StorageGRID 관리

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/storagegrid-120/admin/index.html on July 23, 2026. Always check docs.netapp.com for the latest.

목차

StorageGRID 관리 1
StorageGRID 관리 1
이 지침에 관하여 1
시작하기 전에 1
Grid Manager 시작하기 1
StorageGRID의 웹 브라우저 요구 사항 1
StorageGRID Grid Manager에 로그인합니다. 2
StorageGRID Grid Manager에서 로그아웃합니다 4
StorageGRID Grid Manager 비밀번호를 변경하세요 4
StorageGRID 라이선스 정보 보기 5
StorageGRID 라이선스 정보 업데이트 6
API 사용 6
StorageGRID에 대한 액세스 제어 27
StorageGRID 액세스 제어 27
StorageGRID 프로비저닝 암호를 변경하세요 28
StorageGRID에서 노드 콘솔 암호 변경 29
StorageGRID 관리 노드의 SSH 액세스 암호 변경 31
StorageGRID에서 ID 페더레이션 사용 33
StorageGRID에서 관리자 그룹 관리 38
StorageGRID의 관리 그룹 권한 41
StorageGRID에서 사용자 관리 44
싱글 사인온(SSO) 사용 47
그리드 페더레이션 사용 72
StorageGRID 그리드 연합에 대해 알아보세요 72
StorageGRID의 계정 복제에 대해 알아보십시오 75
StorageGRID의 교차 그리드 복제에 대해 알아보십시오 78
StorageGRID에서 교차 그리드 복제와 CloudMirror 복제 비교 84
StorageGRID 그리드 페더레이션 연결을 생성합니다 86
StorageGRID 그리드 페더레이션 연결 관리 89
StorageGRID 그리드 페더레이션에 허용된 테넌트를 관리합니다. 94
StorageGRID에서 그리드 페더레이션 오류 문제 해결 100
실패한 StorageGRID 복제 작업을 식별하고 다시 시도합니다. 105
보안 관리 109
StorageGRID에서 보안 관리 109
StorageGRID 암호화 방법 검토 109
인증서 관리 112
${post_edited_translations.segment} 143
키 관리 서버 구성 149
프록시 설정 관리 168

방화벽 제어 169
테넌트 관리 176
StorageGRID의 테넌트 계정 176
StorageGRID 테넌트 계정을 생성합니다 177
StorageGRID 테넌트 계정 편집 182
StorageGRID 테넌트의 로컬 루트 사용자 암호 변경 184
StorageGRID 테넌트 계정 삭제 185
플랫폼 서비스 관리 186
StorageGRID의 테넌트 계정에 대한 S3 Select 관리 195
클라이언트 연결 구성 196
StorageGRID에 대한 S3 클라이언트 연결을 구성합니다 196
StorageGRID의 S3 클라이언트 보안 198
S3 설정 마법사 사용 200
HA 그룹 관리 209
${post_edited_translations.segment} 220
StorageGRID에서 S3 엔드포인트 도메인 이름 구성 235
StorageGRID 클라이언트 연결을 위한 IP 주소 및 포트 237
${post_edited_translations.segment} 239
StorageGRID 네트워크 설정을 구성합니다 239
StorageGRID 네트워크 가이드라인 239
StorageGRID에서 IP 주소 보기 241
StorageGRID에서 VLAN 인터페이스 구성 242
관리 인터페이스에 대해 StorageGRID CORS 활성화 246
트래픽 분류 정책 관리 247
StorageGRID의 발신 TLS 연결에 지원되는 암호 253
StorageGRID의 활성, 유휴 및 동시 HTTP 연결의 이점 254
StorageGRID에서 링크 비용 관리 256
AutoSupport 사용 258
StorageGRID의 AutoSupport에 대해 알아보기 258
StorageGRID에서 AutoSupport 구성 262
StorageGRID에서 AutoSupport 패키지를 수동으로 트리거합니다 266
StorageGRID AutoSupport 패키지 문제 해결 266
StorageGRID를 통해 E-Series AutoSupport 패키지 전송 267
${post_edited_translations.segment} 272
저장 옵션 사용 272
StorageGRID에서 객체 메타데이터 스토리지 관리 275
StorageGRID에서 메타데이터 예약 공간 설정 증가 282
StorageGRID에 저장된 객체 압축 283
StorageGRID에서 전체 스토리지 노드 관리 284
관리자 노드 관리 284
StorageGRID에서 여러 관리 노드 사용 284

StorageGRID에서 기본 관리 노드 식별 285

StorageGRID 관리

StorageGRID 관리

StorageGRID 시스템을 구성하고 관리하려면 다음 지침을 따르십시오.

이 지침에 관하여

StorageGRID를 구성하고 관리하기 위한 주요 작업을 통해 다음을 수행할 수 있습니다.

- Grid Manager를 사용하여 그룹과 사용자를 설정합니다.
- S3 클라이언트 애플리케이션이 객체를 저장하고 검색할 수 있도록 테넌트 계정을 생성합니다
- StorageGRID 네트워크 구성 및 관리
- AutoSupport 구성
- 노드 설정 관리

시작하기 전에

- StorageGRID 시스템에 대한 전반적인 이해가 있습니다.
- Linux 명령 셸, 네트워킹, 서버 하드웨어 설정 및 구성에 대한 상당히 자세한 지식을 갖추고 있습니다.

Grid Manager 시작하기

StorageGRID의 웹 브라우저 요구 사항

지원되는 웹 브라우저를 사용해야 합니다.

웹 브라우저	최소 지원 버전
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

브라우저 창의 너비를 권장 너비로 설정하세요.

브라우저 너비	픽셀
최소	1024
최적	1280

StorageGRID Grid Manager에 로그인합니다.

지원되는 웹 브라우저의 주소 표시줄에 관리 노드의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하여 그리드 관리자 로그인 페이지에 접속할 수 있습니다.

각 StorageGRID 시스템에는 기본 관리 노드 1개와 여러 개의 보조 관리 노드가 포함됩니다. 모든 관리 노드에서 Grid Manager에 로그인하여 StorageGRID 시스템을 관리할 수 있습니다. 단, 일부 유지 관리 절차는 기본 관리 노드에서만 수행할 수 있습니다.

HA 그룹에 연결

관리 노드가 고가용성(HA) 그룹에 포함된 경우, HA 그룹의 가상 IP 주소 또는 가상 IP 주소에 매핑되는 정규화된 도메인 이름을 사용하여 연결합니다. 기본 관리 노드를 그룹의 기본 인터페이스로 선택해야 합니다. 이렇게 하면 기본 관리 노드를 사용할 수 없는 경우를 제외하고 Grid Manager에 액세스할 때 기본 관리 노드를 통해 액세스하게 됩니다. "고가용성 그룹 관리"을 참조하십시오.

SSO 사용

로그인 절차는 "싱글 사인온(SSO)이 구성되었습니다."인 경우 약간 다릅니다.

첫 번째 관리 노드에서 Grid Manager에 로그인합니다.

시작하기 전에

- 로그인 정보를 가지고 계십니다.
- 귀하는 "지원되는 웹 브라우저"을(를) 사용하고 있습니다.
- 웹 브라우저에서 쿠키가 활성화되어 있습니다.
- 귀하는 하나 이상의 권한을 가진 사용자 그룹에 속해 있습니다.
- 그리드 관리자의 URL은 다음과 같습니다.

  `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) 이외의 포트를 사용하여 Grid Manager에 액세스하려면 URL에 포트 번호를 포함하십시오.

  `https://FQDN_or_Admin_Node_IP:port/`

  > 제한된 Grid Manager 포트에서는 SSO를 사용할 수 없습니다. 포트 443을 사용해야 합니다.

단계

1. 지원되는 웹 브라우저를 실행합니다.
2. 브라우저 주소 표시줄에 Grid Manager의 URL을 입력합니다.
3. 보안 경고 메시지가 표시되면 브라우저의 설치 마법사를 사용하여 인증서를 설치하십시오. 을 참조하십시오. "보안 인증서 관리"
4. 그리드 관리자에 로그인합니다.

표시되는 로그인 화면은 StorageGRID에 대해 SSO(Single Sign-On)가 구성되었는지 여부에 따라 다릅니다.

SSO를 사용하지 않음

a. Grid Manager의 사용자 이름과 비밀번호를 입력하십시오.

b. *로그인*을 선택합니다.

SSO 사용

- StorageGRID에서 SSO를 사용하고 있고 이 브라우저에서 해당 URL에 처음 접속한 경우:

  i. *로그인*을 선택합니다. 계정 필드에는 0을 그대로 두어도 됩니다.

  ii. 조직의 SSO 로그인 페이지에 표준 SSO 자격 증명을 입력하십시오.

  예를 들어 StorageGRID에서 SSO를 사용하고 있고 이전에 Grid Manager 또는 테넌트 계정에 액세스한 적이 있는 경우:

  A. **0**(Grid Manager 계정 ID)을 입력하거나 최근 계정 목록에 *Grid Manager*가 표시되면 해당 항목을 선택하세요.

  B. *로그인*을 선택합니다.

  C. 조직의 SSO 로그인 페이지에서 표준 SSO 자격 증명을 사용하여 로그인하십시오.

로그인하면 대시보드가 포함된 Grid Manager 홈 페이지가 나타납니다. 제공되는 정보에 대한 자세한 내용은 "대시보드 보기 및 관리"을 참조하십시오.

다른 관리 노드에 로그인합니다

다른 관리 노드에 로그인하려면 다음 단계를 따르십시오.

SSO를 사용하지 않음

단계

1. 브라우저 주소창에 다른 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력하십시오. 필요한 경우 포트 번호도 포함하십시오.
2. Grid Manager의 사용자 이름과 비밀번호를 입력하십시오.
3. *로그인*을 선택합니다.

SSO 사용

StorageGRID에서 SSO를 사용하고 있고 하나의 관리 노드에 로그인한 경우, 다시 로그인할 필요 없이 다른 관리 노드에 액세스할 수 있습니다.

단계

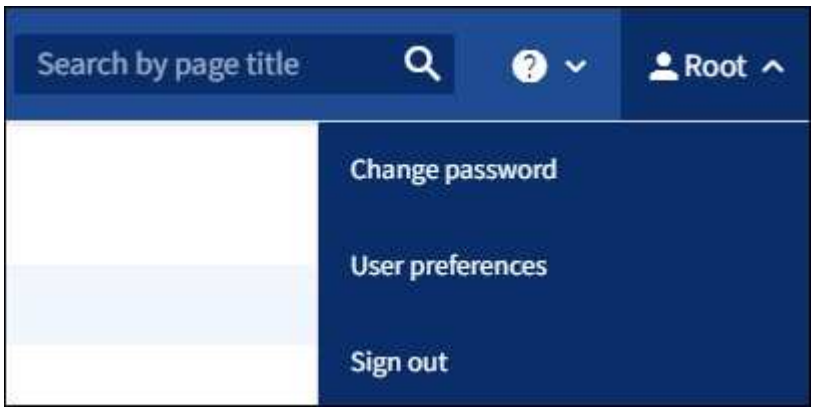
1. 브라우저 주소창에 다른 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력하십시오.
2. SSO 세션이 만료된 경우 자격 증명을 다시 입력하십시오.

StorageGRID Grid Manager에서 로그아웃합니다

Grid Manager 사용을 마친 후에는 로그아웃하여 권한이 없는 사용자가 StorageGRID 시스템에 접근하지 못하도록 해야 합니다. 브라우저의 쿠키 설정에 따라 브라우저를 닫는 것만으로는 시스템에서 로그아웃되지 않을 수 있습니다.

단계

1. 오른쪽 상단에서 사용자 이름을 선택합니다.



2. *로그아웃*을 선택합니다.

옵션	설명
SSO를 사용하지 않음	관리자 노드에서 로그아웃되었습니다. 그리드 관리자 로그인 페이지가 표시됩니다. 참고: 여러 관리자 노드에 로그인한 경우, 각 노드에서 모두 로그아웃해야 합니다.
SSO 활성화됨	현재 접속 중인 모든 관리자 노드에서 로그아웃되었습니다. StorageGRID 로그인 페이지가 표시됩니다. 최근 계정 드롭다운 메뉴에 **Grid Manager***가 기본값으로 표시되고 *계정 **ID** 필드에는 0이 표시됩니다. 참고: SSO가 활성화되어 있고 테넌트 관리자에도 로그인되어 있는 경우, "테넌트 계정에서 로그아웃"하려면 "SSO에서 로그아웃"도 수행해야 합니다.

StorageGRID Grid Manager 비밀번호를 변경하세요

Grid Manager의 로컬 사용자라면 직접 비밀번호를 변경할 수 있습니다.

시작하기 전에

현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.

이 작업 정보

StorageGRID에 페더레이션 사용자로 로그인하거나 SSO(싱글 사인온)가 활성화된 경우 Grid Manager에서 암호를 변경할 수 없습니다. 대신 Active Directory 또는 OpenLDAP과 같은 외부 ID 소스에서 암호를 변경해야 합니다.

단계

1. 그리드 관리자 헤더에서 사용자 이름 > *비밀번호 변경*을 선택합니다.
2. 현재 비밀번호를 입력하세요.
3. 새 비밀번호를 입력하세요.

   비밀번호는 최소 8자, 최대 32자여야 합니다. 비밀번호는 대소문자를 구분합니다.

4. 새 비밀번호를 다시 입력하세요.
5. *저장*을 선택하세요.

StorageGRID 라이선스 정보 보기

필요할 때마다 그리드의 최대 스토리지 용량 등 StorageGRID 시스템의 라이선스 정보를 확인할 수 있습니다.

시작하기 전에

현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.

이 작업 정보

이 StorageGRID 시스템의 소프트웨어 라이선스에 문제가 있는 경우 대시보드의 상태 카드에 라이선스 상태 아이콘과 라이선스 링크가 표시됩니다. 숫자는 라이선스 관련 문제 발생 건수를 나타냅니다.

단계

1. 다음 방법 중 하나를 사용하여 라이선스 페이지에 액세스합니다.
   - 유지보수 > 시스템 > *라이선스*를 선택하십시오.
   - 대시보드의 상태 카드에서 라이선스 상태 아이콘 또는 라이선스 링크를 선택합니다.

     이 링크는 라이선스에 문제가 있는 경우에만 표시됩니다.

2. 현재 라이선스에 대한 읽기 전용 세부 정보를 봅니다.

- StorageGRID 시스템 ID는 해당 StorageGRID 설치를 식별하는 고유 번호입니다.
- 라이센스 일련 번호
- 라이선스 유형은 영구 또는 구독 중 하나입니다.
- 그리드의 라이센스된 스토리지 용량
- 지원되는 스토리지 용량
- 라이선스 만료일. 영구 라이선스의 경우 *N/A*가 표시됩니다.
- 지원 종료일

  이 날짜는 현재 라이선스 파일에서 읽어오며, 라이선스 파일을 발급받은 후 지원 서비스 계약을 연장 또는 갱신한 경우 최신 날짜가 아닐 수 있습니다. 이 값을 업데이트하려면 "StorageGRID 라이선스 정보 업데이트"을 참조하십시오. Active IQ를 사용하여 실제 계약 종료 날짜를 확인할 수도 있습니다.

- 라이선스 텍스트 파일의 내용

StorageGRID 라이선스 정보 업데이트

StorageGRID 라이선스 약관이 변경될 때마다 StorageGRID 시스템의 라이선스 정보를 업데이트해야 합니다. 예를 들어, 그리드에 추가 스토리지 용량을 구매하는 경우 라이선스 정보를 업데이트해야 합니다.

시작하기 전에

- StorageGRID 시스템에 적용할 새 라이선스 파일이 있습니다.
- "특정 액세스 권한"이(가) 있습니다.
- 프로비저닝 암호를 가지고 계십니다.

단계

1. 유지보수 > 시스템 > *라이선스*를 선택하십시오.
2. 라이선스 업데이트 섹션에서 *찾아보기*를 선택합니다.
3. 새 라이선스 파일을 찾아 선택하십시오(`.txt`).

   새 라이선스 파일이 유효성 검사를 거쳐 표시됩니다.

4. 프로비저닝 암호를 입력하십시오.
5. *저장*을 선택하세요.

API 사용

StorageGRID 그리드 관리 **API**를 사용하십시오

Grid Manager 사용자 인터페이스 대신 Grid Management REST API를 사용하여 시스템 관리 작업을 수행할 수 있습니다. 예를 들어, API를 사용하여 작업을 자동화하거나 사용자 등의 여러 엔티티를 더 빠르게 생성할 수 있습니다.

최상위 리소스

그리드 관리 API는 다음과 같은 최상위 리소스를 제공합니다.

- `/grid`: 액세스는 Grid Manager 사용자로 제한되며 구성된 그룹 권한을 기반으로 합니다.
- `/org`: 액세스는 테넌트 계정에 대한 로컬 또는 페더레이션 LDAP 그룹에 속한 사용자로 제한됩니다. 자세한 내용은 "테넌트 계정 사용"을 참조하십시오.
- `/private`: 액세스는 Grid Manager 사용자로 제한되며 구성된 그룹 권한을 기반으로 합니다. 비공개 API는 예고 없이 변경될 수 있습니다. StorageGRID 비공개 엔드포인트는 요청의 API 버전도 무시합니다.

API 요청 발행

Grid Management API는 오픈 소스 API 플랫폼인 Swagger를 사용합니다. Swagger는 개발자와 비개발자 모두 API를 통해 StorageGRID에서 실시간 작업을 수행할 수 있도록 직관적인 사용자 인터페이스를 제공합니다.

Swagger 사용자 인터페이스는 각 API 작업에 대한 완전한 세부 정보와 문서를 제공합니다.

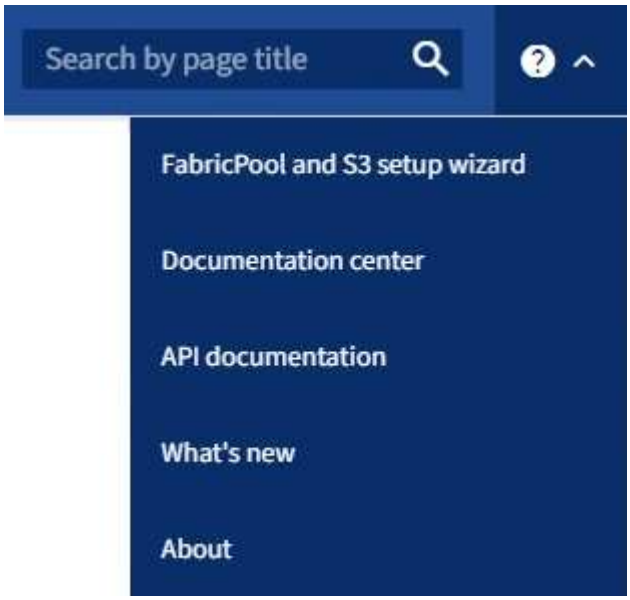
시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.

> API 문서 웹페이지를 사용하여 수행하는 모든 API 작업은 실시간 작업입니다. 실수로 구성 데이터 또는 기타 데이터를 생성, 업데이트 또는 삭제하지 않도록 주의하십시오.

단계

1. 그리드 관리자 헤더에서 도움말 아이콘을 선택한 다음 *API 문서*를 선택합니다.



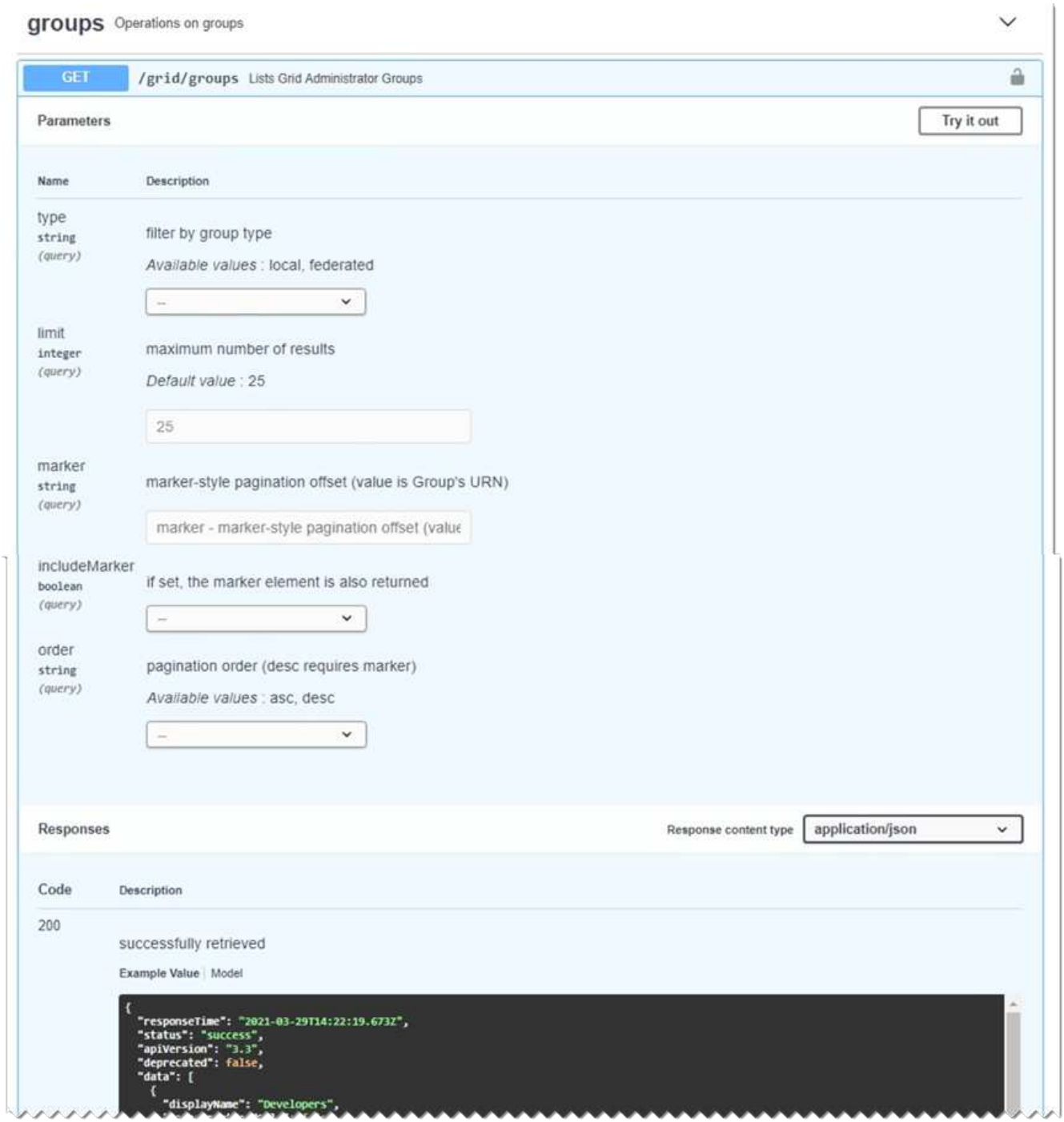
2. 비공개 API를 사용하여 작업을 수행하려면 StorageGRID 관리 API 페이지에서 *비공개 API 문서로 이동*을 선택하십시오.

   비공개 API는 예고 없이 변경될 수 있습니다. StorageGRID 비공개 엔드포인트는 요청의 API 버전을 무시합니다.

3. 원하는 작업을 선택하십시오.

   API 작업을 확장하면 GET, PUT, UPDATE, DELETE와 같은 사용 가능한 HTTP 작업을 확인할 수 있습니다.

4. HTTP 작업을 선택하면 엔드포인트 URL, 필수 또는 선택적 매개변수 목록, 요청 본문 예시(필요한 경우) 및 가능한 응답을 포함한 요청 세부 정보를 볼 수 있습니다.



5. 요청에 그룹 또는 사용자 ID와 같은 추가 매개변수가 필요한지 확인합니다. 그런 다음 이러한 값을 가져옵니다. 필요한 정보를 얻기 위해 다른 API 요청을 먼저 수행해야 할 수도 있습니다.

6. 예제 요청 본문을 수정해야 하는지 판단하세요. 수정해야 하는 경우, *모델*을 선택하여 각 필드에 대한 요구 사항을 확인할 수 있습니다.

7. *직접 사용해보기*를 선택합니다.
8. 필요한 매개변수를 제공하거나 필요에 따라 요청 본문을 수정하십시오.
9. *실행*을 선택합니다.
10. 요청이 성공했는지 여부를 확인하려면 응답 코드를 검토하십시오.

StorageGRID의 Grid Management API 작업

그리드 관리 API는 사용 가능한 작업을 다음 섹션으로 구성합니다.

> 이 목록에는 공개 API에서 사용할 수 있는 작업만 포함되어 있습니다.

- 계정: 스토리지 테넌트 계정을 관리하는 작업으로, 새 계정 생성 및 특정 계정의 스토리지 사용량 조회 등이 포함됩니다.
- **alert-history**: 해결된 경고에 대한 작업 내역입니다.
- **alert-receivers**: 알림 수신자(이메일)에 대한 작업입니다.
- **alert-rules**: 경고 규칙에 대한 작업.
- **alert-silences**: 경보 해제 관련 작업.
- **alerts**: 알림에 대한 작업.
- 감사: 감사 구성을 나열하고 업데이트하는 작업입니다.
- **auth**: 사용자 세션 인증을 수행하는 작업입니다.

  그리드 관리 API는 베어러 토큰 인증 방식을 지원합니다. 로그인하려면 인증 요청의 JSON 본문에 사용자 이름과 비밀번호를 입력해야 합니다(예: `POST /api/v3/authorize`). 사용자 인증에 성공하면 보안 토큰이 반환됩니다. 이 토큰은 이후 API 요청의 헤더에 반드시 포함해야 합니다("Authorization: Bearer *token*"). 토큰은 16시간 후에 만료됩니다.

  > StorageGRID 시스템에서 싱글 사인온(SSO)이 활성화된 경우 인증을 위해 다른 단계를 수행해야 합니다. "싱글 사인온이 활성화된 경우 API 인증"을 참조하십시오.

  인증 보안 개선에 대한 자세한 내용은 "교차 사이트 요청 위조 방지"를 참조하십시오.

- **client-certificates**: 외부 모니터링 도구를 사용하여 StorageGRID에 안전하게 액세스할 수 있도록 클라이언트 인증서를 구성하는 작업입니다.
- **config**: 제품 릴리스 및 그리드 관리 API 버전과 관련된 작업입니다. 제품 릴리스 버전과 해당 릴리스에서 지원하는 그리드 관리 API의 주요 버전을 나열할 수 있으며, 더 이상 사용되지 않는 API 버전을 비활성화할 수 있습니다.
- **deactivated-features**: 비활성화되었을 수 있는 기능을 확인하기 위한 작업입니다.
- **dns-servers**: 구성된 외부 DNS 서버를 나열하고 변경하는 작업입니다.
- **drive-details**: 특정 스토리지 어플라이언스 모델의 드라이브에 대한 작업입니다.
- **endpoint-domain-names**: S3 엔드포인트 도메인 이름을 나열하고 변경하는 작업입니다.
- **erasure-coding**: 이레이저 코딩 프로파일에 대한 작업.
- 확장: 확장에 대한 작업(절차 수준).

- **expansion-nodes**: 확장에 대한 작업(노드 수준).
- **expansion-sites**: 확장(사이트 수준)에 대한 작업.
- **grid-networks**: 그리드 네트워크 목록을 표시하고 변경하는 작업입니다.
- **grid-passwords**: 그리드 암호 관리를 위한 작업입니다.
- 그룹: 로컬 그리드 관리자 그룹을 관리하고 외부 LDAP 서버에서 페더레이션된 그리드 관리자 그룹을 검색하는 작업입니다.
- **identity-source**: 외부 ID 소스를 구성하고 페더레이션된 그룹 및 사용자 정보를 수동으로 동기화하는 작업입니다.
- **ilm**: 정보 라이프사이클 관리(ILM) 관련 운영.
- **in-progress-procedures**: 현재 진행 중인 유지 관리 절차를 검색합니다.
- 라이선스: StorageGRID 라이선스를 검색하고 업데이트하는 작업입니다.
- 로그: 로그 파일을 수집하고 다운로드하는 작업.v
- 메트릭: StorageGRID 메트릭에 대한 작업으로, 특정 시점의 메트릭 쿼리와 특정 기간 동안의 메트릭 쿼리를 포함합니다. Grid Management API는 백엔드 데이터 소스로 Prometheus 시스템 모니터링 도구를 사용합니다. Prometheus 쿼리 구성에 대한 자세한 내용은 Prometheus 웹 사이트를 참조하십시오.

> 이름에 *`private`*이(가) 포함된 메트릭은 내부 용도로만 사용됩니다. 이러한 메트릭은 StorageGRID 릴리스 간에 예고 없이 변경될 수 있습니다.

- **node-details**: 노드 세부 정보에 대한 작업입니다.
- **node-health**: 노드 상태에 대한 작업.
- **node-storage-state**: 노드 스토리지 상태에 대한 작업.
- **ntp-servers**: 외부 네트워크 시간 프로토콜(NTP) 서버를 나열하거나 업데이트하는 작업입니다.
- 객체: 객체 및 객체 메타데이터에 대한 작업.
- 복구: 복구 절차를 위한 작업.
- **recovery-package**: 복구 패키지를 다운로드하는 작업입니다.
- **regions**: 지역을 보고 생성하는 작업입니다.
- **s3-object-lock**: 전역 S3 객체 잠금 설정에 대한 작업입니다.
- **server-certificate**: Grid Manager 서버 인증서를 보고 업데이트하는 작업입니다.
- **snmp**: 현재 SNMP 구성에 대한 작업입니다.
- **storage-watermarks**: 스토리지 노드 워터마크.
- **traffic-classes**: 트래픽 분류 정책에 대한 작업입니다.
- **untrusted-client-network**: 신뢰할 수 없는 클라이언트 네트워크 구성에 대한 작업입니다.
- 사용자: Grid Manager 사용자를 보고 관리하는 작업입니다.

StorageGRID의 **Grid Management API** 버전 관리

그리드 관리 API는 버전 관리를 사용하여 서비스 중단 없는 업그레이드를 지원합니다.

예를 들어, 이 요청 URL은 API 버전 4를 지정합니다.

`https://hostname_or_ip_address/api/v4/authorize`

API의 주 버전은 이전 버전과 호환되지 않는 변경 사항이 있을 때 업데이트됩니다. 반대로 API의 부 버전은 이전 버전과 호환되는 변경 사항이 있을 때 업데이트됩니다. 호환되는 변경 사항에는 새로운 엔드포인트 또는 새로운 속성 추가가 포함됩니다.

다음 예시는 변경 유형에 따라 API 버전이 어떻게 증가하는지 보여줍니다.

API 변경 유형	이전 버전	새 버전
이전 버전과 호환됩니다	2.1	2.2
이전 버전과 호환되지 않습니다	2.1	3.0

StorageGRID 소프트웨어를 처음 설치할 때는 최신 버전의 API만 활성화됩니다. 하지만 StorageGRID의 새 기능 릴리스로 업그레이드할 때는 적어도 하나의 StorageGRID 기능 릴리스 동안 이전 버전의 API를 계속 사용할 수 있습니다.

> 지원되는 버전을 구성할 수 있습니다. "그리드 관리 API"에 대한 Swagger API 문서의 **config** 섹션을 참조하십시오. 모든 API 클라이언트를 최신 버전으로 업데이트한 후에는 이전 버전에 대한 지원을 비활성화해야 합니다.

오래된 요청은 다음과 같은 방식으로 더 이상 사용되지 않는 것으로 표시됩니다.

- 응답 헤더는 "Deprecated: true"입니다.
- JSON 응답 본문에 "deprecated": true가 포함되어 있습니다.
- nms.log 파일에 더 이상 사용되지 않음을 알리는 경고 메시지가 추가됩니다. 예를 들면 다음과 같습니다.

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

현재 릴리스에서 지원되는 **API** 버전 확인

지원되는 API 주요 버전 목록을 반환하려면 `GET /versions` API 요청을 사용하십시오. 이 요청은 Swagger API 문서의 **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 사용할 **API** 버전 지정

API 버전은 경로 매개변수 (`/api/v4`) 또는 헤더 (`Api-Version: 4`)를 사용하여 지정할 수 있습니다. 두 값을 모두 제공하는 경우 헤더 값이 경로 값을 재정의합니다.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

StorageGRID에서 **CSRF(**교차 사이트 요청 위조**)** 방지

쿠키를 사용하는 인증 방식을 강화하기 위해 CSRF 토큰을 사용하면 StorageGRID에 대한 교차 사이트 요청 위조(CSRF) 공격을 방지하는 데 도움이 됩니다. Grid Manager와 Tenant Manager는 이 보안 기능을 자동으로 활성화하며, 다른 API 클라이언트는 로그인 시 활성화 여부를 선택할 수 있습니다.

공격자는 HTTP 폼 POST와 같은 방식으로 다른 사이트에 요청을 보내 로그인한 사용자의 쿠키를 이용해 특정 요청을 발생시킬 수 있습니다.

StorageGRID는 CSRF 토큰을 사용하여 CSRF 공격으로부터 보호합니다. 이 기능이 활성화되면 특정 쿠키의 내용이 특정 헤더 또는 특정 POST 본문 매개변수의 내용과 일치해야 합니다.

이 기능을 활성화하려면 인증 중에 `csrfToken` 매개변수를 `true`으로 설정하십시오. 기본값은 `false`입니다.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

이 값이 true이면 `GridCsrfToken` 쿠키는 Grid Manager 로그인 시 임의의 값으로 설정되고, `AccountCsrfToken` 쿠키는 Tenant Manager 로그인 시 임의의 값으로 설정됩니다.

쿠키가 존재하는 경우, 시스템 상태를 변경할 수 있는 모든 요청(POST, PUT, PATCH, DELETE)에는 다음 중 하나가 반드시 포함되어야 합니다.

- The `X-Csrf-Token` 헤더이며, 헤더의 값은 CSRF 토큰 쿠키의 값으로 설정됩니다.
- 폼 인코딩된 본문을 허용하는 엔드포인트의 경우: A `csrfToken` 폼 인코딩된 요청 본문 매개변수입니다.

추가 예제 및 자세한 내용은 온라인 API 문서를 참조하십시오.

> CSRF 토큰 쿠키가 설정된 요청은 CSRF 공격에 대한 추가적인 보호 조치로 JSON 요청 본문을 예상하는 모든 요청에 대해 "Content-Type: application/json" 헤더를 강제 적용합니다.

싱글 사인온**(SSO)**이 활성화된 경우 **API**를 사용합니다**.**

SSO(Single Sign-On)가 활성화된 경우**(Active Directory) StorageGRID API**를 사용하십시오

"싱글 사인온(SSO)을 구성하고 활성화했습니다."가 있고 Active Directory를 SSO 공급자로 사용하는 경우, 그리드 관리 API 또는 테넌트 관리 API에 유효한 인증 토큰을 얻기 위해 일련의 API 요청을 실행해야 합니다.

싱글 사인온이 활성화된 경우 **API**에 로그인합니다**.**

이 지침은 Active Directory를 SSO ID 공급자로 사용하는 경우에 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 작업 정보

인증 토큰을 얻으려면 다음 예시 중 하나를 사용할 수 있습니다.

- 해당 `storagegrid-ssoauth.py` Python 스크립트는 StorageGRID 설치 파일 디렉터리((`./rpms` RHEL, `./debs` Ubuntu 또는 Debian, `./vsphere` VMware)에 있습니다.
- curl 요청의 예시 워크플로입니다.

  curl 워크플로를 너무 느리게 실행하면 시간 초과 오류가 발생할 수 있습니다. 다음과 같은 오류 메시지가 표시될 수 있습니다. `A valid SubjectConfirmation was not found on this Response`.

  > 예시로 제시된 curl 워크플로는 다른 사용자가 비밀번호를 볼 수 없도록 보호하지 않습니다.

URL 인코딩 문제가 있는 경우 다음과 같은 오류 메시지가 표시될 수 있습니다. `Unsupported SAML version`.

단계

1. 인증 토큰을 얻으려면 다음 방법 중 하나를 선택하십시오.
   - Use the `storagegrid-ssoauth.py` Python 스크립트를 사용합니다. 2단계로 이동합니다.

- curl 요청을 사용합니다. 3단계로 이동합니다.

2. `storagegrid-ssoauth.py` 스크립트를 사용하려면 Python 인터프리터에 스크립트를 전달하고 실행하십시오.

   메시지가 나타나면 다음 인수에 대한 값을 입력하십시오.

   - SSO 방식입니다. ADFS 또는 adfs를 입력하세요.
   - SSO 사용자 이름
   - StorageGRID가 설치된 도메인
   - StorageGRID의 주소
   - 테넌트 관리 API에 액세스하려면 테넌트 계정 ID가 필요합니다.

   ```
   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 토큰이 출력 결과에 제공됩니다. 이제 SSO를 사용하지 않을 때 API를 사용하는 방법과 유사하게 이 토큰을 다른 요청에 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 `TENANTACCOUNTID`로 사용하십시오.

   b. 서명된 인증 URL을 받으려면 `/api/v3/authorize-saml`에 POST 요청을 보내고 응답에서 추가 JSON 인코딩을 제거하십시오.

   이 예시는 `TENANTACCOUNTID`에 대한 서명된 인증 URL의 POST 요청을 보여줍니다. 결과는 JSON 인코딩을 제거하기 위해 `python -m json.tool`에 전달됩니다.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

이 예시의 응답에는 URL 인코딩된 서명된 URL이 포함되지만, 추가적인 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. 응답에서 `SAMLRequest`을(를) 저장하여 이후 명령에서 사용하십시오.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. AD FS에서 클라이언트 요청 ID가 포함된 전체 URL을 가져옵니다.

한 가지 방법은 이전 응답에서 받은 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 ID가 포함되어 있습니다.

```
<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 응답의 양식 작업으로 자격 증명을 전송합니다.

```
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 정보를 포함하여 302 리디렉션을 반환합니다.

> SSO 시스템에 다단계 인증(MFA)이 활성화된 경우, 폼 제출 시 두 번째 암호 또는 기타 자격 증명도 포함됩니다.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. 응답에서 `MSISAuth` 쿠키를 저장합니다.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. 인증 POST 요청에서 받은 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 로그아웃할 때 사용할 AD FS 세션 정보가 포함되고, 응답 본문에는 숨겨진 폼 필드에 SAMLResponse가 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 `SAMLResponse`을(를) 저장합니다.

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 저장된 `SAMLResponse`을 사용하여 StorageGRID `/api/saml-response` 요청을 통해 StorageGRID 인증 토큰을 생성합니다.

`RelayState`의 경우, 테넌트 계정 ID를 사용하거나, 그리드 관리 API에 로그인하려면 0을 사용하십시오.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

응답에는 인증 토큰이 포함되어 있습니다.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 응답에 포함된 인증 토큰을 `MYTOKEN`으로 저장합니다.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

이제 `MYTOKEN`를 SSO를 사용하지 않을 때 API를 사용하는 방식과 유사하게 다른 요청에도 사용할 수 있습니다.

싱글 사인온(SSO)이 활성화된 경우 API에서 로그아웃

싱글 사인온(SSO)이 활성화된 경우, 그리드 관리 API 또는 테넌트 관리 API에서 로그아웃하려면 일련의 API 요청을 실행해야 합니다. 이 지침은 Active Directory를 SSO ID 공급자로 사용하는 경우에 적용됩니다.

이 작업 정보

필요한 경우 조직의 단일 로그아웃 페이지에서 로그아웃하여 StorageGRID API에서 로그아웃할 수 있습니다. 또는 유효한 StorageGRID 베어러 토큰이 필요한 StorageGRID에서 단일 로그아웃(SLO)을 트리거할 수도 있습니다.

단계

1. 서명된 로그아웃 요청을 생성하려면 SLO API에 `cookie "sso=true"`를 전달하세요.

```
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. SLO를 트리거하고 StorageGRID로 다시 리디렉션하려면 로그아웃 URL에 요청을 보내십시오.

```
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 베어러 토큰을 삭제합니다.

StorageGRID 베어러 토큰 삭제는 SSO를 사용하지 않을 때와 동일한 방식으로 작동합니다. 쿠키 `"sso=true"`가 제공되지 않으면 SSO 상태에 영향을 주지 않고 사용자가 StorageGRID에서 로그아웃됩니다.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A `204 No Content` 응답은 사용자가 로그아웃되었음을 나타냅니다.

```
HTTP/1.1 204 No Content
```

싱글 사인온이 활성화된 경우**(Entra ID) StorageGRID API**를 사용하십시오

"싱글 사인온(SSO)을 구성하고 활성화했습니다."가 있고 Entra ID를 SSO 공급자로 사용하는 경우, 두 가지 예제 스크립트를 사용하여 Grid Management API 또는 테넌트 관리 API에 유효한 인증 토큰을 얻을 수 있습니다.

Entra ID 싱글 사인온이 활성화된 경우 **API**에 로그인

이 지침은 Entra ID를 SSO ID 공급자로 사용하는 경우에 적용됩니다.

시작하기 전에

- StorageGRID 사용자 그룹에 속한 페더레이션 사용자의 SSO 이메일 주소와 비밀번호를 알고 있습니다.
- 테넌트 관리 API에 액세스하려면 테넌트 계정 ID를 알고 있어야 합니다.

이 작업 정보

인증 토큰을 얻으려면 다음 예제 스크립트를 사용할 수 있습니다.

- `storagegrid-ssoauth-azure.py` Python 스크립트
- The `storagegrid-ssoauth-azure.js` Node.js 스크립트

두 스크립트 모두 StorageGRID 설치 파일 디렉터리((`./rpms`RHEL, `./debs`Ubuntu 또는 Debian, `./vsphere`VMware)에 있습니다.

Entra ID와의 API 통합을 직접 작성하려면 `storagegrid-ssoauth-azure.py` 스크립트를 참조하세요. 이 Python 스크립트는 StorageGRID에 직접 두 번의 요청(첫 번째는 SAMLRequest를 가져오기 위한 요청, 두 번째는 인증 토큰을 가져오기 위한 요청)을 보내고, Node.js 스크립트를 호출하여 Entra ID와 상호 작용하며 SSO 작업을 수행합니다.

SSO 작업은 일련의 API 요청을 통해 실행할 수 있지만, 그 과정이 간단하지는 않습니다. Puppeteer Node.js 모듈을 사용하여 Entra ID SSO 인터페이스를 스크래핑합니다.

URL 인코딩 문제가 있는 경우 다음과 같은 오류 메시지가 표시될 수 있습니다. `Unsupported SAML version.`

단계

1. 다음과 같이 필요한 종속성을 설치하십시오.
   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. 파이썬 스크립트를 파이썬 인터프리터에 전달하여 스크립트를 실행합니다.

   그러면 파이썬 스크립트는 해당 Node.js 스크립트를 호출하여 Entra ID SSO 상호 작용을 수행합니다.

3. 메시지가 표시되면 다음 인수에 대한 값을 입력하거나 매개변수를 사용하여 전달하십시오.
   - Entra ID에 로그인하는 데 사용되는 SSO 이메일 주소
   - StorageGRID의 주소
   - 테넌트 관리 API에 액세스하려는 경우 테넌트 계정 ID
4. 메시지가 나타나면 비밀번호를 입력하고, 요청 시 Entra ID에 대한 다단계 인증(MFA)을 제공할 준비를 하십시오.

이 스크립트는 Microsoft Authenticator를 사용한 MFA를 가정합니다. 다른 형태의 MFA(예: 문자 메시지로 받은 코드 입력)를 지원하도록 스크립트를 수정해야 할 수도 있습니다.

StorageGRID 인증 토큰이 출력 결과에 제공됩니다. 이제 SSO를 사용하지 않을 때 API를 사용하는 방법과 유사하게 이 토큰을 다른 요청에 사용할 수 있습니다.

SSO(Single Sign-On)가 활성화된 경우**(PingFederate) StorageGRID API**를 사용합니다

"싱글 사인온(SSO)을 구성하고 활성화했습니다."가 있고 PingFederate를 SSO 제공업체로 사용하는 경우, 그리드 관리 API 또는 테넌트 관리 API에 유효한 인증 토큰을 얻기 위해 일련의 API 요청을 실행해야 합니다.

싱글 사인온이 활성화된 경우 **API**에 로그인합니다**.**

이 지침은 SSO ID 공급자로 PingFederate를 사용하는 경우에 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 작업 정보

인증 토큰을 얻으려면 다음 예시 중 하나를 사용할 수 있습니다.

- 해당 `storagegrid-ssoauth.py` Python 스크립트는 StorageGRID 설치 파일 디렉터리((`./rpms` RHEL, `./debs` Ubuntu 또는 Debian, `./vsphere` VMware)에 있습니다.
- curl 요청의 예시 워크플로입니다.

  curl 워크플로를 너무 느리게 실행하면 시간 초과 오류가 발생할 수 있습니다. 다음과 같은 오류 메시지가 표시될 수 있습니다. `A valid SubjectConfirmation was not found on this Response`.

  예시로 제시된 curl 워크플로는 다른 사용자가 비밀번호를 볼 수 없도록 보호하지 않습니다.

  URL 인코딩 문제가 있는 경우 다음과 같은 오류 메시지가 표시될 수 있습니다. `Unsupported SAML version`.

단계

1. 인증 토큰을 얻으려면 다음 방법 중 하나를 선택하십시오.
   - Use the `storagegrid-ssoauth.py` Python 스크립트를 사용합니다. 2단계로 이동합니다.
   - curl 요청을 사용합니다. 3단계로 이동합니다.
2. `storagegrid-ssoauth.py` 스크립트를 사용하려면 Python 인터프리터에 스크립트를 전달하고 실행하십시오.

   메시지가 나타나면 다음 인수에 대한 값을 입력하십시오.
   - SSO 방식입니다. "pingfederate"의 어떤 변형이든 입력할 수 있습니다(PINGFEDERATE, pingfederate 등).
   - SSO 사용자 이름
   - StorageGRID가 설치된 도메인입니다. 이 필드는 PingFederate에 사용되지 않습니다. 비워두거나 임의의

값을 입력할 수 있습니다.

- StorageGRID의 주소
- 테넌트 관리 API에 액세스하려면 테넌트 계정 ID가 필요합니다.

```
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 토큰이 출력 결과에 제공됩니다. 이제 SSO를 사용하지 않을 때 API를 사용하는 방법과 유사하게 이 토큰을 다른 요청에 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 `TENANTACCOUNTID`로 사용하십시오.

   b. 서명된 인증 URL을 받으려면 `/api/v3/authorize-saml`에 POST 요청을 보내고 응답에서 추가 JSON 인코딩을 제거하십시오.

   이 예시는 TENANTACCOUNTID에 대한 서명된 인증 URL을 요청하는 POST 요청을 보여줍니다. 결과는 python -m json.tool에 전달되어 JSON 인코딩이 제거됩니다.

```
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 예시의 응답에는 URL 인코딩된 서명된 URL이 포함되지만, 추가적인 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. 응답에서 `SAMLRequest`을(를) 저장하여 이후 명령에서 사용하십시오.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. 응답과 쿠키를 내보내고 응답을 출력합니다.

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. 'pf.adapterId' 값을 내보내고 응답을 출력합니다.

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. 'href' 값을 내보내고(끝에 있는 슬래시(/)를 제거), 응답을 출력합니다.

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. 'action' 값을 내보냅니다.

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. 쿠키를 자격 증명과 함께 전송:

```
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 `SAMLResponse`을(를) 저장합니다.

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 저장된 `SAMLResponse`을 사용하여 StorageGRID `/api/saml-response` 요청을 통해 StorageGRID 인증 토큰을 생성합니다.

`RelayState`의 경우, 테넌트 계정 `ID`를 사용하거나, 그리드 관리 `API`에 로그인하려면 `0`을 사용하십시오.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

응답에는 인증 토큰이 포함되어 있습니다.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 응답에 포함된 인증 토큰을 `MYTOKEN`으로 저장합니다.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

이제 `MYTOKEN`를 SSO를 사용하지 않을 때 API를 사용하는 방식과 유사하게 다른 요청에도 사용할 수 있습니다.

싱글 사인온(SSO)이 활성화된 경우 API에서 로그아웃

싱글 사인온(SSO)이 활성화된 경우, 그리드 관리 API 또는 테넌트 관리 API에서 로그아웃하려면 일련의 API 요청을

실행해야 합니다. 이 지침은 PingFederate를 SSO ID 공급자로 사용하는 경우에 적용됩니다.

이 작업 정보

필요한 경우 조직의 단일 로그아웃 페이지에서 로그아웃하여 StorageGRID API에서 로그아웃할 수 있습니다. 또는 유효한 StorageGRID 베어러 토큰이 필요한 StorageGRID에서 단일 로그아웃(SLO)을 트리거할 수도 있습니다.

단계

1. 서명된 로그아웃 요청을 생성하려면 SLO API에 `cookie "sso=true"`를 전달하세요.

```
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. SLO를 트리거하고 StorageGRID로 다시 리디렉션하려면 로그아웃 URL에 요청을 보내십시오.

```
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 베어러 토큰을 삭제합니다.

StorageGRID 베어러 토큰 삭제는 SSO를 사용하지 않을 때와 동일한 방식으로 작동합니다. 쿠키 `"sso=true"`가 제공되지 않으면 SSO 상태에 영향을 주지 않고 사용자가 StorageGRID에서 로그아웃됩니다.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A `204 No Content` 응답은 사용자가 로그아웃되었음을 나타냅니다.

```
HTTP/1.1 204 No Content
```

API를 사용하여 **StorageGRID** 기능을 비활성화합니다

StorageGRID 시스템에서 특정 기능을 완전히 비활성화하려면 그리드 관리 API를 사용할 수 있습니다. 기능이 비활성화되면 해당 기능과 관련된 작업을 수행할 수 있는 권한을 누구에게도 부여할 수 없습니다.

이 작업 정보

비활성화된 기능 시스템을 사용하면 StorageGRID 시스템의 특정 기능에 대한 액세스를 차단할 수 있습니다. 기능을 비활성화하는 것은 루트 액세스 권한이 있는 관리자 그룹에 속한 루트 사용자 또는 사용자가 해당 기능을 사용하지 못하도록 하는 유일한 방법입니다.

이 기능이 어떻게 유용할 수 있는지 이해하려면 다음 시나리오를 고려하십시오.

A사는 테넌트 계정을 생성하여 StorageGRID 시스템의 스토리지 용량을 임대하는 서비스 제공업체입니다. A사는 임대 고객의 오브젝트 보안을 보호하기 위해 테넌트 계정 배포 후에는 자사 직원이 어떠한 테넌트 계정에도 액세스할 수 없도록 보장하고자 합니다.

A사는 그리드 관리 API의 기능 비활성화 시스템을 사용하여 이 목표를 달성할 수 있습니다. 그리드 관리자(UI 및 API 모두)에서 테넌트 루트 암호 변경 기능을 완전히 비활성화함으로써, A사는 루트 사용자 및 루트 액세스 권한이 있는 그룹에 속한 사용자를 포함한 관리자 사용자가 어떤 테넌트 계정의 루트 사용자 암호도 변경할 수 없도록 합니다.

단계

1. Grid Management API에 대한 Swagger 문서에 액세스합니다. "그리드 관리 API 사용"을 참조하십시오.
2. 기능 비활성화 엔드포인트를 찾으십시오.
3. 테넌트 루트 암호 변경과 같은 기능을 비활성화하려면 다음과 같은 본문을 API에 전송하십시오.

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   요청이 완료되면 테넌트 루트 암호 변경 기능이 비활성화됩니다. 테넌트 루트 암호 변경 관리 권한은 더 이상 사용자 인터페이스에 표시되지 않으며, 테넌트의 루트 암호를 변경하려는 API 요청은 "403 Forbidden" 오류와 함께 실패합니다.

기본적으로 그리드 관리 API를 사용하여 비활성화된 기능을 다시 활성화할 수 있습니다. 하지만 비활성화된 기능이 다시 활성화되지 않도록 하려면 **activateFeatures** 기능 자체를 비활성화하면 됩니다.

activateFeatures 기능은 다시 활성화할 수 없습니다. 이 기능을 비활성화하면 비활성화된 다른 모든 기능을 영구적으로 다시 활성화할 수 없게 됩니다. 손실된 기능을 복구하려면 기술 지원팀에 문의해야 합니다.

단계

1. 그리드 관리 API에 대한 Swagger 문서를 참조하십시오.
2. 기능 비활성화 엔드포인트를 찾으십시오.
3. 모든 기능을 다시 활성화하려면 다음과 같은 본문을 API로 전송하세요.

```
{ "grid": null }
```

이 요청이 완료되면 테넌트 루트 암호 변경 기능을 포함한 모든 기능이 다시 활성화됩니다. 테넌트 루트 암호 변경 관리 권한이 이제 사용자 인터페이스에 표시되며, 사용자가 루트 액세스 또는 테넌트 루트 암호 변경 관리 권한을 가지고 있는 경우 테넌트의 루트 암호를 변경하려는 모든 API 요청이 성공적으로 처리됩니다.

위 예시는 비활성화된 모든 기능을 다시 활성화합니다. 비활성화된 상태로 유지되어야 하는 다른 기능이 있는 경우, PUT 요청에 해당 기능을 명시적으로 지정해야 합니다. 예를 들어, 테넌트 루트 암호 변경 기능을 다시 활성화하고 storageAdmin 관리 권한은 계속 비활성화하려면 다음과 같은 PUT 요청을 보내십시오.

```
{ "grid": {"storageAdmin": true} }
```

StorageGRID에 대한 액세스 제어

StorageGRID 액세스 제어

StorageGRID 그룹 및 사용자를 생성하거나 가져오고 각 그룹에 권한을 할당하여 StorageGRID에 액세스할 수 있는 사용자와 수행할 수 있는 작업을 제어할 수 있습니다. 선택적으로 단일 로그인(SSO)을 활성화하고, 클라이언트 인증서를 생성하고, 그리드 암호를 변경할 수 있습니다.

그리드 관리자에 대한 액세스 제어

ID 페더레이션 서비스에서 그룹과 사용자를 가져오거나 로컬 그룹과 로컬 사용자를 설정하여 그리드 관리자 및 그리드 관리 API에 액세스할 수 있는 사용자를 결정합니다.

"ID 페더레이션"을 사용하면 "그룹" 및 "사용자" 설정을 더 빠르게 수행할 수 있으며, 사용자가 익숙한 자격 증명을 사용하여 StorageGRID에 로그인할 수 있습니다. Active Directory, OpenLDAP 또는 Oracle Directory Server를 사용하는 경우 자격 증명 페더레이션을 구성할 수 있습니다.

다른 LDAP v3 서비스를 사용하려면 기술 지원팀에 문의하십시오.

각 그룹에 서로 다른 "권한"을 할당하여 각 사용자가 수행할 수 있는 작업을 결정합니다. 예를 들어, 한 그룹의 사용자는

ILM 규칙을 관리할 수 있도록 하고, 다른 그룹의 사용자는 유지 관리 작업을 수행할 수 있도록 할 수 있습니다. 사용자는 시스템에 액세스하려면 최소한 하나의 그룹에 속해야 합니다.

선택적으로 그룹을 읽기 전용으로 구성할 수 있습니다. 읽기 전용 그룹의 사용자는 설정 및 기능만 볼 수 있습니다. Grid Manager 또는 Grid Management API에서 변경하거나 작업을 수행할 수 없습니다.

싱글 사인온 활성화

StorageGRID 시스템은 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용한 싱글 사인온(SSO)을 지원합니다. "SSO 구성 및 활성화" 후 모든 사용자는 Grid Manager, Tenant Manager, Grid Management API 또는 Tenant Management API에 액세스하기 전에 외부 ID 공급자를 통해 인증을 받아야 합니다. 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

프로비저닝 암호 변경

프로비저닝 암호는 여러 설치 및 유지 관리 절차와 StorageGRID 복구 패키지 다운로드에 필요합니다. 또한 StorageGRID 시스템의 그리드 토폴로지 정보 및 암호화 키 백업을 다운로드하는 데에도 암호가 필요합니다. 필요에 따라 "암호를 변경합니다"할 수 있습니다.

노드 콘솔 암호 변경

그리드의 각 노드에는 노드 콘솔 암호가 있으며, 이 암호는 SSH를 사용하여 "admin"으로 노드에 로그인하거나 VM/물리적 콘솔 연결에서 루트 사용자로 로그인하는 데 필요합니다. 필요에 따라 "노드 콘솔 암호 변경" 각 노드에 대해 암호를 설정할 수 있습니다.

StorageGRID 프로비저닝 암호를 변경하세요

이 절차를 사용하여 StorageGRID 프로비저닝 암호를 변경하십시오. 암호는 복구, 확장 및 유지 관리 절차에 필요합니다. 또한 그리드 토폴로지 정보, 그리드 노드 콘솔 암호 및 StorageGRID 시스템의 암호화 키가 포함된 복구 패키지 백업을 다운로드하는 데에도 암호가 필요합니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 현재 프로비저닝 암호를 가지고 계십니다.

이 작업 정보

프로비저닝 암호는 여러 설치 및 유지 관리 절차와 "복구 패키지 다운로드 중"에 필요합니다. 프로비저닝 암호는 `Passwords.txt` 파일에 나열되어 있지 않습니다. 프로비저닝 암호를 문서화하고 안전한 위치에 보관하십시오.

단계

1. 구성 > 액세스 제어 > *그리드 암호*를 선택합니다.
2. *프로비저닝 암호 변경*에서 *변경하기*를 선택합니다.
3. 현재 프로비저닝 암호를 입력하십시오.
4. 새로운 암호를 입력하세요. 암호는 8자 이상 32자 이하여야 합니다. 암호는 대소문자를 구분합니다.

> 프로비저닝 암호를 안전한 장소에 보관하십시오. 설치, 확장 및 유지 관리 절차에 필요합니다.

5. 새 암호를 다시 입력하고 *저장*을 선택합니다.

   프로비저닝 암호 변경이 완료되면 시스템에 녹색 성공 배너가 표시됩니다.

6. *복구 패키지*를 선택합니다.
7. 새 복구 패키지를 다운로드하려면 새 프로비저닝 암호를 입력하십시오.

   프로비저닝 암호를 변경한 후에는 즉시 새 복구 패키지를 다운로드해야 합니다. 복구 패키지 파일을 사용하면 오류 발생 시 시스템을 복원할 수 있습니다.

StorageGRID에서 노드 콘솔 암호 변경

그리드의 각 노드에는 노드 콘솔 암호가 있으며, 이 암호를 사용하여 노드에 로그인합니다. 기본적으로 각 노드에는 고유한 암호가 할당됩니다. 각 노드의 암호를 새롭고 고유한 암호로 변경하거나, 모든 노드의 암호를 전역 암호로 변경할 수 있습니다. 암호는 복구 패키지에 저장됩니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "유지 관리 또는 루트 액세스 권한".
- 현재 프로비저닝 암호를 가지고 계십니다.

이 작업 정보

SSH를 통해 "admin"으로 노드에 로그인하거나 VM/물리적 콘솔 연결에서 루트 사용자로 로그인할 때 노드 콘솔 암호를 사용합니다. 다음 옵션 중 하나를 사용하여 노드 콘솔 암호를 변경할 수 있습니다.

- 각 노드에 자동으로 임의의 암호를 적용합니다.
- 모든 노드에 하나의 전역 암호를 지정하고 적용합니다
- 하나 이상의 노드에 고유한 암호를 지정하고 적용합니다.

암호는 복구 패키지에 포함된 업데이트된 `Passwords.txt` 파일에 저장됩니다. 암호는 파일의 '암호' 열에 나열되어 있습니다.

노드 간 통신에 사용되는 SSH 키의 "SSH 액세스 암호"은(는) 노드 콘솔 암호와 별개입니다. 이 절차는 SSH 접속 암호를 변경하지 않습니다.

마법사에 액세스합니다

단계

1. 구성 > 액세스 제어 > *그리드 암호*를 선택합니다.
2. *노드 콘솔 암호 변경*에서 *변경하기*를 선택합니다.

현재 복구 패키지 다운로드

노드 콘솔 암호를 변경하기 전에 최신 복구 패키지를 다운로드하십시오. 암호 변경 과정이 노드에 대해 실패할 경우 이 파일에 있는 암호를 사용할 수 있습니다.

단계

1. 그리드에 사용할 프로비저닝 암호를 입력하십시오.
2. *복구 패키지 다운로드*를 선택합니다.
3. 복구 패키지 파일((`.zip`)을 안전하고 보안이 유지되는 서로 다른 두 곳에 복사하십시오.

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

4. *Continue*를 선택합니다.

새 비밀번호 제공

1. 원하는 비밀번호 변경 방법을 선택하십시오.
   - 자동: StorageGRID가 모든 노드에 새로운 임의 콘솔 암호를 자동으로 할당합니다.
   - **Custom**: 콘솔 암호를 제공합니다.

자동

1. *Continue*를 선택합니다.

사용자 지정

1. 다음 중 하나를 선택하십시오.
   - 전역 콘솔 암호: 모든 노드에 동일한 콘솔 암호를 적용하십시오.
   - 고유 콘솔 암호: 하나 이상의 노드에 서로 다른 암호를 적용합니다.
2. *전역 콘솔 암호*를 선택한 경우 모든 노드에서 사용할 암호를 입력하십시오.
3. *고유 콘솔 암호*를 선택한 경우 하나 이상의 노드에 대해 고유한 암호를 입력하십시오.
4. *Continue*를 선택합니다.

비밀번호 변경을 완료합니다

1. 확인 대화 상자가 나타나면 StorageGRID 노드 콘솔 암호 변경을 시작하도록 허용하려면 *예*를 선택하십시오.

   일단 시작된 과정은 취소할 수 없습니다.

   StorageGRID가 새 암호가 포함된 새 복구 패키지를 생성합니다.

2. 새 복구 패키지가 준비되면 *새 복구 패키지 다운로드*를 선택하고 복구 패키지를 저장하십시오.
3. `.zip` 파일을 여세요.

4. 콘텐츠에 접근할 수 있는지 확인하십시오. 여기에는 새 노드 콘솔 암호가 포함된 `Passwords.txt` 파일이 포함됩니다.
5. 새 복구 패키지 파일(`.zip`)을 안전하고 보안이 유지되는 서로 다른 두 곳에 복사하십시오.

   > 기존 복구 패키지를 덮어쓰지 마세요.

   복구 파일에는 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가 포함되어 있으므로 복구 파일을 안전하게 보호해야 합니다.

6. 새 복구 패키지를 다운로드하고 내용을 확인했음을 나타내려면 확인란을 선택하십시오.
7. *Continue*를 선택합니다.

   StorageGRID 각 노드의 비밀번호를 업데이트합니다.

   업데이트 과정 중 오류가 발생하면 진행률 표시줄에 암호 변경에 실패한 노드 수가 표시됩니다. 시스템은 암호 변경에 실패한 노드에 대해 자동으로 재시도합니다. 재시도 후에도 일부 노드의 암호가 변경되지 않은 경우 재시도 버튼이 나타납니다.

8. 하나 이상의 노드에서 암호 업데이트가 실패한 경우:
   a. 표에 나열된 오류 메시지를 검토하십시오.
   b. 문제를 해결하세요.
   c. *다시 시도*를 선택합니다.

      > 재시도 기능은 이전 암호 변경 시도에서 실패한 노드의 노드 콘솔 암호만 변경합니다.

9. 진행률 표시줄에 더 이상 업데이트할 내용이 없음을 나타내면 *완료*를 선택하십시오.
10. 모든 노드의 노드 콘솔 암호를 변경한 후 처음 다운로드한 복구 패키지을(를) 삭제하십시오.

StorageGRID 관리 노드의 SSH 액세스 암호 변경

관리자 노드의 SSH 접속 암호를 변경하면 그리드 내 각 노드의 고유한 내부 SSH 키 세트도 업데이트됩니다. 기본 관리자 노드는 이러한 SSH 키를 사용하여 안전하고 암호 없는 인증 방식으로 노드에 접속합니다.

SSH 키를 사용하여 노드에 `admin`로 로그인하거나 VM 또는 물리적 콘솔 연결에서 루트 사용자로 로그인할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "유지 관리 또는 루트 액세스 권한".
- 현재 프로비저닝 암호를 가지고 계십니다.

이 작업 정보

관리자 노드에 대한 새 액세스 암호와 각 노드에 대한 새 내부 키는 복구 패키지의 `Passwords.txt` 파일에 저장되어 있습니다. 키는 해당 파일의 암호 열에 나열되어 있습니다.

노드 간 통신에 사용되는 SSH 키에는 각각 별도의 SSH 접속 암호가 있습니다. 이 절차로는 해당 암호가 변경되지 않습니다.

마법사에 액세스합니다

단계

1. 구성 > 액세스 제어 > *그리드 암호*를 선택합니다.
2. *SSH 키 변경*에서 *변경하기*를 선택합니다.

현재 복구 패키지 다운로드

SSH 액세스 키를 변경하기 전에 최신 복구 패키지를 다운로드하십시오. 키 변경 과정이 실패할 경우 이 파일에 있는 키를 사용할 수 있습니다.

단계

1. 그리드에 사용할 프로비저닝 암호를 입력하십시오.
2. *복구 패키지 다운로드*를 선택합니다.
3. 복구 패키지 파일(`.zip`)을 안전하고 보안이 유지되는 서로 다른 두 곳에 복사하십시오.

> 복구 패키지 파일에는 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 *예*를 선택하십시오.

> 일단 시작된 과정은 취소할 수 없습니다.

SSH 액세스 키 변경

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 몇 분 정도 기다려 주십시오.
2. 새 복구 패키지 다운로드 버튼이 활성화되면 *새 복구 패키지 다운로드*를 선택하고 새 복구 패키지 파일(`.zip`)을 안전하고 서로 다른 두 위치에 저장하십시오.
3. 다운로드가 완료되면:
   a. `.zip` 파일을 여세요.
   b. 새 SSH 액세스 키가 포함된 `Passwords.txt` 파일을 포함하여 콘텐츠에 액세스할 수 있는지 확인하십시오.
   c. 새 복구 패키지 파일(`.zip`)을 안전하고 보안이 유지되는 서로 다른 두 곳에 복사하십시오.

> 기존 복구 패키지를 덮어쓰지 마세요.

복구 패키지 파일에는 StorageGRID 시스템에서 데이터를 가져오는 데 사용할 수 있는 암호화 키와 암호가

포함되어 있으므로 보안을 유지해야 합니다.

4. 각 노드에서 키가 업데이트될 때까지 몇 분 정도 기다립니다.

   모든 노드의 키가 변경되면 녹색 성공 배너가 나타납니다.

   업데이트 과정 중 오류가 발생하면 키 변경에 실패한 노드 수를 나타내는 배너 메시지가 표시됩니다. 시스템은 키 변경에 실패한 노드에 대해 자동으로 재시도합니다. 재시도 후에도 일부 노드의 키가 변경되지 않은 경우 **Retry** 버튼이 나타납니다.

   하나 이상의 노드에서 키 업데이트가 실패한 경우:

   a. 표에 나열된 오류 메시지를 검토하십시오.
   b. 문제를 해결하세요.
   c. *다시 시도*를 선택합니다.

      재시도 기능은 이전 키 변경 시도 중에 실패한 노드의 SSH 액세스 키만 변경합니다.

5. 모든 노드의 SSH 액세스 키를 변경한 후에는 처음 다운로드한 복구 패키지을 삭제하십시오.
6. 필요에 따라 유지 관리 > 시스템 > *복구 패키지*를 선택하여 새 복구 패키지의 추가 사본을 다운로드할 수 있습니다.

StorageGRID에서 ID 페더레이션 사용

ID 페더레이션을 사용하면 그룹 및 사용자 설정이 더 빨라지고 사용자는 익숙한 자격 증명을 사용하여 StorageGRID에 로그인할 수 있습니다.

Grid Manager에 대한 ID 페더레이션 구성

관리자 그룹과 사용자를 Active Directory, Microsoft Entra ID, OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 관리하려면 Grid Manager에서 ID 페더레이션을 구성할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 당신은 "특정 액세스 권한".
- 현재 Active Directory, Microsoft Entra ID, OpenLDAP 또는 Oracle Directory Server를 ID 공급자로 사용하고 있습니다.

  목록에 없는 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의하십시오.

- OpenLDAP을 사용하려면 OpenLDAP 서버를 구성해야 합니다. OpenLDAP 서버 구성 지침을 참조하십시오.
- 싱글 사인온(SSO)을 활성화할 계획이라면 "싱글 사인온(SSO)의 요구 사항 및 고려 사항"을(를) 검토했습니다.
- LDAP 서버와의 통신에 TLS(Transport Layer Security)를 사용할 계획이라면 ID 공급자가 TLS 1.2 또는 1.3을 사용하고 있어야 합니다. "TLS 발신 연결에 지원되는 암호화 방식"을 참조하십시오.

이 작업 정보

Active Directory, Microsoft Entra ID, OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 그룹을

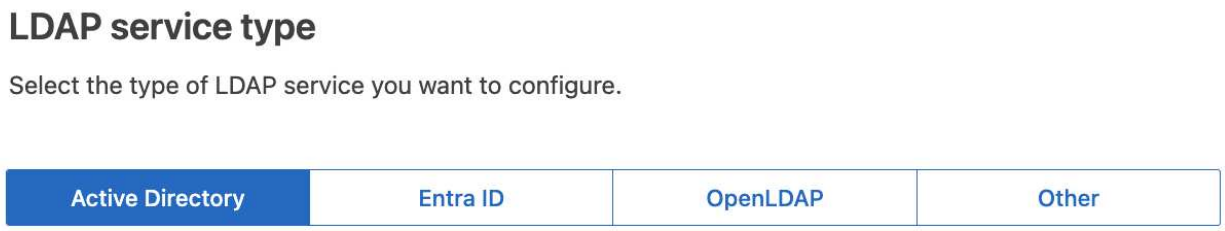
가져오려면 Grid Manager용 ID 소스를 구성할 수 있습니다. 다음 유형의 그룹을 가져올 수 있습니다.

- 관리자 그룹. 관리자 그룹에 속한 사용자는 그룹에 할당된 관리 권한에 따라 그리드 관리자에 로그인하여 작업을 수행할 수 있습니다.
- 자체 ID 소스를 사용하지 않는 테넌트를 위한 테넌트 사용자 그룹입니다. 테넌트 그룹에 속한 사용자는 테넌트 관리자에 로그인하여 테넌트 관리자에서 그룹에 할당된 권한에 따라 작업을 수행할 수 있습니다. 자세한 내용은 "테넌트 계정 생성" 및 "테넌트 계정 사용"을 참조하십시오.

구성 입력

단계

1. 구성 > 액세스 제어 > **ID** 연동 을 선택합니다.
2. *ID 페더레이션 활성화*를 선택합니다.
3. LDAP 서비스 유형 섹션에서 구성하려는 LDAP 서비스 유형을 선택합니다.



Oracle Directory Server를 사용하는 LDAP 서버의 값을 구성하려면 *기타*를 선택하십시오.

4. *기타*를 선택한 경우 LDAP 속성 섹션의 필드를 작성하십시오. 그렇지 않으면 다음 단계로 진행하십시오.
   - 사용자 고유 이름: LDAP 사용자의 고유 식별자를 포함하는 속성 이름입니다. 이 속성은 Active Directory의 경우 `sAMAccountName`, OpenLDAP의 경우 `uid`와 동일합니다. Oracle Directory Server를 구성하는 경우 `uid`를 입력합니다.
   - 사용자 **UUID**: LDAP 사용자의 영구 고유 식별자를 포함하는 속성 이름입니다. 이 속성은 Active Directory의 경우 `objectGUID`와, OpenLDAP의 경우 `entryUUID`와 동일합니다. Oracle Directory Server를 구성하는 경우 `nsuniqueid`를 입력하십시오. 지정된 속성에 대한 각 사용자의 값은 16바이트 또는 문자열 형식의 32자리 16진수여야 하며, 하이픈은 무시됩니다.
   - 그룹 고유 이름: LDAP 그룹의 고유 식별자를 포함하는 속성 이름입니다. 이 속성은 Active Directory의 경우 `sAMAccountName`, OpenLDAP의 경우 `cn`와 동일합니다. Oracle Directory Server를 구성하는 경우 `cn`를 입력합니다.
   - 그룹 **UUID**: LDAP 그룹의 영구 고유 식별자를 포함하는 속성 이름입니다. 이 속성은 Active Directory의 경우 `objectGUID`, OpenLDAP의 경우 `entryUUID`와 동일합니다. Oracle Directory Server를 구성하는 경우 `nsuniqueid`를 입력합니다. 지정된 속성에 대한 각 그룹의 값은 16바이트 또는 문자열 형식의 32자리 16진수여야 하며, 하이픈은 무시됩니다.
5. 모든 LDAP 서비스 유형에 대해 LDAP 서버 구성 섹션에서 필요한 LDAP 서버 및 네트워크 연결 정보를 입력하십시오.
   - 호스트 이름: LDAP 서버의 정규화된 도메인 이름(FQDN) 또는 IP 주소.
   - 포트: LDAP 서버에 연결하는 데 사용되는 포트입니다.

> STARTTLS의 기본 포트는 389이고, LDAPS의 기본 포트는 636입니다. 하지만 방화벽이 올바르게 구성되어 있다면 어떤 포트든 사용할 수 있습니다.

- 사용자 이름: LDAP 서버에 연결할 사용자의 고유 이름(DN) 전체 경로입니다.

  Active Directory의 경우 하위 레벨 로그온 이름 또는 사용자 주체 이름을 지정할 수도 있습니다.

  지정된 사용자는 그룹 및 사용자 목록을 볼 수 있는 권한과 다음 속성에 접근할 수 있는 권한이 있어야 합니다.

  - `sAMAccountName` 또는 `uid`
  - `objectGUID`, `entryUUID` 또는 `nsuniqueid`
  - `cn`
  - `memberOf` 또는 `isMemberOf`
  - **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, 및 `userPrincipalName`
  - **Entra ID**: `accountEnabled` 및 `userPrincipalName`

- **Password**: 사용자 이름과 연결된 비밀번호입니다.

  > 향후 비밀번호를 변경하는 경우, 반드시 이 페이지에서 업데이트해야 합니다.

- 그룹 기본 **DN**: 그룹을 검색할 LDAP 하위 트리의 고유 이름(DN)의 전체 경로입니다. 아래 Active Directory 예시에서 고유 이름이 기본 DN(DC=storagegrid,DC=example,DC=com)을 기준으로 하는 모든 그룹은 페더레이션 그룹으로 사용할 수 있습니다.

  > 그룹 고유 이름 값은 해당 그룹 기본 **DN** 내에서 고유해야 합니다.

- 사용자 기본 **DN**: 사용자를 검색하려는 LDAP 하위 트리의 고유 이름(DN)의 전체 경로입니다.

  > 사용자 고유 이름 값은 해당 사용자 기본 **DN** 내에서 고유해야 합니다.

- 바인드 사용자 이름 형식 (선택 사항): 패턴을 자동으로 확인할 수 없는 경우 StorageGRID에서 사용할 기본 사용자 이름 패턴입니다.

  *바인딩 사용자 이름 형식*을 제공하는 것이 좋습니다. 이렇게 하면 StorageGRID 서비스 계정과 바인딩할 수 없는 경우에도 사용자가 로그인할 수 있습니다.

  다음 패턴 중 하나를 입력하세요:

  - **UserPrincipalName 패턴(AD 및 Entra ID)**: `[USERNAME]@*example*.com`
  - 하위 레벨 로그온 이름 패턴**(AD 및 Entra ID)**: `*example*\[USERNAME]`
  - 고유 이름 패턴: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

    *[USERNAME]*을 정확히 입력하세요.

6. 전송 계층 보안(TLS) 섹션에서 보안 설정을 선택합니다.

- **STARTTLS** 사용: STARTTLS를 사용하여 LDAP 서버와의 통신을 보호합니다. Active Directory, OpenLDAP 또는 기타 시스템에는 이 옵션을 권장하지만, Microsoft Entra ID에서는 이 옵션이 지원되지 않습니다.
- **LDAPS** 사용: LDAPS(SSL을 통한 LDAP) 옵션은 TLS를 사용하여 LDAP 서버에 연결을 설정합니다. Microsoft Entra ID를 사용하려면 이 옵션을 선택해야 합니다.
- **TLS**를 사용하지 마십시오: StorageGRID 시스템과 LDAP 서버 간의 네트워크 트래픽은 보호되지 않습니다. 이 옵션은 Microsoft Entra ID에서 지원되지 않습니다.

> Active Directory 서버에서 LDAP 서명을 강제하는 경우 **TLS**를 사용하지 않음 옵션은 지원되지 않습니다. STARTTLS 또는 LDAPS를 사용해야 합니다.

7. STARTTLS 또는 LDAPS를 선택한 경우 연결을 보호하는 데 사용되는 인증서를 선택하십시오.
   - 운영체제 **CA** 인증서 사용: 연결을 보호하기 위해 운영체제에 설치된 기본 Grid CA 인증서를 사용합니다.
   - 사용자 지정 **CA** 인증서 사용: 사용자 지정 보안 인증서를 사용합니다.

     이 설정을 선택한 경우 사용자 지정 보안 인증서를 CA 인증서 텍스트 상자에 복사하여 붙여넣으세요.

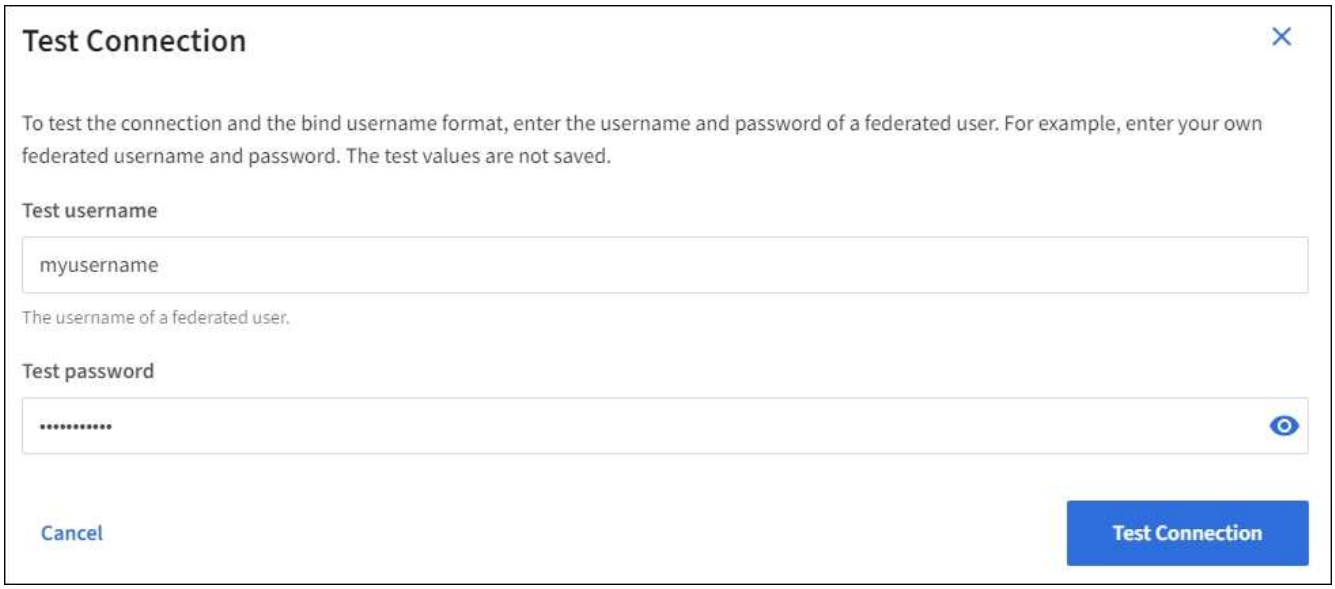
연결을 테스트하고 구성을 저장합니다

모든 값을 입력한 후 구성을 저장하기 전에 연결을 테스트해야 합니다. StorageGRID는 LDAP 서버의 연결 설정과 바인드 사용자 이름 형식(제공한 경우)을 확인합니다.

단계

1. *연결 테스트*를 선택합니다.
2. 바인딩 사용자 이름 형식을 제공하지 않은 경우:
   - 연결 설정이 유효하면 "연결 테스트 성공" 메시지가 나타납니다. *저장*을 선택하여 구성을 저장합니다.
   - 연결 설정이 올바르지 않으면 "테스트 연결을 설정할 수 없습니다"라는 메시지가 나타납니다. *닫기*를 선택합니다. 그런 다음 문제를 해결하고 연결을 다시 테스트하십시오.
3. 바인딩 사용자 이름 형식을 제공한 경우 유효한 페더레이션 사용자의 사용자 이름과 암호를 입력하십시오.

   예를 들어, 본인의 사용자 이름과 비밀번호를 입력하십시오. 사용자 이름에 @ 또는 /와 같은 특수 문자를 포함하지 마십시오.



- 연결 설정이 유효하면 "연결 테스트 성공" 메시지가 나타납니다. *저장*을 선택하여 구성을 저장합니다.
- 연결 설정, 바인딩 사용자 이름 형식 또는 테스트 사용자 이름 및 암호가 유효하지 않으면 오류 메시지가 나타납니다. 문제를 해결한 후 연결을 다시 테스트하십시오.

ID 소스와 강제 동기화

StorageGRID 시스템은 ID 소스에서 페더레이션 그룹 및 사용자를 주기적으로 동기화합니다. 사용자 권한을 최대한 빨리 활성화하거나 제한하려면 동기화를 강제로 시작할 수 있습니다.

단계

1. ID 연동 페이지로 이동합니다.
2. 페이지 상단에서 *동기화 서버*를 선택합니다.

   동기화 과정은 사용 환경에 따라 다소 시간이 걸릴 수 있습니다.

   ID 페더레이션 동기화 실패 경고는 ID 소스에서 페더레이션된 그룹 및 사용자를 동기화하는 데 문제가 발생할 경우 발생합니다.

ID 연동 비활성화

그룹 및 사용자에 대한 ID 페더레이션을 일시적 또는 영구적으로 비활성화할 수 있습니다. ID 페더레이션이 비활성화되면 StorageGRID 와 ID 소스 간의 통신이 중단됩니다. 하지만 구성한 설정은 모두 유지되므로 나중에 ID 페더레이션을 쉽게 다시 활성화할 수 있습니다.

이 작업 정보

ID 페더레이션을 비활성화하기 전에 다음 사항을 숙지해야 합니다.

- 페더레이션 사용자는 로그인할 수 없습니다.
- 현재 로그인 중인 페더레이션 사용자는 세션이 만료될 때까지 StorageGRID 시스템에 계속 액세스할 수 있지만, 세션이 만료된 후에는 로그인할 수 없습니다.
- StorageGRID 시스템과 ID 소스 간의 동기화는 발생하지 않으며, 동기화되지 않은 계정에 대한 알림도 표시되지

않습니다.

- 싱글 사인온(SSO) 상태가 '사용' 또는 '샌드박스 모드'인 경우 'ID 페더레이션 사용' 확인란이 비활성화됩니다. ID 페더레이션을 비활성화하려면 싱글 사인온 페이지의 SSO 상태가 '사용 안 함'이어야 합니다. "싱글 사인온 비활성화"을 참조하십시오.

단계

1. ID 연동 페이지로 이동합니다.
2. **ID** 페더레이션 활성화 확인란의 선택을 해제합니다.

OpenLDAP 서버 구성 지침

ID 페더레이션을 위해 OpenLDAP 서버를 사용하려면 OpenLDAP 서버에서 특정 설정을 구성해야 합니다.

> Active Directory 또는 Microsoft Entra ID가 아닌 ID 소스의 경우, StorageGRID는 외부에서 사용이 중지된 사용자의 S3 액세스를 자동으로 차단하지 않습니다. S3 액세스를 차단하려면 해당 사용자의 S3 키를 삭제하거나 모든 그룹에서 해당 사용자를 제거하십시오.

Memberof 및 **refint** 오버레이

memberof 및 refint 오버레이를 활성화해야 합니다. 자세한 내용은 "OpenLDAP 문서: 버전 2.4 관리자 가이드"의 역방향 그룹 멤버십 유지 관리 지침을 참조하십시오.

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 이름에 대한 도움말에 언급된 필드가 색인화되었는지 확인하십시오.

역방향 그룹 멤버십 유지 관리에 대한 정보는 "OpenLDAP 문서: 버전 2.4 관리자 가이드"을 참조하십시오.

StorageGRID에서 관리자 그룹 관리

관리자 그룹을 생성하여 하나 이상의 관리자 사용자에 대한 보안 권한을 관리할 수 있습니다. 사용자는 StorageGRID 시스템에 액세스하려면 반드시 그룹에 속해야 합니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.
- 연합 그룹을 가져오려면 ID 연합이 구성되어 있어야 하며, 구성된 ID 소스에 연합 그룹이 이미 존재해야 합니다.

관리자 그룹 생성

관리자 그룹을 사용하면 그리드 관리자 및 그리드 관리 API에서 어떤 사용자가 어떤 기능과 작업에 액세스할 수 있는지 결정할 수 있습니다.

마법사에 액세스합니다

단계

1. * 구성 * > * 액세스 제어 * > * 관리자 그룹 * 을 선택합니다.
2. *그룹 생성*을 선택합니다.

그룹 유형을 선택합니다

로컬 그룹을 생성하거나 연합 그룹을 가져올 수 있습니다.

- 로컬 사용자에게 권한을 할당하려면 로컬 그룹을 생성합니다.
- ID 소스에서 사용자를 가져오기 위해 페더레이션 그룹을 생성합니다.

로컬 그룹

단계

1. *로컬 그룹*을 선택합니다.
2. 그룹에 표시할 이름을 입력하세요. 필요에 따라 나중에 수정할 수 있습니다. 예를 들어 "유지 관리 사용자" 또는 "ILM 관리자"와 같이 입력할 수 있습니다.
3. 그룹에 고유한 이름을 입력하세요. 이 이름은 나중에 수정할 수 없습니다.
4. *Continue*를 선택합니다.

연합 그룹

단계

1. *연합 그룹*을 선택합니다.
2. 구성된 ID 소스에 표시된 대로 가져올 그룹 이름을 정확하게 입력하십시오.
   - Active Directory 및 Microsoft Entra ID의 경우 sAMAccountName을 사용하십시오.
   - OpenLDAP의 경우 CN(Common Name)을 사용하십시오.
   - 다른 LDAP의 경우, LDAP 서버에 적합한 고유 이름을 사용하십시오.
3. *Continue*를 선택합니다.

그룹 권한 관리

단계

1. *액세스 모드*에서 그룹 내 사용자가 그리드 관리자 및 그리드 관리 API에서 설정을 변경하고 작업을 수행할 수 있는지, 아니면 설정 및 기능만 볼 수 있는지를 선택합니다.
   - 읽기-쓰기 (기본값): 사용자는 관리자 권한에 따라 설정을 변경하고 허용된 작업을 수행할 수 있습니다.
   - 읽기 전용: 사용자는 설정 및 기능만 볼 수 있습니다. 그리드 관리자 또는 그리드 관리 API에서 변경하거나 작업을 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 비밀번호를 변경할 수 있습니다.

사용자가 여러 그룹에 속해 있고 어떤 그룹이라도 *읽기 전용*으로 설정되어 있는 경우, 해당 사용자는 선택된 모든 설정 및 기능에 대해 읽기 전용 액세스 권한만 갖게 됩니다.

2. 하나 이상의 "관리자 그룹 권한"을(를) 선택하세요.

   각 그룹에는 최소 하나 이상의 권한을 할당해야 합니다. 그렇지 않으면 해당 그룹에 속한 사용자가 StorageGRID에 로그인할 수 없습니다.

3. 로컬 그룹을 생성하는 경우 *계속*을 선택하십시오. 연합 그룹을 생성하는 경우 *그룹 생성*을 선택한 다음 *완료*를 선택하십시오.

사용자 추가 (로컬 그룹만 해당)

단계

1. 선택적으로, 이 그룹에 대해 한 명 이상의 로컬 사용자를 선택할 수 있습니다.

   아직 로컬 사용자를 생성하지 않았다면 사용자를 추가하지 않고 그룹을 저장할 수 있습니다. 사용자 페이지에서 해당 그룹을 사용자에게 추가할 수 있습니다. 자세한 내용은 "사용자 관리"을 참조하십시오.

2. 그룹 만들기 및 *완료*를 선택합니다.

관리자 그룹 보기 및 편집

기존 그룹의 세부 정보를 보거나, 그룹을 수정하거나, 그룹을 복제할 수 있습니다.

- 모든 그룹의 기본 정보를 보려면 그룹 페이지의 표를 참조하십시오.
- 특정 그룹의 모든 세부 정보를 보거나 그룹을 편집하려면 작업 메뉴 또는 세부 정보 페이지를 사용하세요.

작업	작업 메뉴	상세 정보 페이지
그룹 세부 정보 보기	a. 해당 그룹의 확인란을 선택합니다. b. 작업 > *그룹 세부 정보 보기*를 선택합니다.	표에서 그룹 이름을 선택합니다.
표시 이름 편집 (로컬 그룹에만 해당)	a. 해당 그룹의 확인란을 선택합니다. b. * 작업 * > * 그룹 이름 편집 * 을 선택합니다. c. 새 이름을 입력합니다. d. *변경 사항 저장*을 선택합니다.	a. 그룹 이름을 선택하면 세부 정보가 표시됩니다. b. 편집 아이콘 을 선택합니다. c. 새 이름을 입력합니다. d. *변경 사항 저장*을 선택합니다.

작업	작업 메뉴	상세 정보 페이지
접근 모드 또는 권한 편집	a. 해당 그룹의 확인란을 선택합니다. b. 작업 > *그룹 세부 정보 보기*를 선택합니다. c. 필요에 따라 그룹의 액세스 모드를 변경할 수 있습니다. d. 필요에 따라 "관리자 그룹 권한"을(를) 선택하거나 선택 해제합니다. e. *변경 사항 저장*을 선택합니다.	a. 그룹 이름을 선택하면 세부 정보가 표시됩니다. b. 필요에 따라 그룹의 액세스 모드를 변경할 수 있습니다. c. 필요에 따라 "관리자 그룹 권한"을(를) 선택하거나 선택 해제합니다. d. *변경 사항 저장*을 선택합니다.

그룹 복제

단계

1. 해당 그룹의 확인란을 선택합니다.
2. 작업 > *그룹 복제*를 선택합니다.
3. 그룹 복제 마법사를 완료합니다.

그룹 삭제

관리자 그룹을 시스템에서 제거하고 그룹과 관련된 모든 권한을 삭제하려면 관리자 그룹을 삭제할 수 있습니다. 관리자 그룹을 삭제하면 그룹에서 모든 사용자가 제거되지만, 사용자 자체는 삭제되지 않습니다.

단계

1. 그룹 페이지에서 제거하려는 각 그룹의 확인란을 선택합니다.
2. * 작업 * > * 그룹 삭제 * 를 선택합니다.
3. *그룹 삭제*를 선택합니다.

StorageGRID의 관리 그룹 권한

관리자 사용자 그룹을 생성할 때, Grid Manager의 특정 기능에 대한 접근 권한을 제어하기 위해 하나 이상의 권한을 선택합니다. 그런 다음 각 사용자를 이러한 관리자 그룹 중 하나 이상에 할당하여 해당 사용자가 수행할 수 있는 작업을 지정할 수 있습니다.

각 그룹에는 최소 하나 이상의 권한을 할당해야 합니다. 그렇지 않으면 해당 그룹에 속한 사용자는 Grid Manager 또는 Grid Management API에 로그인할 수 없습니다.

기본적으로 하나 이상의 권한을 가진 그룹에 속한 사용자는 다음과 같은 작업을 수행할 수 있습니다.

- Grid Manager에 로그인합니다
- 대시보드 보기
- 노드 페이지 보기
- 현재 및 해결된 알림 보기

- 자신의 암호 변경(로컬 사용자만 해당)
- 구성 및 유지 관리 페이지에 제공된 특정 정보 보기

권한과 액세스 모드 간의 상호 작용

모든 권한에 대해 그룹의 액세스 모드 설정은 사용자가 설정을 변경하고 작업을 수행할 수 있는지 또는 관련 설정 및 기능을 보기만 할 수 있는지를 결정합니다. 사용자가 여러 그룹에 속해 있고 어떤 그룹이라도 *읽기 전용*으로 설정되어 있는 경우, 해당 사용자는 선택된 모든 설정 및 기능에 대해 읽기 전용 액세스 권한만 갖게 됩니다.

다음 섹션에서는 관리자 그룹을 생성하거나 편집할 때 할당할 수 있는 권한에 대해 설명합니다. 명시적으로 언급되지 않은 모든 기능은 루트 액세스 권한이 필요합니다.

루트 액세스

이 권한을 통해 모든 그리드 관리 기능에 접근할 수 있습니다.

테넌트 루트 암호 변경

이 권한을 통해 테넌트 페이지의 루트 암호 변경 옵션에 접근할 수 있으며, 테넌트의 로컬 루트 사용자 암호를 변경할 수 있는 사용자를 제어할 수 있습니다. 또한 이 권한은 S3 키 가져오기 기능이 활성화된 경우 S3 키를 마이그레이션하는 데 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 할당해야 합니다.

ILM

이 권한을 통해 다음 **ILM** 메뉴 옵션에 액세스할 수 있습니다.

- 규칙
- 정책
- 정책 태그
- 스토리지 풀
- 스토리지 등급
- 지역
- 객체 메타데이터 조회

> ⓘ 사용자는 스토리지 등급을 관리하려면 기타 그리드 구성 권한이 있어야 합니다.

유지 관리

사용자는 이러한 옵션을 사용하려면 유지 관리 권한이 있어야 합니다.

- 구성 > 접근 제어:
  - 그리드 비밀번호
- 구성 > 네트워크:

    - S3 엔드포인트 도메인 이름
- 유지보수 > 작업:
    - 폐기
    - 확장
    - 객체 존재 여부 확인
    - 복구
- 유지보수 > 시스템:
    - 복구 패키지
    - 소프트웨어 업데이트
- 지원 > 도구:
    - 로그

유지보수 권한이 없는 사용자는 다음 페이지를 볼 수는 있지만 편집할 수는 없습니다.

- 유지보수 > 네트워크:
    - DNS 서버
    - 그리드 네트워크
    - NTP 서버
- 유지보수 > 시스템:
    - 라이센스
- 구성 > 네트워크:
    - S3 엔드포인트 도메인 이름
- 구성 > 보안:
    - 인증서
- 구성 > 모니터링:
    - 감사 및 syslog 서버

알림 관리

이 권한은 알림 관리 옵션에 대한 접근을 제공합니다. 사용자는 알림 비활성화, 알림 알림 내용 및 알림 규칙을 관리하려면 이 권한이 있어야 합니다.

메트릭 쿼리

이 권한을 통해 다음 항목에 접근할 수 있습니다.

- 지원 > 도구 > 측정항목 페이지
- 그리드 관리 API의 **Metrics** 섹션을 사용한 사용자 지정 Prometheus 메트릭 쿼리
- 메트릭을 포함하는 Grid Manager 대시보드 카드

객체 메타데이터 조회

이 권한은 **ILM** > 객체 메타데이터 조회 페이지에 대한 접근 권한을 제공합니다.

다른 그리드 구성

이 권한을 통해 다음과 같은 추가 그리드 구성 옵션에 접근할 수 있습니다.

- **ILM**:
  - 스토리지 등급
- 구성 > 시스템:
- 지원 > 기타:
  - 링크 비용

스토리지 어플라이언스 관리자

이 권한은 다음을 제공합니다:

- Grid Manager를 통해 스토리지 어플라이언스의 E-Series SANtricity System Manager에 액세스할 수 있습니다.
- 이러한 작업을 지원하는 어플라이언스의 경우, 드라이브 관리 탭에서 문제 해결 및 유지 관리 작업을 수행할 수 있습니다.

테넌트 계정

이 권한을 통해 다음과 같은 작업을 수행할 수 있습니다.

- 테넌트 페이지에 접속하면 테넌트 계정을 생성, 편집 및 삭제할 수 있습니다.
- 기존 트래픽 분류 정책 보기
- 테넌트 세부 정보가 포함된 Grid Manager 대시보드 카드 보기

StorageGRID에서 사용자 관리

로컬 사용자와 연합 사용자를 볼 수 있습니다. 또한 로컬 사용자를 생성하고 로컬 관리자 그룹에 할당하여 해당 사용자가 액세스할 수 있는 Grid Manager 기능을 지정할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.

로컬 사용자 생성

로컬 사용자를 한 명 이상 생성하고 각 사용자를 하나 이상의 로컬 그룹에 할당할 수 있습니다. 그룹 권한은 사용자가 액세스할 수 있는 Grid Manager 및 Grid Management API 기능을 제어합니다.

로컬 사용자만 생성할 수 있습니다. 연합 사용자 및 그룹 관리는 외부 ID 소스를 이용하십시오.

그리드 관리자에는 "root"라는 이름의 미리 정의된 로컬 사용자가 하나 포함되어 있습니다. 루트 사용자는 제거할 수

없습니다.

싱글 사인온(SSO)이 활성화된 경우 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

마법사에 액세스합니다

단계

1. 구성 > 액세스 제어 > *관리자 사용자*를 선택하십시오.
2. *사용자 생성*을 선택합니다.

사용자 자격 증명을 입력하십시오.

단계

1. 사용자의 전체 이름, 고유한 사용자 이름 및 비밀번호를 입력하십시오.
2. 선택적으로, 이 사용자가 Grid Manager 또는 Grid Management API에 액세스해서는 안 되는 경우 *예*를 선택하십시오.
3. *Continue*를 선택합니다.

그룹에 할당

단계

1. 선택적으로 사용자를 하나 이상의 그룹에 할당하여 사용자의 권한을 결정할 수 있습니다.

   아직 그룹을 생성하지 않았다면 그룹을 선택하지 않고 사용자를 저장할 수 있습니다. 그룹 페이지에서 이 사용자를 그룹에 추가할 수 있습니다.

   사용자가 여러 그룹에 속해 있는 경우 권한은 누적됩니다. 자세한 내용은 "관리자 그룹 관리"을 참조하십시오.

2. *사용자 생성*을 선택하고 *완료*를 선택합니다.

로컬 사용자 보기 및 편집

기존 로컬 사용자 및 연합 사용자의 세부 정보를 볼 수 있습니다. 로컬 사용자의 전체 이름, 비밀번호 또는 그룹 멤버십을 변경하여 사용자를 수정할 수 있습니다. 또한 사용자가 Grid Manager 및 Grid Management API에 액세스하지 못하도록 일시적으로 차단할 수도 있습니다.

로컬 사용자만 편집할 수 있습니다. 페더레이션된 사용자는 외부 ID 소스를 사용하여 관리하십시오.

- 모든 로컬 및 페더레이션 사용자에 대한 기본 정보를 보려면 사용자 페이지의 표를 참조하십시오.
- 특정 사용자의 모든 세부 정보를 보거나, 로컬 사용자를 편집하거나, 로컬 사용자의 암호를 변경하려면 작업 메뉴 또는 세부 정보 페이지를 사용하십시오.

  모든 수정 사항은 사용자가 로그아웃한 후 그리드 관리자에 다시 로그인할 때 적용됩니다.

  로컬 사용자는 Grid Manager 배너의 비밀번호 변경 옵션을 사용하여 자신의 비밀번호를 변경할 수 있습니다.

작업	작업 메뉴	상세 정보 페이지
사용자 세부 정보 보기	a. 사용자의 확인란을 선택합니다. b. 작업 > *사용자 세부 정보 보기*를 선택합니다.	표에서 사용자 이름을 선택합니다.
전체 이름 수정 (로컬 사용자만 해당)	a. 사용자의 확인란을 선택합니다. b. 작업 > *전체 이름 편집*을 선택합니다. c. 새 이름을 입력합니다. d. *변경 사항 저장*을 선택합니다.	a. 사용자의 이름을 선택하여 세부 정보를 표시합니다. b. 편집 아이콘 을 선택합니다. c. 새 이름을 입력합니다. d. *변경 사항 저장*을 선택합니다.
StorageGRID 액세스 거부 또는 허용	a. 사용자의 확인란을 선택합니다. b. 작업 > *사용자 세부 정보 보기*를 선택합니다. c. 액세스 탭을 선택합니다. d. 사용자가 그리드 관리자 또는 그리드 관리 API에 로그인하지 못하도록 하려면 *예*를 선택하고, 로그인을 허용하려면 *아니요*를 선택하십시오. e. *변경 사항 저장*을 선택합니다.	a. 사용자의 이름을 선택하여 세부 정보를 표시합니다. b. 액세스 탭을 선택합니다. c. 사용자가 그리드 관리자 또는 그리드 관리 API에 로그인하지 못하도록 하려면 *예*를 선택하고, 로그인을 허용하려면 *아니요*를 선택하십시오. d. *변경 사항 저장*을 선택합니다.
비밀번호 변경 (로컬 사용자만 해당)	a. 사용자의 확인란을 선택합니다. b. 작업 > *사용자 세부 정보 보기*를 선택합니다. c. 비밀번호 탭을 선택합니다. d. 새 비밀번호를 입력하세요. e. *비밀번호 변경*을 선택합니다.	a. 사용자의 이름을 선택하여 세부 정보를 표시합니다. b. 비밀번호 탭을 선택합니다. c. 새 비밀번호를 입력하세요. d. *비밀번호 변경*을 선택합니다.
그룹 변경 (로컬 사용자만 해당)	a. 사용자의 확인란을 선택합니다. b. 작업 > *사용자 세부 정보 보기*를 선택합니다. c. 그룹 탭을 선택합니다. d. 선택적으로 그룹 이름 뒤의 링크를 클릭하여 새 브라우저 탭에서 그룹 세부 정보를 볼 수 있습니다. e. 다른 그룹을 선택하려면 *그룹 편집*을 선택합니다. f. *변경 사항 저장*을 선택합니다.	a. 사용자의 이름을 선택하여 세부 정보를 표시합니다. b. 그룹 탭을 선택합니다. c. 선택적으로 그룹 이름 뒤의 링크를 클릭하여 새 브라우저 탭에서 그룹 세부 정보를 볼 수 있습니다. d. 다른 그룹을 선택하려면 *그룹 편집*을 선택합니다. e. *변경 사항 저장*을 선택합니다.

연합 사용자 가져오기

최대 100명까지 연합 사용자를 하나 이상 사용자 페이지로 직접 가져올 수 있습니다.

단계

1. 구성 > 액세스 제어 > *관리자 사용자*를 선택하십시오.
2. *연합 사용자 가져오기*를 선택합니다.
3. 연합 사용자 한 명 이상의 UUID 또는 사용자 이름을 입력하십시오.

   여러 항목을 입력하려면 각 UUID 또는 사용자 이름을 새 줄에 추가하십시오.

4. *가져오기*를 선택합니다.

   사용자 필드로의 가져오기가 한 명 이상의 사용자에 대해 실패하는 경우 다음 단계를 수행하십시오.

   a. *가져오지 않은 사용자*를 확장하고 *사용자 복사*를 선택합니다.
   b. 이전*을 선택하고 복사한 사용자를 *연합 사용자 가져오기 대화 상자에 붙여넣어 가져오기를 다시 시도하십시오.

   연합 사용자 가져오기 대화 상자를 닫으면 성공적으로 가져온 사용자에 대한 연합 사용자 정보가 사용자 페이지에 표시됩니다.

사용자 복제

기존 사용자를 복제하여 동일한 권한을 가진 새 사용자를 만들 수 있습니다.

단계

1. 사용자의 확인란을 선택합니다.
2. 작업 > *사용자 복제*를 선택합니다.
3. 사용자 복제 마법사를 완료합니다.

사용자 삭제

로컬 사용자를 삭제하면 해당 사용자가 시스템에서 영구적으로 제거됩니다.

ⓘ 루트 사용자는 삭제할 수 없습니다.

단계

1. 사용자 페이지에서 삭제하려는 각 사용자의 확인란을 선택합니다.
2. 작업 > *사용자 삭제*를 선택합니다.
3. *사용자 삭제*를 선택합니다.

싱글 사인온(SSO) 사용

StorageGRID SSO에 대해 알아보십시오

싱글 사인온(SSO)이 활성화된 경우, 사용자는 조직에서 구현한 SSO 로그인 프로세스를 통해 자격 증명이 인증된 경우에만 Grid Manager, Tenant Manager, Grid Management API 또는 Tenant Management API에 액세스할 수 있습니다. 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

StorageGRID 시스템은 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용한 단일 로그인(SSO)을 지원합니다.

SSO(Single Sign-On)를 활성화하기 전에 SSO가 활성화될 때 StorageGRID 로그인 및 로그아웃 프로세스에 어떤 영향을 미치는지 검토하십시오.

SSO가 활성화된 경우 로그인

SSO가 활성화된 상태에서 StorageGRID에 로그인하면 자격 증명을 확인하기 위해 조직의 SSO 페이지로 리디렉션됩니다.

단계

1. 웹 브라우저에 StorageGRID 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력하십시오.

   StorageGRID 로그인 페이지가 나타납니다.

   - 이 브라우저에서 해당 URL에 처음 접속하는 경우 계정 ID를 입력하라는 메시지가 표시됩니다.
   - 이전에 그리드 관리자 또는 테넌트 관리자에 접속한 적이 있는 경우, 최근 계정을 선택하거나 계정 ID를 입력하라는 메시지가 표시됩니다.

   > StorageGRID 테넌트 계정의 전체 URL(즉, 정규화된 도메인 이름 또는 IP 주소 뒤에 `/?accountId=20-digit-account-id`)을 입력하면 StorageGRID 로그인 페이지가 표시되지 않습니다. 대신 조직의 SSO 로그인 페이지로 바로 리디렉션되며, 여기서 SSO 자격 증명으로 로그인하십시오할 수 있습니다.

2. Grid Manager 또는 테넌트 관리자 중 어느 쪽에 액세스할지 표시합니다.
   - 그리드 관리자에 액세스하려면 계정 **ID** 필드를 비워 두거나 계정 ID로 *0*을 입력하거나 최근 계정 목록에 *그리드 관리자*가 표시되면 해당 항목을 선택하십시오.
   - 테넌트 관리자에 액세스하려면 20자리 테넌트 계정 ID를 입력하거나 최근 계정 목록에 테넌트가 표시되는 경우 이름으로 테넌트를 선택하십시오.
3. *로그인*을 선택합니다

   StorageGRID가 조직의 SSO 로그인 페이지로 리디렉션합니다. 예를 들면 다음과 같습니다.

4. SSO 자격 증명으로 로그인하십시오.

   SSO 자격 증명이 올바른 경우:

   a. ID 공급자(IdP)는 StorageGRID에 인증 응답을 제공합니다.
   b. StorageGRID가 인증 응답을 검증합니다.
   c. 응답이 유효하고 StorageGRID 액세스 권한이 있는 연합 그룹에 속해 있는 경우, 선택한 계정에 따라 Grid

Manager 또는 Tenant Manager에 로그인됩니다.

> 서비스 계정에 액세스할 수 없는 경우에도 StorageGRID 액세스 권한이 있는 페더레이션 그룹에 속한 기존 사용자라면 로그인할 수 있습니다.

5. 적절한 권한이 있는 경우, 다른 관리 노드에 액세스하거나 Grid Manager 또는 Tenant Manager에 액세스할 수 있습니다.

   SSO 자격 증명을 다시 입력할 필요가 없습니다.

SSO가 활성화된 경우 로그아웃

StorageGRID에 SSO가 활성화된 경우, 로그아웃 시 발생하는 상황은 현재 로그인 상태와 로그아웃 위치에 따라 다릅니다.

단계

1. 사용자 인터페이스의 오른쪽 상단 모서리에서 로그아웃 링크를 찾습니다.
2. *로그아웃*을 선택합니다.

   StorageGRID 로그인 페이지가 나타납니다. 최근 계정 드롭다운이 업데이트되어 **Grid Manager** 또는 테넌트의 이름이 포함되므로 향후 이러한 사용자 인터페이스에 더 빠르게 액세스할 수 있습니다.

> 이 표는 단일 브라우저 세션을 사용하는 경우 로그아웃 시 발생하는 상황을 요약한 것입니다. 여러 브라우저 세션에서 StorageGRID에 로그인한 경우, 모든 브라우저 세션에서 개별적으로 로그아웃해야 합니다.

로그인되어 있는 경우...	그리고 로그아웃합니다...	로그아웃되었습니다...
하나 이상의 관리 노드에 있는 Grid Manager	모든 관리 노드의 Grid Manager	모든 관리 노드의 Grid Manager 참고: Entra ID를 SSO에 사용하는 경우 모든 관리자 노드에서 로그아웃하는 데 몇 분 정도 소요될 수 있습니다.
하나 이상의 관리 노드에 있는 테넌트 관리자	모든 관리 노드의 테넌트 관리자	모든 관리 노드의 테넌트 관리자
Grid Manager 및 Tenant Manager 모두	Grid Manager	그리드 관리자만 해당됩니다. SSO에서 로그아웃하려면 테넌트 관리자에서도 로그아웃해야 합니다.

StorageGRID SSO에 대한 요구 사항 및 고려 사항

StorageGRID 시스템에 대한 단일 로그인(SSO)을 활성화하기 전에 요구 사항 및 고려 사항을 검토하십시오.

ID 공급자 요구 사항

StorageGRID는 다음과 같은 SSO ID 공급자(IdP)를 지원합니다.

- Active Directory Federation Service(AD FS)
- Microsoft Entra ID
- PingFederate

SSO ID 공급자를 구성하기 전에 StorageGRID 시스템에 대한 ID 페더레이션을 구성해야 합니다. ID 페더레이션에 사용하는 LDAP 서비스 유형에 따라 구현할 수 있는 SSO 유형이 결정됩니다.

구성된 **LDAP** 서비스 유형	**SSO ID** 공급자 옵션
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

AD FS 요구사항

다음 AD FS 버전 중 하나를 사용할 수 있습니다.

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

Windows Server 2016은 "KB3201845 업데이트" 또는 그 이상의 버전을 사용해야 합니다.

추가 요구 사항

- 전송 계층 보안(TLS) 1.2 또는 1.3
- Microsoft .NET Framework, version 3.5.1 이상

Entra ID 관련 고려 사항

Entra ID를 SSO 유형으로 사용하고 사용자의 사용자 주체 이름이 sAMAccountName을 접두사로 사용하지 않는 경우, StorageGRID가 LDAP 서버와의 연결을 끊으면 로그인 문제가 발생할 수 있습니다. 사용자가 로그인할 수 있도록 하려면 LDAP 서버에 대한 연결을 복원해야 합니다.

서버 인증서 요구 사항

기본적으로 StorageGRID는 각 관리 노드에서 관리 인터페이스 인증서를 사용하여 Grid Manager, Tenant Manager, Grid Management API 및 Tenant Management API에 대한 액세스를 보호합니다. StorageGRID에 대한 신뢰 당사자 트러스트(AD FS), 엔터프라이즈 애플리케이션(Entra ID) 또는 서비스 공급자 연결(PingFederate)을 구성할 때 서버 인증서를 StorageGRID 요청에 대한 서명 인증서로 사용합니다.

아직 설치하지 않으셨다면 "관리 인터페이스에 대한 사용자 지정 인증서를 구성했습니다", 지금 바로 설치하십시오.

사용자 지정 서버 인증서를 설치하면 모든 관리 노드에서 사용되며, 모든 StorageGRID 신뢰 당사자 트러스트, 엔터프라이즈 애플리케이션 또는 SP 연결에서 사용할 수 있습니다.

> 관리 노드의 기본 서버 인증서를 신뢰 당사자 트러스트, 엔터프라이즈 애플리케이션 또는 SP 연결에 사용하는 것은 권장되지 않습니다. 노드에 장애가 발생하여 복구하는 경우 새 기본 서버 인증서가 생성됩니다. 복구된 노드에 로그인하려면 먼저 신뢰 당사자 트러스트, 엔터프라이즈 애플리케이션 또는 SP 연결을 새 인증서로 업데이트해야 합니다.

관리자 노드의 서버 인증서는 해당 노드의 명령 셸에 로그인한 다음 `/var/local/mgmt-api` 디렉터리로 이동하면 확인할 수 있습니다. 사용자 지정 서버 인증서의 이름은 `custom-server.crt`입니다. 노드의 기본 서버 인증서의 이름은 `server.crt`입니다.

포트 요구 사항

제한된 Grid Manager 또는 Tenant Manager 포트에서는 싱글 사인온(SSO)을 사용할 수 없습니다. 사용자가 싱글 사인온으로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다. "외부 방화벽에서 액세스 제어"을 참조하십시오.

연합 사용자가 **StorageGRID**에 로그인할 수 있는지 확인합니다

싱글 사인온(SSO)을 활성화하기 전에, 최소 한 명의 페더레이션 사용자가 기존 테넌트 계정에 대해 Grid Manager와 Tenant Manager에 로그인할 수 있는지 확인해야 합니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.
- 이미 ID 페더레이션을 구성했습니다.

단계

1. 기존 테넌트 계정이 있는 경우, 어떤 테넌트도 자체 ID 소스를 사용하고 있지 않은지 확인하십시오.

   > SSO를 활성화하면 테넌트 관리자에 구성된 ID 소스가 그리드 관리자에 구성된 ID 소스로 재정의됩니다. 테넌트의 ID 소스에 속한 사용자는 그리드 관리자 ID 소스에 계정이 없는 경우 더 이상 로그인할 수 없습니다.

   a. 각 테넌트 계정에 대해 Tenant Manager에 로그인하십시오.
   b. 액세스 관리 > *ID 페더레이션*을 선택합니다.
   c. **ID** 페더레이션 사용 확인란이 선택되어 있지 않은지 확인하십시오.
   d. 그렇다면 이 테넌트 계정에 사용 중인 페더레이션 그룹이 더 이상 필요하지 않은지 확인하고 확인란을 선택 해제한 다음 *저장*을 선택하십시오.

2. 페더레이션 사용자가 Grid Manager에 액세스할 수 있는지 확인합니다.
   a. 그리드 관리자에서 구성 > 액세스 제어 > *관리자 그룹*을 선택합니다.
   b. Active Directory ID 소스에서 하나 이상의 페더레이션 그룹을 가져왔고 해당 그룹에 루트 액세스 권한이 할당되었는지 확인하십시오.
   c. 로그아웃합니다.

d. 연합 그룹의 사용자로 그리드 관리자에 다시 로그인할 수 있는지 확인하십시오.

3. 기존 테넌트 계정이 있는 경우, 루트 액세스 권한이 있는 페더레이션 사용자가 로그인할 수 있는지 확인하십시오.
   a. 그리드 관리자에서 *테넌트*를 선택합니다.
   b. 테넌트 계정을 선택하고 작업 > *편집*을 선택합니다.
   c. 세부 정보 입력 탭에서 *계속*을 선택합니다.
   d. 자체 **ID** 소스 사용 확인란이 선택되어 있으면 선택을 해제하고 *저장*을 선택하십시오.

      테넌트 페이지가 나타납니다.

   e. 테넌트 계정을 선택하고 *로그인*을 선택한 다음 로컬 루트 사용자로 테넌트 계정에 로그인합니다.
   f. 테넌트 관리자에서 액세스 관리 > *그룹*을 선택합니다.
   g. 그리드 관리자의 페더레이션 그룹 중 하나 이상에 이 테넌트에 대한 루트 액세스 권한이 할당되어 있는지 확인합니다.
   h. 로그아웃합니다.
   i. 테넌트 연합 그룹의 사용자로 테넌트에 다시 로그인할 수 있는지 확인하십시오.

관련 정보

- "싱글 사인온(SSO)을 위한 요구 사항 및 고려 사항"
- "관리자 그룹 관리"
- "테넌트 계정 사용"

StorageGRID에서 **SSO** 구성

SSO 구성 마법사를 따라 샌드박스 모드로 들어가면 모든 StorageGRID 사용자에게 SSO를 활성화하기 전에 SSO를 구성하고 테스트할 수 있습니다. SSO가 활성화된 후에는 필요에 따라 샌드박스 모드로 돌아가 구성을 변경하거나 다시 테스트할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"
- StorageGRID 시스템에 대한 ID 페더레이션을 구성했습니다.
- ID 페더레이션 *LDAP 서비스 유형*의 경우, 사용하려는 SSO ID 공급자에 따라 Active Directory 또는 Entra ID를 선택했습니다.

구성된 **LDAP** 서비스 유형	**SSO ID** 공급자 옵션
Active Directory Federation Service(AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

이 작업 정보

SSO가 활성화된 상태에서 사용자가 관리자 노드에 로그인하려고 하면 StorageGRID는 SSO ID 공급자에게 인증 요청을 보냅니다. 그러면 SSO ID 공급자는 인증 요청의 성공 여부를 나타내는 인증 응답을 StorageGRID로 다시 보냅니다. 요청이 성공한 경우:

- Active Directory 또는 PingFederate의 응답에는 사용자에 대한 범용 고유 식별자(UUID)가 포함됩니다.
- Entra ID의 응답에는 사용자 주체 이름(UPN)이 포함됩니다.

StorageGRID(서비스 제공업체)와 SSO ID 제공업체가 사용자 인증 요청에 대해 안전하게 통신할 수 있도록 하려면 다음 작업을 완료해야 합니다.

1. StorageGRID에서 설정을 구성합니다.
2. SSO ID 공급자 소프트웨어를 사용하여 각 관리 노드에 대한 신뢰 당사자 트러스트(AD FS), 엔터프라이즈 애플리케이션(Entra ID) 또는 서비스 공급자(PingFederate)를 생성합니다.
3. StorageGRID로 돌아가서 SSO를 활성화합니다.

샌드박스 모드를 사용하면 이러한 설정 변경 과정을 간편하게 수행하고 SSO를 활성화하기 전에 모든 설정을 테스트할 수 있습니다. 샌드박스 모드에서는 사용자가 SSO를 사용하여 로그인할 수 없습니다.

마법사에 액세스합니다

단계

1. * 구성 * > * 액세스 제어 * > * 싱글 사인온 * 을 선택합니다. 싱글 사인온 페이지가 나타납니다.

   SSO 설정 구성 버튼이 비활성화된 경우, ID 공급자를 페더레이션 ID 소스로 구성했는지 확인하십시오. 을(를) 참조하십시오."싱글 사인온(SSO)을 위한 요구 사항 및 고려 사항"

2. *SSO 설정 구성*을 선택합니다. ID 공급자 세부 정보 제공 페이지가 나타납니다.

ID 공급자 세부 정보 제공

단계

1. 드롭다운 목록에서 *SSO 유형*을 선택합니다.
2. SSO 유형으로 Active Directory를 선택한 경우, Active Directory Federation Service(AD FS)에 표시된 대로 ID 공급자의 *페더레이션 서비스 이름*을 정확하게 입력하십시오.

   페더레이션 서비스 이름을 찾으려면 Windows Server Manager로 이동합니다. 도구 > *AD FS 관리*를 선택합니다. 작업 메뉴에서 *페더레이션 서비스 속성 편집*을 선택합니다. 페더레이션 서비스 이름은 두 번째 필드에 표시됩니다.

3. ID 공급자가 StorageGRID 요청에 대한 응답으로 SSO 구성 정보를 전송할 때 연결을 보호하는 데 사용할 TLS 인증서를 지정합니다.
   - 운영체제 **CA** 인증서 사용: 운영체제에 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 붙여넣으세요.

◦ **TLS**를 사용하지 마십시오: 연결 보안을 위해 TLS 인증서를 사용하지 마십시오.

> CA 인증서를 변경한 경우 즉시 "관리 노드에서 mgmt-api 서비스를 재시작하십시오." Grid Manager에 대한 SSO가 성공적으로 작동하는지 테스트하십시오.

4. *계속*을 선택합니다. 신뢰 당사자 식별자 제공 페이지가 나타납니다.

신뢰 당사자 식별자 제공

1. 선택한 SSO 유형에 따라 '신뢰 당사자 식별자 제공' 페이지의 필드를 작성하십시오.

Active Directory

a. StorageGRID의 *Relying party identifier*를 지정합니다. 이 값은 AD FS에서 각 신뢰 당사자 트러스트에 사용할 이름을 제어합니다.

   - 예를 들어, 그리드에 관리 노드가 하나만 있고 향후 관리 노드를 추가할 계획이 없다면 `SG` 또는 `StorageGRID`를 입력하십시오.
   - 그리드에 관리자 노드가 두 개 이상 포함된 경우 식별자에 문자열 `[HOSTNAME]`을 포함하세요. 예를 들어, `SG-[HOSTNAME]`. 이 문자열을 포함하면 노드의 호스트 이름을 기반으로 그리드의 각 관리자 노드에 대한 신뢰 당사자 식별자를 보여주는 테이블이 생성됩니다.

   > StorageGRID 시스템의 각 관리 노드에 대해 신뢰 당사자 트러스트를 생성해야 합니다. 각 관리 노드에 대한 신뢰 당사자 트러스트를 설정하면 사용자가 모든 관리 노드에 안전하게 로그인하고 로그아웃할 수 있습니다.

b. *저장 후 샌드박스 모드로 진입*을 선택합니다.

Entra ID

a. 엔터프라이즈 애플리케이션 섹션에서 StorageGRID의 *엔터프라이즈 애플리케이션 이름*을 지정합니다. 이 값은 Entra ID의 각 엔터프라이즈 애플리케이션에 사용할 이름을 제어합니다.

   - 예를 들어, 그리드에 관리 노드가 하나만 있고 향후 관리 노드를 추가할 계획이 없다면 `SG` 또는 `StorageGRID`를 입력하십시오.
   - 그리드에 관리 노드가 두 개 이상 포함된 경우 식별자에 `[HOSTNAME]` 문자열을 포함하십시오. 예를 들어, `SG-[HOSTNAME]`. 이 문자열을 포함하면 노드의 호스트 이름을 기반으로 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션 이름이 표시되는 표가 생성됩니다.

   > StorageGRID 시스템의 각 관리 노드마다 엔터프라이즈 애플리케이션을 생성해야 합니다. 각 관리 노드에 엔터프라이즈 애플리케이션을 설치하면 사용자가 모든 관리 노드에 안전하게 로그인하고 로그아웃할 수 있습니다.

b. "Entra ID에서 엔터프라이즈 애플리케이션 생성"의 단계에 따라 표에 나열된 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 생성하십시오.

c. Entra ID에서 각 엔터프라이즈 애플리케이션의 페더레이션 메타데이터 URL을 복사합니다. 그런 다음 이 URL을 StorageGRID의 해당 페더레이션 메타데이터 **URL** 필드에 붙여넣습니다.

d. 모든 관리 노드에 대한 페더레이션 메타데이터 URL을 복사하여 붙여넣은 후 *저장하고 샌드박스 모드로 진입*을 선택하십시오.

PingFederate

a. 서비스 제공업체(SP) 섹션에서 StorageGRID의 *SP 연결 ID*를 지정합니다. 이 값은 PingFederate에서 각 SP 연결에 사용하는 이름을 제어합니다.

   - 예를 들어, 그리드에 관리 노드가 하나만 있고 향후 관리 노드를 추가할 계획이 없다면 `SG` 또는 `StorageGRID`를 입력하십시오.
   - 그리드에 관리 노드가 두 개 이상 포함된 경우 식별자에 `[HOSTNAME]` 문자열을 포함하십시오. 예를 들어, `SG-[HOSTNAME]`. 이 문자열을 포함하면 노드의 호스트 이름을 기반으로 시스템의 각 관리 노드에 대한 SP 연결 ID를 보여주는 표가 생성됩니다.

StorageGRID 시스템의 각 관리 노드에 대해 SP 연결을 생성해야 합니다. 각 관리 노드에 SP 연결이 있으면 사용자가 모든 관리 노드에 안전하게 로그인하고 로그아웃할 수 있습니다.

b. 연합 메타데이터 **URL** 필드에 각 관리 노드에 대한 연합 메타데이터 URL을 지정하십시오.

   다음 형식을 사용하십시오.

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
Connection ID>
```

c. *저장 후 샌드박스 모드로 진입*을 선택합니다.

신뢰 당사자 트러스트, 엔터프라이즈 애플리케이션 또는 **SP** 연결 구성

구성을 저장하고 샌드박스 모드로 전환하면 선택한 SSO 유형에 대한 구성을 완료하고 테스트할 수 있습니다.

StorageGRID는 필요한 기간 동안 샌드박스 모드를 유지할 수 있습니다. 단, 페더레이션 사용자 및 로컬 사용자만 로그인할 수 있습니다.

Active Directory

단계

1. Active Directory Federation Services(AD FS)로 이동합니다.
2. StorageGRID SSO 구성 페이지의 표에 표시된 각 신뢰 당사자 식별자를 사용하여 StorageGRID에 대한 하나 이상의 신뢰 당사자 트러스트를 생성합니다.

   표에 표시된 각 관리자 노드에 대해 하나의 트러스트를 생성해야 합니다.

   자세한 안내는 "AD FS에서 신뢰 당사자 트러스트 생성"을 참조하십시오.

Entra ID

단계

1. 현재 로그인한 관리자 노드의 싱글 사인온 페이지에서 SAML 메타데이터를 다운로드하고 저장하는 버튼을 선택합니다.
2. 그런 다음 그리드에 있는 다른 모든 관리 노드에 대해 이 단계를 반복하십시오.
   a. 노드에 로그인합니다.
   b. * 구성 * > * 액세스 제어 * > * 싱글 사인온 * 을 선택합니다.
   c. 해당 노드의 SAML 메타데이터를 다운로드하여 저장하십시오.
3. Azure 포털로 이동합니다.
4. "Entra ID에서 엔터프라이즈 애플리케이션 생성"의 단계에 따라 각 관리 노드에 대한 SAML 메타데이터 파일을 해당 Entra ID 엔터프라이즈 애플리케이션에 업로드합니다.

PingFederate

단계

1. 현재 로그인한 관리자 노드의 싱글 사인온 페이지에서 SAML 메타데이터를 다운로드하고 저장하는 버튼을 선택합니다.
2. 그런 다음 그리드에 있는 다른 모든 관리 노드에 대해 이 단계를 반복하십시오.
   a. 노드에 로그인합니다.
   b. * 구성 * > * 액세스 제어 * > * 싱글 사인온 * 을 선택합니다.
   c. 해당 노드의 SAML 메타데이터를 다운로드하여 저장하십시오.
3. PingFederate로 이동합니다.
4. "StorageGRID에 대한 하나 이상의 서비스 공급자(SP) 연결 생성". 각 관리 노드에 대한 SP 연결 ID(SSO 구성 페이지의 표에 표시됨)와 해당 관리 노드에 대해 다운로드한 SAML 메타데이터를 사용하십시오.

   표에 표시된 각 관리 노드에 대해 SP 연결을 하나씩 생성해야 합니다.

테스트 구성

StorageGRID 시스템 전체에 싱글 사인온(SSO) 사용을 적용하기 전에 각 관리 노드에 대해 싱글 사인온 및 싱글 로그아웃이 올바르게 구성되었는지 확인하십시오.

Active Directory

단계

1. SSO 구성 페이지에서 구성 마법사의 구성 테스트 단계에 있는 링크를 찾습니다.

   URL은 연합 서비스 이름 필드에 입력한 값에서 파생됩니다.

2. 링크를 선택하거나 URL을 복사하여 브라우저에 붙여넣어 ID 제공업체의 로그인 페이지에 접속하십시오.
3. SSO를 사용하여 StorageGRID에 로그인할 수 있는지 확인하려면 *다음 사이트 중 하나에 로그인*을 선택하고 기본 관리 노드에 대한 신뢰 당사자 식별자를 선택한 다음 *로그인*을 선택하십시오.
4. 연동 사용자 이름과 비밀번호를 입력하십시오.
   - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 표시됩니다.
   - SSO 작업이 실패하면 오류 메시지가 표시됩니다. 문제를 해결하려면 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
5. 그리드의 각 관리 노드에 대해 SSO 연결을 확인하려면 이 단계를 반복하십시오.

Entra ID

단계

1. Azure 포털의 싱글 사인온 페이지로 이동합니다.
2. *이 애플리케이션 테스트*를 선택합니다.
3. 연합 사용자 자격 증명을 입력하십시오.
   - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 표시됩니다.
   - SSO 작업이 실패하면 오류 메시지가 표시됩니다. 문제를 해결하려면 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
4. 그리드의 각 관리 노드에 대해 SSO 연결을 확인하려면 이 단계를 반복하십시오.

PingFederate

단계

1. SSO 구성 페이지에서 샌드박스 모드 메시지의 첫 번째 링크를 선택합니다.

   한 번에 하나의 링크만 선택하여 테스트하십시오.

2. 연합 사용자 자격 증명을 입력하십시오.
   - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 표시됩니다.
   - SSO 작업이 실패하면 오류 메시지가 표시됩니다. 문제를 해결하려면 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
3. 그리드에 있는 각 관리 노드의 SSO 연결을 확인하려면 다음 링크를 선택하십시오.

   '페이지 만료' 메시지가 표시되면 브라우저에서 뒤로 버튼을 선택하고 자격 증명을 다시 제출하세요.

싱글 사인온 활성화

각 관리 노드에 SSO를 사용하여 로그인할 수 있음을 확인했으면 전체 StorageGRID 시스템에 대해 SSO를 활성화할

수 있습니다.

SSO가 활성화되면 모든 사용자는 Grid Manager, Tenant Manager, Grid Management API 및 Tenant Management API에 액세스하려면 SSO를 사용해야 합니다. 로컬 사용자는 더 이상 StorageGRID에 액세스할 수 없습니다.

단계

1. SSO 구성 마법사의 테스트 구성 단계에서 *SSO 활성화*를 선택합니다.
2. 경고 메시지를 검토하고 *SSO 활성화*를 선택하십시오.

   싱글 사인온(SSO)이 활성화되었습니다. 싱글 사인온 페이지가 나타나고, 방금 구성한 SSO에 대한 세부 정보가 표시됩니다.

3. 구성을 편집하려면 *편집*을 선택합니다.
4. 싱글 사인온(SSO)을 비활성화하려면 *SSO 비활성화*를 선택합니다.

Azure Portal을 사용하고 Entra ID에 액세스하는 데 사용하는 동일한 컴퓨터에서 StorageGRID에 액세스하는 경우, Azure Portal 사용자가 승인된 StorageGRID 사용자(StorageGRID로 가져온 페더레이션 그룹의 사용자)인지 확인하거나, StorageGRID에 로그인하기 전에 Azure Portal에서 로그아웃하십시오.

AD FS에서 **StorageGRID**에 대한 신뢰 당사자 트러스트 생성

시스템의 각 관리 노드에 대해 Active Directory Federation Services(AD FS)를 사용하여 신뢰 당사자 트러스트를 생성해야 합니다. PowerShell 명령을 사용하거나 StorageGRID에서 SAML 메타데이터를 가져오거나 데이터를 수동으로 입력하여 신뢰 당사자 트러스트를 생성할 수 있습니다.

시작하기 전에

- StorageGRID에 대해 Single Sign-On을 구성했으며 SSO 유형으로 *AD FS*를 선택했습니다.
- Grid Manager에 "샌드박스 모드에 진입했습니다."이(가) 있습니다.
- 시스템에 있는 각 관리 노드의 정규화된 도메인 이름(또는 IP 주소)과 신뢰 당사자 식별자를 알고 있습니다. 이러한 값은 StorageGRID SSO 구성 페이지의 관리 노드 세부 정보 테이블에서 찾을 수 있습니다.

StorageGRID 시스템의 각 관리 노드에 대해 신뢰 당사자 트러스트를 생성해야 합니다. 각 관리 노드에 대한 신뢰 당사자 트러스트를 설정하면 사용자가 모든 관리 노드에 안전하게 로그인하고 로그아웃할 수 있습니다.

- AD FS에서 신뢰 당사자 트러스트를 생성해 본 경험이 있거나 Microsoft AD FS 설명서에 액세스할 수 있어야 합니다.
- 현재 AD FS 관리 스냅인을 사용 중이며 관리자 그룹에 속해 있습니다.
- 신뢰 당사자 트러스트를 수동으로 생성하는 경우 StorageGRID 관리 인터페이스에 업로드된 사용자 지정 인증서가 있거나 명령 셸에서 관리 노드에 로그인하는 방법을 알고 있어야 합니다.

이 작업 정보

이 지침은 Windows Server 2016 AD FS에 적용됩니다. 다른 버전의 AD FS를 사용하는 경우 절차에 약간의 차이가

있을 수 있습니다. 궁금한 점이 있으면 Microsoft AD FS 설명서를 참조하십시오.

Windows PowerShell을 사용하여 신뢰 당사자 트러스트 만들기

Windows PowerShell을 사용하여 하나 이상의 신뢰 당사자 트러스트를 신속하게 생성할 수 있습니다.

단계

1. Windows 시작 메뉴에서 PowerShell 아이콘을 마우스 오른쪽 버튼으로 클릭하고 *관리자 권한으로 실행*을 선택합니다.
2. PowerShell 명령 프롬프트에서 다음 명령을 입력하십시오.

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - `*Admin_Node_Identifier*`의 경우, Single Sign-on 페이지에 표시된 대로 관리자 노드의 신뢰 당사자 식별자(Relying Party Identifier)를 정확히 입력하십시오. 예를 들어, `SG-DC1-ADM1`입니다.
   - `*Admin_Node_FQDN*`에는 동일한 관리 노드의 정규화된 도메인 이름을 입력하십시오. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 단, 여기에 IP 주소를 입력하는 경우 해당 IP 주소가 변경되면 이 신뢰 당사자 트러스트를 업데이트하거나 다시 생성해야 합니다.)
3. Windows 서버 관리자에서 도구 > *AD FS 관리*를 선택합니다.

   AD FS 관리 툴이 나타납니다.
4. **AD FS** > *Relying Party Trusts*를 선택합니다.

   신뢰 당사자 트러스트 목록이 표시됩니다.
5. 새로 생성된 신뢰 당사자 트러스트에 액세스 제어 정책을 추가합니다.
   a. 방금 생성한 신뢰 당사자 트러스트를 찾으십시오.
   b. 트러스트를 마우스 오른쪽 버튼으로 클릭하고 *액세스 제어 정책 편집*을 선택합니다.
   c. 접근 제어 정책을 선택하십시오.
   d. *적용*을 선택하고 *확인*을 선택합니다.
6. 새로 생성된 신뢰 당사자 트러스트에 클레임 발급 정책을 추가합니다.
   a. 방금 생성한 신뢰 당사자 트러스트를 찾으십시오.
   b. 트러스트를 마우스 오른쪽 버튼으로 클릭하고 *클레임 발급 정책 편집*을 선택합니다.
   c. *규칙 추가*를 선택합니다.
   d. 규칙 템플릿 선택 페이지에서 목록에서 *LDAP 속성을 클레임으로 전송*을 선택하고 *다음*을 선택합니다.
   e. 규칙 구성 페이지에서 이 규칙에 대한 표시 이름을 입력합니다.

      예를 들어, **ObjectGUID to Name ID** 또는 **UPN to Name ID**.

   f. 속성 저장소로 *Active Directory*를 선택하십시오.
   g. 매핑 테이블의 LDAP 속성 열에 *objectGUID*를 입력하거나 *User-Principal-Name*을 선택합니다.
   h. 매핑 테이블의 나가는 클레임 유형 열에서 드롭다운 목록에서 *Name ID*를 선택합니다.

i. *마침*을 선택하고 *확인*을 선택합니다.

7. 메타데이터를 성공적으로 가져왔는지 확인하십시오.
   a. 신뢰 당사자 트러스트를 마우스 오른쪽 버튼으로 클릭하여 속성을 엽니다.
   b. 엔드포인트, 식별자, 서명 탭의 모든 필드가 채워져 있는지 확인하십시오.

      메타데이터가 누락된 경우, 페더레이션 메타데이터 주소가 올바른지 확인하거나 값을 수동으로 입력하십시오.

8. StorageGRID 시스템의 모든 관리 노드에 대한 신뢰 당사자 트러스트를 구성하려면 이 단계를 반복하십시오.
9. 완료되면 StorageGRID로 돌아가서 "모든 신뢰 당사자 트러스트를 테스트합니다." 올바르게 구성되었는지 확인하십시오.

페더레이션 메타데이터를 가져와서 신뢰 당사자 트러스트 만들기

각 관리 노드의 SAML 메타데이터에 액세스하여 각 신뢰 당사자 트러스트에 대한 값을 가져올 수 있습니다.

단계

1. Windows 서버 관리자에서 *도구*를 선택한 다음 *AD FS 관리*를 선택합니다.
2. 작업에서 *Add Relying Party Trust*를 선택합니다.
3. 환영 페이지에서 *클레임 인식*을 선택하고 *시작*을 선택합니다.
4. *온라인 또는 로컬 네트워크에 게시된 신뢰 당사자에 대한 데이터 가져오기*를 선택하십시오.
5. *연합 메타데이터 주소(호스트 이름 또는 URL)*에 이 관리 노드의 SAML 메타데이터 위치를 입력합니다.

   `https://Admin_Node_FQDN/api/saml-metadata`

   `_Admin_Node_FQDN_`에는 동일한 관리 노드의 정규화된 도메인 이름을 입력하십시오. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 단, 여기에 IP 주소를 입력하는 경우 해당 IP 주소가 변경되면 이 신뢰 당사자 트러스트를 업데이트하거나 다시 생성해야 합니다.)

6. 신뢰 당사자 트러스트 마법사를 완료하고, 신뢰 당사자 트러스트를 저장한 다음, 마법사를 닫으십시오.

   표시 이름을 입력할 때는 그리드 관리자의 싱글 사인온 페이지에 표시된 관리자 노드의 신뢰 당사자 식별자(Relying Party Identifier)를 그대로 사용하십시오. 예를 들어, `SG-DC1-ADM1`입니다.

7. 클레임 규칙 추가:
   a. 트러스트를 마우스 오른쪽 버튼으로 클릭하고 *클레임 발급 정책 편집*을 선택합니다.
   b. *규칙 추가*를 선택합니다:
   c. 규칙 템플릿 선택 페이지에서 목록에서 *LDAP 속성을 클레임으로 전송*을 선택하고 *다음*을 선택합니다.
   d. 규칙 구성 페이지에서 이 규칙에 대한 표시 이름을 입력합니다.

      예를 들어, **ObjectGUID to Name ID** 또는 **UPN to Name ID**.

   e. 속성 저장소로 *Active Directory*를 선택하십시오.

f. 매핑 테이블의 LDAP 속성 열에 *objectGUID*를 입력하거나 *User-Principal-Name*을 선택합니다.

g. 매핑 테이블의 나가는 클레임 유형 열에서 드롭다운 목록에서 *Name ID*를 선택합니다.

h. *마침*을 선택하고 *확인*을 선택합니다.

8. 메타데이터를 성공적으로 가져왔는지 확인하십시오.

   a. 신뢰 당사자 트러스트를 마우스 오른쪽 버튼으로 클릭하여 속성을 엽니다.

   b. 엔드포인트, 식별자, 서명 탭의 모든 필드가 채워져 있는지 확인하십시오.

      메타데이터가 누락된 경우, 페더레이션 메타데이터 주소가 올바른지 확인하거나 값을 수동으로 입력하십시오.

9. StorageGRID 시스템의 모든 관리 노드에 대한 신뢰 당사자 트러스트를 구성하려면 이 단계를 반복하십시오.

10. 완료되면 StorageGRID로 돌아가서 "모든 신뢰 당사자 트러스트를 테스트합니다." 올바르게 구성되었는지 확인하십시오.

신뢰 당사자 트러스트를 수동으로 생성합니다

신뢰 당사자 신탁에 대한 데이터를 가져오지 않으려면 값을 수동으로 입력할 수 있습니다.

단계

1. Windows 서버 관리자에서 *도구*를 선택한 다음 *AD FS 관리*를 선택합니다.
2. 작업에서 *Add Relying Party Trust*를 선택합니다.
3. 환영 페이지에서 *클레임 인식*을 선택하고 *시작*을 선택합니다.
4. *신뢰 당사자에 대한 데이터를 수동으로 입력하세요*를 선택하고 *다음*을 선택합니다.
5. 신뢰 당사자 트러스트 마법사를 완료합니다.

   a. 이 관리자 노드에 표시할 이름을 입력하십시오.

      일관성을 유지하기 위해 관리자 노드에 대한 신뢰 당사자 식별자(Relying Party Identifier)는 그리드 관리자의 싱글 사인온 페이지에 표시된 것과 정확히 동일하게 사용하십시오. 예를 들어, `SG-DC1-ADM1`.

   b. 선택 사항인 토큰 암호화 인증서 구성 단계를 건너뜁니다.

   c. URL 구성 페이지에서 **SAML 2.0 WebSSO** 프로토콜 지원 활성화 확인란을 선택합니다.

   d. 관리자 노드의 SAML 서비스 엔드포인트 URL을 입력하십시오.

      `https://_Admin_Node_FQDN_/api/saml-response`

      > `_Admin_Node_FQDN_`에는 관리 노드의 정규화된 도메인 이름을 입력하십시오. (필요한 경우 노드의 `IP` 주소를 대신 사용할 수 있습니다. 단, 여기에 `IP` 주소를 입력하는 경우 해당 `IP` 주소가 변경되면 이 신뢰 당사자 트러스트를 업데이트하거나 다시 생성해야 합니다.)

   e. 식별자 구성 페이지에서 동일한 관리 노드에 대한 신뢰 당사자 식별자를 지정합니다.

      Admin_Node_Identifier

`_Admin_Node_Identifier_`의 경우, `Single Sign-on` 페이지에 표시된 대로 관리자 노드의 신뢰 당사자 식별자(`Relying Party Identifier`)를 정확히 입력하십시오. 예를 들어, `SG-DC1-ADM1`입니다.

f. 설정을 검토하고, 신뢰 당사자 트러스트를 저장한 다음 마법사를 닫습니다.

청구 발행 정책 편집 대화 상자가 나타납니다.

대화 상자가 나타나지 않으면 해당 트러스트를 마우스 오른쪽 버튼으로 클릭하고 *클레임 발급 정책 편집*을 선택하십시오.

6. 클레임 규칙 마법사를 시작하려면 *규칙 추가*를 선택합니다.
   a. 규칙 템플릿 선택 페이지에서 목록에서 *LDAP 속성을 클레임으로 전송*을 선택하고 *다음*을 선택합니다.
   b. 규칙 구성 페이지에서 이 규칙에 대한 표시 이름을 입력합니다.

      예를 들어, **ObjectGUID to Name ID** 또는 **UPN to Name ID**.

   c. 속성 저장소로 *Active Directory*를 선택하십시오.
   d. 매핑 테이블의 LDAP 속성 열에 *objectGUID*를 입력하거나 *User-Principal-Name*을 선택합니다.
   e. 매핑 테이블의 나가는 클레임 유형 열에서 드롭다운 목록에서 *Name ID*를 선택합니다.
   f. *마침*을 선택하고 *확인*을 선택합니다.
7. 신뢰 당사자 트러스트를 마우스 오른쪽 버튼으로 클릭하여 속성을 엽니다.
8. 엔드포인트 탭에서 단일 로그아웃(SLO)용 엔드포인트를 구성합니다.
   a. *SAML 추가*를 선택합니다.
   b. 엔드포인트 유형 > *SAML 로그아웃*을 선택합니다.
   c. 바인딩 > *리디렉션*을 선택합니다.
   d. 신뢰할 수 있는 **URL** 필드에 이 관리자 노드에서 단일 로그아웃(SLO)에 사용되는 URL을 입력하십시오.

      `https://Admin_Node_FQDN/api/saml-logout`

   에는 `*Admin_Node_FQDN*`관리 노드의 정규화된 도메인 이름을 입력하십시오. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 단, 여기에 IP 주소를 입력하는 경우 해당 IP 주소가 변경되면 이 신뢰 당사자 트러스트를 업데이트하거나 다시 생성해야 합니다.)

   a. *확인*을 선택합니다.
9. 서명 탭에서 이 신뢰 당사자 트러스트에 사용할 서명 인증서를 지정합니다.
   a. 사용자 지정 인증서를 추가합니다:
      - StorageGRID에 업로드한 사용자 지정 관리 인증서가 있는 경우 해당 인증서를 선택하십시오.
      - 사용자 지정 인증서가 없는 경우 관리자 노드에 로그인하여 `/var/local/mgmt-api` 관리자 노드 디렉터리로 이동한 다음 `custom-server.crt` 인증서 파일을 추가하십시오.

관리자 노드의 기본 인증서 (`server.crt`를 사용하는 것은 권장되지 않습니다. 관리자 노드에 장애가 발생하면 노드를 복구할 때 기본 인증서가 다시 생성되며, 이때 신뢰 당사자 설정을 업데이트해야 합니다.

b. *적용*을 선택하고 *확인*을 선택합니다.

신뢰 당사자 속성이 저장되고 닫힙니다.

10. StorageGRID 시스템의 모든 관리 노드에 대한 신뢰 당사자 트러스트를 구성하려면 이 단계를 반복하십시오.
11. 완료되면 StorageGRID로 돌아가서 "모든 신뢰 당사자 트러스트를 테스트합니다." 올바르게 구성되었는지 확인하십시오.

Entra ID에서 **StorageGRID**용 엔터프라이즈 애플리케이션 생성

Entra ID를 사용하여 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 생성합니다.

시작하기 전에

- StorageGRID에 대한 Single Sign-On 구성을 시작했으며 SSO 유형으로 *Entra ID*를 선택했습니다.
- Grid Manager에 "샌드박스 모드에 진입했습니다."이(가) 있습니다.
- 시스템에는 각 관리 노드에 대한 *엔터프라이즈 애플리케이션 이름*이 있습니다. 이러한 값은 SSO 구성 페이지의 관리 노드 세부 정보 표에서 복사할 수 있습니다.

StorageGRID 시스템의 각 관리 노드마다 엔터프라이즈 애플리케이션을 생성해야 합니다. 각 관리 노드에 엔터프라이즈 애플리케이션을 설치하면 사용자가 모든 관리 노드에 안전하게 로그인하고 로그아웃할 수 있습니다.

- Entra ID를 사용하여 엔터프라이즈 애플리케이션을 개발한 경험이 있으십니다.
- 귀하는 활성 구독이 있는 Entra ID 계정을 보유하고 있습니다.
- Entra ID 계정에는 글로벌 관리자, 클라우드 애플리케이션 관리자, 애플리케이션 관리자 또는 서비스 주체 소유자 중 하나의 역할이 있습니다.

Entra ID 액세스

단계

1. "Azure 포털"에 로그인합니다.
2. 다음으로 이동하세요. "Entra ID"
3. 선택 "기업용 애플리케이션"합니다.

엔터프라이즈 애플리케이션을 생성하고 **StorageGRID SSO** 구성을 저장합니다

StorageGRID에서 Entra ID에 대한 SSO 구성을 저장하려면 Entra ID를 사용하여 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 생성해야 합니다. Entra ID에서 페더레이션 메타데이터 URL을 복사하여 SSO 구성 페이지의 해당 페더레이션 메타데이터 **URL** 필드에 붙여넣습니다.

단계

1. 각 관리 노드에 대해 다음 단계를 반복하십시오.

a. Entra ID 엔터프라이즈 애플리케이션 창에서 *새 애플리케이션*을 선택합니다.

b. *나만의 애플리케이션 만들기*를 선택합니다.

c. 이름에는 SSO 구성 페이지의 관리자 노드 세부 정보 표에서 복사한 *엔터프라이즈 애플리케이션 이름*을 입력하십시오.

d. 갤러리에서 찾을 수 없는 다른 애플리케이션 통합(비갤러리) 라디오 버튼을 선택된 상태로 두십시오.

e. *생성*을 선택합니다.

f. **2.** 싱글 사인온 설정 상자에서 시작하기 링크를 선택하거나 왼쪽 여백에서 싱글 사인온 링크를 선택하세요.

g. **SAML** 상자를 선택합니다.

h. *3단계 SAML 서명 인증서*에서 찾을 수 있는 *앱 페더레이션 메타데이터 URL*을 복사합니다.

i. SSO 구성 페이지로 이동하여 사용한 엔터프라이즈 애플리케이션 이름*에 해당하는 **URL**을 *페더레이션 메타데이터 **URL** 필드에 붙여넣습니다.

2. 각 관리 노드에 대한 페더레이션 메타데이터 URL을 붙여넣고 SSO 구성에 필요한 다른 모든 변경 사항을 적용한 후 SSO 구성 페이지에서 *저장*을 선택하십시오.

모든 관리자 노드에 대한 **SAML** 메타데이터를 다운로드합니다.

SSO 구성이 저장되면 StorageGRID 시스템의 각 관리 노드에 대한 SAML 메타데이터 파일을 다운로드할 수 있습니다.

단계

1. 각 관리 노드에 대해 이 단계를 반복하십시오.

a. 관리 노드에서 StorageGRID에 로그인합니다.

b. * 구성 * > * 액세스 제어 * > * 싱글 사인온 * 을 선택합니다.

c. 해당 관리 노드의 SAML 메타데이터를 다운로드하려면 버튼을 선택하십시오.

d. Entra ID에 업로드할 파일을 저장합니다.

SAML 메타데이터를 각 엔터프라이즈 애플리케이션에 업로드합니다

각 StorageGRID 관리 노드에 대한 SAML 메타데이터 파일을 다운로드한 후 Entra ID에서 다음 단계를 수행하십시오.

단계

1. Azure 포털로 돌아가십시오.
2. 각 엔터프라이즈 애플리케이션에 대해 이 단계를 반복합니다.

> 이전에 추가한 애플리케이션이 목록에 표시되려면 엔터프라이즈 애플리케이션 페이지를 새로고침해야 할 수 있습니다.

a. 엔터프라이즈 애플리케이션의 속성 페이지로 이동합니다.

b. *할당 필요*를 *아니요*로 설정합니다(할당을 별도로 구성하려는 경우는 제외).

c. 싱글 사인온 페이지로 이동합니다.

d. SAML 구성을 완료합니다.

e. 메타데이터 파일 업로드 버튼을 선택하고 해당 관리자 노드에 대해 다운로드한 SAML 메타데이터 파일을 선택하십시오.

f. 파일이 로드되면 *저장*을 선택한 다음 *X*를 선택하여 창을 닫습니다. 그러면 SAML을 사용한 싱글 사인온 설정 페이지로 돌아갑니다.

3. "각 애플리케이션을 테스트합니다.".

StorageGRID에 대한 **PingFederate**에서 서비스 공급자 연결 생성

PingFederate를 사용하여 시스템의 각 관리 노드에 대한 서비스 공급자(SP) 연결을 생성합니다. 프로세스 속도를 높이기 위해 StorageGRID에서 SAML 메타데이터를 가져옵니다.

시작하기 전에

- StorageGRID에 대한 Single Sign-On을 구성했으며 SSO 유형으로 *Ping Federate*를 선택했습니다.
- Grid Manager에 "샌드박스 모드에 진입했습니다."이(가) 있습니다.
- 시스템의 각 관리자 노드에 대한 *SP 연결 ID*가 있습니다. 이러한 값은 SSO 구성 페이지의 관리자 노드 세부 정보 테이블에서 확인할 수 있습니다.
- 시스템의 각 관리자 노드에 대한 *SAML 메타데이터*를 다운로드했습니다.
- PingFederate 서버에서 SP 연결을 생성해 본 경험이 있습니다.
- PingFederate 서버용 "관리자 참조 가이드"이(가) 있습니다. PingFederate 설명서에서 자세한 단계별 지침과 설명을 확인할 수 있습니다.
- PingFederate 서버용 "관리자 권한"이(가) 있습니다.

이 작업 정보

이 지침은 PingFederate 서버 버전 10.3을 StorageGRID의 SSO 공급자로 구성하는 방법을 요약합니다. 다른 버전의 PingFederate를 사용하는 경우 이 지침을 수정해야 할 수 있습니다. 해당 릴리스에 대한 자세한 지침은 PingFederate 서버 설명서를 참조하십시오.

PingFederate에서 사전 요구 사항 완료

StorageGRID에 사용할 SP 연결을 생성하기 전에 PingFederate에서 필수 작업을 완료해야 합니다. SP 연결을 구성할 때 이러한 필수 작업에서 얻은 정보를 사용합니다.

데이터 저장소 생성

아직 데이터 저장소를 생성하지 않았다면 PingFederate를 AD FS LDAP 서버에 연결하는 데이터 저장소를 생성하십시오. StorageGRID에서 "ID 페더레이션 구성" 할 때 사용한 값을 사용하십시오.

- 유형: 디렉터리(LDAP)
- **LDAP** 유형: Active Directory
- 바이너리 속성 이름: LDAP 바이너리 속성 탭에 표시된 대로 *objectGUID*를 정확하게 입력하십시오.

암호 자격 증명 유효성 검사기 생성

아직 비밀번호 자격 증명 유효성 검사기를 만들지 않았다면 지금 만드세요.

- 유형: LDAP 사용자 이름 암호 자격 증명 유효성 검사기
- 데이터 저장소: 생성한 데이터 저장소를 선택합니다.

- 검색 기준: LDAP에서 정보를 입력하십시오(예: DC=saml,DC=sgws).
- 검색 필터: sAMAccountName=${username}
- 범위: 서브트리

IdP 어댑터 인스턴스 생성

아직 IdP 어댑터 인스턴스를 생성하지 않았다면 지금 생성하세요.

단계

1. 인증 > 통합 > *IdP 어댑터*로 이동합니다.
2. *새 인스턴스 생성*을 선택합니다.
3. 유형 탭에서 *HTML Form IdP Adapter*를 선택합니다.
4. IdP 어댑터 탭에서 *'Credential Validators'에 새 행 추가*를 선택합니다.
5. 생성한 비밀번호 자격 증명 유효성 검사기을 선택합니다.
6. 어댑터 속성 탭에서 가명*에 대해 *사용자 이름 속성을 선택합니다.
7. *저장*을 선택하세요.

서명 인증서를 생성하거나 가져옵니다.

아직 서명 인증서를 생성하거나 가져오지 않았다면 지금 생성하거나 가져오세요.

단계

1. 보안 > *서명 및 복호화 키 및 인증서*로 이동합니다.
2. 서명 인증서를 생성하거나 가져옵니다.

PingFederate에서 SP 연결 만들기

PingFederate에서 SP 연결을 생성할 때 관리 노드용으로 StorageGRID에서 다운로드한 SAML 메타데이터를 가져옵니다. 메타데이터 파일에는 필요한 여러 특정 값이 포함되어 있습니다.

StorageGRID 시스템의 각 관리 노드에 대해 SP 연결을 생성해야 사용자가 모든 노드에 안전하게 로그인하고 로그아웃할 수 있습니다. 이 지침에 따라 첫 번째 SP 연결을 생성하십시오. 그런 다음, 추가 SP 연결 생성으로 이동하여 필요한 추가 연결을 생성하십시오.

SP 연결 유형 선택

단계

1. 응용 프로그램 > 통합 > *SP 연결*로 이동하세요.
2. *연결 생성*을 선택합니다.
3. *이 연결에 템플릿을 사용하지 않음*을 선택합니다.
4. 브라우저 SSO 프로필 및 프로토콜로 *SAML 2.0*을 선택합니다.

SP 메타데이터 가져오기

단계

1. 메타데이터 가져오기 탭에서 *파일*을 선택합니다.
2. 관리 노드의 SSO 구성 페이지에서 다운로드한 SAML 메타데이터 파일을 선택하십시오.
3. 메타데이터 요약과 일반 정보 탭에 제공된 정보를 검토하십시오.

   파트너의 엔티티 ID와 연결 이름은 StorageGRID SP 연결 ID로 설정됩니다. (예: 10.96.105.200-DC1-ADM1-105-200). 기본 URL은 StorageGRID 관리 노드의 IP 주소입니다.

4. * 다음 * 을 선택합니다.

IdP 브라우저 **SSO** 구성

단계

1. 브라우저 SSO 탭에서 *브라우저 SSO 구성*을 선택합니다.
2. SAML 프로필 탭에서 **SP-initiated SSO**, **SP-initial SLO**, **IdP-initiated SSO** 및 **IdP-initiated SLO** 옵션을 선택합니다.
3. * 다음 * 을 선택합니다.
4. 어설션 수명 탭에서는 아무것도 변경하지 마십시오.
5. 어설션 생성 탭에서 *어설션 생성 구성*을 선택합니다.
   a. ID 매핑 탭에서 *표준*을 선택합니다.
   b. 속성 계약 탭에서 속성 계약으로 *SAML_SUBJECT*를 사용하고 가져온 지정되지 않은 이름 형식을 사용합니다.
6. 계약 연장의 경우, 사용하지 않는 `urn:oid`을(를) 제거하려면 *삭제*를 선택합니다.

맵 어댑터 인스턴스

단계

1. 인증 소스 매핑 탭에서 *새 어댑터 인스턴스 매핑*을 선택합니다.
2. 어댑터 인스턴스 탭에서 생성한 어댑터 인스턴스을 선택합니다.
3. 매핑 방법 탭에서 *데이터 저장소에서 추가 속성 검색*을 선택합니다.
4. 속성 소스 및 사용자 조회 탭에서 *속성 소스 추가*를 선택합니다.
5. 데이터 저장소 탭에서 설명을 입력하고 추가한 데이터 저장소을 선택합니다.
6. LDAP 디렉터리 검색 탭에서:
   - *기본 DN*을 입력하십시오. 이 값은 LDAP 서버에 대해 StorageGRID에 입력한 값과 정확히 일치해야 합니다.
   - 검색 범위에서 *하위 트리*를 선택합니다.
   - 루트 객체 클래스의 경우, **objectGUID** 또는 **userPrincipalName** 속성 중 하나를 검색하여 추가하십시오.
7. LDAP 이진 속성 인코딩 유형 탭에서 **objectGUID** 속성에 대해 *Base64*를 선택합니다.
8. LDAP 필터 탭에서 *sAMAccountName=${username}*를 입력합니다.
9. 속성 계약 이행 탭에서 소스 드롭다운에서 **LDAP(속성)*을 선택하고 값 드롭다운에서 ***objectGUID** 또는

*userPrincipalName*을 선택합니다.

10. 속성 소스를 검토한 후 저장합니다.
11. Failsave Attribute Source 탭에서 *SSO 트랜잭션 취소*를 선택합니다.
12. 요약 내용을 검토하고 *완료*를 선택합니다.
13. *완료*를 선택합니다.

프로토콜 설정 구성

단계

1. **SP Connection** > **Browser SSO** > **Protocol Settings** 탭에서 *Configure Protocol Settings*를 선택합니다.
2. 어설션 소비자 서비스 URL 탭에서 StorageGRID SAML 메타데이터에서 가져온 기본값(바인딩의 경우 **POST** 및 엔드포인트 URL의 경우 `/api/saml-response`)을 그대로 사용하십시오.
3. SLO 서비스 URL 탭에서 StorageGRID SAML 메타데이터에서 가져온 기본값(바인딩의 경우 **REDIRECT**, 엔드포인트 URL의 경우 `/api/saml-logout`)을 그대로 사용하십시오.
4. 허용 가능한 SAML 바인딩 탭에서 *ARTIFACT*와 *SOAP*를 선택 해제하세요. *POST*와 *REDIRECT*만 필수입니다.
5. 서명 정책 탭에서 인증 요청에 서명 필수 및 항상 어설션에 서명 확인란을 선택된 상태로 둡니다.
6. 암호화 정책 탭에서 *없음*을 선택합니다.
7. 요약 내용을 검토하고 *완료*를 선택하여 프로토콜 설정을 저장하십시오.
8. 요약 내용을 검토하고 *완료*를 선택하여 브라우저 SSO 설정을 저장합니다.

자격 증명 구성

단계

1. SP 연결 탭에서 *자격 증명*을 선택합니다.
2. 자격 증명 탭에서 *자격 증명 구성*을 선택합니다.
3. 생성하거나 가져온 서명 인증서을(를) 선택합니다.
4. *다음*을 선택하여 *서명 확인 설정 관리*로 이동합니다.
   a. 신뢰 모델 탭에서 *고정되지 않음*을 선택합니다.
   b. 서명 확인 인증서 탭에서 StorageGRID SAML 메타데이터에서 가져온 서명 인증서 정보를 검토합니다.
5. 요약 화면을 검토하고 *저장*을 선택하여 SP 연결을 저장하십시오.

추가 **SP** 연결 생성

첫 번째 SP 연결을 복사하여 그리드의 각 관리 노드에 필요한 SP 연결을 생성할 수 있습니다. 각 복사본마다 새로운 메타데이터를 업로드합니다.

> ⓘ 서로 다른 관리 노드에 대한 SP 연결은 파트너 엔티티 ID, 기본 URL, 연결 ID, 연결 이름, 서명 확인 및 SLO 응답 URL을 제외하고는 동일한 설정을 사용합니다.

단계

1. 추가 관리 노드마다 초기 SP 연결의 복사본을 만들려면 작업 > *복사*를 선택하십시오.
2. 복사본에 대한 연결 ID와 연결 이름을 입력하고 *저장*을 선택합니다.
3. 관리 노드에 해당하는 메타데이터 파일을 선택하십시오.
   a. 작업 > *메타데이터로 업데이트*를 선택합니다.
   b. *파일 선택*을 선택하고 메타데이터를 업로드합니다.
   c. * 다음 * 을 선택합니다.
   d. *저장*을 선택하세요.
4. 사용되지 않는 속성으로 인해 발생하는 오류를 해결하세요:
   a. 새 연결을 선택합니다.
   b. *브라우저 SSO 구성 > 어설션 생성 구성 > 속성 계약*을 선택하십시오.
   c. **urn:oid** 항목을 삭제합니다.
   d. *저장*을 선택하세요.

StorageGRID에서 SSO 비활성화

싱글 사인온(SSO) 기능을 더 이상 사용하지 않으려면 비활성화할 수 있습니다. ID 페더레이션을 비활성화하려면 먼저 싱글 사인온을 비활성화해야 합니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.

단계

1. * 구성 * > * 액세스 제어 * > * 싱글 사인온 * 을 선택합니다.

   싱글 사인온 페이지가 나타납니다.

2. *SSO 비활성화*를 선택합니다.
3. *예*를 선택합니다.

   로컬 사용자가 이제 로그인할 수 있다는 경고 메시지가 나타납니다.

다음에 StorageGRID에 로그인하면 StorageGRID 로그인 페이지가 나타나고 로컬 또는 페더레이션 StorageGRID 사용자의 사용자 이름과 암호를 입력해야 합니다.

StorageGRID 관리 노드에 대한 SSO를 일시적으로 비활성화했다가 다시 활성화합니다

싱글 사인온(SSO) 시스템에 장애가 발생하면 그리드 관리자에 로그인할 수 없습니다. 이 경우, 특정 관리 노드에 대해 SSO를 일시적으로 비활성화한 후 다시 활성화할 수 있습니다. SSO를 비활성화한 후 다시 활성화하려면 해당 노드의 명령 셸에 접속해야 합니다.

시작하기 전에

- "특정 액세스 권한"이(가) 있습니다.

- You have the `Passwords.txt` 파일을 가지고 계시네요.
- 로컬 루트 사용자의 암호를 알고 있습니다.

이 작업 정보

하나의 관리 노드에 대해 SSO를 비활성화한 후에는 로컬 루트 사용자로 Grid Manager에 로그인할 수 있습니다. StorageGRID 시스템의 보안을 유지하려면 로그아웃하는 즉시 노드의 명령 셸을 사용하여 관리 노드에서 SSO를 다시 활성화해야 합니다.

하나의 관리자 노드에 대해 SSO를 비활성화해도 그리드 내 다른 관리자 노드의 SSO 설정에는 영향을 미치지 않습니다. 그리드 관리자의 싱글 사인온 페이지에서 **SSO** 활성화 확인란은 선택된 상태로 유지되며, 기존 SSO 설정은 사용자가 업데이트하지 않는 한 그대로 유지됩니다.

단계

1. 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@Admin_Node_IP`
   b. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.
   c. 루트 권한으로 전환하려면 다음 명령을 입력하십시오. `su -`
   d. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.

      루트 계정으로 로그인하면 프롬프트가 `$`에서 `#`로 변경됩니다.

2. 다음 명령을 실행합니다.`disable-saml`

   해당 명령은 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

3. SSO를 비활성화할 것인지 확인합니다.

   해당 노드에서 싱글 사인온(SSO)이 비활성화되었다는 메시지가 표시됩니다.

4. 웹 브라우저를 통해 동일한 관리 노드에서 그리드 관리자에 접속합니다.

   SSO가 비활성화되었으므로 이제 그리드 관리자 로그인 페이지가 표시됩니다.

5. 사용자 이름 root와 로컬 루트 사용자의 암호로 로그인합니다.
6. SSO 구성을 수정해야 하여 SSO를 일시적으로 비활성화한 경우:
   a. * 구성 * > * 액세스 제어 * > * 싱글 사인온 * 을 선택합니다.
   b. 잘못되었거나 오래된 SSO 설정을 변경합니다.
   c. *저장*을 선택하세요.

      싱글 사인온 페이지에서 *저장*을 선택하면 전체 그리드에 대해 SSO가 자동으로 다시 활성화됩니다.

7. 다른 이유로 그리드 관리자에 액세스해야 해서 SSO를 일시적으로 비활성화한 경우:
   a. 필요한 작업을 수행하십시오.
   b. *로그아웃*을 선택하고 Grid Manager를 닫습니다.

c. 관리자 노드에서 SSO를 다시 활성화하십시오. 다음 단계 중 하나를 수행할 수 있습니다.

   - 다음 명령을 실행합니다. `enable-saml`

     해당 명령은 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

   SSO를 활성화할 것인지 확인합니다.

   해당 노드에서 싱글 사인온(SSO)이 활성화되었다는 메시지가 표시됩니다.

   - 그리드 노드를 재부팅하세요: `reboot`

8. 웹 브라우저를 통해 동일한 관리 노드에서 Grid Manager에 접속합니다.
9. StorageGRID 로그인 페이지가 나타나고 Grid Manager에 액세스하려면 SSO 자격 증명을 입력해야 하는지 확인하십시오.

그리드 페더레이션 사용

StorageGRID 그리드 연합에 대해 알아보세요

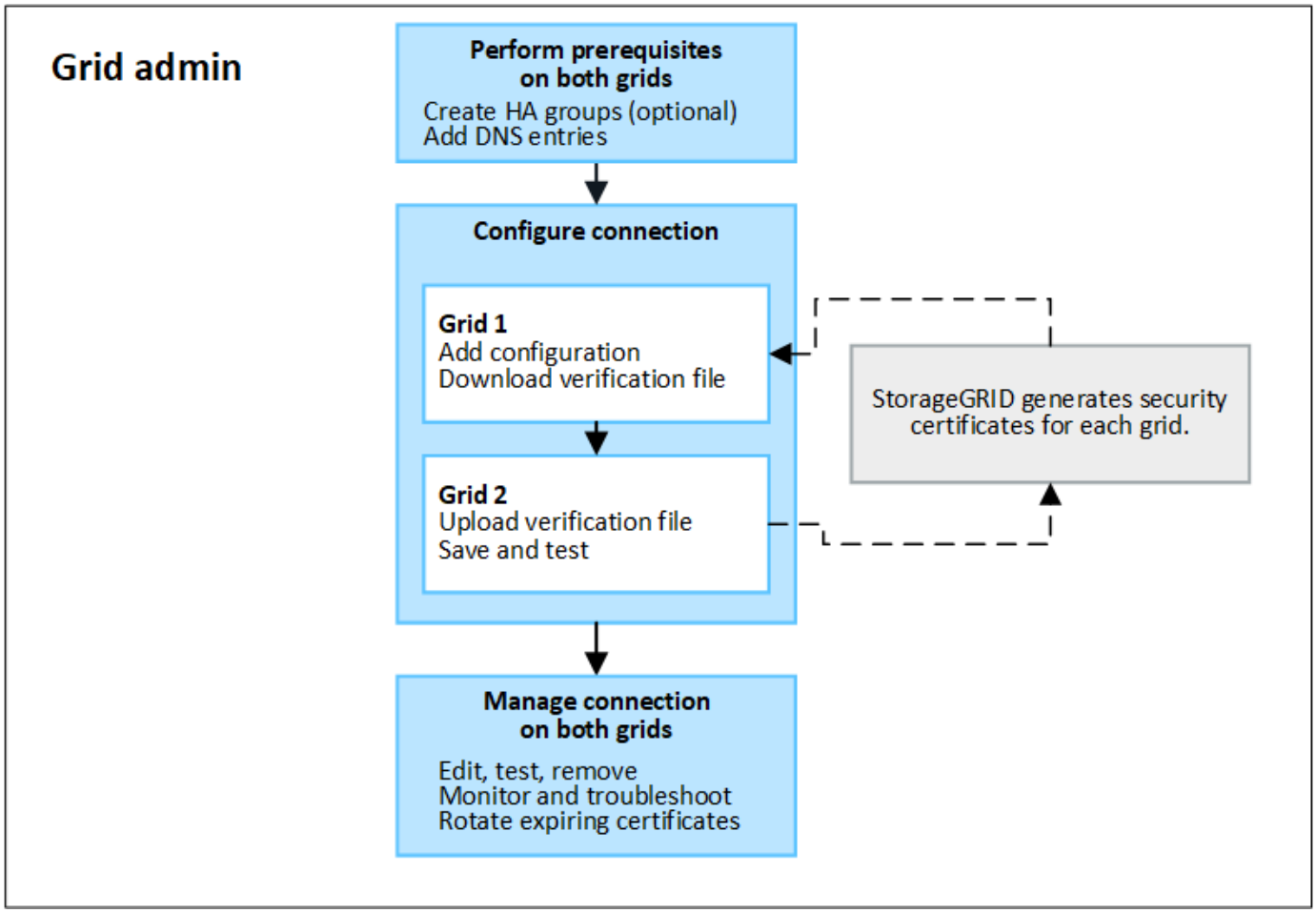
그리드 페더레이션을 사용하면 테넌트를 복제하고 재해 복구를 위해 두 StorageGRID 시스템 간에 객체를 복제할 수 있습니다.

그리드 페더레이션 연결이란 무엇입니까?

그리드 연합 연결은 두 StorageGRID 시스템의 관리 노드와 게이트웨이 노드 간의 양방향, 신뢰할 수 있고 안전한 연결입니다.

그리드 페더레이션을 위한 워크플로

워크플로 다이어그램은 두 그리드 간의 그리드 연합 연결을 구성하는 단계를 요약합니다.



그리드 페더레이션 연결에 대한 고려 사항 및 요구 사항

- 그리드 연합에 사용되는 그리드는 StorageGRID 버전이 동일하거나 주요 버전 차이가 하나 이하이어야 합니다.

  버전 요구 사항에 대한 자세한 내용은 "릴리스 노트"를 참조하십시오. NetApp 계정으로 로그인하거나 계정을 생성하여 릴리스 노트에 액세스해야 합니다.

- 그리드는 다른 그리드와 하나 이상의 그리드 연합 연결을 가질 수 있습니다. 각 그리드 연합 연결은 다른 연결과 독립적입니다. 예를 들어, 그리드 1이 그리드 2와 하나의 연결을 갖고 그리드 3과 또 다른 연결을 갖고 있더라도, 그리드 2와 그리드 3 사이에는 암묵적인 연결이 없습니다.
- 그리드 연합 연결은 양방향입니다. 연결이 설정되면 어느 그리드에서든 연결을 모니터링하고 관리할 수 있습니다.
- "계정 복제" 또는 "교차 그리드 복제"을(를) 사용하려면 먼저 그리드 페더레이션 연결이 하나 이상 있어야 합니다.

네트워킹 및 **IP** 주소 요구 사항

- 그리드 페더레이션 연결은 그리드 네트워크, 관리 네트워크 또는 클라이언트 네트워크에서 발생할 수 있습니다.
- 그리드 페더레이션 연결은 하나의 그리드를 다른 그리드와 연결합니다. 각 그리드의 구성은 다른 그리드에 있는 그리드 페더레이션 엔드포인트를 지정하며, 이 엔드포인트는 관리 노드, 게이트웨이 노드 또는 둘 다로 구성됩니다.
- 최적의 구성 방법은 각 그리드에서 게이트웨이와 관리 노드의 "고가용성(HA) 그룹"을 연결하는 것입니다. HA 그룹을 사용하면 노드에 장애가 발생하더라도 그리드 페더레이션 연결이 온라인 상태로 유지됩니다. 두 HA 그룹 중 하나의 활성 인터페이스에 장애가 발생하면 백업 인터페이스를 사용하여 연결할 수 있습니다.
- 단일 관리 노드 또는 게이트웨이 노드의 IP 주소를 사용하는 그리드 페더레이션 연결을 생성하는 것은 권장되지

않습니다. 해당 노드를 사용할 수 없게 되면 그리드 페더레이션 연결도 사용할 수 없게 됩니다.

- "교차 그리드 복제"객체 관리를 위해서는 각 그리드의 스토리지 노드가 다른 그리드에 구성된 관리 노드 및 게이트웨이 노드에 액세스할 수 있어야 합니다. 각 그리드에서 모든 스토리지 노드가 연결에 사용되는 관리 노드 또는 게이트웨이 노드에 대해 높은 대역폭의 경로를 확보하고 있는지 확인하십시오.

FQDN을 사용하여 연결 로드 밸런싱 수행

운영 환경의 경우, 연결의 각 그리드를 식별하기 위해 정규화된 도메인 이름(FQDN)을 사용하십시오. 그런 다음 다음과 같이 적절한 DNS 항목을 생성하십시오.

- Grid 1의 정규화된 도메인 이름(FQDN)은 Grid 1의 HA 그룹에 대한 하나 이상의 가상 IP(VIP) 주소 또는 Grid 1의 하나 이상의 관리 노드 또는 게이트웨이 노드의 IP 주소에 매핑됩니다.
- Grid 2의 FQDN은 Grid 2의 하나 이상의 VIP 주소 또는 Grid 2의 하나 이상의 관리 노드 또는 게이트웨이 노드의 IP 주소에 매핑됩니다.

여러 개의 DNS 항목을 사용하는 경우, 연결을 사용하려는 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

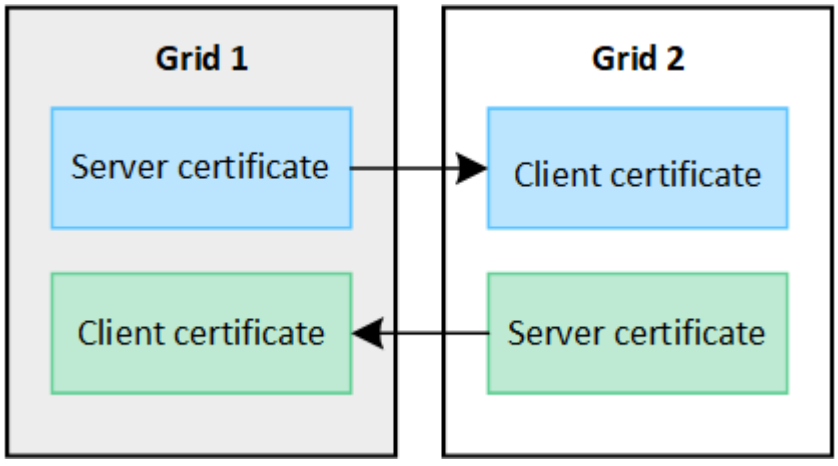
그리드 페더레이션 연결을 생성할 때 23000에서 23999 사이의 사용되지 않는 포트 번호를 지정할 수 있습니다. 이 연결에 참여하는 두 그리드는 동일한 포트를 사용합니다.

두 그리드 모두에서 어떤 노드도 이 포트를 다른 연결에 사용하지 않도록 해야 합니다.

인증서 요구 사항

그리드 페더레이션 연결을 구성하면 StorageGRID가 자동으로 4개의 SSL 인증서를 생성합니다.

- 그리드 1에서 그리드 2로 전송되는 정보를 인증하고 암호화하기 위한 서버 및 클라이언트 인증서
- 그리드 2에서 그리드 1로 전송되는 정보를 인증하고 암호화하기 위한 서버 및 클라이언트 인증서



기본적으로 인증서의 유효 기간은 730일(2년)입니다. 인증서 만료일이 가까워지면 **Expiration of grid federation certificate** 알림이 표시되어 Grid Manager를 통해 인증서를 갱신할 수 있습니다.

연결 양쪽 끝의 인증서가 만료되면 연결이 중단됩니다. 인증서가 업데이트될 때까지 데이터 복제는 보류됩니다.

더 알아보기

- "그리드 페더레이션 연결 생성"
- "그리드 페더레이션 연결 관리"
- "그리드 페더레이션 오류 해결"

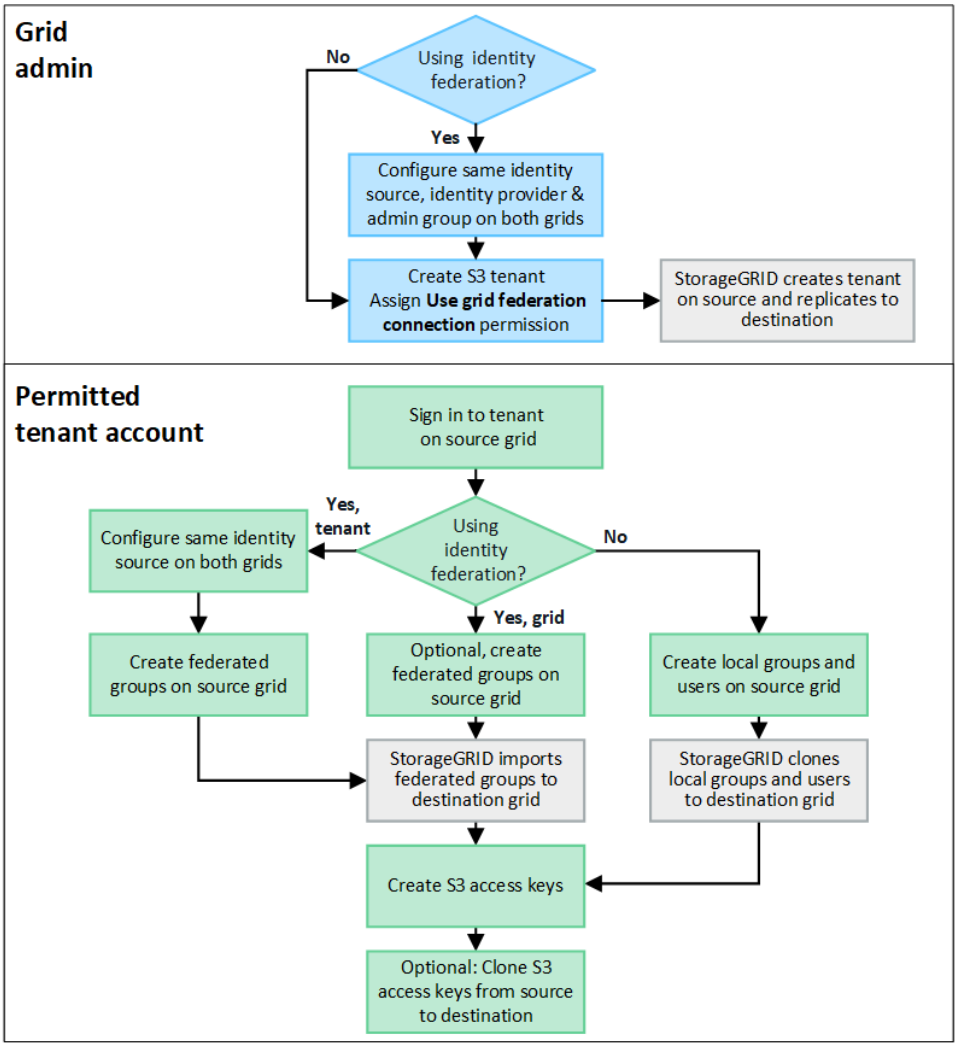
StorageGRID의 계정 복제에 대해 알아보십시오

계정 복제는 "그리드 페더레이션 연결"의 StorageGRID 시스템 간에 테넌트 계정, 테넌트 그룹, 테넌트 사용자 및 선택적으로 S3 액세스 키를 자동으로 복제하는 기능입니다.

계정 복제는 "교차 그리드 복제"에 필요합니다. 소스 StorageGRID 시스템에서 대상 StorageGRID 시스템으로 계정 정보를 복제하면 테넌트 사용자와 그룹이 두 그리드 모두에서 해당 버킷과 객체에 액세스할 수 있습니다.

계정 복제 워크플로

워크플로 다이어그램은 그리드 관리자와 권한이 부여된 테넌트가 계정 복제를 설정하기 위해 수행하는 단계를 보여줍니다. 이러한 단계는 "그리드 페더레이션 연결이 구성되었습니다." 이후에 수행됩니다.



그리드 관리자 워크플로

그리드 관리자가 수행하는 단계는 "그리드 페더레이션 연결"의 StorageGRID 시스템에서 단일 로그인(SSO)을 사용하는지 또는 ID 페더레이션을 사용하는지에 따라 달라집니다.

계정 복제에 대한 **SSO** 구성(선택 사항)

그리드 페더레이션 연결에 있는 StorageGRID 시스템 중 하나라도 SSO를 사용하는 경우, 두 그리드 모두 SSO를 사용해야 합니다. 그리드 페더레이션용 테넌트 계정을 생성하기 전에, 테넌트의 소스 및 대상 그리드의 그리드 관리자는 다음 단계를 수행해야 합니다.

단계

1. 두 그리드에 동일한 ID 소스를 구성하십시오. 을 참조하십시오."ID 페더레이션 사용"
2. 두 그리드 모두에 동일한 SSO ID 공급자(IdP)를 구성하십시오. "싱글 사인온(SSO) 구성"을 참조하십시오.
3. "동일한 관리자 그룹을 생성합니다." 동일한 페더레이션 그룹을 가져와서 두 그리드 모두에서 사용할 수 있습니다.

   테넌트를 생성할 때 소스 및 대상 테넌트 계정 모두에 대해 초기 루트 액세스 권한을 갖도록 이 그룹을 선택합니다.

   > 테넌트를 생성하기 전에 이 관리 그룹이 두 그리드 모두에 존재하지 않으면 테넌트가 대상으로 복제되지 않습니다.

계정 복제에 대한 그리드 수준 **ID** 연동 구성(선택 사항)

StorageGRID 시스템 중 하나라도 SSO 없이 ID 페더레이션을 사용하는 경우, 두 그리드 모두 ID 페더레이션을 사용해야 합니다. 그리드 페더레이션을 위한 테넌트 계정을 생성하기 전에, 테넌트의 소스 및 대상 그리드의 그리드 관리자는 다음 단계를 수행해야 합니다.

단계

1. 두 그리드에 동일한 ID 소스를 구성하십시오. 을 참조하십시오."ID 페더레이션 사용"
2. 선택적으로, 페더레이션 그룹이 소스 및 대상 테넌트 계정 모두에 대해 초기 루트 액세스 권한을 갖도록 하려면 동일한 페더레이션 그룹을 가져와 두 그리드 모두에서 "동일한 관리자 그룹을 생성합니다." 설정합니다.

   > 양쪽 그리드에 모두 존재하지 않는 페더레이션 그룹에 루트 액세스 권한을 할당하면 테넌트가 대상 그리드로 복제되지 않습니다.

3. 연합 그룹이 두 계정 모두에 대해 초기 루트 액세스 권한을 갖지 않도록 하려면 로컬 루트 사용자의 암호를 지정하십시오.

허용된 **S3** 테넌트 계정 생성

선택적으로 SSO 또는 ID 페더레이션을 구성한 후, 그리드 관리자는 다음 단계를 수행하여 어떤 테넌트가 버킷 객체를 다른 StorageGRID 시스템으로 복제할 수 있는지 확인합니다.

단계

1. 테넌트 계정 복제 작업을 위해 테넌트의 소스 그리드로 사용할 그리드를 결정합니다.

   테넌트가 처음 생성되는 그리드를 테넌트의 _소스 그리드_라고 합니다. 테넌트가 복제되는 그리드를 테넌트의 _대상 그리드_라고 합니다.

2. 해당 그리드에서 새 S3 테넌트 계정을 생성하거나 기존 계정을 편집하세요.
3. 그리드 페더레이션 연결 사용 권한을 할당합니다.
4. 테넌트 계정이 자체적으로 페더레이션된 사용자를 관리할 경우, 자체 **ID** 소스 사용 권한을 할당하십시오.

   이 권한이 할당된 경우, 페더레이션 그룹을 생성하기 전에 소스 및 대상 테넌트 계정 모두 동일한 ID 소스를 구성해야 합니다. 소스 테넌트에 추가된 페더레이션 그룹은 두 그리드가 동일한 ID 소스를 사용하지 않는 한 대상 테넌트로 복제할 수 없습니다.

5. 특정 그리드 페더레이션 연결을 선택하십시오.
6. 새 테넌트 또는 수정된 테넌트를 저장합니다.

   그리드 페더레이션 연결 사용 권한이 있는 새 테넌트가 저장되면 StorageGRID는 다음과 같이 다른 그리드에 해당 테넌트의 복제본을 자동으로 생성합니다.

   - 두 테넌트 계정은 동일한 계정 ID, 이름, 스토리지 할당량 및 할당된 권한을 가집니다.
   - 루트 액세스 권한을 가지도록 페더레이션 그룹을 선택한 경우, 해당 그룹이 대상 테넌트에 복제됩니다.
   - 로컬 사용자를 선택하여 테넌트에 대한 루트 액세스 권한을 부여한 경우, 해당 사용자는 대상 테넌트에 복제됩니다. 그러나 해당 사용자의 암호는 복제되지 않습니다.

자세한 내용은 "그리드 페더레이션에 허용된 테넌트 관리"을 참조하십시오.

허용된 테넌트 계정 워크플로

그리드 페더레이션 연결 사용 권한이 있는 테넌트가 대상 그리드로 복제된 후, 허용된 테넌트 계정은 다음 단계를 수행하여 테넌트 그룹, 사용자 및 S3 액세스 키를 복제할 수 있습니다.

단계

1. 테넌트의 소스 그리드에서 테넌트 계정에 로그인합니다.
2. 허용되는 경우 소스 및 대상 테넌트 계정 모두에서 ID 페더레이션을 구성하십시오.
3. 소스 테넌트에서 그룹 및 사용자를 생성합니다.

   원본 테넌트에서 새 그룹 또는 사용자가 생성되면 StorageGRID가 자동으로 해당 항목을 대상 테넌트에 복제하지만, 대상에서 원본으로의 복제는 발생하지 않습니다.

4. S3 액세스 키를 생성합니다.
5. 선택적으로 소스 테넌트에서 대상 테넌트로 S3 액세스 키를 복제합니다.

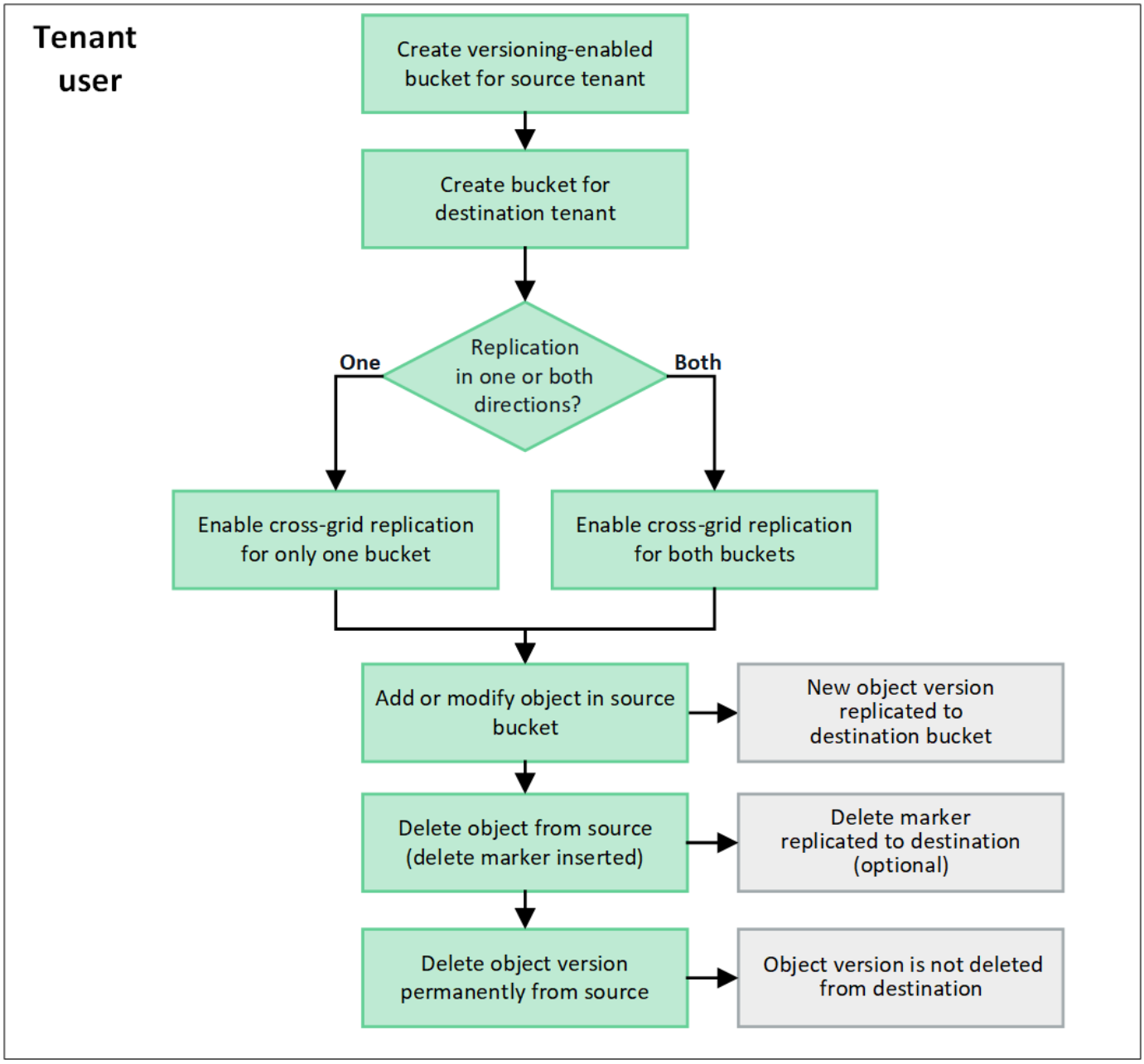
허용된 테넌트 계정 워크플로에 대한 자세한 내용과 그룹, 사용자 및 S3 액세스 키가 복제되는 방법을 알아보려면 "테넌트 그룹 및 사용자 복제" 및 "API를 사용하여 S3 액세스 키 복제"을 참조하세요.

StorageGRID의 교차 그리드 복제에 대해 알아보십시오

크로스 그리드 복제는 "그리드 페더레이션 연결"에 연결된 두 StorageGRID 시스템의 선택된 S3 버킷 간에 객체를 자동으로 복제하는 기능입니다. "계정 복제"은(는) 크로스 그리드 복제에 필요합니다.

그리드 간 복제 워크플로

워크플로 다이어그램은 두 그리드의 버킷 간 교차 그리드 복제를 구성하는 단계를 요약합니다.



그리드 간 복제를 위한 요구 사항

테넌트 계정에 하나 이상의 "그리드 페더레이션 연결"을(를) 사용할 수 있는 그리드 페더레이션 연결 사용 권한이 있는 경우, 루트 액세스 권한이 있는 테넌트 사용자는 각 그리드의 해당 테넌트 계정에 버킷을 생성할 수 있습니다. 이러한 버킷은 다음과 같습니다.

- 서로 다른 이름을 가질 수 있습니다
- 지역마다 다를 수 있습니다.
- 버전 관리 기능이 활성화되어 있어야 합니다.
- 비어 있어야 합니다

두 버킷이 모두 생성된 후에는 두 버킷 중 하나 또는 둘 모두에 대해 그리드 간 복제를 구성할 수 있습니다.

더 알아보기

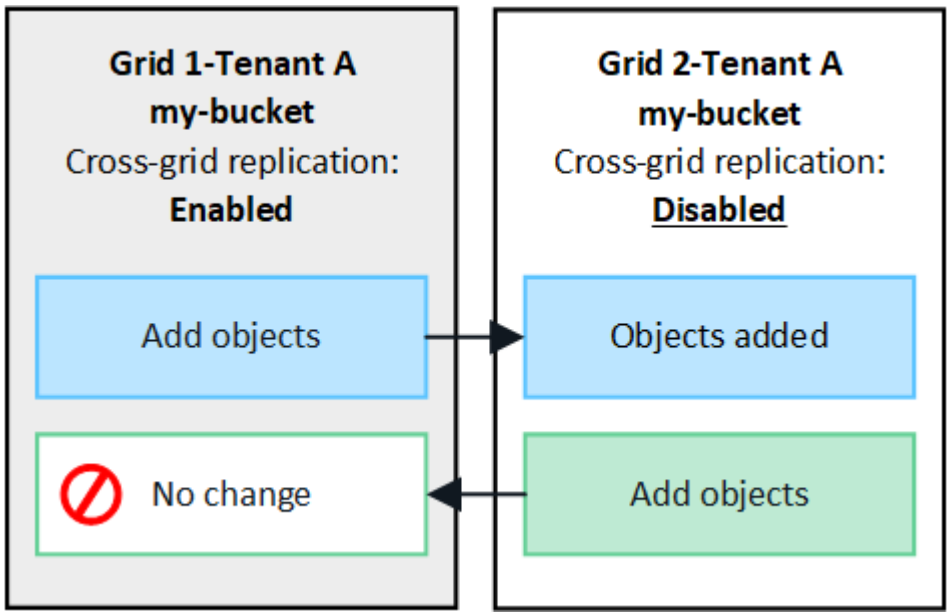
"그리드 간 복제 관리"

그리드 간 복제 작동 방식

그리드 간 복제는 단방향 또는 양방향으로 수행되도록 구성할 수 있습니다.

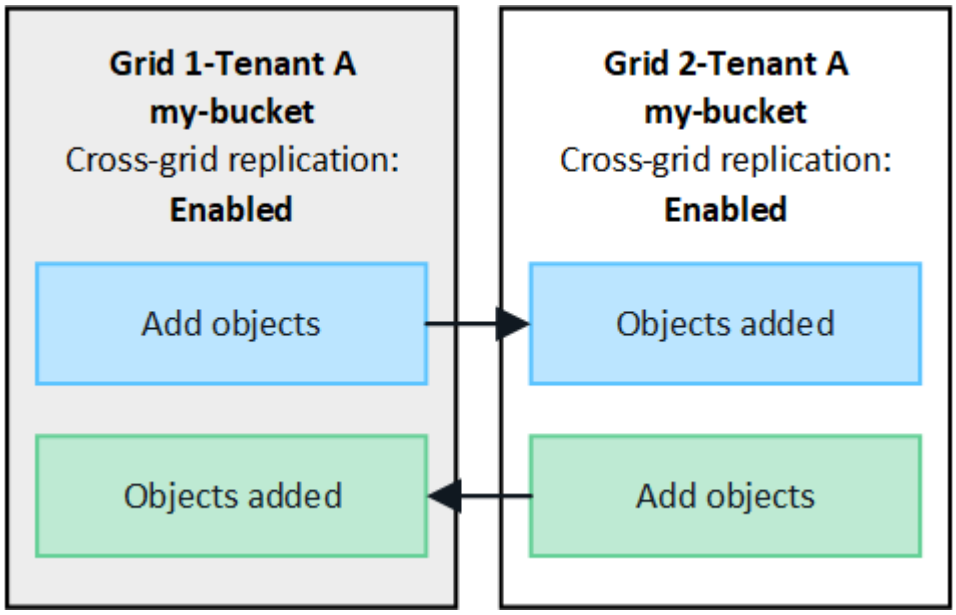
단방향 복제

한 그리드의 버킷에 대해서만 그리드 간 복제를 활성화하면 해당 버킷(원본 버킷)에 추가된 객체는 다른 그리드의 해당 버킷(대상 버킷)으로 복제됩니다. 그러나 대상 버킷에 추가된 객체는 원본 버킷으로 다시 복제되지 않습니다. 그림에서 그리드 간 복제는 `my-bucket` Grid 1에서 Grid 2로 활성화되어 있지만, 반대 방향으로는 활성화되어 있지 않습니다.



양방향 복제

두 그리드 모두에서 동일한 버킷에 대해 그리드 간 복제를 활성화하면 어느 한 버킷에 추가된 객체가 다른 그리드로 복제됩니다. 그림에서는 `my-bucket`에 대해 양방향으로 그리드 간 복제가 활성화되어 있습니다.



오브젝트가 수집될 때 어떻게 됩니까?

크로스 그리드 복제가 활성화된 버킷에 S3 클라이언트가 객체를 추가하면 다음과 같은 현상이 발생합니다.

1. StorageGRID 소스 버킷에서 대상 버킷으로 객체를 자동으로 복제합니다. 이 백그라운드 복제 작업에 소요되는 시간은 대기 중인 다른 복제 작업의 수 등 여러 요인에 따라 달라집니다.

   S3 클라이언트는 GetObject 또는 HeadObject 요청을 실행하여 객체의 복제 상태를 확인할 수 있습니다. 응답에는 StorageGRID 관련 `x-ntap-sg-cgr-replication-status` 응답 헤더가 포함되며, 이 헤더에는 다음 값 중 하나가 있습니다.

그리드	복제 상태
소스	• 완료됨: 모든 그리드 연결에 대한 복제가 성공적으로 완료되었습니다. • **PENDING**: 해당 개체가 하나 이상의 그리드 연결에 복제되지 않았습니다. • **FAILURE**: 복제 작업이 어떤 그리드 연결에 대해서도 보류 중이 아니며, 하나 이상의 연결이 영구적으로 실패했습니다. 사용자가 오류를 해결해야 합니다.
목적지	**REPLICA**: 해당 객체는 원본 그리드에서 복제되었습니다.

   StorageGRID는 `x-amz-replication-status` 헤더를 지원하지 않습니다.

2. StorageGRID는 다른 객체와 마찬가지로 각 그리드의 활성 ILM 정책을 사용하여 객체를 관리합니다. 예를 들어, 그리드 1의 객체 A는 두 개의 복제본으로 저장되어 영구적으로 보존될 수 있으며, 그리드 2로 복제된 객체 A의 복사본은 2+1 이레이저 코딩을 사용하여 저장되고 3년 후에 삭제될 수 있습니다.

객체가 삭제되면 어떻게 됩니까?

앞서 설명한 바와 같이 "데이터 흐름 삭제", StorageGRID는 다음과 같은 이유로 객체를 삭제할 수 있습니다.

- S3 클라이언트가 삭제 요청을 보냅니다.
- 테넌트 관리자 사용자가 "버킷에서 객체 삭제" 옵션을 선택하여 버킷에서 모든 객체를 제거합니다.
- 버킷에는 만료되는 수명 주기 구성이 있습니다.
- 해당 객체에 대한 ILM 규칙의 마지막 기간이 종료되었으며, 더 이상 지정된 배치가 없습니다.

StorageGRID 버킷 내 객체 삭제 작업, 버킷 수명 주기 만료 또는 ILM 배치 만료로 인해 객체를 삭제하는 경우, 복제된 객체는 그리드 페더레이션 연결의 다른 그리드에서 삭제되지 않습니다. 그러나 S3 클라이언트 삭제 작업으로 소스 버킷에 추가된 삭제 마커는 선택적으로 대상 버킷으로 복제될 수 있습니다.

크로스 그리드 복제가 활성화된 버킷에서 S3 클라이언트가 객체를 삭제할 때 발생하는 상황을 이해하려면, 버전 관리가 활성화된 버킷에서 S3 클라이언트가 객체를 삭제하는 방법을 다음과 같이 검토하십시오.

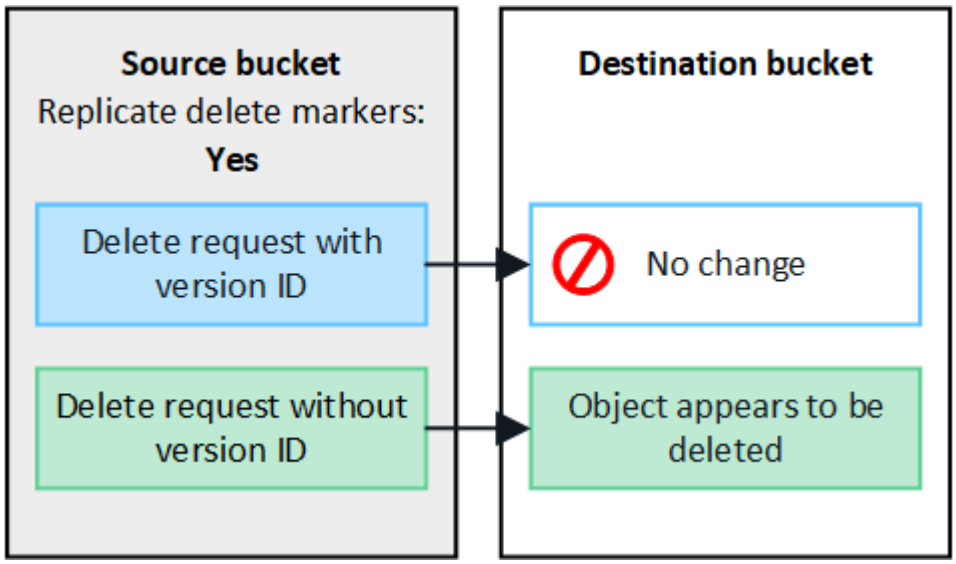
- S3 클라이언트가 버전 ID를 포함한 삭제 요청을 보내면 해당 버전의 객체가 영구적으로 삭제됩니다. 버킷에는 삭제 표시가 추가되지 않습니다.
- S3 클라이언트가 버전 ID를 포함하지 않은 삭제 요청을 보내면 StorageGRID는 객체 버전을 삭제하지 않습니다. 대신 버킷에 삭제 마커를 추가합니다. 이 삭제 마커로 인해 StorageGRID는 객체가 삭제된 것처럼 동작합니다.

- 버전 ID가 없는 GetObject 요청은 다음과 함께 실패합니다. `404 No Object Found`
- 유효한 버전 ID를 사용한 GetObject 요청이 성공하면 요청된 객체 버전이 반환됩니다.

크로스 그리드 복제가 활성화된 버킷에서 S3 클라이언트가 객체를 삭제하면 StorageGRID는 다음과 같이 삭제 요청을 대상으로 복제할지 여부를 결정합니다.

- 삭제 요청에 버전 ID가 포함된 경우 해당 객체 버전은 소스 그리드에서 영구적으로 제거됩니다. 그러나 StorageGRID는 버전 ID가 포함된 삭제 요청을 복제하지 않으므로 대상에서는 동일한 객체 버전이 삭제되지 않습니다.
- 삭제 요청에 버전 ID가 포함되지 않은 경우, StorageGRID는 버킷에 대해 그리드 간 복제가 구성된 방식에 따라 삭제 마커를 선택적으로 복제할 수 있습니다.
  - 삭제 마커 복제(기본값)를 선택하면 소스 버킷에 삭제 마커가 추가되고 대상 버킷으로 복제됩니다. 결과적으로 두 그리드 모두에서 객체가 삭제된 것처럼 보입니다.
  - 삭제 마커 복제를 선택하지 않으면 소스 버킷에는 삭제 마커가 추가되지만 대상 버킷으로는 복제되지 않습니다. 즉, 소스 그리드에서 삭제된 객체는 대상 그리드에서는 삭제되지 않습니다.

그림에서 *삭제 마커 복제*는 "그리드 간 복제가 활성화되었습니다."일 때 *예*로 설정되어 있습니다. 버전 ID가 포함된 소스 버킷의 삭제 요청은 대상 버킷의 객체를 삭제하지 않습니다. 버전 ID가 포함되지 않은 소스 버킷의 삭제 요청은 대상 버킷의 객체를 삭제하는 것처럼 보입니다.



그리드 간 객체 삭제를 동기화하려면 양쪽 그리드의 버킷에 해당하는 "S3 라이프사이클 구성"을 생성하십시오.

암호화된 객체가 복제되는 방식

그리드 간 복제를 사용하여 그리드 간에 객체를 복제할 때 개별 객체를 암호화하거나, 기본 버킷 암호화를 사용하거나, 그리드 전체 암호화를 구성할 수 있습니다. 버킷에 대한 그리드 간 복제를 활성화하기 전이나 후에 기본 버킷 또는 그리드 전체 암호화 설정을 추가, 수정 또는 제거할 수 있습니다.

개별 객체를 암호화하려면 소스 버킷에 객체를 추가할 때 SSE(StorageGRID에서 관리하는 키를 사용하는 서버 측 암호화)를 사용할 수 있습니다. `x-amz-server-side-encryption` 요청 헤더를 사용하고 `AES256`을(를) 지정합니다. "서버 측 암호화 사용"을(를) 참조하십시오.

SSE-C(고객 제공 키를 사용하는 서버 측 암호화)는 그리드 간 복제에 지원되지 않습니다. 데이터 수집 작업이 실패합니다.

버킷에 기본 암호화를 사용하려면 PutBucketEncryption 요청을 사용하고 `SSEAlgorithm` 매개변수를 `AES256`로 설정하십시오. 버킷 수준 암호화는 `x-amz-server-side-encryption` 요청 헤더 없이 수집된 모든 객체에 적용됩니다. "버킷에 대한 작업"을 참조하십시오.

그리드 수준 암호화를 사용하려면 저장된 객체 암호화 옵션을 *AES-256*으로 설정하십시오. 그리드 수준 암호화는 버킷 수준에서 암호화되지 않았거나 `x-amz-server-side-encryption` 요청 헤더 없이 수집된 모든 객체에 적용됩니다. "네트워크 및 객체 옵션 구성"을 참조하십시오.

SSE는 AES-128을 지원하지 않습니다. 소스 그리드에서 **AES-128** 옵션을 사용하여 저장된 객체 암호화 옵션을 활성화하더라도 AES-128 알고리즘은 복제된 객체에 적용되지 않습니다. 대신 복제된 객체는 대상의 기본 버킷 또는 그리드 수준 암호화 설정(사용 가능한 경우)을 사용합니다.

소스 오브젝트를 암호화하는 방법을 결정할 때 StorageGRID는 다음 규칙을 적용합니다.

1. 수집 헤더가 있는 경우 `x-amz-server-side-encryption` 이를 사용합니다.
2. 수집 헤더가 없는 경우, 구성된 경우 버킷의 기본 암호화 설정을 사용합니다.
3. 버킷 설정이 구성되지 않은 경우, 구성된 경우 그리드 전체 암호화 설정을 사용합니다.
4. 그리드 전체에 적용되는 설정이 없는 경우 소스 객체를 암호화하지 마십시오.

복제된 객체를 암호화하는 방법을 결정할 때 StorageGRID는 다음 규칙을 이 순서대로 적용합니다.

1. 소스 객체가 AES-128 암호화를 사용하는 경우를 제외하고, 소스 객체와 동일한 암호화를 사용합니다.
2. 원본 객체가 암호화되지 않았거나 AES-128을 사용하는 경우, 대상 버킷에 기본 암호화 설정이 구성되어 있다면 해당 설정을 사용합니다.
3. 대상 버킷에 암호화 설정이 없는 경우, 구성된 경우 대상의 그리드 전체 암호화 설정을 사용합니다.
4. 그리드 전체에 적용되는 설정이 없는 경우 대상 객체를 암호화하지 마십시오.

S3 객체 잠금을 사용한 크로스 그리드 복제

다음과 같은 상황에서 S3 Object Lock이 활성화된 StorageGRID 버킷 간의 크로스 그리드 복제를 구성할 수 있습니다.

소스 버킷의 **S3 Object Lock**이 설정된 경우…	대상 버킷에 대한 **S3** 객체 잠금은 다음과 같습니다…
활성화됨	활성화됨
비활성화됨	활성화됨

소스 버킷에 S3 객체 잠금이 활성화된 경우:

- 대상 위치에서 객체는 다음 순서대로 보존 설정에 따라 잠깁니다.
  a. 소스 객체의 보존 헤더 값:

     `x-amz-object-lock-mode`

```
x-amz-object-lock-retain-until-date
```

b. 소스 버킷의 기본 보존 기간(설정된 경우).

c. 대상 버킷의 기본 보존 기간(설정된 경우).

대상 버킷의 기본 보존 기간은 소스 객체에서 복제된 보존 설정을 재정의하지 않습니다.

- `x-amz-object-lock-legal-hold`을 사용하여 객체를 업로드할 때 대상 객체에 대한 법적 보존 상태를 설정할 수 있습니다.
- 대상 테넌트 또는 버킷이 소스 객체의 S3 객체 잠금 설정을 지원하지 않으면 오류가 발생합니다. 다음을 참조하십시오. "그리드 간 복제 경고 및 오류."

소스 버킷의 S3 객체 잠금이 비활성화된 경우:

- 대상 버킷의 기본 보존 기간을 구성하여 S3 객체 잠금 보존 설정을 대상 객체에 적용할 수 있습니다.
- 대상 객체는 법적 보존 상태를 설정할 수 없습니다.

PutObjectTagging 및 **DeleteObjectTagging**은 지원되지 않습니다.

PutObjectTagging 및 DeleteObjectTagging 요청은 크로스 그리드 복제가 활성화된 버킷의 객체에 대해 지원되지 않습니다.

S3 클라이언트가 PutObjectTagging 또는 DeleteObjectTagging 요청을 보내면, `501 Not Implemented`이 반환됩니다. 메시지는 `Put(Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured`입니다.

PutObjectRetention 및 **PutObjectLegalHold**는 지원되지 않습니다

PutObjectRetention 및 PutObjectLegalHold 요청은 크로스 그리드 복제가 활성화된 버킷의 객체에 대해서는 완벽하게 지원되지 않습니다.

S3 클라이언트가 PutObjectRetention 또는 PutObjectLegalHold 요청을 보내면 소스 객체의 설정은 수정되지만, 변경 사항은 대상 객체에 적용되지 않습니다.

분할된 객체가 복제되는 방법

원본 그리드의 최대 세그먼트 크기는 대상 그리드로 복제되는 객체에 적용됩니다. 객체를 다른 그리드로 복제할 때 원본 그리드의 최대 세그먼트 크기 설정(구성 > 시스템 > 저장소 옵션)이 두 그리드 모두에 사용됩니다. 예를 들어 원본 그리드의 최대 세그먼트 크기가 1GB이고 대상 그리드의 최대 세그먼트 크기가 50MB라고 가정해 보겠습니다. 원본 그리드에 2GB 크기의 객체를 가져오면 해당 객체는 1GB 세그먼트 두 개로 저장됩니다. 대상 그리드의 최대 세그먼트 크기가 50MB이더라도 해당 객체는 1GB 세그먼트 두 개로 대상 그리드에도 복제됩니다.

StorageGRID에서 교차 그리드 복제와 **CloudMirror** 복제 비교

그리드 페더레이션을 사용하기 시작할 때 "교차 그리드 복제"와 "StorageGRID CloudMirror 복제 서비스"의 유사점과 차이점을 검토하십시오.

CloudMirror를 크로스 그리드 복제로 복제된 버킷에서는 사용할 수 없으며, 그 반대의 경우도 마찬가지입니다.

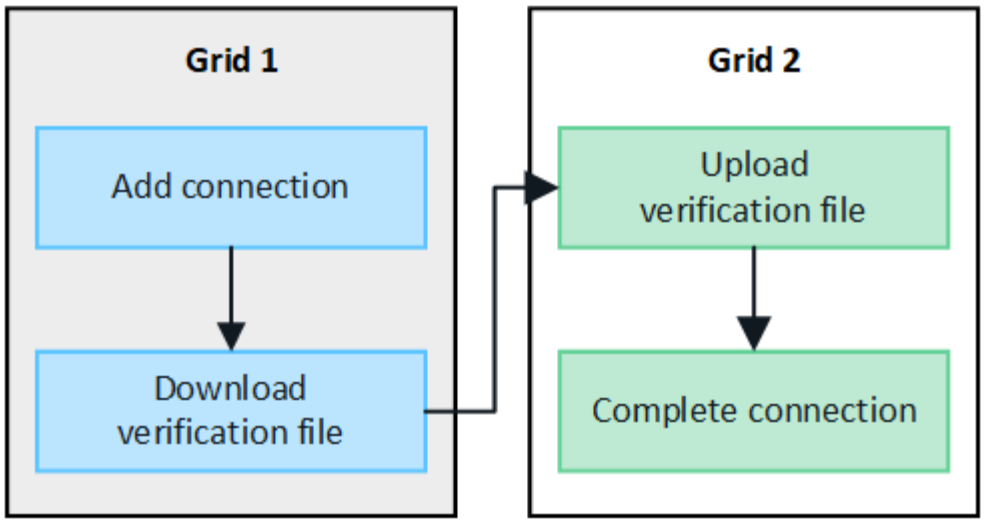
	교차 그리드 복제	**CloudMirror** 복제 서비스
주된 목적은 무엇입니까?	하나의 StorageGRID 시스템이 재해 복구 시스템 역할을 합니다. 버킷의 객체는 그리드 간에 단방향 또는 양방향으로 복제될 수 있습니다.	테넌트가 StorageGRID(원본)의 버킷에서 외부 S3 버킷(대상)으로 객체를 자동으로 복제할 수 있도록 합니다. CloudMirror 복제는 독립적인 S3 인프라에 객체의 독립적인 복사본을 생성합니다. 이 독립적인 복사본은 백업 용도로 사용되지는 않지만, 클라우드에서 추가적인 처리가 이루어지는 경우가 많습니다.
어떻게 구성되어 있나요?	1. 두 그리드 간의 그리드 페더레이션 연결을 구성합니다. 2. 새로운 테넌트 계정을 추가하면 해당 계정이 자동으로 다른 그리드로 복제됩니다. 3. 새로운 테넌트 그룹과 사용자를 추가하면 해당 그룹과 사용자도 복제됩니다. 4. 각 그리드에 해당하는 버킷을 생성하고, 그리드 간 복제가 한 방향 또는 양방향으로 발생하도록 설정합니다.	1. 테넌트 사용자는 테넌트 관리자 또는 S3 API를 사용하여 CloudMirror 엔드포인트(IP 주소, 자격 증명 등)를 정의함으로써 CloudMirror 복제를 구성합니다. 2. 해당 테넌트 계정이 소유한 모든 버킷은 CloudMirror 엔드포인트를 가리키도록 구성할 수 있습니다.
누가 설치를 담당하나요?	• 그리드 관리자는 연결 및 테넌트를 구성합니다. • 테넌트 사용자는 그룹, 사용자, 키 및 버킷을 구성합니다.	일반적으로 테넌트 사용자입니다.
목적지는 어디인가요?	그리드 페더레이션 연결의 다른 StorageGRID 시스템에 있는 대응하는 동일한 S3 버킷입니다.	• 호환되는 모든 S3 인프라(Amazon S3 포함). • Google Cloud Platform (GCP)
객체 버전 관리가 필요합니까?	예, 소스 버킷과 대상 버킷 모두 객체 버전 관리가 활성화되어 있어야 합니다.	아니요, CloudMirror 복제는 소스 및 대상 모두에서 버전 관리되지 않는 버킷과 버전 관리되는 버킷을 어떤 조합으로든 지원합니다.
오브젝트가 대상으로 이동되는 원인은 무엇입니까?	크로스 그리드 복제가 활성화된 버킷에 객체가 추가되면 자동으로 복제됩니다.	CloudMirror 엔드포인트가 구성된 버킷에 객체가 추가되면 자동으로 복제됩니다. CloudMirror 엔드포인트가 구성되기 전에 소스 버킷에 존재했던 객체는 수정되지 않는 한 복제되지 않습니다.
객체는 어떻게 복제됩니까?	크로스 그리드 복제는 버전이 지정된 객체를 생성하고 소스 버킷의 버전 ID를 대상 버킷으로 복제합니다. 이를 통해 두 그리드 모두에서 버전 순서를 유지할 수 있습니다.	CloudMirror 복제는 버전 관리가 활성화된 버킷을 필요로 하지 않으므로, CloudMirror는 동일한 사이트 내에서만 키의 순서를 유지할 수 있습니다. 다른 사이트에 있는 객체에 대한 요청의 순서가 유지된다는 보장은 없습니다.

	교차 그리드 복제	**CloudMirror** 복제 서비스
객체를 복제할 수 없는 경우 어떻게 됩니까?	해당 객체는 메타데이터 저장 용량 제한에 따라 복제 대기열에 추가됩니다.	해당 객체는 플랫폼 서비스 제한에 따라 복제 대기열에 추가됩니다("플랫폼 서비스 이용 관련 권장 사항" 참조).
해당 객체의 시스템 메타데이터가 복제되었습니까?	예, 객체가 다른 그리드로 복제될 때 해당 객체의 시스템 메타데이터도 함께 복제됩니다. 메타데이터는 두 그리드에서 동일합니다.	아니요, 객체가 외부 버킷으로 복제될 때 시스템 메타데이터가 업데이트됩니다. 메타데이터는 수집 시점과 각 S3 인프라의 동작 방식에 따라 위치별로 다릅니다.
객체는 어떻게 검색됩니까?	애플리케이션은 두 그리드 중 하나의 버킷에 요청을 보내 객체를 검색하거나 읽을 수 있습니다.	애플리케이션은 StorageGRID 또는 S3 대상에 요청을 보내 객체를 검색하거나 읽을 수 있습니다. 예를 들어, CloudMirror 복제를 사용하여 파트너 조직에 객체를 미러링한다고 가정해 보겠습니다. 파트너는 자체 애플리케이션을 사용하여 S3 대상에서 직접 객체를 읽거나 업데이트할 수 있습니다. StorageGRID는 필요하지 않습니다.
객체가 삭제되면 어떻게 되나요?	• 버전 ID가 포함된 삭제 요청은 대상 그리드로 복제되지 않습니다. • 버전 ID가 포함되지 않은 삭제 요청은 소스 버킷에 삭제 마커를 추가하며, 이 마커는 선택적으로 대상 그리드로 복제될 수 있습니다. • 교차 그리드 복제가 단방향으로만 구성된 경우 대상 버킷의 객체를 삭제해도 소스에는 영향을 미치지 않습니다.	결과는 소스 및 대상 버킷의 버전 관리 상태에 따라 달라집니다(두 버킷의 버전 관리 상태가 같을 필요는 없습니다). • 두 버킷 모두 버전 관리가 되어 있는 경우, 삭제 요청 시 두 위치 모두에 삭제 표시가 추가됩니다. • 원본 버킷에만 버전 관리가 적용된 경우, 삭제 요청 시 원본 버킷에는 삭제 마커가 추가되지만 대상 버킷에는 추가되지 않습니다. • 두 버킷 모두 버전 관리가 되어 있지 않으면 삭제 요청 시 소스 버킷에서는 객체가 삭제되지만 대상 버킷에서는 삭제되지 않습니다. 마찬가지로 대상 버킷의 객체를 삭제해도 소스 버킷에는 영향을 미치지 않습니다.

StorageGRID 그리드 페더레이션 연결을 생성합니다

테넌트 세부 정보를 복제하고 오브젝트 데이터를 복제하려면 두 StorageGRID 시스템 간에 그리드 페더레이션 연결을 생성할 수 있습니다.

그림에서 보는 것처럼 그리드 연합 연결을 생성하는 과정은 두 그리드 모두에서 단계를 거칩니다. 한 그리드에서 연결을 추가하고 다른 그리드에서 완료합니다. 어느 그리드에서든 시작할 수 있습니다.



시작하기 전에

- 그리드 페더레이션 연결 구성에 대한 "고려사항 및 요구사항"을 검토하셨습니다.
- IP 주소나 VIP 주소 대신 각 그리드에 대해 정규화된 도메인 이름(FQDN)을 사용할 계획이라면, 사용할 이름을 알고 있어야 하며 각 그리드의 DNS 서버에 적절한 항목이 있는지 확인해야 합니다.
- 귀하는 "지원되는 웹 브라우저"을(를) 사용하고 있습니다.
- 두 그리드 모두에 대한 루트 액세스 권한과 프로비저닝 암호가 있습니다.

연결 추가

다음 단계는 두 StorageGRID 시스템 중 하나에서 수행하십시오.

단계

1. 각 그리드의 기본 관리자 노드에서 Grid Manager에 로그인하십시오.
2. 구성 > 시스템 > *그리드 페더레이션*을 선택합니다.
3. *연결 추가*를 선택합니다.
4. 연결에 필요한 세부 정보를 입력하세요.

필드	설명
연결 이름	예를 들어 "Grid 1-Grid 2"와 같이 이 연결을 쉽게 알아볼 수 있도록 고유한 이름을 지정하세요.
이 그리드의 FQDN 또는 IP 주소	다음 중 하나: • 현재 로그인한 그리드의 FQDN • 이 그리드에서 HA 그룹의 VIP 주소입니다. • 이 그리드의 관리 노드 또는 게이트웨이 노드의 IP 주소입니다. 해당 IP 주소는 대상 그리드가 연결할 수 있는 모든 네트워크에 속할 수 있습니다.

필드	설명
포트	이 연결에 사용할 포트입니다. 23000에서 23999 사이의 사용되지 않는 포트 번호를 입력할 수 있습니다. 이 연결에 사용되는 두 그리드는 동일한 포트를 사용합니다. 따라서 두 그리드의 어떤 노드도 이 포트를 다른 연결에 사용하지 않도록 해야 합니다.
이 그리드에 대한 인증서 유효 일수	이 그리드 연결에 사용할 보안 인증서의 유효 기간을 일수로 지정합니다. 기본값은 730일(2년)이지만 1일부터 762일까지의 값을 입력할 수 있습니다. StorageGRID 연결을 저장할 때 각 그리드에 대한 클라이언트 및 서버 인증서를 자동으로 생성합니다.
이 그리드에 대한 프로비저닝 암호문	현재 로그인한 그리드의 프로비저닝 암호입니다.
다른 그리드의 FQDN 또는 IP 주소	다음 중 하나: • 연결하려는 그리드의 FQDN(정규화된 도메인 이름) • 다른 그리드에 있는 HA 그룹의 VIP 주소 • 다른 그리드에 있는 관리 노드 또는 게이트웨이 노드의 IP 주소입니다. 이 IP 주소는 소스 그리드가 연결할 수 있는 모든 네트워크에 속할 수 있습니다.

5. *저장 후 계속*을 선택합니다.
6. 다운로드 확인 파일 단계에서 *다운로드 확인 파일*을 선택합니다.

   다른 그리드와의 연결이 완료되면 더 이상 어느 그리드에서도 검증 파일을 다운로드할 수 없습니다.

7. 다운로드한 파일을 찾아서 (*connection-name*`.grid-federation` 안전한 곳에 저장하십시오.

   이 파일에는 비밀 정보(마스킹됨 *****) 및 기타 민감한 세부 정보가 포함되어 있으므로 안전하게 저장하고 전송해야 합니다.

8. 그리드 연합 페이지로 돌아가려면 *닫기*를 선택합니다.
9. 새 연결이 표시되고 *연결 상태*가 *연결 대기 중*인지 확인하십시오.
10. 다른 그리드의 그리드 관리자에게 *connection-name*`.grid-federation` 파일을 제공하세요.

연결 완료

연결하려는 StorageGRID 시스템(다른 그리드)에서 다음 단계를 수행하십시오.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인하십시오.
2. 구성 > 시스템 > *그리드 페더레이션*을 선택합니다.

3. *인증 파일 업로드*를 선택하여 업로드 페이지에 액세스합니다.
4. *인증 파일 업로드*를 선택하세요. 그런 다음, 첫 번째 그리드에서 다운로드한 파일을 찾아 선택하세요 ((*connection-name*.grid-federation).

   연결에 대한 세부 정보가 표시됩니다.

5. 선택적으로, 이 그리드에 대한 보안 인증서의 유효 일수를 다르게 입력할 수 있습니다. 인증서 유효 일수 항목은 첫 번째 그리드에 입력한 값으로 기본 설정되지만, 각 그리드마다 다른 만료일을 사용할 수 있습니다.

   일반적으로 연결 양쪽의 인증서 유효 기간은 동일하게 설정하십시오.

   > 연결 양쪽 끝의 인증서가 만료되면 연결이 중단되고 인증서가 업데이트될 때까지 복제 작업이 보류됩니다.

6. 현재 로그인한 그리드의 프로비저닝 암호를 입력하십시오.
7. *저장 후 테스트*를 선택합니다.

   인증서가 생성되고 연결이 테스트됩니다. 연결이 유효하면 성공 메시지가 표시되고 새 연결이 그리드 연합 페이지에 나열됩니다. *연결 상태*는 *연결됨*입니다.

   오류 메시지가 나타나면 문제를 해결하십시오. "그리드 페더레이션 오류 해결"을 참조하십시오.

8. 첫 번째 그리드의 그리드 연합 페이지로 이동하여 브라우저를 새로 고침하세요. *연결 상태*가 *연결됨*으로 표시되는지 확인하세요.
9. 연결이 설정되면 검증 파일의 모든 사본을 안전하게 삭제하십시오.

   이 연결을 수정하면 새 검증 파일이 생성됩니다. 기존 파일은 재사용할 수 없습니다.

완료한 후

- "허용된 테넌트 관리"에 대한 고려 사항을 검토하십시오.
- "하나 이상의 새 테넌트 계정 생성", 그리드 페더레이션 연결 사용 권한을 할당하고 새 연결을 선택합니다.
- "연결 관리" 필요에 따라. 연결 값을 편집하거나, 연결을 테스트하거나, 연결 인증서를 교체하거나, 연결을 제거할 수 있습니다.
- "연결 모니터링" 일반적인 StorageGRID 모니터링 활동의 일부로 수행합니다.
- "연결 문제 해결"여기에는 계정 복제 및 그리드 간 복제와 관련된 모든 경고 및 오류 해결이 포함됩니다.

StorageGRID 그리드 페더레이션 연결 관리

StorageGRID 시스템 간의 그리드 페더레이션 연결 관리에는 연결 세부 정보 편집, 인증서 교체, 테넌트 권한 제거 및 사용하지 않는 연결 제거가 포함됩니다.

시작하기 전에

- 현재 두 그리드 중 하나의 그리드 관리자에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 현재 로그인한 그리드에 대한 "루트 액세스 권한"이(가) 있습니다.

그리드 페더레이션 연결 편집

그리드 연합 연결을 편집하려면 연결된 두 그리드 중 하나의 기본 관리자 노드에 로그인하세요. 첫 번째 그리드를 변경한 후에는 새 검증 파일을 다운로드하여 다른 그리드에 업로드해야 합니다.

> 연결 설정을 편집하는 동안 계정 복제 또는 그리드 간 복제 요청은 기존 연결 설정을 계속 사용합니다. 첫 번째 그리드에 대한 모든 편집 내용은 로컬에 저장되지만, 두 번째 그리드에 업로드되어 저장 및 테스트될 때까지는 적용되지 않습니다.

연결 편집 시작

단계

1. 각 그리드의 기본 관리자 노드에서 Grid Manager에 로그인하십시오.
2. *노드*를 선택하고 시스템의 다른 모든 관리 노드가 온라인 상태인지 확인하십시오.

   > 그리드 연합 연결을 편집할 때 StorageGRID는 첫 번째 그리드의 모든 관리 노드에 "후보 구성" 파일을 저장하려고 시도합니다. 이 파일을 모든 관리 노드에 저장할 수 없는 경우, *저장 후 테스트*를 선택하면 경고 메시지가 나타납니다.

3. 구성 > 시스템 > *그리드 페더레이션*을 선택합니다.
4. 그리드 연합 페이지 또는 특정 연결의 세부 정보 페이지에서 작업 메뉴를 사용하여 연결 세부 정보를 편집하세요. 입력할 내용은 "그리드 페더레이션 연결 생성"을 참조하세요.

   작업 메뉴

   a. 연결에 대한 라디오 버튼을 선택합니다.
   b. 작업 * > * 편집 *을 선택합니다.
   c. 새 정보를 입력합니다.

   상세 정보 페이지

   a. 연결 이름을 선택하여 세부 정보를 표시합니다.
   b. *편집*을 선택합니다.
   c. 새 정보를 입력합니다.

5. 로그인한 그리드의 프로비저닝 암호를 입력하십시오.
6. *저장 후 계속*을 선택합니다.

   새로운 값은 저장되지만, 다른 그리드에 새 검증 파일을 업로드하기 전까지는 연결에 적용되지 않습니다.

7. *검증 파일 다운로드*를 선택합니다.

   나중에 이 파일을 다운로드하려면 연결 세부 정보 페이지로 이동하세요.

8. 다운로드한 파일을 찾아서 (*`connection-name`*`.grid-federation` 안전한 곳에 저장하십시오.

   > 검증 파일에는 비밀 정보가 포함되어 있으므로 안전하게 저장하고 전송해야 합니다.

9. 그리드 연합 페이지로 돌아가려면 *닫기*를 선택합니다.
10. *연결 상태*가 *편집 대기 중*인지 확인하십시오.

    연결 편집을 시작할 때 연결 상태가 *연결됨*이 아닌 경우, *편집 대기 중*으로 변경되지 않습니다.

11. 다른 그리드의 그리드 관리자에게 *connection-name*.grid-federation 파일을 제공하세요.

연결 편집 완료

다른 그리드에 검증 파일을 업로드하여 연결 편집을 완료하세요.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인하십시오.
2. 구성 > 시스템 > *그리드 페더레이션*을 선택합니다.
3. *인증 파일 업로드*를 선택하여 업로드 페이지로 이동하세요.
4. *인증 파일 업로드*를 선택합니다. 그런 다음, 첫 번째 그리드에서 다운로드한 파일을 찾아 선택합니다.
5. 현재 로그인한 그리드의 프로비저닝 암호를 입력하십시오.
6. *저장 후 테스트*를 선택합니다.

   수정된 값을 사용하여 연결이 설정되면 성공 메시지가 표시됩니다. 그렇지 않으면 오류 메시지가 표시됩니다. 메시지를 검토하고 문제를 해결하십시오.

7. 마법사를 닫고 그리드 연합 페이지로 돌아가십시오.
8. *연결 상태*가 *연결됨*인지 확인하십시오.
9. 첫 번째 그리드의 그리드 연합 페이지로 이동하여 브라우저를 새로 고침하세요. *연결 상태*가 *연결됨*으로 표시되는지 확인하세요.
10. 연결이 설정되면 검증 파일의 모든 사본을 안전하게 삭제하십시오.

그리드 페더레이션 연결을 테스트합니다.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인하십시오.
2. 구성 > 시스템 > *그리드 페더레이션*을 선택합니다.
3. 그리드 연합 페이지 또는 특정 연결의 세부 정보 페이지에서 작업 메뉴를 사용하여 연결을 테스트하십시오.

   작업 메뉴

   a. 연결에 대한 라디오 버튼을 선택합니다.
   b. 작업 > *테스트*를 선택합니다.

   상세 정보 페이지

   a. 연결 이름을 선택하여 세부 정보를 표시합니다.
   b. *연결 테스트*를 선택합니다.

4. 연결 상태를 검토합니다.

연결 상태	설명
연결됨	두 그리드가 연결되어 정상적으로 통신하고 있습니다.
오류	연결이 오류 상태입니다. 예를 들어 인증서가 만료되었거나 구성 값이 더 이상 유효하지 않습니다.
편집 대기 중	이 그리드에서 연결을 편집했지만, 연결은 여전히 기존 구성을 사용하고 있습니다. 편집을 완료하려면 새 검증 파일을 다른 그리드에 업로드하십시오.
연결 대기 중	이 그리드에서는 연결을 구성했지만, 다른 그리드에서는 연결이 완료되지 않았습니다. 이 그리드에서 검증 파일을 다운로드하여 다른 그리드에 업로드하십시오.
알 수 없음	연결 상태를 알 수 없습니다. 네트워크 문제 또는 오프라인 노드 때문일 수 있습니다.

5. 연결 상태가 *오류*로 표시되면 문제를 해결하세요. 그런 다음 *연결 테스트*를 다시 선택하여 문제가 해결되었는지 확인하십시오.

연결 인증서 교체

각 그리드 연합 연결은 연결을 보호하기 위해 자동으로 생성된 4개의 SSL 인증서를 사용합니다. 각 그리드에 사용되는 두 개의 인증서 만료일이 가까워지면 그리드 연합 인증서 만료 알림이 표시되어 인증서를 교체해야 함을 알려줍니다.

> 연결 양쪽 끝의 인증서가 만료되면 연결이 중단되고 인증서가 업데이트될 때까지 복제 작업이 보류됩니다.

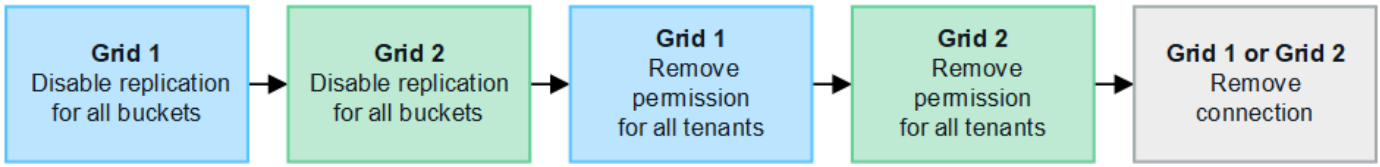
단계

1. 각 그리드의 기본 관리자 노드에서 Grid Manager에 로그인하십시오.
2. 구성 > 시스템 > *그리드 페더레이션*을 선택합니다.
3. 그리드 연합 페이지의 어느 탭에서든 연결 이름을 선택하면 세부 정보가 표시됩니다.
4. 인증서 탭을 선택합니다.
5. *인증서 순환*을 선택합니다.
6. 새 인증서의 유효 기간을 일 단위로 지정하십시오.
7. 로그인한 그리드의 프로비저닝 암호를 입력하십시오.
8. *인증서 순환*을 선택합니다.
9. 필요에 따라 연결된 다른 그리드에서도 이 단계를 반복하십시오.

   일반적으로 연결 양쪽의 인증서 유효 기간은 동일하게 설정하십시오.

그리드 페더레이션 연결 제거

그리드 페더레이션 연결은 연결된 두 그리드 중 어느 한쪽에서든 제거할 수 있습니다. 그림에서 보는 것처럼, 두 그리드 모두에서 사전 준비 단계를 수행하여 해당 연결이 어느 그리드의 테넌트에서도 사용되지 않는지 확인해야 합니다.



연결을 제거하기 전에 다음 사항에 유의하십시오.

- 연결을 제거해도 그리드 간에 이미 복사된 항목은 삭제되지 않습니다. 예를 들어, 두 그리드 모두에 존재하는 테넌트 사용자, 그룹 및 개체는 테넌트의 권한이 제거되더라도 어느 그리드에서도 삭제되지 않습니다. 이러한 항목을 삭제하려면 두 그리드에서 수동으로 삭제해야 합니다.
- 연결을 제거하면 복제 대기 중인 개체(수집되었지만 아직 다른 그리드로 복제되지 않은 개체)의 복제가 영구적으로 실패하게 됩니다.

모든 테넌트 버킷에 대한 복제 비활성화

단계

1. 어느 그리드에서든 시작하여 기본 관리자 노드에서 그리드 관리자에 로그인하십시오.
2. 구성 > 시스템 > *그리드 페더레이션*을 선택합니다.
3. 연결 이름을 선택하면 세부 정보가 표시됩니다.
4. 허용된 테넌트 탭에서 해당 연결이 현재 사용 중인 테넌트가 있는지 확인하십시오.
5. 테넌트가 목록에 있는 경우, 모든 테넌트에게 "그리드 간 복제 비활성화" 연결의 두 그리드 모두에서 자신의 모든 버킷에 대해 설정을 변경하도록 지시하십시오.

> 테넌트 버킷 중 하나라도 그리드 간 복제가 활성화된 경우 그리드 페더레이션 연결 사용 권한을 제거할 수 없습니다. 각 테넌트 계정은 두 그리드 모두에서 해당 버킷에 대한 그리드 간 복제를 비활성화해야 합니다.

각 테넌트에 대한 권한 제거

모든 테넌트 버킷에 대해 그리드 간 복제를 비활성화한 후, 양쪽 그리드의 모든 테넌트에서 *그리드 페더레이션 사용 권한*을 제거하십시오.

단계

1. 구성 > 시스템 > *그리드 페더레이션*을 선택합니다.
2. 연결 이름을 선택하면 세부 정보가 표시됩니다.
3. 허용된 테넌트 탭에서 각 테넌트에 대해 그리드 페더레이션 연결 사용 권한을 제거합니다. "허용된 테넌트 관리"을 참조하십시오.
4. 다른 그리드에 있는 허용된 테넌트에 대해서도 이 단계를 반복하십시오.

연결 제거

단계

1. 두 그리드 모두에서 연결을 사용하는 테넌트가 없는 경우 *제거*를 선택하십시오.
2. 확인 메시지를 검토한 후 *제거*를 선택합니다.
   - 연결을 제거할 수 있으면 성공 메시지가 표시됩니다. 이제 두 그리드 모두에서 그리드 페더레이션 연결이 제거되었습니다.
   - 연결을 제거할 수 없는 경우(예: 연결이 여전히 사용 중이거나 연결 오류가 발생한 경우) 오류 메시지가 표시됩니다. 다음 두 가지 방법 중 하나를 수행할 수 있습니다.
     - 오류를 해결하세요(권장). "그리드 페더레이션 오류 해결"을 참조하십시오.
     - 연결을 강제로 제거하십시오. 다음 섹션을 참조하십시오.

그리드 페더레이션 연결을 강제로 제거합니다.

필요한 경우, 연결됨 상태가 아닌 연결을 강제로 제거할 수 있습니다.

강제 제거는 로컬 그리드에서만 연결을 삭제합니다. 연결을 완전히 제거하려면 양쪽 그리드에서 동일한 단계를 수행하십시오.

단계

1. 확인 대화 상자에서 *강제 제거*를 선택합니다.

   성공 메시지가 표시됩니다. 이 그리드 페더레이션 연결은 더 이상 사용할 수 없습니다. 그러나 테넌트 버킷에 그리드 간 복제가 여전히 활성화되어 있을 수 있으며, 연결된 그리드 간에 일부 객체 복사본이 이미 복제되었을 수 있습니다.

2. 연결된 다른 그리드에서 기본 관리 노드를 통해 그리드 관리자에 로그인하십시오.
3. 구성 > 시스템 > *그리드 페더레이션*을 선택합니다.
4. 연결 이름을 선택하면 세부 정보가 표시됩니다.
5. 제거 및 *예*를 선택합니다.
6. 이 그리드에서 연결을 제거하려면 *강제 제거*를 선택하십시오.

StorageGRID 그리드 페더레이션에 허용된 테넌트를 관리합니다.

S3 테넌트 계정이 두 StorageGRID 시스템 간의 그리드 페더레이션 연결을 사용하도록 허용할 수 있습니다. 테넌트가 연결을 사용하도록 허용된 경우, 테넌트 세부 정보를 수정하거나 테넌트의 연결 사용 권한을 영구적으로 제거하려면 특별한 조치가 필요합니다.

시작하기 전에

- 현재 두 그리드 중 하나의 그리드 관리자에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 현재 로그인한 그리드에 대한 "루트 액세스 권한"이(가) 있습니다.
- 두 개의 그리드 사이에 "그리드 페더레이션 연결을 생성했습니다."이(가) 있습니다.
- "계정 복제" 및 "교차 그리드 복제"에 대한 워크플로를 검토하셨습니다.
- 필요에 따라 연결된 두 그리드 모두에 대해 단일 로그인(SSO) 또는 ID 페더레이션을 이미 구성했습니다. "계정 복제란 무엇인가요?"을 참조하십시오.

허가된 테넌트 생성

새 테넌트 계정 또는 기존 테넌트 계정이 계정 복제 및 그리드 간 복제를 위해 그리드 페더레이션 연결을 사용하도록 허용하려면 "새 S3 테넌트 생성" 또는 "테넌트 계정 수정"에 대한 일반 지침을 따르고 다음 사항에 유의하십시오.

- 테넌트 연결의 어느 그리드에서든 테넌트를 생성할 수 있습니다. 테넌트가 생성되는 그리드가 바로 _테넌트의 소스 그리드_입니다.
- 연결 상태는 *연결됨*이어야 합니다.
- 테넌트를 생성하거나 편집하여 그리드 페더레이션 연결 사용 권한을 활성화한 후 첫 번째 그리드에 저장하면 동일한 테넌트가 다른 그리드로 자동으로 복제됩니다. 테넌트가 복제되는 그리드를 해당 테넌트의 대상 그리드라고 합니다.
- 두 그리드의 테넌트는 동일한 20자리 계정 ID, 이름, 설명, 할당량 및 권한을 갖습니다. 선택적으로 설명 필드를 사용하여 소스 테넌트와 대상 테넌트를 구분할 수 있습니다. 예를 들어, Grid 1에서 생성된 테넌트에 대한 다음 설명은 Grid 2로 복제된 테넌트에도 표시됩니다. "이 테넌트는 Grid 1에서 생성되었습니다."
- 보안상의 이유로 로컬 루트 사용자의 암호는 대상 그리드로 복사되지 않습니다.

> 로컬 루트 사용자가 대상 그리드의 복제된 테넌트에 로그인하려면 먼저 해당 그리드의 그리드 관리자가 "로컬 루트 사용자의 암호 변경"해야 합니다.

- 새 테넌트 또는 수정된 테넌트가 두 그리드 모두에서 사용 가능해지면 테넌트 사용자는 다음과 같은 작업을 수행할 수 있습니다.
  - 테넌트의 소스 그리드에서 그룹과 로컬 사용자를 생성하면, 이들이 자동으로 테넌트의 대상 그리드로 복제됩니다. "테넌트 그룹 및 사용자 복제"을 참조하십시오.
  - 새로운 S3 액세스 키를 생성합니다. 이 키는 선택적으로 테넌트의 대상 그리드에 복제할 수 있습니다. 을 참조하십시오."API를 사용하여 S3 액세스 키 복제"
  - 연결의 두 그리드에 동일한 버킷을 생성하고 한 방향 또는 양방향으로 그리드 간 복제를 활성화합니다. 을 참조하십시오"그리드 간 복제 관리".

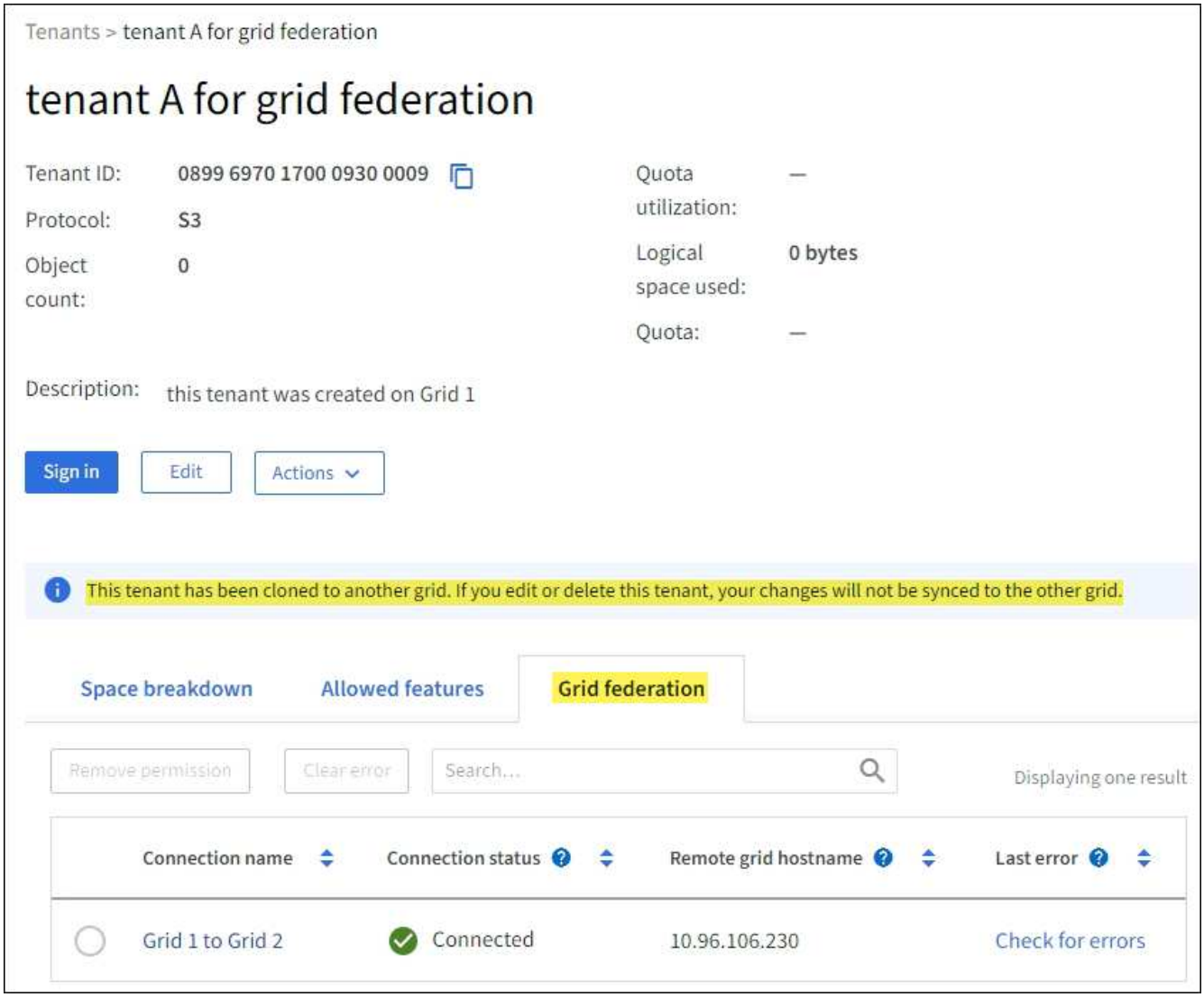
허가된 테넌트 보기

그리드 페더레이션 연결을 사용할 수 있도록 허가된 테넌트에 대한 세부 정보를 확인할 수 있습니다.

단계

1. *테넌트*를 선택합니다.
2. 테넌트 페이지에서 테넌트 이름을 선택하면 테넌트 세부 정보 페이지를 볼 수 있습니다.

   이 그리드가 테넌트의 소스 그리드인 경우(즉, 테넌트가 이 그리드에서 생성된 경우), 테넌트가 다른 그리드로 복제되었음을 알리는 배너가 표시됩니다. 이 테넌트를 편집하거나 삭제해도 변경 사항이 다른 그리드에 동기화되지 않습니다.



3. 선택적으로 **Grid federation** 탭을 선택하여 "그리드 페더레이션 연결 모니터링".

허가된 테넌트 편집

그리드 페더레이션 연결 사용 권한이 있는 테넌트를 편집해야 하는 경우, "테넌트 계정 편집"의 일반 지침을 따르고 다음 사항에 유의하십시오.

- 테넌트에 그리드 페더레이션 연결 사용 권한이 있는 경우, 연결된 두 그리드 중 어느 쪽에서든 테넌트 세부 정보를 편집할 수 있습니다. 하지만 변경 사항은 다른 그리드에 복사되지 않습니다. 그리드 간 테넌트 세부 정보를 동기화하려면 두 그리드 모두에서 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 테넌트 삭제

그리드 페더레이션 연결 사용 권한이 있는 테넌트를 제거해야 하는 경우, "테넌트 계정 삭제"에 대한 일반적인 지침을 따르고 다음 사항에 유의하십시오.

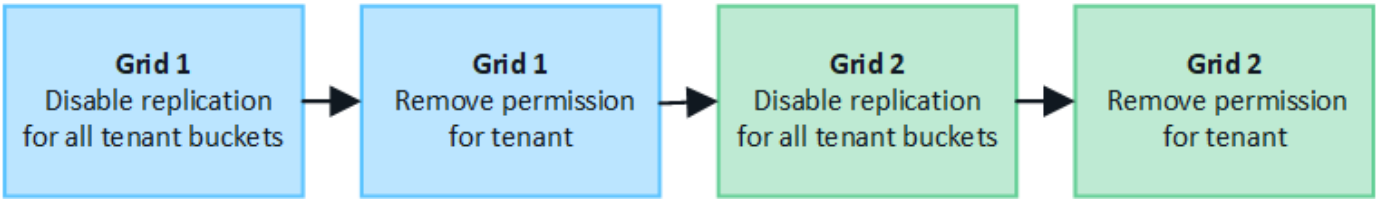
- 소스 그리드에서 원래 테넌트를 제거하려면 먼저 소스 그리드에서 해당 계정의 모든 버킷을 제거해야 합니다.

- 대상 그리드에서 복제된 테넌트를 제거하기 전에 대상 그리드에서 해당 계정의 모든 버킷을 제거해야 합니다.
- 원본 테넌트 또는 복제된 테넌트를 제거하면 해당 계정은 더 이상 그리드 간 복제에 사용할 수 없습니다.
- 원본 그리드에서 기존 테넌트를 제거하는 경우, 대상 그리드로 복제된 테넌트 그룹, 사용자 또는 키는 영향을 받지 않습니다. 복제된 테넌트를 삭제하거나, 자체적으로 그룹, 사용자, 액세스 키 및 버킷을 관리하도록 허용할 수 있습니다.
- 대상 그리드에서 복제된 테넌트를 제거하는 경우, 원본 테넌트에 새 그룹 또는 사용자가 추가되면 복제 오류가 발생합니다.

  이러한 오류를 방지하려면 이 그리드에서 테넌트를 삭제하기 전에 해당 테넌트가 그리드 페더레이션 연결을 사용할 수 있는 권한을 제거하십시오.

그리드 페더레이션 연결 권한 사용 제거

테넌트가 그리드 페더레이션 연결을 사용하지 못하도록 하려면 그리드 페더레이션 연결 사용 권한을 제거해야 합니다.



테넌트의 그리드 페더레이션 연결 사용 권한을 제거하기 전에 다음 사항에 유의하십시오.

- 테넌트의 버킷 중 하나라도 그리드 간 복제가 활성화된 경우 그리드 페더레이션 연결 사용 권한을 제거할 수 없습니다. 테넌트 계정에서 모든 버킷에 대한 그리드 간 복제를 먼저 비활성화해야 합니다.
- 그리드 페더레이션 연결 사용 권한을 제거해도 그리드 간에 이미 복제된 항목은 삭제되지 않습니다. 예를 들어, 두 그리드 모두에 존재하는 테넌트 사용자, 그룹 및 개체는 해당 테넌트의 권한이 제거되더라도 어느 그리드에서도 삭제되지 않습니다. 이러한 항목을 삭제하려면 두 그리드에서 수동으로 삭제해야 합니다.
- 동일한 그리드 페더레이션 연결을 사용하여 이 권한을 다시 활성화하려면 먼저 대상 그리드에서 해당 테넌트를 삭제해야 합니다. 그렇지 않으면 이 권한을 다시 활성화할 때 오류가 발생합니다.

> 그리드 페더레이션 연결 사용 권한을 다시 활성화하면 로컬 그리드가 소스 그리드가 되고, 선택한 그리드 페더레이션 연결에 지정된 원격 그리드로 복제가 시작됩니다. 테넌트 계정이 원격 그리드에 이미 존재하는 경우 복제 시 충돌 오류가 발생합니다.

시작하기 전에

- 귀하는 "지원되는 웹 브라우저"을(를) 사용하고 있습니다.
- 두 그리드 모두에 대한 "루트 액세스 권한"이(가) 있습니다.

테넌트 버킷에 대한 복제 비활성화

첫 번째 단계로 모든 테넌트 버킷에 대해 그리드 간 복제를 비활성화하십시오.

단계

1. 어느 그리드에서든 시작하여 기본 관리자 노드에서 그리드 관리자에 로그인하십시오.
2. 구성 > 시스템 > *그리드 페더레이션*을 선택합니다.

3. 연결 이름을 선택하면 세부 정보가 표시됩니다.
4. 허용된 테넌트 탭에서 해당 테넌트가 연결을 사용하고 있는지 확인하십시오.
5. 테넌트가 목록에 있는 경우, 연결의 두 그리드 모두에서 모든 버킷에 대해 "그리드 간 복제 비활성화"하도록 테넌트에게 지시하십시오.

테넌트 버킷 중 하나라도 그리드 간 복제가 활성화된 경우 그리드 페더레이션 연결 사용 권한을 제거할 수 없습니다. 테넌트는 양쪽 그리드 모두에서 해당 버킷의 그리드 간 복제를 비활성화해야 합니다.

테넌트에 대한 권한 제거

테넌트 버킷에 대한 그리드 간 복제를 비활성화한 후에 테넌트의 그리드 페더레이션 연결 사용 권한을 제거할 수 있습니다.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인하십시오.
2. 그리드 페더레이션 페이지 또는 테넌트 페이지에서 권한을 제거하십시오.

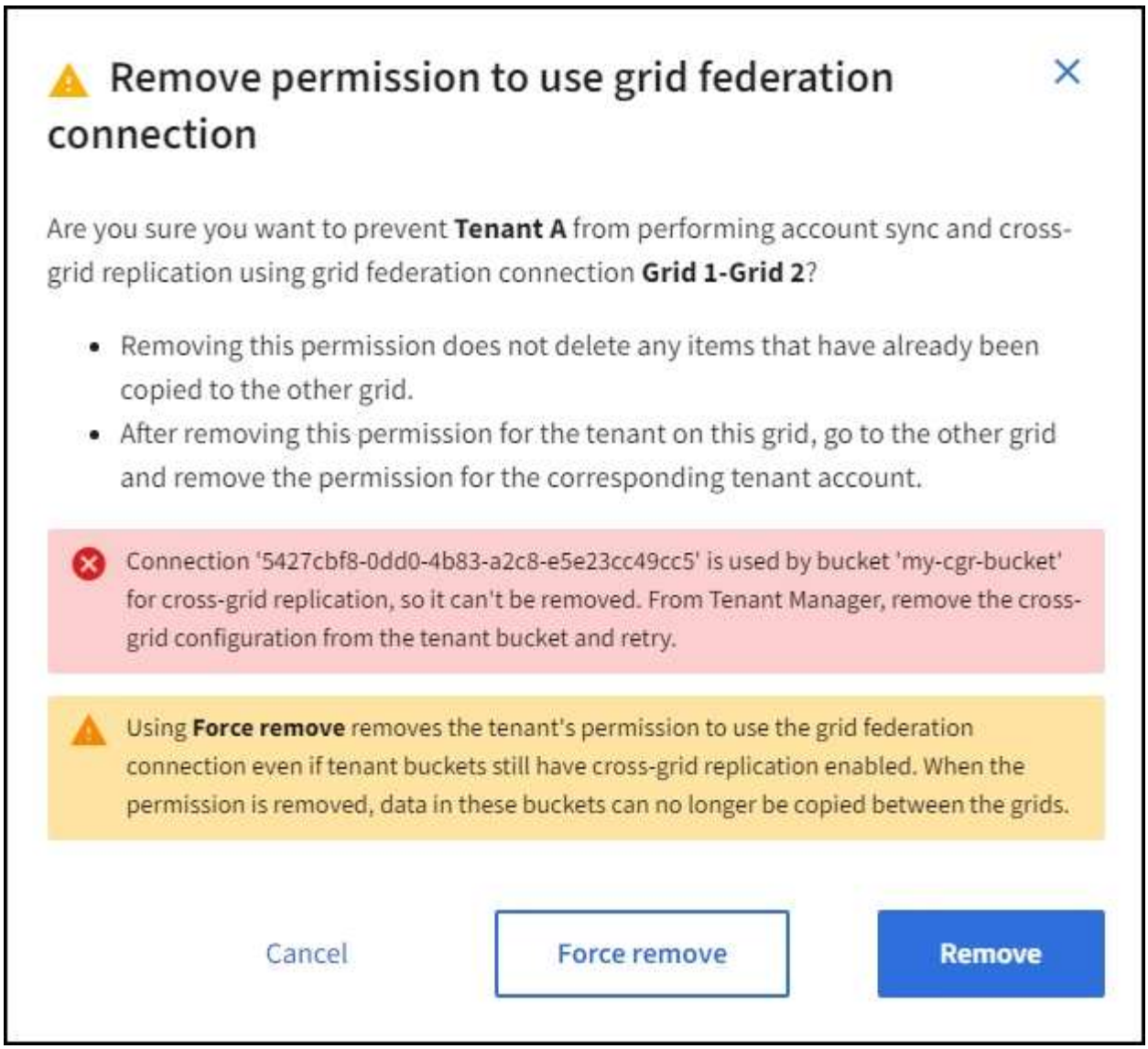
그리드 페더레이션 페이지

a. 구성 > 시스템 > *그리드 페더레이션*을 선택합니다.
b. 연결 이름을 선택하면 해당 연결의 세부 정보 페이지가 표시됩니다.
c. 허용된 테넌트 탭에서 테넌트의 라디오 버튼을 선택합니다.
d. *권한 제거*를 선택합니다.

테넌트 페이지

a. *테넌트*를 선택합니다.
b. 테넌트의 이름을 선택하면 세부 정보 페이지가 표시됩니다.
c. **Grid federation** 탭에서 연결에 대한 라디오 버튼을 선택합니다.
d. *권한 제거*를 선택합니다.

3. 확인 대화 상자에 표시된 경고를 검토하고 *제거*를 선택하십시오.
   - 권한을 제거할 수 있는 경우 세부 정보 페이지로 돌아가고 성공 메시지가 표시됩니다. 이 테넌트는 더 이상 그리드 페더레이션 연결을 사용할 수 없습니다.
   - 하나 이상의 테넌트 버킷에서 크로스 그리드 복제가 여전히 활성화된 경우 오류가 표시됩니다.



다음 두 가지 방법 중 하나를 선택할 수 있습니다.

- (권장 사항.) 테넌트 관리자에 로그인하여 각 테넌트의 버킷에 대한 복제를 비활성화하십시오. "그리드 간 복제 관리"을 참조하십시오. 그런 다음, 그리드 연결 사용 권한을 제거하는 단계를 반복하십시오.
- 권한을 강제로 제거합니다. 다음 섹션을 참조하십시오.

4. 다른 그리드로 이동하여 이 단계를 반복하고 다른 그리드에서도 동일한 테넌트에 대한 권한을 제거하십시오.

권한을 강제로 제거합니다

필요한 경우, 테넌트 버킷에 그리드 간 복제가 활성화되어 있더라도 테넌트가 그리드 페더레이션 연결을 사용할 수 있는 권한을 강제로 제거할 수 있습니다.

테넌트의 권한을 강제로 제거하기 전에 권한 제거에 대한 일반적인 고려 사항과 다음과 같은 추가 고려 사항을 참고하십시오.

- 그리드 페더레이션 연결 사용 권한을 강제로 제거하면 다른 그리드로 복제 대기 중인 객체(수집되었지만 아직 복제되지 않은 객체)는 계속 복제됩니다. 이러한 처리 중인 객체가 대상 버킷에 도달하지 않도록 하려면 다른 그리드에서도 해당 테넌트의 권한을 제거해야 합니다.

- 그리드 페더레이션 연결 사용 권한을 제거한 후 소스 버킷에 수집된 객체는 대상 버킷으로 복제되지 않습니다.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인하십시오.
2. 구성 > 시스템 > *그리드 페더레이션*을 선택합니다.
3. 연결 이름을 선택하면 해당 연결의 세부 정보 페이지가 표시됩니다.
4. 허용된 테넌트 탭에서 테넌트의 라디오 버튼을 선택합니다.
5. *권한 제거*를 선택합니다.
6. 확인 대화 상자의 경고 메시지를 검토하고 *강제 제거*를 선택하십시오.

   성공 메시지가 표시됩니다. 이 테넌트는 더 이상 그리드 페더레이션 연결을 사용할 수 없습니다.

7. 필요에 따라 다른 그리드로 이동하여 동일한 테넌트 계정에 대한 권한을 강제로 제거하려면 이 단계를 반복하십시오. 예를 들어, 처리 중인 객체가 대상 버킷에 도달하지 않도록 하려면 다른 그리드에서도 이 단계를 반복해야 합니다.

StorageGRID에서 그리드 페더레이션 오류 문제 해결

그리드 연동 연결, 계정 복제 및 그리드 간 복제와 관련된 경고 및 오류를 해결해야 할 수 있습니다.

그리드 페더레이션 연결 경고 및 오류

그리드 연합 연결과 관련하여 경고를 받거나 오류가 발생할 수 있습니다.

연결 문제를 해결하기 위해 변경 사항을 적용한 후에는 연결 상태가 *연결됨*으로 돌아왔는지 확인하기 위해 연결을 테스트하십시오. 자세한 지침은 "그리드 페더레이션 연결 관리"을 참조하십시오.

그리드 페더레이션 연결 실패 알림

문제

Grid federation connection failure 경고가 발생했습니다.

세부 정보

이 경고는 그리드 간의 그리드 페더레이션 연결이 작동하지 않음을 나타냅니다.

권장 조치

1. 두 그리드 모두에 대해 그리드 연합 페이지의 설정을 검토하십시오. 모든 값이 올바른지 확인하십시오. "그리드 페더레이션 연결 관리"을 참조하십시오.
2. 연결에 사용된 인증서를 검토하십시오. 만료된 그리드 페더레이션 인증서에 대한 경고가 없는지, 각 인증서의 세부 정보가 유효한지 확인하십시오. 연결 인증서 교체에 대한 지침은 "그리드 페더레이션 연결 관리"을 참조하십시오.
3. 양쪽 그리드의 모든 관리자 및 게이트웨이 노드가 온라인 상태이고 사용 가능한지 확인하십시오. 이러한 노드에 영향을 줄 수 있는 경고를 해결한 후 다시 시도하십시오.
4. 로컬 또는 원격 그리드에 대해 정규화된 도메인 이름(FQDN)을 제공한 경우 DNS 서버가 온라인 상태이고 사용 가능한지 확인하십시오. 네트워킹, IP 주소 및 DNS 요구 사항은 "그리드 페더레이션이란 무엇인가요?"을 참조하십시오.

그리드 페더레이션 인증서 만료 알림

문제

그리드 연동 인증서 만료 알림이 발생했습니다.

세부 정보

이 알림은 하나 이상의 그리드 연합 인증서가 곧 만료될 예정임을 나타냅니다.

권장 조치

연결 인증서를 교체하는 방법에 대한 지침은 "그리드 페더레이션 연결 관리"에서 확인하세요.

그리드 페더레이션 연결 편집 중 오류 발생

문제

그리드 연합 연결을 편집할 때 *저장 후 테스트*를 선택하면 "하나 이상의 노드에서 후보 구성 파일을 생성하는 데 실패했습니다."라는 경고 메시지가 표시됩니다.

세부 정보

그리드 연합 연결을 편집할 때 StorageGRID는 첫 번째 그리드의 모든 관리 노드에 "후보 구성" 파일을 저장하려고 시도합니다. 관리 노드가 오프라인 상태인 경우와 같이 이 파일을 모든 관리 노드에 저장할 수 없는 경우 경고 메시지가 표시됩니다.

권장 조치

1. 연결을 편집하는 데 사용하는 그리드에서 *노드*를 선택합니다.
2. 해당 그리드의 모든 관리 노드가 온라인 상태인지 확인하십시오.
3. 오프라인 상태인 노드가 있으면 해당 노드를 다시 온라인 상태로 전환한 후 연결 편집을 다시 시도하십시오.

계정 복제 오류

복제된 테넌트 계정에 로그인할 수 없습니다.

문제

복제된 테넌트 계정으로는 로그인할 수 없습니다. 테넌트 관리자 로그인 페이지에 "이 계정에 대한 자격 증명이 잘못되었습니다. 다시 시도해 주세요."

세부 정보

보안상의 이유로, 테넌트 계정을 테넌트의 소스 그리드에서 테넌트의 대상 그리드로 복제할 때, 테넌트의 로컬 루트 사용자에 대해 설정한 암호는 복제되지 않습니다. 마찬가지로, 테넌트가 소스 그리드에서 로컬 사용자를 생성할 때, 로컬 사용자 암호는 대상 그리드로 복제되지 않습니다.

권장 조치

루트 사용자가 테넌트의 대상 그리드에 로그인하려면 먼저 그리드 관리자가 대상 그리드에서 "로컬 루트 사용자의 암호 변경"해야 합니다.

복제된 로컬 사용자가 테넌트의 대상 그리드에 로그인하려면 복제된 테넌트의 루트 사용자가 대상 그리드에서 해당 사용자의 암호를 추가해야 합니다. 자세한 내용은 테넌트 관리자 사용 설명서의 "사용자 관리"을 참조하십시오.

클론 없이 테넌트가 생성되었습니다.

문제

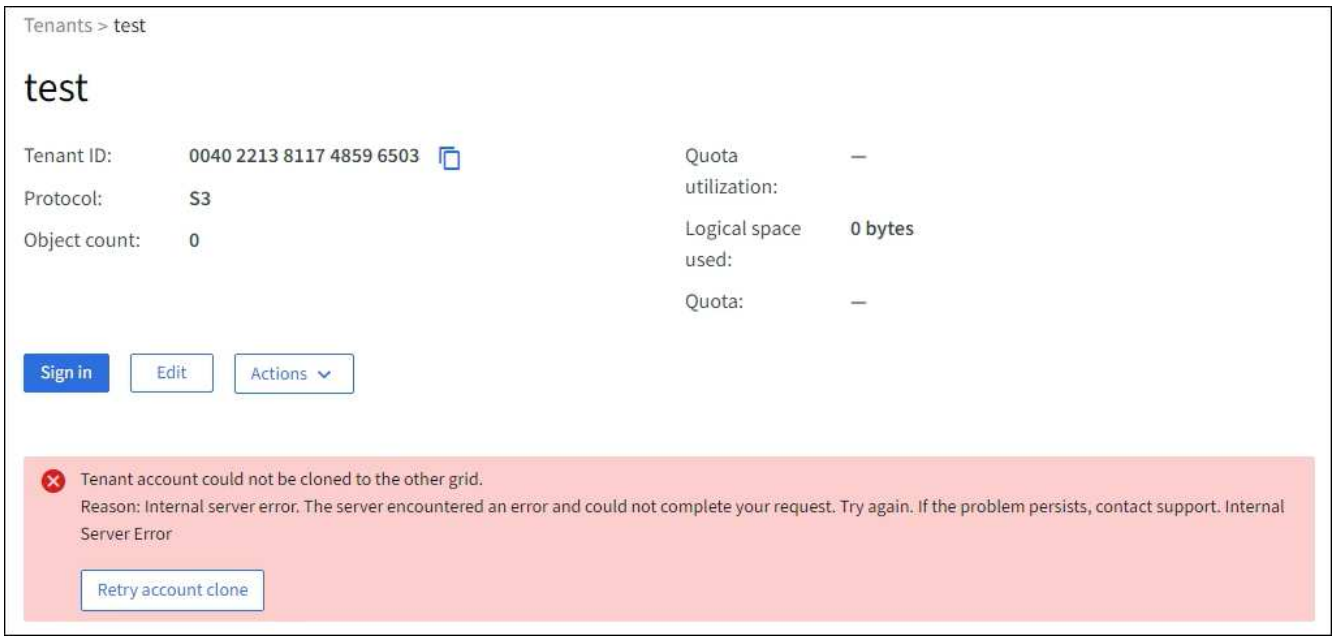
그리드 페더레이션 연결 사용 권한으로 새 테넌트를 생성한 후 "복제 없이 테넌트가 생성되었습니다"라는 메시지가 표시됩니다.

세부 정보

이 문제는 연결 상태 업데이트가 지연될 경우 발생할 수 있으며, 이로 인해 비정상적인 연결이 *연결됨*으로 표시될 수 있습니다.

권장 조치

1. 오류 메시지에 나열된 이유를 검토하고 연결이 작동하지 못하게 하는 네트워크 문제 또는 기타 문제를 해결하십시오. 을 참조하십시오.그리드 페더레이션 연결 경고 및 오류
2. 지침에 따라 "그리드 페더레이션 연결 관리"에서 그리드 연합 연결을 테스트하여 문제가 해결되었는지 확인하십시오.
3. 테넌트 소스 그리드에서 *테넌트*를 선택합니다.
4. 테넌트 복제에 실패한 테넌트 계정을 찾으십시오.
5. 테넌트 이름을 선택하여 세부 정보 페이지를 표시합니다.
6. *계정 복제 다시 시도*를 선택합니다.



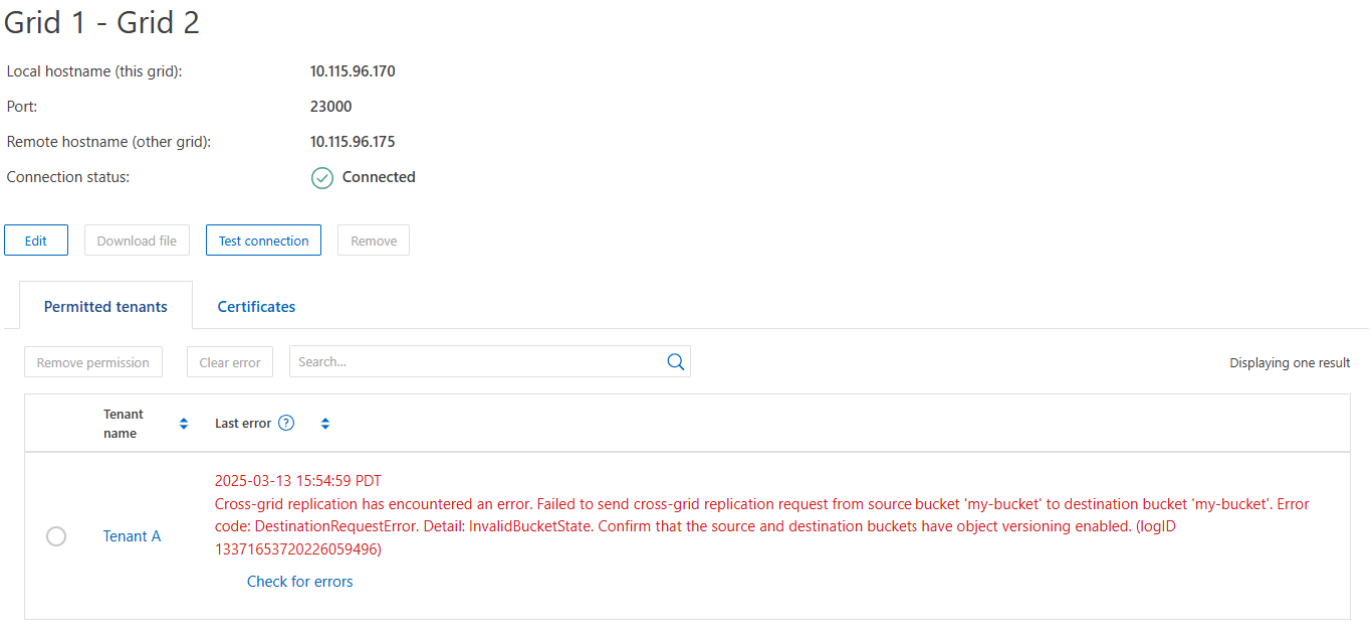
오류가 해결되면 테넌트 계정이 다른 그리드로 복제됩니다.

그리드 간 복제 경고 및 오류

연결 또는 테넌트에 대해 표시된 마지막 오류

문제

"그리드 페더레이션 연결 보기"(또는 연결에 대해 "허용된 테넌트 관리")할 때 연결 세부 정보 페이지의 마지막 오류 열에서 오류를 발견할 수 있습니다. 예를 들어:



세부 정보

각 그리드 페더레이션 연결에 대해 마지막 오류 열에는 테넌트의 데이터가 다른 그리드로 복제되는 동안 발생한 가장 최근의 오류(있는 경우)가 표시됩니다. 이 열에는 가장 최근에 발생한 그리드 간 복제 오류만 표시되며, 이전에 발생했을 수 있는 오류는 표시되지 않습니다. 이 열에 오류가 발생하는 이유는 다음과 같습니다.

- 소스 객체 버전을 찾을 수 없습니다.
- 소스 버킷을 찾을 수 없습니다.
- 대상 버킷이 삭제되었습니다.
- 대상 버킷이 다른 계정에서 다시 생성되었습니다.
- 대상 버킷의 버전 관리가 일시 중단되었습니다.
- 대상 버킷은 동일한 계정으로 다시 생성되었지만 이제 버전 관리가 되지 않습니다.
- 원본 객체의 S3 Object Lock 설정이 대상 그리드의 테넌트 수준 보존 설정과 일치하지 않습니다.
- 원본 객체에는 S3 Object Lock 설정이 있으며, 대상 버킷에서는 S3 Object Lock이 비활성화되어 있습니다.

권장 조치

마지막 오류 열에 오류 메시지가 표시되면 다음 단계를 따르십시오.

1. 메시지 내용을 검토하십시오.
2. 권장되는 조치를 수행하십시오. 예를 들어, 크로스 그리드 복제를 위해 대상 버킷에서 버전 관리가 일시 중단된 경우 해당 버킷에 대해 버전 관리를 다시 활성화하십시오.
3. 표에서 연결 또는 테넌트 계정을 선택하십시오.
4. *오류 지우기*를 선택합니다.
5. 메시지를 지우고 시스템 상태를 업데이트하려면 *예*를 선택하십시오.
6. 5~6분 정도 기다린 후 새 객체를 버킷에 수집합니다. 오류 메시지가 다시 나타나지 않는지 확인하십시오.

오류 메시지가 완전히 사라지도록 하려면 메시지에 표시된 타임스탬프 이후 최소 5분이 지난 후에 새 객체를 수집하십시오.

오류를 해결한 후에도 오류가 발생한 다른 버킷에 객체가 수집되는 경우 새로운 *최근 오류*가 나타날 수 있습니다.

7. 버킷 오류로 인해 복제에 실패한 객체가 있는지 확인하려면 "실패한 복제 작업 식별 및 재시도"을 참조하십시오.

그리드 간 복제 영구 실패 경고

문제

그리드 간 복제 영구 실패 경고가 발생했습니다.

세부 정보

이 경고는 사용자 개입이 필요한 이유로 인해 두 그리드의 버킷 간에 테넌트 객체를 복제할 수 없음을 나타냅니다. 이 경고는 일반적으로 소스 버킷 또는 대상 버킷이 변경되었을 때 발생합니다.

권장 조치

1. 알림이 발생한 그리드에 로그인합니다.
2. 구성 > 시스템 > *그리드 페더레이션*으로 이동하여 경고에 나열된 연결 이름을 찾으십시오.
3. 허용된 테넌트 탭에서 마지막 오류 열을 확인하여 오류가 있는 테넌트 계정을 확인하십시오.
4. 오류에 대한 자세한 내용은 "그리드 페더레이션 연결 모니터링"의 지침을 참조하여 그리드 간 복제 메트릭을 검토하세요.
5. 영향을 받는 각 테넌트 계정에 대해:
   a. "테넌트 활동 모니터링"의 지침을 참조하여 테넌트가 교차 그리드 복제를 위한 대상 그리드의 할당량을 초과하지 않았는지 확인하십시오.
   b. 필요에 따라 대상 그리드에서 테넌트의 할당량을 늘려 새 개체를 저장할 수 있도록 하십시오.
6. 영향을 받는 각 테넌트에 대해 두 그리드 모두에서 테넌트 관리자에 로그인하여 버킷 목록을 비교하십시오.
7. 크로스 그리드 복제가 활성화된 각 버킷에 대해 다음 사항을 확인하십시오.
   - 다른 그리드에도 동일한 테넌트에 대한 해당 버킷이 있습니다(정확한 이름을 사용해야 합니다).
   - 두 버킷 모두 객체 버전 관리가 활성화되어 있습니다(두 그리드 모두에서 버전 관리를 일시 중지할 수 없습니다).
   - 두 버킷 모두 객체 삭제 중**:** 읽기 전용 상태가 아닙니다.
8. 문제가 해결되었는지 확인하려면 "그리드 페더레이션 연결 모니터링"의 지침을 참조하여 교차 그리드 복제 메트릭을 검토하거나 다음 단계를 수행하십시오.
   a. 그리드 페더레이션 페이지로 돌아갑니다.
   b. 영향을 받는 테넌트를 선택하고 마지막 오류 열에서 *오류 지우기*를 선택합니다.
   c. 메시지를 지우고 시스템 상태를 업데이트하려면 *예*를 선택하십시오.
   d. 5~6분 정도 기다린 후 새 객체를 버킷에 수집합니다. 오류 메시지가 다시 나타나지 않는지 확인하십시오.

오류 메시지가 완전히 사라지도록 하려면 메시지에 표시된 타임스탬프 이후 최소 5분이 지난 후에 새 객체를 수집하십시오.

문제가 해결된 후 알림이 해제되는 데 최대 하루가 걸릴 수 있습니다.

a. "실패한 복제 작업 식별 및 재시도"로 이동하여 다른 그리드로 복제되지 못한 개체 또는 삭제 마커를 확인하고, 필요한 경우 복제를 다시 시도하십시오.

그리드 간 복제 리소스를 사용할 수 없음 알림

문제

교차 그리드 복제 리소스를 사용할 수 없음 경고가 발생했습니다.

세부 정보

이 경고는 리소스를 사용할 수 없어서 그리드 간 복제 요청이 보류 중임을 나타냅니다. 예를 들어 네트워크 오류가 발생했을 수 있습니다.

권장 조치

1. 문제가 저절로 해결되는지 알림을 모니터링하십시오.
2. 문제가 지속되면 두 그리드 중 하나에 동일한 연결에 대한 그리드 연합 연결 실패 경고 또는 노드에 대한 노드와 통신할 수 없음 경고가 있는지 확인하십시오. 이러한 경고를 해결하면 이 문제도 해결될 수 있습니다.
3. 오류에 대한 자세한 내용은 "그리드 페더레이션 연결 모니터링"의 지침을 참조하여 그리드 간 복제 메트릭을 검토하세요.
4. 해당 알림을 해결할 수 없는 경우 기술 지원 부서에 문의하십시오.

문제가 해결되면 그리드 간 복제는 정상적으로 진행됩니다.

실패한 StorageGRID 복제 작업을 식별하고 다시 시도합니다.

그리드 간 복제 영구 실패 경고를 해결한 후에는 다른 그리드로 복제되지 못한 개체 또는 삭제 마커가 있는지 확인해야 합니다. 그런 다음 해당 개체를 다시 수집하거나 그리드 관리 API를 사용하여 복제를 다시 시도할 수 있습니다.

그리드 간 복제 영구 실패 경고는 테넌트 객체가 두 그리드의 버킷 간에 복제되지 않는 이유가 있으며, 이를 해결하려면 사용자 개입이 필요함을 나타냅니다. 이 경고는 일반적으로 소스 버킷 또는 대상 버킷이 변경되었을 때 발생합니다. 자세한 내용은 "그리드 페더레이션 오류 해결"을 참조하십시오.

복제에 실패한 객체가 있는지 확인합니다

객체 또는 삭제 마커가 다른 그리드로 복제되지 않았는지 확인하려면 감사 로그에서 "CGRR(Cross-Grid Replication Request)" 메시지를 검색하십시오. 이 메시지는 StorageGRID가 객체, 멀티파트 객체 또는 삭제 마커를 대상 버킷으로 복제하는 데 실패할 경우 로그에 추가됩니다.

"audit-explain 도구"을 사용하여 결과를 더 읽기 쉬운 형식으로 변환할 수 있습니다.

시작하기 전에

- 루트 액세스 권한이 있습니다.
- You have the `Passwords.txt` 파일을 가지고 계시네요.
- 기본 관리 노드의 IP 주소를 알고 있습니다.

단계

1. 기본 관리 노드에 로그인합니다.
   a. 다음 명령줄을 입력합니다: `ssh admin@primary_Admin_Node_IP`
   b. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.
   c. 루트 권한으로 전환하려면 다음 명령을 입력하십시오. `su -`
   d. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.

      루트 계정으로 로그인하면 프롬프트가 `$`에서 `#`로 변경됩니다.

2. audit.log 파일에서 CGRR 메시지를 검색하고 audit-explain 도구를 사용하여 결과를 형식에 맞게 출력하십시오.

   예를 들어, 이 명령은 지난 30분 동안의 모든 CGRR 메시지를 검색하고 audit-explain 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
   ```

   명령 실행 결과는 다음 예시와 같이 6개의 CGRR 메시지 항목을 보여줍니다. 예시에서는 모든 그리드 간 복제 요청이 객체를 복제할 수 없다는 일반 오류를 반환했습니다. 처음 세 개의 오류는 "객체 복제" 작업에 대한 것이고, 마지막 세 개의 오류는 "삭제 마커 복제" 작업에 대한 것입니다.

   ```
   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.

필드	설명
CGRR 크로스 그리드 복제 요청	요청의 이름
테넌트	테넌트의 계정 ID
연결	그리드 페더레이션 연결의 ID
작업	시도 중인 복제 작업 유형: • 객체 복제 • 복제 삭제 마커 • 멀티파트 객체 복제
버킷	버킷 이름
오브젝트	객체 이름
버전	객체의 버전 ID
오류	오류 유형. 그리드 간 복제가 실패한 경우 오류는 "일반 오류"로 표시됩니다.

복제 실패 시 재시도

대상 버킷으로 복제되지 않은 객체 및 삭제 마커 목록을 생성하고 근본적인 문제를 해결한 후에는 다음 두 가지 방법 중 하나로 복제를 다시 시도할 수 있습니다.

- 각 객체를 소스 버킷에 다시 수집합니다.
- 설명된 대로 그리드 관리 비공개 API를 사용하십시오.

단계

1. 그리드 관리자 상단에서 도움말 아이콘을 선택한 다음 *API 문서*를 선택합니다.
2. *비공개 API 문서로 이동*을 선택합니다.

   "비공개"로 표시된 StorageGRID API 엔드포인트는 예고 없이 변경될 수 있습니다. StorageGRID 비공개 엔드포인트는 요청의 API 버전을 무시합니다.

3. **cross-grid-replication-advanced** 섹션에서 다음 엔드포인트를 선택하십시오.

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. *직접 사용해보기*를 선택합니다.
5. 본문 텍스트 상자에서 예시 항목인 *versionID*를 실패한 교차 그리드 복제 요청에 해당하는 audit.log의 버전 ID로 바꾸십시오.

문자열을 둘러싼 큰따옴표를 반드시 유지하십시오.

6. *실행*을 선택합니다.
7. 서버 응답 코드가 *204*인지 확인하십시오. 이는 객체 또는 삭제 마커가 다른 그리드로의 교차 그리드 복제를 위해 보류 중으로 표시되었음을 나타냅니다.

'대기 중'은 그리드 간 복제 요청이 처리를 위해 내부 대기열에 추가되었음을 의미합니다.

복제 재시도 모니터링

복제 재시도 작업이 완료되는지 확인하기 위해 해당 작업을 모니터링해야 합니다.

객체 또는 삭제 표시가 다른 그리드에 복제되는 데 몇 시간 또는 그 이상이 걸릴 수 있습니다.

재시도 작업은 다음 두 가지 방법 중 하나로 모니터링할 수 있습니다.

- S3 "HeadObject" 또는 "GetObject" 요청을 사용하십시오. 응답에는 StorageGRID 관련 `x-ntap-sg-cgr-replication-status` 응답 헤더가 포함되며, 이 헤더에는 다음 값 중 하나가 있습니다.

그리드	복제 상태
소스	• 완료됨: 복제가 성공적으로 완료되었습니다. • **PENDING**: 해당 개체가 아직 복제되지 않았습니다. • **FAILURE**: 복제가 영구적으로 실패했습니다. 사용자가 오류를 해결해야 합니다.
목적지	**REPLICA**: 해당 객체는 원본 그리드에서 복제되었습니다.

- 설명된 대로 그리드 관리 비공개 API를 사용하십시오.

단계

1. 비공개 API 문서의 **cross-grid-replication-advanced** 섹션에서 다음 엔드포인트를 선택하십시오.

```
GET /private/cross-grid-replication-object-status/{id}
```

2. *직접 사용해보기*를 선택합니다.
3. 매개변수 섹션에 `cross-grid-replication-retry-failed` 요청에 사용한 버전 ID를 입력하십시오.
4. *실행*을 선택합니다.
5. 서버 응답 코드가 *200*인지 확인하십시오.
6. 복제 상태를 검토하십시오. 복제 상태는 다음 중 하나입니다.
   - **PENDING**: 해당 개체가 아직 복제되지 않았습니다.
   - 완료됨: 복제가 성공적으로 완료되었습니다.
   - **FAILED**: 복제가 영구적인 오류로 실패했습니다. 사용자가 오류를 해결해야 합니다.

보안 관리

StorageGRID에서 보안 관리

Grid Manager에서 다양한 보안 설정을 구성하여 StorageGRID 시스템의 보안을 강화할 수 있습니다.

암호화 관리

StorageGRID는 데이터를 암호화할 수 있는 여러 옵션을 제공합니다. "사용 가능한 암호화 방법을 검토하십시오."데이터 보호 요구 사항에 맞는 옵션을 선택해야 합니다.

인증서 관리

HTTP 연결에 사용되는 "서버 인증서 구성 및 관리" 또는 클라이언트 또는 사용자 신원을 서버에 인증하는 데 사용되는 클라이언트 인증서를 사용할 수 있습니다.

키 관리 서버 구성

"키 관리 서버"을 사용하면 어플라이언스가 데이터 센터에서 제거되더라도 StorageGRID 데이터를 보호할 수 있습니다. 어플라이언스 볼륨이 암호화된 후에는 노드가 KMS와 통신할 수 없는 한 어플라이언스의 데이터에 액세스할 수 없습니다.

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

프록시 설정 관리

S3 플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 스토리지 노드와 외부 S3 엔드포인트 사이에 "스토리지 프록시 서버"을 구성할 수 있습니다. HTTPS 또는 HTTP를 사용하여 AutoSupport 패키지를 전송하는 경우 관리 노드와 기술 지원 사이에 "관리자 프록시 서버"을 구성할 수 있습니다.

방화벽 제어

시스템 보안을 강화하기 위해 "외부 방화벽"에서 특정 포트를 열거나 닫음으로써 StorageGRID 관리 노드에 대한 액세스를 제어할 수 있습니다. 또한 각 노드의 "내부 방화벽"를 구성하여 네트워크 액세스를 제어할 수도 있습니다. 배포에 필요한 포트를 제외한 모든 포트에 대한 액세스를 차단할 수 있습니다.

StorageGRID 암호화 방법 검토

StorageGRID는 데이터를 암호화하는 여러 옵션을 제공합니다. 사용 가능한 방법을 검토하여 데이터 보호 요구 사항에 맞는 방법을 선택하십시오.

이 표는 StorageGRID에서 사용 가능한 암호화 방법에 대한 개략적인 요약을 제공합니다.

암호화 옵션	작동 방식	적용 대상
Grid Manager의 키 관리 서버(KMS)	StorageGRID 사이트에 대해 "키 관리 서버 구성" 설정하고 "어플라이언스에 대한 노드 암호화 활성화". 그런 다음 어플라이언스 노드가 KMS에 연결하여 키 암호화 키(KEK)를 요청합니다. 이 키는 각 볼륨의 데이터 암호화 키(DEK)를 암호화하고 복호화합니다.	설치 중에 *노드 암호화*가 활성화된 어플라이언스 노드입니다. 어플라이언스의 모든 데이터는 물리적 손실이나 데이터 센터 외부로의 반출로부터 보호됩니다. 참고: KMS를 사용한 암호화 키 관리는 스토리지 노드 및 서비스 어플라이언스에서만 지원됩니다.
StorageGRID Appliance Installer의 드라이브 암호화 페이지	어플라이언스에 하드웨어 암호화를 지원하는 드라이브가 포함된 경우 설치 중에 드라이브 암호를 설정할 수 있습니다. 드라이브 암호를 설정하면 암호를 모르는 사람은 시스템에서 제거된 드라이브에서 유효한 데이터를 복구할 수 없습니다. 설치를 시작하기 전에 하드웨어 구성 > *드라이브 암호화*로 이동하여 노드의 모든 StorageGRID 관리형 자체 암호화 드라이브에 적용되는 드라이브 암호를 설정하십시오.	자체 암호화 드라이브가 내장된 어플라이언스입니다. 보안 드라이브에 저장된 모든 데이터는 물리적 손실이나 데이터 센터 외부 반출로부터 보호됩니다. 드라이브 암호화는 SANtricity에서 관리하는 드라이브에는 적용되지 않습니다. 자체 암호화 드라이브와 SANtricity 컨트롤러가 탑재된 스토리지 어플라이언스를 사용하는 경우 SANtricity에서 드라이브 보안을 활성화할 수 있습니다.
SANtricity System Manager의 드라이브 보안	StorageGRID 어플라이언스에서 드라이브 보안 기능이 활성화된 경우, "SANtricity System Manager"을 사용하여 보안 키를 생성하고 관리할 수 있습니다. 보안 드라이브의 데이터에 액세스하려면 이 키가 필요합니다.	전체 디스크 암호화(FDE) 드라이브 또는 자체 암호화 드라이브가 있는 스토리지 어플라이언스. 보안 드라이브의 모든 데이터는 물리적 손실이나 데이터 센터 외부 반출로부터 보호됩니다. 일부 스토리지 어플라이언스 또는 서비스 어플라이언스와는 함께 사용할 수 없습니다.
저장된 객체 암호화	Grid Manager에서 "저장된 객체 암호화" 옵션을 활성화합니다. 활성화되면 버킷 수준 또는 객체 수준에서 암호화되지 않은 모든 새 객체는 수집 중에 암호화됩니다.	새롭게 수집된 S3 객체 데이터. 기존에 저장된 객체는 암호화되지 않습니다. 객체 메타데이터 및 기타 민감한 데이터도 암호화되지 않습니다.

암호화 옵션	작동 방식	적용 대상
S3 버킷 암호화	PutBucketEncryption 요청을 실행하여 버킷에 대한 암호화를 활성화합니다. 객체 수준에서 암호화되지 않은 모든 새 객체는 수집 중에 암호화됩니다.	새로 수집된 S3 객체 데이터만 해당됩니다. 버킷에 대해 암호화 방식을 지정해야 합니다. 기존 버킷 객체는 암호화되지 않습니다. 객체 메타데이터 및 기타 민감한 데이터는 암호화되지 않습니다. "버킷에 대한 작업"
S3 객체 서버 측 암호화(SSE)	객체를 저장하기 위해 S3 요청을 보내고 `x-amz-server-side-encryption` 요청 헤더를 포함합니다.	새로 수집된 S3 객체 데이터만 해당됩니다. 객체에 대해 암호화 방식을 지정해야 합니다. 객체 메타데이터 및 기타 민감한 데이터는 암호화되지 않습니다. StorageGRID가 키를 관리합니다. "서버 측 암호화 사용"
고객이 제공한 키를 사용한 S3 객체 서버 측 암호화(SSE-C)	객체를 저장하기 위해 S3 요청을 보내고 세 가지 요청 헤더를 포함합니다. • `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 객체 데이터만 해당됩니다. 객체에 대해 암호화 방식을 지정해야 합니다. 객체 메타데이터 및 기타 민감한 데이터는 암호화되지 않습니다. 키는 StorageGRID 외부에서 관리됩니다. "서버 측 암호화 사용"
외부 볼륨 또는 데이터 저장소 암호화	배포 플랫폼에서 지원하는 경우 StorageGRID 외부의 암호화 방법을 사용하여 전체 볼륨 또는 데이터 저장소를 암호화할 수 있습니다.	모든 볼륨 또는 데이터 저장소가 암호화되었다고 가정할 때, 모든 객체 데이터, 메타데이터 및 시스템 구성 데이터. 외부 암호화 방식은 암호화 알고리즘과 키에 대한 더욱 강력한 제어를 제공합니다. 나열된 다른 방식들과 함께 사용할 수 있습니다.

암호화 옵션	작동 방식	적용 대상
StorageGRID 외부의 객체 암호화	StorageGRID에 수집되기 전에 StorageGRID 외부의 암호화 방법을 사용하여 오브젝트 데이터와 메타데이터를 암호화합니다.	객체 데이터 및 메타데이터만 암호화됩니다(시스템 구성 데이터는 암호화되지 않습니다). 외부 암호화 방식은 암호화 알고리즘과 키에 대한 더욱 강력한 제어를 제공합니다. 나열된 다른 방식들과 함께 사용할 수 있습니다. "Amazon Simple Storage Service - 사용자 가이드: 클라이언트 측 암호화를 사용한 데이터 보호"

여러 암호화 방법 사용

필요에 따라 여러 암호화 방식을 동시에 사용할 수 있습니다. 예를 들면 다음과 같습니다.

- KMS를 사용하여 어플라이언스 노드를 보호할 수 있으며, SANtricity System Manager의 드라이브 보안 기능을 사용하여 동일한 어플라이언스에 있는 자체 암호화 드라이브의 데이터를 "이중 암호화"할 수도 있습니다.
- KMS를 사용하여 어플라이언스 노드의 데이터를 보호할 수 있으며, 저장된 객체 암호화 옵션을 사용하여 객체가 수집될 때 모든 객체를 암호화할 수도 있습니다.

객체 중 일부만 암호화가 필요한 경우, 버킷 또는 개별 객체 수준에서 암호화를 제어하는 것을 고려하십시오. 여러 수준의 암호화를 활성화하면 추가적인 성능 비용이 발생합니다.

관련 정보

"FIPS 인증 암호화 옵션에 대해 알아보기"

인증서 관리

StorageGRID에서 보안 인증서 관리

보안 인증서는 StorageGRID 구성 요소 간, 그리고 StorageGRID 구성 요소와 외부 시스템 간에 안전하고 신뢰할 수 있는 연결을 생성하는 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 안전한 연결을 설정하는 데 사용되며, 서버의 신원을 클라이언트에게 인증하고 데이터에 대한 안전한 통신 경로를 제공합니다. 서버와 클라이언트는 각각 인증서 사본을 보유합니다.
- *클라이언트 인증서*는 클라이언트 또는 사용자의 신원을 서버에 인증하여 비밀번호만 사용하는 것보다 더 안전한 인증을 제공합니다. 클라이언트 인증서는 데이터를 암호화하지 않습니다.

클라이언트가 HTTPS를 사용하여 서버에 연결하면 서버는 공개 키가 포함된 서버 인증서를 응답으로 보냅니다. 클라이언트는 서버 서명과 자신이 소유한 인증서의 서명을 비교합니다. 서명이 일치하면 클라이언트는 동일한 공개 키를 사용하여 서버와 세션을 시작합니다.

StorageGRID는 일부 연결(예: 로드 밸런서 엔드포인트)에 대해서는 서버 역할을 하고, 다른 연결(예: CloudMirror 복제

서비스)에 대해서는 클라이언트 역할을 합니다.

기본 그리드 **CA** 인증서

StorageGRID 시스템 설치 중에 내부 Grid CA 인증서를 생성하는 내장 인증 기관(CA)이 있습니다. 이 Grid CA 인증서는 기본적으로 내부 StorageGRID 트래픽을 보호하는 데 사용됩니다. 외부 인증 기관(CA)을 통해 조직의 정보 보안 정책을 완벽하게 준수하는 사용자 지정 인증서를 발급받을 수도 있습니다.

비프로덕션 환경에서는 Grid CA 인증서를 사용하십시오. 운영 환경에서는 외부 인증 기관에서 서명한 사용자 지정 인증서를 사용하십시오. 인증서가 없는 보안되지 않은 연결도 지원되지만 권장하지 않습니다.

- 사용자 지정 CA 인증서는 내부 인증서를 제거하지 않습니다. 다만, 서버 연결 확인을 위해 지정된 인증서는 사용자 지정 인증서여야 합니다.
- 모든 사용자 지정 인증서는 "서버 인증서에 대한 시스템 강화 지침"을(를) 충족해야 합니다.
- StorageGRID는 CA의 인증서를 단일 파일(CA 인증서 번들이라고 함)로 묶는 기능을 지원합니다.

> StorageGRID에는 모든 그리드에서 동일한 운영 체제 CA 인증서도 포함되어 있습니다. 운영 환경에서는 운영 체제 CA 인증서 대신 외부 인증 기관에서 서명한 사용자 지정 인증서를 지정해야 합니다.

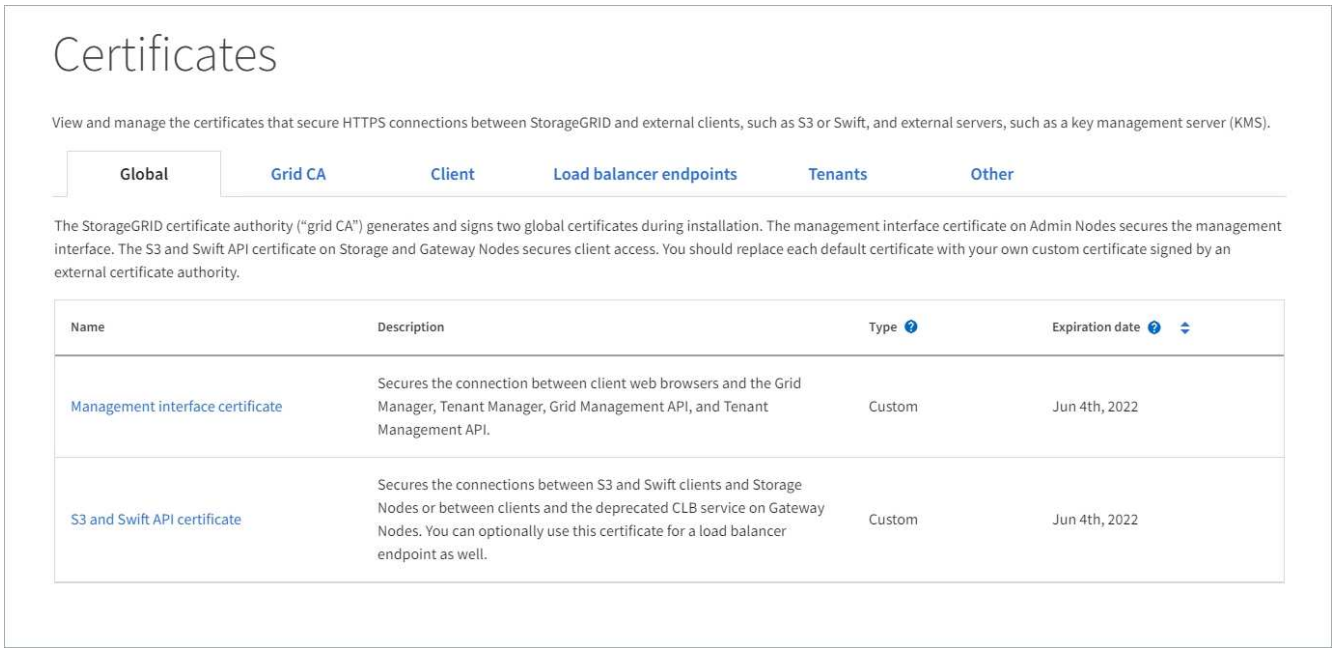
서버 및 클라이언트 인증서 유형의 변형은 여러 가지 방식으로 구현됩니다. 시스템을 구성하기 전에 특정 StorageGRID 구성에 필요한 모든 인증서를 준비해야 합니다.

보안 인증서 액세스

StorageGRID 인증서에 대한 모든 정보를 한 곳에서 확인할 수 있으며, 각 인증서의 구성 워크플로에 대한 링크도 제공됩니다.

단계

1. 그리드 관리자에서 구성 > 보안 > *인증서*를 선택합니다.



2. 인증서 페이지에서 탭을 선택하면 각 인증서 범주에 대한 정보를 확인하고 인증서 설정에 액세스할 수 있습니다.

"적절한 권한"이(가) 있는 경우 탭에 액세스할 수 있습니다.

- 전역: 웹 브라우저 및 외부 API 클라이언트에서 StorageGRID에 대한 액세스를 보호합니다.
- **Grid 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 엔드포인트에서 S3 스토리지 리소스로의 연결을 보호합니다.
- 기타: 특정 인증서가 필요한 StorageGRID 연결을 보호합니다.

  각 탭에 대한 설명과 추가 인증서 세부 정보 링크는 아래에 있습니다.

글로벌

글로벌 인증서는 웹 브라우저 및 외부 S3 API 클라이언트의 StorageGRID 액세스를 보호합니다. StorageGRID 인증 기관은 설치 중에 두 개의 글로벌 인증서를 생성합니다. 운영 환경에서는 외부 인증 기관에서 서명한 사용자 지정 인증서를 사용하는 것이 좋습니다.

- 관리 인터페이스 인증서: 클라이언트 웹 브라우저와 StorageGRID 관리 인터페이스 간의 연결을 보호합니다.
- S3 API 인증서: S3 클라이언트 애플리케이션이 객체 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 포함된 인증서 이름입니다.
- 설명
- 유형: 사용자 지정 또는 기본값. + 그리드 보안 강화를 위해 항상 사용자 지정 인증서를 사용하는 것이 좋습니다.
- 만료일: 기본 인증서를 사용하는 경우 만료일이 표시되지 않습니다.

다음을 수행할 수 있습니다.

- 그리드 보안 강화를 위해 기본 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 교체하십시오.
  - "기본 StorageGRID 생성 관리 인터페이스 인증서 교체" Grid Manager 및 테넌트 관리자 연결에 사용됩니다.
  - "S3 API 인증서 교체"스토리지 노드 및 로드 밸런서 엔드포인트(선택 사항) 연결에 사용됩니다.
- "기본 관리 인터페이스 인증서 복원".
- "기본 S3 API 인증서 복원".
- "스크립트를 사용하여 자체 서명된 새 관리 인터페이스 인증서를 생성합니다.".
- "관리 인터페이스 인증서" 또는 "S3 API 인증서"을 복사하거나 다운로드합니다.

그리드 **CA**

StorageGRID 설치 중에 StorageGRID 인증 기관에서 생성된 그리드 CA 인증서은(는) 모든 내부 StorageGRID 트래픽을 보호합니다.

인증서 정보에는 인증서 만료일과 인증서 내용이 포함됩니다.

"Grid CA 인증서 복사 또는 다운로드"할 수 있지만, 변경할 수는 없습니다.

클라이언트

클라이언트 인증서외부 인증 기관에서 생성된 인증서는 외부 모니터링 도구와 StorageGRID Prometheus 데이터베이스 간의 연결을 보호합니다.

인증서 테이블에는 구성된 각 클라이언트 인증서에 대한 행이 있으며, 해당 인증서를 Prometheus 데이터베이스 액세스에 사용할 수 있는지 여부와 인증서 만료일이 표시됩니다.

다음을 수행할 수 있습니다.

- "클라이언트 인증서를 업로드하거나 새 인증서를 생성합니다."
- 인증서 이름을 선택하면 인증서 세부 정보가 표시됩니다. 여기서 다음을 수행할 수 있습니다.
  - "클라이언트 인증서 이름을 변경합니다."
  - "Prometheus 액세스 권한을 설정합니다."
  - "클라이언트 인증서를 업로드하고 교체하십시오."
  - "클라이언트 인증서를 복사하거나 다운로드하십시오."
  - "클라이언트 인증서를 제거합니다."
- 클라이언트 인증서를 빠르게 "편집", "연결" 또는 "제거"하려면 **Actions***를 선택하십시오**. *Actions** > *Remove*를 사용하여 최대 10개의 클라이언트 인증서를 선택하고 한 번에 제거할 수 있습니다.

로드 밸런서 엔드포인트

로드 밸런서 엔드포인트 인증서StorageGRID 게이트웨이 노드와 관리 노드에서 S3 클라이언트와 StorageGRID 로드 밸런서 서비스 간의 연결을 보호합니다.

로드 밸런서 엔드포인트 테이블에는 구성된 각 로드 밸런서 엔드포인트에 대한 행이 있으며, 해당 엔드포인트에 글로벌 S3 API 인증서 또는 사용자 지정 로드 밸런서 엔드포인트 인증서가 사용되는지 여부를 나타냅니다. 각 인증서의 만료일도 표시됩니다.

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

다음을 수행할 수 있습니다.

- "로드 밸런서 엔드포인트 보기", 인증서 세부 정보를 포함합니다.
- "FabricPool에 대한 로드 밸런서 엔드포인트 인증서를 지정합니다."
- "글로벌 S3 API 인증서 사용" 새로운 로드 밸런서 엔드포인트 인증서를 생성하는 대신.

테넌트

테넌트는 ID 페더레이션 서버 인증서 또는 플랫폼 서비스 엔드포인트 인증서를 사용하여 StorageGRID와의 연결을 보호할 수 있습니다.

테넌트 테이블에는 각 테넌트에 대한 행이 있으며 각 테넌트가 자체 ID 소스 또는 플랫폼 서비스를 사용할 권한이 있는지 여부를 나타냅니다.

다음을 수행할 수 있습니다.

- "Tenant Manager에 로그인하려면 테넌트 이름을 선택하세요."
- "테넌트 이름을 선택하여 테넌트 ID 페더레이션 세부 정보를 확인합니다."
- "테넌트 이름을 선택하여 테넌트 플랫폼 서비스 세부 정보를 확인합니다."
- "엔드포인트 생성 시 플랫폼 서비스 엔드포인트 인증서 지정"

기타

StorageGRID는 특정 목적을 위해 다른 보안 인증서를 사용합니다. 이러한 인증서는 기능 이름으로 나열됩니다. 다른 보안 인증서는 다음과 같습니다.

- 클라우드 스토리지 풀 인증서

- 이메일 알림 인증서
- 외부 syslog 서버 인증서
- 그리드 페더레이션 연결 인증서
- 신원 연동 인증서
- 키 관리 서버(KMS) 인증서
- 싱글 사인온 인증서

이 정보에는 함수가 사용하는 인증서 유형과 서버 및 클라이언트 인증서 만료일(해당하는 경우)이 표시됩니다. 함수 이름을 선택하면 브라우저 탭이 열리고 인증서 세부 정보를 보고 편집할 수 있습니다.

다른 인증서에 대한 정보를 보고 액세스하려면 "적절한 권한"이(가) 있어야 합니다.

다음을 수행할 수 있습니다.

- "S3, C2S S3 또는 Azure 클라우드 스토리지 풀 인증서 지정"
- "알림 이메일 알림에 사용할 인증서를 지정합니다."
- "외부 syslog 서버에 인증서 사용"
- "그리드 페더레이션 연결 인증서 교체"
- "ID 연동 인증서 보기 및 편집"
- "키 관리 서버(KMS) 서버 및 클라이언트 인증서 업로드"
- "신뢰 당사자 트러스트에 대한 SSO 인증서를 수동으로 지정"

보안 인증서 세부 정보

아래에는 각 보안 인증서 유형에 대한 설명과 구현 지침 링크가 제공됩니다.

관리 인터페이스 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	클라이언트 웹 브라우저와 StorageGRID 관리 인터페이스 간의 연결을 인증하여 사용자가 보안 경고 없이 Grid Manager 및 Tenant Manager에 액세스할 수 있도록 합니다. 이 인증서는 Grid Management API 및 Tenant Management API 연결도 인증합니다. 설치 중에 생성된 기본 인증서를 사용하거나 사용자 지정 인증서를 업로드할 수 있습니다.	구성 > 보안 > 인증서*로 이동하여 *전역 탭을 선택한 다음 *관리 인터페이스 인증서*를 선택합니다.	"관리 인터페이스 인증서 구성"

S3 API 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	스토리지 노드 및 로드 밸런서 엔드포인트에 대한 보안 S3 클라이언트 연결을 인증합니다(선택 사항).	구성 > 보안 > 인증서*로 이동하여 *전역 탭을 선택한 다음 *S3 API 인증서*를 선택합니다.	"S3 API 인증서 구성"

그리드 **CA** 인증서

기본 그리드 CA 인증서 설명을 참조하십시오.

관리자 클라이언트 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
클라이언트	각 클라이언트에 설치되어 StorageGRID 외부 클라이언트 액세스를 인증할 수 있도록 합니다. • 승인된 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있도록 합니다. • 외부 도구를 사용하여 StorageGRID를 안전하게 모니터링할 수 있습니다.	구성 > 보안 > 인증서*로 이동한 다음 *클라이언트 탭을 선택합니다.	"클라이언트 인증서 구성"

로드 밸런서 엔드포인트 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	StorageGRID 게이트웨이 노드 및 관리 노드의 StorageGRID 로드 밸런서 서비스와 S3 클라이언트 간의 연결을 인증합니다. 로드 밸런서 엔드포인트를 구성할 때 로드 밸런서 인증서를 업로드하거나 생성할 수 있습니다. 클라이언트 애플리케이션은 StorageGRID에 연결하여 객체 데이터를 저장하고 검색할 때 로드 밸런서 인증서를 사용합니다. 사용자 지정 버전의 글로벌 S3 API 인증서 인증서를 사용하여 로드 밸런서 서비스에 대한 연결을 인증할 수도 있습니다. 글로벌 인증서를 로드 밸런서 연결 인증에 사용하는 경우 각 로드 밸런서 엔드포인트에 대해 별도의 인증서를 업로드하거나 생성할 필요가 없습니다. 참고: 로드 밸런서 인증에 사용되는 인증서는 StorageGRID 정상 작동 중에 가장 많이 사용되는 인증서입니다.	구성 > 네트워크 > 로드 밸런서 엔드포인트	• "로드 밸런서 엔드포인트 구성" • "FabricPool용 로드 밸런서 엔드포인트 생성"

클라우드 스토리지 풀 엔드포인트 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	StorageGRID 클라우드 스토리지 풀에서 S3 Glacier 또는 Microsoft Azure Blob 스토리지와 같은 외부 스토리지 위치로의 연결을 인증합니다. 각 클라우드 공급자 유형마다 다른 인증서가 필요합니다.	**ILM** > 스토리지 풀	"클라우드 스토리지 풀 생성"

이메일 알림 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버와 클라이언트	StorageGRID 알림 전송에 사용되는 SMTP 이메일 서버와 StorageGRID 간의 연결을 인증합니다. • SMTP 서버와의 통신에 전송 계층 보안(TLS)이 필요한 경우 이메일 서버 CA 인증서를 지정해야 합니다. • SMTP 이메일 서버에서 인증을 위해 클라이언트 인증서가 필요한 경우에만 클라이언트 인증서를 지정하십시오.	알림 > 이메일 설정	"알림에 대한 이메일 알림 설정"

외부 **syslog** 서버 인증서

인증서 유형	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 서버 사용"

그리드 페더레이션 연결 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버와 클라이언트	현재 StorageGRID 시스템과 그리드 페더레이션 연결에 있는 다른 그리드 간에 전송되는 정보를 인증하고 암호화합니다.	구성 > 시스템 > 그리드 페더레이션	• "그리드 페더레이션 연결 생성" • "연결 인증서 순환"

ID 페더레이션 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	StorageGRID와 Active Directory, OpenLDAP 또는 Oracle Directory Server와 같은 외부 ID 공급자 간의 연결을 인증합니다. 관리자 그룹과 사용자를 외부 시스템에서 관리할 수 있도록 하는 ID 페더레이션에 사용됩니다.	구성 > 액세스 제어 > **ID** 연동	"ID 페더레이션 사용"

키 관리 서버**(KMS)** 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버와 클라이언트	StorageGRID와 외부 키 관리 서버(KMS) 간의 연결을 인증합니다. KMS는 StorageGRID 어플라이언스 노드에 암호화 키를 제공합니다.	구성 > 보안 > 키 관리 서버	"키 관리 서버(KMS) 추가"

플랫폼 서비스 엔드포인트 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	StorageGRID 플랫폼 서비스와 S3 스토리지 리소스 간의 연결을 인증합니다.	테넌트 관리자 > 스토리지**(S3)** > 플랫폼 서비스 엔드포인트	"플랫폼 서비스 엔드포인트 생성" "플랫폼 서비스 엔드포인트 편집"

싱글 사인온**(SSO)** 인증서

인증서 유형	설명	내비게이션 위치	세부 정보
서버	Active Directory Federation Services(AD FS)와 같은 ID 페더레이션 서비스와 SSO(Single Sign-On) 요청에 사용되는 StorageGRID 간의 연결을 인증합니다.	구성 > 접근 제어 > 싱글 사인온	"싱글 사인온(SSO) 구성"

인증서 예시

예시 **1:** 로드 밸런서 서비스

이 예시에서 StorageGRID는 서버 역할을 합니다.

1. StorageGRID에서 로드 밸런서 엔드포인트를 구성하고 서버 인증서를 업로드하거나 생성합니다.
2. 로드 밸런싱 엔드포인트에 대한 S3 클라이언트 연결을 구성하고 동일한 인증서를 클라이언트에 업로드합니다.
3. 클라이언트가 데이터를 저장하거나 검색하려는 경우, HTTPS를 사용하여 로드 밸런서 엔드포인트에 연결합니다.
4. StorageGRID는 공개 키가 포함된 서버 인증서와 개인 키를 기반으로 한 서명을 응답으로 보냅니다.
5. 클라이언트는 서버의 서명과 자신이 보유한 인증서 사본의 서명을 비교합니다. 서명이 일치하면 클라이언트는 동일한 공개 키를 사용하여 세션을 시작합니다.
6. 클라이언트가 객체 데이터를 StorageGRID에 전송합니다.

예시 **2:** 외부 키 관리 서버**(KMS)**

이 예시에서 StorageGRID는 클라이언트 역할을 합니다.

1. 외부 키 관리 서버 소프트웨어를 사용하여 StorageGRID를 KMS 클라이언트로 구성하고 CA에서 서명한 서버 인증서, 공개 클라이언트 인증서 및 클라이언트 인증서용 개인 키를 얻습니다.
2. 그리드 관리자를 사용하여 KMS 서버를 구성하고 서버 및 클라이언트 인증서와 클라이언트 개인 키를 업로드합니다.
3. StorageGRID 노드가 암호화 키가 필요한 경우, 인증서의 데이터와 개인 키를 기반으로 한 서명을 포함하는 요청을 KMS 서버에 보냅니다.
4. KMS 서버는 인증서 서명을 검증하고 StorageGRID를 신뢰할 수 있다고 결정합니다.
5. KMS 서버는 유효성이 검증된 연결을 사용하여 응답합니다.

StorageGRID에서 지원되는 서버 인증서 유형

StorageGRID 시스템은 RSA 또는 ECDSA(Elliptic Curve Digital Signature Algorithm)로 암호화된 사용자 지정 인증서를 지원합니다.

보안 정책에 사용할 암호화 유형은 서버 인증서 유형과 일치해야 합니다. 예를 들어 RSA 암호화에는 RSA 인증서가 필요하고 ECDSA 암호화에는 ECDSA 인증서가 필요합니다. 자세한 내용은 "보안 인증서 관리"을 참조하십시오. 서버 인증서와 호환되지 않는 사용자 지정 보안 정책을 구성한 경우 "일시적으로 기본 보안 정책으로 되돌립니다.".

StorageGRID 클라이언트 연결을 보호하는 방법에 대한 자세한 내용은 "S3 클라이언트 보안"을 참조하십시오.

StorageGRID에서 관리 인터페이스 인증서를 구성합니다

기본 관리 인터페이스 인증서를 사용자 지정 인증서 하나로 교체하면 사용자가 보안 경고 없이 그리드 관리자 및 테넌트 관리자에 액세스할 수 있습니다. 또한 기본 관리 인터페이스 인증서로 되돌리거나 새 인증서를 생성할 수도 있습니다.

이 작업 정보

기본적으로 모든 관리 노드에는 그리드 CA에서 서명한 인증서가 발급됩니다. 이러한 CA 서명 인증서는 단일 공통 사용자 지정 관리 인터페이스 인증서와 해당 개인 키로 대체할 수 있습니다.

모든 관리 노드에 단일 사용자 지정 관리 인터페이스 인증서가 사용되므로 클라이언트가 그리드 관리자 및 테넌트 관리자에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 그리드의 모든 관리 노드와 일치하도록 사용자 지정 인증서를 정의하십시오.

서버에서 구성을 완료해야 하며, 사용 중인 루트 인증 기관(CA)에 따라 사용자는 Grid Manager 및 Tenant Manager에 액세스하는 데 사용할 웹 브라우저에 Grid CA 인증서를 설치해야 할 수도 있습니다.

서버 인증서 오류로 인해 운영이 중단되는 것을 방지하기 위해, 이 서버 인증서가 만료되려고 할 때 관리 인터페이스용 서버 인증서 만료 알림이 트리거됩니다. 필요한 경우, 구성 > 보안 > *인증서*를 선택하고 전역 탭에서 관리 인터페이스 인증서의 만료일을 확인하여 현재 인증서의 만료일을 볼 수 있습니다.

IP 주소 대신 도메인 이름을 사용하여 Grid Manager 또는 Tenant Manager에 액세스하는 경우 다음 중 하나가 발생하면 브라우저에 인증서 오류가 표시되고 이를 우회할 수 있는 옵션이 제공되지 않습니다.

- 사용자 지정 관리 인터페이스 인증서가 만료됩니다.
- 귀하 사용자 지정 관리 인터페이스 인증서에서 기본 서버 인증서로 되돌리기.

사용자 지정 관리 인터페이스 인증서 추가

사용자 지정 관리 인터페이스 인증서를 추가하려면 자체 인증서를 제공하거나 Grid Manager를 사용하여 인증서를 생성할 수 있습니다.

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 전역 탭에서 *관리 인터페이스 인증서*를 선택합니다.
3. *사용자 지정 인증서 사용*을 선택합니다.
4. 인증서를 업로드하거나 생성합니다.

인증서 업로드

필요한 서버 인증서 파일을 업로드합니다.

a. *인증서 업로드*를 선택합니다.

b. 필요한 서버 인증서 파일을 업로드합니다.

   - 서버 인증서: 사용자 지정 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 기관(CA)의 인증서가 포함된 단일 선택적 파일입니다. 이 파일에는 각 CA 인증서 파일이 PEM 형식으로 인코딩되어 인증서 체인 순서대로 연결되어 있어야 합니다.

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

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

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

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

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

d. *저장*을 선택합니다. + 사용자 지정 관리 인터페이스 인증서는 Grid Manager, Tenant Manager, Grid Manager API 또는 Tenant Manager API에 대한 모든 후속 새 연결에 사용됩니다.

인증서 생성

서버 인증서 파일을 생성합니다.

운영 환경의 모범 사례는 외부 인증 기관에서 서명한 사용자 지정 관리 인터페이스 인증서를 사용하는 것입니다.

a. *인증서 생성*을 선택합니다.

b. 인증서 정보를 지정합니다:

필드	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내려면 와일드카드 문자 *를 사용하십시오.
IP	인증서에 포함할 IP 주소를 하나 이상 입력하십시오.

필드	설명
제목 (선택 사항)	X.509 인증서 소유자의 주체 또는 고유명칭(DN). 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 주체 공통 이름(CN)으로 사용합니다.
유효 기간	인증서 발급일로부터 만료일까지의 일수입니다.
키 사용 확장 추가	선택된 경우(기본값이며 권장됨), 생성된 인증서에 키 사용 및 확장 키 사용 확장 기능이 추가됩니다. 이러한 확장 기능은 인증서에 포함된 키의 용도를 정의합니다. 참고: 인증서에 이러한 확장이 포함된 경우 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택한 상태로 두십시오.

c. *생성*을 선택합니다.

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

   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택합니다.

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

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

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

e. *저장*을 선택합니다. + 사용자 지정 관리 인터페이스 인증서는 Grid Manager, Tenant Manager, Grid Manager API 또는 Tenant Manager API에 대한 모든 후속 새 연결에 사용됩니다.

5. 웹 브라우저가 업데이트되도록 페이지를 새로 고침하십시오.

   새 인증서를 업로드하거나 생성한 후, 관련 인증서 만료 알림이 모두 사라지는 데 최대 하루가 소요될 수 있습니다.

6. 사용자 지정 관리 인터페이스 인증서를 추가하면 관리 인터페이스 인증서 페이지에 사용 중인 인증서에 대한 자세한 정보가 표시됩니다. + 필요에 따라 인증서 PEM을 다운로드하거나 복사할 수 있습니다.

기본 관리 인터페이스 인증서 복원

Grid Manager 및 Tenant Manager 연결에 기본 관리 인터페이스 인증서를 다시 사용하도록 되돌릴 수 있습니다.

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 전역 탭에서 *관리 인터페이스 인증서*를 선택합니다.
3. *기본 인증서 사용*을 선택합니다.

기본 관리 인터페이스 인증서를 복원하면 구성한 사용자 지정 서버 인증서 파일이 삭제되어 시스템에서 복구할 수 없습니다. 이후의 모든 새 클라이언트 연결에는 기본 관리 인터페이스 인증서가 사용됩니다.

4. 웹 브라우저가 업데이트되도록 페이지를 새로 고침하십시오.

스크립트를 사용하여 자체 서명된 새 관리 인터페이스 인증서를 생성합니다.

호스트 이름 유효성 검사가 엄격하게 필요한 경우 스크립트를 사용하여 관리 인터페이스 인증서를 생성할 수 있습니다.

시작하기 전에

- "특정 액세스 권한"이(가) 있습니다.
- You have the `Passwords.txt` 파일을 가지고 계시네요.

이 작업 정보

운영 환경의 모범 사례는 외부 인증 기관에서 서명한 인증서를 사용하는 것입니다.

단계

1. 각 관리 노드의 정규화된 도메인 이름(FQDN)을 확보하십시오.
2. 기본 관리 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
   b. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.
   c. 루트 권한으로 전환하려면 다음 명령을 입력하십시오. `su -`
   d. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.

   루트 계정으로 로그인하면 프롬프트가 `$`에서 `#`로 변경됩니다.
3. StorageGRID에 새 자체 서명 인증서를 구성합니다.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

   - `--domains`의 경우, 모든 관리 노드의 정규화된 도메인 이름을 나타내기 위해 와일드카드를 사용하십시오. 예를 들어, `*.ui.storagegrid.example.com`는 * 와일드카드를 사용하여 `admin1.ui.storagegrid.example.com`와 `admin2.ui.storagegrid.example.com`를 나타냅니다.
   - Set `--type` to `management` 관리 인터페이스 인증서를 구성하려면 이 옵션을 선택하십시오. 이 인증서는 Grid Manager 및 Tenant Manager에서 사용됩니다.
   - 기본적으로 생성된 인증서는 1년(365일) 동안 유효하며 만료되기 전에 다시 생성해야 합니다. `--days` 인수를 사용하여 기본 유효 기간을 재정의할 수 있습니다.

> 인증서의 유효 기간은 `make-certificate`가 실행되는 시점부터 시작됩니다. 관리 클라이언트가 StorageGRID와 동일한 시간 소스에 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 공개 인증서가 포함되어 있습니다.

4. 인증서를 선택하고 복사합니다.

   선택 항목에 BEGIN 태그와 END 태그를 포함하세요.

5. 명령 셸에서 로그아웃하세요. `$ exit`
6. 인증서가 구성되었는지 확인하십시오.
   a. 그리드 관리자에 액세스합니다.
   b. 구성 > 보안 > *인증서*를 선택합니다.
   c. 전역 탭에서 *관리 인터페이스 인증서*를 선택합니다.
7. 복사한 공개 인증서를 사용하도록 관리 클라이언트를 구성하십시오. BEGIN 및 END 태그를 포함하십시오.

관리 인터페이스 인증서 다운로드 또는 복사

관리 인터페이스 인증서 내용을 저장하거나 복사하여 다른 곳에서 사용할 수 있습니다.

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 전역 탭에서 *관리 인터페이스 인증서*를 선택합니다.
3. 서버 또는 **CA** 번들 탭을 선택한 다음 인증서를 다운로드하거나 복사하십시오.

인증서 파일 또는 **CA** 번들 다운로드

인증서 또는 CA 번들 `.pem` 파일을 다운로드하십시오. 선택 사항인 CA 번들을 사용하는 경우 번들에 포함된 각 인증서가 별도의 하위 탭에 표시됩니다.

a. 인증서 다운로드 또는 *CA 번들 다운로드*를 선택합니다.

   CA 번들을 다운로드하는 경우, CA 번들의 보조 탭에 있는 모든 인증서가 단일 파일로 다운로드됩니다.

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

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서 또는 **CA** 번들 **PEM** 복사

인증서 텍스트를 복사하여 다른 곳에 붙여넣으세요. 선택 사항인 CA 번들을 사용하는 경우, 번들에 포함된 각 인증서는 별도의 하위 탭에 표시됩니다.

a. 인증서 **PEM** 복사 또는 *CA 번들 PEM 복사*를 선택합니다.

   CA 번들을 복사하는 경우 CA 번들의 보조 탭에 있는 모든 인증서가 함께 복사됩니다.

b. 복사한 인증서를 텍스트 편집기에 붙여넣으세요.

c. 텍스트 파일을 확장자 `.pem`로 저장하세요.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

StorageGRID에서 **S3 API** 인증서 구성

스토리지 노드 또는 로드 밸런서 엔드포인트에 대한 S3 클라이언트 연결에 사용되는 서버 인증서를 교체하거나 복원할 수 있습니다. 교체용 사용자 지정 서버 인증서는 조직에 특화되어 있습니다.

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

이 작업 정보

기본적으로 모든 스토리지 노드에는 그리드 CA에서 서명한 X.509 서버 인증서가 발급됩니다. 이러한 CA 서명 인증서는 단일 공통 사용자 지정 서버 인증서와 해당 개인 키로 대체할 수 있습니다.

모든 스토리지 노드에 단일 사용자 지정 서버 인증서가 사용되므로 클라이언트가 스토리지 엔드포인트에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 그리드의 모든 스토리지 노드와 일치하도록 사용자 지정 인증서를 정의하십시오.

서버에서 구성을 완료한 후에는 사용 중인 루트 인증 기관(CA)에 따라 시스템에 액세스하는 데 사용할 S3 API 클라이언트에 Grid CA 인증서를 설치해야 할 수도 있습니다.

서버 인증서 오류로 인해 운영이 중단되는 것을 방지하기 위해 루트 서버 인증서 만료 예정 시 **S3 API**용 글로벌 서버 인증서 만료 알림이 발생합니다. 필요에 따라 구성 > 보안 > *인증서*를 선택하고 글로벌 탭에서 S3 API 인증서의 만료일을 확인하여 현재 인증서의 만료일을 확인할 수 있습니다.

사용자 지정 S3 API 인증서를 업로드하거나 생성할 수 있습니다.

사용자 지정 **S3 API** 인증서 추가

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 글로벌 탭에서 *S3 API 인증서*를 선택합니다.
3. *사용자 지정 인증서 사용*을 선택합니다.
4. 인증서를 업로드하거나 생성합니다.

인증서 업로드

필요한 서버 인증서 파일을 업로드합니다.

a. *인증서 업로드*를 선택합니다.

b. 필요한 서버 인증서 파일을 업로드합니다.

   - 서버 인증서: 사용자 지정 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 인증서가 포함된 단일 파일(선택 사항). 이 파일에는 각 CA 인증서 파일이 PEM 형식으로 인코딩되어 인증서 체인 순서대로 연결되어 있어야 합니다.

c. 인증서 세부 정보를 선택하면 업로드된 각 사용자 지정 S3 API 인증서의 메타데이터와 PEM이 표시됩니다. 선택적으로 CA 번들을 업로드한 경우 각 인증서가 별도의 탭에 표시됩니다.

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

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

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

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

d. *저장*을 선택하세요.

   사용자 지정 서버 인증서는 이후의 새로운 S3 클라이언트 연결에 사용됩니다.

인증서 생성

서버 인증서 파일을 생성합니다.

a. *인증서 생성*을 선택합니다.

b. 인증서 정보를 지정합니다:

필드	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내려면 와일드카드 문자 *를 사용하십시오.
IP	인증서에 포함할 IP 주소를 하나 이상 입력하십시오.

필드	설명
제목 (선택 사항)	X.509 인증서 소유자의 주체 또는 고유명칭(DN). 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 주체 공통 이름(CN)으로 사용합니다.
유효 기간	인증서 발급일로부터 만료일까지의 일수입니다.
키 사용 확장 추가	선택된 경우(기본값이며 권장됨), 생성된 인증서에 키 사용 및 확장 키 사용 확장 기능이 추가됩니다. 이러한 확장 기능은 인증서에 포함된 키의 용도를 정의합니다. 참고: 인증서에 이러한 확장이 포함된 경우 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택한 상태로 두십시오.

c. *생성*을 선택합니다.

d. 생성된 사용자 지정 S3 API 인증서의 메타데이터 및 PEM을 표시하려면 *인증서 세부 정보*를 선택하십시오.

   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택합니다.

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

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

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

e. *저장*을 선택하세요.

   사용자 지정 서버 인증서는 이후의 새로운 S3 클라이언트 연결에 사용됩니다.

5. 기본 StorageGRID 서버 인증서, 업로드된 CA 서명 인증서 또는 생성된 사용자 지정 인증서에 대한 메타데이터를 표시하려면 탭을 선택하십시오.

   새 인증서를 업로드하거나 생성한 후, 관련 인증서 만료 알림이 모두 사라지는 데 최대 하루가 소요될 수 있습니다.

6. 웹 브라우저가 업데이트되도록 페이지를 새로 고침하십시오.

7. 사용자 지정 S3 API 인증서를 추가하면 S3 API 인증서 페이지에 사용 중인 사용자 지정 S3 API 인증서에 대한 자세한 정보가 표시됩니다. + 필요에 따라 인증서 PEM을 다운로드하거나 복사할 수 있습니다.

기본 **S3 API** 인증서 복원

스토리지 노드에 대한 S3 클라이언트 연결에는 기본 S3 API 인증서를 다시 사용할 수 있습니다. 하지만 로드 밸런서 엔드포인트에는 기본 S3 API 인증서를 사용할 수 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. 이후 스토리지 노드에 대한 새로운 S3 클라이언트 연결에는 기본 S3 API 인증서가 사용됩니다.

4. 경고를 확인하고 기본 S3 API 인증서를 복원하려면 *확인*을 선택하십시오.

   루트 액세스 권한이 있고 사용자 지정 S3 API 인증서를 로드 밸런서 엔드포인트 연결에 사용한 경우, 기본 S3 API 인증서를 사용하여 더 이상 액세스할 수 없는 로드 밸런서 엔드포인트 목록이 표시됩니다. 영향을 받는 엔드포인트를 편집하거나 제거하려면 "로드 밸런서 엔드포인트 구성"으로 이동하십시오.

5. 웹 브라우저가 업데이트되도록 페이지를 새로 고침하십시오.

S3 API 인증서 다운로드 또는 복사

S3 API 인증서 내용을 저장하거나 복사하여 다른 곳에서 사용할 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 복사하십시오.

인증서 파일 또는 **CA** 번들 다운로드

인증서 또는 CA 번들 `.pem` 파일을 다운로드하십시오. 선택 사항인 CA 번들을 사용하는 경우 번들에 포함된 각 인증서가 별도의 하위 탭에 표시됩니다.

a. 인증서 다운로드 또는 *CA 번들 다운로드*를 선택합니다.

   CA 번들을 다운로드하는 경우, CA 번들의 보조 탭에 있는 모든 인증서가 단일 파일로 다운로드됩니다.

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

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서 또는 **CA** 번들 **PEM** 복사

인증서 텍스트를 복사하여 다른 곳에 붙여넣으세요. 선택 사항인 CA 번들을 사용하는 경우, 번들에 포함된 각 인증서는 별도의 하위 탭에 표시됩니다.

a. 인증서 **PEM** 복사 또는 *CA 번들 PEM 복사*를 선택합니다.

   CA 번들을 복사하는 경우 CA 번들의 보조 탭에 있는 모든 인증서가 함께 복사됩니다.

b. 복사한 인증서를 텍스트 편집기에 붙여넣으세요.

c. 텍스트 파일을 확장자 `.pem`로 저장하세요.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

관련 정보

- "S3 REST API 사용"
- "S3 엔드포인트 도메인 이름 구성"

StorageGRID Grid CA 인증서를 복사합니다

StorageGRID 내부 트래픽 보안을 위해 자체 인증 기관(CA)을 사용합니다. 사용자가 자체 인증서를 업로드하더라도 이 인증서는 변경되지 않습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.

이 작업 정보

사용자 지정 서버 인증서가 구성된 경우 클라이언트 애플리케이션은 사용자 지정 서버 인증서를 사용하여 서버를 확인해야 합니다. StorageGRID 시스템의 CA 인증서를 복사해서는 안 됩니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *그리드 **CA** 탭을 선택합니다.
2. **PEM** 인증서 섹션에서 인증서를 다운로드하거나 복사합니다.

인증서 파일 다운로드

인증서 `.pem` 파일을 다운로드하세요.

a. *인증서 다운로드*를 선택합니다.

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

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서 **PEM** 복사

인증서 텍스트를 복사하여 다른 곳에 붙여넣으십시오.

a. *인증서 PEM 복사*를 선택합니다.

b. 복사한 인증서를 텍스트 편집기에 붙여넣으세요.

c. 텍스트 파일을 확장자 `.pem`로 저장하세요.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

FabricPool을 위한 **StorageGRID** 인증서 구성

엄격한 호스트 이름 유효성 검사를 수행하고 엄격한 호스트 이름 유효성 검사 비활성화를 지원하지 않는 S3 클라이언트(예: FabricPool를 사용하는 ONTAP 클라이언트)의 경우, 로드 밸런서 엔드포인트를 구성할 때 서버 인증서를 생성하거나 업로드할 수 있습니다.

시작하기 전에

- "특정 액세스 권한"이(가) 있습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.

이 작업 정보

로드 밸런싱 엔드포인트를 생성할 때 자체 서명된 서버 인증서를 생성하거나 공인 인증 기관(CA)에서 서명한 인증서를 업로드할 수 있습니다. 운영 환경에서는 공인 CA에서 서명한 인증서를 사용하는 것이 좋습니다. CA에서 서명한 인증서는 서비스 중단 없이 교체할 수 있습니다. 또한 중간자 공격에 대한 방어력이 뛰어나 보안성이 더욱 강화됩니다.

다음 단계는 FabricPool을 사용하는 S3 클라이언트에 대한 일반적인 지침을 제공합니다. 자세한 정보 및 절차는 "StorageGRID를 FabricPool에 대해 구성합니다"을 참조하십시오.

단계

1. 선택적으로 FabricPool이 사용할 고가용성(HA) 그룹을 구성할 수 있습니다.
2. FabricPool이 사용할 S3 로드 밸런서 엔드포인트를 생성합니다.

   HTTPS 로드 밸런서 엔드포인트를 생성할 때 서버 인증서, 인증서 개인 키 및 선택 사항인 CA 번들을 업로드하라는 메시지가 표시됩니다.

3. StorageGRID를 ONTAP의 클라우드 계층으로 연결합니다.

로드 밸런서 엔드포인트 포트와 업로드한 CA 인증서에 사용된 정규화된 도메인 이름을 지정하십시오. 그런 다음 CA 인증서를 제공하십시오.

중간 CA가 StorageGRID 인증서를 발급한 경우, 해당 중간 CA 인증서를 제공해야 합니다. StorageGRID 인증서가 루트 CA에서 직접 발급된 경우, 루트 CA 인증서를 제공해야 합니다.

StorageGRID에서 클라이언트 인증서 구성

클라이언트 인증서를 사용하면 승인된 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있으므로 외부 도구가 StorageGRID를 모니터링할 수 있는 안전한 방법을 제공합니다.

외부 모니터링 도구를 사용하여 StorageGRID에 액세스해야 하는 경우 Grid Manager를 사용하여 클라이언트 인증서를 업로드하거나 생성한 다음 해당 인증서 정보를 외부 도구에 복사해야 합니다.

"보안 인증서 관리" 및 "사용자 지정 서버 인증서 구성"을(를) 참조하십시오.

서버 인증서 오류로 인해 운영이 중단되는 것을 방지하기 위해, 해당 서버 인증서의 만료일이 다가오면 인증서 페이지에서 구성된 클라이언트 인증서 만료 알림이 표시됩니다. 필요에 따라 구성 > 보안 > *인증서*를 선택하고 클라이언트 탭에서 클라이언트 인증서의 만료일을 확인하여 현재 인증서의 만료일을 확인할 수 있습니다.

특수 구성된 어플라이언스 노드의 데이터를 보호하기 위해 키 관리 서버(KMS)를 사용하는 경우, "KMS 클라이언트 인증서 업로드"에 대한 특정 정보를 참조하십시오.

시작하기 전에

- 루트 액세스 권한이 있습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 클라이언트 인증서를 구성하려면:
  - 관리 노드의 IP 주소 또는 도메인 이름을 알고 있습니다.
  - StorageGRID 관리 인터페이스 인증서를 구성한 경우, 관리 인터페이스 인증서를 구성하는 데 사용된 CA, 클라이언트 인증서 및 개인 키를 보유하고 있습니다.
  - 자체 인증서를 업로드하려면 인증서의 개인 키가 로컬 컴퓨터에 있어야 합니다.
  - 개인 키는 생성 당시 저장 또는 기록되어 있어야 합니다. 원래 개인 키가 없는 경우 새 개인 키를 생성해야 합니다.
- 클라이언트 인증서를 편집하려면:
  - 관리 노드의 IP 주소 또는 도메인 이름을 알고 있습니다.
  - 자신의 인증서 또는 새 인증서를 업로드하려면 개인 키, 클라이언트 인증서 및 CA(사용하는 경우)가 로컬 컴퓨터에 있어야 합니다.

클라이언트 인증서 추가

클라이언트 인증서를 추가하려면 다음 절차 중 하나를 사용하십시오.

- 관리 인터페이스 인증서가 이미 구성되었습니다.

- CA에서 발급한 클라이언트 인증서
- Grid Manager에서 생성된 인증서

관리 인터페이스 인증서가 이미 구성되었습니다.

고객이 제공한 CA, 클라이언트 인증서 및 개인 키를 사용하여 관리 인터페이스 인증서가 이미 구성된 경우 이 절차를 사용하여 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 허용*을 선택하십시오.
5. *Continue*를 선택합니다.
6. 인증서 첨부 단계에서는 관리 인터페이스 인증서를 업로드하십시오.
   a. *인증서 업로드*를 선택합니다.
   b. *찾아보기*를 선택하고 관리 인터페이스 인증서 파일을 선택하십시오((`.pem`).
      - 클라이언트 인증서 세부 정보(**Client certificate details**)를 선택하면 인증서 메타데이터와 인증서 PEM이 표시됩니다.
      - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 *인증서 PEM 복사*를 선택하십시오.
   c. 그리드 관리자에 인증서를 저장하려면 *생성*을 선택하십시오.

      새 인증서는 클라이언트 탭에 나타납니다.
7. 외부 모니터링 도구 구성(예: Grafana).

CA에서 발급한 클라이언트 인증서

관리 인터페이스 인증서가 구성되지 않았고 CA에서 발급한 클라이언트 인증서와 개인 키를 사용하는 Prometheus용 클라이언트 인증서를 추가하려는 경우 이 절차를 사용하여 관리자 클라이언트 인증서를 추가하십시오.

단계

1. 다음 단계를 수행하십시오"관리 인터페이스 인증서 구성".
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 허용*을 선택하십시오.
6. *Continue*를 선택합니다.
7. 인증서 첨부 단계에서는 클라이언트 인증서, 개인 키 및 CA 번들 파일을 업로드하십시오.
   a. *인증서 업로드*를 선택합니다.
   b. [찾아보기]를 선택하고 클라이언트 인증서, 개인 키 및 CA 번들 파일을 선택합니다(`.pem`).

- 클라이언트 인증서 세부 정보(**Client certificate details**)를 선택하면 인증서 메타데이터와 인증서 PEM이 표시됩니다.
- 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 *인증서 PEM 복사*를 선택하십시오.

c. 그리드 관리자에 인증서를 저장하려면 *생성*을 선택하십시오.

새 인증서는 클라이언트 탭에 나타납니다.

8. 외부 모니터링 도구 구성(예: Grafana).

Grid Manager에서 생성된 인증서

관리 인터페이스 인증서가 구성되지 않았고 Grid Manager의 인증서 생성 기능을 사용하여 Prometheus용 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 허용*을 선택하십시오.
5. *Continue*를 선택합니다.
6. 인증서 첨부 단계에서는 *인증서 생성*을 선택하십시오.
7. 인증서 정보를 지정합니다:
   - **Subject** (선택 사항): X.509 인증서 소유자의 주체 또는 고유 이름(DN).
   - 유효 기간: 생성된 인증서가 생성된 시점부터 유효한 일수입니다.
   - 키 사용 확장 추가: 이 옵션을 선택하면(기본값이며 권장됨), 생성된 인증서에 키 사용 및 확장 키 사용 확장 기능이 추가됩니다.

     이러한 확장 기능은 인증서에 포함된 키의 용도를 정의합니다.

     인증서에 이러한 확장자가 포함된 경우 이전 클라이언트와의 연결 문제가 발생하지 않는다면 이 확인란을 선택한 상태로 두십시오.

8. *생성*을 선택합니다.
9. *클라이언트 인증서 세부 정보*를 선택하면 인증서 메타데이터와 인증서 PEM이 표시됩니다.

   이 대화 상자를 닫으면 인증서 개인 키를 볼 수 없습니다. 키를 복사하거나 다운로드하여 안전한 위치에 보관하십시오.

   - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 *인증서 PEM 복사*를 선택하십시오.
   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택합니다.

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

예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

- 인증서 개인 키를 복사하여 다른 곳에 붙여넣으려면 *개인 키 복사*를 선택합니다.
- 개인 키를 파일로 저장하려면 *개인 키 다운로드*를 선택합니다.

  개인 키 파일 이름과 다운로드 위치를 지정하십시오.

10. 그리드 관리자에 인증서를 저장하려면 *생성*을 선택하십시오.

    새 인증서는 클라이언트 탭에 나타납니다.

11. 그리드 관리자에서 구성 > 보안 > 인증서*를 선택한 다음 *전역 탭을 선택합니다.
12. *관리 인터페이스 인증서*를 선택하십시오.
13. *사용자 지정 인증서 사용*을 선택합니다.
14. 클라이언트 인증서 세부 정보 단계에서 certificate.pem 및 private_key.pem 파일을 업로드합니다. CA 번들을 업로드할 필요가 없습니다.
    a. *인증서 업로드*를 선택한 다음 *계속*을 선택합니다.
    b. 각 인증서 파일을 업로드하세요(`.pem`).
    c. 그리드 관리자에 인증서를 저장하려면 *저장*을 선택하십시오.

       새 인증서는 관리 인터페이스 인증서 페이지에 나타납니다.

15. 외부 모니터링 도구 구성(예: Grafana).

외부 모니터링 도구 구성

단계

1. Grafana와 같은 외부 모니터링 도구에서 다음 설정을 구성하십시오.
   a. 이름: 연결에 사용할 이름을 입력합니다.

      StorageGRID는 이 정보를 요구하지 않지만, 연결을 테스트하려면 이름을 제공해야 합니다.

   b. **URL**: 관리 노드의 도메인 이름 또는 IP 주소를 입력하십시오. HTTPS 및 포트 9091을 지정하십시오.

      예를 들면 다음과 같습니다. `https://admin-node.example.com:9091`

   c. **TLS** 클라이언트 인증 및 *CA 인증서 사용*을 활성화하십시오.
   d. TLS/SSL 인증 세부 정보 아래에 다음을 복사하여 붙여넣습니다:
      - 관리 인터페이스 CA 인증서를 **CA Cert**로
      - 클라이언트 인증서를 **Client Cert**로 설정합니다.
      - 클라이언트 키의 개인 키
   e. **ServerName**: 관리 노드의 도메인 이름을 입력하십시오.

      ServerName은 관리 인터페이스 인증서에 표시된 도메인 이름과 일치해야 합니다.

2. StorageGRID 또는 로컬 파일에서 복사한 인증서와 개인 키를 저장하고 테스트하십시오.

이제 외부 모니터링 도구를 사용하여 StorageGRID의 Prometheus 메트릭에 액세스할 수 있습니다.

측정 기준에 대한 자세한 내용은 "StorageGRID 모니터링 지침"을 참조하십시오.

클라이언트 인증서 편집

관리자 클라이언트 인증서를 편집하여 이름을 변경하거나, Prometheus 액세스를 활성화 또는 비활성화하거나, 현재 인증서가 만료된 경우 새 인증서를 업로드할 수 있습니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.

   인증서 만료일과 Prometheus 액세스 권한이 표에 나열되어 있습니다. 인증서 만료일이 임박했거나 이미 만료된 경우 표에 메시지가 표시되고 경고가 발생합니다.

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 허용*을 선택하십시오.
6. 그리드 관리자에 인증서를 저장하려면 *계속*을 선택하십시오.

   업데이트된 인증서는 클라이언트 탭에 표시됩니다.

새 클라이언트 인증서 첨부

현재 인증서가 만료되면 새 인증서를 업로드할 수 있습니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.

   인증서 만료일과 Prometheus 액세스 권한이 표에 나열되어 있습니다. 인증서 만료일이 임박했거나 이미 만료된 경우 표에 메시지가 표시되고 경고가 발생합니다.

2. 편집할 인증서를 선택합니다.
3. *편집*을 선택한 다음 편집 옵션을 선택합니다.

인증서 업로드

인증서 텍스트를 복사하여 다른 곳에 붙여넣으십시오.

a. *인증서 업로드*를 선택한 다음 *계속*을 선택합니다.

b. 클라이언트 인증서 이름을 업로드합니다(`.pem`).

   클라이언트 인증서 세부 정보(**Client certificate details**)를 선택하면 인증서 메타데이터와 인증서 PEM이 표시됩니다.

   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택합니다.

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

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

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

c. 그리드 관리자에 인증서를 저장하려면 *생성*을 선택하십시오.

   업데이트된 인증서는 클라이언트 탭에 표시됩니다.

인증서 생성

인증서 텍스트를 생성하여 다른 곳에 붙여넣으세요.

a. *인증서 생성*을 선택합니다.

b. 인증서 정보를 지정합니다:

   - **Subject** (선택 사항): X.509 인증서 소유자의 주체 또는 고유 이름(DN).
   - 유효 기간: 생성된 인증서가 생성된 시점부터 유효한 일수입니다.
   - 키 사용 확장 추가: 이 옵션을 선택하면(기본값이며 권장됨), 생성된 인증서에 키 사용 및 확장 키 사용 확장 기능이 추가됩니다.

     이러한 확장 기능은 인증서에 포함된 키의 용도를 정의합니다.

     인증서에 이러한 확장자가 포함된 경우 이전 클라이언트와의 연결 문제가 발생하지 않는다면 이 확인란을 선택한 상태로 두십시오.

c. *생성*을 선택합니다.

d. 클라이언트 인증서 세부 정보(**Client certificate details**)를 선택하면 인증서 메타데이터와 인증서 PEM이 표시됩니다.

   이 대화 상자를 닫으면 인증서 개인 키를 볼 수 없습니다. 키를 복사하거나 다운로드하여 안전한 위치에 보관하십시오.

   - 인증서 내용을 복사하여 다른 곳에 붙여넣으려면 *인증서 PEM 복사*를 선택하십시오.
   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택합니다.

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

예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

- 인증서 개인 키를 복사하여 다른 곳에 붙여넣으려면 *개인 키 복사*를 선택합니다.
- 개인 키를 파일로 저장하려면 *개인 키 다운로드*를 선택합니다.

  개인 키 파일 이름과 다운로드 위치를 지정하십시오.

e. 그리드 관리자에 인증서를 저장하려면 *생성*을 선택하십시오.

새 인증서는 클라이언트 탭에 나타납니다.

클라이언트 인증서 다운로드 또는 복사

클라이언트 인증서를 다운로드하거나 복사하여 다른 곳에서 사용할 수 있습니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.
2. 복사하거나 다운로드할 인증서를 선택합니다.
3. 인증서를 다운로드하거나 복사합니다.

인증서 파일 다운로드

인증서 `.pem` 파일을 다운로드하세요.

a. *인증서 다운로드*를 선택합니다.
b. 인증서 파일 이름과 다운로드 위치를 지정하십시오. 파일을 확장자 `.pem`로 저장하십시오.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서 복사

인증서 텍스트를 복사하여 다른 곳에 붙여넣으십시오.

a. *인증서 PEM 복사*를 선택합니다.
b. 복사한 인증서를 텍스트 편집기에 붙여넣으세요.
c. 텍스트 파일을 확장자 `.pem`로 저장하세요.

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

클라이언트 인증서 제거

관리자 클라이언트 인증서가 더 이상 필요하지 않으면 삭제할 수 있습니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.
2. 삭제할 인증서를 선택합니다.
3. *삭제*를 선택한 다음 확인합니다.

> 최대 10개의 인증서를 제거하려면 클라이언트 탭에서 제거할 각 인증서를 선택한 다음 작업 > *삭제*를 선택하십시오.

인증서가 제거된 후에는 해당 인증서를 사용하던 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스하려면 새 클라이언트 인증서를 지정해야 합니다.

${post_edited_translations.segment}

StorageGRID에서 **TLS** 및 **SSH** 정책 관리

TLS 및 SSH 정책은 클라이언트 애플리케이션과의 안전한 TLS 연결 및 내부 StorageGRID 서비스와의 안전한 SSH 연결을 설정하는 데 사용되는 프로토콜과 암호화 방식을 결정합니다.

보안 정책은 TLS 및 SSH를 사용하여 전송 중인 데이터를 암호화하는 방식을 제어합니다. 일반적으로 시스템이 Common Criteria를 준수해야 하거나 다른 암호화 방식을 사용해야 하는 경우가 아니라면 최신 호환성(기본값) 정책을 사용하는 것이 좋습니다.

> 일부 StorageGRID 서비스는 이러한 정책에 포함된 암호화 방식을 사용하도록 업데이트되지 않았습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"

보안 정책을 선택합니다

단계

1. 구성 > 보안 > *보안 설정*을 선택합니다.

   TLS 및 **SSH** 정책 탭에는 사용 가능한 정책이 표시됩니다. 현재 활성화된 정책은 정책 타일에 녹색 체크 표시로 나타납니다.

2. 각 탭을 검토하여 사용 가능한 정책에 대해 알아보십시오.

최신 호환성(기본값)

강력한 암호화가 필요하고 특별한 요구 사항이 없는 경우 기본 정책을 사용하십시오. 이 정책은 대부분의 TLS 및 SSH 클라이언트와 호환됩니다.

레거시 호환성

이전 클라이언트와의 추가 호환성 옵션이 필요한 경우 레거시 호환성 정책을 사용하십시오. 이 정책의 추가 옵션으로 인해 최신 호환성 정책보다 보안성이 떨어질 수 있습니다.

공통 기준

공통 기준(Common Criteria) 인증이 필요한 경우 공통 기준 정책을 사용하십시오.

FIPS 엄격

Common Criteria 인증이 필요하고 외부 클라이언트가 로드 밸런서 엔드포인트, Tenant Manager 및 Grid Manager에 연결할 때 NetApp Cryptographic Security Module(NCSM) 3.0.8 또는 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 모듈을 사용해야 하는 경우 FIPS 엄격 정책을 사용하십시오. 이 정책을 사용하면 성능이 저하될 수 있습니다.

NCSM 3.0.8 및 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 모듈은 다음 작업에 사용됩니다.

- NCSM
  - 다음 서비스 간의 TLS 연결: ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw 및 cache-svc
  - 클라이언트와 nginx-gw 서비스(로드 밸런서 엔드포인트) 간의 TLS 연결
  - 클라이언트와 LDR 서비스 간의 TLS 연결
  - SSE-S3, SSE-C 및 저장된 객체 암호화 설정에 대한 객체 콘텐츠 암호화
  - SSH 연결

  자세한 내용은 NIST Cryptographic Algorithm Validation Program "인증서 번호 4838"을 참조하십시오.

- NetApp StorageGRID 커널 암호화 API 모듈

  NetApp StorageGRID 커널 암호화 API 모듈은 VM 및 StorageGRID 어플라이언스 플랫폼에서만 사용할 수 있습니다.

  - 엔트로피 수집
  - 노드 암호화

  자세한 내용은 NIST 암호화 알고리즘 검증 프로그램 "인증서 #A6242 ~ #A6257" 및 "엔트로피 인증서 #E223"을 참조하십시오.

참고: 이 정책을 선택하면 "롤링 재부팅 수행"모든 노드에서 NCSM이 활성화됩니다. 재부팅을 시작하고 모니터링하려면 유지 관리 > *롤링 재부팅*을 사용하십시오.

사용자 지정

사용자 지정 암호화 방식을 적용해야 하는 경우 사용자 지정 정책을 생성하십시오.

선택적으로, StorageGRID에 FIPS 140 암호화 요구 사항이 있는 경우 FIPS 모드 기능을 활성화하여 NCSM 3.0.8 및 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 모듈을 사용할 수 있습니다.

a. `fipsMode` 매개변수를 `true`로 설정합니다.

b. 메시지가 표시되면 "롤링 재부팅 수행" 모든 노드에서 암호화 모듈을 활성화하십시오. 재부팅을 시작하고 모니터링하려면 **Maintenance** > *Rolling reboot*을 사용하십시오.

c. 지원 > *진단*을 선택하여 현재 활성화된 FIPS 모듈 버전을 확인하십시오.

3. 각 정책의 암호화 방식, 프로토콜 및 알고리즘에 대한 자세한 내용을 보려면 *세부 정보 보기*를 선택하십시오.
4. 현재 정책을 변경하려면 *정책 사용*을 선택합니다.

   정책 타일의 현재 정책 옆에 녹색 체크 표시가 나타납니다.

사용자 지정 보안 정책 생성

사용자 지정 암호화 방식을 적용해야 하는 경우 사용자 지정 정책을 만들 수 있습니다.

단계

1. 생성하려는 사용자 지정 정책과 가장 유사한 정책의 타일에서 *세부 정보 보기*를 선택합니다.
2. *클립보드에 복사*를 선택한 다음 *취소*를 선택합니다.

3. 사용자 지정 정책 타일에서 *구성 및 사용*을 선택합니다.
4. 복사한 JSON을 붙여넣고 필요한 변경 사항을 적용하십시오.
5. *사용 정책*을 선택합니다.

   사용자 지정 정책 타일에서 현재 정책 옆에 녹색 체크 표시가 나타납니다.

6. 필요에 따라 *구성 편집*을 선택하여 새 사용자 지정 정책을 추가로 변경할 수 있습니다.

일시적으로 기본 보안 정책으로 되돌리기

사용자 지정 보안 정책을 구성한 경우, 구성된 TLS 정책이 "구성된 서버 인증서"와 호환되지 않으면 Grid Manager에 로그인하지 못할 수 있습니다.

일시적으로 기본 보안 정책으로 되돌릴 수 있습니다.

단계

1. 관리자 노드에 로그인합니다.
   a. 다음 명령을 입력합니다. `ssh admin@Admin_Node_IP`
   b. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.
   c. 루트 권한으로 전환하려면 다음 명령을 입력하십시오. `su -`
   d. `Passwords.txt` 파일에 나와 있는 비밀번호를 입력하십시오.

      루트 계정으로 로그인하면 프롬프트가 `$`에서 `#`로 변경됩니다.
2. 다음 명령을 실행합니다.

   ```
   restore-default-cipher-configurations
   ```
3. 웹 브라우저를 통해 동일한 관리 노드에서 그리드 관리자에 접속합니다.
4. 보안 정책을 선택합니다의 단계에 따라 정책을 다시 구성하십시오.

StorageGRID 네트워크 및 객체 보안을 구성합니다

저장된 객체를 암호화하거나, 특정 S3 요청을 차단하거나, 클라이언트가 스토리지 노드에 연결할 때 HTTPS 대신 HTTP를 사용하도록 허용하는 등 네트워크 및 객체 보안을 구성할 수 있습니다.

저장된 객체 암호화

저장된 객체 암호화 기능을 사용하면 S3를 통해 수집되는 모든 객체 데이터를 암호화할 수 있습니다. 기본적으로 저장된 객체는 암호화되지 않지만, AES-128 또는 AES-256 암호화 알고리즘을 사용하여 객체를 암호화하도록 선택할 수 있습니다. 이 설정을 활성화하면 새로 수집되는 모든 객체가 암호화되지만 기존에 저장된 객체는 변경되지 않습니다. 암호화를 비활성화하면 현재 암호화된 객체는 계속 암호화된 상태로 유지되지만 새로 수집되는 객체는 암호화되지 않습니다.

저장된 객체 암호화 설정은 버킷 수준 또는 객체 수준 암호화로 암호화되지 않은 S3 객체에만 적용됩니다.

StorageGRID 암호화 방법에 대한 자세한 내용은 "StorageGRID 암호화 방법 검토"을 참조하십시오.

클라이언트 수정 방지

클라이언트 수정 방지는 시스템 전체 설정입니다. 클라이언트 수정 방지 옵션을 선택하면 다음 요청이 거부됩니다.

S3 REST API

- DeleteBucket 요청
- 기존 객체의 데이터, 사용자 정의 메타데이터 또는 S3 객체 태깅을 수정하려는 모든 요청

스토리지 노드 연결에 **HTTP** 활성화

기본적으로 클라이언트 애플리케이션은 스토리지 노드에 직접 연결할 때 HTTPS 네트워크 프로토콜을 사용합니다. 필요에 따라 비운영 그리드를 테스트할 때와 같이 이러한 연결에 HTTP를 활성화할 수도 있습니다.

S3 클라이언트가 스토리지 노드에 직접 HTTP 연결을 해야 하는 경우에만 스토리지 노드 연결에 HTTP를 사용하십시오. HTTPS 연결만 사용하는 클라이언트 또는 로드 밸런서 서비스에 연결하는 클라이언트의 경우("각 로드 밸런서 엔드포인트 구성"HTTP 또는 HTTPS를 사용하도록 구성할 수 있으므로) 이 옵션을 사용할 필요가 없습니다.

"요약: 클라이언트 연결을 위한 IP 주소 및 포트"을 참조하여 S3 클라이언트가 HTTP 또는 HTTPS를 사용하여 스토리지 노드에 연결할 때 사용하는 포트를 알아보십시오.

옵션을 선택합니다

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 루트 액세스 권한이 있습니다.

단계

1. 구성 > 보안 > *보안 설정*을 선택합니다.
2. 네트워크 및 개체 탭을 선택합니다.
3. 저장된 객체 암호화의 경우, 저장된 객체를 암호화하지 않으려면 없음(기본값) 설정을 사용하고, 저장된 객체를 암호화하려면 **AES-128** 또는 *AES-256*을 선택하십시오.
4. S3 클라이언트가 특정 요청을 하지 못하도록 하려면 *클라이언트 수정 방지*를 선택적으로 지정할 수 있습니다.

> 이 설정을 변경하면 새 설정이 적용되는 데 약 1분이 소요됩니다. 구성된 값은 성능 및 확장성을 위해 캐시됩니다.

5. 클라이언트가 스토리지 노드에 직접 연결하고 HTTP 연결을 사용하려는 경우 스토리지 노드 연결에 **HTTP** 사용 을 선택적으로 선택할 수 있습니다.

> 운영 환경의 그리드에서 HTTP를 활성화할 때는 요청이 암호화되지 않은 상태로 전송되므로 주의해야 합니다.

6. *저장*을 선택하세요.

StorageGRID 인터페이스 보안 설정을 변경합니다

인터페이스 보안 설정을 통해 사용자가 지정된 시간 이상 활동이 없을 경우 로그아웃되는지 여부와 API 오류 응답에 스택 추적을 포함할지 여부를 제어할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "루트 액세스 권한"이(가) 있습니다.

이 작업 정보

보안 설정 페이지에는 브라우저 비활성 시간 초과 및 관리 **API** 스택 추적 설정이 포함되어 있습니다.

브라우저 비활성 시간 초과

사용자가 로그아웃되기 전에 브라우저가 비활성 상태로 유지될 수 있는 시간을 나타냅니다. 기본값은 15분입니다.

브라우저 비활성 시간 초과는 다음 요소에 의해서도 제어됩니다.

- 시스템 보안을 위해 별도의 구성 불가능한 StorageGRID 타이머가 포함되어 있습니다. 각 사용자의 인증 토큰은 사용자가 로그인한 후 16시간이 지나면 만료됩니다. 사용자 인증이 만료되면 브라우저 비활성 시간 초과가 비활성화되었거나 브라우저 시간 초과 값에 아직 도달하지 않았더라도 해당 사용자는 자동으로 로그아웃됩니다. 토큰을 갱신하려면 사용자는 다시 로그인해야 합니다.
- StorageGRID에 대해 SSO(Single Sign-On)가 활성화된 경우 ID 공급자에 대한 타임아웃 설정입니다.

  SSO가 활성화된 경우 사용자의 브라우저 시간 초과가 발생하면 사용자는 StorageGRID에 다시 액세스하려면 SSO 자격 증명을 다시 입력해야 합니다. 을(를) 참조하십시오. "SSO 작동 방식".

관리 **API** 스택 트레이스

Grid Manager 및 Tenant Manager API 오류 응답에 스택 트레이스를 반환할지 여부를 제어합니다.

이 옵션은 기본적으로 비활성화되어 있지만 테스트 환경에서는 이 기능을 활성화할 수 있습니다. 일반적으로 프로덕션 환경에서는 API 오류 발생 시 내부 소프트웨어 세부 정보가 노출되는 것을 방지하기 위해 스택 추적 기능을 비활성화 상태로 유지하는 것이 좋습니다.

단계

1. 구성 > 보안 > *보안 설정*을 선택합니다.
2. 인터페이스 탭을 선택합니다.
3. 브라우저 비활성 시간 초과 설정을 변경하려면:
   a. 아코디언을 펼치세요.
   b. 타임아웃 기간을 변경하려면 60초에서 7일 사이의 값을 지정하십시오. 기본 타임아웃은 15분입니다.
   c. 이 기능을 비활성화하려면 확인란의 선택을 해제하십시오.
   d. *저장*을 선택하세요.

      새 설정은 현재 로그인한 사용자에게는 영향을 미치지 않습니다. 새 타이머 설정이 적용되려면 사용자는 다시 로그인하거나 브라우저를 새로 고침해야 합니다.
4. 관리 API 스택 추적 설정을 변경하려면 다음 단계를 따르십시오.
   a. 아코디언을 펼치세요.
   b. 그리드 관리자 및 테넌트 관리자 API 오류 응답에 스택 트레이스를 반환하려면 확인란을 선택하십시오.

      API 오류 발생 시 내부 소프트웨어 세부 정보가 노출되는 것을 방지하기 위해 프로덕션 환경에서는 스택 추적 기능을 비활성화하십시오.

   c. *저장*을 선택하세요.

StorageGRID에서 외부 **SSH** 액세스 관리

그리드로 들어오는 트래픽에 대한 SSH 액세스를 외부 액세스 차단 또는 허용으로 관리할 수

있습니다. 외부 SSH 액세스 관리는 그리드 내 노드 간 트래픽에는 영향을 미치지 않습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "루트 액세스 권한"이(가) 있습니다.

이 작업 정보

시스템 보안 강화를 위해 외부 SSH 접속은 기본적으로 차단되어 있습니다. 문제 해결과 같이 인바운드 SSH 접속이 필요한 작업을 수행해야 하는 경우, 외부 접속을 일시적으로 허용하십시오. 작업이 완료되면 외부 접속을 차단하십시오.

단계

1. 구성 > 보안 > *보안 설정*을 선택합니다.
2. **SSH** 차단 탭을 선택합니다.
3. 외부 SSH 액세스를 관리하려면 수신 **SSH** 액세스 차단 옵션을 사용하십시오.
   a. 액세스를 차단하려면 확인란을 선택합니다(기본값).
   b. 액세스를 허용하려면 확인란을 선택 취소하십시오.

   서비스 랩톱과 다른 모든 그리드 노드 간에 22번 포트에 대한 액세스가 필요합니다. 유지 관리 작업이 완료되면 22번 포트에 대한 액세스를 제거하십시오.

4. *저장*을 선택하세요.

키 관리 서버 구성

StorageGRID의 키 관리 서버에 대해 알아보십시오

키 관리 서버(KMS)는 키 관리 상호 운용성 프로토콜(KMIP)을 사용하여 연결된 StorageGRID 사이트의 StorageGRID 어플라이언스 노드에 암호화 키를 제공하는 외부 타사 시스템입니다.

StorageGRID는 특정 키 관리 서버만 지원합니다. 지원되는 제품 및 버전 목록은 "NetApp 상호 운용성 매트릭스 툴(IMT)"을 참조하십시오.

설치 시 노드 암호화 설정이 활성화된 StorageGRID 어플라이언스 노드의 노드 암호화 키를 관리하기 위해 하나 이상의 키 관리 서버를 사용할 수 있습니다. 이러한 어플라이언스 노드에 키 관리 서버를 사용하면 어플라이언스가 데이터 센터에서 제거되더라도 데이터를 보호할 수 있습니다. 어플라이언스 볼륨이 암호화된 후에는 노드가 KMS와 통신할 수 없는 한 어플라이언스의 데이터에 액세스할 수 없습니다.

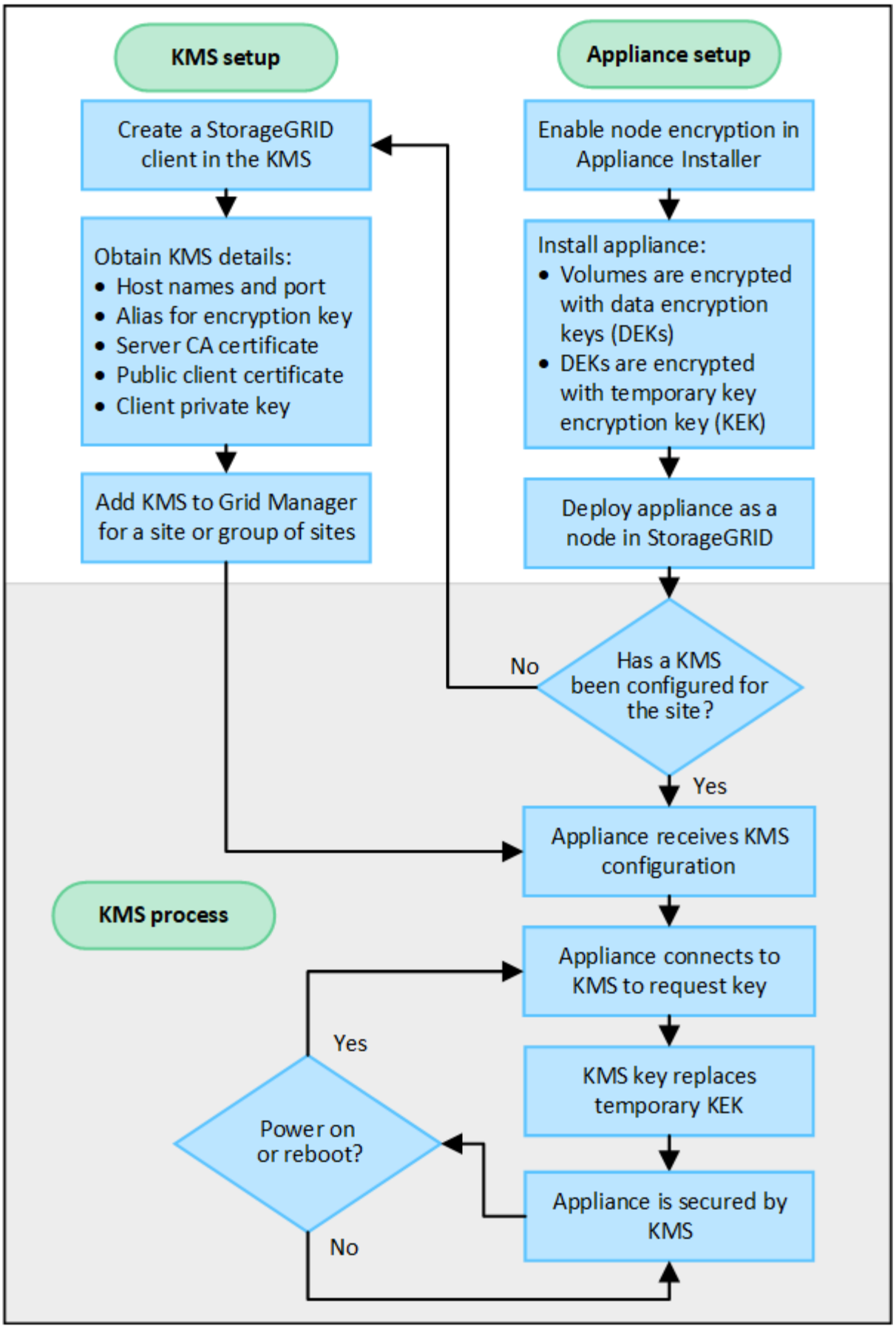
StorageGRID 어플라이언스 노드를 암호화 및 복호화하는 데 사용되는 외부 키를 생성하거나 관리하지 않습니다. StorageGRID 데이터를 보호하기 위해 외부 키 관리 서버를 사용하려는 경우, 해당 서버 설정 방법과 암호화 키 관리 방법을 숙지해야 합니다. 키 관리 작업은 본 설명서의 범위를 벗어납니다. 도움이 필요하면 키 관리 서버 설명서를 참조하거나 기술 지원에 문의하십시오.

StorageGRID 키 관리 서버 및 어플라이언스 구성

StorageGRID 어플라이언스 노드에서 StorageGRID 데이터를 보호하기 위해 키 관리 서버(KMS)를 사용하려면 먼저 두 가지 구성 작업을 완료해야 합니다. 하나 이상의 KMS 서버를

설정하고 어플라이언스 노드에 대한 노드 암호화를 활성화하는 것입니다. 이 두 가지 구성 작업이 완료되면 키 관리 프로세스가 자동으로 진행됩니다.

이 순서도는 KMS를 사용하여 어플라이언스 노드의 StorageGRID 데이터를 보호하는 주요 단계를 보여줍니다.



순서도는 KMS 설정과 어플라이언스 설정이 동시에 진행되는 것을 보여주지만, 요구 사항에 따라 새 어플라이언스

노드에 대한 노드 암호화를 활성화하기 전이나 후에 키 관리 서버를 설정할 수 있습니다.

키 관리 서버(KMS) 설정

키 관리 서버 설정에는 다음과 같은 주요 단계가 포함됩니다.

단계	참조하십시오
KMS 소프트웨어에 액세스하여 각 KMS 또는 KMS 클러스터에 StorageGRID 클라이언트를 추가하십시오.	"KMS에서 StorageGRID를 클라이언트로 구성합니다"
KMS에서 StorageGRID 클라이언트에 필요한 정보를 얻으십시오.	"KMS에서 StorageGRID를 클라이언트로 구성합니다"
그리드 관리자에 KMS를 추가하고, 단일 사이트 또는 기본 사이트 그룹에 할당하고, 필요한 인증서를 업로드하고, KMS 구성을 저장합니다.	"키 관리 서버(KMS) 추가"

어플라이언스를 설정합니다

KMS 사용을 위한 어플라이언스 노드 설정은 다음과 같은 주요 단계를 포함합니다.

1. 어플라이언스 설치의 하드웨어 구성 단계에서 StorageGRID Appliance Installer를 사용하여 어플라이언스에 대한 노드 암호화 설정을 활성화하십시오.

   > 어플라이언스를 그리드에 추가한 후에는 노드 암호화 설정을 활성화할 수 없으며, 노드 암호화가 활성화되지 않은 어플라이언스에는 외부 키 관리를 사용할 수 없습니다.

2. StorageGRID 어플라이언스 설치 프로그램을 실행합니다. 설치 과정에서 다음과 같이 각 어플라이언스 볼륨에 임의의 데이터 암호화 키(DEK)가 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 연결될 때까지 DEK를 암호화하는 임시 키입니다.
3. 어플라이언스 노드를 StorageGRID에 추가합니다.

자세한 내용은 "노드 암호화 활성화"을 참조하십시오.

키 관리 암호화 프로세스(자동으로 발생)

키 관리 암호화에는 자동으로 수행되는 다음과 같은 주요 단계가 포함됩니다.

1. 노드 암호화가 활성화된 어플라이언스를 그리드에 설치하면 StorageGRID는 새 노드가 포함된 사이트에 KMS 구성이 있는지 확인합니다.
   - 사이트에 KMS가 이미 구성되어 있는 경우, 어플라이언스는 KMS 구성을 수신합니다.
   - 사이트에 KMS가 아직 구성되지 않은 경우, 사이트에 KMS를 구성하고 어플라이언스가 KMS 구성을 수신할 때까지 어플라이언스의 데이터는 임시 KEK에 의해 계속 암호화됩니다.

2. 해당 장치는 KMS 구성을 사용하여 KMS에 연결하고 암호화 키를 요청합니다.
3. KMS가 암호화 키를 어플라이언스로 전송합니다. KMS에서 전송된 새 키는 임시 KEK를 대체하며, 이제 어플라이언스 볼륨의 DEK를 암호화 및 복호화하는 데 사용됩니다.

> 암호화된 어플라이언스 노드가 구성된 KMS에 연결되기 전에 존재하는 모든 데이터는 임시 키로 암호화됩니다. 그러나 임시 키가 KMS 암호화 키로 교체될 때까지 어플라이언스 볼륨은 데이터 센터에서 제거되지 않도록 보호되는 것으로 간주해서는 안 됩니다.

4. 기기의 전원이 켜지거나 재부팅되면 KMS에 다시 연결하여 키를 요청합니다. 휘발성 메모리에 저장된 키는 전원 공급이 중단되거나 재부팅되면 손실될 수 있습니다.

StorageGRID 키 관리 서버 요구 사항 및 고려 사항

외부 키 관리 서버(KMS)를 구성하기 전에 고려 사항과 요구 사항을 이해해야 합니다.

지원되는 **KMIP** 버전은 무엇입니까**?**

StorageGRID는 KMIP 버전 1.4를 지원합니다.

"키 관리 상호 운용성 프로토콜 사양 버전 1.4"

네트워크 관련 고려 사항은 무엇인가요**?**

네트워크 방화벽 설정에서 각 어플라이언스 노드가 KMIP(Key Management Interoperability Protocol) 통신에 사용되는 포트를 통해 통신할 수 있도록 허용해야 합니다. KMIP의 기본 포트는 5696입니다.

노드 암호화를 사용하는 각 어플라이언스 노드가 해당 사이트에 대해 구성한 KMS 또는 KMS 클러스터에 네트워크 액세스할 수 있는지 확인해야 합니다.

지원되는 **TLS** 버전은 무엇입니까**?**

어플라이언스 노드와 구성된 KMS 간의 통신은 보안 TLS 연결을 사용합니다. StorageGRID KMS 또는 KMS 클러스터와의 KMIP 연결 시 KMS에서 지원하는 프로토콜 및 "TLS 및 SSH 정책"사용자가 사용하는 프로토콜에 따라 TLS 1.2 또는 TLS 1.3 프로토콜을 지원할 수 있습니다.

StorageGRID는 KMS와 연결할 때 프로토콜 및 암호화(TLS 1.2) 또는 암호화 스위트(TLS 1.3)를 협상합니다. 사용 가능한 프로토콜 버전과 암호화/암호화 스위트를 확인하려면 그리드의 활성 TLS 및 SSH 정책의 `tlsOutbound` 섹션을 참조하십시오(구성 > 보안 보안 설정).

어떤 어플라이언스가 지원됩니까**?**

키 관리 서버(KMS)를 사용하여 노드 암호화 설정이 활성화된 그리드 내 모든 StorageGRID 어플라이언스의 암호화 키를 관리할 수 있습니다. 이 설정은 StorageGRID Appliance Installer를 사용하여 어플라이언스를 설치하는 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 KMS를 StorageGRID 어플라이언스 및 어플라이언스 노드에 사용할 수 있습니다.

다음과 같은 소프트웨어 기반(어플라이언스 이외의) 노드에는 구성된 KMS를 사용할 수 없습니다:

- 가상 머신(VM)으로 배포된 노드
- Linux 호스트의 컨테이너 엔진 내에 배포된 노드

다른 플랫폼에 배포된 노드는 데이터 저장소 또는 디스크 수준에서 StorageGRID 외부의 암호화를 사용할 수 있습니다.

키 관리 서버는 언제 구성해야 합니까?

새로운 설치의 경우, 일반적으로 테넌트를 생성하기 전에 Grid Manager에서 하나 이상의 키 관리 서버를 설정해야 합니다. 이 순서를 따르면 노드에 객체 데이터가 저장되기 전에 노드가 보호됩니다.

어플라이언스 노드를 설치하기 전이나 후에 그리드 관리자에서 키 관리 서버를 구성할 수 있습니다.

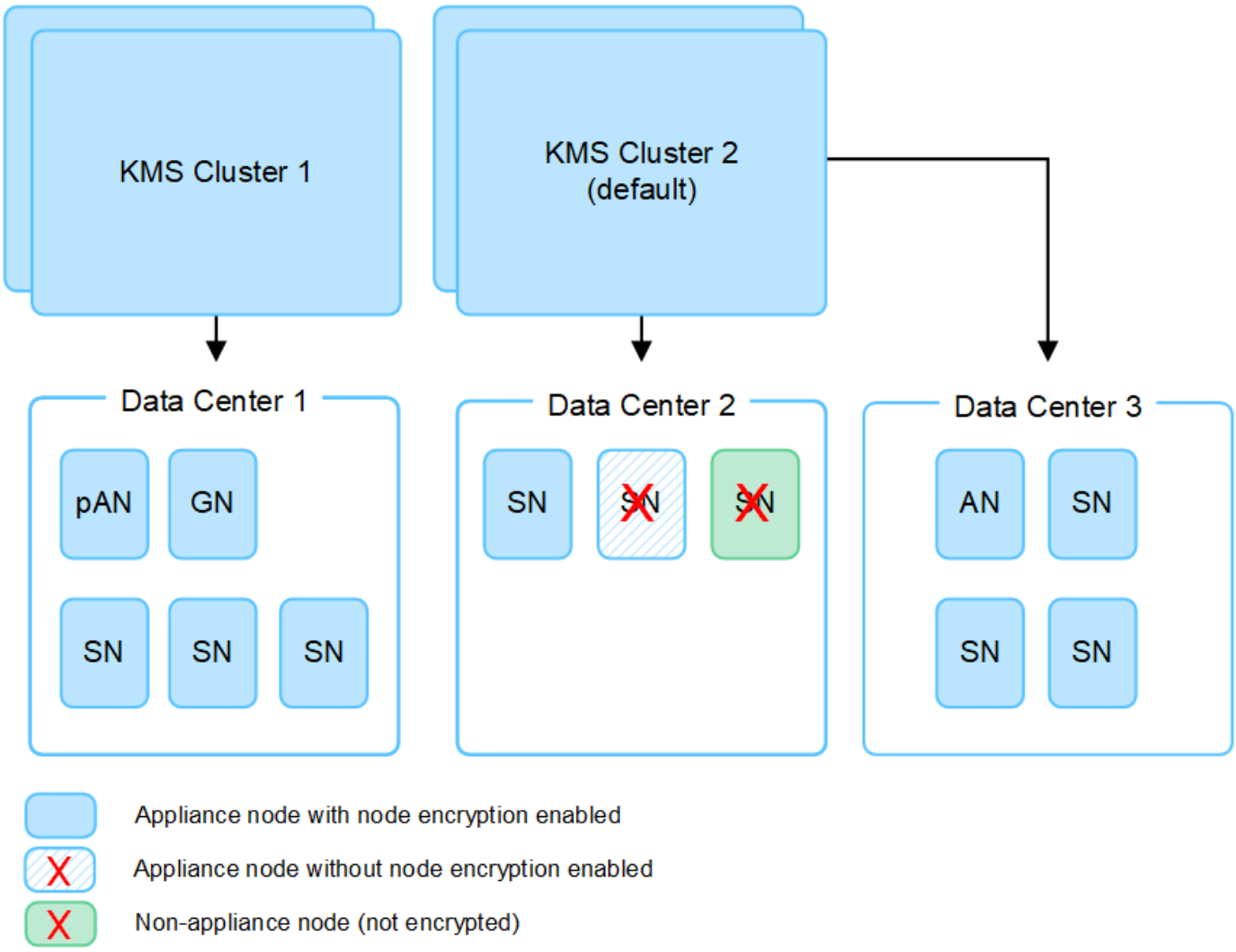
키 관리 서버는 몇 대가 필요합니까?

StorageGRID 시스템의 어플라이언스 노드에 암호화 키를 제공하기 위해 하나 이상의 외부 키 관리 서버(KMS)를 구성할 수 있습니다. 각 KMS는 단일 사이트 또는 여러 사이트에 있는 StorageGRID 어플라이언스 노드에 단일 암호화 키를 제공합니다.

StorageGRID는 KMS 클러스터 사용을 지원합니다. 각 KMS 클러스터는 구성 설정 및 암호화 키를 공유하는 여러 개의 복제된 키 관리 서버를 포함합니다. KMS 클러스터를 키 관리에 사용하면 고가용성 구성의 페일오버 기능이 향상되므로 권장됩니다.

예를 들어, StorageGRID 시스템에 데이터 센터 사이트가 세 개 있다고 가정해 보겠습니다. 첫 번째 KMS 클러스터는 데이터 센터 1의 모든 어플라이언스 노드에 키를 제공하도록 구성하고, 두 번째 KMS 클러스터는 나머지 모든 사이트의 어플라이언스 노드에 키를 제공하도록 구성할 수 있습니다. 두 번째 KMS 클러스터를 추가할 때 데이터 센터 2와 데이터 센터 3에 대한 기본 KMS를 구성할 수 있습니다.

어플라이언스가 아닌 노드 또는 설치 중에 노드 암호화 설정이 활성화되지 않은 어플라이언스 노드에는 KMS를 사용할 수 없습니다.



키를 교체하면 어떻게 됩니까?

보안 모범 사례로서, 구성된 각 KMS에서 사용하는 "암호화 키 교체"을(를) 주기적으로 확인해야 합니다.

새로운 키 버전이 출시되면:

- 해당 키는 KMS와 연결된 사이트의 암호화 어플라이언스 노드에 자동으로 배포됩니다. 배포는 키가 교체된 후 1시간 이내에 이루어져야 합니다.
- 암호화된 어플라이언스 노드가 새 키 버전이 배포될 때 오프라인 상태인 경우, 노드는 재부팅되는 즉시 새 키를 수신하게 됩니다.
- 어떤 이유로든 새 키 버전을 사용하여 어플라이언스 볼륨을 암호화할 수 없는 경우, 어플라이언스 노드에 대해 **KMS** 암호화 키 순환 실패 경고가 발생합니다. 이 경고를 해결하려면 기술 지원팀에 문의해야 할 수 있습니다.

암호화된 어플라이언스 노드를 재사용할 수 있습니까?

암호화된 어플라이언스를 다른 StorageGRID 시스템에 설치해야 하는 경우, 먼저 그리드 노드를 비활성화하여 객체 데이터를 다른 노드로 이동해야 합니다. 그런 다음 StorageGRID 어플라이언스 설치 프로그램을 사용하여 "KMS 구성 지우기". KMS 구성을 지우면 노드 암호화 설정이 비활성화되고 어플라이언스 노드와 StorageGRID 사이트의 KMS 구성 간의 연결이 제거됩니다.

KMS 암호화 키에 액세스할 수 없으면 어플라이언스에 남아 있는 모든 데이터에 더 이상 액세스할 수 없으며 영구적으로 잠깁니다.

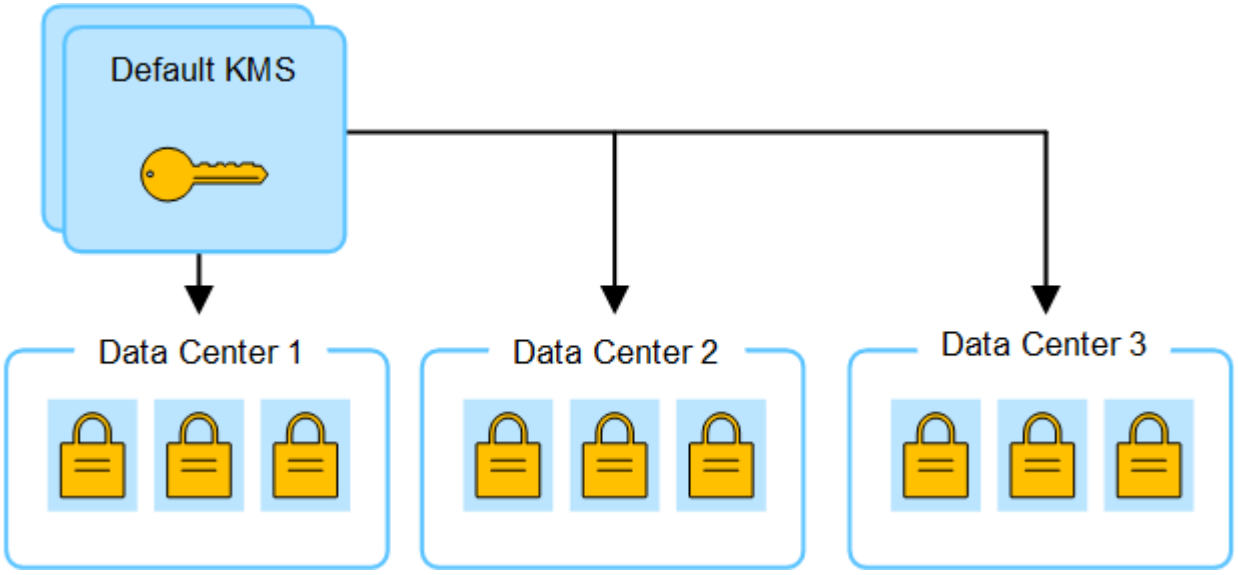
StorageGRID 사이트의 **KMS** 변경 시 고려 사항

각 키 관리 서버(KMS) 또는 KMS 클러스터는 단일 사이트 또는 여러 사이트에 있는 모든 어플라이언스 노드에 암호화 키를 제공합니다. 사이트에서 사용하는 KMS를 변경해야 하는 경우, 한 KMS에서 다른 KMS로 암호화 키를 복사해야 할 수 있습니다.

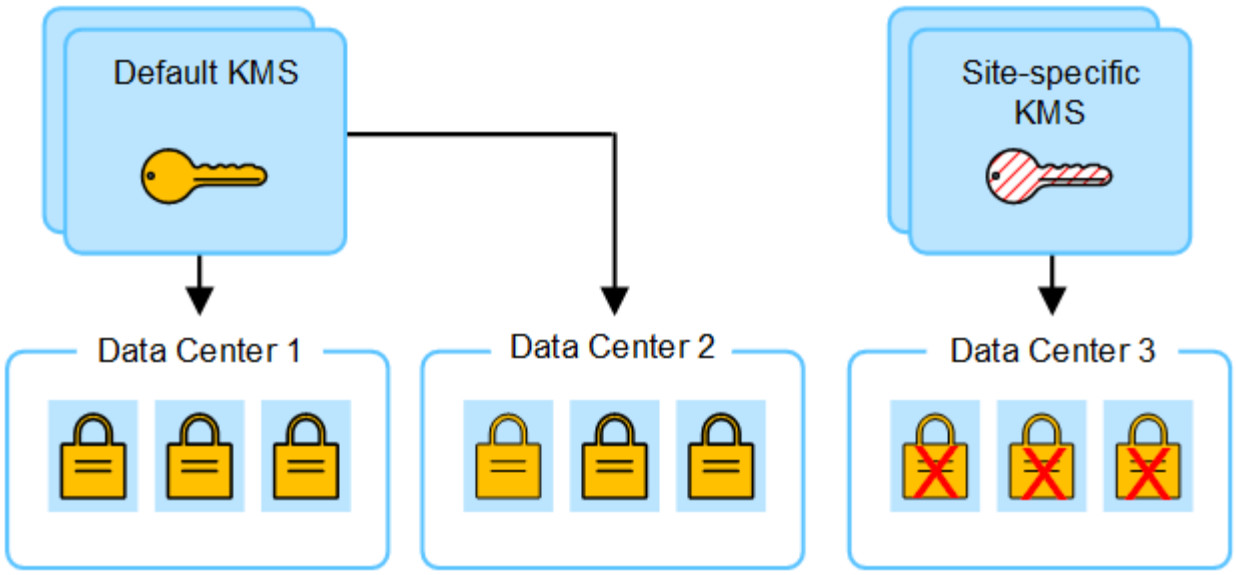
사이트에 사용되는 KMS를 변경하는 경우, 해당 사이트에서 이전에 암호화된 어플라이언스 노드를 새 KMS에 저장된 키를 사용하여 복호화할 수 있는지 확인해야 합니다. 경우에 따라 기존 KMS에서 새 KMS로 현재 버전의 암호화 키를 복사해야 할 수도 있습니다. KMS에 해당 사이트의 암호화된 어플라이언스 노드를 복호화하는 데 필요한 올바른 키가 있는지 반드시 확인해야 합니다.

예를 들면 다음과 같습니다.

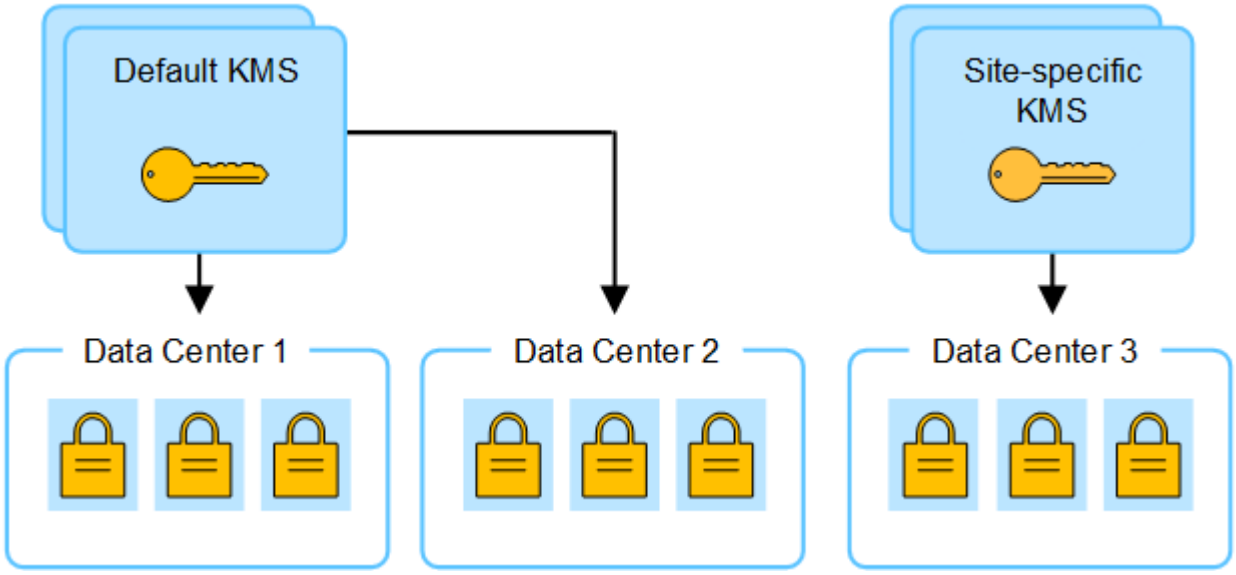
1. 처음에 전용 KMS가 없는 모든 사이트에 적용되는 기본 KMS를 구성합니다.
2. KMS가 저장되면 노드 암호화 설정이 활성화된 모든 어플라이언스 노드가 KMS에 연결하여 암호화 키를 요청합니다. 이 키는 모든 사이트의 어플라이언스 노드를 암호화하는 데 사용됩니다. 또한 동일한 키를 사용하여 해당 어플라이언스를 복호화해야 합니다.



3. 그림에서 데이터 센터 3에 해당하는 한 사이트에 대해 사이트별 KMS를 추가하기로 결정했습니다. 하지만 어플라이언스 노드가 이미 암호화되어 있기 때문에 사이트별 KMS의 구성을 저장하려고 하면 유효성 검사 오류가 발생합니다. 이 오류는 사이트별 KMS에 해당 사이트의 노드를 복호화하는 데 필요한 올바른 키가 없기 때문에 발생합니다.



4. 이 문제를 해결하려면 기본 KMS에서 현재 버전의 암호화 키를 새 KMS로 복사합니다. (엄밀히 말하면, 원래 키를 동일한 별칭을 가진 새 키로 복사하는 것입니다. 원래 키는 새 키의 이전 버전이 됩니다.) 이제 사이트별 KMS에 데이터 센터 3의 어플라이언스 노드를 복호화하는 데 필요한 올바른 키가 있으므로 StorageGRID에 저장할 수 있습니다.



사이트에 사용할 **KMS**를 변경하는 사용 사례

이 표는 사이트의 KMS를 변경하는 가장 일반적인 경우에 필요한 단계를 요약한 것입니다.

사이트 **KMS** 변경 사례	필수 단계
사이트별 KMS 항목이 하나 이상 있으며, 그중 하나를 기본 KMS로 사용하려고 합니다.	사이트별 KMS를 편집합니다. 키 관리 대상 필드에서 *다른 KMS에서 관리되지 않는 사이트(기본 KMS)*를 선택합니다. 이제 사이트별 KMS가 기본 KMS로 사용됩니다. 이는 전용 KMS가 없는 모든 사이트에 적용됩니다. "키 관리 서버(KMS) 편집"

사이트 **KMS** 변경 사례	필수 단계
기본 KMS가 있는 상태에서 확장 기능을 통해 새 사이트를 추가했습니다. 새 사이트에는 기본 KMS를 사용하고 싶지 않습니다.	1. 새 사이트의 어플라이언스 노드가 기본 KMS로 이미 암호화된 경우 KMS 소프트웨어를 사용하여 기본 KMS의 현재 암호화 키 버전을 새 KMS로 복사하십시오. 2. 그리드 관리자를 사용하여 새 KMS를 추가하고 사이트를 선택합니다. "키 관리 서버(KMS) 추가"
사이트의 KMS가 다른 서버를 사용하도록 하려는 경우.	1. 현장의 어플라이언스 노드가 기존 KMS에 의해 이미 암호화된 경우, KMS 소프트웨어를 사용하여 현재 버전의 암호화 키를 기존 KMS에서 새 KMS로 복사하십시오. 2. 그리드 관리자를 사용하여 기존 KMS 구성을 편집하고 새 호스트 이름 또는 IP 주소를 입력합니다. "키 관리 서버(KMS) 추가"

KMS에서 **StorageGRID**를 클라이언트로 구성합니다

KMS를 StorageGRID에 추가하려면 먼저 각 외부 키 관리 서버 또는 KMS 클러스터에 대해 StorageGRID를 클라이언트로 구성해야 합니다.

이 지침은 Thales CipherTrust Manager 및 Hashicorp Vault에 적용됩니다. 지원되는 제품 및 버전 목록은 "NetApp 상호 운용성 매트릭스 툴(IMT)"을 사용하십시오.

단계

1. KMS 소프트웨어에서 사용하려는 각 KMS 또는 KMS 클러스터에 대해 StorageGRID 클라이언트를 생성하십시오.

   각 KMS는 단일 사이트 또는 여러 사이트 그룹에 있는 StorageGRID 어플라이언스 노드에 대한 단일 암호화 키를 관리합니다.

2. 다음 두 가지 방법 중 하나를 사용하여 키를 생성합니다.
   - KMS 제품의 키 관리 페이지를 사용하십시오. 각 KMS 또는 KMS 클러스터에 대해 AES 암호화 키를 생성하십시오.

     암호화 키는 2,048비트 이상이어야 하며, 내보낼 수 있어야 합니다.

   - StorageGRID가 키를 생성하도록 합니다. "클라이언트 인증서 업로드 중" 이후 테스트하고 저장할 때 메시지가 표시됩니다.

3. 각 KMS 또는 KMS 클러스터에 대해 다음 정보를 기록하십시오.

   KMS를 StorageGRID에 추가할 때 이 정보가 필요합니다.

   - 각 서버의 호스트 이름 또는 IP 주소입니다.
   - KMS에서 사용하는 KMIP 포트입니다.
   - KMS에서 암호화 키에 대한 키 별칭입니다.

4. 각 KMS 또는 KMS 클러스터에 대해 인증 기관(CA)에서 서명한 서버 인증서 또는 PEM 형식으로 인코딩된 각 CA 인증서 파일이 인증서 체인 순서대로 연결된 인증서 번들을 확보하십시오.

   서버 인증서를 통해 외부 KMS가 StorageGRID에 자신을 인증할 수 있습니다.

   - 인증서는 개인정보보호 강화 메일(PEM) Base-64 인코딩 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, KMIP 인터페이스는 일반적으로 포트 5696을 사용합니다.

5. 외부 KMS에서 StorageGRID에 발급한 공개 클라이언트 인증서와 해당 클라이언트 인증서의 개인 키를 확보하십시오.

   클라이언트 인증서를 통해 StorageGRID KMS에 자체 인증을 수행할 수 있습니다.

StorageGRID에 키 관리 서버 추가

StorageGRID 키 관리 서버 마법사를 사용하여 각 KMS 또는 KMS 클러스터를 추가합니다.

시작하기 전에

- "키 관리 서버 사용 시 고려 사항 및 요구 사항"를 검토했습니다.
- 귀하는 "KMS에서 StorageGRID를 클라이언트로 구성했습니다.", 그리고 각 KMS 또는 KMS 클러스터에 필요한 정보를 보유하고 있습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"

이 작업 정보

가능하다면, 다른 KMS로 관리되지 않는 모든 사이트에 적용되는 기본 KMS를 구성하기 전에 사이트별 키 관리 서버를 구성하십시오. 기본 KMS를 먼저 생성하면 그리드의 모든 노드 암호화 어플라이언스가 기본 KMS로 암호화됩니다. 나중에 사이트별 KMS를 생성하려면 먼저 기본 KMS에서 현재 버전의 암호화 키를 새 KMS로 복사해야 합니다. 자세한 내용은 "사이트의 KMS를 변경할 때 고려 사항"을 참조하십시오.

1단계**: KMS** 세부 정보

키 관리 서버 추가 마법사의 1단계(KMS 세부 정보)에서는 KMS 또는 KMS 클러스터에 대한 세부 정보를 제공합니다.

단계

1. * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   키 관리 서버 페이지가 구성 세부 정보 탭이 선택된 상태로 나타납니다.

2. *생성*을 선택합니다.

   키 관리 서버 추가 마법사의 1단계(KMS 세부 정보)가 나타납니다.

3. KMS 및 해당 KMS에 구성한 StorageGRID 클라이언트에 대한 다음 정보를 입력하십시오.

필드	설명
KMS 이름	이 KMS를 식별하는 데 도움이 되는 설명적인 이름입니다. 1자에서 64자 사이여야 합니다.
키 이름	KMS의 StorageGRID 클라이언트에 대한 정확한 키 별칭입니다. 1~255자 사이여야 합니다. 참고: KMS 제품을 사용하여 키를 생성하지 않은 경우 StorageGRID에서 키를 생성하라는 메시지가 표시됩니다.
키 관리 대상:	이 KMS와 연결될 StorageGRID 사이트입니다. 가능하면 다른 KMS로 관리되지 않는 모든 사이트에 적용되는 기본 KMS를 구성하기 전에 사이트별 키 관리 서버를 구성해야 합니다. • 이 KMS가 특정 사이트의 어플라이언스 노드에 대한 암호화 키를 관리할 경우 해당 사이트를 선택하십시오. • *다른 KMS에서 관리되지 않는 사이트(기본 KMS)*를 선택하여 전용 KMS가 없는 사이트와 향후 확장에서 추가하는 모든 사이트에 적용될 기본 KMS를 구성합니다. 참고**:** 이전에 기본 KMS로 암호화된 사이트를 선택했지만 새 KMS에 기존 암호화 키의 최신 버전을 제공하지 않은 경우 KMS 구성을 저장할 때 유효성 검사 오류가 발생합니다.
포트	KMS 서버가 키 관리 상호 운용성 프로토콜(KMIP) 통신에 사용하는 포트입니다. 기본값은 KMIP 표준 포트인 5696입니다.
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. 참고**:** 서버 인증서의 SAN(Subject Alternative Name) 필드에는 여기에 입력한 FQDN 또는 IP 주소가 포함되어야 합니다. 그렇지 않으면 StorageGRID가 KMS 또는 KMS 클러스터의 모든 서버에 연결할 수 없습니다.

4. KMS 클러스터를 구성하는 경우, 클러스터의 각 서버에 호스트 이름을 추가하려면 *Add another hostname*을 선택하십시오.
5. *Continue*를 선택합니다.

2단계**:** 서버 인증서 업로드

키 관리 서버 추가 마법사의 2단계(서버 인증서 업로드)에서 KMS용 서버 인증서(또는 인증서 번들)를 업로드합니다. 서버 인증서를 통해 외부 KMS는 StorageGRID에 자신을 인증할 수 있습니다.

단계

1. *2단계(서버 인증서 업로드)*에서 저장된 서버 인증서 또는 인증서 묶음의 위치로 이동합니다.

2. 인증서 파일을 업로드합니다.

   서버 인증서 메타데이터가 표시됩니다.

   > 인증서 묶음을 업로드한 경우 각 인증서의 메타데이터가 별도의 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 통해 StorageGRID KMS에 자체 인증을 수행할 수 있습니다.

단계

1. *3단계(클라이언트 인증서 업로드)*에서 클라이언트 인증서가 있는 위치로 이동합니다.
2. 클라이언트 인증서 파일을 업로드합니다.

   클라이언트 인증서 메타데이터가 표시됩니다.

3. 클라이언트 인증서의 개인 키가 있는 위치로 이동합니다.
4. 개인 키 파일을 업로드합니다.
5. *테스트 후 저장*을 선택합니다.

   키가 없으면 StorageGRID에서 키를 생성하도록 요청하는 메시지가 표시됩니다.

   키 관리 서버와 어플라이언스 노드 간의 연결을 테스트합니다. 모든 연결이 유효하고 KMS에서 올바른 키가 발견되면 새 키 관리 서버가 키 관리 서버 페이지의 표에 추가됩니다.

   > KMS를 추가한 직후 키 관리 서버 페이지의 인증서 상태가 '알 수 없음'으로 표시됩니다. StorageGRID가 각 인증서의 실제 상태를 가져오는 데 최대 30분이 소요될 수 있습니다. 현재 상태를 확인하려면 웹 브라우저를 새로 고침해야 합니다.

6. *테스트 후 저장*을 선택했을 때 오류 메시지가 나타나면 메시지 내용을 확인한 후 *확인*을 선택하십시오.

   예를 들어 연결 테스트에 실패하면 422: Unprocessable Entity 오류가 발생할 수 있습니다.

7. 외부 연결을 테스트하지 않고 현재 구성을 저장해야 하는 경우 *강제 저장*을 선택하십시오.

   > *강제 저장*을 선택하면 KMS 구성이 저장되지만, 각 어플라이언스에서 해당 KMS로의 외부 연결은 테스트되지 않습니다. 구성에 문제가 있는 경우 해당 사이트에서 노드 암호화가 활성화된 어플라이언스 노드를 재부팅할 수 없을 수 있습니다. 문제가 해결될 때까지 데이터에 액세스할 수 없게 될 수도 있습니다.

8. 확인 경고 메시지를 검토하고 구성을 강제 저장하려면 *확인*을 선택합니다.

   KMS 구성이 저장되지만 KMS 연결은 테스트되지 않습니다.

키 관리 서버(KMS) 관리는 세부 정보 보기 또는 편집, 인증서 관리, 암호화된 노드 보기, 더 이상 필요하지 않을 때 KMS 제거 등을 포함합니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "필수 액세스 권한"

KMS 세부 정보 보기

StorageGRID 시스템의 각 키 관리 서버(KMS)에 대한 정보를 확인할 수 있으며, 여기에는 키 세부 정보와 서버 및 클라이언트 인증서의 현재 상태가 포함됩니다.

단계

1. * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   키 관리 서버 페이지가 나타나고 다음 정보가 표시됩니다.

   - 구성 세부 정보 탭에는 구성된 키 관리 서버 목록이 표시됩니다.
   - 암호화된 노드 탭에는 노드 암호화가 활성화된 모든 노드가 나열됩니다.

2. 특정 KMS의 세부 정보를 확인하고 해당 KMS에서 작업을 수행하려면 KMS 이름을 선택하십시오. KMS 세부 정보 페이지에는 다음 정보가 표시됩니다.

필드	설명
키 관리 대상:	KMS와 연결된 StorageGRID 사이트입니다. 이 필드에는 특정 StorageGRID 사이트 또는 *다른 KMS(기본 KMS)에서 관리되지 않는 사이트*의 이름이 표시됩니다.
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. 키 관리 서버가 두 대인 클러스터의 경우, 두 서버의 정규화된 도메인 이름 또는 IP 주소가 모두 나열됩니다. 클러스터에 키 관리 서버가 두 대 이상인 경우, 첫 번째 KMS의 정규화된 도메인 이름 또는 IP 주소와 함께 클러스터에 있는 추가 키 관리 서버의 수가 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 선택하십시오.

3. KMS 세부 정보 페이지에서 탭을 선택하여 다음 정보를 확인하십시오.

탭	필드	설명
주요 세부 정보	키 이름	KMS의 StorageGRID 클라이언트에 대한 키 별칭입니다.

탭	필드	설명
키 UID	키의 최신 버전에 대한 고유 식별자입니다.	최종 수정일
키의 최신 버전 날짜 및 시간입니다.	서버 인증서	메타데이터
인증서의 메타데이터(일련 번호, 만료 날짜 및 시간, 인증서 PEM 등)입니다.	PEM 인증서	인증서용 PEM(privacy enhanced mail) 파일의 내용입니다.
클라이언트 인증서	메타데이터	인증서의 메타데이터(일련 번호, 만료 날짜 및 시간, 인증서 PEM 등)입니다.

4. 조직의 보안 규정에 따라 필요한 만큼 자주 *Rotate key*를 선택하거나 KMS 소프트웨어를 사용하여 키의 새 버전을 생성하십시오.

   키 순환이 성공적으로 완료되면 키 UID 및 최종 수정 필드가 업데이트됩니다.

> KMS 소프트웨어를 사용하여 암호화 키를 교체하는 경우, 마지막으로 사용한 키 버전에서 동일한 키의 새 버전으로 교체해야 합니다. 완전히 다른 키로 교체하지 마십시오.
>
> KMS의 키 이름(별칭)을 변경하여 키를 교체하려고 시도하지 마십시오. StorageGRID는 이전에 사용한 모든 키 버전(및 향후 사용할 모든 키 버전)이 동일한 키 별칭으로 KMS에서 액세스 가능해야 합니다. 구성된 KMS의 키 별칭을 변경하면 StorageGRID가 데이터를 복호화하지 못할 수 있습니다.

인증서 관리

서버 또는 클라이언트 인증서 관련 문제가 발생하면 즉시 해결하십시오. 가능하면 만료 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 KMS의 인증서 만료일 값을 확인하십시오.
3. KMS 인증서 만료일이 '알 수 없음'으로 표시되는 경우, 최대 30분 정도 기다린 후 웹 브라우저를 새로 고침하세요.
4. 인증서 만료 열에 인증서가 만료되었거나 만료가 임박했음을 나타내는 경우, 해당 KMS를 선택하여 KMS 세부 정보 페이지로 이동하십시오.
   a. *서버 인증서*를 선택하고 "만료일" 필드의 값을 확인하십시오.
   b. 인증서를 교체하려면 *인증서 편집*을 선택하여 새 인증서를 업로드합니다.
   c. 위의 하위 단계를 반복하고 서버 인증서 대신 *Client certificate*를 선택하십시오.

5. **KMS CA** 인증서 만료, **KMS** 클라이언트 인증서 만료, **KMS** 서버 인증서 만료 경고가 발생하면 각 경고의 설명을 기록하고 권장 조치를 수행하십시오.

   StorageGRID 인증서 만료일을 업데이트하는 데 최대 30분이 소요될 수 있습니다. 웹 브라우저를 새로 고침하여 최신 값을 확인하십시오.

   서버 인증서 상태를 알 수 없음 상태가 표시되면 KMS에서 클라이언트 인증서 없이 서버 인증서를 가져올 수 있도록 설정되어 있는지 확인하십시오.

암호화된 노드 보기

StorageGRID 시스템에서 노드 암호화 설정이 활성화된 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 키 관리 서버가 표시됩니다.

2. 페이지 상단에서 암호화된 노드 탭을 선택합니다.

   암호화된 노드 탭에는 StorageGRID 시스템에서 노드 암호화 설정이 활성화된 어플라이언스 노드 목록이 표시됩니다.

3. 표에 있는 각 어플라이언스 노드 정보를 검토하십시오.

열	설명
노드 이름	어플라이언스 노드의 이름입니다.
노드 유형	노드 유형: 스토리지, 관리 또는 게이트웨이.
사이트	노드가 설치된 StorageGRID 사이트의 이름입니다.
KMS 이름	노드에 사용되는 KMS의 설명 이름입니다. KMS가 목록에 없으면 [구성 세부 정보] 탭을 선택하여 KMS를 추가하십시오. "키 관리 서버(KMS) 추가"
키 UID	어플라이언스 노드에서 데이터를 암호화 및 복호화하는 데 사용되는 암호화 키의 고유 ID입니다. 전체 키 UID를 보려면 텍스트를 선택하십시오. 하이픈(--)은 키 UID를 알 수 없음을 나타내며, 이는 어플라이언스 노드와 KMS 간의 연결 문제 때문일 수 있습니다.

열	설명
상태	KMS와 어플라이언스 노드 간의 연결 상태입니다. 노드가 연결된 경우 타임스탬프는 30분마다 업데이트됩니다. KMS 구성 변경 후 연결 상태가 업데이트되는 데 몇 분이 소요될 수 있습니다. 참고: 새 값을 보려면 웹 브라우저를 새로 고침하세요.

4. 상태 열에 KMS 문제가 표시되면 즉시 문제를 해결하십시오.

   정상적인 KMS 작동 중에는 상태가 *KMS에 연결됨*으로 표시됩니다. 노드가 그리드에서 연결이 끊어진 경우 노드 연결 상태가 (Administratively Down 또는 Unknown)으로 표시됩니다.

   다른 상태 메시지는 동일한 이름을 가진 StorageGRID 알림에 해당합니다.

   - KMS 구성 로드에 실패했습니다.
   - KMS 연결 오류
   - KMS 암호화 키 이름을 찾을 수 없습니다.
   - KMS 암호화 키 순환 실패
   - KMS 키로 어플라이언스 볼륨을 복호화하는 데 실패했습니다.
   - KMS가 구성되지 않았습니다.

   이러한 알림에 대해 권장되는 조치를 수행하십시오.

   데이터를 완벽하게 보호하려면 모든 문제를 즉시 해결해야 합니다.

KMS 편집

예를 들어 인증서 만료가 임박한 경우 키 관리 서버의 구성을 편집해야 할 수 있습니다.

시작하기 전에

- KMS에 대해 선택한 사이트를 업데이트할 계획이라면, "사이트의 KMS를 변경할 때 고려해야 할 사항"을(를) 검토하셨습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"

단계

1. * 구성 * > * 보안 * > * 키 관리 서버 * 를 선택합니다.

   키 관리 서버 페이지가 나타나고 구성된 모든 키 관리 서버가 표시됩니다.

2. 편집할 KMS를 선택하고 작업 > *편집*을 선택합니다.

   또한 표에서 KMS 이름을 선택하고 KMS 세부 정보 페이지에서 *편집*을 선택하여 KMS를 편집할 수 있습니다.

3. 필요에 따라 키 관리 서버 편집 마법사의 *1단계(KMS 세부 정보)*에서 세부 정보를 업데이트할 수 있습니다.

필드	설명
KMS 이름	이 KMS를 식별하는 데 도움이 되는 설명적인 이름입니다. 1자에서 64자 사이여야 합니다.
키 이름	KMS의 StorageGRID 클라이언트에 대한 정확한 키 별칭입니다. 1~255자 사이여야 합니다. 키 이름을 수정해야 하는 경우는 드뭅니다. 예를 들어, KMS에서 별칭 이름이 변경되었거나 이전 키의 모든 버전이 새 별칭의 버전 기록에 복사된 경우에만 키 이름을 수정해야 합니다.
키 관리 대상:	사이트별 KMS를 편집하는 중이고 기본 KMS가 아직 없는 경우, 선택적으로 *다른 KMS(기본 KMS)에서 관리되지 않는 사이트*를 선택할 수 있습니다. 이 옵션을 선택하면 사이트별 KMS가 기본 KMS로 변환되어 전용 KMS가 없는 모든 사이트와 확장 시 추가된 모든 사이트에 적용됩니다. 참고**:** 사이트별 KMS를 편집하는 경우 다른 사이트를 선택할 수 없습니다. 기본 KMS를 편집하는 경우 특정 사이트를 선택할 수 없습니다.
포트	KMS 서버가 키 관리 상호 운용성 프로토콜(KMIP) 통신에 사용하는 포트입니다. 기본값은 KMIP 표준 포트인 5696입니다.
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. 참고**:** 서버 인증서의 SAN(Subject Alternative Name) 필드에는 여기에 입력한 FQDN 또는 IP 주소가 포함되어야 합니다. 그렇지 않으면 StorageGRID가 KMS 또는 KMS 클러스터의 모든 서버에 연결할 수 없습니다.

4. KMS 클러스터를 구성하는 경우, 클러스터의 각 서버에 호스트 이름을 추가하려면 *Add another hostname*을 선택하십시오.
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 업로드하십시오.
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 업로드하십시오.
9. *테스트 후 저장*을 선택합니다.

   영향을 받는 사이트의 모든 노드 암호화 어플라이언스 노드와 키 관리 서버 간의 연결을 테스트합니다. 모든 노드 연결이 유효하고 KMS에서 올바른 키가 발견되면 키 관리 서버가 키 관리 서버 페이지의 표에 추가됩니다.
10. 오류 메시지가 나타나면 메시지 내용을 검토하고 *확인*을 선택하십시오.

예를 들어, 이 KMS에 대해 선택한 사이트가 이미 다른 KMS에서 관리되고 있거나 연결 테스트에 실패한 경우 422: Unprocessable Entity 오류가 발생할 수 있습니다.

11. 연결 오류를 해결하기 전에 현재 구성을 저장해야 하는 경우 *강제 저장*을 선택하십시오.

> *강제 저장*을 선택하면 KMS 구성이 저장되지만, 각 어플라이언스에서 해당 KMS로의 외부 연결은 테스트되지 않습니다. 구성에 문제가 있는 경우 해당 사이트에서 노드 암호화가 활성화된 어플라이언스 노드를 재부팅할 수 없을 수 있습니다. 문제가 해결될 때까지 데이터에 액세스할 수 없게 될 수도 있습니다.

KMS 구성이 저장되었습니다.

12. 확인 경고 메시지를 검토하고 구성을 강제 저장하려면 *확인*을 선택합니다.

KMS 구성이 저장되지만 KMS 연결은 테스트되지 않습니다.

키 관리 서버(KMS) 제거

경우에 따라 키 관리 서버를 제거해야 할 수도 있습니다. 예를 들어, 사이트를 더 이상 사용하지 않는 경우 사이트별 KMS를 제거해야 할 수 있습니다.

시작하기 전에

- "키 관리 서버 사용 시 고려 사항 및 요구 사항"를 검토했습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"

이 작업 정보

다음과 같은 경우 KMS를 제거할 수 있습니다.

- 사이트가 사용 중지되었거나 노드 암호화가 활성화된 어플라이언스 노드가 없는 경우 사이트별 KMS를 제거할 수 있습니다.
- 노드 암호화가 활성화된 어플라이언스 노드가 있는 각 사이트에 대해 사이트별 KMS가 이미 존재하는 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 작업 > *제거*를 선택합니다.

표에서 KMS 이름을 선택하고 KMS 세부 정보 페이지에서 *제거*를 선택하여 KMS를 삭제할 수도 있습니다.

3. 다음 사항이 사실인지 확인하십시오.
   - 노드 암호화가 활성화된 어플라이언스 노드가 없는 사이트에 대한 사이트별 KMS를 제거하려고 합니다.
   - 기본 KMS를 제거하려고 하지만, 노드 암호화가 있는 각 사이트에 대해 사이트별 KMS가 이미 존재합니다.
4. *예*를 선택합니다.

KMS 구성이 제거되었습니다.

프록시 설정 관리

StorageGRID 스토리지 프록시 구성

플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 스토리지 노드와 외부 S3 엔드포인트 사이에 비투명 프록시를 구성할 수 있습니다. 예를 들어, 플랫폼 서비스 메시지를 인터넷상의 엔드포인트와 같은 외부 엔드포인트로 전송하려면 비투명 프록시가 필요할 수 있습니다.

구성된 스토리지 프록시 설정은 Kafka 플랫폼 서비스 엔드포인트에 적용되지 않습니다.

시작하기 전에

- "특정 액세스 권한"이(가) 있습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.

이 작업 정보

단일 스토리지 프록시에 대한 설정을 구성할 수 있습니다.

단계

1. 구성 > 보안 > *프록시 설정*을 선택합니다.
2. 스토리지 탭에서 스토리지 프록시 활성화 확인란을 선택합니다.
3. 스토리지 프록시의 프로토콜을 선택합니다.
4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. 선택적으로 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.

   이 필드를 비워두면 프로토콜의 기본 포트(HTTP의 경우 80, SOCKS5의 경우 1080)가 사용됩니다.

6. *저장*을 선택하세요.

   스토리지 프록시를 저장한 후에는 플랫폼 서비스 또는 클라우드 스토리지 풀에 대한 새 엔드포인트를 구성하고 테스트할 수 있습니다.

   프록시 변경 사항이 적용되는 데 최대 10분이 소요될 수 있습니다.

7. StorageGRID의 플랫폼 서비스 관련 메시지가 차단되지 않도록 프록시 서버 설정을 확인하십시오.
8. 스토리지 프록시를 비활성화해야 하는 경우 확인란을 선택 해제하고 *저장*을 선택하십시오.

StorageGRID에서 관리자 프록시 설정 구성

HTTP 또는 HTTPS를 사용하여 AutoSupport 패키지를 전송하는 경우 관리 노드와 기술 지원(AutoSupport) 간에 비투명 프록시 서버를 구성할 수 있습니다.

AutoSupport에 대한 자세한 내용은 "AutoSupport 구성"을 참조하십시오.

시작하기 전에

- "특정 액세스 권한"이(가) 있습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.

이 작업 정보

단일 관리 프록시에 대한 설정을 구성할 수 있습니다.

단계

1. 구성 > 보안 > *프록시 설정*을 선택합니다.

   프록시 설정 페이지가 나타납니다. 기본적으로 탭 메뉴에서 저장소가 선택되어 있습니다.

2. **Admin** 탭을 선택합니다.
3. 관리자 프록시 활성화 확인란을 선택하십시오.
4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.
6. 선택적으로 프록시 서버의 사용자 이름과 암호를 입력합니다.

   프록시 서버에 사용자 이름이나 비밀번호가 필요하지 않은 경우 이 필드를 비워 두십시오.

7. 다음 중 하나를 선택하십시오.

   ◦ 관리자 프록시에 대한 연결을 보호하려면 *프록시 인증서 확인*을 선택하십시오. CA 번들을 업로드하여 관리자 프록시 서버에서 제공하는 SSL 인증서의 신뢰성을 확인하십시오.

   > 프록시 인증서가 검증되면 AutoSupport on Demand, StorageGRID를 통한 E-Series AutoSupport 및 StorageGRID 업그레이드 페이지의 업데이트 경로 결정이 작동하지 않습니다.

   CA 번들을 업로드하면 메타데이터가 표시됩니다.

   ◦ 관리자 프록시 서버와 통신할 때 인증서를 확인하지 않으려면 *프록시 인증서 확인 안 함*을 선택하십시오.

8. *저장*을 선택하세요.

   관리자 프록시가 저장되면 관리 노드와 기술 지원 간의 프록시 서버가 구성됩니다.

   > 프록시 변경 사항이 적용되는 데 최대 10분이 소요될 수 있습니다.

9. 관리자 프록시를 비활성화해야 하는 경우 관리자 프록시 활성화 확인란의 선택을 해제한 다음 *저장*을 선택하십시오.

방화벽 제어

외부 방화벽에서 **StorageGRID** 액세스 제어

외부 방화벽에서 특정 포트를 열거나 닫을 수 있습니다.

StorageGRID 관리 노드의 사용자 인터페이스 및 API에 대한 액세스는 외부 방화벽에서 특정 포트를 열거나 닫아

제어할 수 있습니다. 예를 들어, 시스템 액세스를 제어하는 다른 방법 외에도 방화벽에서 테넌트가 Grid Manager에 연결하지 못하도록 차단할 수 있습니다.

StorageGRID 내부 방화벽을 구성하려면 "내부 방화벽 구성"을 참조하십시오.

포트	설명	포트가 열려 있다면...
443	관리자 노드의 기본 HTTPS 포트	웹 브라우저와 관리 API 클라이언트는 그리드 관리자, 그리드 관리 API, 테넌트 관리자 및 테넌트 관리 API에 액세스할 수 있습니다. 참고: 포트 443은 일부 내부 트래픽에도 사용됩니다.
8443	관리 노드의 그리드 관리자 포트 제한	• 웹 브라우저와 관리 API 클라이언트는 HTTPS를 사용하여 그리드 관리자 및 그리드 관리 API에 액세스할 수 있습니다. • 웹 브라우저와 관리 API 클라이언트는 테넌트 관리자 또는 테넌트 관리 API에 접근할 수 없습니다. • 내부 콘텐츠 요청은 거부됩니다.
9443	관리 노드의 테넌트 관리자 포트 제한	• 웹 브라우저와 관리 API 클라이언트는 HTTPS를 사용하여 테넌트 관리자 및 테넌트 관리 API에 액세스할 수 있습니다. • 웹 브라우저와 관리 API 클라이언트는 Grid Manager 또는 Grid Management API에 액세스할 수 없습니다. • 내부 콘텐츠 요청은 거부됩니다.

제한된 Grid Manager 또는 Tenant Manager 포트에서는 싱글 사인온(SSO)을 사용할 수 없습니다. 사용자가 싱글 사인온으로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다.

관련 정보

- "Grid Manager에 로그인합니다"
- "테넌트 계정 생성"
- "외부 통신"

StorageGRID에서 내부 방화벽 제어 관리

StorageGRID는 각 노드에 내부 방화벽을 포함하여 노드에 대한 네트워크 액세스를 제어함으로써 그리드의 보안을 강화합니다. 방화벽을 사용하여 특정 그리드 배포에 필요한 포트를 제외한 모든 포트에 대한 네트워크 액세스를 차단할 수 있습니다. 방화벽 제어 페이지에서 변경한 구성은 각 노드에 적용됩니다.

방화벽 제어 페이지의 세 가지 탭을 사용하여 그리드에 필요한 액세스 권한을 사용자 지정합니다.

- **Privileged address list**: 이 탭을 사용하여 닫힌 포트에 대한 특정 액세스를 허용할 수 있습니다. 외부 액세스 관리

탭에서 닫힌 포트에 액세스할 수 있도록 IP 주소 또는 서브넷(CIDR 표기법)을 추가할 수 있습니다.

- 외부 액세스 관리: 이 탭을 사용하여 기본적으로 열려 있는 포트를 닫거나 이전에 닫았던 포트를 다시 열 수 있습니다.
- 신뢰할 수 없는 클라이언트 네트워크: 이 탭을 사용하여 노드가 클라이언트 네트워크에서 들어오는 트래픽을 신뢰할지 여부를 지정합니다.

  이 탭의 설정은 '외부 액세스 관리' 탭의 설정을 재정의합니다.

  - 신뢰할 수 없는 클라이언트 네트워크를 가진 노드는 해당 노드에 구성된 로드 밸런싱 엔드포인트 포트(전역, 노드 인터페이스 및 노드 유형 바인딩 엔드포인트)에 대한 연결만 허용합니다.
  - 로드 밸런서 엔드포인트 포트는 외부 네트워크 관리 탭의 설정과 관계없이 신뢰할 수 없는 클라이언트 네트워크에서 _유일하게 열려 있는 포트_입니다.
  - 신뢰할 수 있는 경우, 외부 액세스 관리 탭에서 열린 모든 포트와 클라이언트 네트워크에서 열린 모든 로드 밸런서 엔드포인트에 액세스할 수 있습니다.

> ⓘ 한 탭에서 설정한 내용이 다른 탭에서 변경한 액세스 권한에 영향을 줄 수 있습니다. 네트워크가 예상대로 작동하는지 확인하려면 모든 탭의 설정을 확인하십시오.

내부 방화벽 제어를 구성하려면 "방화벽 제어 구성"을 참조하십시오.

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 "외부 방화벽에서 액세스 제어"을 참조하십시오.

특권 주소 목록 및 외부 액세스 관리 탭

'특권 주소 목록' 탭에서는 닫혀 있는 그리드 포트에 대한 액세스 권한이 부여된 하나 이상의 IP 주소를 등록할 수 있습니다. '외부 액세스 관리' 탭에서는 선택한 외부 포트 또는 모든 열린 외부 포트(외부 포트는 기본적으로 그리드에 속하지 않은 노드에서 액세스할 수 있는 포트)에 대한 외부 액세스를 차단할 수 있습니다. 이 두 탭은 그리드에 허용해야 하는 정확한 네트워크 액세스를 사용자 지정하기 위해 함께 사용할 수 있습니다.

> ⓘ 권한 있는 IP 주소는 기본적으로 내부 그리드 포트에 대한 액세스 권한이 없습니다.

예시 **1:** 유지 관리 작업을 위해 점프 호스트 사용

보안이 강화된 호스트인 점프 호스트를 네트워크 관리에 사용하려는 경우를 가정해 보겠습니다. 다음과 같은 일반적인 단계를 따를 수 있습니다.

1. 권한 있는 주소 목록 탭을 사용하여 점프 호스트의 IP 주소를 추가하십시오.
2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단할 수 있습니다.

> ⓘ 포트 443 및 8443을 차단하기 전에 우선 순위 IP 주소를 추가하십시오. 현재 차단된 포트에 연결된 모든 사용자(본인 포함)는 IP 주소가 우선 순위 주소 목록에 추가되지 않으면 Grid Manager에 액세스할 수 없게 됩니다.

구성을 저장하면 그리드의 관리 노드에 있는 모든 외부 포트가 점프 호스트를 제외한 모든 호스트에 대해 차단됩니다. 그러면 점프 호스트를 사용하여 그리드에서 유지 관리 작업을 더욱 안전하게 수행할 수 있습니다.

예시 **2:** 민감한 포트 잠금

민감한 포트와 해당 포트에서 실행되는 서비스를 차단하고 싶다고 가정해 보겠습니다. 다음과 같은 일반적인 단계를 따를 수 있습니다.

1. '권한 있는 주소 목록' 탭을 사용하여 서비스에 액세스해야 하는 호스트에만 액세스 권한을 부여하십시오.
2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단할 수 있습니다.

> Grid Manager 및 Tenant Manager에 액세스하는 데 할당된 포트(기본 설정 포트는 443 및 8443)에 대한 액세스를 차단하기 전에 권한 있는 IP 주소를 추가하십시오. 차단된 포트에 현재 연결된 모든 사용자(본인 포함)는 IP 주소가 권한 있는 주소 목록에 추가되지 않으면 Grid Manager에 액세스할 수 없게 됩니다.

구성을 저장하면 해당 포트와 해당 포트의 서비스는 권한 있는 주소 목록에 있는 호스트에서만 사용할 수 있습니다. 다른 모든 호스트는 요청이 어떤 인터페이스를 통해 들어오든 관계없이 해당 서비스에 액세스할 수 없습니다.

예시 **3:** 사용하지 않는 서비스에 대한 액세스 비활성화

네트워크 수준에서 사용하지 않을 일부 서비스를 비활성화할 수 있습니다. 예를 들어 HTTP S3 클라이언트 트래픽을 차단하려면 외부 액세스 관리 탭에서 토글을 사용하여 18084번 포트를 차단하면 됩니다.

신뢰할 수 없는 클라이언트 네트워크 탭

클라이언트 네트워크를 사용하는 경우, 명시적으로 구성된 엔드포인트에서만 인바운드 클라이언트 트래픽을 허용함으로써 악의적인 공격으로부터 StorageGRID를 보호할 수 있습니다.

기본적으로 각 그리드 노드의 클라이언트 네트워크는 신뢰할 수 있는 상태입니다. 즉, 기본적으로 StorageGRID는 모든 "사용 가능한 외부 포트"에서 각 그리드 노드에 대한 인바운드 연결을 신뢰합니다.

StorageGRID 시스템에 대한 악의적인 공격 위협을 줄이려면 각 노드의 클라이언트 네트워크를 _신뢰할 수 없음_으로 지정하십시오. 노드의 클라이언트 네트워크가 신뢰할 수 없는 경우 해당 노드는 로드 밸런서 엔드포인트로 명시적으로 구성된 포트에서만 수신 연결을 허용합니다. "로드 밸런서 엔드포인트 구성" 및 "방화벽 제어 구성"을 참조하십시오.

예시 **1:** 게이트웨이 노드는 **HTTPS S3** 요청만 허용합니다

게이트웨이 노드가 HTTPS S3 요청을 제외한 클라이언트 네트워크의 모든 인바운드 트래픽을 거부하도록 설정하려면 다음과 같은 일반적인 단계를 수행합니다.

1. 해당 "로드 밸런서 엔드포인트" 페이지에서 포트 443을 통해 HTTPS를 사용하는 S3용 로드 밸런서 엔드포인트를 구성하십시오.
2. 방화벽 제어 페이지에서 Untrusted를 선택하여 게이트웨이 노드의 클라이언트 네트워크를 신뢰할 수 없는 것으로 지정합니다.

구성을 저장하면 게이트웨이 노드의 클라이언트 네트워크로 들어오는 모든 인바운드 트래픽은 차단되지만, 포트 443의 HTTPS S3 요청과 ICMP 에코(핑) 요청은 예외적으로 허용됩니다.

예시 **2:** 스토리지 노드가 **S3** 플랫폼 서비스 요청을 보냅니다

스토리지 노드에서 S3 플랫폼 서비스로의 아웃바운드 트래픽은 허용하되, 클라이언트 네트워크에서 해당 스토리지 노드로의 인바운드 연결은 차단하고 싶다고 가정해 보겠습니다. 이 경우 일반적으로 다음과 같은 단계를 수행합니다.

- 방화벽 제어 페이지의 '신뢰할 수 없는 클라이언트 네트워크' 탭에서 스토리지 노드의 클라이언트 네트워크가 신뢰할 수 없음을 지정합니다.

구성을 저장하면 스토리지 노드는 클라이언트 네트워크에서 들어오는 트래픽을 더 이상 수락하지 않지만, 구성된 플랫폼 서비스 대상으로 나가는 요청은 계속 허용합니다.

예제 **3: Grid Manager**에 대한 액세스를 서브넷으로 제한하기

특정 서브넷에서만 Grid Manager에 대한 액세스를 허용하려고 한다고 가정합니다. 다음 단계를 수행합니다.

1. 관리 노드의 클라이언트 네트워크를 서브넷에 연결하십시오.
2. 신뢰할 수 없는 클라이언트 네트워크 탭을 사용하여 클라이언트 네트워크를 신뢰할 수 없는 네트워크로 구성하십시오.
3. 관리 인터페이스 로드 밸런서 엔드포인트를 생성할 때 포트를 입력하고 해당 포트에서 액세스할 관리 인터페이스를 선택하십시오.
4. 신뢰할 수 없는 클라이언트 네트워크에 대해 *예*를 선택하십시오.
5. '외부 액세스 관리' 탭을 사용하여 모든 외부 포트를 차단할 수 있습니다(해당 서브넷 외부 호스트에 대해 특권 IP 주소를 설정했는지 여부와 관계없음).

구성을 저장하면 지정한 서브넷에 있는 호스트만 Grid Manager에 액세스할 수 있습니다. 다른 모든 호스트는 차단됩니다.

StorageGRID 내부 방화벽을 구성합니다

StorageGRID 방화벽을 구성하여 StorageGRID 노드의 특정 포트에 대한 네트워크 액세스를 제어할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.
- 귀하는 "방화벽 제어 관리" 및 "네트워킹 가이드라인"에 있는 정보를 검토하셨습니다.
- 관리 노드 또는 게이트웨이 노드가 명시적으로 구성된 엔드포인트에서만 수신 트래픽을 허용하도록 하려면 로드 밸런싱 엔드포인트를 정의해야 합니다.

> ⓘ 클라이언트 네트워크 구성을 변경할 때, 로드 밸런서 엔드포인트가 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

이 작업 정보

StorageGRID는 각 노드에 내부 방화벽을 포함하고 있어 그리드 노드의 일부 포트를 열거나 닫을 수 있습니다. 방화벽 제어 탭을 사용하여 그리드 네트워크, 관리 네트워크 및 클라이언트 네트워크에서 기본적으로 열려 있는 포트를 열거나 닫을 수 있습니다. 또한 닫혀 있는 그리드 포트에 액세스할 수 있는 권한 있는 IP 주소 목록을 생성할 수도 있습니다. 클라이언트 네트워크를 사용하는 경우 노드가 클라이언트 네트워크에서 들어오는 트래픽을 신뢰할지 여부를 지정하고 클라이언트 네트워크의 특정 포트에 대한 액세스를 구성할 수 있습니다.

그리드 외부의 IP 주소에 대해 반드시 필요한 포트만 열도록 포트 수를 제한하면 그리드 보안이 강화됩니다. 방화벽 제어 탭 세 곳 각각의 설정을 사용하여 필요한 포트만 열리도록 할 수 있습니다.

방화벽 제어 사용에 대한 자세한 내용(예제 포함)은 "방화벽 제어 관리"을 참조하십시오.

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 "외부 방화벽에서 액세스 제어"을 참조하십시오.

액세스 방화벽 제어

단계

1. * 구성 * > * 보안 * > * 방화벽 제어 * 를 선택합니다.

   이 페이지의 세 탭에 대한 설명은 "방화벽 제어 관리"에 있습니다.

2. 방화벽 설정을 구성하려면 아무 탭이나 선택하십시오.

   이 탭들은 어떤 순서로든 사용할 수 있습니다. 한 탭에서 설정한 구성은 다른 탭에서 수행할 수 있는 작업에 영향을 미치지 않습니다. 그러나 한 탭에서 구성을 변경하면 다른 탭에 구성된 포트의 동작이 변경될 수 있습니다.

권한 있는 주소 목록

권한 있는 주소 목록 탭을 사용하여 기본적으로 닫혀 있거나 외부 액세스 관리 탭의 설정에 따라 닫혀 있는 포트에 호스트가 액세스할 수 있도록 허용할 수 있습니다.

특권 IP 주소 및 서브넷은 기본적으로 내부 그리드 액세스가 허용되지 않습니다. 또한, 특권 주소 목록 탭에서 열린 로드 밸런서 엔드포인트 및 추가 포트는 외부 액세스 관리 탭에서 차단된 경우에도 액세스할 수 있습니다.

'권한 있는 주소 목록' 탭의 설정은 '신뢰할 수 없는 클라이언트 네트워크' 탭의 설정을 재정의할 수 없습니다.

단계

1. Privileged address list 탭에서 닫힌 포트에 대한 액세스 권한을 부여할 주소 또는 IP 서브넷을 입력합니다.
2. 선택적으로 *다른 IP 주소 또는 CIDR 표기법의 서브넷 추가*를 선택하여 권한 있는 클라이언트를 추가할 수 있습니다.

   권한 목록에는 가능한 한 적은 주소만 추가하십시오.

3. 선택적으로 *특권 있는 IP 주소가 StorageGRID 내부 포트에 액세스하도록 허용*을 선택할 수 있습니다. 을 참조하십시오."StorageGRID 내부 포트"

   이 옵션을 선택하면 내부 서비스에 대한 일부 보호 기능이 제거됩니다. 가능하면 이 옵션을 비활성화하십시오.

4. *저장*을 선택하세요.

외부 액세스 관리

'외부 액세스 관리' 탭에서 포트를 닫으면, 해당 IP 주소를 권한 있는 주소 목록에 추가하지 않는 한 그리드 IP 주소가 아닌 다른 IP 주소로는 해당 포트에 액세스할 수 없습니다. 기본적으로 열려 있는 포트만 닫을 수 있으며, 닫아 놓은 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 것으로 설정된 경우, '외부 액세스 관리' 탭에서 SSH/22 포트가 열려 있더라도 클라이언트 네트워크에서는 해당 포트가 차단됩니다. '신뢰할 수 없는 클라이언트 네트워크' 탭의 설정은 클라이언트 네트워크에서 닫힌 포트(예: 443, 8443, 9443)를 재정의합니다.

단계

1. *외부 액세스 관리*를 선택합니다. 해당 탭에는 그리드에 있는 모든 노드의 외부 포트(기본적으로 그리드에 속하지 않은 노드에서 액세스할 수 있는 포트) 목록이 표 형식으로 표시됩니다.
2. 다음 옵션을 사용하여 열고 닫을 포트를 구성하십시오.
   - 각 포트 옆에 있는 토글을 사용하여 선택한 포트를 열거나 닫습니다.
   - 표에 나열된 모든 포트를 열려면 *표시된 모든 포트 열기*를 선택하십시오.
   - 표에 나열된 모든 포트를 닫으려면 *표시된 모든 포트 닫기*를 선택하십시오.

   Grid Manager 포트 443 또는 8443을 닫으면, 귀하를 포함하여 차단된 포트에 현재 연결된 모든 사용자는 IP 주소가 권한 있는 주소 목록에 추가되지 않은 한 Grid Manager에 대한 액세스 권한을 잃게 됩니다.

   표 오른쪽의 스크롤 막대를 사용하여 사용 가능한 모든 포트를 확인하십시오. 검색 필드에 포트 번호를 입력하여 외부 포트 설정을 찾을 수 있습니다. 포트 번호를 부분적으로 입력할 수도 있습니다. 예를 들어 *2*를 입력하면 이름에 "2"가 포함된 모든 포트가 표시됩니다.
3. *저장*을 선택합니다

신뢰할 수 없는 클라이언트 네트워크

노드의 클라이언트 네트워크가 신뢰할 수 없는 경우, 해당 노드는 로드 밸런싱 엔드포인트로 구성된 포트와 이 탭에서 선택적으로 추가한 포트에서만 수신 트래픽을 허용합니다. 또한 이 탭을 사용하여 확장에 추가된 새 노드의 기본 설정을 지정할 수 있습니다.

로드 밸런싱 엔드포인트가 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

신뢰할 수 없는 클라이언트 네트워크 탭에서 변경한 구성 내용은 외부 액세스 관리 탭의 설정을 재정의합니다.

단계

1. *신뢰할 수 없는 클라이언트 네트워크*를 선택하십시오.
2. '새 노드 기본값 설정' 섹션에서 확장 절차에서 새 노드가 그리드에 추가될 때 기본 설정이 무엇이어야 하는지 지정합니다.
   - 신뢰됨(기본값): 확장에 노드가 추가되면 해당 클라이언트 네트워크가 신뢰됩니다.
   - 신뢰할 수 없음: 확장에서 노드가 추가되면 해당 노드의 클라이언트 네트워크는 신뢰할 수 없는 것으로 간주됩니다.

     필요에 따라 이 탭으로 돌아와 특정 새 노드의 설정을 변경할 수 있습니다.

     이 설정은 StorageGRID 시스템의 기존 노드에 영향을 미치지 않습니다.

3. 다음 옵션을 사용하여 명시적으로 구성된 로드 밸런서 엔드포인트 또는 추가로 선택한 포트에서만 클라이언트 연결을 허용해야 하는 노드를 선택하십시오.

   - 표에 표시된 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가하려면 *표시된 노드에 대해 신뢰하지 않음*을 선택하십시오.
   - 표에 표시된 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에서 제거하려면 *표시된 노드에 대한 신뢰*를 선택하십시오.
   - 각 노드 옆에 있는 토글을 사용하여 선택한 노드에 대해 클라이언트 네트워크를 신뢰할 수 있음 또는 신뢰할 수 없음으로 설정하십시오.

     예를 들어, *표시된 노드에 대해 신뢰하지 않음*을 선택하여 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가한 다음, 개별 노드 옆에 있는 토글 버튼을 사용하여 해당 노드만 신뢰할 수 있는 클라이언트 네트워크 목록에 추가할 수 있습니다.

   표 오른쪽의 스크롤 막대를 사용하여 사용 가능한 모든 노드를 확인했는지 확인하십시오. 검색 필드를 사용하여 노드 이름을 입력하면 해당 노드의 설정을 찾을 수 있습니다. 부분적으로 이름을 입력할 수도 있습니다. 예를 들어 *GW*를 입력하면 이름에 "GW"가 포함된 모든 노드가 표시됩니다.

4. *저장*을 선택하세요.

   새 방화벽 설정은 즉시 적용되고 효력이 발생합니다. 로드 밸런서 엔드포인트가 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

테넌트 관리

StorageGRID의 테넌트 계정

테넌트 계정을 사용하면 Simple Storage Service(S3) REST API를 이용하여 StorageGRID 시스템에 객체를 저장하고 검색할 수 있습니다.

Swift 관련 세부 정보는 이 버전의 문서 사이트에서 삭제되었습니다. 참조 "StorageGRID 11.8: 테넌트 관리".

그리드 관리자로서 S3 클라이언트가 객체를 저장하고 검색하는 데 사용하는 테넌트 계정을 생성하고 관리합니다.

각 테넌트 계정에는 연합 또는 로컬 그룹, 사용자, S3 버킷 및 객체가 있습니다.

테넌트 계정을 사용하면 저장된 객체를 서로 다른 엔티티별로 구분할 수 있습니다. 예를 들어, 다음과 같은 두 가지 사용 사례에 여러 테넌트 계정을 사용할 수 있습니다.

- 엔터프라이즈 사용 사례**:** 엔터프라이즈 애플리케이션에서 StorageGRID 시스템을 관리하는 경우, 조직 내 여러 부서별로 그리드의 객체 스토리지를 분리하고 싶을 수 있습니다. 이 경우 마케팅 부서, 고객 지원 부서, 인사 부서 등을 위한 테넌트 계정을 생성할 수 있습니다.

  S3 클라이언트 프로토콜을 사용하면 S3 버킷과 버킷 정책을 활용하여 기업 내 부서 간에 객체를 분리할 수 있습니다. 테넌트 계정을 사용할 필요가 없습니다. 자세한 내용은 "S3 버킷 및 버킷 정책" 구현 지침을 참조하십시오.

- 서비스 제공업체 사용 사례**:** StorageGRID 시스템을 서비스 제공업체로서 관리하는 경우, 그리드의 객체 스토리지를 그리드에서 스토리지를 임대할 여러 주체별로 분리할 수 있습니다. 이 경우, 회사 A, 회사 B, 회사 C 등에 대한 테넌트 계정을 생성하면 됩니다.

자세한 내용은 "테넌트 계정 사용"을 참조하십시오.

테넌트 계정은 어떻게 만드나요**?**

그리드 관리자를 사용하여 테넌트 계정을 생성합니다. 테넌트 계정을 생성할 때 다음 정보를 지정합니다.

- 테넌트 이름, 클라이언트 유형(S3) 및 선택적 스토리지 할당량을 포함한 기본 정보.
- 테넌트 계정에 대한 권한에는 테넌트 계정이 S3 플랫폼 서비스를 사용할 수 있는지, 자체 ID 소스를 구성할 수 있는지, S3 Select를 사용할 수 있는지, 또는 그리드 페더레이션 연결을 사용할 수 있는지 여부가 포함됩니다.
- 테넌트의 초기 루트 액세스는 StorageGRID 시스템이 로컬 그룹 및 사용자, ID 페더레이션 또는 단일 로그인(SSO)을 사용하는지에 따라 결정됩니다.

또한, S3 테넌트 계정이 규제 요건을 준수해야 하는 경우 StorageGRID 시스템에 S3 객체 잠금 설정을 활성화할 수 있습니다. S3 객체 잠금이 활성화되면 모든 S3 테넌트 계정은 규제를 준수하는 버킷을 생성하고 관리할 수 있습니다.

Tenant Manager는 무엇에 사용되나요**?**

테넌트 계정을 생성한 후, 테넌트 사용자는 Tenant Manager에 로그인하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 페더레이션을 설정합니다(ID 소스가 그리드와 공유되는 경우는 제외).
- 그룹 및 사용자 관리
- 계정 복제 및 그리드 간 복제를 위해 그리드 페더레이션을 사용합니다.
- S3 액세스 키 관리
- S3 버킷 생성 및 관리
- S3 플랫폼 서비스 사용
- S3 Select 사용
- 스토리지 사용량 모니터링

S3 테넌트 사용자는 테넌트 관리자를 통해 S3 액세스 키와 버킷을 생성 및 관리할 수 있지만, 객체를 수집하고 관리하려면 S3 클라이언트 애플리케이션을 사용해야 합니다. 자세한 내용은 "S3 REST API 사용"을 참조하십시오.

StorageGRID 테넌트 계정을 생성합니다

StorageGRID 시스템의 스토리지에 대한 액세스를 제어하려면 최소 하나 이상의 테넌트 계정을 생성해야 합니다.

테넌트 계정을 생성하는 단계는 "ID 페더레이션" 및 "싱글 사인온" 구성 여부와 테넌트 계정을 생성하는 데 사용하는 Grid Manager 계정이 루트 액세스 권한이 있는 관리자 그룹에 속해 있는지 여부에 따라 다릅니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.

- 당신은 "루트 액세스 또는 테넌트 계정 권한"을(를) 가지고 있습니다.
- 테넌트 계정이 Grid Manager에 대해 구성된 ID 소스를 사용하고, 페더레이션 그룹에 테넌트 계정에 대한 루트 액세스 권한을 부여하려는 경우, 해당 페더레이션 그룹을 Grid Manager로 가져온 것입니다. 이 관리자 그룹에 Grid Manager 권한을 할당할 필요는 없습니다. "관리자 그룹 관리"을 참조하십시오.
- S3 테넌트가 그리드 페더레이션 연결을 사용하여 계정 데이터를 복제하고 버킷 객체를 다른 그리드로 복제할 수 있도록 허용하려면 다음을 수행합니다.
  - "그리드 페더레이션 연결을 구성했습니다."이(가) 있습니다.
  - 연결 상태는 *연결됨*입니다.
  - 루트 액세스 권한이 있습니다.
  - 귀하는 "그리드 페더레이션에 허용된 테넌트 관리"에 대한 고려 사항을 검토하셨습니다.
  - 테넌트 계정이 Grid Manager에 대해 구성된 ID 소스를 사용하는 경우, 두 그리드 모두에서 동일한 페더레이션 그룹을 Grid Manager로 가져온 것입니다.

    테넌트를 생성할 때 소스 및 대상 테넌트 계정 모두에 대해 초기 루트 액세스 권한을 갖도록 이 그룹을 선택합니다.

테넌트를 생성하기 전에 이 관리 그룹이 두 그리드 모두에 존재하지 않으면 테넌트가 대상으로 복제되지 않습니다.

마법사에 액세스합니다

단계

1. *테넌트*를 선택합니다.
2. *생성*을 선택합니다.

세부 정보를 입력합니다

단계

1. 테넌트에 대한 세부 정보를 입력합니다.

필드	설명
이름	테넌트 계정의 이름입니다. 테넌트 이름은 고유할 필요가 없습니다. 테넌트 계정이 생성되면 고유한 20자리 계정 ID가 부여됩니다.
설명 (선택 사항)	테넌트를 식별하는 데 도움이 되는 설명입니다. 그리드 페더레이션 연결을 사용할 테넌트를 생성하는 경우, 선택적으로 이 필드를 사용하여 소스 테넌트와 대상 테넌트를 식별할 수 있습니다. 예를 들어, Grid 1에서 생성된 테넌트에 대한 다음 설명은 Grid 2로 복제된 테넌트에도 표시됩니다. "이 테넌트는 Grid 1에서 생성되었습니다."
클라이언트 유형	*S3*이어야 합니다.

필드	설명
스토리지 할당량(선택 사항)	이 테넌트에 스토리지 할당량을 설정하려면 할당량의 숫자 값과 단위를 입력하세요.

2. *Continue*를 선택합니다.

권한 선택

단계

1. 선택적으로, 이 테넌트에게 부여할 기본 권한을 선택합니다.

> 일부 권한에는 추가 요구 사항이 있습니다. 자세한 내용은 각 권한에 대한 도움말 아이콘을 선택하십시오.

권한	선택한 경우...
플랫폼 서비스 허용	테넌트는 CloudMirror와 같은 S3 플랫폼 서비스를 사용할 수 있습니다. 을(를) 참조하십시오."S3 테넌트 계정에 대한 플랫폼 서비스 관리"
자체 ID 소스 사용	테넌트는 페더레이션 그룹 및 사용자에 대한 자체 ID 소스를 구성하고 관리할 수 있습니다. StorageGRID 시스템에 대해 "구성된 SSO"한 경우 이 옵션은 비활성화됩니다.
S3 Select 허용	테넌트는 S3 SelectObjectContent API 요청을 통해 객체 데이터를 필터링하고 검색할 수 있습니다. 을 참조하십시오."테넌트 계정에 대한 S3 Select 관리" 중요: SelectObjectContent 요청은 모든 S3 클라이언트와 모든 테넌트의 로드 밸런서 성능을 저하시킬 수 있습니다. 이 기능은 필요한 경우에만, 그리고 신뢰할 수 있는 테넌트에 대해서만 활성화하십시오.

2. 선택적으로, 이 테넌트에게 부여할 고급 권한을 선택합니다.

권한	선택한 경우...
그리드 페더레이션 연결	테넌트는 그리드 페더레이션 연결을 사용할 수 있으며, 이 연결은 다음과 같습니다. • 이 테넌트와 계정에 추가된 모든 테넌트 그룹 및 사용자가 이 그리드(소스 그리드)에서 선택한 연결의 다른 그리드(대상 그리드)로 복제됩니다. • 이 테넌트가 각 그리드의 해당 버킷 간에 그리드 간 복제를 구성할 수 있습니다. "그리드 페더레이션에 허용된 테넌트 관리"을 참조하십시오.

권한	선택한 경우...
S3 Object Lock	테넌트가 S3 오브젝트 잠금의 특정 기능을 사용할 수 있도록 허용합니다. • *최대 보존 기간*은 이 버킷에 새로 추가된 객체를 수집 시점부터 얼마나 오랫동안 보존할지 정의합니다. • *규정 준수 모드 허용*은 보존 기간 동안 사용자가 보호된 오브젝트 버전을 덮어쓰거나 삭제하지 못하도록 합니다.

3. *Continue*를 선택합니다.

루트 액세스 정의 및 테넌트 생성

단계

1. StorageGRID 시스템에서 ID 페더레이션, 싱글 사인온(SSO) 또는 둘 다를 사용하는지 여부에 따라 테넌트 계정에 대한 루트 액세스 권한을 정의하십시오.

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

2. *테넌트 생성*을 선택합니다.

   성공 메시지가 표시되고 새 테넌트가 테넌트 페이지에 나열됩니다. 테넌트 세부 정보를 확인하고 테넌트 활동을 모니터링하는 방법에 대한 자세한 내용은 "테넌트 활동 모니터링"을 참조하십시오.

   테넌트 그리드 전체에 테넌트 설정을 적용하는 데에는 네트워크 연결 상태, 노드 상태 및 Cassandra 작업에 따라 15분 이상 소요될 수 있습니다.

3. 테넌트에 대해 * 그리드 페더레이션 연결 사용 * 권한을 선택한 경우:

   a. 연결된 다른 그리드에 동일한 테넌트가 복제되었는지 확인하십시오. 두 그리드의 테넌트는 동일한 20자리 계정 ID, 이름, 설명, 할당량 및 권한을 갖습니다.

      "클론 없이 테넌트가 생성되었습니다"라는 오류 메시지가 표시되면 "그리드 페더레이션 오류 해결"의 지침을 참조하십시오.

   b. 루트 액세스를 정의할 때 로컬 루트 사용자 암호를 제공한 경우, 복제된 테넌트에 대해 "로컬 루트 사용자의 암호 변경"합니다.

루트 사용자 암호를 변경하기 전까지는 로컬 루트 사용자가 대상 그리드의 테넌트 관리자에 로그인할 수 없습니다.

테넌트에 로그인(선택 사항)

필요에 따라 지금 새 테넌트에 로그인하여 구성을 완료하거나 나중에 테넌트에 로그인할 수 있습니다. 로그인 단계는 기본 포트(443)를 사용하여 Grid Manager에 로그인했는지 또는 제한된 포트를 사용하여 로그인했는지에 따라 다릅니다. "외부 방화벽에서 액세스 제어"을 참조하십시오.

지금 로그인하세요

사용 중인 경우...	이렇게 하세요...
포트 443 및 로컬 루트 사용자에 대한 암호를 설정합니다	1. *루트로 로그인*을 선택합니다. 로그인하면 버킷, ID 페더레이션, 그룹 및 사용자 구성을 위한 링크가 표시됩니다. 2. 테넌트 계정을 구성하려면 링크를 선택하십시오. 각 링크를 클릭하면 테넌트 관리자의 해당 페이지가 열립니다. 페이지를 완료하려면 "테넌트 계정 사용 지침"을 참조하세요.
포트 443을 사용하고 있으며 로컬 루트 사용자의 암호를 설정하지 않은 경우	*로그인*을 선택하고 루트 액세스 페더레이션 그룹에 속한 사용자의 자격 증명을 입력하십시오.
제한된 포트	1. **Finish** 를 선택합니다 2. 테넌트 테이블에서 *제한됨*을 선택하여 해당 테넌트 계정에 액세스하는 방법에 대한 자세한 내용을 확인하십시오. 테넌트 관리자의 URL 형식은 다음과 같습니다. `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ `FQDN_or_Admin_Node_IP`는 정규화된 도메인 이름 또는 관리 노드의 IP 주소입니다. ◦ `port`은(는) 테넌트 전용 포트입니다. ◦ `20-digit-account-id`은(는) 테넌트의 고유 계정 ID입니다.

나중에 로그인

사용 중인 경우...	다음 중 하나를 수행하십시오...
포트 443	• 그리드 관리자에서 *테넌트*를 선택하고 테넌트 이름 오른쪽에 있는 *로그인*을 선택합니다. • 웹 브라우저에 테넌트의 URL을 입력합니다. `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ `FQDN_or_Admin_Node_IP`는 정규화된 도메인 이름 또는 관리 노드의 IP 주소입니다. ◦ `20-digit-account-id`은(는) 테넌트의 고유 계정 ID입니다.
제한된 포트	• 그리드 관리자에서 *테넌트*를 선택한 다음 *제한됨*을 선택합니다. • 웹 브라우저에 테넌트의 URL을 입력합니다. `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ `FQDN_or_Admin_Node_IP`는 정규화된 도메인 이름 또는 관리 노드의 IP 주소입니다. ◦ `port`는 테넌트 전용 제한 포트입니다. ◦ `20-digit-account-id`은(는) 테넌트의 고유 계정 ID입니다.

테넌트 구성

"테넌트 계정 사용"의 지침에 따라 테넌트 그룹 및 사용자, S3 액세스 키, 버킷, 플랫폼 서비스, 계정 복제 및 크로스 그리드 복제를 관리하십시오.

StorageGRID 테넌트 계정 편집

테넌트 계정을 편집하여 표시 이름, 스토리지 할당량 또는 테넌트 권한을 변경할 수 있습니다.

테넌트에게 그리드 페더레이션 연결 사용 권한이 있는 경우, 연결된 두 그리드 중 어느 쪽에서든 테넌트 세부 정보를 편집할 수 있습니다. 단, 한 그리드에서 변경한 내용은 다른 그리드에 복사되지 않습니다. 두 그리드의 테넌트 세부 정보를 정확히 동기화하려면 두 그리드에서 동일한 편집 작업을 수행해야 합니다. "그리드 페더레이션 연결에 허용된 테넌트 관리"을 참조하십시오.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 당신은 "루트 액세스 또는 테넌트 계정 권한"을(를) 가지고 있습니다.

테넌트 그리드 전체에 테넌트 설정을 적용하는 데에는 네트워크 연결 상태, 노드 상태 및 Cassandra 작업에 따라 15분 이상 소요될 수 있습니다.

단계

1. *테넌트*를 선택합니다.

2. 수정하려는 테넌트 계정을 찾습니다.

   검색 상자를 사용하여 테넌트 이름 또는 테넌트 ID로 테넌트를 검색하세요.

3. 테넌트를 선택합니다. 다음 두 가지 방법 중 하나를 선택할 수 있습니다.
   - 테넌트의 확인란을 선택하고 작업 > *편집*을 선택합니다.
   - 테넌트 이름을 선택하여 세부 정보 페이지를 표시한 다음 *편집*을 선택합니다.
4. 필요에 따라 다음 필드의 값을 변경할 수 있습니다.
   - 이름
   - 설명
   - 스토리지 할당량
5. *Continue*를 선택합니다.
6. 테넌트 계정에 대한 권한을 선택하거나 해제합니다.
   - 이미 플랫폼 서비스를 사용 중인 테넌트에 대해 해당 서비스를 비활성화하면 테넌트가 S3 버킷에 대해 구성한 서비스가 작동을 멈춥니다. 테넌트에게 오류 메시지가 전송되지 않습니다. 예를 들어, 테넌트가 S3 버킷에 대해 CloudMirror 복제를 구성한 경우, 해당 버킷에 객체를 계속 저장할 수는 있지만, 엔드포인트로 구성한 외부 S3 버킷에는 더 이상 해당 객체의 복사본이 생성되지 않습니다. "S3 테넌트 계정에 대한 플랫폼 서비스 관리"을 참조하십시오.
   - 테넌트 계정이 자체 ID 소스를 사용할지 아니면 Grid Manager에 구성된 ID 소스를 사용할지 결정하려면 자체 **ID** 소스 사용 설정을 변경하십시오.

     *자체 신원 정보 출처 사용*이 다음과 같은 경우:

     - 비활성화 및 선택된 경우, 테넌트가 이미 자체 ID 소스를 활성화한 것입니다. 테넌트는 Grid Manager에 구성된 ID 소스를 사용하기 전에 먼저 자체 ID 소스를 비활성화해야 합니다.

- 비활성화되어 선택되지 않은 경우, StorageGRID 시스템에 대해 SSO가 활성화됩니다. 테넌트는 Grid Manager에 대해 구성된 ID 소스를 사용해야 합니다.

◦ 필요에 따라 **S3 Select** 허용 권한을 선택하거나 해제하십시오. 을 참조하십시오."테넌트 계정에 대한 S3 Select 관리"

◦ 그리드 페더레이션 연결 사용 권한을 제거하려면:

i. **Grid federation** 탭을 선택합니다.

ii. *권한 제거*를 선택합니다.

◦ 그리드 페더레이션 연결 사용 권한을 추가하려면:

i. **Grid federation** 탭을 선택합니다.

ii. 그리드 페더레이션 연결 사용 확인란을 선택하십시오.

iii. 선택적으로 *기존 로컬 사용자 및 그룹 복제*를 선택하여 원격 그리드로 복제할 수 있습니다. 원하는 경우, 진행 중인 복제를 중지하거나 마지막 복제 작업 완료 후 일부 로컬 사용자 또는 그룹이 복제되지 않은 경우 복제를 다시 시도할 수 있습니다.

◦ 최대 보존 기간을 설정하거나 규정 준수 모드를 허용하려면:

> ⓘ 이 설정을 사용하려면 먼저 그리드에서 S3 객체 잠금 기능을 활성화해야 합니다.

i. **S3** 객체 잠금 탭을 선택합니다.

ii. 최대 보존 기간 설정의 경우 값을 입력하고 드롭다운에서 기간을 선택합니다.

iii. *규정 준수 모드 허용*의 경우 확인란을 선택하십시오.

StorageGRID 테넌트의 로컬 루트 사용자 암호 변경

루트 사용자가 계정에서 잠긴 경우 테넌트의 로컬 루트 사용자의 암호를 변경해야 할 수 있습니다.

시작하기 전에

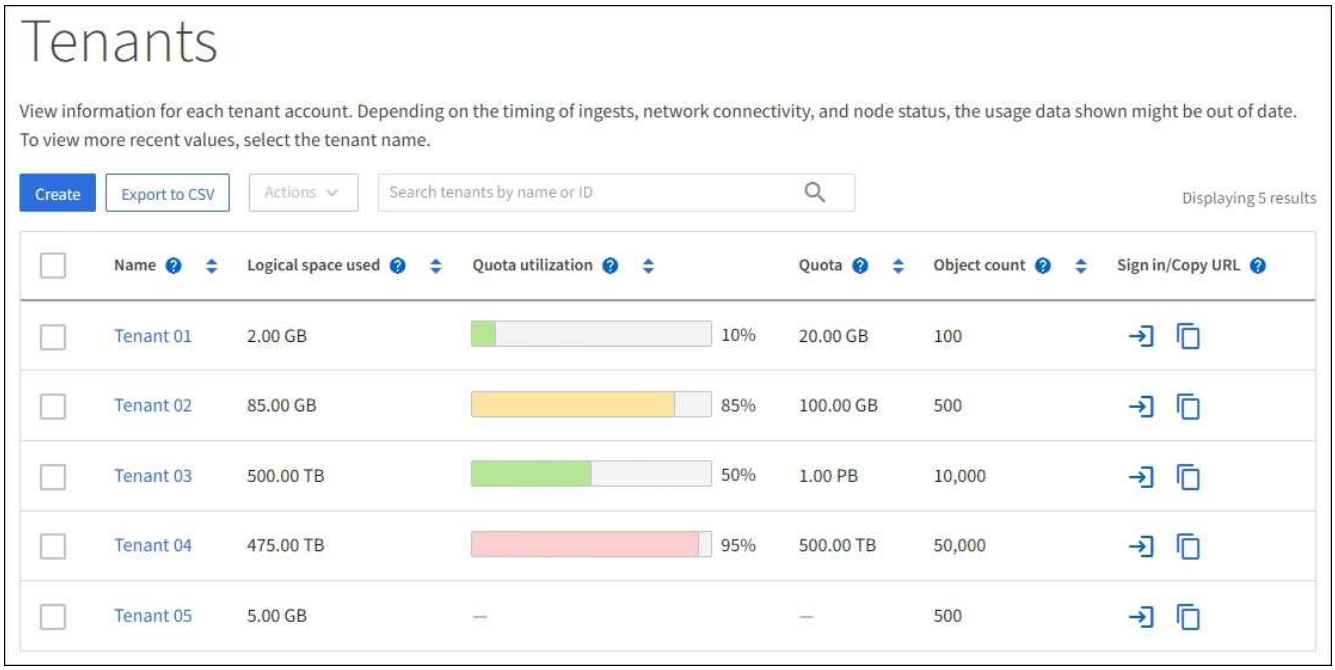
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.

이 작업 정보

StorageGRID 시스템에서 SSO(싱글 사인온)가 활성화된 경우 로컬 루트 사용자는 테넌트 계정에 로그인할 수 없습니다. 루트 사용자 작업을 수행하려면 사용자가 테넌트에 대한 루트 액세스 권한이 있는 페더레이션 그룹에 속해 있어야 합니다.

단계

1. *테넌트*를 선택합니다.



2. 테넌트 계정을 선택합니다. 다음 중 하나를 수행할 수 있습니다.
   - 테넌트의 확인란을 선택하고 작업 > *루트 암호 변경*을 선택합니다.
   - 테넌트 이름을 선택하여 세부 정보 페이지를 표시한 다음 작업 > *루트 암호 변경*을 선택합니다.
3. 테넌트 계정의 새 비밀번호를 입력하십시오.
4. *저장*을 선택하세요.

StorageGRID 테넌트 계정 삭제

테넌트의 시스템 액세스 권한을 영구적으로 제거하려면 테넌트 계정을 삭제할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.
- 테넌트 계정과 연결된 모든 S3 버킷 및 객체를 제거했습니다.
- 테넌트가 그리드 페더레이션 연결을 사용할 수 있도록 허용된 경우, "그리드 페더레이션 연결 사용 권한이 있는 테넌트 삭제"에 대한 고려 사항을 검토했습니다.

단계

1. *테넌트*를 선택합니다.
2. 삭제하려는 테넌트 계정을 찾습니다.

   검색 상자를 사용하여 테넌트 이름 또는 테넌트 ID로 테넌트를 검색하세요.

3. 여러 테넌트를 삭제하려면 확인란을 선택한 다음 작업 > *삭제*를 선택하십시오.
4. 단일 테넌트를 삭제하려면 다음 중 하나를 수행하십시오.
   - 확인란을 선택한 다음 작업 > *삭제*를 선택합니다.

◦ 테넌트 이름을 선택하여 세부 정보 페이지를 표시한 다음 작업 > *삭제*를 선택합니다.

5. *예*를 선택합니다.

플랫폼 서비스 관리

StorageGRID 플랫폼 서비스에 대해 알아보십시오

플랫폼 서비스에는 CloudMirror 복제, 이벤트 알림 및 검색 통합 서비스가 포함됩니다.

S3 테넌트 계정에 플랫폼 서비스를 활성화하는 경우, 테넌트가 이러한 서비스를 사용하는 데 필요한 외부 리소스에 액세스할 수 있도록 그리드를 구성해야 합니다.

플랫폼 서비스는 "브랜치 버킷"에 대해 지원되지 않습니다.

CloudMirror 복제

StorageGRID CloudMirror 복제 서비스는 StorageGRID 버킷의 특정 객체를 지정된 외부 대상으로 미러링하는 데 사용됩니다.

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

CloudMirror 복제는 크로스 그리드 복제 기능과 몇 가지 중요한 유사점과 차이점이 있습니다. 자세한 내용은 "크로스 그리드 복제와 CloudMirror 복제 비교"을 참조하세요.

CloudMirror 소스 버킷에 S3 객체 잠금이 활성화된 경우 CloudMirror 복제가 지원되지 않습니다.

알림

버킷별 이벤트 알림은 객체에 대해 수행된 특정 작업에 대한 알림을 지정된 외부 Kafka 클러스터, 웹훅 엔드포인트 또는 Amazon Simple Notification Service로 전송하는 데 사용됩니다.

예를 들어, 버킷에 추가되는 각 객체에 대해 관리자에게 알림을 보내도록 구성할 수 있습니다. 여기서 객체는 중요한 시스템 이벤트와 관련된 로그 파일을 나타냅니다.

S3 객체 잠금이 활성화된 버킷에서 이벤트 알림을 구성할 수 있지만, 알림 메시지에는 객체의 S3 객체 잠금 메타데이터(보존 기한 및 법적 보존 상태 포함)가 포함되지 않습니다.

검색 통합 서비스

검색 통합 서비스는 S3 객체 메타데이터를 지정된 Elasticsearch 인덱스로 전송하는 데 사용되며, 외부 서비스를 통해 해당 메타데이터를 검색하거나 분석할 수 있습니다.

예를 들어, S3 객체 메타데이터를 원격 Elasticsearch 서비스로 전송하도록 버킷을 구성할 수 있습니다. 그런 다음 Elasticsearch를 사용하여 버킷 전체에서 검색을 수행하고 객체 메타데이터에 있는 패턴에 대한 정교한 분석을 수행할 수 있습니다.

S3 Object Lock이 활성화된 버킷에서 Elasticsearch 통합을 구성할 수 있지만, 객체의 S3 Object Lock 메타데이터(보존 기한 및 법적 보존 상태 포함)는 알림 메시지에 포함되지 않습니다.

플랫폼 서비스를 통해 테넌트는 외부 스토리지 리소스, 알림 서비스, 검색 또는 분석 서비스를 자신의 데이터와 함께 사용할 수 있습니다. 플랫폼 서비스의 대상 위치는 일반적으로 StorageGRID 배포 환경 외부에 있으므로 테넌트가 이러한 서비스를 사용할 수 있도록 허용할지 여부를 결정해야 합니다. 허용하기로 결정했다면 테넌트 계정을 생성하거나 편집할 때 플랫폼 서비스 사용을 활성화해야 합니다. 또한 테넌트가 생성하는 플랫폼 서비스 메시지가 목적지에 도달할 수 있도록 네트워크를 구성해야 합니다.

플랫폼 서비스 이용 관련 권장 사항

플랫폼 서비스를 이용하기 전에 다음 권장 사항을 숙지하십시오.

- StorageGRID 시스템의 S3 버킷에 버전 관리와 CloudMirror 복제가 모두 활성화된 경우, 대상 엔드포인트에 대해서도 S3 버킷 버전 관리를 활성화해야 합니다. 이렇게 하면 CloudMirror 복제를 통해 엔드포인트에 동일한 객체 버전이 생성됩니다.
- CloudMirror 복제, 알림 및 검색 통합이 필요한 S3 요청에 대해 활성 테넌트를 100개 이상 사용하지 않는 것이 좋습니다. 활성 테넌트가 100개를 초과하면 S3 클라이언트 성능이 저하될 수 있습니다.
- 완료할 수 없는 엔드포인트에 대한 요청은 최대 50만 건까지 대기열에 저장됩니다. 이 제한은 활성 테넌트 간에 균등하게 분배됩니다. 신규 테넌트는 일시적으로 이 50만 건 제한을 초과할 수 있으며, 이를 통해 새로 생성된 테넌트가 불공평하게 불이익을 받지 않도록 합니다.

관련 정보

- "플랫폼 서비스 관리"
- "스토리지 프록시 설정 구성"
- "StorageGRID 모니터링"

StorageGRID 플랫폼 서비스용 네트워크 및 포트

S3 테넌트 플랫폼 서비스를 사용하도록 허용하는 경우, 플랫폼 서비스 메시지가 목적지로 전달될 수 있도록 그리드에 대한 네트워킹을 구성해야 합니다.

S3 테넌트 계정을 생성하거나 업데이트할 때 플랫폼 서비스를 활성화할 수 있습니다. 플랫폼 서비스가 활성화되면 테넌트는 S3 버킷에서 CloudMirror 복제, 이벤트 알림 또는 검색 통합 메시지를 수신할 대상 엔드포인트를 생성할 수 있습니다. 이러한 플랫폼 서비스 메시지는 ADC 서비스를 실행하는 스토리지 노드에서 대상 엔드포인트로 전송됩니다.

예를 들어, 테넌트는 다음과 같은 유형의 대상 엔드포인트를 구성할 수 있습니다.

- 로컬에서 호스팅되는 Elasticsearch 클러스터
- Amazon Simple Notification Service 메시지 수신을 지원하는 로컬 애플리케이션
- 로컬에서 호스팅되는 Kafka 클러스터
- HTTP POST 알림 요청을 지원하는 외부 또는 로컬 호스팅 웹훅 엔드포인트.

  이 엔드포인트는 Fluentd와 같은 다양한 웹 서버, 프레임워크 또는 데이터 처리 도구에서 호스팅될 수 있습니다.

- 동일하거나 다른 StorageGRID 인스턴스에 로컬로 호스팅된 S3 버킷
- Amazon Web Services의 엔드포인트와 같은 외부 엔드포인트.

플랫폼 서비스 메시지가 정상적으로 전달되도록 하려면 ADC 스토리지 노드가 포함된 네트워크를 구성해야 합니다. 대상 엔드포인트로 플랫폼 서비스 메시지를 전송하는 데 다음 포트를 사용할 수 있도록 설정해야 합니다.

기본적으로 플랫폼 서비스 메시지는 다음 포트를 통해 전송됩니다.

- **80**: http로 시작하는 엔드포인트 URI(대부분의 엔드포인트)의 경우
- **443**: https로 시작하는 엔드포인트 URI의 경우(대부분의 엔드포인트)
- **9092**: http 또는 https로 시작하는 엔드포인트 URI의 경우(Kafka 엔드포인트만 해당)

테넌트는 엔드포인트를 생성하거나 편집할 때 다른 포트를 지정할 수 있습니다.

> StorageGRID 배포를 CloudMirror 복제 대상으로 사용하는 경우, 복제 메시지가 80번 또는 443번 포트 이외의 포트로 수신될 수 있습니다. 대상 StorageGRID 배포에서 S3에 사용하는 포트가 엔드포인트에 지정되어 있는지 확인하십시오.

투명하지 않은 프록시 서버를 사용하는 경우 인터넷상의 엔드포인트와 같은 외부 엔드포인트로 메시지를 보낼 수 있도록 "스토리지 프록시 설정 구성"도 해야 합니다.

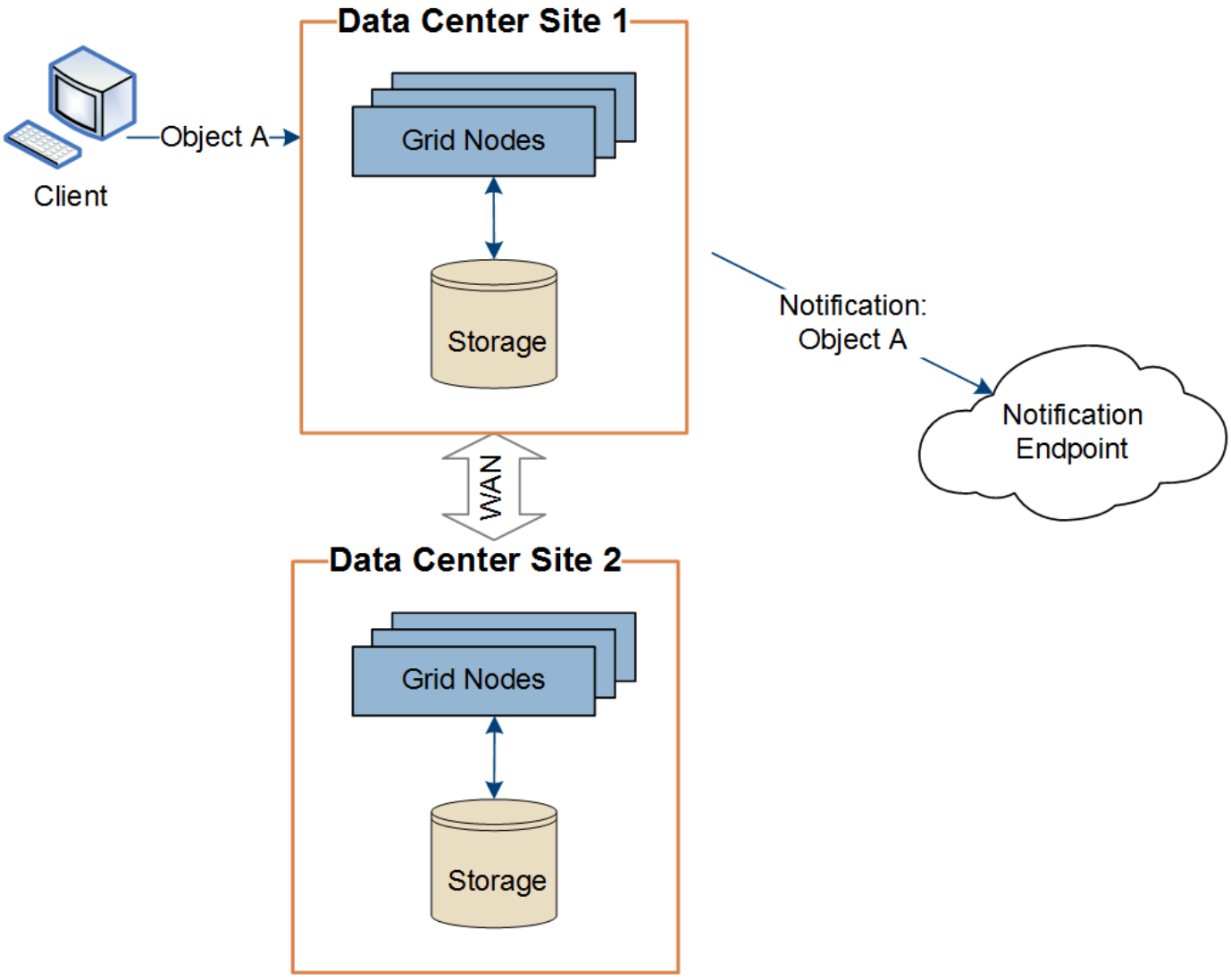
관련 정보

"테넌트 계정 사용"

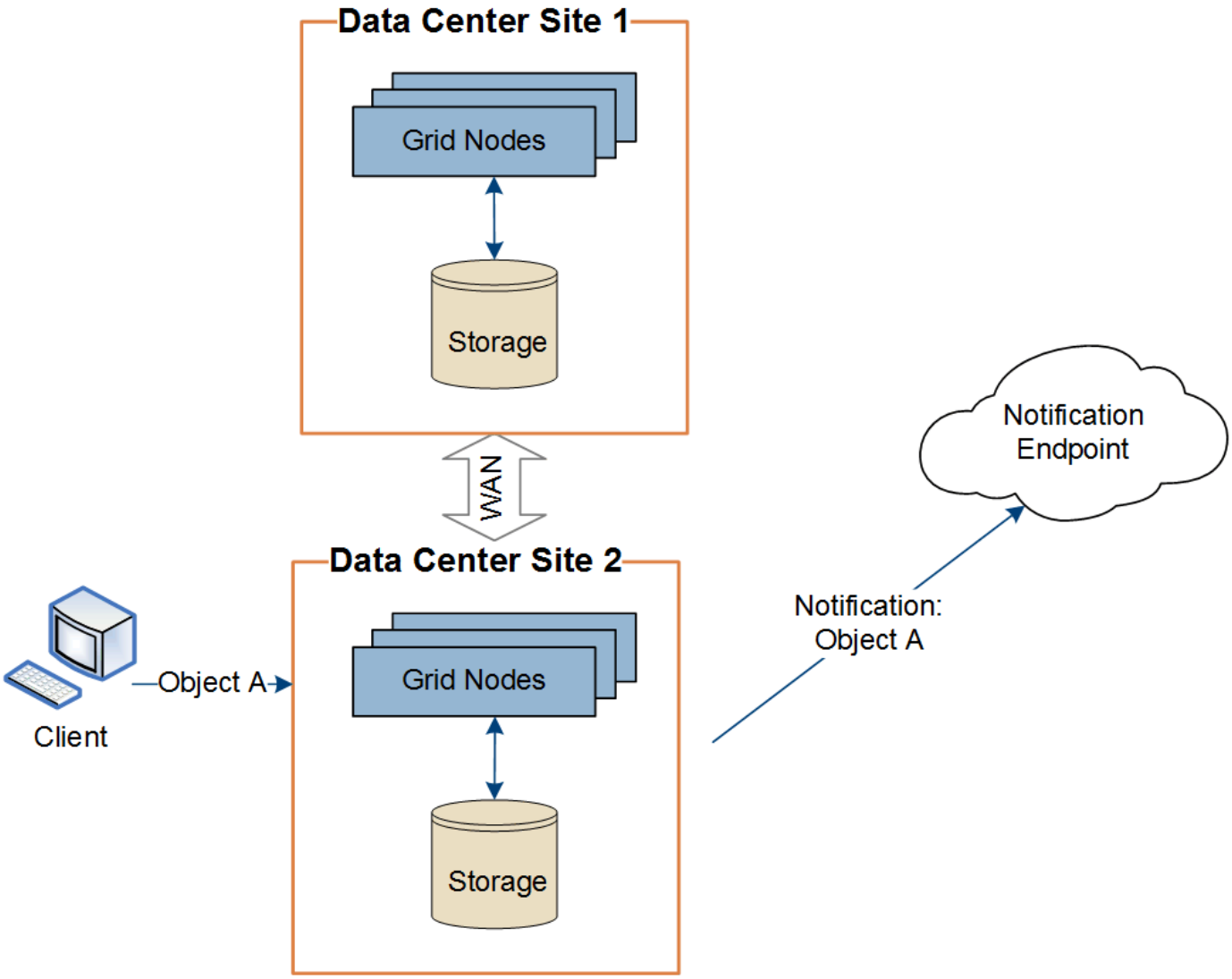
StorageGRID 플랫폼 서비스 메시지의 사이트별 전달

모든 플랫폼 서비스 운영은 사이트별로 수행됩니다.

즉, 테넌트가 클라이언트를 사용하여 데이터 센터 사이트 1의 게이트웨이 노드에 연결하여 객체에 대한 S3 API 생성 작업을 수행하면 해당 작업에 대한 알림이 트리거되어 데이터 센터 사이트 1에서 전송됩니다.



클라이언트가 이후 데이터 센터 사이트 2에서 동일한 객체에 대해 S3 API 삭제 작업을 수행하면 삭제 작업에 대한 알림이 트리거되어 데이터 센터 사이트 2에서 전송됩니다.



각 사이트의 네트워크가 플랫폼 서비스 메시지를 목적지로 전달할 수 있도록 구성되어 있는지 확인하십시오.

StorageGRID 플랫폼 서비스 문제 해결

플랫폼 서비스에서 사용되는 엔드포인트는 테넌트 사용자가 테넌트 관리자에서 생성하고 관리합니다. 하지만 테넌트 플랫폼 서비스 구성 또는 사용에 문제가 있는 경우, 그리드 관리자를 사용하여 문제를 해결할 수 있습니다.

새로운 엔드포인트 관련 문제

테넌트가 플랫폼 서비스를 사용하려면 먼저 테넌트 관리자를 통해 하나 이상의 엔드포인트를 생성해야 합니다. 각 엔드포인트는 StorageGRID S3 버킷, Amazon Web Services 버킷, Amazon Simple Notification Service 토픽, Kafka 토픽 또는 로컬이나 AWS에서 호스팅되는 Elasticsearch 클러스터와 같은 플랫폼 서비스의 외부 대상을 나타냅니다. 각 엔드포인트에는 외부 리소스의 위치와 해당 리소스에 액세스하는 데 필요한 자격 증명이 모두 포함됩니다.

테넌트가 엔드포인트를 생성하면 StorageGRID 시스템은 해당 엔드포인트가 존재하는지, 그리고 지정된 자격 증명을 사용하여 접근할 수 있는지 확인합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

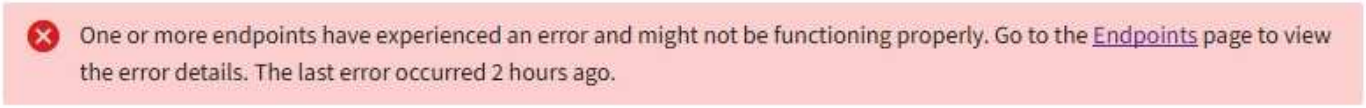
엔드포인트 유효성 검사에 실패하면 실패 사유를 설명하는 오류 메시지가 표시됩니다. 테넌트 사용자는 문제를 해결한

후 엔드포인트를 다시 생성해야 합니다.

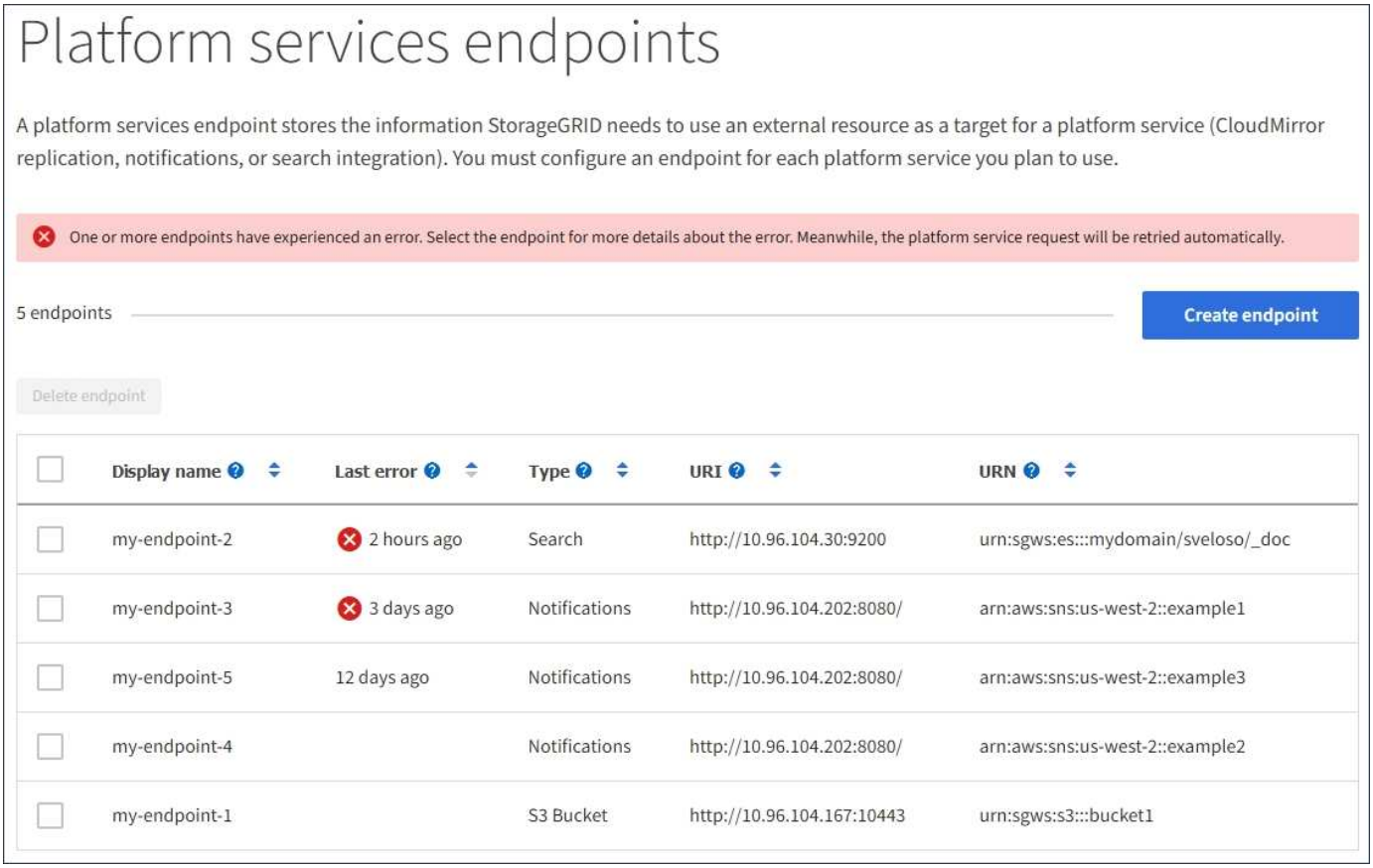
테넌트 계정에 플랫폼 서비스가 활성화되어 있지 않으면 엔드포인트 생성이 실패합니다.

기존 엔드포인트 관련 문제

StorageGRID가 기존 엔드포인트에 연결을 시도하는 동안 오류가 발생하면 테넌트 관리자의 대시보드에 메시지가 표시됩니다.



테넌트 사용자는 엔드포인트 페이지에서 각 엔드포인트에 대한 최근 오류 메시지를 확인하고 오류 발생 시점을 파악할 수 있습니다. 마지막 오류 열에는 각 엔드포인트의 최근 오류 메시지와 오류 발생 시점이 표시됩니다. ⊗ 아이콘이 포함된 오류는 지난 7일 이내에 발생한 오류입니다.



마지막 오류 열의 일부 오류 메시지에는 괄호 안에 logID가 포함될 수 있습니다. 그리드 관리자 또는 기술 지원 담당자는 이 ID를 사용하여 bycast.log에서 오류에 대한 자세한 정보를 찾을 수 있습니다.

프록시 서버 관련 문제

스토리지 노드와 플랫폼 서비스 엔드포인트 간에 "스토리지 프록시"를 구성한 경우, 프록시 서비스에서 StorageGRID의 메시지를 허용하지 않으면 오류가 발생할 수 있습니다. 이러한 문제를 해결하려면 프록시 서버의 설정을 확인하여 플랫폼 서비스 관련 메시지가 차단되지 않도록 하십시오.

오류가 발생했는지 확인합니다.

지난 7일 동안 엔드포인트 오류가 발생한 경우, 테넌트 관리자의 대시보드에 알림 메시지가 표시됩니다. 엔드포인트 페이지에서 오류에 대한 자세한 내용을 확인할 수 있습니다.

클라이언트 작업이 실패합니다.

일부 플랫폼 서비스 문제로 인해 S3 버킷에 대한 클라이언트 작업이 실패할 수 있습니다. 예를 들어, 내부 복제 상태 머신(RSM) 서비스가 중지되거나 전송 대기 중인 플랫폼 서비스 메시지가 너무 많으면 S3 클라이언트 작업이 실패합니다.

서비스 상태를 확인하려면:

1. 노드 > 사이트 > 스토리지 노드 > 개요 를 선택합니다.
2. 알림 테이블에서 활성화된 알림을 확인하십시오.
3. 활성화된 경고를 모두 해결하십시오. 필요한 경우 기술 지원에 문의하십시오.

복구 가능한 엔드포인트 오류 및 복구 불가능한 엔드포인트 오류

엔드포인트가 생성된 후 플랫폼 서비스 요청 오류는 다양한 이유로 발생할 수 있습니다. 일부 오류는 사용자 개입을 통해 복구할 수 있습니다. 예를 들어, 복구 가능한 오류는 다음과 같은 이유로 발생할 수 있습니다.

- 사용자의 자격 증명이 삭제되었거나 만료되었습니다.
- 대상 버킷이 존재하지 않습니다.
- 알림을 전달할 수 없습니다.

StorageGRID에서 복구 가능한 오류가 발생하면 플랫폼 서비스 요청이 성공할 때까지 재시도됩니다.

다른 오류는 복구할 수 없습니다. 예를 들어, 복구 불가능한 오류는 다음과 같은 이유로 발생할 수 있습니다.

- 해당 엔드포인트가 삭제되었습니다.
- 웹훅 엔드포인트 대상이 알림 요청에 `400 Bad Request` 오류로 응답합니다.

StorageGRID에서 복구할 수 없는 엔드포인트 오류가 발생하는 경우:

- Grid Manager에서 지원 > 도구 > 메트릭 > **Grafana** > *플랫폼 서비스 개요*로 이동하여 오류 세부 정보를 확인하십시오.
- 테넌트 관리자에서 **STORAGE (S3)** > *Platform Services Endpoints*로 이동하여 오류 세부 정보를 확인하십시오.
- `/var/local/log/bycast-err.log`관련 오류가 있는지 확인하십시오. ADC 서비스가 있는 스토리지 노드에는 이 로그 파일이 포함되어 있습니다.

플랫폼 서비스 메시지를 전달할 수 없습니다

대상에서 플랫폼 서비스 메시지를 수락할 수 없는 문제가 발생하면 버킷에 대한 클라이언트 작업은 성공하지만 플랫폼 서비스 메시지는 전달되지 않습니다. 예를 들어, 대상의 자격 증명이 업데이트되어 StorageGRID가 더 이상 대상 서비스에 인증할 수 없는 경우 이 오류가 발생할 수 있습니다.

관련 알림을 확인하십시오.

플랫폼 서비스 요청 처리 속도가 느려짐

StorageGRID 소프트웨어는 버킷으로 들어오는 S3 요청 속도가 대상 엔드포인트가 요청을 수신할 수 있는 속도를 초과하는 경우 해당 요청 속도를 제한할 수 있습니다. 속도 제한은 대상 엔드포인트로 전송될 요청이 누적되어 대기 중인 경우에만 발생합니다.

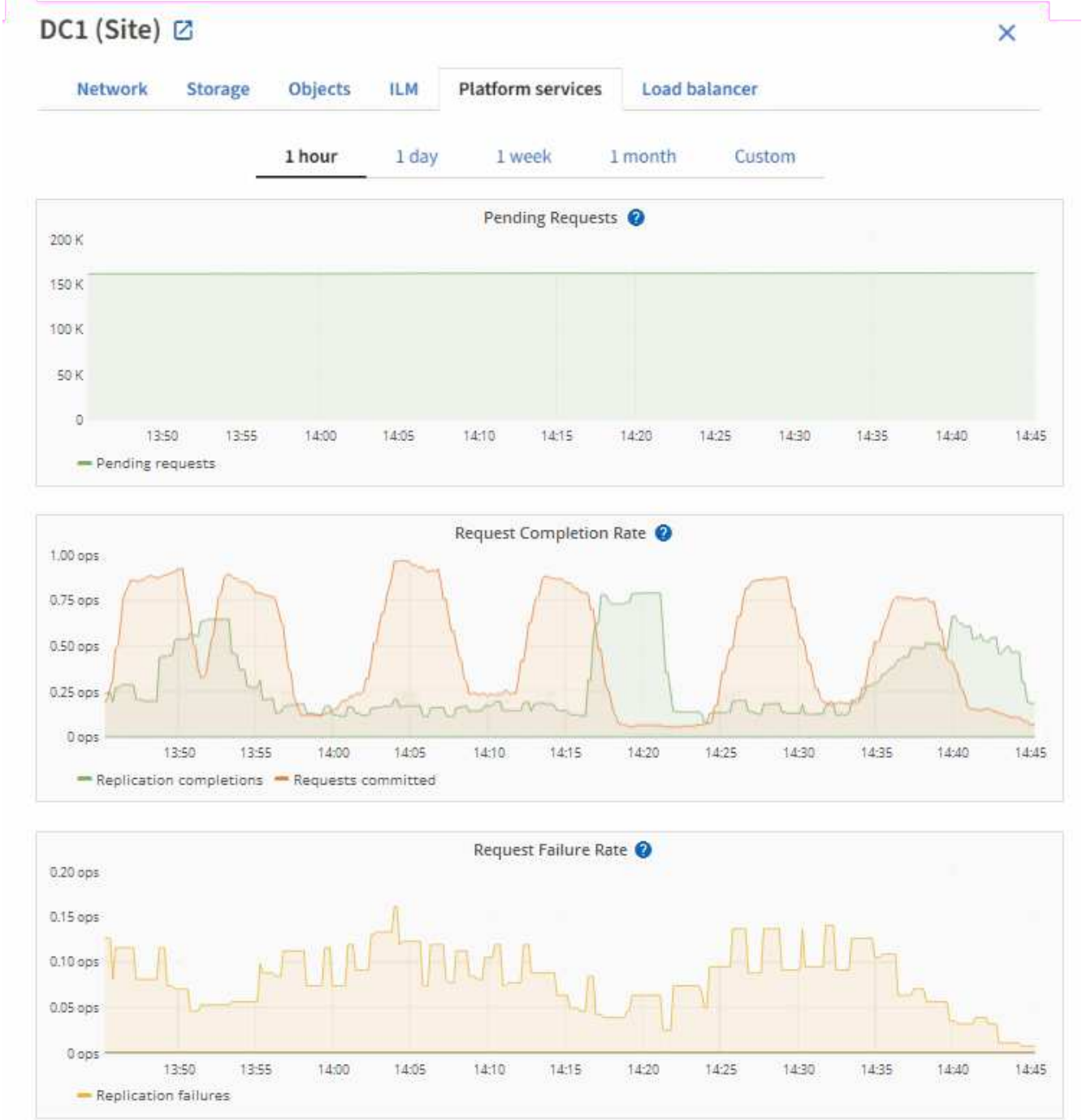
눈에 띄는 유일한 영향은 수신 S3 요청 실행 시간이 더 오래 걸린다는 것입니다. 성능 저하가 현저하게 감지되기 시작하면 수집 속도를 줄이거나 용량이 더 큰 엔드포인트를 사용해야 합니다. 요청 백로그가 계속 증가하면 클라이언트의 S3 작업(예: PUT 요청)이 결국 실패하게 됩니다.

CloudMirror 요청은 일반적으로 검색 통합 또는 이벤트 알림 요청보다 더 많은 데이터 전송을 포함하므로 대상 엔드포인트의 성능에 더 큰 영향을 받을 가능성이 높습니다.

플랫폼 서비스 요청이 실패합니다

플랫폼 서비스의 요청 실패율을 보려면:

1. *노드*를 선택합니다.
2. 사이트 > *플랫폼 서비스*를 선택합니다.
3. 요청 오류율 차트를 확인합니다.



플랫폼 서비스 이용 불가 알림

플랫폼 서비스 이용 불가 경고는 RSM 서비스를 사용하는 스토리지 노드 중 실행 중이거나 사용 가능한 노드 수가 너무 적어 해당 사이트에서 플랫폼 서비스 작업을 수행할 수 없음을 나타냅니다.

RSM 서비스는 플랫폼 서비스 요청이 각각의 엔드포인트로 전송되도록 보장합니다.

이 경고를 해결하려면 사이트에서 RSM 서비스가 포함된 스토리지 노드를 확인하십시오. (RSM 서비스는 ADC 서비스가 포함된 스토리지 노드에 있습니다.) 그런 다음 해당 스토리지 노드 중 과반수가 실행 중이고 사용 가능한 상태인지 확인하십시오.

한 사이트에서 RSM 서비스를 포함하는 스토리지 노드가 두 개 이상 장애가 발생하면 해당 사이트에 대한 보류 중인 플랫폼 서비스 요청이 모두 손실됩니다.

플랫폼 서비스 엔드포인트에 대한 추가 문제 해결 지침

자세한 내용은 테넌트 계정 사용 › 플랫폼 서비스 엔드포인트 문제 해결을 참조하십시오.

관련 정보

"StorageGRID 시스템 문제 해결"

StorageGRID의 테넌트 계정에 대한 S3 Select 관리

특정 S3 테넌트가 S3 Select를 사용하여 개별 개체에 대한 SelectObjectContent 요청을 실행할 수 있도록 허용할 수 있습니다.

S3 Select는 데이터베이스 및 관련 리소스를 배포하지 않고도 대량의 데이터를 효율적으로 검색할 수 있는 방법을 제공합니다. 또한 데이터 검색 비용과 지연 시간을 줄여줍니다.

S3 Select란 무엇인가요?

S3 Select를 사용하면 S3 클라이언트가 SelectObjectContent 요청을 통해 객체에서 필요한 데이터만 필터링하고 검색할 수 있습니다. StorageGRID 의 S3 Select 구현에는 S3 Select 명령 및 기능의 일부가 포함되어 있습니다.

S3 Select 사용을 위한 고려 사항 및 요구 사항

Grid 관리 요구사항

그리드 관리자는 테넌트에게 S3 Select 권한을 부여해야 합니다. *S3 Select 허용*은 "테넌트 생성" 또는 "테넌트 편집" 할 때 선택합니다.

객체 형식 요구 사항

조회하려는 객체는 다음 형식 중 하나여야 합니다.

- **CSV**. 있는 그대로 사용하거나 GZIP 또는 BZIP2 아카이브로 압축할 수 있습니다.
- **Parquet**. Parquet 객체에 대한 추가 요구사항:
  - S3 Select는 GZIP 또는 Snappy를 사용한 컬럼형 압축만 지원합니다. S3 Select는 Parquet 객체에 대한 전체 객체 압축을 지원하지 않습니다.
  - S3 Select는 Parquet 출력을 지원하지 않습니다. 출력 형식을 CSV 또는 JSON으로 지정해야 합니다.
  - 압축되지 않은 행 그룹의 최대 크기는 512MB입니다.
  - 객체의 스키마에 명시된 데이터 형식을 사용해야 합니다.
  - INTERVAL, JSON, LIST, TIME 또는 UUID 논리 유형은 사용할 수 없습니다.

엔드포인트 요구 사항

SelectObjectContent 요청은 "StorageGRID 로드 밸런서 엔드포인트"으로 전송되어야 합니다.

엔드포인트에서 사용하는 관리 노드 및 게이트웨이 노드는 다음 중 하나여야 합니다.

- 서비스 어플라이언스 노드
- VMware 기반 소프트웨어 노드
- cgroup v2가 활성화된 커널을 실행하는 베어메탈 노드

일반적인 고려 사항

쿼리를 스토리지 노드로 직접 보낼 수 없습니다.

SelectObjectContent 요청은 모든 S3 클라이언트와 모든 테넌트의 로드 밸런서 성능을 저하시킬 수 있습니다. 이 기능은 필요한 경우에만, 그리고 신뢰할 수 있는 테넌트에 대해서만 활성화하십시오.

"S3 Select 사용 설명서"을 참조하십시오.

시간 경과에 따른 S3 Select 작업의 "Grafana 차트"을(를) 보려면 그리드 관리자에서 지원 > 도구 > *메트릭*을 선택하십시오.

클라이언트 연결 구성

StorageGRID에 대한 **S3** 클라이언트 연결을 구성합니다

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

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

구성 작업

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

필수 작업

다음 사항을 확보해야 합니다.

- IP 주소
- 도메인 이름
- SSL 인증서

선택적 작업

선택적으로 구성합니다.

- ID 페더레이션
- SSO

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

S3 설정 마법사 사용

S3 설정 마법사의 단계를 따르십시오.

수동으로 구성

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

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

   필요에 따라 추가적인 애플리케이션 설정을 수행하십시오.

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

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

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

어떤 값이 필요합니까**?**

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

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

가치	값이 구성된 위치	값이 사용되는 곳
버킷/컨테이너 이름	StorageGRID > 테넌트 및 버킷	클라이언트 애플리케이션

이 값을 어떻게 얻을 수 있습니까?

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

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

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

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

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

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

StorageGRID의 S3 클라이언트 보안

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

요약

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

연결 보안
: TLS

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

클라이언트 인증
: S3 계정 액세스 키 ID 및 비밀 액세스 키

클라이언트 승인
: 버킷 소유권 및 모든 관련 액세스 제어 정책

StorageGRID가 클라이언트 애플리케이션에 보안을 제공하는 방법

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

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

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

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

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

  HTTPS가 기본 프로토콜이며 권장됩니다.

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

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

보안 인증서 및 클라이언트 애플리케이션

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

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

  "로드 밸런싱 고려 사항"을 참조하십시오.

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

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

TLS 라이브러리에서 지원하는 해싱 및 암호화 알고리즘

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

지원되는 **TLS** 버전

StorageGRID는 TLS 1.2 및 TLS 1.3을 지원합니다.

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

S3 설정 마법사 사용

StorageGRID S3 setup wizard 고려 사항 및 요구 사항

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

S3 설정 마법사를 사용하는 경우

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

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

마법사를 사용하기 전에

마법사를 사용하기 전에 다음 필수 조건을 모두 충족했는지 확인하십시오.

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

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

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

ID 페더레이션 및 **SSO** 구성

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

도메인 이름 획득 및 구성

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

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

로드 밸런서 및 보안 인증서 요구 사항 검토

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

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

그리드 페더레이션 연결 구성

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

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

StorageGRID에서 **S3** 설정 마법사에 액세스하여 완료합니다

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

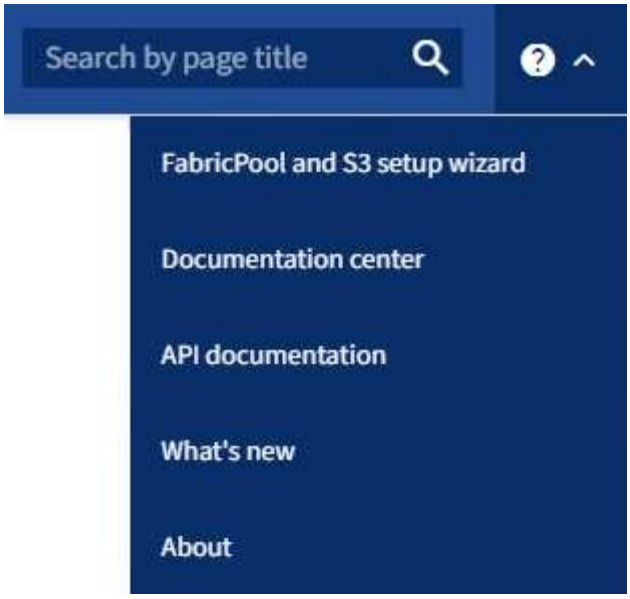
시작하기 전에

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

마법사에 액세스합니다

단계

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



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

6단계 중 **1**단계**: HA** 그룹 구성

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

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

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

단계

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

HA 그룹 생성

a. 새 HA 그룹을 생성하려면 *HA 그룹 생성*을 선택하십시오.

b. 세부 정보 입력 단계에서 다음 필드를 입력합니다.

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

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

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

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

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

행을 드래그하여 우선순위 순서 열의 값을 변경합니다.

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

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

e. **IP** 주소 입력 단계에서 다음 필드를 입력합니다.

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

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

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

g. 로드 밸런싱 단계로 이동하려면 *계속*을 선택하십시오.

기존 **HA** 그룹 사용

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

b. 로드 밸런싱 단계로 이동하려면 *계속*을 선택하십시오.

6단계 중 **2**단계**:** 로드 밸런싱 엔드포인트 구성

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

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

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

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

엔드포인트 생성

단계

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

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

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

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

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

4. 테넌트 액세스 단계에서는 다음 중 하나를 선택하십시오.

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

5. 인증서 첨부 단계에서는 다음 중 하나를 선택하십시오.

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

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

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

기존 로드 밸런서 엔드포인트 사용

단계

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

외부 로드 밸런서 사용

단계

1. 외부 로드 밸런서를 사용하려면 다음 필드를 작성하십시오.

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

2. *계속*을 선택하여 테넌트 및 버킷 단계로 이동합니다.

6단계 중 **3**단계**:** 테넌트 및 버킷 생성

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

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

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

단계

1. 테넌트 계정의 이름을 입력합니다.

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

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

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

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

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

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

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

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

      버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

   b. 이 버킷에 대한 *지역*을 선택합니다.

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

5. *생성하고 계속하기*를 선택합니다.

6단계 중 4단계: 데이터 다운로드

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

단계

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

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

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

6단계 중 5단계: S3에 대한 ILM 규칙 및 ILM 정책 검토

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

단계

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

6단계 중 **6**단계**:** 요약 검토

단계

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

HA 그룹 관리

StorageGRID 고가용성 그룹에 대해 알아보세요

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

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

각 HA 그룹은 선택된 노드의 공유 서비스에 대한 액세스를 제공합니다.

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

HA 그룹은 어떻게 생성하나요**?**

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

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

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

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

지침은 "고가용성 그룹 구성"을 참조하십시오.

활성 인터페이스란 무엇입니까?

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

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

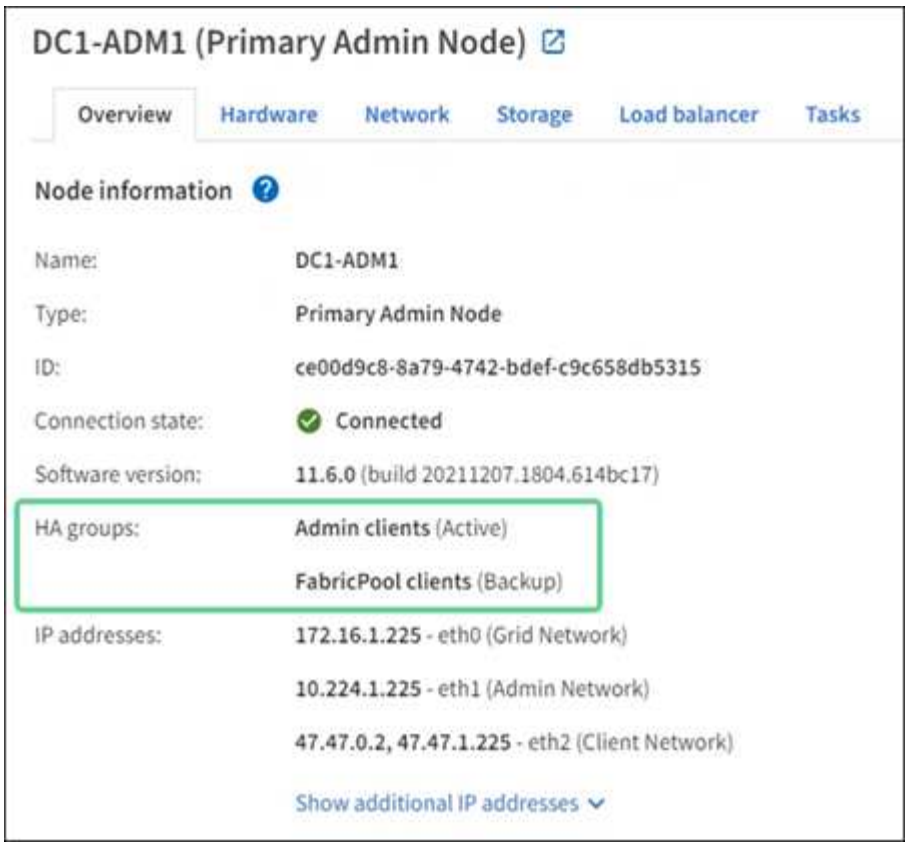
노드의 현재 HA 그룹 상태 보기

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

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

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

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



활성 인터페이스에 오류가 발생하면 어떻게 됩니까**?**

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

장애 조치는 다음과 같은 이유로 발생할 수 있습니다.

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

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

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

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

StorageGRID HA 그룹이 고가용성을 제공하는 방법

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

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

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

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

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

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

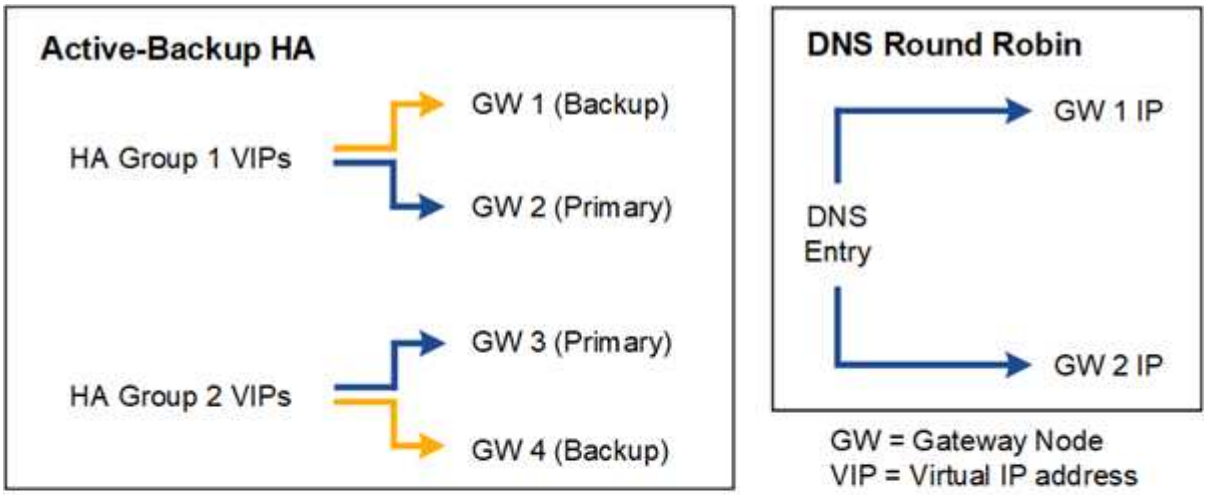
그리드 관리자 또는 테넌트 관리자 서비스에 장애가 발생하면 HA 그룹 페일오버가 트리거되지 않습니다.

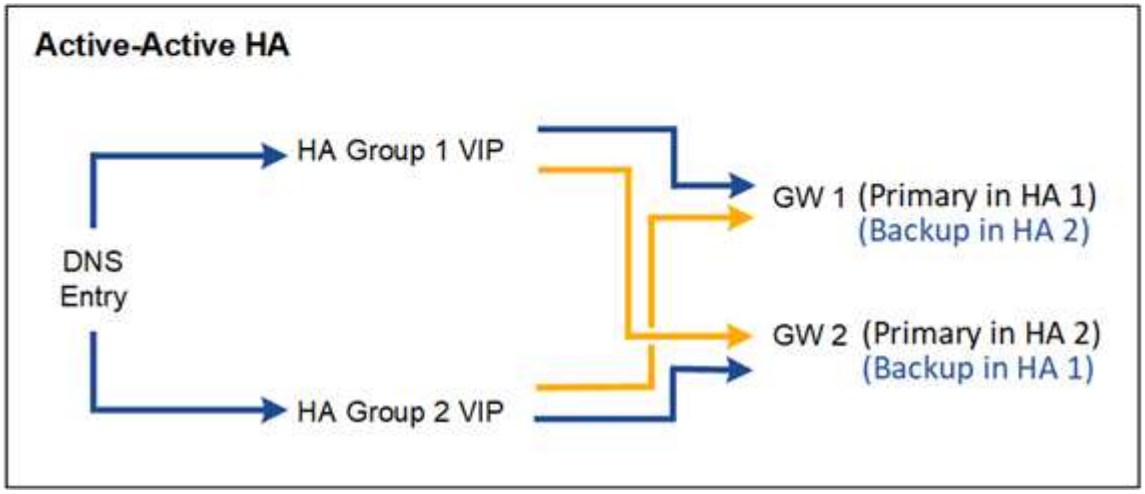
장애 조치가 발생할 때 Grid Manager 또는 테넌트 관리자에 로그인되어 있는 경우 로그아웃되므로 작업을 재개하려면 다시 로그인해야 합니다.

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

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

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





이 표는 다이어그램에 표시된 각 HA 구성의 이점을 요약합니다.

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

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

StorageGRID에서 고가용성 그룹 구성

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

StorageGRID 시스템은 최대 255개의 HA 그룹을 가질 수 있습니다.

시작하기 전에

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

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

고가용성 그룹 생성

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

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

마법사에 액세스합니다

단계

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

HA 그룹에 대한 세부 정보를 입력합니다**.**

단계

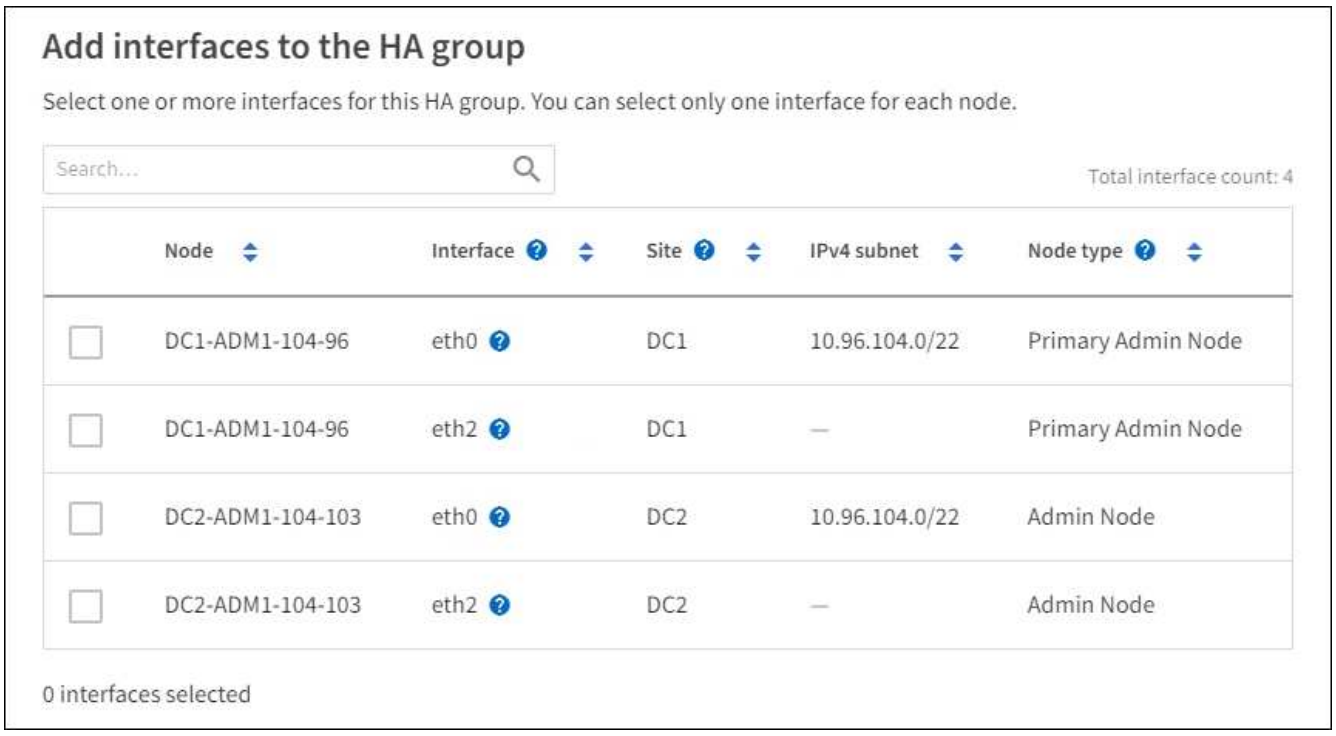
1. HA 그룹에 고유한 이름을 제공하십시오.
2. 선택적으로 HA 그룹에 대한 설명을 입력할 수 있습니다.
3. *Continue*를 선택합니다.

HA 그룹에 인터페이스 추가

단계

1. 이 HA 그룹에 추가할 인터페이스를 하나 이상 선택하십시오.

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

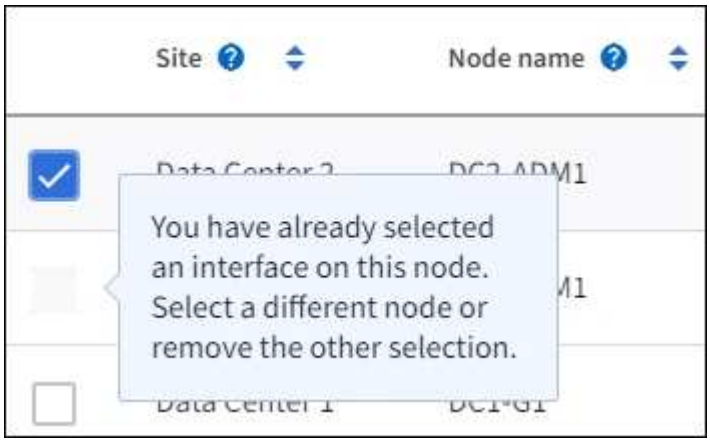


VLAN 인터페이스를 생성한 후 새 인터페이스가 테이블에 나타날 때까지 최대 5분 정도 기다리십시오.

인터페이스 선택 가이드라인

- 최소한 하나의 인터페이스를 선택해야 합니다.
- 노드당 하나의 인터페이스만 선택할 수 있습니다.

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



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

2. *Continue*를 선택합니다.

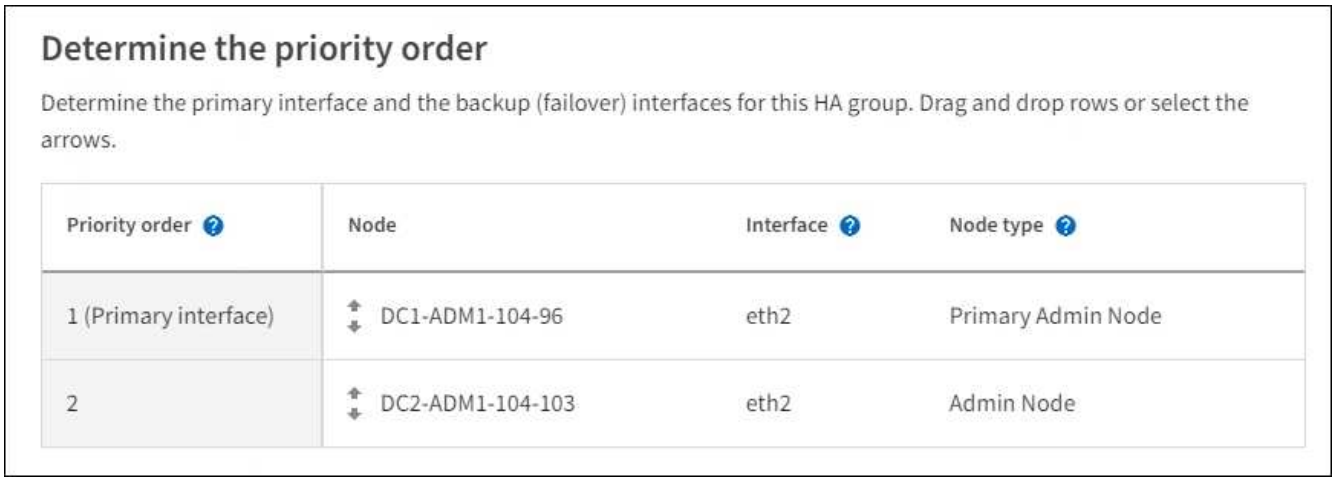
우선순위 결정

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

단계

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

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



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

2. *Continue*를 선택합니다.

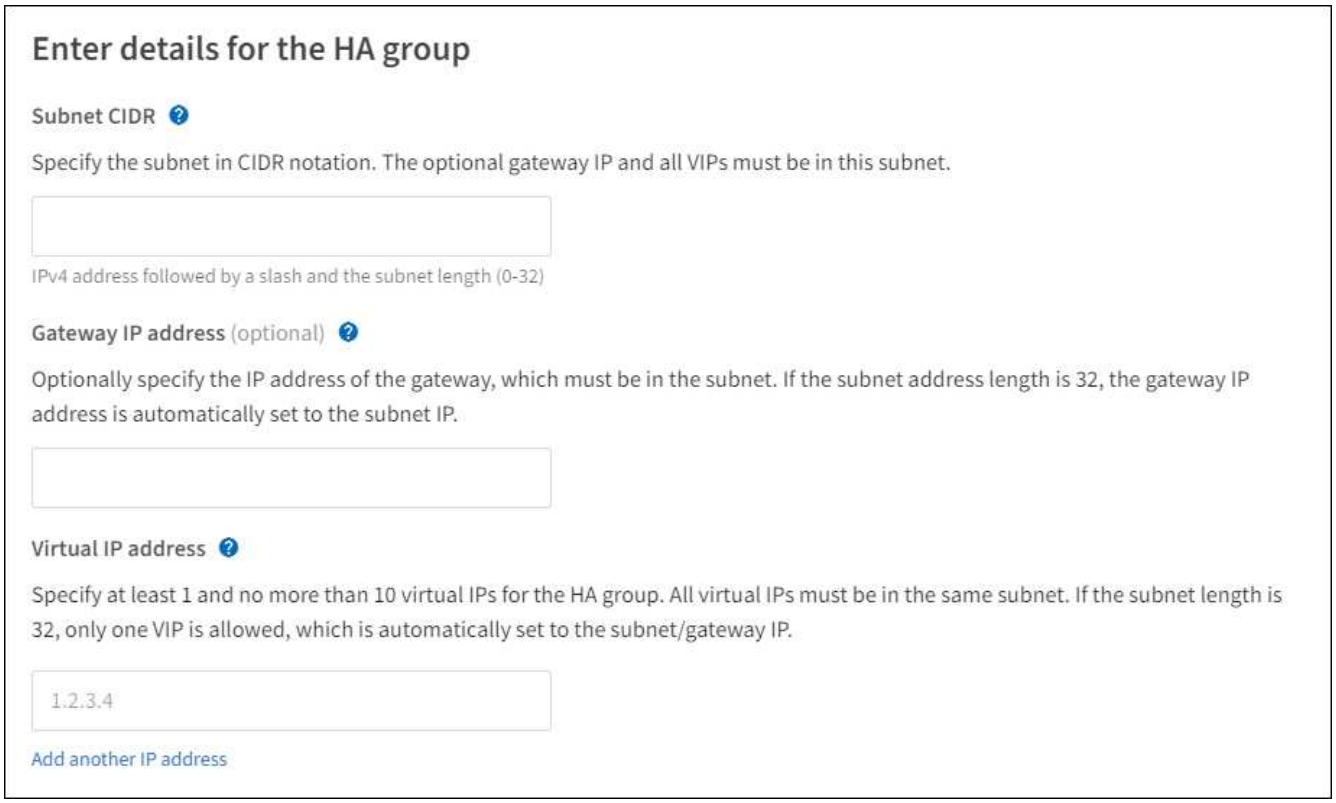
IP 주소를 입력합니다

단계

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

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

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



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

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

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

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

4. *HA 그룹 생성*을 선택하고 *완료*를 선택합니다.

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

다음 단계

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

고가용성 그룹 편집

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

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

단계

1. 구성 > 네트워크 > *고가용성 그룹*을 선택하십시오.

   고가용성 그룹 페이지에는 기존의 모든 HA 그룹이 표시됩니다.

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

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

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

고가용성 그룹 제거

한 번에 하나 이상의 고가용성(HA) 그룹을 제거할 수 있습니다.

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

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

단계

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

c. 작업 > *엔드포인트 바인딩 모드 편집*을 선택합니다.

d. HA 그룹을 제거하도록 바인딩 모드를 업데이트합니다.

e. *변경 사항 저장*을 선택합니다.

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

4. 작업 > *HA 그룹 제거*를 선택합니다.

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

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

${post_edited_translations.segment}

StorageGRID 로드 밸런싱에 대해 알아보십시오

로드 밸런싱을 사용하여 S3 클라이언트의 데이터 수집 및 검색 워크로드를 처리할 수 있습니다.

로드 밸런싱이란 무엇입니까**?**

클라이언트 애플리케이션이 StorageGRID 시스템에서 데이터를 저장하거나 검색할 때, StorageGRID는 로드 밸런서를 사용하여 수집 및 검색 워크로드를 관리합니다. 로드 밸런싱은 워크로드를 여러 스토리지 노드에 분산시켜 속도와 연결 용량을 극대화합니다.

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

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

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

로드 밸런싱 노드는 몇 개가 필요합니까**?**

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

로드 밸런서 엔드포인트란 무엇인가요**?**

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

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

- "로드 밸런서 엔드포인트 구성"

- "S3 설정 마법사 사용"
- "FabricPool 설정 마법사 사용"

로드 밸런서 캐싱에 대한 고려 사항

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

로드 밸런서 엔드포인트를 생성할 때 다음 사항을 고려하세요.

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

캐싱에 적합한 워크로드의 예시

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

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

캐싱에 적합하지 않은 워크로드의 예

- FabricPool
- 백업 애플리케이션
- 스토리지 계층화

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

캐시되지 않는 객체 및 요청 유형

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

캐시되지 않은 요청은 캐시가 활성화되지 않은 것처럼 상위 LDR로 전달됩니다.

관련 정보

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

포트에 대한 고려 사항

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

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

네트워크 프로토콜 고려 사항

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

로드 밸런서 엔드포인트 인증서에 대한 고려 사항

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

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

  로드 밸런서 엔드포인트를 생성하기 전에 다음 파일들을 확보해야 합니다.

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

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

어떤 값이 필요합니까?

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

인증서의 주체 **DN**(고유 이름) 항목에는 클라이언트 애플리케이션이 StorageGRID에 사용할 정규화된 도메인 이름이 포함되어야 합니다. 예를 들면 다음과 같습니다.

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

필요에 따라 인증서는 와일드카드를 사용하여 로드 밸런서 서비스를 실행하는 모든 관리 노드 및 게이트웨이 노드의 정규화된 도메인 이름을 나타낼 수 있습니다. 예를 들어, `.storagegrid.example.com` 와일드카드를 사용하여 `adm1.storagegrid.example.com` 및 `gn1.storagegrid.example.com`을 나타냅니다.

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

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

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

보안 인증서에 있는 각 이름에 대해 DNS 항목을 정의해야 합니다.

만료 예정인 인증서는 어떻게 관리하나요?

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

인증서 만료 문제를 방지하려면 다음 모범 사례를 따르십시오.

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

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

결합 모드에 대한 고려 사항

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

다음 바인딩 모드 중 하나를 지정할 수 있습니다.

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

테넌트 액세스 관련 고려 사항

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

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

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

테넌트 액세스 예시

이 보안 기능이 어떻게 작동하는지 이해하려면 다음 예를 살펴보십시오.

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

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

CPU 가용성

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

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

StorageGRID 로드 밸런서 엔드포인트를 구성합니다

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

시작하기 전에

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

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

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

참조하십시오.

로드 밸런서 엔드포인트 생성

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

마법사에 액세스합니다

단계

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

엔드포인트 세부 정보를 입력합니다

단계

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

S3 클라이언트

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

관리 인터페이스

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

필드	설명
신뢰할 수 없는 클라이언트 네트워크	이 엔드포인트를 신뢰할 수 없는 클라이언트 네트워크에서 액세스할 수 있도록 하려면 *예*를 선택하십시오. 그렇지 않으면 *아니요*를 선택하십시오. '예'를 선택하면 신뢰할 수 없는 모든 클라이언트 네트워크에서 해당 포트가 열립니다. 참고: 로드 밸런서 엔드포인트를 생성할 때만 신뢰할 수 없는 클라이언트 네트워크에 대해 포트를 열거나 닫도록 구성할 수 있습니다.

1. *Continue*를 선택합니다.

바인딩 모드를 선택합니다

단계

1. 엔드포인트에 대한 바인딩 모드를 선택하여 모든 IP 주소를 사용하거나 특정 IP 주소 및 네트워크 인터페이스를 사용하여 엔드포인트에 액세스하는 방식을 제어할 수 있습니다.

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

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

둘 이상의 엔드포인트가 동일한 포트를 사용하는 경우 StorageGRID는 다음 우선순위 순서를 사용하여 사용할 엔드포인트를 결정합니다. **HA** 그룹의 가상 **IP** > 노드 인터페이스 > 노드 유형 > 전역.

관리 인터페이스 엔드포인트를 생성하는 경우 관리자 노드만 허용됩니다.

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

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

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

테넌트 액세스 제어

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

단계

1. 테넌트 액세스 단계에서는 다음 중 하나를 선택하십시오.

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

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

인증서 첨부

단계

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

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

   - 인증서 업로드. 사용자 지정 인증서를 업로드하려면 이 옵션을 선택하십시오.

- 인증서 생성. 사용자 지정 인증서를 생성하는 데 필요한 값이 있는 경우 이 옵션을 선택하십시오.
- **StorageGRID S3** 인증서 사용. 이 옵션을 선택하면 스토리지 노드에 직접 연결하는 데에도 사용할 수 있는 글로벌 S3 API 인증서를 사용할 수 있습니다.

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

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

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

인증서 업로드

a. *인증서 업로드*를 선택합니다.

b. 필요한 서버 인증서 파일을 업로드합니다.

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

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

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

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

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

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

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

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

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

인증서 생성

a. *인증서 생성*을 선택합니다.

b. 인증서 정보를 지정합니다:

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

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

c. *생성*을 선택합니다.

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

   - 인증서 파일을 저장하려면 *인증서 다운로드*를 선택합니다.

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

   예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

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

e. *생성*을 선택합니다.

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

완료한 후

단계

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

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

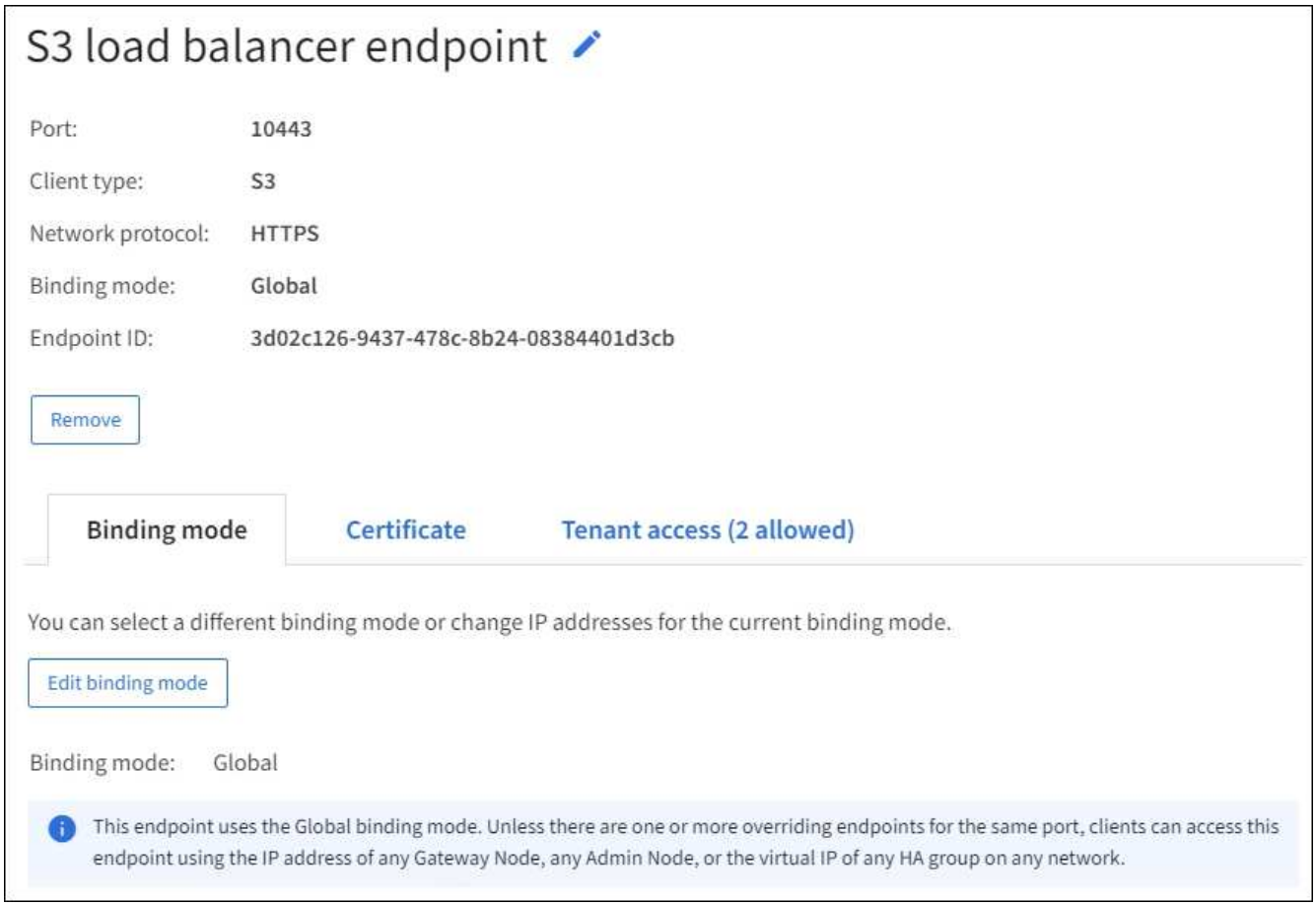
   - HA 그룹을 구성한 경우 클라이언트는 해당 HA 그룹의 가상 IP 주소로 연결됩니다.
   - HA 그룹을 사용하지 않는 경우 클라이언트는 게이트웨이 노드 또는 관리 노드의 IP 주소를 사용하여 StorageGRID 로드 밸런서 서비스에 연결합니다.

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

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

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

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



- 엔드포인트를 편집하려면 로드 밸런서 엔드포인트 페이지의 작업 메뉴를 사용하십시오.

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

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

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

로드 밸런서 엔드포인트 제거

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

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

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

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

StorageGRID에서 S3 엔드포인트 도메인 이름 구성

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

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

시작하기 전에

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

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

이 작업 정보

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

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

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

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

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

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

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

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

S3 엔드포인트 도메인 이름 추가

단계

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

결과

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

S3 엔드포인트 도메인 이름 변경

S3 애플리케이션에서 사용하는 이름을 변경하면 가상 호스팅 방식 요청이 실패합니다.

단계

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

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

S3 엔드포인트 도메인 이름 삭제

S3 애플리케이션에서 사용하는 이름을 제거하면 가상 호스팅 방식 요청이 실패합니다.

단계

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

관련 정보

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

StorageGRID 클라이언트 연결을 위한 IP 주소 및 포트

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

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

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

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

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

예시 **URL**

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

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

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

`https://192.0.2.5:10443`

IP 주소를 찾는 방법

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

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

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

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

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

b. 사용하려는 엔드포인트의 포트 번호를 기록해 두십시오.

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

c. 표에서 엔드포인트 이름을 선택합니다.

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

${post_edited_translations.segment}

StorageGRID 네트워크 설정을 구성합니다

Grid Manager에서 다양한 네트워크 설정을 구성하여 StorageGRID 시스템의 작동을 세밀하게 조정할 수 있습니다.

VLAN 인터페이스 구성

"가상 LAN(VLAN) 인터페이스 생성"를 사용하여 보안, 유연성 및 성능을 위해 트래픽을 격리하고 분할할 수 있습니다. 각 VLAN 인터페이스는 관리 노드 및 게이트웨이 노드의 하나 이상의 상위 인터페이스와 연결됩니다. HA 그룹 및 로드 밸런서 엔드포인트에서 VLAN 인터페이스를 사용하여 애플리케이션 또는 테넌트별로 클라이언트 또는 관리 트래픽을 분리할 수 있습니다.

트래픽 분류 정책

"트래픽 분류 정책"을 사용하여 특정 버킷, 테넌트, 클라이언트 서브넷 또는 로드 밸런서 엔드포인트와 관련된 트래픽을 포함하여 다양한 유형의 네트워크 트래픽을 식별하고 처리할 수 있습니다. 이러한 정책은 트래픽 제한 및 모니터링에 도움이 됩니다.

StorageGRID 네트워크 가이드라인

Grid Manager를 사용하여 StorageGRID 네트워크 및 연결을 구성하고 관리할 수 있습니다.

"S3 클라이언트 연결 구성"을 참조하여 S3 클라이언트를 연결하는 방법을 알아보세요.

기본 StorageGRID 네트워크

기본적으로 StorageGRID는 그리드 노드당 3개의 네트워크 인터페이스를 지원하므로 보안 및 액세스 요구 사항에 맞게 각 그리드 노드의 네트워킹을 개별적으로 구성할 수 있습니다.

네트워크 토폴로지에 대한 자세한 내용은 "네트워킹 가이드라인"을 참조하십시오.

그리드 네트워크

필수 항목입니다. 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용됩니다. 모든 사이트 및 서브넷에 걸쳐 그리드의 모든 노드 간 연결을 제공합니다.

관리자 네트워크

선택 사항입니다. 관리자 네트워크는 일반적으로 시스템 관리 및 유지 보수에 사용됩니다. 클라이언트 프로토콜 액세스에도 사용할 수 있습니다. 관리자 네트워크는 일반적으로 사설 네트워크이며 사이트 간 라우팅이 필요하지 않습니다.

클라이언트 네트워크

선택 사항입니다. 클라이언트 네트워크는 일반적으로 S3 클라이언트 애플리케이션에 대한 액세스를 제공하는 데 사용되는 개방형 네트워크이므로 그리드 네트워크를 격리하고 보안을 강화할 수 있습니다. 클라이언트 네트워크는 로컬 게이트웨이를 통해 연결할 수 있는 모든 서브넷과 통신할 수 있습니다.

지침

- 각 StorageGRID 노드는 할당된 각 네트워크에 대해 전용 네트워크 인터페이스, IP 주소, 서브넷 마스크 및 게이트웨이가 필요합니다.
- 그리드 노드는 네트워크에서 두 개 이상의 인터페이스를 가질 수 없습니다.
- 네트워크 및 그리드 노드당 하나의 게이트웨이만 지원되며, 해당 게이트웨이는 노드와 동일한 서브넷에 있어야 합니다. 필요한 경우 게이트웨이에서 더 복잡한 라우팅을 구현할 수 있습니다.
- 각 노드에서 각 네트워크는 특정 네트워크 인터페이스에 매핑됩니다.

네트워크	인터페이스 이름
그리드	eth0
관리자 (선택 사항)	eth1
클라이언트 (선택 사항)	eth2

- 노드가 StorageGRID 어플라이언스에 연결된 경우 각 네트워크에 특정 포트가 사용됩니다. 자세한 내용은 해당 어플라이언스의 설치 지침을 참조하십시오.
- 기본 경로는 노드별로 자동으로 생성됩니다. eth2가 활성화된 경우 0.0.0.0/0은 eth2의 클라이언트 네트워크를 사용합니다. eth2가 활성화되지 않은 경우 0.0.0.0/0은 eth0의 그리드 네트워크를 사용합니다.
- 클라이언트 네트워크는 그리드 노드가 그리드에 연결될 때까지 작동되지 않습니다.
- 관리자 네트워크는 그리드 노드 배포 중에 구성하여 그리드가 완전히 설치되기 전에 설치 사용자 인터페이스에 액세스할 수 있도록 할 수 있습니다.

선택적 인터페이스

선택적으로 노드에 추가 인터페이스를 추가할 수 있습니다. 예를 들어, 관리 노드나 게이트웨이 노드에 트렁크 인터페이스를 추가하여 "VLAN 인터페이스"을 사용해 서로 다른 애플리케이션이나 테넌트에 속하는 트래픽을 분리할 수 있습니다. 또는 "고가용성(HA) 그룹"에서 사용할 액세스 인터페이스를 추가할 수도 있습니다.

트렁크 또는 액세스 인터페이스를 추가하려면 다음을 참조하십시오.

- **VMware (**노드 설치 후**)**: "VMware: 노드에 트렁크 또는 액세스 인터페이스 추가"
  - **Linux (**노드 설치 전**)**: "노드 구성 파일 생성"

◦ **Linux** (노드 설치 후): "노드에 트렁크 또는 액세스 인터페이스 추가"

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

StorageGRID에서 IP 주소 보기

StorageGRID 시스템에서 각 그리드 노드의 IP 주소를 확인할 수 있습니다. 이 IP 주소를 사용하여 명령줄에서 그리드 노드에 로그인하고 다양한 유지 관리 절차를 수행할 수 있습니다.

시작하기 전에

현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.

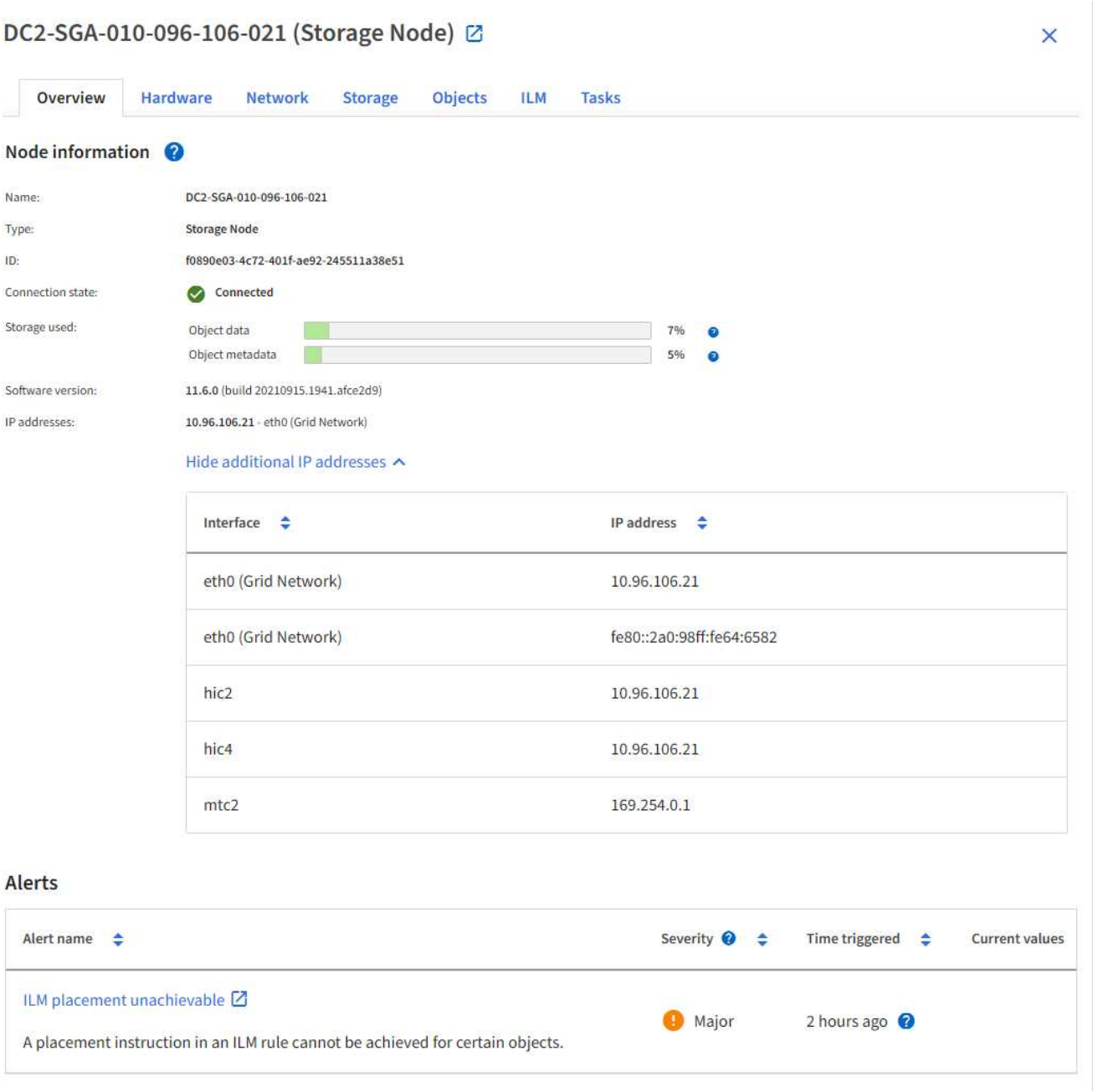
이 작업 정보

IP 주소 변경에 대한 자세한 내용은 "IP 주소 구성"을 참조하십시오.

단계

1. 노드 > ***grid node*** > *개요*를 선택합니다.
2. IP 주소 제목 오른쪽에 있는 *더 보기*를 선택합니다.

   해당 그리드 노드의 IP 주소는 표에 나와 있습니다.



StorageGRID에서 VLAN 인터페이스 구성

관리 노드와 게이트웨이 노드에 가상 LAN(VLAN) 인터페이스를 생성하고, 이를 HA 그룹 및 로드 밸런서 엔드포인트에 사용하여 보안, 유연성 및 성능 향상을 위해 트래픽을 격리하고 분할할 수 있습니다. HA 그룹에서 선택된 노드들은 VLAN 인터페이스를 통해 최대 10개의 가상 IP 주소를 공유할 수 있으므로, 한 노드에 장애가 발생하더라도 다른 노드가 해당 가상 IP 주소로 들어오고 나가는 트래픽을 인계받을 수 있습니다.

VLAN 인터페이스 고려 사항

- VLAN 인터페이스를 생성하려면 VLAN ID를 입력하고 하나 이상의 노드에서 상위 인터페이스를 선택해야 합니다.
- 상위 인터페이스는 스위치에서 트렁크 인터페이스로 구성되어야 합니다.

- 상위 인터페이스는 그리드 네트워크(eth0), 클라이언트 네트워크(eth2) 또는 VM이나 베어메탈 호스트용 추가 트렁크 인터페이스(예: ens256)일 수 있습니다.
- 각 VLAN 인터페이스에 대해 특정 노드에는 하나의 상위 인터페이스만 선택할 수 있습니다. 예를 들어, 동일한 게이트웨이 노드에서 동일한 VLAN의 상위 인터페이스로 그리드 네트워크 인터페이스와 클라이언트 네트워크 인터페이스를 모두 사용할 수 없습니다.
- VLAN 인터페이스가 Grid Manager 및 Tenant Manager와 관련된 트래픽을 포함하는 관리 노드 트래픽용인 경우 관리 노드에서만 인터페이스를 선택하십시오.
- VLAN 인터페이스가 S3 클라이언트 트래픽용인 경우 관리 노드 또는 게이트웨이 노드에서 인터페이스를 선택하십시오.
- 트렁크 인터페이스를 추가해야 하는 경우 자세한 내용은 다음을 참조하십시오.
  - **VMware (**노드 설치 후**)**: "VMware: 노드에 트렁크 또는 액세스 인터페이스 추가"
  - **Linux (**노드 설치 전**)**: "노드 구성 파일 생성"
  - **Linux (**노드 설치 후**)**: "노드에 트렁크 또는 액세스 인터페이스 추가"

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

VLAN 인터페이스 생성

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"
- 네트워크에 트렁크 인터페이스가 구성되어 VM 또는 Linux 노드에 연결되었습니다. 트렁크 인터페이스의 이름을 알고 있습니다.
- 구성하려는 VLAN의 ID를 알고 있습니다.

이 작업 정보

네트워크 관리자는 서로 다른 애플리케이션이나 테넌트에 속하는 클라이언트 또는 관리 트래픽을 분리하기 위해 하나 이상의 트렁크 인터페이스와 하나 이상의 VLAN을 구성했을 수 있습니다. 각 VLAN은 숫자 ID 또는 태그로 식별됩니다. 예를 들어, 네트워크에서 FabricPool 트래픽에는 VLAN 100을, 아카이브 애플리케이션에는 VLAN 200을 사용할 수 있습니다.

Grid Manager를 사용하여 클라이언트가 특정 VLAN에서 StorageGRID에 액세스할 수 있도록 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. *생성*을 선택합니다.

VLAN 인터페이스에 대한 세부 정보를 입력하십시오.

단계

1. 네트워크에서 사용할 VLAN의 ID를 지정하십시오. 1에서 4094 사이의 값을 입력할 수 있습니다.

   VLAN ID는 고유할 필요가 없습니다. 예를 들어, 한 사이트의 관리 트래픽에 VLAN ID 200을 사용하고 다른 사이트의 클라이언트 트래픽에 동일한 VLAN ID를 사용할 수 있습니다. 각 사이트에서 서로 다른 상위 인터페이스 세트를 사용하여 별도의 VLAN 인터페이스를 생성할 수 있습니다. 그러나 동일한 ID를 가진 두 개의 VLAN 인터페이스는 노드에서 동일한 인터페이스를 공유할 수 없습니다. 이미 사용 중인 ID를 지정하면 메시지가 나타납니다.

2. 선택적으로 VLAN 인터페이스에 대한 간단한 설명을 입력합니다.
3. *Continue*를 선택합니다.

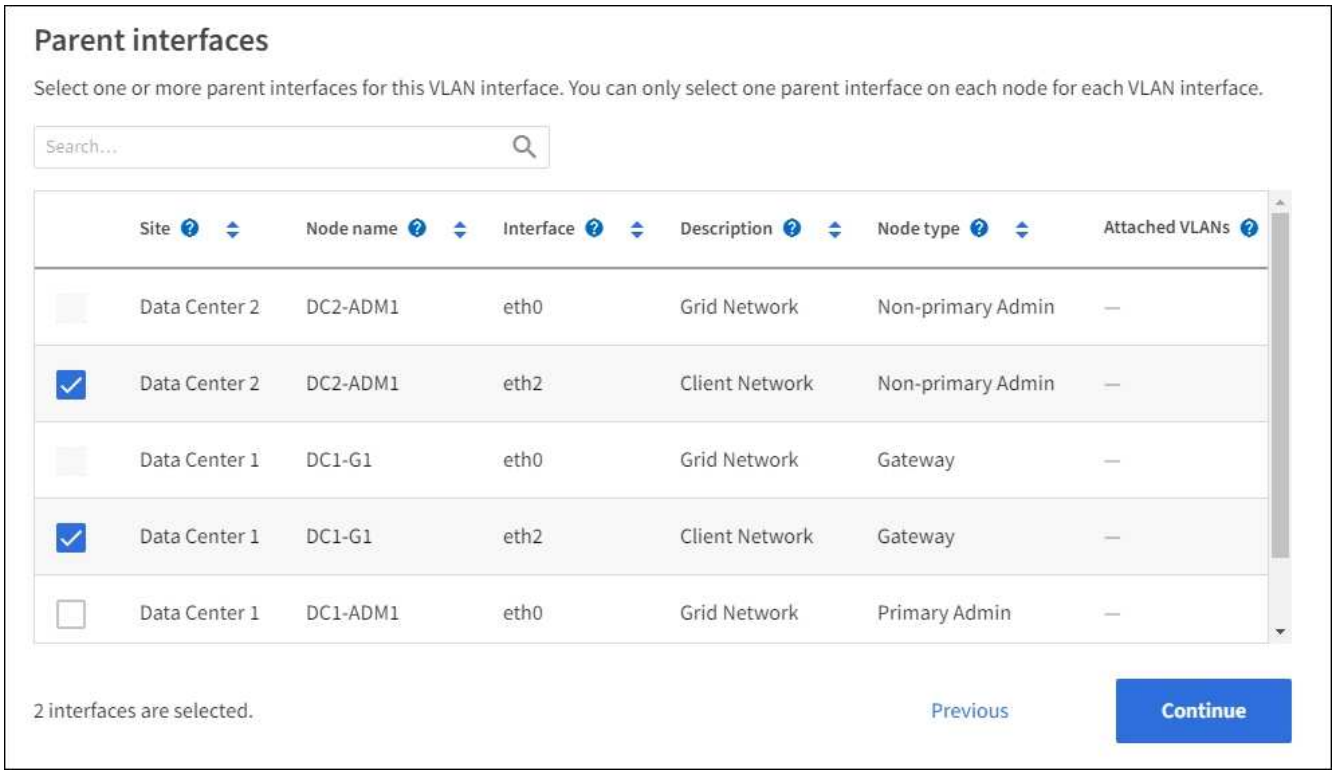
상위 인터페이스 선택

이 표는 그리드의 각 사이트에 있는 모든 관리 노드와 게이트웨이 노드에서 사용 가능한 인터페이스를 나열합니다. 관리 네트워크(eth1) 인터페이스는 상위 인터페이스로 사용할 수 없으므로 표시되지 않습니다.

단계

1. 이 VLAN을 연결할 상위 인터페이스를 하나 이상 선택하십시오.

   예를 들어 게이트웨이 노드와 관리 노드에 대해 클라이언트 네트워크(eth2) 인터페이스에 VLAN을 연결할 수 있습니다.



2. *Continue*를 선택합니다.

설정을 확인합니다

단계

1. 구성을 검토하고 필요한 변경 사항을 적용하십시오.

◦ VLAN ID 또는 설명을 변경해야 하는 경우 페이지 상단에서 *VLAN 세부 정보 입력*을 선택하십시오.

◦ 상위 인터페이스를 변경해야 하는 경우 페이지 상단의 *상위 인터페이스 선택*을 선택하거나 *이전*을 선택하십시오.

◦ 상위 인터페이스를 제거해야 하는 경우 휴지통 을 선택하세요.

2. *저장*을 선택하세요.
3. 새 인터페이스가 고가용성 그룹 페이지에서 선택 항목으로 나타나고 노드의 네트워크 인터페이스 테이블(노드 > 상위 인터페이스 노드 > 네트워크)에 표시될 때까지 최대 5분 정도 기다려 주십시오.

VLAN 인터페이스 편집

VLAN 인터페이스를 편집할 때 다음과 같은 유형의 변경을 수행할 수 있습니다.

- VLAN ID 또는 설명을 변경합니다.
- 상위 인터페이스를 추가하거나 제거합니다.

예를 들어, 연결된 노드를 더 이상 사용하지 않으려면 VLAN 인터페이스에서 상위 인터페이스를 제거해야 할 수 있습니다.

다음 사항에 유의하십시오.

- VLAN 인터페이스가 HA 그룹에서 사용되는 경우 VLAN ID를 변경할 수 없습니다.
- HA 그룹에서 사용되는 상위 인터페이스는 제거할 수 없습니다.

  예를 들어, VLAN 200이 노드 A와 B의 상위 인터페이스에 연결되어 있다고 가정해 보겠습니다. HA 그룹이 노드 A에는 VLAN 200 인터페이스를, 노드 B에는 eth2 인터페이스를 사용하는 경우, 노드 B에서 사용하지 않는 상위 인터페이스는 제거할 수 있지만, 노드 A에서 사용 중인 상위 인터페이스는 제거할 수 없습니다.

단계

1. 구성 > 네트워크 > **VLAN** 인터페이스 를 선택합니다.
2. 편집하려는 VLAN 인터페이스의 확인란을 선택합니다. 그런 다음 작업 > *편집*을 선택합니다.
3. 선택적으로 VLAN ID 또는 설명을 업데이트합니다. 그런 다음 *계속*을 선택하십시오.

   HA 그룹에서 사용되는 VLAN의 경우 VLAN ID를 업데이트할 수 없습니다.

4. 선택적으로 체크박스를 선택하거나 선택 취소하여 상위 인터페이스를 추가하거나 사용하지 않는 인터페이스를 제거할 수 있습니다. 그런 다음 *계속*을 선택하십시오.
5. 구성을 검토하고 필요한 변경 사항을 적용하십시오.
6. *저장*을 선택하세요.

VLAN 인터페이스 제거

VLAN 인터페이스를 하나 이상 제거할 수 있습니다.

HA 그룹에 포함된 VLAN 인터페이스는 제거할 수 없습니다. VLAN 인터페이스를 제거하려면 먼저 HA 그룹에서 해당 인터페이스를 제거해야 합니다.

고객 트래픽에 지장을 주지 않으려면 다음 중 하나를 고려하십시오.

- 이 VLAN 인터페이스를 제거하기 전에 HA 그룹에 새 VLAN 인터페이스를 추가하십시오.
- 이 VLAN 인터페이스를 사용하지 않는 새로운 HA 그룹을 생성하십시오.
- 제거하려는 VLAN 인터페이스가 현재 활성 인터페이스인 경우 HA 그룹을 편집합니다. 제거하려는 VLAN 인터페이스를 우선순위 목록의 맨 아래로 이동합니다. 새 기본 인터페이스에서 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. 제거하려는 각 VLAN 인터페이스의 확인란을 선택합니다. 그런 다음 작업 > *삭제*를 선택합니다.
3. 선택을 확정하려면 *예*를 선택하세요.

   선택한 모든 VLAN 인터페이스가 제거되었습니다. VLAN 인터페이스 페이지에 녹색 성공 배너가 나타납니다.

관리 인터페이스에 대해 **StorageGRID CORS** 활성화

그리드 관리자는 다른 도메인의 관리 API를 사용하여 StorageGRID의 데이터에 액세스할 수 있도록 하려는 경우 StorageGRID에 대한 관리 API 요청에 대해 CORS(Cross-Origin Resource Sharing)를 활성화할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "루트 액세스 권한"은(는) 모든 CORS 구성 요청에 대한 액세스를 제공합니다.

이 작업 정보

CORS는 한 도메인의 클라이언트 웹 애플리케이션이 다른 도메인의 리소스에 액세스할 수 있도록 하는 보안 메커니즘입니다. 예를 들어, 도메인 `http://www.example.com`에서 `StorageGRID`에 대한 모니터링 대시보드를 구축한다고 가정해 보겠습니다. `StorageGRID`에서 `\http://www.example.com` 및 "Grid Manager"에 대해 CORS를 활성화하면 StorageGRID 도메인은 `\http://www.example.com`에서 오는 Grid Management API 요청에 응답합니다.

`application/json`을 사용하는 Management API(mgmt-api) 요청 또는 `Content-Type`에 대한 `multipart/formdata` 요청은 CORS에 대해 지원됩니다.

단계

1. Grid Manager에서 구성 > 네트워크 > *관리 인터페이스 CORS 설정*으로 이동합니다.
2. **Grid Manager**, **Tenant Manager** 또는 두 옵션 모두를 선택하십시오.
   - **Grid Manager**: 도메인 간 그리드 관리 API 요청에 대한 CORS를 활성화합니다.
   - **Tenant Manager**: 도메인 간 테넌트 관리 API 요청에 대한 CORS를 활성화합니다.
3. 도메인 필드에 다른 도메인의 URL을 입력합니다.

   둘 이상의 도메인에 대해 StorageGRID에서 CORS를 활성화하려면 *다른 도메인 추가*를 선택하십시오.

4. *저장*을 선택하세요.

관련 정보

"버킷 및 객체에 대한 StorageGRID CORS 구성"

트래픽 분류 정책 관리

StorageGRID의 트래픽 분류 정책

트래픽 분류 정책을 사용하면 다양한 유형의 네트워크 트래픽을 식별하고 모니터링할 수 있습니다. 이러한 정책은 트래픽 제한 및 모니터링에 도움이 되어 서비스 품질(QoS)을 향상시킬 수 있습니다.

트래픽 분류 정책은 게이트웨이 노드 및 관리 노드용 StorageGRID 로드 밸런서 서비스의 엔드포인트에 적용됩니다. 트래픽 분류 정책을 생성하려면 로드 밸런서 엔드포인트가 이미 생성되어 있어야 합니다.

일치 규칙

각 트래픽 분류 정책에는 다음 항목 중 하나 이상과 관련된 네트워크 트래픽을 식별하기 위한 하나 이상의 일치 규칙이 포함되어 있습니다.

- 버킷
- 서브넷
- 테넌트
- 로드 밸런서 엔드포인트

StorageGRID는 정책의 목적에 따라 정책 내의 규칙과 일치하는 트래픽을 모니터링합니다. 정책의 규칙과 일치하는 모든 트래픽은 해당 정책에 따라 처리됩니다. 반대로, 특정 엔티티를 제외한 모든 트래픽과 일치하도록 규칙을 설정할 수도 있습니다.

트래픽 제한

선택적으로 정책에 다음과 같은 제한 유형을 추가할 수 있습니다.

- 애그리게이트 대역폭
- 요청당 대역폭
- 동시 요청
- 요청 속도

제한 값은 로드 밸런서별로 적용됩니다. 트래픽이 여러 로드 밸런서에 동시에 분산되는 경우, 총 최대 전송률은 지정한 전송률 제한 값의 배수가 됩니다.

> 애그리게이트 대역폭을 제한하거나 요청별 대역폭을 제한하는 정책을 생성할 수 있습니다. 하지만 StorageGRID는 두 가지 유형의 대역폭을 동시에 제한할 수 없습니다. 애그리게이트 대역폭 제한은 제한되지 않은 트래픽에 약간의 추가적인 성능 영향을 미칠 수 있습니다.

애그리게이트 또는 요청별 대역폭 제한의 경우, 요청은 설정한 속도로 들어오거나 나갑니다. StorageGRID는 하나의 속도만 적용할 수 있으므로, 매처 유형별로 가장 구체적인 정책 일치 항목이 적용됩니다. 요청에서 소비되는 대역폭은

애그리게이트 대역폭 제한 정책을 포함하는 다른 덜 구체적인 일치 정책에 포함되지 않습니다. 다른 모든 제한 유형의 경우, 클라이언트 요청은 250밀리초 지연되며, 일치하는 정책 제한을 초과하는 요청에 대해서는 503 Slow Down 응답이 수신됩니다.

Grid Manager에서 트래픽 차트를 보고 정책이 예상한 트래픽 제한을 적용하고 있는지 확인할 수 있습니다.

SLA와 함께 트래픽 분류 정책 사용

트래픽 분류 정책을 용량 제한 및 데이터 보호와 함께 사용하여 용량, 데이터 보호 및 성능에 대한 구체적인 내용을 명시하는 서비스 수준 계약(SLA)을 시행할 수 있습니다.

다음 예시는 SLA의 세 가지 계층을 보여줍니다. 각 SLA 계층의 성능 목표를 달성하기 위해 트래픽 분류 정책을 생성할 수 있습니다.

서비스 수준 등급	용량	데이터 보호	최대 허용 성능	비용
골드	1PB 스토리지 허용	3개 복사본 ILM 규칙	초당 25K 요청 5 GB/sec(40 Gbps) 대역폭	월 $$$
실버	250TB 스토리지 허용	2개 복사본 ILM 규칙	초당 1만 건의 요청 1.25 GB/초(10Gbps) 대역폭	월 $$
브론즈	100TB 스토리지 허용	2개 복사본 ILM 규칙	초당 5천 건의 요청 1 GB/sec (8 Gbps) 대역폭	월 $

StorageGRID 트래픽 분류 정책 생성

버킷, 버킷 정규식, CIDR, 로드 밸런서 엔드포인트 또는 테넌트별로 네트워크 트래픽을 모니터링하고 선택적으로 제한하려는 경우 트래픽 분류 정책을 생성할 수 있습니다. 선택적으로 대역폭, 동시 요청 수 또는 요청 속도를 기준으로 정책에 대한 제한을 설정할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"
- 원하는 로드 밸런서 엔드포인트를 모두 생성했습니다.
- 원하는 테넌트를 모두 생성했습니다.

단계

1. 구성 > 네트워크 > *트래픽 분류*를 선택하십시오.
2. *생성*을 선택합니다.
3. 정책의 이름과 설명(선택 사항)을 입력하고 *계속*을 선택합니다.

예를 들어, 이 트래픽 분류 정책이 적용되는 대상과 제한 사항을 설명하십시오.

4. *규칙 추가*를 선택하고 다음 세부 정보를 지정하여 정책에 대한 하나 이상의 일치 규칙을 만드십시오. 생성하는 모든 정책에는 최소 하나 이상의 일치 규칙이 있어야 합니다. *계속*을 선택하십시오.

필드	설명
유형	일치 규칙을 적용할 트래픽 유형을 선택하십시오. 트래픽 유형에는 버킷, 버킷 정규식, CIDR, 로드 밸런서 엔드포인트 및 테넌트가 있습니다.
일치 값	선택한 유형에 맞는 값을 입력하십시오. • 버킷: 하나 이상의 버킷 이름을 입력하세요. • 버킷 정규 표현식: 버킷 이름 집합과 일치하는 하나 이상의 정규 표현식을 입력하십시오. 정규 표현식은 고정되지 않습니다. 버킷 이름의 시작 부분을 일치시키려면 ^ 앵커를 사용하고, 이름의 끝 부분을 일치시키려면 $ 앵커를 사용하십시오. 정규 표현식 일치는 PCRE(Perl 호환 정규 표현식) 구문의 일부를 지원합니다. • CIDR: 원하는 서브넷과 일치하는 하나 이상의 IPv4 서브넷을 CIDR 표기법으로 입력하십시오. • 로드 밸런서 엔드포인트: 엔드포인트 이름을 선택하세요. 이는 "로드 밸런서 엔드포인트 구성"에 정의한 로드 밸런서 엔드포인트입니다. • 테넌트: 테넌트 일치는 액세스 키 ID를 사용합니다. 요청에 액세스 키 ID가 포함되어 있지 않은 경우(예: 익명 액세스) 액세스한 버킷의 소유권을 사용하여 테넌트를 결정합니다.
역방향 일치	방금 정의한 유형 및 일치 값과 일치하는 트래픽을 제외한 모든 네트워크 트래픽을 일치시키려면 역일치 확인란을 선택하십시오. 그렇지 않으면 확인란을 선택 해제된 상태로 두십시오. 예를 들어, 이 정책을 로드 밸런서 엔드포인트 중 하나를 제외한 모든 엔드포인트에 적용하려면 제외할 로드 밸런서 엔드포인트를 지정하고 *역일치*를 선택하십시오. 여러 개의 매처가 포함된 정책에서 적어도 하나가 역매처인 경우, 모든 요청과 일치하는 정책을 만들지 않도록 주의해야 합니다.

5. 선택적으로 *제한 추가*를 선택하고 다음 세부 정보를 선택하여 규칙에 따라 일치하는 네트워크 트래픽을 제어하기 위한 하나 이상의 제한을 추가할 수 있습니다.

> StorageGRID 제한을 추가하지 않아도 메트릭을 수집하므로 트래픽 추세를 파악할 수 있습니다.

필드	설명
유형	규칙에 의해 일치된 네트워크 트래픽에 적용할 제한 유형입니다. 예를 들어 대역폭 또는 요청 속도를 제한할 수 있습니다. 참고: 애그리게이트 대역폭을 제한하거나 요청별 대역폭을 제한하는 정책을 생성할 수 있습니다. 그러나 StorageGRID는 두 가지 유형의 대역폭을 동시에 제한할 수 없습니다. 애그리게이트 대역폭이 사용 중일 때는 요청별 대역폭을 사용할 수 없습니다. 반대로 요청별 대역폭이 사용 중일 때는 애그리게이트 대역폭을 사용할 수 없습니다. 애그리게이트 대역폭 제한은 제한되지 않은 트래픽에 약간의 추가적인 성능 영향을 미칠 수 있습니다. 대역폭 제한의 경우, StorageGRID는 설정된 제한 유형과 가장 잘 일치하는 정책을 적용합니다. 예를 들어, 한 방향으로만 트래픽을 제한하는 정책이 있는 경우, 반대 방향의 트래픽은 대역폭 제한이 있는 다른 정책과 일치하는 트래픽이 있더라도 무제한으로 허용됩니다. StorageGRID는 대역폭 제한에 대한 "최적의" 일치 항목을 다음 순서로 구현합니다. • 정확한 IP 주소(/32 마스크) • 버킷의 정확한 이름 • 버킷 정규식 • 테넌트 • 엔드포인트 • CIDR이 정확히 일치하지 않음(/32 제외) • 역일치
적용 대상	이 제한이 클라이언트의 읽기 요청(GET 또는 HEAD)에 적용되는지, 아니면 쓰기 요청(PUT, POST 또는 DELETE)에 적용되는지 여부.
가치	선택한 단위에 따라 네트워크 트래픽이 제한될 값입니다. 예를 들어, 10을 입력하고 MiB/s를 선택하면 이 규칙에 해당하는 네트워크 트래픽이 10 MiB/s를 초과하지 않도록 제한할 수 있습니다. 참고: 단위 설정에 따라 사용 가능한 단위는 이진수(예: GiB) 또는 십진수(예: GB)가 될 수 있습니다. 단위 설정을 변경하려면 그리드 관리자 오른쪽 상단의 사용자 드롭다운 메뉴를 선택한 다음 *사용자 기본 설정*을 선택하십시오.
단위	입력한 값을 나타내는 단위입니다.

예를 들어, SLA 계층에 대해 4GB/s의 대역폭 제한을 설정하려면 두 가지 애그리게이트 대역폭 제한을 생성합니다. GET/HEAD에 대해 4GB/s, PUT/POST/DELETE에 대해 4GB/s입니다.

6. *Continue*를 선택합니다.
7. 트래픽 분류 정책을 읽고 검토하십시오. 이전 버튼을 사용하여 이전 페이지로 돌아가 필요한 변경 사항을 적용하십시오. 정책이 만족스러우면 *저장 후 계속*을 선택하십시오.

   이제 S3 클라이언트 트래픽은 트래픽 분류 정책에 따라 처리됩니다.

완료한 후

"네트워크 트래픽 메트릭 보기" 정책이 예상하는 트래픽 제한을 올바르게 적용하고 있는지 확인합니다.

StorageGRID 트래픽 분류 정책을 편집합니다

트래픽 분류 정책을 편집하여 이름이나 설명을 변경하거나, 정책에 대한 규칙이나 제한 사항을 생성, 편집 또는 삭제할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"

단계

1. 구성 > 네트워크 > *트래픽 분류*를 선택하십시오.

   트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

2. 작업 메뉴 또는 세부 정보 페이지를 사용하여 정책을 편집합니다. 입력할 내용은 "트래픽 분류 정책 생성"을 참조하십시오.

   작업 메뉴

   a. 해당 정책의 확인란을 선택합니다.

   b. 작업 * > * 편집 *을 선택합니다.

   상세 정보 페이지

   a. 정책 이름을 선택합니다.

   b. 정책 이름 옆에 있는 편집 버튼을 선택합니다.

3. 정책 이름 입력 단계에서는 선택적으로 정책 이름 또는 설명을 편집하고 *계속*을 선택합니다.
4. 일치하는 규칙 추가 단계에서는 선택적으로 규칙을 추가하거나 기존 규칙의 유형 및 *일치 값*을 편집한 후 *계속*을 선택합니다.
5. 제한 설정 단계에서는 필요에 따라 제한을 추가, 편집 또는 삭제하고 *계속*을 선택합니다.
6. 업데이트된 정책을 검토하고 *저장 후 계속*을 선택합니다.

   정책 변경 사항이 저장되었으며, 이제 네트워크 트래픽은 트래픽 분류 정책에 따라 처리됩니다. 트래픽 차트를 확인하여 정책이 예상대로 트래픽 제한을 적용하고 있는지 확인할 수 있습니다.

StorageGRID 트래픽 분류 정책을 삭제합니다

더 이상 필요하지 않은 트래픽 분류 정책은 삭제할 수 있습니다. 삭제된 정책은 복구할 수 없으므로 올바른 정책을 삭제했는지 확인하십시오.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.

- 다음이 있습니다. "루트 액세스 권한"

단계

1. 구성 > 네트워크 > *트래픽 분류*를 선택하십시오.

   트래픽 분류 정책 페이지가 표시되며 기존 정책들이 표 형식으로 나열됩니다.

2. 작업 메뉴 또는 세부 정보 페이지를 사용하여 정책을 삭제합니다.

   작업 메뉴

   a. 해당 정책의 확인란을 선택합니다.

   b. * 작업 * > * 제거 * 를 선택합니다.

   정책 세부 정보 페이지

   a. 정책 이름을 선택합니다.

   b. 정책 이름 옆에 있는 제거 버튼을 선택합니다.

3. 정책을 삭제하려면 *예*를 선택하여 확인하십시오.

   해당 정책이 삭제되었습니다.

StorageGRID에서 네트워크 트래픽 메트릭 보기

트래픽 분류 정책 페이지에서 제공되는 그래프를 통해 네트워크 트래픽을 모니터링할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 당신은 "루트 액세스 또는 테넌트 계정 권한"을(를) 가지고 있습니다.

이 작업 정보

기존 트래픽 분류 정책의 경우, 로드 밸런서 서비스에 대한 지표를 확인하여 해당 정책이 네트워크 전체의 트래픽을 성공적으로 제한하는지 여부를 판단할 수 있습니다. 그래프의 데이터를 통해 정책 조정이 필요한지 여부를 결정할 수 있습니다.

트래픽 분류 정책에 제한이 설정되어 있지 않더라도 메트릭이 수집되고 그래프는 트래픽 추세를 파악하는 데 유용한 정보를 제공합니다.

단계

1. 구성 > 네트워크 > *트래픽 분류*를 선택하십시오.

   트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

2. 측정항목을 보려는 트래픽 분류 정책 이름을 선택합니다.
3. 측정항목 탭을 선택합니다.

트래픽 분류 정책 그래프가 나타납니다. 이 그래프는 선택된 정책과 일치하는 트래픽에 대한 지표만 표시합니다.

다음 그래프들이 페이지에 포함되어 있습니다.

- 요청량: 이 그래프는 모든 로드 밸런서에서 이 정책에 맞춰 처리된 대역폭 양을 보여줍니다. 수신 데이터에는 모든 요청의 요청 헤더와 본문 데이터가 있는 응답의 본문 데이터 크기가 포함됩니다. 전송 데이터에는 모든 요청의 응답 헤더와 응답에 본문 데이터가 포함된 요청의 응답 본문 데이터 크기가 포함됩니다.

  > ⓘ 요청이 완료되면 이 차트는 대역폭 사용량만 표시합니다. 느리거나 대용량 객체 요청의 경우 실제 순간 대역폭이 이 그래프에 표시된 값과 다를 수 있습니다.

- 오류 응답률: 이 그래프는 이 정책과 일치하는 요청이 클라이언트에게 오류(HTTP 상태 코드 >= 400)를 반환하는 대략적인 비율을 보여줍니다.
- 평균 요청 소요 시간(오류 제외): 이 그래프는 해당 정책에 부합하는 성공적인 요청의 평균 소요 시간을 보여줍니다.
- 정책 대역폭 사용량: 이 그래프는 모든 로드 밸런서에서 이 정책과 일치하는 대역폭 사용량을 보여줍니다. 수신 데이터에는 모든 요청의 요청 헤더와 본문 데이터가 있는 응답의 본문 데이터 크기가 포함됩니다. 전송 데이터에는 모든 요청의 응답 헤더와 응답에 본문 데이터가 포함된 요청의 응답 본문 데이터 크기가 포함됩니다.

4. 선 그래프 위에 마우스 커서를 올려놓으면 그래프의 특정 부분에 대한 값이 팝업으로 표시됩니다.
5. 정책에 대한 모든 그래프를 보려면 메트릭 제목 바로 아래에 있는 **Grafana** 대시보드*를 선택하세요**.** *메트릭 탭의 네 가지 그래프 외에도 두 가지 그래프를 더 볼 수 있습니다.
   - 객체 크기별 쓰기 요청 속도: 이 정책과 일치하는 PUT/POST/DELETE 요청 속도입니다. 개별 셀에 위치하면 초당 속도를 확인할 수 있습니다. 마우스 오버 시 표시되는 속도는 정수로 잘려서 표시되며, 버킷에 0이 아닌 요청이 있는 경우에도 0으로 표시될 수 있습니다.
   - 객체 크기별 읽기 요청률: 이 정책과 일치하는 GET/HEAD 요청의 비율입니다. 각 셀에 마우스를 올리면 초당 요청률을 확인할 수 있습니다. 마우스 오버 시 표시되는 비율은 정수로 잘려서 표시되며, 버킷에 0이 아닌 요청이 있는 경우에도 0으로 표시될 수 있습니다.
6. 또는 지원 메뉴에서 그래프에 액세스할 수도 있습니다.
   a. 지원 > 도구 > *측정항목*을 선택합니다.
   b. **Grafana** 섹션에서 **Traffic Classification Policy** 를 선택합니다.
   c. 페이지 왼쪽 상단의 메뉴에서 정책을 선택합니다.
   d. 그래프 위에 커서를 올리면 샘플링 날짜 및 시간, 집계에 포함된 객체 크기, 해당 기간 동안의 초당 요청 수를 보여주는 팝업 창이 나타납니다.

      트래픽 분류 정책은 ID로 식별됩니다. 정책 ID는 트래픽 분류 정책 페이지에 나열되어 있습니다.

7. 그래프를 분석하여 정책이 트래픽을 제한하는 빈도와 정책 조정이 필요한지 여부를 판단하십시오.

StorageGRID의 발신 TLS 연결에 지원되는 암호

StorageGRID 시스템은 ID 연동 및 클라우드 스토리지 풀에 사용되는 외부 시스템과의 전송 계층 보안(TLS) 연결을 위해 제한된 수의 암호화 제품군을 지원합니다.

지원되는 **TLS** 버전

StorageGRID는 ID 연동 및 클라우드 스토리지 풀에 사용되는 외부 시스템과의 연결을 위해 TLS 1.2 및 TLS 1.3을 지원합니다.

외부 시스템과의 호환성을 보장하기 위해 외부 시스템에서 사용 가능한 TLS 암호화 방식이 선정되었습니다. 이 목록은 S3 클라이언트 애플리케이션에서 지원하는 암호화 방식 목록보다 더 큽니다. 암호화 방식을 구성하려면 구성 > 보안 > *보안 설정*으로 이동하여 *TLS 및 SSH 정책*을 선택하십시오.

> 프로토콜 버전, 암호, 키 교환 알고리즘, MAC 알고리즘 등의 TLS 구성 옵션은 StorageGRID에서 구성할 수 없습니다. 이러한 설정에 대한 구체적인 요청 사항이 있는 경우 NetApp 담당자에게 문의하십시오.

StorageGRID의 활성, 유휴 및 동시 HTTP 연결의 이점

HTTP 연결 구성 방식은 StorageGRID 시스템의 성능에 영향을 미칠 수 있습니다. HTTP 연결이 활성 상태인지, 유휴 상태인지, 또는 여러 연결이 동시에 실행되는지에 따라 구성 방식이 달라집니다.

다음과 같은 유형의 HTTP 연결에서 성능 향상 효과를 확인할 수 있습니다.

- 유휴 HTTP 연결
- 활성 HTTP 연결
- 동시 HTTP 연결

유휴 **HTTP** 연결을 열어두는 것의 이점

클라이언트 애플리케이션이 유휴 상태일 때는 추후 트랜잭션을 위해 HTTP 연결을 열어 두십시오. 유휴 HTTP 연결은 최대 10분 동안 열어 둘 수 있습니다. StorageGRID는 10분 이상 열려 있고 유휴 상태인 HTTP 연결을 자동으로 닫을 수 있습니다.

열려 있고 유휴 상태인 HTTP 연결은 다음과 같은 이점을 제공합니다.

- StorageGRID 시스템이 HTTP 트랜잭션을 수행해야 한다고 판단한 시점부터 실제로 트랜잭션을 수행할 수 있는 시점까지의 지연 시간이 단축되었습니다.

  지연 시간 감소가 가장 큰 장점이며, 특히 TCP/IP 및 TLS 연결을 설정하는 데 필요한 시간을 줄여줍니다.

- 이전에 수행된 전송으로 TCP/IP 슬로우 스타트 알고리즘을 사전 준비하여 데이터 전송 속도를 향상시켰습니다
- 클라이언트 애플리케이션과 StorageGRID 시스템 간의 연결을 방해하는 여러 유형의 오류 상황에 대한 즉각적인 알림 기능

느린 시작의 이점과 리소스 할당 사이의 균형을 고려하여 유휴 연결을 얼마나 오랫동안 열어둘지 결정하십시오.

활성 **HTTP** 연결의 이점

스토리지 노드에 직접 연결하는 경우, HTTP 연결에서 지속적으로 트랜잭션을 수행하더라도 활성 HTTP 연결 시간은 최대 10분으로 제한해야 합니다.

연결을 유지할 최대 시간을 결정하는 것은 연결 지속성의 이점과 내부 시스템 리소스에 연결을 최적으로 할당하는 것

사이의 균형을 맞추는 문제입니다.

스토리지 노드에 대한 클라이언트 연결의 경우, 활성 HTTP 연결을 제한하면 다음과 같은 이점을 얻을 수 있습니다.

- StorageGRID 시스템 전체에서 최적의 로드 밸런싱을 지원합니다.

  시간이 지남에 따라 로드 밸런싱 요구 사항이 변경되면 HTTP 연결이 더 이상 최적의 방식이 아닐 수 있습니다. 클라이언트 애플리케이션이 각 트랜잭션마다 별도의 HTTP 연결을 설정할 때 시스템은 최상의 로드 밸런싱 성능을 발휘하지만, 이 방법은 영구 연결을 통해 얻을 수 있는 중요한 이점을 상쇄합니다.

- 클라이언트 애플리케이션이 사용 가능한 공간이 있는 LDR 서비스로 HTTP 트랜잭션을 보낼 수 있도록 합니다.
- 유지보수 절차를 시작할 수 있도록 합니다.

  일부 유지 관리 절차는 진행 중인 모든 HTTP 연결이 완료된 후에만 시작됩니다.

로드 밸런서 서비스에 대한 클라이언트 연결의 경우, 연결 유지 시간을 제한하면 일부 유지 관리 절차가 신속하게 시작될 수 있습니다. 클라이언트 연결 유지 시간을 제한하지 않으면 활성 연결이 자동으로 종료되는 데 몇 분이 걸릴 수 있습니다.

동시 **HTTP** 연결의 이점

StorageGRID 시스템에 여러 개의 TCP/IP 연결을 열어 두면 병렬 처리가 가능하여 성능이 향상됩니다. 최적의 병렬 연결 수는 다양한 요인에 따라 달라집니다.

동시 HTTP 연결은 다음과 같은 이점을 제공합니다.

- 지연 시간 감소

  다른 거래가 완료될 때까지 기다릴 필요 없이 즉시 거래를 시작할 수 있습니다.

- 처리량 증가

  StorageGRID 시스템은 병렬 트랜잭션을 수행하여 전체 트랜잭션 처리량을 향상시킬 수 있습니다.

클라이언트 애플리케이션은 여러 개의 HTTP 연결을 설정해야 합니다. 클라이언트 애플리케이션이 트랜잭션을 수행해야 할 경우, 현재 트랜잭션을 처리 중이지 않은 설정된 연결을 선택하여 즉시 사용할 수 있습니다.

각 StorageGRID 시스템의 토폴로지는 동시 트랜잭션 및 연결에 대한 최대 처리량이 다릅니다. 최대 처리량은 컴퓨팅, 네트워크, 스토리지 리소스, WAN 링크, 그리고 StorageGRID 시스템이 지원하는 서버, 서비스 및 애플리케이션의 수에 따라 달라집니다.

StorageGRID 시스템은 여러 클라이언트 애플리케이션을 지원하는 경우가 많습니다. 최대 동시 연결 수를 결정할 때 이 점을 염두에 두십시오. 클라이언트 애플리케이션이 StorageGRID 시스템에 각각 연결을 설정하는 여러 소프트웨어 엔티티로 구성된 경우, 모든 엔티티의 연결을 합산해야 합니다. 다음과 같은 상황에서는 최대 동시 연결 수를 조정해야 할 수 있습니다.

- StorageGRID 시스템의 토폴로지는 시스템이 지원할 수 있는 최대 동시 트랜잭션 및 연결 수에 영향을 미칩니다.
- 대역폭이 제한된 네트워크를 통해 StorageGRID 시스템과 상호 작용하는 클라이언트 애플리케이션은 개별 트랜잭션이 적절한 시간 내에 완료되도록 동시 처리 수준을 낮춰야 할 수 있습니다.
- 여러 클라이언트 애플리케이션이 StorageGRID 시스템을 공유하는 경우 시스템 제한을 초과하지 않도록 동시 실행 수준을 낮춰야 할 수 있습니다.

읽기 및 쓰기 작업을 위한 **HTTP** 연결 풀 분리

읽기 및 쓰기 작업에 대해 별도의 HTTP 연결 풀을 사용하고 각 작업에 사용할 풀의 양을 제어할 수 있습니다. HTTP 연결 풀을 분리하면 트랜잭션을 더 효과적으로 제어하고 로드 밸런싱을 개선할 수 있습니다.

클라이언트 애플리케이션은 읽기 작업이 주를 이루는 부하 또는 쓰기 작업이 주를 이루는 부하를 생성할 수 있습니다. 읽기 및 쓰기 트랜잭션에 대해 별도의 HTTP 연결 풀을 사용하면 각 풀에서 읽기 또는 쓰기 트랜잭션에 할당할 비율을 조정할 수 있습니다.

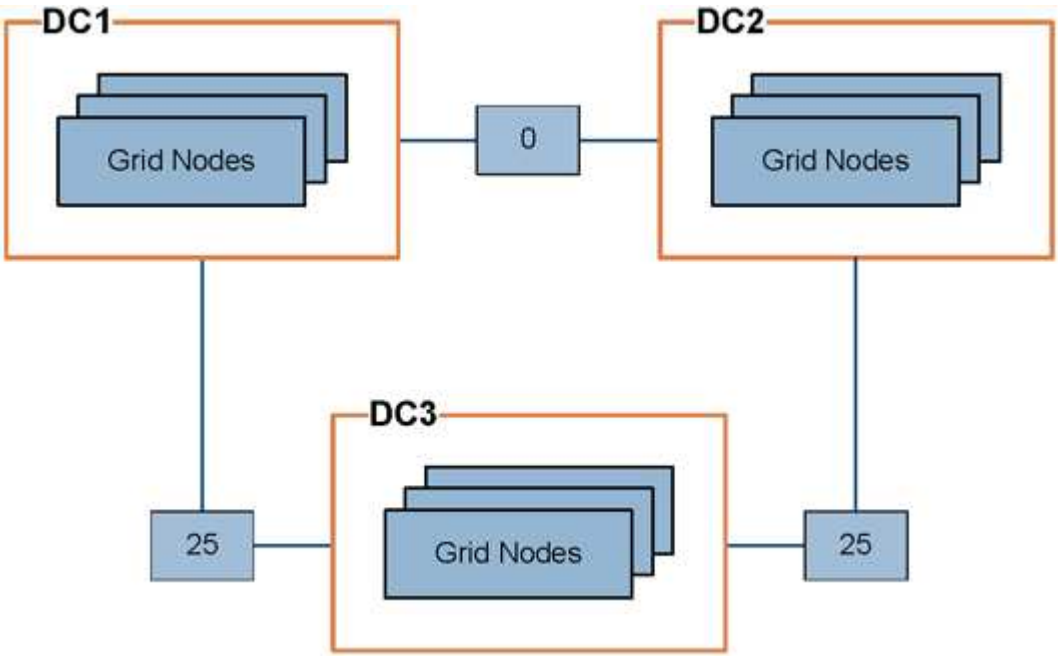
StorageGRID에서 링크 비용 관리

링크 비용을 사용하면 두 개 이상의 데이터 센터 사이트가 있는 경우 요청된 서비스를 제공할 데이터 센터 사이트의 우선순위를 지정할 수 있습니다. 사이트 간 지연 시간을 반영하여 링크 비용을 조정할 수 있습니다.

링크 비용이란 무엇입니까?

- 링크 비용은 객체 검색을 수행하는 데 사용할 객체 복사본의 우선순위를 정하는 데 사용됩니다.
- 링크 비용은 Grid Management API와 Tenant Management API에서 사용할 내부 StorageGRID 서비스를 결정하는 데 사용됩니다.
- 링크 비용은 관리 노드와 게이트웨이 노드의 로드 밸런서 서비스에서 클라이언트 연결을 지정하는 데 사용됩니다. "로드 밸런싱 고려 사항"을 참조하십시오.

이 다이어그램은 사이트 간 링크 비용이 구성된 3개 사이트 그리드를 보여줍니다.



- 관리 노드와 게이트웨이 노드의 로드 밸런싱 서비스는 클라이언트 연결을 동일한 데이터 센터 사이트의 모든 스토리지 노드와 링크 비용이 0인 모든 데이터 센터 사이트로 균등하게 분산합니다.

  예시에서 데이터 센터 사이트 1(DC1)의 게이트웨이 노드는 클라이언트 연결을 DC1의 스토리지 노드와 DC2의 스토리지 노드에 균등하게 분산합니다. DC3의 게이트웨이 노드는 클라이언트 연결을 DC3의 스토리지 노드로만 보냅니다.

- 여러 개의 복제본으로 존재하는 객체를 검색할 때 StorageGRID는 링크 비용이 가장 낮은 데이터 센터의 복제본을 검색합니다.

  예시에서 DC2의 클라이언트 애플리케이션이 DC1과 DC3 모두에 저장된 객체를 검색하는 경우 DC1에서 객체를 검색합니다. 이는 DC1에서 DC2로의 링크 비용이 0으로 DC3에서 DC2로의 링크 비용(25)보다 낮기 때문입니다.

링크 비용은 특정 측정 단위가 없는 임의의 상대적인 수치입니다. 예를 들어, 링크 비용 50은 링크 비용 25보다 선호도가 낮습니다. 아래 표는 일반적으로 사용되는 링크 비용을 보여줍니다.

링크	링크 비용	참고
물리적 데이터 센터 사이트 간	25 (기본값)	WAN 링크로 연결된 데이터 센터.
동일한 물리적 위치에 있는 논리적 데이터 센터 사이트 간	0	동일한 물리적 건물 또는 캠퍼스 내에 위치하고 LAN으로 연결된 논리적 데이터 센터.

링크 비용 업데이트

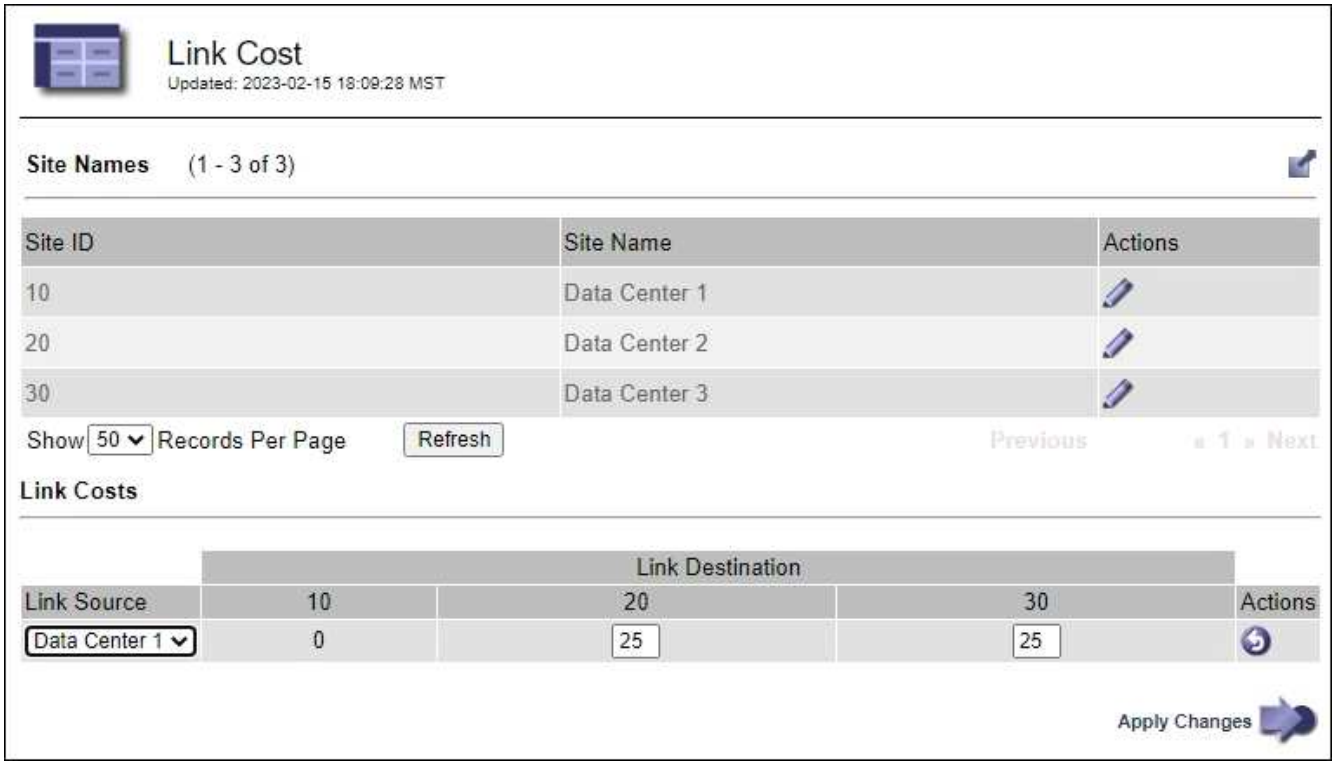
데이터 센터 사이트 간 링크 비용을 업데이트하여 사이트 간 지연 시간을 반영할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "기타 그리드 구성 권한".

단계

1. 지원 > 기타 > *링크 비용*을 선택합니다.



2. *링크 소스*에서 사이트를 선택하고 *링크 대상*에 0에서 100 사이의 비용 값을 입력하십시오.

   출발지와 목적지가 동일한 경우 링크 비용을 변경할 수 없습니다.

   변경 사항을 취소하려면 *Revert*를 선택하세요.

3. *변경 사항 적용*을 선택합니다.

AutoSupport 사용

StorageGRID의 AutoSupport에 대해 알아보기

AutoSupport 기능을 사용하면 StorageGRID가 상태 및 현황 패키지를 NetApp 기술 지원에 전송할 수 있습니다.

AutoSupport를 사용하면 문제를 더 빠르게 해결할 수 있습니다. 기술 지원팀은 시스템의 스토리지 요구 사항을 모니터링하고 새 노드 또는 사이트를 추가해야 하는지 여부를 판단하는 데 도움을 줄 수 있습니다. 선택적으로 AutoSupport는 패키지를 추가 목적지 한 곳으로 전송할 수 있습니다.

StorageGRID 에는 두 가지 유형의 AutoSupport가 있습니다:

- **StorageGRID AutoSupport** StorageGRID 소프트웨어 문제를 보고합니다. StorageGRID를 처음 설치할 때 기본적으로 활성화됩니다. 필요한 경우 "기본 AutoSupport 구성 변경" 수 있습니다.

  > StorageGRID AutoSupport가 활성화되어 있지 않으면 그리드 관리자 대시보드에 메시지가 표시됩니다. 이 메시지에는 AutoSupport 구성 페이지 링크가 포함되어 있습니다. 메시지를 닫으면 AutoSupport가 비활성화된 상태이더라도 브라우저 캐시를 삭제하기 전까지는 다시 표시되지 않습니다.

- *어플라이언스 하드웨어 AutoSupport*은 StorageGRID 어플라이언스 문제를 보고합니다. 반드시 "각 어플라이언스에서 하드웨어 AutoSupport 구성".

Active IQ란 무엇입니까?

Active IQ는 NetApp의 기존 고객 기반에서 축적된 예측 분석 및 커뮤니티 노하우를 활용하는 클라우드 기반 디지털 어드바이저입니다. 지속적인 위험 평가, 예측 알림, 맞춤형 지침 및 자동화된 조치를 통해 문제가 발생하기 전에 예방하여 시스템 상태를 개선하고 가용성을 높일 수 있습니다.

NetApp 지원 사이트에서 Active IQ 대시보드 및 기능을 사용하려면 AutoSupport를 활성화해야 합니다.

"Active IQ Digital Advisor 문서"

AutoSupport 패키지에 포함된 정보

AutoSupport 패키지에는 다음과 같은 파일과 세부 정보가 포함되어 있습니다.

파일 이름	필드	설명
AUTOSUPPORT-HISTORY.XML	AutoSupport 시퀀스 번호 + 이 AutoSupport의 대상 + 전달 상태 + 전달 시도 횟수 + AutoSupport 제목 + 전달 URI + 마지막 오류 + AutoSupport PUT 파일 이름 + 생성 시간 + Autosupport 압축 크기 + Autosupport 압축 해제 크기 + 총 수집 시간(밀리초)	AutoSupport 기록 파일.
AUTOSUPPORT.XML	노드 + 지원팀에 연락할 프로토콜 + HTTP/HTTPS용 지원 URL + 지원 주소 + AutoSupport OnDemand 상태 + AutoSupport OnDemand 서버 URL + AutoSupport OnDemand 폴링 간격	AutoSupport 상태 파일입니다. 사용된 프로토콜, 기술 지원 URL 및 주소, 폴링 간격, 그리고 OnDemand AutoSupport 활성화/비활성화 여부에 대한 세부 정보를 제공합니다.
BUCKETS.XML	버킷 ID + 계정 ID + 빌드 버전 + 위치 제약 조건 구성 + 규정 준수 활성화 + 규정 준수 구성 + S3 Object Lock 활성화 + S3 Object Lock 구성 + 일관성 구성 + CORS 활성화 + CORS 구성 + 마지막 액세스 시간 활성화 + 정책 활성화 + 정책 구성 + 알림 활성화 + 알림 구성 + 클라우드 미러 활성화 + 클라우드 미러 구성 + 검색 활성화 + 검색 구성 + 버킷 태깅 활성화 + 버킷 태깅 구성 + 버전 관리 구성	버킷 수준의 구성 세부 정보와 통계를 제공합니다. 버킷 구성의 예로는 플랫폼 서비스, 규정 준수 및 버킷 일관성이 있습니다.
GRID-CONFIGURATIONS.XML	속성 ID + 속성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	그리드 전체 구성 정보 파일입니다. 그리드 인증서, 메타데이터 예약 공간, 그리드 전체 구성 설정(규정 준수, S3 객체 잠금, 객체 압축, 경고, syslog 및 ILM 구성), 소거 코딩 프로필 세부 정보, DNS 이름 및 "NMS 이름"에 대한 정보가 포함되어 있습니다.
GRID-SPEC.XML	그리드 사양, 원시 XML	StorageGRID 구성 및 배포에 사용됩니다. 그리드 사양, NTP 서버 IP, DNS 서버 IP, 네트워크 토폴로지 및 노드의 하드웨어 프로필이 포함되어 있습니다.
GRID-TASKS.XML	노드 + 서비스 경로 + 속성 ID + 속성 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.

파일 이름	필드	설명
GRID.JSON	그리드 + 개정판 + 소프트웨어 버전 + 설명 + 라이선스 + 비밀번호 + DNS + NTP + 사이트 + 노드	그리드 정보.
ILM-CONFIGURATION.XML	속성 ID + 속성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	ILM 구성에 사용되는 속성 목록입니다.
ILM-STATUS.XML	노드 + 서비스 경로 + 속성 ID + 속성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	ILM 메트릭 정보 파일입니다. 각 노드의 ILM 평가율과 그리드 전체 메트릭을 포함합니다.
ILM.XML	ILM 원시 XML	ILM 활성 정책 파일. 스토리지 풀 ID, 수집 동작, 필터, 규칙 및 설명과 같은 활성 ILM 정책에 대한 세부 정보를 포함합니다.
LOG.TGZ	해당 없음	다운로드 가능한 로그 파일. 각 노드의 `bycast-err.log` 및 `servermanager.log`이(가) 포함되어 있습니다.
MANIFEST.XML	수집 순서 + AutoSupport 이 데이터에 대한 콘텐츠 파일 이름 + 이 데이터 항목에 대한 설명 + 수집된 바이트 수 + 수집에 소요된 시간 + 이 데이터 항목의 상태 + 오류 설명 + AutoSupport 이 데이터에 대한 콘텐츠 유형	AutoSupport 메타데이터와 모든 AutoSupport 파일에 대한 간략한 설명이 포함되어 있습니다.
NMS-ENTITIES.XML	속성 인덱스 + 엔티티 OID + 노드 ID + 장치 모델 ID + 장치 모델 버전 + 엔티티 이름	그룹 및 서비스 엔티티를 보여 "NMS 트리" 줍니다. 그리드 토폴로지 세부 정보를 제공합니다. 노드는 해당 노드에서 실행 중인 서비스를 기반으로 확인할 수 있습니다.
OBJECTS-STATUS.XML	노드 + 서비스 경로 + 속성 ID + 속성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	객체 상태에는 백그라운드 스캔 상태, 활성 전송, 전송 속도, 총 전송 횟수, 삭제 속도, 손상된 조각, 손실된 객체, 누락된 객체, 복구 시도 횟수, 스캔 속도, 예상 스캔 기간 및 복구 완료 상태가 포함됩니다.

파일 이름	필드	설명
SERVER-STATUS.XML	노드 + 서비스 경로 + 속성 ID + 속성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	서버 구성. 각 노드에 대한 다음 세부 정보가 포함됩니다. 플랫폼 유형, 운영 체제, 설치된 메모리, 사용 가능한 메모리, 스토리지 연결, 스토리지 어플라이언스 섀시 일련 번호, 스토리지 컨트롤러 고장 드라이브 수, 컴퓨팅 컨트롤러 섀시 온도, 컴퓨팅 하드웨어, 컴퓨팅 컨트롤러 일련 번호, 전원 공급 장치, 드라이브 크기 및 드라이브 유형.
SERVICE-STATUS.XML	노드 + 서비스 경로 + 속성 ID + 속성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	서비스 노드 정보 파일. 할당된 테이블 공간, 사용 가능한 테이블 공간, 데이터베이스의 Reaper 메트릭, 세그먼트 복구 시간, 복구 작업 시간, 자동 작업 재시작 및 자동 작업 종료와 같은 세부 정보가 포함되어 있습니다.
STORAGE-GRADES.XML	스토리지 등급 ID + 스토리지 등급 이름 + 스토리지 노드 ID + 스토리지 노드 경로	각 스토리지 노드에 대한 스토리지 등급 정의 파일입니다.
SUMMARY-ATTRIBUTES.XML	그룹 OID + 그룹 경로 + 요약 속성 ID + 요약 속성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	StorageGRID 사용 정보를 요약한 상위 수준 시스템 상태 데이터입니다. 그리드 이름, 사이트 이름, 그리드 및 사이트별 스토리지 노드 수, 라이선스 유형, 라이선스 용량 및 사용량, 소프트웨어 지원 조건, S3 운영 세부 정보 등의 정보를 제공합니다.
SYSTEM-ALERTS.XML	이름 + 심각도 + 노드 이름 + 경고 상태 + 사이트 이름 + 경고 발생 시간 + 경고 해결 시간 + 규칙 ID + 노드 ID + 사이트 ID + 무시됨 + 기타 주석 + 기타 레이블	StorageGRID 시스템에서 발생할 수 있는 잠재적인 문제를 나타내는 현재 시스템 경고입니다.
USERAGENTS.XML	사용자 에이전트 + 기간(일) + 총 HTTP 요청 수 + 총 수집 바이트 수 + 총 검색 바이트 수 + PUT 요청 수 + GET 요청 수 + DELETE 요청 수 + HEAD 요청 수 + POST 요청 수 + OPTIONS 요청 수 + 평균 요청 시간(밀리초) + 평균 PUT 요청 시간(밀리초) + 평균 GET 요청 시간(밀리초) + 평균 DELETE 요청 시간(밀리초) + 평균 HEAD 요청 시간(밀리초) + 평균 POST 요청 시간(밀리초) + 평균 OPTIONS 요청 시간(밀리초)	애플리케이션 사용자 에이전트를 기반으로 한 통계입니다. 예를 들어, 사용자 에이전트별 PUT/GET/DELETE/HEAD 작업 횟수 및 각 작업의 총 바이트 크기 등을 확인할 수 있습니다.

파일 이름	필드	설명
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name	AutoSupport 헤더 데이터.

StorageGRID에서 AutoSupport 구성

기본적으로 StorageGRID AutoSupport 기능은 StorageGRID를 처음 설치할 때 활성화됩니다. 하지만 각 어플라이언스에서 하드웨어 AutoSupport를 구성해야 합니다. 필요에 따라 AutoSupport 구성을 변경할 수 있습니다.

StorageGRID AutoSupport 구성을 변경하려면 기본 관리 노드에서만 변경하십시오. 각 어플라이언스에서 하드웨어 AutoSupport 구성해야 합니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"
- AutoSupport 패키지를 전송할 때 HTTPS를 사용하려면 기본 관리 노드에 직접 또는 "프록시 서버 사용"(수신 연결은 필요하지 않음) 발신 인터넷 액세스 권한을 제공해야 합니다.
- StorageGRID AutoSupport 페이지에서 HTTP가 선택된 경우, AutoSupport 패키지를 HTTPS로 전달하려면 "프록시 서버를 구성했습니다"해야 합니다. NetApp의 AutoSupport 서버는 HTTP를 사용하여 전송된 패키지를 거부합니다.
- AutoSupport 패키지에 SMTP 프로토콜을 사용하려면 SMTP 메일 서버를 구성해야 합니다.

이 작업 정보

다음 옵션 중 원하는 조합을 사용하여 AutoSupport 패키지를 기술 지원 팀에 보낼 수 있습니다:

- 주간: AutoSupport 패키지를 매주 한 번 자동으로 발송합니다. 기본 설정: 활성화됨.
- 이벤트 기반: 매시간 또는 중요한 시스템 이벤트 발생 시 AutoSupport 패키지를 자동으로 전송합니다. 기본 설정: 활성화됨.
- 요청 시: 기술 지원팀이 StorageGRID 시스템에서 AutoSupport 패키지를 자동으로 전송하도록 요청할 수 있습니다. 이는 기술 지원팀이 문제를 적극적으로 해결하는 동안 유용합니다(HTTPS AutoSupport 전송 프로토콜 필요). 기본 설정: 비활성화됨.
- 사용자 실행: 언제든지 수동으로 AutoSupport 패키지를 보낼 수 있습니다.
- 로그 수집: "수동으로 로그 파일과 시스템 데이터를 수집하여 AutoSupport 패키지를 전송합니다.".

AutoSupport 패키지에 대한 프로토콜을 지정합니다.

AutoSupport 패키지를 전송하는 데에는 다음 프로토콜 중 하나를 사용할 수 있습니다.

- **HTTPS**: 이는 새 설치 시 기본 설정이며 권장되는 설정입니다. 이 프로토콜은 443번 포트를 사용합니다.

AutoSupport 온디맨드 기능 활성화하려면 HTTPS를 사용해야 합니다.

- **HTTP**: HTTP를 선택하는 경우, AutoSupport 패키지를 HTTPS로 전달하도록 프록시 서버를 구성해야 합니다. NetApp의 AutoSupport 서버는 HTTP를 사용하여 전송된 패키지를 거부합니다. 이 프로토콜은 80번 포트를 사용합니다.
- **SMTP**: AutoSupport 패키지를 이메일로 받으려면 이 옵션을 사용하십시오.

설정한 프로토콜은 모든 유형의 AutoSupport 패키지를 전송하는 데 사용됩니다.

단계

1. 지원 > 도구 > **AutoSupport** > *설정*을 선택합니다.
2. AutoSupport 패키지를 전송하는 데 사용할 프로토콜을 선택하십시오.
3. *HTTPS*를 선택한 경우, NetApp 지원 인증서(TLS 인증서)를 사용하여 기술 지원 서버와의 연결을 보호할지 여부를 선택하십시오.
   - 인증서 확인(기본값): AutoSupport 패키지 전송의 보안을 보장합니다. NetApp 지원 인증서는 StorageGRID 소프트웨어와 함께 이미 설치되어 있습니다.
   - 인증서 확인 안 함: 인증서에 일시적인 문제가 있는 경우와 같이 인증서 유효성 검사를 사용하지 않아야 할 타당한 이유가 있을 때만 이 옵션을 선택하십시오.
4. *저장*을 선택합니다. 선택한 프로토콜을 사용하여 모든 주간, 사용자 요청 및 이벤트 트리거 패키지가 전송됩니다.

주간 **AutoSupport** 비활성화

기본적으로 StorageGRID 시스템은 일주일에 한 번 기술 지원에 AutoSupport 패키지를 보내도록 구성되어 있습니다.

주간 AutoSupport 패키지 발송 일정을 확인하려면 **AutoSupport** > 결과 탭으로 이동하세요. 주간 **AutoSupport** 섹션에서 다음 예정 시간 값을 확인하세요.

주간 AutoSupport 패키지의 자동 전송은 언제든지 비활성화할 수 있습니다.

단계

1. 지원 > 도구 > **AutoSupport** > *설정*을 선택합니다.
2. 주간 **AutoSupport** 활성화 확인란의 선택을 해제합니다.
3. *저장*을 선택하세요.

이벤트 기반 **AutoSupport** 비활성화

기본적으로 StorageGRID 시스템은 매시간 기술 지원팀에 AutoSupport 패키지를 전송하도록 구성되어 있습니다.

이벤트 기반 AutoSupport는 언제든지 비활성화할 수 있습니다.

단계

1. 지원 > 도구 > **AutoSupport** > *설정*을 선택합니다.
2. 이벤트 기반 **AutoSupport** 활성화 확인란의 선택을 해제합니다.
3. *저장*을 선택하세요.

주문형 **AutoSupport** 활성화

AutoSupport on Demand는 기술 지원 팀이 현재 처리 중인 문제를 해결하는 데 도움을 줄 수 있습니다.

기본적으로 AutoSupport on Demand는 비활성화되어 있습니다. 이 기능을 활성화하면 기술 지원팀이 StorageGRID 시스템에 AutoSupport 패키지를 자동으로 전송하도록 요청할 수 있습니다. 기술 지원팀은 AutoSupport on Demand 쿼리에 대한 폴링 시간 간격을 설정할 수도 있습니다.

기술 지원은 AutoSupport on Demand를 활성화하거나 비활성화할 수 없습니다.

단계

1. 지원 > 도구 > **AutoSupport** > *설정*을 선택합니다.
2. 프로토콜로 *HTTPS*를 선택합니다.
3. 주간 **AutoSupport** 활성화 확인란을 선택합니다.
4. * AutoSupport on Demand 활성화* 확인란을 선택하십시오.
5. *저장*을 선택하세요.

   AutoSupport on Demand가 활성화되어 있으며, 기술 지원팀이 AutoSupport on Demand 요청을 StorageGRID로 보낼 수 있습니다.

소프트웨어 업데이트 확인 비활성화

기본적으로 StorageGRID는 NetApp에 연결하여 시스템에 사용할 수 있는 소프트웨어 업데이트가 있는지 확인합니다. StorageGRID 핫픽스 또는 새 버전이 있는 경우 StorageGRID 업그레이드 페이지에 새 버전이 표시됩니다.

필요에 따라 소프트웨어 업데이트 확인 기능을 선택적으로 비활성화할 수 있습니다. 예를 들어, 시스템에 WAN 액세스가 없는 경우 다운로드 오류를 방지하기 위해 업데이트 확인 기능을 비활성화해야 합니다.

단계

1. 지원 > 도구 > **AutoSupport** > *설정*을 선택합니다.
2. 소프트웨어 업데이트 확인 확인란을 선택 해제하세요.
3. *저장*을 선택하세요.

추가 **AutoSupport** 대상 추가

AutoSupport를 활성화하면 상태 및 건강 관련 패키지가 기술 지원 팀으로 전송됩니다. 모든 AutoSupport 패키지에 대해 추가 전송 대상을 하나 지정할 수 있습니다.

AutoSupport 패키지를 전송하는 데 사용되는 프로토콜을 확인하거나 변경하려면 AutoSupport 패키지에 대한 프로토콜을 지정합니다. 지침을 참조하십시오.

> SMTP 프로토콜을 사용하여 AutoSupport 패키지를 추가 목적지로 전송할 수 없습니다.

단계

1. 지원 > 도구 > **AutoSupport** > *설정*을 선택합니다.
2. *추가 AutoSupport 대상 활성화*를 선택하십시오.

3. 다음을 지정합니다.

   호스트 이름

   추가 AutoSupport 대상 서버의 서버 호스트 이름 또는 IP 주소입니다.

   ⓘ 추가 목적지는 한 곳만 입력할 수 있습니다.

   포트

   추가 AutoSupport 대상 서버에 연결하는 데 사용되는 포트입니다. 기본값은 HTTP의 경우 80번 포트이고 HTTPS의 경우 443번 포트입니다.

   인증서 유효성 검사

   추가 목적지와의 연결을 보호하기 위해 TLS 인증서가 사용되는지 여부.

   - 인증서 유효성 검사를 사용하려면 *인증서 확인*을 선택하십시오.
   - 인증서 유효성 검사 없이 AutoSupport 패키지를 보내려면 *인증서 확인 안 함*을 선택하십시오.

     인증서 유효성 검사를 사용하지 않아야 할 타당한 이유가 있는 경우(예: 인증서에 일시적인 문제가 발생한 경우)에만 이 옵션을 선택하십시오.

4. *인증서 확인*을 선택한 경우 다음을 수행합니다.
   a. CA 인증서가 있는 위치로 이동합니다.
   b. CA 인증서 파일을 업로드합니다.

      CA 인증서 메타데이터가 표시됩니다.

5. *저장*을 선택하세요.

   향후 모든 주간, 이벤트 기반 및 사용자 트리거 방식의 AutoSupport 패키지는 지정된 추가 수신처로 전송됩니다.

어플라이언스에 대한 **AutoSupport** 구성

AutoSupport 어플라이언스용 AutoSupport는 StorageGRID 하드웨어 문제를 보고하고, StorageGRID AutoSupport는 StorageGRID 소프트웨어 문제를 보고합니다. 단, SGF6112의 경우 StorageGRID AutoSupport가 하드웨어 및 소프트웨어 문제를 모두 보고합니다. 추가 구성이 필요하지 않은 SGF6112를 제외한 각 어플라이언스에서 AutoSupport를 구성해야 합니다. AutoSupport는 서비스 어플라이언스와 스토리지 어플라이언스에서 다르게 구현됩니다.

SANtricity를 사용하여 각 스토리지 어플라이언스에 대한 AutoSupport를 활성화할 수 있습니다. 어플라이언스 초기 설정 중 또는 어플라이언스 설치 후 SANtricity AutoSupport를 구성할 수 있습니다.

- SG6000 및 SG5700 기기의 경우, "SANtricity System Manager에서 AutoSupport 구성"

"SANtricity System Manager"에서 프록시를 통한 AutoSupport 전송을 구성하면 E-Series 어플라이언스의 AutoSupport 패키지를 StorageGRID AutoSupport에 포함할 수 있습니다.

StorageGRID AutoSupport은(는) DIMM 또는 호스트 인터페이스 카드(HIC) 오류와 같은 하드웨어 문제를 보고하지 않습니다. 그러나 일부 구성 요소 오류는 "하드웨어 경고"을(를) 트리거할 수 있습니다. 베이스보드 관리 컨트롤러(BMC)가 있는 StorageGRID 어플라이언스의 경우 하드웨어 오류를 보고하도록 이메일 및 SNMP 트랩을 구성할 수

있습니다.

- "BMC 알림에 대한 이메일 알림을 설정합니다"
- "BMC에 대한 SNMP 설정 구성"

관련 정보

"NetApp 지원"

StorageGRID에서 AutoSupport 패키지를 수동으로 트리거합니다

StorageGRID 시스템의 문제 해결 시 기술 지원을 원활하게 진행하기 위해, 수동으로 AutoSupport 패키지를 전송하도록 트리거할 수 있습니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 루트 액세스 권한 또는 기타 그리드 구성 권한이 있습니다.

단계

1. 지원 > 도구 > *AutoSupport*을 선택합니다.
2. 작업 탭에서 *사용자 트리거 AutoSupport 보내기*를 선택합니다.

   StorageGRID가 AutoSupport 패키지를 NetApp 지원 사이트로 전송하려고 시도합니다. 시도가 성공하면 결과 탭의 최근 결과 및 마지막 성공 시간 값이 업데이트됩니다. 문제가 발생하면 최근 결과 값이 "실패"로 업데이트되고 StorageGRID는 AutoSupport 패키지를 다시 전송하려고 시도하지 않습니다.

3. 1분 후 브라우저에서 AutoSupport 페이지를 새로고침하여 최신 결과를 확인하십시오.

> 또한, "보다 광범위한 로그 파일과 시스템 데이터를 수집합니다."해당 내용을 NetApp 지원 사이트로 보내실 수도 있습니다.

StorageGRID AutoSupport 패키지 문제 해결

AutoSupport 패키지 전송 시도가 실패하면 StorageGRID 시스템은 AutoSupport 패키지 유형에 따라 다른 조치를 취합니다. AutoSupport 패키지의 상태는 지원 > 도구 > **AutoSupport** > *결과*를 선택하여 확인할 수 있습니다.

AutoSupport 패키지 전송에 실패하면 **AutoSupport** 페이지의 결과 탭에 "실패"가 표시됩니다.

> 프록시 서버를 구성하여 AutoSupport 패키지를 NetApp에 전달하도록 설정한 경우, "프록시 서버 구성 설정이 올바른지 확인하십시오."해야 합니다.

주간 **AutoSupport** 패키지 오류

주간 AutoSupport 패키지 전송에 실패할 경우 StorageGRID 시스템은 다음과 같은 조치를 취합니다.

1. 최근 결과 속성을 재시도 중으로 업데이트합니다.

2. AutoSupport 패키지를 1시간 동안 4분 간격으로 15회 재전송하려고 시도합니다.
3. 전송 실패가 1시간 동안 지속되면 '최근 결과' 속성을 '실패'로 업데이트합니다.
4. 다음 예정된 시간에 AutoSupport 패키지를 다시 보내려고 시도합니다.
5. NMS 서비스를 사용할 수 없어 패키지 전송이 실패하거나 7일이 지나기 전에 패키지가 전송된 경우 정기적인 AutoSupport 일정을 유지합니다.
6. NMS 서비스가 다시 사용 가능해지면, 7일 이상 패키지가 전송되지 않은 경우 AutoSupport 패키지를 즉시 전송합니다.

사용자 또는 이벤트에 의해 발생한 **AutoSupport** 패키지 오류

사용자 또는 이벤트에 의해 트리거된 AutoSupport 패키지 전송에 실패하면 StorageGRID 시스템은 다음과 같은 조치를 취합니다.

1. 알려진 오류인 경우 오류 메시지를 표시합니다. 예를 들어, 사용자가 올바른 이메일 구성 설정을 제공하지 않고 SMTP 프로토콜을 선택하면 다음과 같은 오류 메시지가 표시됩니다. `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. 패키지를 다시 보내려고 시도하지 않습니다.
3. 오류를 `nms.log`에 기록합니다.

오류가 발생하고 SMTP가 선택된 프로토콜인 경우, StorageGRID 시스템의 이메일 서버가 올바르게 구성되어 있고 이메일 서버가 실행 중인지 확인하십시오(지원 > 알람(레거시) > 레거시 이메일 설정). 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.`

"이메일 서버 설정 구성" 방법을 알아보십시오.

AutoSupport 패키지 오류 수정

오류가 발생하고 SMTP가 선택된 프로토콜인 경우, StorageGRID 시스템의 이메일 서버가 올바르게 구성되어 있고 사용자의 이메일 서버가 실행 중인지 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.`

StorageGRID를 통해 E-Series AutoSupport 패키지 전송

E-Series SANtricity System Manager AutoSupport 패키지는 스토리지 어플라이언스 관리 포트 대신 StorageGRID 관리 노드를 통해 기술 지원팀으로 보낼 수 있습니다.

`https://docs.netapp.com/us-en/e-series-santricity/sm-support/autosupport-feature-overview.html["E-시리즈 하드웨어 AutoSupport"^]E-시리즈 어플라이언스에서 AutoSupport를 사용하는 방법에 대한 자세한 내용은 해당 문서를 참조하십시오.`

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 당신은 "스토리지 어플라이언스 관리자 또는 루트 액세스 권한"을(를) 가지고 있습니다.

- SANtricity AutoSupport를 구성했습니다:
  - SG6000 및 SG5700 기기의 경우, "SANtricity System Manager에서 AutoSupport 구성"

> Grid Manager를 사용하여 SANtricity System Manager에 액세스하려면 SANtricity 펌웨어 8.70 이상이 필요합니다.

이 작업 정보

E-Series AutoSupport 패키지에는 스토리지 하드웨어의 세부 정보가 포함되어 있으며 StorageGRID 시스템에서 전송하는 다른 AutoSupport 패키지보다 더 구체적입니다.

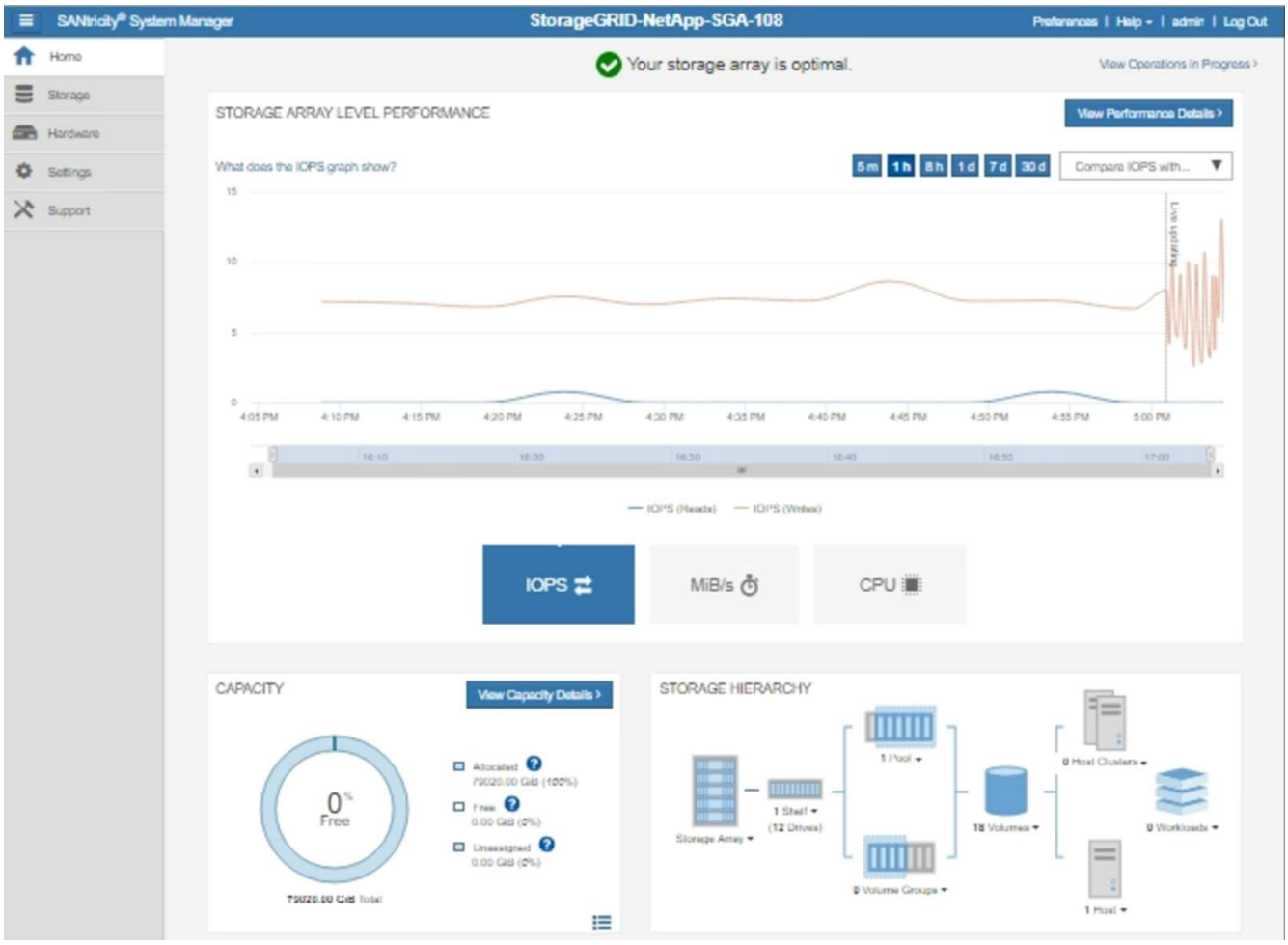
SANtricity System Manager에서 특수 프록시 서버 주소를 구성하면 어플라이언스의 관리 포트를 사용하지 않고 StorageGRID 관리 노드를 통해 AutoSupport 패키지를 전송할 수 있습니다. 이러한 방식으로 전송되는 AutoSupport 패키지는 "기본 발신자 관리 노드"에 의해 전송되며, Grid Manager에 구성된 "관리자 프록시 설정"를 사용합니다.

> 이 절차는 E-Series AutoSupport 패키지용 StorageGRID 프록시 서버를 구성하기 위한 것입니다. E-Series AutoSupport 구성에 대한 자세한 내용은 "NetApp E-Series 및 SANtricity 설명서"을 참조하십시오.

단계

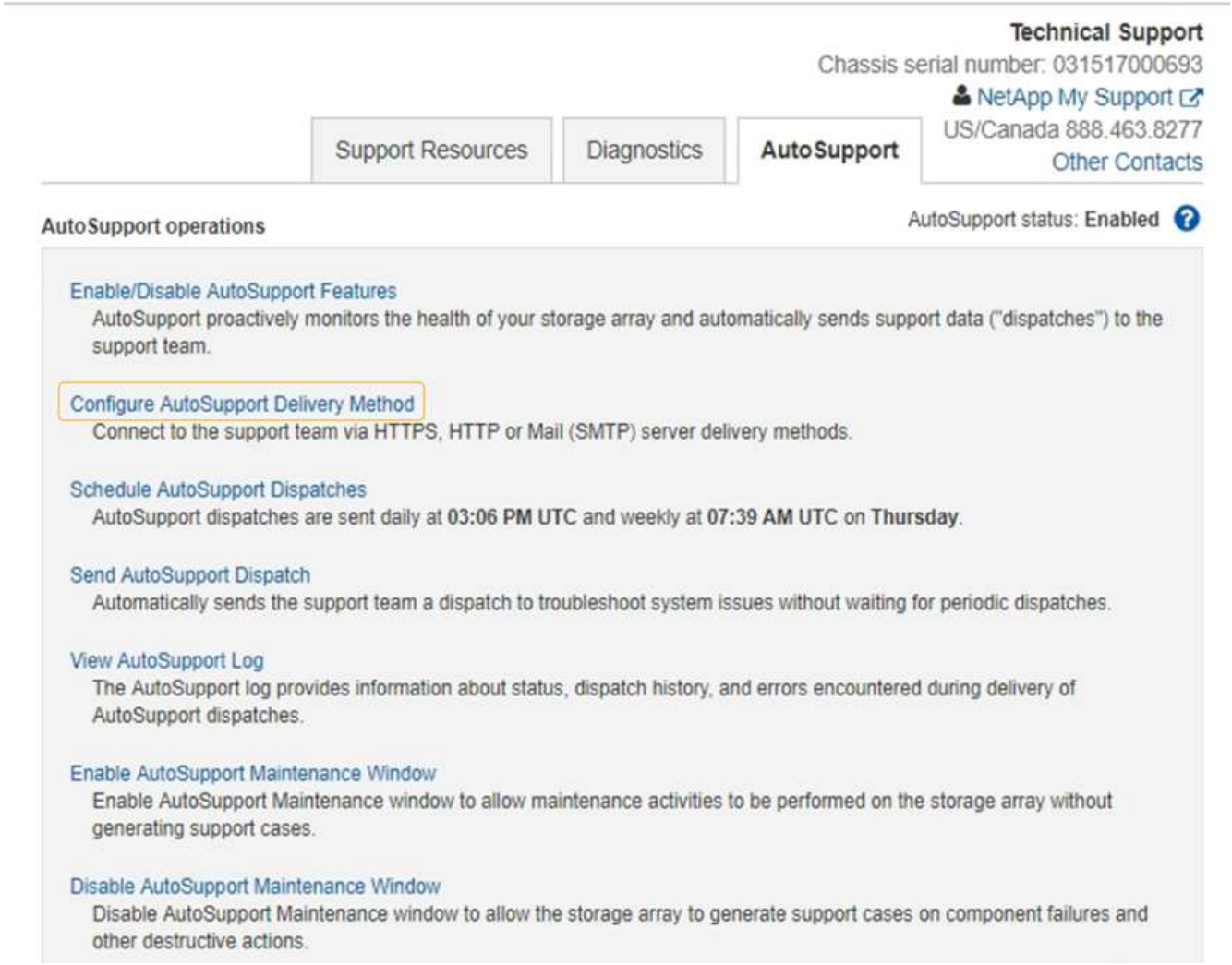
1. Grid Manager에서 *노드*를 선택합니다.
2. 왼쪽의 노드 목록에서 구성할 스토리지 어플라이언스 노드를 선택합니다.
3. *SANtricity System Manager*를 선택합니다.

   SANtricity System Manager 홈 페이지가 나타납니다.



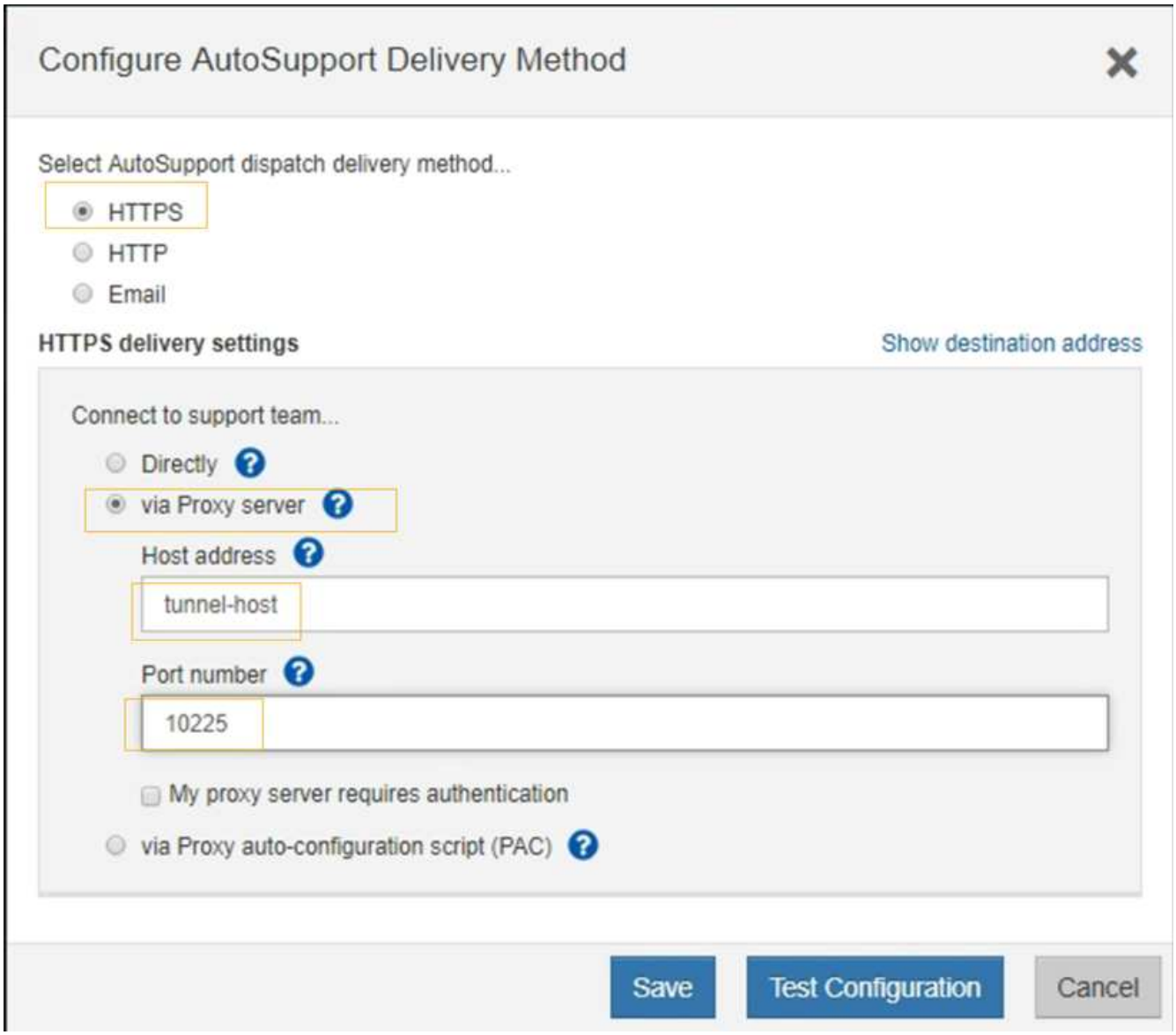
4. 지원 > 지원 센터 > *AutoSupport*를 선택합니다.

   AutoSupport 작업 페이지가 나타납니다.



5. **AutoSupport** 전달 방법 *구성*을 선택합니다.

   AutoSupport 전송 방법 구성 페이지가 나타납니다.



6. 전송 방법으로 *HTTPS*를 선택합니다.

   HTTPS를 활성화하는 인증서가 미리 설치되어 있습니다.

7. *프록시 서버를 통해*를 선택합니다.
8. `tunnel-host`를 *호스트 주소*로 입력합니다.

   `tunnel-host`은(는) 관리자 노드를 사용하여 E-Series AutoSupport 패키지를 전송하기 위한 특별 주소입니다.

9. *포트 번호*에 `10225`를 입력합니다.

   `10225`은(는) 어플라이언스의 E-Series 컨트롤러에서 AutoSupport 패키지를 수신하는 StorageGRID 프록시 서버의 포트 번호입니다.

10. *구성 테스트*를 선택하여 AutoSupport 프록시 서버의 라우팅 및 구성을 테스트합니다.

    올바른 경우 녹색 배너에 "AutoSupport 구성이 확인되었습니다."라는 메시지가 나타납니다.

테스트에 실패하면 빨간색 배너에 오류 메시지가 표시됩니다. StorageGRID DNS 설정 및 네트워킹을 확인하고 "기본 발신자 관리 노드"가 NetApp 지원 사이트에 연결할 수 있는지 확인한 후 테스트를 다시 시도하십시오.

11. *저장*을 선택하세요.

    구성이 저장되고 "AutoSupport 전달 방식이 구성되었습니다."라는 확인 메시지가 나타납니다.

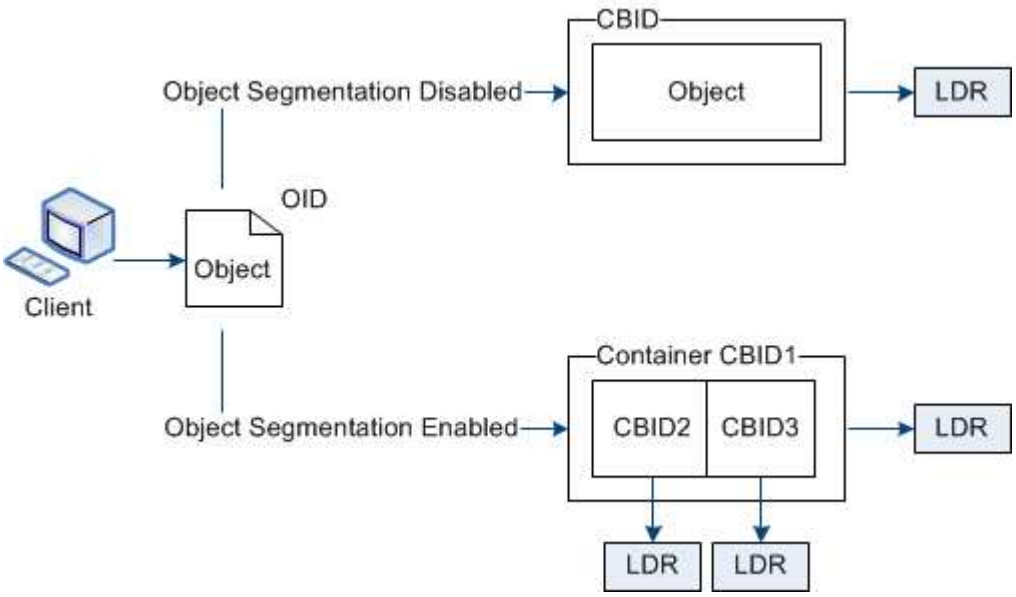
${post_edited_translations.segment}

저장 옵션 사용

StorageGRID의 오브젝트 세그먼트화에 대해 알아보십시오

객체 분할은 대형 객체를 더 작은 고정 크기 객체들의 모음으로 나누어 저장 공간과 리소스 사용을 최적화하는 과정입니다. S3 멀티파트 업로드 또한 분할된 객체를 생성하며, 각 파트는 하나의 객체로 표현됩니다.

객체가 StorageGRID 시스템에 수집되면 LDR 서비스는 객체를 세그먼트로 분할하고 모든 세그먼트의 헤더 정보를 콘텐츠로 나열하는 세그먼트 컨테이너를 생성합니다.



세그먼트 컨테이너를 검색할 때 LDR 서비스는 해당 세그먼트들로부터 원래 객체를 조립하여 클라이언트에 반환합니다.

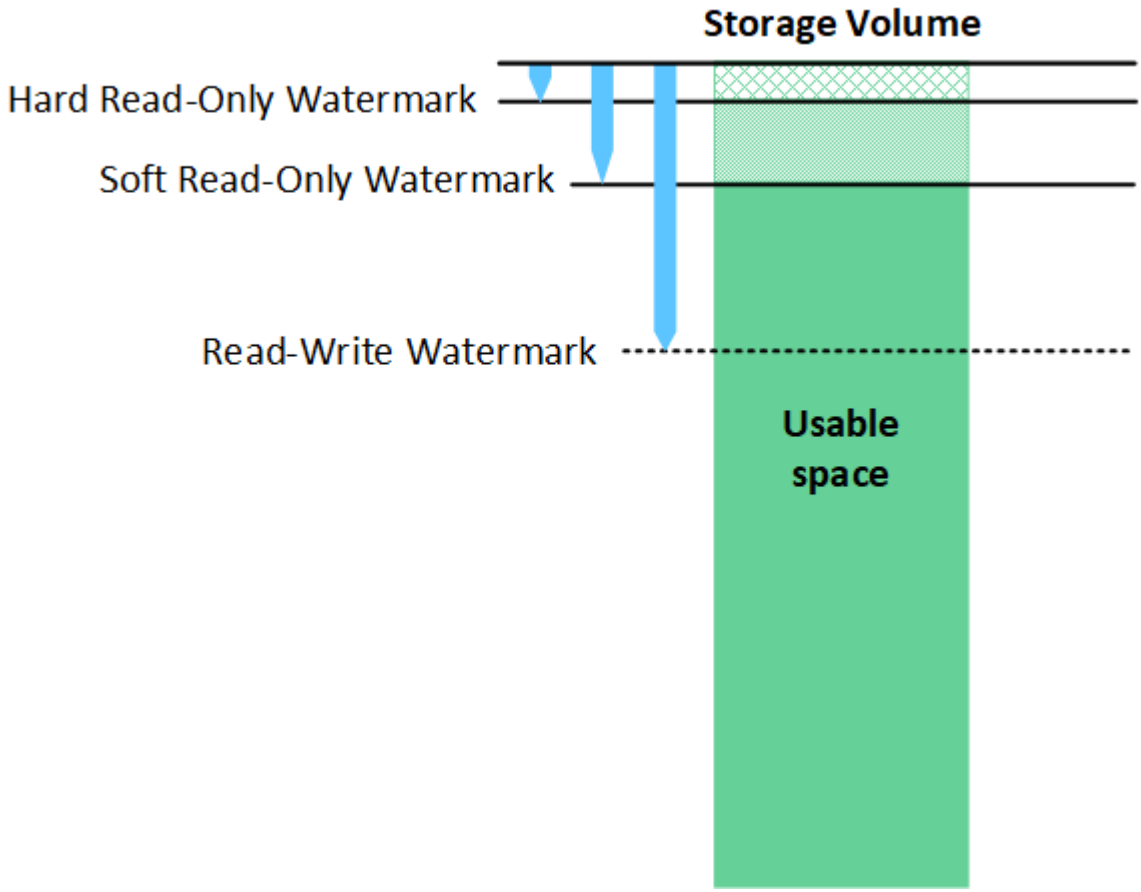
컨테이너와 세그먼트는 반드시 동일한 스토리지 노드에 저장될 필요는 없습니다. 컨테이너와 세그먼트는 ILM 규칙에 지정된 스토리지 풀 내의 모든 스토리지 노드에 저장될 수 있습니다.

각 세그먼트는 StorageGRID 시스템에서 독립적으로 처리되며 관리 객체 및 저장된 객체와 같은 속성 수에 반영됩니다. 예를 들어, StorageGRID 시스템에 저장된 객체가 두 개의 세그먼트로 분할되면 데이터 수집이 완료된 후 관리 객체 값은 다음과 같이 3만큼 증가합니다.

```
segment container + segment 1 + segment 2 = three stored objects
```

StorageGRID의 스토리지 볼륨 워터마크에 대해 알아보십시오

StorageGRID는 스토리지 노드의 공간이 심각하게 부족해지기 전에 안전하게 읽기 전용 상태로 전환하고, 읽기 전용 상태로 전환된 스토리지 노드가 다시 읽기/쓰기 가능 상태로 돌아갈 수 있도록 세 가지 스토리지 볼륨 워터마크를 사용합니다.



저장 볼륨 워터마크는 복제 및 소거 코딩된 객체 데이터에 사용되는 공간에만 적용됩니다. 볼륨 0의 객체 메타데이터에 예약된 공간에 대한 자세한 내용은 "객체 메타데이터 저장소 관리"을 참조하십시오.

소프트 읽기 전용 워터마크란 무엇인가요**?**

*storage volume soft read-only watermark*는 스토리지 노드의 객체 데이터 사용 가능 공간이 거의 다 찼음을 나타내는 첫 번째 워터마크입니다.

스토리지 노드의 각 볼륨에 남은 여유 공간이 해당 볼륨의 소프트 읽기 전용 워터마크보다 적으면 스토리지 노드는 읽기 전용 모드로 전환됩니다. 읽기 전용 모드란 스토리지 노드가 StorageGRID 시스템의 다른 부분에 읽기 전용 서비스를 제공한다고 알리지만, 보류 중인 모든 쓰기 요청은 처리하는 것을 의미합니다.

예를 들어, 스토리지 노드의 각 볼륨에 10GB의 소프트 읽기 전용 워터마크가 설정되어 있다고 가정해 보겠습니다. 각 볼륨의 사용 가능한 공간이 10GB 미만이 되면 스토리지 노드는 소프트 읽기 전용 모드로 전환됩니다.

하드 읽기 전용 워터마크란 무엇인가요**?**

*스토리지 볼륨 하드 읽기 전용 워터마크*는 노드의 객체 데이터 사용 가능 공간이 거의 다 되었음을 나타내는 다음 단계의 워터마크입니다.

볼륨의 여유 공간이 해당 볼륨의 하드 읽기 전용 워터마크보다 작으면 해당 볼륨에 대한 쓰기 작업이 실패합니다. 그러나 다른 볼륨에 대한 쓰기 작업은 해당 볼륨의 여유 공간이 하드 읽기 전용 워터마크보다 작아질 때까지 계속될 수 있습니다.

예를 들어, 스토리지 노드의 각 볼륨에 5GB의 읽기 전용 하드 워터마크가 설정되어 있다고 가정해 보겠습니다. 각 볼륨의 사용 가능한 공간이 5GB 미만이 되면 스토리지 노드는 더 이상 쓰기 요청을 수락하지 않습니다.

하드 읽기 전용 워터마크는 항상 소프트 읽기 전용 워터마크보다 크기가 작습니다.

읽기/쓰기 워터마크란 무엇인가요?

*스토리지 볼륨 읽기/쓰기 워터마크*는 읽기 전용 모드로 전환된 스토리지 노드에만 적용됩니다. 이는 노드가 다시 읽기/쓰기 모드로 전환될 수 있는 시점을 결정합니다. 스토리지 노드의 특정 스토리지 볼륨에 있는 여유 공간이 해당 볼륨의 읽기/쓰기 워터마크보다 커지면 노드는 자동으로 읽기/쓰기 상태로 전환됩니다.

예를 들어, 스토리지 노드가 읽기 전용 모드로 전환되었다고 가정해 보겠습니다. 또한 각 볼륨에 30GB의 읽기/쓰기 워터마크가 설정되어 있다고 가정합니다. 어떤 볼륨의 사용 가능한 공간이 30GB에 도달하는 즉시 노드는 다시 읽기/쓰기 모드로 전환됩니다.

읽기/쓰기 워터마크는 항상 소프트 읽기 전용 워터마크와 하드 읽기 전용 워터마크보다 큽니다.

스토리지 볼륨 워터마크 보기

현재 워터마크 설정과 시스템 최적화 값을 확인할 수 있습니다. 최적화된 워터마크를 사용하지 않는 경우, 설정을 조정할 수 있는지 또는 조정해야 하는지 판단할 수 있습니다.

시작하기 전에

- StorageGRID 11.6 이상으로 업그레이드를 완료했습니다.
- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한"

현재 워터마크 설정 보기

현재 저장소 워터마크 설정은 Grid Manager에서 확인할 수 있습니다.

단계

1. 지원 > 기타 > *저장소 워터마크*를 선택합니다.
2. 스토리지 워터마크 페이지에서 '최적화된 값 사용' 확인란을 확인하십시오.
   - 해당 확인란을 선택하면 스토리지 노드의 크기와 볼륨의 상대적 용량을 기준으로 모든 스토리지 노드의 모든 스토리지 볼륨에 대해 세 가지 워터마크가 모두 최적화됩니다.

     이는 기본 설정이며 권장 설정입니다. 이 값을 업데이트하지 마십시오. 필요에 따라 최적화된 스토리지 워터마크 보기할 수 있습니다.
   - '최적화된 값 사용' 확인란이 선택 해제된 경우, 사용자 지정(최적화되지 않은) 워터마크가 사용됩니다. 사용자 지정 워터마크 설정 사용은 권장되지 않습니다. 설정을 조정할 수 있는지 또는 조정해야 하는지 여부는 "낮은 읽기 전용 워터마크 재정의 알림 문제 해결"의 지침을 참조하십시오.

     사용자 지정 워터마크 설정을 지정할 때는 0보다 큰 값을 입력해야 합니다.

최적화된 스토리지 워터마크 보기

StorageGRID는 스토리지 볼륨의 소프트 읽기 전용 워터마크에 대해 계산된 최적화 값을 표시하기 위해 두 가지 Prometheus 메트릭을 사용합니다. 그리드의 각 스토리지 노드에 대한 최소 및 최대 최적화 값을 확인할 수 있습니다.

1. 지원 > 도구 > *측정항목*을 선택합니다.
2. Prometheus 섹션에서 링크를 선택하여 Prometheus 사용자 인터페이스에 액세스합니다.
3. 권장되는 최소 읽기 전용 워터마크를 확인하려면 다음 Prometheus 메트릭을 입력하고 *실행*을 선택하십시오.

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   마지막 열에는 각 스토리지 노드의 모든 스토리지 볼륨에 대한 소프트 읽기 전용 워터마크의 최소 최적화 값이 표시됩니다. 이 값이 스토리지 볼륨 소프트 읽기 전용 워터마크에 대한 사용자 지정 설정보다 크면 해당 스토리지 노드에 대해 **Low read-only watermark override** 경고가 트리거됩니다.

4. 권장되는 최대 소프트 읽기 전용 워터마크를 확인하려면 다음 Prometheus 메트릭을 입력하고 *실행*을 선택하십시오.

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   마지막 열은 각 스토리지 노드의 모든 스토리지 볼륨에 대해 최적화된 최대 소프트 읽기 전용 워터마크 값을 보여줍니다.

StorageGRID에서 객체 메타데이터 스토리지 관리

StorageGRID 시스템의 객체 메타데이터 용량은 해당 시스템에 저장할 수 있는 최대 객체 수를 결정합니다. StorageGRID 시스템에 새 객체를 저장할 충분한 공간이 있는지 확인하려면 StorageGRID가 객체 메타데이터를 저장하는 위치와 방법을 이해해야 합니다.

객체 메타데이터란 무엇입니까?

객체 메타데이터는 객체를 설명하는 모든 정보입니다. StorageGRID는 객체 메타데이터를 사용하여 그리드 전체의 모든 객체 위치를 추적하고 시간에 따라 각 객체의 수명 주기를 관리합니다.

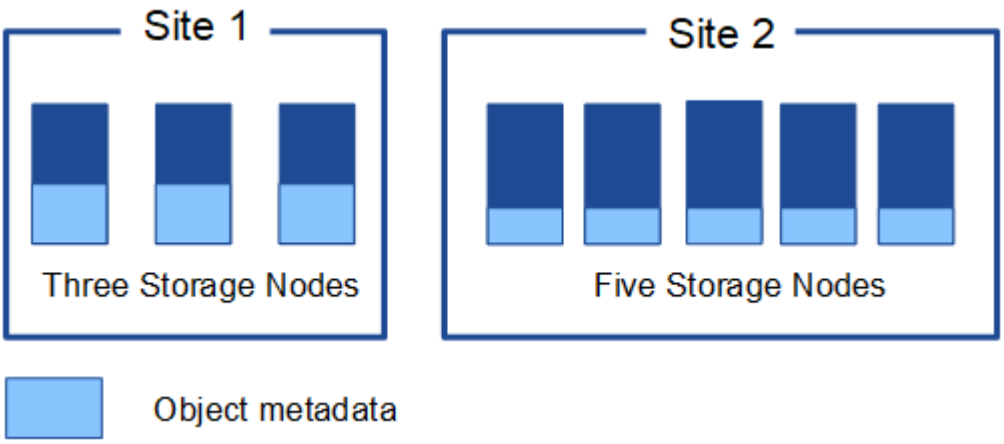
StorageGRID의 오브젝트 메타데이터에는 다음과 같은 유형의 정보가 포함됩니다.

- 시스템 메타데이터에는 각 객체의 고유 ID(UUID), 객체 이름, S3 버킷 이름, 테넌트 계정 이름 또는 ID, 객체의 논리적 크기, 객체가 처음 생성된 날짜 및 시간, 객체가 마지막으로 수정된 날짜 및 시간이 포함됩니다.
- 해당 객체와 연결된 모든 사용자 지정 메타데이터 키-값 쌍입니다.
- S3 객체의 경우, 해당 객체와 연결된 모든 객체 태그 키-값 쌍입니다.
- 복제된 객체 복사본의 경우, 각 복사본의 현재 저장 위치입니다.
- 삭제 코딩된 오브젝트 복사본의 경우, 각 조각의 현재 저장 위치입니다.
- 클라우드 스토리지 풀에 있는 객체 복사본의 경우, 외부 버킷 이름과 객체의 고유 식별자를 포함한 객체의 위치입니다.
- 분할된 객체 및 멀티파트 객체의 경우, 세그먼트 식별자 및 데이터 크기.

객체 메타데이터는 어떻게 저장되나요?

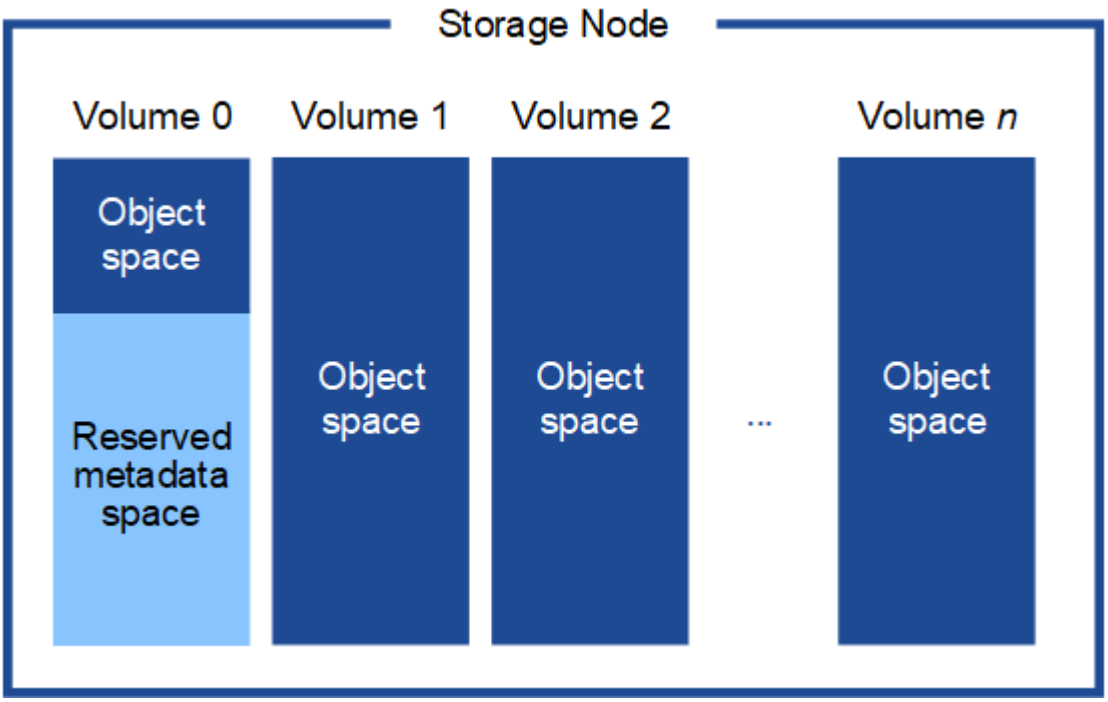
StorageGRID는 객체 메타데이터를 Cassandra 데이터베이스에 저장하며, 이 메타데이터는 객체 데이터와는 별도로 저장됩니다. 데이터 중복성을 확보하고 객체 메타데이터 손실을 방지하기 위해 StorageGRID는 시스템 내 모든 객체의 메타데이터 사본을 각 사이트에 세 개씩 저장합니다.

이 그림은 두 사이트의 스토리지 노드를 나타냅니다. 각 사이트는 동일한 양의 객체 메타데이터를 가지며, 각 사이트의 메타데이터는 해당 사이트의 모든 스토리지 노드에 분산되어 저장됩니다.



객체 메타데이터는 어디에 저장되나요?

이 그림은 단일 스토리지 노드의 스토리지 볼륨을 나타냅니다.



그림에서 보는 바와 같이, StorageGRID는 각 스토리지 노드의 스토리지 볼륨 0에 객체 메타데이터를 위한 공간을 예약합니다. 예약 공간은 객체 메타데이터를 저장하고 필수적인 데이터베이스 작업을 수행하는 데 사용됩니다. 스토리지 볼륨 0과 스토리지 노드의 다른 모든 스토리지 볼륨에 남아 있는 공간은 객체 데이터(복제본 및 소거 부호화된 조각) 저장에만 사용됩니다.

특정 스토리지 노드에서 객체 메타데이터를 위해 예약되는 공간의 크기는 아래에 설명된 여러 요인에 따라 달라집니다.

메타데이터 예약 공간 설정

_메타데이터 예약 공간_은 모든 스토리지 노드의 볼륨 0에 메타데이터를 위해 예약될 공간의 양을 나타내는 시스템 전체 설정입니다. 표에 표시된 것처럼 이 설정의 기본값은 다음을 기준으로 합니다.

- StorageGRID를 처음 설치할 때 사용한 소프트웨어 버전입니다.
- 각 스토리지 노드의 RAM 용량.

초기 **StorageGRID** 설치에 사용된 버전	스토리지 노드의 **RAM** 용량	기본 메타데이터 예약 공간 설정
11.5~12.0	그리드의 각 스토리지 노드에 128GB 이상	8TB(8,000GB)
	그리드 내 어떤 스토리지 노드에서도 128GB 미만	3TB(3,000GB)
11.1~11.4	사이트 내 각 스토리지 노드에 128GB 이상	4TB(4,000GB)
	각 사이트의 스토리지 노드당 128GB 미만	3TB(3,000GB)
11.0 또는 이전 버전	어떤 금액이든	2TB(2,000GB)

메타데이터 예약 공간 설정 보기

StorageGRID 시스템의 메타데이터 예약 공간 설정을 보려면 다음 단계를 따르십시오.

단계

1. * 구성 * > * 시스템 * > * 저장 설정 * 을 선택합니다.
2. 저장소 설정 페이지에서 메타데이터 예약 공간 섹션을 확장합니다.

StorageGRID 11.8 이상 버전의 경우 메타데이터 예약 공간 값은 최소 100GB, 최대 1PB여야 합니다.

각 스토리지 노드에 128GB 이상의 RAM이 있는 StorageGRID 11.6 이상의 새 설치에 대한 기본 설정은 8,000GB(8TB)입니다.

메타데이터의 실제 예약 공간

시스템 전체 메타데이터 예약 공간 설정과 달리, 객체 메타데이터의 _실제 예약 공간_은 각 스토리지 노드별로 결정됩니다. 특정 스토리지 노드의 경우, 메타데이터의 실제 예약 공간은 해당 노드의 볼륨 0 크기와 시스템 전체 메타데이터 예약 공간 설정에 따라 달라집니다.

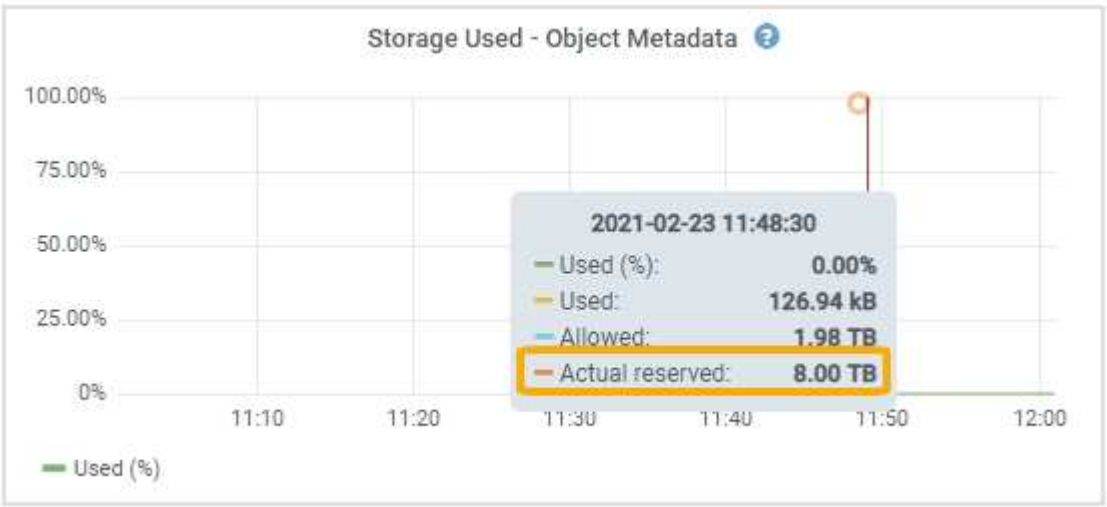
노드의 볼륨 **0** 크기	메타데이터의 실제 예약 공간
500GB 미만 (비프로덕션 용도)	볼륨 0의 10%
500 GB 이상 + 또는 + 메타데이터 전용 스토리지 노드	다음 값 중 더 작은 값: • 볼륨 0 • 메타데이터 예약 공간 설정 참고: 메타데이터 전용 스토리지 노드에는 rangedb가 하나만 필요합니다.

메타데이터의 실제 예약 공간 보기

특정 스토리지 노드에서 메타데이터에 대한 실제 예약 공간을 보려면 다음 단계를 따르십시오.

단계

1. 그리드 관리자에서 노드 > *_Storage Node_*를 선택합니다.
2. **Storage** 탭을 선택합니다.
3. Storage Used - Object Metadata 차트 위에 커서를 놓고 실제 예약된 값을 찾으세요.



스크린샷에서 실제 예약 값은 8TB입니다. 이 스크린샷은 새로운 StorageGRID 11.6 설치의 대형 스토리지 노드에 대한 것입니다. 시스템 전체 메타데이터 예약 공간 설정이 이 스토리지 노드의 볼륨 0보다 작기 때문에 이 노드의 실제 예약 공간은 메타데이터 예약 공간 설정과 같습니다.

실제 예약된 메타데이터 공간의 예시

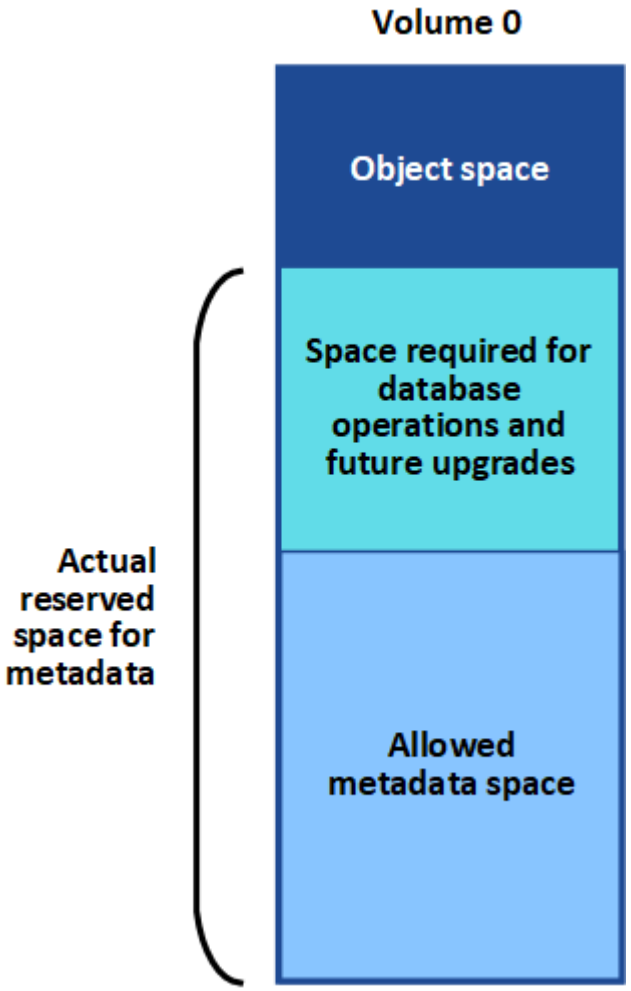
StorageGRID 버전 11.7 이상을 사용하여 새로운 StorageGRID 시스템을 설치한다고 가정해 보겠습니다. 이 예에서는 각 스토리지 노드에 128GB 이상의 RAM이 있고 스토리지 노드 1(SN1)의 볼륨 0이 6TB라고 가정합니다. 이러한 값을 기준으로 다음과 같은 결과를 얻습니다.

- 시스템 전체의 *메타데이터 예약 공간*은 8TB로 설정되어 있습니다. (이는 각 스토리지 노드에 128GB 이상의 RAM이 있는 경우 StorageGRID 11.6 이상 버전을 새로 설치할 때의 기본값입니다.)

- SN1의 메타데이터에 대해 실제로 예약된 공간은 6TB입니다. (볼륨 0이 메타데이터 예약 공간 설정보다 작기 때문에 전체 볼륨이 예약됩니다.)

허용된 메타데이터 공간

각 스토리지 노드의 메타데이터에 대한 실제 예약 공간은 객체 메타데이터에 사용 가능한 공간(허용된 메타데이터 공간)과 필수 데이터베이스 작업(압축 및 복구 등) 및 향후 하드웨어 및 소프트웨어 업그레이드에 필요한 공간으로 나뉩니다. 허용된 메타데이터 공간은 전체 객체 용량을 결정합니다.



다음 표는 StorageGRID가 노드의 메모리 용량과 메타데이터의 실제 예약 공간을 기반으로 다양한 스토리지 노드에 대해 *허용된 메타데이터 공간*을 계산하는 방법을 보여줍니다.

		Storage Node의 메모리 용량	
	< 128 GB	>= 128 GB	메타데이터의 실제 예약 공간

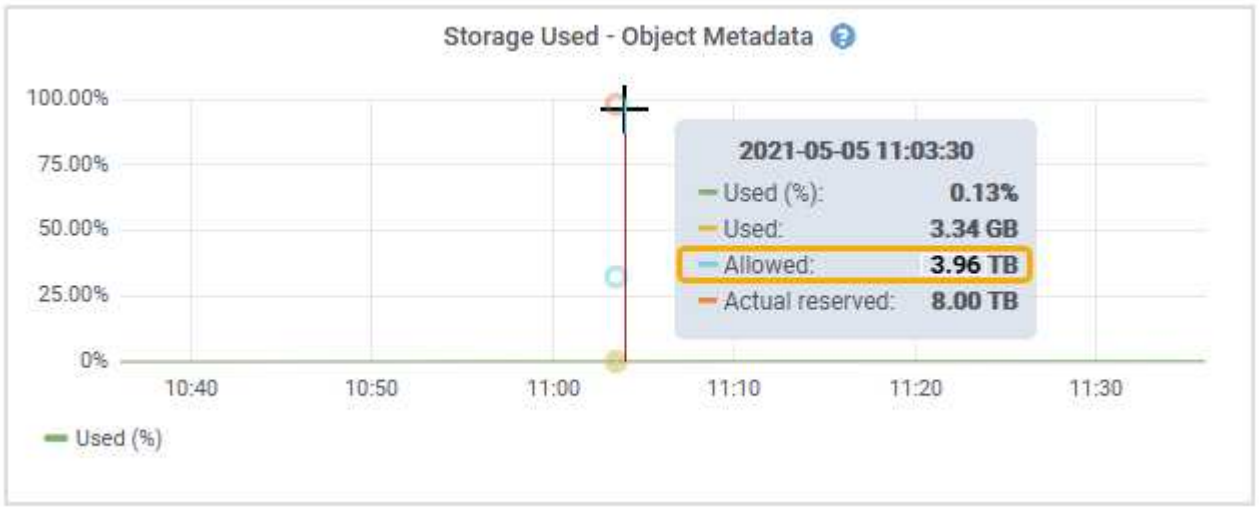
⇐ 4 TB	실제 예약 공간의 60%를 메타데이터에 사용하며, 최대 1.32TB까지 가능합니다.	실제 예약 공간의 60%를 메타데이터에 사용하며, 최대 1.98TB까지 사용 가능합니다.	4 TB

허용된 메타데이터 공간 보기

스토리지 노드에 허용된 메타데이터 공간을 확인하려면 다음 단계를 따르십시오.

단계

1. Grid Manager에서 * Nodes * 를 선택합니다.
2. 스토리지 노드를 선택하십시오.
3. **Storage** 탭을 선택합니다.
4. 저장 공간 사용량 - 객체 메타데이터 차트 위에 커서를 놓고 허용된 값을 찾습니다.



스크린샷에서 허용된 값은 3.96TB이며, 이는 메타데이터의 실제 예약 공간이 4TB를 초과하는 스토리지 노드의 최대값입니다.

허용된 값은 다음 Prometheus 메트릭에 해당합니다.

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

허용된 메타데이터 공간의 예

StorageGRID 버전 11.6을 사용하여 StorageGRID 시스템을 설치했다고 가정해 보겠습니다. 이 예에서는 각 스토리지 노드에 128GB 이상의 RAM이 있고 스토리지 노드 1(SN1)의 볼륨 0이 6TB라고 가정합니다. 이러한 값을 기반으로:

- 시스템 전체의 *메타데이터 예약 공간*은 8TB로 설정되어 있습니다. (이는 각 스토리지 노드에 128GB 이상의 RAM이 있는 경우 StorageGRID 11.6 이상 버전의 기본값입니다.)
- SN1의 메타데이터에 대해 실제로 예약된 공간은 6TB입니다. (볼륨 0이 메타데이터 예약 공간 설정보다 작기

때문에 전체 볼륨이 예약됩니다.)

- SN1의 메타데이터에 허용된 공간은 3TB이며, 이는 메타데이터에 허용된 공간에 대한 표에 표시된 계산식인 (메타데이터의 실제 예약 공간 – 1TB) × 60%를 기반으로 하며, 최대 3.96TB까지 허용됩니다.

크기가 다른 스토리지 노드가 객체 용량에 미치는 영향

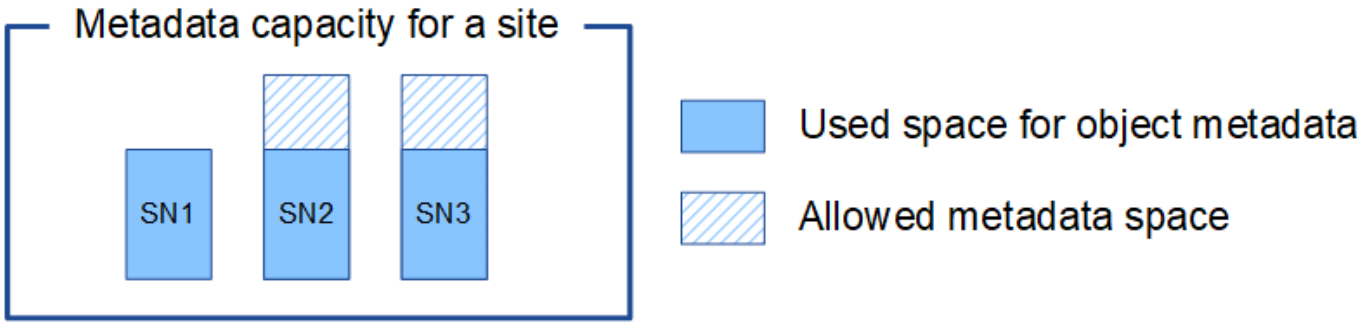
위에서 설명한 바와 같이 StorageGRID는 각 사이트의 스토리지 노드에 객체 메타데이터를 균등하게 분산합니다. 따라서 사이트에 크기가 다른 스토리지 노드가 있는 경우 해당 사이트에서 가장 작은 노드가 사이트의 메타데이터 용량을 결정합니다.

다음 예를 살펴보십시오.

- 서로 다른 크기의 스토리지 노드 3개가 포함된 단일 사이트 그리드가 있습니다.
- 메타데이터 예약 공간 설정은 4TB입니다.
- 스토리지 노드는 실제 예약된 메타데이터 공간과 허용된 메타데이터 공간에 대해 다음과 같은 값을 갖습니다.

스토리지 노드	볼륨 크기 **0**	실제 예약된 메타데이터 공간	허용된 메타데이터 공간
SN1	2.2 TB	2.2 TB	1.32 TB
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

객체 메타데이터는 사이트 내 스토리지 노드 전체에 균등하게 분산되므로, 이 예시에서 각 노드는 1.32TB의 메타데이터만 보유할 수 있습니다. SN2와 SN3에 허용된 추가 메타데이터 공간 0.66TB는 사용할 수 없습니다.



마찬가지로 StorageGRID는 각 사이트에서 StorageGRID 시스템의 모든 객체 메타데이터를 유지 관리하므로 StorageGRID 시스템의 전체 메타데이터 용량은 가장 작은 사이트의 객체 메타데이터 용량에 따라 결정됩니다.

객체 메타데이터 용량이 최대 객체 수를 제어하기 때문에, 한 노드의 메타데이터 용량이 부족해지면 그리드는 사실상 가득 차게 됩니다.

관련 정보

- 각 스토리지 노드의 객체 메타데이터 용량을 모니터링하는 방법을 알아보려면 "StorageGRID 모니터링"의 지침을 참조하십시오.
- 시스템의 오브젝트 메타데이터 용량을 늘리려면 새로운 Storage Node를 추가하여 "그리드를 확장합니다"하십시오.

StorageGRID에서 메타데이터 예약 공간 설정 증가

스토리지 노드가 특정 RAM 및 사용 가능 공간 요구 사항을 충족하는 경우 메타데이터 예약 공간 시스템 설정을 늘릴 수 있습니다.

필요한 것

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- 다음이 있습니다. "루트 액세스 권한 또는 기타 그리드 구성 권한"

이 작업 정보

시스템 전체 메타데이터 예약 공간 설정을 수동으로 최대 8TB까지 늘릴 수 있습니다.

시스템 전체 메타데이터 예약 공간 설정 값을 늘리려면 다음 두 가지 조건이 모두 충족되어야 합니다.

- 시스템 내 모든 사이트의 스토리지 노드에는 각각 128GB 이상의 RAM이 있습니다.
- 시스템의 모든 사이트에 있는 스토리지 노드는 스토리지 볼륨 0에 충분한 사용 가능한 공간을 확보하고 있습니다.

이 설정을 높이면 모든 스토리지 노드의 스토리지 볼륨 0에서 객체 스토리지에 사용할 수 있는 공간이 동시에 줄어든다는 점에 유의하십시오. 따라서 예상되는 객체 메타데이터 요구 사항에 따라 메타데이터 예약 공간을 8TB보다 작은 값으로 설정하는 것이 좋습니다.

> 일반적으로 낮은 값보다는 높은 값을 사용하는 것이 좋습니다. 메타데이터 예약 공간 설정이 너무 크면 나중에 줄일 수 있습니다. 반대로 나중에 값을 늘리면 시스템에서 공간을 확보하기 위해 객체 데이터를 이동해야 할 수도 있습니다.

메타데이터 예약 공간 설정이 특정 스토리지 노드의 객체 메타데이터 저장에 허용되는 공간에 미치는 영향에 대한 자세한 설명은 "객체 메타데이터 저장소 관리"을 참조하십시오.

단계

1. 현재 메타데이터 예약 공간 설정을 확인합니다.
   a. * 구성 * > * 시스템 * > * 저장 설정 * 을 선택합니다.
   b. 메타데이터 예약 공간 값을 확인하십시오.
2. 각 스토리지 노드의 스토리지 볼륨 0에 이 값을 늘릴 수 있는 충분한 여유 공간이 있는지 확인하십시오.
   a. *노드*를 선택합니다.
   b. 그리드에서 첫 번째 스토리지 노드를 선택합니다.
   c. 스토리지 탭을 선택합니다.
   d. 볼륨 섹션에서 **/var/local/rangedb/0** 항목을 찾으십시오.
   e. 사용 가능한 값이 사용하려는 새 값과 현재 메타데이터 예약 공간 값의 차이와 같거나 큰지 확인하십시오.

      예를 들어, 메타데이터 예약 공간 설정이 현재 4TB이고 이를 6TB로 늘리려면 사용 가능 값이 2TB 이상이어야 합니다.

   f. 모든 스토리지 노드에 대해 이 단계를 반복하십시오.
      - 하나 이상의 스토리지 노드에 사용 가능한 공간이 부족한 경우 메타데이터 예약 공간 값을 늘릴 수 없습니다. 이 절차를 계속 진행하지 마십시오.

- 각 스토리지 노드의 볼륨 0에 사용 가능한 공간이 충분하면 다음 단계로 진행하십시오.

3. 각 스토리지 노드에 최소 128GB의 RAM이 있는지 확인하십시오.
   a. *노드*를 선택합니다.
   b. 그리드에서 첫 번째 스토리지 노드를 선택합니다.
   c. 하드웨어 탭을 선택합니다.
   d. 메모리 사용량 차트에 마우스 커서를 올려놓으십시오. *총 메모리*가 128GB 이상인지 확인하십시오.
   e. 모든 스토리지 노드에 대해 이 단계를 반복하십시오.
      - 하나 이상의 스토리지 노드에 사용 가능한 총 메모리가 부족한 경우 메타데이터 예약 공간 값을 늘릴 수 없습니다. 이 절차를 계속 진행하지 마십시오.
      - 각 스토리지 노드의 총 메모리가 128GB 이상인 경우 다음 단계로 진행하십시오.
4. 메타데이터 예약 공간 설정을 업데이트합니다.
   a. * 구성 * > * 시스템 * > * 저장 설정 * 을 선택합니다.
   b. *메타데이터 예약 공간*을 선택합니다.
   c. 새 값을 입력합니다.

      예를 들어, 지원되는 최대값인 8TB를 입력하려면 **8000000000000** (8 뒤에 0이 12개 붙음)을 입력하십시오.

   d. *저장*을 선택하세요.

StorageGRID에 저장된 객체 압축

StorageGRID에 저장된 객체의 크기를 줄이기 위해 객체 압축을 활성화할 수 있으며, 이렇게 하면 객체가 차지하는 저장 공간이 줄어듭니다.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.

이 작업 정보

기본적으로 객체 압축은 비활성화되어 있습니다. 압축을 활성화하면 StorageGRID 객체를 저장할 때 무손실 압축을 사용하여 각 객체를 압축하려고 시도합니다.

> 이 설정을 변경하면 새 설정이 적용되는 데 약 1분이 소요됩니다. 구성된 값은 성능 및 확장성을 위해 캐시됩니다.

객체 압축을 활성화하기 전에 다음 사항에 유의하십시오.

- 저장하려는 데이터가 압축 가능한지 확실히 알지 못하는 한 저장된 객체 압축 옵션을 선택해서는 안 됩니다.
- StorageGRID에 객체를 저장하는 애플리케이션은 저장하기 전에 객체를 압축할 수 있습니다. 클라이언트 애플리케이션이 StorageGRID에 저장하기 전에 이미 객체를 압축한 경우, 이 옵션을 선택해도 객체 크기가 추가로 줄어들지는 않습니다.
- NetApp FabricPool을 StorageGRID와 함께 사용하는 경우 *저장된 객체 압축*을 선택하지 마십시오.

- 저장된 객체 압축 옵션을 선택한 경우, S3 클라이언트 애플리케이션은 반환할 바이트 범위를 지정하는 GetObject 작업을 수행하지 않아야 합니다. 이러한 "범위 읽기" 작업은 StorageGRID가 요청된 바이트에 접근하기 위해 객체를 사실상 압축 해제해야 하므로 비효율적입니다. GetObject 작업 중 매우 큰 객체에서 작은 바이트 범위를 요청하는 경우는 특히 비효율적입니다. 예를 들어, 50GB로 압축된 객체에서 10MB 범위를 읽는 것은 비효율적입니다.

  압축된 객체에서 범위를 읽어오는 경우 클라이언트 요청 시간이 초과될 수 있습니다.

  > 객체를 압축해야 하고 클라이언트 애플리케이션에서 범위 읽기를 사용해야 하는 경우 애플리케이션의 읽기 시간 제한을 늘리십시오.

단계

1. 구성 > 시스템 > 스토리지 설정 > *객체 압축*을 선택합니다.
2. 저장된 개체 압축 확인란을 선택하십시오.
3. *저장*을 선택하세요.

StorageGRID에서 전체 스토리지 노드 관리

스토리지 노드의 용량이 한계에 도달하면 새 스토리지를 추가하여 StorageGRID 시스템을 확장해야 합니다. 확장 방법에는 스토리지 볼륨 추가, 스토리지 확장 셸프 추가, 스토리지 노드 추가의 세 가지 옵션이 있습니다.

스토리지 볼륨 추가

각 스토리지 노드는 최대 스토리지 볼륨 수를 지원합니다. 정의된 최대 볼륨 수는 플랫폼에 따라 다릅니다. 스토리지 노드에 최대 스토리지 볼륨 수보다 적은 볼륨이 있는 경우 볼륨을 추가하여 용량을 늘릴 수 있습니다. "StorageGRID 시스템 확장"에 대한 지침을 참조하십시오.

스토리지 확장 선반 추가

StorageGRID SG6060 또는 SG6160과 같은 일부 StorageGRID 어플라이언스 스토리지 노드는 추가 스토리지 셸프를 지원할 수 있습니다. StorageGRID 확장 기능을 갖춘 StorageGRID 어플라이언스가 아직 최대 용량까지 확장되지 않은 경우 스토리지 셸프를 추가하여 용량을 늘릴 수 있습니다. 다음 지침을 참조하십시오. "StorageGRID 시스템 확장"

스토리지 노드 추가

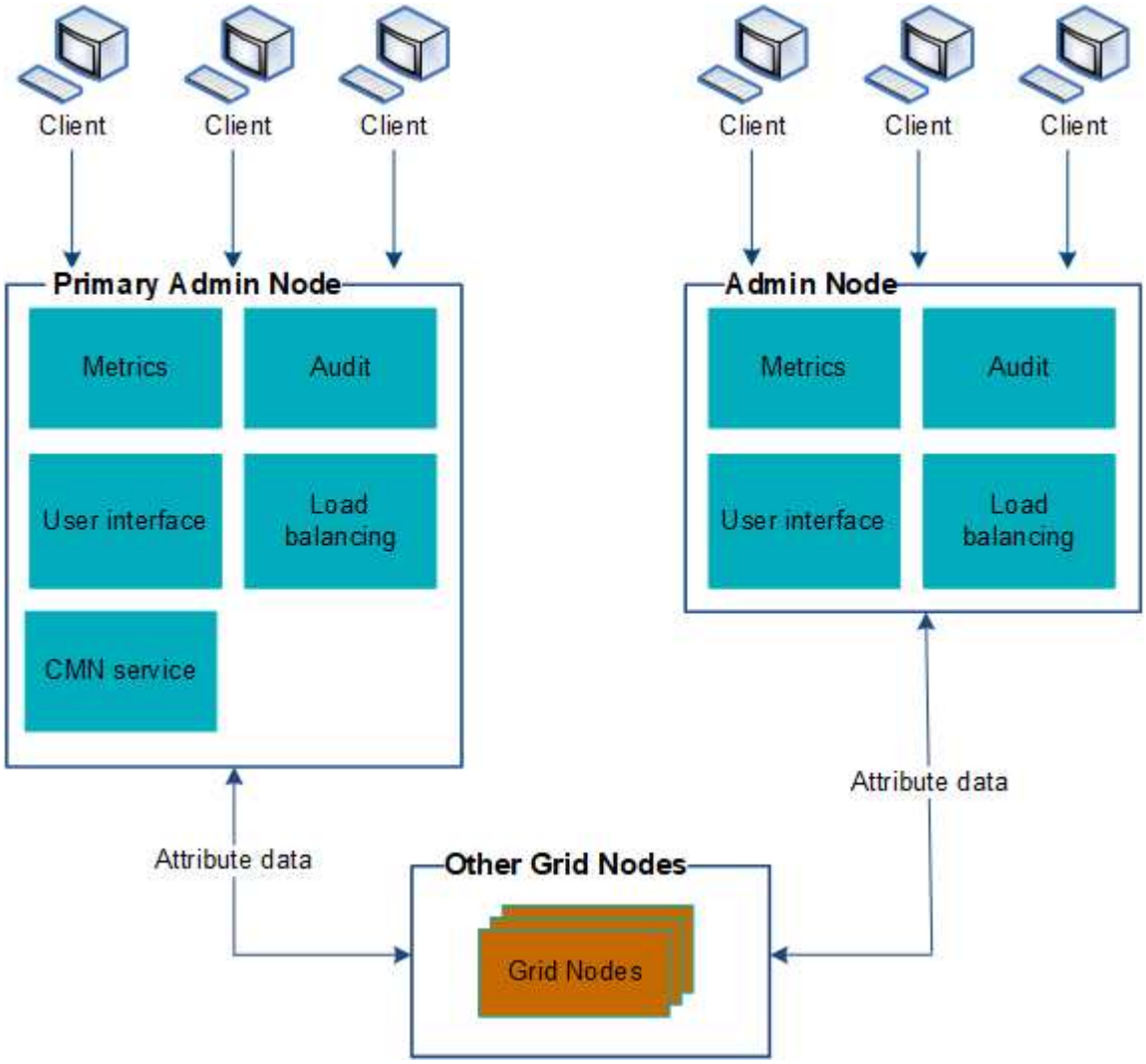
스토리지 노드를 추가하여 스토리지 용량을 늘릴 수 있습니다. 스토리지를 추가할 때는 현재 활성화된 ILM 규칙과 용량 요구 사항을 신중하게 고려해야 합니다. 자세한 내용은 "StorageGRID 시스템 확장" 지침을 참조하십시오.

관리자 노드 관리

StorageGRID에서 여러 관리 노드 사용

StorageGRID 시스템은 여러 개의 관리 노드를 포함할 수 있으므로 하나의 관리 노드에 장애가 발생하더라도 StorageGRID 시스템을 지속적으로 모니터링하고 구성할 수 있습니다.

관리자 노드를 사용할 수 없게 되더라도 속성 처리는 계속되고, 경고는 계속 발생하며, 이메일 알림 및 AutoSupport 패키지도 계속 전송됩니다. 하지만 여러 개의 관리자 노드를 사용하더라도 알림 및 AutoSupport 패키지를 제외하고는 장애 조치 보호 기능은 제공되지 않습니다.



StorageGRID 관리 노드에 장애가 발생할 경우 StorageGRID 시스템을 계속 보고 구성하는 방법은 두 가지가 있습니다.

- 웹 클라이언트는 사용 가능한 다른 관리 노드에 다시 연결할 수 있습니다.
- 시스템 관리자가 관리 노드의 고가용성 그룹을 구성한 경우 웹 클라이언트는 HA 그룹의 가상 IP 주소를 사용하여 Grid Manager 또는 테넌트 Manager에 계속 액세스할 수 있습니다. 을 참조하십시오. "고가용성 그룹 관리"

> HA 그룹을 사용하는 경우 활성 관리 노드에 장애가 발생하면 액세스가 중단됩니다. 사용자는 HA 그룹의 가상 IP 주소가 그룹 내 다른 관리 노드로 페일오버된 후 다시 로그인해야 합니다.

일부 유지 관리 작업은 기본 관리 노드를 통해서만 수행할 수 있습니다. 기본 관리 노드에 장애가 발생하면 StorageGRID 시스템이 완전히 복구되기 전에 해당 노드를 복구해야 합니다.

StorageGRID에서 기본 관리 노드 식별

기본 관리 노드는 비기본 관리 노드보다 더 많은 기능을 제공합니다. 예를 들어, 일부 유지 관리

절차는 기본 관리 노드를 사용하여 수행해야 합니다.

관리자 노드에 대한 자세한 내용은 "관리자 노드란 무엇인가요?"을 참조하십시오.

시작하기 전에

- 현재 Grid Manager에 "지원되는 웹 브라우저"을(를) 사용하여 로그인되어 있습니다.
- "특정 액세스 권한"이(가) 있습니다.

단계

1. *노드*를 선택합니다.
2. 검색 상자에 *primary*를 입력합니다.

   검색 결과에서 유형 열에 "Primary Admin Node"라고 표시된 노드를 찾으십시오. 기본 관리 노드가 하나만 표시되어야 합니다.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.