소프트웨어를 업그레이드합니다

StorageGRID 소프트웨어를 업그레이드합니다

다음 지침에 따라 StorageGRID 시스템을 새 릴리즈로 업그레이드하십시오.

업그레이드를 수행하면 StorageGRID 시스템의 모든 노드가 업그레이드됩니다.

시작하기 전에

이 항목을 검토하여 StorageGRID 11.9의 새로운 기능과 향상된 기능에 대해 알아보고, 더 이상 사용되지 않거나 제거된 기능이 있는지 확인하고, StorageGRID API의 변경 사항에 대해 알아보십시오.

- "StorageGRID 11.9의 새로운 기능"
- "제거되거나 사용되지 않는 기능"
- "Grid Management API 변경"
- "테넌트 관리 API의 변경 사항"

StorageGRID 11.9의 새로운 기능

이 StorageGRID 릴리스는 다음과 같은 기능 및 기능 변경 사항을 소개합니다.

확장성

데이터 전용 스토리지 노드

이제 를 설치하여 보다 세분화된 확장을 "데이터 전용 스토리지 노드"수행할 수 있습니다. 메타데이터 처리가 중요하지 않은 경우 인프라를 비용 효율적으로 최적화할 수 있습니다. 이러한 유연성 덕분에 다양한 워크로드와 성장 패턴을 수용할 수 있습니다.

클라우드 스토리지 풀 개선

어디서나 **IAM** 역할 수행

StorageGRID에서는 이제 를 사용하여 단기 자격 증명을 "클라우드 스토리지 풀용 Amazon S3의 모든 위치에서 IAM 역할"지원합니다.

장기 자격 증명을 사용하여 S3 버킷에 액세스하면 이러한 자격 증명이 손상되는 경우 보안 위험이 발생합니다. 단기 자격 증명의 수명은 제한되어 있어 무단 액세스의 위험이 줄어듭니다.

S3 오브젝트 잠금 버킷

이제 할 수 "Amazon S3 엔드포인트를 사용하여 클라우드 스토리지 풀을 구성합니다"있습니다. S3 오브젝트 잠금을 통해 오브젝트가 실수로 또는 악의적으로 삭제되지 않도록 방지합니다. StorageGRID에서 Amazon S3로 데이터를 계층화하는 경우 두 시스템 모두에서 오브젝트 잠금이 설정되어 있으면 데이터 라이프사이클 전체에서 데이터 보호가 향상됩니다.

멀티 테넌시

버킷 제한

"S3 버킷에 대한 설정 제한"에서는 테넌트가 용량을 독점하지 못하도록 할 수 있습니다. 또한, 폭발적인 증가는 예상치 못한 비용을 초래할 수 있습니다. 제한을 정의하면 테넌트 스토리지 비용을 보다 효율적으로 예측할 수 있습니다.

테넌트당 **5,000**개의 버킷

확장성 향상을 위해 StorageGRID는 현재 까지 "테넌트당 5,000개의 S3 버킷"지원합니다. 각 그리드에는 최대 100,000개의 버킷을 포함할 수 있습니다.

5,000개의 버킷을 지원하려면 그리드의 각 스토리지 노드에 최소 64GB의 RAM이 있어야 합니다.

S3 오브젝트 잠금 개선 사항

테넌트별 구성 기능은 유연성과 데이터 보안의 적절한 균형을 제공합니다. 이제 테넌트별 보존 설정을 다음과 같이 구성할 수 있습니다.

- 준수 모드를 허용하거나 허용하지 않습니다
- 최대 보존 기간을 설정합니다

참조:

- "S3 오브젝트 잠금으로 오브젝트 관리"
- "그리드 관리자가 개체 보존을 제어하는 방법"
- "테넌트 계정을 생성합니다"

S3 호환성

X-amz-checksum - SHA256 체크섬

- 이제 S3 REST API에서 다음 링크를 지원합니다…/S3/operations-on-objects.html[`x-amz-checksum-sha256` checksum].
- StorageGRID는 이제 PUT, GET 및 HEAD 작업에 SHA-256 체크섬 지원을 제공합니다. 이러한 체크섬은 데이터 무결성을 향상시킵니다.

S3 프로토콜 지원으로 변경합니다

- Amazon S3에 대한 마운트 지점 지원을 추가하여 애플리케이션을 로컬 파일 시스템처럼 S3 버킷에 직접 연결할 수 있음 이제 더 많은 애플리케이션과 더 많은 사용 사례에 StorageGRID를 사용할 수 있습니다.
- 마운트 지점에 대한 지원을 추가하기 위해 StorageGRID 11.9에는 이 "S3 프로토콜 지원에 대한 추가 변경 사항 "포함되어 있습니다.

유지 관리 및 지원 가능성

AutoSupport

"AutoSupport" 이제 기존 어플라이언스에 대한 하드웨어 장애 사례가 자동으로 생성됩니다.

확장된 노드 클론 작업

노드 클론 사용 편의성이 확장되어 더 큰 스토리지 노드를 지원할 수 있게 되었습니다.

만료된 삭제 마커의 **ILM** 처리가 개선되었습니다

기간이 며칠인 ILM 수집 시간 규칙으로 인해 만료된 오브젝트 삭제 표시자도 제거됩니다. 삭제 표시자는 기간이

경과하고 현재 삭제 작성기가 만료되었을 때만 제거됩니다(현재 버전이 아닌 경우).

"S3 버전 오브젝트 삭제 방법"및 "ILM 정책보다 우선 순위가 높은 버킷 라이프사이클의 예"을 참조하십시오.

노드 서비스 해제 개선

StorageGRID 차세대 하드웨어로 원활하고 효율적으로 전환할 수 있도록 이 "노드 폐기"개선되었습니다.

로드 밸런서 엔드포인트를 위한 **syslog**

부하 분산 장치 끝점 액세스 로그에는 HTTP 상태 코드와 같은 문제 해결 정보가 포함되어 있습니다. StorageGRID가 이제 "이러한 로그를 외부 syslog 서버로 내보냅니다"지원합니다. 이 향상된 기능을 통해 로그를 보다 효율적으로 관리하고 기존 모니터링 및 알림 시스템과의 통합을 수행할 수 있습니다.

유지 관리 및 지원 기능을 위한 추가 개선 사항

- 메트릭 UI 업데이트
- 새 운영 체제 자격 평가
- 새로운 타사 구성 요소 지원

보안

SSH 액세스 키 순환

이제 그리드 관리자가 수행할 수 "SSH 키를 업데이트하고 회전합니다"있습니다. SSH 키를 회전하는 기능은 보안 모범 사례이자 사전 방어 메커니즘입니다.

루트 로그인에 대한 경고

알 수 없는 엔티티가 그리드 관리자에 루트로 로그인할 때"알림이 트리거됩니다". 루트 SSH 로그인 모니터링은 인프라를 보호하기 위한 사전 예방적인 단계입니다.

Grid Manager의 향상된 기능

삭제 코딩 프로필 페이지가 이동되었습니다

삭제 코딩 프로필 페이지는 이제 * configuration * > * System * > * Erasure coding * 에 있습니다. ILM 메뉴에 있었습니다.

검색 기능 향상

이제 에는 "그리드 관리자의 검색 필드"더 나은 일치 논리가 포함되어 있어 페이지 내에서 일반적인 약어와 특정 설정의 이름을 검색하여 페이지를 찾을 수 있습니다. 또한 노드, 사용자 및 테넌트 계정과 같은 더 많은 유형의 항목을 검색할 수도 있습니다.

제거되거나 더 이상 사용되지 않는 기능

이 릴리스에서는 일부 기능이 제거되거나 더 이상 사용되지 않습니다. 업그레이드 전에 클라이언트 응용 프로그램을 업데이트하거나 구성을 수정해야 하는지 여부를 이해하려면 이 항목을 검토하십시오.

정의

사용되지 않음

이 기능은 새 생산 환경에서 사용할 수 없습니다 *. 기존 운영 환경에서 이 기능을 계속 사용할 수 있습니다.

수명 종료

이 기능을 지원하는 마지막으로 배송된 버전입니다. 경우에 따라 이 단계에서 기능에 대한 문서가 제거될 수 있습니다.

제거되었습니다

이 기능을 지원하지 * 않는 * 첫 번째 버전입니다.

StorageGRID 기능 지원 종료

더 이상 사용되지 않는 기능은 N+2 주 버전에서 제거됩니다. 예를 들어 버전 N(예: 6.3)에서 기능이 더 이상 사용되지 않는 경우 해당 기능이 있는 마지막 버전은 N+1(예: 6.4)입니다. 이 기능이 제품에 없는 경우 버전 N+2(예: 6.5)가 첫 번째 릴리스입니다.

자세한 내용은 를 "소프트웨어 버전 지원 페이지" 참조하십시오.

특정 상황에서 NetApp는 특정 기능에 대한 지원을 예상보다 빨리 종료할 수 있습니다.

피처	사용되지 않음	수명 종료	제거되었습니다	이전 문서에 대한 링크
레거시 알람(*NOT Alerts*)	11.7	11.8	11.9	"알람 기준(StorageGRID 11.8)"
아카이브 노드 지원	11.7	11.8	11.9	"아카이브 노드 해제 시 고려 사항(StorageGRID 11.8)" • 참고 *: 업그레이드를 시작하기 전에 다음을 수행해야 합니다. 1. 모든 아카이브 노드를 해제합니다. 을 "그리드 노드 폐기(StorageGRID 11.8 문서 사이트)"참조하십시오. 2. 스토리지 풀 및 ILM 정책에서 모든 아카이브 노드 참조를 제거합니다. 을 "NetApp 기술 자료: StorageGRID 11.9 소프트웨어 업그레이드 해결 가이드 "참조하십시오.
CIFS/Samba를 통한 내보내기 감사	11.1	11.6	11.7	
CLB 서비스	11.4	11.6	11.7	

피처	사용되지 않음	수명 종료	제거되었습니다	이전 문서에 대한 링크
Docker 컨테이너 엔진	11.8	11.9	미정	소프트웨어 전용 배포를 위한 컨테이너 엔진으로 Docker에 대한 지원은 더 이상 사용되지 않습니다. Docker는 향후 릴리즈에서 다른 컨테이너 엔진으로 대체될 예정입니다. 을 "현재 지원되는 Docker 버전 목록입니다"참조하십시오.
NFS 감사 엑스포트	11.8	11.9	12.0	"NFS에 대한 감사 클라이언트 액세스 구성(StorageGRID 11.8)"
Swift API 지원	11.7	11.9	12.0	"Swift REST API 사용(StorageGRID 11.8)"
RHEL 8.8 를 참조하십시오	11.9	11.9	12.0	
RHEL 9.0 를 참조하십시오	11.9	11.9	12.0	
RHEL 9.2 를 참조하십시오	11.9	11.9	12.0	
Ubuntu 18.04	11.9	11.9	12.0	
Ubuntu 20.04	11.9	11.9	12.0	
데비안 11	11.9	11.9	12.0	

참고 항목:

- "Grid Management API 변경"
- "테넌트 관리 API의 변경 사항"

Grid Management API 변경

StorageGRID 11.9은 그리드 관리 API 버전 4를 사용합니다. 버전 4는 버전 3을 사용하지 않지만 버전 1, 2 및 3은 계속 지원됩니다.

> StorageGRID 11.9에서는 더 이상 사용되지 않는 관리 API 버전을 계속 사용할 수 있지만, 이러한 API 버전에 대한 지원은 향후 StorageGRID 릴리즈에서 제거될 예정입니다. StorageGRID 11.9로 업그레이드한 후 API를 사용하여 더 이상 사용되지 않는 API를 비활성화할 수 `PUT /grid/config/management` 있습니다.

자세한 내용은 을 "Grid Management API를 사용합니다"참조하십시오.

글로벌 **S3** 오브젝트 잠금을 활성화한 후 규정 준수 설정을 검토합니다

글로벌 S3 Object Lock 설정을 활성화한 후 기존 테넌트의 규정 준수 설정을 검토하십시오. 이 설정을 활성화하면 테넌트가 생성된 시점의 StorageGRID 릴리스에 따라 S3 오브젝트 잠금 설정이 달라집니다.

레거시 관리 **API** 요청이 제거되었습니다

이러한 레거시 요청이 제거되었습니다.

`/grid/server-types`

`/grid/ntp-roles`

API 변경 `GET /private/storage-usage`

- 응답 본문에 새 속성, `usageCacheDuration`이 추가되었습니다. 이 속성은 사용 조회 캐시가 유효한 상태로 유지되는 기간(초)을 지정합니다. 이 값은 테넌트 스토리지 할당량 및 버킷 용량 제한에 대한 사용량을 확인할 때 적용됩니다.
- `GET /api/v4/private/storage-usage`스키마의 중첩과 일치하도록 동작이 수정되었습니다.
- 이러한 변경 사항은 전용 API에만 적용됩니다.

API 변경 `GET cross-grid-replication`

/org/containers/:name/cross-grid-replication * get API에는 더 이상 루트 액세스(`rootAccess`) (`viewAllContainers`권한이 필요하지 않습니다. 그러나 모든 (`manageAllContainers`버킷 관리 또는 모든 버킷 보기 권한이 있는 사용자 그룹에 속해야 합니다.

/org/containers/:name/cross-grid-replication * PUT API는 변경되지 않으며 루트 액세스 (`rootAccess`권한이 필요합니다.

테넌트 관리 **API**의 변경 사항

StorageGRID 11.9에서는 테넌트 관리 API 버전 4를 사용합니다. 버전 4는 버전 3을 사용하지 않지만 버전 1, 2 및 3은 계속 지원됩니다.

> StorageGRID 11.9에서는 더 이상 사용되지 않는 버전의 테넌트 관리 API를 계속 사용할 수 있지만, 이러한 API 버전에 대한 지원은 향후 StorageGRID 릴리즈에서 제거될 예정입니다. StorageGRID 11.9로 업그레이드한 후 API를 사용하여 더 이상 사용되지 않는 API를 비활성화할 수 `PUT /grid/config/management` 있습니다.

자세한 내용은 을 "테넌트 관리 API 이해"참조하십시오.

버킷 용량 제한에 대한 새로운 **API**

API를 Get/Put 작업과 함께 사용하여 버킷의 스토리지 용량 제한을 가져오고 설정할 수 `/org/containers/{bucketName}/quota-object-bytes` 있습니다.

업그레이드를 계획하고 준비합니다

업그레이드를 완료하는 데 걸리는 시간을 예상합니다

업그레이드 소요 시간에 따라 업그레이드 시기를 고려하십시오. 업그레이드의 각 단계에서 수행할 수 있는 작업과 수행할 수 없는 작업에 유의하십시오.

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
사전 점검을 실행하고 기본 관리 노드를 업그레이드 합니다	업그레이드 사전 점검을 실행하고 기본 관리 노드가 중지, 업그레이드 및 재시작됩니다.	서비스 어플라이언스 노드에서 가장 많은 시간이 필요한 경우 30분에서 1시간까지 소요됨 해결되지 않은 사전 검사 오류가 발생하면 이 시간이 늘어납니다.	기본 관리자 노드에 액세스할 수 없습니다. 연결 오류가 보고될 수 있으며 이 오류는 무시할 수 있습니다. 업그레이드를 시작하기 전에 업그레이드 사전 점검을 실행하면 예약된 업그레이드 유지 관리 기간 전에 오류를 해결할 수 있습니다.
업그레이드 서비스를 시작합니다	소프트웨어 파일이 배포되고 업그레이드 서비스가 시작됩니다.	그리드 노드당 3분	
다른 그리드 노드를 업그레이드 합니다	다른 모든 그리드 노드의 소프트웨어는 노드를 승인하는 순서대로 업그레이드됩니다. 시스템의 모든 노드가 한 번에 하나씩 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.
기능을 활성화합니다	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.

업그레이드 작업	설명	필요한 대략적인 시간입니다	수행해야 합니다
데이터베이스를 업그레이드합니다	업그레이드 프로세스에서는 각 노드를 검사하여 Cassandra 데이터베이스를 업데이트할 필요가 없는지 확인합니다.	노드당 10초 또는 전체 그리드에 대해 몇 분	StorageGRID 11.8에서 11.9로 업그레이드할 때는 Cassandra 데이터베이스를 업그레이드할 필요가 없습니다. 하지만 Cassandra 서비스는 각 스토리지 노드에서 중지했다가 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 추가하여 파일을 다운로드하고 사전 검사 검증을 실행하고 최종 업그레이드 단계를 완료하는 데 필요한 시간을 `.upgrade` 설명합니다.
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 11.9**로 업그레이드하는 데 걸리는 예상 시간입니다

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.

   시스템을 StorageGRID 11.9.0으로 업그레이드하는 데 최대 17시간이 걸릴 수 있습니다.

필요에 따라 여러 세션에서 업그레이드할 그리드 노드의 하위 집합을 승인하여 유지 관리 창을 더 작은 창으로 분할할 수 있습니다. 예를 들어, 한 세션에서 사이트 A의 노드를 업그레이드한 다음 이후 세션에서 사이트 B의 노드를 업그레이드할 수 있습니다. 둘 이상의 세션에서 업그레이드를 수행하도록 선택한 경우 모든 노드가 업그레이드될 때까지 새 기능을 사용할 수 없습니다.

업그레이드 중 시스템에 미치는 영향

업그레이드 중에 StorageGRID 시스템이 어떤 영향을 받는지 알아보십시오.

StorageGRID 업그레이드는 무중단으로 수행할 수 있습니다

StorageGRID 시스템은 업그레이드 프로세스 전반에서 클라이언트 애플리케이션의 데이터를 수집하고 검색할 수 있습니다. 같은 유형의 모든 노드를 업그레이드(예: 스토리지 노드)하도록 승인하면 노드가 한 번에 하나씩 중단되므로 특정 유형의 모든 그리드 노드 또는 모든 그리드 노드를 사용할 수 없게 되는 시간은 없습니다.

지속적인 가용성을 보장하기 위해 ILM 정책에 각 개체의 여러 복사본을 저장하도록 지정하는 규칙이 포함되어 있는지 확인합니다. 또한 모든 외부 S3 클라이언트가 다음 중 하나로 요청을 보내도록 구성되었는지 확인해야 합니다.

- 고가용성(HA) 그룹 가상 IP 주소입니다
- 고가용성 타사 로드 밸런서
- 각 클라이언트에 대해 여러 게이트웨이 노드가 있습니다
- 각 클라이언트에 대해 여러 스토리지 노드

클라이언트 애플리케이션은 단기간 동안 중단될 수 있습니다

StorageGRID 시스템은 업그레이드 프로세스 전반에서 클라이언트 애플리케이션에서 데이터를 수집 및 검색할 수 있지만, 업그레이드에 따라 해당 노드에서 서비스를 다시 시작해야 하는 경우 개별 게이트웨이 노드 또는 스토리지 노드에 대한 클라이언트 연결이 일시적으로 중단될 수 있습니다. 업그레이드 프로세스가 완료되고 개별 노드에서 서비스가 재개되면 연결이 복원됩니다.

단기간 동안 연결이 끊길 수 없는 경우 업그레이드를 적용하기 위해 다운타임을 예약해야 할 수도 있습니다. 선택적 승인을 사용하여 특정 노드가 업데이트되는 시기를 예약할 수 있습니다.

여러 게이트웨이 및 고가용성(HA) 그룹을 사용하여 업그레이드 프로세스 중에 자동 페일오버를 제공할 수 있습니다. 의 지침을 "고가용성 그룹 구성"참조하십시오.

어플라이언스 펌웨어가 업그레이드되었습니다

StorageGRID 11.9 업그레이드 중:

- 모든 StorageGRID 어플라이언스 노드는 StorageGRID 어플라이언스 설치 프로그램 펌웨어 버전 3.9로 자동 업그레이드됩니다.
- SG6060 및 SGF6024 어플라이언스는 자동으로 BIOS 펌웨어 버전 3B08.EX 및 BMC 펌웨어 버전 4.00.07로 업그레이드됩니다.
- SG100 및 SG1000 어플라이언스는 자동으로 BIOS 펌웨어 버전 3B13.EC 및 BMC 펌웨어 버전 4.74.07로 업그레이드됩니다.
- SGF6112, SG6160, SG110 및 SG1100 어플라이언스는 BMC 펌웨어 버전 3.16.07로 자동 업그레이드됩니다.

ILM 정책은 상태에 따라 다르게 처리됩니다

- 활성 정책은 업그레이드 후에도 동일하게 유지됩니다.
- 업그레이드 시 최신 10개의 과거 정책만 유지됩니다.
- 제안된 정책이 있는 경우 업그레이드 중에 삭제됩니다.

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 중지될 때 * node와 통신할 수 없음 * 경고가 표시되거나 일부 노드가 StorageGRID 11.9로 업그레이드되었지만 다른 노드는 여전히 StorageGRID 11.8을 실행 중인 경우 * Cassandra 통신 오류 * 경고가 표시될 수 있습니다. 일반적으로 이러한 알림은 업그레이드가 완료되면 지워집니다.

StorageGRID 11.9로 업그레이드 중에 스토리지 노드가 중지되면 * ILM 배치를 달성 불가 * 경고가 트리거될 수 있습니다. 이 알림은 업그레이드가 완료된 후 1일 동안 지속될 수 있습니다.

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 활성화 * 확인란(* 구성 * > * 모니터링 * > * SNMP 에이전트 *)을 선택 취소합니다. 그런 다음 업그레이드가 완료된 후 알림을 다시 활성화합니다.

구성 변경이 제한됩니다

> 이 목록은 특히 StorageGRID 11.8에서 StorageGRID 11.9로 업그레이드하는 데 적용됩니다. 다른 StorageGRID 릴리즈로 업그레이드하는 경우 해당 릴리즈의 업그레이드 지침에 있는 제한된 변경 사항 목록을 참조하십시오.

새 기능 사용 * 작업이 완료될 때까지 다음을 수행합니다.

- 그리드 구성을 변경하지 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.

> 업그레이드 중에 노드를 복구해야 하는 경우 기술 지원 부서에 문의하십시오.

- StorageGRID 11.9로 업그레이드하는 동안에는 HA 그룹, VLAN 인터페이스 또는 로드 밸런서 엔드포인트를 관리해서는 안 됩니다.
- StorageGRID 11.9로의 업그레이드가 완료될 때까지 HA 그룹을 삭제하지 마십시오. 다른 HA 그룹의 가상 IP 주소에 액세스하지 못할 수 있습니다.

최종 업그레이드 단계 * 작업이 완료될 때까지:

- 확장 절차를 수행하지 마십시오.
- 서비스 해제 절차를 수행하지 마십시오.

테넌트 관리자에서 버킷 세부 정보를 보거나 버킷을 관리할 수 없습니다

StorageGRID 11.9로 업그레이드하는 동안(즉, 시스템이 혼합 버전 환경으로 작동하는 동안) 테넌트 관리자를 사용하여 버킷 세부 정보를 보거나 버킷을 관리할 수 없습니다. Tenant Manager의 Bucket 페이지에 다음 오류 중 하나가 나타납니다.

- 11.9로 업그레이드하는 동안에는 이 API를 사용할 수 없습니다.
- 11.9로 업그레이드하는 동안에는 테넌트 관리자에서 버킷 버전 관리 세부 정보를 볼 수 없습니다.

이 오류는 11.9로의 업그레이드가 완료되면 해결됩니다.

해결 방법

11.9 업그레이드가 진행되는 동안 다음 툴을 사용하여 테넌트 관리자를 사용하는 대신 버킷 세부 정보를 보거나 버킷을 관리할 수 있습니다.

- 버킷에서 표준 S3 작업을 수행하려면 또는 를 "S3 REST API""테넌트 관리 API"사용합니다.
- 버킷에서 StorageGRID 사용자 지정 작업(예: 버킷 일관성 보기 및 수정, 마지막 액세스 시간 업데이트 활성화 또는 비활성화, 검색 통합 구성)을 수행하려면 테넌트 관리 API를 사용합니다.

설치된 **StorageGRID** 버전을 확인합니다

업그레이드를 시작하기 전에 이전 버전의 StorageGRID가 현재 설치되어 있고 사용 가능한 최신 핫픽스가 적용되었는지 확인합니다.

이 작업에 대해

StorageGRID 11.9로 업그레이드하기 전에 그리드에 StorageGRID 11.8이 설치되어 있어야 합니다. 현재 이전 버전의 StorageGRID를 사용 중인 경우 그리드의 현재 버전이 StorageGRID 11.8._x.y_가 될 때까지 모든 이전 업그레이드 파일을 최신 핫픽스와 함께 설치해야 합니다(적극 권장).

에 가능한 업그레이드 경로 중 하나가 예나와 있습니다.

> 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. "NetApp 다운로드: StorageGRID"자세한 내용은 및 각 핫픽스에 대한 릴리스 노트를 참조하십시오.

단계

1. 을 사용하여 그리드 관리자에 "지원되는 웹 브라우저"로그인합니다.
2. 그리드 관리자 상단에서 * 도움말 * > * 정보 * 를 선택합니다.
3. 버전 * 이 11.8._x.y_인지 확인합니다.

   StorageGRID 11.8._x.y_version 번호:

◦ major release * 의 _x_value는 0(11.8.0)입니다.

◦ 핫픽스*가 적용된 경우 _y_value(예: 11.8.0.1)가 있습니다.

4. 버전 * 이 11.8._x.y_가 아니면 로 "NetApp 다운로드: StorageGRID" 이동하여 각 릴리스의 최신 핫픽스를 포함하여 각 이전 릴리스의 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 "StorageGRID 핫픽스 절차"참조하십시오.

예: 버전 **11.6**에서 **StorageGRID 11.9**로 업그레이드

다음 예에서는 StorageGRID 11.9 업그레이드를 준비하기 위해 StorageGRID 버전 11.6에서 버전 11.8로 업그레이드하는 단계를 보여 줍니다.

시스템을 업그레이드할 수 있도록 다음 순서로 소프트웨어를 다운로드하여 설치합니다.

1. StorageGRID 11.6.0 주요 릴리즈로 업그레이드하십시오.
2. 최신 StorageGRID 11.6.0._y_hotfix를 적용합니다.
3. StorageGRID 11.7.0 주요 릴리즈로 업그레이드하십시오.
4. 최신 StorageGRID 11.7.0._y_hotfix를 적용합니다.
5. StorageGRID 11.8.0 주요 릴리즈로 업그레이드하십시오.
6. 최신 StorageGRID 11.8.0._y_hotfix를 적용합니다.

소프트웨어 업그레이드에 필요한 자료를 확보합니다

소프트웨어 업그레이드를 시작하기 전에 필요한 모든 자료를 구하십시오.

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.
프로비저닝 암호	StorageGRID 시스템을 처음 설치할 때 암호가 생성되고 문서화됩니다. 프로비저닝 암호가 파일에 나열되지 `Passwords.txt` 않습니다.

항목	참고
Linux RPM 또는 DEB 아카이브	Linux 호스트에 배포된 노드가 있는 경우 업그레이드를 시작하기 전에 먼저 해야 "RPM 또는 DEB 패키지를 모든 호스트에 다운로드하고 설치합니다"합니다. 운영 체제가 StorageGRID의 최소 커널 버전 요구 사항을 충족하는지 확인합니다. • "Red Hat Enterprise Linux 호스트에 StorageGRID를 설치합니다" • "Ubuntu 또는 Debian 호스트에 StorageGRID를 설치합니다"
StorageGRID 설명서	• "릴리스 정보" StorageGRID 11.9의 경우(로그인 필요). 업그레이드를 시작하기 전에 이 내용을 주의 깊게 읽으십시오. • "StorageGRID 소프트웨어 업그레이드 해결 가이드" 업그레이드 중인 주 버전의 경우(로그인 필요) • 기타 "StorageGRID 설명서"(필요한 경우)

시스템 상태를 확인합니다

StorageGRID 시스템을 업그레이드하기 전에 시스템이 업그레이드를 수용할 준비가 되었는지 확인합니다. 시스템이 정상적으로 실행되고 있고 모든 그리드 노드가 작동하는지 확인합니다.

단계

1. 을 사용하여 그리드 관리자에 "지원되는 웹 브라우저"로그인합니다.
2. 활성 경고를 확인하고 해결합니다.
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. 업그레이드하기 전에 및 "외부 통신"을 "내부 그리드 노드 통신"참조하여 StorageGRID 11.9에 필요한 포트가 모두 열려 있는지 확인합니다.

   StorageGRID 11.9로 업그레이드할 때 추가 포트가 필요하지 않습니다.

   다음 필수 포트가 StorageGRID 11.7에 추가되었습니다. StorageGRID 11.9로 업그레이드하기 전에 먼저 제품을 사용할 수 있는지 확인합니다.

포트	설명
18086	StorageGRID 로드 밸런서에서 LDR 및 새 LDR 서비스로의 S3 요청에 사용되는 TCP 포트입니다. 업그레이드하기 전에 이 포트가 모든 그리드 노드에서 모든 스토리지 노드로 열려 있는지 확인하십시오. 이 포트를 차단하면 StorageGRID 11.9로 업그레이드한 후 S3 서비스가 중단됩니다.

사용자 지정 방화벽 포트를 연 경우 업그레이드 사전 확인 중에 알림이 표시됩니다. 업그레이드를 진행하기 전에 기술 지원 부서에 문의해야 합니다.

소프트웨어 업그레이드

업그레이드 빠른 시작

업그레이드를 시작하기 전에 일반 워크플로를 검토하십시오. StorageGRID 업그레이드 페이지에서는 각 업그레이드 단계를 안내합니다.

1 **Linux** 호스트를 준비합니다

StorageGRID 노드가 Linux 호스트에 배포된 경우 "각 호스트에 RPM 또는 DEB 패키지를 설치합니다"업그레이드를 시작하기 전에

2 업그레이드 및 핫픽스 파일을 업로드합니다

기본 관리 노드에서 StorageGRID 업그레이드 페이지에 액세스하고 필요한 경우 업그레이드 파일과 핫픽스 파일을 업로드합니다.

3 복구 패키지를 다운로드합니다

업그레이드를 시작하기 전에 현재 복구 패키지를 다운로드합니다.

4 업그레이드 사전 검사를 실행합니다

업그레이드 사전 검사는 문제를 감지하는 데 도움이 되므로 실제 업그레이드를 시작하기 전에 문제를 해결할 수 있습니다.

5 업그레이드를 시작합니다

업그레이드를 시작하면 사전 검사가 다시 실행되고 기본 관리자 노드가 자동으로 업그레이드됩니다. 기본 관리자 노드가 업그레이드 중인 동안에는 그리드 관리자에 액세스할 수 없습니다. 감사 로그도 사용할 수 없습니다. 이 업그레이드에는 최대 30분이 소요될 수 있습니다.

6 복구 패키지를 다운로드합니다

기본 관리 노드를 업그레이드한 후 새 복구 패키지를 다운로드합니다.

7 노드 승인

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.

관련 정보

"업그레이드를 완료하는 데 걸리는 시간을 예상합니다"

Linux: 모든 호스트에 **RPM** 또는 **DEB** 패키지를 다운로드하고 설치합니다

Linux 호스트에 구축된 StorageGRID 노드가 있는 경우 업그레이드를 시작하기 전에 각 호스트에 RPM 또는 DEB 패키지를 추가로 다운로드하여 설치하십시오.

업그레이드, **Linux** 및 핫픽스 파일을 다운로드합니다

그리드 관리자에서 StorageGRID 업그레이드를 수행할 때 업그레이드 아카이브와 필요한 핫픽스를 첫 번째 단계로 다운로드하라는 메시지가 표시됩니다. 그러나 Linux 호스트를 업그레이드하기 위해 파일을 다운로드해야 하는 경우 필요한 모든 파일을 미리 다운로드하여 시간을 절약할 수 있습니다.

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. 주의/MustRead 알림이 나타나면 핫픽스 번호를 기록하고 확인란을 선택합니다.
5. 최종 사용자 사용권 계약(EULA)을 읽고 확인란을 선택한 다음 * Accept & Continue * 를 선택합니다.

   선택한 버전의 다운로드 페이지가 나타납니다. 이 페이지에는 세 개의 열이 있습니다.
6. 두 번째 열(* Upgrade StorageGRID*)에서 두 개의 파일을 다운로드합니다.
   - 최신 릴리스에 대한 업그레이드 아카이브(이 파일은 * VMware, SG1000 또는 SG100 기본 관리 노드 * 라는 섹션에 있음) 이 파일은 업그레이드를 수행할 때까지 필요하지 않지만 지금 다운로드하면 시간이 절약됩니다.
   - 또는 `.zip` 형식의 RPM 또는 DEB 아카이브입니다. `.tgz` `.zip`서비스 랩톱에서 Windows를 실행하는 경우

파일을 선택합니다.

- Red Hat Enterprise Linux+
  `StorageGRID-Webscale-version-RPM-uniqueID.zip`+
  `StorageGRID-Webscale-version-RPM-uniqueID.tgz`
- Ubuntu 또는 Debian+
  `StorageGRID-Webscale-version-DEB-uniqueID.zip`+
  `StorageGRID-Webscale-version-DEB-uniqueID.tgz`

7. 필요한 핫픽스로 인해 주의/MustRead 고지에 동의해야 하는 경우 핫픽스를 다운로드하십시오.
   a. 로 돌아갑니다 "NetApp 다운로드: StorageGRID".
   b. 드롭다운에서 핫픽스 번호를 선택합니다.
   c. 주의 통지 및 EULA에 다시 동의합니다.
   d. 핫픽스와 추가 정보를 다운로드하여 저장합니다.

      업그레이드를 시작할 때 StorageGRID 업그레이드 페이지에 핫픽스 파일을 업로드하라는 메시지가 표시됩니다.

모든 **Linux** 호스트에 아카이브를 설치합니다

StorageGRID 소프트웨어를 업그레이드하기 전에 다음 단계를 수행하십시오.

단계

1. 설치 파일에서 RPM 또는 DEB 패키지를 추출합니다.
2. 모든 Linux 호스트에 RPM 또는 DEB 패키지를 설치합니다.

   설치 지침은 StorageGRID 호스트 서비스 설치 단계를 참조하십시오.

   - "Red Hat Enterprise Linux: StorageGRID 호스트 서비스를 설치합니다"
   - "Ubuntu 또는 Debian: StorageGRID 호스트 서비스를 설치합니다"

   새 패키지는 추가 패키지로 설치됩니다.

이전 버전의 설치 아카이브를 제거합니다

Linux 호스트에서 공간을 확보하기 위해 더 이상 필요하지 않은 이전 버전의 StorageGRID에 대한 설치 아카이브를 제거할 수 있습니다.

단계

1. 이전 StorageGRID 설치 아카이브를 제거합니다.

Red Hat

1. 설치된 StorageGRID 패키지 목록을 캡처합니다 `dnf list | grep -i storagegrid`.

   예:

```
[root@rhel-example ~]# dnf list | grep -i storagegrid
StorageGRID-Webscale-Images-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Images-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Images-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Images-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
StorageGRID-Webscale-Service-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Service-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Service-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Service-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
[root@rhel-example ~]#
```

2. 이전 StorageGRID 패키지 제거: `dnf remove images-package service-package`

   > 현재 실행 중인 StorageGRID 버전 또는 업그레이드할 StorageGRID 버전에 대한 설치 보관을 제거하지 마십시오.

   표시되는 경고를 무시해도 됩니다. 새 StorageGRID 패키지를 설치할 때 교체된 파일을 말합니다.

   예:

```
[root@rhel-example ~]# dnf remove StorageGRID-Webscale-Images-11-6-
0.x86_64 StorageGRID-Webscale-Service-11-6-0.x86_64
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can
use subscription-manager to register.

Dependencies resolved.
================================================================================
========
```

```
Package            Architecture      Version           Repository
Size
================================================================================
========
Removing:
StorageGRID-Webscale-Images-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 2.7 G
StorageGRID-Webscale-Service-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 7.5 M

Transaction Summary
================================================================================
========
Remove 2 Packages

Freed space: 2.8 G
Is this ok [y/N]: y
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing: 1/1
  Running scriptlet: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
  Erasing: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv6.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv4.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui64.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui48.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/__init__.
pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/sets.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
```

```
packages/netapp/storagegrid/vendor/latest/netaddr/ip/rfc1924.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/nmap.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/iana.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/glob.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/fbsocket.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/ieee.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/core.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/subnet_spl
itter.pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/__init__.p
yc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/compat.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/__init__.pyc:
remove failed: No such file or directory

  Erasing: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64   2/2
  Verifying: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
  Verifying: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  2/2
Installed products updated.
```

```
Removed:
  StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64
  StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64

Complete!
[root@rhel-example ~]#
```

Ubuntu 및 Debian

1. 설치된 StorageGRID 패키지 목록을 캡처합니다. `dpkg -l | grep storagegrid`

   예:

```
root@debian-example:~# dpkg -l | grep storagegrid
ii  storagegrid-webscale-images-11-6-0  11.6.0-20220210.0232.8d56cfe
amd64 StorageGRID Webscale docker images for 11.6.0
ii  storagegrid-webscale-images-11-7-0  11.7.0-
20230424.2238.1a2cf8c.dev-signed amd64 StorageGRID Webscale docker
images for 11.7.0
ii  storagegrid-webscale-images-11-8-0  11.8.0-20240131.0139.e3e0c87
amd64 StorageGRID Webscale docker images for 11.8.0
ii  storagegrid-webscale-images-11-9-0  11.9.0-20240826.1753.4aeeb70
amd64 StorageGRID Webscale docker images for 11.9.0
ii  storagegrid-webscale-service-11-6-0 11.6.0-20220210.0232.8d56cfe
amd64 StorageGRID Webscale host services for 11.6.0
ii  storagegrid-webscale-service-11-7-0 11.7.0-20230424.2238.1a2cf8c
amd64 StorageGRID Webscale host services for 11.7.0
ii  storagegrid-webscale-service-11-8-0 11.8.0-20240131.0139.e3e0c87
amd64 StorageGRID Webscale host services for 11.8.0
ii  storagegrid-webscale-service-11-9-0 11.9.0-20240826.1753.4aeeb70
amd64 StorageGRID Webscale host services for 11.9.0
root@debian-example:~#
```

2. 이전 StorageGRID 패키지 제거: `dpkg -r images-package service-package`

   > 현재 실행 중인 StorageGRID 버전 또는 업그레이드할 StorageGRID 버전에 대한 설치 보관을 제거하지 마십시오.

   예:

```
root@debian-example:~# dpkg -r storagegrid-webscale-service-11-6-0
storagegrid-webscale-images-11-6-0
(Reading database ... 38190 files and directories currently
installed.)
Removing storagegrid-webscale-service-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
locale: Cannot set LC_CTYPE to default locale: No such file or
directory
locale: Cannot set LC_MESSAGES to default locale: No such file or
directory
locale: Cannot set LC_ALL to default locale: No such file or
directory
dpkg: warning: while removing storagegrid-webscale-service-11-6-0,
directory '/usr/lib/python2.7/dist-
packages/netapp/storagegrid/vendor/latest' not empty so not removed
Removing storagegrid-webscale-images-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
root@debian-example:~#
```

1. StorageGRID 컨테이너 이미지를 제거합니다.

Docker 를 참조하십시오

1. 설치된 컨테이너 이미지 목록을 캡처합니다. `docker images`

   예:

```
[root@docker-example ~]# docker images
REPOSITORY           TAG             IMAGE ID       CREATED
SIZE
storagegrid-11.9.0   Admin_Node      610f2595bcb4   2 days ago
2.77GB
storagegrid-11.9.0   Storage_Node    7f73d33eb880   2 days ago
2.65GB
storagegrid-11.9.0   API_Gateway     2f0bb79526e9   2 days ago
1.82GB
storagegrid-11.8.0   Storage_Node    7125480de71b   7 months ago
2.54GB
storagegrid-11.8.0   Admin_Node      404e9f1bd173   7 months ago
2.63GB
storagegrid-11.8.0   Archive_Node    c3294a29697c   7 months ago
2.39GB
storagegrid-11.8.0   API_Gateway     1f88f24b9098   7 months ago
1.74GB
storagegrid-11.7.0   Storage_Node    1655350eff6f   16 months ago
2.51GB
storagegrid-11.7.0   Admin_Node      872258dd0dc8   16 months ago
2.48GB
storagegrid-11.7.0   Archive_Node    121e7c8b6d3b   16 months ago
2.41GB
storagegrid-11.7.0   API_Gateway     5b7a26e382de   16 months ago
1.77GB
storagegrid-11.6.0   Admin_Node      ee39f71a73e1   2 years ago
2.38GB
storagegrid-11.6.0   Storage_Node    f5ef895dcad0   2 years ago
2.08GB
storagegrid-11.6.0   Archive_Node    5782de552db0   2 years ago
1.95GB
storagegrid-11.6.0   API_Gateway     cb480ed37eea   2 years ago
1.35GB
[root@docker-example ~]#
```

2. 이전 StorageGRID 버전의 컨테이너 이미지를 제거합니다. `docker rmi image id`

   현재 실행 중인 StorageGRID 버전 또는 업그레이드할 StorageGRID 버전에 대한 컨테이너 이미지를 제거하지 마십시오.

예:

```
[root@docker-example ~]# docker rmi cb480ed37eea
Untagged: storagegrid-11.6.0:API_Gateway
Deleted:
sha256:cb480ed37eea0ae9cf3522de1dadfbff0075010d89c1c0a2337a3178051dd
f02
Deleted:
sha256:5f269aabf15c32c1fe6f36329c304b6c6ecb563d973794b9b59e8e5ab8ccc
afa
Deleted:
sha256:47c2b2c295a77b312b8db69db58a02d8e09e929e121352bec713fa12dae66
bde
[root@docker-example ~]#
```

팟맨

1. 설치된 컨테이너 이미지 목록을 캡처합니다. `podman images`

   예:

```
[root@podman-example ~]# podman images
REPOSITORY                    TAG           IMAGE ID      CREATED
SIZE
localhost/storagegrid-11.8.0  Storage_Node  7125480de71b  7 months
ago   2.57 GB
localhost/storagegrid-11.8.0  Admin_Node    404e9f1bd173  7 months
ago   2.67 GB
localhost/storagegrid-11.8.0  Archive_Node  c3294a29697c  7 months
ago   2.42 GB
localhost/storagegrid-11.8.0  API_Gateway   1f88f24b9098  7 months
ago   1.77 GB
localhost/storagegrid-11.7.0  Storage_Node  1655350eff6f  16 months
ago  2.54 GB
localhost/storagegrid-11.7.0  Admin_Node    872258dd0dc8  16 months
ago  2.51 GB
localhost/storagegrid-11.7.0  Archive_Node  121e7c8b6d3b  16 months
ago  2.44 GB
localhost/storagegrid-11.7.0  API_Gateway   5b7a26e382de  16 months
ago  1.8 GB
localhost/storagegrid-11.6.0  Admin_Node    ee39f71a73e1  2 years
ago    2.42 GB
localhost/storagegrid-11.6.0  Storage_Node  f5ef895dcad0  2 years
ago    2.11 GB
localhost/storagegrid-11.6.0  Archive_Node  5782de552db0  2 years
ago    1.98 GB
localhost/storagegrid-11.6.0  API_Gateway   cb480ed37eea  2 years
ago    1.38 GB
[root@podman-example ~]#
```

2. 이전 StorageGRID 버전의 컨테이너 이미지를 제거합니다. `podman rmi image id`

> ⚠ 현재 실행 중인 StorageGRID 버전 또는 업그레이드할 StorageGRID 버전에 대한 컨테이너 이미지를 제거하지 마십시오.

예:

```
[root@podman-example ~]# podman rmi f5ef895dcad0
Untagged: localhost/storagegrid-11.6.0:Storage_Node
Deleted:
f5ef895dcad0d78d0fd21a07dd132d7c7f65f45d80ee7205a4d615494e44cbb7
[root@podman-example ~]#
```

StorageGRID 11.9로 업그레이드하고 해당 릴리즈에 대한 최신 핫픽스를 동시에 적용할 수 있습니다. StorageGRID 업그레이드 페이지에는 권장 업그레이드 경로와 올바른 다운로드 페이지로 직접 연결되는 링크가 제공됩니다.

시작하기 전에

모든 고려 사항을 검토하고 모든 계획 및 준비 단계를 완료했습니다.

StorageGRID 업그레이드 페이지에 액세스합니다

첫 번째 단계에서는 그리드 관리자의 StorageGRID 업그레이드 페이지에 액세스합니다.

단계

1. 을 사용하여 그리드 관리자에 "지원되는 웹 브라우저"로그인합니다.
2. 유지보수 * > * 시스템 * > * 소프트웨어 업데이트 * 를 선택합니다.
3. StorageGRID 업그레이드 타일에서 * 업그레이드 * 를 선택합니다.

파일을 선택합니다

StorageGRID 업그레이드 페이지의 업데이트 경로는 최신 StorageGRID 릴리스를 설치하기 위해 설치해야 하는 주요 버전(예: 11.9.0) 및 핫픽스(예: 11.9.0.1)를 나타냅니다. 권장 버전 및 핫픽스를 표시된 순서대로 설치해야 합니다.

> 업데이트 경로가 표시되지 않으면 브라우저에서 NetApp Support 사이트에 액세스할 수 없거나 AutoSupport 페이지의 * 소프트웨어 업데이트 확인 * 확인란(* 지원 * > * 툴 * > * AutoSupport * > * 설정 *)이 사용 안 함으로 설정될 수 있습니다.

단계

1. 파일 선택 * 단계의 경우 업데이트 경로를 검토하십시오.
2. 파일 다운로드 섹션에서 각 * 다운로드 * 링크를 선택하여 NetApp Support 사이트에서 필요한 파일을 다운로드합니다.

   업데이트 경로가 표시되지 않으면 로 "NetApp 다운로드: StorageGRID" 이동하여 새 버전이나 핫픽스를 사용할 수 있는지 확인하고 필요한 파일을 다운로드합니다.

   > 모든 Linux 호스트에 RPM 또는 DEB 패키지를 다운로드하여 설치해야 하는 경우, 업데이트 경로에 이미 StorageGRID 업그레이드 및 핫픽스 파일이 나열되어 있을 수 있습니다.

3. 찾아보기 * 를 선택하여 버전 업그레이드 파일을 StorageGRID에 업로드합니다.
   `NetApp_StorageGRID_11.9.0_Software_uniqueID.upgrade`

   업로드 및 확인 프로세스가 완료되면 파일 이름 옆에 녹색 확인 표시가 나타납니다.

4. 핫픽스 파일을 다운로드한 경우 * 찾아보기 * 를 선택하여 해당 파일을 업로드합니다. 핫픽스는 버전 업그레이드의 일부로 자동으로 적용됩니다.
5. Continue * 를 선택합니다.

사전 점검을 실행합니다

사전 점검을 실행하면 그리드 업그레이드를 시작하기 전에 업그레이드 문제를 감지하고 해결할 수 있습니다.

단계

1. 사전 점검 * 실행 단계에서는 그리드에 대한 프로비저닝 암호를 입력하여 시작합니다.
2. 복구 패키지 다운로드 * 를 선택합니다.

   기본 관리 노드를 업그레이드하기 전에 복구 패키지 파일의 현재 복사본을 다운로드해야 합니다. 복구 패키지 파일을 사용하면 오류가 발생할 경우 시스템을 복원할 수 있습니다.

3. 파일이 다운로드되면 파일을 포함한 콘텐츠에 액세스할 수 있는지 `Passwords.txt` 확인합니다.
4. 다운로드한 파일 복사(`.zip`)를 안전하고 안전한 두 개의 별도 위치에 복사합니다.

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

5. 사전 점검 실행 * 을 선택하고 사전 점검을 완료할 때까지 기다립니다.
6. 보고된 각 사전 점검에 대한 세부 정보를 검토하고 보고된 오류를 해결합니다. StorageGRID 11.9 릴리즈의 경우 를 "StorageGRID 소프트웨어 업그레이드 해결 가이드" 참조하십시오.

   시스템을 업그레이드하기 전에 모든 precheck_errors_를 해결해야 합니다. 그러나 업그레이드하기 전에 precheck_warnings_를 처리할 필요는 없습니다.

   사용자 지정 방화벽 포트를 연 경우 사전 검사 확인 중에 알림을 받습니다. 업그레이드를 진행하기 전에 기술 지원 부서에 문의해야 합니다.

7. 보고된 문제를 해결하기 위해 구성을 변경한 경우 * 사전 점검 실행 * 을 다시 선택하여 업데이트된 결과를 확인하십시오.

   모든 오류가 해결되면 업그레이드를 시작하라는 메시지가 표시됩니다.

업그레이드를 시작하고 기본 관리 노드를 업그레이드합니다

업그레이드를 시작하면 업그레이드 사전 점검을 다시 실행하고 기본 관리 노드가 자동으로 업그레이드됩니다. 업그레이드 시 이 작업은 최대 30분이 소요될 수 있습니다.

기본 관리 노드를 업그레이드하는 동안에는 다른 그리드 관리자 페이지에 액세스할 수 없습니다. 감사 로그도 사용할 수 없습니다.

단계

1. 업그레이드 시작 * 을 선택합니다.

   그리드 관리자에 대한 액세스 권한을 일시적으로 상실함을 알리는 경고가 나타납니다.

2. 경고를 확인하고 업그레이드를 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.

그리드에 온라인 상태가 되고 준비된 다른 관리 노드가 있는 경우 이를 사용하여 기본 관리 노드의 상태를 모니터링할 수 있습니다. 운영 관리자 노드가 업그레이드되는 즉시 다른 그리드 노드를 승인할 수 있습니다.

4. 필요에 따라 * 다른 노드 업그레이드 * 단계에 액세스하려면 * 계속 * 을 선택하십시오.

다른 노드를 업그레이드합니다

모든 그리드 노드를 업그레이드해야 하지만 여러 업그레이드 세션을 수행하고 업그레이드 시퀀스를 사용자 지정할 수 있습니다. 예를 들어, 한 세션에서 사이트 A의 노드를 업그레이드한 다음 이후 세션에서 사이트 B의 노드를 업그레이드할 수 있습니다. 둘 이상의 세션에서 업그레이드를 수행하도록 선택한 경우 모든 노드가 업그레이드될 때까지 새 기능을 사용할 수 없습니다.

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.

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.

단계

1. 다른 노드 업그레이드 * 단계에서는 전체 업그레이드를 위한 시작 시간과 각 주요 업그레이드 작업의 상태를 제공하는 요약을 검토하십시오.
   - * 업그레이드 서비스 시작 * 은 첫 번째 업그레이드 작업입니다. 이 작업 중에 소프트웨어 파일이 그리드 노드로 배포되고 각 노드에서 업그레이드 서비스가 시작됩니다.
   - 업그레이드 서비스 시작 * 작업이 완료되면 * 다른 그리드 노드 업그레이드 * 작업이 시작되고 복구 패키지의 새 복사본을 다운로드하라는 메시지가 표시됩니다.
2. 메시지가 표시되면 프로비저닝 암호를 입력하고 복구 패키지의 새 복사본을 다운로드합니다.

   기본 관리 노드를 업그레이드한 후 복구 패키지 파일의 새 복사본을 다운로드해야 합니다. 복구 패키지 파일을 사용하면 오류가 발생할 경우 시스템을 복원할 수 있습니다.

3. 각 노드 유형에 대한 상태 테이블을 검토합니다. 비기본 관리 노드, 게이트웨이 노드 및 스토리지 노드에 대한 테이블이 있습니다.

   그리드 노드는 테이블이 처음 나타날 때 다음 단계 중 하나일 수 있습니다.

   - 업그레이드 포장 풀기
   - 다운로드 중입니다
   - 승인을 기다리는 중입니다
4. 업그레이드할 그리드 노드를 선택할 준비가 되었을 때(또는 선택한 노드의 승인을 취소할 필요가 있는 경우) 다음 지침을 따르십시오.

작업	지침
특정 사이트의 모든 노드와 같이 승인할 특정 노드를 검색합니다	검색 문자열을 * 검색 * 필드에 입력합니다
업그레이드할 모든 노드를 선택합니다	Approve all nodes * 를 선택합니다
업그레이드할 유형이 동일한 모든 노드(예: 모든 스토리지 노드)를 선택합니다.	노드 유형에 대해 * Approve All * (모두 승인) 버튼을 선택합니다 동일한 유형의 노드를 두 개 이상 승인하는 경우 노드는 한 번에 하나씩 업그레이드됩니다.
업그레이드할 개별 노드를 선택합니다	노드에 대해 * Approve * (승인 *) 버튼을 선택합니다
선택한 모든 노드에서 업그레이드를 연기합니다	모든 노드 * 승인 취소 를 선택합니다
같은 유형의 선택한 모든 노드에서 업그레이드를 연기합니다	노드 유형에 대해 * Unap증전 * 버튼을 선택합니다
개별 노드의 업그레이드를 연기합니다	노드에 대해 * Unap증정하기 * 버튼을 선택합니다

5. 승인된 노드가 다음 업그레이드 단계를 진행할 때까지 기다립니다.
   - 승인되어 업그레이드 대기 중입니다
   - 서비스를 중지하는 중입니다

     스테이지가 * 서비스 중지 * 에 도달하면 노드를 제거할 수 없습니다. Unap증서 * 버튼이 비활성화됩니다.

   - 컨테이너를 중지하는 중입니다
   - Docker 이미지를 정리하는 중입니다
   - 기본 OS 패키지를 업그레이드 중입니다

     어플라이언스 노드가 이 단계에 도달하면 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램 소프트웨어가 업데이트됩니다. 이러한 자동 프로세스를 통해 StorageGRID 어플라이언스 설치 프로그램 버전이 StorageGRID 소프트웨어 버전과 동기화된 상태로 유지됩니다.

   - 재부팅 중입니다

     펌웨어 및 BIOS를 업그레이드하기 위해 일부 어플라이언스 모델이 여러 번 재부팅될 수 있습니다.

   - 재부팅 후 단계 수행
   - 서비스를 시작하는 중입니다

◦ 완료

6. 모든 그리드 노드가 업그레이드될 때까지 필요한 만큼 를 승인 단계반복합니다.

업그레이드를 완료합니다

모든 그리드 노드가 업그레이드 단계를 완료하면 * 다른 그리드 노드 업그레이드 * 작업이 완료된 것으로 표시됩니다. 나머지 업그레이드 작업은 백그라운드에서 자동으로 수행됩니다.

단계

1. 기능 활성화 * 작업이 완료되면(빠르게 발생) 업그레이드된 StorageGRID 버전에서 를 사용할 수 있습니다"새로운 기능".
2. 업그레이드 데이터베이스 * 작업 중에 업그레이드 프로세스에서는 각 노드를 검사하여 Cassandra 데이터베이스를 업데이트할 필요가 없는지 확인합니다.

> StorageGRID 11.8에서 11.9로 업그레이드할 때는 Cassandra 데이터베이스를 업그레이드할 필요가 없습니다. 하지만 Cassandra 서비스는 각 스토리지 노드에서 중지했다가 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 * 가 완료될 때까지 몇 분 정도 기다립니다.
4. 최종 업그레이드 단계 * 가 완료되면 업그레이드가 완료됩니다. 첫 번째 단계인 * 파일 선택 * 이 녹색 성공 배너와 함께 다시 표시됩니다.
5. 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

업그레이드를 수행할 때 문제가 발생하면 직접 문제를 해결할 수 있습니다. 문제를 해결할 수 없는 경우 최대한 많은 정보를 수집한 다음 기술 지원 팀에 문의하십시오.

업그레이드가 완료되지 않습니다

다음 섹션에서는 업그레이드가 부분적으로 실패한 상황에서 복구하는 방법에 대해 설명합니다.

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.

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 문제

업그레이드 도중 또는 이후에 Grid Manager 또는 테넌트 관리자에 문제가 발생할 수 있습니다.

그리드 관리자는 업그레이드 중에 여러 오류 메시지를 표시합니다

기본 관리자 노드가 업그레이드되는 동안 브라우저를 새로 고치거나 다른 그리드 관리자 페이지로 이동하는 경우 "503: 서비스를 사용할 수 없음" 및 "서버에 연결하는 데 문제가 있음" 메시지가 여러 개 표시될 수 있습니다. 이러한 메시지는 무시해도 됩니다. 노드가 업그레이드되는 즉시 표시되지 않습니다.

업그레이드를 시작한 후 한 시간 이상 이러한 메시지가 나타나면 기본 관리 노드를 업그레이드하지 못하게 하는 문제가 발생한 것일 수 있습니다. 직접 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

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 "지원되는 웹 브라우저"확인합니다.

  > 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 확인**"** 오류 메시지

업그레이드 프로세스를 시작하려고 할 때 "다음 문제가 Docker 이미지 가용성 검사 유효성 검사 제품군으로 식별되었습니다."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 파일이 {file_path} 예상 형식과 일치하지 않습니다.	업그레이드 패키지가 손상되었습니다.	업그레이드 패키지를 다시 업로드하고 다시 시도하십시오. 문제가 지속되면 기술 지원 팀에 문의하십시오.
업그레이드 버전 정보 파일을 {file_path} 찾을 수 없습니다. 업그레이드 버전을 확인할 수 없습니다.	업그레이드 패키지가 손상되었습니다.	업그레이드 패키지를 다시 업로드하고 다시 시도하십시오. 문제가 지속되면 기술 지원 팀에 문의하십시오.
에서 현재 설치된 릴리스 버전을 확인할 수 {node_name} 없습니다.	노드의 중요 파일이 손상되었습니다.	기술 지원 부서에 문의하십시오.
에서 버전을 나열하려는 중 연결 오류가 발생했습니다 {node_name}	노드가 오프라인이거나 연결이 끊어졌습니다.	모든 노드가 온라인 상태이고 운영 관리 노드에서 연결할 수 있는지 확인한 후 다시 시도하십시오.
노드의 호스트에 {node_name} StorageGRID 이미지가 로드되어 있지 {upgrade_version} 않습니다. 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 "Linux: 모든 호스트에 RPM 또는 DEB 패키지를 설치합니다 "참조하십시오.
노드를 확인하는 동안 오류가 발생했습니다 {node_name}	예기치 않은 오류가 발생했습니다.	몇 분 정도 기다린 후 다시 시도하십시오.
사전 점검 실행 중 오류가 발생했습니다. {error_string}	예기치 않은 오류가 발생했습니다.	몇 분 정도 기다린 후 다시 시도하십시오.

StorageGRID 핫픽스를 적용합니다

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

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. "GRID 버전"은 11._A.B. y_입니다.
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.

자세한 내용은 을 "대체 운영 관리자 노드를 구성합니다"참조하십시오.

핫픽스를 적용할 때 시스템이 영향을 받는 방식

핫픽스를 적용할 때 StorageGRID 시스템이 어떤 영향을 받는지 알아야 합니다.

StorageGRID 핫픽스는 무중단으로 운영됩니다

StorageGRID 시스템은 핫픽스 프로세스 전반에 걸쳐 클라이언트 응용 프로그램에서 데이터를 수집하고 검색할 수 있습니다. 같은 유형의 모든 노드를 핫픽스로 승인하면(예: 스토리지 노드) 노드가 한 번에 하나씩 다운되므로 모든

그리드 노드 또는 특정 유형의 모든 그리드 노드를 사용할 수 없는 시간이 없습니다.

지속적인 가용성을 보장하기 위해 ILM 정책에 각 개체의 여러 복사본을 저장하도록 지정하는 규칙이 포함되어 있는지 확인합니다. 또한 모든 외부 S3 클라이언트가 다음 중 하나로 요청을 보내도록 구성되었는지 확인해야 합니다.

- 고가용성(HA) 그룹 가상 IP 주소입니다
- 고가용성 타사 로드 밸런서
- 각 클라이언트에 대해 여러 게이트웨이 노드가 있습니다
- 각 클라이언트에 대해 여러 스토리지 노드

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 "고가용성 그룹 구성"참조하십시오.

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.

항목	참고
• 네트워크 포트 • "지원되는 웹 브라우저" • SSH 클라이언트(예: PuTTY)	
복구 패키지(`.zip`) 파일입니다	핫픽스를 적용하기 전에 "최신 복구 패키지 파일을 다운로드합니다"핫픽스 중에 문제가 발생할 경우 그런 다음 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. 이 `Passwords.txt` 파일은 복구 패키지 파일의 `.zip` 일부입니다.
프로비저닝 암호	StorageGRID 시스템을 처음 설치할 때 암호가 생성되고 문서화됩니다. 프로비저닝 암호가 파일에 나열되지 `Passwords.txt` 않습니다.
관련 문서	`readme.txt` 핫픽스에 대한 파일입니다. 이 파일은 핫픽스 다운로드 페이지에 포함되어 있습니다. `readme`핫픽스를 적용하기 전에 파일을 주의 깊게 검토하십시오.

핫픽스 파일을 다운로드합니다

핫픽스를 적용하려면 먼저 핫픽스 파일을 다운로드해야 합니다.

단계

1. 로 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.

   ⓘ 핫픽스를 적용해야 하는 경우 "기본 관리자 노드를 복구했습니다"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 사항의 요약을 봅니다.

4. 핫픽스의 다운로드 버튼을 선택하고 파일을 저장합니다.

   이 파일의 이름을 변경하지 마십시오.

   macOS 장치를 사용하는 경우 핫픽스 파일이 자동으로 파일로 저장될 수 `.txt` 있습니다. 이 경우 확장자 없이 파일 이름을 변경해야 `.txt` 합니다.

5. 다운로드할 위치를 선택하고 * 저장 * 을 선택합니다.

핫픽스를 적용하기 전에 시스템 상태를 확인하십시오

핫픽스가 시스템에 적용되었는지 확인해야 합니다.

1. 을 사용하여 그리드 관리자에 "지원되는 웹 브라우저"로그인합니다.
2. 가능한 경우 시스템이 정상적으로 실행되고 있고 모든 그리드 노드가 그리드에 연결되어 있는지 확인합니다.

   연결된 노드의 노드 페이지에는 녹색 체크 표시가 있습니다.

3. 가능한 경우 현재 경고를 확인하고 해결합니다.
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.

   노드나 사이트의 경우 "서비스 해제 절차가 일시 중지되었습니다"핫픽스를 안전하게 적용할 수 있습니다. 또한 StorageGRID 업그레이드 절차의 마지막 단계에서 핫픽스를 적용할 수도 있습니다. 의 지침을 "StorageGRID 소프트웨어 업그레이드 중"참조하십시오.

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.

시작하기 전에

- 를 검토했습니다."핫픽스 적용 시 고려 사항"
- 프로비저닝 암호가 있습니다.
- 루트 액세스 또는 유지 관리 권한이 있습니다.

이 작업에 대해

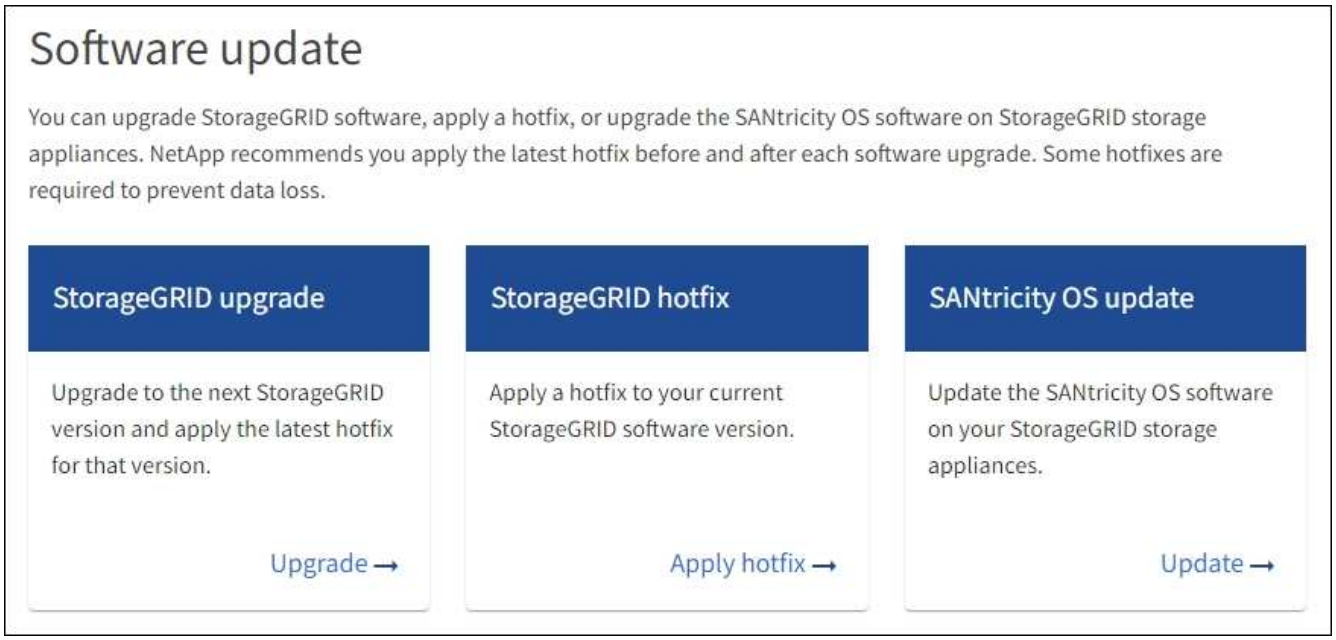
- 노드에 핫픽스 적용을 지연할 수 있지만 모든 노드에 핫픽스를 적용할 때까지 핫픽스 프로세스는 완료되지 않습니다.

- 핫픽스 프로세스를 완료할 때까지 StorageGRID 소프트웨어 업그레이드 또는 SANtricity OS 업데이트를 수행할 수 없습니다.

단계

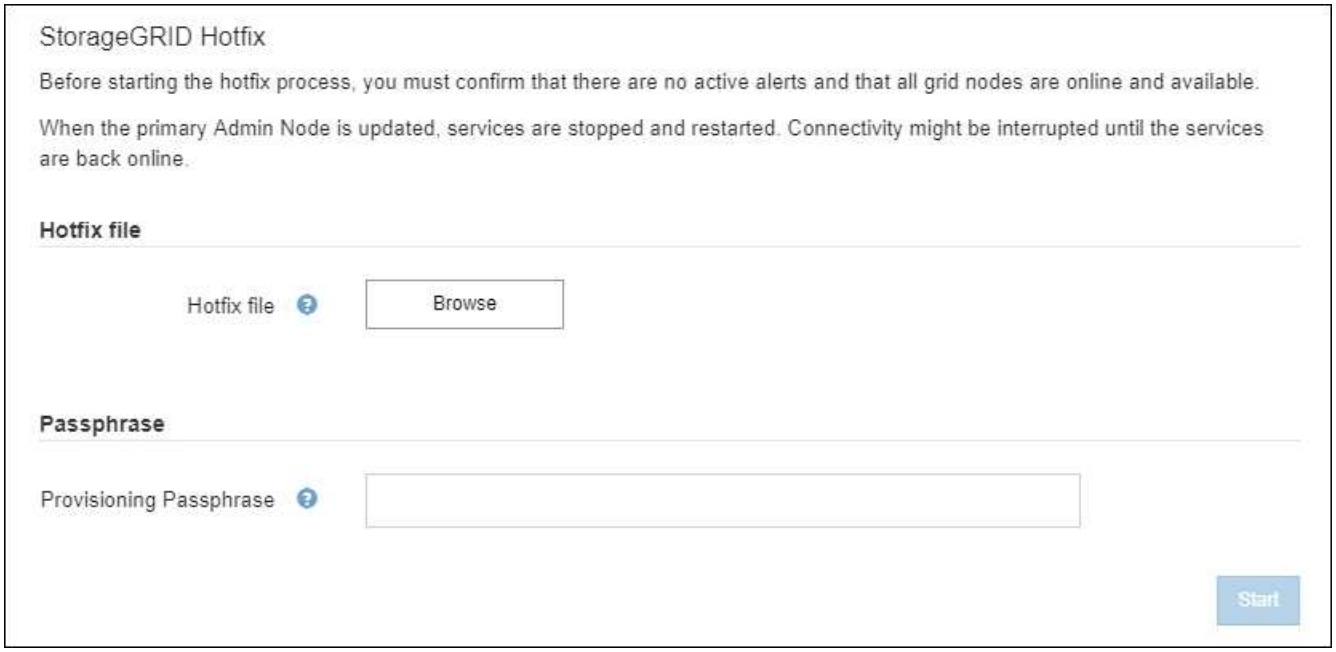
1. 을 사용하여 그리드 관리자에 "지원되는 웹 브라우저"로그인합니다.
2. 유지보수 * > * 시스템 * > * 소프트웨어 업데이트 * 를 선택합니다.

   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:

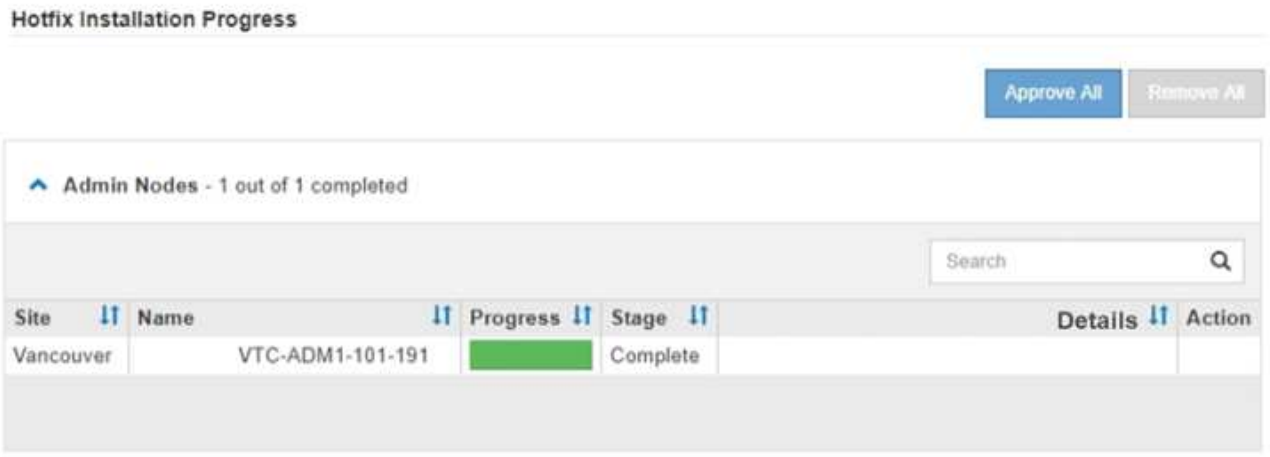
a. 핫픽스 검증이 실행됩니다.

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 유형(관리 노드, 게이트웨이 노드 및 스토리지 노드)별로 그룹화됩니다.

c. 진행률 표시줄이 완료에 도달하면 기본 관리자 노드가 "완료"로 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 확실하지 않은 경우 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.

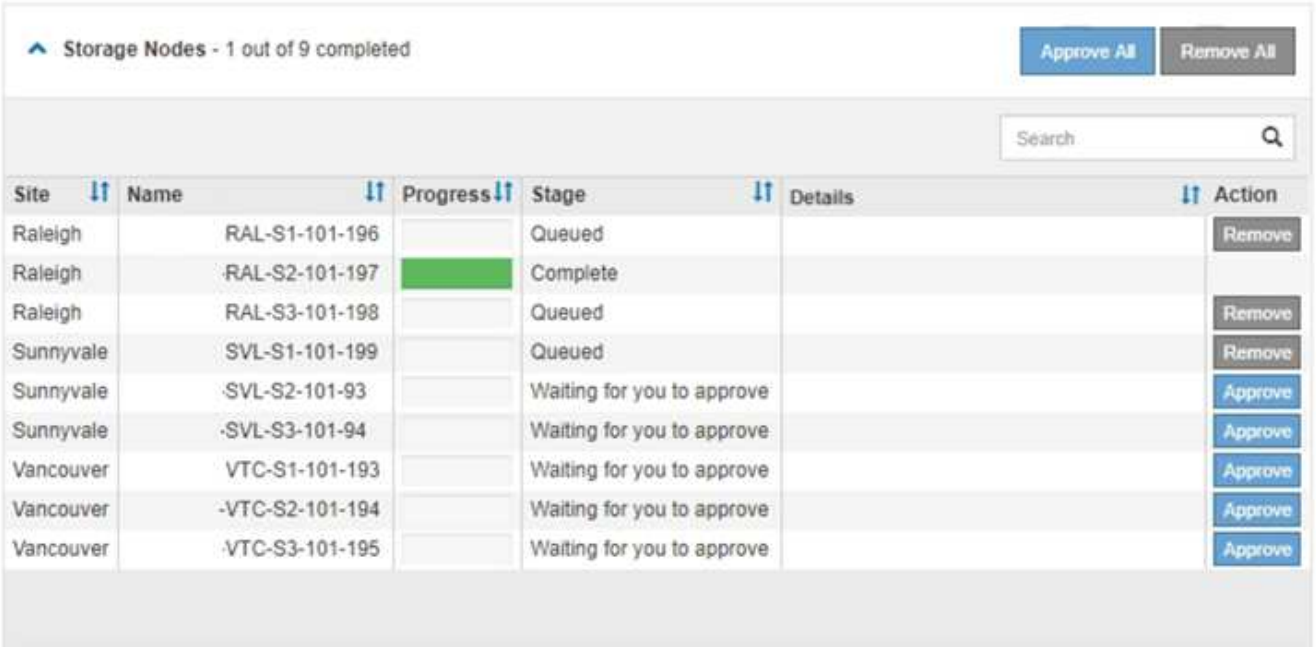
     페이지 상단의 * Approve All * (모두 승인) 버튼을 클릭하면 페이지에 나열된 모든 노드가 승인되고, 테이블 그룹 상단의 * Approve All * (모두 승인) 버튼을 누르면 해당 그룹의 모든 노드만 승인됩니다. 노드 업그레이드 순서가 중요한 경우 노드 또는 노드 그룹을 한 번에 하나씩 승인하고 다음 노드를 승인하기 전에 각 노드에서 업그레이드가 완료될 때까지 기다립니다.

   - 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"을 넘으면 * Remove * 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.

StorageGRID 시스템을 구성하고 관리합니다

StorageGRID 관리

StorageGRID 관리

다음 지침에 따라 StorageGRID 시스템을 구성하고 관리합니다.

참조하십시오

StorageGRID 구성 및 관리를 위한 기본 작업을 통해 다음을 수행할 수 있습니다.

- 그리드 관리자를 사용하여 그룹 및 사용자를 설정합니다
- S3 클라이언트 애플리케이션이 오브젝트를 저장하고 검색할 수 있도록 테넌트 계정을 생성합니다
- StorageGRID 네트워크를 구성하고 관리합니다
- AutoSupport를 구성합니다
- 노드 설정을 관리합니다

시작하기 전에

- StorageGRID 시스템에 대해 전반적으로 이해하고 있습니다.
- Linux 명령 셸, 네트워킹 및 서버 하드웨어 설정 및 구성에 대한 매우 상세한 지식을 보유하고 있습니다.

Grid Manager를 시작합니다

웹 브라우저 요구 사항

지원되는 웹 브라우저를 사용해야 합니다.

웹 브라우저	최소 지원 버전
Google Chrome	119
Microsoft Edge를 참조하십시오	119
Mozilla Firefox	119

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.

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 일부 유지 보수 절차는 기본 관리자 노드에서만 수행할 수 있습니다.

HA 그룹에 연결합니다

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. 을 "고가용성 그룹을 관리합니다"참조하십시오.

SSO를 사용합니다

의 경우 로그인 단계가 약간 "SSO(Single Sign-On)가 구성되었습니다"다릅니다.

첫 번째 관리 노드에서 그리드 관리자에 로그인합니다

시작하기 전에

- 로그인 자격 증명이 있습니다.
- 을 사용하고 "지원되는 웹 브라우저"있습니다.
- 쿠키는 웹 브라우저에서 활성화됩니다.
- 하나 이상의 권한이 있는 사용자 그룹에 속해 있습니다.
- Grid Manager에 대한 URL이 있습니다.

  `https://FQDN_or_Admin_Node_IP/`

  정규화된 도메인 이름, 관리 노드의 IP 주소 또는 관리 노드의 HA 그룹의 가상 IP 주소를 사용할 수 있습니다.

  HTTPS의 기본 포트(443)가 아닌 포트에서 Grid Manager에 액세스하려면 URL에 포트 번호를 포함시킵니다.

  `https://FQDN_or_Admin_Node_IP:port/`

  > ⓘ SSO는 제한된 Grid Manager 포트에서 사용할 수 없습니다. 포트 443을 사용해야 합니다.

단계

1. 지원되는 웹 브라우저를 실행합니다.
2. 브라우저의 주소 표시줄에 Grid Manager의 URL을 입력합니다.
3. 보안 경고 메시지가 나타나면 브라우저의 설치 마법사를 사용하여 인증서를 설치합니다. 을 "보안 인증서를 관리합니다"참조하십시오.
4. Grid Manager에 로그인합니다.

   표시되는 로그인 화면은 SSO(Single Sign-On)가 StorageGRID에 대해 구성되었는지 여부에 따라 달라집니다.

SSO를 사용하지 않습니다

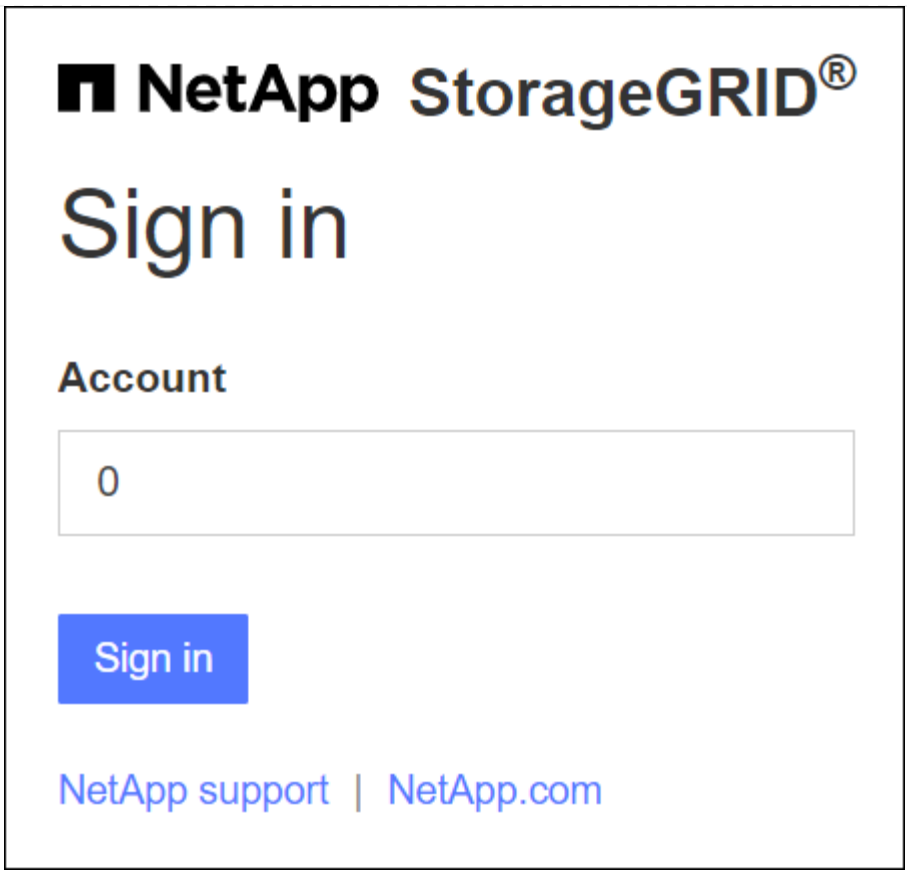
a. Grid Manager의 사용자 이름과 암호를 입력합니다.

b. 로그인 * 을 선택합니다.

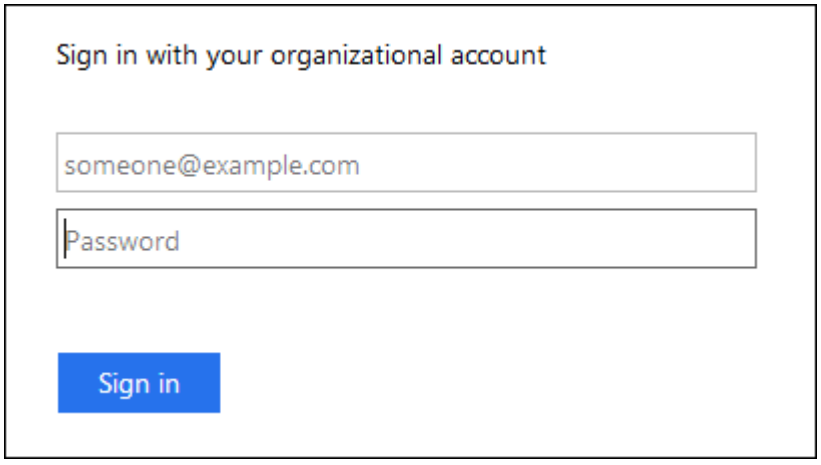
SSO 사용

◦ StorageGRID가 SSO를 사용하고 있고 이 브라우저에서 URL에 처음 액세스한 경우:

i. 로그인 * 을 선택합니다. 계정 필드에 0을 그대로 둘 수 있습니다.



ii. 조직의 SSO 로그인 페이지에 표준 SSO 자격 증명을 입력합니다. 예를 들면 다음과 같습니다.



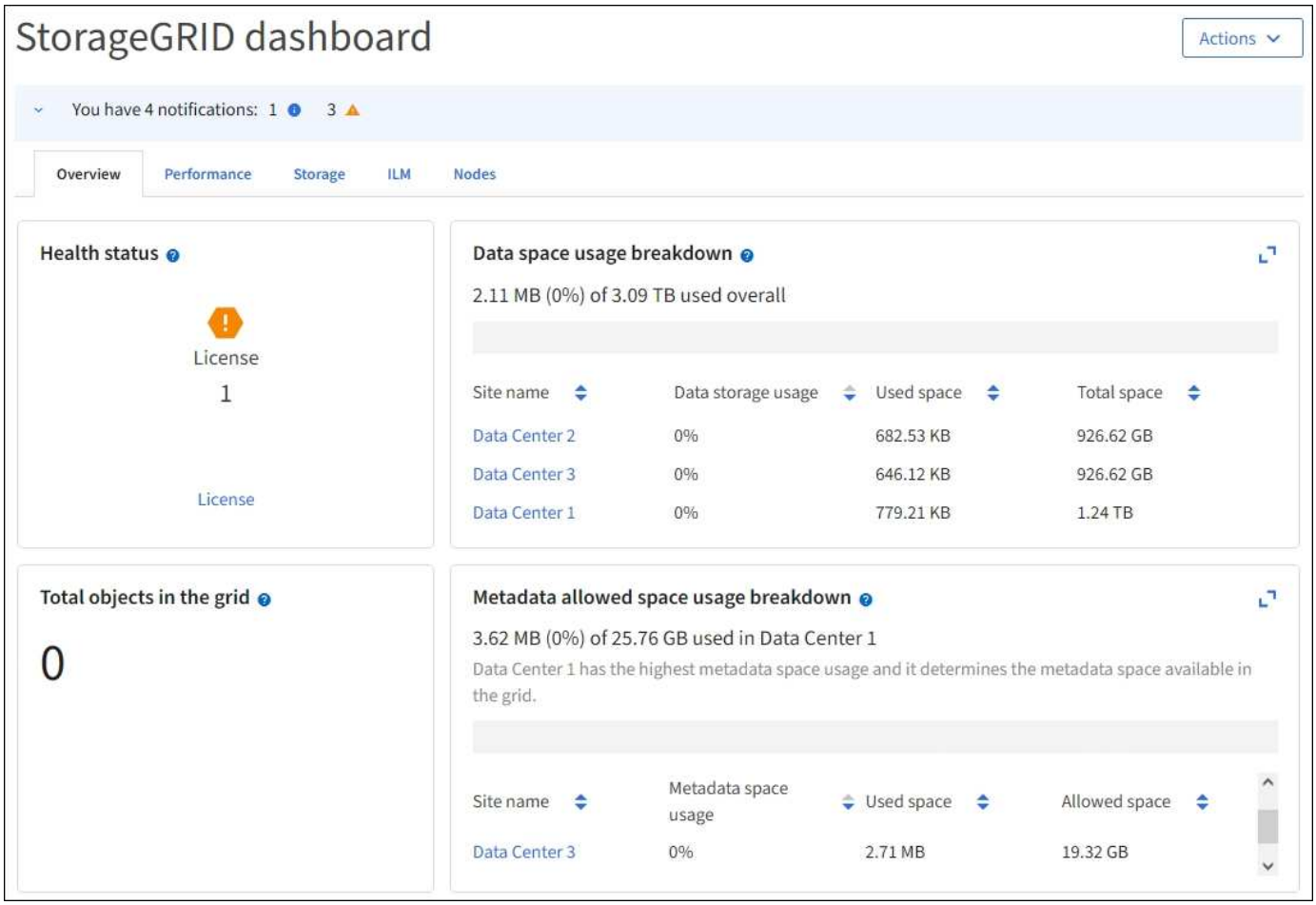
◦ StorageGRID가 SSO를 사용하고 있고 이전에 그리드 관리자 또는 테넌트 계정에 액세스한 경우:

i. 최신 계정 목록에 * 0 * (Grid Manager의 계정 ID)을 입력하거나 * Grid Manager * 를 선택합니다.

ii. 로그인 * 을 선택합니다.

iii. 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"대시보드를 보고 관리합니다".



다른 관리자 노드에 로그인합니다

다음 단계에 따라 다른 관리자 노드에 로그인합니다.

SSO를 사용하지 않습니다

단계

1. 브라우저의 주소 표시줄에 다른 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력합니다. 필요에 따라 포트 번호를 포함시킵니다.
2. Grid Manager의 사용자 이름과 암호를 입력합니다.
3. 로그인 * 을 선택합니다.

SSO 사용

StorageGRID가 SSO를 사용하고 있고 하나의 관리 노드에 로그인한 경우 다시 로그인하지 않고도 다른 관리 노드에 액세스할 수 있습니다.

단계

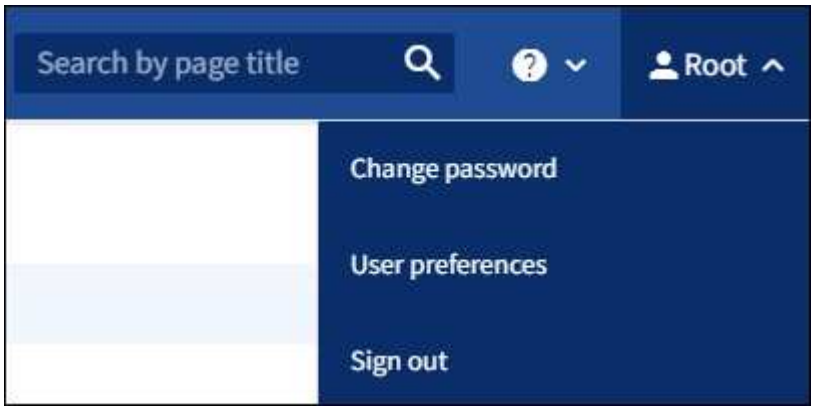
1. 브라우저의 주소 표시줄에 다른 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력합니다.
2. SSO 세션이 만료된 경우 자격 증명을 다시 입력하십시오.

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 Tenant Manager에도 로그인한 경우, 에도 로그인해야 "테넌트 계정에서 로그아웃합니다"합니다"SSO에서 로그아웃합니다".

암호를 변경합니다

Grid Manager의 로컬 사용자인 경우 사용자 고유의 암호를 변경할 수 있습니다.

시작하기 전에

을 사용하여 그리드 관리자에 로그인되어 있습니다."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.

StorageGRID 라이센스 정보를 봅니다

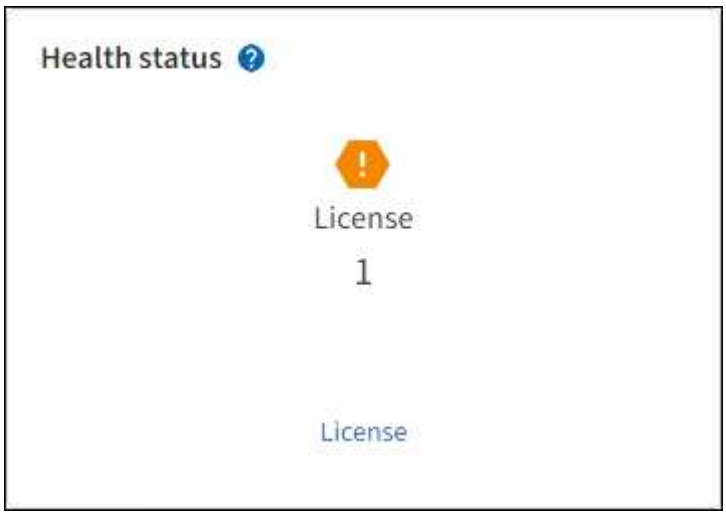
필요한 경우 그리드의 최대 스토리지 용량과 같은 StorageGRID 시스템에 대한 라이센스 정보를 볼 수 있습니다.

시작하기 전에

을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"

이 작업에 대해

이 StorageGRID 시스템의 소프트웨어 라이센스에 문제가 있는 경우 대시보드의 상태 카드에 라이센스 상태 아이콘과 * 라이센스 * 링크가 포함됩니다. 이 숫자는 라이센스 관련 문제의 수를 나타냅니다.



단계

1. 다음 중 하나를 수행하여 라이센스 페이지에 액세스합니다.
   - 유지 관리 * > * 시스템 * > * 라이센스 * 를 선택합니다.
   - 대시보드의 상태 카드에서 라이센스 상태 아이콘 또는 * 라이센스 * 링크를 선택합니다.

     이 링크는 라이센스에 문제가 있는 경우에만 나타납니다.

2. 현재 라이센스에 대한 읽기 전용 세부 정보 보기:

- StorageGRID 시스템 ID로, 이 StorageGRID 설치의 고유 식별 번호입니다
- 라이센스 일련 번호입니다
- 라이센스 유형, * 영구 * 또는 * 가입 *
- 그리드의 라이센스가 부여된 스토리지 용량입니다
- 지원되는 스토리지 용량입니다
- 라이선스 종료 날짜. 영구 라이센스에 대해 * 해당 없음 * 이 나타납니다.
- 지원 종료 날짜입니다

  이 날짜는 현재 라이센스 파일에서 읽으며 라이센스 파일을 얻은 후 지원 서비스 계약을 연장하거나 갱신한 경우 최신 날짜가 아닐 수 있습니다. 이 값을 업데이트하려면 을 참조하십시오"StorageGRID 라이센스 정보를 업데이트합니다". Active IQ를 사용하여 실제 계약 종료 날짜를 볼 수도 있습니다.

- 라이센스 텍스트 파일의 내용입니다

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.

시작하기 전에

- StorageGRID 시스템에 적용할 새 라이센스 파일이 있습니다.
- 있습니다. "특정 액세스 권한"
- 프로비저닝 암호가 있습니다.

단계

1. 유지 관리 * > * 시스템 * > * 라이센스 * 를 선택합니다.
2. 라이센스 업데이트 섹션에서 * 찾아보기 * 를 선택합니다.
3. 새 라이센스 파일을 찾아 (`.txt`선택합니다).

   새 라이센스 파일의 유효성을 검사한 후 표시합니다.

4. 프로비저닝 암호를 입력합니다.
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`: 액세스가 Grid Manager 사용자로 제한되며 구성된 그룹 권한을 기반으로 합니다.
- `/org`: 테넌트 계정에 대한 로컬 또는 페더레이션 LDAP 그룹에 속한 사용자로 액세스가 제한됩니다. 자세한 내용은 을 참조하십시오 "테넌트 계정을 사용합니다".
- `/private`: 액세스가 Grid Manager 사용자로 제한되며 구성된 그룹 권한을 기반으로 합니다. 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.

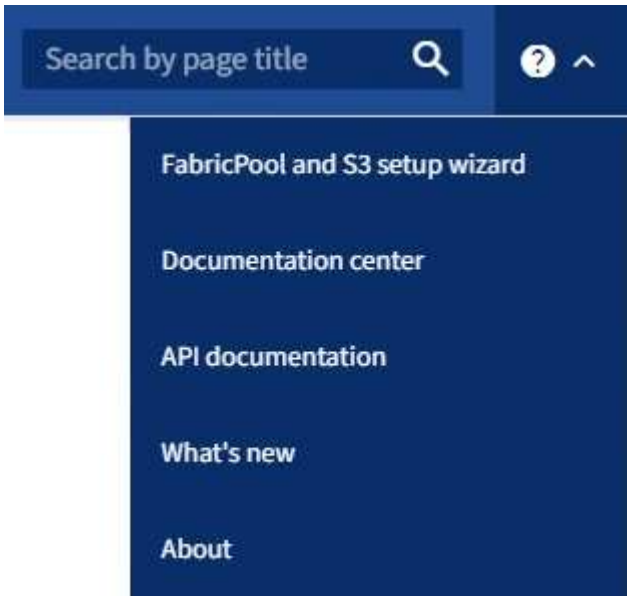
시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

> API 문서 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.



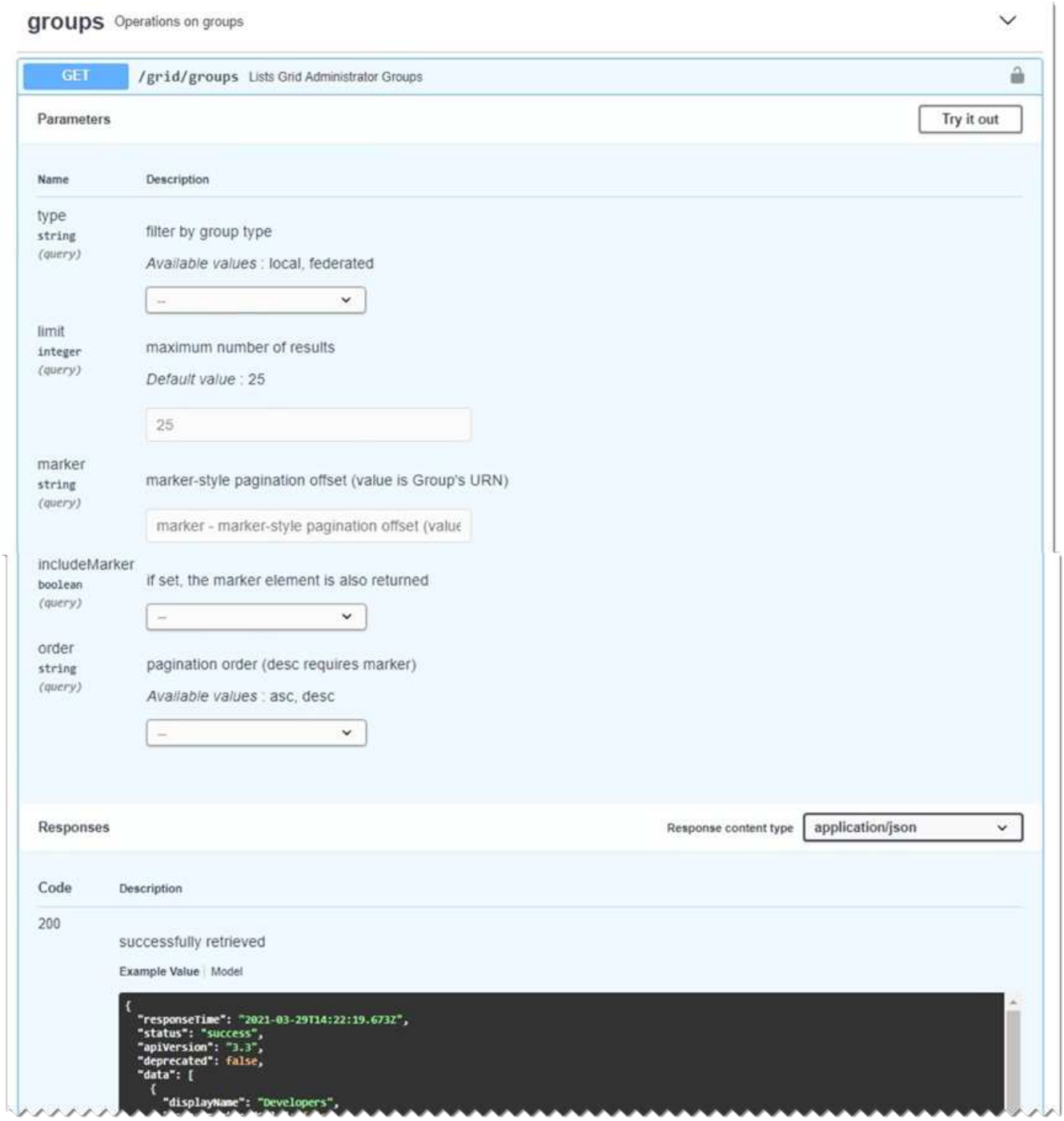
2. 전용 API로 작업을 수행하려면 StorageGRID 관리 API 페이지에서 * 전용 API 설명서 * 로 이동 * 을 선택합니다.

   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 API 작업

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.
- * alert-history *: 해결된 알림의 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 본문에 사용자 이름과 암호를 입력합니다(즉, `POST /api/v3/authorize`). 사용자가 성공적으로 인증되면 보안 토큰이 반환됩니다. 이 토큰은 후속 API 요청 헤더("Authorization:Bearer_token_")에 제공되어야 합니다. 토큰은 16시간 후에 만료됩니다.

  StorageGRID 시스템에 대해 Single Sign-On이 활성화된 경우 인증을 위해 다른 단계를 수행해야 합니다. "SSO(Single Sign-On)가 활성화된 경우 API에 로그인 인증"을 참조하십시오.

  인증 보안 강화에 대한 자세한 내용은 "사이트 간 요청 위조로부터 보호"를 참조하십시오.

- * 클라이언트-인증서 *: 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.
- * 비활성화됨 - 기능 *: 비활성화된 기능을 보기 위한 작업.
- * DNS-서버 *: 구성된 외부 DNS 서버를 나열하고 변경하는 작업.
- * 드라이브 세부 정보 *: 특정 스토리지 어플라이언스 모델을 위한 드라이브 작업.
- * endpoint-domain-names *: S3 끝점 도메인 이름을 나열하고 변경하는 작업.
- * 삭제 코딩 * : 삭제 코딩 프로필에 대한 작업.
- * 확장 *: 확장 작업(절차 수준).

- * 확장 노드 *: 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)의 운영
- **In-progress-procedures**: 현재 진행 중인 유지보수 절차를 검색합니다.
- 라이센스 *: StorageGRID 라이센스를 검색하고 업데이트하는 작업.
- **logs**: 로그 파일을 수집하고 다운로드하는 작업입니다
- * 메트릭 *: 일정 기간 동안 단일 시점 및 범위 메트릭 쿼리의 인스턴스 메트릭 쿼리를 비롯한 StorageGRID 메트릭의 작업 Grid Management API는 Prometheus 시스템 모니터링 도구를 백엔드 데이터 소스로 사용합니다. Prometheus 쿼리 구성에 대한 자세한 내용은 Prometheus 웹 사이트를 참조하십시오.

> 이름에 포함된 메트릭은 *private*내부용으로만 사용할 수 있습니다. 이러한 메트릭은 사전 통지 없이 StorageGRID 릴리스 간에 변경될 수 있습니다.

- * 노드 세부 정보 *: 노드 세부 정보에 대한 작업.
- * 노드 상태 *: 노드 상태에 대한 작업
- * 노드-스토리지-상태 *: 노드 스토리지 상태의 작업.
- * NTP-서버 *: 외부 NTP(Network Time Protocol) 서버를 나열하거나 업데이트하는 작업.
- * 오브젝트 *: 오브젝트 및 오브젝트 메타데이터의 작동
- * 복구 *: 복구 절차를 위한 작업.
- * recovery-package *: 복구 패키지를 다운로드하기 위한 작업.
- * 지역 *: 영역을 보고 만드는 작업.
- * S3 오브젝트 잠금 *: 글로벌 S3 오브젝트 잠금 설정 시 작업.
- * server-certificate *: Grid Manager 서버 인증서를 보고 업데이트하는 작업.
- * SNMP *: 현재 SNMP 구성에 대한 작업.
- * 스토리지 - 워터마크 *: 스토리지 노드 워터마크입니다.
- * 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 API 버전 4를 지정합니다.

`https://hostname_or_ip_address/api/v4/authorize`

이전 버전과 호환되지 않는 변경 사항이 발생하면 API의 주 버전이 범핑됩니다. API의 부 버전은 이전 버전과 _ 호환 _ 을(를) 변경할 때 범핑됩니다. 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 최신 버전의 API만 활성화됩니다. 그러나 StorageGRID의 새 기능 릴리즈로 업그레이드하면 하나 이상의 StorageGRID 기능 릴리즈에 대한 이전 API 버전에 계속 액세스할 수 있습니다.

> 지원되는 버전을 구성할 수 있습니다. 자세한 내용은 Swagger API 설명서의 * config * 섹션을 참조하십시오"Grid Management API를 참조하십시오". 최신 버전을 사용하려면 모든 API 클라이언트를 업데이트한 후 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 v2 API at POST "/api/v2/authorize"
```

현재 릴리즈에서 지원되는 **API** 버전을 확인합니다

API 요청을 사용하여 `GET /versions` 지원되는 API 주요 버전 목록을 반환합니다. 이 요청은 Swagger API 설명서의 * config * 섹션에 있습니다.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

요청에 대한 **API** 버전을 지정합니다

경로 매개 변수(`/api/v4`) 또는 헤더를 사용하여 API 버전을 지정할 수 (`Api-Version: 4`있습니다. 두 값을 모두 제공하면 헤더 값이 경로 값을 재정의합니다.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" 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 `csrfToken` 인증 중에 매개 변수를 로 `true` 설정합니다. 기본값은 입니다 `false`.

```
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"
```

true 인 경우, `GridCsrfToken` 쿠키는 Grid Manager 로그인에 대한 임의 값으로 설정되고 `AccountCsrfToken` 쿠키는 Tenant Manager에 로그인하기 위한 임의 값으로 설정됩니다.

쿠키가 있는 경우 시스템 상태(POST, PUT, 패치, 삭제)를 수정할 수 있는 모든 요청에 다음 중 하나가 포함되어야 합니다.

- `X-Csrf-Token`헤더 값이 CSRF 토큰 쿠키의 값으로 설정된 헤더입니다.
- 폼으로 인코딩된 본문을 수락하는 끝점의 경우: `csrfToken` 폼으로 인코딩된 요청 본문 매개 변수입니다.

추가 예제 및 세부 정보는 온라인 API 설명서를 참조하십시오.

CSRF 토큰 쿠키 세트가 있는 요청은 CSRF 공격에 대한 추가 보호로서 JSON 요청 본문을 기대하는 모든 요청에 대해 "Content-Type: application/json" 헤더를 적용합니다.

SSO(Single Sign-On)가 활성화된 경우 API 사용(Active Directory)

Active Directory가 있고 SSO 공급자로 사용하는 경우 "SSO(Single Sign-On) 구성 및 활성화"그리드 관리 API 또는 테넌트 관리 API에 유효한 인증 토큰을 얻기 위해 일련의 API 요청을 실행해야 합니다.

SSO(Single Sign-On)가 활성화된 경우 API에 로그인합니다

Active Directory를 SSO ID 공급자로 사용하는 경우 다음 지침이 적용됩니다.

시작하기 전에

- 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-ssoauth.py`Python 스크립트는 `Red Hat Enterprise Linux, `./debs` Ubuntu 또는 Debian 및 VMware용 `./vsphere` StorageGRID 설치 파일 디렉토리에 (`./rpms`있습니다.
- curl 요청의 워크플로 예

  컬을 너무 느리게 수행하면 컬링 작업 시간이 초과될 수 있습니다. 다음 오류가 표시될 수 있습니다 `A valid SubjectConfirmation was not found on this Response`.

  > 예제 curl 워크플로는 다른 사용자가 암호를 볼 수 없도록 보호하지 않습니다.

URL 인코딩 문제가 있는 경우 다음 오류가 표시될 수 있습니다 `Unsupported SAML version`.

단계

1. 인증 토큰을 얻으려면 다음 방법 중 하나를 선택합니다.
   - `storagegrid-ssoauth.py`Python 스크립트를 사용합니다. 2단계로 이동합니다.
   - curl 요청을 사용합니다. 3단계로 이동합니다.
2. 스크립트를 사용하려면 `storagegrid-ssoauth.py` 스크립트를 Python 인터프리터에 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'
```

   그리드 관리 API에 액세스하려면 0을 로 `TENANTACCOUNTID`사용합니다.

   b. 서명된 인증 URL을 수신하려면 에 POST 요청을 발행하고 `/api/v3/authorize-saml` 응답에서 추가 JSON 인코딩을 제거합니다.

   이 예제에서는 에 대해 서명된 인증 URL에 대한 POST 요청을 보여 `TENANTACCOUNTID` 줍니다. 결과는 에 전달되어 `python -m json.tool` 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://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 후속 명령에서 사용할 수 있도록 응답에서 를 `SAMLRequest` 저장합니다.

```
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. `MSISAuth`응답에서 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 를 저장합니다 `SAMLResponse`.

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 저장된 를 사용하여 `SAMLResponse` StorageGRID`/api/saml-response` 요청을 만들어 StorageGRID 인증 토큰을 생성합니다.

에서는 `RelayState` 테넌트 계정 ID를 사용하거나 그리드 관리 API에 로그인하려면 0을 사용합니다.

```
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 로 `MYTOKEN`저장합니다.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

이제 SSO를 사용하지 않는 경우 API를 사용하는 방법과 유사한 다른 요청에 를 사용할 수 `MYTOKEN` 있습니다.

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 로그아웃하여 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 "cookie "sso=true"를 SLO API에 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"가 제공되지 않으면 사용자는 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 No Content`사용자가 현재 로그아웃되었음을 나타내는 응답입니다.

```
HTTP/1.1 204 No Content
```

SSO(Single Sign-On)가 활성화된 경우 **API** 사용**(Azure)**

이 있고 Azure를 SSO 공급자로 사용하는 경우 "SSO(Single Sign-On) 구성 및 활성화"두 가지 예제 스크립트를 사용하여 그리드 관리 API 또는 테넌트 관리 API에 유효한 인증 토큰을 얻을 수 있습니다.

Azure Single Sign-On이 활성화된 경우 API에 로그인합니다

Azure를 SSO ID 공급자로 사용하는 경우 다음 지침이 적용됩니다

시작하기 전에

- 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.

- `storagegrid-ssoauth-azure.py`Python 스크립트
- `storagegrid-ssoauth-azure.js`Node.js 스크립트

두 스크립트 모두 Red Hat Enterprise Linux, `./debs` Ubuntu 또는 Debian 및 VMware용 `./vsphere` StorageGRID 설치 파일 디렉토리에 (`./rpms`있습니다.

Azure와 자체 API 통합을 작성하려면 스크립트를 참조하십시오 `storagegrid-ssoauth-azure.py`. 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 다음 오류가 표시될 수 있습니다 `Unsupported SAML version`.

단계

1. 다음과 같이 필요한 종속성을 설치합니다.
   a. Node.js를 설치합니다(참조 "https://nodejs.org/en/download/").
   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. 다른 형태의 MFA를 지원하도록 스크립트를 수정해야 할 수도 있습니다(예: 텍스트 메시지에 수신된 코드 입력).

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)

PingFederate를 SSO 공급자로 사용하는 경우"SSO(Single Sign-On) 구성 및 활성화", 그리드 관리 API 또는 테넌트 관리 API에 유효한 인증 토큰을 얻기 위해 일련의 API 요청을 실행해야 합니다.

SSO(Single Sign-On)가 활성화된 경우 API에 로그인합니다

이 지침은 PingFederate를 SSO ID 공급자로 사용하는 경우 적용됩니다

시작하기 전에

- 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-ssoauth.py`Python 스크립트는 `Red Hat Enterprise Linux, `./debs` Ubuntu 또는 Debian 및 VMware용 `./vsphere` StorageGRID 설치 파일 디렉토리에 (`./rpms`있습니다.
- curl 요청의 워크플로 예

  컬을 너무 느리게 수행하면 컬링 작업 시간이 초과될 수 있습니다. 다음 오류가 표시될 수 있습니다 `A valid SubjectConfirmation was not found on this Response`.

  예제 curl 워크플로는 다른 사용자가 암호를 볼 수 없도록 보호하지 않습니다.

  URL 인코딩 문제가 있는 경우 다음 오류가 표시될 수 있습니다 `Unsupported SAML version`.

단계

1. 인증 토큰을 얻으려면 다음 방법 중 하나를 선택합니다.
   - `storagegrid-ssoauth.py`Python 스크립트를 사용합니다. 2단계로 이동합니다.
   - curl 요청을 사용합니다. 3단계로 이동합니다.

2. 스크립트를 사용하려면 `storagegrid-ssoauth.py` 스크립트를 Python 인터프리터에 전달하고 스크립트를 실행합니다.

   프롬프트가 표시되면 다음 인수에 대한 값을 입력합니다.

   - SSO 방법 "pingfederate"(PINGFEDERATE, Pingfederate 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'
   ```

   그리드 관리 API에 액세스하려면 0을 로 `TENANTACCOUNTID`사용합니다.

   b. 서명된 인증 URL을 수신하려면 에 POST 요청을 발행하고 `/api/v3/authorize-saml` 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 명령에서 사용할 수 있도록 응답에서 를 `SAMLRequest` 저장합니다.

```
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 를 저장합니다 `SAMLResponse`.

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 저장된 를 사용하여 `SAMLResponse` StorageGRID`/api/saml-response` 요청을 만들어 StorageGRID 인증 토큰을 생성합니다.

에서는 `RelayState` 테넌트 계정 ID를 사용하거나 그리드 관리 API에 로그인하려면 0을 사용합니다.

```
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 로 `MYTOKEN`저장합니다.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

이제 SSO를 사용하지 않는 경우 API를 사용하는 방법과 유사한 다른 요청에 를 사용할 수 `MYTOKEN` 있습니다.

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. 이 지침은 PingFederate를 SSO ID 공급자로 사용하는 경우 적용됩니다

이 작업에 대해

필요한 경우 조직의 단일 로그아웃 페이지에서 로그아웃하여 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 "cookie "sso=true"를 SLO API에 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"가 제공되지 않으면 사용자는 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 No Content`사용자가 현재 로그아웃되었음을 나타내는 응답입니다.

```
HTTP/1.1 204 No Content
```

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 관리자에서 * 테넌트 루트 암호 변경 * 기능을 완전히 비활성화함으로써(UI 및 API 모두) 회사 A는 루트 사용자 및 * 루트 액세스 * 권한을 가진 그룹에 속한 사용자를 포함하여 관리자 사용자가 테넌트 계정의 루트 사용자에 대한 암호를 변경할 수 없도록 합니다

단계

1. Grid Management API에 대한 Swagger 문서에 액세스합니다. 을 "Grid Management API를 사용합니다 "참조하십시오.
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. 테넌트 루트 암호 변경 * 관리 권한이 더 이상 사용자 인터페이스에 표시되지 않으며 테넌트의 루트 암호를 변경하려고 시도하는 모든 API 요청이 "403 사용 권한 없음"과 함께 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 * 기능을 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 StorageAdmin 관리 권한을 계속 비활성화하려면 다음 PUT 요청을 보내십시오.

```
{ "grid": {"storageAdmin": true} }
```

StorageGRID에 대한 액세스를 제어합니다

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.

을 "ID 제휴" 사용하면 설정이 "그룹" "사용자"빨라지고 사용자가 친숙한 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 다른 작업을 할당하여 각 사용자가 수행할 수 있는 작업을 "권한"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. 그런 다음 "SSO를 구성하고 사용하도록 설정합니다"모든 사용자가 그리드 관리자, 테넌트 관리자, 그리드 관리 API 또는 테넌트 관리 API에 액세스하기 전에 외부 ID 공급자에 의해 인증되어야 합니다. 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

프로비저닝 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 할 수 "암호를 변경합니다"있습니다.

노드 콘솔 암호를 변경합니다

그리드의 각 노드에는 고유한 노드 콘솔 암호가 있습니다. 이 암호는 SSH를 사용하여 노드에 "admin"으로 로그인하거나 VM/물리적 콘솔 연결의 루트 사용자에게 로그인해야 합니다. 필요한 경우 각 노드에 대해 수행할 수 "노드 콘솔 암호를 변경합니다"있습니다.

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 현재 프로비저닝 암호가 있습니다.

이 작업에 대해

프로비저닝 암호는 많은 설치 및 유지 관리 절차 및 에 "복구 패키지 다운로드 중"필요합니다. 프로비저닝 암호가 파일에 나열되지 `Passwords.txt` 않습니다. 프로비저닝 암호를 문서화하고 안전한 장소에 보관해야 합니다.

단계

1. 구성 * > * 액세스 제어 * > * 그리드 비밀번호 * 를 선택합니다.
2. 프로비저닝 암호 변경 * 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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"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 프로세스는 그리드의 각 노드에 대한 새 암호를 만들고 복구 패키지의 업데이트된 파일에 암호를 `Passwords.txt` 저장합니다. 암호는 Passwords.txt 파일의 암호 열에 나열됩니다.

> 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 파일(`.zip`)을 안전하고 별도의 두 위치에 복사합니다.

> 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. 파일을 엽니다 `.zip`.

   b. 새 노드 콘솔 암호가 포함된 파일을 포함하여 콘텐츠에 액세스할 수 있는지 확인합니다 `Passwords.txt`.

   c. 새 복구 패키지 파일(`.zip`)을 안전하고 별도의 두 위치에 복사합니다.

   > 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 를 다운로드한 첫 번째 복구 패키지삭제합니다.
7. 필요에 따라 * 복구 패키지 * 링크를 사용하여 새 복구 패키지의 추가 복사본을 다운로드합니다.

관리 노드의 **SSH** 액세스 암호를 변경합니다

관리 노드의 SSH 액세스 암호를 변경하면 그리드의 각 노드에 대한 내부 SSH 키의 고유한 세트도 업데이트됩니다. 기본 관리자 노드는 이러한 SSH 키를 사용하여 보안 암호 없는 인증을 사용하여 노드에 액세스합니다.

SSH 키를 사용하여 노드에 `admin` 또는 VM 또는 물리적 콘솔 연결에서 루트 사용자로 로그인합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.
- 현재 프로비저닝 암호가 있습니다.

이 작업에 대해

관리 노드의 새 액세스 암호와 각 노드의 새 내부 키는 `Passwords.txt` 복구 패키지의 파일에 저장됩니다. 해당 파일의 암호 열에 키가 나열됩니다.

노드 간 통신에 사용되는 SSH 키에 대해 별도의 SSH 액세스 암호가 있습니다. 이 절차는 변경되지 않습니다.

마법사에 액세스합니다

단계

1. 구성 * > * 액세스 제어 * > * 그리드 비밀번호 * 를 선택합니다.
2. SSH 키 변경 * 아래에서 * 변경 * 을 선택합니다.

현재 복구 패키지를 다운로드합니다

SSH 액세스 키를 변경하기 전에 현재 복구 패키지를 다운로드합니다. 노드에 대해 키 변경 프로세스가 실패하면 이 파일에서 키를 사용할 수 있습니다.

단계

1. 그리드의 프로비저닝 암호를 입력합니다.
2. 복구 패키지 다운로드 * 를 선택합니다.
3. 복구 패키지 파일(`.zip`)을 안전하고 별도의 두 위치에 복사합니다.

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

4. Continue * 를 선택합니다.
5. 확인 대화 상자가 나타나면 SSH 액세스 키 변경을 시작할 준비가 되었으면 * Yes * 를 선택합니다.

   이 프로세스가 시작된 후에는 취소할 수 없습니다.

SSH 액세스 키를 변경합니다

SSH 액세스 키 변경 프로세스가 시작되면 새 키가 포함된 새 복구 패키지가 생성됩니다. 그런 다음 각 노드에서 키가 업데이트됩니다.

단계

1. 새 복구 패키지가 생성될 때까지 기다립니다. 몇 분 정도 걸릴 수 있습니다.
2. 새 복구 패키지 다운로드 버튼이 활성화되면 * 새 복구 패키지 다운로드 * 를 선택하고 새 복구 패키지 파일 저장(`.zip`)을 두 개의 안전한 위치에 각각 저장합니다.
3. 다운로드가 완료되면 다음을 수행합니다.

   a. 파일을 엽니다 `.zip`.

   b. 새 SSH 액세스 키가 포함된 파일을 포함하여 콘텐츠에 액세스할 수 있는지 확인합니다 `Passwords.txt`.

   c. 새 복구 패키지 파일(`.zip`)을 안전하고 별도의 두 위치에 복사합니다.

      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. 각 노드에서 키가 업데이트될 때까지 기다립니다. 몇 분 정도 걸릴 수 있습니다.

   모든 노드의 키를 변경하면 녹색 성공 배너가 나타납니다.

   업데이트 프로세스 중에 오류가 발생하면 배너 메시지에 키 변경에 실패한 노드 수가 나열됩니다. 시스템은 키 변경에 실패한 노드에서 프로세스를 자동으로 재시도합니다. 일부 노드에 변경 키가 없는 경우 * Retry *(재시도) 버튼이 나타납니다.

하나 이상의 노드에 대한 키 업데이트가 실패한 경우:

a. 표에 나열된 오류 메시지를 검토합니다.

b. 문제를 해결합니다.

c. 재시도 * 를 선택합니다.

다시 시도하면 이전 키 변경 시도 중에 장애가 발생한 노드에서 SSH 액세스 키만 변경됩니다.

5. 모든 노드의 SSH 액세스 키를 변경한 후 를 다운로드한 첫 번째 복구 패키지삭제합니다.
6. 필요한 경우 * 유지 관리 * > * 시스템 * > * 복구 패키지 * 를 선택하여 새 복구 패키지의 추가 복사본을 다운로드할 수 있습니다.

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"
- 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 OpenLDAP 서버 구성 지침참조하십시오.
- SSO(Single Sign-On)를 활성화하려는 경우 를 검토한 "SSO(Single Sign-On)에 대한 요구 사항 및 고려 사항 "것입니다.
- LDAP 서버와의 통신에 TLS(Transport Layer Security)를 사용하려는 경우 ID 공급자는 TLS 1.2 또는 1.3을 사용합니다. 을 "발신 TLS 연결에 지원되는 암호"참조하십시오.

이 작업에 대해

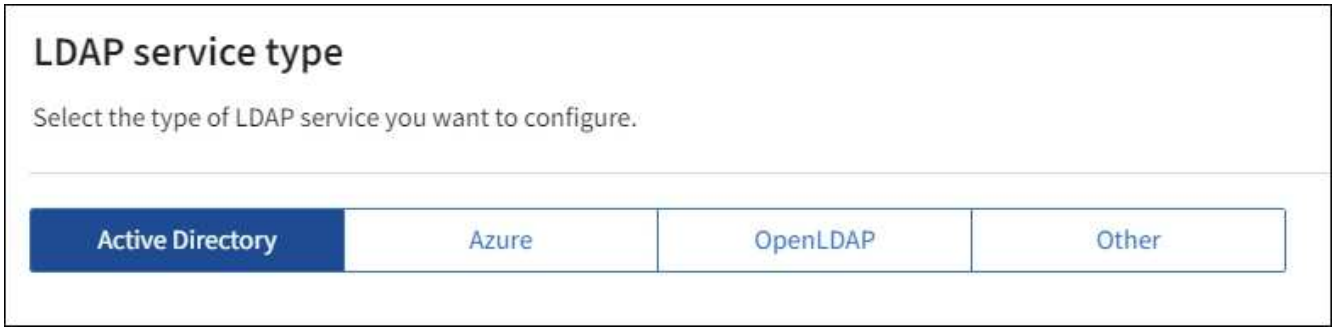
Active Directory, Azure AD, OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 그룹을 가져오려면 Grid Manager의 ID 소스를 구성할 수 있습니다. 다음 유형의 그룹을 가져올 수 있습니다.

- 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. 자세한 내용은 및 "테넌트 계정을 사용합니다"를 "테넌트 계정을 생성합니다"참조하십시오.

구성을 입력합니다

단계

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 Directory 및 OpenLDAP에 대해 `uid` 와 동일합니다 `sAMAccountName`. Oracle Directory Server를 구성하는 경우 를 입력합니다 `uid`.
   - * 사용자 UUID *: LDAP 사용자의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 Active Directory 및 OpenLDAP에 대해 `entryUUID` 와 동일합니다 `objectGUID`. Oracle Directory Server를 구성하는 경우 를 입력합니다 `nsuniqueid`. 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 Directory 및 OpenLDAP에 대해 `cn` 와 동일합니다 `sAMAccountName`. Oracle Directory Server를 구성하는 경우 를 입력합니다 `cn`.
   - * 그룹 UUID *: LDAP 그룹의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 Active Directory 및 OpenLDAP에 대해 `entryUUID` 와 동일합니다 `objectGUID`. Oracle Directory Server를 구성하는 경우 를 입력합니다 `nsuniqueid`. 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.

- `sAMAccountName` 또는 `uid`
- `objectGUID` `entryUUID`, 또는 `nsuniqueid`
- `cn`
- `memberOf` 또는 `isMemberOf`
- * Active Directory *: `objectSid`, `primaryGroupID`, `userAccountControl` 및 `userPrincipalName`
- * Azure *: `accountEnabled` 및 `userPrincipalName`

◦ * 암호 *: 사용자 이름과 연결된 암호입니다.

> ⓘ 나중에 암호를 변경하는 경우 이 페이지에서 암호를 업데이트해야 합니다.

◦ * 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\[USERNAME]`
- * 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.

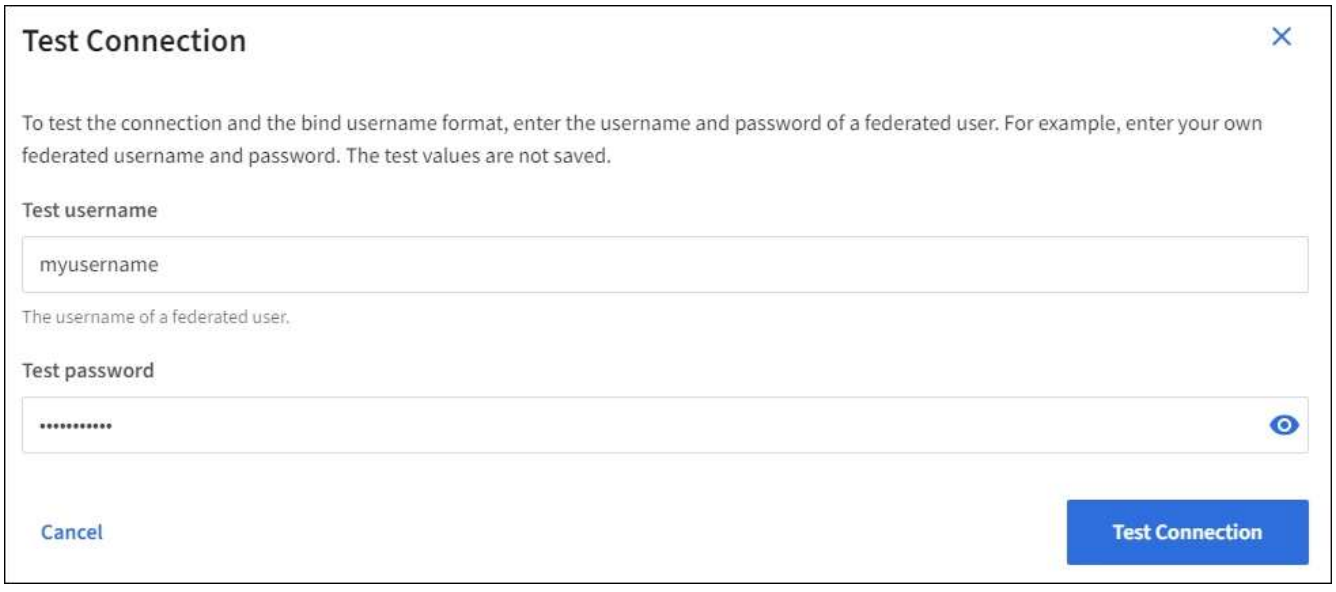
연결을 테스트하고 구성을 저장합니다

모든 값을 입력한 후 구성을 저장하기 전에 연결을 테스트해야 합니다. StorageGRID는 LDAP 서버에 대한 연결 설정과 바인딩 사용자 이름 형식(제공한 경우)을 확인합니다.

단계

1. Test connection * 을 선택합니다.
2. 바인딩 사용자 이름 형식을 제공하지 않은 경우:
   - 연결 설정이 유효한 경우 "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 유효한 경우 "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 대해서는 알림이 발생하지 않습니다.
- SSO(Single Sign-On)가 * Enabled * 또는 * Sandbox Mode * 로 설정된 경우 * Enable identity federation * 확인란이 비활성화됩니다. ID 페더레이션을 비활성화하려면 Single Sign-On 페이지의 SSO 상태가 * 사용 안 함 * 이어야 합니다. 을 "SSO(Single Sign-On)를 비활성화합니다"참조하십시오.

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 삭제하거나 모든 그룹에서 사용자를 제거합니다.

MemberOf 및 구체화 오버레이

MemberOf 및 구체화 오버레이를 활성화해야 합니다. 자세한 내용은 에서 역방향 그룹 구성원 유지 관리에 대한 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`
- `olcDbIndex: 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 "OpenLDAP 설명서: 버전 2.4 관리자 가이드"참조하십시오.

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"
- 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

단계

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

단계

1. 로컬 그룹 * 을 선택합니다.
2. 나중에 필요에 따라 업데이트할 수 있는 그룹의 표시 이름을 입력합니다. 예: "유지 보수 사용자" 또는 "ILM 관리자".
3. 나중에 업데이트할 수 없는 그룹의 고유 이름을 입력합니다.
4. Continue * 를 선택합니다.

통합 그룹

단계

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

단계

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 이상을 선택합니다"관리자 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)

단계

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. 자세한 내용은 을 "사용자 관리" 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. 선택적으로 을 선택하거나 선택 "관리자 그룹 권한"취소합니다. e. 변경 내용 저장 * 을 선택합니다.	a. 세부 정보를 표시할 그룹 이름을 선택합니다. b. 선택적으로 그룹의 액세스 모드를 변경합니다. c. 선택적으로 을 선택하거나 선택 "관리자 그룹 권한"취소합니다. d. 변경 내용 저장 * 을 선택합니다.

그룹을 복제합니다

단계

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.

단계

1. 그룹 페이지에서 제거할 각 그룹에 대한 확인란을 선택합니다.

2. Actions * > * Delete group * 을 선택합니다.
3. 그룹 삭제 * 를 선택합니다.

관리자 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
- 현재 및 해결된 경고를 봅니다
- 자신의 암호 변경(로컬 사용자만 해당)
- 구성 및 유지 관리 페이지에 제공된 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.

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.

> 그리드 토폴로지 페이지는 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다.

ILM을 참조하십시오

이 권한은 다음 * ILM * 메뉴 옵션에 대한 액세스를 제공합니다.

- 규칙
- 정책
- 정책 태그
- 지원합니다
- 보관 등급
- 지역
- 개체 메타데이터 조회

> 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
- * 구성 * > * 네트워크 *:
  - S3 끝점 도메인 이름
- * 유지보수 * > * 작업 *:
  - 서비스 해제
  - 확장
  - 개체 존재 여부 검사
  - 복구
- * 유지보수 * > * 시스템 *:
  - 복구 패키지
  - 소프트웨어 업데이트
- 지원 * > * 툴 *:
  - 로그

유지 관리 권한이 없는 사용자는 다음 페이지를 볼 수 있지만 편집할 수는 없습니다.

- * 유지보수 * > * 네트워크 *:
  - DNS 서버
  - 그리드 네트워크
  - NTP 서버

- * 유지보수 * > * 시스템 *:
  - 라이센스
- * 구성 * > * 네트워크 *:
  - S3 끝점 도메인 이름
- * 구성 * > * 보안 *:
  - 인증서
- * 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 다음에 대한 액세스를 제공합니다.

- 지원 * > * 도구 * > * 메트릭 * 페이지
- Grid Management API의 * Metrics * 섹션을 사용하여 맞춤형 Prometheus 메트릭 쿼리를 수행합니다
- 메트릭이 포함된 Grid Manager 대시보드 카드

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 * > * 시스템 *:
- 지원 * > * 기타 *:
  - 링크 비용

스토리지 어플라이언스 관리자

이 권한은 다음을 제공합니다.

- 그리드 관리자를 통해 스토리지 어플라이언스에서 E-Series SANtricity System Manager에 액세스할 수 있습니다.
- 이러한 작업을 지원하는 어플라이언스에 대한 드라이브 관리 탭에서 문제 해결 및 유지 관리 작업을 수행하는 기능.

테넌트 계정

이 권한은 다음 기능을 제공합니다.

- 테넌트 페이지에 액세스하여 테넌트 계정을 생성, 편집 및 제거할 수 있습니다
- 기존 트래픽 분류 정책을 봅니다
- 테넌트 세부 정보가 포함된 Grid Manager 대시보드 카드를 봅니다

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

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 사용자 한 명이 포함되어 있습니다. 루트 사용자를 제거할 수 없습니다.

SSO(Single Sign-On)가 활성화된 경우 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

마법사에 액세스합니다

단계

1. 구성 * > * 액세스 제어 * > * 관리자 사용자 * 를 선택합니다.
2. 사용자 생성 * 을 선택합니다.

사용자 자격 증명을 입력합니다

단계

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

단계

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. 자세한 내용은 을 "관리 그룹을 관리합니다" 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 배너에 있는 * 암호 변경 * 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.
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.

작업	작업 메뉴	세부 정보 페이지
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.

단계

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.

단계

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

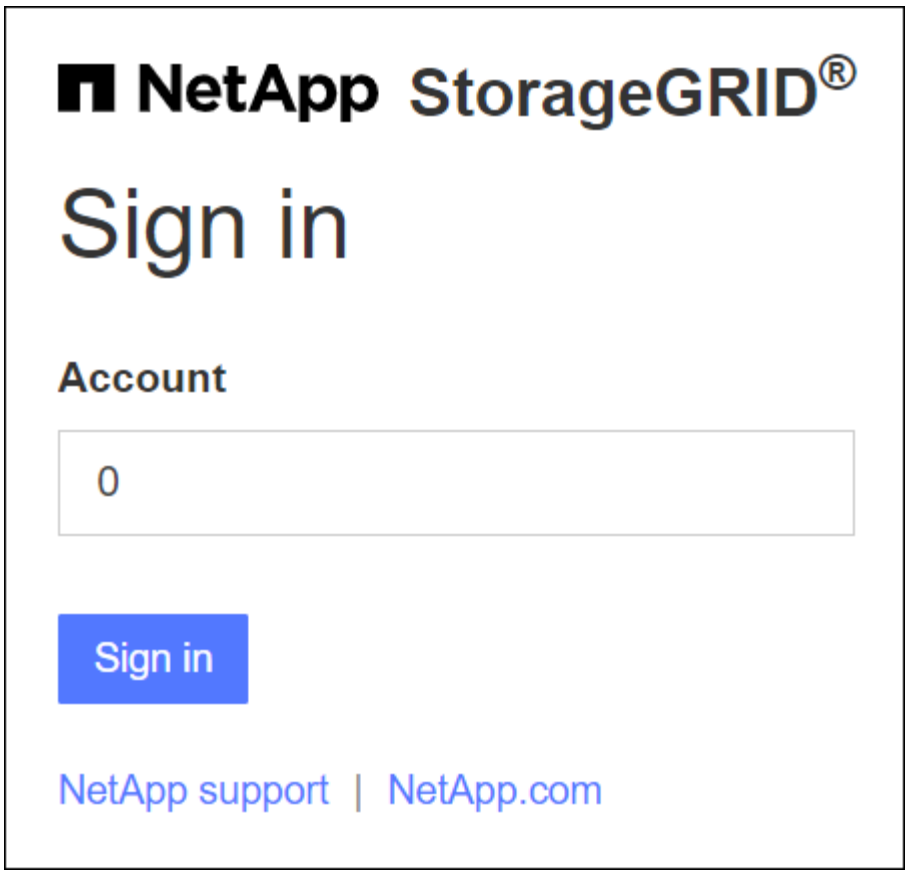
SSO가 활성화되어 있고 StorageGRID에 로그인하면 조직의 SSO 페이지로 리디렉션되어 자격 증명을 검증합니다.

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.

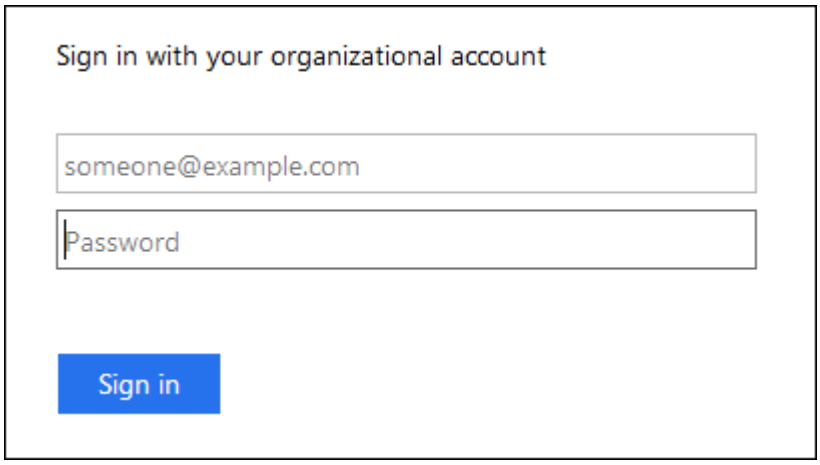


◦ 이전에 Grid Manager 또는 Tenant Manager에 액세스한 경우, 최근 계정을 선택하거나 계정 ID를 입력하라는 메시지가 나타납니다.

테넌트 계정에 대한 전체 URL(즉, 정규화된 도메인 이름 또는 IP 주소 다음에 가 오는 경우)을 입력하면 StorageGRID 로그인 페이지가 표시되지 않습니다 `/?accountId=20-digit-account-id`. 대신 조직의 SSO 로그인 페이지로 바로 리디렉션됩니다SSO 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.

SSO(Single Sign-On)에 대한 요구 사항 및 고려 사항

StorageGRID 시스템에 대해 SSO(Single Sign-On)를 활성화하기 전에 요구 사항 및 고려 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 2016은, 이상을 사용해야 "KB3201845 업데이트" 합니다.

추가 요구 사항

- TLS(전송 계층 보안) 1.2 또는 1.3
- Microsoft .NET Framework 버전 3.5.1 이상

Azure 고려 사항

Azure를 SSO 유형으로 사용하고 sAMAccountName을 접두사로 사용하지 않는 사용자 기본 이름이 있는 경우 StorageGRID와 LDAP 서버 간의 연결이 끊어지면 로그인 문제가 발생할 수 있습니다. 사용자가 로그인할 수 있도록 하려면 LDAP 서버에 대한 연결을 복원해야 합니다.

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 하지 않았다면 "관리 인터페이스에 대한 사용자 지정 인증서를 구성했습니다"지금 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 디렉터리로 이동하여 관리자 노드의 서버 인증서에 액세스할 수 `/var/local/mgmt-api` 있습니다. 사용자 지정 서버 인증서의 이름은 `custom-server.crt`입니다. 노드의 기본 서버 인증서 이름은 `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 "외부 방화벽에서 액세스를 제어합니다"참조하십시오.

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"
- 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.

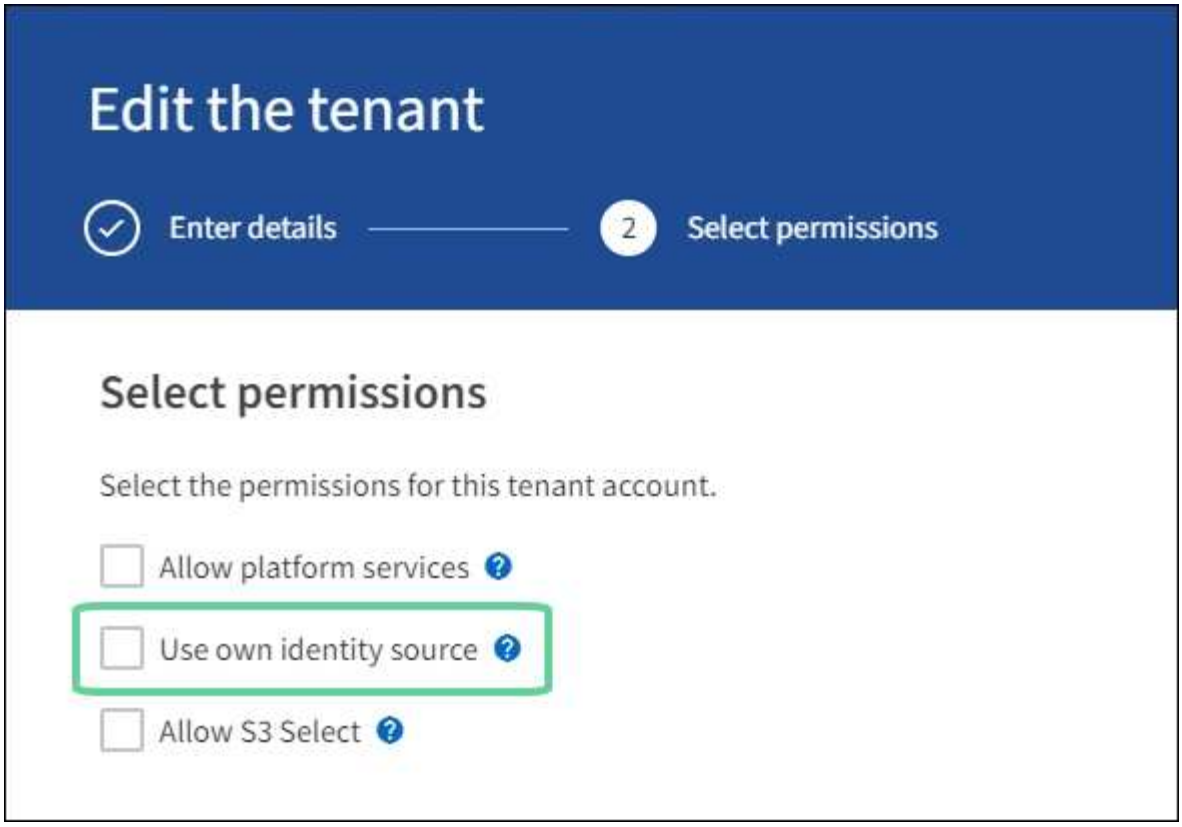
   a. 각 테넌트 계정의 테넌트 관리자에 로그인합니다.
   b. 액세스 관리 * > * ID 페더레이션 * 을 선택합니다.
   c. ID 페더레이션 사용 * 확인란이 선택되지 않았는지 확인합니다.
   d. 이 경우 이 테넌트 계정에 사용 중인 모든 통합 그룹이 더 이상 필요하지 않은지 확인하고 확인란을 선택 취소하고 * Save * 를 선택합니다.

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, 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

- "SSO(Single Sign-On)에 대한 요구 사항 및 고려 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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"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.

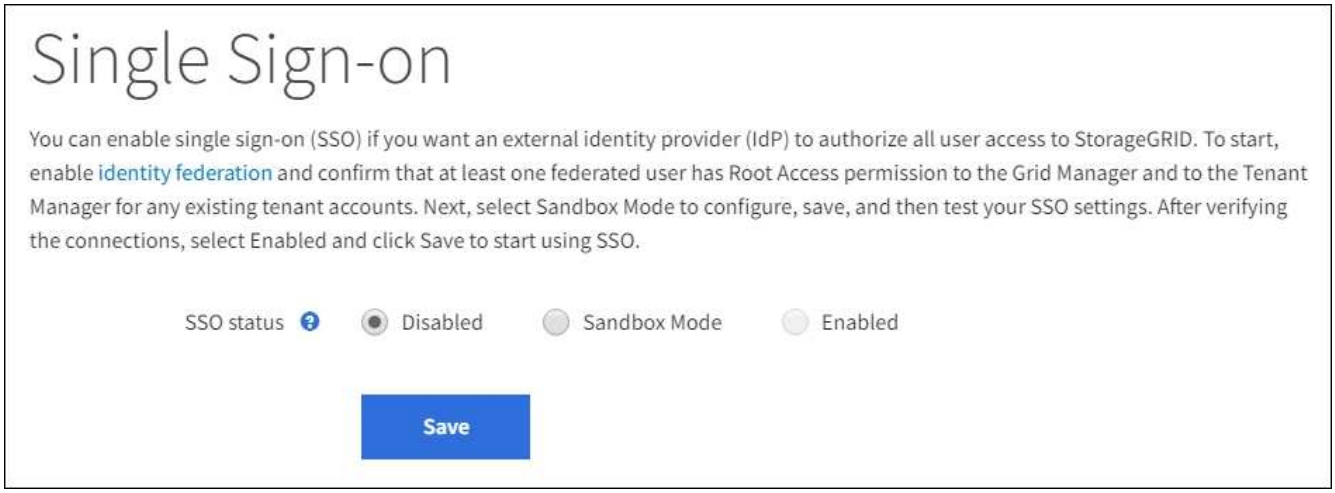
sandbox 모드를 사용하면 SSO를 활성화하기 전에 이 전면과 후면을 간편하게 구성하고 모든 설정을 테스트할 수 있습니다. 샌드박스 모드를 사용하는 경우 사용자는 SSO를 사용하여 로그인할 수 없습니다.

sandbox 모드에 액세스합니다

단계

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 "SSO(Single Sign-On)에 대한 요구 사항 및 고려 사항"참조하십시오.

2. Sandbox 모드 * 를 선택합니다.

   ID 공급자 섹션이 나타납니다.

ID 공급자 세부 정보를 입력합니다

단계

1. 드롭다운 목록에서 * SSO 유형 * 을 선택합니다.
2. 선택한 SSO 유형에 따라 ID 공급자 섹션의 필드를 작성합니다.

Active Directory를 클릭합니다

a. 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.

b. 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.

> CA 인증서를 변경하는 경우 즉시 "관리 노드에서 mgmt-API 서비스를 다시 시작합니다"그리드 관리자에서 성공적인 SSO를 테스트합니다.

c. StorageGRID에 대한 * 사용 당사자 식별자 * 를 관련 당사자 섹션에서 지정합니다. 이 값은 AD FS의 각 기반 당사자 신뢰에 사용하는 이름을 제어합니다.

- 예를 들어 그리드에 관리자 노드가 하나만 있고 앞으로 관리자 노드를 더 추가할 계획이 없는 경우 또는 `StorageGRID` 를 입력합니다. `SG`
- 그리드에 둘 이상의 관리자 노드가 포함되어 있는 경우 해당 문자열을 `[HOSTNAME]` 식별자에 포함합니다. `SG-[HOSTNAME]`예를 들어, 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.

d. 저장 * 을 선택합니다.

몇 초 동안 * Save * (저장 *) 버튼에 녹색 확인 표시가 나타납니다.

Azure를 지원합니다

a. 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.

> CA 인증서를 변경하는 경우 즉시 "관리 노드에서 mgmt-API 서비스를 다시 시작합니다"그리드 관리자에서 성공적인 SSO를 테스트합니다.

b. 엔터프라이즈 응용 프로그램 섹션에서 StorageGRID의 * 엔터프라이즈 응용 프로그램 이름 * 을 지정합니다. 이 값은 Azure AD의 각 엔터프라이즈 애플리케이션에 사용하는 이름을 제어합니다.

- 예를 들어 그리드에 관리자 노드가 하나만 있고 앞으로 관리자 노드를 더 추가할 계획이 없는 경우 또는 `StorageGRID` 를 입력합니다. `SG`
- 그리드에 둘 이상의 관리자 노드가 포함되어 있는 경우 해당 문자열을 `[HOSTNAME]` 식별자에 포함합니다. `SG-[HOSTNAME]`예를 들어, 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.

c. 의 단계에 따라 "Azure AD에서 엔터프라이즈 애플리케이션을 생성합니다"표에 나열된 각 관리자 노드에 대한 엔터프라이즈 애플리케이션을 생성합니다.

d. Azure AD에서 각 엔터프라이즈 애플리케이션의 연합 메타데이터 URL을 복사합니다. 그런 다음 이 URL을 StorageGRID의 해당 * 페더레이션 메타데이터 URL * 필드에 붙여 넣습니다.

e. 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)

a. 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.

> CA 인증서를 변경하는 경우 즉시 "관리 노드에서 mgmt-API 서비스를 다시 시작합니다"그리드 관리자에서 성공적인 SSO를 테스트합니다.

b. 서비스 공급자(SP) 섹션에서 StorageGRID에 대한 * SP 접속 ID * 를 지정합니다. 이 값은

PingFederate의 각 SP 연결에 사용할 이름을 제어합니다.

- 예를 들어 그리드에 관리자 노드가 하나만 있고 앞으로 관리자 노드를 더 추가할 계획이 없는 경우 또는 `StorageGRID` 를 입력합니다. `SG`
- 그리드에 둘 이상의 관리자 노드가 포함되어 있는 경우 해당 문자열을 `[HOSTNAME]` 식별자에 포함합니다. `SG-[HOSTNAME]`예를 들어, 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.

c. 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>
```

d. 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

단계

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 을 "AD FS에서 기반 당사자 트러스트를 생성합니다"참조하십시오.

Azure를 지원합니다

단계

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 단계에 따라 "Azure AD에서 엔터프라이즈 애플리케이션을 생성합니다"각 관리자 노드에 대한 SAML 메타데이터 파일을 해당 Azure 엔터프라이즈 애플리케이션에 업로드합니다.

PingFederate(PingFederate)

단계

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

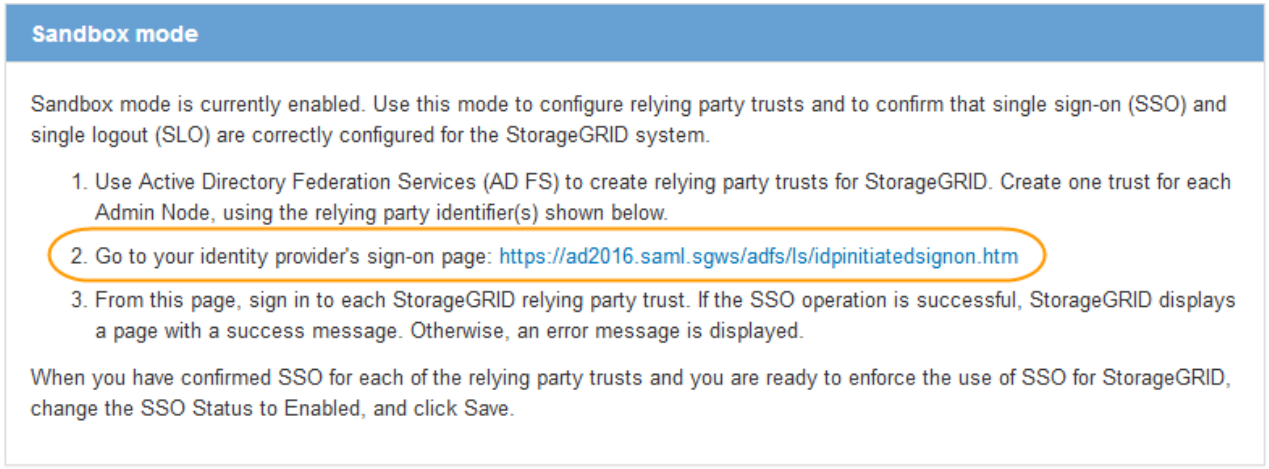
전체 StorageGRID 시스템에 대해 SSO(Single Sign-On)를 사용하기 전에 각 관리 노드에 대해 SSO(Single Sign-On)와 단일 로그아웃이 올바르게 구성되어 있는지 확인해야 합니다.

Active Directory를 클릭합니다

단계

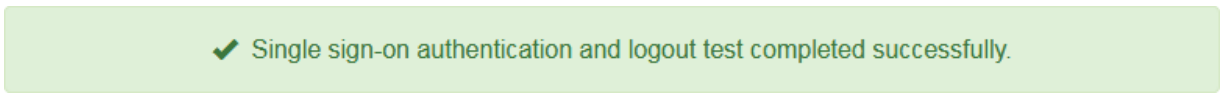
1. StorageGRID 단일 사인온 페이지의 Sandbox 모드 메시지에서 링크를 찾습니다.

   URL은 * 페더레이션 서비스 이름 * 필드에 입력한 값에서 파생됩니다.



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.

4. 통합 사용자 이름과 암호를 입력합니다.
   - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 나타납니다.



   - 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

단계

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.

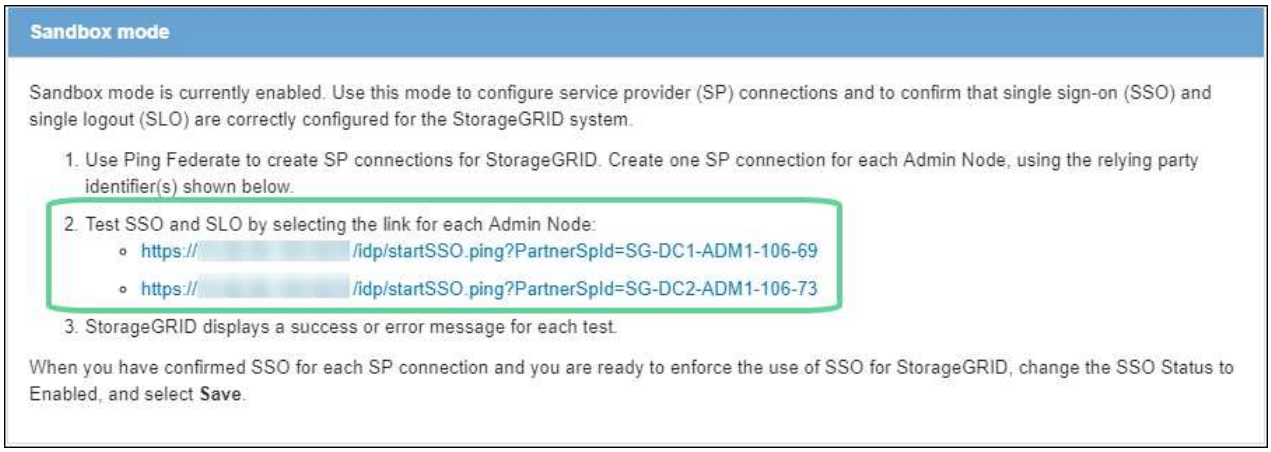
   - SSO 작업이 실패하면 오류 메시지가 나타납니다. 문제를 해결하고 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
4. 이 단계를 반복하여 그리드의 각 관리 노드에 대한 SSO 연결을 확인합니다.

PingFederate(PingFederate)

단계

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.

단계

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.

시작하기 전에

- StorageGRID에 대해 Single Sign-On을 구성하고 SSO 유형으로 * AD FS * 를 선택했습니다.
- * Sandbox 모드 * 는 Grid Manager의 Single Sign-On 페이지에서 선택됩니다. 을 "sandbox 모드를 사용합니다 "참조하십시오.
- 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_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - 의 경우 *Admin_Node_Identifier* 단일 사인온 페이지에 표시된 대로 관리자 노드의 종속 당사자 식별자를 입력합니다. `SG-DC1-ADM1`예를 들어,
   - 의 경우 *Admin_Node_FQDN* 동일한 관리자 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 * objectGUID를 이름 ID * 로, * UPN을 이름 ID * 로 지정합니다.
   f. 특성 저장소의 경우 * Active Directory * 를 선택합니다.
   g. Mapping 테이블의 LDAP Attribute 열에서 * objectGUID * 를 입력하거나 * User-Principal-Name * 을 선택합니다.

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. 자세한 내용은 을 "Sandbox 모드를 사용합니다" 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`

의 경우 *Admin_Node_FQDN* 동일한 관리자 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. `SG-DC1-ADM1`예를 들어,

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 * objectGUID를 이름 ID * 로, * UPN을 이름 ID * 로 지정합니다.

e. 특성 저장소의 경우 * Active Directory * 를 선택합니다.

f. Mapping 테이블의 LDAP Attribute 열에서 * objectGUID * 를 입력하거나 * User-Principal-Name * 을 선택합니다.

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. 자세한 내용은 을 "Sandbox 모드를 사용합니다" 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. `SG-DC1-ADM1`예를 들어,

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`

의 경우 *Admin_Node_FQDN* 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

의 경우 *Admin_Node_Identifier* 단일 사인온 페이지에 표시된 대로 관리자 노드의 종속 당사자 식별자를 입력합니다. `SG-DC1-ADM1`예를 들어,

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 * objectGUID를 이름 ID * 로, * UPN을 이름 ID * 로 지정합니다.

   c. 특성 저장소의 경우 * Active Directory * 를 선택합니다.
   d. Mapping 테이블의 LDAP Attribute 열에서 * objectGUID * 를 입력하거나 * User-Principal-Name * 을 선택합니다.
   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`

      의 경우 *Admin_Node_FQDN* 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 지정 인증서가 없는 경우 관리자 노드에 로그인하고 관리자 노드의 디렉터리로 이동하여 `/var/local/mgmt-api` 인증서 파일을 추가합니다 `custom-server.crt`.

      > 관리자 노드의 기본 인증서 (`server.crt`사용)은 사용하지 않는 것이 좋습니다. 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. 자세한 내용은 을 "sandbox 모드를 사용합니다" 참조하십시오.

Azure AD에서 엔터프라이즈 애플리케이션을 생성합니다

Azure AD를 사용하여 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 생성합니다.

시작하기 전에

- StorageGRID에 대한 SSO(Single Sign-On) 구성을 시작했으며 SSO 유형으로 * Azure * 를 선택했습니다.
- * Sandbox 모드 * 는 Grid Manager의 Single Sign-On 페이지에서 선택됩니다. 을 "sandbox 모드를 사용합니다 "참조하십시오.
- 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

단계

1. 에 "Azure 포털"로그인합니다.
2. 로 이동합니다 "Azure Active Directory를 클릭합니다".
3. 을 "엔터프라이즈 애플리케이션"선택합니다.

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.

단계

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.

단계

1. 각 관리 노드에 대해 이 단계를 반복합니다.

a. 관리자 노드에서 StorageGRID에 로그인합니다.

b. 구성 * > * 액세스 제어 * > * 단일 사인온 * 을 선택합니다.

c. 버튼을 선택하여 해당 Admin Node에 대한 SAML 메타데이터를 다운로드합니다.

d. 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.

단계

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 단계에 따라 "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.

시작하기 전에

- StorageGRID에 대한 SSO(Single Sign-On)를 구성하고 SSO 유형으로 * Ping 남부연합을 선택했습니다.
- * Sandbox 모드 * 는 Grid Manager의 Single Sign-On 페이지에서 선택됩니다. 을 "sandbox 모드를 사용합니다"참조하십시오.
- 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.
- PingFederate Server용 이 "관리자 참조 안내서"있습니다. PingFederate 설명서는 자세한 단계별 지침과 설명을 제공합니다.
- PingFederate Server용 이 "관리자 권한"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. StorageGRID에서 사용한 값을 "ID 페더레이션을 구성하는 중입니다"사용합니다.

- * 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.

단계

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. 작성한 을 암호 자격 증명 유효성 검사기가 있습니다선택합니다.
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.

단계

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 추가 SP 접속을 생성합니다 이동하여 필요한 추가 연결을 만듭니다.

SP 접속 유형을 선택합니다

단계

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

단계

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 탭에 제공된 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

단계

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 사용하지 않는 를 제거합니다 `urn:oid`.

어댑터 인스턴스를 매핑합니다

단계

1. 인증 소스 매핑 탭에서 * 새 어댑터 인스턴스 매핑 * 을 선택합니다.
2. 어댑터 인스턴스 탭에서 작성한 을 어댑터 인스턴스선택합니다.
3. 매핑 방법 탭에서 * 데이터 저장소에서 추가 특성 검색 * 을 선택합니다.
4. 특성 원본 및 사용자 조회 탭에서 * 특성 원본 추가 * 를 선택합니다.
5. 데이터 저장소 탭에서 설명을 입력하고 추가한 을 데이터 저장소선택합니다.
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 * 또는 * userPrincipalName * 속성 중 하나를 검색하여 추가합니다.
7. LDAP 바이너리 특성 인코딩 형식 탭에서 * objectGUID * 특성에 대해 * Base64 * 를 선택합니다.
8. LDAP 필터 탭에서 * sAMAccountName=${username} * 을 입력합니다.
9. 특성 계약 이행 탭의 소스 드롭다운에서 * LDAP (attribute) * 를 선택하고 값 드롭다운에서 * objectGUID * 또는 * userPrincipalName * 을 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

단계

1. SP Connection * > * Browser SSO * > * Protocol Settings * 탭에서 * Configure Protocol Settings * 를 선택합니다.
2. 어설션 소비자 서비스 URL 탭에서 StorageGRID SAML 메타데이터(* 바인딩 및 끝점 URL의 경우 * POST *)에서 가져온 기본값을 수락합니다. `/api/saml-response`
3. SLO 서비스 URL 탭에서 StorageGRID SAML 메타데이터(* 바인딩 및 끝점 URL의 경우 * 리디렉션 *)에서 가져온 기본값을 그대로 `/api/saml-logout` 사용합니다.
4. 허용 가능한 SAML 바인딩 탭에서 * Artifact * 및 * SOAP * 를 지웁니다. POST * 및 * REDIRECT * 만 필요합니다.
5. 서명 정책 탭에서 * Authn 요청 서명 필요 * 및 * 항상 설정 서명 * 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

단계

1. SP 연결 탭에서 * 자격 증명 * 을 선택합니다.
2. 자격 증명 탭에서 * 자격 증명 구성 * 을 선택합니다.
3. 만들거나 가져온 을 서명 인증서선택합니다.
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.

단계

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

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.

시작하기 전에

- 있습니다. "특정 액세스 권한"
- `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 * 확인란은 선택된 상태로 남아 있으며, 기존 SSO 설정은 모두 업데이트하지 않는 한 유지됩니다.

단계

1. 관리자 노드에 로그인:
   a. 다음 명령을 입력합니다. `ssh admin@Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 다음 명령을 실행합니다.`disable-saml`

   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.
      - 다음 명령을 실행합니다. `enable-saml`

명령이 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

SSO를 활성화할지 확인합니다.

노드에서 Single Sign-On이 설정되었음을 나타내는 메시지가 표시됩니다.

- 그리드 노드를 재부팅합니다. `reboot`

8. 웹 브라우저에서 동일한 관리 노드에서 그리드 관리자에 액세스합니다.
9. StorageGRID 로그인 페이지가 나타나고 그리드 관리자에 액세스하려면 SSO 자격 증명을 입력해야 합니다.

그리드 페더레이션을 사용합니다

그리드 페더레이션은 무엇입니까?

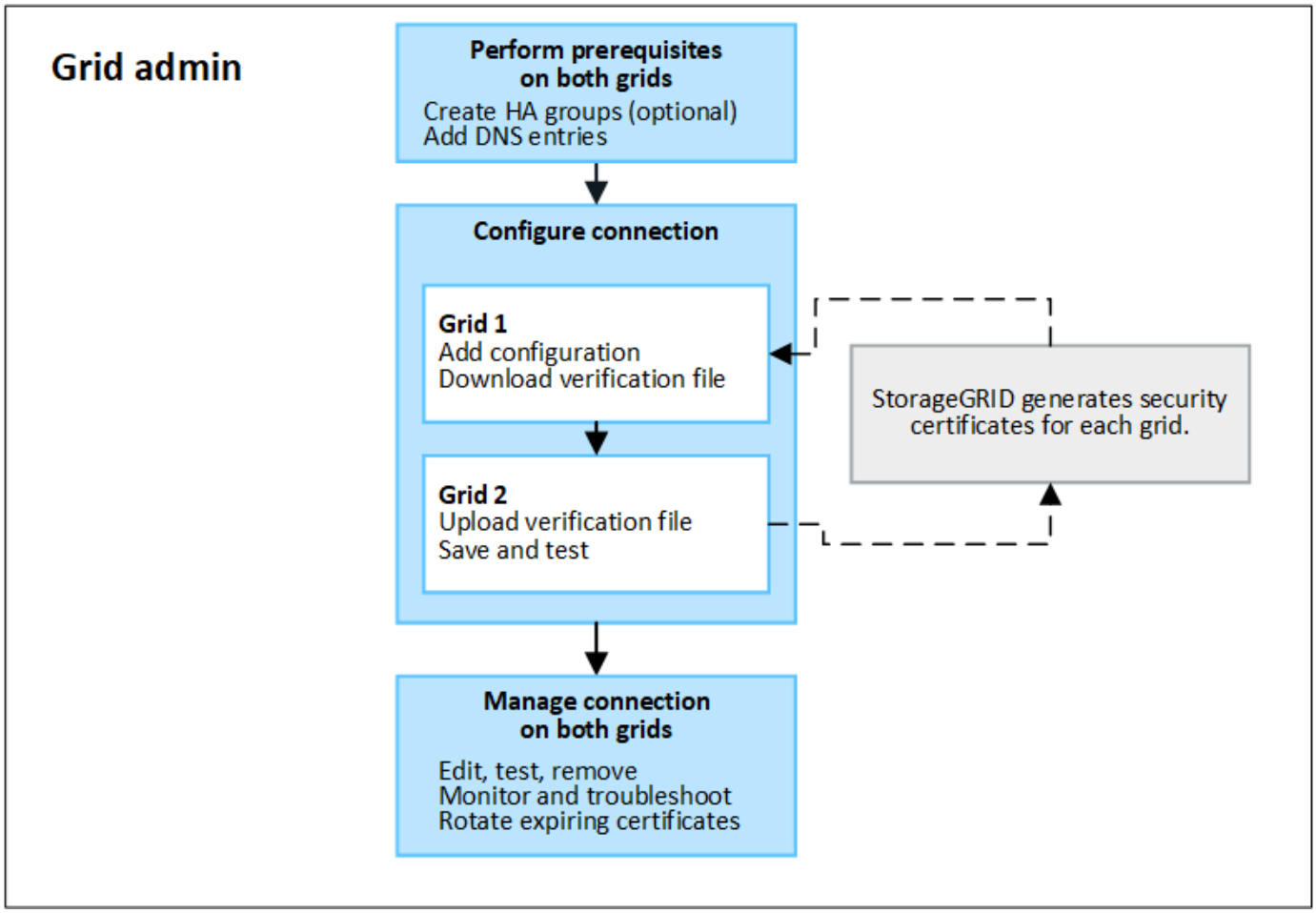
그리드 페더레이션을 사용하여 테넌트를 클론 복제하고 재해 복구를 위해 두 StorageGRID 시스템 간에 개체를 복제할 수 있습니다.

그리드 페더레이션 연결이란 무엇입니까?

그리드 페더레이션 연결은 두 StorageGRID 시스템에서 관리자 노드와 게이트웨이 노드 간에 양방향으로 안전하게 연결됩니다.

그리드 페더레이션을 위한 워크플로

워크플로 다이어그램은 두 그리드 간의 그리드 페더레이션 연결을 구성하는 단계를 요약합니다.



그리드 페더레이션 연결에 대한 고려 사항 및 요구 사항

- 그리드 페더레이션에 사용되는 그리드는 동일하거나 둘 이상의 주요 버전 차이가 없는 StorageGRID 버전을 실행해야 합니다.

  버전 요구 사항에 대한 자세한 내용은 를 "릴리스 정보"참조하십시오.

- 그리드에는 다른 그리드에 대한 하나 이상의 그리드 페더레이션 연결이 있을 수 있습니다. 각 그리드 페더레이션 연결은 다른 연결과 독립적입니다. 예를 들어, 그리드 1이 그리드 2와 1개의 연결을 가지고 있고 그리드 3과 2번째 연결이 있는 경우 그리드 2와 그리드 3 사이에는 묵시적 연결이 없습니다.
- 그리드 페더레이션 연결은 양방향입니다. 연결이 설정되면 두 그리드 중 하나에서 연결을 모니터링하고 관리할 수 있습니다.
- 또는 을 사용하려면 하나 이상의 그리드 페더레이션 연결이 있어야 "계정 클론""교차 그리드 복제"합니다.

네트워킹 및 **IP** 주소 요구 사항

- 그리드 페더레이션 연결은 그리드 네트워크, 관리자 네트워크 또는 클라이언트 네트워크에서 발생할 수 있습니다.
- 그리드 페더레이션 연결은 한 그리드를 다른 그리드에 연결합니다. 각 그리드의 구성은 관리 노드, 게이트웨이 노드 또는 둘 모두로 구성된 다른 그리드의 그리드 통합 끝점을 지정합니다.
- Best Practice는 각 그리드에서 게이트웨이 및 관리 노드를 연결하는 "고가용성(HA) 그룹"것입니다. HA 그룹을 사용하면 노드를 사용할 수 없게 될 경우 그리드 페더레이션 연결이 온라인 상태로 유지됩니다. 두 HA 그룹 중 하나의 활성 인터페이스에 장애가 발생하면 연결에서 백업 인터페이스를 사용할 수 있습니다.

- 단일 관리 노드 또는 게이트웨이 노드의 IP 주소를 사용하는 그리드 페더레이션 연결을 만드는 것은 권장되지 않습니다. 노드를 사용할 수 없게 되면 그리드 페더레이션 연결도 사용할 수 없게 됩니다.
- "교차 그리드 복제" 객체의 경우 각 그리드의 스토리지 노드가 다른 그리드에서 구성된 관리 및 게이트웨이 노드에 액세스할 수 있어야 합니다. 각 그리드에 대해 모든 스토리지 노드가 연결에 사용되는 관리자 노드 또는 게이트웨이 노드로 향하는 고대역폭 경로를 가지고 있는지 확인합니다.

FQDN을 사용하여 연결 밸런스를 로드합니다

운영 환경의 경우 FQDN(정규화된 도메인 이름)을 사용하여 연결의 각 그리드를 식별합니다. 그런 다음 다음과 같이 적절한 DNS 항목을 만듭니다.

- 그리드 1의 FQDN은 그리드 1의 HA 그룹에 대한 하나 이상의 가상 IP(VIP) 주소 또는 그리드 1에 있는 하나 이상의 관리 또는 게이트웨이 노드의 IP 주소에 매핑됩니다.
- 그리드 2의 FQDN은 그리드 2의 하나 이상의 VIP 주소 또는 그리드 2의 하나 이상의 관리 또는 게이트웨이 노드의 IP 주소에 매핑됩니다.

여러 DNS 항목을 사용하는 경우 연결 사용 요청은 다음과 같이 로드 밸런싱됩니다.

- 여러 HA 그룹의 VIP 주소에 매핑되는 DNS 항목은 HA 그룹의 활성 노드 간에 로드 밸런싱됩니다.
- 여러 관리 노드 또는 게이트웨이 노드의 IP 주소에 매핑되는 DNS 항목은 매핑된 노드 간에 로드 밸런싱됩니다.

포트 요구 사항

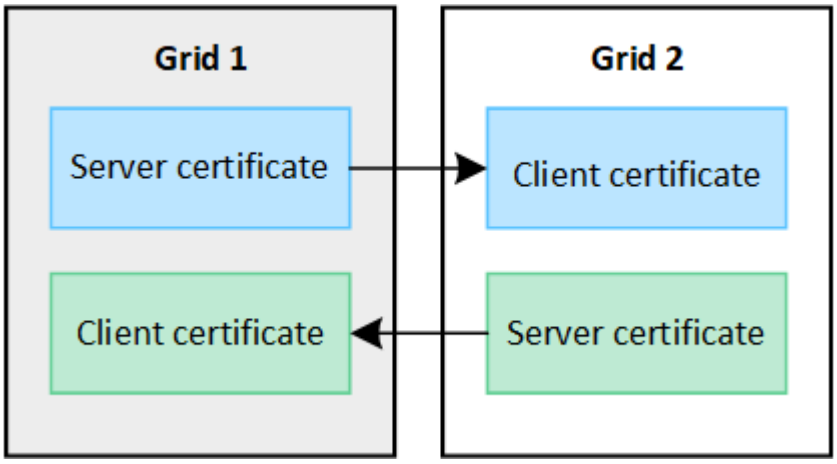
그리드 페더레이션 연결을 생성할 때 사용하지 않는 포트 번호를 23000에서 23999까지 지정할 수 있습니다. 이 연결의 두 그리드는 동일한 포트를 사용합니다.

두 그리드 중 어떤 노드도 다른 연결에 이 포트를 사용하지 않도록 해야 합니다.

인증서 요구 사항

그리드 페더레이션 연결을 구성할 때 StorageGRID는 자동으로 네 개의 SSL 인증서를 생성합니다.

- 그리드 1에서 그리드 2로 전송되는 정보를 인증 및 암호화하는 서버 및 클라이언트 인증서입니다
- 그리드 2에서 그리드 1로 전송되는 정보를 인증 및 암호화하는 서버 및 클라이언트 인증서입니다



기본적으로 인증서는 730일(2년)에 유효합니다. 이러한 인증서가 만료 날짜에 근접하면 * 그리드 페더레이션 인증서 만료 * 알림이 인증서를 회전하라는 알림을 표시합니다. 이 알림은 그리드 관리자를 사용하여 수행할 수 있습니다.

연결 양 끝에 있는 인증서가 만료되면 연결이 중지됩니다. 인증서가 업데이트될 때까지 데이터 복제가 보류됩니다.

자세한 정보

- "그리드 페더레이션 연결을 만듭니다"
- "그리드 페더레이션 연결을 관리합니다"
- "그리드 통합 오류 문제 해결"

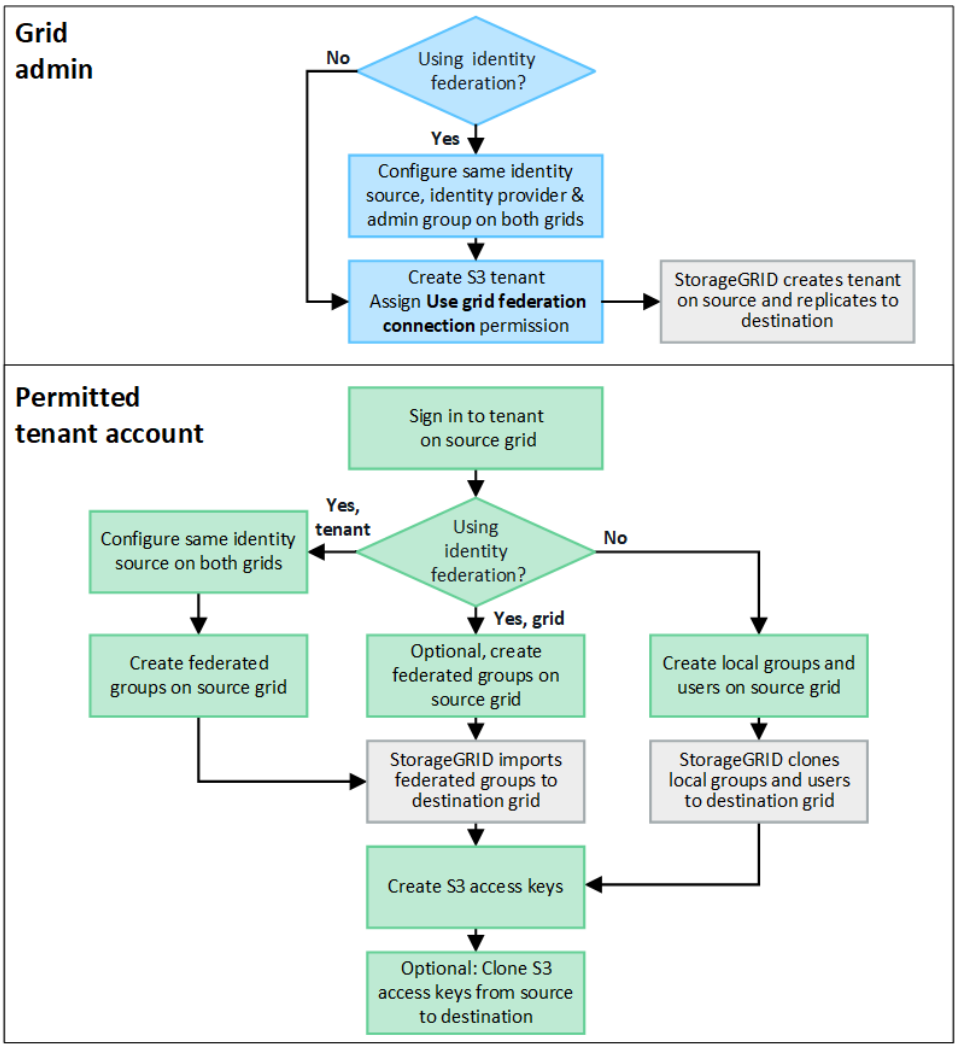
계정 클론이란 무엇입니까?

계정 클론은 테넌트 계정, 테넌트 그룹, 테넌트 사용자 및 의 StorageGRID 시스템 간에 선택적으로 S3 액세스 키를 자동으로 복제하는 "그리드 페더레이션 연결"것입니다.

에 계정 클론이 필요합니다."교차 그리드 복제" 소스 StorageGRID 시스템에서 대상 StorageGRID 시스템으로 계정 정보를 클론 복제하면 테넌트 사용자 및 그룹이 두 그리드 중 하나의 해당 버킷과 객체에 액세스할 수 있습니다.

계정 클론 워크플로우

워크플로우 다이어그램은 그리드 관리자 및 허용된 테넌트가 계정 클론을 설정하기 위해 수행하는 단계를 보여 줍니다. 이러한 단계는 이후에 "그리드 페더레이션 연결이 구성되어 있습니다"수행됩니다.



그리드 관리자가 수행하는 단계는 의 StorageGRID 시스템이 SSO(Single Sign-On)를 사용하는지 ID 페더레이션을 사용하는지에 따라 "그리드 페더레이션 연결"다릅니다.

계정 클론에 대한 **SSO** 구성(선택 사항)

그리드 페더레이션 연결의 StorageGRID 시스템 중 하나에서 SSO를 사용하는 경우 두 그리드에서 모두 SSO를 사용해야 합니다. 그리드 페더레이션을 위해 테넌트 계정을 생성하기 전에 테넌트의 소스 및 대상 그리드에 대한 그리드 관리자가 다음 단계를 수행해야 합니다.

단계

1. 두 그리드에 대해 동일한 ID 소스를 구성합니다. 을 "ID 페더레이션을 사용합니다"참조하십시오.
2. 두 그리드에 대해 동일한 SSO ID 공급자(IDP)를 구성합니다. 을 "Single Sign-On 구성"참조하십시오.
3. "동일한 관리 그룹을 생성합니다" 동일한 통합 그룹을 가져와서 두 그리드 모두에서

   테넌트를 생성할 때 소스 및 대상 테넌트 계정에 대한 초기 루트 액세스 권한을 가지려면 이 그룹을 선택합니다.

   > ⓘ 이 관리 그룹이 테넌트를 생성하기 전에 두 그리드에 없는 경우 테넌트는 대상에 복제되지 않습니다.

계정 클론에 대한 그리드 수준 **ID** 페더레이션 구성(선택 사항)

StorageGRID 시스템 중 하나에서 SSO 없이 ID 페더레이션을 사용하는 경우 두 그리드 모두 ID 페더레이션을 사용해야 합니다. 그리드 페더레이션을 위해 테넌트 계정을 생성하기 전에 테넌트의 소스 및 대상 그리드에 대한 그리드 관리자가 다음 단계를 수행해야 합니다.

단계

1. 두 그리드에 대해 동일한 ID 소스를 구성합니다. 을 "ID 페더레이션을 사용합니다"참조하십시오.
2. 필요에 따라 통합 그룹에 소스 및 대상 테넌트 계정 모두에 대한 초기 루트 액세스 권한이 있는 경우, "동일한 관리 그룹을 생성합니다"동일한 통합 그룹을 가져와 두 그리드 모두에서 사용할 수 있습니다.

   > ⓘ 두 그리드에 없는 통합 그룹에 루트 액세스 권한을 할당하면 해당 테넌트가 대상 그리드에 복제되지 않습니다.

3. 통합 그룹에 두 계정에 대한 초기 루트 액세스 권한이 없는 경우 로컬 루트 사용자의 암호를 지정합니다.

허용된 **S3** 테넌트 계정을 생성합니다

선택적으로 SSO 또는 ID 페더레이션을 구성한 후 그리드 관리자는 다음 단계를 수행하여 버킷 객체를 다른 StorageGRID 시스템으로 복제할 수 있는 테넌트를 결정합니다.

단계

1. 계정 클론 작업을 위해 테넌트의 소스 그리드로 사용할 그리드를 결정합니다.

   테넌트가 처음 생성된 그리드를 테넌트의 _source GRID_라고 합니다. 테넌트가 복제되는 그리드를 테넌트의_destination grid _ 라고 합니다.

2. 이 그리드에서 새 S3 테넌트 계정을 만들거나 기존 계정을 편집합니다.

3. 그리드 페더레이션 연결 사용 * 권한을 할당합니다.
4. 테넌트 계정이 자신의 통합 사용자를 관리할 경우 * 사용자 ID 소스 사용 * 권한을 할당합니다.

   이 권한이 할당된 경우 소스 및 대상 테넌트 계정 모두 통합 그룹을 생성하기 전에 동일한 ID 소스를 구성해야 합니다. 소스 테넌트에 추가된 통합 그룹은 두 그리드 모두 동일한 ID 소스를 사용하지 않는 한 대상 테넌트에 복제할 수 없습니다.

5. 특정 그리드 페더레이션 연결을 선택합니다.
6. 새 테넌트 또는 수정된 테넌트를 저장합니다.

   그리드 통합 연결 사용 * 권한이 있는 새 테넌트가 저장된 경우 StorageGRID는 다음과 같이 다른 그리드에 해당 테넌트의 복제본을 자동으로 생성합니다.

   - 두 테넌트 계정 모두 동일한 계정 ID, 이름, 스토리지 할당량 및 할당된 권한이 있습니다.
   - 테넌트에 대한 루트 액세스 권한이 있는 통합 그룹을 선택한 경우 해당 그룹이 대상 테넌트에 복제됩니다.
   - 테넌트에 대한 루트 액세스 권한이 있는 로컬 사용자를 선택한 경우 해당 사용자는 대상 테넌트에 복제됩니다. 그러나 해당 사용자의 암호는 복제되지 않습니다.

자세한 내용은 을 참조하십시오 "그리드 페더레이션에 허용된 테넌트 관리".

허용된 테넌트 계정 워크플로

그리드 페더레이션 연결 사용 * 권한이 있는 테넌트가 대상 그리드에 복제된 후에 허용된 테넌트 계정은 테넌트 그룹, 사용자 및 S3 액세스 키를 클론 복제하기 위해 다음 단계를 수행할 수 있습니다.

단계

1. 테넌트의 소스 격자에서 테넌트 계정에 로그인합니다.
2. 허용되는 경우 소스 및 대상 테넌트 계정 모두에서 ID 페더레이션을 구성합니다.
3. 소스 테넌트에 그룹 및 사용자를 생성합니다.

   소스 테넌트에 새 그룹 또는 사용자가 생성되면 StorageGRID는 자동으로 대상 테넌트에 클론을 생성하지만 대상에서 다시 소스로 클론을 생성하지 않습니다.

4. S3 액세스 키를 생성합니다.
5. 필요에 따라 소스 테넌트에서 대상 테넌트로 S3 액세스 키를 복제합니다.

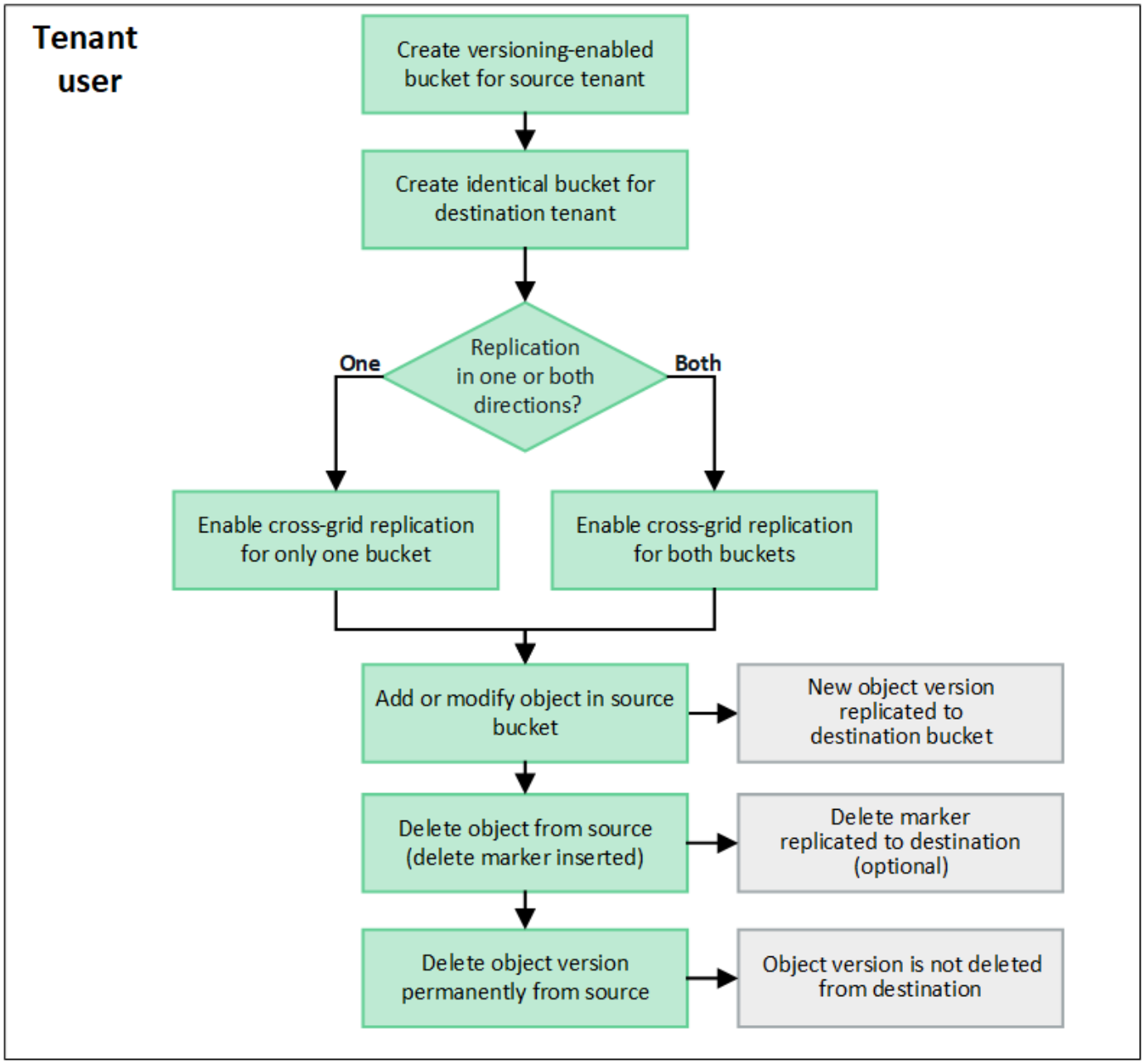
허용되는 테넌트 계정 워크플로에 대한 자세한 내용과 그룹, 사용자 및 S3 액세스 키의 클론 생성 방법에 대한 자세한 내용은 및 을 참조하십시오"클론 테넌트 그룹 및 사용자""API를 사용하여 S3 액세스 키의 클론을 생성합니다".

교차 그리드 복제란 무엇입니까?

그리드 간 복제는 에 연결된 두 StorageGRID 시스템에서 선택한 S3 버킷 간에 오브젝트를 자동 복제하는 것입니다"그리드 페더레이션 연결". "계정 클론" 그리드 간 복제에 필요합니다.

그리드 간 복제를 위한 워크플로우

워크플로우 다이어그램은 두 그리드에 있는 버킷 간의 크로스 그리드 복제를 구성하는 단계를 요약합니다.



크로스 그리드 복제 요구 사항

테넌트 계정에 하나 이상의 그리드 페더레이션 연결 사용 * 권한이 "그리드 페더레이션 연결"있는 경우 루트 액세스 권한이 있는 테넌트 사용자는 각 그리드의 해당 테넌트 계정에 동일한 버킷을 만들 수 있습니다. 이러한 버킷:

- 이름은 같아야 하지만 영역이 다를 수 있습니다
- 버전 관리가 활성화되어 있어야 합니다
- S3 오브젝트 잠금을 비활성화해야 합니다
- 비어 있어야 합니다

두 버킷이 모두 생성된 후 크로스 그리드 복제를 둘 중 하나 또는 두 버킷에 대해 구성할 수 있습니다.

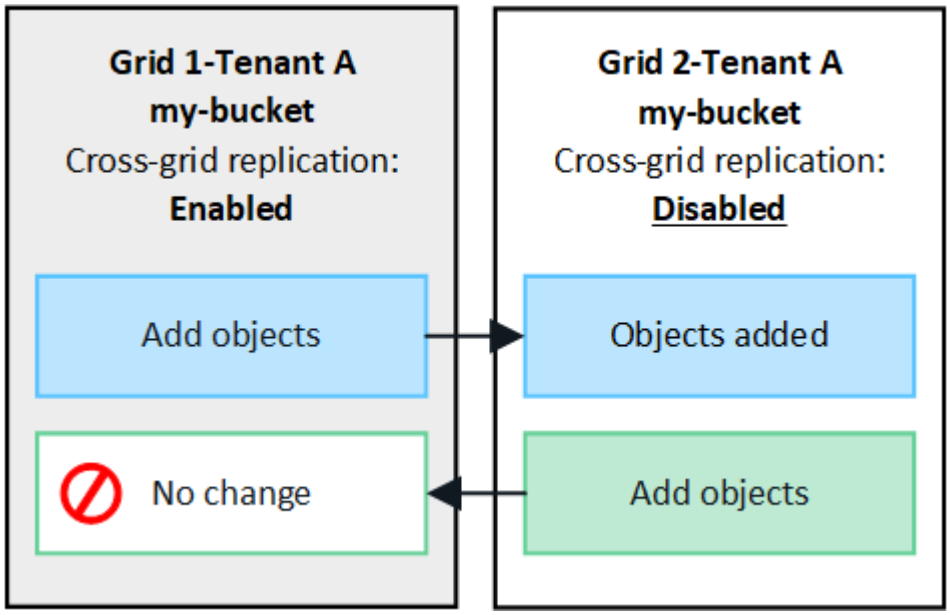
자세한 정보

"교차 그리드 복제 관리"

교차 그리드 복제는 한 방향 또는 양쪽 방향으로 실행되도록 구성할 수 있습니다.

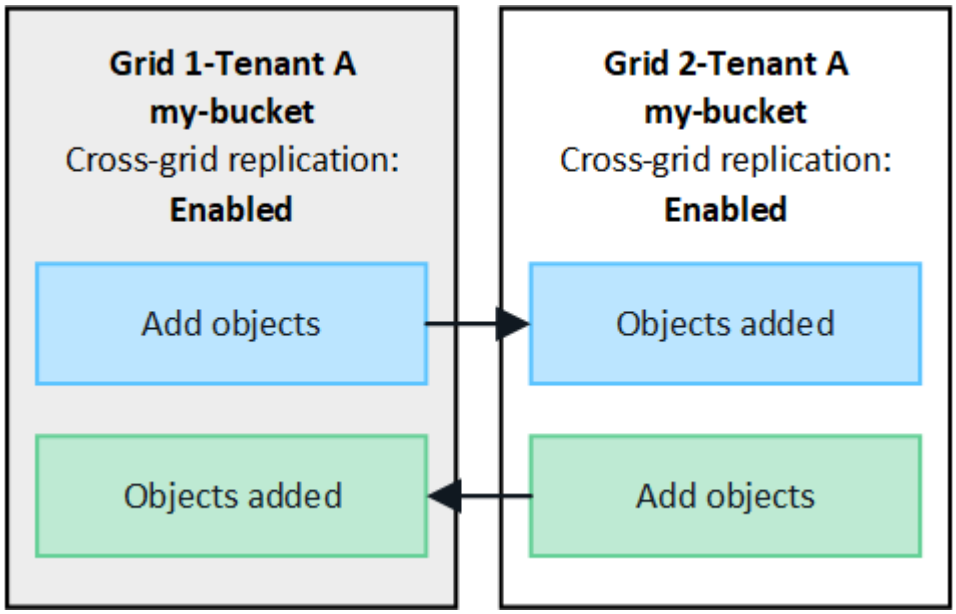
복제 기능을 제공합니다

하나의 그리드에서만 버킷에 대해 교차 그리드 복제를 활성화하면 해당 버킷(소스 버킷)에 추가된 객체가 다른 그리드(대상 버킷)의 해당 버킷에 복제됩니다. 하지만 대상 버킷에 추가된 오브젝트는 다시 소스에 복제되지 않습니다. 그림에서 그리드 1에서 그리드 2로 교차 그리드 복제가 활성화되지만 `my-bucket` 다른 방향에서는 활성화되지 않습니다.



양방향으로 복제

두 그리드에서 동일한 버킷에 대해 교차 그리드 복제를 활성화하면 두 버킷에 추가된 객체가 다른 그리드에 복제됩니다. 그림에서 교차 그리드 복제는 양방향으로 에 대해 `my-bucket` 활성화됩니다.



오브젝트를 수집하면 어떻게 됩니까?

S3 클라이언트가 교차 그리드 복제를 사용하도록 설정된 버킷에 오브젝트를 추가하면 다음과 같은 현상이 발생합니다.

1. StorageGRID는 소스 버킷에서 대상 버킷으로 오브젝트를 자동으로 복제합니다. 이 백그라운드 복제 작업을 수행하는 시간은 보류 중인 다른 복제 작업의 수를 비롯한 여러 요인에 따라 달라집니다.

   S3 클라이언트는 GetObject 또는 HeadObject 요청을 실행하여 개체의 복제 상태를 확인할 수 있습니다. 응답에는 다음 값 중 하나가 있는 StorageGRID 관련 `x-ntap-sg-cgr-replication-status` 응답 헤더가 포함됩니다. S3 클라이언트는 GetObject 또는 HeadObject 요청을 실행하여 개체의 복제 상태를 확인할 수 있습니다. 응답에는 다음 값 중 하나가 있는 StorageGRID 관련 `x-ntap-sg-cgr-replication-status` 응답 헤더가 포함됩니다.

그리드	복제 상태입니다
출처	• * 완료 *: 모든 그리드 연결에 대해 복제가 성공했습니다. • * 보류 중 *: 객체가 하나 이상의 그리드 연결에 복제되지 않았습니다. • * 실패 *: 그리드 연결에 대해 복제가 보류 중이 아니며 영구적인 장애로 인해 하나 이상의 복제가 실패했습니다. 사용자가 오류를 해결해야 합니다.
목적지	• replica *: 객체가 소스 그리드에서 복제되었습니다.

   StorageGRID는 헤더를 지원하지 `x-amz-replication-status` 않습니다.

2. StorageGRID는 다른 오브젝트와 마찬가지로 각 그리드의 활성 ILM 정책을 사용하여 오브젝트를 관리합니다. 예를 들어, 그리드 1의 오브젝트 A는 두 개의 복제된 복사본으로 저장되고 영구적으로 보존되는 반면, 그리드 2에 복제된 오브젝트 A는 2+1 삭제 코딩을 사용하여 저장하고 3년 후에 삭제될 수 있습니다.

오브젝트를 삭제하면 어떻게 됩니까?

에 설명된 대로 "데이터 흐름을 삭제합니다"StorageGRID는 다음과 같은 이유로 개체를 삭제할 수 있습니다.

- S3 클라이언트가 삭제 요청을 실행합니다.
- 테넌트 관리자 사용자는 "버킷에서 오브젝트를 삭제합니다"버킷에서 모든 오브젝트를 제거하는 옵션을 선택합니다.
- 버킷에는 수명 주기 구성이 만료되어 있습니다.
- 개체에 대한 ILM 규칙의 마지막 기간이 종료되며 더 이상 지정된 배치가 없습니다.

StorageGRID가 버킷 작업, 버킷 수명 주기 만료 또는 ILM 배치 만료에서 오브젝트 삭제로 인해 오브젝트를 삭제하면 그리드 통합 연결의 다른 그리드에서 복제된 오브젝트는 삭제되지 않습니다. 하지만 S3 클라이언트에서 소스 버킷에 추가된 삭제 마커는 선택적으로 대상 버킷에 복제할 수 있습니다.

S3 클라이언트가 교차 그리드 복제가 활성화된 버킷에서 오브젝트를 삭제할 때 어떤 일이 발생하는지 이해하려면 S3 클라이언트가 버전 관리가 활성화된 버킷에서 오브젝트를 삭제하는 방법을 다음과 같이 검토하십시오.

- S3 클라이언트가 버전 ID가 포함된 삭제 요청을 실행하면 해당 오브젝트 버전이 영구적으로 제거됩니다. 버킷에 추가된 삭제 마커가 없습니다.
- S3 클라이언트가 버전 ID가 포함되지 않은 삭제 요청을 발급하는 경우 StorageGRID은 오브젝트 버전을 삭제하지

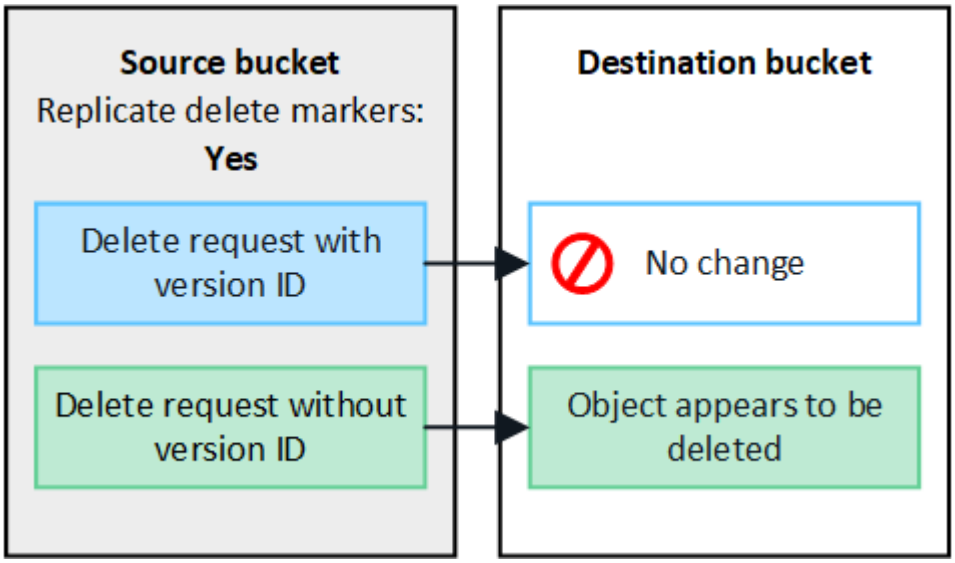
않습니다. 대신 삭제 표식이 버킷에 추가됩니다. 삭제 마커로 인해 StorageGRID는 객체가 삭제된 것처럼 작동합니다.

  - 버전 ID가 없는 GetObject 요청이 에서 실패합니다 `404 No Object Found`
  - 유효한 버전 ID를 가진 GetObject 요청이 성공하고 요청된 개체 버전을 반환합니다.

S3 클라이언트가 교차 그리드 복제가 활성화된 버킷에서 오브젝트를 삭제하면 StorageGRID은 다음과 같이 삭제 요청을 대상에 복제할지 여부를 결정합니다.

- 삭제 요청에 버전 ID가 포함되어 있으면 해당 개체 버전이 소스 그리드에서 영구적으로 제거됩니다. 그러나 StorageGRID는 버전 ID가 포함된 삭제 요청을 복제하지 않으므로 동일한 객체 버전이 대상에서 삭제되지 않습니다.
- 삭제 요청에 버전 ID가 포함되지 않은 경우 StorageGRID는 버킷에 대해 크로스 그리드 복제가 구성된 방식에 따라 삭제 마커를 선택적으로 복제할 수 있습니다.
  - 삭제 마커(기본값)를 복제하도록 선택하면 삭제 마커가 소스 버킷에 추가되고 대상 버킷에 복제됩니다. 실제로 두 그리드에서 오브젝트가 삭제된 것으로 나타납니다.
  - 삭제 마커를 복제하지 않도록 선택하면 삭제 마커가 소스 버킷에 추가되지만 대상 버킷에 복제되지 않습니다. 실제로 소스 그리드에서 삭제된 개체는 대상 그리드에서 삭제되지 않습니다.

그림에서 * Replicate delete marker * 는 * Yes * 로 설정되어 "교차 그리드 복제가 설정되었습니다"있습니다. 버전 ID가 포함된 소스 버킷에 대한 삭제 요청은 대상 버킷에서 오브젝트를 삭제하지 않습니다. 버전 ID가 포함되지 않은 소스 버킷에 대한 삭제 요청은 대상 버킷에서 오브젝트를 삭제하는 것으로 나타납니다.



그리드 간에 객체 삭제를 동기화된 상태로 유지하려면 "S3 라이프사이클 구성"양쪽 그리드에서 버킷을 생성합니다.

암호화된 개체가 복제되는 방식

교차 그리드 복제를 사용하여 그리드 간에 오브젝트를 복제할 때 개별 오브젝트를 암호화하거나 기본 버킷 암호화를 사용하거나 그리드 전체 암호화를 구성할 수 있습니다. 버킷에 대해 교차 그리드 복제를 활성화하기 전이나 후에 기본 버킷 또는 그리드 전체 암호화 설정을 추가, 수정 또는 제거할 수 있습니다.

개별 오브젝트를 암호화하려면 소스 버킷에 오브젝트를 추가할 때 SSE(StorageGRID 관리 키가 있는 서버 측 암호화)를 사용할 수 있습니다. `x-amz-server-side-encryption`요청 헤더를 사용하고 를 지정하십시오

`AES256. 을 "서버측 암호화를 사용합니다"참조하십시오.

> SSE-C(고객이 제공한 키와 서버측 암호화)를 사용하는 것은 교차 그리드 복제의 경우 지원되지 않습니다. 수집 작업이 실패합니다.

버킷에 기본 암호화를 사용하려면 PutBucketEncryption 요청을 사용하고 `SSEAlgorithm` 매개 변수를 로 `AES256`설정합니다. 버킷 수준 암호화는 요청 헤더 없이 수집된 모든 객체에 `x-amz-server-side-encryption` 적용됩니다. 을 "버킷 작업"참조하십시오.

그리드 수준 암호화를 사용하려면 * 저장된 오브젝트 암호화 * 옵션을 * AES-256 * 로 설정합니다. 그리드 수준 암호화는 버킷 수준에서 암호화되지 않거나 요청 헤더 없이 수집된 모든 오브젝트에 `x-amz-server-side-encryption` 적용됩니다. 을 "네트워크 및 개체 옵션을 구성합니다"참조하십시오.

> SSE는 AES-128을 지원하지 않습니다. AES-128 * 옵션을 사용하여 소스 그리드에 대해 * Stored object encryption * 옵션을 활성화하면 AES-128 알고리즘 사용이 복제된 오브젝트로 전파되지 않습니다. 대신, 가능한 경우 복제된 객체는 대상의 기본 버킷 또는 그리드 레벨 암호화 설정을 사용합니다.

소스 객체를 암호화하는 방법을 결정할 때 StorageGRID는 다음 규칙을 적용합니다.

1. `x-amz-server-side-encryption`인제스트 헤더가 있는 경우 사용합니다.
2. 수집 헤더가 없는 경우 구성된 경우 버킷 기본 암호화 설정을 사용합니다.
3. 버킷 설정이 구성되지 않은 경우 그리드 전체 암호화 설정을 사용합니다(구성된 경우).
4. 눈금 단위 설정이 없으면 소스 개체를 암호화하지 마십시오.

복제된 개체를 암호화하는 방법을 결정할 때 StorageGRID는 다음 규칙을 다음 순서로 적용합니다.

1. 해당 개체에서 AES-128 암호화를 사용하지 않는 한 소스 객체와 동일한 암호화를 사용합니다.
2. 소스 객체가 암호화되지 않았거나 AES-128을 사용하는 경우, 구성된 경우 대상 버킷의 기본 암호화 설정을 사용합니다.
3. 대상 버킷에 암호화 설정이 없는 경우 구성된 경우 대상의 전체 그리드 암호화 설정을 사용합니다.
4. 눈금 단위 설정이 없으면 대상 개체를 암호화하지 마십시오.

PutObjectTagging 및 **DeleteObjectTagging**은 지원되지 않습니다

PutObjectTagging 및 DeleteObjectTagging 요청은 교차 그리드 복제가 활성화된 버킷의 객체에 대해 지원되지 않습니다.

S3 클라이언트가 PutObjectTagging 또는 DeleteObjectTagging 요청을 실행하면 `501 Not Implemented` 이 반환됩니다. 메시지는 입니다 `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured.`

분할된 객체가 복제되는 방식

소스 그리드의 최대 세그먼트 크기는 대상 그리드에 복제된 객체에 적용됩니다. 개체를 다른 그리드에 복제하면 소스 그리드의 * 최대 세그먼트 크기 * 설정(* 구성 * > * 시스템 * > * 스토리지 옵션 *)이 두 그리드에 모두 사용됩니다. 예를 들어 소스 그리드의 최대 세그먼트 크기가 1GB이고 대상 그리드의 최대 세그먼트 크기는 50MB라고 가정합니다. 소스 그리드에서 2GB 오브젝트를 수집하는 경우 해당 오브젝트는 두 개의 1GB 세그먼트로 저장됩니다. 또한 그리드의 최대

세그먼트 크기가 50MB인 경우에도 대상 그리드에 1GB 세그먼트 2개로 복제됩니다.

교차 그리드 복제와 **CloudMirror** 복제를 비교합니다

그리드 페더레이션을 사용하기 시작할 때 및 의 유사점과 차이점을 "교차 그리드 복제 ""StorageGRID CloudMirror 복제 서비스입니다"검토하십시오.

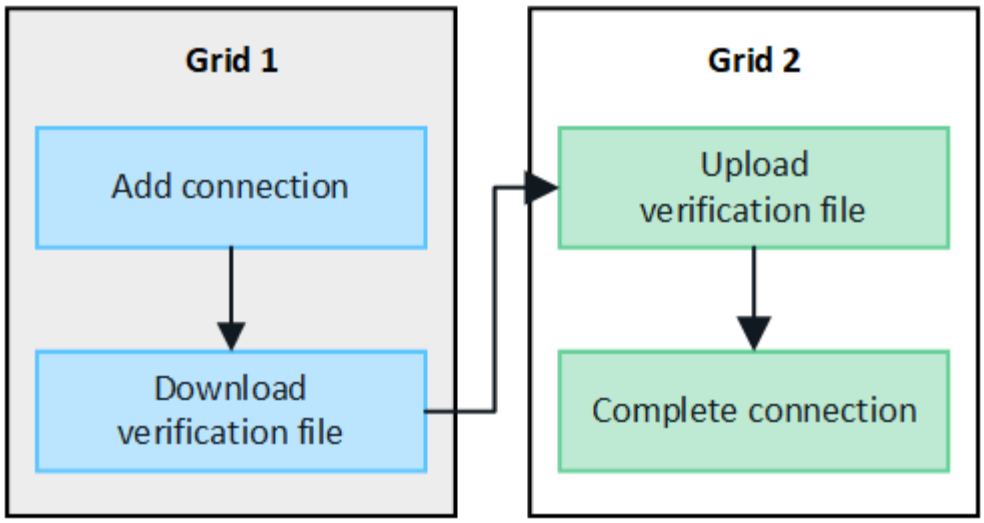
	교차 그리드 복제	**CloudMirror** 복제 서비스
주요 목적은 무엇입니까?	하나의 StorageGRID 시스템이 재해 복구 시스템 역할을 합니다. 버킷의 오브젝트는 한 방향 또는 두 방향으로 그리드 간에 복제될 수 있습니다.	테넌트가 StorageGRID(소스)의 버킷에서 외부 S3 버킷(대상)으로 오브젝트를 자동으로 복제할 수 있습니다. CloudMirror 복제는 독립 S3 인프라에서 개체의 독립적인 복사본을 생성합니다. 이 독립 복제본은 백업으로 사용되지 않고 클라우드에서 추가로 처리되는 경우가 많습니다.
어떻게 설정합니까?	1. 두 그리드 간의 그리드 페더레이션 연결을 구성합니다. 2. 다른 그리드에 자동으로 클론이 생성되는 새 테넌트 계정을 추가합니다. 3. 클론 복제된 새 테넌트 그룹 및 사용자를 추가합니다. 4. 각 그리드에 해당하는 버킷을 생성하고 교차 그리드 복제가 한 방향 또는 양쪽 방향으로 이루어질 수 있도록 합니다.	1. 테넌트 사용자는 테넌트 관리자 또는 S3 API를 사용하여 CloudMirror 엔드포인트(IP 주소, 자격 증명 등)를 정의하여 CloudMirror 복제를 구성합니다. 2. 해당 테넌트 계정이 소유한 버킷은 CloudMirror 엔드포인트를 가리키도록 구성할 수 있습니다.
누가 설정해야 합니까?	• 그리드 관리자는 접속 및 테넌트를 구성합니다. • 테넌트 사용자는 그룹, 사용자, 키 및 버킷을 구성합니다.	일반적으로 테넌트 사용자입니다.
대상은 무엇입니까?	그리드 페더레이션 연결에서 다른 StorageGRID 시스템에 있는 상응하는 동일한 S3 버킷.	• 모든 호환 가능한 S3 인프라(Amazon S3 포함). • Google Cloud Platform(GCP)
오브젝트 버전 관리가 필요합니까?	예. 소스 및 대상 버킷 모두에 오브젝트 버전 관리가 활성화되어 있어야 합니다.	아니요. CloudMirror 복제는 소스 및 대상 모두에서 버전이 지정되지 않은 버킷과 버전 관리가 된 버킷의 조합을 지원합니다.
오브젝트를 대상으로 이동하는 원인은 무엇입니까?	객체가 교차 그리드 복제가 활성화된 버킷에 추가되면 자동으로 복제됩니다.	객체는 CloudMirror 엔드포인트로 구성된 버킷에 추가될 때 자동으로 복제됩니다. 버킷이 CloudMirror 엔드포인트로 구성되기 전에 소스 버킷에 있던 객체는 수정되지 않으면 복제되지 않습니다.

	교차 그리드 복제	**CloudMirror** 복제 서비스
객체는 어떻게 복제됩니까?	교차 그리드 복제는 버전이 있는 오브젝트를 생성하고 소스 버킷에서 대상 버킷으로 버전 ID를 복제합니다. 이렇게 하면 버전 순서가 양쪽 그리드에 걸쳐 유지됩니다.	CloudMirror 복제에는 버전 관리가 활성화된 버킷이 필요하지 않으므로 CloudMirror는 사이트 내의 키에 대한 주문만 유지할 수 있습니다. 다른 사이트의 개체에 대한 요청에 대해 주문이 유지되도록 보장하는 것은 없습니다.
개체를 복제할 수 없는 경우 어떻게 해야 합니까?	객체는 메타데이터 스토리지 제한에 따라 복제 대기열에 추가됩니다.	플랫폼 서비스 제한에 따라 객체가 복제를 위해 대기하고 있습니다(참조"플랫폼 서비스 사용을 위한 권장 사항").
개체의 시스템 메타데이터가 복제됩니까?	예. 객체가 다른 그리드에 복제되면 해당 시스템 메타데이터도 복제됩니다. 메타데이터는 두 그리드에서 모두 동일합니다.	아니요. 객체가 외부 버킷에 복제되면 해당 시스템 메타데이터가 업데이트됩니다. 메타데이터는 수집 시간과 독립적인 S3 인프라의 동작에 따라 여러 위치에 따라 달라집니다.
객체를 검색하는 방법은 무엇입니까?	애플리케이션은 두 그리드 중 하나의 버킷에 대한 요청을 함으로써 객체를 검색하거나 읽을 수 있습니다.	애플리케이션은 StorageGRID 또는 S3 대상을 요청하여 오브젝트를 검색하거나 읽을 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.
개체를 삭제하면 어떻게 됩니까?	• 버전 ID가 포함된 삭제 요청은 대상 그리드에 복제되지 않습니다. • 버전 ID가 포함되지 않은 삭제 요청은 소스 버킷에 삭제 마커를 추가합니다. 이 마커는 대상 그리드에 선택적으로 복제할 수 있습니다. • 교차 그리드 복제가 한 방향으로만 구성된 경우 소스에 영향을 주지 않고 대상 버킷의 오브젝트를 삭제할 수 있습니다.	결과는 소스 및 대상 버킷의 버전 관리 상태에 따라 달라집니다(동일할 필요는 없음). • 두 버킷의 버전이 모두 설정된 경우 삭제 요청은 두 위치에 삭제 마커를 추가합니다. • 소스 버킷만 버전 관리되는 경우 삭제 요청이 원본에 삭제 표식을 추가하지만 대상에는 추가하지 않습니다. • 버킷의 버전이 지정되지 않은 경우 삭제 요청이 소스에서 개체를 삭제하지만 대상에서 삭제하지는 않습니다. 마찬가지로, 소스에 영향을 주지 않고 대상 버킷의 오브젝트를 삭제할 수 있습니다.

그리드 페더레이션 연결을 만듭니다

테넌트 세부 정보의 클론을 생성하고 객체 데이터를 복제하려는 경우 두 StorageGRID 시스템 간에 그리드 페더레이션 연결을 생성할 수 있습니다.

그림에 표시된 것처럼 그리드 페더레이션 연결을 만드는 작업은 두 그리드 모두에 대한 단계를 포함합니다. 한 그리드에 연결을 추가하고 다른 그리드에서 연결을 완료합니다. 두 눈금 중 하나에서 시작할 수 있습니다.



시작하기 전에

- 그리드 페더레이션 연결을 구성하기 위해 을 검토했습니다."고려 사항 및 요구 사항"
- IP 또는 VIP 주소 대신 각 그리드에 대해 FQDN(정규화된 도메인 이름)을 사용하려는 경우 사용할 이름을 알고 각 그리드의 DNS 서버에 적절한 항목이 있는지 확인합니다.
- 을 사용하고 "지원되는 웹 브라우저"있습니다.
- 두 그리드 모두에 대한 루트 액세스 권한과 프로비저닝 암호가 있습니다.

연결을 추가합니다

두 StorageGRID 시스템 중 하나에서 다음 단계를 수행합니다.

단계

1. 두 그리드 중 하나의 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
2. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.
3. 연결 추가 * 를 선택합니다.
4. 연결에 대한 세부 정보를 입력합니다.

필드에 입력합니다	설명
연결 이름입니다	이 연결을 쉽게 인식할 수 있는 고유한 이름(예: "그리드 1 - 그리드 2")
이 그리드의 FQDN 또는 IP입니다	다음 중 하나: • 현재 로그인한 그리드의 FQDN입니다 • 이 그리드에서 HA 그룹의 VIP 주소입니다 • 이 그리드에 있는 관리 노드 또는 게이트웨이 노드의 IP 주소입니다. IP는 대상 그리드가 연결할 수 있는 모든 네트워크에 있을 수 있습니다.

필드에 입력합니다	설명
포트	이 연결에 사용할 포트입니다. 사용하지 않는 포트 번호는 23000에서 23999까지 입력할 수 있습니다. 이 연결의 두 그리드는 동일한 포트를 사용합니다. 두 그리드 중 어떤 노드도 다른 연결에 이 포트를 사용하지 않도록 해야 합니다.
이 그리드에 대한 인증서 유효 일일입니다	연결에서 이 그리드에 대한 보안 인증서를 유효하게 만들 일 수입니다. 기본값은 730일(2년)이지만 1일에서 762일 사이의 값을 입력할 수 있습니다. StorageGRID는 연결을 저장할 때 각 그리드에 대해 클라이언트 및 서버 인증서를 자동으로 생성합니다.
이 그리드에 대한 프로비저닝 암호입니다	로그인한 그리드의 프로비저닝 암호입니다.
다른 그리드의 FQDN 또는 IP입니다	다음 중 하나: • 연결할 그리드의 FQDN입니다 • 다른 그리드에서 HA 그룹의 VIP 주소입니다 • 다른 그리드에 있는 관리 노드 또는 게이트웨이 노드의 IP 주소입니다. IP는 소스 그리드가 연결할 수 있는 모든 네트워크에 있을 수 있습니다.

5. Save and continue * 를 선택합니다.
6. 다운로드 확인 파일 단계에서 * 확인 파일 다운로드 * 를 선택합니다.

   다른 그리드에서 연결이 완료된 후에는 두 그리드 중 하나에서 확인 파일을 더 이상 다운로드할 수 없습니다.

7. 다운로드한 파일을 찾아 (`*connection-name*.grid-federation`안전한 위치에 저장합니다.

   이 파일에는 비밀(마스킹된 AS) 및 기타 민감한 정보가 포함되어 * 있으므로 안전하게 저장하고 전송해야 합니다.

8. 그리드 페더레이션 페이지로 돌아가려면 * 닫기 * 를 선택합니다.
9. 새 연결이 표시되고 해당 * 연결 상태 * 가 * 연결 대기 * 인지 확인합니다.
10. `*connection-name*.grid-federation`다른 그리드의 그리드 관리자에게 파일을 제공합니다.

연결을 완료합니다

연결 중인 StorageGRID 시스템(다른 그리드)에서 다음 단계를 수행합니다.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
2. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.

3. 업로드 페이지에 액세스하려면 * 검증 파일 업로드 * 를 선택합니다.
4. 검증 파일 업로드 * 를 선택합니다. 그런 다음 첫 번째 그리드에서 다운로드한 파일을 찾아 (`*connection-name*.grid-federation`선택합니다).

   연결에 대한 세부 정보가 표시됩니다.

5. 필요에 따라 이 그리드의 보안 인증서에 대해 다른 유효 일수를 입력합니다. 인증서 유효 일 * 항목은 기본적으로 첫 번째 그리드에 입력한 값으로 설정되지만 각 그리드에는 서로 다른 만료 날짜를 사용할 수 있습니다.

   일반적으로 연결의 양쪽에 있는 인증서에 대해 동일한 일 수를 사용합니다.

   > 연결 끝 중 하나의 인증서가 만료되면 연결이 중지되고 인증서가 업데이트될 때까지 복제가 보류됩니다.

6. 현재 로그인한 그리드의 프로비저닝 암호를 입력합니다.
7. Save and test * 를 선택합니다.

   인증서가 생성되고 연결이 테스트됩니다. 연결이 유효한 경우 성공 메시지가 나타나고 새 연결이 그리드 페더레이션 페이지에 나열됩니다. 연결 상태 * 는 * 연결됨 * 이 됩니다.

   오류 메시지가 나타나면 문제를 해결하십시오. 을 "그리드 통합 오류 문제 해결"참조하십시오.

8. 첫 번째 그리드의 그리드 페더레이션 페이지로 이동하여 브라우저를 새로 고칩니다. 연결 상태 * 가 지금 * 연결됨 * 인지 확인합니다.
9. 연결이 설정되면 확인 파일의 모든 복사본을 안전하게 삭제합니다.

   이 연결을 편집하면 새 확인 파일이 생성됩니다. 원본 파일을 다시 사용할 수 없습니다.

작업을 마친 후

- 에 대한 고려 사항을 "허용된 테넌트 관리"검토합니다.
- "하나 이상의 새 테넌트 계정을 생성합니다"을 클릭하고 * 그리드 페더레이션 연결 사용 * 권한을 할당하고 새 연결을 선택합니다.
- "연결을 관리합니다" 필요한 경우. 연결 값을 편집하거나, 연결을 테스트하거나, 연결 인증서를 회전하거나, 연결을 제거할 수 있습니다.
- "연결을 모니터링합니다" 를 일반적인 StorageGRID 모니터링 활동의 일부로 활용합니다.
- "연결 문제를 해결합니다"계정 클론 및 교차 그리드 복제와 관련된 경고 및 오류 해결을 포함합니다.

그리드 페더레이션 연결을 관리합니다

StorageGRID 시스템 간의 그리드 페더레이션 연결 관리에는 연결 세부 정보 편집, 인증서 회전, 테넌트 권한 제거 및 사용되지 않는 연결 제거가 포함됩니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 로그인한 그리드에 대한 가 "루트 액세스 권한"있습니다.

[[EDIT_GRID_FED_CONNECTION]] 그리드 페더레이션 연결을 편집합니다

연결의 두 그리드 중 하나에서 기본 관리 노드에 로그인하여 그리드 페더레이션 연결을 편집할 수 있습니다. 첫 번째 그리드를 변경한 후에는 새 검증 파일을 다운로드하여 다른 그리드에 업로드해야 합니다.

> ⓘ 연결을 편집하는 동안 계정 클론 또는 교차 그리드 복제 요청은 기존 연결 설정을 계속 사용합니다. 첫 번째 격자에 대한 편집 내용은 로컬에 저장되지만 두 번째 격자에 업로드되고 저장 및 테스트될 때까지 사용되지 않습니다.

연결 편집을 시작합니다

단계

1. 두 그리드 중 하나의 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
2. nodes * 를 선택하고 시스템의 다른 모든 관리 노드가 온라인 상태인지 확인합니다.

   > ⓘ 그리드 페더레이션 연결을 편집할 때 StorageGRID는 첫 번째 그리드의 모든 관리 노드에 "대상 구성" 파일을 저장하려고 시도합니다. 이 파일을 모든 관리 노드에 저장할 수 없는 경우 * 저장 및 테스트 * 를 선택하면 경고 메시지가 나타납니다.

3. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.
4. 그리드 페더레이션 페이지의 * 작업 * 메뉴 또는 특정 연결에 대한 세부 정보 페이지를 사용하여 연결 세부 정보를 편집합니다. 입력할 항목은 을 "그리드 페더레이션 연결을 만듭니다"참조하십시오.

   작업 메뉴

   a. 연결에 사용할 라디오 버튼을 선택합니다.
   b. Actions * > * Edit * 를 선택합니다.
   c. 새 정보를 입력합니다.

   세부 정보 페이지

   a. 세부 정보를 표시할 연결 이름을 선택합니다.
   b. 편집 * 을 선택합니다.
   c. 새 정보를 입력합니다.

5. 로그인한 그리드의 프로비저닝 암호를 입력합니다.
6. Save and continue * 를 선택합니다.

   새 값은 저장되지만 다른 그리드에 새 검증 파일을 업로드하기 전에는 연결에 적용되지 않습니다.

7. 검증 파일 다운로드 * 를 선택합니다.

   나중에 이 파일을 다운로드하려면 연결에 대한 세부 정보 페이지로 이동합니다.

8. 다운로드한 파일을 찾아 (`*connection-name*.grid-federation`안전한 위치에 저장합니다.

   > ⓘ 확인 파일에는 비밀이 포함되어 있으며 안전하게 저장하고 전송해야 합니다.

9. 그리드 페더레이션 페이지로 돌아가려면 * 닫기 * 를 선택합니다.
10. 연결 상태 * 가 * 편집 보류 * 인지 확인합니다.

    연결 편집을 시작할 때 연결 상태가 * 연결됨 * 이 아닌 경우 * 편집 보류 * 로 변경되지 않습니다.

11. `*connection-name*.grid-federation`다른 그리드의 그리드 관리자에게 파일을 제공합니다.

연결 편집을 마칩니다

다른 그리드에 확인 파일을 업로드하여 연결 편집을 마칩니다.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
2. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.
3. 업로드 페이지에 액세스하려면 * 검증 파일 업로드 * 를 선택합니다.
4. 검증 파일 업로드 * 를 선택합니다. 그런 다음 첫 번째 그리드에서 다운로드한 파일을 찾아 선택합니다.
5. 현재 로그인한 그리드의 프로비저닝 암호를 입력합니다.
6. Save and test * 를 선택합니다.

   편집한 값을 사용하여 연결을 설정할 수 있으면 성공 메시지가 나타납니다. 그렇지 않으면 오류 메시지가 나타납니다. 메시지를 검토하고 문제를 해결합니다.

7. 마법사를 닫고 그리드 페더레이션 페이지로 돌아갑니다.
8. 연결 상태 * 가 * 연결됨 * 인지 확인합니다.
9. 첫 번째 그리드의 그리드 페더레이션 페이지로 이동하여 브라우저를 새로 고칩니다. 연결 상태 * 가 지금 * 연결됨 * 인지 확인합니다.
10. 연결이 설정되면 확인 파일의 모든 복사본을 안전하게 삭제합니다.

[[TEST_GRID_FED_CONNECTION] 그리드 페더레이션 연결을 테스트합니다

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
2. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.
3. 그리드 페더레이션 페이지의 * 작업 * 메뉴 또는 특정 연결에 대한 세부 정보 페이지를 사용하여 연결을 테스트합니다.

작업 메뉴

a. 연결에 사용할 라디오 버튼을 선택합니다.

b. Actions * > * Test * 를 선택합니다.

세부 정보 페이지

a. 세부 정보를 표시할 연결 이름을 선택합니다.

b. Test connection * 을 선택합니다.

4. 연결 상태를 검토합니다.

연결 상태입니다	설명
연결되었습니다	두 그리드 모두 연결되어 있고 정상적으로 통신하고 있습니다.
오류	연결이 오류 상태입니다. 예를 들어 인증서가 만료되었거나 구성 값이 더 이상 유효하지 않습니다.
편집 보류 중	이 그리드에서 연결을 편집했지만 연결이 여전히 기존 구성을 사용하고 있습니다. 편집을 완료하려면 새 검증 파일을 다른 그리드에 업로드합니다.
연결 대기 중입니다	이 그리드에서 연결을 구성했지만 다른 그리드에서 연결이 완료되지 않았습니다. 이 그리드에서 확인 파일을 다운로드하여 다른 그리드에 업로드합니다.
알 수 없음	네트워크 문제 또는 오프라인 노드로 인해 연결이 알 수 없는 상태입니다.

5. 연결 상태가 * 오류 * 인 경우 모든 문제를 해결하십시오. 그런 다음 * Test connection * 을 다시 선택하여 문제가 해결되었는지 확인합니다.

연결 인증서를 회전합니다

각 그리드 페더레이션 연결은 자동으로 생성된 4개의 SSL 인증서를 사용하여 연결을 보호합니다. 각 그리드의 만료 날짜 근처에 두 개의 인증서가 있으면 * 그리드 페더레이션 인증서 만료 * 알림이 인증서를 회전하도록 알려 줍니다.

연결 끝 중 하나의 인증서가 만료되면 연결이 중지되고 인증서가 업데이트될 때까지 복제가 보류됩니다.

단계

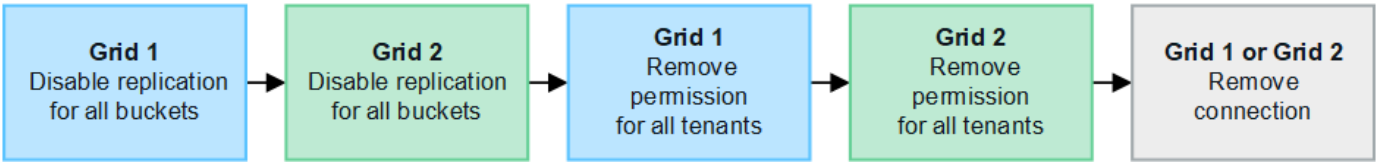
1. 두 그리드 중 하나의 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
2. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.
3. Grid Federation(그리드 통합) 페이지의 어느 탭에서든 세부 정보를 표시할 연결 이름을 선택합니다.
4. 인증서 * 탭을 선택합니다.
5. 인증서 회전 * 을 선택합니다.
6. 새 인증서가 유효해야 하는 일 수를 지정합니다.

7. 로그인한 그리드의 프로비저닝 암호를 입력합니다.
8. 인증서 회전 * 을 선택합니다.
9. 필요에 따라 연결의 다른 격자에서 이 단계를 반복합니다.

   일반적으로 연결의 양쪽에 있는 인증서에 대해 동일한 일 수를 사용합니다.

그리드 페더레이션 연결을 제거합니다

연결의 각 그리드에서 그리드 페더레이션 연결을 제거할 수 있습니다. 그림에 표시된 것처럼 두 그리드에 대해 선행 단계를 수행하여 두 그리드 중 하나의 테넌트에서 연결이 사용되고 있지 않은지 확인해야 합니다.



연결을 제거하기 전에 다음 사항에 유의하십시오.

- 연결을 제거해도 그리드 간에 이미 복사된 항목은 삭제되지 않습니다. 예를 들어, 테넌트의 권한이 제거되면 두 그리드에 있는 테넌트 사용자, 그룹 및 객체가 두 그리드 모두에서 삭제되지 않습니다. 이러한 항목을 삭제하려면 두 그리드 모두에서 수동으로 삭제해야 합니다.
- 연결을 제거하면 대기 중인 복제(수집되었지만 아직 다른 그리드에 복제되지 않은) 객체가 영구적으로 복제되지 않습니다.

모든 테넌트 버킷에 대한 복제를 비활성화합니다

단계

1. 두 그리드 중 하나에서 시작하여 기본 관리 노드에서 그리드 관리자에 로그인합니다.
2. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.
3. 세부 정보를 표시할 연결 이름을 선택합니다.
4. 허용된 테넌트 * 탭에서 테넌트가 연결을 사용 중인지 확인합니다.
5. 테넌트가 나열되면 모든 테넌트가 연결의 두 그리드에 있는 모든 버킷에 대해 에 지시합니다."크로스 그리드 복제를 비활성화합니다"

> 테넌트 버킷에 교차 그리드 복제가 활성화된 경우 * 그리드 통합 연결 사용 * 권한을 제거할 수 없습니다. 각 테넌트 계정은 양쪽 그리드의 해당 버킷에 대해 교차 그리드 복제를 비활성화해야 합니다.

각 테넌트에 대한 권한을 제거합니다

모든 테넌트 버킷에 대해 교차 그리드 복제를 비활성화한 후 두 그리드의 모든 테넌트에서 * 그리드 통합 사용 권한 * 을 제거합니다.

단계

1. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.
2. 세부 정보를 표시할 연결 이름을 선택합니다.

3. 허용된 테넌트 * 탭의 각 테넌트에 대해 각 테넌트에서 * 그리드 페더레이션 연결 사용 * 권한을 제거합니다. 을 "허용된 테넌트 관리"참조하십시오.
4. 다른 그리드에서 허용된 테넌트에 대해 이 단계를 반복합니다.

연결을 제거합니다

단계

1. 두 그리드 중 어느 한 테넌트가 연결을 사용하고 있지 않으면 * 제거 * 를 선택합니다.
2. 확인 메시지를 검토하고 * 제거 * 를 선택합니다.
   - 연결을 제거할 수 있는 경우 성공 메시지가 표시됩니다. 그리드 페더레이션 연결이 이제 두 그리드에서 제거됩니다.
   - 연결을 제거할 수 없는 경우(예: 여전히 사용 중이거나 연결 오류가 있는 경우) 오류 메시지가 표시됩니다. 다음 중 하나를 수행할 수 있습니다.
     - 오류를 해결합니다(권장). 을 "그리드 통합 오류 문제 해결"참조하십시오.
     - 강제로 연결을 제거합니다. 다음 섹션을 참조하십시오.

그리드 페더레이션 연결을 강제로 제거합니다

필요한 경우 * Connected * 상태가 없는 연결을 강제로 제거할 수 있습니다.

강제 제거는 로컬 격자에서 연결을 삭제만 합니다. 연결을 완전히 제거하려면 두 그리드에서 동일한 단계를 수행합니다.

단계

1. 확인 대화 상자에서 * 강제 제거 * 를 선택합니다.

   성공 메시지가 나타납니다. 이 그리드 페더레이션 연결은 더 이상 사용할 수 없습니다. 그러나 테넌트 버킷은 여전히 교차 그리드 복제를 사용하고 일부 오브젝트 복사본은 연결의 그리드 간에 이미 복제되었을 수 있습니다.

2. 연결의 다른 그리드에서 기본 관리 노드에서 그리드 관리자에 로그인합니다.
3. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.
4. 세부 정보를 표시할 연결 이름을 선택합니다.
5. 제거 * 및 * 예 * 를 선택합니다.
6. 이 그리드에서 연결을 제거하려면 * 강제 제거 * 를 선택합니다.

그리드 페더레이션을 위해 허용된 테넌트를 관리합니다

S3 테넌트 계정에서 두 StorageGRID 시스템 간의 그리드 페더레이션 연결을 사용하도록 허용할 수 있습니다. 테넌트가 연결을 사용할 수 있는 경우 테넌트 세부 정보를 편집하거나 연결을 사용할 테넌트의 권한을 영구적으로 제거하려면 특별한 단계가 필요합니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 로그인한 그리드에 대한 가 "루트 액세스 권한"있습니다.
- "그리드 페더레이션 연결을 만들었습니다"두 그리드 사이에 있습니다.

- 및 에 대한 워크플로를 검토했습니다."계정 클론""교차 그리드 복제"
- 필요한 경우 이미 SSO(Single Sign-On)를 구성했거나 연결의 두 그리드에 대한 페더레이션을 식별했습니다. 을 "계정 클론이란 무엇입니까"참조하십시오.

허용된 테넌트를 생성합니다

새 테넌트 계정이나 기존 테넌트 계정에서 계정 클론 생성 및 교차 그리드 복제에 그리드 페더레이션 연결을 사용하도록 허용하려면 또는 "테넌트 계정을 편집합니다"의 일반 지침을 "새 S3 테넌트를 생성합니다"따르고 다음 사항에 유의하십시오.

- 연결의 두 그리드 중 하나에서 테넌트를 생성할 수 있습니다. 테넌트가 생성되는 그리드는 _ 테넌트의 소스 그리드 _ 입니다.
- 연결 상태는 * 연결됨 * 이어야 합니다.
- 테넌트를 만들거나 편집하여 * 그리드 페더레이션 연결 사용 * 권한을 활성화한 다음 첫 번째 그리드에 저장하면 동일한 테넌트가 자동으로 다른 그리드에 복제됩니다. 테넌트가 복제되는 그리드는 _ 테넌트의 대상 그리드 _ 입니다.
- 두 그리드의 테넌트는 동일한 20자리 계정 ID, 이름, 설명, 할당량 및 권한을 갖습니다. 선택적으로 * Description * 필드를 사용하여 소스 테넌트와 대상 테넌트를 식별할 수 있습니다. 예를 들어 그리드 1에서 생성된 테넌트에 대한 이 설명은 그리드 2에 복제된 테넌트에 대해서도 나타납니다. "이 테넌트는 그리드 1에 생성되었습니다."
- 보안상의 이유로 로컬 루트 사용자의 암호는 대상 그리드에 복사되지 않습니다.

> 로컬 루트 사용자가 대상 그리드에서 복제된 테넌트에 로그인하려면 먼저 해당 그리드의 그리드 관리자가 있어야 "로컬 루트 사용자의 암호를 변경합니다"합니다.

- 두 그리드 모두에서 새 테넌트 또는 편집된 테넌트를 사용할 수 있게 되면 테넌트 사용자는 다음 작업을 수행할 수 있습니다.
  - 테넌트의 소스 그리드에서 그룹과 로컬 사용자를 생성합니다. 이 그룹은 테넌트의 대상 그리드에 자동으로 복제됩니다. 을 "클론 테넌트 그룹 및 사용자"참조하십시오.
  - 필요에 따라 테넌트의 대상 그리드에 클론 복제할 수 있는 새 S3 액세스 키를 생성합니다. 을 "API를 사용하여 S3 액세스 키의 클론을 생성합니다"참조하십시오.
  - 연결의 두 그리드에 동일한 버킷을 생성하고 한 방향 또는 양쪽 방향에서 크로스 그리드 복제를 가능하게 합니다. 을 "교차 그리드 복제 관리"참조하십시오.

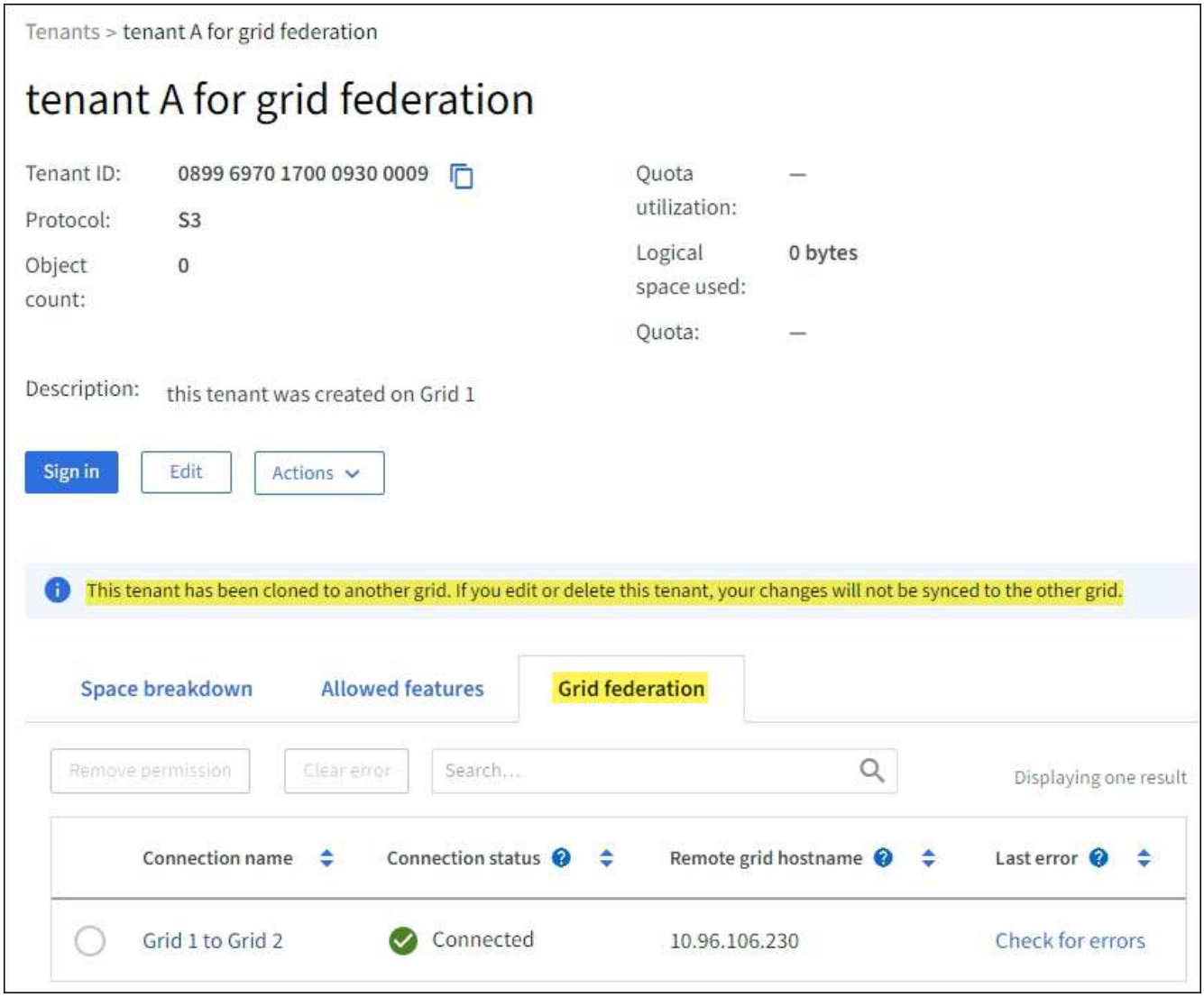
허용된 테넌트를 봅니다

그리드 페더레이션 연결을 사용하도록 허용된 테넌트에 대한 세부 정보를 볼 수 있습니다.

단계

1. Tenants * 를 선택합니다.
2. 테넌트 페이지에서 테넌트 이름을 선택하여 테넌트 세부 정보 페이지를 표시합니다.

   테넌트의 소스 그리드(즉, 테넌트가 이 그리드에 생성된 경우)인 경우 테넌트가 다른 그리드에 클론 생성되었다는 배너가 나타납니다. 이 테넌트를 편집하거나 삭제하면 변경 내용이 다른 눈금에 동기화되지 않습니다.



3. 필요에 따라 에 * Grid Federation * 탭을 선택합니다"그리드 페더레이션 연결을 모니터링합니다".

허용된 테넌트를 편집합니다

그리드 페더레이션 연결 사용* 권한이 있는 테넌트를 편집해야 하는 경우 에 대한 일반 지침을 "테넌트 계정 편집"따르고 다음 사항에 유의하십시오.

- 테넌트에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 연결의 각 그리드에서 테넌트 세부 정보를 편집할 수 있습니다. 그러나 변경한 내용은 다른 눈금에 복사되지 않습니다. 테넌트 세부 정보를 그리드 간에 동기화된 상태로 유지하려면 두 그리드에 대해 동일한 편집 작업을 수행해야 합니다.
- 테넌트를 편집할 때 * 그리드 페더레이션 연결 사용 * 권한을 지울 수 없습니다.
- 테넌트를 편집할 때는 다른 그리드 페더레이션 연결을 선택할 수 없습니다.

허용된 테넌트를 삭제합니다

그리드 페더레이션 연결 사용* 권한이 있는 테넌트를 제거해야 하는 경우 에 대한 일반 지침을 "테넌트 계정을 삭제하는 중입니다"따르고 다음 사항에 유의하십시오.

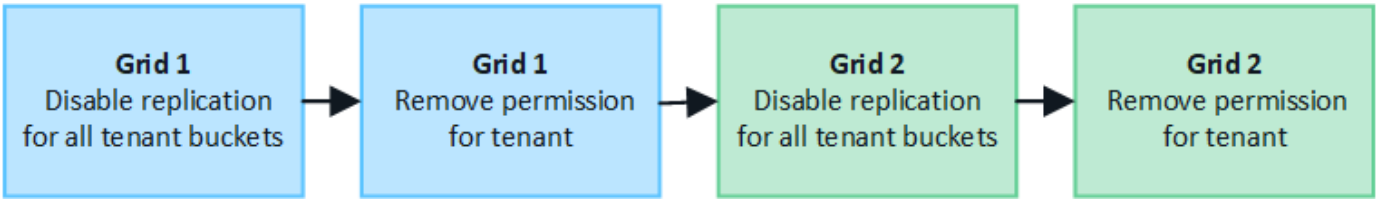
- 소스 그리드에서 원래 테넌트를 제거하려면 먼저 소스 그리드에서 해당 계정에 대한 모든 버킷을 제거해야 합니다.

- 대상 그리드에서 복제된 테넌트를 제거하려면 먼저 대상 그리드에서 계정에 대한 모든 버킷을 제거해야 합니다.
- 원래 테넌트 또는 복제된 테넌트를 제거하면 해당 계정을 더 이상 교차 그리드 복제에 사용할 수 없습니다.
- 소스 그리드에서 원래 테넌트를 제거하는 경우 대상 그리드에 클론 복제된 테넌트 그룹, 사용자 또는 키는 영향을 받지 않습니다. 클론 생성된 테넌트를 삭제하거나 해당 테넌트가 자신의 그룹, 사용자, 액세스 키 및 버킷을 관리하도록 허용할 수 있습니다.
- 대상 그리드에서 복제된 테넌트를 제거하는 경우 새 그룹 또는 사용자가 원래 테넌트에 추가되면 클론 오류가 발생합니다.

  이러한 오류를 방지하려면 이 그리드에서 테넌트를 삭제하기 전에 그리드 페더레이션 연결을 사용하도록 테넌트의 권한을 제거합니다.

그리드 페더레이션 연결 사용 권한을 제거합니다

테넌트가 그리드 페더레이션 연결을 사용하지 않도록 하려면 * 그리드 페더레이션 연결 사용 * 권한을 제거해야 합니다.



그리드 페더레이션 연결을 사용하는 테넌트의 권한을 제거하기 전에 다음 사항에 유의하십시오.

- 테넌트의 버킷에서 교차 그리드 복제가 활성화된 경우 * 그리드 페더레이션 연결 사용 * 권한을 제거할 수 없습니다. 테넌트 계정은 먼저 모든 버킷에 대해 교차 그리드 복제를 비활성화해야 합니다.
- 그리드 통합 연결 사용 * 권한을 제거해도 그리드 간에 이미 복제된 항목은 삭제되지 않습니다. 예를 들어, 테넌트의 사용 권한이 제거되면 두 그리드에 있는 테넌트 사용자, 그룹 및 객체가 두 그리드 모두에서 삭제되지 않습니다. 이러한 항목을 삭제하려면 두 그리드 모두에서 수동으로 삭제해야 합니다.
- 동일한 그리드 페더레이션 연결을 사용하여 이 권한을 다시 활성화하려면 먼저 대상 그리드에서 이 테넌트를 삭제하십시오. 그렇지 않으면 이 권한을 다시 설정하면 오류가 발생합니다.

> ⓘ 그리드 페더레이션 연결 사용 * 권한을 다시 활성화하면 로컬 그리드가 소스 그리드로 바뀌고 선택한 그리드 페더레이션 연결에 지정된 원격 그리드에 대한 복제가 트리거됩니다. 테넌트 계정이 이미 원격 그리드에 있는 경우 클론 생성으로 인해 충돌 오류가 발생합니다.

시작하기 전에

- 을 사용하고 "지원되는 웹 브라우저"있습니다.
- 두 그리드 모두에 대한 가 "루트 액세스 권한"있습니다.

테넌트 버킷에 대한 복제를 비활성화합니다

첫 번째 단계로 모든 테넌트 버킷에 대해 교차 그리드 복제를 비활성화합니다.

단계

1. 두 그리드 중 하나에서 시작하여 기본 관리 노드에서 그리드 관리자에 로그인합니다.
2. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.

3. 세부 정보를 표시할 연결 이름을 선택합니다.
4. 허용된 테넌트 * 탭에서 테넌트가 연결을 사용 중인지 확인합니다.
5. 테넌트가 나열되면 연결의 두 그리드에 있는 모든 버킷을 에 대해 으로 "크로스 그리드 복제를 비활성화합니다 "안내합니다.

테넌트 버킷에 교차 그리드 복제가 활성화된 경우 * 그리드 통합 연결 사용 * 권한을 제거할 수 없습니다. 테넌트는 두 그리드의 해당 버킷에 대해 교차 그리드 복제를 비활성화해야 합니다.

테넌트에 대한 권한을 제거합니다

테넌트 버킷에 대해 교차 그리드 복제를 비활성화한 후 그리드 페더레이션 연결을 사용할 수 있는 테넌트의 권한을 제거할 수 있습니다.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
2. 그리드 페더레이션 페이지 또는 테넌트 페이지에서 권한을 제거합니다.

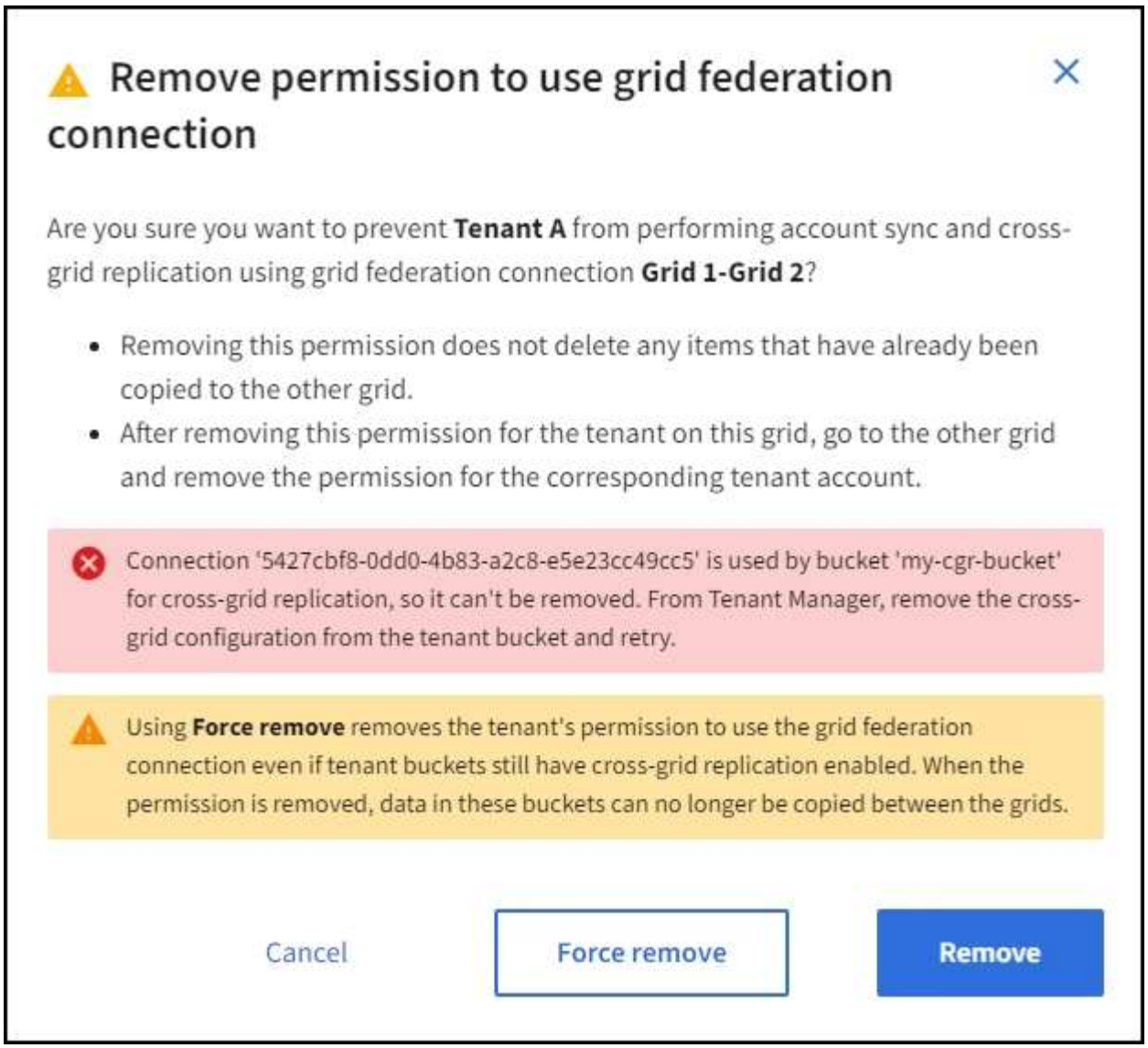
그리드 페더레이션 페이지

a. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.
b. 세부 정보 페이지를 표시하려면 연결 이름을 선택합니다.
c. 허용된 테넌트 * 탭에서 테넌트에 대한 라디오 버튼을 선택합니다.
d. 권한 제거 * 를 선택합니다.

Tenants 페이지

a. Tenants * 를 선택합니다.
b. 세부 정보 페이지를 표시하려면 테넌트 이름을 선택합니다.
c. Grid Federation * (그리드 통합 *) 탭에서 연결에 대한 라디오 버튼을 선택합니다.
d. 권한 제거 * 를 선택합니다.

3. 확인 대화 상자에서 경고를 검토하고 * 제거 * 를 선택합니다.
   - 권한을 제거할 수 있는 경우 세부 정보 페이지로 돌아가며 성공 메시지가 표시됩니다. 이 테넌트는 더 이상 그리드 페더레이션 연결을 사용할 수 없습니다.
   - 하나 이상의 테넌트 버킷에서 교차 그리드 복제가 활성화된 경우 오류가 표시됩니다.



다음 중 하나를 수행할 수 있습니다.

- (권장) 테넌트 관리자에 로그인하고 각 테넌트의 버킷에 대한 복제를 비활성화합니다. 을 "교차 그리드 복제 관리"참조하십시오. 그런 다음 단계를 반복하여 * 그리드 연결 사용 * 권한을 제거합니다.
- 권한을 강제로 제거합니다. 다음 섹션을 참조하십시오.

4. 다른 그리드로 이동하여 이 단계를 반복하여 다른 그리드에서 동일한 테넌트에 대한 권한을 제거합니다.

권한을 강제로 제거합니다

필요한 경우 테넌트 버킷에 교차 그리드 복제가 활성화되어 있는 경우에도 테넌트의 권한 제거를 통해 그리드 페더레이션 연결을 사용하도록 할 수 있습니다.

테넌트의 권한을 강제로 제거하기 전에 에 대한 일반적인 고려 사항 및 다음과 같은 추가 고려 사항에 권한을 제거합니다유의하십시오.

- 그리드 페더레이션 연결 사용 * 권한을 강제로 제거하면 다른 그리드(수집되었지만 아직 복제되지 않음)로 복제 보류 중인 모든 객체가 계속 복제됩니다. 이러한 처리 중인 객체가 대상 버킷에 도달하지 않도록 하려면 다른 그리드에 대한 테넌트의 권한도 제거해야 합니다.

- 그리드 통합 연결 사용 * 권한을 제거한 후 소스 버킷으로 인제된 모든 오브젝트는 대상 버킷에 복제되지 않습니다.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
2. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.
3. 세부 정보 페이지를 표시하려면 연결 이름을 선택합니다.
4. 허용된 테넌트 * 탭에서 테넌트에 대한 라디오 버튼을 선택합니다.
5. 권한 제거 * 를 선택합니다.
6. 확인 대화 상자에서 경고를 검토하고 * 강제 제거 * 를 선택합니다.

   성공 메시지가 나타납니다. 이 테넌트는 더 이상 그리드 페더레이션 연결을 사용할 수 없습니다.

7. 필요한 경우 다른 그리드로 이동하여 이 단계를 반복하여 다른 그리드에서 동일한 테넌트 계정에 대한 권한을 강제로 제거합니다. 예를 들어, 다른 그리드에서 이 단계를 반복하여 처리 중인 오브젝트가 대상 버킷에 도달하지 못하게 해야 합니다.

그리드 통합 오류 문제 해결

그리드 페더레이션 연결, 계정 클론 및 교차 그리드 복제와 관련된 경고 및 오류를 해결해야 할 수 있습니다.

그리드 페더레이션 연결 경고 및 오류

그리드 페더레이션 연결에서 경고를 받거나 오류가 발생할 수 있습니다.

연결 문제를 해결하기 위해 변경한 후 연결을 테스트하여 연결 상태가 * 연결됨 * 으로 돌아가는지 확인합니다. 자세한 내용은 을 "그리드 페더레이션 연결을 관리합니다"참조하십시오.

그리드 페더레이션 연결 실패 알림

문제

그리드 페더레이션 연결 실패 * 경고가 트리거되었습니다.

세부 정보

이 알림은 그리드 간의 그리드 페더레이션 연결이 작동하지 않음을 나타냅니다.

권장 조치

1. 두 그리드에 대한 Grid Federation(그리드 통합) 페이지의 설정을 검토합니다. 모든 값이 올바른지 확인합니다. 을 "그리드 페더레이션 연결을 관리합니다"참조하십시오.
2. 연결에 사용되는 인증서를 검토합니다. 만료된 그리드 페더레이션 인증서에 대한 알림이 없고 각 인증서에 대한 세부 정보가 유효한지 확인합니다. 에서 연결 인증서 회전에 대한 지침을 "그리드 페더레이션 연결을 관리합니다 "참조하십시오.
3. 양쪽 그리드의 모든 관리자 및 게이트웨이 노드가 온라인 상태이고 사용 가능한지 확인합니다. 이러한 노드에 영향을 줄 수 있는 알림을 모두 해결한 후 다시 시도하십시오.
4. 로컬 또는 원격 그리드에 대해 FQDN(정규화된 도메인 이름)을 제공한 경우 DNS 서버가 온라인 상태이고 사용 가능한지 확인합니다. 네트워킹, IP 주소 및 DNS 요구 사항은 를 "그리드 페더레이션은 무엇입니까?"참조하십시오.

그리드 페더레이션 인증서 알림의 만료

문제

그리드 페더레이션 인증서 만료 * 알림이 트리거되었습니다.

세부 정보

이 알림은 하나 이상의 그리드 페더레이션 인증서가 곧 만료됨을 나타냅니다.

권장 조치

에서 연결 인증서 회전에 대한 지침을 "그리드 페더레이션 연결을 관리합니다"참조하십시오.

그리드 페더레이션 연결을 편집하는 동안 오류가 발생했습니다

문제

그리드 페더레이션 연결을 편집할 때 * 저장 및 테스트 * 를 선택하면 "하나 이상의 노드에서 대상 구성 파일을 만들지 못했습니다."라는 경고 메시지가 표시됩니다.

세부 정보

그리드 페더레이션 연결을 편집할 때 StorageGRID는 첫 번째 그리드의 모든 관리 노드에 "대상 구성" 파일을 저장하려고 시도합니다. 관리 노드가 오프라인이기 때문에 이 파일을 모든 관리 노드에 저장할 수 없는 경우 경고 메시지가 나타납니다.

권장 조치

1. 연결을 편집하는 데 사용하는 그리드에서 * nodes * 를 선택합니다.
2. 해당 그리드의 모든 관리 노드가 온라인 상태인지 확인합니다.
3. 노드가 오프라인인 경우 노드를 다시 온라인 상태로 전환하고 연결을 다시 편집하십시오.

계정 클론 오류입니다

복제된 테넌트 계정에 로그인할 수 없습니다

문제

복제된 테넌트 계정에 로그인할 수 없습니다. Tenant Manager 로그인 페이지의 오류 메시지는 "이 계정에 대한 자격 증명이 잘못되었습니다. 다시 시도하십시오."

세부 정보

보안상의 이유로 테넌트 계정의 클론을 테넌트의 소스 그리드에서 테넌트의 대상 그리드로 생성할 때 테넌트의 로컬 루트 사용자에 대해 설정한 암호는 복제되지 않습니다. 마찬가지로 테넌트가 소스 그리드에 로컬 사용자를 생성할 때 로컬 사용자 암호가 대상 그리드에 복제되지 않습니다.

권장 조치

루트 사용자가 테넌트의 대상 그리드에 로그인하려면 먼저 그리드 관리자가 대상 그리드에서 로그인해야 "로컬 루트 사용자의 암호를 변경합니다"합니다.

클론 복제된 로컬 사용자가 테넌트의 대상 그리드에 로그인하기 전에 클론 생성된 테넌트의 루트 사용자는 대상 그리드에 사용자의 암호를 추가해야 합니다. 자세한 내용은 테넌트 관리자 사용 지침의 를 "로컬 사용자를 관리합니다 "참조하십시오.

클론 없이 테넌트가 생성되었습니다

문제

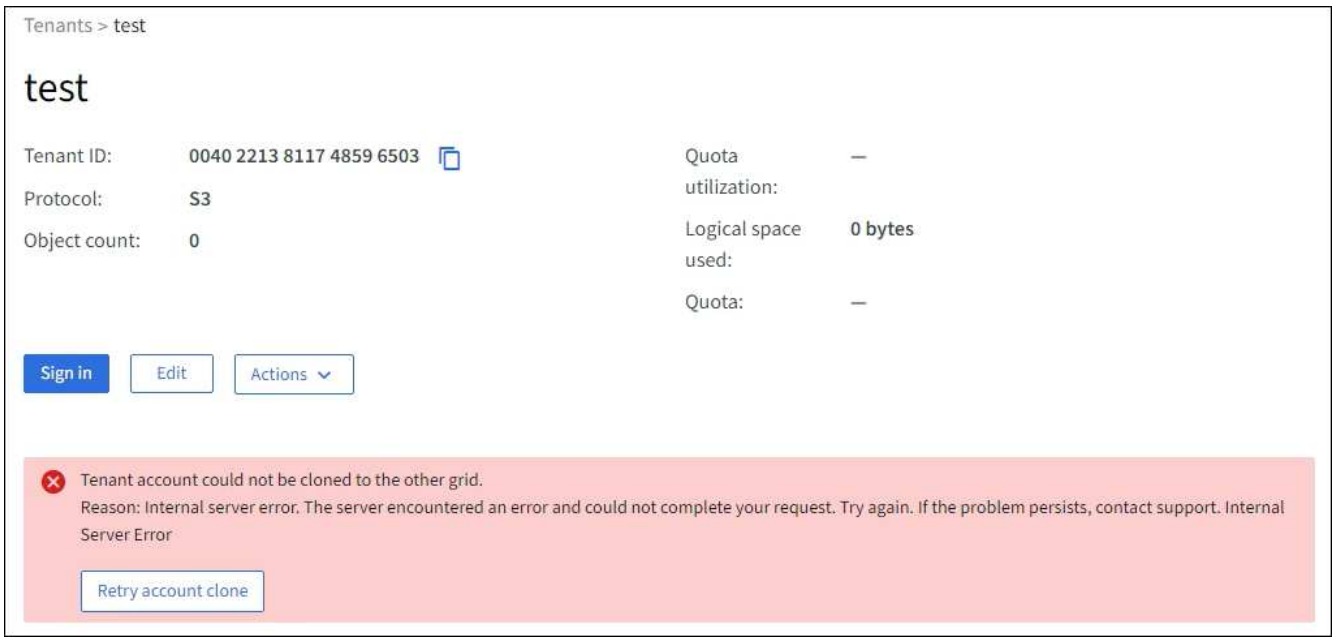
Use GRID Federation connection * 권한으로 새 테넌트를 생성한 후 "클론 없이 테넌트가 생성됨"이라는 메시지가 표시됩니다.

세부 정보

이 문제는 연결 상태 업데이트가 지연되어 상태가 불량한 연결이 * 연결됨 * 으로 나열되는 경우에 발생할 수 있습니다.

권장 조치

1. 오류 메시지에 나열된 이유를 검토하고 연결이 작동하지 않을 수 있는 네트워킹 또는 기타 문제를 해결합니다. 을 그리드 페더레이션 연결 경고 및 오류참조하십시오.
2. 지침에 따라 에서 그리드 페더레이션 연결을 "그리드 페더레이션 연결을 관리합니다"테스트하여 문제가 해결되었는지 확인합니다.
3. 테넌트의 소스 그리드에서 * Tenants * 를 선택합니다.
4. 클론 생성에 실패한 테넌트 계정을 찾습니다.
5. 테넌트 이름을 선택하여 세부 정보 페이지를 표시합니다.
6. 계정 클론 재시도 * 를 선택합니다.



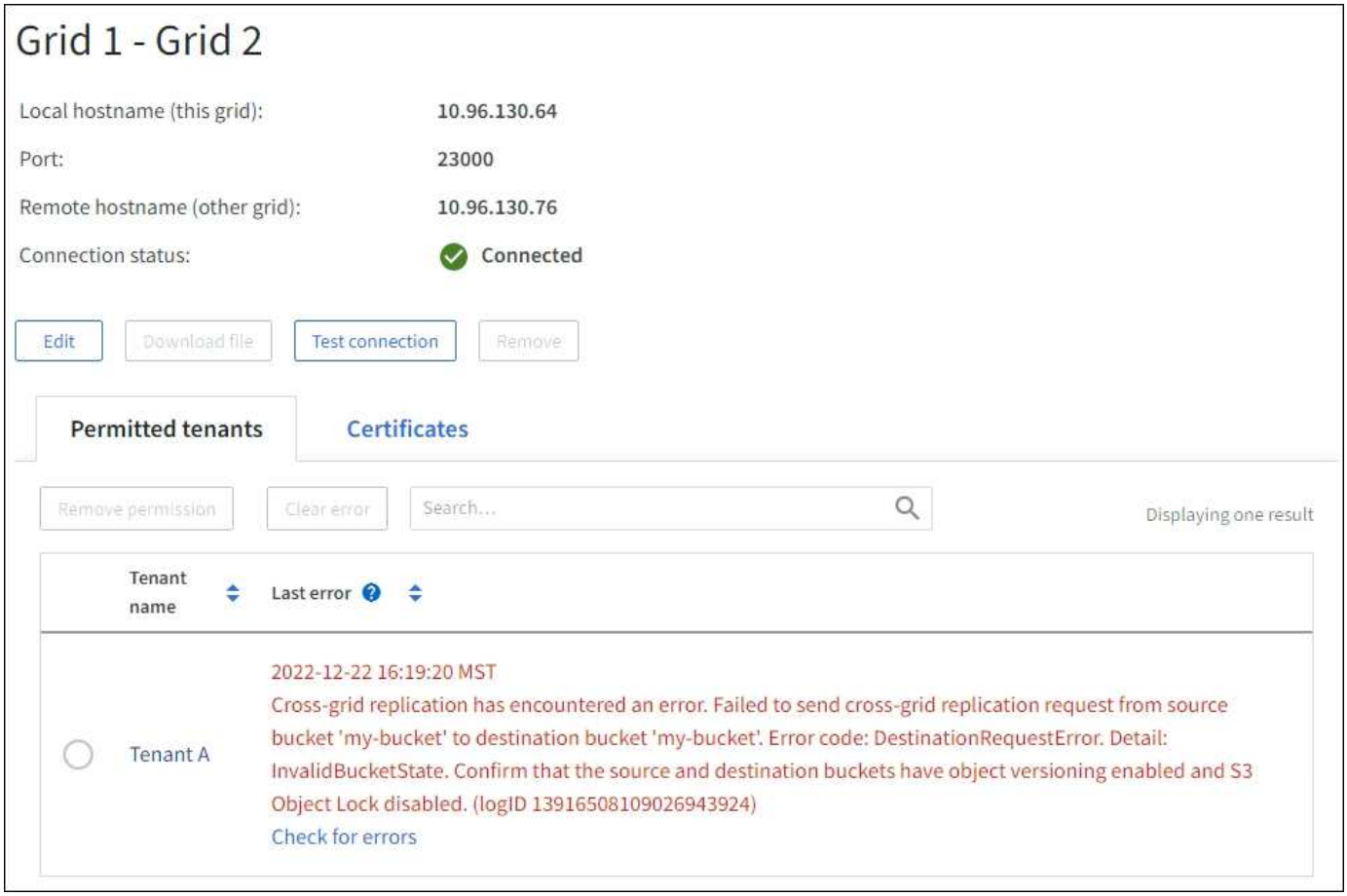
오류가 해결된 경우 테넌트 계정은 이제 다른 그리드에 복제됩니다.

교차 그리드 복제 경고 및 오류

연결 또는 테넌트에 대해 마지막 오류가 표시됩니다

문제

"그리드 페더레이션 연결 보기"연결 세부 정보 페이지의 * 마지막 오류 * 열에 오류가 있는 경우(또는 연결 시"허용된 테넌트 관리") 예를 들면 다음과 같습니다.



세부 정보

각 그리드 페더레이션 연결에 대해 * Last error * (마지막 오류 *) 열에는 테넌트의 데이터가 다른 그리드에 복제되고 있을 때 발생하는 가장 최근의 오류가 표시됩니다. 이 열에는 마지막으로 발생한 교차 그리드 복제 오류만 표시됩니다. 이전에 발생한 오류는 표시되지 않습니다. 다음 이유 중 하나로 인해 이 열에 오류가 발생할 수 있습니다.

- 소스 객체 버전을 찾을 수 없습니다.
- 소스 버킷을 찾을 수 없습니다.
- 대상 버킷이 삭제되었습니다.
- 대상 버킷이 다른 계정에 의해 다시 생성되었습니다.
- 대상 버킷에 버전 관리가 일시 중지되었습니다.
- 대상 버킷은 동일한 계정으로 다시 생성되었지만 현재는 버전이 지정되지 않았습니다.

권장 조치

마지막 오류 * 열에 오류 메시지가 나타나면 다음 단계를 수행하십시오.

1. 메시지 텍스트를 검토합니다.
2. 권장되는 작업을 수행합니다. 예를 들어 교차 그리드 복제를 위해 대상 버킷에서 버전 관리가 일시 중단된 경우 해당 버킷의 버전 관리를 다시 사용하도록 설정합니다.
3. 테이블에서 접속 또는 테넌트 계정을 선택합니다.
4. Clear error * 를 선택합니다.

5. 메시지를 지우고 시스템 상태를 업데이트하려면 * 예 * 를 선택하십시오.
6. 5-6분 정도 기다린 다음 새 오브젝트를 버킷에 넣습니다. 오류 메시지가 다시 나타나지 않는지 확인합니다.

   오류 메시지가 지워졌는지 확인하려면 새 개체를 수신하기 전에 메시지의 타임스탬프가 나타난 후 5분 이상 기다립니다.

   오류를 지운 후 오류가 있는 다른 버킷에서 오브젝트를 섭취할 경우 새 * 마지막 오류 * 가 나타날 수 있습니다.

7. 버킷 오류로 인해 객체를 복제하지 못했는지 확인하려면 을 참조하십시오."실패한 복제 작업을 식별하고 다시 시도하십시오"

교차 그리드 복제 영구 실패 알림

문제

Cross-grid replication permanent failure * 알림이 트리거되었습니다.

세부 정보

이 알림은 사용자가 해결해야 하는 이유 때문에 두 그리드의 버킷 간에 테넌트 객체를 복제할 수 없음을 나타냅니다. 이 알림은 일반적으로 소스 또는 대상 버킷의 변경으로 인해 발생합니다.

권장 조치

1. 경고가 트리거된 그리드에 로그인합니다.
2. 구성 * > * 시스템 * > * 그리드 페더레이션 * 으로 이동하여 알림에 나열된 연결 이름을 찾습니다.
3. 허용된 테넌트 탭에서 * 마지막 오류 * 열을 확인하여 오류가 있는 테넌트 계정을 확인합니다.
4. 오류에 대한 자세한 내용은 의 지침을 "그리드 페더레이션 연결을 모니터링합니다"참조하여 교차 그리드 복제 메트릭을 검토하십시오.
5. 영향을 받는 각 테넌트 계정에 대해 다음을 수행합니다.
   a. 테넌트가 교차 그리드 복제를 위해 대상 그리드에서 할당량을 초과하지 않았는지 확인하려면 의 지침을 "테넌트 작업을 모니터링합니다"참조하십시오.
   b. 필요에 따라 새 객체를 저장할 수 있도록 대상 그리드에 대한 테넌트 할당량을 늘리십시오.
6. 영향을 받는 각 테넌트의 경우 두 그리드의 테넌트 관리자에 로그인하여 버킷 목록을 비교할 수 있습니다.
7. 교차 그리드 복제가 활성화된 각 버킷에 대해 다음을 확인합니다.
   - 다른 그리드에 동일한 테넌트의 해당 버킷이 있습니다(정확한 이름을 사용해야 함).
   - 두 버킷에는 모두 개체 버전 관리가 활성화되어 있습니다(두 그리드 중 하나에서 버전 관리를 중단할 수 없음).
   - 두 버킷에는 S3 오브젝트 잠금이 비활성화됩니다.
   - 버킷이 * 오브젝트 삭제: 읽기 전용 * 상태에 있지 않습니다.
8. 문제가 해결되었는지 확인하려면 의 지침을 "그리드 페더레이션 연결을 모니터링합니다"참조하여 교차 그리드 복제 메트릭을 검토하거나 다음 단계를 수행하십시오.
   a. 그리드 페더레이션 페이지로 돌아갑니다.
   b. 영향을 받는 테넌트를 선택하고 * Last error * (마지막 오류 *) 열에서 * Clear Error * (오류 지우기 *)를

선택합니다.

c. 메시지를 지우고 시스템 상태를 업데이트하려면 * 예 * 를 선택하십시오.

d. 5-6분 정도 기다린 다음 새 오브젝트를 버킷에 넣습니다. 오류 메시지가 다시 나타나지 않는지 확인합니다.

> 오류 메시지가 지워졌는지 확인하려면 새 개체를 수신하기 전에 메시지의 타임스탬프가 나타난 후 5분 이상 기다립니다.

> 알림이 해결된 후 지우는 데 하루 정도 걸릴 수 있습니다.

a. 로 "실패한 복제 작업을 식별하고 다시 시도하십시오"이동하여 다른 그리드로 복제되지 않은 개체를 식별하거나 마커를 삭제하고 필요에 따라 복제를 다시 시도하십시오.

교차 그리드 복제 리소스를 사용할 수 없음 경고

문제

Cross-grid replication resource unavailable * 경고가 트리거되었습니다.

세부 정보

이 알림은 리소스를 사용할 수 없기 때문에 교차 그리드 복제 요청이 보류 중임을 나타냅니다. 예를 들어, 네트워크 오류가 있을 수 있습니다.

권장 조치

1. 알림을 모니터링하여 문제가 자체적으로 해결되는지 확인합니다.
2. 문제가 지속되면 동일한 연결에 대해 * 그리드 페더레이션 연결 실패 * 경고가 있는지 또는 노드에 대한 * 노드 * 경고와 통신할 수 없는지 확인합니다. 이 경고는 이러한 경고를 해결할 때 해결될 수 있습니다.
3. 오류에 대한 자세한 내용은 의 지침을 "그리드 페더레이션 연결을 모니터링합니다"참조하여 교차 그리드 복제 메트릭을 검토하십시오.
4. 알림을 해결할 수 없는 경우 기술 지원 팀에 문의하십시오.

문제가 해결된 후에는 교차 그리드 복제가 정상적으로 진행됩니다.

실패한 복제 작업을 식별하고 다시 시도하십시오

Cross-grid replication permanent failure * 경고를 해결한 후에는 어떤 개체나 삭제 표식을 다른 그리드에 복제하지 못했는지 확인해야 합니다. 그런 다음 이러한 객체를 다시 수집하거나 Grid Management API를 사용하여 복제를 다시 시도할 수 있습니다.

Cross-grid replication permanent failure * 알림은 사용자 개입이 필요한 이유로 두 그리드의 버킷 간에 테넌트 객체를 복제할 수 없음을 나타냅니다. 이 알림은 일반적으로 소스 또는 대상 버킷의 변경으로 인해 발생합니다. 자세한 내용은 을 참조하십시오 "그리드 통합 오류 문제 해결".

복제하지 못한 개체가 있는지 확인합니다

개체 또는 삭제 표식이 다른 그리드에 복제되지 않았는지 확인하려면 감사 로그에서 메시지를 검색할 "CGRR(Cross-Grid Replication Request)"수 있습니다. 이 메시지는 StorageGRID가 대상 버킷에 오브젝트, 다중 파트 오브젝트 또는 삭제 마커를 복제하지 못할 때 로그에 추가됩니다.

을 사용하여 결과를 읽기 쉬운 형식으로 변환할 수 "감사 - 설명 도구"있습니다.

시작하기 전에

- 루트 액세스 권한이 있습니다.
- `Passwords.txt`파일이 있습니다.
- 기본 관리 노드의 IP 주소를 알고 있습니다.

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. audit.log 에서 CGRR 메시지를 검색하고 감사 설명 도구를 사용하여 결과를 포맷합니다.

   예를 들어 이 명령은 지난 30분 동안 모든 CGRR 메시지에 대해 greps를 수행하고 감사 설명 도구를 사용합니다.

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

   명령의 결과는 이 예와 같이 되며, 이 예제에는 6개의 CGRR 메시지에 대한 항목이 있습니다. 이 예에서는 모든 크로스 그리드 복제 요청이 객체를 복제할 수 없기 때문에 일반 오류를 반환했습니다. 처음 세 가지 오류는 "개체 복제" 작업이고, 마지막 세 가지 오류는 "마커 복제" 작업용입니다.

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

각 항목에는 다음 정보가 포함되어 있습니다.

필드에 입력합니다	설명
CGRR 교차 그리드 복제 요청	요청 이름입니다
테넌트	테넌트의 계정 ID입니다
연결	그리드 페더레이션 연결의 ID입니다
작동	시도 중인 복제 작업의 유형: • 오브젝트 복제 • 삭제 마커를 복제합니다 • 다중 파트 개체를 복제합니다
버킷	버킷 이름입니다
오브젝트	개체 이름입니다
버전	객체의 버전 ID입니다

필드에 입력합니다	설명
오류	오류 유형입니다. 크로스 그리드 복제에 실패한 경우 오류는 "일반 오류 "입니다.

실패한 복제를 다시 시도하십시오

객체 목록을 생성하고 대상 버킷에 복제되지 않은 마커를 삭제하고 기본 문제를 해결한 후 다음 두 가지 방법 중 하나로 복제를 재시도할 수 있습니다.

- 각 오브젝트를 소스 버킷으로 재수집하십시오.
- 그리드 관리 전용 API를 사용합니다(설명 참조).

단계

1. Grid Manager 상단에서 도움말 아이콘을 선택하고 * API documentation * 을 선택합니다.
2. 전용 API 문서로 이동 * 을 선택합니다.

   "비공개"로 표시된 StorageGRID API 끝점은 예고 없이 변경될 수 있습니다. StorageGRID 전용 엔드포인트도 요청의 API 버전을 무시합니다.

3. Cross-grid-replication-advanced * 섹션에서 다음 끝점을 선택합니다.

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. 체험하기 * 를 선택합니다.
5. body * 텍스트 상자에서 * versionID * 의 예제 항목을 실패한 교차 그리드 복제 요청에 해당하는 audit.log 의 버전 ID로 바꿉니다.

   문자열 주위에 큰따옴표를 붙여야 합니다.

6. Execute * 를 선택합니다.
7. 서버 응답 코드가 * 204 * 인지 확인합니다. 이는 개체 또는 삭제 마커가 다른 그리드에 교차 그리드 복제를 위해 보류 중으로 표시되었음을 나타냅니다.

   보류 중 은 교차 그리드 복제 요청이 처리를 위해 내부 대기열에 추가되었음을 의미합니다.

복제 재시도를 모니터링합니다

복제 재시도 작업을 모니터링하여 작업이 완료되었는지 확인해야 합니다.

개체 또는 삭제 마커를 다른 그리드에 복제하려면 몇 시간 이상이 걸릴 수 있습니다.

다음 두 가지 방법 중 하나로 재시도 작업을 모니터링할 수 있습니다.

- S3 사용 "HeadObject 를 선택합니다"또는 "GetObject 를 참조하십시오" 요청 응답에는 다음 값 중 하나가 있는 StorageGRID 관련 `x-ntap-sg-cgr-replication-status` 응답 헤더가 포함됩니다.

그리드	복제 상태입니다
출처	• * 완료됨 *: 복제가 성공했습니다. • * 보류 중 *: 객체가 아직 복제되지 않았습니다. • * 실패 *: 영구적인 장애로 인해 복제에 실패했습니다. 사용자가 오류를 해결해야 합니다.
목적지	• replica *: 객체가 소스 그리드에서 복제되었습니다.

- 그리드 관리 전용 API를 사용합니다(설명 참조).

단계

1. 전용 API 설명서의 * cross-grid-replication-advanced * 섹션에서 다음 끝점을 선택합니다.

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. 체험하기 * 를 선택합니다.
3. 매개 변수 섹션에서 요청에 사용한 버전 ID를 `cross-grid-replication-retry-failed` 입력합니다.
4. Execute * 를 선택합니다.
5. 서버 응답 코드가 * 200 * 인지 확인합니다.
6. 다음 중 하나인 복제 상태를 검토합니다.
   - * 보류 중 *: 객체가 아직 복제되지 않았습니다.
   - * 완료됨 *: 복제가 성공했습니다.
   - * 실패 *: 영구적인 장애로 인해 복제에 실패했습니다. 사용자가 오류를 해결해야 합니다.

보안 관리

보안 관리

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

암호화 관리

StorageGRID는 데이터 암호화를 위한 여러 옵션을 제공합니다. "사용 가능한 암호화 방법을 검토합니다"데이터 보호 요구사항을 충족하는 솔루션을 결정해야 합니다.

인증서를 관리합니다

HTTP 연결이나 서버에 대한 클라이언트 또는 사용자 ID를 인증하는 데 사용되는 클라이언트 인증서에 사용할 수 "서버 인증서를 구성하고 관리합니다"있습니다.

키 관리 서버를 구성합니다

를 "키 관리 서버입니다" 사용하면 어플라이언스를 데이터 센터에서 제거할 경우에도 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 설정을 관리합니다

S3 플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 스토리지 노드와 외부 S3 엔드 포인트 간에 를 구성할 수 "스토리지 프록시 서버입니다"있습니다. HTTPS 또는 HTTP를 사용하여 AutoSupport 패키지를 보내는 경우 관리 노드와 기술 지원 간에 를 구성할 수 있습니다"관리 프록시 서버".

방화벽을 제어합니다

시스템 보안을 강화하기 위해 에서 특정 포트를 열거나 닫아 StorageGRID 관리 노드에 대한 액세스를 제어할 수 있습니다"외부 방화벽". 또한 노드를 구성하여 각 노드에 대한 네트워크 액세스를 제어할 수도 "내부 방화벽"있습니다. 배포에 필요한 포트를 제외한 모든 포트에 대한 액세스를 차단할 수 있습니다.

StorageGRID 암호화 방법을 검토합니다

StorageGRID는 데이터 암호화를 위한 여러 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)	"키 관리 서버를 구성합니다 "StorageGRID 사이트 및 "어플라이언스에 대해 노드 암호화를 활성화합니다"의 경우 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. • 참고 *: KMS를 사용한 암호화 키 관리는 스토리지 노드 및 서비스 어플라이언스에서만 지원됩니다.
StorageGRID 어플라이언스 설치 프로그램의 드라이브 암호화 페이지	어플라이언스에 하드웨어 암호화를 지원하는 드라이브가 포함된 경우 설치 중에 드라이브 암호를 설정할 수 있습니다. 드라이브 암호를 설정하면 암호를 모르는 경우 시스템에서 제거된 드라이브에서 유효한 데이터를 복구할 수 없습니다. 설치를 시작하기 전에 * 하드웨어 구성 * > * 드라이브 암호화 * 로 이동하여 노드의 모든 StorageGRID에서 관리하는 자체 암호화 드라이브에 적용되는 드라이브 암호를 설정하십시오.	자체 암호화 드라이브를 포함하는 어플라이언스: 보안 드라이브의 모든 데이터는 데이터 센터에서 물리적 손실 또는 제거로부터 보호됩니다. 드라이브 암호화는 SANtricity에서 관리하는 드라이브에는 적용되지 않습니다. 자체 암호화 드라이브와 SANtricity 컨트롤러가 포함된 스토리지 어플라이언스가 있는 경우 SANtricity에서 드라이브 보안을 활성화할 수 있습니다.

암호화 옵션	작동 방식	적용 대상
SANtricity 시스템 관리자의 드라이브 보안	StorageGRID 어플라이언스에 드라이브 보안 기능이 활성화된 경우를 사용하여 보안 키를 생성하고 관리할 수 "SANtricity 시스템 관리자" 있습니다. 보안 드라이브의 데이터에 액세스하려면 키가 필요합니다.	FDE(전체 디스크 암호화) 드라이브 또는 자체 암호화 드라이브를 사용하는 스토리지 어플라이언스 보안 드라이브의 모든 데이터는 데이터 센터에서 물리적 손실 또는 제거로부터 보호됩니다. 일부 스토리지 어플라이언스나 서비스 어플라이언스와 함께 사용할 수 없습니다.
저장된 오브젝트 암호화	"저장된 오브젝트 암호화"그리드 관리자에서 옵션을 활성화합니다. 이 기능을 사용하도록 설정하면 버킷 레벨이나 오브젝트 레벨에서 암호화되지 않은 새로운 모든 객체가 수집 중에 암호화됩니다.	새로 수집된 S3 오브젝트 데이터 저장된 기존 객체는 암호화되지 않습니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다.
S3 버킷 암호화	버킷에 대한 암호화를 사용하도록 설정하기 위한 PutBucketEncryption 요청을 발행합니다. 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. "버킷 작업"
S3 오브젝트 서버 측 암호화(SSE)	S3 요청을 실행하여 객체를 저장하고 `x-amz-server-side-encryption` 요청 헤더를 포함합니다.	새로 수집된 S3 오브젝트 데이터만 객체에 대해 암호화를 지정해야 합니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다. StorageGRID가 키를 관리합니다. "서버측 암호화를 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-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	새로 수집된 S3 오브젝트 데이터만 객체에 대해 암호화를 지정해야 합니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다. 키는 StorageGRID 외부에서 관리됩니다. "서버측 암호화를 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 - 사용자 가이드: 클라이언트 측 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 보호할 수 있으며 저장된 개체 암호화 옵션을 사용하여 수집될 때 모든 개체를 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.

보안 인증서를 관리합니다

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 를 충족해야 "서버 인증서에 대한 시스템 강화 지침"합니다.
- 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.

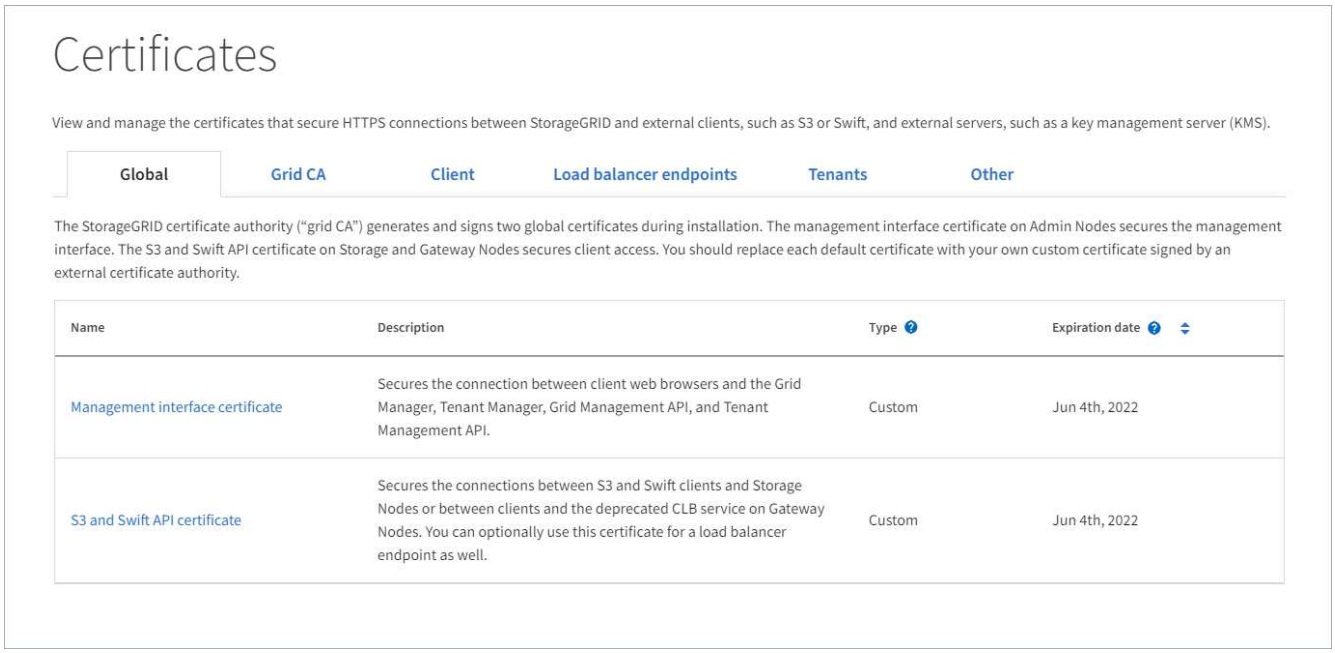
서버 및 클라이언트 인증서 유형의 변형은 여러 가지 방법으로 구현됩니다. 시스템을 구성하기 전에 특정 StorageGRID 구성에 필요한 모든 인증서를 준비해야 합니다.

보안 인증서에 액세스합니다

각 인증서의 구성 워크플로 링크와 함께 모든 StorageGRID 인증서에 대한 정보에 액세스할 수 있습니다.

단계

1. Grid Manager에서 * 구성 * > * 보안 * > * 인증서 * 를 선택합니다.



2. 인증서 페이지에서 탭을 선택하여 각 인증서 범주에 대한 정보를 확인하고 인증서 설정에 액세스합니다. 가 있는 경우 탭에 액세스할 수 "적절한 권한"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 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 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 연결의 보안을 유지합니다.
- S3 API 인증서: S3 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 API 인증서를 교체합니다" 스토리지 노드 및 로드 밸런서 엔드포인트(선택 사항) 연결에 사용됩니다.
- "기본 관리 인터페이스 인증서를 복원합니다"..
- "기본 S3 API 인증서를 복원합니다"..
- "스크립트를 사용하여 자체 서명된 새 관리 인터페이스 인증서를 생성합니다"..
- 또는 을 복사하거나 "관리 인터페이스 인증서입니다""S3 API 인증서"다운로드합니다.

그리드 **CA**

Grid CA 인증서StorageGRID 설치 중에 StorageGRID 인증 기관에서 생성한 는 모든 내부 StorageGRID 트래픽을 보호합니다.

인증서 정보에는 인증서 만료 날짜 및 인증서 내용이 포함됩니다.

"Grid CA 인증서를 복사하거나 다운로드합니다"변경할 수는 있지만 변경할 수는 없습니다.

클라이언트

클라이언트 인증서외부 인증 기관에서 생성한 로 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."
- 작업 * 을 선택하여 빠르게 "편집"또는 "첨부" "제거"클라이언트 인증서를 선택합니다. 클라이언트 인증서를 최대 10개까지 선택하고 * Actions * > * Remove * 를 사용하여 한 번에 제거할 수 있습니다.

부하 분산 장치 엔드포인트

로드 밸런서 끝점 인증서 게이트웨이 노드 및 관리 노드에서 S3 클라이언트와 StorageGRID 로드 밸런서 서비스 간의 연결을 보호합니다.

로드 밸런서 끝점 테이블에는 구성된 각 로드 밸런서 끝점에 대한 행이 있으며, 글로벌 S3 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.

- "로드 밸런서 끝점을 봅니다"인증서 세부 정보가 포함됩니다.
- "FabricPool에 대한 로드 밸런서 끝점 인증서를 지정합니다."
- "글로벌 S3 API 인증서를 사용합니다" 새 로드 밸런서 엔드포인트 인증서를 생성하는 대신

테넌트

테넌트는 또는 플랫폼 서비스 끝점 인증서 를 사용하여 StorageGRID과의 연결을 보호할 수 ID 페더레이션 서버 인증서있습니다.

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.

- 클라우드 스토리지 풀 인증서

- 이메일 경고 알림 인증서
- 외부 syslog 서버 인증서
- 그리드 페더레이션 연결 인증서
- ID 페더레이션 인증서
- KMS(키 관리 서버) 인증서
- SSO(Single Sign-On) 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.

가 있는 경우에만 다른 인증서의 정보를 보고 액세스할 수 "적절한 권한"있습니다.

다음을 수행할 수 있습니다.

- "S3, C2S S3 또는 Azure에 대한 클라우드 스토리지 풀 인증서를 지정합니다"
- "경고 e-메일 알림에 사용할 인증서를 지정합니다"
- "외부 syslog 서버에 인증서를 사용합니다"
- "그리드 페더레이션 연결 인증서를 회전합니다"
- "ID 페더레이션 인증서를 보고 편집합니다"
- "KMS(키 관리 서버) 서버 및 클라이언트 인증서를 업로드합니다"
- "신뢰할 수 있는 당사자 트러스트를 위해 SSO 인증서를 수동으로 지정합니다"

보안 인증서 세부 정보입니다

각 보안 인증서 유형은 구현 지침에 대한 링크와 함께 아래에 설명되어 있습니다.

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 API 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	스토리지 노드 및 로드 밸런서 엔드포인트에 대한 보안 S3 클라이언트 연결을 인증합니다(선택 사항).	• configuration * > * Security * > * Certificates * 에서 * 글로벌 * 탭을 선택한 다음 * S3 API certificate * 를 선택합니다	"S3 API 인증서를 구성합니다"

Grid CA 인증서

를 기본 그리드 CA 인증서 설명입니다참조하십시오.

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 노드 및 관리 노드에서 S3 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. 전역 인증서의 사용자 지정 버전을 사용하여 부하 분산 서비스에 대한 연결을 인증할 수도 S3 API 인증서있습니다. 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"

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"

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 *	"외부 syslog 서버를 사용합니다"

그리드 페더레이션 연결 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버 및 클라이언트	그리드 페더레이션 연결에서 현재 StorageGRID 시스템과 다른 그리드 간에 전송된 정보를 인증하고 암호화합니다.	• 구성 * > * 시스템 * > * 그리드 페더레이션 *	• "그리드 페더레이션 연결을 만듭니다" • "연결 인증서를 회전합니다"

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"

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"

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"

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"

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 대한 S3 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.

지원되는 서버 인증서 유형입니다

StorageGRID 시스템은 RSA 또는 ECDSA(Elliptic Curve Digital Signature Algorithm)로 암호화된 사용자 지정 인증서를 지원합니다.

보안 정책의 암호화 유형은 서버 인증서 유형과 일치해야 합니다. 예를 들어, RSA cipherer는 RSA 인증서가 필요하며, ECDSA cipherer는 ECDSA 인증서가 필요합니다. 을 "보안 인증서를 관리합니다 "참조하십시오. 서버 인증서와 호환되지 않는 사용자 지정 보안 정책을 구성할 수 "일시적으로 기본 보안 정책으로 돌아갑니다"있습니다.

StorageGRID가 클라이언트 연결을 보호하는 방법에 대한 자세한 내용은 을 참조하십시오"S3 클라이언트에 대한 보안 ".

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.
- 여러분사용자 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`).

     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. 확장자를 사용하여 파일을 `.pem` 저장합니다.

     예를 들면 다음과 같습니다. `storagegrid_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.

필드에 입력합니다	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
IP	인증서에 포함할 하나 이상의 IP 주소입니다.

필드에 입력합니다	설명
제목(선택 사항)	X.509 인증서 소유자의 주체 또는 고유 이름(DN)입니다. 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 CN(Subject Common Name)으로 사용합니다.
일 유효	인증서가 만료된 후 경과한 일 수입니다.
키 사용 확장을 추가합니다	이 옵션을 선택하면(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다. 이러한 확장은 인증서에 포함된 키의 용도를 정의합니다. • 참고 *: 인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

c. Generate * 를 선택합니다.

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

   ▪ 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

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

   예를 들면 다음과 같습니다. `storagegrid_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.

시작하기 전에

- 있습니다. "특정 액세스 권한"
- `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. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.
3. 자체 서명된 새 인증서를 사용하여 StorageGRID를 구성합니다.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

   - 의 경우 `--domains` 모든 관리 노드의 정규화된 도메인 이름을 나타내는 와일드카드를 사용합니다. 예를 들어, 에서는 `*.ui.storagegrid.example.com` * 와일드카드를 사용하여 `admin1.ui.storagegrid.example.com` 및 `admin2.ui.storagegrid.example.com`를 나타냅니다.
   - `--type`Grid Manager 및 Tenant Manager에서 사용하는 관리 인터페이스 인증서를 구성하려면 로 `management` 설정합니다.
   - 기본적으로 생성된 인증서는 1년(365일) 동안 유효하며 만료되기 전에 다시 만들어야 합니다. 인수를 사용하여 기본 유효 기간을 재정의할 수 `--days` 있습니다.

> 인증서의 유효 기간은 가 실행될 때 `make-certificate` 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. 확장자를 사용하여 파일을 `.pem` 저장합니다.

   예를 들면 다음과 같습니다. `storagegrid_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 확장자로 `.pem`저장합니다.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

S3 API 인증서를 구성합니다

스토리지 노드에 대한 S3 클라이언트 연결이나 로드 밸런서 끝점에 사용되는 서버 인증서를 교체하거나 복원할 수 있습니다. 교체 사용자 지정 서버 인증서는 조직에 따라 다릅니다.

이 버전의 문서 사이트에서 Swift 세부 정보가 제거되었습니다. 을 "StorageGRID 11.8: S3 및 Swift API 인증서를 구성합니다"참조하십시오.

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.

서버에서 구성을 완료한 후 사용하는 루트 CA(인증 기관)에 따라 시스템에 액세스하는 데 사용할 S3 API 클라이언트에 그리드 CA 인증서를 설치해야 할 수도 있습니다.

실패한 서버 인증서로 인해 작업이 중단되지 않도록 루트 서버 인증서가 만료될 때 * S3 API * 에 대한 글로벌 서버 인증서 만료 알림이 트리거됩니다. 필요에 따라 글로벌 탭에서 * 구성 * > * 보안 * > * 인증서 * 를 선택하고 S3 API 인증서의 만료 날짜를 확인하여 현재 인증서가 만료되는 시점을 확인할 수 있습니다.

사용자 지정 S3 API 인증서를 업로드하거나 생성할 수 있습니다.

사용자 지정 **S3 API** 인증서를 추가합니다

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택합니다.
2. 글로벌 * 탭에서 * S3 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`).

     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. 인증서 세부 정보를 선택하여 업로드된 각 사용자 지정 S3 API 인증서의 메타데이터 및 PEM을 표시합니다. 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. 확장자를 사용하여 파일을 `.pem` 저장합니다.

     예를 들면 다음과 같습니다. `storagegrid_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 이후의 새 S3 클라이언트 연결에 사용됩니다.

인증서를 생성합니다

서버 인증서 파일을 생성합니다.

a. 인증서 생성 * 을 선택합니다.

b. 인증서 정보를 지정합니다.

필드에 입력합니다	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
IP	인증서에 포함할 하나 이상의 IP 주소입니다.

필드에 입력합니다	설명
제목(선택 사항)	X.509 인증서 소유자의 주체 또는 고유 이름(DN)입니다. 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 CN(Subject Common Name)으로 사용합니다.
일 유효	인증서가 만료된 후 경과한 일 수입니다.
키 사용 확장을 추가합니다	이 옵션을 선택하면(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다. 이러한 확장은 인증서에 포함된 키의 용도를 정의합니다. • 참고 *: 인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

c. Generate * 를 선택합니다.

d. 생성된 사용자 지정 S3 API 인증서의 메타데이터와 PEM을 표시하려면 * Certificate Details * 를 선택하십시오.

   ▪ 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

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

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

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

e. 저장 * 을 선택합니다.

   사용자 지정 서버 인증서는 이후의 새 S3 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 API 인증서를 추가하면 S3 API 인증서 페이지에 사용 중인 사용자 지정 S3 API 인증서에 대한 자세한 인증서 정보가 표시됩니다. + 필요에 따라 인증서 PEM을 다운로드하거나 복사할 수 있습니다.

기본 **S3 API** 인증서를 복원합니다

스토리지 노드에 대한 S3 클라이언트 연결에 기본 S3 API 인증서를 사용하도록 되돌릴 수 있습니다. 그러나 부하 분산 끝점에 기본 S3 API 인증서를 사용할 수는 없습니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택합니다.
2. 글로벌 * 탭에서 * S3 API 인증서 * 를 선택합니다.
3. 기본 인증서 사용 * 을 선택합니다.

   글로벌 S3 API 인증서의 기본 버전을 복원하면 구성한 사용자 지정 서버 인증서 파일이 삭제되어 시스템에서 복구할 수 없습니다. 기본 S3 API 인증서는 스토리지 노드에 대한 이후 새 S3 클라이언트 연결에 사용됩니다.

4. 경고를 확인하고 기본 S3 API 인증서를 복원하려면 * 확인 * 을 선택하십시오.

   루트 액세스 권한이 있고 사용자 지정 S3 API 인증서가 부하 분산 장치 끝점 연결에 사용된 경우 기본 S3 API 인증서를 사용하여 더 이상 액세스할 수 없는 로드 밸런서 끝점의 목록이 표시됩니다. 로 "로드 밸런서 엔드포인트를 구성합니다" 이동하여 영향을 받는 끝점을 편집하거나 제거합니다.

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

S3 API 인증서를 다운로드하거나 복사합니다

다른 곳에서 사용할 S3 API 인증서 콘텐츠를 저장하거나 복사할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 인증서 * 를 선택합니다.
2. 글로벌 * 탭에서 * S3 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. 확장자를 사용하여 파일을 `.pem` 저장합니다.

   예를 들면 다음과 같습니다. `storagegrid_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 확장자로 `.pem`저장합니다.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

관련 정보

- "S3 REST API 사용"
- "S3 끝점 도메인 이름을 구성합니다"

Grid CA 인증서를 복사합니다

StorageGRID는 내부 CA(인증 기관)를 사용하여 내부 트래픽을 보호합니다. 인증서를 업로드해도 이 인증서는 변경되지 않습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

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. 확장자를 사용하여 파일을 `.pem` 저장합니다.

   예를 들면 다음과 같습니다. `storagegrid_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 확장자로 `.pem`저장합니다.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

FabricPool용 **StorageGRID** 인증서를 구성합니다

엄격한 호스트 이름 유효성 검사를 수행하고 FabricPool를 사용하는 ONTAP 클라이언트와 같은 엄격한 호스트 이름 유효성 검사 비활성화를 지원하지 않는 S3 클라이언트의 경우 로드 밸런서 끝점을 구성할 때 서버 인증서를 생성하거나 업로드할 수 있습니다.

시작하기 전에

- 있습니다. "특정 액세스 권한"
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."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 "FabricPool용 StorageGRID를 구성합니다"참조하십시오.

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.

"보안 인증서를 관리합니다"및 을 "사용자 지정 서버 인증서를 구성합니다"참조하십시오.

실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 이 서버 인증서가 곧 만료될 때 인증서 페이지 * 알림에 구성된 * 클라이언트 인증서 만료 알림이 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".

시작하기 전에

- 루트 액세스 권한이 있습니다.
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."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

클라이언트 인증서를 추가하려면 다음 절차 중 하나를 사용합니다.

- 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. 인증서 이름을 입력합니다.
4. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
5. Continue * 를 선택합니다.
6. 인증서 첨부 * 단계의 경우 관리 인터페이스 인증서를 업로드합니다.
   a. 인증서 업로드 * 를 선택합니다.
   b. 찾아보기 * 를 선택하고 관리 인터페이스 인증서 파일을 (`.pem`선택합니다.)
      - 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. 외부 모니터링 툴을 구성합니다그래파나와 같은

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 "관리 인터페이스 인증서를 구성합니다"수행합니다.
2. 그리드 관리자에서 * 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 클라이언트 * 탭을 선택합니다.
3. 추가 * 를 선택합니다.
4. 인증서 이름을 입력합니다.
5. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
6. Continue * 를 선택합니다.
7. 인증서 첨부 * 단계의 경우 클라이언트 인증서, 개인 키 및 CA 번들 파일을 업로드합니다.
   a. 인증서 업로드 * 를 선택합니다.
   b. 찾아보기 * 를 선택하고 클라이언트 인증서, 개인 키 및 CA 번들 파일을 (`.pem`선택합니다.

- 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.

8. 외부 모니터링 툴을 구성합니다그래파나와 같은

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. 인증서 이름을 입력합니다.
4. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
5. Continue * 를 선택합니다.
6. 인증서 첨부 * 단계에서 * 인증서 생성 * 을 선택합니다.
7. 인증서 정보를 지정합니다.
   - * subject * (선택 사항): X.509 주체 또는 인증서 소유자의 고유 이름(DN).
   - 유효한 * 일 수 *: 생성된 인증서가 생성된 시점부터 생성된 유효 일 수입니다.
   - * 키 사용 확장 추가 *: 선택한 경우(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다.

     이러한 확장은 인증서에 포함된 키의 용도를 정의합니다.

     인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트에 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

8. Generate * 를 선택합니다.
9. [[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. 확장자를 사용하여 파일을 `.pem` 저장합니다.

예를 들면 다음과 같습니다. `storagegrid_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.

10. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

새 인증서가 클라이언트 탭에 나타납니다.

11. 그리드 관리자에서 * 구성 * > * 보안 * > * 인증서 * 를 선택한 다음 * 글로벌 * 탭을 선택합니다.
12. Management Interface certificate * 를 선택합니다.
13. 사용자 정의 인증서 사용 * 을 선택합니다.
14. 단계에서 certificate.pem 및 private_key.pem 파일을 업로드합니다.클라이언트 인증서 세부 정보입니다 CA 번들을 업로드할 필요가 없습니다.
    a. 인증서 업로드 * 를 선택한 다음 * 계속 * 을 선택합니다.
    b. 각 인증서 파일 업로드(`.pem`).
    c. 인증서를 Grid Manager에 저장하려면 * 저장 * 을 선택합니다.

    새 인증서가 관리 인터페이스 인증서 페이지에 나타납니다.

15. 외부 모니터링 툴을 구성합니다그래파나와 같은

외부 모니터링 툴을 설정한다

단계

1. 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.

    예를 들면 다음과 같습니다. `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.

2. 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. 인증서 이름을 입력합니다.
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 이름을 업로드합니다.(`.pem`

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. 확장자를 사용하여 파일을 `.pem` 저장합니다.

예를 들면 다음과 같습니다. `storagegrid_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.

- * subject * (선택 사항): X.509 주체 또는 인증서 소유자의 고유 이름(DN).
- 유효한 * 일 수 *: 생성된 인증서가 생성된 시점부터 생성된 유효 일 수입니다.
- * 키 사용 확장 추가 *: 선택한 경우(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다.

  이러한 확장은 인증서에 포함된 키의 용도를 정의합니다.

  인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트에 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

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. 확장자를 사용하여 파일을 `.pem` 저장합니다.

예를 들면 다음과 같습니다. `storagegrid_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. 확장자를 사용하여 파일을 `.pem` 저장합니다.

   예를 들면 다음과 같습니다. `storagegrid_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 확장자로 `.pem`저장합니다.

   예를 들면 다음과 같습니다. `storagegrid_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.

보안 설정을 구성합니다

TLS 및 SSH 정책을 관리합니다

TLS 및 SSH 정책은 클라이언트 응용 프로그램과 보안 TLS 연결을 설정하고 내부 StorageGRID 서비스에 대한 보안 SSH 연결을 설정하는 데 사용되는 프로토콜과 암호를 결정합니다.

보안 정책은 TLS 및 SSH가 이동 중인 데이터를 암호화하는 방법을 제어합니다. 일반적으로 시스템이 일반 조건 호환이거나 다른 암호를 사용해야 하는 경우가 아니면 최신 호환성(기본값) 정책을 사용합니다.

> 이러한 정책에서 암호를 사용하도록 일부 StorageGRID 서비스가 업데이트되지 않았습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.

보안 정책을 선택합니다

단계

1. 구성 * > * 보안 * > * 보안 설정 * 을 선택합니다.

   TLS 및 SSH 정책 * 탭에는 사용 가능한 정책이 표시됩니다. 현재 활성 정책은 정책 타일에 녹색 확인 표시로 표시됩니다.

2. 타일을 검토하여 사용 가능한 정책에 대해 알아봅니다.

정책	설명
최신 호환성(기본값)	강력한 암호화가 필요하거나 특별한 요구 사항이 없는 경우 기본 정책을 사용합니다. 이 정책은 대부분의 TLS 및 SSH 클라이언트와 호환됩니다.
레거시 호환성	이전 클라이언트에 대한 추가 호환성 옵션이 필요한 경우 이 정책을 사용합니다. 이 정책의 추가 옵션을 사용하면 최신 호환성 정책보다 보안이 덜 강화될 수 있습니다.
일반 조건	일반 조건 인증이 필요한 경우 이 정책을 사용합니다.
FIPS 엄격한	일반 조건 인증이 필요하고 로드 밸런서 끝점, 테넌트 관리자 및 그리드 관리자에 대한 외부 클라이언트 연결에 NetApp 암호화 보안 모듈 3.0.8을 사용해야 하는 경우 이 정책을 사용합니다. 이 정책을 사용하면 성능이 저하될 수 있습니다. 참고: 이 정책을 선택한 후에는 모든 노드가 NetApp 암호화 보안 모듈을 활성화해야 "롤링 방식으로 재부팅했습니다"합니다. 재부팅을 시작하고 모니터링하려면 * Maintenance * > * Rolling Reboot * 를 사용하십시오.
맞춤형	자신의 암호를 적용해야 하는 경우 사용자 지정 정책을 만듭니다.

3. 각 정책의 암호화, 프로토콜 및 알고리즘에 대한 세부 정보를 보려면 * 상세 정보 보기 * 를 선택합니다.
4. 현재 정책을 변경하려면 * 정책 사용 * 을 선택합니다.

   정책 타일에서 * 현재 정책 * 옆에 녹색 확인 표시가 나타납니다.

사용자 지정 보안 정책을 만듭니다

사용자 고유의 암호를 적용해야 하는 경우 사용자 지정 정책을 만들 수 있습니다.

단계

1. 만들려는 사용자 지정 정책과 가장 유사한 정책 타일에서 * 세부 정보 보기 * 를 선택합니다.
2. 클립보드로 복사 * 를 선택한 다음 * 취소 * 를 선택합니다.

3. 사용자 정의 정책 * 타일에서 * 구성 및 사용 * 을 선택합니다.
4. 복사한 JSON을 붙여 넣고 필요한 내용을 변경합니다.
5. Use policy * 를 선택합니다.

   사용자 지정 정책 타일의 * 현재 정책 * 옆에 녹색 확인 표시가 나타납니다.

6. 필요에 따라 * 구성 편집 * 을 선택하여 새 사용자 지정 정책을 더 많이 변경합니다.

일시적으로 기본 보안 정책으로 돌아갑니다

사용자 지정 보안 정책을 구성한 경우 구성된 TLS 정책이 과 호환되지 않으면 그리드 관리자에 로그인하지 못할 수 "구성된 서버 인증서입니다"있습니다.

일시적으로 기본 보안 정책으로 되돌릴 수 있습니다.

단계

1. 관리자 노드에 로그인:
   a. 다음 명령을 입력합니다. `ssh admin@Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 다음 명령을 실행합니다.

   ```
   restore-default-cipher-configurations
   ```

3. 웹 브라우저에서 동일한 관리 노드의 그리드 관리자에 액세스합니다.
4. 의 단계에 따라 보안 정책을 선택합니다정책을 다시 구성합니다.

네트워크 및 개체 보안을 구성하여 저장된 개체를 암호화하거나, 특정 S3 요청을 방지하거나, 스토리지 노드에 대한 클라이언트 연결이 HTTPS 대신 HTTP를 사용하도록 할 수 있습니다.

저장된 오브젝트 암호화

저장된 오브젝트 암호화를 통해 S3를 통해 수집된 모든 오브젝트 데이터를 암호화할 수 있습니다. 기본적으로 저장된 개체는 암호화되지 않지만 AES - 128 또는 AES - 256 암호화 알고리즘을 사용하여 개체를 암호화하도록 선택할 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.

저장된 오브젝트 암호화 설정은 버킷 레벨 또는 오브젝트 레벨 암호화로 암호화되지 않은 S3 오브젝트에만 적용됩니다.

StorageGRID 암호화 방법에 대한 자세한 내용은 을 "StorageGRID 암호화 방법을 검토합니다"참조하십시오.

클라이언트 수정을 방지합니다

클라이언트 수정 방지 는 시스템 전체 설정입니다. 클라이언트 수정 방지 * 옵션을 선택하면 다음 요청이 거부됩니다.

S3 REST API

- DeleteBucket 요청
- 기존 오브젝트의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태그 지정을 수정하는 요청

스토리지 노드 연결에 대해 **HTTP**를 설정합니다

기본적으로 클라이언트 애플리케이션은 스토리지 노드에 대한 직접 연결에 HTTPS 네트워크 프로토콜을 사용합니다. 비프로덕션 그리드를 테스트할 때와 같이 이러한 연결에 대해 HTTP를 선택적으로 활성화할 수 있습니다.

S3 클라이언트가 스토리지 노드에 직접 HTTP 연결을 만들어야 하는 경우에만 스토리지 노드 연결에 HTTP를 사용합니다. HTTPS 연결만 사용하는 클라이언트 또는 부하 분산 서비스에 연결하는 클라이언트(HTTP 또는 HTTPS를 사용할 수 있으므로)에는 이 옵션을 사용할 필요가 없습니다."각 로드 밸런서 엔드포인트를 구성합니다"

HTTP 또는 HTTPS를 사용하여 스토리지 노드에 연결할 때 S3 클라이언트가 사용하는 포트에 대해 알아보려면 를 참조하십시오"요약: 클라이언트 연결을 위한 IP 주소 및 포트".

옵션을 선택합니다

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 루트 액세스 권한이 있습니다.

단계

1. 구성 * > * 보안 * > * 보안 설정 * 을 선택합니다.
2. Network and objects * 탭을 선택합니다.
3. 저장된 개체 암호화의 경우 저장된 개체를 암호화하지 않으려면 * 없음 * (기본값) 설정을 사용하거나 * AES-128 * 또는 * AES-256 * 을 선택하여 저장된 개체를 암호화합니다.

4. 필요에 따라 S3 클라이언트가 특정 요청을 하지 못하도록 하려면 * 클라이언트 수정 방지 * 를 선택합니다.

   이 설정을 변경하면 새 설정을 적용하는 데 약 1분이 걸립니다. 구성된 값이 성능 및 확장을 위해 캐싱됩니다.

5. 클라이언트가 스토리지 노드에 직접 접속하고 HTTP 연결을 사용하려는 경우 선택적으로 * 스토리지 노드 연결에 HTTP 사용 * 을 선택합니다.

   요청이 암호화되지 않은 상태로 전송되므로 프로덕션 그리드에 대해 HTTP를 설정할 때는 주의해야 합니다.

6. 저장 * 을 선택합니다.

인터페이스 보안 설정을 변경합니다

인터페이스 보안 설정을 사용하면 사용자가 지정된 시간 이상 비활성 상태인 경우 로그아웃할지 여부 및 스택 추적이 API 오류 응답에 포함되는지 여부를 제어할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "루트 액세스 권한"

이 작업에 대해

보안 설정 * 페이지에는 * 브라우저 비활성 시간 제한 * 및 * 관리 API 스택 추적 * 설정이 포함됩니다.

브라우저 비활성 시간 초과

사용자가 로그아웃되기 전까지 사용자의 브라우저가 비활성화될 수 있는 시간을 나타냅니다. 기본값은 15분입니다.

브라우저 비활성 시간 초과는 다음과 같은 방법으로 제어됩니다.

- 시스템 보안을 위해 포함되어 있는 별도의 구성 불가능한 StorageGRID 타이머입니다. 각 사용자의 인증 토큰은 사용자가 로그인한 후 16시간 후에 만료됩니다. 사용자의 인증이 만료되면 브라우저 비활성 시간 제한이 비활성화되거나 브라우저 시간 제한 값에 도달하지 않은 경우에도 해당 사용자는 자동으로 로그아웃됩니다. 토큰을 갱신하려면 사용자가 다시 로그인해야 합니다.
- StorageGRID에 대해 SSO(Single Sign-On)가 활성화된 경우 ID 공급자에 대한 시간 제한 설정입니다.

  SSO가 활성화되어 있고 사용자의 브라우저가 시간 초과되면 사용자는 SSO 자격 증명을 다시 입력하여 StorageGRID에 다시 액세스해야 합니다. 을 "Single Sign-On 구성"참조하십시오.

관리 **API** 스택 추적

Grid Manager 및 Tenant Manager API 오류 응답에서 스택 추적이 반환되는지 여부를 제어합니다.

이 옵션은 기본적으로 비활성화되어 있지만 테스트 환경에서 이 기능을 사용할 수 있습니다. 일반적으로 API 오류가 발생할 때 내부 소프트웨어 세부 정보가 노출되지 않도록 프로덕션 환경에서 스택 추적을 비활성화해야 합니다.

단계

1. 구성 * > * 보안 * > * 보안 설정 * 을 선택합니다.

2. 인터페이스 * 탭을 선택합니다.
3. 브라우저 비활성 시간 초과 설정을 변경하려면:
   a. 아코디언을 확장합니다.
   b. 제한 시간을 변경하려면 60초에서 7일 사이의 값을 지정합니다. 기본 시간 제한은 15분입니다.
   c. 이 기능을 비활성화하려면 확인란을 선택 취소합니다.
   d. 저장 * 을 선택합니다.

      새 설정은 현재 로그인한 사용자에게는 영향을 주지 않습니다. 새 시간 초과 설정을 적용하려면 사용자가 다시 로그인하거나 브라우저를 새로 고쳐야 합니다.
4. 관리 API 스택 추적 설정을 변경하려면 다음을 수행합니다.
   a. 아코디언을 확장합니다.
   b. Grid Manager 및 Tenant Manager API 오류 응답에서 스택 추적을 반환하려면 확인란을 선택합니다.

      API 오류가 발생할 때 내부 소프트웨어 세부 정보가 노출되지 않도록 프로덕션 환경에서 스택 추적을 비활성화하십시오.

   c. 저장 * 을 선택합니다.

키 관리 서버를 구성합니다

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.

StorageGRID는 특정 키 관리 서버만 지원합니다. 지원되는 제품 및 버전 목록을 보려면 을 "NetApp 상호 운용성 매트릭스 툴(IMT)" 사용합니다.

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.

KMS 및 어플라이언스 구성

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 을 "노드 암호화를 설정합니다" 참조하십시오.

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.

지원되는 **KMIP** 버전은 무엇입니까**?**

StorageGRID는 KMIP 버전 1.4를 지원합니다.

"키 관리 상호 운용성 프로토콜 사양 버전 1.4"

네트워크 고려 사항은 무엇입니까**?**

네트워크 방화벽 설정을 통해 각 어플라이언스 노드가 KMIP(Key Management Interoperability Protocol) 통신에 사용되는 포트를 통해 통신할 수 있어야 합니다. 기본 KMIP 포트는 5696입니다.

노드 암호화를 사용하는 각 어플라이언스 노드에서 사이트에 대해 구성한 KMS 또는 KMS 클러스터에 대한 네트워크 액세스 권한이 있는지 확인해야 합니다.

지원되는 **TLS** 버전은 무엇입니까**?**

어플라이언스 노드와 구성된 KMS 간의 통신은 보안 TLS 연결을 사용합니다. StorageGRID는 KMS가 지원하는 것과 사용 중인 것에 따라 KMS 또는 KMS 클러스터에 KMIP 연결을 설정할 때 TLS 1.2 또는 TLS 1.3 프로토콜을 지원할 수 있습니다"TLS 및 SSH 정책".

StorageGRID는 연결을 만들 때 KMS와 프로토콜 및 암호(TLS 1.2) 또는 암호 그룹(TLS 1.3)을 협상합니다. 사용할 수 있는 프로토콜 버전 및 암호화/암호화 제품군을 확인하려면 `tlsOutbound` 그리드의 활성 TLS 및 SSH 정책(* 구성 * > * 보안 * * * * 보안 설정 *) 섹션을 검토하십시오.

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 어플라이언스에는 외부 키 관리를 사용할 수 없습니다.

구성된 KMS for StorageGRID 어플라이언스 및 어플라이언스 노드를 사용할 수 있습니다.

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.

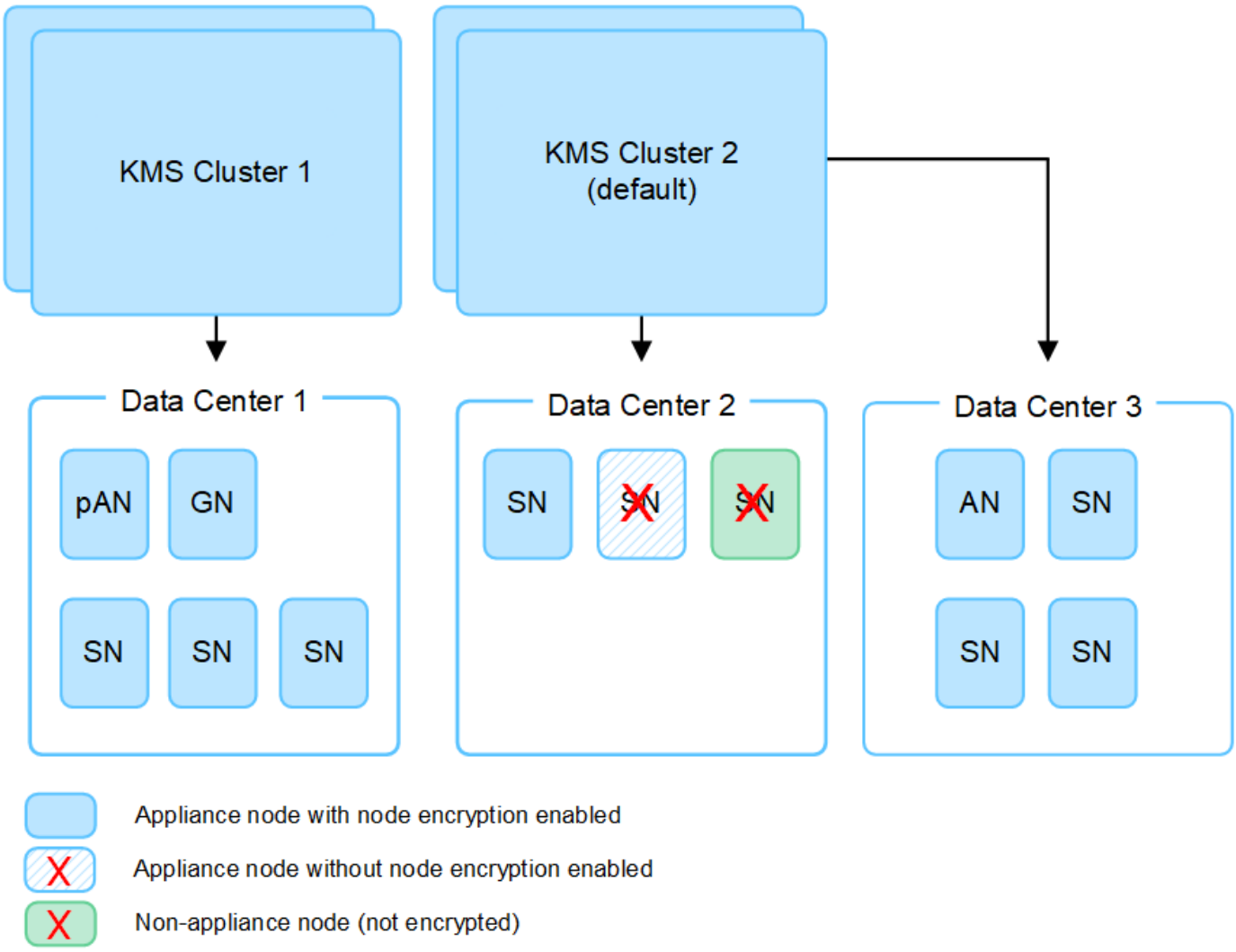
몇 개의 키 관리 서버가 필요합니까?

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 주기적으로 사용해야 "암호화 키를 회전합니다"합니다.

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 에연결할 수 "KMS 구성을 지웁니다" 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.

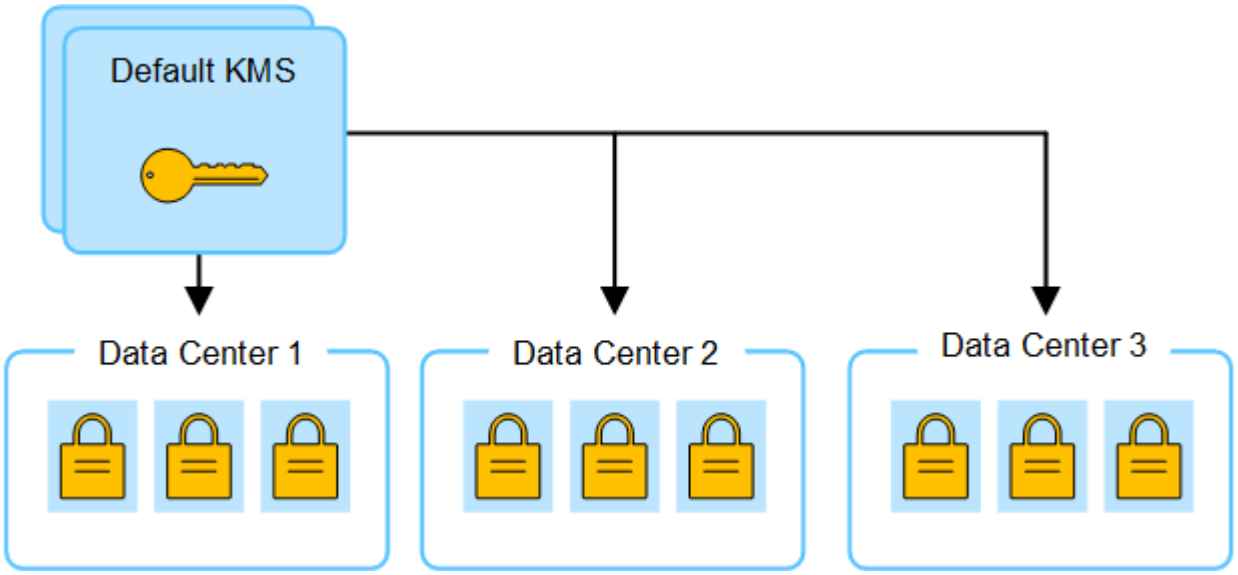
사이트의 **KMS**를 변경할 때의 고려 사항

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.

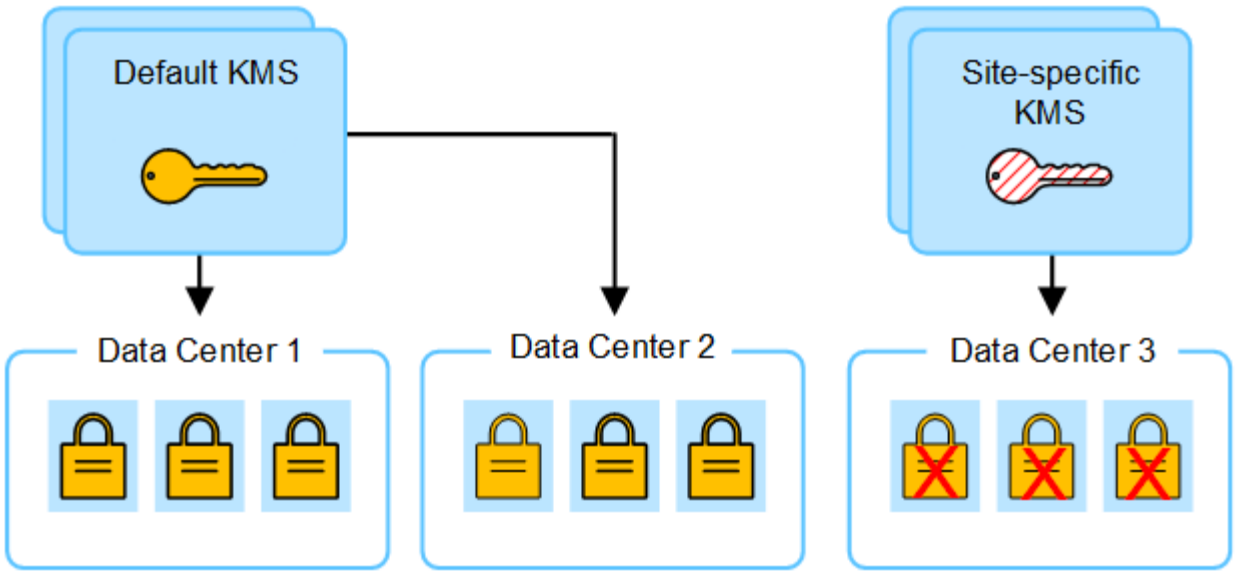
사이트에 사용되는 KMS를 변경하는 경우 해당 사이트에서 이전에 암호화된 어플라이언스 노드를 새 KMS에 저장된 키를 사용하여 해독할 수 있는지 확인해야 합니다. 경우에 따라 기존 KMS에서 새 KMS로 최신 버전의 암호화 키를 복사해야 할 수도 있습니다. KMS가 사이트에서 암호화된 어플라이언스 노드를 해독할 수 있는 올바른 키를 가지고 있는지 확인해야 합니다.

예를 들면 다음과 같습니다.

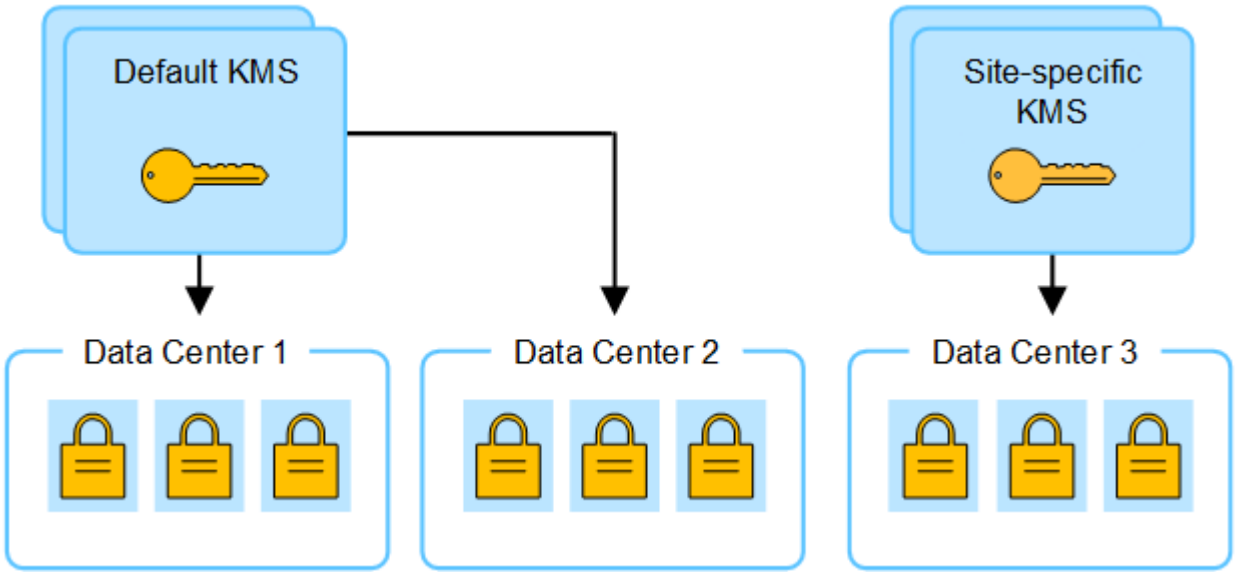
1. 처음에는 전용 KMS가 없는 모든 사이트에 적용되는 기본 KMS를 구성합니다.
2. KMS가 저장되면 * 노드 암호화 * 설정이 활성화된 모든 어플라이언스 노드가 KMS에 연결하여 암호화 키를 요청합니다. 이 키는 모든 사이트에서 어플라이언스 노드를 암호화하는 데 사용됩니다. 이러한 어플라이언스의 암호를 해독하는 데에도 이 동일한 키를 사용해야 합니다.



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.) 사이트별 KMS에는 이제 데이터 센터 3에서 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"

사이트의 **KMS**를 변경하는 사용 사례	필요한 단계
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"

KMS에서 **StorageGRID**를 클라이언트로 구성합니다

KMS를 StorageGRID에 추가하려면 각 외부 키 관리 서버 또는 KMS 클러스터에 대해 StorageGRID를 클라이언트로 구성해야 합니다.

이러한 지침은 Thales CipherTrust Manager 및 Hashicorp Vault에 적용됩니다. 지원되는 제품 및 버전 목록을 보려면 을 "NetApp 상호 운용성 매트릭스 툴(IMT)" 사용합니다.

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. 다음 두 가지 방법 중 하나를 사용하여 키를 만듭니다.
   - KMS 제품의 키 관리 페이지를 사용합니다. 각 KMS 또는 KMS 클러스터에 대해 AES 암호화 키를 생성합니다.

     암호화 키는 2,048비트 이상이어야 하며 내보낼 수 있어야 합니다.

   - StorageGRID에서 키를 생성하도록 합니다. 테스트 후 저장하면 메시지가 "클라이언트 인증서를 업로드하는 중입니다"표시됩니다.
3. 각 KMS 또는 KMS 클러스터에 대해 다음 정보를 기록합니다.

   KMS를 StorageGRID에 추가할 때 다음 정보가 필요합니다.

   - 각 서버의 호스트 이름 또는 IP 주소입니다.
   - KMS에서 KMIP 포트를 사용합니다.
   - KMS의 암호화 키에 대한 키 별칭입니다.
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.

KMS(키 관리 서버**)** 추가

StorageGRID 키 관리 서버 마법사를 사용하여 각 KMS 또는 KMS 클러스터를 추가합니다.

시작하기 전에

- 를 검토했습니다."키 관리 서버 사용에 대한 고려 사항 및 요구 사항"
- "KMS에서 StorageGRID를 클라이언트로 구성했습니다"각 KMS 또는 KMS 클러스터에 필요한 정보가 있습니다.
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"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. 자세한 내용은 을 "사이트의 KMS를 변경할 때의 고려 사항" 참조하십시오.

1단계**: KMS** 세부 정보

KMS(Key Management Server 추가) 마법사의 1단계(KMS 세부 정보)에서 KMS 또는 KMS 클러스터에 대한 세부 정보를 제공합니다.

단계

1. 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   구성 세부 정보 탭이 선택된 키 관리 서버 페이지가 나타납니다.

2. Create * 를 선택합니다.

   키 관리 서버 추가 마법사의 1단계(KMS 세부 정보)가 나타납니다.

3. KMS에 구성한 KMS 및 StorageGRID 클라이언트에 대한 다음 정보를 입력합니다.

필드에 입력합니다	설명
KMS 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. • 참고 *: KMS 제품을 사용하여 키를 만들지 않은 경우 StorageGRID에서 키를 만들라는 메시지가 표시됩니다.
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. • 전용 KMS가 없는 사이트와 후속 확장에 추가한 사이트에 적용되는 기본 KMS를 구성하려면 * 다른 KMS(기본 KMS)에서 관리하지 않는 사이트 * 를 선택합니다. ◦ 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.
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 주체 대체 이름(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 * 다른 호스트 이름 추가 * 를 선택하여 클러스터의 각 서버에 대한 호스트 이름을 추가합니다.
5. Continue * 를 선택합니다.

2단계**:** 서버 인증서를 업로드합니다

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. Continue * 를 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.
5. 테스트 및 저장 * 을 선택합니다.

   키가 없으면 StorageGRID에서 키를 만들라는 메시지가 표시됩니다.

   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. 테스트 및 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.

KMS를 관리합니다

KMS(키 관리 서버) 관리에는 세부 정보 보기 또는 편집, 인증서 관리, 암호화된 노드 보기, KMS

제거 등이 포함됩니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "필수 액세스 권한"있습니다.

KMS 세부 정보 보기

키 세부 정보, 서버 및 클라이언트 인증서의 현재 상태 등 StorageGRID 시스템의 각 KMS(키 관리 서버)에 대한 정보를 볼 수 있습니다.

단계

1. 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   키 관리 서버 페이지가 나타나고 다음 정보가 표시됩니다.

   - 구성 세부 정보 탭에는 구성된 모든 키 관리 서버가 나열됩니다.
   - 암호화된 노드 탭에는 노드 암호화가 활성화된 모든 노드가 나열됩니다.

2. 특정 KMS에 대한 세부 정보를 보고 해당 KMS에 대한 작업을 수행하려면 KMS의 이름을 선택합니다. KMS의 세부 정보 페이지에는 다음 정보가 나열됩니다.

필드에 입력합니다	설명
의 키를 관리합니다	KMS와 관련된 StorageGRID 사이트 이 필드에는 특정 StorageGRID 사이트 또는 다른 KMS(기본 KMS)가 관리하지 않는 사이트의 이름이 표시됩니다.*
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. 예 `10.10.10.10 and 10.10.10.11`: 또는 `10.10.10.10 and 2 others`. 클러스터의 모든 호스트 이름을 보려면 KMS를 선택하고 * 편집 * 또는 * 작업 * > * 편집 * 을 선택합니다.

3. KMS 세부 정보 페이지에서 탭을 선택하여 다음 정보를 봅니다.

탭을 클릭합니다	필드에 입력합니다	설명
키 세부 정보	키 이름	KMS에서 StorageGRID 클라이언트의 키 별칭입니다.

탭을 클릭합니다	필드에 입력합니다	설명
키 UID	최신 버전의 키에 대한 고유 식별자입니다.	마지막 수정
키의 최신 버전 날짜 및 시간입니다.	서버 인증서	메타데이터
인증서의 메타데이터(예: 일련 번호, 만료 날짜 및 시간, 인증서 PEM)	인증서 PEM	인증서에 대한 PEM(개인 정보 보호 강화 메일) 파일의 내용입니다.
클라이언트 인증서	메타데이터	인증서의 메타데이터(예: 일련 번호, 만료 날짜 및 시간, 인증서 PEM)

4.] 조직의 보안 관행에 필요한 만큼 * Rotate key * 를 선택하거나 KMS 소프트웨어를 사용하여 새 버전의 키를 만듭니다.

   키 회전이 성공하면 키 UID 및 마지막으로 수정된 필드가 업데이트됩니다.

> KMS 소프트웨어를 사용하여 암호화 키를 회전하는 경우 마지막으로 사용한 키 버전에서 동일한 키의 새 버전으로 회전합니다. 완전히 다른 키로 회전하지 마십시오.
>
> KMS의 키 이름(별칭)을 변경하여 키를 회전하려고 하지 마십시오. 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.

인증서를 관리합니다

모든 서버 또는 클라이언트 인증서 문제를 즉시 해결합니다. 가능하면 만료되기 전에 인증서를 교체하십시오.

> 데이터 액세스를 유지하려면 가능한 한 빨리 인증서 문제를 해결해야 합니다.

단계

1. 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.
2. 표에서 각 KMS에 대한 인증서 만료 값을 확인합니다.
3. KMS에 대한 인증서 만료가 알 수 없는 경우 최대 30분 정도 기다린 다음 웹 브라우저를 새로 고칩니다.
4. 인증서 만료 열에 인증서가 만료되었거나 만료가 임박했음을 나타내는 경우 KMS를 선택하여 KMS 세부 정보 페이지로 이동합니다.
   a. 서버 인증서 * 를 선택하고 "만료 날짜" 필드에 대한 값을 확인합니다.
   b. 인증서를 교체하려면 * 인증서 편집 * 을 선택하여 새 인증서를 업로드합니다.
   c. 이 하위 단계를 반복하고 서버 인증서 대신 * 클라이언트 인증서 * 를 선택합니다.

5. KMS CA 인증서 만료 *, * KMS 클라이언트 인증서 만료 * 및 * KMS 서버 인증서 만료 * 알림이 트리거되면 각 경고에 대한 설명을 기록하고 권장 조치를 수행합니다.

   인증서 만료에 대한 업데이트를 받는 데 30분 정도 걸릴 수 StorageGRID 있습니다. 현재 값을 보려면 웹 브라우저를 새로 고치십시오.

> 서버 인증서 상태가 알 수 없음 * 인 경우 KMS에서 클라이언트 인증서 없이도 서버 인증서를 받을 수 있도록 허용하는지 확인합니다.

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 유형입니다	노드 유형: 스토리지, 관리자 또는 게이트웨이
사이트	노드가 설치된 StorageGRID 사이트의 이름입니다.
KMS 이름	노드에 사용된 KMS의 설명 이름입니다. KMS가 나열되지 않으면 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 텍스트를 선택합니다. 대시(--)는 어플라이언스 노드와 KMS 사이의 연결 문제로 인해 키 UID를 알 수 없음을 나타냅니다.

열	설명
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 고치십시오.

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

   이러한 경고에 대해 권장되는 작업을 수행합니다.

   데이터를 완벽하게 보호하려면 모든 문제를 즉시 해결해야 합니다.

KMS를 편집합니다

예를 들어 인증서가 곧 만료될 경우 키 관리 서버의 구성을 편집해야 할 수 있습니다.

시작하기 전에

- KMS에 대해 선택한 사이트를 업데이트할 계획이 있는 경우 를 검토한 "사이트의 KMS를 변경할 때의 고려 사항 "것입니다.
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.

단계

1. 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   키 관리 서버 페이지가 나타나고 구성된 모든 키 관리 서버가 표시됩니다.

2. 편집할 KMS를 선택하고 * Actions * > * Edit * 를 선택합니다.

   KMS 세부 정보 페이지에서 KMS 이름을 선택하고 * 편집 * 을 선택하여 KMS를 편집할 수도 있습니다.

3. 선택적으로 키 관리 서버 편집 마법사의 * 1단계(KMS 세부 정보) * 에 있는 세부 정보를 업데이트합니다.

필드에 입력합니다	설명
KMS 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.
의 키를 관리합니다	사이트별 KMS를 편집하고 있고 기본 KMS가 아직 없는 경우 선택적으로 * 다른 KMS(기본 KMS)에서 관리하지 않는 사이트 * 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 경우 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 주체 대체 이름(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 * 다른 호스트 이름 추가 * 를 선택하여 클러스터의 각 서버에 대한 호스트 이름을 추가합니다.
5. Continue * 를 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. Continue * 를 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. 테스트 및 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 구성이 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.

시작하기 전에

- 를 검토했습니다."키 관리 서버 사용에 대한 고려 사항 및 요구 사항"
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"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.

키 관리 서버 페이지가 나타나고 구성된 모든 키 관리 서버가 표시됩니다.

2. 제거할 KMS를 선택하고 * Actions * > * Remove * 를 선택합니다.

KMS 세부 정보 페이지에서 KMS 이름을 선택하고 * Remove * 를 선택하여 KMS를 제거할 수도 있습니다.

3. 다음 내용이 맞는지 확인합니다.
   - 노드 암호화가 활성화된 어플라이언스 노드가 없는 사이트에 대한 사이트별 KMS를 제거하고 있습니다.
   - 기본 KMS를 제거하고 있지만 노드 암호화를 사용하는 각 사이트에 대해 사이트별 KMS가 이미 있습니다.
4. 예 * 를 선택합니다.

KMS 구성이 제거되었습니다.

스토리지 프록시를 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.

구성된 스토리지 프록시 설정은 Kafka 플랫폼 서비스 엔드포인트에 적용되지 않습니다.

시작하기 전에

- 있습니다. "특정 액세스 권한"
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"

이 작업에 대해

단일 스토리지 프록시에 대한 설정을 구성할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 프록시 설정 * 을 선택합니다.
2. Storage * 탭에서 * Enable storage proxy * 확인란을 선택합니다.
3. 스토리지 프록시의 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 사용하려면 이 필드를 비워 둡니다.

6. 저장 * 을 선택합니다.

   스토리지 프록시가 저장된 후 플랫폼 서비스 또는 클라우드 스토리지 풀의 새 엔드포인트를 구성하고 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.
8. 스토리지 프록시를 비활성화해야 하는 경우 확인란을 선택 취소하고 * 저장 * 을 선택합니다.

관리자 프록시 설정을 구성합니다

HTTP 또는 HTTPS를 사용하여 AutoSupport 패키지를 보내는 경우 관리 노드와 기술 지원(AutoSupport) 간에 비투명 프록시 서버를 구성할 수 있습니다.

AutoSupport에 대한 자세한 내용은 을 "AutoSupport를 구성합니다"참조하십시오.

시작하기 전에

- 있습니다. "특정 액세스 권한"

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"

이 작업에 대해

단일 관리자 프록시에 대한 설정을 구성할 수 있습니다.

단계

1. 구성 * > * 보안 * > * 프록시 설정 * 을 선택합니다.

   프록시 설정 페이지가 나타납니다. 기본적으로 탭 메뉴에서 스토리지가 선택되어 있습니다.

2. 관리 * 탭을 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. 필요한 경우 프록시 서버의 사용자 이름과 암호를 입력합니다.

   프록시 서버에 사용자 이름 또는 암호가 필요하지 않은 경우 이 필드를 비워 둡니다.

7. 다음 중 하나를 선택합니다.

   - 관리자 프록시에 대한 연결을 보호하려면 * 프록시 인증서 확인 * 을 선택합니다. CA 번들을 업로드하여 관리 프록시 서버에서 제공하는 SSL 인증서의 신뢰성을 확인합니다.

     프록시 인증서가 확인된 경우 AutoSupport on Demand, StorageGRID를 통한 E-Series AutoSupport 및 StorageGRID 업그레이드 페이지의 업데이트 경로 확인이 작동하지 않습니다.

   CA 번들을 업로드하면 해당 메타데이터가 나타납니다.

   - 관리자 프록시 서버와 통신할 때 인증서의 유효성을 검사하지 않으려면 * 프록시 인증서 확인 안 함 * 을 선택합니다.

8. 저장 * 을 선택합니다.

   관리자 프록시가 저장된 후 관리 노드와 기술 지원 간의 프록시 서버가 구성됩니다.

   프록시 변경 사항이 적용되려면 최대 10분이 소요될 수 있습니다.

9. 관리자 프록시를 비활성화해야 하는 경우 * 관리자 프록시 사용 * 확인란의 선택을 취소한 다음 * 저장 * 을 선택합니다.

방화벽을 제어합니다

외부 방화벽에서 액세스를 제어합니다

외부 방화벽에서 특정 포트를 열거나 닫을 수 있습니다.

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.

StorageGRID 내부 방화벽을 구성하려면 를 참조하십시오"내부 방화벽을 구성합니다".

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"

내부 방화벽 제어를 관리합니다

StorageGRID에는 노드에 대한 네트워크 액세스를 제어할 수 있도록 함으로써 그리드의 보안을 강화하는 각 노드에 대한 내부 방화벽이 포함되어 있습니다. 방화벽을 사용하여 특정 그리드 구축에 필요한 포트를 제외한 모든 포트의 네트워크 액세스를 방지합니다. 방화벽 제어 페이지에서 변경한 구성은 각 노드에 배포됩니다.

방화벽 제어 페이지의 세 가지 탭을 사용하여 그리드에 필요한 액세스를 사용자 지정합니다.

- * 특별 권한 주소 목록 *: 이 탭을 사용하면 닫힌 포트에 대한 선택된 액세스를 허용할 수 있습니다. 외부 액세스 관리 탭을 사용하여 닫은 포트에 액세스할 수 있는 IP 주소 또는 서브넷을 CIDR 표시법으로 추가할 수 있습니다.
- * 외부 액세스 관리 *: 이 탭을 사용하여 기본적으로 열려 있는 포트를 닫거나 이전에 닫은 포트를 다시 열 수 있습니다.

- * 신뢰할 수 없는 클라이언트 네트워크 *: 노드가 클라이언트 네트워크의 인바운드 트래픽을 신뢰하는지 여부를 지정하려면 이 탭을 사용합니다.

  이 탭의 설정은 외부 액세스 관리 탭의 설정보다 우선합니다.

  - 신뢰할 수 없는 클라이언트 네트워크가 있는 노드는 해당 노드에 구성된 로드 밸런서 엔드포인트 포트(글로벌, 노드 인터페이스 및 노드 유형 바운드 엔드포인트)의 연결만 받아들입니다.
  - 부하 분산 장치 엔드포인트 포트 _ 는(는) 신뢰할 수 없는 클라이언트 네트워크에서 외부 네트워크 관리 탭의 설정에 관계없이 열려 있는 유일한 포트입니다.
  - 신뢰할 수 있는 경우 외부 액세스 관리 탭에서 열린 모든 포트와 클라이언트 네트워크에 열려 있는 모든 로드 밸런서 끝점에 액세스할 수 있습니다.

> ⓘ 한 탭에서 설정한 내용은 다른 탭의 액세스 변경에 영향을 줄 수 있습니다. 모든 탭의 설정을 확인하여 네트워크가 예상한 대로 작동하는지 확인하십시오.

내부 방화벽 제어를 구성하려면 를 참조하십시오"방화벽 제어를 구성합니다".

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 을 "외부 방화벽에서 액세스를 제어합니다"참조하십시오.

특별 권한 주소 목록 및 외부 액세스 관리 탭

특별 권한 주소 목록 탭을 사용하면 닫힌 그리드 포트에 대한 액세스 권한이 부여된 하나 이상의 IP 주소를 등록할 수 있습니다. 외부 액세스 관리 탭을 사용하면 선택한 외부 포트 또는 열려 있는 모든 외부 포트에 대한 외부 액세스를 닫을 수 있습니다(외부 포트는 기본적으로 비 그리드 노드가 액세스할 수 있는 포트입니다). 이러한 두 탭을 함께 사용하여 그리드에 필요한 정확한 네트워크 액세스를 사용자 지정할 수 있습니다.

> ⓘ 권한이 있는 IP 주소는 기본적으로 내부 그리드 포트 액세스를 갖지 않습니다.

예 **1:** 유지 보수 작업에 점프 호스트를 사용합니다

네트워크 관리에 점프 호스트(보안 강화 호스트)를 사용하려는 경우를 가정해 보겠습니다. 다음과 같은 일반 단계를 사용할 수 있습니다.

1. 특별 권한 주소 목록 탭을 사용하여 점프 호스트의 IP 주소를 추가합니다.
2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단합니다.

> ⓘ 포트 443 및 8443을 차단하기 전에 권한이 있는 IP 주소를 추가합니다. 사용자를 포함하여 현재 차단된 포트에 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다.

구성을 저장하면 이동 호스트를 제외한 모든 호스트에 대해 그리드의 관리 노드에 있는 모든 외부 포트가 차단됩니다. 그런 다음 점프 호스트를 사용하여 그리드에 대한 유지 관리 작업을 보다 안전하게 수행할 수 있습니다.

예 **2:** 민감한 포트를 잠급니다

중요한 포트와 해당 포트의 서비스(예: 포트 22의 SSH)를 잠그려고 한다고 가정합니다. 다음과 같은 일반 단계를 사용할 수 있습니다.

1. 특별 권한 주소 목록 탭을 사용하여 서비스에 액세스해야 하는 호스트에만 액세스 권한을 부여합니다.

2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단합니다.

> Grid Manager 및 Tenant Manager 액세스에 할당된 포트에 대한 액세스를 차단하기 전에 권한 있는 IP 주소를 추가합니다(사전 설정된 포트는 443 및 8443). 사용자를 포함하여 현재 차단된 포트에 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다.

구성을 저장하면 권한이 있는 주소 목록의 호스트에서 포트 22 및 SSH 서비스를 사용할 수 있습니다. 다른 모든 호스트는 요청이 어떤 인터페이스에서 제공되든 서비스에 대한 액세스가 거부됩니다.

예 **3:** 사용하지 않는 서비스에 대한 액세스를 비활성화합니다

네트워크 수준에서는 사용하지 않을 일부 서비스를 사용하지 않도록 설정할 수 있습니다. 예를 들어 HTTP S3 클라이언트 트래픽을 차단하려면 외부 액세스 관리 탭의 토글을 사용하여 포트 18084를 차단할 수 있습니다.

신뢰할 수 없는 클라이언트 네트워크 탭

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 모든 의 각 그리드 노드에 대한 인바운드 연결을 신뢰합니다."사용 가능한 외부 포트"

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. "로드 밸런서 엔드포인트를 구성합니다"및 을 "방화벽 제어를 구성합니다 "참조하십시오.

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. "부하 분산 장치 엔드포인트"페이지에서 포트 443에서 HTTPS를 통한 S3에 대한 로드 밸런서 끝점을 구성합니다.
2. 방화벽 제어 페이지에서 신뢰할 수 없음 을 선택하여 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.

- 방화벽 제어 페이지의 신뢰할 수 없는 클라이언트 네트워크 탭에서 스토리지 노드의 클라이언트 네트워크를 신뢰할 수 없음을 나타냅니다.

구성을 저장한 후 스토리지 노드는 더 이상 클라이언트 네트워크에서 들어오는 트래픽을 허용하지 않지만 구성된 플랫폼 서비스 대상에 대한 아웃바운드 요청은 계속 허용합니다.

예 **3:** 그리드 관리자에 대한 액세스를 서브넷으로 제한

특정 서브넷에서만 Grid Manager 액세스를 허용한다고 가정합니다. 다음 단계를 수행합니다.

1. 관리 노드의 클라이언트 네트워크를 서브넷에 연결합니다.
2. 신뢰할 수 없는 클라이언트 네트워크 탭을 사용하여 클라이언트 네트워크를 신뢰할 수 없음으로 구성합니다.
3. 관리 인터페이스 로드 밸런서 엔드포인트를 생성할 때 port를 입력하고 포트가 액세스할 관리 인터페이스를 선택합니다.
4. 신뢰할 수 없는 클라이언트 네트워크에 대해 * 예 * 를 선택합니다.
5. 외부 액세스 관리 탭을 사용하여 모든 외부 포트(해당 서브넷 외부의 호스트에 대해 설정된 권한이 있는 IP 주소 포함 또는 제외)를 차단합니다.

구성을 저장한 후에는 지정한 서브넷의 호스트만 Grid Manager에 액세스할 수 있습니다. 다른 호스트는 모두 차단됩니다.

내부 방화벽을 구성합니다

StorageGRID 노드의 특정 포트에 대한 네트워크 액세스를 제어하도록 StorageGRID 방화벽을 구성할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"
- 및 의 정보를 검토했습니다."방화벽 제어 관리""네트워킹 지침"
- 관리자 노드 또는 게이트웨이 노드가 명시적으로 구성된 끝점에서만 인바운드 트래픽을 수락하도록 하려면 로드 밸런서 끝점을 정의해야 합니다.

> 클라이언트 네트워크의 구성을 변경할 때 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

이 작업에 대해

StorageGRID에는 그리드의 노드에서 일부 포트를 열거나 닫을 수 있도록 각 노드에 대한 내부 방화벽이 포함되어 있습니다. 방화벽 제어 탭을 사용하여 그리드 네트워크, 관리자 네트워크 및 클라이언트 네트워크에서 기본적으로 열려 있는 포트를 열거나 닫을 수 있습니다. 닫힌 그리드 포트에 액세스할 수 있는 권한이 있는 IP 주소 목록을 만들 수도 있습니다. 클라이언트 네트워크를 사용하는 경우 노드가 클라이언트 네트워크의 인바운드 트래픽을 신뢰하는지 여부를 지정하고 클라이언트 네트워크의 특정 포트에 대한 액세스를 구성할 수 있습니다.

그리드 외부의 IP 주소에 열려 있는 포트 수를 절대적으로 필요한 포트로만 제한하면 그리드의 보안이 향상됩니다. 세 개의 방화벽 제어 탭 각각에서 설정을 사용하여 필요한 포트만 열도록 합니다.

예를 비롯한 방화벽 제어 사용에 대한 자세한 내용은 을 참조하십시오"방화벽 제어 관리".

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 을 "외부 방화벽에서 액세스를 제어합니다"참조하십시오.

방화벽 컨트롤에 액세스합니다

단계

1. 구성 * > * 보안 * > * 방화벽 제어 * 를 선택합니다.

   이 페이지의 세 가지 탭은 에 "방화벽 제어 관리"설명되어 있습니다.

2. 탭을 선택하여 방화벽 컨트롤을 구성합니다.

   이러한 탭은 순서에 상관없이 사용할 수 있습니다. 한 탭에서 설정한 구성은 다른 탭에서 수행할 수 있는 작업을 제한하지 않지만 한 탭에서 변경한 구성은 다른 탭에 구성된 포트의 동작을 변경할 수 있습니다.

특별 권한 주소 목록

특별 권한 주소 목록 탭을 사용하여 외부 액세스 관리 탭의 설정에 따라 기본적으로 닫히거나 닫힌 포트에 대한 호스트 액세스 권한을 부여할 수 있습니다.

권한이 있는 IP 주소 및 서브넷에는 기본적으로 내부 그리드 액세스가 없습니다. 또한 외부 액세스 관리 탭에서 차단된 경우에도 권한이 있는 주소 목록 탭에서 열린 로드 밸런서 끝점과 추가 포트에 액세스할 수 있습니다.

> 권한이 있는 주소 목록 탭의 설정은 신뢰할 수 없는 클라이언트 네트워크 탭의 설정을 재정의할 수 없습니다.

단계

1. 특별 권한 주소 목록 탭에서 닫힌 포트에 대한 액세스를 허용할 주소 또는 IP 서브넷을 입력합니다.
2. 선택적으로 * CIDR 표기법 * 으로 다른 IP 주소 또는 서브넷 추가 를 선택하여 권한이 있는 클라이언트를 추가합니다.

   > 가능한 한 적은 수의 주소를 권한 있는 목록에 추가합니다.

3. 선택적으로 * 권한이 있는 IP 주소가 StorageGRID 내부 포트에 액세스하도록 허용 * 을 선택합니다. 을 "StorageGRID 내부 포트"참조하십시오.

   > 이 옵션은 내부 서비스에 대한 일부 보호를 제거합니다. 가능한 경우 비활성화 상태로 둡니다.

4. 저장 * 을 선택합니다.

외부 액세스를 관리합니다

외부 액세스 관리 탭에서 포트가 닫힌 경우 권한이 있는 주소 목록에 IP 주소를 추가하지 않으면 비 그리드 IP 주소로 포트에 액세스할 수 없습니다. 기본적으로 열려 있는 포트만 닫을 수 있으며 닫은 포트만 열 수 있습니다.

> 외부 액세스 관리 탭의 설정은 신뢰할 수 없는 클라이언트 네트워크 탭의 설정을 재정의할 수 없습니다. 예를 들어, 노드가 신뢰할 수 없는 경우 외부 액세스 관리 탭에 열려 있어도 클라이언트 네트워크에서 포트 SSH/22가 차단됩니다. 신뢰할 수 없는 클라이언트 네트워크 탭의 설정은 클라이언트 네트워크의 닫힌 포트(예: 443, 8443, 9443)를 재정의합니다.

단계

1. 외부 액세스 관리 * 를 선택합니다. 이 탭에는 그리드의 노드에 대해 모든 외부 포트(기본적으로 비 그리드 노드가 액세스할 수 있는 포트)가 포함된 테이블이 표시됩니다.
2. 다음 옵션을 사용하여 열고 닫을 포트를 구성합니다.

- 각 포트 옆의 토글을 사용하여 선택한 포트를 열거나 닫습니다.
- 표시된 모든 포트 열기 * 를 선택하여 표에 나열된 모든 포트를 엽니다.
- 표에 나열된 모든 포트를 닫으려면 * 표시된 모든 포트 닫기 * 를 선택합니다.

> Grid Manager 포트 443 또는 8443을 닫으면 사용자를 포함하여 차단된 포트에 현재 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다.

> 테이블 오른쪽에 있는 스크롤 막대를 사용하여 사용 가능한 모든 포트를 확인합니다. 검색 필드를 사용하여 포트 번호를 입력하여 외부 포트의 설정을 찾습니다. 일부 포트 번호를 입력할 수 있습니다. 예를 들어 * 2 * 를 입력하면 이름에 문자열 "2"가 포함된 모든 포트가 표시됩니다.

3. 저장 * 을 선택합니다

신뢰할 수 없는 클라이언트 네트워크

노드의 클라이언트 네트워크를 신뢰할 수 없는 경우 노드는 로드 밸런서 끝점으로 구성된 포트의 인바운드 트래픽만 허용하고 선택적으로 이 탭에서 선택하는 추가 포트만 허용합니다. 이 탭을 사용하여 확장에 추가된 새 노드의 기본 설정을 지정할 수도 있습니다.

> 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

신뢰할 수 없는 클라이언트 네트워크* 탭에서 변경한 구성은 * 외부 액세스 관리 * 탭의 설정보다 우선합니다.

단계

1. 신뢰할 수 없는 클라이언트 네트워크 * 를 선택합니다.
2. 새 노드 기본값 설정 섹션에서 확장 절차에서 그리드에 새 노드를 추가할 때 기본 설정을 지정합니다.
   - * 신뢰 * (기본값): 확장 시 노드를 추가하면 해당 클라이언트 네트워크가 신뢰됩니다.
   - * 신뢰할 수 없음 *: 확장 시 노드가 추가되면 해당 클라이언트 네트워크를 신뢰할 수 없습니다.

     필요에 따라 이 탭으로 돌아가 특정 새 노드의 설정을 변경할 수 있습니다.

     > 이 설정은 StorageGRID 시스템의 기존 노드에는 영향을 주지 않습니다.

3. 다음 옵션을 사용하여 명시적으로 구성된 로드 밸런싱 장치 엔드포인트 또는 추가 선택 포트에서만 클라이언트 연결을 허용할 노드를 선택합니다.
   - 표시된 노드에서 신뢰 해제 * 를 선택하여 테이블에 표시된 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가합니다.
   - 표시된 노드의 신뢰 * 를 선택하여 신뢰할 수 없는 클라이언트 네트워크 목록에서 표에 표시된 모든 노드를 제거합니다.
   - 각 노드 옆의 토글을 사용하여 선택한 노드에 대해 클라이언트 네트워크를 신뢰할 수 있는 또는 신뢰할 수 없는 것으로 설정합니다.

     예를 들어 표시된 노드에서 * 언트러스트 * 를 선택하여 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가한 다음 개별 노드 옆의 토글을 사용하여 해당 단일 노드를 신뢰할 수 있는 클라이언트 네트워크

목록에 추가할 수 있습니다.

> 테이블 오른쪽에 있는 스크롤 막대를 사용하여 사용 가능한 모든 노드를 확인합니다. 검색 필드를 사용하여 노드 이름을 입력하여 노드 설정을 찾습니다. 부분 이름을 입력할 수 있습니다. 예를 들어 * GW * 를 입력하면 이름에 "GW" 문자열이 포함된 모든 노드가 표시됩니다.

4. 저장 * 을 선택합니다.

   새 방화벽 설정이 즉시 적용되고 적용됩니다. 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

테넌트 관리

테넌트 계정이란 무엇입니까?

테넌트 계정을 사용하면 S3(Simple Storage Service) REST API를 사용하여 StorageGRID 시스템에 오브젝트를 저장하고 검색할 수 있습니다.

> 이 버전의 문서 사이트에서 Swift 세부 정보가 제거되었습니다. 을 "StorageGRID 11.8: 테넌트 관리 "참조하십시오.

그리드 관리자는 S3 클라이언트가 오브젝트를 저장하고 검색하는 데 사용하는 테넌트 계정을 만들고 관리합니다.

각 테넌트 계정에는 페더레이션 또는 로컬 그룹, 사용자, S3 버킷 및 오브젝트가 있습니다.

테넌트 계정은 저장된 객체를 다른 엔터티로 분리하는 데 사용할 수 있습니다. 예를 들어, 다음과 같은 사용 사례에서 여러 테넌트 계정을 사용할 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 계정을 사용할 필요가 없습니다. 자세한 내용은 구현 지침을 "S3 버킷 및 버킷 정책"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.

자세한 내용은 을 "테넌트 계정을 사용합니다"참조하십시오.

테넌트 계정은 어떻게 생성합니까?

그리드 관리자를 사용하여 테넌트 계정을 생성합니다. 테넌트 계정을 생성할 때 다음 정보를 지정합니다.

- 테넌트 이름, 클라이언트 유형(S3) 및 선택적 스토리지 할당량을 포함한 기본 정보입니다.
- 테넌트 계정에서 S3 플랫폼 서비스를 사용할 수 있는지 여부, 해당 ID 소스를 구성할 수 있는지 여부, S3 Select를 사용할 것인지, 그리드 페더레이션 연결을 사용할 수 있는지 여부 등의 테넌트 계정에 대한 사용 권한

- StorageGRID 시스템에서 로컬 그룹 및 사용자, ID 페더레이션 또는 SSO(Single Sign-On)를 사용하는지 여부에 따라 테넌트의 초기 루트 액세스입니다.

또한 S3 테넌트 계정이 규정 요구 사항을 준수해야 하는 경우 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.

테넌트 관리자는 무엇에 사용됩니까?

테넌트 계정을 생성한 후 테넌트 사용자는 테넌트 관리자에 로그인하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 페더레이션 설정(ID 소스가 그리드와 공유되지 않는 경우)
- 그룹 및 사용자를 관리합니다
- 계정 클론 및 교차 그리드 복제에 그리드 페더레이션을 사용합니다
- S3 액세스 키를 관리합니다
- S3 버킷을 생성하고 관리합니다
- S3 플랫폼 서비스 사용
- S3 Select를 사용합니다
- 스토리지 사용량을 모니터링합니다

S3 테넌트 사용자는 테넌트 관리자를 사용하여 S3 액세스 키와 버킷을 생성하고 관리할 수 있지만, S3 클라이언트 애플리케이션을 사용하여 오브젝트를 수집 및 관리해야 합니다. 자세한 내용은 을 "S3 REST API 사용" 참조하십시오.

테넌트 계정을 생성합니다

StorageGRID 시스템의 스토리지에 대한 액세스를 제어하려면 하나 이상의 테넌트 계정을 생성해야 합니다.

테넌트 계정을 만드는 단계는 및 "SSO(Single Sign-On)" 의 구성 여부와 테넌트 계정을 만드는 데 사용하는 그리드 관리자 계정이 루트 액세스 권한이 있는 관리자 그룹에 속하는지 여부에 따라 "ID 제휴"다릅니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 또는 테넌트 계정 권한"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 필요가 없습니다. 을 "관리 그룹을 관리합니다"참조하십시오.
- S3 테넌트가 계정 데이터를 복제하고 그리드 통합 연결을 사용하여 버킷 오브젝트를 다른 그리드에 복제하도록 허용하려면
  - 있습니다. "그리드 페더레이션 연결을 구성했습니다"
  - 연결 상태는 * 연결됨 * 입니다.
  - 루트 액세스 권한이 있습니다.

◦ 에 대한 고려 사항을 검토했습니다."그리드 페더레이션에 허용된 테넌트 관리"

◦ 테넌트 계정에서 Grid Manager용으로 구성된 ID 소스를 사용할 경우 동일한 통합 그룹을 두 그리드의 Grid Manager로 가져왔습니다.

테넌트를 생성할 때 소스 및 대상 테넌트 계정에 대한 초기 루트 액세스 권한을 가지려면 이 그룹을 선택합니다.

이 관리 그룹이 테넌트를 생성하기 전에 두 그리드에 없는 경우 테넌트는 대상에 복제되지 않습니다.

마법사에 액세스합니다

단계

1. Tenants * 를 선택합니다.
2. Create * 를 선택합니다.

세부 정보를 입력합니다

단계

1. 테넌트에 대한 세부 정보를 입력합니다.

필드에 입력합니다	설명
이름	테넌트 계정의 이름입니다. 테넌트 이름은 고유해야 할 필요가 없습니다. 테넌트 계정이 생성되면 고유한 20자리 계정 ID를 받습니다.
설명(선택 사항)	테넌트를 식별하는 데 도움이 되는 설명입니다. 그리드 페더레이션 연결을 사용할 테넌트를 생성하는 경우 이 필드를 사용하여 소스 테넌트인지 대상 테넌트인지 확인할 수 있습니다. 예를 들어 그리드 1에서 생성된 테넌트에 대한 이 설명은 그리드 2에 복제된 테넌트에 대해서도 나타납니다. "이 테넌트는 그리드 1에 생성되었습니다."
클라이언트 유형입니다	이 테넌트가 사용할 클라이언트 프로토콜 유형으로 * S3 * 또는 * Swift * 가 있습니다. • 참고 *: Swift 클라이언트 응용 프로그램에 대한 지원은 더 이상 사용되지 않으며 향후 릴리스에서 제거될 예정입니다.
스토리지 할당량(선택 사항)	이 테넌트에 스토리지 할당량을 사용하려면 할당량과 유닛에 대한 숫자 값입니다.

2. Continue * 를 선택합니다.

권한을 선택합니다

단계

1. 필요에 따라 이 테넌트에 부여할 기본 권한을 선택합니다.

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

권한	선택한 경우...
플랫폼 서비스를 허용합니다	테넌트는 CloudMirror와 같은 S3 플랫폼 서비스를 사용할 수 있습니다. 을 "S3 테넌트 계정에 대한 플랫폼 서비스 관리"참조하십시오.
고유 ID 소스를 사용합니다	테넌트는 통합 그룹 및 사용자에 대한 자체 ID 소스를 구성하고 관리할 수 있습니다. 이 옵션은 StorageGRID 시스템에 대해 비활성화되어 "SSO를 구성했습니다 "있습니다.
S3 선택 허용	테넌트는 오브젝트 데이터를 필터링하고 검색하기 위해 S3 SelectObjectContent API 요청을 실행할 수 있습니다. 을 "관리 S3 테넌트 계정에 대해 선택"참조하십시오. • 중요 *: SelectObjectContent 요청은 모든 S3 클라이언트 및 모든 테넌트의 로드 밸런서 성능을 감소시킬 수 있습니다. 신뢰할 수 있는 테넌트에만 필요한 경우에만 이 기능을 사용하도록 설정합니다.

2. 필요에 따라 이 테넌트에 부여할 고급 권한을 선택합니다.

권한	선택한 경우...
그리드 페더레이션 연결	테넌트는 다음과 같은 그리드 페더레이션 연결을 사용할 수 있습니다. • 이 테넌트 및 계정에 추가된 모든 테넌트 그룹 및 사용자가 이 그리드(*source grid*)에서 선택한 연결의 다른 그리드(*destination grid*)로 복제되도록 합니다. • 이 테넌트가 각 그리드의 해당 버킷 간에 교차 그리드 복제를 구성할 수 있도록 허용합니다. 을 "그리드 페더레이션을 위해 허용된 테넌트를 관리합니다"참조하십시오.
S3 오브젝트 잠금	테넌트가 S3 오브젝트 잠금의 특정 기능을 사용하도록 허용: • * 최대 보존 기간 설정 * 이 버킷에 추가된 새 객체가 수집된 시점부터 유지되는 기간을 정의합니다. • * Allow compliance mode * 는 사용자가 보존 기간 동안 보호된 객체 버전을 덮어쓰거나 삭제할 수 없도록 합니다.

3. Continue * 를 선택합니다.

루트 액세스를 정의하고 테넌트를 생성합니다

단계

1. StorageGRID 시스템에서 ID 페더레이션, SSO(Single Sign-On) 또는 둘 다를 사용하는지 여부에 따라 테넌트 계정에 대한 루트 액세스를 정의합니다.

옵션을 선택합니다	이렇게 하십시오
ID 페더레이션이 활성화되지 않은 경우	테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션이 활성화된 경우	a. 테넌트에 대한 루트 액세스 권한이 있는 기존 통합 그룹을 선택합니다. b. 필요에 따라 테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션 및 SSO(Single Sign-On)가 모두 활성화된 경우	테넌트에 대한 루트 액세스 권한이 있는 기존 통합 그룹을 선택합니다. 로컬 사용자는 로그인할 수 없습니다.

2. 테넌트 생성 * 을 선택합니다.

   성공 메시지가 나타나고 새 테넌트가 테넌트 페이지에 나열됩니다. 테넌트 세부 정보를 보고 테넌트 활동을 모니터링하는 방법에 대한 자세한 내용은 을 참조하십시오"테넌트 작업을 모니터링합니다".

   네트워크 연결, 노드 상태 및 Cassandra 작업에 따라 그리드 전체에 테넌트 설정을 적용하는 데 15분 이상이 걸릴 수 있습니다.

3. 테넌트에 대해 * 그리드 페더레이션 연결 사용 * 권한을 선택한 경우:

   a. 동일한 테넌트가 연결의 다른 그리드에 복제되었는지 확인합니다. 두 그리드의 테넌트는 동일한 20자리 계정 ID, 이름, 설명, 할당량 및 권한을 갖습니다.

      "Tenant created without a clone"이라는 오류 메시지가 나타나면 의 지침을 참조하십시오 "그리드 통합 오류 문제 해결".

   b. 복제된 테넌트에 대해 루트 액세스를 정의할 때 로컬 루트 사용자 암호를 제공한 경우"로컬 루트 사용자의 암호를 변경합니다"

      로컬 루트 사용자는 암호가 변경될 때까지 대상 그리드의 테넌트 관리자에 로그인할 수 없습니다.

테넌트에 로그인(선택 사항)

필요에 따라 새 테넌트에 지금 로그인하여 구성을 완료하거나 나중에 테넌트에 로그인할 수 있습니다. 로그인 단계는 기본 포트(443) 또는 제한된 포트를 사용하여 Grid Manager에 로그인했는지 여부에 따라 달라집니다. 을 "외부 방화벽에서 액세스를 제어합니다"참조하십시오.

지금 로그인하십시오

사용 중인 경우...	수행할 작업...
포트 443을 사용하여 로컬 루트 사용자의 암호를 설정합니다	1. root로 로그인 * 을 선택합니다. 로그인하면 버킷, ID 통합, 그룹 및 사용자를 구성하기 위한 링크가 나타납니다. 2. 테넌트 계정을 구성할 링크를 선택합니다. 각 링크는 테넌트 관리자에서 해당 페이지를 엽니다. 페이지를 완료하려면 을 참조하십시오"테넌트 계정 사용 지침".
포트 443을 사용하고 로컬 루트 사용자의 암호를 설정하지 않았습니다	로그인 * 을 선택하고 루트 액세스 통합 그룹에 사용자의 자격 증명을 입력합니다.
제한된 포트	1. 마침 * 을 선택합니다 2. 테넌트 테이블에서 * 제한 * 을 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* 은 관리자 노드의 정규화된 도메인 이름 또는 IP 주소입니다 ◦ *port* 는 테넌트 전용 포트입니다 ◦ *20-digit-account-id* 테넌트의 고유 계정 ID입니다

나중에 로그인하십시오

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* 은 관리자 노드의 정규화된 도메인 이름 또는 IP 주소입니다 ◦ *20-digit-account-id* 테넌트의 고유 계정 ID입니다

사용 중인 경우...	다음 중 하나를 수행합니다.
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* 은 관리자 노드의 정규화된 도메인 이름 또는 IP 주소입니다 ◦ *port* 는 테넌트 전용 제한된 포트입니다 ◦ *20-digit-account-id* 테넌트의 고유 계정 ID입니다

테넌트를 구성합니다

의 지침에 따라 "테넌트 계정을 사용합니다"테넌트 그룹 및 사용자, S3 액세스 키, 버킷, 플랫폼 서비스, 계정 클론 및 그리드 간 복제를 관리합니다.

테넌트 계정을 편집합니다

테넌트 계정을 편집하여 표시 이름, 스토리지 할당량 또는 테넌트 권한을 변경할 수 있습니다.

테넌트에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 연결의 각 그리드에서 테넌트 세부 정보를 편집할 수 있습니다. 그러나 연결의 한 그리드에서 변경한 내용은 다른 그리드로 복사되지 않습니다. 테넌트 세부 정보를 그리드 간에 정확하게 동기화하려면 두 그리드에 동일한 편집 작업을 수행합니다. 을 "그리드 페더레이션 연결에 대해 허용된 테넌트를 관리합니다"참조하십시오.

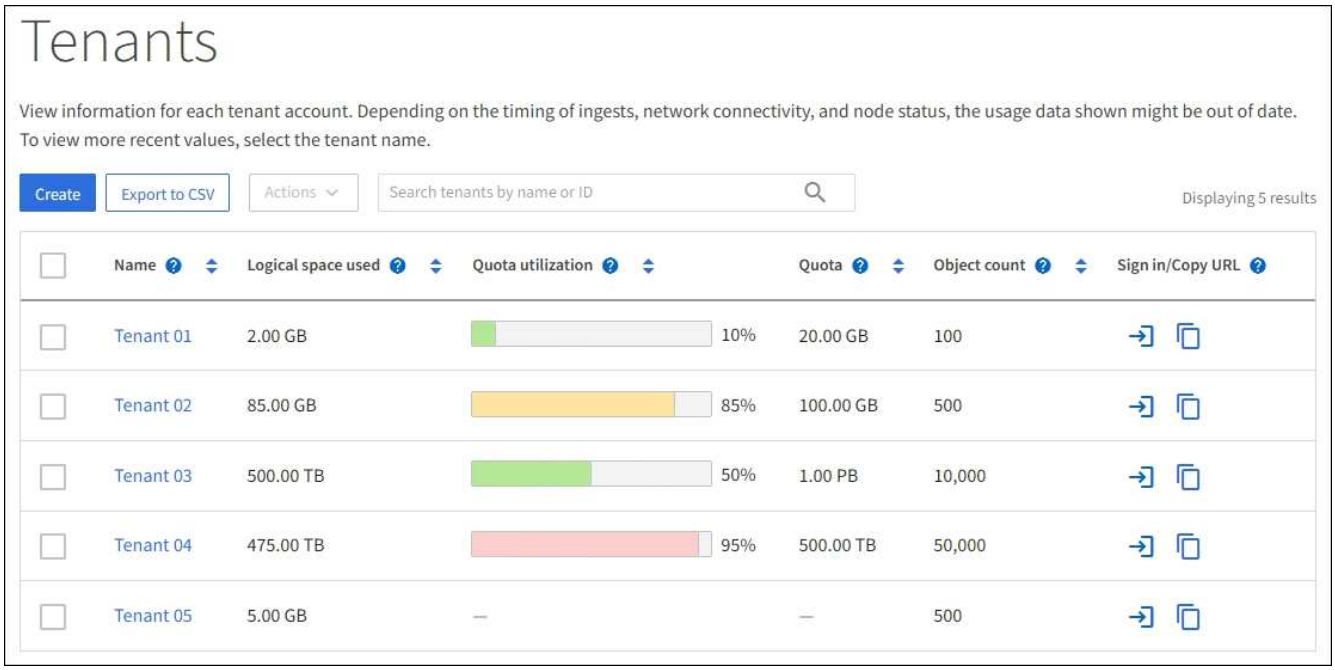
시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 또는 테넌트 계정 권한"있습니다.

네트워크 연결, 노드 상태 및 Cassandra 작업에 따라 그리드 전체에 테넌트 설정을 적용하는 데 15분 이상이 걸릴 수 있습니다.

단계

1. Tenants * 를 선택합니다.



2. 편집할 테넌트 계정을 찾습니다.

   검색 상자를 사용하여 이름 또는 테넌트 ID로 테넌트를 검색합니다.

3. 테넌트를 선택합니다. 다음 중 하나를 수행할 수 있습니다.
   - 테넌트에 대한 확인란을 선택하고 * Actions * > * Edit * 를 선택합니다.
   - 테넌트 이름을 선택하여 세부 정보 페이지를 표시하고 * Edit * 를 선택합니다.
4. 필요에 따라 다음 필드의 값을 변경합니다.
   - * 이름 *
   - * 설명 *
   - * 스토리지 할당량 *
5. Continue * 를 선택합니다.
6. 테넌트 계정에 대한 권한을 선택하거나 지웁니다.
   - 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. 을 "S3 테넌트 계정에 대한 플랫폼 서비스 관리"참조하십시오.
   - 테넌트 계정에서 그리드 관리자를 위해 구성된 ID 소스 또는 고유한 ID 소스를 사용할지 여부를 결정하려면 * 고유한 ID 소스 사용 * 의 설정을 변경합니다.

     고유한 ID 소스 사용 * 이 다음과 같은 경우:

     - 비활성화되었으며 이 옵션을 선택하면 테넌트가 이미 자체 ID 소스를 사용하도록 설정되어 있습니다. 테넌트는 그리드 관리자에 대해 구성된 ID 소스를 사용하기 전에 해당 ID 소스를 비활성화해야 합니다.
     - 비활성화되었으며 선택되지 않았습니다. StorageGRID 시스템에 대해 SSO가 활성화됩니다. 테넌트는 Grid Manager에 대해 구성된 ID 소스를 사용해야 합니다.
   - 필요한 경우 * Allow S3 Select * (S3 선택 * 허용) 권한을 선택하거나 지웁니다. 을 "관리 S3 테넌트 계정에

대해 선택"참조하십시오.

- 그리드 페더레이션 연결 사용 * 권한을 제거하려면 다음을 수행합니다.
  i. Grid Federation * 탭을 선택합니다.
  ii. 권한 제거 * 를 선택합니다.
- 그리드 페더레이션 연결 사용 * 권한을 추가하려면
  i. Grid Federation * 탭을 선택합니다.
  ii. Use grid federation connection * 확인란을 선택합니다.
  iii. 필요에 따라 * 기존 로컬 사용자 및 그룹 복제 * 를 선택하여 원격 그리드에 복제합니다. 필요한 경우 마지막 클론 작업이 완료된 후 일부 로컬 사용자 또는 그룹의 클론이 생성되지 않은 경우 클론 생성을 중지하거나 복제를 다시 시도할 수 있습니다.
- 최대 보존 기간을 설정하거나 규정 준수 모드를 허용하려면

  이 설정을 사용하려면 먼저 그리드에서 S3 오브젝트 잠금을 활성화해야 합니다.

  i. S3 오브젝트 잠금 * 탭을 선택합니다.
  ii. Set maximum retention period * 에 값을 입력하고 풀다운 메뉴에서 기간을 선택합니다.
  iii. Allow compliance mode * 에서 확인란을 선택합니다.

테넌트의 로컬 루트 사용자에 대한 암호를 변경합니다

루트 사용자가 계정에서 잠겨 있는 경우 테넌트의 로컬 루트 사용자의 암호를 변경해야 할 수 있습니다.

시작하기 전에

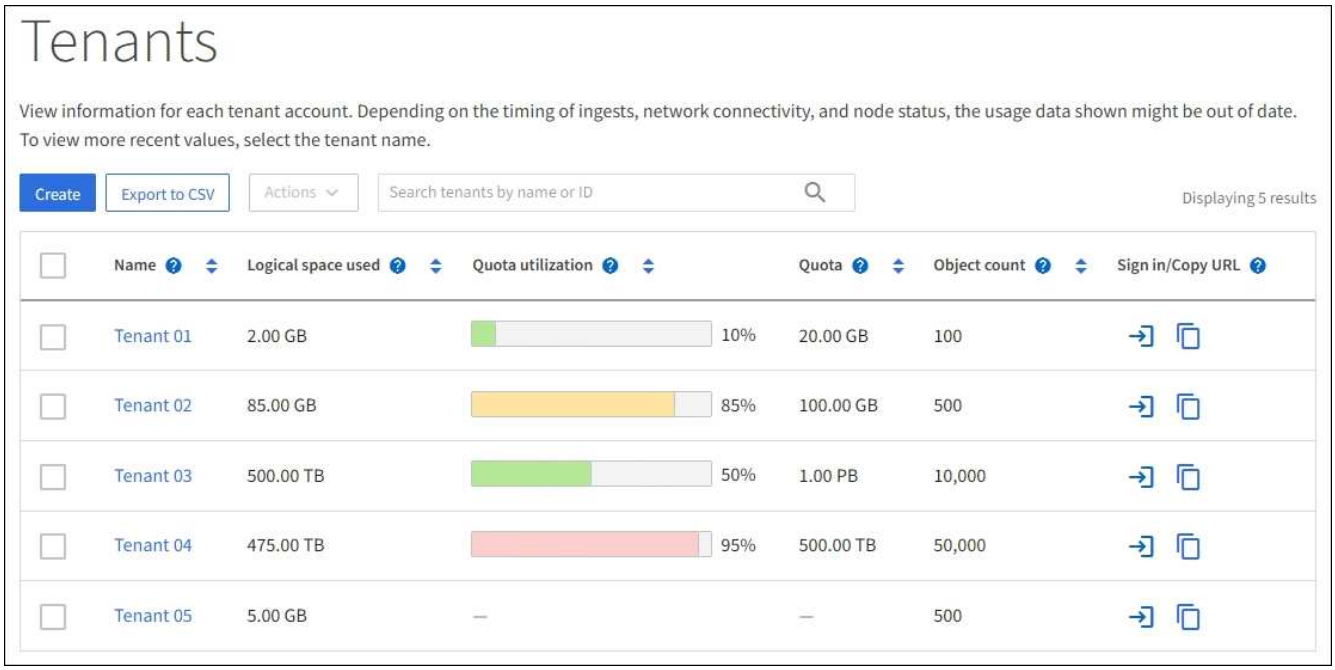
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

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. 테넌트 계정을 선택합니다. 다음 중 하나를 수행할 수 있습니다.
   - 테넌트 확인란을 선택하고 * 작업 * > * 루트 암호 변경 * 을 선택합니다.
   - 세부 정보 페이지를 표시하려면 테넌트 이름을 선택하고 * 작업 * > * 루트 암호 변경 * 을 선택합니다.
3. 테넌트 계정의 새 암호를 입력합니다.
4. 저장 * 을 선택합니다.

테넌트 계정을 삭제합니다

테넌트의 시스템 액세스를 영구적으로 제거하려면 테넌트 계정을 삭제할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"
- 테넌트 계정과 연결된 모든 S3 버킷 및 오브젝트를 제거했습니다.
- 테넌트가 그리드 페더레이션 연결을 사용하도록 허용된 경우 에 대한 고려 사항을 검토했습니다."그리드 페더레이션 연결 사용 권한이 있는 테넌트 삭제"

단계

1. Tenants * 를 선택합니다.
2. 삭제할 테넌트 계정 또는 계정을 찾습니다.

   검색 상자를 사용하여 이름 또는 테넌트 ID로 테넌트를 검색합니다.

3. 여러 테넌트를 삭제하려면 확인란을 선택하고 * Actions * > * Delete * 를 선택합니다.
4. 단일 테넌트를 삭제하려면 다음 중 하나를 수행합니다.
   - 확인란을 선택하고 * Actions * > * Delete * 를 선택합니다.

◦ 테넌트 이름을 선택하여 세부 정보 페이지를 표시한 다음 * 작업 * > * 삭제 * 를 선택합니다.

5. 예 * 를 선택합니다.

플랫폼 서비스 관리

플랫폼 서비스란 무엇입니까?

플랫폼 서비스에는 CloudMirror 복제, 이벤트 알림 및 검색 통합 서비스가 포함됩니다.

S3 테넌트 계정에 대해 플랫폼 서비스를 설정하는 경우 테넌트가 이러한 서비스를 사용하는 데 필요한 외부 리소스에 액세스할 수 있도록 그리드를 구성해야 합니다.

CloudMirror 복제

StorageGRID CloudMirror 복제 서비스는 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.

> CloudMirror 복제는 교차 그리드 복제 기능과 몇 가지 중요한 유사점과 차이점이 있습니다. 자세한 내용은 을 참조하십시오"교차 그리드 복제와 CloudMirror 복제를 비교합니다".

> 소스 버킷에 S3 오브젝트 잠금이 설정된 경우 CloudMirror 복제가 지원되지 않습니다.

알림

버킷별 이벤트 알림은 오브젝트에 대해 수행된 특정 작업에 대한 알림을 지정된 외부 Kafka 클러스터 또는 Amazon Simple Notification Service로 전송하는 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 S3 오브젝트 메타데이터를 지정된 Elasticsearch 인덱스로 전송하는 데 사용되며, 여기에서 외부 서비스를 사용하여 메타데이터를 검색 또는 분석할 수 있습니다.

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

- "플랫폼 서비스 관리"
- "스토리지 프록시 설정을 구성합니다"
- "StorageGRID 모니터링"

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
- Amazon Simple Notification Service 메시지 수신을 지원하는 로컬 애플리케이션입니다
- 로컬에서 호스팅되는 Kafka 클러스터
- 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 URI(대부분의 끝점)용

- *443 *: https로 시작하는 끝점 URI(대부분의 끝점)
- * 9092 *: http 또는 https로 시작하는 엔드포인트 URI(Kafka 엔드포인트만 해당)

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 경우 인터넷의 끝점과 같은 외부 끝점으로 메시지를 보낼 수 있도록 허용해야 "스토리지 프록시 설정을 구성합니다"합니다.

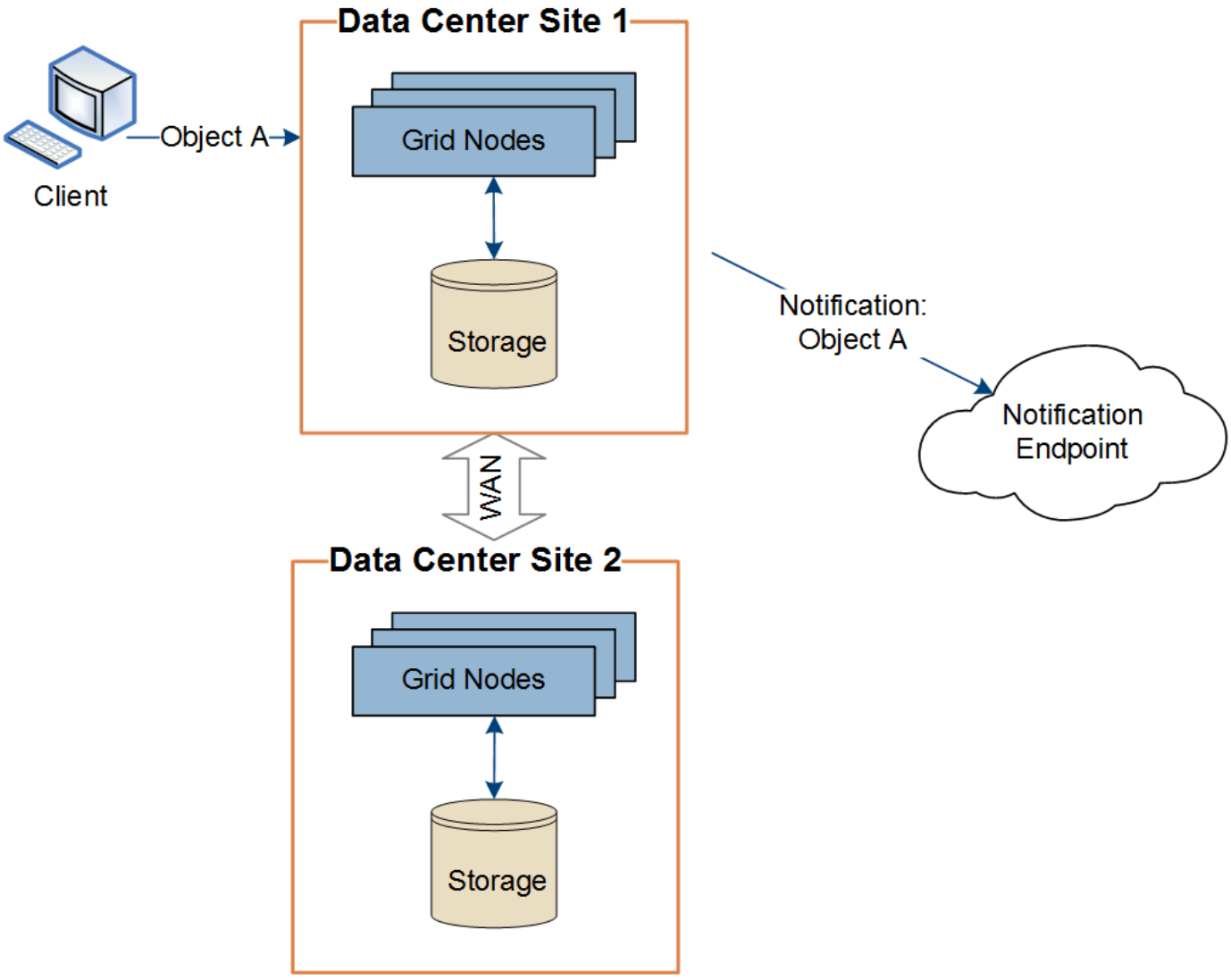
관련 정보

"테넌트 계정을 사용합니다"

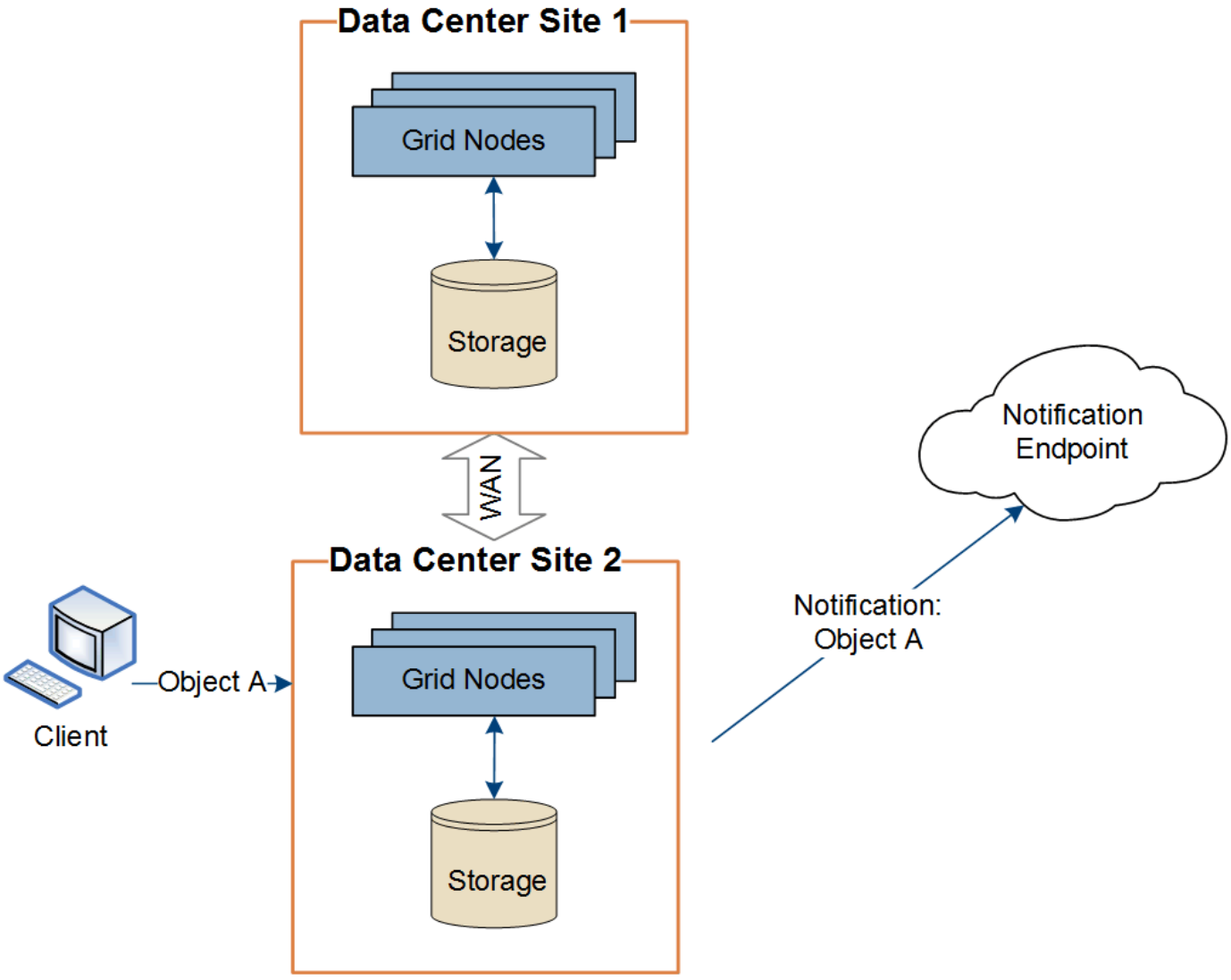
플랫폼 서비스 메시지를 사이트별로 전달

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 Web Services 버킷, Amazon Simple Notification Service 주제, Kafka 주제 또는 로컬 또는 AWS에서 호스팅되는 Elasticsearch 클러스터와 같이 단일 플랫폼 서비스에 대한 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.

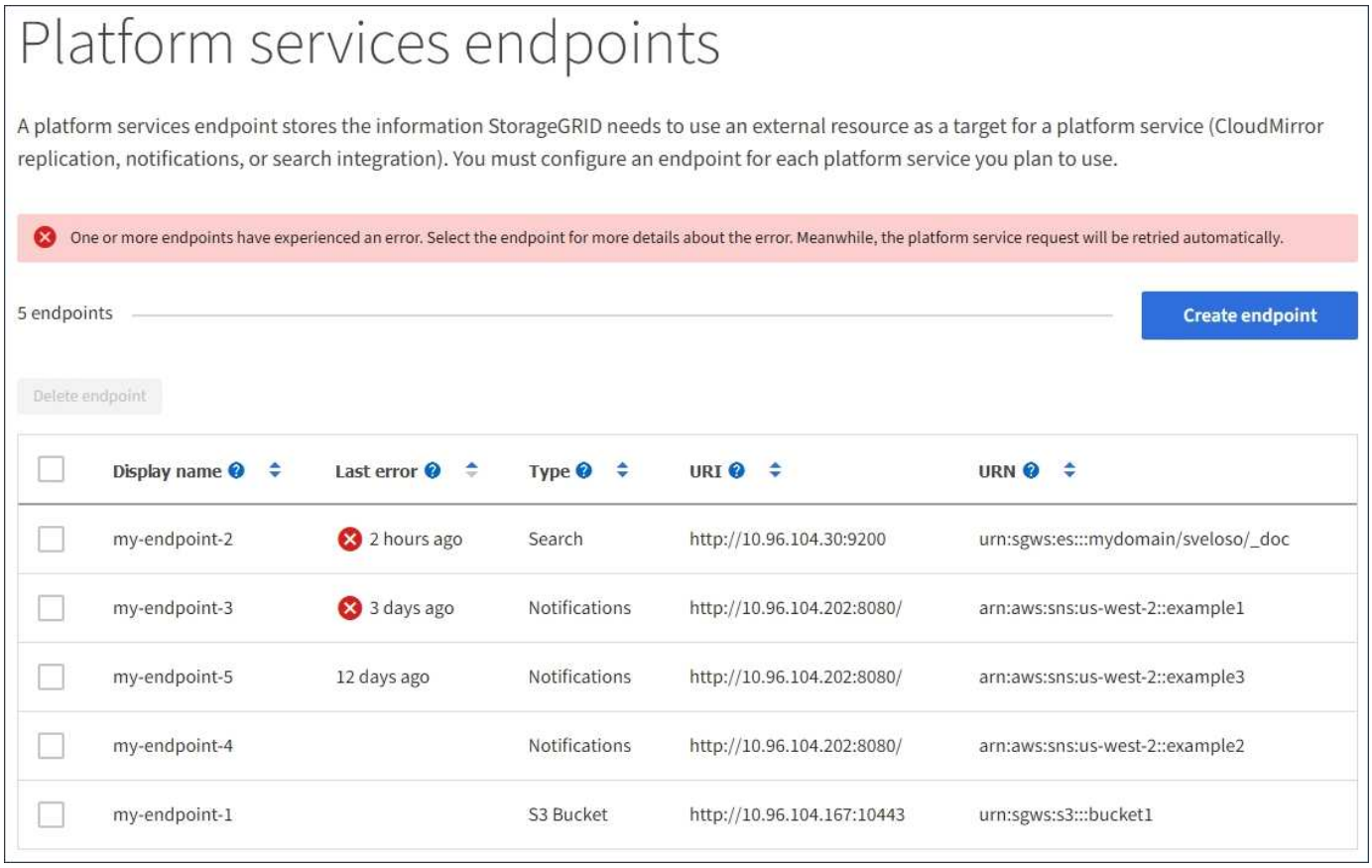
테넌트 계정에 플랫폼 서비스가 활성화되어 있지 않으면 엔드포인트 생성이 실패합니다.

기존 엔드포인트에 문제가 있습니다

StorageGRID가 기존 끝점에 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. 아이콘이 포함된 오류는 지난 7일 내에 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 끝점 간에 를 구성한 "스토리지 프록시"경우 프록시 서비스에서 StorageGRID의 메시지를 허용하지 않는 경우 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 전송할 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 발생하는 경우:

- Grid Manager에서 * 지원 * > * 툴 * > * 메트릭 * > * Grafana * > * 플랫폼 서비스 개요 * 로 이동하여 오류 세부 정보를 확인하십시오.
- 테넌트 관리자에서 * 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 * 로 이동하여 오류 세부 정보를 확인합니다.
- 에 `/var/local/log/bycast-err.log` 관련된 오류가 있는지 확인합니다. ADC 서비스가 있는 스토리지 노드에는 이 로그 파일이 포함되어 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.

관련 경고를 확인합니다.

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.

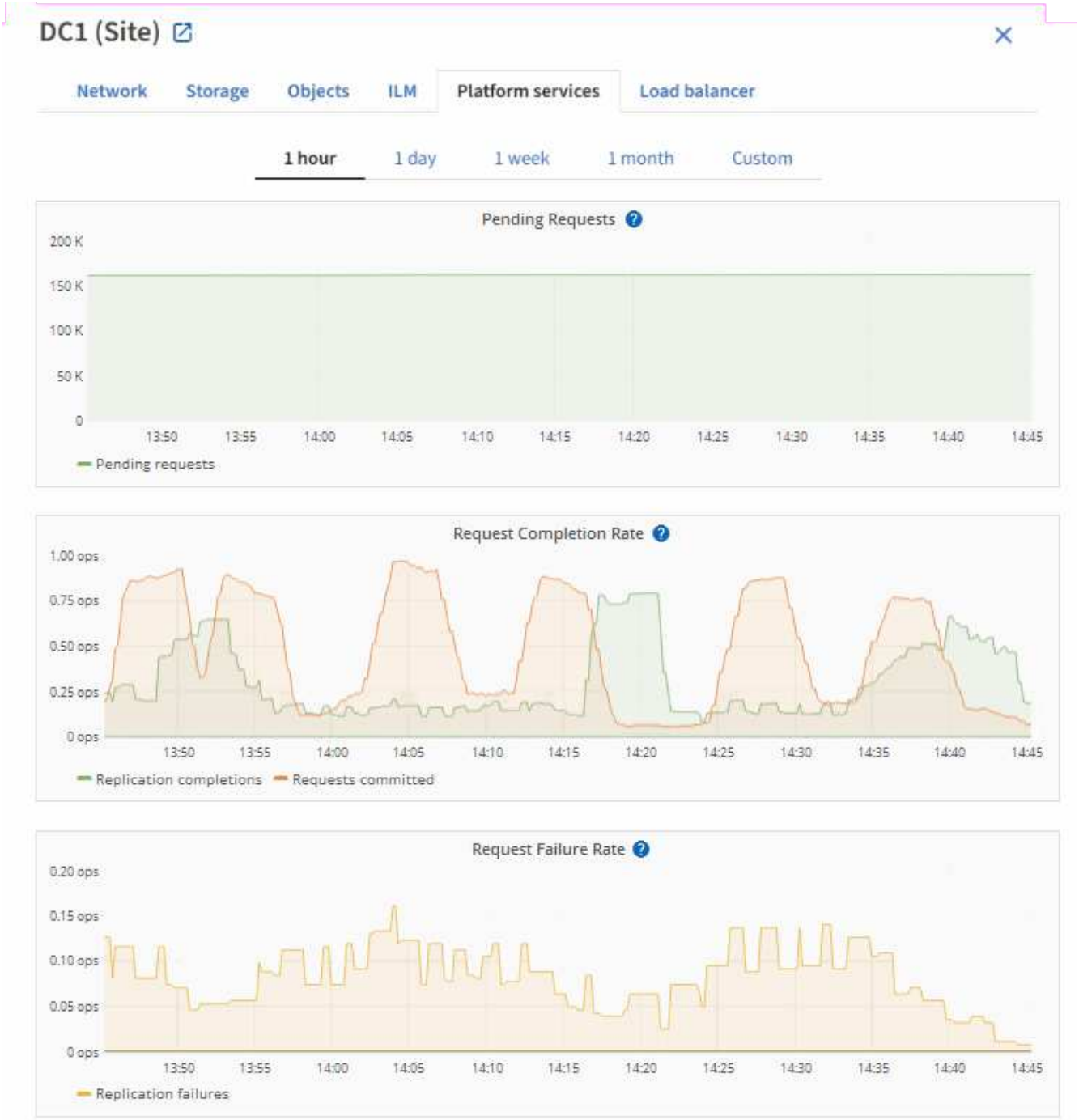
단, 들어오는 S3 요청의 실행 시간이 더 오래 걸린다는 점을 알 수 있습니다. 속도가 현저히 느린 성능을 감지하기 시작하는 경우 수집 속도를 줄이거나 용량이 더 큰 엔드포인트를 사용해야 합니다. 요청 백로그가 계속 증가하는 경우 PUT 요청과 같은 클라이언트 S3 작업이 결국 실패합니다.

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 일부만 실행되고 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

자세한 내용은 을 "테넌트 계정 및 GT 사용, 플랫폼 서비스 끝점 문제 해결"참조하십시오.

관련 정보

"StorageGRID 시스템 문제를 해결합니다"

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

그리드 관리 요구 사항

그리드 관리자는 테넌트에 S3 Select 기능을 부여해야 합니다. 또는 를 선택하면 * Allow S3 Select * "테넌트 생성" "테넌트 편집"가 선택됩니다.

오브젝트 형식 요구사항

쿼리할 객체는 다음 형식 중 하나여야 합니다.

- CSV *. GZIP 또는 BZIP2 보관 파일로 압축하거나 그대로 사용할 수 있습니다.
- * 파케 *. Parquet 객체에 대한 추가 요구 사항:
  - S3 Select는 GZIP 또는 Snappy를 사용한 컬럼 압축만 지원합니다. S3 Select는 Parquet 오브젝트에 대한 전체 오브젝트 압축을 지원하지 않습니다.
  - S3 Select는 Parquet 출력을 지원하지 않습니다. 출력 형식을 CSV 또는 JSON으로 지정해야 합니다.
  - 압축되지 않은 최대 행 그룹 크기는 512MB입니다.
  - 개체의 스키마에 지정된 데이터 형식을 사용해야 합니다.
  - 간격, JSON, 목록, 시간 또는 UUID 논리적 유형은 사용할 수 없습니다.

엔드포인트 요구 사항

SelectObjectContent 요청을 로 보내야 "StorageGRID 로드 밸런서 엔드포인트"합니다.

끝점에서 사용하는 관리자 및 게이트웨이 노드는 다음 중 하나여야 합니다.

- 서비스 어플라이언스 노드입니다
- VMware 기반 소프트웨어 노드입니다
- cgroup v2가 활성화된 커널을 실행하는 베어 메탈 노드

일반 고려 사항

쿼리를 스토리지 노드로 직접 보낼 수 없습니다.

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 "S3 Select 사용에 대한 지침"참조하십시오.

시간에 따른 S3 Select 작업을 보려면 "Grafana 차트"그리드 관리자에서 * 지원 * > * 툴 * > * 메트릭 * 을 선택합니다.

클라이언트 연결을 구성합니다

S3 클라이언트 연결을 구성합니다

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

이 버전의 문서 사이트에서 Swift 세부 정보가 제거되었습니다. 을 "StorageGRID 11.8: S3 및 Swift 클라이언트 연결 구성"참조하십시오.

구성 작업

1. 클라이언트 응용 프로그램이 StorageGRID에 연결되는 방법에 따라 StorageGRID에서 필수 작업을 수행합니다.

필수 작업

다음 정보를 얻어야 합니다.

- IP 주소
- 도메인 이름
- SSL 인증서

선택적 태스크입니다

필요에 따라 다음을 구성합니다.

- ID 제휴
- SSO

1. StorageGRID를 사용하여 응용 프로그램이 그리드에 연결하는 데 필요한 값을 얻습니다. S3 설정 마법사를 사용하거나 각 StorageGRID 엔터티를 수동으로 구성할 수 있습니다. 를 누릅니다

S3 설정 마법사를 사용합니다

S3 설정 마법사의 단계를 따릅니다.

수동으로 구성합니다

1. 고가용성 그룹을 생성합니다
2. 로드 밸런서 끝점을 만듭니다
3. 테넌트 계정을 생성합니다
4. 버킷 및 액세스 키를 생성합니다
5. ILM 규칙 및 정책을 구성합니다

1. S3 애플리케이션을 사용하여 StorageGRID에 대한 연결을 완료합니다. DNS 항목을 만들어 사용하려는 도메인 이름에 IP 주소를 연결합니다.

   필요에 따라 추가 애플리케이션 설정을 수행합니다.

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

StorageGRID를 클라이언트 애플리케이션에 연결하는 데 필요한 정보입니다

StorageGRID를 S3 클라이언트 응용 프로그램에 연결하려면 먼저 StorageGRID에서 구성 단계를 수행하고 특정 값을 얻어야 합니다.

어떤 가치가 필요합니까**?**

다음 표에는 StorageGRID에서 구성해야 하는 값과 S3 응용 프로그램 및 DNS 서버에서 이러한 값을 사용하는 위치가 나와 있습니다.

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

이러한 값을 얻으려면 어떻게 해야 합니까?

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

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

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

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

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

- * 항목을 수동으로 구성 *. S3 응용 프로그램에 연결하는 경우 S3 설정 마법사를 사용하지 않으려면 수동으로 구성을 수행하여 필요한 값을 얻을 수 있습니다. 다음 단계를 수행하십시오.
  a. S3 애플리케이션에 사용할 고가용성(HA) 그룹을 구성합니다. 을 "고가용성 그룹을 구성합니다"참조하십시오.
  b. S3 애플리케이션에서 사용할 로드 밸런서 끝점을 생성합니다. 을 "로드 밸런서 엔드포인트를 구성합니다 "참조하십시오.
  c. S3 응용 프로그램에서 사용할 테넌트 계정을 만듭니다. 을 "테넌트 계정을 생성합니다"참조하십시오.
  d. S3 테넌트의 경우 테넌트 계정에 로그인하고 응용 프로그램에 액세스할 각 사용자에 대한 액세스 키 ID 및 비밀 액세스 키를 생성합니다. 을 "사용자 고유의 액세스 키를 생성합니다"참조하십시오.
  e. 테넌트 계정 내에 하나 이상의 S3 버킷을 생성합니다. S3의 경우 을 "S3 버킷을 생성합니다"참조하십시오.
  f. 새 테넌트 또는 버킷/컨테이너에 속한 개체에 대한 특정 배치 지침을 추가하려면 새 ILM 규칙을 생성하고 해당 규칙을 사용하도록 새 ILM 정책을 활성화합니다. "ILM 규칙을 생성합니다"및 을 "ILM 정책을 생성합니다 "참조하십시오.

S3 클라이언트에 대한 보안

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

요약

다음 목록에는 S3 REST API에 대해 보안이 구현되는 방식이 요약되어 있습니다.

연결 보안
: TLS

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

클라이언트 인증

S3 계정 액세스 키 ID 및 비밀 액세스 키

클라이언트 인증

버킷 소유권 및 모든 적용 가능한 액세스 제어 정책

StorageGRID가 클라이언트 응용 프로그램에 보안을 제공하는 방법

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

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

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

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

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

  HTTPS가 기본값이며 권장됩니다.

  HTTP는 보안이 약하고 암호화되지 않은 통신을 제공하지만 비운영 또는 테스트 그리드의 경우 선택적으로 사용할 수 "활성화됨"있습니다.

- 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.
- 클라이언트가 REST API 작업을 수행하려면 StorageGRID에 을 제공해야 "HTTP 인증 헤더"합니다.

보안 인증서 및 클라이언트 응용 프로그램

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

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

  을 "로드 균형 조정에 대한 고려 사항"참조하십시오.

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

클라이언트가 TLS 연결을 설정하는 데 사용하는 인증서를 신뢰하도록 구성해야 합니다.

TLS 라이브러리에 대해 지원되는 해시 및 암호화 알고리즘

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

지원되는 **TLS** 버전입니다

StorageGRID는 TLS 1.2 및 TLS 1.3을 지원합니다.

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

S3 설정 마법사를 사용합니다

S3 설정 마법사 고려 사항 및 요구 사항을 사용합니다

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

S3 설정 마법사를 사용하는 경우

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

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

마법사를 사용하기 전에

마법사를 사용하기 전에 이러한 사전 요구 사항을 완료했는지 확인합니다.

IP 주소를 얻고 **VLAN** 인터페이스를 설정합니다

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

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

ID 페더레이션 및 **SSO**를 구성합니다

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

도메인 이름 가져오기 및 구성

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

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

로드 밸런서 및 보안 인증서 요구 사항을 검토합니다

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

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

모든 그리드 페더레이션 연결을 구성합니다

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

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

S3 설정 마법사를 액세스하고 완료합니다

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

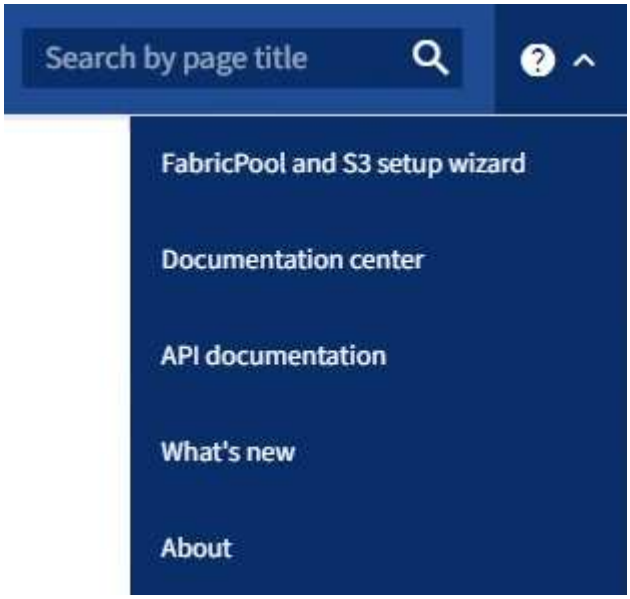
시작하기 전에

- 이 "루트 액세스 권한"있습니다.
- 마법사 사용을 위해 을 검토했습니다."고려 사항 및 요구 사항"

마법사에 액세스합니다

단계

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



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

단계 **1/6: HA** 그룹 구성

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

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

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

단계

1. 외부 로드 밸런서를 사용할 계획이라면 HA 그룹을 생성할 필요가 없습니다. 이 단계 건너뛰기 * 를 선택하고 로 이동합니다6단계 중 2단계: 로드 밸런서 끝점을 구성합니다.
2. StorageGRID 로드 밸런서를 사용하려면 새 HA 그룹을 생성하거나 기존 HA 그룹을 사용할 수 있습니다.

HA 그룹을 생성합니다

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

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

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

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

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

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

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

행을 드래그하여 * Priority order * 열의 값을 변경합니다.

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

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

e. IP 주소 입력 * 단계에 대해 다음 필드를 입력합니다.

필드에 입력합니다	설명
서브넷 CIDR	CIDR 표기법 &#8212의 VIP 서브넷 주소, IPv4 주소, 슬래시 및 서브넷 길이(0-32). 네트워크 주소에는 호스트 비트가 설정되어 있지 않아야 합니다. `192.16.0.0/22`예를 들어,
게이트웨이 IP 주소(선택 사항)	StorageGRID 액세스에 사용되는 S3 IP 주소가 StorageGRID VIP 주소와 동일한 서브넷에 없는 경우 StorageGRID VIP 로컬 게이트웨이 IP 주소를 입력합니다. 로컬 게이트웨이 IP 주소는 VIP 서브넷 내에 있어야 합니다.

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

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

g. 로드 밸런서 단계로 이동하려면 * 계속 * 을 선택합니다.

기존 **HA** 그룹 사용

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

b. 로드 밸런서 단계로 이동하려면 * 계속 * 을 선택합니다.

6단계 중 **2**단계**:** 로드 밸런서 끝점을 구성합니다

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

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

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

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

끝점 작성

단계

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

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

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

모드를 선택합니다	설명
글로벌(기본값)	클라이언트는 게이트웨이 노드 또는 관리 노드의 IP 주소, 네트워크에 있는 HA 그룹의 가상 IP(VIP) 주소 또는 해당 FQDN을 사용하여 끝점에 액세스할 수 있습니다. 이 끝점의 접근성을 제한할 필요가 없는 경우 * Global * (글로벌 *) 설정(기본값)을 사용합니다.
HA 그룹의 가상 IP입니다	클라이언트는 HA 그룹의 가상 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다. 이 바인딩 모드의 엔드포인트는 엔드포인트에 대해 선택한 HA 그룹이 겹치지 않는 한 모두 동일한 포트 번호를 사용할 수 있습니다.
노드 인터페이스	클라이언트는 선택한 노드 인터페이스의 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다.

모드를 선택합니다	설명
노드 유형입니다	선택한 노드 유형에 따라 클라이언트는 관리 노드의 IP 주소(또는 해당 FQDN)나 게이트웨이 노드의 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다.

4. 테넌트 액세스 단계에서 다음 중 하나를 선택합니다.

필드에 입력합니다	설명
모든 테넌트 허용(기본값)	모든 테넌트 계정은 이 엔드포인트를 사용하여 해당 버킷에 액세스할 수 있습니다.
선택한 테넌트 허용	선택한 테넌트 계정만 이 끝점을 사용하여 해당 버킷을 액세스할 수 있습니다.
선택한 테넌트 차단	선택한 테넌트 계정은 이 끝점을 사용하여 해당 버킷을 액세스할 수 없습니다. 다른 모든 테넌트는 이 끝점을 사용할 수 있습니다.

5. 인증서 연결 * 단계에서 다음 중 하나를 선택합니다.

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

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

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

기존 로드 밸런서 끝점을 사용합니다

단계

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

외부 로드 밸런서를 사용합니다

단계

1. 외부 로드 밸런서를 사용하려면 다음 필드를 완료합니다.

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

2. 테넌트 및 버킷 단계로 이동하려면 * 계속 * 을 선택합니다.

6단계 중 **3**단계**:** 테넌트 및 버킷을 생성합니다

테넌트는 S3 애플리케이션을 사용하여 StorageGRID에 오브젝트를 저장하고 검색할 수 있는 엔터티입니다. 각 테넌트에는 자체 사용자, 액세스 키, 버킷, 오브젝트 및 특정 기능 세트가 있습니다.

버킷은 테넌트의 오브젝트 및 오브젝트 메타데이터를 저장하는 데 사용되는 컨테이너입니다. 테넌트에 버킷이 많을 수도 있지만 마법사를 사용하면 가장 빠르고 쉽게 테넌트와 버킷을 만들 수 있습니다. 나중에 버킷을 추가하거나 옵션을 설정해야 하는 경우 Tenant Manager를 사용할 수 있습니다.

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

단계

1. 테넌트 계정의 이름을 입력합니다.

   테넌트 이름은 고유해야 할 필요가 없습니다. 테넌트 계정이 생성되면 고유한 숫자 계정 ID를 받습니다.

2. StorageGRID 시스템에서"ID 제휴", "SSO(Single Sign-On)"또는 둘 모두를 사용하는지 여부에 따라 테넌트 계정에 대한 루트 액세스를 정의합니다.

옵션을 선택합니다	이렇게 하십시오
ID 페더레이션이 활성화되지 않은 경우	테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션이 활성화된 경우	a. 테넌트에 대해 가질 기존 페더레이션 그룹을 "루트 액세스 권한 "선택합니다. b. 필요에 따라 테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션 및 SSO(Single Sign-On)가 모두 활성화된 경우	테넌트에 대해 가질 기존 페더레이션 그룹을 "루트 액세스 권한"선택합니다. 로컬 사용자는 로그인할 수 없습니다.

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

테넌트의 유일한 사용자가 루트 사용자인 경우 이 옵션을 선택합니다. 다른 사용자가 이 테넌트를 사용할 경우 "Tenant Manager를 사용합니다"키와 권한을 구성합니다.

4. 지금 이 테넌트에 대한 버킷을 생성하려면 * 이 테넌트에 대한 버킷 생성 * 을 선택합니다.

> 그리드에 S3 오브젝트 잠금이 활성화된 경우 이 단계에서 생성한 버킷에 S3 오브젝트 잠금이 활성화되지 않습니다. 이 S3 애플리케이션에 S3 오브젝트 잠금 버킷을 사용해야 하는 경우 지금 버킷을 생성하도록 선택하지 마십시오. 대신 나중에 테넌트 관리자를 "버킷을 생성합니다 "사용하십시오.

   a. S3 애플리케이션에서 사용할 버킷의 이름을 입력합니다. `s3-bucket`예를 들어,

      버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

   b. 이 버킷의 * 지역 * 을 선택합니다.

      (`us-east-1`나중에 ILM을 사용하여 버킷 영역을 기준으로 오브젝트를 필터링하지 않을 경우 기본 영역을 사용합니다.

5. Create and continue * 를 선택합니다.

단계 **4 / 6:** 데이터 다운로드

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

단계

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

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

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

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

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

단계

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

6단계 중 **6**단계**:** 요약 검토

단계

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

HA 그룹 관리

고가용성**(HA)** 그룹이란**?**

HA(고가용성) 그룹은 S3 클라이언트를 위한 고가용성 데이터 연결과 Grid Manager 및 Tenant Manager에 대한 고가용성 연결을 제공합니다.

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.

각 HA 그룹은 선택한 노드의 공유 서비스에 대한 액세스를 제공합니다.

- 게이트웨이 노드, 관리 노드 또는 둘 모두를 포함하는 HA 그룹은 S3 클라이언트에 고가용성 데이터 연결을 제공합니다.
- 관리 노드만 포함하는 HA 그룹은 Grid Manager 및 테넌트 관리자에 대한 고가용성 연결을 제공합니다.
- 서비스 어플라이언스와 VMware 기반 소프트웨어 노드만 포함하는 HA 그룹은 용 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 "고가용성 그룹을 구성합니다"참조하십시오.

액티브 인터페이스란 무엇입니까?

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

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

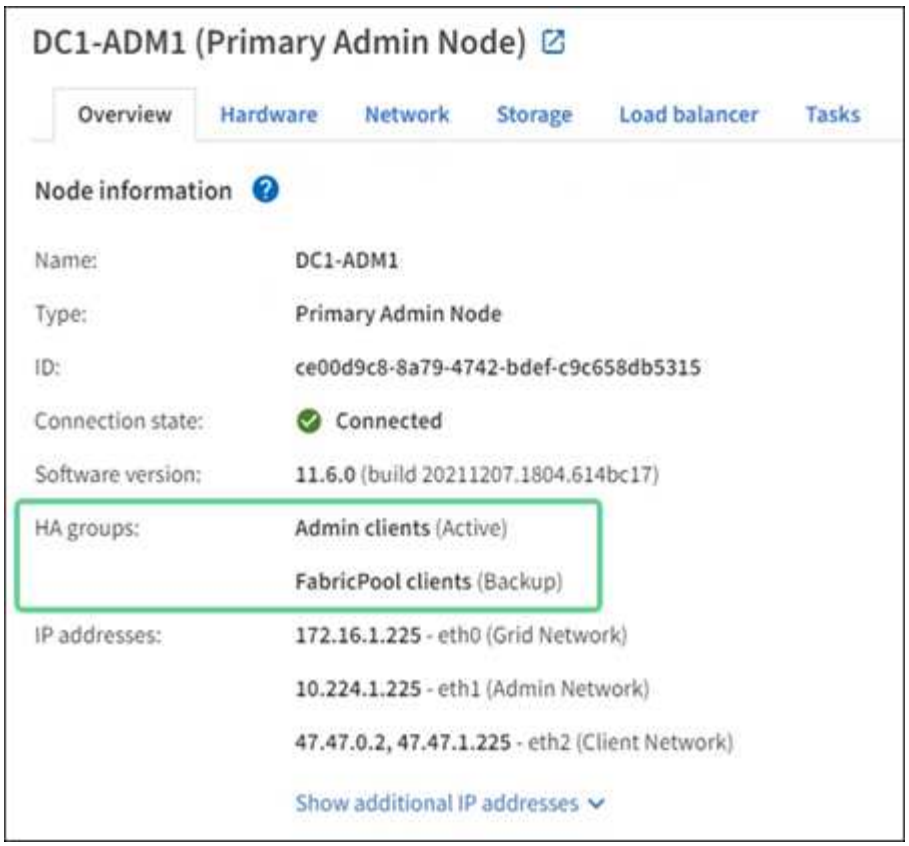
노드의 현재 HA 그룹 상태를 봅니다

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

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

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

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



활성 인터페이스가 실패하면 어떻게 됩니까**?**

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

페일오버는 다음과 같은 이유로 트리거될 수 있습니다.

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

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

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

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

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 클라이언트에 고가용성 데이터 연결을 제공할 수 있습니다.
- 인터페이스가 하나만 포함된 HA 그룹을 사용하면 많은 VIP 주소를 제공하고 IPv6 주소를 명시적으로 설정할 수 있습니다.

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

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

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

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

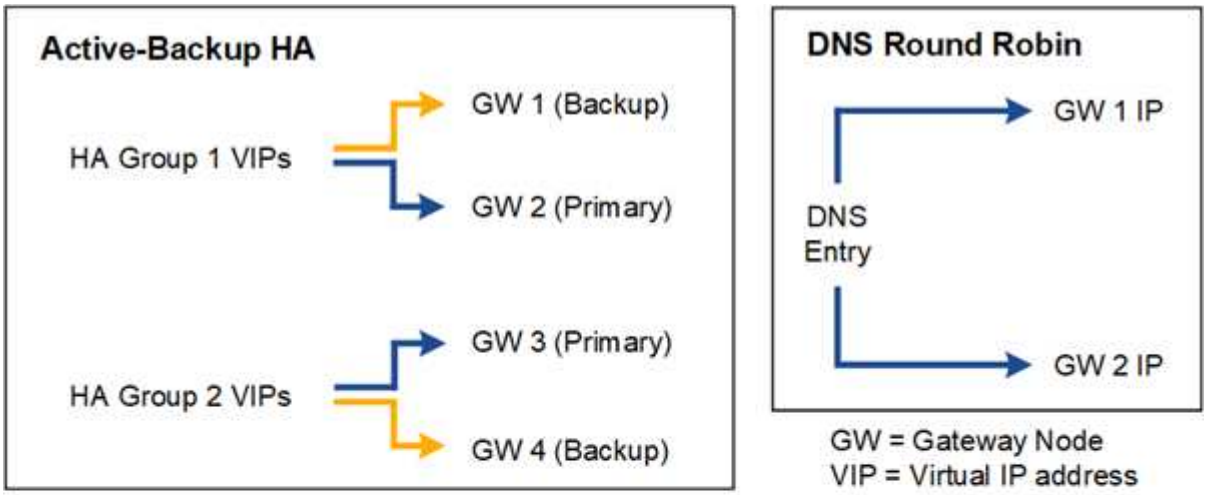
Grid Manager 또는 Tenant Manager 서비스에 장애가 발생하면 HA 그룹 페일오버가 트리거되지 않습니다.

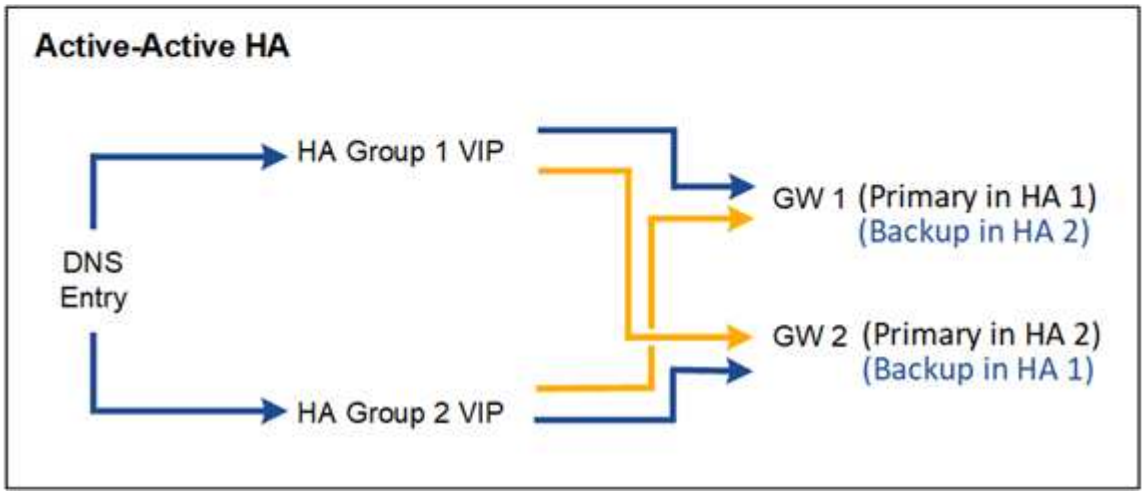
페일오버가 발생했을 때 Grid Manager 또는 Tenant Manager에 로그인한 경우, 로그아웃되며 작업을 재개하려면 다시 로그인해야 합니다.

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

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

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





이 표에는 다이어그램에 표시된 각 HA 구성의 이점이 요약되어 있습니다.

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

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

고가용성 그룹을 구성합니다

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

시작하기 전에

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

고가용성 그룹을 생성합니다

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

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

마법사에 액세스합니다

단계

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

HA 그룹에 대한 세부 정보를 입력합니다

단계

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

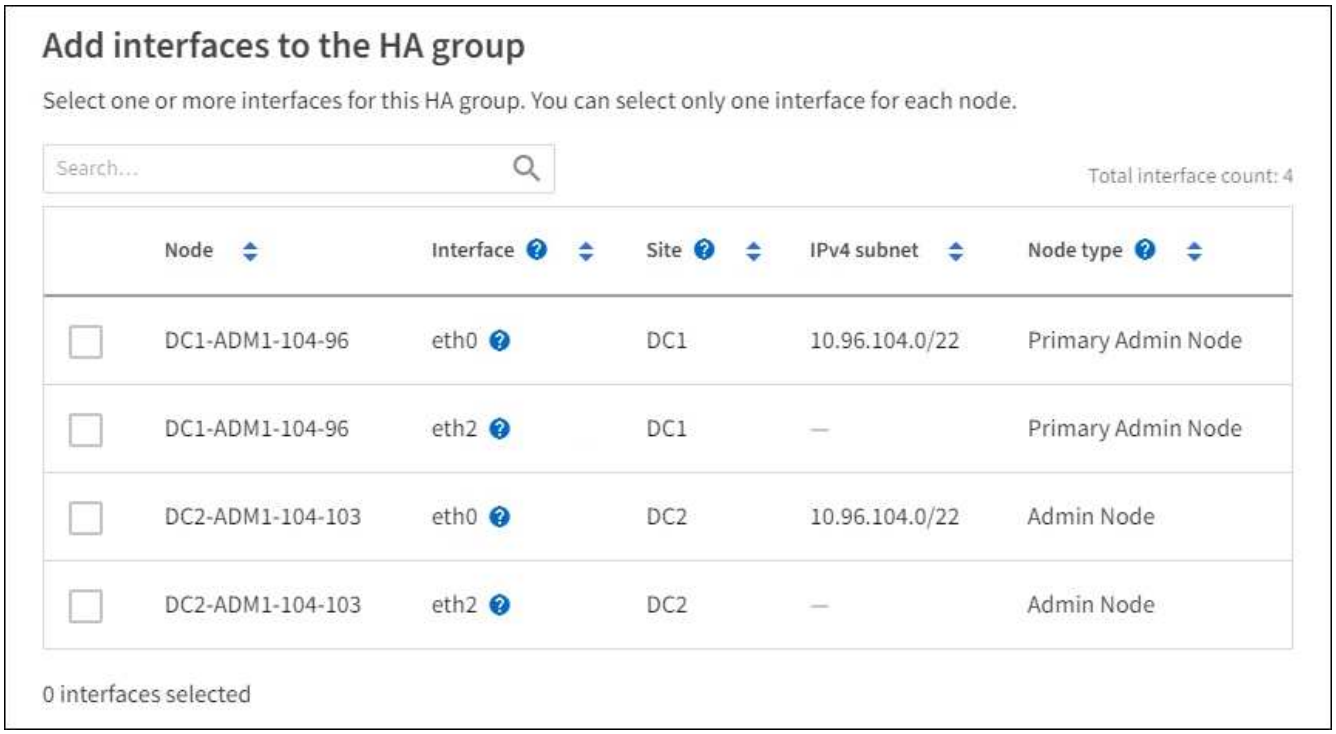
3. Continue * 를 선택합니다.

HA 그룹에 인터페이스를 추가합니다

단계

1. 이 HA 그룹에 추가할 인터페이스를 하나 이상 선택하십시오.

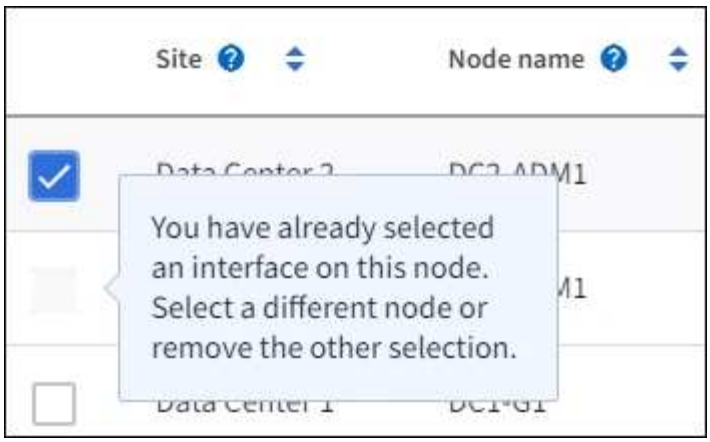
   열 머리글을 사용하여 행을 정렬하거나 검색어를 입력하여 인터페이스를 보다 빠르게 찾을 수 있습니다.



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

   인터페이스 선택을 위한 지침

   - 인터페이스를 하나 이상 선택해야 합니다.
   - 한 노드에 대해 하나의 인터페이스만 선택할 수 있습니다.
   - HA 그룹이 그리드 관리자 및 테넌트 관리자를 포함하는 관리 노드 서비스의 HA 보호를 위한 경우 관리 노드에서만 인터페이스를 선택합니다.
   - HA 그룹이 S3 클라이언트 트래픽의 HA 보호를 지원하는 경우 관리 노드, 게이트웨이 노드 또는 둘 다에 있는 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 선택한 다른 인터페이스와 충돌하는 경우 인터페이스를 선택할 수 없습니다.
- 정적 IP 주소가 없는 경우 구성된 인터페이스를 선택할 수 없습니다.

2. Continue * 를 선택합니다.

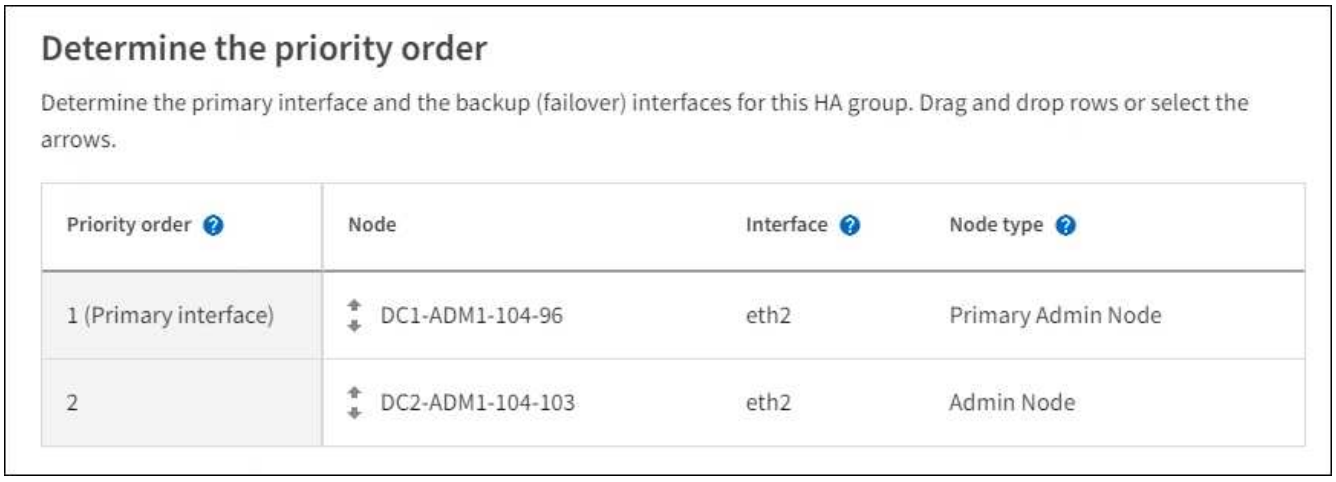
우선 순위 순서를 결정합니다

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

단계

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

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



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

2. Continue * 를 선택합니다.

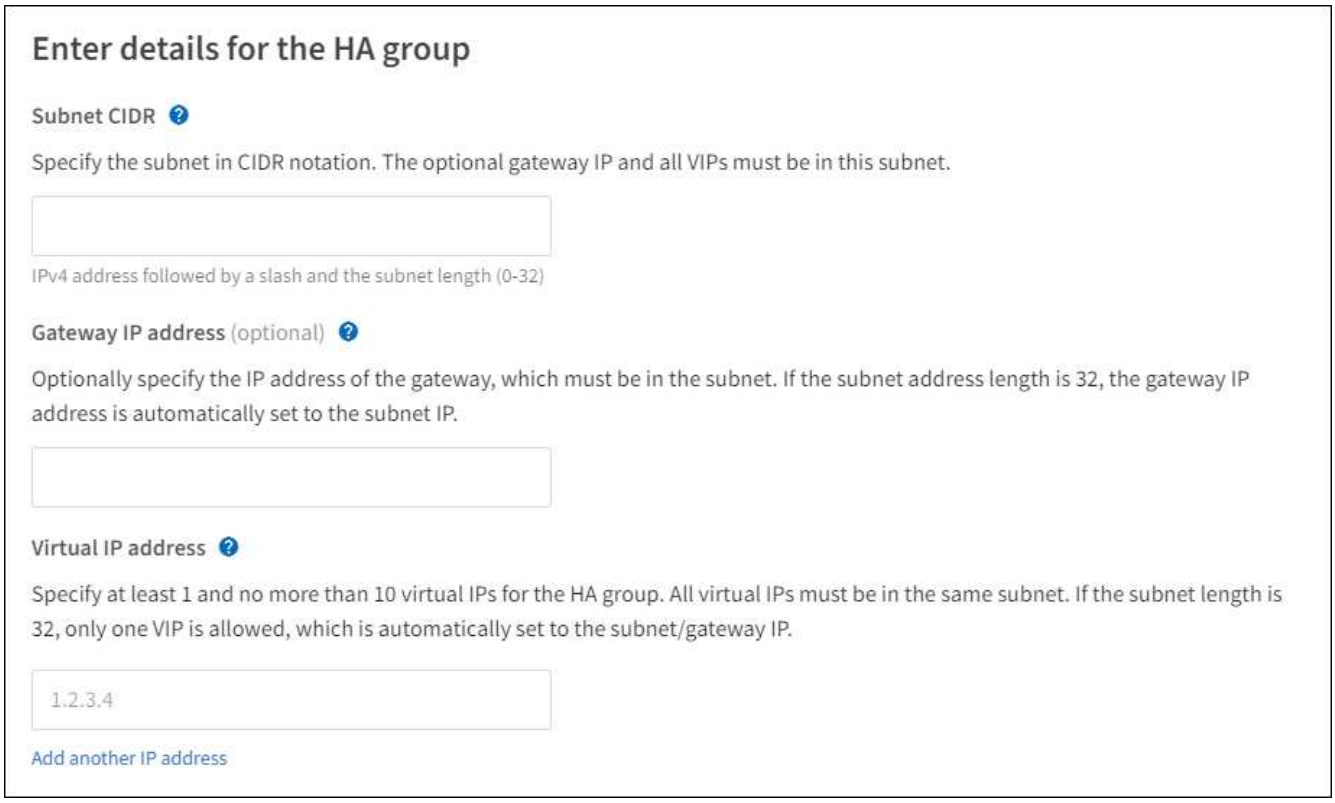
IP 주소를 입력합니다

단계

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

   네트워크 주소에는 호스트 비트가 설정되어 있지 않아야 합니다. `192.16.0.0/22`예를 들어,

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



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

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

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

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

4. HA 그룹 생성 * 을 선택하고 * 마침 * 을 선택합니다.

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

다음 단계

이 HA 그룹을 로드 밸런싱에 사용하려면 로드 밸런서 엔드포인트를 생성하여 포트 및 네트워크 프로토콜을 결정하고

필요한 인증서를 연결합니다. 을 "로드 밸런서 엔드포인트를 구성합니다"참조하십시오.

High Availability 그룹을 편집합니다

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

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

단계

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

   고가용성 그룹 페이지에는 기존의 모든 HA 그룹이 표시됩니다.

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

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

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

High Availability 그룹을 제거합니다

HA(고가용성) 그룹을 한 번에 하나 이상 제거할 수 있습니다.

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

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

사용하여 연결할 각 클라이언트를 업데이트합니다.

단계

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

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

로드 밸런싱 관리

로드 균형 조정에 대한 고려 사항

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

로드 밸런싱이란 무엇입니까?

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

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

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

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

몇 개의 로드 밸런싱 노드가 필요합니까?

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

로드 밸런서 엔드포인트란 무엇입니까?

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

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

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

포트에 대한 고려 사항

로드 밸런서 끝점의 포트는 사용자가 만든 첫 번째 끝점의 경우 기본적으로 10433으로 설정되지만 사용하지 않는 외부 포트는 1에서 65535 사이로 지정할 수 있습니다. 포트 80 또는 443을 사용하는 경우 엔드포인트는 게이트웨이 노드에서만 로드 밸런서 서비스를 사용합니다. 이러한 포트는 관리 노드에 예약되어 있습니다. 두 개 이상의 끝점에 동일한 포트를 사용하는 경우 각 끝점에 대해 다른 바인딩 모드를 지정해야 합니다.

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

네트워크 프로토콜에 대한 고려 사항

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

로드 밸런서 끝점 인증서에 대한 고려 사항

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

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

  로드 밸런서 끝점을 만들기 전에 다음 파일을 얻어야 합니다.

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

어떤 가치가 필요합니까?

인증서를 만들려면 S3 클라이언트 응용 프로그램이 끝점에 액세스하는 데 사용할 모든 도메인 이름과 IP 주소를 알고

있어야 합니다.

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

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

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

S3 가상 호스팅 스타일 요청을 사용하려는 경우 인증서에는 와일드카드 이름을 포함하여 구성한 각 항목에 대해 * Alternative Name * 항목도 포함되어야 "S3 끝점 도메인 이름입니다"합니다. 예를 들면 다음과 같습니다.

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

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

보안 인증서의 각 이름에 대한 DNS 항목도 정의해야 합니다.

만료 예정인 인증서를 관리하려면 어떻게 해야 합니까**?**

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

인증서 만료 문제를 방지하려면 다음 모범 사례를 따르십시오.

- 로드 밸런서 엔드포인트 인증서 만료 * 및 * S3 API용 글로벌 서버 인증서 만료 * 경고와 같이 인증서 만료 날짜가 다가올 경우 경고를 주의 깊게 모니터링하십시오.
- 항상 StorageGRID 및 S3 애플리케이션 버전의 인증서를 동기화된 상태로 유지합니다. 로드 밸런서 끝점에 사용되는 인증서를 교체하거나 갱신하는 경우 S3 애플리케이션에서 사용하는 동등한 인증서를 교체하거나 갱신해야 합니다.
- 공개적으로 서명된 CA 인증서를 사용합니다. CA에서 서명한 인증서를 사용하는 경우 만료 예정 인증서를 중단 없이 교체할 수 있습니다.
- 자체 서명된 StorageGRID 인증서를 생성했으며 인증서가 곧 만료될 경우 기존 인증서가 만료되기 전에 StorageGRID 및 S3 응용 프로그램 모두에서 수동으로 인증서를 교체해야 합니다.

바인딩 모드에 대한 고려 사항

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

다음 바인딩 모드 중 하나를 지정할 수 있습니다.

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

테넌트 액세스에 대한 고려 사항

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

이 기능을 사용하여 테넌트와 해당 끝점 간의 보안 격리를 향상시킬 수 있습니다. 예를 들어, 이 기능을 사용하여 한 테넌트가 소유한 기밀 자료 또는 기밀 자료를 다른 테넌트에서 완전히 액세스할 수 없도록 할 수 있습니다.

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

테넌트 액세스 예

이 보안 기능의 작동 방식을 이해하려면 다음 예제를 고려해 보십시오.

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

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

CPU 가용성

각 관리자 노드 및 게이트웨이 노드의 로드 밸런서 서비스는 S3 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 엔드포인트는 게이트웨이 및 관리 노드의 StorageGRID 로드 밸런서에 연결할 때

S3 클라이언트가 사용할 수 있는 포트 및 네트워크 프로토콜을 결정합니다. 끝점을 사용하여 그리드 관리자, 테넌트 관리자 또는 둘 다에 액세스할 수도 있습니다.

이 버전의 문서 사이트에서 Swift 세부 정보가 제거되었습니다. 을 "S3 및 Swift 클라이언트 연결을 구성합니다"참조하십시오.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.
- 를 검토했습니다."로드 균형 조정에 대한 고려 사항"
- 로드 밸런서 끝점에 사용할 포트를 이전에 다시 매핑한 경우 이 있는 "포트 재맵을 제거했습니다"것입니다.
- 사용할 고가용성(HA) 그룹을 만들었습니다. HA 그룹이 권장되지만 필수는 아닙니다. 을 "고가용성 그룹을 관리합니다"참조하십시오.
- 에서 로드 밸런서 엔드포인트를 사용할 경우 "S3 테넌트를 선택합니다"베어 메탈 노드의 IP 주소 또는 FQDN을 사용하지 않아야 합니다. S3 Select에 사용되는 로드 밸런서 엔드포인트에 서비스 어플라이언스 및 VMware 기반 소프트웨어 노드만 허용됩니다.
- 사용할 VLAN 인터페이스를 구성했습니다. 을 "VLAN 인터페이스를 구성합니다"참조하십시오.
- 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 클라이언트가 끝점에 액세스하는 데 사용할 모든 도메인 이름과 IP 주소가 필요합니다. 제목(고유 이름)도 알아야 합니다.
  - StorageGRID S3 API 인증서(스토리지 노드에 직접 연결하는 데 사용할 수도 있음)를 사용하려는 경우 이미 기본 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 대체한 것입니다. 을 "S3 API 인증서를 구성합니다"참조하십시오.

로드 밸런서 끝점을 만듭니다

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

마법사에 액세스합니다

단계

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

끝점 세부 정보를 입력합니다

단계

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

S3 또는 **Swift** 클라이언트

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

관리 인터페이스

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

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

1. Continue * 를 선택합니다.

바인딩 모드를 선택합니다

단계

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

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

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

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

관리 인터페이스 엔드포인트를 생성하는 경우 관리 노드만 허용됩니다.

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

   관리 인터페이스 끝점을 생성하는 경우 관리 노드에만 연결된 VIP를 선택합니다.

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

테넌트 액세스를 제어합니다

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

단계

1. Tenant access * 단계에서 다음 중 하나를 선택합니다.

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

2. HTTP* 끝점을 만드는 경우에는 인증서를 첨부할 필요가 없습니다. 새 로드 밸런서 끝점을 추가하려면 * Create * 를 선택합니다. 그런 다음 로 이동합니다작업을 마친 후. 그렇지 않으면 * 계속 * 을 선택하여 인증서를 첨부하십시오.

인증서를 첨부합니다

단계

1. HTTPS* 끝점을 만드는 경우 끝점에 연결할 보안 인증서 유형을 선택합니다.

   인증서는 관리자 노드 또는 게이트웨이 노드에서 S3 클라이언트와 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 인증서 사용 *. 스토리지 노드에 대한 직접 연결에도 사용할 수 있는 글로벌 S3 API 인증서를 사용하려면 이 옵션을 선택합니다.

그리드 CA에서 서명한 기본 S3 API 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 대체하지 않는 한 이 옵션을 선택할 수 없습니다. 을 "S3 API 인증서를 구성합니다"참조하십시오.

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

2. StorageGRID S3 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`).

     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. 확장자를 사용하여 파일을 `.pem` 저장합니다.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

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

d. Create * 를 선택합니다. + 로드 밸런서 끝점이 생성됩니다. 사용자 지정 인증서는 S3 클라이언트 또는 관리 인터페이스와 끝점 간의 모든 후속 새 연결에 사용됩니다.

인증서를 생성합니다

a. 인증서 생성 * 을 선택합니다.

b. 인증서 정보를 지정합니다.

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

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

c. Generate * 를 선택합니다.

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

   ▪ 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

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

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

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

e. Create * 를 선택합니다.

   로드 밸런서 끝점이 생성됩니다. 사용자 지정 인증서는 S3 클라이언트 또는 관리 인터페이스와 이 끝점 간의 모든 후속 새 연결에 사용됩니다.

작업을 마친 후

단계

1. DNS를 사용하는 경우 DNS에 StorageGRID FQDN(정규화된 도메인 이름)을 클라이언트가 연결에 사용할 각 IP 주소에 연결하는 레코드가 포함되어 있는지 확인합니다.

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

   ◦ HA 그룹을 구성한 경우 클라이언트는 해당 HA 그룹의 가상 IP 주소에 연결됩니다.

   ◦ HA 그룹을 사용하지 않는 경우 클라이언트는 게이트웨이 노드 또는 관리 노드의 IP 주소를 사용하여 StorageGRID 로드 밸런서 서비스에 연결됩니다.

   또한 DNS 레코드가 와일드카드 이름을 포함하여 필요한 모든 끝점 도메인 이름을 참조하는지 확인해야 합니다.

2. S3 클라이언트에 엔드포인트에 연결하는 데 필요한 정보 제공:

   ◦ 포트 번호입니다

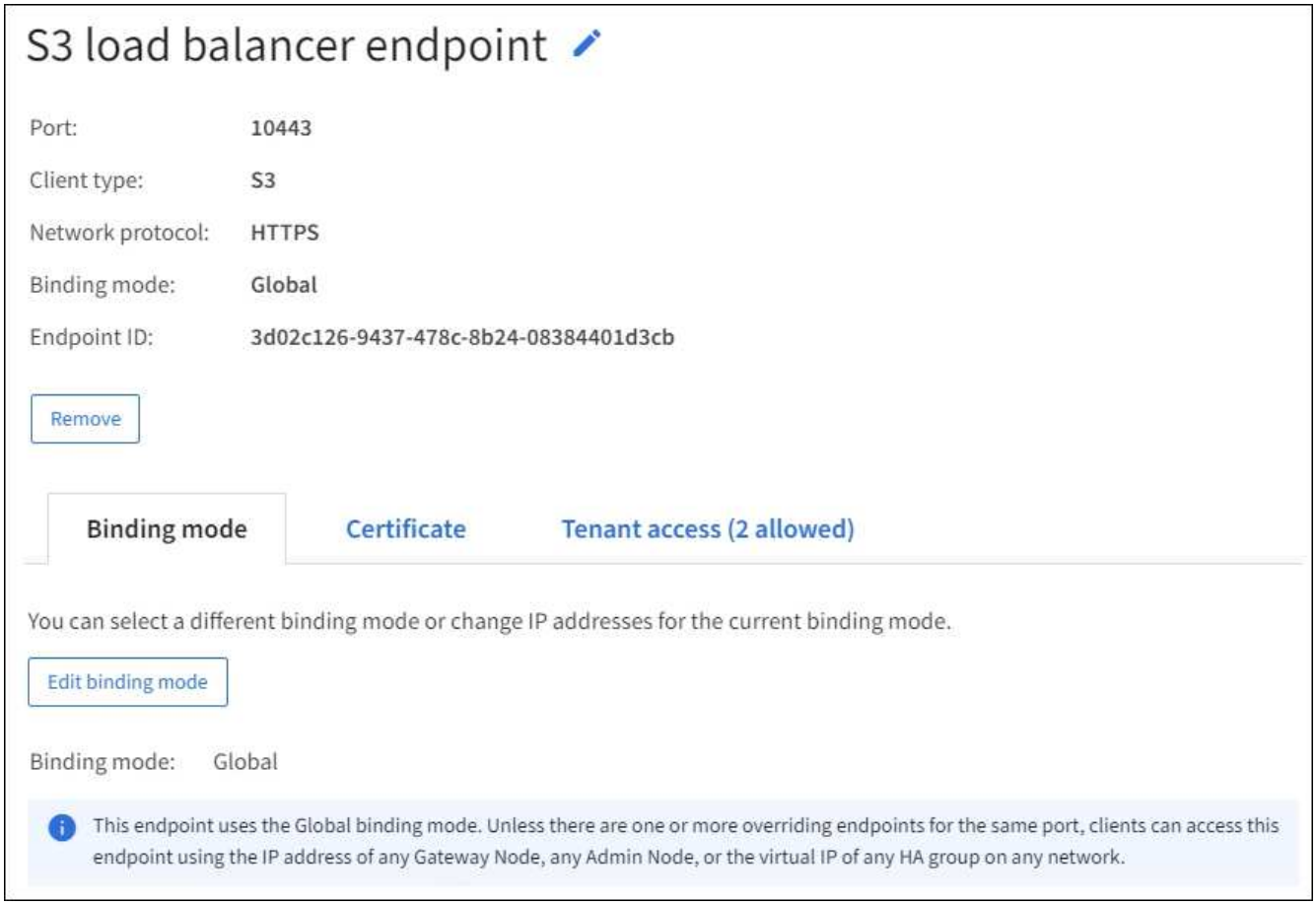
   ◦ 정규화된 도메인 이름 또는 IP 주소입니다

   ◦ 필요한 인증서 세부 정보입니다

로드 밸런서 끝점을 보고 편집합니다

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

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



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

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

끝점을 편집한 후 변경 내용이 모든 노드에 적용될 때까지 최대 15분 정도 기다려야 할 수 있습니다.

작업	작업 메뉴	세부 정보 페이지
끝점 이름을 편집합니다	a. 끝점의 확인란을 선택합니다. b. 작업 * > * 끝점 이름 편집 * 을 선택합니다. c. 새 이름을 입력합니다. d. 저장 * 을 선택합니다.	a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. 편집 아이콘을 선택합니다. c. 새 이름을 입력합니다. d. 저장 * 을 선택합니다.
엔드포인트 포트를 편집합니다	a. 끝점의 확인란을 선택합니다. b. Actions * > * Edit Endpoint port * 를 선택합니다 c. 유효한 포트 번호를 입력하십시오. d. 저장 * 을 선택합니다.	*n/a*
끝점 바인딩 모드를 편집합니다	a. 끝점의 확인란을 선택합니다. b. 작업 * > * 끝점 바인딩 모드 편집 * 을 선택합니다. c. 필요에 따라 바인딩 모드를 업데이트합니다. d. 변경 내용 저장 * 을 선택합니다.	a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. 바인딩 모드 편집 * 을 선택합니다. c. 필요에 따라 바인딩 모드를 업데이트합니다. d. 변경 내용 저장 * 을 선택합니다.
끝점 인증서를 편집합니다	a. 끝점의 확인란을 선택합니다. b. 작업 * > * 끝점 인증서 편집 * 을 선택합니다. c. 필요에 따라 새 사용자 지정 인증서를 업로드 또는 생성하거나 글로벌 S3 인증서를 사용합니다. 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 업로드 또는 생성하거나 글로벌 S3 인증서를 사용합니다. e. 변경 내용 저장 * 을 선택합니다.
테넌트 액세스를 편집합니다	a. 끝점의 확인란을 선택합니다. b. 작업 * > * 테넌트 액세스 편집 * 을 선택합니다. c. 다른 액세스 옵션을 선택하거나 목록에서 테넌트를 선택하거나 제거하거나 둘 모두를 수행합니다. d. 변경 내용 저장 * 을 선택합니다.	a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. Tenant access * 탭을 선택합니다. c. Edit tenant access * 를 선택합니다. d. 다른 액세스 옵션을 선택하거나 목록에서 테넌트를 선택하거나 제거하거나 둘 모두를 수행합니다. e. 변경 내용 저장 * 을 선택합니다.

로드 밸런서 끝점을 제거합니다

Actions * 메뉴를 사용하여 하나 이상의 끝점을 제거하거나 세부 정보 페이지에서 단일 끝점을 제거할 수 있습니다.

> 클라이언트 중단을 방지하려면 로드 밸런서 엔드포인트를 제거하기 전에 영향을 받는 S3 클라이언트 애플리케이션을 모두 업데이트하십시오. 다른 로드 밸런서 끝점에 할당된 포트를 사용하여 연결할 각 클라이언트를 업데이트합니다. 필요한 인증서 정보도 업데이트해야 합니다.

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

- 하나 이상의 끝점을 제거하려면:
  a. 부하 분산 장치 페이지에서 제거할 각 끝점에 대한 확인란을 선택합니다.
  b. Actions * > * Remove * 를 선택합니다.
  c. OK * 를 선택합니다.
- 세부 정보 페이지에서 끝점 하나를 제거하려면 다음을 수행합니다.
  a. 부하 분산 페이지에서 끝점 이름을 선택합니다.
  b. 세부 정보 페이지에서 * 제거 * 를 선택합니다.
  c. OK * 를 선택합니다.

S3 끝점 도메인 이름을 구성합니다

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

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

시작하기 전에

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

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

이 작업에 대해

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

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

  예를 들어, 끝점이 인 경우 HTTPS 연결에 사용되는 인증서에 끝점과 끝점의 와일드카드 SAN(Subject Alternative Name) `*.s3.company.com`이 `s3.company.com` 포함되어 있는지 확인해야 `s3.company.com` 합니다.

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

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

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

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

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

S3 엔드포인트 도메인 이름을 추가합니다

단계

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

결과

이제 클라이언트가 끝점을 사용하면 *bucket.s3.company.com* DNS 서버가 올바른 끝점으로 확인되고 인증서가 예상대로 끝점을 인증합니다.

S3 끝점 도메인 이름 바꾸기

S3 애플리케이션에서 사용하는 이름을 변경하면 가상 호스팅 스타일 요청이 실패합니다.

단계

1. 구성 * > * 네트워크 * > * S3 엔드포인트 도메인 이름 * 을 선택합니다.
2. 편집할 도메인 이름 필드를 선택하고 필요한 내용을 변경합니다.
3. 저장 * 을 선택합니다.
4. 예 * 를 선택하여 변경 사항을 확인합니다.

S3 끝점 도메인 이름을 삭제합니다

S3 애플리케이션에서 사용하는 이름을 제거하면 가상 호스팅 스타일 요청이 실패합니다.

단계

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

관련 정보

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

요약: 클라이언트 연결을 위한 IP 주소 및 포트

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

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

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

연결 위치	클라이언트가 연결하는 서비스입니다	IP 주소입니다	포트
HA 그룹	로드 밸런서	HA 그룹의 가상 IP 주소입니다	로드 밸런서 끝점에 할당된 포트입니다
관리자 노드	로드 밸런서	관리 노드의 IP 주소입니다	로드 밸런서 끝점에 할당된 포트입니다
게이트웨이 노드	로드 밸런서	게이트웨이 노드의 IP 주소입니다	로드 밸런서 끝점에 할당된 포트입니다
스토리지 노드	LDR	스토리지 노드의 IP 주소입니다	기본 S3 포트: • HTTPS: 18082 • HTTP: 18084

URL의 예

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

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

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

`https://192.0.2.5:10443`

IP 주소를 찾을 위치

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

   클라이언트 응용 프로그램에서 목록의 IP 주소로의 연결을 설정할 수 있습니다.

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

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

3. 고가용성 그룹의 가상 IP 주소를 찾으려면 다음을 수행합니다.
   a. 구성 * > * 네트워크 * > * 고가용성 그룹 * 을 선택합니다.
   b. 표에서 HA 그룹의 가상 IP 주소를 확인합니다.
4. 로드 밸런서 끝점의 포트 번호를 찾으려면 다음을 수행합니다.
   a. 구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 * 를 선택합니다.
   b. 사용할 끝점의 포트 번호를 확인합니다.

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

   c. 테이블에서 끝점 이름을 선택합니다.
   d. 클라이언트 유형 * (S3)이 끝점을 사용할 클라이언트 응용 프로그램과 일치하는지 확인합니다.

네트워크 및 연결을 관리합니다

네트워크 설정을 구성합니다

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

VLAN 인터페이스를 구성합니다

보안, 유연성 및 성능을 위해 트래픽을 격리하고 파티셔닝할 수 "VLAN(Virtual LAN) 인터페이스를 생성합니다 "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.

트래픽 분류 정책

를 사용하면 특정 버킷, 테넌트, 클라이언트 서브넷 또는 로드 밸런서 끝점과 관련된 트래픽을 포함하여 다양한 유형의 네트워크 트래픽을 식별하고 처리할 수 "트래픽 분류 정책"있습니다. 이러한 정책은 트래픽 제한 및 모니터링을 지원할 수 있습니다.

StorageGRID 네트워크 지침

그리드 관리자를 사용하여 StorageGRID 네트워크 및 연결을 구성하고 관리할 수 있습니다.

S3 클라이언트 연결 방법은 를 "S3 클라이언트 연결을 구성합니다"참조하십시오.

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 "네트워킹 지침"참조하십시오.

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 클라이언트 응용 프로그램에 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 노드에는 할당된 각 네트워크에 대해 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)	윤리2

- 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, 트렁크 인터페이스를 관리자 또는 게이트웨이 노드에 추가하여 를 서로 다른 애플리케이션 또는 테넌트에 속한 트래픽을 분리할 수 "VLAN 인터페이스"있습니다. 또는 에서 사용할 액세스 인터페이스를 추가할 수도 "고가용성(HA) 그룹"있습니다.

트렁크 또는 액세스 인터페이스를 추가하려면 다음을 참조하십시오.

- * VMware(노드 설치 후) *: "VMware: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다"
  - * Red Hat Enterprise Linux(노드 설치 전) *: "노드 구성 파일을 생성합니다"
  - * Ubuntu 또는 Debian (노드를 설치하기 전에) *: "노드 구성 파일을 생성합니다"
  - * RHEL, 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.

시작하기 전에

을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"

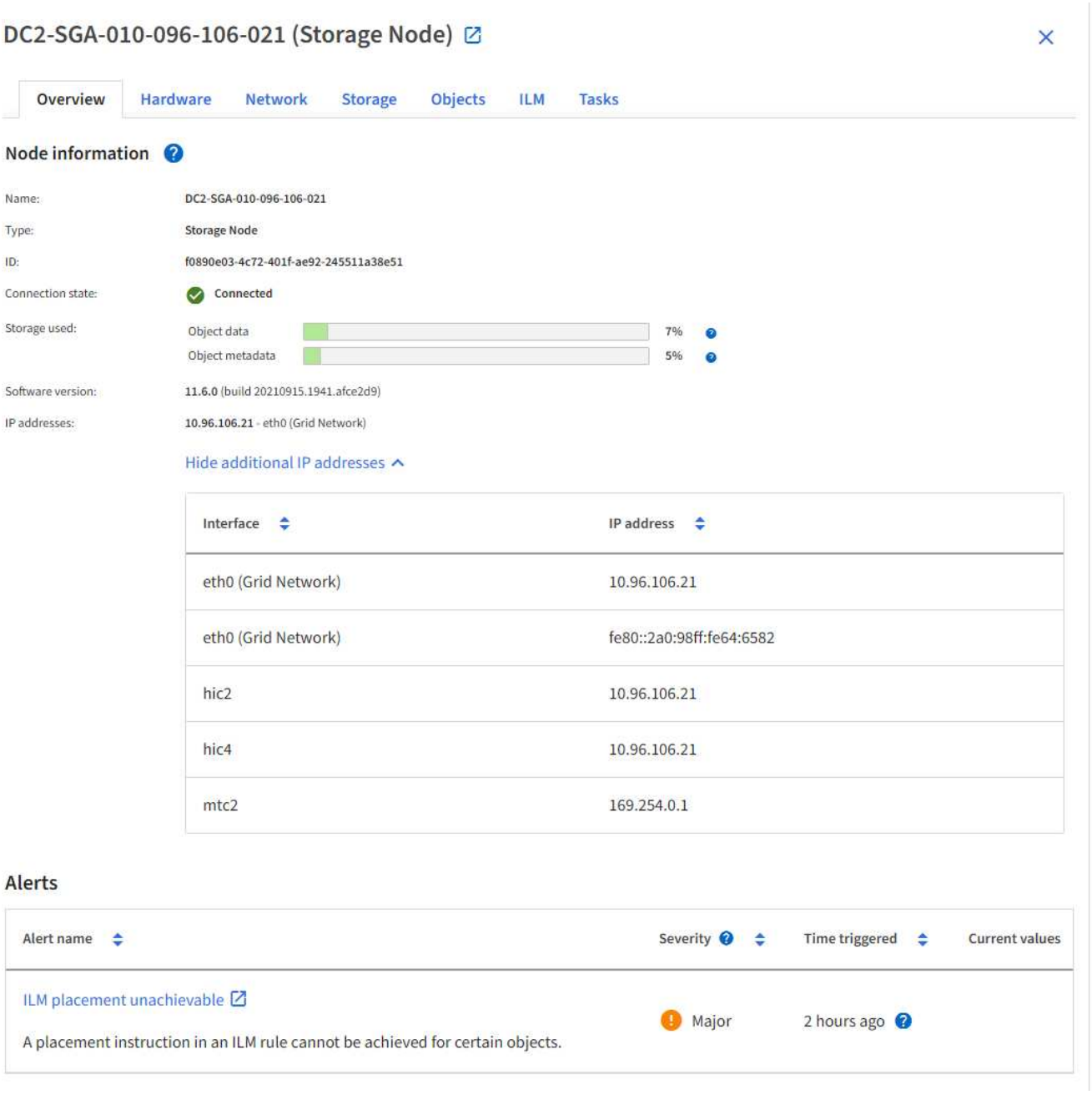
이 작업에 대해

IP 주소 변경에 대한 자세한 내용은 를 "IP 주소를 구성합니다"참조하십시오.

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.



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 VLAN에 대한 상위 인터페이스와 동일한 게이트웨이 노드에서 그리드 네트워크 인터페이스와 클라이언트 네트워크 인터페이스를 모두 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 클라이언트 트래픽용 인터페이스인 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(노드 설치 전) *: "노드 구성 파일을 생성합니다"
  - * Ubuntu 또는 Debian (노드를 설치하기 전에) *: "노드 구성 파일을 생성합니다"
  - * RHEL, Ubuntu 또는 Debian(노드 설치 후) *: "Linux: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다"

VLAN 인터페이스를 생성합니다

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"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

단계

1. 구성 * > * 네트워크 * > * VLAN 인터페이스 * 를 선택합니다.

2. Create * 를 선택합니다.

VLAN 인터페이스에 대한 세부 정보를 입력합니다

단계

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.

2. 선택적으로 VLAN 인터페이스에 대한 간단한 설명을 입력합니다.
3. Continue * 를 선택합니다.

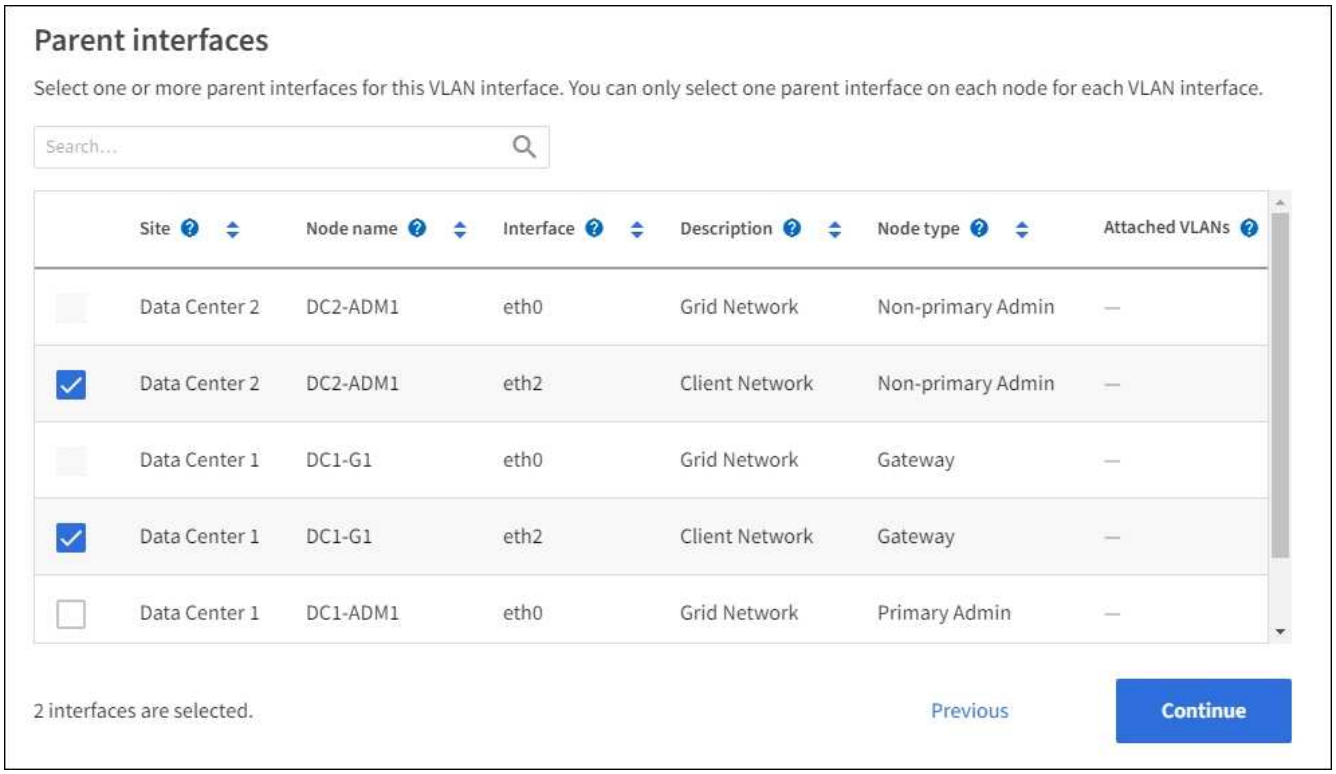
상위 인터페이스를 선택합니다

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.

단계

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

단계

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 휴지통을 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 A 및 B의 상위 인터페이스에 연결되어 있다고 가정합니다. HA 그룹이 노드 A의 VLAN 200 인터페이스와 노드 B의 eth2 인터페이스를 사용하는 경우 노드 B의 사용되지 않는 상위 인터페이스를 제거할 수는 있지만 노드 A에서 사용된 상위 인터페이스를 제거할 수는 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.

트래픽 분류 정책을 관리합니다

트래픽 분류 정책이란 무엇입니까?

트래픽 분류 정책을 사용하면 다양한 유형의 네트워크 트래픽을 식별하고 모니터링할 수 있습니다. 이러한 정책은 트래픽 제한 및 모니터링을 지원하여 QoS(Quality-of-Service) 서비스를 향상시킬 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
- 서브넷
- 테넌트
- 부하 분산 장치 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 제한 유형을 정책에 추가할 수 있습니다.

- 애그리게이트 대역폭
- 요청 당 대역폭
- 동시 요청
- 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. 요청에 사용된 대역폭은 총 대역폭 제한 정책을 포함하는 비교적 덜 특정한 다른 정책에 포함되지 않습니다. 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.

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	최대 성능이 허용됩니다	비용
골드	1PB의 스토리지가 허용됩니다	ILM 규칙 3개 복사	초당 25K 요청 5GB/sec(40Gbps) 대역폭	$$/월
실버	250TB 스토리지 허용	ILM 규칙 2개 복사	초당 10K 요청 1.25GB/sec(10Gbps) 대역폭	$$/월
브론즈	100TB 스토리지 허용	ILM 규칙 2개 복사	초당 5K 요청 1 GB/sec(8Gbps) 대역폭	$/월

트래픽 분류 정책을 생성합니다

트래픽 분류 정책을 생성하고 버킷, 버킷 regex, CIDR, 부하 분산 단말 장치 또는 테넌트별로

네트워크 트래픽을 선택적으로 제한할 수 있습니다. 필요에 따라 대역폭, 동시 요청 수 또는 요청 속도를 기준으로 정책에 대한 제한을 설정할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.
- 일치시킬 로드 밸런서 끝점을 만들었습니다.
- 일치시킬 테넌트를 만들었습니다.

단계

1. 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택합니다.
2. Create * 를 선택합니다.
3. 정책의 이름과 설명(선택 사항)을 입력하고 * Continue * 를 선택합니다.

   예를 들어, 이 트래픽 분류 정책이 적용되는 대상 및 제한할 내용에 대해 설명하십시오.

4. 규칙 추가 * 를 선택하고 다음 세부 정보를 지정하여 정책에 일치하는 규칙을 하나 이상 만듭니다. 생성하는 모든 정책에는 하나 이상의 일치하는 규칙이 있어야 합니다. Continue * 를 선택합니다.

필드에 입력합니다	설명
유형	일치하는 규칙이 적용되는 트래픽 유형을 선택합니다. 트래픽 유형은 버킷, 버킷 regex, CIDR, 부하 분산 단말 장치 및 테넌트입니다.
일치 값	선택한 유형과 일치하는 값을 입력합니다. • 버킷: 하나 이상의 버킷 이름을 입력합니다. • 버킷 정규식: 버킷 이름 집합과 일치하는 데 사용되는 하나 이상의 정규식을 입력합니다. 정규식이 고정 해제됩니다. ^anchor를 사용하여 버킷 이름의 시작 부분에 일치시키고 $ anchor를 사용하여 이름 끝에 일치시킵니다. 정규식 일치는 PCRE(Perl 호환 정규식) 구문의 하위 집합을 지원합니다. • CIDR: 원하는 서브넷과 일치하는 하나 이상의 IPv4 서브넷을 CIDR 표기법으로 입력합니다. • 로드 밸런서 끝점: 끝점 이름을 선택합니다. 에서 정의한 로드 밸런서 엔드포인트입니다."로드 밸런서 엔드포인트를 구성합니다" • 테넌트: 테넌트 일치는 액세스 키 ID를 사용합니다. 요청에 액세스 키 ID(예: 익명 액세스)가 없으면 액세스한 버킷의 소유권이 테넌트를 결정하는 데 사용됩니다.

필드에 입력합니다	설명
역일치	방금 정의한 유형 및 일치 값과 일치하는 모든 network traffic_except_traffic을 일치시키려면 * 역일치 * 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 * 역일치 * 를 선택합니다. 하나 이상의 교자가 역마쳐인 여러 마처를 포함하는 정책의 경우 모든 요청과 일치하는 정책을 만들지 않도록 주의하십시오.

5. 필요에 따라 * 제한 추가 * 를 선택하고 다음 세부 정보를 선택하여 규칙에 일치하는 네트워크 트래픽을 제어하는 하나 이상의 제한을 추가합니다.

> StorageGRID는 제한을 추가하지 않아도 메트릭을 수집하므로 트래픽 추세를 파악할 수 있습니다.

필드에 입력합니다	설명
유형	규칙에 일치하는 네트워크 트래픽에 적용할 제한 유형입니다. 예를 들어, 대역폭 또는 요청 속도를 제한할 수 있습니다. • 참고 *: 정책을 작성하여 총 대역폭을 제한하거나 요청 당 대역폭을 제한할 수 있습니다. 그러나 StorageGRID는 두 가지 유형의 대역폭을 동시에 제한할 수 없습니다. 애그리게이트 대역폭이 사용 중인 경우 요청당 대역폭을 사용할 수 없습니다. 반대로, 요청 당 대역폭이 사용 중일 때는 총 대역폭을 사용할 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
적용 대상	이 제한이 클라이언트 읽기 요청(GET 또는 HEAD) 또는 쓰기 요청(PUT, POST 또는 DELETE)에 적용될지 여부를 나타냅니다.

필드에 입력합니다	설명
값	선택한 장치에 따라 네트워크 트래픽이 로 제한됩니다. 예를 들어, 10을 입력하고 MiB/s를 선택하면 이 규칙에 일치하는 네트워크 트래픽이 10MiB/s를 초과하지 않습니다 • 참고 *: 단위 설정에 따라 사용 가능한 단위는 2진수(예: GiB) 또는 10진수(예: GB)가 됩니다. 단위 설정을 변경하려면 그리드 관리자 오른쪽 상단의 사용자 드롭다운을 선택한 다음 * 사용자 기본 설정 * 을 선택합니다.
단위	입력한 값을 설명하는 단위입니다.

예를 들어 SLA 계층에 대해 40GB/s 대역폭 제한을 생성하려면 40GB/s에서 GET/HEAD 및 PUT/POST/DELETE의 두 가지 집계 대역폭 제한을 생성합니다

6. Continue * 를 선택합니다.
7. 트래픽 분류 정책을 읽고 검토하십시오. Previous * (이전 *) 버튼을 사용하여 돌아가서 필요에 따라 변경합니다. 정책에 만족하면 * Save and continue * 를 선택합니다.

   이제 S3 클라이언트 트래픽이 트래픽 분류 정책에 따라 처리됩니다.

작업을 마친 후

"네트워크 트래픽 메트릭을 확인합니다" 정책이 예상한 트래픽 제한을 적용하고 있는지 확인합니다.

트래픽 분류 정책을 편집합니다

트래픽 분류 정책을 편집하여 이름 또는 설명을 변경하거나 정책에 대한 규칙 또는 제한을 생성, 편집 또는 삭제할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.

단계

1. 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택합니다.

   트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

2. 작업 메뉴 또는 세부 정보 페이지를 사용하여 정책을 편집합니다. 입력할 항목은 을 "트래픽 분류 정책을 생성합니다"참조하십시오.

작업 메뉴

a. 정책 확인란을 선택합니다.

b. Actions * > * Edit * 를 선택합니다.

세부 정보 페이지

a. 정책 이름을 선택합니다.

b. 정책 이름 옆의 * Edit * 버튼을 선택합니다.

3. Enter policy name(정책 이름 입력) 단계에서 필요에 따라 정책 이름 또는 설명을 편집하고 * Continue *(계속 *)를 선택합니다.
4. 일치하는 규칙 추가 단계에서는 필요에 따라 규칙을 추가하거나 기존 규칙의 * 유형 * 및 * 일치 값 * 을 편집하고 * 계속 * 을 선택합니다.
5. Set limits(제한 설정) 단계에서 필요에 따라 제한을 추가, 편집 또는 삭제하고 * Continue *(계속 *)를 선택합니다.
6. 업데이트된 정책을 검토하고 * Save and continue * 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

더 이상 필요하지 않은 경우 트래픽 분류 정책을 삭제할 수 있습니다. 삭제 시 정책을 검색할 수 없으므로 올바른 정책을 삭제해야 합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.

단계

1. 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택합니다.

   트래픽 분류 정책 페이지가 테이블에 나열된 기존 정책과 함께 나타납니다.

2. 작업 메뉴 또는 세부 정보 페이지를 사용하여 정책을 삭제합니다.

작업 메뉴

a. 정책 확인란을 선택합니다.

b. Actions * > * Remove * 를 선택합니다.

정책 세부 정보 페이지

a. 정책 이름을 선택합니다.

b. 정책 이름 옆의 * 제거 * 버튼을 선택합니다.

3. 예 * 를 선택하여 정책을 삭제할 것임을 확인합니다.

   정책이 삭제됩니다.

네트워크 트래픽 메트릭을 확인합니다

트래픽 분류 정책 페이지에서 사용할 수 있는 그래프를 보고 네트워크 트래픽을 모니터링할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 또는 테넌트 계정 권한"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 여부를 결정할 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.

2. 메트릭을 보려는 트래픽 분류 정책 이름을 선택합니다.
3. 메트릭 * 탭을 선택합니다.

   트래픽 분류 정책 그래프가 나타납니다. 그래프에는 선택한 정책과 일치하는 트래픽에 대한 메트릭만 표시됩니다.

   다음 그래프가 페이지에 포함되어 있습니다.

   - 요청 속도: 이 그래프는 모든 로드 밸런싱 장치가 처리하는 이 정책과 일치하는 대역폭을 제공합니다. 수신된 데이터에는 모든 요청에 대한 요청 헤더와 본문 데이터가 있는 응답에 대한 본문 데이터 크기가 포함됩니다. 보낸 편지에는 모든 요청에 대한 응답 헤더와 응답에 본문 데이터가 포함된 요청에 대한 응답 본문 데이터 크기가 포함됩니다.

     > 요청이 완료되면 이 차트는 대역폭 사용량만 표시합니다. 오브젝트 요청이 느리거나 큰 경우 실제 순간 대역폭은 이 그래프에 보고된 값과 다를 수 있습니다.

   - 오류 응답 속도: 이 그래프는 이 정책과 일치하는 요청이 클라이언트에 오류(HTTP 상태 코드 >= 400)를 반환하는 대략적인 속도를 제공합니다.
   - 평균 요청 기간(오류 없음): 이 그래프는 이 정책과 일치하는 성공적인 요청의 평균 기간을 제공합니다.
   - 정책 대역폭 사용량: 이 그래프는 모든 로드 밸런싱 장치가 처리하는 이 정책과 일치하는 대역폭을 제공합니다. 수신된 데이터에는 모든 요청에 대한 요청 헤더와 본문 데이터가 있는 응답에 대한 본문 데이터 크기가 포함됩니다. 보낸 편지에는 모든 요청에 대한 응답 헤더와 응답에 본문 데이터가 포함된 요청에 대한 응답 본문 데이터 크기가 포함됩니다.

4. 커서를 선 그래프 위에 놓으면 그래프의 특정 부분에 값 팝업이 표시됩니다.
5. 메트릭 제목 바로 아래에 있는 * Grafana 대시보드 * 를 선택하여 정책에 대한 모든 그래프를 봅니다. Metrics * 탭의 네 가지 그래프 외에도 두 개의 그래프를 더 볼 수 있습니다.
   - 객체 크기별 쓰기 요청 비율: 이 정책과 일치하는 PUT/POST/DELETE 요청 비율. 개별 셀에 위치하면 초당 비율이 표시됩니다. 호버 보기에 표시된 속도는 정수 수로 잘리고 버켓에 0이 아닌 요청이 있을 경우 0으로 보고할 수 있습니다.
   - 객체 크기별 읽기 요청 비율: 이 정책과 일치하는 GET/HEAD 요청의 비율 개별 셀에 위치하면 초당 비율이 표시됩니다. 호버 보기에 표시된 속도는 정수 수로 잘리고 버켓에 0이 아닌 요청이 있을 경우 0으로 보고할 수 있습니다.
6. 또는 * 지원 * 메뉴에서 그래프에 액세스하십시오.
   a. 지원 * > * 도구 * > * 메트릭 * 을 선택합니다.
   b. Grafana * 섹션에서 * 트래픽 분류 정책 * 을 선택합니다.
   c. 페이지 왼쪽 상단의 메뉴에서 정책을 선택합니다.
   d. 그래프 위에 커서를 놓으면 샘플의 날짜 및 시간, 개수로 집계된 개체 크기 및 해당 기간 동안 초당 요청 수를 보여 주는 팝업이 표시됩니다.

      트래픽 분류 정책은 ID로 식별됩니다. 정책 ID는 트래픽 분류 정책 페이지에 나열되어 있습니다.
7. 그래프를 분석하여 정책에 따라 트래픽이 제한되는 빈도와 정책을 조정해야 하는지 여부를 결정합니다.

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 클라이언트 애플리케이션에서 사용할 수 있도록 지원되는 암호화 목록보다 큽니다. 암호를 구성하려면 * 구성 * > * 보안 * > * 보안 설정 * 으로 이동하여 * TLS 및 SSH 정책 * 을 선택합니다.

> 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.

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 노드에 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.

스토리지 노드에 대한 클라이언트 연결의 경우 활성 HTTP 연결을 제한하면 다음과 같은 이점이 있습니다.

- StorageGRID 시스템 전체에서 최적의 로드 밸런싱을 지원합니다.

  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.

- 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.

링크 비용 관리

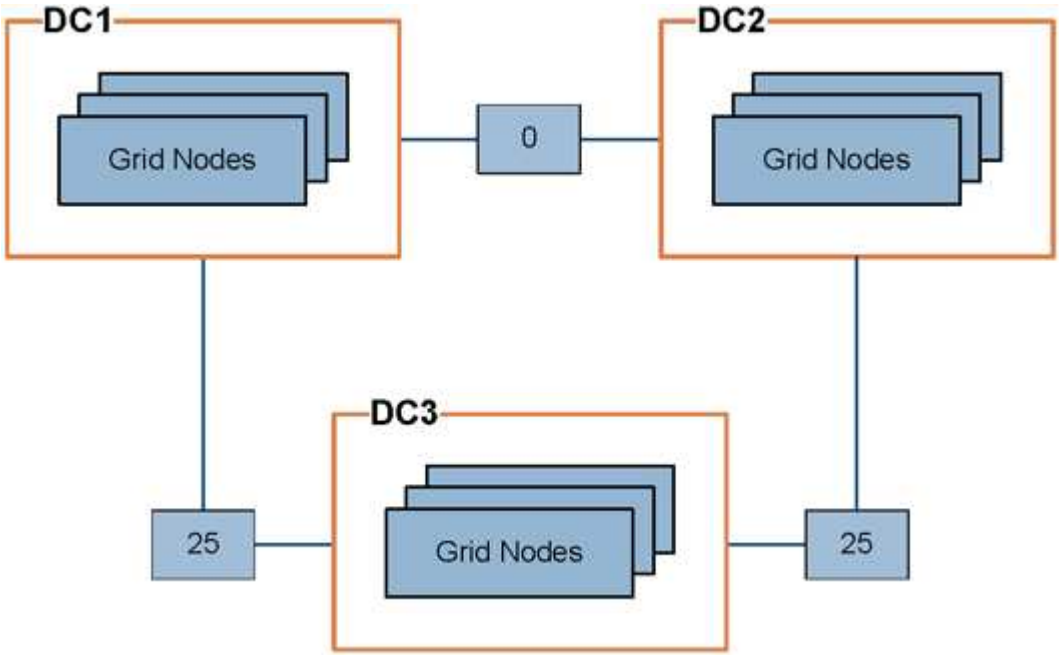
링크 비용을 사용하면 둘 이상의 데이터 센터 사이트가 있을 때 요청된 서비스를 제공하는 데이터 센터 사이트의 우선 순위를 지정할 수 있습니다. 링크 비용을 조정하여 사이트 간 지연 시간을 반영할 수 있습니다.

링크 비용이란 무엇입니까**?**

- 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 관리 노드 및 게이트웨이 노드의 부하 분산 서비스에서 클라이언트 연결을 연결하는 데 사용됩니다. 을 "로드 균형 조정에 대한 고려 사항"참조하십시오.

다이어그램에는 사이트 간에 구성된 링크 비용이 있는 세 개의 사이트 표가 표시됩니다.



- 관리 노드 및 게이트웨이 노드의 부하 분산 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 모두 저장된 개체를 검색할 경우 DC1에서 DC2로의 링크 비용은 DC3에서 DC2로의 링크 비용(25)보다 낮은 0이므로 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
동일한 물리적 위치의 논리적 데이터 센터 사이트 간	0	LAN으로 연결된 동일한 물리적 건물 또는 캠퍼스의 논리적 데이터 센터

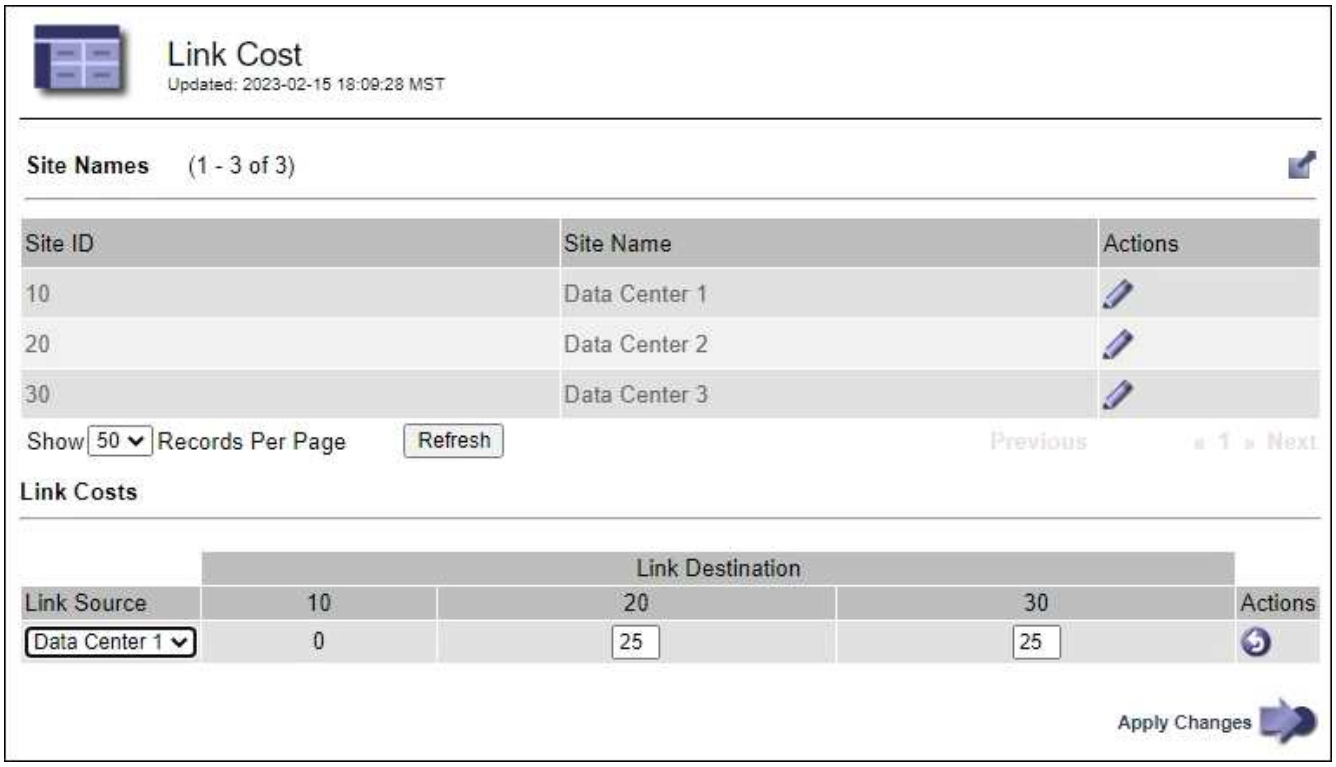
사이트 간 지연 시간을 반영하기 위해 데이터 센터 사이트 간의 링크 비용을 업데이트할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "그리드 토폴로지 페이지 구성 권한"있습니다.

단계

1. 지원 * > * 기타 * > * 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 * 복원 * 을 선택합니다.

3. Apply Changes * 를 선택합니다.

AutoSupport를 사용합니다

AutoSupport란 무엇입니까?

AutoSupport 기능을 사용하면 StorageGRID에서 상태 패키지를 NetApp 기술 지원으로 보낼 수 있습니다.

AutoSupport를 사용하면 문제를 훨씬 빠르게 확인하고 해결할 수 있습니다. 기술 지원 부서에서는 시스템의 스토리지 요구 사항을 모니터링하여 새 노드나 사이트를 추가해야 하는지 여부를 결정할 수 있습니다. 선택적으로 하나의 추가 대상으로 AutoSupport 패키지를 보내도록 구성할 수 있습니다.

StorageGRID에는 두 가지 유형의 AutoSupport가 있습니다.

- * StorageGRID AutoSupport * 는 StorageGRID 소프트웨어 문제를 보고합니다. StorageGRID를 처음 설치할 때 기본적으로 사용됩니다. 필요한 경우 수행할 수 "기본 AutoSupport 구성을 변경합니다"있습니다.

> StorageGRID 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.

- * 어플라이언스 하드웨어 AutoSupport * 는 StorageGRID 어플라이언스 문제를 보고합니다. 반드시 해야 "각 어플라이언스에 하드웨어 AutoSupport를 구성합니다"합니다.

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 패키지에 포함된 정보입니다

AutoSupport 패키지에는 다음과 같은 파일과 세부 정보가 들어 있습니다.

파일 이름입니다	필드를 선택합니다	설명
autosupport-history.xml	이 AutoSupport에 대한 AutoSupport 시퀀스 번호 + 대상 + 전달 상태 + 전송 시도 + AutoSupport 제목 + 전송 URI + 마지막 오류 + AutoSupport 파일 이름 + 생성 시간 + AutoSupport 압축 크기 + AutoSupport 압축 해제 크기 + 총 수집 시간(ms)	AutoSupport 기록 파일.
AutoSupport.xml을 참조하십시오	지원 문의 지원 + HTTP/HTTPS에 대한 지원 URL + 지원 주소 + AutoSupport OnDemand 상태 + AutoSupport OnDemand 서버 URL + AutoSupport OnDemand 폴링 간격	AutoSupport 상태 파일. 사용된 프로토콜, 기술 지원 URL 및 주소, 폴링 간격 및 활성화 또는 비활성화한 경우 OnDemand AutoSupport에 대한 자세한 내용은 에 나와 있습니다.

파일 이름입니다	필드를 선택합니다	설명
버킷.xml	버킷 ID + 계정 ID + 빌드 버전 + 위치 제약 구성 + 규정 준수 활성화 + 규정 준수 구성 + S3 오브젝트 잠금 활성화 + S3 오브젝트 잠금 구성 + 일관성 구성 + CORS 활성화 + CORS 구성 + 마지막 액세스 시간 활성화 + 정책 활성화 + 정책 구성 + 알림 설정 + 클라우드 미러 구성 + 활성화 검색 + 검색 구성 + 버킷 태깅 지원	버킷 수준의 구성 세부 정보 및 통계를 제공합니다. 버킷 구성의 예로는 플랫폼 서비스, 규정 준수 및 버킷 일관성이 있습니다.
그리드-설정.xml	특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	그리드 전체의 구성 정보 파일입니다. 그리드 인증서, 메타데이터 예약 공간, 그리드 전체 구성 설정(규정 준수, S3 오브젝트 잠금, 오브젝트 압축, 경고, syslog 및 ILM 구성), 삭제 코딩 프로필 세부 정보, DNS 이름 및 ILM 구성 등에 대한 정보가 포함되어 있습니다"NMS 이름".
그리드 사양 XML	그리드 사양, 원시 XML	StorageGRID 구성 및 배포에 사용됩니다. 그리드 사양, NTP 서버 IP, DNS 서버 IP, 네트워크 토폴로지 및 노드의 하드웨어 프로필을 포함합니다.
그리드 - tasks.xml	노드 + 서비스 경로 + 특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	그리드 작업(유지보수 절차) 상태 파일입니다. 그리드의 활성, 종료, 완료, 실패 및 보류 중인 작업에 대한 세부 정보를 제공합니다.
그리드.JSON	그리드 + 개정 + 소프트웨어 버전 + 설명 + 라이센스 + 암호 + DNS + NTP + 사이트 + 노드	그리드 정보
ILM-configuration.xml을 참조하십시오	특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	ILM 구성에 대한 특성 목록입니다.
ILM-STATUS.xml입니다	노드 + 서비스 경로 + 특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	ILM 메트릭 정보 파일 각 노드에 대한 ILM 평가율과 그리드 전체 메트릭에 대한 ILM 평가율이 포함되어 있습니다.
ILM.xml을 참조하십시오	ILM 원시 XML	ILM 활성 정책 파일 스토리지 풀 ID, 수집 동작, 필터, 규칙 및 설명과 같은 활성 ILM 정책에 대한 세부 정보를 제공합니다.
Log.TGZ(로그 TGZ	*n/a*	로그 파일을 다운로드할 수 있습니다. 각 노드에서 및 `servermanager.log` 을 `bycast-err.log` 포함합니다.

파일 이름입니다	필드를 선택합니다	설명
매니페스트.xml	이 데이터에 대한 수집 순서 + AutoSupport 콘텐츠 파일 이름 + 이 데이터 항목에 대한 설명 + 수집된 바이트 수 + 수집에 소요된 시간 + 이 데이터 항목의 상태 + 이 데이터에 대한 AutoSupport 콘텐츠 형식 설명 +	AutoSupport 메타데이터와 모든 AutoSupport 파일에 대한 간략한 설명을 포함합니다.
nms-entities.xml입니다	속성 인덱스 + 엔터티 OID + 노드 ID + 장치 모델 ID + 장치 모델 버전 + 엔터티 이름	의 그룹 및 서비스 엔티티"NMS 트리" 그리드 토폴로지 세부 정보를 제공합니다. 노드는 노드에서 실행되는 서비스를 기반으로 확인할 수 있습니다.
개체 - 상태 .xml	노드 + 서비스 경로 + 특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	배경 스캔 상태, 활성 전송, 전송 속도, 총 전송, 삭제 속도, 손상된 조각, 손실된 개체, 누락된 개체, 복구 시도, 스캔 속도, 예상 스캔 기간 및 복구 완료 상태를 포함한 개체 상태.
서버 상태 .xml	노드 + 서비스 경로 + 특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	서버 구성. 각 노드에 대한 세부 정보가 포함됩니다. 플랫폼 유형, 운영 체제, 설치된 메모리, 사용 가능한 메모리, 스토리지 연결, 스토리지 어플라이언스 섀시 일련 번호, 스토리지 컨트롤러 오류 드라이브 수, 컴퓨팅 컨트롤러 섀시 온도, 컴퓨팅 하드웨어, 컴퓨팅 컨트롤러 일련 번호, 전원 공급 장치, 드라이브 크기, 드라이브 유형.
서비스 상태 .xml	노드 + 서비스 경로 + 특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	서비스 노드 정보 파일입니다. 할당된 테이블 공간, 사용 가능한 테이블 공간, 데이터베이스의 Reaper 메트릭, 세그먼트 복구 기간, 복구 작업 기간, 자동 작업 재시작 및 자동 작업 종료와 같은 세부 정보가 포함됩니다.
저장 - 등급 .xml	스토리지 등급 ID + 스토리지 등급 이름 + 스토리지 노드 ID + 스토리지 노드 경로입니다	각 스토리지 노드에 대한 스토리지 등급 정의 파일입니다.
요약 - attributes.xml	그룹 OID + 그룹 경로 + 요약 속성 ID + 요약 속성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	StorageGRID 사용 정보를 요약하는 상위 수준의 시스템 상태 데이터입니다. 그리드 이름, 사이트 이름, 그리드당 및 사이트당 스토리지 노드 수, 라이센스 유형, 라이센스 용량 및 사용, 소프트웨어 지원 조건, S3 작업 세부 정보와 같은 세부 정보를 제공합니다.

파일 이름입니다	필드를 선택합니다	설명
System-alerts.xml을 참조하십시오	이름 + 심각도 + 노드 이름 + 경고 상태 + 사이트 이름 + 경고 트리거 시간 + 경고 해결 시간 + 규칙 ID + 노드 ID + 사이트 ID + 해제 + 기타 주석 + 기타 레이블	StorageGRID 시스템의 잠재적 문제를 나타내는 현재 시스템 알림입니다.
USERAGENTS.xml을 참조하십시오	사용자 에이전트 + 일 수 + 총 HTTP 요청 수 + 수집된 총 바이트 수 + 검색된 총 바이트 수 + 검색된 총 바이트 수 + 요청 가져오기 + 요청 가져오기 + 헤더 요청 + POST 요청 + 옵션 요청 + 평균 요청 시간(ms) + 평균 수신 요청 시간(ms) + 평균 삭제 요청 시간(ms) + 평균 헤드 요청 시간(ms) + 평균 POST 요청 시간(ms) + 평균 POST 요청 시간(ms) + 평균 요청 시간(ms)	애플리케이션 사용자 에이전트를 기준으로 한 통계입니다. 예를 들어, 사용자 에이전트당 Put/get/delete/head 작업 수와 각 작업의 총 바이트 크기입니다.
X-헤더-데이터	X-NetApp-ASUP-Generated-on+X-NetApp-ASUP-hostname+X-NetApp-ASUP-OS-버전+X-NetApp-ASUP-serial-num+X-NetApp-ASUP-subject+X-NetApp-ASUP-system-id+X-NetApp-ASUP-MODEL-NAME+	AutoSupport 헤더 데이터

AutoSupport를 구성합니다

기본적으로 StorageGRID AutoSupport 기능은 StorageGRID를 처음 설치할 때 활성화됩니다. 그러나 각 어플라이언스에서 하드웨어 AutoSupport을 구성해야 합니다. 필요에 따라 AutoSupport 구성을 변경할 수 있습니다.

StorageGRID AutoSupport의 구성을 변경하려면 기본 관리자 노드에서만 변경하십시오. 반드시 각 제품에 부착해야 하드웨어 AutoSupport를 구성합니다합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.
- AutoSupport 패키지를 보내기 위해 HTTPS를 사용할 경우, 직접 또는 (인바운드 연결 필요 없음) 기본 관리자 노드에 대한 아웃바운드 인터넷 액세스를 제공한 "프록시 서버 사용"것입니다.
- StorageGRID AutoSupport 페이지에서 HTTP를 선택한 경우 AutoSupport 패키지를 HTTPS로 전달해야 "프록시 서버를 구성했습니다"합니다. NetApp의 AutoSupport 서버는 HTTP를 사용하여 전송된 패키지를 거부합니다.
- SMTP를 AutoSupport 패키지의 프로토콜로 사용할 경우 SMTP 메일 서버를 구성한 것입니다.

이 작업에 대해

다음 옵션 중 원하는 옵션을 조합하여 AutoSupport 패키지를 기술 지원으로 보낼 수 있습니다.

- * 매주 *: 매주 AutoSupport 패키지를 자동으로 발송합니다. 기본 설정: 사용.
- * 이벤트 트리거 *: 매 시간마다 또는 중요한 시스템 이벤트가 발생할 때 자동으로 AutoSupport 패키지를 전송합니다. 기본 설정: 사용.
- * 온디맨드 *: 기술 지원 부서에서 StorageGRID 시스템에서 AutoSupport 패키지를 자동으로 보내도록 요청하도록 허용합니다. 이는 문제가 활발하게 발생할 때 유용합니다(HTTPS AutoSupport 전송 프로토콜 필요). 기본 설정: 사용 안 함
- * 사용자 트리거 * : 언제든지 수동으로 AutoSupport 패키지를 보내십시오.

AutoSupport 패키지의 프로토콜을 지정합니다

다음 프로토콜을 사용하여 AutoSupport 패키지를 보낼 수 있습니다.

- * HTTPS *: 새 설치에 대한 기본 권장 설정입니다. 이 프로토콜은 포트 443을 사용합니다. 원하는 경우 AutoSupport 온디맨드 기능을 활성화합니다HTTPS를 사용해야 합니다.
- **HTTP**: HTTP를 선택하는 경우 AutoSupport 패키지를 HTTPS로 전달하도록 프록시 서버를 구성해야 합니다. NetApp의 AutoSupport 서버는 HTTP를 사용하여 전송된 패키지를 거부합니다. 이 프로토콜은 포트 80을 사용합니다.
- **SMTP**: AutoSupport 패키지를 이메일로 보내려면 이 옵션을 사용하십시오.

설정한 프로토콜은 모든 유형의 AutoSupport 패키지를 보내는 데 사용됩니다.

단계

1. 지원 * > * 툴 * > * AutoSupport * > * 설정 * 을 선택합니다.
2. AutoSupport 패키지를 보내는 데 사용할 프로토콜을 선택합니다.
3. HTTPS * 를 선택한 경우 NetApp 지원 인증서(TLS 인증서)를 사용하여 기술 지원 서버에 대한 연결을 보호할지 여부를 선택합니다.
   - * 인증서 확인 * (기본값): AutoSupport 패키지 전송이 안전한지 확인합니다. 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. 모든 주간, 사용자 트리거 및 이벤트 트리거 패키지는 선택한 프로토콜을 사용하여 전송됩니다.

Weekly AutoSupport를 비활성화합니다

기본적으로 StorageGRID 시스템은 일주일에 한 번 AutoSupport 패키지를 기술 지원부로 보내도록 구성되어 있습니다.

주간 AutoSupport 패키지의 전송 시기를 결정하려면 * AutoSupport * > * 결과 * 탭으로 이동하십시오. Weekly AutoSupport * 섹션에서 * 다음 예약 시간 * 의 값을 확인합니다.

언제든지 주간 AutoSupport 패키지의 자동 전송을 비활성화할 수 있습니다.

단계

1. 지원 * > * 툴 * > * AutoSupport * > * 설정 * 을 선택합니다.
2. Weekly AutoSupport * 활성화 확인란의 선택을 취소합니다.
3. 저장 * 을 선택합니다.

이벤트가 트리거된 **AutoSupport**를 비활성화합니다

기본적으로 StorageGRID 시스템은 한 시간마다 AutoSupport 패키지를 기술 지원으로 보내도록 구성되어 있습니다.

이벤트에 의해 트리거되는 AutoSupport는 언제든지 비활성화할 수 있습니다.

단계

1. 지원 * > * 툴 * > * AutoSupport * > * 설정 * 을 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 사용하도록 설정하면 기술 지원 부서에서 StorageGRID 시스템에 AutoSupport 패키지를 자동으로 보내도록 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 * > * 툴 * > * AutoSupport * > * 설정 * 을 선택합니다.
2. 프로토콜에 대해 * HTTPS * 를 선택합니다.
3. Weekly AutoSupport * 활성화 확인란을 선택합니다.
4. AutoSupport On Demand * 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 * > * 툴 * > * AutoSupport * > * 설정 * 을 선택합니다.
2. 소프트웨어 업데이트 확인 * 확인란의 선택을 취소합니다.

3. 저장 * 을 선택합니다.

AutoSupport 대상을 추가합니다

AutoSupport를 활성화하면 상태 패키지와 상태 패키지가 기술 지원으로 전송됩니다. 모든 AutoSupport 패키지에 대해 하나의 추가 대상을 지정할 수 있습니다.

AutoSupport 패키지 전송에 사용되는 프로토콜을 확인하거나 변경하려면 에 있는 지침을 참조하십시오AutoSupport 패키지의 프로토콜을 지정합니다.

SMTP 프로토콜을 사용하여 AutoSupport 패키지를 추가 대상으로 보낼 수 없습니다.

단계

1. 지원 * > * 툴 * > * AutoSupport * > * 설정 * 을 선택합니다.
2. AutoSupport 대상 추가 활성화 * 를 선택합니다.
3. 다음을 지정합니다.

   호스트 이름

   추가 AutoSupport 대상 서버의 서버 호스트 이름 또는 IP 주소입니다.

   하나의 추가 대상만 입력할 수 있습니다.

   포트

   추가 AutoSupport 대상 서버에 연결하는 데 사용되는 포트입니다. 기본값은 HTTP의 경우 포트 80, HTTPS의 경우 포트 443입니다.

   인증서 검증

   TLS 인증서를 사용하여 추가 대상에 대한 연결을 보호할지 여부를 나타냅니다.

   - 인증서 유효성 검사를 사용하려면 * 인증서 확인 * 을 선택합니다.
   - 인증서 확인 없이 AutoSupport 패키지를 보내려면 * 인증서 확인 안 함 * 을 선택합니다.

     인증서에 일시적인 문제가 있는 경우와 같이 인증서 유효성 검사를 사용하지 않는 좋은 이유가 있는 경우에만 이 옵션을 선택합니다.

4. 인증서 확인 * 을 선택한 경우 다음을 수행합니다.
   a. CA 인증서의 위치를 찾습니다.
   b. CA 인증서 파일을 업로드합니다.

      CA 인증서 메타데이터가 나타납니다.

5. 저장 * 을 선택합니다.

   향후의 모든 주간, 이벤트 트리거 및 사용자 트리거 AutoSupport 패키지가 추가 대상으로 전송됩니다.

어플라이언스용 AutoSupport가 StorageGRID 하드웨어 문제를 보고하며 StorageGRID AutoSupport은 StorageGRID 소프트웨어 문제를 보고하지만, SGF6112의 경우 StorageGRID AutoSupport에서 하드웨어 및 소프트웨어 문제를 모두 보고합니다. 추가 구성이 필요하지 않은 SGF6112를 제외하고 각 어플라이언스에서 AutoSupport을 구성해야 합니다. AutoSupport는 서비스 어플라이언스와 스토리지 어플라이언스에 대해 서로 다르게 구현됩니다.

SANtricity를 사용하여 각 스토리지 어플라이언스에 대해 AutoSupport를 사용하도록 설정할 수 있습니다. 초기 어플라이언스 설정 중 또는 어플라이언스 설치 후 SANtricity AutoSupport를 구성할 수 있습니다.

- SG6000 및 SG5700 어플라이언스의 경우, "SANtricity 시스템 관리자에서 AutoSupport를 구성합니다"

에서 AutoSupport 제공을 프록시 구성하는 경우 E-Series 어플라이언스의 AutoSupport 패키지를 StorageGRID AutoSupport에 포함할 수 "SANtricity 시스템 관리자"있습니다.

StorageGRID AutoSupport은 DIMM 또는 HIC(호스트 인터페이스 카드) 오류와 같은 하드웨어 문제를 보고하지 않습니다. 하지만 일부 구성 요소 장애가 트리거될 수 "하드웨어 경고"있습니다. BMC(베이스보드 관리 컨트롤러)가 있는 StorageGRID 어플라이언스의 경우 e-메일 및 SNMP 트랩을 구성하여 하드웨어 오류를 보고할 수 있습니다.

- "BMC 알림에 대한 이메일 알림을 설정합니다"
- "BMC에 대한 SNMP 설정을 구성합니다"

관련 정보

"NetApp 지원"

AutoSupport 패키지를 수동으로 트리거합니다

StorageGRID 시스템 관련 문제 해결에 대한 기술 지원을 지원하기 위해 AutoSupport 패키지를 수동으로 전송할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인해야 "지원되는 웹 브라우저"합니다.
- 루트 액세스 권한 또는 기타 그리드 구성 권한이 있어야 합니다.

단계

1. 지원 * > * 도구 * > * AutoSupport * 를 선택합니다.
2. 작업 * 탭에서 * 사용자 트리거 AutoSupport 전송 * 을 선택합니다.

   StorageGRID에서 NetApp Support 사이트로 AutoSupport 패키지 보내기를 시도합니다. 시도가 성공하면 * Results * 탭의 * Most Recent Result * 및 * Last Successful Time * 값이 업데이트됩니다. 문제가 발생하면 * Most latest result * 값이 "Failed"로 업데이트되고 StorageGRID는 AutoSupport 패키지를 다시 보내지 않습니다.

   사용자가 트리거한 AutoSupport 패키지를 보낸 후 1분 후에 브라우저에서 AutoSupport 페이지를 새로 고쳐 최신 결과에 액세스합니다.

AutoSupport 패키지 문제 해결

AutoSupport 패키지 전송 시도가 실패하면 StorageGRID 시스템은 AutoSupport 패키지

유형에 따라 다른 작업을 수행합니다. AutoSupport 패키지의 상태는 * 지원 * > * 툴 * > * AutoSupport * > * 결과 * 를 선택하여 확인할 수 있습니다.

AutoSupport 패키지를 전송하지 못했으면 * AutoSupport * 페이지의 * 결과 * 탭에 "실패"가 표시됩니다.

> AutoSupport 패키지를 NetApp에 전달하도록 프록시 서버를 구성한 경우"프록시 서버 구성 설정이 올바른지 확인합니다",

주별 **AutoSupport** 패키지 오류

주별 AutoSupport 패키지를 전송하지 못한 경우 StorageGRID 시스템은 다음 작업을 수행합니다.

1. 가장 최근의 결과 속성을 다시 시도하도록 업데이트합니다.
2. AutoSupport 패키지를 1시간 동안 4분마다 15회 재전송합니다.
3. 전송 실패 1시간 후 는 가장 최근의 결과 속성을 실패 로 업데이트합니다.
4. 다음 예약 시간에 AutoSupport 패키지 전송을 다시 시도합니다.
5. NMS 서비스를 이용할 수 없어 패키지가 실패하는 경우, 7일 전에 패키지가 발송되는 경우, AutoSupport 스케줄을 정기적으로 유지
6. NMS 서비스를 다시 사용할 수 있게 되면 는 패키지를 7일 이상 보내지 않은 경우 즉시 AutoSupport 패키지를 보냅니다.

사용자가 트리거하거나 이벤트가 트리거된 **AutoSupport** 패키지 오류입니다

사용자가 트리거하거나 이벤트가 트리거된 AutoSupport 패키지를 전송하지 못하는 경우 StorageGRID 시스템은 다음 작업을 수행합니다.

1. 오류가 알려진 경우 오류 메시지를 표시합니다. 예를 들어, 사용자가 올바른 이메일 구성 설정을 제공하지 않고 SMTP 프로토콜을 선택하면 다음 오류가 표시됩니다. `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. 패키지를 다시 보내지 않습니다.
3. 에 오류를 `nms.log` 기록합니다.

오류가 발생하고 SMTP가 선택한 프로토콜인 경우 StorageGRID 시스템의 이메일 서버가 올바르게 구성되어 있고 이메일 서버가 실행 중인지(* 지원 * > * 알람(레거시) * > * 레거시 이메일 설정 *) 확인하십시오. AutoSupport 페이지에 다음과 같은 오류 메시지가 나타날 수 있습니다. `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

의 방법을 "이메일 서버 설정을 구성합니다"알아보십시오.

AutoSupport 패키지 오류를 해결합니다

오류가 발생하고 SMTP가 선택한 프로토콜인 경우 StorageGRID 시스템의 이메일 서버가 올바르게 구성되어 있고 이메일 서버가 실행 중인지 확인합니다. AutoSupport 페이지에 다음과 같은 오류 메시지가 나타날 수 있습니다. `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

StorageGRID를 통해 **E-Series AutoSupport** 패키지를 전송합니다

E-Series SANtricity System Manager AutoSupport 패키지는 스토리지 어플라이언스의 관리 포트가 아니라 StorageGRID 관리자 노드를 통해 기술 지원으로 보낼 수 있습니다.

E-Series 어플라이언스와 함께 AutoSupport 사용에 대한 자세한 내용은 을 "E-Series 하드웨어 AutoSupport" 참조하십시오.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인됩니다."지원되는 웹 브라우저"
- 이 "스토리지 어플라이언스 관리자 또는 루트 액세스 권한"있습니다.
- SANtricity AutoSupport를 구성했습니다.
  - SG6000 및 SG5700 어플라이언스의 경우, "SANtricity 시스템 관리자에서 AutoSupport를 구성합니다"

> 그리드 관리자를 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 펌웨어 8.70 이상이 있어야 합니다.

이 작업에 대해

E-Series AutoSupport 패키지는 스토리지 하드웨어에 대한 세부 정보를 포함하며 StorageGRID 시스템에서 보내는 다른 AutoSupport 패키지보다 구체적입니다.

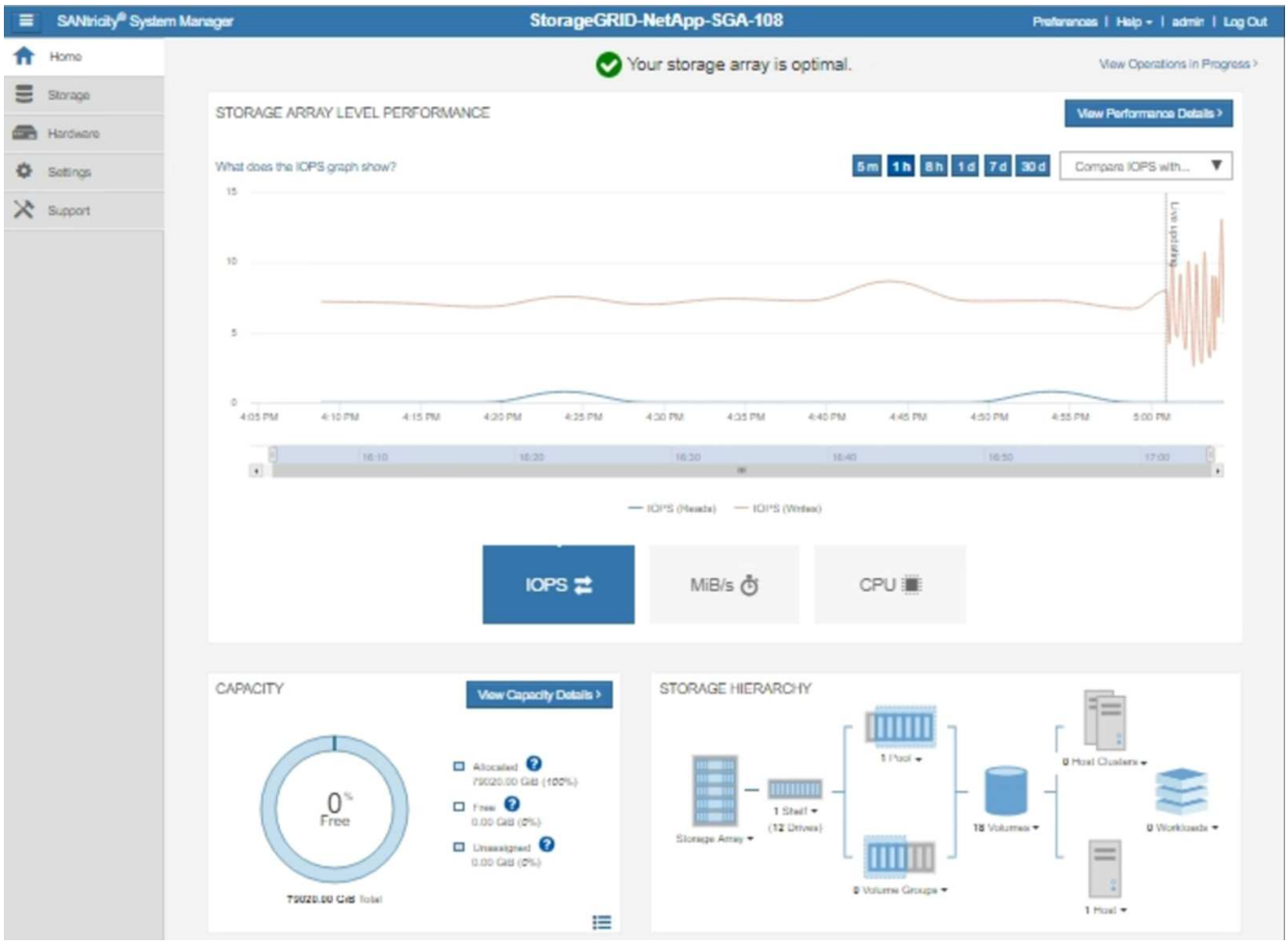
SANtricity 시스템 관리자에서 어플라이언스의 관리 포트를 사용하지 않고 StorageGRID 관리자 노드를 통해 AutoSupport 패키지를 전송하도록 특수 프록시 서버 주소를 구성할 수 있습니다. 이러한 방식으로 전송된 AutoSupport 패키지는 에서 전송하며 "기본 설정 보낸 사람 관리자 노드" "관리자 프록시 설정"그리드 관리자에서 구성된 패키지를 사용합니다.

> 이 절차는 E-Series AutoSupport 패키지용 StorageGRID 프록시 서버를 구성하는 경우에만 적용됩니다. E-Series AutoSupport 구성에 대한 자세한 내용은 을 참조하십시오 "NetApp E-Series 및 SANtricity 문서".

단계

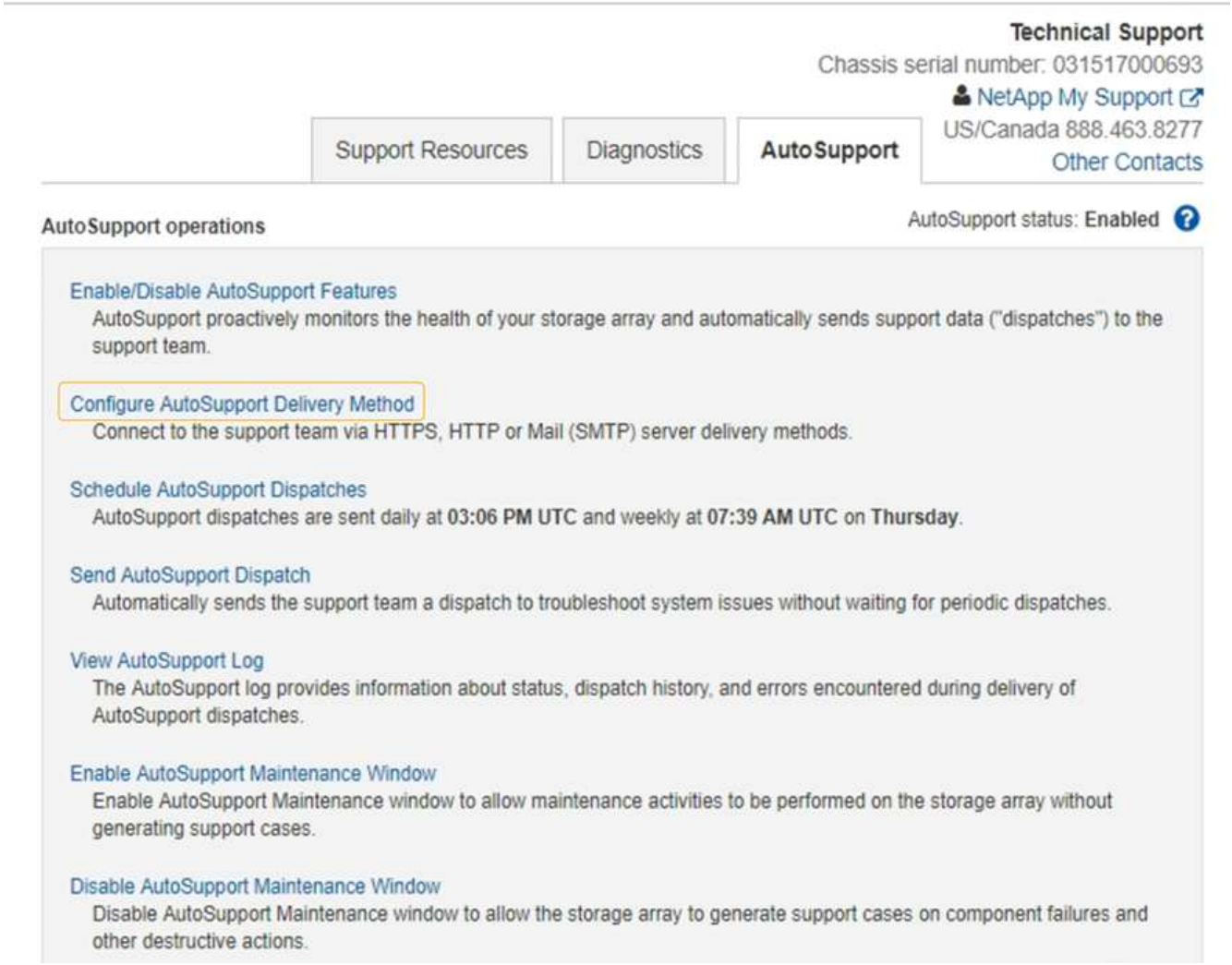
1. Grid Manager에서 * nodes * 를 선택합니다.
2. 왼쪽의 노드 목록에서 구성할 스토리지 어플라이언스 노드를 선택합니다.
3. SANtricity 시스템 관리자 * 를 선택합니다.

   SANtricity 시스템 관리자 홈 페이지가 나타납니다.



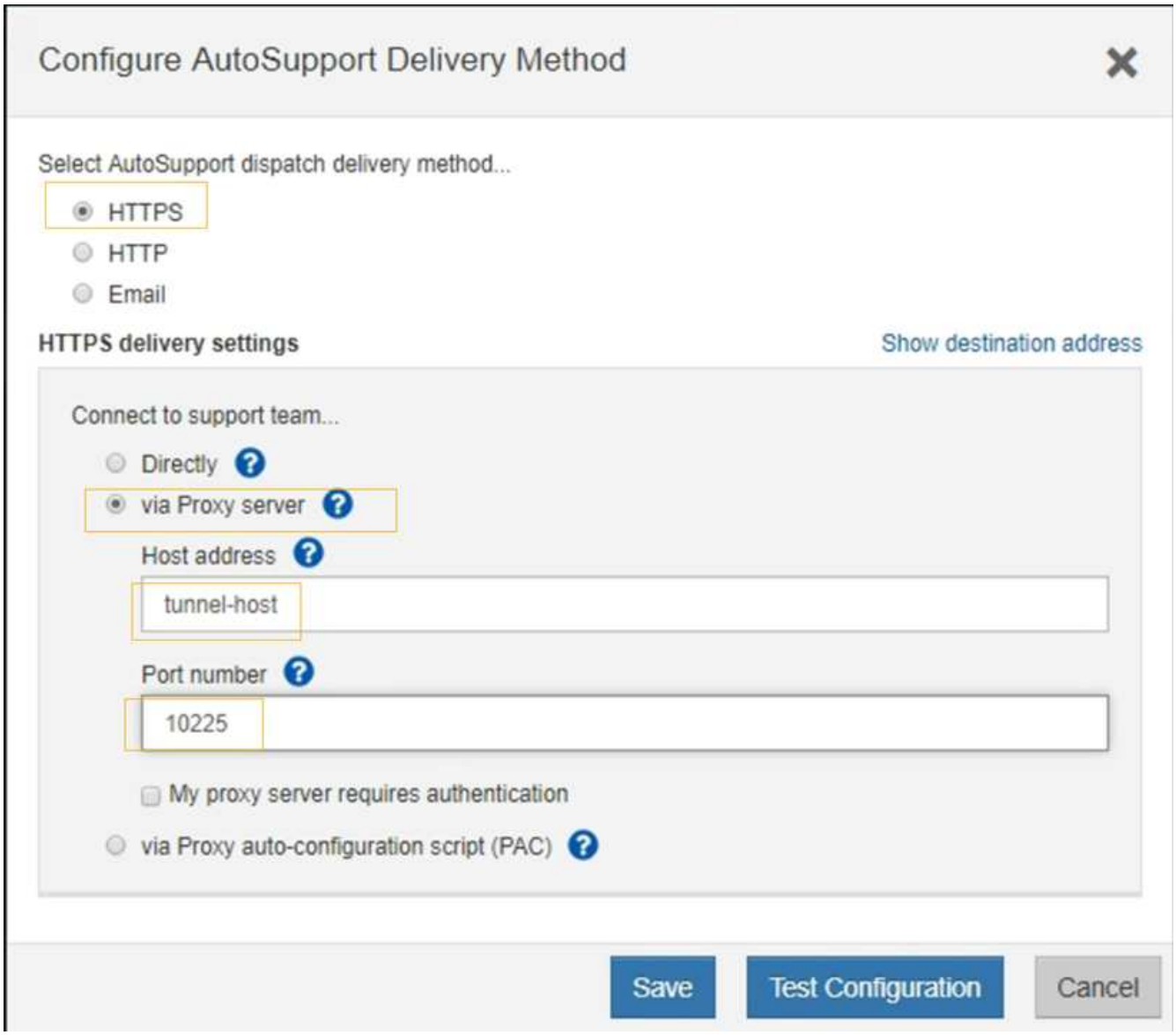
4. 지원 * > * 지원 센터 * > * AutoSupport * 를 선택합니다.

   AutoSupport 작업 페이지가 나타납니다.



5. AutoSupport 제공 방법 구성 * 을 선택합니다.

   AutoSupport 배달 방법 구성 페이지가 나타납니다.



6. 전달 방법으로 * HTTPS * 를 선택합니다.

   HTTPS를 활성화하는 인증서가 미리 설치되어 있습니다.

7. 프록시 서버를 통해 * 를 선택합니다.
8. 호스트 주소 * 에 대해 를 `tunnel-host` 입력합니다.

   `tunnel-host` 은 관리자 노드를 사용하여 E-Series AutoSupport 패키지를 전송하기 위한 특수 주소입니다.

9. 포트 번호 * 에 대해 를 `10225` 입력합니다.

   `10225` 은 어플라이언스의 E-Series 컨트롤러에서 AutoSupport 패키지를 수신하는 StorageGRID 프록시 서버의 포트 번호입니다.

10. AutoSupport 프록시 서버의 라우팅 및 구성을 테스트하려면 * 구성 테스트 * 를 선택합니다.

    올바른 경우 녹색 배너에 "AutoSupport 구성이 확인되었습니다."라는 메시지가 나타납니다.

테스트에 실패하면 빨간색 배너에 오류 메시지가 나타납니다. StorageGRID DNS 설정 및 네트워킹을 확인하고 가 NetApp 지원 사이트에 연결할 수 있는지 "기본 설정 보낸 사람 관리자 노드"확인한 후 테스트를 다시 시도하십시오.

11. 저장 * 을 선택합니다.

    구성이 저장되고 "AutoSupport 배달 방법이 구성되었습니다."라는 확인 메시지가 나타납니다.

스토리지 노드 관리

스토리지 노드 관리

스토리지 노드는 디스크 스토리지 용량 및 서비스를 제공합니다. 스토리지 노드 관리는 다음을 수반합니다.

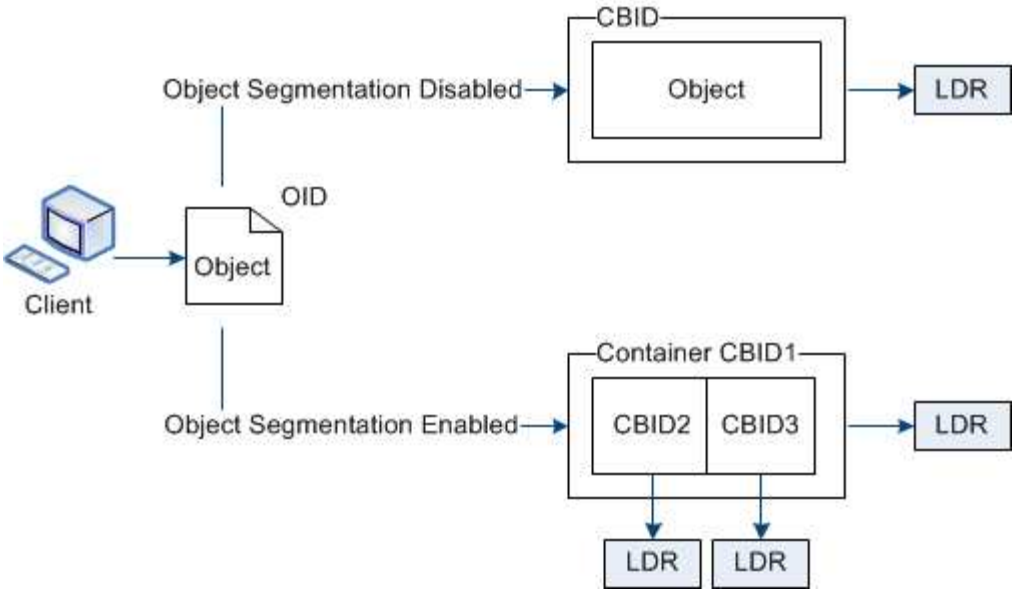
- 스토리지 옵션 관리
- 스토리지 볼륨 워터마크의 정의 및 워터마크 덮어쓰기를 사용하여 스토리지 노드가 읽기 전용이 되는 시점을 제어하는 방법을 이해합니다
- 오브젝트 메타데이터에 사용되는 공간 모니터링 및 관리
- 저장된 개체에 대한 전역 설정 구성
- 스토리지 노드 구성 설정을 적용하는 중입니다
- 전체 스토리지 노드 관리

스토리지 옵션을 사용합니다

객체 분할이란 무엇입니까**?**

객체 분할은 객체를 더 작은 고정 크기 객체 컬렉션으로 분할하여 큰 객체에 대한 스토리지 및 리소스 사용을 최적화하는 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.

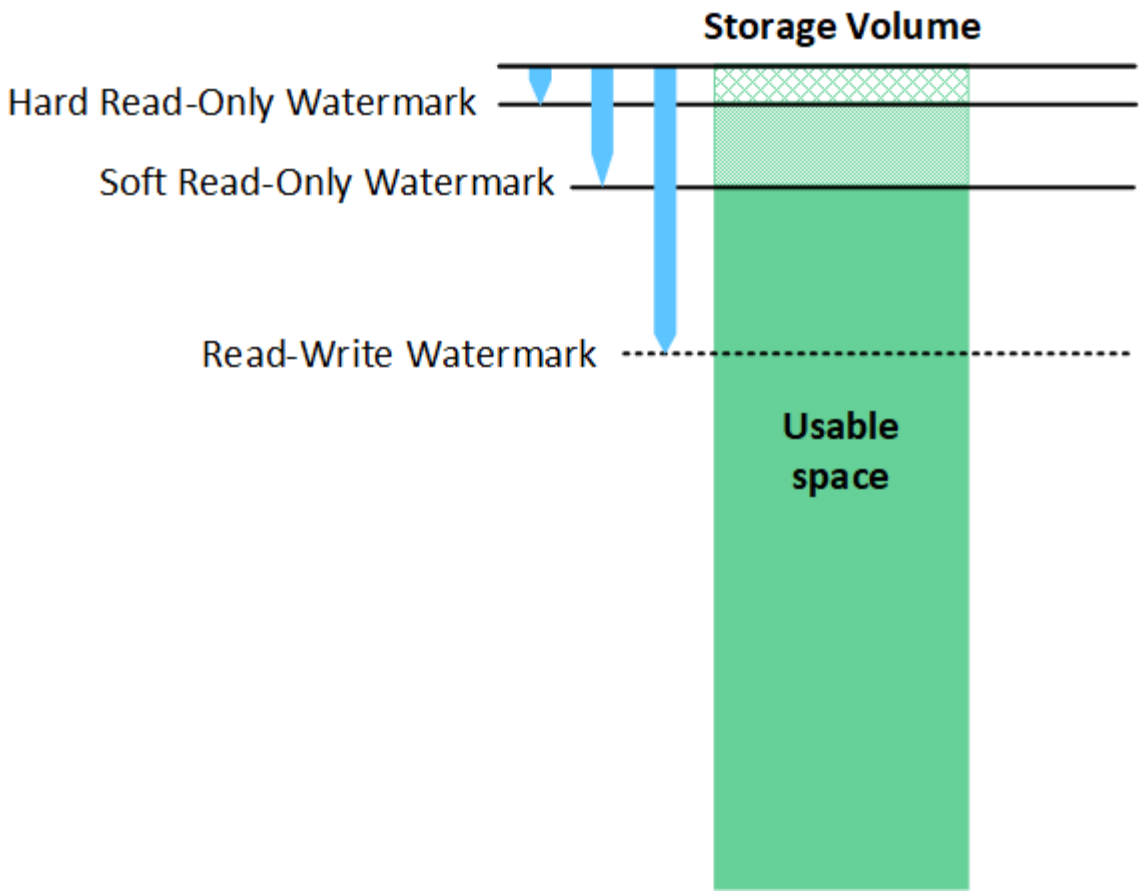
컨테이너와 세그먼트가 반드시 동일한 스토리지 노드에 저장되지는 않습니다. 컨테이너 및 세그먼트는 ILM 규칙에 지정된 스토리지 풀 내의 모든 스토리지 노드에 저장할 수 있습니다.

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.

```
segment container + segment 1 + segment 2 = three stored objects
```

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 메타데이터용으로 예약된 공간에 대한 자세한 내용은 을 참조하십시오"오브젝트 메타데이터 스토리지 관리".

소프트 읽기 전용 워터마크란 무엇입니까?

스토리지 볼륨 소프트 읽기 전용 워터마크 * 는 객체 데이터에 대한 스토리지 노드의 가용 공간이 가득 차있음을 나타내는 첫 번째 워터마크입니다.

스토리지 노드의 각 볼륨에 사용 가능한 공간이 해당 볼륨의 소프트 읽기 전용 워터마크보다 적은 경우 스토리지 노드는 _READ-ONLY MODE_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 워터마크란 무엇입니까?

스토리지 볼륨 하드 읽기 전용 워터마크 * 는 오브젝트 데이터에 대한 노드의 사용 가능한 공간이 가득 차있음을 나타내는 다음 워터마크입니다.

볼륨의 여유 공간이 해당 볼륨의 하드 읽기 전용 워터마크보다 작으면 볼륨에 대한 쓰기가 실패합니다. 그러나 다른 볼륨에 대한 쓰기는 해당 볼륨의 여유 공간이 하드 읽기 전용 워터마크보다 작아질 때까지 계속될 수 있습니다.

예를 들어 스토리지 노드의 각 볼륨에 하드 읽기 전용 워터마크가 5GB라고 가정합니다. 각 볼륨의 사용 가능한 공간이 5GB 미만이면 스토리지 노드가 더 이상 쓰기 요청을 수락하지 않습니다.

하드 읽기 전용 워터마크는 항상 소프트 읽기 전용 워터마크보다 작습니다.

읽기-쓰기 워터마크란 무엇입니까?

스토리지 볼륨 읽기/쓰기 워터마크 * 는 읽기 전용 모드로 전환된 스토리지 노드에만 적용됩니다. 노드가 다시 읽기-쓰기가 될 수 있는 시기를 결정합니다. 스토리지 노드에 있는 스토리지 볼륨 중 하나의 사용 가능한 공간이 해당 볼륨의 읽기-쓰기 워터마크보다 크면 노드는 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 워터마크는 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.

시작하기 전에

- StorageGRID 11.6 이상으로 업그레이드를 완료했습니다.
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.

현재 워터마크 설정을 봅니다

그리드 관리자에서 현재 스토리지 워터마크 설정을 볼 수 있습니다.

단계

1. support * > * 기타 * > * 스토리지 워터마크 * 를 선택합니다.
2. 스토리지 워터마크 페이지에서 최적화된 값 사용 확인란을 확인합니다.
   - 이 확인란을 선택하면 스토리지 노드의 크기와 볼륨의 상대적 용량에 따라 모든 스토리지 노드의 모든 스토리지 볼륨에 대해 세 개의 워터마크가 모두 최적화됩니다.

     이 설정이 기본값이며 권장 설정입니다. 이 값을 업데이트하지 마십시오. 선택적으로, 할 수 최적화된 스토리지 워터마크를 봅니다있습니다.
   - 최적화된 값 사용 확인란이 선택되어 있지 않으면 사용자 지정(최적화되지 않은) 워터마크가 사용됩니다. 사용자 지정 배경무늬 설정은 사용하지 않는 것이 좋습니다. 의 지침에 "낮은 읽기 전용 배경무늬 재정의 알림 문제 해결"따라 설정을 조정할 수 있는지 또는 조정할 수 있는지 결정합니다.

     사용자 지정 워터마크 설정을 지정할 때는 0보다 큰 값을 입력해야 합니다.

최적화된 스토리지 워터마크를 봅니다

StorageGRID는 두 가지 Prometheus 메트릭을 사용하여 스토리지 볼륨 소프트 읽기 전용 워터마크에 대해 계산된 최적화된 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.

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   마지막 열에는 각 스토리지 노드의 모든 스토리지 볼륨에 대한 소프트 읽기 전용 워터마크의 최소화된 값이 표시됩니다. 이 값이 스토리지 볼륨 소프트 읽기 전용 워터마크에 대한 사용자 지정 설정보다 크면 스토리지 노드에 대해 * 낮은 읽기 전용 워터마크 무시 * 경고가 트리거됩니다.

4. 권장되는 최대 소프트 읽기 전용 워터마크를 보려면 다음 Prometheus 메트릭을 입력하고 * Execute * 를 선택합니다.

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   마지막 열에는 각 스토리지 노드의 모든 스토리지 볼륨에 대한 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.

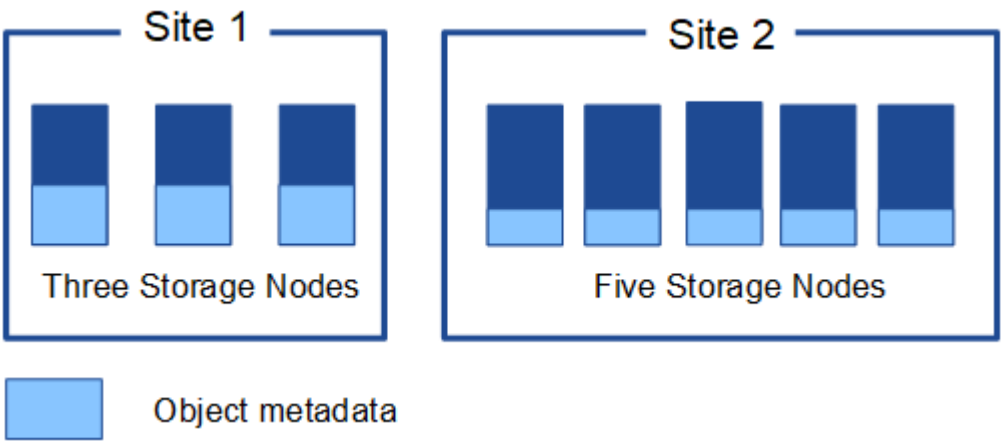
- 각 오브젝트의 고유 ID(UUID), 오브젝트 이름, S3 버킷의 이름, 테넌트 계정 이름 또는 ID, 오브젝트의 논리적 크기, 오브젝트를 처음 생성한 날짜와 시간, 오브젝트를 마지막으로 수정한 날짜와 시간이 포함된 시스템 메타데이터
- 객체와 연결된 모든 사용자 메타데이터 키 값 쌍입니다.
- S3 오브젝트의 경우 오브젝트와 연결된 오브젝트 태그 키 값 쌍이 됩니다.
- 복제된 오브젝트 복사본의 경우 각 복제본의 현재 스토리지 위치입니다.
- 삭제 코딩 오브젝트 복사본의 경우 각 분절의 현재 스토리지 위치입니다.
- 클라우드 스토리지 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 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.

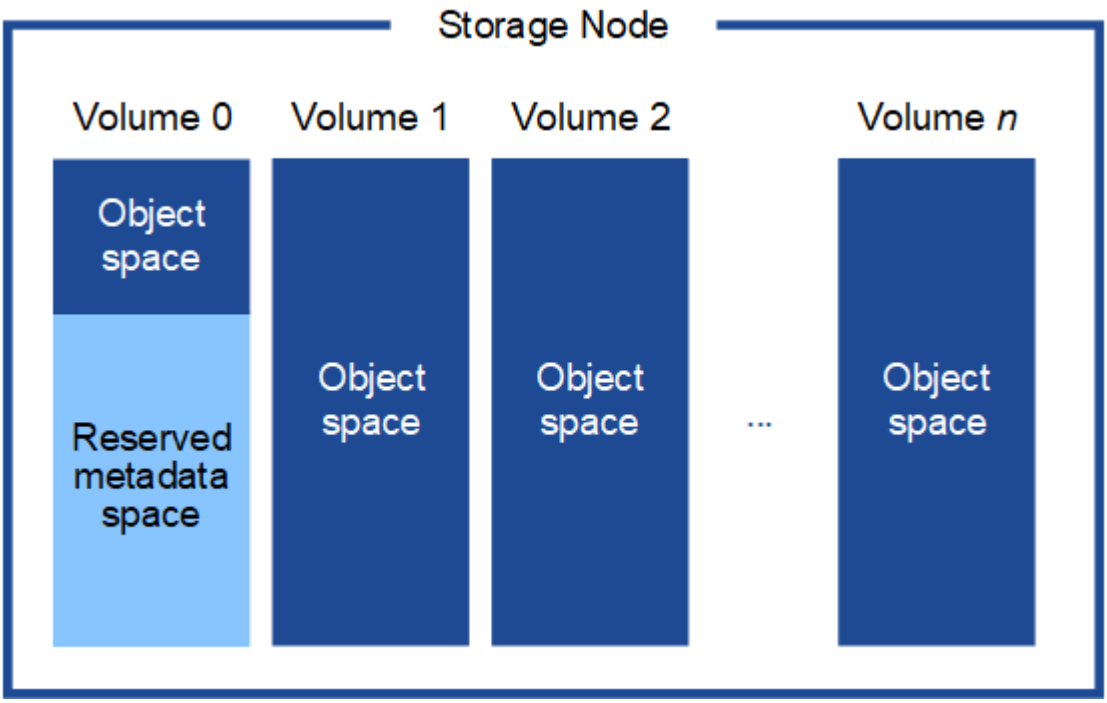
이 그림은 두 사이트의 스토리지 노드를 나타냅니다. 각 사이트에는 동일한 양의 오브젝트 메타데이터가 있으며 각

사이트의 메타데이터는 해당 사이트의 모든 스토리지 노드 간에 세분됩니다.



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 노드의 개체 메타데이터에 예약된 공간의 양은 아래에 설명된 여러 요인에 따라 달라집니다.

메타데이터 예약 공간 설정입니다

Metadata Reserved space_는 모든 스토리지 노드의 볼륨 0에서 메타데이터로 예약될 공간의 양을 나타내는 시스템 차원의 설정입니다. 표에 나와 있는 것처럼 이 설정의 기본값은 다음을 기반으로 합니다.

- StorageGRID를 처음 설치할 때 사용한 소프트웨어 버전입니다.
- 각 스토리지 노드의 RAM 용량입니다.

초기 **StorageGRID** 설치에 사용되는 버전입니다	스토리지 노드의 **RAM** 크기입니다	기본 메타데이터 예약 공간 설정입니다
11.5 - 11.9	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)

메타데이터 예약 공간 설정을 봅니다

StorageGRID 시스템의 메타데이터 예약 공간 설정을 보려면 다음 단계를 수행하십시오.

단계

1. 구성 * > * 시스템 * > * 스토리지 설정 * 을 선택합니다.
2. 저장소 설정 페이지에서 * 메타데이터 예약 공간 * 섹션을 확장합니다.

StorageGRID 11.8 이상의 경우 메타데이터 예약 공간 값은 100GB 이상 1PB 이하여야 합니다.

각 스토리지 노드에 128GB 이상의 RAM이 있는 새로운 StorageGRID 11.6 이상 설치의 기본 설정은 8,000GB(8TB)입니다.

메타데이터의 실제 예약 공간입니다

시스템 차원 메타데이터 예약 공간 설정과 달리 각 스토리지 노드에 대해 _actual reserved space_for object 메타데이터가 결정됩니다. 지정된 스토리지 노드에 대해 메타데이터의 실제 예약된 공간은 노드의 볼륨 0 크기 및 시스템 차원의 메타데이터 예약 공간 설정에 따라 달라집니다.

노드에 대한 볼륨 **0**의 크기입니다	메타데이터의 실제 예약 공간입니다
500GB 미만(비운영 용도)	볼륨 0의 10%

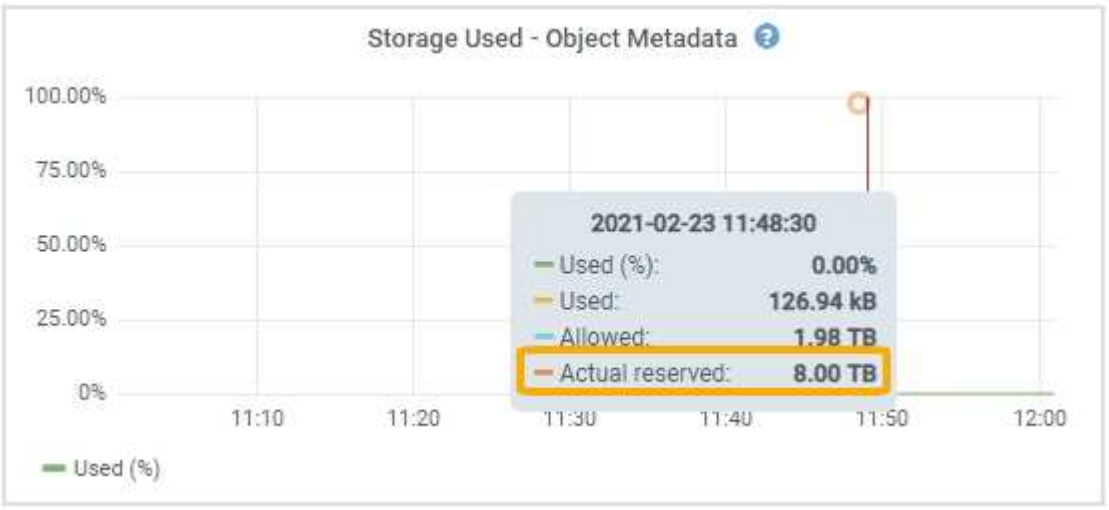
노드에 대한 볼륨 **0**의 크기입니다	메타데이터의 실제 예약 공간입니다
500GB 이상 + 또는 + 메타데이터 전용 스토리지 노드	다음 값 중 더 작은 값: • 볼륨 0 • 메타데이터 예약 공간 설정입니다 • 참고 *: 메타데이터 전용 스토리지 노드에는 하나의 rangedb만 필요합니다.

메타데이터에 대한 실제 예약 공간을 봅니다

특정 스토리지 노드의 메타데이터에 대한 실제 예약 공간을 보려면 다음 단계를 따르십시오.

단계

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.



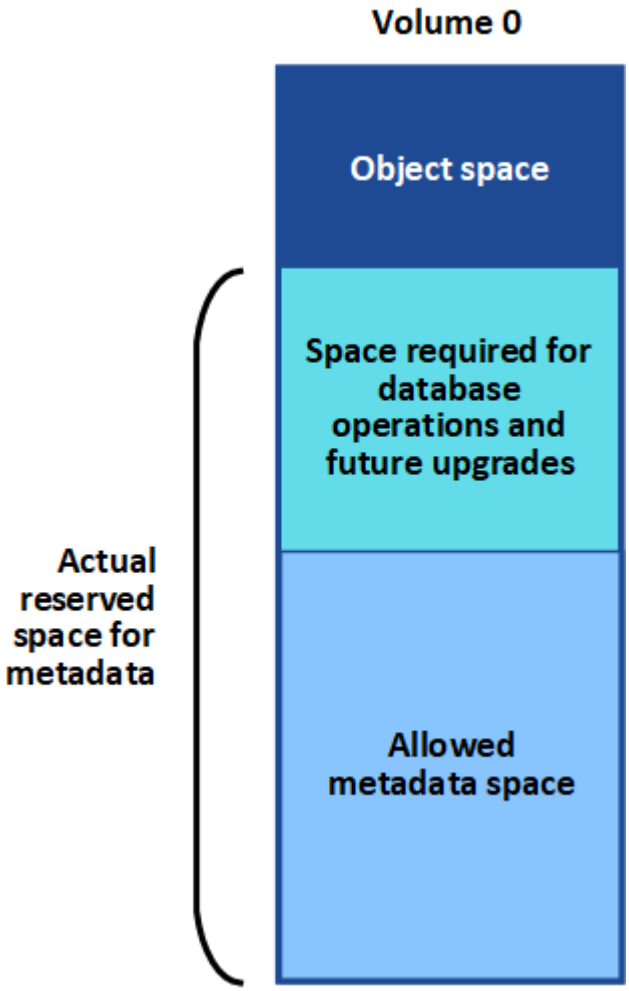
스크린샷에서 * Actual Reserved * 값은 8TB입니다. 이 스크린샷은 새 StorageGRID 11.6 설치의 대규모 스토리지 노드에 대한 것입니다. 이 스토리지 노드의 시스템 차원 메타데이터 예약 공간 설정이 볼륨 0보다 작기 때문에 이 노드의 실제 예약 공간은 메타데이터 예약 공간 설정과 같습니다.

실제 예약 메타데이터 공간의 예

버전 11.7 이상을 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 * 이 8TB로 설정되어 있습니다. (각 스토리지 노드에 128GB RAM이 넘는 경우 새 StorageGRID 11.6 이상 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.

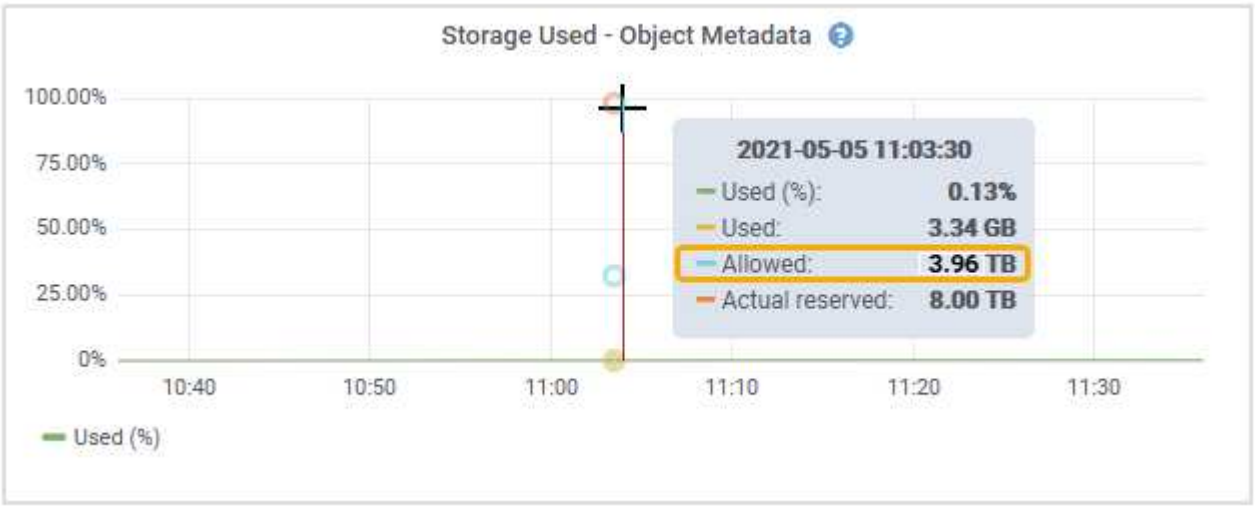
		• 스토리지 노드의 메모리 양 *	
	lt; 128GB(&L)	GT; = 128GB(&G	• 메타데이터에 대한 실제 예약 공간 *
lt; = 4 TB.(&L	메타데이터를 위해 실제 예약된 공간의 60%, 최대 1.32TB	메타데이터를 위해 실제 예약된 공간의 60%, 최대 1.98TB	GT, 4TB(&G

허용된 메타데이터 공간을 봅니다

스토리지 노드에 대해 허용되는 메타데이터 공간을 보려면 다음 단계를 따르십시오.

단계

1. Grid Manager에서 * nodes * 를 선택합니다.
2. 스토리지 노드를 선택합니다.
3. Storage * 탭을 선택합니다.
4. 커서를 Storage Used-object 메타데이터 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.

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

허용되는 메타데이터 공간의 예

버전 11.6를 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 * 이 8TB로 설정되어 있습니다. (각 스토리지 노드에 128GB RAM이 넘는 경우 StorageGRID 11.6 이상의 기본값입니다.)
- SN1의 메타데이터에 대한 실제 예약 공간은 6TB입니다. (볼륨 0이 * Metadata Reserved space * 설정보다 작기 때문에 전체 볼륨이 예약됩니다.)
- SN1의 메타데이터에 허용되는 공간은 3TB이며메타데이터에 허용되는 공간에 대한 테이블입니다, 이 계산 결과는 메타데이터 -1TB의 실제 예약된 공간) × 60%(최대 3.96TB)입니다.

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

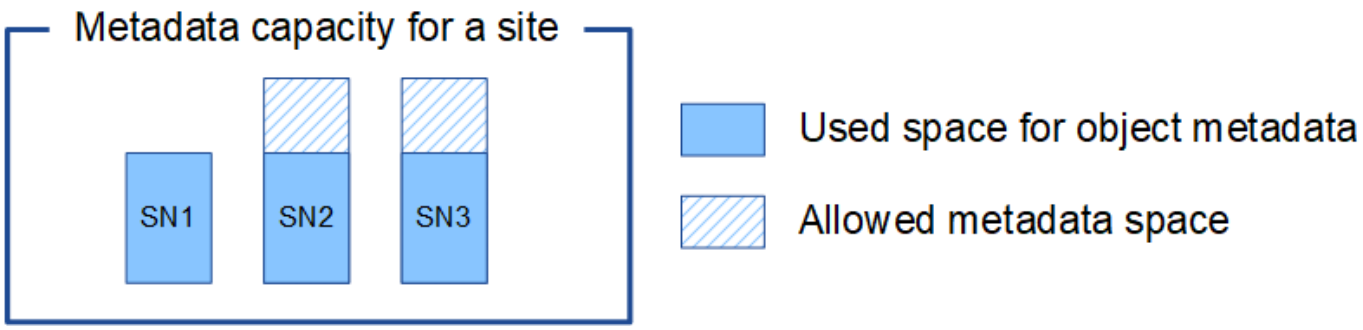
결정합니다.

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 0의 크기입니다	실제 예약된 메타데이터 공간입니다	허용된 메타데이터 공간입니다
SN1을 참조하십시오	2.2TB	2.2TB	1.32TB
에스엔2	5TB	4TB	1.98TB
SN3을 참조하십시오	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 오브젝트 메타데이터 용량을 모니터링하는 방법은 의 지침을 참조하십시오."StorageGRID 모니터링"
- 새 스토리지 노드를 추가하여 시스템의 오브젝트 메타데이터 용량을 "그리드를 확장합니다"늘립니다.

메타데이터 예약 공간 증가 설정을 사용합니다

스토리지 노드가 RAM 및 사용 가능한 공간에 대한 특정 요구 사항을 충족할 경우 메타데이터 예약 공간 시스템 설정을 늘릴 수 있습니다.

필요한 것

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"

- 이 "루트 액세스 권한 또는 그리드 토폴로지 페이지 구성 및 기타 그리드 구성 권한"있습니다.

> 그리드 토폴로지 페이지는 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다.

이 작업에 대해

시스템 전체의 메타데이터 예약 공간 설정을 수동으로 최대 8TB까지 늘릴 수 있습니다.

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 노드에서 개체 메타데이터 저장소에 허용되는 공간에 미치는 영향에 대한 자세한 설명은 을 참조하십시오."오브젝트 메타데이터 스토리지 관리"

단계

1. 현재 메타데이터 예약 공간 설정을 확인합니다.
   a. 구성 * > * 시스템 * > * 스토리지 옵션 * 을 선택합니다.
   b. 스토리지 워터마크 섹션에서 * Metadata Reserved Space * 의 값을 확인합니다.
2. 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.
3. 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.

4. 메타데이터 예약 공간 설정을 업데이트합니다.

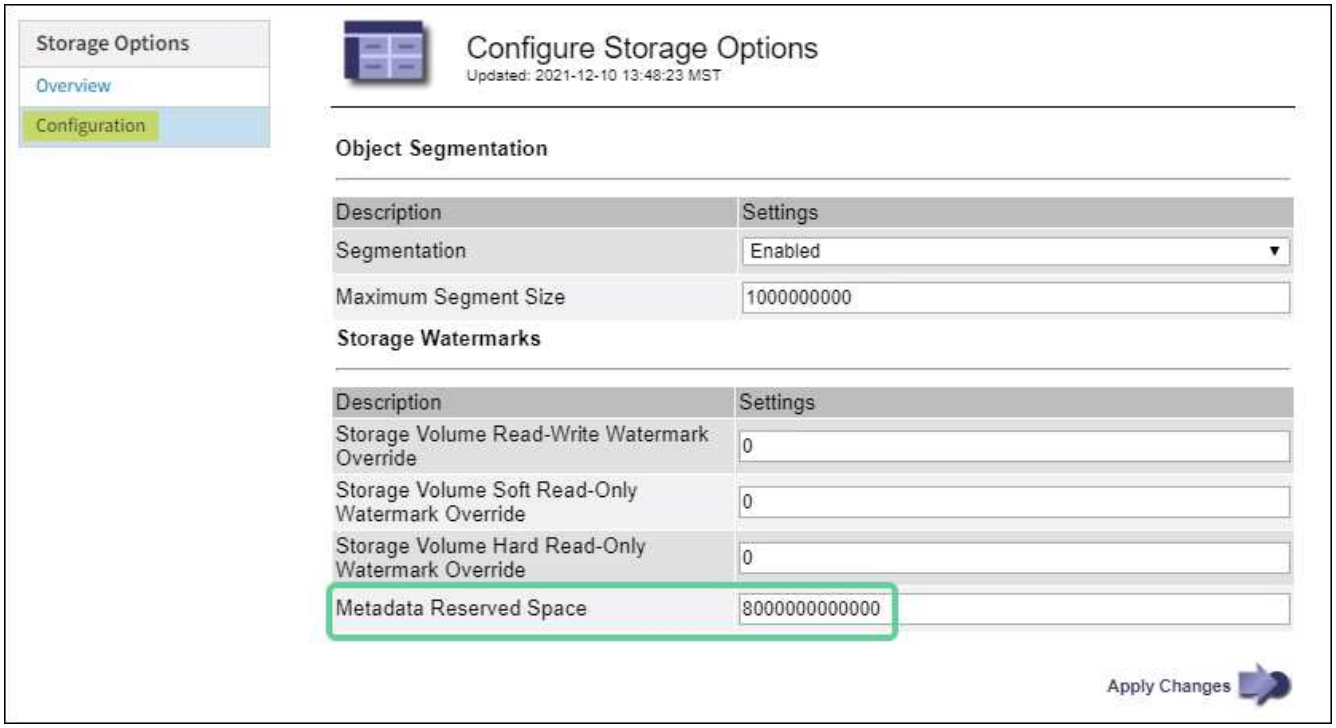
a. 구성 * > * 시스템 * > * 스토리지 옵션 * 을 선택합니다.

b. 구성 탭을 선택합니다.

c. 스토리지 워터마크 섹션에서 * 메타데이터 예약 공간 * 을 선택합니다.

d. 새 값을 입력합니다.

예를 들어, 지원되는 최대 값인 8TB를 입력하려면 * 8000000000000 * (8, 0이 12개 있음)을 입력합니다.



a. Apply Changes * 를 선택합니다.

저장된 객체를 압축합니다

오브젝트 압축을 활성화하여 StorageGRID에 저장된 오브젝트 크기를 줄일 수 있으므로 오브젝트가 더 적은 스토리지를 소비하도록 할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"

- 있습니다. "특정 액세스 권한"

이 작업에 대해

기본적으로 오브젝트 압축은 비활성화되어 있습니다. 압축을 설정하면 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.

오브젝트 압축을 설정하기 전에 다음 사항을 숙지하십시오.

- 저장 중인 데이터가 압축될 수 있다는 것을 모를 경우 * Compress stored objects * 를 선택하면 안 됩니다.
- 개체를 StorageGRID에 저장하는 응용 프로그램은 개체를 저장하기 전에 압축할 수 있습니다. 클라이언트 응용 프로그램이 개체를 StorageGRID에 저장하기 전에 이미 압축한 경우 이 옵션을 선택하면 개체의 크기가 더 작아지지 않습니다.
- StorageGRID에서 NetApp FabricPool를 사용하는 경우 * 저장된 오브젝트 압축 * 을 선택하지 마십시오.
- 저장된 개체 압축 * 을 선택하면 S3 클라이언트 응용 프로그램에서 반환되는 바이트 범위를 지정하는 GetObject 작업을 수행하지 않도록 해야 합니다. 이러한 "범위 읽기" 작업은 StorageGRID에서 요청된 바이트에 액세스하기 위해 개체의 압축을 효과적으로 해제해야 하기 때문에 비효율적입니다. 매우 큰 개체에서 작은 범위의 바이트를 요청하는 GetObject 작업은 특히 비효율적입니다. 예를 들어, 50GB의 압축된 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. Select * 구성 * > * 시스템 * > * 스토리지 설정 * > * 오브젝트 압축 * 을 선택합니다.
2. 저장된 객체 압축 * 확인란을 선택합니다.
3. 저장 * 을 선택합니다.

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 "StorageGRID 시스템 확장"참조하십시오.

스토리지 확장 쉘프를 추가합니다

SG6060 또는 SG6160 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 "StorageGRID 시스템 확장"참조하십시오.

스토리지 노드 추가

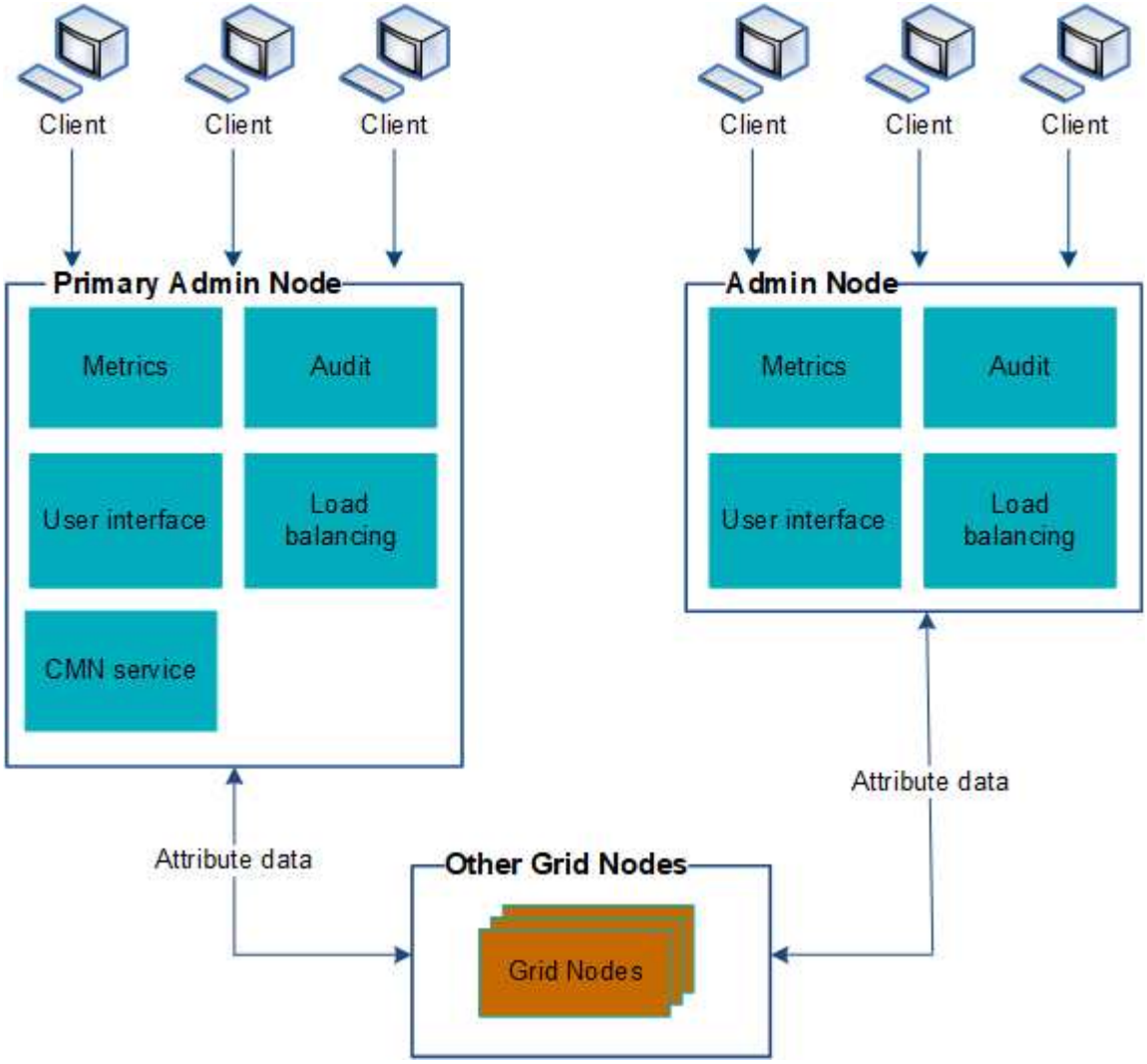
스토리지 노드를 추가하여 스토리지 용량을 늘릴 수 있습니다. 스토리지를 추가할 때 현재 활성 상태인 ILM 규칙 및 용량 요구 사항을 신중하게 고려해야 합니다. 의 지침을 "StorageGRID 시스템 확장"참조하십시오.

관리 노드 관리

여러 관리자 노드 사용

StorageGRID 시스템에는 여러 관리 노드가 포함되어 있어 하나의 관리 노드에 장애가 발생하더라도 StorageGRID 시스템을 지속적으로 모니터링하고 구성할 수 있습니다.

관리자 노드를 사용할 수 없게 되면 속성 처리가 계속되고 알림이 계속 트리거되며 이메일 알림 및 AutoSupport 패키지가 계속 전송됩니다. 그러나 관리 노드가 여러 개인 경우에는 알림 및 AutoSupport 패키지를 제외한 페일오버 보호 기능을 제공하지 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 "고가용성 그룹을 관리합니다"참조하십시오.

> HA 그룹을 사용하는 경우 활성 관리 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 관리자 노드는 비기본 관리자 노드보다 더 많은 기능을 제공합니다. 예를 들어, 일부 유지 보수 절차는 기본 관리자 노드를 사용하여 수행해야 합니다.

관리 노드에 대한 자세한 내용은 을 참조하십시오"관리자 노드란 무엇입니까".

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

단계

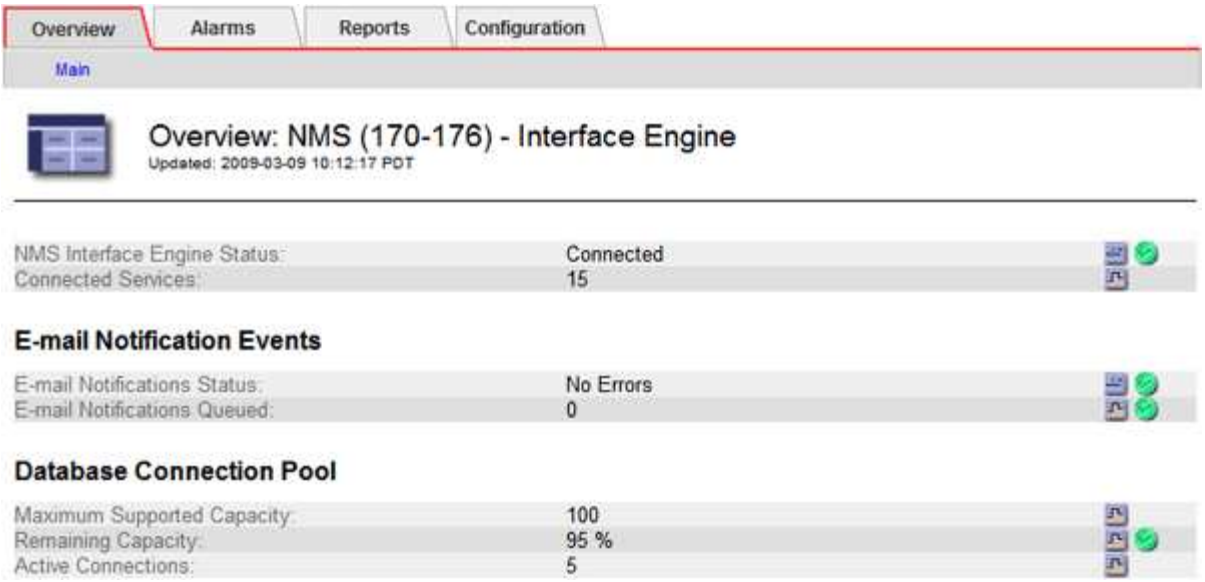
1. 노드 * 를 선택합니다.
2. 검색 상자에 * primary * 를 입력합니다.

   검색 결과에서 유형 열에 "기본 관리자 노드"가 표시된 노드를 확인합니다. 하나의 기본 관리자 노드가 나열되어야 합니다.

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. 그런 다음 **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.

ILM을 사용하여 개체를 관리합니다

ILM을 사용하여 개체를 관리합니다

ILM 정책의 정보 라이프사이클 관리(ILM) 규칙은 오브젝트 데이터의 복사본을 생성 및 배포하는 방법과 시간이 지남에 따라 복사본을 관리하는 방법을 StorageGRID에 안내합니다.

참조하십시오

ILM 규칙 및 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.

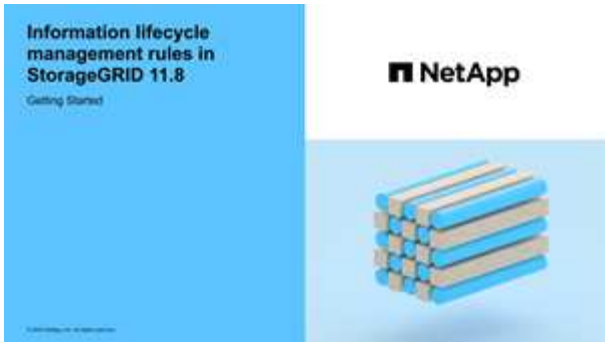
다음 지침을 따르십시오.

- 을 포함하여 StorageGRID ILM에 대해 "ILM이 개체 수명 전반에 걸쳐 작동하는 방식"알아보십시오.
- "지원합니다", "클라우드 스토리지 풀"및 를 구성하는 방법에 대해 "ILM 규칙"알아봅니다.
- 이를 통해 하나 이상의 사이트에서 오브젝트 데이터를 보호하는 방법에 대해 "ILM 정책을 생성, 시뮬레이션 및 활성화합니다"알아보십시오.
- "S3 오브젝트 잠금으로 오브젝트 관리"특정 S3 버킷의 객체가 지정된 시간 동안 삭제되거나 덮어쓰지 않도록 하는 방법에 대해 알아봅니다.

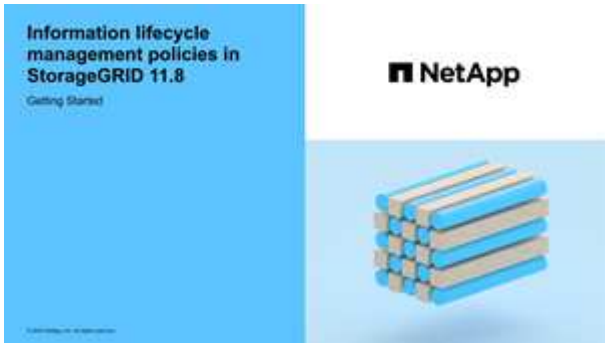
자세한 정보

자세한 내용은 다음 비디오를 참조하십시오.

- "비디오: ILM 규칙 개요"..



- "비디오: ILM 정책 개요"



ILM 및 오브젝트 라이프사이클

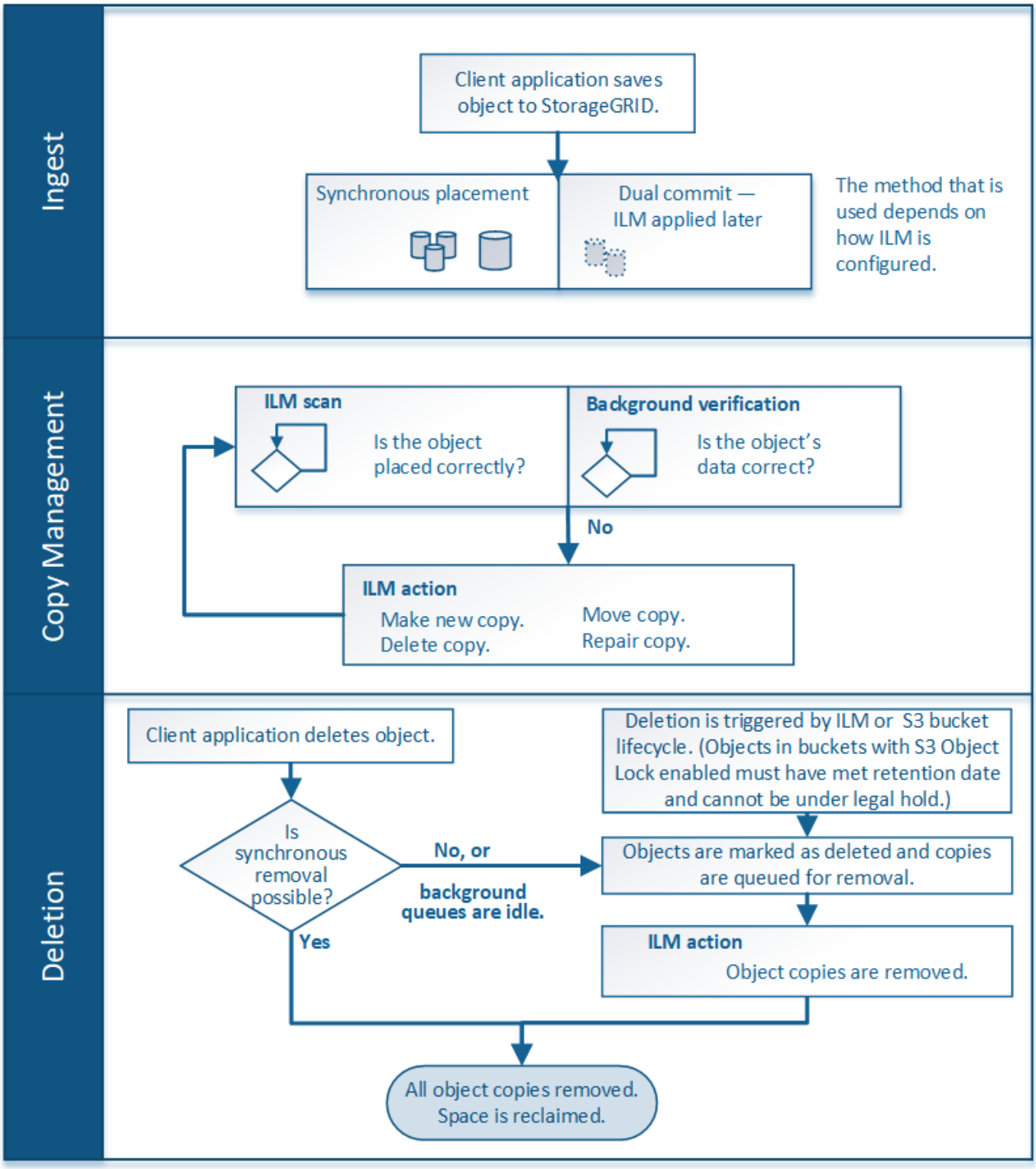
ILM이 개체 수명 전반에 걸쳐 작동하는 방식

StorageGRID에서 ILM을 사용하여 삶의 모든 단계에서 개체를 관리하는 방법을 이해하면 더 효과적인 정책을 설계하는 데 도움이 됩니다.

- * Ingest *: Ingest는 S3 클라이언트 응용 프로그램이 StorageGRID 시스템에 개체를 저장하기 위한 연결을 설정할 때 시작되며 StorageGRID가 클라이언트에 "수집 성공" 메시지를 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 *: StorageGRID는 그리드에 저장된 객체 목록을 지속적으로 검사하고 현재 복사본이 ILM 요구 사항을 충족하는지 확인합니다. 오브젝트 복사본의 유형, 숫자 또는 위치가 서로 다른 경우 StorageGRID은 필요에 따라 복사본을 생성, 삭제 또는 이동합니다.
  - * 배경 검증 * : StorageGRID는 객체 데이터의 무결성을 확인하기 위해 지속적으로 백그라운드 검증을 수행합니다. 문제가 발견되면 StorageGRID는 현재 ILM 요구사항을 충족하는 위치에 새 오브젝트 복사본 또는 삭제 코딩 된 대체 오브젝트 조각을 자동으로 생성합니다. 을 "개체 무결성을 확인합니다"참조하십시오.
- * 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

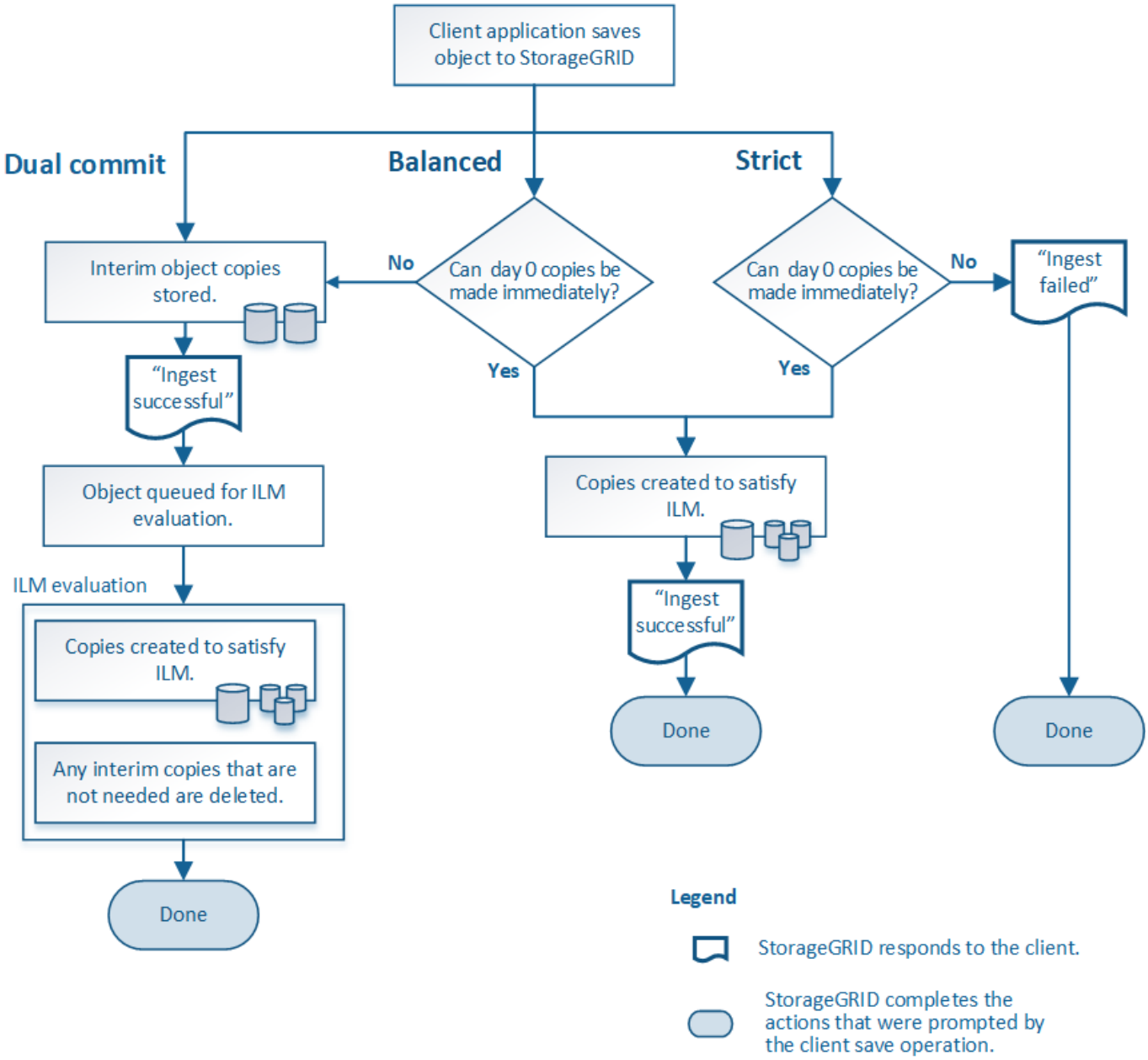
수집 옵션

ILM 규칙을 생성할 때 수집 시 개체를 보호하기 위한 세 가지 옵션 중 하나인 이중 커밋, Strict 또는 균형 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 옵션의 흐름도

이 순서도는 세 가지 수집 옵션 각각을 사용하는 ILM 규칙에 따라 오브젝트가 일치할 때 발생하는 상황을 보여 줍니다.



이중 커밋

Dual Commit 옵션을 선택하면 StorageGRID는 즉시 서로 다른 두 스토리지 노드에 임시 객체 복사본을 만들고 "ingest successful" 메시지를 클라이언트에 반환합니다. 개체는 ILM 평가를 위해 대기하며 규칙의 배치 지침을 충족하는 복사본은 나중에 만들어집니다. 이중 커밋 후 ILM 정책을 즉시 처리할 수 없는 경우 사이트 손실 보호를 달성하는 데 시간이 걸릴 수 있습니다.

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 ILM을 충족하지 못하는 경우 그리드에서 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.

균형(기본값)

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 없는 경우에는 Dual commit 을 대신 사용합니다. ILM 정책이 여러 사이트의 배치를 사용하고 즉각적인 사이트 손실 방지를 달성할 수 없는 경우 * ILM 배치 불가능 * 경고가 트리거됩니다.

균형 옵션을 사용하면 데이터 보호, 그리드 성능 및 수집 성공을 최적으로 조합하여 달성할 수 있습니다. ILM 규칙 만들기 마법사의 기본 옵션은 균형 조정입니다.

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.

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.

을 "예 5: 엄격한 수집 동작을 위한 ILM 규칙 및 정책"참조하십시오.

수집 옵션의 장점, 단점 및 제한 사항

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.

수집 옵션에 대한 개요는 를 참조하십시오"수집 옵션".

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 커밋 사용에 대한 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 또는 Strict 옵션을 사용하는 경우 삭제 코딩 단편이나 복제된 복제본이 모두 생성 및 저장될 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 수집이 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 ILM이 수집되는 개체의 각 부분에 대해 계산되고, 멀티파트 업로드가 완료되면 개체 전체에 대해 평가됩니다. 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 개체에 대한 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 오브젝트 위치는 즉시 변경되지 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 및 엄격 옵션을 사용한 개체 배치 제한

다음 배치 지침이 있는 ILM 규칙에는 균형 또는 엄격 옵션을 사용할 수 없습니다.

- 0일에 클라우드 스토리지 풀에 배치.
- 규칙에 사용자 정의 생성 시간이 레퍼런스 시간으로 설정된 경우의 클라우드 스토리지 풀 배치

이러한 제한 사항은 StorageGRID가 클라우드 스토리지 풀에 대한 복제본을 동기식으로 만들 수 없고 사용자 정의 생성 시간이 현재로 해결될 수 있기 때문입니다.

ILM 규칙 및 일관성이 상호 작용하여 데이터 보호에 영향을 미치는 방법

ILM 규칙과 정합성 보장 선택은 모두 오브젝트를 보호하는 방법에 영향을 미칩니다. 이러한 설정은 상호 작용할 수 있습니다.

예를 들어, ILM 규칙을 위해 선택된 수집 동작은 오브젝트 복사본의 초기 배치에 영향을 미치며, 오브젝트가 저장될 때 사용되는 일관성은 오브젝트 메타데이터의 초기 배치에 영향을 미칩니다. StorageGRID에서는 클라이언트 요청을 이행하기 위해 오브젝트의 데이터와 메타데이터에 모두 액세스해야 하기 때문에 정합성 보장 및 수집 동작에 대해

일치하는 보호 수준을 선택하면 초기 데이터 보호 수준을 높이고 시스템 응답을 예측할 수 있습니다.

다음은 StorageGRID에서 사용할 수 있는 정합성 보장 값에 대한 간략한 요약입니다.

- * ALL *: 모든 노드가 즉시 객체 메타데이터를 수신하거나 요청이 실패합니다.
- **Strong-global**: 개체 메타데이터가 모든 사이트에 즉시 배포됩니다. 모든 사이트에서 모든 클라이언트 요청에 대해 쓰기 후 읽기 정합성을 보장합니다.
- **Strong-site**: 개체 메타데이터가 사이트의 다른 노드에 즉시 배포됩니다. 사이트 내의 모든 클라이언트 요청에 대해 쓰기 후 읽기 일관성을 보장합니다.
- **Read-after-new-write**: 새 개체에 대해 읽기-쓰기 후 일관성을 제공하고 개체 업데이트에 대한 최종 일관성을 제공합니다. 고가용성 및 데이터 보호 보장 제공 대부분의 경우에 권장됩니다.
- * 사용 가능 *: 새 객체 및 객체 업데이트 모두에 대한 최종 일관성을 제공합니다. S3 버킷의 경우 필요한 경우에만 사용하십시오(예: 거의 읽지 않는 로그 값이 포함된 버킷의 경우 또는 존재하지 않는 키의 헤드 또는 GET 작업의 경우). S3 FabricPool 버킷은 지원되지 않습니다.

> 정합성 보장 값을 선택하기 전에 를 "일관성에 대한 전체 설명을 읽어 보십시오"참조하십시오. 기본값을 변경하기 전에 이점과 제한 사항을 이해해야 합니다.

일관성과 **ILM** 규칙이 상호 작용하는 방법의 예

다음과 같은 ILM 규칙과 다음과 같은 일관성이 있는 2개 사이트 그리드가 있다고 가정합니다.

- * ILM 규칙 *: 로컬 사이트와 원격 사이트에 각각 하나씩, 두 개의 오브젝트 복사본을 만듭니다. 엄격한 수집 동작을 사용합니다.
- * Consistency *: 강력한 글로벌(오브젝트 메타데이터는 모든 사이트에 즉시 배포됨).

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 규칙과 강력한 사이트 일관성을 사용한 경우 개체 데이터가 원격 사이트에 복제된 후 개체 메타데이터가 이 사이트에 배포되기 전에 클라이언트에서 성공 메시지를 받을 수 있습니다. 이 경우 오브젝트 메타데이터의 보호 수준이 오브젝트 데이터의 보호 수준과 일치하지 않습니다. 수집 후 곧바로 로컬 사이트가 손실되면 오브젝트 메타데이터가 손실됩니다. 개체를 검색할 수 없습니다.

일관성과 ILM 규칙 간의 상호 관계는 복잡할 수 있습니다. 도움이 필요하면 NetApp에 문의하십시오.

관련 정보

"예 5: 엄격한 수집 동작을 위한 ILM 규칙 및 정책"

오브젝트 저장 방법(복제 또는 삭제 코딩)

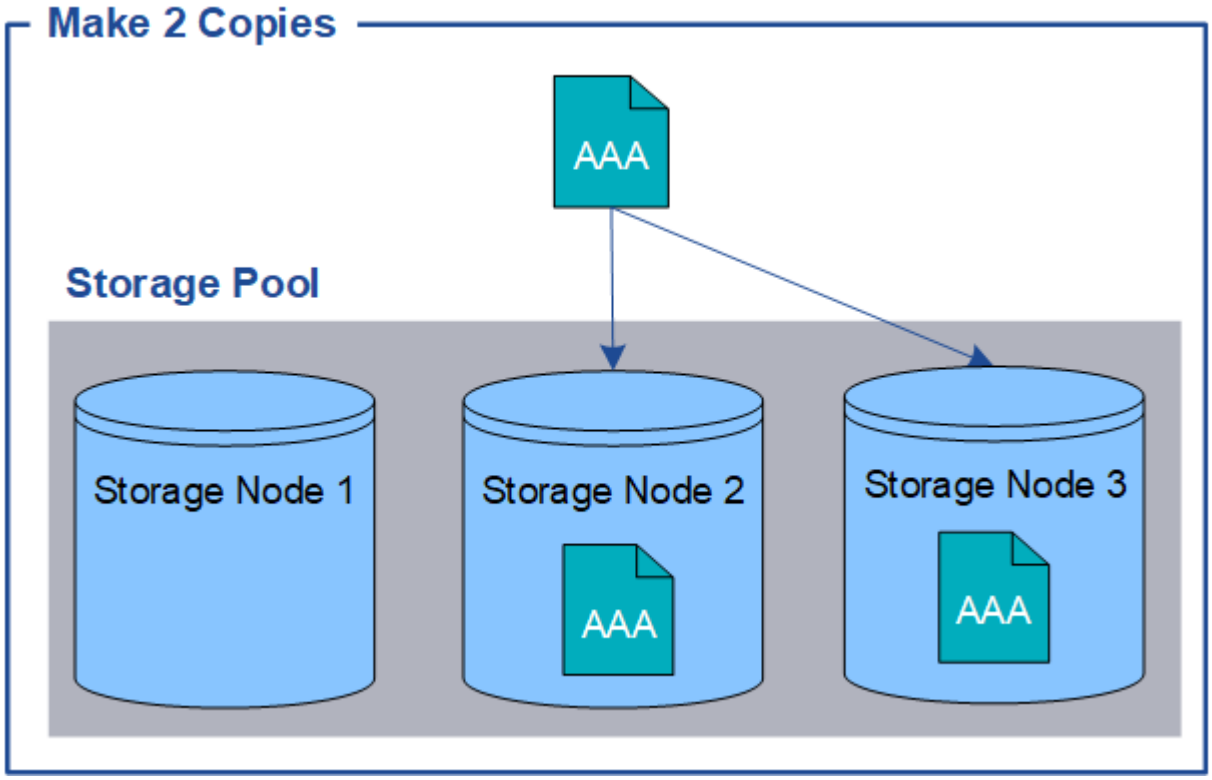
복제란 무엇입니까?

복제는 StorageGRID에서 오브젝트 데이터를 저장하는 데 사용하는 두 가지 방법 중 하나입니다(삭제 코딩은 다른 방법). 오브젝트가 복제를 사용하는 ILM 규칙과 일치하면 시스템은

오브젝트 데이터의 정확한 복사본을 생성하고 복사본을 스토리지 노드에 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

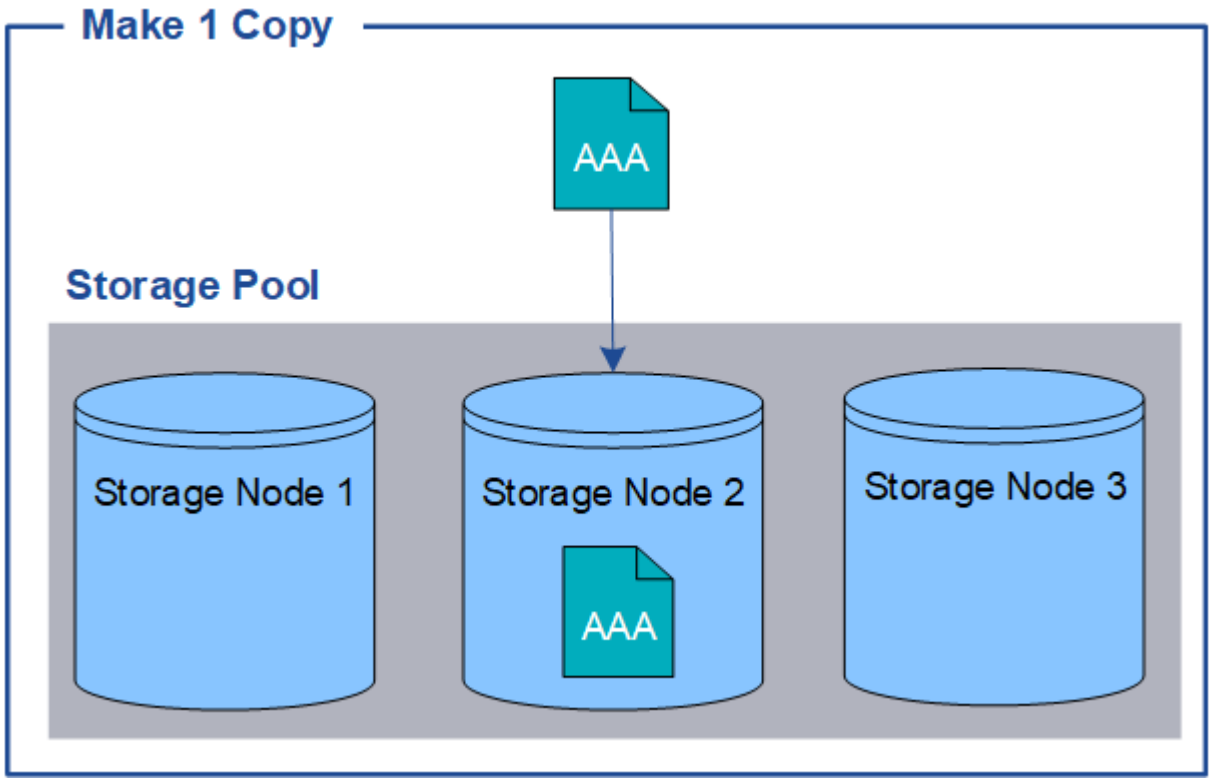
- "삭제 코딩이란 무엇입니까"
- "스토리지 풀이란 무엇입니까"
- "복제 및 삭제 코딩을 사용하여 사이트 손실을 보호합니다"

단일 복사본 복제를 사용하지 않아야 하는 이유

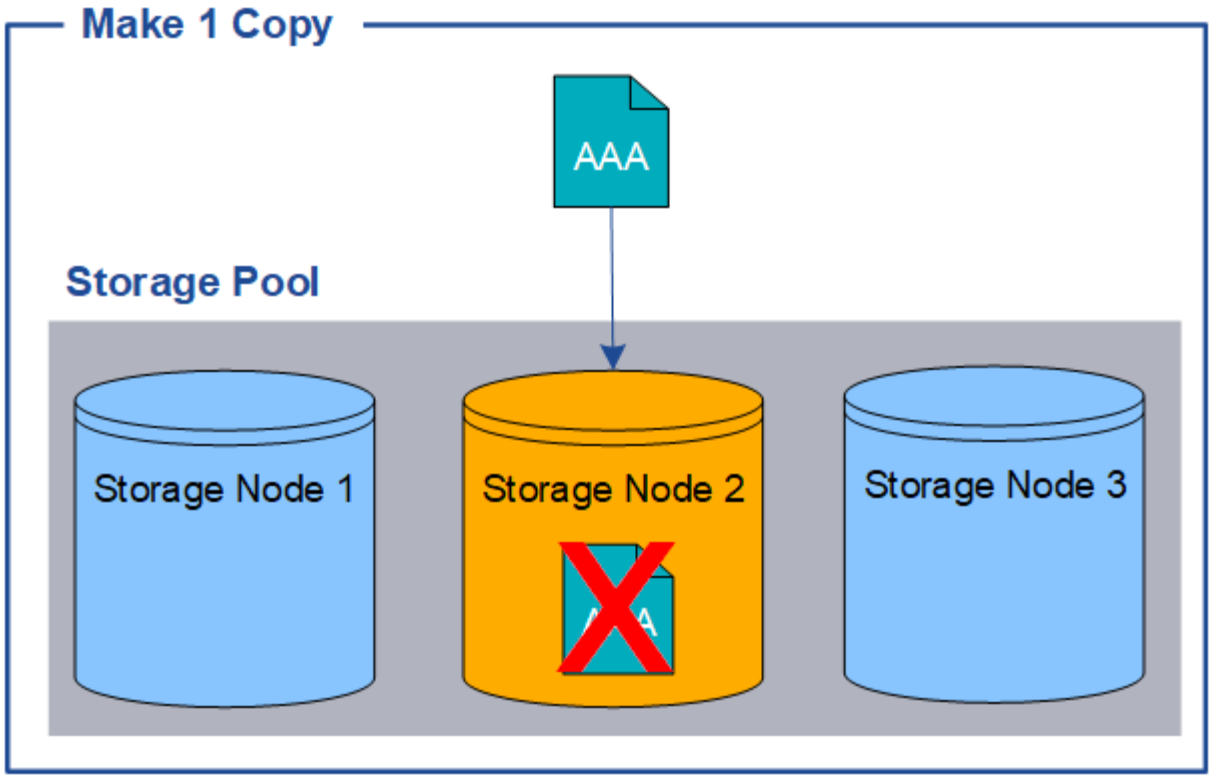
ILM 규칙을 생성하여 복제된 복사본을 만들 때는 항상 배치 지침에 두 개 이상의 복사본을 지정해야 합니다.

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.

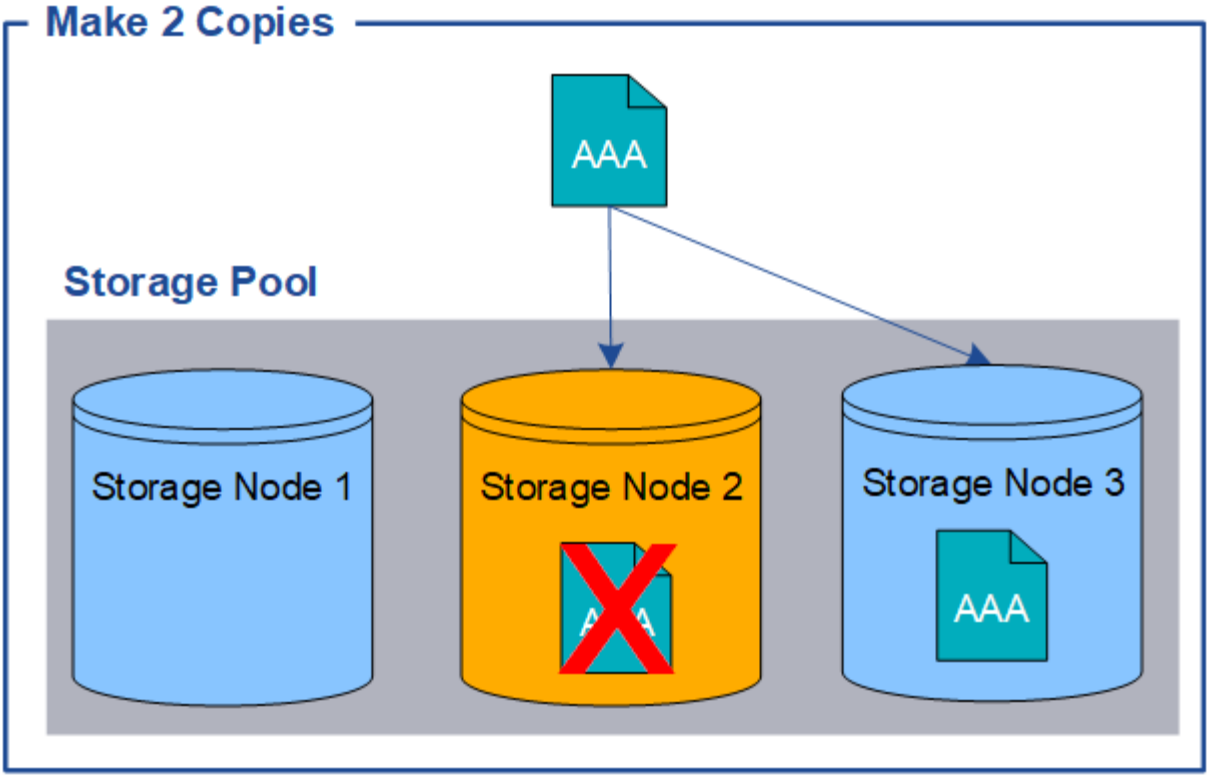
다음 예제에서 Make 1 Copy ILM 규칙은 세 개의 스토리지 노드가 포함된 스토리지 풀에 개체의 복제된 복사본 하나를 배치하도록 지정합니다. 이 규칙과 일치하는 객체가 수집되면 StorageGRID는 하나의 스토리지 노드에만 단일 복제본을 배치합니다.



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.



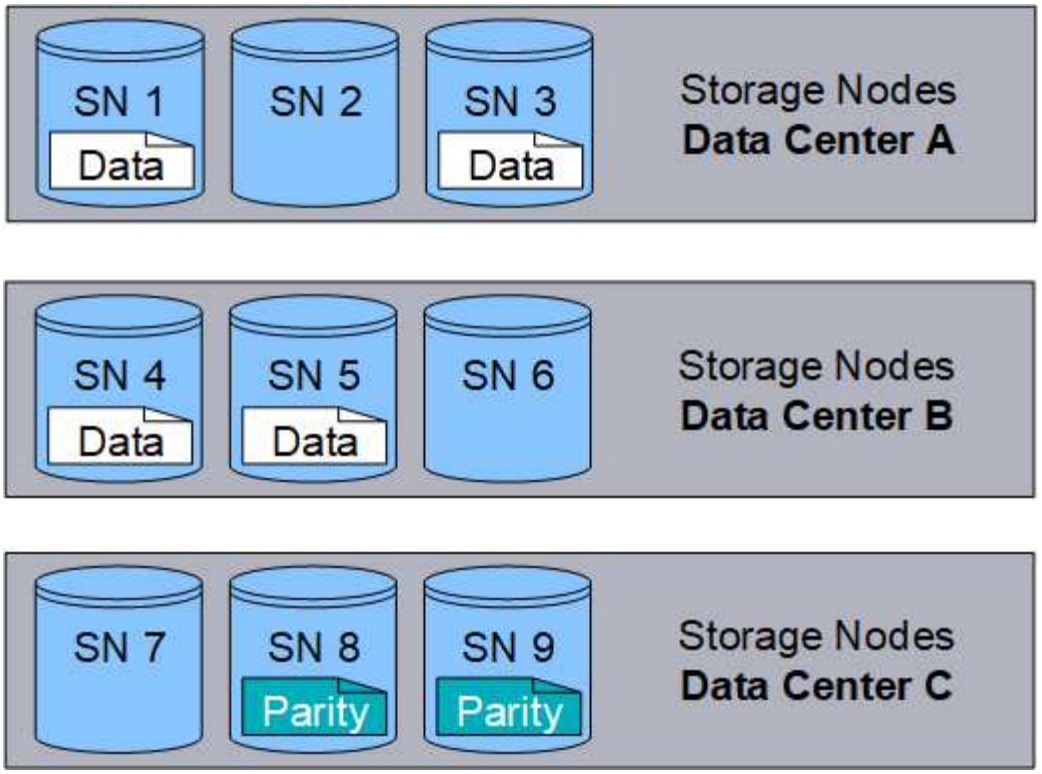
삭제 코딩이란 무엇입니까?

삭제 코딩은 StorageGRID에서 오브젝트 데이터를 저장하는 데 사용하는 두 가지 방법 중 하나입니다(복제는 다른 방법). 오브젝트가 삭제 코딩을 사용하는 ILM 규칙과 일치하면 해당 오브젝트는 데이터 조각으로 분할, 추가 패리티 조각들이 계산되고 각 조각은 다른 스토리지 노드에 저장됩니다.

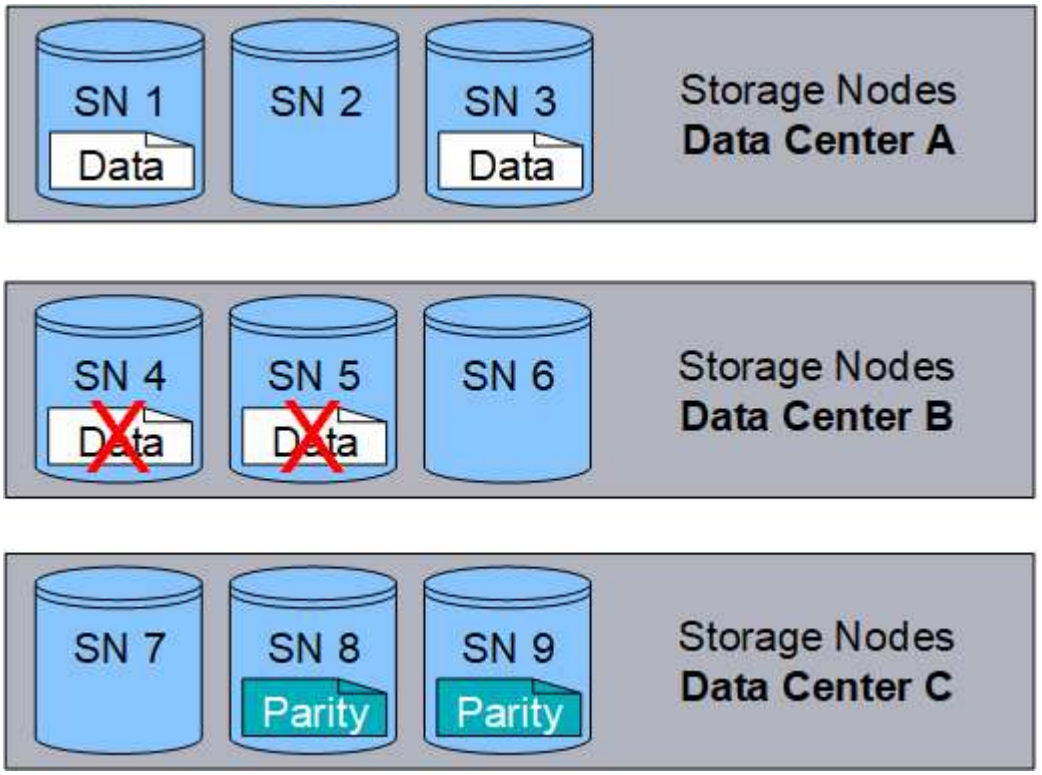
개체에 액세스하면 저장된 조각을 사용하여 다시 조립됩니다. 데이터 또는 패리티 조각이 손상되거나 손실될 경우, 삭제 코딩 알고리즘이 나머지 데이터 및 패리티 조각의 일부를 사용하여 해당 조각을 다시 생성할 수 있습니다.

ILM 규칙을 생성할 때 StorageGRID은 해당 규칙을 지원하는 삭제 코딩 프로필을 생성합니다. 삭제 코딩 프로필, "삭제 코딩 프로필의 이름을 바꿉니다"또는 의 목록을 볼 수 있습니다."삭제 코딩 프로필이 현재 ILM 규칙에 사용되지 않는 경우 비활성화합니다"

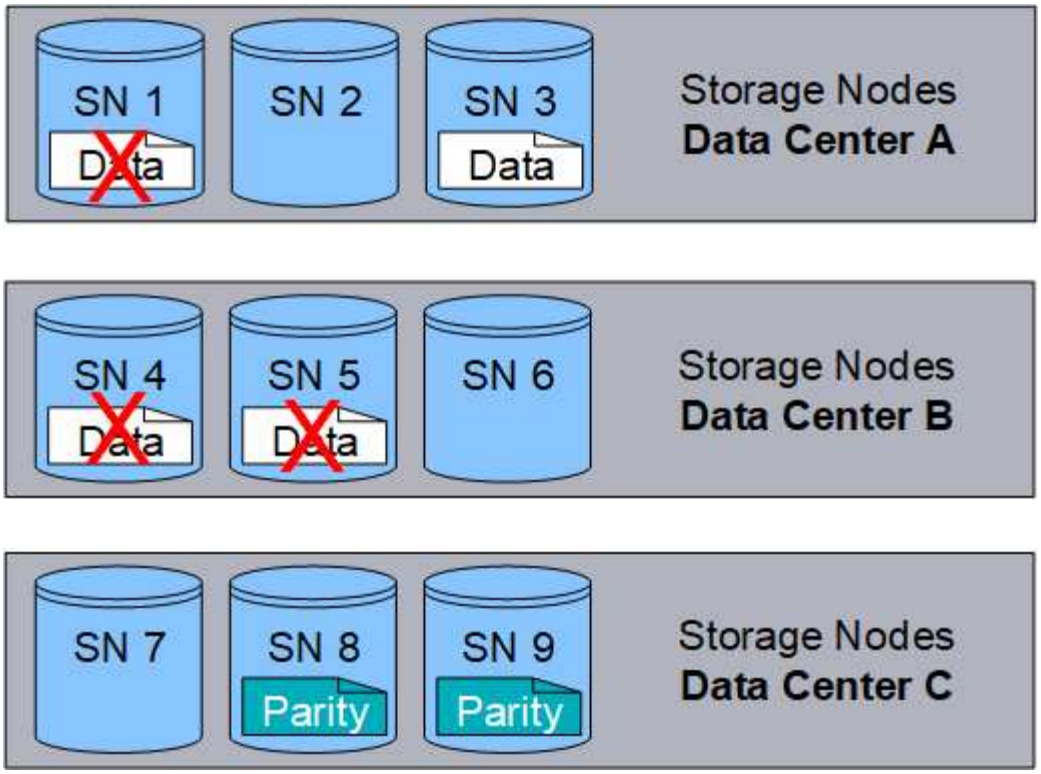
다음 예제에서는 오브젝트의 데이터에서 삭제 코딩 알고리즘을 사용하는 방법을 보여 줍니다. 이 예제에서 ILM 규칙은 4+2 삭제 코딩 체계를 사용합니다. 각 개체는 4개의 동일한 데이터 조각으로 분할되며 두 개의 패리티 조각은 개체 데이터에서 계산됩니다. 6개의 각 단편은 3개의 데이터 센터 사이트에서 서로 다른 노드에 저장되어 노드 장애 또는 사이트 손실에 대한 데이터 보호를 제공합니다.



4+2 삭제 코딩 방식은 다양한 방법으로 구성할 수 있습니다. 예를 들어 6개의 스토리지 노드가 포함된 단일 사이트 스토리지 풀을 구성할 수 있습니다. 의 경우 "사이트 손실 방지"각 사이트에 스토리지 노드 3개가 있는 사이트 3개가 포함된 스토리지 풀을 사용할 수 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 사이트가 손실된 경우에도 다른 모든 조각에 액세스할 수 있는 한 개체를 검색하거나 복구할 수 있습니다.



두 개 이상의 스토리지 노드가 손실되면 객체를 검색할 수 없습니다.



관련 정보

- "복제란 무엇입니까"
- "스토리지 풀이란 무엇입니까"
- "삭제 코딩 체계란 무엇입니까"
- "삭제 코딩 프로필의 이름을 바꿉니다"
- "삭제 코딩 프로필을 비활성화합니다"

삭제 코딩 체계란 무엇입니까?

삭제 코딩 스키마를 통해 각 오브젝트에 대해 생성되는 데이터 조각과 패리티 조각의 수를 제어합니다.

ILM 규칙을 생성하거나 편집할 때 사용 가능한 삭제 코딩 체계를 선택합니다. 사용할 스토리지 풀을 구성하는 스토리지 노드 및 사이트의 수에 따라 StorageGRID에서 삭제 코딩 체계를 자동으로 생성합니다.

데이터 보호

StorageGRID 시스템은 Reed-Solomon 삭제 코딩 알고리즘을 사용합니다. 알고리즘은 오브젝트를 데이터 `m` 조각으로 분할하고 `k` 패리티 조각을 계산합니다.

`k + m = n`조각은 다음과 같이 데이터 보호를 제공하기 위해 스토리지 노드 전체에 분산됩니다. `n`

- 오브젝트를 검색하거나 복구하려면 `k` 조각이 필요합니다.

- 오브젝트는 손실되거나 손상된 조각까지 유지할 수 `m` 있습니다. 값이 클수록 `m` 오류 허용 오차가 커집니다.

최고의 데이터 보호는 스토리지 풀 내에서 가장 높은 노드 또는 볼륨 장애를 허용하는 삭제 코딩 체계를 통해 제공됩니다.

스토리지 오버헤드

삭제 코딩 체계의 스토리지 오버헤드는 패리티 조각의 (`m`수를 데이터 조각의 수로 나누어 (`k`계산합니다. 스토리지 오버헤드를 사용하여 각 삭제 코딩 오브젝트에 필요한 디스크 공간을 계산할 수 있습니다.

```
disk space = object size + (object size * storage overhead)
```

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.

귀사의 요구사항을 충족하는 의 총액이 가장 낮은 삭제 코딩 체계를 선택합니다 `k+m`. 조각 수가 적은 삭제 코딩 체계를 사용하는 것이 보다 효율적인 이유는 다음과 같습니다.

- 오브젝트당 생성 및 분산(또는 검색)되는 조각의 수가 더 적습니다
- 조각 크기가 크기 때문에 성능이 더 좋습니다
- 따라서 에 추가할 수 있는 노드 수를 줄일 수 있습니다 "추가 스토리지가 필요할 때 확장"

스토리지 풀에 대한 지침

삭제 코딩 복사본을 생성할 규칙에 사용할 스토리지 풀을 선택할 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 코딩을 사용할 수 없습니다.

  - 3개 이상의 사이트가 포함된 스토리지 풀의 삭제 코딩 체계
  - 단일 사이트 스토리지 풀에 대한 삭제 코딩 구성표
- 모든 사이트 사이트를 포함하는 스토리지 풀을 사용하지 마십시오.
- 스토리지 풀에는 오브젝트 데이터를 저장할 수 있는 스토리지 노드 이상이 `k+m +1` 포함되어야 합니다.

  > ⓘ 스토리지 노드는 설치 중에 오브젝트 데이터가 아닌 오브젝트 메타데이터만 포함하도록 구성할 수 있습니다. 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

  필요한 최소 스토리지 노드 수는 입니다 `k+m`. 그러나 필요한 스토리지 노드를 일시적으로 사용할 수 없는 경우 하나 이상의 추가 스토리지 노드를 사용하면 수집 실패 또는 ILM 백로그를 방지할 수 있습니다.

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 스키마를 통해 사이트 손실을 보호할 수 있습니다. 한 사이트는 손실될 수 있으며 개체는 계속 액세스할 수 있습니다.

사이트 손실 보호를 제공하는 삭제 코딩 구성의 경우 각 사이트에는 최소 3개의 스토리지 노드가 필요하므로 스토리지 풀에서 권장 스토리지 노드 수가 을 초과합니다 `k+m +1`.

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 *: 패리티 세그먼트가 많을수록 내결함성(즉, 값이 더 높은 경우 `m`)이 증가합니다.
- * 네트워크 트래픽 * : 실패에서 복구 할 때 더 많은 조각이 있는 체계(즉, 더 높은 총계 `k+m`)를 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 스토리지 노드가 있는 스토리지 풀을 사용하는 `k+m +1` 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%

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 사이트에 복제된 10MB 개체는 20MB의 디스크 공간(복사본 2개)을 소비하고, 6+3 삭제 코딩 체계를 사용하여 세 사이트에서 삭제 코딩된 개체는 15MB의 디스크 공간만 소비합니다.

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.

- 삭제 코딩 체계에 따라 스토리지 노드 및 사이트의 수를 늘리는 것이 좋습니다. 반면, 오브젝트 데이터를 복제할 경우 각 복제본마다 스토리지 노드가 하나만 필요합니다. "3개 이상의 사이트가 포함된 스토리지 풀의 삭제 코딩 체계"및 을 "단일 사이트 스토리지 풀에 대한 삭제 코딩 구성표"참조하십시오.
- 스토리지 확장의 비용 및 복잡성 증가 복제를 사용하는 배포를 확장하려면 개체 복사본이 만들어지는 모든 위치에 스토리지 용량을 추가해야 합니다. 삭제 코딩을 사용하는 배포를 확장하려면 사용 중인 삭제 코딩 체계와 기존 스토리지 노드의 전체 용량을 고려해야 합니다. 예를 들어, 기존 노드가 100%로 꽉 찰 때까지 기다린 경우 스토리지 노드를 하나 이상 추가해야 `k+m` 하지만, 기존 노드가 70% 차 있을 때 확장하는 경우 사이트당 2개의 노드를 추가하여 사용 가능한 스토리지 용량을 최대화할 수 있습니다. 자세한 내용은 을 "삭제 코딩 오브젝트를 위한 스토리지 용량을 추가합니다"참조하십시오.
- 지리적으로 분산된 사이트에서 삭제 코딩을 사용하면 검색 지연 시간이 늘어납니다. 삭제 코딩되어 원격 사이트에 배포된 오브젝트의 오브젝트 조각은 복제되고 로컬에서 사용 가능한 오브젝트(클라이언트가 연결하는 동일한 사이트)에 비해 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 다음 방법을 사용하여 개체가 StorageGRID에 저장되는 기간을 제어할 수 있습니다.

- 그리드에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 S3 테넌트 사용자는 S3 오브젝트 잠금이 활성화된 상태로 버킷을 생성한 다음 각 버킷에 대해 * 기본 보존 기간 * 을 선택할 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 설정된 버킷의 오브젝트는 ILM이 "영구"로 유지합니다. 그러나 보존 기한에 도달한 후에는 클라이언트 요청 또는 버킷 라이프사이클의 만료에 의해 오브젝트 버전을 삭제할 수 있습니다. 을 "S3 오브젝트 잠금으로 오브젝트 관리"참조하십시오.
- 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 "S3 라이프사이클 구성을 생성합니다"참조하십시오.
- S3 클라이언트에서 객체 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 다음 방법을 사용하여 객체 보존을 제어할 수 있습니다.

- 각 테넌트의 S3 오브젝트 잠금 최대 보존 기간을 설정합니다. 그런 다음 테넌트 사용자는 각 버킷에 대해 기본 보존 기간을 설정할 수 있습니다. 최대 보존 기간은 해당 버킷에 대해 새로 수집된 객체(객체의 유지 종료 날짜)에도 적용됩니다.
- ILM 배치 지침을 생성하여 개체 저장 기간을 제어합니다. ILM 규칙에 따라 오브젝트가 일치하는 경우 StorageGRID는 ILM 규칙의 마지막 기간이 경과할 때까지 해당 오브젝트를 저장합니다. 배치 명령에 "영구"가 지정된 경우 객체는 무기한 유지됩니다.
- 누가 오브젝트 보존 기간을 제어하든 ILM 설정은 저장되는 오브젝트 복사본(복제 또는 삭제 코딩)과 복사본의 위치(스토리지 노드 또는 클라우드 스토리지 풀)를 제어합니다.

S3 버킷 수명 주기와 **ILM**이 상호 작용하는 방식

S3 버킷 라이프사이클이 구성된 경우 라이프사이클 만료 작업이 라이프사이클 필터와 일치하는 오브젝트에 대한 ILM 정책을 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 **ILM**보다 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 **ILM**을 재정의합니다

ILM을 참조하십시오

스토리지 노드에 "영구" 복사본 2개 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 노드에 "영구" 복사본 2개 저장

클라이언트 삭제 요청

2024-03-31일에 발행되었습니다

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 클라이언트가 삭제를 요청하는데 다음 조건 중 하나 이상이 참입니다. ◦ 예를 들어, 개체 위치를 일시적으로 사용할 수 없기 때문에 복사본을 30초 이내에 삭제할 수 없습니다. ◦ 백그라운드 삭제 대기열은 유휴 상태입니다.

삭제 수행 방법	사용 시
객체가 즉시 제거됩니다(동기식 삭제).	S3 클라이언트가 삭제 요청을 하고 다음 조건 중 * 모든 * 가 충족되는 경우: • 모든 사본은 30초 이내에 제거할 수 있습니다. • 백그라운드 삭제 대기열에는 처리할 객체가 포함됩니다.

S3 클라이언트가 삭제 요청을 하면 StorageGRID는 삭제 큐에 개체를 추가하는 것으로 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 필요한 시간입니다

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 개체를 삭제한 후 삭제 속도가 느린 것으로 보일 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.

개체를 삭제한 후 공간을 확보하는 데 필요한 시간은 다음과 같은 여러 요소에 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 개체의 현재 버전으로 0바이트 삭제 마커를 만들어서 이전 버전의 개체를 "비최신"으로 만듭니다. 개체 삭제 표식은 현재 버전이고 현재 버전이 아닌 경우 만료된 개체 삭제 표식이 됩니다.

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.

버전 지정된 개체를 삭제할 때 공간을 확보하거나 삭제 표식을 제거하려면 다음 중 하나를 사용합니다.

- * S3 클라이언트 요청 *: S3 오브젝트 삭제 요청에서 객체 버전 ID를 (`DELETE /object?versionId=ID` 지정합니다.) 이 요청은 지정된 버전의 오브젝트 복사본만 제거합니다(다른 버전은 계속 공간을 소모함).
- * 버킷 수명 주기 * : 버킷 수명 주기 `NoncurrentVersionExpiration` 구성에 작업을 사용합니다. 지정된 NoncurrentDays 수가 충족되면 StorageGRID에서 현재 버전이 아닌 개체 버전의 모든 복사본을 영구적으로 제거합니다. 이러한 개체 버전은 복구할 수 없습니다.

  `NewerNoncurrentVersions`버킷 수명 주기 구성의 작업은 버전 `S3` 버킷에 보존되는 비최신 버전 수를 지정합니다. 지정된 것보다 더 많은 비최신 버전이 있으면 `NewerNoncurrentVersions` StorageGRID는 `NoncurrentDays` 값이 경과되었을 때 이전 버전을 제거합니다. `NewerNoncurrentVersions`임계값은 `ILM`에서 제공하는 수명주기 규칙을 재정의합니다. 즉, `ILM`이 삭제를 요청할 경우 임계값 내에 버전이 있는 현재 개체가 `NewerNoncurrentVersions` 보존됩니다.

  만료된 개체 삭제 표식을 제거하려면 `Expiration`,, `Days` 또는 `Date` 태그 중 하나와 함께 작업을 `ExpiredObjectDeleteMarker` 사용합니다.

- * ILM *"활성 정책의 클론을 생성합니다": 새 정책에 두 가지 ILM 규칙을 추가합니다.
  - 첫 번째 규칙: "비현재 시간"을 참조 시간으로 사용하여 객체의 현재 버전과 일치시킵니다. 에서 "ILM 규칙 생성 마법사의 1단계(세부 정보 입력)""버전 관리가 활성화된 S3 버킷의 이전 개체 버전에만 이 규칙을 적용하시겠습니까?"라는 질문에 대해 * 예 * 를 선택합니다.
  - 두 번째 규칙: * Ingest Time * 을 사용하여 현재 버전과 일치시킵니다. "비현재 시간" 규칙은 * Ingest Time * 규칙 위의 정책에 나타나야 합니다.

    만료된 오브젝트 삭제 마커를 제거하려면 * Ingest Time * 규칙을 사용하여 현재 삭제 마커와 일치시킵니다. 삭제 표시자는 * 시간 간격 * / * 일 * 이 경과하고 현재 삭제 작성기가 만료되었을 때만 제거됩니다(최신 버전이 아님).

- * 버킷에서 오브젝트 삭제 *: "모든 개체 버전을 삭제합니다"버킷에서 삭제 마커를 포함하여 테넌트 관리자를 사용합니다.

버전이 지정된 개체가 삭제되면 StorageGRID는 개체의 현재 버전으로 0바이트 삭제 표식을 만듭니다. 버전이 지정된 버킷을 삭제하려면 먼저 모든 오브젝트 및 삭제 마커를 제거해야 합니다.

- StorageGRID 11.7 이하 버전에서 생성된 삭제 표식은 S3 클라이언트 요청을 통해서만 제거할 수 있으며, ILM, 버킷 라이프사이클 규칙에 의해 제거되거나 버킷 작업의 오브젝트 삭제 에 의해 제거되지 않습니다.
- StorageGRID 11.8 이상에서 생성된 버킷의 삭제 마커는 ILM, 버킷 라이프사이클 규칙, 버킷 작업의 오브젝트 삭제 또는 명시적 S3 클라이언트 삭제로 제거할 수 있습니다.

관련 정보

- "S3 REST API 사용"
- "예 4: S3 버전 오브젝트에 대한 ILM 규칙 및 정책"

저장 점수를 생성하고 할당합니다

스토리지 등급은 스토리지 노드에서 사용하는 스토리지 유형을 식별합니다. ILM 규칙을 사용하여 특정 스토리지 노드에 특정 객체를 배치하려는 경우 스토리지 성적을 생성할 수

있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

이 작업에 대해

StorageGRID를 처음 설치하면 * 기본 * 스토리지 등급이 시스템의 모든 스토리지 노드에 자동으로 할당됩니다. 필요에 따라 사용자 지정 스토리지 등급을 정의하고 이를 다른 스토리지 노드에 할당할 수 있습니다.

사용자 지정 스토리지 등급을 사용하면 특정 유형의 스토리지 노드만 포함하는 ILM 스토리지 풀을 생성할 수 있습니다. 예를 들어, StorageGRID All-Flash 스토리지 어플라이언스 와 같이 가장 빠른 스토리지 노드에 특정 오브젝트를 저장할 수 있습니다.

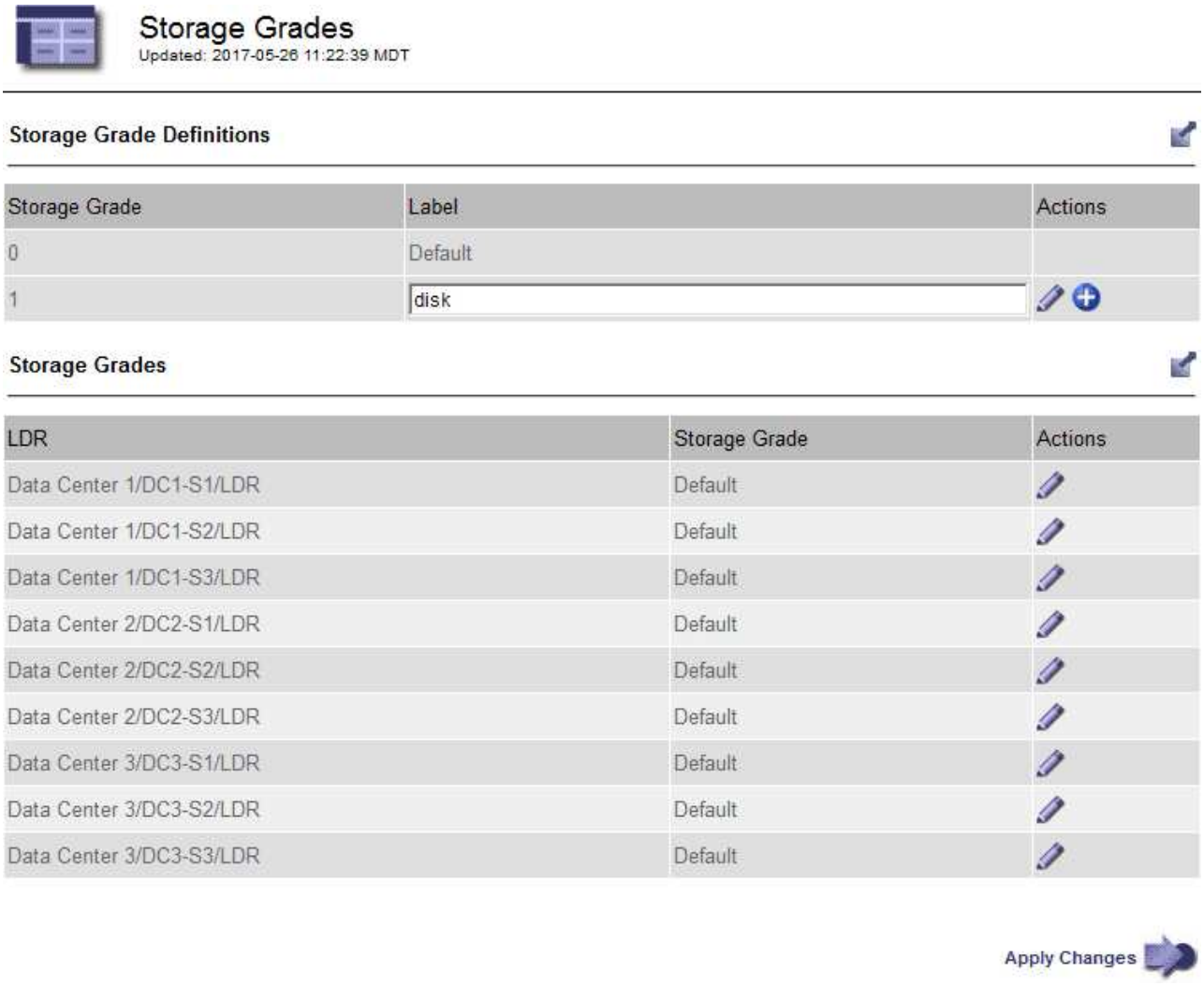
> 스토리지 노드는 설치 중에 오브젝트 데이터가 아닌 오브젝트 메타데이터만 포함하도록 구성할 수 있습니다. 메타데이터 전용 스토리지 노드는 스토리지 등급을 할당할 수 없습니다. 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

스토리지 등급이 중요하지 않은 경우(예: 모든 스토리지 노드가 동일함) 이 절차를 건너뛰고 스토리지 등급에 대한 * 모든 스토리지 등급 포함 * 선택을 사용할 수 "스토리지 풀을 생성합니다"있습니다. 이 선택 항목을 사용하면 스토리지 등급에 관계없이 스토리지 풀에 사이트의 모든 스토리지 노드가 포함됩니다.

> 필요한 것보다 더 많은 저장 점수를 생성하지 마십시오. 예를 들어, 각 스토리지 노드에 대한 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. 사용자 정의 저장 평점 정의:
   a. 추가할 각 사용자 지정 스토리지 등급에 대해 * Insert * 를 선택하여  행을 추가합니다.
   b. 설명 라벨을 입력합니다.



c. Apply Changes * 를 선택합니다.

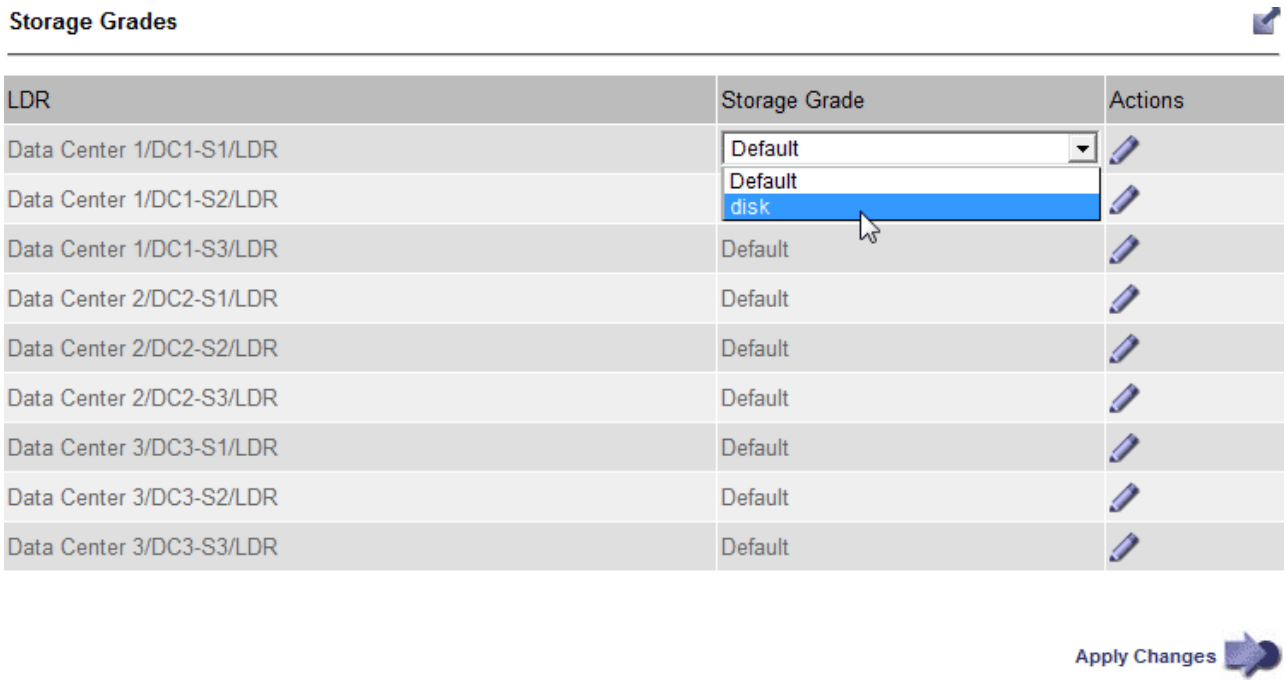
d. 필요한 경우, 저장된 라벨을 수정해야 하는 경우 * 편집 * 을 선택하고 * 변경 사항 적용 * 을 선택합니다.

저장 평점을 삭제할 수 없습니다.

3. 스토리지 노드에 새 스토리지 등급 할당:

a. LDR 목록에서 스토리지 노드를 찾고 해당 * Edit * 아이콘을 선택합니다.

b. 목록에서 적절한 스토리지 등급을 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 사용합니다

스토리지 풀이란 무엇입니까?

스토리지 풀은 스토리지 노드의 논리적 그룹입니다.

StorageGRID를 설치하면 사이트당 하나의 스토리지 풀이 자동으로 생성됩니다. 스토리지 요구 사항에 따라 추가 스토리지 풀을 구성할 수 있습니다.

설치 중에 오브젝트 데이터와 오브젝트 메타데이터 또는 오브젝트 메타데이터만 포함하도록 스토리지 노드를 구성할 수 있습니다. 메타데이터 전용 스토리지 노드는 스토리지 풀에서 사용할 수 없습니다. 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

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 위치와 사용되는 스토리지 유형을 결정합니다. 복제용 ILM 규칙을 구성할 때 하나 이상의 스토리지 풀을 선택합니다.

스토리지 풀 생성 지침

여러 사이트에 데이터를 분산하여 데이터 손실을 방지하기 위해 스토리지 풀을 구성 및

사용합니다. 복제된 복사본 및 삭제 코딩 복사본을 사용하려면 다른 스토리지 풀 구성이 필요합니다.

을 "복제 및 삭제 코딩을 사용하여 사이트 손실을 방지할 수 있는 방법의 예"참조하십시오.

모든 스토리지 풀에 대한 지침입니다

- 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.
- 일반적으로 모든 스토리지 노드 스토리지 풀(StorageGRID 11.6 이하) 또는 모든 사이트 사이트를 사용하지 마십시오. 이러한 항목은 확장에 추가한 새 사이트를 포함하도록 자동으로 업데이트되며, 이는 원하는 동작이 아닐 수 있습니다.

복제된 복제본에 사용되는 스토리지 풀에 대한 지침입니다

- 를 사용하여 사이트 손실 보호를 수행하려면 "복제"에서 사이트별 스토리지 풀을 하나 이상 "각 ILM 규칙에 대한 배치 지침"지정합니다.

  StorageGRID를 설치하는 동안 각 사이트에 대해 스토리지 풀 하나가 자동으로 생성됩니다.

  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 사이트만 포함하는 새 스토리지 풀을 생성합니다. 그런 다음 "ILM 규칙을 업데이트합니다"새 사이트에 저장되는 개체를 제어합니다.
- 복제본 수가 스토리지 풀 수보다 적은 경우 시스템은 복제본을 분산하여 풀 간에 디스크 사용량을 밸런싱합니다.
- 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.

삭제 코딩 복사본에 사용되는 스토리지 풀에 대한 지침입니다

- 를 사용하여 사이트 손실 보호를 "삭제 코딩"수행하려면 최소 3개의 사이트로 구성된 스토리지 풀을 생성합니다. 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.
- 스토리지 풀에 포함된 스토리지 노드 및 사이트의 수에 따라 사용 가능한 스토리지 노드가 "삭제 코딩 구성표 "결정됩니다.
- 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.
- 처리량이 많은 경우 여러 사이트가 포함된 스토리지 풀을 사용하는 것은 사이트 간 네트워크 지연 시간이 100ms를 초과하는 경우에는 권장되지 않습니다. 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 검색 시 달성 가능한 최대 속도에 영향을 미치거나(수집 동작으로 Balanced 또는 Strict를 선택한 경우) ILM 대기열 백로그로 이어질 수 있습니다(수집 동작으로 이중 커밋을 선택한 경우). 을 "ILM 규칙 수집 동작"참조하십시오.

그리드에 사이트가 하나만 포함된 경우에는 삭제 코딩 프로필에서 모든 스토리지 노드 스토리지 풀(StorageGRID 11.6 이하) 또는 모든 사이트 사이트를 사용할 수 없습니다. 이 동작은 두 번째 사이트가 추가될 때 프로필이 무효화될 수 없도록 합니다.

사이트 손실 방지

StorageGRID 구축에 사이트가 두 개 이상 포함된 경우 적절하게 구성된 스토리지 풀과 함께 복제 및 삭제 코딩을 사용하여 사이트 손실을 보호할 수 있습니다.

복제 및 삭제 코딩에 필요한 스토리지 풀 구성은 다음과 같습니다.

- 사이트 손실 보호를 위해 복제를 사용하려면 StorageGRID 설치 중에 자동으로 생성되는 사이트별 스토리지 풀을 사용합니다. 그런 다음 여러 스토리지 풀을 지정하는 ILM 규칙을 생성하여 "배치 지침"각 개체의 복사본을 각 사이트에 배치합니다.
- 사이트 손실 보호를 위해 삭제 "여러 사이트로 구성된 스토리지 풀을 생성합니다"코딩을 사용하려면 다음을 수행합니다. 그런 다음 여러 사이트와 사용 가능한 삭제 코딩 스키마로 구성된 스토리지 풀 하나를 사용하는 ILM 규칙을 만듭니다.

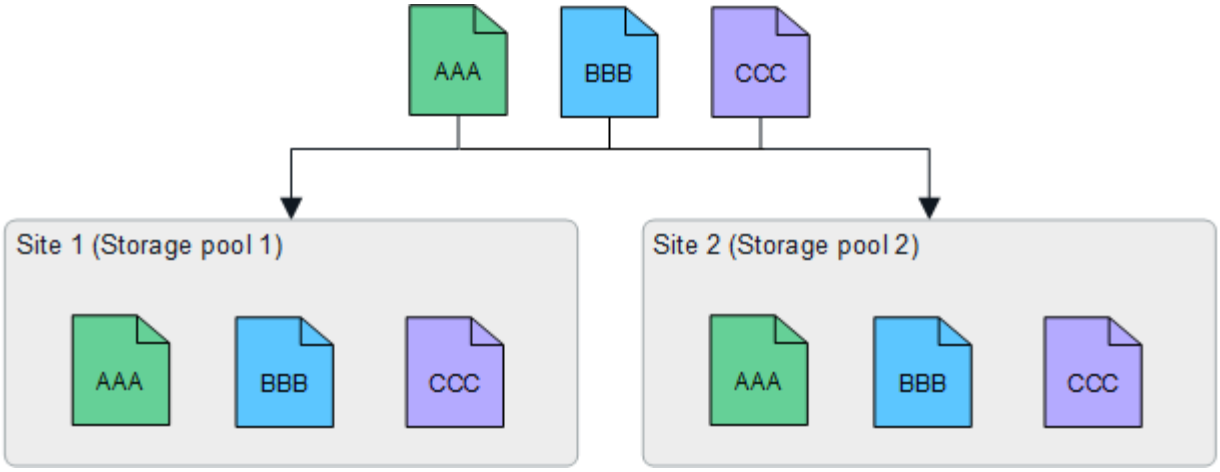
사이트 손실 방지를 위해 StorageGRID 배포를 구성할 때는 및 의 영향도 고려해야 "수집 옵션"합니다. "정합성"

복제 예

기본적으로 StorageGRID를 설치하는 동안 각 사이트에 대해 하나의 스토리지 풀이 생성됩니다. 한 사이트만으로 구성된 스토리지 풀을 사용하면 사이트 손실 방지를 위해 복제를 사용하는 ILM 규칙을 구성할 수 있습니다. 이 예에서

- 스토리지 풀 1에는 사이트 1가 포함되어 있습니다
- 스토리지 풀 2에는 사이트 2가 포함되어 있습니다
- ILM 규칙에는 두 개의 배치가 포함되어 있습니다.
  - 사이트 1에서 복사본 1개를 복제하여 객체를 저장합니다
  - 사이트 2에서 복사본 1개를 복제하여 개체를 저장합니다

ILM 규칙 배치:



한 사이트가 손실되면 다른 사이트에서 개체의 복사본을 사용할 수 있습니다.

삭제 코딩 예

스토리지 풀당 둘 이상의 사이트로 구성된 스토리지 풀을 사용하면 사이트 손실 방지를 위해 삭제 코딩을 사용하는 ILM 규칙을 구성할 수 있습니다. 이 예에서

- 스토리지 풀 1에는 사이트 1부터 3까지 포함됩니다
- ILM 규칙에는 배치 하나가 포함되어 있습니다. 세 개의 사이트가 포함된 스토리지 풀 1에서 4+2 EC 스키마를 사용하여 삭제 코딩을 사용하여 오브젝트를 저장합니다

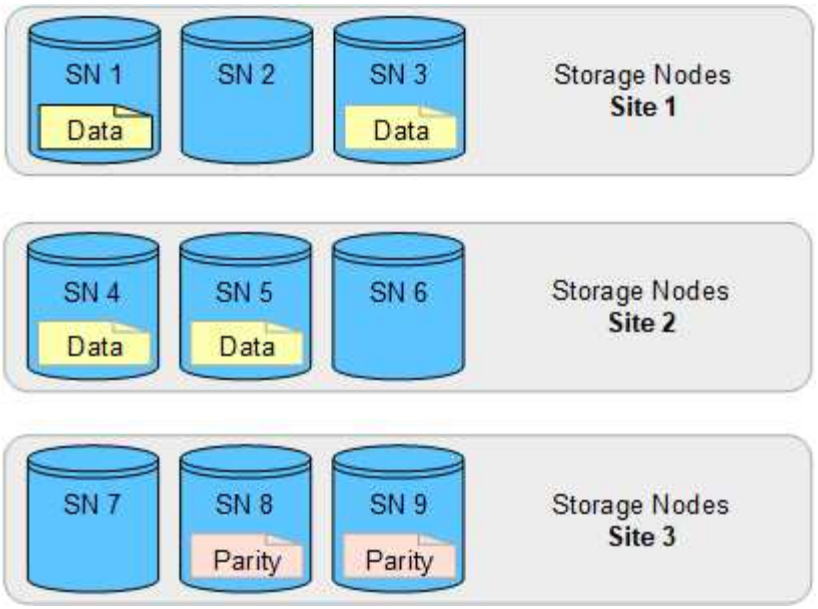
ILM 규칙 배치:

이 예에서

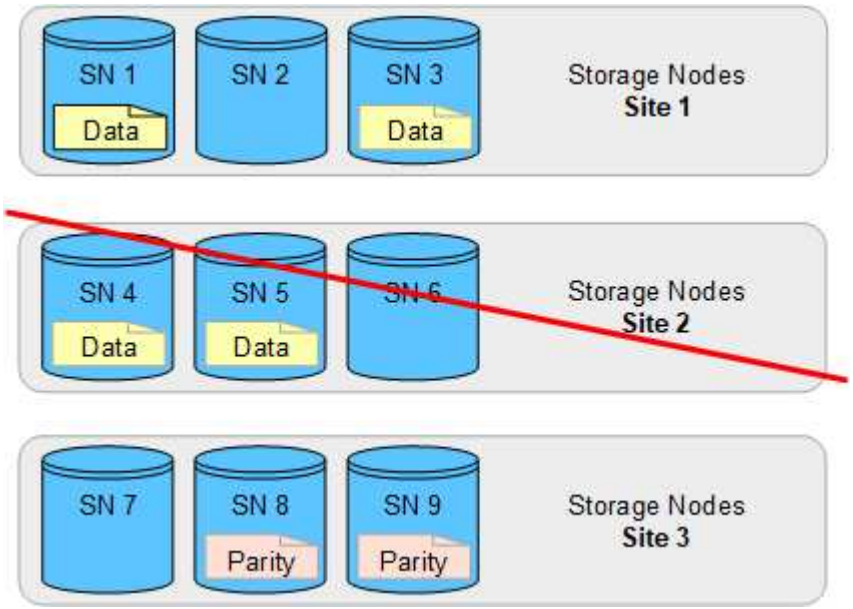
- ILM 규칙은 4+2 삭제 코딩 스키마를 사용합니다.
- 각 개체는 4개의 동일한 데이터 조각으로 분할되며 두 개의 패리티 조각은 개체 데이터에서 계산됩니다.
- 6개의 각 단편은 3개의 데이터 센터 사이트에서 서로 다른 노드에 저장되어 노드 장애 또는 사이트 손실에 대한 데이터 보호를 제공합니다.

삭제 코딩은 두 개의 사이트를 제외한 모든 수의 사이트가 포함된 스토리지 풀에서 허용됩니다.

4+2 삭제 코딩 체계를 사용하는 ILM 규칙:



한 사이트가 손실되어도 데이터를 복구할 수 있습니다.



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.

> 새 그리드에 StorageGRID 11.9을 설치하면 각 사이트에 대해 스토리지 풀이 자동으로 생성됩니다. 그러나 StorageGRID 11.6 이하 버전을 처음 설치한 경우 각 사이트에 대해 스토리지 풀이 자동으로 생성되지 않습니다.

StorageGRID 시스템 외부에 오브젝트 데이터를 저장할 클라우드 스토리지 풀을 생성하려면 을 참조하십시오.
"클라우드 스토리지 풀 사용에 대한 정보"

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"
- 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.

> 삭제 코딩 프로필에 사용될 스토리지 풀에 모든 사이트 사이트를 포함하지 마십시오. 대신 삭제 코딩 데이터를 저장할 각 사이트의 스토리지 풀에 별도의 항목을 추가하십시오. 예를 보려면 을 이 단계참조하십시오.

- 스토리지 등급이 두 개 이상인 경우 단일 사이트에서 서로 다른 스토리지 등급이 포함된 스토리지 풀을 생성하지 마십시오. 를 "스토리지 풀 생성 지침"참조하십시오.

단계

1. ILM * > * 스토리지 풀 * 을 선택합니다.

   스토리지 풀 탭에는 정의된 모든 스토리지 풀이 나열됩니다.

   > StorageGRID 11.6 이하를 새로 설치하는 경우 새 데이터 센터 사이트를 추가할 때마다 모든 스토리지 노드 스토리지 풀이 자동으로 업데이트됩니다. ILM 규칙에서 이 풀을 사용하지 마십시오.

2. 새 스토리지 풀을 생성하려면 * Create * 를 선택합니다.
3. 스토리지 풀의 고유한 이름을 입력합니다. 삭제 코딩 프로필과 ILM 규칙을 구성할 때 쉽게 식별할 수 있는 이름을 사용합니다.
4. Site * (사이트 *) 드롭다운 목록에서 이 스토리지 풀의 사이트를 선택합니다.

   사이트를 선택하면 테이블의 스토리지 노드 수가 자동으로 업데이트됩니다.

   일반적으로 스토리지 풀에서 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.

   스토리지 등급인 _ 에는 모든 스토리지 등급이 포함되며 _ 은(는) 선택한 사이트의 모든 스토리지 노드가 포함됩니다. 그리드에 스토리지 노드에 대한 추가 스토리지 점수를 생성한 경우 해당 스토리지 등급이 드롭다운에 나열됩니다.

6.] 다중 사이트 삭제 코딩 프로필에서 스토리지 풀을 사용하려면 * Add more nodes * 를 선택하여 각 사이트의 항목을 스토리지 풀에 추가합니다.

한 사이트에 대해 서로 다른 저장소 평점이 있는 항목을 두 개 이상 추가하면 경고가 표시됩니다.

항목을 제거하려면 삭제 아이콘을 선택합니다.

7. 선택 사항에 만족하면 * 저장 * 을 선택합니다.

   새 스토리지 풀이 목록에 추가됩니다.

스토리지 풀 세부 정보를 봅니다

스토리지 풀의 세부 정보를 확인하여 스토리지 풀이 사용되는 위치를 확인하고 포함된 노드와 스토리지 등급을 확인할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

단계

1. ILM * > * 스토리지 풀 * 을 선택합니다.

   스토리지 풀 테이블에는 스토리지 노드가 포함된 각 스토리지 풀에 대한 다음 정보가 포함됩니다.

   - * 이름 *: 스토리지 풀의 고유한 표시 이름입니다.
   - * 노드 수 *: 스토리지 풀의 노드 수
   - * 스토리지 사용 *: 이 노드의 오브젝트 데이터에 사용된 총 사용 가능 공간의 비율입니다. 이 값에는 개체 메타데이터가 포함되지 않습니다.
   - * 총 용량 *: 스토리지 풀의 크기로, 스토리지 풀의 모든 노드에 대해 오브젝트 데이터에 사용할 수 있는 총 공간의 크기와 같습니다.
   - * ILM 사용 *: 스토리지 풀이 현재 사용 중인 방법 스토리지 풀이 사용되지 않거나 하나 이상의 ILM 규칙, 삭제 코딩 프로필 또는 둘 다에서 사용될 수 있습니다.

2. 특정 스토리지 풀에 대한 세부 정보를 보려면 해당 이름을 선택합니다.

   스토리지 풀의 세부 정보 페이지가 나타납니다.

3. 스토리지 풀에 포함된 스토리지 노드에 대한 자세한 내용은 * Nodes * 탭을 참조하십시오.

   표에는 각 노드에 대한 다음 정보가 나와 있습니다.

   - 노드 이름
   - 사이트 이름
   - 보관 등급
   - 스토리지 사용량: 스토리지 노드에 사용된 객체 데이터의 총 가용 공간의 비율입니다.

   각 스토리지 노드에 대한 스토리지 사용 객체 데이터 차트에는 동일한 스토리지 사용(%) 값이 표시됩니다(* nodes * > **Storage Node* * > * Storage * 선택).

4. ILM 사용 * 탭을 보고 스토리지 풀이 현재 ILM 규칙 또는 삭제 코딩 프로필에 사용되고 있는지 확인합니다.
5. 필요한 경우 * ILM 규칙 페이지 * 로 이동하여 스토리지 풀을 사용하는 모든 규칙에 대해 알아보고 관리합니다.

   를 "ILM 규칙 작업 지침"참조하십시오.

스토리지 풀을 편집합니다

스토리지 풀을 편집하여 이름을 변경하거나 사이트 및 스토리지 등급을 업데이트할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"
- 를 검토했습니다."스토리지 풀 생성 지침"
- 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 사이트 또는 스토리지 등급을 추가하는 경우 새 사이트 또는 스토리지 등급의 스토리지 노드가 자동으로 사용되지 않는다는 점에 유의하십시오. StorageGRID에서 새 사이트 또는 스토리지 등급을 사용하도록 강제하려면 편집된 스토리지 풀을 저장한 후 새 ILM 정책을 활성화해야 합니다.

단계

1. ILM * > * 스토리지 풀 * 을 선택합니다.
2. 편집할 스토리지 풀의 확인란을 선택합니다.

   모든 스토리지 노드 스토리지 풀(StorageGRID 11.6 이하)은 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 사용되는 경우 사이트 또는 스토리지 등급을 변경할 수 없으며 이로 인해 삭제 코딩 체계가 유효하지 않게 됩니다. 예를 들어, 삭제 코딩 프로필에 사용된 스토리지 풀에 현재 사이트가 하나만 있는 스토리지 등급이 포함된 경우, 이 변경 사항으로 인해 삭제 코딩 체계가 무효화되기 때문에 두 사이트에 대해 스토리지 등급을 사용할 수 없습니다.

   > 기존 스토리지 풀에서 사이트를 추가하거나 제거하더라도 삭제 인코딩된 데이터는 이동되지 않습니다. 사이트에서 기존 데이터를 이동하려면 새 스토리지 풀과 EC 프로필을 생성하여 데이터를 다시 인코딩해야 합니다.

6. 저장 * 을 선택합니다.

작업을 마친 후

활성 ILM 정책에 사용된 스토리지 풀에 새 사이트 또는 스토리지 성적을 추가한 경우 새 ILM 정책을 활성화하여 StorageGRID가 새 사이트 또는 스토리지 등급을 사용하도록 강제합니다. 예를 들어, 기존 ILM 정책을 클론 복제한 다음 클론을 활성화합니다. 을 "ILM 규칙 및 ILM 정책 작업"참조하십시오.

스토리지 풀을 제거합니다

사용되지 않는 스토리지 풀을 제거할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "액세스 권한이 필요합니다"있습니다.

단계

1. ILM * > * 스토리지 풀 * 을 선택합니다.
2. 표에서 ILM 사용 열을 확인하여 스토리지 풀을 제거할 수 있는지 확인합니다.

   스토리지 풀을 ILM 규칙 또는 삭제 코딩 프로필에 사용 중인 경우에는 제거할 수 없습니다. 필요한 경우 **storage pool name* * > * ILM usage * 를 선택하여 스토리지 풀이 사용되는 위치를 확인합니다.

3. 제거하려는 스토리지 풀을 사용하지 않는 경우 확인란을 선택합니다.
4. 제거 * 를 선택합니다.
5. OK * 를 선택합니다.

클라우드 스토리지 풀 사용

클라우드 스토리지 풀이란 무엇입니까**?**

클라우드 스토리지 풀을 사용하면 ILM을 사용하여 StorageGRID 시스템 외부로 오브젝트 데이터를 이동할 수 있습니다. 예를 들어, 자주 액세스하지 않는 오브젝트를 Microsoft Azure Blob 스토리지의 Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud 또는 Archive 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 노드로 구성되지만 클라우드 스토리지 풀은 외부 버킷(S3) 또는 컨테이너(Azure Blob 스토리지)로 구성됩니다.

이 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	Grid Manager에서 * ILM * > * 스토리지 풀 * > * 클라우드 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 내 하나 이상의 스토리지 노드에 있습니다.	StorageGRID 시스템 외부의 Amazon S3 버킷, Azure Blob 스토리지 컨테이너 또는 Google Cloud에 액세스할 수 있습니다. 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 스토리지 클래스 및 S3 RestoreObject 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 Cloud Storage Pool에 사용되는 컨테이너에 대한 Azure Blob 저장소 수명 주기 관리를 구성하지 않습니다. 클라우드 스토리지 풀에 있는 객체에 대한 RestoreObject 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 방법을 사용합니까?	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: • 참고 *: FabricPool 데이터는 클라우드 스토리지 풀로 계층화할 수 없습니다.

Cloud Storage Pool 개체의 수명주기입니다

클라우드 스토리지 풀을 구현하기 전에 각 유형의 클라우드 스토리지 풀에 저장된 개체의 라이프사이클을 검토하십시오.

S3: 클라우드 스토리지 풀 오브젝트의 수명 주기

S3 Cloud Storage Pool에 저장된 오브젝트의 라이프사이클 단계를 설명합니다.

> "Glacier"는 Glacier 스토리지 클래스와 Glacier Deep Archive 스토리지 클래스를 모두 지칭합니다. 단, Glacier Deep Archive 스토리지 클래스는 Expedited 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 오브젝트를 Glacier 스토리지로 전환하지 않은 한 클라이언트 애플리케이션은 StorageGRID의 S3 GetObject 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 전환하려면 외부 S3 버킷에 대한 라이프사이클 구성을 생성해야 하며 Glacier 스토리지 클래스를 구현하고 S3 RestoreObject API를 지원하는 스토리지 솔루션을 사용해야 합니다.

   - 전환 중에 클라이언트 애플리케이션은 S3 HeadObject 요청을 사용하여 객체의 상태를 모니터링할 수 있습니다.
4. * Glacier 스토리지에서 개체 복원 *

   오브젝트가 Glacier 스토리지로 전환된 경우 클라이언트 애플리케이션은 S3 RestoreObject 요청을 실행하여 검색 가능한 복사본을 S3 클라우드 스토리지 풀에 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 노드에 하나 이상의 객체 복제본이 있는 경우 RestoreObject 요청을 실행하여 Glacier에서 객체를 복원할 필요가 없습니다. 대신 GetObject 요청을 사용하여 로컬 복사본을 직접 검색할 수 있습니다.

5. * 객체 검색됨 *

   개체가 복원되면 클라이언트 응용 프로그램에서 복원된 개체를 검색하기 위한 GetObject 요청을 실행할 수 있습니다.

Azure: Cloud Storage Pool 개체의 수명 주기

이 단계에서는 Azure Cloud Storage Pool에 저장된 개체의 라이프사이클 단계를 설명합니다.

1. * StorageGRID * 에 저장된 개체

   수명 주기를 시작하기 위해 클라이언트 응용 프로그램은 StorageGRID에 개체를 저장합니다.

2. * Azure 클라우드 스토리지 풀로 이동된 객체 *

   Azure 클라우드 스토리지 풀을 배치 위치로 사용하는 ILM 규칙과 일치하는 오브젝트가 있는 경우 StorageGRID는 해당 오브젝트를 클라우드 스토리지 풀에 의해 지정된 외부 Azure Blob 스토리지 컨테이너로 이동합니다.

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 *

   오브젝트가 아카이브 계층으로 이전된 경우 클라이언트 애플리케이션은 S3 RestoreObject 요청을 실행하여 검색 가능한 복사본을 Azure Cloud Storage Pool에 복원할 수 있습니다.

   StorageGRID가 RestoreObject를 수신하면 일시적으로 개체를 Azure Blob 스토리지 냉각 계층으로 전환합니다. RestoreObject 요청의 만료 날짜에 도달하면 StorageGRID는 객체를 다시 아카이브 계층으로 전환합니다.

   > StorageGRID 내의 스토리지 노드에 하나 이상의 객체 복제본이 있는 경우 RestoreObject 요청을 실행하여 아카이브 액세스 계층에서 객체를 복구할 필요가 없습니다. 대신 GetObject 요청을 사용하여 로컬 복사본을 직접 검색할 수 있습니다.

5. * 객체 검색됨 *

   개체가 Azure 클라우드 스토리지 풀에 복원되면 클라이언트 응용 프로그램에서 복원된 개체를 검색하기 위한 GetObject 요청을 실행할 수 있습니다.

관련 정보

"S3 REST API 사용"

클라우드 스토리지 풀을 사용하는 경우

Cloud Storage Pool을 사용하면 데이터를 외부 위치에 백업하거나 계층화할 수 있습니다. 또한 둘 이상의 클라우드에 데이터를 백업하거나 계층화할 수 있습니다.

StorageGRID 데이터를 외부 위치에 백업합니다

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 RestoreObject 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 Cloud Storage Pool 엔드포인트를 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 Cloud Storage Pool 엔드포인트를 사용할 경우 한 번에 하나의 Cloud Storage Pool에만 개체를 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 일정 시간 동안 오브젝트를 클라우드 스토리지 풀 A에 저장한 다음 클라우드 스토리지 풀 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.

- FabricPool에서 클라우드 스토리지 풀 타겟의 객체를 검색하는 지연 시간이 추가되었기 때문에 클라우드 스토리지 풀을 사용할 수 없습니다.
- S3 오브젝트 잠금이 설정된 오브젝트를 클라우드 스토리지 풀에 배치할 수 없습니다.
- 클라우드 스토리지 풀의 대상 S3 버킷에 S3 오브젝트 잠금이 설정되어 있는 경우 버킷 복제(PutBucketReplication) 구성 시도가 실패하고 AccessDenied 오류가 발생합니다.
- 다음 플랫폼, 인증 및 S3 오브젝트 잠금과 프로토콜 조합은 클라우드 스토리지 풀에 대해 지원되지 않습니다.
  - * 플랫폼 *: Google Cloud Platform 및 Azure
  - * 인증 유형 * : IAM 역할 어디서나 익명 액세스
  - * 프로토콜 *: HTTP

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 경우 인터넷의 끝점과 같은 외부 끝점으로 메시지를 보낼 수 있도록 허용해야 "스토리지 프록시를 구성합니다"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 구성합니다. 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 버킷에 대한 정책은 오브젝트를 버킷으로 이동하고, 오브젝트의 상태를 가져오고, 필요할 경우 Glacier 스토리지에서 오브젝트를 복원하는 등의 작업에 대한 StorageGRID 권한을 부여해야 합니다. StorageGRID는 버킷에 대한 모든 제어 액세스 권한을 가져야 (`s3:*`합니다. 그러나 이것이 가능하지 않은 경우 버킷 정책은 StorageGRID에 다음 S3 권한을 부여해야 합니다.

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: 외부 버킷의 수명 주기에 대한 고려 사항

클라우드 스토리지 풀에 지정된 StorageGRID와 외부 S3 버킷 간에 오브젝트 이동은 ILM 규칙과 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 전환하려면 외부 S3 버킷에서 적절한 라이프사이클 구성을 생성해야 하며, Glacier 스토리지 클래스를 구현하고 S3 RestoreObject 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.

클라우드 스토리지 풀의 오브젝트를 Amazon S3 Glacier로 전환하지 않고 S3 Glacier Deep Archive로 전환하려면 버킷 라이프사이클에 을 `<StorageClass>DEEP_ARCHIVE</StorageClass>` 지정합니다. 그러나 이 계층을 사용하여 S3 Glacier Deep Archive에서 오브젝트를 복원할 수는 `Expedited` 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 Pool에서 사용되는 컨테이너에 Azure Blob 스토리지 라이프사이클 관리를 사용하지 마십시오. 라이프사이클 작업은 Cloud Storage Pool 작업을 방해할 수 있습니다.

관련 정보

"클라우드 스토리지 풀을 생성합니다"

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?	아카이브 타겟 역할을 합니다. Cloud Storage Pool의 오브젝트 복사본은 개체의 유일한 복사본이거나 추가 복사본일 수 있습니다. 즉, 복사본을 두 개에 유지하는 대신 StorageGRID 내에 하나의 복사본을 유지하고 복사본을 클라우드 스토리지 풀에 보낼 수 있습니다.	테넌트가 StorageGRID(소스)의 버킷에서 외부 S3 버킷(대상)으로 오브젝트를 자동으로 복제할 수 있습니다. 독립 S3 인프라에서 개체의 독립적인 복사본을 생성합니다.
어떻게 설정합니까?	그리드 관리자 또는 그리드 관리 API를 사용하여 스토리지 풀과 동일한 방식으로 정의됩니다. ILM 규칙의 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 관리자 또는 S3 API를 사용하여 CloudMirror 엔드포인트(IP 주소, 자격 증명 등)를 정의하여 테넌트 사용자"CloudMirror 복제 구성" CloudMirror 엔드포인트를 설정한 후 해당 테넌트 계정이 소유한 모든 버킷이 CloudMirror 엔드포인트를 가리키도록 구성할 수 있습니다.
누가 설정해야 합니까?	일반적으로 그리드 관리자	일반적으로 테넌트 사용자입니다
대상은 무엇입니까?	• 호환 가능한 S3 인프라(Amazon S3 포함) • Azure Blob 아카이브 계층입니다 • Google Cloud Platform(GCP)	• 호환 가능한 S3 인프라(Amazon S3 포함) • Google Cloud Platform(GCP)
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 버킷으로 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.

	클라우드 스토리지 풀	**CloudMirror** 복제 서비스
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 풀은 단일 외부 Amazon S3 버킷 또는 기타 S3 호환 공급자 또는 Azure Blob 스토리지 컨테이너를 지정합니다.

클라우드 스토리지 풀을 생성할 때 StorageGRID에서 오브젝트를 저장할 외부 버킷 또는 컨테이너의 이름과 위치, 클라우드 공급자 유형(Amazon S3/GCP 또는 Azure Blob 스토리지) 및 StorageGRID이 외부 버킷 또는 컨테이너에 액세스하는 데 필요한 정보를 지정합니다.

StorageGRID는 저장하는 즉시 클라우드 스토리지 풀을 검증하므로, 클라우드 스토리지 풀에 지정된 버킷이나 컨테이너가 존재하고 연결 가능한지 확인해야 합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "액세스 권한이 필요합니다"있습니다.
- 를 검토했습니다."클라우드 스토리지 풀에 대한 고려 사항"
- 클라우드 스토리지 풀에서 참조하는 외부 버킷 또는 컨테이너가 이미 있으며 이 서비스 끝점 정보입니다있습니다.
- 버킷 또는 컨테이너에 접근하려면 를 선택할 수 인증 유형에 대한 계정 정보입니다있습니다.

단계

1. ILM * > * 스토리지 풀 * > * 클라우드 스토리지 풀 * 을 선택합니다.
2. Create * 를 선택한 후 다음 정보를 입력합니다.

필드에 입력합니다	설명
클라우드 스토리지 풀 이름입니다	Cloud Storage Pool과 그 용도를 간략하게 설명하는 이름입니다. ILM 규칙을 구성할 때 쉽게 식별할 수 있는 이름을 사용합니다.

필드에 입력합니다	설명
공급자 유형입니다	이 클라우드 스토리지 풀에 사용할 클라우드 공급자: • * Amazon S3/GCP *: Amazon S3, C2S(Commercial Cloud Services) S3, GCP(Google Cloud Platform) 또는 기타 S3 호환 공급자의 경우 이 옵션을 선택합니다. • * Azure Blob 저장소 *
버킷 또는 용기	외부 S3 버킷 또는 Azure 컨테이너의 이름입니다. 클라우드 스토리지 풀을 저장한 후에는 이 값을 변경할 수 없습니다.

3. 제공자 유형 선택에 따라 서비스 끝점 정보를 입력합니다.

Amazon S3/GCP

a. 프로토콜에서 HTTPS 또는 HTTP를 선택합니다.

> 중요한 데이터에 HTTP 연결을 사용하지 마십시오.

b. 호스트 이름을 입력합니다. 예:

`s3-aws-region.amazonaws.com`

c. URL 스타일 선택:

옵션을 선택합니다	설명
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.
가상 호스팅 방식	가상 호스팅 방식의 URL을 사용하여 버킷에 액세스합니다. 가상 호스팅 방식의 URL에는 도메인 이름의 일부로 버킷 이름이 포함됩니다. 예: `https://bucket-name.s3.company.com/key-name`
경로 스타일	경로 스타일 URL을 사용하여 버킷에 액세스합니다. 경로 스타일 URL의 끝에는 버킷 이름이 포함됩니다 예: `https://s3.company.com/bucket-name/key-name` • 참고: * 경로 스타일 URL 옵션은 권장되지 않으며 향후 StorageGRID 릴리스에서 더 이상 사용되지 않습니다.

d. 필요한 경우 포트 번호를 입력하거나 기본 포트 443을 HTTPS에 사용하거나 80을 HTTP에 사용합니다.

Azure Blob 저장소

a. 다음 형식 중 하나를 사용하여 서비스 끝점의 URI를 입력합니다.

- `https://host:port`
- `http://host:port`

예: `https://myaccount.blob.core.windows.net:443`

포트를 지정하지 않으면 기본적으로 포트 443이 HTTPS에 사용되고 포트 80은 HTTP에 사용됩니다.

4. * Continue * 를 선택합니다. 그런 다음 인증 유형을 선택하고 Cloud Storage Pool 엔드포인트를 위한 필수 정보를 입력합니다.

액세스 키

_ Amazon S3/GCP 또는 기타 S3 호환 제공업체의 경우 _

a. * 액세스 키 ID *: 외부 버킷을 소유한 계정의 액세스 키 ID를 입력하십시오.
b. * 비밀 액세스 키 * : 비밀 액세스 키를 입력합니다.

어디서나 **IAM** 역할 수행

_ AWS IAM 역할 Anywhere 서비스의 경우 _

StorageGRID은 AWS STS(Security Token Service)를 사용하여 AWS 리소스에 액세스하기 위한 단기 토큰을 동적으로 생성합니다.

a. * AWS IAM 역할 Anywhere 지역 *: 클라우드 스토리지 풀의 지역을 선택합니다. `us-east-1`예를 들어,
b. **Trust anchor URN**: 단기간 STS 자격 증명에 대한 요청의 유효성을 검사하는 신뢰 앵커의 URN을 입력합니다. 루트 또는 중간 CA일 수 있습니다.
c. * Profile URN *: IAM Roles Anywhere 프로파일의 URN을 입력합니다. 이 프로파일에는 신뢰할 수 있는 사람이 추론할 수 있는 역할이 나열되어 있습니다.
d. * 역할 URN * : 신뢰할 수 있는 사람이 추정하는 IAM 역할의 URN을 입력하십시오.
e. * 세션 기간 *: 임시 보안 자격 증명과 역할 세션의 기간을 입력합니다. 15분 이상 12시간 이내로 입력하십시오.
f. * 서버 CA 인증서 * (선택 사항): 하나 이상의 신뢰할 수 있는 CA 인증서(PEM 형식), IAM 역할 Anywhere 서버 확인을 위한 인증서. 생략하면 서버가 확인되지 않습니다.
g. 최종 엔터티 인증서: 신뢰 앵커에서 서명한 X509 인증서의 PEM 형식의 공개 키입니다. AWS IAM Roles Anywhere는 이 키를 사용하여 STS 토큰을 발급합니다.
h. * 최종 엔티티 개인 키 *: 최종 엔티티 인증서의 개인 키입니다.

CAP(C2S 액세스 포털**)**

_C2S(Commercial Cloud Services) S3 서비스 _

a. * 임시 자격 증명 URL *: C2S 계정에 할당된 모든 필수 및 선택적 API 매개 변수를 포함하여 StorageGRID가 CAP 서버에서 임시 자격 증명을 얻기 위해 사용할 전체 URL을 입력하십시오.
b. * 서버 CA 인증서 *: * 찾아보기 * 를 선택하고 StorageGRID가 CAP 서버를 확인하는 데 사용할 CA 인증서를 업로드합니다. 인증서는 PEM으로 인코딩되어 적절한 CA(정부 인증 기관)에서 발급해야 합니다.
c. * 클라이언트 인증서 *: * 찾아보기 * 를 선택하고 StorageGRID가 CAP 서버에 자신을 식별하는 데 사용할 인증서를 업로드합니다. 클라이언트 인증서는 PEM 인코딩되어 적절한 CA(정부 인증 기관)에서 발급되고 C2S 계정에 대한 액세스 권한이 부여되어야 합니다.
d. * 클라이언트 개인 키 *: * 찾아보기 * 를 선택하고 클라이언트 인증서에 대한 PEM 인코딩된 개인 키를 업로드합니다.
e. 클라이언트 개인 키가 암호화된 경우 클라이언트 개인 키의 암호를 해독하기 위한 암호를 입력합니다. 그렇지 않으면 * 클라이언트 개인 키 암호 * 필드를 비워 둡니다.

클라이언트 인증서가 암호화될 경우 암호화에 기존 형식을 사용합니다. PKCS #8 암호화된 형식은 지원되지 않습니다.

Azure Blob 저장소

_ Azure Blob 스토리지의 경우, 공유 키만 _

a. * 계정 이름 *: 외부 컨테이너를 소유하는 저장소 계정의 이름을 입력합니다

b. * 계정 키 *: 스토리지 계정의 비밀 키를 입력합니다

Azure 포털을 사용하여 이러한 값을 찾을 수 있습니다.

익명

추가 정보가 필요하지 않습니다.

5. Continue * 를 선택합니다. 그런 다음 사용할 서버 확인 유형을 선택합니다.

옵션을 선택합니다	설명
스토리지 노드 OS에서 루트 CA 인증서를 사용합니다	운영 체제에 설치된 Grid CA 인증서를 사용하여 연결을 보호합니다.
사용자 지정 CA 인증서를 사용합니다	사용자 지정 CA 인증서를 사용합니다. 찾아보기 * 를 선택하고 PEM 인코딩된 인증서를 업로드합니다.
인증서를 확인하지 않습니다	이 옵션을 선택하면 클라우드 스토리지 풀에 대한 TLS 연결이 안전하지 않습니다.

6. 저장 * 을 선택합니다.

   클라우드 스토리지 풀을 저장할 때 StorageGRID은 다음을 수행합니다.

   - 버킷 또는 컨테이너와 서비스 엔드포인트가 있는지, 그리고 지정한 자격 증명을 사용하여 해당 엔드포인트에 도달할 수 있는지 검증합니다.
   - 버킷이나 컨테이너에 마커 파일을 기록하여 클라우드 스토리지 풀로 식별합니다. 이름이 인 이 파일은 제거하지 마십시오 `x-ntap-sgws-cloud-pool-uuid`.

     Cloud Storage Pool 검증이 실패하면 검증에 실패한 이유를 설명하는 오류 메시지가 표시됩니다. 예를 들어 인증서 오류가 있거나 지정한 버킷 또는 컨테이너가 이미 없는 경우 오류가 보고될 수 있습니다.

7. 오류가 발생하면"클라우드 스토리지 풀 문제 해결을 위한 지침", 문제를 해결한 다음 클라우드 스토리지 풀을 다시 저장해 보십시오.

클라우드 스토리지 풀 세부 정보를 봅니다

클라우드 스토리지 풀의 세부 정보를 확인하여 사용된 위치를 확인하고 포함된 노드 및 스토리지 등급을 확인할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

단계

1. ILM * > * 스토리지 풀 * > * 클라우드 스토리지 풀 * 을 선택합니다.

   클라우드 스토리지 풀 테이블에는 스토리지 노드를 포함하는 각 클라우드 스토리지 풀에 대한 다음 정보가 포함됩니다.

   - * 이름 * : 풀의 고유한 표시 이름입니다.
   - * URI *: 클라우드 스토리지 풀의 균일한 리소스 식별자입니다.
   - * 공급자 유형 *: 이 클라우드 스토리지 풀에 사용되는 클라우드 공급자입니다.
   - * 컨테이너 *: 클라우드 스토리지 풀에 사용되는 버킷의 이름입니다.
   - * ILM 사용 *: 풀이 현재 사용되는 방법입니다. 클라우드 스토리지 풀이 사용되지 않거나 하나 이상의 ILM 규칙, 삭제 코딩 프로필 또는 둘 다에서 사용될 수 있습니다.
   - * 마지막 오류 *: 이 클라우드 스토리지 풀의 상태 점검 중에 발견된 마지막 오류.

2. 특정 클라우드 스토리지 풀에 대한 세부 정보를 보려면 해당 이름을 선택합니다.

   풀에 대한 세부 정보 페이지가 나타납니다.

3. 이 클라우드 스토리지 풀의 인증 유형에 대해 알아보고 인증 세부 정보를 편집하려면 * Authentication * 탭을 확인하십시오.
4. 서버 확인 * 탭을 보고 확인 세부 정보, 확인 편집, 새 인증서 다운로드 또는 인증서 PEM을 복사하십시오.
5. ILM 사용 * 탭을 보고 클라우드 스토리지 풀이 현재 ILM 규칙 또는 삭제 코딩 프로필에 사용되고 있는지 확인합니다.
6. 필요에 따라 클라우드 스토리지 풀을 사용하는 ILM 규칙 페이지 * 로 이동합니다"규칙에 대해 알아보고 관리하세요".

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"
- 를 검토했습니다."클라우드 스토리지 풀에 대한 고려 사항"

단계

1. ILM * > * 스토리지 풀 * > * 클라우드 스토리지 풀 * 을 선택합니다.

   클라우드 스토리지 풀 테이블에는 기존 클라우드 스토리지 풀이 나열됩니다.

2. 편집할 클라우드 스토리지 풀의 확인란을 선택한 다음 * Actions * > * Edit * 를 선택합니다.

   또는 클라우드 스토리지 풀의 이름을 선택한 다음 * Edit * 를 선택합니다.

3. 필요에 따라 클라우드 스토리지 풀 이름, 서비스 끝점, 인증 자격 증명 또는 인증서 확인 방법을 변경합니다.

클라우드 스토리지 풀의 공급자 유형 또는 S3 버킷 또는 Azure 컨테이너는 변경할 수 없습니다.

이전에 서버 또는 클라이언트 인증서를 업로드한 경우 * 인증서 세부 정보 * 아코디언을 확장하여 현재 사용 중인 인증서를 검토할 수 있습니다.

4. 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.

   지침을 "클라우드 스토리지 풀 문제 해결"참조하여 문제를 해결한 다음 클라우드 스토리지 풀을 다시 저장해 보십시오.

클라우드 스토리지 풀을 제거합니다

ILM 규칙에 사용되지 않고 오브젝트 데이터가 없는 경우 클라우드 스토리지 풀을 제거할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "액세스 권한이 필요합니다"있습니다.

필요한 경우 **ILM**을 사용하여 오브젝트 데이터를 이동합니다

제거하려는 Cloud Storage Pool에 오브젝트 데이터가 포함된 경우 ILM을 사용하여 데이터를 다른 위치로 이동해야 합니다. 예를 들어 데이터를 그리드의 스토리지 노드 또는 다른 클라우드 스토리지 풀로 이동할 수 있습니다.

단계

1. ILM * > * 스토리지 풀 * > * 클라우드 스토리지 풀 * 을 선택합니다.
2. 표에서 ILM 사용 열을 확인하여 클라우드 스토리지 풀을 제거할 수 있는지 확인합니다.

   클라우드 스토리지 풀을 ILM 규칙 또는 삭제 코딩 프로필에 사용 중인 경우에는 제거할 수 없습니다.

3. 클라우드 스토리지 풀을 사용 중인 경우 **cloud* 스토리지 풀 이름 * > * ILM 사용량 * 을 선택합니다.
4. "각 ILM 규칙을 복제합니다" 현재 제거할 클라우드 스토리지 풀에 객체가 배치됩니다.
5. 복제한 각 규칙에 의해 관리되는 기존 개체를 이동할 위치를 결정합니다.

   하나 이상의 스토리지 풀 또는 다른 클라우드 스토리지 풀을 사용할 수 있습니다.

6. 복제한 각 규칙을 편집합니다.

   ILM 규칙 생성 마법사의 2단계에 대해 * copies at * 필드에서 새 위치를 선택합니다.

7. "새 ILM 정책을 생성합니다" 이전 규칙을 각각 복제된 규칙으로 바꿉니다.
8. 새 정책을 활성화합니다.

9. ILM이 클라우드 스토리지 풀에서 개체를 제거하고 새 위치에 놓을 때까지 기다립니다.

클라우드 스토리지 풀을 삭제합니다

Cloud Storage Pool이 비어 있고 ILM 규칙에 사용되지 않는 경우 삭제할 수 있습니다.

시작하기 전에

- 풀을 사용했을 수 있는 ILM 규칙을 제거했습니다.
- S3 버킷 또는 Azure 컨테이너에 오브젝트가 포함되지 않음을 확인했습니다.

  클라우드 스토리지 풀에 객체가 포함된 경우 해당 풀을 제거하려고 하면 오류가 발생합니다. 을 "클라우드 스토리지 풀 문제 해결"참조하십시오.

> 클라우드 스토리지 풀을 생성할 때 StorageGRID은 마커 파일을 버킷 또는 컨테이너에 작성하여 클라우드 스토리지 풀로 식별합니다. 이름이 인 이 파일은 제거하지 `x-ntap-sgws-cloud-pool-uuid`마십시오.

단계

1. ILM * > * 스토리지 풀 * > * 클라우드 스토리지 풀 * 을 선택합니다.
2. ILM 사용 열에 클라우드 스토리지 풀이 사용되지 않고 있다고 표시되면 확인란을 선택합니다.
3. Actions * > * Remove * 를 선택합니다.
4. OK * 를 선택합니다.

클라우드 스토리지 풀 문제 해결

클라우드 스토리지 풀을 생성, 편집 또는 삭제할 때 발생할 수 있는 오류를 해결하려면 다음 문제 해결 단계를 사용하십시오.

오류가 발생했는지 확인합니다

StorageGRID는 알려진 개체를 읽어 모든 클라우드 스토리지 풀에 대한 간단한 상태 점검을 수행하여 클라우드 스토리지 풀에 `x-ntap-sgws-cloud-pool-uuid` 액세스할 수 있고 올바르게 작동하는지 확인합니다. StorageGRID는 엔드포인트에서 오류가 발생하면 각 스토리지 노드에서 1분마다 상태 점검을 수행합니다. 오류가 해결되면 상태 검사가 중지됩니다. 상태 검사에서 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 엔드포인트를 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: 상태를 확인하지 못했습니다. 끝점에서 오류가 발생했습니다

이 버킷을 클라우드 스토리지 풀에 사용하기 시작한 후 Amazon S3 버킷에 대해 기본 보존으로 S3 오브젝트 잠금을 설정하면 이 오류가 발생할 수 있습니다. 이 오류는 PUT 작업에 과 같은 페이로드 체크섬 값을 가진 HTTP 헤더가 없을 때 `Content-MD5` 발생합니다. 이 헤더 값은 S3 오브젝트 잠금이 설정된 버킷으로 작업을 수행하는 데 AWS에서 필요합니다.

이 문제를 해결하려면 변경하지 않고 의 단계를 "클라우드 스토리지 풀을 편집합니다"수행하십시오. 이 작업은 클라우드 스토리지 풀 엔드포인트 구성에서 S3 오브젝트 잠금 플래그를 자동으로 감지하고 업데이트하는 클라우드 스토리지 풀 구성의 검증을 트리거합니다.

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 마커 파일이 포함되어 있지만 해당 파일에 예상 UUID가 있는 메타데이터 필드가 없는 경우 `x-ntap-sgws-cloud-pool-uuid` 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.
- 파일을 포함하여 타겟 버킷 내의 기존 객체를 모두 삭제하고 `x-ntap-sgws-cloud-pool-uuid` 클라우드 스토리지 풀을 다시 구성해 보십시오.

오류: 클라우드 스토리지 풀을 생성하거나 업데이트할 수 없습니다. 끝점에서 오류가 발생했습니다

다음과 같은 상황에서 이 오류가 발생할 수 있습니다.

- 클라우드 스토리지 풀을 생성하거나 편집하려는 경우
- 새로운 클라우드 스토리지 풀을 구성할 때 S3 Object Lock과 함께 지원되지 않는 플랫폼, 인증 또는 프로토콜 조합을 선택하는 경우 을 "클라우드 스토리지 풀에 대한 고려 사항"참조하십시오.

이 오류는 접속 또는 구성 문제로 인해 StorageGRID가 클라우드 스토리지 풀에 쓸 수 없음을 나타냅니다.

문제를 해결하려면 끝점에서 오류 메시지를 검토하십시오.

- 오류 메시지에 이 포함되어 있으면 `Get *url*: EOF` 클라우드 스토리지 풀에 사용된 서비스 끝점에서 HTTPS가 필요한 컨테이너나 버킷에 대해 HTTP를 사용하지 않는지 확인합니다.
- 오류 메시지에 이 포함되어 있으면 `Get *url*: net/http: request canceled while waiting for connection` 네트워크 구성에서 스토리지 노드가 클라우드 스토리지 풀에 사용되는 서비스 끝점에 액세스할 수 있는지 확인합니다.
- 지원되지 않는 플랫폼, 인증 또는 프로토콜로 인해 오류가 발생한 경우 S3 오브젝트 잠금을 사용하여 지원되는 구성으로 변경하고 새 클라우드 스토리지 풀을 다시 저장해 보십시오.
- 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 마커 파일이 포함되지 `x-ntap-sgws-cloud-pool-uuid` 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. ILM을 통해 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 개체의 라이프사이클"에서 오브젝트를 StorageGRID로 다시 이동하는 지침을 따릅니다.
- 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 끝점 간에 투명하지 않은 스토리지 프록시를 구성한 경우 이 오류가 발생할 수 있습니다. 이 오류는 외부 프록시 서버가 Cloud Storage Pool 끝점에 연결할 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.

오류: **X.509** 인증서의 유효 기간이 만료되었습니다

클라우드 스토리지 풀을 삭제하려고 하면 이 오류가 발생할 수 있습니다. 이 오류는 올바른 외부 클라우드 스토리지 풀의 유효성을 검사하고 클라우드 스토리지 풀 구성이 삭제되기 전에 외부 풀이 비어 있는지 확인하기 위해 인증에 X.509 인증서가 필요할 때 발생합니다.

다음 단계를 수행하여 문제를 해결하십시오.

- 인증을 위해 구성된 인증서를 클라우드 스토리지 풀에 업데이트합니다.
- 이 클라우드 스토리지 풀에 대한 인증서 만료 경고가 모두 해결되었는지 확인합니다.

관련 정보

"Cloud Storage Pool 개체의 수명주기입니다"

삭제 코딩 프로필을 관리합니다

삭제 코딩 프로필에 대한 세부 정보를 보고 필요한 경우 프로필의 이름을 바꿀 수 있습니다. 삭제 코딩 프로필이 현재 ILM 규칙에 사용되지 않는 경우 이 프로필을 비활성화할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "액세스 권한이 필요합니다"있습니다.

삭제 코딩 프로필 세부 정보를 봅니다

삭제 코딩 프로필의 세부 정보를 확인하여 상태, 사용된 삭제 코딩 체계 및 기타 정보를 결정할 수 있습니다.

단계

1. 구성 * > * 시스템 * > * 삭제 코딩 * 을 선택합니다.
2. 프로파일을 선택합니다. 프로필의 상세 페이지가 나타납니다.
3. 필요한 경우 프로필을 사용하는 ILM 규칙 목록과 해당 규칙을 사용하는 ILM 정책을 보려면 ILM 규칙 탭을 참조하십시오.
4. 필요한 경우 스토리지 노드 탭을 확인하여 프로필의 스토리지 풀에 있는 각 스토리지 노드(예: 해당 스토리지 노드가 있는 사이트 및 스토리지 사용량)에 대한 세부 정보를 확인할 수 있습니다.

삭제 코딩 프로필의 이름을 바꿉니다

삭제 코딩 프로필의 이름을 보다 명확하게 지정하여 삭제 코딩 프로필의 이름을 변경할 수 있습니다.

단계

1. 구성 * > * 시스템 * > * 삭제 코딩 * 을 선택합니다.
2. 이름을 바꿀 프로파일을 선택합니다.
3. 이름 바꾸기 * 를 선택합니다.
4. 삭제 코딩 프로필의 고유한 이름을 입력합니다.

   삭제 코딩 프로필 이름은 ILM 규칙의 배치 지침에서 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

삭제 코딩 프로필을 더 이상 사용할 계획이 없고 프로필이 현재 ILM 규칙에 사용되지 않는 경우 삭제 코딩 프로필을 비활성화할 수 있습니다.

> 삭제 코딩된 데이터 복구 작업 또는 서비스 해제 절차가 진행 중이 아닌지 확인합니다. 이러한 작업 중 하나가 진행되는 동안 삭제 코딩 프로필을 비활성화하려고 하면 오류 메시지가 반환됩니다.

이 작업에 대해

StorageGRID는 다음 중 하나에 해당할 경우 삭제 코딩 프로필을 비활성화하지 못하도록 합니다.

- 삭제 코딩 프로필이 현재 ILM 규칙에서 사용되고 있습니다.
- 삭제 코딩 프로필은 더 이상 ILM 규칙에서 사용되지 않지만 프로필에 대한 오브젝트 데이터 및 패리티 조각은 여전히 존재합니다.

단계

1. 구성 * > * 시스템 * > * 삭제 코딩 * 을 선택합니다.
2. 활성 탭에서 * 상태 * 열을 검토하여 비활성화하려는 삭제 코딩 프로필이 ILM 규칙에 사용되지 않는지 확인합니다.

   삭제 코딩 프로파일을 ILM 규칙에 사용하는 경우 비활성화할 수 없습니다. 이 예에서 2+1 Data Center 1 프로필은 하나 이상의 ILM 규칙에 사용됩니다.

Profile name	Status	Storage pool	Erasure-coding scheme
2+1 Data Center 1	Used in 5 rules	Data Center 1	2+1
New profile	Deactivated	Data Center 1	2+1

3. ILM 규칙에서 프로파일을 사용하는 경우 다음 단계를 따릅니다.

a. ILM * > * 규칙 * 을 선택합니다.

b. 각 규칙을 선택하고 보존 다이어그램을 검토하여 비활성화하려는 삭제 코딩 프로필을 규칙이 사용하는지 확인합니다.

c. ILM 규칙이 비활성화하려는 삭제 코딩 프로필을 사용하는 경우 해당 규칙이 ILM 정책에 사용되고 있는지 확인합니다.

d. 삭제 코딩 프로필이 사용되는 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"
현재 활성 ILM 정책에 있는 ILM 규칙입니다	i. 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. 삭제 코딩 프로파일이 데이터와 연결되어 있는 동안 안전하게 비활성화할 수 있지만 비활성화 작업은 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"

프로필은 어디에 사용되었습니까?	프로필을 비활성화하기 전에 수행할 추가 단계입니다	다음 추가 지침을 참조하십시오
현재 ILM 정책에 있는 ILM 규칙입니다	i. 정책을 편집합니다. ii. 삭제 코딩 프로필을 사용하는 ILM 규칙을 제거합니다. iii. 하나 이상의 새 ILM 규칙을 추가하여 모든 개체가 보호되도록 합니다. iv. 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"

e. 삭제 - 코딩 프로필 페이지를 새로 고쳐 프로필이 ILM 규칙에 사용되지 않도록 합니다.

4. 프로파일이 ILM 규칙에 사용되지 않으면 라디오 버튼을 선택하고 * Deactivate * 를 선택합니다. 삭제 코딩 프로필 비활성화 대화 상자가 나타납니다.

> 각 프로파일이 어떤 규칙에서도 사용되지 않는 한 여러 개의 프로파일을 선택하여 동시에 비활성화할 수 있습니다.

5. 프로필을 비활성화하려면 * Deactivate * 를 선택합니다.

결과

- StorageGRID에서 삭제 코딩 프로필을 비활성화할 수 있는 경우 상태는 Deactivated입니다. 더 이상 ILM 규칙에 대해 이 프로파일을 선택할 수 없습니다. 비활성화된 프로필은 다시 활성화할 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.

> 버킷이 생성된 후에는 버킷 영역을 변경할 수 없습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

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, 해당 지역에서 생성된 S3 버킷의 오브젝트에만 적용되는 규칙을 설계할 수 `us-west-2` 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 해당 지역에 속하는 것으로 `us-east-1` 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 구분합니다. 유효한 문자는 숫자, 문자 및 하이픈입니다.

> EU는 EU-West-1의 별칭으로 간주되지 않습니다. EU 또는 EU-West-1 지역을 사용하려면 정확한 이름을 사용해야 합니다.

- 모든 정책에 할당된 규칙(활성 또는 비활성)에서 사용되는 영역은 삭제하거나 수정할 수 없습니다.
- ILM 규칙의 고급 필터로 잘못된 영역을 사용하는 경우 해당 규칙을 정책에 추가할 수 없습니다.

  ILM 규칙에서 영역을 고급 필터로 사용하지만 나중에 해당 영역을 삭제하거나 Grid Management API를 사용하여 규칙을 만들고 정의되지 않은 영역을 지정하면 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 수정하거나 제거할 수 없는 기본 지역을 `us-east-1` 표시합니다.

2. 영역을 추가하려면:
   a. Add another region * 을 선택합니다.
   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 정책에서 사용 중인 영역(활성 또는 비활성)을 제거하려고 하면 오류 메시지가 나타납니다.

4. 변경을 완료하면 * Save * 를 선택합니다.

   이제 ILM 규칙 만들기 마법사의 1단계에 있는 고급 필터 섹션에서 이러한 영역을 선택할 수 있습니다. 을 "ILM 규칙에서 고급 필터를 사용합니다"참조하십시오.

ILM 규칙을 생성합니다

ILM 규칙을 사용하여 오브젝트를 관리합니다

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.

> 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.

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 Behavior *: 규칙의 수집 동작을 통해 규칙에 의해 필터링된 객체가 수집될 때 보호되는 방식을 선택할 수 있습니다(S3 클라이언트가 객체를 그리드에 저장하는 경우).

ILM 규칙 필터링

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. 이러한 필터를 사용하면 특정 테넌트 계정, 특정 S3 버킷 또는 둘 다에 규칙을 적용할 수 있습니다.

  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.

- 고급 필터를 통해 세밀한 제어가 가능합니다. 필터를 만들어 다음 개체 속성을 기준으로 개체를 선택할 수 있습니다.
  - 수집 시간
  - 마지막 액세스 시간입니다
  - 개체 이름의 전체 또는 일부(키)
  - 위치 제약 조건(S3만 해당)
  - 개체 크기

- 사용자 메타데이터
- 오브젝트 태그(S3만 해당)

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 필터를 단일 규칙으로 결합할 수 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 만드는 한편, 각 규칙의 필터를 사용하여 규칙이 적용되는 특정 유형의 개체를 식별할 수 있습니다.

ILM 규칙 배치 지침

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.

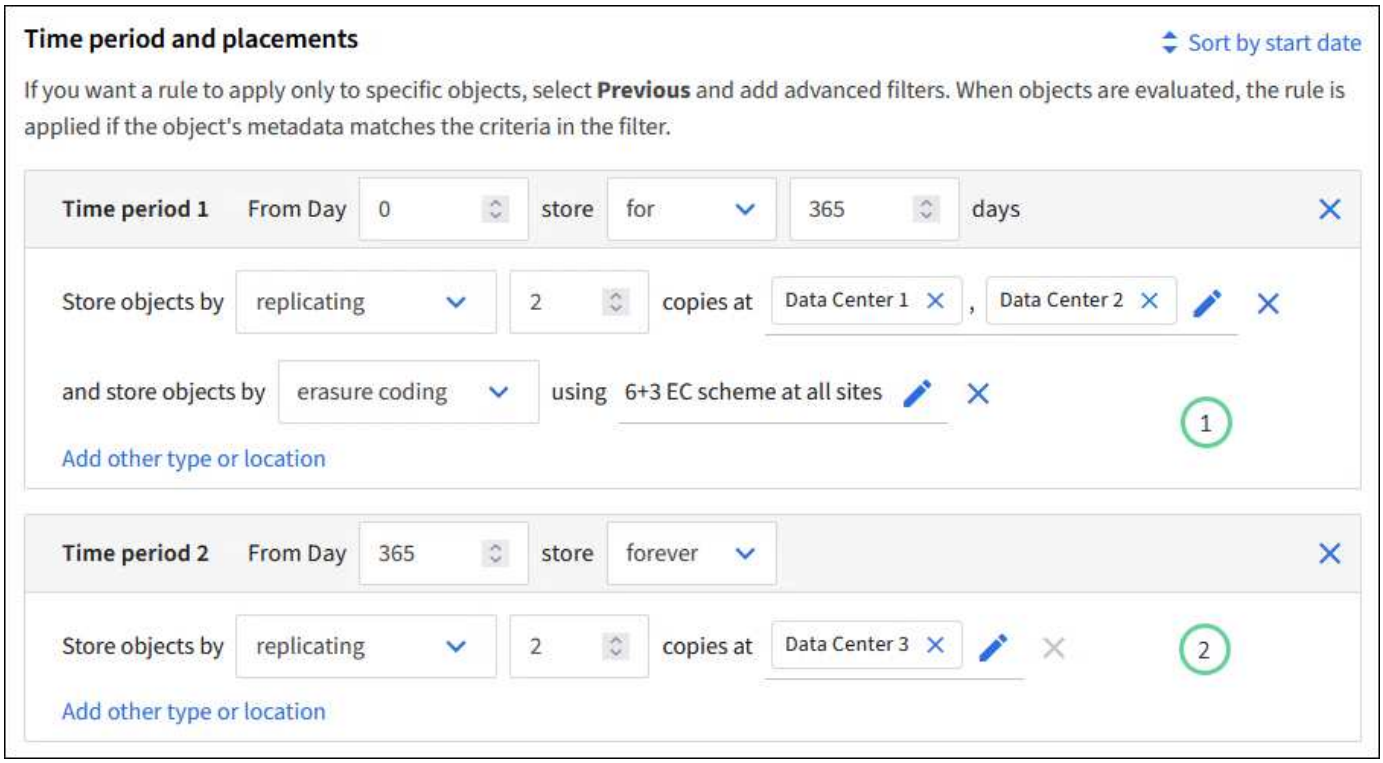
배치 지침을 작성할 때:

- 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 * 다른 유형 또는 위치 추가 * 를 선택하여 해당 기간에 대해 두 개 이상의 라인을 추가합니다.
- 다른 기간의 다른 위치에 오브젝트를 배치하려면 * 다른 기간 추가 * 를 선택하여 다음 기간을 추가합니다. 그런 다음 기간 내에 하나 이상의 라인을 지정합니다.

이 예에서는 ILM 규칙 생성 마법사의 배치 정의 페이지에 있는 두 가지 배치 지침을 보여 줍니다.



첫 번째 배치 지침에는 (1) 첫 해에 대한 두 줄이 있습니다.

- 첫 번째 줄에서는 두 개의 데이터 센터 사이트에 두 개의 복제된 개체 복사본을 만듭니다.
- 두 번째 줄에서는 모든 데이터 센터 사이트를 사용하여 6+3 삭제 코딩 복사본을 생성합니다.

두 번째 배치 지침에서는 (2) 1년 후에 두 개의 복사본을 만들고 이 복사본을 영구적으로 유지합니다.

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 수집 동작

수집 동작은 규칙의 지침에 따라 오브젝트 복사본을 즉시 배치할지, 중간 복사본을 만들어 나중에 배치 지침을 적용할지 여부를 제어합니다. ILM 규칙에 대해 다음과 같은 수집 동작을 사용할 수 있습니다.

- * 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.
- * Strict * : ILM 규칙에 지정된 모든 사본은 클라이언트에 반환되기 전에 만들어야 합니다.
- * 이중 커밋 *: StorageGRID은 즉시 개체의 임시 복사본을 만들고 클라이언트에 성공을 반환합니다. ILM 규칙에 지정된 복사본은 가능한 경우 만들어집니다.

관련 정보

- "수집 옵션"

- "수집 옵션의 장점, 단점 및 제한 사항"
- "일관성과 ILM 규칙이 데이터 보호에 영향을 미치는 방식"

ILM 규칙 예

예를 들어 ILM 규칙에서 다음을 지정할 수 있습니다.

- 테넌트 A에 속하는 객체에만 적용합니다
- 이러한 개체의 복제 복사본을 두 개 만들고 각 복사본을 다른 사이트에 저장합니다.
- 두 개의 복사본을 "영원히" 보존합니다. 즉, StorageGRID에서 자동으로 삭제하지 않습니다. 대신, StorageGRID는 이러한 객체가 클라이언트 삭제 요청에 의해 삭제되거나 버킷 수명 주기가 만료될 때까지 해당 객체를 유지합니다.
- 수집 동작에 균형 옵션을 사용합니다. 필요한 두 복제본을 모두 즉시 생성할 수 없는 경우 테넌트 A가 StorageGRID에 객체를 저장하는 즉시 2개 사이트 배치 명령이 적용됩니다.

  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

- "스토리지 풀이란 무엇입니까"
- "클라우드 스토리지 풀이란 무엇입니까"

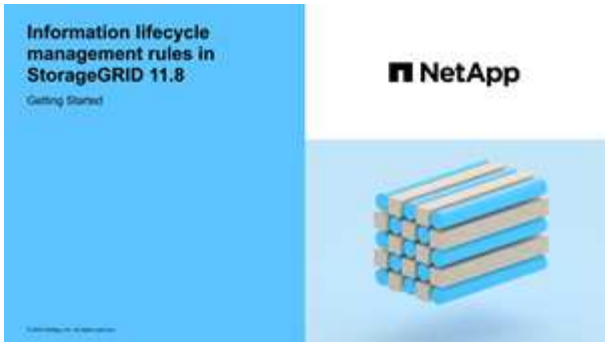
ILM 규칙 만들기 마법사에 액세스합니다

ILM 규칙을 사용하여 시간에 따른 오브젝트 데이터 배치를 관리할 수 있습니다. ILM 규칙을 만들려면 ILM 규칙 만들기 마법사를 사용합니다.

정책에 대한 기본 ILM 규칙을 생성하려면 대신 를 "기본 ILM 규칙 생성에 대한 지침"따르십시오.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"
- 이 규칙이 적용되는 테넌트 계정을 지정하려면 "테넌트 계정 권한"각 계정의 계정 ID를 알고 있어야 합니다.
- 규칙이 마지막 액세스 시간 메타데이터에서 오브젝트를 필터링하도록 하려면 S3 버킷에서 마지막 액세스 시간 업데이트를 활성화해야 합니다.
- 사용할 클라우드 스토리지 풀을 구성했습니다. 을 "클라우드 스토리지 풀을 생성합니다"참조하십시오.
- 에 대해 잘 알고 "수집 옵션"있습니다.
- S3 오브젝트 잠금과 함께 사용할 규정 준수 규칙을 생성해야 하는 경우 에 익숙합니다."S3 오브젝트 잠금에 대한 요구사항"
- 선택적으로 비디오를 시청했습니다 "비디오: ILM 규칙 개요".



이 작업에 대해

ILM 규칙 생성 시:

- StorageGRID 시스템의 토폴로지 및 스토리지 구성을 고려하십시오.
- 만들려는 오브젝트 복사본의 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.
- 사용할 수집 옵션(균형, 엄격 또는 이중 커밋)을 결정합니다.

단계

1. ILM * > * 규칙 * 을 선택합니다.
2. Create * 를 선택합니다. "1단계(세부 정보 입력)" ILM 규칙 생성 마법사가 나타납니다.

단계 **1/3:** 세부 정보를 입력합니다

ILM 규칙 만들기 마법사의 * 세부 정보 입력 * 단계를 사용하면 규칙에 대한 이름과 설명을 입력하고 규칙에 대한 필터를 정의할 수 있습니다.

규칙에 대한 설명을 입력하고 필터를 정의하는 것은 선택 사항입니다.

이 작업에 대해

에 대해 개체를 평가할 때 "ILM 규칙"StorageGRID는 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.
2. 필요에 따라 * Description * (설명 *) 필드에 규칙에 대한 간단한 설명을 입력합니다.

   나중에 규칙을 인식할 수 있도록 규칙의 목적 또는 기능을 설명해야 합니다.

3. 필요에 따라 이 규칙이 적용될 S3 테넌트 계정을 하나 이상 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. 필요한 경우 이 규칙이 적용되는 S3 버킷을 지정합니다.

   모든 버킷에 적용 * 이 선택된 경우(기본값) 모든 S3 버킷에 규칙이 적용됩니다.

5. S3 테넌트의 경우 선택적으로 * 예 * 를 선택하여 버전 관리가 활성화된 S3 버킷의 이전 오브젝트 버전에만 규칙을 적용합니다.

   예 * 를 선택하면 의 참조 시간으로 "비현재 시간"이 자동으로 "ILM 규칙 만들기 마법사의 2단계"선택됩니다.

   > 현재 시간이 아닌 시간은 버전 관리가 활성화된 버킷의 S3 오브젝트에만 적용됩니다. "버킷 작업, PutBucketVersioning"및 을 "S3 오브젝트 잠금으로 오브젝트 관리"참조하십시오.

   이 옵션을 사용하면 버전이 아닌 개체 버전을 필터링하여 버전이 지정된 개체의 스토리지 영향을 줄일 수 있습니다. 을 "예 4: S3 버전 오브젝트에 대한 ILM 규칙 및 정책"참조하십시오.

6. 선택적으로 * 고급 필터 추가 * 를 선택하여 추가 필터를 지정합니다.

   고급 필터링을 구성하지 않으면 기본 필터와 일치하는 모든 개체에 규칙이 적용됩니다. 고급 필터링에 대한 자세한 내용은 ILM 규칙에서 고급 필터를 사용합니다 및 여러 메타데이터 유형과 값을 지정합니다를 참조하십시오.

7. Continue * 를 선택합니다. "2단계(배치 정의)" ILM 규칙 생성 마법사가 나타납니다.

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	• 있습니다 • 그렇지 않습니다 • 않습니다 • 이(가) 켜져 있거나 이전에 있습니다 • 그 이후입니다 • 이(가) 켜져 있거나 이후에 있습니다	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 오브젝트 키의 전체 또는 일부. 예를 들어 로 끝나거나 로 시작하는 `test-object/` 개체를 일치시킬 수 `.txt` 있습니다.
마지막 액세스 시간입니다	• 있습니다 • 그렇지 않습니다 • 않습니다 • 이(가) 켜져 있거나 이전에 있습니다 • 그 이후입니다 • 이(가) 켜져 있거나 이후에 있습니다	개체를 마지막으로 검색한 시간 및 날짜(읽기 또는 보기). • 참고: * 고급 필터로 사용하려는 경우 "마지막 액세스 시간을 사용합니다"S3 버킷에 대해 마지막 액세스 시간 업데이트를 활성화해야 합니다.
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. 을 "영역 구성(옵션 및 S3만 해당)"참조하십시오.
개체 크기	• 같음 • 같지 않습니다 • 보다 작음 • 보다 작거나 같음 • 보다 큼 • 보다 크거나 같음	개체의 크기입니다. 삭제 코딩은 1MB 이상의 오브젝트에 가장 적합합니다. 매우 작은 삭제 코딩 조각을 관리해야 하는 오버헤드를 방지하기 위해 200KB 미만의 오브젝트에 삭제 코딩을 사용하지 마십시오.

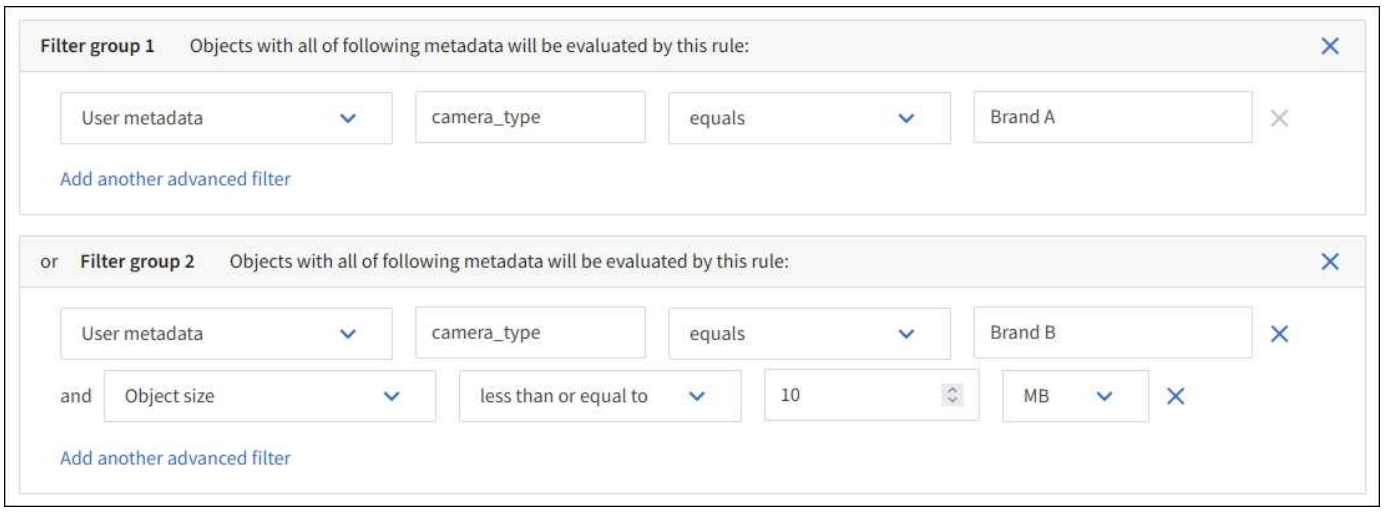
메타데이터 유형입니다	지원되는 연산자	메타데이터 값입니다
사용자 메타데이터	• 포함 • 로 끝납니다 • 같음 • 있습니다 • 로 시작합니다 • 포함하지 않음 • 로 끝나지는 않습니다 • 같지 않습니다 • 존재하지 않습니다 • 로 시작하지 않습니다	키 값 쌍. 여기서 * 사용자 메타데이터 이름 * 은 키이고 * 메타데이터 값 * 은 값입니다. 예를 들어 사용자 메타데이터가 있는 객체를 필터링하려면 `color=blue` `color` * 사용자 메타데이터 이름 *, 연산자 및 `blue` * 메타데이터 `equals` 값 * 을 지정합니다. • 참고: * 사용자 메타데이터 이름은 대/소문자를 구분하지 않으며 사용자 메타데이터 값은 대/소문자를 구분합니다.
오브젝트 태그(S3만 해당)	• 포함 • 로 끝납니다 • 같음 • 있습니다 • 로 시작합니다 • 포함하지 않음 • 로 끝나지는 않습니다 • 같지 않습니다 • 존재하지 않습니다 • 로 시작하지 않습니다	키 값 쌍. 여기서 * 개체 태그 이름 * 은 키이고 * 개체 태그 값 * 은 값입니다. 예를 들어, 오브젝트 태그가 인 오브젝트를 필터링하려면 `Image=True` * 오브젝트 태그 이름 *, 연산자에 대해 `True` * 오브젝트 태그 값 * `equals` 을 `Image` 지정합니다. • 참고: * 개체 태그 이름 및 개체 태그 값은 대/소문자를 구분합니다. 이러한 항목은 개체에 대해 정의된 대로 정확하게 입력해야 합니다.

여러 메타데이터 유형과 값을 지정합니다

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 CAMERA_TYPE 사용자 메타데이터의 값으로 브랜드 A 또는 브랜드 B가 있는 개체에 적용됩니다. 그러나 이 규칙은 10MB보다 작은 브랜드 B 객체에만 적용됩니다.



단계 **2/3:** 배치 정의

ILM 규칙 생성 마법사의 * 배치 정의 * 단계를 통해 객체 저장 기간, 복제본 유형(복제 또는 삭제 코딩), 저장 위치 및 복제본 수를 결정하는 배치 지침을 정의할 수 있습니다.

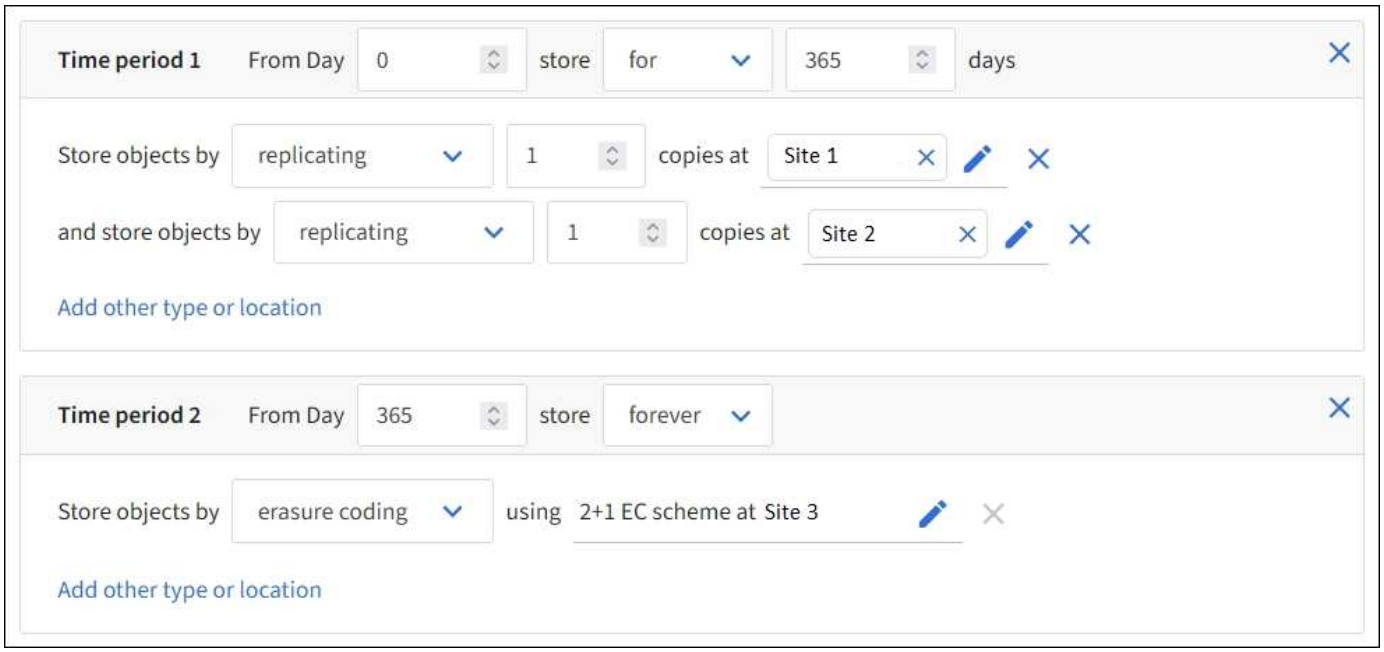
표시된 스크린샷은 예시입니다. 결과는 StorageGRID 버전에 따라 다를 수 있습니다.

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 예에서 ILM 규칙은 복제된 복사본 하나를 사이트 1에 저장하고 복제된 복사본을 사이트 2에 1년간 저장합니다. 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) 이 옵션을 사용하려면 S3 버킷에 대해 마지막 액세스 시간에 대한 업데이트를 활성화해야 합니다. 을 "ILM 규칙에서 마지막 액세스 시간을 사용합니다"참조하십시오.
사용자 정의 생성 시간입니다	사용자 정의 메타데이터에 지정된 시간입니다.
현재 시간이 아닙니다	에서 "버전 관리가 활성화된 S3 버켓의 이전 오브젝트 버전에만 이 규칙 적용" 질문에 대해 * 예 * 를 선택한 경우 "비현재 시간"이 자동으로 선택됩니다"ILM 규칙 만들기 마법사의 1단계".

_compliant_rule을 생성하려면 * Ingest Time * 을 선택해야 합니다. 을 "S3 오브젝트 잠금으로 오브젝트 관리 "참조하십시오.

2. 시간 간격 및 배치 * 섹션에서 시작 시간과 첫 번째 기간의 기간을 입력합니다.

   예를 들어, 첫 번째 연도의 오브젝트를 저장할 위치를 지정할 수 있습니다(_365일의 경우 0일 점포 _). 적어도 하나의 명령은 0일에 시작해야 합니다.

3. 복제된 복사본을 생성하려면 다음을 수행합니다.

   a. Store objects by *(개체 저장 기준 *) 드롭다운 목록에서 * Replicating *(복제 *)을 선택합니다.

   b. 복사할 매수를 선택합니다.

매수를 1로 변경하면 경고가 나타납니다. 특정 기간 동안 복제된 복사본을 하나만 생성하는 ILM 규칙은 데이터가 영구적으로 손실될 위험이 있습니다. 을 "단일 복사본 복제를 사용하지 않아야 하는 이유 "참조하십시오.

위험을 방지하려면 다음 중 하나 이상을 수행하십시오.

- 해당 기간의 사본 수를 늘립니다.
- 다른 스토리지 풀 또는 클라우드 스토리지 풀에 복사본을 추가합니다.
- 복제 * 대신 * 삭제 코딩 * 을 선택하십시오.

  이 규칙이 모든 기간에 대해 여러 복사본을 이미 생성한 경우 이 경고를 무시해도 됩니다.

c. copies at * 필드에서 추가할 스토리지 풀을 선택합니다.

- 스토리지 풀을 하나만 지정하는 경우 * StorageGRID는 지정된 스토리지 노드에 복제된 객체 복사본을 하나만 저장할 수 있습니다. 그리드에 스토리지 노드 3개가 포함되어 있고 복제본 수로 4를 선택한 경우 복제본 3개만 생성하고 각 스토리지 노드에 대해 복제본 1개를 생성합니다.

  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 모든 스토리지 노드 스토리지 풀(StorageGRID 11.6 이하)과 다른 스토리지 풀을 지정하지 마십시오.

4. 삭제 코딩 복사본을 만들려면:

a. Store objects by * (개체 저장 기준 *) 드롭다운 목록에서 * 삭제 코딩 * 을 선택합니다.

> 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. 200KB보다 큰 값에 대해 개체 크기 필터를 추가하지 않은 경우 * Previous * 를 선택하여 1단계로 돌아갑니다. 그런 다음 * 고급 필터 추가 * 를 선택하고 * 개체 크기 * 필터를 200KB보다 큰 값으로 설정합니다.

c. 추가할 스토리지 풀 및 사용할 삭제 코딩 체계를 선택합니다.

  삭제 코딩 복사본의 스토리지 위치에는 삭제 코딩 체계의 이름과 스토리지 풀의 이름이 차례로 포함됩니다.

사용 가능한 삭제 코딩 체계는 선택한 스토리지 풀에 있는 스토리지 노드의 수에 따라 제한됩니다. `Recommended`배지가 을 제공하는 구성표 옆에 "최상의 보호 또는 스토리지 오버헤드"나타납니다.

5. 선택 사항:

a. 다른 위치에 사본을 추가로 생성하려면 * 다른 유형 또는 위치 추가 * 를 선택합니다.

b. 다른 기간을 추가하려면 * 다른 기간 추가 * 를 선택합니다.

개체는 다음 설정에 따라 삭제됩니다.

- 다른 기간이 * Forever * 로 끝나지 않는 한 개체는 최종 기간이 끝날 때 자동으로 삭제됩니다.
- 에 따라 "버킷 및 테넌트 보존 기간 설정"ILM 보존 기간이 종료되어도 개체가 삭제되지 않을 수 있습니다.

6. 클라우드 스토리지 풀에 오브젝트를 저장하려면 다음을 수행합니다.
   a. Store objects by *(개체 저장 기준 *) 드롭다운 목록에서 * Replicating *(복제 *)을 선택합니다.
   b. 매수 * 필드를 선택한 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.
      - 오브젝트를 StorageGRID에서 복제 또는 삭제 코딩 복사본으로 저장하는 동시에 클라우드 스토리지 풀에 저장할 수 있습니다. 그러나 해당 기간의 배치 지침에는 여러 줄을 포함해야 각 위치에 대한 사본의 수와 유형을 지정할 수 있습니다.

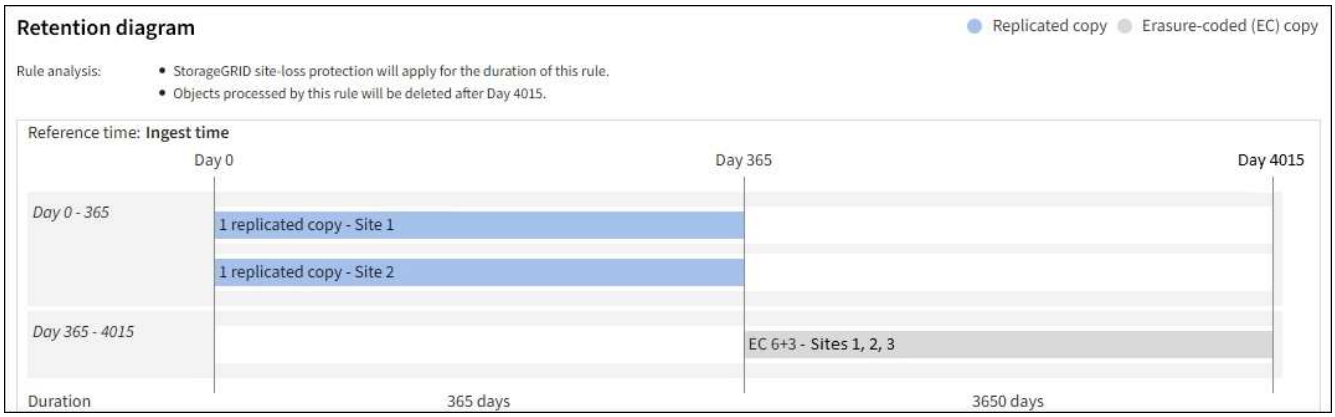
7. 고정 다이어그램에서 배치 지침을 확인합니다.

   이 예에서 ILM 규칙은 복제된 복사본 하나를 사이트 1에 저장하고 복제된 복사본을 사이트 2에 1년간 저장합니다. 1년 후 10년 동안 삭제 코딩 복사본을 6개 이상의 3개 사이트에 저장할 수 있습니다. 총 11년이 지나면 StorageGRID에서 객체가 삭제됩니다.

   보존 다이어그램의 규칙 분석 섹션에 나와 있는 내용은 다음과 같습니다.

   - StorageGRID 사이트 손실 보호는 이 규칙 기간 동안 적용됩니다.
   - 이 규칙에 의해 처리된 객체는 Day 4015 이후에 삭제됩니다.

     을 참조하십시오 "사이트 손실 방지"



8. Continue * 를 선택합니다. "3단계(수집 동작 선택)" ILM 규칙 생성 마법사가 나타납니다.

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 개체의 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 필터로 사용하거나 참조 시간으로 사용하는 경우 S3 버킷에 대한 마지막 액세스 시간 업데이트를 활성화해야 합니다. 또는 을 사용할 수 "테넌트 관리자""테넌트 관리 API"있습니다.

  S3 버킷의 경우 마지막 액세스 시간 업데이트가 기본적으로 해제되어 있습니다.

  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 시간이 업데이트되는지 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

3단계 중 **3**단계**:** 수집 동작을 선택합니다

ILM 규칙 생성 마법사의 * 수집 동작 선택 * 단계를 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. 사용할 을 선택합니다"수집 동작".

   자세한 내용은 을 "수집 옵션의 장점, 단점 및 제한 사항"참조하십시오.

   > 규칙에서 다음 배치 중 하나를 사용하는 경우 균형 또는 엄격 옵션을 사용할 수 없습니다.
   >
   > ◦ 0일의 클라우드 스토리지 풀
   > ◦ 규칙이 사용자 정의 생성 시간을 참조 시간으로 사용하는 경우 클라우드 스토리지 풀입니다
   >
   > 을 "예 5: 엄격한 수집 동작을 위한 ILM 규칙 및 정책"참조하십시오.

2. Create * 를 선택합니다.

   ILM 규칙이 생성됩니다. 규칙이 에 추가되고 해당 정책이 활성화될 때까지 이 규칙이 "ILM 정책"활성화되지 않습니다.

   규칙의 세부 정보를 보려면 ILM 규칙 페이지에서 규칙 이름을 선택합니다.

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

이 작업에 대해

기본 규칙은 ILM 정책에서 평가할 마지막 규칙이므로 필터를 사용할 수 없습니다. 기본 규칙의 배치 지침은 정책의 다른 규칙과 일치하지 않는 모든 개체에 적용됩니다.

이 예제 정책에서 첫 번째 규칙은 test-tenant-1에 속하는 객체에만 적용됩니다. 마지막 기본 규칙은 다른 모든 테넌트 계정에 속한 개체에 적용됩니다.

기본 규칙을 만들 때 다음 요구 사항을 염두에 두십시오.

- 기본 규칙은 정책에 추가할 때 자동으로 마지막 규칙으로 배치됩니다.
- 기본 규칙에서는 기본 필터 또는 고급 필터를 사용할 수 없습니다.
- 기본 규칙은 모든 개체 버전에 적용되어야 합니다.
- 기본 규칙은 복제된 복사본을 만들어야 합니다.

> 삭제 코딩 복사본을 정책의 기본 규칙으로 만드는 규칙을 사용하지 마십시오. 삭제 코딩 규칙은 고급 필터를 사용하여 작은 오브젝트가 삭제 코딩되지 않도록 해야 합니다.

- 일반적으로 기본 규칙은 개체를 영구적으로 유지해야 합니다.
- 글로벌 S3 오브젝트 잠금 설정을 사용 중이거나 사용할 계획인 경우 기본 규칙이 준수되어야 합니다.

단계

1. ILM * > * 규칙 * 을 선택합니다.
2. Create * 를 선택합니다.

   ILM 규칙 생성 마법사의 1단계(세부 정보 입력)가 나타납니다.

3. 규칙 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(버킷 이름) 드롭다운 선택 항목을 * Apply to all Bucket(모든 버킷에 적용) * 으로 둡니다.

   기본 규칙은 모든 S3 버킷에 적용되어야 합니다.

7. "버전 관리가 활성화된 S3 버킷의 이전 개체 버전에만 이 규칙을 적용하시겠습니까?"라는 질문에 대해 기본 답변 * 아니요 * 를 유지합니다.
8. 고급 필터를 추가하지 마십시오.

   기본 규칙은 필터를 지정할 수 없습니다.

9. 다음 * 을 선택합니다.

   2단계(배치 정의)가 나타납니다.

10. 참조 시간 으로 원하는 옵션을 선택합니다.

    "이전 개체 버전에만 이 규칙을 적용하시겠습니까?"라는 질문에 대해 기본 대답 * 아니요 * 를 유지했다면 비현재 시간은 풀다운 목록에 포함되지 않습니다. 기본 규칙은 모든 개체 버전을 적용해야 합니다.

11. 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 작은 객체가 삭제 코딩되지 않도록 하기 위해 200KB보다 큰 * 객체 크기(MB) * 고급 필터가 포함되어야 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.
- Ingest Time을 참조 시간으로 사용하여 배치 지침의 최소 한 줄이 0일에 시작되어야 합니다.
- 배치 지침의 최소 한 줄은 "영구"여야 합니다.

12. 고정 다이어그램을 참조하여 배치 지침을 확인합니다.
13. Continue * 를 선택합니다.

    3단계(수집 동작 선택)가 나타납니다.

14. 사용할 수집 옵션을 선택하고 * 생성 * 을 선택합니다.

ILM 정책 관리

ILM 정책 사용

ILM(정보 수명 주기 관리) 정책은 StorageGRID 시스템이 시간 경과에 따라 오브젝트 데이터를 관리하는 방법을 결정하는 일련의 정렬된 ILM 규칙 세트입니다.

> 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.

기본 ILM 정책

StorageGRID를 설치하고 사이트를 추가하면 다음과 같은 기본 ILM 정책이 자동으로 생성됩니다.

- 눈금에 사이트가 한 개 포함된 경우 기본 정책에는 해당 사이트에서 각 개체의 복사본을 두 개 복제하는 기본 규칙이 포함됩니다.
- 그리드에 사이트가 두 개 이상 포함된 경우 기본 규칙은 각 사이트에 있는 각 개체의 복사본을 하나씩 복제합니다.

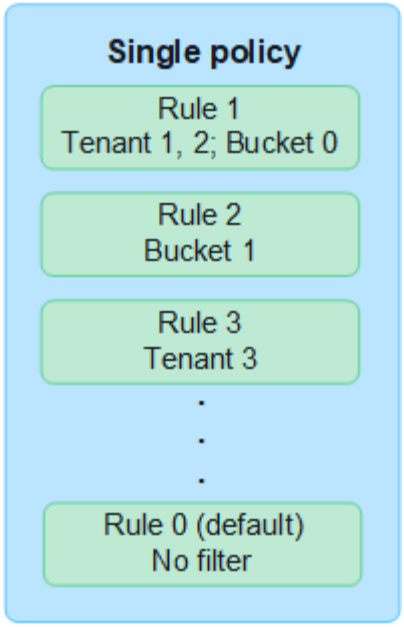
기본 정책이 스토리지 요구 사항을 충족하지 않는 경우 고유한 규칙 및 정책을 생성할 수 있습니다. "ILM 규칙을 생성합니다"및 을 "ILM 정책을 생성합니다"참조하십시오.

활성 ILM 정책이 하나 이상 있습니까?

한 번에 하나 이상의 활성 ILM 정책을 가질 수 있습니다.

하나의 정책

그리드에서 몇 가지 테넌트별 및 버킷별 규칙이 포함된 간단한 데이터 보호 체계를 사용할 경우 활성 ILM 정책을 하나 사용합니다. ILM 규칙에는 다양한 버킷 또는 테넌트를 관리하기 위한 필터가 포함될 수 있습니다.



하나의 정책만 있고 테넌트의 요구 사항이 변경된 경우 새 ILM 정책을 생성하거나 기존 정책을 복제하여 변경 사항을 적용하고 시뮬레이션한 다음 새 ILM 정책을 활성화해야 합니다. ILM 정책을 변경하면 오브젝트 이동이 수행되어 며칠이 소요되고 시스템 지연 시간이 발생할 수 있습니다.

다수의 정책

테넌트에 다양한 서비스 품질 옵션을 제공하기 위해 한 번에 두 개 이상의 활성 정책을 사용할 수 있습니다. 각 정책은 특정 테넌트, S3 버킷 및 오브젝트를 관리할 수 있습니다. 특정 테넌트 또는 오브젝트 세트에 대해 하나의 정책을 적용하거나 변경해도 다른 테넌트 및 오브젝트에 적용되는 정책은 영향을 받지 않습니다.

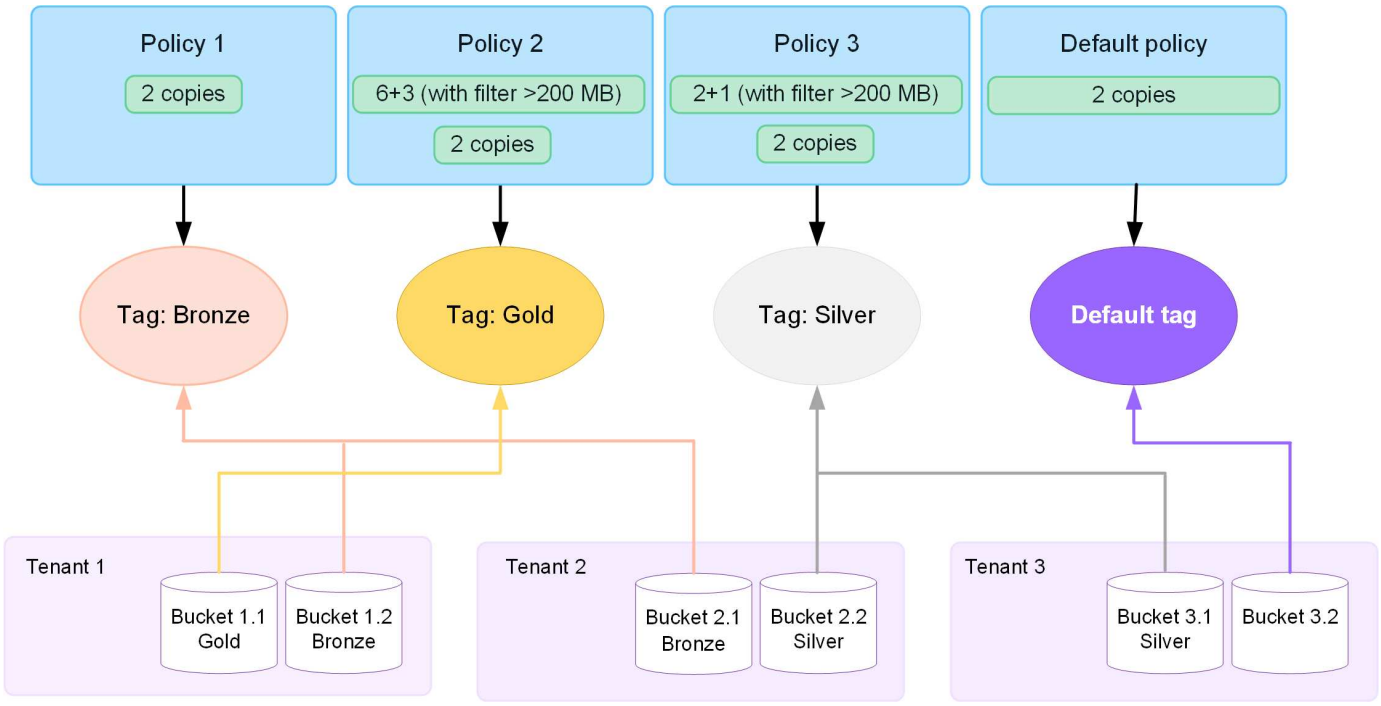
ILM 정책 태그

테넌트가 버킷별로 여러 데이터 보호 정책 간에 쉽게 전환할 수 있도록 하려면 _ ILM 정책 태그 _ 를 사용하여 여러 ILM 정책을 사용하십시오. 각 ILM 정책을 태그에 할당한 다음 테넌트는 버킷에 태그를 지정하여 해당 버킷에 정책을 적용합니다. S3 버킷에만 ILM 정책 태그를 설정할 수 있습니다.

예를 들어 골드, 실버, 브론즈라는 세 개의 태그가 있을 수 있습니다. 정책이 오브젝트를 저장하는 위치와 기간에 따라 각 태그에 ILM 정책을 할당할 수 있습니다. 테넌트는 버킷에 태그를 지정하여 사용할 정책을 선택할 수 있습니다. Bucket Tagged Gold는 Gold 정책에 의해 관리되며 Gold 레벨의 데이터 보호 및 성능을 받습니다.

기본 **ILM** 정책 태그입니다

기본 ILM 정책 태그는 StorageGRID를 설치할 때 자동으로 생성됩니다. 모든 그리드에는 Default 태그에 할당된 활성 정책이 하나 있어야 합니다. 기본 정책은 태그가 지정되지 않은 모든 S3 버킷에 적용됩니다.



ILM 정책은 개체를 어떻게 평가합니까**?**

활성 ILM 정책은 오브젝트의 배치, 기간 및 데이터 보호를 제어합니다.

클라이언트가 StorageGRID에 개체를 저장하면 다음과 같이 정책의 순서가 지정된 ILM 규칙 집합을 기준으로 개체가 평가됩니다.

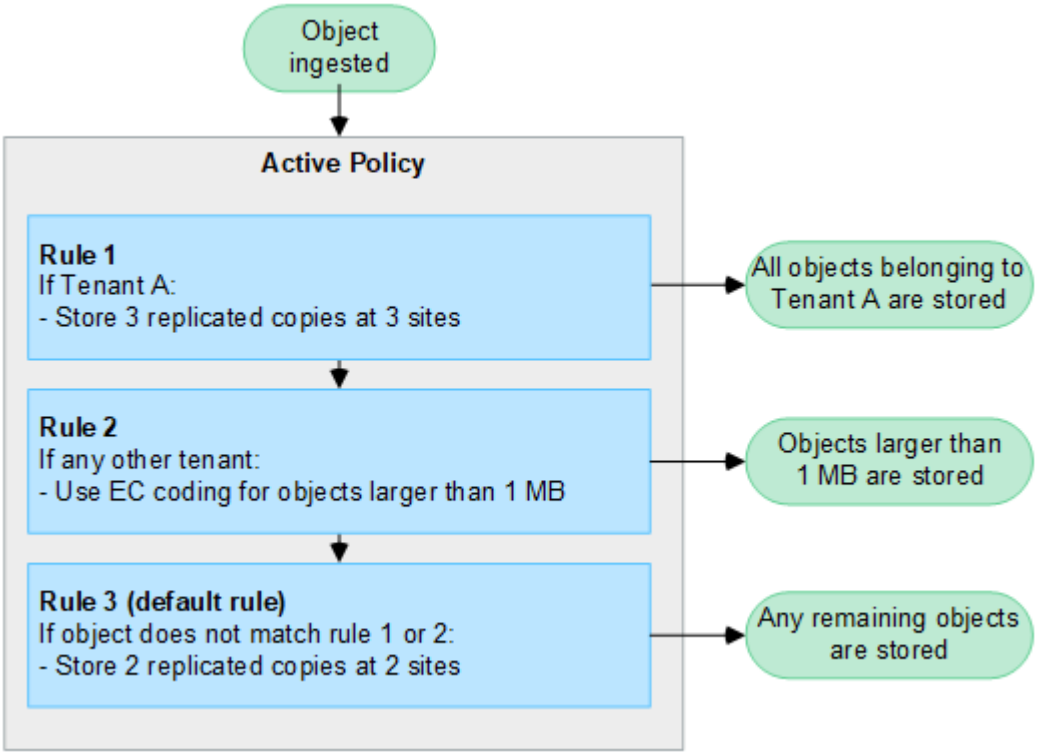
1. 정책의 첫 번째 규칙에 대한 필터가 개체와 일치하면 해당 규칙의 수집 동작에 따라 개체가 수집되고 해당 규칙의 배치 지침에 따라 저장됩니다.
2. 첫 번째 규칙의 필터가 개체와 일치하지 않으면 일치가 이루어질 때까지 해당 개체가 정책의 다음 각 규칙에 대해 평가됩니다.
3. 개체와 일치하는 규칙이 없으면 정책의 기본 규칙에 대한 수집 동작 및 배치 지침이 적용됩니다. 기본 규칙은 정책의 마지막 규칙입니다. 기본 규칙은 모든 테넌트, 모든 S3 버킷 및 모든 오브젝트 버전에 적용되어야 하며 고급 필터를 사용할 수 없습니다.

ILM 정책의 예

예를 들어 ILM 정책에 다음을 지정하는 세 가지 ILM 규칙이 포함될 수 있습니다.

- * 규칙 1: 테넌트 A * 에 대해 복제된 복사본
  - 테넌트 A에 속하는 모든 객체를 일치시킵니다
  - 이러한 객체를 3개의 사이트에 3개의 복제된 복제본으로 저장합니다.
  - 다른 테넌트에 속한 개체는 규칙 1에 의해 일치하지 않으므로 규칙 2에 대해 평가됩니다.
- * 규칙 2: 1MB * 이상의 개체에 대한 삭제 코딩
  - 다른 테넌트의 모든 객체를 일치하지만 1MB 이상인 경우에만 일치시킵니다. 이러한 큰 오브젝트는 3개의 사이트에서 6+3 삭제 코딩을 사용하여 저장됩니다.
  - 이(가) 1MB 이하의 객체와 일치하지 않으므로 이러한 오브젝트는 규칙 3에 대해 평가됩니다.

- * 규칙 3:2개 데이터 센터 2개 복사 * (기본값)
  - 정책의 마지막 기본 규칙입니다. 필터를 사용하지 않습니다.
  - 규칙 1 또는 규칙 2(1MB 이하의 테넌트 A에 속하지 않는 객체)에 의해 일치하지 않는 모든 객체의 복제된 복제본을 두 개 만듭니다.



활성 및 비활성 정책이란 무엇입니까?

모든 StorageGRID 시스템에는 하나 이상의 활성 ILM 정책이 있어야 합니다. 두 개 이상의 활성 ILM 정책을 사용하려면 ILM 정책 태그를 생성하고 각 태그에 정책을 할당합니다. 그런 다음 테넌트는 S3 버킷에 태그를 적용합니다. 기본 정책은 정책 태그가 할당되지 않은 버킷의 모든 개체에 적용됩니다.

ILM 정책을 처음 생성할 때 하나 이상의 ILM 규칙을 선택하고 특정 순서로 정렬합니다. 정책을 시뮬레이션하여 동작을 확인한 후 활성화합니다.

하나의 ILM 정책을 활성화하면 StorageGRID은 해당 정책을 사용하여 기존 오브젝트와 새로 수집된 오브젝트를 포함한 모든 오브젝트를 관리합니다. 새 정책의 ILM 규칙을 구현할 때 기존 개체를 새 위치로 이동할 수 있습니다.

한 번에 둘 이상의 ILM 정책을 활성화하고 테넌트가 S3 버킷에 정책 태그를 적용하는 경우 각 버킷의 오브젝트는 태그에 할당된 정책에 따라 관리됩니다.

StorageGRID 시스템은 활성화 또는 비활성화된 정책 기록을 추적합니다.

ILM 정책을 생성할 때의 고려 사항

- 테스트 시스템에서는 시스템에서 제공한 정책, 베이스라인 2 복사본 정책만 사용하십시오. StorageGRID 11.6 이전 버전의 경우 이 정책의 2개 복사본 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.

모든 스토리지 노드 스토리지 풀은 StorageGRID 11.6 이하를 설치하는 동안 자동으로 생성됩니다. 최신 버전의 StorageGRID로 업그레이드하는 경우 모든 스토리지 노드 풀이 여전히 존재합니다. StorageGRID 11.7 이상을 새로 설치하는 경우 모든 스토리지 노드 풀이 생성되지 않습니다.

- 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 해당 개체는 다른 규칙에 의해 평가되지 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.

ILM 정책을 생성합니다

서비스 품질 요구사항을 충족하는 하나 이상의 ILM 정책을 생성합니다.

하나의 활성 ILM 정책을 사용하면 모든 테넌트와 버킷에 동일한 ILM 규칙을 적용할 수 있습니다.

여러 개의 활성 ILM 정책을 사용하면 특정 테넌트와 버킷에 적절한 ILM 규칙을 적용하여 여러 서비스 품질 요구사항을 충족할 수 있습니다.

ILM 정책을 생성합니다

이 작업에 대해

자체 정책을 생성하기 전에 가 스토리지 요구 사항을 충족하지 않는지 "기본 ILM 정책"확인하십시오.

테스트 시스템에서는 시스템 제공 정책, 2개 복사본 정책(단일 사이트 그리드의 경우) 또는 사이트당 복제본(다중 사이트 그리드의 경우) 1개만 사용하십시오. StorageGRID 11.6 이전 버전의 경우 이 정책의 기본 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.

의 경우 "전역 S3 오브젝트 잠금 설정이 활성화되었습니다"ILM 정책이 S3 오브젝트 잠금이 설정된 버킷의 요구사항을 준수하는지 확인해야 합니다. 이 섹션에서 S3 오브젝트 잠금이 설정되었다는 지침을 따릅니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "액세스 권한이 필요합니다"있습니다.
- "ILM 규칙을 만들었습니다"S3 오브젝트 잠금이 설정되어 있는지 여부를 기반으로 합니다.

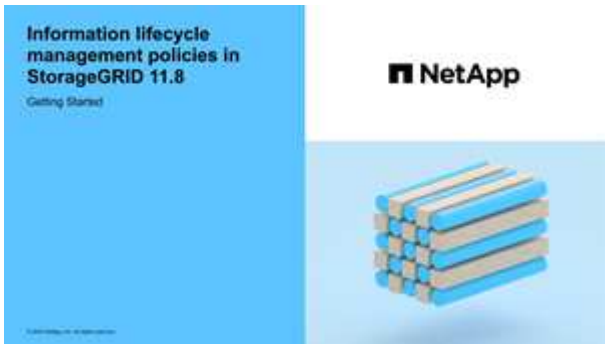
S3 오브젝트 잠금이 활성화되지 않았습니다

- "ILM 규칙을 만들었습니다"정책에 추가하려고 합니다. 필요에 따라 정책을 저장하고 추가 규칙을 만든 다음 정책을 편집하여 새 규칙을 추가할 수 있습니다.
- "기본 ILM 규칙을 만들었습니다"에 필터가 포함되어 있지 않습니다.

S3 오브젝트 잠금이 설정되었습니다

- "글로벌 S3 오브젝트 잠금 설정이 이미 활성화되어 있습니다"StorageGRID 시스템용 입니다.
- "규정 준수 및 비준수 ILM 규칙을 만들었습니다"정책에 추가하려고 합니다. 필요에 따라 정책을 저장하고 추가 규칙을 만든 다음 정책을 편집하여 새 규칙을 추가할 수 있습니다.
- "기본 ILM 규칙을 만들었습니다"정책을 준수해야 합니다.

- 비디오를 시청한 경우(선택 사항): "비디오: ILM 정책 개요"



도 "ILM 정책 사용"참조하십시오.

단계

1. ILM * > * 정책 * 을 선택합니다.

   전역 S3 개체 잠금 설정이 활성화된 경우 ILM 정책 페이지에는 호환되는 ILM 규칙이 표시됩니다.

2. ILM 정책을 생성할 방법을 결정합니다.

   새 정책을 생성합니다

   a. Create policy * 를 선택합니다.

   기존 정책을 복제합니다

   a. 시작할 정책의 확인란을 선택한 다음 * Clone * 을 선택합니다.

   기존 정책을 편집합니다

   a. 정책이 비활성 상태인 경우 편집할 수 있습니다. 시작할 비활성 정책의 확인란을 선택한 다음 * 편집 * 을 선택합니다.

3. 정책 이름 * 필드에 정책의 고유한 이름을 입력합니다.
4. 필요에 따라 * 변경 사유 * 필드에 새 정책을 생성하는 이유를 입력합니다.

5. 정책에 규칙을 추가하려면 * 규칙 선택 * 을 선택합니다. 규칙 이름을 선택하여 해당 규칙의 설정을 봅니다.

   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 필터를 사용한 경우 새 기본 규칙을 선택하라는 메시지가 표시됩니다.
   - 기본 규칙이 마지막 규칙이 아닌 경우 새 정책의 끝으로 규칙을 이동할 수 있습니다.

   S3 오브젝트 잠금이 활성화되지 않았습니다

   a. 정책에 대한 기본 규칙 하나를 선택합니다. 새 기본 규칙을 생성하려면 * ILM 규칙 페이지 * 를 선택합니다.

      기본 규칙은 정책의 다른 규칙과 일치하지 않는 개체에 적용됩니다. 기본 규칙은 필터를 사용할 수 없으며 항상 마지막으로 평가됩니다.

      > Make 2 Copies 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.

   S3 오브젝트 잠금이 설정되었습니다

   a. 정책에 대한 기본 규칙 하나를 선택합니다. 새 기본 규칙을 생성하려면 * ILM 규칙 페이지 * 를 선택합니다.

      규칙 목록에는 규정을 준수하며 필터를 사용하지 않는 규칙만 포함됩니다.

      > Make 2 Copies 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.

   b. 비준수 S3 버킷의 오브젝트에 대해 다른 "기본" 규칙이 필요한 경우 * 비준수 S3 버킷에 대한 필터가 없는 규칙 포함 * 을 선택하고 필터를 사용하지 않는 비준수 규칙 하나를 선택합니다.

      예를 들어, Cloud Storage Pool을 사용하여 S3 Object Lock이 활성화되지 않은 버킷에 오브젝트를 저장할 수 있습니다.

      > 필터를 사용하지 않는 비준수 규칙을 하나만 선택할 수 있습니다.

   도 "예 7: S3 오브젝트 잠금에 대한 규정 준수 ILM 정책"참조하십시오.

6. 기본 규칙을 모두 선택했으면 * Continue * 를 선택합니다.
7. 다른 규칙 단계에서는 정책에 추가할 다른 규칙을 선택합니다. 이러한 규칙은 하나 이상의 필터(테넌트 계정, 버킷 이름, 고급 필터 또는 비현재 참조 시간)를 사용합니다. 그런 다음 * 선택 * 을 선택합니다.

   이제 정책 생성 창에 선택한 규칙이 나열됩니다. 기본 규칙은 끝에 있으며 다른 규칙은 그 위에 있습니다.

S3 오브젝트 잠금이 설정되어 있고 비준수 "기본" 규칙도 선택한 경우 해당 규칙은 정책에서 두 번째-마지막 규칙으로 추가됩니다.

> 규칙이 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.

8. 기본 규칙이 아닌 규칙의 행을 끌어서 이러한 규칙이 평가되는 순서를 결정합니다.

   기본 규칙을 이동할 수 없습니다. S3 오브젝트 잠금이 설정된 경우 비준수 "기본" 규칙을 선택한 경우에도 이동할 수 없습니다.

   > ILM 규칙이 올바른 순서로 되어 있는지 확인해야 합니다. 정책이 활성화되면 위에서 시작하여 나열된 순서대로 새 개체와 기존 개체가 평가됩니다.

9. 필요에 따라 * 규칙 선택 * 을 선택하여 규칙을 추가하거나 제거합니다.
10. 완료되면 * Save * 를 선택합니다.
11. 이 단계를 반복하여 추가 ILM 정책을 생성합니다.
12. ILM 정책을 시뮬레이션합니다.. 정책을 활성화하기 전에 항상 시뮬레이트하여 예상대로 작동하는지 확인해야 합니다.

정책 시뮬레이션

정책을 활성화하고 운영 데이터에 적용하기 전에 테스트 객체에 대한 정책을 시뮬레이션합니다.

시작하기 전에

- 테스트할 각 오브젝트의 S3 버킷/오브젝트 키를 알 수 있습니다.

단계

1. S3 클라이언트 또는 를 사용하여 "S3 콘솔"각 규칙을 테스트하는 데 필요한 오브젝트를 수집합니다.
2. ILM 정책 페이지에서 정책의 확인란을 선택한 다음 * 시뮬레이션 * 을 선택합니다.
3. Object * 필드에 테스트 객체에 대한 S3를 `bucket/object-key` 입력합니다. `bucket-01/filename.png`예를 들어,
4. S3 버전 관리가 활성화된 경우 * 버전 ID * 필드에 객체의 버전 ID를 선택적으로 입력합니다.
5. 시뮬레이션 * 을 선택합니다.
6. Simulation 결과 섹션에서 각 개체가 올바른 규칙과 일치하는지 확인합니다.
7. 어떤 스토리지 풀 또는 삭제 코딩 프로필이 적용되었는지 확인하려면 일치하는 규칙의 이름을 선택하여 규칙 세부 정보 페이지로 이동합니다.

> 기존 복제 및 삭제 코딩 개체의 배치에 대한 변경 사항을 검토합니다. 기존 오브젝트의 위치를 변경하면 새로운 배치가 평가되고 구현될 때 일시적인 리소스 문제가 발생할 수 있습니다.

결과

정책 규칙에 대한 모든 편집 내용은 시뮬레이션 결과에 반영되고 새 일치 항목과 이전 일치 항목이 표시됩니다. 시뮬레이션 정책 창은 Simulation 결과 목록에서 * Clear All * 또는 각 개체에 대한 제거 아이콘을 선택할 때까지 테스트한 개체를 ✕유지합니다.

관련 정보

"ILM 정책 시뮬레이션의 예"

정책을 활성화합니다

새로운 단일 ILM 정책을 활성화하면 기존 오브젝트 및 새로 수집된 오브젝트가 해당 정책에 의해 관리됩니다. 여러 정책을 활성화할 때 버킷에 할당된 ILM 정책 태그는 관리할 오브젝트를 결정합니다.

새 정책을 활성화하기 전에:

1. 정책을 시뮬레이션하여 예상한 대로 작동하는지 확인합니다.
2. 기존 복제 및 삭제 코딩 개체의 배치에 대한 변경 사항을 검토합니다. 기존 오브젝트의 위치를 변경하면 새로운 배치가 평가되고 구현될 때 일시적인 리소스 문제가 발생할 수 있습니다.

ILM 정책의 오류로 인해 복구할 수 없는 데이터 손실이 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 구현하려고 대기합니다. 주요 내용은 다음과 같습니다.

- 정책을 변경하여 * 데이터 중복성 또는 내구성을 높이면 * 이러한 변경 사항이 즉시 적용됩니다. 예를 들어, 2개 복사본 규칙 대신 3개 복사본 규칙이 포함된 새 정책을 활성화하면 데이터 중복성이 증가하므로 해당 정책이 즉시 구현됩니다.
- 정책을 변경하여 * 데이터 중복성 또는 내구성을 저하시킬 수 있는 경우 * 모든 그리드 노드를 사용할 수 있을 때까지 해당 변경 사항이 구현되지 않습니다. 예를 들어 3개 복제본 규칙 대신 2개 복제본 규칙을 사용하는 새 정책을 활성화하면 새 정책이 활성 정책 탭에 나타나지만 모든 노드가 온라인 상태가 되어 사용 가능할 때까지 적용됩니다.

단계

정책 하나 또는 여러 개를 활성화하는 단계를 따릅니다.

하나의 정책을 활성화합니다

활성 정책이 하나만 있는 경우 다음 단계를 수행하십시오. 이미 활성 정책이 하나 이상 있고 추가 정책을 활성화하는 경우 여러 정책을 활성화하는 단계를 따릅니다.

1. 정책을 활성화할 준비가 되면 * ILM * > * Policies * 를 선택합니다.

   또는 * ILM * > * 정책 태그 * 페이지에서 단일 정책을 활성화할 수 있습니다.

2. 정책 탭에서 활성화할 정책의 확인란을 선택한 다음 * 활성화 * 를 선택합니다.
3. 적절한 단계를 따릅니다.
   - 정책을 활성화할지 확인하는 경고 메시지가 나타나면 * OK * 를 선택합니다.
   - 정책에 대한 세부 정보가 포함된 경고 메시지가 나타나는 경우:
     i. 세부 정보를 검토하여 정책이 데이터를 예상대로 관리하는지 확인합니다.
     ii. 기본 규칙에 제한된 기간 동안 개체를 저장하는 경우 보존 다이어그램을 검토한 다음 텍스트 상자에 해당 일 수를 입력합니다.
     iii. 기본 규칙에서 개체를 영구적으로 저장하지만 하나 이상의 다른 규칙이 보존이 제한된 경우 텍스트 상자에 * yes * 를 입력합니다.
     iv. 정책 활성화 * 를 선택합니다.

여러 정책을 활성화합니다

여러 정책을 활성화하려면 태그를 생성하고 각 태그에 정책을 할당해야 합니다.

여러 태그를 사용하는 경우 테넌트가 정책 태그를 버킷에 자주 재할당하면 그리드 성능이 영향을 받을 수 있습니다. 신뢰할 수 없는 테넌트가 있는 경우 기본 태그만 사용하는 것이 좋습니다.

1. ILM * > * 정책 태그 * 를 선택합니다.
2. Create * 를 선택합니다.
3. 정책 태그 만들기 대화 상자에서 태그 이름을 입력하고 원하는 경우 태그에 대한 설명을 입력합니다.

Tenant에서 태그 이름과 설명을 볼 수 있습니다. 테넌트가 버킷에 할당할 정책 태그를 선택할 때 정보에 입각한 결정을 내리는 데 도움이 되는 값을 선택합니다. 예를 들어, 할당된 정책이 일정 시간이 지난 후 개체를 삭제하는 경우 설명에 해당 정보를 전달할 수 있습니다. 이러한 필드에는 중요한 정보를 포함하지 마십시오.

4. 태그 만들기 * 를 선택합니다.
5. ILM 정책 태그 표에서 풀다운 메뉴를 사용하여 태그에 할당할 정책을 선택합니다.
6. 정책 제한 사항 열에 경고가 나타나면 * 정책 세부 정보 보기 * 를 선택하여 정책을 검토하십시오.
7. 각 정책이 예상대로 데이터를 관리하는지 확인합니다.
8. 할당된 정책 활성화 * 를 선택합니다. 또는 * 변경 내용 지우기 * 를 선택하여 정책 할당을 제거합니다.
9. 새 태그를 사용하여 정책 활성화 대화 상자에서 각 태그, 정책 및 규칙이 개체를 관리하는 방법에 대한 설명을 검토합니다. 필요에 따라 변경하여 정책이 개체를 예상대로 관리하도록 합니다.
10. 정책을 활성화하려면 텍스트 상자에 * 예 * 를 입력한 다음 * 정책 활성화 * 를 선택합니다.

관련 정보

"예 6: ILM 정책 변경"

ILM 정책 시뮬레이션의 예

ILM 정책 시뮬레이션의 예는 환경에 맞는 시뮬레이션을 구조화하고 수정하기 위한 지침을 제공합니다.

예 **1: ILM** 정책을 시뮬레이션할 때 규칙을 확인합니다

이 예제에서는 정책을 시뮬레이션할 때 규칙을 확인하는 방법을 설명합니다.

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.

정책을 시뮬레이션한 후 각 개체가 올바른 규칙에 일치하는지 확인합니다.

이 예에서

- `bucket-a/bucket-a object.pdf` 에서 개체를 필터링하는 첫 번째 규칙을 올바르게 일치시켰습니다. `bucket-a`
- `bucket-b/test object greater than 1 MB.pdf` 에 `bucket-b` 있으므로 첫 번째 규칙과 일치하지 않습니다. 대신 1MB보다 큰 객체를 필터링하는 두 번째 규칙에 의해 올바르게 일치되었습니다.
- `bucket-b/test object less than 1 MB.pdf` 처음 두 규칙의 필터와 일치하지 않으므로 필터를 포함하지 않는 기본 규칙에 따라 배치됩니다.

예 **2: ILM** 정책을 시뮬레이션할 때 규칙 순서 바꾸기

이 예제에서는 정책을 시뮬레이션할 때 결과를 변경하기 위해 규칙의 순서를 변경하는 방법을 보여 줍니다.

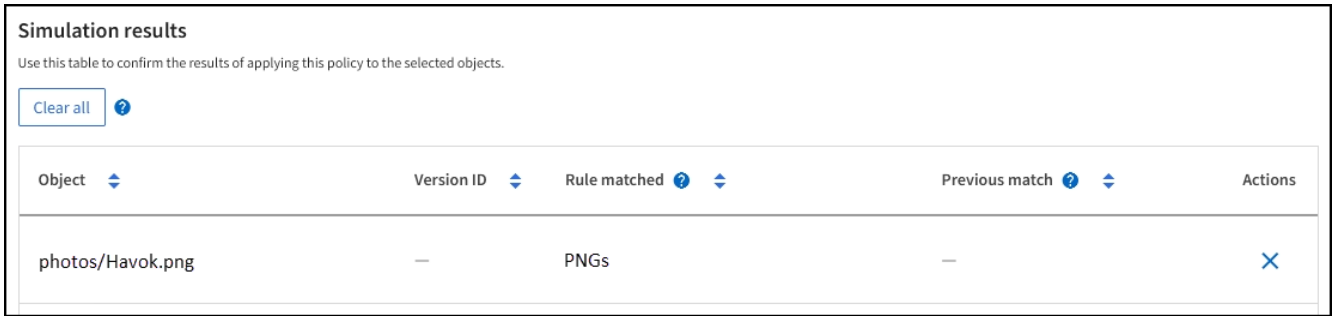
이 예에서는 * Demo * 정책을 시뮬레이션하고 있습니다. 이 정책은 시리즈 = x-men 사용자 메타데이터가 있는 개체를 찾기 위해 다음과 같은 세 가지 규칙을 포함합니다.

- 첫 번째 규칙인 * PNG * 는 로 끝나는 키 이름을 필터링합니다. `.png`
- 두 번째 규칙인 * X-men * 은 테넌트 A의 객체에만 적용되며 사용자 메타데이터의 필터에는 `series=x-men` 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. Object * 필드에 테스트 객체의 S3 버킷/오브젝트 키를 입력하고 * Simulate * 를 선택합니다.

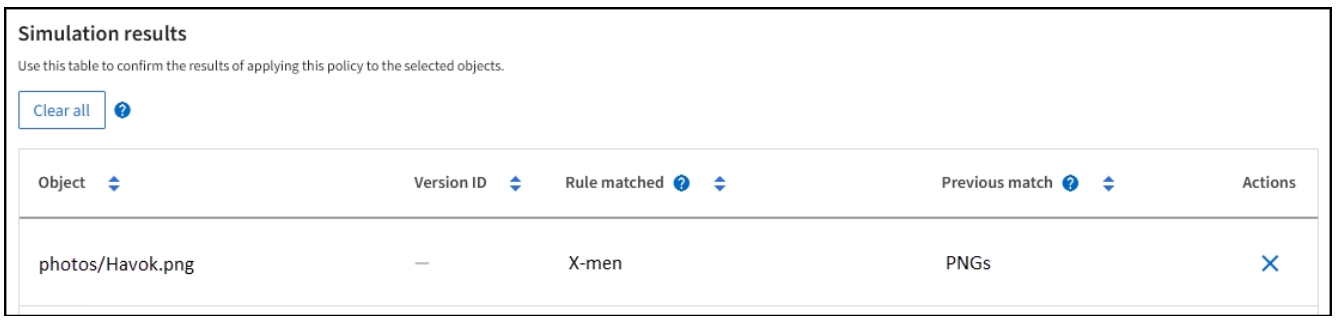
   개체가 * PNG * 규칙에 의해 일치했음을 보여주는 시뮬레이션 결과가 `Havok.png` 나타납니다.



   그러나 는 `Havok.png` * X-Men * 규칙을 테스트하기 위한 것입니다.

3. 문제를 해결하려면 규칙을 다시 정렬하십시오.
   a. ILM 정책 시뮬레이션 창을 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.

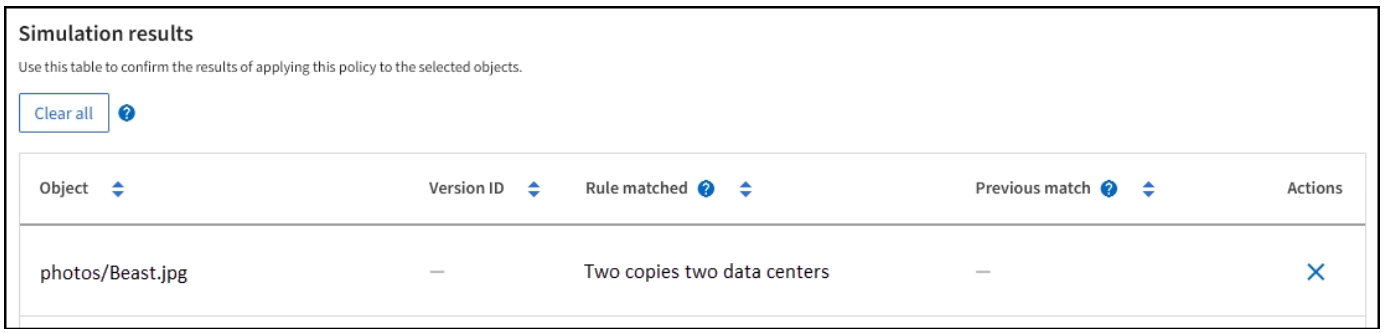
   이전에 테스트한 객체는 업데이트된 정책에 대해 재평가되고 새 시뮬레이션 결과가 표시됩니다. 이 예에서 규칙 일치 열은 개체가 이제 예상대로 X-Men 메타데이터 규칙과 일치함을 보여 줍니다 `Havok.png`. 이전 일치 열은 PNG 규칙이 이전 시뮬레이션에서 개체와 일치했음을 나타냅니다.



예 **3: 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 사용자 메타데이터가 있는 개체를 찾기 `series=x-men` 위한 것입니다. 그러나 개체에 대해 이 정책을 시뮬레이션하는 동안 예기치 않은 결과가 `Beast.jpg` 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.

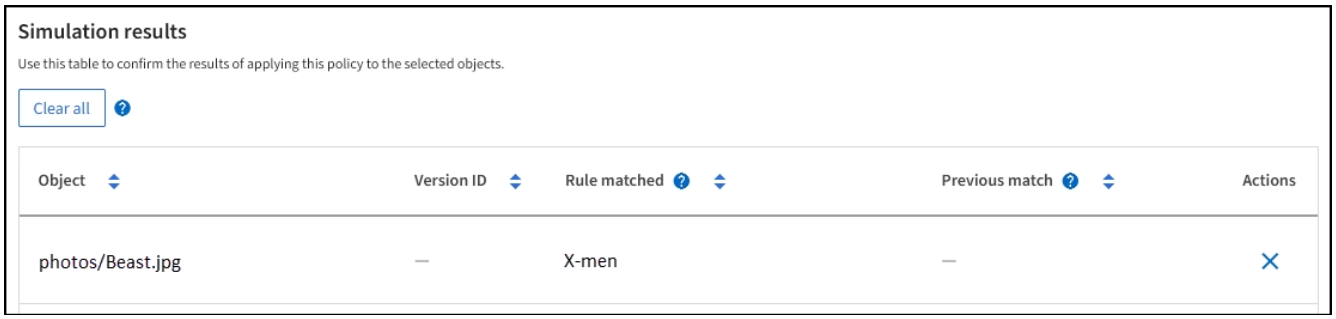
단계

1. Finish * 를 선택하여 Simulate policy 대화상자를 닫습니다. 정책의 세부 정보 페이지에서 * 보존 다이어그램 * 을 선택합니다. 그런 다음 필요에 따라 각 규칙에 대해 * Expand All * 또는 * View details * 를 선택합니다.
2. 규칙의 테넌트 계정, 참조 시간 및 필터링 기준을 검토합니다.

   예를 들어, X-men 규칙의 메타데이터가 "x-men" 대신 "x-men01"으로 입력되었다고 가정합니다.

3. 오류를 해결하려면 다음과 같이 규칙을 수정하십시오.
   - 규칙이 정책의 일부인 경우 규칙을 클론 복제하거나 정책에서 규칙을 제거한 다음 편집할 수 있습니다.
   - 규칙이 활성 정책의 일부인 경우 규칙을 복제해야 합니다. 활성 정책에서 규칙을 편집하거나 제거할 수 없습니다.
4. 시뮬레이션을 다시 수행합니다.

   이 예에서 수정된 X-men 규칙은 이제 사용자 메타데이터를 기반으로 개체를 `series=x-men` 예상한 대로 일치시킵니다. `Beast.jpg`



ILM 정책 태그를 관리합니다

ILM 정책 태그 세부 정보를 보거나 태그를 편집하거나 태그를 제거할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "액세스 권한이 필요합니다"있습니다.

ILM 정책 태그 세부 정보를 봅니다

태그에 대한 세부 정보를 보려면:

1. ILM * > * 정책 태그 * 를 선택합니다.
2. 테이블에서 정책 이름을 선택합니다. 태그에 대한 세부 정보 페이지가 나타납니다.
3. 세부 정보 페이지에서 할당된 정책의 이전 기록을 봅니다.
4. 정책을 선택하여 봅니다.

ILM 정책 태그를 편집합니다

> Tenant에서 태그 이름과 설명을 볼 수 있습니다. 테넌트가 버킷에 할당할 정책 태그를 선택할 때 정보에 입각한 결정을 내리는 데 도움이 되는 값을 선택합니다. 예를 들어, 할당된 정책이 일정 시간이 지난 후 개체를 삭제하는 경우 설명에 해당 정보를 전달할 수 있습니다. 이러한 필드에는 중요한 정보를 포함하지 마십시오.

기존 태그에 대한 설명을 편집하려면:

1. ILM * > * 정책 태그 * 를 선택합니다.
2. 태그 확인란을 선택한 다음 * 편집 * 을 선택합니다.

   또는 태그 이름을 선택합니다. 태그에 대한 세부 정보 페이지가 나타나고 해당 페이지에서 * 편집 * 을 선택할 수 있습니다.

3. 필요에 따라 태그 설명을 변경합니다
4. 저장 * 을 선택합니다.

ILM 정책 태그를 제거합니다

정책 태그를 제거하면 해당 태그가 지정된 모든 버킷에 기본 정책이 적용됩니다.

태그 제거하기:

1. ILM * > * 정책 태그 * 를 선택합니다.
2. 태그 확인란을 선택한 다음 * 제거 * 를 선택합니다. 확인 대화 상자가 나타납니다.

   또는 태그 이름을 선택합니다. 태그에 대한 세부 정보 페이지가 나타나고 해당 페이지에서 * 제거 * 를 선택할 수 있습니다.

3. 태그를 삭제하려면 * Yes * 를 선택합니다.

개체 메타데이터 조회를 통해 ILM 정책을 확인합니다

ILM 정책을 활성화한 후 StorageGRID 시스템에 대표 테스트 오브젝트를 수집한 다음 오브젝트

메타데이터 조회를 수행하여 복사본이 의도한 대로 만들어지고 올바른 위치에 배치되어 있는지 확인합니다.

시작하기 전에

개체 식별자가 있습니다. * UUID *: 개체의 Universally Unique Identifier 중 하나일 수 있습니다. * * CBID *: StorageGRID 내의 객체의 고유 식별자입니다. 감사 로그에서 개체의 CBID를 가져올 수 있습니다. CBID를 모두 대문자로 입력합니다. * S3 버킷 및 오브젝트 키 *: 오브젝트가 S3 인터페이스를 통해 수집될 때 클라이언트 애플리케이션은 버킷 및 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.

단계

1. 오브젝트 수집:
2. ILM * > * 개체 메타데이터 조회 * 를 선택합니다.
3. 식별자 * 필드에 개체의 식별자를 입력합니다. UUID, CBID 또는 S3 버킷/오브젝트 키를 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.

   - UUID(개체 ID), 결과 유형(개체, 삭제 마커, S3 버킷) 및 오브젝트의 논리적 크기와 같은 시스템 메타데이터. 자세한 내용은 아래 예제 스크린샷을 참조하십시오.
   - 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.
6. 개체가 올바른 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".

다음 예는 2개의 복제된 복사본으로 저장된 S3 테스트 개체에 대한 오브젝트 메타데이터 조회 결과를 보여 줍니다.

> 다음 스크린샷은 예제입니다. 결과는 StorageGRID 버전에 따라 달라집니다.

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

"S3 REST API 사용"

ILM 정책 및 ILM 규칙 사용

스토리지 요구사항이 변경됨에 따라 추가 정책을 적용하거나 정책과 연결된 ILM 규칙을 수정해야 할 수 있습니다. ILM 메트릭을 확인하여 시스템 성능을 결정할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

ILM 정책을 봅니다

활성 및 비활성 ILM 정책 및 정책 활성화 기록을 보려면 다음을 수행합니다.

1. ILM * > * 정책 * 을 선택합니다.
2. 활성 및 비활성 정책 목록을 보려면 * Policies * 를 선택합니다. 이 표에는 각 정책의 이름, 정책이 할당된 태그 및 정책이 활성 상태인지 비활성 상태인지 여부가 나열됩니다.
3. 정책에 대한 활성화 시작 및 종료 날짜 목록을 보려면 * 활성화 기록 * 을 선택하십시오.
4. 정책에 대한 세부 정보를 보려면 정책 이름을 선택합니다.

상태가 편집 또는 삭제된 정책에 대한 세부 정보를 보면 지정된 기간 동안 활성 상태였으며 이후 편집 또는 삭제된 정책의 버전을 보고 있음을 설명하는 메시지가 나타납니다.

ILM 정책을 편집합니다

비활성 정책만 편집할 수 있습니다. 활성 정책을 편집하려면 정책을 비활성화하거나 클론을 생성하고 클론을 편집합니다.

정책을 편집하려면

1. ILM * > * 정책 * 을 선택합니다.
2. 편집할 정책의 확인란을 선택한 다음 * 편집 * 을 선택합니다.
3. 의 지침에 따라 정책을 "ILM 정책을 생성합니다"편집합니다.
4. 정책을 다시 활성화하기 전에 시뮬레이션합니다.

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 복제합니다

ILM 정책을 클론 복제하려면:

1. ILM * > * 정책 * 을 선택합니다.
2. 복제할 정책의 확인란을 선택한 다음 * Clone * 을 선택합니다.
3. 의 지침에 따라 클론한 정책부터 시작하여 새 정책을 "ILM 정책을 생성합니다"만듭니다.

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 제거합니다

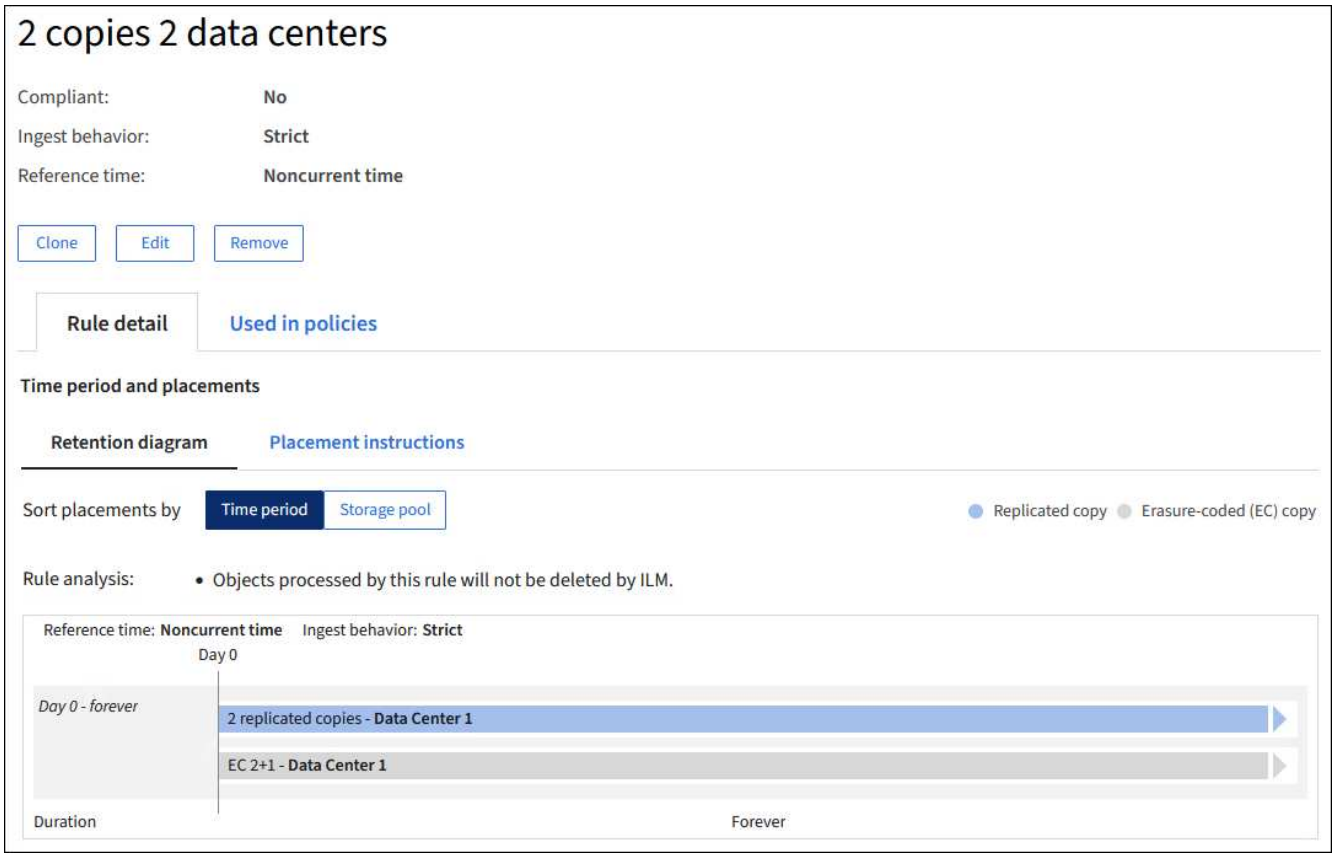
ILM 정책이 비활성 상태인 경우에만 제거할 수 있습니다. 정책을 제거하려면 다음을 수행합니다.

1. ILM * > * 정책 * 을 선택합니다.
2. 제거할 비활성 정책의 확인란을 선택합니다.
3. 제거 * 를 선택합니다.

ILM 규칙 세부 정보를 봅니다

규칙의 보존 다이어그램 및 배치 지침을 포함하여 ILM 규칙에 대한 세부 정보를 보려면 다음을 수행합니다.

1. ILM * > * 규칙 * 을 선택합니다.
2. 세부 정보를 보려는 규칙의 이름을 선택합니다. 예:



또한 세부 정보 페이지를 사용하여 규칙을 복제, 편집 또는 제거할 수 있습니다. 어떤 정책에서도 사용된 규칙은 편집하거나 제거할 수 없습니다.

ILM 규칙 클론 복제

기존 규칙의 일부 설정을 사용하는 새 규칙을 만들려는 경우 기존 규칙을 복제할 수 있습니다. 정책에 사용되는 규칙을 편집해야 하는 경우에는 대신 규칙을 클론 복제하고 클론을 변경합니다. 클론을 변경한 후에는 정책에서 원래 규칙을 제거하고 필요에 따라 수정된 버전으로 교체할 수 있습니다.

StorageGRID 버전 10.2 이하를 사용하여 ILM 규칙을 생성한 경우에는 클론 복제할 수 없습니다.

단계

1. ILM * > * 규칙 * 을 선택합니다.
2. 클론 복제할 규칙의 확인란을 선택한 다음 * Clone * 을 선택합니다. 또는 규칙 이름을 선택한 다음 규칙 세부 정보 페이지에서 * 클론 * 을 선택합니다.
3. 및 의 단계를 따라 복제된 규칙을 ILM 규칙 편집"ILM 규칙에서 고급 필터 사용"업데이트합니다.

   ILM 규칙을 복제할 때 새 이름을 입력해야 합니다.

ILM 규칙을 편집합니다

필터 또는 배치 지침을 변경하려면 ILM 규칙을 편집해야 할 수 있습니다.

ILM 정책에 사용된 규칙은 편집할 수 없습니다. 대신 복제된 복사본을 필요에 따라 변경할 수 규칙을 복제합니다있습니다.

> 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.

단계

1. ILM * > * 규칙 * 을 선택합니다.
2. 편집하려는 규칙이 ILM 정책에서 사용되지 않는지 확인합니다.
3. 편집하려는 규칙이 사용 중이 아닌 경우 규칙의 확인란을 선택하고 * Actions * > * Edit * 를 선택합니다. 또는 규칙 이름을 선택한 다음 규칙 세부 정보 페이지에서 * 편집 * 을 선택합니다.
4. ILM 규칙 편집 마법사의 단계를 완료합니다. 필요한 경우 및 의 단계를 "ILM 규칙 만들기""ILM 규칙에서 고급 필터 사용"따릅니다.

   ILM 규칙을 편집할 때는 해당 이름을 변경할 수 없습니다.

ILM 규칙을 제거합니다

현재 ILM 규칙 목록을 관리할 수 있도록 유지하려면 사용하지 않을 수 있는 ILM 규칙을 모두 제거해야 합니다.

단계

활성 정책에서 현재 사용되고 있는 ILM 규칙을 제거하려면 다음을 수행합니다.

1. 정책의 클론을 생성합니다.
2. 정책 클론에서 ILM 규칙을 제거합니다.
3. 새 정책을 저장, 시뮬레이션 및 활성화하여 객체가 예상대로 보호되도록 합니다.
4. 비활성 정책에서 현재 사용되고 있는 ILM 규칙을 제거하는 단계로 이동합니다.

비활성 정책에서 현재 사용되고 있는 ILM 규칙을 제거하려면 다음을 수행합니다.

1. 비활성 정책을 선택합니다.
2. 정책 또는 에서 ILM 규칙을 제거합니다정책을 제거합니다.
3. 현재 사용되지 않는 ILM 규칙을 제거하는 단계로 이동합니다.

현재 사용되지 않는 ILM 규칙을 제거하려면 다음을 수행합니다.

1. ILM * > * 규칙 * 을 선택합니다.
2. 제거하려는 규칙이 어떤 정책에서도 사용되지 않는지 확인합니다.
3. 제거하려는 규칙이 사용 중이 아닌 경우 규칙을 선택하고 * Actions * > * Remove * 를 선택하십시오. 여러 규칙을 선택하고 동시에 모두 제거할 수 있습니다.

4. ILM 규칙을 제거할 것인지 확인하려면 * 예 * 를 선택합니다.

ILM 메트릭을 봅니다

대기열에 있는 개체 수 및 평가율과 같은 ILM의 메트릭을 볼 수 있습니다. 이러한 메트릭을 모니터링하여 시스템 성능을 확인할 수 있습니다. 대기열 또는 평가 속도가 크면 시스템이 수집 속도를 따라가지 못하거나, 클라이언트 애플리케이션의 로드가 과도하거나, 비정상적인 상태가 있음을 나타낼 수 있습니다.

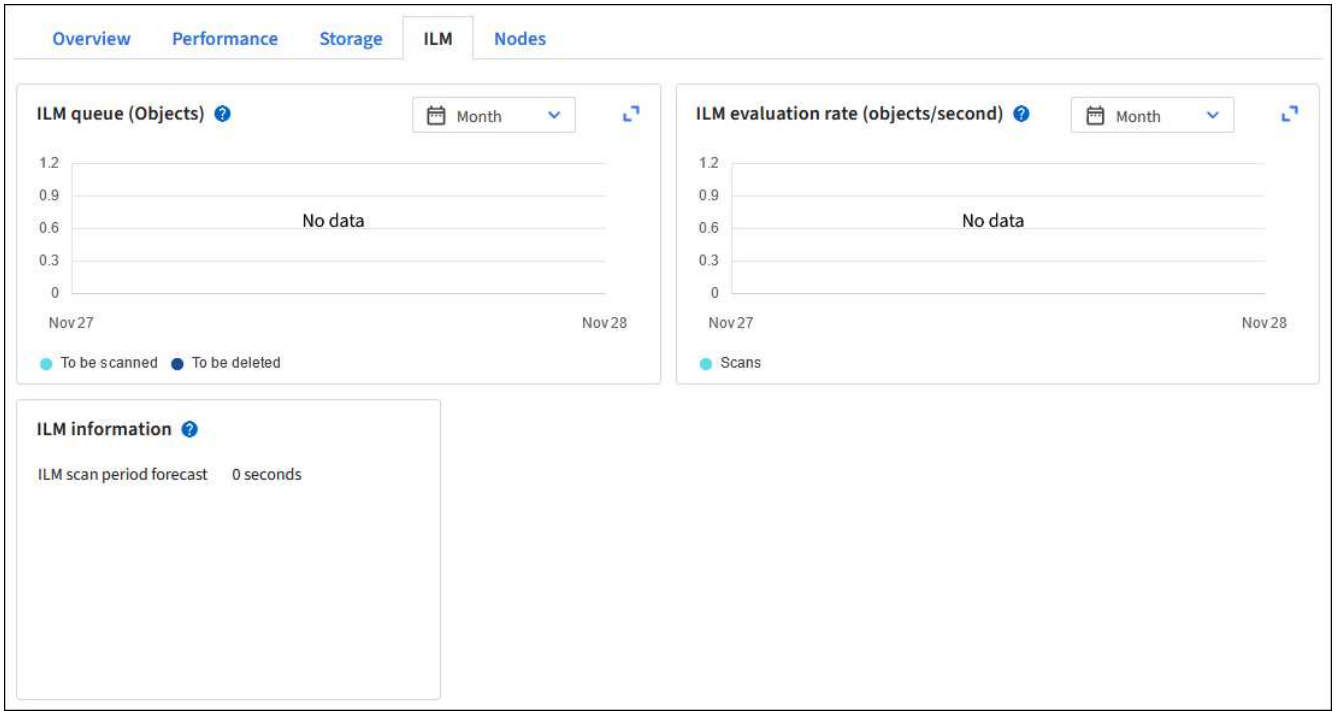
단계

1. 대시보드 * > * ILM * 을 선택합니다.

   대시보드를 사용자 지정할 수 있으므로 ILM 탭을 사용하지 못할 수 있습니다.

2. ILM 탭에서 메트릭을 모니터링합니다.

   물음표를 선택하면 ILM 탭의 항목에 대한 설명을 볼 수 있습니다.



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.

StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 S3 테넌트 계정에서 S3 오브젝트 잠금이 활성화되어 있거나 사용되지 않고 버킷을 생성할 수 있습니다. 버킷에 S3 오브젝트 잠금이 활성화된 경우 버킷 버전 관리가 필요하며 자동으로 활성화됩니다.

*S3 오브젝트 잠금이 없는 버킷은 보존 설정이 지정되지 않은 오브젝트만 가질 수 있습니다. 수집된 객체에는 보존 설정이 없습니다.

- S3 오브젝트 잠금이 있는 버킷은 S3 클라이언트 애플리케이션에 지정된 보존 설정이 있거나 없는 객체를 포함할 수 있습니다. 수집된 일부 객체에는 보존 설정이 있습니다.
- S3 오브젝트 잠금 및 기본 보존이 구성된 버킷 * 은 보존 설정이 지정된 객체와 보존 설정이 없는 새 객체를 업로드할 수 있습니다. 개체 수준에서 보존 설정이 구성되지 않았기 때문에 새 개체는 기본 설정을 사용합니다.

기본적으로 보존이 구성되면 새로 수집된 모든 객체에 보존 설정이 적용됩니다. 개체 보존 설정이 없는 기존 개체는 영향을 받지 않습니다.

보존 모드

StorageGRID S3 오브젝트 잠금 기능은 두 가지 보존 모드를 지원하여 오브젝트에 다양한 보호 수준을 적용합니다. 이러한 모드는 Amazon S3 보존 모드에 해당합니다.

- 규정 준수 모드:
  - 보존 기한 에 도달할 때까지 개체를 삭제할 수 없습니다.
  - 오브젝트의 보존 기한 을 늘릴 수 있지만 줄일 수는 없습니다.
  - 개체의 보존 기한 은 해당 날짜에 도달할 때까지 제거할 수 없습니다.
- 거버넌스 모드:
  - 특수 권한이 있는 사용자는 요청에서 우회 헤더를 사용하여 특정 보존 설정을 수정할 수 있습니다.
  - 이러한 사용자는 보존 기한이 되기 전에 개체 버전을 삭제할 수 있습니다.
  - 이러한 사용자는 개체의 보존 기간(Retain-until-date)을 증가, 감소 또는 제거할 수 있습니다.

개체 버전에 대한 보존 설정입니다

버킷이 S3 오브젝트 잠금이 설정된 상태로 생성된 경우 사용자는 S3 클라이언트 애플리케이션을 사용하여 버킷에 추가되는 각 오브젝트에 대해 다음 보존 설정을 선택적으로 지정할 수 있습니다.

- * 보존 모드 *: 규정 준수 또는 거버넌스 중 하나입니다.
- * Retain-until-date *: 개체 버전의 Retain-until-date가 미래인 경우 개체를 검색할 수 있지만 삭제할 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.

  개체가 법적 보류 중인 경우 보존 모드에 관계없이 개체를 삭제할 수 없습니다.

개체 설정에 대한 자세한 내용은 을 참조하십시오"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다".

버킷을 위한 기본 보존 설정입니다

버킷이 S3 오브젝트 잠금이 활성화된 상태로 생성된 경우 사용자는 버킷에 대해 다음 기본 설정을 선택적으로 지정할 수 있습니다.

- * 기본 보존 모드 *: 규정 준수 또는 거버넌스 중 하나입니다.
- * 기본 보존 기간 *: 이 버킷에 추가된 새 오브젝트 버전이 추가되는 날부터 보존되어야 하는 기간입니다.

기본 버킷 설정은 고유한 보존 설정이 없는 새 오브젝트에만 적용됩니다. 이러한 기본 설정을 추가하거나 변경할 때 기존 버킷 개체는 영향을 받지 않습니다.

"S3 버킷을 생성합니다"및 을 "S3 오브젝트 잠금 기본 보존 업데이트"참조하십시오.

S3 오브젝트 잠금을 레거시 규정 준수와 비교합니다

S3 오브젝트 잠금은 이전 StorageGRID 버전에서 사용할 수 있었던 규정 준수 기능을 대체합니다. S3 오브젝트 잠금 기능은 Amazon S3 요구사항을 준수하므로 "레거시 규정 준수"라고 하는 독점적인 StorageGRID 규정 준수 기능이 더 이상 사용되지 않습니다.

> 글로벌 규정 준수 설정은 더 이상 사용되지 않습니다. 이전 버전의 StorageGRID를 사용하여 이 설정을 활성화하면 S3 오브젝트 잠금 설정이 자동으로 활성화됩니다. StorageGRID를 계속 사용하여 기존 준수 버킷의 설정을 관리할 수 있지만 새로운 준수 버킷을 생성할 수는 없습니다. 자세한 내용은 을 참조하십시오 "NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법".

이전 버전의 StorageGRID에서 레거시 규정 준수 기능을 사용한 경우 다음 표를 참조하여 StorageGRID의 S3 오브젝트 잠금 기능과 어떻게 다른지 알아보십시오.

	S3 오브젝트 잠금	규정 준수(레거시)
이 기능은 전역적으로 어떻게 활성화됩니까?	그리드 관리자에서 * 구성 * > * 시스템 * > * S3 오브젝트 잠금 * 을 선택합니다.	더 이상 지원되지 않습니다.
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.	더 이상 지원되지 않습니다.
버킷 버전 관리가 지원됩니까?	예. 버킷에 대해 S3 오브젝트 잠금이 활성화된 경우 버킷 버전 관리가 필요하며 자동으로 활성화됩니다.	아니요
개체 보존은 어떻게 설정됩니까?	사용자는 각 오브젝트 버전에 대해 보존 기간을 설정하거나 각 버킷에 대한 기본 보존 기간을 설정할 수 있습니다.	사용자는 전체 버킷의 보존 기간을 설정해야 합니다. 보존 기간은 버킷의 모든 객체에 적용됩니다.

	S3 오브젝트 잠금	규정 준수(레거시)
보존 기간을 변경할 수 있습니까?	• 규정 준수 모드에서는 오브젝트 버전의 보존 기간을 늘릴 수 있지만 줄일 수는 없습니다. • 거버넌스 모드에서 특수 권한이 있는 사용자는 개체의 보존 설정을 줄이거나 제거할 수도 있습니다.	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?	• 규정 준수 모드에서는 개체가 법적 증거 자료 보관 상태에 있지 않은 경우, 보존 기한이 만료된 후에도 개체 버전을 삭제할 수 있습니다. • 거버넌스 모드에서 특수 권한이 있는 사용자는 개체가 법적 증거 자료 보관 상태에 있지 않은 경우 보존 기한이 되기 전에 개체를 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 작업

그리드 관리자는 테넌트 사용자와 긴밀하게 협력하여 보존 요구 사항을 충족하는 방식으로 객체가 보호되도록 해야 합니다.

네트워크 연결, 노드 상태 및 Cassandra 작업에 따라 그리드 전체에 테넌트 설정을 적용하는 데 15분 이상이 걸릴 수 있습니다.

그리드 관리자 및 테넌트 사용자를 위한 다음 목록에는 S3 오브젝트 잠금 기능을 사용하기 위한 상위 수준의 작업이 포함되어 있습니다.

그리드 관리자

- 전체 StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정을 사용합니다.
- 정보 수명 주기 관리(ILM) 정책이 _ 준수되는지 확인합니다. 즉, 이 정책이 을"S3 오브젝트 잠금이 설정된 버킷 요구사항"(를) 충족하는지 확인합니다.
- 필요에 따라 테넌트가 규정 준수를 보존 모드로 사용할 수 있도록 허용합니다. 그렇지 않으면 거버넌스 모드만 허용됩니다.
- 필요에 따라 테넌트의 최대 보존 기간을 설정합니다.

테넌트 사용자입니다

- S3 오브젝트 잠금을 통해 버킷 및 오브젝트에 대한 고려 사항을 검토하십시오.
- 필요한 경우 그리드 관리자에게 문의하여 글로벌 S3 오브젝트 잠금 설정을 활성화하고 권한을 설정합니다.
- S3 오브젝트 잠금이 설정된 상태로 버킷을 생성합니다.
- 필요에 따라 버킷의 기본 보존 설정을 구성합니다.
  - 기본 보존 모드: 그리드 관리자가 허용하는 경우 거버넌스 또는 규정 준수
  - 기본 보존 기간: 그리드 관리자가 설정한 최대 보존 기간 이하여야 합니다.
- S3 클라이언트 애플리케이션을 사용하여 오브젝트를 추가하고 필요에 따라 오브젝트별 보존을 설정합니다.
  - 보존 모드. 거버넌스 또는 규정 준수(그리드 관리자가 허용하는 경우)
  - 보관 종료 날짜: 그리드 관리자가 설정한 최대 보존 기간 이하여야 합니다.

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.
- 모든 활성 ILM 정책의 기본 규칙이 *compliant*(즉, 기본 규칙이 S3 오브젝트 잠금이 설정된 버킷 요구사항을 준수해야 함)가 아니면 글로벌 S3 오브젝트 잠금을 활성화할 수 없습니다.
- 글로벌 S3 오브젝트 잠금 설정을 사용하는 경우 정책의 기본 규칙이 준수되지 않는 한 새 ILM 정책을 생성하거나 기존 ILM 정책을 활성화할 수 없습니다. 전역 S3 개체 잠금 설정이 활성화된 후 ILM 규칙 및 ILM 정책 페이지는 어떤 ILM 규칙이 준수되는지 나타냅니다.

규정 준수 **ILM** 규칙 요구 사항

글로벌 S3 오브젝트 잠금 설정을 사용하려면 모든 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.
- 최소 한 줄의 배치 지침은 * Ingest Time * 을 기준 시간으로 사용하여 0일에 시작해야 합니다.
- 배치 지침의 최소 한 줄은 "영구"여야 합니다.

ILM 정책 요구 사항

글로벌 S3 오브젝트 잠금 설정이 활성화되면 활성 및 비활성 ILM 정책에 준수 규칙과 비준수 규칙이 모두 포함될 수 있습니다.

- 활성 또는 비활성 ILM 정책의 기본 규칙은 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.

"S3 오브젝트 잠금에 대한 규정 준수 ILM 정책의 예"

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.
- S3 오브젝트 잠금을 사용하려는 경우 버킷을 생성할 때 S3 오브젝트 잠금을 활성화해야 합니다. 기존 버킷에 S3 오브젝트 잠금을 설정할 수 없습니다.
- 버킷에 대해 S3 오브젝트 잠금이 활성화된 경우 StorageGRID는 해당 버킷의 버전 관리를 자동으로 활성화합니다. 버킷의 S3 오브젝트 잠금을 비활성화하거나 버전 관리를 일시 중단할 수 없습니다.
- 필요에 따라 테넌트 관리자, 테넌트 관리 API 또는 S3 REST API를 사용하여 각 버킷의 기본 보존 모드 및 보존 기간을 지정할 수 있습니다. 버킷의 기본 보존 설정은 고유한 보존 설정이 없는 버킷에 추가된 새 오브젝트에만 적용됩니다. 이 기본 설정은 업로드할 때 각 개체 버전에 대해 보존 모드 및 보존 종료 날짜를 지정하여 재정의할 수 있습니다.
- S3 오브젝트 잠금이 설정된 버킷에 대해 버킷 라이프사이클 구성이 지원됩니다.
- S3 오브젝트 잠금이 설정된 버킷에는 CloudMirror 복제가 지원되지 않습니다.

S3 오브젝트 잠금이 설정된 버킷의 오브젝트 요구사항

- 개체 버전을 보호하려면 버킷의 기본 보존 설정을 지정하거나 각 오브젝트 버전에 대한 보존 설정을 지정할 수 있습니다. 오브젝트 레벨의 보존 설정은 S3 클라이언트 애플리케이션 또는 S3 REST API를 사용하여 지정할 수 있습니다.
- 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 단계를 거칩니다.

1. * 오브젝트 수집 *

   오브젝트 버전이 S3 오브젝트 잠금이 설정된 버킷에 추가되면 보존 설정이 다음과 같이 적용됩니다.

   - 개체에 대한 보존 설정이 지정된 경우 개체 수준 설정이 적용됩니다. 기본 버킷 설정은 무시됩니다.
   - 개체에 대해 보존 설정을 지정하지 않으면 기본 버킷 설정이 적용됩니다(있는 경우).
   - 오브젝트 또는 버킷에 대해 보존 설정을 지정하지 않으면 S3 오브젝트 잠금으로 오브젝트가 보호되지 않습니다.

보존 설정이 적용되는 경우 오브젝트와 S3 사용자 정의 메타데이터는 모두 보호됩니다.

2. * 개체 보존 및 삭제 *

   StorageGRID는 지정된 보존 기간 동안 보호된 각 개체의 복사본을 여러 개 저장합니다. 오브젝트 복사본 및 스토리지 위치의 정확한 수와 유형은 활성 ILM 정책의 규정 준수 규칙에 따라 결정됩니다. 보존 기한이 되기 전에 보호된 개체를 삭제할 수 있는지 여부는 보존 모드에 따라 다릅니다.

   ◦ 개체가 법적 보류 중인 경우 보존 모드에 관계없이 개체를 삭제할 수 없습니다.

관련 정보

- "S3 버킷을 생성합니다"
- "S3 오브젝트 잠금 기본 보존 업데이트"
- "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
- "예 7: S3 오브젝트 잠금에 대한 규정 준수 ILM 정책"

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.

시작하기 전에

- 이 "루트 액세스 권한"있습니다.
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- S3 오브젝트 잠금 워크플로우를 검토하고 고려 사항을 이해합니다.
- 활성 ILM 정책의 기본 규칙이 준수된다는 것을 확인했습니다. 자세한 내용은 을 "기본 ILM 규칙을 생성합니다" 참조하십시오.

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 사용하도록 설정한 후에는 비활성화할 수 없습니다.

글로벌 S3 Object Lock 설정을 활성화한 후 기존 테넌트의 규정 준수 설정을 검토하십시오. 이 설정을 활성화하면 테넌트가 생성된 시점의 StorageGRID 릴리스에 따라 S3 오브젝트 잠금 설정이 달라집니다.

> ⓘ 글로벌 규정 준수 설정은 더 이상 사용되지 않습니다. 이전 버전의 StorageGRID를 사용하여 이 설정을 활성화하면 S3 오브젝트 잠금 설정이 자동으로 활성화됩니다. StorageGRID를 계속 사용하여 기존 준수 버킷의 설정을 관리할 수 있지만 새로운 준수 버킷을 생성할 수는 없습니다. 자세한 내용은 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.

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 호환되는 경우 S3 오브젝트 잠금이 전체 그리드에 대해 활성화되며 비활성화할 수 없습니다.
   - 기본 규칙을 준수하지 않으면 오류가 나타납니다. 규정 준수 규칙을 기본 규칙으로 포함하는 새 ILM 정책을 만들고 활성화해야 합니다. OK * 를 선택합니다. 그런 다음 새 정책을 생성하고 시뮬레이션한 다음 활성화합니다. 자세한 내용은 을 "ILM 정책을 생성합니다" 참조하십시오.

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 오류가 반환됩니다.

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

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"
- "S3 REST API 사용"
- "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 시뮬레이션하여 콘텐츠 손실을 방지하기 위한 의도대로 작동하는지 확인합니다.

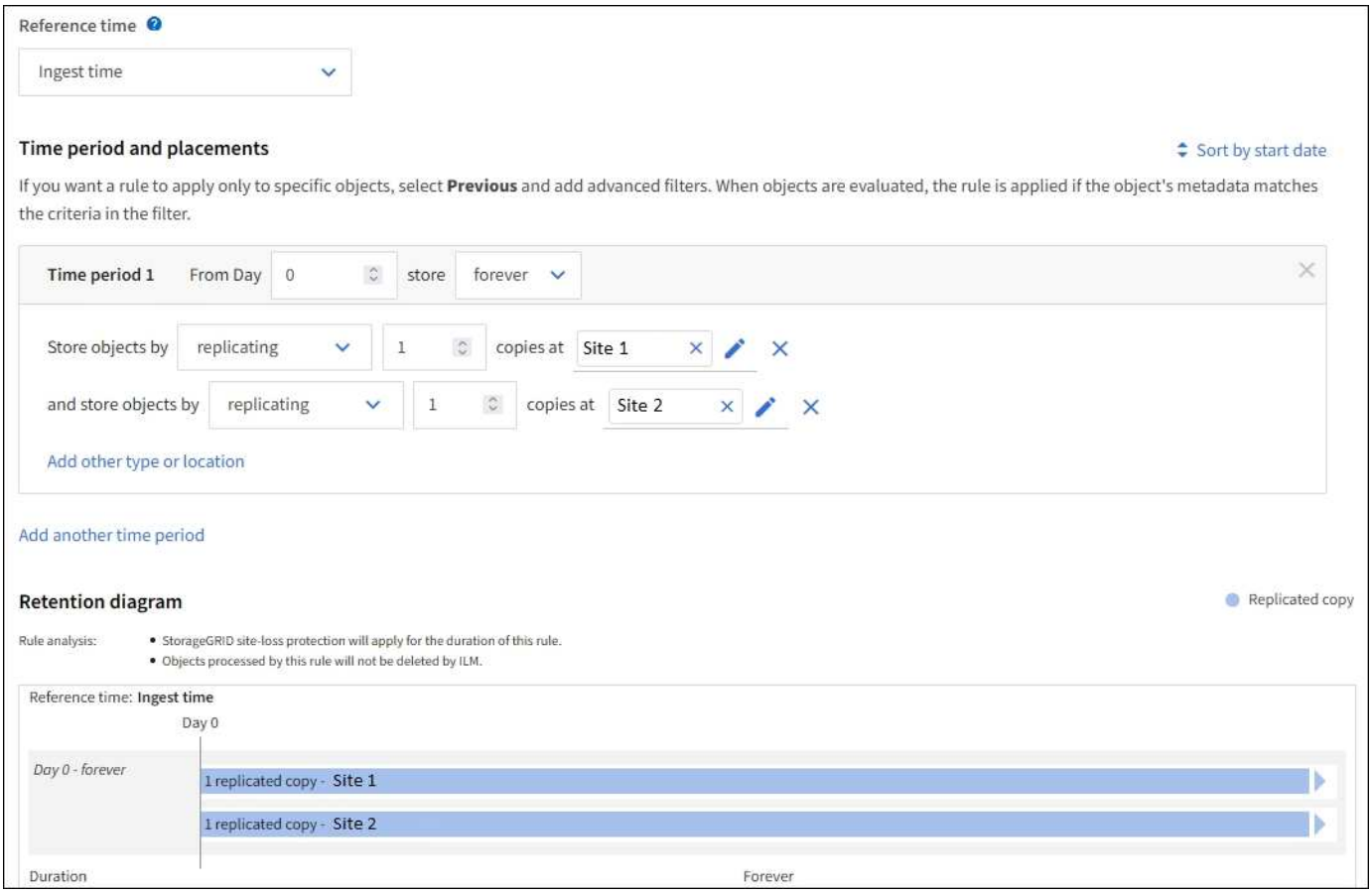
예를 들어 ILM 규칙 1: 개체 데이터를 두 사이트로 복사합니다

이 ILM 규칙 예에서는 개체 데이터를 두 사이트의 스토리지 풀로 복사합니다.

규칙 정의	예제 값
단일 사이트 스토리지 풀	각각 사이트 1과 사이트 2라는 서로 다른 사이트를 포함하는 두 개의 스토리지 풀
규칙 이름	두 개의 복제본 두 개의 사이트
참조 시간	수집 시간
배치	0일째부터 영원까지, 사이트 1에 복제된 복사본 하나와 사이트 2에 복제된 복사본 하나를 유지합니다.

보존 다이어그램의 규칙 분석 섹션에 나와 있는 내용은 다음과 같습니다.

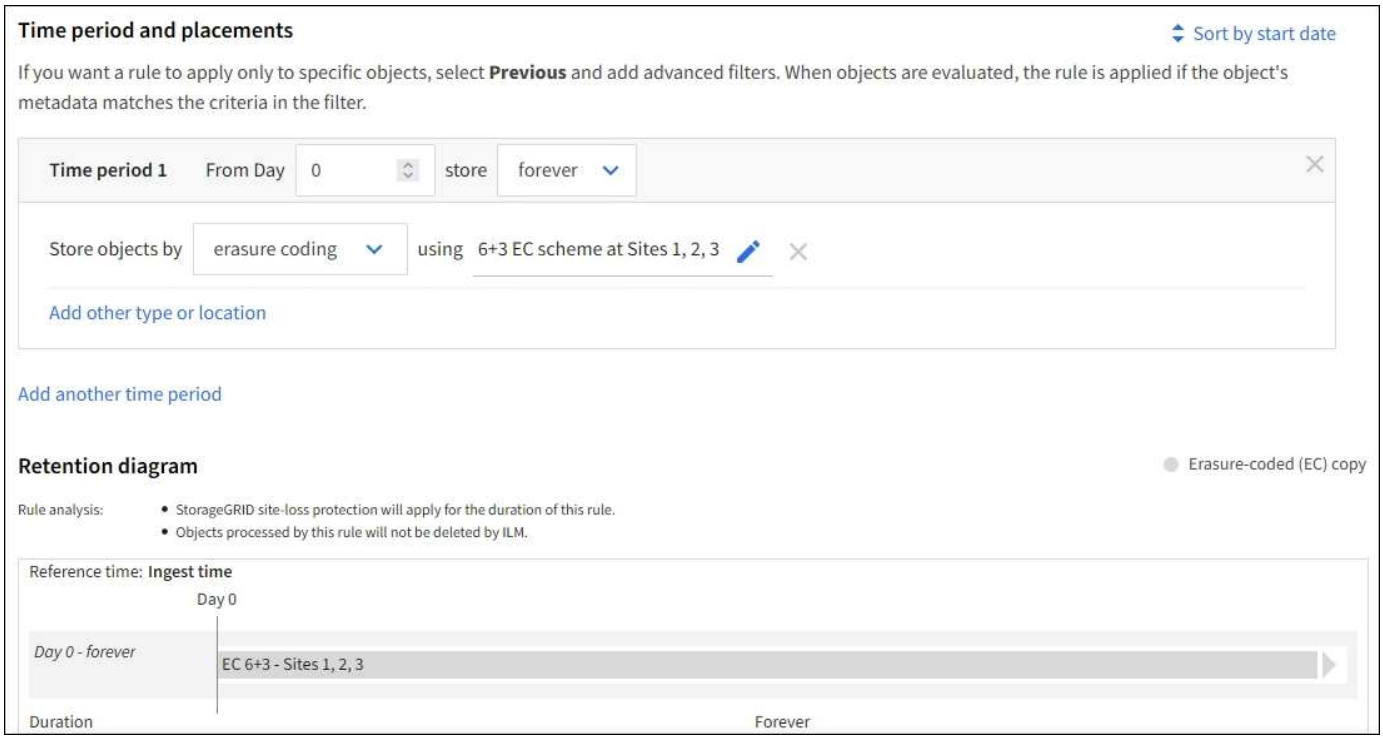
- StorageGRID 사이트 손실 보호는 이 규칙 기간 동안 적용됩니다.
- 이 규칙에 의해 처리된 객체는 ILM에 의해 삭제되지 않습니다.



예 **1**의 **ILM** 규칙 **2:** 버킷 매칭 시 삭제 코딩 프로필

이 예제 ILM 규칙은 삭제 코딩 프로필과 S3 버킷을 사용하여 오브젝트가 저장되는 위치 및 기간을 결정합니다.

규칙 정의	예제 값
여러 사이트가 있는 스토리지 풀입니다	• 3개 사이트에 걸친 스토리지 풀 1개(사이트 1, 2, 3) • 6+3 삭제 코딩 방법을 사용합니다
규칙 이름	S3 버킷 재무 기록
참조 시간	수집 시간
배치	S3 버킷에 재무 레코드라는 오브젝트의 경우 삭제 코딩 프로필에 지정된 풀에서 삭제 코딩 복사본 1개를 생성합니다. 이 복사본을 영구적으로 유지하십시오.

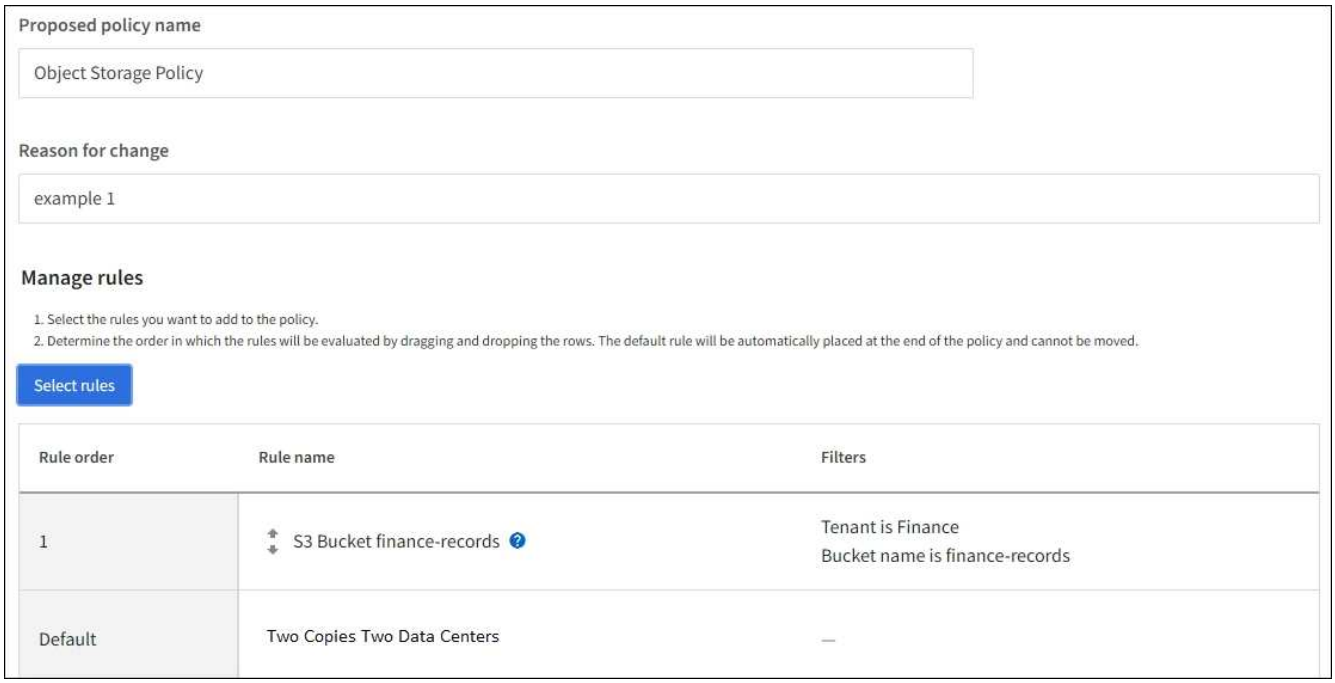


예 **1**의 **ILM** 정책

실제로 대부분의 ILM 정책은 StorageGRID 시스템을 통해 정교하고 복잡한 ILM 정책을 설계할 수 있지만 간단합니다.

다중 사이트 그리드에 대한 일반적인 ILM 정책에는 다음과 같은 ILM 규칙이 포함될 수 있습니다.

- 수집 시, 이라는 S3 버킷에 속하는 모든 오브젝트를 `finance-records` 3개 사이트가 포함된 스토리지 풀에 저장합니다. 6+3 삭제 코딩을 사용합니다.
- 개체가 첫 번째 ILM 규칙과 일치하지 않으면 정책의 기본 ILM 규칙, 두 개의 복사본 두 개의 데이터 센터를 사용하여 해당 개체의 복사본 하나를 사이트 1에 저장하고 한 복사본은 사이트 2에 저장합니다.



관련 정보

- "ILM 정책 사용"
- "ILM 정책을 생성합니다"

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 시뮬레이션하여 콘텐츠 손실을 방지하기 위한 의도대로 작동하는지 확인합니다.

예를 들어, ILM 규칙 1: 1MB 이상의 개체에 EC를 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	EC 전용 개체 > 1MB
참조 시간	수집 시간
개체 크기에 대한 고급 필터	객체 크기가 1MB를 초과합니다
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 필터	없음
배치	0일째부터 영원까지, 사이트 1에 복제된 복사본 하나와 사이트 2에 복제된 복사본 하나를 유지합니다.

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 1MB보다 큰 이미지를 삭제하고 작은 이미지로 두 개의 복사본을 만들 수 있습니다.

다음 ILM 규칙 및 정책은 예일 뿐입니다. ILM 규칙을 구성하는 방법은 여러 가지가 있습니다. 새 정책을 활성화하기 전에 시뮬레이션하여 콘텐츠 손실을 방지하기 위한 의도대로 작동하는지 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 필터	객체 크기가 1MB를 초과합니다
키에 대한 고급 필터	• jpg로 끝납니다 • .png로 끝납니다
배치	3개의 사이트를 사용하여 2+1 삭제 코딩 복사본을 생성합니다

이 규칙은 정책의 첫 번째 규칙으로 구성되므로 삭제 코딩 배치 지침은 1MB 이상인 .jpg 및 .png 파일에만 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	2 이미지 파일의 복사본
참조 시간	수집 시간
키에 대한 고급 필터	• jpg로 끝납니다 • .png로 끝납니다
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 버킷이 있는 경우 ILM 정책에 "비현재 시간"을 참조 시간으로 사용하는 규칙을 포함하여 현재 오브젝트 버전을 관리할 수 있습니다.

개체에 대해 제한된 보존 시간을 지정하면 해당 기간이 만료된 후에 해당 개체가 영구적으로 삭제됩니다. 개체가 유지되는 기간을 이해해야 합니다.

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 시뮬레이션하여 콘텐츠 손실을 방지하기 위한 의도대로 작동하는지 확인합니다.

개체의 현재 버전이 아닌 버전에서 ILM 정책 시뮬레이션을 수행하려면 개체 버전의 UUID 또는 CBID를 알아야 합니다. UUID 및 CBID를 찾으려면 객체가 최신 상태인 동안 를 "개체 메타데이터 조회 "사용합니다.

관련 정보

"오브젝트 삭제 방법"

예를 들어 **ILM** 규칙 **1: 10**년 동안 복사본 **3**개를 저장합니다

이 ILM 규칙은 10년 동안 3개의 사이트에 각 개체의 복사본을 저장합니다.

이 규칙은 버전 적용 여부에 관계없이 모든 개체에 적용됩니다.

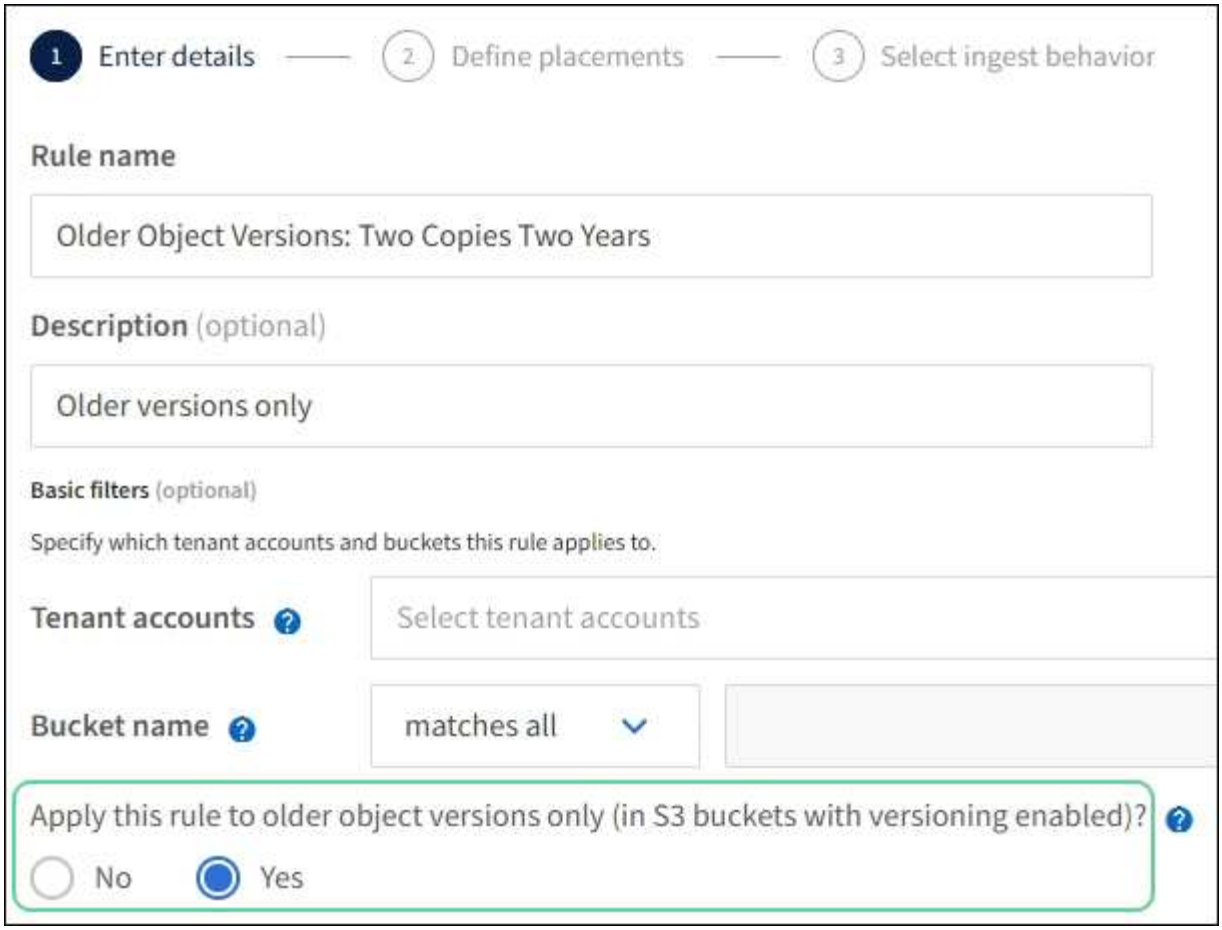
규칙 정의	예제 값
지원합니다	각각 사이트 1, 사이트 2 및 사이트 3이라는 서로 다른 데이터 센터로 구성된 스토리지 풀 3개
규칙 이름	10년 동안 3부
참조 시간	수집 시간
배치	0일째, 복제된 복사본 3개를 10년(3,652일), 사이트 1에 1개, 사이트 2에 1개, 사이트 3에 1개씩 보관합니다. 10년이 끝나면 개체의 복사본을 모두 삭제합니다.

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.

"비현재 시간"을 참조 시간으로 사용하는 규칙을 만들려면 "버전 관리가 활성화된 S3 버킷의 이전 개체 버전에만 이 규칙을 적용하시겠습니까?"라는 질문에 대해 * 예 * 를 선택합니다. ILM 규칙 생성 마법사의 1단계(세부 정보 입력)에서 Yes * 를 선택하면 참조 시간에 대해 _noncurrent time_이 자동으로 선택되며 다른 참조 시간을 선택할 수 없습니다.



이 예제에서는 비최신 버전의 복사본 두 개만 저장되고 이 복사본은 2년 동안 저장됩니다.

규칙 정의	예제 값
스토리지 풀	사이트 1과 사이트 2의 서로 다른 데이터 센터에 각각 2개의 스토리지 풀이 있습니다.
규칙 이름	비최신 버전: 2부 2년
참조 시간	현재 시간이 아닙니다 "버전 관리가 활성화된 S3 버킷의 경우 이전 개체 버전에만 이 규칙 적용"에 대해 * 예 * 를 선택하면 자동으로 선택됩니까? ILM 규칙 생성 마법사
배치	비현재 시간에 상대적인 제0일(즉, 객체 버전이 비최신 버전이 되는 날부터 시작)에서는 2년(730일) 동안 비최신 객체 버전의 복제된 복사본 2개를 사이트 1과 사이트 2의 복제본 1개로 유지합니다. 2년이 끝나면 최신 버전이 아닌 버전을 삭제합니다.

ILM 정책(예**: 4:S3** 버전 오브젝트

개체의 이전 버전을 현재 버전과 다르게 관리하려면 "현재 시간"을 참조 시간으로 사용하는 규칙이 현재 개체 버전에 적용되는 규칙 앞에 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.

> "비현재 시간" 규칙은 현재 개체 버전에 적용되는 규칙 앞에 정책에서 나타나야 합니다. 그렇지 않으면 현재 개체 버전이 "비현재 시간" 규칙과 일치하지 않습니다.

- 수집 시 3개의 복제 복사본을 생성하고 3개 사이트 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).
- 현재 개체 버전은 두 번째 규칙에 따라 일치됩니다. 현재 개체 버전이 10년 동안 저장된 경우 ILM 프로세스에서 삭제 마커를 현재 개체 버전으로 추가하고 이전 개체 버전을 "비최신"으로 만듭니다. 다음 번에 ILM 평가를 수행할 때 이 비최신 버전은 첫 번째 규칙에 따라 일치합니다. 따라서 사이트 3에서 복사본이 제거되고 사이트 1과 사이트 2의 두 복사본이 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 시뮬레이션하여 콘텐츠 손실을 방지하기 위한 의도대로 작동하는지 확인합니다.

관련 정보

- "수집 옵션"
- "ILM 규칙 생성: 수집 동작을 선택합니다"

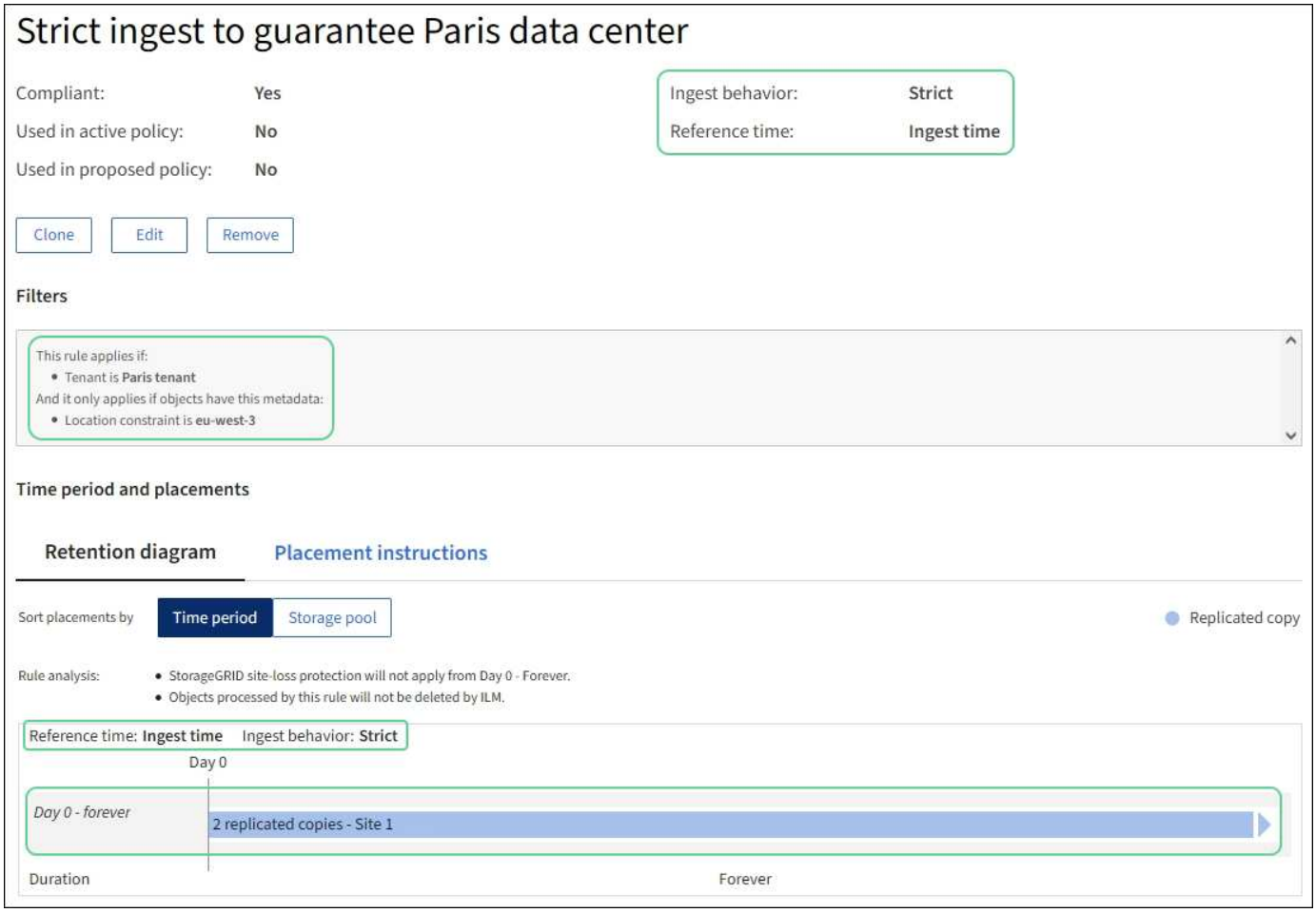
예를 들어 **ILM** 규칙 **1:** 파리 데이터 센터를 보장하기 위한 엄격한 수집

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 계정입니다	파리 테넌트
고급 필터	위치 제한은 EU-West-3과 동일합니다
지원합니다	사이트 1(파리)

규칙 정의	예제 값
규칙 이름	엄격한 인제스트로 파리 데이터 센터 보장
참조 시간	수집 시간
배치	0일째, 2개의 복제된 복사본을 사이트 1(파리)에 영구 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 복사본은 사용 가능한 위치에 저장됩니다.

이 규칙은 모든 테넌트 및 영역에 속하는 객체에 적용됩니다.

규칙 정의	예제 값
테넌트 계정입니다	무시
고급 필터	_ 지정 안 됨 _
지원합니다	사이트 1(파리) 및 사이트 2(미국)
규칙 이름	2 2개의 데이터 센터를 복사합니다
참조 시간	수집 시간
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 보호를 변경하거나 새 사이트를 추가해야 하는 경우 새 ILM 정책을 만들고 활성화할 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 새로운 활성 ILM

정책을 구현해야 합니다. 새 활성 정책을 구현하려면 먼저 를 "정책을 생성합니다"수행합니다. 그런 다음 "활성화"새 정책을 적용해야 "시뮬레이션"합니다.

> 다음 ILM 규칙 및 정책은 예일 뿐입니다. ILM 규칙을 구성하는 방법은 여러 가지가 있습니다. 새 정책을 활성화하기 전에 시뮬레이션하여 콘텐츠 손실을 방지하기 위한 의도대로 작동하는지 확인합니다.

ILM 정책을 변경하면 성능에 미치는 영향

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.

새 ILM 정책이 복제된 기존 객체 및 삭제 코딩 객체의 배치에 영향을 미치지 않도록 할 수 "수집 시간 필터를 사용하여 ILM 규칙을 생성합니다"있습니다. 예를 들어, * Ingest Time_은 _<*date and time*> * 이거나 그 이후이므로 새 규칙은 지정된 날짜 및 시간 이후에 수집된 개체에만 적용됩니다.

StorageGRID 성능에 일시적으로 영향을 미칠 수 있는 ILM 정책 변경 유형은 다음과 같습니다.

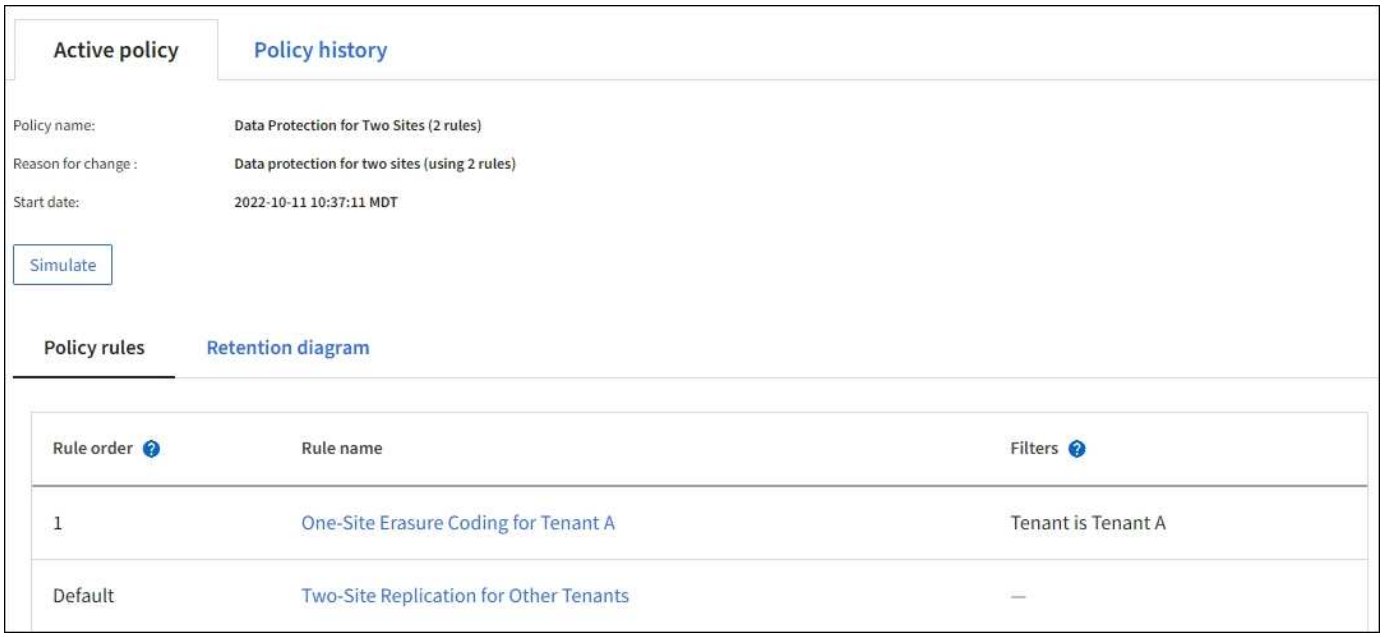
- 기존 삭제 코딩 오브젝트에 다른 삭제 코딩 프로필 적용

> StorageGRID는 각 삭제 코딩 프로필을 고유한 것으로 간주하며 새 프로필을 사용할 때 삭제 코딩 조각을 재사용하지 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)

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.



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.

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	사이트 1
배치	사이트 1의 2 + 1 삭제 코딩이 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	사이트 1 및 사이트 2
배치	사이트 1에 복사본 1개와 사이트 2에 복사본 1개로, 복제 복사본을 2일부터 영원히 복제할 수 있습니다.

예 6의 ILM 정책: 세 사이트에서 데이터 보호

이 예에서 ILM 정책은 3개 사이트 StorageGRID 시스템에 대한 새 정책으로 대체됩니다.

새 사이트를 추가하기 위해 확장을 수행한 후 그리드 관리자는 두 개의 새 스토리지 풀, 즉 사이트 3의 스토리지 풀과 세 사이트를 모두 포함하는 스토리지 풀(모든 스토리지 노드의 기본 스토리지 풀과 동일하지 않음)을 만들었습니다. 그런 다음 이 관리자는 세 사이트 모두에서 데이터를 보호하도록 설계된 두 가지 새로운 ILM 규칙과 새로운 ILM 정책을 개발했습니다.

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 A의 3개 사이트 삭제 코딩

규칙 정의	예제 값
규칙 이름	테넌트 A의 3개 사이트 삭제 코딩
테넌트 계정	테넌트 A
스토리지 풀	3개 사이트 모두(사이트 1, 사이트 2 및 사이트 3 포함)
배치	3개 사이트 모두에서 2개 이상의 삭제 코딩(0일부터 영구적)을 삭제합니다

규칙 2: 다른 테넌트를 위한 3개 사이트 복제

규칙 정의	예제 값
규칙 이름	다른 테넌트를 위한 3개 사이트 복제
테넌트 계정	무시
스토리지 풀	사이트 1, 사이트 2 및 사이트 3
배치	사이트 1에 복사본 1개, 사이트 2에 복사본 1개, 사이트 3에 복사본 1개로 구성된 복사본을 사이트 0에서 영구적으로 복제하는 3개

예를 들어 ILM 정책 활성화 6

새로운 ILM 정책을 활성화하면 신규 또는 업데이트된 규칙의 배치 지침에 따라 기존 오브젝트를 새 위치로 이동하거나 기존 오브젝트에 대한 새 오브젝트 복사본을 생성할 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 사이트 1에서 2+1 삭제 코딩을 사용하여 보호됩니다. 새로운 ILM 정책에서 테넌트 A에 속하는 개체는 사이트 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 사이트에 저장됩니다.
- 현재 진행 중인 ILM 스캔 프로세스 중에 테넌트 A에 속한 기존 객체가 다시 평가됩니다. ILM 배치 지침에서는 새로운 삭제 코딩 프로필을 사용하므로 완전히 새로운 삭제 코딩 조각이 생성되어 세 개의 사이트에 배포됩니다.

사이트 1의 기존 2 + 1 조각은 다시 사용되지 않습니다. StorageGRID는 각 삭제 코딩 프로필을 고유한 것으로 간주하며 새 프로필을 사용할 때 삭제 코딩 조각을 재사용하지 않습니다.

복제 지침이 변경될 때 수행되는 작업

이 예의 현재 활성 ILM 정책에서 다른 테넌트에 속한 개체는 사이트 1 및 2의 스토리지 풀에 복제된 복사본 두 개를 사용하여 보호됩니다. 새로운 ILM 정책에서 다른 테넌트에 속한 개체는 사이트 1, 2 및 3의 스토리지 풀에서 복제된 복사본 3개를 사용하여 보호됩니다.

새 ILM 정책이 활성화되면 다음 ILM 작업이 수행됩니다.

- 테넌트 A 이외의 테넌트가 새 객체를 링하면 StorageGRID는 복제본 3개를 생성하고 각 사이트에 복제본 1개를 저장합니다.
- 이러한 다른 테넌트에 속한 기존 객체는 지속적인 ILM 검색 프로세스 중에 재평가됩니다. 사이트 1과 사이트 2의 기존 오브젝트 복사본이 새로운 ILM 규칙의 복제 요구사항을 계속해서 충족하므로 StorageGRID은 사이트 3에 대한 개체의 새 복사본만 만들면 됩니다.

이 정책 활성화의 성능 영향

이 예의 ILM 정책이 활성화되면 이 StorageGRID 시스템의 전반적인 성능에 일시적으로 영향을 미칩니다. 다른 테넌트의 기존 오브젝트에 대해 테넌트 A의 기존 오브젝트와 사이트 3에 새로운 복제된 복제본에 대한 새로운 삭제 코딩 조각을 생성하려면 정상적인 그리드 리소스보다 높은 수준이 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 시뮬레이션하여 콘텐츠 손실을 방지하기 위한 의도대로 작동하는지 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 추가된 각 오브젝트 및 오브젝트 버전은 및 `legal hold` 설정에 다음 값을 `retain-until-date` 사용합니다.

각 개체에 대한 설정입니다	예제 값
`retain-until-date`	"2030-12-30T23:59:59Z"(2030년 12월 30일) 각 개체 버전에는 고유한 `retain-until-date` 설정이 있습니다. 이 설정은 늘릴 수 있지만 줄일 수는 없습니다.

각 개체에 대한 설정입니다	예제 값
`legal hold`	"꺼짐"(적용되지 않음) 보존 기간 동안 언제든지 개체 버전에 대한 법적 지류를 설정하거나 인양할 수 있습니다. 목적물이 법적 증거 자료 보관 중인 경우에는 에 도달하였더라도 그 목적물을 삭제할 `retain-until-date` 수 없다.

S3 오브젝트 잠금에 대한 **ILM** 규칙 **1** 예**:** 버킷 일치를 포함하는 삭제 코딩 프로필

이 ILM 규칙 예는 Bank of ABC라는 S3 테넌트 계정에만 적용됩니다. 버킷의 모든 오브젝트를 일치시킨 다음 `bank-records` 삭제 코딩을 사용하여 6+3 삭제 코딩 프로필을 사용하여 3개의 데이터 센터 사이트에 있는 스토리지 노드에 오브젝트를 저장합니다. 이 규칙은 S3 오브젝트 잠금이 설정된 버킷의 요구 사항을 충족합니다. 즉, 인제스트 시간을 참조 시간으로 사용하여 복사본을 0일부터 영원까지 스토리지 노드에 보관합니다.

규칙 정의	예제 값
규칙 이름	준수 규칙: 은행 내 EC 객체 - 레코드 버킷 - ABC 은행
테넌트 계정	ABC 은행
버킷 이름	`bank-records`
고급 필터	객체 크기(MB)가 1보다 큽니다 • 참고: * 이 필터는 오브젝트 1MB 이하의 오브젝트에 삭제 코딩이 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	규정을 준수하지 않는 규칙: 클라우드 스토리지 풀 사용

규칙 정의	예제 값
테넌트 계정	지정되지 않음
버킷 이름	지정되지 않았지만 S3 오브젝트 잠금(또는 레거시 규정 준수 기능)이 활성화되지 않은 버킷에만 적용됩니다.
고급 필터	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: 두 개의 데이터 센터를 복사합니다
테넌트 계정입니다	지정되지 않음
버킷 이름	지정되지 않음
고급 필터	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 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.

정책을 시뮬레이션합니다

정책에 규칙을 추가하고 기본 준수 규칙을 선택하고 다른 규칙을 정렬한 후에는 S3 오브젝트 잠금이 설정된 상태로 버킷에서 오브젝트를 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 BANK BANK에서 객체 1MB 이하 - BANC 테넌트의 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.

예 **8: S3** 버킷 라이프사이클 및 **ILM** 정책의 우선순위

라이프사이클 구성에 따라 오브젝트는 S3 버킷 라이프사이클 또는 ILM 정책의 보존 설정을 따릅니다.

ILM 정책보다 우선 순위가 높은 버킷 라이프사이클의 예

ILM 정책

- 비현재 시간 참조 기준 규칙: 0일차에 X개 복사본을 20일 동안 유지합니다
- 수집 시간 참조 기반 규칙(기본값): Day 0에 X 복사본을 50일 동안 유지합니다

버킷 수명 주기

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

결과

- "docs/text"라는 이름의 개체가 수집됩니다. "docs/" 접두사의 버킷 수명 주기 필터와 일치합니다.
  - 100일이 지나면 삭제 표식이 만들어지고 "문서/텍스트"가 비최신 상태가 됩니다.

- 5일 후 수집 후 총 105일이 지나면 "docs/text"가 삭제됩니다.
- 95일 후, 수집 이후 총 200일, 삭제 마커 생성 후 100일이 지나면 만료된 삭제 마커가 삭제됩니다.

- "비디오/동영상"이라는 이름의 개체가 수집됩니다. 필터와 일치하지 않으며 ILM 보존 정책을 사용합니다.
  - 50일이 지나면 삭제 마커가 생성되고 "비디오/동영상"이 비최신 상태가 됩니다.
  - 20일 후 수집 후 총 70일이 지나면 "비디오/동영상"이 삭제됩니다.
  - 30일 후, 수집 후 총 100일, 삭제 마커 생성 후 50일이 지나면 만료된 삭제 마커가 삭제됩니다.

버킷 수명 주기의 예 - 영구 보관

ILM 정책

- 비현재 시간 참조 기준 규칙: 0일차에 X개 복사본을 20일 동안 유지합니다
- 수집 시간 참조 기반 규칙(기본값): Day 0에 X 복사본을 50일 동안 유지합니다

버킷 수명 주기

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

결과

- "docs/text"라는 이름의 개체가 수집됩니다. "docs/" 접두사의 버킷 수명 주기 필터와 일치합니다.

  이 `Expiration` 작업은 만료된 삭제 표식에만 적용되며, 이는 "docs/"로 시작하는 다른 모든 항목을 영구적으로 유지함을 의미합니다.

  "docs/"로 시작하는 삭제 마커는 만료될 때 제거됩니다.

- "비디오/동영상"이라는 이름의 개체가 수집됩니다. 필터와 일치하지 않으며 ILM 보존 정책을 사용합니다.
  - 50일이 지나면 삭제 마커가 생성되고 "비디오/동영상"이 비최신 상태가 됩니다.
  - 20일 후 수집 후 총 70일이 지나면 "비디오/동영상"이 삭제됩니다.
  - 30일 후, 수집 후 총 100일, 삭제 마커 생성 후 50일이 지나면 만료된 삭제 마커가 삭제됩니다.

버킷 수명 주기를 사용하여 **ILM**을 복제하고 만료된 삭제 마커를 정리하는 예

ILM 정책

- 비현재 시간 참조 기준 규칙: 0일차에 X개 복사본을 20일 동안 유지합니다
- 수집 시간 참조 기준 규칙(기본값): Day 0에 X 복사본을 영구적으로 유지합니다

버킷 수명 주기

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

결과

- ILM 정책이 버킷 수명주기에 복제됩니다.
  - ILM 정책의 영구 규칙은 개체를 수동으로 제거하고 20일 후에 비최신 버전을 정리하도록 설계되었습니다. 따라서 수집 시간 규칙은 만료된 삭제 마커를 영구적으로 유지합니다.

- 버킷 수명 주기는 추가하는 동안 ILM 정책의 동작을 복제하므로 `"ExpiredObjectDeleteMarker": true` 만료 후 삭제 마커가 제거됩니다

- 개체가 수집됩니다. 필터가 없다는 것은 버킷 수명주기가 모든 객체에 적용되고 ILM 보존 설정이 재정의됨을 의미합니다.
  - 테넌트가 개체 삭제 요청을 실행하면 삭제 표식이 만들어지고 개체가 비최신 상태가 됩니다.
  - 20일이 지나면 비현재 개체가 삭제되고 삭제 표식이 만료됩니다.
  - 잠시 후 만료된 삭제 마커가 삭제됩니다.

시스템 강화

시스템 강화에 대한 일반 고려 사항

시스템 강화는 StorageGRID 시스템에서 가능한 한 많은 보안 위험을 제거하는 프로세스입니다.

StorageGRID를 설치 및 구성할 때 이 지침을 사용하여 기밀성, 무결성 및 가용성에 대해 규정된 모든 보안 목표를 충족할 수 있습니다.

시스템 강화를 위해 업계 표준 모범 사례를 이미 사용하고 있어야 합니다. 예를 들어 StorageGRID에 강력한 암호를 사용하고, HTTP 대신 HTTPS를 사용하고, 가능한 경우 인증서 기반 인증을 사용하도록 설정할 수 있습니다.

StorageGRID는 을 "NetApp 취약성 처리 정책"따릅니다. 보고된 취약점은 제품 보안 사고 대응 프로세스에 따라 확인 및 해결됩니다.

StorageGRID 시스템을 강화할 때는 다음 사항을 고려하십시오.

- * 세 가지 StorageGRID 네트워크 중 어떤 네트워크를 구현했습니까 *. 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 유형 *. 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 계정은 얼마나 신뢰할 수 있습니까 *. 신뢰할 수 없는 테넌트 계정을 사용하는 서비스 공급자라면 신뢰할 수 있는 내부 테넌트만 사용하는 것과 보안 문제가 다릅니다.
- * 어떤 보안 요구 사항 및 규약 * 귀하의 조직에서 따라야 합니까? 특정 규정 또는 기업 요구 사항을 준수해야 할 수 있습니다.

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.

https://imt.netapp.com/matrix/#welcome["NetApp 상호 운용성 매트릭스 툴"^]사용할 StorageGRID 소프트웨어 버전을 확인하려면 (IMT)를 참조하십시오. 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 "NetApp 다운로드: StorageGRID" 로 이동하십시오.
- StorageGRID 소프트웨어를 업그레이드하려면 를 "업그레이드 지침"참조하십시오.
- 핫픽스를 적용하려면 을 "StorageGRID 핫픽스 절차"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.

지원되는 버전 목록은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

하이퍼바이저로 업그레이드

StorageGRID 노드가 VMware 또는 다른 하이퍼바이저에서 실행 중인 경우 하이퍼바이저 소프트웨어 및 펌웨어를 최신 상태로 유지해야 합니다.

지원되는 버전 목록은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

* **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.

지원되는 버전 목록은 를 참조하십시오 "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.

StorageGRID 네트워크에 대한 자세한 내용은 를 "StorageGRID 네트워크 유형입니다"참조하십시오.

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. 를 "내부 포트 목록입니다"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. 를 "내부 포트 목록입니다"참조하십시오.
- 명시적으로 구성된 끝점에서만 인바운드 클라이언트 트래픽을 허용합니다. 에 대한 정보를 "방화벽 제어 관리 "참조하십시오.

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.

BMC에 대한 원격 **IPMI** 액세스를 제어합니다

BMC를 포함하는 모든 어플라이언스에 대해 원격 IPMI 액세스를 활성화 또는 비활성화할 수 있습니다. 원격 IPMI 인터페이스를 사용하면 BMC 계정 및 암호를 가진 모든 사용자가 StorageGRID 어플라이언스에 낮은 수준의 하드웨어 액세스를 할 수 있습니다. BMC에 대한 원격 IPMI 액세스가 필요하지 않으면 이 옵션을 비활성화합니다.

- Grid Manager에서 BMC에 대한 원격 IPMI 액세스를 제어하려면 * configuration * > * Security * > * Security settings * > * Appliances *:
  - BMC에 대한 IPMI 액세스를 비활성화하려면 * 원격 IPMI 액세스 활성화 * 확인란을 선택 취소합니다.
  - BMC에 대한 IPMI 액세스를 활성화하려면 * 원격 IPMI 액세스 활성화 * 확인란을 선택합니다.

방화벽 구성

시스템 강화 프로세스의 일환으로 외부 방화벽 구성을 검토하고 트래픽이 IP 주소 및 해당 IP 주소가 반드시 필요한 포트에서만 허용되도록 수정해야 합니다.

StorageGRID에는 노드에 대한 네트워크 액세스를 제어할 수 있도록 함으로써 그리드의 보안을 강화하는 각 노드에 대한 내부 방화벽이 포함되어 있습니다. 특정 그리드 배포에 필요한 포트를 제외한 모든 포트에서 네트워크 액세스를 금지해야 "내부 방화벽 제어를 관리합니다"합니다. 방화벽 제어 페이지에서 변경한 구성은 각 노드에 배포됩니다.

특히, 다음과 같은 영역을 관리할 수 있습니다.

- * 특별 권한 주소 *: 선택한 IP 주소 또는 서브넷이 외부 액세스 관리 탭의 설정으로 닫힌 포트에 액세스하도록 허용할 수 있습니다.
- * 외부 액세스 관리 *: 기본적으로 열려 있는 포트를 닫거나 이전에 닫은 포트를 다시 열 수 있습니다.
- * 신뢰할 수 없는 클라이언트 네트워크 *: 노드가 클라이언트 네트워크의 인바운드 트래픽을 신뢰하는지 여부와 신뢰할 수 없는 클라이언트 네트워크가 구성될 때 열려는 추가 포트를 트러스트할지 여부를 지정할 수 있습니다.

이 내부 방화벽은 일부 일반적인 위협에 대한 추가 보호 계층을 제공하지만 외부 방화벽의 필요성을 제거하지 않습니다.

StorageGRID에서 사용하는 모든 내부 및 외부 포트 목록은 을 참조하십시오"네트워크 포트 참조".

사용하지 않는 서비스를 비활성화합니다

모든 StorageGRID 노드에 대해 사용하지 않는 서비스에 대한 액세스를 비활성화하거나 차단해야 합니다. 예를 들어 DHCP를 사용할 계획이 없는 경우 그리드 관리자를 사용하여 포트 68을 닫습니다. configuration * > * Firewall control * > * 외부 액세스 관리 * 를 선택합니다. 그런 다음 포트 68에 대한 상태 토글을 * 열기 * 에서 * 닫힘 * 으로 변경합니다.

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.

설치하는 동안 노드를 보호합니다

노드가 설치될 때 신뢰할 수 없는 사용자가 네트워크를 통해 StorageGRID 노드에 액세스하도록 허용하지 않습니다. 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 직접 액세스할 수 없도록 허용해서는 안 됩니다. 대신 신뢰할 수 없는 테넌트가 테넌트 관리 API와 상호 작용하는 테넌트 포털 또는 외부 테넌트 관리 시스템을 사용하도록 합니다.
- 필요한 경우 관리자 프록시를 사용하여 관리 노드에서 NetApp 지원으로의 AutoSupport 통신을 더욱 강력하게 제어할 수 있습니다. 의 단계를 "관리자 프록시를 만드는 중입니다"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 의 지침을 "StorageGRID 관리"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. 의 단계를 "테넌트 계정을 생성하는 중입니다"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 더욱 강력하게 제어할 수 있습니다. 의 단계를 "스토리지 프록시 생성"참조하십시오.
- 선택적으로 클라이언트 네트워크를 사용하여 외부 서비스에 연결합니다. 그런 다음 * 구성 * > * 보안 * > * 방화벽 제어 * > * 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.

- 로드 밸런서 엔드포인트를 구성하고 사용합니다. 을 "로드 균형 조정에 대한 고려 사항"참조하십시오.
- 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 * > * 보안 * > * 방화벽 제어 * > * 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.

> BMC를 포함하는 모든 어플라이언스에 대해 원격 IPMI 액세스를 활성화 또는 비활성화할 수 있습니다. 원격 IPMI 인터페이스를 사용하면 BMC 계정 및 암호를 가진 모든 사용자가 StorageGRID 어플라이언스에 낮은 수준의 하드웨어 액세스를 할 수 있습니다. BMC에 대한 원격 IPMI 액세스가 필요하지 않은 경우 다음 방법 중 하나를 사용하여 이 옵션을 사용하지 않도록 설정합니다. + 그리드 관리자에서 * configuration * > * Security * > * Security settings * > * Appliances * 로 이동한 다음 * 원격 IPMI 액세스 활성화 * 확인란의 선택을 취소합니다. + 그리드 관리 API에서 전용 끝점을 사용합니다 `PUT /private/bmc`.

- SANtricity System Manager로 관리하는 SED, FDE 또는 FIPS NL-SAS 드라이브가 포함된 어플라이언스 모델의 경우, "SANtricity 드라이브 보안을 활성화하고 구성합니다"
- StorageGRID 어플라이언스 설치 프로그램 및 그리드 관리자를 사용하여 관리하는 SED 또는 FIPS NVMe SSD가 포함된 어플라이언스 모델의 경우, "StorageGRID 드라이브 암호화를 설정하고 구성합니다"
- SED, FDE 또는 FIPS 드라이브가 없는 어플라이언스의 경우 StorageGRID 소프트웨어 노드 암호화를 활성화하고 "KMS(키 관리 서버) 사용" 구성합니다.

TLS 및 SSH에 대한 강화 지침

설치 중에 생성된 기본 인증서를 교체하고 TLS 및 SSH 연결에 적합한 보안 정책을 선택해야 합니다.

인증서 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 API 인증서 *: S3 클라이언트 응용 프로그램이 객체 데이터를 업로드 및 다운로드하는 데 사용하는 스토리지 노드 및 게이트웨이 노드에 대한 액세스를 보호하는 데 사용됩니다.

자세한 내용 및 지침은 을 "보안 인증서를 관리합니다"참조하십시오.

> StorageGRID는 로드 밸런서 끝점에 사용되는 인증서를 별도로 관리합니다. 부하 분산 장치 인증서를 구성하려면 을 참조하십시오"로드 밸런서 엔드포인트를 구성합니다".

사용자 지정 서버 인증서를 사용하는 경우 다음 지침을 따르십시오.

- 인증서에는 StorageGRID의 DNS 항목과 일치하는 가 있어야 *subjectAltName* 합니다. 자세한 내용은 의 4.2.1.6절 "주체 대체 이름"을 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. 과 같은 와일드카드 패턴을 `*.s3.example.com` 사용하고 다른 응용 프로그램에는 접미사를 사용하지 `s3.example.com` 마십시오. 이 패턴은 같은 경로 스타일 S3 액세스에서도 사용할 수 `dc1-s1.s3.example.com/mybucket` 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.

TLS 및 **SSH** 정책 강화 지침

보안 정책을 선택하여 클라이언트 응용 프로그램과 보안 TLS 연결을 설정하고 내부 StorageGRID 서비스에 대한 SSH 연결을 보안하는 데 사용되는 프로토콜과 암호를 결정할 수 있습니다.

보안 정책은 TLS 및 SSH가 이동 중인 데이터를 암호화하는 방법을 제어합니다. 가장 좋은 방법은 응용 프로그램 호환성에 필요하지 않은 암호화 옵션을 비활성화하는 것입니다. 시스템이 공통 기준 호환이거나 다른 암호를 사용해야 하는 경우가 아니면 기본 최신 정책을 사용합니다.

자세한 내용 및 지침은 을 "TLS 및 SSH 정책을 관리합니다"참조하십시오.

기타 강화 지침

StorageGRID 네트워크 및 노드에 대한 강화 지침을 따르는 것 외에도 StorageGRID 시스템의 다른 영역에 대한 강화 지침을 따라야 합니다.

임시 설치 암호

설치 중에 StorageGRID 시스템을 보호하려면 StorageGRID 설치 UI 또는 설치 API의 임시 설치 관리자 암호 페이지에서 암호를 설정합니다. 이 암호를 설정하면 사용자 인터페이스, 설치 API 및 스크립트를 포함하여 StorageGRID를 설치하는 모든 방법에 이 암호가 `configure-storagegrid.py` 적용됩니다.

자세한 내용은 다음을 참조하십시오.

- "Red Hat Enterprise Linux에 StorageGRID를 설치합니다"
- "Ubuntu 또는 Debian에 StorageGRID를 설치합니다"

- "VMware에 StorageGRID를 설치합니다"
- "StorageGRID 어플라이언스를 설치합니다"

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 를 "로그 파일 참조"참조하십시오. StorageGRID 감사 메시지에 대한 자세한 내용은 을 "감사 메시지"참조하십시오.

NetApp AutoSupport를 참조하십시오

StorageGRID의 AutoSupport 기능을 사용하면 시스템의 상태를 사전에 모니터링하고 패키지를 NetApp Support 사이트, 조직의 내부 지원 팀 또는 지원 파트너에게 자동으로 보낼 수 있습니다. 기본적으로 AutoSupport 패키지를 NetApp로 보내는 기능은 StorageGRID를 처음 구성할 때 사용됩니다.

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 패키지는 매우 민감하므로 NetApp에서 AutoSupport 패키지를 NetApp에 전송하기 위한 기본 전송 프로토콜로 HTTPS를 사용하는 것이 좋습니다.

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.

의 단계를 "CORS(Cross-Origin Resource Sharing) 구성"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.

랜섬웨어 완화

의 권장 사항을 따라 랜섬웨어 공격으로부터 오브젝트 데이터를 보호합니다 "StorageGRID를 통한 랜섬웨어 방어".

FabricPool용 StorageGRID를 구성합니다

FabricPool용 StorageGRID를 구성합니다

NetApp ONTAP 소프트웨어를 사용하는 경우 NetApp FabricPool를 사용하여 비활성 데이터를 NetApp StorageGRID 오브젝트 스토리지 시스템에 계층화할 수 있습니다.

다음 지침을 따르십시오.

- FabricPool 워크로드에 대한 StorageGRID 구성을 위한 고려 사항 및 모범 사례에 대해 알아보십시오.
- FabricPool에서 사용할 StorageGRID 오브젝트 스토리지 시스템을 구성하는 방법에 대해 알아보십시오.
- StorageGRID를 FabricPool 클라우드 계층으로 연결할 때 ONTAP에 필요한 가치를 제공하는 방법에 대해 알아보십시오.

FabricPool용 **StorageGRID** 구성을 빠르게 시작합니다

1 구성을 계획합니다

- 비활성 ONTAP 데이터를 StorageGRID에 계층화하는 데 사용할 FabricPool 볼륨 계층화 정책을 결정합니다.
- 스토리지 용량 및 성능 요구 사항을 충족하도록 StorageGRID 시스템 계획 및 설치
- 및 를 포함한 StorageGRID 시스템 소프트웨어에 익숙해지십시오."그리드 관리자""테넌트 관리자"
- "HA 그룹""로드 밸런싱", "ILM을 참조하십시오"및 에 대한 FabricPool 모범 사례를 "자세히"검토합니다.
- ONTAP 및 FabricPool의 사용 및 구성에 대한 자세한 내용을 제공하는 다음 추가 리소스를 검토하십시오.

  "TR-4598: ONTAP에서의 FabricPool 모범 사례"

  "FabricPool에 대한 ONTAP 설명서"

2 필수 작업을 수행합니다

"StorageGRID를 클라우드 계층으로 연결하는 데 필요한 정보"다음을 포함하여 를 얻습니다.

- IP 주소
- 도메인 이름
- SSL 인증서

필요에 따라 "ID 제휴"및 를 "SSO(Single Sign-On)"구성합니다.

3 **StorageGRID** 설정을 구성합니다

StorageGRID를 사용하여 ONTAP가 그리드에 연결하는 데 필요한 값을 얻습니다.

를 사용하는 "FabricPool 설정 마법사"것이 모든 항목을 구성하는 데 가장 빠르고 권장되는 방법이지만 필요한 경우 각 요소를 수동으로 구성할 수도 있습니다.

4 **ONTAP** 및 **DNS**를 구성합니다

StorageGRID 값을 사용하는 경우 ONTAP "클라우드 계층 추가"를 사용합니다. 그런 다음 "DNS 항목을 구성합니다"IP 주소를 사용하려는 도메인 이름에 연결합니다.

5 모니터링 및 관리

시스템이 가동 및 실행 중일 경우 ONTAP 및 StorageGRID에서 지속적인 작업을 수행하여 시간에 따른 FabricPool 데이터 계층화를 관리하고 모니터링할 수 있습니다.

FabricPool란 무엇입니까**?**

FabricPool는 고성능 플래시 애그리게이트를 성능 계층으로 사용하고 오브젝트 저장소를 클라우드 계층으로 사용하는 ONTAP 하이브리드 스토리지 솔루션입니다. FabricPool 지원 애그리게이트를 사용하면 성능, 효율성 또는 보호 기능에 영향을 주지 않으면서 스토리지 비용을 절감할 수 있습니다.

FabricPool는 클라우드 계층(StorageGRID와 같은 외부 오브젝트 저장소)을 로컬 계층(ONTAP 스토리지 애그리게이트)에 연결하여 디스크의 복합 컬렉션을 생성합니다. 그런 다음 FabricPool 내의 볼륨은 활성(핫) 데이터를 고성능 스토리지(로컬 계층)에 유지하고 비활성(콜드) 데이터를 외부 오브젝트 저장소(클라우드 계층)에 계층화하여 계층화를 활용할 수 있습니다.

아키텍처를 변경할 필요가 없으며 중앙 ONTAP 스토리지 시스템에서 데이터 및 애플리케이션 환경을 계속 관리할 수 있습니다.

StorageGRID란 무엇입니까**?**

NetApp 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 스토리지 제공업체에 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.

StorageGRID를 클라우드 계층으로 연결하는 데 필요한 정보

StorageGRID를 FabricPool의 클라우드 계층으로 연결하려면 먼저 StorageGRID에서 구성 단계를 수행하고 ONTAP에서 사용할 수 있는 특정 값을 얻어야 합니다.

어떤 가치가 필요합니까**?**

다음 표에서는 StorageGRID에서 구성해야 하는 값과 ONTAP 및 DNS 서버에서 이러한 값을 사용하는 방법을 보여 줍니다.

값	값이 구성된 위치	값이 사용되는 위치
가상 IP(VIP) 주소입니다	StorageGRID > HA 그룹 을 선택합니다	DNS 항목
포트	StorageGRID > 부하 분산 장치 끝점	ONTAP 시스템 관리자 > 클라우드 계층 추가 를 클릭합니다
SSL 인증서	StorageGRID > 부하 분산 장치 끝점	ONTAP 시스템 관리자 > 클라우드 계층 추가 를 클릭합니다
서버 이름(FQDN)	StorageGRID > 부하 분산 장치 끝점	DNS 항목
액세스 키 ID 및 비밀 액세스 키	StorageGRID > 테넌트 및 버킷	ONTAP 시스템 관리자 > 클라우드 계층 추가 를 클릭합니다
버킷/컨테이너 이름입니다	StorageGRID > 테넌트 및 버킷	ONTAP 시스템 관리자 > 클라우드 계층 추가 를 클릭합니다

이러한 값을 얻으려면 어떻게 해야 합니까**?**

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

- 를 사용합니다"FabricPool 설정 마법사". FabricPool 설정 마법사를 사용하면 StorageGRID에서 필요한 값을 빠르게 구성하고 ONTAP 시스템 관리자를 구성하는 데 사용할 수 있는 파일을 출력할 수 있습니다. 마법사는 필요한 단계를 안내하고 StorageGRID 및 FabricPool 모범 사례에 맞게 설정을 조정할 수 있도록 도와줍니다.
- 각 항목을 수동으로 구성합니다. 그런 다음 ONTAP 시스템 관리자 또는 ONTAP CLI에 값을 입력합니다. 다음 단계를 수행하십시오.
  a. "FabricPool에 대한 고가용성(HA) 그룹을 구성합니다"..
  b. "FabricPool용 로드 밸런서 끝점을 만듭니다"..
  c. "FabricPool에 대한 테넌트 계정을 생성합니다"..
  d. 테넌트 계정에 "루트 사용자에 대한 버킷 및 액세스 키를 생성합니다"로그인합니다.
  e. FabricPool 데이터에 대한 ILM 규칙을 생성하여 활성 ILM 정책에 추가합니다. 을 "FabricPool 데이터에 대한 ILM을 구성합니다"참조하십시오.
  f. 선택적으로,"FabricPool에 대한 트래픽 분류 정책을 생성합니다"

FabricPool 설정 마법사를 사용합니다

FabricPool 설정 마법사 고려 사항 및 요구 사항을 사용합니다

FabricPool 설정 마법사를 사용하여 StorageGRID를 FabricPool 클라우드 계층에 대한 오브젝트 스토리지 시스템으로 구성할 수 있습니다. 설정 마법사를 완료한 후 ONTAP 시스템 관리자에 필요한 세부 정보를 입력할 수 있습니다.

FabricPool 설정 마법사를 사용하는 경우

FabricPool 설정 마법사는 FabricPool에서 사용하도록 StorageGRID를 구성하는 각 단계를 안내하고 ILM 및 트래픽 분류 정책과 같은 특정 엔터티를 자동으로 구성합니다. 마법사 완료 시 ONTAP 시스템 관리자에 값을 입력하는 데 사용할 수 있는 파일을 다운로드합니다. 마법사를 사용하여 시스템을 보다 빠르게 구성하고 설정이 StorageGRID 및 FabricPool 모범 사례에 맞는지 확인합니다.

루트 액세스 권한이 있는 경우 StorageGRID 그리드 관리자를 사용할 때 FabricPool 설치 마법사를 완료할 수 있으며, 나중에 마법사에 액세스하여 완료할 수도 있습니다. 요구 사항에 따라 필요한 항목의 일부 또는 전체를 수동으로 구성한 다음 마법사를 사용하여 ONTAP에 필요한 값을 단일 파일로 취합할 수도 있습니다.

특별한 요구 사항이 있거나 구현 시 상당한 사용자 지정이 필요한 경우가 아니면 FabricPool 설치 마법사를 사용하십시오.

마법사를 사용하기 전에

이 필수 단계를 완료했는지 확인합니다.

모범 사례를 검토합니다

- 에 대한 일반적인 이해도를 가지고 "StorageGRID를 클라우드 계층으로 연결하는 데 필요한 정보"있습니다.
- 다음에 대한 FabricPool 모범 사례를 검토했습니다.
  - "고가용성(HA) 그룹"
  - "로드 밸런싱"
  - "ILM 규칙 및 정책"

IP 주소를 얻고 VLAN 인터페이스를 설정합니다

HA 그룹을 구성할 경우 ONTAP가 연결할 노드 및 사용할 StorageGRID 네트워크를 알고 있어야 합니다. 서브넷 CIDR, 게이트웨이 IP 주소 및 가상 IP(VIP) 주소에 대해 입력할 값도 알고 있습니다.

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

ID 페더레이션 및 SSO를 구성합니다

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

도메인 이름 가져오기 및 구성

- StorageGRID에 사용할 FQDN(정규화된 도메인 이름)을 알고 있습니다. DNS(Domain Name Server) 항목은 이 FQDN을 마법사를 사용하여 생성한 HA 그룹의 가상 IP(VIP) 주소에 매핑합니다. 을 "DNS 서버를 구성합니다 "참조하십시오.
- S3 가상 호스팅 방식의 요청을 사용할 계획이라면 이 "S3 끝점 도메인 이름을 구성했습니다"있습니다. ONTAP에서는 기본적으로 경로 스타일 URL을 사용하지만 가상 호스팅 스타일 요청을 사용하는 것이 좋습니다.

로드 밸런서 및 보안 인증서 요구 사항을 검토합니다

StorageGRID 로드 밸런서를 사용할 계획이라면 일반을 검토하셨습니다."로드 균형 조정에 대한 고려 사항" 업로드할 인증서 또는 인증서를 생성하는 데 필요한 값이 있습니다.

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

ILM 스토리지 풀 구성을 확인합니다

처음에 StorageGRID 11.6 또는 이전 버전을 설치한 경우 사용할 스토리지 풀을 구성했습니다. 일반적으로 ONTAP 데이터를 저장하는 데 사용할 각 StorageGRID 사이트에 대해 스토리지 풀을 생성해야 합니다.

> 이 필수 구성 요소는 처음에 StorageGRID 11.7 또는 11.8을 설치한 경우에는 적용되지 않습니다. 이러한 버전 중 하나를 처음 설치하면 각 사이트에 대해 스토리지 풀이 자동으로 생성됩니다.

ONTAP와 **StorageGRID** 클라우드 계층 간의 관계

FabricPool 마법사는 StorageGRID 테넌트 1개, 액세스 키 세트 1개 및 StorageGRID 버킷 1개가 포함된 단일 StorageGRID 클라우드 계층을 생성하는 프로세스를 안내합니다. 이 StorageGRID 클라우드 계층을 하나 이상의 ONTAP 로컬 계층에 연결할 수 있습니다.

일반적인 모범 사례는 클러스터의 여러 로컬 계층에 단일 클라우드 계층을 연결하는 것입니다. 하지만 요구사항에 따라 단일 클러스터에서 로컬 계층에 둘 이상의 버킷 또는 하나 이상의 StorageGRID 테넌트를 사용할 수 있습니다. 다양한 버킷과 테넌트를 사용하여 ONTAP 로컬 계층 간에 데이터 및 데이터 액세스를 격리할 수 있지만 구성 및 관리가 다소 복잡합니다.

NetApp은 여러 클러스터의 로컬 계층에 단일 클라우드 계층을 연결하는 것을 권장하지 않습니다.

> NetApp MetroCluster ™ 및 FabricPool Mirror와 함께 StorageGRID를 사용하는 모범 사례는 를 참조하십시오. "TR-4598: ONTAP에서의 FabricPool 모범 사례"

선택 사항**:** 각 로컬 계층에 대해 다른 버킷을 사용하십시오

ONTAP 클러스터에서 로컬 계층에 둘 이상의 버킷을 사용하려면 ONTAP에 둘 이상의 StorageGRID 클라우드 계층을 추가하십시오. 각 클라우드 계층은 동일한 HA 그룹, 로드 밸런서 엔드포인트, 테넌트 및 액세스 키를 공유하지만 다른 컨테이너(StorageGRID 버킷)를 사용합니다. 다음 일반 단계를 따릅니다.

1. StorageGRID 그리드 관리자에서 첫 번째 클라우드 계층에 대한 FabricPool 설정 마법사를 완료합니다.
2. ONTAP 시스템 관리자에서 클라우드 계층을 추가하고 StorageGRID에서 다운로드한 파일을 사용하여 필요한 값을 제공합니다.
3. StorageGRID 테넌트 관리자에서 마법사에서 생성한 테넌트에 로그인하고 두 번째 버킷을 생성합니다.
4. FabricPool 마법사를 다시 완료합니다. 기존 HA 그룹, 로드 밸런서 엔드포인트 및 테넌트를 선택합니다. 그런 다음 수동으로 생성한 새 버킷을 선택합니다. 새 버킷에 대한 새 ILM 규칙을 생성하고 해당 규칙을 포함하도록 ILM 정책을 활성화합니다.
5. ONTAP에서 두 번째 클라우드 계층을 추가하고 새 버킷 이름을 제공합니다.

선택 사항**:** 각 로컬 계층에 대해 다른 테넌트와 버킷을 사용합니다

ONTAP 클러스터에서 로컬 계층에 대해 둘 이상의 테넌트 및 다른 액세스 키 세트를 사용하려면 ONTAP에 둘 이상의 StorageGRID 클라우드 계층을 추가합니다. 각 클라우드 계층은 동일한 HA 그룹, 로드 밸런서 엔드포인트를 공유하지만 다른 테넌트, 액세스 키 및 컨테이너(StorageGRID 버킷)를 사용합니다. 다음 일반 단계를 따릅니다.

1. StorageGRID 그리드 관리자에서 첫 번째 클라우드 계층에 대한 FabricPool 설정 마법사를 완료합니다.
2. ONTAP 시스템 관리자에서 클라우드 계층을 추가하고 StorageGRID에서 다운로드한 파일을 사용하여 필요한 값을 제공합니다.
3. FabricPool 마법사를 다시 완료합니다. 기존 HA 그룹 및 로드 밸런서 엔드포인트를 선택합니다. 새 테넌트 및 버킷을 생성합니다. 새 버킷에 대한 새 ILM 규칙을 생성하고 해당 규칙을 포함하도록 ILM 정책을 활성화합니다.
4. ONTAP에서 두 번째 클라우드 계층을 추가하고 새 액세스 키, 암호 키 및 버킷 이름을 제공합니다.

FabricPool 설정 마법사를 액세스하고 완료합니다

FabricPool 설정 마법사를 사용하여 StorageGRID를 FabricPool 클라우드 계층에 대한 오브젝트 스토리지 시스템으로 구성할 수 있습니다.

시작하기 전에

- FabricPool 설정 마법사를 사용하기 위한 를 검토했습니다."고려 사항 및 요구 사항"

> 다른 S3 클라이언트 애플리케이션에서 사용하도록 StorageGRID를 구성하려면 로 이동합니다"S3 설정 마법사를 사용합니다".

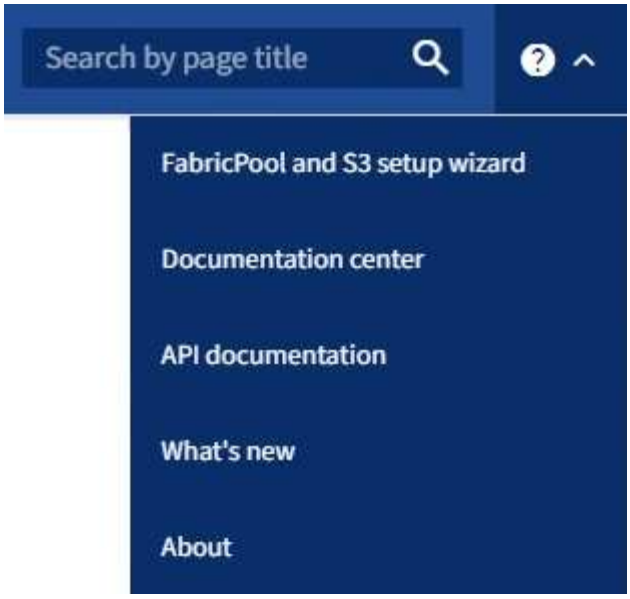
- 이 "루트 액세스 권한"있습니다.

마법사에 액세스합니다

StorageGRID 그리드 관리자 사용을 시작할 때 FabricPool 설정 마법사를 완료하거나 나중에 마법사를 액세스하여 완료할 수 있습니다.

단계

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



3. FabricPool 및 S3 설정 마법사 페이지의 FabricPool 섹션에서 * 지금 구성 * 을 선택합니다.
   - 9단계 중 1단계: HA 그룹 구성 * 이 나타납니다.

단계 **1/9: HA** 그룹 구성

HA(고가용성) 그룹은 각각 StorageGRID 로드 밸런서 서비스를 포함하는 노드의 모음입니다. HA 그룹에는 게이트웨이 노드, 관리자 노드 또는 둘 다 포함될 수 있습니다.

HA 그룹을 사용하면 FabricPool 데이터 연결을 계속 사용할 수 있습니다. HA 그룹은 가상 IP 주소(VIP)를 사용하여 로드 밸런서 서비스에 대한 고가용성 액세스를 제공합니다. HA 그룹의 액티브 인터페이스에 장애가 발생할 경우 백업 인터페이스에서 FabricPool 작업에 거의 영향을 주지 않고 워크로드를 관리할 수 있습니다

이 작업에 대한 자세한 내용은 "고가용성 그룹을 관리합니다" 및 "고가용성 그룹에 대한 Best Practice"을 참조하십시오.

단계

1. 외부 로드 밸런서를 사용할 계획이라면 HA 그룹을 생성할 필요가 없습니다. 이 단계 건너뛰기 * 를 선택하고 로 이동합니다9단계 중 2단계: 로드 밸런서 끝점을 구성합니다.
2. StorageGRID 로드 밸런서를 사용하려면 새 HA 그룹을 생성하거나 기존 HA 그룹을 사용합니다.

HA 그룹을 생성합니다

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

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

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

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

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

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

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

행을 드래그하여 * Priority order * 열의 값을 변경합니다.

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

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

e. IP 주소 입력 * 단계에 대해 다음 필드를 입력합니다.

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

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

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

g. 로드 밸런서 단계로 이동하려면 * 계속 * 을 선택합니다.

기존 **HA** 그룹 사용

a. 기존 HA 그룹을 사용하려면 * HA 그룹 선택 * 드롭다운 목록에서 HA 그룹 이름을 선택합니다.

b. 로드 밸런서 단계로 이동하려면 * 계속 * 을 선택합니다.

9단계 중 **2**단계**:** 로드 밸런서 끝점을 구성합니다

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

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

이 작업에 대한 자세한 내용은 일반 "로드 균형 조정에 대한 고려 사항" 및 을 "FabricPool의 로드 밸런싱 모범 사례 "참조하십시오.

단계

1. StorageGRID 로드 밸런서 끝점을 선택하거나 만들거나 외부 로드 밸런서를 사용합니다.

끝점 작성

a. 끝점 만들기 * 를 선택합니다.

b. Enter endpoint details * 단계에서 다음 필드를 입력합니다.

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

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

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

d. Tenant access * 단계에서 다음 중 하나를 선택합니다.

필드에 입력합니다	설명
모든 테넌트 허용(기본값)	모든 테넌트 계정은 이 엔드포인트를 사용하여 해당 버킷에 액세스할 수 있습니다. • 모든 테넌트 허용 * 은 거의 항상 FabricPool에 사용되는 로드 밸런서 끝점에 적합한 옵션입니다. 새 StorageGRID 시스템에 대해 FabricPool 설정 마법사를 사용하고 아직 테넌트 계정을 생성하지 않은 경우 이 옵션을 선택해야 합니다.
선택한 테넌트 허용	선택한 테넌트 계정만 이 끝점을 사용하여 해당 버킷을 액세스할 수 있습니다.
선택한 테넌트 차단	선택한 테넌트 계정은 이 끝점을 사용하여 해당 버킷을 액세스할 수 없습니다. 다른 모든 테넌트는 이 끝점을 사용할 수 있습니다.

e. 인증서 연결 * 단계에서 다음 중 하나를 선택합니다.

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

f. FabricPool 설정 마법사로 돌아가려면 * 마침 * 을 선택합니다.

g. 테넌트 및 버킷 단계로 이동하려면 * 계속 * 을 선택합니다.

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

기존 로드 밸런서 끝점을 사용합니다

a. 로드 밸런서 끝점 선택 * 드롭다운 목록에서 기존 끝점의 이름을 선택합니다.

b. 테넌트 및 버킷 단계로 이동하려면 * 계속 * 을 선택합니다.

외부 로드 밸런서를 사용합니다

a. 외부 로드 밸런서에 대해 다음 필드를 작성합니다.

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

b. 테넌트 및 버킷 단계로 이동하려면 * 계속 * 을 선택합니다.

9단계 중 **3**단계**:** 테넌트 및 버킷

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

버킷은 테넌트의 오브젝트 및 오브젝트 메타데이터를 저장하는 데 사용되는 컨테이너입니다. 일부 테넌트는 여러 개의 버킷을 가질 수 있지만 마법사에서 한 번에 하나의 테넌트와 하나의 버킷만 생성하거나 선택할 수 있습니다. 나중에 테넌트 관리자를 사용하여 필요한 추가 버킷을 추가할 수 있습니다.

FabricPool용 새 테넌트 및 버킷을 생성하거나 기존 테넌트와 버킷을 선택할 수 있습니다. 새 테넌트를 생성하는 경우 시스템은 테넌트의 루트 사용자에 대한 액세스 키 ID 및 비밀 액세스 키를 자동으로 생성합니다.

이 작업에 대한 자세한 내용은 "FabricPool에 대한 테넌트 계정을 생성합니다" 및 "S3 버킷을 생성하고 액세스 키를 얻습니다"을 참조하십시오.

단계

새 테넌트와 버킷을 생성하거나 기존 테넌트를 선택합니다.

새로운 테넌트 및 버킷

1. 새 테넌트 및 버킷을 생성하려면 * 테넌트 이름 * 을 입력합니다. `FabricPool tenant`예를 들어,
2. StorageGRID 시스템에서"ID 제휴", "SSO(Single Sign-On)"또는 둘 모두를 사용하는지 여부에 따라 테넌트 계정에 대한 루트 액세스를 정의합니다.

옵션을 선택합니다	이렇게 하십시오
ID 페더레이션이 활성화되지 않은 경우	테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션이 활성화된 경우	a. 테넌트에 대한 루트 액세스 권한이 있는 기존 통합 그룹을 선택합니다. b. 필요에 따라 테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션 및 SSO(Single Sign-On)가 모두 활성화된 경우	테넌트에 대한 루트 액세스 권한이 있는 기존 통합 그룹을 선택합니다. 로컬 사용자는 로그인할 수 없습니다.

3. 버킷 이름 * 에 대해 FabricPool가 ONTAP 데이터를 저장하는 데 사용할 버킷 이름을 입력합니다. `fabricpool-bucket`예를 들어,

   버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

4. 이 버킷의 * 지역 * 을 선택합니다.

   (`us-east-1`나중에 ILM을 사용하여 버킷 영역을 기준으로 오브젝트를 필터링하지 않을 경우 기본 영역을 사용합니다.

5. Create and Continue * 를 선택하여 테넌트와 버킷을 생성하고 데이터 다운로드 단계로 이동합니다

테넌트 및 버킷을 선택합니다

기존 테넌트 계정에는 버전 관리를 사용하지 않는 하나 이상의 버킷이 있어야 합니다. 해당 테넌트에 대한 버킷이 없으면 기존 테넌트 계정을 선택할 수 없습니다.

1. Tenant name * 드롭다운 목록에서 기존 Tenant를 선택합니다.
2. 버킷 이름 * 드롭다운 목록에서 기존 버킷을 선택합니다.

   FabricPool는 오브젝트 버전 관리를 지원하지 않으므로 버전 관리가 활성화된 버킷은 표시되지 않습니다.

   FabricPool에서 사용할 S3 오브젝트 잠금이 설정된 버킷을 선택하지 마십시오.

3. 다운로드 데이터 단계로 이동하려면 * 계속 * 을 선택합니다.

9단계 중 **4**단계**: ONTAP** 설정 다운로드

이 단계에서 ONTAP System Manager에 값을 입력하는 데 사용할 수 있는 파일을 다운로드합니다.

단계

1. 선택적으로 복사 아이콘( )을 선택하여 액세스 키 ID와 비밀 액세스 키를 모두 클립보드에 복사합니다.

   이러한 값은 다운로드 파일에 포함되어 있지만 별도로 저장할 수 있습니다.

2. ONTAP 설정 다운로드 * 를 선택하여 지금까지 입력한 값이 포함된 텍스트 파일을 다운로드합니다.

   이 `ONTAP_FabricPool_settings_bucketname.txt` 파일에는 StorageGRID을 FabricPool 클라우드 계층의 오브젝트 스토리지 시스템으로 구성하는 데 필요한 정보가 포함되어 있습니다.

   - 서버 이름(FQDN), 포트 및 인증서를 비롯한 로드 밸런서 연결 세부 정보
   - 버킷 이름
   - 테넌트 계정의 루트 사용자에 대한 액세스 키 ID 및 암호 액세스 키입니다

3. 복사한 키와 다운로드한 파일을 안전한 위치에 저장합니다.

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

4. 이 확인란을 선택하여 액세스 키 ID 및 비밀 액세스 키를 다운로드 또는 복사했는지 확인합니다.
5. ILM 스토리지 풀 단계로 이동하려면 * 계속 * 을 선택합니다.

단계 **5/9:** 스토리지 풀을 선택합니다

스토리지 풀은 스토리지 노드 그룹입니다. 스토리지 풀을 선택할 때 StorageGRID에서 ONTAP의 데이터 계층에 저장하는 데 사용할 노드를 결정합니다.

이 단계에 대한 자세한 내용은 을 "스토리지 풀을 생성합니다"참조하십시오.

단계

1. Site * (사이트 *) 드롭다운 목록에서 ONTAP에서 계층화할 데이터에 사용할 StorageGRID 사이트를 선택합니다.
2. 스토리지 풀 * 드롭다운 목록에서 해당 사이트의 스토리지 풀을 선택합니다.

   사이트의 스토리지 풀에는 해당 사이트의 모든 스토리지 노드가 포함됩니다.

3. ILM 규칙 단계로 이동하려면 * 계속 * 을 선택합니다.

9단계 중 **6**단계**: FabricPool**에 대한 **ILM** 규칙을 검토하십시오

ILM(정보 라이프사이클 관리) 규칙은 StorageGRID 시스템의 모든 개체에 대한 배치, 기간 및 수집 동작을 제어합니다.

FabricPool 설정 마법사는 FabricPool 사용을 위한 권장 ILM 규칙을 자동으로 생성합니다. 이 규칙은 지정한 버킷에만 적용됩니다. 단일 사이트에서 2+1 삭제 코딩을 사용하여 ONTAP에서 계층화된 데이터를 저장합니다.

이 단계에 대한 자세한 내용은 "ILM 규칙을 생성합니다" 및 "FabricPool 데이터에 ILM을 사용하는 모범 사례"을 참조하십시오.

단계

1. 규칙 세부 정보를 검토합니다.

필드에 입력합니다	설명
규칙 이름	자동으로 생성되며 변경할 수 없습니다
설명	자동으로 생성되며 변경할 수 없습니다
필터	버킷 이름입니다 이 규칙은 지정한 버킷에 저장된 오브젝트에만 적용됩니다.
참조 시간	수집 시간 배치 지침은 객체가 처음에 버킷에 저장될 때 시작됩니다.
배치 지침	2+1 삭제 코딩 사용

2. 보존 다이어그램을 * 기간 * 및 * 스토리지 풀 * 별로 정렬하여 배치 지침을 확인합니다.
   - 규칙의 * 기간 * 은 * 일 0 - 영구 * 입니다. * 일 0 * 은 데이터가 ONTAP에서 계층화할 때 규칙이 적용됨을 의미합니다. * Forever * 는 StorageGRID ILM이 ONTAP에서 계층화된 데이터를 삭제하지 않음을 의미합니다.
   - 규칙의 * 스토리지 풀 * 은 선택한 스토리지 풀입니다. * EC 2+1 * 은 데이터가 2+1 삭제 코딩을 사용하여 저장됨을 의미합니다. 각 오브젝트는 2개의 데이터 단편과 1개의 패리티 단편으로 저장됩니다. 각 오브젝트에 대한 세 개의 조각은 단일 사이트의 서로 다른 스토리지 노드에 저장됩니다.
3. Create and Continue * 를 선택하여 이 규칙을 생성하고 ILM 정책 단계로 이동합니다.

9단계 중 **7**단계**: ILM** 정책을 검토 및 활성화합니다

FabricPool 설정 마법사에서 FabricPool용 ILM 규칙을 생성하면 ILM 정책이 생성됩니다. 이 정책을 활성화하기 전에 신중하게 시뮬레이션하고 검토해야 합니다.

이 단계에 대한 자세한 내용은 "ILM 정책을 생성합니다" 및 "FabricPool 데이터에 ILM을 사용하는 모범 사례"을 참조하십시오.

> 새로운 ILM 정책을 활성화하면 StorageGRID은 해당 정책을 사용하여 기존 오브젝트 및 새로 수집된 오브젝트를 비롯하여 그리드에 있는 모든 오브젝트의 배치, 기간 및 데이터 보호를 관리합니다. 경우에 따라 새 정책을 활성화하면 기존 객체가 새 위치로 이동할 수 있습니다.

> 데이터 손실을 방지하려면 FabricPool 클라우드 계층 데이터를 만료 또는 삭제할 ILM 규칙을 사용하지 마십시오. StorageGRID ILM에서 FabricPool 객체가 삭제되지 않도록 보존 기간을 * Forever * 로 설정합니다.

단계

1. 선택적으로 시스템에서 생성한 * 정책 이름 * 을 업데이트합니다. 기본적으로 시스템은 활성 또는 비활성 정책의 이름에 "+FabricPool"를 추가하지만 사용자가 직접 이름을 입력할 수 있습니다.
2. 비활성 정책의 규칙 목록을 검토합니다.

- 그리드에 비활성 ILM 정책이 없는 경우 마법사는 활성 정책을 복제하고 맨 위에 새 규칙을 추가하여 비활성 정책을 만듭니다.
- 그리드에 이미 비활성 ILM 정책이 있고 해당 정책이 활성 ILM 정책과 동일한 규칙 및 순서를 사용하는 경우 마법사는 비활성 정책의 맨 위에 새 규칙을 추가합니다.
- 비활성 정책에 활성 정책과 다른 규칙이 있거나 순서가 포함되어 있으면 활성 정책을 복제하고 새 규칙을 맨 위에 추가하여 새 비활성 정책을 만듭니다.

3. 새 비활성 정책의 규칙 순서를 검토합니다.

   FabricPool 규칙은 첫 번째 규칙이므로 FabricPool 버킷의 모든 오브젝트는 정책의 다른 규칙 앞에 배치됩니다. 다른 모든 버킷의 오브젝트는 정책의 후속 규칙에 의해 배치됩니다.

4. 보존 다이어그램을 검토하여 여러 개체를 유지하는 방법을 알아보십시오.
   a. 비활성 정책의 각 규칙에 대한 보존 다이어그램을 보려면 * Expand All * 을 선택합니다.
   b. 보존 다이어그램을 검토하려면 * 기간 * 및 * 스토리지 풀 * 을 선택합니다. FabricPool 버킷 또는 테넌트에 적용되는 모든 규칙이 오브젝트 * 영구 * 를 유지하는지 확인합니다.
5. 비활성 정책을 검토했으면 * 활성화 및 계속 * 을 선택하여 정책을 활성화하고 트래픽 분류 단계로 이동합니다.

> ILM 정책의 오류로 인해 복구할 수 없는 데이터 손실이 발생할 수 있습니다. 활성화하기 전에 정책을 주의 깊게 검토하십시오.

9단계 중 **8**단계**:** 트래픽 분류 정책을 생성합니다

FabricPool 설정 마법사는 FabricPool 워크로드를 모니터링하는 데 사용할 수 있는 트래픽 분류 정책을 생성할 수 있는 옵션으로 제공됩니다. 시스템에서 생성한 정책은 일치하는 규칙을 사용하여 생성한 버킷과 관련된 모든 네트워크 트래픽을 식별합니다. 이 정책은 트래픽만 모니터링하며, FabricPool 또는 다른 클라이언트의 트래픽은 제한하지 않습니다.

이 단계에 대한 자세한 내용은 을 "FabricPool에 대한 트래픽 분류 정책을 생성합니다"참조하십시오.

단계

1. 정책을 검토합니다.
2. 이 트래픽 분류 정책을 만들려면 * 생성 및 계속 * 을 선택합니다.

   FabricPool에서 StorageGRID로 데이터 계층화를 시작하는 즉시 트래픽 분류 정책 페이지로 이동하여 이 정책에 대한 네트워크 트래픽 메트릭을 볼 수 있습니다. 나중에 규칙을 추가하여 다른 워크로드를 제한하고 FabricPool 워크로드에 대부분의 대역폭이 있는지 확인할 수도 있습니다.

3. 그렇지 않으면 * 이 단계 건너뛰기 * 를 선택합니다.

9단계**:** 요약 검토

요약에서는 부하 분산 장치, 테넌트 및 버킷 이름, 트래픽 분류 정책 및 활성 ILM 정책 등 구성한 항목에 대한 세부 정보를 제공합니다.

단계

1. 요약 내용을 검토합니다.
2. 마침 * 을 선택합니다.

다음 단계

FabricPool 마법사를 완료한 후 다음 추가 단계를 수행합니다.

단계

1. 로 "ONTAP 시스템 관리자를 구성합니다" 이동하여 저장된 값을 입력하고 연결의 ONTAP 측을 완료합니다. StorageGRID를 클라우드 계층으로 추가하고, 클라우드 계층을 로컬 계층에 연결하여 FabricPool를 생성하고, 볼륨 계층화 정책을 설정해야 합니다.
2. 로 "DNS 서버를 구성합니다" 이동하여 StorageGRID 서버 이름(정규화된 도메인 이름)을 사용할 각 StorageGRID IP 주소에 연결하는 레코드가 DNS에 포함되어 있는지 확인합니다.
3. StorageGRID 감사 로그 및 기타 글로벌 구성 옵션에 대한 모범 사례를 보려면 를 "기타 StorageGRID 및 FabricPool 모범 사례"참조하십시오.

StorageGRID를 수동으로 구성합니다

FabricPool에 대한 고가용성(HA) 그룹을 생성합니다

FabricPool와 함께 사용하도록 StorageGRID를 구성할 때 HA(고가용성) 그룹을 하나 이상 선택적으로 생성할 수 있습니다. HA 그룹은 각 노드에 StorageGRID 로드 밸런서 서비스가 포함된 노드 모음입니다. HA 그룹에는 게이트웨이 노드, 관리자 노드 또는 둘 다 포함될 수 있습니다.

HA 그룹을 사용하면 FabricPool 데이터 연결을 계속 사용할 수 있습니다. HA 그룹은 가상 IP 주소(VIP)를 사용하여 로드 밸런서 서비스에 대한 고가용성 액세스를 제공합니다. HA 그룹의 액티브 인터페이스에 장애가 발생할 경우 백업 인터페이스에서 FabricPool 작업에 거의 영향을 주지 않고 워크로드를 관리할 수 있습니다.

이 작업에 대한 자세한 내용은 을 "고가용성 그룹을 관리합니다"참조하십시오. FabricPool 설정 마법사를 사용하여 이 작업을 완료하려면 로 이동합니다"FabricPool 설정 마법사를 액세스하고 완료합니다".

시작하기 전에

- 를 검토했습니다."고가용성 그룹에 대한 Best Practice"
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.
- VLAN을 사용하려는 경우 VLAN 인터페이스를 만들었습니다. 을 "VLAN 인터페이스를 구성합니다"참조하십시오.

단계

1. 구성 * > * 네트워크 * > * 고가용성 그룹 * 을 선택합니다.
2. Create * 를 선택합니다.
3. Enter details * (세부 정보 입력) 단계에 대해 다음 필드를 작성합니다.

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

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

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

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

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

   행을 드래그하여 * Priority order * 열의 값을 변경합니다.

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

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

6. IP 주소 입력 * 단계에 대해 다음 필드를 입력합니다.

필드에 입력합니다	설명
서브넷 CIDR	CIDR 표기법 &#8212의 VIP 서브넷 주소, IPv4 주소, 슬래시 및 서브넷 길이(0-32). 네트워크 주소에는 호스트 비트가 설정되어 있지 않아야 합니다. `192.16.0.0/22`예를 들어,
게이트웨이 IP 주소(선택 사항)	선택 사항. 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.
가상 IP 주소입니다	HA 그룹에 액티브 인터페이스에 대한 VIP 주소는 하나 이상, 10개 이하로 입력하십시오. 모든 VIP 주소는 VIP 서브넷 내에 있어야 합니다. 하나 이상의 주소는 IPv4여야 합니다. 선택적으로 추가 IPv4 및 IPv6 주소를 지정할 수 있습니다.

7. Create HA group * 을 선택한 다음 * Finish * 를 선택합니다.

FabricPool용 로드 밸런서 끝점을 만듭니다

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

FabricPool와 함께 사용하도록 StorageGRID를 구성할 때는 로드 밸런서 끝점을 구성하고 ONTAP와 StorageGRID 간의 연결을 보호하는 데 사용되는 로드 밸런서 끝점 인증서를 업로드하거나 생성해야 합니다.

FabricPool 설정 마법사를 사용하여 이 작업을 완료하려면 로 이동합니다"FabricPool 설정 마법사를 액세스하고

완료합니다".

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.
- 일반 및 에 대한 검토를 "로드 균형 조정에 대한 고려 사항""FabricPool의 로드 밸런싱 모범 사례"마쳤습니다.

단계

1. 구성 * > * 네트워크 * > * 로드 밸런서 엔드포인트 * 를 선택합니다.
2. Create * 를 선택합니다.
3. Enter endpoint details * 단계에서 다음 필드를 입력합니다.

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

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

모드를 선택합니다	설명
글로벌(기본값)	클라이언트는 게이트웨이 노드 또는 관리 노드의 IP 주소, 네트워크에 있는 HA 그룹의 가상 IP(VIP) 주소 또는 해당 FQDN을 사용하여 끝점에 액세스할 수 있습니다. 이 끝점의 접근성을 제한할 필요가 없는 경우 * Global * (글로벌 *) 설정(기본값)을 사용합니다.

모드를 선택합니다	설명
HA 그룹의 가상 IP입니다	클라이언트는 HA 그룹의 가상 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다. 이 바인딩 모드의 엔드포인트는 엔드포인트에 대해 선택한 HA 그룹이 겹치지 않는 한 모두 동일한 포트 번호를 사용할 수 있습니다.
노드 인터페이스	클라이언트는 선택한 노드 인터페이스의 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다.
노드 유형입니다	선택한 노드 유형에 따라 클라이언트는 관리 노드의 IP 주소(또는 해당 FQDN)나 게이트웨이 노드의 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다.

5. Tenant access * 단계에서 다음 중 하나를 선택합니다.

필드에 입력합니다	설명
모든 테넌트 허용(기본값)	모든 테넌트 계정은 이 엔드포인트를 사용하여 해당 버킷에 액세스할 수 있습니다. • 모든 테넌트 허용 * 은 거의 항상 FabricPool에 사용되는 로드 밸런서 끝점에 적합한 옵션입니다. 테넌트 계정을 아직 생성하지 않은 경우 이 옵션을 선택해야 합니다.
선택한 테넌트 허용	선택한 테넌트 계정만 이 끝점을 사용하여 해당 버킷을 액세스할 수 있습니다.
선택한 테넌트 차단	선택한 테넌트 계정은 이 끝점을 사용하여 해당 버킷을 액세스할 수 없습니다. 다른 모든 테넌트는 이 끝점을 사용할 수 있습니다.

6. 인증서 연결 * 단계에서 다음 중 하나를 선택합니다.

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

7. 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.

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.

이 작업에 대한 자세한 내용은 을 "테넌트 계정을 생성합니다"참조하십시오. FabricPool 설정 마법사를 사용하여 이 작업을 완료하려면 로 이동합니다"FabricPool 설정 마법사를 액세스하고 완료합니다".

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

단계

1. Tenants * 를 선택합니다.
2. Create * 를 선택합니다.
3. 세부 정보 입력 단계에 대해 다음 정보를 입력합니다.

필드에 입력합니다	설명
이름	테넌트 계정의 이름입니다. 테넌트 이름은 고유해야 할 필요가 없습니다. 테넌트 계정이 생성되면 고유한 숫자 계정 ID를 받습니다.
설명(선택 사항)	테넌트를 식별하는 데 도움이 되는 설명입니다.
클라이언트 유형입니다	FabricPool의 경우 * S3 * 이어야 합니다.
스토리지 할당량(선택 사항)	FabricPool의 경우 이 필드를 비워 둡니다.

4. 권한 선택 단계의 경우:
   a. 플랫폼 서비스 허용 * 을 선택하지 마십시오.

      FabricPool 테넌트는 일반적으로 CloudMirror 복제와 같은 플랫폼 서비스를 사용할 필요가 없습니다.

   b. 필요에 따라 * 고유 ID 소스 사용 * 을 선택합니다.
   c. S3 선택 허용 * 을 선택하지 마십시오.

      FabricPool 테넌트는 일반적으로 S3 Select를 사용할 필요가 없습니다.

   d. 필요에 따라 * Use GRID Federation connection * 을 선택하여 테넌트가 계정 클론 및 교차 그리드 복제에 를

사용할 수 있도록 "그리드 페더레이션 연결"합니다. 그런 다음 사용할 그리드 페더레이션 연결을 선택합니다.

5. 루트 액세스 정의 단계의 경우 StorageGRID 시스템에서"ID 제휴", "SSO(Single Sign-On)"또는 둘 모두를 사용하는지 여부에 따라 테넌트 계정에 대한 초기 루트 액세스 권한을 가질 사용자를 지정합니다.

옵션을 선택합니다	이렇게 하십시오
ID 페더레이션이 활성화되지 않은 경우	테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션이 활성화된 경우	a. 테넌트에 대한 루트 액세스 권한이 있는 기존 통합 그룹을 선택합니다. b. 필요에 따라 테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션 및 SSO(Single Sign-On)가 모두 활성화된 경우	테넌트에 대한 루트 액세스 권한이 있는 기존 통합 그룹을 선택합니다. 로컬 사용자는 로그인할 수 없습니다.

6. 테넌트 생성 * 을 선택합니다.

S3 버킷을 생성하고 접근 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.

이 작업에 대한 자세한 내용은 "S3 버킷을 생성합니다" 및 "자체 S3 액세스 키를 생성합니다"을 참조하십시오. FabricPool 설정 마법사를 사용하여 이 작업을 완료하려면 로 이동합니다"FabricPool 설정 마법사를 액세스하고 완료합니다".

시작하기 전에

- FabricPool 사용을 위해 테넌트 계정을 만들었습니다.
- 테넌트 계정에 대한 루트 액세스 권한이 있습니다.

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. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.

   b. Create bucket * 을 선택합니다.

   c. FabricPool에 사용할 StorageGRID 버킷의 이름을 입력합니다. `fabricpool-bucket`예를 들어,

버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

d. 이 버킷의 영역을 선택합니다.

   기본적으로 모든 버킷은 해당 `us-east-1` 지역에서 생성됩니다.

e. Continue * 를 선택합니다.

f. Create bucket * 을 선택합니다.

FabricPool 버킷에 대해 * 개체 버전 관리 사용 * 을 선택하지 마십시오. 마찬가지로, * 사용 가능 * 또는 기본값이 아닌 일관성을 사용하도록 FabricPool 버킷을 편집하지 마십시오. FabricPool 버킷에 권장되는 버킷 일관성은 새 버킷의 기본 정합성 보장인 * 새 버킷에 대한 Read-after-new-write * 입니다.

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 StorageGRID에서 새 액세스 키와 비밀 액세스 키를 생성하는 경우 StorageGRID에서 이전 값을 삭제하기 전에 새 키를 ONTAP에 입력합니다. 그렇지 않으면 ONTAP에서 일시적으로 StorageGRID에 액세스하지 못할 수 있습니다.

FabricPool 데이터에 대한 **ILM**을 구성합니다

이 간단한 예제 정책을 자신의 ILM 규칙 및 정책의 시작 지점으로 사용할 수 있습니다.

이 예제에서는 콜로라도주 덴버의 단일 데이터 센터에 4개의 스토리지 노드가 있는 StorageGRID 시스템에 대한 ILM 규칙 및 ILM 정책을 디자인한다고 가정합니다. 이 예제의 FabricPool 데이터는 이라는 버킷을 `fabricpool-bucket` 사용합니다.

다음 ILM 규칙 및 정책은 예일 뿐입니다. ILM 규칙을 구성하는 방법은 여러 가지가 있습니다. 새 정책을 활성화하기 전에 시뮬레이션하여 콘텐츠 손실을 방지하기 위한 의도대로 작동하는지 확인합니다. 자세한 내용은 을 참조하십시오"ILM을 사용하여 개체를 관리합니다".

데이터 손실을 방지하려면 FabricPool 클라우드 계층 데이터를 만료 또는 삭제할 ILM 규칙을 사용하지 마십시오. StorageGRID ILM에서 FabricPool 객체가 삭제되지 않도록 보존 기간을 * Forever * 로 설정합니다.

시작하기 전에

- 를 검토했습니다."FabricPool 데이터에 ILM을 사용하는 모범 사례"

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "ILM 또는 루트 액세스 권한"있습니다.
- 이전 StorageGRID 버전에서 StorageGRID 11.9로 업그레이드한 경우 사용할 스토리지 풀을 구성한 것입니다. 일반적으로 데이터를 저장하는 데 사용할 각 StorageGRID 사이트에 대해 스토리지 풀을 생성해야 합니다.

> 이 필수 구성 요소는 처음에 StorageGRID 11.7 또는 11.8을 설치한 경우에는 적용되지 않습니다. 이러한 버전 중 하나를 처음 설치하면 각 사이트에 대해 스토리지 풀이 자동으로 생성됩니다.

단계

1. 의 데이터에만 적용되는 ILM 규칙을 `fabricpool-bucket` 생성합니다. 이 예제 규칙은 삭제 코딩 복사본을 만듭니다.

규칙 정의	예제 값
규칙 이름	FabricPool 데이터에 대한 2+1 삭제 코딩
버킷 이름	`fabricpool-bucket` FabricPool 테넌트 계정에서도 필터링할 수 있습니다.
고급 필터	객체 크기가 0.2MB를 초과합니다. • 참고: * FabricPool는 4MB 객체만 쓰지만 이 규칙이 삭제 코딩을 사용하기 때문에 객체 크기 필터를 추가해야 합니다.
참조 시간	수집 시간
기간 및 배치	0일째 매장에서 영원히 덴버에서 2+1 EC 방식을 사용하여 삭제 코딩을 통해 오브젝트를 저장하고 이러한 오브젝트를 StorageGRID에 영구 보관합니다. 데이터 손실을 방지하려면 FabricPool 클라우드 계층 데이터를 만료 또는 삭제할 ILM 규칙을 사용하지 마십시오.
수집 동작	균형

2. 첫 번째 규칙과 일치하지 않는 개체의 복제된 복사본 2개를 생성하는 기본 ILM 규칙을 생성합니다. 기본 필터(테넌트 계정 또는 버킷 이름) 또는 고급 필터를 선택하지 마십시오.

규칙 정의	예제 값
규칙 이름	2개의 복제 복사본
버킷 이름	없음

규칙 정의	예제 값
고급 필터	없음
참조 시간	수집 시간
기간 및 배치	0일째 매장에서 영원히 덴버에서 2개의 복사본을 복제하여 개체를 저장합니다.
수집 동작	균형

3. ILM 정책을 생성하고 두 규칙을 선택합니다. 복제 규칙에서는 필터를 사용하지 않으므로 정책의 기본(마지막) 규칙일 수 있습니다.
4. 테스트 오브젝트를 그리드에 수집.
5. 테스트 개체를 사용하여 정책을 시뮬레이션하여 동작을 확인합니다.
6. 정책을 활성화합니다.

이 정책이 활성화되면 StorageGRID는 다음과 같이 오브젝트 데이터를 배치합니다.

- 의 FabricPool에서 계층화된 데이터는 `fabricpool-bucket` 2+1 삭제 코딩 체계를 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.
- 복사본은 StorageGRID에서 영구적으로 유지됩니다. StorageGRID ILM은 이러한 개체를 삭제하지 않습니다.

FabricPool에 대한 트래픽 분류 정책을 생성합니다

FabricPool 워크로드에 대한 서비스 품질을 최적화하기 위해 StorageGRID 트래픽 분류 정책을 선택적으로 설계할 수 있습니다.

이 작업에 대한 자세한 내용은 을 "트래픽 분류 정책을 관리합니다"참조하십시오. FabricPool 설정 마법사를 사용하여 이 작업을 완료하려면 로 이동합니다"FabricPool 설정 마법사를 액세스하고 완료합니다".

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"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 워크로드에 대부분의 대역폭이 있는지 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 서비스 품질 제한을 두지 않아야 하며 다른 워크로드만 제한해야 합니다.
- 다른 워크로드에 대한 제한에는 이러한 워크로드의 동작이 고려되어야 합니다. 또한 그리드 크기 조정 및 기능과 예상되는 활용률에 따라 제한이 달라집니다.

단계

1. 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택합니다.
2. Create * 를 선택합니다.
3. 정책의 이름과 설명(선택 사항)을 입력하고 * Continue * 를 선택합니다.
4. 일치하는 규칙 추가 단계에 대해 하나 이상의 규칙을 추가합니다.
   a. 규칙 추가 * 를 선택합니다
   b. 유형 에서 * 로드 밸런서 끝점 * 을 선택하고 FabricPool용으로 생성한 로드 밸런서 끝점을 선택합니다.

      FabricPool 테넌트 계정 또는 버킷을 선택할 수도 있습니다.

   c. 이 트래픽 정책이 다른 끝점의 트래픽을 제한하도록 하려면 * 역일치 * 를 선택합니다.
5. 필요에 따라 규칙에 일치하는 네트워크 트래픽을 제어하기 위해 하나 이상의 제한을 추가합니다.

   StorageGRID는 제한을 추가하지 않아도 메트릭을 수집하므로 트래픽 추세를 파악할 수 있습니다.

   a. 제한 추가 * 를 선택합니다.
   b. 제한할 트래픽 유형과 적용할 제한을 선택합니다.
6. Continue * 를 선택합니다.
7. 트래픽 분류 정책을 읽고 검토하십시오. Previous * (이전 *) 버튼을 사용하여 돌아가서 필요에 따라 변경합니다. 정책에 만족하면 * Save and continue * 를 선택합니다.

작업을 마친 후

"네트워크 트래픽 메트릭을 확인합니다" 정책이 예상한 트래픽 제한을 적용하고 있는지 확인합니다.

ONTAP 시스템 관리자를 구성합니다

필요한 StorageGRID 정보를 확인한 후 ONTAP로 이동하여 StorageGRID을 클라우드 계층으로 추가할 수 있습니다.

시작하기 전에

- FabricPool 설정 마법사를 완료하면 다운로드한 파일이 있는 `ONTAP_FabricPool_settings_bucketname.txt` 것입니다.
- StorageGRID를 수동으로 구성한 경우 StorageGRID에 사용하고 있는 FQDN(정규화된 도메인 이름)이나 StorageGRID HA 그룹의 VIP(가상 IP) 주소, 로드 밸런서 끝점의 포트 번호, 로드 밸런서 인증서, 테넌트 계정의 루트 사용자에 대한 액세스 키 ID 및 암호 키와 해당 테넌트에서 버킷 ONTAP의 이름이 사용됩니다.

ONTAP 시스템 관리자에 액세스합니다

다음 지침은 ONTAP System Manager를 사용하여 StorageGRID를 클라우드 계층으로 추가하는 방법을 설명합니다. ONTAP CLI를 사용하여 동일한 구성을 완료할 수 있습니다. 자세한 내용은 을 "FabricPool에 대한 ONTAP 설명서 "참조하십시오.

단계

1. StorageGRID에 계층화할 ONTAP 클러스터에 대한 System Manager에 액세스합니다.
2. 클러스터의 관리자로 로그인합니다.
3. 스토리지 * > * 계층 * > * 클라우드 계층 추가 * 로 이동합니다.
4. 오브젝트 저장소 공급자 목록에서 * StorageGRID * 를 선택합니다.

StorageGRID 값을 입력합니다

자세한 내용은 을 "FabricPool에 대한 ONTAP 설명서" 참조하십시오.

단계

1. 수동으로 얻은 파일 또는 값을 사용하여 클라우드 계층 추가 양식을 `ONTAP_FabricPool_settings_bucketname.txt` 작성합니다.

필드에 입력합니다	설명
이름	이 클라우드 계층의 고유한 이름을 입력하십시오. 기본값을 사용할 수 있습니다.
URL 스타일	"S3 끝점 도메인 이름을 구성했습니다"가상 호스트 스타일 URL * 을 선택합니다. ONTAP의 기본값은 * 경로 스타일 URL * 이지만 StorageGRID에 가상 호스팅 스타일 요청을 사용하는 것이 좋습니다. FQDN(서버 이름) * 필드에 도메인 이름 대신 IP 주소를 제공하는 경우 * 경로 스타일 URL * 을 사용해야 합니다.
서버 이름(FQDN)	StorageGRID에 사용 중인 FQDN(정규화된 도메인 이름)이나 StorageGRID HA 그룹의 VIP(가상 IP) 주소를 입력합니다. `s3.storagegrid.*company*.com`예를 들어, 다음 사항에 유의하십시오. • 여기에서 지정하는 IP 주소 또는 도메인 이름은 StorageGRID 로드 밸런서 끝점에 대해 업로드하거나 생성한 인증서와 일치해야 합니다. • 도메인 이름을 제공하는 경우 DNS 레코드는 StorageGRID에 연결하는 데 사용할 각 IP 주소에 매핑되어야 합니다. 을 "DNS 서버를 구성합니다 "참조하십시오.
SSL	Enabled(기본값).

필드에 입력합니다	설명
오브젝트 저장소 인증서	및 `-----END CERTIFICATE-----` 을 포함하여 StorageGRID 로드 밸런서 끝점에 사용 중인 인증서 PEM을 붙여 넣습니다 `-----BEGIN CERTIFICATE-----`. • 참고: * 중간 CA가 StorageGRID 인증서를 발급한 경우 중간 CA 인증서를 제공해야 합니다. StorageGRID 인증서가 루트 CA에서 직접 발급된 경우 루트 CA 인증서를 제공해야 합니다.
포트	StorageGRID 로드 밸런서 끝점에서 사용하는 포트를 입력합니다. ONTAP는 StorageGRID에 연결할 때 이 포트를 사용합니다. 예: 10433.
액세스 키 및 비밀 키	StorageGRID 테넌트 계정의 루트 사용자에 대한 액세스 키 ID 및 암호 액세스 키를 입력합니다. • 팁 *: 나중에 StorageGRID에서 새 액세스 키와 비밀 액세스 키를 생성하는 경우 StorageGRID에서 이전 값을 삭제하기 전에 새 키를 ONTAP에 입력합니다. 그렇지 않으면 ONTAP에서 일시적으로 StorageGRID에 액세스하지 못할 수 있습니다.
컨테이너 이름입니다	이 ONTAP 계층에서 사용하기 위해 생성한 StorageGRID 버킷의 이름을 입력합니다.

2. ONTAP에서 최종 FabricPool 구성을 완료합니다.
   a. 하나 이상의 애그리게이트를 클라우드 계층에 연결
   b. 필요한 경우 볼륨 계층화 정책을 생성합니다.

DNS 서버를 구성합니다

고가용성 그룹, 로드 밸런서 끝점 및 S3 끝점 도메인 이름을 구성한 후에는 DNS에 StorageGRID에 필요한 항목이 포함되어 있는지 확인해야 합니다. 보안 인증서와 사용할 수 있는 각 IP 주소에 각 이름에 대한 DNS 항목을 포함해야 합니다.

을 "로드 균형 조정에 대한 고려 사항"참조하십시오.

StorageGRID 서버 이름에 대한 DNS 항목입니다

DNS 항목을 추가하여 StorageGRID 서버 이름(정규화된 도메인 이름)을 사용할 각 StorageGRID IP 주소에 연결합니다. DNS에 입력하는 IP 주소는 로드 밸런싱 노드의 HA 그룹을 사용하는지 여부에 따라 달라집니다.

- HA 그룹을 구성한 경우 ONTAP는 해당 HA 그룹의 가상 IP 주소에 연결됩니다.
- HA 그룹을 사용하지 않는 경우 ONTAP는 게이트웨이 노드 또는 관리 노드의 IP 주소를 사용하여 StorageGRID 로드 밸런서 서비스에 연결할 수 있습니다.
- 서버 이름이 둘 이상의 IP 주소로 확인되는 경우 ONTAP는 모든 IP 주소(최대 16개의 IP 주소)를 사용하여 클라이언트 연결을 설정합니다. 연결이 설정되면 IP 주소가 라운드 로빈 방식으로 선택됩니다.

가상 호스팅 스타일 요청에 대한 **DNS** 항목

을 정의하고 가상 호스팅 스타일 요청을 사용할 경우 "S3 끝점 도메인 이름"모든 와일드카드 이름을 포함하여 필요한 모든 S3 끝점 도메인 이름에 DNS 항목을 추가합니다.

FabricPool에 대한 StorageGRID 모범 사례

고가용성**(HA)** 그룹에 대한 모범 사례

StorageGRID를 FabricPool 클라우드 계층으로 연결하기 전에 StorageGRID HA(고가용성) 그룹에 대해 알아보고 FabricPool에 HA 그룹을 사용한 모범 사례를 검토하십시오.

HA 그룹이란 무엇입니까?

HA(고가용성) 그룹은 여러 StorageGRID 게이트웨이 노드, 관리 노드 또는 둘 모두의 인터페이스 모음입니다. HA 그룹을 사용하면 클라이언트 데이터 연결을 계속 사용할 수 있습니다. HA 그룹의 액티브 인터페이스에 장애가 발생할 경우 백업 인터페이스에서 FabricPool 작업에 거의 영향을 주지 않고 워크로드를 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.

고가용성 그룹에 대한 자세한 내용은 을 참조하십시오"고가용성(HA) 그룹 관리".

HA 그룹 사용

FabricPool용 StorageGRID HA 그룹을 생성하는 모범 사례는 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. 다른 HA 구성의 이점에 대한 자세한 내용은 을 참조하십시오"HA 그룹에 대한 구성 옵션".

FabricPool의 로드 밸런싱 모범 사례

StorageGRID를 FabricPool 클라우드 계층으로 연결하기 전에 로드 밸런서와 FabricPool를 함께 사용하는 모범 사례를 검토하십시오.

StorageGRID 로드 밸런서 및 로드 밸런서 인증서에 대한 일반적인 내용은 을 참조하십시오."로드 균형 조정에 대한 고려 사항"

FabricPool에 사용되는 로드 밸런서 끝점에 대한 테넌트 액세스에 대한 모범 사례

특정 부하 분산 엔드포인트를 사용하여 해당 버킷에 액세스할 수 있는 테넌트를 제어할 수 있습니다. 모든 테넌트를 허용하거나, 일부 테넌트를 허용하거나, 일부 테넌트를 차단할 수 있습니다. FabricPool 사용을 위해 로드 균형 조정 끝점을 만들 때 * 모든 테넌트 허용 * 을 선택합니다. ONTAP는 StorageGRID 버킷에 저장된 데이터를 암호화하므로 이 추가 보안 계층에서는 추가 보안이 제공되지 않습니다.

FabricPool 사용을 위해 StorageGRID 로드 밸런서 끝점을 만들 때 ONTAP가 StorageGRID를 사용하여 인증할 수 있도록 하는 보안 인증서를 제공합니다.

대부분의 경우 ONTAP와 StorageGRID 간의 연결은 TLS(전송 계층 보안) 암호화를 사용해야 합니다. TLS 암호화 없이 FabricPool를 사용하는 것은 지원되지만 권장되지 않습니다. StorageGRID 로드 밸런서 끝점에 대한 네트워크 프로토콜을 선택할 때 * HTTPS * 를 선택합니다. 그런 다음 ONTAP에서 StorageGRID를 인증할 수 있도록 보안 인증서를 제공합니다.

로드 밸런싱 끝점의 서버 인증서에 대한 자세한 내용은 다음을 참조하십시오.

- "보안 인증서를 관리합니다"
- "로드 균형 조정에 대한 고려 사항"
- "서버 인증서에 대한 강화 지침"

ONTAP에 인증서를 추가합니다

StorageGRID를 FabricPool 클라우드 계층으로 추가하는 경우 루트 및 하위 CA(인증 기관) 인증서를 포함하여 ONTAP 클러스터에 동일한 인증서를 설치해야 합니다.

인증서 만료 관리

> ONTAP와 StorageGRID 간의 연결을 보호하는 데 사용되는 인증서가 만료되면 FabricPool가 일시적으로 작동을 멈추고 ONTAP가 StorageGRID로 계층화된 데이터에 대한 액세스를 일시적으로 상실합니다.

인증서 만료 문제를 방지하려면 다음 모범 사례를 따르십시오.

- 로드 밸런서 엔드포인트 인증서 만료 * 및 * S3 API용 글로벌 서버 인증서 만료 * 경고와 같이 인증서 만료 날짜가 다가올 경우 경고를 주의 깊게 모니터링하십시오.
- 항상 인증서의 StorageGRID 및 ONTAP 버전을 동기화된 상태로 유지합니다. 로드 밸런서 끝점에 사용되는 인증서를 교체하거나 갱신하는 경우 클라우드 계층에 대해 ONTAP에서 사용하는 것과 동일한 인증서를 교체하거나 갱신해야 합니다.
- 공개적으로 서명된 CA 인증서를 사용합니다. CA에서 서명한 인증서를 사용하는 경우 그리드 관리 API를 사용하여 인증서 회전을 자동화할 수 있습니다. 따라서 만료 임박한 인증서를 중단 없이 교체할 수 있습니다.
- 자체 서명된 StorageGRID 인증서를 생성했으며 인증서가 곧 만료될 경우 기존 인증서가 만료되기 전에 StorageGRID 및 ONTAP에서 수동으로 인증서를 교체해야 합니다. 자체 서명된 인증서가 이미 만료된 경우 ONTAP에서 인증서 유효성 검사를 해제하면 액세스 손실이 방지됩니다.

  자세한 내용은 을 "NetApp 기술 자료: 기존 ONTAP FabricPool 배포에서 새로운 StorageGRID 자체 서명 서버 인증서를 구성하는 방법" 참조하십시오.

FabricPool 데이터에 **ILM**을 사용하는 모범 사례

FabricPool를 사용하여 데이터를 StorageGRID에 계층화할 경우 FabricPool 데이터에 대한 StorageGRID 정보 라이프사이클 관리(ILM)를 사용하기 위한 요구사항을 이해해야 합니다.

FabricPool에는 StorageGRID ILM 규칙 또는 정책에 대한 지식이 없습니다. StorageGRID ILM 정책이 잘못 구성된 경우 데이터 손실이 발생할 수 있습니다. 자세한 내용은 및 을 "ILM 규칙을 사용하여 오브젝트를 관리합니다""ILM 정책을 생성합니다"참조하십시오.

FabricPool에서 **ILM** 사용 지침

FabricPool 설정 마법사를 사용하면 마법사는 사용자가 생성하는 각 S3 버킷에 대한 새 ILM 규칙을 자동으로 생성하고 해당 규칙을 비활성 정책에 추가합니다. 정책을 활성화하라는 메시지가 표시됩니다. 자동으로 생성된 규칙은 권장되는 모범 사례를 따릅니다. 단일 사이트에서 2+1 삭제 코딩을 사용합니다.

FabricPool 설정 마법사를 사용하지 않고 StorageGRID를 수동으로 구성하는 경우에는 이러한 지침을 검토하여 ILM 규칙 및 ILM 정책이 FabricPool 데이터 및 비즈니스 요구 사항에 적합한지 확인하십시오. 이러한 지침을 충족하기 위해 새 규칙을 생성하고 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.

- 필요한 경우"StorageGRID에서 FabricPool 데이터를 제거합니다", ONTAP를 사용하여 FabricPool 볼륨에 대한 모든 데이터를 검색하고 성능 계층으로 승격합니다.

  데이터 손실을 방지하려면 FabricPool 클라우드 계층 데이터를 만료 또는 삭제할 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. 클라우드 스토리지 풀을 사용하여 FabricPool 데이터를 다른 오브젝트 저장소로 이동할 수는 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.

기타 **StorageGRID** 및 **FabricPool** 모범 사례

FabricPool와 함께 사용하도록 StorageGRID 시스템을 구성할 때 다른 StorageGRID 옵션을

변경해야 할 수 있습니다. 글로벌 설정을 변경하기 전에 변경이 다른 S3 애플리케이션에 어떤 영향을 미치는지 고려하십시오.

감사 메시지 및 로그 대상

FabricPool 워크로드는 읽기 작업의 비율이 높아 대량의 감사 메시지를 생성할 수 있는 경우가 많습니다.

- FabricPool 또는 다른 S3 응용 프로그램에 대한 클라이언트 읽기 작업 기록이 필요하지 않은 경우 * 구성 * > * 모니터링 * > * 감사 및 syslog 서버 * 로 이동합니다. 클라이언트 읽기 * 설정을 * 오류 * 로 변경하여 감사 로그에 기록되는 감사 메시지 수를 줄입니다. 자세한 내용은 을 "감사 메시지 및 로그 대상을 구성합니다" 참조하십시오.
- 대규모 그리드가 있거나, 여러 유형의 S3 애플리케이션을 사용하거나, 모든 감사 데이터를 보존하려는 경우, 외부 syslog 서버를 구성하고 감사 정보를 원격으로 저장합니다. 외부 서버를 사용하면 감사 데이터의 완성도를 낮추지 않고도 감사 메시지 로깅의 성능 영향을 최소화할 수 있습니다. 자세한 내용은 을 "외부 syslog 서버에 대한 고려 사항" 참조하십시오.

오브젝트 암호화

StorageGRID를 구성할 때 다른 StorageGRID 클라이언트에 데이터 암호화가 필요한 경우 을 선택적으로 설정할 수 "저장된 오브젝트 암호화에 대한 글로벌 옵션입니다"있습니다. FabricPool에서 StorageGRID로 계층화된 데이터는 이미 암호화되므로 StorageGRID 설정을 활성화할 필요가 없습니다. 클라이언트측 암호화 키는 ONTAP의 소유입니다.

오브젝트 압축

StorageGRID를 구성할 때는 를 활성화하지 마십시오."저장된 개체를 압축하는 전역 옵션" FabricPool에서 StorageGRID로 계층화된 데이터는 이미 압축된 상태입니다. StorageGRID 옵션을 사용하면 개체의 크기가 더 작아지지 않습니다.

버킷 일관성

FabricPool 버킷의 경우 새 버킷의 기본 정합성 보장인 * 새 버킷의 경우 Read-after-new-write * 가 권장됩니다. 사용 가능 * 또는 * 강력한 사이트 * 를 사용하도록 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.

StorageGRID에서 FabricPool 데이터를 제거합니다

현재 StorageGRID에 저장된 FabricPool 데이터를 제거해야 하는 경우 ONTAP를 사용하여 FabricPool 볼륨에 대한 모든 데이터를 검색하고 성능 계층으로 상향 이동시켜야 합니다.

시작하기 전에

- 의 지침과 고려 사항을 검토했습니다. "데이터를 성능 계층으로 상향 이동"

- ONTAP 9.8 이상을 사용하고 있습니다.
- 을 사용하고 "지원되는 웹 브라우저"있습니다.
- 가 있는 FabricPool 테넌트 계정의 StorageGRID 사용자 그룹에 속해 "모든 버킷 또는 루트 액세스 권한을 관리합니다"있습니다.

이 작업에 대해

다음 지침은 StorageGRID에서 FabricPool로 데이터를 다시 이동하는 방법을 설명합니다. ONTAP 및 StorageGRID 테넌트 관리자를 사용하여 이 절차를 수행합니다.

단계

1. ONTAP에서 명령을 `volume modify` 실행합니다.

   ```
   `tiering-policy`를 로 `none` 설정하여 새로운 계층화를 중지하고 `cloud-retrieval-policy` `promote` 이전에 StorageGRID에 계층화된 모든 데이터를 반환하도록 설정합니다.
   ```

   을 "FabricPool 볼륨의 모든 데이터를 성능 계층으로 상향 이동합니다"참조하십시오.

2. 작업이 완료될 때까지 기다립니다.

   명령을 옵션과 함께 `tiering` 사용하여 을 수행할 "성능 계층 프로모션의 상태를 확인합니다" 수 `volume object-store` 있습니다.

3. 상향 이동 작업이 완료되면 FabricPool 테넌트 계정에 대한 StorageGRID 테넌트 관리자에 로그인합니다.
4. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
5. FabricPool 버킷이 비어 있는지 확인합니다.
6. 버킷이 비어 있는 경우"버킷을 삭제합니다".

작업을 마친 후

버킷을 삭제하면 FabricPool에서 StorageGRID로의 계층화를 더 이상 계속할 수 없습니다. 하지만 로컬 계층이 StorageGRID 클라우드 계층에 아직 연결되어 있으므로 ONTAP 시스템 관리자는 버킷에 액세스할 수 없음을 나타내는 오류 메시지를 반환합니다.

이러한 오류 메시지를 방지하려면 다음 중 하나를 수행하십시오.

- FabricPool 미러를 사용하여 애그리게이트에 다른 클라우드 계층을 연결할 수 있습니다.
- FabricPool 애그리게이트에서 비 FabricPool 애그리게이트로 데이터를 이동한 다음 사용되지 않은 애그리게이트를 삭제합니다.

자세한 내용은 를 "FabricPool에 대한 ONTAP 설명서" 참조하십시오.

StorageGRID 테넌트 및 클라이언트 사용

테넌트 계정을 사용합니다

테넌트 계정을 사용합니다

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.

테넌트 계정은 저장된 객체를 다른 엔터티로 분리하는 데 사용할 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. 자세한 내용은 구현 지침을 "S3 버킷 및 버킷 정책"참조하십시오.

- * 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 "그리드 관리자를 사용하는 StorageGRID 그리드 관리자"생성됩니다. 테넌트 계정을 생성할 때 그리드 관리자는 다음을 지정합니다.

- 테넌트 이름, 클라이언트 유형(S3) 및 선택적 스토리지 할당량을 포함한 기본 정보입니다.
- 테넌트 계정에서 S3 플랫폼 서비스를 사용할 수 있는지 여부, 해당 ID 소스를 구성할 수 있는지 여부, S3 Select를 사용할 것인지, 그리드 페더레이션 연결을 사용할 수 있는지 여부 등의 테넌트 계정에 대한 사용 권한
- StorageGRID 시스템에서 로컬 그룹 및 사용자, ID 페더레이션 또는 SSO(Single Sign-On)를 사용하는지 여부에 따라 테넌트의 초기 루트 액세스입니다.

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

그런 다음 "S3 테넌트 계정이 생성됩니다"테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 페더레이션 설정(ID 소스가 그리드와 공유되지 않는 경우)

- 그룹 및 사용자를 관리합니다
- 계정 클론 및 교차 그리드 복제에 그리드 페더레이션을 사용합니다
- S3 액세스 키를 관리합니다
- S3 버킷을 생성하고 관리합니다
- S3 플랫폼 서비스 사용
- S3 Select를 사용합니다
- 스토리지 사용량을 모니터링합니다

테넌트 관리자로 S3 버킷을 생성하고 관리할 수 있지만, 또는 "S3 콘솔"을 사용하여 "S3 클라이언트 "오브젝트를 수집 및 관리해야 합니다.

로그인 및 로그아웃 방법

테넌트 관리자에 로그인합니다

의 주소 표시줄에 테넌트의 URL을 입력하여 테넌트 관리자에 "지원되는 웹 브라우저 "액세스합니다.

시작하기 전에

- 로그인 자격 증명이 있습니다.
- 그리드 관리자가 제공한 테넌트 관리자 액세스 URL이 있습니다. 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
  ```

  URL에는 항상 FQDN(정규화된 도메인 이름), 관리 노드의 IP 주소 또는 관리 노드의 HA 그룹의 가상 IP 주소가 포함됩니다. 포트 번호, 20자리 테넌트 계정 ID 또는 둘 다 포함될 수도 있습니다.

- URL에 테넌트의 20자리 계정 ID가 포함되어 있지 않은 경우 이 계정 ID가 있는 것입니다.
- 을 사용하고 "지원되는 웹 브라우저"있습니다.
- 쿠키는 웹 브라우저에서 활성화됩니다.
- 가 있는 사용자 그룹에 속해 "특정 액세스 권한"있습니다.

단계

1. 를 실행합니다."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.

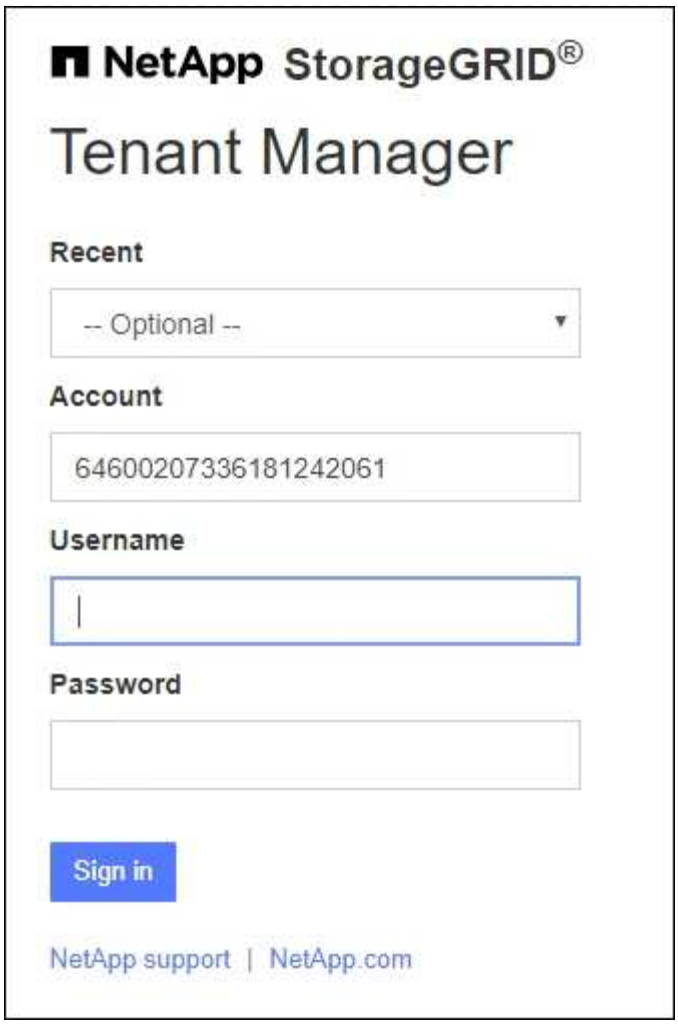
표시되는 로그인 화면은 입력한 URL과 StorageGRID에 대해 SSO(Single Sign-On)가 구성되었는지 여부에 따라 달라집니다.

SSO를 사용하지 않습니다

StorageGRID에서 SSO를 사용하지 않는 경우 다음 화면 중 하나가 나타납니다.

- Grid Manager 로그인 페이지 Tenant Sign-In * 링크를 선택합니다.

- Tenant Manager 로그인 페이지. 아래와 같이 * Account * 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 선택합니다.

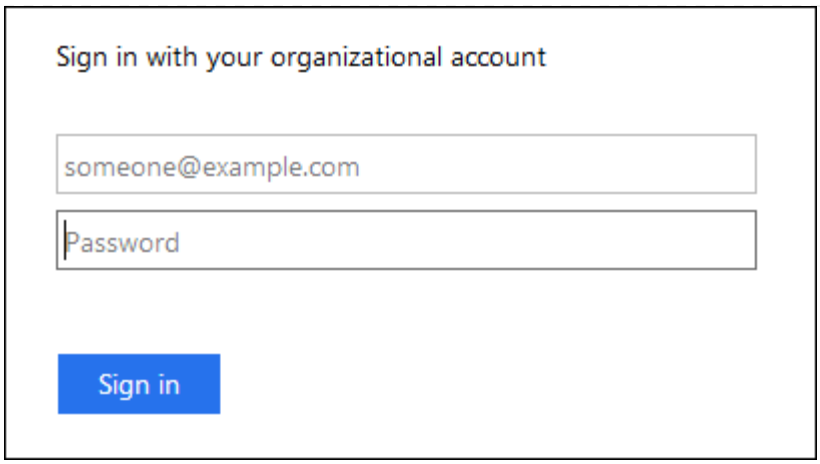
Tenant Manager 대시보드가 나타납니다.

iv. 다른 사람으로부터 초기 암호를 받은 경우 **username* * > * 암호 변경 * 을 선택하여 계정을 보호하십시오.

SSO 사용

StorageGRID에서 SSO를 사용하는 경우 다음 화면 중 하나가 나타납니다.

◦ 조직의 SSO 페이지 예를 들면 다음과 같습니다.



표준 SSO 자격 증명을 입력하고 * 로그인 * 을 선택합니다.

◦ 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 선택합니다.

iii. 조직의 SSO 로그인 페이지에서 표준 SSO 자격 증명을 사용하여 로그인합니다.

Tenant Manager 대시보드가 나타납니다.

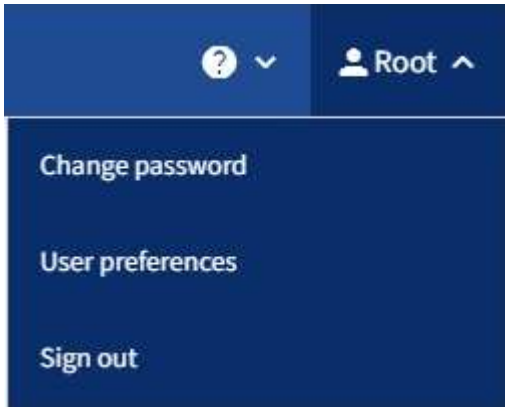
테넌트 관리자에서 로그아웃합니다

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.

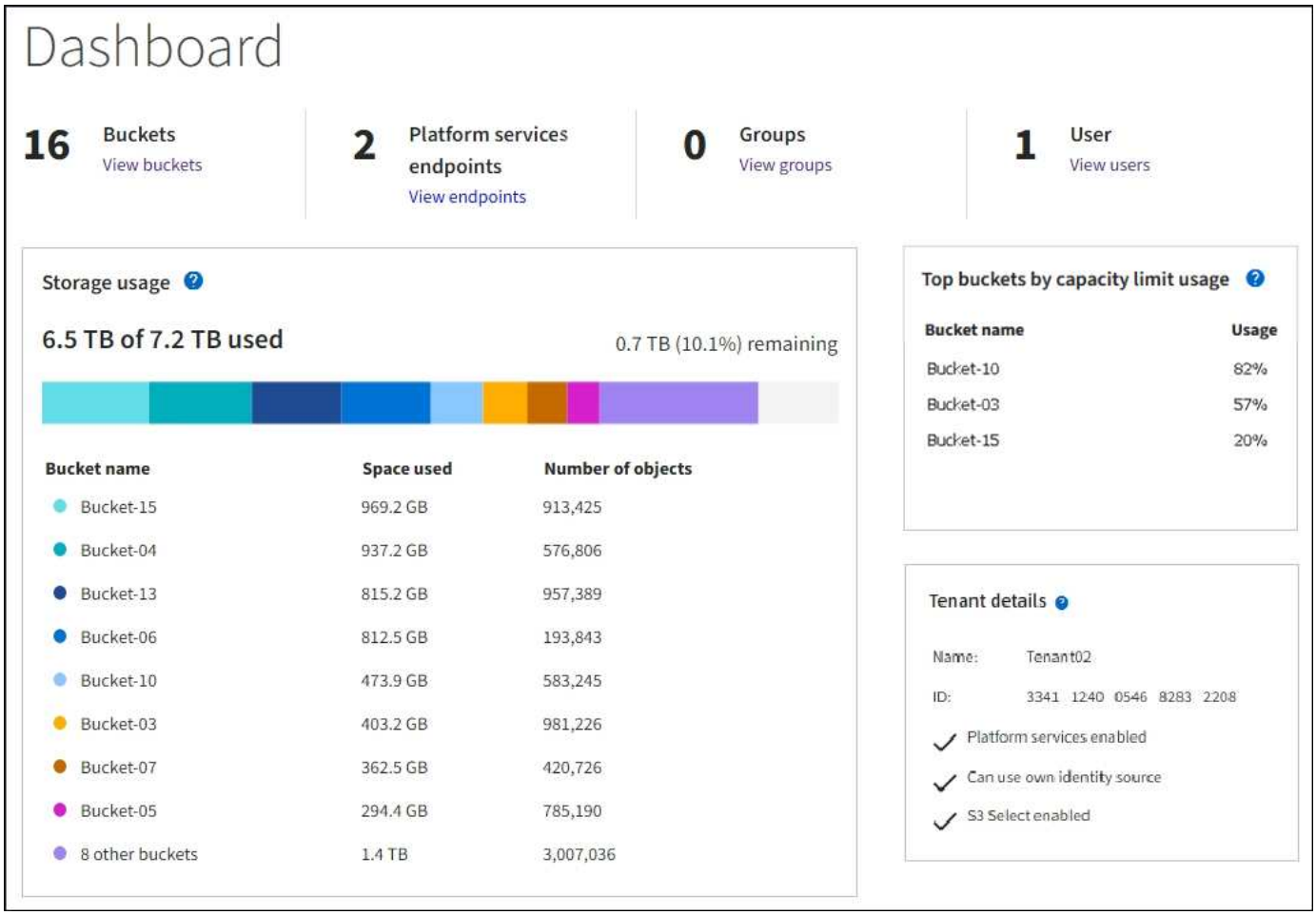
   SSO가 활성화되어 있고 Grid Manager에도 로그인한 경우, Grid Manager에서 로그아웃하여 SSO를 로그아웃해야 합니다.

테넌트 관리자 대시보드 이해

Tenant Manager 대시보드는 테넌트 계정의 구성과 테넌트의 버킷(S3) 또는 컨테이너(Swift)에 있는 오브젝트가 사용하는 공간의 양에 대한 개요를 제공합니다. 테넌트에 할당량이 있는 경우 대시보드에는 사용된 할당량의 양과 남아 있는 양이 표시됩니다. 테넌트 계정과 관련된 오류가 있는 경우 오류가 대시보드에 표시됩니다.

사용된 공간 값은 추정값입니다. 이러한 추정치는 베스트 타이밍, 네트워크 연결 및 노드 상태의 영향을 받습니다.

객체가 업로드되면 대시보드는 다음 예와 같이 표시됩니다.



테넌트 계정 정보입니다

대시보드 상단에는 구성된 버킷 또는 컨테이너, 그룹 및 사용자의 수가 표시됩니다. 또한 구성된 플랫폼 서비스 끝점의 수도 표시됩니다. 세부 정보를 보려면 링크를 선택하십시오.

사용 중인 과 구성한 옵션에 따라 "테넌트 관리 권한"대시보드의 나머지 부분에는 지침, 스토리지 사용, 개체 정보 및 테넌트 세부 정보의 다양한 조합이 표시됩니다.

스토리지 및 할당량 사용

Storage usage(저장소 사용) 패널에는 다음과 같은 정보가 포함되어 있습니다.

- 테넌트에 대한 객체 데이터의 양입니다.

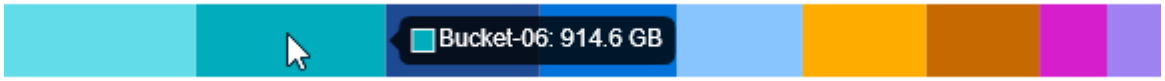
  이 값은 업로드된 총 오브젝트 데이터 양을 나타내며 해당 오브젝트 및 해당 메타데이터의 복사본을 저장하는 데 사용되는 공간을 나타내지 않습니다.

- 할당량이 설정된 경우 개체 데이터에 사용할 수 있는 총 공간과 남은 공간의 양과 백분율이 표시됩니다. 할당량은 섭취 가능한 오브젝트 데이터의 양을 제한합니다.

할당량 사용은 내부 추정치에 기초하며 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 사용이 다시 계산될 때까지 테넌트가 일시적으로 새 개체를 업로드하지 못할 수 있습니다. 할당량 사용량 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.

테넌트 관리자에 표시된 스토리지 값의 단위를 변경하려면 테넌트 관리자 오른쪽 상단의 사용자 드롭다운을 선택한 다음 * User preferences * 를 선택합니다.

할당량 사용 알림을 표시합니다

Grid Manager에서 할당량 사용 경고가 활성화된 경우 할당량이 낮거나 초과되면 다음과 같이 테넌트 관리자에 이러한 경고가 표시됩니다.

- 테넌트 할당량의 90% 이상이 사용된 경우 * Tenant quota usage high * 경고가 트리거됩니다.

그리드 관리자에게 할당량을 늘리도록 요청하십시오.

- 할당량을 초과하면 새 개체를 업로드할 수 없다는 알림이 표시됩니다.

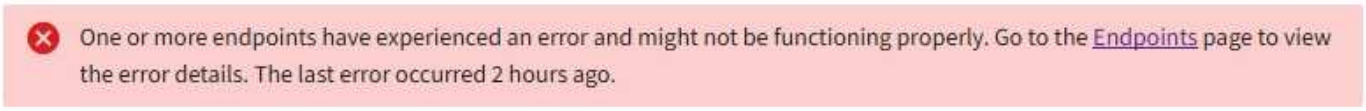
용량 제한 사용량

버킷에 대한 용량 제한을 설정한 경우 Tenant Manager 대시보드는 용량 제한 사용량별로 상위 버킷 목록을 표시합니다.

버킷에 제한이 설정되어 있지 않으면 해당 용량은 무제한입니다. 그러나 테넌트 계정에 총 저장소 할당량이 있고 이 할당량에 도달한 경우 버킷의 남은 용량 제한에 관계없이 더 많은 오브젝트를 수집할 수 없습니다.

끝점 오류

Grid Manager를 사용하여 플랫폼 서비스에 사용할 하나 이상의 엔드포인트를 구성한 경우, 지난 7일 내에 끝점 오류가 발생한 경우 Tenant Manager 대시보드에 경고가 표시됩니다.



에 대한 세부 정보를 "플랫폼 서비스 끝점 오류입니다"보려면 * 끝점 * 을 선택하여 끝점 페이지를 표시합니다.

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.

1. 테넌트 관리자에 로그인합니다.
2. 테넌트 관리자 상단에서 도움말 아이콘을 선택하고 * API documentation * 을 선택합니다.

API 운영

테넌트 관리 API는 사용 가능한 API 작업을 다음 섹션으로 구성합니다.

- * 계정 *: 스토리지 사용 정보를 가져오는 것을 포함하여 현재 테넌트 계정의 작업.
- * 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.

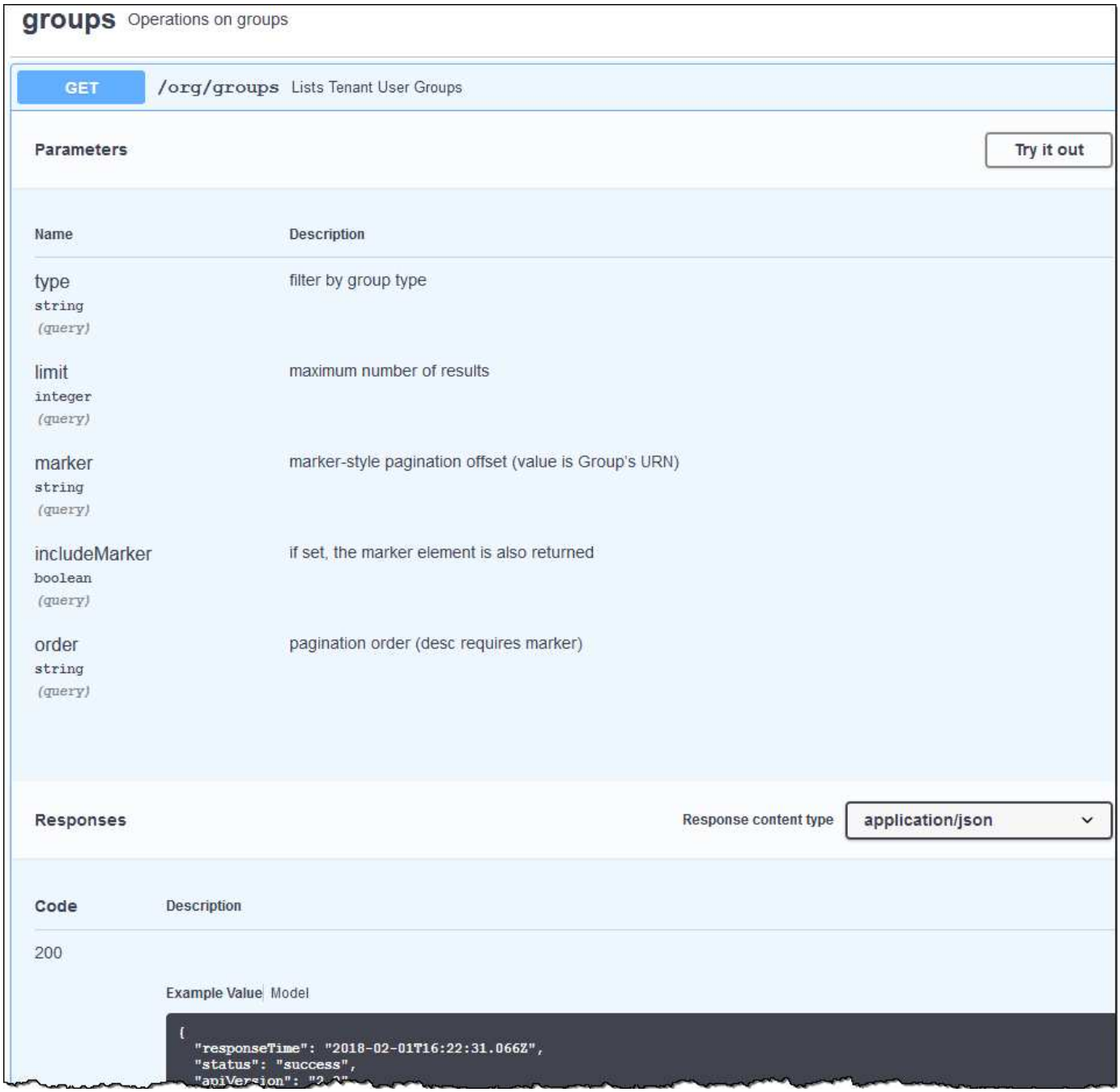
인증 보안 강화에 대한 자세한 내용은 를 "사이트 간 요청 위조 방지"참조하십시오.

StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 인증을 위해 다른 단계를 수행해야 합니다. 를 "Grid Management API 사용 지침"참조하십시오.

- * 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 작업
- * 비활성화됨 - 기능 *: 비활성화된 기능을 보기 위한 작업.
- * 엔드포인트 *: 엔드포인트를 관리하는 운영 엔드포인트는 S3 버킷이 StorageGRID CloudMirror 복제, 알림 또는 검색 통합에 외부 서비스를 사용할 수 있도록 합니다.
- * 그리드 페더레이션 - 연결 *: 그리드 페더레이션 연결 및 교차 그리드 복제에서의 작업.
- * 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
- * ILM *: 정보 수명 주기 관리(ILM) 설정에 대한 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 문서 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 API 버전 4를 지정합니다.

`https://hostname_or_ip_address/api/v4/authorize`

이전 버전과 호환되지 않는 변경 사항이 발생하면 API의 주 버전이 범핑됩니다. API의 부 버전은 이전 버전과 _ 호환 _ 을(를) 변경할 때 범핑됩니다. 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 최신 버전의 API만 활성화됩니다. 그러나 StorageGRID의 새 기능 릴리즈로 업그레이드하면 하나 이상의 StorageGRID 기능 릴리즈에 대한 이전 API 버전에 계속 액세스할 수 있습니다.

> 지원되는 버전을 구성할 수 있습니다. 자세한 내용은 Swagger API 설명서의 * config * 섹션을 참조하십시오"Grid Management API를 참조하십시오". 최신 버전을 사용하려면 모든 API 클라이언트를 업데이트한 후 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 v2 API at POST "/api/v2/authorize"
```

현재 릴리즈에서 지원되는 **API** 버전을 확인합니다

API 요청을 사용하여 `GET /versions` 지원되는 API 주요 버전 목록을 반환합니다. 이 요청은 Swagger API 설명서의 * config * 섹션에 있습니다.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

요청에 대한 **API** 버전을 지정합니다

경로 매개 변수(`/api/v4`) 또는 헤더를 사용하여 API 버전을 지정할 수 (`Api-Version: 4`있습니다. 두 값을 모두 제공하면 헤더 값이 경로 값을 재정의합니다.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" 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 `csrfToken` 인증 중에 매개 변수를 로 `true` 설정합니다. 기본값은 입니다 `false`.

```
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"
```

true 인 경우, `GridCsrfToken` 쿠키는 Grid Manager 로그인에 대한 임의 값으로 설정되고 `AccountCsrfToken` 쿠키는 Tenant Manager에 로그인하기 위한 임의 값으로 설정됩니다.

쿠키가 있는 경우 시스템 상태(POST, PUT, 패치, 삭제)를 수정할 수 있는 모든 요청에 다음 중 하나가 포함되어야 합니다.

- `X-Csrf-Token`헤더 값이 CSRF 토큰 쿠키의 값으로 설정된 헤더입니다.
- 폼으로 인코딩된 본문을 수락하는 끝점의 경우: `csrfToken` 폼으로 인코딩된 요청 본문 매개 변수입니다.

CSRF 보호를 구성하려면 또는 를 "Grid Management API를 참조하십시오""테넌트 관리 API"사용합니다.

> CSRF 토큰 쿠키 세트가 있는 요청은 CSRF 공격에 대한 추가 보호로서 JSON 요청 본문을 기대하는 모든 요청에 대해 "Content-Type: application/json" 헤더를 적용합니다.

그리드 페더레이션 연결을 사용합니다

클론 테넌트 그룹 및 사용자

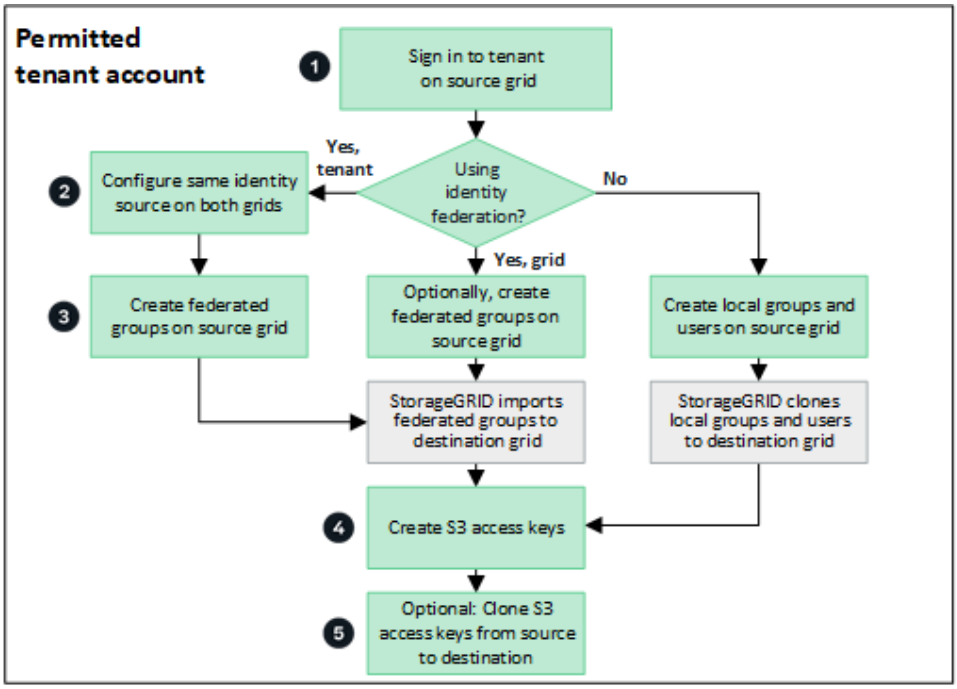
그리드 페더레이션 연결을 사용하도록 테넌트를 만들거나 편집한 경우 해당 테넌트는 한 StorageGRID 시스템(소스 테넌트)에서 다른 StorageGRID 시스템(복제본 테넌트)으로 복제됩니다. 테넌트가 복제되면 소스 테넌트에 추가된 모든 그룹 및 사용자가 복제본 테넌트에 클론됩니다.

테넌트가 처음 생성된 StorageGRID 시스템은 테넌트의 _source GRID_입니다. 테넌트가 복제되는 StorageGRID 시스템은 테넌트의_destination GRID_입니다. 두 테넌트 계정 모두 동일한 계정 ID, 이름, 설명, 스토리지 할당량 및 할당된 권한이 있습니다. 그러나 대상 테넌트는 처음에 루트 사용자 암호를 가지고 있지 않습니다. 자세한 내용은 및 을 "계정 클론이란 무엇입니까""허용된 테넌트 관리"참조하십시오.

버킷 객체의 경우 테넌트 계정 정보의 복제가 "교차 그리드 복제"필요합니다. 두 그리드에 동일한 테넌트 그룹 및 사용자가 있으면 양쪽 그리드의 해당 버킷 및 오브젝트에 액세스할 수 있습니다.

계정 클론에 대한 테넌트 워크플로우

테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 워크플로 다이어그램을 검토하여 그룹, 사용자 및 S3 액세스 키를 복제하는 단계를 확인합니다.



워크플로의 주요 단계는 다음과 같습니다.

1 테넌트에 로그인합니다

소스 그리드(테넌트가 처음 생성된 그리드)에서 테넌트 계정에 로그인합니다.

2 필요한 경우 **ID** 페더레이션을 구성합니다

테넌트 계정에 통합 그룹 및 사용자를 사용할 수 있는 * 고유 ID 소스 사용 * 권한이 있는 경우 소스 및 대상 테넌트 계정 모두에 대해 동일한 ID 소스(동일한 설정 사용)를 구성합니다. 두 그리드에서 동일한 ID 소스를 사용하고 있지 않으면 통합 그룹과 사용자를 복제할 수 없습니다. 자세한 내용은 을 "ID 페더레이션을 사용합니다"참조하십시오.

3 그룹 및 사용자를 생성합니다

그룹 및 사용자를 생성할 때는 항상 테넌트의 소스 그리드에서 시작합니다. 새 그룹을 추가하면 StorageGRID에서 자동으로 대상 그리드에 클론을 생성합니다.

- 전체 StorageGRID 시스템 또는 테넌트 계정에 대해 ID 페더레이션이 구성된 경우 ID 소스에서 페더레이션 "새 테넌트 그룹을 생성합니다" 그룹을 가져옵니다.
- ID 페더레이션을 사용하지 않는 경우"새 로컬 그룹을 생성합니다""로컬 사용자를 생성합니다"

4 **S3** 액세스 키를 생성합니다

소스 그리드 또는 대상 그리드에서 또는 로 "다른 사용자의 액세스 키를 생성합니다"이동하여 해당 그리드의 버킷을 액세스할 수 "사용자 고유의 액세스 키를 생성합니다"있습니다.

5 필요한 경우 **S3** 액세스 키를 클론 복제합니다

두 그리드에 동일한 액세스 키가 있는 버킷에 액세스해야 하는 경우 소스 그리드에 액세스 키를 생성한 다음 테넌트 관리자 API를 사용하여 수동으로 대상 그리드에 클론을 생성합니다. 자세한 내용은 을 "API를 사용하여 S3 액세스 키의 클론을 생성합니다"참조하십시오.

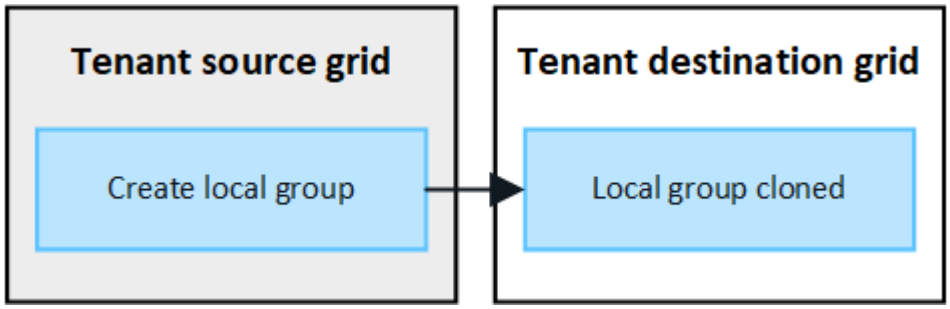
그룹, 사용자 및 **S3** 액세스 키의 클론을 생성하는 방법은 무엇입니까**?**

이 섹션을 검토하여 테넌트 소스 그리드와 테넌트 대상 그리드 간에 그룹, 사용자 및 S3 액세스 키의 클론 생성 방법을 이해합니다.

소스 그리드에 생성된 로컬 그룹이 복제됩니다

테넌트 계정이 생성되어 대상 그리드에 복제된 후 StorageGRID는 테넌트의 소스 그리드에 추가한 모든 로컬 그룹을 테넌트의 대상 그리드에 자동으로 복제합니다.

원래 그룹과 해당 클론 모두에 동일한 액세스 모드, 그룹 권한 및 S3 그룹 정책이 있습니다. 자세한 내용은 을 "S3 테넌트용 그룹을 생성합니다"참조하십시오.

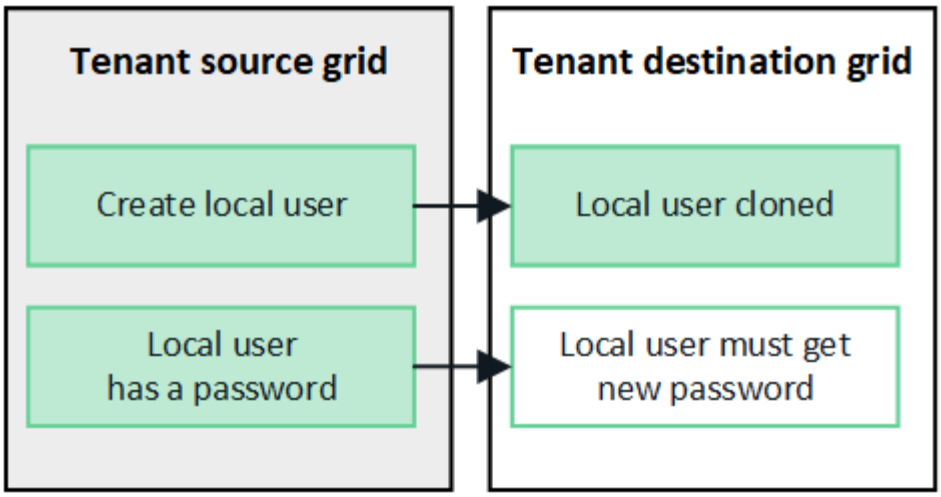


> 소스 그리드에 로컬 그룹을 생성할 때 선택한 사용자는 그룹이 대상 그리드에 클론될 때 포함되지 않습니다. 따라서 그룹을 만들 때 사용자를 선택하지 마십시오. 대신 사용자를 생성할 때 그룹을 선택합니다.

소스 그리드에 생성된 로컬 사용자의 클론이 생성됩니다

소스 그리드에 새 로컬 사용자를 생성하면 StorageGRID는 해당 사용자를 대상 그리드에 자동으로 복제합니다. 원래 사용자와 해당 클론 모두에 동일한 전체 이름, 사용자 이름 및 * 액세스 거부 * 설정이 있습니다. 두 사용자 모두 동일한 그룹에 속해 있습니다. 자세한 내용은 을 "로컬 사용자를 관리합니다"참조하십시오.

보안상의 이유로 로컬 사용자 암호는 대상 그리드에 복제되지 않습니다. 로컬 사용자가 대상 그리드의 테넌트 관리자에 액세스해야 하는 경우 테넌트 계정의 루트 사용자는 대상 그리드에 해당 사용자의 암호를 추가해야 합니다. 자세한 내용은 을 "로컬 사용자를 관리합니다"참조하십시오.

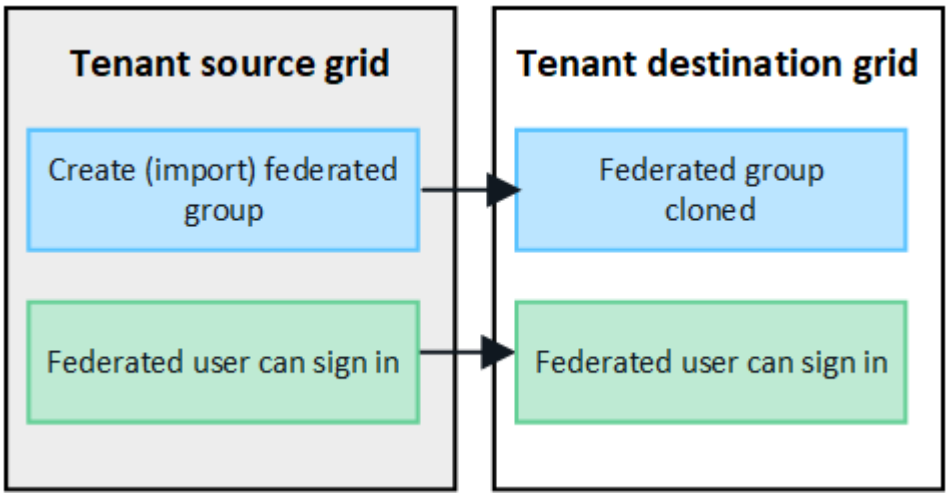


소스 그리드에 생성된 연합 그룹이 클론됩니다

에서 계정 클론을 사용하기 위한 요구 사항이 충족되었다고 가정할 때 "SSO(Single Sign-On)" "ID 제휴"소스 그리드에서 테넌트에 대해 생성(가져오기)한 페더레이션 그룹이 대상 그리드의 테넌트에 자동으로 복제됩니다.

두 그룹 모두 동일한 액세스 모드, 그룹 권한 및 S3 그룹 정책을 가집니다.

소스 테넌트의 통합 그룹이 생성되고 대상 테넌트에 클론이 생성되면 통합 사용자는 두 그리드 중 하나에서 테넌트에 로그인할 수 있습니다.

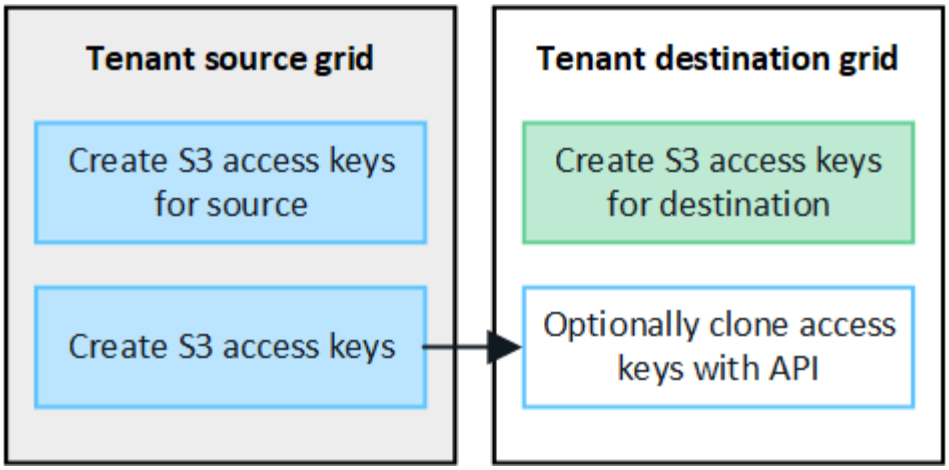


S3 액세스 키를 수동으로 복제할 수 있습니다

StorageGRID는 각 그리드에 서로 다른 키를 추가하여 보안을 강화하기 때문에 S3 액세스 키를 자동으로 복제하지 않습니다.

두 그리드에서 액세스 키를 관리하려면 다음 중 하나를 수행합니다.

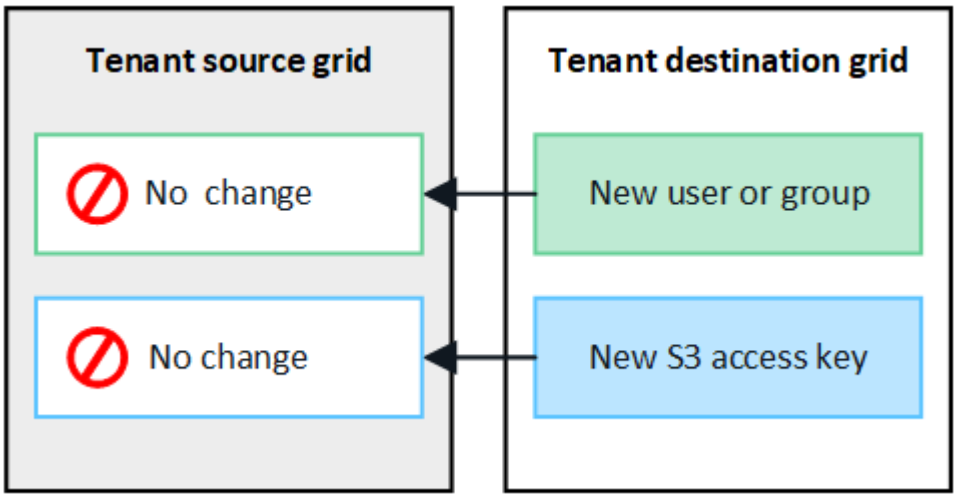
- 각 그리드에 대해 동일한 키를 사용할 필요가 없는 경우 또는 "다른 사용자의 액세스 키를 생성합니다"각 그리드에서 사용할 수 "사용자 고유의 액세스 키를 생성합니다"있습니다.
- 두 그리드 모두에서 동일한 키를 사용해야 하는 경우 소스 그리드에 키를 생성한 다음 Tenant Manager API를 사용하여 대상 그리드로 수동으로 이동할 수 "키를 복제합니다"있습니다.



통합 사용자의 S3 액세스 키를 클론하면 사용자 및 S3 액세스 키가 모두 대상 테넌트에 복제됩니다.

대상 그리드에 추가된 그룹 및 사용자는 클론이 생성되지 않습니다

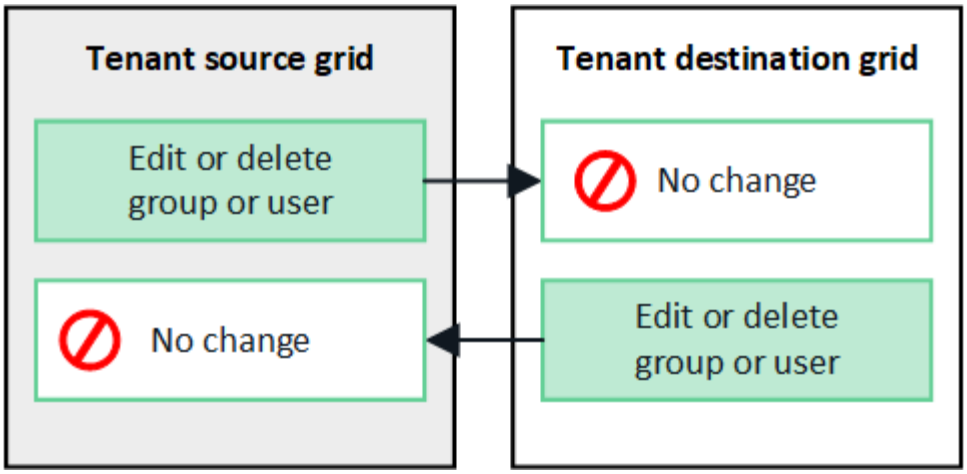
클론 생성은 테넌트의 소스 그리드에서 테넌트의 대상 그리드로만 이루어집니다. 테넌트의 대상 그리드에 그룹 및 사용자를 생성하거나 가져오는 경우 StorageGRID는 이러한 항목을 테넌트의 소스 그리드에 다시 복제하지 않습니다.



편집 또는 삭제된 그룹, 사용자 및 액세스 키는 복제되지 않습니다

클론 생성은 새 그룹 및 사용자를 생성할 때만 발생합니다.

두 눈금 중 하나에서 그룹, 사용자 또는 액세스 키를 편집하거나 삭제하면 변경 내용이 다른 눈금에 복제되지 않습니다.



API를 사용하여 **S3** 액세스 키의 클론을 생성합니다

테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 테넌트 관리 API를 사용하여 소스 그리드의 테넌트에서 대상 그리드의 테넌트로 S3 액세스 키를 수동으로 복제할 수 있습니다.

시작하기 전에

- 테넌트 계정에는 * 그리드 페더레이션 연결 사용 * 권한이 있습니다.
- 그리드 페더레이션 연결에는 * 연결 상태 * 가 * 연결됨 * 으로 표시됩니다.
- 를 사용하여 테넌트의 소스 그리드에서 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "자신의 S3 자격 증명 또는 루트 액세스 권한을 관리합니다"있습니다.
- 로컬 사용자에 대한 액세스 키를 클론하는 경우 사용자는 이미 두 그리드에 존재합니다.

> 통합 사용자의 S3 액세스 키를 클론하면 사용자 및 S3 액세스 키가 모두 대상 테넌트에 추가됩니다.

사용자 고유의 액세스 키를 복제합니다

두 그리드의 동일한 버킷에 액세스해야 하는 경우 고유한 액세스 키를 복제할 수 있습니다.

단계

1. 소스 그리드에서 Tenant Manager를 사용하여 "사용자 고유의 액세스 키를 생성합니다" `.csv`파일을 다운로드합니다.
2. 테넌트 관리자 상단에서 도움말 아이콘을 선택하고 * API documentation * 을 선택합니다.
3. S3 * 섹션에서 다음 끝점을 선택합니다.

```
POST /org/users/current-user/replicate-s3-access-key
```

4. 체험하기 * 를 선택합니다.
5. body * 텍스트 상자에서 * AccessKey * 및 * secretAccessKey * 의 예제 항목을 다운로드한 *.csv * 파일의 값으로 바꿉니다.

각 문자열 주위에 큰따옴표를 붙여야 합니다.

6. 키가 만료되면 * Expires * 에 대한 예제 항목을 ISO 8601 데이터-시간 형식(예:)의 문자열로 `2024-02-28T22:46:33-08:00` 대체합니다. 키가 만료되지 않으면 * expires * 항목의 값으로 * null * 을 입력하거나 * expires * 행 및 앞의 쉼표를 제거합니다.
7. Execute * 를 선택합니다.
8. 서버 응답 코드가 * 204 * 인지 확인합니다. 이는 키가 대상 그리드에 성공적으로 복제되었음을 나타냅니다.

다른 사용자의 액세스 키를 복제합니다

두 그리드의 동일한 버킷에 액세스해야 하는 경우 다른 사용자의 액세스 키를 복제할 수 있습니다.

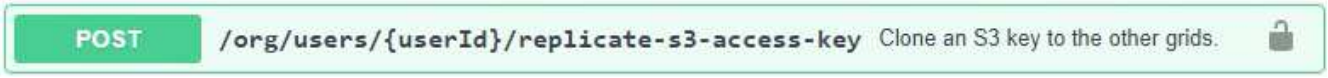
단계

1. 소스 그리드에서 Tenant Manager를 사용하여 "다른 사용자의 S3 액세스 키를 생성합니다" `.csv`파일을 다운로드합니다.
2. 테넌트 관리자 상단에서 도움말 아이콘을 선택하고 * API documentation * 을 선택합니다.
3. 사용자 ID를 얻습니다. 다른 사용자의 액세스 키를 복제하려면 이 값이 필요합니다.
   a. 사용자 * 섹션에서 다음 끝점을 선택합니다.

      `GET /org/users`

   b. 체험하기 * 를 선택합니다.
   c. 사용자를 찾을 때 사용할 매개 변수를 지정합니다.
   d. Execute * 를 선택합니다.
   e. 복제할 키가 있는 사용자를 찾고 * id * 필드에 번호를 복사합니다.
4. S3 * 섹션에서 다음 끝점을 선택합니다.

   `POST /org/users/{userId}/replicate-s3-access-key`



5. 체험하기 * 를 선택합니다.
6. userId * 텍스트 상자에 복사한 사용자 ID를 붙여 넣습니다.
7. body * 텍스트 상자에서 * 예제 액세스 키 * 및 * 비밀 액세스 키 * 와 같은 항목을 해당 사용자의 *.csv * 파일 값으로 바꿉니다.

문자열 주위에 큰따옴표를 붙여야 합니다.

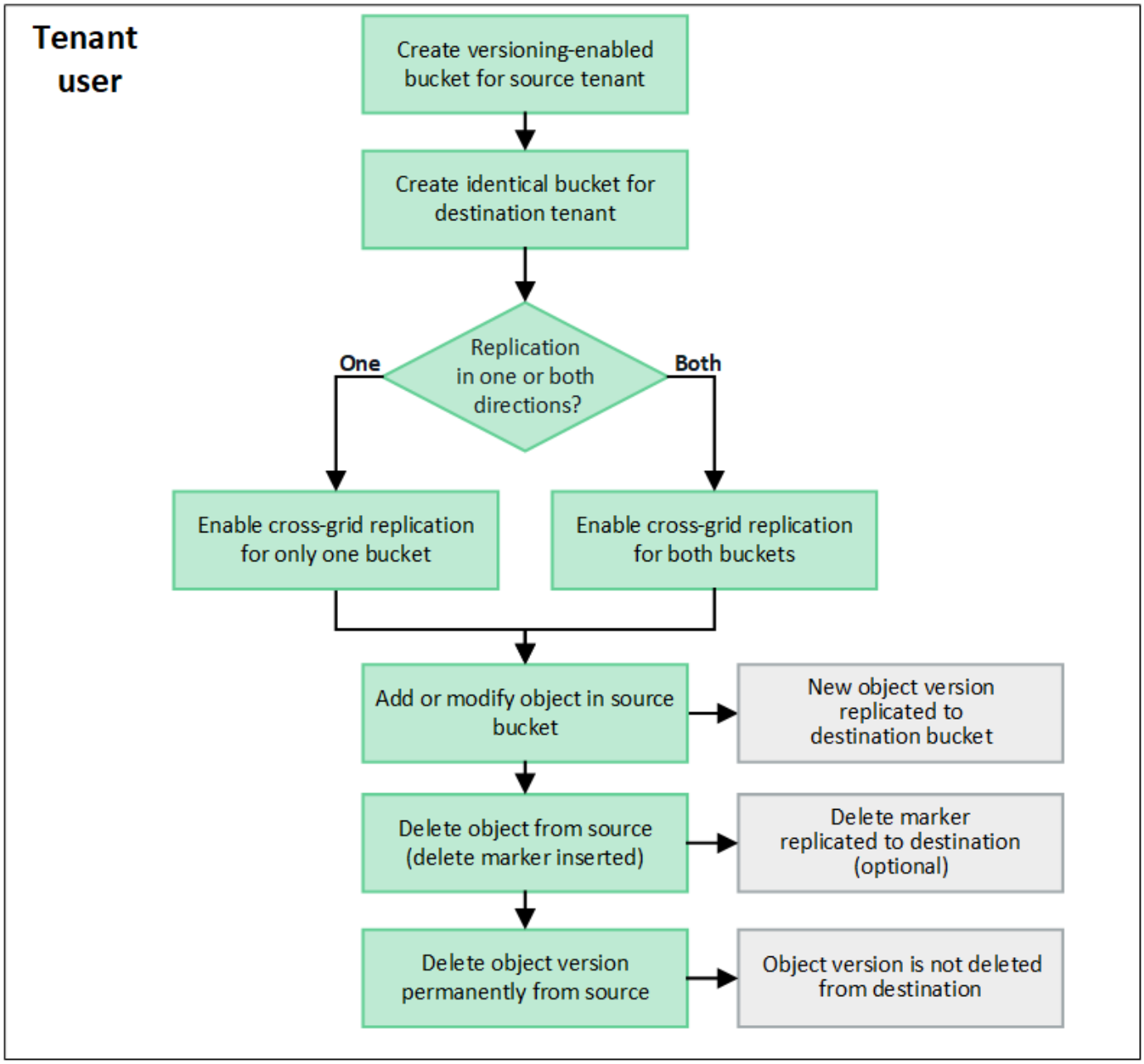
8. 키가 만료되면 * Expires * 에 대한 예제 항목을 ISO 8601 데이터-시간 형식(예:)의 문자열로 `2023-02-28T22:46:33-08:00` 대체합니다. 키가 만료되지 않으면 * expires * 항목의 값으로 * null * 을 입력하거나 * expires * 행 및 앞의 쉼표를 제거합니다.
9. Execute * 를 선택합니다.
10. 서버 응답 코드가 * 204 * 인지 확인합니다. 이는 키가 대상 그리드에 성공적으로 복제되었음을 나타냅니다.

교차 그리드 복제 관리

테넌트 계정이 생성되었을 때 * 그리드 페더레이션 연결 사용 * 권한이 할당된 경우 교차 그리드 복제를 사용하여 테넌트의 소스 그리드에 있는 버킷과 테넌트 대상 그리드에 있는 버킷 간에 객체를 자동으로 복제할 수 있습니다. 크로스 그리드 복제는 한 방향 또는 두 방향으로 수행될 수 있습니다.

그리드 간 복제를 위한 워크플로우

워크플로우 다이어그램은 두 그리드에 있는 버킷 간 크로스 그리드 복제를 구성하기 위해 수행할 단계를 요약합니다. 이러한 단계는 아래에 자세히 설명되어 있습니다.



교차 그리드 복제를 구성합니다

교차 그리드 복제를 사용하려면 먼저 각 그리드의 해당 테넌트 계정에 로그인하고 동일한 버킷을 생성해야 합니다. 그런 다음 둘 중 하나 또는 두 버킷에서 교차 그리드 복제를 활성화할 수 있습니다.

시작하기 전에

- 교차 그리드 복제의 요구 사항을 검토했습니다. 을 "크로스 그리드 복제란"참조하십시오.
- 을 사용하고 "지원되는 웹 브라우저"있습니다.
- 테넌트 계정에는 * 그리드 페더레이션 연결 사용 * 권한이 있으며 동일한 테넌트 계정이 두 그리드에 있습니다. 을 "그리드 페더레이션 연결에 대해 허용된 테넌트를 관리합니다"참조하십시오.
- 로그인하려는 테넌트 사용자는 두 그리드 모두에 이미 있으며 이 있는 사용자 그룹에 속해 "루트 액세스 권한 "있습니다.
- 테넌트의 대상 그리드에 로컬 사용자로 로그인하는 경우 테넌트 계정의 루트 사용자가 해당 그리드에서 사용자

계정의 암호를 설정했습니다.

두 개의 동일한 버킷을 생성합니다

첫 번째 단계로 각 그리드의 해당 테넌트 계정에 로그인하여 동일한 버킷을 생성합니다.

단계

1. 그리드 페더레이션 연결의 두 그리드 중 하나에서 시작하여 새 버킷을 만듭니다.
   a. 두 그리드에 있는 테넌트 사용자의 자격 증명을 사용하여 테넌트 계정에 로그인합니다.

      테넌트의 대상 그리드에 로컬 사용자로 로그인할 수 없는 경우 테넌트 계정의 루트 사용자가 사용자 계정의 암호를 설정했는지 확인합니다.

   b. 의 지침을 "S3 버킷을 생성합니다"따릅니다.
   c. 개체 설정 관리 * 탭에서 * 개체 버전 관리 사용 * 을 선택합니다.
   d. StorageGRID 시스템에 S3 오브젝트 잠금이 설정된 경우 버킷에 S3 오브젝트 잠금을 활성화하지 마십시오.
   e. Create bucket * 을 선택합니다.
   f. 마침 * 을 선택합니다.
2. 그리드 페더레이션 연결의 다른 그리드에 동일한 테넌트 계정에 대해 동일한 버킷을 생성하려면 이 단계를 반복합니다.

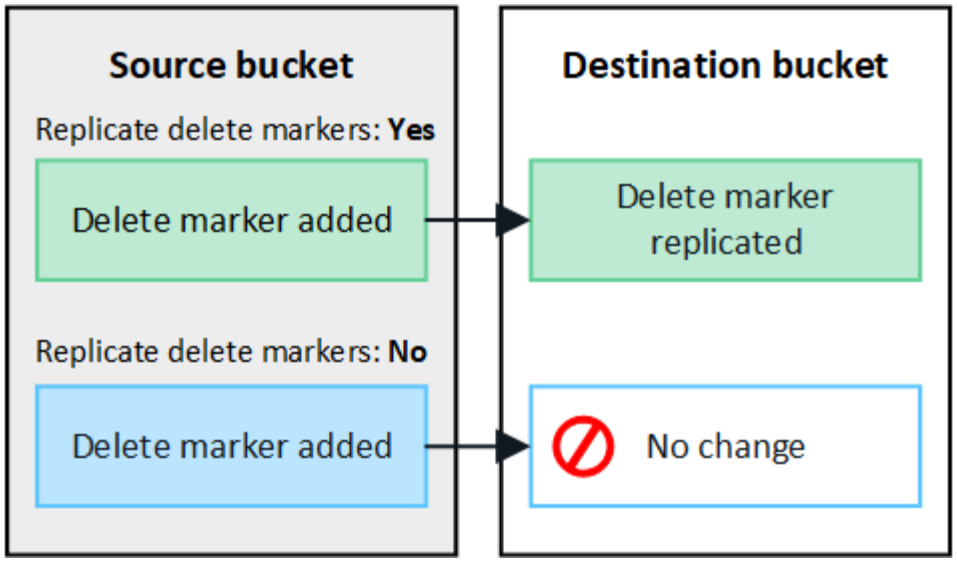
   필요에 따라 각 버킷은 다른 지역을 사용할 수 있습니다.

교차 그리드 복제를 설정합니다

두 버킷 중 하나에 물체를 추가하기 전에 이 단계를 수행해야 합니다.

단계

1. 복제할 객체가 있는 그리드에서 시작하여 "한 방향으로 크로스 그리드 복제"다음을 활성화합니다.
   a. 버켓의 테넌트 계정에 로그인합니다.
   b. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
   c. 버킷 세부 정보 페이지에 액세스하려면 테이블에서 버킷 이름을 선택합니다.
   d. Cross-grid replication * 탭을 선택합니다.
   e. 사용 * 을 선택하고 요구 사항 목록을 검토합니다.
   f. 모든 요구 사항이 충족되면 사용할 그리드 페더레이션 연결을 선택합니다.
   g. 선택적으로 * Delete Markers 복제 * 의 설정을 변경하여 S3 클라이언트가 버전 ID가 포함되지 않은 소스 그리드에 삭제 요청을 발행하는 경우 대상 그리드에 어떤 일이 발생하는지 확인합니다.
      - * 예 * (기본값): 삭제 마커가 소스 버킷에 추가되고 대상 버킷에 복제됩니다.
      - * 아니요 *: 삭제 마커가 소스 버킷에 추가되지만 대상 버킷에 복제되지 않습니다.



삭제 요청에 버전 ID가 포함된 경우 해당 객체 버전이 소스 버킷에서 영구적으로 제거됩니다. StorageGRID는 버전 ID가 포함된 삭제 요청을 복제하지 않으므로 동일한 객체 버전이 대상에서 삭제되지 않습니다.

자세한 내용은 을 "크로스 그리드 복제란" 참조하십시오.

a. 필요에 따라 * 교차 그리드 복제 * 감사 범주의 설정을 변경하여 감사 메시지의 볼륨을 관리합니다.
   - * Error * (기본값): 실패한 교차 그리드 복제 요청만 감사 출력에 포함됩니다.
   - * 정상 *: 모든 교차 그리드 복제 요청이 포함되어 감사 출력 볼륨을 크게 높입니다.
b. 선택 사항을 검토합니다. 두 버킷이 모두 비어 있지 않으면 이 설정을 변경할 수 없습니다.
c. Enable and test * 를 선택합니다.

   잠시 후 성공 메시지가 나타납니다. 이 버킷에 추가된 오브젝트는 이제 다른 그리드에 자동으로 복제됩니다. * 교차 그리드 복제 * 는 버킷 세부 정보 페이지에서 활성화된 기능으로 표시됩니다.

2. 필요에 따라 다른 그리드의 해당 버킷으로 이동하고"양방향 교차 그리드 복제를 활성화합니다".

그리드 간의 복제를 테스트합니다

버킷에 대해 교차 그리드 복제가 활성화된 경우 연결 및 교차 그리드 복제가 올바르게 작동하고 소스 및 대상 버킷이 모든 요구 사항을 충족하는지 확인해야 할 수 있습니다(예: 버전 관리가 계속 활성화됨).

시작하기 전에

- 을 사용하고 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "루트 액세스 권한"있습니다.

단계

1. 버켓의 테넌트 계정에 로그인합니다.
2. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
3. 버킷 세부 정보 페이지에 액세스하려면 테이블에서 버킷 이름을 선택합니다.
4. Cross-grid replication * 탭을 선택합니다.

5. Test connection * 을 선택합니다.

   연결이 정상이면 성공 배너가 나타납니다. 그렇지 않으면 사용자 및 그리드 관리자가 문제를 해결하는 데 사용할 수 있는 오류 메시지가 나타납니다. 자세한 내용은 을 참조하십시오 "그리드 통합 오류 문제 해결".

6. 양방향 복제가 수행되도록 구성된 경우 다른 그리드의 해당 버킷으로 이동하여 * Test connection * 을 선택하여 교차 그리드 복제가 다른 방향으로 작동하는지 확인합니다.

크로스 그리드 복제를 비활성화합니다

더 이상 다른 그리드에 객체를 복사하지 않으려는 경우 그리드 간 복제를 영구적으로 중지할 수 있습니다.

교차 그리드 복제를 사용하지 않도록 설정하기 전에 다음 사항에 유의하십시오.

- 교차 그리드 복제를 비활성화해도 그리드 간에 이미 복제된 개체는 제거되지 않습니다. 예를 들어 그리드 1의 객체가 `my-bucket` 그리드 2에서 에 복사된 `my-bucket` 경우 해당 버킷에 대해 교차 그리드 복제를 사용하지 않도록 설정하면 제거되지 않습니다. 이러한 개체를 삭제하려면 해당 개체를 수동으로 제거해야 합니다.
- 각 버킷에 대해 교차 그리드 복제가 설정된 경우(즉, 양방향으로 복제가 발생하는 경우), 하나 또는 두 버킷에 대해 교차 그리드 복제를 비활성화할 수 있습니다. 예를 들어, 그리드 1에서 그리드 2 `my-bucket`로 객체를 복제하는 동시에 그리드 2에서 그리드 1 `my-bucket`로 객체를 계속 `my-bucket` 복제할 수 없도록 설정할 수 `my-bucket` 있습니다.
- 그리드 페더레이션 연결을 사용하기 위해 테넌트의 권한을 제거하려면 먼저 교차 그리드 복제를 비활성화해야 합니다. 을 "허용된 테넌트 관리"참조하십시오.
- 오브젝트가 포함된 버킷에 대해 교차 그리드 복제를 사용하지 않도록 설정하면 소스 및 대상 버킷에서 모든 오브젝트를 삭제하지 않는 한 교차 그리드 복제를 다시 활성화할 수 없습니다.

  ! 두 버킷이 모두 비어 있지 않으면 복제를 다시 설정할 수 없습니다.

시작하기 전에

- 을 사용하고 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "루트 액세스 권한"있습니다.

단계

1. 더 이상 복제할 객체가 없는 그리드에서 시작하여 버킷에 대한 교차 그리드 복제를 중지합니다.
   a. 버켓의 테넌트 계정에 로그인합니다.
   b. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
   c. 버킷 세부 정보 페이지에 액세스하려면 테이블에서 버킷 이름을 선택합니다.
   d. Cross-grid replication * 탭을 선택합니다.
   e. 복제 비활성화 * 를 선택합니다.
   f. 이 버킷에 대해 교차 그리드 복제를 비활성화하려면 텍스트 상자에 * Yes * 를 입력하고 * Disable * 을 선택합니다.

      잠시 후 성공 메시지가 나타납니다. 이 버킷에 추가된 새 오브젝트는 더 이상 다른 그리드에 자동으로 복제될 수 없습니다. * 교차 그리드 복제 * 는 버킷 페이지에서 더 이상 활성화 기능으로 표시되지 않습니다.

2. 양방향 복제가 수행되도록 구성된 경우 다른 그리드의 해당 버킷으로 이동하여 다른 방향으로 크로스 그리드 복제를

중지합니다.

그리드 페더레이션 연결을 봅니다

테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 허용된 연결을 볼 수 있습니다.

시작하기 전에

- 테넌트 계정에는 * 그리드 페더레이션 연결 사용 * 권한이 있습니다.
- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "루트 액세스 권한"있습니다.

단계

1. 스토리지(S3) * > * 그리드 페더레이션 연결 * 을 선택합니다.

   그리드 페더레이션 연결 페이지가 나타나고 다음 정보를 요약하는 테이블이 포함됩니다.

열	설명
연결 이름입니다	이 테넌트가 사용할 수 있는 그리드 페더레이션 연결이 있습니다.
크로스 그리드 복제를 포함한 버킷	각 그리드 페더레이션 연결에 대해 교차 그리드 복제가 활성화된 테넌트 버킷입니다. 이러한 버킷에 추가된 객체는 연결의 다른 그리드에 복제됩니다.
마지막 오류	각 그리드 페더레이션 연결에 대해 데이터가 다른 그리드에 복제되는 경우 가장 최근의 오류가 발생합니다. 을 마지막 오류를 지웁니다참조하십시오.

2. 필요한 경우 버킷 이름을 "버킷 세부 정보를 봅니다"선택합니다.

마지막 오류를 지웁니다

다음 이유 중 하나로 인해 * Last error * (마지막 오류 *) 열에 오류가 나타날 수 있습니다.

- 소스 객체 버전을 찾을 수 없습니다.
- 소스 버킷을 찾을 수 없습니다.
- 대상 버킷이 삭제되었습니다.
- 대상 버킷이 다른 계정에 의해 다시 생성되었습니다.
- 대상 버킷에 버전 관리가 일시 중지되었습니다.
- 대상 버킷은 동일한 계정으로 다시 생성되었지만 현재는 버전이 지정되지 않았습니다.

> 이 열에는 마지막으로 발생한 교차 그리드 복제 오류만 표시됩니다. 이전에 발생한 오류는 표시되지 않습니다.

단계

1. 마지막 오류 * 열에 메시지가 나타나면 메시지 텍스트를 확인합니다.

예를 들어, 이 오류는 버전 관리가 일시 중단되었거나 S3 오브젝트 잠금이 설정되었기 때문에 교차 그리드 복제의 대상 버킷이 잘못된 상태에 있음을 나타냅니다.

2. 권장되는 작업을 수행합니다. 예를 들어 교차 그리드 복제를 위해 대상 버킷에서 버전 관리가 일시 중단된 경우 해당 버킷의 버전 관리를 다시 사용하도록 설정합니다.
3. 테이블에서 연결을 선택합니다.
4. Clear error * 를 선택합니다.
5. 메시지를 지우고 시스템 상태를 업데이트하려면 * 예 * 를 선택하십시오.
6. 5-6분 정도 기다린 다음 새 오브젝트를 버킷에 넣습니다. 오류 메시지가 다시 나타나지 않는지 확인합니다.

> 오류 메시지가 지워졌는지 확인하려면 새 개체를 수신하기 전에 메시지의 타임스탬프가 나타난 후 5분 이상 기다립니다.

7. 버킷 오류로 인해 객체를 복제하지 못했는지 확인하려면 을 참조하십시오."실패한 복제 작업을 식별하고 다시 시도하십시오"

그룹 및 사용자를 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.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "루트 액세스 권한"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 OpenLDAP 서버 구성 지침참조하십시오.
- LDAP 서버와의 통신에 TLS(Transport Layer Security)를 사용하려는 경우 ID 공급자는 TLS 1.2 또는 1.3을 사용해야 합니다. 을 "발신 TLS 연결에 지원되는 암호"참조하십시오.

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.

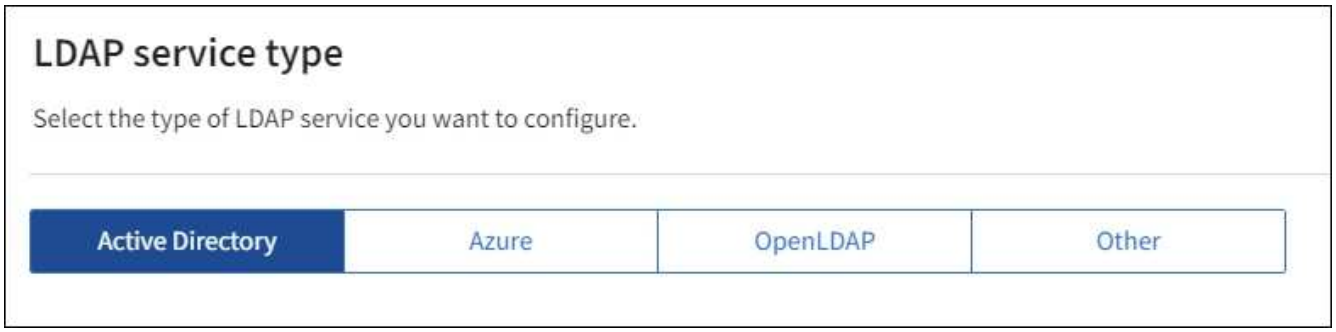
> This tenant account uses the LDAP server that is configured for the Grid Manager.
> Contact the grid administrator for information or to change this setting.

구성을 입력합니다

Identify 페더레이션을 구성할 때 StorageGRID가 LDAP 서비스에 연결하는 데 필요한 값을 제공합니다.

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 Directory 및 OpenLDAP에 대해 `uid` 와 동일합니다 `sAMAccountName`. Oracle Directory Server를 구성하는 경우 를 입력합니다 `uid`.
   - * 사용자 UUID *: LDAP 사용자의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 Active Directory 및 OpenLDAP에 대해 `entryUUID` 와 동일합니다 `objectGUID`. Oracle Directory Server를 구성하는 경우 를 입력합니다 `nsuniqueid`. 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 Directory 및 OpenLDAP에 대해 `cn` 와 동일합니다 `sAMAccountName`. Oracle Directory Server를 구성하는 경우 를 입력합니다 `cn`.
   - * 그룹 UUID *: LDAP 그룹의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 Active Directory 및 OpenLDAP에 대해 `entryUUID` 와 동일합니다 `objectGUID`. Oracle Directory Server를 구성하는 경우 를 입력합니다 `nsuniqueid`. 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.

     - `sAMAccountName` 또는 `uid`
     - `objectGUID` `entryUUID`, 또는 `nsuniqueid`
     - `cn`
     - `memberOf` 또는 `isMemberOf`
     - * Active Directory *: `objectSid`, `primaryGroupID`, `userAccountControl` 및 `userPrincipalName`
     - * Azure *: `accountEnabled` 및 `userPrincipalName`

   - * 암호 *: 사용자 이름과 연결된 암호입니다.

     나중에 암호를 변경하는 경우 이 페이지에서 암호를 업데이트해야 합니다.

   - * 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\[USERNAME]`

- * 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.

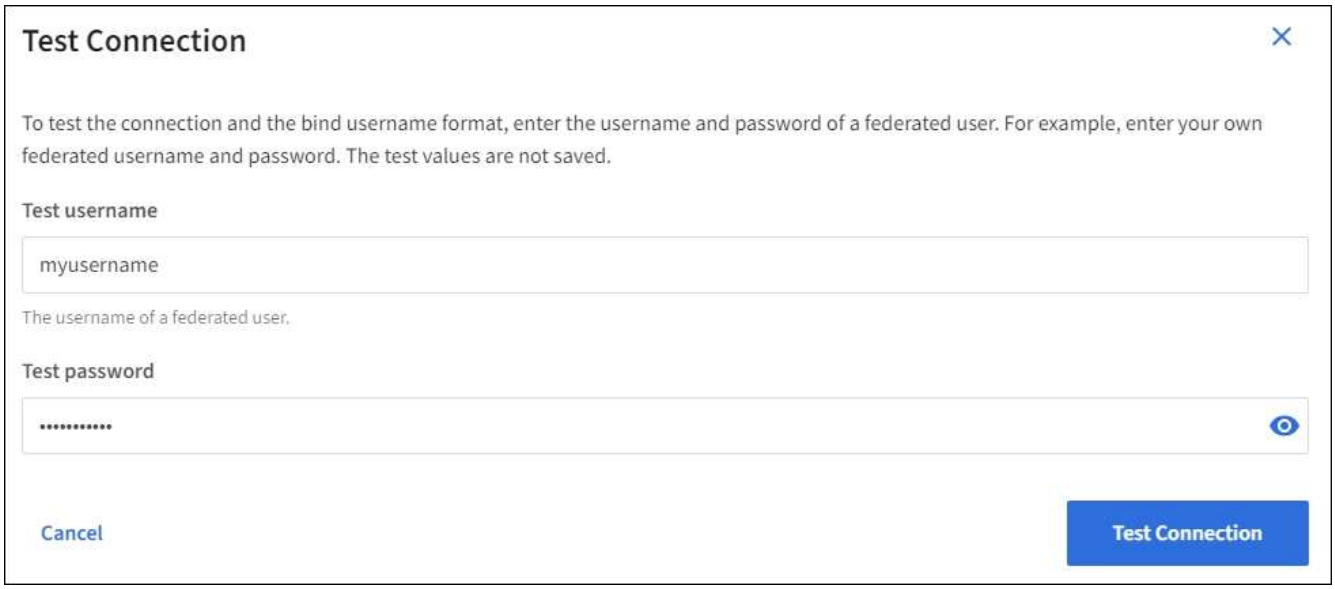
연결을 테스트하고 구성을 저장합니다

모든 값을 입력한 후 구성을 저장하기 전에 연결을 테스트해야 합니다. StorageGRID는 LDAP 서버에 대한 연결 설정과 바인딩 사용자 이름 형식(제공한 경우)을 확인합니다.

단계

1. Test connection * 을 선택합니다.
2. 바인딩 사용자 이름 형식을 제공하지 않은 경우:
   - 연결 설정이 유효한 경우 "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 유효한 경우 "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 대해서는 알림이

발생하지 않습니다.

- SSO(Single Sign-On)가 * Enabled * 또는 * Sandbox Mode * 로 설정된 경우 * Enable identity federation * 확인란이 비활성화됩니다. ID 페더레이션을 비활성화하려면 Single Sign-On 페이지의 SSO 상태가 * 사용 안 함 * 이어야 합니다. 을 "SSO(Single Sign-On)를 비활성화합니다"참조하십시오.

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 삭제하거나 모든 그룹에서 사용자를 제거합니다.

MemberOf 및 구체화 오버레이

MemberOf 및 구체화 오버레이를 활성화해야 합니다. 자세한 내용은 에서 역방향 그룹 구성원 유지 관리에 대한 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`
- `olcDbIndex: 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 "OpenLDAP 설명서: 버전 2.4 관리자 가이드"참조하십시오.

테넌트 그룹을 관리합니다

S3 테넌트에 대한 그룹을 생성합니다

통합 그룹을 가져오거나 로컬 그룹을 생성하여 S3 사용자 그룹에 대한 권한을 관리할 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "루트 액세스 권한"있습니다.
- 통합 그룹을 가져오려는 경우 이 "ID 페더레이션을 구성했습니다"있으며 페더레이션 그룹이 구성된 ID 원본에 이미 있습니다.

- 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있으면 에 대한 워크플로 및 고려 사항을 검토한 후 "테넌트 그룹 및 사용자를 클론 생성합니다"테넌트의 소스 그리드에 로그인됩니다.

그룹 생성 마법사에 액세스합니다

첫 번째 단계로 그룹 생성 마법사에 액세스합니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 이 그리드에 생성된 새 그룹이 연결의 다른 그리드에 있는 동일한 테넌트에 복제됨을 나타내는 파란색 배너가 나타나는지 확인합니다. 이 배너가 나타나지 않으면 테넌트의 대상 그리드에 로그인되었을 수 있습니다.

3. Create group * 을 선택합니다.

그룹 유형을 선택합니다

로컬 그룹을 생성하거나 통합 그룹을 가져올 수 있습니다.

단계

1. 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.

2. 그룹의 이름을 입력합니다.
   - * 로컬 그룹 *: 표시 이름과 고유 이름을 모두 입력합니다. 나중에 표시 이름을 편집할 수 있습니다.

     테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 대상 그리드에 해당 테넌트에 대해 동일한 * 고유 이름 * 이 이미 있으면 클론 생성 오류가 발생합니다.

   - * 페더레이션 그룹 *: 고유한 이름을 입력합니다. Active Directory의 경우 고유 이름은 속성과 연결된 `sAMAccountName` 이름입니다. OpenLDAP의 경우 고유 이름은 속성과 연결된 `uid` 이름입니다.

3. Continue * 를 선택합니다.

그룹 권한을 관리합니다

그룹 권한은 테넌트 관리자 및 테넌트 관리 API에서 사용자가 수행할 수 있는 작업을 제어합니다.

단계

1. 액세스 모드 * 의 경우 다음 중 하나를 선택합니다.
   - * 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.

   > ⓘ 사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.

2. 이 그룹에 대한 권한을 하나 이상 선택합니다.

   을 "테넌트 관리 권한"참조하십시오.

3. Continue * 를 선택합니다.

S3 그룹 정책을 설정합니다

그룹 정책은 사용자가 가질 S3 액세스 권한을 결정합니다.

단계

1. 이 그룹에 사용할 정책을 선택합니다.

그룹 정책	설명
S3 액세스 없음	기본값. 버킷 정책을 통해 액세스 권한이 부여되지 않은 한 이 그룹의 사용자는 S3 리소스에 액세스할 수 없습니다. 이 옵션을 선택하면 루트 사용자만 기본적으로 S3 리소스에 액세스할 수 있습니다.
읽기 전용 액세스	이 그룹의 사용자는 S3 리소스에 읽기 전용 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 문자열을 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 문자열을 편집할 수 없습니다.

그룹 정책	설명
랜섬웨어 완화	이 예제 정책은 이 테넌트의 모든 버킷에 적용됩니다. 이 그룹의 사용자는 일반적인 작업을 수행할 수 있지만 개체 버전 관리가 활성화된 버킷에서 개체를 영구적으로 삭제할 수는 없습니다. Manage All Bucket * 권한이 있는 테넌트 관리자 사용자는 이 그룹 정책을 재정의할 수 있습니다. 모든 버킷 관리 권한을 신뢰할 수 있는 사용자로 제한하고 가능한 경우 MFA(Multi-Factor Authentication)를 사용합니다.
맞춤형	그룹의 사용자에게는 텍스트 상자에 지정한 사용 권한이 부여됩니다.

2. 사용자 정의 * 를 선택한 경우 그룹 정책을 입력합니다. 각 그룹 정책은 크기 제한이 5,120바이트입니다. 올바른 JSON 형식 문자열을 입력해야 합니다.

   언어 구문 및 예제를 포함한 그룹 정책에 대한 자세한 내용은 을 참조하십시오"그룹 정책의 예".

3. 로컬 그룹을 만드는 경우 * 계속 * 을 선택합니다. 통합 그룹을 만드는 경우 * 그룹 생성 * 및 * 마침 * 을 선택합니다.

사용자 추가(로컬 그룹만 해당)

사용자를 추가하지 않고 그룹을 저장하거나 이미 존재하는 로컬 사용자를 선택적으로 추가할 수 있습니다.

> 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 소스 그리드에 로컬 그룹을 생성할 때 선택한 모든 사용자는 대상 그리드에 그룹이 클론 생성될 때 포함되지 않습니다. 따라서 그룹을 만들 때 사용자를 선택하지 마십시오. 대신 사용자를 생성할 때 그룹을 선택합니다.

단계

1. 필요에 따라 이 그룹에 대해 하나 이상의 로컬 사용자를 선택합니다.
2. Create group * 과 * Finish * 를 선택합니다.

   생성한 그룹이 그룹 목록에 나타납니다.

   테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있고 테넌트의 소스 그리드에 있는 경우 새 그룹이 테넌트의 대상 그리드에 복제됩니다. * 성공 * 은 그룹 세부 정보 페이지의 개요 섹션에 * 클론 생성 상태 * 로 표시됩니다.

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.

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

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.

- 이 있는 사용자 그룹에 속해 "루트 액세스 권한"있습니다.
- 통합 그룹을 가져오려는 경우 이 "ID 페더레이션을 구성했습니다"있으며 페더레이션 그룹이 구성된 ID 원본에 이미 있습니다.

그룹 생성 마법사에 액세스합니다

단계

첫 번째 단계로 그룹 생성 마법사에 액세스합니다.

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. Create group * 을 선택합니다.

그룹 유형을 선택합니다

로컬 그룹을 생성하거나 통합 그룹을 가져올 수 있습니다.

단계

1. 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.

2. 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 고유 이름은 속성과 연결된 `sAMAccountName` 이름입니다. OpenLDAP의 경우 고유 이름은 속성과 연결된 `uid` 이름입니다.
3. Continue * 를 선택합니다.

그룹 권한을 관리합니다

그룹 권한은 테넌트 관리자 및 테넌트 관리 API에서 사용자가 수행할 수 있는 작업을 제어합니다.

단계

1. 액세스 모드 * 의 경우 다음 중 하나를 선택합니다.
   - * 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.

   > ⓘ 사용자가 여러 그룹에 속해 있고 모든 그룹이 읽기 전용으로 설정되어 있는 경우 사용자는 선택한 모든 설정 및 기능에 대해 읽기 전용 권한을 갖게 됩니다.

2. 그룹 사용자가 테넌트 관리자 또는 테넌트 관리 API에 로그인해야 하는 경우 * Root access * 확인란을 선택합니다.
3. Continue * 를 선택합니다.

Swift 그룹 정책을 설정합니다

Swift 사용자는 컨테이너를 생성하고 오브젝트를 수집하려면 Swift REST API에 인증하는 관리자 권한이 필요합니다.

1. 그룹 사용자가 Swift REST API를 사용하여 컨테이너 및 객체를 관리해야 하는 경우 * Swift administrator * 확인란을 선택합니다.
2. 로컬 그룹을 만드는 경우 * 계속 * 을 선택합니다. 통합 그룹을 만드는 경우 * 그룹 생성 * 및 * 마침 * 을 선택합니다.

사용자 추가(로컬 그룹만 해당)

사용자를 추가하지 않고 그룹을 저장하거나 이미 존재하는 로컬 사용자를 선택적으로 추가할 수 있습니다.

단계

1. 필요에 따라 이 그룹에 대해 하나 이상의 로컬 사용자를 선택합니다.

   아직 로컬 사용자를 만들지 않은 경우 사용자 페이지에서 이 그룹을 사용자에게 추가할 수 있습니다. 을 "로컬 사용자를 관리합니다"참조하십시오.

2. Create group * 과 * Finish * 를 선택합니다.

   생성한 그룹이 그룹 목록에 나타납니다.

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.

권한	설명	세부 정보
루트 액세스	테넌트 관리자 및 테넌트 관리 API에 대한 전체 액세스를 제공합니다.	Swift 사용자는 테넌트 계정에 로그인하려면 루트 액세스 권한이 있어야 합니다.

권한	설명	세부 정보
관리자	Swift 테넌트만 해당. 이 테넌트 계정에 대한 Swift 컨테이너 및 객체에 대한 전체 액세스를 제공합니다	Swift 사용자는 Swift REST API를 사용하여 작업을 수행하려면 Swift 관리자 권한이 있어야 합니다.
자체 S3 자격 증명을 관리합니다	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 버킷을 봅니다	• S3 테넌트 *: 모든 버킷 및 버킷 구성을 볼 수 있습니다. • Swift 테넌트 *: Swift 사용자가 테넌트 관리 API를 사용하여 모든 컨테이너 및 컨테이너 구성을 볼 수 있습니다.	모든 버킷 보기 또는 모든 버킷 관리 권한이 없는 사용자에게는 * Bucket * 메뉴 옵션이 표시되지 않습니다. 이 권한은 모든 버킷 관리 권한으로 대체됩니다. S3 클라이언트 또는 S3 콘솔에서 사용하는 S3 버킷 또는 그룹 정책에 영향을 미치지 않습니다. 이 권한은 테넌트 관리 API에서만 Swift 그룹에 할당할 수 있습니다. 테넌트 관리자를 사용하여 Swift 그룹에 이 권한을 할당할 수 없습니다.
모든 버킷을 관리합니다	• 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 위한 설정을 관리할 수 있습니다. • Swift 테넌트 *: Swift 사용자가 테넌트 관리 API를 사용하여 Swift 컨테이너의 일관성을 제어할 수 있습니다.	모든 버킷 보기 또는 모든 버킷 관리 권한이 없는 사용자에게는 * Bucket * 메뉴 옵션이 표시되지 않습니다. 이 권한은 모든 버킷 보기 권한보다 우선합니다. S3 클라이언트 또는 S3 콘솔에서 사용하는 S3 버킷 또는 그룹 정책에 영향을 미치지 않습니다. 이 권한은 테넌트 관리 API에서만 Swift 그룹에 할당할 수 있습니다. 테넌트 관리자를 사용하여 Swift 그룹에 이 권한을 할당할 수 없습니다.
엔드포인트 관리	사용자가 테넌트 관리자 또는 테넌트 관리 API를 사용하여 플랫폼 서비스 엔드포인트를 생성하거나 편집할 수 있습니다. 이 엔드포인트는 StorageGRID 플랫폼 서비스의 대상으로 사용됩니다.	이 권한이 없는 사용자는 * 플랫폼 서비스 끝점 * 메뉴 옵션이 표시되지 않습니다.
S3 콘솔 탭을 사용합니다	모든 버킷 보기 또는 모든 버킷 관리 권한과 함께 사용하면 사용자가 버킷에 대한 세부 정보 페이지의 S3 콘솔 탭에서 오브젝트를 보고 관리할 수 있습니다.	

그룹을 관리합니다

필요에 따라 테넌트 그룹을 관리하여 그룹 보기, 편집 또는 복제 등을 수행할 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "루트 액세스 권한"있습니다.

그룹을 보거나 편집합니다

각 그룹의 기본 정보와 세부 정보를 보고 편집할 수 있습니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 그룹 페이지에 제공된 정보를 검토하여 이 테넌트 계정의 모든 로컬 및 통합 그룹에 대한 기본 정보를 나열합니다.

   테넌트 계정에 * Use GRID Federation Connection * 권한이 있고 테넌트의 소스 그리드에서 그룹을 보고 있는 경우:

   - 그룹을 편집하거나 제거하면 변경 내용이 다른 그리드와 동기화되지 않음을 나타내는 배너 메시지가 표시됩니다.
   - 필요에 따라 대상 그리드의 테넌트에 그룹이 복제되지 않았는지 여부를 나타내는 배너 메시지가 표시됩니다. 하지만 그룹 클론을 재시도하십시오실패했어요.
3. 그룹 이름을 변경하려면:
   a. 그룹의 확인란을 선택합니다.
   b. Actions * > * Edit group name * 을 선택합니다.
   c. 새 이름을 입력합니다.
   d. 변경 사항 저장 * 을 선택합니다
4. 자세한 내용을 보거나 추가로 편집하려면 다음 중 하나를 수행합니다.
   - 그룹 이름을 선택합니다.
   - 그룹의 확인란을 선택하고 * Actions * > * View group details * 를 선택합니다.
5. 각 그룹에 대해 다음 정보를 보여 주는 개요 섹션을 검토합니다.
   - 표시 이름
   - 고유한 이름입니다
   - 유형
   - 액세스 모드
   - 권한
   - S3 정책
   - 이 그룹의 사용자 수입니다
   - 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있고 테넌트의 소스 격자에서 그룹을 보고 있는 경우 추가 필드:
     - 복제 상태, * 성공 * 또는 * 실패 *
     - 이 그룹을 편집하거나 삭제하면 변경 내용이 다른 눈금과 동기화되지 않음을 나타내는 파란색 배너입니다.
6. 필요에 따라 그룹 설정을 편집합니다. 입력할 항목에 대한 자세한 내용은 "S3 테넌트에 대한 그룹을 생성합니다" 및 "Swift 테넌트의 그룹을 생성합니다"을 참조하십시오.

a. 개요 섹션에서 이름이나 편집 아이콘을 선택하여 표시 이름을 변경합니다.

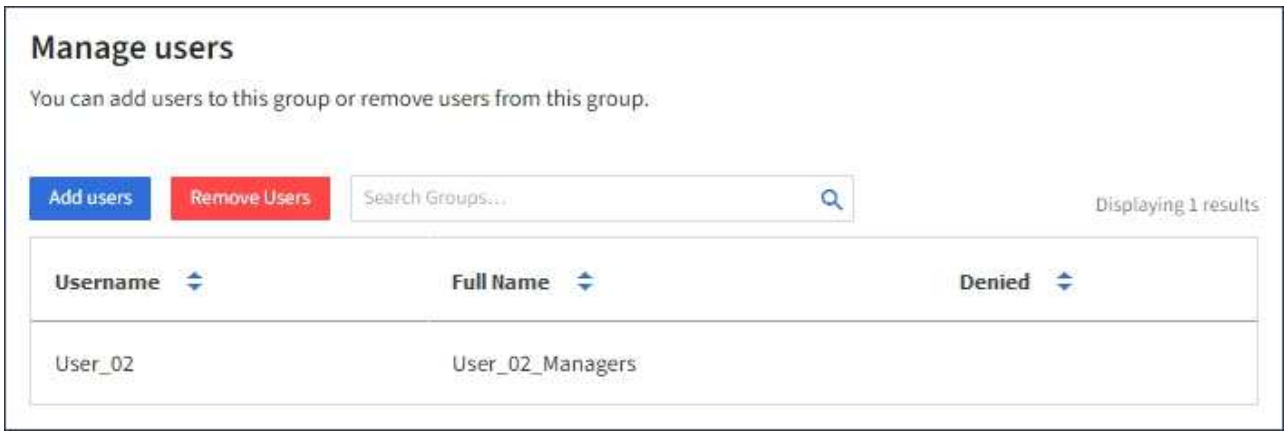
b. 그룹 권한 * 탭에서 권한을 업데이트하고 * 변경 사항 저장 * 을 선택합니다.

c. 그룹 정책 * 탭에서 변경을 수행하고 * 변경 사항 저장 * 을 선택합니다.

- S3 그룹을 편집하는 경우 필요에 따라 다른 S3 그룹 정책을 선택하거나 사용자 지정 정책의 JSON 문자열을 입력합니다.
- Swift 그룹을 편집 중인 경우 * Swift 관리자 * 확인란을 선택하거나 선택 취소합니다.

7. 그룹에 기존 로컬 사용자를 하나 이상 추가하려면 다음을 수행합니다.

a. 사용자 탭을 선택합니다.



b. 사용자 추가 * 를 선택합니다.

c. 추가할 기존 사용자를 선택하고 * 사용자 추가 * 를 선택합니다.

오른쪽 위에 성공 메시지가 나타납니다.

8. 그룹에서 로컬 사용자 제거하기:

a. 사용자 탭을 선택합니다.

b. 사용자 제거 * 를 선택합니다.

c. 제거할 사용자를 선택하고 * 사용자 제거 * 를 선택합니다.

오른쪽 위에 성공 메시지가 나타납니다.

9. 변경한 각 섹션에 대해 * 변경 사항 저장 * 을 선택했는지 확인합니다.

그룹이 중복되었습니다

기존 그룹을 복제하여 새 그룹을 더 빠르게 만들 수 있습니다.

테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있고 테넌트의 소스 그리드에서 그룹을 복제하는 경우 복제된 그룹은 테넌트의 대상 그리드에 복제됩니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 복제할 그룹의 확인란을 선택합니다.

3. Actions * > * Duplicate group * 을 선택합니다.
4. 입력할 항목에 대한 자세한 내용은 "S3 테넌트에 대한 그룹을 생성합니다" 또는 "Swift 테넌트의 그룹을 생성합니다"을 참조하십시오.
5. Create group * 을 선택합니다.

그룹 클론을 다시 시도하십시오

실패한 클론을 재시도하려면 다음을 수행합니다.

1. 그룹 이름 아래에 _ (클론 생성 실패) _ 을(를) 나타내는 각 그룹을 선택합니다.
2. Actions * > * Clone groups * 를 선택합니다.
3. 클론 생성 중인 각 그룹의 세부 정보 페이지에서 클론 작업의 상태를 봅니다.

자세한 내용은 를 참조하십시오"클론 테넌트 그룹 및 사용자".

하나 이상의 그룹을 삭제합니다

하나 이상의 그룹을 삭제할 수 있습니다. 삭제된 그룹에만 속하는 사용자는 더 이상 테넌트 관리자에 로그인하거나 테넌트 계정을 사용할 수 없습니다.

> 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있고 그룹을 삭제하는 경우 StorageGRID는 다른 그리드에서 해당 그룹을 삭제하지 않습니다. 이 정보를 동기화해야 하는 경우 두 그리드에서 동일한 그룹을 삭제해야 합니다.

단계

1. 액세스 관리 * > * 그룹 * 을 선택합니다.
2. 삭제할 각 그룹의 확인란을 선택합니다.
3. Actions * > * Delete group * 또는 * Actions * > * Delete groups * 를 선택합니다.

   확인 대화 상자가 나타납니다.

4. 그룹 삭제 * 또는 * 그룹 삭제 * 를 선택합니다.

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 사용자 한 명이 포함됩니다. 로컬 사용자를 추가하고 제거할 수는 있지만 루트 사용자를 제거할 수는 없습니다.

> StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 로컬 사용자는 그룹 권한에 따라 클라이언트 애플리케이션을 사용하여 테넌트의 리소스에 액세스할 수 있지만 테넌트 관리자 또는 테넌트 관리 API에 로그인할 수 없습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "루트 액세스 권한"있습니다.

- 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있으면 에 대한 워크플로 및 고려 사항을 검토한 후 "테넌트 그룹 및 사용자를 클론 생성합니다"테넌트의 소스 그리드에 로그인됩니다.

로컬 사용자를 생성합니다

로컬 사용자를 만들어 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.

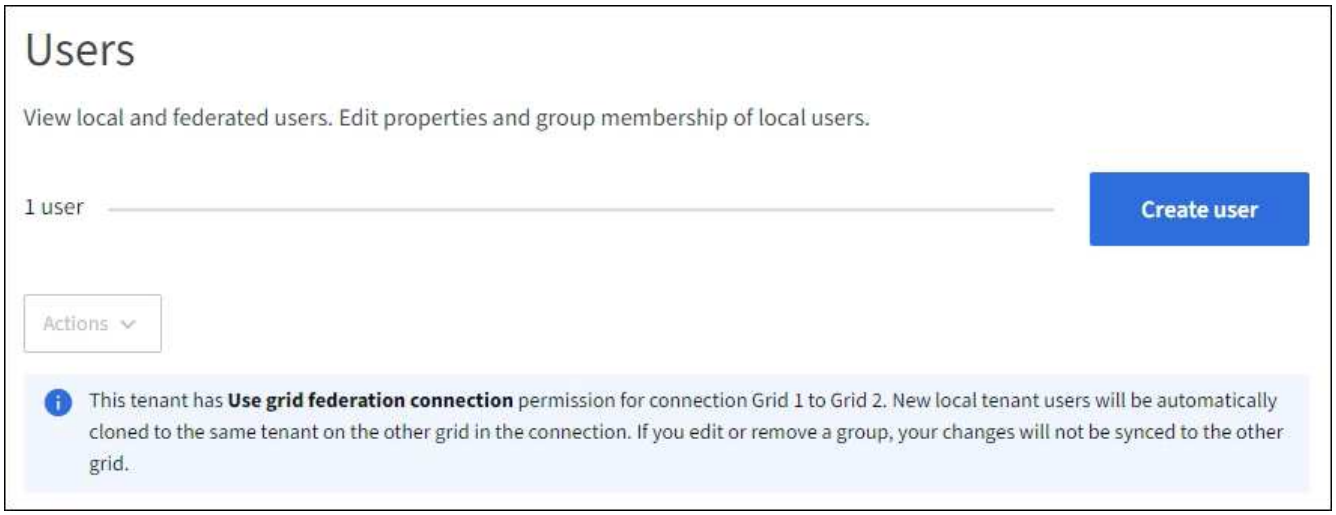
그룹에 속하지 않는 Swift 사용자는 관리 권한이나 Swift 컨테이너 액세스 권한이 없습니다.

사용자 생성 마법사에 액세스합니다

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.

   테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 파란색 배너는 해당 테넌트의 소스 그리드임을 나타냅니다. 이 그리드에서 만드는 모든 로컬 사용자는 연결의 다른 그리드에 복제됩니다.



2. 사용자 생성 * 을 선택합니다.

자격 증명을 입력합니다

단계

1. 사용자 자격 증명 입력 * 단계에 대해 다음 필드를 입력합니다.

필드에 입력합니다	설명
전체 이름	이 사용자의 전체 이름(예: 사용자의 이름 및 성 또는 응용 프로그램의 이름).

필드에 입력합니다	설명
사용자 이름	이 사용자가 로그인하는 데 사용할 이름입니다. 사용자 이름은 고유해야 하며 변경할 수 없습니다. • 참고 *: 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 대상 그리드에 해당 테넌트에 대해 동일한 * 사용자 이름 * 이 이미 있으면 클론 생성 오류가 발생합니다.
암호 및 암호 확인	사용자가 로그인할 때 처음 사용할 암호입니다.
액세스를 거부합니다	이 사용자가 하나 이상의 그룹에 속해 있더라도 테넌트 계정에 로그인하지 못하도록 하려면 * 예 * 를 선택합니다. 예를 들어, * 예 * 를 선택하여 사용자의 로그인 기능을 일시적으로 중단시킵니다.

2. Continue * 를 선택합니다.

그룹에 할당합니다

단계

1. 사용자를 하나 이상의 로컬 그룹에 할당하여 수행할 수 있는 작업을 결정합니다.

   그룹에 사용자를 할당하는 것은 선택 사항입니다. 원하는 경우 그룹을 만들거나 편집할 때 사용자를 선택할 수 있습니다.

   그룹에 속하지 않은 사용자에게는 관리 권한이 없습니다. 권한은 누적됩니다. 사용자는 자신이 속한 모든 그룹에 대한 모든 권한을 갖게 됩니다. 을 "테넌트 관리 권한"참조하십시오.

2. 사용자 생성 * 을 선택합니다.

   테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있고 테넌트의 소스 그리드에 있는 경우 새 로컬 사용자는 테넌트의 대상 그리드에 복제됩니다. * 성공 * 은 사용자 세부 정보 페이지의 개요 섹션에 * 클론 생성 상태 * 로 표시됩니다.

3. 사용자 페이지로 돌아가려면 * 마침 * 을 선택합니다.

로컬 사용자를 보거나 편집합니다

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.
2. 사용자 페이지에 제공된 정보를 검토하여 이 테넌트 계정에 대한 모든 로컬 및 통합 사용자의 기본 정보를 나열합니다.

   테넌트 계정에 * Use grid 페더레이션 연결 * 권한이 있고 테넌트의 소스 그리드에서 사용자를 보고 있는 경우:

   ◦ 배너 메시지는 사용자를 편집하거나 제거하면 변경 내용이 다른 그리드와 동기화되지 않음을 나타냅니다.

   ◦ 필요에 따라 배너 메시지는 사용자가 대상 그리드의 테넌트에 복제되지 않았는지 여부를 나타냅니다. 할 수 실패한 사용자 클론을 재시도합니다있습니다.

3. 사용자의 전체 이름을 변경하려면:
   a. 사용자의 확인란을 선택합니다.
   b. 작업 * > * 전체 이름 편집 * 을 선택합니다.
   c. 새 이름을 입력합니다.
   d. 변경 사항 저장 * 을 선택합니다
4. 자세한 내용을 보거나 추가로 편집하려면 다음 중 하나를 수행합니다.
   - 사용자 이름을 선택합니다.
   - 사용자의 확인란을 선택하고 * Actions * > * View user details * 를 선택합니다.
5. 각 사용자에 대해 다음 정보를 보여 주는 개요 섹션을 검토합니다.
   - 전체 이름
   - 사용자 이름
   - 사용자 유형
   - 액세스가 거부되었습니다
   - 액세스 모드
   - 그룹 구성원 자격
   - 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있고 테넌트의 소스 격자에서 사용자를 보는 경우 추가 필드:
     - 복제 상태, * 성공 * 또는 * 실패 *
     - 이 사용자를 편집하면 변경 내용이 다른 눈금과 동기화되지 않음을 나타내는 파란색 배너입니다.
6. 필요에 따라 사용자 설정을 편집합니다. 입력할 내용에 대한 자세한 내용은 을 로컬 사용자를 생성합니다참조하십시오.
   a. 개요 섹션에서 이름 또는 편집 아이콘을 선택하여 전체 이름을 변경합니다.

      사용자 이름은 변경할 수 없습니다.

   b. 암호 * 탭에서 사용자 암호를 변경하고 * 변경 사항 저장 * 을 선택합니다.
   c. 액세스 * 탭에서 * 아니요 * 를 선택하여 사용자가 로그인할 수 있도록 하거나 * 예 * 를 선택하여 사용자가 로그인할 수 없도록 합니다. 그런 다음 * 변경 사항 저장 * 을 선택합니다.
   d. 액세스 키 * 탭에서 * 키 생성 * 을 선택하고 의 지침을 "다른 사용자의 S3 액세스 키 생성"따릅니다.
   e. 그룹 * 탭에서 * 그룹 편집 * 을 선택하여 사용자를 그룹에 추가하거나 그룹에서 제거합니다. 그런 다음 * 변경 사항 저장 * 을 선택합니다.
7. 변경한 각 섹션에 대해 * 변경 사항 저장 * 을 선택했는지 확인합니다.

로컬 사용자를 복제하십시오

로컬 사용자를 복제하면 새 사용자를 보다 빠르게 만들 수 있습니다.

> 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있고 테넌트의 소스 그리드에서 사용자를 복제하면 복제된 사용자는 테넌트의 대상 그리드에 복제됩니다.

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.
2. 복제할 사용자의 확인란을 선택합니다.
3. Actions * > * Duplicate user * 를 선택합니다.
4. 입력할 내용에 대한 자세한 내용은 을 로컬 사용자를 생성합니다참조하십시오.
5. 사용자 생성 * 을 선택합니다.

사용자 클론을 다시 시도하십시오

실패한 클론을 재시도하려면 다음을 수행합니다.

1. 사용자 이름 아래에 _ (클론 생성 실패) _ 을(를) 나타내는 각 사용자를 선택합니다.
2. Actions * > * Clone users * 를 선택합니다.
3. 클론 복제할 각 사용자의 세부 정보 페이지에서 클론 작업의 상태를 확인합니다.

자세한 내용은 를 참조하십시오"클론 테넌트 그룹 및 사용자".

하나 이상의 로컬 사용자를 삭제합니다

StorageGRID 테넌트 계정에 더 이상 액세스할 필요가 없는 하나 이상의 로컬 사용자를 영구적으로 삭제할 수 있습니다.

테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있고 로컬 사용자를 삭제하는 경우 StorageGRID는 다른 그리드에서 해당 사용자를 삭제하지 않습니다. 이 정보를 동기화해야 하는 경우 두 그리드에서 동일한 사용자를 삭제해야 합니다.

통합 사용자를 삭제하려면 통합 ID 소스를 사용해야 합니다.

단계

1. 액세스 관리 * > * 사용자 * 를 선택합니다.
2. 삭제할 각 사용자에 대한 확인란을 선택합니다.
3. Actions * > * Delete user * 또는 * Actions * > * Delete users * 를 선택합니다.

   확인 대화 상자가 나타납니다.

4. 사용자 삭제 * 또는 * 사용자 삭제 * 를 선택합니다.

S3 액세스 키를 관리합니다

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.

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. 버킷과 오브젝트에 액세스하려면 액세스 키가 있어야 합니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "자신의 S3 자격 증명 또는 루트 액세스 권한을 관리합니다"있습니다.

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.

     > 만료 날짜는 현재 날짜로부터 최대 5년일 수 있습니다. 만료 시간은 현재 시간에서 최소 1분이 될 수 있습니다.

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.

7. 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우, 필요에 따라 테넌트 관리 API를 사용하여 소스 그리드의 테넌트에서 대상 그리드의 테넌트로 S3 액세스 키를 수동으로 복제합니다. 을 "API를 사용하여 S3 액세스 키의 클론을 생성합니다"참조하십시오.

S3 액세스 키를 봅니다

S3 테넌트를 사용 중이고 이 있는 경우 "적절한 권한"S3 액세스 키 목록을 볼 수 있습니다. 만료 시간을 기준으로 목록을 정렬할 수 있으므로 곧 만료되는 키를 확인할 수 있습니다. 필요에 따라 를 사용할 수도 있고 "키를 삭제합니다"더 이상 사용하지 않을 수도 "새 키를 만듭니다"있습니다.

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.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 자신의 S3 자격 증명을 관리하는 사용자 그룹에 속해 "권한"있습니다.

단계

1. 스토리지(S3) * > * 내 액세스 키 * 를 선택합니다.
2. 내 액세스 키 페이지에서 * 만료 시간 * 또는 * 액세스 키 ID * 를 기준으로 기존 액세스 키를 정렬합니다.
3. 필요에 따라 새 키를 만들거나 더 이상 사용하지 않는 키를 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.

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.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.

- 이 "S3 자격 증명 사용 권한을 관리합니다"있습니다.

> 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.
2. 내 액세스 키 페이지에서 제거할 각 액세스 키에 대한 확인란을 선택합니다.
3. Delete key * 를 선택합니다.
4. 확인 대화 상자에서 * 키 삭제 * 를 선택합니다.

   페이지의 오른쪽 상단에 확인 메시지가 나타납니다.

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.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "루트 액세스 권한"있습니다.

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 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 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 정기적으로 새 키를 만들 필요가 없는 경우 키에 대한 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.

   만료 날짜는 현재 날짜로부터 최대 5년일 수 있습니다. 만료 시간은 현재 시간에서 최소 1분이 될 수 있습니다.

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.

8. 테넌트 계정에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우, 필요에 따라 테넌트 관리 API를 사용하여 소스 그리드의 테넌트에서 대상 그리드의 테넌트로 S3 액세스 키를 수동으로 복제합니다. 을 "API를 사용하여 S3 액세스 키의 클론을 생성합니다"참조하십시오.

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.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 "루트 액세스 권한"있습니다.

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. 사용자 페이지에서 S3 액세스 키를 보려는 사용자를 선택합니다.
3. 사용자 세부 정보 페이지에서 * 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.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 "루트 액세스 권한"있습니다.

> 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. 사용자 페이지에서 관리할 S3 액세스 키가 있는 사용자를 선택합니다.
3. 사용자 세부 정보 페이지에서 * 액세스 키 * 를 선택한 다음 삭제할 각 액세스 키에 대한 확인란을 선택합니다.
4. Actions * > * Delete Selected key * 를 선택합니다.
5. 확인 대화 상자에서 * 키 삭제 * 를 선택합니다.

   페이지의 오른쪽 상단에 확인 메시지가 나타납니다.

S3 버킷을 관리합니다

S3 버킷을 생성합니다

테넌트 관리자를 사용하여 오브젝트 데이터용 S3 버킷을 생성할 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 루트 액세스 또는 모든 버킷을 관리하는 사용자 그룹에 속해 "권한"있습니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

버킷 또는 오브젝트의 S3 오브젝트 잠금 속성을 설정하거나 수정할 수 있는 권한은 에서 부여할 수 "버킷 정책 또는 그룹 정책"있습니다.

- 버킷에 S3 오브젝트 잠금을 설정할 계획이라면 그리드 관리자가 StorageGRID 시스템에 대한 글로벌 S3 오브젝트 잠금 설정을 활성화했으며 S3 오브젝트 잠금 버킷 및 오브젝트 요구 사항을 검토했습니다.
- 각 테넌트에 5,000개의 버킷이 있는 경우 그리드의 각 스토리지 노드에 최소 64GB의 RAM이 있습니다.

각 그리드에는 최대 100,000개의 버킷을 포함할 수 있습니다.

마법사에 액세스합니다

단계

1. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. Create bucket * 을 선택합니다.

세부 정보를 입력합니다

단계

1. 버킷에 대한 세부 정보를 입력합니다.

필드에 입력합니다	설명
버킷 이름	다음 규칙을 준수하는 버킷의 이름: • 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 요청에는 기간을 포함할 수 없습니다. 마침표는 서버 와일드카드 인증서 확인에 문제를 일으킬 수 있습니다. 자세한 내용은 를 "버킷 명명 규칙에 대한 AWS(Amazon Web Services) 문서입니다"참조하십시오. • 참고 *: 버킷을 만든 후에는 버킷 이름을 변경할 수 없습니다.
지역	버켓의 지역. StorageGRID 관리자가 사용 가능한 영역을 관리합니다. 버킷 영역은 오브젝트에 적용되는 데이터 보호 정책에 영향을 미칠 수 있습니다. 기본적으로 모든 버킷은 해당 `us-east-1` 지역에서 생성됩니다. • 참고 *: 버킷을 생성한 후에는 지역을 변경할 수 없습니다.

2. Continue * 를 선택합니다.

설정을 관리합니다

단계

1. 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. 버킷이 교차 그리드 복제에 사용될 경우 오브젝트 버전 관리를 활성화해야 합니다.

2. 전역 S3 오브젝트 잠금 설정이 활성화된 경우 버킷에 WORM(Write-Once-Read-Many) 모델을 사용하여 오브젝트를 저장할 수 있도록 S3 오브젝트 잠금을 선택적으로 설정합니다.

   특정 규정 요구 사항을 충족하기 위해 개체를 일정 시간 동안 유지해야 하는 경우에만 버킷에 대해 S3 오브젝트 잠금을 활성화합니다. S3 오브젝트 잠금은 고정된 시간 또는 무기한으로 오브젝트를 삭제 또는 덮어쓰는 것을 방지하는 영구 설정입니다.

   > 버킷에 대해 S3 오브젝트 잠금 설정이 활성화된 후에는 비활성화할 수 없습니다. 올바른 권한이 있는 사용자는 변경할 수 없는 객체를 이 버킷에 추가할 수 있습니다. 이러한 오브젝트 또는 버킷 자체를 삭제하지 못할 수 있습니다.

   버킷에 대해 S3 오브젝트 잠금을 설정하면 버킷 버전 관리가 자동으로 활성화됩니다.

3. S3 오브젝트 잠금 활성화 * 를 선택한 경우 이 버킷에 대해 * 기본 보존 * 을 선택적으로 활성화합니다.

   > 그리드 관리자가 사용자에게 권한을 부여해야 "S3 오브젝트 잠금의 특정 기능 사용"합니다.

   기본 보존 * 이 활성화되면 버킷에 추가된 새 오브젝트는 삭제 또는 덮어쓰기가 되지 않도록 자동으로 보호됩니다. 기본 보존 * 설정은 고유한 보존 기간이 있는 개체에는 적용되지 않습니다.

   a. 기본 보존 * 이 활성화된 경우 버킷에 대한 * 기본 보존 모드 * 를 지정합니다.

기본 보존 모드	설명
기대치를 설정합니다	• 있는 사용자는 `s3:BypassGovernanceRetention`권한이 요청 헤더를 사용하여 보존 설정을 무시할 수 `x-amz-bypass-governance-retention: true` 있습니다. • 이러한 사용자는 보존 기한이 되기 전에 개체 버전을 삭제할 수 있습니다. • 이러한 사용자는 개체의 보존 기간(Retain-until-date)을 증가, 감소 또는 제거할 수 있습니다.

기본 보존 모드	설명
규정 준수	• 보존 기한 에 도달할 때까지 개체를 삭제할 수 없습니다. • 오브젝트의 보존 기한 을 늘릴 수 있지만 줄일 수는 없습니다. • 개체의 보존 기한 은 해당 날짜에 도달할 때까지 제거할 수 없습니다. ◦ 참고 *: 그리드 관리자가 규정 준수 모드를 사용할 수 있도록 허용해야 합니다.

b. 기본 보존 * 이 활성화된 경우 버킷의 * 기본 보존 기간 * 을 지정합니다.

기본 보존 기간 * 은 이 버킷에 추가된 새 오브젝트를 인제스트할 시간부터 보존 기간을 나타냅니다. 그리드 관리자가 설정한 테넌트의 최대 보존 기간보다 작거나 같은 값을 지정하십시오.

그리드 관리자가 테넌트를 생성할 때 1일에서 100년 사이의 값을 지정할 수 있는 _MAXIMUM_RETENTION 기간이 설정됩니다. _default_retention 기간을 설정하면 최대 보존 기간에 설정된 값을 초과할 수 없습니다. 필요한 경우 그리드 관리자에게 최대 보존 기간을 늘리거나 줄이도록 요청하십시오.

4. (용량 제한 활성화) 필요에 따라 * Enable capacity limit * 를 선택합니다.

용량 제한은 이 버킷의 오브젝트에 사용할 수 있는 최대 용량입니다. 이 값은 물리 크기(디스크의 크기)가 아닌 논리 양(개체 크기)을 나타냅니다.

제한을 설정하지 않으면 이 버킷의 용량은 무제한입니다. 자세한 내용은 을 "용량 제한 사용량" 참조하십시오.

5. Create bucket * 을 선택합니다.

버킷이 생성되어 버킷 페이지의 테이블에 추가됩니다.

6. 필요에 따라 * 버킷 세부 정보 페이지로 이동 * 을 선택하여 "버킷 세부 정보를 봅니다"추가 구성을 수행합니다.

버킷 세부 정보를 봅니다

테넌트 계정의 버킷을 볼 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "루트 액세스, 모든 버킷 관리 또는 모든 버킷 보기 권한"있습니다. 이러한 권한은 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

단계

1. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.

Bucket 페이지가 나타납니다.

2. 각 버킷에 대한 요약 표를 검토합니다.

필요에 따라 모든 열을 기준으로 정보를 정렬하거나 목록 앞뒤에 페이지를 표시할 수 있습니다.

표시되는 개체 수, 사용된 공간 및 사용 현황 값은 추정값입니다. 이러한 추정치는 베스트 타이밍, 네트워크 연결 및 노드 상태의 영향을 받습니다. 버킷에 버전 관리가 활성화된 경우 삭제된 개체 버전은 오브젝트 수에 포함됩니다.

이름
: 버킷의 고유한 이름이며 변경할 수 없습니다.

활성화된 기능
: 버킷에 대해 활성화된 기능 목록입니다.

S3 오브젝트 잠금
: 버킷에 대해 S3 오브젝트 잠금이 설정되었는지 여부

  이 열은 그리드에 S3 오브젝트 잠금이 활성화된 경우에만 나타납니다. 또한 이 열에는 레거시 준수 버킷에 대한 정보도 표시됩니다.

지역
: 변경할 수 없는 버킷의 영역입니다. 이 열은 기본적으로 숨겨져 있습니다.

개체 수입니다
: 이 버킷의 오브젝트 수 버킷에 버전 관리가 활성화된 경우 현재 버전이 아닌 개체 버전이 이 값에 포함됩니다.

  개체를 추가하거나 삭제할 때 이 값은 즉시 업데이트되지 않을 수 있습니다.

사용된 공간
: 버킷에 있는 모든 오브젝트의 논리적 크기입니다. 논리적 크기에는 복제 또는 삭제 코딩 복사본 또는 오브젝트 메타데이터에 필요한 실제 공간이 포함되지 않습니다.

  이 값을 업데이트하는 데 최대 10분이 걸릴 수 있습니다.

사용
: 버킷의 용량 제한에 사용된 백분율(설정된 경우).

  사용률은 내부 추정치를 기준으로 하며 경우에 따라 초과될 수 있습니다. 예를 들어, StorageGRID는 테넌트가 객체 업로드를 시작할 때 용량 제한을 확인하고 테넌트가 용량 제한을 초과하는 경우 이 버킷에 대한 새 수신을 거부합니다. 그러나 StorageGRID는 용량 제한을 초과했는지 확인할 때 현재 업로드 크기를 고려하지 않습니다. 객체가 삭제되면 용량 제한 사용량이 다시 계산될 때까지 테넌트가 이 버킷에 새 객체를 업로드하지 못할 수 있습니다. 계산에는 10분 이상이 걸릴 수 있습니다.

  이 값은 객체 및 해당 메타데이터를 저장하는 데 필요한 물리적 크기가 아니라 논리적 크기를 나타냅니다.

용량
: 설정된 경우 버킷의 용량 제한입니다.

만든 날짜
: 버킷이 생성된 날짜 및 시간입니다. 이 열은 기본적으로 숨겨져 있습니다.

3. 특정 버킷의 세부 정보를 보려면 테이블에서 버킷 이름을 선택합니다.
   a. 웹 페이지 상단에 있는 요약 정보를 확인하여 지역 및 오브젝트 수와 같은 버킷의 세부 정보를 확인합니다.

b. 용량 제한 사용 막대를 봅니다. 사용량이 100% 또는 100%에 가까운 경우 제한을 늘리거나 일부 개체를 삭제하는 것이 좋습니다.

c. 필요에 따라 * Delete objects in bucket * 과 * Delete bucket * 을 선택합니다.

> 각 옵션을 선택할 때 나타나는 주의 사항에 각별히 주의하십시오. 자세한 내용은 다음을 참조하십시오.
>
> - "버킷의 모든 오브젝트를 삭제합니다"
> - "버킷을 삭제합니다" (버킷은 비어 있어야 함)

d. 필요에 따라 각 탭에서 버킷의 설정을 보거나 변경합니다.

- * S3 콘솔 * : 버킷에 대한 객체를 봅니다. 자세한 내용은 을 "S3 콘솔 사용"참조하십시오.
- * 버킷 옵션 * : 옵션 설정을 보거나 변경합니다. 버킷이 생성된 후에는 S3 Object Lock과 같은 일부 설정을 변경할 수 없습니다.
  - "버킷 일관성 관리"
  - "마지막 액세스 시간 업데이트"
  - "용량 제한"
  - "오브젝트 버전 관리"
  - "S3 오브젝트 잠금"
  - "기본 버킷 보유"
  - "교차 그리드 복제 관리" (테넌트에 대해 허용되는 경우)
- * 플랫폼 서비스 *"플랫폼 서비스 관리": (테넌트에 대해 허용되는 경우)
- * 버킷 액세스 * : 옵션 설정을 보거나 변경합니다. 특정 액세스 권한이 있어야 합니다.
  - "CORS(Cross-Origin Resource Sharing)"버킷의 버킷과 객체가 다른 도메인의 웹 애플리케이션에 액세스할 수 있도록 구성합니다.
  - "사용자 액세스를 제어합니다" S3 버킷과 해당 버킷의 오브젝트용.

버킷에 **ILM** 정책 태그를 적용합니다

오브젝트 스토리지 요구사항에 따라 버킷에 적용할 ILM 정책 태그를 선택합니다.

ILM 정책은 오브젝트 데이터의 저장 위치와 일정 기간 후에 삭제되는지 여부를 제어합니다. 그리드 관리자는 ILM 정책을 만들고 활성 정책을 여러 개 사용할 때 ILM 정책 태그에 할당합니다.

> 버킷의 정책 태그를 자주 재할당하지 마십시오. 그렇지 않으면 성능 문제가 발생할 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "루트 액세스, 모든 버킷 관리 또는 모든 버킷 보기 권한"있습니다. 이러한 권한은 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

단계

1. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.

   Bucket 페이지가 나타납니다. 필요에 따라 모든 열을 기준으로 정보를 정렬하거나 목록 앞뒤에 페이지를 표시할 수 있습니다.

2. ILM 정책 태그를 할당할 버킷의 이름을 선택합니다.

   이미 태그가 할당된 버킷의 ILM 정책 태그 할당을 변경할 수도 있습니다.

   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. Bucket options 탭에서 ILM 정책 태그 아코디언을 확장합니다. 이 아코디언은 그리드 관리자가 사용자 지정 정책 태그를 사용하도록 설정한 경우에만 나타납니다.
4. 각 정책 태그에 대한 설명을 읽고 버킷에 적용할 태그를 결정합니다.

   버킷의 ILM 정책 태그를 변경하면 버킷의 모든 오브젝트에 대한 ILM 재평가가 트리거됩니다. 새 정책에 따라 제한된 시간 동안 오브젝트를 유지하는 경우 이전 오브젝트는 삭제됩니다.

5. 버킷에 할당할 태그의 라디오 버튼을 선택합니다.
6. 변경 내용 저장 * 을 선택합니다. 새 S3 버킷 태그는 키와 ILM 정책 태그 이름의 값을 사용하여 버킷에 `NTAP-SG-ILM-BUCKET-TAG` 설정됩니다.

   S3 애플리케이션이 실수로 새 버킷 태그를 무시하거나 삭제하지 않도록 하십시오. 새 TagSet를 버킷에 적용할 때 이 태그를 생략하면 버킷의 객체가 기본 ILM 정책에 대해 평가되는 것으로 되돌아갑니다.

   ILM 정책 태그가 검증된 테넌트 관리자 또는 테넌트 관리자 API만 사용하여 ILM 정책 태그를 설정하고 수정합니다. S3 PutBucketTagging API 또는 S3 DeleteBucketTagging API를 사용하여 ILM 정책 태그를 수정하지 마십시오 `NTAP-SG-ILM-BUCKET-TAG`.

   버킷에 할당된 정책 태그를 변경하면 새로운 ILM 정책을 사용하여 오브젝트를 재평가하는 동안 성능에 일시적으로 영향을 미칩니다.

버킷 정책을 관리합니다

S3 버킷 및 해당 버킷의 오브젝트에 대한 사용자 액세스를 제어할 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "루트 액세스 권한"있습니다. 모든 버킷 보기 및 모든 버킷 관리 권한만 볼 수 있습니다.
- 필요한 수의 스토리지 노드 및 사이트를 사용할 수 있는지 확인했습니다. 사이트 내에서 두 개 이상의 스토리지 노드를 사용할 수 없거나 사이트를 사용할 수 없는 경우 이러한 설정을 변경하지 못할 수 있습니다.

단계

1. Bucket * 을 선택한 다음 관리하려는 버킷을 선택합니다.
2. 버킷 세부 정보 페이지에서 * Bucket access * > * Bucket policy * 를 선택합니다.
3. 다음 중 하나를 수행합니다.
   - Enable policy * 확인란을 선택하여 버킷 정책을 입력합니다. 그런 다음 유효한 JSON 형식 문자열을 입력하십시오.

     각 버킷 정책의 크기 제한은 20,480바이트입니다.
   - 문자열을 편집하여 기존 정책을 수정합니다.
   - 정책 활성화 * 를 선택 취소하여 정책을 비활성화합니다.

언어 구문 및 예제를 포함한 버킷 정책에 대한 자세한 내용은 를 참조하십시오"버킷 정책의 예".

버킷 일관성 관리

일관성 값을 사용하여 버킷 설정 변경의 가용성을 지정하고 버킷 내의 오브젝트 가용성과 서로 다른 스토리지 노드 및 사이트에서 이러한 오브젝트의 일관성 간에 균형을 유지할 수 있습니다. 정합성 보장 값을 기본값과 다르게 변경하여 클라이언트 애플리케이션이 운영 요구사항을 충족할 수 있도록 할 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "모든 버킷 또는 루트 액세스 권한을 관리합니다"있습니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

버킷 일관성 지침

버킷 정합성 보장은 해당 S3 버킷 내의 오브젝트에 영향을 주는 클라이언트 애플리케이션의 정합성을 결정하는 데 사용됩니다. 일반적으로 버킷에는 * Read-after-new-write * 일관성을 사용해야 합니다.

버킷 일관성을 변경합니다

Read-after-new-write * 일관성이 클라이언트 애플리케이션의 요구 사항을 충족하지 않는 경우 버킷 일관성을 설정하거나 헤더를 사용하여 일관성을 변경할 수 `Consistency-Control` 있습니다. `Consistency-Control`헤더가 버킷 일관성을 재정의합니다.

> 버킷의 일관성을 변경하면 변경 후 수집되는 객체만 수정된 설정을 충족할 수 있습니다.

단계

1. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. 테이블에서 버킷 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.
3. Bucket options * 탭에서 ** 아코디언을 선택합니다.
4. 이 버킷의 객체에서 수행되는 작업에 대한 일관성을 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 필요한 경우에만 사용하십시오(예: 거의 읽지 않는 로그 값이 포함된 버킷의 경우 또는 존재하지 않는 키의 헤드 또는 GET 작업의 경우). S3 FabricPool 버킷은 지원되지 않습니다.

5. 변경 내용 저장 * 을 선택합니다.

버킷 설정을 변경하면 어떻게 됩니까

버킷에는 버킷 및 해당 버킷 내의 객체의 동작에 영향을 주는 여러 설정이 있습니다.

다음 버킷 설정은 기본적으로 * 강한 * 일관성을 사용합니다. 사이트 내에서 두 개 이상의 스토리지 노드를 사용할 수 없거나 사이트를 사용할 수 없는 경우 이러한 설정을 변경하지 못할 수 있습니다.

- "배경이 비어 있는 버킷 삭제"
- "마지막 액세스 시간입니다"
- "버킷 수명 주기"
- "버킷 정책"
- "버킷 태그 지정"
- "버킷 버전 관리"
- "S3 오브젝트 잠금"
- "버킷 암호화"

버킷 버전 관리, S3 오브젝트 잠금 및 버킷 암호화에 대한 정합성 보장 값을 강력하게 일치하지 않는 값으로 설정할 수 없습니다.

다음 버킷 설정은 강력한 일관성을 사용하지 않으며 변경에 대한 가용성이 높습니다. 이러한 설정을 변경하는 데 시간이 걸릴 수 있습니다.

- "플랫폼 서비스 구성: 알림, 복제 또는 검색 통합"
- "CORS 구성"
- 버킷 일관성을 변경합니다

버킷 설정 변경 시 사용되는 기본 일관성이 클라이언트 애플리케이션의 요구 사항을 충족하지 않는 경우 의 헤더를 "S3 REST API"사용하거나 의 또는 `force` 옵션을 사용하여 `reducedConsistency` 일관성을 변경할 수 있습니다 `Consistency-Control`"테넌트 관리 API".

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 고급 필터 또는 참조 시간으로 * 마지막 액세스 시간 * 옵션을 사용하는 ILM 규칙을 하나 이상 포함하는 StorageGRID 시스템에만 적용됩니다. StorageGRID 시스템에 이러한 규칙이 포함되어 있지 않으면 이 지침을 무시할 수 있습니다. 자세한 내용은 을 "ILM 규칙에서 마지막 액세스 시간을 사용합니다" 참조하십시오.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "모든 버킷 또는 루트 액세스 권한을 관리합니다"있습니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

이 작업에 대해

- 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.

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
개체 또는 개체 버전을 나열하는 요청입니다	아니요	아니요	아니요	아니요
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. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. 테이블에서 버킷 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

3. Bucket options * 탭에서 * Last access time updates * 아코디언을 선택합니다.
4. 마지막 액세스 시간 업데이트를 사용하거나 사용하지 않도록 설정합니다.
5. 변경 내용 저장 * 을 선택합니다.

버킷의 오브젝트 버전 관리를 변경합니다

S3 테넌트를 사용하는 경우 S3 버킷의 버전 관리 상태를 변경할 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "모든 버킷 또는 루트 액세스 권한을 관리합니다"있습니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.
- 필요한 수의 스토리지 노드 및 사이트를 사용할 수 있는지 확인했습니다. 사이트 내에서 두 개 이상의 스토리지 노드를 사용할 수 없거나 사이트를 사용할 수 없는 경우 이러한 설정을 변경하지 못할 수 있습니다.

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

자세한 내용은 다음을 참조하십시오.

- "오브젝트 버전 관리"
- "S3 버전 오브젝트 ILM 규칙 및 정책(예 4)"
- "오브젝트 삭제 방법"

단계

1. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. 테이블에서 버킷 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

3. Bucket options * 탭에서 * Object Version * 아코디언을 선택합니다.
4. 이 버킷의 오브젝트에 대한 버전 관리 상태를 선택합니다.

   오브젝트 버전 관리는 교차 그리드 복제에 사용되는 버킷에 대해 활성화된 상태를 유지해야 합니다. 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.

S3 오브젝트 잠금을 사용하여 오브젝트를 보존합니다

버킷과 오브젝트가 보존 규정 요구사항을 준수해야 하는 경우 S3 오브젝트 잠금을 사용할 수 있습니다.

그리드 관리자는 귀하에게 S3 오브젝트 잠금의 특정 기능을 사용할 수 있는 권한을 부여해야 합니다.

S3 오브젝트 잠금이란 무엇입니까**?**

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 설정이 활성화된 경우 S3 테넌트 계정에서 S3 오브젝트 잠금이

활성화되어 있거나 사용되지 않고 버킷을 생성할 수 있습니다. 버킷에 S3 오브젝트 잠금이 활성화된 경우 버킷 버전 관리가 필요하며 자동으로 활성화됩니다.

*S3 오브젝트 잠금이 없는 버킷은 보존 설정이 지정되지 않은 오브젝트만 가질 수 있습니다. 수집된 객체에는 보존 설정이 없습니다.

- S3 오브젝트 잠금이 있는 버킷은 S3 클라이언트 애플리케이션에 지정된 보존 설정이 있거나 없는 객체를 포함할 수 있습니다. 수집된 일부 객체에는 보존 설정이 있습니다.
- S3 오브젝트 잠금 및 기본 보존이 구성된 버킷 * 은 보존 설정이 지정된 객체와 보존 설정이 없는 새 객체를 업로드할 수 있습니다. 개체 수준에서 보존 설정이 구성되지 않았기 때문에 새 개체는 기본 설정을 사용합니다.

기본적으로 보존이 구성되면 새로 수집된 모든 객체에 보존 설정이 적용됩니다. 개체 보존 설정이 없는 기존 개체는 영향을 받지 않습니다.

보존 모드

StorageGRID S3 오브젝트 잠금 기능은 두 가지 보존 모드를 지원하여 오브젝트에 다양한 보호 수준을 적용합니다. 이러한 모드는 Amazon S3 보존 모드에 해당합니다.

- 규정 준수 모드:
  - 보존 기한 에 도달할 때까지 개체를 삭제할 수 없습니다.
  - 오브젝트의 보존 기한 을 늘릴 수 있지만 줄일 수는 없습니다.
  - 개체의 보존 기한 은 해당 날짜에 도달할 때까지 제거할 수 없습니다.
- 거버넌스 모드:
  - 특수 권한이 있는 사용자는 요청에서 우회 헤더를 사용하여 특정 보존 설정을 수정할 수 있습니다.
  - 이러한 사용자는 보존 기한이 되기 전에 개체 버전을 삭제할 수 있습니다.
  - 이러한 사용자는 개체의 보존 기간(Retain-until-date)을 증가, 감소 또는 제거할 수 있습니다.

개체 버전에 대한 보존 설정입니다

버킷이 S3 오브젝트 잠금이 설정된 상태로 생성된 경우 사용자는 S3 클라이언트 애플리케이션을 사용하여 버킷에 추가되는 각 오브젝트에 대해 다음 보존 설정을 선택적으로 지정할 수 있습니다.

- * 보존 모드 *: 규정 준수 또는 거버넌스 중 하나입니다.
- * Retain-until-date *: 개체 버전의 Retain-until-date가 미래인 경우 개체를 검색할 수 있지만 삭제할 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.

  개체가 법적 보류 중인 경우 보존 모드에 관계없이 개체를 삭제할 수 없습니다.

개체 설정에 대한 자세한 내용은 을 참조하십시오"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다".

버킷을 위한 기본 보존 설정입니다

버킷이 S3 오브젝트 잠금이 활성화된 상태로 생성된 경우 사용자는 버킷에 대해 다음 기본 설정을 선택적으로 지정할 수

있습니다.

- * 기본 보존 모드 *: 규정 준수 또는 거버넌스 중 하나입니다.
- * 기본 보존 기간 *: 이 버킷에 추가된 새 오브젝트 버전이 추가되는 날부터 보존되어야 하는 기간입니다.

기본 버킷 설정은 고유한 보존 설정이 없는 새 오브젝트에만 적용됩니다. 이러한 기본 설정을 추가하거나 변경할 때 기존 버킷 개체는 영향을 받지 않습니다.

"S3 버킷을 생성합니다"및 을 "S3 오브젝트 잠금 기본 보존 업데이트"참조하십시오.

S3 오브젝트 잠금 작업

그리드 관리자 및 테넌트 사용자를 위한 다음 목록에는 S3 오브젝트 잠금 기능을 사용하기 위한 상위 수준의 작업이 포함되어 있습니다.

그리드 관리자

- 전체 StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정을 사용합니다.
- 정보 수명 주기 관리(ILM) 정책이 _ 준수되는지 확인합니다. 즉, 이 정책이 을"S3 오브젝트 잠금이 설정된 버킷 요구사항"(를) 충족하는지 확인합니다.
- 필요에 따라 테넌트가 규정 준수를 보존 모드로 사용할 수 있도록 허용합니다. 그렇지 않으면 거버넌스 모드만 허용됩니다.
- 필요에 따라 테넌트의 최대 보존 기간을 설정합니다.

테넌트 사용자입니다

- S3 오브젝트 잠금을 통해 버킷 및 오브젝트에 대한 고려 사항을 검토하십시오.
- 필요한 경우 그리드 관리자에게 문의하여 글로벌 S3 오브젝트 잠금 설정을 활성화하고 권한을 설정합니다.
- S3 오브젝트 잠금이 설정된 상태로 버킷을 생성합니다.
- 필요에 따라 버킷의 기본 보존 설정을 구성합니다.
  - 기본 보존 모드: 그리드 관리자가 허용하는 경우 거버넌스 또는 규정 준수
  - 기본 보존 기간: 그리드 관리자가 설정한 최대 보존 기간 이하여야 합니다.
- S3 클라이언트 애플리케이션을 사용하여 오브젝트를 추가하고 필요에 따라 오브젝트별 보존을 설정합니다.
  - 보존 모드. 거버넌스 또는 규정 준수(그리드 관리자가 허용하는 경우)
  - 보관 종료 날짜: 그리드 관리자가 설정한 최대 보존 기간 이하여야 합니다.

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.
- S3 오브젝트 잠금을 사용하려는 경우 버킷을 생성할 때 S3 오브젝트 잠금을 활성화해야 합니다. 기존 버킷에 S3 오브젝트 잠금을 설정할 수 없습니다.
- 버킷에 대해 S3 오브젝트 잠금이 활성화된 경우 StorageGRID는 해당 버킷의 버전 관리를 자동으로 활성화합니다. 버킷의 S3 오브젝트 잠금을 비활성화하거나 버전 관리를 일시 중단할 수 없습니다.
- 필요에 따라 테넌트 관리자, 테넌트 관리 API 또는 S3 REST API를 사용하여 각 버킷의 기본 보존 모드 및 보존 기간을 지정할 수 있습니다. 버킷의 기본 보존 설정은 고유한 보존 설정이 없는 버킷에 추가된 새 오브젝트에만

적용됩니다. 이 기본 설정은 업로드할 때 각 개체 버전에 대해 보존 모드 및 보존 종료 날짜를 지정하여 재정의할 수 있습니다.

- S3 오브젝트 잠금이 설정된 버킷에 대해 버킷 라이프사이클 구성이 지원됩니다.
- S3 오브젝트 잠금이 설정된 버킷에는 CloudMirror 복제가 지원되지 않습니다.

S3 오브젝트 잠금이 설정된 버킷의 오브젝트 요구사항

- 개체 버전을 보호하려면 버킷의 기본 보존 설정을 지정하거나 각 오브젝트 버전에 대한 보존 설정을 지정할 수 있습니다. 오브젝트 레벨의 보존 설정은 S3 클라이언트 애플리케이션 또는 S3 REST API를 사용하여 지정할 수 있습니다.
- 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 단계를 거칩니다.

1. * 오브젝트 수집 *

   오브젝트 버전이 S3 오브젝트 잠금이 설정된 버킷에 추가되면 보존 설정이 다음과 같이 적용됩니다.

   - 개체에 대한 보존 설정이 지정된 경우 개체 수준 설정이 적용됩니다. 기본 버킷 설정은 무시됩니다.
   - 개체에 대해 보존 설정을 지정하지 않으면 기본 버킷 설정이 적용됩니다(있는 경우).
   - 오브젝트 또는 버킷에 대해 보존 설정을 지정하지 않으면 S3 오브젝트 잠금으로 오브젝트가 보호되지 않습니다.

   보존 설정이 적용되는 경우 오브젝트와 S3 사용자 정의 메타데이터는 모두 보호됩니다.

2. * 개체 보존 및 삭제 *

   StorageGRID는 지정된 보존 기간 동안 보호된 각 개체의 복사본을 여러 개 저장합니다. 오브젝트 복사본 및 스토리지 위치의 정확한 수와 유형은 활성 ILM 정책의 규정 준수 규칙에 따라 결정됩니다. 보존 기한이 되기 전에 보호된 개체를 삭제할 수 있는지 여부는 보존 모드에 따라 다릅니다.

   - 개체가 법적 보류 중인 경우 보존 모드에 관계없이 개체를 삭제할 수 없습니다.

레거시 준수 버킷을 계속 관리할 수 있습니까?

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 을 "NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"참조하십시오.

S3 오브젝트 잠금 기본 보존 업데이트

버킷을 생성할 때 S3 오브젝트 잠금을 설정한 경우 버킷을 편집하여 기본 보존 설정을 변경할 수 있습니다. 기본 보존을 사용하거나 사용하지 않도록 설정하고 기본 보존 모드 및 보존 기간을 설정할 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "모든 버킷 또는 루트 액세스 권한을 관리합니다"있습니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.
- S3 오브젝트 잠금은 StorageGRID 시스템에 대해 전역적으로 활성화되며 버킷을 생성할 때 S3 오브젝트 잠금을 활성화했습니다. 을 "S3 오브젝트 잠금을 사용하여 오브젝트를 보존합니다"참조하십시오.

단계

1. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
2. 테이블에서 버킷 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

3. Bucket options * 탭에서 * S3 Object Lock * 아코디언을 선택합니다.
4. 이 버킷에 대해 * 기본 보존 * 을 활성화 또는 비활성화할 수 있습니다(선택 사항).

   이 설정의 변경 사항은 버킷에 이미 있는 오브젝트 또는 자체 보존 기간이 있을 수 있는 오브젝트에는 적용되지 않습니다.

5. 기본 보존 * 이 활성화된 경우 버킷에 대한 * 기본 보존 모드 * 를 지정합니다.

기본 보존 모드	설명
기대치를 설정합니다	• 있는 사용자는 `s3:BypassGovernanceRetention`권한이 요청 헤더를 사용하여 보존 설정을 무시할 수 `x-amz-bypass-governance-retention: true` 있습니다. • 이러한 사용자는 보존 기한이 되기 전에 개체 버전을 삭제할 수 있습니다. • 이러한 사용자는 개체의 보존 기간(Retain-until-date)을 증가, 감소 또는 제거할 수 있습니다.
규정 준수	• 보존 기한 에 도달할 때까지 개체를 삭제할 수 없습니다. • 오브젝트의 보존 기한 을 늘릴 수 있지만 줄일 수는 없습니다. • 개체의 보존 기한 은 해당 날짜에 도달할 때까지 제거할 수 없습니다. ◦ 참고 *: 그리드 관리자가 규정 준수 모드를 사용할 수 있도록 허용해야 합니다.

6. 기본 보존 * 이 활성화된 경우 버킷의 * 기본 보존 기간 * 을 지정합니다.

   기본 보존 기간 * 은 이 버킷에 추가된 새 오브젝트를 인제스트할 시간부터 보존 기간을 나타냅니다. 그리드 관리자가 설정한 테넌트의 최대 보존 기간보다 작거나 같은 값을 지정하십시오.

   그리드 관리자가 테넌트를 생성할 때 1일에서 100년 사이의 값을 지정할 수 있는 _MAXIMUM_RETENTION 기간이 설정됩니다. _default_retention 기간을 설정하면 최대 보존 기간에 설정된 값을 초과할 수 없습니다. 필요한 경우 그리드 관리자에게 최대 보존 기간을 늘리거나 줄이도록 요청하십시오.

7. 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.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- GET CORS 구성 요청의 경우 이 있는 사용자 그룹에 속해 "모든 버킷을 관리하거나 모든 버킷을 봅니다"있습니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.
- PUT CORS 구성 요청의 경우 이 있는 사용자 그룹에 속해 "모든 버킷 사용 권한을 관리합니다"있습니다. 이 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.
- 는 "루트 액세스 권한"모든 CORS 구성 요청에 대한 액세스를 제공합니다.

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, 이라는 S3 버킷을 사용하여 그래픽을 저장한다고 가정해 `Images` 보겠습니다. 버킷에 대한 CORS를 구성하면 `Images` 해당 버킷의 이미지가 웹사이트에 표시되도록 할 수 `http://www.example.com` 있습니다.

버킷에 대해 CORS를 활성화합니다

단계

1. 텍스트 편집기를 사용하여 필요한 XML을 만듭니다. 이 예에서는 S3 버킷에 대해 CORS를 활성화하는 데 사용되는 XML을 보여 줍니다. 주요 내용은 다음과 같습니다.
   - 모든 도메인이 버킷으로 GET 요청을 보낼 수 있도록 허용합니다
   - 도메인에서만 GET, POST 및 삭제 요청을 보낼 수 있습니다 `http://www.example.com`
   - 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) 설명서: Amazon Simple Storage Service 사용 설명서".

2. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.
3. 테이블에서 버킷 이름을 선택합니다.

   버킷 세부 정보 페이지가 나타납니다.

4. Bucket access * 탭에서 * CORS(Cross-Origin Resource Sharing) * 아코디언을 선택합니다.
5. CORS * 활성화 확인란을 선택합니다.
6. 텍스트 상자에 CORS 구성 XML을 붙여 넣습니다.
7. 변경 내용 저장 * 을 선택합니다.

CORS 설정을 수정합니다

단계

1. 텍스트 상자에서 CORS 구성 XML을 업데이트하거나 다시 시작하려면 * Clear * 를 선택합니다.
2. 변경 내용 저장 * 을 선택합니다.

CORS 설정을 비활성화합니다

단계

1. CORS * 활성화 확인란의 선택을 취소합니다.
2. 변경 내용 저장 * 을 선택합니다.

버킷에서 오브젝트를 삭제합니다

Tenant Manager를 사용하여 하나 이상의 버킷에서 오브젝트를 삭제할 수 있습니다.

고려 사항 및 요구 사항

이 단계를 수행하기 전에 다음 사항을 확인하십시오.

- 버킷에서 오브젝트를 삭제하면 StorageGRID은 StorageGRID 시스템의 모든 노드와 사이트에서 선택한 각 버킷의 모든 오브젝트 및 모든 오브젝트 버전을 영구적으로 제거합니다. StorageGRID 는 관련된 개체 메타데이터도 제거합니다. 이 정보를 복구할 수 없습니다.
- 오브젝트, 오브젝트 복사본 및 동시 작업의 수에 따라 버킷의 모든 오브젝트를 삭제하는 데 몇 분, 일 또는 몇 주가 걸릴 수 있습니다.
- 버킷이 있는 경우 "S3 오브젝트 잠금이 설정되었습니다"_years_에 대해 * 오브젝트 삭제: 읽기 전용 * 상태로 남아 있을 수 있습니다.

  S3 오브젝트 잠금을 사용하는 버킷은 모든 오브젝트에 대한 보존 날짜가 도달하고 법적 보관에 도달할 때까지 * 오브젝트 삭제: 읽기 전용 * 상태로 유지됩니다.

- 오브젝트가 삭제될 때 버킷의 상태는 * 오브젝트 삭제: 읽기 전용 * 입니다. 이 상태에서는 버킷에 새 오브젝트를 추가할 수 없습니다.
- 모든 오브젝트가 삭제된 경우 버킷은 읽기 전용 상태로 유지됩니다. 다음 중 하나를 수행할 수 있습니다.

- 쓰기 모드로 버킷을 되돌리십시오. 새 오브젝트에 이 버킷을 재사용하십시오
- 버킷을 삭제합니다
- 나중에 사용할 수 있도록 버킷을 읽기 전용 모드로 유지합니다

- 버킷에 오브젝트 버전 관리가 활성화된 경우 버킷 작업에서 오브젝트 삭제 작업을 사용하여 StorageGRID 11.8 이상에서 생성된 삭제 표식을 제거할 수 있습니다.
- 버킷에 개체 버전 관리가 활성화된 경우 오브젝트 삭제 작업은 StorageGRID 11.7 이하에서 생성된 삭제 표식을 제거하지 않습니다. 에서 버킷의 오브젝트 삭제에 대한 정보를 "S3 버전 오브젝트 삭제 방법"참조하십시오.
- 을 사용하는 경우 "교차 그리드 복제"다음 사항에 유의하십시오.
  - 이 옵션을 사용해도 다른 그리드의 버킷에서 오브젝트가 삭제되지 않습니다.
  - 소스 버킷에 대해 이 옵션을 선택하면 다른 그리드의 대상 버킷에 오브젝트를 추가하면 * 크로스 그리드 복제 실패 * 경고가 트리거됩니다. 보장하지 못할 경우, 모든 버킷 오브젝트를 삭제하기 전에 다른 그리드의 버킷에 객체를 추가하지 "크로스 그리드 복제를 비활성화합니다"않습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "루트 액세스 권한"있습니다. 이 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.

단계

1. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.

   Bucket 페이지가 나타나고 기존의 모든 S3 버킷을 표시합니다.

2. 특정 버킷의 * 작업 * 메뉴 또는 세부 정보 페이지를 사용합니다.

   작업 메뉴

   a. 오브젝트를 삭제할 각 버킷의 확인란을 선택합니다.

   b. Actions * > * Delete objects in bucket * 을 선택합니다.

   세부 정보 페이지

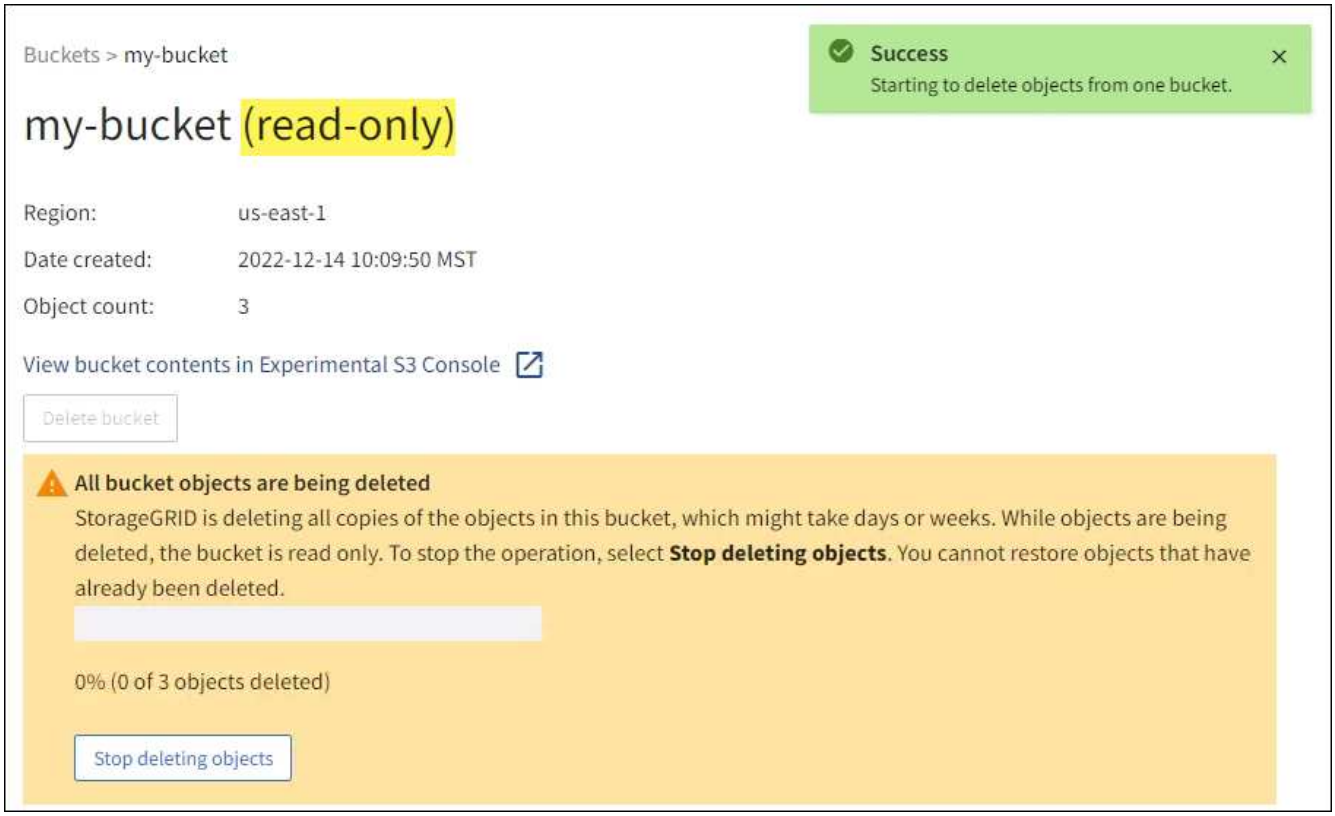
   a. 버킷 이름을 선택하여 세부 정보를 표시합니다.

   b. 버킷에서 오브젝트 삭제 * 를 선택합니다.

3. 확인 대화 상자가 나타나면 세부 정보를 검토하고 * 예 * 를 입력한 다음 * 확인 * 을 선택합니다.
4. 삭제 작업이 시작될 때까지 기다립니다.

   몇 분 후:

   - 버킷 세부 정보 페이지에 노란색 상태 배너가 나타납니다. 진행률 표시줄은 삭제된 개체의 비율을 나타냅니다.
   - * (읽기 전용) * 버킷 세부 정보 페이지에서 버킷 이름 뒤에 나타납니다.
   - * (오브젝트 삭제: 읽기 전용) * 버킷 페이지의 버킷 이름 옆에 표시됩니다.

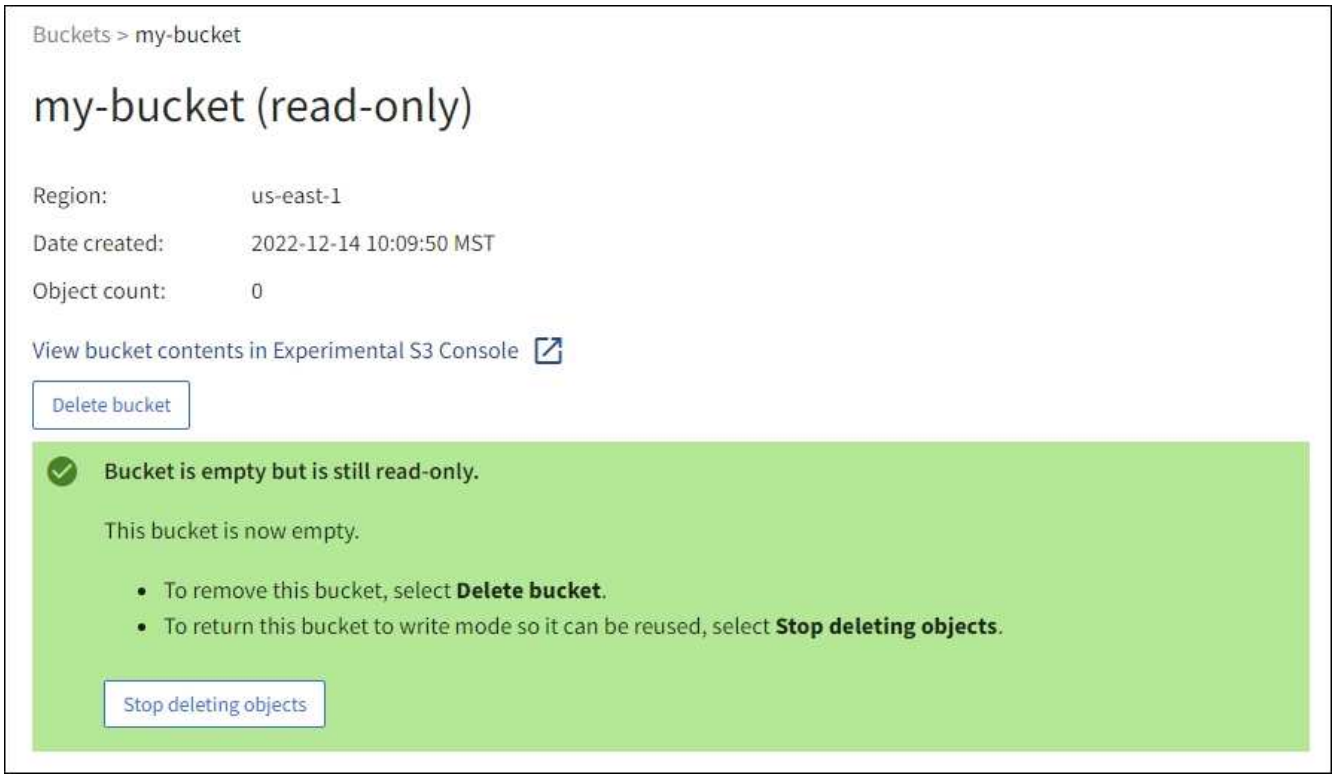


5. 작업이 실행되는 동안 필요에 따라 * 개체 삭제 중지 * 를 선택하여 프로세스를 중단합니다. 그런 다음 필요에 따라 * 버킷 안의 오브젝트 삭제 * 를 선택하여 프로세스를 재개합니다.

   오브젝트 삭제 중지 * 를 선택하면 버킷이 쓰기 모드로 돌아가지만 삭제된 오브젝트는 액세스하거나 복구할 수 없습니다.

6. 작업이 완료될 때까지 기다립니다.

   버킷이 비어 있으면 상태 배너가 업데이트되지만 버킷은 읽기 전용으로 유지됩니다.



7. 다음 중 하나를 수행합니다.
   - 버킷을 읽기 전용 모드로 유지하려면 페이지를 종료하십시오. 예를 들어, 빈 버킷을 읽기 전용 모드로 유지하여 나중에 사용할 수 있도록 버킷 이름을 예약할 수 있습니다.
   - 버킷을 삭제합니다. 단일 버킷을 삭제하거나 버킷 페이지를 반환하려면 * 버킷 삭제 * 를 선택하고 둘 이상의 버킷을 제거하려면 * 작업 * > * 삭제 * 버킷을 선택할 수 있습니다.

     모든 오브젝트를 삭제한 후 버전이 있는 버킷을 삭제할 수 없는 경우 삭제 마커가 남아 있을 수 있습니다. 버킷을 삭제하려면 나머지 삭제 마커를 모두 제거해야 합니다.

   - 쓰기 모드로 버킷을 되돌리십시오. 그리고 필요에 따라 새 오브젝트에 버킷을 다시 사용할 수 있습니다. 단일 버킷에 대해 * 오브젝트 삭제 중지 * 를 선택하거나 버킷 페이지로 돌아가서 * 작업 * > * 오브젝트 삭제 중지 * 를 선택하여 둘 이상의 버킷에 대해 삭제할 수 있습니다.

S3 버킷을 삭제합니다

테넌트 관리자를 사용하여 비어 있는 하나 이상의 S3 버킷을 삭제할 수 있습니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "모든 버킷 또는 루트 액세스 권한을 관리합니다"있습니다. 이러한 권한은 그룹 또는 버킷 정책의 사용 권한 설정을 재정의합니다.
- 삭제할 버킷이 비어 있습니다. 삭제하려는 버킷이 _NOT_EMIVE인 경우"버킷에서 오브젝트를 삭제합니다"

이 작업에 대해

다음 지침은 Tenant Manager를 사용하여 S3 버킷을 삭제하는 방법을 설명합니다. 또는 를 사용하여 S3 버킷을 삭제할 수도 "테넌트 관리 API""S3 REST API"있습니다.

S3 버킷에 오브젝트, 비현재 오브젝트 버전이 포함되어 있거나 마커를 삭제할 수 없습니다. S3 버전 개체가 삭제되는 방법에 대한 자세한 내용은 을 참조하십시오"오브젝트 삭제 방법".

단계

1. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 스토리지(S3) * > * 버킷 * 을 선택합니다.

   Bucket 페이지가 나타나고 기존의 모든 S3 버킷을 표시합니다.

2. 특정 버킷의 * 작업 * 메뉴 또는 세부 정보 페이지를 사용합니다.

   작업 메뉴

   a. 삭제할 각 버킷의 확인란을 선택합니다.

   b. Actions * > * Delete Bucket * 을 선택합니다.

   세부 정보 페이지

   a. 버킷 이름을 선택하여 세부 정보를 표시합니다.

   b. 버킷 삭제 * 를 선택합니다.

3. 확인 대화 상자가 나타나면 * 예 * 를 선택합니다.

   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 해야 "버킷의 모든 오브젝트와 삭제 표식을 삭제합니다"합니다.

S3 콘솔 사용

S3 콘솔을 사용하여 S3 버킷의 오브젝트를 보고 관리할 수 있다.

S3 콘솔을 통해 다음을 수행할 수 있습니다.

- 업로드, 다운로드, 이름 바꾸기, 복사, 이동, 개체를 삭제합니다
- 개체 버전을 보고, 되돌리고, 다운로드하고, 삭제합니다
- 접두사로 오브젝트를 검색합니다
- 오브젝트 태그 관리
- 개체 메타데이터를 봅니다
- 보기, 만들기, 이름 바꾸기, 복사, 이동, 폴더를 삭제합니다

S3 콘솔은 가장 일반적인 경우에 향상된 사용자 환경을 제공합니다. 모든 상황에서 CLI 또는 API 작업을 대체하도록 설계되지 않았습니다.

S3 콘솔을 사용할 때 작업 시간이 너무 오래 걸리는 경우(예: 분 또는 시간) 다음을 고려하십시오.

- 선택한 개체의 수를 줄입니다
- 비그래픽(API 또는 CLI) 방법을 사용하여 데이터에 액세스합니다

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 개체를 관리하려면 루트 액세스 권한이 있는 사용자 그룹에 속해 있어야 합니다. 또는 S3 콘솔 사용 탭 권한 및 모든 버킷 보기 권한 또는 모든 버킷 관리 권한이 있는 사용자 그룹에 속하게 됩니다. 을 "테넌트 관리 권한"참조하십시오.
- 사용자에 대해 S3 그룹 또는 버킷 정책이 구성되었습니다. 을 "버킷 및 그룹 액세스 정책을 사용합니다 "참조하십시오.
- 사용자의 액세스 키 ID와 비밀 액세스 키를 알고 있습니다. 필요한 경우 이 정보가 포함된 파일이 있을 수도 `.csv` 있습니다. 를 "액세스 키 생성에 대한 지침"참조하십시오.

단계

1. 스토리지 * > * Bucket * > * *bucket name* * 를 선택합니다.
2. S3 콘솔 탭을 선택합니다.
3. 액세스 키 ID와 비밀 액세스 키를 필드에 붙여 넣습니다. 그렇지 않으면 * Upload access keys * 를 선택하고 `.csv` 파일을 선택합니다.
4. 로그인 * 을 선택합니다.
5. 버킷 객체의 테이블이 나타납니다. 필요에 따라 개체를 관리할 수 있습니다.

추가 정보

- * 접두사로 검색 *: 접두사 검색 기능은 현재 폴더와 관련된 특정 단어로 시작하는 오브젝트만 검색합니다. 검색에는 다른 위치에 단어가 포함된 개체가 포함되지 않습니다. 이 규칙은 폴더 내의 개체에도 적용됩니다. 예를 들어, 에 대한 검색은 `folder1/folder2/somefile-` 폴더 내에 있는 객체를 반환하고 `folder1/folder2/` 단어로 시작합니다 `somefile-`.
- * 드래그 앤 드롭 * : 컴퓨터의 파일 관리자에서 S3 콘솔로 파일을 끌어다 놓을 수 있습니다. 그러나 폴더를 업로드할 수는 없습니다.
- * 폴더에 대한 작업 * : 폴더를 이동, 복사 또는 이름 바꾸면 폴더의 모든 개체가 한 번에 하나씩 업데이트되어 시간이 걸릴 수 있습니다.
- *버킷 버전 관리가 비활성화된 경우 영구 삭제 *: 버전 관리가 비활성화된 상태로 버킷의 오브젝트를 덮어쓰거나 삭제하면 작업이 영구적입니다. 을 "버킷의 오브젝트 버전 관리를 변경합니다"참조하십시오.

S3 플랫폼 서비스 관리

S3 플랫폼 서비스

플랫폼 서비스 개요 및 고려 사항

플랫폼 서비스를 구현하기 전에 이러한 서비스 사용에 대한 개요 및 고려 사항을 검토하십시오.

S3에 대한 자세한 내용은 을 "S3 REST API 사용"참조하십시오.

플랫폼 서비스 개요

StorageGRID 플랫폼 서비스를 사용하면 S3 오브젝트 및 오브젝트 메타데이터의 이벤트 알림과 복사본을 외부 대상에 보낼 수 있으므로 하이브리드 클라우드 전략을 구현할 수 있습니다.

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, 및 "알림"StorageGRID S3 버킷에서 특정 오브젝트를 Amazon S3(Simple Storage Service)에 미러링하는 동시에 각 오브젝트에 대한 알림을 타사 모니터링 애플리케이션에 전송하여 AWS 비용을 추적할 수 있도록 할 "CloudMirror 서비스"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 또는 를 사용하여 구성한 외부 끝점과 통신합니다."테넌트 관리자""테넌트 관리 API" 각 엔드포인트는 StorageGRID S3 버킷, Amazon Web Services 버킷, Amazon SNS 주제 또는 로컬이나 AWS 등에 호스팅된 Elasticsearch 클러스터와 같은 외부 대상을 나타냅니다.

외부 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.

- 키가 로 시작하는 모든 오브젝트를 Amazon S3 버킷에 복제하려면 복제 구성을 소스 버킷에 추가해야 합니다. `/images`
- 이러한 객체가 버킷에 저장될 때 알림을 보내려면 알림 구성을 추가해야 합니다.
- 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**	을 참조하십시오
CloudMirror 복제	• GetBucketReplication 을 참조하십시오 • PutBucketReplication을 참조하십시오	• "CloudMirror 복제" • "버킷 작업"
알림	• GetBuckNotificationConfiguration 을 참조하십시오 • PutBucketNotificationConfiguration을 참조하십시오	• "알림" • "버킷 작업"
검색 통합	• Bucket 메타데이터 알림 구성 가져오기 • Put Bucket 메타데이터 알림 구성	• "검색 통합" • "StorageGRID 사용자 정의 작업"

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 Amazon Simple Notification Service의 삭제 동작과 일치시키기 위해 StorageGRID ILM 규칙으로 인해 소스 버킷의 오브젝트가 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
Kafka 엔드포인트 사용	Kafka 엔드포인트의 경우 상호 TLS는 지원되지 않습니다. 그 결과, Kafka 브로커 구성에서 로 설정한 `required` 경우 `ssl.client.auth` Kafka 엔드포인트 구성 문제가 발생할 수 있습니다. Kafka 엔드포인트 인증은 다음과 같은 인증 유형을 사용합니다. 이러한 유형은 Amazon SNS와 같은 다른 엔드포인트의 인증에 사용되는 유형과는 다르며 사용자 이름 및 암호 자격 증명이 필요합니다. • SASL/일반 • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 • 참고: * 구성된 스토리지 프록시 설정은 Kafka 플랫폼 서비스 엔드포인트에 적용되지 않습니다.

CloudMirror 복제 서비스 사용에 대한 고려 사항

고려 사항	세부 정보
복제 상태입니다	StorageGRID는 헤더를 지원하지 `x-amz-replication-status` 않습니다.
개체 크기	CloudMirror 복제 서비스를 통해 대상 버킷에 복제할 수 있는 개체의 최대 크기는 5TiB이며, 이는 maximum_supported_object 크기와 같습니다. • 참고 *: 단일 PutObject 작업의 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 PutObjectTagging 또는 DeleteObjectTagging 요청을 복제하지 않습니다. 소스 및 대상의 버전 ID는 관련이 없으므로 특정 버전 ID에 대한 태그 업데이트를 복제할 수 없습니다. 반면, CloudMirror 서비스는 버전 ID를 지정하지 않는 PutObjectTagging 요청이나 DeleteObjectTagging 요청을 복제합니다. 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.

고려 사항	세부 정보
멀티 파트 업로드 및 `ETag` 값	여러 부분 업로드를 사용하여 업로드한 개체를 미러링할 때 CloudMirror 서비스는 해당 파트를 보존하지 않습니다. 따라서 `ETag` 대칭 복사된 개체의 값은 `ETag` 원래 개체의 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 할 때 SSE-C 요청 헤더를 포함하면 작업이 실패합니다.
S3 오브젝트 잠금이 활성화된 버킷	S3 오브젝트 잠금이 활성화된 소스 또는 대상 버킷에는 복제가 지원되지 않습니다.

CloudMirror 복제 서비스를 이해합니다

StorageGRID가 버킷에 추가된 지정된 오브젝트를 하나 이상의 외부 대상 버킷에 복제하도록 하려는 경우 S3 버킷에 대해 CloudMirror 복제를 활성화할 수 있습니다.

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.

CloudMirror 및 **ILM**

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.

CloudMirror 및 교차 그리드 복제

CloudMirror 복제는 교차 그리드 복제 기능과의 중요한 유사점과 차이점이 있습니다. 을 "교차 그리드 복제와 CloudMirror 복제를 비교합니다"참조하십시오.

CloudMirror 및 **S3** 버킷

CloudMirror 복제는 일반적으로 외부 S3 버킷을 대상으로 사용하도록 구성됩니다. 그러나 다른 StorageGRID 배포나 S3 호환 서비스를 사용하도록 복제를 구성할 수도 있습니다.

기존 버킷

기존 버킷에 대해 CloudMirror 복제를 활성화하면 해당 버킷에 추가된 새 오브젝트만 복제됩니다. 버킷의 기존 객체는 복제되지 않습니다. 기존 오브젝트의 복제를 강제로 수행하려면 오브젝트 복사를 수행하여 기존 오브젝트의 메타데이터를 업데이트할 수 있습니다.

CloudMirror 복제를 사용하여 Amazon S3 대상으로 오브젝트를 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.

다중 대상 버킷

단일 버킷의 오브젝트를 여러 대상 버킷으로 복제하려면 복제 구성 XML에서 각 규칙의 대상을 지정합니다. 객체를 둘 이상의 버킷에 동시에 복제할 수 없습니다.

버전 또는 버전 해제된 버킷

버전 또는 버전이 지정되지 않은 버킷에서 CloudMirror 복제를 구성할 수 있습니다. 대상 버킷의 버전을 지정하거나 버전을 취소할 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.

삭제, 복제 루프 및 이벤트입니다

삭제 동작

는 Amazon S3 서비스, 지역 간 복제(CRR)의 삭제 동작과 동일합니다. 소스 버킷에서 오브젝트를 삭제하면 대상에서 복제된 오브젝트가 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 오브젝트를 삭제하지 않습니다.

복제 루프로부터 보호합니다

오브젝트가 대상 버킷에 복제되면 StorageGRID는 객체를 "복제본"으로 표시합니다. 대상 StorageGRID 버킷은 복제본으로 표시된 객체를 다시 복제하지 않으므로 실수로 인한 복제 루프가 발생하지 않습니다. 이 복제 마킹은 StorageGRID 내부에 있으며 Amazon S3 버킷을 대상으로 사용할 때 AWS CRR을 활용할 수 없습니다.

복제본을 표시하는 데 사용되는 사용자 지정 헤더는 입니다 `x-ntap-sg-replica`. 이 표시는 계단식 미러를 방지합니다. StorageGRID는 두 그리드 간의 양방향 CloudMirror를 지원합니다.

목적지 버킷의 이벤트

목적지 버킷에서 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.

버킷에 대한 알림을 이해합니다

StorageGRID에서 지정된 이벤트에 대한 알림을 대상 Kafka 클러스터 또는 Amazon Simple Notification Service로 보내려면 S3 버킷에 대한 이벤트 알림을 활성화할 수 있습니다.

예를 들어, 버킷에 추가된 각 오브젝트에 대해 관리자에게 경고가 전송되도록 구성할 수 있습니다. 여기서 객체는 중요한 시스템 이벤트와 연결된 로그 파일을 나타냅니다.

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 키를 사용하여 Amazon S3 설명서에 설명된 대로 특정 객체에 대한 이벤트 순서를 결정할 수 `sequencer` 있습니다.

StorageGRID 이벤트 알림은 Amazon S3 API를 따르지만 몇 가지 제한 사항을 따릅니다.

- 지원되는 이벤트 유형은 다음과 같습니다.
  - S3:ObjectCreated:
  - S3:오브젝트 생성:PUT
  - S3:오브젝트 작성:우편
  - S3:오브젝트 생성:복사
  - S3:ObjectCreated:CompleteMultipartUpload
  - S3:ObjectRemoved:
  - S3:ObjectRemoved:Delete
  - S3:ObjectRemoved:DeleteMarkerCreated
  - S3:ObjectRestore:게시
- StorageGRID에서 보낸 이벤트 알림은 표준 JSON 형식을 사용하지만 일부 키는 포함하지 않으며 표에 나와 있는 대로 다른 키의 특정 값을 사용합니다.

키 이름	**StorageGRID** 값
이벤트 소스	`sgws:s3`
awsRegion	_ 포함되지 않음 _
X-amz-id-2	_ 포함되지 않음 _
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 개체가 생성 또는 삭제되거나 해당 메타데이터 또는 태그가 업데이트될 때마다 S3 오브젝트 메타데이터를 대상 엔드포인트에 자동으로 비동기적으로 전송하는 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.

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(Retain To Date 및 Legal Hold 상태 포함)는 Elasticsearch로 전송되는 메타데이터에 포함되지 않습니다.

> 검색 통합 서비스가 개체 메타데이터를 대상으로 전송하도록 하기 때문에 해당 구성 XML을 "_metadata_notification 구성 XML"이라고 합니다. 이 구성 XML은 enable_event_notifications에 사용되는 "notification configuration xml"과 다릅니다.

검색 통합 및 **S3** 버킷

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.

메타데이터 알림은 버킷 이름, 개체 이름 및 버전 ID(있는 경우)로 명명된 JSON 문서 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.

알림을 검색합니다

메타데이터 알림은 다음과 같은 경우에 생성되고 배달 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. 하지만 이미 버킷에 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.

검색 통합 서비스 및 **Elasticsearch**

StorageGRID 검색 통합 서비스는 Elasticsearch 클러스터를 대상으로 지원합니다. 다른 플랫폼 서비스와 마찬가지로 대상은 서비스의 구성 XML에서 URN이 사용되는 끝점에서 지정됩니다. 를 사용하여 "NetApp 상호 운용성 매트릭스 툴" 지원되는 Elasticsearch 버전을 확인합니다.

플랫폼 서비스 끝점을 관리합니다

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. 단일 테넌트의 경우 최대 500개의 플랫폼 서비스 엔드포인트를 구성할 수 있습니다. 자세한 내용은 StorageGRID 관리자에게 문의하십시오.

플랫폼 서비스 엔드포인트란 무엇입니까?

플랫폼 서비스 끝점은 StorageGRID가 외부 대상에 액세스하는 데 필요한 정보를 지정합니다.

예를 들어, StorageGRID 버킷에서 Amazon S3 버킷으로 오브젝트를 복제하려는 경우 StorageGRID에서 Amazon의 대상 버킷에 액세스하는 데 필요한 정보 및 자격 증명이 포함된 플랫폼 서비스 엔드포인트를 생성합니다.

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. 하나 이상의 엔드포인트를 대상으로 사용하도록 소스 버킷을 구성할 수도 있습니다. 이를 통해 하나의 Amazon SNS(Simple Notification Service) 주제에 객체 생성에 대한 알림을 보내고 두 번째 Amazon SNS 주제에 대한 객체 삭제에 대한 알림을 보낼 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 Amazon SNS 및 Kafka 엔드포인트를 지원합니다. SQS(Simple Queue Service) 또는 AWS Lambda 엔드포인트는 지원되지 않습니다.

Kafka 엔드포인트의 경우 상호 TLS는 지원되지 않습니다. 그 결과, Kafka 브로커 구성에서 로 설정한 `required` 경우 `ssl.client.auth` Kafka 엔드포인트 구성 문제가 발생할 수 있습니다.

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 **URN**을 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 또는 `urn:mysite` 로 시작해야 합니다 `arn:aws`.

- 서비스가 AWS(Amazon Web Services)에서 호스팅되는 경우 를 사용합니다 `arn:aws`
- 서비스가 Google Cloud Platform(GCP)에서 호스팅되는 경우 를 사용합니다 `arn:aws`
- 서비스가 로컬로 호스팅되는 경우 를 사용합니다 `urn:mysite`

예를 들어, StorageGRID에서 호스팅되는 CloudMirror 끝점에 대해 URN을 지정하는 경우 URN은 로 시작할 수 `urn:sgws` 있습니다.

URN의 다음 요소는 다음과 같이 플랫폼 서비스의 유형을 지정합니다.

서비스	유형
CloudMirror 복제	`s3`
알림	`sns` 또는 `kafka`
검색 통합	`es`

예를 들어, StorageGRID에서 호스팅되는 CloudMirror 끝점에 대해 URN을 계속 지정하려면 GET에 `urn:sgws:s3` 을 추가합니다 `s3`.

URN의 마지막 요소는 대상 URI에서 특정 대상 리소스를 식별합니다.

서비스	특정 리소스
CloudMirror 복제	`bucket-name`
알림	`sns-topic-name` 또는 `kafka-topic-name`
검색 통합	`domain-name/index-name/type-name` • 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 끝점의 경우 에 `domain-name` 나와 있는 리터럴 문자열이 포함되어야 `domain/` 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
```

  StorageGRID에 호스팅된 CloudMirror 엔드포인트의 경우 다음으로 시작하는 유효한 URN을 지정할 수 `urn:sgws` 있습니다.

```
urn:sgws:s3:optional:optional:bucket-name
```

- 알림:

  Amazon Simple Notification Service 끝점 지정:

```
urn:mysite:sns:optional:optional:sns-topic-name
```

  Kafka 끝점 지정:

```
urn:mysite:kafka:optional:optional:kafka-topic-name
```

- 검색 통합:

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```

로컬로 호스팅되는 검색 통합 끝점의 경우 `domain-name` 끝점의 URN이 고유하면 모든 문자열이 요소가 될 수 있습니다.

플랫폼 서비스 끝점을 만듭니다

플랫폼 서비스를 사용하려면 먼저 올바른 유형의 끝점을 하나 이상 만들어야 합니다.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 활성화했습니다.
- 이 있는 사용자 그룹에 속해 "끝점 또는 루트 액세스 권한을 관리합니다"있습니다.
- 플랫폼 서비스 끝점에서 참조하는 리소스가 생성되었습니다.
  - CloudMirror 복제: S3 버킷
  - 이벤트 알림: Amazon SNS(Simple Notification Service) 또는 Kafka 토픽입니다
  - 검색 알림: 대상 클러스터가 인덱스를 자동으로 생성하도록 구성되지 않은 경우 Elasticsearch index입니다.
- 대상 리소스에 대한 정보가 있습니다.
  - 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):

검색 통합 끝점

검색 통합 끝점의 경우 다음 자격 증명을 사용할 수 있습니다.

- 액세스 키: 액세스 키 ID 및 비밀 액세스 키
- 기본 HTTP: 사용자 이름 및 암호

CloudMirror 복제 엔드포인트

CloudMirror 복제 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

- 액세스 키: 액세스 키 ID 및 비밀 액세스 키
- CAP(C2S Access Portal): 임시 자격 증명 URL, 서버 및 클라이언트 인증서, 클라이언트 키 및 선택적 클라이언트 개인 키 암호.

Amazon SNS 엔드포인트입니다

Amazon SNS 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

- 액세스 키: 액세스 키 ID 및 비밀 액세스 키

Kafka 엔드포인트

Kafka 엔드포인트의 경우 다음 자격 증명을 사용할 수 있습니다.

- SASL /plain: 사용자 이름 및 암호
- SASL/SCRAM-SHA-256: 사용자 이름 및 암호
- SASL/SCRAM-SHA-512: 사용자 이름 및 암호

  - 보안 인증서(사용자 지정 CA 인증서를 사용하는 경우)

- Elasticsearch 보안 기능이 활성화된 경우 연결 테스트에 대한 모니터 클러스터 권한, 쓰기 인덱스 권한 또는 문서 업데이트에 대한 인덱스 및 삭제 권한 모두가 있습니다.

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 표시되므로 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 다음과 같은 기본 포트가 사용됩니다.

- HTTPS URI의 경우 포트 443, HTTP URI의 경우 포트 80(대부분의 끝점)
- HTTPS 및 HTTP URI용 포트 9092(Kafka 엔드포인트만 해당)

예를 들어 StorageGRID에서 호스팅되는 버킷의 URI는 다음과 같습니다.

```
https://s3.example.com:10443
```

이 예에서 는 `s3.example.com` StorageGRID HA(고가용성) 그룹의 VIP(가상 IP)에 대한 DNS 항목을 나타내고 `10443` 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 선택합니다.

검색 통합 끝점

검색 통합 끝점에 대한 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

CloudMirror 복제 엔드포인트

CloudMirror 복제 엔드포인트에 대한 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
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)

Amazon SNS 엔드포인트입니다

Amazon SNS 끝점에 대한 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

Kafka 엔드포인트

Kafka 엔드포인트에 대한 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.
SASL/일반	사용자 이름과 암호를 일반 텍스트로 사용하여 대상에 대한 연결을 인증합니다.	• 사용자 이름 • 암호
SASL/SCRAM-SHA-256	Challenge-Response 프로토콜 및 SHA-256 해싱을 사용하여 사용자 이름과 암호를 사용하여 대상에 대한 연결을 인증합니다.	• 사용자 이름 • 암호
SASL/SCRAM-SHA-512	Challenge-Response 프로토콜 및 SHA-512 해싱을 사용하여 사용자 이름과 암호를 사용하여 대상에 대한 연결을 인증합니다.	• 사용자 이름 • 암호

사용자 이름과 암호가 Kafka 클러스터에서 가져온 위임 토큰에서 파생되는 경우 * Use 위임 인증 사용 * 을 선택합니다.

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.

인증서 확인 유형입니다	설명
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.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "끝점 또는 루트 액세스 권한을 관리합니다"있습니다.

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.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "끝점 또는 루트 액세스 권한을 관리합니다"있습니다.

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.
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.
      - 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.

시작하기 전에

- 를 사용하여 테넌트 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 이 있는 사용자 그룹에 속해 "끝점 또는 루트 액세스 권한을 관리합니다"있습니다.

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.

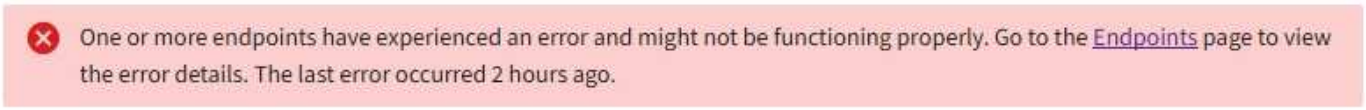
4. 끝점 삭제 * 를 선택합니다.

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 오류는 지난 7일 내에 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. 메시지는 "끝점 자격 증명 또는 대상 액세스를 업데이트해야 합니다."이고 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. 이러한 이유로 플랫폼 서비스를 사용하려고 할 때 오류(예: "403 금지됨")가 발생하면 끝점의 자격 증명과 연결된 사용 권한을 확인하십시오.

관련 정보

- "StorageGRID 및 GT 관리, 플랫폼 서비스 문제 해결"
- "플랫폼 서비스 끝점을 만듭니다"
- "플랫폼 서비스 끝점에 대한 연결을 테스트합니다"
- "플랫폼 서비스 끝점을 편집합니다"

버킷에 대해 CloudMirror 복제를 활성화하려면 유효한 버킷 복제 구성 XML을 생성하고 적용합니다.

시작하기 전에

- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 활성화했습니다.
- 복제 소스로 사용할 버킷을 이미 생성했습니다.
- CloudMirror 복제의 대상으로 사용하려는 엔드포인트가 이미 있으며 URN이 있습니다.
- 이 있는 사용자 그룹에 속해 "모든 버킷 또는 루트 액세스 권한을 관리합니다"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.

버킷 복제에 대한 일반적인 정보와 이를 구성하는 방법은 을 참조하십시오 "Amazon S3(Simple Storage Service) 문서: 오브젝트 복제". StorageGRID에서 GetBucketReplication, DeleteBucketReplication 및 PutBucketReplication을 구현하는 방법에 대한 자세한 내용은 를 참조하십시오"버킷 작업".

> CloudMirror 복제는 교차 그리드 복제 기능과의 중요한 유사점과 차이점이 있습니다. 자세한 내용은 을 참조하십시오"교차 그리드 복제와 CloudMirror 복제를 비교합니다".

CloudMirror 복제를 구성할 때 다음과 같은 요구 사항 및 특성에 유의하십시오.

- 유효한 버킷 복제 구성 XML을 만들고 적용할 때 각 대상에 대해 S3 버킷 끝점의 URN을 사용해야 합니다.
- S3 오브젝트 잠금이 활성화된 소스 또는 대상 버킷에는 복제가 지원되지 않습니다.
- 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 요소 사용을 지원하지 `Filter` 않으며 객체 버전을 삭제하기 위한 V1 규칙을 따릅니다. 자세한 내용은 복제 구성에 대한 Amazon 설명서를 참조하십시오.
     - S3 버킷 엔드포인트의 URN을 대상으로 사용합니다.
     - 선택적으로 `<StorageClass>` 요소를 추가하고 다음 중 하나를 지정합니다.
       - `STANDARD`: 기본 스토리지 클래스입니다. 개체를 업로드할 때 저장소 클래스를 지정하지 않으면 `STANDARD` 저장소 클래스가 사용됩니다.

- `STANDARD_IA`: (표준 - 자주 액세스하지 않음) 자주 액세스하지 않지만 필요할 때 빠르게 액세스해야 하는 데이터에 이 스토리지 클래스를 사용합니다.
- `REDUCED_REDUNDANCY`: 스토리지 클래스보다 낮은 중복성으로 저장할 수 있는 비중요하고 재현 가능한 데이터에 이 스토리지 클래스를 `STANDARD` 사용합니다.

- 구성 XML에서 을 `Role` 지정하면 이 작업은 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. 대시보드에서 * 버킷 보기 * 를 선택하거나 * 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.

      앞에 나와 있는 예에서 접두사 "2020"과 일치하는 객체가 복제됩니다.

   b. 객체가 대상 버킷에 복제되었는지 확인합니다.

      오브젝트 크기가 작은 경우 복제가 빠르게 수행됩니다.

관련 정보

"플랫폼 서비스 끝점을 만듭니다"

알림 구성 XML을 생성하고 테넌트 관리자를 사용하여 XML을 버킷에 적용하여 버킷에 대한 알림을 활성화합니다.

시작하기 전에

- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 활성화했습니다.
- 알림 소스로 사용할 버킷을 이미 생성했습니다.
- 이벤트 알림 대상으로 사용하려는 엔드포인트가 이미 있으며 URN이 있습니다.
- 이 있는 사용자 그룹에 속해 "모든 버킷 또는 루트 액세스 권한을 관리합니다"있습니다. 이러한 권한은 테넌트 관리자를 사용하여 버킷을 구성할 때 그룹 또는 버킷 정책의 권한 설정을 재정의합니다.

이 작업에 대해

알림 구성 XML을 소스 버킷과 연결하여 이벤트 알림을 구성합니다. 알림 구성 XML은 끝점 URN으로 지정된 대상 Kafka 또는 Amazon SNS 항목과 함께 버킷 알림을 구성하는 S3 규칙을 따릅니다.

이벤트 알림에 대한 일반적인 정보와 이벤트 알림을 구성하는 방법은 을 "아마존 문서"참조하십시오. StorageGRID에서 S3 버킷 알림 구성 API를 구현하는 방법에 대한 자세한 내용은 를 "S3 클라이언트 애플리케이션 구현 지침 "참조하십시오.

버킷에 대한 이벤트 알림을 구성할 때는 다음 요구 사항 및 특성을 참고하십시오.

- 유효한 알림 구성 XML을 만들고 적용할 때 각 대상에 대한 이벤트 알림 끝점의 URN을 사용해야 합니다.
- S3 오브젝트 잠금이 설정된 버킷에서 이벤트 알림을 구성할 수 있지만, 오브젝트의 S3 오브젝트 잠금 메타데이터(보존 기한 및 법적 증거 자료 보관 상태 포함)는 알림 메시지에 포함되지 않습니다.
- 이벤트 알림을 구성한 후 소스 버킷의 오브젝트에 대해 지정된 이벤트가 발생할 때마다 알림이 생성되어 대상 끝점으로 사용되는 Amazon SNS 또는 Kafka 토픽으로 전송됩니다.
- 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 접두사를 사용하여 개체를 만들 때마다 이벤트 알림이 `images/` 전송됩니다.

   b. 알림이 대상 Amazon SNS 또는 Kafka 토픽에 전달되었는지 확인합니다.

      예를 들어 대상 주제가 Amazon SNS에 호스팅되어 있는 경우 알림이 배달될 때 이메일을 보내도록 서비스를 구성할 수 있습니다.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "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"

"S3 REST API 사용"

"플랫폼 서비스 끝점을 만듭니다"

검색 통합 서비스를 구성합니다

검색 통합 XML을 만들고 테넌트 관리자를 사용하여 XML을 버킷에 적용하여 버킷에 대한 검색 통합을 활성화합니다.

시작하기 전에

- StorageGRID 관리자가 테넌트 계정에 대해 플랫폼 서비스를 활성화했습니다.
- 인덱싱할 콘텐츠가 있는 S3 버킷을 이미 생성했습니다.
- 검색 통합 서비스의 대상으로 사용하려는 엔드포인트가 이미 있으며 URN이 있습니다.
- 이 있는 사용자 그룹에 속해 "모든 버킷 또는 루트 액세스 권한을 관리합니다"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 해당 메타데이터가 대상 검색 인덱스에 추가되도록 합니다.

단계

1. 버킷에 대한 검색 통합 활성화:
   - 텍스트 편집기를 사용하여 검색 통합을 활성화하는 데 필요한 메타데이터 알림 XML을 만듭니다.
   - XML을 구성할 때는 검색 통합 끝점의 URN을 대상으로 사용합니다.

     개체 이름의 접두어를 기준으로 개체를 필터링할 수 있습니다. 예를 들어, 접두사가 있는 개체의 메타데이터는 한 대상에, 접두사가 있는 개체의 메타데이터는 다른 대상에 `videos` 보낼 수 `images` 있습니다. 접두사가 겹치는 구성은 유효하지 않으며 제출될 때 거부됩니다. 예를 들어, 접두사가 있는 객체에 대한 규칙 하나와 접두사가 있는 객체에 대한 두 번째 규칙이 `test2` 포함된 구성은 `test` 허용되지 않습니다.

     필요한 경우 을 메타데이터 구성 XML의 예참조하십시오.

     ```
     <MetadataNotificationConfiguration>
      <Rule>
         <Status>Enabled</Status>
         <Prefix></Prefix>
         <Destination>
            <Urn>/Urn>
            </Destination>
      </Rule>
     </MetadataNotificationConfiguration>
     ```

     메타데이터 알림 구성 XML의 요소:

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
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. • `es` 세 번째 요소여야 합니다. • URN은 메타데이터가 저장되는 인덱스 및 형식으로 끝나야 `domain-name/myindex/mytype` 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

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.

예: 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>
```

예: 두 개의 규칙이 있는 메타데이터 알림 구성

이 예에서는 접두사와 일치하는 개체의 개체 메타데이터가 `/images` 한 대상으로 전송되고, 접두사와 일치하는 개체의 개체 메타데이터가 `/videos` 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>
```

버킷에 대한 검색 통합 서비스를 활성화하면 개체 메타데이터 또는 태그를 추가, 업데이트 또는 삭제할 때마다 JSON 문서가 생성되어 대상 끝점으로 전송됩니다.

이 예제는 키가 있는 개체가 라는 버킷에 `test` 생성될 때 생성될 수 있는 JSON의 예를 보여줍니다 `SGWS/Tagging.txt`. `test`버킷이 버전이 아니므로 `versionId` 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"
  }
}
```

JSON 문서에 포함된 필드입니다

문서 이름에는 버킷 이름, 오브젝트 이름 및 버전 ID(있는 경우)가 포함됩니다.

버킷 및 오브젝트 정보

`bucket`: 버킷의 이름입니다

`key`: 개체 키 이름입니다

`versionID`: 버전 버킷의 객체에 대한 객체 버전입니다

`region`: 버킷 영역(예: `us-east-1`

시스템 메타데이터

`size`: HTTP 클라이언트에서 볼 수 있는 개체 크기(바이트)

`md5`: 개체 해시입니다

사용자 메타데이터

`metadata`: 객체에 대한 모든 사용자 메타데이터, 키-값 쌍

`key:value`

태그

`tags`: 객체에 대해 키-값 쌍으로 정의된 모든 객체 태그

```
key:value
```

Elasticsearch에서 결과를 보는 방법

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 사용하도록 설정합니다. 문서가 인덱싱된 후에는 인덱스에서 문서의 필드 형식을 편집할 수 없습니다.

S3 REST API 사용

S3 REST API 지원 버전 및 업데이트

StorageGRID는 REST(Representational State Transfer) 웹 서비스 세트로 구현되는 S3(Simple Storage Service) API를 지원합니다.

S3 REST API를 지원하므로 StorageGRID 시스템을 사용하는 사내 오브젝트 스토리지를 통해 S3 웹 서비스용으로 개발된 서비스 지향 애플리케이션을 연결할 수 있습니다. 클라이언트 애플리케이션의 현재 S3 REST API 호출 사용에 대한 최소 변경 사항이 필요합니다.

지원되는 버전

StorageGRID는 다음과 같은 S3 및 HTTP 버전을 지원합니다.

항목	버전
S3 API 사양	"AWS(Amazon Web Services) 문서: Amazon Simple Storage Service API Reference 를 참조하십시오"
HTTP	1.1 HTTP에 대한 자세한 내용은 HTTP/1.1(RFC 7230-35)을 참조하십시오. "IETF RFC 2616:HTTP/1.1(Hypertext Transfer Protocol)" • 참고 *: StorageGRID는 HTTP/1.1 파이프라이닝을 지원하지 않습니다.

S3 REST API 지원 업데이트

놓습니다	설명
11.9	• 다음 요청 및 지원되는 헤더에 대해 미리 계산된 SHA-256 체크섬 값에 대한 지원이 추가되었습니다. 이 기능을 사용하여 업로드된 개체의 무결성을 확인할 수 있습니다. ◦ CompleteMultipartUpload: `x-amz-checksum-sha256` ◦ CreateMultipartUpload: `x-amz-checksum-algorithm` ◦ GetObject(개체 가져오기): `x-amz-checksum-mode` ◦ 제목 개체: `x-amz-checksum-mode` ◦ 목록 파트 ◦ Put개체: `x-amz-checksum-sha256` ◦ 업로드 부품: `x-amz-checksum-sha256` • 그리드 관리자가 테넌트 레벨 보존 및 규정 준수 설정을 제어할 수 있는 기능이 추가되었습니다. 이러한 설정은 S3 오브젝트 잠금 설정에 영향을 줍니다. ◦ 버킷 기본 보존 모드 및 객체 보존 모드: 그리드 관리자가 허용하는 경우 거버넌스 또는 규정 준수 ◦ 버킷 기본 보존 기간 및 객체 유지 기한: 그리드 관리자가 설정한 최대 보존 기간에 허용되는 값보다 작거나 같아야 합니다. • 콘텐츠 인코딩 및 스트리밍 `x-amz-content-sha256` 값에 대한 지원이 `aws-chunked` 향상되었습니다. 제한 사항: ◦ 있는 경우 `chunk-signature` 는 선택 사항이며 검증되지 않았습니다 ◦ 있는 경우 `x-amz-trailer` 콘텐츠는 무시됩니다
11.8	에 사용된 이름과 일치하도록 S3 작업의 이름을 업데이트했습니다. "AWS(Amazon Web Services) 문서: Amazon Simple Storage Service API Reference 를 참조하십시오"
11.7	• "빠른 참조: 지원되는 S3 API 요청"추가되었습니다. • S3 Object Lock을 통한 거버넌스 모드 사용을 지원합니다. • Get Object 및 Head Object 요청에 대한 StorageGRID별 응답 헤더에 대한 지원이 추가되었습니다 `x-ntap-sg-cgr-replication-status`. 이 헤더는 크로스 그리드 복제를 위한 객체의 복제 상태를 제공합니다. • SelectObjectContent 요청이 이제 Parquet 객체를 지원합니다.
11.6	• GET Object 및 HEAD Object 요청에서 REQUEST 매개 변수 사용에 대한 지원이 추가되었습니다 `partNumber`. • S3 오브젝트 잠금의 버킷 레벨에서 기본 보존 모드 및 기본 보존 기간에 대한 지원이 추가되었습니다. • 객체에 대해 허용되는 보존 기간의 범위를 설정하기 위해 정책 조건 키에 대한 지원이 추가되었습니다 `s3:object-lock-remaining-retention-days`. • 단일 PUT 객체 작업의 Maximum_Recommended_size를 5GiB(5,368,709,120바이트)로 변경했습니다. 5GiB보다 큰 객체가 있는 경우 대신 멀티파트 업로드를 사용합니다.

놓습니다	설명
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`이제 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. • 이벤트 유형에 버킷 알림에 대한 지원이 `s3:ObjectRestore:Post` 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 지원이 추가되었습니다
11.3	• 고객이 제공한 키(SSE-C)를 사용하여 오브젝트 데이터의 서버측 암호화에 대한 지원이 추가되었습니다. • 삭제, 가져오기 및 넣기 버킷 라이프사이클 작업(만료 작업에만 해당) 및 응답 헤더에 대한 지원이 추가되었습니다 `x-amz-expiration`. • 수집 시 동기식 배치를 사용하는 ILM 규칙의 영향을 설명하기 위해 PUT 개체, Put Object-Copy 및 MultiPart Upload가 업데이트되었습니다. • TLS 1.1 암호가 더 이상 지원되지 않습니다.
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 버킷에 대한 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 위치 제약 조건 및 사용 가능한 정합성 보장에 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.

놓습니다	설명
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.

빠른 참조: 지원되는 **S3 API** 요청

이 페이지에서는 StorageGRID에서 Amazon S3(Simple Storage Service) API를 지원하는 방법을 요약합니다.

이 페이지에는 StorageGRID에서 지원하는 S3 작업만 포함됩니다.

각 작업에 대한 AWS 설명서를 보려면 제목에서 링크를 선택합니다.

공통 **URI** 쿼리 매개 변수 및 요청 헤더

별도로 지정하지 않으면 다음과 같은 공통 URI 쿼리 매개 변수가 지원됩니다.

- `versionId` (개체 작업에 필요한 경우)

별도로 명시되지 않은 경우 다음과 같은 일반적인 요청 헤더가 지원됩니다.

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

관련 정보

- "S3 REST API 구현 세부 정보"
- "Amazon Simple Storage Service API 참조: 일반 요청 헤더"

"AbortMultipartUpload 를 클릭합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두 지원하며공통 매개 변수 및 머리글, 이 추가 URI 쿼리 매개 변수는 다음과 같습니다.

- `uploadId`

요청 본문

없음

StorageGRID 설명서

"멀티파트 업로드 작업"

"CompleteMultipartUpload를 클릭합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두 지원하며공통 매개 변수 및 머리글, 이 추가 URI 쿼리 매개 변수는 다음과 같습니다.

- `uploadId`
- `x-amz-checksum-sha256`

본문 **XML** 태그를 요청합니다

StorageGRID는 다음과 같은 요청 본문 XML 태그를 지원합니다.

- `ChecksumSHA256`
- `CompleteMultipartUpload`
- `ETag`
- `Part`
- `PartNumber`

StorageGRID 설명서

"CompleteMultipartUpload를 클릭합니다"

"CopyObject 를 선택합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글항목과 다음 추가 헤더를 지원합니다.

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`

- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

요청 본문

없음

StorageGRID 설명서

"CopyObject 를 선택합니다"

"CreateBucket"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글항목과 다음 추가 헤더를 지원합니다.

- `x-amz-bucket-object-lock-enabled`

요청 본문

StorageGRID는 구현 시 Amazon S3 REST API에 의해 정의된 모든 요청 본문 매개 변수를 지원합니다.

StorageGRID 설명서

"버킷 작업"

"CreateMultptUpload 를 클릭합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글항목과 다음 추가 헤더를 지원합니다.

- `Cache-Control`
- `Content-Disposition`

- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

요청 본문

없음

StorageGRID 설명서

"CreateMultptUpload 를 클릭합니다"

"삭제 버킷"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

StorageGRID 설명서

"버킷 작업"

"DeleteBucketCors"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"DeleteBucketEncryption"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"DeleteBucketLifecycle"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

- "버킷 작업"
- "S3 라이프사이클 구성을 생성합니다"

"DeleteBuckketPolicy를 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"DeleteBuckReplication 을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"삭제 BucketTagging"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"DeleteObject 를 클릭합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글지원과 다음 추가 요청 헤더를 지원합니다.

- `x-amz-bypass-governance-retention`

요청 본문

없음

StorageGRID 설명서

"객체에 대한 작업"

"DeleteObjects 를 클릭합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글지원과 다음 추가 요청 헤더를 지원합니다.

- `x-amz-bypass-governance-retention`

요청 본문

StorageGRID는 구현 시 Amazon S3 REST API에 의해 정의된 모든 요청 본문 매개 변수를 지원합니다.

StorageGRID 설명서

"객체에 대한 작업"

"DeleteObjectTagging 을 선택합니다"

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"객체에 대한 작업"

"GetBuckketAcl"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"GetBuckketCors 를 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"GetBuckketEncryption을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"GetBuckLifecycleConfiguration 을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

- "버킷 작업"
- "S3 라이프사이클 구성을 생성합니다"

"GetBucketLocation 을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"GetBuckNotificationConfiguration 을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"GetBuckketPolicy를 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"GetBucketReplication 을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"GetBucketTagging"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"GetBuckketVersioning 을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"GetObject 를 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두 지원하며 공통 매개 변수 및 머리글다음과 같은 추가 URI 쿼리 매개 변수를 지원합니다.

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

그리고 이러한 추가 요청 헤더는 다음과 같습니다.

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

요청 본문

없음

StorageGRID 설명서

"GetObject 를 참조하십시오"

"GetObjectAcl"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"객체에 대한 작업"

"GetObjectLegalHold 를 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"

"GetObjectLockConfiguration 을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"

"GetObjectRetention을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"

"GetObjectTagging"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"객체에 대한 작업"

"머리버킷"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"HeadObject 를 선택합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글항목과 다음 추가 헤더를 지원합니다.

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

요청 본문

없음

StorageGRID 설명서

"HeadObject 를 선택합니다"

"ListBucket"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

없음

StorageGRID 설명서

"서비스 및 GT, ListBucket에 대한 작업"

"ListMultipartUploads 를 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글정보와 다음과 같은 추가 매개 변수를 지원합니다.

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

요청 본문

없음

StorageGRID 설명서

"ListMultipartUploads 를 참조하십시오"

"ListObjects 를 선택합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글정보와 다음과 같은 추가 매개 변수를 지원합니다.

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"ListObjectsV2 를 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글정보와 다음과 같은 추가 매개 변수를 지원합니다.

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"ListObjectVersions 를 선택합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글정보와 다음과 같은 추가 매개 변수를 지원합니다.

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

요청 본문

없음

StorageGRID 설명서

"버킷 작업"

"목록 파트"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글정보와 다음과 같은 추가 매개 변수를 지원합니다.

- `max-parts`

- part-number-marker
- uploadId

요청 본문

없음

StorageGRID 설명서

"ListMultipartUploads 를 참조하십시오"

"BuckketCors의"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

StorageGRID는 구현 시 Amazon S3 REST API에 의해 정의된 모든 요청 본문 매개 변수를 지원합니다.

StorageGRID 설명서

"버킷 작업"

"PutBucketEncryption을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

본문 **XML** 태그를 요청합니다

StorageGRID는 다음과 같은 요청 본문 XML 태그를 지원합니다.

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

StorageGRID 설명서

"버킷 작업"

"PutBucketLifecycleConfiguration을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

본문 **XML** 태그를 요청합니다

StorageGRID는 다음과 같은 요청 본문 XML 태그를 지원합니다.

- And
- Days

- `Expiration`
- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`
- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

StorageGRID 설명서

- "버킷 작업"
- "S3 라이프사이클 구성을 생성합니다"

"PutBucketNotificationConfiguration을 참조하십시오**"**

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

본문 **XML** 태그를 요청합니다

StorageGRID는 다음과 같은 요청 본문 XML 태그를 지원합니다.

- `Event`
- `Filter`
- `FilterRule`
- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`

- `Value`

StorageGRID 설명서

"버킷 작업"

"BucketPolicy를 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

지원되는 JSON 본문 필드에 대한 자세한 내용은 을 "버킷 및 그룹 액세스 정책을 사용합니다"참조하십시오.

"PutBucketReplication을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

본문 **XML** 태그를 요청합니다

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

StorageGRID 설명서

"버킷 작업"

"BucketTagging"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

StorageGRID는 구현 시 Amazon S3 REST API에 의해 정의된 모든 요청 본문 매개 변수를 지원합니다.

StorageGRID 설명서

"버킷 작업"

"PutBucketVersioning을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

바디 매개 변수를 요청합니다

StorageGRID는 다음과 같은 요청 본문 매개 변수를 지원합니다.

- `VersioningConfiguration`
- `Status`

StorageGRID 설명서

"버킷 작업"

"PutObject 를 선택합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글항목과 다음 추가 헤더를 지원합니다.

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

요청 본문

- 개체의 이진 데이터입니다

StorageGRID 설명서

"PutObject 를 선택합니다"

"PutObjectLegalHold를 선택합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

StorageGRID는 구현 시 Amazon S3 REST API에 의해 정의된 모든 요청 본문 매개 변수를 지원합니다.

StorageGRID 설명서

"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"

"PutObjectLockConfiguration 을 참조하십시오"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

StorageGRID는 구현 시 Amazon S3 REST API에 의해 정의된 모든 요청 본문 매개 변수를 지원합니다.

StorageGRID 설명서

"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"

"PutObjectRetention"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대한 모든 공통 매개 변수 및 머리글항목과 다음 추가 헤더를 지원합니다.

- `x-amz-bypass-governance-retention`

요청 본문

StorageGRID는 구현 시 Amazon S3 REST API에 의해 정의된 모든 요청 본문 매개 변수를 지원합니다.

StorageGRID 설명서

"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"

"PutObjectTagging"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

StorageGRID는 구현 시 Amazon S3 REST API에 의해 정의된 모든 요청 본문 매개 변수를 지원합니다.

StorageGRID 설명서

"객체에 대한 작업"

"RestoreObject 를 선택합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

지원되는 본문 필드에 대한 자세한 내용은 을 "RestoreObject 를 선택합니다"참조하십시오.

"SelectObjectContent 를 선택합니다"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두를 공통 매개 변수 및 머리글지원합니다.

요청 본문

지원되는 본문 필드에 대한 자세한 내용은 다음을 참조하십시오.

- "S3 Select를 사용합니다"
- "SelectObjectContent 를 선택합니다"

"업로드 파트"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두 지원하며 공통 매개 변수 및 머리글다음과 같은 추가 URI 쿼리 매개 변수를 지원합니다.

- `partNumber`
- `uploadId`

그리고 이러한 추가 요청 헤더는 다음과 같습니다.

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

요청 본문

- 파트의 이진 데이터

StorageGRID 설명서

"업로드 파트"

"업로드파트 복사"

Uri 쿼리 매개 변수 및 요청 헤더

StorageGRID는 이 요청에 대해 모두 지원하며 공통 매개 변수 및 머리글다음과 같은 추가 URI 쿼리 매개 변수를 지원합니다.

- `partNumber`
- `uploadId`

그리고 이러한 추가 요청 헤더는 다음과 같습니다.

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`

- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

요청 본문

없음

StorageGRID 설명서

"업로드파트 복사"

S3 REST API 구성을 테스트합니다

AWS CLI(Amazon Web Services 명령줄 인터페이스)를 사용하여 시스템에 대한 연결을 테스트하고 개체를 읽고 쓸 수 있는지 확인할 수 있습니다.

시작하기 전에

- 에서 AWS CLI를 다운로드하여 "aws.amazon.com/cli" 설치했습니다.
- 필요한 경우 가 "로드 밸런서 끝점을 생성했습니다"있습니다. 그렇지 않으면 연결할 스토리지 노드의 IP 주소와 사용할 포트 번호를 알 수 있습니다. 을 "클라이언트 연결용 IP 주소 및 포트"참조하십시오.
- 있습니다. "S3 테넌트 계정을 생성했습니다"
- 테넌트 및 에 로그인했습니다"선택키를 만들었습니다".

이러한 단계에 대한 자세한 내용은 을 "클라이언트 연결을 구성합니다"참조하십시오.

단계

1. StorageGRID 시스템에서 생성한 계정을 사용하도록 AWS CLI 설정을 구성합니다.
   a. 구성 모드로 전환: `aws configure`
   b. 생성한 계정의 액세스 키 ID를 입력합니다.
   c. 생성한 계정의 암호 액세스 키를 입력합니다.
   d. 사용할 기본 영역을 입력합니다. `us-east-1`예를 들어,
   e. 사용할 기본 출력 형식을 입력하거나 * Enter * 를 눌러 JSON을 선택합니다.
2. 버킷을 만듭니다.

이 예에서는 IP 주소 10.96.101.17 및 포트 10443을 사용하도록 로드 밸런서 끝점을 구성했다고 가정합니다.

```
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"
```

3. 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.

4. 버킷의 내용을 나열하여 객체가 업로드되었는지 확인합니다.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. 개체를 삭제합니다.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. 버킷을 삭제합니다.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

StorageGRID에서 S3 REST API를 구현하는 방법

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 값

정합성 보장은 서로 다른 스토리지 노드 및 사이트에서 객체의 가용성과 객체 일관성 간의 균형을 제공합니다. 애플리케이션에 필요한 만큼 일관성을 변경할 수 있습니다.

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.

개체 작업을 다른 일관성으로 수행하려는 경우 다음을 수행할 수 있습니다.

- 에 대한 일관성을 각 버킷지정합니다.
- 에 대한 일관성을 각 API 작동지정합니다.
- 다음 작업 중 하나를 수행하여 그리드 전체의 기본 일관성을 변경합니다.
  - 그리드 관리자에서 * 구성 * > * 시스템 * > * 스토리지 설정 * > * 기본 일관성 * 로 이동합니다.
  - ..

> 그리드 전체의 일관성에 대한 변경은 설정이 변경된 후에 생성된 버킷에만 적용됩니다. 변경에 대한 세부 정보를 확인하려면 에 있는 감사 로그를 참조하십시오 `/var/local/log`(* consistencyLevel* 검색).

일관성 값

일관성은 StorageGRID이 오브젝트를 추적하는 데 사용하는 메타데이터가 노드 간에 분산되는 방식과 클라이언트 요청을 위한 개체의 가용성에 영향을 줍니다.

버킷 또는 API 작업의 정합성을 다음 값 중 하나로 설정할 수 있습니다.

- * ALL *: 모든 노드가 즉시 데이터를 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 개체에 대해 읽기-쓰기 후 일관성을 제공하고 개체 업데이트에 대한 최종 일관성을 제공합니다. 고가용성 및 데이터 보호 보장 제공 대부분의 경우에 권장됩니다.
- * 사용 가능 *: 새 객체 및 객체 업데이트 모두에 대한 최종 일관성을 제공합니다. S3 버킷의 경우 필요한 경우에만 사용하십시오(예: 거의 읽지 않는 로그 값이 포함된 버킷의 경우 또는 존재하지 않는 키의 헤드 또는 GET 작업의 경우). S3 FabricPool 버킷은 지원되지 않습니다.

"Read-after-new-write" 및 **"Available"** 정합성 보장을 사용합니다

HEAD 또는 GET 작업에서 "Read-after-new-write" 일관성을 사용하는 경우 StorageGRID는 다음과 같이 여러 단계로 조회를 수행합니다.

- 먼저 낮은 일관성을 사용하여 오브젝트를 찾습니다.
- 이 조회가 실패하면 다음 일관성 값에서 조회를 반복하여 강력한 글로벌 동작과 동일한 일관성을 유지합니다.

HEAD 또는 GET 작업에서 "Read-after-new-write" 일관성을 사용하지만 객체가 존재하지 않는 경우 객체 조회는 항상 강력한 글로벌 동작과 동일한 일관성을 유지합니다. 이 일관성을 유지하기 위해서는 각 사이트에서 개체 메타데이터의 여러 복사본을 사용할 수 있어야 하므로, 같은 사이트에 있는 두 개 이상의 스토리지 노드를 사용할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다.

Amazon S3와 유사한 일관성 보장이 필요하지 않은 경우 일관성을 "사용 가능"으로 설정하여 헤드 및 가져오기 작업에 대한 이러한 오류를 방지할 수 있습니다. 두부 또는 GET 작업에서 "사용 가능한" 일관성을 사용하는 경우 StorageGRID는 최종 일관성을 제공합니다. 일관성 향상을 위해 실패한 작업을 다시 시도하지 않으므로 개체 메타데이터의 여러 복사본을 사용할 필요가 없습니다.

API 작업에 대한 일관성을 지정합니다

개별 API 작업에 대한 일관성을 설정하려면 작업에 대해 정합성 보장 값을 지원해야 하며 요청 헤더에서 일관성을 지정해야 합니다. 이 예제에서는 GetObject 작업의 일관성을 "Strong-site"로 설정합니다.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

> PutObject 및 GetObject 작업 모두에 대해 동일한 일관성을 사용해야 합니다.

버킷의 일관성을 지정합니다

버킷의 일관성을 설정하려면 StorageGRID 요청을 사용할 수 "버킷 일관성을 유지합니다"있습니다. 또는 Tenant Manager에서 수행할 수 "버킷의 일관성을 변경합니다"있습니다.

버킷의 일관성을 설정할 때 다음 사항에 유의하십시오.

- 버킷의 일관성을 설정하면 버킷의 오브젝트나 버킷 구성에 수행되는 S3 작업에 사용되는 일관성이 결정됩니다. 버킷 자체의 작동에는 영향을 미치지 않습니다.
- 개별 API 작업의 일관성이 버킷의 일관성을 재정의합니다.
- 일반적으로 버킷은 "Read-after-new-write"라는 기본 일관성을 사용해야 합니다. 요청이 올바르게 작동하지 않는 경우 가능한 경우 응용 프로그램 클라이언트 동작을 변경합니다. 또는 각 API 요청의 일관성을 지정하도록 클라이언트를 구성합니다. 버킷 수준의 일관성을 마지막 수단으로 설정합니다.

일관성 및 ILM 규칙이 데이터 보호에 영향을 미치는 방식

일관성을 선택하고 ILM 규칙을 따르는 것은 오브젝트가 보호되는 방식에 영향을 미칩니다. 이러한 설정은 상호 작용할 수 있습니다.

예를 들어, 오브젝트가 저장될 때 사용되는 일관성은 오브젝트 메타데이터의 초기 배치에 영향을 주고, ILM 규칙에 대해 선택된 수집 동작은 오브젝트 복사본의 초기 배치에 영향을 미칩니다. StorageGRID에서는 클라이언트 요청을 이행하기 위해 오브젝트의 메타데이터와 해당 데이터에 모두 액세스해야 하므로 일관성 및 수집 동작에 대해 일치하는 보호 수준을 선택하면 초기 데이터 보호 수준을 높이고 시스템 응답을 보다 예측 가능하게 할 수 있습니다.

ILM 규칙에 사용할 수 있는 항목은 다음과 "수집 옵션"같습니다.

이중 커밋

StorageGRID는 즉시 개체의 중간 복사본을 만들고 클라이언트에 성공을 반환합니다. ILM 규칙에 지정된 복사본은 가능한 경우 만들어집니다.

엄격한

ILM 규칙에 지정된 모든 복제본이 클라이언트에 반환되기 전에 만들어져야 합니다.

균형

StorageGRID는 수집 시 ILM 규칙에 지정된 모든 복제본을 만들려고 합니다. 이 작업이 불가능할 경우 중간 복제본이 만들어지고 성공이 클라이언트에 반환됩니다. ILM 규칙에 지정된 복사본은 가능한 경우 만들어집니다.

일관성과 **ILM** 규칙이 상호 작용하는 방법의 예

다음과 같은 ILM 규칙과 다음과 같은 일관성이 있는 2개 사이트 그리드가 있다고 가정합니다.

- * ILM 규칙 *: 로컬 사이트와 원격 사이트에 각각 하나씩, 두 개의 오브젝트 복사본을 만듭니다. 엄격한 수집 동작을 사용합니다.
- * Consistency *: 강력한 글로벌(오브젝트 메타데이터는 모든 사이트에 즉시 배포됨).

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 규칙과 강력한 사이트 일관성을 사용한 경우 개체 데이터가 원격 사이트에 복제된 후 개체 메타데이터가 이 사이트에 배포되기 전에 클라이언트에서 성공 메시지를 받을 수 있습니다. 이 경우 오브젝트 메타데이터의 보호 수준이 오브젝트 데이터의 보호 수준과 일치하지 않습니다. 수집 후 곧바로 로컬 사이트가 손실되면 오브젝트 메타데이터가 손실됩니다. 개체를 검색할 수 없습니다.

일관성과 ILM 규칙 간의 상호 관계는 복잡할 수 있습니다. 도움이 필요하면 NetApp에 문의하십시오.

오브젝트 버전 관리

각 오브젝트의 여러 버전을 유지하려면 버킷의 버전 관리 상태를 설정할 수 있습니다. 버킷에 대한 버전 관리를 사용하면 실수로 개체가 삭제되지 않도록 보호하고 이전 버전의 개체를 검색 및 복원할 수 있습니다.

StorageGRID 시스템은 대부분의 기능을 지원하는 버전 관리를 구현하지만 몇 가지 제한 사항이 있습니다. StorageGRID는 각 오브젝트의 버전을 최대 10,000개까지 지원합니다.

오브젝트 버전 관리를 StorageGRID ILM(정보 라이프사이클 관리) 또는 S3 버킷 라이프사이클 구성과 결합할 수 있습니다. 각 버킷에 대해 버전 관리를 명시적으로 설정해야 합니다. 버킷에 대해 버전 관리를 사용하도록 설정하면 버킷에 추가된 각 오브젝트에 버전 ID가 할당되며, StorageGRID 시스템에서 생성됩니다.

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 관리 지원 버킷의 S3 객체의 경우 버전 관리 지원을 통해 "현재 시간"을 참조 시간으로 사용하는 ILM 규칙을 만들 수 있습니다(의 "이전 객체 버전에만 이 규칙을 적용하시겠습니까?"라는 질문에 대해 * 예 * 를 선택"ILM 규칙 만들기 마법사의 1단계"). 개체가 업데이트되면 이전 버전은 업데이트되지 않습니다. "비현재 시간" 필터를 사용하면 이전 버전의 객체가 스토리지에 미치는 영향을 줄이는 정책을 만들 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.

관련 정보

- "S3 버전 오브젝트 삭제 방법"
- "S3 버전 오브젝트 ILM 규칙 및 정책(예 4)"..

S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다

StorageGRID 시스템에서 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 S3 오브젝트 잠금이 활성화된 버킷을 생성할 수 있습니다. 각 오브젝트 버전에 대해 각 버킷의 기본 보존 또는 보존 설정을 지정할 수 있습니다.

버킷에 대해 S3 오브젝트 잠금을 활성화하는 방법

StorageGRID 시스템에 대해 글로벌 S3 오브젝트 잠금 설정이 활성화된 경우 각 버킷을 생성할 때 선택적으로 S3 오브젝트 잠금을 활성화할 수 있습니다.

S3 오브젝트 잠금은 버킷을 생성할 때만 활성화할 수 있는 영구 설정입니다. 버킷을 생성한 후에는 S3 오브젝트 잠금을 추가하거나 비활성화할 수 없습니다.

버킷에 대해 S3 오브젝트 잠금을 설정하려면 다음 방법 중 하나를 사용하십시오.

- 테넌트 관리자를 사용하여 버킷을 생성합니다. 을 "S3 버킷을 생성합니다"참조하십시오.
- 요청 헤더가 있는 CreateBucket 요청을 사용하여 버킷을 `x-amz-bucket-object-lock-enabled` 만듭니다. 을 "버킷 작업"참조하십시오.

S3 오브젝트 잠금에서는 버킷 버전 관리가 필요하며, 이 버전은 버킷을 생성할 때 자동으로 활성화됩니다. 버킷의 버전 관리는 일시 중단할 수 없습니다. 을 "오브젝트 버전 관리"참조하십시오.

버킷의 기본 보존 설정입니다

버킷에 대해 S3 오브젝트 잠금이 활성화된 경우 버킷에 대한 기본 보존을 선택적으로 설정하고 기본 보존 모드 및 기본 보존 기간을 지정할 수 있습니다.

기본 보존 모드

- 규정 준수 모드:
  - 보존 기한 에 도달할 때까지 개체를 삭제할 수 없습니다.
  - 오브젝트의 보존 기한 을 늘릴 수 있지만 줄일 수는 없습니다.
  - 개체의 보존 기한 은 해당 날짜에 도달할 때까지 제거할 수 없습니다.
- 거버넌스 모드:
  - 있는 사용자는 `s3:BypassGovernanceRetention`권한이 요청 헤더를 사용하여 보존 설정을 무시할 수 `x-amz-bypass-governance-retention: true` 있습니다.
  - 이러한 사용자는 보존 기한이 되기 전에 개체 버전을 삭제할 수 있습니다.
  - 이러한 사용자는 개체의 보존 기간(Retain-until-date)을 증가, 감소 또는 제거할 수 있습니다.

기본 보존 기간

각 버킷에는 년 또는 일 단위로 지정된 기본 보존 기간이 있을 수 있습니다.

버킷의 기본 보존 설정 방법

버킷의 기본 보존을 설정하려면 다음 방법 중 하나를 사용합니다.

- 테넌트 관리자에서 버킷 설정을 관리합니다. "S3 버킷을 생성합니다"및 을 "S3 오브젝트 잠금 기본 보존 업데이트 "참조하십시오.
- 버킷에 대한 PutObjectLockConfiguration 요청을 실행하여 기본 모드와 기본 일 또는 년 수를 지정합니다.

PutObjectLockConfiguration 을 참조하십시오

PutObjectLockConfiguration 요청을 사용하면 S3 오브젝트 잠금이 설정된 버킷의 기본 보존 모드 및 기본 보존 기간을 설정하고 수정할 수 있습니다. 이전에 구성한 기본 보존 설정을 제거할 수도 있습니다.

새 오브젝트 버전이 버킷에 수집되면 및 `x-amz-object-lock-retain-until-date` 이 지정되지 않은 경우 기본 보존 모드가 `x-amz-object-lock-mode` 적용됩니다. 이 지정되지 않은 경우 기본 보존 기간은 유지 종료 날짜를 계산하는 데 `x-amz-object-lock-retain-until-date` 사용됩니다.

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 권한이 있거나 계정 루트여야 `s3:PutBucketObjectLockConfiguration` 합니다.

`Content-MD5`PUT 요청에 요청 헤더를 지정해야 합니다.

요청 예

이 예에서는 버킷에 대해 S3 Object Lock을 설정하고 기본 보존 모드를 규정 준수 로 설정하고 기본 보존 기간을 6년으로 설정합니다.

```
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>
```

버킷의 기본 보존 결정 방법

버킷에 대해 S3 오브젝트 잠금이 설정되었는지 확인하고 기본 보존 모드 및 보존 기간을 확인하려면 다음 방법 중 하나를 사용하십시오.

- 테넌트 관리자에서 버킷을 확인합니다. 을 "S3 버킷을 봅니다"참조하십시오.
- GetObjectLockConfiguration 요청을 실행합니다.

GetObjectLockConfiguration 을 참조하십시오

GetObjectLockConfiguration 요청을 사용하면 버킷에 대해 S3 오브젝트 잠금이 설정되어 있는지 확인하고, 사용하도록 설정되어 있는 경우 버킷에 대해 구성된 기본 보존 모드 및 보존 기간이 있는지 확인할 수 있습니다.

새 오브젝트 버전이 버킷에 수집되면 이 지정되지 않은 경우 기본 보존 모드가 `x-amz-object-lock-mode` 적용됩니다. 이 지정되지 않은 경우 기본 보존 기간은 유지 종료 날짜를 계산하는 데 `x-amz-object-lock-retain-until-date` 사용됩니다.

이 작업을 완료하려면 권한이 있거나 계정 루트여야 `s3:GetBucketObjectLockConfiguration` 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>
```

개체의 보존 설정을 지정하는 방법

S3 오브젝트 잠금이 활성화된 버킷에는 S3 오브젝트 잠금 보존 설정이 있는 오브젝트와 없는 오브젝트의 조합이 포함될 수 있습니다.

오브젝트 레벨의 보존 설정은 S3 REST API를 사용하여 지정됩니다. 객체에 대한 보존 설정은 버킷의 기본 보존 설정보다 우선합니다.

각 개체에 대해 다음 설정을 지정할 수 있습니다.

- * 보존 모드 *: 규정 준수 또는 거버넌스 중 하나입니다.
- * Retain-until-date *: StorageGRID에서 개체 버전을 유지해야 하는 기간을 지정하는 날짜입니다.
  - 준수 모드에서 보존 기한이 미래인 경우 오브젝트를 검색할 수 있지만 수정하거나 삭제할 수 없습니다. 보관 기한 을 늘릴 수 있지만 이 날짜는 감소 또는 제거할 수 없습니다.

◦ 거버넌스 모드에서 특별 권한이 있는 사용자는 보존 기한 설정을 무시할 수 있습니다. 보존 기간이 경과하기 전에 객체 버전을 삭제할 수 있습니다. 또한 보존 기간을 늘리거나 줄이거나 제거할 수도 있습니다.

- * 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.

  개체에 대한 법적 보류 설정은 보존 모드 및 보존 기한 과 무관합니다. 개체 버전이 법적 증거 자료 보관 중인 경우 해당 버전을 삭제할 수 없습니다.

오브젝트 버전을 버킷에 추가할 때 S3 오브젝트 잠금 설정을 지정하려면"PutObject 를 선택합니다", 를 실행하거나 "CopyObject 를 선택합니다" "CreateMultptUpload 를 클릭합니다"요청을 실행하십시오.

다음을 사용할 수 있습니다.

- `x-amz-object-lock-mode`규정 준수 또는 거버넌스일 수 있습니다(대소문자 구분).

  을 지정한 `x-amz-object-lock-mode` 경우에는 도 지정해야 `x-amz-object-lock-retain-until-date`합니다.

- `x-amz-object-lock-retain-until-date`
  - 유지 기한 값은 형식이어야 `2020-08-10T21:46:00Z`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.

- `Content-MD5`요청 헤더가 `PutObject` 요청에 있는 경우 요청 `x-amz-object-lock-*` 헤더가 필요합니다. `Content-MD5` CopyObject 또는 CreateMultipartUpload에는 필요하지 않습니다.
- 버킷에 S3 오브젝트 잠금이 설정되어 있지 않고 요청 헤더가 있는 경우 `x-amz-object-lock-*` 400 Bad Request(InvalidRequest) 오류가 반환됩니다.
- PutObject 요청에서는 AWS 동작을 일치시키기 위해 의 사용을 `x-amz-storage-class: REDUCED_REDUNDANCY` 지원합니다. 하지만 오브젝트가 S3 오브젝트 잠금이 설정된 버킷으로 수집되면 StorageGRID는 항상 이중 커밋 수집을 수행합니다.
- 이후의 Get 또는 HeadObject 버전 응답에는 헤더 `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date` 및 `x-amz-object-lock-legal-hold`, 구성된 경우 요청 보낸 사람에게 올바른 권한이 있는지 여부가 `s3:Get*` 포함됩니다.

정책 조건 키를 사용하여 개체에 대해 허용되는 최소 및 최대 보존 기간을 제한할 수 `s3:object-lock-remaining-retention-days` 있습니다.

개체의 보존 설정을 업데이트하는 방법

기존 개체 버전에 대한 법적 증거 자료 보관 또는 보존 설정을 업데이트해야 하는 경우 다음 개체 하위 리소스 작업을 수행할 수 있습니다.

- `PutObjectLegalHold`

  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.

- `PutObjectRetention`
  - 모드 값은 규정 준수 또는 거버넌스(대/소문자 구분)일 수 있습니다.
  - 유지 기한 값은 형식이어야 `2020-08-10T21:46:00Z`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.

거버넌스 모드 사용 방법

권한이 있는 사용자는 `s3:BypassGovernanceRetention` 거버넌스 모드를 사용하는 개체의 활성 보존 설정을 무시할 수 있습니다. 삭제 또는 PutObjectRetention 작업은 요청 헤더를 포함해야 `x-amz-bypass-governance-retention:true` 합니다. 이러한 사용자는 다음과 같은 추가 작업을 수행할 수 있습니다.

- DeleteObject 또는 DeleteObjects 작업을 수행하여 보존 기간이 경과하기 전에 개체 버전을 삭제합니다.

  법적 증거 자료 보관 중인 객체는 삭제할 수 없습니다. 법적 증거 자료 보관 기능을 해제해야 합니다.

- 개체의 보존 기간이 경과하기 전에 개체 버전의 모드를 거버넌스에서 규정 준수로 변경하는 PutObjectRetention 작업을 수행합니다.

  규정 준수 모드를 거버넌스로 변경하는 것은 허용되지 않습니다.

- PutObjectRetention 작업을 수행하여 개체 버전의 보존 기간을 증가, 감소 또는 제거합니다.

관련 정보

- "S3 오브젝트 잠금으로 오브젝트 관리"
- "S3 오브젝트 잠금을 사용하여 오브젝트를 보존합니다"
- "Amazon Simple Storage Service 사용자 가이드: 오브젝트 잠금"

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 사용자 가이드: 객체 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

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

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.

- DeleteBucketLifecycle
- GetBuckLifecycleConfiguration 을 참조하십시오
- PutBucketLifecycleConfiguration을 참조하십시오

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/ `key2` 와 일치하고 값이 인 `tag2` 개체에만 `category1` 적용됩니다. `Expiration`매개 변수는 필터와 일치하는 개체가 2020년 8월 22일 자정에 만료되도록 지정합니다.
2. 규칙 2는 접두사/ 과 일치하는 개체에만 `category2` 적용됩니다. `Expiration`매개 변수는 필터와 일치하는 개체가 수집된 후 100일 후에 만료되도록 지정합니다.

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

3. 규칙 3은 접두사/ 과 일치하는 개체에만 `category3` 적용됩니다. `Expiration`매개 변수는 일치하는 개체의 현재 버전이 아닌 경우 50일 후에 만료되도록 지정합니다.

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

버킷에 라이프사이클 구성을 적용합니다

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

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

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

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

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

성공적으로 응답하면 방금 적용한 문서 수정 상태 설정이 나열됩니다.

버킷 수명 주기 만료가 객체에 적용되는지 확인합니다

PutObject, HeadObject 또는 GetObject 요청을 실행할 때 수명 주기 구성의 만료 규칙이 특정 개체에 적용되는지 여부를 확인할 수 있습니다. 규칙이 적용되는 경우 응답에는 `Expiration` 개체가 만료되는 시점과 일치하는 만료 규칙을 나타내는 매개 변수가 포함됩니다.

> 버킷 수명 주기가 ILM을 재정의하기 때문에 `expiry-date` 표시된 날짜는 오브젝트가 삭제될 실제 날짜입니다. 자세한 내용은 을 참조하십시오 "개체 보존이 결정되는 방식".

예를 들어, 이 PutObject 요청은 2020년 6월 22일에 발행되었으며 버킷에 객체를 `testbucket` 배치합니다.

```
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 HeadObject 요청은 testbucket의 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": {}
}
```

버전 관리를 사용하는 버킷의 경우 `x-amz-expiration` 응답 헤더는 현재 버전의 객체에만 적용됩니다.

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 존재할 것으로 예상하지 않는 경로에 개체가 있는지 정기적으로 확인하는 경우 "사용 가능"을 사용해야 "정합성"합니다. 예를 들어, 응용 프로그램이 해당 위치에 배치하기 전에 해당 위치를 헤딩하는 경우 "사용 가능한" 일관성을 사용해야 합니다.

그렇지 않으면 헤드 작업에서 객체를 찾지 못할 경우 같은 사이트에 있는 두 개 이상의 스토리지 노드를 사용할 수 없거나 원격 사이트에 연결할 수 없는 경우 500개의 내부 서버 오류가 발생할 수 있습니다.

요청을 사용하여 각 버킷에 대해 "사용 가능한" 일관성을 설정하거나 개별 API 작업에 대한 요청 헤더에서 일관성을 지정할 수 "버킷 일관성을 유지합니다"있습니다.

개체 키에 대한 권장 사항

버킷이 처음 생성된 시점을 기준으로 오브젝트 키 이름에 대한 다음 권장 사항을 따르십시오.

StorageGRID 11.4 또는 이전 버전에서 생성된 버킷

- 개체 키의 처음 네 문자로 임의 값을 사용하지 마십시오. 이는 이전 AWS에서 권장하는 키 접두사와 다릅니다. 대신 와 같이 고유하지 않은 임의 접두사를 사용합니다 `image`.
- 이전 AWS 권장 사항에 따라 키 접두사에 랜덤 및 고유 문자를 사용하려면 오브젝트 키에 디렉토리 이름이 접두사로 지정됩니다. 즉, 다음 형식을 사용합니다.

  `mybucket/mydir/f8e3-image3132.jpg`

이 형식 대신:

```
mybucket/f8e3-image3132.jpg
```

StorageGRID 11.4 이상에서 생성된 버킷

성능 모범 사례에 맞게 개체 키 이름을 제한하는 것은 필요하지 않습니다. 대부분의 경우 개체 키 이름의 처음 4개 문자에 임의의 값을 사용할 수 있습니다.

> 단, 짧은 시간 내에 모든 오브젝트를 지속적으로 제거하는 S3 워크로드가 예외입니다. 이 사용 사례에 대한 성능 영향을 최소화하려면 키와 같은 1000개의 오브젝트마다 주요 이름의 앞부분을 다르게 지정해야 합니다. 예를 들어, S3 클라이언트가 일반적으로 초당 2,000개의 오브젝트를 기록하고 ILM 또는 버킷 라이프사이클 정책에 따라 3일 후에 모든 오브젝트를 제거한다고 가정해 보겠습니다. 성능에 미치는 영향을 최소화하기 위해 다음과 같은 패턴을 사용하여 키의 이름을 지정할 수 있습니다.
>
> `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

"범위 읽기"에 대한 권장 사항

이 설정된 경우 "저장된 개체를 압축하는 전역 옵션"S3 클라이언트 응용 프로그램은 반환되는 바이트 범위를 지정하는 GetObject 작업을 수행하지 않아야 합니다. 이러한 "범위 읽기" 작업은 StorageGRID에서 요청된 바이트에 액세스하기 위해 개체의 압축을 효과적으로 해제해야 하기 때문에 비효율적입니다. 매우 큰 개체에서 작은 범위의 바이트를 요청하는 GetObject 작업은 특히 비효율적입니다. 예를 들어, 50GB의 압축된 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.

Amazon S3 REST API 지원

S3 REST API 구현 세부 정보

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 헤더를 포함하면 `x-amz-date` 날짜 요청 헤더에 지정된 모든 값이 재정의됩니다. AWS Signature 버전 4를 사용할 `x-amz-date` 경우 날짜 헤더가 지원되지 않으므로 서명된 요청에 헤더가 있어야 합니다.

공통 요청 헤더

StorageGRID 시스템은 한 가지 예외를 제외하고 에서 정의한 일반 요청 헤더를 "Amazon Simple Storage Service API 참조: 일반 요청 헤더" 지원합니다.

요청 헤더	구축
권한 부여	AWS Signature 버전 2에 대한 전체 지원 다음 경우를 제외하고 AWS Signature 버전 4 지원: • 에서 실제 페이로드 체크섬 값을 `x-amz-content-sha256` 제공하면 헤더에 값이 제공된 것처럼 값이 유효성 검사 없이 수락됩니다. `UNSIGNED-PAYLOAD` 스트리밍을 의미하는 헤더 값 `aws-chunked`(예: streaming-AWS4-HMAC-SHA256 페이로드)을 제공하면 `x-amz-content-sha256` 청크 데이터에 대해 청크 서명이 확인되지 않습니다.
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 헤더와 쿼리 매개 변수 사용이라는 두 가지 인증 방법을 `Authorization` 지원합니다.

HTTP 인증 헤더를 사용합니다

HTTP `Authorization` 헤더는 버킷 정책에서 허용하는 익명 요청을 제외하고 모든 S3 API 작업에서 사용됩니다. `Authorization`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 없으며, 이를 통해 타사에 리소스에 대한 제한된 액세스를 제공할 수 있습니다.

서비스에 대한 작업

StorageGRID 시스템은 서비스에 대해 다음 작업을 지원합니다.

작동	구축
ListBucket (이전 명칭: Get Service)	모든 Amazon S3 REST API 동작으로 구현됩니다. 예고 없이 변경될 수 있습니다.
스토리지 사용량을 가져옵니다	StorageGRID "스토리지 사용량을 가져옵니다"요청에서는 계정에 의해 사용 중인 총 저장소 양과 계정에 연결된 각 버킷에 대해 알려줍니다. 이 작업은 / 의 경로와 사용자 지정 쿼리 매개 변수(`?x-ntap-sg-usage`)가 추가된 서비스에 대한 작업입니다.
옵션 /	클라이언트 애플리케이션은 스토리지 노드의 사용 가능 여부를 확인하기 위해 S3 인증 자격 증명을 제공하지 않고 스토리지 노드의 S3 포트에 요청을 전송할 수 있습니다 `OPTIONS /`. 이 요청을 사용하여 모니터링을 수행하거나, 외부 로드 밸런서가 스토리지 노드가 다운된 시점을 식별하도록 할 수 있습니다.

버킷 작업

StorageGRID 시스템은 각 S3 테넌트 계정에 대해 최대 5,000개의 버킷을 지원합니다.

각 그리드에는 최대 100,000개의 버킷을 포함할 수 있습니다.

5,000개의 버킷을 지원하려면 그리드의 각 스토리지 노드에 최소 64GB의 RAM이 있어야 합니다.

버킷 이름 제한은 AWS US 표준 지역 제한을 따르지만, S3 가상 호스팅 스타일 요청을 지원하기 위해 DNS 명명 규칙으로 제한해야 합니다.

자세한 내용은 다음을 참조하십시오.

- "Amazon Simple Storage Service 사용자 가이드: 버킷 할당량, 제한 및 제한 사항"
- "S3 끝점 도메인 이름을 구성합니다"

ListObjects(Get Bucket) 및 ListObjectVersions(Get Bucket 개체 버전) 작업은 StorageGRID를 "일관성 값 "지원합니다.

개별 버킷에 대해 마지막 액세스 시간에 대한 업데이트가 설정되었는지 여부를 확인할 수 있습니다. 을 "버킷 최종 액세스 시간 가져오기"참조하십시오.

다음 표에서는 StorageGRID에서 S3 REST API 버킷 작업을 구축하는 방법을 설명합니다. 이러한 작업을 수행하려면 계정에 필요한 액세스 자격 증명을 제공해야 합니다.

작동	구축
CreateBucket	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 지역에 생성되지만 `us-east-1` 요청 본문의 요청 요소를 사용하여 다른 영역을 지정할 수 `LocationConstraint` 있습니다. 요소를 사용할 때는 `LocationConstraint` 그리드 관리자 또는 그리드 관리 API를 사용하여 정의된 영역의 정확한 이름을 지정해야 합니다. 사용할 지역 이름을 모르는 경우 시스템 관리자에게 문의하십시오. 참고: CreateBucket 요청이 StorageGRID에 정의되지 않은 영역을 사용하는 경우 오류가 발생합니다. • 요청 헤더를 포함하여 S3 오브젝트 잠금이 설정된 버킷을 생성할 수 `x-amz-bucket-object-lock-enabled` 있습니다. 을 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"참조하십시오. 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.
삭제 버킷	버킷을 삭제합니다.
DeleteBucketCors	버킷에 대한 CORS 구성을 삭제합니다.
DeleteBucketEncryption	버킷에서 기본 암호화를 삭제합니다. 암호화된 기존 개체는 암호화된 상태로 유지되지만 버킷에 추가된 새 개체는 암호화되지 않습니다.
DeleteBucketLifecycle	버킷에서 문서 수정 상태 설정을 삭제합니다. 을 "S3 라이프사이클 구성을 생성합니다 "참조하십시오.
DeleteBuckketPolicy를 참조하십시오	버킷에 연결된 정책을 삭제합니다.

작동	구축
DeleteBuckReplication 을 참조하십시오	버킷에 연결된 복제 구성을 삭제합니다.
삭제 BucketTagging	하위 리소스를 사용하여 `tagging` 버킷에서 모든 태그를 제거합니다. 주의: 이 버킷에 대해 기본값이 아닌 ILM 정책 태그가 설정된 경우 이 버킷에 `NTAP-SG-ILM-BUCKET-TAG` 할당된 값이 있는 버킷 태그가 있습니다. 버킷 태그가 있는 경우 DeleteBucketTagging 요청을 `NTAP-SG-ILM-BUCKET-TAG` 실행하지 마십시오. 대신 태그 및 할당된 값만 사용하여 PutBucketTagging 요청을 `NTAP-SG-ILM-BUCKET-TAG` 실행하여 버킷에서 다른 모든 태그를 제거합니다. 버킷 태그를 수정하거나 제거하지 `NTAP-SG-ILM-BUCKET-TAG` 마십시오.
GetBuckketAcl	양수 응답과 ID, DisplayName 및 버킷 소유자의 사용 권한을 반환합니다. 이는 소유자가 버킷에 대한 모든 액세스 권한을 가지고 있음을 나타냅니다.
GetBuckketCors 를 참조하십시오	버킷의 구성을 반환합니다 `cors`.
GetBuckketEncryption을 참조하십시오	버킷의 기본 암호화 구성을 반환합니다.
GetBuckLifecycleConfiguration 을 참조하십시오 (이전 명칭 Get Bucket 수명주기)	버킷의 수명주기 구성을 반환합니다. 을 "S3 라이프사이클 구성을 생성합니다 "참조하십시오.
GetBucketLocation 을 참조하십시오	CreateBucket 요청에서 요소를 사용하여 설정한 영역을 반환합니다 `LocationConstraint`. 버킷의 영역이 인 경우 `us-east-1` 영역에 대해 빈 문자열이 반환됩니다.
GetBuckNotificationConfiguration 을 참조하십시오 (이전 명칭 Get Bucket 알림)	버킷에 연결된 알림 구성을 반환합니다.
GetBuckketPolicy를 참조하십시오	버킷에 연결된 정책을 반환합니다.
GetBucketReplication 을 참조하십시오	버킷에 연결된 복제 구성을 반환합니다.

작동	구축
GetBucketTagging	하위 리소스를 사용하여 `tagging` 버킷의 모든 태그를 반환합니다. 주의: 이 버킷에 대해 기본값이 아닌 ILM 정책 태그가 설정된 경우 이 버킷에 `NTAP-SG-ILM-BUCKET-TAG` 할당된 값이 있는 버킷 태그가 있습니다. 이 태그를 수정하거나 제거하지 마십시오.
GetBuckketVersioning 을 참조하십시오	이 구현에서는 하위 리소스를 사용하여 `versioning` 버킷의 버전 관리 상태를 반환합니다. • *blank*: 버전 관리가 활성화되지 않았습니다(버킷이 "버전 없음"). • 사용: 버전 관리가 활성화됩니다 • 일시 중단됨: 버전 관리가 이전에 활성화되었으며 일시 중단되었습니다
GetObjectLockConfiguration 을 참조하십시오	구성된 경우 버킷 기본 보존 모드와 기본 보존 기간을 반환합니다. 을 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"참조하십시오.
머리버킷	버킷이 존재하는지, 버킷에 액세스할 수 있는 권한이 있는지 확인합니다. 이 작업은 다음을 반환합니다. • `x-ntap-sg-bucket-id`: UUID 형식의 버킷의 UUID입니다. • `x-ntap-sg-trace-id`: 연결된 요청의 고유한 추적 ID입니다.
ListObjects 및 ListObjectsV2 를 참조하십시오 (이전 명칭 Get Bucket)	버킷에 있는 오브젝트의 일부 또는 전체(최대 1,000개)를 반환합니다. 객체에 대한 스토리지 클래스는 스토리지가 스토리지 클래스 옵션으로 수집된 경우에도 두 값 중 하나를 가질 수 있습니다. `REDUCED_REDUNDANCY` • `STANDARD`객체가 스토리지 노드로 구성된 스토리지 풀에 저장되었음을 나타냅니다. • `GLACIER`- 클라우드 스토리지 풀에 지정된 외부 버킷으로 오브젝트가 이동되었음을 나타냅니다. 버킷에 접두사가 같은 삭제된 키가 많은 경우 키가 포함되지 않은 키가 응답에 포함될 수 `CommonPrefixes` 있습니다.
ListObjectVersions 를 선택합니다 (이전에 명명된 Get Bucket Object 버전)	버킷에서 읽기 권한을 가진 경우 이 작업을 하위 리소스와 함께 `versions` 사용하면 버킷에 있는 모든 오브젝트 버전의 메타데이터가 나열됩니다.

작동	구축
BuckketCors의	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, 이라는 S3 버킷을 사용하여 그래픽을 저장한다고 가정해 `images` 보겠습니다. 버킷에 대한 CORS 구성을 설정하면 `images` 해당 버킷의 이미지가 웹사이트에 표시되도록 할 수 `http://www.example.com` 있습니다.
PutBucketEncryption을 참조하십시오	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. 서버측 암호화 구성 규칙을 지정할 때 매개 변수를 로 `AES256` 설정하고 `SSEAlgorithm` 매개 변수를 사용하지 마십시오 `KMSMasterKeyID`. 객체 업로드 요청이 이미 암호화를 지정한 경우(즉, 요청에 요청 헤더가 포함된 경우) 버킷 기본 암호화 구성은 `x-amz-server-side-encryption-*` 무시됩니다.
PutBucketLifecycleConfiguration을 참조하십시오 (이전에 명명된 Put Bucket 수명 주기)	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, ExpiredObjectDeleteMarker) • 비currentVersionExpiration(NewerNoncurrentVersions, NoncurrentDays) • 필터(접두사, 태그) • 상태 • ID입니다 StorageGRID는 다음 작업을 지원하지 않습니다. • AbortIncompleteMultipartUpload를 중단합니다 • 전환 을 "S3 라이프사이클 구성을 생성합니다"참조하십시오. 버킷 수명 주기의 만료 작업이 ILM 배치 지침과 상호 작용하는 방식을 이해하려면 을 참조하십시오."ILM이 개체 수명 전반에 걸쳐 작동하는 방식" • 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

PutBucketNotificationConfiguration을 참조하십시오
 	
(이전에 명명된 Put Bucket 알림)
	요청 본문에 포함된 알림 구성 XML을 사용하여 버킷에 대한 알림을 구성합니다. 다음과 같은 구현 세부 사항에 유의해야 합니다.
	
	• StorageGRID는 Amazon SNS(Simple Notification Service) 또는 Kafka 토픽을 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 `400 Bad Request` 코드와 함께 오류가 `InvalidArgument` 반환됩니다.
	
	• 다음 이벤트 유형에 대한 알림을 구성할 수 없습니다. 이러한 이벤트 유형은 * 지원되지 않습니다 *.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• StorageGRID에서 보낸 이벤트 알림은 다음 목록에 표시된 것처럼 일부 키를 포함하지 않고 다른 키에 대해 특정 값을 사용한다는 점을 제외하고 표준 JSON 형식을 사용합니다.
	◦ * eventSource * 를 선택합니다
	
	`sgws:s3`
	
	◦ * awsRegion *
	
	포함되지 않음
	
	◦ x-amz-id-2 *
	
	포함되지 않음
	
	◦ * 표시 *
	
	`urn:sgws:s3:::bucket_name`

BucketPolicy를 참조하십시오	버킷에 연결된 정책을 설정합니다. 을 "버킷 및 그룹 액세스 정책을 사용합니다 "참조하십시오.

작동	구축
PutBucketReplication을 참조하십시오	"StorageGRID CloudMirror 복제"요청 본문에 제공된 복제 구성 XML을 사용하여 버킷을 구성합니다. CloudMirror 복제의 경우 다음과 같은 구축 세부 정보를 알고 있어야 합니다. • StorageGRID는 복제 구성의 V1만 지원합니다. 즉, StorageGRID는 규칙에 요소 사용을 지원하지 `Filter` 않으며 객체 버전을 삭제하기 위한 V1 규칙을 따릅니다. 자세한 내용은 을 참조하십시오 "Amazon Simple Storage Service 사용 설명서: 복제 구성". • 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. 을 "CloudMirror 복제를 구성합니다 "참조하십시오. 복제 구성이 성공하려면 엔드포인트가 있어야 합니다. 끝점이 없으면 요청이 A로 실패합니다 `400 Bad Request`. 오류 메시지는 다음과 같습니다. `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • 구성 XML에서 을 지정할 `Role` 필요는 없습니다. 이 값은 StorageGRID에서 사용되지 않으며 제출될 경우 무시됩니다. • 구성 XML에서 스토리지 클래스를 생략하면 StorageGRID에서는 `STANDARD` 기본적으로 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 통지되지 않습니다. ◦ 복제된 후 오브젝트 또는 버킷을 삭제하면 StorageGRID는 지역 간 복제 V1에 대한 표준 Amazon S3 삭제 동작을 따릅니다.

작동	구축
BucketTagging	에서는 하위 리소스를 사용하여 `tagging` 버킷의 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. 주의: 이 버킷에 대해 기본값이 아닌 ILM 정책 태그가 설정된 경우 이 버킷에 `NTAP-SG-ILM-BUCKET-TAG` 할당된 값이 있는 버킷 태그가 있습니다. `NTAP-SG-ILM-BUCKET-TAG`버킷 태그가 모든 PutBucketTagging 요청에 할당된 값과 함께 포함되어 있는지 확인합니다. 이 태그를 수정하거나 제거하지 마십시오. 참고: 이 작업은 버킷에 이미 있는 현재 태그를 덮어씁니다. 기존 태그를 세트에서 생략하면 해당 태그가 버킷에 대해 제거됩니다.
PutBucketVersioning을 참조하십시오	하위 리소스를 사용하여 `versioning` 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 객체는 버전 ID를 `null`받습니다.
PutObjectLockConfiguration 을 참조하십시오	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. 자세한 내용은 을 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다 "참조하십시오.

객체에 대한 작업

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 값"는 다음과 같은 경우를 제외하고 개체의 모든 작업에서 지원됩니다.
  - GetObjectAcl
  - `OPTIONS /`

- PutObjectLegalHold를 선택합니다
- PutObjectRetention
- SelectObjectContent 를 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
DeleteObject 를 클릭합니다	MFA(다중 요소 인증) 및 응답 헤더는 `x-amz-mfa` 지원되지 않습니다. DeleteObject 요청을 처리할 때 StorageGRID는 저장된 모든 위치에서 개체의 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 하고 하위 리소스를 사용해야 `versionId` 합니다. 이 하위 리소스를 사용하면 버전이 영구적으로 삭제됩니다. 가 삭제 마커에 해당하는 경우 `versionId` 응답 헤더는 `x-amz-delete-marker` 로 설정된 상태로 `true`반환됩니다. • 버전 관리가 활성화된 버킷에서 하위 리소스 없이 오브젝트를 삭제하면 `versionId` 삭제 마커가 생성됩니다. 응답 헤더를 `x-amz-delete-marker` 사용하여 삭제 마커에 대한 를 `versionId` 반환하고 `x-amz-version-id` 응답 헤더를 로 반환한다. `true` • 버전 관리가 일시 중지된 버킷에서 하위 리소스 없이 개체를 삭제하면 `versionId` 기존 'null' 버전 또는 'null' 삭제 마커가 영구적으로 삭제되고 새 'null' 삭제 마커가 생성됩니다. `x-amz-delete-marker`응답 헤더가 로 설정된 `true` 상태로 반환됩니다. • 참고 *: 경우에 따라 객체에 대해 여러 개의 삭제 마커가 존재할 수 있습니다. 거버넌스 모드에서 개체 버전을 삭제하는 방법은 을 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"참조하십시오.

작동	구축
DeleteObjects 를 클릭합니다 (이전에 이름이 여러 개체 삭제)	MFA(다중 요소 인증) 및 응답 헤더는 `x-amz-mfa` 지원되지 않습니다. 동일한 요청 메시지에서 여러 객체를 삭제할 수 있습니다. 거버넌스 모드에서 개체 버전을 삭제하는 방법은 을 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"참조하십시오.
DeleteObjectTagging 을 선택합니다	에서는 하위 리소스를 사용하여 `tagging` 개체에서 모든 태그를 제거합니다. 버전 관리 쿼리 매개 변수가 요청에 지정되지 않은 경우 `versionId` 작업은 버전 버킷의 가장 최신 버전의 객체에서 모든 태그를 삭제합니다. 개체의 현재 버전이 삭제 표식이면 응답 헤더가 로 설정된 `true` 상태로 "MethodNotAllowed" 상태가 `x-amz-delete-marker` 반환됩니다.
GetObject 를 참조하십시오	"GetObject 를 참조하십시오"
GetObjectAcl	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.
GetObjectLegalHold 를 참조하십시오	"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
GetObjectRetention을 참조하십시오	"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
GetObjectTagging	에서는 하위 리소스를 사용하여 `tagging` 개체의 모든 태그를 반환합니다. 버전 관리 쿼리 매개 변수가 요청에 지정되지 않은 경우 `versionId` 작업은 버전이 지정된 버킷에 있는 가장 최신 버전의 객체에서 모든 태그를 반환합니다. 개체의 현재 버전이 삭제 표식이면 응답 헤더가 로 설정된 `true` 상태로 "MethodNotAllowed" 상태가 `x-amz-delete-marker` 반환됩니다.
HeadObject 를 선택합니다	"HeadObject 를 선택합니다"
RestoreObject 를 선택합니다	"RestoreObject 를 선택합니다"
PutObject 를 선택합니다	"PutObject 를 선택합니다"
CopyObject 를 선택합니다 (이전에 명명된 Put Object - Copy)	"CopyObject 를 선택합니다"

작동	구축
PutObjectLegalHold를 선택합니다	"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
PutObjectRetention	"S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
PutObjectTagging	에서는 하위 리소스를 사용하여 `tagging` 기존 개체에 태그 집합을 추가합니다. 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 PutObjectTagging을 사용하여 개체의 태그를 업데이트하는 경우 StorageGRID는 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 쿼리 매개 변수가 요청에 지정되지 않은 경우 `versionId` 작업은 버전이 지정된 버킷에서 가장 최신 버전의 객체에 태그를 추가합니다. 개체의 현재 버전이 삭제 표식이면 응답 헤더가 로 설정된 `true` 상태로 "MethodNotAllowed" 상태가 `x-amz-delete-marker` 반환됩니다.
SelectObjectContent 를 선택합니다	"SelectObjectContent 를 선택합니다"

S3 Select를 사용합니다

StorageGRID는 에 대해 다음과 같은 Amazon S3 Select 절, 데이터 형식 및 연산자를 "SelectObjectContent 명령"지원합니다.

목록에 없는 항목은 지원되지 않습니다.

구문은 을 참조하십시오"SelectObjectContent 를 선택합니다". S3 Select에 대한 자세한 내용은 를 "S3 Select용 AWS 문서" 참조하십시오.

S3 Select가 활성화된 테넌트 계정만 SelectObjectContent 쿼리를 실행할 수 있습니다. 를 "S3 Select 사용에 대한 고려 사항 및 요구 사항"참조하십시오.

절을 참조하십시오

- 목록을 선택합니다
- FROM 절
- 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;=.(&G
- =
- =
- 를 누릅니다
- !=
- 사이
- 인치

패턴 일치 연산자

- 좋아요
- _
- %

단일 작업자

- NULL입니다
- NULL이 아닙니다

수학 연산자

- 를 누릅니다
- -
- *
- /
- %

StorageGRID는 Amazon 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-server-side-encryption
```

SSE 요청 헤더는 다음 오브젝트 작업에서 지원됩니다.

- "PutObject 를 선택합니다"
- "CopyObject 를 선택합니다"
- "CreateMultptUpload 를 클릭합니다"

SSE-C를 사용합니다

관리하는 고유 키로 개체를 암호화하려면 다음 세 가지 요청 헤더를 사용합니다.

요청 헤더	설명
`x-amz-server-side-encryption-customer-algorithm`	암호화 알고리즘을 지정합니다. 헤더 값은 `AES256` 이어야 합니다.
`x-amz-server-side-encryption-customer-key`	개체를 암호화하거나 해독하는 데 사용할 암호화 키를 지정합니다. 키의 값은 256비트 base64로 인코딩되어야 합니다.
`x-amz-server-side-encryption-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.

- "GetObject 를 참조하십시오"
- "HeadObject 를 선택합니다"
- "PutObject 를 선택합니다"
- "CopyObject 를 선택합니다"
- "CreateMultptUpload 를 클릭합니다"
- "업로드 파트"
- "업로드파트 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 모든 요청을 거부합니다. 보안을 위해 http를 사용하여 실수로 보낸 모든 키가 손상되는 것을 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.

- 버킷에 대해 교차 그리드 복제 또는 CloudMirror 복제가 구성된 경우 SSE-C 객체를 수집할 수 없습니다. 수집 작업이 실패합니다.

관련 정보

"Amazon S3 사용자 가이드: SSE-C(고객 제공 키)와 함께 서버측 암호화 사용"

CopyObject 를 선택합니다

S3 CopyObject 요청을 사용하여 이미 S3에 저장된 개체의 복사본을 만들 수 있습니다. CopyObject 작업은 GetObject 를 수행한 다음 PutObject 를 수행하는 작업과 같습니다.

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 PutObject 작업의 maximum_recommended_size는 5GiB(5,368,709,120바이트)입니다. 5GiB보다 큰 오브젝트가 있는 경우 대신 를 "멀티파트 업로드"사용하십시오.

단일 PutObject 작업의 maximum_supported_size는 5TiB(5,497,558,138,880바이트)입니다.

StorageGRID 11.6 이하에서 업그레이드한 경우 5GiB를 초과하는 객체를 업로드하려고 하면 S3 PUT 개체 크기가 너무 큼 경고가 트리거됩니다. StorageGRID 11.7 또는 11.8을 새로 설치한 경우 경고가 트리거되지 않습니다. 하지만 StorageGRID의 향후 릴리즈에서는 AWS S3 표준에 맞춰 5GiB보다 큰 오브젝트 업로드를 지원하지 않습니다.

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.
- 키 이름 또는 값의 해석된 값에 인쇄할 수 없는 문자가 포함된 경우 StorageGRID는 헤더를 반환하지 `x-amz-missing-meta` 않습니다.

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- `Content-Type`
- `x-amz-copy-source`

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, 그 뒤에 사용자 정의 메타데이터를 포함하는 이름-값 쌍이 옵니다
- `x-amz-metadata-directive`: 기본값은 로 `COPY`, 개체 및 관련 메타데이터를 복사할 수 있습니다.

  개체를 복사할 때 기존 메타데이터를 덮어쓰도록 지정하거나 개체 메타데이터를 업데이트하도록 지정할 수 `REPLACE` 있습니다.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: 기본값은 로 `COPY`, 개체 및 모든 태그를 복사할 수 있습니다.

  개체를 복사할 때 기존 태그를 덮어쓰도록 지정하거나 태그를 업데이트하도록 지정할 수 `REPLACE` 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 오브젝트 버전 모드와 보존 기간을 계산합니다. 을 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"참조하십시오.

- SSE 요청 헤더:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    을 참조하십시오 서버측 암호화에 대한 요청 헤더

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

  개체를 복사할 때 소스 개체에 체크섬이 있으면 StorageGRID에서 해당 체크섬 값을 새 개체에 복사하지 않습니다. 이 동작은 개체 요청에서 을 사용하려고 하는지 여부에 관계없이 `x-amz-checksum-algorithm` 적용됩니다.

- `x-amz-website-redirect-location`

스토리지 클래스 옵션

`x-amz-storage-class`요청 헤더가 지원되며 일치하는 `ILM` 규칙이 `Dual Commit` 또는 `Balanced`를 사용할 경우 `StorageGRID`에서 생성하는 객체 복제본 수에 영향을 xref:{relative_path}../ilm/data-protection-options-for-ingest.html["수집 옵션"]줍니다.

- `STANDARD`

  (기본값) ILM 규칙이 이중 커밋 옵션을 사용하거나 균형 옵션이 중간 복사본 생성으로 돌아올 때 이중 커밋 수집 작업을 지정합니다.

- `REDUCED_REDUNDANCY`

  ILM 규칙이 이중 커밋 옵션을 사용하거나 균형 옵션이 중간 복사본 생성으로 돌아올 때 단일 커밋 수집 작업을 지정합니다.

  > S3 오브젝트 잠금이 설정된 상태에서 오브젝트를 버킷에 수집하면 `REDUCED_REDUNDANCY` 옵션이 무시됩니다. 오브젝트를 레거시 준수 버킷에 수집하는 경우 `REDUCED_REDUNDANCY` 옵션은 오류를 반환합니다. StorageGRID은 규정 준수 요구 사항이 충족될 수 있도록 항상 이중 커밋 수집을 수행합니다.

CopyObject에서 **x-amz-copy-source** 사용

헤더에 지정된 소스 버킷 및 키가 대상 버킷 및 키와 다른 경우 `x-amz-copy-source` 소스 오브젝트 데이터의 복사본이 대상에 기록됩니다.

소스와 대상이 일치하고 헤더가 로 지정된 `REPLACE` 경우 `x-amz-metadata-directive` 객체의 메타데이터는 요청에 제공된 메타데이터 값으로 업데이트됩니다. 이 경우 StorageGRID는 오브젝트를 다시 수집하지 않습니다. 여기에는 두 가지 중요한 결과가 있습니다.

- 기존 개체를 현재 위치에서 암호화하거나 기존 개체의 암호화를 변경하는 데 CopyObject 를 사용할 수 없습니다. 헤더나 `x-amz-server-side-encryption-customer-algorithm` 헤더를 제공하면 `x-amz-server-side-encryption` StorageGRID는 요청을 거부하고 반환합니다 `XNotImplemented`.
- 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

사용자가 "서버측 암호화를 사용합니다"제공하는 요청 헤더는 소스 개체가 암호화되어 있는지 여부와 대상 개체를 암호화할 계획인지에 따라 달라집니다.

- 소스 객체가 SSE-C(고객 제공 키)를 사용하여 암호화되는 경우 CopyObject 요청에 다음 세 개의 헤더를 포함해야 객체를 해독한 후 복사할 수 있습니다.
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: `AES256` 지정합니다.
  - `x-amz-copy-source-server-side-encryption-customer-key`: 원본 개체를 만들 때 제공한 암호화 키를 지정합니다.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: 원본 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-server-side-encryption-customer-algorithm`: `AES256` 지정합니다.
  - `x-amz-server-side-encryption-customer-key`: 대상 객체에 대한 새 암호화 키를 지정합니다.
  - `x-amz-server-side-encryption-customer-key-MD5`: 새 암호화 키의 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 에 대한 고려 사항을 "서버 측 암호화 사용 "검토하십시오.

- SSE(StorageGRID)에서 관리하는 고유 키를 사용하여 대상 개체(복사본)를 암호화하려는 경우 CopyObject 요청에 다음 헤더를 포함합니다.
  - `x-amz-server-side-encryption`

> `server-side-encryption`개체 값을 업데이트할 수 없습니다. 대신 다음을 사용하여 새 값으로 `x-amz-metadata-directive` 복사본을 `server-side-encryption` 만듭니다 `REPLACE`.

버전 관리

소스 버킷의 버전이 관리되는 경우 헤더를 사용하여 개체의 최신 버전을 복사할 수 `x-amz-copy-source` 있습니다. 개체의 특정 버전을 복사하려면 하위 리소스를 사용하여 복사할 버전을 명시적으로 지정해야 `versionId` 합니다. 대상 버킷의 버전이 지정된 경우 생성된 버전이 `x-amz-version-id` 응답 헤더에 반환됩니다. 대상 버킷에 대한 버전 관리가 일시 중단된 경우 `x-amz-version-id` "null" 값이 반환됩니다.

GetObject 를 참조하십시오

S3 GetObject 요청을 사용하여 S3 버킷에서 객체를 검색할 수 있습니다.

GetObject 및 multipart 개체

요청 매개변수를 사용하여 멀티파트나 분할된 오브젝트의 특정 부분을 검색할 수 partNumber 있습니다. `x-amz-mp-parts-count`응답 요소는 개체의 파트 수를 나타냅니다.

분할/다중 파트 오브젝트 및 비분할/비다중 파트 오브젝트 모두에 대해 1로 설정할 수 partNumber 있지만 x-amz-mp-parts-count 응답 요소는 분할된 오브젝트 또는 다중 파트 오브젝트에 대해서만 반환됩니다.

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 요청 가져오기 키 이름 또는 값에 인쇄할 수 없는 문자가 포함된 경우 헤더를 반환하지 x-amz-missing-meta 않습니다.

지원되는 요청 헤더

다음 요청 헤더가 지원됩니다.

- x-amz-checksum-mode: 지정합니다 ENABLED

> `Range`헤더는 GetObject 에 대해 지원되지 `x-amz-checksum-mode` 않습니다. 활성화된 상태로 요청에 `x-amz-checksum-mode` 포함하면 `Range` StorageGRID는 응답에 체크섬 값을 반환하지 않습니다.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않으며 XNotImplemented 반환됩니다.

- x-amz-website-redirect-location

버전 관리

하위 리소스가 지정되지 않은 경우 versionId 이 작업은 버전이 지정된 버킷에서 가장 최신 버전의 개체를 가져옵니다. 객체의 현재 버전이 삭제 마커인 경우 응답 헤더가 로 설정된 true 상태에서 "찾을 수 없음" 상태가 x-amz-delete-marker 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-server-side-encryption-customer-algorithm: AES256 지정합니다.
- x-amz-server-side-encryption-customer-key: 개체의 암호화 키를 지정합니다.
- x-amz-server-side-encryption-customer-key-MD5: 개체의 암호화 키의 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 의 고려 사항을 검토하십시오"서버측 암호화를 사용합니다".

클라우드 스토리지 풀 객체에 대한 **GetObject**의 동작입니다

개체가 에 저장된 경우 "클라우드 스토리지 풀"GetObject 요청의 동작은 개체의 상태에 따라 달라집니다. 자세한 내용은 을 "HeadObject 를 선택합니다"참조하십시오.

> 오브젝트가 클라우드 스토리지 풀에 저장되고 하나 이상의 오브젝트 복제본이 그리드에 있는 경우 GetObject 요청은 클라우드 스토리지 풀에서 검색하기 전에 그리드에서 데이터 검색을 시도합니다.

개체의 상태입니다	**GetObject** 의 동작입니다
StorageGRID로 수집되었지만 아직 ILM에 의해 평가되지 않은 오브젝트 또는 기존 스토리지 풀에 저장된 오브젝트 또는 삭제 코딩 사용	`200 OK` 개체의 복사본이 검색됩니다.
Cloud Storage Pool의 개체이지만 아직 검색할 수 없는 상태로 전환되지 않았습니다	`200 OK` 개체의 복사본이 검색됩니다.
개체가 검색할 수 없는 상태로 전환되었습니다	`403 Forbidden, InvalidObjectState` 요청을 사용하여 "RestoreObject 를 선택합니다"객체를 검색 가능한 상태로 복원합니다.
복구할 수 없는 상태에서 복원 중인 개체입니다	`403 Forbidden, InvalidObjectState` RestoreObject 요청이 완료될 때까지 기다립니다.
객체가 클라우드 스토리지 풀에 완전히 복구되었습니다	`200 OK` 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. 개체의 일부 부분이 이미 검색할 수 없는 상태로 전환되었거나 개체의 일부 부분이 아직 복원되지 않은 경우 GetObject 요청이 잘못 반환될 수 `200 OK` 있습니다.

다음과 같은 경우:

- GetObject 요청에서 일부 데이터를 반환하지만 전송 도중에 중지됩니다.
- 이후의 GetObject 요청이 반환될 수 `403 Forbidden` 있습니다.

GetObject 및 교차 그리드 복제

를 사용 중이며 "교차 그리드 복제"버킷에 대해 활성화된 경우 "그리드 통합"S3 클라이언트는 GetObject 요청을 실행하여 개체의 복제 상태를 확인할 수 있습니다. 응답에는 다음 값 중 하나가 있는 StorageGRID 관련 `x-ntap-sg-cgr-replication-status` 응답 헤더가 포함됩니다.

그리드	복제 상태입니다
출처	• * 완료됨 *: 복제가 성공했습니다. • * 보류 중 *: 객체가 아직 복제되지 않았습니다. • * 실패 *: 영구적인 장애로 인해 복제에 실패했습니다. 사용자가 오류를 해결해야 합니다.
목적지	• replica *: 객체가 소스 그리드에서 복제되었습니다.

StorageGRID는 헤더를 지원하지 `x-amz-replication-status` 않습니다.

HeadObject 를 선택합니다

S3 HeadObject 요청을 사용하여 개체 자체를 반환하지 않고 개체에서 메타데이터를 검색할 수 있습니다. 객체가 클라우드 스토리지 풀에 저장된 경우 HeadObject 를 사용하여 객체의 전환 상태를 확인할 수 있습니다.

HeadObject 및 **multipart** 개체

요청 매개 변수를 사용하여 멀티파트 또는 분할된 개체의 특정 부분에 대한 메타데이터를 검색할 수 `partNumber` 있습니다. `x-amz-mp-parts-count`응답 요소는 개체의 파트 수를 나타냅니다.

분할/다중 파트 오브젝트 및 비분할/비다중 파트 오브젝트 모두에 대해 1로 설정할 수 `partNumber` 있지만 `x-amz-mp-parts-count` 응답 요소는 분할된 오브젝트 또는 다중 파트 오브젝트에 대해서만 반환됩니다.

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 헤더를 반환하지 `x-amz-missing-meta` 않습니다.

지원되는 요청 헤더

다음 요청 헤더가 지원됩니다.

- `x-amz-checksum-mode`

> `partNumber`매개 변수 및 `Range` 머리글은 `HeadObject` 에 대해 지원되지 `x-amz-checksum-mode` 않습니다. 활성화된 상태로 요청에 포함하면 `x-amz-checksum-mode` StorageGRID는 응답에 체크섬 값을 반환하지 않습니다.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않으며 `XNotImplemented` 반환됩니다.

- `x-amz-website-redirect-location`

버전 관리

하위 리소스가 지정되지 않은 경우 `versionId` 이 작업은 버전이 지정된 버킷에서 가장 최신 버전의 개체를 가져옵니다. 객체의 현재 버전이 삭제 마커인 경우 응답 헤더가 로 설정된 `true` 상태에서 "찾을 수 없음" 상태가 `x-amz-delete-marker` 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-server-side-encryption-customer-algorithm`: `AES256` 지정합니다.
- `x-amz-server-side-encryption-customer-key`: 개체의 암호화 키를 지정합니다.
- `x-amz-server-side-encryption-customer-key-MD5`: 개체의 암호화 키의 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 의 고려 사항을 검토하십시오"서버측 암호화를 사용합니다".

클라우드 스토리지 풀 객체에 대한 **HeadObject** 응답입니다

개체가 에 저장된 경우 "클라우드 스토리지 풀"다음 응답 헤더가 반환됩니다.

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

응답 헤더는 클라우드 스토리지 풀로 이동되는 오브젝트의 상태에 대한 정보를 제공하며, 선택적으로 검색할 수 없는 상태로 전환된 후 복구됩니다.

개체의 상태입니다	**HeadObject**에 대한 응답입니다
StorageGRID로 수집되었지만 아직 ILM에 의해 평가되지 않은 오브젝트 또는 기존 스토리지 풀에 저장된 오브젝트 또는 삭제 코딩 사용	`200 OK` (특수 응답 헤더가 반환되지 않음)

Cloud Storage Pool의 개체이지만 아직 검색할 수 없는 상태로 전환되지 않았습니다	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	오브젝트가 검색 불가능한 상태로 전환될 때까지 의 값은 `expiry-date` 나중에 먼 시간으로 설정됩니다. 정확한 전환 시간은 StorageGRID 시스템에 의해 제어되지 않습니다.

개체의 상태입니다	**HeadObject**에 대한 응답입니다

개체가 검색할 수 없는 상태로 전환되었지만 하나 이상의 복사본이 그리드에 있습니다	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	의 값은 `expiry-date` 나중에 먼 시간으로 설정됩니다.
	
	• 참고 *: 그리드의 복제본을 사용할 수 없는 경우(예: 스토리지 노드가 다운된 경우), 객체를 성공적으로 검색하기 전에 클라우드 스토리지 풀에서 복제본을 복원하도록 요청을 해야 "RestoreObject 를 선택합니다"합니다.

개체가 검색할 수 없는 상태로 전환되었으며 그리드에 복사본이 없습니다	`200 OK`
	
	`x-amz-storage-class: GLACIER`

복구할 수 없는 상태에서 복원 중인 개체입니다	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

객체가 클라우드 스토리지 풀에 완전히 복구되었습니다	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	는 `expiry-date` 클라우드 스토리지 풀의 객체가 검색할 수 없는 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. 개체의 일부 부분이 이미 검색할 수 없는 상태로 전환되었거나 개체의 일부 부분이 아직 복원되지 않은 경우 HeadObject 요청이 잘못 반환될 수 `x-amz-restore: ongoing-request="false"` 있습니다.

HeadObject 및 교차 그리드 복제

를 사용 중이며 "교차 그리드 복제"버킷에 대해 활성화된 경우 "그리드 통합"S3 클라이언트는 HeadObject 요청을 실행하여 객체의 복제 상태를 확인할 수 있습니다. 응답에는 다음 값 중 하나가 있는 StorageGRID 관련 `x-ntap-sg-`

cgr-replication-status 응답 헤더가 포함됩니다.

그리드	복제 상태입니다
출처	• * 완료됨 *: 복제가 성공했습니다. • * 보류 중 *: 객체가 아직 복제되지 않았습니다. • * 실패 *: 영구적인 장애로 인해 복제에 실패했습니다. 사용자가 오류를 해결해야 합니다.
목적지	• replica *: 객체가 소스 그리드에서 복제되었습니다.

StorageGRID는 헤더를 지원하지 x-amz-replication-status 않습니다.

PutObject 를 선택합니다

S3 PutObject 요청을 사용하여 객체를 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 PutObject 작업의 maximum_recommended_size는 5GiB(5,368,709,120바이트)입니다. 5GiB보다 큰 오브젝트가 있는 경우 대신 를 "멀티파트 업로드"사용하십시오.

단일 PutObject 작업의 maximum_supported_size는 5TiB(5,497,558,138,880바이트)입니다.

StorageGRID 11.6 이하에서 업그레이드한 경우 5GiB를 초과하는 객체를 업로드하려고 하면 S3 PUT 개체 크기가 너무 큼 경고가 트리거됩니다. StorageGRID 11.7 또는 11.8을 새로 설치한 경우 경고가 트리거되지 않습니다. 하지만 StorageGRID의 향후 릴리즈에서는 AWS S3 표준에 맞춰 5GiB보다 큰 오브젝트 업로드를 지원하지 않습니다.

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 PutObject, CopyObject, GetObject 및 HeadObject 요청이 성공합니다.
- 키 이름 또는 값의 해석된 값에 인쇄할 수 없는 문자가 포함된 경우 StorageGRID는 헤더를 반환하지 `x-amz-missing-meta` 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.

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  `Content-Encoding`StorageGRID에 대해 를 `aws-chunked` 지정하면 다음 항목이 검증되지 않습니다.

  - StorageGRID는 청크 데이터에 대해 를 확인하지 `chunk-signature` 않습니다.
  - StorageGRID는 사용자가 개체에 대해 제공한 값을 확인하지 `x-amz-decoded-content-length` 않습니다.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  페이로드 서명도 사용되는 경우 청크 전송 인코딩이 `aws-chunked` 지원됩니다.

- `x-amz-checksum-sha256`
- `x-amz-meta-`, 그 뒤에 사용자 정의 메타데이터를 포함하는 이름-값 쌍이 옵니다.

  사용자 정의 메타데이터에 대한 이름 값 쌍을 지정할 때 다음 일반 형식을 사용합니다.

```
x-amz-meta-name: value
```

사용자 정의 생성 시간 * 옵션을 ILM 규칙의 참조 시간으로 사용하려면 객체를 생성할 때 기록하는 메타데이터의 이름으로 를 사용해야 `creation-time` 합니다. 예를 들면 다음과 같습니다.

```
x-amz-meta-creation-time: 1443399726
```

의 값은 `creation-time` 1970년 1월 1일 이후 초로 계산됩니다.

> ILM 규칙은 참조 시간에 * 사용자 정의 생성 시간 * 과 Balanced 또는 Strict 수집 옵션을 모두 사용할 수 없습니다. ILM 규칙을 만들면 오류가 반환됩니다.

- `x-amz-tagging`
- 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 오브젝트 버전 모드와 보존 기간을 계산합니다. 을 "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"참조하십시오.
- SSE 요청 헤더:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    을 참조하십시오 서버측 암호화에 대한 요청 헤더

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

```
`x-amz-website-redirect-location`헤더가 를 `XNotImplemented`반환합니다.
```

`x-amz-storage-class`요청 헤더가 지원됩니다. 에 제출된 `x-amz-storage-class` 값은 StorageGRID 시스템(ILM에 의해 결정됨)에 저장되는 오브젝트의 영구 사본의 수가 아니라 수집 중에 StorageGRID가 오브젝트 데이터를 보호하는 방법에 영향을 줍니다.

수집된 객체와 일치하는 ILM 규칙이 Strict 수집 옵션을 사용하는 경우 x-amz-storage-class 헤더는 영향을 미치지 않습니다.

다음 값을 사용할 수 x-amz-storage-class 있습니다.

- STANDARD (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.

    StorageGRID가 ILM 규칙(동기식 배치)에 지정된 모든 오브젝트 복사본을 즉시 생성할 수 있다면 x-amz-storage-class 헤더는 효과가 없습니다.
- REDUCED_REDUNDANCY
  - * 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. 이 REDUCED_REDUNDANCY 옵션은 오브젝트와 일치하는 ILM 규칙이 복제된 단일 복사본을 생성할 때 가장 적합합니다. 이 경우 를 REDUCED_REDUNDANCY 사용하면 모든 수집 작업에서 불필요한 추가 오브젝트 복사본을 생성하여 삭제할 필요가 없습니다.

  다른 상황에서는 이 옵션을 사용하지 REDUCED_REDUNDANCY 않는 것이 좋습니다. REDUCED_REDUNDANCY 수집 중 오브젝트 데이터가 손실될 위험이 증가함 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.

`REDUCED_REDUNDANCY`지정하면 오브젝트를 처음 수집할 때 생성되는 복사본의 개수만 영향을 줍니다. 활성 ILM 정책에 따라 오브젝트를 평가할 때 생성되는 오브젝트 복사본 수에 영향을 미치지 않으며 StorageGRID 시스템에서 더 낮은 수준의 이중화로 데이터가 저장되지는 않습니다.

S3 오브젝트 잠금이 설정된 상태에서 오브젝트를 버킷에 수집하면 `REDUCED_REDUNDANCY` 옵션이 무시됩니다. 오브젝트를 레거시 준수 버킷에 수집하는 경우 `REDUCED_REDUNDANCY` 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-server-side-encryption`

    머리글이 PutObject 요청에 포함되어 있지 않으면 `x-amz-server-side-encryption` PutObject 응답에서 그리드 전체의 머리글이 "저장된 개체 암호화 설정입니다"생략됩니다.

- * SSE-C *: 사용자가 제공 및 관리하는 고유 키로 객체를 암호화하려면 이 헤더 세 개를 모두 사용합니다.
  - `x-amz-server-side-encryption-customer-algorithm`: `AES256` 지정합니다.
  - `x-amz-server-side-encryption-customer-key`: 새 개체에 대한 암호화 키를 지정합니다.
  - `x-amz-server-side-encryption-customer-key-MD5`: 새 개체의 암호화 키의 MD5 다이제스트를 지정합니다.

제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 에 대한 고려 사항을 "서버 측 암호화 사용"검토하십시오.

개체가 SSE 또는 SSE-C로 암호화된 경우 버킷 수준 또는 그리드 수준 암호화 설정은 무시됩니다.

버전 관리

버킷에 대해 버전 관리를 사용하도록 설정하면 저장되는 오브젝트 버전에 대해 고유한 `versionId` 버전이 자동으로 생성됩니다. `versionId`응답 헤더를 사용하여 응답에서도 `x-amz-version-id` 반환됩니다.

버전 관리가 일시 중단되면 개체 버전이 null로 저장되고 null 버전이 이미 있는 경우 해당 버전을 `versionId` 덮어씁니다.

승인 헤더의 서명 계산

헤더를 사용하여 요청을 인증하는 경우 `Authorization` StorageGRID는 다음과 같은 점에서 AWS와 다릅니다.

- StorageGRID에서는 머리글이 에 포함될 `CanonicalHeaders` 필요가 `host` 없습니다.
- StorageGRID는 `Content-Type` 에 포함되지 `CanonicalHeaders` 않아도 됩니다.
- StorageGRID에서는 머리글이 에 포함될 `CanonicalHeaders` 필요가 `x-amz-*` 없습니다.

일반적으로 이러한 헤더를 항상 포함시켜 유효성을 확인하지만 이러한 헤더를 `CanonicalHeaders` 제외하면 StorageGRID에서 오류를 반환하지 않습니다.

자세한 내용은 을 "승인 헤더에 대한 서명 계산:단일 청크(AWS 서명 버전 4)로 페이로드 전송"참조하십시오.

관련 정보

- "ILM을 사용하여 개체를 관리합니다"
- "Amazon Simple Storage Service API 참조: PutObject"

RestoreObject 를 선택합니다

S3 RestoreObject 요청을 사용하여 클라우드 스토리지 풀에 저장된 개체를 복원할 수 있습니다.

지원되는 요청 유형입니다

StorageGRID에서는 객체를 복원하기 위한 RestoreObject 요청만 지원합니다. 복원 유형을 지원하지 `SELECT` 않습니다. 요청 반환 을 선택합니다 `XNotImplemented`.

버전 관리

선택적으로 `versionId` 버전 지정된 버킷에서 특정 버전의 개체를 복원하도록 지정합니다. 을 지정하지 `versionId`않으면 개체의 최신 버전이 복원됩니다

클라우드 스토리지 풀 객체에서 **RestoreObject**의 동작입니다

개체가 에 저장된 경우 "클라우드 스토리지 풀"RestoreObject 요청에는 개체의 상태에 따라 다음과 같은 동작이 발생합니다. 자세한 내용은 을 "HeadObject 를 선택합니다"참조하십시오.

> 객체가 클라우드 스토리지 풀에 저장되어 있고 하나 이상의 객체 복제본도 그리드에 있는 경우 RestoreObject 요청을 실행하여 객체를 복구할 필요가 없습니다. 대신 GetObject 요청을 사용하여 로컬 복사본을 직접 검색할 수 있습니다.

개체의 상태입니다	**RestoreObject**의 동작입니다
StorageGRID로 수집되었지만 ILM에서 아직 평가되지 않은 오브젝트 또는 클라우드 스토리지 풀에 없는 오브젝트	`403 Forbidden, InvalidObjectState`
Cloud Storage Pool의 개체이지만 아직 검색할 수 없는 상태로 전환되지 않았습니다	`200 OK` 변경되지 않았습니다. • 참고 * : 개체가 검색 불가능한 상태로 전환되기 전에 개체를 변경할 수 `expiry-date` 없습니다.

개체의 상태입니다	**RestoreObject**의 동작입니다
개체가 검색할 수 없는 상태로 전환되었습니다	`202 Accepted` 요청 본문에 지정된 일 수 동안 객체의 검색 가능한 복제본을 클라우드 스토리지 풀에 복구합니다. 이 기간이 끝나면 객체는 복구할 수 없는 상태로 돌아갑니다. 필요한 경우, request 요소를 사용하여 `Tier` 복원 작업이 완료되는 데 걸리는 시간을 (`Expedited` `Standard`결정합니다, 또는 `Bulk`). 지정하지 않으면 `Tier` `Standard` 계층이 사용됩니다. • 중요 *: 개체가 S3 Glacier Deep Archive로 전환되었거나 클라우드 스토리지 풀이 Azure Blob 스토리지를 사용하는 경우 계층을 사용하여 복원할 수 없습니다 `Expedited`. 다음 오류가 `403 Forbidden` 반환됩니다 `InvalidTier` `Retrieval option is not supported by this storage class.`
복구할 수 없는 상태에서 복원 중인 개체입니다	`409 Conflict`, `RestoreAlreadyInProgress`
객체가 클라우드 스토리지 풀에 완전히 복구되었습니다	`200 OK` • 참고: * 오브젝트가 검색 가능한 상태로 복원된 경우 에 대한 새 값으로 RestoreObject 요청을 다시 실행하여 오브젝트를 `Days` 변경할 수 `expiry-date` 있습니다. 복원 날짜는 요청 시간을 기준으로 업데이트됩니다.

SelectObjectContent 를 선택합니다

S3 SelectObjectContent 요청을 사용하여 간단한 SQL 문을 기반으로 S3 개체의 내용을 필터링할 수 있습니다.

자세한 내용은 을 "Amazon Simple Storage Service API 참조: SelectObjectContent"참조하십시오.

시작하기 전에

- 테넌트 계정에 S3 Select 권한이 있습니다.
- `s3:GetObject`쿼리할 개체에 대한 사용 권한이 있습니다.
- 쿼리할 객체는 다음 형식 중 하나여야 합니다.
  - CSV *. GZIP 또는 BZIP2 보관 파일로 압축하거나 그대로 사용할 수 있습니다.
  - * 파케 *. Parquet 객체에 대한 추가 요구 사항:
    - S3 Select는 GZIP 또는 Snappy를 사용한 컬럼 압축만 지원합니다. S3 Select는 Parquet 오브젝트에 대한 전체 오브젝트 압축을 지원하지 않습니다.
    - S3 Select는 Parquet 출력을 지원하지 않습니다. 출력 형식을 CSV 또는 JSON으로 지정해야 합니다.
    - 압축되지 않은 최대 행 그룹 크기는 512MB입니다.
    - 개체의 스키마에 지정된 데이터 형식을 사용해야 합니다.
    - 간격, JSON, 목록, 시간 또는 UUID 논리적 유형은 사용할 수 없습니다.

- SQL 식의 최대 길이는 256KB입니다.
- 입력 또는 결과에 있는 모든 레코드의 최대 길이는 1MiB입니다.

CSV 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>
```

쪽모이 세공 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>
      <PARQUET>
      </PARQUET>
   </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. 상태가 아닌 파일의 레코드는 무시됩니다.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

쿼리할 파일의 처음 몇 줄은 `SUB-EST2020_ALL.csv` 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(CSV)

```
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 줄은 `changes.csv` 다음과 같습니다.

```
Alabama,4779736,4854803,1.57052607089596580229535689837262978 54
Alaska,710231,738430,3.97039836334938914240578065446312537 75
Arizona,6392017,6832810,6.89599229789282475312565658070058324 31
Arkansas,2915918,2979732,2.18847032049598102552952449280123789 49
California,37253956,38904296,4.42997248399606205579885261044491489 71
Colorado,5029196,5454328,8.45327960970302211327615785902955462 46
```

AWS-CLI 사용 예(Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' 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

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 ListMultipartUploads 쿼리의 결과가 불완전한 결과를 반환할 수 있으므로 단일 버킷에 대한 동시 다중 파트 업로드가 1,000개를 초과해서는 안 됩니다.
- 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 Balanced 또는 Strict를 사용하는 경우, ILM은 수집 시 멀티파트 개체의 각 부분과 다중 파트 업로드가 완료될 때 개체 전체에 대해 평가됩니다."수집 옵션" 이 사항이 개체 및 파트 배치에 미치는 영향에 대해 알고 있어야 합니다.
  - S3 다중 파트 업로드가 진행되는 동안 ILM이 변경되면 다중 파트 업로드가 완료될 때 개체의 일부 부분이 현재 ILM 요구사항을 충족하지 못할 수 있습니다. 올바르게 배치되지 않은 모든 부품은 ILM 재평가를 위해 대기열에 추가되고 나중에 올바른 위치로 이동됩니다.
  - 파트에 대한 ILM을 평가할 때 StorageGRID은 개체의 크기가 아닌 파트 크기를 필터링합니다. 즉, 개체의

일부를 개체에 대한 ILM 요구 사항을 전체가 충족하지 않는 위치에 저장할 수 있습니다. 예를 들어, 모든 작은 오브젝트가 DC2에 저장되지만 10GB 이상의 오브젝트는 모두 DC1에 저장되도록 규칙이 지정된 경우 10부분 다중 부분 업로드의 각 1GB 부분은 인제스트 시 DC2에 저장됩니다. 그러나 개체 전체에 대해 ILM을 평가하면 개체의 모든 부분이 DC1로 이동됩니다.

- 모든 멀티 파트 업로드 작업은 StorageGRID를 "일관성 값"지원합니다.
- 멀티파트 업로드를 사용하여 개체를 수집하는 경우 이 "객체 분할 임계값(1GiB)"적용되지 않습니다.
- 필요에 따라 멀티파트 업로드와 함께 을 사용할 수 "서버 측 암호화"있습니다. SSE(StorageGRID 관리 키가 있는 서버측 암호화)를 사용하려면 CreateMultipartUpload 요청에만 요청 헤더를 포함합니다 `x-amz-server-side-encryption`. SSE-C(고객 제공 키를 사용한 서버측 암호화)를 사용하려면 CreateMultipartUpload 요청과 이후의 각 UploadPart 요청에서 동일한 3개의 암호화 키 요청 헤더를 지정합니다.

작동	구축
AbortMultipartUpload 를 클릭합니다	모든 Amazon S3 REST API 동작으로 구현됩니다. 예고 없이 변경될 수 있습니다.
CompleteMultipartUpload를 클릭합니다	을 참조하십시오 "CompleteMultipartUpload를 클릭합니다"
CreateMultptUpload 를 클릭합니다 (이전에 명명된 다중 파트 업로드 시작)	을 참조하십시오 "CreateMultptUpload 를 클릭합니다"
ListMultipartUploads 를 참조하십시오	을 참조하십시오 "ListMultipartUploads 를 참조하십시오"
목록 파트	모든 Amazon S3 REST API 동작으로 구현됩니다. 예고 없이 변경될 수 있습니다.
업로드 파트	을 참조하십시오 "업로드 파트"
업로드파트 복사	을 참조하십시오 "업로드파트 복사"

CompleteMultipartUpload를 클릭합니다

CompleteMultipartUpload 작업은 이전에 업로드한 부품을 조립하여 객체의 다중 부분 업로드를 완료합니다.

StorageGRID는 CompleteMultipartUpload를 사용하여 요청 매개 변수에 대해 비연속 값을 오름차순으로 `partNumber` 지원합니다. 매개 변수는 어떤 값으로든 시작할 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.

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

  `x-amz-storage-class`일치하는 ILM 규칙이 을 지정한 경우 머리글에 StorageGRID에서 생성하는 개체 복사본 수에 영향을 xref:{relative_path}../ilm/data-protection-options-for-ingest.html["이중 커밋 또는 Balanced 인제스트 옵션"]줍니다.

- `STANDARD`

  (기본값) ILM 규칙이 이중 커밋 옵션을 사용하거나 균형 옵션이 중간 복사본 생성으로 돌아올 때 이중 커밋 수집 작업을 지정합니다.

- `REDUCED_REDUNDANCY`

  ILM 규칙이 이중 커밋 옵션을 사용하거나 균형 옵션이 중간 복사본 생성으로 돌아올 때 단일 커밋 수집 작업을 지정합니다.

  S3 오브젝트 잠금이 설정된 상태에서 오브젝트를 버킷에 수집하면 `REDUCED_REDUNDANCY` 옵션이 무시됩니다. 오브젝트를 레거시 준수 버킷에 수집하는 경우 `REDUCED_REDUNDANCY` 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.

`ETag`반환되는 값은 데이터의 MD5 합계가 아니라 다중 개체 값의 Amazon S3 API 구현을 `ETag` 따릅니다.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

버전 관리

이 작업은 여러 부분 업로드를 완료합니다. 버켓에 대해 버전 관리가 활성화된 경우 다중 파트 업로드가 완료된 후 개체 버전이 생성됩니다.

버킷에 대해 버전 관리를 사용하도록 설정하면 저장되는 오브젝트 버전에 대해 고유한 `versionId` 버전이 자동으로 생성됩니다. `versionId`응답 헤더를 사용하여 응답에서도 `x-amz-version-id` 반환됩니다.

버전 관리가 일시 중단되면 개체 버전이 null로 저장되고 null 버전이 이미 있는 경우 해당 버전을 `versionId` 덮어씁니다.

> 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.

테넌트는 개체의 메타데이터 또는 태그를 업데이트하여 실패한 복제 또는 알림을 트리거할 수 있습니다. 테넌트는 불필요한 변경을 방지하기 위해 기존 값을 다시 제출할 수 있습니다.

을 "플랫폼 서비스 문제 해결"참조하십시오.

CreateMultptUpload 를 클릭합니다

CreateMultipartUpload(이전에 이름이 Multipart Upload 시작) 작업은 개체에 대한 다중 부분 업로드를 시작하고 업로드 ID를 반환합니다.

`x-amz-storage-class`요청 헤더가 지원됩니다. 에 제출된 `x-amz-storage-class` 값은 `StorageGRID` 시스템(`ILM`에 의해 결정됨)에 저장되는 오브젝트의 영구 사본의 수가 아니라 수집 중에 `StorageGRID`가 오브젝트 데이터를 보호하는 방법에 영향을 줍니다.

수집된 객체와 일치하는 ILM 규칙이 Strict 를 사용하는 경우 "수집 옵션" `x-amz-storage-class`헤더는 영향을 미치지 않습니다.

다음 값을 사용할 수 `x-amz-storage-class` 있습니다.

- `STANDARD` (기본값)
  - * Dual Commit *: ILM 규칙이 Dual Commit Ingest 옵션을 지정하는 경우 오브젝트가 수집되는 즉시 해당 오브젝트의 두 번째 복사본이 생성되어 다른 스토리지 노드(Dual Commit)로 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.

    StorageGRID가 ILM 규칙(동기식 배치)에 지정된 모든 오브젝트 복사본을 즉시 생성할 수 있다면 `x-amz-storage-class` 헤더는 효과가 없습니다.
- `REDUCED_REDUNDANCY`
  - * Dual Commit *: ILM 규칙이 Dual Commit 옵션을 지정하는 경우 StorageGRID는 개체가 수집될 때(단일 커밋) 하나의 중간 복사본을 생성합니다.
  - * 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. 이 REDUCED_REDUNDANCY 옵션은 오브젝트와 일치하는 ILM 규칙이 복제된 단일 복사본을 생성할 때 가장 적합합니다. 이 경우 를 REDUCED_REDUNDANCY 사용하면 모든 수집 작업에서 불필요한 추가 오브젝트 복사본을 생성하여 삭제할 필요가 없습니다.

다른 상황에서는 이 옵션을 사용하지 REDUCED_REDUNDANCY 않는 것이 좋습니다. REDUCED_REDUNDANCY 수집 중 오브젝트 데이터가 손실될 위험이 증가함 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.

`REDUCED_REDUNDANCY`지정하면 오브젝트를 처음 수집할 때 생성되는 복사본의 개수만 영향을 줍니다. 활성 ILM 정책에 따라 오브젝트를 평가할 때 생성되는 오브젝트 복사본 수에 영향을 미치지 않으며 StorageGRID 시스템에서 더 낮은 수준의 이중화로 데이터가 저장되지는 않습니다.

S3 오브젝트 잠금이 설정된 상태에서 오브젝트를 버킷에 수집하면 REDUCED_REDUNDANCY 옵션이 무시됩니다. 오브젝트를 레거시 준수 버킷에 수집하는 경우 REDUCED_REDUNDANCY 옵션은 오류를 반환합니다. StorageGRID은 규정 준수 요구 사항이 충족될 수 있도록 항상 이중 커밋 수집을 수행합니다.

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- Content-Type
- x-amz-checksum-algorithm

  현재는 의 SHA256 값만 x-amz-checksum-algorithm 지원됩니다.

- x-amz-meta-, 그 뒤에 사용자 정의 메타데이터를 포함하는 이름-값 쌍이 옵니다

  사용자 정의 메타데이터에 대한 이름 값 쌍을 지정할 때 다음 일반 형식을 사용합니다.

  ```
  x-amz-meta-_name_: `value`
  ```

  사용자 정의 생성 시간 * 옵션을 ILM 규칙의 참조 시간으로 사용하려면 객체를 생성할 때 기록하는 메타데이터의 이름으로 를 사용해야 creation-time 합니다. 예를 들면 다음과 같습니다.

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  의 값은 creation-time 1970년 1월 1일 이후 초로 계산됩니다.

`creation-time`기존 Compliance가 활성화된 버킷에 오브젝트를 추가하는 경우 사용자 정의 메타데이터로 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 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"

- SSE 요청 헤더:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    서버측 암호화에 대한 요청 헤더

StorageGRID에서 UTF-8 문자를 처리하는 방법에 대한 자세한 내용은 을 참조하십시오"PutObject를 선택합니다".

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 개체를 암호화하려면 CreateMultipartUpload 요청에서 다음 헤더를 사용합니다. UploadPart 요청에는 이 헤더를 지정하지 마십시오.
  - `x-amz-server-side-encryption`
- * SSE-C *: 제공 및 관리하는 고유 키로 개체를 암호화하려면 CreateMultipartUpload 요청(및 이후의 각 UploadPart 요청)에 이 헤더 세 개를 모두 사용하십시오.
  - `x-amz-server-side-encryption-customer-algorithm`: `AES256` 지정합니다.
  - `x-amz-server-side-encryption-customer-key`: 새 개체에 대한 암호화 키를 지정합니다.
  - `x-amz-server-side-encryption-customer-key-MD5`: 새 개체의 암호화 키의 MD5 다이제스트를 지정합니다.

제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 에 대한 고려 사항을 "서버 측 암호화 사용"검토하십시오.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

- `x-amz-website-redirect-location`

> `x-amz-website-redirect-location`헤더가 를 `XNotImplemented`반환합니다.

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. CompleteMultipartUpload 작업이 수행될 때 객체가 생성되고 해당되는 경우 버전이 지정됩니다.

ListMultipartUploads 를 참조하십시오

ListMultipartUploads 작업은 버킷에 대해 진행 중인 다중 파트 업로드를 나열합니다.

지원되는 요청 매개 변수는 다음과 같습니다.

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. CompleteMultipartUpload 작업이 수행될 때 객체가 생성되고 해당되는 경우 버전이 지정됩니다.

업로드 파트

UploadPart 작업은 객체에 대한 다중 부분 업로드의 파트를 업로드합니다.

지원되는 요청 헤더입니다

지원되는 요청 헤더는 다음과 같습니다.

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

서버측 암호화에 대한 요청 헤더

CreateMultipartUpload 요청에 대해 SSE-C 암호화를 지정한 경우 각 UploadPart 요청에 다음 요청 머리글도 포함해야 합니다.

- `x-amz-server-side-encryption-customer-algorithm`: `AES256` 지정합니다.
- `x-amz-server-side-encryption-customer-key`: CreateMultipartUpload 요청에서 제공한 것과 동일한 암호화 키를 지정합니다.
- `x-amz-server-side-encryption-customer-key-MD5`: CreateMultipartUpload 요청에 제공한 것과 동일한 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 의 고려 사항을 검토하십시오"서버측 암호화를 사용합니다".

CreateMultipartUpload 요청 중에 SHA-256 체크섬을 지정한 경우 각 UploadPart 요청에 다음 요청 헤더도 포함해야 합니다.

- `x-amz-checksum-sha256`: 이 부품에 대한 SHA-256 체크섬을 지정합니다.

지원되지 않는 요청 헤더입니다

다음 요청 헤더는 지원되지 않습니다.

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. CompleteMultipartUpload 작업이 수행될 때 객체가 생성되고 해당되는 경우 버전이 지정됩니다.

업로드파트 복사

UploadPartCopy 작업은 기존 개체의 데이터를 데이터 소스로 복사하여 개체의 일부를 업로드합니다.

UploadPartCopy 작업은 모든 Amazon S3 REST API 동작으로 구현됩니다. 예고 없이 변경될 수 있습니다.

이 요청은 StorageGRID 시스템 내에 지정된 오브젝트 데이터를 읽고 `x-amz-copy-source-range` 씁니다.

지원되는 요청 헤더는 다음과 같습니다.

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

서버측 암호화에 대한 요청 헤더

CreateMultipartUpload 요청에 대해 SSE-C 암호화를 지정한 경우 각 UploadPartCopy 요청에 다음 요청 머리글도 포함해야 합니다.

- `x-amz-server-side-encryption-customer-algorithm`: `AES256` 지정합니다.
- `x-amz-server-side-encryption-customer-key`: CreateMultipartUpload 요청에서 제공한 것과 동일한 암호화 키를 지정합니다.
- `x-amz-server-side-encryption-customer-key-MD5`: CreateMultipartUpload 요청에 제공한 것과 동일한 MD5 다이제스트를 지정합니다.

소스 객체가 SSE-C(고객 제공 키)를 사용하여 암호화되는 경우 UploadPartCopy 요청에 다음 세 개의 헤더를 포함해야 객체를 해독한 후 복사할 수 있습니다.

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: `AES256` 지정합니다.
- `x-amz-copy-source-server-side-encryption-customer-key`: 원본 개체를 만들 때 제공한 암호화 키를 지정합니다.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: 원본 개체를 만들 때 제공한 MD5 다이제스트를 지정합니다.

> 제공한 암호화 키는 저장되지 않습니다. 암호화 키를 분실하면 해당 개체가 손실됩니다. 고객이 제공한 키를 사용하여 개체 데이터를 보호하기 전에 의 고려 사항을 검토하십시오"서버측 암호화를 사용합니다".

버전 관리

멀티파트 업로드는 업로드 시작, 리스팅 업로드, 파트 업로드, 업로드된 파트 조립 및 업로드 완료를 위한 별도의 작업으로 구성됩니다. CompleteMultipartUpload 작업이 수행될 때 객체가 생성되고 해당되는 경우 버전이 지정됩니다.

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

이름	**HTTP** 상태입니다
내부 오류입니다	500 내부 서버 오류입니다
InvalidAccessKeyId 입니다	403 사용 금지
InvalidArgument 를 선택합니다	400 잘못된 요청
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

이름	**HTTP** 상태입니다
NoSuchBucket	404를 찾을 수 없습니다
NoSuchKey를 클릭합니다	404를 찾을 수 없습니다
NoSuchUpload 를 클릭합니다	404를 찾을 수 없습니다
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

이름	설명	HTTP 상태입니다
XMissingInternalRequestHeader를 참조하십시오	내부 요청의 헤더가 누락되었습니다.	400 잘못된 요청
XNoSuchBuckketCompliance	지정된 버킷에 레거시 준법 기능이 설정되어 있지 않습니다.	404를 찾을 수 없습니다
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 사용자 정의 작업

StorageGRID 사용자 정의 작업

StorageGRID 시스템은 S3 REST API에 추가된 사용자 지정 작업을 지원합니다.

다음 표에서는 StorageGRID에서 지원하는 사용자 지정 작업을 보여 줍니다.

작동	설명
"버킷 일관성 확보"	특정 버킷에 적용되는 일관성을 반환합니다.
"버킷 일관성을 유지합니다"	특정 버킷에 적용되는 일관성을 설정합니다.
"버킷 최종 액세스 시간 가져오기"	특정 버킷에 대해 마지막 액세스 시간 업데이트를 사용할 수 있는지 여부를 반환합니다.
"버킷 최종 접근 시간"	특정 버킷에 대한 마지막 액세스 시간 업데이트를 활성화하거나 비활성화할 수 있습니다.
"버킷 메타데이터 알림 구성을 삭제합니다"	특정 버킷과 연결된 메타데이터 알림 구성 XML을 삭제합니다.
"Bucket 메타데이터 알림 구성 가져오기"	특정 버킷과 연결된 메타데이터 알림 구성 XML을 반환합니다.
"Put Bucket 메타데이터 알림 구성"	버킷에 대한 메타데이터 알림 서비스를 구성합니다.
"스토리지 사용량을 가져옵니다"	계정과 연결된 각 버킷에서 사용 중인 총 저장소 양을 나타냅니다.
"사용되지 않음: 규정 준수 설정이 있는 CreateBucket"	더 이상 사용되지 않으며 지원되지 않음: Compliance를 사용하는 새 버킷을 더 이상 생성할 수 없습니다.

작동	설명
"사용되지 않음: 버킷 준수 가져오기"	더 이상 사용되지 않지만 지원됨: 기존 레거시 준수 버킷에 대해 현재 적용되는 규정 준수 설정을 반환합니다.
"사용되지 않음: 버킷 준수"	사용되지 않지만 지원됨: 기존 레거시 준수 버킷의 준수 설정을 수정할 수 있습니다.

버킷 일관성 확보

Get Bucket Consistency 요청을 사용하면 특정 버킷에 적용되는 일관성을 확인할 수 있습니다.

기본 정합성 보장은 새로 생성된 개체에 대해 쓰기 후 읽기를 보장하도록 설정됩니다.

이 작업을 완료하려면 S3:GetBucketConsistency 권한이 있거나 계정 루트여야 합니다.

요청 예

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

응답

응답 XML에서 은 `<Consistency>` 다음 값 중 하나를 반환합니다.

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

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 값"

버킷 일관성을 유지합니다

Put Bucket Consistency 요청을 사용하면 버킷에서 수행된 작업에 적용할 일관성을 지정할 수 있습니다.

기본 정합성 보장은 새로 생성된 개체에 대해 쓰기 후 읽기를 보장하도록 설정됩니다.

시작하기 전에

이 작업을 완료하려면 S3:PutBucketConsistency 권한이 있거나 계정 루트여야 합니다.

요청하십시오

매개 변수에는 `x-ntap-sg-consistency` 다음 값 중 하나가 포함되어야 합니다.

정합성	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 대부분의 경우에 권장됩니다.

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

- 참고: * 일반적으로 "Read-after-new-write" 일관성을 사용해야 합니다. 요청이 올바르게 작동하지 않는 경우 가능한 경우 응용 프로그램 클라이언트 동작을 변경합니다. 또는 각 API 요청의 일관성을 지정하도록 클라이언트를 구성합니다. 버킷 수준의 일관성을 마지막 수단으로 설정합니다.

요청 예

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

관련 정보

"일관성 값"

버킷 최종 액세스 시간 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 루트여야 합니다.

요청 예

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

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 접근 시간

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:PutBuckketLastAccessTime 권한이 있거나 계정 루트여야 합니다.

> 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. Put Bucket 마지막 액세스 시간 요청을 사용하거나 Tenant Manager의 버킷에 대한 세부 정보 페이지에서 마지막 액세스 시간에 대한 업데이트를 활성화 또는 비활성화할 수 있습니다. 을 "마지막 액세스 시간 업데이트를 사용하거나 사용하지 않도록 설정합니다"참조하십시오.

버킷에 대해 마지막 액세스 시간 업데이트가 비활성화된 경우 버킷의 작업에 다음 동작이 적용됩니다.

- GetObject, GetObjectAcl, GetObjectTagging 및 HeadObject 요청은 마지막 액세스 시간을 업데이트하지 않습니다. ILM(정보 수명 주기 관리) 평가를 위해 객체가 대기열에 추가되지 않습니다.
- 메타데이터만 업데이트하는 CopyObject 및 PutObjectTagging 요청도 마지막 액세스 시간을 업데이트합니다. ILM 평가를 위해 오브젝트가 대기열에 추가됩니다.
- 소스 버킷에 대해 마지막 액세스 시간에 대한 업데이트를 사용할 수 없는 경우 CopyObject 요청이 소스 버킷의 마지막 액세스 시간을 업데이트하지 않습니다. 복사된 객체는 소스 버킷에 대한 ILM 평가를 위해 대기열에 추가되지 않습니다. 그러나 대상의 경우 CopyObject 요청은 항상 마지막 액세스 시간을 업데이트합니다. ILM 평가를 위해 개체의 복사본이 대기열에 추가됩니다.
- CompleteMultipartUpload 요청이 마지막 액세스 시간을 업데이트합니다. 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: date
Authorization: authorization string
Host: host
```

이 예제에서는 버킷의 마지막 액세스 시간을 비활성화합니다.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

버킷 메타데이터 알림 구성을 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 권한이 있거나 계정 루트여야 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: date
Authorization: authorization string
Host: host
```

Bucket 메타데이터 알림 구성 가져오기

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 권한이 있거나 계정 루트여야 합니다.

요청 예

이 요청은 이름이 인 버킷에 대한 메타데이터 알림 구성을 `bucket` 검색합니다.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

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
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

이름	설명	필수 요소입니다
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
urn	객체 메타데이터가 전송되는 대상의 urn입니다. 다음 속성을 가진 StorageGRID 끝점의 URN이어야 합니다. • `es` 세 번째 요소여야 합니다. • URN은 메타데이터가 저장되는 인덱스 및 형식으로 끝나야 `domain-name/myindex/mytype` 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

태그 사이에 포함된 XML은 `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>`검색 통합 끝점과의 통합이 버킷에 대해 구성되는 방법을 보여 줍니다. 이 예제에서 개체 메타데이터는 이름이 인 `AWS` 도메인에서 호스팅되는 `records` 이름이 `2017` 인 Elasticsearch 인덱스로 보내집니다. `current`

```
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 Bucket 메타데이터 알림 구성

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 S3:PutBucketMetadataNotification 권한이 있거나 계정 루트여야 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, 접두사가 있는 개체의 메타데이터를 한 대상으로 보내고, 접두사가 있는 개체는 `/videos` 다른 대상으로 보낼 수 `/images` 있습니다.

중복되는 접두사가 있는 구성은 유효하지 않으며 제출될 때 거부됩니다. 예를 들어, 접두사가 있는 객체에 대한 하나의 규칙과 접두사가 있는 객체에 대한 두 번째 규칙이 `test2` 포함된 구성은 `test` 허용되지 않습니다.

대상은 StorageGRID 끝점의 URN을 사용하여 지정해야 합니다. 메타데이터 알림 구성이 제출될 때 끝점이 존재해야 합니다. 그렇지 않으면 요청이 로 `400 Bad Request` 실패합니다. 오류 메시지는 다음과 같습니다. `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: 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. • `es` 세 번째 요소여야 합니다. • URN은 메타데이터가 저장되는 인덱스 및 형식으로 끝나야 `domain-name/myindex/mytype` 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

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: date
Authorization: authorization string
Host: host

<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 접두사와 일치하는 개체의 개체 메타데이터가 `/images` 한 대상으로 전송되고, 접두사와 일치하는 개체의 개체 메타데이터가 `/videos` 두 번째 대상으로 전송됩니다.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<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 예제는 키가 있는 개체가 라는 버킷에 `test` 생성될 때 생성될 수 있는 JSON의 예를 보여줍니다 `SGWS/Tagging.txt`. `test`버킷이 버전이 아니므로 `versionId` 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	버킷 영역(예: `us-east-1`
시스템 메타데이터	크기	HTTP 클라이언트에 표시되는 개체 크기(바이트)입니다
시스템 메타데이터	MD5(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

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.

관련 정보

"테넌트 계정을 사용합니다"

스토리지 사용 요청 가져오기

Get Storage Usage 요청은 계정이 사용하는 총 스토리지 양과 계정과 연결된 각 버킷에 대해 알려줍니다.

계정과 해당 버킷에서 사용하는 스토리지의 양은 쿼리 매개 변수를 사용하여 수정된 ListBucket 요청에서 가져올 수 `x-ntap-sg-usage` 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 루트여야 합니다.

요청 예

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

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 응답의 및 `DataBytes` 값에 영향을 `ObjectCount` 줍니다. 표식 삭제는 합계에 추가되지 `ObjectCount` 않습니다.

관련 정보

"일관성 값"

레거시 규정 준수를 위한 더 이상 사용되지 않는 버킷 요청

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 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
- "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 규정 준수"

  Get Bucket 준수 요청은 더 이상 사용되지 않습니다. 그러나 이 요청을 계속 사용하여 기존 레거시 준수 버킷에 현재 적용되는 준수 설정을 확인할 수 있습니다.

- "사용되지 않음 - Put 버킷 준수"

  Put Bucket 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 위한 **CreateBucket** 요청 수정

SGCompliance XML 요소는 사용되지 않습니다. 이전에는 이 StorageGRID 사용자 지정 요소를 CreateBucket 요청의 선택적 XML 요청 본문에 포함시켜 준수 버킷을 만들 수 있었습니다.

> 이전 StorageGRID 버전에서 사용할 수 있었던 StorageGRID 규정 준수 기능은 더 이상 사용되지 않으며 S3 오브젝트 잠금으로 대체되었습니다. 자세한 내용은 다음을 참조하십시오.
>
> - "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
> - "NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

Compliance가 설정된 새 버킷을 더 이상 생성할 수 없습니다. 규정 준수를 위해 CreateBucket 요청 수정을 사용하여 새 준수 버킷을 생성하려고 하면 다음 오류 메시지가 반환됩니다.

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

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. 자세한 내용은 다음을 참조하십시오.
>
> - "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
> - "NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

이 작업을 완료하려면 S3:GetBucketCompliance 권한이 있거나 계정 루트여야 합니다.

요청 예

이 예제 요청을 사용하면 이름이 인 버킷에 대한 준수 설정을 결정할 `mybucket` 수 있습니다.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

응답 예

응답 XML에 `<SGCompliance>` 버킷에 대해 적용되는 준수 설정이 나열됩니다. 이 예제 응답에서는 오브젝트를 그리드에 인제스트하는 시점을 시작으로 각 오브젝트를 1년(525,600분)동안 보존할 버킷의 규정 준수 설정을 보여 줍니다. 현재 이 버킷에 대한 법적 보류가 없습니다. 각 개체는 1년 후에 자동으로 삭제됩니다.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
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.

이름	설명
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

버킷이 규정을 준수하도록 생성되지 않은 경우 응답에 대한 HTTP 상태 코드는 S3 오류 코드 인 `XNoSuchBucketCompliance` 입니다 `404 Not Found`.

폐기됨: 버킷 준수 요청을 넣으십시오

Put Bucket 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. 자세한 내용은 다음을 참조하십시오.
>
> • "S3 REST API를 사용하여 S3 오브젝트 잠금을 구성합니다"
> • "NetApp 기술 자료: StorageGRID 11.5에서 레거시 준수 버킷을 관리하는 방법"

이 작업을 완료하려면 S3:PutBucketCompliance 권한이 있거나 계정 루트 권한이 있어야 합니다.

PUT 버킷 준수 요청을 발행할 때 준수 설정의 모든 필드에 값을 지정해야 합니다.

요청 예

이 예제 요청은 이름이 인 버킷의 준수 설정을 `mybucket` 수정합니다. 이 예에서 의 객체는 이제 1년이 아닌 2년 동안(1,051,200분) 보존되며, 이는 객체가 `mybucket` 그리드로 유입되는 시점부터 시작됩니다. 이 버킷에는 법적 구속이 없습니다. 각 개체는 2년 후에 자동으로 삭제됩니다.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
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. • 중요 * RetentionPeriodMinutes 에 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 설정에 대한 일관성

PUT 버킷 준수 요청으로 S3 버킷의 준수 설정을 업데이트하면 StorageGRID는 그리드 전체에서 버킷의 메타데이터를 업데이트하려고 시도합니다. 기본적으로 StorageGRID은 * 강력한 글로벌 * 일관성을 사용하여 버킷 메타데이터가 포함된 모든 데이터 센터 사이트와 모든 스토리지 노드에서 변경된 규정 준수 설정에 대해 쓰기 후 읽기 정합성을 보장합니다.

데이터 센터 사이트 또는 사이트의 여러 스토리지 노드를 사용할 수 없기 때문에 StorageGRID에서 * 강력한 글로벌 * 일관성을 달성할 수 없는 경우 응답에 대한 HTTP 상태 코드는 입니다 `503 Service Unavailable.`

이 응답을 받으면 그리드 관리자에게 문의하여 필요한 스토리지 서비스를 가능한 빨리 사용할 수 있도록 해야 합니다. 그리드 관리자가 각 사이트에서 스토리지 노드를 충분히 사용할 수 없는 경우 기술 지원 부서에서 * 강력한 사이트 * 일관성을 적용하여 실패한 요청을 다시 시도하도록 지시할 수 있습니다.

기술 지원 부서의 지시가 있거나 이 레벨을 사용할 때 발생할 수 있는 결과를 이해하지 않는 한, Put Bucket 준수를 위해 *Strong-site * 일관성을 강제로 적용하지 마십시오.

일관성이 * 강력한 사이트 * 로 감소하면 StorageGRID는 업데이트된 규정 준수 설정이 사이트 내 클라이언트 요청에 대해서만 쓰기 후 읽기 일관성을 유지할 수 있도록 보장합니다. 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 중에 두고 일관성을 더 낮게 설정하면 일부 데이터 센터 사이트에서 버킷의 이전 규정 준수 설정(즉, 법적 증거 자료 보관)이 계속 적용될 수 있습니다. 따라서 보존 기간이 만료되면 사용자나 자동 삭제(활성화된 경우)에 의해 법적 보류라고 생각하는 개체가 삭제될 수 있습니다.

Strong-site * 일관성을 강제로 사용하려면 다음과 같이 Put Bucket 준수 요청을 다시 발행하고 HTTP 요청 헤더를 포함시킵니다. `Consistency-Control`

```
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 입니다 `404 Not Found`.
- 요청에서 버킷의 현재 보존 기간보다 작은 경우 `RetentionPeriodMinutes` HTTP 상태 코드는 입니다 `400 Bad Request`.

관련 정보

"사용되지 않음: 규정 준수를 위해 버킷 요청 수정을 배치합니다"

버킷 및 그룹 액세스 정책

버킷 및 그룹 액세스 정책을 사용합니다

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 * - GetBucketPolicy, PutBucketPolicy 및 DeleteBucketPolicy S3 API 작업 또는 테넌트 관리자 또는 테넌트 관리 API를 사용하여 관리됩니다. 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.

그룹 정책과 버킷 정책 간에는 우선 순위에 차이가 없습니다.

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.
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 것 외에는 와일드카드 문자는 지원되지 않습니다. 예를 들어 와일드카드(*)를 Principal 값으로 설정합니다.

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

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

다음 예제에서는 Effect , Principal , Action 및 Resource 요소를 사용합니다. 이 예에서는 "허용"의 효과를 사용하여 Principals, 관리자 그룹 및 재무 그룹 `federated-group/finance`, 이름이 지정된 버킷에서 `mybucket` 작업을 수행할 수 있는 권한 `s3:ListBucket` 및 해당 버킷 내의 모든 객체에 대한 작업을 `s3:GetObject` 제공하는 완전한 버킷 정책 문을 보여 `federated-group/admin` 줍니다.

```
{
  "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:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

버킷 정책은 크기 제한이 20,480바이트이고 그룹 정책은 크기 제한이 5,120바이트입니다.

정책의 일관성

기본적으로 그룹 정책에 대한 모든 업데이트는 최종적으로 일치합니다. 그룹 정책이 일관되면 정책 캐싱으로 인해 변경 내용이 적용되는 데 15분이 더 걸릴 수 있습니다. 기본적으로 버킷 정책에 대한 모든 업데이트는 매우 일관적입니다.

필요에 따라 버킷 정책 업데이트의 일관성 보장을 변경할 수 있습니다. 예를 들어 사이트 중단 중에 버킷 정책의 변경을 사용할 수 있도록 할 수 있습니다.

이 경우 PutBucketPolicy 요청에서 헤더를 설정하거나 Put Bucket 정합성 요청을 사용할 수 `Consistency-Control` 있습니다. 버킷 정책의 정합성이 보장되면 정책 캐싱으로 인해 변경 내용이 적용되는 데 8초 더 걸릴 수 있습니다.

> 일시적 상황을 해결하기 위해 일관성을 다른 값으로 설정한 경우 작업을 마치면 버킷 수준 설정을 원래 값으로 다시 설정해야 합니다. 그렇지 않으면 이후의 모든 버킷 요청에 수정된 설정이 사용됩니다.

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"

  PutBucketPolicy 작업에 대한 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 요소로 표시되거나 `NotResource` 제외를 위해

요소로 `Resource` 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.

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 주체는 "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 Alex가 조직을 떠나고 사용자 이름이 삭제된다고 가정해 `Alex` 보겠습니다. 새 Alex가 조직에 합류하여 동일한 사용자 이름이 할당된 경우 `Alex` 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.

> 이제 Amazon S3는 PutBucketReplication 및 DeleteBucketReplication 작업 모두에 대해 S3:PutReplicationConfiguration 권한을 사용합니다. StorageGRID는 원래 Amazon S3 사양과 일치하는 각 작업에 대해 별도의 권한을 사용합니다.

> 기존 값을 덮어쓰는 데 PUT을 사용할 때 삭제가 수행됩니다.

버킷에 적용되는 권한

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:생성 버킷	CreateBucket	예. • 참고 *: 그룹 정책에만 사용합니다.
S3:삭제 버킷	삭제 버킷	

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:DeleteBucketMetadataNotification	버킷 메타데이터 알림 구성을 삭제합니다	예
S3:삭제 BucketPolicy	DeleteBuckketPolicy를 참조하십시오	
S3:DeleteReplicationConfiguration	DeleteBuckReplication 을 참조하십시오	예, 삽입 및 삭제 권한을 구분합니다
S3:GetBuckketAcl	GetBuckketAcl	
S3:GetBucketCompliance	버킷 규정 준수 가져오기(더 이상 사용되지 않음)	예
S3:GetBuckketConsistency	버킷 일관성 확보	예
S3:GetBuckketCORS	GetBuckketCors 를 참조하십시오	
S3:GetEncryptionConfiguration	GetBuckketEncryption을 참조하십시오	
S3:GetBucketLastAccessTime	버킷 최종 액세스 시간 가져오기	예
S3:GetBucketLocation	GetBucketLocation 을 참조하십시오	
S3:GetBuckMetadataNotification 을 참조하십시오	Bucket 메타데이터 알림 구성 가져오기	예
S3:GetBucketNotification 을 참조하십시오	GetBuckNotificationConfiguration 을 참조하십시오	
S3:GetBuckketObjectLockConfiguration	GetObjectLockConfiguration 을 참조하십시오	
S3:GetBuckketPolicy를 참조하십시오	GetBuckketPolicy를 참조하십시오	
S3:GetBucketTagging	GetBucketTagging	
S3:GetBucketVersioning	GetBuckketVersioning 을 참조하십시오	
S3:GetLifecycleConfiguration	GetBuckLifecycleConfiguration 을 참조하십시오	
S3:GetReplicationConfiguration	GetBucketReplication 을 참조하십시오	

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:ListAllMyBucket	• ListBucket • 스토리지 사용량을 가져옵니다	예, 스토리지 사용량 가져오기. • 참고 *: 그룹 정책에만 사용합니다.
S3:목록 버킷	• ListObjects 를 선택합니다 • 머리버킷 • RestoreObject 를 선택합니다	
S3:ListBuckketMultipartUploads	• ListMultipartUploads 를 참조하십시오 • RestoreObject 를 선택합니다	
S3:목록 BuckketVersions	버킷 버전 가져오기	
S3: PutBucketCompliance	버킷 규정 준수(폐기됨)	예
S3: PutBucketConsistency	버킷 일관성을 유지합니다	예
S3: PutBucketCORS	• DeleteBucketCors † • BuckketCors의	
S3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption을 참조하십시오	
S3:PutBucketLastAccessTime	버킷 최종 접근 시간	예
S3:PutBucketMetadataNotification	Put Bucket 메타데이터 알림 구성	예
S3: PutBucketNotification	PutBucketNotificationConfiguration을 참조하십시오	
S3:PutBucketObjectLockConfiguration	• 요청 헤더가 있는 CreateBucket `x-amz-bucket-object-lock-enabled: true`(S3:CreateBucket 권한도 필요) • PutObjectLockConfiguration 을 참조하십시오	
S3: PutBucketPolicy	BucketPolicy를 참조하십시오	

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3: PutBucketTagging	• DeleteBucketTagging † 를 참조하십시오 • BucketTagging	
S3: PutBucketVersioning	PutBucketVersioning을 참조하십시오	
S3: PutLifecycleConfiguration	• DeleteBucketLifecycle † 을 참조하십시오 • PutBucketLifecycleConfiguration을 참조하십시오	
S3:PutReplicationConfiguration	PutBucketReplication을 참조하십시오	예, 삽입 및 삭제 권한을 구분합니다

객체에 적용되는 권한

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:중단멀티업로드입니다	• AbortMultipartUpload 를 클릭합니다 • RestoreObject 를 선택합니다	
S3:BypassGovernanceRetention	• DeleteObject 를 클릭합니다 • DeleteObjects 를 클릭합니다 • PutObjectRetention	
S3:DeleteObject 를 선택합니다	• DeleteObject 를 클릭합니다 • DeleteObjects 를 클릭합니다 • RestoreObject 를 선택합니다	
S3:삭제 ObjectTagging	DeleteObjectTagging 을 선택합니다	
S3:DeleteObjectVersionTagging	DeleteObjectTagging(개체의 특정 버전)	
S3:DeleteObjectVersion	DeleteObject(개체의 특정 버전)	
S3:GetObject	• GetObject 를 참조하십시오 • HeadObject 를 선택합니다 • RestoreObject 를 선택합니다 • SelectObjectContent 를 선택합니다	

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:GetObjectAcl	GetObjectAcl	
S3:GetObjectLegalHold	GetObjectLegalHold 를 참조하십시오	
S3:GetObjectRetention	GetObjectRetention을 참조하십시오	
S3:GetObjectTagging	GetObjectTagging	
S3:GetObjectVersionTagging	GetObjectTagging(개체의 특정 버전)	
S3:GetObjectVersion	GetObject(개체의 특정 버전)	
S3:ListMultipartUploadParts(S3:ListMultimpartUploadParts) 를	ListParts, RestoreObject 를 참조하십시오	
S3:PutObject	• PutObject 를 선택합니다 • CopyObject 를 선택합니다 • RestoreObject 를 선택합니다 • CreateMultptUpload 를 클릭합니다 • CompleteMultipartUpload를 클릭합니다 • 업로드 파트 • 업로드파트 복사	
S3:PutObjectLegalHold	PutObjectLegalHold를 선택합니다	
S3:PutObjectRetention	PutObjectRetention	
S3:PutObjectTagging	PutObjectTagging	
S3:PutObjectVersionTagging	PutObjectTagging(개체의 특정 버전)	
S3:PutOverwriteObject	• PutObject 를 선택합니다 • CopyObject 를 선택합니다 • PutObjectTagging • DeleteObjectTagging 을 선택합니다 • CompleteMultipartUpload를 클릭합니다	예
S3:RestoreObject	RestoreObject 를 선택합니다	

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 관리를 사용하는 경우 거부 설정을 사용하면 PutObjectTagging 또는 DeleteObjectTagging 작업에서 개체 및 해당 비최신 버전에 대한 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 * > * 보안 설정 * > * 네트워크 및 개체 *) 해당 설정은 PutOverwriteObject 권한 설정을 재정의합니다.

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).
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? 와일드카드 문자를 포함할 수 있습니다.
StringNotLike 를 참조하십시오	키를 부정 일치(대/소문자 구분)를 기반으로 문자열 값과 비교합니다. 및? 와일드카드 문자를 포함할 수 있습니다.
NumericEquals	정확한 일치를 기준으로 키를 숫자 값과 비교합니다.
NumericNotEquals	키를 부정 일치를 기준으로 숫자 값과 비교합니다.
NumericGreaterThan	"보다 큼" 일치를 기준으로 키를 숫자 값과 비교합니다.
NumericGreaterThanEquals	"보다 크거나 같음" 일치를 기준으로 키를 숫자 값과 비교합니다.
NumericLessThan	"보다 작음" 일치를 기준으로 키를 숫자 값과 비교합니다.
NumericLessThanEquals	"보다 작거나 같음" 일치를 기준으로 키를 숫자 값과 비교합니다.
불입니다	"true 또는 false" 일치를 기준으로 키를 부울 값과 비교합니다.
IP 주소	키를 IP 주소 또는 IP 주소 범위와 비교합니다.

조건 연산자	설명
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

상태 키	작업	설명
AWS: SOURCEIP	IP 연산자	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`헤더의 유효성을 확인할 수 없으므로 헤더는 무시됩니다.
AWS: 사용자 이름	리소스/ID입니다	요청이 전송된 보낸 사람의 사용자 이름과 비교합니다. 버킷 또는 오브젝트 작업에 사용할 수 있습니다.
S3: 구분 기호	S3:ListBucket 및 S3: ListBuckketVersions 권한	는 ListObjects 또는 ListObjectVersions 요청에 지정된 구분 기호 매개 변수와 비교됩니다.

상태 키	작업	설명
S3: ExistingObjectTag/<tag-key>	S3:삭제 ObjectTagging S3:DeleteObjectVersionTagging S3:GetObject S3:GetObjectAcl 3: GetObjectTagging S3:GetObjectVersion S3:GetObjectVersionAcl S3:GetObjectVersionTagging S3: PutObjectAcl S3:PutObjectTagging S3: PutObjectVersionAcl S3:PutObjectVersionTagging	기존 개체에 특정 태그 키와 값이 있어야 합니다.
S3: 최대 키	S3:ListBucket 및 S3: ListBuckketVersions 권한	는 ListObjects 또는 ListObjectVersions 요청에 지정된 max-keys 매개 변수와 비교됩니다.
S3: 오브젝트 잠금 장치 - 남은 보존 기간(일)	S3:PutObject	요청 헤더에 지정되거나 버킷 기본 보존 기간에서 계산된 유지 종료 날짜와 비교하여 `x-amz-object-lock-retain-until-date` 이러한 값이 다음 요청에 대해 허용되는 범위 내에 있는지 확인합니다. • PutObject 를 선택합니다 • CopyObject 를 선택합니다 • CreateMultptUpload 를 클릭합니다
S3: 오브젝트 잠금 장치 - 남은 보존 기간(일)	S3:PutObjectRetention	PutObjectRetention 요청에 지정된 유지 종료 날짜와 비교하여 허용 범위 내에 있는지 확인합니다.
S3: 접두어	S3:ListBucket 및 S3: ListBuckketVersions 권한	는 ListObjects 또는 ListObjectVersions 요청에 지정된 접두사 매개 변수와 비교됩니다.

상태 키	작업	설명
S3: RequestObjectTag/<tag-key>	S3:PutObject S3:PutObjectTagging S3:PutObjectVersionTagging	개체 요청에 태그가 포함된 경우 특정 태그 키와 값이 필요합니다.

정책에 변수를 지정합니다

정책의 변수를 사용하여 사용 가능한 정책 정보를 채울 수 있습니다. 요소의 문자열 비교와 요소에 `Condition` 정책 변수를 사용할 수 `Resource` 있습니다.

이 예제에서 변수는 `${aws:username}` Resource 요소의 일부입니다.

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

이 예제에서 변수는 `${aws:username}` 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 리터럴? 문자로 사용합니다.
`${$}`	특수 문자. 문자를 리터럴 $ 문자로 사용합니다.

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 * > * 보안 * > * 보안 설정 * > * 네트워크 및 개체 * 로 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 PutObject 허용 작업을 추가합니다.

> S3 정책에서 DeleteObject를 DENY로 설정해도 "30일 후 복사본 제로" 같은 규칙이 있을 때 ILM이 개체를 삭제할 수 없습니다.

> 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

- "StorageGRID ILM 규칙이 개체를 관리하는 방법"

- "버킷 정책의 예"
- "그룹 정책의 예"
- "ILM을 사용하여 개체를 관리합니다"
- "테넌트 계정을 사용합니다"

버킷 정책의 예

이 섹션의 예를 사용하여 버킷에 대한 StorageGRID 액세스 정책을 구축합니다.

버킷 정책은 정책이 연결된 버킷에 대한 액세스 권한을 지정합니다. 다음 툴 중 하나를 통해 S3 PutBucketPolicy API를 사용하여 버킷 정책을 구성합니다.

- "테넌트 관리자"..
- 다음 명령을 사용하는 AWS CLI(참조"버킷 작업"):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

예: 모든 사용자가 버킷에 읽기 전용 액세스를 허용합니다

이 예제에서는 anonymous를 비롯한 모든 사용자가 버킷의 오브젝트를 나열하고 버킷의 모든 오브젝트에 대해 GetObject 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 한 계정의 모든 사용자가 버킷에 대한 전체 액세스를 허용하지만 다른 지정된 계정의 모든 사용자는 버킷을 나열하고 오브젝트 키 접두사로 시작하는 버킷의 객체에 대해 GetObject 작업을 수행할 수만 `shared/` 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 예제에서는 anonymous를 포함한 모든 사용자가 버킷의 모든 오브젝트에 대해 버킷을 나열하고 GetObject 작업을 수행할 수 있지만 지정된 계정의 그룹에 속한 사용자만 `Marketing` 전체 액세스를 허용합니다.

```
{
  "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 버킷 및 해당 객체에 대한 전체 액세스를 `examplebucket` 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::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

예: **PutOverwriteObject** 권한

이 예제에서 `Deny` PutOverwriteObject 및 DeleteObject 의 효과는 아무도 개체의 데이터, 사용자 정의 메타데이터 및 S3 개체 태그를 덮어쓰거나 삭제할 수 없도록 합니다.

```
{
  "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/*"
    }
  ]
}
```

그룹 정책의 예

이 섹션의 예제를 사용하여 그룹에 대한 StorageGRID 액세스 정책을 작성합니다.

그룹 정책은 정책이 연결된 그룹에 대한 액세스 권한을 지정합니다. `Principal`이 정책은 암시적이기 때문에 정책에 요소가 없습니다. 그룹 정책은 테넌트 관리자 또는 API를 사용하여 구성됩니다.

예: 테넌트 관리자를 사용하여 그룹 정책을 설정합니다

테넌트 관리자에서 그룹을 추가하거나 편집할 때 그룹 정책을 선택하여 이 그룹의 구성원이 가질 S3 액세스 권한을 결정할 수 있습니다. 을 "S3 테넌트에 대한 그룹을 생성합니다"참조하십시오.

- * S3 액세스 없음 *: 기본 옵션. 버킷 정책을 통해 액세스 권한이 부여되지 않은 한 이 그룹의 사용자는 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 문자열을 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 문자열을 편집할 수 없습니다.
- * 랜섬웨어 완화 *: 이 샘플 정책은 이 테넌트의 모든 버킷에 적용됩니다. 이 그룹의 사용자는 일반적인 작업을 수행할 수 있지만 개체 버전 관리가 활성화된 버킷에서 개체를 영구적으로 삭제할 수는 없습니다.

  모든 버킷 관리 권한이 있는 테넌트 관리자 사용자는 이 그룹 정책을 재정의할 수 있습니다. 모든 버킷 관리 권한을 신뢰할 수 있는 사용자로 제한하고 가능한 경우 MFA(Multi-Factor Authentication)를 사용합니다.

- * 사용자 정의 *: 그룹의 사용자에게는 텍스트 상자에 지정한 사용 권한이 부여됩니다.

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 "폴더"에만 모든 권한을 부여할 수 있습니다

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}/*"
    }
  ]
}
```

감사 로그에서 **S3** 작업을 추적했습니다

감사 메시지는 StorageGRID 서비스에서 생성되고 텍스트 로그 파일에 저장됩니다. 감사 로그에서 S3별 감사 메시지를 검토하여 버킷 및 오브젝트 작업에 대한 세부 정보를 확인할 수 있습니다.

감사 로그에서 버킷 작업을 추적했습니다

- CreateBucket
- 삭제 버킷
- 삭제 BucketTagging
- DeleteObjects 를 클릭합니다
- GetBucketTagging
- 머리버킷
- ListObjects 를 선택합니다
- ListObjectVersions 를 선택합니다
- 버킷 규정 준수
- BucketTagging
- PutBucketVersioning을 참조하십시오

감사 로그에서 추적된 객체 작업입니다

- CompleteMultipartUpload를 클릭합니다
- CopyObject 를 선택합니다
- DeleteObject 를 클릭합니다
- GetObject 를 참조하십시오
- HeadObject 를 선택합니다
- PutObject 를 선택합니다
- RestoreObject 를 선택합니다
- 개체 를 선택합니다
- UploadPart(ILM 규칙이 Balanced 또는 Strict 수집을 사용하는 경우)
- UploadPartCopy(ILM 규칙이 Balanced 또는 Strict 수집을 사용하는 경우)

관련 정보

- "감사 로그 파일에 액세스합니다"
- "클라이언트가 감사 메시지를 기록합니다"
- "클라이언트가 감사 메시지를 읽습니다"

Swift REST API 사용(지원 종료)

Swift REST API를 사용합니다

Swift API에 대한 지원이 중단되었으며 향후 릴리즈에서 제거될 예정입니다.

이 버전의 문서 사이트에서 Swift 세부 정보가 제거되었습니다. 을 "StorageGRID 11.8: Swift REST API 사용"참조하십시오.

StorageGRID 시스템을 모니터링하고 문제 해결

StorageGRID 시스템을 모니터링합니다

StorageGRID 시스템을 모니터링합니다

StorageGRID 시스템을 정기적으로 모니터링하여 예상대로 작동하는지 확인합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

> Grid Manager에 표시된 스토리지 값의 단위를 변경하려면 Grid Manager의 오른쪽 상단에서 사용자 드롭다운을 선택한 다음 * User preferences * 를 선택합니다.

이 작업에 대해

이 지침에서는 다음을 수행하는 방법을 설명합니다.

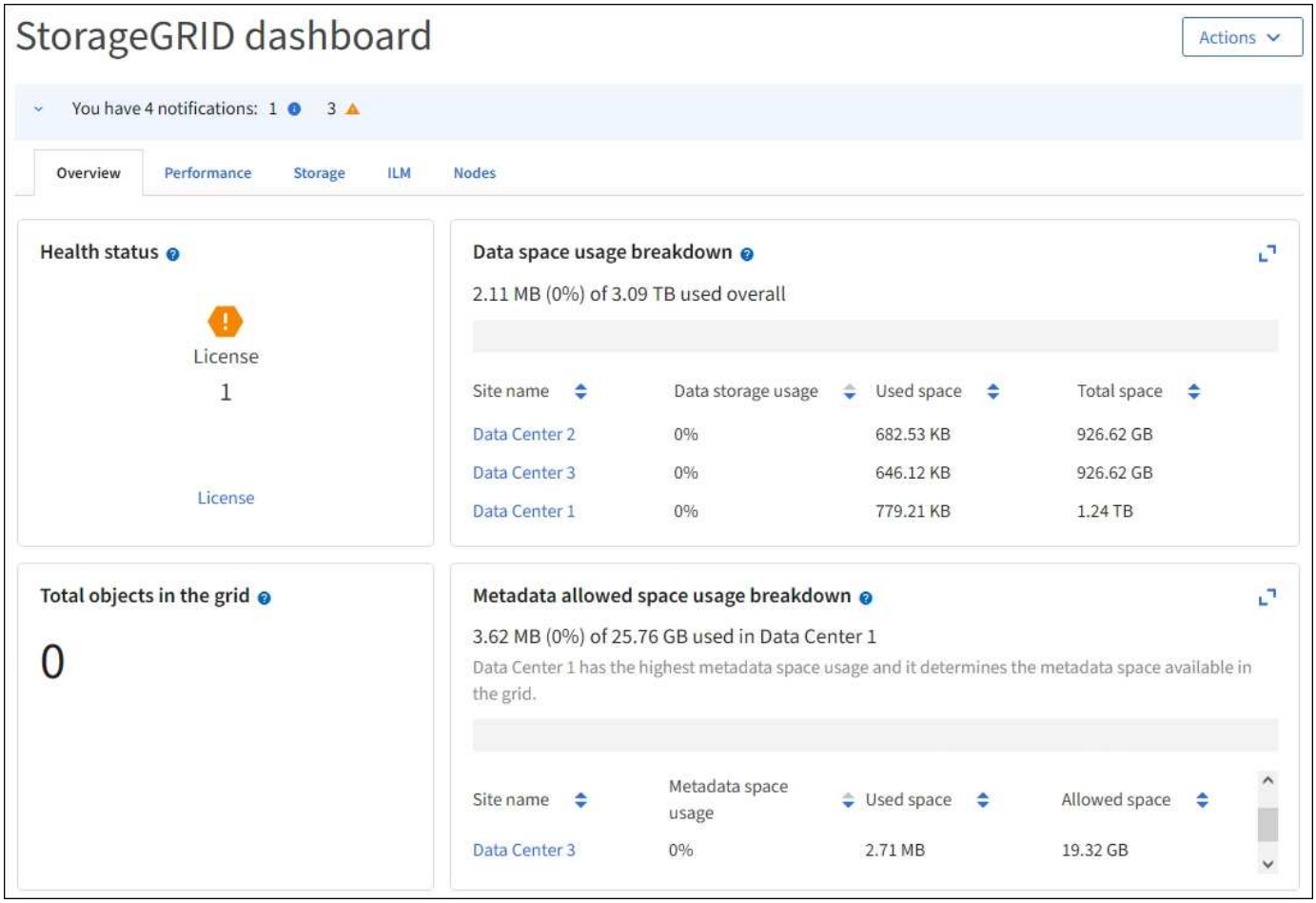
- "대시보드를 보고 관리합니다"
- "노드 페이지를 봅니다"
- "시스템의 이러한 측면을 정기적으로 모니터링합니다."
  - "시스템 상태입니다"
  - "스토리지 용량"
  - "정보 수명 주기 관리"
  - "네트워킹 및 시스템 리소스"
  - "테넌트 작업"
  - "로드 밸런싱 작업"
  - "그리드 페더레이션 연결"
- "알림을 관리합니다"
- "로그 파일을 봅니다"
- "감사 메시지 및 로그 대상을 구성합니다"
- "외부 syslog 서버를 사용합니다" 감사 정보를 수집합니다
- "모니터링에 SNMP를 사용합니다"
- "추가 StorageGRID 데이터를 가져옵니다"측정 지표 및 진단 포함

대시보드를 보고 관리합니다

대시보드를 사용하여 시스템 작업을 한 눈에 모니터링할 수 있습니다. 사용자 지정 대시보드를 만들어 StorageGRID 구현을 모니터링할 수 있습니다.

Grid Manager에 표시된 스토리지 값의 단위를 변경하려면 Grid Manager의 오른쪽 상단에서 사용자 드롭다운을 선택한 다음 * User preferences * 를 선택합니다.

대시보드는 시스템 구성에 따라 다를 수 있습니다.



대시보드 보기

대시보드는 StorageGRID 시스템에 대한 특정 정보가 포함된 탭으로 구성됩니다. 각 탭에는 카드에 표시되는 정보의 범주가 포함되어 있습니다.

시스템에서 제공하는 대시보드를 그대로 사용할 수 있습니다. 또한 StorageGRID 구현 모니터링과 관련된 탭과 카드만 포함하는 사용자 지정 대시보드를 만들 수 있습니다.

시스템에서 제공하는 대시보드 탭에는 다음과 같은 유형의 정보가 있는 카드가 포함되어 있습니다.

Tab 키를 눌러 시스템 제공 대시보드로 이동합니다	포함
개요	활성 알림, 공간 사용량, 그리드의 총 개체 등 그리드에 대한 일반 정보입니다.
성능	공간 사용량, 시간에 따른 스토리지, S3 작업, 요청 기간, 오류율

Tab 키를 눌러 시스템 제공 대시보드로 이동합니다	포함
스토리지	테넌트 할당량 사용 및 논리적 공간 사용. 사용자 데이터 및 메타데이터의 공간 사용량을 예측합니다.
ILM을 참조하십시오	정보 수명 주기 관리 대기열 및 평가 비율.
노드	노드별 CPU, 데이터 및 메모리 사용량 노드별 S3 작업 노드-사이트 배포

일부 카드는 보다 쉽게 볼 수 있도록 최대화할 수 있습니다. 카드의 오른쪽 상단 모서리에 있는 최대화 아이콘을 선택합니다. 최대화된 카드를 닫으려면 최소화 아이콘을 선택하거나 * 닫기 * 를 선택합니다.

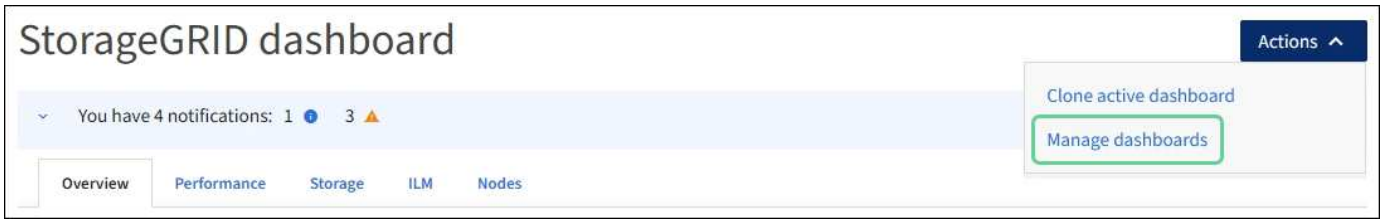
대시보드를 관리합니다

루트 액세스 권한이 있는 경우(참조"관리자 그룹 권한") 대시보드에 대해 다음 관리 작업을 수행할 수 있습니다.

- 처음부터 사용자 지정 대시보드를 만듭니다. 사용자 지정 대시보드를 사용하여 표시되는 StorageGRID 정보와 해당 정보의 구성 방법을 제어할 수 있습니다.
- 대시보드를 복제하여 사용자 지정 대시보드를 생성합니다.
- 사용자의 활성 대시보드를 설정합니다. 액티브 대시보드는 시스템 제공 대시보드 또는 사용자 지정 대시보드일 수 있습니다.
- 기본 대시보드를 설정합니다. 이 대시보드는 모든 사용자가 자신의 대시보드를 활성화하지 않는 한 표시됩니다.
- 대시보드 이름을 편집합니다.
- 대시보드를 편집하여 탭과 카드를 추가하거나 제거합니다. 최소 1개 및 최대 20개의 탭을 사용할 수 있습니다.
- 대시보드를 제거합니다.

루트 액세스 이외의 다른 권한이 있는 경우 활성 대시보드만 설정할 수 있습니다.

대시보드를 관리하려면 * Actions * > * Manage Dashboards * 를 선택합니다.



대시보드를 구성합니다

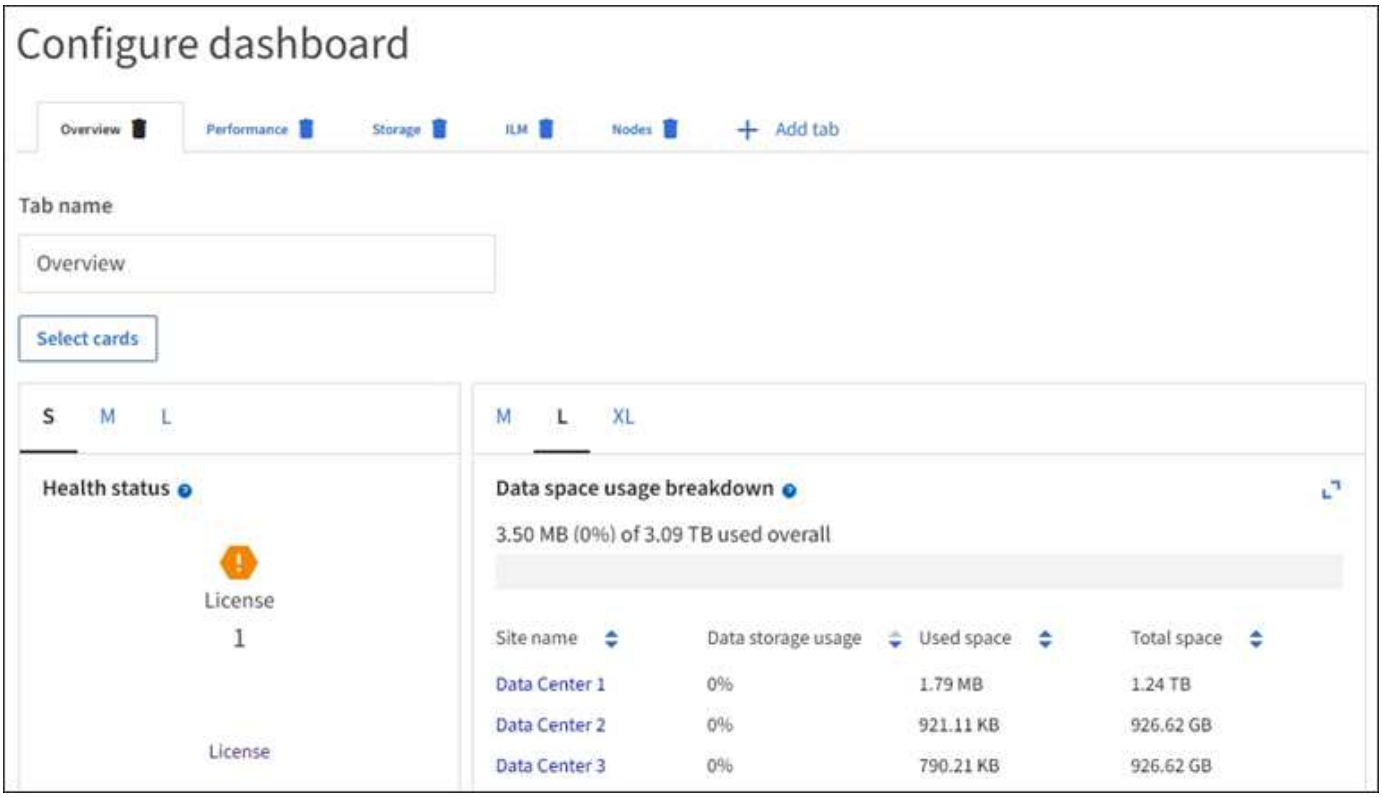
활성 대시보드를 복제하여 새 대시보드를 생성하려면 * Actions * > * Clone active dashboard * 를 선택합니다.

기존 대시보드를 편집하거나 복제하려면 * 작업 * > * 대시보드 관리 * 를 선택합니다.

시스템에서 제공하는 대시보드는 편집하거나 제거할 수 없습니다.

대시보드를 구성할 때 다음을 수행할 수 있습니다.

- 탭을 추가하거나 제거합니다
- 탭 이름을 바꾸고 새 탭에 고유한 이름을 지정합니다
- 각 탭에 대한 카드를 추가, 제거 또는 다시 정렬(끌기)합니다
- 카드 상단에서 * S *, * M *, * L * 또는 * XL * 을 선택하여 개별 카드의 크기를 선택합니다



노드 페이지를 봅니다

노드 페이지를 봅니다

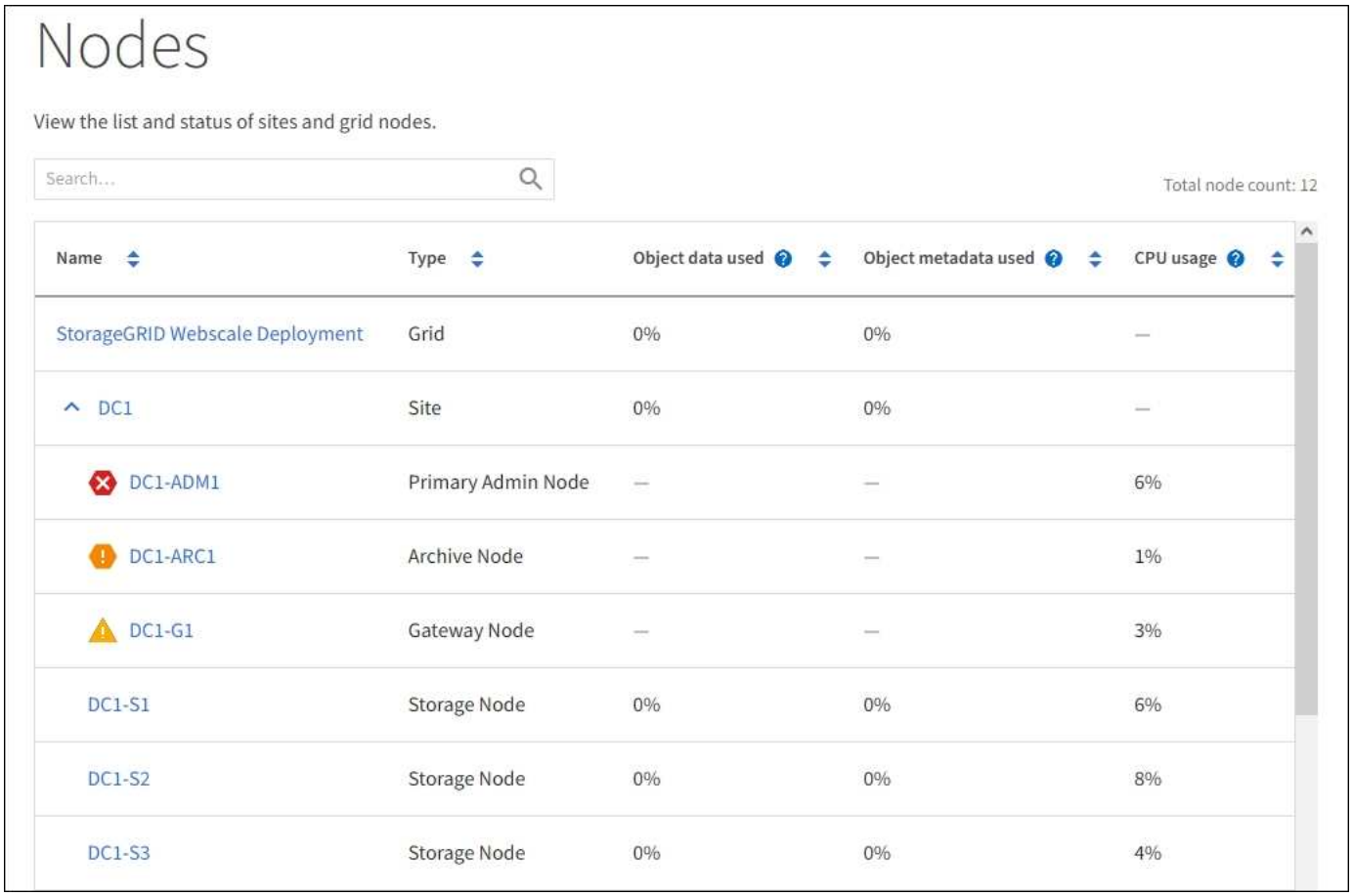
대시보드에서 제공하는 것보다 StorageGRID 시스템에 대한 자세한 정보가 필요한 경우 노드 페이지를 사용하여 전체 그리드, 그리드의 각 사이트 및 사이트의 각 노드에 대한 메트릭을 볼 수 있습니다.

노드 테이블에는 전체 그리드, 각 사이트 및 각 노드에 대한 요약 정보가 나열됩니다. 노드의 연결이 끊겼거나 활성 경고가 있는 경우 노드 이름 옆에 아이콘이 표시됩니다. 노드가 연결되어 있고 활성 경고가 없는 경우 아이콘이 표시되지 않습니다.

업그레이드 중 또는 연결 끊김 상태와 같이 노드가 그리드에 연결되어 있지 않으면 특정 메트릭을 사용할 수 없거나 사이트 및 그리드 합계에서 제외할 수 있습니다. 노드가 그리드에 다시 연결되면 값이 안정화될 때까지 몇 분 동안 기다립니다.

Grid Manager에 표시된 스토리지 값의 단위를 변경하려면 Grid Manager의 오른쪽 상단에서 사용자 드롭다운을 선택한 다음 * User preferences * 를 선택합니다.

표시된 스크린샷은 예시입니다. 결과는 StorageGRID 버전에 따라 다를 수 있습니다.



연결 상태 아이콘

노드가 그리드에서 분리되어 있는 경우 노드 이름 옆에 다음 아이콘 중 하나가 표시됩니다.

아이콘을 클릭합니다	설명	작업이 필요합니다
	• 연결되지 않음 - 알 수 없음 * 알 수 없는 이유로 노드의 연결이 끊기거나 노드의 서비스가 예기치 않게 다운되었습니다. 예를 들어, 노드의 서비스가 중지되거나 전원 장애 또는 예기치 않은 정전으로 인해 노드의 네트워크 연결이 끊겼을 수 있습니다. 노드 * 와 통신할 수 없음 알림도 트리거될 수 있습니다. 다른 알림도 활성화될 수 있습니다.	즉각적인 주의가 필요합니다. "각 경고를 선택합니다" 를 클릭하고 권장 조치를 따릅니다. 예를 들어, 노드의 호스트를 중지하거나 다시 시작한 서비스를 다시 시작해야 할 수 있습니다. • 참고 *: 관리되는 종료 작업 중에 노드가 알 수 없음으로 나타날 수 있습니다. 이러한 경우 알 수 없음 상태를 무시할 수 있습니다.

아이콘을 클릭합니다	설명	작업이 필요합니다
	• 연결되지 않음 - 관리 중단 * 예상된 이유로 노드가 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. 이러한 노드는 기본적인 문제를 기반으로 하여 별도의 개입 없이 온라인 상태로 되곤 합니다.	이 노드에 영향을 주는 알림이 있는지 확인합니다. 하나 이상의 알림이 활성화된 경우 "각 경고를 선택합니다"권장 조치를 따릅니다.

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.

* Critical *: StorageGRID 노드 또는 서비스의 정상 작동을 중지한 비정상 상태가 존재함. 기본 문제를 즉시 해결해야 합니다. 문제가 해결되지 않으면 서비스가 중단되거나 데이터가 손실될 수 있습니다.

Major: 현재 작업에 영향을 미치거나 중요 경고에 대한 임계값에 접근하는 비정상적인 상태가 존재합니다. StorageGRID 노드나 서비스의 정상 작동을 비정상적인 상태로 중지하지 않도록 주요 경고를 조사하고 모든 기본 문제를 해결해야 합니다.

Minor: 시스템이 정상적으로 작동하고 있지만, 시스템이 계속 작동할 경우 시스템 작동 능력에 영향을 줄 수 있는 비정상적인 상태가 있습니다. 보다 심각한 문제를 초래하지 않도록 자체적으로 명확하지 않은 사소한 경고를 모니터링하고 해결해야 합니다.

시스템, 사이트 또는 노드에 대한 세부 정보를 봅니다

노드 테이블에 표시된 정보를 필터링하려면 * 검색 * 필드에 검색 문자열을 입력합니다. 시스템 이름, 표시 이름 또는 유형별로 검색할 수 있습니다(예: * gat * 를 입력하여 모든 게이트웨이 노드를 빠르게 찾을 수 있습니다).

그리드, 사이트 또는 노드에 대한 정보를 보려면 다음을 수행합니다.

- 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.

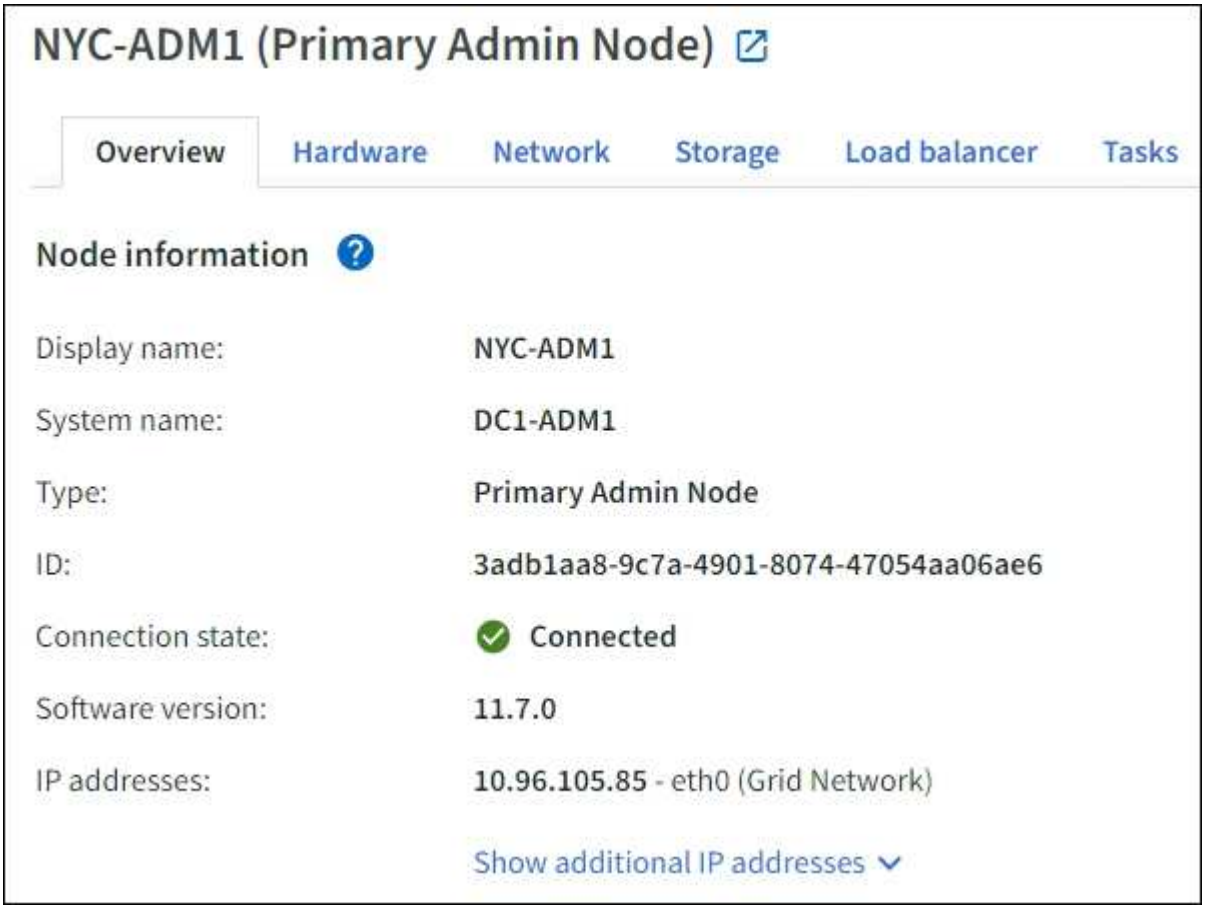
개요 탭을 봅니다

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 노드에 대한 기본 정보가 나열됩니다.



노드에 대한 개요 정보는 다음과 같습니다.

- * 표시 이름 * (노드 이름이 변경된 경우에만 표시됨): 노드의 현재 표시 이름입니다. 절차를 사용하여 "그리드, 사이트 및 노드의 이름을 바꿉니다"이 값을 업데이트합니다.
- * 시스템 이름 *: 설치하는 동안 노드에 대해 입력한 이름입니다. 시스템 이름은 내부 StorageGRID 작업에 사용되며 변경할 수 없습니다.
- * 유형 *: 노드 유형 - 관리자 노드, 기본 관리자 노드, 스토리지 노드 또는 게이트웨이 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 연결되지 않았거나 하나 이상의 서비스가 예기치 않게 다운되었습니다. 예를 들어, 노드 간 네트워크 연결이 끊어지거나, 전원이 꺼지거나, 서비스가 다운된 경우 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.

- *Administratively down* : 노드가 예상된 이유로 그리드에 연결되지 않았습니다. 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

개요 탭의 경고 섹션에 모든 항목이 "이 노드에 영향을 주는 경고로서, 해제되지 않았습니다"나열됩니다. 추가 세부 정보 및 권장 조치를 보려면 알림 이름을 선택하십시오.

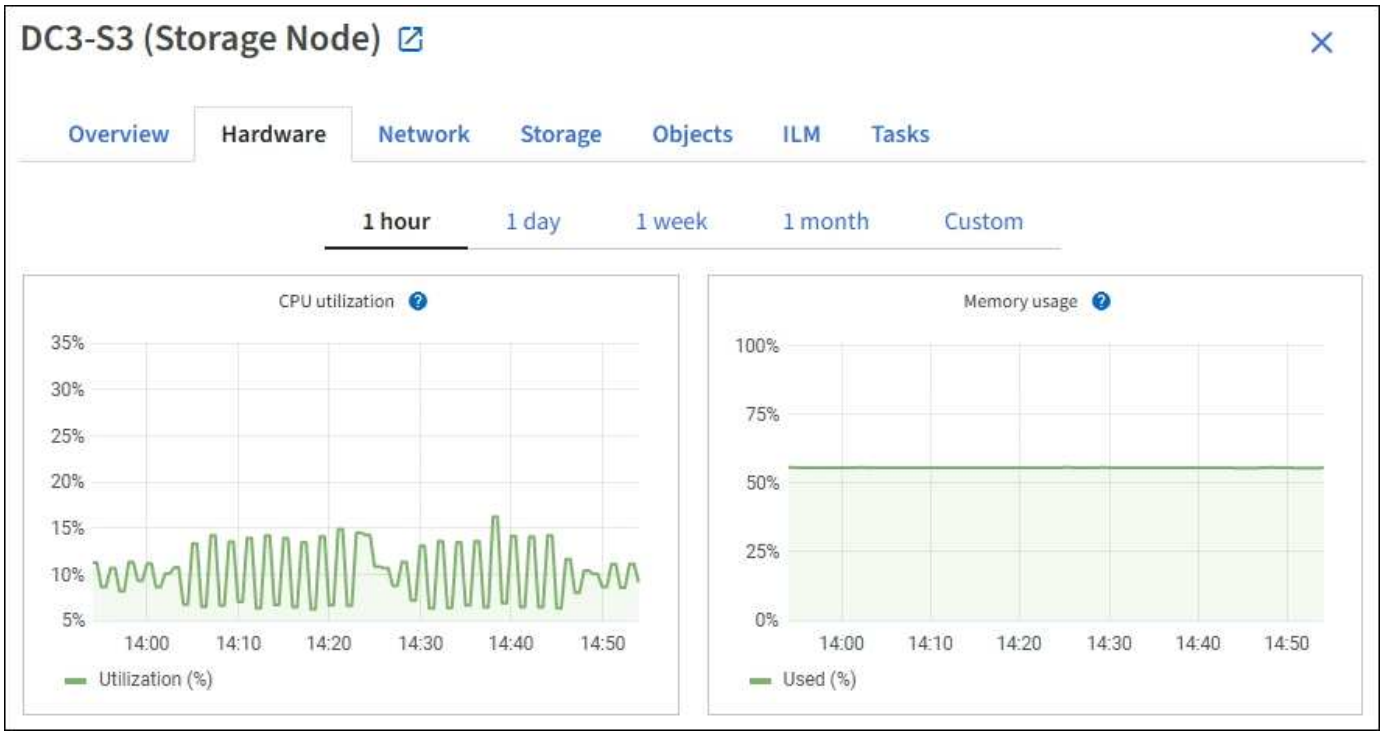
에 대한 알림도 "노드 연결 상태입니다"포함됩니다.

하드웨어 탭을 봅니다

하드웨어 탭에는 각 노드의 CPU 사용률 및 메모리 사용량, 어플라이언스에 대한 추가 하드웨어 정보가 표시됩니다.

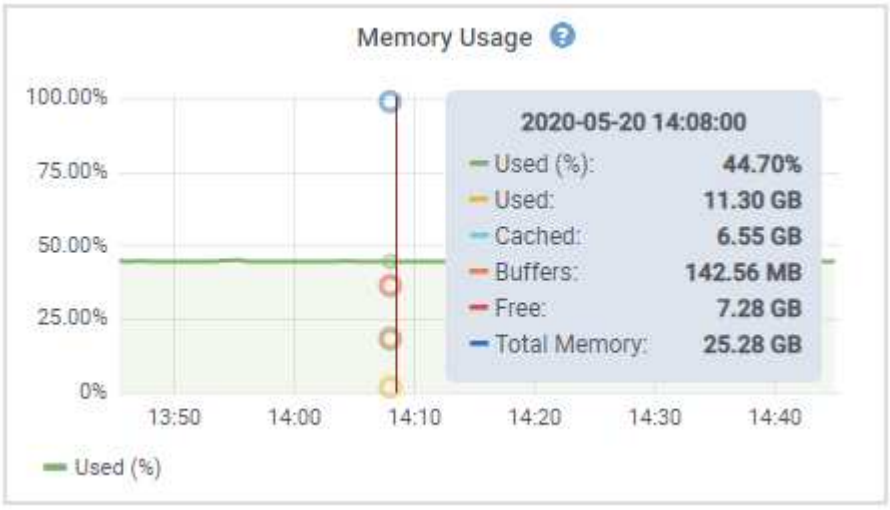
Grid Manager는 각 릴리스와 함께 업데이트되며 이 페이지의 예제 스크린샷과 일치하지 않을 수 있습니다.

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 각 그래프 위에 커서를 놓습니다.



노드가 어플라이언스 노드인 경우 이 탭에는 어플라이언스 하드웨어에 대한 자세한 정보가 있는 섹션도 포함되어 있습니다.

어플라이언스 스토리지 노드에 대한 정보를 봅니다

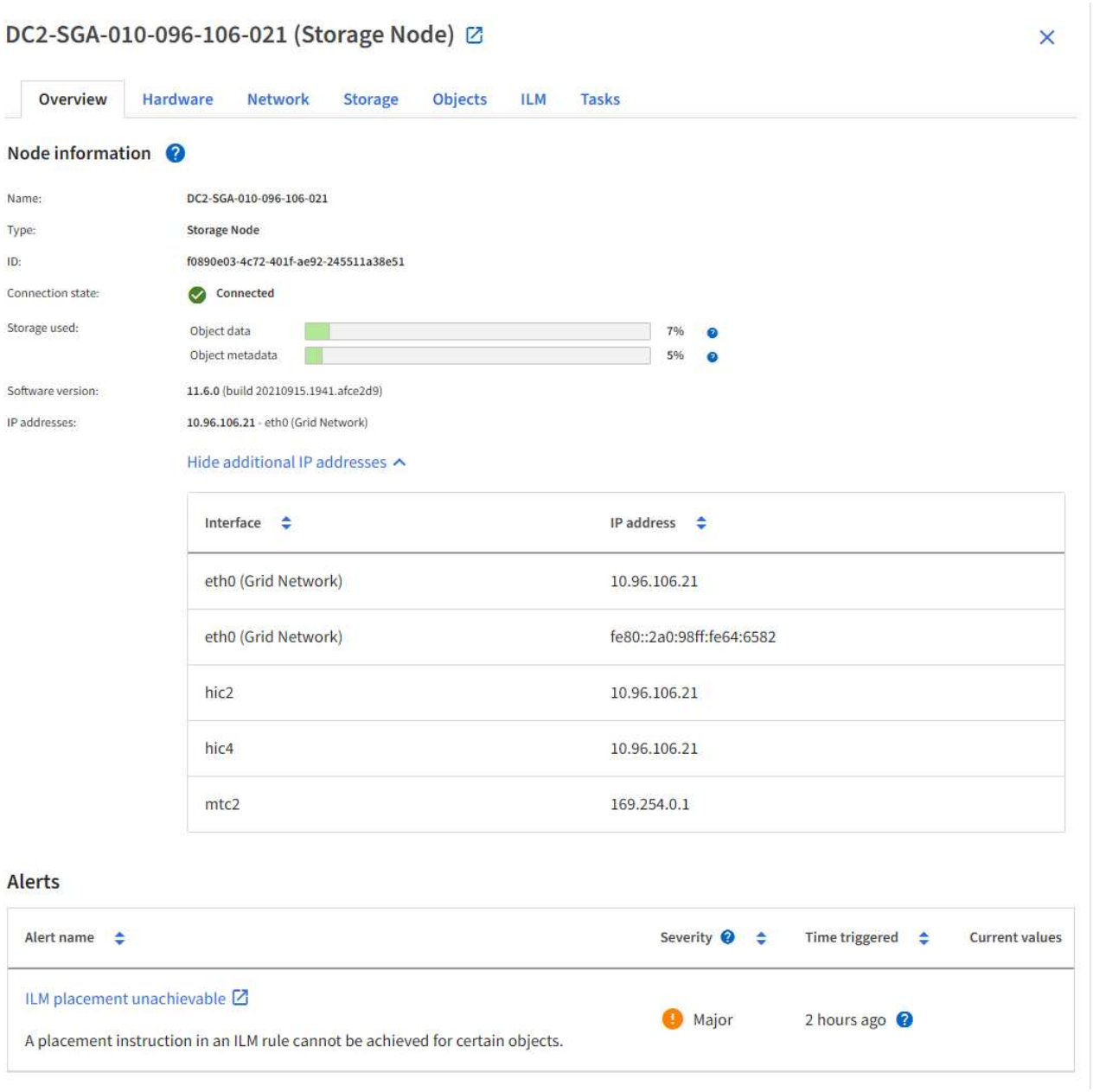
노드 페이지에는 서비스 상태에 대한 정보와 각 어플라이언스 스토리지 노드의 모든 컴퓨팅, 디스크 디바이스 및 네트워크 리소스에 대한 정보가 나열됩니다. 또한 메모리, 스토리지 하드웨어, 컨트롤러 펌웨어 버전, 네트워크 리소스, 네트워크 인터페이스, 네트워크 주소, 데이터 수신 및 전송

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.

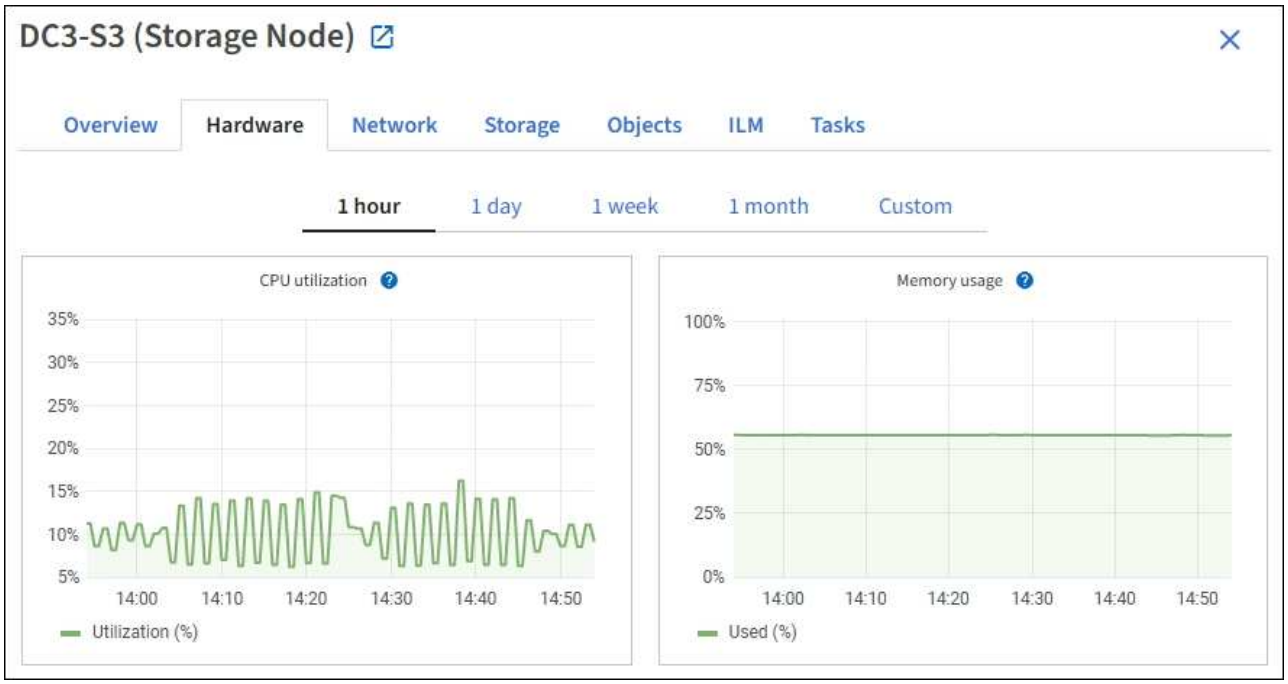
   - * eth *: 그리드 네트워크, 관리자 네트워크 또는 클라이언트 네트워크.
   - * hic *: 어플라이언스에 있는 물리적 10GbE, 25 또는 100GbE 포트 중 하나입니다. 이러한 포트는 함께 연결되어 StorageGRID 그리드 네트워크(eth0) 및 클라이언트 네트워크(eth2)에 연결할 수 있습니다.
   - * MTC *: 어플라이언스에 있는 물리적 1GbE 포트 중 하나입니다. 하나 이상의 MTC 인터페이스가 StorageGRID 관리 네트워크 인터페이스(eth1)를 형성하도록 연결됩니다. 다른 MTC 인터페이스를 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.

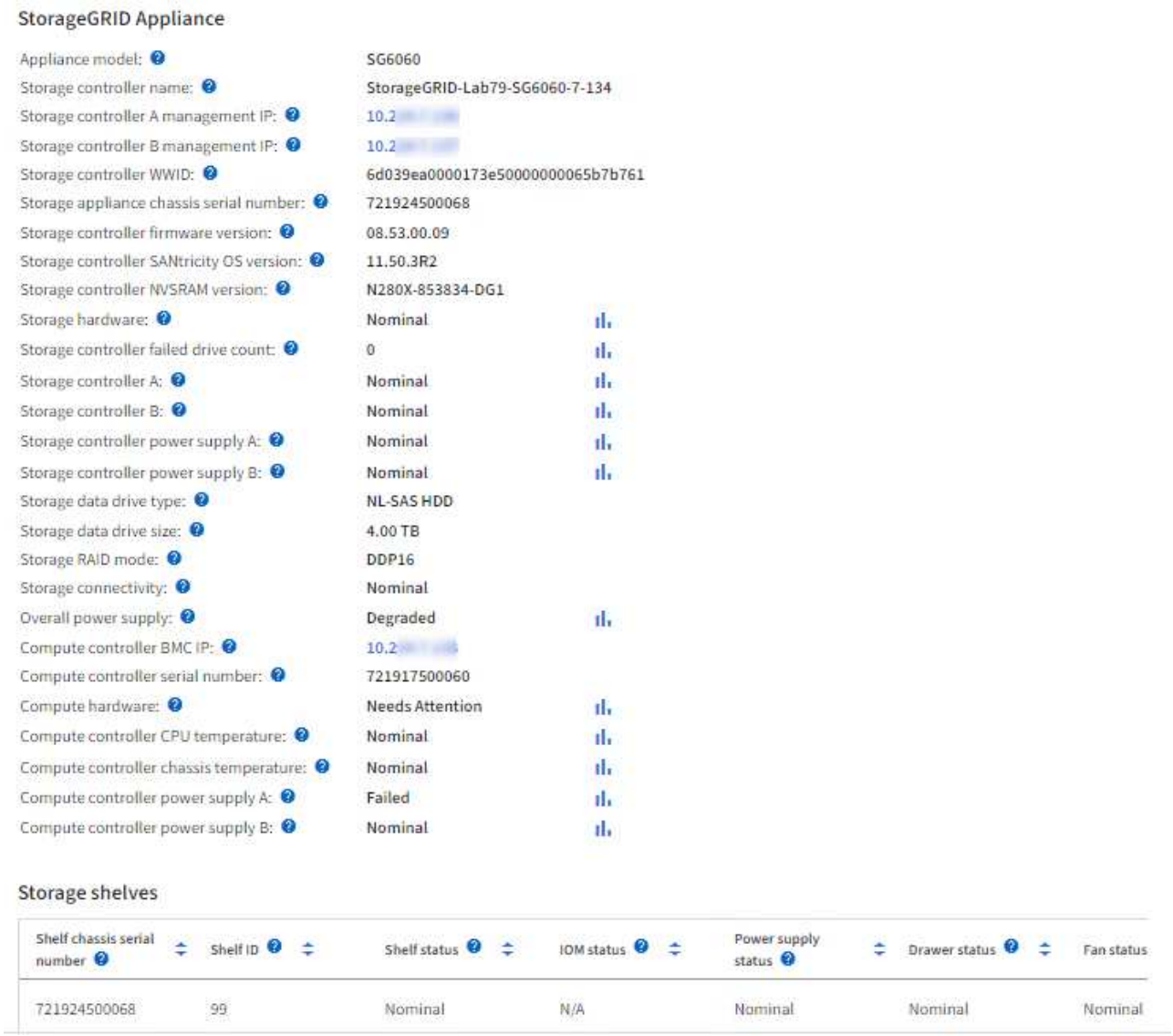
   a. CPU Utilization(CPU 사용률) 및 Memory(메모리) 그래프를 보고 시간에 따른 CPU 및 메모리 사용량 비율을 확인합니다. 다른 시간 간격을 표시하려면 차트 또는 그래프 위에 있는 컨트롤 중 하나를 선택합니다. 1시간, 1일, 1주 또는 1개월 간격으로 사용 가능한 정보를 표시할 수 있습니다. 날짜 및 시간 범위를 지정할 수 있는 사용자 지정 간격을 설정할 수도 있습니다.



   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 OS에 나와 있습니다.
스토리지 컨트롤러 이름입니다	SANtricity OS에 표시된 이 StorageGRID 어플라이언스의 이름입니다.
스토리지 컨트롤러 A 관리 IP	스토리지 컨트롤러 A의 관리 포트 1의 IP 주소. 이 IP를 사용하여 SANtricity OS에 액세스하여 스토리지 문제를 해결할 수 있습니다.
스토리지 컨트롤러 B 관리 IP	스토리지 컨트롤러 B의 관리 포트 1에 대한 IP 주소입니다. 스토리지 문제를 해결하기 위해 이 IP를 사용하여 SANtricity OS에 액세스합니다. 일부 어플라이언스 모델에는 스토리지 컨트롤러 B가 없습니다
스토리지 컨트롤러 WWID입니다	SANtricity OS에 표시되는 스토리지 컨트롤러의 전 세계적 식별자입니다.

Appliance 테이블의 필드	설명
스토리지 어플라이언스 섀시 일련 번호입니다	어플라이언스의 섀시 일련 번호입니다.
스토리지 컨트롤러 펌웨어 버전입니다	이 어플라이언스에 대한 스토리지 컨트롤러의 펌웨어 버전입니다.
스토리지 컨트롤러 SANtricity OS 버전입니다	스토리지 컨트롤러 A의 SANtricity OS 버전입니다
스토리지 컨트롤러 NVSRAM 버전입니다	SANtricity System Manager에서 보고한 스토리지 컨트롤러의 NVSRAM 버전입니다. SG6060 및 SG6160의 경우 두 컨트롤러 간에 NVSRAM 버전이 일치하지 않으면 컨트롤러 A 버전이 표시됩니다. 컨트롤러 A가 설치되지 않았거나 작동하지 않으면 컨트롤러 B 버전이 표시됩니다.
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 OS를 사용하여 스토리지 컨트롤러를 확인합니다. 그런 다음 컴퓨팅 컨트롤러에 적용되는 다른 경고가 없는지 확인합니다.
스토리지 컨트롤러의 드라이브 수가 실패했습니다	최적의 드라이브 수가 아닙니다.
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 드라이브) 또는 SSD(Solid State Drive)와 같은 어플라이언스의 드라이브 유형입니다.
스토리지 데이터 드라이브 크기입니다	하나의 데이터 드라이브의 유효 크기입니다. SG6160의 경우 캐시 드라이브의 크기도 표시됩니다. • 참고 *: 확장 셸프가 있는 노드의 경우 대신 를 각 쉘프의 데이터 드라이브 크기입니다사용하십시오. 유효 드라이브 크기는 쉘프마다 다를 수 있습니다.

Appliance 테이블의 필드	설명
스토리지 RAID 모드	어플라이언스에 대해 구성된 RAID 모드입니다.
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 셸프는 SG6060 및 SG6160에만 적용됩니다.
쉘프 상태입니다	스토리지 쉘프의 전체 상태입니다.
IOM 상태입니다	확장 셸프의 입출력 모듈(IOM)의 상태입니다. 해당 없음 - 확장 쉘프가 아닌 경우.
전원 공급 장치 상태입니다	스토리지 쉘프의 전원 공급 장치의 전체 상태입니다.

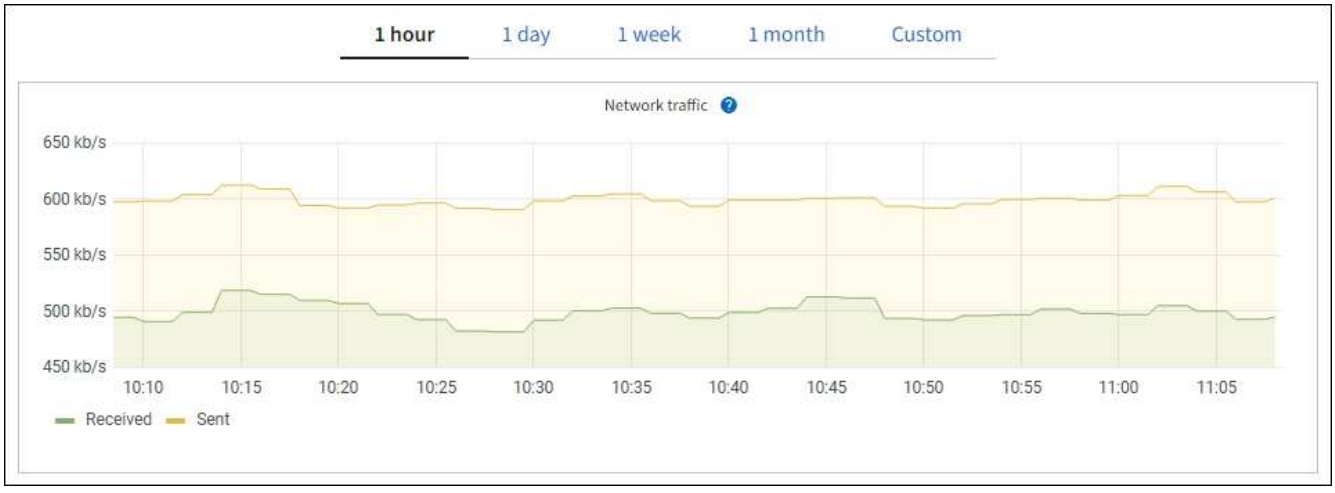
열을 클릭합니다	설명
문서함 상태입니다	스토리지 쉘프에 있는 드로어의 상태입니다. 해당 없음 - 선반에 서랍이 없는 경우
팬 상태입니다	스토리지 쉘프에 있는 냉각 팬의 전체 상태입니다.
드라이브 슬롯	스토리지 쉘프의 총 드라이브 슬롯 수입니다.
데이터 드라이브	스토리지 쉘프의 드라이브 수로, 데이터 스토리지에 사용됩니다.
데이터 드라이브 크기	스토리지 쉘프에 있는 데이터 드라이브 1개의 유효 크기입니다.
캐시 드라이브	캐시로 사용되는 스토리지 쉘프의 드라이브 수입니다.
캐시 드라이브 크기입니다	스토리지 쉘프에서 가장 작은 캐시 드라이브의 크기입니다. 일반적으로 캐시 드라이브는 모두 크기가 같습니다.
구성 상태입니다	스토리지 셸프의 구성 상태입니다.

a. 모든 상태가 "공칭"인지 확인합니다.

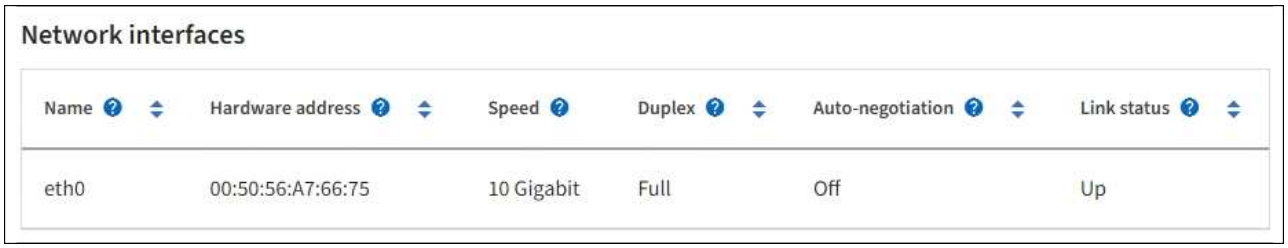
상태가 "공칭"이 아닌 경우 현재 경고를 검토합니다. SANtricity 시스템 관리자를 사용하여 이러한 하드웨어 값 중 일부에 대해 자세히 알아볼 수도 있습니다. 제품 설치 및 유지 관리 지침을 참조하십시오.

4. 각 네트워크에 대한 정보를 보려면 * Network * 를 선택하십시오.

네트워크 트래픽 그래프는 전체 네트워크 트래픽에 대한 요약을 제공합니다.



a. 네트워크 인터페이스 섹션을 검토합니다.



네트워크 인터페이스 테이블의 * Speed * 열에 있는 값을 사용하여 어플라이언스의 10/25-GbE 네트워크 포트가 액티브/백업 모드 또는 LACP 모드를 사용하도록 구성되었는지 확인하십시오.

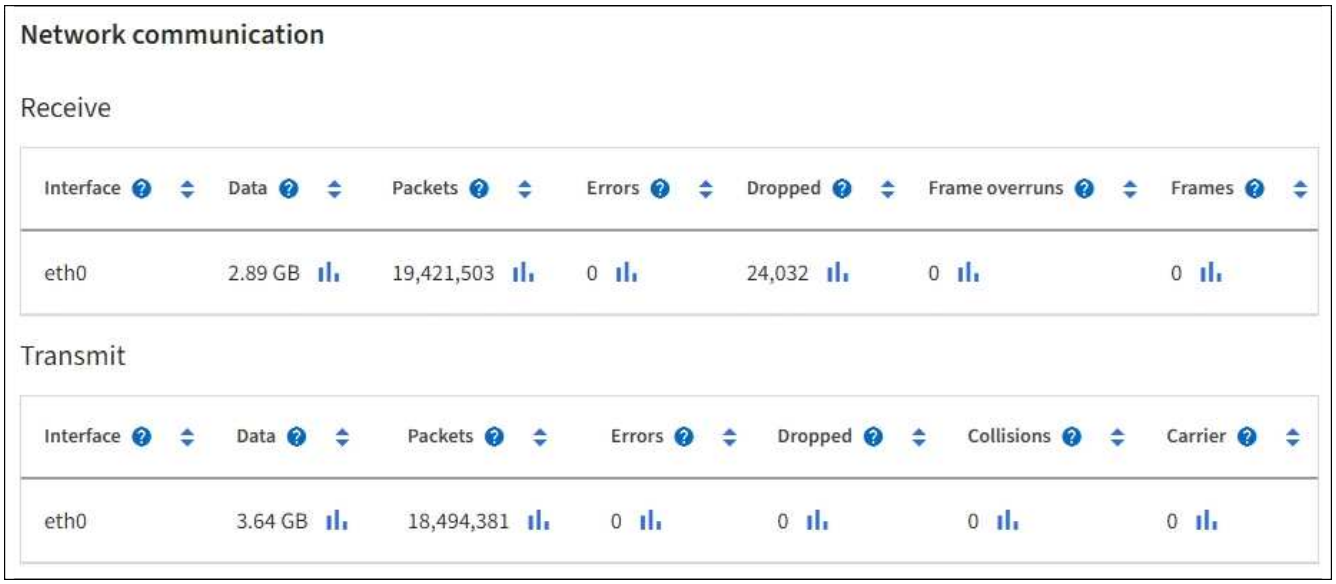
표에 표시된 값은 4개의 링크가 모두 사용된다고 가정합니다.

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

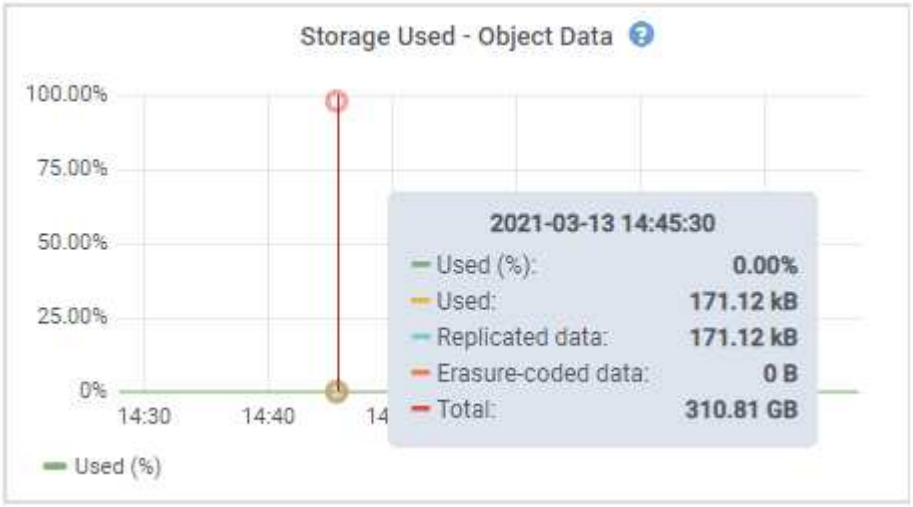
10/25-GbE 포트 구성에 대한 자세한 내용은 을 "네트워크 링크를 구성합니다" 참조하십시오.

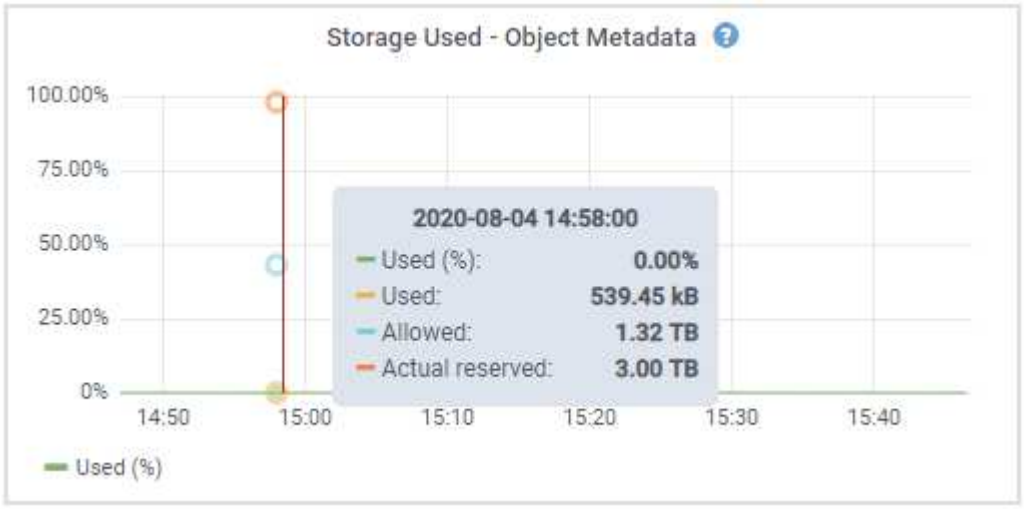
b. 네트워크 통신 섹션을 검토합니다.

Receive 및 Transmit 테이블은 각 네트워크를 통해 수신 및 전송된 바이트 및 패킷의 수와 기타 수신 및 전송 메트릭을 보여줍니다.



5. 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.

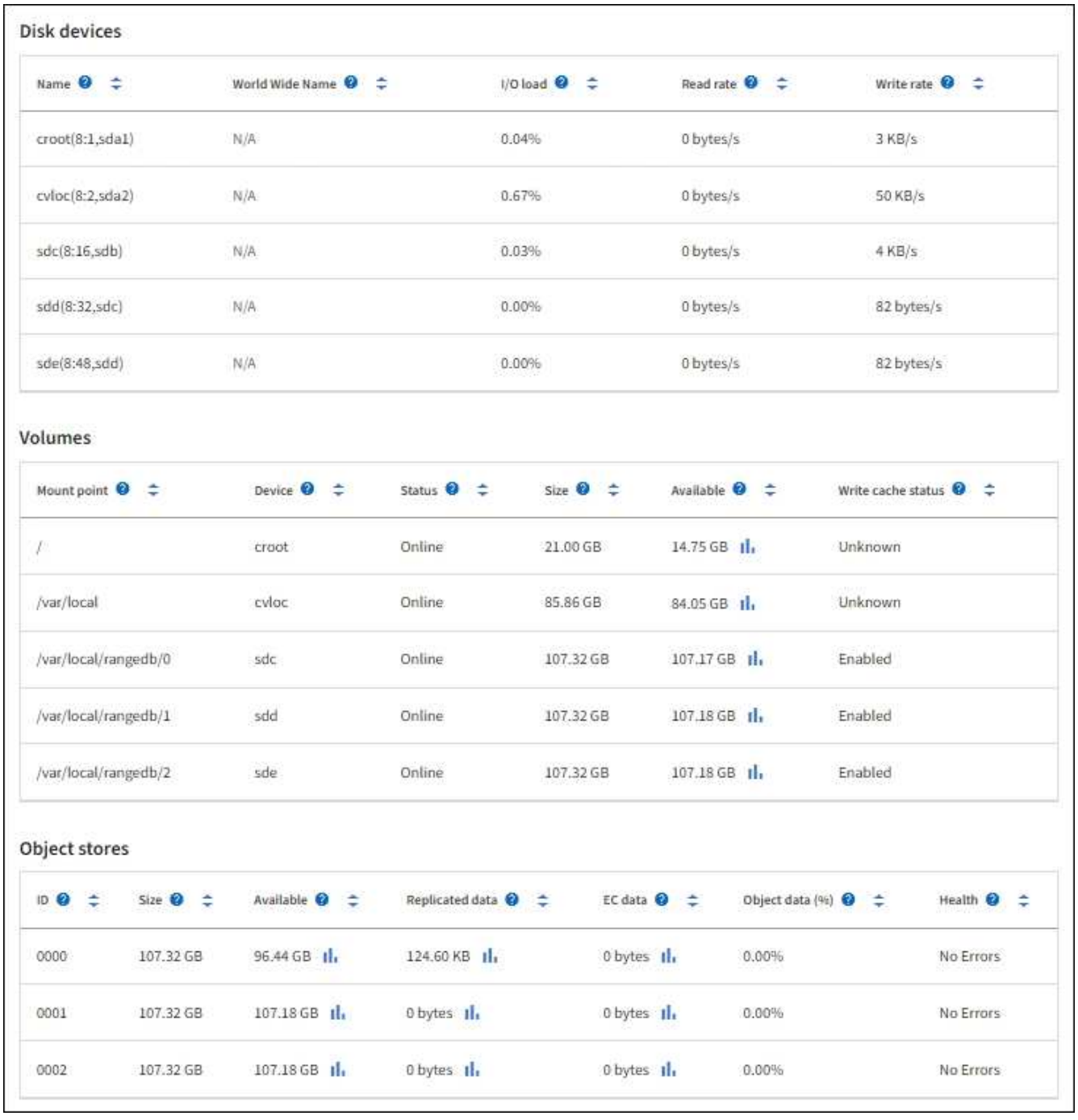




a. 아래로 스크롤하여 각 볼륨 및 오브젝트 저장소에서 사용 가능한 스토리지 양을 확인합니다.

각 디스크의 전 세계 이름은 SANtricity OS(어플라이언스의 스토리지 컨트롤러에 연결된 관리 소프트웨어)에서 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

어플라이언스 관리 노드 및 게이트웨이 노드에 대한 정보를 봅니다

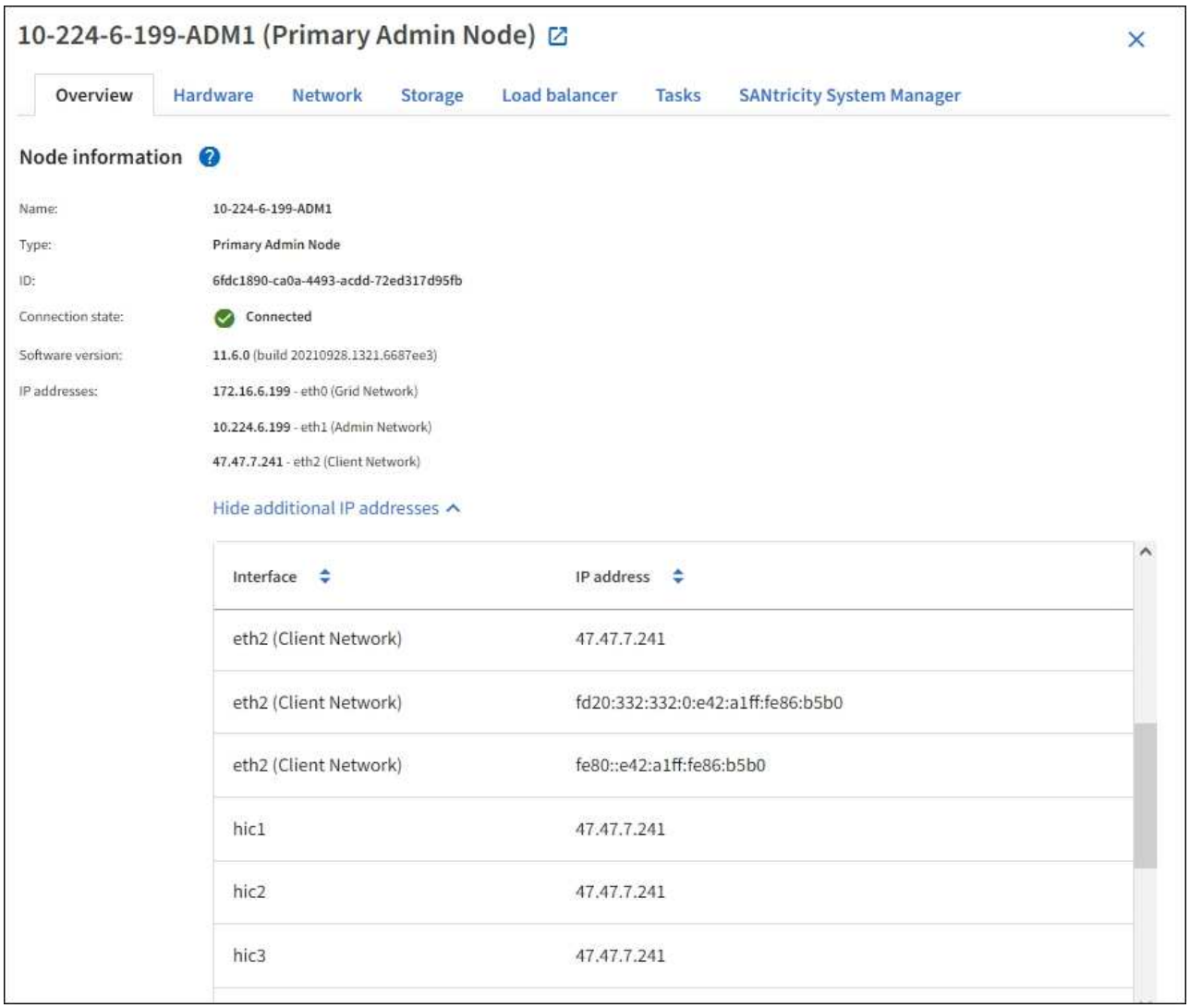
노드 페이지에는 서비스 상태에 대한 정보와 관리 노드 또는 게이트웨이 노드로 사용되는 각 서비스 어플라이언스에 대한 모든 컴퓨팅, 디스크 디바이스 및 네트워크 리소스에 대한 정보가 나열됩니다. 또한 메모리, 스토리지 하드웨어, 네트워크 리소스, 네트워크 인터페이스, 네트워크 주소, 데이터를 수신하고 전송합니다.

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.

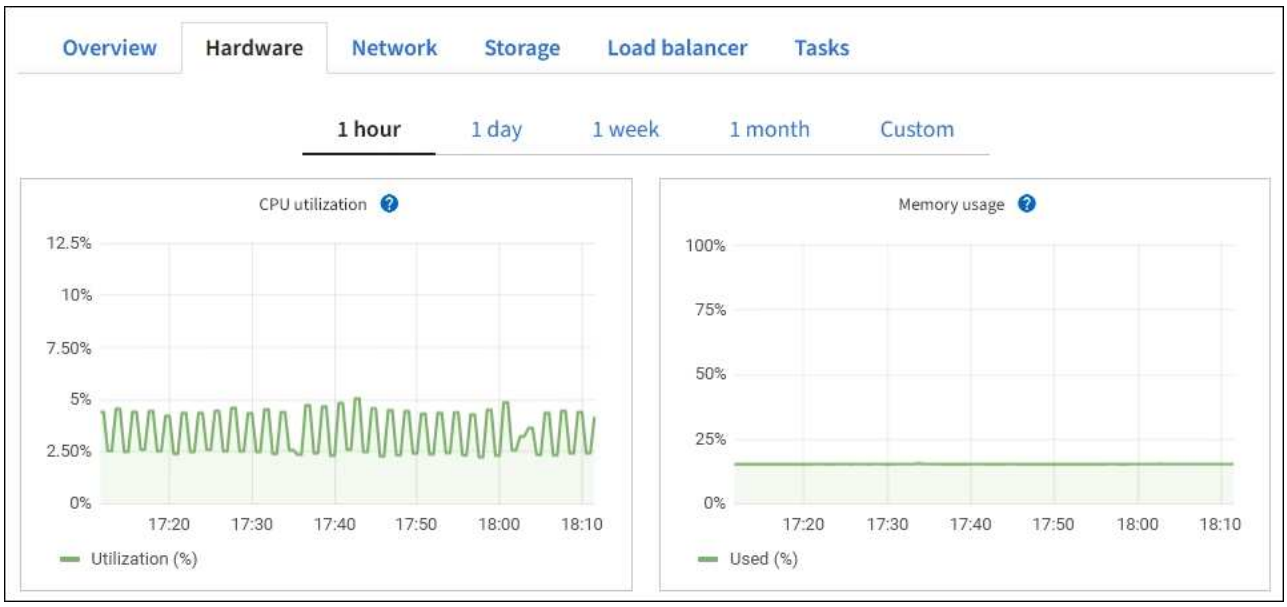


   개요 탭의 경고 섹션에는 노드에 대한 활성 경고가 표시됩니다.

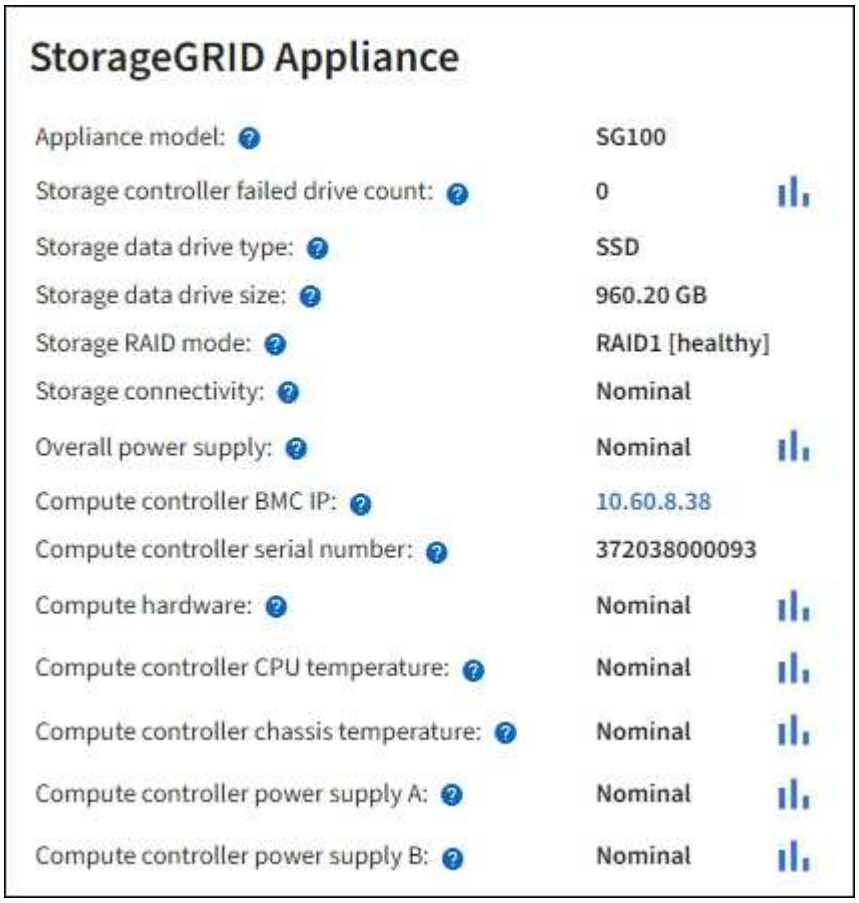
3. 어플라이언스에 대한 자세한 내용을 보려면 * 하드웨어 * 를 선택하십시오.

   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.



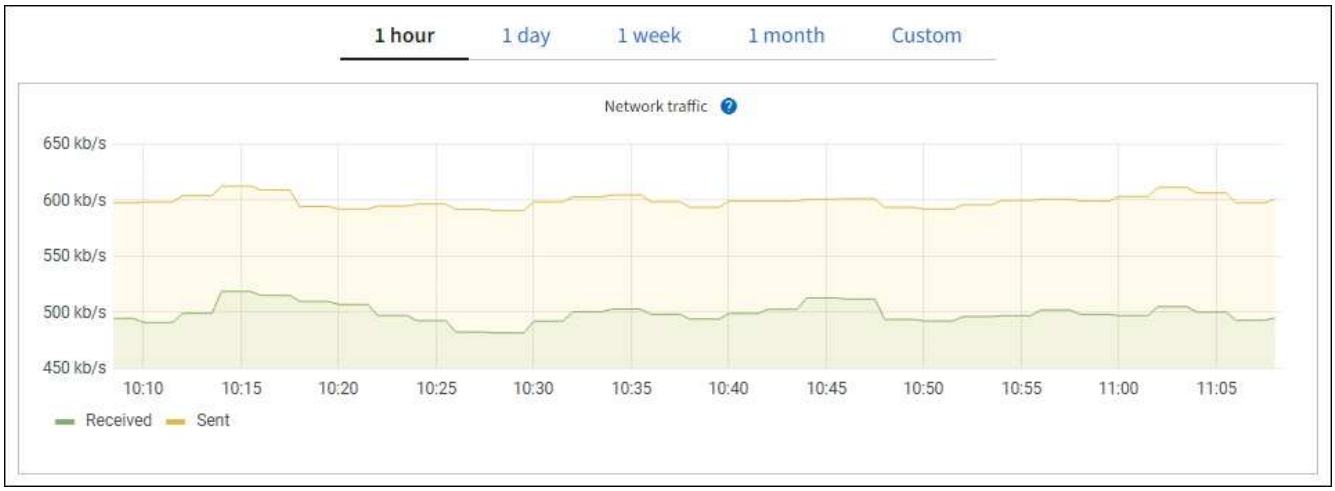
Appliance 테이블의 필드	설명
어플라이언스 모델	이 StorageGRID 어플라이언스의 모델 번호입니다.
스토리지 컨트롤러의 드라이브 수가 실패했습니다	최적의 드라이브 수가 아닙니다.
스토리지 데이터 드라이브 유형입니다	HDD(하드 드라이브) 또는 SSD(Solid State Drive)와 같은 어플라이언스의 드라이브 유형입니다.
스토리지 데이터 드라이브 크기입니다	하나의 데이터 드라이브의 유효 크기입니다.
스토리지 RAID 모드	어플라이언스의 RAID 모드입니다.
전체 전원 공급 장치	어플라이언스에 있는 모든 전원 공급 장치의 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 상태가 "공칭"인지 확인합니다.

   상태가 "공칭"이 아닌 경우 현재 경고를 검토합니다.

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

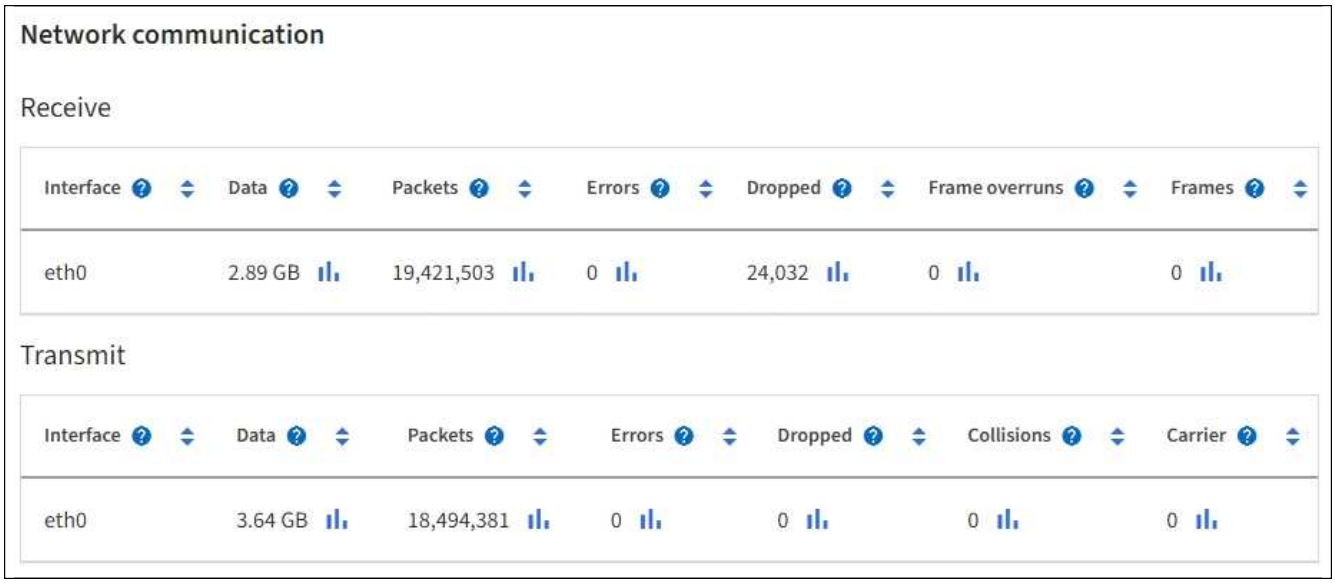
네트워크 인터페이스 테이블의 * Speed * 열에 있는 값을 사용하여 어플라이언스의 40개/100GbE 네트워크 포트 4개가 액티브/백업 모드 또는 LACP 모드를 사용하도록 구성되었는지 확인하십시오.

표에 표시된 값은 4개의 링크가 모두 사용된다고 가정합니다.

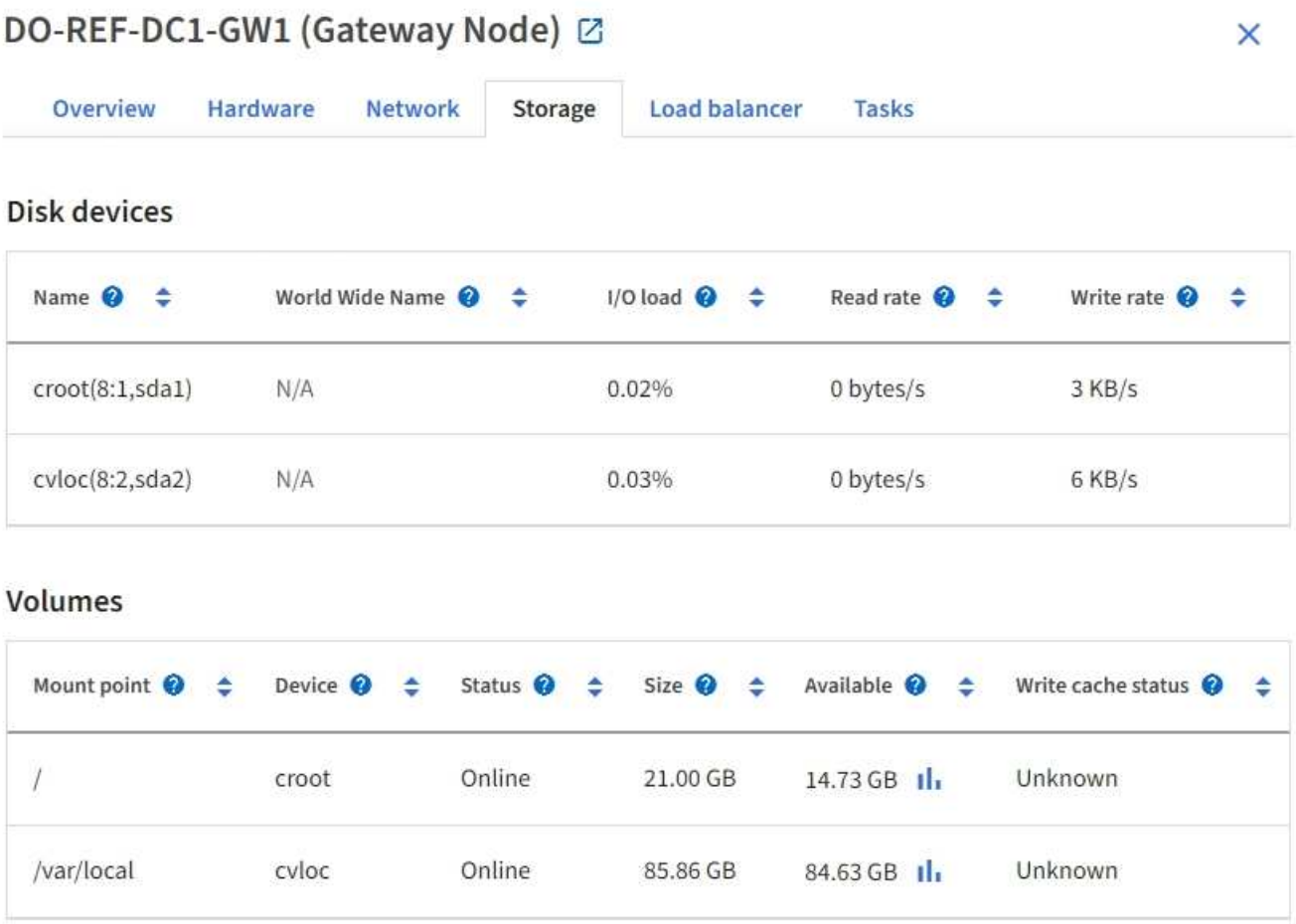
링크 모드	본드 모드	개별 **HIC** 링크 속도**(hic1, hic2, hic3, hic4)**	예상 그리드/클라이언트 네트워크 속도**(eth0, eth2)**
집계	LACP	100	400
고정	LACP	100	200
고정	Active/Backup(활성/백업)	100	100
집계	LACP	40	160
고정	LACP	40	80
고정	Active/Backup(활성/백업)	40	40

b. 네트워크 통신 섹션을 검토합니다.

Receive 및 Transmit 테이블은 각 네트워크에서 수신 및 전송된 바이트 및 패킷의 수와 기타 수신 및 전송 메트릭을 보여줍니다.



5. 서비스 어플라이언스의 디스크 장치 및 볼륨에 대한 정보를 보려면 * Storage * 를 선택합니다.



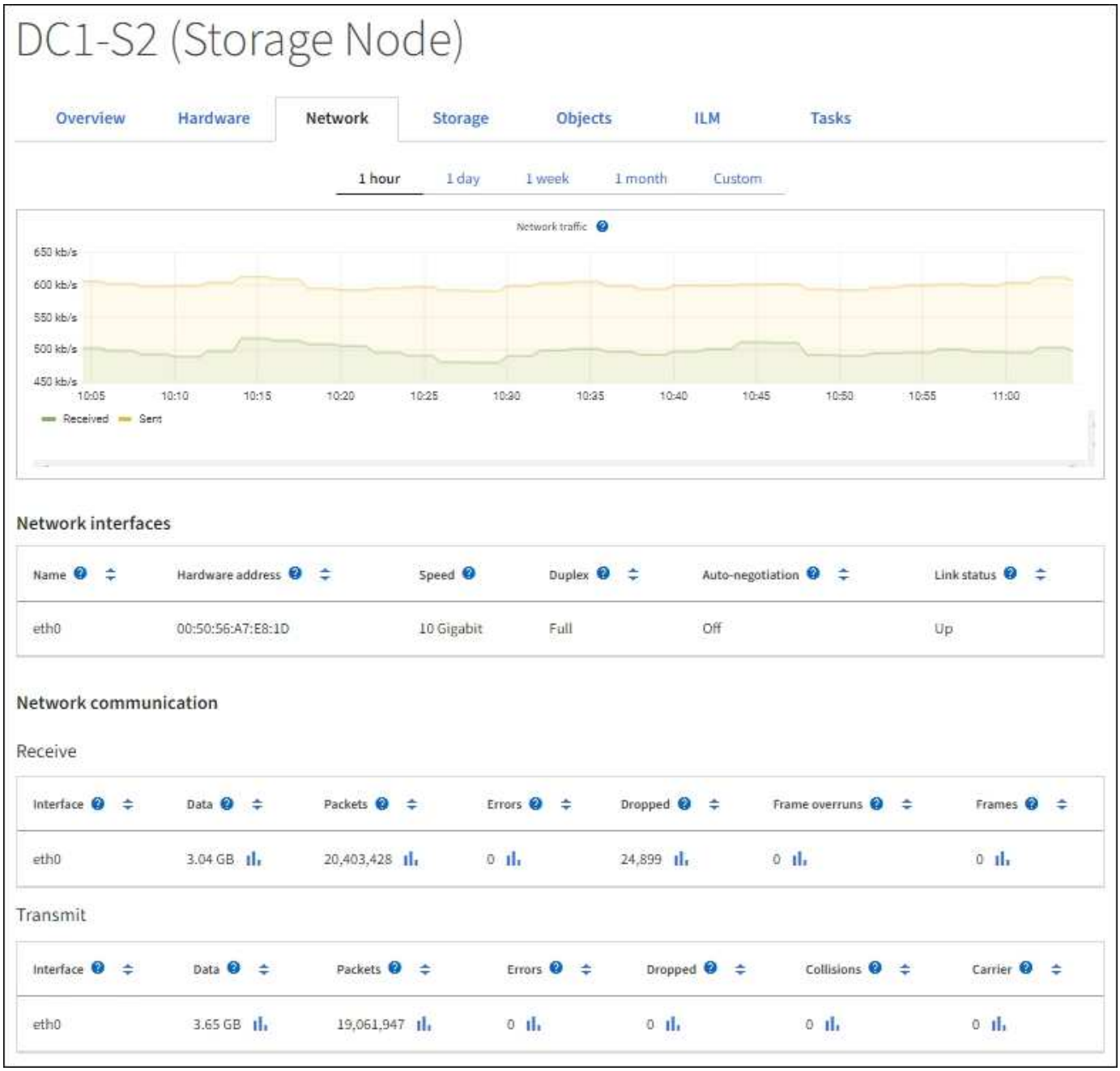
네트워크 탭을 봅니다

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

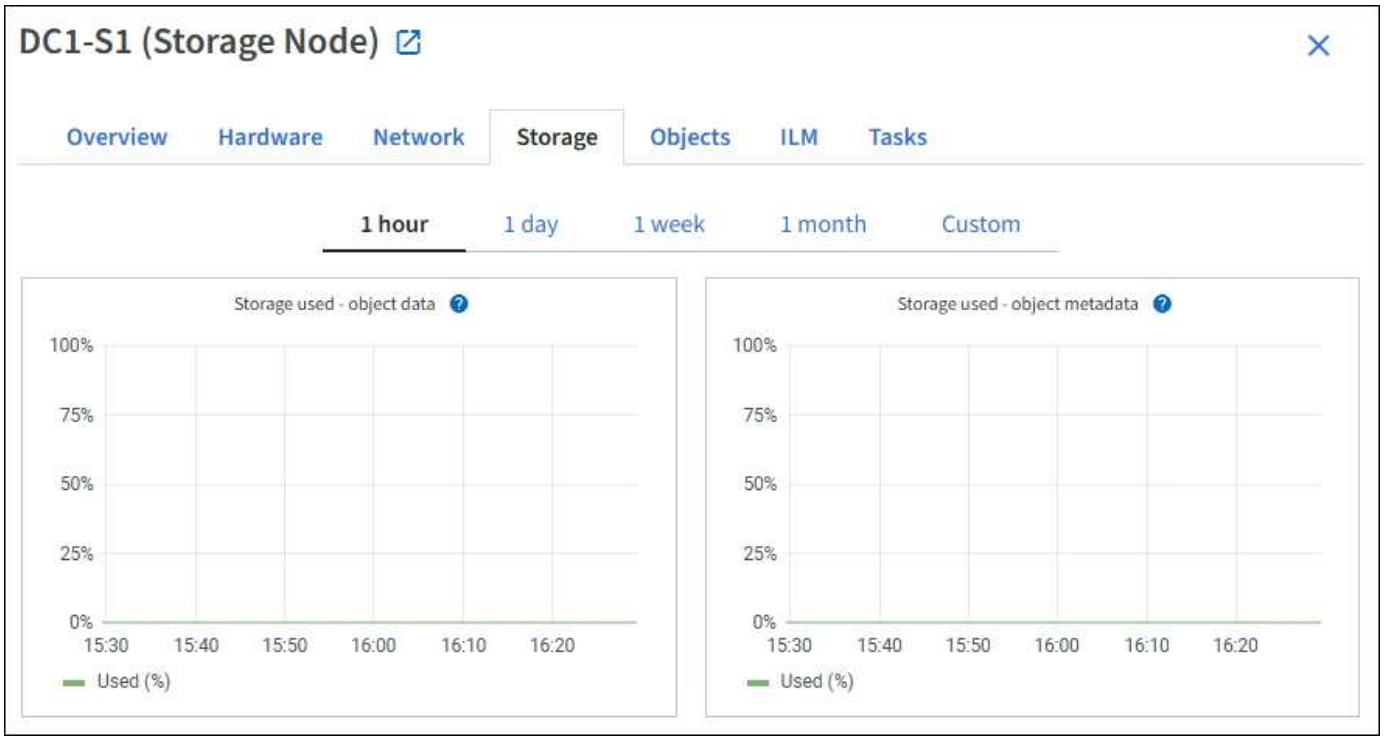
스토리지 탭에는 스토리지 가용성 및 기타 스토리지 메트릭이 요약되어 있습니다.

스토리지 탭은 모든 노드, 각 사이트 및 전체 그리드에 대해 표시됩니다.

스토리지 사용 그래프

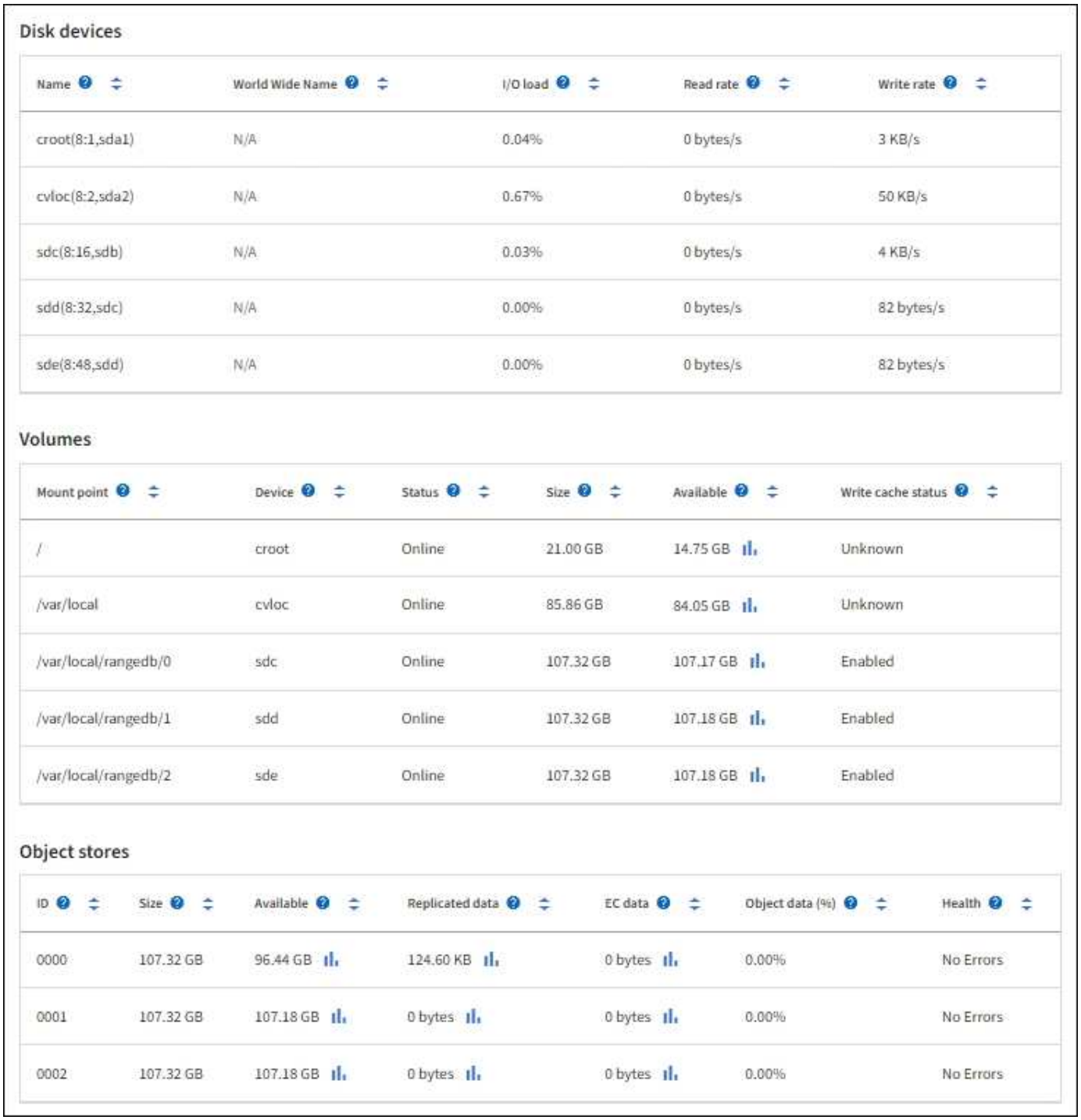
스토리지 노드, 각 사이트 및 전체 그리드의 경우 스토리지 탭에는 시간 경과에 따라 오브젝트 데이터 및 오브젝트 메타데이터에 사용된 스토리지 양이 표시된 그래프가 포함됩니다.

업그레이드 중 또는 연결 끊김 상태와 같이 노드가 그리드에 연결되어 있지 않으면 특정 메트릭을 사용할 수 없거나 사이트 및 그리드 합계에서 제외할 수 있습니다. 노드가 그리드에 다시 연결되면 값이 안정화될 때까지 몇 분 동안 기다립니다.



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

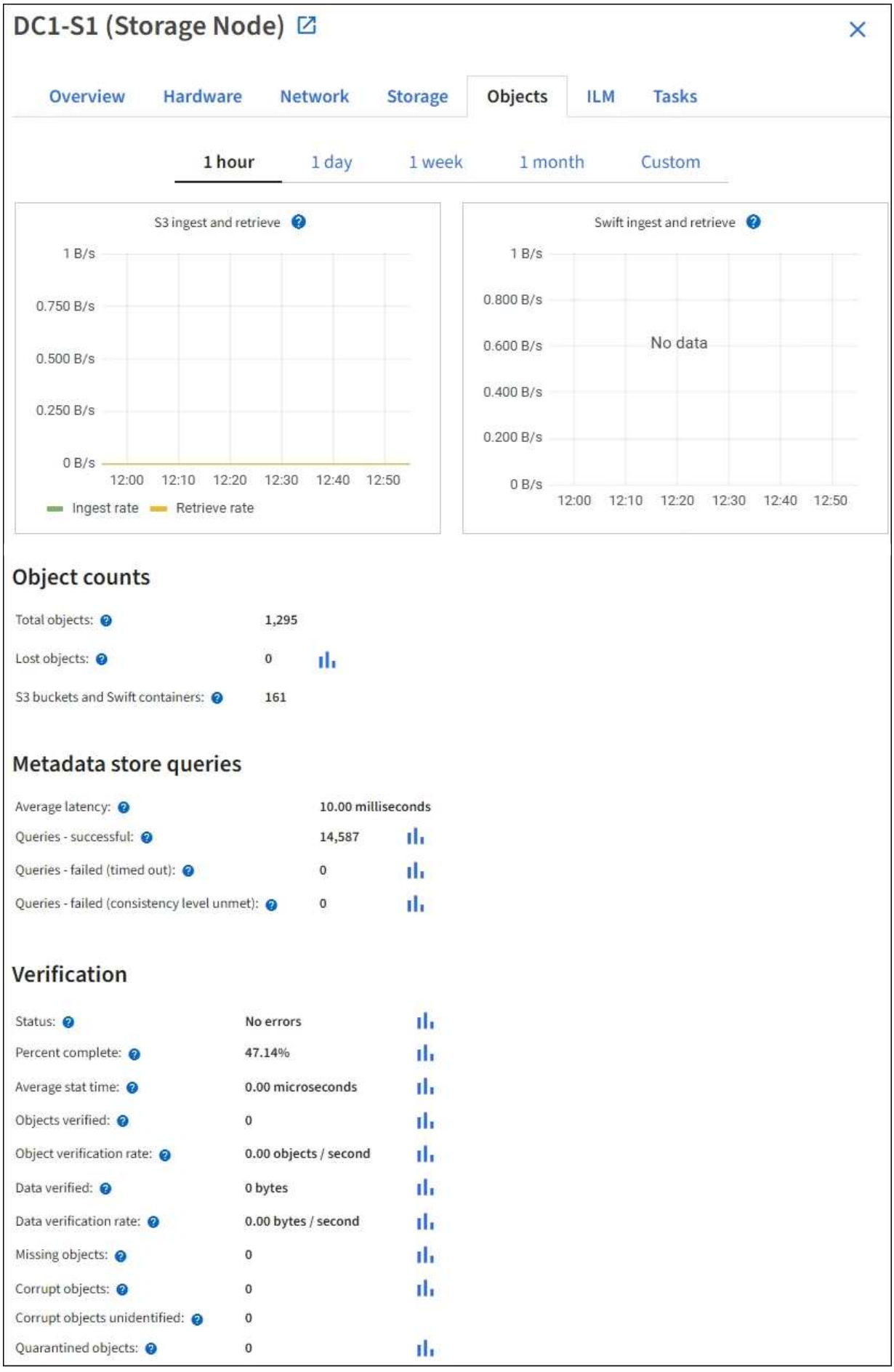
관련 정보

"스토리지 용량을 모니터링합니다"

개체 탭을 봅니다

에 대한 자세한 내용은 개체 탭에 "S3 수집 및 검색 속도"나와 있습니다.

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.

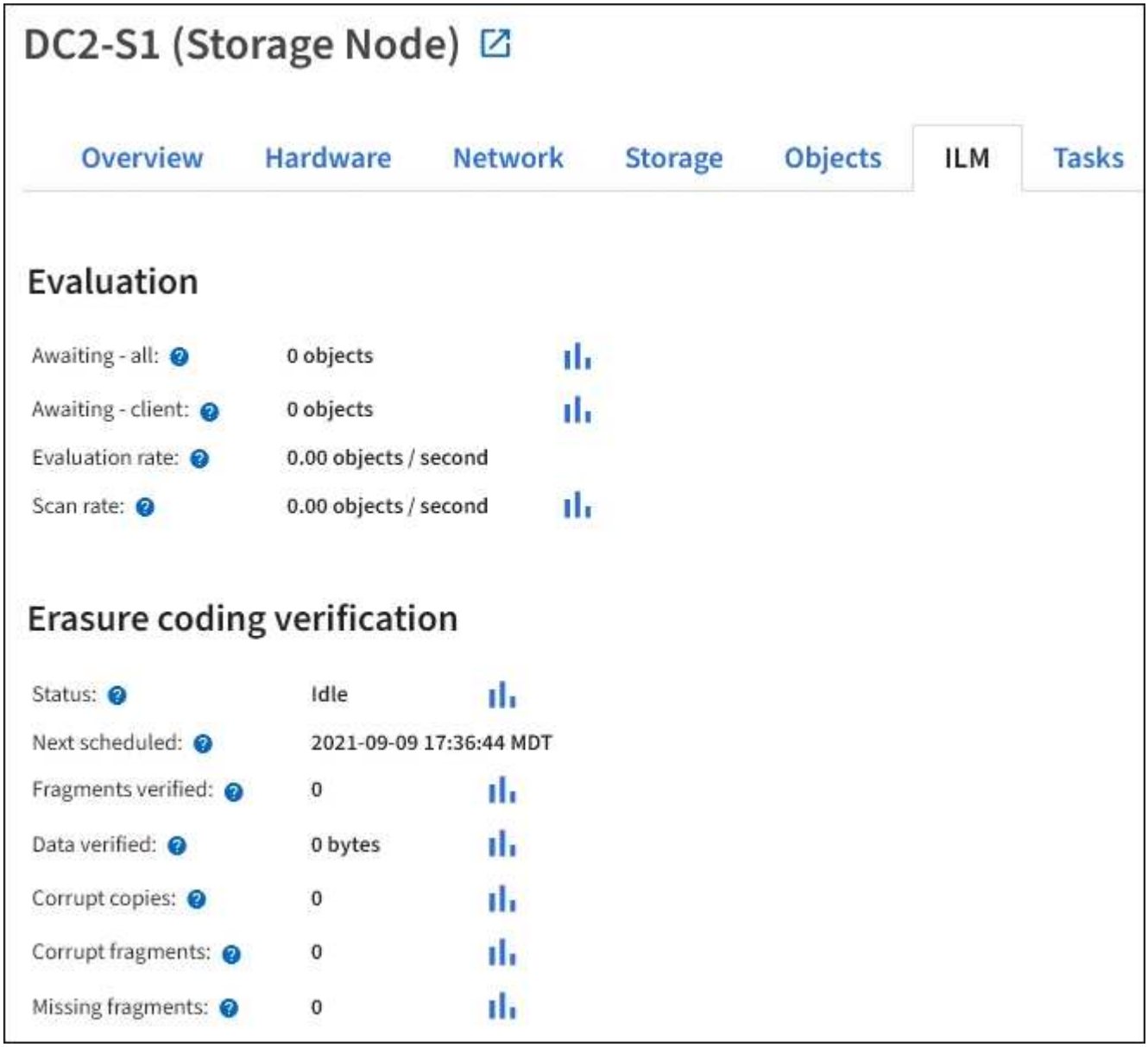

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 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 라이프사이클 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 탭에는 삭제 코딩 개체에 대한 ILM 평가 및 백그라운드 검증에 대한 세부 정보가 제공됩니다.



관련 정보

- "정보 수명 주기 관리를 모니터링합니다"
- "StorageGRID 관리"

작업 탭을 사용합니다

모든 노드에 대해 작업 탭이 표시됩니다. 이 탭을 사용하여 노드의 이름을 바꾸거나 재부팅하거나

어플라이언스 노드를 유지보수 모드로 전환할 수 있습니다.

이 탭의 각 옵션에 대한 전체 요구 사항 및 지침은 다음을 참조하십시오.

- "그리드, 사이트 및 노드의 이름을 바꿉니다"
- "그리드 노드를 재부팅합니다"
- "제품을 유지보수 모드로 전환합니다"

부하 분산 장치 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.

부하 분산 서비스를 통해 실행 중인 입출력이 없거나 로드 밸런서가 구성되어 있지 않으면 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.

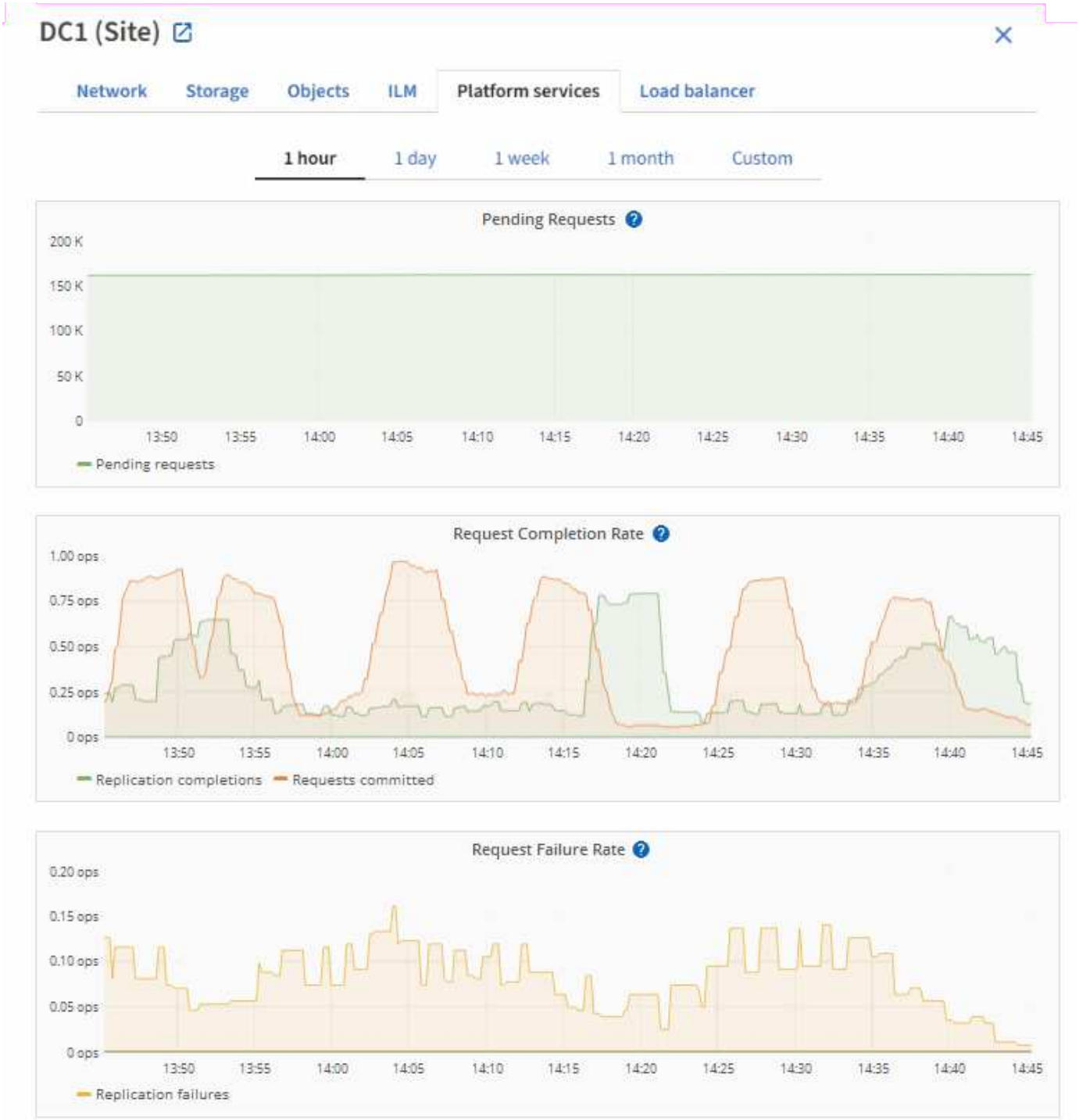
관련 정보

- "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 비롯한 S3 플랫폼 서비스에 대한 자세한 내용은 를 참조하십시오"StorageGRID 관리 지침".

드라이브 관리 탭을 봅니다

Manage drives(드라이브 관리) 탭에서는 이 기능을 지원하는 어플라이언스의 드라이브에 대한 세부 정보에 액세스하고 문제 해결 및 유지 관리 작업을 수행할 수 있습니다.

드라이브 관리 탭을 사용하여 다음을 수행할 수 있습니다.

- 어플라이언스에 있는 데이터 스토리지 드라이브의 레이아웃을 봅니다

- 각 드라이브 위치, 유형, 상태, 펌웨어 버전 및 일련 번호가 나열된 표를 봅니다
- 각 드라이브에서 문제 해결 및 유지 관리 기능을 수행합니다

드라이브 관리 탭에 액세스하려면 가 있어야 "스토리지 어플라이언스 관리자 또는 루트 액세스 권한"합니다.

드라이브 관리 탭 사용에 대한 자세한 내용은 을 "드라이브 관리 탭을 사용합니다"참조하십시오.

SANtricity System Manager 탭 보기(E-Series만 해당)

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.

> 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 유지 관리 지침을 따르십시오. SANtricity 펌웨어를 업그레이드하려면 사용 중인 스토리지 어플라이언스에 대한 를 "유지보수 구성 절차" 참조하십시오.

> SANtricity System Manager 탭은 E-Series 하드웨어를 사용하는 스토리지 어플라이언스 노드에 대해서만 표시됩니다.

SANtricity 시스템 관리자를 사용하여 다음을 수행할 수 있습니다.

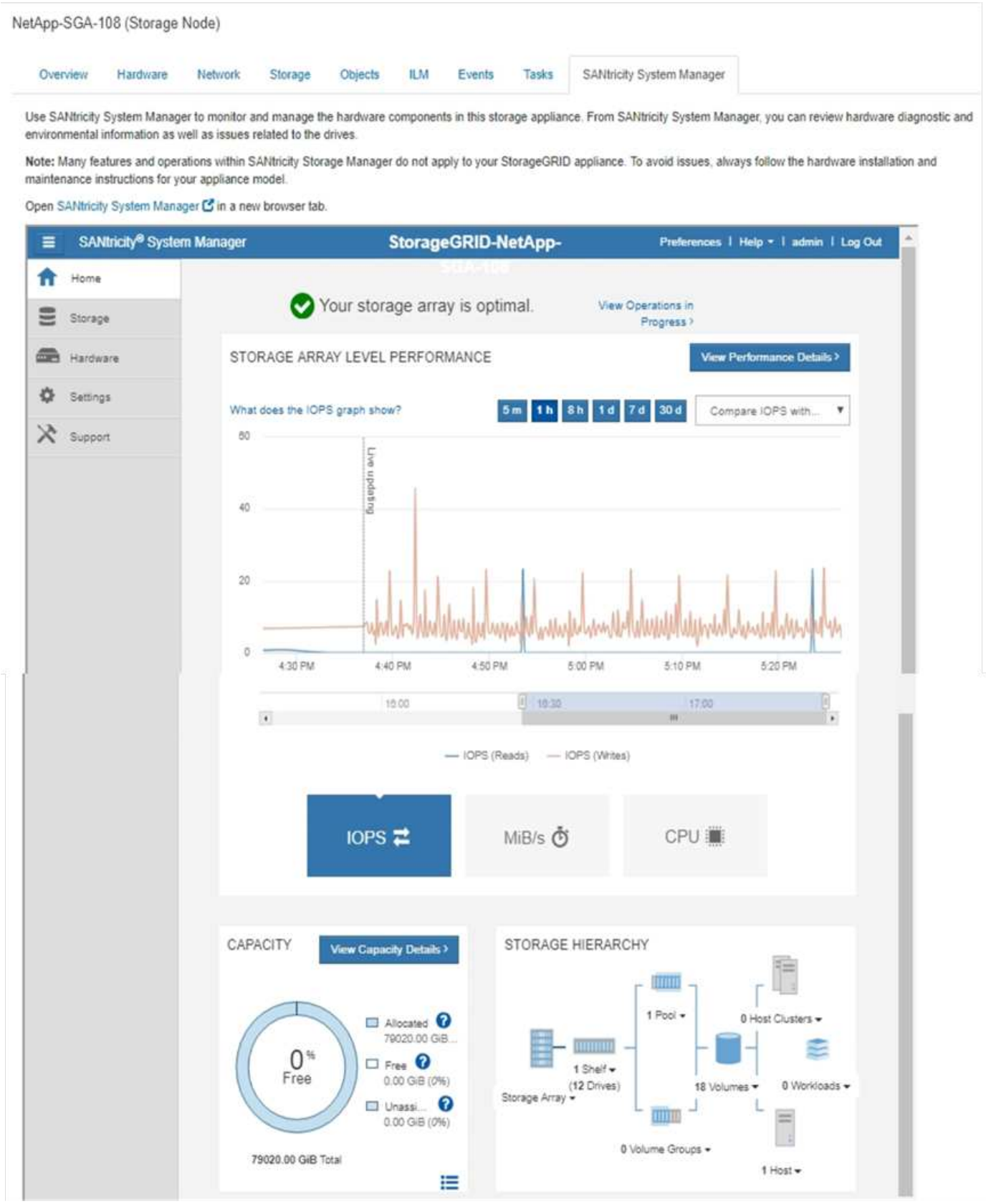
- 스토리지 어레이 레벨 성능, I/O 지연 시간, 스토리지 컨트롤러 CPU 활용률, 처리량과 같은 성능 데이터를 봅니다.
- 하드웨어 구성 요소 상태를 확인합니다.
- 진단 데이터 보기 및 E-Series AutoSupport 구성과 같은 지원 기능을 수행합니다.

> SANtricity System Manager를 사용하여 E-Series AutoSupport에 대한 프록시를 구성하려면 를 참조하십시오."StorageGRID를 통해 E-Series AutoSupport 패키지를 전송합니다"

그리드 관리자를 통해 SANtricity 시스템 관리자에 액세스하려면 이 있어야 "스토리지 어플라이언스 관리자 또는 루트 액세스 권한"합니다.

> 그리드 관리자를 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 펌웨어 8.70 이상이 있어야 합니다.

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 어레이 레벨 성능 및 용량 사용량에 대한 세부 정보를 보려면 각 그래프 위에 커서를 놓습니다.

SANtricity System Manager 탭에서 액세스할 수 있는 정보를 보는 방법에 대한 자세한 내용은 를 참조하십시오. "NetApp E-Series 및 SANtricity 문서"

정기적으로 모니터링할 정보

모니터링 대상 및 시기

오류가 발생하거나 그리드의 일부를 사용할 수 없는 경우에도 StorageGRID 시스템이 계속 작동할 수 있지만, 잠재적인 문제가 그리드의 효율성 또는 가용성에 영향을 미치기 전에 이를 모니터링하고 해결해야 합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

작업 모니터링 정보

사용량이 많은 시스템에서는 많은 양의 정보가 생성됩니다. 다음 목록은 지속적으로 모니터링할 가장 중요한 정보에 대한 지침을 제공합니다.

모니터링할 대상	주파수
"시스템 상태"	매일
소비되는 속도입니다"스토리지 노드 오브젝트 및 메타데이터 용량"	매주
"정보 수명 주기 관리 작업"	매주
"네트워킹 및 시스템 리소스"	매주
"테넌트 작업"	매주
"S3 클라이언트 작업"	매주
"로드 밸런싱 작업"	초기 설정 후 및 구성 변경 후
"그리드 페더레이션 연결"	매주

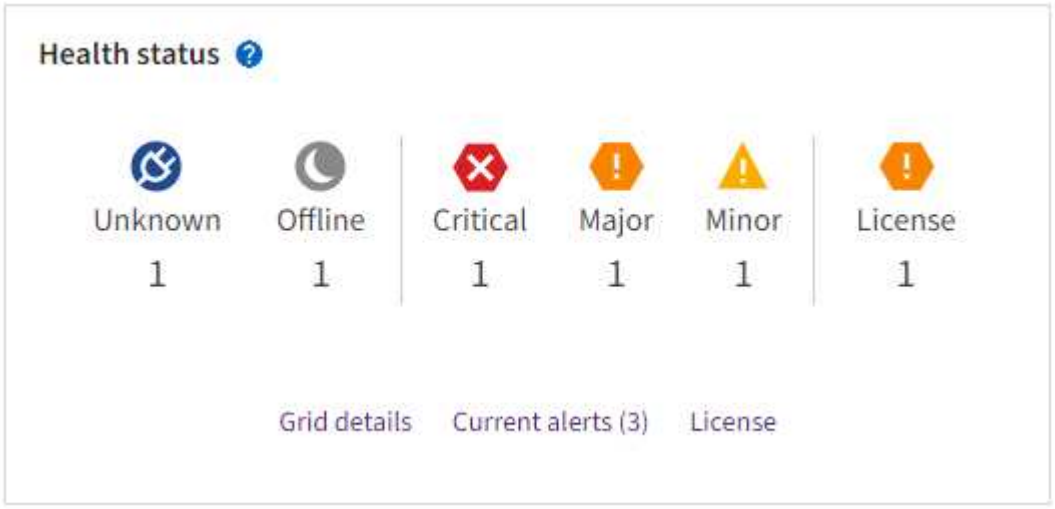
시스템 상태를 모니터링합니다

매일 StorageGRID 시스템의 전반적인 상태를 모니터링합니다.

이 작업에 대해

그리드의 일부를 사용할 수 없는 경우에도 StorageGRID 시스템은 계속 작동할 수 있습니다. 경고로 표시되는 잠재적인 문제가 반드시 시스템 작동에 문제가 되는 것은 아닙니다. Grid Manager 대시보드의 상태 카드에 요약된 문제를 조사합니다.

알림이 트리거되는 즉시 알림을 받으려면 또는 을"SNMP 트랩을 구성합니다"(를) 수행할 수 있습니다 "알림에 대한 이메일 알림을 설정합니다".



문제가 발생하면 추가 세부 정보를 볼 수 있는 링크가 나타납니다.

링크	다음과 같은 경우에 나타납니다.
그리드 세부 정보	모든 노드의 연결이 끊어졌습니다(접속 상태를 알 수 없음 또는 관리상 중단).
현재 경고(위험, 주, 보조)	경고는 입니다현재 활성 상태입니다.
최근에 해결된 경고	지난 주에 트리거된 알림입니다.이제 해결됩니다
라이센스	이 StorageGRID 시스템의 소프트웨어 라이센스에 문제가 있습니다. 할 수 "필요에 따라 라이센스 정보를 업데이트합니다"있습니다.

노드 연결 상태를 모니터링합니다

하나 이상의 노드가 그리드에서 분리되면 중요한 StorageGRID 작업이 영향을 받을 수 있습니다. 노드 연결 상태를 모니터링하고 문제를 즉시 해결합니다.

아이콘을 클릭합니다	설명	작업이 필요합니다
	• 연결되지 않음 - 알 수 없음 * 알 수 없는 이유로 노드의 연결이 끊기거나 노드의 서비스가 예기치 않게 다운되었습니다. 예를 들어, 노드의 서비스가 중지되거나 전원 장애 또는 예기치 않은 정전으로 인해 노드의 네트워크 연결이 끊겼을 수 있습니다. 노드 * 와 통신할 수 없음 알림도 트리거될 수 있습니다. 다른 알림도 활성화될 수 있습니다.	즉각적인 주의가 필요합니다. 각 경고를 선택합니다 를 클릭하고 권장 조치를 따릅니다. 예를 들어, 노드의 호스트를 중지하거나 다시 시작한 서비스를 다시 시작해야 할 수 있습니다. • 참고 *: 관리되는 종료 작업 중에 노드가 알 수 없음으로 나타날 수 있습니다. 이러한 경우 알 수 없음 상태를 무시할 수 있습니다.

아이콘을 클릭합니다	설명	작업이 필요합니다
	• 연결되지 않음 - 관리 중단 * 예상된 이유로 노드가 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. 이러한 노드는 기본적인 문제를 기반으로 하여 별도의 개입 없이 온라인 상태로 되곤 합니다.	이 노드에 영향을 주는 알림이 있는지 확인합니다. 하나 이상의 알림이 활성화된 경우 각 경고를 선택합니다권장 조치를 따릅니다.
	• 연결됨 * 노드가 그리드에 연결되어 있습니다.	별도의 조치가 필요 없습니다.

현재 및 해결된 경고를 봅니다

- 현재 경고 *: 경고가 트리거되면 경고 아이콘이 대시보드에 표시됩니다. 노드 페이지의 노드에 대한 알림 아이콘도 표시됩니다. 이 경우 "경고 e-메일 알림이 구성되었습니다"알림을 해제하지 않는 한 이메일 알림도 전송됩니다.
- 해결된 경고 *: 해결된 경고 기록을 검색하고 볼 수 있습니다.

비디오를 시청한 경우(선택 사항): "비디오: 경고 개요"

다음 표에서는 현재 및 해결된 경고에 대해 Grid Manager에 표시되는 정보를 설명합니다.

열 머리글	설명
이름 또는 제목	알림의 이름과 설명입니다.

열 머리글	설명
심각도입니다	알림의 심각도입니다. 현재 알림의 경우 여러 알림이 그룹화되면 제목 행에 각 심각도에 대해 발생한 알림의 인스턴스 수가 표시됩니다.  * Critical *: StorageGRID 노드 또는 서비스의 정상 작동을 중지한 비정상 상태가 존재함. 기본 문제를 즉시 해결해야 합니다. 문제가 해결되지 않으면 서비스가 중단되거나 데이터가 손실될 수 있습니다.  **Major**: 현재 작업에 영향을 미치거나 중요 경고에 대한 임계값에 접근하는 비정상적인 상태가 존재합니다. StorageGRID 노드나 서비스의 정상 작동을 비정상적인 상태로 중지하지 않도록 주요 경고를 조사하고 모든 기본 문제를 해결해야 합니다.  **Minor**: 시스템이 정상적으로 작동하고 있지만, 시스템이 계속 작동할 경우 시스템 작동 능력에 영향을 줄 수 있는 비정상적인 상태가 있습니다. 보다 심각한 문제를 초래하지 않도록 자체적으로 명확하지 않은 사소한 경고를 모니터링하고 해결해야 합니다.
시간 트리거됨	• 현재 경고 *: 현지 시간 및 UTC에서 알림이 트리거된 날짜 및 시간입니다. 여러 개의 경고가 그룹화되면 제목 행에 경고의 가장 최근 인스턴스(*l*최신형)와 가장 오래된 인스턴스(*oldest*)에 대한 시간이 표시됩니다. • 해결된 경고 *: 알림이 트리거된 지 얼마 전입니다.
사이트/노드	알림이 발생했거나 발생한 사이트 및 노드의 이름입니다.
상태	경고가 활성, 해제 또는 해결되었는지 여부 여러 개의 경고가 그룹화되고 드롭다운에서 * All alerts * 를 선택하면 제목 행에 해당 경고의 활성 인스턴스 수와 해제된 인스턴스 수가 표시됩니다.
해결된 시간(해결된 알림만 해당)	알림이 해결된 지 얼마 전입니다.
현재 값 또는 _ 데이터 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. • 참고: * 현재 경고가 여러 개 그룹화되어 있으면 제목 행에 현재 값이 표시되지 않습니다.
트리거된 값(해결된 알림만 해당)	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.

단계

1. 해당 범주의 경고 목록을 보려면 * Current alerts * 또는 * Resolved alerts * 링크를 선택하십시오. 또한 * Nodes *

> *NODE* > * Overview * 를 선택한 다음 Alerts 테이블에서 알림을 선택하여 알림에 대한 세부 정보를 볼 수도 있습니다.

기본적으로 현재 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 알림 페이지는 2분마다 새로 고쳐집니다.

2. 알림 그룹을 확장하려면 아래쪽 캐럿을 선택합니다. 그룹에서 개별 알림을 축소하려면 위로 캐럿을 선택하거나 그룹 이름을 선택합니다.
3. 알림 그룹 대신 개별 경고를 표시하려면 * Group alerts * 확인란의 선택을 취소합니다.
4. 현재 알림 또는 알림 그룹을 정렬하려면 각 열 머리글에서 위쪽/아래쪽 화살표를 선택합니다.
   - 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 * 가 지워지면 전체 경고 목록이 정렬됩니다. 예를 들어, 특정 노드에 영향을 주는 모든 경고를 보기 위해 * 노드/사이트 * 별로 모든 경고를 정렬할 수 있습니다.
5. 현재 경고를 상태(* All alerts *, * Active * 또는 * Silenced * 로 필터링하려면 테이블 상단의 드롭다운 메뉴를 사용합니다.

   을 "알림 메시지를 해제합니다"참조하십시오.

6. 해결된 경고를 정렬하려면
   - 트리거 시 * 드롭다운 메뉴에서 기간을 선택합니다.
   - 심각도 * 드롭다운 메뉴에서 하나 이상의 심각도를 선택합니다.
   - 경고 규칙 * 드롭다운 메뉴에서 하나 이상의 기본 또는 사용자 지정 경고 규칙을 선택하여 특정 경고 규칙과 관련된 해결된 경고를 필터링합니다.
   - 노드 * 드롭다운 메뉴에서 하나 이상의 노드를 선택하여 특정 노드와 관련된 해결된 경고를 필터링합니다.
7. 특정 경고에 대한 세부 정보를 보려면 경고를 선택합니다. 대화 상자는 선택한 경고에 대한 세부 정보 및 권장 조치를 제공합니다.
8. (선택 사항) 특정 경고의 경우 이 알림을 트리거한 알림 규칙을 해제하려면 이 알림 해제 를 선택합니다.

   알림 규칙을 해제하려면 가 있어야 "알림 또는 루트 액세스 권한을 관리합니다"합니다.

   > 경고 규칙을 해제할 때는 주의하십시오. 경고 규칙이 해제된 경우 중요한 작업이 완료되지 못하도록 하기 전까지는 기본 문제를 감지하지 못할 수 있습니다.

9. 알림 규칙의 현재 조건을 보려면:
   a. 경고 세부 정보에서 * 조건 보기 * 를 선택합니다.

정의된 각 심각도에 대한 Prometheus 표현식이 나열된 팝업이 나타납니다.

b. 팝업을 닫으려면 팝업 외부의 아무 곳이나 클릭합니다.

10. 선택적으로 * 규칙 편집 * 을 선택하여 이 경고가 트리거되도록 한 경고 규칙을 편집합니다.

알림 규칙을 편집하려면 이 있어야 "알림 또는 루트 액세스 권한을 관리합니다"합니다.

> 알림 규칙을 편집하기로 결정할 때는 주의해야 합니다. 트리거 값을 변경하는 경우 중요한 작업이 완료되지 못할 때까지 기본 문제를 감지하지 못할 수 있습니다.

11. 경고 세부 정보를 닫으려면 * 닫기 * 를 선택합니다.

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.

StorageGRID 시스템의 각 사이트 및 각 스토리지 노드에 대해 전체 그리드를 사용할 수 "스토리지 용량 정보를 봅니다 "있습니다.

전체 그리드에 대한 스토리지 용량을 모니터링합니다

그리드의 전체 스토리지 용량을 모니터링하여 오브젝트 데이터 및 오브젝트 메타데이터에 대한 충분한 여유 공간이 유지되도록 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.

Grid Manager 대시보드를 사용하면 전체 그리드와 각 데이터 센터에 사용할 수 있는 스토리지 양을 신속하게 평가할 수 있습니다. 노드 페이지에서는 오브젝트 데이터 및 오브젝트 메타데이터에 대한 자세한 값을 제공합니다.

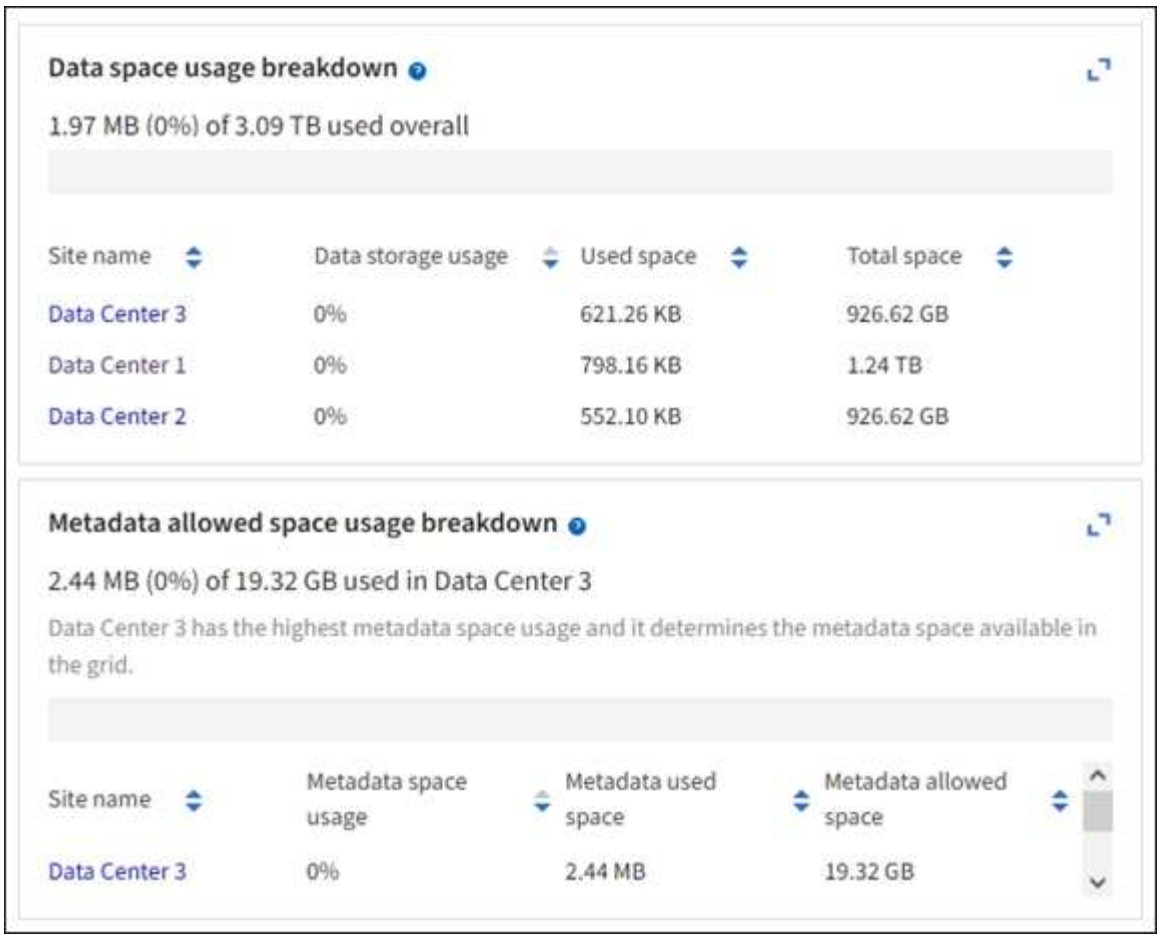
단계

1. 전체 그리드 및 각 데이터 센터에 사용할 수 있는 스토리지 양을 평가합니다.

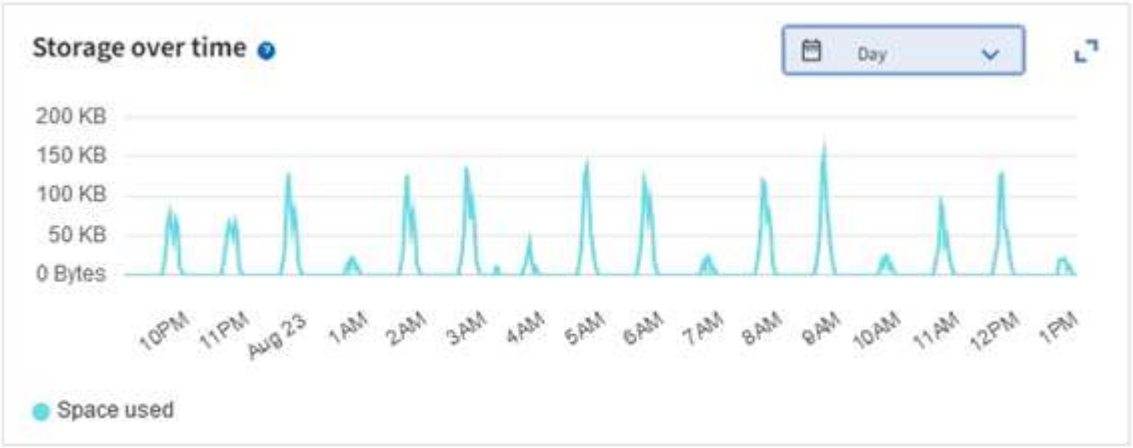
   a. 대시보드 > 개요 * 를 선택합니다.

   b. 데이터 공간 사용량 분석 및 메타데이터 허용 공간 사용량 분석 카드의 값을 확인합니다. 각 카드에는 스토리지 사용 비율, 사용된 공간 용량 및 사이트에서 사용 가능하거나 허용되는 총 공간이 나열됩니다.

      > 요약에는 아카이브 미디어가 포함되지 않습니다.



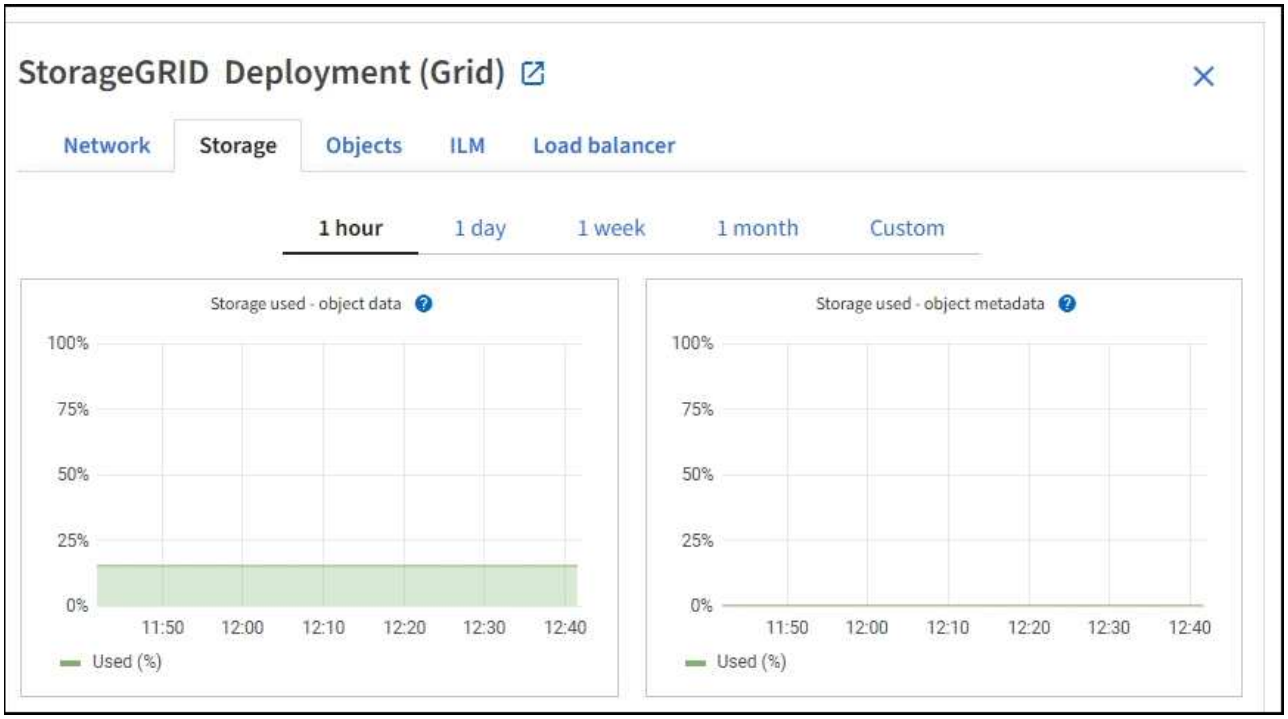
a. Storage Over Time 카드의 차트를 참조하십시오. 기간 드롭다운을 사용하여 스토리지 사용 속도를 결정할 수 있습니다.



2. 사용된 스토리지 양과 오브젝트 데이터 및 오브젝트 메타데이터에 대해 그리드에 사용 가능한 스토리지 양에 대한 자세한 내용은 노드 페이지를 참조하십시오.

a. 노드 * 를 선택합니다.

b. **GRID* * > * 스토리지 * 를 선택합니다.



c. 커서를 * Storage Used-object data * 및 * Storage Used-object metadata * 차트 위에 놓으면 전체 그리드에 사용 가능한 오브젝트 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 메트릭을 보고하지 않은 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.

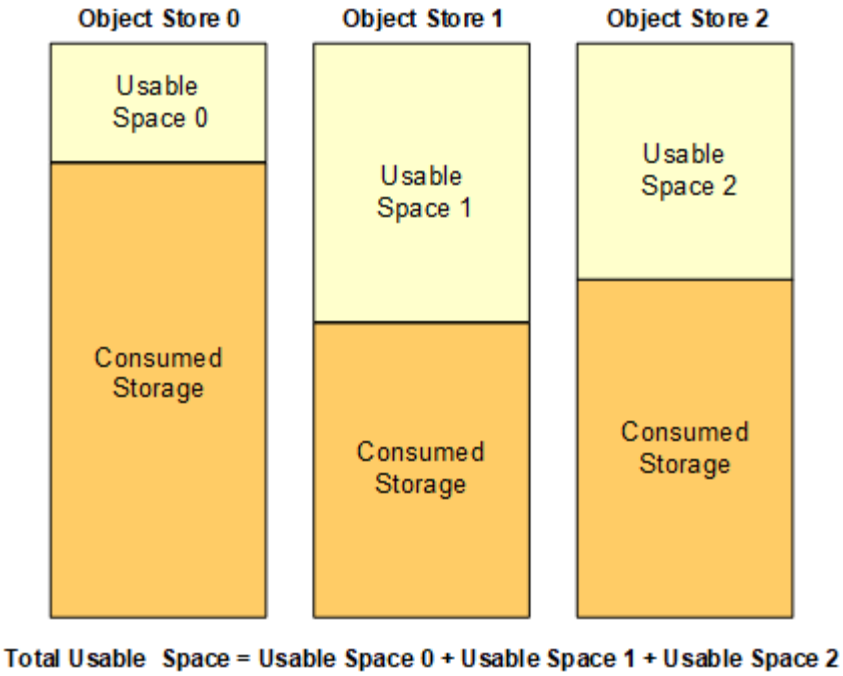
   스토리지 확장 계획에 대한 자세한 내용은 을 "StorageGRID 확장 지침"참조하십시오.

각 스토리지 노드의 스토리지 용량을 모니터링합니다

각 스토리지 노드의 총 사용 가능 공간을 모니터링하여 노드에 새 객체 데이터를 위한 충분한 공간이 있는지 확인합니다.

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

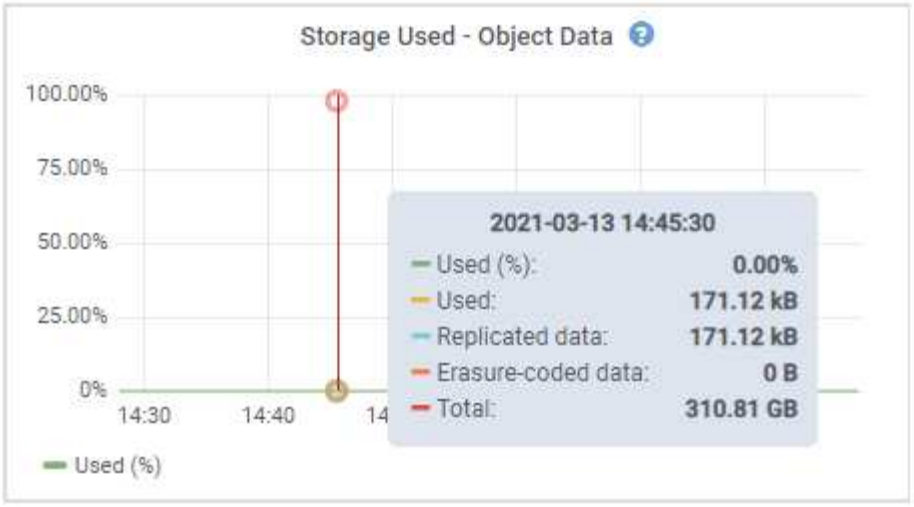
1. nodes * > **Storage Node* * > * Storage * 를 선택합니다.

   노드에 대한 그래프와 표가 나타납니다.

2. 커서를 Storage Used-object 데이터 그래프 위에 놓습니다.

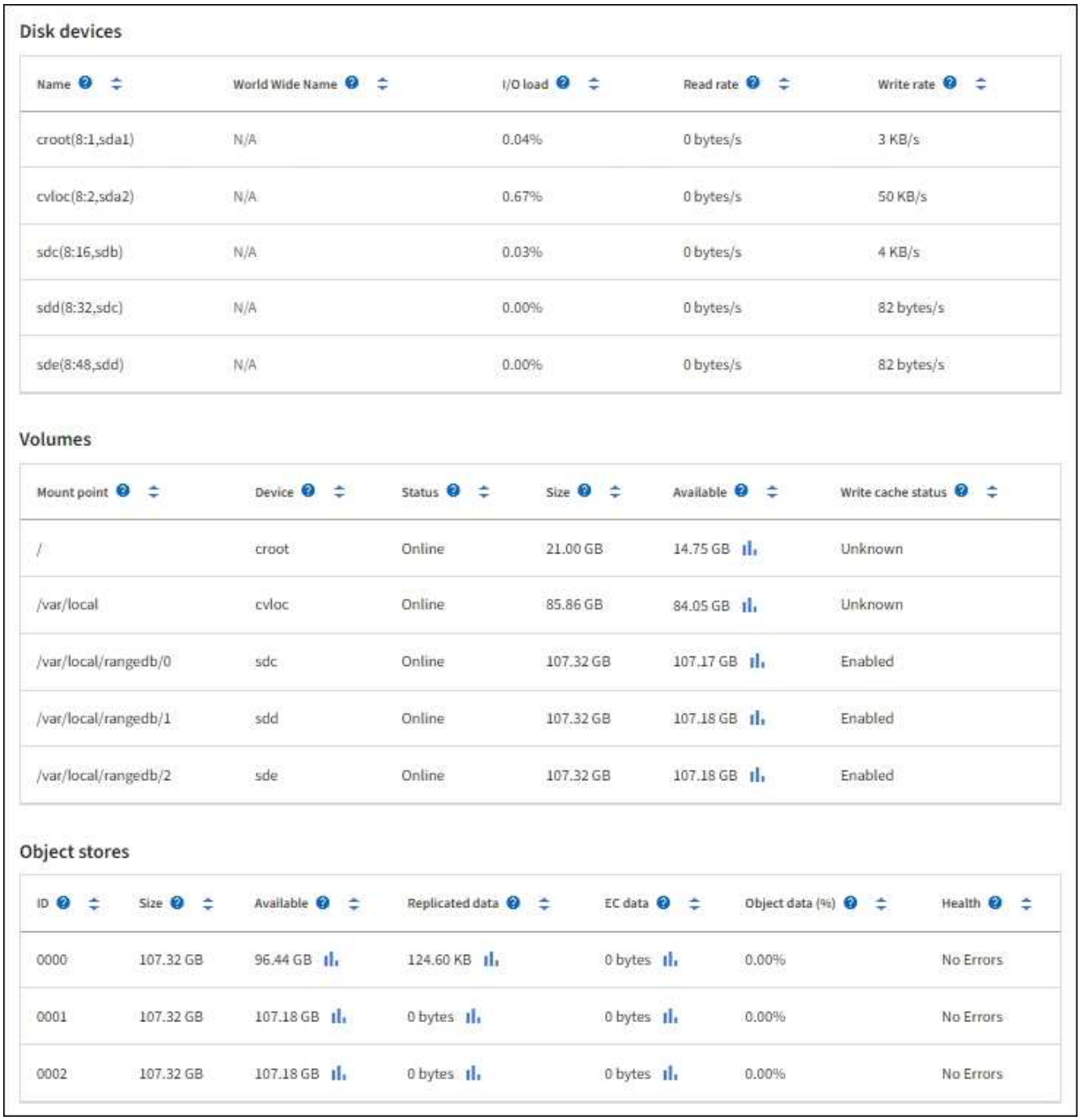
   다음 값이 표시됩니다.

   - * 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 `storagegrid_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 사용 가능한 열에서 차트 아이콘을 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 을 "StorageGRID 확장 지침"참조하십시오.

   이 "오브젝트 데이터 스토리지가 부족합니다" 알림은 스토리지 노드에 객체 데이터를 저장하기 위한 공간이 부족할

때 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.

이 작업에 대해

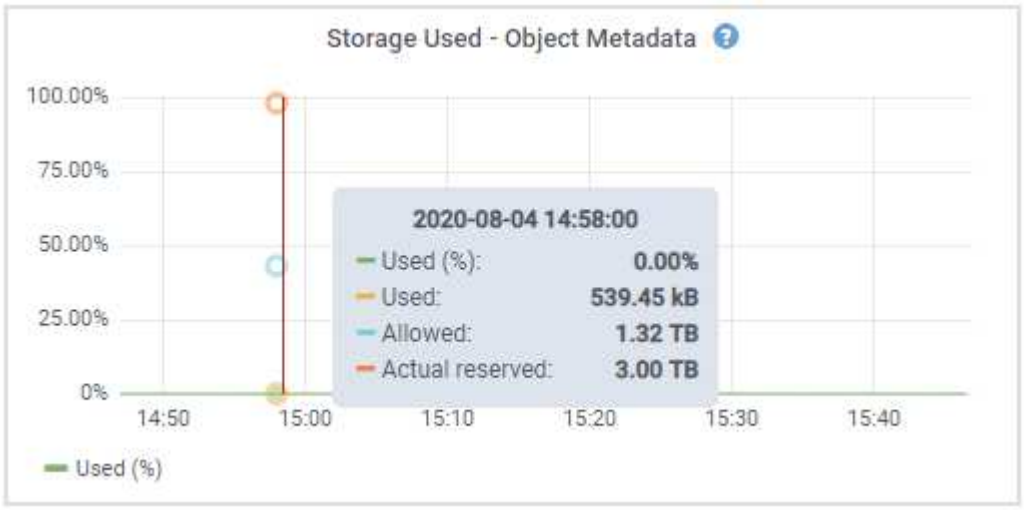
StorageGRID는 이중화를 제공하고 오브젝트 메타데이터를 손실로부터 보호하기 위해 각 사이트에 3개의 오브젝트 메타데이터 복사본을 유지합니다. 이 세 복제본은 각 스토리지 노드의 스토리지 볼륨 0에 있는 메타데이터에 예약된 공간을 사용하여 각 사이트의 모든 스토리지 노드에 균등하게 분산됩니다.

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.



사용됨**(%)**

이 스토리지 노드에서 사용된 허용된 메타데이터 공간의 비율입니다.

Prometheus 메트릭: `storagegrid_storage_utilization_metadata_bytes` 및 `storagegrid_storage_utilization_metadata_allowed_bytes`

사용됨

이 스토리지 노드에서 사용된 허용되는 메타데이터 공간의 바이트

Prometheus 메트릭: `storagegrid_storage_utilization_metadata_bytes`

허용됨

이 스토리지 노드의 객체 메타데이터에 허용되는 공간입니다. 각 스토리지 노드에 대해 이 값이 어떻게 결정되는지 알아보려면 을 참조하십시오"허용되는 메타데이터 공간에 대한 전체 설명입니다".

Prometheus 메트릭: `storagegrid_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 어떻게 계산되는지 알아보려면 을 참조하십시오 "메타데이터에 대한 실제 예약 공간의 전체 설명입니다".

_Prometheus 메트릭은 향후 릴리스에 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 "StorageGRID 시스템 확장을 위한 지침"참조하십시오.

공간 사용 예측을 모니터링합니다

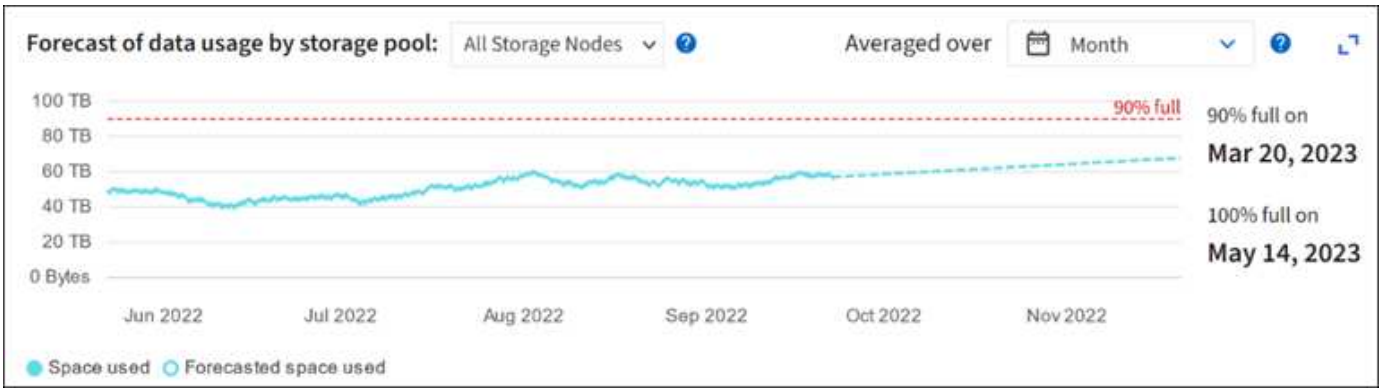
사용자 데이터와 메타데이터에 대한 공간 사용 예측을 모니터링하여 필요한 시기를 "그리드를 확장합니다"예측합니다.

시간에 따라 소비율이 변화하는 것을 알게 되면 * Averaged Over * (평균 초과 *) 풀다운 메뉴에서 가장 최근의 수집 패턴만 반영하는 더 짧은 범위를 선택합니다. 계절별 패턴을 발견한 경우 더 긴 범위를 선택합니다.

새 StorageGRID를 설치한 경우 공간 사용 예측을 평가하기 전에 데이터와 메타데이터가 축적되도록 합니다.

단계

1. 대시보드에서 * Storage * 를 선택합니다.
2. 대시보드 카드, 스토리지 풀별 데이터 사용량 예측 및 사이트별 메타데이터 사용량 예측 을 확인합니다.
3. 이 값을 사용하여 데이터 및 메타데이터 스토리지에 새 스토리지 노드를 추가해야 하는 시기를 예측할 수 있습니다.



정보 수명 주기 관리를 모니터링합니다

ILM(정보 수명 주기 관리) 시스템은 그리드에 저장된 모든 개체에 대한 데이터 관리 기능을 제공합니다. ILM 작업을 모니터링하여 그리드가 현재 로드를 처리할 수 있는지 또는 추가 리소스가 필요한지 여부를 파악해야 합니다.

이 작업에 대해

StorageGRID 시스템은 활성 ILM 정책을 적용하여 오브젝트를 관리합니다. ILM 정책 및 관련 ILM 규칙은 생성할 복사본의 수, 생성할 복사본의 유형, 복사본을 배치할 위치 및 각 복사본을 보존할 기간을 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. StorageGRID가 클라이언트 작업을 수행하고 있는지 모니터링해야 합니다.

Grid Manager 대시보드 탭을 사용합니다

단계

Grid Manager 대시보드의 ILM 탭을 사용하여 ILM 작업을 모니터링합니다.

1. Grid Manager에 로그인합니다.
2. 대시보드에서 ILM 탭을 선택하고 ILM 대기열(개체) 카드 및 ILM 평가율 카드의 값을 확인합니다.

   대시보드의 ILM 대기열(개체) 카드가 일시적으로 급증할 수 있습니다. 그러나 대기열이 계속 증가하고 감소하지 않으면 그리드를 효율적으로 운영하는 데 더 많은 리소스가 필요합니다. 즉, 스토리지 노드를 추가하거나 ILM 정책에 따라 원격 위치에 개체를 배치하면 네트워크 대역폭이 증가합니다.

노드 페이지를 사용합니다

단계

또한 다음과 같이 * nodes * 페이지를 사용하여 ILM 대기열을 조사합니다.

nodes * 페이지의 차트는 향후 StorageGRID 릴리스에서 해당 대시보드 카드로 대체될 예정입니다.

1. 노드 * 를 선택합니다.
2. *GRID NAME* * > * ILM * 을 선택합니다.
3. ILM 대기열 그래프 위에 커서를 올려 놓으면 지정된 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.

- * 스캔 기간 - 추정 * : 모든 개체의 전체 ILM 스캔을 완료하는 데 걸리는 예상 시간입니다.

> 전체 스캔은 ILM이 모든 개체에 적용되었다고 보장하지 않습니다.

- * Repairs attemed *: 시도한 복제된 데이터에 대한 총 개체 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. 시도한 수리 수가 더 이상 증가하지 않고 전체 검사가 완료된 경우 수리가 완료된 것일 수 있습니다.

네트워킹 및 시스템 리소스를 모니터링합니다

노드와 사이트 간 네트워크의 무결성과 대역폭, 개별 그리드 노드의 리소스 사용은 효율적인 운영에 매우 중요합니다.

네트워크 연결 및 성능을 모니터링합니다

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) 또는 수집 성능 저하 및 ILM 백로그가 발생할 수 있습니다.

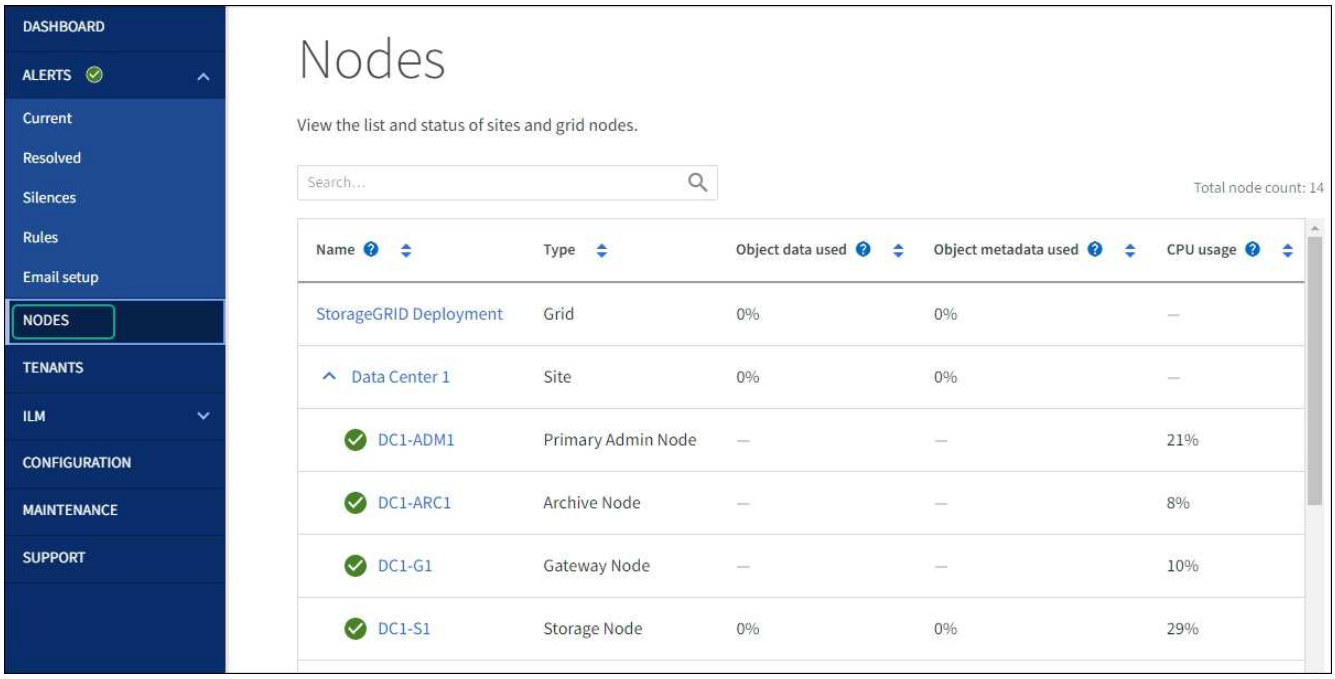
Grid Manager를 사용하여 연결 및 네트워크 성능을 모니터링하면 문제를 즉시 해결할 수 있습니다.

또한 특정 테넌트, 버킷, 서브넷 또는 로드 밸런서 끝점과 관련된 트래픽을 모니터링할 수 있도록 하는 것도 "네트워크 트래픽 분류 정책을 생성합니다"고려하십시오. 필요에 따라 트래픽 제한 정책을 설정할 수 있습니다.

단계

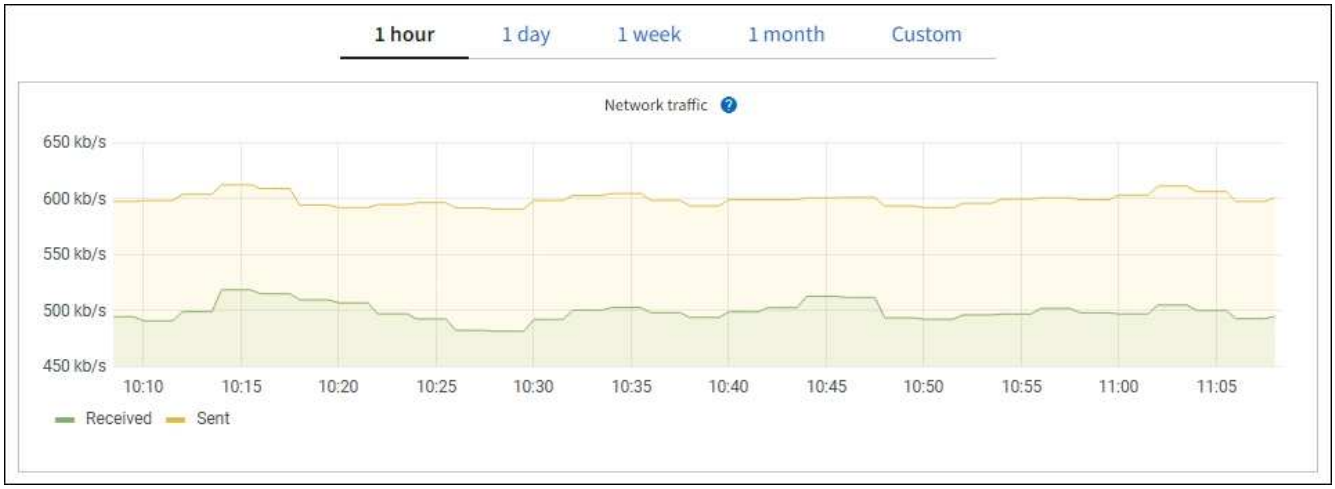
1. 노드 * 를 선택합니다.

   노드 페이지가 나타납니다. 그리드의 각 노드는 테이블 형식으로 나열됩니다.

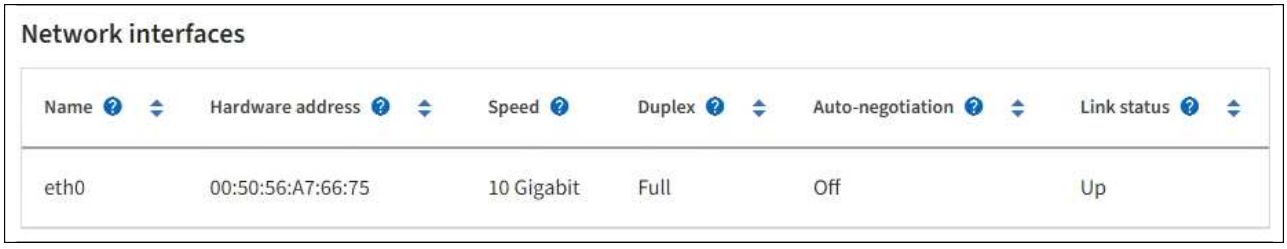


2. 그리드 이름, 특정 데이터 센터 사이트 또는 그리드 노드를 선택한 다음 * 네트워크 * 탭을 선택합니다.

   네트워크 트래픽 그래프는 그리드의 전체 네트워크 트래픽, 데이터 센터 사이트 또는 노드에 대한 요약 정보를 제공합니다.

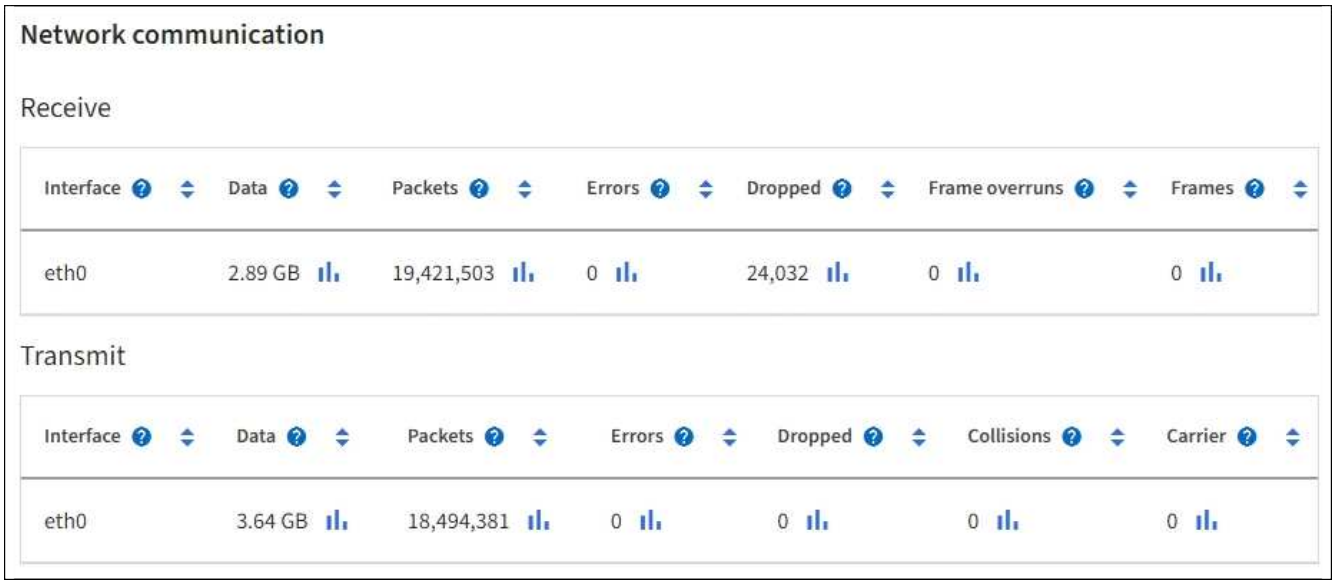


   a. 그리드 노드를 선택한 경우 아래로 스크롤하여 페이지의 * 네트워크 인터페이스 * 섹션을 검토합니다.



   b. 그리드 노드의 경우 아래로 스크롤하여 페이지의 * 네트워크 통신 * 섹션을 검토합니다.

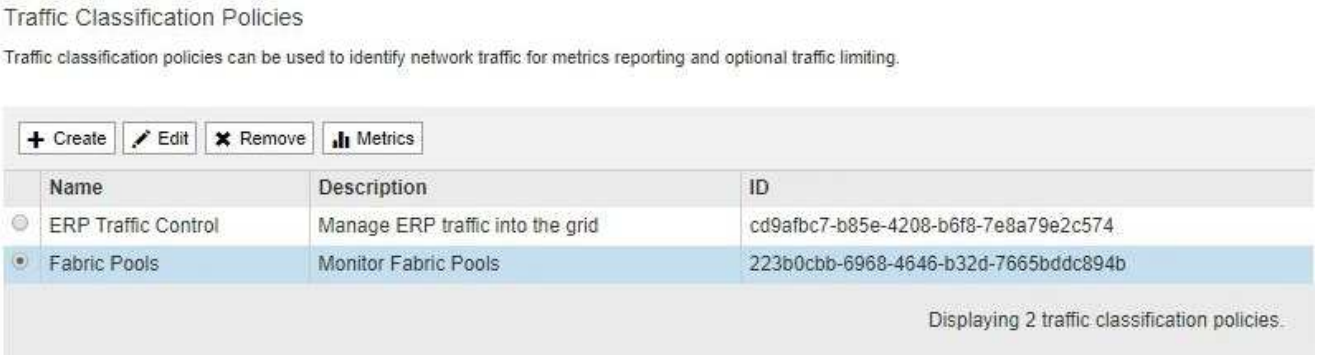
      Receive 및 Transmit 테이블은 각 네트워크에서 수신 및 전송된 바이트 및 패킷의 수와 기타 수신 및 전송 메트릭을 보여줍니다.



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.



   a. 정책과 연결된 네트워킹 메트릭을 보여주는 그래프를 보려면 정책 왼쪽의 라디오 버튼을 선택한 다음 * Metrics * 를 클릭합니다.

   b. 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".

관련 정보

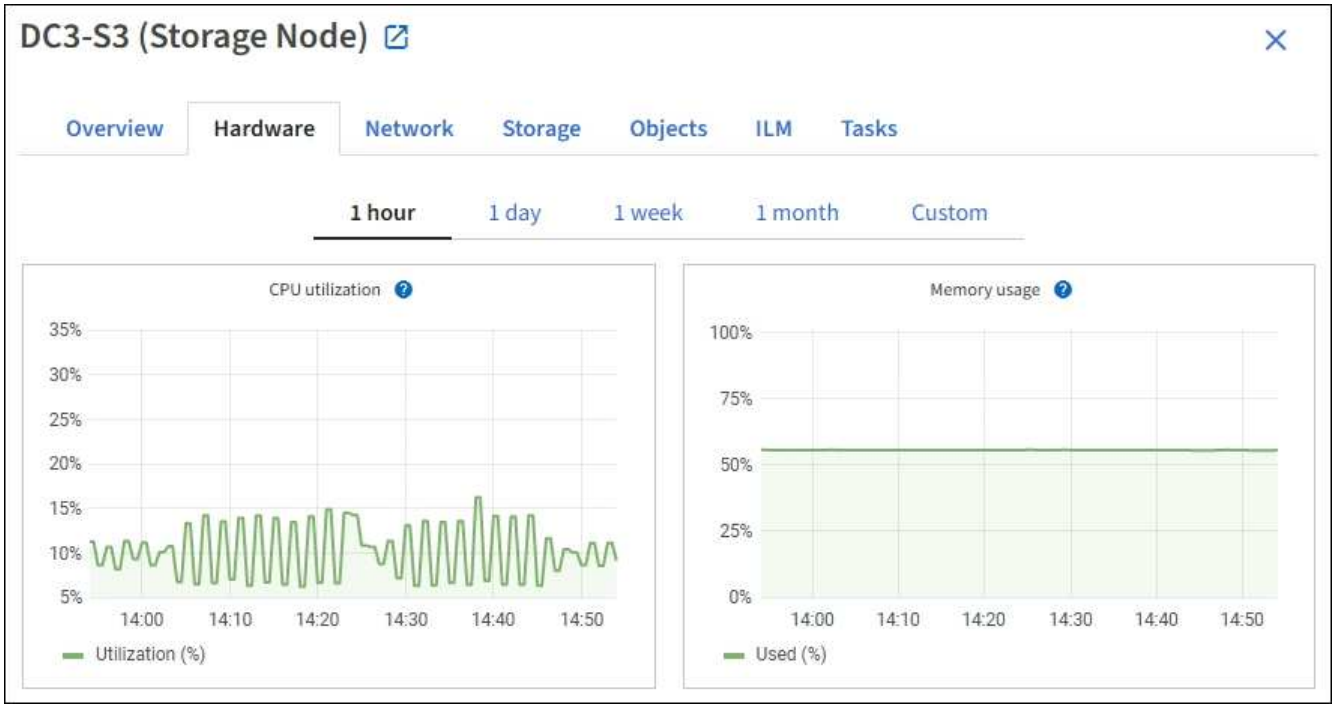
- "네트워크 탭을 봅니다"
- "노드 연결 상태를 모니터링합니다"

노드 레벨 리소스를 모니터링합니다

개별 그리드 노드를 모니터링하여 리소스 사용 수준을 확인합니다. 노드가 지속적으로 과부하 상태가 되면 효율적인 작업에 더 많은 노드가 필요할 수 있습니다.

단계

1. nodes * 페이지에서 노드를 선택합니다.
2. Hardware * 탭을 선택하여 CPU 사용률 및 메모리 사용량 그래프를 표시합니다.



3. 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.
4. 노드가 스토리지 어플라이언스 또는 서비스 어플라이언스에서 호스팅되는 경우 아래로 스크롤하여 구성 요소 테이블을 확인합니다. 모든 구성 요소의 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 S3 클라이언트 작업은 StorageGRID 테넌트 계정과 연결됩니다. Grid Manager를 사용하여 모든 테넌트 또는 특정 테넌트의 스토리지 사용량 또는 네트워크 트래픽을 모니터링할 수 있습니다. 감사 로그 또는 Grafana 대시보드를 사용하여 테넌트가 StorageGRID를 사용하는 방법에 대한 자세한 정보를 수집할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 또는 테넌트 계정 권한"있습니다.

모든 테넌트를 봅니다

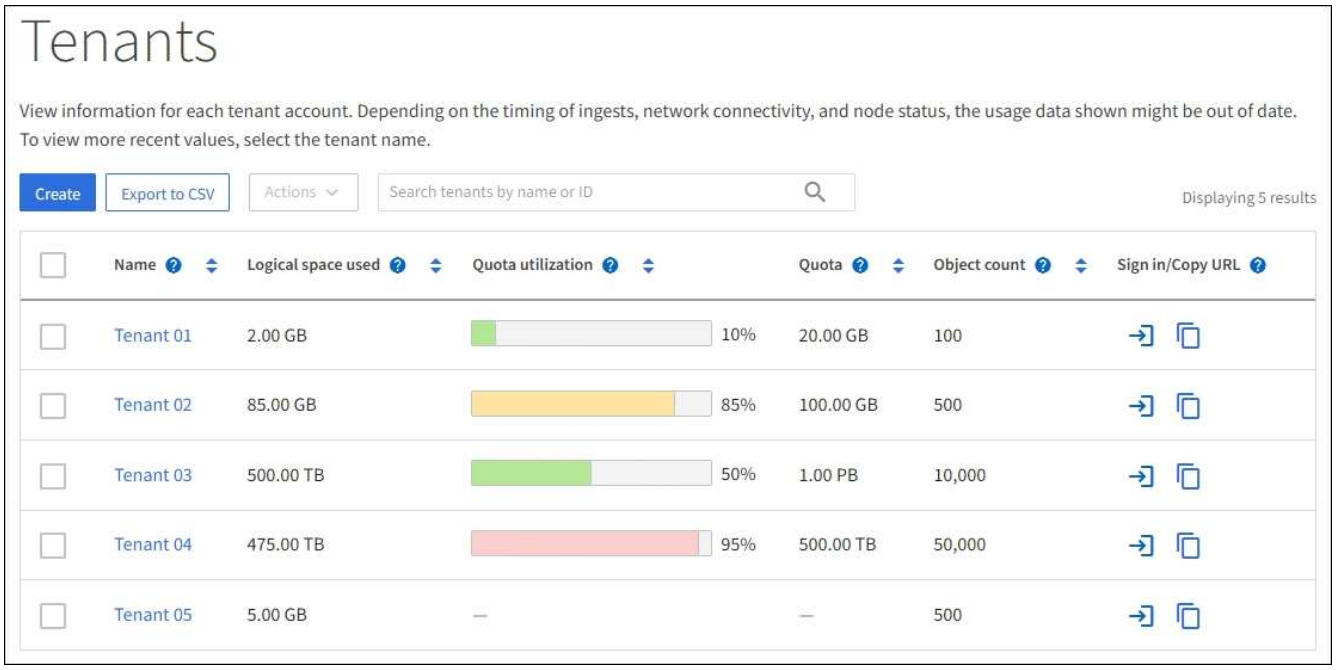
Tenants 페이지에는 현재 모든 테넌트 계정에 대한 기본 정보가 표시됩니다.

단계

1. Tenants * 를 선택합니다.
2. 테넌트 페이지에 표시된 정보를 검토합니다.

   각 테넌트에 대해 사용된 논리적 공간, 할당량 사용량, 할당량 및 객체 수가 나열됩니다. 테넌트에 대해 할당량이 설정되지 않은 경우 할당량 사용 및 할당량 필드에는 대시(—)가 포함됩니다.

   > 사용된 공간 값은 추정값입니다. 이러한 추정치는 베스트 타이밍, 네트워크 연결 및 노드 상태의 영향을 받습니다.



3. 필요한 경우 * 로그인/URL 복사 * 열에서 로그인 링크를 선택하여 테넌트 계정에 로그인합니다.
4. 필요한 경우 * 로그인/URL 복사 * 열에서 URL 복사 링크를 선택하여 테넌트의 로그인 페이지에 대한 URL을 복사합니다.
5. 필요에 따라 * CSV로 내보내기 * 를 선택하여 모든 테넌트에 대한 사용 값이 포함된 파일을 보고 `.csv` 내보냅니다.

   파일을 열거나 저장하라는 메시지가 `.csv` 표시됩니다.

   파일의 내용은 `.csv` 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

   파일을 스프레드시트 응용 프로그램에서 열거나 자동화에서 사용할 수 `.csv` 있습니다.

6. 오브젝트가 나열되지 않은 경우 선택적으로 * 작업 * > * 삭제 * 를 선택하여 하나 이상의 테넌트를 제거합니다. 을 "테넌트 계정을 삭제합니다"참조하십시오.

계정에 버킷이나 컨테이너가 포함된 경우 테넌트 계정을 제거할 수 없습니다.

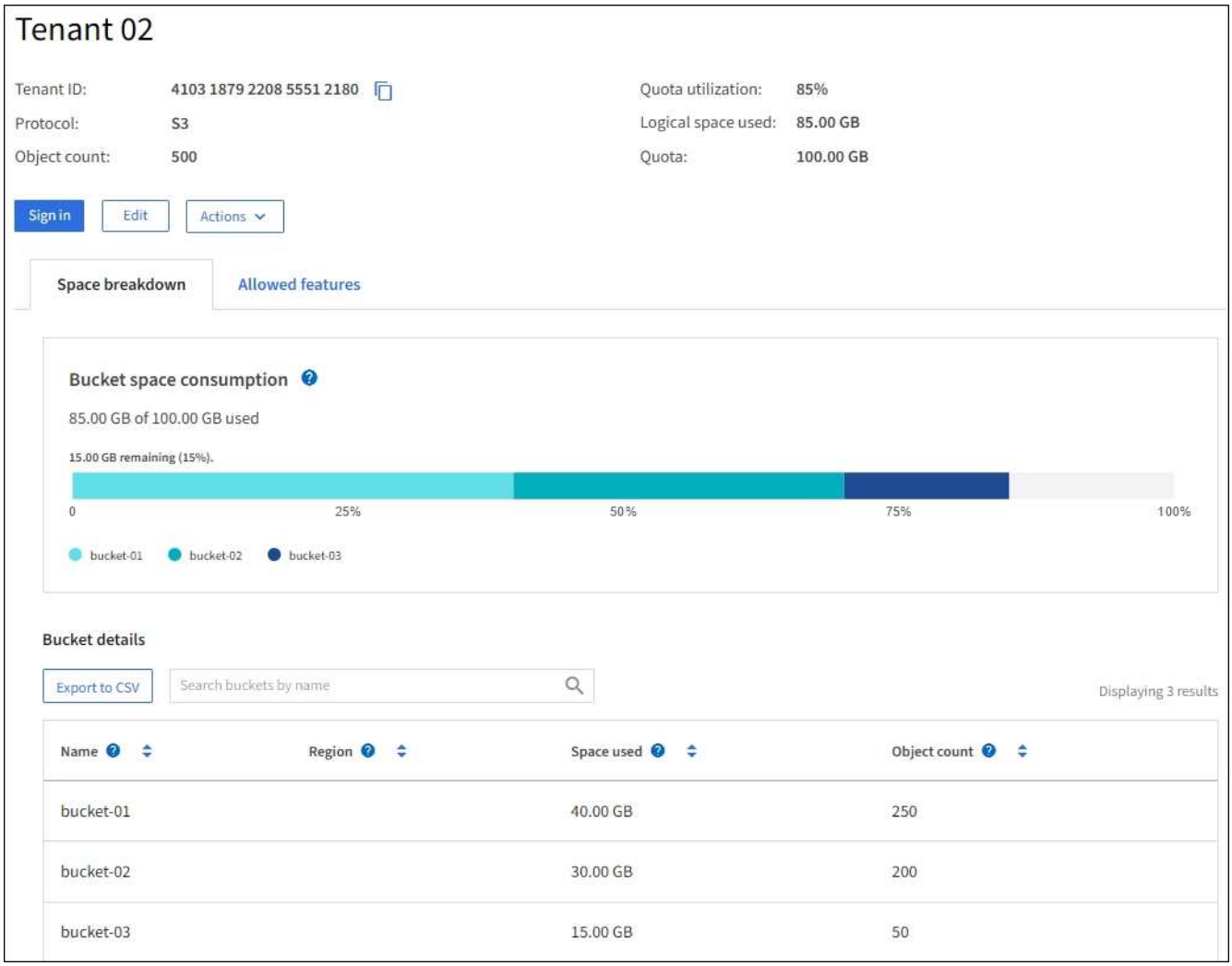
특정 테넌트를 봅니다

특정 테넌트의 세부 정보를 볼 수 있습니다.

단계

1. 테넌트 페이지에서 테넌트 이름을 선택합니다.

   테넌트 세부 정보 페이지가 나타납니다.



2. 페이지 상단의 테넌트 개요를 검토합니다.

   세부 정보 페이지의 이 섹션에서는 테넌트의 개체 수, 할당량 사용, 사용된 논리적 공간 및 할당량 설정을 비롯한 테넌트에 대한 요약 정보를 제공합니다.

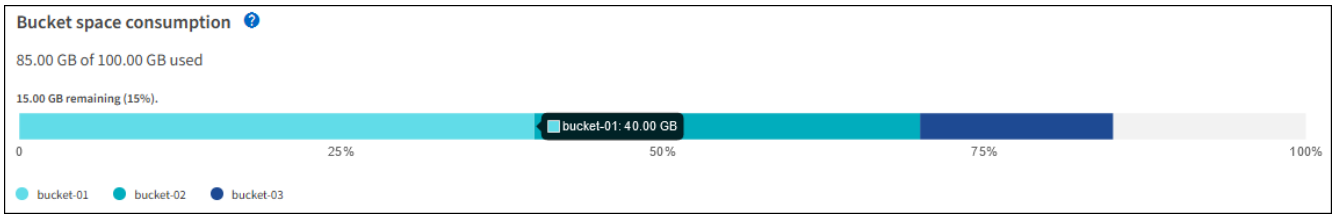
3. Space 고장 * 탭에서 * 공간 소비 * 차트를 검토하십시오.

   이 차트에는 테넌트의 모든 S3 버킷에 대한 총 공간 소비량이 표시됩니다.

   이 테넌트에 할당량이 설정된 경우 사용된 할당량과 남은 할당량이 텍스트로 표시됩니다(예: `85.00 GB of 100 GB used`). 할당량이 설정되지 않은 경우 테넌트는 무제한 할당량을 가지며 텍스트에는 사용된 공간(예:)만 `85.00`

GB used 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 사용은 내부 추정치에 기초하며 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 사용이 다시 계산될 때까지 테넌트가 일시적으로 새 개체를 업로드하지 못할 수 있습니다. 할당량 사용량 계산에는 10분 이상이 소요될 수 있습니다.

테넌트의 할당량 사용량은 테넌트가 StorageGRID에 업로드한 총 개체 데이터 양(논리적 크기)을 나타냅니다. 할당량 사용량은 이러한 객체의 복제본과 해당 메타데이터(물리적 크기)를 저장하는 데 사용되는 공간을 나타내지 않습니다.

테넌트 할당량 사용량 높음 * 알림 규칙을 설정하여 테넌트가 할당량을 사용하고 있는지 확인할 수 있습니다. 활성화된 경우 테넌트가 할당량의 90%를 사용한 경우 이 경고가 트리거됩니다. 자세한 내용은 을 "알림 규칙을 편집합니다"참조하십시오.

4. Space 고장 * 탭에서 * Bucket 세부 정보 * 를 검토합니다.

   이 표에는 테넌트의 S3 버킷이 나와 있습니다. 사용된 공간 은 버킷 또는 컨테이너에 있는 오브젝트 데이터의 총 양입니다. 이 값은 ILM 복사본 및 개체 메타데이터에 필요한 스토리지 공간을 나타내지 않습니다.

5. 필요에 따라 * CSV로 내보내기 * 를 선택하여 각 버킷 또는 컨테이너의 사용량 값이 포함된 .csv 파일을 보고 내보냅니다.

   개별 S3 테넌트 파일의 내용은 .csv 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

   파일을 스프레드시트 응용 프로그램에서 열거나 자동화에서 사용할 수 .csv 있습니다.

6. 필요에 따라 * Allowed features * 탭을 선택하여 테넌트에 대해 활성화된 권한 및 기능의 목록을 확인합니다. "테넌트 계정을 편집합니다"이러한 설정을 변경해야 하는지 확인하십시오.
7. 테넌트에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 * 그리드 페더레이션 * 탭을 선택하여 연결에 대해 자세히 알아보십시오.

   "그리드 페더레이션은 무엇입니까?"및 을 "그리드 페더레이션을 위해 허용된 테넌트를 관리합니다"참조하십시오.

네트워크 트래픽을 봅니다

테넌트를 위한 트래픽 분류 정책이 마련되어 있는 경우 해당 테넌트의 네트워크 트래픽을 검토하십시오.

단계

1. 구성 * > * 네트워크 * > * 트래픽 분류 * 를 선택합니다.

   트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

2. 정책 목록을 검토하여 특정 테넌트에 적용되는 정책을 식별합니다.
3. 정책과 관련된 메트릭을 보려면 정책 왼쪽의 라디오 버튼을 선택하고 * Metrics * 를 선택합니다.
4. 그래프를 분석하여 정책에 따라 트래픽이 제한되는 빈도와 정책을 조정해야 하는지 여부를 결정합니다.

자세한 내용은 을 "트래픽 분류 정책을 관리합니다" 참조하십시오.

감사 로그를 사용합니다

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 을 "감사 로그를 검토합니다" 참조하십시오.

Prometheus 메트릭을 사용합니다

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.

자세한 내용은 을 "지원 메트릭을 검토합니다" 참조하십시오.

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"

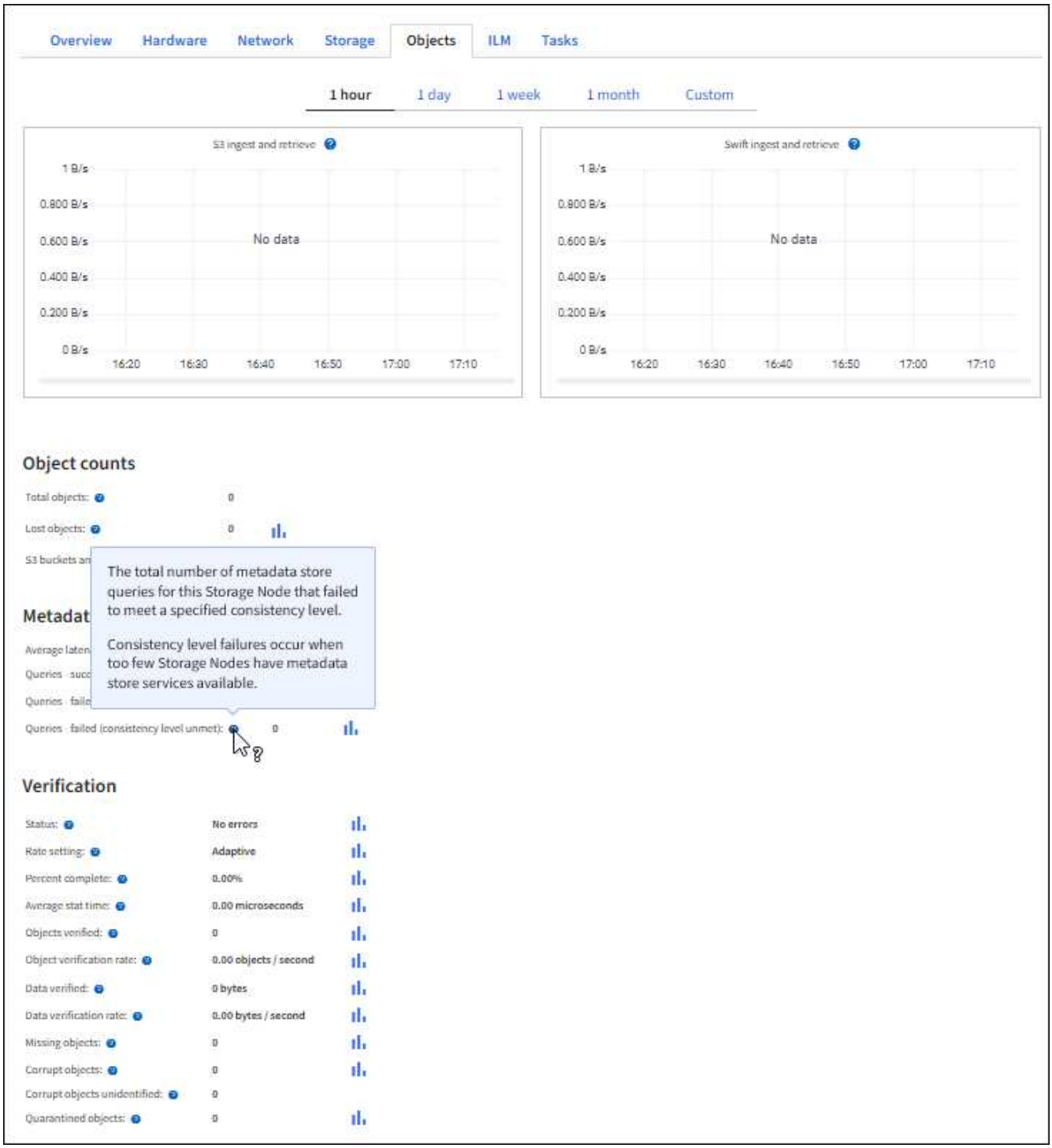
단계

1. 대시보드에서 * 성능 * 탭을 선택합니다.
2. 스토리지 노드에서 수행하는 클라이언트 작업 수와 선택한 기간 동안 스토리지 노드에서 수신한 API 요청 수를 요약한 S3 차트를 참조하십시오.
3. nodes * 를 선택하여 Nodes 페이지에 액세스합니다.
4. 노드 홈 페이지(그리드 수준)에서 * Objects * 탭을 선택합니다.

   이 차트에서는 전체 StorageGRID 시스템에 대한 S3 수집 및 검색 속도와 수집 또는 검색된 데이터의 양을 초당 바이트 단위로 보여 줍니다. 시간 간격을 선택하거나 사용자 지정 간격을 적용할 수 있습니다.

5. 특정 스토리지 노드에 대한 정보를 보려면 왼쪽의 목록에서 노드를 선택하고 * Objects * 탭을 선택합니다.

   차트에는 노드의 수집 및 검색 속도가 표시됩니다. 이 탭에는 개체 수, 메타데이터 쿼리 및 검증 작업에 대한 메트릭도 포함됩니다.



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.

이 작업에 대해

관리 노드 또는 게이트웨이 노드에서 로드 밸런서 서비스를 사용하거나 외부 타사 로드 밸런서를 사용하여 여러 스토리지 노드에 클라이언트 요청을 분산할 수 있습니다.

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.

자세한 내용은 을 "S3 클라이언트 연결을 구성합니다"참조하십시오.

단계

1. S3 클라이언트가 로드 밸런서 서비스를 사용하여 연결하는 경우 관리 노드 또는 게이트웨이 노드가 예상한 대로 트래픽을 적극적으로 분산하는지 확인하십시오.
   a. 노드 * 를 선택합니다.
   b. 게이트웨이 노드 또는 관리자 노드를 선택합니다.
   c. Overview * 탭에서 노드 인터페이스가 HA 그룹에 있는지, 노드 인터페이스가 Primary 역할을 하는지 확인합니다.

      운영 노드 및 HA 그룹에 속하지 않는 노드 역할이 있는 노드는 클라이언트에 요청을 능동적으로 분산해야 합니다.

   d. 클라이언트 요청을 능동적으로 배포해야 하는 각 노드에 대해 을 "부하 분산 탭"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 동안에는 노드가 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. 선택적으로 트래픽 분류 정책을 사용하여 부하 분산 서비스가 제공하는 트래픽에 대한 보다 자세한 분석을 볼 수 있습니다.
2. 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.

그리드 페더레이션 연결을 모니터링합니다

모든 기본 정보"그리드 페더레이션 연결", 특정 연결에 대한 세부 정보 또는 교차 그리드 복제 작업에 대한 Prometheus 메트릭을 모니터링할 수 있습니다. 두 그리드 중 하나에서 연결을 모니터링할 수 있습니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인되어 "지원되는 웹 브라우저"있습니다.
- 로그인한 그리드에 대한 가 "루트 액세스 권한"있습니다.

그리드 페더레이션 페이지에는 모든 그리드 페더레이션 연결과 그리드 페더레이션 연결을 사용하도록 허용된 모든 테넌트 계정에 대한 기본 정보가 표시됩니다.

단계

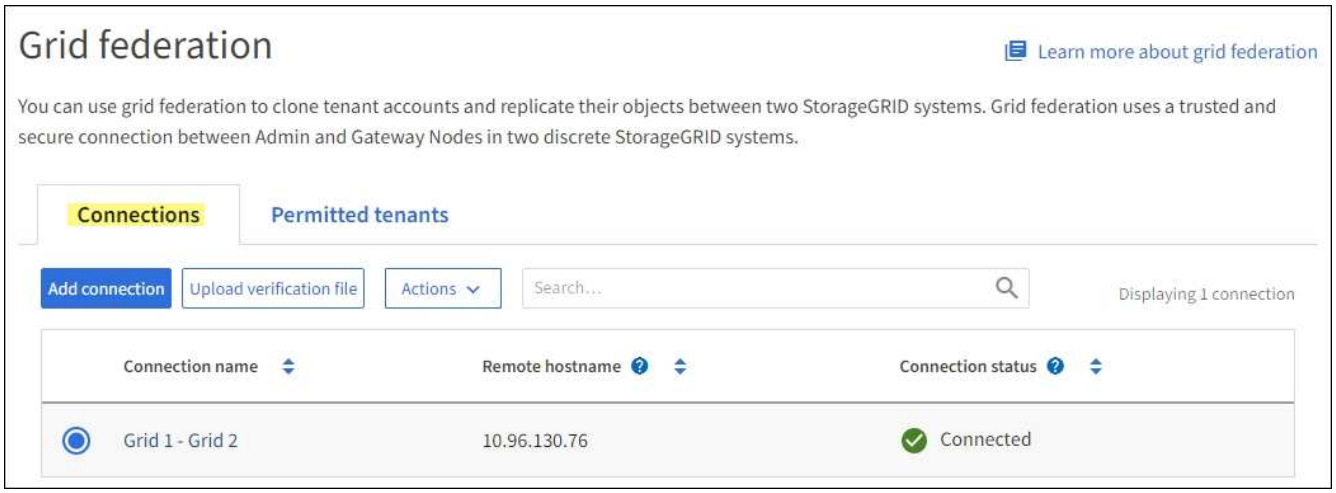
1. 구성 * > * 시스템 * > * 그리드 페더레이션 * 을 선택합니다.

   그리드 페더레이션 페이지가 나타납니다.

2. 이 그리드의 모든 연결에 대한 기본 정보를 보려면 * 연결 * 탭을 선택합니다.

   이 탭에서 다음을 수행할 수 있습니다.

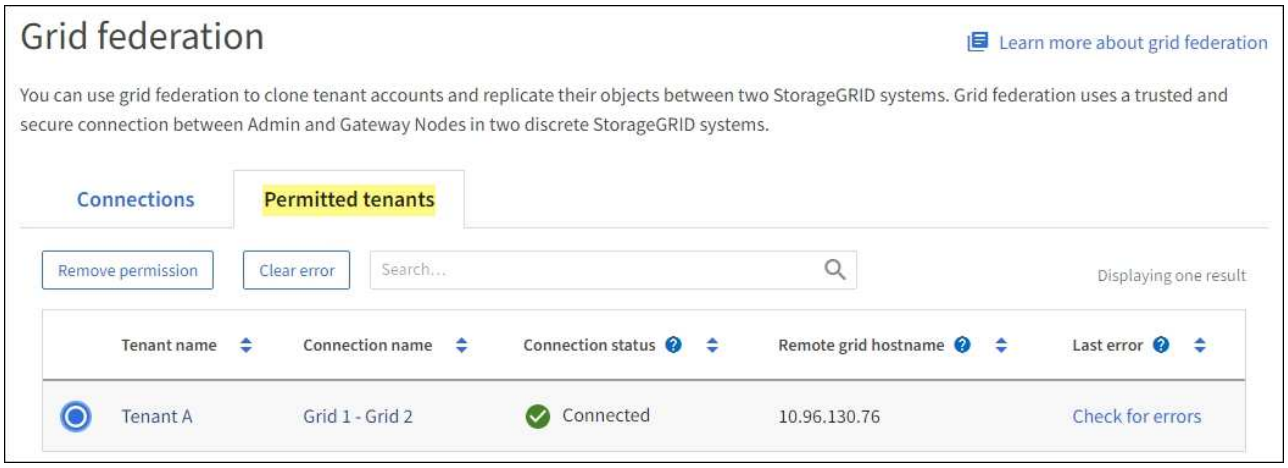
   - "새 연결을 만듭니다"..
   - 에 대한 기존 연결을 "편집 또는 테스트"선택합니다.



3. 그리드 페더레이션 연결 사용 * 권한이 있는 이 그리드의 모든 테넌트 계정에 대한 기본 정보를 보려면 * 허용된 테넌트 * 탭을 선택합니다.

   이 탭에서 다음을 수행할 수 있습니다.

   - "허용된 각 테넌트의 세부 정보 페이지를 봅니다"..
   - 각 연결에 대한 세부 정보 페이지를 봅니다. 을 특정 연결을 봅니다참조하십시오.
   - 허용된 테넌트를 선택하고 "권한을 제거합니다"을 선택합니다.
   - 교차 그리드 복제 오류가 있는지 확인하고 마지막 오류가 있으면 지웁니다. 을 "그리드 통합 오류 문제 해결 "참조하십시오.



특정 연결을 봅니다

특정 그리드 페더레이션 연결에 대한 세부 정보를 볼 수 있습니다.

단계

1. Grid Federation(그리드 통합) 페이지에서 탭 중 하나를 선택한 다음 테이블에서 연결 이름을 선택합니다.

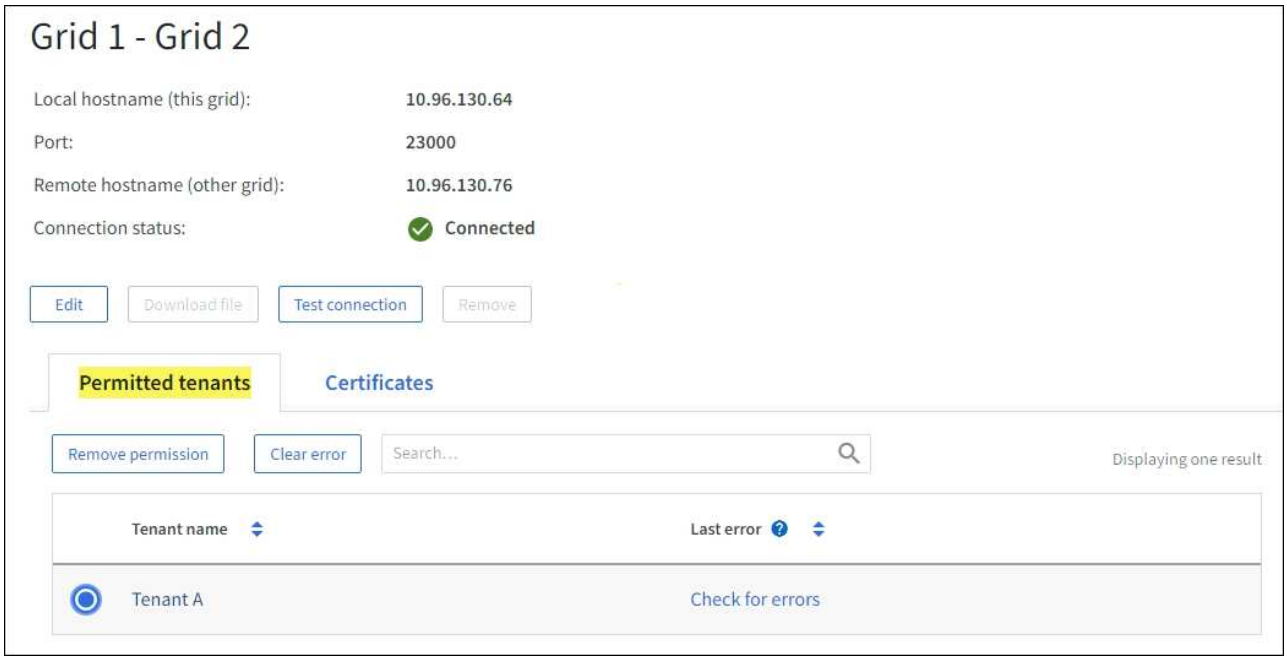
   연결에 대한 세부 정보 페이지에서 다음을 수행할 수 있습니다.

   - 로컬 및 원격 호스트 이름, 포트 및 연결 상태를 포함하여 연결에 대한 기본 상태 정보를 참조하십시오.
   - 에 대한 연결을 "편집, 테스트 또는 제거"선택합니다.

2. 특정 연결을 볼 때 * 허용된 테넌트 * 탭을 선택하여 연결에 대해 허용된 테넌트에 대한 세부 정보를 봅니다.

   이 탭에서 다음을 수행할 수 있습니다.

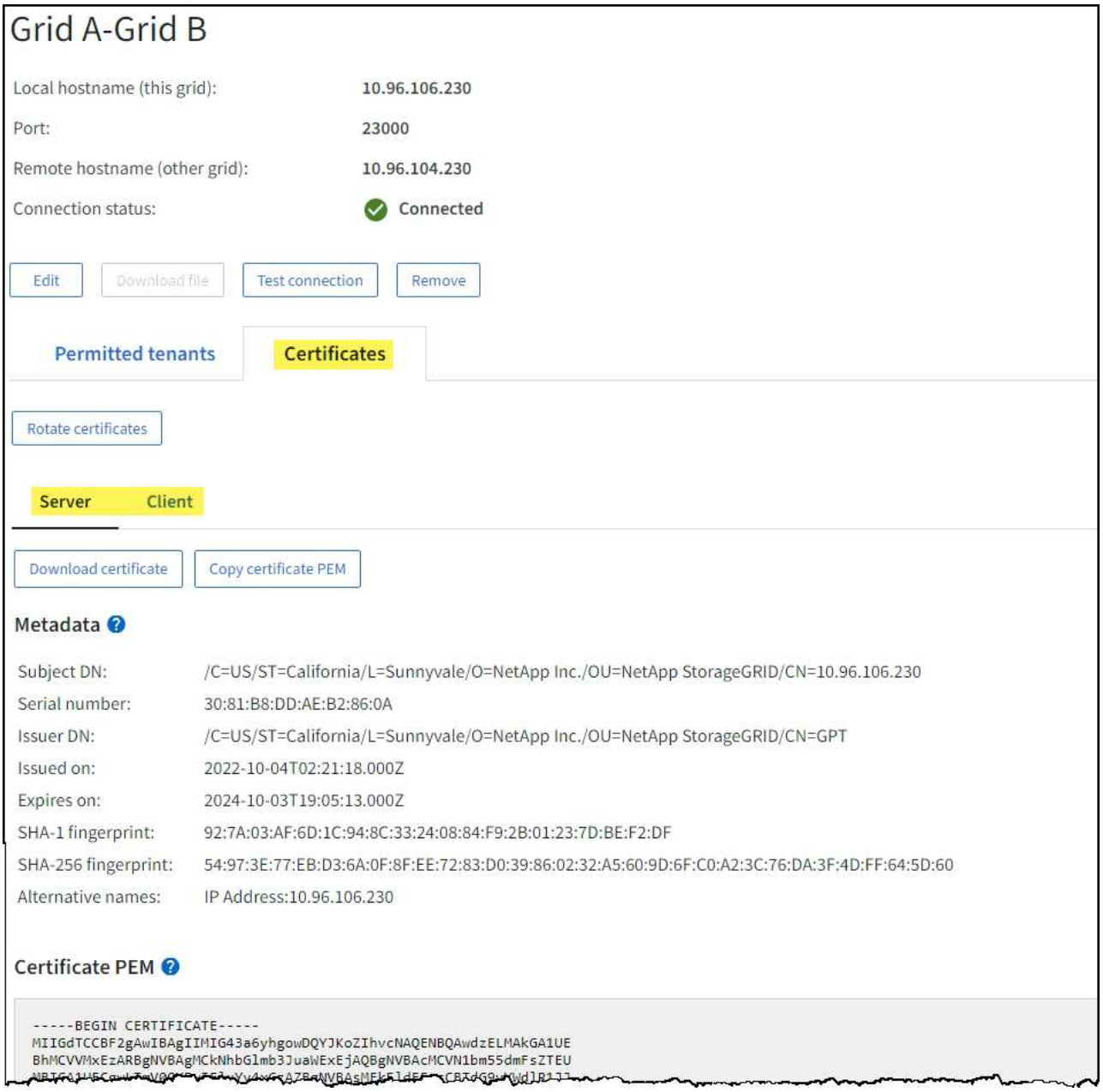
   - "허용된 각 테넌트의 세부 정보 페이지를 봅니다"..
   - "테넌트의 권한을 제거합니다" 연결을 사용합니다.
   - 교차 그리드 복제 오류를 확인하고 마지막 오류를 지웁니다. 을 "그리드 통합 오류 문제 해결"참조하십시오.



3. 특정 연결을 볼 때 이 연결에 대한 시스템 생성 서버 및 클라이언트 인증서를 보려면 * 인증서 * 탭을 선택합니다.

   이 탭에서 다음을 수행할 수 있습니다.

   - "연결 인증서를 회전합니다"..
   - 연결된 인증서를 보거나 다운로드하거나 인증서 PEM을 복사하려면 * 서버 * 또는 * 클라이언트 * 를 선택합니다.



교차 그리드 복제 메트릭을 검토합니다

Grafana의 Cross-Grid Replication 대시보드를 사용하여 그리드의 교차 그리드 복제 작업에 대한 Prometheus 메트릭을 볼 수 있습니다.

단계

1. Grid Manager에서 * 지원 * > * 도구 * > * 메트릭 * 을 선택합니다.

> 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 "일반적으로 사용되는 Prometheus 메트릭입니다"참조하십시오.

2. 페이지의 Grafana 섹션에서 * Cross Grid Replication * 을 선택합니다.

   자세한 지침은 을 참조하십시오"지원 메트릭을 검토합니다".

3. 복제에 실패한 개체의 복제를 다시 시도하려면 을 참조하십시오"실패한 복제 작업을 식별하고 다시 시도하십시오".

알림을 관리합니다

알림을 관리합니다

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

알림은 알림 규칙 조건이 true로 평가될 때 특정 심각도 수준에서 트리거됩니다. 경고가 트리거되면 다음 작업이 수행됩니다.

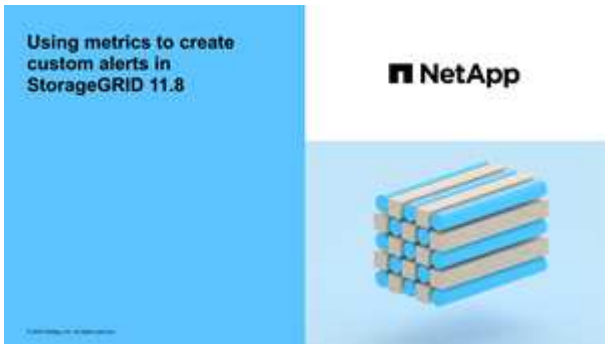
- 그리드 관리자의 대시보드에 경고 심각도 아이콘이 표시되고 현재 경고의 수가 증가합니다.
- 이 알림은 * nodes * 요약 페이지와 * nodes * > **node* * > * Overview * 탭에 표시됩니다.
- SMTP 서버를 구성하고 수신자에 대한 이메일 주소를 제공한 경우 이메일 알림이 전송됩니다.
- StorageGRID SNMP 에이전트를 구성한 경우 SNMP(Simple Network Management Protocol) 알림이 전송됩니다.

사용자 지정 알림을 생성하고, 알림을 편집 또는 비활성화하고, 경고 알림을 관리할 수 있습니다.

자세한 내용:

- 비디오 검토: "비디오: 경고 개요"

- 비디오 검토: "비디오: 사용자 지정 경고"



- 를 "경고 참조"참조하십시오.

경고 규칙은 트리거하는 조건을 "특정 경고"정의합니다. 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.

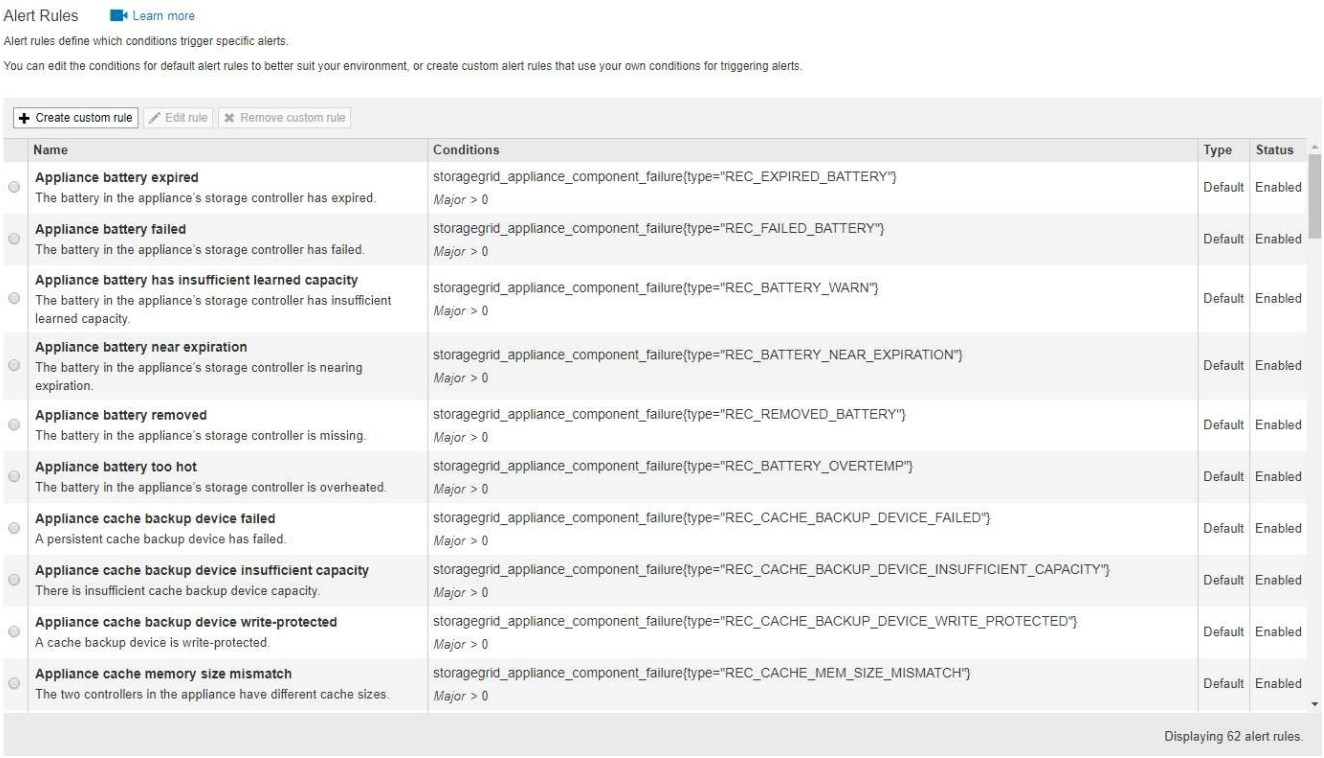
시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "알림 또는 루트 액세스 권한을 관리합니다"있습니다.
- 비디오를 시청한 경우(선택 사항): "비디오: 경고 개요"

단계

1. 알림 * > * 규칙 * 을 선택합니다.

   경고 규칙 페이지가 나타납니다.



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. • * Critical *: StorageGRID 노드 또는 서비스의 정상 작동을 중지한 비정상 상태가 존재함. 기본 문제를 즉시 해결해야 합니다. 문제가 해결되지 않으면 서비스가 중단되거나 데이터가 손실될 수 있습니다. • *Major*: 현재 작업에 영향을 미치거나 중요 경고에 대한 임계값에 접근하는 비정상적인 상태가 존재합니다. StorageGRID 노드나 서비스의 정상 작동을 비정상적인 상태로 중지하지 않도록 주요 경고를 조사하고 모든 기본 문제를 해결해야 합니다. • *Minor*: 시스템이 정상적으로 작동하고 있지만, 시스템이 계속 작동할 경우 시스템 작동 능력에 영향을 줄 수 있는 비정상적인 상태가 있습니다. 보다 심각한 문제를 초래하지 않도록 자체적으로 명확하지 않은 사소한 경고를 모니터링하고 해결해야 합니다.

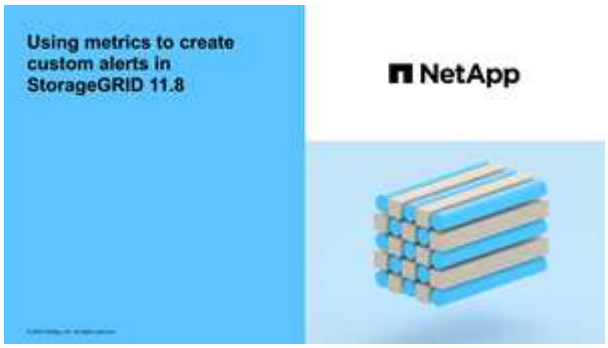
열 머리글	설명
유형	알림 규칙의 유형: • * 기본값 *: 시스템과 함께 제공되는 경고 규칙입니다. 기본 알림 규칙을 비활성화하거나 기본 알림 규칙의 조건 및 기간을 편집할 수 있습니다. 기본 경고 규칙을 제거할 수 없습니다. • * 기본값**: 편집된 조건 또는 기간이 포함된 기본 경고 규칙입니다. 필요에 따라 수정된 조건을 원래 기본값으로 쉽게 되돌릴 수 있습니다. • * 사용자 정의 *: 사용자가 만든 알림 규칙입니다. 사용자 지정 경고 규칙을 비활성화, 편집 및 제거할 수 있습니다.
상태	이 경고 규칙의 현재 활성화 또는 비활성화 여부를 나타냅니다. 비활성화된 알림 규칙의 조건은 평가되지 않으므로 경고가 트리거되지 않습니다.

사용자 지정 알림 규칙을 생성합니다

사용자 지정 알림 규칙을 만들어 알림을 트리거할 자체 조건을 정의할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "알림 또는 루트 액세스 권한을 관리합니다"있습니다.
- 에 대해 잘 알고 "일반적으로 사용되는 Prometheus 메트릭입니다"있습니다.
- 을 이해했습니다. "Prometheus 쿼리의 구문"
- 선택적으로 비디오를 시청했습니다 "비디오: 사용자 지정 경고".



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 식을 테스트할 때 "성공" 응답은 빈 응답 본문(트리거되지 않음)일 수 있습니다. 알림이 실제로 트리거되었는지 확인하려면 임계값을 현재 참인 것으로 예상되는 값으로 일시적으로 설정할 수 있습니다.

  예를 들어 식을 테스트하려면 `node_memory_MemTotal_bytes < 24000000000` 먼저 를 `node_memory_MemTotal_bytes >= 0` 실행하고 예상 결과를 가져왔는지 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.

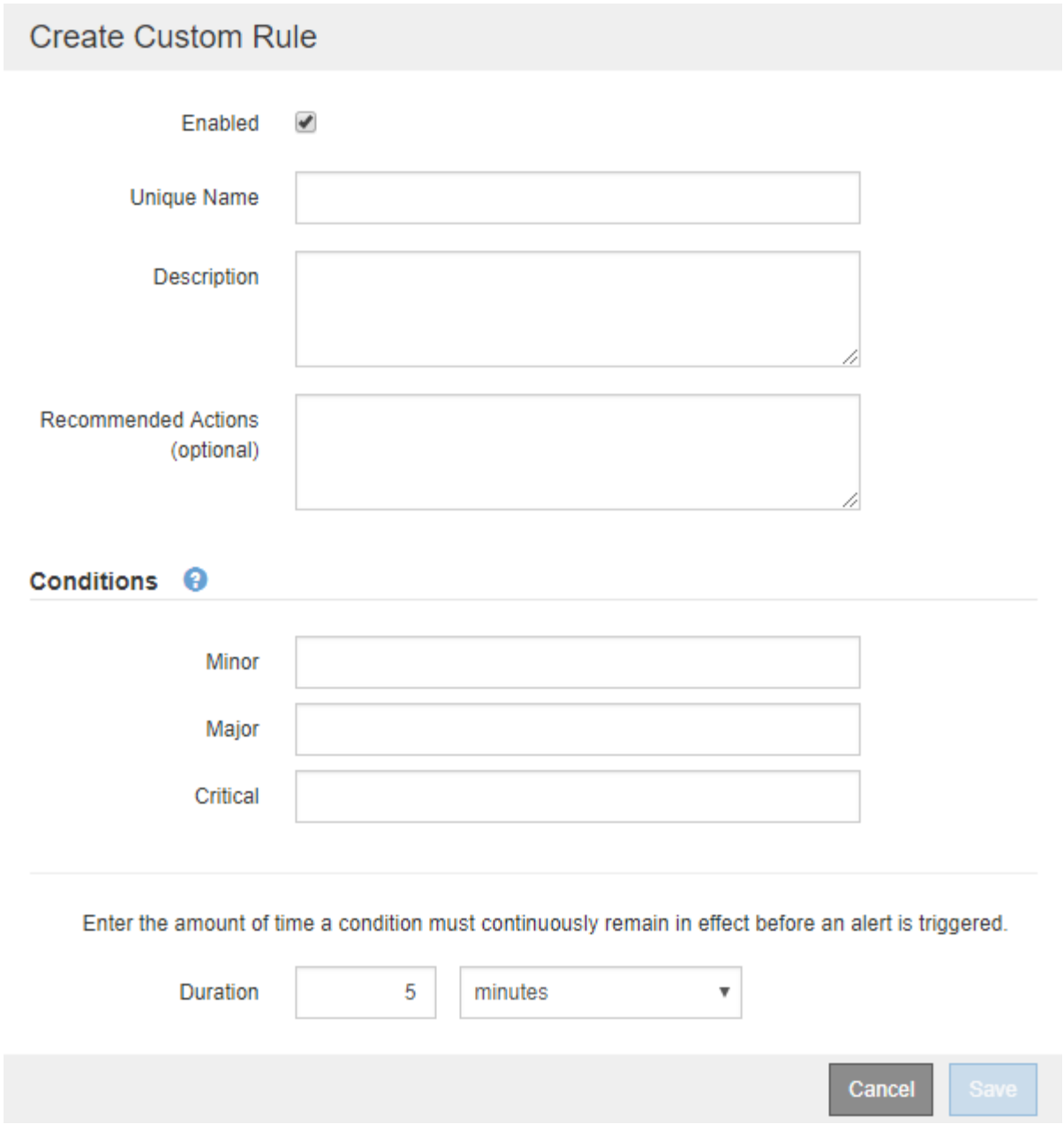
단계

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 확인하려면 * Enabled * 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.
설명	발생한 문제에 대한 설명입니다. 설명은 경고 페이지와 이메일 알림에 표시되는 경고 메시지입니다. 알림 규칙에 대한 설명은 1자에서 128자 사이여야 합니다.

필드에 입력합니다	설명
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 보고 Prometheus 식을 테스트하려면 도움말 아이콘을 선택하고 그리드 관리 API의 메트릭 섹션으로 연결되는 링크를 따르십시오.

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "알림 또는 루트 액세스 권한을 관리합니다"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.

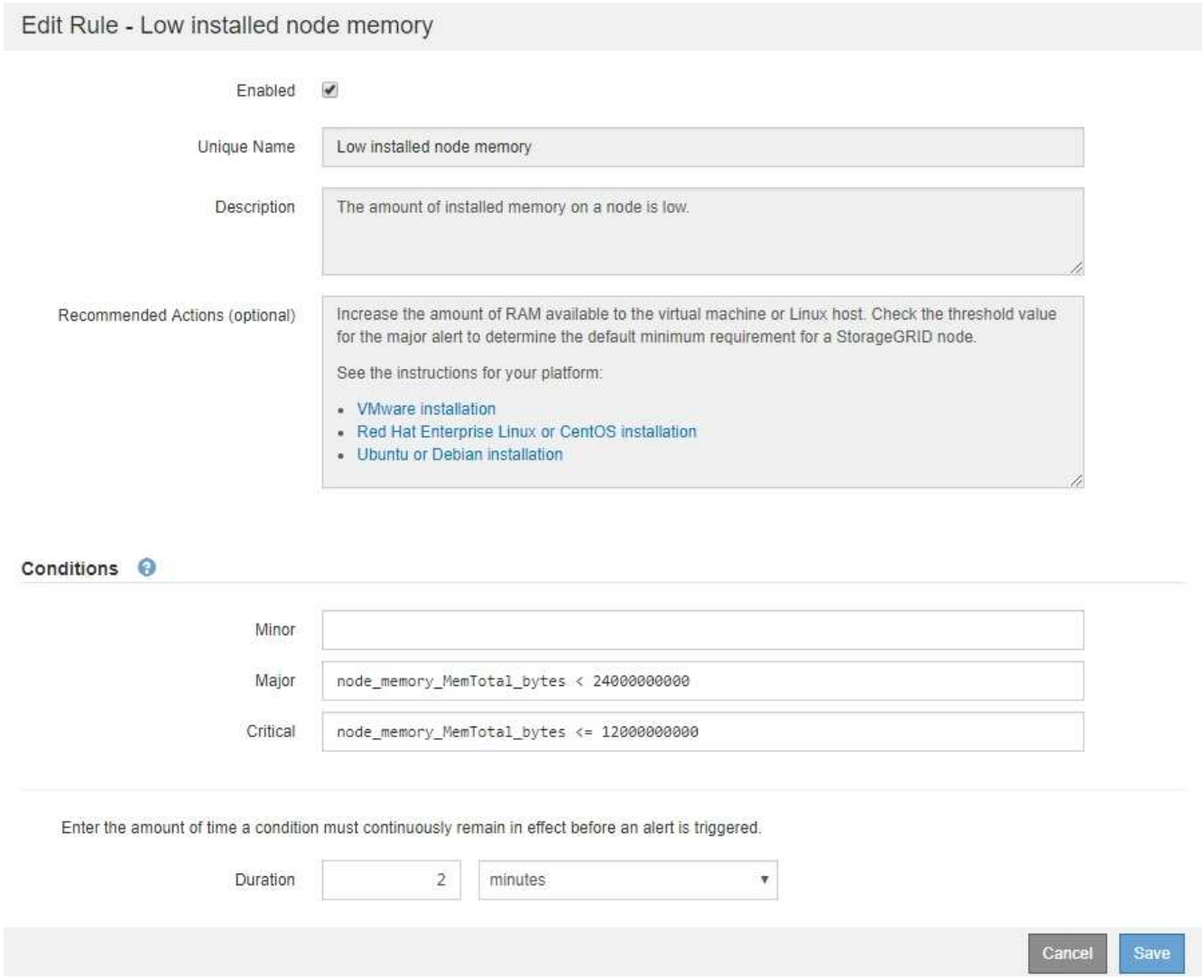
단계

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 확인하려면 * Enabled * 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.

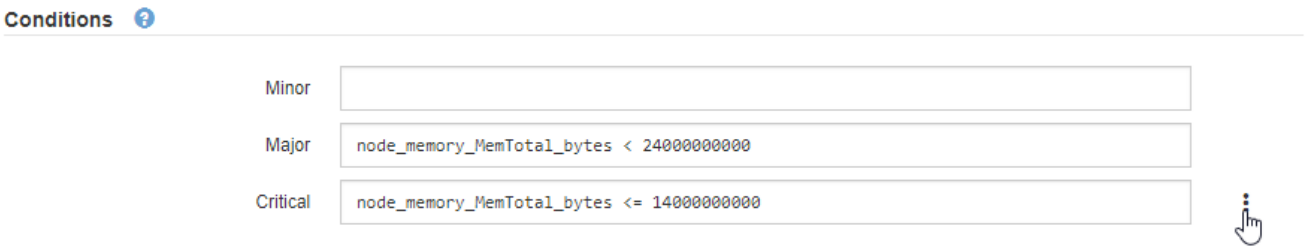
5. 사용자 지정 알림 규칙의 경우 필요에 따라 다음 정보를 업데이트합니다.

   기본 경고 규칙에 대한 이 정보는 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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "알림 또는 루트 액세스 권한을 관리합니다"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 확인하려면 * Enabled * 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 경고 규칙을 제거합니다

사용자 지정 알림 규칙을 더 이상 사용하지 않으려는 경우 제거할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"

- 이 "알림 또는 루트 액세스 권한을 관리합니다"있습니다.

단계

1. 알림 * > * 규칙 * 을 선택합니다.

   경고 규칙 페이지가 나타납니다.

2. 제거할 사용자 지정 알림 규칙의 라디오 버튼을 선택합니다.

   기본 경고 규칙을 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 "SNMP 모니터링을 사용합니다"참조하십시오.

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 "알림 메시지를 해제합니다"참조하십시오.

StorageGRID 구축에 여러 관리자 노드가 포함된 경우 기본 관리자 노드가 경고 알림, AutoSupport 패키지, SNMP 트랩 및 알림을 보내는 기본 보낸 사람이 됩니다. 기본 관리 노드를 사용할 수 없게 되면 다른 관리 노드에서 알림을 임시로 보냅니다. 을 "관리 노드란 무엇입니까?"참조하십시오.

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "알림 또는 루트 액세스 권한을 관리합니다"있습니다.

이 작업에 대해

경고 알림에 사용되는 이메일 설정은 AutoSupport 패키지에 사용되지 않습니다. 그러나 모든 알림에 동일한 이메일 서버를 사용할 수 있습니다.

StorageGRID 구축에 여러 관리자 노드가 포함된 경우 기본 관리자 노드가 경고 알림, AutoSupport 패키지, SNMP 트랩 및 알림을 보내는 기본 보낸 사람이 됩니다. 기본 관리 노드를 사용할 수 없게 되면 다른 관리 노드에서 알림을 임시로 보냅니다. 을 "관리 노드란 무엇입니까?"참조하십시오.

단계

1. 알림 * > * 이메일 설정 * 을 선택합니다.

   이메일 설정 페이지가 나타납니다.

2. 이메일 알림 활성화 * 확인란을 선택하여 알림이 구성된 임계값에 도달할 때 알림 이메일을 보내도록 지정합니다.

   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 다음과 같습니다. `storagegrid-alerts@example.com`

   b. 받는 사람 섹션에서 경고가 발생할 때 전자 메일을 받아야 하는 각 전자 메일 목록의 전자 메일 주소를 입력합니다.

      수신자를 추가하려면 더하기 아이콘을 선택합니다.

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.

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 대해 전송되지 않습니다.
중요 전용	경고 규칙에 대한 위험 조건이 충족된 경우에만 이메일 알림이 전송됩니다. 경미하거나 중요한 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 e-메일을 보내는 AutoSupport 패키지 테스트와 대조적입니다.

8. 저장 * 을 선택합니다.

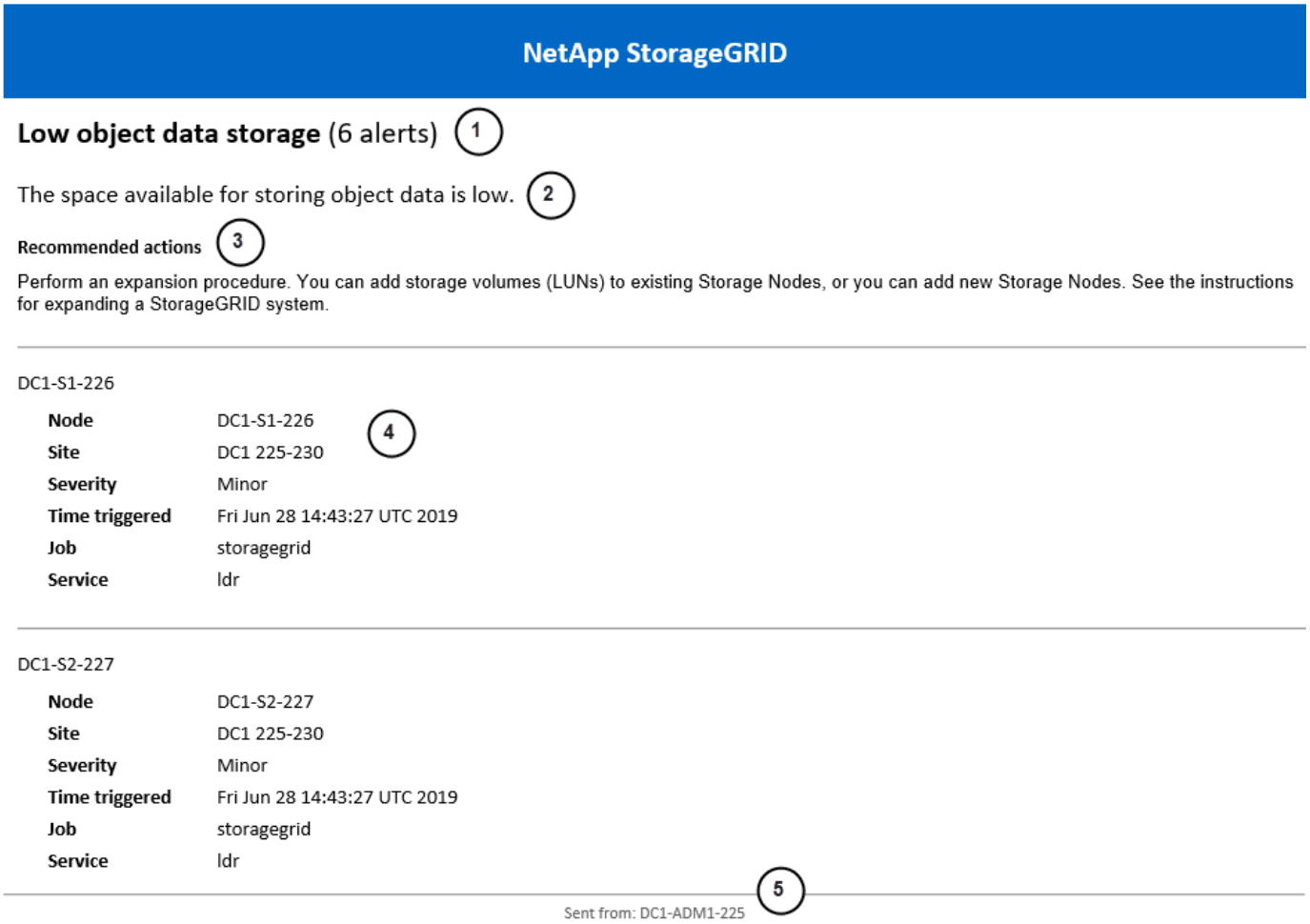
   테스트 이메일을 전송해도 설정이 저장되지 않습니다. 저장 * 을 선택해야 합니다.

   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 "알림 메시지를 해제합니다"참조하십시오.

이메일 알림에는 다음 정보가 포함됩니다.



속성 표시기	설명
1	알림의 이름, 이 알림의 활성 인스턴스 수 순으로 표시됩니다.
2	알림에 대한 설명입니다.

속성 표시기	설명
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. 경고 A는 노드 1에서 08:00에 트리거됩니다. 알림이 전송되지 않습니다. 2. 경고 A는 노드 2에서 08:01에 트리거됩니다. 알림이 전송되지 않습니다. 3. 08:02에 알림의 두 인스턴스를 모두 보고하도록 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. 경고 A는 노드 1에서 08:00에 트리거됩니다. 통지는 08:02에 전송됩니다. 2. 경고 A는 노드 2에서 08:05에 트리거됩니다. 두 번째 통지는 08:15(10분 후)에 전송됩니다. 두 노드가 모두 보고됩니다.

동작	예
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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "알림 또는 루트 액세스 권한을 관리합니다"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 "로그 파일 및 시스템 데이터를 수집합니다"참조하십시오.

알림 메시지를 해제합니다

선택적으로, 알림 알림을 일시적으로 표시하지 않도록 Silence를 구성할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "알림 또는 루트 액세스 권한을 관리합니다"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.

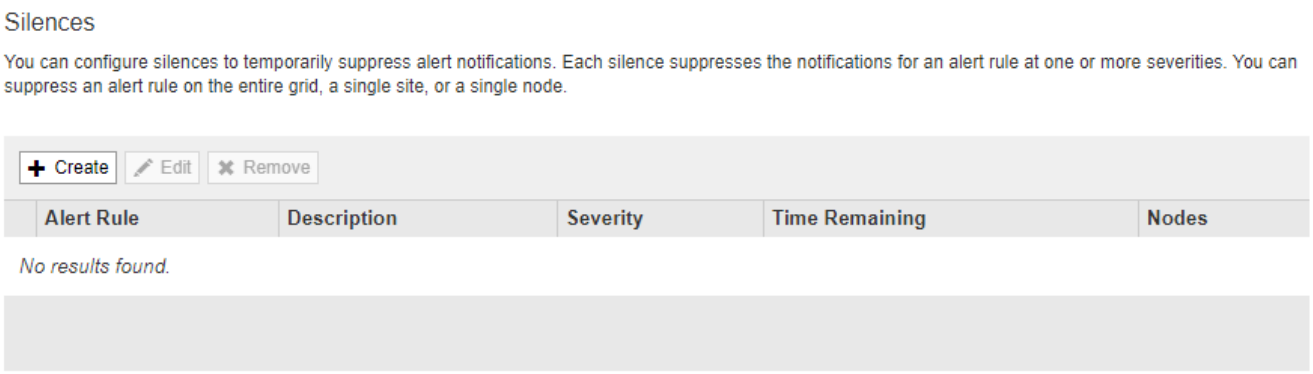
SNMP 에이전트를 사용하도록 설정한 경우, 이 옵션을 해제해도 SNMP 트랩이 억제되고 에 알립니다.

> 경고 규칙을 해제할 때는 주의하십시오. 경고를 음소거하면 중요한 작업이 완료되지 못하게 될 때까지 기본 문제를 감지하지 못할 수 있습니다.

단계

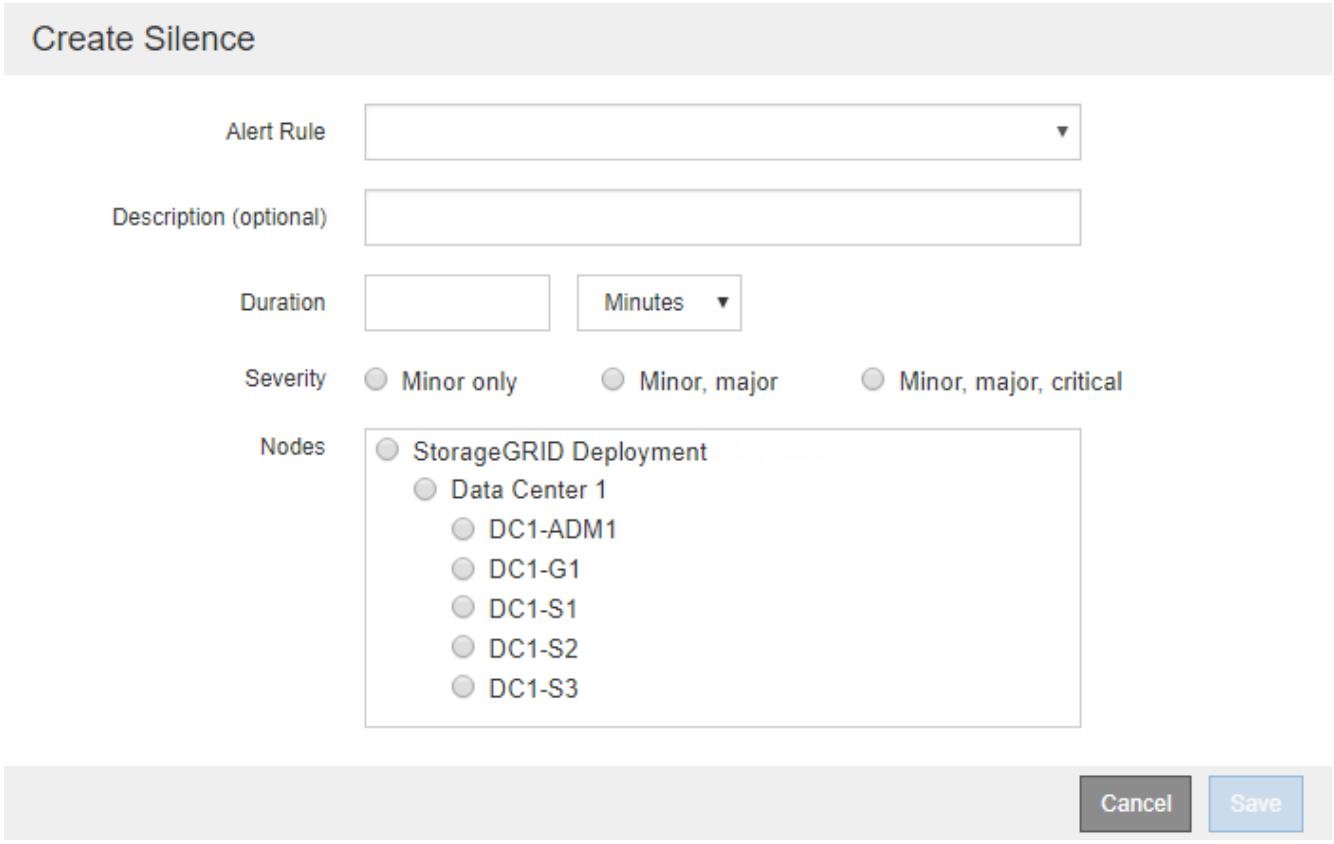
1. alerts * > * silences * 를 선택합니다.

   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.
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.

필드에 입력합니다	설명
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"

경고 참조

이 참조에는 Grid Manager에 나타나는 기본 경고가 나열됩니다. 권장 조치는 수신하는 경고 메시지에 있습니다.

필요에 따라 시스템 관리 방식에 맞게 사용자 지정 경고 규칙을 만들 수 있습니다.

일부 기본 알림은 을 "Prometheus 측정 지표"사용합니다.

경고 이름입니다	설명
어플라이언스 배터리가 만료되었습니다	제품의 저장소 컨트롤러 배터리가 만료되었습니다.
어플라이언스 배터리 고장	제품의 저장소 컨트롤러 에 있는 배터리가 실패했습니다.
어플라이언스 배터리가 학습된 용량이 부족합니다	제품의 저장 장치 컨트롤러의 배터리가 학습된 용량이 부족합니다.
어플라이언스 배터리 수명이 거의 다 되었습니다	어플라이언스 저장소 컨트롤러의 배터리 수명이 거의 다했습니다.
제품 배터리가 제거되었습니다	제품의 저장 컨트롤러에 배터리가 없습니다.
제품 배터리가 너무 뜨겁습니다	제품 보관 컨트롤러의 배터리가 과열되었습니다.
어플라이언스 BMC 통신 오류입니다	베이스보드 관리 컨트롤러(BMC)와의 통신이 끊어졌습니다.
어플라이언스 부팅 장치 오류가 감지되었습니다	어플라이언스의 부팅 장치에서 문제가 감지되었습니다.
어플라이언스 캐시 백업 디바이스에 장애가 발생했습니다	영구 캐시 백업 디바이스가 실패했습니다.
어플라이언스 캐시 백업 디바이스의 용량이 부족합니다	캐시 백업 디바이스 용량이 부족합니다.
어플라이언스 캐시 백업 디바이스 쓰기 방지	캐시 백업 디바이스가 쓰기 금지되어 있습니다.
어플라이언스 캐시 메모리 크기가 일치하지 않습니다	어플라이언스의 두 컨트롤러는 캐시 크기가 다릅니다.
어플라이언스 CMOS 배터리 오류입니다	어플라이언스의 CMOS 배터리에서 문제가 감지되었습니다.
어플라이언스의 컴퓨팅 컨트롤러 섀시 온도가 너무 높습니다	StorageGRID 어플라이언스의 컴퓨팅 컨트롤러 온도가 공칭 임계값을 초과했습니다.
어플라이언스의 컴퓨팅 컨트롤러 CPU 온도가 너무 높습니다	StorageGRID 어플라이언스의 컴퓨팅 컨트롤러에 있는 CPU 온도가 공칭 임계값을 초과했습니다.

경고 이름입니다	설명
어플라이언스 컴퓨팅 컨트롤러에 주의가 필요합니다	StorageGRID 어플라이언스의 컴퓨팅 컨트롤러에서 하드웨어 장애가 감지되었습니다.
어플라이언스 컴퓨팅 컨트롤러 전원 공급 장치 A에 문제가 있습니다	컴퓨팅 컨트롤러의 전원 공급 장치 A에 문제가 있습니다.
어플라이언스 컴퓨팅 컨트롤러 전원 공급 장치 B에 문제가 있습니다	컴퓨팅 컨트롤러의 전원 공급 장치 B에 문제가 있습니다.
어플라이언스 컴퓨팅 하드웨어 모니터 서비스가 중단되었습니다	스토리지 하드웨어 상태를 모니터링하는 서비스가 중단되었습니다.
어플라이언스 DAS 드라이브가 일일 데이터 쓰기 제한을 초과합니다	매일 과도한 양의 데이터가 드라이브에 기록되고 있으므로 보증이 무효화될 수 있습니다.
어플라이언스 DAS 드라이브 장애가 감지되었습니다	어플라이언스의 DAS(직접 연결 스토리지) 드라이브에서 문제가 감지되었습니다.
어플라이언스 DAS 드라이브 로케이터 표시등이 켜집니다	어플라이언스 스토리지 노드에서 하나 이상의 DAS(직접 연결 스토리지) 드라이브에 대한 드라이브 로케이터 표시등이 켜져 있습니다.
어플라이언스 DAS 드라이브 재구축	DAS(직접 연결 스토리지) 드라이브를 재구축하고 있습니다. 이는 최근에 교체 또는 제거/재삽입된 경우에 발생합니다.
어플라이언스 팬 장애가 감지되었습니다	제품의 팬 장치에 문제가 감지되었습니다.
어플라이언스 Fibre Channel 장애가 감지되었습니다	어플라이언스 스토리지 컨트롤러와 컴퓨팅 컨트롤러 간에 파이버 채널 링크 문제가 감지되었습니다
어플라이언스 Fibre Channel HBA 포트 오류입니다	Fibre Channel HBA 포트에 장애가 발생했거나 장애가 발생했습니다.
어플라이언스 플래시 캐시 드라이브가 최적이 아닙니다	SSD 캐시에 사용되는 드라이브가 최적화되지 않았습니다.
어플라이언스 상호 연결/배터리 캐니스터가 제거되었습니다	상호 연결/배터리 캐니스터가 없습니다.
어플라이언스 LACP 포트가 누락되었습니다	StorageGRID 어플라이언스의 포트가 LACP 결합에 사용되고 있지 않습니다.
어플라이언스 NIC 장애가 감지되었습니다	어플라이언스의 네트워크 인터페이스 카드(NIC)에 문제가 감지되었습니다.

경고 이름입니다	설명
어플라이언스의 전체 전원 공급 장치 성능이 저하되었습니다	StorageGRID 제품의 전원이 권장 작동 전압을 벗어나 있습니다.
어플라이언스 SSD 위험 경고	어플라이언스 SSD가 심각한 경고를 보고합니다.
어플라이언스 스토리지 컨트롤러 A에 장애가 발생했습니다	StorageGRID 어플라이언스의 스토리지 컨트롤러 A에 장애가 발생했습니다.
어플라이언스 스토리지 컨트롤러 B에 장애가 발생했습니다	StorageGRID 어플라이언스의 스토리지 컨트롤러 B에 장애가 발생했습니다.
어플라이언스 스토리지 컨트롤러 드라이브 오류입니다	StorageGRID 어플라이언스에 있는 하나 이상의 드라이브가 실패했거나 최적이 아닙니다.
어플라이언스 스토리지 컨트롤러 하드웨어 문제입니다	SANtricity 소프트웨어가 StorageGRID 어플라이언스의 구성 요소에 대해 "주의 필요"를 보고하고 있습니다.
어플라이언스 스토리지 컨트롤러 전원 공급 장치 A 고장	StorageGRID 제품의 전원 공급 장치 A가 권장 작동 전압을 벗어나고 있습니다.
어플라이언스 스토리지 컨트롤러 전원 공급 장치 B 오류입니다	StorageGRID 제품의 전원 공급 장치 B가 권장 작동 전압을 벗어나 있습니다.
어플라이언스 스토리지 하드웨어 모니터 서비스가 중단되었습니다	스토리지 하드웨어 상태를 모니터링하는 서비스가 중단되었습니다.
어플라이언스 스토리지 쉘프 성능이 저하되었습니다	스토리지 어플라이언스의 스토리지 쉘프에 있는 구성 요소 중 하나의 상태가 성능 저하입니다.
제품 온도가 초과되었습니다	제품 보관 컨트롤러의 공칭 또는 최대 온도를 초과했습니다.
제품 온도 센서가 제거되었습니다	온도 센서가 제거되었습니다.
어플라이언스 UEFI 보안 부팅 오류	어플라이언스가 안전하게 부팅되지 않았습니다.
디스크 I/O가 매우 느립니다	매우 느린 디스크 I/O는 그리드 성능에 영향을 줄 수 있습니다.
스토리지 어플라이언스 팬 장애가 감지되었습니다	스토리지 컨트롤러의 팬 장치에서 어플라이언스에 문제가 감지되었습니다.
스토리지 어플라이언스 스토리지 연결이 저하되었습니다	컴퓨팅 컨트롤러와 스토리지 컨트롤러 사이에 하나 이상의 연결에 문제가 있습니다.

경고 이름입니다	설명
스토리지 디바이스를 액세스할 수 없습니다	스토리지 디바이스를 액세스할 수 없습니다.

감사 및 **syslog** 경고

경고 이름입니다	설명
감사 로그가 인메모리 대기열에 추가되고 있습니다	노드가 로컬 syslog 서버로 로그를 전송할 수 없고 인메모리 큐가 가득 찬 경우
외부 syslog 서버 전달 오류입니다	노드가 외부 syslog 서버로 로그를 전달할 수 없습니다.
대규모 감사 대기열	감사 메시지의 디스크 대기열이 가득 찼습니다. 이 상태가 해결되지 않으면 S3 또는 Swift 작업이 실패할 수 있습니다.
로그가 디스크 대기열에 추가되고 있습니다	노드가 외부 syslog 서버로 로그를 전달할 수 없고 디스크 내 대기열이 가득 찬 경우

버킷 경고

경고 이름입니다	설명
FabricPool 버킷은 버킷 정합성 설정을 지원하지 않습니다	FabricPool 버킷은 지원되지 않는 사용 가능 또는 강력한 사이트 정합성 보장 수준을 사용합니다.
FabricPool 버킷에 지원되지 않는 버전 관리 설정이 있습니다	FabricPool 버킷에는 버전 관리 또는 S3 오브젝트 잠금이 설정되어 있지만 이는 지원되지 않습니다.

Cassandra 알림

경고 이름입니다	설명
Cassandra 자동 콤팩터 오류입니다	Cassandra 자동 콤팩터에 오류가 발생했습니다.
Cassandra 자동 콤팩터 메트릭이 최신 상태가 아닙니다	Cassandra 자동 콤팩터를 설명하는 메트릭이 최신 상태가 아닙니다.
Cassandra 통신 오류입니다	Cassandra 서비스를 실행하는 노드는 서로 통신하는 데 문제가 있습니다.
Cassandra 압축 과부하입니다	Cassandra 컴팩션 프로세스가 과부하 상태입니다.
Cassandra 크기 초과 쓰기 오류입니다	내부 StorageGRID 프로세스에서 Cassandra에 대해 너무 큰 쓰기 요청을 전송했습니다.

경고 이름입니다	설명
Cassandra 복구 메트릭이 최신 상태가 아닙니다	Cassandra 복구 작업을 설명하는 메트릭이 최신 상태가 아닙니다.
Cassandra 복구 진행률이 느립니다	Cassandra 데이터베이스 복구 진행률이 느립니다.
Cassandra 복구 서비스를 사용할 수 없습니다	Cassandra 복구 서비스를 사용할 수 없습니다.
Cassandra 테이블 손상	Cassandra가 테이블 손상을 감지했습니다. 테이블 손상이 감지되면 Cassandra가 자동으로 다시 시작됩니다.

Cloud Storage Pool 알림

경고 이름입니다	설명
클라우드 스토리지 풀 연결 오류입니다	클라우드 스토리지 풀의 상태 점검에서 하나 이상의 새 오류가 감지되었습니다.
IAM 역할 모든 위치에서 최종 엔티티 인증 만료	IAM 역할 모든 위치에서 최종 엔티티 인증서가 곧 만료됩니다.

교차 그리드 복제 경고

경고 이름입니다	설명
크로스 그리드 복제 영구 오류입니다	그리드 간 복제 오류가 발생하여 사용자 개입이 필요합니다.
교차 그리드 복제 리소스를 사용할 수 없습니다	리소스를 사용할 수 없기 때문에 교차 그리드 복제 요청이 보류 중입니다.

DHCP 경고

경고 이름입니다	설명
DHCP 리스가 만료되었습니다	네트워크 인터페이스의 DHCP 리스가 만료되었습니다.
DHCP 임대가 곧 만료됩니다	네트워크 인터페이스의 DHCP 임대가 곧 만료됩니다.
DHCP 서버를 사용할 수 없습니다	DHCP 서버를 사용할 수 없습니다.

디버그 및 추적 경고

경고 이름입니다	설명
디버그 성능 영향	디버그 모드가 활성화되면 시스템 성능에 부정적인 영향을 줄 수 있습니다.
추적 구성이 활성화되었습니다	추적 구성이 활성화되면 시스템 성능에 부정적인 영향을 줄 수 있습니다.

이메일 및 **AutoSupport** 경고

경고 이름입니다	설명
AutoSupport 메시지를 보내지 못했습니다	가장 최근의 AutoSupport 메시지를 보내지 못했습니다.
도메인 이름을 확인하지 못했습니다	StorageGRID 노드에서 도메인 이름을 확인할 수 없습니다.
이메일 알림 실패	알림에 대한 이메일 알림을 보낼 수 없습니다.
SNMP 알림 오류	트랩 대상에 SNMP 알림 알림을 보내는 중 오류가 발생했습니다.
SSH 또는 콘솔 로그인이 감지되었습니다	지난 24시간 동안 사용자가 웹 콘솔 또는 SSH로 로그인했습니다.

EC(삭제 코딩**)** 경고

경고 이름입니다	설명
EC 재조정 실패	EC 재조정 절차가 실패했거나 중지되었습니다.
EC 복구 실패	EC 데이터에 대한 복구 작업이 실패했거나 중지되었습니다.
EC 복구가 중단되었습니다	EC 데이터에 대한 복구 작업이 중단되었습니다.
삭제 코딩 조각 검증 오류입니다	삭제 코딩 조각은 더 이상 검증할 수 없습니다. 손상된 조각은 복구되지 않을 수 있습니다.

인증서 경고 만료

경고 이름입니다	설명
관리 프록시 CA 인증서 만료	관리 프록시 서버 CA 번들에 있는 하나 이상의 인증서가 곧 만료됩니다.
클라이언트 인증서 만료	하나 이상의 클라이언트 인증서가 곧 만료됩니다.
S3 및 Swift에 대한 글로벌 서버 인증서 만료	S3 및 Swift에 대한 글로벌 서버 인증서가 곧 만료됩니다.

경고 이름입니다	설명
로드 밸런서 끝점 인증서 만료	하나 이상의 로드 밸런서 끝점 인증서가 곧 만료됩니다.
관리 인터페이스에 대한 서버 인증서 만료	관리 인터페이스에 사용되는 서버 인증서가 곧 만료됩니다.
외부 syslog CA 인증서 만료	외부 syslog 서버 인증서에 서명하는 데 사용되는 CA(인증 기관) 인증서가 곧 만료됩니다.
외부 syslog 클라이언트 인증서 만료	외부 syslog 서버에 대한 클라이언트 인증서가 곧 만료됩니다.
외부 syslog 서버 인증서 만료	외부 syslog 서버가 제공하는 서버 인증서가 곧 만료됩니다.

그리드 네트워크 경고

경고 이름입니다	설명
그리드 네트워크 MTU가 일치하지 않습니다	그리드 네트워크 인터페이스(eth0)에 대한 MTU 설정은 그리드의 노드 간에 크게 다릅니다.

그리드 페더레이션 알림

경고 이름입니다	설명
그리드 페더레이션 인증서의 만료	하나 이상의 그리드 페더레이션 인증서가 곧 만료됩니다.
그리드 페더레이션 연결에 실패했습니다	로컬 그리드와 원격 그리드 간의 그리드 페더레이션 연결이 작동하지 않습니다.

사용량이 높거나 지연 시간이 긴 알림

경고 이름입니다	설명
높은 Java 힙 사용	Java 힙 공간의 높은 비율이 사용되고 있습니다.
메타데이터 쿼리를 위한 높은 지연 시간	Cassandra 메타데이터 쿼리의 평균 시간이 너무 깁니다.

ID 페더레이션 알림

경고 이름입니다	설명
ID 페더레이션 동기화 실패	ID 소스에서 페더레이션 그룹과 사용자를 동기화할 수 없습니다.

경고 이름입니다	설명
테넌트의 ID 페더레이션 동기화 실패	테넌트가 구성한 ID 소스에서 페더레이션 그룹과 사용자를 동기화할 수 없습니다.

ILM(정보 수명 주기 관리**)** 경고

경고 이름입니다	설명
ILM 배치를 달성 할 수 없습니다	ILM 규칙의 배치 지침은 특정 개체에 대해 달성할 수 없습니다.
ILM 스캔 속도가 낮습니다	ILM 스캔 속도는 초당 100개 미만으로 설정됩니다.

KMS(키 관리 서버**)** 경고

경고 이름입니다	설명
KMS CA 인증서 만료	KMS(키 관리 서버) 인증서에 서명하는 데 사용되는 CA(인증 기관) 인증서가 곧 만료됩니다.
KMS 클라이언트 인증서 만료	키 관리 서버의 클라이언트 인증서가 곧 만료됩니다
KMS 구성을 로드하지 못했습니다	키 관리 서버에 대한 구성이 있지만 로드하지 못했습니다.
KMS 연결 오류입니다	어플라이언스 노드가 사이트의 키 관리 서버에 연결할 수 없습니다.
KMS 암호화 키 이름을 찾을 수 없습니다	구성된 키 관리 서버에 제공된 이름과 일치하는 암호화 키가 없습니다.
KMS 암호화 키 회전이 실패했습니다	모든 어플라이언스 볼륨이 성공적으로 해독되었지만 하나 이상의 볼륨이 최신 키로 회전할 수 없습니다.
KMS가 구성되지 않았습니다	이 사이트에 대한 키 관리 서버가 없습니다.
킬로미터 키가 어플라이언스 볼륨을 해독하지 못했습니다	노드 암호화가 활성화된 어플라이언스에서 하나 이상의 볼륨을 현재 KMS 키로 해독할 수 없습니다.
KMS 서버 인증서 만료	KMS(키 관리 서버)에서 사용하는 서버 인증서가 곧 만료됩니다.
KMS 서버 연결 실패	어플라이언스 노드가 해당 사이트의 키 관리 서버 클러스터에 있는 하나 이상의 서버에 연결할 수 없습니다.

로드 밸런서 경고

경고 이름입니다	설명
상승된 제로 요청 로드 밸런서 연결부	요청을 수행하지 않고 연결이 끊어진 로드 밸런서 끝점에 대한 연결 비율입니다.

로컬 클록 오프셋 경고입니다

경고 이름입니다	설명
로컬 시계 대형 시간 오프셋	로컬 시계와 NTP(네트워크 시간 프로토콜) 시간 사이의 오프셋이 너무 큽니다.

메모리 부족 또는 공간 부족 경고

경고 이름입니다	설명
감사 로그 디스크 용량이 낮습니다	감사 로그에 사용할 수 있는 공간이 부족합니다. 이 상태가 해결되지 않으면 S3 또는 Swift 작업이 실패할 수 있습니다.
사용 가능한 노드 메모리가 부족합니다	노드에서 사용할 수 있는 RAM 용량이 부족합니다.
스토리지 풀의 사용 가능한 공간이 부족합니다	스토리지 노드에 오브젝트 데이터를 저장하는 데 사용할 수 있는 공간이 부족합니다.
설치된 노드 메모리가 부족합니다	노드에 설치된 메모리 양이 부족합니다.
낮은 메타데이터 스토리지	오브젝트 메타데이터를 저장하는 데 사용할 수 있는 공간이 부족합니다.
낮은 메트릭 디스크 용량	메트릭 데이터베이스에 사용할 수 있는 공간이 부족합니다.
오브젝트 데이터 스토리지가 부족합니다	오브젝트 데이터를 저장하는 데 사용할 수 있는 공간이 부족합니다.
읽기 전용 로우 워터마크가 무시됩니다	스토리지 볼륨 소프트 읽기 전용 워터마크 재정의가 스토리지 노드에 대해 최적화된 최소 워터마크보다 작습니다.
루트 디스크 용량이 부족합니다	루트 디스크의 사용 가능한 공간이 부족합니다.
시스템 데이터 용량이 부족합니다	/var/local에 사용할 수 있는 공간이 부족합니다. 이 상태가 해결되지 않으면 S3 또는 Swift 작업이 실패할 수 있습니다.
tmp 디렉토리 여유 공간이 부족합니다	/tmp 디렉토리에 사용 가능한 공간이 부족합니다.

노드 또는 노드 네트워크 경고

경고 이름입니다	설명
관리 네트워크 수신 사용	관리 네트워크의 수신 사용량이 높습니다.
관리 네트워크 전송 사용	관리 네트워크의 전송 사용량이 높습니다.
방화벽 구성 실패	방화벽 구성을 적용하지 못했습니다.
대체 모드의 관리 인터페이스 끝점입니다	모든 관리 인터페이스 엔드포인트가 너무 오래 기본 포트로 돌아가고 있습니다.
노드 네트워크 연결 오류입니다	노드 간에 데이터를 전송하는 동안 오류가 발생했습니다.
노드 네트워크 수신 프레임 오류입니다	노드에서 수신한 네트워크 프레임의 비율이 높은 경우 오류가 발생했습니다.
노드가 NTP 서버와 동기화되지 않았습니다	노드가 NTP(네트워크 시간 프로토콜) 서버와 동기화되지 않습니다.
NTP 서버로 잠겨 있지 않은 노드입니다	노드가 네트워크 시간 프로토콜(NTP) 서버에 잠기지 않았습니다.
비어플라이언스 노드 네트워크가 다운되었습니다	하나 이상의 네트워크 장치가 다운되었거나 연결이 끊어졌습니다.
관리 네트워크에서 서비스 어플라이언스 링크가 다운되었습니다	관리 네트워크(eth1)에 대한 어플라이언스 인터페이스가 다운되거나 연결이 끊겼습니다.
관리 네트워크 포트 1에서 서비스 어플라이언스 링크가 다운되었습니다	어플라이언스의 관리 네트워크 포트 1이 다운되었거나 연결이 해제되었습니다.
클라이언트 네트워크에서 서비스 어플라이언스 링크가 다운되었습니다	클라이언트 네트워크(eth2)에 대한 어플라이언스 인터페이스가 중단되거나 연결이 끊겼습니다.
네트워크 포트 1에서 서비스 어플라이언스 링크가 다운되었습니다	어플라이언스의 네트워크 포트 1가 다운되었거나 연결 해제되었습니다.
네트워크 포트 2에서 서비스 어플라이언스 링크가 다운되었습니다	어플라이언스의 네트워크 포트 2가 다운되었거나 연결 해제되었습니다.
네트워크 포트 3에서 서비스 어플라이언스 링크가 다운되었습니다	어플라이언스의 네트워크 포트 3가 다운되었거나 연결 해제되었습니다.
네트워크 포트 4에서 서비스 어플라이언스 링크가 다운되었습니다	어플라이언스의 네트워크 포트 4가 다운되었거나 연결 해제되었습니다.

경고 이름입니다	설명
관리 네트워크에서 스토리지 어플라이언스 링크가 다운되었습니다	관리 네트워크(eth1)에 대한 어플라이언스 인터페이스가 다운되거나 연결이 끊겼습니다.
관리 네트워크 포트 1에서 스토리지 어플라이언스 링크가 다운되었습니다	어플라이언스의 관리 네트워크 포트 1이 다운되었거나 연결이 해제되었습니다.
클라이언트 네트워크에서 스토리지 어플라이언스 링크가 다운되었습니다	클라이언트 네트워크(eth2)에 대한 어플라이언스 인터페이스가 중단되거나 연결이 끊겼습니다.
네트워크 포트 1에서 스토리지 어플라이언스 링크가 다운되었습니다	어플라이언스의 네트워크 포트 1가 다운되었거나 연결 해제되었습니다.
네트워크 포트 2에서 스토리지 어플라이언스 링크가 다운되었습니다	어플라이언스의 네트워크 포트 2가 다운되었거나 연결 해제되었습니다.
네트워크 포트 3에서 스토리지 어플라이언스 링크가 다운되었습니다	어플라이언스의 네트워크 포트 3가 다운되었거나 연결 해제되었습니다.
네트워크 포트 4에서 스토리지 어플라이언스 링크가 다운되었습니다	어플라이언스의 네트워크 포트 4가 다운되었거나 연결 해제되었습니다.
스토리지 노드가 원하는 스토리지 상태가 아닙니다	내부 오류 또는 볼륨 관련 문제로 인해 스토리지 노드의 LDR 서비스가 원하는 상태로 전환될 수 없습니다
TCP 연결 사용	이 노드의 TCP 연결 수가 추적할 수 있는 최대 수에 근접하고 있습니다.
노드와 통신할 수 없습니다	하나 이상의 서비스가 응답하지 않거나 노드에 연결할 수 없습니다.
예기치 않은 노드 재부팅	지난 24시간 동안 노드가 예기치 않게 재부팅되었습니다.

개체 알림

경고 이름입니다	설명
개체 존재 여부를 확인하지 못했습니다	개체 존재 확인 작업이 실패했습니다.
개체 존재 검사가 중단되었습니다	개체 존재 확인 작업이 중단되었습니다.
객체가 손실되었습니다	그리드에서 하나 이상의 오브젝트가 손실되었습니다.
S3이 개체 크기를 너무 크게 설정합니다	클라이언트가 S3 크기 제한을 초과하는 Put Object 작업을 시도하고 있습니다.

경고 이름입니다	설명
알 수 없는 손상된 개체가 감지되었습니다	복제된 오브젝트로 식별되지 않는 파일이 복제된 오브젝트 스토리지에 있습니다.

플랫폼 서비스 경고

경고 이름입니다	설명
플랫폼 서비스 보류 중인 요청 용량이 부족합니다	대기 중인 플랫폼 서비스 요청 수가 용량에 근접하고 있습니다.
플랫폼 서비스를 사용할 수 없습니다	RSM 서비스가 실행 중이거나 사이트에서 사용 가능한 스토리지 노드가 너무 적습니다.

스토리지 볼륨 경고

경고 이름입니다	설명
스토리지 볼륨에 주의가 필요합니다	스토리지 볼륨이 오프라인 상태이므로 주의가 필요합니다.
스토리지 볼륨을 복원해야 합니다	스토리지 볼륨이 복구되었으며 복원해야 합니다.
스토리지 볼륨이 오프라인 상태입니다	저장소 볼륨이 5분 이상 오프라인 상태입니다.
스토리지 볼륨 다시 마운트가 시도되었습니다	스토리지 볼륨이 오프라인 상태이고 자동 다시 마운트가 트리거되었습니다. 이는 드라이브 문제나 파일 시스템 오류를 나타낼 수 있습니다.
볼륨 복원에서 복제된 데이터 복구를 시작하지 못했습니다	복구된 볼륨에 대해 복제된 데이터 복구를 자동으로 시작할 수 없습니다.

StorageGRID 서비스 경고

경고 이름입니다	설명
백업 구성을 사용하는 Nginx 서비스	nginx 서비스의 구성이 잘못되었습니다. 이제 이전 구성을 사용하고 있습니다.
백업 구성을 사용하는 Nginx-GW 서비스	nginx-GW 서비스의 구성이 유효하지 않습니다. 이제 이전 구성을 사용하고 있습니다.
FIPS를 비활성화하려면 재부팅해야 합니다	보안 정책에는 FIPS 모드가 필요하지 않지만 NetApp 암호화 보안 모듈이 활성화되어 있습니다.
FIPS를 활성화하려면 재부팅해야 합니다	보안 정책에는 FIPS 모드가 필요하지만 NetApp 암호화 보안 모듈이 비활성화되어 있습니다.

경고 이름입니다	설명
백업 구성을 사용하는 SSH 서비스입니다	SSH 서비스 구성이 잘못되었습니다. 이제 이전 구성을 사용하고 있습니다.

테넌트 알림

경고 이름입니다	설명
테넌트 할당량 사용량이 높습니다	할당량 공간의 높은 비율이 사용되고 있습니다. 이 규칙은 너무 많은 알림을 발생시킬 수 있으므로 기본적으로 비활성화되어 있습니다.

일반적으로 사용되는 **Prometheus** 메트릭입니다

기본 알림 규칙의 조건을 더 잘 이해하거나 사용자 지정 알림 규칙의 조건을 구성하려면 일반적으로 사용되는 Prometheus 메트릭의 목록을 참조하십시오.

할 수도 모든 메트릭의 전체 목록을 얻습니다있습니다.

Prometheus 쿼리 구문에 대한 자세한 내용은 을 참조하십시오 "Prometheus 쿼리".

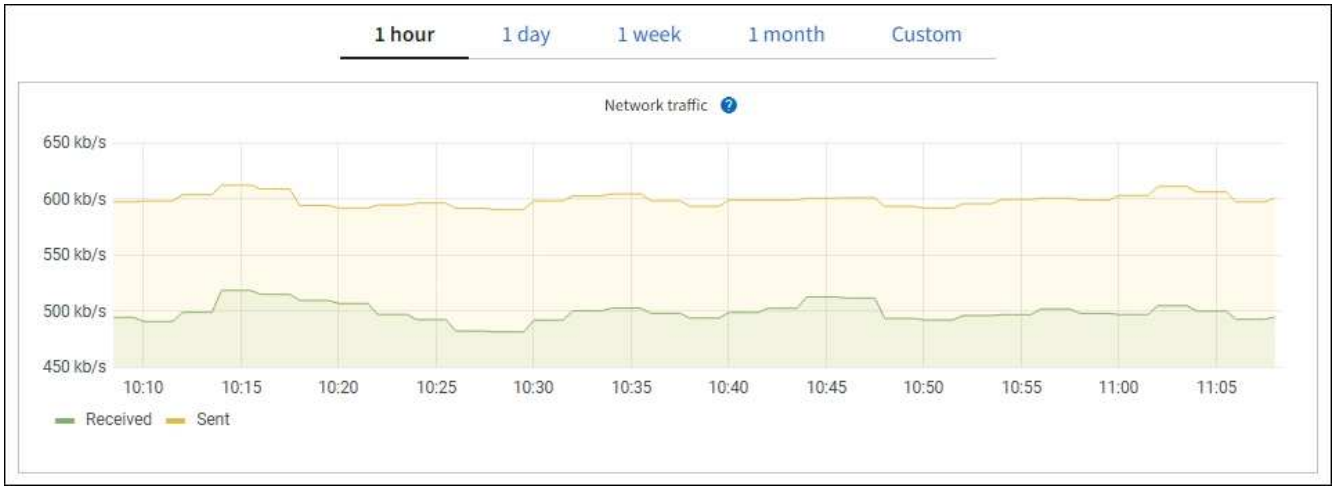
Prometheus 메트릭이란 무엇입니까**?**

Prometheus 메트릭은 시계열 측정입니다. 관리 노드의 Prometheus 서비스는 모든 노드의 서비스에서 이러한 메트릭을 수집합니다. 메트릭은 Prometheus 데이터에 예약된 공간이 가득 찰 때까지 각 관리 노드에 저장됩니다. 볼륨이 용량에 도달하면 `/var/local/mysql_ibdata/` 가장 오래된 메트릭이 먼저 삭제됩니다.

Prometheus 메트릭은 어디에 사용됩니까**?**

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. (그리드 관리자 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 여러 가지 도구 및 차트를 제공합니다.

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

가장 일반적인 메트릭의 목록입니다

다음 목록에는 가장 일반적으로 사용되는 Prometheus 메트릭이 포함되어 있습니다.

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

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
의 캐리어 값 `/sys/class/net/iface`.

node_network_Receive_errs_total
네트워크 장치 통계입니다. `receive_errs`

node_network_transmit_errs_total
네트워크 장치 통계입니다. `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 드라이브 수가 있습니다.

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 S3를 통해 시스템과 상호 작용하는 클라이언트 애플리케이션에서 생성된 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.

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 NTP(Network Time Protocol) 서버에 잠기지 않습니다.

StorageGRID_S3_data_transfers_bytes_ingested입니다

속성이 마지막으로 재설정된 이후 S3 클라이언트에서 이 스토리지 노드로 수집된 총 데이터 양입니다.

StorageGRID_S3_data_transfers_bytes_retrieved입니다

속성이 마지막으로 재설정된 이후 이 스토리지 노드에서 S3 클라이언트가 검색한 총 데이터 양입니다.

StorageGRID_S3_OPERATIONS_FAILED

S3 승인 실패로 인해 발생한 작업을 제외한 총 S3 작업 실패 횟수(HTTP 상태 코드 4xx 및 5xx).

StorageGRID_S3_OPERATIONS_SUCCESS입니다

성공한 S3 작업의 총 수(HTTP 상태 코드 2xx).

StorageGRID_S3_OPERATIONS_UNABLED

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

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_데이터_바이트

스토리지 노드에서 복제 및 삭제 코딩된 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).

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.

모든 메트릭의 목록을 가져옵니다

메트릭의 전체 목록을 보려면 Grid Management API를 사용하십시오.

1. Grid Manager 상단에서 도움말 아이콘을 선택하고 * API documentation * 을 선택합니다.
2. 메트릭 * 작업을 찾습니다.
3. `GET /grid/metric-names`작업을 실행합니다.
4. 결과를 다운로드합니다.

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"
- "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 액세스합니다

로그에 액세스하려면 하나 이상의 노드에서 단일 로그 파일 아카이브로 액세스할 수 "로그 파일 및 시스템 데이터를 수집합니다"있습니다. 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. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
2. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
3. 다음 명령을 입력하여 루트로 전환합니다. `su -`
4. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

syslog 서버로 로그를 내보냅니다

로그를 syslog 서버로 내보내면 다음과 같은 기능이 제공됩니다.

- S3 및 Swift 요청 외에 모든 Grid Manager 및 Tenant Manager 요청 목록을 수신합니다.
- 감사 로깅 방법으로 인한 성능에 영향을 미치지 않고 오류를 반환하는 S3 요청에 대한 가시성 향상
- 구문 분석하기 쉬운 HTTP 계층 요청 및 오류 코드에 액세스할 수 있습니다.
- 로드 밸런서의 트래픽 분류자에 의해 차단된 요청에 대한 가시성 향상

로그를 내보내려면 을 "감사 메시지 및 로그 대상을 구성합니다"참조하십시오.

로그 파일 범주

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.

보관 위치	설명
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	프로필 ID별 현재 노드 및 EC 그룹 정보에 대한 VCS 정보
그리드	디버그를 포함한 일반 그리드 로그(`bycast.log`) 및 `servermanager` 로그
그리드제이슨	모든 노드에서 공유되는 그리드 구성 파일입니다. 또한 는 `node.json` 현재 노드에만 적용됩니다.
해그루	고가용성 그룹 메트릭 및 로그
설치합니다	`Gdu-server` 및 설치 로그.
람다 - 중재인	S3 Select 프록시 요청과 관련된 로그입니다.
lumberjack.log	로그 수집과 관련된 디버그 메시지입니다.
메트릭	Grafana, Jaeger, 노드 수출자 및 Prometheus에 대한 서비스 로그.
오류	Miscd 액세스 및 오류 로그.
MySQL	MariaDB 데이터베이스 구성 및 관련 로그.
결과	네트워킹 관련 스크립트 및 Dynip 서비스에서 생성된 로그입니다.
Nginx	로드 밸런서와 그리드 페더레이션 구성 파일 및 로그 그리드 관리자 및 테넌트 관리자 트래픽 로그도 포함됩니다.

보관 위치	설명
Nginx-GW	• `access.log`: Grid Manager 및 Tenant Manager 요청 로그 메시지. ◦ syslog를 사용하여 내보낼 때 이러한 메시지 앞에 가 `mgmt:` 붙습니다. ◦ 이러한 로그 메시지의 형식은 입니다 `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`: 인바운드 교차 그리드 복제 요청. ◦ syslog를 사용하여 내보낼 때 이러한 메시지 앞에 가 `cgr:` 붙습니다. ◦ 이러한 로그 메시지의 형식은 입니다 `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`: 로드 밸런서 엔드포인트에 대한 S3 및 Swift 요청. ◦ syslog를 사용하여 내보낼 때 이러한 메시지 앞에 가 `endpoint:` 붙습니다. ◦ 이러한 로그 메시지의 형식은 입니다 `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`: 새 DNS 확인 알림과 관련이 있습니다.
NTP	NTP 구성 파일 및 로그
고아 개체	분리된 객체에 대한 로그입니다.
OS	서비스를 포함한 노드 및 그리드 상태 파일 `pid`
기타	다른 폴더에 수집되지 않은 아래의 로그 파일 `/var/local/log`.
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.
SSH를 클릭합니다	SSH 구성 및 서비스와 관련된 로그
SNMP를 선택합니다	SNMP 알림을 보내는 데 사용되는 SNMP 에이전트 구성입니다.
소켓 - 데이터	네트워크 디버그용 소켓 데이터

보관 위치	설명
system-commands.txt	StorageGRID 컨테이너 명령의 출력 네트워킹 및 디스크 사용과 같은 시스템 정보를 포함합니다.
synchronize-recovery-package	ADC 서비스를 호스팅하는 모든 관리 노드 및 스토리지 노드에서 최신 복구 패키지의 일관성 유지와 관련됩니다.

StorageGRID 소프트웨어 로그

StorageGRID 로그를 사용하여 문제를 해결할 수 있습니다.

로그를 외부 syslog 서버로 전송하거나 및 와 `nms.log` 같은 감사 정보의 대상을 `bycast.log` 변경하려면 을 참조하십시오."감사 메시지 및 로그 대상을 구성합니다"

일반 **StorageGRID** 로그

파일 이름입니다	참고	에 있습니다
/var/local/log/bycast.log 를 참조하십시오	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 를 참조하십시오	의 하위 집합 `bycast.log`(심각도 오류 및 심각도가 있는 메시지)을 포함합니다. 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. • 참고 *: 파일은 `/var/local/core/kexec_cmd` 일반적으로 어플라이언스 노드에 존재하며 오류를 나타내지 않습니다.	모든 노드

암호화 관련 로그

파일 이름입니다	참고	에 있습니다
/var/local/log/ssh-config-generation.log 를 참조하십시오	SSH 구성 생성 및 SSH 서비스 재로드와 관련된 로그를 포함합니다.	모든 노드

파일 이름입니다	참고	에 있습니다
/var/local/log/nginx/config-generation.log 를 참조하십시오	nginx 구성 생성 및 nginx 서비스 재로드와 관련된 로그를 포함합니다.	모든 노드
/var/local/log/nginx-GW/config-generation.log 를 참조하십시오	nginx-GW 구성 생성(및 nginx-GW 서비스 재로딩)과 관련된 로그를 포함합니다.	관리자 및 게이트웨이 노드
/var/local/log/update-cipher-configurations.log 를 참조하십시오	TLS 및 SSH 정책 구성과 관련된 로그를 포함합니다.	모든 노드

그리드 페더레이션 로그

파일 이름입니다	참고	에 있습니다
/var/local/log/update_grid_federation_config.log 를 참조하십시오	그리드 페더레이션 연결을 위한 nginx 및 nginx-GW 구성 생성과 관련된 로그를 포함합니다.	모든 노드

NMS 로그

파일 이름입니다	참고	에 있습니다
/var/local/log/nms.log 를 참조하십시오	• Grid Manager 및 테넌트 관리자의 알림을 캡처합니다. • NMS 서비스 작동과 관련된 이벤트를 캡처합니다. 예를 들어, 이메일 알림 및 구성 변경 사항이 있습니다. • 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.errlog입니다	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

파일 이름입니다	참고	에 있습니다
/var/local/log/NMS.requestlog입니다	관리 API에서 내부 StorageGRID 서비스로 나가는 연결에 대한 정보를 포함합니다.	관리자 노드

서버 관리자 로그

파일 이름입니다	참고	에 있습니다
/var/local/log/servermanager.log 를 참조하십시오	서버에서 실행 중인 Server Manager 응용 프로그램의 로그 파일입니다.	모든 노드
/var/local/log/GridstatBackend.errlog입니다	Server Manager GUI 백엔드 애플리케이션에 대한 로그 파일입니다.	모든 노드
/var/local/log/gridstat.errlog입니다	서버 관리자 GUI에 대한 로그 파일입니다.	모든 노드

StorageGRID 서비스 로그

파일 이름입니다	참고	에 있습니다
/var/local/log/acct.errlog입니다		ADC 서비스를 실행하는 스토리지 노드
/var/local/log/ADC.errlog입니다	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.errlog입니다		관리자 노드
/var/local/log/cassandra/system.log 를 참조하십시오	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 를 참조하십시오	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.errlog입니다		스토리지 노드
/var/local/log/CMN.errlog입니다		관리자 노드

파일 이름입니다	참고	에 있습니다
/var/local/log/CMS.errlog 를 참조하십시오	이 로그 파일은 이전 버전의 StorageGRID에서 업그레이드된 시스템에 있을 수 있습니다. 기존 정보가 포함되어 있습니다.	스토리지 노드
/var/local/log/dS.errlog를 참조하십시오		스토리지 노드
/var/local/log/DMV.errlog입니다		스토리지 노드
/var/local/log/dynip * 를 참조하십시오	동적 IP 변경을 위해 그리드를 모니터링하고 로컬 구성을 업데이트하는 dynip 서비스와 관련된 로그를 포함합니다.	모든 노드
/var/local/log/grafana.log 를 참조하십시오	Grafana 서비스와 연관된 로그로, Grid Manager에서 메트릭 시각화에 사용됩니다.	관리자 노드
/var/local/log/hagroups.log 를 참조하십시오	고가용성 그룹과 연결된 로그입니다.	관리 노드 및 게이트웨이 노드
/var/local/log/hagroups_events.log 를 참조하십시오	백업에서 마스터로 전환 또는 오류와 같은 상태 변경을 추적합니다.	관리 노드 및 게이트웨이 노드
/var/local/log/idnt.errlog입니다		ADC 서비스를 실행하는 스토리지 노드
/var/local/log/jaeger.log 를 참조하십시오	추적 수집에 사용되는 Jaeger 서비스와 연관된 로그입니다.	모든 노드
/var/local/log/kstn.errlog입니다		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 "S3 관리자 및 게이트웨이 노드에 대한 요구 사항 및 제한 사항을 선택합니다"참조하십시오.
/var/local/log/LDR.errlog입니다		스토리지 노드

파일 이름입니다	참고	에 있습니다
/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
/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	오류 로그를 포함하여 nginx-GW 서비스와 관련된 일반 로그 및 관리 노드의 제한된 관리 포트에 대한 로그가 포함되어 있습니다.	관리 노드 및 게이트웨이 노드
/var/local/log/nginx-GW/cgr-access.log.gz 를 참조하십시오	교차 그리드 복제 트래픽과 관련된 액세스 로그를 포함합니다.	그리드 통합 구성에 따라 관리 노드, 게이트웨이 노드 또는 둘 다 교차 그리드 복제용 대상 그리드에서만 찾을 수 있습니다.
/var/local/log/nginx-GW/endpoint-access.log.gz 를 참조하십시오	클라이언트에서 스토리지 노드로의 S3 트래픽의 로드 밸런싱을 제공하는 로드 밸런서 서비스에 대한 액세스 로그를 포함합니다.	관리 노드 및 게이트웨이 노드
/var/local/log/persistence * 입니다	재부팅 시 유지되어야 하는 루트 디스크의 파일을 관리하는 Persistence 서비스에 대한 로그를 포함합니다.	모든 노드
/var/local/log/prometheus.log 를 참조하십시오	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 를 참조하십시오	RAFT 프로토콜에 대해 RSM 서비스에서 사용하는 라이브러리의 출력을 포함합니다.	RSM 서비스가 있는 스토리지 노드

파일 이름입니다	참고	에 있습니다
/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.errlog입니다		모든 노드
/var/local/log/update-s3vs-domains.log 를 참조하십시오	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. * 를 참조하십시오	SNMP를 위해 관리되는 방화벽 포트와 관련된 로그를 포함합니다.	모든 노드
/var/local/log/update-sysl.log 를 참조하십시오	시스템 syslog 구성에 대한 변경 사항과 관련된 로그를 포함합니다.	모든 노드
/var/local/log/update-traffic-classes.log 를 참조하십시오	트래픽 분류자 구성 변경과 관련된 로그를 포함합니다.	관리자 및 게이트웨이 노드
/var/local/log/update-utcn.log 를 참조하십시오	이 노드의 신뢰할 수 없는 클라이언트 네트워크 모드와 관련된 로그를 포함합니다.	모든 노드

관련 정보

- "bycast.log 정보"
- "S3 REST API 사용"

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 를 참조하십시오	소프트웨어 설치 중에 생성됩니다. 설치 이벤트 기록을 포함합니다.	모든 노드
/var/local/log/expansion-progress.log 를 참조하십시오	확장 작업 중에 생성됩니다. 확장 이벤트의 레코드를 포함합니다.	스토리지 노드
/var/local/log/pa-move.log 를 참조하십시오	스크립트를 실행하는 동안 `pa-move.sh` 생성됩니다.	기본 관리자 노드

파일 이름입니다	참고	에 있습니다
/var/local/log/pa-move-new_pa.log 를 참조하십시오	스크립트를 실행하는 동안 `pa-move.sh` 생성됩니다.	기본 관리자 노드
/var/local/log/pa-move-old_pa.log 를 참조하십시오	스크립트를 실행하는 동안 `pa-move.sh` 생성됩니다.	기본 관리자 노드
/var/local/log/gdu-server.log 를 참조하십시오	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 를 참조하십시오	설치 중에 생성됩니다. 기본 관리 노드와의 노드 통신과 관련된 디버깅 정보를 포함합니다.	모든 노드
/var/local/log/upgrade.log 를 참조하십시오	소프트웨어 업그레이드 중에 생성됩니다. 소프트웨어 업데이트 이벤트 기록을 포함합니다.	모든 노드

bycast.log 정보

이 파일은 `/var/local/log/bycast.log` StorageGRID 소프트웨어의 기본 문제 해결 파일입니다. `bycast.log`모든 그리드 노드에 대한 파일이 있습니다. 이 파일에는 해당 그리드 노드와 관련된 메시지가 들어 있습니다.

파일이 `/var/local/log/bycast-err.log` 의 하위 집합입니다. `bycast.log` 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 "감사 메시지 및 로그 대상을 구성합니다 "참조하십시오.

bycast.log 파일 회전

파일이 1GB에 도달하면 `bycast.log` 기존 파일이 저장되고 새 로그 파일이 시작됩니다.

저장된 파일의 이름이 바뀌고 `bycast.log.1` 새 파일의 이름이 `bycast.log`지정됩니다. 새 파일이 1GB에 `bycast.log.1` 도달하면 `bycast.log` 이름이 변경되고 압축되어 가 되고 `bycast.log.2.gz` `bycast.log` 이름이 `bycast.log.1`변경됩니다.

의 회전 제한은 `bycast.log` 21개 파일입니다. 22번째 버전의 파일이 생성되면 `bycast.log` 가장 오래된 파일이 삭제됩니다.

의 회전 제한은 `bycast-err.log` 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 "감사 메시지 및 로그 대상을 구성합니다 "참조하십시오.

관련 정보

"로그 파일 및 시스템 데이터를 수집합니다"

bycast.log 의 메시지

의 메시지는 `bycast.log` ADE(Asynchronous Distributed Environment)에 의해 기록됩니다. 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 ID	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

의 메시지에는 `bycast.log` 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.

의 오류 코드입니다 `bycast.log`

의 대부분의 오류 메시지에는 `bycast.log` 오류 코드가 포함되어 있습니다.

다음 표에서는 에서 숫자가 아닌 일반적인 코드를 `bycast.log` 보여 줍니다. 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 표에서는 의 숫자 오류 코드를 `bycast.log` 보여 줍니다.

오류 번호	오류 코드	의미
001	EPERM	작업이 허용되지 않습니다
002	이비인후과	해당 파일 또는 디렉토리가 없습니다

오류 번호	오류 코드	의미
003	ESRCH	그러한 프로세스가 없습니다
004	EINTR	시스템 호출이 중단되었습니다
005	EIO	I/O 오류
006	ENXIO	해당 장치 또는 주소가 없습니다
007	E2BIG/이투비그	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

오류 번호	오류 코드	의미
024	EMFILE	열려 있는 파일이 너무 많습니다
025	ENOTTY	타자가 아닙니다
026	ETXTBSY	텍스트 파일이 사용 중입니다
027	EFBIG	파일이 너무 큽니다
028	ENOSPC	장치에 남은 공간이 없습니다
029	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	이엘투NSYNC	레벨 2가 동기화되지 않았습니다
046	EL3HLT/엘쓰리엘트	레벨 3가 정지되었습니다
047	EL3RST 를 참조하십시오	레벨 3 재설정
048	ELNNG	링크 번호가 범위를 벗어났습니다
049	EUNATCH	프로토콜 드라이버가 연결되지 않았습니다
050	ENOCSI	사용 가능한 CSI 구조가 없습니다
051	EL2HLT/엘투훌트	레벨 2가 정지되었습니다
052	EBADE	잘못된 교환입니다
053	EBADR	요청 설명자가 잘못되었습니다
054	엑블	Exchange가 가득 찼습니다
055	에노ANO	양극 없음
056	EBADRQC	잘못된 요청 코드입니다
057	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
064	ENONET	컴퓨터가 네트워크에 없습니다
065	ENOPKG	패키지가 설치되지 않았습니다

오류 번호	오류 코드	의미
066	EREMOTE	객체가 원격입니다
067	ENOLINK	링크가 분리되었습니다
068	EADV	오류 알림
069	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	EREMCHG	원격 주소가 변경되었습니다
079	ElibACC	필요한 공유 라이브러리에 액세스할 수 없습니다
080	온라인 서비스	손상된 공유 라이브러리에 액세스 중입니다
081	엘리브SCN	
082	엘리브맥스	너무 많은 공유 라이브러리에서 연결을 시도하는 중입니다
083	ELIBEXEC	공유 라이브러리를 직접 실행 할 수 없습니다
084	에일세큐	잘못된 바이트 시퀀스입니다
085	ERESTART	중단된 시스템 통화를 다시 시작해야 합니다
086	테스트 IPE	스트림 파이프 오류입니다

오류 번호	오류 코드	의미
087	EUSERS	사용자가 너무 많습니다
088	ENOTSOCK	비소켓에서 소켓 작동
089	EDESTADDREQ	대상 주소가 필요합니다
090	EMSGSIZE	메시지가 너무 깁니다
091	EPROTOTYPE	소켓 프로토콜 유형이 잘못되었습니다
092	ENOPROTOOPT	프로토콜을 사용할 수 없습니다
093	EPROTONOSUPPORT를 참조하십시오	지원되지 않는 프로토콜입니다
094	ESOCKTNOSUPPORT	지원되지 않는 소켓 유형입니다
095	EOPNOTSUPP	전송 엔드포인트에서 지원되지 않는 작업입니다
096	EPFNOSUPPORT	프로토콜 제품군이 지원되지 않습니다
097	EAFNOSUPPORT를 참조하십시오	프로토콜에서 지원되지 않는 주소 제품군입니다
098	EADDRINUSE	이미 사용 중인 주소입니다
099	EADDRNOTAVAIL	요청한 주소를 할당할 수 없습니다
100	ENETDOWN	네트워크가 다운되었습니다
101	ENETUNREACH를 참조하십시오	네트워크에 연결할 수 없습니다
102	네테세트	재설정으로 인해 네트워크 연결이 끊어졌습니다
103	연결\nECONNABORTED	소프트웨어에서 연결을 종료했습니다
104	ECONNRESET	피어에 의해 연결이 재설정되었습니다
105	ENOBUFS	사용 가능한 버퍼 공간이 없습니다
106	EISCONN	전송 엔드포인트가 이미 연결되어 있습니다

오류 번호	오류 코드	의미
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
123	ENOMEDIUM	미디어를 찾을 수 없습니다
124	EMEDIUMTYPE	잘못된 매체 유형입니다
125	ECANCELED	작업이 취소되었습니다
126	ENOKEY	필수 키를 사용할 수 없습니다
127	에케예피레드	키가 만료되었습니다

오류 번호	오류 코드	의미
128	EKEYREVOKED	키가 취소되었습니다
129	EKEYREJECTED	서비스가 키를 거부했습니다
130	EOWNERDEAD	확실한 돌연변이: 주인이 죽었다
131	복구불가	강력한 뮤텍스의 경우: 상태를 복구할 수 없습니다

감사 메시지 및 로그 대상을 구성합니다

외부 **syslog** 서버 사용 시 고려 사항

외부 syslog 서버는 단일 위치에서 시스템 감사 정보를 수집하는 데 사용할 수 있는 StorageGRID 외부의 서버입니다. 외부 syslog 서버를 사용하면 관리 노드의 네트워크 트래픽을 줄이고 정보를 보다 효율적으로 관리할 수 있습니다. StorageGRID의 경우 아웃바운드 syslog 메시지 패킷 형식은 RFC 3164와 호환됩니다.

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** 서버를 사용해야 하는 경우

외부 syslog 서버는 큰 그리드가 있거나 여러 유형의 S3 애플리케이션을 사용하거나 모든 감사 데이터를 보존하려는 경우에 특히 유용합니다. 감사 정보를 외부 syslog 서버로 전송하면 다음을 수행할 수 있습니다.

- 감사 메시지, 응용 프로그램 로그 및 보안 이벤트와 같은 감사 정보를 보다 효율적으로 수집하고 관리합니다.
- 관리자 노드를 거치지 않고도 감사 정보가 다양한 스토리지 노드에서 외부 syslog 서버로 직접 전송되므로 관리자 노드의 네트워크 트래픽이 감소합니다.

로그가 외부 syslog 서버로 전송되면 메시지가 끝날 때 8,192바이트보다 큰 단일 로그가 잘려서 외부 syslog 서버 구현의 일반적인 제한 사항을 준수합니다.

외부 syslog 서버에 장애가 발생할 경우 전체 데이터 복구 옵션을 극대화하기 위해 (`localaudit.log`각 노드에서 최대 20GB의 감사 레코드 로컬 로그)가 유지됩니다.

외부 **syslog** 서버를 구성하는 방법

외부 syslog 서버를 구성하는 방법은 을 참조하십시오"감사 메시지 및 외부 syslog 서버를 구성합니다".

TLS 또는 RELP/TLS 프로토콜 사용을 구성하려면 다음 인증서가 있어야 합니다.

- * 서버 CA 인증서 *: PEM 인코딩에서 외부 syslog 서버를 확인하기 위한 하나 이상의 신뢰할 수 있는 CA 인증서. 이 인수를 생략하면 기본 Grid CA 인증서가 사용됩니다.
- * 클라이언트 인증서 * : PEM 인코딩에서 외부 syslog 서버에 인증하기 위한 클라이언트 인증서입니다.
- * 클라이언트 개인 키 *: PEM 인코딩의 클라이언트 인증서에 대한 개인 키입니다.

> 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.

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 다음 S3 필드의 값(GET 대비)과 평균 크기(바이트)입니다(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.
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.
에스3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷에 대한 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 합계에 대한 평균 크기를 나타내겠습니다. 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 비율 = 8 x S3 작업 비율
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 대 삭제 코딩), S3 작업의 백분율(GET/기타) 및 평균 크기(바이트)입니다(표에서 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.
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.
에스3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷에 대한 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 합계에 대한 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 합계에 대한 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 대해 사이징된 경우 워크로드는 50%가 되고 S3 계정 이름, 버킷 이름 객체 이름은 평균 90바이트로, 외부 syslog 서버는 초당 2,250개의 애플리케이션 로그를 지원하도록 크기를 조정하고 초당 0.6MB의 속도로 애플리케이션 데이터를 수신(일반적으로 저장)할 수 있어야 합니다.

감사 메시지 및 외부 **syslog** 서버를 구성합니다

감사 메시지와 관련된 여러 설정을 구성할 수 있습니다. 기록된 감사 메시지 수를 조정하고, 클라이언트 읽기 및 쓰기 감사 메시지에 포함할 HTTP 요청 헤더를 정의하며, 외부 syslog 서버를 구성하고, 감사 로그, 보안 이벤트 로그 및 StorageGRID 소프트웨어 로그를 보낼 위치를 지정할 수 있습니다.

감사 메시지와 로그는 시스템 활동 및 보안 이벤트를 기록하고, 모니터링 및 문제 해결에 필수적인 도구입니다. 모든 StorageGRID 노드는 감사 메시지와 로그를 생성하여 시스템 활동 및 이벤트를 추적합니다.

필요에 따라 감사 정보를 원격으로 저장하도록 외부 syslog 서버를 구성할 수 있습니다. 외부 서버를 사용하면 감사

데이터의 완성도를 낮추지 않고도 감사 메시지 로깅의 성능에 미치는 영향을 최소화할 수 있습니다. 외부 syslog 서버는 큰 그리드가 있거나 여러 유형의 S3 애플리케이션을 사용하거나 모든 감사 데이터를 보존하려는 경우에 특히 유용합니다. 자세한 내용은 을 "감사 메시지 및 외부 syslog 서버를 구성합니다" 참조하십시오.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.
- 외부 syslog 서버를 구성하려는 경우 를 검토하고 "외부 syslog 서버 사용 시 고려 사항"로그 파일을 수신하고 저장할 수 있는 충분한 용량을 서버에 확보했는지 확인했습니다.
- TLS 또는 RELP/TLS 프로토콜을 사용하여 외부 syslog 서버를 구성하려는 경우 필요한 서버 CA 및 클라이언트 인증서, 클라이언트 개인 키가 있습니다.

감사 메시지 수준을 변경합니다

감사 로그에서 다음 메시지 범주에 대해 서로 다른 감사 수준을 설정할 수 있습니다.

감사 범주	기본 설정	추가 정보
시스템	정상	"시스템 감사 메시지"
스토리지	오류	"오브젝트 스토리지 감사 메시지"
관리	정상	"관리 감사 메시지입니다"
클라이언트 읽기	정상	"클라이언트가 감사 메시지를 읽습니다"
클라이언트 쓰기	정상	"클라이언트가 감사 메시지를 기록합니다"
ILM을 참조하십시오	정상	"ILM 감사 메시지"
교차 그리드 복제	오류	"CGRR: 교차 그리드 복제 요청"

이 기본값은 버전 10.3 이상을 사용하여 StorageGRID를 처음 설치한 경우에 적용됩니다. 이전 버전의 StorageGRID를 처음 사용한 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.
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.

S3 응용 프로그램에 대한 클라이언트 읽기 작업에 대한 자세한 레코드가 필요하지 않은 경우 * 클라이언트 읽기 * 설정을 * 오류 * 로 변경하여 감사 로그에 기록되는 감사 메시지 수를 줄입니다.

3. 저장 * 을 선택합니다.

   녹색 배너는 구성이 저장되었음을 나타냅니다.

HTTP 요청 헤더를 정의합니다

클라이언트 읽기 및 쓰기 감사 메시지에 포함할 HTTP 요청 헤더를 선택적으로 정의할 수 있습니다. 이러한 프로토콜 헤더는 S3 요청에만 적용됩니다.

단계

1. Audit protocol headers * 섹션에서 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.

2. 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.

3. 저장 * 을 선택합니다

   녹색 배너는 구성이 저장되었음을 나타냅니다.

외부 syslog 서버를 사용합니다

필요에 따라 감사 로그, 응용 프로그램 로그 및 보안 이벤트 로그를 그리드 외부의 위치에 저장하도록 외부 syslog 서버를 구성할 수 있습니다.

외부 syslog 서버를 사용하지 않으려면 이 단계를 건너뛰고 로 이동합니다감사 정보 대상을 선택합니다.

이 절차에서 사용할 수 있는 구성 옵션이 요구 사항을 충족하기에 충분히 유연하지 않은 경우 의 전용 API 섹션에 있는 끝점을 사용하여 추가 구성 옵션을 적용할 수 `audit-destinations`"Grid Management API를 참조하십시오" 있습니다. 예를 들어, 노드 그룹마다 서로 다른 syslog 서버를 사용하려는 경우 API를 사용할 수 있습니다.

syslog 정보를 입력합니다

외부 syslog 서버 구성 마법사에 액세스하여 StorageGRID가 외부 syslog 서버에 액세스하는 데 필요한 정보를 제공합니다.

단계

1. 감사 및 syslog 서버 페이지에서 * 외부 syslog 서버 구성 * 을 선택합니다. 또는 이전에 외부 syslog 서버를 구성한 경우 * 외부 syslog 서버 편집 * 을 선택합니다.

   외부 syslog 서버 구성 마법사가 나타납니다.

2. 마법사의 * syslog 정보 입력 * 단계에 대해 유효한 정규화된 도메인 이름 또는 외부 syslog 서버에 대한 IPv4 또는 IPv6 주소를 * Host * 필드에 입력합니다.
3. 외부 syslog 서버의 대상 포트를 입력합니다(1과 65535 사이의 정수여야 함). 기본 포트는 514입니다.
4. 외부 syslog 서버로 감사 정보를 보내는 데 사용되는 프로토콜을 선택합니다.

   TLS * 또는 * RELP/TLS * 를 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 "보안 인증서를 관리합니다"참조하십시오.

   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.

5. Continue * 를 선택합니다.
6.] * TLS * 또는 * RELP/TLS * 를 선택한 경우 서버 CA 인증서, 클라이언트 인증서 및 클라이언트 개인 키를 업로드합니다.
   a. 사용할 인증서 또는 키를 * 찾아보기 * 를 선택합니다.
   b. 인증서 또는 키 파일을 선택합니다.
   c. 파일을 업로드하려면 * 열기 * 를 선택합니다.

      인증서 또는 키 파일 이름 옆에 녹색 확인 표시가 나타나 성공적으로 업로드되었음을 알려줍니다.

7. Continue * 를 선택합니다.

syslog 콘텐츠를 관리합니다

외부 syslog 서버로 보낼 정보를 선택할 수 있습니다.

단계

1. 마법사의 * syslog 콘텐츠 관리 * 단계에서 외부 syslog 서버로 보낼 감사 정보의 각 유형을 선택합니다.
   - * 감사 로그 전송 *: StorageGRID 이벤트 및 시스템 활동을 전송합니다
   - * 보안 이벤트 전송 *: 권한이 없는 사용자가 로그인을 시도하거나 사용자가 루트로 로그인하는 등의 보안 이벤트를 전송합니다
   - * 응용 프로그램 로그 보내기 *: 다음을 포함하여 문제 해결에 유용한 전송"StorageGRID 소프트웨어 로그 파일":
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (관리 노드 전용)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
   - * 액세스 로그 전송 *: 외부 요청에 대한 HTTP 액세스 로그를 Grid Manager, Tenant Manger, 구성된 로드 밸런서 엔드포인트 및 원격 시스템의 그리드 페더레이션 요청에 보냅니다.
2. 드롭다운 메뉴를 사용하여 보내려는 감사 정보의 각 범주에 대한 심각도 및 시설(메시지 유형)을 선택합니다.

   심각도 및 항목 값을 설정하면 보다 쉽게 분석할 수 있도록 로그를 사용자 지정 가능한 방식으로 집계할 수 있습니다.

   a. 심각도 * 에 대해 * 통과 * 를 선택하거나 0에서 7 사이의 심각도 값을 선택합니다.

      값을 선택하면 선택한 값이 이 유형의 모든 메시지에 적용됩니다. 심각도를 고정 값으로 재정의하면 다른 심각도에 대한 정보가 손실됩니다.

심각도입니다	설명
패스스루	외부 syslog로 전송되는 각 메시지는 노드에 로컬로 로그온한 경우와 동일한 심각도 값을 갖습니다. • 감사 로그의 심각도는 "info"입니다. • 보안 이벤트의 경우 심각도 값은 노드의 Linux 배포판에 의해 생성됩니다. • 응용 프로그램 로그의 심각도는 문제의 심각도에 따라 "정보"와 "알림" 사이에 차이가 있습니다. 예를 들어 NTP 서버를 추가하고 HA 그룹을 구성하면 "info"라는 값이 제공되지만 SSM 또는 RSM 서비스를 의도적으로 중지하면 "notice"라는 값이 제공됩니다. • 액세스 로그의 심각도는 "info"입니다.
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

b. Facilty * 의 경우 * PassThrough * 를 선택하거나 0에서 23 사이의 시설 값을 선택합니다.

값을 선택하면 이 유형의 모든 메시지에 적용됩니다. 시설을 고정 값으로 재정의하면 다른 시설에 대한 정보가 손실됩니다.

있습니다	설명
패스스루	외부 syslog로 전송되는 각 메시지는 노드에 로컬로 로그온한 경우와 동일한 시설 값을 갖습니다. • 감사 로그의 경우 외부 syslog 서버로 전송되는 기능은 "local7"입니다. • 보안 이벤트의 경우 노드의 Linux 배포에 의해 항목 값이 생성됩니다. • 응용 프로그램 로그의 경우 외부 syslog 서버로 전송된 응용 프로그램 로그에는 다음 항목 값이 있습니다. ◦ `bycast.log`: 사용자 또는 데몬 ◦ `bycast-err.log`사용자, 데몬, local3 또는 local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: 로컬3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6 • 액세스 로그의 경우 외부 syslog 서버로 전송된 기능은 "local0"입니다.
0	Kern(커널 메시지)
1	사용자(사용자 수준 메시지)
2	메일
3	데몬(시스템 데몬)

있습니다	설명
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
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.

단계

1. 외부 syslog 서버가 제대로 구성되어 있고 그리드의 모든 노드에서 감사 정보를 수신할 수 있으므로 테스트 메시지를 전송하지 않으려면 * Skip and finish * 를 선택합니다.

   녹색 배너는 구성이 저장되었음을 나타냅니다.

2. 그렇지 않으면 * 테스트 메시지 전송 * (권장)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.

   오류를 해결하는 데 도움이 되는 내용은 을 "외부 syslog 서버의 문제를 해결합니다"참조하십시오.

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. 녹색 배너는 syslog 서버 구성이 저장되었음을 나타냅니다.

   > StorageGRID 감사 정보는 외부 syslog 서버가 포함된 대상을 선택할 때까지 외부 syslog 서버로 전송되지 않습니다.

감사 정보 대상을 선택합니다

감사 로그, 보안 이벤트 로그 및 를 보낼 위치를 지정할 수 "StorageGRID 소프트웨어 로그"있습니다.

StorageGRID은 기본적으로 로컬 노드 감사 대상으로 설정되며 감사 정보를 에 `/var/local/log/localaudit.log`저장합니다.

을 사용하는 경우 `/var/local/log/localaudit.log` 그리드 관리자 및 테넌트 관리자 감사 로그 항목이 스토리지 노드로 전송될 수 있습니다. 명령을 사용하여 가장 최근 항목이 있는 노드를 찾을 수 `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` 있습니다.

일부 대상은 외부 syslog 서버를 구성한 경우에만 사용할 수 있습니다.

단계

1. 감사 및 syslog 서버 페이지에서 감사 정보의 대상을 선택합니다.

* 로컬 노드만 * 및 * 외부 syslog 서버 * 는 일반적으로 더 나은 성능을 제공합니다.

옵션을 선택합니다	설명
로컬 노드만(기본값)	감사 메시지, 보안 이벤트 로그 및 응용 프로그램 로그는 관리 노드로 전송되지 않습니다. 대신, 이 파일은 해당 노드를 생성한 노드에만 저장됩니다("로컬 노드"). 모든 로컬 노드에서 생성된 감사 정보는 에 `/var/local/log/localaudit.log`저장됩니다. • 참고 *: StorageGRID는 주기적으로 로테이션에서 로컬 로그를 제거하여 공간을 확보합니다. 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.
관리 노드/로컬 노드	감사 메시지는 관리 노드의 감사 로그로 전송되고 보안 이벤트 로그와 애플리케이션 로그는 감사 로그를 생성한 노드에 저장됩니다. 감사 정보는 다음 파일에 저장됩니다. • 관리 노드(운영 및 비운영): `/var/local/audit/export/audit.log` • All nodes(모든 노드): `/var/local/log/localaudit.log` 일반적으로 파일이 비어 있거나 없습니다. 여기에는 일부 메시지의 추가 복사본과 같은 보조 정보가 포함될 수 있습니다.
외부 syslog 서버	감사 정보는 외부 syslog 서버로 전송되고 로컬 노드에 (`/var/local/log/localaudit.log`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 감사 로그로 전송되며 (`/var/local/audit/export/audit.log`, 감사 정보는 외부 syslog 서버로 전송되고 로컬 노드에 (`/var/local/log/localaudit.log`저장됩니다. 전송되는 정보의 유형은 외부 syslog 서버를 구성한 방식에 따라 다릅니다. 이 옵션은 외부 syslog 서버를 구성한 후에만 활성화됩니다.

2. 저장 * 을 선택합니다.

   경고 메시지가 나타납니다.

3. 감사 정보의 대상을 변경하려면 * OK * 를 선택합니다.

   녹색 배너는 감사 구성이 저장되었음을 나타냅니다.

   새 로그가 선택한 대상으로 전송됩니다. 기존 로그는 현재 위치에 남아 있습니다.

SNMP 모니터링을 사용합니다

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 MIB를 제공하는 SNMP 에이전트 또는 데몬을 실행합니다. StorageGRID MIB에는 경고에 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.

그리드 노드에 MIB 파일을 다운로드할지 여부를 확인하십시오"MIB 파일에 액세스합니다".

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

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.

알림

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.

다음과 같은 경우 트랩 및 알림 알림이 전송됩니다.

- 기본 또는 사용자 지정 알림은 모든 심각도 수준에서 트리거됩니다. 알림에 대한 SNMP 알림을 표시하지 않으려면 해당 알림에 대해 설정해야 "무음을 구성합니다"합니다. 경고 알림은 에서 "기본 설정 보낸 사람 관리자 노드

"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 경고 목록은 을 참조하십시오"경고 참조".

SNMP 버전 지원

이 표에는 각 SNMP 버전에서 지원되는 항목에 대한 자세한 요약 정보가 나와 있습니다.

	SNMPv1을 참조하십시오	**SNMPv2c**	**SNMPv3**를 참조하십시오
쿼리 (Get and GetNext)(가져오기 및 GetNext)	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 (트랩 및 정보 제공)	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.

SNMP 에이전트를 구성합니다

읽기 전용 MIB 액세스 및 알림에 타사 SNMP 관리 시스템을 사용하도록 StorageGRID SNMP 에이전트를 구성할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.

이 작업에 대해

StorageGRID SNMP 에이전트는 SNMPv1, SNMPv2c 및 SNMPv3를 지원합니다. 하나 이상의 버전에 대해 에이전트를 구성할 수 있습니다. SNMPv3의 경우 USM(User Security Model) 인증만 지원됩니다.

그리드의 모든 노드는 동일한 SNMP 구성을 사용합니다.

기본 구성을 지정합니다

첫 번째 단계로 StorageGRID SMNP 에이전트를 활성화하고 기본 정보를 제공합니다.

단계

1. 구성 * > * 모니터링 * > * SNMP 에이전트 * 를 선택합니다.

   SNMP 에이전트 페이지가 나타납니다.

2. 모든 그리드 노드에서 SNMP 에이전트를 활성화하려면 * SNMP * 활성화 확인란을 선택합니다.
3. 기본 구성 섹션에 다음 정보를 입력합니다.

필드에 입력합니다	설명
시스템 연락처	선택 사항. StorageGRID 시스템의 기본 연락처로, SNMP 메시지에서 sysContact로 반환됩니다. 시스템 연락처는 일반적으로 전자 메일 주소입니다. 이 값은 StorageGRID 시스템의 모든 노드에 적용됩니다. * 시스템 연락처 * 는 최대 255자까지 입력할 수 있습니다.
시스템 위치	선택 사항. SNMP 메시지에 sysLocation 으로 반환되는 StorageGRID 시스템의 위치입니다. 시스템 위치는 StorageGRID 시스템의 위치를 식별하는 데 유용한 정보가 될 수 있습니다. 예를 들어 시설의 주소를 사용할 수 있습니다. 이 값은 StorageGRID 시스템의 모든 노드에 적용됩니다. * 시스템 위치 * 는 최대 255자까지 입력할 수 있습니다.
SNMP 에이전트 알림을 설정합니다	• 이 옵션을 선택하면 StorageGRID SNMP 에이전트가 트랩 및 알림 알림을 보냅니다. • 이 옵션을 선택하지 않으면 SNMP 에이전트는 읽기 전용 MIB 액세스를 지원하지만 SNMP 알림을 보내지 않습니다.
인증 트랩을 활성화합니다	이 옵션을 선택하면 StorageGRID SNMP 에이전트가 잘못 인증된 프로토콜 메시지를 수신하는 경우 인증 트랩을 보냅니다.

커뮤니티 문자열을 입력합니다

SNMPv1 또는 SNMPv2c를 사용하는 경우 커뮤니티 문자열 섹션을 완료하십시오.

관리 시스템이 StorageGRID MIB를 쿼리하면 커뮤니티 문자열을 보냅니다. 커뮤니티 문자열이 여기에 지정된 값 중 하나와 일치하면 SNMP 에이전트는 관리 시스템에 응답을 보냅니다.

단계

1. 읽기 전용 커뮤니티 * 의 경우 IPv4 및 IPv6 에이전트 주소에서 읽기 전용 MIB 액세스를 허용하는 커뮤니티 문자열을 선택적으로 입력합니다.

   > StorageGRID 시스템의 보안을 유지하려면 커뮤니티 문자열로 "public"을 사용하지 마십시오. 이 필드를 비워 두면 SNMP 에이전트는 StorageGRID 시스템의 그리드 ID를 커뮤니티 문자열로 사용합니다.

   각 커뮤니티 문자열은 최대 32자이고 공백 문자를 포함할 수 없습니다.

2. 추가 문자열을 추가하려면 * Add another community string * 을 선택합니다.

   최대 5개의 문자열이 허용됩니다.

트랩 목적지를 작성하십시오

기타 구성 섹션의 트랩 대상 탭을 사용하여 StorageGRID 트랩 또는 알림 알림에 대한 하나 이상의 대상을 정의합니다. SNMP 에이전트를 활성화하고 * 저장 * 을 선택하면 StorageGRID는 경고가 트리거될 때 정의된 각 대상에 알림을 보냅니다. 지원되는 MIB-II 엔티티에 대해서도 표준 알림이 전송됩니다(예: ifdown 및 coldstart).

단계

1. 기본 트랩 커뮤니티 * 필드에 SNMPv1 또는 SNMPv2 트랩 대상에 사용할 기본 커뮤니티 문자열을 선택적으로 입력합니다.

   필요에 따라 특정 트랩 대상을 정의할 때 다른("custom") 커뮤니티 문자열을 제공할 수 있습니다.

   ◦ 기본 트랩 커뮤니티 * 는 최대 32자이며 공백 문자를 포함할 수 없습니다.

2. 트랩 대상을 추가하려면 * Create * 를 선택합니다.
3. 이 트랩 대상에 사용할 SNMP 버전을 선택합니다.
4. 선택한 버전에 대한 Create trap destination 양식을 작성합니다.

SNMPv1을 참조하십시오

SNMPv1을 버전으로 선택한 경우 이 필드를 작성합니다.

필드에 입력합니다	설명
유형	SNMPv1의 트랩이어야 합니다.
호스트	트랩을 수신할 IPv4 또는 IPv6 주소 또는 FQDN(정규화된 도메인 이름)입니다.
포트	다른 값을 사용해야 하는 경우를 제외하고 SNMP 트랩의 표준 포트인 162를 사용합니다.
프로토콜	TCP를 사용할 필요가 없는 경우 표준 SNMP 트랩 프로토콜인 UDP를 사용합니다.
커뮤니티 문자열	기본 트랩 커뮤니티(지정된 경우)를 사용하거나 이 트랩 대상에 대한 사용자 지정 커뮤니티 문자열을 입력합니다. 사용자 지정 커뮤니티 문자열은 최대 32자이며 공백을 포함할 수 없습니다.

SNMPv2c

SNMPv2c을 버전으로 선택한 경우 이 필드를 작성합니다.

필드에 입력합니다	설명
유형	목적지가 트랩에 사용되는지 또는 알림에 사용되는지 여부를 나타냅니다.
호스트	트랩을 수신할 IPv4 또는 IPv6 주소 또는 FQDN입니다.
포트	다른 값을 사용해야 하는 경우를 제외하고 SNMP 트랩의 표준 포트인 162를 사용합니다.
프로토콜	TCP를 사용할 필요가 없는 경우 표준 SNMP 트랩 프로토콜인 UDP를 사용합니다.
커뮤니티 문자열	기본 트랩 커뮤니티(지정된 경우)를 사용하거나 이 트랩 대상에 대한 사용자 지정 커뮤니티 문자열을 입력합니다. 사용자 지정 커뮤니티 문자열은 최대 32자이며 공백을 포함할 수 없습니다.

SNMPv3를 참조하십시오

SNMPv3을 버전으로 선택한 경우 이 필드를 작성합니다.

필드에 입력합니다	설명
유형	목적지가 트랩에 사용되는지 또는 알림에 사용되는지 여부를 나타냅니다.
호스트	트랩을 수신할 IPv4 또는 IPv6 주소 또는 FQDN입니다.
포트	다른 값을 사용해야 하는 경우를 제외하고 SNMP 트랩의 표준 포트인 162를 사용합니다.
프로토콜	TCP를 사용할 필요가 없는 경우 표준 SNMP 트랩 프로토콜인 UDP를 사용합니다.
USM 사용자입니다	인증에 사용할 USM 사용자입니다. • Trap * 을 선택하면 권한 있는 엔진 ID가 없는 USM 사용자만 표시됩니다. • 알림 * 을 선택하면 권한 있는 엔진 ID가 있는 USM 사용자만 표시됩니다. • 사용자가 표시되지 않는 경우: i. 트랩 대상을 생성하고 저장합니다. ii. 로 USM 사용자를 생성합니다 이동하여 사용자를 생성합니다. iii. Trap Destinations(트랩 대상) 탭으로 돌아가서 테이블에서 저장된 대상을 선택하고 * Edit(편집) * 를 선택합니다. iv. 사용자를 선택합니다.

5. Create * 를 선택합니다.

   트랩 대상이 생성되어 테이블에 추가됩니다.

에이전트 주소를 만듭니다

필요에 따라 기타 구성 섹션의 상담원 주소 탭을 사용하여 하나 이상의 "수신 주소"를 지정합니다. SNMP 에이전트가 쿼리를 수신할 수 있는 StorageGRID 주소입니다.

에이전트 주소를 구성하지 않으면 기본 수신 주소는 모든 StorageGRID 네트워크에서 UDP 포트 161입니다.

단계

1. Create * 를 선택합니다.
2. 다음 정보를 입력합니다.

필드에 입력합니다	설명
인터넷 프로토콜	이 주소가 IPv4 또는 IPv6를 사용할지 여부를 나타냅니다. 기본적으로 SNMP는 IPv4를 사용합니다.
전송 프로토콜	이 주소가 UDP 또는 TCP를 사용할지 여부를 나타냅니다. 기본적으로 SNMP는 UDP를 사용합니다.
StorageGRID 네트워크	상담원이 수신 대기할 StorageGRID 네트워크 • 그리드, 관리 및 클라이언트 네트워크: SNMP 에이전트는 세 네트워크 모두에서 쿼리를 수신합니다. • 그리드 네트워크 • 관리자 네트워크 • 클라이언트 네트워크 참고: 클라이언트 네트워크를 비보안 데이터에 사용하고 클라이언트 네트워크에 대한 에이전트 주소를 만드는 경우 SNMP 트래픽도 안전하지 않습니다.
포트	선택적으로 SNMP 에이전트가 수신해야 하는 포트 번호입니다. SNMP 에이전트의 기본 UDP 포트는 161이지만 사용하지 않는 포트 번호를 입력할 수 있습니다. • 참고 *: SNMP 에이전트를 저장하면 StorageGRID가 자동으로 내부 방화벽에서 에이전트 주소 포트를 엽니다. 모든 외부 방화벽이 이러한 포트에 대한 액세스를 허용하는지 확인해야 합니다.

3. Create * 를 선택합니다.

   상담원 주소가 생성되어 테이블에 추가됩니다.

USM 사용자를 생성합니다

SNMPv3을 사용하는 경우 Other configurations 섹션의 USM users 탭을 사용하여 MIB를 쿼리하거나 트랩 및 알림을 받을 권한이 있는 USM 사용자를 정의합니다.

> SNMPv3_inform_destinations에 엔진 ID가 있는 사용자가 있어야 합니다. SNMPv3_trap_destination은 엔진 ID를 가진 사용자를 가질 수 없습니다.

SNMPv1 또는 SNMPv2c만 사용하는 경우에는 이 단계가 적용되지 않습니다.

단계

1. Create * 를 선택합니다.

2. 다음 정보를 입력합니다.

필드에 입력합니다	설명
사용자 이름	이 USM 사용자의 고유한 이름입니다. 사용자 이름은 최대 32자이며 공백 문자를 포함할 수 없습니다. 사용자가 생성된 후에는 사용자 이름을 변경할 수 없습니다.
읽기 전용 MIB 액세스	이 옵션을 선택하면 이 사용자는 MIB에 대한 읽기 전용 액세스 권한이 있어야 합니다.
신뢰할 수 있는 엔진 ID입니다	이 사용자를 알림 대상에서 사용하는 경우 이 사용자에 대한 신뢰할 수 있는 엔진 ID입니다. 공백 없이 10 - 64개의 16진수 문자(5 - 32바이트)를 입력합니다. 이 값은 알림을 위해 트랩 대상에서 선택될 USM 사용자에게 필요합니다. 트랩의 트랩 대상에서 선택할 USM 사용자에게는 이 값이 허용되지 않습니다. • 참고 *: 읽기 전용 MIB 액세스 * 를 선택한 경우에는 이 필드가 표시되지 않습니다. 읽기 전용 MIB 액세스 권한이 있는 USM 사용자는 엔진 ID를 가질 수 없기 때문입니다.
보안 수준	USM 사용자의 보안 수준: • * 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.
인증 프로토콜	항상 지원되는 유일한 프로토콜(HMAC-SHA-96)인 SHA로 설정합니다.
암호	이 사용자가 인증에 사용할 암호입니다.
개인 정보 보호 프로토콜	authPriv * 를 선택하고 항상 AES로 설정한 경우에만 표시됩니다. 이 프로토콜은 지원되는 유일한 개인정보 보호 프로토콜입니다.
암호	authPriv * 를 선택한 경우에만 표시됩니다. 이 사용자가 개인 정보 보호를 위해 사용할 암호입니다.

3. Create * 를 선택합니다.

   USM 사용자가 생성되어 테이블에 추가됩니다.

4. SNMP 에이전트 구성을 완료하면 * Save * 를 선택합니다.

   새 SNMP 에이전트 구성이 활성화됩니다.

SNMP 알림을 비활성화하거나 커뮤니티 문자열을 업데이트하거나 에이전트 주소, USM 사용자 및 트랩 대상을 추가 또는 제거할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.

이 작업에 대해

SNMP 에이전트 페이지의 각 필드에 대한 자세한 내용은 을 "SNMP 에이전트를 구성합니다"참조하십시오. 각 탭에서 변경한 내용을 적용하려면 페이지 맨 아래에 있는 * 저장 * 을 선택해야 합니다.

단계

1. 구성 * > * 모니터링 * > * SNMP 에이전트 * 를 선택합니다.

   SNMP 에이전트 페이지가 나타납니다.

2. 모든 그리드 노드에서 SNMP 에이전트를 비활성화하려면 * Enable SNMP * 확인란을 선택 취소하고 * Save * 를 선택합니다.

   SNMP 에이전트를 다시 활성화하면 이전의 모든 SNMP 구성 설정이 유지됩니다.

3. 필요한 경우 기본 구성 섹션의 정보를 업데이트합니다.

   a. 필요에 따라 * 시스템 연락처 * 및 * 시스템 위치 * 를 업데이트합니다.

   b. 필요에 따라 StorageGRID SNMP 에이전트가 트랩 및 알림 알림을 전송할지 여부를 제어하려면 * SNMP 에이전트 알림 활성화 * 확인란을 선택하거나 선택 취소합니다.

      이 확인란의 선택을 취소하면 SNMP 에이전트는 읽기 전용 MIB 액세스를 지원하지만 SNMP 알림을 보내지 않습니다.

   c. 필요에 따라 * 인증 트랩 활성화 * 확인란을 선택하거나 선택 취소하여 StorageGRID SNMP 에이전트가 잘못 인증된 프로토콜 메시지를 받을 때 인증 트랩을 전송할지 여부를 제어합니다.

4. SNMPv1 또는 SNMPv2c를 사용하는 경우 선택적으로 커뮤니티 문자열 섹션에서 * 읽기 전용 커뮤니티 * 를 업데이트하거나 추가합니다.
5. 트랩 대상을 업데이트하려면 Other configuration(기타 구성) 섹션에서 Trap Destinations(트랩 대상) 탭을 선택합니다.

   이 탭을 사용하여 StorageGRID 트랩 또는 알림 알림에 대한 하나 이상의 대상을 정의합니다. SNMP 에이전트를 활성화하고 * 저장 * 을 선택하면 StorageGRID는 경고가 트리거될 때 정의된 각 대상에 알림을 보냅니다. 지원되는 MIB-II 엔티티에 대해서도 표준 알림이 전송됩니다(예: ifdown 및 coldstart).

   입력할 항목에 대한 자세한 내용은 을 "트랩 대상을 생성합니다"참조하십시오.

   - 필요한 경우 기본 트랩 커뮤니티를 업데이트하거나 제거합니다.

     기본 트랩 커뮤니티를 제거하는 경우 먼저 기존 트랩 대상이 사용자 지정 커뮤니티 문자열을 사용하는지 확인해야 합니다.

- 트랩 대상을 추가하려면 * Create * 를 선택합니다.
- 트랩 대상을 편집하려면 라디오 버튼을 선택하고 * 편집 * 을 선택합니다.
- 트랩 대상을 제거하려면 라디오 버튼을 선택하고 * 제거 * 를 선택합니다.
- 변경 내용을 적용하려면 페이지 맨 아래에 있는 * 저장 * 을 선택합니다.

6. 상담원 주소를 업데이트하려면 기타 구성 섹션에서 상담원 주소 탭을 선택합니다.

   이 탭을 사용하여 하나 이상의 "수신 주소"를 지정할 수 있습니다. SNMP 에이전트가 쿼리를 수신할 수 있는 StorageGRID 주소입니다.

   입력할 항목에 대한 자세한 내용은 을 "에이전트 주소를 만듭니다"참조하십시오.

   - 상담원 주소를 추가하려면 * 생성 * 을 선택합니다.
   - 상담원 주소를 편집하려면 라디오 버튼을 선택하고 * 편집 * 을 선택합니다.
   - 상담원 주소를 제거하려면 라디오 단추를 선택하고 * 제거 * 를 선택합니다.
   - 변경 내용을 적용하려면 페이지 맨 아래에 있는 * 저장 * 을 선택합니다.

7. USM 사용자를 업데이트하려면 Other configuration(기타 구성) 섹션에서 USM users(USM 사용자) 탭을 선택합니다.

   이 탭을 사용하여 MIB를 쿼리하거나 트랩 및 알림을 받을 권한이 있는 USM 사용자를 정의합니다.

   입력할 항목에 대한 자세한 내용은 을 "USM 사용자를 생성합니다"참조하십시오.

   - USM 사용자를 추가하려면 * Create * 를 선택합니다.
   - USM 사용자를 편집하려면 라디오 버튼을 선택하고 * 편집 * 을 선택합니다.

     기존 USM 사용자의 사용자 이름을 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 대상을 편집하거나 제거해야 합니다. 그렇지 않으면 SNMP 에이전트 구성을 저장할 때 유효성 검사 오류가 발생합니다.

   - USM 사용자를 제거하려면 라디오 버튼을 선택하고 * 제거 * 를 선택합니다.

     > 제거한 사용자가 트랩 대상에 대해 현재 선택된 경우 대상을 편집하거나 제거해야 합니다. 그렇지 않으면 SNMP 에이전트 구성을 저장할 때 유효성 검사 오류가 발생합니다.

   - 변경 내용을 적용하려면 페이지 맨 아래에 있는 * 저장 * 을 선택합니다.

8. SNMP 에이전트 구성을 업데이트했으면 * Save * 를 선택합니다.

MIB 파일에 액세스합니다

MIB 파일에는 그리드의 노드에 대한 관리되는 리소스 및 서비스의 속성에 대한 정의 및 정보가 들어 있습니다. StorageGRID에 대한 객체 및 알림을 정의하는 MIB 파일에 액세스할 수 있습니다. 이러한 파일은 그리드를 모니터링하는 데 유용할 수 있습니다.

SNMP 및 MIB 파일에 대한 자세한 내용은 을 "SNMP 모니터링을 사용합니다"참조하십시오.

MIB 파일에 액세스합니다

MIB 파일에 액세스하려면 다음 단계를 수행하십시오.

단계

1. 구성 * > * 모니터링 * > * SNMP 에이전트 * 를 선택합니다.
2. SNMP 에이전트 페이지에서 다운로드할 파일을 선택합니다.
   - * NetApp-StorageGrid-MIB.txt *: 모든 관리 노드에서 액세스할 수 있는 알림 테이블 및 알림(트랩)을 정의합니다.
   - * ES-NetApp-06-MIB.MIB *: E-Series 기반 어플라이언스에 대한 객체 및 알림을 정의합니다.
   - * MIB_1_10.zip *: BMC 인터페이스를 사용하는 어플라이언스에 대한 객체 및 알림을 정의합니다.

   StorageGRID 노드의 다음 위치에서 MIB 파일에 액세스할 수도 있습니다. `/usr/share/snmp/mibs`

3. MIB 파일에서 StorageGRID OID를 추출하려면:
   a. StorageGRID MIB 루트의 OID를 가져옵니다.

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   결과 `.1.3.6.1.4.1.789.28669` (`28669`: 항상 StorageGRID의 OID입니다.)

   a. 전체 트리에서 StorageGRID OID에 대한 GRIP(라인 합치기 위해 사용 `paste`):

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

`snmptranslate`명령에는 MIB를 탐색하는 데 유용한 여러 옵션이 있습니다. 이 명령은 모든 StorageGRID 노드에서 사용할 수 있습니다.

MIB 파일 내용

모든 객체는 StorageGRID OID 아래에 있습니다.

개체 이름	**OID(개체 ID)**	설명
	1.3.6.1.4.1.789.28669	NetApp StorageGRID 엔터티용 MIB 모듈

MIB 개체

개체 이름	**OID(개체 ID)**	설명
활성 경고 수		활성 경고 테이블의 활성 경고 수입니다.

개체 이름	**OID(**개체 **ID)**	설명
활성 경고 테이블		StorageGRID의 활성 경고 테이블
활성 경고 ID입니다		알림의 ID입니다. 현재 활성 알림 집합에서 고유한 항목만 표시됩니다.
활성 경고 이름		알림의 이름입니다.
활성 경고 인스턴스		알림을 생성한 엔터티의 이름, 일반적으로 노드 이름입니다.
활성 경고 심각도		알림의 심각도입니다.
활성 경고 시작 시간		알림이 트리거된 날짜 및 시간입니다.

알림 유형(트랩)

모든 알림은 varbind로 다음 변수를 포함합니다.

- 활성 경고 ID입니다
- 활성 경고 이름
- 활성 경고 인스턴스
- 활성 경고 심각도
- 활성 경고 시작 시간

알림 유형입니다	**OID(**개체 **ID)**	설명
활성 MinorAlert		경미하게 심각도가 있는 경고
활성 MajorAlert		심각도를 나타내는 경고입니다
활성 CriticalAlert		심각도를 나타내는 경고입니다

추가 **StorageGRID** 데이터를 수집합니다

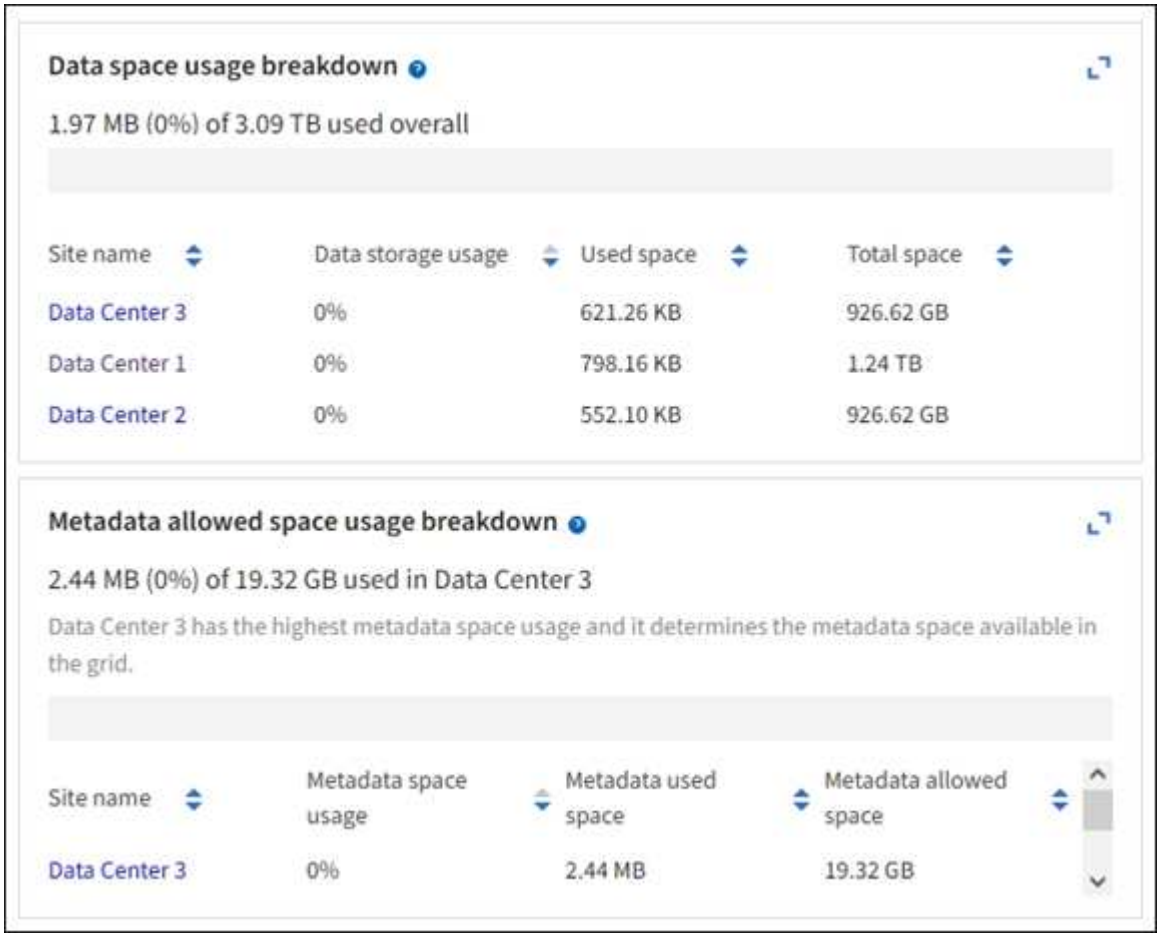
차트와 그래프를 사용합니다

차트와 보고서를 사용하여 StorageGRID 시스템의 상태를 모니터링하고 문제를 해결할 수 있습니다.

Grid Manager는 각 릴리스와 함께 업데이트되며 이 페이지의 예제 스크린샷과 일치하지 않을 수 있습니다.

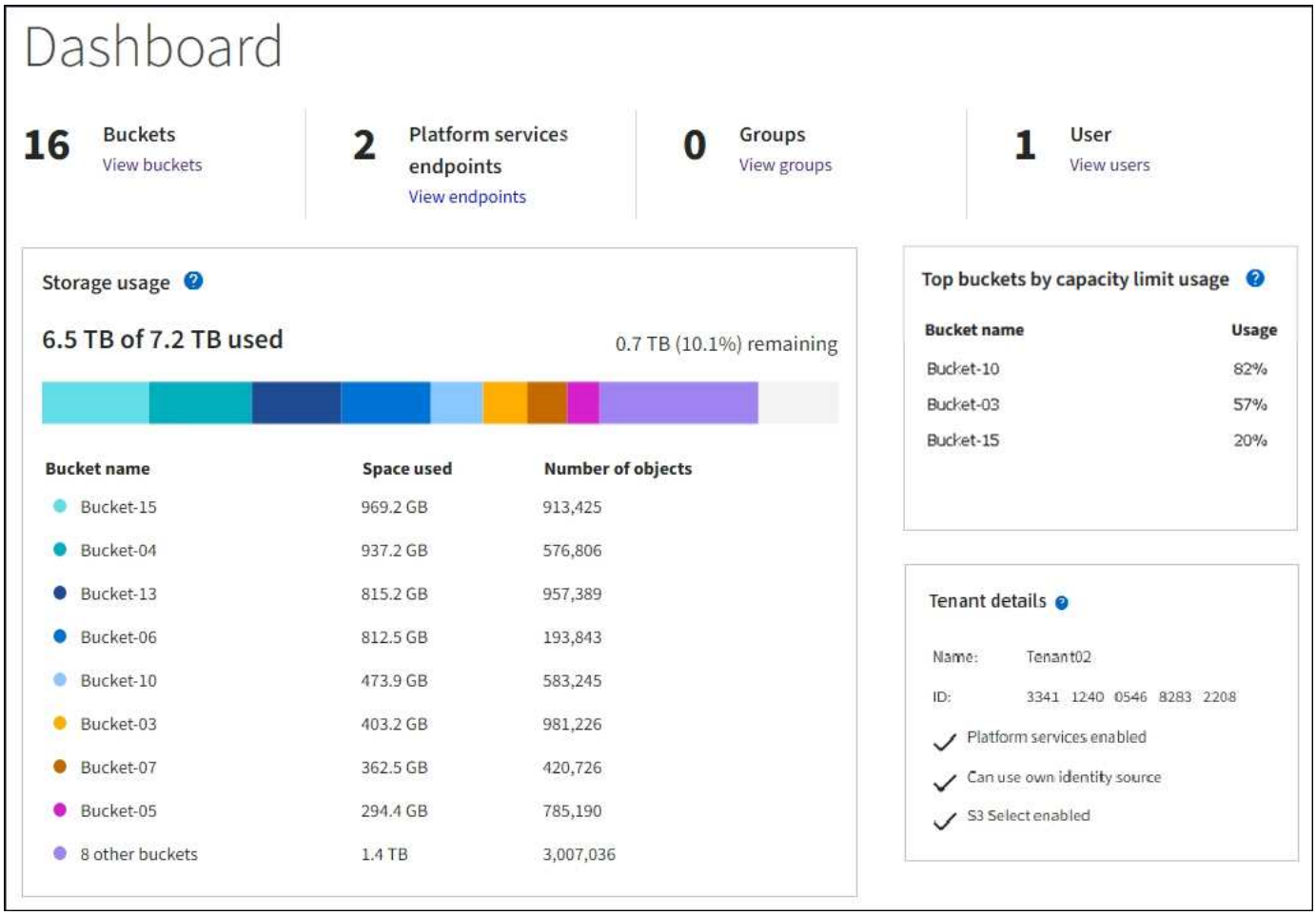
차트와 그래프에는 특정 StorageGRID 메트릭 및 특성의 값이 요약되어 있습니다.

Grid Manager 대시보드에는 그리드 및 각 사이트에 사용할 수 있는 저장소를 요약하는 카드가 포함되어 있습니다.



Tenant Manager 대시보드의 Storage usage 패널에 표시되는 내용은 다음과 같습니다.

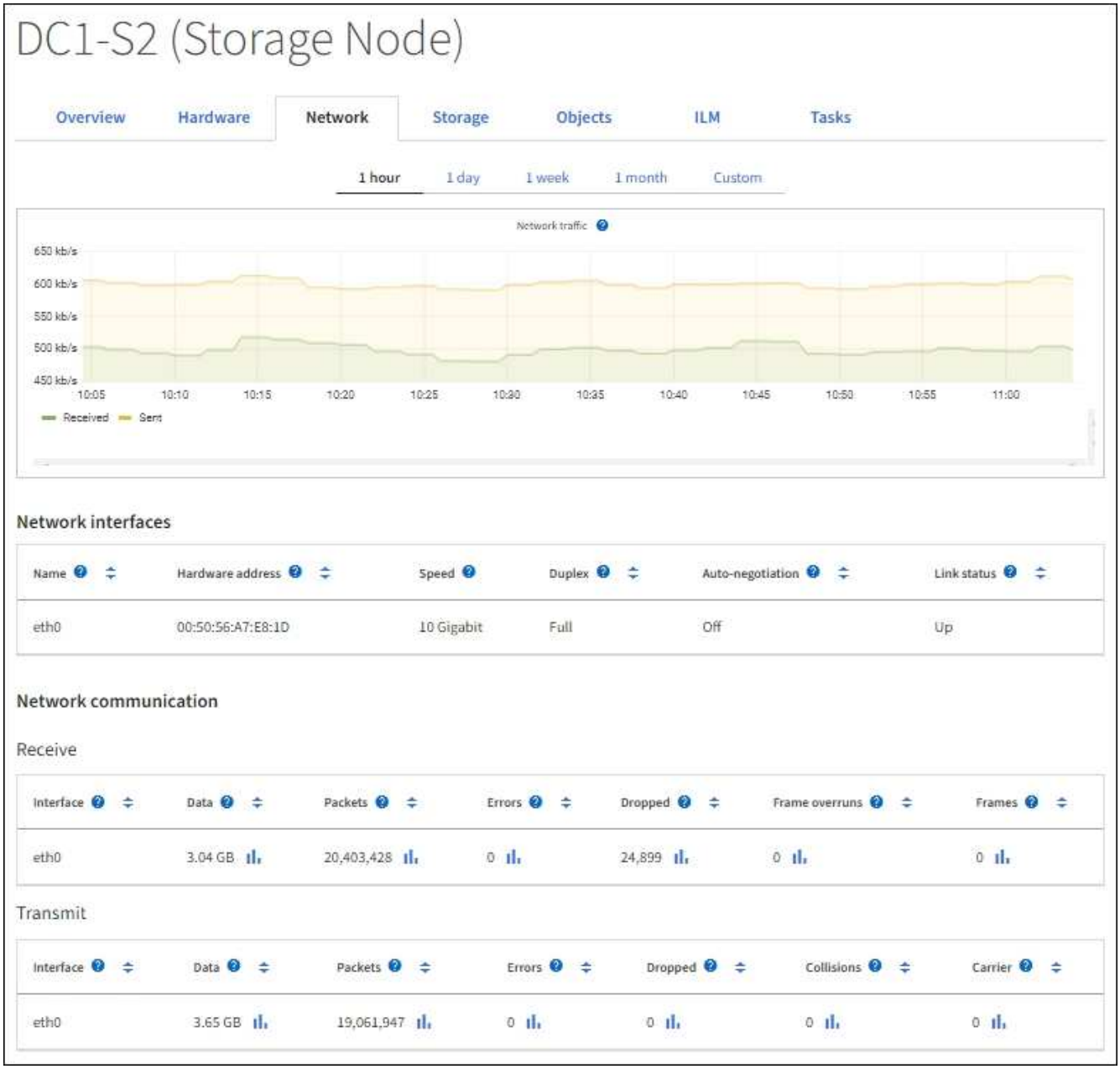
- 테넌트를 위해 가장 큰 버킷(S3) 또는 컨테이너(Swift)의 목록입니다
- 가장 큰 버킷 또는 컨테이너의 상대적 크기를 나타내는 막대 차트
- 사용된 총 공간 및 할당량이 설정된 경우 남은 공간의 양과 백분율이 표시됩니다



또한 노드 페이지 및 * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지에서 StorageGRID 메트릭 및 속성이 시간에 따라 변경되는 방식을 보여 주는 그래프입니다.

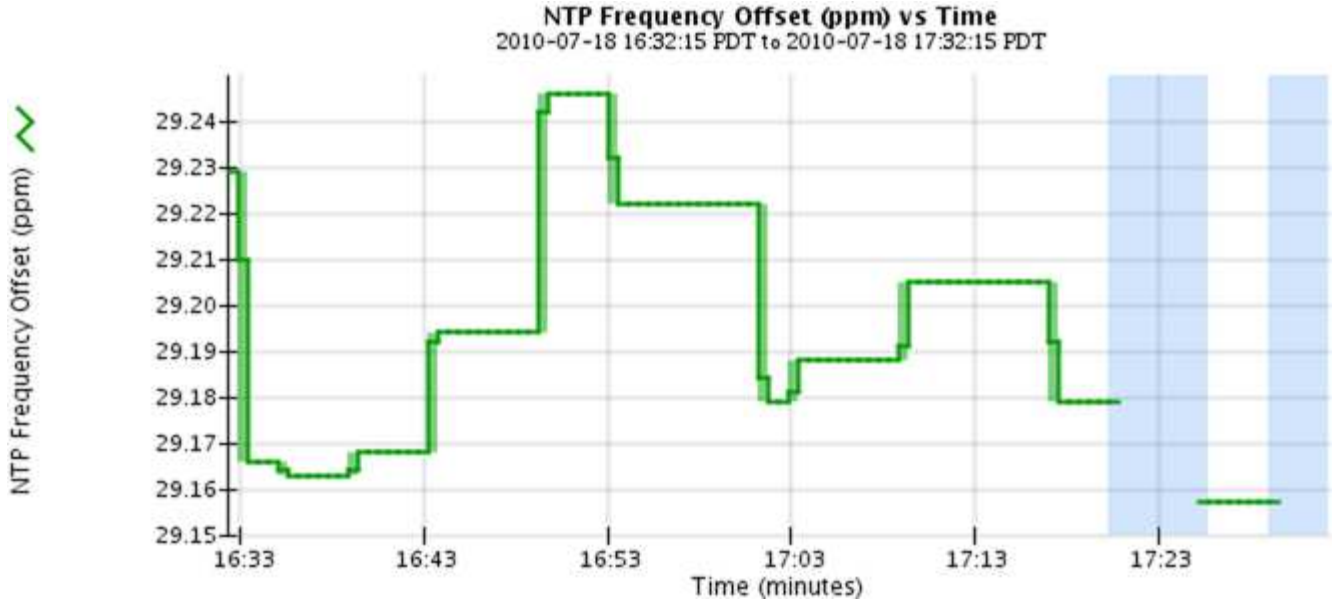
그래프에는 네 가지 유형이 있습니다.

- * 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.

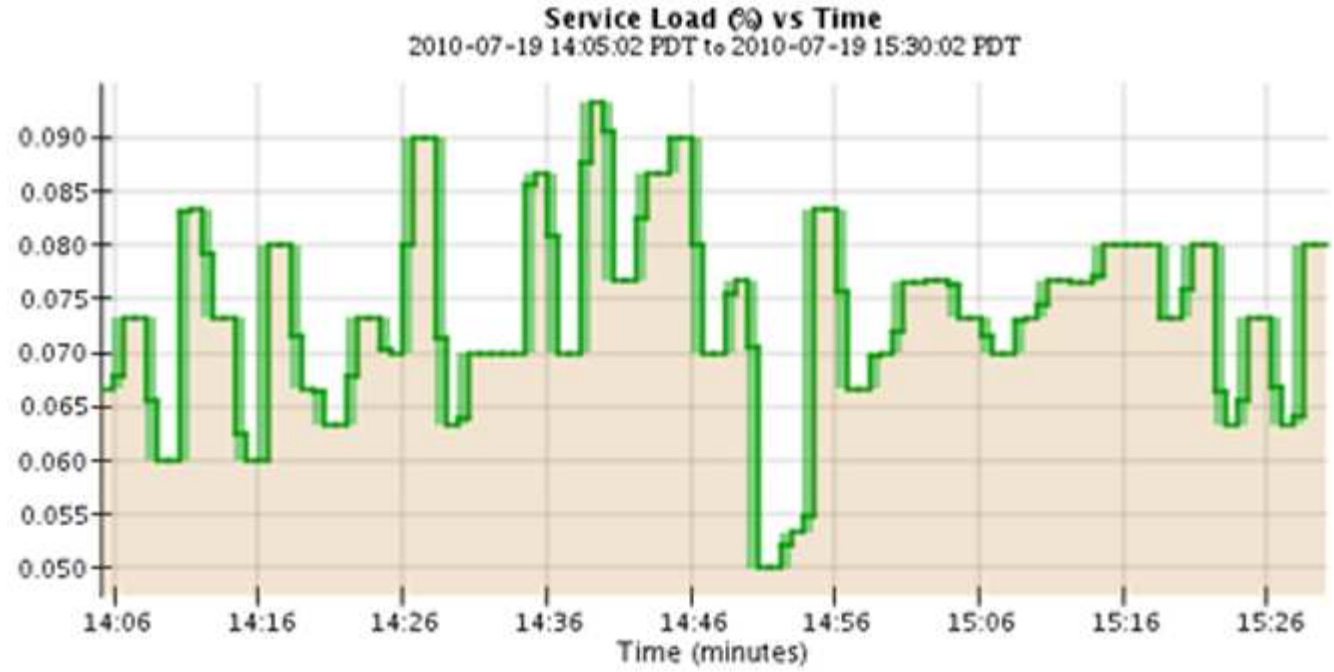


Grafana 차트는 * 지원 * > * 도구 * > * 메트릭 * 페이지에서 사용할 수 있는 사전 구성된 대시보드에도 포함되어 있습니다.

- * 라인 그래프 *: 노드 페이지와 * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지(데이터 값 뒤의 차트 아이콘 선택)에서 사용할 수 있는 라인 그래프는 단위 값이 있는 StorageGRID 속성 값(예: NTP 주파수 오프셋, ppm)을 플로팅하는 데 사용됩니다. 값의 변경 내용은 시간 경과에 따른 정규 데이터 간격(빈)으로 표시됩니다.

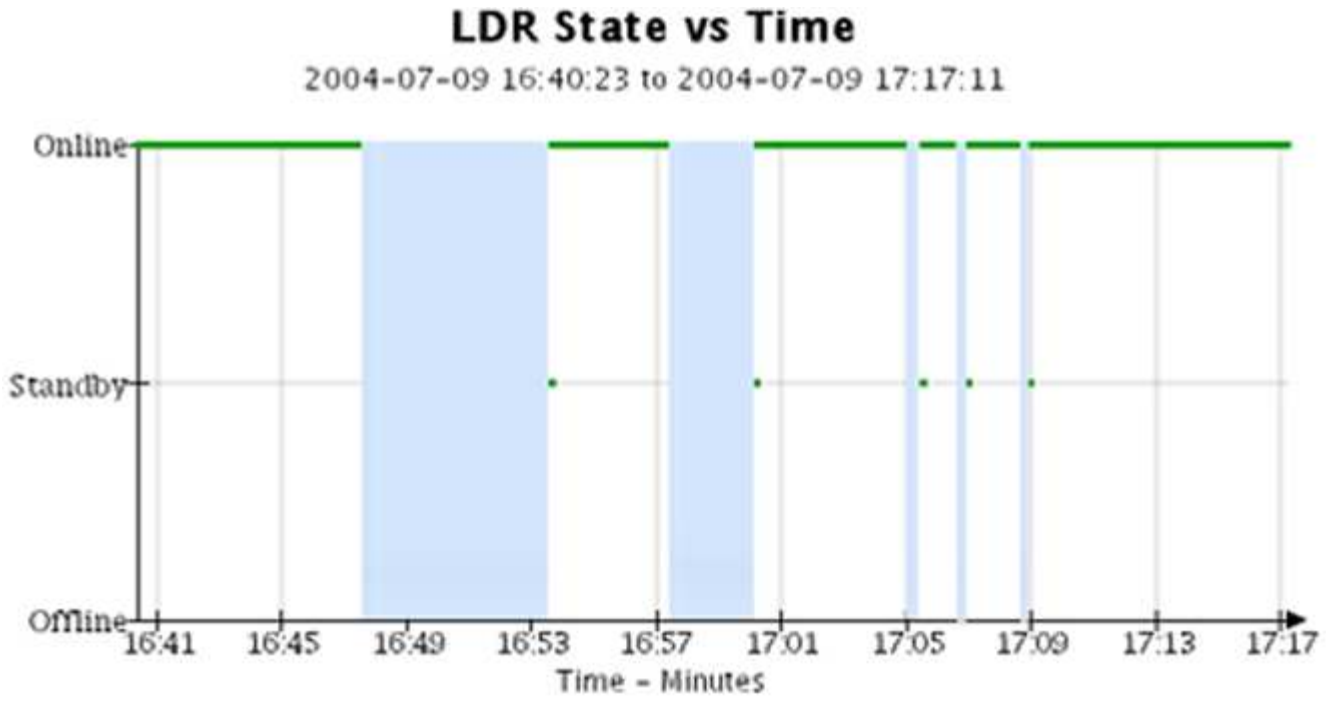


- * 영역 그래프 *: 노드 페이지 및 * 지원 * > * 도구 * > * 그리드 토폴로지 * 페이지(데이터 값 뒤에 차트 아이콘 선택)에서 사용할 수 있으며 영역 그래프는 오브젝트 수 또는 서비스 로드 값과 같은 체적 특성 수량을 플롯하는 데 사용됩니다. 영역 그래프는 선 그래프와 비슷하지만 선 아래에 밝은 갈색 음영을 포함합니다. 값의 변경 내용은 시간 경과에 따른 정규 데이터 간격(빈)으로 표시됩니다.



- 일부 그래프는 다른 유형의 차트 아이콘으로 표시되며 형식이 다릅니다.

- * 상태 그래프 *: * support * > * Tools * > * Grid topology * 페이지(데이터 값 뒤의 차트 아이콘 선택), 상태 그래프는 온라인, 대기 또는 오프라인일 수 있는 서비스 상태와 같은 고유한 상태를 나타내는 특성 값을 플롯하는 데 사용됩니다. 상태 그래프는 선 그래프와 유사하지만 전이는 불연속입니다. 즉, 값이 한 상태 값에서 다른 상태 값으로 이동합니다.

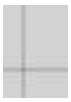


관련 정보

- "노드 페이지를 봅니다"
- "그리드 토폴로지 트리를 봅니다"
- "지원 메트릭을 검토합니다"

차트 범례

차트를 그리는 데 사용되는 선과 색상은 특정한 의미를 갖습니다.

예	의미
	보고된 속성 값은 진한 녹색 선으로 표시됩니다.
	진한 초록색 선 주위의 연한 녹색 음영은 해당 시간 범위의 실제 값이 변하고 빠른 플로팅을 위해 "비닝"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.

시작하기 전에

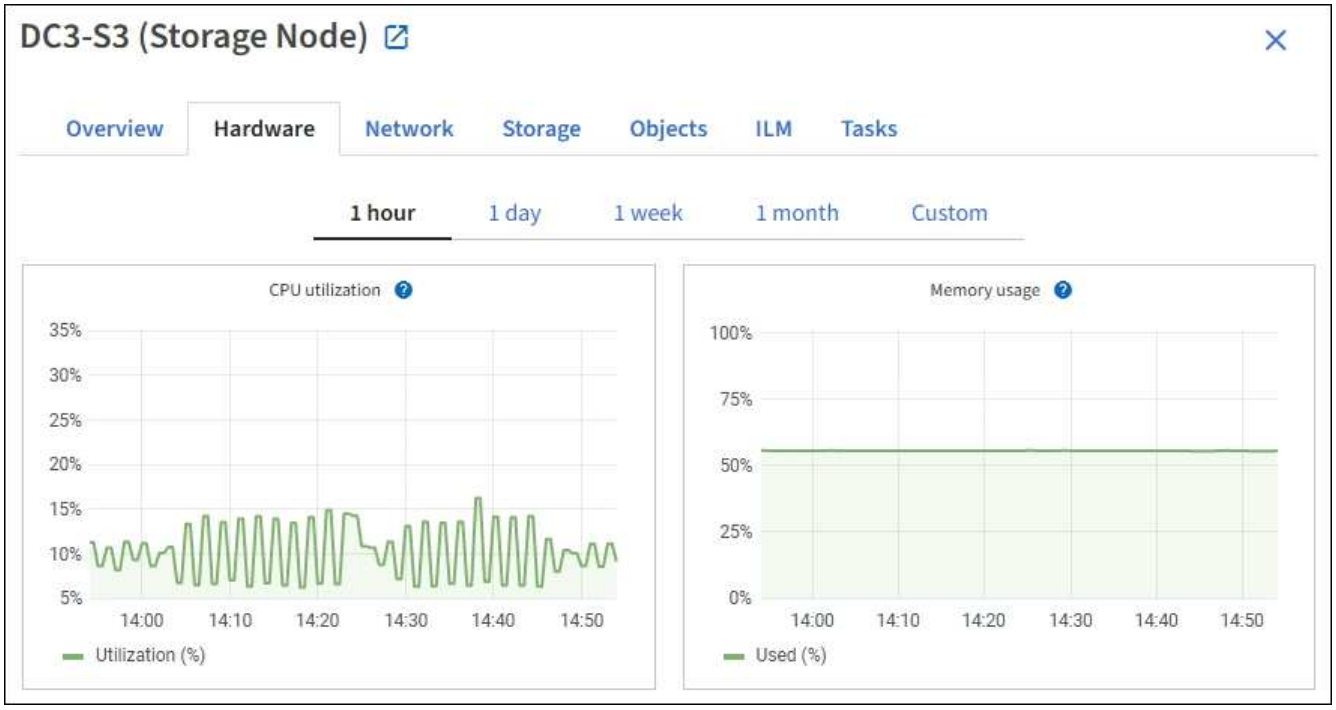
을 사용하여 그리드 관리자에 로그인해야 "지원되는 웹 브라우저"합니다.

단계

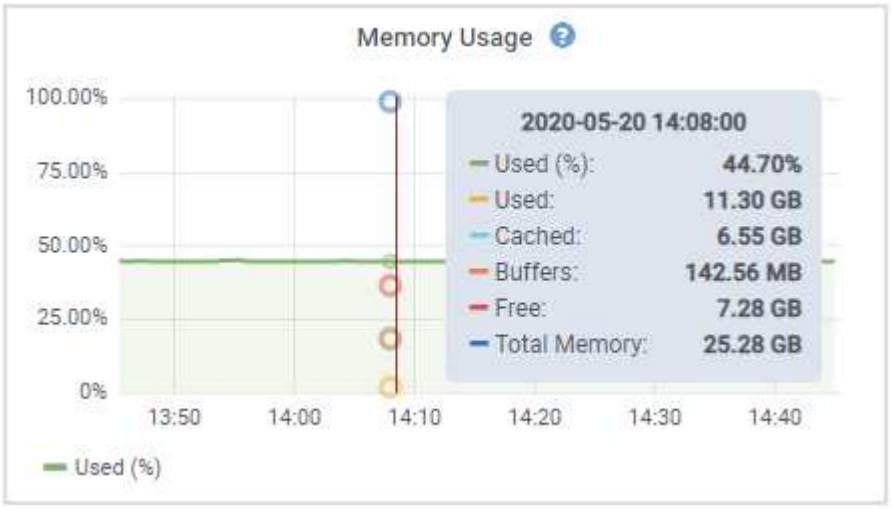
1. 노드 * 를 선택합니다. 그런 다음 노드, 사이트 또는 전체 그리드를 선택합니다.
2. 정보를 보려는 탭을 선택합니다.

   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.



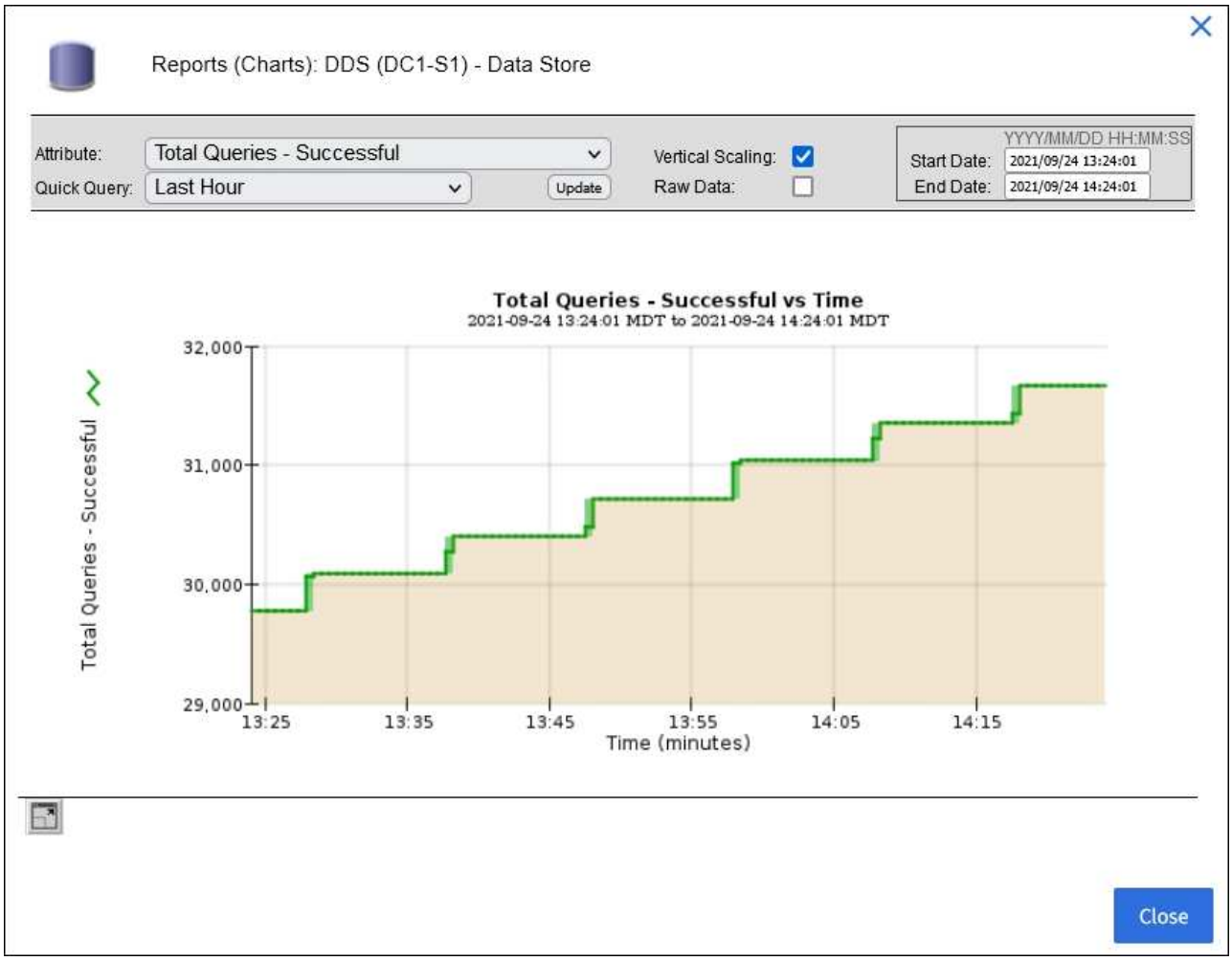
3. 필요에 따라 특정 시점에 대한 보다 자세한 값을 보려면 차트 위에 커서를 놓습니다.

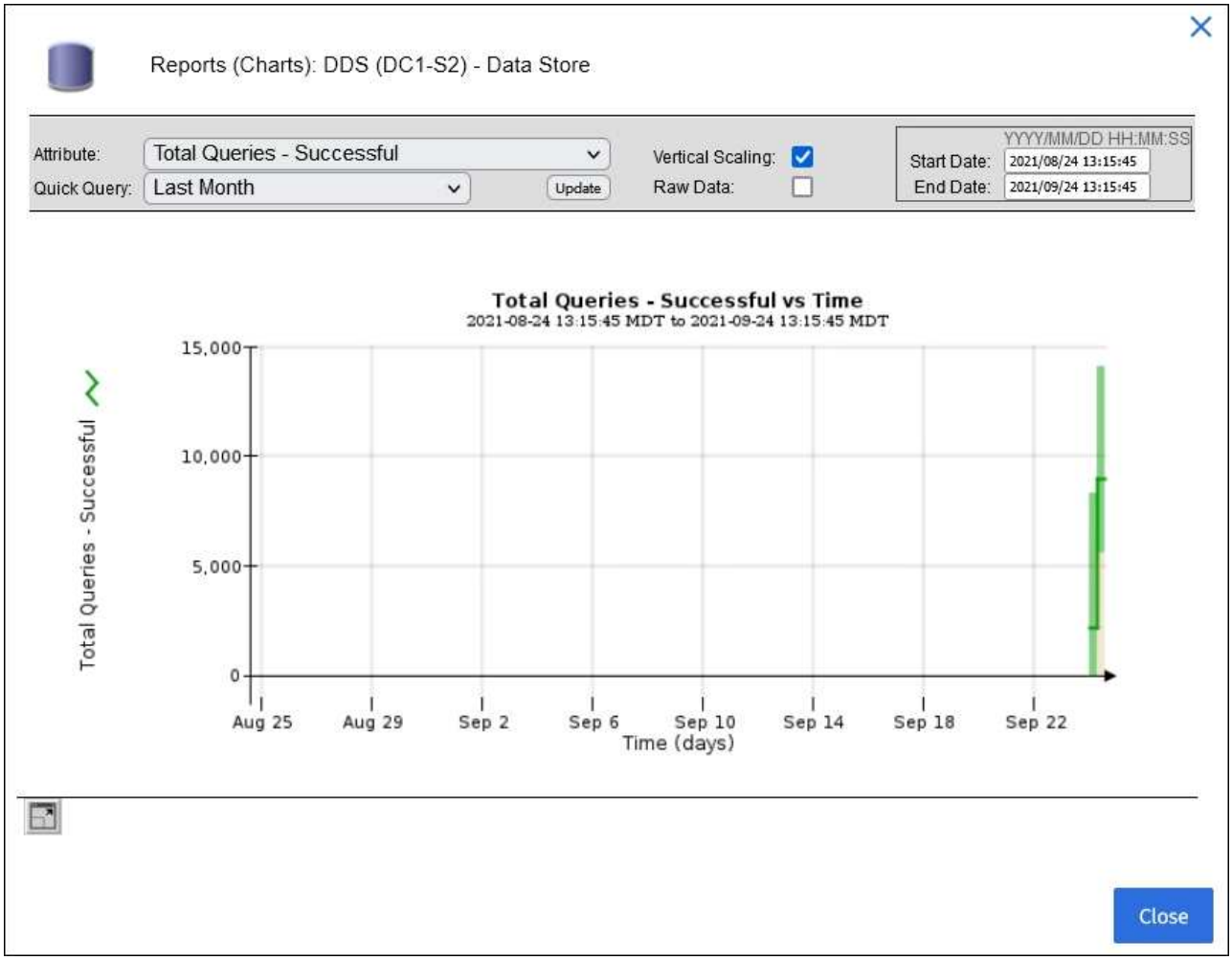


4. 필요에 따라 특정 특성 또는 메트릭에 대한 차트를 표시할 수 있습니다. 노드 페이지의 테이블에서 속성 이름 오른쪽에 있는 차트 아이콘을 선택합니다.

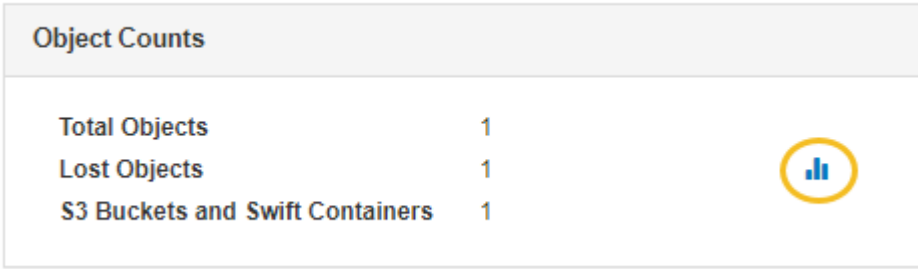
> 일부 메트릭 및 특성에는 차트를 사용할 수 없습니다.

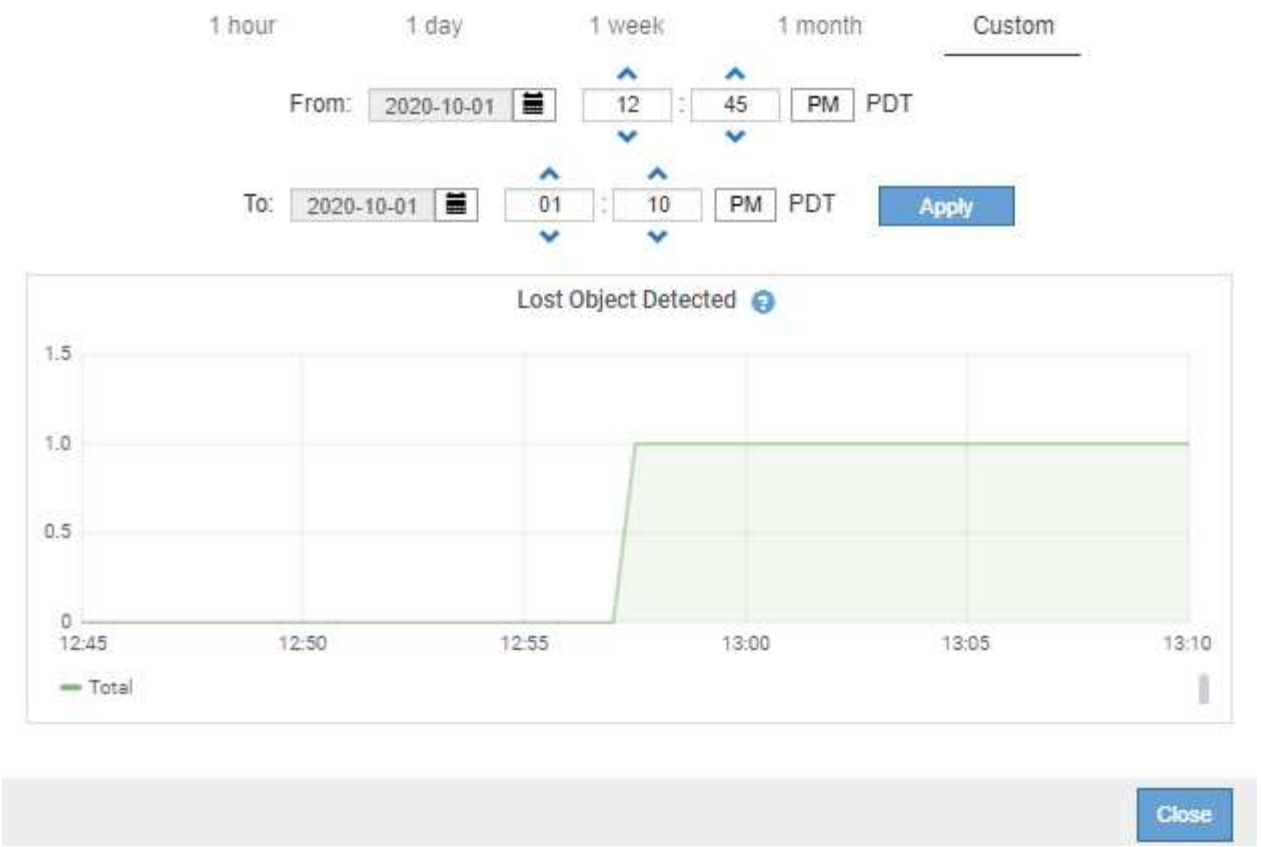
◦ 예제 1 *: 스토리지 노드의 객체 탭에서 차트 아이콘을 선택하면 스토리지 노드에 대해 성공한 총 메타데이터 저장소 쿼리 수를 볼 수 있습니다.


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

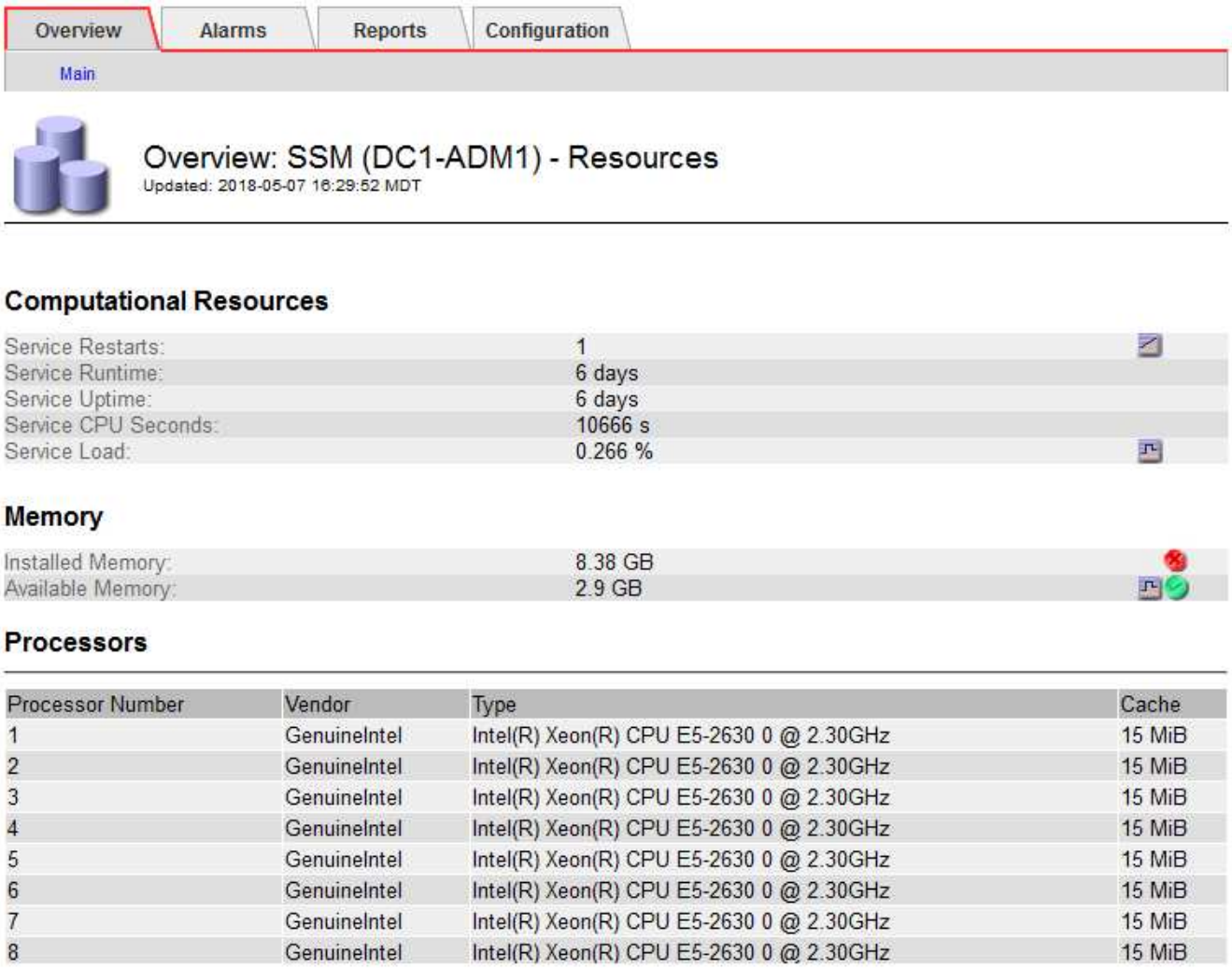


◦ 예제 2 *: 스토리지 노드의 개체 탭에서 차트 아이콘을 선택하면 시간이 지남에 따라 감지된 손실된 개체 수의 그래파나 그래프가 표시됩니다.





5. 노드 페이지에 표시되지 않은 특성에 대한 차트를 표시하려면 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
6. grid node_ * > * *component* 또는 *service* * > * Overview * > * Main * 을 선택합니다.



7. 속성 옆에 있는 차트 아이콘을 선택합니다.

   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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인해야 "지원되는 웹 브라우저"합니다.
- 있습니다. "특정 액세스 권한"

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 * 확인란의 선택을 취소합니다.

5. 값을 전체 정밀도로 표시하려면 * Raw Data * 확인란을 선택하거나 값을 최대 3자리(예: 비율로 보고된 속성)로 반올림하려면 * Raw Data * 확인란의 선택을 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 시간으로 형식을 *YYYY/MM/DDHH:MM:SS* 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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인해야 "지원되는 웹 브라우저"합니다.
- 있습니다. "특정 액세스 권한"

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 * Raw Data * 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 시간으로 형식을 `YYYY/MM/DDHH:MM:SS` 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

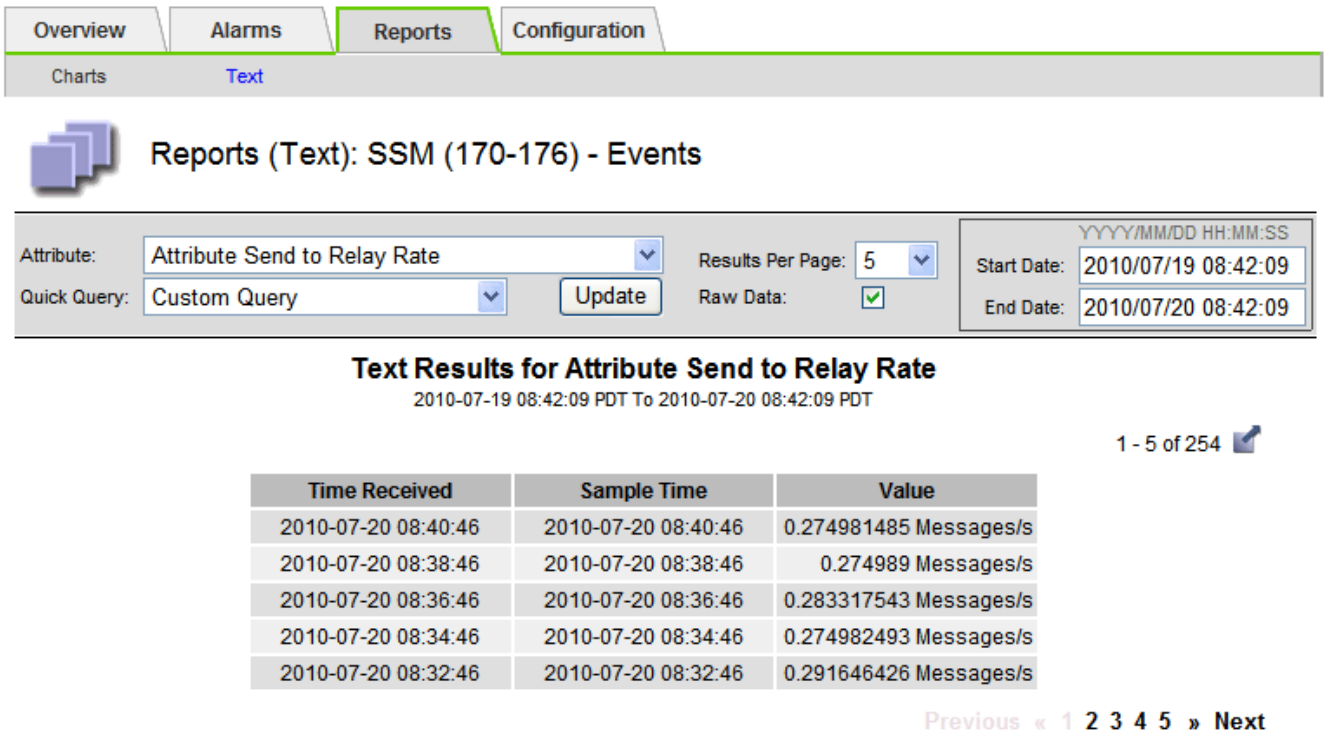
내보낸 텍스트 보고서는 데이터를 선택하고 복사할 수 있는 새 브라우저 탭을 엽니다.

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: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
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 S3테스터 애플리케이션을 사용하여 S3 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

의 "감사 로그"메시지는 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. 또한 삭제, 가져오기, 헤드, 메타데이터 업데이트됨, POST, PUT 등의 S3 작업에 대한 감사 메시지에서 시간 속성을 찾을 수 있습니다

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.

- 할 수 "github에서 S3tester를 다운로드합니다"있습니다.

StorageGRID 시스템은 스토리지 노드에서 오브젝트 데이터의 무결성을 검사하여 손상된 오브젝트와 누락된 오브젝트가 모두 있는지 확인할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.

이 작업에 대해

두 가지 "검증 프로세스" 기능이 함께 작동하여 데이터 무결성을 보장합니다.

- * 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 검증은 클라우드 스토리지 풀의 개체에 대해 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.

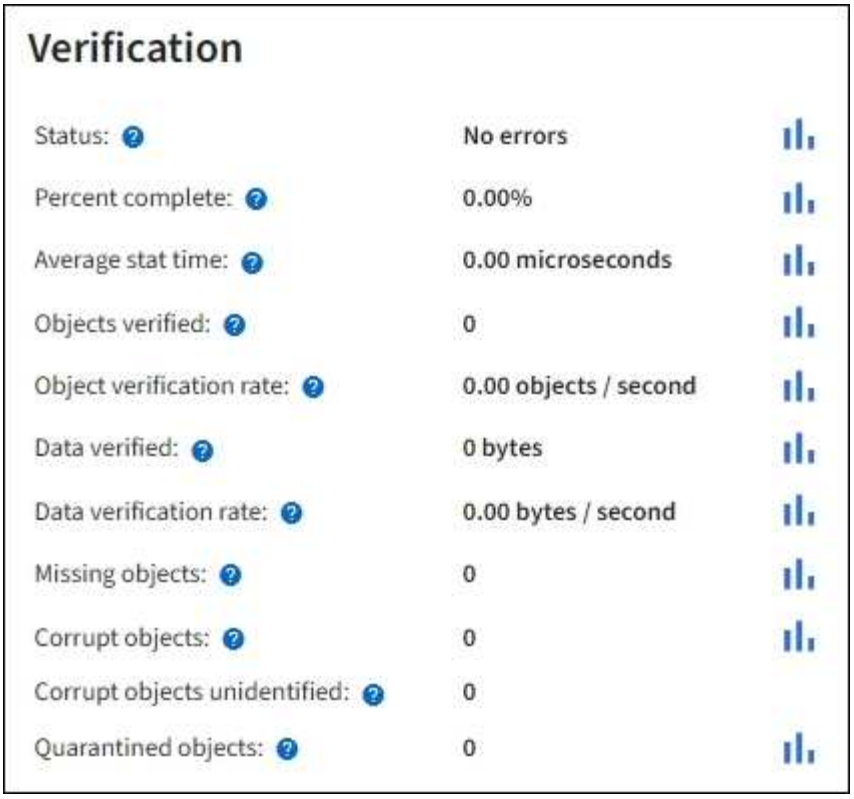
단계

1. 배경 검증에서 얻은 결과를 검토합니다.

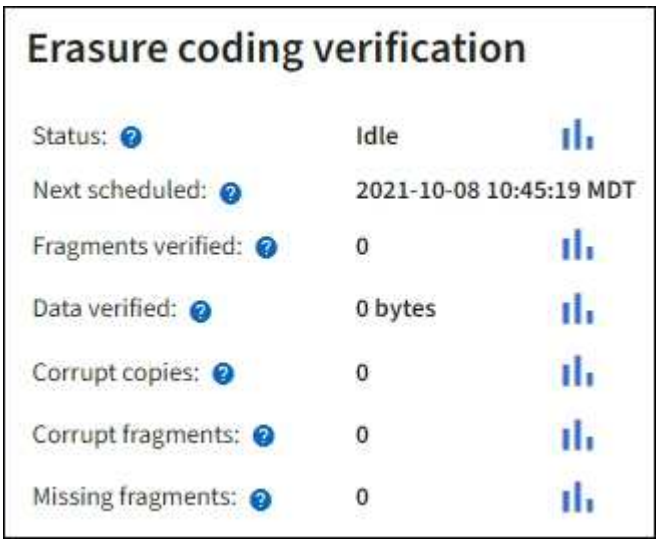
   a. 노드 * > *스토리지 노드 * > * 오브젝트 * 를 선택합니다.

   b. 확인 결과를 확인합니다.

      - 복제된 오브젝트 데이터 검증을 확인하려면 검증 섹션에서 특성을 확인하십시오.

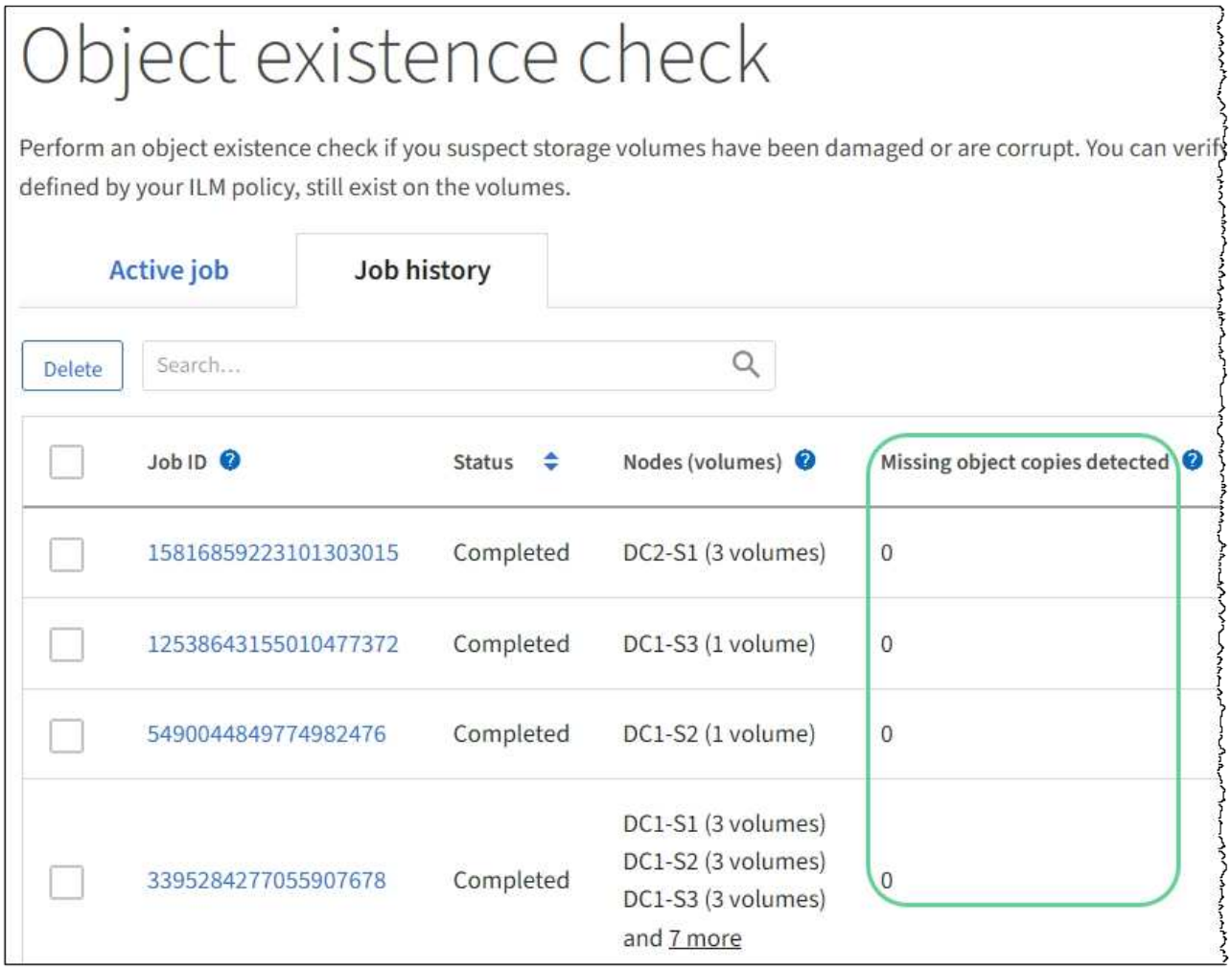


- 삭제 코딩 조각 검증을 확인하려면 * *Storage Node* * > * ILM * 을 선택하고 삭제 코딩 검증 섹션에서 속성을 확인하십시오.



도움말 텍스트를 표시하려면 속성 이름 옆에 있는 물음표를 선택합니다.

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 객체 사본을 생성하고 * Objects Lost * 경고가 트리거된 경우 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 로그 파일에도 `/var/local/log/bycast-err.log` 표시됩니다. 를 "로그 파일 참조 "참조하십시오.

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.

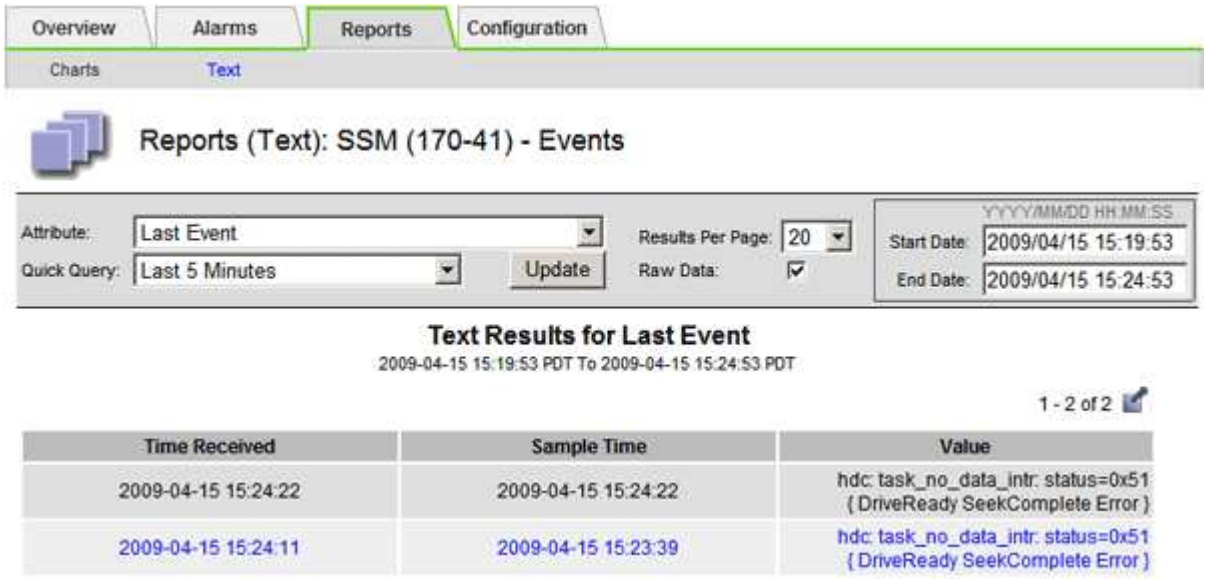
c. 텍스트 * 를 선택합니다.

마지막 이벤트 * 속성은 에 표시되지 "차트 보기"않습니다. 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.

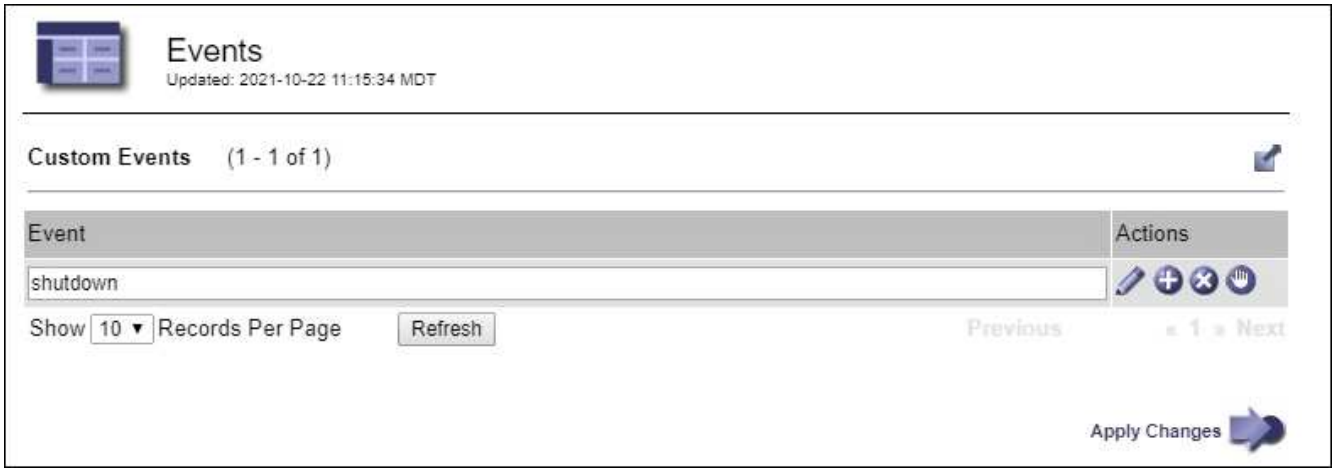
- 사용자 지정 이벤트가 생성되면 이벤트가 발생할 때마다 모니터링됩니다.
- 파일의 키워드를 기반으로 사용자 지정 이벤트를 생성하려면 `/var/local/log/messages` 해당 파일의 로그는 다음과 같아야 합니다.
  - 커널에 의해 생성됩니다
  - 오류 또는 위험 수준에서 데몬 또는 사용자 프로그램에 의해 생성됩니다

참고**:** 파일의 모든 항목이 위에 명시된 요구 사항을 충족하지 않는 한 일치하지는 않습니다 `/var/local/log/messages`.

단계

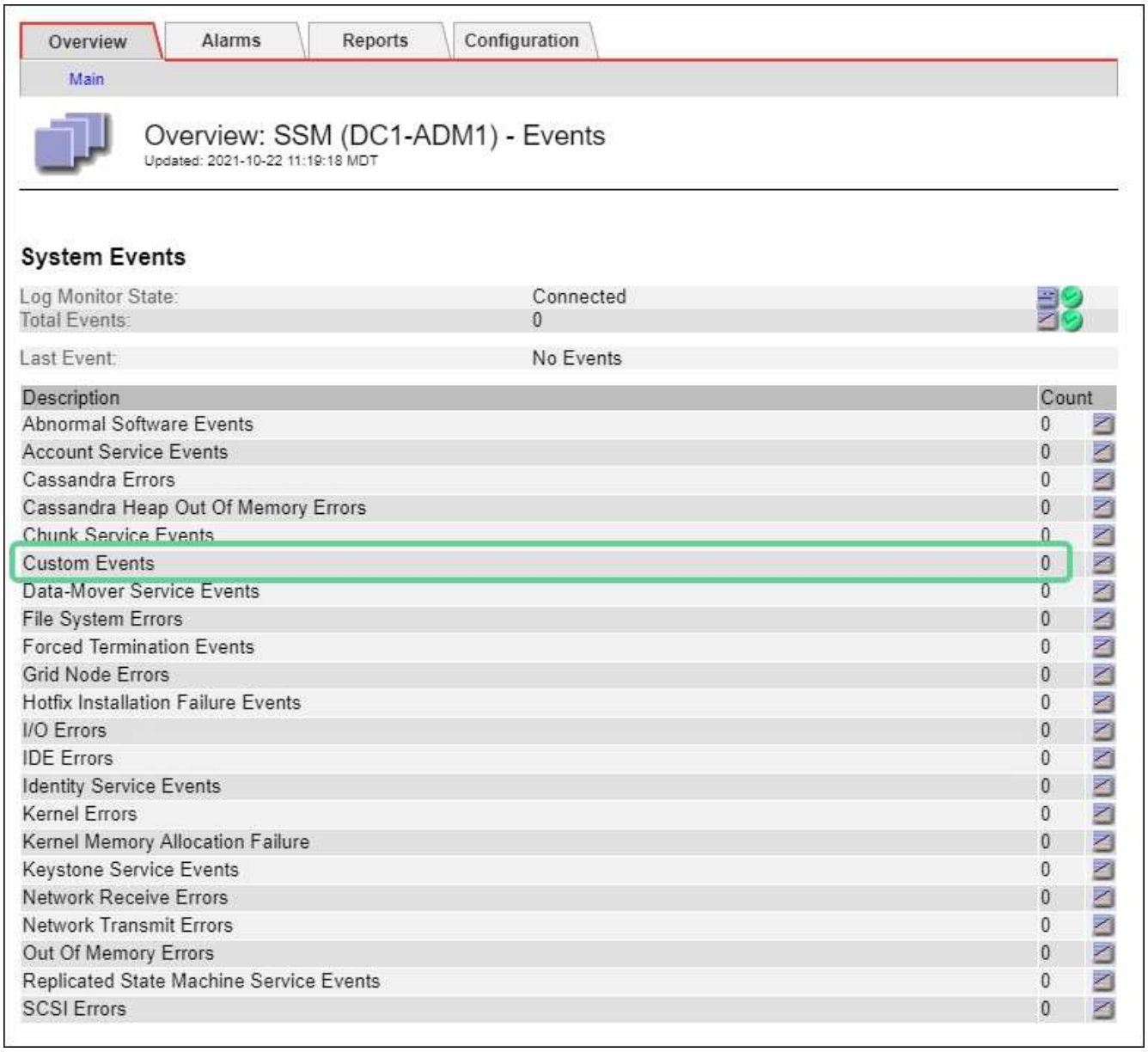
1. 지원 * > * 알람(레거시) * > * 사용자 정의 이벤트 * 를 선택합니다.
2. Edit * (또는 첫 번째 이벤트가 아닌 경우 * Insert *)를 클릭합니다.

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.



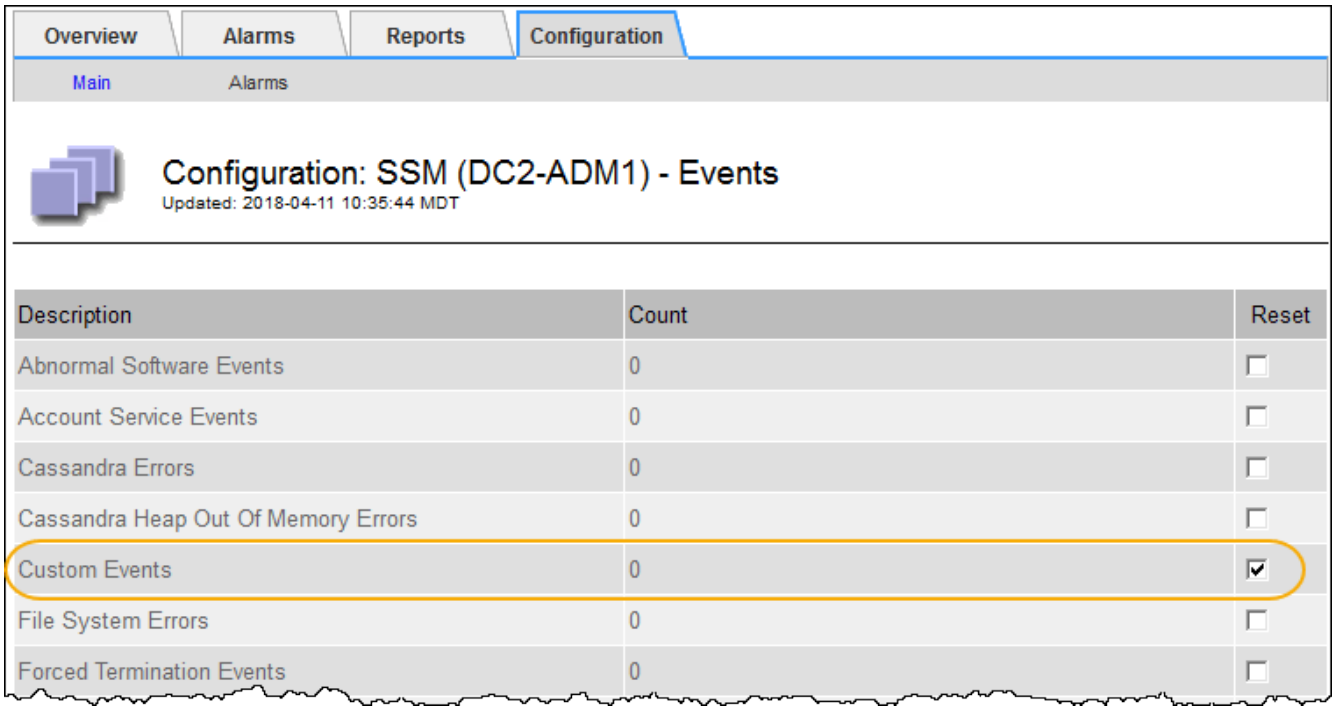
사용자 지정 이벤트 수를 **0**으로 재설정합니다

사용자 지정 이벤트에 대해서만 카운터를 재설정하려면 지원 메뉴의 그리드 토폴로지 페이지를 사용해야 합니다.

카운터를 재설정하면 다음 이벤트에 의해 알람이 트리거됩니다. 반면, 알람을 확인할 때 해당 알람은 다음 임계값 수준에 도달한 경우에만 다시 트리거됩니다.

단계

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.
- 클라이언트 읽기 및 쓰기 감사 메시지는 S3 클라이언트 애플리케이션이 오브젝트를 생성, 수정 또는 검색하도록 요청할 때 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.

관리자 노드의 명령줄에서 직접 감사 로그 파일에 액세스할 수 있습니다.

StorageGRID는 기본적으로 감사 정보를 보내거나 대상을 변경할 수 있습니다.

- StorageGRID의 기본값은 로컬 노드 감사 대상입니다.
- 그리드 관리자 및 테넌트 관리자 감사 로그 항목이 스토리지 노드로 전송될 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.

- "감사 메시지 및 로그 대상 구성에 대해 자세히 알아봅니다"..

감사 로그 파일, 감사 메시지 형식, 감사 메시지 유형 및 감사 메시지 분석에 사용할 수 있는 도구에 대한 자세한 내용은 을 참조하십시오."감사 로그를 검토합니다"

로그 파일 및 시스템 데이터를 수집합니다

그리드 관리자를 사용하여 StorageGRID 시스템에 대한 로그 파일 및 시스템 데이터(구성 데이터 포함)를 검색할 수 있습니다.

시작하기 전에

- 를 사용하여 기본 관리자 노드에서 그리드 관리자에 로그인해야 "지원되는 웹 브라우저"합니다.
- 있습니다. "특정 액세스 권한"
- 프로비저닝 암호가 있어야 합니다.

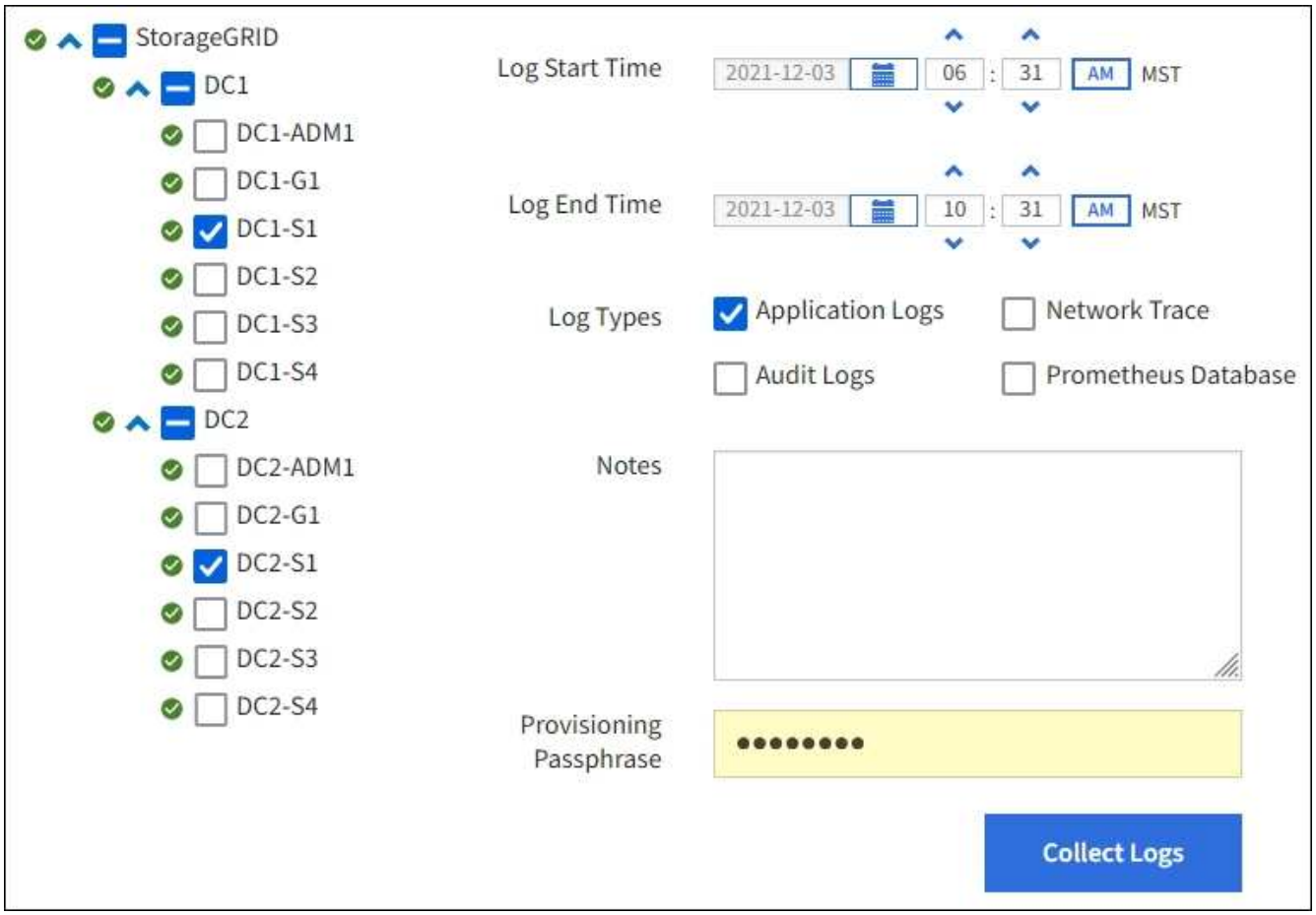
이 작업에 대해

그리드 관리자를 사용하여 "로그 파일"선택한 기간 동안 그리드 노드에서 시스템 데이터 및 구성 데이터를 수집할 수 있습니다. 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 "감사 메시지 및 로그 대상을 구성합니다 "참조하십시오.

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. 로그 파일 수집에 대한 기타 정보와 함께 메모가 이라는 파일에 `info.txt` 추가됩니다. `info.txt`파일이 로그 파일 보관 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 패키지를 수동으로 트리거합니다

StorageGRID 시스템 관련 문제 해결에 대한 기술 지원을 지원하기 위해 AutoSupport 패키지를 수동으로 전송할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인해야 "지원되는 웹 브라우저"합니다.
- 루트 액세스 권한 또는 기타 그리드 구성 권한이 있어야 합니다.

단계

1. 지원 * > * 도구 * > * AutoSupport * 를 선택합니다.
2. 작업 * 탭에서 * 사용자 트리거 AutoSupport 전송 * 을 선택합니다.

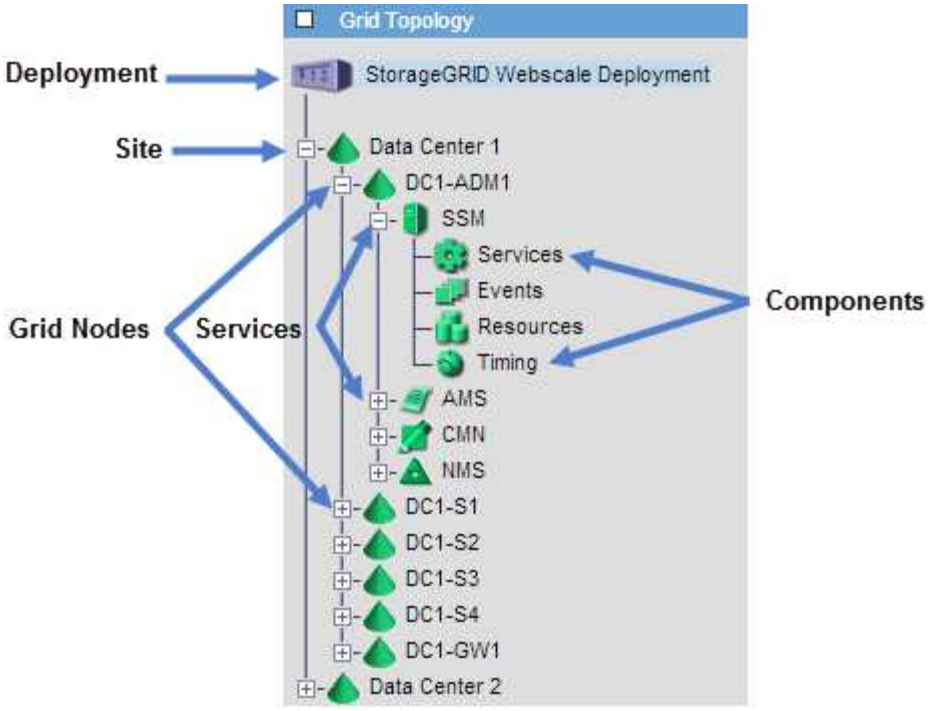
   StorageGRID에서 NetApp Support 사이트로 AutoSupport 패키지 보내기를 시도합니다. 시도가 성공하면 * Results * 탭의 * Most Recent Result * 및 * Last Successful Time * 값이 업데이트됩니다. 문제가 발생하면 * Most latest result * 값이 "Failed"로 업데이트되고 StorageGRID는 AutoSupport 패키지를 다시 보내지 않습니다.

   사용자가 트리거한 AutoSupport 패키지를 보낸 후 1분 후에 브라우저에서 AutoSupport 페이지를 새로 고쳐 최신 결과에 액세스합니다.

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 사이트, 노드 또는 서비스 수준에서 또는 ⊟를 클릭합니다⊞. 전체 사이트 또는 각 노드의 모든 항목을 확장하거나 축소하려면 * <Ctrl> * 키를 누른 상태에서 클릭합니다.

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.)
- * 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.

지원 메트릭을 검토합니다

문제를 해결할 때 기술 지원 팀과 협력하여 StorageGRID 시스템에 대한 자세한 메트릭 및 차트를 검토할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인해야 "지원되는 웹 브라우저"합니다.
- 있습니다. "특정 액세스 권한"

이 작업에 대해

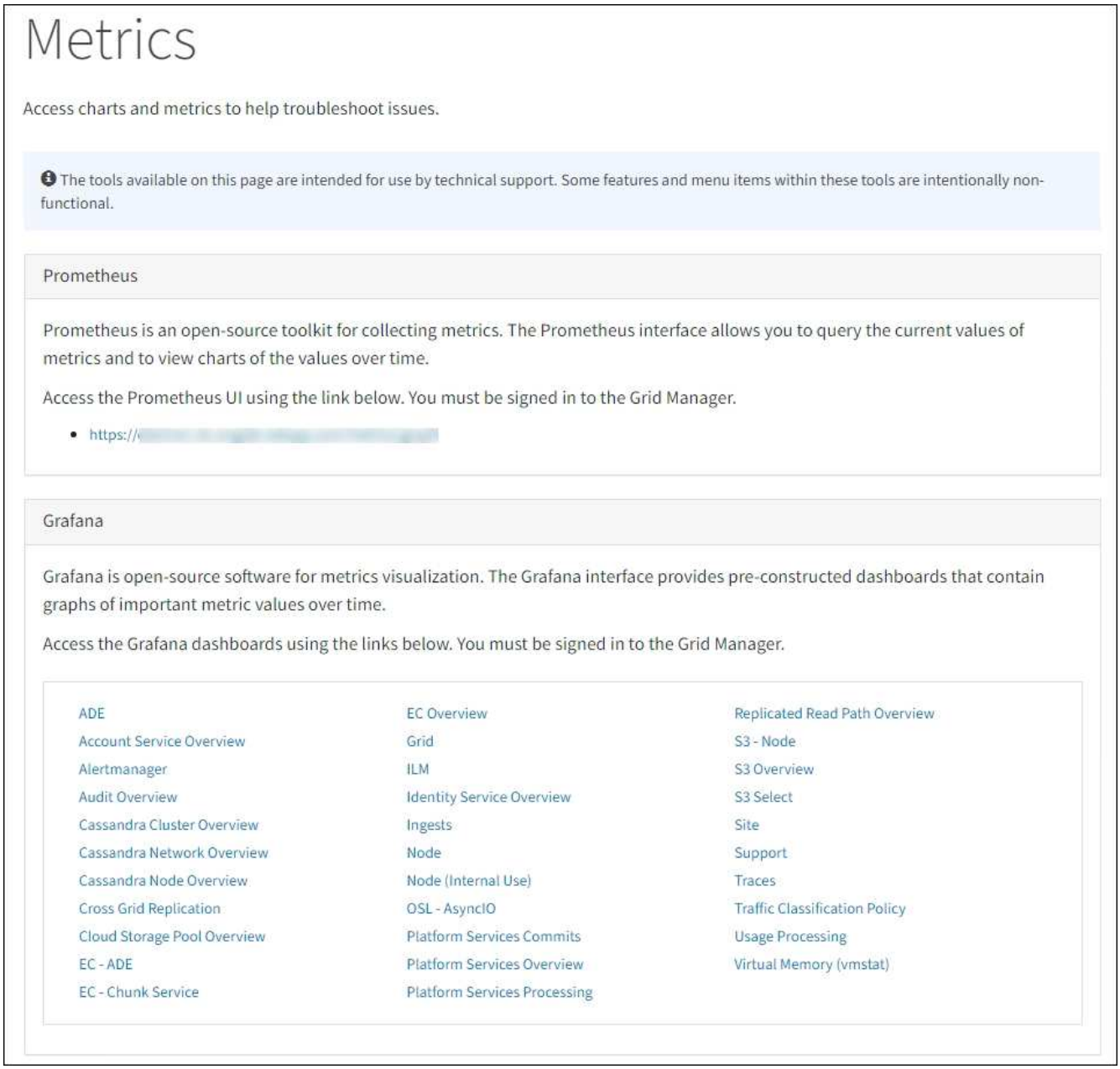
메트릭 페이지에서는 Prometheus 및 Grafana 사용자 인터페이스에 액세스할 수 있습니다. Prometheus는 메트릭 수집을 위한 오픈 소스 소프트웨어입니다. Grafana는 메트릭 시각화를 위한 오픈 소스 소프트웨어입니다.

> 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 "일반적으로 사용되는 Prometheus 메트릭입니다"참조하십시오.

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"

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

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 상당히 벗어났습니다.

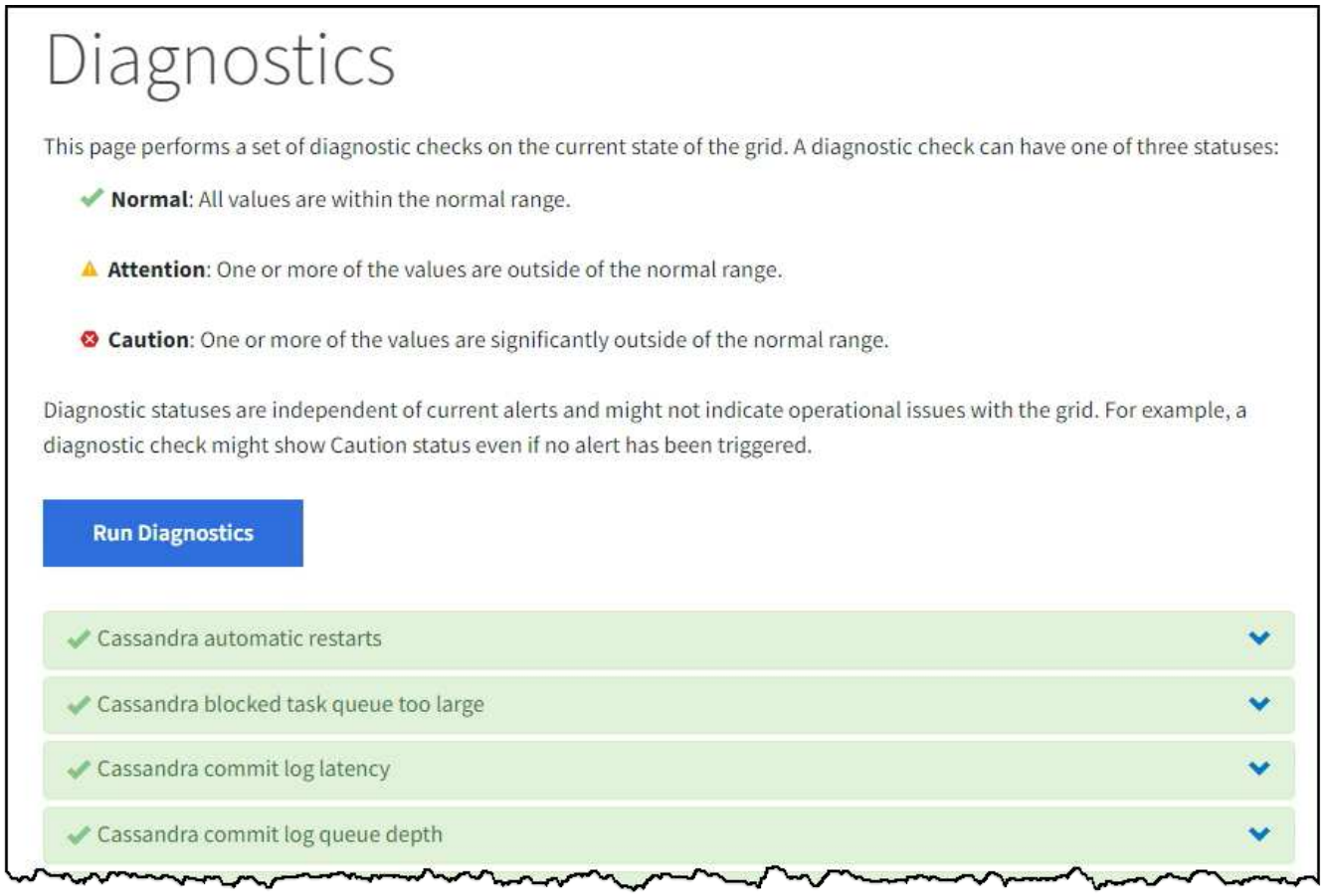
진단 상태는 현재 알림과 독립적이며, 그리드에 작동 문제를 나타내지 않을 수 있습니다. 예를 들어, 경고가 트리거되지 않았더라도 진단 점검에 주의 상태가 표시될 수 있습니다.

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.

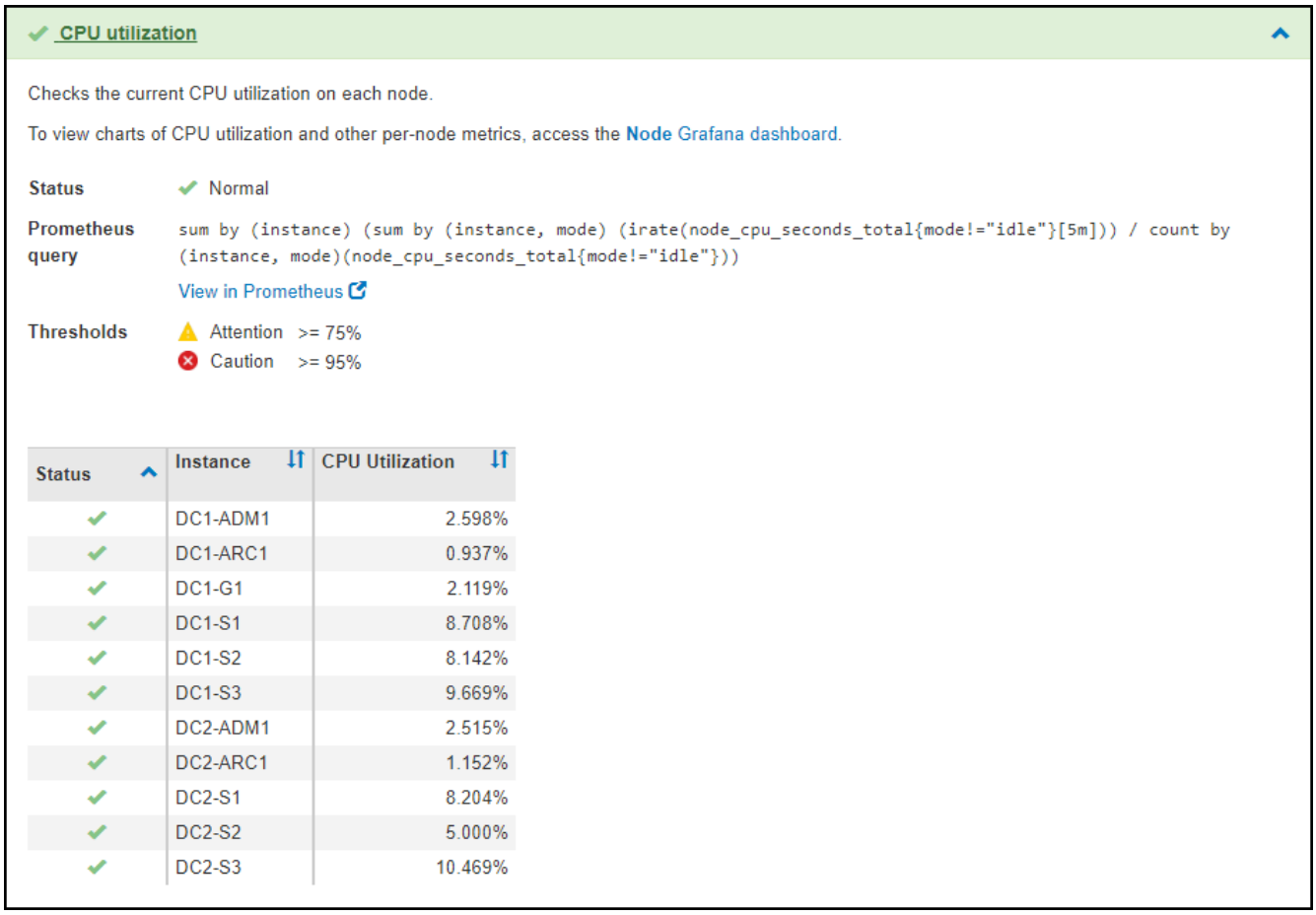
   진단 및 현재 결과에 대한 세부 정보가 나타납니다. 다음 세부 정보가 나열됩니다.

   - * 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.



3. * 선택 사항 *: 이 진단과 관련된 Grafana 차트를 보려면 * Grafana 대시보드 * 링크를 클릭하십시오.

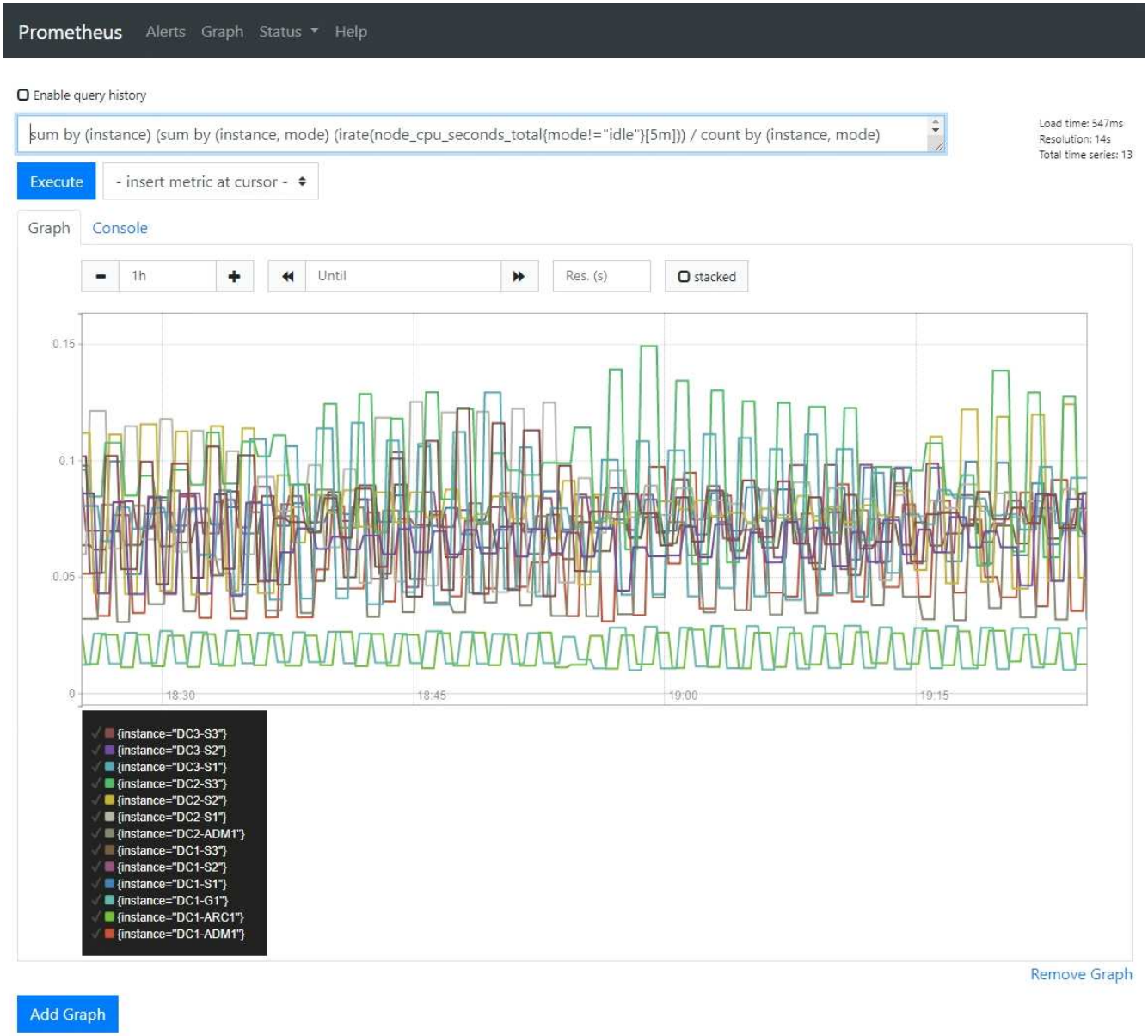
이 링크는 일부 진단 유틸리티에는 표시되지 않습니다.

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.



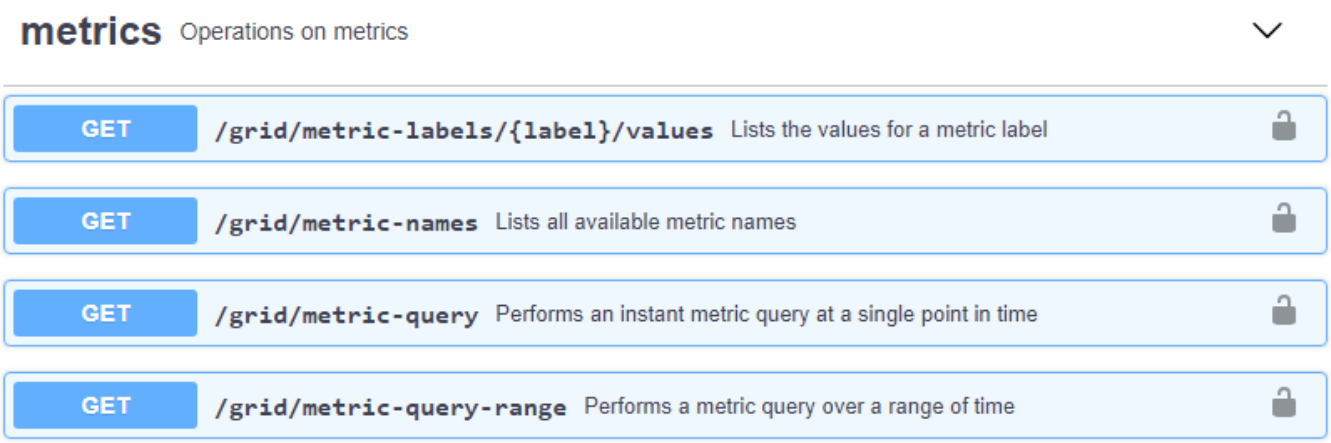
맞춤형 모니터링 애플리케이션을 생성합니다

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 "StorageGRID 관리 지침"참조하십시오.

사용 가능한 메트릭의 전체 목록을 포함하여 메트릭 API 작업을 보려면 Grid Manager로 이동하십시오. 페이지 상단에서 도움말 아이콘을 선택하고 * api documentation * > * metrics * 를 선택합니다.



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.

문제를 직접 해결할 수 있는 경우가 많지만, 기술 지원 부서에 일부 문제를 에스컬레이션해야 할 수도 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	응답의 예
StorageGRID 시스템의 기능은 무엇입니까? 또는 작동하지 않습니다. 증상은 무엇입니까?	클라이언트 애플리케이션이 객체를 StorageGRID로 인제스트할 수 없다고 보고합니다.
문제가 언제 시작되었습니까?	2020년 1월 8일 약 14:50에 오브젝트 수집이 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.

질문	응답의 예
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	응답의 예
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 애플리케이션은 StorageGRID 시스템에 객체를 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
알림을 검토합니다	알림은 원인일 수 있는 근본 문제에 대한 중요한 단서를 제공하여 문제의 근본 원인을 빠르게 파악하는 데 도움이 될 수 있습니다. 현재 알림 목록을 검토하여 StorageGRID에서 문제의 근본 원인을 식별했는지 확인합니다. 과거에 트리거된 알림을 검토하여 추가 정보를 확인합니다.	• "현재 및 해결된 경고를 봅니다"

수집할 데이터의 유형입니다	이 데이터를 수집하는 이유	지침
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"
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 패키지를 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?
- StorageGRID 시스템 또는 환경에 다른 변경 사항이 있습니까?

기준 설정

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. 커서를 차트 위에 올려 놓으면 매일 사용되는 메타데이터 스토리지가 얼마나 되는지 추정할 수 있습니다 전체 시스템 또는 특정 데이터 센터에 대해 이 정보를 수집할 수 있습니다.
S3/Swift 작업의 속도입니다	작업/초	Grid Manager 대시보드에서 * Performance * > * S3 operations * 또는 * Performance * > * Swift operations * 를 선택합니다. 특정 사이트 또는 노드에 대한 수집 및 검색 속도 및 카운트를 보려면 * 노드 * > * _ 사이트 또는 스토리지 노드 _ * > * 개체 * 를 선택합니다. S3에 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 * 평가 비율 * 의 기준값을 추정합니다.
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 개체 * 에 대한 기준 값이 표시됩니다.
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.

- 경고를 사용하여 장애 지점 및 병목 지점을 찾습니다.
- 경고 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

✔	항목	참고
	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? • ILM은 복제된 오브젝트를 만들거나 삭제 코딩 된 오브젝트를 만드는가? ILM이 사이트 중복을 보장합니까? ILM 규칙이 균형, 엄격 또는 이중 커밋 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"
	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 필요할 수 "오브젝트 데이터가 저장되는 위치를 확인합니다"있습니다. 예를 들어, ILM 정책이 예상대로 수행되고 있고 대상 데이터가 원하는 위치에 저장되어 있는지 확인해야 할 수 있습니다.

시작하기 전에

- 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 *: 오브젝트를 를 통해 수집할 때 "S3 인터페이스"클라이언트 애플리케이션은 버켓과 오브젝트 키 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.

   가 "개체 메타데이터 조회 결과"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 보여 줍니다.

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",
```


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

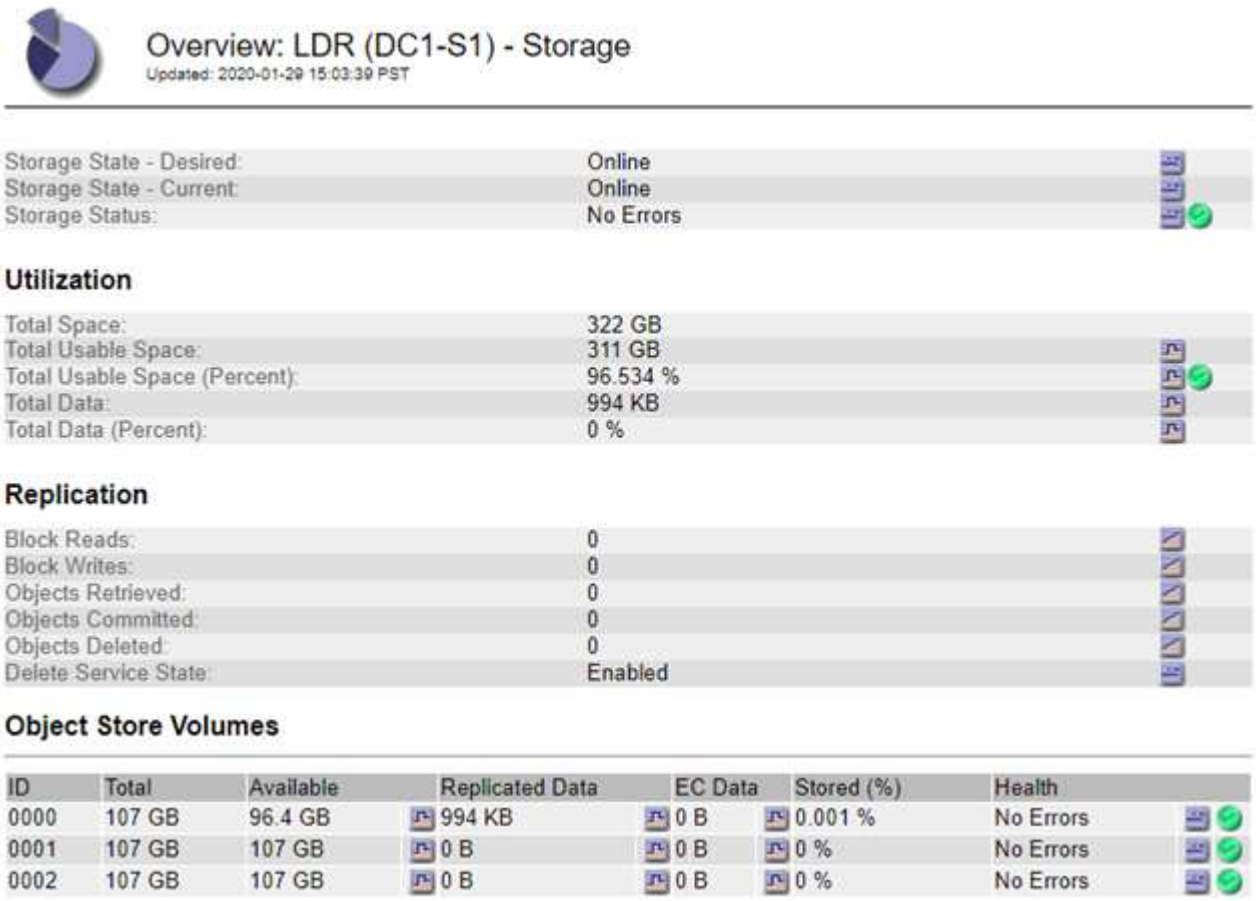
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	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

자세한 내용을 보려면 "각 스토리지 노드에 대한 세부 정보입니다"다음 단계를 따르십시오.

1. 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다.
2. site_ * > **Storage Node* * > * LDR * > * Storage * > * Overview * > * Main * 을 선택합니다.



장애의 특성에 따라 스토리지 볼륨의 장애가 에 반영될 수 "스토리지 볼륨 경고"있습니다. 스토리지 볼륨에 장애가 발생하면 장애가 발생한 스토리지 볼륨을 복구하여 스토리지 노드를 최대한 빨리 전체 기능으로 복원해야 합니다. 필요한 경우 * 구성 * 탭으로 이동하여 StorageGRID 시스템에서 서버의 전체 복구를 준비하는 동안 데이터 검색에 이 탭을 "스토리지 노드를 읽기 전용 상태로 둡니다"사용할 수 있습니다.

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 활성 ILM 정책을 충족하기 위해 손상되지 않은 새 복사본이 생성되고 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 부서에 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. 클라우드 스토리지 풀의 오브젝트는 검사하지 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 확인과 관련된 경고

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인해야 "지원되는 웹 브라우저"합니다.
- 있습니다. "특정 액세스 권한"

이 작업에 대해

스토리지 노드에서 백그라운드 검증을 위한 검증 비율을 변경할 수 있습니다.

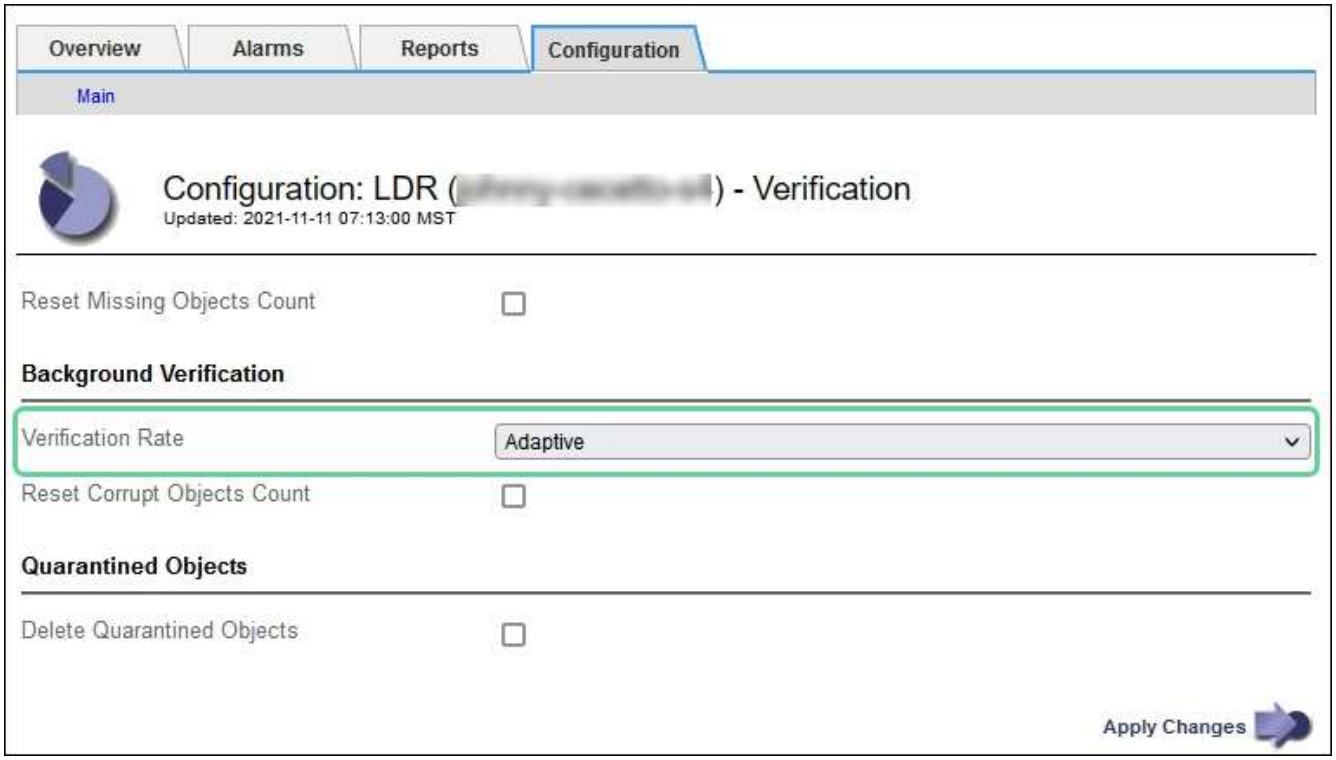
- 적응: 기본 설정. 이 작업은 최대 4MB/s 또는 10개의 오브젝트/s(둘 중 먼저 초과되는 값)에서 확인하도록 설계되었습니다.
- 높음: 일반적인 시스템 작업을 느리게 할 수 있는 속도로 스토리지 검증이 빠르게 진행됩니다.

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.



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 어느 곳에서나 새 복사본을 만들 수 있습니다.
      - 개체 식별자가 손상되어 추출할 수 없는 경우 * 손상된 개체 식별되지 않음 * 메트릭이 증가하고 * 식별되지 않은 손상된 개체가 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.

> Objects Lost * 경고가 트리거된 경우 기술 지원 부서에서는 격리된 개체에 액세스하여 근본적인 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 일관성을 선택할 수도 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"

- 이 "유지 관리 또는 루트 액세스 권한"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

개체 존재 여부 확인 작업은 그리드의 개체 수, 선택한 스토리지 노드와 볼륨 및 선택한 정합성 보장에 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 일관성을 선택합니다.

   일관성은 개체 존재 여부 확인에 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

     일관성에 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.

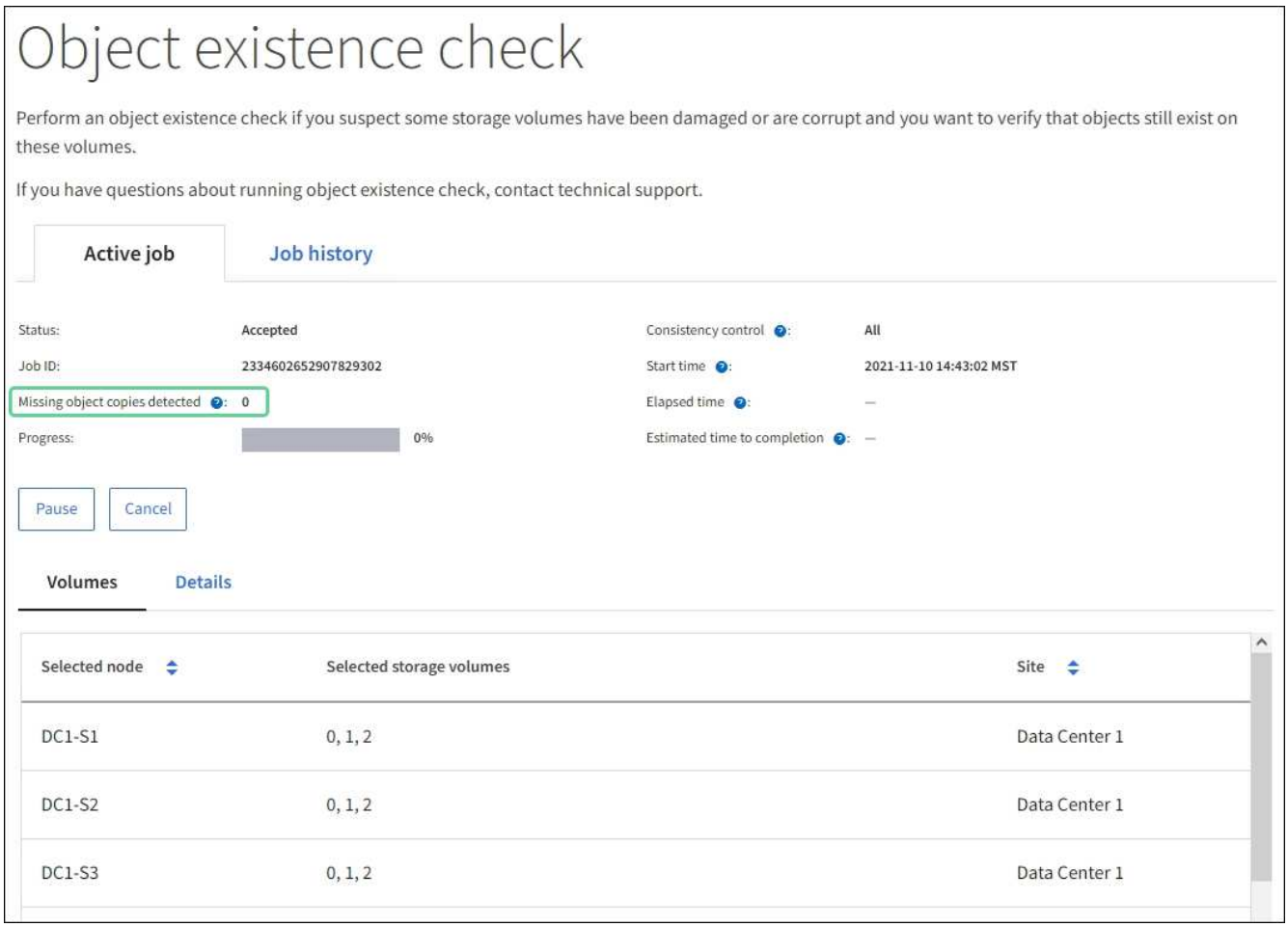
   - 작업이 완료됩니다.
   - 작업을 일시 중지하거나 취소합니다. 일시 중지한 작업은 다시 시작할 수 있지만 취소한 작업은 다시 시작할 수 없습니다.
   - 작업이 멈춥니다. Object existence check has Stallered * 경고가 트리거됩니다. 경고에 지정된 수정 조치를 따릅니다.
   - 작업이 실패합니다. 개체 존재 확인 실패 * 경고가 트리거됩니다. 경고에 지정된 수정 조치를 따릅니다.
   - "서비스를 사용할 수 없음" 또는 "내부 서버 오류" 메시지가 나타납니다. 1분 후 페이지를 새로 고쳐 작업을 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 메시지를 추출하여 손실된 객체 복사본을 조사할 수 있습니다 `grep LLST audit_file_name`.

      이 절차는 의 절차와 비슷하지만 대신"분실된 물체를 조사 중입니다" 검색하는 개체 복사본의 경우 `LLST` 이 `OLST` 절차와 비슷합니다.

12. 작업에 대해 강력한 사이트 또는 강력한 글로벌 일관성을 선택한 경우 메타데이터 일관성을 위해 약 3주를 기다린 다음 같은 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.

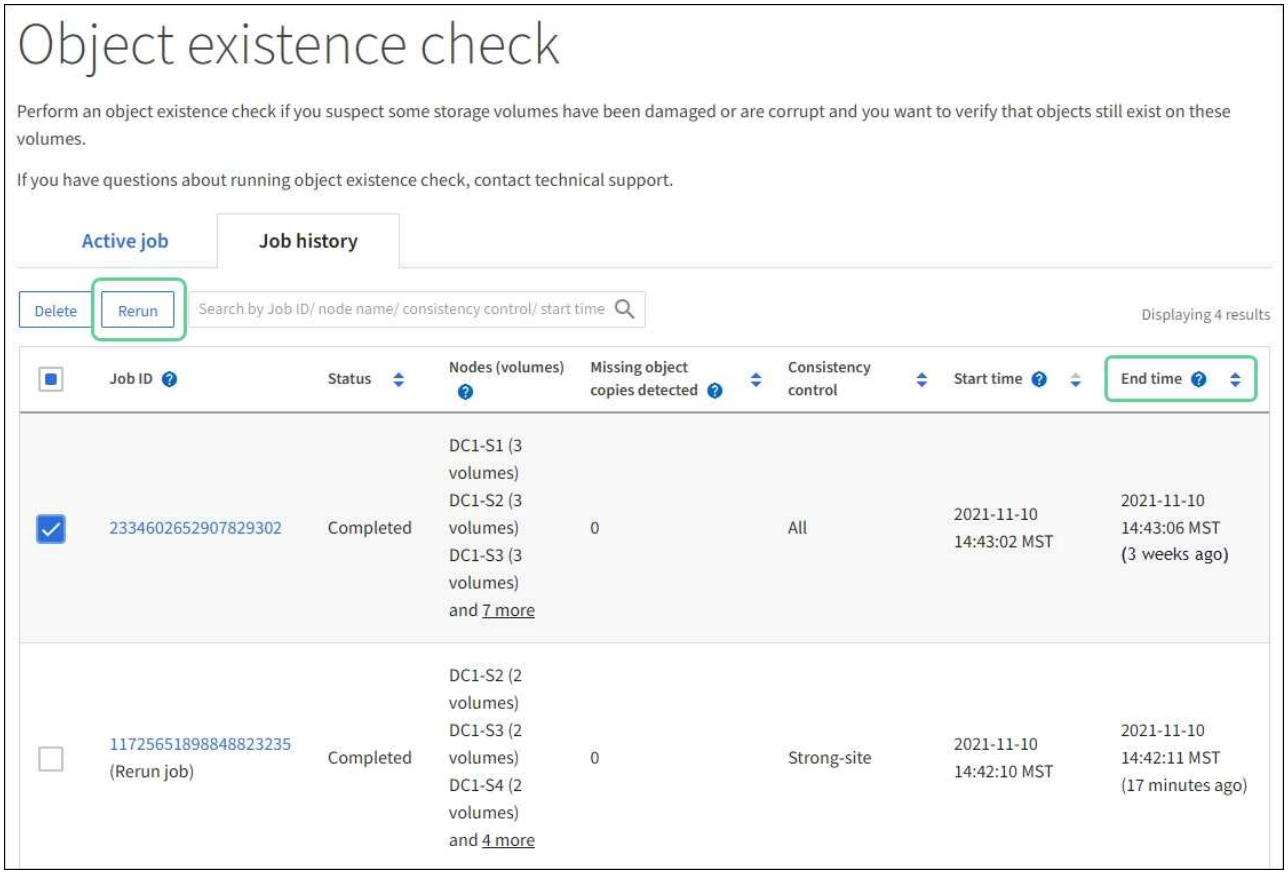
    a. 유지보수 * > * 개체 존재 확인 * > * 작업 내역 * 을 선택합니다.

    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 작업의 확인란을 선택한 다음 * 재실행 * 을 선택합니다.



d. 작업 다시 실행 마법사에서 선택한 노드와 볼륨 및 일관성을 검토합니다.

e. 작업을 다시 실행할 준비가 되면 * 재실행 * 을 선택합니다.

활성 작업 탭이 나타납니다. 선택한 모든 작업이 강력한 사이트의 일관성에서 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.

S3 Put Object size too large 경고 문제 해결

테넌트가 S3 크기 제한인 5GiB를 초과하는 다중 부품 PutObject가 아닌 작업을 시도하면 S3 Put Object 크기가 너무 큼 알림이 트리거됩니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

5GiB보다 큰 객체를 사용하는 테넌트를 확인하여 이를 알릴 수 있습니다.

단계

1. 구성 * > * 모니터링 * > * 감사 및 syslog 서버 * 로 이동합니다.
2. Client Writes가 Normal인 경우 감사 로그에 액세스합니다.

   a. 를 입력합니다 `ssh admin@primary_Admin_Node_IP`

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

   e. 를 입력합니다 `cd /var/local/log`

   "감사 정보의 대상에 대해 자세히 알아봅니다"..

   f. 5GiB보다 큰 객체를 사용하는 테넌트를 식별합니다.

      i. 를 입력합니다 `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

      ii. 결과의 각 감사 메시지에 대해 필드를 보고 `S3AI` 테넌트 계정 ID를 확인합니다. 메시지의 다른 필드를 사용하여 클라이언트, 버킷 및 개체에서 사용된 IP 주소를 확인합니다.

코드	설명
SAIP	소스 IP
에스쓰리아이주식회사	테넌트 ID입니다
에스쓰리비케이주식회사	버킷
에스3KY	오브젝트
CSRZ	크기(바이트)

      - 감사 로그 결과의 예 *

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):804317333
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. 클라이언트 쓰기가 정상이 아닌 경우 알림의 테넌트 ID를 사용하여 테넌트를 식별합니다.

   a. 지원 * > * 도구 * > * 로그 * 로 이동합니다. 알림에 있는 스토리지 노드에 대한 애플리케이션 로그를 수집합니다. 알림 전후 15분을 지정합니다.

   b. 파일 압축을 풀고 다음으로 이동합니다 `bycast.log`.

      /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log

   c. 로그에서 `method=PUT` 클라이언트를 검색하고 필드에서 클라이언트를 `clientIP` 식별합니다.

      ▪ bycast.log의 예 *

```
Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
2023-01-05T18:33:41.208790| NOTICE   1404 af23cb66b7e3efa5 S3RQ:
EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
```

4. 최대 PutObject 크기가 5GiB이고 5GiB보다 큰 오브젝트에 대해 다중 파트 업로드를 사용하도록 테넌트에 알립니다.
5. 응용 프로그램이 변경된 경우 1주일 동안 경고를 무시하십시오.

분실하거나 누락된 오브젝트 데이터 문제를 해결합니다

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 간주되어 경고가 트리거됩니다.
- 삭제 코딩 복제본의 경우 예상 위치에서 복제본을 검색할 수 없는 경우 다른 위치에서 복사본을 검색하려고 시도하기 전에 ECOR(Corrupt Copies Detected) 속성이 1씩 증가합니다. 다른 복사본을 찾을 수 없으면 경고가 트리거됩니다.

모든 * Objects Lost * 알림을 즉시 조사하여 손실의 근본 원인을 파악하고 객체가 오프라인 또는 현재 사용할 수 없는 스토리지 노드에 여전히 존재하는지 확인해야 합니다. 을 "손실된 개체를 조사합니다"참조하십시오.

복사본 없이 오브젝트 데이터를 손실할 경우 복구 솔루션이 없습니다. 그러나 손실된 개체를 다시 설정하여 손실된 개체를 새로 마스킹하지 못하도록 해야 합니다. 을 "분실 및 누락된 개체 수를 재설정합니다"참조하십시오.

손실된 개체를 조사합니다

Objects Lost * 경고가 트리거되면 즉시 조사해야 합니다. 영향을 받는 개체에 대한 정보를 수집하고 기술 지원 부서에 문의하십시오.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인해야 "지원되는 웹 브라우저"합니다.
- 있습니다. "특정 액세스 권한"
- 파일이 있어야 `Passwords.txt` 합니다.

이 작업에 대해

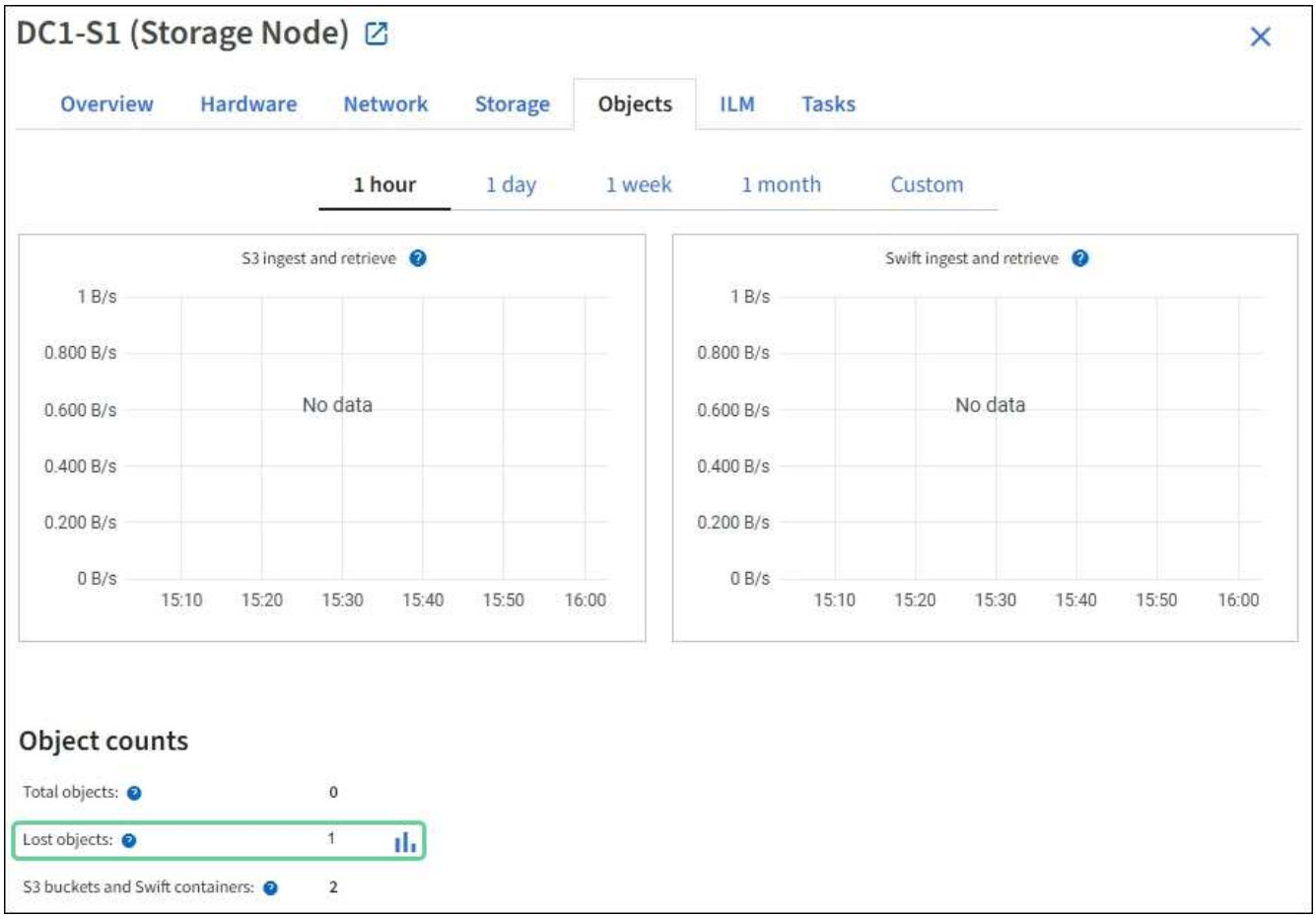
Objects Lost * 알림은 StorageGRID가 그리드에 개체의 복사본이 없다고 판단함을 나타냅니다. 데이터가 영구적으로 손실되었을 수 있습니다.

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. 관리자 노드에서 "감사 로그에 액세스합니다"* Objects Lost * 경고를 트리거한 개체의 UUID(고유 식별자)를 확인하려면 다음을 수행합니다.

   a. 그리드 노드에 로그인합니다.

      i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

      ii. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      iii. 다음 명령을 입력하여 루트로 전환합니다. `su -`

      iv. 파일에 나열된 암호를 `Passwords.txt` 입력합니다. 루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

   b. 감사 로그가 있는 디렉토리로 변경합니다. 다음을 입력합니다. `cd /var/local/log/`

      "감사 정보의 대상에 대해 자세히 알아봅니다"..

   c. grep를 사용하여 OLST(Object Lost) 감사 메시지를 추출합니다. 다음을 입력합니다. `grep OLST audit_file_name`

   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. UUID를 사용하여 손실된 개체의 메타데이터를 찾습니다.
   a. ILM * > * 개체 메타데이터 조회 * 를 선택합니다.
   b. UUID를 입력하고 * 조회 * 를 선택합니다.
   c. 메타데이터의 위치를 검토하고 적절한 작업을 수행합니다.

메타데이터	결론
객체 <object_identifier>를 찾을 수 없습니다	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 절차에서는 "잠재적으로 손실된 개체를 검색합니다"노드 ID를 사용하여 올바른 스토리지 노드를 찾는 방법에 대해 설명합니다.) 개체가 있는 경우 * Objects Lost * 의 개수를 다시 설정하여 경고를 지울 수 있습니다.
위치 = 0	출력에 나열된 위치가 없으면 개체가 누락될 수 있습니다. 직접 시도하거나 기술 지원에 문의할 수 "개체를 검색하고 복원합니다"있습니다. 기술 지원 부서에서 진행 중인 스토리지 복구 절차가 있는지 확인하도록 요청할 수 있습니다. 및 에 대한 정보를 "Grid Manager를 사용하여 개체 데이터를 복원합니다""오브젝트 데이터를 스토리지 볼륨에 복원 중입니다"참조하십시오.

잠재적으로 손실된 개체를 검색하여 복원합니다

객체 손실 * 경고와 기존 객체 손실(손실) 경보를 트리거하고 잠재적으로 손실된 것으로 식별된

객체를 찾아 복원할 수 있습니다.

시작하기 전에

- 에서 식별된 대로 손실된 개체의 UUID가 있습니다"손실된 개체를 조사합니다".
- `Passwords.txt`파일이 있습니다.

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. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

      ii. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      iii. 다음 명령을 입력하여 루트로 전환합니다. `su -`

      iv. 파일에 나열된 암호를 `Passwords.txt` 입력합니다. 루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

   b. 감사 로그가 있는 디렉터리로 변경합니다. `cd /var/local/log/`

      "감사 정보의 대상에 대해 자세히 알아봅니다"..

   c. grep를 사용하여 의 압축을 "잠재적으로 손실된 개체와 관련된 감사 메시지입니다"풀고 출력 파일로 보냅니다. 다음을 입력합니다. `grep uuid-value audit_file_name > output_file_name`

      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. 다음을 입력합니다. `grep LLST output_file_name`

      예를 들면 다음과 같습니다.

      ```
      Admin: # grep LLST messages_about_lost_objects.txt
      ```

      LLST 감사 메시지는 이 예제 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.

a. 이 LDR 노드 ID와 연결된 스토리지 노드를 찾습니다. Grid Manager에서 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택합니다. 그런 다음 *데이터 센터 * > *스토리지 노드 * > * LDR * 을 선택합니다.

LDR 서비스의 노드 ID는 Node Information 테이블에 있습니다. 이 LDR을 호스팅하는 스토리지 노드를 찾을 때까지 각 스토리지 노드에 대한 정보를 검토하십시오.

2. 감사 메시지에 표시된 스토리지 노드에 객체가 있는지 확인합니다.

a. 그리드 노드에 로그인합니다.

i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

ii. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

iii. 다음 명령을 입력하여 루트로 전환합니다. `su -`

iv. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

b. 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'
```

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 다음 단계를 계속 진행합니다. 검색된 객체를 다시 StorageGRID로 복원할 수 있습니다.

3. 개체 경로를 찾은 경우 개체를 StorageGRID로 복원해 보십시오.

   a. 동일한 스토리지 노드에서 StorageGRID에서 관리할 수 있도록 객체 파일의 소유권을 변경합니다. 다음을 입력합니다. `chown ldr-user:bycast 'file_path_of_object'`

   b. LDR 콘솔에 액세스하려면 localhost 1402에 Telnet을 사용합니다. 다음을 입력합니다. `telnet 0 1402`

   c. 다음을 입력합니다. `cd /proc/STOR`

   d. 다음을 입력합니다. `Object_Found 'file_path_of_object'`

      예를 들어 다음을 입력합니다.

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      명령을 실행하면 `Object_Found` 개체의 위치를 그리드에 알립니다. 또한 활성 ILM 정책이 트리거되어 각 정책에 지정된 대로 추가 복사본이 생성됩니다.

      > 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 `Object_Found` 개체에 대한 해당 파일 경로를 사용하여 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'
        ```

        다음 단계를 계속합니다.

4. 개체가 StorageGRID에 성공적으로 복원된 경우 새 위치가 생성되었는지 확인합니다.

   a. 을 사용하여 그리드 관리자에 "지원되는 웹 브라우저"로그인합니다.

   b. ILM * > * 개체 메타데이터 조회 * 를 선택합니다.

   c. UUID를 입력하고 * 조회 * 를 선택합니다.

   d. 메타데이터를 검토하고 새 위치를 확인합니다.

5. 관리 노드에서 이 객체에 대한 ORLM 감사 메시지에 대한 감사 로그를 검색하여 ILM(정보 수명 주기 관리)이 필요에 따라 복제본을 배치했는지 확인합니다.

   a. 그리드 노드에 로그인합니다.

      i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

ii. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

iii. 다음 명령을 입력하여 루트로 전환합니다. `su -`

iv. 파일에 나열된 암호를 `Passwords.txt` 입력합니다. 루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

b. 감사 로그가 있는 디렉터리로 변경합니다. `cd /var/local/log/`

c. grep를 사용하여 개체와 관련된 감사 메시지를 출력 파일에 추출합니다. 다음을 입력합니다. `grep uuid-value audit_file_name > output_file_name`

예를 들면 다음과 같습니다.

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_restored_object.txt
```

d. grep를 사용하여 이 출력 파일에서 ORLM(Object Rules MET) 감사 메시지를 추출합니다. 다음을 입력합니다. `grep ORLM output_file_name`

예를 들면 다음과 같습니다.

```
Admin: # grep ORLM messages_about_restored_object.txt
```

ORLM 감사 메시지는 이 예제 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]]
```

a. 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.

6. "분실 및 누락된 개체 수를 재설정합니다" 그리드 관리자

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인해야 "지원되는 웹 브라우저"합니다.
- 있습니다. "특정 액세스 권한"

이 작업에 대해

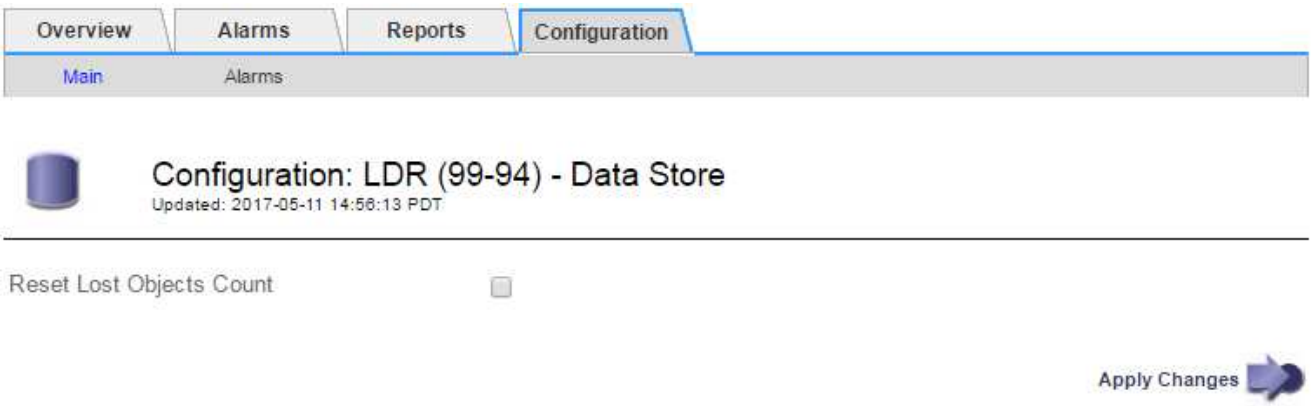
다음 페이지 중 하나에서 Lost Objects 카운터를 재설정할 수 있습니다.

- * 지원 * > * 툴 * > * 그리드 토폴로지 * > * *Site* * > * *Storage Node* * > * LDR * > * 데이터 저장소 * > * 개요 * > * Main *
- * 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 개체가 필요하지 않은 경우 * 격리된 개체 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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"

이 작업에 대해

스토리지 노드에서 복제되고 삭제 코딩된 객체 데이터의 총 양이 알림 규칙에 구성된 조건 중 하나를 충족할 때 * 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:

- `storagegrid_storage_utilization_data_bytes` 스토리지 노드에 대해 복제된 오브젝트 및 삭제 코딩된 오브젝트 데이터의 총 크기에 대한 추정치입니다.
- `storagegrid_storage_utilization_usable_space_bytes` 스토리지 노드에 대해 남은 총 개체 스토리지 공간입니다.

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.

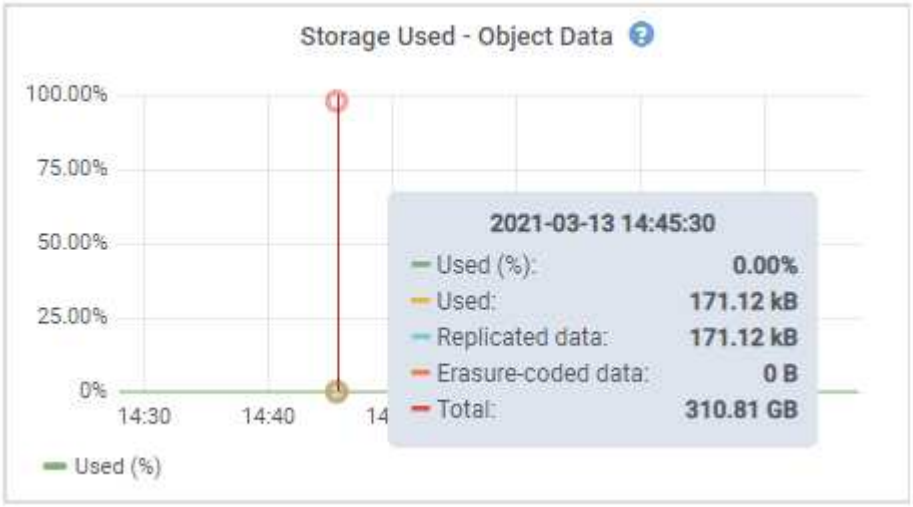
3. 대화 상자에서 세부 정보를 검토하고 다음 사항을 확인합니다.
   - 시간 트리거됨
   - 사이트 및 노드의 이름입니다

◦ 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 `storagegrid_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 "스토리지 용량을 추가합니다"그리드로 이동합니다.

   기존 스토리지 노드에 스토리지 볼륨(LUN)을 추가하거나 새 스토리지 노드를 추가할 수 있습니다.

   자세한 내용은 을 "전체 스토리지 노드 관리"참조하십시오.

낮은 읽기 전용 배경무늬 재정의 알림 문제 해결

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 릴리즈에서 세 가지 "스토리지 볼륨 워터마크입니다" 설정은 글로벌 설정 및 #8212였습니다. 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 11.6 이상으로 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 워터마크에 대한 사용자 지정 값이 너무 작으면 StorageGRID에서 * 로우 읽기 전용 워터마크 무시 * 경고를 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 워터마크의 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 워터마크를 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.

시작하기 전에

- StorageGRID 11.6 이상으로 업그레이드를 완료했습니다.
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한"있습니다.

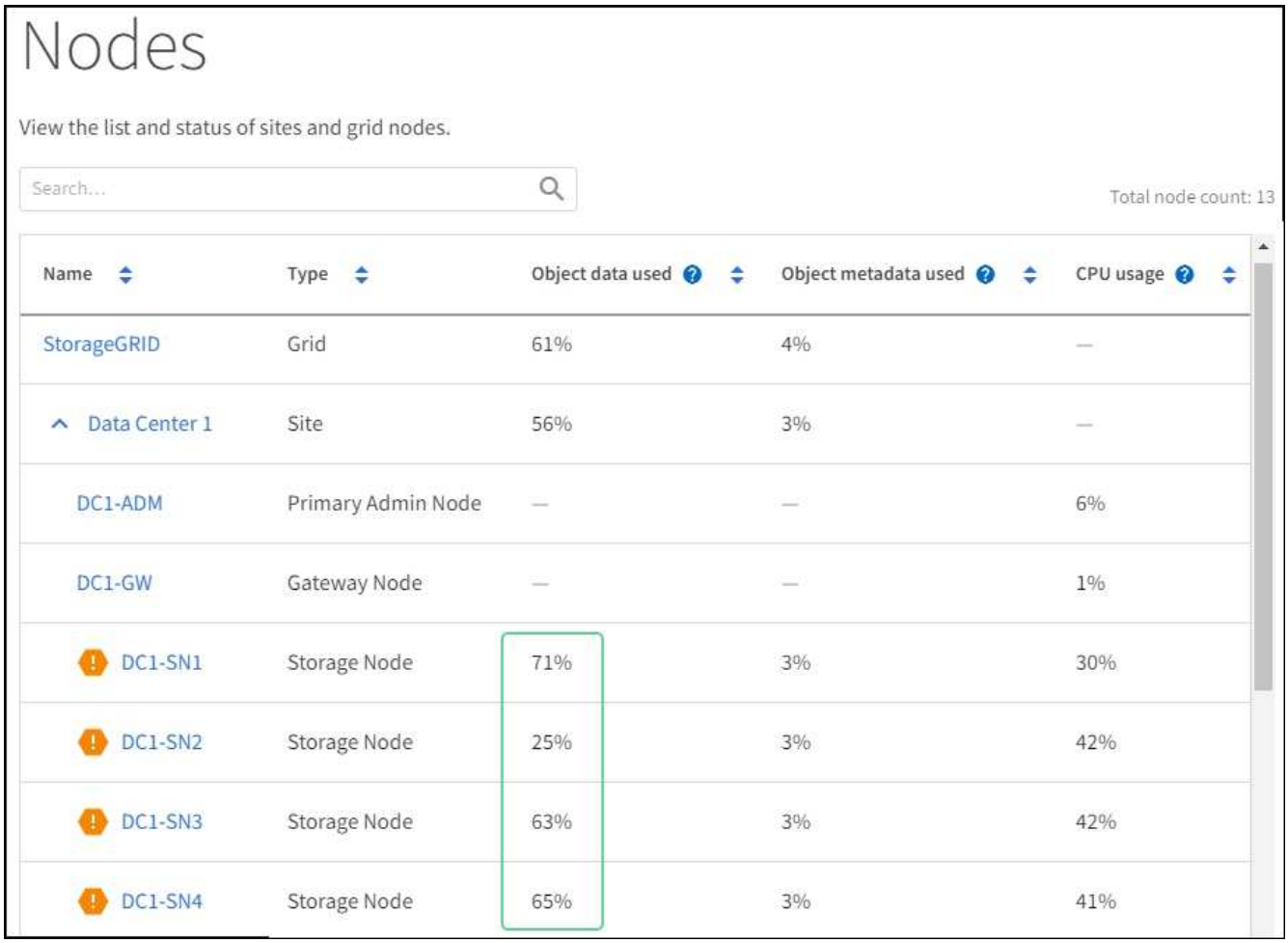
이 작업에 대해

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

단계

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. 적절한 단계를 따릅니다.
   a. 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
   b. ILM 규칙이 엄격한 수집 동작을 사용하거나 특정 스토리지 풀이 거의 꽉 찬 경우 및 의 단계를 최적화된 스토리지 워터마크를 봅니다최적화된 워터마크를 사용할 수 있는지 확인합니다수행합니다.

최적화된 스토리지 워터마크를 봅니다

StorageGRID는 두 가지 Prometheus 메트릭을 사용하여 스토리지 볼륨 소프트 읽기 전용 워터마크에 대해 계산된 최적화된 값을 표시합니다. 그리드의 각 스토리지 노드에 대해 최적화된 최소 및 최대 값을 볼 수 있습니다.

단계

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.

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   마지막 열에는 각 스토리지 노드의 모든 스토리지 볼륨에 대한 소프트 읽기 전용 워터마크의 최소화된 값이 표시됩니다. 이 값이 스토리지 볼륨 소프트 읽기 전용 워터마크에 대한 사용자 지정 설정보다 크면 스토리지 노드에 대해 * 낮은 읽기 전용 워터마크 무시 * 경고가 트리거됩니다.

4. 권장되는 최대 소프트 읽기 전용 워터마크를 보려면 다음 Prometheus 메트릭을 입력하고 * Execute * 를 선택합니다.

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   마지막 열에는 각 스토리지 노드의 모든 스토리지 볼륨에 대한 소프트 읽기 전용 워터마크의 최대 최적화 값이 표시됩니다.

5. 각 스토리지 노드에 대해 최적화된 최대 값을 기록합니다.

최적화된 워터마크를 사용할 수 있는지 결정합니다

단계

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 이동하여 최적화된 워터마크를 최적화된 워터마크를 사용합니다 사용합니다.

   그렇지 않으면 가능한 한 빨리 그리드를 확장합니다. "스토리지 볼륨을 추가합니다"을 기존 노드 또는 "새 스토리지 노드를 추가합니다"로 변경합니다. 그런 다음 으로 최적화된 워터마크를 사용합니다 이동하여 워터마크 설정을 업데이트합니다.

4. 저장소 볼륨 워터마크에 대해 사용자 지정 값을 계속 사용해야 하거나 "사용 안 함"* 낮은 읽기 전용 워터마크가 무시 * 경고를 사용해야 하는 경우"침묵"

   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

단계

1. 지원 * > * 기타 * > * 스토리지 워터마크 * 로 이동합니다.
2. 최적화된 값 사용 * 확인란을 선택합니다.
3. 저장 * 을 선택합니다.

스토리지 노드의 크기와 볼륨의 상대적 용량에 따라 최적화된 스토리지 볼륨 워터마크 설정이 각 스토리지 볼륨에 적용됩니다.

메타데이터 문제를 해결합니다

메타데이터 문제가 발생하면 경고가 문제의 출처와 권장 조치를 알려 줍니다. 특히, Low metadata storage 경고가 트리거된 경우 새 스토리지 노드를 추가해야 합니다.

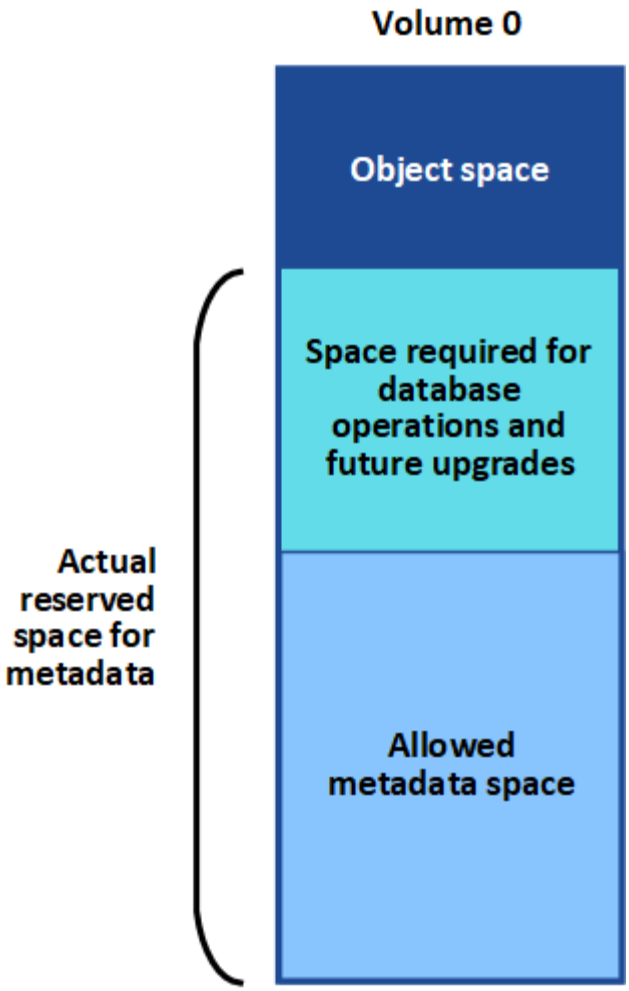
시작하기 전에

을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"

이 작업에 대해

트리거된 각 메타데이터 관련 알림에 대해 권장되는 작업을 수행합니다. 메타데이터 스토리지 부족 * 경고가 트리거되면 새 스토리지 노드를 추가해야 합니다.

StorageGRID는 각 스토리지 노드의 볼륨 0에 개체 메타데이터를 위한 일정한 양의 공간을 예약합니다. _actual reserved space_라고 하는 이 공간은 개체 메타데이터(허용된 메타데이터 공간)에 허용되는 공간과 압축 및 복구와 같은 필수 데이터베이스 작업에 필요한 공간으로 세분화됩니다. 허용되는 메타데이터 공간은 전체 오브젝트 용량을 관리합니다.



오브젝트 메타데이터가 메타데이터에 허용된 공간의 100% 이상을 소비하면 데이터베이스 작업을 효율적으로 실행할 수 없으며 오류가 발생합니다.

오류를 예측하여 오류가 발생하기 전에 수정할 수 있도록 도울 수 "각 스토리지 노드의 객체 메타데이터 용량을 모니터링합니다"있습니다.

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.

> 개체 메타데이터가 허용되는 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.

> 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 경우 동일한 수의 스토리지 노드로도 추가해야 "다른 사이트를 확장합니다"합니다.

확장을 수행한 후 StorageGRID는 기존 오브젝트 메타데이터를 새 노드로 재분산하여 그리드의 전체 메타데이터 용량을 늘립니다. 사용자 작업이 필요하지 않습니다. Low metadata storage * 알림이 지워집니다.

인증서 오류 문제 해결

웹 브라우저, S3 클라이언트 또는 외부 모니터링 도구를 사용하여 StorageGRID에 연결하려고 할 때 보안 또는 인증서 문제가 나타나면 인증서를 확인해야 합니다.

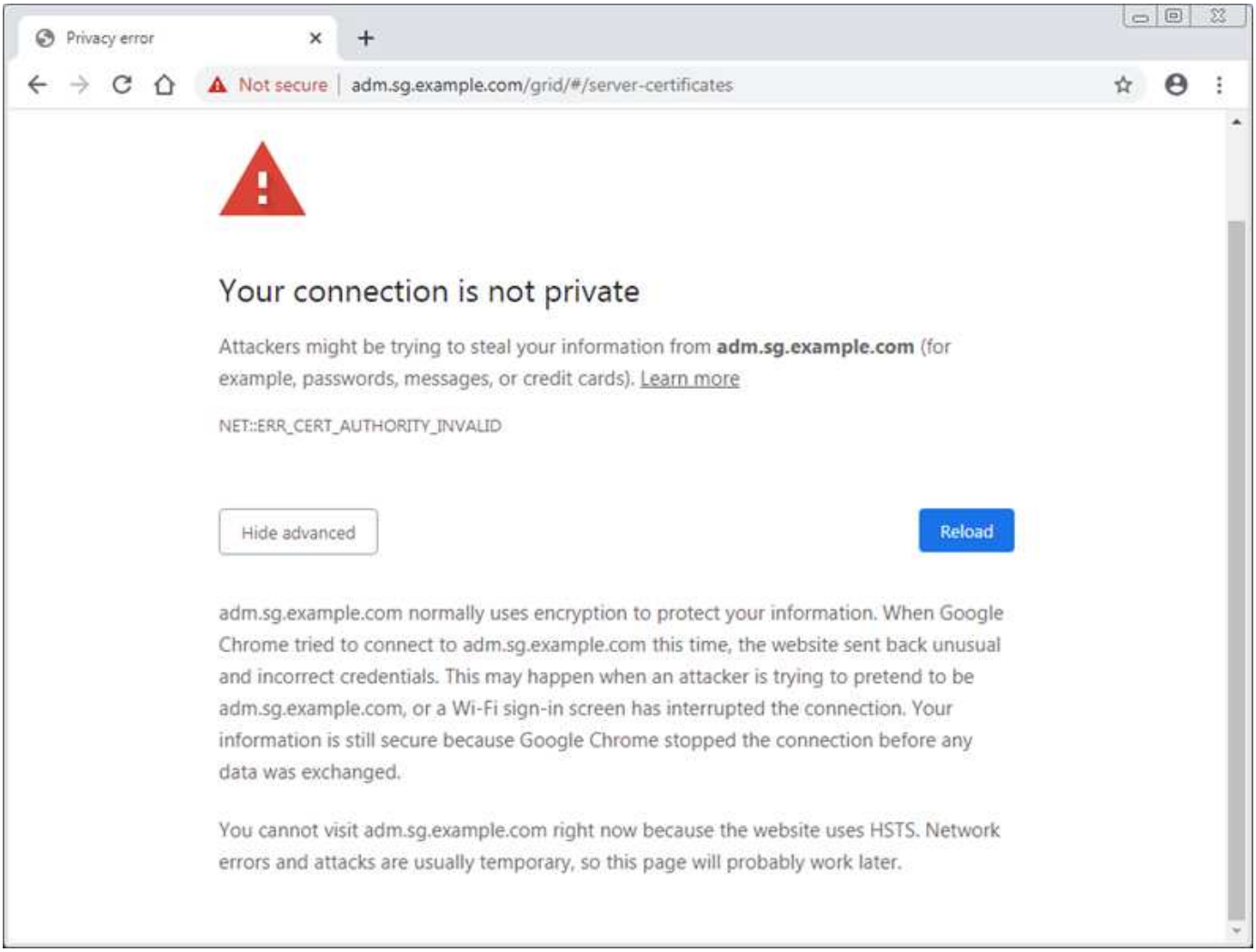
이 작업에 대해

그리드 관리자, 그리드 관리 API, 테넌트 관리자 또는 테넌트 관리 API를 사용하여 StorageGRID에 연결하려고 하면 인증서 오류로 인해 문제가 발생할 수 있습니다. S3 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. configuration * > * Security * > * Certificates * 를 선택한 후"적절한 인증서 탭을 선택합니다"

1. 인증서의 유효 기간을 확인합니다. + 일부 웹 브라우저 및 S3 클라이언트는 유효 기간이 398일 이상인 인증서를 허용하지 않습니다.
2. 인증서가 만료되었거나 곧 만료될 예정이면 새 인증서를 업로드하거나 생성합니다.
   - 서버 인증서의 경우 의 단계를 "Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성 "참조하십시오.
   - 클라이언트 인증서의 경우 의 단계를 "클라이언트 인증서 구성"참조하십시오.
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 * configuration * > * Security * > * Certificates * 를 선택한 다음 새 사용자 지정 인증서를 설치하거나 기본 인증서로 계속 사용합니다"적절한 인증서 탭을 선택합니다".
  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.

관리자 노드 로그인 오류

StorageGRID 관리자 노드에 로그인할 때 오류가 발생하는 경우 시스템에 OR "하드웨어" 문제, "관리자 노드 서비스 "또는 "Cassandra 데이터베이스 관련 문제입니다"연결된 스토리지 노드에 문제가 있을 수 있습니다"네트워킹".

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- `Passwords.txt`파일이 있습니다.
- 있습니다. "특정 액세스 권한"

이 작업에 대해

관리 노드에 로그인하려고 할 때 다음 오류 메시지가 나타나면 다음 문제 해결 지침을 사용하십시오.

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

단계

1. 10분 정도 기다린 후 다시 로그인하세요.

   오류가 자동으로 해결되지 않으면 다음 단계로 이동합니다.

2. StorageGRID 시스템에 둘 이상의 관리자 노드가 있는 경우 다른 관리자 노드에서 그리드 관리자에 로그인하여 사용할 수 없는 관리자 노드의 상태를 확인하십시오.
   - 로그인할 수 있는 경우 * 대시보드 *, * 노드 *, * 알림 * 및 * 지원 * 옵션을 사용하여 오류의 원인을 확인할 수 있습니다.
   - 관리 노드가 하나뿐이거나 여전히 로그인할 수 없는 경우 다음 단계로 이동합니다.
3. 노드의 하드웨어가 오프라인인지 확인합니다.
4. StorageGRID 시스템에 SSO(Single Sign-On)가 활성화된 경우 의 단계를 "Single Sign-On 구성"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. 알림을 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. 다음 명령을 입력합니다. `ssh admin@Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

7. 그리드 노드에서 실행 중인 모든 서비스의 상태를 봅니다. `storagegrid-status`

   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 실행 중인지 확인한다 `# service nginx-gw status`
9. lumberjack을 사용하여 로그를 수집합니다. `# /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
```

```
# gpt-list-services adc
```

관리 노드는 인증 프로세스 중에 ADC 서비스를 사용합니다.

12. 관리자 노드에서 ssh를 사용하여 식별한 IP 주소를 사용하여 각 ADC 스토리지 노드에 로그인합니다.
13. 그리드 노드에서 실행 중인 모든 서비스의 상태를 봅니다. `storagegrid-status`

idnt, acct, nginx 및 cassandra 서비스가 모두 실행 중인지 확인합니다.

14. 및 로그를 검토합니다단계를 반복하여 로그를 수집하려면 Lumberjack을 사용합니다스토리지 노드의 로그를 검토합니다.
15. 문제를 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

기술 지원 팀에 수집한 로그를 제공합니다. 도 "로그 파일 참조"참조하십시오.

사용자 인터페이스 문제

StorageGRID 소프트웨어를 업그레이드한 후 그리드 관리자 또는 테넌트 관리자의 사용자 인터페이스가 예상대로 응답하지 않을 수 있습니다.

단계

1. 을 사용하고 있는지 "지원되는 웹 브라우저"확인합니다.
2. 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.

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 엔터티**"** 오류

422:처리할 수 없는 엔터티는 여러 가지 이유로 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.

`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 표시된 대로 나가는 TLS 연결에 중 하나를 사용해야 합니다"StorageGRID에서 지원하는 Cipherer".

그리드 네트워크 **MTU** 불일치 알림

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`다음 쿼리를 찾아서 입력합니다. `node_network_mtu_bytes{device="eth0"}
2. "MTU 설정을 수정합니다" 필요한 경우 모든 노드에서 그리드 네트워크 인터페이스(eth0)에 대해 동일한지 확인합니다.
   - Linux 및 VMware 기반 노드의 경우 다음 명령을 사용합니다. `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`
     - 예 *: `change-ip.py -n node 1500 grid admin`

       참고: Linux 기반 노드에서 컨테이너의 네트워크에 대해 원하는 MTU 값이 호스트 인터페이스에 이미 구성된 값을 초과할 경우 먼저 호스트 인터페이스를 원하는 MTU 값으로 구성한 다음 스크립트를 사용하여 컨테이너의 네트워크 MTU 값을 변경해야 `change-ip.py` 합니다.

     Linux 또는 VMware 기반 노드에서 MTU를 수정하려면 다음 인수를 사용하십시오.

위치 인수	설명
`mtu`	설정할 MTU입니다. 1280 ~ 9216 범위에 있어야 합니다.
`network`	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.

노드 네트워크 수신 프레임 오류 경고입니다

- 노드 네트워크 수신 프레임 오류 * 경고는 StorageGRID와 네트워크 하드웨어 간의 연결 문제로 인해 발생할 수 있습니다. 이 알림은 기본 문제가 해결된 후에 자동으로 지워집니다.

이 작업에 대해

- 노드 네트워크 수신 프레임 오류 * 경고는 StorageGRID에 연결되는 네트워킹 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 구성에 따라 이 경고의 모든 잠재적 원인에 대한 문제 해결 단계를 수행하십시오.
2. 오류의 원인에 따라 다음 단계를 수행하십시오.

FEC가 일치하지 않습니다

> 이 단계는 StorageGRID 어플라이언스에서 FEC 불일치로 인해 발생한 * 노드 네트워크 수신 프레임 오류 * 경고에만 적용됩니다.

a. StorageGRID 어플라이언스에 연결된 스위치에 있는 포트의 FEC 상태를 확인합니다.

b. 제품에서 스위치로 연결되는 케이블의 물리적 무결성을 점검하십시오.

c. 경고 해결을 시도하기 위해 FEC 설정을 변경하려면 먼저 어플라이언스가 StorageGRID 어플라이언스 설치 프로그램의 링크 구성 페이지에서 * 자동 * 모드로 구성되어 있는지 확인하십시오(어플라이언스 지침 참조:

   - "SG6160"
   - "SGF6112를 참조하십시오"
   - "SG6000 을 참조하십시오"
   - "SG5800을 참조하십시오"
   - "SG5700입니다"
   - "SG110 및 SG1100"
   - "SG100 및 SG1000"

d. 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. 일반적인 FEC 설정이 없으면 네트워크가 "no-FEC" 모드로 전환됩니다. FEC를 사용하지 않으면 전기 노이즈로 인해 발생한 오류가 연결에 더 취약합니다.

   > StorageGRID 어플라이언스는 FC(Firecode) 및 RS(Reed Solomon) FEC를 지원하며 FEC도 지원하지 않습니다.

스위치 포트와 **NIC MTU**가 일치하지 않습니다

스위치 포트 및 NIC MTU 불일치로 인해 경고가 발생한 경우 노드에 구성된 MTU 크기가 스위치 포트에 대한 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 구성으로 가능하다면 * 노드 네트워크 수신 프레임 오류 * 경고가 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. 자세한 내용은 을 Grid Network MTU 불일치 알림 문제를 해결합니다 참조하십시오.

도 "MTU 설정을 변경합니다" 참조하십시오.

높은 링크 오류율

a. FEC가 아직 활성화되지 않은 경우 FEC를 활성화합니다.
b. 네트워크 케이블 연결 품질이 양호하며 손상되었거나 잘못 연결되지 않았는지 확인합니다.
c. 케이블이 문제가 아닌 경우 기술 지원 부서에 문의하십시오.

전기 소음이 많은 환경에서 높은 오류율을 느낄 수 있습니다.

NIC 링 버퍼 오버런

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.

3. 문제가 해결되지 않으면 문제를 모니터링하고 기술 지원 부서에 문의하십시오.

시간 동기화 오류입니다

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 수준의 StorageGRID를 설치하는 경우 "외부 NTP 소스를 지정합니다"Windows Server 2016 이전 버전의 Windows에서는 W32Time(Windows Time) 서비스를 사용하지 마십시오. 이전 버전의 Windows의 시간 서비스는 정확하지 않으며 StorageGRID와 같은 고정밀 환경에서 사용하기 위해 Microsoft에서 지원되지 않습니다.

Linux: 네트워크 연결 문제

Linux 호스트에서 호스팅되는 StorageGRID 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 생성하려면 또는 의 지침을 참조하십시오"Red Hat Enterprise Linux""Ubuntu 또는 Debian".

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 클론 생성 활성화에 대한 자세한 내용은 또는 의 지침을 "Red Hat Enterprise Linux""Ubuntu 또는 Debian"참조하십시오.

무차별 모드

MAC 주소 클로닝을 사용하지 않고 하이퍼바이저에 의해 할당된 것이 아닌 MAC 주소에 대한 데이터를 모든 인터페이스에서 수신 및 전송하도록 허용하려면 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.

무차별 모드 사용에 대한 자세한 내용은 또는 의 지침을 참조하십시오"Red Hat Enterprise Linux""Ubuntu 또는 Debian".

Linux: 노드 상태가 **"고립된"** 상태입니다**.**

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. 다음 명령을 실행하여 노드를 다시 시작합니다. `$ sudo storagegrid node start node-name`

   ```
   $ 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 들면 다음과 같습니다 `.sudo docker stop --time secondscontainer-name`

   의 경우 `seconds` 컨테이너가 중지될 때까지 대기할 시간(초)을 입력합니다(일반적으로 15분 이하). 예를 들면 다음과 같습니다.

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. 노드를 다시 시작합니다. `storagegrid node start node-name`

```
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

그리드 노드에 할당된 IPv6 주소를 보려면

1. nodes * 를 선택하고 노드를 선택합니다.
2. 개요 탭에서 * IP 주소 * 옆에 있는 * 추가 IP 주소 표시 * 를 선택합니다.

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. 다음 명령을 실행합니다. `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

결과는 0이어야 합니다.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

> 결과가 0이 아닌 경우 설정 변경에 대한 운영 체제 설명서를 `sysctl` 참조하십시오. 그런 다음 계속하기 전에 값을 0으로 변경합니다.

3. StorageGRID 노드 컨테이너 입력: `storagegrid node enter node-name`
4. 다음 명령을 실행합니다. `sysctl net.ipv6.conf.all.disable_ipv6`

```
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. 컨테이너를 종료합니다. `exit`

```
root@DC1-S1:~ # exit
```

6. 루트로 다음 파일을 편집합니다 `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
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 표에는 외부 syslog 서버와 관련하여 발생할 수 있는 오류 메시지와 해결 조치가 나와 있습니다.

외부 syslog 서버로 감사 정보를 보내는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- "외부 syslog 서버 사용 시 고려 사항"
- "감사 메시지 및 외부 syslog 서버를 구성합니다"

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") 표기법에서 유효한 IP 주소인지 확인합니다. 2. DNS 서버가 올바르게 구성되었는지 확인합니다. 3. 각 노드가 DNS 서버의 IP 주소에 액세스할 수 있는지 확인합니다.

오류 메시지	설명 및 권장 조치
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.
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(그리드, 관리 또는 클라이언트)를 사용하여 트래픽을 syslog 서버로 라우팅하도록 구성되었는지 확인합니다. 3. 방화벽이 syslog 서버의 IP 및 포트에 나열된 노드에서 TCP/TLS 연결에 대한 액세스를 차단하지 않는지 확인합니다.

오류 메시지	설명 및 권장 조치
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. 이 문제를 해결하려면: 1. syslog 서버에 대해 올바른 FQDN 또는 IP 주소, 포트 및 프로토콜을 입력했는지 확인합니다. 2. TLS를 사용하는 경우 syslog 서버도 TLS를 사용하고 있는지 확인합니다. TCP를 사용하는 경우 syslog 서버도 TCP를 사용하고 있는지 확인합니다. 3. 유휴 TCP 연결을 종료하도록 중간 방화벽이 구성되어 있지 않은지 확인합니다.
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 서버도 TLS를 사용하고 있는지 확인합니다. TCP를 사용하는 경우 syslog 서버도 TCP를 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.

오류 메시지	설명 및 권장 조치
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.

감사 로그를 검토합니다

감사 메시지 및 로그

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"

감사 메시지 흐름 및 보존

모든 StorageGRID 서비스는 정상적인 시스템 작동 중에 감사 메시지를 생성합니다. 이러한 감사 메시지가 StorageGRID 시스템을 통해 파일로 이동하는 방법을 이해해야 `audit.log` 합니다.

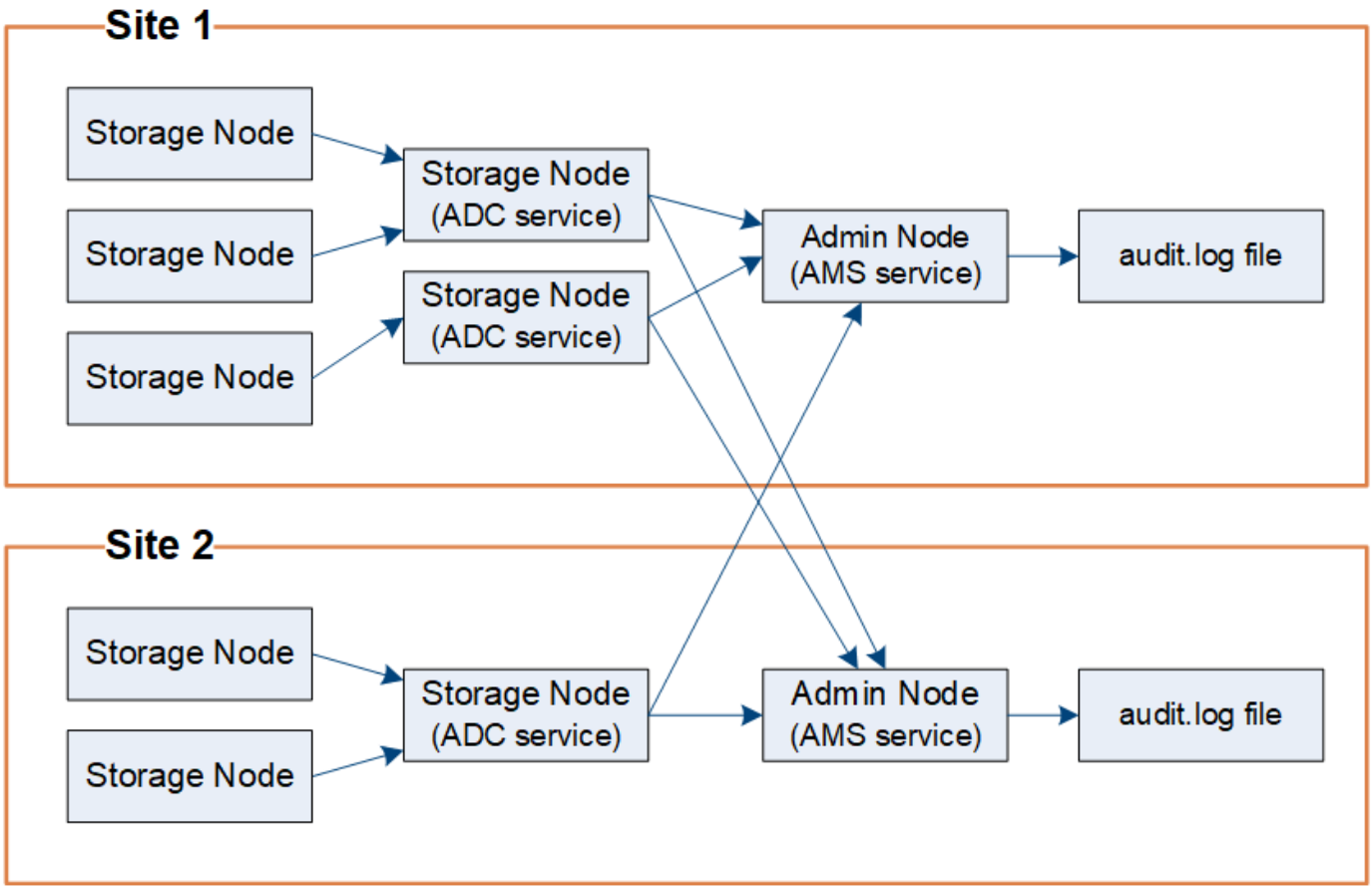
감사 메시지 흐름

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.

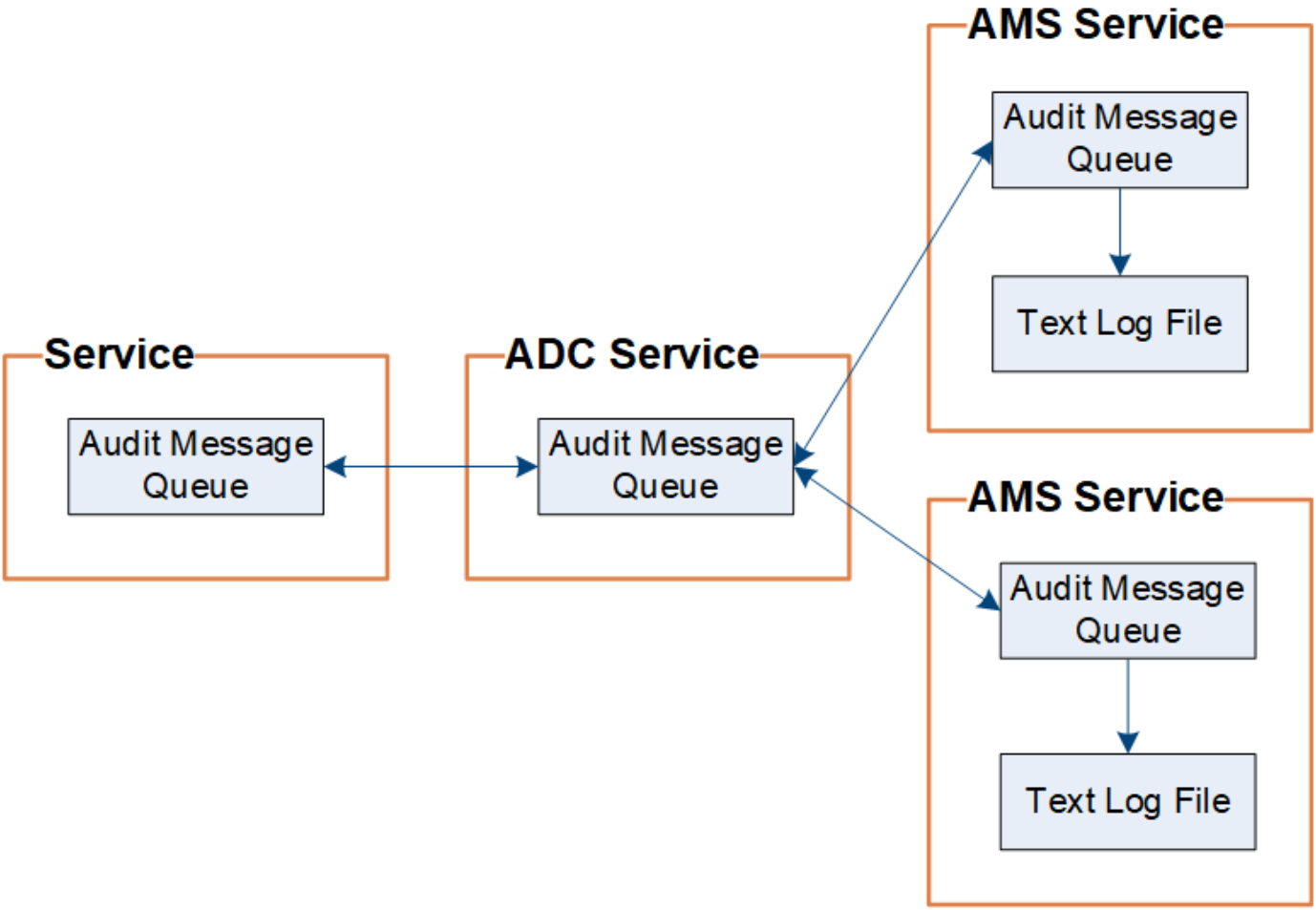
각 관리자 노드는 감사 메시지를 텍스트 로그 파일에 저장하며 활성 로그 파일의 이름은 `audit.log`지정됩니다.



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. 메시지가 관리자 노드의 디렉토리에 있는 감사 로그 파일에 기록될 때까지 메시지 복사본은 항상 감사 메시지 큐에 보관됩니다. `/var/local/log` 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 증가하면 각 노드의 디렉터리에서 사용 가능한 공간을 더 많이 소비합니다. `/var/local/` 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.

- 관리자 노드에서 사용하는 디렉토리가 가득 차면 `/var/local/log` 해당 디렉토리가 더 이상 가득 찰 때까지 관리자 노드가 새 감사 메시지에 사용할 수 없는 것으로 표시됩니다. S3 클라이언트 요청은 영향을 받지 않습니다. 감사 리포지토리에 연결할 수 없을 때 XAMS(Unreachable Audit Repositories) 경보가 트리거됩니다.
- ADC 서비스가 있는 스토리지 노드에서 사용하는 디렉토리가 92%가 차면 `/var/local/` 디렉토리가 87%만 가득 찰 때까지 노드가 메시지를 감사할 수 없는 것으로 표시됩니다. 다른 노드에 대한 S3 클라이언트 요청은 영향을 받지 않습니다. 감사 릴레이에 연결할 수 없는 경우 NRLY(사용 가능한 감사 릴레이) 경보가 트리거됩니다.

> ADC 서비스에 사용 가능한 저장소 노드가 없는 경우 저장소 노드는 감사 메시지를 파일에 로컬로 `/var/local/log/localaudit.log` 저장합니다.

- 스토리지 노드에서 사용하는 디렉토리가 85%가 가득 차면 `/var/local/` 노드가 에서 S3 클라이언트 요청을 거부하기 `503 Service Unavailable` 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.
- `/var/local/`감사 메시지와 무관한 이유로 ADC 저장소 노드의 공간이 가득 차있습니다. 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. 을 "감사 메시지 및 로그 대상을 구성합니다"참조하십시오.

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 공유에는 활성 `audit.log` 파일과 압축된 감사 로그 파일이 포함됩니다. 관리자 노드의 명령줄에서 직접 감사 로그 파일에 액세스할 수 있습니다.

시작하기 전에

- 있습니다. "특정 액세스 권한"
- 파일이 있어야 `Passwords.txt` 합니다.
- 관리 노드의 IP 주소를 알아야 합니다.

단계

1. 관리자 노드에 로그인:
   a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 감사 로그 파일이 포함된 디렉토리로 이동합니다.

   ```
   cd /var/local/log
   ```

3. 필요에 따라 현재 또는 저장된 감사 로그 파일을 봅니다.

로그 파일 회전을 감사합니다

감사 로그 파일은 관리자 노드의 `/var/local/log` 디렉터리에 저장됩니다. 활성 감사 로그 파일의 이름이 `audit.log`지정됩니다.

> 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 "감사 메시지 및 로그 대상을 구성합니다"참조하십시오.

하루에 한 번 활성 `audit.log` 파일이 저장되고 새 `audit.log` 파일이 시작됩니다. 저장된 파일의 이름은 해당 파일이 저장된 시점을 형식으로 *`yyyy-mm-dd.txt`* 나타냅니다. 하루에 감사 로그가 두 개 이상 만들어지는 경우 파일 이름은 파일이 저장된 날짜(숫자 뒤에 붙음)를 형식으로 *`yyyy-mm-dd.txt.n`* 사용합니다. 예를 `2018-04-15.txt` 들어, 및 `2018-04-15.txt.1` 는 2018년 4월 15일에 생성되고 저장되는 첫 번째 및 두 번째 로그 파일입니다.

하루가 지나면 저장된 파일이 압축되고 원래 날짜가 보존되는 형식으로 이름이 *`yyyy-mm-dd.txt.gz`* 변경됩니다. 시간이 지남에 따라 이로 인해 관리 노드의 감사 로그에 할당된 스토리지가 소비됩니다. 스크립트는 감사 로그 공간 소비를 모니터링하고 필요에 따라 로그 파일을 삭제하여 디렉토리의 공간을 `/var/local/log` 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 활성 파일, 전날의 파일(`2018-04-15.txt`) 및 전날의 압축된 파일을 보여 `audit.log`(`2018-04-14.txt.gz` 줍니다.

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

감사 로그 파일 형식

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.UUUUUU`, 여기서 *`UUUUUU`* 마이크로초입니다.

- 대괄호 안에 들어 있고 로 시작하는 감사 메시지 자체입니다. `AUDT`

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::17530064241597054
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::17530064241597054
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::17530064241597054
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. 를 사용하여 "감사 - 설명 도구"감사 로그의 감사 메시지에 대한 간단한 요약을 얻을 수 있습니다. 를 사용하여 기록된 쓰기, 읽기 및 삭제 작업의 수와 이러한 작업에 소요되는 시간을 요약할 수 "감사 합계 도구"있습니다.

감사 설명 도구를 사용합니다

이 도구를 사용하여 감사 로그에서 감사 메시지를 읽기 쉬운 형식으로 변환할 수 `audit-explain` 있습니다.

시작하기 전에

- 있습니다. "특정 액세스 권한"
- 파일이 있어야 `Passwords.txt` 합니다.
- 기본 관리 노드의 IP 주소를 알아야 합니다.

이 작업에 대해

기본 관리자 노드에서 사용할 수 있는 이 `audit-explain` 도구는 감사 로그에 감사 메시지에 대한 간단한 요약을 제공합니다.

> 이 `audit-explain` 도구는 주로 문제 해결 작업 중에 기술 지원 부서에서 사용하도록 제작되었습니다. 쿼리를 처리하면 `audit-explain` 많은 양의 CPU 성능이 소모될 수 있으며, 이로 인해 StorageGRID 작업에 영향을 줄 수 있습니다.

이 예에서는 도구의 일반적인 출력을 보여 `audit-explain` 줍니다. 이 4개의 "SPUT" 감사 메시지는 계정 ID가 92484777680322627870인 S3 테넌트가 S3 PUT 요청을 사용하여 "bucket1"이라는 버킷을 생성하고 해당 버켓에 3개의 객체를 추가할 때 생성됩니다.

```
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
```

이 `audit-explain` 도구는 다음을 수행할 수 있습니다.

- 일반 또는 압축 감사 로그를 처리합니다. 예를 들면 다음과 같습니다.

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- 여러 파일을 동시에 처리합니다. 예를 들면 다음과 같습니다.

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/log/*
  ```

- 파이프의 입력을 수락하면 명령 또는 다른 방법으로 입력을 필터링하고 사전 처리할 수 있습니다. `grep` 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 있기 때문에 전체 파일이 아닌 파트에서 보고 실행할 부분을

필터링하여 시간을 절약할 수 audit-explain 있습니다.

> 이 audit-explain 도구는 압축된 파일을 파이프 입력 파일로 허용하지 않습니다. 압축된 파일을 처리하려면 파일 이름을 명령줄 인수로 제공하거나 도구를 사용하여 zcat 먼저 파일의 압축을 푸십시오. 예를 들면 다음과 같습니다.
>
> ```
> zcat audit.log.gz | audit-explain
> ```

옵션을 사용하여 help (-h) 사용 가능한 옵션을 확인합니다. 예를 들면 다음과 같습니다.

```
$ audit-explain -h
```

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. ssh admin@*primary_Admin_Node_IP*
   b. 파일에 나열된 암호를 Passwords.txt 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. su -
   d. 파일에 나열된 암호를 Passwords.txt 입력합니다.

      루트로 로그인하면 프롬프트가 에서 $ 로 `#`변경됩니다.

2. 다음 명령을 입력합니다. 여기서 는 분석할 파일의 이름과 위치를 나타냅니다. /var/local/log/audit.log

   ```
   $ audit-explain /var/local/log/audit.log
   ```

   이 audit-explain 도구는 지정된 파일에 있는 모든 메시지에 대해 사람이 읽을 수 있는 해석을 인쇄합니다.

   > 선 길이를 줄이고 가독성을 높이기 위해 타임스탬프가 기본적으로 표시되지 않습니다. 타임스탬프를 보려면 타임스탬프(-t) 옵션을 사용하십시오.

감사 합계 도구를 사용합니다

이 도구를 사용하여 감사 메시지를 쓰기, 읽기, 헤드 및 삭제하고 각 작업 유형에 대한 최소, 최대 및 평균 시간(또는 크기)을 확인할 수 audit-sum 있습니다.

시작하기 전에

- 있습니다. "특정 액세스 권한"
- 파일이 있어야 Passwords.txt 합니다.
- 기본 관리 노드의 IP 주소를 알아야 합니다.

이 작업에 대해

기본 관리자 노드에서 사용할 수 있는 이 audit-sum 툴은 기록된 쓰기, 읽기 및 삭제 작업의 수와 이러한 작업에 걸리는 시간을 요약합니다.

이 audit-sum 도구는 주로 문제 해결 작업 중에 기술 지원 부서에서 사용하도록 제작되었습니다. 쿼리를 처리하면 audit-sum 많은 양의 CPU 성능이 소모될 수 있으며, 이로 인해 StorageGRID 작업에 영향을 줄 수 있습니다.

이 예에서는 도구의 일반적인 출력을 보여 audit-sum 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 audit-sum 툴은 감사 로그에서 다음과 같은 S3, Swift 및 ILM 감사 메시지의 수와 시간을 제공합니다.

기능이 더 이상 사용되지 않으므로 제품 및 설명서에서 감사 코드가 제거됩니다. 여기에 나열되지 않은 감사 코드가 발생하는 경우 이전 SG 릴리스에 대한 이 항목의 이전 버전을 확인하십시오. "감사 합계 도구 문서 사용 StorageGRID 11.8"예를 들어,

코드	설명	을 참조하십시오
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"
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"

코드	설명	을 참조하십시오
WPUT	SwiFT PUT: 새 개체 또는 컨테이너를 생성하기 위해 트랜잭션을 성공적으로 기록합니다.	"WPUT: Swift Put"

이 `audit-sum` 도구는 다음을 수행할 수 있습니다.

- 일반 또는 압축 감사 로그를 처리합니다. 예를 들면 다음과 같습니다.

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- 여러 파일을 동시에 처리합니다. 예를 들면 다음과 같습니다.

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/log/*
```

- 파이프의 입력을 수락하면 명령 또는 다른 방법으로 입력을 필터링하고 사전 처리할 수 있습니다. `grep` 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 도구를 사용하여 `zcat` 먼저 파일의 압축을 푸십시오. 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 작업 시간이 표시되지만 옵션을 사용하면 개체 크기를 확인할 수 `size (-s)` 있습니다.

옵션을 사용하여 `help (-h)` 사용 가능한 옵션을 확인합니다. 예를 들면 다음과 같습니다.

```
$ audit-sum -h
```

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 쓰기, 읽기, 헤드 및 삭제 작업과 관련된 모든 메시지를 분석하려면 다음 단계를 수행하십시오.

   a. 다음 명령을 입력합니다. 여기서 는 분석할 파일의 이름과 위치를 나타냅니다. `/var/local/log/audit.log`

   ```
   $ audit-sum /var/local/log/audit.log
   ```

   이 예에서는 도구의 일반적인 출력을 보여 `audit-sum` 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 long 출력 옵션을 (`-l`추가하여 객체 경로를 포함시킵니다.

   ```
   grep SGET audit.log | audit-sum -l
   ```

   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 개체의 크기를 확인하려면 크기 옵션을 (`-s`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 로그에서 명령을 실행하고 group-by-time 옵션을 사용한 (`-gt`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
```

이 결과는 S3 GET 트래픽이 06:00에서 07:00사이에 급증함을 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 매시간마다 검색되는 크기 개체를 확인하려면 (`-s`명령에 size 옵션)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 를 사용하여 "감사 - 설명 도구"해당 시간 동안 모든 SGET 작업을 검토합니다.

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

grep 명령의 출력이 여러 줄로 예상되는 경우 감사 로그 파일의 내용을 한 번에 한 페이지(한 화면)씩 표시하는 명령을 추가합니다 `less`.

5. 버킷의 SPUT 작업이 개체에 대한 SPUT 작업보다 느리는지 확인하려면 다음을 수행합니다.

a. 오브젝트 및 버킷 작업에 대한 메시지를 별도로 그룹화하는 옵션을 사용하여 시작합니다 `-go`.

```
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. SPUT 작업이 가장 느린 버킷을 확인하려면 버킷별로 `-gb` 메시지를 그룹화하는 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 개체 크기가 가장 큰 버킷의 크기를 확인하려면 및 `-s` 옵션을 모두 `-gb` 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
```

감사 메시지 형식

감사 메시지 형식

StorageGRID 시스템 내에서 교환되는 감사 메시지에는 모든 메시지에 공통되는 표준 정보 및 보고되는 이벤트 또는 활동을 설명하는 특정 콘텐츠가 포함됩니다.

및 "감사 합계"도구에서 제공하는 요약 정보가 충분하지 않은 경우 "감사 - 설명"이 섹션을 참조하여 모든 감사 메시지의 일반적인 형식을 이해합니다.

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 대괄호로 묶임(`[ ]`, 문자열의 각 특성 요소는 다음과 같은 특성을 갖습니다.

- 대괄호로 묶입니다 `[ ]`
- 감사 메시지를 나타내는 문자열에 의해 도입되었습니다 `AUDT`
- 앞 또는 뒤에 구분 기호(쉼표 또는 공백 없음)를 사용하지 않습니다
- 줄 바꿈 문자에 의해 종료됩니다 `\n`

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 요소가 특정 순서로 나열되지 않습니다.

다음 목록에서는 특성 요소에 대해 설명합니다.

- `ATTR` 보고되는 특성에 대한 4자리 코드입니다. 모든 감사 메시지에 공통적으로 적용되는 일부 특성 및 이벤트별 특성이 있습니다.
- `type` UI64, FC32 등과 같은 값의 프로그래밍 데이터 형식에 대한 4자리 식별자입니다. 형식은 괄호로 묶여 `( )` 있습니다.
- `value` 특성의 내용, 일반적으로 숫자 또는 텍스트 값입니다. 값은 항상 콜론 뒤에 (`:`옵니다.) 데이터 형식 CStr의 값은 큰따옴표 ""로 둘러싸여 있습니다.

데이터 유형

감사 메시지에 정보를 저장하는 데 사용되는 데이터 유형은 다양합니다.

유형	설명
UI32 를 참조하십시오	부호 없는 긴 정수(32비트). 0에서 4,294,967,295 사이의 숫자를 저장할 수 있습니다.
UI64 를 참조하십시오	부호 없는 이중 긴 정수(64비트). 0에서 18,446,744,073,709,551,615까지의 숫자를 저장할 수 있습니다.
에프씨32	4자 상수. 32비트 부호 없는 정수 값은 "ABCD"와 같은 4개의 ASCII 문자로 표시됩니다.
아이패드	IP 주소에 사용됩니다.
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 열린 컨테이너 다음에 `[AUDT:` 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 `ATYP` 예제에서는 밑줄이 그어진 요소를 사용하여 메시지를 생성한 이벤트를 식별합니다. 이 예제 메시지에는 메시지 코드([ATYP(FC32):Shea])가 포함되어 "셰어"있으며, 이는 S3 헤드 요청이 성공적으로 생성되었음을 나타냅니다.

감사 메시지의 공통 요소

모든 감사 메시지에는 공통 요소가 포함됩니다.

코드	유형	설명
있습니다	에프씨32	모듈 ID: 메시지를 생성한 모듈 ID의 4자리 식별자입니다. 이것은 감사 메시지가 생성된 코드 세그먼트를 나타냅니다.
ANID	UI32 를 참조하십시오	노드 ID: 메시지를 생성한 서비스에 할당된 그리드 노드 ID입니다. 각 서비스는 StorageGRID 시스템을 구성하고 설치할 때 고유 식별자를 할당합니다. 이 ID는 변경할 수 없습니다.
ASE	UI64 를 참조하십시오	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 를 참조하십시오	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 를 참조하십시오	추적 ID: 단일 이벤트에 의해 트리거된 메시지 집합에서 공유하는 식별자입니다.
ATIM	UI64 를 참조하십시오	Timestamp: 감사 메시지를 트리거한 이벤트가 생성된 시간으로, 운영 체제 Epoch(1970년 1월 1일 00:00:00 UTC) 이후 마이크로초 단위로 측정됩니다. 타임 스탬프를 로컬 날짜 및 시간으로 변환하는 데 사용할 수 있는 대부분의 도구는 밀리초를 기반으로 합니다. 로깅된 타임스탬프의 반올림 또는 잘라내기가 필요할 수 있습니다. 파일의 감사 메시지 시작 부분에 나타나는 사람이 읽을 수 있는 시간은 `audit.log` ISO 8601 형식의 ATIM 속성입니다. 날짜 및 시간은 로 *`YYYY-MMDDTHH:MM:SS.UUUUUU`* 표시되며, 여기서 는 `T` 날짜의 시간 세그먼트의 시작을 나타내는 리터럴 문자열 문자입니다. *`UUUUUU`* 마이크로초입니다.

코드	유형	설명
ATYP	에프씨32	이벤트 유형: 기록되는 이벤트의 4자리 식별자입니다. 이는 메시지의 "페이로드" 콘텐츠, 즉 포함된 속성을 제어합니다.
비버	UI32 를 참조하십시오	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	에프씨32	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 파일에 나타날 수 있는 감사 메시지의 예입니다 `audit.log`.

```
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. "SPUT" 오브젝트 수집을 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 특성의 사람이 읽을 수 있는 버전입니다.

```
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 값은 `1405631878959669` 2014년 7월 17일 목요일 21:17:59 UTC로 변환됩니다.

감사 메시지 및 개체 수명 주기

감사 메시지는 언제 생성됩니까**?**

감사 메시지는 개체가 수집되거나 검색되거나 삭제될 때마다 생성됩니다. S3 API별 감사 메시지를 찾아 감사 로그에서 이러한 트랜잭션을 식별할 수 있습니다.

감사 메시지는 각 프로토콜에 특정한 식별자를 통해 연결됩니다.

프로토콜	코드
S3 작업 연결	S3BK(버킷), S3KY(키) 또는 둘 다
Swift 작업 연결	WCON(컨테이너), WOBJ(오브젝트) 또는 둘 다
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.

S3 API 관련 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"

예**: S3** 오브젝트 수집

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 Make 2 Copies ILM 규칙이 포함되어 있습니다.

> 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 개체의 경우 Locs 필드에는 삭제 코딩 프로필 ID와 삭제 코딩 그룹 ID가 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

S3 API 관련 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 DeleteObject 요청을 LDR 서비스로 보내면 객체 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

S3 API별 감사 메시지를 찾아 감사 로그에서 오브젝트를 검색하여 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 GetObject 요청을 LDR 서비스로 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 자신이 소유하지 않은 버킷에 저장된 개체에 대해 GetObject 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 Select 요청의 승인(S3SR 필드는 "선택"으로 설정됨)을 수행하는 감사 메시지와 처리 중에 스토리지에서 데이터를 검색하는 후속 표준 GET 작업이라는 두 가지 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 (`x-amz-meta-\*`S3 객체(S3KY)에 대해 지정된 메타데이터를 업데이트하도록 요청(SUPD)을 수행합니다. 이 예제에서는 요청 헤더가 감사 프로토콜 헤더로 구성되었으므로 HTRH 필드에 요청 헤더가 포함되어 있습니다(구성 > 모니터링 > 감사 및 **syslog** 서버). 을 "감사 메시지 및 로그 대상을 구성합니다"참조하십시오.

```
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]]
```

감사 메시지

감사 메시지 설명

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 사용하여 특정 메시지에 대한 정보를 찾을 수 있습니다.

이 장에서 사용되는 4자리 코드는 다음 예제 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

시스템 감사 메시지

시스템 감사 범주에 속하는 감사 메시지는 감사 시스템 자체, 그리드 노드 상태, 시스템 전체 작업(그리드 작업) 및 서비스 백업 작업과 관련된 이벤트에 사용됩니다.

코드	메시지 제목 및 설명입니다	을 참조하십시오
ECMC	Missing Erasure - Coded Data Fragment: 누락된 삭제 코딩 데이터 조각이 감지되었음을 나타냅니다.	"ECMC: 삭제 누락 - 코드 데이터 조각"
ECOC	손상된 삭제 - 코딩된 데이터 조각: 손상된 삭제 코딩 데이터 조각이 감지되었음을 나타냅니다.	"ECOC: 손상된 삭제 - 코드화된 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"
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"
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"
추가	보안 감사 비활성화: 감사 메시지 로깅이 꺼졌습니다.	"추가: 보안 감사 비활성화"
사드	보안 감사 활성화: 감사 메시지 로깅이 복원되었습니다.	"Sade: 보안 감사 활성화"

코드	메시지 제목 및 설명입니다	을 참조하십시오
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"
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"

오브젝트 스토리지 감사 메시지

오브젝트 스토리지 감사 범주에 속하는 감사 메시지는 StorageGRID 시스템 내의 오브젝트 스토리지 및 관리와 관련된 이벤트에 사용됩니다. 여기에는 오브젝트 스토리지 및 검색, 그리드 노드에서 그리드 노드 전송, 검증도 포함됩니다.

기능이 더 이상 사용되지 않으므로 제품 및 설명서에서 감사 코드가 제거됩니다. 여기에 나열되지 않은 감사 코드가 발생하는 경우 이전 SG 릴리스에 대한 이 항목의 이전 버전을 확인하십시오. "StorageGRID 11.8 오브젝트 스토리지 감사 메시지"예를 들어,

코드	설명	을 참조하십시오
브루	버킷 읽기 전용 요청: 버킷이 읽기 전용 모드로 들어가거나 종료되었습니다.	"BROR: 버킷 읽기 전용 요청"
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"
CGRR	교차 그리드 복제 요청: StorageGRID는 그리드 연합 연결에서 버킷 간에 객체를 복제하기 위해 교차 그리드 복제 작업을 시도했습니다.	"CGRR: 교차 그리드 복제 요청"
EBDL	빈 버킷 삭제: ILM 스캐너가 모든 오브젝트를 삭제 중인 버킷 객체를 삭제했습니다(빈 버킷 작업 수행).	"EBDL: 빈 버킷 삭제"

코드	설명	을 참조하십시오
EBKR	빈 버킷 요청: 사용자가 빈 버킷을 켜거나 끄라는 요청을 보냈습니다(즉, 버킷 오브젝트를 삭제하거나 오브젝트 삭제를 중지하기 위해).	"EBKR: 빈 버킷 요청"
SCMT	오브젝트 저장소 커밋: 콘텐츠 블록이 완전히 저장되고 확인되었으므로 이제 요청할 수 있습니다.	"SCMT: 오브젝트 저장소 커밋 요청"
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 클라이언트 애플리케이션이 객체 검색을 요청할 때 기록됩니다.

코드	설명	사용자	을 참조하십시오
에스쓰리에스엘주식회사	S3 선택 요청: S3 선택 요청이 클라이언트에 반환된 후 완료를 기록합니다. S3SL 메시지에는 오류 메시지 및 오류 코드 세부 정보가 포함될 수 있습니다. 요청이 성공적으로 완료되지 않았을 수 있습니다.	S3 클라이언트	"S3SL:S3 선택 요청"
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

클라이언트 쓰기 감사 메시지는 S3 클라이언트 애플리케이션이 오브젝트를 생성하거나 수정하도록 요청할 때 기록됩니다.

코드	설명	사용자	을 참조하십시오
OVWR	오브젝트 덮어쓰기: 트랜잭션을 로그하여 한 오브젝트를 다른 오브젝트로 덮어씁니다.	S3 및 Swift 클라이언트	"OVWR: 개체 덮어쓰기"
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"

ILM 감사 메시지

ILM 감사 범주에 속하는 감사 메시지는 ILM(정보 수명 주기 관리) 작업과 관련된 이벤트에 사용됩니다.

코드	메시지 제목 및 설명입니다	을 참조하십시오
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"
ORLM	개체 규칙 충족: 이 감사 메시지는 ILM 규칙에 지정된 대로 개체 데이터가 저장될 때 생성됩니다.	"ORLM: 개체 규칙이 충족되었습니다"

감사 메시지 참조

BROR: 버킷 읽기 전용 요청

LDR 서비스는 버킷이 읽기 전용 모드로 들어가거나 나갈 때 이 감사 메시지를 생성합니다. 예를 들어 버킷은 모든 오브젝트가 삭제되는 동안 읽기 전용 모드로 전환됩니다.

코드	필드에 입력합니다	설명
BKHD	버킷 UUID	버킷 ID입니다.
브롬	버킷 읽기 전용 요청 값	버킷이 읽기 전용인지 읽기 전용 상태(1 = 읽기 전용, 0 = 읽기 전용 아님)에서 벗어나지 않아야 합니다.
브롬	버킷 읽기 전용 이유	버킷을 읽기 전용으로 만들거나 읽기 전용 상태로 두는 이유. 예를 들어, emptyBucket 과 같이 입력합니다.
에스쓰리아이주식회사	S3 테넌트 계정 ID입니다	요청을 보낸 테넌트 계정의 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.

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.

코드	필드에 입력합니다	설명
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.
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.

코드	필드에 입력합니다	설명
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 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 종료되었습니다

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.
CTSR	원본 요소	CBID 전송 소스(보낸 사람)의 노드 ID입니다.
CTDS	대상 요소	CBID 전송 대상(수신기)의 노드 ID입니다.

코드	필드에 입력합니다	설명
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.
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 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 종료되었습니다

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.

CGRR: 교차 그리드 복제 요청

이 메시지는 StorageGRID가 그리드 페더레이션 연결에서 버킷 간에 객체를 복제하기 위해 교차 그리드 복제 작업을 시도할 때 생성됩니다.

코드	필드에 입력합니다	설명
CSRZ	개체 크기	오브젝트의 크기(바이트)입니다. CSIZ 특성은 StorageGRID 11.8에 도입되었습니다. 따라서 StorageGRID 11.7에서 11.8 업그레이드를 포괄하는 교차 그리드 복제 요청의 총 개체 크기가 정확하지 않을 수 있습니다.
에스쓰리아이주식회사	S3 테넌트 계정 ID입니다	객체가 복제되는 버킷을 소유하는 테넌트 계정의 ID입니다.
GFID	그리드 페더레이션 연결 ID입니다	그리드 간 복제에 사용되고 있는 그리드 페더레이션 연결의 ID입니다.
작업	CGR 작동	시도된 교차 그리드 복제 작업의 유형: • 0 = 객체 복제 • 1 = 다중 파트 개체 복제 • 2 = 삭제 마커를 복제합니다
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.

코드	필드에 입력합니다	설명
에스3KY	S3 키	버킷 이름을 제외한 S3 키 이름.
VSID 를 선택합니다	버전 ID	복제되고 있는 개체의 특정 버전의 버전 ID입니다.
RSLT	결과 코드	SUID(SUCS) 또는 GENERAL ERROR(GERR)를 반환합니다.

EBDL: 빈 버킷 삭제

ILM 스캐너가 모든 오브젝트를 삭제 중인 버킷 내 오브젝트를 삭제했습니다(빈 버킷 작업 수행).

코드	필드에 입력합니다	설명
CSRZ	개체 크기	오브젝트의 크기(바이트)입니다.
경로	S3 버킷/키	S3 버킷 이름 및 S3 키 이름.
SEGC	컨테이너 UUID입니다	분할된 객체에 대한 컨테이너의 UUID입니다. 이 값은 개체가 분할된 경우에만 사용할 수 있습니다.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
RSLT	삭제 작업의 결과	이벤트, 프로세스 또는 트랜잭션의 결과 이 메시지와 관련이 없으면 메시지가 실수로 필터링되지 않도록 SUCS 대신 사용되지 않습니다.

EBKR: 빈 버킷 요청

이 메시지는 사용자가 빈 버킷을 설정 또는 해제하라는 요청을 보냈음을 나타냅니다(즉, 버킷 오브젝트를 삭제하거나 오브젝트 삭제를 중지).

코드	필드에 입력합니다	설명
BUID	버킷 UUID	버킷 ID입니다.
EBJS	버킷 JSON 구성이 비어 있습니다	현재 비어 있는 Bucket 구성을 나타내는 JSON을 포함합니다.
에스쓰리아이주식회사	S3 테넌트 계정 ID입니다	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.

ECMC: 삭제 누락 **-** 코드 데이터 조각

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 **-** 코드화된 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 ID	업데이트 요청을 시작한 서비스의 노드 ID입니다.

코드	필드에 입력합니다	설명
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 ID	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.

코드	필드에 입력합니다	설명
RSLT	결과	그리드 작업의 최종 상태 결과: • SUCS: 그리드 작업이 성공적으로 완료되었습니다. • ABRT: 롤백 오류 없이 그리드 작업이 종료되었습니다. • Rolf: 그리드 작업이 종료되어 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.
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.
- * 비준수 S3 버킷 * 의 객체용. 이 메시지는 현재 활성 ILM 정책의 배치 명령이 개체에 적용되지 않기 때문에 ILM이 개체 삭제 프로세스를 시작할 때 생성됩니다.

코드	필드에 입력합니다	설명
CBID	콘텐츠 블록 식별자	객체의 CBID입니다.
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. 버킷에 대한 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 개체의 경우 삭제 코딩 프로필 ID 및 개체의 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	S3 버킷 이름 및 S3 키 이름.
RSLT	결과	ILM 작업의 결과. SUCS: ILM 작업이 성공했습니다.

코드	필드에 입력합니다	설명
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.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
VSID 를 선택합니다	버전 ID	삭제된 개체의 특정 버전의 버전 ID입니다. 버전이 지정되지 않은 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 클라이언트에서 이미 개체가 포함된 경로에 개체를 쓸 때 개체를 덮어쓰게 됩니다. 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	S3 버킷 이름 및 S3 키 이름.
SEGC	컨테이너 UUID입니다	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.

LKDM: 유출된 개체 정리

이 메시지는 유출된 청크가 정리 또는 삭제되었을 때 생성됩니다. 청크는 복제된 개체나 삭제 인코딩된 개체의 일부가 될 수 있습니다.

코드	필드에 입력합니다	설명
CLOC를 선택합니다	청크 위치	삭제된 유출된 청크의 파일 경로입니다.

CTYP(CTYP	청크 유형입니다	청크 유형:
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

LTYP	누출 유형입니다	감지할 수 있는 5가지 누출 유형:
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM입니다	청크 생성 시간입니다	누출된 청크가 생성된 시간입니다.
UUID입니다	범용 고유 식별자	청크가 속한 개체의 식별자입니다.
CBID	콘텐츠 블록 식별자	누출된 청크가 속한 오브젝트의 CBID입니다.
CSRZ	콘텐츠 크기	청크 크기(바이트)입니다.

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
ECPR	삭제 - 코딩 프로필	삭제 코딩 오브젝트 데이터의 경우: 사용된 삭제 코딩 프로필의 ID입니다.

코드	필드에 입력합니다	설명
LTYP	위치 유형	CLDI(온라인): 복제된 개체 데이터의 경우 CLEC(온라인): 삭제 코딩 오브젝트 데이터 CLNL(Nearline): 아카이빙된 복제 객체 데이터의 경우
귀도	소스 노드 ID입니다	위치가 손실된 노드 ID입니다.
PCLD	복제된 객체에 대한 경로입니다	손실된 개체 데이터의 디스크 위치에 대한 전체 경로입니다. LTYP에 CLDI 값(즉, 복제된 개체의 경우)이 있는 경우에만 반환됩니다. 폼을 사용합니다 `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
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
UUID입니다	범용 고유 ID입니다	StorageGRID 시스템에서 영향을 받는 개체의 식별자입니다.

MGAU: 관리 감사 메시지

관리 범주는 사용자 요청을 관리 API에 기록합니다. 유효한 API URI에 대한 GET 또는 HEAD 요청이 아닌 모든 HTTP 요청은 API에 대한 사용자 이름, IP 및 요청 유형을 포함하는 응답을 기록합니다. 잘못된 API URI(예: /api/v3-authorize) 및 유효한 API URI에 대한 잘못된 요청은 기록되지 않습니다.

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.
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.

코드	필드에 입력합니다	설명
귀도	노드 ID	사용 가능한 경우 손실된 개체의 마지막으로 알려진 직접 또는 니어라인 위치입니다. 볼륨 정보를 사용할 수 없는 경우 볼륨 ID 없이 노드 ID만 가질 수 있습니다.
경로	S3 버킷/키	사용 가능한 경우 S3 버킷 이름 및 S3 키 이름입니다.
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	가능한 경우 손실된 객체의 마지막으로 알려진 위치에 대한 스토리지 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 개체의 경우 삭제 코딩 프로필 ID 및 개체의 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	S3 버킷 이름 및 S3 키 이름.

코드	필드에 입력합니다	설명
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 UUID입니다	분할된 객체에 대한 컨테이너의 UUID입니다. 이 값은 개체가 분할된 경우에만 사용할 수 있습니다.
SGCB	컨테이너 CBID입니다	분할된 객체에 대한 컨테이너의 CBID입니다. 이 값은 세그먼트화된 개체와 여러 부분으로 구성된 개체에만 사용할 수 있습니다.
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.
VSID 를 선택합니다	버전 ID	버전 관리되는 버킷에서 생성된 새 개체의 버전 ID입니다. 버전이 지정되지 않은 버킷의 버킷 및 오브젝트에 대한 작업에는 이 필드가 포함되지 않습니다.

단일 객체에 대해 ORLM 감사 메시지를 두 번 이상 발행할 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.
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 오브젝트 경로	이전 오브젝트와 새 오브젝트 모두에 사용된 S3 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.

S3SL:S3 선택 요청

이 메시지는 S3 Select 요청이 클라이언트에 반환된 후 완료를 기록합니다. S3SL 메시지에는 오류 메시지 및 오류 코드 세부 정보가 포함될 수 있습니다. 요청이 성공적으로 완료되지 않았을 수 있습니다.

코드	필드에 입력합니다	설명
BYSC	스캔된 바이트 수	스토리지 노드에서 스캔(수신)된 바이트 수입니다. 객체가 압축되면 BYSC와 BYPR은 다를 수 있습니다. 개체가 압축된 BYSC인 경우 압축된 바이트 수가 있고, BYPR은 압축 해제 후 바이트가 됩니다.
BYPR	처리된 바이트 수	처리된 바이트 수입니다. S3 Select 작업에서 실제로 처리되거나 작업된 "스캔한 바이트"의 바이트 수를 나타냅니다.
BYRT	반환된 바이트 수입니다	S3 Select 작업이 클라이언트에 반환한 바이트 수입니다.

코드	필드에 입력합니다	설명
재등록	레코드가 처리되었습니다	스토리지 노드에서 S3 Select 작업이 수신한 레코드 또는 행 수입니다.
오류	레코드가 반환되었습니다	클라이언트로 반환된 S3 Select 작업의 레코드 또는 행 수입니다.
JOFI	작업이 완료되었습니다	S3 Select 작업의 처리 완료 여부를 나타냅니다. 이 값이 거짓이면 작업이 완료되지 못했으며 오류 필드에 데이터가 있을 수 있습니다. 클라이언트가 일부 결과를 받았거나 전혀 결과를 받지 않았을 수 있습니다.
리드	요청 ID	S3 선택 요청의 식별자입니다.
EXTM	실행 시간	S3 Select 작업을 완료하는 데 걸리는 시간(초)입니다.
ERMG	오류 메시지	S3 Select 작업이 생성되었다는 오류 메시지입니다.
어티	오류 유형	S3 Select 작업이 생성한 오류 유형입니다.
ERST	오류 StackTrace	S3 선택 작업이 생성한 오류 StackTrace.
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.
S3AK(S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 S3 액세스 키 ID입니다.
에스쓰리아이주식회사	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다.
에스3KY	S3 키	버킷 이름을 제외한 S3 키 이름.

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.

코드	필드에 입력합니다	설명
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.

S3 클라이언트가 삭제 트랜잭션을 실행할 때 지정된 오브젝트 또는 버킷을 제거하거나 버킷/오브젝트 하위 리소스를 제거하도록 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. 버킷에 대한 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.
CSRZ	콘텐츠 크기	삭제된 개체의 크기(바이트)입니다. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.
DMRK	마커 버전 ID를 삭제합니다	버전이 있는 버킷에서 오브젝트를 삭제할 때 생성된 삭제 마커의 버전 ID입니다. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.
GFID	그리드 페더레이션 연결 ID입니다	교차 그리드 복제 삭제 요청과 연결된 그리드 페더레이션 연결의 연결 ID입니다. 대상 그리드의 감사 로그에만 포함됩니다.
GFSA	그리드 페더레이션 소스 계정 ID입니다	크로스 그리드 복제 삭제 요청에 대한 소스 그리드의 테넌트 계정 ID입니다. 대상 그리드의 감사 로그에만 포함됩니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. `X-Forwarded-For` 요청이 요청에 있고 값이 요청 보낸 사람 IP 주소(SAIP 감사 필드)와 다른 경우 자동으로 포함됩니다 `X-Forwarded-For`. `x-amz-bypass-governance-retention` 요청에 있는 경우 자동으로 포함됩니다.
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

코드	필드에 입력합니다	설명
에스쓰리아이주식회사	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3AK(S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 해시된 S3 액세스 키 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.
에스3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.
S3SR을 참조하십시오	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.
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. 예를 들면 다음과 같습니다. `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.

코드	필드에 입력합니다	설명
UUDM입니다	삭제 마커의 Universally Unique Identifier입니다	삭제 표시자의 식별자입니다. 감사 로그 메시지는 UUUDM 또는 UUID를 지정합니다. 여기서 UUDM은 객체 삭제 요청의 결과로 생성된 삭제 마커를 나타내고 UUID는 객체를 나타냅니다.
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
VSID 를 선택합니다	버전 ID	삭제된 개체의 특정 버전의 버전 ID입니다. 버전이 지정되지 않은 버킷의 버킷 및 오브젝트에 대한 작업에는 이 필드가 포함되지 않습니다.

SGET: S3 GET

S3 클라이언트가 가져오기 트랜잭션을 실행할 때 오브젝트를 검색하거나 버킷에 있는 오브젝트를 나열하거나 버킷/오브젝트 하위 리소스를 제거하기 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. 버킷에 대한 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.
CSRZ	콘텐츠 크기	검색된 객체의 크기(바이트)입니다. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. `X-Forwarded-For` 요청이 요청에 있고 값이 요청 보낸 사람 IP 주소(SAIP 감사 필드)와 다른 경우 자동으로 포함됩니다 `X-Forwarded-For`.
라일스	ListObjectsV2 를 참조하십시오	A_v2 format_response가 요청되었습니다. 자세한 내용은 을 참조하십시오 "AWS ListObjectsV2 를 참조하십시오". 버킷 가져오기 작업에만 해당됩니다.
NCHD의 약어입니다	어린이 수	키 및 일반 접두사를 포함합니다. 버킷 가져오기 작업에만 해당됩니다.
벨이 울렸습니다	Range Read(범위 읽기)	범위 읽기 작업에만 해당됩니다. 이 요청에서 읽은 바이트 범위를 나타냅니다. 슬래시(/) 뒤의 값은 전체 오브젝트의 크기를 표시합니다.

코드	필드에 입력합니다	설명
RSLT	결과 코드	Get 트랜잭션의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
에스쓰리아이주식회사	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3AK(S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 해시된 S3 액세스 키 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.
에스3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.
S3SR을 참조하십시오	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.
SUSR	S3 사용자 URN(요청 발신자)	테넌트 계정 ID 및 요청을 하는 사용자의 사용자 이름입니다. 사용자는 로컬 사용자 또는 LDAP 사용자일 수 있습니다. 예를 들면 다음과 같습니다. `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.
티알엔씨	잘리거나 잘리지 않습니다	모든 결과가 반환되면 false로 설정합니다. 반환할 수 있는 결과가 더 있으면 true 로 설정합니다. 버킷 가져오기 작업에만 해당됩니다.

코드	필드에 입력합니다	설명
UUID입니다	범용 고유 식별자	StorageGRID 시스템 내의 개체의 식별자입니다.
VSID 를 선택합니다	버전 ID	요청된 개체의 특정 버전의 버전 ID입니다. 버전이 지정되지 않은 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. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.
CNID	연결 식별자	TCP/IP 연결에 대한 고유한 시스템 식별자입니다.
CSRZ	콘텐츠 크기	선택한 오브젝트의 크기(바이트)입니다. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. `X-Forwarded-For` 요청이 요청에 있고 값이 요청 보낸 사람 IP 주소(SAIP 감사 필드)와 다른 경우 자동으로 포함됩니다 `X-Forwarded-For`.
RSLT	결과 코드	Get 트랜잭션의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
에스쓰리아이주식회사	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3AK(S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 해시된 S3 액세스 키 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.
에스3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷에 대한 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. 예를 들면 다음과 같습니다. `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. 버전이 지정되지 않은 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. `X-Forwarded-For` 요청이 요청에 있고 값이 요청 보낸 사람 IP 주소(SAIP 감사 필드)와 다른 경우 자동으로 포함됩니다 `X-Forwarded-For`. (spos는 예상되지 않음).
RSLT	결과 코드	RestoreObject 요청의 결과입니다. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
에스쓰리아이주식회사	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3AK(S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 해시된 S3 액세스 키 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.
에스3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.
S3SR을 참조하십시오	S3 하위 리소스	해당되는 경우, 작동 중인 버킷 또는 오브젝트 하위 자원. S3 Select 작업에 대해 "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.
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.

코드	필드에 입력합니다	설명
SUSR	S3 사용자 URN(요청 발신자)	테넌트 계정 ID 및 요청을 하는 사용자의 사용자 이름입니다. 사용자는 로컬 사용자 또는 LDAP 사용자일 수 있습니다. 예를 들면 다음과 같습니다. `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. 버전이 지정되지 않은 버킷의 버킷 및 오브젝트에 대한 작업에는 이 필드가 포함되지 않습니다.

SPUT: S3 PUT

S3 클라이언트가 PUT 트랜잭션을 실행할 때 새 오브젝트 또는 버킷을 생성하거나 버킷 /오브젝트 하위 리소스를 제거하도록 요청을 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. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.
CMPS	준수 설정	요청에 버킷을 생성할 때 사용되는 준수 설정(처음 1024자로 잘림)입니다.
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. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.
GFID	그리드 페더레이션 연결 ID입니다	교차 그리드 복제 PUT 요청과 연결된 그리드 페더레이션 연결의 연결 ID입니다. 대상 그리드의 감사 로그에만 포함됩니다.

코드	필드에 입력합니다	설명
GFSA	그리드 페더레이션 소스 계정 ID입니다	크로스 그리드 복제 PUT 요청에 대한 소스 그리드의 테넌트 계정 ID입니다. 대상 그리드의 감사 로그에만 포함됩니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. `X-Forwarded-For` 요청이 요청에 있고 값이 요청 보낸 사람 IP 주소(SAIP 감사 필드)와 다른 경우 자동으로 포함됩니다 `X-Forwarded-For`. x-amz-bypass-governance-retention 요청에 있는 경우 자동으로 포함됩니다.
LKEN	개체 잠금이 활성화되었습니다	요청에 있는 경우 요청 헤더의 x-amz-bucket-object-lock-enabled 값입니다.
LKLH	개체 잠금 법적 보류	PutObject 요청에 있는 경우 요청 헤더의 x-amz-object-lock-legal-hold 값입니다.
LKMD	개체 잠금 보존 모드	PutObject 요청에 있는 경우 요청 헤더의 x-amz-object-lock-mode 값입니다.
LKRU	개체 잠금 종료 날짜를 유지합니다	PutObject 요청에 있는 경우 요청 헤더의 x-amz-object-lock-retain-until-date 값입니다. 값은 객체가 수집된 날짜로부터 100년 이내로 제한됩니다.
MTME	마지막 수정 시간	객체가 마지막으로 수정된 시간을 나타내는 Unix 타임 스탬프(단위: 마이크로초)입니다.
RSLT	결과 코드	PUT 트랜잭션의 결과입니다. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다
에스쓰리아이주식회사	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3AK(S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 해시된 S3 액세스 키 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.

코드	필드에 입력합니다	설명
에스3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.
S3SR을 참조하십시오	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. 예를 들면 다음과 같습니다. `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.
ULID	업로드 ID입니다	CompleteMultipartUpload 작업에 대한 SPUT 메시지에만 포함됩니다. 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. 버전이 지정되지 않은 버킷의 버킷 및 오브젝트에 대한 작업에는 이 필드가 포함되지 않습니다.
VSST	버전 관리 상태	버킷의 새로운 버전 관리 상태입니다. "enabled" 또는 "Suspended"의 두 가지 상태가 사용됩니다. 개체 작업에 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. 버킷에 대한 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. 버킷에 대한 작업에는 이 필드가 포함되지 않습니다.
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. `X-Forwarded-For` 요청이 요청에 있고 값이 요청 보낸 사람 IP 주소(SAIP 감사 필드)와 다른 경우 자동으로 포함됩니다 `X-Forwarded-For`.
RSLT	결과 코드	Get 트랜잭션의 결과. 결과는 항상 다음과 같습니다. SUCS: 성공했습니다

코드	필드에 입력합니다	설명
에스쓰리아이주식회사	S3 테넌트 계정 ID(요청 발신자)	요청을 보낸 사용자의 테넌트 계정 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
S3AK(S3AK	S3 액세스 키 ID(요청 발신자)	요청을 보낸 사용자의 해시된 S3 액세스 키 ID입니다. 빈 값은 익명 액세스를 나타냅니다.
에스쓰리비케이주식회사	S3 버킷	S3 버킷 이름입니다.
에스3KY	S3 키	버킷 이름을 제외한 S3 키 이름. 버킷에 대한 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.
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. 예를 들면 다음과 같습니다. `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. 버전이 지정되지 않은 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.

이 메시지는 자세히 모니터링해야 합니다. 콘텐츠 검증 실패는 하드웨어 오류가 임박한 것을 의미할 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.
RSLT	결과	이 필드에는 '없음' 값이 있습니다. RSLT는 필수 메시지 필드이지만 이 메시지와 관련이 없습니다. 이 메시지가 필터링되지 않도록 'UCS' 대신 '없음'이 사용됩니다.

SVRU:Object Store Verify Unknown audit 메시지는 면밀하게 모니터링되어야 합니다. 오브젝트 저장소에서 예기치 않은 오브젝트 데이터 복사본이 감지되었음을 의미합니다. 이러한 상황은 즉각적인 조사를 통해 이러한 복사본이 어떻게 생성되었는지 확인해야 합니다. 이는 곧 하드웨어 오류가 발생할 수 있기 때문입니다.

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.

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. `X-Forwarded-For` 요청이 요청에 있고 값이 요청 보낸 사람 IP 주소(SAIP 감사 필드)와 다른 경우 자동으로 포함됩니다 `X-Forwarded-For`.
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.

코드	필드에 입력합니다	설명
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.
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. `X-Forwarded-For` 요청이 요청에 있고 값이 요청 보낸 사람 IP 주소(SAIP 감사 필드)와 다른 경우 자동으로 포함됩니다 `X-Forwarded-For`.

코드	필드에 입력합니다	설명
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.
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.

코드	필드에 입력합니다	설명
HTRH	HTTP 요청 헤더	구성 중에 선택한 로그 HTTP 요청 헤더 이름 및 값 목록입니다. `X-Forwarded-For` 요청이 요청에 있고 값이 요청 보낸 사람 IP 주소(SAIP 감사 필드)와 다른 경우 자동으로 포함됩니다 `X-Forwarded-For`.
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. `X-Forwarded-For` 요청이 요청에 있고 값이 요청 보낸 사람 IP 주소(SAIP 감사 필드)와 다른 경우 자동으로 포함됩니다 `X-Forwarded-For`.
MTME	마지막 수정 시간	객체가 마지막으로 수정된 시간을 나타내는 Unix 타임 스탬프(단위: 마이크로초)입니다.
RSLT	결과 코드	PUT 트랜잭션의 결과입니다. 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.
WUSR	SwiFT 계정 사용자	트랜잭션을 수행하는 클라이언트를 고유하게 식별하는 Swift 계정 사용자 이름입니다.

그리드를 확장합니다

확장 유형

시스템 운영을 중단하지 않고 StorageGRID 시스템의 용량이나 기능을 확장할 수 있습니다.

StorageGRID 확장을 통해 다음을 추가할 수 있습니다.

- 스토리지 노드에서 스토리지 볼륨으로 이동합니다
- 기존 사이트에 대한 새 그리드 노드
- 완전히 새로운 사이트

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.

수행 중인 확장 유형에 대한 단계를 따릅니다.

스토리지 볼륨을 추가합니다

의 단계를 "스토리지 노드에 스토리지 볼륨을 추가하는 중입니다"따릅니다.

그리드 노드를 추가합니다

1. 의 단계를 "기존 사이트에 그리드 노드 추가"따릅니다.
2. "서브넷을 업데이트합니다"..
3. 그리드 노드 구축:
   - "어플라이언스"
   - "VMware"
   - "리눅스"

   "Linux"는 Red Hat Enterprise Linux, Ubuntu 또는 Debian 배포를 의미합니다. 지원되는 버전 목록은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴(IMT)".
4. "확장을 수행합니다"..
5. "확장된 시스템을 구성합니다"..

새 사이트를 추가합니다

1. 의 단계를 "새 사이트 추가"따릅니다.
2. "서브넷을 업데이트합니다"..
3. 그리드 노드 구축:
   - "어플라이언스"
   - "VMware"
   - "리눅스"

   "Linux"는 Red Hat Enterprise Linux, Ubuntu 또는 Debian 배포를 의미합니다. 지원되는 버전 목록은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴(IMT)".
4. "확장을 수행합니다"..
5. "확장된 시스템을 구성합니다"..

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 또는 에 사용할 수 있는 스토리지를 증가시킬 "복제된 개체"위치 및 시기를 "스토리지 볼륨을 추가합니다""삭제 코딩 오브젝트"결정해야 합니다.
- 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 어플라이언스에 하나 또는 두 개의 확장 쉘프를 추가할 수 있습니다. 각 확장 쉘프에는 16개의 스토리지 볼륨이 추가됩니다. 두 확장 셸프가 모두 설치된 SG6060은 총 48개의 스토리지 볼륨을 지원할 수 있습니다.
- 각 SG6160 어플라이언스에 하나 또는 두 개의 확장 쉘프를 추가할 수 있습니다. 각 확장 쉘프에는 60개의 스토리지 볼륨이 추가됩니다. 두 확장 셸프가 모두 설치된 SG6160은 총 180개의 스토리지 볼륨을 지원할 수 있습니다.
- 스토리지 볼륨을 다른 스토리지 어플라이언스에 추가할 수 없습니다.
- 기존 스토리지 볼륨의 크기는 늘릴 수 없습니다.
- 시스템 업그레이드, 복구 작업 또는 다른 확장을 수행하는 동시에 스토리지 볼륨을 스토리지 노드에 추가할 수 없습니다.

스토리지 볼륨을 추가하고 ILM 정책을 충족하기 위해 확장해야 하는 스토리지 노드를 결정한 후에는 사용 중인 스토리지 노드 유형에 대한 지침을 따르십시오.

- 하나 또는 두 개의 확장 쉘프를 SG6060 스토리지 어플라이언스에 추가하려면 로 이동합니다 "배포된 SG6060에 확장 쉘프를 추가합니다".
- 하나 또는 두 개의 확장 쉘프를 SG6160 스토리지 어플라이언스에 추가하려면 로 이동합니다 "배포된 SG6160에 확장 쉘프를 추가합니다"
- 소프트웨어 기반 노드의 경우 의 지침을 "스토리지 노드에 스토리지 볼륨을 추가하는 중입니다"따릅니다.

스토리지 노드 추가 지침

기존 사이트에 스토리지 노드를 추가하기 전에 다음 지침 및 제한 사항을 검토하십시오.

- 현재 ILM 규칙을 검토하여 또는 에 사용할 수 있는 스토리지를 늘리기 위해 스토리지 노드를 추가할 위치와 시기를 결정해야 "복제된 개체""삭제 코딩 오브젝트"합니다.
- 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 "데이터 복구 작업을 확인합니다"참조하십시오.
- 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 시스템은 각 사이트에서 그리고 항상 을 사용할 수 있어야 "ADC 서비스 쿼럼입니다"합니다.
- 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 예로, 2개 사이트 그리드와 각 사이트에 개체 복사본을 만드는 ILM 규칙이 있는 경우 각 사이트에 연결하여 그리드의 전체 개체 용량을 늘려야 합니다"스토리지 추가". 개체 복제에 대한 자세한 내용은 을 참조하십시오"복제란 무엇입니까".

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. 그리드 관리자를 사용하여 "스토리지 용량을 모니터링하고 차트로 작성합니다 "수행할 수 있습니다.

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. 삭제 코딩 프로필에 대한 자세한 내용은 을 "삭제 코딩 체계란 무엇입니까"참조하십시오.

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.

이러한 권장 사항을 유발한 요인을 더 잘 이해하거나 사이트에 대한 보다 정확한 계획을 개발하려면 을(를) 참조하십시오"삭제 코딩 데이터의 재조정에 대한 고려사항". 귀사의 상황에 최적화된 맞춤형 권장사항을 보려면 NetApp 프로페셔널 서비스 컨설턴트에게 문의하십시오.

삭제 코딩 데이터의 재조정에 대한 고려사항

스토리지 노드를 추가하기 위해 확장을 수행하고 ILM 규칙을 사용하여 코드 데이터를 삭제하는 경우 사용 중인 삭제 코딩 체계에 스토리지 노드를 충분히 추가할 수 없는 경우 EC(삭제 코딩) 재조정 절차를 수행해야 할 수 있습니다.

이러한 고려 사항을 검토한 후 확장을 수행한 다음 로 "스토리지 노드를 추가한 후 삭제 코딩 데이터의 균형을 재조정합니다" 이동하여 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 사이트에서 기존 스토리지 노드와 새로 추가된 스토리지 노드 간에 재분배합니다.

EC 재조정 절차:

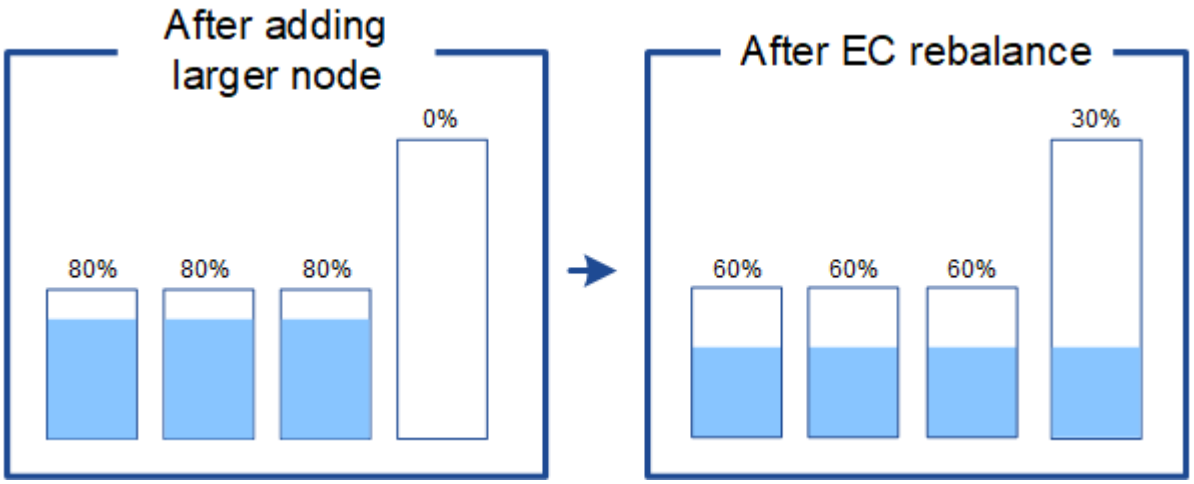
- 삭제 코딩 오브젝트 데이터만 이동합니다. 복제된 오브젝트 데이터는 이동하지 않습니다.
- 사이트 내에서 데이터를 재배포합니다. 사이트 간에 데이터를 이동하지 않습니다.
- 사이트의 모든 스토리지 노드 간에 데이터를 재배포합니다. 스토리지 볼륨 내에서 데이터를 재배포하지 않습니다.
- 에서는 삭제 코딩 데이터를 이동할 위치를 결정할 때 각 스토리지 노드에서 복제된 데이터 사용을 고려하지 않습니다.
- 각 노드의 상대적 용량을 고려하지 않고 삭제 코딩 데이터를 스토리지 노드 간에 균등하게 다시 분산합니다.
- 에서 삭제 코딩 데이터를 80% 이상 차 있는 스토리지 노드에 배포하지 않습니다.
- ILM 작업 및 S3 클라이언트 작업 실행 시 &#8212를 줄일 수 있음. 삭제 코딩 조각을 재배포하기 위해 추가 리소스가 필요합니다.

EC 재조정 절차가 완료되면 다음을 수행합니다.

- 삭제 코딩 데이터는 사용 가능한 공간이 적은 스토리지 노드에서 사용 가능한 공간이 더 많은 스토리지 노드로 이동됩니다.
- 삭제 코딩 오브젝트의 데이터 보호는 변경되지 않습니다.
- 사용된 (%) 값은 다음 두 가지 이유로 스토리지 노드 간에 다를 수 있습니다.
    - 복제된 오브젝트 복사본은 기존 노드 &#8212의 공간을 계속 사용합니다. EC 재조정 절차는 복제된 데이터를 이동하지 않습니다.

◦ 모든 노드가 비슷한 양의 삭제 코딩 데이터로 끝나더라도 용량이 큰 노드는 용량이 작은 노드보다 용량이 적은 노드로 비교적 적게 가득 차게 됩니다.

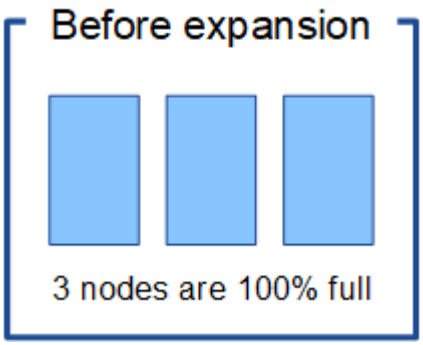
예를 들어, 200TB 노드 3개가 각각 80%(200 및 #215, 0.8 = 160TB, 사이트의 경우 480TB)로 채워졌다고 가정합니다. 400TB 노드를 추가하고 재조정 절차를 실행하면 모든 노드에 대략 동일한 양의 삭제 코드 데이터(480/4 = 120TB)가 제공됩니다. 그러나 더 큰 노드에 사용된 (%)은 더 작은 노드에 사용된 (%)보다 작습니다.



언제 삭제 코딩 데이터의 균형을 재조정할 수 있으며

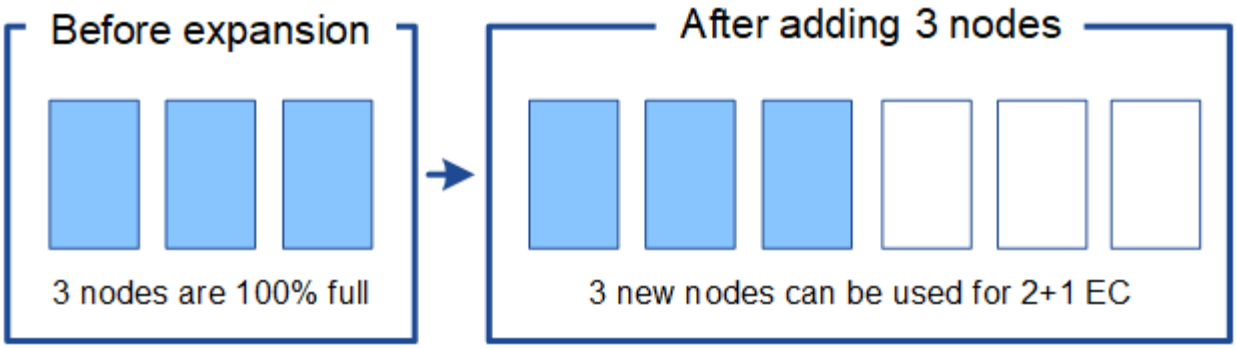
다음 시나리오를 고려해 보십시오.

- StorageGRID는 단일 사이트에서 실행 중이며 3개의 스토리지 노드가 있습니다.
- ILM 정책은 1.0 MB보다 큰 모든 개체에 2+1 삭제 코딩 규칙을 사용하고 더 작은 개체에 2-복사 복제 규칙을 사용합니다.
- 모든 스토리지 노드가 꽉 찼습니다. 주요 심각도 수준에서 * Low Object Storage * 경고가 트리거되었습니다.



노드를 충분히 추가하는 경우에는 재조정이 필요하지 않습니다

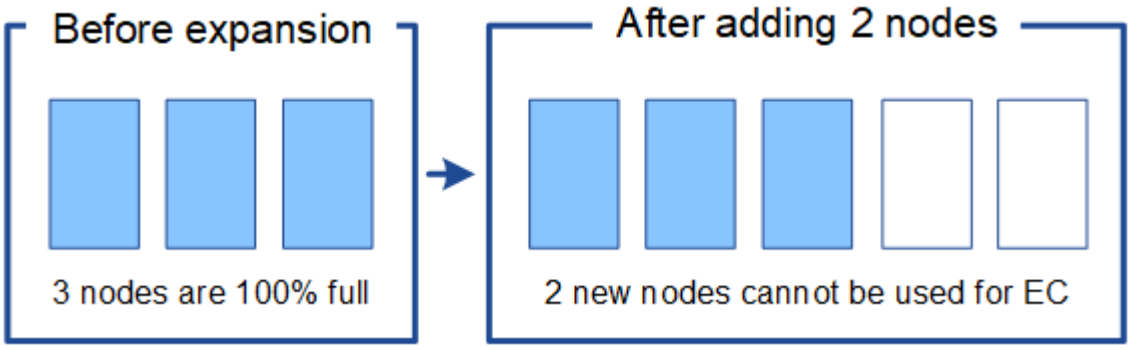
EC 균형 조정이 필요하지 않은 시기를 이해하려면 세 개 이상의 새 스토리지 노드를 추가했다고 가정합니다. 이 경우 EC 균형 조정을 수행할 필요가 없습니다. 원래 스토리지 노드가 가득 찬 상태로 유지되지만 새 오브젝트는 이제 2+1 삭제 코딩 및 #8212에 3개의 새 노드를 사용합니다. 두 데이터 조각과 하나의 패리티 조각을 각각 다른 노드에 저장할 수 있습니다.



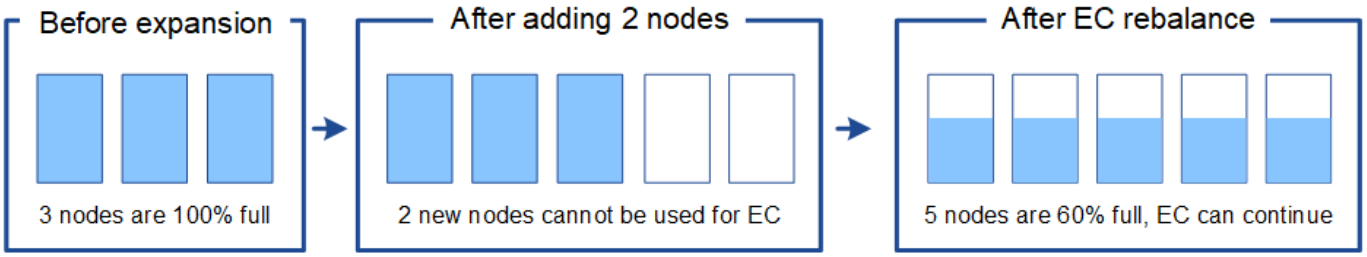
이 경우 EC 재조정 절차를 실행할 수 있지만 기존 삭제 코딩 데이터를 이동하면 그리드 성능이 일시적으로 저하되어 클라이언트 작업에 영향을 줄 수 있습니다.

노드를 충분히 추가할 수 없는 경우 재조정이 필요합니다

EC 균형 조정이 필요한 시기를 이해하려면 세 개가 아닌 두 개의 스토리지 노드만 추가할 수 있다고 가정합니다. 2+1 구성표에 사용 가능한 공간이 세 개 이상의 스토리지 노드가 필요하므로 빈 노드는 새로운 삭제 코딩 데이터에 사용할 수 없습니다.



새 스토리지 노드를 사용하려면 EC 재조정 절차를 실행해야 합니다. 이 절차를 실행하면 StorageGRID는 사이트의 모든 스토리지 노드 간에 기존의 삭제 코딩 데이터 및 패리티 조각을 재배포합니다. 이 예에서 EC 재조정 절차가 완료되면 5개 노드 모두 60%만 채워지고 모든 스토리지 노드의 2+1 삭제 코딩 체계에 오브젝트가 계속 수집될 수 있습니다.



EC 재조정 권장 사항

다음 중 _ALL_이 맞으면 NetApp에서 EC 재조정을 요구합니다.

- 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 사용할 새 스토리지 노드를 추가할 수 없습니다. 을 "삭제 코딩 오브젝트를 위한 스토리지 용량을 추가합니다"참조하십시오.
- S3 클라이언트는 EC 재조정 절차가 실행되는 동안 쓰기 및 읽기 작업에 대해 낮은 성능을 허용할 수 있습니다.

스토리지 노드를 비슷한 수준으로 채우도록 하고 EC 재조정 절차가 실행되는 동안 S3 클라이언트에서 쓰기 및 읽기 작업 성능이 저하될 수 있는 경우 선택적으로 EC 재조정 절차를 실행할 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 추가한 후 EC 균형 조정 절차를 실행합니다.
업그레이드 절차	아니요 StorageGRID 소프트웨어를 업그레이드해야 하는 경우 EC 재조정 절차를 실행하기 전이나 후에 업그레이드 절차를 수행합니다. 필요에 따라 EC 재조정 절차를 종료하여 소프트웨어 업그레이드를 수행할 수 있습니다.
어플라이언스 노드 클론 절차	아니요 어플라이언스 스토리지 노드를 복제해야 하는 경우 새 노드를 추가한 후 EC 재조정 절차를 실행합니다.
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 실행되는 동안 기존 삭제 코딩 오브젝트의 위치를 변경할 수 있는 ILM을 변경하지 마십시오. 예를 들어 삭제 코딩 프로필이 다른 ILM 규칙을 사용하지 마십시오. 이러한 ILM을 변경해야 하는 경우 EC 재조정 절차를 종료해야 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.
- 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.

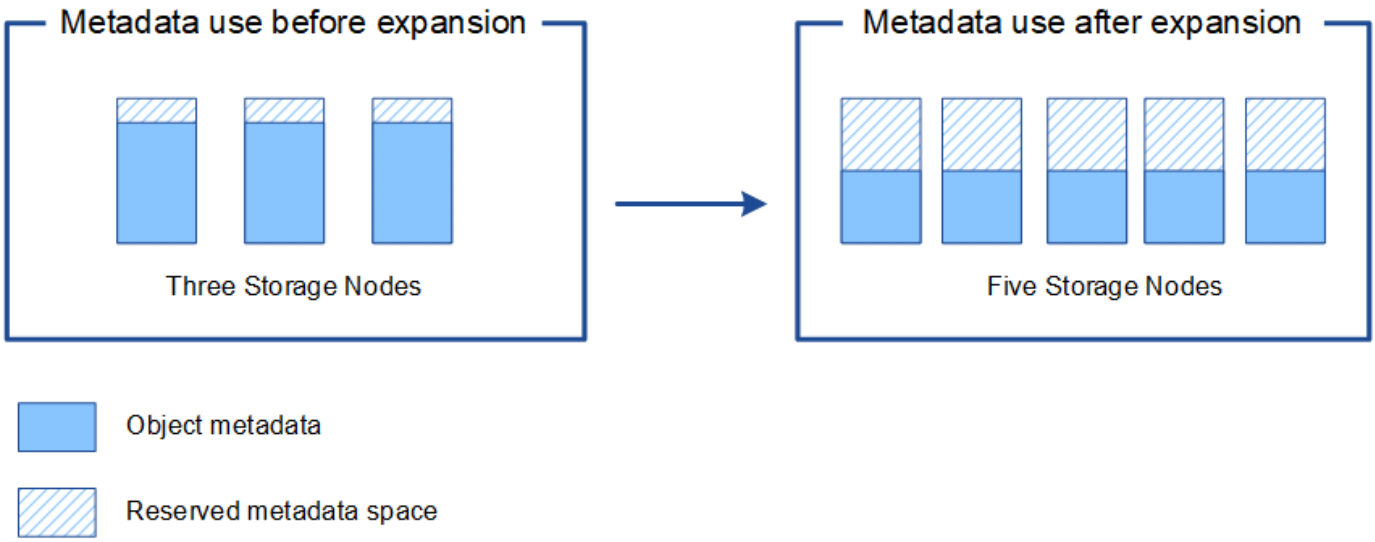
를 "메타데이터 예약된 공간에 대한 설명입니다"참조하십시오.

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 보여 줍니다. 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 고가용성(HA) 그룹에서 사용할 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

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 "오브젝트 용량 추가 지침 "참조하십시오.

- 방화벽 제어 페이지의 신뢰할 수 없는 클라이언트 네트워크 탭에서 * 새 노드 기본값 설정 * 옵션이 * 신뢰할 수 없음 * 인 경우 클라이언트 네트워크를 사용하여 확장 노드에 연결하는 클라이언트 응용 프로그램은 로드 밸런서 끝점 포트(* 구성 * > * 보안 * > * 방화벽 제어 *)를 사용하여 연결해야 합니다. 및 의 지침을 "새 노드의 보안 설정을 변경합니다""로드 밸런서 엔드포인트를 구성합니다"참조하십시오.

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 를 참조하십시오"ILM 정책 변경 예".

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 StorageGRID 설치 파일 다운로드 및 추출참조하십시오. • 참고: * 기존 스토리지 노드에 새 스토리지 볼륨을 추가하거나 새 StorageGRID 어플라이언스를 설치하는 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 암호가 `Passwords.txt` 파일에 없습니다.
StorageGRID 설명서	• "StorageGRID 관리" • "릴리스 정보" • 플랫폼에 대한 설치 지침 ◦ "Red Hat Enterprise Linux에 StorageGRID를 설치합니다" ◦ "Ubuntu 또는 Debian에 StorageGRID를 설치합니다" ◦ "VMware에 StorageGRID를 설치합니다"
현재 사용 중인 플랫폼에 대한 설명서입니다	지원되는 버전은 를 "상호 운용성 매트릭스 툴(IMT)"참조하십시오.

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. 로 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 `.tgz` 플랫폼에 대한 또는 `.zip` 파일을 선택합니다.

   설치 아카이브 파일에 표시된 버전이 현재 설치된 소프트웨어 버전과 일치해야 합니다.

   서비스 랩톱에서 Windows를 실행하는 경우 이 `.zip` 파일을 사용합니다.

플랫폼	설치 아카이브
Red Hat Enterprise Linux	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
Ubuntu 또는 Debian 또는 어플라이언스	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`
VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`
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 시스템을 확장하는 경우 적절한 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 호스트에 StorageGRID 노드 이미지를 설치하기 위한 rpm 패키지입니다.

경로 및 파일 이름입니다	설명
	RHEL 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	스크립트와 함께 사용할 예제 구성 파일 `configure-storagegrid.py`
	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제 이 스크립트를 Ping 연합 통합에 사용할 수도 있습니다.
/rpms/configure -StorageGrid.blank.json을 지정합니다	스크립트와 함께 사용할 빈 구성 `configure-storagegrid.py` 파일입니다.
	StorageGRID 컨테이너 배포를 위해 RHEL 호스트를 구성하기 위한 Ansible 역할 및 플레이북 예 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.
	Active Directory 또는 Ping 연방을 사용하여 SSO(Single Sign-On)를 사용하도록 설정한 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/rpms/StorageGrid-ssoauth-Azure.js	Azure와의 SSO 상호 작용을 수행하기 위해 Python 스크립트에 의해 호출되는 도우미 스크립트입니다. `storagegrid-ssoauth-azure.py`
/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	파일의 MD5 체크섬 `/debs/storagegrid-webscale-images-version-SHA.deb`.
/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 이 스크립트를 Ping 연합 통합에 사용할 수도 있습니다.
/debs/configure -StorageGrid.sample.json 을 참조하십시오	스크립트와 함께 사용할 예제 구성 파일 `configure-storagegrid.py`
/debs/configure -StorageGrid.blank.json 을 참조하십시오	스크립트와 함께 사용할 빈 구성 `configure-storagegrid.py` 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.
	Active Directory 또는 Ping 연방을 사용하여 SSO(Single Sign-On)를 사용하도록 설정한 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제

경로 및 파일 이름입니다	설명
/debs/StorageGrid-ssoauth-Azure.js를 입력합니다	Azure와의 SSO 상호 작용을 수행하기 위해 Python 스크립트에 의해 호출되는 도우미 스크립트입니다. `storagegrid-ssoauth-azure.py`
/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.
	Open Virtualization Format 템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 기본 관리자 노드를 배포할 수 있습니다.
	템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 비기본 관리 노드를 배포합니다.
	템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 게이트웨이 노드를 배포할 수 있습니다.
	템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 가상 머신 기반 스토리지 노드를 구축합니다.
배포 스크립팅 도구	설명
	가상 그리드 노드의 배포를 자동화하는 데 사용되는 Bash 쉘 스크립트입니다.

경로 및 파일 이름입니다	설명
	스크립트와 함께 사용할 예제 구성 파일 `deploy-vsphere-ovftool.sh`
	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 스크립트의 예 이 스크립트를 Ping 연합 통합에 사용할 수도 있습니다.
/vSphere/configure -StorageGrid.sample.json을 참조하십시오	스크립트와 함께 사용할 예제 구성 파일 `configure-storagegrid.py`
/vSphere/configure -StorageGrid.blank.json 을 참조하십시오	스크립트와 함께 사용할 빈 구성 `configure-storagegrid.py` 파일입니다.
	Active Directory 또는 Ping 연방을 사용하여 SSO(Single Sign-On)를 사용하도록 설정한 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/vSphere/StorageGrid-ssoauth-Azure.js	Azure와의 SSO 상호 작용을 수행하기 위해 Python 스크립트에 의해 호출되는 도우미 스크립트입니다. `storagegrid-ssoauth-azure.py`
/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	파일의 MD5 체크섬 `/debs/storagegridwebscale-images-version-SHA.deb`.

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). 특히, 확장에서 추가하는 새 노드와 기본 관리 노드 사이에 다음 TCP 포트가 열려 있는지 확인합니다.
  - 1055
  - 7443
  - 8011
  - 10342를 참조하십시오

  을 "내부 그리드 노드 통신"참조하십시오.
- 기본 관리 노드는 StorageGRID 시스템을 호스트하기 위한 모든 확장 서버와 통신할 수 있습니다.
- 새 노드 중 이전에 사용되지 않은 서브넷에 그리드 네트워크 IP 주소가 있는 노드가 있으면 그리드 네트워크 서브넷 목록에 이미 있는 "새 서브넷을 추가했습니다"것입니다. 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.

시작하기 전에

스토리지 볼륨을 추가하기 전에 를 검토하여 "오브젝트 용량 추가 지침"ILM 정책의 요구 사항을 충족하기 위해 볼륨을 추가할 위치를 알고 있는지 확인합니다.

> 이 지침은 소프트웨어 기반 스토리지 노드에만 적용됩니다. 확장 셸프를 설치하여 스토리지 볼륨을 SG6060 또는 SG6160에 추가하는 방법은 또는 "배포된 SG6160에 확장 쉘프를 추가합니다" 를 참조하십시오 "배포된 SG6060에 확장 쉘프를 추가합니다". 다른 어플라이언스 스토리지 노드를 확장할 수 없습니다.

이 작업에 대해

스토리지 노드의 기본 스토리지는 스토리지 볼륨으로 분할됩니다. 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 개체 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 OS(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.

시작하기 전에

- VMware 배포용 StorageGRID 설치 지침을 액세스할 수 있습니다.
  - "VMware에 StorageGRID를 설치합니다"
- `Passwords.txt`파일이 있습니다.
- 있습니다. "특정 액세스 권한"

> 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 다음 명령을 입력하여 가상 머신을 다시 시작합니다.`sudo reboot`

   > 가상 컴퓨터를 다시 시작하기 위해 * Power Off * 또는 * Reset * 을 사용하지 마십시오.
4. 스토리지 노드에서 사용할 새 스토리지를 구성합니다.
   a. 그리드 노드에 로그인합니다.
      i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
      ii. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
      iii. 다음 명령을 입력하여 루트로 전환합니다. `su -`

iv. 파일에 나열된 암호를 `Passwords.txt` 입력합니다. 루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

b. 새 스토리지 볼륨 구성:

```
sudo add_rangedbs.rb
```

이 스크립트는 새 스토리지 볼륨을 찾아 포맷하라는 메시지를 표시합니다.

c. y * 를 입력하여 서식을 적용합니다.

d. 이전에 포맷된 볼륨이 있는 경우 다시 포맷할지 여부를 결정합니다.

- 다시 포맷하려면 * y * 를 입력합니다.
- 포맷을 건너뛰려면 * n * 을 입력합니다.

`setup_rangedbs.sh`스크립트가 자동으로 실행됩니다.

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. 을 사용하여 그리드 관리자에 "지원되는 웹 브라우저"로그인합니다.

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.

시작하기 전에

- Linux 플랫폼용 StorageGRID 설치 지침을 액세스할 수 있습니다.
  - "Red Hat Enterprise Linux에 StorageGRID를 설치합니다"
  - "Ubuntu 또는 Debian에 StorageGRID를 설치합니다"
- `Passwords.txt`파일이 있습니다.
- 있습니다. "특정 액세스 권한"

> 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 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 에서 찾을 수 있는 스토리지 노드의 노드 구성 파일을 편집합니다. `/etc/storagegrid/nodes/<node-name>.conf`
7. 기존 오브젝트 스토리지 블록 디바이스 매핑이 포함된 노드 구성 파일의 섹션을 찾습니다.

   이 예에서 `BLOCK_DEVICE_RANGEDB_00` 에 는 `BLOCK_DEVICE_RANGEDB_03` 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 단계부터 `BLOCK_DEVICE_RANGEDB_nn` 시작해야 합니다. 간격을 두지 마십시오.

   - 위의 예제를 기준으로 부터 `BLOCK_DEVICE_RANGEDB_04` 시작합니다.
   - 아래 예에서는 새로운 블록 스토리지 볼륨 4개가 node: `BLOCK_DEVICE_RANGEDB_04`에 `BLOCK_DEVICE_RANGEDB_07`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 유사한 오류가 관찰되면 노드 구성 파일이 에 대해 <PURPOSE> 사용되는 블록 장치를 Linux 파일 시스템의 에 <path-name> 매핑하려고 <node-name> 하지만 해당 위치에 유효한 블록 장치 특수 파일(또는 블록 장치 특수 파일에 대한 소프트링크)이 없다는 의미입니다.

```
Checking configuration file for node <node-name>…
ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
<path-name> is not a valid block device
```

을(를) 올바르게 입력했는지 <path-name> 확인합니다.

10. 다음 명령을 실행하여 새 블록 디바이스 매핑이 있는 노드를 다시 시작합니다.

```
sudo storagegrid node start <node-name>
```

11. 파일에 나열된 암호를 사용하여 스토리지 노드에 admin으로 `Passwords.txt` 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.

    b. 스토리지 볼륨을 포맷하려면 * y * 를 입력합니다.
    c. 이전에 포맷된 볼륨이 있는 경우 다시 포맷할지 여부를 결정합니다.
       - 다시 포맷하려면 * y * 를 입력합니다.
       - 포맷을 건너뛰려면 * n * 을 입력합니다.

       `setup_rangedbs.sh`스크립트가 자동으로 실행됩니다.

14. 스토리지 노드의 스토리지 상태가 온라인 상태인지 확인합니다.
    a. 을 사용하여 그리드 관리자에 "지원되는 웹 브라우저"로그인합니다.
    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.
15. 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

기존 사이트에 그리드 노드를 추가하거나 새 사이트를 추가하려면 다음 절차를 따르십시오. 한 번에 하나의 확장 유형만 수행할 수 있습니다.

시작하기 전에

- 이 "루트 액세스 또는 유지 관리 권한"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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"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. CIDR 표시법으로 새 서브넷을 추가하려면 * 다른 서브넷 추가 * 를 선택합니다.

   예를 들어, 을 `10.96.104.0/22`입력합니다.

3. 프로비저닝 암호를 입력하고 * Save * 를 선택합니다.
4. 변경 사항이 적용될 때까지 기다린 다음 새 복구 패키지를 다운로드합니다.
   a. 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
   b. Provisioning Passphrase * 를 입력합니다.

> ⚠ 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다. 또한 기본 관리 노드를 복구하는 데 사용됩니다.

지정한 서브넷은 StorageGRID 시스템에 대해 자동으로 구성됩니다.

새 그리드 노드를 배포합니다

확장 시 새 그리드 노드를 구축하는 단계는 그리드를 처음 설치할 때 사용한 단계와 동일합니다. 확장을 수행하려면 먼저 모든 새 그리드 노드를 배포해야 합니다.

그리드를 확장할 때 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. 새로운 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.

시작하기 전에

- 사용 중인 Linux 버전에 대한 StorageGRID 설치 지침이 있으며 하드웨어 및 스토리지 요구 사항을 검토했습니다.
  - "Red Hat Enterprise Linux에 StorageGRID를 설치합니다"
  - "Ubuntu 또는 Debian에 StorageGRID를 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 노드가 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

모든 새 그리드 노드를 배포한 후 "확장을 수행합니다"수행할 수 있습니다.

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.

시작하기 전에

- 이 제품은 랙 또는 캐비닛에 설치되었고 네트워크에 연결되어 있으며 전원이 켜져 있습니다.
- "하드웨어를 설정합니다"단계를 완료했습니다.

어플라이언스 하드웨어 설정에는 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. 버전이 호환되지 않는 경우 StorageGRID 어플라이언스 설치 프로그램 펌웨어를 업그레이드해야 합니다.
- 가 있는 서비스 랩톱이 "지원되는 웹 브라우저"있습니다.
- 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 배포해야 하는 경우 어플라이언스 설치 스크립트를 사용하여 설치 프로세스를 자동화할 수 `configure-sga.py` 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 활성화 * 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 활성화 * 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.

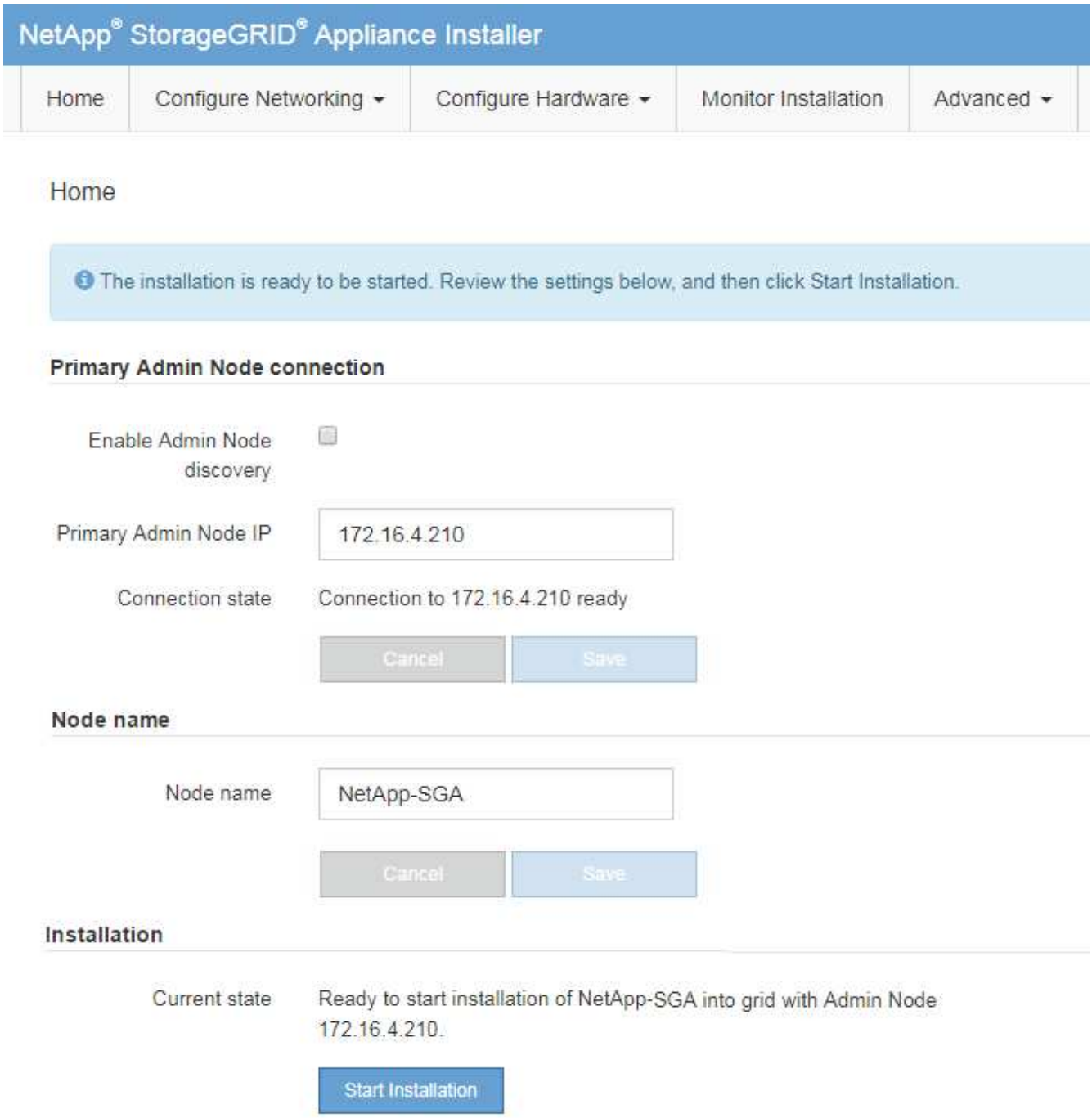
4. 노드 이름 * 필드에 이 어플라이언스 노드에 사용할 이름을 입력하고 * 저장 * 을 선택합니다.

   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. Installation * 섹션에서 현재 상태가 "기본 Admin Node_admin_IP_로 _node name_into GRID 설치를 시작할 준비가 되었습니다"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 유지보수 지침을 참조하십시오.

6. StorageGRID 어플라이언스 설치 관리자 홈 페이지에서 * 설치 시작 * 을 선택합니다.



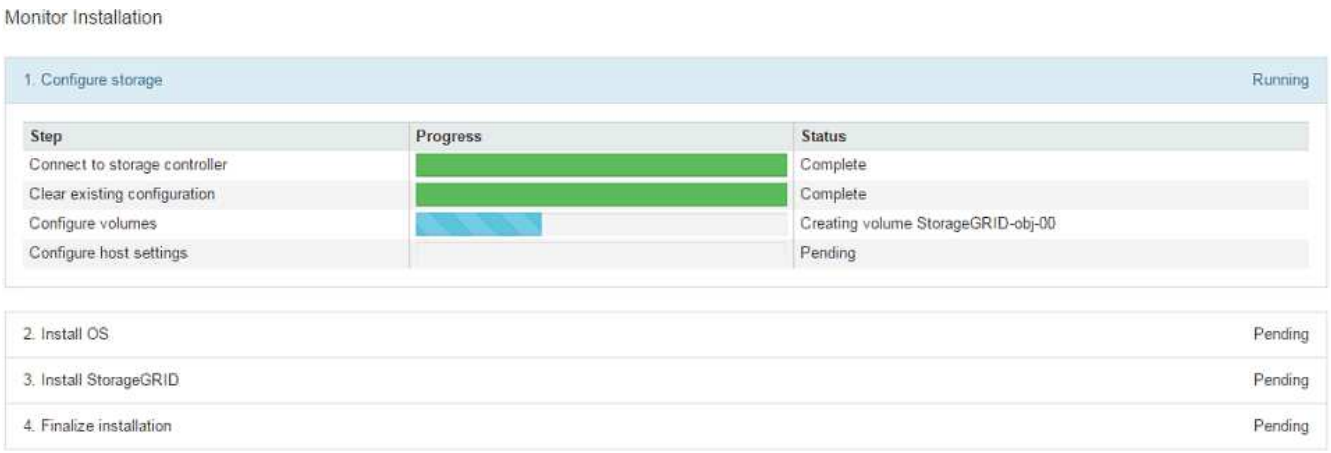
현재 상태가 "Installation is in progress(설치 진행 중)"로 변경되고 Monitor Installation(모니터 설치) 페이지가 표시됩니다.

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 실행하는 경우 다시 실행할 필요가 없는 작업은 녹색 상태 표시줄과 "건너뜀"으로 표시됩니다.

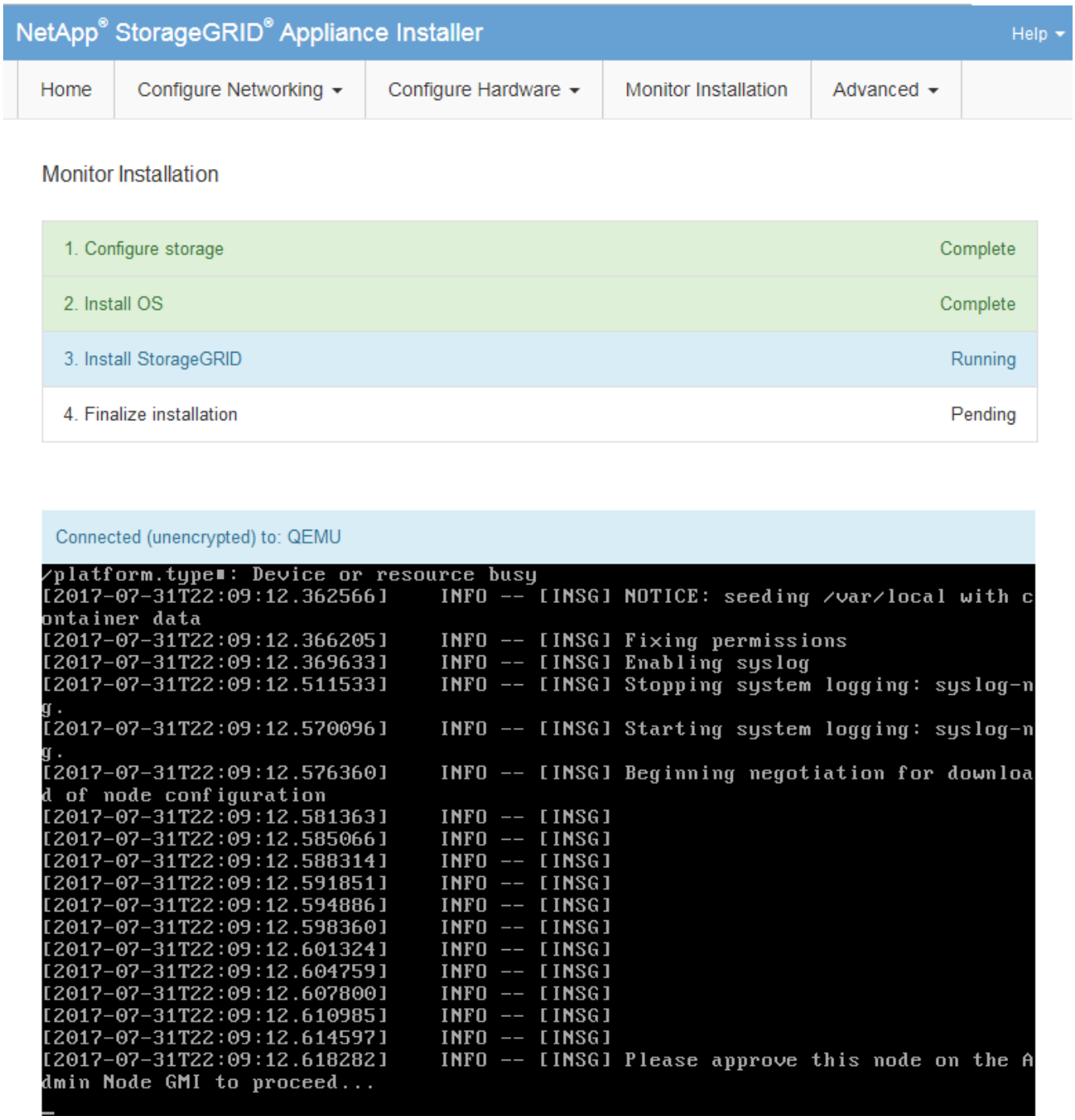
9. 처음 두 설치 단계의 진행 상황을 검토합니다.
   - 1. 어플라이언스 구성 *

     이 단계에서 다음 프로세스 중 하나가 발생합니다.

     - 스토리지 어플라이언스의 경우 설치 프로그램이 스토리지 컨트롤러에 연결하고, 기존 구성을 지우고, SANtricity OS와 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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 프로비저닝 암호가 있습니다.
- 이 확장에서 추가되는 모든 그리드 노드를 배포했습니다.
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.

- 스토리지 노드를 추가하는 경우 복구의 일부로 수행된 모든 데이터 복구 작업이 완료되었음을 확인했습니다. 을 "데이터 복구 작업을 확인합니다"참조하십시오.
- 스토리지 노드를 추가하는 경우 해당 노드에 사용자 지정 스토리지 등급을 할당하려는 경우 이미 을"사용자 지정 스토리지 등급을 생성했습니다"(를) 보유하고 있습니다. 루트 액세스 권한이나 유지 관리 및 ILM 권한도 모두 있습니다.
- 새 사이트를 추가하는 경우 ILM 규칙을 검토 및 업데이트했습니다. 확장이 완료될 때까지 오브젝트 복사본이 새 사이트에 저장되지 않도록 해야 합니다. 예를 들어, 규칙이 기본 스토리지 풀(* All Storage Nodes *)을 사용하는 경우 기존 스토리지 노드 및 새 스토리지 풀을 사용하려면 ILM 정책만 "ILM 규칙을 업데이트합니다"포함해야 "새 스토리지 풀을 생성합니다"합니다. 그렇지 않으면 해당 사이트의 첫 번째 노드가 활성 상태가 되는 즉시 새 사이트에 개체가 복사됩니다.

이 작업에 대해

확장을 수행하는 작업에는 다음과 같은 주요 사용자 작업이 포함됩니다.

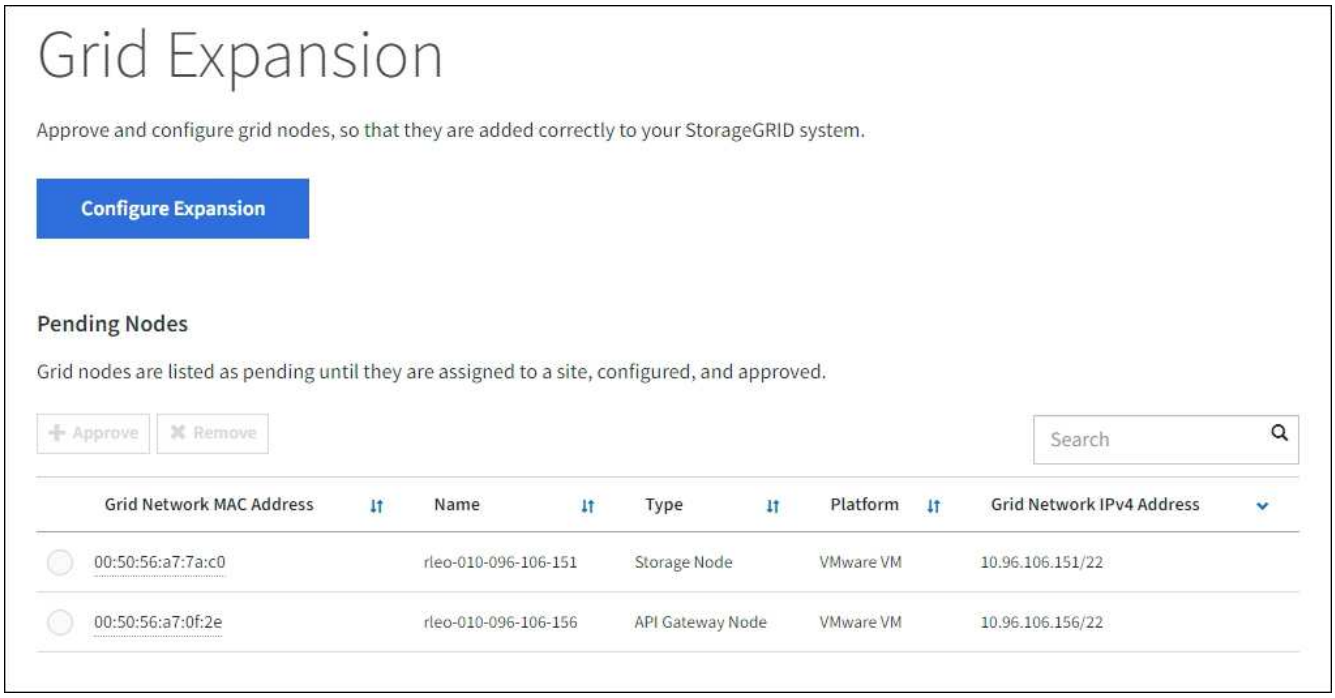
1. 확장을 구성합니다.
2. 확장을 시작합니다.
3. 새 복구 패키지 파일을 다운로드합니다.
4. 모든 새 노드가 설치 및 구성되고 모든 서비스가 시작될 때까지 확장 단계 및 단계를 모니터링합니다.

> 일부 확장 단계 및 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 노드가 나열됩니다.

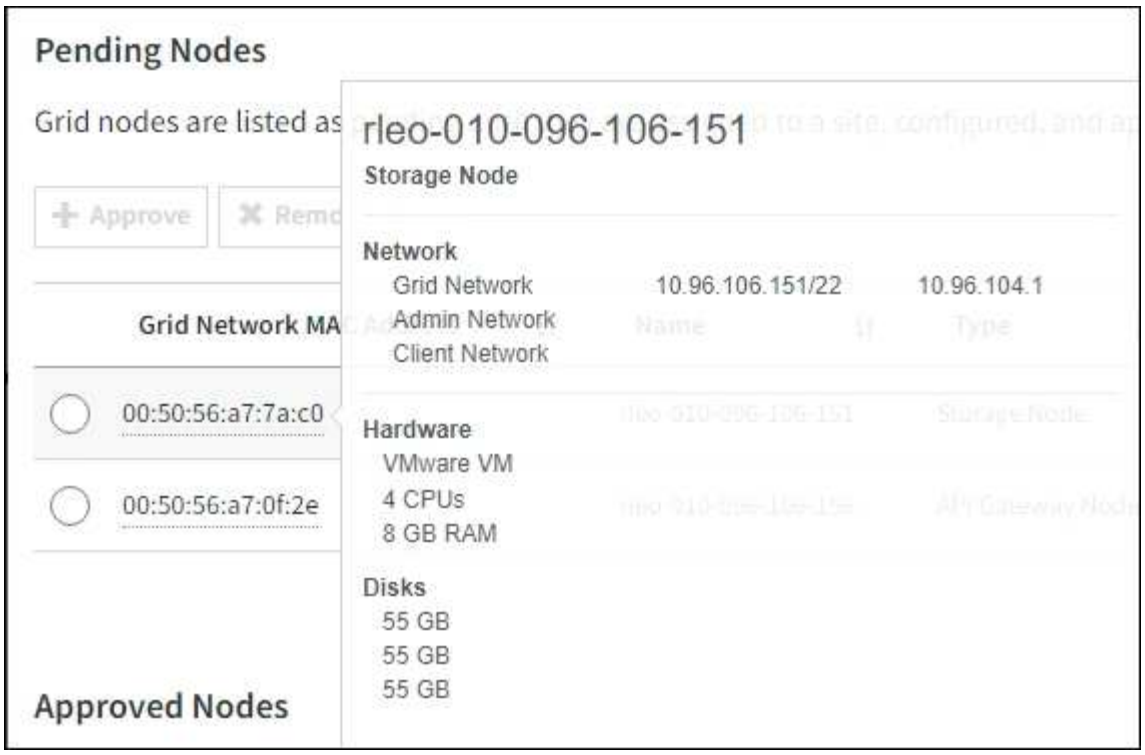


2. Configure Expansion * 을 선택합니다.

   사이트 선택 대화 상자가 나타납니다.

3. 시작할 확장 유형을 선택합니다.
   - 새 사이트를 추가하는 경우 * New * 를 선택하고 새 사이트의 이름을 입력합니다.
   - 기존 사이트에 하나 이상의 노드를 추가하는 경우 * Existing * 을 선택합니다.
4. 저장 * 을 선택합니다.
5. Pending Nodes * 목록을 검토하고 배포한 모든 그리드 노드가 표시되는지 확인합니다.

   필요한 경우 노드의 * Grid Network MAC Address * 위에 커서를 놓으면 해당 노드에 대한 세부 정보를 볼 수 있습니다.



노드가 누락된 경우 성공적으로 배포되었는지 확인합니다.

6. 보류 중인 노드 목록에서 이 확장에 추가할 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.

필드에 입력합니다	설명
사이트	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	노드의 시스템 이름입니다. 시스템 이름은 내부 StorageGRID 작업에 필요하며 변경할 수 없습니다.
스토리지 유형(스토리지 노드만 해당)	• * 데이터 및 메타데이터 * ("결합"): 오브젝트 데이터 및 메타데이터 스토리지 노드 • * 데이터 전용 *: 오브젝트 데이터만 포함하는 스토리지 노드(메타데이터 없음) • * 메타데이터 전용 *: 메타데이터만 포함하는 스토리지 노드(오브젝트 데이터 없음)

필드에 입력합니다	설명
NTP 역할입니다	그리드 노드의 NTP(Network Time Protocol) 역할: • NTP 역할을 노드에 자동으로 할당하려면 * Automatic * (기본값)을 선택합니다. 기본 역할은 관리 노드, ADC 서비스가 있는 스토리지 노드, 게이트웨이 노드 및 비정적 IP 주소가 있는 모든 그리드 노드에 할당됩니다. 클라이언트 역할은 다른 모든 그리드 노드에 할당됩니다. • 기본 NTP 역할을 노드에 수동으로 할당하려면 * Primary * 를 선택합니다. 외부 타이밍 소스에 대한 중복 시스템 액세스를 제공하려면 각 사이트에 최소 2개의 노드가 기본 역할을 가져야 합니다. • 클라이언트 NTP 역할을 노드에 수동으로 할당하려면 * 클라이언트 * 를 선택합니다.
ADC 서비스(결합 또는 메타데이터 전용 스토리지 노드)	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. • 교체할 스토리지 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. • 시스템에서 이 노드에 ADC 서비스가 필요한지 여부를 결정하도록 하려면 * Automatic * 을 선택합니다. 에 대해 자세히 "ADC 쿼럼"알아보십시오.
스토리지 등급(결합 또는 데이터 전용 스토리지 노드)	기본 * 스토리지 등급을 사용하거나 이 새 노드에 할당할 사용자 지정 스토리지 등급을 선택합니다. 스토리지 등급은 ILM 스토리지 풀에서 사용되므로 선택한 항목은 스토리지 노드에 배치할 개체에 영향을 줄 수 있습니다.

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

> 노드를 승인하는 동안 그리드 네트워크에서 노드가 중복 IP 주소를 가지고 있는 경우 확장을 취소하고 비중복 IP로 가상 시스템 또는 어플라이언스를 재배포한 다음 확장을 다시 시작해야 합니다.

- * 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.

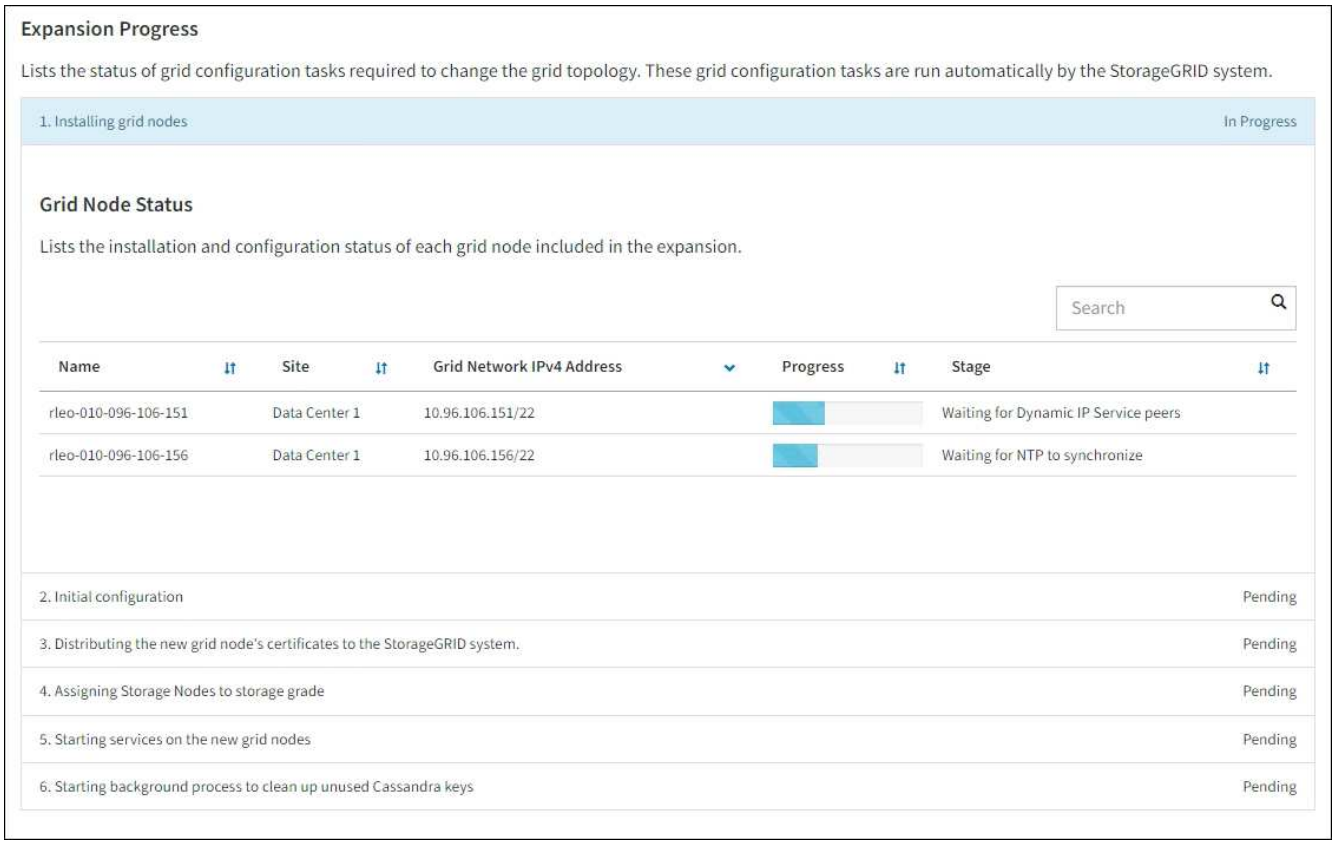
f. 승인하려는 보류 중인 각 그리드 노드에 대해 이 단계를 반복합니다.

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.

새 어플라이언스에 대한 "그리드 노드 설치" 단계에서 StorageGRID 어플라이언스 설치 프로그램은 3단계에서 4단계로 이동한 설치 완료, 설치를 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 파일을 열고 `.zip` 파일을 포함한 콘텐츠에 액세스할 수 있는지 `Passwords.txt` 확인합니다.

d. 다운로드한 복구 패키지 파일(`.zip`)을 안전한 별도의 두 위치에 복사합니다.

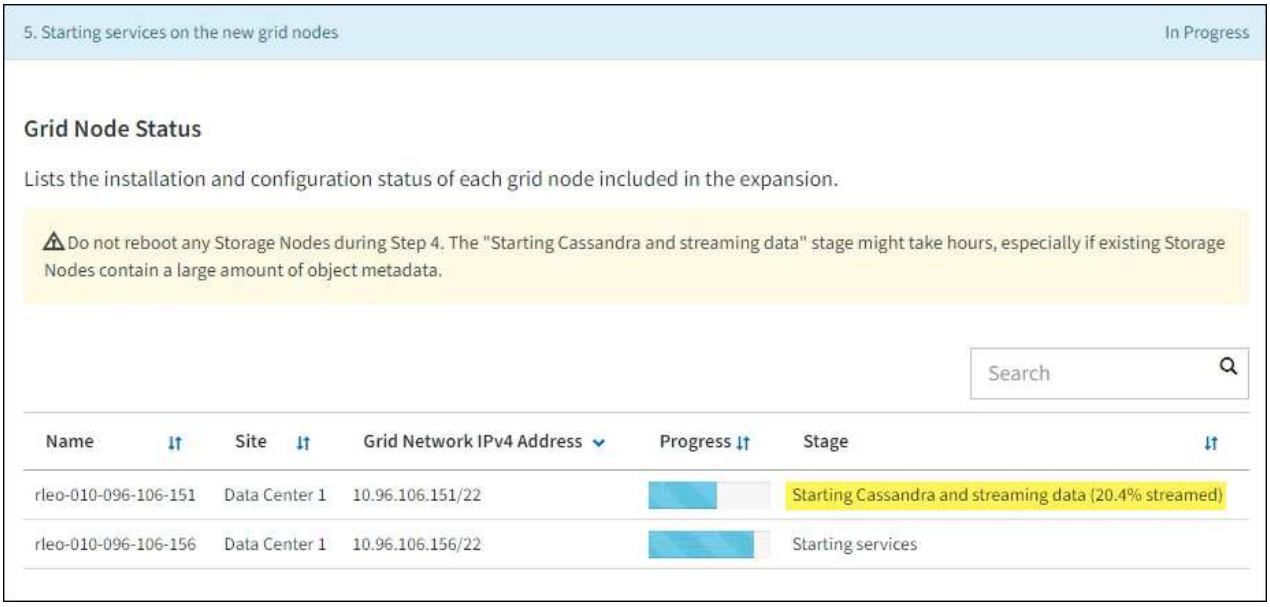
> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다.

9. 기존 사이트에 스토리지 노드를 추가하거나 사이트를 추가하는 경우 새 그리드 노드에서 서비스가 시작될 때 Cassandra 단계를 모니터링합니다.

> "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.

스토리지 노드 추가

기존 사이트에 스토리지 노드를 추가하는 경우 "Starting Cassandra and streaming data" 상태 메시지에 표시된 비율을 검토합니다.



이 백분율은 Cassandra 스트리밍 작업이 완료된 정도를 추정합니다. 이 수치는 사용 가능한 Cassandra 데이터의 총 양과 이미 새 노드에 기록된 데이터를 기준으로 합니다.

사이트 추가

새 사이트를 추가하는 경우 를 사용하여 `nodetool status` Cassandra 스트리밍 진행 상황을 모니터링하고 "Cassandra 클러스터 확장" 단계에서 새 사이트에 복사된 메타데이터의 양을 확인합니다. 새 사이트의 총 데이터 로드는 현재 사이트의 총 데이터 로드 중 약 20% 이내여야 합니다.

10. 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 수행합니다. 을 "확장 후 구성 단계"참조하십시오.

확장된 시스템을 구성합니다

확장 후 구성 단계

확장을 완료한 후에는 추가 통합 및 구성 단계를 수행해야 합니다.

이 작업에 대해

확장 시 추가하는 그리드 노드 또는 사이트에 대해 아래 나열된 구성 작업을 완료해야 합니다. 시스템 설치 및 관리 시 선택한 옵션과 확장 중에 추가한 노드 및 사이트를 구성하는 방법에 따라 일부 작업은 선택 사항일 수 있습니다.

단계

1. 사이트를 추가한 경우:

- "스토리지 풀을 생성합니다" 새 스토리지 노드에 대해 선택한 사이트 및 각 스토리지 등급에 대해
- ILM 정책이 새로운 요구 사항을 충족하는지 확인합니다. 규칙 변경이 필요한 경우, "새 규칙을 만듭니다" 및"ILM 정책을 업데이트합니다". 규칙이 이미 올바른 경우 "새 정책을 활성화합니다"StorageGRID가 새 노드를 사용하도록 하기 위해 규칙이 변경되지 않습니다.
- 해당 사이트에서 NTP(Network Time Protocol) 서버에 액세스할 수 있는지 확인합니다. 을 "NTP 서버를 관리합니다"참조하십시오.

> 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.

2. 기존 사이트에 하나 이상의 스토리지 노드를 추가한 경우:
   - "스토리지 풀 세부 정보를 봅니다" 추가한 각 노드가 예상 스토리지 풀에 포함되어 있고 예상 ILM 규칙에 사용되는지 확인합니다.
   - ILM 정책이 새로운 요구 사항을 충족하는지 확인합니다. 규칙 변경이 필요한 경우, "새 규칙을 만듭니다" 및"ILM 정책을 업데이트합니다". 규칙이 이미 올바른 경우 "새 정책을 활성화합니다"StorageGRID가 새 노드를 사용하도록 하기 위해 규칙이 변경되지 않습니다.
   - "스토리지 노드가 활성 상태인지 확인합니다" 또한, 오브젝트를 수집할 수 있습니다.
   - 권장 스토리지 노드 수를 추가할 수 없는 경우 삭제 코딩 데이터의 균형을 재조정합니다. 을 "스토리지 노드를 추가한 후 삭제 코딩 데이터의 균형을 재조정합니다"참조하십시오.
3. 게이트웨이 노드를 추가한 경우:
   - 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 "고가용성 그룹을 구성합니다"참조하십시오.
4. 관리 노드를 추가한 경우:
   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 "Single Sign-On 구성"참조하십시오.
   b. 관리 노드에서 로드 밸런서 서비스를 사용하려는 경우 필요에 따라 새 관리 노드를 HA 그룹에 추가합니다. 구성 * > * 네트워크 * > * 고가용성 그룹 * 을 선택하여 기존 HA 그룹 목록을 검토하고 새 노드를 추가합니다. 을 "고가용성 그룹을 구성합니다"참조하십시오.
   c. 필요에 따라 각 관리 노드에서 속성과 감사 정보를 일관되게 유지하려면 운영 관리 노드에서 확장 관리 노드로 관리 노드 데이터베이스를 복사합니다. 을 "관리 노드 데이터베이스를 복사합니다"참조하십시오.
   d. 필요에 따라 각 관리 노드에서 기간별 메트릭을 일관되게 유지하려면 Prometheus 데이터베이스를 기본 관리 노드에서 확장 관리 노드로 복사합니다. 을 "Prometheus 메트릭을 복사합니다"참조하십시오.
   e. 필요에 따라 각 관리 노드에서 기록 로그 정보를 일관되게 유지하려면 기존 감사 로그를 기본 관리 노드에서 확장 관리 노드로 복사합니다. 을 "감사 로그를 복사합니다"참조하십시오.
5. 신뢰할 수 없는 클라이언트 네트워크로 확장 노드가 추가되었는지 확인하거나 노드의 클라이언트 네트워크가 신뢰할 수 없는 것인지 여부를 변경하려면 * 구성 * > * 보안 * > * 방화벽 제어 * 로 이동하십시오.

   확장 노드의 클라이언트 네트워크를 신뢰할 수 없는 경우 로드 밸런서 끝점을 사용하여 클라이언트 네트워크의 노드에 연결해야 합니다. "로드 밸런서 엔드포인트를 구성합니다"및 을 "방화벽 제어 관리"참조하십시오.

6. DNS를 구성합니다.

   각 그리드 노드에 대해 DNS 설정을 별도로 지정한 경우 새 노드에 대해 노드별 DNS 설정을 사용자 지정해야 합니다. 을 "단일 그리드 노드에 대한 DNS 구성을 수정합니다"참조하십시오.

제대로 작동하려면 DNS 서버를 두 대 또는 세 대 지정합니다. 3개 이상을 지정하면 일부 플랫폼의 알려진 OS 제한 때문에 3개만 사용할 수 있습니다. 사용자 환경에 라우팅 제한이 있는 경우 개별 노드(일반적으로 사이트의 모든 노드)에서 최대 3개의 DNS 서버로 구성된 다른 세트를 사용할 수 "DNS 서버 목록을 사용자 지정합니다"있습니다.

가능한 경우 각 사이트에서 로컬로 액세스할 수 있는 DNS 서버를 사용하여 isfan 사이트가 외부 대상의 FQDN을 확인할 수 있도록 합니다.

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. 을 사용하여 그리드 관리자에 "지원되는 웹 브라우저"로그인합니다.
2. nodes * > **Expansion Storage Node* * > * Storage * 를 선택합니다.
3. 커서를 * Storage Used - Object Data * 그래프 위에 놓으면 * Used * 의 값을 볼 수 있습니다. 이 값은 오브젝트 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.

시작하기 전에

- 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
- 노드 페이지의 레거시 스타일 차트에 사용되는 내역 특성 데이터입니다

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. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
      ii. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
      iii. 다음 명령을 입력하여 루트로 전환합니다. `su -`
      iv. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   b. 다음 명령을 실행합니다. `recover-access-points`
   c. 프로비저닝 암호를 입력합니다.
   d. MI 서비스를 중지합니다. `service mi stop`
   e. 관리 응용 프로그램 인터페이스(mgmt-API) 서비스를 중지합니다. `service mgmt-api stop`
2. 확장 관리 노드에서 다음 단계를 완료합니다.
   a. 확장 관리 노드에 로그인합니다.
      i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
      ii. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
      iii. 다음 명령을 입력하여 루트로 전환합니다. `su -`
      iv. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   b. MI 서비스를 중지합니다. `service mi stop`
   c. mgmt-API 서비스 중지: `service mgmt-api stop`
   d. SSH 에이전트에 SSH 개인 키를 추가합니다. 다음을 입력합니다.`ssh-add`
   e. 파일에 나열된 SSH 액세스 암호를 `Passwords.txt` 입력합니다.
   f. 소스 관리자 노드에서 확장 관리자 노드로 데이터베이스 복사: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   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. 다음을 입력합니다.`ssh-add -D`
3. 기본 관리자 노드에서 서비스를 다시 시작합니다. `service servermanager start`

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.

시작하기 전에

- 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. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
2. 소스 관리자 노드에서 Prometheus 서비스를 중지합니다. `service prometheus stop`
3. 새 관리 노드에서 다음 단계를 완료합니다.
   a. 새 관리자 노드에 로그인합니다.
      i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
      ii. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
      iii. 다음 명령을 입력하여 루트로 전환합니다. `su -`
      iv. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   b. Prometheus 서비스를 중지합니다. `service prometheus stop`
   c. SSH 에이전트에 SSH 개인 키를 추가합니다. 다음을 입력합니다.`ssh-add`
   d. 파일에 나열된 SSH 액세스 암호를 `Passwords.txt` 입력합니다.
   e. 소스 관리자 노드에서 새 관리자 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.

```
Database cloned, starting services
```

a. 다른 서버에 대한 암호 없는 액세스가 더 이상 필요하지 않으면 SSH 에이전트에서 개인 키를 제거합니다. 입력:

```
ssh-add -D
```

4. 소스 관리 노드에서 Prometheus 서비스를 다시 시작합니다.

```
service prometheus start
```

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.

시작하기 전에

- 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.
>
> 자세한 내용은 을 "감사 메시지 및 로그 대상을 구성합니다" 참조하십시오.

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@_primary_Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. AMS 서비스를 중지하면 새 파일이 생성되지 않습니다. `service ams stop`

3. 감사 내보내기 디렉터리로 이동합니다.

   ```
   cd /var/local/log
   ```

4. 소스 파일의 이름을 `audit.log` 변경하여 복사할 확장 관리자 노드의 파일을 덮어쓰지 않도록 합니다.

   ```
   ls -l
   mv audit.log _new_name_.txt
   ```

5. 모든 감사 로그 파일을 확장 관리자 노드의 대상 위치로 복사합니다.

   ```
   scp -p * IP_address:/var/local/log
   ```

6. 에 대한 암호를 입력하라는 메시지가 표시되면 파일에 나열된 기본 관리자 노드의 SSH 액세스 암호를 `Passwords.txt` 입력합니다 `/root/.ssh/id_rsa`.

7. 원본 파일 복원 `audit.log`:

   ```
   mv new_name.txt audit.log
   ```

8. AMS 서비스를 시작합니다.

   ```
   service ams start
   ```

9. 서버에서 로그아웃합니다.

   ```
   exit
   ```

10. 확장 관리 노드에 로그인합니다.
    a. 다음 명령을 입력합니다. `ssh admin@expansion_Admin_Node_IP`
    b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
    c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
    d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

       루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

11. 감사 로그 파일에 대한 사용자 및 그룹 설정을 업데이트합니다.

    ```
    cd /var/local/log

    chown ams-user:bycast *
    ```

12. 서버에서 로그아웃합니다.

    ```
    exit
    ```

스토리지 노드를 추가한 후 삭제 코딩 데이터의 균형을 재조정합니다

스토리지 노드를 추가한 후 삭제 코딩(EC) 재조정 절차를 사용하여 기존 및 새 스토리지 노드 간에 삭제 코딩 조각을 재배포할 수 있습니다.

시작하기 전에

- 새 스토리지 노드를 추가하는 확장 단계를 완료했습니다.
- 를 검토했습니다."삭제 코딩 데이터의 재조정에 대한 고려사항"
- 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 절차를 실행하면 어떻게 됩니까

절차를 시작하기 전에 다음 사항에 유의하십시오.

- 하나 이상의 볼륨이 오프라인 상태(마운트 해제)이거나 온라인 상태(마운트)이지만 오류 상태인 경우 EC 균형 조정 절차가 시작되지 않습니다.
- 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 절차가 진행되는 동안 볼륨이 오프라인 상태가 되면 재조정 절차가 종료됩니다. 이미 이동된 데이터 조각은 새 위치에 유지되며 데이터는 손실되지 않습니다.

  모든 볼륨이 다시 온라인 상태가 된 후 절차를 다시 실행할 수 있습니다.

- EC 재조정 절차가 실행되면 ILM 작업 및 S3 클라이언트 작업의 성능에 영향을 미칠 수 있습니다.

> 오브젝트(또는 오브젝트 파트)를 업로드하는 S3 API 작업이 완료되는 데 24시간 이상이 필요한 경우 EC 재조정 절차 중에 실패할 수 있습니다. 해당 ILM 규칙이 수집 시 균형 또는 엄격 배치를 사용하는 경우 장기 PUT 작업이 실패합니다. 다음 오류가 보고됩니다 `500 Internal Server Error`.

- 이 절차 중에 모든 노드의 스토리지 용량은 80%로 제한됩니다. 이 제한을 초과하지만 여전히 대상 데이터 파티션 아래에 저장되는 노드는 다음 대상에서 제외됩니다.
  - 사이트 불균형 값입니다
  - 모든 작업 완료 조건

> 대상 데이터 파티션은 사이트의 전체 데이터를 노드 수로 나누어 계산합니다.

- * 작업 완료 조건 *. EC 재조정 절차는 다음 중 하나에 해당하면 완료된 것으로 간주됩니다.
  - 삭제 코딩 데이터를 더 이상 이동할 수 없습니다.
  - 모든 노드의 데이터가 대상 데이터 파티션의 5% 편차 내에 있습니다.
  - 이 절차는 30일 동안 실행되었습니다.

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. 커서를 Storage Used-Object Data 차트 위에 놓으면 스토리지 노드에서 복제된 데이터의 현재 양과 삭제 코딩 데이터를 볼 수 있습니다.
   e. 사이트에서 다른 스토리지 노드를 보려면 다음 단계를 반복합니다.
2. 기본 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.
3. 절차를 시작합니다.

   're balance-data start—site "*site-name*"

   "*site-name*"의 경우 새 스토리지 노드를 추가한 첫 번째 사이트를 지정합니다. 따옴표로 묶습니다. `site-name`

   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`

     의 경우 *`job-id`* 프로시저를 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 --help`
6. 반환된 상태에 따라 추가 단계를 수행합니다.
   - 이(가) `In progress` 인 경우 `State` EC 재조정 작업이 계속 실행 중입니다. 절차가 완료될 때까지 주기적으로 모니터링해야 합니다.

     이 값을 사용하여 `Site Imbalance` 사이트의 스토리지 노드 전체에서 불균형한 삭제 코드 데이터 사용이

어떻게 되는지 평가하십시오. 이 값의 범위는 1.0에서 0까지이며, 0은 삭제 코딩 데이터 사용량이 사이트의 모든 스토리지 노드에 걸쳐 완전히 균형 조정되었음을 나타냅니다.

EC 재조정 작업은 완료된 것으로 간주되며 모든 노드의 데이터가 대상 데이터 파티션의 5% 편차 내에 있을 때 중지됩니다.

- 가 인 `Success` 경우 `State` 필요에 따라 오브젝트 스토리지 검토사이트의 업데이트된 세부 정보를 볼 수 있습니다.

  이제 삭제 코딩 데이터가 사이트의 스토리지 노드 간에 더 균형 있게 균형 있게 조정되어야 합니다.

- `Failure`다음과 같은 경우 `State`:

  i. 사이트의 모든 스토리지 노드가 그리드에 연결되어 있는지 확인합니다.

  ii. 이러한 스토리지 노드에 영향을 줄 수 있는 알림을 확인하고 해결합니다.

  iii. EC 재조정 절차를 다시 시작합니다.

  ```
  rebalance-data start --job-id job-id
  ```

  iv. 상태를 봅니다 를 참조하십시오. 이(가) 계속 `Failure` 표시되면 `State` 기술 지원 부서에 문의하십시오.

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
   ```

   EC 재조정 절차를 종료하면 이미 이동된 데이터 조각이 새 위치에 남아 있습니다. 데이터가 원래 위치로 다시 이동되지 않습니다.

9. 둘 이상의 사이트에서 삭제 코딩을 사용하는 경우 영향을 받는 다른 모든 사이트에 대해 이 절차를 실행합니다.

확장 문제 해결

그리드 확장 프로세스 중에 해결할 수 없는 오류가 발생하거나 그리드 작업이 실패하는 경우 로그 파일을 수집하고 기술 지원 부서에 문의하십시오.

기술 지원에 문의하기 전에 문제 해결에 도움이 되는 필요한 로그 파일을 수집합니다.

단계

1. 장애가 발생한 확장 노드에 연결:

   a. 다음 명령을 입력합니다.`ssh -p 8022 admin@grid_node_IP`

      포트 8022는 기본 OS의 SSH 포트이고, 포트 22는 StorageGRID를 실행하는 컨테이너 엔진의 SSH 포트입니다.

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 설치에 도달한 단계에 따라 그리드 노드에서 사용할 수 있는 다음 로그를 검색합니다.

플랫폼	로그
VMware	• `/var/log/daemon.log` • `/var/log/storagegrid/daemon.log` • `/var/log/storagegrid/nodes/<node-name>.log`
리눅스	• `/var/log/storagegrid/daemon.log` • `/etc/storagegrid/nodes/<node-name>.conf` (장애가 발생한 각 노드에 대해) • `/var/log/storagegrid/nodes/<node-name>.log` (장애가 발생한 각 노드에 대해, 존재하지 않을 수 있음)

StorageGRID 시스템을 유지 관리합니다

그리드 유지 관리

그리드 유지 관리 작업에는 노드 또는 사이트 사용 중단, 그리드, 노드 또는 사이트 이름 변경, 네트워크 유지 관리가 포함됩니다. 또한 호스트 및 미들웨어 절차와 그리드 노드 프로시저를 수행할 수 있습니다.

이 지침에서 "Linux"는 Red Hat ® Enterprise Linux ®, Ubuntu ® 또는 Debian ® 배포를 나타냅니다. 지원되는 버전 목록은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

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 를 "StorageGRID 어플라이언스 유지보수 지침"참조하십시오.

복구 패키지를 다운로드합니다

복구 패키지 파일을 사용하면 오류가 발생할 경우 StorageGRID 시스템을 복원할 수 있습니다.

시작하기 전에

- 기본 관리자 노드에서 를 사용하여 그리드 관리자에 로그인됩니다."지원되는 웹 브라우저"
- 프로비저닝 암호가 있습니다.
- 있습니다. "특정 액세스 권한"

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 파일을 열고 `.zip` 파일을 포함한 콘텐츠에 액세스할 수 있는지 `Passwords.txt` 확인합니다.

4. 다운로드한 복구 패키지 파일(`.zip`)을 안전한 별도의 두 위치에 복사합니다.

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

노드 또는 사이트를 파기합니다

노드 또는 사이트를 해제합니다

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.

- 를 "그리드 노드 해제" 수행하여 하나 이상의 사이트에 있는 하나 이상의 노드를 제거합니다. 제거하는 노드는 온라인 상태일 수 있으며 StorageGRID 시스템에 연결되어 있을 수도 있고 오프라인일 수도 있고 연결이 끊어질 수도 있습니다.
- 를 "사이트 파기" 수행하여 사이트를 제거합니다. 모든 노드가 StorageGRID에 연결되어 있는 경우 * 연결된 사이트 파기 * 를 수행합니다. 모든 노드가 StorageGRID에서 분리되어 있는 경우 * 연결 해제된 사이트 서비스 해제 * 를 수행합니다. 사이트에 연결된 노드와 연결되지 않은 노드가 혼합되어 있는 경우 모든 오프라인 노드를 다시 온라인 상태로 전환해야 합니다.

> 연결이 끊긴 사이트 해제를 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.

노드 서비스 해제

그리드 노드 해제

노드 서비스 해제 절차를 사용하여 하나 이상의 사이트에서 하나 이상의 그리드 노드를 제거할 수 있습니다. 기본 관리 노드를 해제할 수 없습니다.

노드를 해제해야 하는 경우

다음 중 하나가 참인 경우 노드 해제 절차를 사용하십시오.

- 확장에서 더 큰 스토리지 노드를 추가한 경우 하나 이상의 더 작은 스토리지 노드를 제거하는 동시에 객체를 보존하려고 합니다.

> 이전 어플라이언스를 최신 어플라이언스로 교체하려면 확장 시 새 어플라이언스를 추가한 다음 기존 어플라이언스를 사용 중단하는 대신 고려해 "어플라이언스 노드 클론 생성" 보십시오.

- 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.
- 그리드에는 아카이브 노드가 포함되어 있습니다.

노드를 해제하는 방법

연결된 그리드 노드 또는 연결되지 않은 그리드 노드를 해제할 수 있습니다.

연결된 노드를 해제합니다

일반적으로 그리드 노드가 StorageGRID 시스템에 연결되어 있고 모든 노드가 정상 상태인 경우에만 그리드 노드를 해제해야 합니다(* nodes * 페이지와 * Decommission Nodes * 페이지에 녹색 아이콘이 있음).

자세한 내용은 을 "연결된 그리드 노드 해제"참조하십시오.

연결이 끊어진 노드를 해제합니다

경우에 따라 현재 그리드에 연결되어 있지 않은 그리드 노드(상태가 알 수 없음 또는 사용자 다운)를 해제해야 할 수도 있습니다.

자세한 내용은 을 "연결이 끊긴 그리드 노드의 서비스 해제"참조하십시오.

노드를 서비스 해제하기 전에 고려해야 할 사항

두 절차 중 하나를 수행하기 전에 각 노드 유형에 대한 고려 사항을 검토하십시오.

- "관리자 또는 게이트웨이 노드 서비스 해제를 위한 고려 사항"
- "스토리지 노드 파기 관련 고려 사항"

관리자 또는 게이트웨이 노드 해체 시 고려 사항

관리자 노드 또는 게이트웨이 노드 서비스 해제와 관련된 고려 사항을 검토합니다.

관리자 노드에 대한 고려 사항

- 기본 관리 노드를 해제할 수 없습니다.
- 네트워크 인터페이스 중 하나가 고가용성(HA) 그룹의 일부인 경우 관리자 노드를 해제할 수 없습니다. 먼저 HA 그룹에서 네트워크 인터페이스를 제거해야 합니다. 의 지침을 "HA 그룹 관리"참조하십시오.
- 필요에 따라 관리자 노드를 서비스 해제하는 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.
- 을 사용하는 경우 "그리드 통합"사용 중단하는 노드의 IP 주소가 그리드 페더레이션 연결에 대해 지정되지 않았는지 확인합니다.
- 연결이 끊긴 관리 노드를 서비스 해제할 경우 해당 노드에서 감사 로그가 손실되지만 이러한 로그는 기본 관리 노드에도 존재해야 합니다.

게이트웨이 노드에 대한 고려 사항

- 네트워크 인터페이스 중 하나가 HA(고가용성) 그룹의 일부인 경우 게이트웨이 노드를 해제할 수 없습니다. 먼저 HA 그룹에서 네트워크 인터페이스를 제거해야 합니다. 의 지침을 "HA 그룹 관리"참조하십시오.

- 필요에 따라 게이트웨이 노드를 해제하면서 ILM 정책을 안전하게 변경할 수 있습니다.
- 을 사용하는 경우 "그리드 통합"사용 중단하는 노드의 IP 주소가 그리드 페더레이션 연결에 대해 지정되지 않았는지 확인합니다.
- 연결이 끊어진 상태에서 게이트웨이 노드를 안전하게 해제할 수 있습니다.

스토리지 노드에 대한 고려 사항

스토리지 노드 폐기에 대한 고려 사항

스토리지 노드를 해제하기 전에 노드를 복제할 수 있는지 여부를 고려하십시오. 그런 다음 노드를 해제하기로 결정한 경우 서비스 해제 절차 동안 StorageGRID에서 오브젝트 및 메타데이터를 관리하는 방법을 검토하십시오.

노드를 서비스 해제하지 않고 클론을 생성할 때

이전 어플라이언스 스토리지 노드를 최신 또는 더 큰 어플라이언스로 교체하려면 확장에 새 어플라이언스를 추가한 다음 이전 어플라이언스를 사용하지 않고 어플라이언스 노드의 클론을 생성하는 것이 좋습니다.

어플라이언스 노드 클론 생성을 사용하면 기존 어플라이언스 노드를 동일한 StorageGRID 사이트에서 호환되는 어플라이언스로 쉽게 교체할 수 있습니다. 클론 생성 프로세스는 모든 데이터를 새 어플라이언스로 전송하고 새 어플라이언스를 가동하고 이전 어플라이언스를 설치 전 상태로 둡니다.

다음과 같은 경우에 어플라이언스 노드를 클론 복제할 수 있습니다.

- 수명이 다한 제품을 교체하십시오.
- 향상된 어플라이언스 기술을 활용하려면 기존 노드를 업그레이드하십시오.
- StorageGRID 시스템에서 스토리지 노드 수를 변경하지 않고 그리드 스토리지 용량을 늘립니다.
- RAID 모드 변경과 같은 스토리지 효율성 향상

자세한 내용은 을 "어플라이언스 노드 클론 복제" 참조하십시오.

접속된 스토리지 노드에 대한 고려 사항

접속된 스토리지 노드 해체 시 고려 사항을 검토합니다.

- 단일 서비스 해제 노드 절차에서 10개 이상의 스토리지 노드를 서비스 해제할 수 없습니다.
- 시스템은 항상 및 활성 을 포함한 운영 요구 사항을 충족할 수 있는 충분한 스토리지 노드를 포함해야 "ADC 쿼럼""ILM 정책"합니다. 이러한 제한을 충족하려면 기존 스토리지 노드를 폐기하기 전에 확장 작업에서 새 스토리지 노드를 추가해야 할 수 있습니다.

  소프트웨어 기반 메타데이터 전용 노드가 포함된 그리드에서 스토리지 노드를 해제할 때는 주의하십시오. store_both_objects 및 메타데이터로 구성된 모든 노드를 해제하면 그리드에서 객체를 저장하는 기능이 제거됩니다. 메타데이터 전용 스토리지 노드에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

- 스토리지 노드를 제거하면 대량의 객체 데이터가 네트워크를 통해 전송됩니다. 이러한 전송은 정상적인 시스템 작동에 영향을 주지 않지만 StorageGRID 시스템에서 사용하는 총 네트워크 대역폭에 영향을 미칠 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.
- 스토리지 노드를 제거하는 동안 다른 유지 관리 절차를 수행해야 하는 경우 다른 절차가 완료된 후 다시 시작할 수 "서비스 해제 절차를 일시 중지합니다"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.

- 서비스 해제 작업이 실행 중일 때는 그리드 노드에서 데이터 복구 작업을 실행할 수 없습니다.
- 스토리지 노드를 사용 중지하는 동안에는 ILM 정책을 변경하지 않아야 합니다.
- 데이터를 영구적으로 안전하게 제거하려면 서비스 해제 절차가 완료된 후 스토리지 노드의 드라이브를 지워야 합니다.

연결이 끊어진 스토리지 노드에 대한 고려 사항

연결이 끊어진 스토리지 노드를 해제할 때 고려해야 할 사항을 검토합니다.

- 연결이 끊긴 노드를 온라인 상태로 전환하거나 복구할 수 없다고 확신할 수 없는 경우에는 서비스를 해제하지 마십시오.

> 노드에서 오브젝트 데이터를 복구할 수 있다고 생각되면 이 절차를 수행하지 마십시오. 대신 기술 지원 부서에 문의하여 노드 복구가 가능한지 확인하십시오.

- 연결이 끊긴 스토리지 노드를 서비스 해제하면 StorageGRID은 다른 스토리지 노드의 데이터를 사용하여 연결이 끊어진 노드에 있었던 오브젝트 데이터 및 메타데이터를 재구성합니다.
- 연결이 끊긴 스토리지 노드를 두 개 이상 해제하는 경우 데이터가 손실될 수 있습니다. 오브젝트 복사본, 삭제 코딩 조각 또는 오브젝트 메타데이터가 충분하지 않은 경우 시스템에서 데이터를 재구성하지 못할 수 있습니다. 소프트웨어 기반 메타데이터 전용 노드를 통해 그리드에서 스토리지 노드를 해제할 경우 오브젝트와 메타데이터를 모두 저장하도록 구성된 모든 노드를 서비스 해제하면 그리드에서 모든 오브젝트 스토리지가 제거됩니다. 메타데이터 전용 스토리지 노드에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

> 복구할 수 없는 스토리지 노드가 두 개 이상 연결되어 있는 경우 기술 지원 부서에 문의하여 최상의 조치를 취하십시오.

- 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 "데이터 복구 작업을 확인합니다"참조하십시오.
- 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.

ADC 쿼럼이란 무엇입니까**?**

서비스 해제 후 남아 있는 관리 도메인 컨트롤러(ADC) 서비스가 너무 적은 경우 사이트에서 특정 스토리지 노드를 서비스 해제하지 못할 수 있습니다.

일부 스토리지 노드에 있는 ADC 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. 서비스 해제 중 ADC 쿼럼을 충족하려면 각 사이트에서 최소 3개의 스토리지 노드에 ADC 서비스가 있어야 합니다. 사이트에 ADC 서비스가 포함된 스토리지 노드가 3개 이상 있는 경우 이러한 노드의 대부분은 서비스 해제 후에도 사용 가능한 상태로 유지되어야 합니다. `((0.5 * Storage Nodes with ADC) + 1)`

> 소프트웨어 기반 메타데이터 전용 노드가 포함된 그리드에서 스토리지 노드를 해제할 때는 주의하십시오. store_both_objects 및 메타데이터로 구성된 모든 노드를 해제하면 그리드에서 객체를 저장하는 기능이 제거됩니다. 메타데이터 전용 스토리지 노드에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

예를 들어 사이트에 현재 ADC 서비스가 포함된 6개의 스토리지 노드가 있고 3개의 스토리지 노드를 해제하려는 경우를 가정해 보겠습니다. ADC quorum 요구 사항으로 인해 다음과 같이 2개의 서비스 해제 절차를 완료해야 합니다.

- 첫 번째 서비스 해제 절차에서는 ADC 서비스가 있는 4개의 스토리지 노드를 계속 사용할 수 있도록 해야 합니다 `((0.5 * 6) + 1)`. 즉, 처음에 2개의 스토리지 노드만 서비스 해제할 수 있습니다.
- 두 번째 서비스 해제 절차에서는 ADC 쿼럼에 세 개의 ADC 서비스만 사용 가능하도록 필요하므로 세 번째 스토리지 노드를 제거할 수 `((0.5 * 4) + 1)` 있습니다.

저장소 노드를 서비스 해제해야 하지만 ADC 쿼럼 요구 사항으로 인해 서비스를 수행할 수 없는 경우 에 새 저장소 노드를 "확장"추가하고 ADC 서비스가 있어야 함을 지정합니다. 그런 다음 기존 스토리지 노드를 해제합니다.

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.

각 규칙을 검토하여 StorageGRID 시스템이 스토리지 노드 폐기를 수용할 수 있는 올바른 유형과 올바른 위치에 충분한 용량을 계속 보유할 수 있는지 확인해야 "활성 ILM 정책"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 바와 같이"스토리지 노드 통합", 이전 버전을 사용 중지하기 전에 해야 "새 스토리지 노드를 추가합니다"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.

- 시스템에 활성 ILM 정책을 만족하기에 충분한 스토리지 노드가 항상 포함됩니까?

> 충족되지 않는 ILM 정책은 백로그와 경고를 발생시키고 StorageGRID 시스템 작동을 중단할 수 있습니다.

서비스 해제 프로세스로 인해 제안된 토폴로지가 표에 나열된 영역을 평가하여 ILM 정책을 충족하는지 확인합니다.

평가할 영역	고려할 사항
사용 가능한 용량입니다	스토리지 노드에 현재 저장되어 있는 오브젝트 데이터의 영구 복사본을 포함하여 StorageGRID 시스템에 저장된 모든 오브젝트 데이터를 수용할 수 있는 충분한 스토리지 용량이 있습니까? 사용 중단이 완료된 후 적절한 시간 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 규칙은 콘텐츠가 노후화되면 한 스토리지 유형에서 다른 스토리지 유형으로 콘텐츠를 이동할 수 있습니다. 이 경우 StorageGRID 시스템의 최종 구성에서 적절한 유형의 스토리지를 충분히 사용할 수 있는지 확인해야 합니다.

스토리지 노드 통합

스토리지 노드를 통합하여 스토리지 용량을 늘리면서 사이트 또는 구축의 스토리지 노드 수를 줄일 수 있습니다.

스토리지 노드를 통합할 경우 "StorageGRID 시스템을 확장합니다"더 큰 용량의 새로운 스토리지 노드를 추가한 다음 이전의 더 작은 용량 스토리지 노드를 폐기합니다. 서비스 해제 절차 중에 오브젝트는 이전 스토리지 노드에서 새 스토리지 노드로 마이그레이션됩니다.

> 구형 어플라이언스와 소형 어플라이언스를 새로운 모델 또는 대용량 어플라이언스와 통합하는 경우 일대일 교체를 "어플라이언스 노드 클론 생성" 수행하지 않는 경우 어플라이언스 노드 클론 생성 및 서비스 해제 절차를 고려하십시오.

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.

둘 이상의 스토리지 노드를 제거해야 하는 경우 순차적으로 또는 병렬로 서비스 해제할 수 있습니다.

> 소프트웨어 기반 메타데이터 전용 노드가 포함된 그리드에서 스토리지 노드를 해제할 때는 주의하십시오. store_both_objects 및 메타데이터로 구성된 모든 노드를 해제하면 그리드에서 객체를 저장하는 기능이 제거됩니다. 메타데이터 전용 스토리지 노드에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

- 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 복사본이 "읽기 전용"으로 표시되어 이 기능이 활성화된 그리드에서 삭제를 일시적으로 비활성화하는 상황이 발생할 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.

이 작업에 대해

연결이 끊긴 스토리지 노드의 서비스를 해제해야 하는 경우 서비스 해제 절차가 완료된 후 이러한 단계를 완료하여 데이터 복구 작업이 성공적으로 완료되었는지 확인할 수도 있습니다. 제거된 노드에 있었던 삭제 코딩 조각이 성공적으로 복구되었는지 확인해야 합니다.

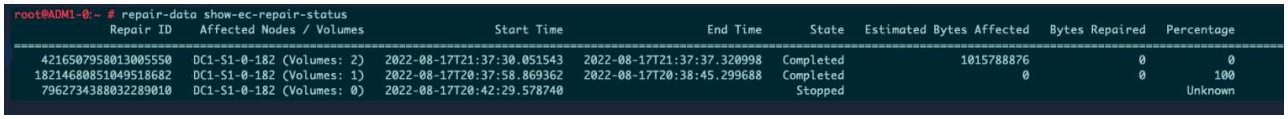
이 단계는 삭제 코딩 오브젝트가 있는 시스템에만 적용됩니다.

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 실행 중인 수리 확인: `repair-data show-ec-repair-status`
   - 데이터 복구 작업을 실행하지 않은 경우 출력은 입니다 `No job found`. 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.



선택적으로 그리드 관리자를 사용하여 진행 중인 복원 프로세스를 모니터링하고 복원 기록을 표시할 수 있습니다. 을 "Grid Manager를 사용하여 개체 데이터를 복원합니다"참조하십시오.

3. 모든 수리의 상태가 인 경우 `Completed` 복구 작업을 다시 시작할 필요가 없습니다.
4. 수리 시/도가 인 경우 `Stopped` 해당 수리를 다시 시작해야 합니다.
   a. 출력에서 실패한 복구에 대한 수리 ID를 얻습니다.
   b. `repair-data start-ec-node-repair`명령을 실행합니다.

      옵션을 사용하여 `--repair-id` 수리 ID를 지정합니다. 예를 들어 복구 ID 949292를 사용하여 복구를 다시 시도하려면 다음 명령을 실행합니다. `repair-data start-ec-node-repair --repair-id 949292`

   c. 모든 수리의 상태가 가 될 때까지 EC 데이터 수리의 상태를 계속 `Completed` 추적합니다.

필요한 자료를 수집합니다

그리드 노드 해제를 수행하기 전에 다음 정보를 얻어야 합니다.

항목	참고
복구 패키지 `.zip` 파일	반드시 보관해야 "최신 복구 패키지를 다운로드합니다" `.zip` (`sgws-recovery-package-*id-revision*.zip`함). 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 암호가 `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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.

> 소프트웨어 기반 메타데이터 전용 노드가 포함된 그리드에서 스토리지 노드를 해제할 때는 주의하십시오. store_both_objects 및 메타데이터로 구성된 모든 노드를 해제하면 그리드에서 객체를 저장하는 기능이 제거됩니다. 메타데이터 전용 스토리지 노드에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

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.

   이 예에서 가능한 서비스 해제 열은 게이트웨이 노드 및 네 개의 스토리지 노드 중 하나를 해제할 수 있음을 나타냅니다.

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-	✓	No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC1-ARC1	Data Center 1	Archive Node	-	✓	No, you can't decommission an Archive Node unless the node is disconnected.
DC1-G1	Data Center 1	API Gateway Node	-	✓	✓
DC1-S1	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S2	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S3	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S4	Data Center 1	Storage Node	No	✓	✓

3. 서비스 해제하려는 각 노드에 대해 * 서비스 해제 가능 * 열을 검토합니다.

   그리드 노드를 해체할 수 있는 경우 이 열에는 녹색 확인 표시가 있고 왼쪽 열에는 확인란이 포함됩니다. 노드를 해체할 수 없는 경우 이 열에 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, _node type_disposing은 지원되지 않습니다.	기본 관리 노드를 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 경우 연결된 그리드 노드를 해제할 수 없습니다. 상태 * 열에는 연결이 끊긴 그리드 노드에 대한 다음 아이콘 중 하나가 포함됩니다. • (회색): 사용자 다운 • (파란색): 알 수 없음	연결이 끊긴 모든 노드를 다시 온라인 상태로 전환하거나 연결된 노드를 제거하려면 먼저 연결이 끊긴 노드를 모두 제거해야 "연결이 끊어진 모든 노드를 해제합니다"합니다. 참고: 그리드에 여러 개의 연결이 끊긴 노드가 포함되어 있는 경우, 소프트웨어에서 모든 노드를 동시에 해제해야 하므로 예기치 않은 결과가 발생할 가능성이 높아집니다.
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:_그룹 이름 _. 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. 을 "고가용성 그룹을 구성합니다"참조하십시오.
아니요. site_x_에는 ADC 서비스를 포함하는 최소 _n_개의 스토리지 노드가 필요합니다.	• 스토리지 노드 전용. * 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. 에 대한 정보를 "ADC 쿼럼 "참조하십시오.

사용 중지 가능한 이유	설명	해결 단계
아니요. 하나 이상의 삭제 코딩 프로필에 최소한 _n_스토리지 노드가 필요합니다. ILM 규칙에서 프로파일을 사용하지 않는 경우 비활성화할 수 있습니다.	• 스토리지 노드 전용. * 기존 삭제 코딩 프로필에 충분한 노드가 남아 있지 않으면 스토리지 노드를 해제할 수 없습니다. 예를 들어, 4+2 삭제 코딩에 대한 삭제 코딩 프로필이 있는 경우 스토리지 노드 6개를 유지해야 합니다.	영향을 받는 각 삭제 코딩 프로필에 대해 프로필이 사용되는 방식에 따라 다음 단계 중 하나를 수행합니다. • * 활성 ILM 정책에 사용됨 *: 확장을 수행합니다. 삭제 코딩을 계속할 수 있도록 새 스토리지 노드를 추가합니다. 의 지침을 "그리드 확장"참조하십시오. • * ILM 규칙에는 사용되지만 활성 ILM 정책에는 사용되지 않음 *: 규칙을 편집하거나 삭제한 다음 삭제 코딩 프로필을 비활성화합니다. • *ILM 규칙에 사용되지 않음 *: 삭제 코딩 프로파일을 비활성화합니다. 참고: 삭제 코딩 프로파일을 비활성화하려고 시도해도 개체 데이터가 여전히 프로필과 연결되어 있으면 오류 메시지가 나타납니다. 비활성화 프로세스를 다시 시도하기 전에 몇 주를 기다려야 할 수 있습니다. 에 대해 자세히 "삭제 코딩 프로필 비활성화"알아보십시오.
아니요. 노드의 연결이 끊어지지 않으면 아카이브 노드를 해제할 수 없습니다.	보관 노드가 여전히 연결되어 있으면 제거할 수 없습니다.	• 참고 *: 아카이브 노드에 대한 지원이 제거되었습니다. 아카이브 노드를 해제해야 하는 경우 를 참조하십시오 "그리드 노드 폐기(StorageGRID 11.8 문서 사이트)"

연결이 끊긴 그리드 노드의 서비스 해제

현재 그리드에 연결되어 있지 않은 노드(상태가 알 수 없거나 관리상 중단된 노드)를 해제해야 할 수 있습니다.

시작하기 전에

- 서비스 해제 시 고려 사항 및 서비스 해제 시 고려 "관리자 및 게이트웨이 노드""스토리지 노드"사항을 이해합니다.
- 모든 필수 항목을 확보했습니다.
- 활성화된 데이터 복구 작업이 없도록 했습니다. 을 "데이터 복구 작업을 확인합니다"참조하십시오.
- 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 있습니다.

이 작업에 대해

Health* 열에서 파란색 Unknown 아이콘 또는 회색 Administratively Down 아이콘을 찾아 연결이 끊어진 노드를 식별할 수 있습니다.

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 스토리지 노드를 한 번에 두 개 이상 해제하는 경우 데이터가 손실될 수 있습니다. 을 "연결이 끊어진 스토리지 노드에 대한 고려 사항"참조하십시오.

  소프트웨어 기반 메타데이터 전용 노드가 포함된 그리드에서 스토리지 노드를 해제할 때는 주의하십시오. store_both_objects 및 메타데이터로 구성된 모든 노드를 해제하면 그리드에서 객체를 저장하는 기능이 제거됩니다. 메타데이터 전용 스토리지 노드에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

- 연결이 끊긴 노드를 제거할 수 없는 경우(예: ADC 쿼럼에 필요한 스토리지 노드) 연결이 끊긴 다른 노드는 제거할 수 없습니다.

단계

1. 아카이브 노드(연결 해제되어야 함)를 해제하지 않는 한 연결이 끊어진 그리드 노드를 다시 온라인 상태로 전환하거나 복구해 보십시오.

   자세한 내용은 을 "그리드 노드 복구 절차" 참조하십시오.

2. 연결이 끊긴 그리드 노드를 복구할 수 없고 연결이 끊긴 동안 노드 서비스를 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 주의하십시오. 복구할 수 없는 스토리지 노드가 두 개 이상 연결되어 있는 경우 기술 지원 부서에 문의하여 최상의 조치를 취하십시오.

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 "복구 패키지 다운로드 중"참조하십시오.

   > 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

- 복제된 복구의 예상 완료율을 얻으려면 repair-data 명령에 옵션을 추가합니다 `show-replicated-repair-status`.

```
repair-data show-replicated-repair-status
```

- 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.

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.
   - 다음 명령을 사용하여 특정 작업의 상태를 `repair-data` 확인합니다.

```
repair-data show-ec-repair-status --repair-id repair ID
```

   - 이 명령을 사용하여 모든 수리를 나열합니다.

```
repair-data show-ec-repair-status
```

출력에는 이전 및 현재 실행 중인 모든 수리에 대한 정보가 `repair ID` 표시됩니다.

2. 출력에 복구 작업이 실패했다고 표시되는 경우 옵션을 사용하여 `--repair-id` 복구를 재시도합니다.

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 노드 복구를 재시도합니다.

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 볼륨 복구를 다시 시도합니다.

   ```
   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. 자세한 내용은 을 "유지보수 모드에서 노드 암호화를 모니터링합니다"참조하십시오.

연결된 그리드 노드 해제

그리드에 연결된 노드를 사용 중지하고 영구적으로 제거할 수 있습니다.

시작하기 전에

- 서비스 해제 시 고려 사항 및 서비스 해제 시 고려 "관리자 및 게이트웨이 노드""스토리지 노드"사항을 이해합니다.
- 필요한 모든 자료를 수집했습니다.
- 활성화된 데이터 복구 작업이 없도록 했습니다.
- 스토리지 노드 복구가 그리드의 어느 곳에서든 진행되고 있지 않음을 확인했습니다. 있는 경우 복구 과정에서 Cassandra 재구축이 완료될 때까지 기다립니다. 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.
- 프로비저닝 암호가 있습니다.
- 그리드 노드가 연결되어 있습니다.
- 서비스 해제하려는 노드에 대한 * 서비스 해제 가능 * 열에는 녹색 확인 표시가 포함됩니다.

> 하나 이상의 볼륨이 오프라인 상태(마운트 해제)이거나 온라인 상태(마운트 해제)이지만 오류 상태인 경우 서비스 해제가 시작되지 않습니다.

서비스 해제가 진행되는 동안 하나 이상의 볼륨이 오프라인 상태가 되면 해당 볼륨이 다시 온라인 상태가 된 후 서비스 해제 프로세스가 완료됩니다.

- 모든 그리드 노드의 상태는 정상(녹색) 상태입니다. 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 "데이터 복구 작업을 확인합니다"참조하십시오.

이 절차에서 지시될 때까지 그리드 노드의 가상 머신 또는 기타 리소스를 제거하지 마십시오.

소프트웨어 기반 메타데이터 전용 노드가 포함된 그리드에서 스토리지 노드를 해제할 때는 주의하십시오. store_both_objects 및 메타데이터로 구성된 모든 노드를 해제하면 그리드에서 객체를 저장하는 기능이 제거됩니다. 메타데이터 전용 스토리지 노드에 대한 자세한 내용은 을 "스토리지 노드 유형"참조하십시오.

이 작업에 대해

노드를 폐기하면 서비스가 비활성화되고 노드가 자동으로 종료됩니다.

단계

1. 서비스 해제 노드 페이지에서 서비스 해제할 각 그리드 노드에 대한 확인란을 선택합니다.
2. 프로비저닝 암호를 입력합니다.

   서비스 해제 시작 * 버튼이 활성화됩니다.

3. Start Decommission * 을 선택합니다.
4. 확인 대화 상자에서 노드 목록을 검토하고 * OK * 를 선택합니다.

   노드 서비스 해제 절차가 시작되고 각 노드에 대한 진행률이 표시됩니다.

   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 배너에서 복구 패키지 링크를 선택하거나 * 유지 관리 * > * 시스템 * > * 복구

패키지 * 를 선택하여 복구 패키지 페이지에 액세스합니다. 그런 다음 `.zip` 파일을 다운로드합니다.

을 "복구 패키지 다운로드 중"참조하십시오.

> 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.

작업을 마친 후

노드 사용 중단 절차를 완료한 후 다음 단계를 완료합니다.

1. 플랫폼에 맞는 적절한 단계를 따릅니다. 예를 들면 다음과 같습니다.
   - Linux *: 설치 중에 생성한 노드 구성 파일을 삭제하고 볼륨을 분리할 수 있습니다. "Red Hat Enterprise Linux에 StorageGRID를 설치합니다"및 을 "Ubuntu 또는 Debian에 StorageGRID를 설치합니다 "참조하십시오.
   - * 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.
2. 해체된 그리드 노드의 드라이브가 깨끗하게 지워졌는지 확인합니다. 상용 데이터 삭제 도구 또는 서비스를 사용하여 드라이브에서 데이터를 영구적으로 안전하게 제거합니다.
3. 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. 자세한 내용은 을 "유지보수 모드에서 노드 암호화를 모니터링합니다"참조하십시오.

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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.

단계

1. 유지 관리 * > * 작업 * > * 서비스 해제 * 를 선택합니다.

서비스 해제 페이지가 나타납니다.

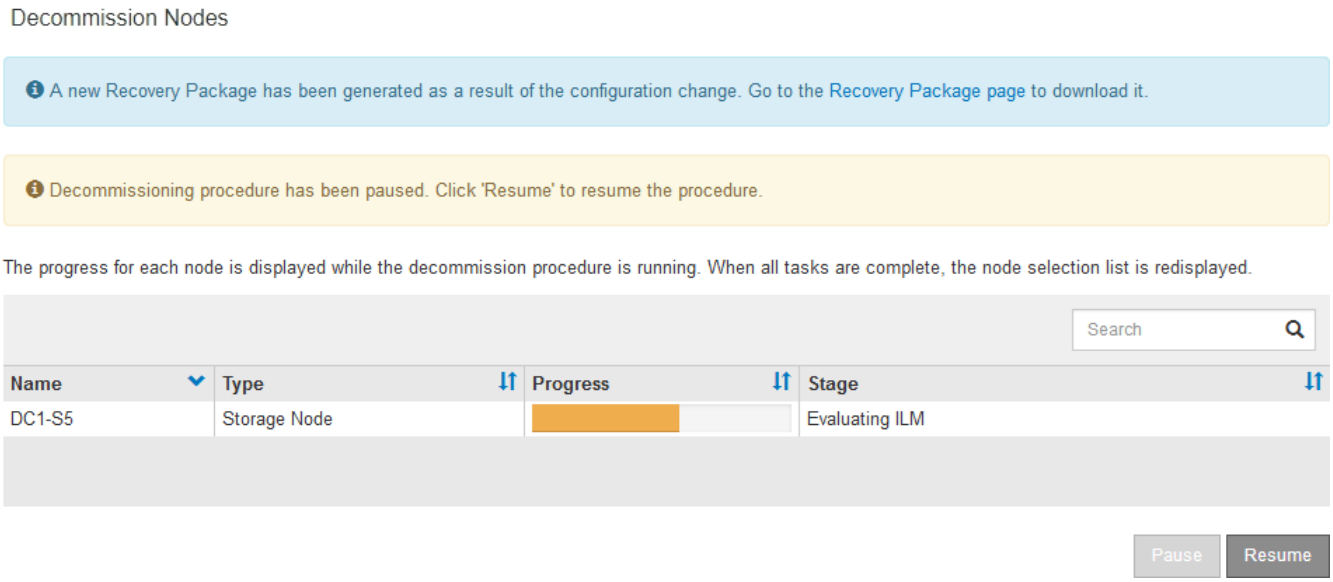
2. 서비스 해제 노드 * 를 선택합니다.

   서비스 해제 노드 페이지가 나타납니다. 서비스 해제 절차가 다음 단계 중 하나에 도달하면 * Pause * (일시 중지 *) 버튼이 활성화됩니다.

   - ILM 평가 중
   - 삭제 해제 - 코드화된 데이터

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.

사이트 파기

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.
- 사이트를 참조하는 스토리지 풀이나 삭제 코딩 프로필을 더 이상 사용할 수 없습니다. StorageGRID에서 사이트를 압축 해제하면 이러한 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 노드()와 연결되지 않은 노드(또는)가 혼합되어 있는 경우 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.
- HA(고가용성) 그룹에 속한 인터페이스가 있는 노드는 사이트 서비스를 해제할 수 없습니다. 노드의 인터페이스를 제거하거나 전체 HA 그룹을 제거하려면 HA 그룹을 편집해야 합니다.
- 연결된() 노드와 연결되지 않은(또는) 노드가 혼합되어 있는 경우 사이트를 해제할 수 없습니다.
- 다른 사이트의 노드 연결이 끊긴 경우(또는) 사이트를 서비스 해제할 수 없습니다.
- EC 노드 복구 작업이 진행 중인 경우에는 사이트 서비스 해제 절차를 시작할 수 없습니다. 삭제 코딩 데이터의 복구를 추적하려면 을 참조하십시오."데이터 복구 작업을 확인합니다"
- 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 사이트 사용 중단 중에 다른 유지 보수 절차를 "스토리지 노드를 제거하는 동안 절차를 일시 중지합니다"수행해야 하는 경우 다음을 수행할 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. 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.

- 이 사이트는 ILM 정책에서 참조되지 않습니다. 정책이 있는 경우, 정책을 편집하거나 새로운 ILM 규칙을 사용하여 정책을 생성하고 활성화해야 합니다.
- ILM 규칙은 정책에 사용되지 않더라도 사이트를 참조하지 않습니다. 사이트를 참조하는 모든 규칙을 삭제하거나 편집해야 합니다.

StorageGRID에서 사이트를 압축 해제하면 사이트를 참조하는 사용하지 않는 삭제 코딩 프로필이 자동으로 비활성화되고 사이트를 참조하는 미사용 스토리지 풀이 자동으로 삭제됩니다. 모든 스토리지 노드 스토리지 풀(StorageGRID 11.6 이하)이 있는 경우 모든 사이트를 사용하므로 이 스토리지 풀은 제거됩니다.

사이트를 제거하기 전에 새 ILM 규칙을 생성하고 새 ILM 정책을 활성화해야 할 수 있습니다. 이 지침에서는 ILM의 작동 방식을 잘 이해하고 있으며 스토리지 풀 생성, 삭제 코딩 프로필, ILM 규칙 및 ILM 정책을 시뮬레이션하고 활성화하는 데 익숙하다고 가정합니다. 을 "ILM을 사용하여 개체를 관리합니다"참조하십시오.

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 사이트에서 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 사용할 수 있도록 하려면 이 절차를 수행하기 전에 스토리지 볼륨 또는 스토리지 노드를 기존 사이트에 추가하거나 새 사이트를 추가해야 할 수 "그리드를 확장합니다"있습니다.

- 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 노드의 연결 상태는 * Connected * ()여야 하지만 노드에 활성 경고가 있을 수 있습니다.

> 하나 이상의 노드의 연결이 끊어진 경우 사이트 서비스 해제 마법사의 1-4단계를 완료할 수 있습니다. 그러나 마법사의 5단계를 완료할 수 없습니다. 그러면 모든 노드가 연결되어 있지 않으면 서비스 해제 프로세스가 시작됩니다.

- 제거하려는 사이트에 로드 밸런싱에 사용되는 게이트웨이 노드 또는 관리자 노드가 포함된 경우 다른 사이트에 해당하는 새 노드를 추가해야 할 수 "그리드를 확장합니다"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. 하지만 모든 HA 그룹에서 이러한 노드를 제거할 때까지 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 모든 객체 데이터를 수용할 수 있도록 나머지 사이트에 충분한 공간을 제공해야 합니다. 경우에 따라 "그리드를 확장합니다"스토리지 노드, 스토리지 볼륨 또는 새 사이트를 추가하여 연결된 사이트 폐기를 완료할 수 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. 을 "기술 지원 부서에서 사이트를 복구하는 방법 "참조하십시오.

- 사이트의 모든 노드에는 다음 중 하나의 연결 상태가 있어야 합니다.
  - 알 수 없음( ): 알 수 없는 이유로 노드 연결이 끊기거나 노드의 서비스가 예기치 않게 다운됩니다. 예를 들어, 노드의 서비스가 중지되거나 전원 장애 또는 예기치 않은 정전으로 인해 노드의 네트워크 연결이 끊겼을 수 있습니다.
  - **Administratively Down**( ): 노드가 예상된 이유로 그리드에 연결되지 않았습니다. 예를 들어, 노드의 노드 또는 서비스가 정상적으로 종료되었습니다.
- 다른 모든 사이트의 모든 노드는 연결 상태 * Connected *()여야 하지만 이러한 다른 노드는 활성 알림을 가질 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 것을 이해해야 합니다.

사이트를 제거할 때의 일관성 고려 사항

S3 버킷의 일관성은 오브젝트 수집이 성공적임을 클라이언트에 알리기 전에 StorageGRID가 오브젝트 메타데이터를 모든 노드 및 사이트에 완전히 복제하는지 여부를 결정합니다. 정합성 보장은 서로 다른 스토리지 노드 및 사이트에서 객체의 가용성과 객체 일관성 간의 균형을 제공합니다.

StorageGRID에서 사이트를 제거할 때는 제거할 사이트에 데이터가 기록되지 않도록 해야 합니다. 따라서 각 버킷 또는 컨테이너의 일관성을 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.

필요한 자료를 수집합니다

사이트를 해체하기 전에 다음 자료를 확보해야 합니다.

항목	참고
복구 패키지 `.zip` 파일	최신 복구 패키지 파일을 다운로드해야 `.zip`(`sgws-recovery-package-id-revision.zip` 합니다.) 장애가 발생할 경우 복구 패키지 파일을 사용하여 시스템을 복원할 수 있습니다. "복구 패키지를 다운로드합니다"
`Passwords.txt` 파일	이 파일에는 명령줄에서 그리드 노드에 액세스하는 데 필요한 암호가 들어 있으며 복구 패키지에 포함되어 있습니다.

항목	참고
프로비저닝 암호	StorageGRID 시스템을 처음 설치할 때 암호가 생성되고 문서화됩니다. 프로비저닝 암호가 `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"

1단계**:** 사이트를 선택합니다

사이트를 해제할 수 있는지 확인하려면 서비스 해제 사이트 마법사에 액세스하여 시작합니다.

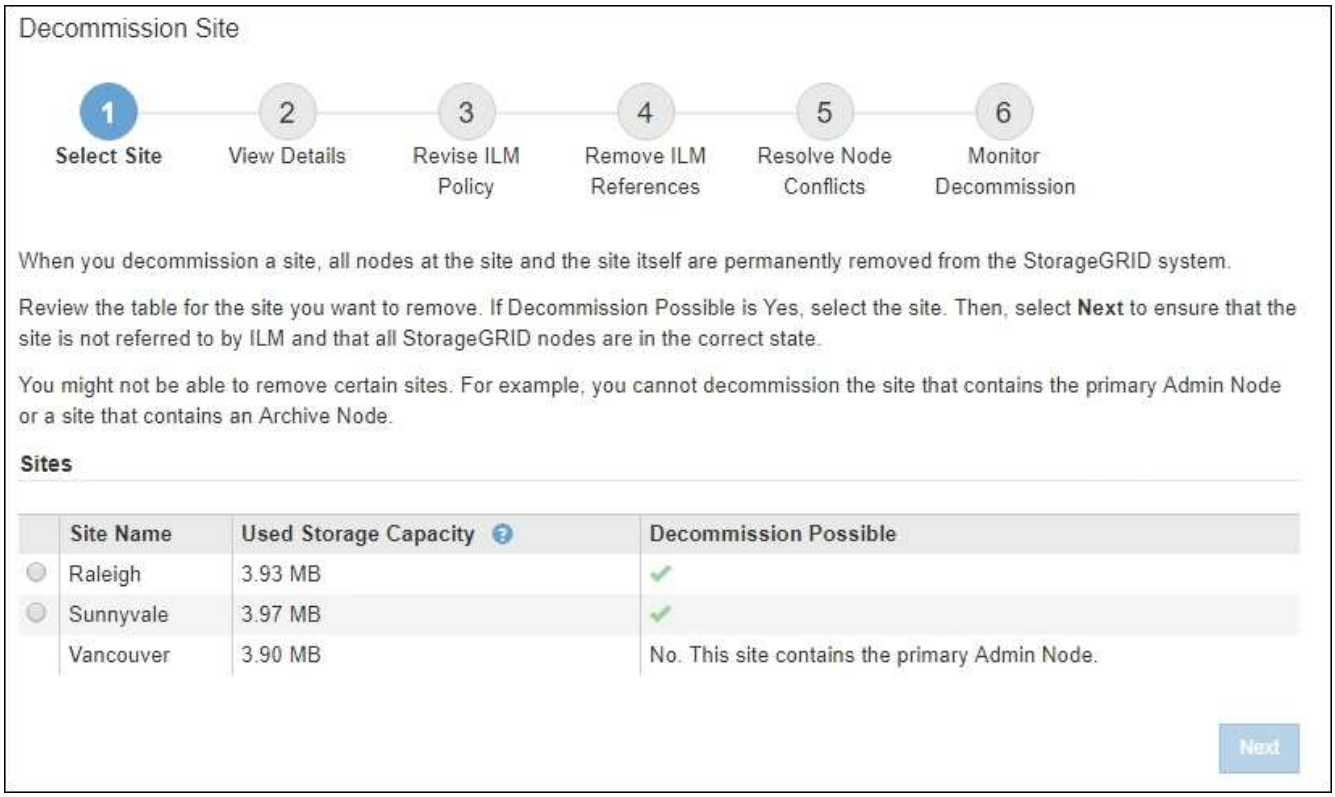
시작하기 전에

- 필요한 모든 자료를 확보했습니다.
- 사이트 제거 시 고려 사항을 검토했습니다.
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 권한 또는 유지 관리 및 ILM 권한"있습니다.

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 관리자 노드가 포함되어 있습니다.	기본 관리자 노드가 포함된 사이트의 서비스 해제는 불가능합니다.	없음. 이 절차를 수행할 수 없습니다.

사용 중지 가능한 이유	설명	다음 단계
아니요. 이 사이트에는 하나 이상의 보관 노드가 있습니다.	아카이브 노드가 포함된 사이트는 서비스 해제할 수 없습니다.	없음. 이 절차를 수행할 수 없습니다.
아니요. 이 사이트의 모든 노드 연결이 끊겼습니다. NetApp 어카운트 담당자에게 문의하십시오.	사이트의 모든 노드가 연결되어 있지 않으면 연결된 사이트 서비스 해제를 수행할 수 없습니다( ).	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. Raleigh 및 Sunnyvale 사이트의 녹색 확인 표시()는 해당 사이트를 서비스 해제할 수 있음을 나타냅니다. 그러나 기본 관리 노드가 포함되어 있으므로 밴쿠버 사이트를 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.

시작하기 전에

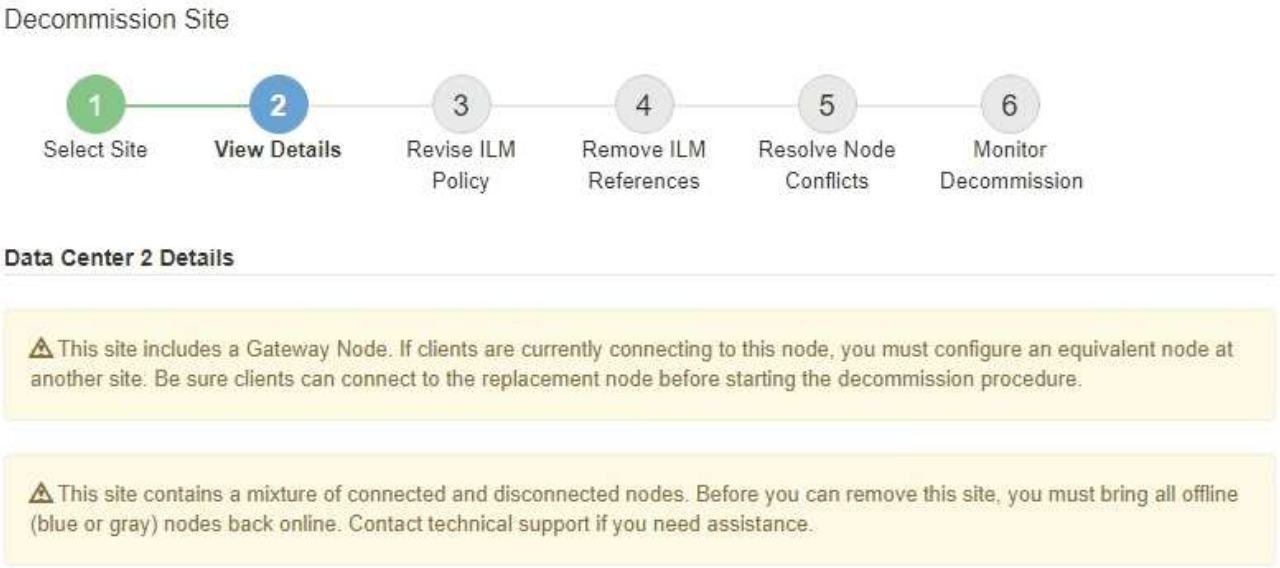
사이트를 해제하기 전에 사이트에 있는 개체 데이터의 양을 검토해야 합니다.

- 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. 을 "사이트 손실 방지"참조하십시오.

단계

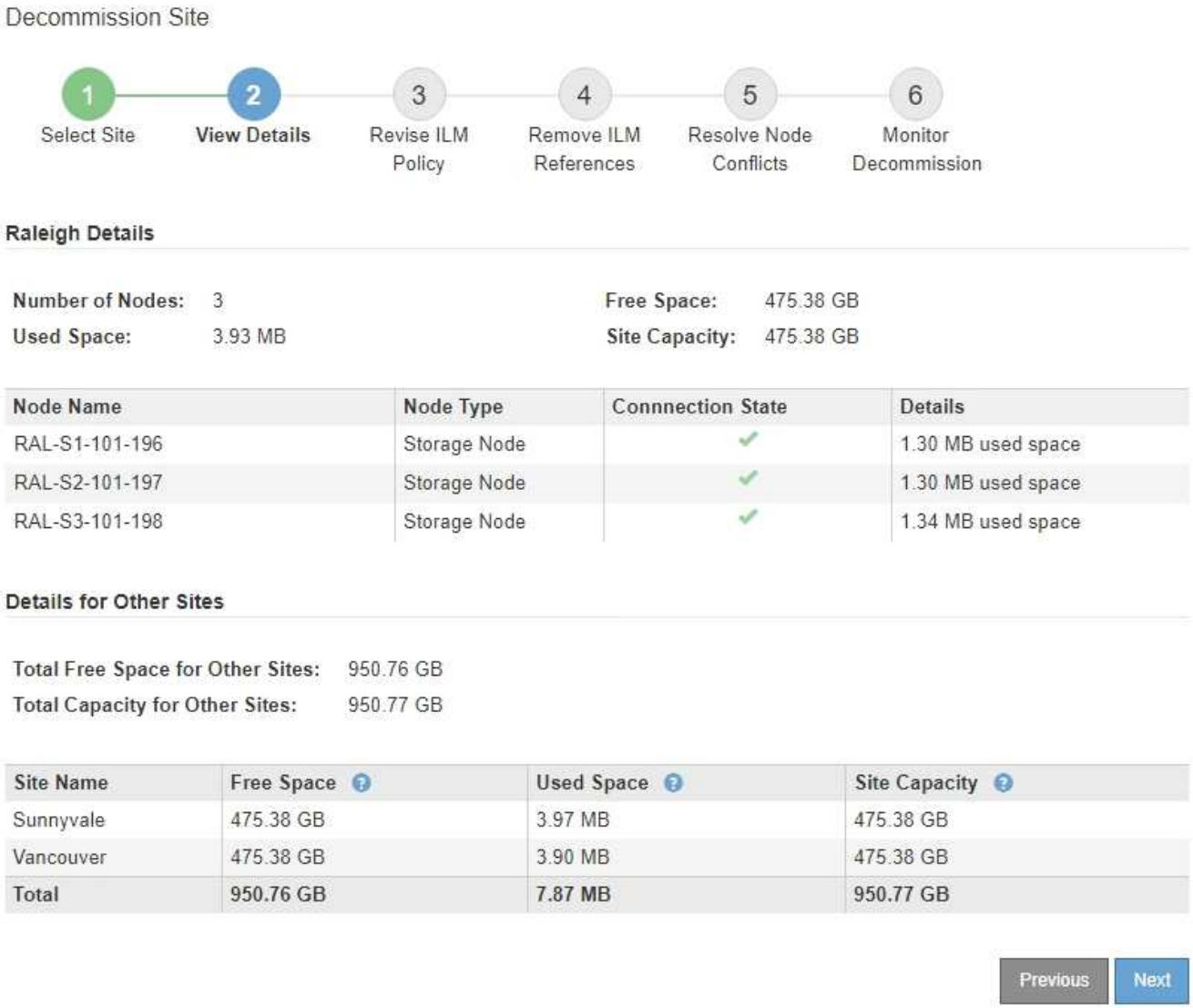
1. 2단계(세부 정보 보기)에서 제거하려는 사이트와 관련된 경고를 검토합니다.



   다음과 같은 경우 경고가 나타납니다.

   - 이 사이트에는 게이트웨이 노드가 포함되어 있습니다. S3 클라이언트가 현재 이 노드에 접속하는 경우 다른 사이트에서 해당 노드를 구성해야 합니다. 서비스 해제 절차를 계속하기 전에 클라이언트가 교체 노드에 연결할 수 있는지 확인하십시오.
   - 사이트에는 연결된 노드()와 분리된 노드(또는)가 혼합되어 있습니다. 이 사이트를 제거하려면 먼저 오프라인 노드를 모두 다시 온라인 상태로 전환해야 합니다.

2. 제거하려는 사이트에 대한 세부 정보를 검토합니다.



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)
  - (사용자 중단)
  - (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 서비스 해제할 수 없습니다. 서비스 해제를 시작하기 전에 HA 그룹을 편집하여 사이트의 모든 노드를 제거하거나, 이 사이트의 노드만 포함하는 HA 그룹을 제거하십시오. 자세한 내용은 을 "고가용성(HA) 그룹 관리"참조하십시오.

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.

3단계**: ILM** 정책을 수정합니다

사이트 해제 마법사의 3단계(ILM 정책 수정)에서 사이트가 ILM 정책에 의해 참조되는지 확인할 수 있습니다.

시작하기 전에

방법을 잘 알고 "ILM을 사용하여 오브젝트를 관리합니다"있습니다. 스토리지 풀 및 ILM 규칙을 생성하고 ILM 정책을 시뮬레이션하고 활성화하는 데 익숙합니다.

이 작업에 대해

StorageGRID는 정책(활성 또는 비활성)에서 ILM 규칙이 해당 사이트를 참조하는 경우 사이트를 해제할 수 없습니다.

ILM 정책이 폐기하려는 사이트를 참조하는 경우 해당 정책을 제거하거나 편집하여 다음 요구사항을 충족해야 합니다.

- 모든 오브젝트 데이터를 완벽하게 보호
- 사용 중단하는 사이트를 참조하지 마십시오.
- 사이트를 참조하는 스토리지 풀을 사용하거나 모든 사이트 옵션을 사용하지 마십시오.
- 사이트를 참조하는 삭제 코딩 프로필을 사용하지 마십시오.

- StorageGRID 11.6 이전 버전의 설치에서는 복사본 2개 만들기 규칙을 사용하지 마십시오.

> 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 서비스 해제 _ 를 수행하는 경우 StorageGRID에서 제거할 사이트에서 현재 개체 데이터를 관리하는 방법을 고려해야 합니다. 데이터 보호 요구사항에 따라 새로운 규칙을 통해 기존 오브젝트 데이터를 다른 사이트로 이동하거나 더 이상 필요하지 않은 추가 오브젝트 복사본을 삭제할 수 있습니다.

새 정책을 설계하는 데 도움이 필요한 경우 기술 지원 부서에 문의하십시오.

단계

1. 3단계(ILM 정책 수정)에서 ILM 정책이 서비스 해제하도록 선택한 사이트를 참조하는지 확인합니다.
2. 정책이 나열되지 않으면 * Next * 를 선택하여 로 이동합니다"4단계: ILM 참조 제거".
3. 하나 이상의_ACTIVE_ILM 정책이 나열되면 각 기존 정책을 클론하거나 사용 중지되는 사이트를 참조하지 않는 새 정책을 생성합니다.

   a. Policy Name 열에서 정책 링크를 선택합니다.

      정책에 대한 ILM 정책 세부 정보 페이지가 새 브라우저 탭에 나타납니다. 서비스 해제 사이트 페이지는 기타 탭에 계속 열려 있습니다.

   b. 필요에 따라 다음 지침과 지침을 따르십시오.

      - ILM 규칙 작업:
        - "하나 이상의 스토리지 풀을 생성합니다" 사이트를 참조하지 않습니다.
        - "규칙을 편집하거나 바꿉니다" 사이트를 참조하십시오.

          > 2개 복사본 만들기 * 규칙을 선택하지 마십시오. 이 규칙은 허용되지 않는 * 모든 스토리지 노드 * 스토리지 풀을 사용하기 때문입니다.

      - ILM 정책 작업:
        - "기존 ILM 정책을 복제합니다""새 ILM 정책을 생성합니다" 또는.
        - 기본 규칙 및 기타 규칙이 사이트를 참조하지 않도록 합니다.

          > ILM 규칙이 올바른 순서로 되어 있는지 확인해야 합니다. 정책이 활성화되면 위에서 시작하여 나열된 순서대로 새 개체와 기존 개체가 평가됩니다.

   c. 테스트 개체를 수집하고 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.

d. 새 정책을 활성화하고 이전 정책이 비활성화되었는지 확인합니다.

여러 정책을 활성화하려면"단계에 따라 ILM 정책 태그를 생성합니다",

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).

4. 각_inactive_policy에 대해 이전 단계에서 설명한 대로 먼저 각 정책에 대한 링크를 선택하여 해당 링크를 편집하거나 제거합니다.
   - "정책을 편집합니다" 따라서 사이트를 서비스 중단하는 것을 의미하지 않습니다.
   - "정책을 제거합니다"..
5. ILM 규칙 및 정책을 변경한 후에는 3단계(ILM 정책 수정)에 나열된 정책이 더 이상 없어야 합니다. 다음 * 을 선택합니다.

   4단계(ILM 참조 제거)가 나타납니다.

4단계**: ILM** 참조 제거

사이트 해제 마법사의 4단계(ILM 참조 제거)에서 해당 규칙을 ILM 정책에 사용하지 않는 경우에도 사이트를 참조하는 사용하지 않는 ILM 규칙을 삭제하거나 편집해야 합니다.

단계

1. 사용하지 않는 ILM 규칙이 사이트를 참조하는지 확인합니다.

   ILM 규칙이 나열되더라도 해당 규칙은 사이트를 참조하지만 정책에서 사용되지 않습니다.

   StorageGRID에서 사이트를 압축 해제하면 사이트를 참조하는 사용하지 않는 삭제 코딩 프로필이 자동으로 비활성화되고 사이트를 참조하는 미사용 스토리지 풀이 자동으로 삭제됩니다. 모든 스토리지 노드 스토리지 풀(StorageGRID 11.6 이하)은 모든 사이트 사이트를 사용하므로 제거됩니다.

2. 사용하지 않는 각 규칙 편집 또는 삭제:
   - 규칙을 편집하려면 ILM 규칙 페이지로 이동하여 사이트를 참조하는 삭제 코딩 프로필 또는 스토리지 풀을 사용하는 모든 배치를 업데이트합니다. 그런 다음 * 4단계(ILM 참조 제거) * 로 돌아갑니다.
   - 규칙을 삭제하려면 휴지통 아이콘을 선택하고 * 확인 * 을 선택합니다.

     사이트를 해제하려면 먼저 * 복사본 2개 만들기 * 규칙을 삭제해야 합니다.

3. 사용하지 않는 ILM 규칙이 사이트를 참조하지 않고 * 다음 * 버튼이 활성화되어 있는지 확인합니다.
4. 다음 * 을 선택합니다.

> 사이트를 제거하면 사이트를 참조하는 나머지 스토리지 풀 및 삭제 코딩 프로필이 무효화됩니다. StorageGRID에서 사이트를 압축 해제하면 사이트를 참조하는 사용하지 않는 삭제 코딩 프로필이 자동으로 비활성화되고 사이트를 참조하는 미사용 스토리지 풀이 자동으로 삭제됩니다. 모든 스토리지 노드 스토리지 풀(StorageGRID 11.6 이하)은 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.

시작하기 전에

다음과 같이 StorageGRID 시스템의 모든 노드가 올바른 상태인지 확인해야 합니다.

- StorageGRID 시스템의 모든 노드가 연결되어 있어야 합니다().

> 연결이 끊긴 사이트 서비스 해제를 수행하는 경우 제거하려는 사이트의 모든 노드의 연결을 끊어야 하며 다른 모든 사이트의 모든 노드를 연결해야 합니다.

> 하나 이상의 볼륨이 오프라인 상태(마운트 해제)이거나 온라인 상태(마운트 해제)이지만 오류 상태인 경우 서비스 해제가 시작되지 않습니다.

> 서비스 해제가 진행되는 동안 하나 이상의 볼륨이 오프라인 상태가 되면 해당 볼륨이 다시 온라인 상태가 된 후 서비스 해제 프로세스가 완료됩니다.

- 제거하려는 사이트에 HA(고가용성) 그룹에 속한 인터페이스가 있을 수 없습니다.

이 작업에 대해

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.

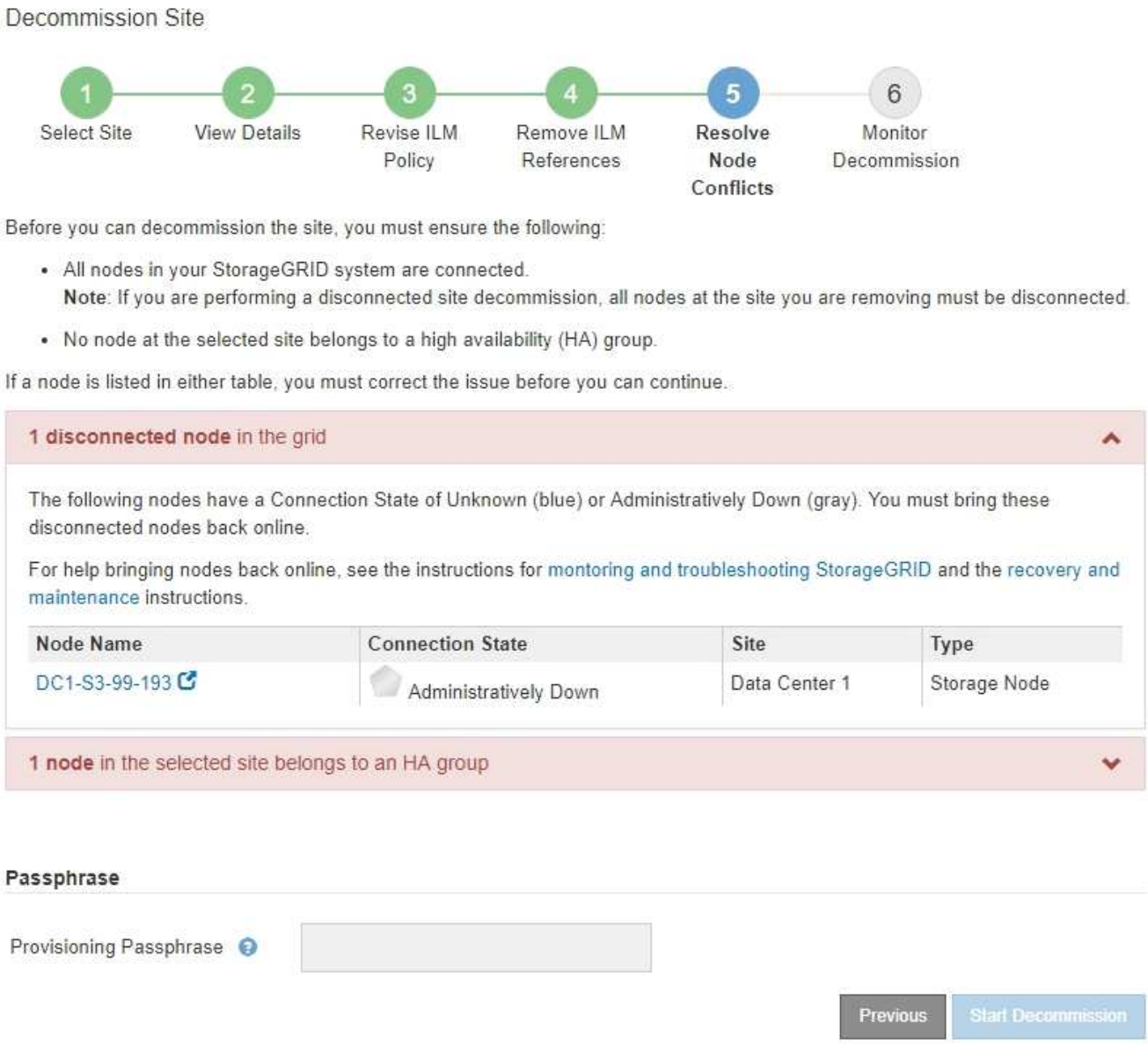
◦ 확장 또는 업그레이드와 같은 다른 유지보수 절차는 수행할 수 없습니다.

> 연결된 사이트의 서비스 해제 중에 다른 유지보수 절차를 수행해야 하는 경우 스토리지 노드가 제거되는 동안 절차를 일시 중지할 수 있습니다. Pause * 버튼은 "Disclosure Replicated and Erasure-Coded Data(복제 및 삭제 코딩 데이터 해제)" 단계에서 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 시스템의 노드가 연결 상태를 알 수 없음( ) 또는 사용자 다운()인지 확인합니다.

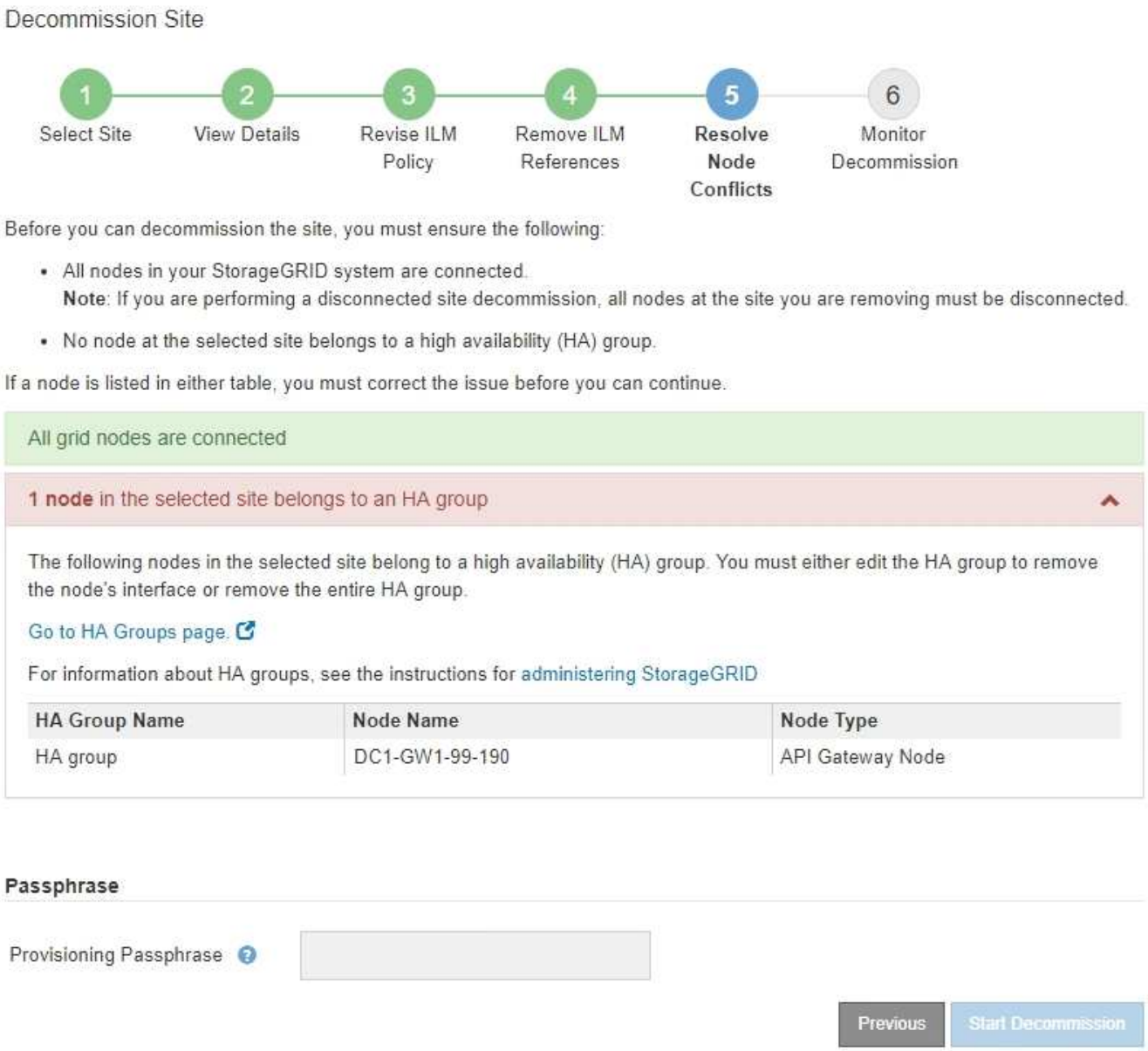


2. 노드의 연결이 끊어진 경우 다시 온라인 상태로 전환합니다.

   를 "노드 절차"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.



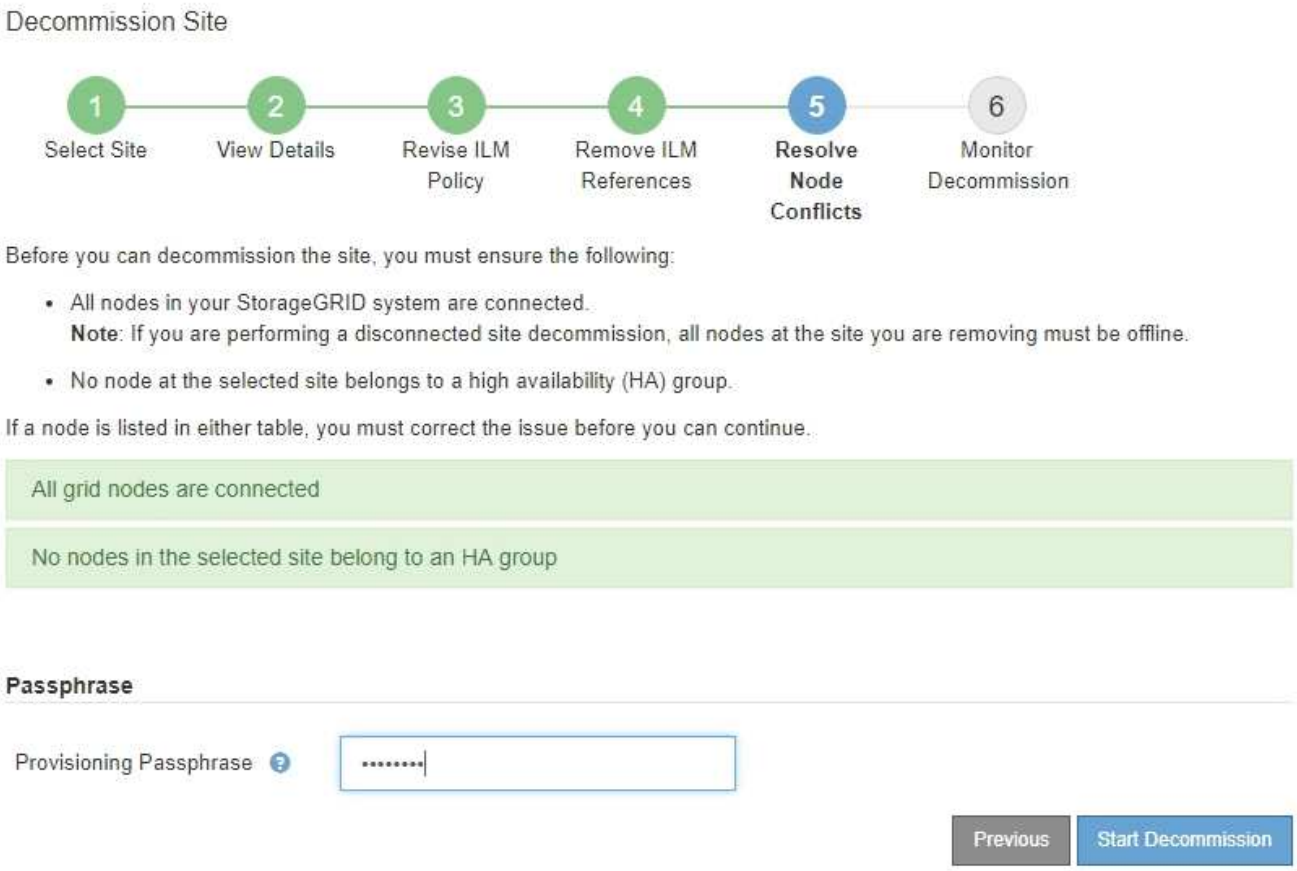
4. 노드가 나열된 경우 다음 중 하나를 수행합니다.

   - 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.

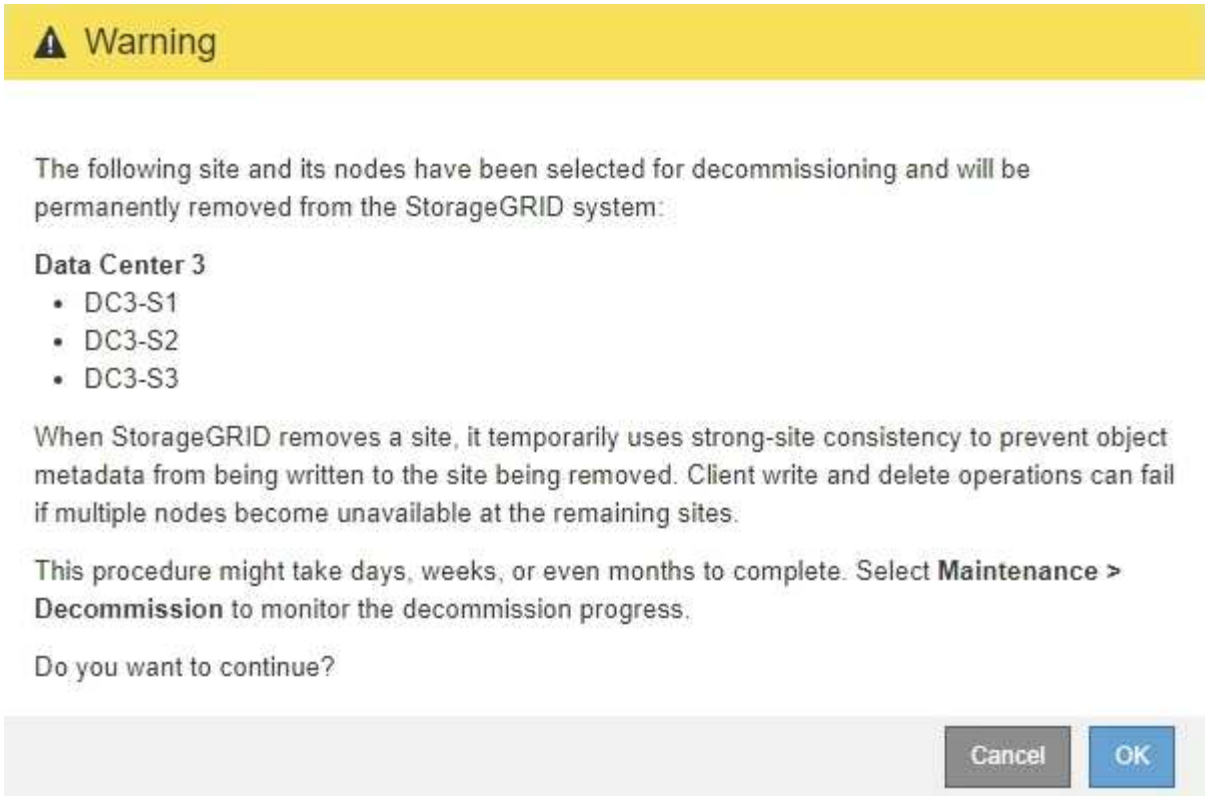
5. 프로비저닝 암호를 입력합니다.

   서비스 해제 시작 * 버튼이 활성화됩니다.



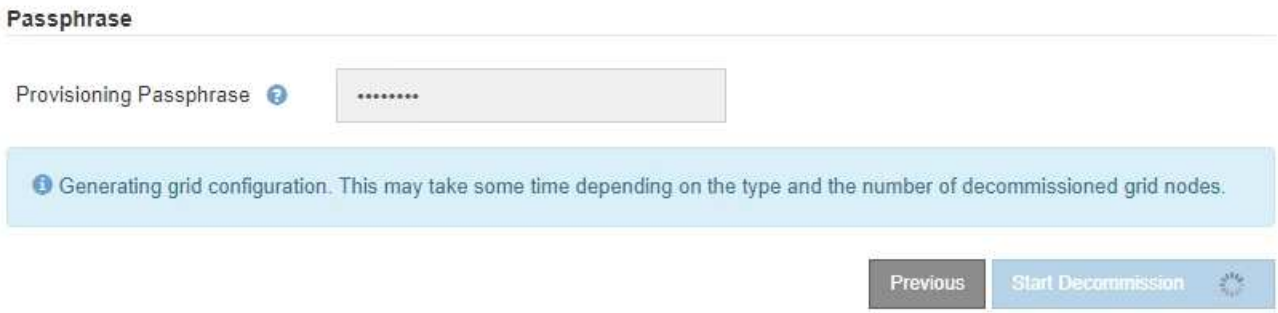
6. 사이트 서비스 해제 절차를 시작할 준비가 되면 * 서비스 해제 시작 * 을 선택합니다.

   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.

6단계**:** 서비스 해제 모니터링

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.

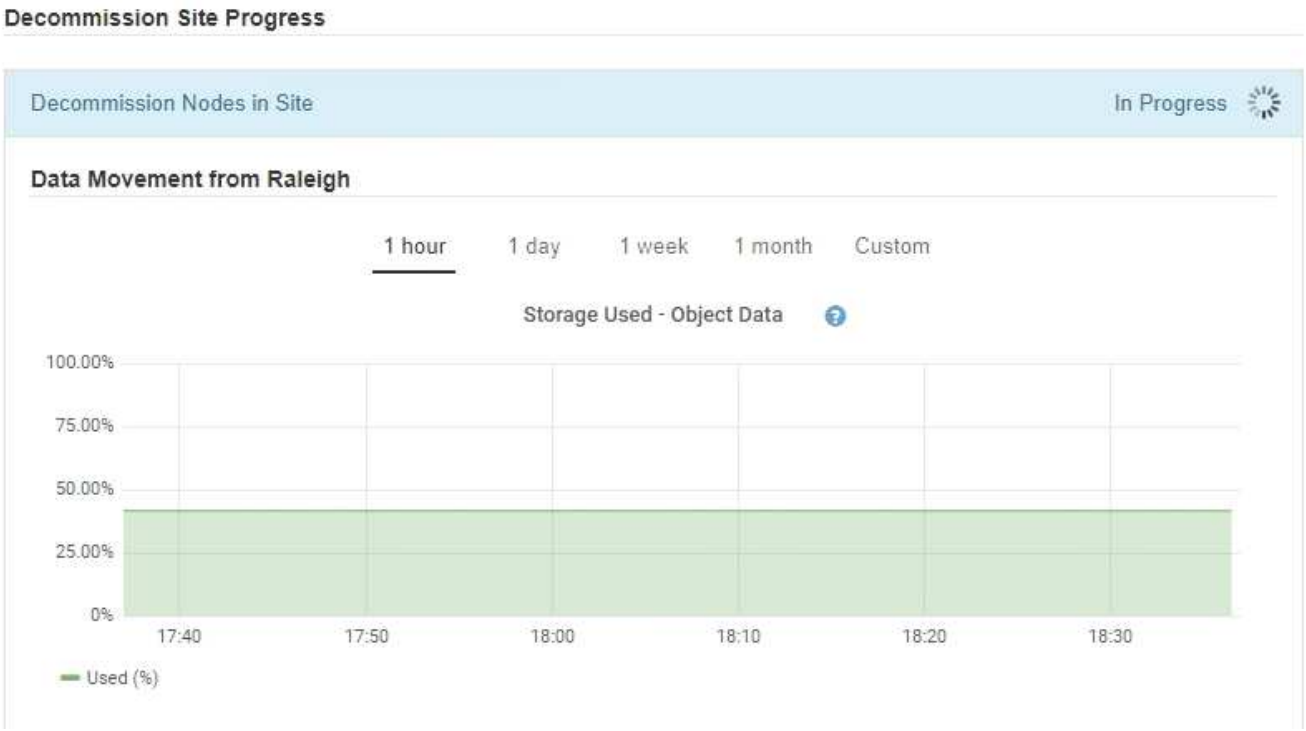
a. 메시지에서 링크를 선택하거나 * 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
b. `.zip`파일을 다운로드합니다.

의 지침을 "복구 패키지 다운로드 중"참조하십시오.

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

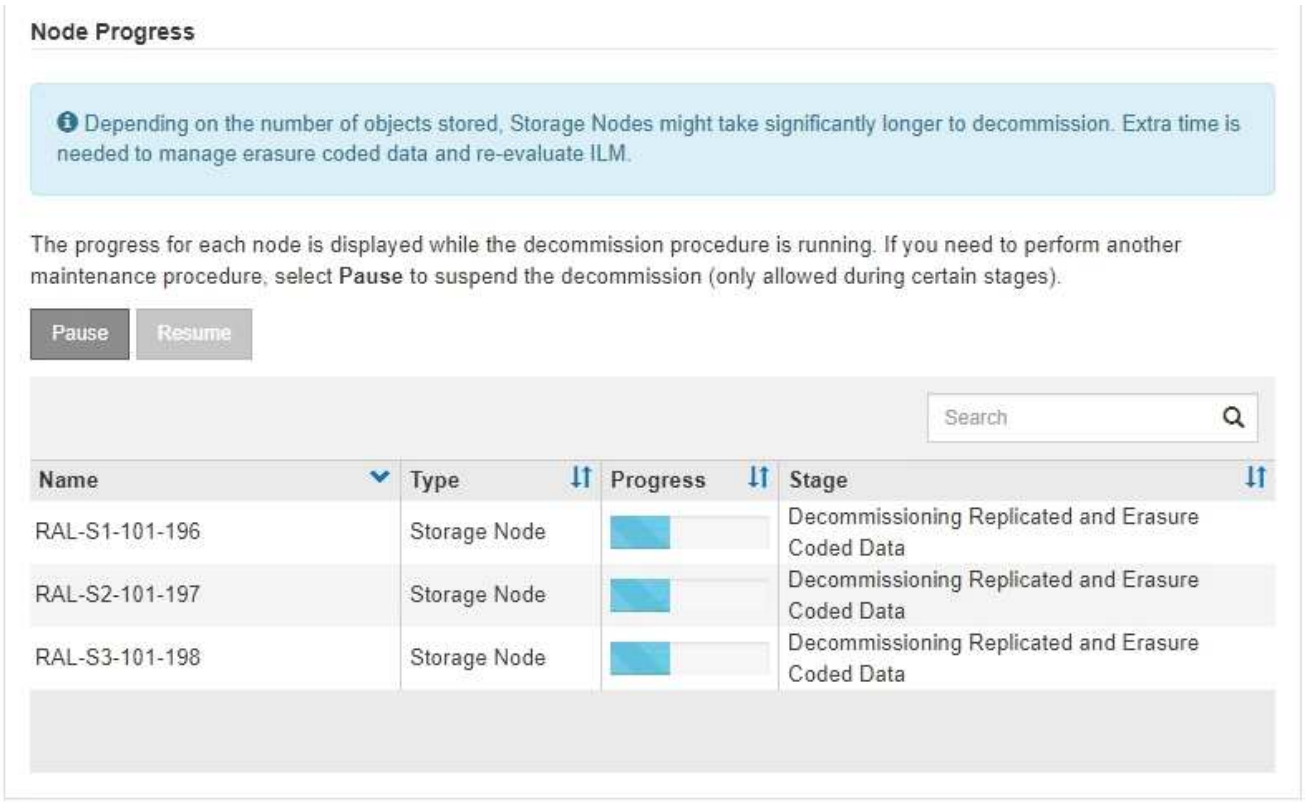
2. 데이터 이동 차트를 사용하여 이 사이트에서 다른 사이트로 개체 데이터의 이동을 모니터링합니다.

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.

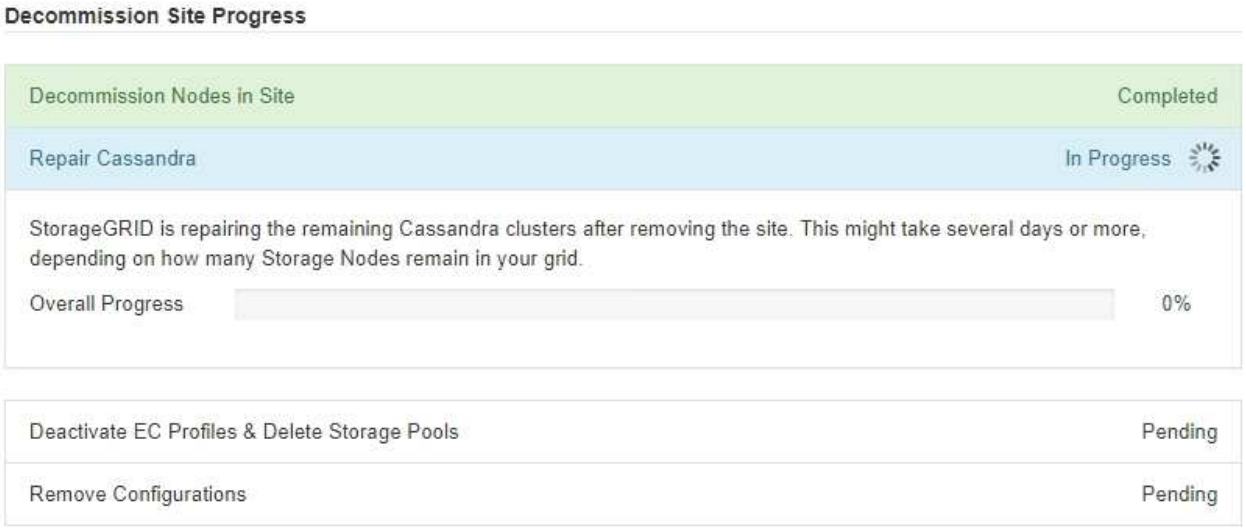
단계	예상 기간
보류 중	분 이하
잠금 대기	분
작업 준비	분 이하
LDR 사용 중지 표시	분
복제 및 삭제 해제 - 코드 데이터	데이터 양을 기준으로 한 시간, 일 또는 주 • 참고 *: 다른 유지보수 활동을 수행해야 하는 경우 이 단계 동안 사이트 파기를 일시 중지할 수 있습니다.
LDR 설정 상태	분
감사 대기열 플러시	메시지 수 및 네트워크 대기 시간을 기준으로 분~시간
완료	분

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
도면요소 제거	분

단계	예상 기간
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.

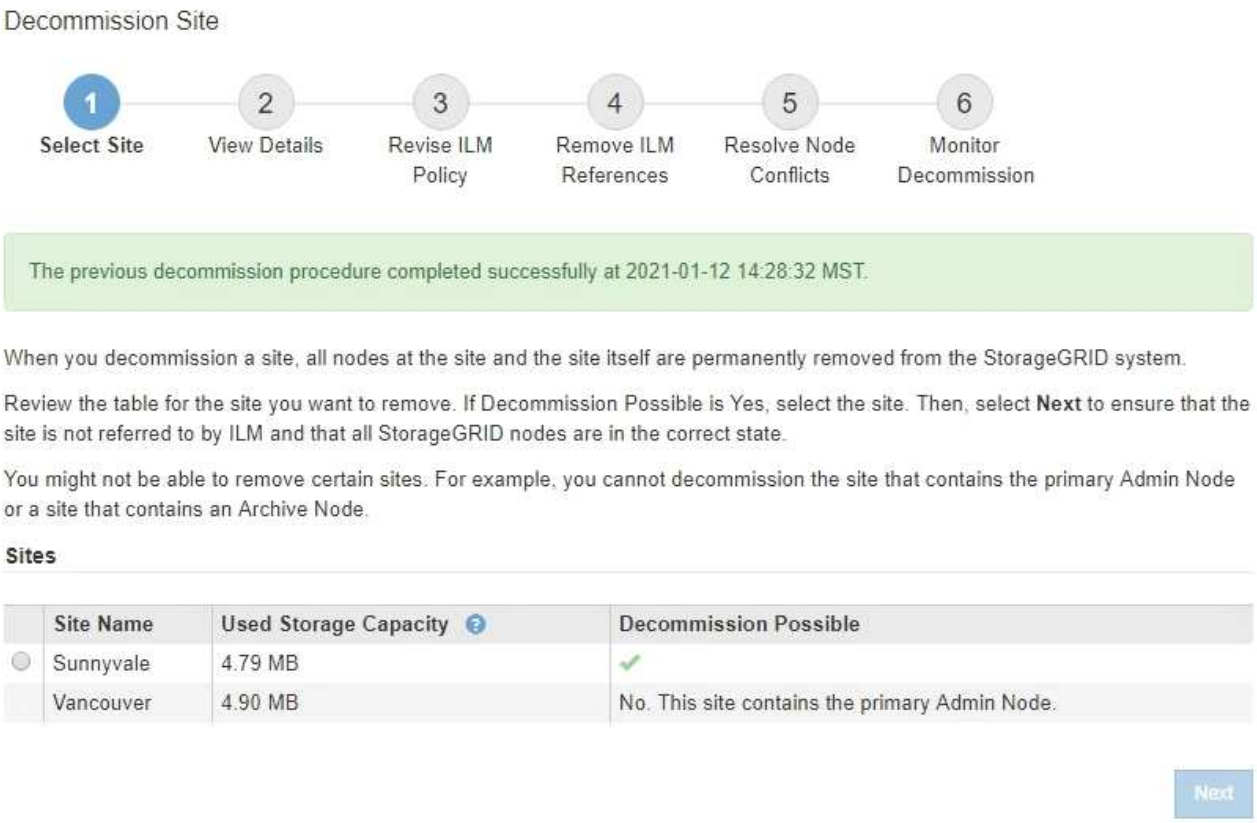


   - EC 프로파일 비활성화 및 스토리지 풀 삭제 * 단계에서 다음 ILM이 변경됩니다.
     - 사이트를 참조한 모든 삭제 코딩 프로필이 비활성화됩니다.
     - 사이트를 참조하는 모든 스토리지 풀이 삭제됩니다.

> 모든 스토리지 노드 스토리지 풀(StorageGRID 11.6 이하)은 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.

그리드, 사이트 또는 노드의 이름을 바꿉니다

이름 바꾸기 절차를 사용합니다

필요에 따라 전체 그리드, 각 사이트 및 각 노드에 대해 그리드 관리자 전체에 표시되는 표시 이름을 변경할 수 있습니다. 필요할 때마다 표시 이름을 안전하게 업데이트할 수 있습니다.

이름 바꾸기 절차는 무엇입니까?

처음에 StorageGRID를 설치할 때 그리드, 각 사이트 및 각 노드의 이름을 지정합니다. 이러한 초기 이름은 _system names_로 알려져 있으며 StorageGRID 전체에서 처음에 표시된 이름입니다.

시스템 이름은 내부 StorageGRID 작업에 필요하며 변경할 수 없습니다. 그러나 이름 바꾸기 절차를 사용하여 그리드,

각 사이트 및 각 노드에 대해 new_display names_를 정의할 수 있습니다. 이러한 표시 이름은 기본 시스템 이름 대신 (또는 일부 경우) 다양한 StorageGRID 위치에 표시됩니다.

이름 바꾸기 절차를 사용하여 오타를 수정하거나, 다른 명명 규칙을 구현하거나, 사이트 및 모든 노드의 위치가 변경되었음을 나타낼 수 있습니다. 시스템 이름과 달리, 표시 이름은 StorageGRID 작업에 영향을 주지 않고 필요할 때마다 업데이트할 수 있습니다.

시스템 및 표시 이름은 어디에 표시됩니까?

다음 표에는 StorageGRID 사용자 인터페이스 및 StorageGRID 파일에서 시스템 이름과 표시 이름이 표시되는 위치가 요약되어 있습니다.

위치	시스템 이름입니다	표시 이름
Grid Manager 페이지	항목의 이름이 바뀌지 않으면 표시됩니다	항목의 이름이 변경된 경우 다음 위치에서 시스템 이름 대신 표시됩니다. • 대시보드 • 노드 페이지 • 고가용성 그룹을 위한 구성 페이지, 로드 밸런서 엔드포인트, VLAN 인터페이스, 키 관리 서버, 그리드 암호, 방화벽 제어 기능을 제공합니다 • 경고 • 스토리지 풀 정의 • 개체 메타데이터 조회 페이지입니다 • 업그레이드, 핫픽스, SANtricity OS 업그레이드, 서비스 해제, 확장, 복구, 개체 존재 여부 검사 • 지원 페이지(로그 및 진단) • 관리 노드 세부 정보에 대한 테이블의 관리자 노드 호스트 이름 옆에 있는 단일 로그인 페이지
노드에 대한 * 노드 * > * 개요 * 탭	항상 표시됩니다	항목의 이름이 변경된 경우에만 표시됩니다
그리드 관리자의 레거시 페이지(예: * 지원 * > * 그리드 토폴로지 *)	표시됩니다	표시되지 않습니다
• 노드 상태 * API	항상 반환됩니다	항목의 이름이 변경된 경우에만 반환됩니다

위치	시스템 이름입니다	표시 이름

SSH를 사용하여 노드에 액세스할 때 확인 메시지를 표시합니다	항목의 이름이 바뀌지 않은 경우 기본 이름으로 표시됩니다.
	
	`admin@SYSTEM-NAME: ~ $`
	
	항목 이름이 변경될 때 괄호 안에 포함:
	
	`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`
		항목의 이름을 바꿀 때 기본 이름으로 표시됩니다.
		
		`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`

`Passwords.txt` 복구 패키지의 파일입니다	다음과 같이 표시됩니다 `Server Name`	다음과 같이 표시됩니다 `Display Name`
`/etc/hosts` 모든 노드의 파일 예를 들면 다음과 같습니다. `10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host`	항상 두 번째 열에 표시됩니다	항목의 이름이 변경되면 네 번째 열에 표시됩니다
`topology-display-names.json`AutoSupport 데이터에 포함되어 있습니다	포함되지 않음	항목의 이름이 바뀌지 않으면 비어 있고, 그렇지 않으면 그리드, 사이트 및 노드 ID가 표시 이름에 매핑됩니다.

표시 이름 요구 사항

이 절차를 사용하기 전에 표시 이름에 대한 요구 사항을 검토하십시오.

노드의 이름을 표시합니다

노드의 표시 이름은 다음 규칙을 따라야 합니다.

- StorageGRID 시스템에서 고유해야 합니다.
- StorageGRID 시스템의 다른 항목에 대한 시스템 이름과 같을 수 없습니다.
- 1자 이상 32자 이하여야 합니다.
- 숫자, 하이픈(-) 및 대문자와 소문자를 포함할 수 있습니다.
- 문자나 숫자로 시작하거나 끝날 수 있지만 하이픈으로 시작하거나 끝날 수 없습니다.
- 모든 숫자가 될 수 없습니다.
- 대/소문자를 구분하지 않습니다. 예를 들어, `DC1-ADM` 및 `dc1-adm` 은 중복 항목으로 간주됩니다.

이름 바꾸로 인해 표시 이름 또는 시스템 이름이 중복되지 않는 한, 다른 노드에서 이전에 사용한 표시 이름으로 노드 이름을 바꿀 수 있습니다.

그리드 및 사이트의 이름을 표시합니다

눈금 및 사이트의 표시 이름은 다음과 같은 예외 사항과 동일한 규칙을 따릅니다.

- 공백을 포함할 수 있습니다.
- 다음 특수 문자를 포함할 수 있습니다. `= - _ : , . @ !`
- 하이픈을 포함하여 특수 문자로 시작하거나 끝날 수 있습니다.
- 모든 숫자 또는 특수 문자일 수 있습니다.

모범 사례를 제시합니다

여러 항목의 이름을 바꾸려는 경우 이 절차를 사용하기 전에 일반 명명 체계를 문서화합니다. 이름이 고유하고 일관되며 이해하기 쉽도록 한 눈에 파악할 수 있는 시스템을 제공합니다.

조직의 요구 사항에 맞는 명명 규칙을 사용할 수 있습니다. 다음과 같은 기본적인 권장 사항을 고려하십시오.

- * 사이트 표시기 *: 사이트가 여러 개인 경우 각 노드 이름에 사이트 코드를 추가합니다.
- * 노드 유형 *: 노드 이름은 일반적으로 노드 유형을 나타냅니다. , `adm` 및 `gw` (스토리지 노드, 관리자 노드 및 게이트웨이 노드)와 같은 약어를 사용할 수 `s` 있습니다.
- * 노드 번호 *: 사이트에 특정 노드 형식이 둘 이상 포함된 경우 각 노드 이름에 고유 번호를 추가합니다.

시간에 따라 변경될 수 있는 이름에 특정 세부 정보를 추가하기 전에 두 번 생각해 보십시오. 예를 들어, 노드 이름은 변경할 수 있으므로 IP 주소를 포함하지 마십시오. 마찬가지로, 장비를 이동하거나 하드웨어를 업그레이드할 경우 랙 위치 또는 어플라이언스 모델 번호가 변경될 수 있습니다.

표시 이름의 예

StorageGRID 시스템에 세 개의 데이터 센터가 있고 각 데이터 센터에 서로 다른 유형의 노드가 있다고 가정해 보겠습니다. 표시 이름은 다음과 같이 간단할 수 있습니다.

- * 그리드 *: `StorageGRID Deployment`
- * 첫 번째 사이트 *: `Data Center 1`
  - `dc1-adm1`
  - `dc1-s1`
  - `dc1-s2`
  - `dc1-s3`
  - `dc1-gw1`
- * 두 번째 사이트 *: `Data Center 2`
  - `dc2-adm2`
  - `dc2-s1`
  - `dc2-s2`

- dc2-s3

- * 세 번째 사이트 *: Data Center 3
  - dc3-s1
  - dc3-s2
  - dc3-s3

표시 이름을 추가하거나 업데이트합니다

이 절차를 사용하여 그리드, 사이트 및 노드에 사용되는 표시 이름을 추가하거나 업데이트할 수 있습니다. 단일 항목, 여러 항목 또는 모든 항목의 이름을 동시에 변경할 수 있습니다. 표시 이름을 정의하거나 업데이트해도 StorageGRID 작업에는 영향을 주지 않습니다.

시작하기 전에

- 기본 관리자 노드 * 에서 를 사용하여 그리드 관리자에 로그인됩니다."지원되는 웹 브라우저"

> 기본 관리 노드가 아닌 노드에서 표시 이름을 추가하거나 업데이트할 수 있지만 복구 패키지를 다운로드하려면 기본 관리 노드에 로그인해야 합니다.

- 이 "유지 관리 또는 루트 액세스 권한"있습니다.
- 프로비저닝 암호가 있습니다.
- 표시 이름의 요구사항 및 모범 사례를 이해합니다. 을 "그리드, 사이트 및 노드의 이름을 바꿉니다"참조하십시오.

그리드, 사이트 또는 노드의 이름을 바꾸는 방법

StorageGRID 시스템, 하나 이상의 사이트 또는 하나 이상의 노드 이름을 바꿀 수 있습니다.

이름 바꾸로 인해 표시 이름이나 시스템 이름이 중복되지 않는 한, 다른 노드에서 이전에 사용한 표시 이름을 사용할 수 있습니다.

이름을 바꿀 항목을 선택합니다

시작하려면 이름을 바꿀 항목을 선택합니다.

단계

1. 유지보수 * > * 작업 * > * 그리드, 사이트, 노드 이름 바꾸기 * 를 선택합니다.
2. 이름 선택 * 단계에서 이름을 바꿀 항목을 선택합니다.

변경할 항목입니다	지침
시스템의 모든 이름(또는 거의 모든 이름)입니다	a. Select All * 을 선택합니다. b. 선택적으로 이름을 바꾸지 않을 항목을 지웁니다.
그리드의 이름입니다	그리드의 확인란을 선택합니다.

변경할 항목입니다	지침
사이트 이름 및 해당 노드의 일부 또는 전입니다	a. 사이트의 표 머리글에서 확인란을 선택합니다. b. 필요에 따라 이름을 바꾸지 않을 노드의 선택을 취소합니다.
사이트의 이름입니다	사이트의 확인란을 선택합니다.
노드의 이름입니다	노드의 확인란을 선택합니다.

3. Continue * 를 선택합니다.
4. 선택한 항목이 포함된 표를 검토합니다.
   - 표시 이름 * 열에는 각 항목의 현재 이름이 표시됩니다. 항목의 이름을 바꾼 적이 없으면 표시 이름은 해당 시스템 이름과 같습니다.
   - 시스템 이름 * 열에는 설치 중에 각 항목에 입력한 이름이 표시됩니다. 시스템 이름은 내부 StorageGRID 작업에 사용되며 변경할 수 없습니다. 예를 들어 노드의 시스템 이름은 호스트 이름일 수 있습니다.
   - Type * 열은 항목의 유형(그리드, 사이트 또는 특정 노드 유형)을 나타냅니다.

새 이름 제안

새 이름 제안 * 단계에서는 각 항목의 표시 이름을 개별적으로 입력하거나 항목 이름을 대량으로 바꿀 수 있습니다.

항목 이름을 개별적으로 변경합니다

다음 단계에 따라 이름을 바꾸려는 각 항목의 표시 이름을 입력합니다.

단계

1. 표시 이름 * 필드에 목록의 각 항목에 대해 제안된 표시 이름을 입력합니다.

   명명 요구 사항에 대한 자세한 내용은 을 "그리드, 사이트 및 노드의 이름을 바꿉니다"참조하십시오.

2. 이름을 바꾸지 않을 항목을 제거하려면 * 목록에서 제거 * 열을 선택합니다✕.

   항목의 새 이름을 제안하지 않을 경우에는 테이블에서 해당 이름을 제거해야 합니다.

3. 테이블의 모든 항목에 대해 새 이름을 제안했으면 * Rename * 을 선택합니다.

   성공 메시지가 나타납니다. 이제 그리드 관리자 전체에서 새 표시 이름이 사용됩니다.

항목 이름을 대량으로 변경합니다

항목 이름이 다른 문자열로 바꿀 공통 문자열을 공유하는 경우 일괄 이름 바꾸기 도구를 사용합니다.

단계

1. 새 이름 제안 * 단계에서 * 대량 이름 바꾸기 도구 사용 * 을 선택합니다.

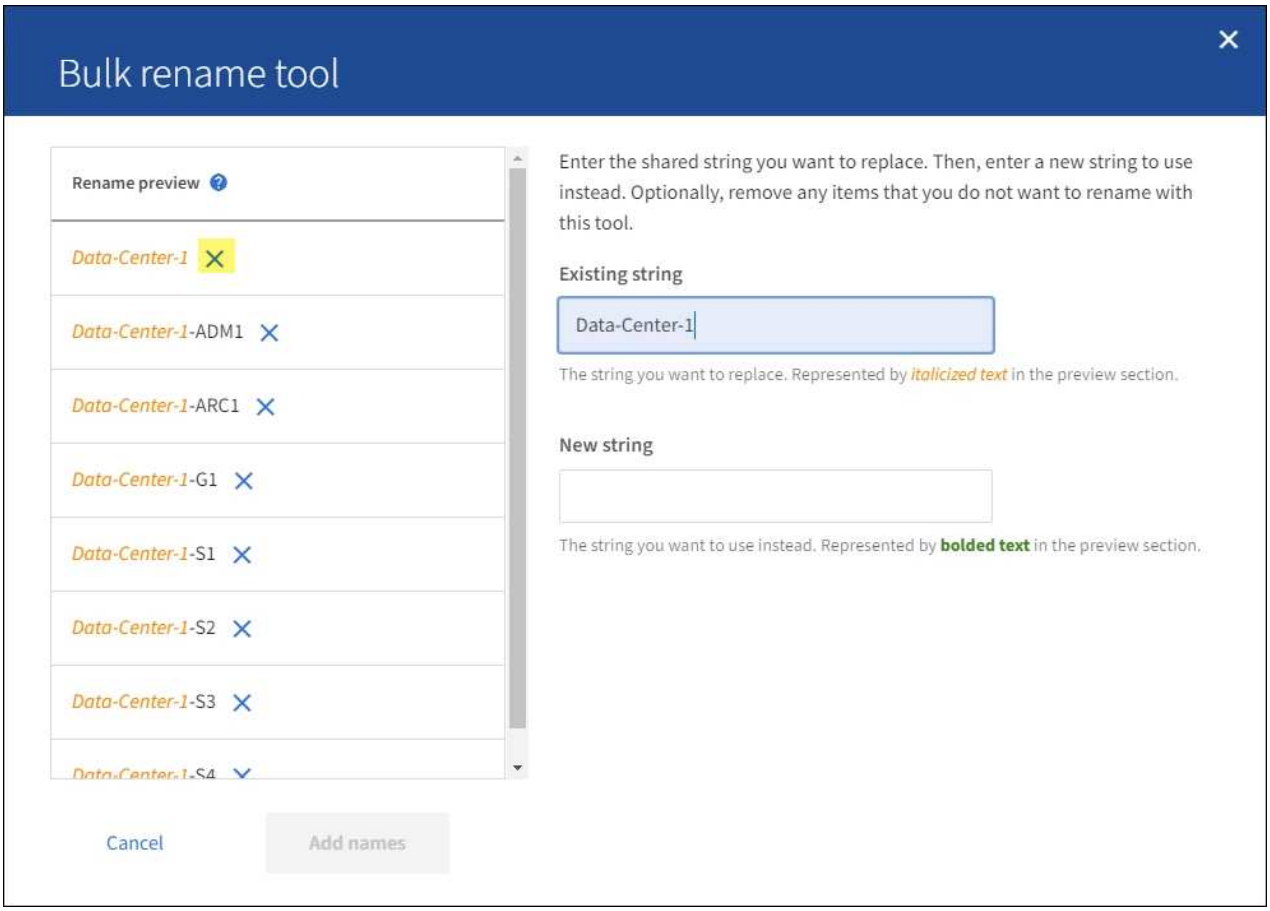
   이름 바꾸기 미리 보기 * 에는 * 새 이름 제안 * 단계에 대해 표시된 모든 항목이 포함됩니다. 미리 보기를 사용하여 공유 문자열을 교체한 후 표시 이름이 어떻게 표시되는지 확인할 수 있습니다.

2. 기존 문자열 * 필드에 바꾸려는 공유 문자열을 입력합니다. 예를 들어, 바꾸려는 문자열이 인 `Data-Center-1` 경우 * Data-Center-1 * 을 입력합니다.

   입력할 때 텍스트는 왼쪽 이름에 있는 모든 위치에 강조 표시됩니다.

3. 이 도구로 이름을 바꾸지 않을 항목을 제거하려면 선택합니다✕.

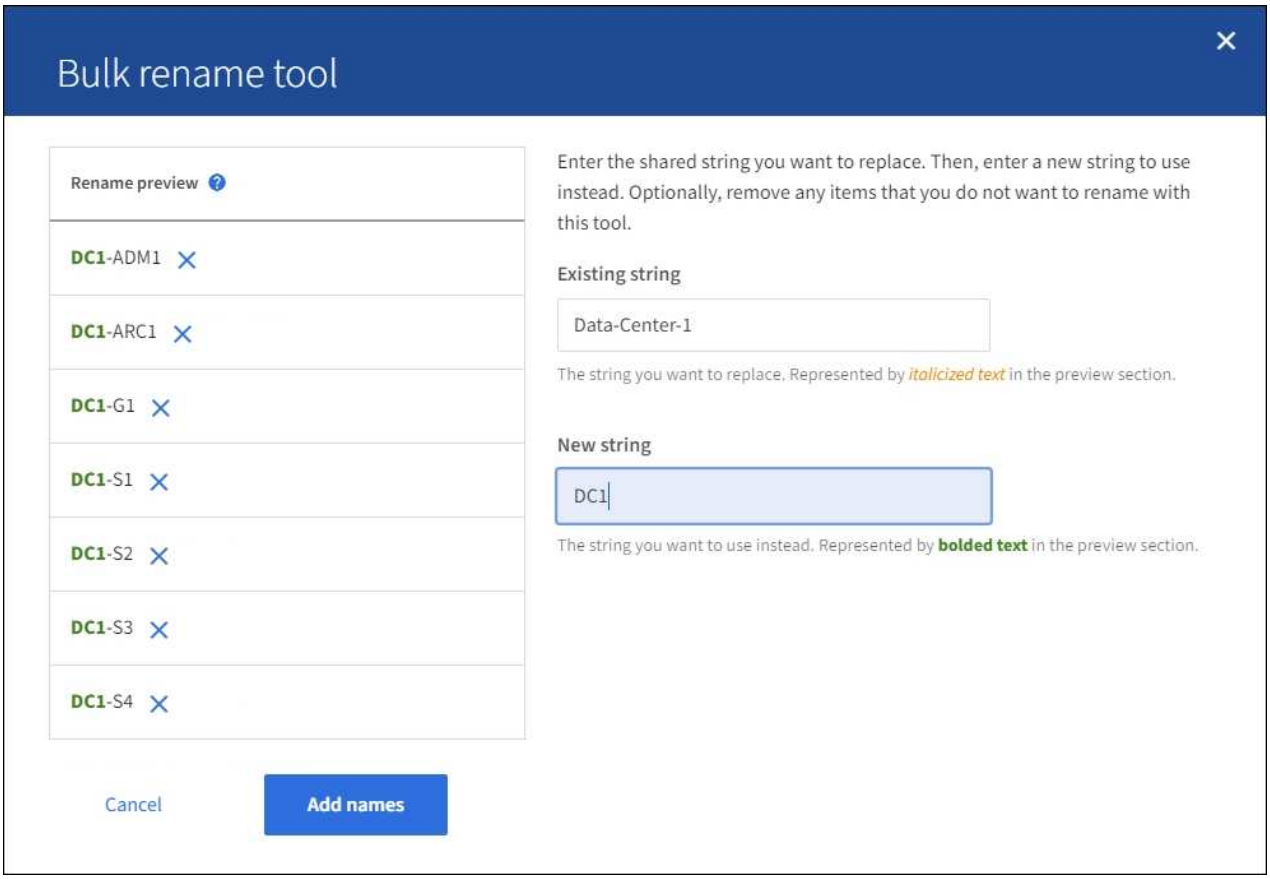
   예를 들어 문자열을 포함하는 모든 노드의 이름을 바꾸지만 사이트 자체의 이름을 바꾸지 않으려는 `Data-Center-1` 경우를 가정해 `Data-Center-1` 봅니다. 이름 바꾸기 미리 보기에서 사이트를 제거하려면 선택합니다✕.



4. 새 문자열 * 필드에 대신 사용할 대체 문자열을 입력합니다. 예를 들어 * DC1 * 을 입력합니다.

   명명 요구 사항에 대한 자세한 내용은 을 "그리드, 사이트 및 노드의 이름을 바꿉니다"참조하십시오.

   대체 문자열을 입력하면 왼쪽에 있는 이름이 업데이트되므로 새 이름이 올바른지 확인할 수 있습니다.



5. 미리 보기에 표시된 이름이 만족스러우면 * 이름 추가 * 를 선택하여 * 새 이름 제안 * 단계에 대한 이름을 테이블에 추가합니다.
6. 필요한 항목을 추가로 변경하거나 ✕이름을 바꾸지 않을 항목을 모두 제거합니다.
7. 테이블의 모든 항목의 이름을 바꿀 준비가 되면 * Rename * 을 선택합니다.

   성공 메시지가 표시됩니다. 이제 그리드 관리자 전체에서 새 표시 이름이 사용됩니다.

복구 패키지를 다운로드합니다

항목 이름 바꾸기를 마치면 새 복구 패키지를 다운로드하여 저장합니다. 이름을 바꾼 항목의 새 표시 이름이 `Passwords.txt` 파일에 포함됩니다.

단계

1. 프로비저닝 암호를 입력합니다.
2. 복구 패키지 다운로드 * 를 선택합니다.

   다운로드가 즉시 시작됩니다.

3. 다운로드가 완료되면 파일을 열어 `Passwords.txt` 모든 노드의 서버 이름과 이름이 바뀐 노드의 표시 이름을 확인합니다.
4. `sgws-recovery-package-*id-revision*.zip`파일을 안전하고 안전한 두 개의 별도 위치에 복사합니다.

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

5. 첫 번째 단계로 돌아가려면 * 마침 * 을 선택합니다.

표시 이름을 시스템 이름으로 되돌립니다

이름이 바뀐 그리드, 사이트 또는 노드를 원래 시스템 이름으로 되돌릴 수 있습니다. 항목을 시스템 이름으로 되돌리면 그리드 관리자 페이지 및 기타 StorageGRID 위치에 해당 항목의 * 표시 이름 * 이 더 이상 표시되지 않습니다. 항목의 시스템 이름만 표시됩니다.

단계

1. 유지보수 * > * 작업 * > * 그리드, 사이트, 노드 이름 바꾸기 * 를 선택합니다.
2. 이름 선택 * 단계에서 시스템 이름으로 되돌리려는 항목을 선택합니다.
3. Continue * 를 선택합니다.
4. 새 이름 제안 * 단계에서는 표시 이름을 개별적으로 또는 대량으로 시스템 이름으로 되돌립니다.

시스템 이름으로 개별적으로 되돌립니다

a. 각 항목의 원래 시스템 이름을 복사하여 * 표시 이름 * 필드에 붙여 넣거나, 되돌리지 않을 항목을 제거하려면 선택합니다❌.

표시 이름을 되돌리려면 시스템 이름이 * 표시 이름 * 필드에 나타나야 하지만 이름은 대소문자를 구분하지 않습니다.

b. 이름 바꾸기 * 를 선택합니다.

성공 메시지가 나타납니다. 이러한 항목의 표시 이름은 더 이상 사용되지 않습니다.

시스템 이름으로 일괄 되돌리기

a. 새 이름 제안 * 단계에서 * 대량 이름 바꾸기 도구 사용 * 을 선택합니다.
b. 기존 문자열 * 필드에 바꿀 표시 이름 문자열을 입력합니다.
c. 새 문자열 * 필드에 대신 사용할 시스템 이름 문자열을 입력합니다.
d. 새 이름 제안 * 단계에 대한 이름을 테이블에 추가하려면 * 이름 추가 * 를 선택합니다.
e. Display name* 필드의 각 항목이 * System name* 필드의 이름과 일치하는지 확인합니다. 변경하거나 되돌리지 않을 항목을 제거하려면 선택합니다❌.

표시 이름을 되돌리려면 시스템 이름이 * 표시 이름 * 필드에 나타나야 하지만 이름은 대소문자를 구분하지 않습니다.

f. 이름 바꾸기 * 를 선택합니다.

성공 메시지가 표시됩니다. 이러한 항목의 표시 이름은 더 이상 사용되지 않습니다.

5. 새 복구 패키지를 다운로드하여 저장합니다..

되돌린 항목의 표시 이름은 더 이상 파일에 포함되지 `Passwords.txt` 않습니다.

노드 절차

노드 유지 관리 절차

특정 그리드 노드 또는 노드 서비스와 관련된 유지 관리 절차를 수행해야 할 수도 있습니다.

서버 관리자 절차

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.

서버 관리자 절차를 수행하려면 일반적으로 노드의 명령줄에 액세스해야 합니다.

> 기술 지원 부서에서 지시하는 경우에만 서버 관리자에 액세스해야 합니다.

> Server Manager를 완료한 후 현재 명령 셸 세션을 닫고 로그아웃해야 합니다. 다음을 입력합니다. `exit`

노드 재부팅, 종료 및 전원 절차

다음 절차를 사용하여 노드를 하나 이상 재부팅하거나, 노드를 종료 및 재시작하거나, 노드 전원을 껐다가 다시 켤 수 있습니다.

포트 재매핑 절차

이전에 다시 매핑된 포트를 사용하여 로드 밸런서 끝점을 구성하려는 경우 등에 포트 리매핑 절차를 사용하여 노드에서 포트 리맵을 제거할 수 있습니다.

서버 관리자 절차

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.

시작하기 전에

`Passwords.txt`파일이 있습니다.

단계

1. 그리드 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 그리드 노드에서 실행 중인 서버 관리자의 현재 상태를 봅니다. **`service servermanager status`**

그리드 노드에서 실행 중인 Server Manager의 현재 상태가 보고됩니다(실행 여부). 서버 관리자의 상태가 인 경우 `running` 마지막으로 시작한 이후 실행된 시간이 나열됩니다. 예를 들면 다음과 같습니다.

```
servermanager running for 1d, 13h, 0m, 30s
```

3. 그리드 노드에서 실행 중인 서버 관리자의 현재 버전을 봅니다. **`service servermanager version`**

현재 버전이 나열됩니다. 예를 들면 다음과 같습니다.

```
11.1.0-20180425.1905.39c9493
```

4. 명령 셸에서 로그아웃합니다. **`exit`**

모든 서비스의 현재 상태를 봅니다

그리드 노드에서 실행 중인 모든 서비스의 현재 상태를 언제든지 볼 수 있습니다.

시작하기 전에

`Passwords.txt`파일이 있습니다.

단계

1. 그리드 노드에 로그인합니다.

a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

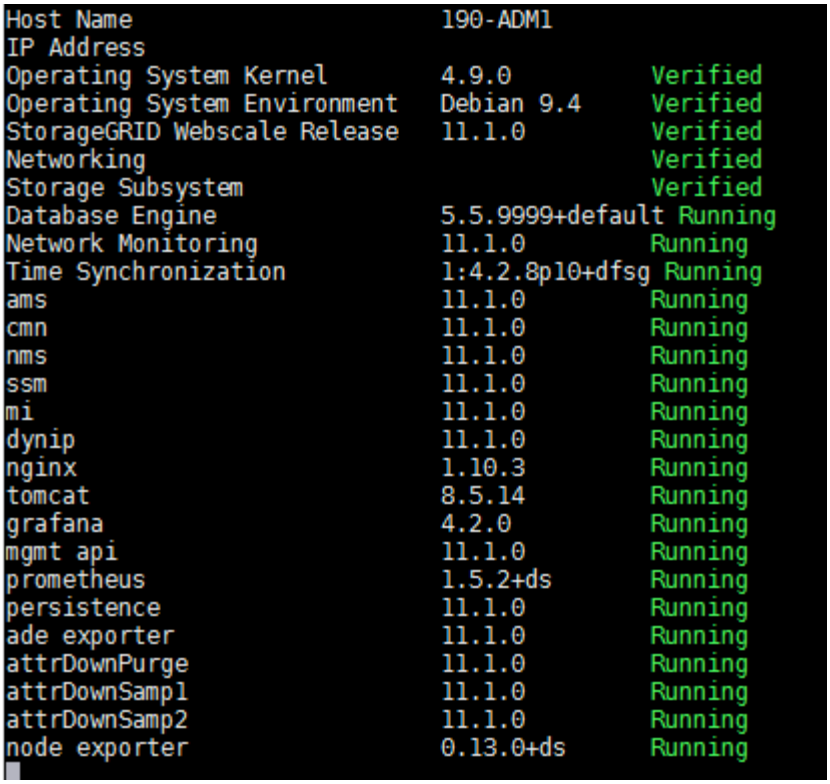
c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 그리드 노드에서 실행 중인 모든 서비스의 상태를 봅니다. `storagegrid-status`

예를 들어 기본 관리 노드의 출력은 AMS, CMN 및 NMS 서비스의 현재 상태를 실행 중으로 표시합니다. 이 출력은 서비스 상태가 변경되면 즉시 업데이트됩니다.



3. 명령줄로 돌아가 * Ctrl * + * C * 를 누릅니다.
4. 필요에 따라 그리드 노드에서 실행되는 모든 서비스에 대한 정적 보고서를 봅니다. `/usr/local/servermanager/reader.rb`

   이 보고서에는 계속 업데이트되는 보고서와 같은 정보가 포함되어 있지만 서비스 상태가 변경되면 업데이트되지 않습니다.

5. 명령 셸에서 로그아웃합니다. `exit`

서버 관리자 및 모든 서비스를 시작합니다

서버 관리자를 시작해야 할 수도 있습니다. 그러면 그리드 노드에서 모든 서비스가 시작됩니다.

시작하기 전에

`Passwords.txt`파일이 있습니다.

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. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 서버 관리자 시작: `service servermanager start`

3. 명령 셸에서 로그아웃합니다. `exit`

서버 관리자 및 모든 서비스를 다시 시작합니다

서버 관리자와 그리드 노드에서 실행 중인 모든 서비스를 다시 시작해야 할 수 있습니다.

시작하기 전에

`Passwords.txt`파일이 있습니다.

단계

1. 그리드 노드에 로그인합니다.

a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 서버 관리자 및 그리드 노드의 모든 서비스를 다시 시작합니다. `service servermanager restart`

서버 관리자와 그리드 노드의 모든 서비스가 중지되었다가 다시 시작됩니다.

명령 사용은 `restart` 명령 다음에 `start` 명령을 사용하는 것과 `stop` 같습니다.

3. 명령 셸에서 로그아웃합니다. `exit`

서버 관리자 및 모든 서비스를 중지합니다

Server Manager는 항상 실행되도록 되어 있지만 서버 관리자 및 그리드 노드에서 실행되는 모든 서비스를 중지해야 할 수 있습니다.

시작하기 전에

`Passwords.txt`파일이 있습니다.

단계

1. 그리드 노드에 로그인합니다.

a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 서버 관리자 및 그리드 노드에서 실행되는 모든 서비스를 중지합니다. `service servermanager stop`

   서버 관리자와 그리드 노드에서 실행되는 모든 서비스가 정상적으로 종료됩니다. 서비스를 종료하는 데 최대 15분이 소요될 수 있습니다.

3. 명령 셸에서 로그아웃합니다. `exit`

서비스의 현재 상태를 봅니다

그리드 노드에서 실행 중인 서비스의 현재 상태를 언제든지 볼 수 있습니다.

시작하기 전에

`Passwords.txt`파일이 있습니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

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 셸에서 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.

시작하기 전에

`Passwords.txt`파일이 있습니다.

이 작업에 대해

이 단계를 사용하여 서비스를 "관리 방식으로 중지"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. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 개별 서비스 중지: `service servicename stop`

   예를 들면 다음과 같습니다.

   ```
   service ldr stop
   ```

   서비스를 중지하는 데 최대 11분이 걸릴 수 있습니다.

3. 명령 셸에서 로그아웃합니다. `exit`

관련 정보

"서비스 강제 종료"

서비스 강제 종료

서비스를 즉시 중지해야 하는 경우 명령을 사용할 수 `force-stop` 있습니다.

시작하기 전에

`Passwords.txt`파일이 있습니다.

단계

1. 그리드 노드에 로그인합니다.

a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 수동으로 서비스 종료: `service servicename force-stop`

예를 들면 다음과 같습니다.

```
service ldr force-stop
```

시스템은 30초 후에 서비스를 종료합니다.

3. 명령 셸에서 로그아웃합니다. `exit`

서비스를 시작하거나 다시 시작합니다

중지된 서비스를 시작해야 하거나 서비스를 중지했다가 다시 시작해야 할 수 있습니다.

시작하기 전에

`Passwords.txt`파일이 있습니다.

단계

1. 그리드 노드에 로그인합니다.

a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 서비스가 현재 실행 중인지 또는 중지되었는지 여부에 따라 실행할 명령을 결정합니다.

◦ 서비스가 현재 중지된 경우 명령을 사용하여 `start` 서비스를 수동으로 시작합니다. `service servicename start`

예를 들면 다음과 같습니다.

```
service ldr start
```

◦ 서비스가 현재 실행 중인 경우 명령을 사용하여 `restart` 서비스를 중지한 다음 다시 시작합니다. `service servicename restart`

예를 들면 다음과 같습니다.

```
service ldr restart
```

+

명령 사용은 `restart` 명령 다음에 `start` 명령을 사용하는 것과 `stop` 같습니다. 서비스가 현재 중지된 경우에도 발급할 수 `restart` 있습니다.

3. 명령 셸에서 로그아웃합니다. `exit`

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.

시작하기 전에

`Passwords.txt`파일이 있습니다.

단계

1. 그리드 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 $ 로 `#`변경됩니다.

2. DoNotStart 파일 추가: `touch /etc/sv/service/DoNotStart`

   여기서 `service` 는 시작을 금지할 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 로그아웃합니다. `exit`

서비스에 대한 **DoNotStart** 파일을 제거합니다

서비스 시작을 방해하는 DoNotStart 파일을 제거할 경우 해당 서비스를 시작해야 합니다.

시작하기 전에

`Passwords.txt`파일이 있습니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 $ 로 `#`변경됩니다.

2. 서비스 디렉터리에서 DoNotStart 파일을 제거합니다. `rm /etc/sv/service/DoNotStart`

   여기서 `service` 는 서비스 이름입니다. 예를 들면, 다음과 같습니다.

   ```
   rm /etc/sv/ldr/DoNotStart
   ```

3. 서비스를 시작합니다. `service servicename start`
4. 명령 셸에서 로그아웃합니다. `exit`

서버 관리자 문제를 해결합니다

Server Manager를 사용할 때 문제가 발생하면 로그 파일을 확인하십시오.

서버 관리자와 관련된 오류 메시지는 다음 위치에 있는 서버 관리자 로그 파일에 캡처됩니다.
`/var/local/log/servermanager.log`

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.

시작하기 전에

`Passwords.txt`파일이 있습니다.

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. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 서비스의 오류 상태를 확인합니다. `service servicename status`

   예를 들면 다음과 같습니다.

   ```
   service ldr status
   ```

   서비스가 오류 상태인 경우 다음 메시지가 반환됩니다 *servicename* `in error state`. 예를 들면 다음과 같습니다.

   ```
   ldr in error state
   ```

   > ⓘ 서비스 상태가 인 경우 `disabled` 의 지침을 "서비스에 대한 DoNotStart 파일 제거"참조하십시오.

3. 서비스를 다시 시작하여 오류 상태를 제거해 보십시오. `service servicename restart`

   서비스가 다시 시작되지 않으면 기술 지원 부서에 문의하십시오.

4. 명령 셸에서 로그아웃합니다. `exit`

재부팅, 종료 및 전원 절차를 수행합니다

롤링 재부팅을 수행합니다

서비스 중단 없이 여러 그리드 노드를 재부팅하도록 롤링 재부팅을 수행할 수 있습니다.

시작하기 전에

- 기본 관리자 노드에서 그리드 관리자에 로그인되어 있으며 를 사용하고 "지원되는 웹 브라우저"있습니다.

  이 절차를 수행하려면 기본 관리자 노드에 로그인해야 합니다.

- 이 "유지 관리 또는 루트 액세스 권한"있습니다.

이 작업에 대해

여러 노드를 동시에 재부팅해야 하는 경우 이 절차를 사용하십시오. 예를 들어, 그리드의 FIPS 모드를 변경한 후에 이 절차를 사용할 수 "TLS 및 SSH 보안 정책"있습니다. FIPS 모드가 변경될 경우 변경 사항을 적용하려면 모든 노드를 재부팅해야 합니다.

한 노드만 재부팅해야 하는 경우 가능합니다"Tasks 탭에서 노드를 재부팅합니다".

StorageGRID가 그리드 노드를 재부팅하면 각 노드에서 명령을 발행하여 `reboot` 노드가 종료되었다가 다시 시작됩니다. 모든 서비스가 자동으로 다시 시작됩니다.

- VMware 노드를 재부팅하면 가상 머신이 재부팅됩니다.
- Linux 노드를 재부팅하면 컨테이너가 재부팅됩니다.
- StorageGRID 어플라이언스 노드를 재부팅하면 컴퓨팅 컨트롤러가 재부팅됩니다.

롤링 재부팅 절차에서 여러 노드를 동시에 재부팅할 수 있지만 다음과 같은 경우는 예외입니다.

- 같은 유형의 두 노드는 동시에 재부팅되지 않습니다.
- 게이트웨이 노드와 관리 노드는 동시에 재부팅되지 않습니다.

대신 이러한 노드는 HA 그룹, 오브젝트 데이터 및 중요 노드 서비스를 항상 사용 가능한 상태로 유지하기 위해 순차적으로 재부팅됩니다.

기본 관리자 노드를 재부팅하면 브라우저에서 그리드 관리자에 대한 액세스가 일시적으로 중단되므로 더 이상 절차를 모니터링할 수 없습니다. 따라서 기본 관리자 노드가 마지막으로 재부팅됩니다.

롤링 재부팅을 수행합니다

재부팅할 노드를 선택하고 선택 항목을 검토하며 재부팅 절차를 시작하고 진행 상황을 모니터링합니다.

노드를 선택합니다

첫 번째 단계로 Rolling Reboot 페이지에 액세스하여 재부팅할 노드를 선택합니다.

단계

1. maintenance * > * 작업 * > * 롤링 재부팅 * 을 선택합니다.
2. 노드 이름 * 열에서 연결 상태 및 경고 아이콘을 검토합니다.

   노드가 그리드에서 분리된 경우 재부팅할 수 없습니다. 노드의 경우 또는 아이콘이 다음과 같은 경우 확인란이 비활성화됩니다 .

3. 노드에 활성 경고가 있는 경우 * Alert summary * 열에서 경고 목록을 검토합니다.

   노드에 대한 현재 알림을 모두 보려면 를 선택할 수도 "노드 및 GT, 개요 탭"있습니다.

4. 필요한 경우 현재 경고를 해결하기 위해 권장되는 작업을 수행합니다.
5. 모든 노드가 연결되어 있고 모든 노드를 재부팅하려는 경우 테이블 헤더에서 확인란을 선택하고 * Select All * 을 선택합니다. 그렇지 않으면 재부팅할 각 노드를 선택합니다.

   테이블의 필터 옵션을 사용하여 노드의 하위 집합을 볼 수 있습니다. 예를 들어 특정 사이트의 스토리지 노드만 보거나 모든 노드를 선택하고 선택할 수 있습니다.

6. Review selection * 을 선택합니다.

선택 사항을 검토합니다

이 단계에서는 총 재부팅 절차에 소요되는 시간을 확인하고 올바른 노드를 선택했는지 확인할 수 있습니다.

1. Review selection(검토 선택) 페이지에서 Summary(요약)를 검토합니다. Summary(요약)는 재부팅될 노드 수와 모든 노드가 재부팅될 것으로 예상되는 총 시간을 나타냅니다.
2. 선택적으로 재부팅 목록에서 특정 노드를 제거하려면 * Remove * 를 선택합니다.
3. 노드를 추가하려면 * 이전 단계 * 를 선택하고 추가 노드를 선택한 다음 * 선택 검토 * 를 선택합니다.
4. 선택한 모든 노드에 대해 롤링 재부팅 절차를 시작할 준비가 되면 * 노드 재부팅 * 을 선택합니다.
5. 기본 관리자 노드를 재부팅하도록 선택한 경우 정보 메시지를 읽고 * 예 * 를 선택합니다.

   기본 관리자 노드가 마지막 재부팅 노드가 됩니다. 이 노드가 재부팅되는 동안 브라우저의 연결이 끊어집니다. 기본 관리자 노드를 다시 사용할 수 있게 되면 롤링 재부팅 페이지를 다시 로드해야 합니다.

롤링 재부팅을 모니터링합니다

롤링 재부팅 절차가 실행되는 동안 기본 관리자 노드에서 모니터링할 수 있습니다.

단계

1. 다음 정보가 포함된 작업의 전반적인 진행 상황을 검토합니다.
   - 재부팅된 노드 수입니다
   - 재부팅 프로세스 중인 노드 수입니다
   - 재부팅될 남아 있는 노드 수입니다

2. 각 노드 유형에 대한 표를 검토합니다.

   이 표에는 각 노드에서의 작업 진행 표시줄이 표시되며 해당 노드의 재부팅 단계는 다음 중 하나입니다.

   - 재부팅을 기다리는 중입니다
   - 서비스를 중지하는 중입니다
   - 시스템을 재부팅하는 중입니다
   - 서비스를 시작하는 중입니다
   - 재부팅이 완료되었습니다

롤링 재부팅 절차를 중지합니다

기본 관리자 노드에서 롤링 재부팅 절차를 중지할 수 있습니다. 절차를 중지하면 "서비스 중지 중", "시스템 재부팅" 또는 "서비스 시작" 상태의 모든 노드에서 재부팅 작업이 완료됩니다. 그러나 이러한 노드는 더 이상 절차의 일부로 추적되지 않습니다.

단계

1. maintenance * > * 작업 * > * 롤링 재부팅 * 을 선택합니다.
2. 모니터 재부팅 * 단계에서 * 재부팅 중지 절차 * 를 선택합니다.

작업 탭에서 그리드 노드를 재부팅합니다

노드 페이지의 작업 탭에서 개별 그리드 노드를 재부팅할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.
- 프로비저닝 암호가 있습니다.
- 기본 관리자 노드 또는 스토리지 노드를 재부팅하는 경우 다음 사항을 검토했습니다.
  - 기본 관리자 노드를 재부팅하면 브라우저에서 그리드 관리자에 대한 액세스가 일시적으로 중단됩니다.
  - 특정 사이트에서 두 개 이상의 스토리지 노드를 재부팅하면 재부팅 기간 동안 특정 객체에 액세스하지 못할 수 있습니다. 이 문제는 ILM 규칙이 * Dual commit * 수집 옵션을 사용하는 경우(또는 규칙이 * Balanced * 를 지정하고 필요한 모든 복제본을 즉시 생성할 수 없는 경우) 발생할 수 있습니다. 이 경우 StorageGRID는 새로 수집된 오브젝트를 동일한 사이트에 있는 두 스토리지 노드에 커밋하고 나중에 ILM을 평가합니다.
  - 스토리지 노드가 재부팅되는 동안 모든 개체에 액세스할 수 있도록 노드를 재부팅하기 전에 약 1시간 동안 사이트에서 객체 인제스트를 중지하십시오.

이 작업에 대해

StorageGRID가 그리드 노드를 재부팅하면 노드에서 명령을 발행하여 `reboot` 노드가 종료되고 재시작됩니다. 모든 서비스가 자동으로 다시 시작됩니다.

- VMware 노드를 재부팅하면 가상 머신이 재부팅됩니다.
- Linux 노드를 재부팅하면 컨테이너가 재부팅됩니다.
- StorageGRID 어플라이언스 노드를 재부팅하면 컴퓨팅 컨트롤러가 재부팅됩니다.

둘 이상의 노드를 재부팅해야 하는 경우 를 사용할 수 있습니다"롤링 재부팅 절차".

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 선택합니다.
6. 노드가 재부팅될 때까지 기다립니다.

   서비스가 종료되는 데 약간의 시간이 걸릴 수 있습니다.

   노드가 재부팅 중인 경우 Nodes 페이지의 노드에 대해 회색 (Administrative Down) 아이콘이 나타납니다. 모든 서비스가 다시 시작되고 노드가 그리드에 성공적으로 연결되면 노드 페이지에 일반 상태(노드 이름 왼쪽에 아이콘 없음)가 표시되어야 하며, 이는 알림이 활성화되지 않고 노드가 그리드에 연결되어 있음을 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.

시작하기 전에

`Passwords.txt`파일이 있습니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

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 재부팅합니다. `reboot`

4. 명령 셸에서 로그아웃합니다. `exit`

그리드 노드를 종료합니다

노드의 명령 셸에서 그리드 노드를 종료할 수 있습니다.

시작하기 전에

- `Passwords.txt`파일이 있습니다.

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), StorageGRID은 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. 을 "ILM을 사용하여 개체를 관리합니다"참조하십시오.

단계

1. 그리드 노드에 로그인합니다.

   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

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 명령을 실행합니다. `shutdown -h now`

   명령 결과에 관계없이 이 단계를 `service servermanager stop` 수행합니다.

어플라이언스 노드에서 명령을 실행한 후에는 `shutdown -h now` 어플라이언스의 전원을 껐다가 켜서 노드를 다시 시작해야 합니다.

제품의 경우, 이 명령은 컨트롤러를 종료하지만 제품의 전원은 계속 켜져 있습니다. 다음 단계를 완료해야 합니다.

4. 어플라이언스 노드의 전원을 끄는 경우 어플라이언스 단계를 따르십시오.

SG6160

a. SG6100-CN 스토리지 컨트롤러의 전원을 끕니다.

b. SG6100-CN 스토리지 컨트롤러의 파란색 전원 LED가 꺼질 때까지 기다립니다.

SGF6112를 참조하십시오

a. 제품의 전원을 끕니다.

b. 파란색 전원 LED가 꺼질 때까지 기다립니다.

SG6000 을 참조하십시오

a. 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.

b. 제품의 전원을 끄고 파란색 전원 LED가 꺼질 때까지 기다리십시오.

SG5800을 참조하십시오

a. 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.

b. SANtricity 시스템 관리자의 홈 페이지에서 * 진행 중인 작업 보기 * 를 선택합니다.

c. 다음 단계를 계속하기 전에 모든 작업이 완료되었는지 확인하십시오.

d. 컨트롤러 쉘프의 두 전원 스위치를 끄고 컨트롤러 쉘프의 모든 LED가 꺼질 때까지 기다립니다.

SG5700입니다

a. 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.

b. 제품의 전원을 끄고 모든 LED 및 7세그먼트 디스플레이 작동이 멈출 때까지 기다리십시오.

SG100 또는 **SG1000**

a. 제품의 전원을 끕니다.

b. 파란색 전원 LED가 꺼질 때까지 기다립니다.

호스트의 전원을 끄기 전에 해당 호스트의 모든 그리드 노드에서 서비스를 중지해야 합니다.

단계

1. 그리드 노드에 로그인합니다.

   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 노드에서 실행 중인 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. 호스트의 각 노드에 대해 1단계와 2단계를 반복합니다.

4. Linux 호스트가 있는 경우:

   a. 호스트 운영 체제에 로그인합니다.

   b. 노드를 중지합니다. `storagegrid node stop`

   c. 호스트 운영 체제를 종료합니다.

5. 노드가 VMware 가상 머신에서 실행 중이거나 어플라이언스 노드인 경우 shutdown 명령을 실행합니다. `shutdown -h now`

   명령 결과에 관계없이 이 단계를 `service servermanager stop` 수행합니다.

   > ⓘ 어플라이언스 노드에서 명령을 실행한 후에는 `shutdown -h now` 어플라이언스의 전원을 껐다가 켜서 노드를 다시 시작해야 합니다.

   제품의 경우, 이 명령은 컨트롤러를 종료하지만 제품의 전원은 계속 켜져 있습니다. 다음 단계를 완료해야 합니다.

6. 어플라이언스 노드의 전원을 끄는 경우 어플라이언스 단계를 따르십시오.

SG6160

a. SG6100-CN 스토리지 컨트롤러의 전원을 끕니다.

b. SG6100-CN 스토리지 컨트롤러의 파란색 전원 LED가 꺼질 때까지 기다립니다.

SGF6112를 참조하십시오

a. 제품의 전원을 끕니다.

b. 파란색 전원 LED가 꺼질 때까지 기다립니다.

SG6000 을 참조하십시오

a. 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.

b. 제품의 전원을 끄고 파란색 전원 LED가 꺼질 때까지 기다리십시오.

SG5800을 참조하십시오

a. 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.

b. SANtricity 시스템 관리자의 홈 페이지에서 * 진행 중인 작업 보기 * 를 선택합니다.

c. 다음 단계를 계속하기 전에 모든 작업이 완료되었는지 확인하십시오.

d. 컨트롤러 쉘프의 두 전원 스위치를 끄고 컨트롤러 쉘프의 모든 LED가 꺼질 때까지 기다립니다.

SG5700입니다

a. 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.

b. 제품의 전원을 끄고 모든 LED 및 7세그먼트 디스플레이 작동이 멈출 때까지 기다리십시오.

SG110 또는 **SG1100**

a. 제품의 전원을 끕니다.

b. 파란색 전원 LED가 꺼질 때까지 기다립니다.

SG100 또는 **SG1000**

a. 제품의 전원을 끕니다.

b. 파란색 전원 LED가 꺼질 때까지 기다립니다.

7. 명령 셸에서 로그아웃합니다. `exit`

관련 정보

- "SGF6112 및 SG6160 스토리지 어플라이언스"
- "SG6000 스토리지 어플라이언스"
- "SG5700 스토리지 어플라이언스"
- "SG5800 스토리지 어플라이언스"
- "SG110 및 SG1100 서비스 어플라이언스"
- "SG100 및 SG1000 서비스 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 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 그리드의 기능이나 가용성에 영향을 주지 않고 호스트 유지 관리를 수행할 수 "Linux 호스트 간에 노드를 마이그레이션합니다"있습니다.

단계

1. 모든 클라이언트 응용 프로그램이 그리드에 액세스하는 것을 중지합니다.
2. [[log_in_to_gn] 각 게이트웨이 노드에 로그인:
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.
3. 노드에서 실행 중인 모든 서비스를 중지합니다. `service servermanager stop`

서비스를 종료하는 데 최대 15분이 걸릴 수 있으며, 종료 프로세스를 모니터링하기 위해 시스템에 원격으로 로그인하기를 원할 수 있습니다.

4. 위의 두 단계를 반복하여 모든 스토리지 노드 및 비기본 관리 노드에서 서비스를 중지합니다.

   이러한 노드의 서비스는 순서에 관계없이 중지할 수 있습니다.

   > ⓘ 어플라이언스 스토리지 노드에서 서비스를 중지하는 명령을 실행하는 경우 `service servermanager stop` 어플라이언스 전원을 껐다가 켜서 노드를 다시 시작해야 합니다.

5. 기본 관리자 노드에 대해 및 의 단계를 노드에 로그인합니다노드에서 모든 서비스를 중지하는 중입니다반복합니다.

6. Linux 호스트에서 실행 중인 노드의 경우:

   a. 호스트 운영 체제에 로그인합니다.

   b. 노드를 중지합니다. `storagegrid node stop`

   c. 호스트 운영 체제를 종료합니다.

7. VMware 가상 머신 및 어플라이언스 스토리지 노드에서 실행 중인 노드의 경우 shutdown 명령을 실행합니다. `shutdown -h now`

   명령 결과에 관계없이 이 단계를 `service servermanager stop` 수행합니다.

   어플라이언스의 경우 이 명령은 컴퓨팅 컨트롤러를 종료하지만 어플라이언스 전원은 여전히 켜져 있습니다. 다음 단계를 완료해야 합니다.

8. 어플라이언스 노드가 있는 경우 어플라이언스 단계를 따릅니다.

SG110 또는 **SG1100**

a. 제품의 전원을 끕니다.

b. 파란색 전원 LED가 꺼질 때까지 기다립니다.

SG100 또는 **SG1000**

a. 제품의 전원을 끕니다.

b. 파란색 전원 LED가 꺼질 때까지 기다립니다.

SG6160

a. SG6100-CN 스토리지 컨트롤러의 전원을 끕니다.

b. SG6100-CN 스토리지 컨트롤러의 파란색 전원 LED가 꺼질 때까지 기다립니다.

SGF6112를 참조하십시오

a. 제품의 전원을 끕니다.

b. 파란색 전원 LED가 꺼질 때까지 기다립니다.

SG6000 을 참조하십시오

a. 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.

b. 제품의 전원을 끄고 파란색 전원 LED가 꺼질 때까지 기다리십시오.

SG5800을 참조하십시오

a. 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.

b. SANtricity 시스템 관리자의 홈 페이지에서 * 진행 중인 작업 보기 * 를 선택합니다.

c. 다음 단계를 계속하기 전에 모든 작업이 완료되었는지 확인하십시오.

d. 컨트롤러 쉘프의 두 전원 스위치를 끄고 컨트롤러 쉘프의 모든 LED가 꺼질 때까지 기다립니다.

SG5700입니다

a. 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.

b. 제품의 전원을 끄고 모든 LED 및 7세그먼트 디스플레이 작동이 멈출 때까지 기다리십시오.

9. 필요한 경우 명령 셸에서 로그아웃합니다. `exit`

   StorageGRID 그리드가 이제 종료되었습니다.

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.

가능한 경우 다음 순서대로 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 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.

관련 정보

- "SGF6112 및 SG6160 스토리지 어플라이언스"
- "SG110 및 SG1100 서비스 어플라이언스"
- "SG100 및 SG1000 서비스 어플라이언스"
- "SG6000 스토리지 어플라이언스"
- "SG5800 스토리지 어플라이언스"
- "SG5700 스토리지 어플라이언스"

포트 재매핑 절차

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 끝점 구성에 대한 자세한 내용은 을 "부하 분산 장치 엔드포인트 구성"참조하십시오.

> 포트 재매핑이 클라이언트 액세스를 제공하는 경우 서비스 손실을 방지하기 위해 다른 포트를 로드 밸런서 끝점으로 사용하도록 클라이언트를 다시 구성합니다. 그렇지 않으면 포트 매핑을 제거하면 클라이언트 액세스가 손실되며 적절하게 예약되어야 합니다.

> 베어 메탈 호스트에 컨테이너로 배포된 StorageGRID 시스템에서는 이 절차를 사용할 수 없습니다. 의 지침을 "베어 메탈 호스트에서 포트 리맵을 제거합니다"참조하십시오.

단계

1. 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh -p 8022 admin@node_IP`

      포트 8022는 기본 OS의 SSH 포트이고, 포트 22는 StorageGRID를 실행하는 컨테이너 엔진의 SSH 포트입니다.

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 다음 스크립트를 실행합니다. `remove-port-remap.sh`
3. 노드를 재부팅합니다. `reboot`
4. 명령 셸에서 로그아웃합니다. `exit`
5. 재매핑된 포트가 충돌하는 각 관리 노드와 게이트웨이 노드에서 이 단계를 반복합니다.

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.

이 작업에 대해

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 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. 다음 명령을 실행하여 노드를 일시적으로 사용하지 않도록 설정합니다. `sudo storagegrid node stop node-name`
3. vim 또는 pico와 같은 텍스트 편집기를 사용하여 노드의 노드 구성 파일을 편집합니다.

   노드 구성 파일은 에서 찾을 수 `/etc/storagegrid/nodes/node-name.conf` 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 내용을 검증합니다. `sudo storagegrid node validate node-name`

   다음 단계로 진행하기 전에 오류 또는 경고를 모두 해결하십시오.

7. 다음 명령을 실행하여 포트 재매핑 없이 노드를 다시 시작합니다. `sudo storagegrid node start node-name`
8. 파일에 나열된 암호를 사용하여 노드에 admin으로 `Passwords.txt` 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.

네트워크 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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.
- 프로비저닝 암호가 있습니다.
- 구성할 서브넷의 네트워크 주소(CIDR 표기법)가 있습니다.

이 작업에 대해

새 서브넷 추가를 포함하는 확장 작업을 수행하는 경우 확장 절차를 시작하기 전에 그리드 네트워크 서브넷 목록에 새 서브넷을 추가해야 합니다. 그렇지 않으면 확장을 취소하고 새 서브넷을 추가한 다음 확장을 다시 시작해야 합니다.

서브넷을 추가합니다

단계

1. 유지보수 * > * 네트워크 * > * 그리드 네트워크 * 를 선택합니다.
2. CIDR 표시법으로 새 서브넷을 추가하려면 * 다른 서브넷 추가 * 를 선택합니다.

   예를 들어, 을 `10.96.104.0/22`입력합니다.

3. 프로비저닝 암호를 입력하고 * Save * 를 선택합니다.
4. 변경 사항이 적용될 때까지 기다린 다음 새 복구 패키지를 다운로드합니다.
   a. 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
   b. Provisioning Passphrase * 를 입력합니다.

> 복구 패키지 파일은 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 보안을 유지해야 합니다. 또한 기본 관리 노드를 복구하는 데 사용됩니다.

지정한 서브넷은 StorageGRID 시스템에 대해 자동으로 구성됩니다.

서브넷을 편집합니다

단계

1. 유지보수 * > * 네트워크 * > * 그리드 네트워크 * 를 선택합니다.
2. 편집할 서브넷을 선택하고 필요한 내용을 변경합니다.
3. 프로비저닝 암호를 입력하고 * Save * 를 선택합니다.
4. 확인 대화 상자에서 * 예 * 를 선택합니다.
5. 변경 사항이 적용될 때까지 기다린 다음 새 복구 패키지를 다운로드합니다.
   a. 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
   b. Provisioning Passphrase * 를 입력합니다.

서브넷을 삭제합니다

단계

1. 유지보수 * > * 네트워크 * > * 그리드 네트워크 * 를 선택합니다.
2. 서브넷 옆의 삭제 아이콘을 선택합니다.
3. 프로비저닝 암호를 입력하고 * Save * 를 선택합니다.
4. 확인 대화 상자에서 * 예 * 를 선택합니다.
5. 변경 사항이 적용될 때까지 기다린 다음 새 복구 패키지를 다운로드합니다.
   a. 유지보수 * > * 시스템 * > * 복구 패키지 * 를 선택합니다.
   b. Provisioning Passphrase * 를 입력합니다.

IP 주소를 구성합니다

IP 주소 지침

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.

IP 변경 절차는 중단 절차가 될 수 있습니다. 새 구성이 적용될 때까지 그리드의 부분을 사용할 수 없습니다.

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.

그리드에 있는 모든 노드의 그리드 네트워크 IP 주소를 변경하려면 를 "그리드 전체의 변경 특수 절차 "사용합니다.

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.

DHCP를 선택합니다

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 인터페이스에 구성된 HA 그룹에 할당된 기존 가상 IP 주소의 값으로 클라이언트 네트워크 IP 주소를 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.

시작하기 전에

`Passwords.txt`파일이 있습니다.

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.

- "Red Hat Enterprise Linux에 StorageGRID를 설치합니다"
- "Ubuntu 또는 Debian에 StorageGRID를 설치합니다"
- 어플라이언스: * StorageGRID 어플라이언스의 경우 초기 설치 중에 StorageGRID 어플라이언스 설치 프로그램에 클라이언트 또는 관리자 네트워크가 구성되어 있지 않으면 IP 변경 도구만 사용하여 네트워크를 추가할 수 없습니다. 먼저 링크를 구성하고 어플라이언스를 정상 작동 모드로 되돌린 다음 IP 변경 도구를 사용하여 네트워크 구성을 수정해야 "제품을 유지보수 모드로 두십시오" 합니다. 를 "네트워크 링크 구성 절차"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. 의 지침을 "SSO를 구성하는 중입니다"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. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`

b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

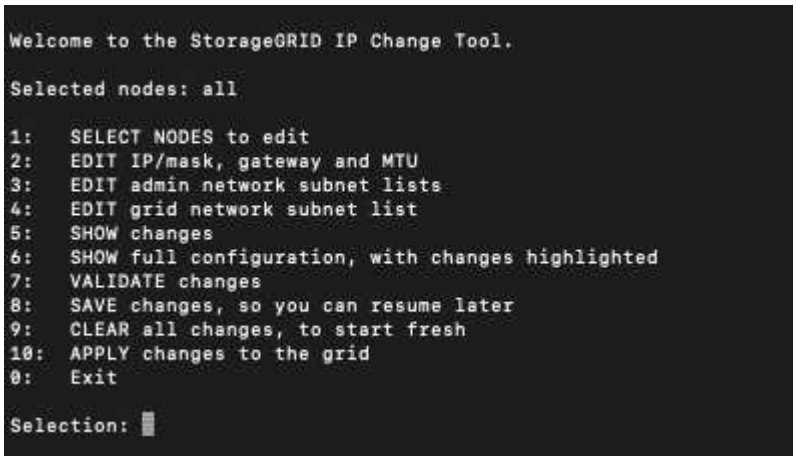
c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 다음 명령을 입력하여 IP 변경 도구를 시작합니다. `change-ip`
3. 프롬프트에 프로비저닝 암호를 입력합니다.

기본 메뉴가 나타납니다.



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

선택한 후 프롬프트에 노드 이름, 네트워크 이름(그리드, 관리 또는 클라이언트), 데이터 유형(IP/마스크,

게이트웨이 또는 MTU)와 현재 값

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.

로 구성된 인터페이스는 `fixed` 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 형식이 인 경우 `IP/mask` * d * 또는 * 0.0.0.0/0 * 을 입력하여 노드에서 관리 또는 클라이언트 네트워크를 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.

이러한 검증을 통해 그리드, 관리자 및 클라이언트 네트워크에 대한 규칙(예: 중복되는 서브넷 사용 안 함)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. 유효성 검사를 통과한 후 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 스테이징하면 그리드 구성 변경의 결과로 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: 처음 노드를 관리 네트워크 또는 클라이언트 네트워크에 추가하는 경우 에 설명된 대로 인터페이스를 추가했는지 "Linux: 기존 노드에 인터페이스를 추가합니다"확인합니다.

    a. 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.

관리자 네트워크에서 서브넷 목록을 추가하거나 변경합니다

하나 이상의 노드의 관리 네트워크 서브넷 목록에서 서브넷을 추가, 삭제 또는 변경할 수 있습니다.

시작하기 전에

- `Passwords.txt`파일이 있습니다.

관리자 네트워크 서브넷 목록에 있는 모든 노드에 서브넷을 추가, 삭제 또는 변경할 수 있습니다.

단계

1. 기본 관리자 노드에 로그인합니다.

    a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`

    b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

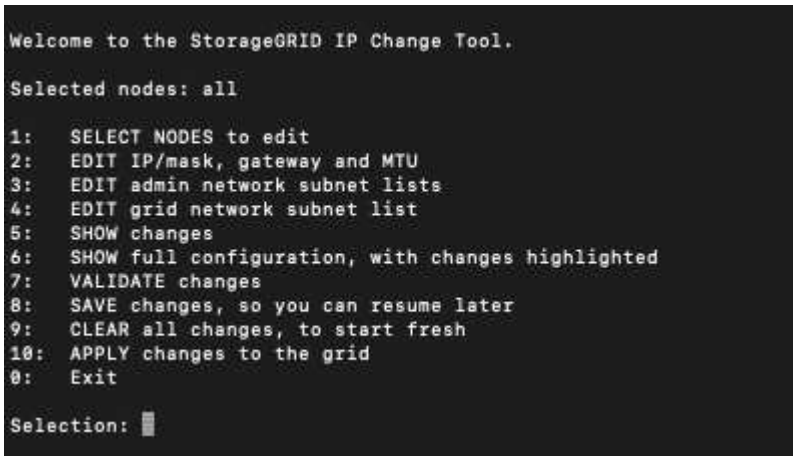
    c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

    d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

    루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 다음 명령을 입력하여 IP 변경 도구를 시작합니다. `change-ip`
3. 프롬프트에 프로비저닝 암호를 입력합니다.

   기본 메뉴가 나타납니다.



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.
   - 다음 명령을 입력하여 서브넷을 추가합니다. `add CIDR`
   - 다음 명령을 입력하여 서브넷을 삭제합니다. `del CIDR`
   - 다음 명령을 입력하여 서브넷 목록을 설정합니다. `set CIDR`

   모든 명령에 대해 다음 형식을 사용하여 여러 주소를 입력할 수 있습니다. `add CIDR, CIDR`

   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 불러와서 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 "All" 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 aren't
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
aren't 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 don't 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 다음 예제 출력에 표시된 것처럼 업데이트가 적용되면 출력에 상태가 표시됩니다.

```
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.

그리드 네트워크에서 서브넷 목록을 추가하거나 변경합니다

IP 변경 도구를 사용하여 그리드 네트워크에 서브넷을 추가하거나 변경할 수 있습니다.

시작하기 전에

- `Passwords.txt`파일이 있습니다.

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. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 다음 명령을 입력하여 IP 변경 도구를 시작합니다. `change-ip`

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.

- 다음 명령을 입력하여 서브넷을 추가합니다. `add CIDR`
- 다음 명령을 입력하여 서브넷을 삭제합니다. `del CIDR`
- 다음 명령을 입력하여 서브넷 목록을 설정합니다. `set CIDR`

> ⓘ 모든 명령에 대해 다음 형식을 사용하여 여러 주소를 입력할 수 있습니다. `add CIDR, CIDR`

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 불러와서 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 다음 예제 출력에 표시된 것처럼 업데이트가 적용되면 출력에 상태가 표시됩니다.

      ```
      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 시작하십시오.

    - * 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 스테이징하면 그리드 구성 변경의 결과로 새 복구 패키지가 생성됩니다.

12. 오류로 인해 구성을 중지할 경우 다음 옵션을 사용할 수 있습니다.
    - IP 변경 절차를 종료하고 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.

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 사용하면 그리드 전체의 그리드 네트워크 IP를 변경할 수 없습니다.

시작하기 전에

- `Passwords.txt`파일이 있습니다.

그리드가 성공적으로 시작되도록 하려면 모든 변경 사항을 동시에 수행해야 합니다.

이 절차는 그리드 네트워크에만 적용됩니다. 이 절차를 사용하여 관리 또는 클라이언트 네트워크의 IP 주소를 변경할 수 없습니다.

한 사이트에서만 노드의 IP 주소와 MTU를 변경하려면 "노드 네트워크 구성을 변경합니다"지침을 따릅니다.

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.

새 IP 주소의 그리드에서 기존 NTP 서버에 액세스할 수 없는 경우 IP 변경 절차를 수행하기 전에 새 NTP 서버를 추가합니다.

새 IP 주소의 그리드에서 기존 DNS 서버에 액세스할 수 없는 경우 IP 변경 절차를 수행하기 전에 새 DNS 서버를 추가합니다.

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 을 "Single Sign-On 구성"참조하십시오.

필요한 경우 새 IP 주소에 대한 새 서브넷을 추가합니다.

2. 기본 관리자 노드에 로그인합니다.

   a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

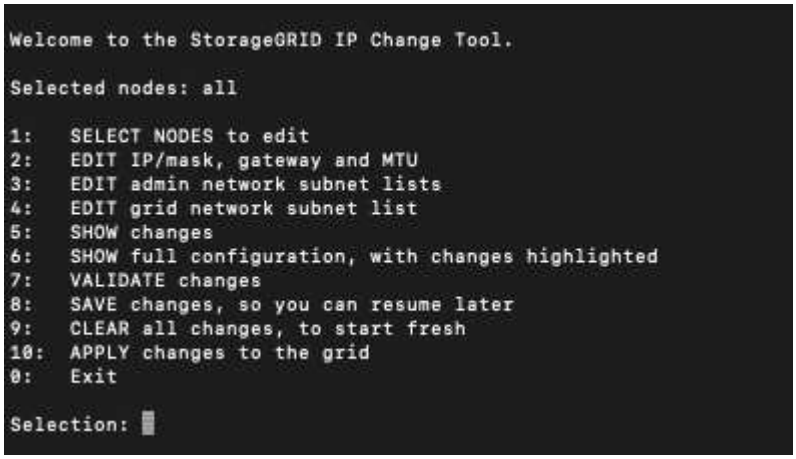
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

3. 다음 명령을 입력하여 IP 변경 도구를 시작합니다. `change-ip`

4. 프롬프트에 프로비저닝 암호를 입력합니다.

   기본 메뉴가 나타납니다. 기본적으로 `Selected nodes` 이 필드는 로 설정되어 `all` 있습니다.



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.

   로 구성된 인터페이스는 `fixed` 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 통과한 후 * 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 종료해야 합니다.

12. 필요한 물리적 또는 가상 네트워킹을 변경합니다.
13. 모든 그리드 노드가 다운되었는지 확인합니다.
14. 모든 노드의 전원을 켭니다.
15. 그리드가 성공적으로 시작된 후:
    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

- "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 Linux에 StorageGRID를 설치합니다"
- "Ubuntu 또는 Debian에 StorageGRID를 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 "노드 네트워크 구성을 변경합니다"참조하십시오.

단계

1. 노드를 호스팅하는 Linux 서버에 로그인합니다.
2. 노드 구성 파일을 편집합니다 `/etc/storagegrid/nodes/node-name.conf`.

   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.

시작하기 전에

- Linux 플랫폼에 StorageGRID를 설치하는 지침을 액세스할 수 있습니다.
  - "Red Hat Enterprise Linux에 StorageGRID를 설치합니다"
  - "Ubuntu 또는 Debian에 StorageGRID를 설치합니다"
- `Passwords.txt`파일이 있습니다.
- 있습니다. "특정 액세스 권한"

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.

   `INTERFACE_TARGET_nnnn=value`

   _nnnn_의 경우 추가할 각 항목에 대해 고유한 번호를 `INTERFACE_TARGET` 지정하십시오.

   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.

   `INTERFACE_TARGET_0001=ens256, Trunk`

   > 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

- 트렁크 인터페이스를 하나 이상 추가한 경우 로 "VLAN 인터페이스를 구성합니다" 이동하여 각 새 상위 인터페이스에 대해 하나 이상의 VLAN 인터페이스를 구성합니다.
- 하나 이상의 액세스 인터페이스를 추가한 경우, 로 "고가용성 그룹을 구성합니다" 이동하여 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.

시작하기 전에

- 의 지침에 액세스할 수 "VMware 플랫폼에 StorageGRID 설치"있습니다.
- 관리 노드 및 게이트웨이 노드 VMware 가상 시스템이 있습니다.

- 그리드, 관리자 또는 클라이언트 네트워크로 사용되지 않는 네트워크 서브넷이 있습니다.
- `Passwords.txt`파일이 있습니다.
- 있습니다. "특정 액세스 권한"

> 소프트웨어 업그레이드, 복구 절차 또는 확장 절차가 활성 상태인 동안에는 노드에 인터페이스를 추가하지 마십시오.

이 작업에 대해

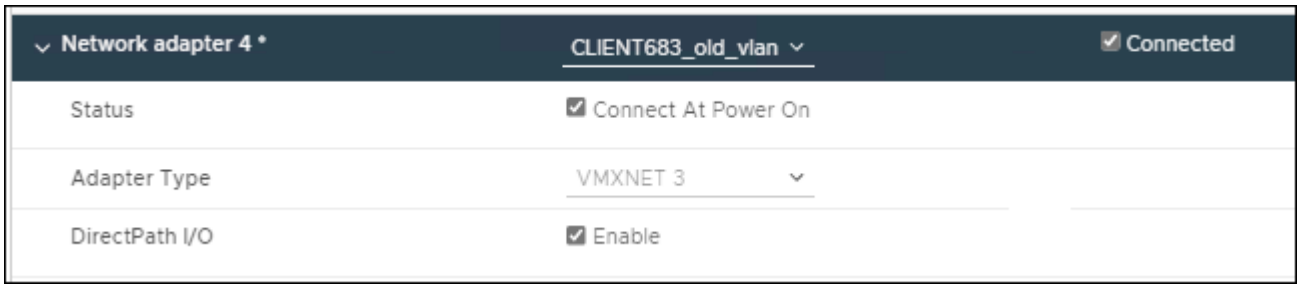
노드를 설치한 후 VMware 노드에 인터페이스를 하나 이상 추가하려면 다음 단계를 수행합니다. 예를 들어, 관리 또는 게이트웨이 노드에 트렁크 인터페이스를 추가하여 VLAN 인터페이스를 사용하여 다른 애플리케이션이나 테넌트에 속한 트래픽을 분리할 수 있습니다. 또는 고가용성(HA) 그룹에서 사용할 액세스 인터페이스를 추가할 수도 있습니다.

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. 를 사용하여 `ip link show` 새 네트워크 인터페이스 ens256이 감지되는지 확인합니다.

```
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

- 트렁크 인터페이스를 하나 이상 추가한 경우 로 "VLAN 인터페이스를 구성합니다" 이동하여 각 새 상위 인터페이스에 대해 하나 이상의 VLAN 인터페이스를 구성합니다.
- 하나 이상의 액세스 인터페이스를 추가한 경우, 로 "고가용성 그룹을 구성합니다" 이동하여 새 인터페이스를 HA 그룹에 직접 추가합니다.

DNS 서버를 구성합니다

DNS 서버를 추가, 업데이트 및 제거하여 IP 주소 대신 FQDN(정규화된 도메인 이름) 호스트 이름을 사용할 수 있습니다.

외부 대상의 호스트 이름을 지정할 때 IP 주소 대신 FQDN(정규화된 도메인 이름)을 사용하려면 사용할 각 DNS 서버의 IP 주소를 지정합니다. 이러한 항목은 AutoSupport, 경고 이메일, SNMP 알림, 플랫폼 서비스 엔드포인트, 클라우드 스토리지 풀, 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.
- 구성할 DNS 서버의 IP 주소가 있습니다.

이 작업에 대해

제대로 작동하려면 DNS 서버를 두 대 또는 세 대 지정합니다. 3개 이상을 지정하면 일부 플랫폼의 알려진 OS 제한 때문에 3개만 사용할 수 있습니다. 사용자 환경에 라우팅 제한이 있는 경우 개별 노드(일반적으로 사이트의 모든 노드)에서 최대 3개의 DNS 서버로 구성된 다른 세트를 사용할 수 "DNS 서버 목록을 사용자 지정합니다"있습니다.

가능한 경우 각 사이트에서 로컬로 액세스할 수 있는 DNS 서버를 사용하여 isfan 사이트가 외부 대상의 FQDN을 확인할 수 있도록 합니다.

DNS 서버를 추가합니다

DNS 서버를 추가하려면 다음 단계를 수행하십시오.

단계

1. 유지보수 * > * 네트워크 * > * DNS 서버 * 를 선택합니다.
2. DNS 서버를 추가하려면 * 다른 서버 추가 * 를 선택합니다.
3. 저장 * 을 선택합니다.

DNS 서버를 수정합니다

DNS 서버를 수정하려면 다음 단계를 수행하십시오.

단계

1. 유지보수 * > * 네트워크 * > * DNS 서버 * 를 선택합니다.
2. 편집할 서버 이름의 IP 주소를 선택하고 필요한 내용을 변경합니다.
3. 저장 * 을 선택합니다.

DNS 서버를 삭제합니다

DNS 서버의 IP 주소를 삭제하려면 다음 단계를 수행하십시오.

단계

1. 유지보수 * > * 네트워크 * > * DNS 서버 * 를 선택합니다.
2. IP 주소 옆에 있는 삭제 아이콘을 선택합니다.
3. 저장 * 을 선택합니다.

단일 그리드 노드에 대한 **DNS** 구성을 수정합니다

전체 배포에 대해 DNS를 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.

단계

1. 기본 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

   e. SSH 에이전트에 SSH 개인 키를 추가합니다. 다음을 입력합니다. `ssh-add`

f. 파일에 나열된 SSH 액세스 암호를 `Passwords.txt` 입력합니다.

2. 사용자 지정 DNS 구성으로 업데이트할 노드에 로그인합니다. `ssh *node_IP_address*`

3. DNS 설정 스크립트를 실행합니다. `setup_resolv.rb.`

   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. 네트워크에 도메인 이름 서비스를 제공하는 서버의 IPv4 주소를 추가합니다. `add <nameserver IP_address>`

5. 명령을 반복하여 `add nameserver` 이름 서버를 추가합니다.

6. 다른 명령을 묻는 메시지가 나타나면 지침을 따릅니다.
7. 변경 사항을 저장하고 응용 프로그램을 종료합니다. `save`
8. 서버에서 명령 셸을 닫습니다. `exit`
9. 각 그리드 노드에 대해 ~ 단계를 노드에 로그인합니다명령 셸을 닫습니다반복합니다.
10. 다른 서버에 대한 암호 없는 액세스가 더 이상 필요하지 않으면 SSH 에이전트에서 개인 키를 제거합니다. 다음을 입력합니다. `ssh-add -D`

NTP 서버를 관리합니다

StorageGRID 시스템의 그리드 노드 간에 데이터가 정확하게 동기화되도록 NTP(네트워크 시간 프로토콜) 서버를 추가, 업데이트 또는 제거할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.
- 프로비저닝 암호가 있습니다.
- 구성할 NTP 서버의 IPv4 주소가 있습니다.

StorageGRID에서 NTP를 사용하는 방법

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 역할을 가진 노드를 두 개 이상 지정하는 것이 좋습니다.

NTP 서버 지침

타이밍 문제로부터 보호하려면 다음 지침을 따르십시오.

- 외부 NTP 서버는 이전에 기본 NTP 역할을 할당한 노드에 연결됩니다. 따라서 주 NTP 역할을 가진 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 StorageGRID를 비롯한 정확도가 높은 환경에서 사용할 수 있도록 Microsoft에서 지원되지 않습니다. 자세한 내용은 을 참조하십시오 "정확도가 높은 환경에 대한 Windows 시간 서비스를 구성하기 위한 경계를 지원합니다".

NTP 서버를 구성합니다

다음 단계에 따라 NTP 서버를 추가, 업데이트 또는 제거합니다.

단계

1. 유지보수 * > * 네트워크 * > * NTP 서버 * 를 선택합니다.
2. Servers 섹션에서 필요에 따라 NTP 서버 항목을 추가, 업데이트 또는 제거합니다.

   NTP 서버는 4개 이상 포함해야 하며 최대 6개의 서버를 지정할 수 있습니다.

3. StorageGRID 시스템의 프로비저닝 암호를 입력하고 * Save * 를 선택합니다.

   구성 업데이트가 완료될 때까지 페이지가 비활성화됩니다.

   새 NTP 서버를 저장한 후 모든 NTP 서버가 연결 테스트에 실패하면 계속 진행하지 마십시오. 기술 지원 부서에 문의하십시오.

NTP 서버 문제를 해결합니다

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.

격리된 노드의 네트워크 연결을 복구합니다

특정 상황에서는 하나 이상의 노드 그룹이 그리드의 나머지 부분과 접촉하지 못할 수 있습니다. 예를 들어 사이트 또는 그리드 전체 IP 주소를 변경하면 노드가 격리될 수 있습니다.

이 작업에 대해

노드 격리는 다음과 같이 표시됩니다.

- 노드와 통신할 수 없음 * (* 경고 * > * 현재 *)
- 연결 관련 진단(* 지원 * > * 툴 * > * 진단 *)

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 사용할 수 없는 경우 격리된 각 노드에서 명령줄 유틸리티를 실행해야 할 수 있습니다.

단계

일부 서비스만 오프라인 상태이거나 통신 오류를 보고하는 경우에는 이 절차가 적용되지 않습니다.

1. 노드에 액세스하여 `/var/local/log/dynip.log` 격리 메시지를 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 might be required.
   ```

   VMware 콘솔을 사용 중인 경우 노드를 격리할 수 있다는 메시지가 표시됩니다.

   Linux 배포에서는 격리 메시지가 `/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.
   - 명령을 실행한 후 동적 IP 서비스의 상태가 "실행 중" `storagegrid-status`입니다.
   - 노드 페이지에서 노드가 더 이상 그리드의 나머지 부분과 연결되지 않은 상태로 표시되지 않습니다.

명령을 실행해도 문제가 해결되지 않으면 `add_node_ip.py` 해결해야 하는 다른 네트워킹 문제가 있을 수 있습니다.

호스트 및 미들웨어 절차

Linux: 그리드 노드를 새 호스트로 마이그레이션

한 Linux 호스트(*source host*)에서 다른 Linux 호스트(*target host*)로 하나 이상의 StorageGRID 노드를 마이그레이션하여 그리드의 기능이나 가용성에 영향을 주지 않고 호스트 유지 관리를 수행할 수 있습니다.

예를 들어, OS 패치 및 재부팅을 수행하기 위해 노드를 마이그레이션할 수 있습니다.

시작하기 전에

- 마이그레이션 지원을 포함하도록 StorageGRID 배포를 계획했습니다.
  - "Red Hat Enterprise Linux의 노드 컨테이너 마이그레이션 요구 사항"
  - "Ubuntu 또는 Debian에 대한 노드 컨테이너 마이그레이션 요구 사항"
- 타겟 호스트가 이미 StorageGRID를 사용할 준비가 되었습니다.
- 공유 스토리지는 모든 노드별 스토리지 볼륨에 사용됩니다
- 네트워크 인터페이스는 호스트 간에 일관된 이름을 갖습니다.

> 운영 구축 환경에서는 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.

소스 호스트에서 노드를 내보냅니다

첫 번째 단계로 그리드 노드를 종료하고 소스 Linux 호스트에서 내보냅니다.

소스 호스트 _ 에서 다음 명령을 실행합니다.

단계

1. 소스 호스트에서 현재 실행 중인 모든 노드의 상태를 가져옵니다.

   ```
   sudo storagegrid node status all
   ```

   예제 출력:

   ```
   Name Config-State Run-State
   DC1-ADM1 Configured Running
   DC1-ARC1 Configured Running
   DC1-GW1 Configured Running
   DC1-S1 Configured Running
   DC1-S2 Configured Running
   DC1-S3 Configured Running
   ```

2. 마이그레이션할 노드의 이름을 식별하고 해당 Run-State가 실행 중인 경우 중지합니다.

```
sudo storagegrid node stop DC1-S3
```

예제 출력:

```
Stopping node DC1-S3
Waiting up to 630 seconds for node shutdown
```

3. 소스 호스트에서 노드를 내보냅니다.

```
sudo storagegrid node export DC1-S3
```

예제 출력:

```
Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.
Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you
want to import it again.
```

4. `import`출력에 표시되는 권장 명령을 기록합니다.

   다음 단계에서 타겟 호스트에서 이 명령을 실행합니다.

대상 호스트에서 노드를 가져옵니다

소스 호스트에서 노드를 내보낸 후 타겟 호스트에서 노드를 가져오고 유효성을 검사합니다. 검증에서 노드가 소스 호스트와 동일한 블록 스토리지 및 네트워크 인터페이스 디바이스를 액세스할 수 있는지 확인합니다.

타겟 host_에서 다음 명령을 실행합니다.

단계

1. 타겟 호스트에서 노드를 가져옵니다.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

예제 출력:

```
Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.
You should run 'storagegrid node validate DC1-S3'
```

2. 새 호스트에서 노드 구성을 검증합니다.

```
sudo storagegrid node validate DC1-S3
```

예제 출력:

```
Confirming existence of node DC1-S3... PASSED
Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node
DC1-S3... PASSED
Checking for duplication of unique values... PASSED
```

3. 유효성 검사 오류가 발생하면 마이그레이션된 노드를 시작하기 전에 이를 해결하십시오.

   문제 해결 정보는 Linux 운영 체제의 StorageGRID 설치 지침을 참조하십시오.

   - "Red Hat Enterprise Linux에 StorageGRID를 설치합니다"
   - "Ubuntu 또는 Debian에 StorageGRID를 설치합니다"

마이그레이션된 노드를 시작합니다

마이그레이션된 노드의 유효성을 검사한 후에는 _target host_에서 명령을 실행하여 노드를 시작합니다.

단계

1. 새 호스트에서 노드를 시작합니다.

   ```
   sudo storagegrid node start DC1-S3
   ```

2. Grid Manager에 로그인하여 노드 상태가 경보 없이 녹색인지 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.

3. Grid Manager에 액세스할 수 없는 경우 10분 정도 기다린 후 다음 명령을 실행합니다.

   ```
   sudo storagegrid node status _node-name
   ```

   마이그레이션된 노드에 실행 상태가 실행 중인지 확인합니다.

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.

노드 복구 또는 교체

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 복원하지 마십시오. 대신 각 노드 유형에 대한 복구 및 유지보수 절차를 참조하십시오.

전체 StorageGRID 사이트에 장애가 발생한 경우 기술 지원 팀에 문의하십시오. 기술 지원 부서는 고객과 협력하여 복구되는 데이터의 양을 최대화하고 비즈니스 목표를 충족하는 사이트 복구 계획을 개발하고 실행합니다. 을 "기술 지원 부서에서 사이트를 복구하는 방법"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.
- 그리드 노드에 장애가 발생하면 일상적인 작업의 효율성에 영향을 줄 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, 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 프로그램 버전은 에 설명된 대로 StorageGRID 시스템의 소프트웨어 버전과 "StorageGRID 어플라이언스 설치 프로그램 버전을 확인하고 업그레이드합니다" 일치합니다.
- 운영 관리 노드 이외의 그리드 노드를 복구하는 경우 복구되는 그리드 노드와 운영 관리 노드 사이에 연결이 있습니다.
- 어플라이언스 스토리지 노드를 복구하는 경우 어플라이언스 설치 중에 원래 어플라이언스와 동일한 스토리지 유형(결합, 메타데이터 전용 또는 데이터 전용)을 지정해야 합니다. 다른 스토리지 유형을 지정하면 복구가 실패하고 올바른 스토리지 유형으로 어플라이언스를 재설치해야 합니다.

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 플랫폼에 대해 를 수행해야 StorageGRID 설치 파일을 다운로드합니다합니다. • 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"
복구 패키지 `.zip` 파일	가장 최근의 복구 패키지 파일 복사본 가져오기 `.zip`: `sgws-recovery-package-`*`id-revision`*`.zip` 파일 내용은 `.zip` 시스템이 수정될 때마다 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 검토합니다. `/var/local/install/sgws-recovery-package-`*`grid-id-revision`*`.zip.gpg` 가장 높은 수정 번호가 있는 복구 패키지를 사용합니다.
`Passwords.txt` 파일	명령줄에서 그리드 노드에 액세스하는 데 필요한 암호를 포함합니다. 복구 패키지에 포함되어 있습니다.

항목	참고
프로비저닝 암호	StorageGRID 시스템을 처음 설치할 때 암호가 생성되고 문서화됩니다. 프로비저닝 암호가 `Passwords.txt` 파일에 없습니다.
현재 사용 중인 플랫폼에 대한 설명서입니다	플랫폼 공급업체의 웹 사이트에서 설명서를 참조하십시오. 현재 지원되는 플랫폼 버전에 대한 자세한 내용은 을 "NetApp 상호 운용성 매트릭스 툴"참조하십시오.

StorageGRID 설치 파일을 다운로드하고 압축을 풉니다

([다운로드 및 추출-설치-파일-복구])

소프트웨어를 다운로드하고 파일 압축을 "스토리지 노드에서 장애가 발생한 스토리지 볼륨 복구"풉니다.

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 버전의 형식은 다음과 같습니다 `11.x.y`.

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 `.tgz` 플랫폼에 대한 또는 `.zip` 파일을 선택합니다.

   설치 아카이브 파일에 표시된 버전이 현재 설치된 소프트웨어 버전과 일치해야 합니다.

   Windows를 실행하는 경우 이 `.zip` 파일을 사용합니다.

플랫폼	설치 아카이브
Red Hat Enterprise Linux	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
Ubuntu 또는 Debian 또는 어플라이언스	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`
VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip` `StorageGRID-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 시스템"적절한 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 호스트에 StorageGRID 노드 이미지를 설치하기 위한 rpm 패키지입니다.
	RHEL 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	스크립트와 함께 사용할 예제 구성 파일 `configure-storagegrid.py`
	SSO(Single Sign-On)가 활성화된 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제 이 스크립트를 Ping 연합 통합에 사용할 수도 있습니다.
/rpms/configure -StorageGrid.blank.json을 지정합니다	스크립트와 함께 사용할 빈 구성 `configure-storagegrid.py` 파일입니다.
	StorageGRID 컨테이너 배포를 위해 RHEL 호스트를 구성하기 위한 Ansible 역할 및 플레이북 예 필요에 따라 역할 또는 플레이북을 사용자 지정할 수 있습니다.
	Active Directory 또는 Ping 연방을 사용하여 SSO(Single Sign-On)를 사용하도록 설정한 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제

경로 및 파일 이름입니다	설명
/rpms/StorageGrid-ssoauth-Azure.js	Azure와의 SSO 상호 작용을 수행하기 위해 Python 스크립트에 의해 호출되는 도우미 스크립트입니다. `storagegrid-ssoauth-azure.py`
/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 시스템"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	파일의 MD5 체크섬 `/debs/storagegrid-webscale-images-version-SHA.deb`.
/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 이 스크립트를 Ping 연합 통합에 사용할 수도 있습니다.

경로 및 파일 이름입니다	설명
/debs/configure -StorageGrid.sample.json 을 참조하십시오	스크립트와 함께 사용할 예제 구성 파일 `configure-storagegrid.py`
/debs/configure -StorageGrid.blank.json 을 참조하십시오	스크립트와 함께 사용할 빈 구성 `configure-storagegrid.py` 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.
	Active Directory 또는 Ping 연방을 사용하여 SSO(Single Sign-On)를 사용하도록 설정한 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/debs/StorageGrid-ssoauth-Azure.js를 입력합니다	Azure와의 SSO 상호 작용을 수행하기 위해 Python 스크립트에 의해 호출되는 도우미 스크립트입니다. `storagegrid-ssoauth-azure.py`
/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 시스템"적절한 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.
	Open Virtualization Format 템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 기본 관리자 노드를 배포할 수 있습니다.

경로 및 파일 이름입니다	설명
	템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 비기본 관리 노드를 배포합니다.
	템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 게이트웨이 노드를 배포할 수 있습니다.
	템플릿 파일(`.ovf`) 및 매니페스트 파일(`.mf`)을 사용하여 가상 머신 기반 스토리지 노드를 구축합니다.
배포 스크립팅 도구	설명
	가상 그리드 노드의 배포를 자동화하는 데 사용되는 Bash 쉘 스크립트입니다.
	스크립트와 함께 사용할 예제 구성 파일 `deploy-vsphere-ovftool.sh`
	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 스크립트의 예 이 스크립트를 Ping 연합 통합에 사용할 수도 있습니다.
/vSphere/configure -StorageGrid.sample.json을 참조하십시오	스크립트와 함께 사용할 예제 구성 파일 `configure-storagegrid.py`
/vSphere/configure -StorageGrid.blank.json 을 참조하십시오	스크립트와 함께 사용할 빈 구성 `configure-storagegrid.py` 파일입니다.
	Active Directory 또는 Ping 연방을 사용하여 SSO(Single Sign-On)를 사용하도록 설정한 경우 Grid Management API에 로그인하는 데 사용할 수 있는 Python 스크립트 예제
/vSphere/StorageGrid-ssoauth-Azure.js	Azure와의 SSO 상호 작용을 수행하기 위해 Python 스크립트에 의해 호출되는 도우미 스크립트입니다. `storagegrid-ssoauth-azure.py`

경로 및 파일 이름입니다	설명
/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	파일의 MD5 체크섬 `/debs/storagegridwebscale-images-version-SHA.deb`.

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 사이트를 복구하는 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"

그리드 노드	복구 절차
게이트웨이 노드	"게이트웨이 노드에서 복구"
아카이브 노드	"아카이브 노드 장애 복구(StorageGRID 11.8 문서 사이트)"

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

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 문의하십시오.	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.
한 사이트에서 둘 이상의 스토리지 노드에 장애가 발생했거나 전체 사이트에 장애가 발생했습니다.	기술 지원 부서에 문의하십시오. 사이트 복구 절차를 수행해야 할 수 있습니다.	기술 지원 부서에서 고객의 상황을 평가하고 복구 계획을 개발합니다. 을 "기술 지원 부서에서 사이트를 복구하는 방법"참조하십시오.
어플라이언스 스토리지 노드에 장애가 발생했습니다.	"어플라이언스 스토리지 노드를 복구합니다"	어플라이언스 스토리지 노드의 복구 절차는 모든 장애 시 동일합니다.

문제	조치	참고
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. "Reaper" 또는 "Cassandra repair"라는 스크립트 출력을 확인할 수 있습니다. 복구가 실패했음을 나타내는 오류 메시지가 표시되면 오류 메시지에 표시된 명령을 실행합니다.

어플라이언스 스토리지 노드를 복구합니다

어플라이언스 스토리지 노드 복구에 대한 경고

장애가 발생한 StorageGRID 어플라이언스 스토리지 노드를 복구하는 절차는 시스템 드라이브 손실 또는 스토리지 볼륨 손실에서 복구하든 동일합니다.

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. 을 "기술 지원 부서에서 사이트를 복구하는 방법"참조하십시오.

ILM 규칙이 복제된 복사본을 하나만 저장하도록 구성되어 있고 해당 복사본이 실패한 스토리지 볼륨에 있으면 개체를 복구할 수 없습니다.

컨트롤러 교체 또는 SANtricity OS 재설치 지침과 같은 하드웨어 유지 관리 절차는 를 참조하십시오 "보관 어플라이언스 유지보수 지침".

어플라이언스 스토리지 노드의 재설치를 준비합니다

어플라이언스 스토리지 노드를 복구할 때는 먼저 StorageGRID 소프트웨어 재설치를 위한 어플라이언스를 준비해야 합니다.

단계

1. 장애가 발생한 스토리지 노드에 로그인:

a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. StorageGRID 소프트웨어 설치를 위해 어플라이언스 스토리지 노드를 준비합니다. `sgareinstall`
3. 계속하라는 메시지가 나타나면 다음을 입력합니다. `y`

어플라이언스가 재부팅되고 SSH 세션이 종료됩니다. StorageGRID 어플라이언스 설치 프로그램을 사용할 수 있게 되기까지 일반적으로 5분이 걸리지만 경우에 따라 최대 30분까지 기다려야 할 수도 있습니다.

> 전원을 껐다가 켜거나 제품을 리셋하여 재부팅을 가속화하려고 하지 마십시오. 자동 BIOS, BMC 또는 기타 펌웨어 업그레이드를 중단할 수 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.

> `sgareinstall`명령을 실행하면 StorageGRID 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.

시작하기 전에

- 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 어플라이언스의 설치 지침에 따라 이러한 필수 작업을 완료했습니다. 을 "하드웨어 설치를 빠르게 시작합니다"참조하십시오.
- 을 사용하고 "지원되는 웹 브라우저"있습니다.
- 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.

- 운영 관리 노드의 IP 주소와 노드의 호스트 이름(시스템 이름)을 지정하거나 확인합니다.
- 설치를 시작하고 볼륨이 구성되고 소프트웨어가 설치될 때까지 기다립니다.

> 어플라이언스 스토리지 노드를 복구하는 경우 원래 어플라이언스와 동일한 스토리지 유형(결합된 스토리지, 메타데이터 전용 또는 데이터 전용)으로 재설치합니다. 다른 스토리지 유형을 지정하면 복구가 실패하고 올바른 스토리지 유형으로 어플라이언스를 재설치해야 합니다.

- 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.

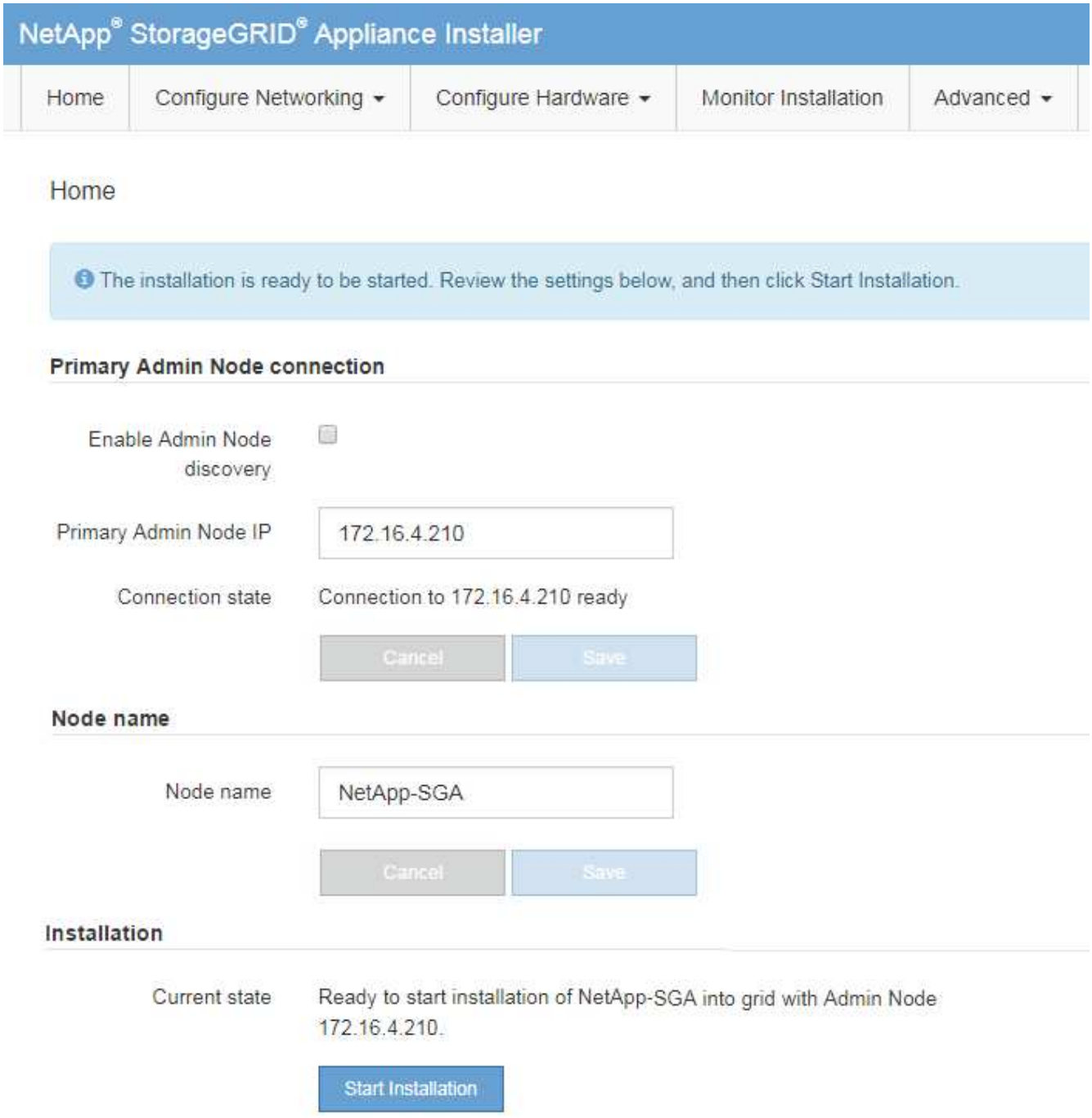
3. 이 IP 주소가 표시되지 않거나 변경해야 하는 경우 주소를 지정합니다.

옵션을 선택합니다	단계
수동 IP 입력	a. 관리자 노드 검색 활성화 * 확인란의 선택을 취소합니다. b. IP 주소를 수동으로 입력합니다. c. 저장 * 을 클릭합니다. d. 새 IP 주소의 연결 상태가 "준비"가 될 때까지 기다립니다.
연결된 모든 운영 관리 노드의 자동 검색	a. 관리자 노드 검색 활성화 * 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 "준비"가 될 때까지 기다립니다.

4. Node Name * 필드에 복구 중인 노드에 사용된 것과 동일한 호스트 이름(시스템 이름)을 입력하고 * Save * 를 클릭합니다.
5. 설치 섹션에서 현재 상태가 "기본 관리자 노드 '*ADMIN_IP*'를 사용하여 그리드로 설치를 시작할 준비가 되었습니다 "이고 * 설치 시작 * 버튼이 활성화되어 있는지 확인합니다 `node name`.

   설치 시작 * 버튼이 활성화되지 않은 경우 네트워크 구성 또는 포트 설정을 변경해야 할 수 있습니다. 자세한 내용은 제품의 유지보수 지침을 참조하십시오.

6. StorageGRID 어플라이언스 설치 관리자 홈 페이지에서 * 설치 시작 * 을 클릭합니다.



현재 상태가 "Installation is in progress(설치 진행 중)"로 변경되고 Monitor Installation(모니터 설치) 페이지가 표시됩니다.

모니터 설치 페이지에 수동으로 액세스해야 하는 경우 메뉴 모음에서 * 모니터 설치 * 를 클릭합니다.

을 "어플라이언스 설치를 모니터링합니다"참조하십시오.

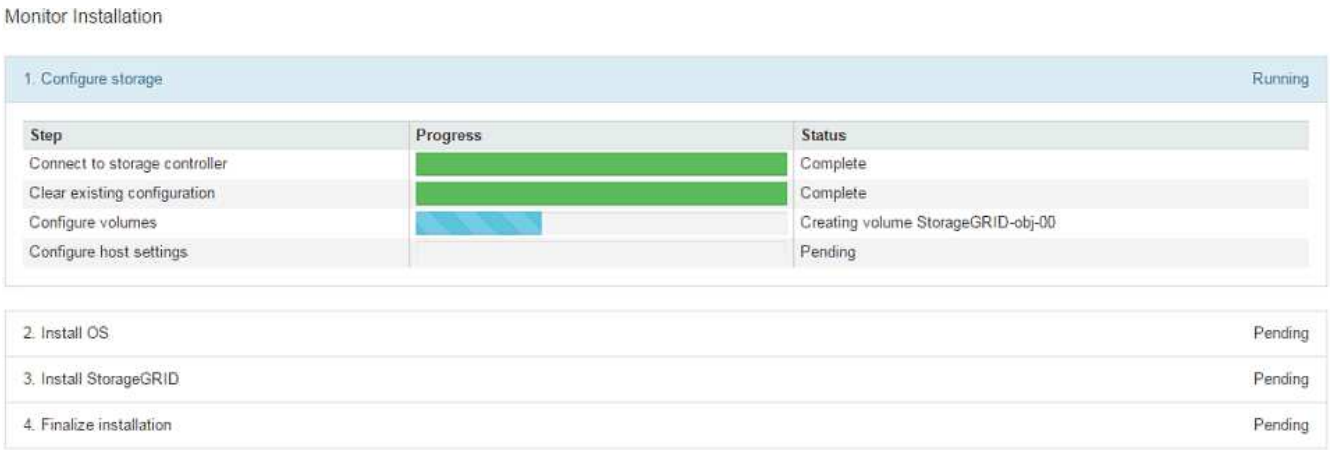
StorageGRID 어플라이언스 설치를 모니터링합니다

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 실행하는 경우 다시 실행할 필요가 없는 작업은 녹색 상태 표시줄과 "건너뜀"으로 표시됩니다.

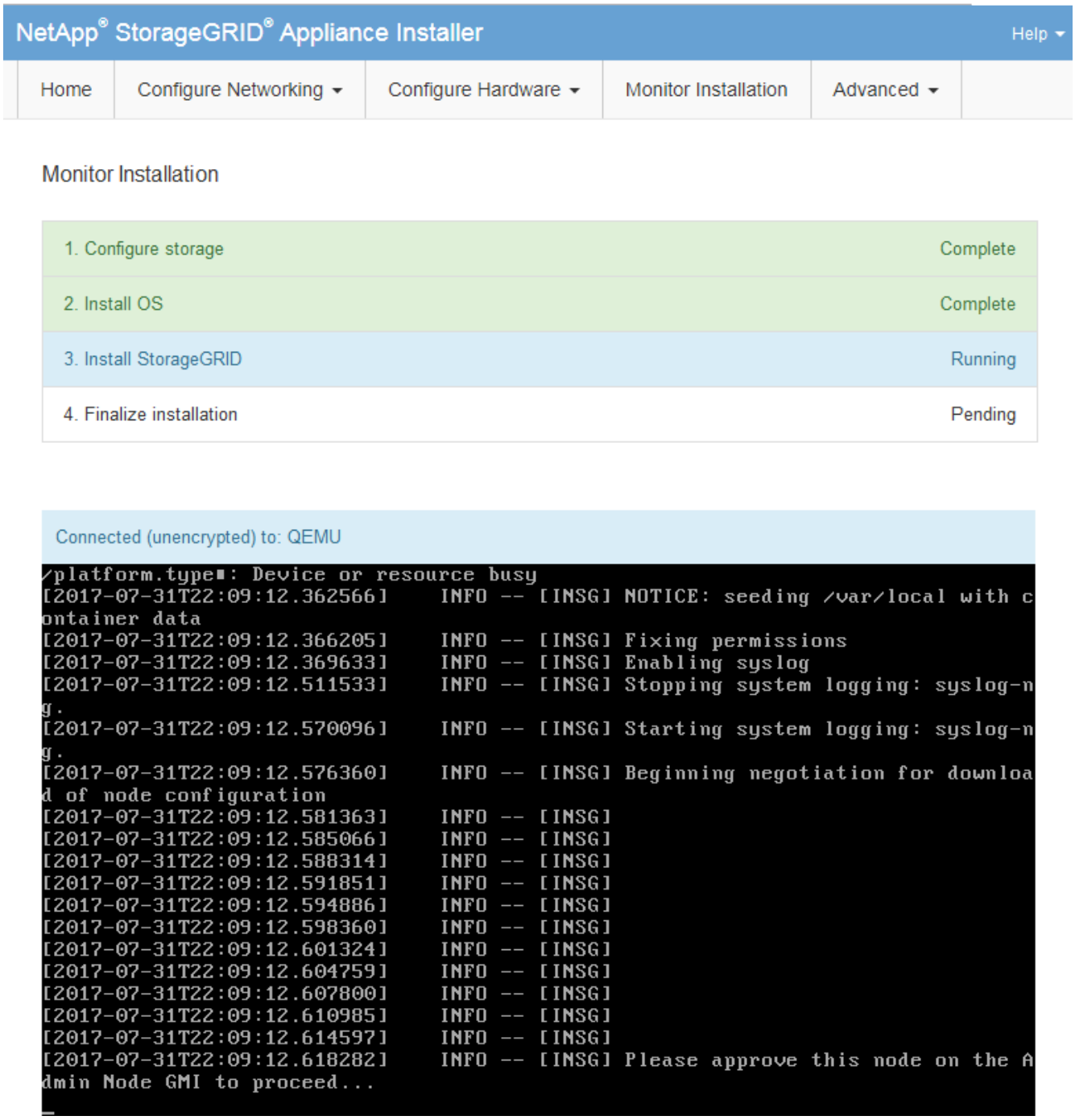
2. 처음 두 설치 단계의 진행 상황을 검토합니다.
   - * 1. 스토리지 구성 *

     이 단계에서 설치 관리자는 스토리지 컨트롤러에 연결하고, 기존 구성을 지우고, SANtricity OS와 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. 로 이동합니다. "Start Recovery(복구 시작) 를 선택하여 어플라이언스 스토리지 노드를 구성합니다"

Start Recovery(복구 시작) 를 선택하여 어플라이언스 스토리지 노드를 구성합니다

장애가 발생한 노드의 대체품으로 어플라이언스 스토리지 노드를 구성하려면 그리드 관리자에서 복구 시작을 선택해야 합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.
- 프로비저닝 암호가 있습니다.

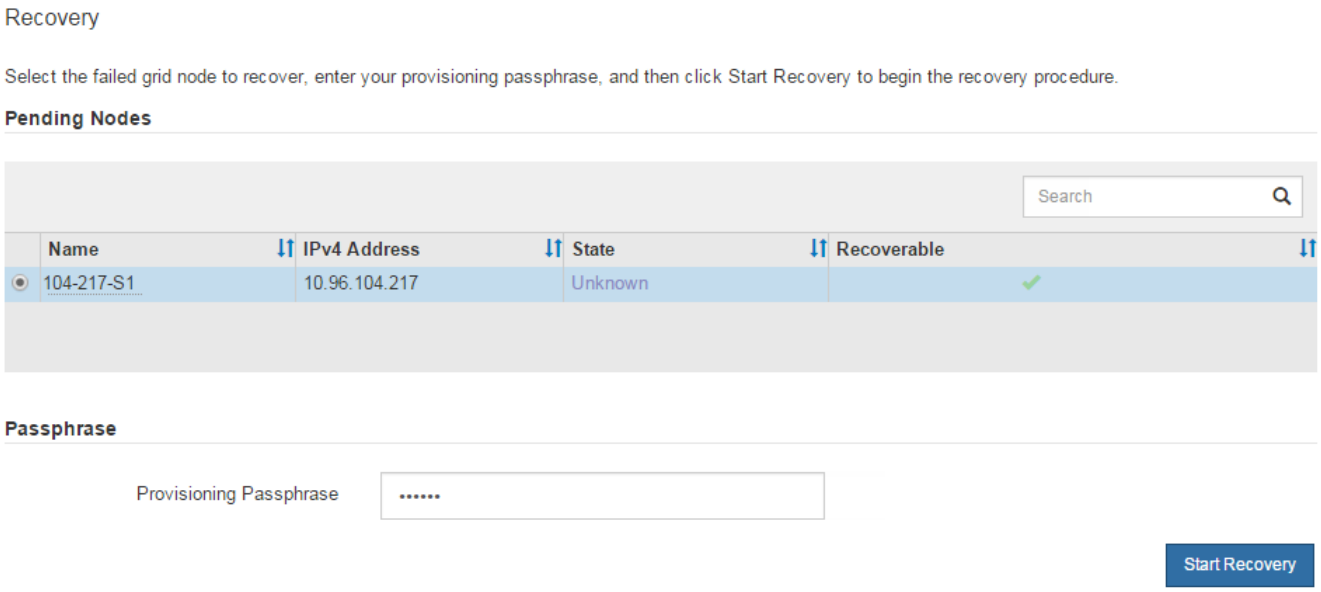
- 복구 어플라이언스 스토리지 노드를 구축했습니다.
- 삭제 코딩 데이터에 대한 복구 작업의 시작 날짜가 있습니다.
- 스토리지 노드가 지난 15일 이내에 재구축되지 않은 것을 확인했습니다.

단계

1. Grid Manager에서 * 유지보수 * > * 작업 * > * 복구 * 를 선택합니다.
2. Pending Nodes 목록에서 복구할 그리드 노드를 선택합니다.

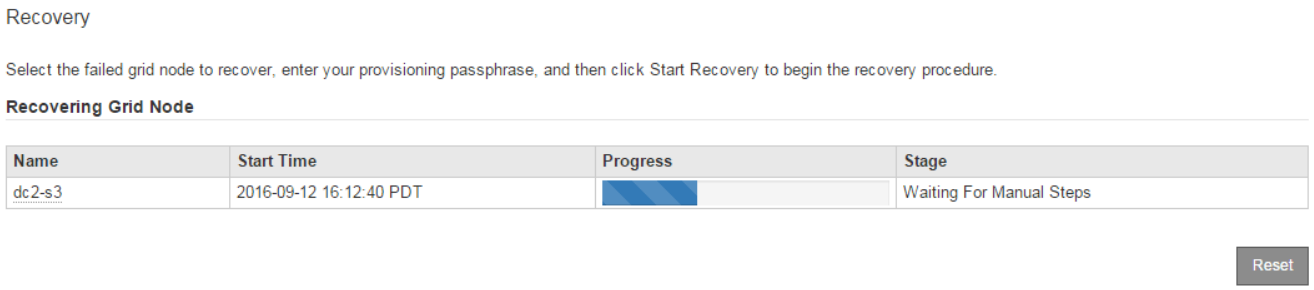
   노드가 실패한 후 목록에 나타나지만 다시 설치되고 복구 준비가 될 때까지 노드를 선택할 수 없습니다.

3. Provisioning Passphrase * 를 입력합니다.
4. 복구 시작 * 을 클릭합니다.

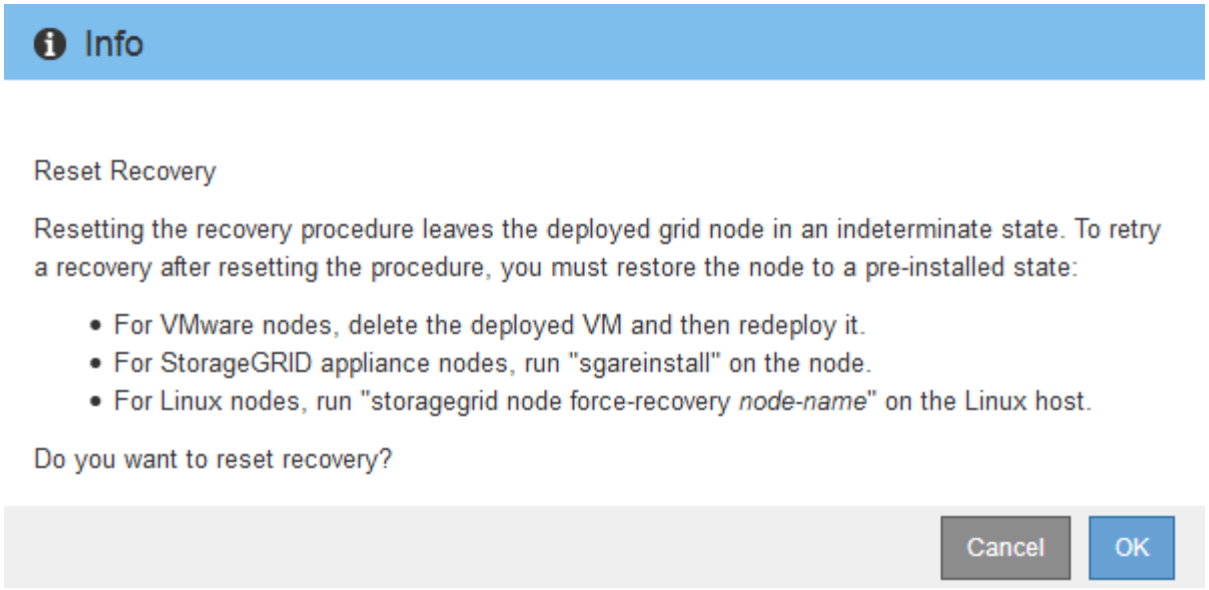


5. 복구 그리드 노드 테이블에서 복구 진행률을 모니터링합니다.

   그리드 노드가 "수동 단계 대기" 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 대화 상자가 나타납니다.



절차를 재설정한 후 복구를 다시 시도하려면 노드에서 를 실행하여 어플라이언스 노드를 사전 설치된 상태로 복원해야 `sgareinstall` 합니다.

어플라이언스 스토리지 볼륨 다시 마운트 및 다시 포맷(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.

시작하기 전에

- 장애가 발생한 스토리지 볼륨의 하드웨어를 교체하도록 이미 교체했습니다.

  스크립트를 실행하면 `sn-remount-volumes` 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. 스크립트를 실행하지 `sn-recovery-postinstall.sh` 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.
- `sn-remount-volumes`스크립트를 실행하여 올바르게 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 실행 `sn-recovery-postinstall.sh`(4단계)하여 실패한 스토리지 볼륨을 다시 포맷하고 객체 메타데이터를 복구하십시오. 완료되기 전에 스토리지 노드를 재부팅하면 `sn-recovery-postinstall.sh` 시작을 시도하고 StorageGRID 어플라이언스 노드가 유지보수 모드를 종료하는 서비스에 오류가 발생합니다.

- 스크립트가 마운트하지 못했거나 잘못 포맷된 스토리지 볼륨을 다시 `sn-remount-volumes` 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. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

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. 다음 스크립트를 실행합니다. `sn-remount-volumes`

      이 스크립트는 데이터가 포함된 스토리지 볼륨에서 실행되는 데 몇 시간이 걸릴 수 있습니다.

   b. 스크립트가 실행되면 출력을 검토하고 프롬프트에 응답합니다.

필요한 경우 명령을 사용하여 스크립트의 로그 파일 내용을 모니터링할 수 `tail -f (/var/local/log/sn-remount-volumes.log` 있습니다. 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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't 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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't 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` XFS 파일 시스템 일관성 검사를 통과했으며 유효한 볼륨 구조가 있어 성공적으로 다시 마운트되었습니다. 스크립트에 의해 다시 마운트된 디바이스의 데이터는 보존됩니다.
- `/dev/sdc` 스토리지 볼륨이 새 볼륨이거나 손상되었기 때문에 XFS 파일 시스템 일관성 검사에 실패했습니다.
- `/dev/sdd` 디스크가 초기화되지 않았거나 디스크의 슈퍼블록이 손상되었기 때문에 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-remount-volumes.log` 로그 파일에 저장됩니다.

- `/dev/sde` XFS 파일 시스템 일관성 검사를 통과했으며 유효한 볼륨 구조를 가지고 있지만 파일의 LDR 노드 ID가 `volID` 이 스토리지 노드의 ID(맨 위에 표시됨)와 일치하지 `configured LDR noid` 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 대한 스크립트 실행의 의미를 이해해야 `sn-recovery-postinstall.sh` 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. 스크립트를 실행하면 `sn-recovery-postinstall.sh` 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. 이 ID는 스크립트를 실행하여 볼륨에 객체 데이터를 복원할 때 입력해야 `repair-data` 합니다(다음 절차).

d. 마운트 해제된 모든 디바이스를 복구하거나 교체한 후 `sn-remount-volumes` 스크립트를 다시 실행하여 다시 마운트할 수 있는 모든 스토리지 볼륨이 다시 마운트되었는지 확인합니다.

> 스토리지 볼륨을 마운트할 수 없거나 잘못 포맷된 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.

> 장애가 발생한 스토리지 볼륨에 남아 있는 데이터를 그리드의 다른 위치에서 재구축할 수 없다고 생각하는 경우(예: ILM 정책이 하나의 복사본만 만드는 규칙을 사용하는 경우 또는 여러 노드에서 볼륨이 장애가 발생한 경우) 스크립트를 실행하지 마십시오 `sn-recovery-postinstall.sh`. 대신 기술 지원 부서에 문의하여 데이터 복구 방법을 확인하십시오.

4. `sn-recovery-postinstall.sh`다음 스크립트를 실행합니다. `sn-recovery-postinstall.sh`

이 스크립트는 마운트할 수 없거나 잘못 포맷된 스토리지 볼륨을 다시 포맷하고, 필요한 경우 노드에서 Cassandra 데이터베이스를 재구축하고, 스토리지 노드에서 서비스를 시작합니다.

다음 사항에 유의하십시오.

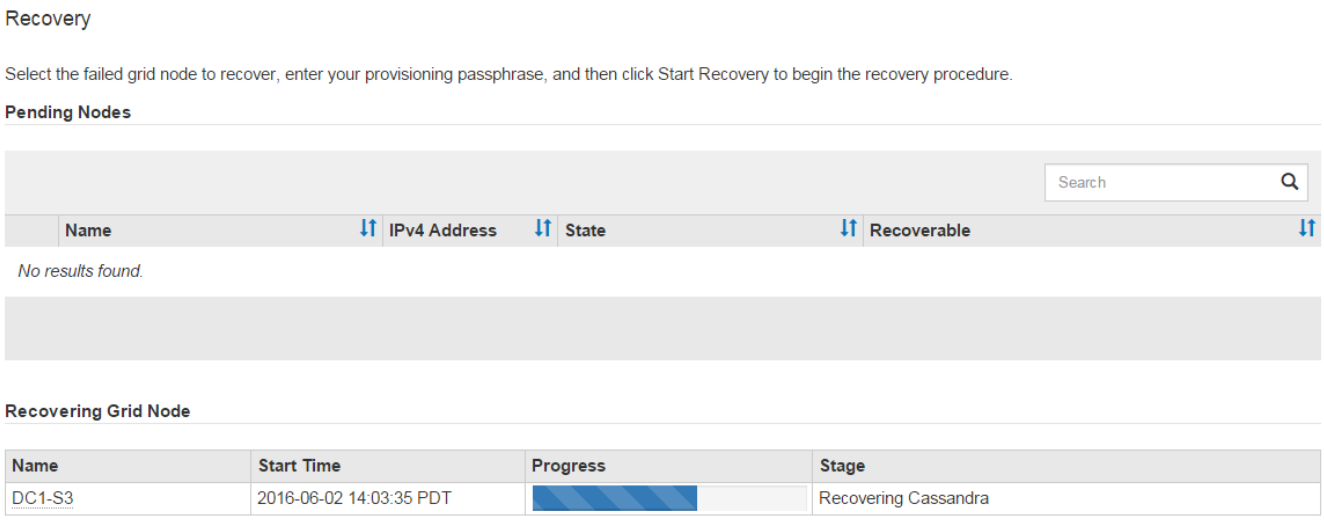
- 스크립트를 실행하는 데 몇 시간이 걸릴 수 있습니다.
- 일반적으로 스크립트가 실행되는 동안에는 SSH 세션만 남겨야 합니다.
- SSH 세션이 활성화되어 있는 동안에는 * Ctrl + C * 를 누르지 마십시오.
- 네트워크 중단이 발생하여 SSH 세션을 종료하는 경우 스크립트는 백그라운드에서 실행되지만 복구 페이지에서 진행률을 볼 수 있습니다.
- 스토리지 노드가 RSM 서비스를 사용하는 경우 노드 서비스가 다시 시작됨에 따라 스크립트가 5분 동안 정지되는 것처럼 보일 수 있습니다. RSM 서비스가 처음 부팅될 때마다 5분 정도 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. "Reaper" 또는 "Cassandra repair"라는 스크립트 출력을 확인할 수 있습니다. 복구가 실패했음을 나타내는 오류 메시지가 표시되면 오류 메시지에 표시된 명령을 실행합니다.

5. 스크립트가 실행되면 `sn-recovery-postinstall.sh` 그리드 관리자에서 복구 페이지를 모니터링합니다.

   복구 페이지의 진행 표시줄과 단계 열은 스크립트의 상위 수준 상태를 `sn-recovery-postinstall.sh` 제공합니다.



6. 스크립트가 노드에서 서비스를 시작한 후에는 `sn-recovery-postinstall.sh` 스크립트로 포맷된 모든 스토리지 볼륨에 오브젝트 데이터를 복원할 수 있습니다.

   이 스크립트는 Grid Manager 볼륨 복원 프로세스를 사용할 것인지 묻습니다.

   - 대부분의 경우, 당신은 해야 "Grid Manager를 사용하여 개체 데이터를 복원합니다"합니다. 대답은 `y` 그리드 관리자를 사용합니다.
   - 기술 지원 부서의 지시가 있거나 교체 노드에 원래 노드보다 오브젝트 스토리지에 사용할 수 있는 볼륨 수가 적다는 것을 알고 있는 경우 `repair-data`스크립트를 사용해야 합니다."개체 데이터를 수동으로 복원합니다" 이러한 경우 중 하나가 적용되면 답변합니다 `n`.

Grid Manager 볼륨 복원 프로세스 사용에 대한 대답인 경우 `n`(개체 데이터를 수동으로 복원):

- Grid Manager를 사용하여 개체 데이터를 복원할 수 없습니다.
- Grid Manager를 사용하여 수동 복원 작업의 진행률을 모니터링할 수 있습니다.

선택한 후에는 스크립트가 완료되고 객체 데이터를 복구하는 다음 단계가 표시됩니다. 이러한 단계를 검토한 후 아무 키나 눌러 명령줄로 돌아갑니다.

어플라이언스의 스토리지 볼륨에 오브젝트 데이터를 복원합니다

어플라이언스 스토리지 노드의 스토리지 볼륨을 복구한 후에는 스토리지 노드에 장애가 발생할 때 손실된 복제 또는 삭제 코딩 오브젝트 데이터를 복원할 수 있습니다.

어떤 절차를 사용해야 합니까**?**

가능한 경우 그리드 관리자의 * 볼륨 복원 * 페이지를 사용하여 개체 데이터를 복원합니다.

- 볼륨이 * 유지 관리 * > * 볼륨 복원 * > * 에 나열되어 있는 경우 * 복원할 노드 * 는 를 사용하여 오브젝트 데이터를 복원합니다."Grid Manager의 볼륨 복원 페이지"
- 볼륨이 * 유지 관리 * > * 볼륨 복원 * > * 복원할 노드 * 에 표시되지 않으면 스크립트를 사용하여 오브젝트 데이터를 복원하는 다음 단계를 따르십시오. `repair-data`

  복구된 스토리지 노드에 교체 중인 노드보다 적은 수의 볼륨이 포함된 경우 스크립트를 사용해야 `repair-data` 합니다.

repair-data 스크립트는 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다. 가능하면 를 사용합니다"Grid Manager(그리드 관리자)의 볼륨 복원 절차".

스크립트를 사용하여 `repair-data` 객체 데이터를 복원합니다

시작하기 전에

- 복구된 스토리지 노드의 그리드 관리자의 * nodes * > * Overview * 탭에서 연결 상태가 * Connected * 인 것을 확인했습니다.

이 작업에 대해

개체 복사본을 사용할 수 있도록 그리드의 ILM 규칙이 구성되어 있다고 가정하면 다른 스토리지 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.

스크립트 정보를 참조하십시오 `repair-data`

객체 데이터를 복원하려면 `repair-data` 스크립트를 실행합니다. 이 스크립트는 개체 데이터 복원 프로세스를 시작하고 ILM 스캔 작업을 통해 ILM 규칙이 충족되는지 확인합니다.

아래의 * 복제 데이터 * 또는 * 삭제 코딩(EC) 데이터 * 를 선택하여 복제된 데이터를 복원하는지 또는 삭제 코딩 데이터를 복원하는지 여부에 따라 스크립트에 대한 다양한 옵션을 `repair-data` 확인하십시오. 두 유형의 데이터를 모두 복원해야 하는 경우 두 명령 집합을 모두 실행해야 합니다.

스크립트에 대한 자세한 내용을 `repair-data` 보려면 기본 관리자 노드의 명령줄에서 를 `repair-data --help` 입력합니다.

repair-data 스크립트는 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다. 가능하면 를 사용합니다"Grid Manager(그리드 관리자)의 볼륨 복원 절차".

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

repair-data start-replicated-volume-repair
```

다음 명령을 사용하여 복제된 데이터의 복구를 추적할 수 있습니다.

```
repair-data show-replicated-repair-status
```

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-repair

repair-data start-ec-volume-repair
```

다음 명령을 사용하여 삭제 코딩 데이터의 복구를 추적할 수 있습니다.

```
repair-data show-ec-repair-status
```

일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 하지만 삭제 코딩 데이터를 모두 처리할 수 없는 경우 복구를 완료할 수 없습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

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. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 파일을 사용하여 `/etc/hosts` 복구된 스토리지 볼륨에 대한 스토리지 노드의 호스트 이름을 찾습니다. 그리드에 있는 모든 노드의 목록을 보려면 다음을 입력합니다 `cat /etc/hosts`.

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 볼륨에만 장애가 발생한 경우 로 이동합니다일부 볼륨만 장애가 발생한 경우 데이터를 복구합니다.

> 둘 이상의 노드에 대한 작업을 동시에 실행할 수 `repair-data` 없습니다. 여러 노드를 복구하려면 기술 지원 팀에 문의하십시오.

복제된 데이터

그리드에 복제된 데이터가 포함되어 있는 경우 `repair-data start-replicated-node-repair` 명령을 옵션(여기서 `--nodes` 는 호스트 이름(시스템 이름))과 함께 `--nodes` 사용하여 전체 스토리지 노드를 복구합니다.

이 명령은 SG-DC-SN3이라는 스토리지 노드에서 복제된 데이터를 복구합니다.

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> 개체 데이터가 복원되면 StorageGRID 시스템에서 복제된 개체 데이터를 찾을 수 없는 경우 * 개체 손실 * 경고가 트리거됩니다. 시스템 전체의 스토리지 노드에서 경고가 트리거될 수 있습니다. 손실의 원인과 복구가 가능한지 확인해야 합니다. 을 "손실된 개체를 조사합니다"참조하십시오.

삭제 코딩**(EC)** 데이터

그리드에 삭제 코딩 데이터가 포함되어 있는 경우 명령을 옵션과 함께 `--nodes` 사용합니다. 여기서 는 호스트 이름(시스템 이름) 옵션을 `--nodes` 사용하여 `repair-data start-ec-node-repair` 전체 스토리지 노드를 복구합니다.

이 명령은 이름이 SG-DC-SN3인 스토리지 노드에서 삭제 코딩 데이터를 복구합니다.

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

이 작업은 이 작업을 식별하는 `repair_data` 고유 을 `repair ID` 반환합니다. 이 버튼을 사용하여 `repair ID` 작업의 진행 상황과 결과를 `repair_data` 추적합니다. 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 볼륨에 오류가 발생한 경우 로 이동합니다모든 볼륨이 실패한 경우 데이터를 복구합니다.

볼륨 ID를 16진수로 입력합니다. 예를 들어 `0000`, 은 첫 번째 볼륨이고 `000F` 는 16번째 볼륨입니다. 하나의 볼륨, 하나의 볼륨 범위 또는 하나의 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 포함되어 있는 경우 `start-replicated-volume-repair` 명령을 옵션과 함께 `--nodes` 사용하여 노드를 식별합니다(여기서 `--nodes` 는 노드의 호스트 이름). 그런 다음 다음 다음 `--volumes` 예제와 같이 또는 `--volume-range` 옵션을 추가합니다.

- 단일 볼륨 *: 이 명령은 복제된 데이터를 SG-DC-SN3이라는 스토리지 노드의 볼륨에 복원합니다 `0002`.

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

- 볼륨 범위 *: 이 명령은 `0009` SG-DC-SN3이라는 이름의 스토리지 노드에 있는 범위 내의 모든 볼륨에 복제된 데이터를 복원합니다 `0003`.

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

*연속되지 않은 여러 볼륨 *: 이 명령은 복제된 데이터를 볼륨, `0005` `0008` SG-DC-SN3이라는 스토리지 노드에서 복원합니다. `0001`

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> 개체 데이터가 복원되면 StorageGRID 시스템에서 복제된 개체 데이터를 찾을 수 없는 경우 * 개체 손실 * 경고가 트리거됩니다. 시스템 전체의 스토리지 노드에서 경고가 트리거될 수 있습니다. 경고 설명 및 권장 조치를 참고하여 손실의 원인을 파악하고 복구가 가능한지 여부를 확인합니다.

삭제 코딩**(EC)** 데이터

그리드에 삭제 코딩 데이터가 포함되어 있는 경우 `start-ec-volume-repair` 명령을 옵션과 함께 `--nodes` 사용하여 노드를 식별합니다(여기서 `--nodes` 는 노드의 호스트 이름). 그런 다음 다음 다음 `--volumes` 예제와 같이 또는 `--volume-range` 옵션을 추가합니다.

- 단일 볼륨 *: 이 명령은 SG-DC-SN3이라는 이름의 스토리지 노드의 볼륨에 삭제 코딩 데이터를 복원합니다 `0007`.

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

- 볼륨 범위 *: 이 명령은 `0006` SG-DC-SN3이라는 이름의 스토리지 노드에 있는 범위 내의 모든 볼륨에 삭제 코딩 데이터를 복원합니다 `0004`.

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

*연속되지 않은 여러 볼륨 *: 이 명령은 삭제 코딩 데이터를 볼륨, `000C` `000E` SG-DC-SN3이라는 스토리지 노드에서 복원합니다. `000A`

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

`repair-data`이 작업은 이 작업을 식별하는 `repair_data` 고유 을 `repair ID` 반환합니다. 이 버튼을 사용하여 `repair ID` 작업의 진행 상황과 결과를 `repair_data` 추적합니다. 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.

또한 처리 중인 볼륨 복원 작업의 상태를 모니터링하고 에서 완료된 복원 작업의 기록을 볼 수 "그리드 관리자"있습니다.

복제된 데이터

- 복제된 복구의 예상 완료율을 얻으려면 repair-data 명령에 옵션을 추가합니다 `show-replicated-repair-status`.

```
repair-data show-replicated-repair-status
```

- 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.

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.
   - 다음 명령을 사용하여 특정 작업의 상태를 `repair-data` 확인합니다.

```
repair-data show-ec-repair-status --repair-id repair ID
```

   - 이 명령을 사용하여 모든 수리를 나열합니다.

```
repair-data show-ec-repair-status
```

출력에는 이전 및 현재 실행 중인 모든 수리에 대한 정보가 `repair ID` 표시됩니다.

2. 출력에 복구 작업이 실패했다고 표시되는 경우 옵션을 사용하여 `--repair-id` 복구를 재시도합니다.

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 노드 복구를 재시도합니다.

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 볼륨 복구를 다시 시도합니다.

   ```
   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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."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

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 복구 절차는 소프트웨어 기반 스토리지 노드에만 적용됩니다. 어플라이언스 스토리지 노드에서 스토리지 볼륨에 장애가 발생한 경우 어플라이언스 절차를 대신 사용하십시오"어플라이언스 스토리지 노드를 복구합니다".

이 복구 절차에는 다음 작업이 포함됩니다.

- "스토리지 볼륨 복구에 대한 경고를 검토합니다"
- "장애가 발생한 스토리지 볼륨을 식별하고 마운트 해제합니다"
- "볼륨을 복구하고 Cassandra 데이터베이스를 재구성합니다"
- "객체 데이터를 복원합니다"
- "스토리지 상태를 확인합니다"

저장소 볼륨 복구에 대한 경고

스토리지 노드의 실패한 스토리지 볼륨을 복구하기 전에 다음 경고를 검토하십시오.

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. 을 "기술 지원 부서에서 사이트를 복구하는 방법"참조하십시오.

ILM 규칙이 복제된 복사본을 하나만 저장하도록 구성되어 있고 해당 복사본이 실패한 스토리지 볼륨에 있으면 개체를 복구할 수 없습니다.

관련 정보

"그리드 노드 복구에 대한 경고 및 고려 사항"

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.

시작하기 전에

을 사용하여 그리드 관리자에 로그인되어 있습니다."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 스크립트를 실행할 때 `reformat_storage_block_devices.rb` 파일 시스템 오류가 발생하여 스크립트가 중단되거나 실패할 수 있습니다.

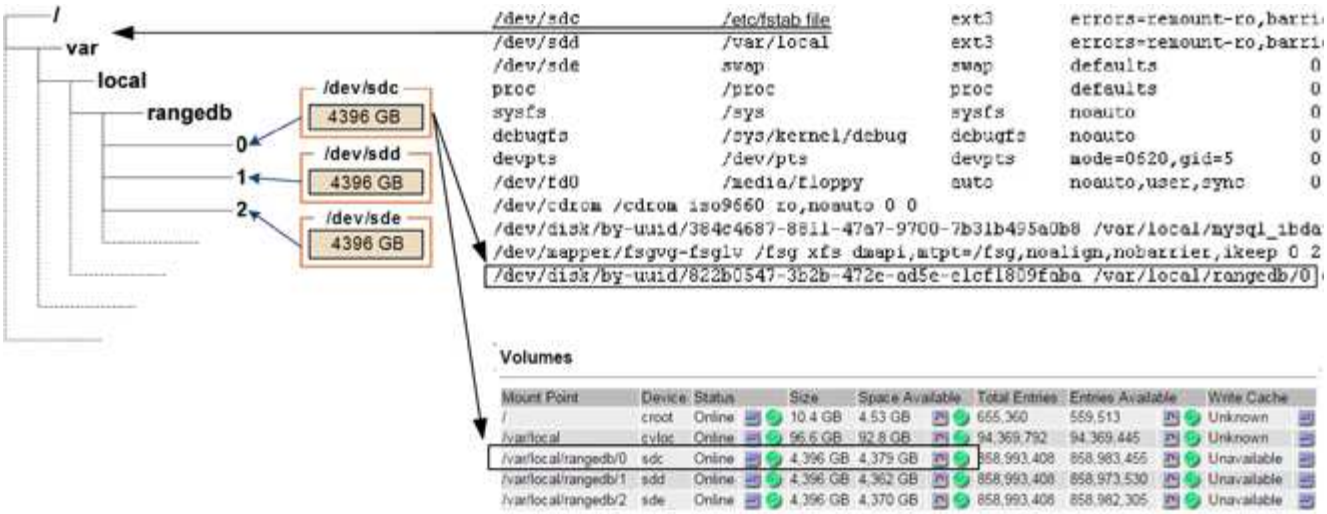
> 명령을 실행하기 전에 하드웨어를 복구하고 디스크를 제대로 `reboot` 연결합니다.

> 장애가 발생한 스토리지 볼륨을 신중하게 식별합니다. 이 정보를 사용하여 재포맷해야 하는 볼륨을 확인할 수 있습니다. 볼륨을 다시 포맷한 후에는 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 UUID 및 rangedb 디렉토리가 `/etc/fstab` 파일에 나열됩니다. 디바이스 이름, rangedb 디렉토리 및 마운트된 볼륨의 크기가 Grid Manager에 표시됩니다.

다음 예에서 디바이스의 `/dev/sdc` 볼륨 크기는 4TB이며 `/etc/fstab`파일의 디바이스 이름을 사용하여 `/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba` 에 마운트됩니다 `/var/local/rangedb/0`.



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 개체 저장소는 디바이스 이름 sdc와 크기가 107GB인 에 `/var/local/rangedb/0` 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. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

3. 다음 스크립트를 실행하여 장애가 발생한 스토리지 볼륨을 마운트 해제합니다.

`sn-unmount-volume object_store_ID`

는 `object_store_ID` 장애가 발생한 스토리지 볼륨의 ID입니다. 예를 들어, ID가 0000인 오브젝트 저장소에 대한 명령에서 를 `0` 지정하십시오.

4. 메시지가 표시되면 * y * 를 눌러 스토리지 볼륨 0에 따라 Cassandra 서비스를 중지합니다.

Cassandra 서비스가 이미 중지되어 있으면 메시지가 표시되지 않습니다. Cassandra 서비스는 볼륨 0에만 중지됩니다.

```
root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
Services depending on storage volume 0 (cassandra) aren't down.
Services depending on storage volume 0 must be stopped before running
this script.
Stop services that require storage volume 0 [y/N]? y
Shutting down services that require storage volume 0.
Services requiring storage volume 0 stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

몇 초 후 볼륨이 마운트 해제됩니다. 프로세스의 각 단계를 나타내는 메시지가 나타납니다. 마지막 메시지는 볼륨이 마운트 해제되었음을 나타냅니다.

5. 볼륨이 사용 중이어서 마운트 해제에 실패하면 다음 옵션을 사용하여 강제로 마운트 해제할 수 `--use-umountof` 있습니다.

옵션을 사용하여 강제로 마운트 해제하면 `--use-umountof` 볼륨을 사용하는 프로세스나 서비스가 예기치 않게 동작하거나 충돌할 수 있습니다.

```
root@Storage-180:~ # sn-unmount-volume --use-umountof
/var/local/rangedb/2
Unmounting /var/local/rangedb/2 using umountof
/var/local/rangedb/2 is unmounted.
Informing LDR service of changes to storage volumes
```

장애가 발생한 스토리지 볼륨에서 스토리지를 다시 포맷하고 다시 마운트하는 스크립트를 실행하고, 시스템에서 필요하다고 판단할 경우 스토리지 노드에서 Cassandra 데이터베이스를 재구성해야 합니다.

시작하기 전에

- `Passwords.txt`파일이 있습니다.
- 서버의 시스템 드라이브가 손상되지 않았습니다.
- 실패의 원인이 확인되었으며, 필요한 경우 교체 스토리지 하드웨어를 이미 확보했습니다.
- 교체 스토리지의 총 크기는 원본과 동일합니다.
- 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"

단계

1. 필요에 따라 이전에 확인 및 마운트 해제한 실패한 스토리지 볼륨과 연결된 장애가 발생한 물리적 또는 가상 스토리지를 교체하십시오.

   이 단계에서 볼륨을 다시 마운트하지 마십시오. 스토리지가 다시 마운트되고 이후 단계에서 에 `/etc/fstab` 추가됩니다.

2. 그리드 관리자에서 * nodes * >> * Hardware * 로 이동합니다 **`appliance Storage Node`**. 페이지의 StorageGRID 어플라이언스 섹션에서 스토리지 RAID 모드가 정상인지 확인합니다.
3. 장애가 발생한 스토리지 노드에 로그인:
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

4. 텍스트 편집기(vi 또는 vim)를 사용하여 파일에서 실패한 볼륨을 삭제한 `/etc/fstab` 다음 파일을 저장합니다.

   > 파일에서 실패한 볼륨에 주석을 다는 `/etc/fstab` 것은 충분하지 않습니다. 복구 프로세스에서 파일의 모든 행이 마운트된 파일 시스템과 일치하는지 확인하므로 `fstab` 볼륨을 에서 삭제해야 `fstab` 합니다.

5. 장애가 발생한 스토리지 볼륨을 다시 포맷하고 필요한 경우 Cassandra 데이터베이스를 재구축합니다. 다음을 입력합니다. `reformat_storage_block_devices.rb`
   - 스토리지 볼륨 0이 마운트 해제되면 프롬프트 및 메시지는 Cassandra 서비스가 중지 중임을 나타냅니다.
   - 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 다음과 같은 메시지가 표시되면 다음 응답 중 하나를 입력합니다. `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`

- 오류가 있는 드라이브를 다시 포맷하려면 * y * 를 누릅니다. 그러면 저장소 볼륨이 다시 포맷되고 다시 포맷된 저장소 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. "Reaper" 또는 "Cassandra repair"라는 스크립트 출력을 확인할 수 있습니다. 복구가 실패했음을 나타내는 오류 메시지가 표시되면 오류 메시지에 표시된 명령을 실행합니다.

다음 출력 예에서는 드라이브를 `/dev/sdf` 다시 포맷해야 하며 Cassandra를 재구축할 필요가 없습니다.

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
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 b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done.  Now do manual steps to
restore copies of data.
```

스토리지 볼륨을 다시 포맷하고 다시 마운트하고 필요한 Cassandra 작업이 완료된 후에 작업을 "Grid Manager를 사용하여 개체 데이터를 복원합니다"수행할 수 있습니다.

시스템 드라이브가 손상되지 않은 스토리지 노드에서 스토리지 볼륨을 복구한 후에는 스토리지 볼륨 장애 시 손실된 복제된 또는 삭제 코딩 오브젝트 데이터를 복원할 수 있습니다.

어떤 절차를 사용해야 합니까?

가능한 경우 그리드 관리자의 * 볼륨 복원 * 페이지를 사용하여 개체 데이터를 복원합니다.

- 볼륨이 * 유지 관리 * > * 볼륨 복원 * > * 에 나열되어 있는 경우 * 복원할 노드 * 는 를 사용하여 오브젝트 데이터를 복원합니다."Grid Manager의 볼륨 복원 페이지"
- 볼륨이 * 유지 관리 * > * 볼륨 복원 * > * 복원할 노드 * 에 표시되지 않으면 스크립트를 사용하여 오브젝트 데이터를 복원하는 다음 단계를 따르십시오. `repair-data`

  복구된 스토리지 노드에 교체 중인 노드보다 적은 수의 볼륨이 포함된 경우 스크립트를 사용해야 `repair-data` 합니다.

repair-data 스크립트는 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다. 가능하면 를 사용합니다"Grid Manager(그리드 관리자)의 볼륨 복원 절차".

스크립트를 사용하여 `repair-data` 객체 데이터를 복원합니다

시작하기 전에

- 복구된 스토리지 노드의 그리드 관리자의 * nodes * > * Overview * 탭에서 연결 상태가 * Connected * 인 것을 확인했습니다.

이 작업에 대해

개체 복사본을 사용할 수 있도록 그리드의 ILM 규칙이 구성되어 있다고 가정하면 다른 스토리지 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.

스크립트 정보를 참조하십시오 `repair-data`

객체 데이터를 복원하려면 `repair-data` 스크립트를 실행합니다. 이 스크립트는 개체 데이터 복원 프로세스를 시작하고 ILM 스캔 작업을 통해 ILM 규칙이 충족되는지 확인합니다.

아래의 * 복제 데이터 * 또는 * 삭제 코딩(EC) 데이터 * 를 선택하여 복제된 데이터를 복원하는지 또는 삭제 코딩 데이터를 복원하는지 여부에 따라 스크립트에 대한 다양한 옵션을 `repair-data` 확인하십시오. 두 유형의 데이터를 모두 복원해야 하는 경우 두 명령 집합을 모두 실행해야 합니다.

스크립트에 대한 자세한 내용을 `repair-data` 보려면 기본 관리자 노드의 명령줄에서 를 `repair-data --help` 입력합니다.

repair-data 스크립트는 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다. 가능하면 를 사용합니다"Grid Manager(그리드 관리자)의 볼륨 복원 절차".

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

repair-data start-replicated-volume-repair
```

다음 명령을 사용하여 복제된 데이터의 복구를 추적할 수 있습니다.

```
repair-data show-replicated-repair-status
```

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-repair

repair-data start-ec-volume-repair
```

다음 명령을 사용하여 삭제 코딩 데이터의 복구를 추적할 수 있습니다.

```
repair-data show-ec-repair-status
```

일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 하지만 삭제 코딩 데이터를 모두 처리할 수 없는 경우 복구를 완료할 수 없습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

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. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 파일을 사용하여 `/etc/hosts` 복구된 스토리지 볼륨에 대한 스토리지 노드의 호스트 이름을 찾습니다. 그리드에 있는 모든 노드의 목록을 보려면 다음을 입력합니다 `cat /etc/hosts`.

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 볼륨에만 장애가 발생한 경우 로 이동합니다일부 볼륨만 장애가 발생한 경우 데이터를 복구합니다.

> 둘 이상의 노드에 대한 작업을 동시에 실행할 수 `repair-data` 없습니다. 여러 노드를 복구하려면 기술 지원 팀에 문의하십시오.

복제된 데이터

그리드에 복제된 데이터가 포함되어 있는 경우 `repair-data start-replicated-node-repair` 명령을 옵션(여기서 `--nodes` 는 호스트 이름(시스템 이름))과 함께 `--nodes` 사용하여 전체 스토리지 노드를 복구합니다.

이 명령은 SG-DC-SN3이라는 스토리지 노드에서 복제된 데이터를 복구합니다.

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> 개체 데이터가 복원되면 StorageGRID 시스템에서 복제된 개체 데이터를 찾을 수 없는 경우 * 개체 손실 * 경고가 트리거됩니다. 시스템 전체의 스토리지 노드에서 경고가 트리거될 수 있습니다. 손실의 원인과 복구가 가능한지 확인해야 합니다. 을 "손실된 개체를 조사합니다"참조하십시오.

삭제 코딩**(EC)** 데이터

그리드에 삭제 코딩 데이터가 포함되어 있는 경우 명령을 옵션과 함께 `--nodes` 사용합니다. 여기서 는 호스트 이름(시스템 이름) 옵션을 `--nodes` 사용하여 `repair-data start-ec-node-repair` 전체 스토리지 노드를 복구합니다.

이 명령은 이름이 SG-DC-SN3인 스토리지 노드에서 삭제 코딩 데이터를 복구합니다.

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

이 작업은 이 작업을 식별하는 `repair_data` 고유 을 `repair ID` 반환합니다. 이 버튼을 사용하여 `repair ID` 작업의 진행 상황과 결과를 `repair_data` 추적합니다. 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 볼륨에 오류가 발생한 경우 로 이동합니다모든 볼륨이 실패한 경우 데이터를 복구합니다.

볼륨 ID를 16진수로 입력합니다. 예를 들어 `0000`, 은 첫 번째 볼륨이고 `000F` 는 16번째 볼륨입니다. 하나의 볼륨, 하나의 볼륨 범위 또는 하나의 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 포함되어 있는 경우 `start-replicated-volume-repair` 명령을 옵션과 함께 `--nodes` 사용하여 노드를 식별합니다(여기서 `--nodes` 는 노드의 호스트 이름). 그런 다음 다음 다음 `--volumes` 예제와 같이 또는 `--volume-range` 옵션을 추가합니다.

- 단일 볼륨 *: 이 명령은 복제된 데이터를 SG-DC-SN3이라는 스토리지 노드의 볼륨에 복원합니다 `0002`.

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

- 볼륨 범위 *: 이 명령은 `0009` SG-DC-SN3이라는 이름의 스토리지 노드에 있는 범위 내의 모든 볼륨에 복제된 데이터를 복원합니다 `0003`.

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

*연속되지 않은 여러 볼륨 *: 이 명령은 복제된 데이터를 볼륨, `0005` `0008` SG-DC-SN3이라는 스토리지 노드에서 복원합니다. `0001`

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> 개체 데이터가 복원되면 StorageGRID 시스템에서 복제된 개체 데이터를 찾을 수 없는 경우 * 개체 손실 * 경고가 트리거됩니다. 시스템 전체의 스토리지 노드에서 경고가 트리거될 수 있습니다. 경고 설명 및 권장 조치를 참고하여 손실의 원인을 파악하고 복구가 가능한지 여부를 확인합니다.

삭제 코딩**(EC)** 데이터

그리드에 삭제 코딩 데이터가 포함되어 있는 경우 `start-ec-volume-repair` 명령을 옵션과 함께 `--nodes` 사용하여 노드를 식별합니다(여기서 `--nodes` 는 노드의 호스트 이름). 그런 다음 다음 다음 `--volumes` 예제와 같이 또는 `--volume-range` 옵션을 추가합니다.

- 단일 볼륨 *: 이 명령은 SG-DC-SN3이라는 이름의 스토리지 노드의 볼륨에 삭제 코딩 데이터를 복원합니다 `0007`.

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

- 볼륨 범위 *: 이 명령은 `0006` SG-DC-SN3이라는 이름의 스토리지 노드에 있는 범위 내의 모든 볼륨에 삭제 코딩 데이터를 복원합니다 `0004`.

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

*연속되지 않은 여러 볼륨 *: 이 명령은 삭제 코딩 데이터를 볼륨, `000C` `000E` SG-DC-SN3이라는 스토리지 노드에서 복원합니다. `000A`

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

`repair-data`이 작업은 이 작업을 식별하는 `repair_data` 고유 을 `repair ID` 반환합니다. 이 버튼을 사용하여 `repair ID` 작업의 진행 상황과 결과를 `repair_data` 추적합니다. 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.

또한 처리 중인 볼륨 복원 작업의 상태를 모니터링하고 에서 완료된 복원 작업의 기록을 볼 수 "그리드 관리자"있습니다.

복제된 데이터

- 복제된 복구의 예상 완료율을 얻으려면 repair-data 명령에 옵션을 추가합니다 `show-replicated-repair-status`.

```
repair-data show-replicated-repair-status
```

- 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.

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.
   - 다음 명령을 사용하여 특정 작업의 상태를 `repair-data` 확인합니다.

```
repair-data show-ec-repair-status --repair-id repair ID
```

   - 이 명령을 사용하여 모든 수리를 나열합니다.

```
repair-data show-ec-repair-status
```

출력에는 이전 및 현재 실행 중인 모든 수리에 대한 정보가 `repair ID` 표시됩니다.

2. 출력에 복구 작업이 실패했다고 표시되는 경우 옵션을 사용하여 `--repair-id` 복구를 재시도합니다.

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 노드 복구를 재시도합니다.

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 볼륨 복구를 다시 시도합니다.

   ```
   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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."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

스토리지 노드 시스템 드라이브 복구에 대한 경고

스토리지 노드의 장애가 발생한 시스템 드라이브를 복구하기 전에 일반 "그리드 노드 복구에 대한 경고 및 고려 사항"경고 및 다음 특정 경고를 검토하십시오.

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. 을 "기술 지원 부서에서 사이트를 복구하는 방법"참조하십시오.

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. 의 지침을 "시스템 드라이브가 손상되지 않은 스토리지 볼륨 장애로부터 복구합니다"참조하십시오.

ILM 규칙이 복제된 복사본을 하나만 저장하도록 구성되어 있고 해당 복사본이 실패한 스토리지 볼륨에 있으면 개체를 복구할 수 없습니다.

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. 에는 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"

플랫폼	절차를 참조하십시오
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 의 절차를 "Linux 노드 교체"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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.
- 프로비저닝 암호가 있습니다.
- 교체 노드를 구축하고 구성했습니다.
- 삭제 코딩 데이터에 대한 복구 작업의 시작 날짜가 있습니다.
- 스토리지 노드가 지난 15일 이내에 재구축되지 않은 것을 확인했습니다.

이 작업에 대해

스토리지 노드가 Linux 호스트에 컨테이너로 설치되어 있는 경우 다음 중 하나가 참인 경우에만 이 단계를 수행해야 합니다.

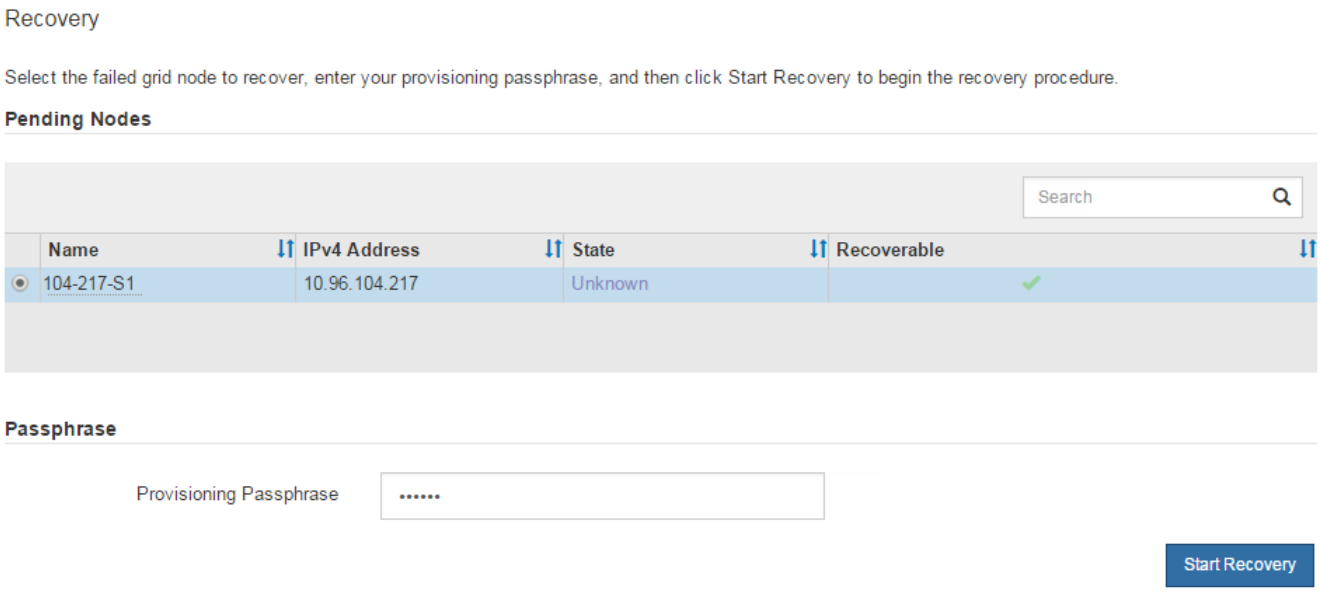
- 노드를 가져오기 위해 플래그를 사용해야 `--force` 하거나 명령을 실행했습니다 `storagegrid node force-recovery node-name`
- 전체 노드를 다시 설치하거나 /var/local을 복원해야 했습니다.

단계

1. Grid Manager에서 * 유지보수 * > * 작업 * > * 복구 * 를 선택합니다.
2. Pending Nodes 목록에서 복구할 그리드 노드를 선택합니다.

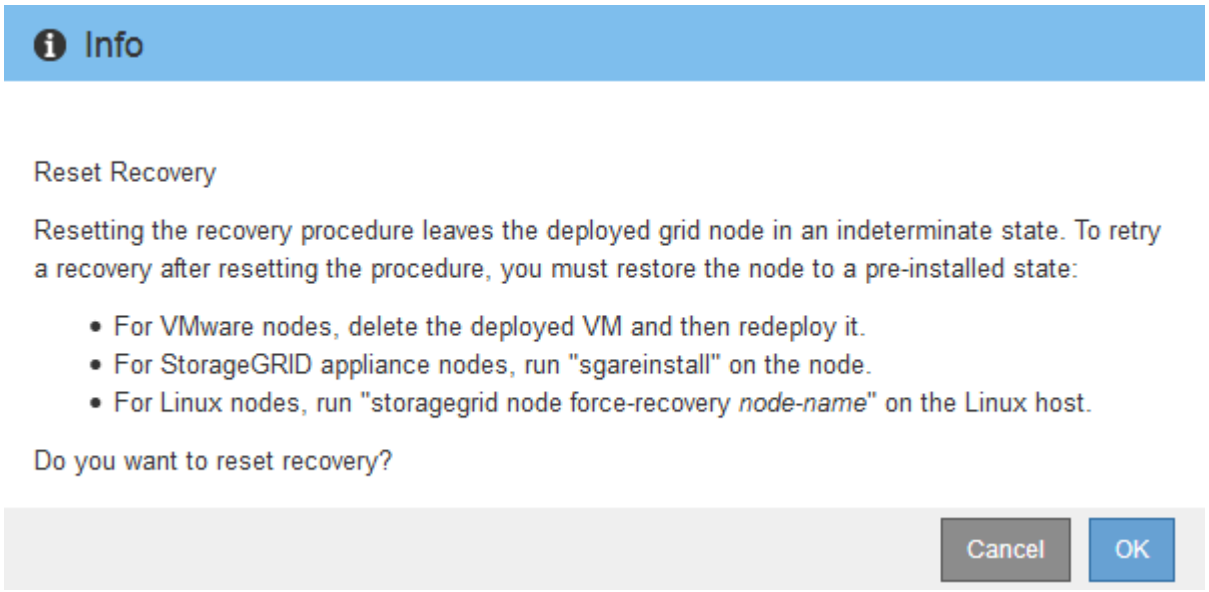
   노드가 실패한 후 목록에 나타나지만 다시 설치되고 복구 준비가 될 때까지 노드를 선택할 수 없습니다.

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 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 다음 명령을 실행하여 노드를 다시 시작합니다. `storagegrid node force-recovery node-name`

6. 스토리지 노드가 "수동 단계 대기 중" 단계에 도달하면 로 이동합니다"스토리지 볼륨 다시 마운트 및 다시 포맷(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.

시작하기 전에

- 장애가 발생한 스토리지 볼륨의 하드웨어를 교체하도록 이미 교체했습니다.

  스크립트를 실행하면 `sn-remount-volumes` 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. 스크립트를 실행하지 `sn-recovery-postinstall.sh` 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.
- `sn-remount-volumes`스크립트를 실행하여 올바르게 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 중에는 실패한 스토리지 볼륨을 다시 포맷하고 객체 메타데이터를 복구하기 위해 실행하기 전에 스토리지 노드를 재부팅하지 마십시오 `sn-recovery-postinstall.sh`. 완료되기 전에 스토리지 노드를 재부팅하면 `sn-recovery-postinstall.sh` 시작을 시도하고 StorageGRID 어플라이언스 노드가 유지보수 모드를 종료하는 서비스에 오류가 발생합니다. 의 단계를 설치 후 스크립트참조하십시오.

  - 스크립트가 마운트하지 못했거나 잘못 포맷된 스토리지 볼륨을 다시 `sn-remount-volumes` 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. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

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. 다음 스크립트를 실행합니다. `sn-remount-volumes`

      이 스크립트는 데이터가 포함된 스토리지 볼륨에서 실행되는 데 몇 시간이 걸릴 수 있습니다.

   b. 스크립트가 실행되면 출력을 검토하고 프롬프트에 응답합니다.

      필요한 경우 명령을 사용하여 스크립트의 로그 파일 내용을 모니터링할 수 `tail -f` (`/var/local/log/sn-remount-volumes.log` 있습니다. 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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't 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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't 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` XFS 파일 시스템 일관성 검사를 통과했으며 유효한 볼륨 구조가 있어 성공적으로 다시 마운트되었습니다. 스크립트에 의해 다시 마운트된 디바이스의 데이터는 보존됩니다.
- `/dev/sdc` 스토리지 볼륨이 새 볼륨이거나 손상되었기 때문에 XFS 파일 시스템 일관성 검사에 실패했습니다.
- `/dev/sdd` 디스크가 초기화되지 않았거나 디스크의 슈퍼블록이 손상되었기 때문에 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-remount-volumes.log` 로그 파일에 저장됩니다.
- `/dev/sde` XFS 파일 시스템 일관성 검사를 통과했으며 유효한 볼륨 구조를 가지고 있지만 volid 파일의 LDR 노드 ID가 이 스토리지 노드의 ID(맨 위에 표시됨)와 일치하지 `configured LDR noid` 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 대한 스크립트 실행의 의미를 이해해야 `sn-recovery-postinstall.sh` 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 의 출력에는 `/dev/sde` 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. 스크립트를 실행하면 `sn-recovery-postinstall.sh` 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. 이 ID는 스크립트를 실행하여 볼륨에 객체 데이터를 복원할 때 입력해야 `repair-data` 합니다(다음 절차).

d. 마운트 해제된 모든 디바이스를 복구하거나 교체한 후 `sn-remount-volumes` 스크립트를 다시 실행하여 다시 마운트할 수 있는 모든 스토리지 볼륨이 다시 마운트되었는지 확인합니다.

   스토리지 볼륨을 마운트할 수 없거나 잘못 포맷된 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.

장애가 발생한 스토리지 볼륨에 남아 있는 데이터를 그리드의 다른 위치에서 재구축할 수 없다고 생각하는 경우(예: ILM 정책이 하나의 복사본만 만드는 규칙을 사용하는 경우 또는 여러 노드에서 볼륨이 장애가 발생한 경우) 스크립트를 실행하지 마십시오 `sn-recovery-postinstall.sh`. 대신 기술 지원 부서에 문의하여 데이터 복구 방법을 확인하십시오.

4. `sn-recovery-postinstall.sh`다음 스크립트를 실행합니다. `sn-recovery-postinstall.sh`

   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.

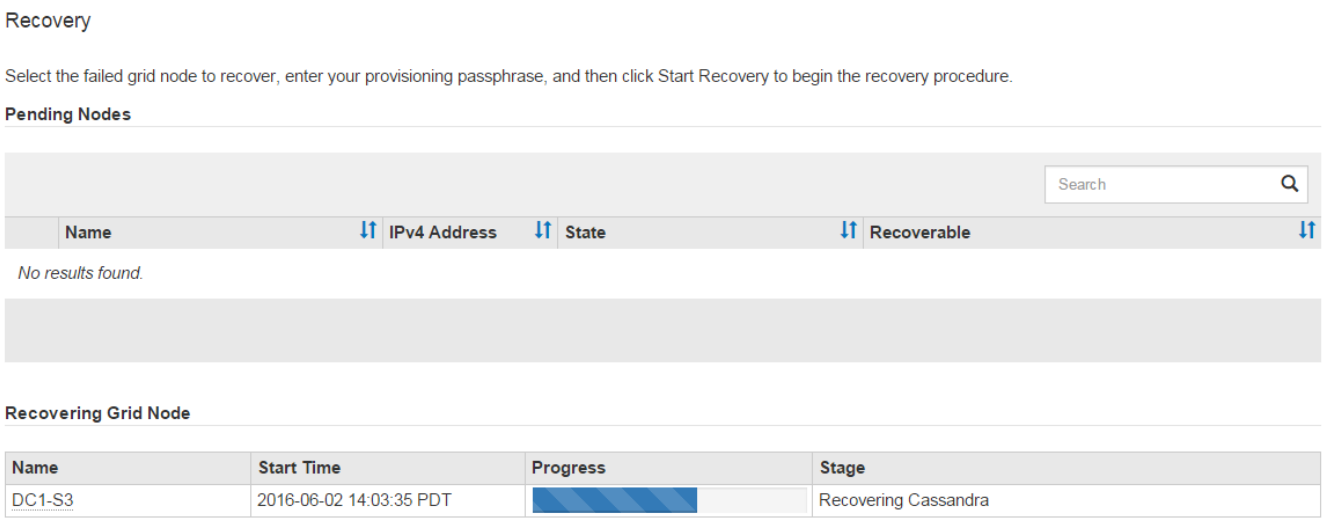
- SSH 세션이 활성화되어 있는 동안에는 * Ctrl + C * 를 누르지 마십시오.
- 네트워크 중단이 발생하여 SSH 세션을 종료하는 경우 스크립트는 백그라운드에서 실행되지만 복구 페이지에서 진행률을 볼 수 있습니다.
- 스토리지 노드가 RSM 서비스를 사용하는 경우 노드 서비스가 다시 시작됨에 따라 스크립트가 5분 동안 정지되는 것처럼 보일 수 있습니다. RSM 서비스가 처음 부팅될 때마다 5분 정도 지연될 수 있습니다.

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. "Reaper" 또는 "Cassandra repair"라는 스크립트 출력을 확인할 수 있습니다. 복구가 실패했음을 나타내는 오류 메시지가 표시되면 오류 메시지에 표시된 명령을 실행합니다.

5.] 스크립트가 실행되면 `sn-recovery-postinstall.sh` 그리드 관리자에서 복구 페이지를 모니터링합니다.

복구 페이지의 진행 표시줄과 단계 열은 스크립트의 상위 수준 상태를 `sn-recovery-postinstall.sh` 제공합니다.



6. 스크립트가 노드에서 서비스를 시작한 후에는 `sn-recovery-postinstall.sh` 스크립트로 포맷된 모든 스토리지 볼륨에 오브젝트 데이터를 복원할 수 있습니다.

이 스크립트는 Grid Manager 볼륨 복원 프로세스를 사용할 것인지 묻습니다.

- 대부분의 경우, 당신은 해야 "Grid Manager를 사용하여 개체 데이터를 복원합니다"합니다. 대답은 `y` 그리드 관리자를 사용합니다.
- 기술 지원 부서의 지시가 있거나 교체 노드에 원래 노드보다 오브젝트 스토리지에 사용할 수 있는 볼륨 수가 적다는 것을 알고 있는 경우 `repair-data`스크립트를 사용해야 합니다."개체 데이터를 수동으로 복원합니다" 이러한 경우 중 하나가 적용되면 답변합니다 `n`.

Grid Manager 볼륨 복원 프로세스 사용에 대한 대답인 경우 `n`(개체 데이터를 수동으로 복원):

- Grid Manager를 사용하여 개체 데이터를 복원할 수 없습니다.
- Grid Manager를 사용하여 수동 복원 작업의 진행률을 모니터링할 수 있습니다.

선택한 후에는 스크립트가 완료되고 객체 데이터를 복구하는 다음 단계가 표시됩니다. 이러한 단계를 검토한 후 아무 키나 눌러 명령줄로 돌아갑니다.

오브젝트 데이터를 스토리지 볼륨으로 복원(시스템 드라이브 장애)

비어플라이언스 스토리지 노드의 스토리지 볼륨을 복구한 후에는 스토리지 노드에 장애가 발생할 때 손실된 복제 또는 삭제 코딩 오브젝트 데이터를 복구할 수 있습니다.

어떤 절차를 사용해야 합니까?

가능한 경우 그리드 관리자의 * 볼륨 복원 * 페이지를 사용하여 개체 데이터를 복원합니다.

- 볼륨이 * 유지 관리 * > * 볼륨 복원 * > * 에 나열되어 있는 경우 * 복원할 노드 * 는 를 사용하여 오브젝트 데이터를 복원합니다."Grid Manager의 볼륨 복원 페이지"
- 볼륨이 * 유지 관리 * > * 볼륨 복원 * > * 복원할 노드 * 에 표시되지 않으면 스크립트를 사용하여 오브젝트 데이터를 복원하는 다음 단계를 따르십시오. `repair-data`

  복구된 스토리지 노드에 교체 중인 노드보다 적은 수의 볼륨이 포함된 경우 스크립트를 사용해야 `repair-data` 합니다.

repair-data 스크립트는 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다. 가능하면 를 사용합니다"Grid Manager(그리드 관리자)의 볼륨 복원 절차".

스크립트를 사용하여 `repair-data` 객체 데이터를 복원합니다

시작하기 전에

- 복구된 스토리지 노드의 그리드 관리자의 * nodes * > * Overview * 탭에서 연결 상태가 * Connected * 인 것을 확인했습니다.

이 작업에 대해

개체 복사본을 사용할 수 있도록 그리드의 ILM 규칙이 구성되어 있다고 가정하면 다른 스토리지 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.

스크립트 정보를 참조하십시오 `repair-data`

객체 데이터를 복원하려면 `repair-data` 스크립트를 실행합니다. 이 스크립트는 개체 데이터 복원 프로세스를 시작하고 ILM 스캔 작업을 통해 ILM 규칙이 충족되는지 확인합니다.

아래의 * 복제 데이터 * 또는 * 삭제 코딩(EC) 데이터 * 를 선택하여 복제된 데이터를 복원하는지 또는 삭제 코딩 데이터를 복원하는지 여부에 따라 스크립트에 대한 다양한 옵션을 `repair-data` 확인하십시오. 두 유형의 데이터를

모두 복원해야 하는 경우 두 명령 집합을 모두 실행해야 합니다.

스크립트에 대한 자세한 내용을 `repair-data` 보려면 기본 관리자 노드의 명령줄에서 를 `repair-data --help` 입력합니다.

repair-data 스크립트는 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다. 가능하면 를 사용합니다"Grid Manager(그리드 관리자)의 볼륨 복원 절차".

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

repair-data start-replicated-volume-repair
```

다음 명령을 사용하여 복제된 데이터의 복구를 추적할 수 있습니다.

```
repair-data show-replicated-repair-status
```

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-repair

repair-data start-ec-volume-repair
```

다음 명령을 사용하여 삭제 코딩 데이터의 복구를 추적할 수 있습니다.

```
repair-data show-ec-repair-status
```

일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 하지만 삭제 코딩 데이터를 모두 처리할 수 없는 경우 복구를 완료할 수 없습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

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. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 파일을 사용하여 `/etc/hosts` 복구된 스토리지 볼륨에 대한 스토리지 노드의 호스트 이름을 찾습니다. 그리드에 있는 모든 노드의 목록을 보려면 다음을 입력합니다 `cat /etc/hosts`.

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 볼륨에만 장애가 발생한 경우 로 이동합니다일부 볼륨만 장애가 발생한 경우 데이터를 복구합니다.

> 둘 이상의 노드에 대한 작업을 동시에 실행할 수 `repair-data` 없습니다. 여러 노드를 복구하려면 기술 지원 팀에 문의하십시오.

복제된 데이터

그리드에 복제된 데이터가 포함되어 있는 경우 `repair-data start-replicated-node-repair` 명령을 옵션(여기서 `--nodes` 는 호스트 이름(시스템 이름))과 함께 `--nodes` 사용하여 전체 스토리지 노드를 복구합니다.

이 명령은 SG-DC-SN3이라는 스토리지 노드에서 복제된 데이터를 복구합니다.

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> 개체 데이터가 복원되면 StorageGRID 시스템에서 복제된 개체 데이터를 찾을 수 없는 경우 * 개체 손실 * 경고가 트리거됩니다. 시스템 전체의 스토리지 노드에서 경고가 트리거될 수 있습니다. 손실의 원인과 복구가 가능한지 확인해야 합니다. 을 "손실된 개체를 조사합니다"참조하십시오.

삭제 코딩**(EC)** 데이터

그리드에 삭제 코딩 데이터가 포함되어 있는 경우 명령을 옵션과 함께 `--nodes` 사용합니다. 여기서 는 호스트 이름(시스템 이름) 옵션을 `--nodes` 사용하여 `repair-data start-ec-node-repair` 전체 스토리지 노드를 복구합니다.

이 명령은 이름이 SG-DC-SN3인 스토리지 노드에서 삭제 코딩 데이터를 복구합니다.

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

이 작업은 이 작업을 식별하는 `repair_data` 고유 을 `repair ID` 반환합니다. 이 버튼을 사용하여 `repair ID` 작업의 진행 상황과 결과를 `repair_data` 추적합니다. 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 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 볼륨에 오류가 발생한 경우 로 이동합니다모든 볼륨이 실패한 경우 데이터를 복구합니다.

볼륨 ID를 16진수로 입력합니다. 예를 들어 `0000`, 은 첫 번째 볼륨이고 `000F` 는 16번째 볼륨입니다. 하나의 볼륨, 하나의 볼륨 범위 또는 하나의 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 포함되어 있는 경우 `start-replicated-volume-repair` 명령을 옵션과 함께 `--nodes` 사용하여 노드를 식별합니다(여기서 `--nodes` 는 노드의 호스트 이름). 그런 다음 다음 다음 `--volumes` 예제와 같이 또는 `--volume-range` 옵션을 추가합니다.

- 단일 볼륨 *: 이 명령은 복제된 데이터를 SG-DC-SN3이라는 스토리지 노드의 볼륨에 복원합니다 `0002`.

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

- 볼륨 범위 *: 이 명령은 `0009` SG-DC-SN3이라는 이름의 스토리지 노드에 있는 범위 내의 모든 볼륨에 복제된 데이터를 복원합니다 `0003`.

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

*연속되지 않은 여러 볼륨 *: 이 명령은 복제된 데이터를 볼륨, `0005` `0008` SG-DC-SN3이라는 스토리지 노드에서 복원합니다. `0001`

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> 개체 데이터가 복원되면 StorageGRID 시스템에서 복제된 개체 데이터를 찾을 수 없는 경우 * 개체 손실 * 경고가 트리거됩니다. 시스템 전체의 스토리지 노드에서 경고가 트리거될 수 있습니다. 경고 설명 및 권장 조치를 참고하여 손실의 원인을 파악하고 복구가 가능한지 여부를 확인합니다.

삭제 코딩**(EC)** 데이터

그리드에 삭제 코딩 데이터가 포함되어 있는 경우 `start-ec-volume-repair` 명령을 옵션과 함께 `--nodes` 사용하여 노드를 식별합니다(여기서 `--nodes` 는 노드의 호스트 이름). 그런 다음 다음 다음 `--volumes` 예제와 같이 또는 `--volume-range` 옵션을 추가합니다.

- 단일 볼륨 *: 이 명령은 SG-DC-SN3이라는 이름의 스토리지 노드의 볼륨에 삭제 코딩 데이터를 복원합니다 `0007`.

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

- 볼륨 범위 *: 이 명령은 `0006` SG-DC-SN3이라는 이름의 스토리지 노드에 있는 범위 내의 모든 볼륨에 삭제 코딩 데이터를 복원합니다 `0004`.

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

*연속되지 않은 여러 볼륨 *: 이 명령은 삭제 코딩 데이터를 볼륨, `000C` `000E` SG-DC-SN3이라는 스토리지 노드에서 복원합니다. `000A`

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

`repair-data`이 작업은 이 작업을 식별하는 `repair_data` 고유 을 `repair ID` 반환합니다. 이 버튼을 사용하여 `repair ID` 작업의 진행 상황과 결과를 `repair_data` 추적합니다. 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.

또한 처리 중인 볼륨 복원 작업의 상태를 모니터링하고 에서 완료된 복원 작업의 기록을 볼 수 "그리드 관리자"있습니다.

복제된 데이터

- 복제된 복구의 예상 완료율을 얻으려면 repair-data 명령에 옵션을 추가합니다 `show-replicated-repair-status`.

  ```
  repair-data show-replicated-repair-status
  ```

- 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.

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.
   - 다음 명령을 사용하여 특정 작업의 상태를 `repair-data` 확인합니다.

     ```
     repair-data show-ec-repair-status --repair-id repair ID
     ```

   - 이 명령을 사용하여 모든 수리를 나열합니다.

     ```
     repair-data show-ec-repair-status
     ```

출력에는 이전 및 현재 실행 중인 모든 수리에 대한 정보가 `repair ID` 표시됩니다.

2. 출력에 복구 작업이 실패했다고 표시되는 경우 옵션을 사용하여 `--repair-id` 복구를 재시도합니다.

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 노드 복구를 재시도합니다.

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 볼륨 복구를 다시 시도합니다.

   ```
   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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."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.

Grid Manager를 사용하여 개체 데이터를 복원합니다

Grid Manager를 사용하여 장애가 발생한 스토리지 볼륨 또는 스토리지 노드에 대한 객체 데이터를 복구할 수 있습니다. 또한 Grid Manager를 사용하여 진행 중인 복원 프로세스를 모니터링하고 복원 기록을 표시할 수도 있습니다.

시작하기 전에

- 다음 절차 중 하나를 수행하여 장애가 발생한 볼륨을 포맷했습니다.
  - "어플라이언스 스토리지 볼륨 다시 마운트 및 다시 포맷(수동 단계)"

- "스토리지 볼륨 다시 마운트 및 다시 포맷(수동 단계)"

- 오브젝트를 복원할 스토리지 노드의 그리드 관리자의 * nodes * > * Overview * 탭에서 연결 상태 * Connected * 가 있는지 확인했습니다.
- 다음 사항을 확인했습니다.
  - 스토리지 노드를 추가하기 위한 그리드 확장이 진행 중이 아닙니다.
  - 스토리지 노드 해제가 진행 중이거나 실패했습니다.
  - 실패한 스토리지 볼륨의 복구가 진행 중입니다.
  - 장애가 발생한 시스템 드라이브가 있는 스토리지 노드 복구가 진행 중이 아닙니다.
  - EC 재조정 작업이 진행 중이 아닙니다.
  - 어플라이언스 노드 클로닝이 진행 중이 아닙니다.

이 작업에 대해

드라이브를 교체하고 볼륨을 포맷하기 위한 수동 단계를 수행한 후 Grid Manager는 볼륨을 * 유지보수 * > * 볼륨 복원 * > * 복원할 노드 * 탭에서 복원 대상으로 표시합니다.

가능한 경우 그리드 관리자의 볼륨 복원 페이지를 사용하여 오브젝트 데이터를 복원합니다. 또는 볼륨을 복원할 준비가 되면 볼륨 복원을 자동으로 시작할 수 자동 복원 모드를 활성화합니다수동으로 볼륨 복원을 수행합니다있습니다. 다음 지침을 따르십시오.

- 볼륨이 * 유지보수 * > * 볼륨 복원 * > * 복원할 노드 * 에 나열되면 아래 단계에 설명된 대로 개체 데이터를 복원합니다. 다음과 같은 경우 볼륨이 나열됩니다.
  - 노드의 일부 스토리지 볼륨에 장애가 발생했습니다
  - 노드의 모든 스토리지 볼륨이 장애가 발생했으며 같은 수의 볼륨 또는 더 많은 볼륨으로 대체되고 있습니다

  Grid Manager(그리드 관리자)의 Volume restoration(볼륨 복원복원 기록을 봅니다) 페이지에서 및 을(를) 수행할 수도 볼륨 복원 프로세스를 모니터링합니다있습니다.

- 그리드 관리자에 볼륨이 복원 대상으로 나열되지 않은 경우 스크립트를 사용하여 객체 데이터를 복원하는 적절한 단계를 따르십시오 `repair-data`.
  - "오브젝트 데이터를 스토리지 볼륨에 복원(시스템 드라이브 장애)"
  - "시스템 드라이브가 손상되지 않은 스토리지 볼륨에 개체 데이터를 복원합니다"
  - "어플라이언스의 스토리지 볼륨에 오브젝트 데이터를 복원합니다"

  > repair-data 스크립트는 더 이상 사용되지 않으며 향후 릴리즈에서 제거될 예정입니다.

  복구된 스토리지 노드에 교체 중인 노드보다 적은 수의 볼륨이 포함된 경우 스크립트를 사용해야 `repair-data` 합니다.

다음과 같은 두 가지 유형의 오브젝트 데이터를 복원할 수 있습니다.

- 그리드의 ILM 규칙이 오브젝트 복사본을 사용할 수 있도록 구성되었다고 가정할 때 복제된 데이터 오브젝트는 다른 위치에서 복원됩니다.
  - 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.

- 삭제 코딩(EC) 데이터 오브젝트는 저장된 조각을 재조립하여 복원합니다. 손상되거나 손실된 조각은 나머지 데이터 및 패리티 조각에서 삭제 코딩 알고리즘을 통해 다시 생성됩니다.

  일부 스토리지 노드가 오프라인인 상태에서 삭제 코딩 데이터 복구를 시작할 수 있습니다. 하지만 삭제 코딩된 모든 데이터를 설명할 수 없는 경우에는 복구를 완료할 수 없습니다. 모든 노드를 사용할 수 있게 되면 복구가 완료됩니다.

볼륨 복구는 오브젝트 복사본이 저장되는 리소스의 가용성에 따라 달라집니다. 볼륨 복원 진행은 비선형적이며 완료하는 데 며칠 또는 몇 주가 걸릴 수 있습니다.

] 자동 복원 모드를 활성화합니다

자동 복원 모드를 활성화하면 볼륨을 복원할 준비가 되면 볼륨 복원이 자동으로 시작됩니다.

단계

1. Grid Manager에서 * 유지 관리 * > * 볼륨 복원 * 으로 이동합니다.
2. 복원할 노드 * 탭을 선택한 다음 * 자동 복원 모드 * 의 토글을 활성화된 위치로 밉니다.
3. 확인 대화 상자가 나타나면 세부 정보를 검토합니다.

   - 모든 노드에서 볼륨 복원 작업을 수동으로 시작할 수 없습니다.
   - 다른 유지 보수 절차가 진행 중인 경우에만 볼륨 복구가 자동으로 시작됩니다.
   - 진행률 모니터링 페이지에서 작업의 상태를 모니터링할 수 있습니다.
   - StorageGRID는 시작되지 않은 볼륨 복원을 자동으로 재시도합니다.

4. 자동 복원 모드를 활성화한 결과를 이해하면 확인 대화 상자에서 * 예 * 를 선택합니다.

   언제든지 자동 복원 모드를 비활성화할 수 있습니다.

장애가 발생한 볼륨 또는 노드를 수동으로 복원합니다

장애가 발생한 볼륨 또는 노드를 복원하려면 다음 단계를 수행하십시오.

단계

1. Grid Manager에서 * 유지 관리 * > * 볼륨 복원 * 으로 이동합니다.
2. 복원할 노드 * 탭을 선택한 다음 * 자동 복원 모드 * 의 토글을 비활성 위치로 밉니다.

   탭의 숫자는 복원이 필요한 볼륨의 노드 수를 나타냅니다.

3. 각 노드를 확장하여 복원이 필요한 IT 볼륨의 볼륨과 상태를 확인합니다.
4. 각 볼륨의 복원을 방해하는 모든 문제를 해결합니다. 볼륨 상태로 표시되는 경우 * 수동 단계 대기 * 를 선택하면 문제가 표시됩니다.
5. 모든 볼륨이 복구 준비 상태를 나타내는 노드를 선택하여 복원합니다.

한 번에 하나의 노드에 대한 볼륨만 복원할 수 있습니다.

노드의 각 볼륨은 복원 준비가 되었음을 나타내야 합니다.

6. 복원 시작 * 을 선택합니다.
7. 나타날 수 있는 경고를 모두 다루거나 * 그래도 시작 * 을 선택하여 경고를 무시하고 복원을 시작합니다.

복원을 시작할 때 * 복원할 노드 * 탭에서 * 복원 진행률 * 탭으로 노드가 이동됩니다.

볼륨 복원을 시작할 수 없는 경우 노드는 복원할 * 노드 탭으로 돌아갑니다.

복원 진행 상황을 봅니다

복원 진행률 * 탭은 볼륨 복원 프로세스의 상태와 복원 중인 노드의 볼륨에 대한 정보를 표시합니다.

모든 볼륨에서 복제 및 삭제 코딩 개체의 데이터 복구 속도는 스크립트를 사용하여 시작된 복구를 포함하여 처리 중인 모든 복구를 요약한 평균입니다. `repair-data` 손상되지 않았고 복원이 필요하지 않은 볼륨의 개체 비율도 표시됩니다.

> 복제된 데이터 복원은 복제된 복사본이 저장되는 리소스의 가용성에 따라 달라집니다. 복제된 데이터 복원 진행은 비선형적이며 완료하는 데 며칠 또는 몇 주가 걸릴 수 있습니다.

복원 작업 섹션에는 Grid Manager에서 시작된 볼륨 복원에 대한 정보가 표시됩니다.

- 복원 작업 섹션 제목의 숫자는 복원 중이거나 복원을 위해 대기 중인 볼륨의 수를 나타냅니다.
- 이 표에는 복구 중인 노드의 각 볼륨 및 진행 상황에 대한 정보가 표시됩니다.
  - 각 노드의 진행률은 각 작업의 백분율을 표시합니다.
  - 자세히 열을 확장하여 복원 시작 시간 및 작업 ID를 표시합니다.
- 볼륨 복원이 실패한 경우:
  - 상태 열에 가 표시되고 `failed (attempting retry)` 자동으로 재시도됩니다.
  - 여러 복원 작업이 실패한 경우 가장 최근의 작업이 먼저 자동으로 다시 시도됩니다.
  - 재시도가 계속 실패할 경우 * EC 복구 실패 * 경고가 트리거됩니다. 경고의 단계에 따라 문제를 해결합니다.

복원 이력을 조회한다

복원 기록 * 탭은 성공적으로 완료된 모든 볼륨 복원에 대한 정보를 표시합니다.

> 크기는 복제된 개체에 적용할 수 없으며 삭제 코딩(EC) 데이터 개체가 포함된 복원에만 나타납니다.

수리 - 데이터 작업을 모니터링합니다

명령줄의 스크립트를 사용하여 복구 작업의 상태를 모니터링할 수 `repair-data` 있습니다.

여기에는 수동으로 시작한 작업 또는 서비스 해제 절차의 일부로 StorageGRID가 자동으로 시작한 작업이 포함됩니다.

볼륨 복원 작업을 실행하는 경우 "진행 상황을 모니터링하고 Grid Manager에서 해당 작업의 기록을 확인합니다"대신

복제된 데이터 *, * 삭제 코딩(EC) 데이터 * 또는 둘 모두를 사용하는지 여부에 따라 작업 상태를 `repair-data` 모니터링합니다.

복제된 데이터

- 복제된 복구의 예상 완료율을 얻으려면 repair-data 명령에 옵션을 추가합니다 `show-replicated-repair-status`.

```
repair-data show-replicated-repair-status
```

- 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.

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.
   - 다음 명령을 사용하여 특정 작업의 상태를 `repair-data` 확인합니다.

```
repair-data show-ec-repair-status --repair-id repair ID
```

   - 이 명령을 사용하여 모든 수리를 나열합니다.

```
repair-data show-ec-repair-status
```

출력에는 이전 및 현재 실행 중인 모든 수리에 대한 정보가 `repair ID` 표시됩니다.

2. 출력에 복구 작업이 실패했다고 표시되는 경우 옵션을 사용하여 `--repair-id` 복구를 재시도합니다.

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 노드 복구를 재시도합니다.

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   이 명령은 복구 ID 6949309319275667690을 사용하여 실패한 볼륨 복구를 다시 시도합니다.

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

관리자 노드 오류에서 복구

기본 또는 비기본 관리자 노드 복구

관리 노드의 복구 프로세스는 기본 관리 노드인지 또는 비기본 관리 노드인지에 따라 달라집니다.

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.

선택

- "운영 관리 노드 오류에서 복구"
- "운영 관리자 노드가 아닌 노드에서 복구합니다"

운영 관리 노드 오류에서 복구

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.

> 장애가 발생한 운영 관리자 노드를 즉시 복구하거나 교체해야 합니다. 그렇지 않으면 그리드에서 새 오브젝트를 수집하는 기능이 상실될 수 있습니다. 정확한 기간은 개체 수집 속도에 따라 다릅니다. 그리드에 대한 기간을 더 정확하게 평가하려면 기술 지원 부서에 문의하십시오.

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.

기본 관리자 노드를 복구하려면 다음 상위 단계를 따르십시오.

1. "실패한 기본 관리 노드에서 감사 로그를 복사합니다"
2. "기본 관리자 노드를 교체합니다"

3. "교체용 기본 관리자 노드를 구성합니다"
4. "복구된 기본 관리자 노드에 대한 핫픽스 요구 사항이 있는지 확인합니다"
5. "복구된 기본 관리자 노드에서 감사 로그를 복원합니다"
6. "기본 관리자 노드를 복구할 때 관리자 노드 데이터베이스를 복구합니다"
7. "기본 관리자 노드를 복구할 때 Prometheus 메트릭을 복원합니다"

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 작업에 대해

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.

> 지금 실패한 관리 노드에서 감사 로그에 액세스할 수 없는 경우 호스트 복구 후 나중에 감사 로그에 액세스할 수 있습니다.

단계

1. 가능한 경우 실패한 관리 노드에 로그인합니다. 그렇지 않으면 기본 관리자 노드 또는 다른 관리자 노드(있는 경우)에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

      루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.
2. AMS 서비스를 중지하면 새 로그 파일이 생성되지 않습니다.`service ams stop`
3. 감사 내보내기 디렉터리로 이동합니다.

   ```
   cd /var/local/log
   ```

4. 원본 파일의 이름을 `audit.log` 번호가 매겨진 고유한 파일 이름으로 바꿉니다. 예를 들어, audit.log 파일의 이름을 로 `2023-10-25.txt.1`변경합니다.

   ```
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```

5. AMS 서비스를 다시 시작합니다. `service ams start`
6. 디렉토리를 생성하여 모든 감사 로그 파일을 별도의 그리드 노드의 임시 위치에 복사합니다. `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   메시지가 표시되면 admin의 암호를 입력합니다.

7. 모든 감사 로그 파일을 임시 위치에 복사: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   메시지가 표시되면 admin의 암호를 입력합니다.

8. 루트로 로그아웃: `exit`

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"
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 의 절차를 "Linux 노드 교체"따릅니다.

대체 운영 관리자 노드를 구성합니다

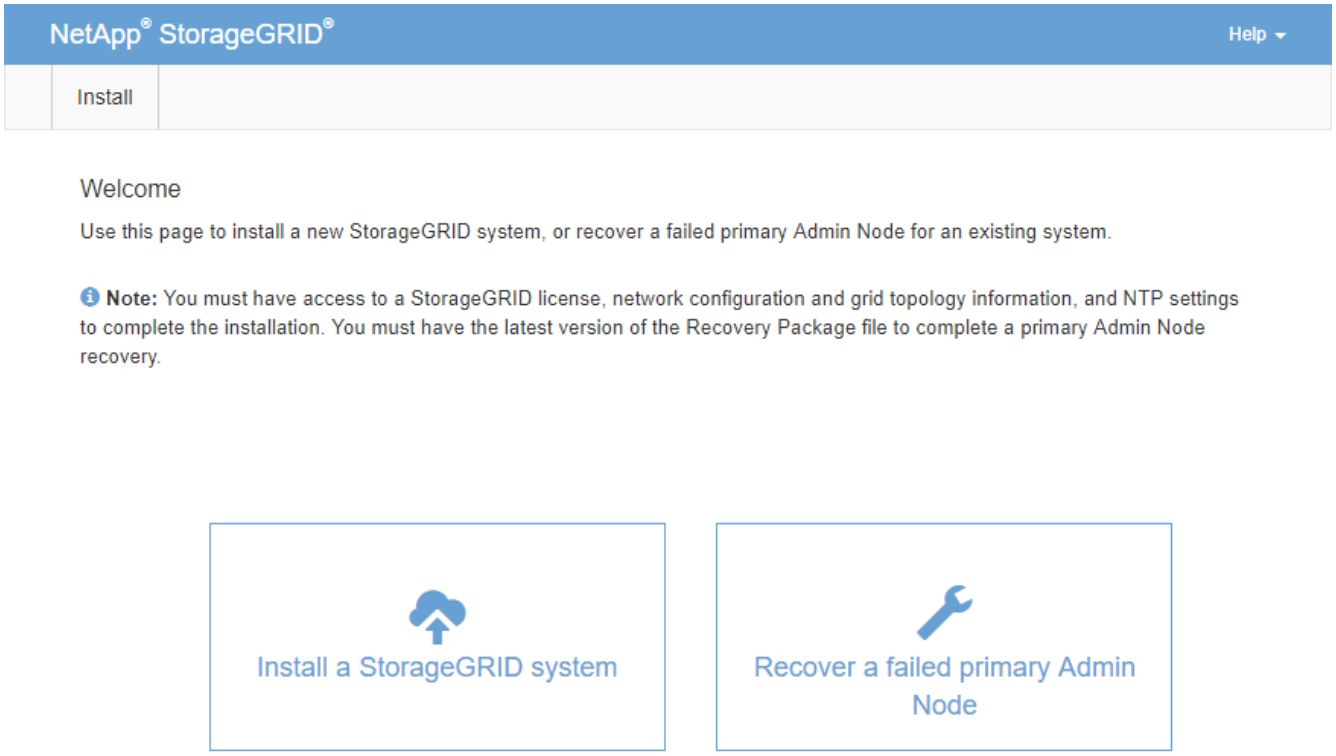
교체 노드는 StorageGRID 시스템의 기본 관리 노드로 구성해야 합니다.

시작하기 전에

- 가상 시스템에서 호스팅되는 운영 관리 노드의 경우 가상 머신이 구축, 전원 켜기 및 초기화되었습니다.
- 서비스 어플라이언스에서 호스팅되는 운영 관리 노드의 경우 어플라이언스를 교체하고 소프트웨어를 설치했습니다. 를 "어플라이언스에 대한 설치 지침"참조하십시오.
- 복구 패키지 파일의 최신 백업이 있는 (`sgws-recovery-package-*id-revision*.zip`경우).
- 프로비저닝 암호가 있습니다.

단계

1. 웹 브라우저를 열고 로 이동합니다 `https://primary_admin_node_ip`.
2. 필요에 따라 임시 설치 관리자 암호를 관리합니다.
   - 이러한 방법 중 하나를 사용하여 암호를 이미 설정한 경우 암호를 입력하여 계속 진행합니다.
     - 사용자가 이전에 설치 프로그램에 액세스하는 동안 암호를 설정했습니다
     - 베어 메탈 시스템의 경우, 에서 노드 구성 파일에서 암호를 자동으로 가져왔습니다 `/etc/storagegrid/nodes/<node_name>.conf`
     - VM의 경우 OVF 속성에서 SSH/콘솔 암호를 자동으로 가져왔습니다
   - 암호를 설정하지 않은 경우 StorageGRID 설치 프로그램을 보호할 암호를 선택적으로 설정합니다.
3. 실패한 운영 관리자 노드 복구 * 를 클릭합니다.



4. 복구 패키지의 최신 백업 업로드:
   a. 찾아보기 * 를 클릭합니다.
   b. StorageGRID 시스템에 대한 최신 복구 패키지 파일을 찾아 * 열기 * 를 클릭합니다.
5. 프로비저닝 암호를 입력합니다.
6. 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.

7. 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.

종속 당사자 트러스트를 구성하려면 을 참조하십시오"Single Sign-On 구성". 기본 서버 인증서에 액세스하려면 관리 노드의 명령 셸에 로그인합니다. 디렉터리로 `server.crt` 이동하여 `/var/local/mgmt-api` 파일을 선택합니다.

운영 관리 노드를 복구한 후,"핫픽스를 적용해야 하는지 확인합니다"

기본 관리자 노드에 대한 핫픽스 요구 사항을 결정합니다

기본 관리 노드를 복구한 후 핫픽스를 적용해야 하는지 확인합니다.

시작하기 전에

기본 관리 노드 복구가 완료되었습니다.

단계

1. 을 사용하여 그리드 관리자에 "지원되는 웹 브라우저"로그인합니다.
2. 노드 * 를 선택합니다.
3. 왼쪽 목록에서 기본 관리 노드를 선택합니다.
4. 개요 탭의 * 소프트웨어 버전 * 필드에 표시된 버전을 확인합니다.
5. 다른 그리드 노드를 선택합니다.
6. 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 복구된 기본 관리자 노드를 동일한 버전으로 업데이트해야 "핫픽스를 적용합니다"합니다.

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.

시작하기 전에

- 복구된 관리자 노드가 설치되고 실행 중입니다.
- 원래 관리 노드에 장애가 발생한 후 감사 로그를 다른 위치로 복사했습니다.

이 작업에 대해

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.

자세한 내용은 을 "감사 메시지 및 로그 대상을 구성합니다" 참조하십시오.

단계

1. 복구된 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@recovery_Admin_Node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.
2. 보존된 감사 파일 확인: `cd /var/local/log`
3. 보존된 감사 로그 파일을 복구된 관리자 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 관리자 노드에서 감사 로그 파일의 사용자 및 그룹 설정을 업데이트합니다. `chown ams-user: bycast *`
6. 루트로 로그아웃: `exit`

운영 관리자 노드를 복구할 때 관리 노드 데이터베이스를 복구합니다

실패한 기본 관리자 노드에 대한 속성 및 경고에 대한 기록 정보를 유지하려면 관리자 노드 데이터베이스를 복원할 수 있습니다. StorageGRID 시스템에 다른 관리 노드가 포함된 경우에만 이 데이터베이스를 복원할 수 있습니다.

시작하기 전에

- 복구된 관리자 노드가 설치되고 실행 중입니다.
- StorageGRID 시스템에는 최소 2개의 관리 노드가 포함됩니다.
- `Passwords.txt`파일이 있습니다.
- 프로비저닝 암호가 있습니다.

이 작업에 대해

관리 노드에 장애가 발생하면 해당 관리 노드 데이터베이스에 저장된 기록 정보가 손실됩니다. 이 데이터베이스에는 다음 정보가 포함되어 있습니다.

- 알림 기록
- 노드 페이지의 레거시 스타일 차트에 사용되는 내역 특성 데이터입니다

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.

단계

1. 소스 관리 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
2. 소스 관리자 노드에서 MI 서비스를 중지합니다. `service mi stop`
3. 소스 관리자 노드에서 관리 애플리케이션 프로그램 인터페이스(mgmt-API) 서비스를 중지합니다. `service mgmt-api stop`
4. 복구된 관리자 노드에서 다음 단계를 완료합니다.
   a. 복구된 관리자 노드에 로그인합니다.
      i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
      ii. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
      iii. 다음 명령을 입력하여 루트로 전환합니다. `su -`
      iv. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   b. MI 서비스를 중지합니다. `service mi stop`
   c. mgmt-API 서비스 중지: `service mgmt-api stop`
   d. SSH 에이전트에 SSH 개인 키를 추가합니다. 다음을 입력합니다.`ssh-add`
   e. 파일에 나열된 SSH 액세스 암호를 `Passwords.txt` 입력합니다.
   f. 소스 관리자 노드에서 복구된 관리자 노드로 데이터베이스 복사: `/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.

다음을 입력합니다.`ssh-add -D`

5. 소스 관리자 노드에서 서비스를 다시 시작합니다. `service servermanager start`

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.

시작하기 전에

- 복구된 관리자 노드가 설치되고 실행 중입니다.
- StorageGRID 시스템에는 최소 2개의 관리 노드가 포함됩니다.
- `Passwords.txt`파일이 있습니다.
- 프로비저닝 암호가 있습니다.

이 작업에 대해

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.

단계

1. 소스 관리 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
2. 소스 관리자 노드에서 Prometheus 서비스를 중지합니다. `service prometheus stop`
3. 복구된 관리자 노드에서 다음 단계를 완료합니다.
   a. 복구된 관리자 노드에 로그인합니다.
      i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
      ii. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
      iii. 다음 명령을 입력하여 루트로 전환합니다. `su -`
      iv. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   b. Prometheus 서비스를 중지합니다. `service prometheus stop`

c. SSH 에이전트에 SSH 개인 키를 추가합니다. 다음을 입력합니다.`ssh-add`

d. 파일에 나열된 SSH 액세스 암호를 `Passwords.txt` 입력합니다.

e. 소스 관리자 노드에서 복구된 관리자 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. 다음을 입력합니다.`ssh-add -D`

4. 소스 관리자 노드에서 Prometheus 서비스를 다시 시작합니다.`service prometheus start`

운영 관리자 노드가 아닌 노드에서 복구합니다

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.

기본 관리자 노드가 아닌 노드를 복구하려면 다음 상위 단계를 따르십시오.

1. "장애가 발생한 비기본 관리자 노드에서 감사 로그를 복사합니다"
2. "기본 관리자 노드가 아닌 관리자 노드를 교체합니다"
3. "복구 시작 을 선택하여 비 기본 관리자 노드를 구성합니다"
4. "복구된 비기본 관리자 노드에서 감사 로그를 복원합니다"
5. "비기본 관리자 노드를 복구할 때 관리자 노드 데이터베이스를 복구합니다"
6. "비기본 관리자 노드를 복구할 때 Prometheus 메트릭을 복원합니다"

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.

> 지금 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. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.
2. AMS 서비스를 중지하면 새 로그 파일이 생성되지 않습니다.`service ams stop`
3. 감사 내보내기 디렉터리로 이동합니다.

   ```
   cd /var/local/log
   ```
4. 소스 audit.log 파일의 이름을 고유한 번호 지정 파일 이름으로 바꿉니다. 예를 들어, audit.log 파일의 이름을 로 `2023-10-25.txt.1`변경합니다.

   ```
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```
5. AMS 서비스를 다시 시작합니다. `service ams start`
6. 디렉토리를 생성하여 모든 감사 로그 파일을 별도의 그리드 노드의 임시 위치에 복사합니다. `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   메시지가 표시되면 admin의 암호를 입력합니다.
7. 모든 감사 로그 파일을 임시 위치에 복사: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   메시지가 표시되면 admin의 암호를 입력합니다.
8. 루트로 로그아웃: `exit`

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"
리눅스	"Linux 노드를 교체합니다"
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 의 절차를 "Linux 노드 교체"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.

시작하기 전에

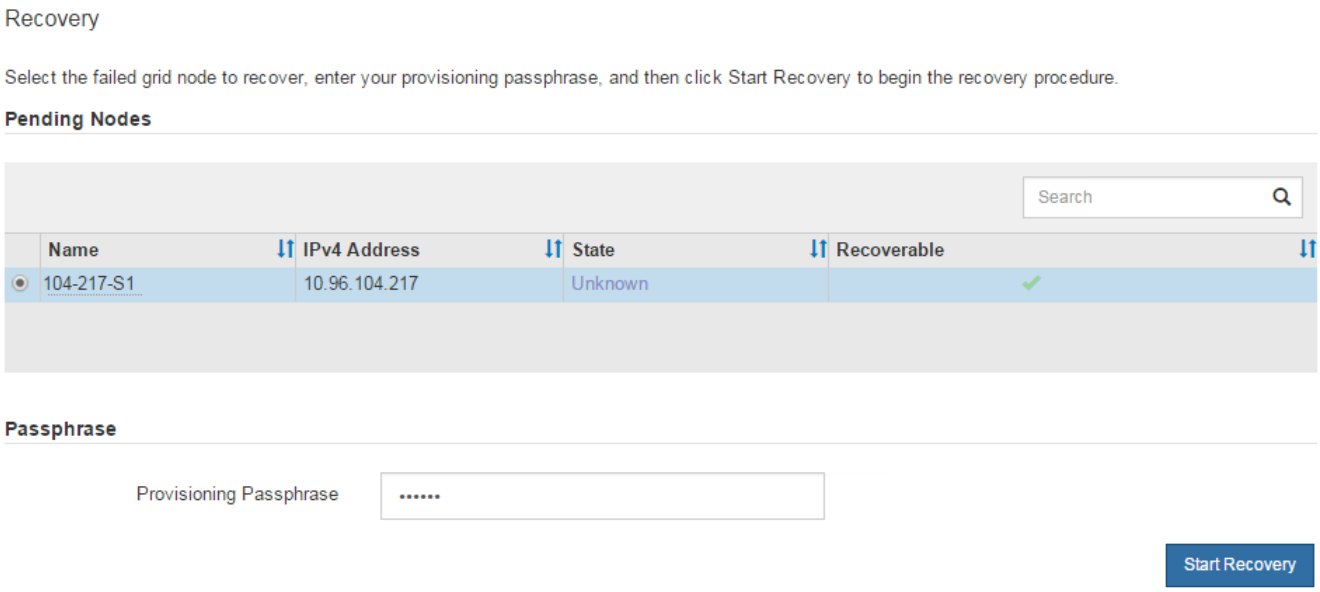
- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.
- 프로비저닝 암호가 있습니다.
- 교체 노드를 구축하고 구성했습니다.

단계

1. Grid Manager에서 * 유지보수 * > * 작업 * > * 복구 * 를 선택합니다.
2. Pending Nodes 목록에서 복구할 그리드 노드를 선택합니다.

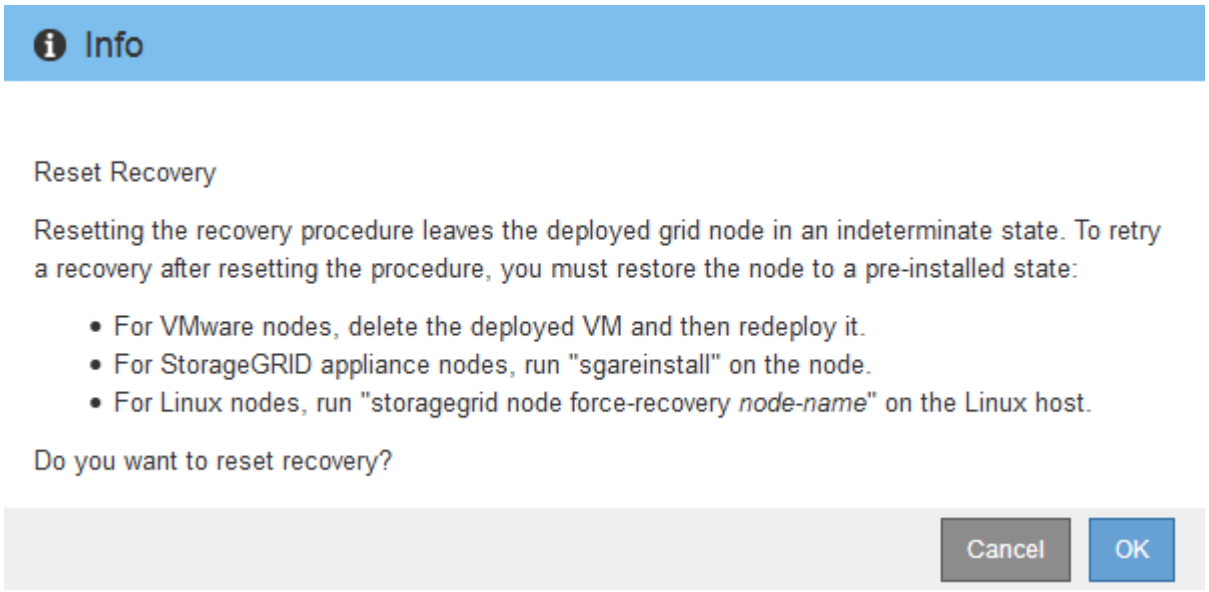
   노드가 실패한 후 목록에 나타나지만 다시 설치되고 복구 준비가 될 때까지 노드를 선택할 수 없습니다.

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 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 다음 명령을 실행하여 노드를 다시 시작합니다. `storagegrid node force-recovery node-name`
- * 어플라이언스 *: 절차를 재설정한 후 복구를 다시 시도하려면 노드에서 실행하여 어플라이언스 노드를 사전 설치된 상태로 복원해야 `sgareinstall` 합니다. 을 "어플라이언스 재설치 준비(플랫폼 교체만 해당)"참조하십시오.

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.

종속 당사자 트러스트를 구성하려면 을 참조하십시오"Single Sign-On 구성". 기본 서버 인증서에 액세스하려면 관리 노드의 명령 셸에 로그인합니다. 디렉터리로 `server.crt` 이동하여 `/var/local/mgmt-api` 파일을 선택합니다.

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.

시작하기 전에

- 복구된 관리자 노드가 설치되고 실행 중입니다.
- 원래 관리 노드에 장애가 발생한 후 감사 로그를 다른 위치로 복사했습니다.

이 작업에 대해

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.

자세한 내용은 을 "감사 메시지 및 로그 대상을 구성합니다" 참조하십시오.

단계

1. 복구된 관리자 노드에 로그인합니다.

   a. 다음 명령을 입력합니다.
   `ssh admin@recovery_Admin_Node_IP`

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. 어떤 감사 파일이 보존되었는지 확인합니다.

   ```
   cd /var/local/log
   ```

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 관리 노드에서 감사 로그 파일의 사용자 및 그룹 설정을 업데이트합니다.

   ```
   chown ams-user:bycast *
   ```

6. 루트로 로그아웃: `exit`

비운영 관리자 노드를 복구할 때 관리 노드 데이터베이스를 복원합니다

실패한 기본 관리자 노드가 아닌 관리자 노드에 대한 속성 및 경고에 대한 기록 정보를 보존하려면 기본 관리자 노드에서 관리자 노드 데이터베이스를 복구할 수 있습니다.

시작하기 전에

- 복구된 관리자 노드가 설치되고 실행 중입니다.
- StorageGRID 시스템에는 최소 2개의 관리 노드가 포함됩니다.
- `Passwords.txt`파일이 있습니다.
- 프로비저닝 암호가 있습니다.

이 작업에 대해

관리 노드에 장애가 발생하면 해당 관리 노드 데이터베이스에 저장된 기록 정보가 손실됩니다. 이 데이터베이스에는 다음 정보가 포함되어 있습니다.

- 알림 기록
- 노드 페이지의 레거시 스타일 차트에서 사용되는 내역 특성 데이터입니다

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.

단계

1. 소스 관리 노드에 로그인합니다.

a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

2. 소스 관리 노드에서 다음 명령을 실행합니다. 그런 다음 메시지가 나타나면 프로비저닝 암호를 입력합니다. `recover-access-points`

3. 소스 관리자 노드에서 MI 서비스를 중지합니다. `service mi stop`

4. 소스 관리자 노드에서 관리 애플리케이션 프로그램 인터페이스(mgmt-API) 서비스를 중지합니다. `service mgmt-api stop`

5. 복구된 관리자 노드에서 다음 단계를 완료합니다.

a. 복구된 관리자 노드에 로그인합니다.

i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

ii. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

iii. 다음 명령을 입력하여 루트로 전환합니다. `su -`

iv. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

b. MI 서비스를 중지합니다. `service mi stop`

c. mgmt-API 서비스 중지: `service mgmt-api stop`

d. SSH 에이전트에 SSH 개인 키를 추가합니다. 다음을 입력합니다.`ssh-add`

e. 파일에 나열된 SSH 액세스 암호를 `Passwords.txt` 입력합니다.

f. 소스 관리자 노드에서 복구된 관리자 노드로 데이터베이스 복사: `/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. 다음을 입력합니다.`ssh-add -D`

6. 소스 관리자 노드에서 서비스를 다시 시작합니다. `service servermanager start`

비운영 관리자 노드를 복구할 때 **Prometheus** 메트릭을 복원합니다

선택적으로, 장애가 발생한 비 운영 관리 노드에서 Prometheus가 유지 관리하는 기간별 메트릭을 유지할 수 있습니다.

시작하기 전에

- 복구된 관리자 노드가 설치되고 실행 중입니다.
- StorageGRID 시스템에는 최소 2개의 관리 노드가 포함됩니다.
- `Passwords.txt`파일이 있습니다.

- 프로비저닝 암호가 있습니다.

이 작업에 대해

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.

단계

1. 소스 관리 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
2. 소스 관리자 노드에서 Prometheus 서비스를 중지합니다. `service prometheus stop`
3. 복구된 관리자 노드에서 다음 단계를 완료합니다.
   a. 복구된 관리자 노드에 로그인합니다.
      i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
      ii. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
      iii. 다음 명령을 입력하여 루트로 전환합니다. `su -`
      iv. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
   b. Prometheus 서비스를 중지합니다. `service prometheus stop`
   c. SSH 에이전트에 SSH 개인 키를 추가합니다. 다음을 입력합니다.`ssh-add`
   d. 파일에 나열된 SSH 액세스 암호를 `Passwords.txt` 입력합니다.
   e. 소스 관리자 노드에서 복구된 관리자 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. 다음을 입력합니다.`ssh-add -D`

4. 소스 관리자 노드에서 Prometheus 서비스를 다시 시작합니다.`service prometheus start`

게이트웨이 노드에서 복구

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"
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 의 절차를 "Linux 노드 교체"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.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.
- 프로비저닝 암호가 있습니다.
- 교체 노드를 구축하고 구성했습니다.

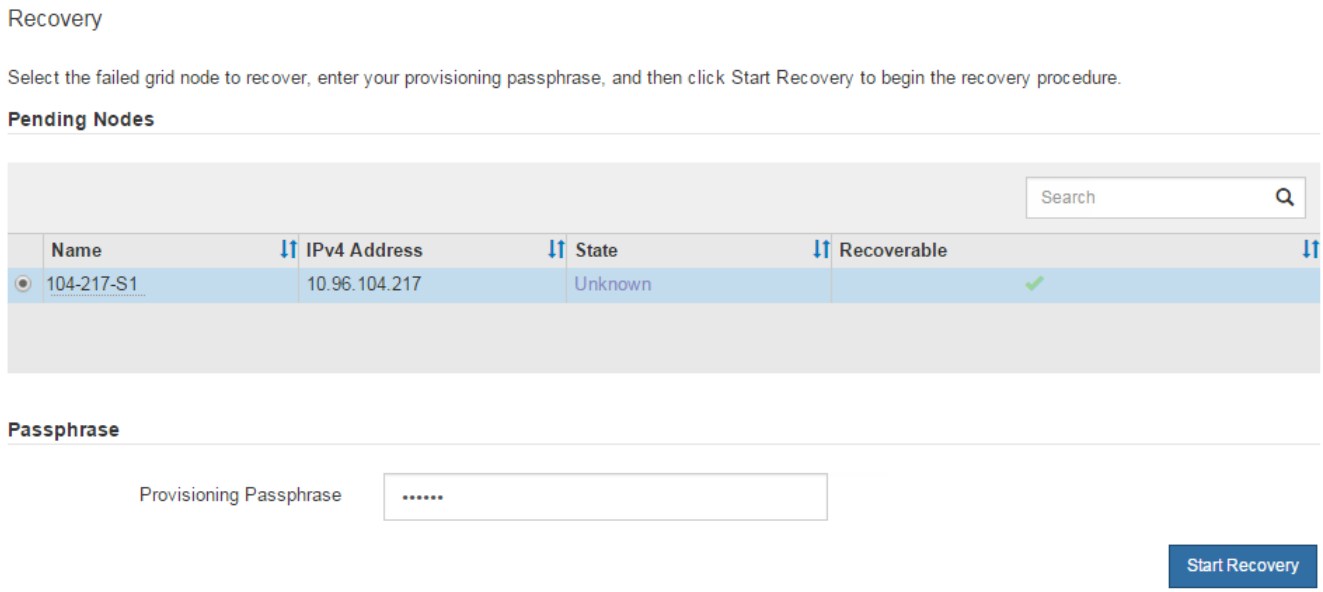
단계

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.

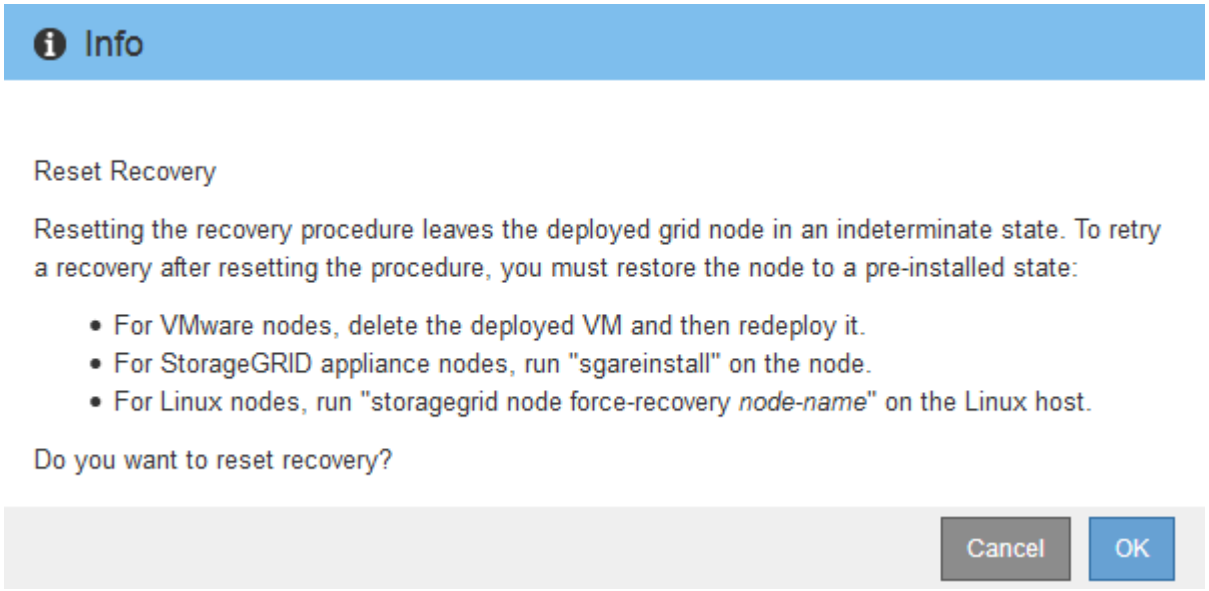
3. Provisioning Passphrase * 를 입력합니다.

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 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 다음 명령을 실행하여 노드를 다시 시작합니다. `storagegrid node force-recovery node-name`
- * 어플라이언스 *: 절차를 재설정한 후 복구를 다시 시도하려면 노드에서 실행하여 어플라이언스 노드를 사전 설치된 상태로 복원해야 `sgareinstall` 합니다. 을 "어플라이언스 재설치 준비(플랫폼 교체만 해당)"참조하십시오.

아카이브 노드 장애에서 복구

아카이브 노드 장애에서 복구

아카이브 노드에 대한 지원이 제거되었습니다.

아카이브 노드 복구에 대한 자세한 내용은 을 "아카이브 노드 장애 복구(StorageGRID 11.8 문서 사이트)"참조하십시오.

Linux 노드를 교체합니다

Linux 노드를 교체합니다

장애가 발생하여 하나 이상의 새로운 물리적 또는 가상 호스트를 구축해야 하거나 기존 호스트에 Linux를 재설치해야 하는 경우 그리드 노드를 복구하기 전에 대체 호스트를 배포하고 구성하십시오. 이 절차는 모든 유형의 그리드 노드에 대한 그리드 노드 복구 프로세스의 한 단계입니다.

"Linux"는 Red Hat ® Enterprise Linux ®, Ubuntu ® 또는 Debian ® 배포를 의미합니다. 지원되는 버전 목록은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴(IMT)".

이 절차는 소프트웨어 기반 스토리지 노드, 운영 또는 비운영 관리 노드 또는 게이트웨이 노드를 복구하는 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.

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.

- "Linux 설치(Red Hat Enterprise Linux)"
- "Linux(Ubuntu 또는 Debian) 설치"

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. "그리드 노드 배포" 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 일부 또는 전체 드라이브 또는 SSD를 장애가 발생한 노드에서 교체 노드로 이동한 경우 원래 호스트에 있던 것과 동일한 스토리지 매핑을 다시 설정해야 합니다. 예를 들어, 설치 지침에서 권장하는 대로 에서 WWID 및 별칭을 사용한 경우 `/etc/multipath.conf` 교체 호스트에서 에서 동일한 별칭/WWID 쌍을 `/etc/multipath.conf` 사용해야 합니다.
- StorageGRID 노드가 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.

그리드 노드를 호스트에 복구합니다

장애가 발생한 그리드 노드를 새 Linux 호스트로 복원하려면 다음 단계를 수행하여 노드 구성 파일을 복원합니다.

1. 노드를 복원 및 확인합니다 노드 구성 파일을 복구합니다. 새 설치의 경우 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.
2. StorageGRID 호스트 서비스를 시작합니다..
3. 필요한 시작하지 못한 노드를 복구합니다경우.

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.

그리드 노드 복원 및 검증

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 볼륨이 손실되지 않은 경우 호스트에 있어야 하는 모든 그리드 노드를 가져올 수 `/var/local` 있습니다. 예를 들어 `/var/local`, Linux 운영 체제에 대한 StorageGRID 설치 지침에 설명된 대로 StorageGRID 시스템 데이터 볼륨에 공유 스토리지를 사용한 경우에도 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 볼륨 위치에 대한 자세한 내용은 설치 지침을 참조하십시오 `/var/local`.

- "Red Hat Enterprise Linux에 StorageGRID를 설치합니다"
- "Ubuntu 또는 Debian에 StorageGRID를 설치합니다"

단계

1. 복구된 호스트의 명령줄에 현재 구성된 모든 StorageGRID 노드를 나열합니다.`sudo storagegrid node list`

   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
```

   호스트에 구성해야 하는 일부 또는 모든 그리드 노드가 나열되지 않은 경우 누락된 그리드 노드를 복원해야 합니다.

2. 볼륨이 있는 그리드 노드를 `/var/local` 가져오려면

   a. 가져올 각 노드에 대해 다음 명령을 실행합니다.`sudo storagegrid node import node-var-local-volume-path`

   `storagegrid node import`명령은 타겟 노드가 마지막으로 실행된 호스트에서 완전히 종료된 경우에만 성공합니다. 그렇지 않으면 다음과 유사한 오류가 발생합니다.

```
This node (node-name) appears to be owned by another host (UUID host-uuid).

Use the --force flag if you are sure import is safe.
```

   a. 다른 호스트가 소유하고 있는 노드에 대한 오류가 표시되면 플래그를 사용하여 명령을 다시 `--force` 실행하여 가져오기를 완료합니다.`sudo storagegrid --force node import node-var-local-volume-path`

   플래그로 가져온 모든 노드는 `--force` 에 설명된 대로 그리드에 다시 연결하려면 추가 복구 단계가 "다음 단계: 필요한 경우 추가 복구 단계를 수행합니다"필요합니다.

3. 볼륨이 없는 그리드 노드의 경우 `/var/local` 노드의 구성 파일을 다시 생성하여 호스트에 복구합니다. 자세한 내용은 다음을 참조하십시오.

   - "Red Hat Enterprise Linux용 노드 구성 파일을 생성합니다"
   - "Ubuntu 또는 Debian용 노드 구성 파일을 만듭니다"

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).

새 블록 디바이스(StorageGRID 노드가 이전에 사용하지 않은 디바이스)를 노드에 대한 구성 파일을 다시 생성할 때 로 시작하는 구성 변수의 값으로 사용하는 경우 의 지침을 따릅니다 `BLOCK_DEVICE_`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.

누락된 네트워크 인터페이스 오류를 수정합니다

호스트 네트워크가 올바르게 구성되지 않았거나 이름의 철자가 틀린 경우 StorageGRID에서 파일에 지정된 매핑을 확인할 때 오류가 `/etc/storagegrid/nodes/node-name.conf` 발생합니다.

이 패턴과 일치하는 오류 또는 경고가 나타날 수 있습니다.

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
       <node-name>: Interface <host-interface-name>' does not exist
```

그리드 네트워크, 관리 네트워크 또는 클라이언트 네트워크에 대한 오류가 보고될 수 있습니다. 이 오류는 파일이 표시된 StorageGRID 네트워크를 이라는 호스트 인터페이스에 매핑하지만 *host-interface-name* 현재 호스트에 해당 이름을 가진 인터페이스가 없음을 의미합니다 `/etc/storagegrid/nodes/node-name.conf`.

이 오류가 발생하면 의 단계를 완료했는지 "새 Linux 호스트를 배포합니다"확인합니다. 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.

시스템은 복구된 각 노드가 유효한 블록 디바이스 특수 파일 또는 블록 디바이스 특수 파일에 대한 유효한 소프트링크에 매핑되는지 확인합니다. StorageGRID가 파일에서 잘못된 매핑을 발견하면 `/etc/storagegrid/nodes/node-name.conf` 블록 디바이스 누락 오류가 표시됩니다.

이 패턴과 일치하는 오류가 발생하는 경우:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: BLOCK_DEVICE_PURPOSE = <path-name>
       <node-name>: <path-name> does not exist
```

즉, 은 `/etc/storagegrid/nodes/node-name.conf` _node-name_for에 사용되는 블록 디바이스를 Linux 파일 시스템의 지정된 경로 이름에 매핑하지만 `PURPOSE` 해당 위치에 유효한 블록 디바이스 특수 파일 또는 소프트링크가 없는 블록 디바이스 특수 파일입니다.

의 단계를 완료했는지 "새 Linux 호스트를 배포합니다"확인합니다. 원래 호스트에서 사용된 것과 동일한 영구 디바이스 이름을 모든 블록 디바이스에 사용합니다.

누락된 블록 디바이스 특수 파일을 복원하거나 다시 생성할 수 없는 경우 적절한 크기 및 스토리지 범주의 새 블록 디바이스를 할당하고 노드 구성 파일을 편집하여 의 값을 새 블록 디바이스 특수 파일을 가리키도록 변경할 수 `BLOCK_DEVICE_PURPOSE` 있습니다.

Linux 운영 체제의 표를 사용하여 적절한 크기 및 스토리지 범주를 확인합니다.

- "Red Hat Enterprise Linux의 스토리지 및 성능 요구 사항"
- "Ubuntu 또는 Debian에 대한 스토리지 및 성능 요구 사항"

블록 디바이스 교체를 진행하기 전에 호스트 스토리지 구성에 대한 권장 사항을 검토하십시오.

- "Red Hat Enterprise Linux용 호스트 스토리지를 구성합니다"
- "Ubuntu 또는 Debian용 호스트 스토리지를 구성합니다"

장애가 발생한 호스트에서 원래 블록 디바이스가 손실되었기 때문에 로 시작하는 구성 파일 변수에 대해 새 블록 스토리지 디바이스를 제공해야 하는 `BLOCK_DEVICE_` 경우 추가 복구 절차를 시도하기 전에 새 블록 디바이스가 포맷되지 않았는지 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.

새 블록 스토리지 디바이스에 대해서만 다음 명령을 실행합니다. 블록 스토리지에 복구 중인 노드에 대한 유효한 데이터가 계속 포함되어 있다고 생각되면 이 명령을 실행하지 마십시오. 디바이스의 데이터가 모두 손실됩니다.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

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
```

3. 노드가 "not running" 또는 "stopped" 상태를 반환하는 경우 다음 명령을 실행합니다.

```
sudo storagegrid node start node-name
```

4. 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 연결되지 않고 복구 가능으로 표시되지 않으면 손상된 것일 수 있습니다. 노드를 복구 모드로 강제 전환할 수 있습니다.

단계

1. 노드의 네트워크 구성이 올바른지 확인합니다.

   잘못된 네트워크 인터페이스 매핑이나 잘못된 그리드 네트워크 IP 주소 또는 게이트웨이로 인해 노드가 그리드에 다시 연결되지 않았을 수 있습니다.

2. 네트워크 구성이 올바르면 `force-recovery` 다음 명령을 실행합니다.

   ```
   sudo storagegrid node force-recovery node-name
   ```

3. 노드에 대해 추가 복구 단계를 수행합니다. 을 "다음 단계: 필요한 경우 추가 복구 단계를 수행합니다"참조하십시오.

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 플래그를 사용해야 `--force` 했습니다.
- 모든 의 경우 `<PURPOSE>` 구성 파일 변수의 값은 `BLOCK_DEVICE_<PURPOSE>` 호스트 장애 전에 수행했던 것과 동일한 데이터를 포함하지 않는 블록 디바이스를 나타냅니다.
- 노드에 대해 발급한 `storagegrid node force-recovery node-name` 값입니다.
- 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"
스토리지 노드(소프트웨어 기반): • 노드를 가져오기 위해 플래그를 사용해야 하거나 명령을 `storagegrid node force-recovery node-name` 실행했습니다 `--force` • 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 • 에 대해 구성 파일 변수의 값이 `BLOCK_DEVICE_<PURPOSE>` 호스트 장애 전에 수행했던 것과 동일한 데이터를 포함하지 않는 블록 디바이스를 참조하는 경우 `<PURPOSE>`	"시스템 드라이브가 손상되지 않은 스토리지 볼륨 장애로부터 복구합니다"

VMware 노드를 교체합니다

VMware에서 호스팅되어 장애가 발생한 StorageGRID 노드를 복구하면 장애가 발생한 노드를 제거하고 복구 노드를 배포합니다.

시작하기 전에

가상 머신을 복구할 수 없으며 교체해야 한다고 판단했습니다.

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 및 게이트웨이 노드를 포함한 모든 VMware 노드에 대해 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. 자세한 내용은 을 "StorageGRID 노드를 가상 시스템으로 구축"참조하십시오.

   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.

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"

장애가 발생한 노드를 서비스 어플라이언스로 교체합니다

장애가 발생한 노드를 서비스 어플라이언스로 교체합니다

서비스 어플라이언스를 사용하여 장애가 발생한 게이트웨이 노드, 장애가 발생한 기본 관리자 노드 또는 VMware, Linux 호스트 또는 서비스 어플라이언스에서 호스팅되었던 장애가 발생한 기본 관리자 노드를 복구할 수 있습니다. 이 절차는 그리드 노드 복구 절차의 한 단계입니다.

시작하기 전에

- 다음 상황 중 하나가 참인 것으로 판단했습니다.
  - 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.
- 서비스 어플라이언스의 StorageGRID 어플라이언스 설치 프로그램 버전이 StorageGRID 시스템의 소프트웨어 버전과 일치하는지 확인했습니다. 을 "StorageGRID 어플라이언스 설치 프로그램 버전을 확인하고 업그레이드합니다"참조하십시오.

> SG110과 SG1100 서비스 어플라이언스 또는 SG100 및 SG1000 서비스 어플라이언스를 같은 사이트에 배포하지 마십시오. 성능을 예측할 수 없습니다.

이 작업에 대해

다음과 같은 경우 서비스 어플라이언스를 사용하여 장애가 발생한 그리드 노드를 복구할 수 있습니다.

- 장애가 발생한 노드가 VMware 또는 Linux에서 호스팅됨"플랫폼 변경"()
- 장애가 발생한 노드가 서비스 어플라이언스에서 호스팅되었습니다"플랫폼 교체"().

서비스 어플라이언스 설치(플랫폼 변경 전용)

VMware 또는 Linux 호스트에서 호스팅되는 장애가 발생한 그리드 노드를 복구하는 경우 교체 노드에 대해 서비스 어플라이언스를 사용하는 경우, 먼저 장애가 발생한 노드와 동일한 노드 이름(시스템 이름)을 사용하여 새 어플라이언스 하드웨어를 설치해야 합니다.

시작하기 전에

장애가 발생한 노드에 대한 다음 정보가 있습니다.

- * 노드 이름 *: 서비스 어플라이언스는 장애가 발생한 노드와 동일한 노드 이름을 사용하여 설치해야 합니다. 노드 이름은 호스트 이름(시스템 이름)입니다.
- * 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.

이 작업에 대해

VMware 또는 Linux에서 호스팅되어 서비스 어플라이언스에서 호스팅되는 노드로 대체되는 장애가 발생한 노드를 복구하는 경우에만 이 절차를 수행하십시오.

단계

1. 새 서비스 어플라이언스 설치에 대한 지침을 따릅니다. 을 "하드웨어 설치를 빠르게 시작합니다"참조하십시오.
2. 노드 이름을 묻는 메시지가 표시되면 장애가 발생한 노드의 노드 이름을 사용합니다.

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 다음 단계를 수행하지 마십시오.

단계

1. 장애가 발생한 그리드 노드에 로그인합니다.

   a. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

   b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   c. 다음 명령을 입력하여 루트로 전환합니다. `su -`

   d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

   루트로 로그인하면 프롬프트가 에서 `$` 로 `#`변경됩니다.

2. StorageGRID 소프트웨어 설치를 위해 어플라이언스를 준비합니다. 다음을 입력합니다. `sgareinstall`
3. 계속하라는 메시지가 나타나면 다음을 입력합니다. `y`

   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.

   > `sgareinstall`명령을 실행하면 StorageGRID 프로비저닝된 모든 계정, 암호 및 SSH 키가 제거되고 새 호스트 키가 생성됩니다.

서비스 어플라이언스에서 소프트웨어 설치를 시작합니다

서비스 어플라이언스에 게이트웨이 노드 또는 관리자 노드를 설치하려면 어플라이언스에 포함된 StorageGRID 어플라이언스 설치 프로그램을 사용합니다.

시작하기 전에

- 이 어플라이언스는 랙에 설치되고 네트워크에 연결되고 전원이 켜집니다.
- 네트워크 링크 및 IP 주소는 StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스에 대해 구성됩니다.
- 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 정의됩니다.

  을 "하드웨어 설치를 빠르게 시작합니다"참조하십시오.

- 을 사용하고 "지원되는 웹 브라우저"있습니다.
- 어플라이언스에 할당된 IP 주소 중 하나가 있습니다. 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

서비스 어플라이언스에 StorageGRID 소프트웨어를 설치하려면:

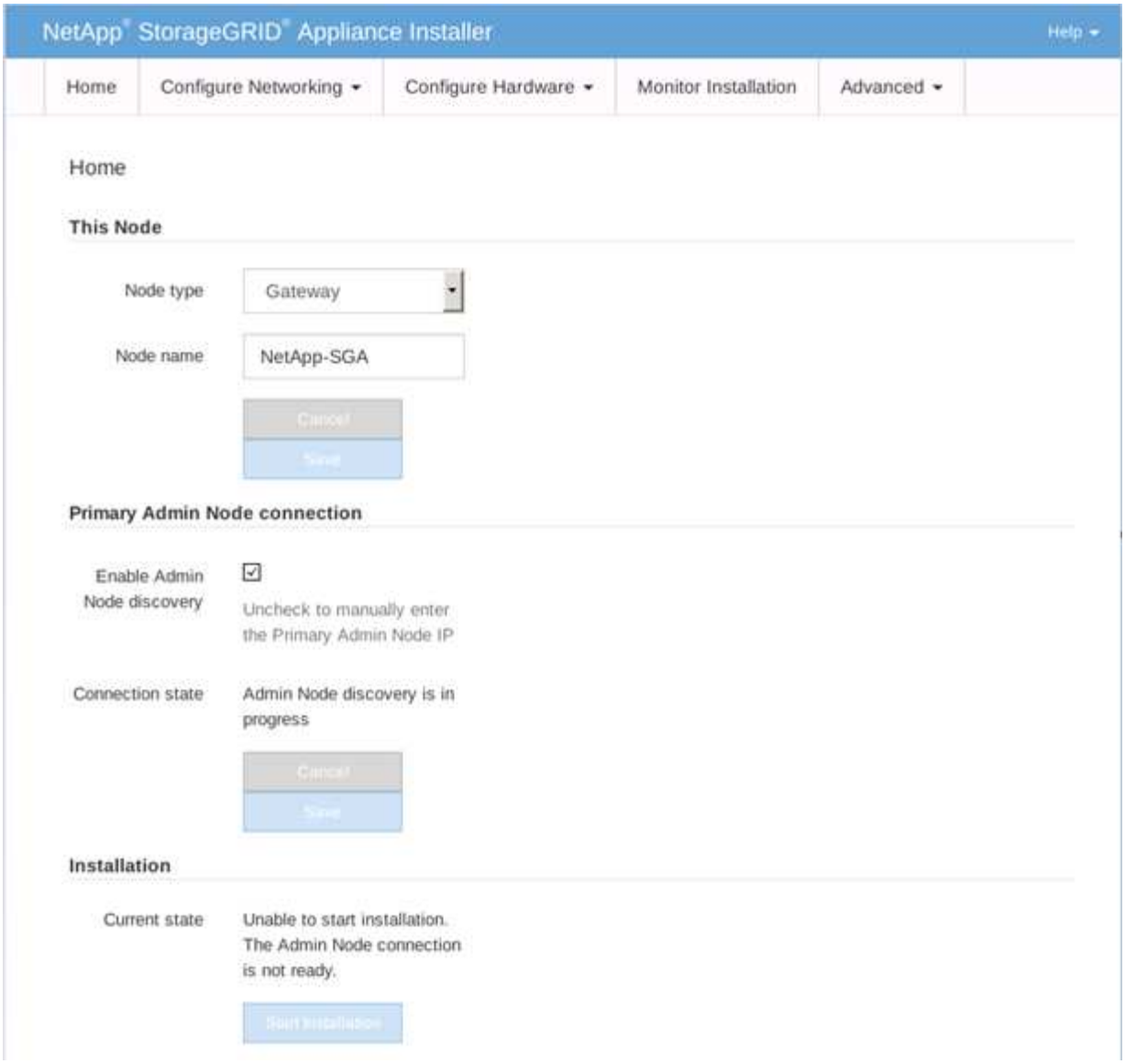
- 기본 관리 노드의 경우 노드 이름을 지정한 다음 적절한 소프트웨어 패키지를 업로드합니다(필요한 경우).
- 비 기본 관리 노드 또는 게이트웨이 노드의 경우 기본 관리 노드의 IP 주소와 노드 이름을 지정하거나 확인합니다.
- 설치를 시작하고 볼륨이 구성되고 소프트웨어가 설치될 때까지 기다립니다.
- 프로세스가 중간에 진행되면 설치가 일시 중지됩니다. 설치를 다시 시작하려면 그리드 관리자에 로그인하고 보류 중인 노드를 장애 발생 노드의 대체용으로 구성해야 합니다.
- 노드를 구성한 후에는 어플라이언스 설치 프로세스가 완료되고 어플라이언스가 재부팅됩니다.

단계

1. 브라우저를 열고 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.

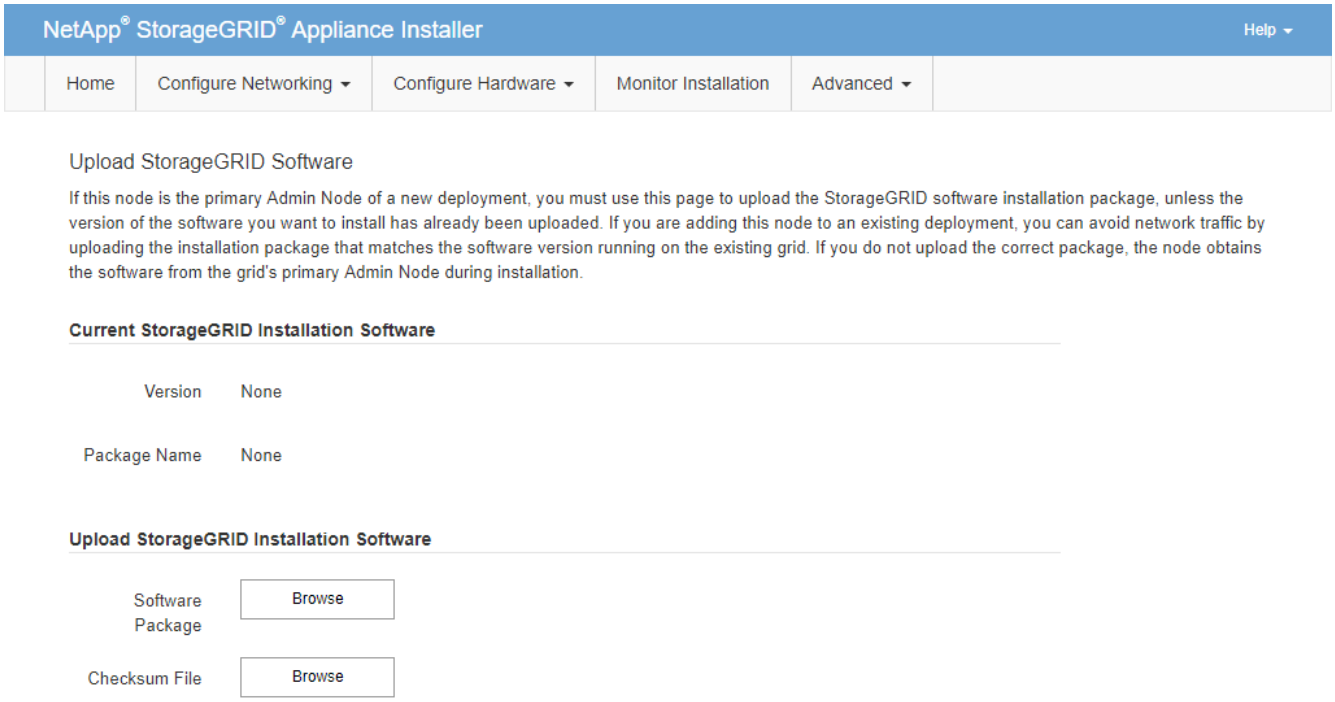
   b. Node Name * 필드에 복구 중인 노드에 사용된 이름과 동일한 이름을 입력하고 * Save * 를 클릭합니다.

   c. 설치 섹션에서 현재 상태에 나열된 소프트웨어 버전을 확인합니다

      설치할 준비가 된 소프트웨어 버전이 올바르면 으로 설치 단계건너뜁니다.

   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 활성화 * 확인란의 선택을 취소합니다. b. IP 주소를 수동으로 입력합니다. c. 저장 * 을 클릭합니다. d. 새 IP 주소의 연결 상태가 "준비"가 될 때까지 기다립니다.

옵션을 선택합니다	설명
연결된 모든 운영 관리 노드의 자동 검색	a. 관리자 노드 검색 활성화 * 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 "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 유지보수 지침을 참조하십시오.

5. StorageGRID 어플라이언스 설치 관리자 홈 페이지에서 * 설치 시작 * 을 클릭합니다.

   현재 상태가 "Installation is in progress(설치 진행 중)"로 변경되고 Monitor Installation(모니터 설치) 페이지가 표시됩니다.

   모니터 설치 페이지에 수동으로 액세스해야 하는 경우 메뉴 모음에서 * 모니터 설치 * 를 클릭합니다.

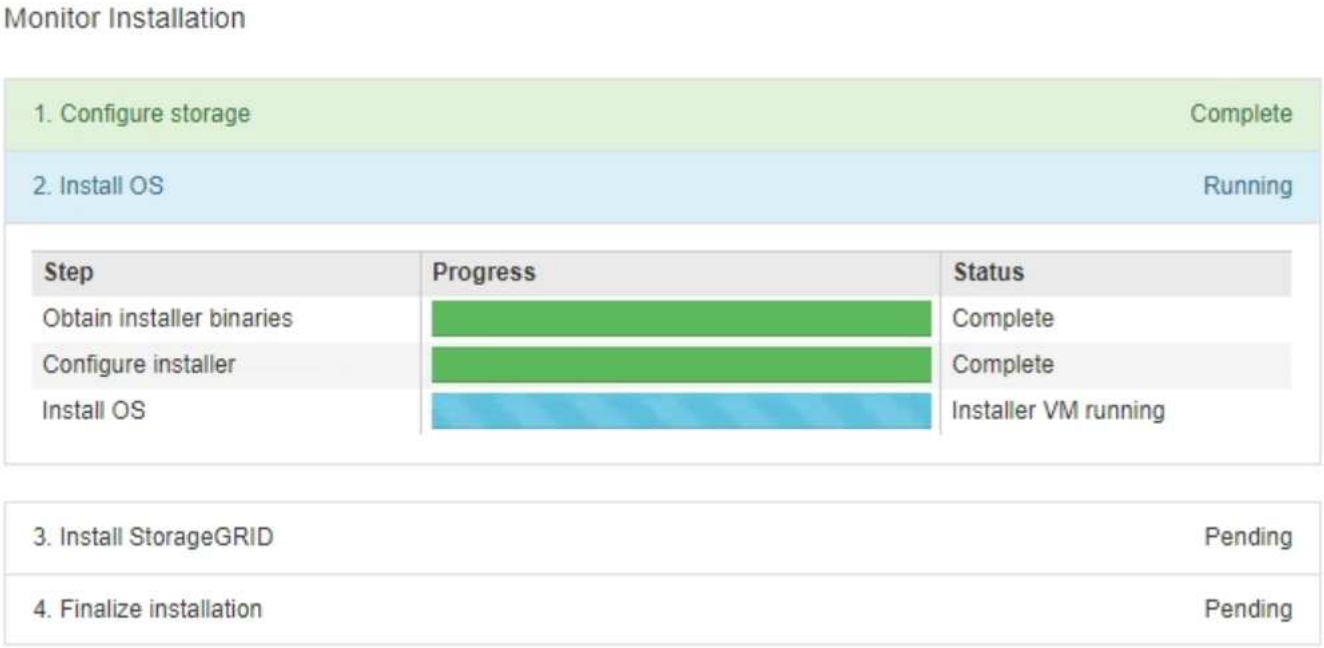
서비스 어플라이언스 설치를 모니터링합니다

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 실행하는 경우 다시 실행할 필요가 없는 작업은 녹색 상태 표시줄과 "건너뜀"으로 표시됩니다.

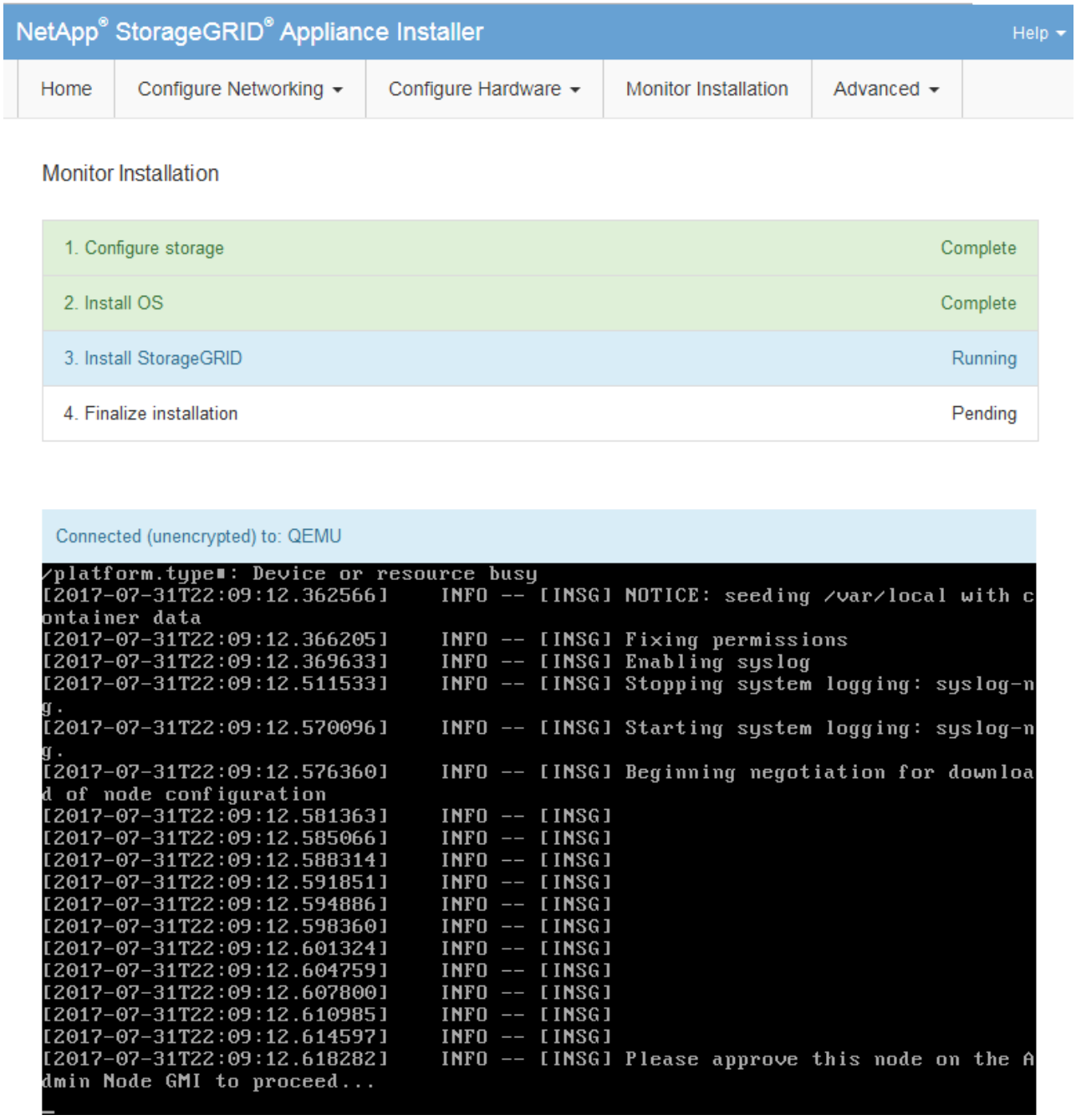
2. 처음 두 설치 단계의 진행 상황을 검토합니다.
   - * 1. 스토리지 구성 *

     이 단계에서 설치 관리자는 드라이브에서 기존 구성을 지우고 호스트 설정을 구성합니다.

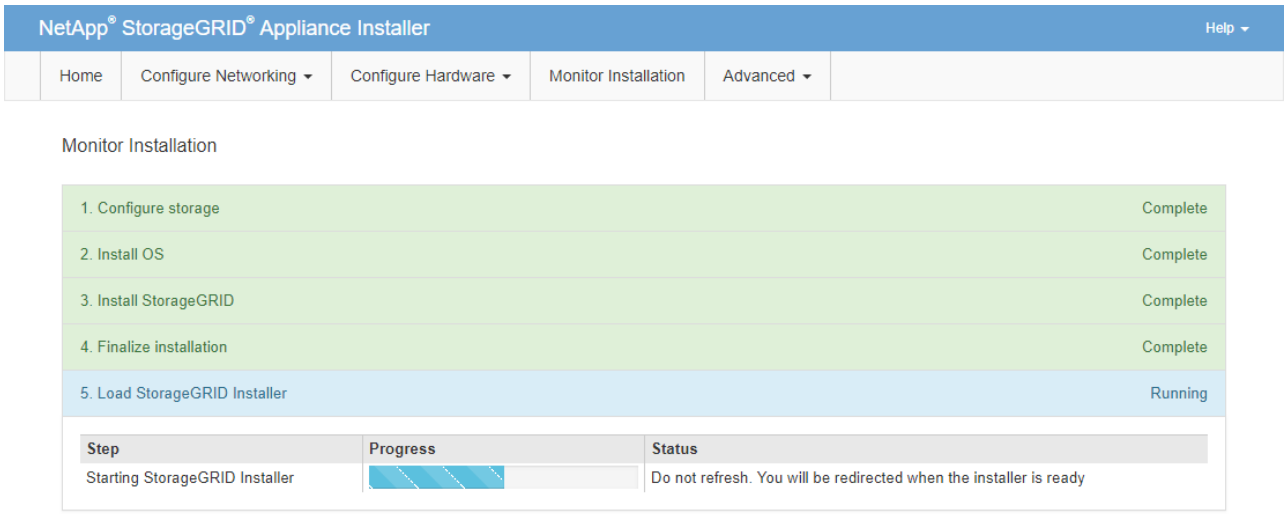
   - * 2. OS * 를 설치합니다

     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 사이트를 복구하는 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 정상인지 또는 스토리지 노드에 복구 가능한 객체가 포함되어 있는지 확인하십시오. 유효한 데이터가 포함된 노드 또는 스토리지 볼륨을 재구축할 경우 불필요한 데이터 손실이 발생할 수 있습니다.
- * 활성 ILM 정책 *: 그리드에 있는 개체 복사본의 수, 유형 및 위치는 활성 ILM 정책에 의해 제어됩니다. ILM 정책의 세부 사항은 복구 가능한 데이터의 양과 복구에 필요한 특정 기술에 영향을 미칠 수 있습니다.

사이트에 개체의 복사본만 포함되어 있고 사이트가 손실되면 개체가 손실됩니다.

- * 버킷(또는 컨테이너) 일관성 *: 버킷(또는 컨테이너)에 적용되는 일관성은 StorageGRID이 오브젝트 메타데이터를 모든 노드와 사이트에 완전히 복제하는지 여부에 영향을 미쳐 오브젝트 수집이 성공했음을 클라이언트에 알려줍니다. 정합성 보장 값이 최종 일관성을 허용하는 경우 사이트 장애 시 일부 개체 메타데이터가 손실되었을 수 있습니다. 이는 복구 가능한 데이터의 양과 복구 절차의 세부 정보에 영향을 줄 수 있습니다.
- * 최근 변경 내역 *: 복구 절차의 세부 사항은 오류 발생 시 유지 보수 절차가 진행 중이었는지 여부 또는 ILM 정책이 최근에 변경되었는지 여부에 따라 영향을 받을 수 있습니다. 기술 지원 부서에서는 사이트 복구를 시작하기 전에 그리드의 최근 내역과 현재 상황을 평가해야 합니다.

사이트 복구는 기술 지원 부서에서 수행할 수 있습니다.

다음은 기술 지원 부서에서 장애가 발생한 사이트를 복구하는 데 사용하는 프로세스의 일반적인 개요입니다.

1. 기술 지원:
   a. 실패에 대한 자세한 평가를 수행합니다.
   b. 귀사와 협력하여 비즈니스 목표를 검토합니다.
   c. 고객의 상황에 맞는 복구 계획을 개발합니다.
2. 기본 관리자 노드에 오류가 발생한 경우 기술 지원 부서에서 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 기술 지원 부서에서는 특수한 명령을 사용하여 개체 및 개체 메타데이터를 성공적으로 복원합니다.
4. 기술 지원은 장애가 발생한 다른 노드를 복구합니다.

   개체 메타데이터 및 데이터가 복구된 후 기술 지원 부서에서는 표준 절차를 사용하여 장애가 발생한 게이트웨이 노드 또는 비기본 관리 노드를 복구합니다.

관련 정보

"사이트 파기"

사용자 환경에서 **StorageGRID**를 활성화하는 방법

StorageGRID 환경에서 애플리케이션을 테스트하고 지원하는 방법에 대해 알아보려면 로 "StorageGRID를 활성화하는 방법" 이동하십시오.

BlueXP 를 사용하여 StorageGRID를 관리하는 방법

로 "BlueXP를 사용한 StorageGRID 관리" 이동하여 BlueXP 에서 그리드 관리자를 사용하여 StorageGRID 시스템을 관리하는 방법을 알아보고 백업, 데이터 계층화 등에 BlueXP의 데이터 서비스를 사용하는 방법을 알아보십시오.

기타 버전의 NetApp StorageGRID 설명서

다른 버전의 NetApp StorageGRID 소프트웨어에 대한 설명서는 다음 웹 사이트에서 찾을 수 있습니다.

- "StorageGRID 11.8 설명서"
- "StorageGRID 11.7 설명서"
- "StorageGRID 11.6 설명서"
- "StorageGRID 11.5 설명서"
- "StorageGRID 11.4 설명서 센터"
- "StorageGRID 11.3 설명서 센터"

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/ECMLP3330669