



StorageGRID 관리

StorageGRID software

NetApp
January 15, 2026

목차

StorageGRID 관리	1
StorageGRID 관리	1
참조하십시오	1
시작하기 전에	1
Grid Manager를 시작합니다	1
웹 브라우저 요구 사항	1
Grid Manager에 로그인합니다	2
Grid Manager에서 로그아웃합니다	3
암호를 변경합니다	4
StorageGRID 라이센스 정보를 봅니다	5
StorageGRID 라이센스 정보를 업데이트합니다	6
API를 사용합니다	6
StorageGRID에 대한 액세스를 제어합니다	27
StorageGRID 액세스를 제어합니다	27
프로비저닝 암호를 변경합니다	28
노드 콘솔 암호를 변경합니다	29
관리 노드의 SSH 액세스 암호를 변경합니다	31
ID 페더레이션을 사용합니다	33
관리 그룹을 관리합니다	38
관리자 그룹 권한	41
사용자 관리	44
SSO(Single Sign-On) 사용	47
그리드 페더레이션을 사용합니다	72
그리드 페더레이션은 무엇입니까?	72
계정 클론이란 무엇입니까?	75
교차 그리드 복제란 무엇입니까?	78
교차 그리드 복제와 CloudMirror 복제를 비교합니다	84
그리드 페더레이션 연결을 만듭니다	86
그리드 페더레이션 연결을 관리합니다	89
그리드 페더레이션을 위해 허용된 테넌트를 관리합니다	94
그리드 통합 오류 문제 해결	100
실패한 복제 작업을 식별하고 다시 시도하십시오	105
보안 관리	109
보안 관리	109
StorageGRID 암호화 방법을 검토합니다	109
인증서를 관리합니다	112
보안 설정을 구성합니다	142
키 관리 서버를 구성합니다	148
프록시 설정을 관리합니다	165

방화벽을 제어합니다	166
테넌트 관리	173
테넌트 계정이란 무엇입니까?	173
테넌트 계정을 생성합니다	174
테넌트 계정을 편집합니다	179
테넌트의 로컬 루트 사용자에 대한 암호를 변경합니다	181
테넌트 계정을 삭제합니다	182
플랫폼 서비스 관리	183
관리 S3 테넌트 계정에 대해 선택	192
클라이언트 연결을 구성합니다	193
S3 클라이언트 연결을 구성합니다	193
S3 클라이언트에 대한 보안	195
S3 설정 마법사를 사용합니다	197
HA 그룹 관리	206
로드 밸런싱 관리	216
S3 끝점 도메인 이름을 구성합니다	231
요약: 클라이언트 연결을 위한 IP 주소 및 포트	233
네트워크 및 연결을 관리합니다	235
네트워크 설정을 구성합니다	235
StorageGRID 네트워크 지침	235
IP 주소를 봅니다	236
VLAN 인터페이스를 구성합니다	238
관리 인터페이스에 StorageGRID CORS 활성화	241
트래픽 분류 정책을 관리합니다	242
발신 TLS 연결에 지원되는 암호	249
활성, 유휴 및 동시 HTTP 연결의 이점	250
링크 비용 관리	252
AutoSupport를 사용합니다	254
AutoSupport란 무엇입니까?	254
AutoSupport를 구성합니다	258
AutoSupport 패키지를 수동으로 트리거합니다	261
AutoSupport 패키지 문제 해결	262
StorageGRID를 통해 E-Series AutoSupport 패키지를 전송합니다	263
스토리지 노드 관리	267
스토리지 옵션을 사용합니다	267
오브젝트 메타데이터 스토리지 관리	270
메타데이터 예약 공간 증가 설정을 사용합니다	276
저장된 객체를 압축합니다	278
전체 스토리지 노드 관리	279
관리 노드 관리	279
여러 관리자 노드 사용	279

StorageGRID 관리

StorageGRID 관리

다음 지침에 따라 StorageGRID 시스템을 구성하고 관리합니다.

참조하십시오

StorageGRID 구성 및 관리를 위한 기본 작업을 통해 다음을 수행할 수 있습니다.

- 그리드 관리자를 사용하여 그룹 및 사용자를 설정합니다
- S3 클라이언트 애플리케이션이 오브젝트를 저장하고 검색할 수 있도록 테넌트 계정을 생성합니다
- StorageGRID 네트워크를 구성하고 관리합니다
- AutoSupport를 구성합니다
- 노드 설정을 관리합니다

시작하기 전에

- StorageGRID 시스템에 대해 전반적으로 이해하고 있습니다.
- Linux 명령 셸, 네트워킹 및 서버 하드웨어 설정 및 구성에 대한 매우 상세한 지식을 보유하고 있습니다.

Grid Manager를 시작합니다

웹 브라우저 요구 사항

지원되는 웹 브라우저를 사용해야 합니다.

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

브라우저 창을 권장 너비로 설정하세요.

브라우저 폭	픽셀
최소	1024
최적	1280

Grid Manager에 로그인합니다

지원되는 웹 브라우저의 주소 표시줄에 FQDN(정규화된 도메인 이름) 또는 관리 노드의 IP 주소를 입력하여 Grid Manager 로그인 페이지에 액세스합니다.

각 StorageGRID 시스템에는 1개의 기본 관리 노드와 1차 관리자가 아닌 노드 수가 포함되어 있습니다. 관리자 노드의 그리드 관리자에 로그인하여 StorageGRID 시스템을 관리할 수 있습니다. 그러나 일부 유지 보수 절차는 기본 관리자 노드에서만 수행할 수 있습니다.

HA 그룹에 연결합니다

HA(고가용성) 그룹에 관리 노드가 포함된 경우 HA 그룹의 가상 IP 주소 또는 가상 IP 주소에 매핑되는 정규화된 도메인 이름을 사용하여 연결합니다. 기본 관리 노드를 그룹의 기본 인터페이스로 선택해야 그리드 관리자에 액세스할 때 기본 관리 노드를 사용할 수 없는 경우를 제외하고 기본 관리 노드에서 액세스할 수 있습니다. 을 "[고가용성 그룹을 관리합니다](#)" 참조하십시오.

SSO를 사용합니다

로그인 단계는 다음과 같이 약간 다릅니다. "[SSO\(Single Sign-On\)가 구성되었습니다](#)" .

첫 번째 관리 노드에서 그리드 관리자에 로그인합니다

시작하기 전에

- 로그인 자격 증명이 있습니다.
- 을 사용하고 "[지원되는 웹 브라우저](#)"입니다.
- 쿠키는 웹 브라우저에서 활성화됩니다.
- 하나 이상의 권한이 있는 사용자 그룹에 속해 있습니다.
- Grid Manager에 대한 URL이 있습니다.

`https://FQDN_or_Admin_Node_IP/`

정규화된 도메인 이름, 관리 노드의 IP 주소 또는 관리 노드의 HA 그룹의 가상 IP 주소를 사용할 수 있습니다.

HTTPS의 기본 포트(443)가 아닌 포트에서 Grid Manager에 액세스하려면 URL에 포트 번호를 포함시킵니다.

`https://FQDN_or_Admin_Node_IP:port/`



SSO는 제한된 Grid Manager 포트에서 사용할 수 없습니다. 포트 443을 사용해야 합니다.

단계

- 지원되는 웹 브라우저를 실행합니다.
- 브라우저의 주소 표시줄에 Grid Manager의 URL을 입력합니다.
- 보안 경고 메시지가 나타나면 브라우저의 설치 마법사를 사용하여 인증서를 설치합니다. 을 "[보안 인증서를 관리합니다](#)" 참조하십시오.
- Grid Manager에 로그인합니다.

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

SSO를 사용하지 않습니다

- a. Grid Manager의 사용자 이름과 암호를 입력합니다.
- b. 로그인 * 을 선택합니다.

SSO 사용

- StorageGRID가 SSO를 사용하고 있고 이 브라우저에서 URL에 처음 액세스한 경우:

- i. 로그인 * 을 선택합니다. 계정 필드에 0을 그대로 둘 수 있습니다.
- ii. 조직의 SSO 로그인 페이지에 표준 SSO 자격 증명을 입력합니다.

예를 들어, StorageGRID 가 SSO를 사용하고 이전에 Grid Manager 또는 테넌트 계정에 액세스한 적이 있는 경우:

- A. 최신 계정 목록에 * 0 * (Grid Manager의 계정 ID)을 입력하거나 * Grid Manager * 를 선택합니다.
- B. 로그인 * 을 선택합니다.
- C. 조직의 SSO 로그인 페이지에서 표준 SSO 자격 증명을 사용하여 로그인합니다.

로그인하면 대시보드가 포함된 그리드 관리자의 홈 페이지가 나타납니다. 제공되는 정보에 대한 자세한 내용은 [을 참조하십시오"대시보드를 보고 관리합니다".](#)

다른 관리자 노드에 로그인합니다

다음 단계에 따라 다른 관리자 노드에 로그인합니다.

SSO를 사용하지 않습니다

단계

1. 브라우저의 주소 표시줄에 다른 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력합니다. 필요에 따라 포트 번호를 포함시킵니다.
2. Grid Manager의 사용자 이름과 암호를 입력합니다.
3. 로그인 * 을 선택합니다.

SSO 사용

StorageGRID가 SSO를 사용하고 있고 하나의 관리 노드에 로그인한 경우 다시 로그인하지 않고도 다른 관리 노드에 액세스할 수 있습니다.

단계

1. 브라우저의 주소 표시줄에 다른 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력합니다.
2. SSO 세션이 만료된 경우 자격 증명을 다시 입력하십시오.

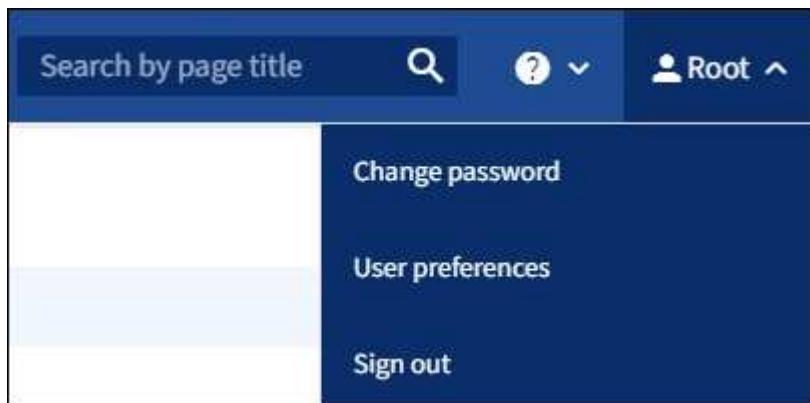
Grid Manager에서 로그아웃합니다

그리드 관리자 작업을 마치면 로그아웃하여 권한이 없는 사용자가 StorageGRID 시스템에

액세스할 수 없도록 해야 합니다. 브라우저를 닫아도 브라우저 쿠키 설정에 따라 시스템에서 로그아웃되지 않을 수 있습니다.

단계

1. 오른쪽 위 모서리에서 사용자 이름을 선택합니다.



2. 로그아웃 * 을 선택합니다.

옵션을 선택합니다	설명
SSO가 사용되지 않습니다	<p>관리자 노드에서 로그아웃되었습니다.</p> <p>그리드 관리자 로그인 페이지가 표시됩니다.</p> <ul style="list-style-type: none">참고: * 둘 이상의 관리자 노드에 로그인한 경우 각 노드에서 로그아웃해야 합니다.
SSO가 활성화되었습니다	<p>액세스 중인 모든 관리 노드에서 로그아웃되었습니다. StorageGRID 로그인 페이지가 표시됩니다. * 그리드 관리자 * 는 * 최근 계정 * 드롭다운에 기본값으로 나열되고 * 계정 ID * 필드는 0으로 표시됩니다.</p> <p>참고: SSO가 활성화되어 있고 테넌트 관리자에도 로그인한 경우 다음도 수행해야 합니다. "테넌트 계정에서 로그아웃합니다" 에게 "SSO에서 로그아웃합니다".</p>

암호를 변경합니다

Grid Manager의 로컬 사용자인 경우 사용자 고유의 암호를 변경할 수 있습니다.

시작하기 전에

을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"

이 작업에 대해

통합 사용자로 StorageGRID에 로그인하거나 SSO(Single Sign-On)가 활성화된 경우 그리드 관리자에서 암호를 변경할 수 없습니다. 대신 Active Directory 또는 OpenLDAP와 같은 외부 ID 소스에서 암호를 변경해야 합니다.

단계

1. Grid Manager 헤더에서 *사용자 이름* > *암호 변경* 을 선택합니다.
2. 현재 암호를 입력합니다.
3. 새 암호를 입력합니다.

암호는 8자 이상 32자 이하여야 합니다. 암호는 대/소문자를 구분합니다.

4. 새 암호를 다시 입력합니다.
5. 저장 * 을 선택합니다.

StorageGRID 라이센스 정보를 봅니다

필요한 경우 그리드의 최대 스토리지 용량과 같은 StorageGRID 시스템에 대한 라이센스 정보를 볼 수 있습니다.

시작하기 전에

을 사용하여 그리드 관리자에 로그인되어 있습니다.["지원되는 웹 브라우저"](#)

이 작업에 대해

이 StorageGRID 시스템의 소프트웨어 라이센스에 문제가 있는 경우 대시보드의 상태 카드에 라이센스 상태 아이콘과 * 라이센스 * 링크가 포함됩니다. 이 숫자는 라이센스 관련 문제의 수를 나타냅니다.



단계

1. 다음 중 하나를 수행하여 라이센스 페이지에 액세스합니다.
 - ° 유지관리 > 시스템 > *라이선스*를 선택하세요.
 - ° 대시보드의 상태 카드에서 라이센스 상태 아이콘 또는 * 라이센스 * 링크를 선택합니다.

이 링크는 라이센스에 문제가 있는 경우에만 나타납니다.
2. 현재 라이센스에 대한 읽기 전용 세부 정보 보기:
 - ° StorageGRID 시스템 ID로, 이 StorageGRID 설치의 고유 식별 번호입니다
 - ° 라이센스 일련 번호입니다

- 라이센스 유형, * 영구 * 또는 * 가입 *
- 그리드의 라이센스가 부여된 스토리지 용량입니다
- 지원되는 스토리지 용량입니다
- 라이선스 종료 날짜. 영구 라이센스에 대해 * 해당 없음 * 이 나타납니다.
- 지원 종료 날짜입니다

이 날짜는 현재 라이센스 파일에서 읽으며 라이센스 파일을 얻은 후 지원 서비스 계약을 연장하거나 갱신한 경우 최신 날짜가 아닐 수 있습니다. 이 값을 업데이트하려면 [을 참조하십시오 "StorageGRID 라이센스 정보를 업데이트합니다"](#). Active IQ를 사용하여 실제 계약 종료 날짜를 볼 수도 있습니다.

- 라이센스 텍스트 파일의 내용입니다

StorageGRID 라이센스 정보를 업데이트합니다

라이센스 조건이 변경될 때마다 StorageGRID 시스템의 라이센스 정보를 업데이트해야 합니다. 예를 들어 그리드에 대한 추가 스토리지 용량을 구입한 경우 라이센스 정보를 업데이트해야 합니다.

시작하기 전에

- StorageGRID 시스템에 적용할 새 라이센스 파일이 있습니다.
- 있습니다. ["특정 액세스 권한"](#)
- 프로비저닝 암호가 있습니다.

단계

1. 유지관리 > 시스템 > *라이선스*를 선택하세요.
 2. 라이센스 업데이트 섹션에서 * 찾아보기 * 를 선택합니다.
 3. 새 라이센스 파일을 찾아 (`txt`선택합니다).
- 새 라이센스 파일의 유효성을 검사한 후 표시합니다.
4. 프로비저닝 암호를 입력합니다.
 5. 저장 * 을 선택합니다.

API를 사용합니다

Grid Management API를 사용합니다

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

최고 수준의 리소스

Grid Management API는 다음과 같은 최상위 리소스를 제공합니다.

- /grid: 액세스가 Grid Manager 사용자로 제한되며 구성된 그룹 권한을 기반으로 합니다.
- /org: 테넌트 계정에 대한 로컬 또는 페더레이션 LDAP 그룹에 속한 사용자로 액세스가 제한됩니다. 자세한 내용은을 참조하십시오 ["테넌트 계정을 사용합니다"](#).
- /private: 액세스가 Grid Manager 사용자로 제한되며 구성된 그룹 권한을 기반으로 합니다. 사설 API는 사전 통보 없이 변경될 수 있습니다. StorageGRID 전용 엔드포인트도 요청의 API 버전을 무시합니다.

API 요청을 발행합니다

Grid Management API는 Swagger 오픈 소스 API 플랫폼을 사용합니다. Swagger는 개발자와 개발자가 아닌 사용자가 API를 사용하여 StorageGRID에서 실시간 작업을 수행할 수 있도록 직관적인 사용자 인터페이스를 제공합니다.

Swagger 사용자 인터페이스는 각 API 작동에 대한 전체 세부 정보와 문서를 제공합니다.

시작하기 전에

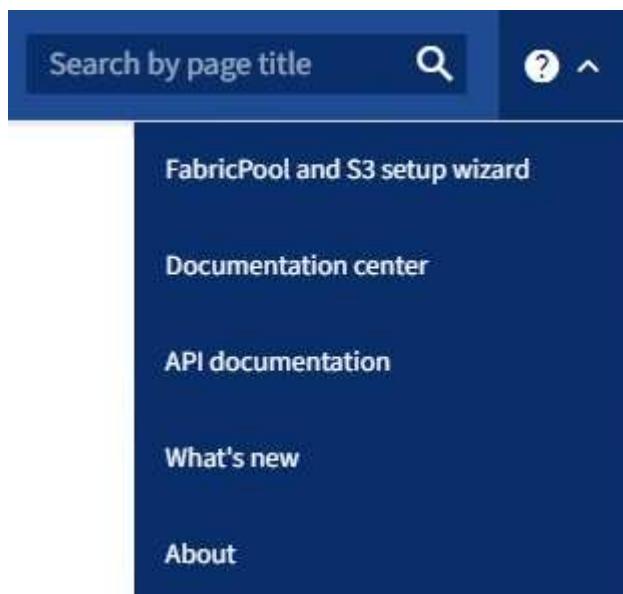
- 을 사용하여 그리드 관리자에 로그인되어 있습니다. ["지원되는 웹 브라우저"](#)
- 있습니다. ["특정 액세스 권한"](#)



API 문서 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

단계

1. Grid Manager 헤더에서 도움말 아이콘을 선택하고 * API documentation * 을 선택합니다.



2. 전용 API로 작업을 수행하려면 StorageGRID 관리 API 페이지에서 * 전용 API 설명서 * 로 이동 * 을 선택합니다.

사설 API는 사전 통보 없이 변경될 수 있습니다. StorageGRID 전용 엔드포인트도 요청의 API 버전을 무시합니다.

3. 원하는 작업을 선택합니다.

API 작업을 확장하면 가져오기, 가져오기, 업데이트 및 삭제와 같은 사용 가능한 HTTP 작업을 볼 수 있습니다.

4. 끝점 URL, 필수 또는 선택적 매개 변수 목록, 요청 본문(필요한 경우) 예제 및 가능한 응답을 비롯한 요청 세부 정보를 보려면 HTTP 작업을 선택합니다.

groups Operations on groups

GET /grid/groups Lists Grid Administrator Groups

Parameters

Name	Description
type string (query)	filter by group type <i>Available values : local, federated</i>
limit integer (query)	maximum number of results <i>Default value : 25</i>
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker) <i>Available values : asc, desc</i>

Responses

Response content type: application/json

Code	Description
200	successfully retrieved

Example Value: Model

```
{
  "responseTime": "2021-03-29T14:22:19.673Z",
  "status": "success",
  "apiVersion": "3.3",
  "deprecated": false,
  "data": [
    {
      "displayName": "Developers"
    }
  ]
}
```

5. 요청에 그룹 또는 사용자 ID와 같은 추가 매개 변수가 필요한지 확인합니다. 그런 다음 이 값을 구합니다. 필요한 정보를 얻기 위해 먼저 다른 API 요청을 발급해야 할 수도 있습니다.
6. 예제 요청 본문을 수정해야 하는지 확인합니다. 이 경우 * Model * 을 선택하여 각 필드의 요구 사항을 확인할 수 있습니다.
7. 체험하기 * 를 선택합니다.
8. 필요한 매개 변수를 제공하거나 요청 본문을 필요에 따라 수정합니다.
9. Execute * 를 선택합니다.

10. 응답 코드를 검토하여 요청이 성공했는지 확인합니다.

Grid Management API 작업

Grid Management API는 사용 가능한 작업을 다음 섹션으로 구성합니다.



이 목록에는 공용 API에서 사용할 수 있는 작업만 포함됩니다.

- * ACCOUNT *: 새 계정 생성 및 지정된 계정의 스토리지 사용량 검색을 포함하여 스토리지 테넌트 계정을 관리하는 작업입니다.
- * alert-history *: 해결된 알림의 작업.
- 알림 메시지 수신자 *: 경고 알림 수신자(이메일)에 대한 작업.
- * alert-rules *: 경고 규칙에 대한 작업.
- * alert-silences *: 경고 작동 중.
- * 경고 *: 경고 작업.
- * 감사 *: 감사 구성을 나열하고 업데이트하는 작업.
- * auth *: 사용자 세션 인증을 수행하기 위한 작업.

Grid Management API는 Bearer Token Authentication Scheme을 지원한다. 로그인하려면 인증 요청의 JSON 본문에 사용자 이름과 암호를 입력합니다(즉, POST /api/v3/authorize). 사용자가 성공적으로 인증되면 보안 토큰이 반환됩니다. 이 토큰은 후속 API 요청 헤더("Authorization:Bearer_token_")에 제공되어야 합니다. 토큰은 16시간 후에 만료됩니다.



StorageGRID 시스템에 대해 Single Sign-On이 활성화된 경우 인증을 위해 다른 단계를 수행해야 합니다. "SSO(Single Sign-On)가 활성화된 경우 API에 로그인 인증"을 참조하십시오.

인증 보안 강화에 대한 자세한 내용은 "사이트 간 요청 위조로부터 보호"를 참조하십시오.

- * 클라이언트-인증서 *: 외부 모니터링 도구를 사용하여 StorageGRID에 안전하게 액세스할 수 있도록 클라이언트 인증서를 구성하는 작업
- * config *: 그리드 관리 API 제품 릴리스 및 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 Grid Management API의 주요 버전을 나열할 수 있으며 더 이상 사용되지 않는 API 버전을 사용하지 않도록 설정할 수 있습니다.
- * 비활성화됨 - 기능 *: 비활성화된 기능을 보기 위한 작업.
- * DNS-서버 *: 구성된 외부 DNS 서버를 나열하고 변경하는 작업.
- * 드라이브 세부 정보 *: 특정 스토리지 어플라이언스 모델을 위한 드라이브 작업.
- * endpoint-domain-names *: S3 끝점 도메인 이름을 나열하고 변경하는 작업.
- * 삭제 코딩 * : 삭제 코딩 프로필에 대한 작업.
- * 확장 *: 확장 작업(절차 수준).
- * 확장 노드 *: 확장 시 작업(노드 레벨).
- * 확장 사이트 *: 확장 시 운영(사이트 레벨)
- * GRID-NETWORKS *: 그리드 네트워크 목록을 나열하고 변경하는 작업.

- * GRID-Passwords *: 그리드 암호 관리 작업.
- * 그룹 *: 로컬 그리드 관리자 그룹을 관리하고 외부 LDAP 서버에서 통합 그리드 관리자 그룹을 검색하는 작업.
- * identity-source *: 외부 ID 소스를 구성하고 통합 그룹 및 사용자 정보를 수동으로 동기화하는 작업
- * ILM *: 정보 수명 주기 관리(ILM)의 운영
- **In-progress-procedures**: 현재 진행 중인 유지보수 절차를 검색합니다.
- 라이센스 *: StorageGRID 라이센스를 검색하고 업데이트하는 작업.
- **logs**: 로그 파일을 수집하고 다운로드하는 작업입니다
- * 메트릭 *: 일정 기간 동안 단일 시점 및 범위 메트릭 쿼리의 인스턴스 메트릭 쿼리를 비롯한 StorageGRID 메트릭의 작업 Grid Management API는 Prometheus 시스템 모니터링 도구를 백엔드 데이터 소스로 사용합니다. Prometheus 쿼리 구성에 대한 자세한 내용은 Prometheus 웹 사이트를 참조하십시오.



이름에 포함된 메트릭은 *private* 내부용으로만 사용할 수 있습니다. 이러한 메트릭은 사전 통지 없이 StorageGRID 릴리스 간에 변경될 수 있습니다.

- * 노드 세부 정보 *: 노드 세부 정보에 대한 작업.
- * 노드 상태 *: 노드 상태에 대한 작업
- * 노드-스토리지-상태 *: 노드 스토리지 상태의 작업.
- * NTP-서버 *: 외부 NTP(Network Time Protocol) 서버를 나열하거나 업데이트하는 작업.
- * 오브젝트 *: 오브젝트 및 오브젝트 메타데이터의 작동
- * 복구 *: 복구 절차를 위한 작업.
- 복구 패키지: 복구 패키지를 다운로드하는 작업입니다.
- * 지역 *: 영역을 보고 만드는 작업.
- * S3 오브젝트 잠금 *: 글로벌 S3 오브젝트 잠금 설정 시 작업.
- * server-certificate *: Grid Manager 서버 인증서를 보고 업데이트하는 작업.
- * SNMP *: 현재 SNMP 구성에 대한 작업.
- * 스토리지 - 워터마크 *: 스토리지 노드 워터마크입니다.
- * traffic-classes *: 트래픽 분류 정책을 위한 운영.
- * 신뢰할 수 없는 클라이언트-네트워크 *: 신뢰할 수 없는 클라이언트 네트워크 구성에서의 작업.
- * 사용자 *: 그리드 관리자 사용자를 보고 관리하는 작업.

Grid Management API 버전 관리

Grid Management API는 버전 관리를 사용하여 무중단 업그레이드를 지원합니다.

예를 들어, 이 요청 URL은 API 버전 4를 지정합니다.

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

이전 버전과 호환되지 않는 변경 사항이 발생하면 API의 주 버전이 범핑됩니다. API의 부 버전은 이전 버전과 _호환_ 을(를) 변경할 때 범핑됩니다. 호환 가능한 변경 사항에는 새 끝점 또는 새 속성 추가가 포함됩니다.

다음 예제에서는 변경 유형에 따라 API 버전을 충돌하는 방법을 보여 줍니다.

API 변경 유형입니다	이전 버전	새 버전
이전 버전과 호환 가능합니다	2.1	2.2
이전 버전과 호환되지 않습니다	2.1	3.0

StorageGRID 소프트웨어를 처음 설치하면 최신 버전의 API만 활성화됩니다. 그러나 StorageGRID의 새 기능 릴리즈로 업그레이드하면 하나 이상의 StorageGRID 기능 릴리즈에 대한 이전 API 버전에 계속 액세스할 수 있습니다.



지원되는 버전을 구성할 수 있습니다. 자세한 내용은 Swagger API 설명서의 * config * 섹션을 참조하십시오 "[Grid Management API를 참조하십시오](#)". 최신 버전을 사용하려면 모든 API 클라이언트를 업데이트한 후 이전 버전에 대한 지원을 비활성화해야 합니다.

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

- 응답 헤더가 "DEPRECATED:TRUE"입니다.
- JSON 응답 본문에는 "DEPRECATED"가 포함됩니다. TRUE
- 더 이상 사용되지 않는 경고가 NMS.log에 추가됩니다. 예를 들면 다음과 같습니다.

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

현재 릴리즈에서 지원되는 API 버전을 확인합니다

API 요청을 사용하여 GET /versions 지원되는 API 주요 버전 목록을 반환합니다. 이 요청은 Swagger API 설명서의 * config * 섹션에 있습니다.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

요청에 대한 API 버전을 지정합니다

경로 매개 변수(/api/v4) 또는 헤더를 사용하여 API 버전을 지정할 수 ('Api-Version: 4'입니다. 두 값을 모두 제공하면 헤더 값이 경로 값을 재정의합니다).

```
curl https://[IP-Address]/api/v4/grid/accounts  
curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

사이트 간 요청 위조(CSRF)로부터 보호

CSRF 토큰을 사용하여 쿠키를 사용하는 인증을 강화하면 StorageGRID에 대한 CSRF(사이트 간 요청 위조) 공격으로부터 보호할 수 있습니다. Grid Manager 및 Tenant Manager는 이 보안 기능을 자동으로 활성화합니다. 다른 API 클라이언트는 로그인할 때 활성화 여부를 선택할 수 있습니다.

HTTP 양식 POST와 같이 다른 사이트에 대한 요청을 트리거할 수 있는 공격자는 로그인한 사용자의 쿠키를 사용하여 특정 요청을 만들 수 있습니다.

StorageGRID는 CSRF 토큰을 사용하여 CSRF 공격으로부터 보호합니다. 활성화된 경우 특정 쿠키의 내용은 특정 헤더 또는 특정 POST 본문 매개 변수의 내용과 일치해야 합니다.

이 기능을 활성화하려면 csrfToken 인증 중에 매개 변수를 true 설정합니다. 기본값은 입니다 false.

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

true 인 경우, GridCsrfToken 쿠키는 Grid Manager 로그인에 대한 임의 값으로 설정되고 AccountCsrfToken 쿠키는 Tenant Manager에 로그인하기 위한 임의 값으로 설정됩니다.

쿠키가 있는 경우 시스템 상태(POST, PUT, 패치, 삭제)를 수정할 수 있는 모든 요청에 다음 중 하나가 포함되어야 합니다.

- `X-Csrf-Token` 헤더 값이 CSRF 토큰 쿠키의 값으로 설정된 헤더입니다.
- 폼으로 인코딩된 본문을 수락하는 끝점의 경우: csrfToken 폼으로 인코딩된 요청 본문 매개 변수입니다.

추가 예제 및 세부 정보는 온라인 API 설명서를 참조하십시오.



CSRF 토큰 쿠키 세트가 있는 요청은 CSRF 공격에 대한 추가 보호로서 JSON 요청 본문을 기대하는 모든 요청에 대해 "Content-Type: application/json" 헤더를 적용합니다.

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

SSO(Single Sign-On)가 활성화된 경우 **API** 사용(**Active Directory**)

만약 당신이 가지고 있다면 "**SSO(Single Sign-On) 구성 및 활성화**" SSO 공급자로 Active

Directory를 사용하는 경우 Grid Management API 또는 Tenant Management API에 유효한 인증 토큰을 얻기 위해 일련의 API 요청을 발행해야 합니다.

SSO(Single Sign-On)가 활성화된 경우 API에 로그인합니다

Active Directory를 SSO ID 공급자로 사용하는 경우 다음 지침이 적용됩니다.

시작하기 전에

- StorageGRID 사용자 그룹에 속한 페더레이션 사용자의 SSO 사용자 이름과 암호를 알고 있습니다.
- 테넌트 관리 API에 액세스하려면 테넌트 계정 ID를 알고 있어야 합니다.

이 작업에 대해

인증 토큰을 얻으려면 다음 예 중 하나를 사용할 수 있습니다.

- 그만큼 `storagegrid-ssoauth.py` StorageGRID 설치 파일 디렉토리에 있는 Python 스크립트(`./rpms` RHEL의 경우, `./debs` Ubuntu 또는 Debian의 경우 `./vsphere` VMware의 경우).
- curl 요청의 워크플로 예

컬을 너무 느리게 수행하면 커링 작업 시간이 초과될 수 있습니다. 다음 오류가 표시될 수 있습니다 A valid SubjectConfirmation was not found on this Response.



예제 curl 워크플로는 다른 사용자가 암호를 볼 수 없도록 보호하지 않습니다.

URL 인코딩 문제가 있는 경우 다음 오류가 표시될 수 있습니다 Unsupported SAML version.

단계

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

프롬프트가 표시되면 다음 인수에 대한 값을 입력합니다.

- SSO 방법 ADFS 또는 ADFS를 입력합니다.
- SSO 사용자 이름입니다
- StorageGRID가 설치된 도메인입니다
- StorageGRID의 주소입니다
- 테넌트 관리 API에 액세스하려는 경우 테넌트 계정 ID입니다.

```

python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****
*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7

```

StorageGRID 인증 토큰은 출력에 제공됩니다. 이제 SSO가 사용되지 않는 경우 API를 사용하는 방법과 유사하게 다른 요청에 토큰을 사용할 수 있습니다.

3. curl 요청을 사용하려면 다음 절차를 따르십시오.

a. 로그인에 필요한 변수를 선언합니다.

```

export SAMLUER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'

```



그리드 관리 API에 액세스하려면 0을 로 `TENANTACCOUNTID` 사용합니다.

b. 서명된 인증 URL을 수신하려면 POST 요청을 발행하고 /api/v3/authorize-saml 응답에서 추가 JSON 인코딩을 제거합니다.

이 예제에서는 예 대해 서명된 인증 URL에 대한 POST 요청을 보여 TENANTACCOUNTID 줍니다. 결과는 예 전달되어 python -m json.tool JSON 인코딩을 제거합니다.

```

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

```

이 예제의 응답에는 URL로 인코딩된 서명된 URL이 포함되어 있지만 추가 JSON 인코딩 계층은 포함되지 않습니다.

```
{
  "apiVersion": "3.0",
  "data":
    "https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
    ss1%2BfQ33cvfwA%3D&RelayState=12345",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

- c. 후속 명령에서 사용할 수 있도록 응답에서 를 SAMLRequest 저장합니다.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...ss1%2BfQ33cvfwA%3D'
```

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

한 가지 옵션은 이전 응답의 URL을 사용하여 로그인 양식을 요청하는 것입니다.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

응답에는 클라이언트 요청 ID:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRT0MwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&cli
ent-request-id=00000000-0000-0000-ee02-0080000000de" >
```

- e. 응답에서 클라이언트 요청 ID를 저장합니다.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

- f. 이전 응답에서 양식 작업으로 자격 증명을 보냅니다.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMPLPASSWORD&AuthMethod=formsAuthentication" --include
```

AD FS는 헤더에 추가 정보가 포함된 302 리디렉션을 반환합니다.



SSO 시스템에 대해 MFA(다중 요소 인증)가 활성화된 경우 양식 게시물에는 두 번째 암호 또는 다른 자격 증명도 포함됩니다.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRT0MwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNTJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. `MSISAuth` 응답에서 쿠키를 저장합니다.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNTJvWY='
```

h. 인증 POST에서 쿠키를 사용하여 지정된 위치로 GET 요청을 보냅니다.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
\$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

응답 헤더에는 나중에 로그아웃 사용을 위한 AD FS 세션 정보가 포함되며 응답 본문에는 숨겨진 양식 필드에 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=a3dpbnRlcnMtUHJpbWFyeS1BZG1ppi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bk11MnFuUSUzzCUzzCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjoxMjoxOVpcMQ==;
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="PHNhbw0lJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

- i. 숨겨진 필드에서 를 저장합니다 SAMLResponse.

```
export SAMLResponse='PHNhbw0lJlc3BvbnN...1scDpSZXNwb25zZT4='
```

- j. 저장된 를 사용하여 SAMLResponse StorageGRID/api/saml-response 요청을 만들어 StorageGRID 인증 토큰을 생성합니다.

에서는 RelayState 테넌트 계정 ID를 사용하거나 그리드 관리 API에 로그인하려면 0을 사용합니다.

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

응답에는 인증 토큰이 포함됩니다.

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

- a. 응답에 인증 토큰을 로 `MYTOKEN` 저장합니다.

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

이제 SSO를 사용하지 않는 경우 API를 사용하는 방법과 유사한 다른 요청에 사용할 수 MYTOKEN 있습니다.

SSO(Single Sign-On)가 활성화된 경우 API에서 로그아웃합니다

SSO(Single Sign-On)가 활성화된 경우 그리드 관리 API 또는 테넌트 관리 API에서 로그아웃하기 위해 일련의 API 요청을 실행해야 합니다. Active Directory를 SSO ID 공급자로 사용하는 경우 다음 지침이 적용됩니다

이 작업에 대해

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

단계

- 서명된 로그아웃 요청을 생성하려면 "cookie "sso=true"를 SLO API에 전달합니다.

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

로그아웃 URL이 반환됩니다.

```
{
    "apiVersion": "3.0",
    "data": "https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. 로그아웃 URL을 저장합니다.

```
export LOGOUT_REQUEST  
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%  
3D'
```

3. 로그아웃 URL에 요청을 보내 SLO를 트리거하고 StorageGRID로 다시 리디렉션합니다.

```
curl --include "$LOGOUT_REQUEST"
```

302 응답이 반환됩니다. 리디렉션 위치는 API 전용 로그아웃에는 적용되지 않습니다.

```
HTTP/1.1 302 Found  
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-  
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256  
Set-Cookie: MSISignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018  
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. StorageGRID bearer token을 삭제한다.

StorageGRID 베어러 토큰을 삭제하는 것은 SSO를 사용하지 않는 것과 동일한 방식으로 작동합니다. 'cookie "sso=true"'가 제공되지 않으면 사용자는 SSO 상태에 영향을 주지 않고 StorageGRID에서 로그아웃됩니다.

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

`204 No Content` 사용자가 현재 로그아웃되었음을 나타내는 응답입니다.

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

Single Sign-On이 활성화된 경우 API를 사용하세요(Entra ID)

만약 당신이 가지고 있다면 "[SSO\(Single Sign-On\) 구성 및 활성화](#)" SSO 공급자로 Entra ID를 사용하는 경우 두 개의 예제 스크립트를 사용하여 Grid Management API 또는 Tenant Management API에 유효한 인증 토큰을 얻을 수 있습니다.

Entra ID 단일 로그인이 활성화된 경우 API에 Sign in.

이 지침은 SSO ID 공급자로 Entra ID를 사용하는 경우에 적용됩니다.

시작하기 전에

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

이 작업에 대해

인증 토큰을 얻으려면 다음 예제 스크립트를 사용할 수 있습니다.

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

두 스크립트 모두 StorageGRID 설치 파일 디렉토리에 있습니다.(./rpms RHEL의 경우, ./debs Ubuntu 또는 Debian의 경우 ./vsphere VMware의 경우).

Entra ID를 사용하여 자체 API 통합을 작성하려면 다음을 참조하세요. `storagegrid-ssoauth-azure.py` 스크립트. Python 스크립트는 StorageGRID에 직접 두 가지 요청을 합니다(먼저 SAMLRequest를 가져오고, 나중에는 인증 토큰을 가져오는 것). 또한 Node.js 스크립트를 호출하여 Entra ID와 상호 작용하여 SSO 작업을 수행합니다.

SSO 작업은 일련의 API 요청을 사용하여 실행할 수 있지만, 그렇게 하는 것은 간단하지 않습니다. Puppeteer Node.js 모듈은 Entra ID SSO 인터페이스를 스크래핑하는 데 사용됩니다.

URL 인코딩 문제가 있는 경우 다음 오류가 표시될 수 있습니다 `Unsupported SAML version.`

단계

1. 다음과 같이 필요한 종속성을 설치합니다.
 - a. Node.js를 설치합니다(참조 "<https://nodejs.org/en/download/>").
 - b. 필요한 Node.js 모듈(puppeteer 및 jsdom)을 설치합니다.

```
npm install -g <module>
```

2. Python 스크립트를 Python 인터프리터로 전달하여 스크립트를 실행합니다.

그러면 Python 스크립트가 해당 Node.js 스크립트를 호출하여 Entra ID SSO 상호 작용을 수행합니다.

3. 프롬프트가 표시되면 다음 인수에 대한 값을 입력하거나 매개 변수를 사용하여 전달합니다.
 - Entra ID에 로그인하는 데 사용되는 SSO 이메일 주소
 - StorageGRID의 주소입니다
 - 테넌트 관리 API에 액세스하려는 경우 테넌트 계정 ID입니다
4. 메시지가 표시되면 비밀번호를 입력하고, 요청 시 Entra ID에 대한 MFA 승인을 제공할 준비를 하세요.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com  
--sg-address storagegrid.example.com --tenant-account-id 0  
Enter the user's SSO password:  
*****  
  
Watch for and approve a 2FA authorization request  
*****  
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion': '3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



이 스크립트는 MFA가 Microsoft Authenticator를 사용하여 수행된 것으로 가정합니다. 다른 형태의 MFA를 지원하도록 스크립트를 수정해야 할 수도 있습니다(예: 텍스트 메시지에 수신된 코드 입력).

StorageGRID 인증 토큰은 출력에 제공됩니다. 이제 SSO가 사용되지 않는 경우 API를 사용하는 방법과 유사하게 다른 요청에 토큰을 사용할 수 있습니다.

SSO(Single Sign-On)가 활성화된 경우 API 사용(PingFederate)

만약 당신이 가지고 있다면 "[SSO\(Single Sign-On\) 구성 및 활성화](#)" PingFederate를 SSO 공급자로 사용하는 경우 Grid Management API 또는 Tenant Management API에 유효한 인증 토큰을 얻기 위해 일련의 API 요청을 발행해야 합니다.

SSO(Single Sign-On)가 활성화된 경우 API에 로그인합니다

이 지침은 PingFederate를 SSO ID 공급자로 사용하는 경우 적용됩니다

시작하기 전에

- StorageGRID 사용자 그룹에 속한 페더레이션 사용자의 SSO 사용자 이름과 암호를 알고 있습니다.
- 테넌트 관리 API에 액세스하려면 테넌트 계정 ID를 알고 있어야 합니다.

이 작업에 대해

인증 토큰을 얻으려면 다음 예 중 하나를 사용할 수 있습니다.

- 그만큼 `storagegrid-ssoauth.py` StorageGRID 설치 파일 디렉토리에 있는 Python 스크립트(`./rpms` RHEL의 경우, `./debs` Ubuntu 또는 Debian의 경우 `./vsphere` VMware의 경우).
- curl 요청의 워크플로 예

컬을 너무 느리게 수행하면 커링 작업 시간이 초과될 수 있습니다. 다음 오류가 표시될 수 있습니다 A valid SubjectConfirmation was not found on this Response.



예제 curl 워크플로는 다른 사용자가 암호를 볼 수 없도록 보호하지 않습니다.

URL 인코딩 문제가 있는 경우 다음 오류가 표시될 수 있습니다 Unsupported SAML version.

단계

- 인증 토큰을 얻으려면 다음 방법 중 하나를 선택합니다.
 - `storagegrid-ssoauth.py` Python 스크립트를 사용합니다. 2단계로 이동합니다.
 - curl 요청을 사용합니다. 3단계로 이동합니다.

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

프롬프트가 표시되면 다음 인수에 대한 값을 입력합니다.

- SSO 방법 "pingfederate"(PINGFEDERATE, Pingfederate 등)의 모든 변형을 입력할 수 있습니다.
- SSO 사용자 이름입니다
- StorageGRID가 설치된 도메인입니다. 이 필드는 PingFederate에 사용되지 않습니다. 빈 칸으로 두거나 원하는 값을 입력할 수 있습니다.
- StorageGRID의 주소입니다
- 테넌트 관리 API에 액세스하려는 경우 테넌트 계정 ID입니다.

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_domain:
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****
*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

StorageGRID 인증 토큰은 출력에 제공됩니다. 이제 SSO가 사용되지 않는 경우 API를 사용하는 방법과 유사하게 다른 요청에 토큰을 사용할 수 있습니다.

3. curl 요청을 사용하려면 다음 절차를 따르십시오.

- a. 로그인에 필요한 변수를 선언합니다.

```
export SAMLUSER='my-sso-username'
export SAMPLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```



그리드 관리 API에 액세스하려면 0을 로 `TENANTACCOUNTID` 사용합니다.

- b. 서명된 인증 URL을 수신하려면 POST 요청을 발행하고 /api/v3/authorize-saml 응답에서 추가 JSON 인코딩을 제거합니다.

이 예제에서는 TENANTACCOUNTID에 대한 서명된 인증 URL에 대한 POST 요청을 보여 줍니다. 결과는 python-m json.tool에 전달되어 JSON 인코딩을 제거합니다.

```

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

```

이 예제의 응답에는 URL로 인코딩된 서명된 URL이 포함되어 있지만 추가 JSON 인코딩 계층은 포함되지 않습니다.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

- c. 후속 명령에서 사용할 수 있도록 응답에서 를 SAMLRequest 저장합니다.

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

- d. 응답과 쿠키를 내보내고 응답을 에코합니다.

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

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

- e. 'pf.adapterId' 값을 내보내고 응답을 에코합니다.

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

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

- f. 'href' 값을 내보내고(후행 슬래시/ 제거) 응답을 에코합니다.

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

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

g. '조치' 값 내보내기:

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

h. 자격 증명과 함께 쿠키 보내기:

```
curl -b <(echo "$RESPONSE") -x POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=$SAMPLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER" \
--include
```

i. 숨겨진 필드에서 를 저장합니다 SAMLResponse.

```
export SAMLResponse='PHNhbWxwO1Jlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 저장된 를 사용하여 SAMLResponse StorageGRID/api/saml-response 요청을 만들어 StorageGRID 인증 토큰을 생성합니다.

에서는 RelayState 테넌트 계정 ID를 사용하거나 그리드 관리 API에 로그인하려면 0을 사용합니다.

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

응답에는 인증 토큰이 포함됩니다.

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

a. 응답에 인증 토큰을 로 `MYTOKEN`저장합니다.

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

이제 SSO를 사용하지 않는 경우 API를 사용하는 방법과 유사한 다른 요청에를 사용할 수 MYTOKEN 있습니다.

SSO(Single Sign-On)가 활성화된 경우 API에서 로그아웃합니다

SSO(Single Sign-On)가 활성화된 경우 그리드 관리 API 또는 테넌트 관리 API에서 로그아웃하기 위해 일련의 API 요청을 실행해야 합니다. 이 지침은 PingFederate를 SSO ID 공급자로 사용하는 경우 적용됩니다.

이 작업에 대해

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

단계

- 서명된 로그아웃 요청을 생성하려면 "cookie "sso=true"를 SLO API에 전달합니다.

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

로그아웃 URL이 반환됩니다.

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

- 로그아웃 URL을 저장합니다.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

- 로그아웃 URL에 요청을 보내 SLO를 트리거하고 StorageGRID로 다시 리디렉션합니다.

```
curl --include "$LOGOUT_REQUEST"
```

302 응답이 반환됩니다. 리디렉션 위치는 API 전용 로그아웃에는 적용되지 않습니다.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. StorageGRID bearer token을 삭제한다.

StorageGRID 베어러 토큰을 삭제하는 것은 SSO를 사용하지 않는 것과 동일한 방식으로 작동합니다. 'cookie "sso=true"'가 제공되지 않으면 사용자는 SSO 상태에 영향을 주지 않고 StorageGRID에서 로그아웃됩니다.

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

`204 No Content` 사용자가 현재 로그아웃되었음을 나타내는 응답입니다.

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

API를 사용하여 기능을 비활성화합니다

그리드 관리 API를 사용하여 StorageGRID 시스템의 특정 기능을 완전히 비활성화할 수 있습니다. 기능이 비활성화되면 해당 기능과 관련된 작업을 수행할 수 있는 권한을 아무도 할당할 수 없습니다.

이 작업에 대해

비활성화된 기능 시스템을 사용하면 StorageGRID 시스템의 특정 기능에 액세스하지 못하게 할 수 있습니다. 루트 사용자 또는 * 루트 액세스 * 권한이 있는 관리자 그룹에 속한 사용자가 해당 기능을 사용할 수 없도록 하는 유일한 방법은 기능을 비활성화하는 것입니다.

이 기능이 어떻게 유용한지 이해하려면 다음 시나리오를 고려해 보십시오.

_Company A는 테넌트 계정을 생성하여 StorageGRID 시스템의 스토리지 용량을 임대하는 서비스 공급자입니다. 회사 A는 임차자의 객체 보안을 보호하기 위해 계정이 배포된 후 자신의 직원이 테넌트 계정에 액세스할 수 없도록 하려고 합니다. _

_회사 A는 그리드 관리 API에서 기능 비활성화 시스템을 사용하여 이 목표를 달성을 수 있습니다. 그리드 관리자에서 * 테넌트 루트 암호 변경 * 기능을 완전히 비활성화함으로써(UI 및 API 모두) 회사 A는 루트 사용자 및 * 루트 액세스 * 권한을 가진 그룹에 속한 사용자를 포함하여 관리자 사용자가 테넌트 계정의 루트 사용자에 대한 암호를 변경할 수 없도록 합니다

단계

1. Grid Management API에 대한 Swagger 문서에 액세스합니다. 을 "Grid Management API를 사용합니다" 참조하십시오.
2. 기능 비활성화 끝점을 찾습니다.
3. 테넌트 루트 암호 변경 등의 기능을 비활성화하려면 다음과 같이 API로 본문을 보냅니다.

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

요청이 완료되면 테넌트 루트 암호 변경 기능이 비활성화됩니다. 테넌트 루트 암호 변경 * 관리 권한이 더 이상 사용자 인터페이스에 표시되지 않으며 테넌트의 루트 암호를 변경하려고 시도하는 모든 API 요청이 "403 사용 권한 없음"과 함께 실패합니다.

비활성화된 피처를 다시 활성화합니다

기본적으로 그리드 관리 API를 사용하여 비활성화된 기능을 다시 활성화할 수 있습니다. 그러나 비활성화된 피처가 다시 활성화되지 않도록 하려면 * activateFeatures * 기능 자체를 비활성화할 수 있습니다.

 activateFeatures * 기능을 다시 활성화할 수 없습니다. 이 기능을 비활성화하려는 경우 비활성화된 다른 모든 기능을 다시 활성화할 수 있는 기능이 영구적으로 손실됩니다. 손실된 기능을 복원하려면 기술 지원 부서에 문의해야 합니다.

단계

1. Grid Management API에 대한 Swagger 문서에 액세스합니다.
2. 기능 비활성화 끝점을 찾습니다.
3. 모든 기능을 다시 활성화하려면 다음과 같이 API로 본문을 보내십시오.

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

이 요청이 완료되면 테넌트 루트 암호 변경 기능을 포함한 모든 기능이 다시 활성화됩니다. 이제 사용자 인터페이스에 * 테넌트 루트 암호 변경 * 관리 권한이 표시되며, 사용자에게 * 루트 액세스 * 또는 * 테넌트 루트 암호 변경 * 관리 권한이 있는 경우 테넌트의 루트 암호를 변경하려고 시도하는 모든 API 요청이 성공합니다.

 이전 예에서는 _ALL_DEACTED 피처가 재활성화됩니다. 비활성화된 상태로 유지되어야 하는 다른 기능이 비활성화된 경우, PUT 요청에 명시적으로 지정해야 합니다. 예를 들어 테넌트 루트 암호 변경 기능을 다시 활성화하고 StorageAdmin 관리 권한을 계속 비활성화하려면 다음 PUT 요청을 보내십시오.

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

StorageGRID에 대한 액세스를 제어합니다

StorageGRID 액세스를 제어합니다

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

그리드 관리자에 대한 액세스를 제어합니다

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

을 "ID 제휴" 사용하면 설정이 "그룹" "사용자" 빨라지고 사용자가 친숙한 자격 증명을 사용하여 StorageGRID에 로그인할 수 있습니다. Active Directory, OpenLDAP 또는 Oracle Directory Server를 사용하는 경우 ID 페더레이션을 구성할 수 있습니다.



다른 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의하십시오.

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

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

SSO(Single Sign-On)를 활성화합니다

StorageGRID 시스템은 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용하여 SSO(Single Sign-On)를 지원합니다. 당신이 후에 ["SSO를 구성하고 사용하도록 설정합니다"](#) 모든 사용자는 Grid Manager, Tenant Manager, Grid Management API 또는 Tenant Management API에 액세스하기 전에 외부 ID 공급자로부터 인증을 받아야 합니다. 로컬 사용자는 StorageGRID 에 로그인할 수 없습니다.

프로비저닝 암호를 변경합니다

프로비저닝 암호는 많은 설치 및 유지 관리 절차와 StorageGRID 복구 패키지를 다운로드하는 데 필요합니다. StorageGRID 시스템의 그리드 토플로지 정보와 암호화 키의 백업을 다운로드하려면 암호도 필요합니다. 당신은 할 수 있습니다 ["암호를 변경합니다"](#) 필요에 따라.

노드 콘솔 암호를 변경합니다

그리드의 각 노드에는 노드 콘솔 비밀번호가 있는데, SSH를 사용하여 "admin"으로 노드에 로그인하거나 VM/물리적 콘솔 연결에서는 루트 사용자로 로그인해야 합니다. 필요에 따라 다음을 수행할 수 있습니다. ["노드 콘솔 암호를 변경합니다"](#) 각 노드에 대해.

프로비저닝 암호를 변경합니다

이 절차를 사용하여 StorageGRID 프로비저닝 암호를 변경합니다. 암호는 복구, 확장 및 유지 관리 절차에 필요합니다. StorageGRID 시스템의 그리드 토플로지 정보, 그리드 노드 콘솔 비밀번호, 암호화 키가 포함된 복구 패키지 백업을 다운로드하려면 암호도 필요합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. ["지원되는 웹 브라우저"](#)
- 유지 관리 또는 루트 액세스 권한이 있습니다.
- 현재 프로비저닝 암호가 있습니다.

이 작업에 대해

프로비저닝 암호는 많은 설치 및 유지 관리 절차에 필요하며 "[복구 패키지 다운로드](#)". 프로비저닝 암호가 나열되어 있지 않습니다. `Passwords.txt` 파일. 프로비저닝 암호를 문서화하고 안전하고 보안이 유지되는 곳에 보관하세요.

단계

1. 구성 > 액세스 제어 > *그리드 비밀번호*를 선택합니다.
2. 프로비저닝 암호 변경 *에서 *변경*을 선택합니다
3. 현재 프로비저닝 암호를 입력합니다.
4. 새 암호를 입력합니다. 암호는 8자 이상 32자 이하여야 합니다. 암호는 대/소문자를 구분합니다.



프로비저닝 암호를 안전한 곳에 보관하세요. 설치, 확장, 유지관리 절차에 필요합니다.

5. 새 암호를 다시 입력하고 *Save*를 선택합니다.

프로비저닝 암호 변경이 완료되면 녹색 성공 배너가 표시됩니다.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

6. 복구 패키지 *를 선택합니다.
7. 새로운 복구 패키지를 다운로드하려면 새로운 프로비저닝 암호를 입력하세요.



프로비저닝 암호를 변경한 후에는 즉시 새로운 복구 패키지를 다운로드해야 합니다. 복구 패키지 파일을 사용하면 장애가 발생할 경우 시스템을 복원할 수 있습니다.

노드 콘솔 암호를 변경합니다

그리드의 각 노드에는 노드 콘솔 비밀번호가 있으며, 이를 사용하여 노드에 로그인합니다. 기본적으로 각 노드에는 고유한 비밀번호가 있습니다. 각 비밀번호를 새로운 고유 비밀번호로 변경할 수도 있고, 모든 노드의 비밀번호를 변경하여 글로벌 비밀번호를 사용할 수도 있습니다. 비밀번호는 복구 패키지에 저장됩니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 이 "[유지 관리 또는 루트 액세스 권한](#)"입니다.
- 현재 프로비저닝 암호가 있습니다.

이 작업에 대해

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

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

비밀번호는 업데이트된 위치에 저장됩니다. `Passwords.txt` 복구 패키지의 파일입니다. 비밀번호는 파일의 비밀번호

열에 나열되어 있습니다.



그만큼 "SSH 접속 비밀번호" 노드 간 통신에 사용되는 SSH 키는 노드 콘솔 비밀번호와 분리되어 있습니다. 이 절차는 SSH 액세스 비밀번호를 변경하지 않습니다.

마법사에 액세스합니다

단계

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

현재 복구 패키지를 다운로드합니다

노드 콘솔 비밀번호를 변경하기 전에 최신 복구 패키지를 다운로드하세요. 어떤 노드에서든 비밀번호 변경 프로세스가 실패하면 이 파일에 있는 비밀번호를 사용할 수 있습니다.

단계

1. 그리드의 프로비저닝 암호를 입력합니다.
2. 복구 패키지 다운로드 *를 선택합니다.
3. 복구 패키지 파일을 복사합니다(.zip) 두 개의 안전하고 보안이 유지되는 별도 장소로 이동합니다.



복구 패키지 파일은 StorageGRID 시스템에서 데이터를 얻는 데 사용할 수 있는 암호화 키와 비밀번호가 포함되어 있으므로 보호되어야 합니다.

4. Continue *를 선택합니다.

새로운 비밀번호를 제공하세요

1. 사용할 비밀번호 변경 방법을 선택하세요.
 - 자동: StorageGRID 모든 노드에 새로운 무작위 콘솔 비밀번호를 자동으로 할당합니다.
 - 사용자 지정: 콘솔 비밀번호를 제공합니다.

오토매트

1. Continue *를 선택합니다.

맞춤형

1. 다음 중 하나를 선택합니다.
 - 글로벌 콘솔 비밀번호: 모든 노드에 동일한 콘솔 비밀번호를 적용합니다.
 - 고유 콘솔 비밀번호: 하나 이상의 노드에 다른 비밀번호를 적용합니다.
2. *글로벌 콘솔 비밀번호*를 선택한 경우 모든 노드에 사용할 비밀번호를 입력합니다.
3. *고유 콘솔 비밀번호*를 선택한 경우 하나 이상의 노드에 대한 고유한 비밀번호를 입력합니다.
4. Continue *를 선택합니다.

비밀번호 변경을 완료하세요

1. 확인 대화 상자가 나타나면 StorageGRID 가 노드 콘솔 비밀번호 변경을 시작할 준비가 되었다면 *예*를 선택합니다.



이 프로세스가 시작된 후에는 취소할 수 없습니다.

StorageGRID 새로운 비밀번호가 포함된 새로운 복구 패키지를 생성합니다.

2. 새로운 복구 패키지가 준비되면 *새로운 복구 패키지 다운로드*를 선택하고 복구 패키지를 저장합니다.
3. 파일을 엽니다 .zip.
4. 새 노드 콘솔 암호가 포함된 파일을 포함하여 컨텐츠에 액세스할 수 있는지 확인합니다 Passwords.txt.
5. 새로운 복구 패키지 파일을 복사합니다.(.zip) 두 개의 안전하고 보안이 유지되는 별도 장소로 이동합니다.



이전 복구 패키지를 덮어쓰지 마세요.

StorageGRID 시스템에서 데이터를 얻는 데 사용할 수 있는 암호화 키와 비밀번호가 포함되어 있으므로 복구 파일을 보호해야 합니다.

6. 새로운 복구 패키지를 다운로드하고 내용을 확인했음을 나타내려면 확인란을 선택하세요.
7. Continue * 를 선택합니다.

StorageGRID 각 노드의 비밀번호를 업데이트합니다.

업데이트 프로세스 중에 오류가 발생하면 진행률 표시줄에 비밀번호 변경에 실패한 노드 수가 나열됩니다. 시스템은 비밀번호 변경에 실패한 모든 노드에서 자동으로 프로세스를 다시 시도합니다. 프로세스가 종료되어 일부 노드의 비밀번호가 변경되지 않은 경우, 다시 시도 버튼이 나타납니다.

8. 하나 이상의 노드에 대한 암호 업데이트가 실패한 경우:
 - a. 표에 나열된 오류 메시지를 검토합니다.
 - b. 문제를 해결합니다.
 - c. 재시도 * 를 선택합니다.



다시 시도하면 이전 암호 변경 시도 중에 실패한 노드의 노드 콘솔 암호만 변경됩니다.

9. 진행률 표시줄에 업데이트가 더 이상 남아 있지 않다고 표시되면 *마침*을 선택합니다.
10. 모든 노드의 노드 콘솔 암호가 변경된 후 삭제합니다.[처음 다운로드한 복구 패키지](#).

관리 노드의 SSH 액세스 암호를 변경합니다

관리 노드의 SSH 액세스 암호를 변경하면 그리드의 각 노드에 대한 내부 SSH 키의 고유한 세트도 업데이트됩니다. 기본 관리자 노드는 이러한 SSH 키를 사용하여 보안 암호 없는 인증을 사용하여 노드에 액세스합니다.

SSH 키를 사용하여 노드에 admin 또는 VM 또는 물리적 콘솔 연결에서 루트 사용자로 로그인합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "유지 관리 또는 루트 액세스 권한"있습니다.
- 현재 프로비저닝 암호가 있습니다.

이 작업에 대해

관리 노드의 새 액세스 암호와 각 노드의 새 내부 키는 다음에 저장됩니다. `Passwords.txt` 복구 패키지의 파일입니다. 키는 해당 파일의 비밀번호 열에 나열되어 있습니다.

노드 간 통신에 사용되는 SSH 키에 대해 별도의 SSH 액세스 암호가 있습니다. 이 절차는 변경되지 않습니다.

마법사에 액세스합니다

단계

1. 구성 > 액세스 제어 > *그리드 비밀번호*를 선택합니다.
2. SSH 키 변경 * 아래에서 * 변경 * 을 선택합니다.

현재 복구 패키지를 다운로드합니다

SSH 액세스 키를 변경하기 전에 최신 복구 패키지를 다운로드하세요. 어떤 노드에서든 키 변경 프로세스가 실패하면 이 파일에 있는 키를 사용할 수 있습니다.

단계

1. 그리드의 프로비저닝 암호를 입력합니다.
2. 복구 패키지 다운로드 * 를 선택합니다.
3. 복구 패키지 파일을 복사합니다(.zip) 두 개의 안전하고 보안이 유지되는 별도 장소로 이동합니다.



복구 패키지 파일은 StorageGRID 시스템에서 데이터를 얻는 데 사용할 수 있는 암호화 키와 비밀번호가 포함되어 있으므로 보호되어야 합니다.

4. Continue * 를 선택합니다.
5. 확인 대화 상자가 나타나면 SSH 액세스 키 변경을 시작할 준비가 되었으면 * Yes * 를 선택합니다.



이 프로세스가 시작된 후에는 취소할 수 없습니다.

SSH 액세스 키를 변경합니다

SSH 액세스 키 변경 프로세스가 시작되면 새 키가 포함된 새로운 복구 패키지가 생성됩니다. 그런 다음 각 노드의 키가 업데이트됩니다.

단계

1. 새로운 복구 패키지가 생성될 때까지 기다리세요. 몇 분 정도 걸릴 수 있습니다.
2. 새 복구 패키지 다운로드 버튼이 활성화되면 *새 복구 패키지 다운로드*를 선택하고 새 복구 패키지 파일을 저장합니다.(.zip) 두 개의 안전하고 보안이 유지되는 별도 장소로 이동합니다.
3. 다운로드가 완료되면 다음을 수행합니다.

- a. 파일을 엽니다 .zip.
- b. 새 SSH 액세스 키가 포함된 파일을 포함하여 콘텐츠에 액세스할 수 있는지 확인합니다 Passwords.txt.
- c. 새로운 복구 패키지 파일을 복사합니다.(.zip) 두 개의 안전하고 보안이 유지되는 별도 장소로 이동합니다.



이전 복구 패키지를 덮어쓰지 마세요.

복구 패키지 파일은 StorageGRID 시스템에서 데이터를 얻는 데 사용할 수 있는 암호화 키와 비밀번호가 포함되어 있으므로 보호되어야 합니다.

4. 각 노드에서 키가 업데이트될 때까지 기다립니다. 몇 분 정도 걸릴 수 있습니다.

모든 노드의 키를 변경하면 녹색 성공 배너가 나타납니다.

업데이트 프로세스 중에 오류가 발생하면 배너 메시지에 키 변경에 실패한 노드 수가 나열됩니다. 시스템은 키 변경에 실패한 노드에서 프로세스를 자동으로 재시도합니다. 일부 노드에 변경 키가 없는 경우 * Retry *(재시도) 버튼이 나타납니다.

하나 이상의 노드에 대한 키 업데이트가 실패한 경우:

- a. 표에 나열된 오류 메시지를 검토합니다.
- b. 문제를 해결합니다.
- c. 재시도 * 를 선택합니다.

다시 시도하면 이전 키 변경 시도 중에 장애가 발생한 노드에서 SSH 액세스 키만 변경됩니다.

5. 모든 노드에 대한 SSH 액세스 키가 변경된 후 삭제합니다.[처음 다운로드한 복구 패키지](#).

6. 선택적으로 유지 관리 > 시스템 > *복구 패키지*를 선택하여 새 복구 패키지의 추가 사본을 다운로드합니다.

ID 페더레이션을 사용합니다

ID 페더레이션을 사용하면 그룹 및 사용자를 더 빠르게 설정할 수 있으며, 사용자는 익숙한 자격 증명을 사용하여 StorageGRID에 로그인할 수 있습니다.

Grid Manager의 ID 페더레이션을 구성합니다

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

시작하기 전에

- 다음을 사용하여 Grid Manager에 로그인했습니다.["지원되는 웹 브라우저"](#).
- 당신은["특정 액세스 권한"](#).
- ID 공급자로 Active Directory, Microsoft Entra ID, OpenLDAP 또는 Oracle Directory Server를 사용하고 있습니다.



나열되지 않은 LDAP v3 서비스를 사용하려면 기술 지원팀에 문의하세요.

- OpenLDAP를 사용하려면 OpenLDAP 서버를 구성해야 합니다. 을 [OpenLDAP 서버 구성 지침](#) 참조하십시오.
- SSO(Single Sign-On)를 활성화하려는 경우 다음을 검토해야 합니다. "[SSO\(Single Sign-On\)에 대한 요구 사항 및 고려 사항](#)" .
- LDAP 서버와의 통신에 TLS(Transport Layer Security)를 사용하려는 경우 ID 공급자는 TLS 1.2 또는 1.3을 사용합니다. 을 "[발신 TLS 연결에 지원되는 암호](#)" 참조하십시오.

이 작업에 대해

Active Directory, Microsoft Entra ID, OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 그룹을 가져오려면 Grid Manager에 대한 ID 소스를 구성할 수 있습니다. 다음 유형의 그룹을 가져올 수 있습니다.

- 관리 그룹: 관리자 그룹의 사용자는 그룹에 할당된 관리 권한에 따라 Grid Manager에 로그인하여 작업을 수행할 수 있습니다.
- 자신의 ID 소스를 사용하지 않는 테넌트의 테넌트 사용자 그룹 테넌트 그룹의 사용자는 테넌트 관리자의 그룹에 할당된 권한을 기반으로 테넌트 관리자에 로그인하여 작업을 수행할 수 있습니다. 자세한 내용은 및 "[테넌트 계정을 사용합니다](#)"를 "[테넌트 계정을 생성합니다](#)" 참조하십시오.

구성을 입력합니다

단계

1. 구성 > 액세스 제어 > *ID 페더레이션*을 선택합니다.
2. ID 페더레이션 사용 * 을 선택합니다.
3. LDAP 서비스 유형 섹션에서 구성할 LDAP 서비스 유형을 선택합니다.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other
------------------	----------	----------	-------

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

4. 기타 * 를 선택한 경우 LDAP 속성 섹션의 필드를 작성합니다. 그렇지 않으면 다음 단계로 이동합니다.
 - 사용자 고유 이름: LDAP 사용자의 고유 식별자를 포함하는 속성의 이름입니다. 이 속성은 다음과 동일합니다. sAMAccountName Active Directory 및 uid OpenLDAP용. Oracle Directory Server를 구성하는 경우 다음을 입력하세요. uid .
 - 사용자 UUID: LDAP 사용자의 영구 고유 식별자를 포함하는 속성의 이름입니다. 이 속성은 다음과 동일합니다. objectGUID Active Directory 및 entryUUID OpenLDAP용. Oracle Directory Server를 구성하는 경우 다음을 입력하세요. nsuniqueid . 지정된 속성에 대한 각 사용자 값은 16바이트 또는 문자열 형식의 32자리 16진수여야 하며, 하이픈은 무시됩니다.
 - 그룹 고유 이름: LDAP 그룹의 고유 식별자를 포함하는 속성의 이름입니다. 이 속성은 다음과 동일합니다. sAMAccountName Active Directory 및 cn OpenLDAP용. Oracle Directory Server를 구성하는 경우 다음을 입력하세요. cn .
 - 그룹 UUID: LDAP 그룹의 영구 고유 식별자를 포함하는 속성의 이름입니다. 이 속성은 다음과 동일합니다.

`objectGUID` Active Directory 및 `entryUUID` OpenLDAP용. Oracle Directory Server를 구성하는 경우 다음을 입력하세요. `nsuniqueid`. 지정된 속성에 대한 각 그룹의 값은 하이픈이 무시되는 16바이트 또는 문자열 형식의 32자리 16진수여야 합니다.

5. 모든 LDAP 서비스 유형에 대해 LDAP 서버 구성 섹션에 필요한 LDAP 서버 및 네트워크 연결 정보를 입력합니다.

- * 호스트 이름 *: LDAP 서버의 FQDN(정규화된 도메인 이름) 또는 IP 주소입니다.
- * 포트 *: LDAP 서버에 연결하는 데 사용되는 포트입니다.



STARTTLS의 기본 포트는 389이고 LDAPS의 기본 포트는 636입니다. 그러나 방화벽이 올바르게 구성된 경우 모든 포트를 사용할 수 있습니다.

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

Active Directory의 경우 아래쪽 로그온 이름 또는 사용자 기본 이름을 지정할 수도 있습니다.

지정된 사용자는 그룹 및 사용자를 나열하고 다음 속성에 액세스할 수 있는 권한이 있어야 합니다.

- `sAMAccountName` 또는 `uid`
- `objectGUID` `entryUUID`, 또는 `nsuniqueid`
- `cn`
- `memberOf` 또는 `isMemberOf`
- * Active Directory *: `objectSid`, `primaryGroupID`, `userAccountControl` 및 `userPrincipalName`
- 입장 ID: `accountEnabled` 그리고 `userPrincipalName`
- * 암호 *: 사용자 이름과 연결된 암호입니다.



나중에 암호를 변경하는 경우 이 페이지에서 암호를 업데이트해야 합니다.

- * Group Base DN *: 그룹을 검색할 LDAP 하위 트리에 대한 DN(고유 이름)의 전체 경로입니다. Active Directory 예제(아래)에서 고유 이름이 기본 DN(`DC=StorageGrid, DC=example, DC=com`)과 관련된 모든 그룹을 통합 그룹으로 사용할 수 있습니다.



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

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



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

- * 사용자 이름 형식 바인딩 * (선택 사항): 패턴을 자동으로 확인할 수 없는 경우 StorageGRID에서 기본 사용자 이름 패턴을 사용해야 합니다.

StorageGRID가 서비스 계정에 바인딩할 수 없는 경우 사용자가 로그인할 수 있으므로 * 사용자 이름 형식 바인딩 * 을 제공하는 것이 좋습니다.

다음 패턴 중 하나를 입력합니다.

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

[UserName] * 을 서면 그대로 포함합니다.

6. TLS(전송 계층 보안) 섹션에서 보안 설정을 선택합니다.

- **STARTTLS 사용:** STARTTLS를 사용하여 LDAP 서버와의 통신을 보호합니다. 이 옵션은 Active Directory, OpenLDAP 또는 기타에 권장되지만 Microsoft Entra ID에서는 지원되지 않습니다.
- **LDAPS 사용:** LDAPS(SSL을 통한 LDAP) 옵션은 TLS를 사용하여 LDAP 서버에 연결합니다. Microsoft Entra ID의 경우 이 옵션을 선택해야 합니다.
- **TLS를 사용하지 마세요:** StorageGRID 시스템과 LDAP 서버 간의 네트워크 트래픽이 보호되지 않습니다. 이 옵션은 Microsoft Entra ID에서 지원되지 않습니다.



Active Directory 서버에서 LDAP 서명을 적용하는 경우 **TLS** 사용 안 함 옵션은 지원되지 않습니다. STARTTLS 또는 LDAPS를 사용해야 합니다.

7. STARTTLS 또는 LDAPS를 선택한 경우 연결 보안에 사용되는 인증서를 선택합니다.

- * 운영 체제 CA 인증서 사용 *: 운영 체제에 설치된 기본 그리드 CA 인증서를 사용하여 연결을 보호합니다.
- * 사용자 지정 CA 인증서 사용 *: 사용자 지정 보안 인증서를 사용합니다.

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

연결을 테스트하고 구성을 저장합니다

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

단계

1. Test connection * 을 선택합니다.
2. 바인드 사용자 이름 형식을 제공하지 않은 경우:
 - 연결 설정이 유효한 경우 "Test connection successful(연결 테스트 성공)" 메시지가 나타납니다. Save * 를 선택하여 설정을 저장합니다.
 - 연결 설정이 잘못된 경우 "테스트 연결을 설정할 수 없습니다." 메시지가 나타납니다. 닫기 * 를 선택합니다. 그런 다음 문제를 해결하고 연결을 다시 테스트합니다.
3. 바인딩 사용자 이름 형식을 제공한 경우 유효한 통합 사용자의 사용자 이름과 암호를 입력합니다.

예를 들어 사용자 이름과 암호를 입력합니다. @ 또는 / 같은 특수 문자를 사용자 이름에 포함하지 마십시오.

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

.....

Cancel

Test Connection

- 연결 설정이 유효한 경우 "Test connection successful(연결 테스트 성공)" 메시지가 나타납니다. Save * 를 선택하여 설정을 저장합니다.
- 연결 설정, 바인딩 사용자 이름 형식 또는 테스트 사용자 이름과 암호가 올바르지 않으면 오류 메시지가 나타납니다. 모든 문제를 해결하고 연결을 다시 테스트합니다.

ID 소스와 강제로 동기화합니다

StorageGRID 시스템은 ID 소스에서 페더레이션 그룹과 사용자를 정기적으로 동기화합니다. 사용자 권한을 최대한 빨리 설정하거나 제한하려는 경우 동기화를 강제로 시작할 수 있습니다.

단계

- ID 페더레이션 페이지로 이동합니다.
- 페이지 맨 위에서 * 서버 동기화 * 를 선택합니다.

동기화 프로세스는 환경에 따라 다소 시간이 걸릴 수 있습니다.



ID 소스에서 페더레이션 그룹과 사용자를 동기화하는 데 문제가 있는 경우 * ID 페더레이션 동기화 실패 * 경고가 트리거됩니다.

ID 페더레이션을 비활성화합니다

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

이 작업에 대해

ID 페더레이션을 사용하지 않도록 설정하기 전에 다음 사항을 확인해야 합니다.

- 페더레이션 사용자는 로그인할 수 없습니다.
- 현재 로그인한 페더레이션 사용자는 세션이 만료될 때까지 StorageGRID 시스템에 대한 액세스 권한을 유지하지만 세션이 만료된 후에는 로그인할 수 없습니다.



- StorageGRID 시스템과 ID 소스 간의 동기화가 발생하지 않으며, 동기화되지 않은 계정에 대한 경고는 발생하지 않습니다.
- 단일 로그인(SSO) 상태가 활성화 또는 샌드박스 모드*인 경우 *ID 페더레이션 사용 확인란은 비활성화됩니다. ID 페더레이션을 비활성화하려면 Single Sign-on 페이지에서 SSO 상태를 *비활성화*해야 합니다. 보다 "[SSO\(Single Sign-On\)를 비활성화합니다](#)" .

단계

1. ID 페더레이션 페이지로 이동합니다.
2. ID 페더레이션 사용 * 확인란의 선택을 취소합니다.

OpenLDAP 서버 구성 지침

OpenLDAP 서버를 ID 페더레이션에 사용하려면 OpenLDAP 서버에서 특정 설정을 구성해야 합니다.



Active Directory 또는 Microsoft Entra ID가 아닌 ID 소스의 경우 StorageGRID 외부에서 비활성화된 사용자의 S3 액세스를 자동으로 차단하지 않습니다. S3 액세스를 차단하려면 해당 사용자의 S3 키를 삭제하거나 모든 그룹에서 사용자를 제거하세요.

MemberOf 및 구체화 오버레이

MemberOf 및 구체화 오버레이를 활성화해야 합니다. 자세한 내용은 [에서 역방향 그룹 구성원 유지 관리에 대한 지침을 참조하십시오](http://www.openldap.org/doc/admin24/index.html) ["OpenLDAP 설명서: 버전 2.4 관리자 가이드"].

인덱싱

지정된 인덱스 키워드를 사용하여 다음 OpenLDAP 속성을 구성해야 합니다.

- olcDbIndex: objectClass eq
- olcDbIndex: uid eq,pres,sub
- olcDbIndex: cn eq,pres,sub
- olcDbIndex: entryUUID eq

또한 최적의 성능을 위해 사용자 이름 도움말에 언급된 필드를 인덱싱해야 합니다.

에서 역방향 그룹 구성원 유지 관리에 대한 정보를 ["OpenLDAP 설명서: 버전 2.4 관리자 가이드"](#) 참조하십시오.

관리 그룹을 관리합니다

관리자 그룹을 만들어 하나 이상의 관리자 사용자에 대한 보안 권한을 관리할 수 있습니다. StorageGRID 시스템에 대한 액세스 권한을 부여하려면 사용자가 그룹에 속해야 합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 있습니다. "[특정 액세스 권한](#)"
- 통합 그룹을 가져오려는 경우 ID 페더레이션을 구성하고 통합 그룹이 이미 구성된 ID 소스에 있습니다.

관리자 그룹을 생성합니다

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

마법사에 액세스합니다

단계

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

그룹 유형을 선택합니다

로컬 그룹을 생성하거나 통합 그룹을 가져올 수 있습니다.

- 로컬 사용자에게 권한을 할당하려면 로컬 그룹을 만듭니다.
- 통합 그룹을 생성하여 ID 소스에서 사용자를 가져옵니다.

로컬 그룹

단계

1. 로컬 그룹 * 을 선택합니다.
2. 나중에 필요에 따라 업데이트할 수 있는 그룹의 표시 이름을 입력합니다. 예: "유지 보수 사용자" 또는 "ILM 관리자".
3. 나중에 업데이트할 수 없는 그룹의 고유 이름을 입력합니다.
4. Continue * 를 선택합니다.

통합 그룹

단계

1. 페더레이션 그룹 * 을 선택합니다.
2. 구성된 ID 소스에 표시된 대로 가져올 그룹의 이름을 정확하게 입력합니다.
 - Active Directory 및 Microsoft Entra ID의 경우 sAMAccountName을 사용하세요.
 - OpenLDAP의 경우 CN(일반 이름)을 사용합니다.
 - 다른 LDAP의 경우 LDAP 서버에 적절한 고유한 이름을 사용합니다.
3. Continue * 를 선택합니다.

그룹 권한을 관리합니다

단계

1. 액세스 모드 * 의 경우 그룹의 사용자가 그리드 관리자 및 그리드 관리 API에서 설정을 변경하고 작업을 수행할 수 있는지 또는 설정과 기능만 볼 수 있는지 여부를 선택합니다.
 - * 읽기-쓰기 * (기본값): 사용자는 설정을 변경하고 관리 권한에서 허용하는 작업을 수행할 수 있습니다.
 - * 읽기 전용 *: 사용자는 설정 및 기능만 볼 수 있습니다. 그리드 관리자 또는 그리드 관리 API에서 어떠한 변경이나 작업도 수행할 수 없습니다. 로컬 읽기 전용 사용자는 자신의 암호를 변경할 수 있습니다.



사용자가 여러 그룹에 속해 있고 모든 그룹이 * 읽기 전용 * 으로 설정된 경우 사용자는 선택된 모든 설정 및 기능에 대한 읽기 전용 액세스 권한을 갖게 됩니다.

2. 하나 이상을 선택합니다 "관리자 그룹 권한".

각 그룹에 적어도 하나의 권한을 할당해야 합니다. 그렇지 않으면 그룹에 속한 사용자가 StorageGRID에 로그인할 수 없습니다.

3. 로컬 그룹을 만드는 경우 * 계속 * 을 선택합니다. 통합 그룹을 만드는 경우 * 그룹 생성 * 및 * 마침 * 을 선택합니다.

사용자 추가(로컬 그룹만 해당)

단계

1. 필요에 따라 이 그룹에 대해 하나 이상의 로컬 사용자를 선택합니다.

아직 로컬 사용자를 만들지 않은 경우 사용자를 추가하지 않고 그룹을 저장할 수 있습니다. 사용자 페이지에서 이 그룹을 사용자에게 추가할 수 있습니다. 자세한 내용은 ["사용자 관리"](#) 참조하십시오.

2. Create group * 과 * Finish * 를 선택합니다.

관리 그룹을 보고 편집합니다

기존 그룹에 대한 세부 정보를 보거나 그룹을 수정하거나 그룹을 복제할 수 있습니다.

- 모든 그룹의 기본 정보를 보려면 그룹 페이지의 표를 검토하십시오.
- 특정 그룹에 대한 모든 세부 정보를 보거나 그룹을 편집하려면 * 작업 * 메뉴 또는 세부 정보 페이지를 사용하십시오.

작업	작업 메뉴	세부 정보 페이지
그룹 세부 정보를 봅니다 (로컬 그룹만 해당)	a. 그룹의 확인란을 선택합니다. b. Actions * > * View group details * 를 선택합니다.	테이블에서 그룹 이름을 선택합니다.
표시 이름 편집(로컬 그룹만 해당)	a. 그룹의 확인란을 선택합니다. b. Actions * > * Edit group name * 을 선택합니다. c. 새 이름을 입력합니다. d. 변경 내용 저장 * 을 선택합니다.	a. 세부 정보를 표시할 그룹 이름을 선택합니다. b. 편집 아이콘을 선택합니다  c. 새 이름을 입력합니다. d. 변경 내용 저장 * 을 선택합니다.

작업	작업 메뉴	세부 정보 페이지
액세스 모드 또는 권한을 편집합니다	<ul style="list-style-type: none"> a. 그룹의 확인란을 선택합니다. b. Actions * > * View group details * 를 선택합니다. c. 선택적으로 그룹의 액세스 모드를 변경합니다. d. 선택적으로 을 선택하거나 선택 "관리자 그룹 권한"취소합니다. e. 변경 내용 저장 * 을 선택합니다. 	<ul style="list-style-type: none"> a. 세부 정보를 표시할 그룹 이름을 선택합니다. b. 선택적으로 그룹의 액세스 모드를 변경합니다. c. 선택적으로 을 선택하거나 선택 "관리자 그룹 권한"취소합니다. d. 변경 내용 저장 * 을 선택합니다.

그룹을 복제합니다

단계

1. 그룹의 확인란을 선택합니다.
2. Actions * > * Duplicate group * 을 선택합니다.
3. 복제 그룹 마법사를 완료합니다.

그룹을 삭제합니다

시스템에서 그룹을 제거하고 그룹과 관련된 모든 권한을 제거하려면 관리자 그룹을 삭제할 수 있습니다. 관리자 그룹을 삭제하면 그룹에서 모든 사용자가 제거되지만 사용자는 삭제되지 않습니다.

단계

1. 그룹 페이지에서 제거할 각 그룹에 대한 확인란을 선택합니다.
2. Actions * > * Delete group * 을 선택합니다.
3. 그룹 삭제 * 를 선택합니다.

관리자 그룹 권한

관리자 사용자 그룹을 만들 때 그리드 관리자의 특정 기능에 대한 액세스를 제어하는 권한을 하나 이상 선택합니다. 그런 다음 각 사용자를 이러한 관리 그룹 중 하나 이상에 할당하여 사용자가 수행할 수 있는 작업을 결정할 수 있습니다.

각 그룹에 적어도 하나의 권한을 할당해야 합니다. 그렇지 않으면 해당 그룹에 속한 사용자가 Grid Manager 또는 Grid Management API에 로그인할 수 없습니다.

기본적으로 하나 이상의 사용 권한이 있는 그룹에 속한 사용자는 다음 작업을 수행할 수 있습니다.

- Grid Manager에 로그인합니다
- 대시보드 보기
- 노드 페이지를 봅니다
- 현재 및 해결된 경고를 봅니다

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

사용 권한과 액세스 모드 간의 상호 작용

모든 권한에 대해 그룹의 * 액세스 모드 * 설정은 사용자가 설정을 변경하고 작업을 수행할 수 있는지 또는 관련 설정 및 기능만 볼 수 있는지 여부를 결정합니다. 사용자가 여러 그룹에 속해 있고 모든 그룹이 * 읽기 전용 * 으로 설정된 경우 사용자는 선택된 모든 설정 및 기능에 대한 읽기 전용 액세스 권한을 갖게 됩니다.

다음 섹션에서는 관리자 그룹을 만들거나 편집할 때 할당할 수 있는 권한에 대해 설명합니다. 명시적으로 언급되지 않은 기능을 사용하려면 * 루트 액세스 * 권한이 필요합니다.

루트 액세스

이 권한은 모든 그리드 관리 기능에 대한 액세스를 제공합니다.

테넌트 루트 암호를 변경합니다

이 권한은 테넌트 페이지의 * 루트 암호 변경 * 옵션에 대한 액세스를 제공하므로 테넌트의 로컬 루트 사용자의 암호를 변경할 수 있는 사용자를 제어할 수 있습니다. 이 권한은 S3 키 가져오기 기능이 활성화된 경우 S3 키를 마이그레이션하는 데도 사용됩니다. 이 권한이 없는 사용자는 * 루트 암호 변경 * 옵션을 볼 수 없습니다.



루트 암호 변경 * 옵션이 포함된 테넌트 페이지에 대한 액세스 권한을 부여하려면 * 테넌트 계정 * 권한도 할당합니다.

ILM을 참조하십시오

이 권한은 다음 * ILM * 메뉴 옵션에 대한 액세스를 제공합니다.

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



사용자는 저장 등급을 관리하려면 기타 그리드 구성 권한이 있어야 합니다.

유지 관리

다음 옵션을 사용하려면 사용자에게 유지 관리 권한이 있어야 합니다.

- 구성 > 접근 제어:
 - 그리드 암호
- 구성 > 네트워크:

- S3 끝점 도메인 이름

- 유지관리 > 작업:

- 서비스 해제
- 확장
- 개체 존재 여부 검사
- 복구

- 유지관리 > 시스템:

- 복구 패키지
- 소프트웨어 업데이트

- 지원 > 도구:

- 로그

유지 관리 권한이 없는 사용자는 다음 페이지를 볼 수 있지만 편집할 수는 없습니다.

- 유지관리 > 네트워크:

- DNS 서버
- 그리드 네트워크
- NTP 서버

- 유지관리 > 시스템:

- 라이센스

- 구성 > 네트워크:

- S3 끝점 도메인 이름

- 구성 > 보안:

- 인증서

- 구성 > 모니터링:

- 감사 및 syslog 서버

알림을 관리합니다

이 권한은 알림 관리 옵션에 대한 액세스를 제공합니다. 사용자는 이 권한을 가지고 있어야 Silence, 경고 알림 및 경고 규칙을 관리할 수 있습니다.

메트릭 쿼리

이 권한은 다음에 대한 액세스를 제공합니다.

- 지원 > 도구 > 측정항목 페이지
- Grid Management API의 * Metrics * 섹션을 사용하여 맞춤형 Prometheus 메트릭 쿼리를 수행합니다
- 메트릭이 포함된 Grid Manager 대시보드 카드

개체 메타데이터 조회

이 권한은 * ILM * > * 개체 메타데이터 조회 * 페이지에 대한 액세스를 제공합니다.

기타 그리드 구성

이 권한은 다음과 같은 추가 그리드 구성 옵션에 대한 액세스를 제공합니다.

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

스토리지 어플라이언스 관리자

이 권한은 다음을 제공합니다.

- 그리드 관리자를 통해 스토리지 어플라이언스에서 E-Series SANtricity System Manager에 액세스할 수 있습니다.
- 이러한 작업을 지원하는 어플라이언스에 대한 드라이브 관리 탭에서 문제 해결 및 유지 관리 작업을 수행하는 기능.

테넌트 계정

이 권한은 다음 기능을 제공합니다.

- 테넌트 페이지에 액세스하여 테넌트 계정을 생성, 편집 및 제거할 수 있습니다
- 기존 트래픽 분류 정책을 봅니다
- 테넌트 세부 정보가 포함된 Grid Manager 대시보드 카드를 봅니다

사용자 관리

로컬 및 통합 사용자를 볼 수 있습니다. 로컬 사용자를 만들고 로컬 관리자 그룹에 할당하여 이러한 사용자가 액세스할 수 있는 그리드 관리자 기능을 결정할 수도 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 있습니다. "[특정 액세스 권한](#)"

로컬 사용자를 생성합니다

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

로컬 사용자만 생성할 수 있습니다. 외부 ID 소스를 사용하여 연결된 사용자 및 그룹을 관리합니다.

Grid Manager에는 "root"라는 이름의 미리 정의된 로컬 사용자 한 명이 포함되어 있습니다. 루트 사용자를 제거할 수 없습니다.



SSO(Single Sign-On)가 활성화된 경우 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

마법사에 액세스합니다

단계

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

사용자 자격 증명을 입력합니다

단계

1. 사용자의 전체 이름, 고유한 사용자 이름 및 암호를 입력합니다.
2. 이 사용자가 그리드 관리자 또는 그리드 관리 API에 액세스할 수 없는 경우 * 예 * 를 선택합니다(선택 사항).
3. Continue * 를 선택합니다.

그룹에 할당합니다

단계

1. 필요에 따라 사용자를 하나 이상의 그룹에 할당하여 사용자의 권한을 결정합니다.

아직 그룹을 만들지 않은 경우 그룹을 선택하지 않고 사용자를 저장할 수 있습니다. 이 사용자를 그룹 페이지의 그룹에 추가할 수 있습니다.

사용자가 여러 그룹에 속한 경우 권한은 누적됩니다. 자세한 내용은 ["관리 그룹을 관리합니다"](#) 참조하십시오.

2. Create user * 를 선택하고 * Finish * 를 선택합니다.

로컬 사용자를 보고 편집합니다

기존 로컬 및 통합 사용자에 대한 세부 정보를 볼 수 있습니다. 로컬 사용자를 수정하여 사용자의 전체 이름, 암호 또는 그룹 구성원을 변경할 수 있습니다. 사용자가 그리드 관리자 및 그리드 관리 API에 일시적으로 액세스하지 못하도록 할 수도 있습니다.

로컬 사용자만 편집할 수 있습니다. 외부 ID 소스를 사용하여 페더레이션 사용자를 관리합니다.

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

다음에 사용자가 로그아웃한 다음 다시 그리드 관리자에 로그인할 때 모든 편집 내용이 적용됩니다.



로컬 사용자는 Grid Manager 배너에 있는 * 암호 변경 * 옵션을 사용하여 자신의 암호를 변경할 수 있습니다.

작업	작업 메뉴	세부 정보 페이지
사용자 세부 정보를 봅니다	<ul style="list-style-type: none"> a. 사용자의 확인란을 선택합니다. b. Actions * > * View user details * 를 선택합니다. 	테이블에서 사용자 이름을 선택합니다.
전체 이름 편집(로컬 사용자만 해당)	<ul style="list-style-type: none"> a. 사용자의 확인란을 선택합니다. b. 작업 * > * 전체 이름 편집 * 을 선택합니다. c. 새 이름을 입력합니다. d. 변경 내용 저장 * 을 선택합니다. 	<ul style="list-style-type: none"> a. 사용자 이름을 선택하여 세부 정보를 표시합니다. b. 편집 아이콘을 선택합니다 . c. 새 이름을 입력합니다. d. 변경 내용 저장 * 을 선택합니다.
StorageGRID 액세스를 거부하거나 허용합니다	<ul style="list-style-type: none"> a. 사용자의 확인란을 선택합니다. b. Actions * > * View user details * 를 선택합니다. c. 액세스 탭을 선택합니다. d. 사용자가 그리드 관리자 또는 그리드 관리 API에 로그인하지 못하도록 하려면 * 예 * 를 선택하고, 사용자가 로그인할 수 있도록 하려면 * 아니요 * 를 선택합니다. e. 변경 내용 저장 * 을 선택합니다. 	<ul style="list-style-type: none"> a. 사용자 이름을 선택하여 세부 정보를 표시합니다. b. 액세스 탭을 선택합니다. c. 사용자가 그리드 관리자 또는 그리드 관리 API에 로그인하지 못하도록 하려면 * 예 * 를 선택하고, 사용자가 로그인할 수 있도록 하려면 * 아니요 * 를 선택합니다. d. 변경 내용 저장 * 을 선택합니다.
암호 변경(로컬 사용자만 해당)	<ul style="list-style-type: none"> a. 사용자의 확인란을 선택합니다. b. Actions * > * View user details * 를 선택합니다. c. 암호 탭을 선택합니다. d. 새 암호를 입력합니다. e. 암호 변경 * 을 선택합니다. 	<ul style="list-style-type: none"> a. 사용자 이름을 선택하여 세부 정보를 표시합니다. b. 암호 탭을 선택합니다. c. 새 암호를 입력합니다. d. 암호 변경 * 을 선택합니다.
그룹 변경(로컬 사용자만 해당)	<ul style="list-style-type: none"> a. 사용자의 확인란을 선택합니다. b. Actions * > * View user details * 를 선택합니다. c. 그룹 탭을 선택합니다. d. 필요에 따라 그룹 이름 뒤에 있는 링크를 선택하여 새 브라우저 탭에서 그룹의 세부 정보를 봅니다. e. 다른 그룹을 선택하려면 * Edit groups * 를 선택합니다. f. 변경 내용 저장 * 을 선택합니다. 	<ul style="list-style-type: none"> a. 사용자 이름을 선택하여 세부 정보를 표시합니다. b. 그룹 탭을 선택합니다. c. 필요에 따라 그룹 이름 뒤에 있는 링크를 선택하여 새 브라우저 탭에서 그룹의 세부 정보를 봅니다. d. 다른 그룹을 선택하려면 * Edit groups * 를 선택합니다. e. 변경 내용 저장 * 을 선택합니다.

페더레이션 사용자 가져오기

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

단계

1. 구성 > 액세스 제어 > *관리자 사용자*를 선택합니다.
2. *연합 사용자 가져오기*를 선택합니다.
3. 하나 이상의 페더레이션 사용자에 대한 UUID 또는 사용자 이름을 입력하세요.

여러 항목이 있는 경우 각 UUID 또는 사용자 이름을 새 줄에 추가합니다.

4. *가져오기*를 선택하세요.

한 명 이상의 사용자에 대해 사용자 필드로의 가져오기가 실패하면 다음 단계를 수행하세요.

- a. *사용자를 가져오지 않음*을 확장하고 *사용자 복사*를 선택합니다.
- b. 이전*을 선택하고 복사한 사용자를 *연합 사용자 가져오기 대화 상자*에 붙여넣어 가져오기를 다시 시도합니다.

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

사용자를 복제합니다

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

단계

1. 사용자의 확인란을 선택합니다.
2. Actions * > * Duplicate user * 를 선택합니다.
3. 사용자 복제 마법사를 완료합니다.

사용자를 삭제합니다

로컬 사용자를 삭제하여 해당 사용자를 시스템에서 영구적으로 제거할 수 있습니다.



루트 사용자는 삭제할 수 없습니다.

단계

1. 사용자 페이지에서 제거할 각 사용자에 대한 확인란을 선택합니다.
2. Actions * > * Delete user * 를 선택합니다.
3. 사용자 삭제 * 를 선택합니다.

SSO(Single Sign-On) 사용

SSO 작동 방식

SSO(Single Sign-On)가 활성화된 경우 사용자는 조직에서 구현한 SSO 로그인 프로세스를

통해 자격 증명이 승인된 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 사용하여 SSO(Single Sign-On)를 지원합니다.

SSO(Single Sign-On)를 활성화하기 전에 SSO를 사용할 때 StorageGRID 로그인 및 로그아웃 프로세스가 어떻게 영향을 받는지 검토하십시오.

SSO가 활성화되면 로그인하십시오

SSO가 활성화되어 있고 StorageGRID에 로그인하면 조직의 SSO 페이지로 리디렉션되어 자격 증명을 검증합니다.

단계

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

StorageGRID 로그인 페이지가 나타납니다.

- 이 브라우저에서 처음으로 URL에 접속하는 경우 계정 ID를 입력하라는 메시지가 표시됩니다.
- 이전에 Grid Manager나 Tenant Manager에 접속한 적이 있는 경우 최근 계정을 선택하거나 계정 ID를 입력하라는 메시지가 표시됩니다.



테넌트 계정에 대한 전체 URL(즉, 정규화된 도메인 이름 또는 IP 주소 다음에 가오는 경우)을 입력하면 StorageGRID 로그인 페이지가 표시되지 않습니다 /?accountId=20-digit-account-id. 대신 조직의 SSO 로그인 페이지로 바로 리디렉션됩니다 [SSO 자격 증명으로 로그인합니다](#).

2. 그리드 관리자 또는 테넌트 관리자에 액세스할지 여부를 지정합니다.

- Grid Manager에 액세스하려면 * Account ID * 필드를 비워 두고 계정 ID로 * 0 * 을 입력하거나, 최근 계정 목록에 * Grid Manager * 를 선택합니다.
- Tenant Manager에 액세스하려면 20자리 테넌트 계정 ID를 입력하거나 최근 계정 목록에 나타나는 경우 이름으로 Tenant를 선택합니다.

3. 로그인 * 을 선택합니다

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

4. SSO 자격 증명으로 로그인합니다.

SSO 자격 증명이 올바른 경우:

- a. IDP(Identity Provider)는 StorageGRID에 인증 응답을 제공합니다.
- b. StorageGRID는 인증 응답을 검증합니다.
- c. 응답이 유효하고 StorageGRID 액세스 권한이 있는 통합 그룹에 속해 있는 경우 선택한 계정에 따라 그리드 관리자 또는 테넌트 관리자에 로그인됩니다.



서비스 계정에 액세스할 수 없는 경우 StorageGRID 액세스 권한이 있는 통합 그룹에 속한 기존 사용자라면 계속 로그인할 수 있습니다.

- 필요한 경우 다른 관리 노드에 액세스하거나 적절한 권한이 있는 경우 그리드 관리자 또는 테넌트 관리자에 액세스합니다.

SSO 자격 증명을 다시 입력하지 않아도 됩니다.

SSO가 활성화되면 로그아웃합니다

StorageGRID에 대해 SSO가 활성화된 경우 로그아웃할 때 발생하는 작업은 로그인한 대상 및 로그아웃 위치에 따라 달라집니다.

단계

- 사용자 인터페이스의 오른쪽 상단 모서리에 있는 * 로그아웃 * 링크를 찾습니다.
- 로그아웃 * 을 선택합니다.

StorageGRID 로그인 페이지가 나타납니다. 최근 계정 * 드롭다운은 * 그리드 관리자 * 또는 테넌트 이름을 포함하도록 업데이트되므로 나중에 이러한 사용자 인터페이스에 보다 빠르게 액세스할 수 있습니다.



이 표에는 단일 브라우저 세션을 사용하는 경우 로그아웃할 때 발생하는 동작이 요약되어 있습니다. 여러 브라우저 세션에서 StorageGRID에 로그인한 경우 모든 브라우저 세션에서 별도로 로그아웃해야 합니다.

에 로그인한 경우...	에서 로그아웃합니다.	에서 로그아웃되었습니다...
하나 이상의 관리 노드에서 그리드 관리자	모든 관리 노드의 그리드 관리자	모든 관리 노드의 그리드 관리자 참고: SSO에 Entra ID를 사용하는 경우 모든 관리 노드에서 로그아웃하는 데 몇 분이 걸릴 수 있습니다.
하나 이상의 관리 노드에서 테넌트 관리자	모든 관리 노드의 테넌트 관리자	모든 관리 노드의 테넌트 관리자
Grid Manager와 Tenant Manager 모두	그리드 관리자	그리드 관리자 전용. SSO에서 로그아웃하려면 테넌트 관리자에서 로그아웃해야 합니다.

SSO에 대한 요구 사항 및 고려 사항

StorageGRID 시스템에 대해 SSO(Single Sign-On)를 활성화하기 전에 요구 사항 및 고려 사항을 검토하십시오.

ID 공급자 요구 사항

StorageGRID는 다음 SSO ID 공급자(IDP)를 지원합니다.

- AD FS(Active Directory Federation Service)
- 마이크로소프트 엔트라 ID

- PingFederate(PingFederate)

SSO ID 공급자를 구성하려면 먼저 StorageGRID 시스템에 대한 ID 페더레이션을 구성해야 합니다. ID 페더레이션에 사용하는 LDAP 서비스 유형은 구현할 수 있는 SSO 유형을 제어합니다.

구성된 LDAP 서비스 유형입니다	SSO ID 공급자에 대한 옵션
Active Directory를 클릭합니다	<ul style="list-style-type: none"> • Active Directory를 클릭합니다 • 엔트라 ID • PingFederate(PingFederate)
엔트라 ID	엔트라 ID

AD FS 요구 사항

다음 버전의 AD FS를 사용할 수 있습니다.

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



Windows Server 2016은, 이상을 사용해야 "["KB3201845 업데이트"](#) 합니다.

추가 요구 사항

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

Entra ID에 대한 고려 사항

SSO 유형으로 Entra ID를 사용하고 사용자의 사용자 주체 이름이 접두사로 sAMAccountName을 사용하지 않는 경우 StorageGRID LDAP 서버와 연결이 끊어지면 로그인 문제가 발생할 수 있습니다. 사용자가 로그인할 수 있도록 하려면 LDAP 서버에 대한 연결을 복원해야 합니다.

서버 인증서 요구 사항

기본적으로 StorageGRID 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 구성하는 경우 StorageGRID 요청에 대한 서명 인증서로 서버 인증서를 사용합니다.

아직 하지 않았다면 "["관리 인터페이스에 대한 사용자 지정 인증서를 구성했습니다"](#)" 지금 그렇게 해야 합니다. 사용자 지정 서버 인증서는 모든 관리 노드에 사용되며 모든 StorageGRID 신뢰할 수 있는 당사자, 엔터프라이즈 응용 프로그램 또는 SP 연결에서 사용할 수 있습니다.



사용 중인 신뢰, 엔터프라이즈 응용 프로그램 또는 SP 연결에서 관리 노드의 기본 서버 인증서를 사용하는 것은 권장되지 않습니다. 노드가 실패하고 복구되면 새로운 기본 서버 인증서가 생성됩니다. 복구된 노드에 로그인하려면 먼저 신뢰할 수 있는 당사자 신뢰, 엔터프라이즈 애플리케이션 또는 SP 연결을 새 인증서로 업데이트해야 합니다.

노드의 명령 셸에 로그인하고 디렉터리로 이동하여 관리자 노드의 서버 인증서에 액세스할 수 `/var/local/mgmt-api` 있습니다. 사용자 지정 서버 인증서의 이름은 `custom-server.crt`입니다. 노드의 기본 서버 인증서 이름은 `server.crt`입니다.

포트 요구 사항

제한된 Grid Manager 또는 테넌트 관리자 포트에서는 SSO(Single Sign-On)를 사용할 수 없습니다. 사용자가 SSO(Single Sign-On)로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다. 을 "외부 방화벽에서 액세스를 제어합니다" 참조하십시오.

페더레이션 사용자가 로그인할 수 있는지 확인합니다

SSO(Single Sign-On)를 활성화하기 전에 하나 이상의 통합 사용자가 Grid Manager에 로그인하고 기존 테넌트 계정에 대한 테넌트 관리자에 로그인할 수 있는지 확인해야 합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "지원되는 웹 브라우저"
- 있습니다. "특정 액세스 권한"
- ID 페더레이션을 이미 구성했습니다.

단계

1. 기존 테넌트 계정이 있는 경우 해당 테넌트가 자신의 ID 소스를 사용하고 있지 않은지 확인합니다.



SSO를 활성화하면 테넌트 관리자에 구성된 ID 소스가 그리드 관리자에 구성된 ID 소스에 의해 재정의됩니다. 테넌트의 ID 소스에 속하는 사용자는 Grid Manager ID 소스의 계정이 없으면 더 이상 로그인할 수 없습니다.

- a. 각 테넌트 계정의 테넌트 관리자에 로그인합니다.
b. 액세스 관리 > *ID 페더레이션*을 선택합니다.
c. ID 페더레이션 사용 * 확인란이 선택되지 않았는지 확인합니다.
d. 이 경우 이 테넌트 계정에 사용 중인 모든 통합 그룹이 더 이상 필요하지 않은지 확인하고 확인란을 선택 취소하고 * Save * 를 선택합니다.
2. 통합 사용자가 Grid Manager에 액세스할 수 있는지 확인합니다.
 - a. 그리드 관리자에서 구성 > 액세스 제어 > *관리자 그룹*을 선택합니다.
 - b. Active Directory ID 소스에서 하나 이상의 통합 그룹을 가져오고 루트 액세스 권한이 할당되었는지 확인합니다.
 - c. 로그아웃합니다.
 - d. 통합 그룹의 사용자로 그리드 관리자에 다시 로그인할 수 있는지 확인합니다.
3. 기존 테넌트 계정이 있는 경우 루트 액세스 권한이 있는 페더레이션 사용자가 로그인할 수 있는지 확인합니다.
 - a. 그리드 관리자에서 *테넌트*를 선택합니다.

- b. 테넌트 계정을 선택하고 * 작업 * > * 편집 * 을 선택합니다.
- c. 세부 정보 입력 탭에서 * 계속 * 을 선택합니다.
- d. Use own identity source * (고유 ID 소스 사용 *) 확인란을 선택한 경우, 상자의 선택을 취소하고 * Save * (저장 *)를 선택합니다.

테넌트 페이지가 나타납니다.

- e. 테넌트 계정을 선택하고 * 로그인 * 을 선택한 다음 테넌트 계정에 로컬 루트 사용자로 로그인합니다.
- f. 테넌트 관리자에서 액세스 관리 > *그룹*을 선택합니다.
- g. Grid Manager에서 하나 이상의 통합 그룹에 이 테넌트에 대한 루트 액세스 권한이 할당되었는지 확인합니다.
- h. 로그아웃합니다.
- i. 통합 그룹의 사용자로 테넌트에 다시 로그인할 수 있는지 확인합니다.

관련 정보

- "[SSO\(Single Sign-On\)에 대한 요구 사항 및 고려 사항](#)"
- "[관리 그룹을 관리합니다](#)"
- "[테넌트 계정을 사용합니다](#)"

SSO 구성

SSO 구성 마법사를 따라 샌드박스 모드로 들어가서 모든 StorageGRID 사용자에 대해 SSO(단일 로그인)를 활성화하기 전에 SSO를 구성하고 테스트할 수 있습니다. SSO가 활성화된 후 구성을 변경하거나 다시 테스트해야 할 때 샌드박스 모드로 돌아갈 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 이 "[루트 액세스 권한](#)"입니다.
- StorageGRID 시스템에 대해 ID 페더레이션을 구성했습니다.
- ID 페더레이션 *LDAP 서비스 유형*의 경우, 사용하려는 SSO ID 공급자에 따라 Active Directory 또는 Entra ID를 선택했습니다.

구성된 LDAP 서비스 유형입니다	SSO ID 공급자에 대한 옵션
AD FS(Active Directory Federation Service)	<ul style="list-style-type: none"> • Active Directory를 클릭합니다 • 엔트라 ID • PingFederate(PingFederate)
엔트라 ID	엔트라 ID

이 작업에 대해

SSO가 활성화되어 있고 사용자가 관리자 노드에 로그인을 시도하면 StorageGRID는 인증 요청을 SSO ID 공급자에 보냅니다. 또한 SSO ID 공급자는 인증 요청이 성공했는지 여부를 나타내는 인증 응답을 StorageGRID로 다시

보냅니다. 성공적인 요청의 경우:

- Active Directory 또는 PingFederate의 응답에는 사용자의 UUID(Universally Unique Identifier)가 포함됩니다.
- Entra ID의 응답에는 UPN(사용자 주체 이름)이 포함되어 있습니다.

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

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

샌드박스 모드를 사용하면 이러한 왕복 구성을 쉽게 수행하고 SSO를 활성화하기 전에 모든 설정을 테스트할 수 있습니다. 샌드박스 모드를 사용하는 경우 사용자는 SSO를 사용하여 로그인할 수 없습니다.

마법사에 액세스합니다

단계

1. 구성 > 액세스 제어 > *단일 로그인*을 선택합니다. Single Sign-On 페이지가 나타납니다.



SSO 설정 구성 버튼이 비활성화된 경우 ID 공급자를 페더레이션 ID 소스로 구성했는지 확인하세요.
"SSO(Single Sign-On)에 대한 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 ID 공급자에 대한 *페더레이션 서비스 이름*을 Active Directory 페더레이션 서비스(AD FS)에 표시된 대로 정확하게 입력합니다.



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

3. ID 공급자가 StorageGRID 요청에 대한 응답으로 SSO 구성 정보를 보낼 때 연결을 보호하는 데 사용할 TLS 인증서를 지정합니다.
 - *운영 체제 CA 인증서 사용*: 운영 체제에 설치된 기본 CA 인증서를 사용하여 연결을 보호합니다.
 - *사용자 지정 CA 인증서 사용*: 사용자 지정 CA 인증서를 사용하여 연결을 보호합니다.

이 설정을 선택한 경우 사용자 지정 인증서의 텍스트를 복사하여 *CA 인증서* 텍스트 상자에 붙여 넣습니다.

◦ *TLS* 사용 안 함: TLS 인증서를 사용하여 연결을 보호하지 마십시오.



CA 인증서를 변경하는 경우 즉시 "관리 노드에서 mgmt-API 서비스를 다시 시작합니다" 그리드 관리자에서 성공적인 SSO를 테스트합니다.

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

신뢰하는 당사자 식별자 제공

1. 선택한 SSO 유형에 따라 신뢰 당사자 식별자 제공 페이지에서 필드를 완성합니다.

Active Directory를 클릭합니다

- a. StorageGRID에 대한 *신뢰 당사자 식별자*를 지정합니다. 이 값은 AD FS에서 각 신뢰 당사자 신뢰에 사용하는 이름을 제어합니다.
 - 예를 들어 그리드에 관리자 노드가 하나만 있고 앞으로 관리자 노드를 더 추가할 계획이 없는 경우 또는 StorageGRID를 입력합니다. SG
 - 그리드에 두 개 이상의 관리 노드가 포함된 경우 다음 문자열을 포함합니다. [HOSTNAME] 식별자에서. 예를 들어, SG-[HOSTNAME]. 이 문자열을 포함하면 노드의 호스트 이름을 기반으로 그리드의 각 관리 노드에 대한 신뢰 당사자 식별자를 보여주는 표가 생성됩니다.



StorageGRID 시스템의 각 관리 노드에 대한 신뢰할 수 있는 상대 신뢰를 만들어야 합니다. 각 관리 노드에 대한 신뢰할 수 있는 당사자 덕분에 사용자는 모든 관리 노드에 안전하게 로그인할 수 있습니다.

- b. *저장하고 샌드박스 모드로 들어가기*를 선택하세요.

엔트라 ID

- a. 엔터프라이즈 애플리케이션 섹션에서 StorageGRID에 대한 *엔터프라이즈 애플리케이션 이름*을 지정합니다. 이 값은 Entra ID에서 각 엔터프라이즈 애플리케이션에 사용하는 이름을 제어합니다.
 - 예를 들어 그리드에 관리자 노드가 하나만 있고 앞으로 관리자 노드를 더 추가할 계획이 없는 경우 또는 StorageGRID를 입력합니다. SG
 - 그리드에 두 개 이상의 관리 노드가 포함된 경우 다음 문자열을 포함합니다. [HOSTNAME] 식별자에서. 예를 들어, SG-[HOSTNAME]. 이 문자열을 포함하면 노드의 호스트 이름을 기반으로 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션 이름을 보여주는 표가 생성됩니다.



StorageGRID 시스템의 각 관리 노드에 대해 엔터프라이즈 애플리케이션을 만들어야 합니다. 각 관리 노드에 엔터프라이즈 애플리케이션을 사용하면 사용자가 관리자 노드에 안전하게 로그인할 수 있습니다.

- b. 다음 단계를 따르세요 "[Entra ID에서 엔터프라이즈 애플리케이션 만들기](#)" 표에 나열된 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 생성합니다.
- 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 *저장 및 샌드박스 모드 전환*을 선택합니다.

PingFederate(PingFederate)

- a. 서비스 공급자(SP) 섹션에서 StorageGRID에 대한 *SP 접속 ID*를 지정합니다. 이 값은 PingFederate의 각 SP 연결에 사용할 이름을 제어합니다.
 - 예를 들어 그리드에 관리자 노드가 하나만 있고 앞으로 관리자 노드를 더 추가할 계획이 없는 경우 또는 StorageGRID를 입력합니다. SG
 - 그리드에 두 개 이상의 관리 노드가 포함된 경우 다음 문자열을 포함합니다. [HOSTNAME] 식별자에서. 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 접속을 생성해야 합니다. 각 관리 노드에 대해 SP를 연결하면 사용자가 관리자 노드에 안전하게 로그인할 수 있습니다.

- b. Federation metadata URL * 필드에서 각 관리 노드에 대한 페더레이션 메타데이터 URL을 지정합니다.

다음 형식을 사용합니다.

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

- c. *저장하고 샌드박스 모드로 들어가기*를 선택하세요.

신뢰할 수 있는 파티 트러스트, 엔터프라이즈 애플리케이션 또는 **SP** 연결을 구성합니다

구성을 저장하고 샌드박스 모드로 들어간 후, 선택한 SSO 유형에 대한 구성을 완료하고 테스트할 수 있습니다.

StorageGRID 필요한 만큼 샌드박스 모드를 유지할 수 있습니다. 하지만 연합 사용자와 로컬 사용자만 로그인할 수 있습니다.

Active Directory를 클릭합니다

단계

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

테이블에 표시된 각 관리 노드에 대해 하나의 신뢰를 만들어야 합니다.

자세한 내용은 ["AD FS에서 기반 당사자 트러스트를 생성합니다"](#) 참조하십시오.

엔트라 ID

단계

1. 현재 로그인한 Admin Node의 Single Sign-On 페이지에서 SAML 메타데이터를 다운로드하고 저장할 버튼을 선택합니다.
2. 그리드에서 다른 관리 노드에 대해 다음 단계를 반복합니다.
 - a. 노드에 로그인합니다.
 - b. 구성 > 액세스 제어 > *단일 로그인*을 선택합니다.
 - c. 해당 노드에 대한 SAML 메타데이터를 다운로드하고 저장합니다.
3. Azure Portal로 이동합니다.
4. 다음 단계를 따르세요 "[Entra ID에서 엔터프라이즈 애플리케이션 만들기](#)" 각 관리 노드의 SAML 메타데이터 파일을 해당 Entra ID 엔터프라이즈 애플리케이션에 업로드합니다.

PingFederate(PingFederate)

단계

1. 현재 로그인한 Admin Node의 Single Sign-On 페이지에서 SAML 메타데이터를 다운로드하고 저장할 버튼을 선택합니다.
2. 그리드에서 다른 관리 노드에 대해 다음 단계를 반복합니다.
 - a. 노드에 로그인합니다.
 - b. 구성 > 액세스 제어 > *단일 로그인*을 선택합니다.
 - c. 해당 노드에 대한 SAML 메타데이터를 다운로드하고 저장합니다.
3. PingFederate로 이동합니다.
4. "[StorageGRID에 대한 SP\(서비스 공급자\) 연결을 하나 이상 생성합니다](#)". 각 관리 노드의 SP 연결 ID(SSO 구성 페이지의 표에 표시됨)와 해당 관리 노드에 대해 다운로드한 SAML 메타데이터를 사용합니다.

표에 표시된 각 관리 노드에 대해 하나의 SP 접속을 생성해야 합니다.

테스트 구성

StorageGRID 시스템 전체에 대해 단일 로그인 사용을 강제로 적용하기 전에 각 관리 노드에 대해 단일 로그인 및 단일 로그아웃이 올바르게 구성되었는지 확인하세요.

Active Directory를 클릭합니다

단계

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

URL은 * 패더레이션 서비스 이름 * 필드에 입력한 값에서 파생됩니다.

2. ID 공급자의 로그인 페이지에 액세스하려면 링크를 선택하거나 URL을 복사하여 브라우저에 붙여 넣으십시오.
3. SSO를 사용하여 StorageGRID에 로그인할 수 있는지 확인하려면 * 다음 사이트 중 하나에 로그인 * 을 선택하고, 기본 관리자 노드에 대한 보조 당사자 식별자를 선택한 다음 * 로그인 * 을 선택합니다.
4. 통합 사용자 이름과 암호를 입력합니다.
 - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 나타납니다.
 - SSO 작업이 실패하면 오류 메시지가 나타납니다. 문제를 해결하고 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
5. 이 단계를 반복하여 그리드의 각 관리 노드에 대한 SSO 연결을 확인합니다.

엔트라 ID

단계

1. Azure 포털의 Single Sign-On 페이지로 이동합니다.
2. 이 응용 프로그램 테스트 * 를 선택합니다.
3. 통합 사용자의 자격 증명을 입력합니다.
 - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 나타납니다.
 - SSO 작업이 실패하면 오류 메시지가 나타납니다. 문제를 해결하고 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
4. 이 단계를 반복하여 그리드의 각 관리 노드에 대한 SSO 연결을 확인합니다.

PingFederate(PingFederate)

단계

1. SSO 구성 페이지에서 샌드박스 모드 메시지의 첫 번째 링크를 선택합니다.
링크를 한 번에 하나씩 선택하여 테스트합니다.
2. 통합 사용자의 자격 증명을 입력합니다.
 - SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 나타납니다.
 - SSO 작업이 실패하면 오류 메시지가 나타납니다. 문제를 해결하고 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.
3. 다음 링크를 선택하여 그리드의 각 관리 노드에 대한 SSO 연결을 확인합니다.

페이지 만료 메시지가 표시되면 브라우저에서 * 뒤로 * 버튼을 선택하고 자격 증명을 다시 제출하십시오.

SSO(Single Sign-On)를 활성화합니다

SSO를 사용하여 각 관리 노드에 로그인할 수 있는지 확인한 후 전체 StorageGRID 시스템에 대해 SSO를 활성화할 수 있습니다.



SSO가 활성화된 경우 모든 사용자는 SSO를 사용하여 Grid Manager, Tenant Manager, Grid Management API 및 Tenant Management API에 액세스해야 합니다. 로컬 사용자는 더 이상 StorageGRID에 액세스할 수 없습니다.

단계

1. SSO 구성 마법사의 테스트 구성 단계에서 *SSO 사용*을 선택합니다.
2. 경고 메시지를 검토하고 *SSO 사용*을 선택하세요.

이제 Single Sign-On이 활성화되었습니다. Single Sign-On 페이지가 나타나고 방금 구성한 SSO에 대한 세부 정보가 포함됩니다.

3. 구성을 편집하려면 *편집*을 선택하세요.
4. Single Sign-On을 비활성화하려면 *SSO 비활성화*를 선택하세요.



Azure Portal을 사용하고 Entra ID에 액세스하는 데 사용하는 것과 동일한 컴퓨터에서 StorageGRID에 액세스하는 경우 Azure Portal 사용자가 권한이 있는 StorageGRID 사용자(StorageGRID로 가져온 페더레이션 그룹의 사용자)인지 확인하거나 StorageGRID에 로그인을 시도하기 전에 Azure Portal에서 로그아웃하세요.

AD FS에서 기반 당사자 트러스트를 생성합니다

AD FS(Active Directory Federation Services)를 사용하여 시스템의 각 관리 노드에 대한 기반 당사자 신뢰를 만들어야 합니다. PowerShell 명령을 사용하거나, StorageGRID에서 SAML 메타데이터를 가져오거나, 데이터를 수동으로 입력하여 의존할 수 있는 회사 트러스트를 만들 수 있습니다.

시작하기 전에

- StorageGRID에 대해 Single Sign-On을 구성하고 SSO 유형으로 * AD FS * 를 선택했습니다.
- 당신은 가지고 있다 "샌드박스 모드로 들어갔습니다" 그리드 관리자에서.
- 시스템의 각 관리 노드에 대한 정규화된 도메인 이름(또는 IP 주소)과 신뢰 당사자 식별자를 알고 있습니다. 이러한 값은 StorageGRID SSO 구성 페이지의 관리 노드 세부 정보 표에서 찾을 수 있습니다.



StorageGRID 시스템의 각 관리 노드에 대한 신뢰할 수 있는 상대 신뢰를 만들어야 합니다. 각 관리 노드에 대한 신뢰할 수 있는 당사자 덕분에 사용자는 모든 관리 노드에 안전하게 로그인할 수 있습니다.

- AD FS에서 기반 당사자 트러스트를 만드는 경험이 있거나 Microsoft AD FS 문서에 액세스할 수 있습니다.
- AD FS 관리 스냅인을 사용하고 있으며 사용자는 Administrators 그룹에 속해 있습니다.
- 수동으로 신뢰할 수 있는 상대 신뢰를 만드는 경우 StorageGRID 관리 인터페이스에 대해 업로드된 사용자 지정 인증서가 있거나 명령 셸에서 관리 노드에 로그인하는 방법을 알고 있어야 합니다.

이 작업에 대해

이 지침은 Windows Server 2016 AD FS에 적용됩니다. 다른 버전의 AD FS를 사용하는 경우 절차에 약간의 차이가 있을 수 있습니다. 질문이 있는 경우 Microsoft AD FS 설명서를 참조하십시오.

Windows PowerShell을 사용하여 신뢰할 수 있는 사용자 신뢰를 만듭니다

Windows PowerShell을 사용하여 하나 이상의 신뢰할 수 있는 파티 트러스트를 빠르게 만들 수 있습니다.

단계

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

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

- 의 경우 Admin_Node_Identifier 단일 사인온 페이지에 표시된 대로 관리자 노드의 종속 당사자 식별자를 입력합니다. 'SG-DC1-ADM1' 예를 들어,
- 의 경우 Admin_Node_FQDN 동일한 관리자 노드에 대해 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)

3. Windows Server Manager에서 * Tools * > * AD FS Management * 를 선택합니다.

AD FS 관리 도구가 나타납니다.

4. AD FS * > * 기반 당사자 신뢰 * 를 선택합니다.

신뢰할 수 있는 당사자 목록이 나타납니다.

5. 새로 만든 신뢰할 수 있는 상대 신뢰에 액세스 제어 정책 추가:

- a. 방금 만든 신뢰할 수 있는 상대자를 찾습니다.
- b. 트러스트를 마우스 오른쪽 단추로 클릭하고 * 액세스 제어 정책 편집 * 을 선택합니다.
- c. 액세스 제어 정책을 선택합니다.
- d. Apply * 를 선택하고 * OK * 를 선택합니다

6. 새로 생성된 신뢰할 수 있는 당사자 신탁에 클레임 발급 정책 추가:

- a. 방금 만든 신뢰할 수 있는 상대자를 찾습니다.
- b. 신뢰를 마우스 오른쪽 버튼으로 클릭하고 * 클레임 발급 정책 편집 * 을 선택합니다.
- c. 규칙 추가 * 를 선택합니다.
- d. 규칙 템플릿 선택 페이지의 목록에서 * 청구로 LDAP 속성 보내기 * 를 선택하고 * 다음 * 을 선택합니다.
- e. 규칙 구성 페이지에서 이 규칙의 표시 이름을 입력합니다.

예를 들어 * objectGUID를 이름 ID * 로, * UPN을 이름 ID * 로 지정합니다.

- f. 특성 저장소의 경우 * Active Directory * 를 선택합니다.
- g. Mapping 테이블의 LDAP Attribute 열에서 * objectGUID * 를 입력하거나 * User-Principal-Name * 을 선택합니다.

- h. 매핑 테이블의 발신 클레임 유형 열에서 드롭다운 목록에서 * 이름 ID * 를 선택합니다.
- i. 마침 * 을 선택하고 * 확인 * 을 선택합니다.

7. 메타데이터를 성공적으로 가져왔는지 확인합니다.

- a. 신뢰할 수 있는 상대 신뢰를 마우스 오른쪽 단추로 클릭하여 속성을 엽니다.
- b. Endpoints *, * Identifiers * 및 * Signature * 탭의 필드가 채워져 있는지 확인합니다.

메타데이터가 누락된 경우 페더레이션 메타데이터 주소가 올바른지 확인하거나 값을 수동으로 입력합니다.

8. 이 단계를 반복하여 StorageGRID 시스템의 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 구성합니다.
9. 완료되면 StorageGRID 로 돌아가서 "[모든 신뢰 당사자 트러스트를 테스트합니다](#)" 올바르게 구성되었는지 확인하세요.

페더레이션 메타데이터를 가져와 사용 상대 신뢰를 만듭니다

각 관리 노드에 대한 SAML 메타데이터에 액세스하여 각 의존자 신뢰의 값을 가져올 수 있습니다.

단계

1. Windows Server Manager에서 * Tools * 를 선택한 다음 * AD FS Management * 를 선택합니다.
2. 작업에서 * 신뢰할 수 있는 당사자 신뢰 추가 * 를 선택합니다.
3. 시작 페이지에서 * 클레임 인식 * 을 선택하고 * 시작 * 을 선택합니다.
4. 온라인 또는 로컬 네트워크에 게시된 의존자에 대한 데이터 가져오기 * 를 선택합니다.
5. Federation 메타데이터 주소(호스트 이름 또는 URL) * 에 이 관리 노드에 대한 SAML 메타데이터의 위치를 입력합니다.

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

의 경우 Admin_Node_FQDN 동일한 관리자 노드에 대해 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)

6. 신뢰할 수 있는 당사자 신뢰 마법사를 완료하고 신뢰할 수 있는 상대 신뢰를 저장한 다음 마법사를 닫습니다.



표시 이름을 입력할 때 그리드 관리자의 단일 사인온 페이지에 나타나는 것과 동일하게 관리 노드에 대한 기반 당사자 식별자를 사용합니다. `SG-DC1-ADM1` 예를 들어,

7. 청구 규칙 추가:

- a. 신뢰를 마우스 오른쪽 버튼으로 클릭하고 * 클레임 발급 정책 편집 * 을 선택합니다.
- b. 규칙 추가 * 선택:
- c. 규칙 템플릿 선택 페이지의 목록에서 * 청구로 LDAP 속성 보내기 * 를 선택하고 * 다음 * 을 선택합니다.
- d. 규칙 구성 페이지에서 이 규칙의 표시 이름을 입력합니다.

예를 들어 * objectGUID를 이름 ID * 로, * UPN을 이름 ID * 로 지정합니다.

- e. 특성 저장소의 경우 * Active Directory * 를 선택합니다.

- f. Mapping 테이블의 LDAP Attribute 열에서 * objectGUID * 를 입력하거나 * User-Principal-Name * 을 선택합니다.
 - g. 매핑 테이블의 발신 클레임 유형 열에서 드롭다운 목록에서 * 이름 ID * 를 선택합니다.
 - h. 마침 * 을 선택하고 * 확인 * 을 선택합니다.
8. 메타데이터를 성공적으로 가져왔는지 확인합니다.
- a. 신뢰할 수 있는 상대 신뢰를 마우스 오른쪽 단추로 클릭하여 속성을 엽니다.
 - b. Endpoints *, * Identifiers * 및 * Signature * 탭의 필드가 채워져 있는지 확인합니다.
- 메타데이터가 누락된 경우 페더레이션 메타데이터 주소가 올바른지 확인하거나 값을 수동으로 입력합니다.
9. 이 단계를 반복하여 StorageGRID 시스템의 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 구성합니다.
10. 완료되면 StorageGRID 로 돌아가서 "[모든 신뢰 당사자 트러스트를 테스트합니다](#)" 을 바르게 구성되었는지 확인하세요.

수동으로 신뢰할 수 있는 상대 신뢰를 만듭니다

의존 파트 트러스트의 데이터를 불러오지 않도록 선택하면 값을 직접 입력할 수 있습니다.

단계

1. Windows Server Manager에서 * Tools * 를 선택한 다음 * AD FS Management * 를 선택합니다.
 2. 작업에서 * 신뢰할 수 있는 당사자 신뢰 추가 * 를 선택합니다.
 3. 시작 페이지에서 * 클레임 인식 * 을 선택하고 * 시작 * 을 선택합니다.
 4. [의지하는 자에 대한 데이터 입력]을 선택하고 * [다음]을 선택합니다.
 5. 신뢰할 수 있는 당사자 신뢰 마법사를 완료합니다.
- a. 이 관리 노드의 표시 이름을 입력합니다.

일관성을 위해 그리드 관리자의 단일 사인온 페이지에 표시되는 것과 동일하게 관리자 노드에 대한 기반 당사자 식별자를 사용합니다. 'SG-DC1-ADM1' 예를 들어,

- b. 선택적 토큰 암호화 인증서를 구성하려면 단계를 건너뜁니다.
- c. URL 구성 페이지에서 SAML 2.0 WebSSO 프로토콜 * 지원 활성화 확인란을 선택합니다.
- d. 관리 노드에 대한 SAML 서비스 끝점 URL을 입력합니다.

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

의 경우 Admin_Node_FQDN 관리자 노드의 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)

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

`Admin_Node_Identifier`

의 경우 Admin_Node_Identifier 단일 사인온 페이지에 표시된 대로 관리자 노드의 종속 당사자 식별자를 입력합니다. 'SG-DC1-ADM1' 예를 들어,

f. 설정을 검토하고 신뢰할 수 있는 상대 신뢰를 저장한 다음 마법사를 닫습니다.

청구 발급 정책 편집 대화 상자가 나타납니다.



대화 상자가 나타나지 않으면 트러스트를 마우스 오른쪽 단추로 클릭하고 * 클레임 발급 정책 편집 * 을 선택합니다.

6. 클레임 규칙 마법사를 시작하려면 * 규칙 추가 * 를 선택합니다.

a. 규칙 템플릿 선택 페이지의 목록에서 * 청구로 LDAP 속성 보내기 * 를 선택하고 * 다음 * 을 선택합니다.

b. 규칙 구성 페이지에서 이 규칙의 표시 이름을 입력합니다.

예를 들어 * objectGUID를 이름 ID * 로, * UPN을 이름 ID * 로 지정합니다.

c. 특성 저장소의 경우 * Active Directory * 를 선택합니다.

d. Mapping 테이블의 LDAP Attribute 열에서 * objectGUID * 를 입력하거나 * User-Principal-Name * 을 선택합니다.

e. 매핑 테이블의 발신 클레임 유형 열에서 드롭다운 목록에서 * 이름 ID * 를 선택합니다.

f. 마침 * 을 선택하고 * 확인 * 을 선택합니다.

7. 신뢰할 수 있는 상대 신뢰를 마우스 오른쪽 단추로 클릭하여 속성을 엽니다.

8. 엔드포인트 * 탭에서 단일 로그아웃(SLO)에 대한 엔드포인트를 구성합니다.

a. SAML 추가 * 를 선택합니다.

b. Endpoint Type * > * SAML Logout * 을 선택합니다.

c. Binding * > * Redirect * 를 선택합니다.

d. 신뢰할 수 있는 URL * 필드에 이 관리 노드에서 단일 로그아웃(SLO)에 사용되는 URL을 입력합니다.

https://Admin_Node_FQDN/api/saml-logout

의 경우 Admin_Node_FQDN 관리자 노드의 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)

a. OK * 를 선택합니다.

9. 서명* 탭에서 이 신뢰할 수 있는 당사자 트러스트의 서명 인증서를 지정합니다.

a. 사용자 지정 인증서 추가:

- StorageGRID에 업로드한 사용자 지정 관리 인증서가 있는 경우 해당 인증서를 선택합니다.

- 사용자 지정 인증서가 없는 경우 관리자 노드에 로그인하고 관리자 노드의 디렉터리로 이동하여 /var/local/mgmt-api 인증서 파일을 추가합니다 custom-server.crt.



관리자 노드의 기본 인증서 ('server.crt' 사용)은 사용하지 않는 것이 좋습니다. 관리자 노드에 장애가 발생하면 노드를 복구할 때 기본 인증서가 다시 생성되고, 신뢰할 수 있는 상대 트러스트를 업데이트해야 합니다.

b. Apply * 를 선택하고 * OK * 를 선택합니다.

종속된 당사자 속성이 저장되고 닫힙니다.

10. 이 단계를 반복하여 StorageGRID 시스템의 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 구성합니다.
11. 완료되면 StorageGRID로 돌아가서 "모든 신뢰 당사자 트러스트를 테스트합니다" 올바르게 구성되었는지 확인하세요.

Entra ID에서 엔터프라이즈 애플리케이션 만들기

Entra ID를 사용하면 시스템의 각 관리 노드에 대한 엔터프라이즈 애플리케이션을 만들 수 있습니다.

시작하기 전에

- StorageGRID에 대한 단일 로그인 구성을 시작했으며 SSO 유형으로 *Entra ID*를 선택했습니다.
- 당신은 가지고 있다 "샌드박스 모드로 들어갔습니다" 그리드 관리자에서.
- 시스템의 각 관리 노드에는 *엔터프라이즈 애플리케이션 이름*이 있습니다. SSO 구성 페이지의 관리 노드 세부 정보 표에서 이러한 값을 복사할 수 있습니다.



StorageGRID 시스템의 각 관리 노드에 대해 엔터프라이즈 애플리케이션을 만들어야 합니다. 각 관리 노드에 엔터프라이즈 애플리케이션을 사용하면 사용자가 관리자 노드에 안전하게 로그인할 수 있습니다.

- Entra ID에서 엔터프라이즈 애플리케이션을 만든 경험이 있습니다.
- 활성화된 구독이 있는 Entra ID 계정이 있습니다.
- Entra ID 계정에는 글로벌 관리자, 클라우드 애플리케이션 관리자, 애플리케이션 관리자 또는 서비스 주체 소유자라는 역할 중 하나가 있습니다.

엔트라 ID 접속

단계

1. 에 "Azure 포털"로 로그인합니다.
2. 로 이동 "엔트라 ID".
3. 을 "엔터프라이즈 애플리케이션"선택합니다.

엔터프라이즈 애플리케이션을 생성하고 **StorageGRID SSO** 구성을 저장합니다

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

단계

1. 각 관리 노드에 대해 다음 단계를 반복합니다.
 - a. Entra ID Enterprise 애플리케이션 창에서 *새 애플리케이션*을 선택합니다.
 - b. 사용자 정의 응용 프로그램 만들기 * 를 선택합니다.
 - c. 이름에는 SSO 구성 페이지의 관리 노드 세부 정보 표에서 복사한 *엔터프라이즈 애플리케이션 이름*을 입력합니다.

- d. 갤러리에서 찾을 수 없는 * 다른 응용 프로그램 통합(갤러리 외) * 라디오 버튼을 선택된 상태로 둡니다.
 - e. Create * 를 선택합니다.
 - f. 2에서 * 시작하기 * 링크를 선택합니다. Single Sign On * 상자를 설정하거나 왼쪽 여백에서 * Single Sign-On * 링크를 선택합니다.
 - g. SAML * 상자를 선택합니다.
 - h. 앱 페더레이션 메타데이터 URL * 을 복사합니다. * 3단계 SAML 서명 인증서 * 에서 찾을 수 있습니다.
 - i. 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 모든 변경을 한 후 SSO 구성 페이지에서 *저장*을 선택합니다.

모든 관리 노드에 대해 **SAML** 메타데이터를 다운로드합니다

SSO 구성은 저장한 후 StorageGRID 시스템의 각 관리 노드에 대해 SAML 메타데이터 파일을 다운로드할 수 있습니다.

단계

1. 각 관리 노드에 대해 이 단계를 반복합니다.
 - a. 관리자 노드에서 StorageGRID에 로그인합니다.
 - b. 구성 > 액세스 제어 > *단일 로그인*을 선택합니다.
 - c. 버튼을 선택하여 해당 Admin Node에 대한 SAML 메타데이터를 다운로드합니다.
 - d. Entra ID에 업로드할 파일을 저장합니다.

각 엔터프라이즈 애플리케이션에 **SAML** 메타데이터를 업로드합니다

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

단계

1. Azure 포털로 돌아갑니다.
2. 각 엔터프라이즈 애플리케이션에 대해 다음 단계를 반복합니다.



이전에 목록에 추가한 응용 프로그램을 보려면 엔터프라이즈 응용 프로그램 페이지를 새로 고쳐야 할 수 있습니다.

- a. 엔터프라이즈 애플리케이션의 속성 페이지로 이동합니다.
- b. 할당 필요 * 를 * 아니오 * 로 설정합니다(할당을 별도로 구성하지 않는 경우).
- c. Single Sign-On 페이지로 이동합니다.
- d. SAML 구성을 완료합니다.
- e. Upload metadata file * 버튼을 선택하고 해당 Admin Node에 대해 다운로드한 SAML 메타데이터 파일을 선택합니다.
- f. 파일을 로드한 후 * Save * 를 선택하고 * X * 를 선택하여 창을 닫습니다. SAML로 단일 사인온 설정 페이지로 돌아갑니다.

3. "각 응용 프로그램을 테스트하세요".

PingFederate에서 서비스 공급자(SP) 연결을 생성합니다

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

시작하기 전에

- StorageGRID에 대한 SSO(Single Sign-On)를 구성하고 SSO 유형으로 * Ping 남부연합을 선택했습니다.
- 당신은 가지고 있다 "[샌드박스 모드로 들어갔습니다](#)" 그리드 관리자에서.
- 시스템의 각 관리 노드에는 * SP 연결 ID*가 있습니다. 이러한 값은 SSO 구성 페이지의 관리 노드 세부 정보 표에서 찾을 수 있습니다.
- 시스템의 각 관리 노드에 대해 * SAML 메타데이터 * 를 다운로드했습니다.
- PingFederate Server에서 SP 연결을 생성하는 경험이 있습니다.
- PingFederate Server용 이 "[관리자 참조 안내서](#)" 있습니다. PingFederate 설명서는 자세한 단계별 지침과 설명을 제공합니다.
- 당신은 가지고 있다 "[관리자 권한](#)" PingFederate 서버용.

이 작업에 대해

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

PingFederate에서 필수 구성 요소를 완료합니다

StorageGRID에 사용할 SP 연결을 생성하려면 PingFederate에서 사전 요구 작업을 완료해야 합니다. SP 접속을 구성할 때 이러한 사전 요구 사항의 정보를 사용합니다.

데이터 저장소 생성

아직 연결하지 않은 경우 데이터 저장소를 생성하여 PingFederate를 AD FS LDAP 서버에 연결합니다. StorageGRID에서 사용한 값을 "[ID 페더레이션을 구성하는 중입니다](#)" 사용합니다.

- * 유형 *: 디렉토리(LDAP)
- * LDAP 유형 *: Active Directory
- * 바이너리 특성 이름 *: LDAP 바이너리 특성 탭의 * objectGUID * 를 그림과 같이 정확하게 입력합니다.

암호 자격 증명 유효성 검사기 [[암호 유효성 검사기]] 만들기

아직 설치하지 않은 경우 암호 자격 증명 유효성 검사기를 만듭니다.

- * 유형 *: LDAP 사용자 이름 암호 자격 증명 검사기
- * 데이터 저장소 *: 만든 데이터 저장소를 선택합니다.
- * 검색 기준 *: LDAP의 정보를 입력합니다(예: DC=SAML, DC=SGWs).
- * 검색 필터 *: sAMAccountName=\${username}

- * 범위 *: 하위 트리

IDP 어댑터 인스턴스 만들기

아직 IDP 어댑터 인스턴스를 만들지 않은 경우 생성합니다.

단계

1. 인증 * > * 통합 * > * IDP 어댑터 * 로 이동합니다.
2. 새 인스턴스 만들기 * 를 선택합니다.
3. 유형 탭에서 * HTML 양식 IDP 어댑터 * 를 선택합니다.
4. IDP Adapter 탭에서 * Add a new row to 'Credential Validators' * 를 선택합니다.
5. 선택하세요[암호 자격 증명 유효성 검사기가 있습니다](#) 당신이 창조했습니다.
6. 어댑터 특성 탭에서 * 가명 * 에 대한 * 사용자 이름 * 속성을 선택합니다.
7. 저장 * 을 선택합니다.

서명 인증서 만들기 또는 가져오기

서명 인증서를 아직 만들지 않은 경우 서명 인증서를 만들거나 가져옵니다.

단계

1. 보안 * > * 서명 및 암호 해독 키 및 인증서 * 로 이동합니다.
2. 서명 인증서를 만들거나 가져옵니다.

PingFederate에서 SP 접속을 생성합니다

PingFederate에서 SP 연결을 생성할 때 StorageGRID에서 다운로드한 SAML 메타데이터를 관리자 노드에 대해 가져옵니다. 메타데이터 파일에는 필요한 많은 특정 값이 들어 있습니다.



사용자가 모든 노드에 안전하게 로그인할 수 있도록 StorageGRID 시스템의 각 관리 노드에 대해 SP 접속을 생성해야 합니다. 이 지침에 따라 첫 번째 SP 접속을 생성합니다. 그런 다음 [추가 SP 접속을 생성합니다](#) 이동하여 필요한 추가 연결을 만듭니다.

SP 접속 유형을 선택합니다

단계

1. 응용 프로그램 * > * 통합 * > * SP 연결 * 으로 이동합니다.
2. Create Connection * 을 선택합니다.
3. 이 연결에 템플릿을 사용하지 않음 * 을 선택합니다.
4. 프로토콜로 * Browser SSO Profiles * 및 * SAML 2.0 * 을 선택합니다.

SP 메타데이터를 가져옵니다

단계

1. 메타데이터 가져오기 탭에서 * 파일 * 을 선택합니다.

2. 관리 노드의 SSO 구성 페이지에서 다운로드한 SAML 메타데이터 파일을 선택합니다.

3. 메타데이터 요약 및 일반 정보 탭에 제공된 정보를 검토합니다.

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

4. 다음 * 을 선택합니다.

IDP 브라우저 SSO를 구성합니다

단계

1. Browser SSO(브라우저 SSO) 탭에서 * Configure Browser SSO *(브라우저 SSO * 구성)를 선택합니다.

2. SAML 프로필 탭에서 * SP 시작 SSO *, * SP 초기 SLO *, * IDP 시작 SSO * 및 * IDP 시작 SLO * 옵션을 선택합니다.

3. 다음 * 을 선택합니다.

4. 어설션 수명 탭에서 변경하지 않습니다.

5. 어설션 작성 탭에서 * 어설션 작성 설정 * 을 선택합니다.

a. ID 매핑 탭에서 * 표준 * 을 선택합니다.

b. [속성 계약] 탭에서 [속성 계약] 및 가져온 지정되지 않은 이름 형식으로 * SAML_subject * 를 사용합니다.

6. 계약 연장에서 * 삭제 * 를 선택하여 사용하지 않는 를 제거합니다 urn:oid.

어댑터 인스턴스를 매핑합니다

단계

1. 인증 소스 매핑 탭에서 * 새 어댑터 인스턴스 매핑 * 을 선택합니다.

2. 어댑터 인스턴스 탭에서 작성한 을 [어댑터 인스턴스](#)선택합니다.

3. 매핑 방법 탭에서 * 데이터 저장소에서 추가 특성 검색 * 을 선택합니다.

4. 특성 원본 및 사용자 조회 탭에서 * 특성 원본 추가 * 를 선택합니다.

5. 데이터 저장소 탭에서 설명을 입력하고 추가한 을 [데이터 저장소선택합니다](#).

6. LDAP 딕렉토리 검색 탭에서 다음을 수행합니다.

◦ 기본 DN * 을 입력합니다. 이 값은 LDAP 서버에 대해 StorageGRID에 입력한 값과 정확히 일치해야 합니다.

◦ 검색 범위에서 * 하위 트리 * 를 선택합니다.

◦ 루트 개체 클래스의 경우 * objectGUID * 또는 * userPrincipalName * 속성 중 하나를 검색하여 추가합니다.

7. LDAP 바이너리 특성 인코딩 형식 탭에서 * objectGUID * 특성에 대해 * Base64 * 를 선택합니다.

8. LDAP 필터 탭에서 * sAMAccountName=\${username} * 을 입력합니다.

9. 특성 계약 이행 탭의 소스 드롭다운에서 * LDAP (attribute) * 를 선택하고 값 드롭다운에서 * objectGUID * 또는 * userPrincipalName * 을 선택합니다.

10. 특성 소스를 검토한 후 저장합니다.

11. Failsave 특성 소스 탭에서 * SSO 트랜잭션 중단 * 을 선택합니다.

12. 요약을 검토하고 * 완료 * 를 선택합니다.

13. 완료 * 를 선택합니다.

프로토콜 설정을 구성합니다

단계

1. SP Connection * > * Browser SSO * > * Protocol Settings * 탭에서 * Configure Protocol Settings * 를 선택합니다.
2. 어설션 소비자 서비스 URL 탭에서 StorageGRID SAML 메타데이터(* 바인딩 및 끝점 URL의 경우 * POST *)에서 가져온 기본값을 수락합니다. /api/saml-response
3. SLO 서비스 URL 탭에서 StorageGRID SAML 메타데이터(* 바인딩 및 끝점 URL의 경우 * 리디렉션 *)에서 가져온 기본값을 그대로 /api/saml-logout 사용합니다.
4. 허용 가능한 SAML 바인딩 탭에서 * Artifact * 및 * SOAP * 를 지웁니다. POST * 및 * REDIRECT * 만 필요합니다.
5. 서명 정책 탭에서 * Authn 요청 서명 필요 * 및 * 항상 설정 서명 * 확인란을 선택된 상태로 둡니다.
6. 암호화 정책 탭에서 * 없음 * 을 선택합니다.
7. 요약을 검토하고 * Done * (완료 *)을 선택하여 프로토콜 설정을 저장합니다.
8. 요약을 검토하고 * 완료 * 를 선택하여 브라우저 SSO 설정을 저장합니다.

자격 증명을 구성합니다

단계

1. SP 연결 탭에서 * 자격 증명 * 을 선택합니다.
2. 자격 증명 탭에서 * 자격 증명 구성 * 을 선택합니다.
3. 선택하세요 [서명 인증서](#) 귀하가 만들거나 가져왔습니다.
4. 다음 * 을 선택하여 * 서명 확인 설정 관리 * 로 이동합니다.
 - a. 보안 모델 탭에서 * 앵커 지정되지 않음 * 을 선택합니다.
 - b. 서명 확인 인증서 탭에서 StorageGRID SAML 메타데이터에서 가져온 서명 인증서 정보를 검토합니다.
5. 요약 화면을 검토하고 * 저장 * 을 선택하여 SP 접속을 저장합니다.

추가 **SP** 접속을 생성합니다

첫 번째 SP 접속을 복제하여 그리드의 각 관리 노드에 필요한 SP 접속을 생성할 수 있습니다. 각 복사본에 대한 새 메타데이터를 업로드합니다.



파트너의 엔티티 ID, 기본 URL, 연결 ID, 연결 이름, 서명 확인을 제외하고 서로 다른 관리 노드의 SP 연결은 동일한 설정을 사용합니다. SLO 응답 URL이 있습니다.

단계

1. 각 추가 관리 노드에 대한 초기 SP 연결의 복제본을 생성하려면 * Action * > * Copy * 를 선택합니다.
2. 복사본의 연결 ID와 연결 이름을 입력하고 * 저장 * 을 선택합니다.
3. 관리 노드에 해당하는 메타데이터 파일을 선택합니다.
 - a. 작업 * > * 메타데이터 업데이트 * 를 선택합니다.

- b. 파일 선택 * 을 선택하고 메타데이터를 업로드합니다.
 - c. 다음 * 을 선택합니다.
 - d. 저장 * 을 선택합니다.
4. 미사용 속성으로 인한 오류를 해결합니다.
- a. 새 연결을 선택합니다.
 - b. Configure Browser SSO > Configure Assertion Creation > Attribute Contract * 를 선택합니다.
 - c. urn:OID*에 대한 항목을 삭제합니다.
 - d. 저장 * 을 선택합니다.

SSO 비활성화

이 기능을 더 이상 사용하지 않으려면 SSO(Single Sign-On)를 사용하지 않도록 설정할 수 있습니다. ID 페더레이션을 비활성화하려면 먼저 SSO(Single Sign-On)를 비활성화해야 합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 있습니다. "[특정 액세스 권한](#)"

단계

1. 구성 > 액세스 제어 > *단일 로그인*을 선택합니다.

단일 사인온 페이지가 나타납니다.

2. *SSO 비활성화*를 선택하세요.
3. 예 * 를 선택합니다.

로컬 사용자가 로그인할 수 있음을 나타내는 경고 메시지가 나타납니다.

다음에 StorageGRID에 로그인할 때 StorageGRID 로그인 페이지가 나타나고 로컬 또는 통합 StorageGRID 사용자의 사용자 이름과 암호를 입력해야 합니다.

한 관리 노드에 대해 SSO를 일시적으로 비활성화하고 다시 활성화합니다.

SSO(Single Sign-On) 시스템이 다운되면 Grid Manager에 로그인하지 못할 수 있습니다. 이 경우 한 관리 노드에 대해 SSO를 일시적으로 비활성화 및 다시 활성화할 수 있습니다. SSO를 사용하지 않도록 설정한 다음 다시 사용하도록 설정하려면 노드의 명령 셸에 액세스해야 합니다.

시작하기 전에

- 있습니다. "[특정 액세스 권한](#)"
- `Passwords.txt` 파일이 있습니다.
- 로컬 루트 사용자의 암호를 알고 있습니다.

이 작업에 대해

한 관리 노드에 대해 SSO를 비활성화한 후 그리드 관리자에 로컬 루트 사용자로 로그인할 수 있습니다. StorageGRID 시스템을 보호하려면 로그아웃하는 즉시 노드의 명령 셸을 사용하여 관리자 노드에서 SSO를 다시 활성화해야 합니다.



한 관리 노드에 대해 SSO를 비활성화해도 그리드의 다른 관리 노드에 대한 SSO 설정에는 영향을 주지 않습니다. Grid Manager의 Single Sign-On 페이지에 있는 * Enable SSO * 확인란은 선택된 상태로 남아 있으며, 기존 SSO 설정은 모두 업데이트하지 않는 한 유지됩니다.

단계

1. 관리자 노드에 로그인:

- 다음 명령을 입력합니다. `ssh admin@Admin_Node_IP`
- 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
- 다음 명령을 입력하여 루트로 전환합니다. `su -`
- 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 \$로 '#'로 변경됩니다.

2. 다음 명령을 실행합니다.`disable-saml`

명령이 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

3. SSO를 비활성화할지 확인합니다.

노드에서 SSO(Single Sign-On)가 비활성화되었다는 메시지가 표시됩니다.

4. 웹 브라우저에서 동일한 관리 노드의 그리드 관리자에 액세스합니다.

이제 SSO가 비활성화되어 Grid Manager 로그인 페이지가 표시됩니다.

5. 사용자 이름 루트와 로컬 루트 사용자 암호를 사용하여 로그인합니다.

6. SSO 구성을 수정해야 하므로 SSO를 일시적으로 비활성화한 경우:

- 구성 > 액세스 제어 > *단일 로그인*을 선택합니다.
- 잘못된 또는 오래된 SSO 설정을 변경합니다.
- 저장 * 을 선택합니다.

단일 사인온 페이지에서 * 저장 * 을 선택하면 전체 그리드에 대한 SSO가 자동으로 다시 활성화됩니다.

7. 다른 이유로 인해 그리드 관리자에 액세스해야 하기 때문에 SSO를 일시적으로 비활성화한 경우:

- 수행해야 할 작업 또는 작업을 모두 수행합니다.
- 로그아웃 * 을 선택하고 그리드 관리자를 닫습니다.
- 관리자 노드에서 SSO를 다시 활성화합니다. 다음 단계 중 하나를 수행할 수 있습니다.

▪ 다음 명령을 실행합니다. `enable-saml`

명령이 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

SSO를 활성화할지 확인합니다.

노드에서 Single Sign-On이 설정되었음을 나타내는 메시지가 표시됩니다.

- 그리드 노드를 재부팅합니다. reboot

8. 웹 브라우저에서 동일한 관리 노드에서 그리드 관리자에 액세스합니다.
9. StorageGRID 로그인 페이지가 나타나고 그리드 관리자에 액세스하려면 SSO 자격 증명을 입력해야 합니다.

그리드 페더레이션을 사용합니다

그리드 페더레이션은 무엇입니까?

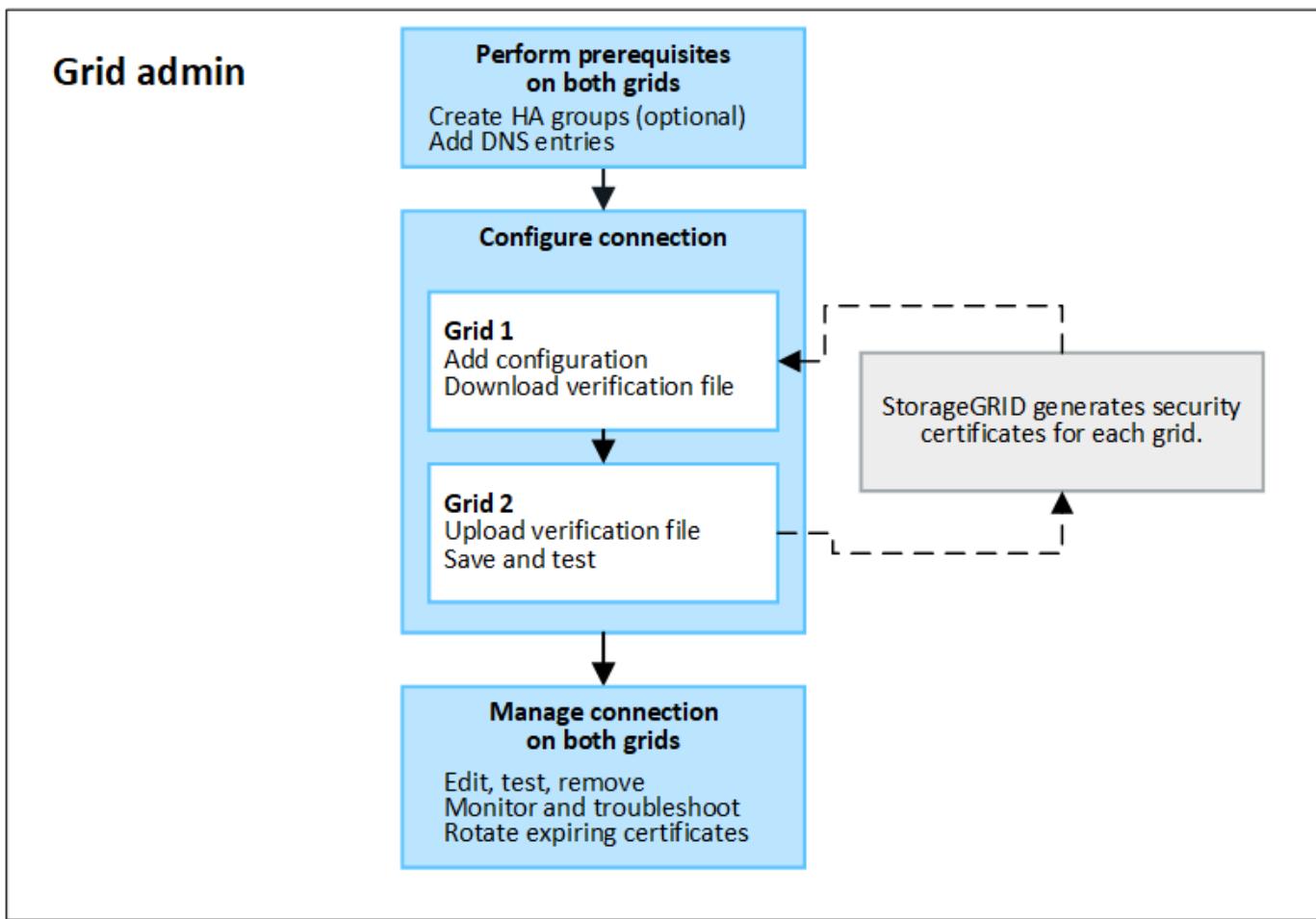
그리드 페더레이션을 사용하여 테넌트를 클론 복제하고 재해 복구를 위해 두 StorageGRID 시스템 간에 개체를 복제할 수 있습니다.

그리드 페더레이션 연결이란 무엇입니까?

그리드 페더레이션 연결은 두 StorageGRID 시스템에서 관리자 노드와 게이트웨이 노드 간에 양방향으로 안전하게 연결됩니다.

그리드 페더레이션을 위한 워크플로

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



그리드 페더레이션 연결에 대한 고려 사항 및 요구 사항

- 그리드 페더레이션에 사용되는 그리드는 동일하거나 둘 이상의 주요 버전 차이가 없는 StorageGRID 버전을 실행해야 합니다.

버전 요구 사항에 대한 자세한 내용은 ["릴리스 정보"](#) 참조하십시오.

- 그리드에는 다른 그리드에 대한 하나 이상의 그리드 페더레이션 연결이 있을 수 있습니다. 각 그리드 페더레이션 연결은 다른 연결과 독립적입니다. 예를 들어, 그리드 1이 그리드 2와 1개의 연결을 가지고 있고 그리드 3과 2번째 연결이 있는 경우 그리드 2와 그리드 3 사이에는 묵시적 연결이 없습니다.
- 그리드 페더레이션 연결은 양방향입니다. 연결이 설정되면 두 그리드 중 하나에서 연결을 모니터링하고 관리할 수 있습니다.
- 또는 을 사용하려면 하나 이상의 그리드 페더레이션 연결이 있어야 ["계정 클론""교차 그리드 복제"](#)합니다.

네트워킹 및 IP 주소 요구 사항

- 그리드 페더레이션 연결은 그리드 네트워크, 관리자 네트워크 또는 클라이언트 네트워크에서 발생할 수 있습니다.
- 그리드 페더레이션 연결은 한 그리드를 다른 그리드에 연결합니다. 각 그리드의 구성은 관리 노드, 게이트웨이 노드 또는 둘 모두로 구성된 다른 그리드의 그리드 통합 끝점을 지정합니다.
- Best Practice는 각 그리드에서 게이트웨이 및 관리 노드를 연결하는 ["고가용성\(HA\) 그룹"](#) 것입니다. HA 그룹을 사용하면 노드를 사용할 수 없게 될 경우 그리드 페더레이션 연결이 온라인 상태로 유지됩니다. 두 HA 그룹 중 하나의 활성 인터페이스에 장애가 발생하면 연결에서 백업 인터페이스를 사용할 수 있습니다.

- 단일 관리 노드 또는 게이트웨이 노드의 IP 주소를 사용하는 그리드 페더레이션 연결을 만드는 것은 권장되지 않습니다. 노드를 사용할 수 없게 되면 그리드 페더레이션 연결도 사용할 수 없게 됩니다.
- "교차 그리드 복제" 객체의 경우 각 그리드의 스토리지 노드가 다른 그리드에서 구성된 관리 및 게이트웨이 노드에 액세스할 수 있어야 합니다. 각 그리드에 대해 모든 스토리지 노드가 연결에 사용되는 관리자 노드 또는 게이트웨이 노드로 향하는 고대역폭 경로를 가지고 있는지 확인합니다.

FQDN을 사용하여 연결 밸런스를 로드합니다

운영 환경의 경우 FQDN(정규화된 도메인 이름)을 사용하여 연결의 각 그리드를 식별합니다. 그런 다음 다음과 같이 적절한 DNS 항목을 만듭니다.

- 그리드 1의 FQDN은 그리드 1의 HA 그룹에 대한 하나 이상의 가상 IP(VIP) 주소 또는 그리드 1에 있는 하나 이상의 관리 또는 게이트웨이 노드의 IP 주소에 매핑됩니다.
- 그리드 2의 FQDN은 그리드 2의 하나 이상의 VIP 주소 또는 그리드 2의 하나 이상의 관리 또는 게이트웨이 노드의 IP 주소에 매핑됩니다.

여러 DNS 항목을 사용하는 경우 연결 사용 요청은 다음과 같이 로드 밸런싱됩니다.

- 여러 HA 그룹의 VIP 주소에 매핑되는 DNS 항목은 HA 그룹의 활성 노드 간에 로드 밸런싱됩니다.
- 여러 관리 노드 또는 게이트웨이 노드의 IP 주소에 매핑되는 DNS 항목은 매핑된 노드 간에 로드 밸런싱됩니다.

포트 요구 사항

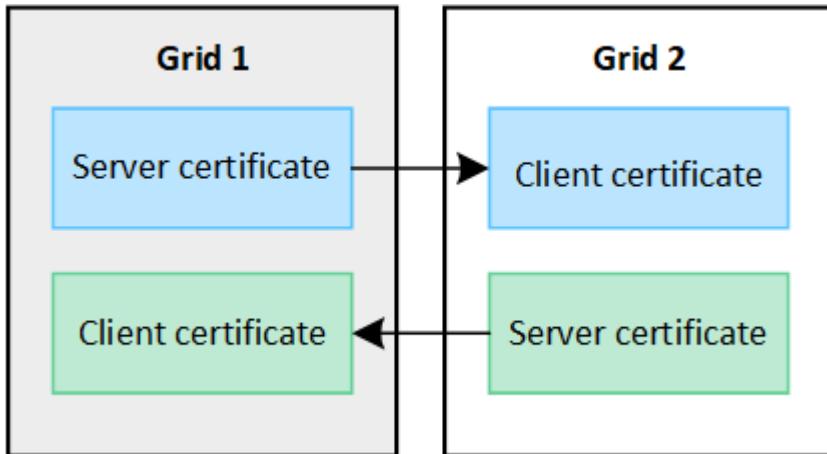
그리드 페더레이션 연결을 생성할 때 사용하지 않는 포트 번호를 23000에서 23999까지 지정할 수 있습니다. 이 연결의 두 그리드는 동일한 포트를 사용합니다.

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

인증서 요구 사항

그리드 페더레이션 연결을 구성할 때 StorageGRID는 자동으로 네 개의 SSL 인증서를 생성합니다.

- 그리드 1에서 그리드 2로 전송되는 정보를 인증 및 암호화하는 서버 및 클라이언트 인증서입니다
- 그리드 2에서 그리드 1로 전송되는 정보를 인증 및 암호화하는 서버 및 클라이언트 인증서입니다



기본적으로 인증서는 730일(2년)에 유효합니다. 이러한 인증서가 만료 날짜에 근접하면 * 그리드 페더레이션 인증서 만료 * 알림이 인증서를 회전하라는 알림을 표시합니다. 이 알림은 그리드 관리자를 사용하여 수행할 수 있습니다.



연결 양 끝에 있는 인증서가 만료되면 연결이 중지됩니다. 인증서가 업데이트될 때까지 데이터 복제가 보류됩니다.

자세한 정보

- "[그리드 페더레이션 연결을 만듭니다](#)"
- "[그리드 페더레이션 연결을 관리합니다](#)"
- "[그리드 통합 오류 문제 해결](#)"

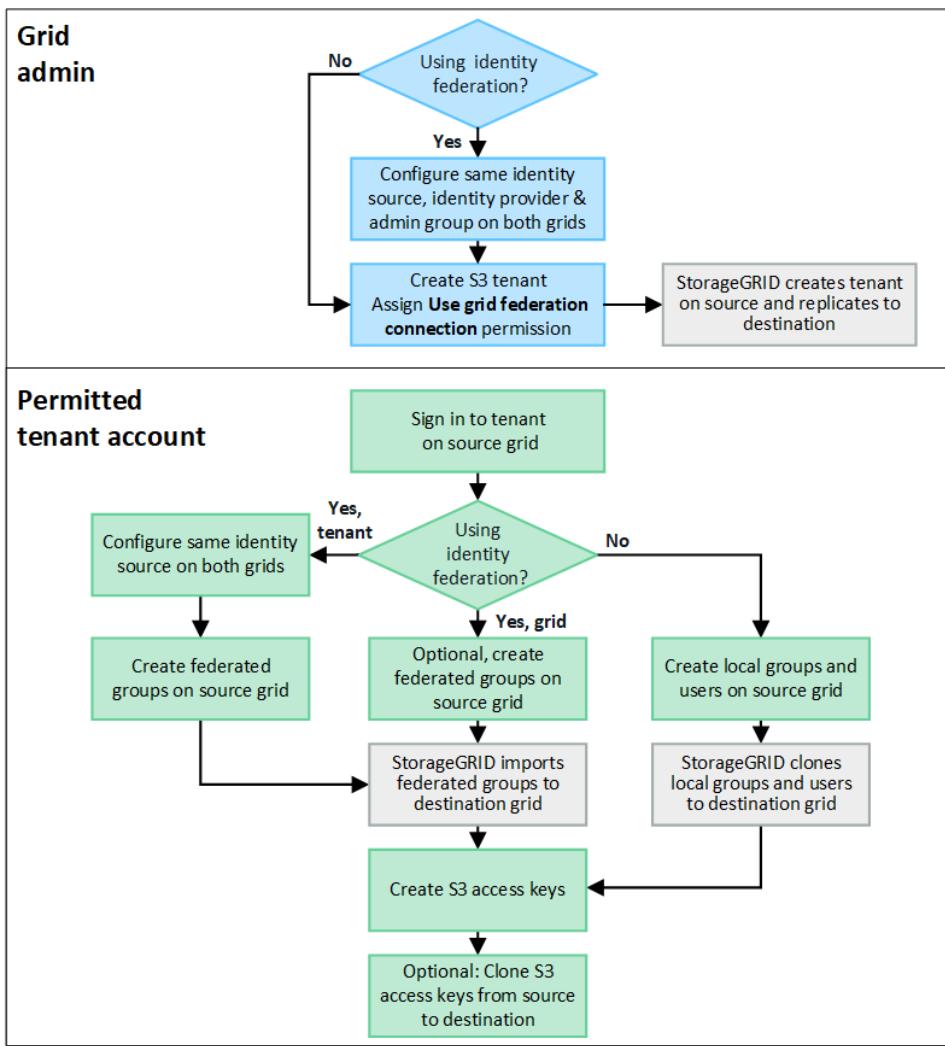
계정 클론이란 무엇입니까?

계정 클론은 테넌트 계정, 테넌트 그룹, 테넌트 사용자 및 의 StorageGRID 시스템 간에 선택적으로 S3 액세스 키를 자동으로 복제하는 "[그리드 페더레이션 연결](#)" 것입니다.

에 계정 클론이 필요합니다. "[교차 그리드 복제](#)" 소스 StorageGRID 시스템에서 대상 StorageGRID 시스템으로 계정 정보를 클론 복제하면 테넌트 사용자 및 그룹이 두 그리드 중 하나의 해당 버킷과 객체에 액세스할 수 있습니다.

계정 클론 워크플로우

워크플로우 다이어그램은 그리드 관리자 및 허용된 테넌트가 계정 클론을 설정하기 위해 수행하는 단계를 보여 줍니다. 이러한 단계는 이후에 "[그리드 페더레이션 연결이 구성되어 있습니다](#)" 수행됩니다.



그리드 관리자 워크플로

그리드 관리자가 수행하는 단계는 StorageGRID 시스템이 SSO(Single Sign-On)를 사용하는지 ID 페더레이션을 사용하는지에 따라 "그리드 페더레이션 연결"다릅니다.

계정 클론에 대한 SSO 구성(선택 사항)

그리드 페더레이션 연결의 StorageGRID 시스템 중 하나에서 SSO를 사용하는 경우 두 그리드에서 모두 SSO를 사용해야 합니다. 그리드 페더레이션을 위해 테넌트 계정을 생성하기 전에 테넌트의 소스 및 대상 그리드에 대한 그리드 관리자가 다음 단계를 수행해야 합니다.

단계

1. 두 그리드에 대해 동일한 ID 소스를 구성합니다. 을 "ID 페더레이션을 사용합니다" 참조하십시오.
2. 두 그리드에 동일한 SSO ID 공급자(IdP)를 구성합니다. 보다 "Single Sign-On 구성".
3. "동일한 관리 그룹을 생성합니다" 동일한 통합 그룹을 가져와서 두 그리드 모두에서 테넌트를 생성할 때 소스 및 대상 테넌트 계정에 대한 초기 루트 액세스 권한을 가지려면 이 그룹을 선택합니다.

테넌트를 생성할 때 소스 및 대상 테넌트 계정에 대한 초기 루트 액세스 권한을 가지려면 이 그룹을 선택합니다.



이 관리 그룹이 테넌트를 생성하기 전에 두 그리드에 없는 경우 테넌트는 대상에 복제되지 않습니다.

계정 클론에 대한 그리드 수준 ID 페더레이션 구성(선택 사항)

StorageGRID 시스템 중 하나에서 SSO 없이 ID 페더레이션을 사용하는 경우 두 그리드 모두 ID 페더레이션을 사용해야 합니다. 그리드 페더레이션을 위해 테넌트 계정을 생성하기 전에 테넌트의 소스 및 대상 그리드에 대한 그리드 관리자가 다음 단계를 수행해야 합니다.

단계

1. 두 그리드에 대해 동일한 ID 소스를 구성합니다. 을 "[ID 페더레이션을 사용합니다](#)" 참조하십시오.
2. 필요에 따라 통합 그룹에 소스 및 대상 테넌트 계정 모두에 대한 초기 루트 액세스 권한이 있는 경우, "[동일한 관리 그룹을 생성합니다](#)" 동일한 통합 그룹을 가져와 두 그리드 모두에서 사용할 수 있습니다.



두 그리드에 없는 통합 그룹에 루트 액세스 권한을 할당하면 해당 테넌트가 대상 그리드에 복제되지 않습니다.

3. 통합 그룹에 두 계정에 대한 초기 루트 액세스 권한이 없는 경우 로컬 루트 사용자의 암호를 지정합니다.

허용된 S3 테넌트 계정을 생성합니다

선택적으로 SSO 또는 ID 페더레이션을 구성한 후 그리드 관리자는 다음 단계를 수행하여 버킷 객체를 다른 StorageGRID 시스템으로 복제할 수 있는 테넌트를 결정합니다.

단계

1. 계정 클론 작업을 위해 테넌트의 소스 그리드로 사용할 그리드를 결정합니다.

테넌트가 처음 생성된 그리드를 테넌트의 _source GRID_라고 합니다. 테넌트가 복제되는 그리드를 테넌트의 _destination grid_라고 합니다.

2. 이 그리드에서 새 S3 테넌트 계정을 만들거나 기존 계정을 편집합니다.
3. 그리드 페더레이션 연결 사용 * 권한을 할당합니다.
4. 테넌트 계정이 자신의 통합 사용자를 관리할 경우 * 사용자 ID 소스 사용 * 권한을 할당합니다.

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

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

그리드 통합 연결 사용 * 권한이 있는 새 테넌트가 저장된 경우 StorageGRID는 다음과 같이 다른 그리드에 해당 테넌트의 복제본을 자동으로 생성합니다.

- 두 테넌트 계정 모두 동일한 계정 ID, 이름, 스토리지 할당량 및 할당된 권한이 있습니다.
- 테넌트에 대한 루트 액세스 권한이 있는 통합 그룹을 선택한 경우 해당 그룹이 대상 테넌트에 복제됩니다.
- 테넌트에 대한 루트 액세스 권한이 있는 로컬 사용자를 선택한 경우 해당 사용자는 대상 테넌트에 복제됩니다. 그러나 해당 사용자의 암호는 복제되지 않습니다.

자세한 내용은 을 참조하십시오 "[그리드 페더레이션에 허용된 테넌트 관리](#)".

허용된 테넌트 계정 워크플로

그리드 페더레이션 연결 사용 * 권한이 있는 테넌트가 대상 그리드에 복제된 후에 허용된 테넌트 계정은 테넌트 그룹, 사용자 및 S3 액세스 키를 클론 복제하기 위해 다음 단계를 수행할 수 있습니다.

단계

1. 테넌트의 소스 격자에서 테넌트 계정에 로그인합니다.
 2. 허용되는 경우 소스 및 대상 테넌트 계정 모두에서 ID 페더레이션을 구성합니다.
 3. 소스 테넌트에 그룹 및 사용자를 생성합니다.
- 소스 테넌트에 새 그룹 또는 사용자가 생성되면 StorageGRID는 자동으로 대상 테넌트에 클론을 생성하지만 대상에서 다시 소스로 클론을 생성하지 않습니다.
4. S3 액세스 키를 생성합니다.
 5. 필요에 따라 소스 테넌트에서 대상 테넌트로 S3 액세스 키를 복제합니다.

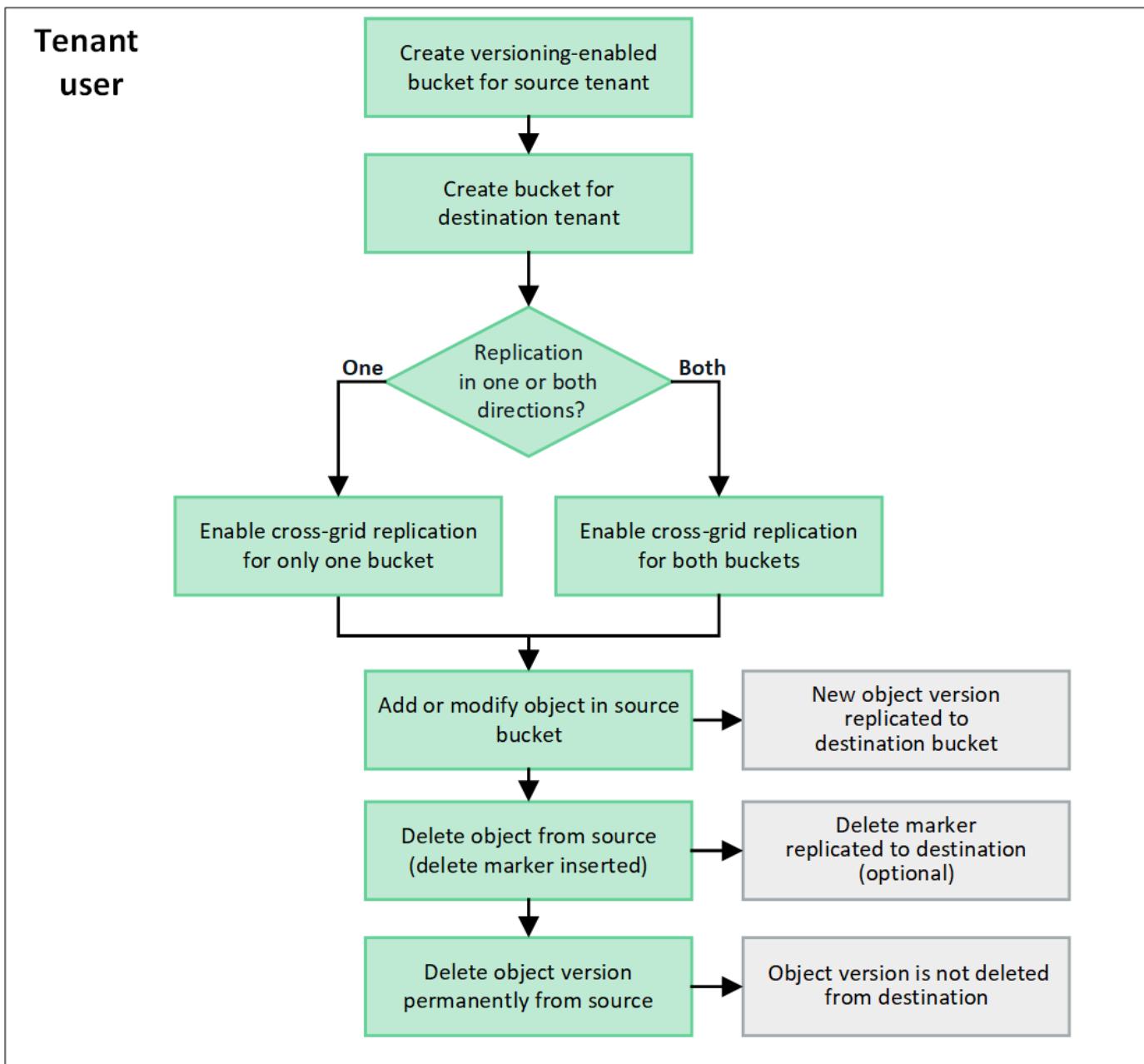
허용되는 테넌트 계정 워크플로에 대한 자세한 내용과 그룹, 사용자 및 S3 액세스 키의 클론 생성 방법에 대한 자세한 내용은 및 을 참조하십시오 "[클론 테넌트 그룹 및 사용자](#)" "[API를 사용하여 S3 액세스 키의 클론을 생성합니다](#)".

교차 그리드 복제란 무엇입니까?

그리드 간 복제는 에 연결된 두 StorageGRID 시스템에서 선택한 S3 버킷 간에 오브젝트를 자동 복제하는 것입니다 "[그리드 페더레이션 연결](#)". "[계정 클론](#)" 그리드 간 복제에 필요합니다.

그리드 간 복제를 위한 워크플로우

워크플로 디어그램은 두 그리드의 버킷 간에 크로스 그리드 복제를 구성하는 단계를 요약한 것입니다.



크로스 그리드 복제 요구 사항

테넌트 계정에 하나 이상의 그리드 페더레이션 연결을 사용할 수 있는 그리드 페더레이션 연결 사용 권한이 있는 경우 ["그리드 페더레이션 연결"](#) 루트 액세스 권한이 있는 테넌트 사용자는 각 그리드의 해당 테넌트 계정에 버킷을 생성할 수 있습니다. 이 버킷:

- 서로 다른 이름을 가질 수 있습니다
- 다른 지역을 가질 수 있습니다
- 버전 관리가 활성화되어 있어야 합니다
- 비어 있어야 합니다

두 버킷이 모두 생성된 후 크로스 그리드 복제를 둘 중 하나 또는 두 버킷에 대해 구성할 수 있습니다.

자세한 정보

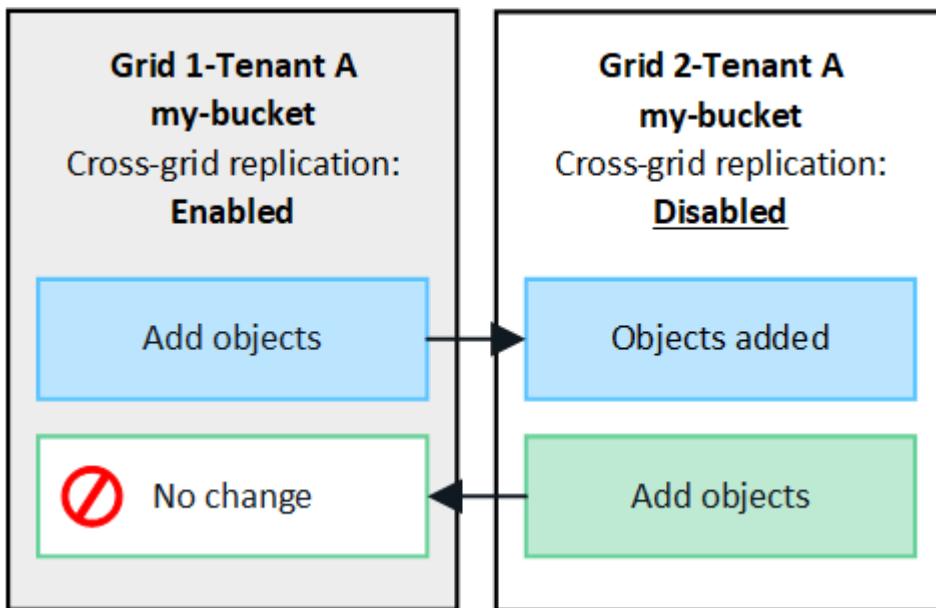
"교차 그리드 복제 관리"

교차 그리드 복제의 작동 방식

그리드 간 복제를 단방향 또는 양방향으로 구성하여 수행할 수 있습니다.

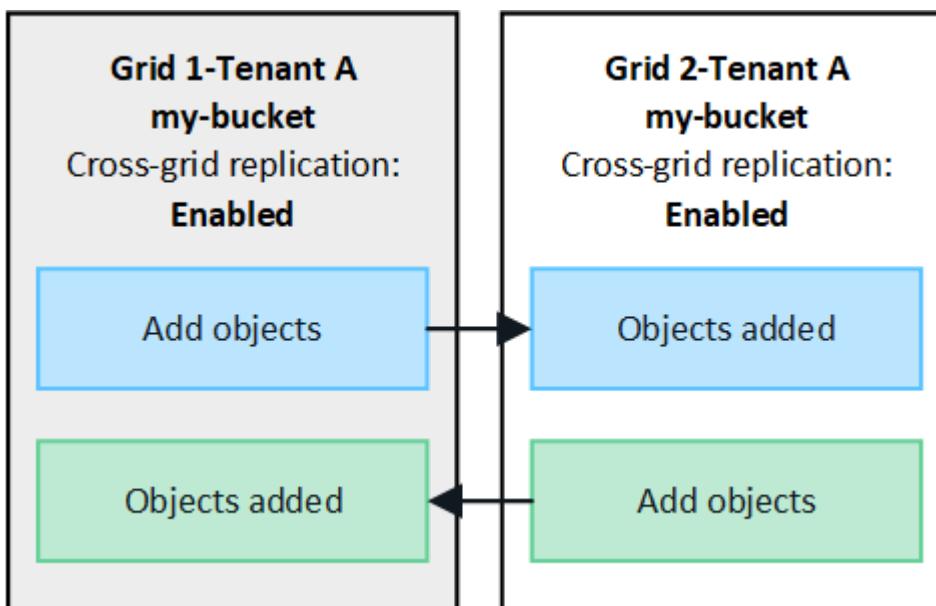
복제 기능을 제공합니다

한 그리드의 버킷에 대해서만 교차 그리드 복제를 활성화하는 경우 해당 버킷(소스 버킷)에 추가된 객체는 다른 그리드의 해당 버킷(대상 버킷)에 복제됩니다. 하지만 대상 버킷에 추가된 객체는 소스로 다시 복제되지 않습니다. 그림에서 크로스 그리드 복제가 활성화되었습니다. my-bucket 그리드 1에서 그리드 2로의 이동은 가능하지만 반대 방향으로는 활성화되어 있지 않습니다.



양방향으로 복제

두 그리드에서 동일한 버킷에 대해 교차 그리드 복제를 활성화하면 두 버킷에 추가된 객체가 다른 그리드에 복제됩니다. 그림에서 교차 그리드 복제는 양방향으로 대해 my-bucket 활성화됩니다.



오브젝트를 수집하면 어떻게 됩니까?

S3 클라이언트가 교차 그리드 복제를 사용하도록 설정된 버킷에 오브젝트를 추가하면 다음과 같은 현상이 발생합니다.

- StorageGRID는 소스 버킷에서 대상 버킷으로 오브젝트를 자동으로 복제합니다. 이 백그라운드 복제 작업을 수행하는 시간은 보류 중인 다른 복제 작업의 수를 비롯한 여러 요인에 따라 달라집니다.

S3 클라이언트는 GetObject 또는 HeadObject 요청을 실행하여 객체의 복제 상태를 확인할 수 있습니다. 응답에는 StorageGRID 관련 내용이 포함됩니다. `x-ntap-sg-cgr-replication-status` 다음 값 중 하나를 갖는 응답 헤더:

그리드	복제 상태입니다
출처	<ul style="list-style-type: none">* 완료 *: 모든 그리드 연결에 대해 복제가 성공했습니다.* 보류 중 *: 객체가 하나 이상의 그리드 연결에 복제되지 않았습니다.실패: 그리드 연결에 대한 복제가 보류되지 않았으며 적어도 하나는 영구적인 오류로 실패했습니다. 사용자는 오류를 해결해야 합니다.
목적지	<ul style="list-style-type: none">replica *: 객체가 소스 그리드에서 복제되었습니다.



StorageGRID 지원하지 않습니다 `x-amz-replication-status` 헤더.

- StorageGRID는 다른 오브젝트와 마찬가지로 각 그리드의 활성 ILM 정책을 사용하여 오브젝트를 관리합니다. 예를 들어, 그리드 1의 오브젝트 A는 두 개의 복제된 복사본으로 저장되고 영구적으로 보존되는 반면, 그리드 2에 복제된 오브젝트 A는 2+1 삭제 코딩을 사용하여 저장하고 3년 후에 삭제될 수 있습니다.

오브젝트를 삭제하면 어떻게 됩니까?

예 설명된 대로 "[데이터 흐름을 삭제합니다](#)" StorageGRID는 다음과 같은 이유로 개체를 삭제할 수 있습니다.

- S3 클라이언트가 삭제 요청을 실행합니다.
- 테넌트 관리자 사용자는 "[버킷에서 오브젝트를 삭제합니다](#)" 버킷에서 모든 오브젝트를 제거하는 옵션을 선택합니다.
- 버킷에는 수명 주기 구성이 만료되어 있습니다.
- 개체에 대한 ILM 규칙의 마지막 기간이 종료되며 더 이상 지정된 배치가 없습니다.

StorageGRID가 버킷 작업, 버킷 수명 주기 만료 또는 ILM 배치 만료에서 오브젝트 삭제로 인해 오브젝트를 삭제하면 그리드 통합 연결의 다른 그리드에서 복제된 오브젝트는 삭제되지 않습니다. 하지만 S3 클라이언트에서 소스 버킷에 추가된 삭제 마커는 선택적으로 대상 버킷에 복제할 수 있습니다.

S3 클라이언트가 교차 그리드 복제가 활성화된 버킷에서 오브젝트를 삭제할 때 어떤 일이 발생하는지 이해하려면 S3 클라이언트가 버전 관리가 활성화된 버킷에서 오브젝트를 삭제하는 방법을 다음과 같이 검토하십시오.

- S3 클라이언트가 버전 ID가 포함된 삭제 요청을 실행하면 해당 오브젝트 버전이 영구적으로 제거됩니다. 버킷에 추가된 삭제 마커가 없습니다.
- S3 클라이언트가 버전 ID를 포함하지 않는 삭제 요청을 발행하는 경우 StorageGRID 어떤 객체 버전도 삭제하지 않습니다. 대신 버킷에 삭제 마커를 추가합니다. 삭제 마커를 사용하면 StorageGRID 개체가 삭제된 것처럼 작동합니다.

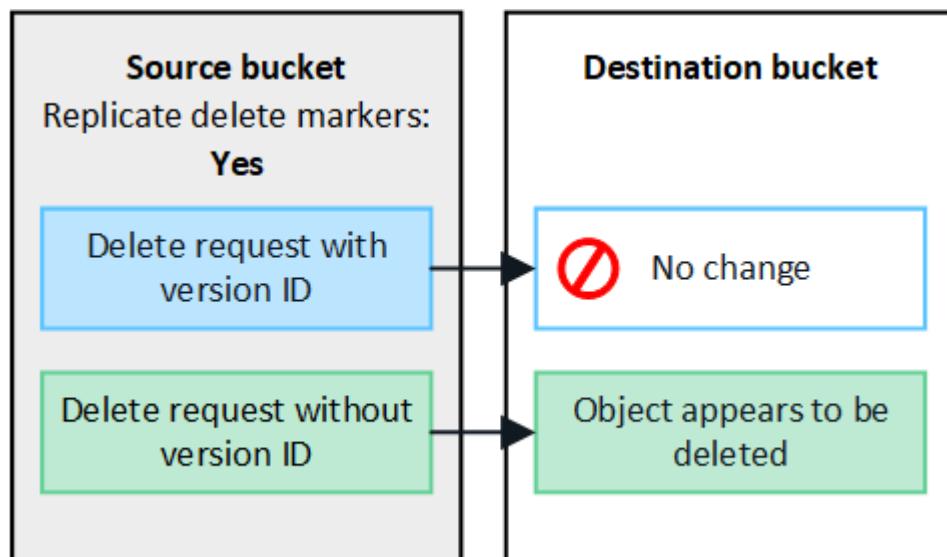
◦ 버전 ID가 없는 GetObject 요청은 다음과 같이 실패합니다. 404 No Object Found

◦ 유효한 버전 ID가 있는 GetObject 요청은 성공하고 요청된 개체 버전을 반환합니다.

S3 클라이언트가 교차 그리드 복제가 활성화된 버킷에서 오브젝트를 삭제하면 StorageGRID은 다음과 같이 삭제 요청을 대상에 복제할지 여부를 결정합니다.

- 삭제 요청에 버전 ID가 포함되어 있는 경우 해당 개체 버전은 소스 그리드에서 영구적으로 제거됩니다. 하지만 StorageGRID 버전 ID가 포함된 삭제 요청을 복제하지 않으므로 대상에서 동일한 개체 버전이 삭제되지 않습니다.
- 삭제 요청에 버전 ID가 포함되지 않은 경우 StorageGRID 버킷에 대해 크로스 그리드 복제가 구성된 방식에 따라 선택적으로 삭제 마커를 복제할 수 있습니다.
 - 삭제 마커(기본값)를 복제하도록 선택하면 삭제 마커가 소스 버킷에 추가되고 대상 버킷에 복제됩니다. 실제로 두 그리드에서 오브젝트가 삭제된 것으로 나타납니다.
 - 삭제 마커를 복제하지 않도록 선택하면 삭제 마커가 소스 버킷에 추가되지만 대상 버킷에는 복제되지 않습니다. 실제로 소스 그리드에서 삭제된 개체는 대상 그리드에서 삭제되지 않습니다.

그림에서 *삭제 마커 복제*는 *예*로 설정되었습니다. "교차 그리드 복제가 설정되었습니다". 버전 ID가 포함된 소스 버킷에 대한 삭제 요청은 대상 버킷의 개체를 삭제하지 않습니다. 버전 ID가 포함되지 않은 소스 버킷에 대한 삭제 요청은 대상 버킷의 객체를 삭제하는 것으로 보입니다.



그리드 간에 객체 삭제를 동기화된 상태로 유지하려면 "S3 라이프사이클 구성" 양쪽 그리드에서 버킷을 생성합니다.

암호화된 개체가 복제되는 방식

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

개별 오브젝트를 암호화하려면 소스 버킷에 오브젝트를 추가할 때 SSE(StorageGRID 관리 키가 있는 서버 측 암호화)를 사용할 수 있습니다. `x-amz-server-side-encryption` 요청 헤더를 사용하고 `AES256`을 "서버측 암호화를 사용합니다" 참조하십시오.



고객이 제공한 키를 사용한 서버 측 암호화(SSE-C)는 크로스 그리드 복제에 지원되지 않습니다. 수집 작업이 실패합니다.

버킷에 기본 암호화를 사용하려면 PutBucketEncryption 요청을 사용하고 SSEAlgorithm 매개 변수를로 AES256 설정합니다. 버킷 수준 암호화는 요청 헤더 없이 수집된 모든 객체에 `x-amz-server-side-encryption` 적용됩니다. 을 "[버킷 작업](#)" 참조하십시오.

그리드 수준 암호화를 사용하려면 * 저장된 오브젝트 암호화 * 옵션을 * AES-256 *로 설정합니다. 그리드 수준 암호화는 버킷 수준에서 암호화되지 않거나 요청 헤더 없이 수집된 모든 오브젝트에 x-amz-server-side-encryption 적용됩니다. 을 "[네트워크 및 개체 옵션을 구성합니다](#)" 참조하십시오.



SSE는 AES-128을 지원하지 않습니다. **AES-128** 옵션을 사용하여 소스 그리드에 대해 저장된 개체 암호화 옵션이 활성화된 경우, AES-128 알고리즘 사용이 복제된 개체로 전파되지 않습니다. 대신 복제된 개체는 대상의 기본 버킷이나 그리드 수준 암호화 설정(사용 가능한 경우)을 사용합니다.

소스 객체를 암호화하는 방법을 결정할 때 StorageGRID는 다음 규칙을 적용합니다.

1. `x-amz-server-side-encryption` 인제스트 헤더가 있는 경우 사용합니다.
2. 수집 헤더가 없으면 구성된 경우 버킷 기본 암호화 설정을 사용합니다.
3. 버킷 설정이 구성되지 않은 경우, 구성된 경우 그리드 전체 암호화 설정을 사용합니다.
4. 그리드 전체 설정이 없으면 소스 객체를 암호화하지 마세요.

복제된 개체를 암호화하는 방법을 결정할 때 StorageGRID는 다음 규칙을 다음 순서로 적용합니다.

1. 해당 개체에서 AES-128 암호화를 사용하지 않는 한 소스 개체와 동일한 암호화를 사용합니다.
2. 소스 개체가 암호화되지 않았거나 AES-128을 사용하는 경우 대상 버킷의 기본 암호화 설정(구성된 경우)을 사용합니다.
3. 대상 버킷에 암호화 설정이 없으면 대상의 그리드 전체 암호화 설정(구성된 경우)을 사용합니다.
4. 그리드 전체 설정이 없으면 대상 개체를 암호화하지 마세요.

S3 객체 잠금을 통한 크로스 그리드 복제

다음과 같은 상황에서 S3 개체 잠금이 활성화된 StorageGRID 버킷 간에 크로스 그리드 복제를 구성할 수 있습니다.

소스 버킷의 S3 객체 잠금이 설정된 경우...	그리고 대상 버킷의 S3 객체 잠금은...
활성화됨	활성화됨
장애가 있는	활성화됨

소스 버킷에서 S3 개체 잠금이 활성화된 경우:

- 대상에서 다음 순서대로 보존 설정을 사용하여 객체를 잠깁니다.

- a. 소스 개체의 보존 헤더 값:

x-amz-object-lock-mode

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

- b. 설정된 경우 소스 버킷의 기본 보존 기간입니다.
- c. 설정된 경우 대상 버킷의 기본 보존 기간입니다.

대상 버킷의 기본 보존 기간은 소스 개체에서 복제된 보존 기간 설정보다 우선하지 않습니다.

- 다음을 사용하여 대상 개체에 대한 법적 보류 상태를 설정할 수 있습니다. x-amz-object-lock-legal-hold 객체를 업로드할 때.
- 대상 테넌트 또는 버킷이 소스 개체의 S3 개체 잠금 설정을 지원하지 않으면 오류가 발생합니다. 다음을 참조하세요. "[그리드 간 복제 알림 및 오류](#)".

소스 버킷의 S3 개체 잠금이 비활성화된 경우:

- 대상 버킷에서 기본 보존 기간을 구성하여 대상 객체에 S3 객체 잠금 보존 기간을 적용할 수 있습니다.
- 대상 개체는 법적 보존 상태를 설정할 수 없습니다.

PutObjectTagging 및 **DeleteObjectTagging**은 지원되지 않습니다

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

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

PutObjectRetention 및 **PutObjectLegalHold**는 지원되지 않습니다.

PutObjectRetention 및 PutObjectLegalHold 요청은 크로스 그리드 복제가 활성화된 버킷의 개체에 대해 완전히 지원되지 않습니다.

S3 클라이언트가 PutObjectRetention 또는 PutObjectLegalHold 요청을 실행하면 소스 개체의 설정이 수정되지만 변경 사항은 대상에 적용되지 않습니다.

분할된 객체가 복제되는 방식

소스 그리드의 최대 세그먼트 크기는 대상 그리드에 복제된 개체에 적용됩니다. 객체가 다른 그리드에 복제되면 소스 그리드의 최대 세그먼트 크기 설정(구성 > 시스템 > 저장소 옵션)이 두 그리드 모두에 사용됩니다. 예를 들어, 소스 그리드의 최대 세그먼트 크기가 1GB이고 대상 그리드의 최대 세그먼트 크기가 50MB라고 가정해 보겠습니다. 소스 그리드에서 2GB 객체를 수집하는 경우 해당 객체는 두 개의 1GB 세그먼트로 저장됩니다. 해당 그리드의 최대 세그먼트 크기가 50MB인 경우에도 대상 그리드에 1GB 세그먼트 두 개로 복제됩니다.

교차 그리드 복제와 CloudMirror 복제를 비교합니다

그리드 페더레이션을 사용하기 시작할 때 및 의 유사점과 차이점을 "[교차 그리드 복제](#) ["StorageGRID CloudMirror 복제 서비스입니다"](#)" 검토하십시오.



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

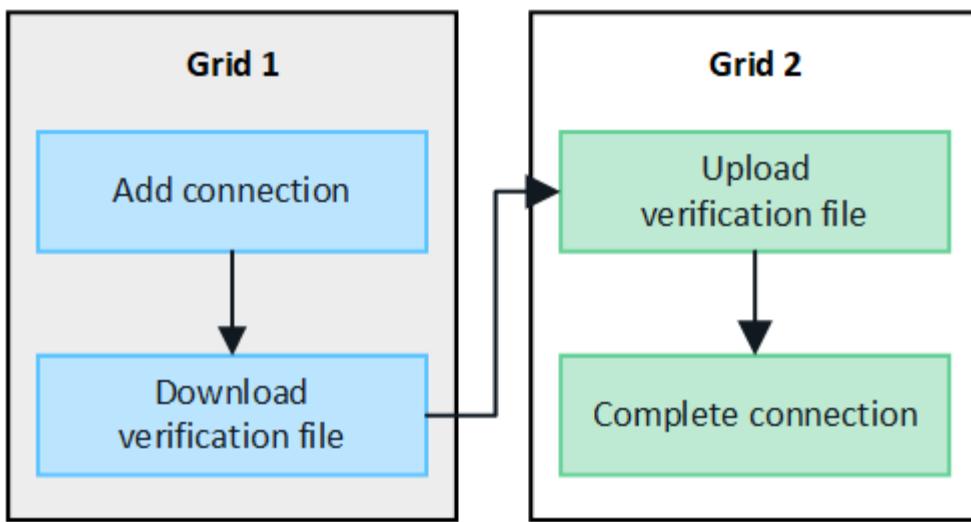
	교차 그리드 복제	CloudMirror 복제 서비스
주요 목적은 무엇입니까?	하나의 StorageGRID 시스템이 재해 복구 시스템 역할을 합니다. 버킷의 오브젝트는 한 방향 또는 두 방향으로 그리드 간에 복제될 수 있습니다.	테넌트가 StorageGRID(소스)의 버킷에서 외부 S3 버킷(대상)으로 오브젝트를 자동으로 복제할 수 있습니다. CloudMirror 복제는 독립적인 S3 인프라에서 객체의 독립적인 사본을 생성합니다. 이러한 독립적인 사본은 백업으로 사용되지 않지만, 종종 클라우드에서 추가 처리됩니다.
어떻게 설정합니까?	<ol style="list-style-type: none"> 두 그리드 간의 그리드 페더레이션 연결을 구성합니다. 다른 그리드에 자동으로 클론이 생성되는 새 테넌트 계정을 추가합니다. 클론 복제된 새 테넌트 그룹 및 사용자를 추가합니다. 각 그리드에 해당하는 버킷을 생성하고 교차 그리드 복제가 한 방향 또는 양쪽 방향으로 이루어질 수 있도록 합니다. 	<ol style="list-style-type: none"> 테넌트 사용자는 테넌트 관리자 또는 S3 API를 사용하여 CloudMirror 엔드포인트(IP 주소, 자격 증명 등)를 정의하여 CloudMirror 복제를 구성합니다. 해당 테넌트 계정이 소유한 버킷은 CloudMirror 엔드포인트를 가리키도록 구성할 수 있습니다.
누가 설정해야 합니까?	<ul style="list-style-type: none"> 그리드 관리자는 접속 및 테넌트를 구성합니다. 테넌트 사용자는 그룹, 사용자, 키 및 버킷을 구성합니다. 	일반적으로 테넌트 사용자입니다.
대상은 무엇입니까?	그리드 페더레이션 연결에서 다른 StorageGRID 시스템에 있는 상응하는 동일한 S3 버킷.	<ul style="list-style-type: none"> 모든 호환 가능한 S3 인프라(Amazon S3 포함). Google Cloud Platform(GCP)
오브젝트 버전 관리가 필요합니까?	예. 소스 및 대상 버킷 모두에 오브젝트 버전 관리가 활성화되어 있어야 합니다.	아니요. CloudMirror 복제는 소스 및 대상 모두에서 버전이 지정되지 않은 버킷과 버전 관리가 된 버킷의 조합을 지원합니다.
오브젝트를 대상으로 이동하는 원인은 무엇입니까?	객체가 교차 그리드 복제가 활성화된 버킷에 추가되면 자동으로 복제됩니다.	객체는 CloudMirror 엔드포인트로 구성된 버킷에 추가될 때 자동으로 복제됩니다. 버킷이 CloudMirror 엔드포인트로 구성되기 전에 소스 버킷에 있던 객체는 수정되지 않으면 복제되지 않습니다.
객체는 어떻게 복제됩니까?	교차 그리드 복제는 버전이 있는 오브젝트를 생성하고 소스 버킷에서 대상 버킷으로 버전 ID를 복제합니다. 이렇게 하면 버전 순서가 양쪽 그리드에 걸쳐 유지됩니다.	CloudMirror 복제에는 버전 관리가 활성화된 버킷이 필요하지 않으므로 CloudMirror는 사이트 내의 키에 대한 주문만 유지할 수 있습니다. 다른 사이트의 개체에 대한 요청에 대해 주문이 유지되도록 보장하는 것은 없습니다.

	교차 그리드 복제	CloudMirror 복제 서비스
개체를 복제할 수 없는 경우 어떻게 해야 합니까?	객체는 메타데이터 스토리지 제한에 따라 복제 대기열에 추가됩니다.	플랫폼 서비스 제한에 따라 객체가 복제를 위해 대기하고 있습니다(참조 "플랫폼 서비스 사용을 위한 권장 사항").
개체의 시스템 메타데이터가 복제됩니까?	예. 객체가 다른 그리드에 복제되면 해당 시스템 메타데이터도 복제됩니다. 메타데이터는 두 그리드에서 모두 동일합니다.	아니요. 객체가 외부 버킷에 복제되면 해당 시스템 메타데이터가 업데이트됩니다. 메타데이터는 수집 시간과 독립적인 S3 인프라의 동작에 따라 여러 위치에 따라 달라집니다.
객체를 검색하는 방법은 무엇입니까?	애플리케이션은 두 그리드 중 하나의 버킷에 대한 요청을 함으로써 객체를 검색하거나 읽을 수 있습니다.	애플리케이션은 StorageGRID 또는 S3 대상을 요청하여 오브젝트를 검색하거나 읽을 수 있습니다. 예를 들어 CloudMirror 복제를 사용하여 객체를 파트너 조직에 미러링한다고 가정합니다. 파트너는 자체 애플리케이션을 사용하여 S3 대상에서 직접 오브젝트를 읽거나 업데이트할 수 있습니다. StorageGRID를 사용할 필요가 없습니다.
개체를 삭제하면 어떻게 됩니까?	<ul style="list-style-type: none"> 버전 ID가 포함된 삭제 요청은 대상 그리드에 복제되지 않습니다. 버전 ID가 포함되지 않은 삭제 요청은 소스 버킷에 삭제 마커를 추가합니다. 이 마커는 대상 그리드에 선택적으로 복제할 수 있습니다. 교차 그리드 복제가 한 방향으로만 구성된 경우 소스에 영향을 주지 않고 대상 버킷의 오브젝트를 삭제할 수 있습니다. 	<p>결과는 소스 및 대상 버킷의 버전 관리 상태에 따라 달라집니다(동일할 필요는 없음).</p> <ul style="list-style-type: none"> 두 버킷의 버전이 모두 설정된 경우 삭제 요청은 두 위치에 삭제 마커를 추가합니다. 소스 버킷만 버전 관리되는 경우 삭제 요청이 원본에 삭제 표식을 추가하지만 대상에는 추가하지 않습니다. 버킷의 버전이 지정되지 않은 경우 삭제 요청이 소스에서 개체를 삭제하지만 대상에서 삭제하지는 않습니다. <p>마찬가지로, 소스에 영향을 주지 않고 대상 버킷의 오브젝트를 삭제할 수 있습니다.</p>

그리드 페더레이션 연결을 만듭니다

테넌트 세부 정보의 클론을 생성하고 객체 데이터를 복제하려는 경우 두 StorageGRID 시스템 간에 그리드 페더레이션 연결을 생성할 수 있습니다.

그림에 표시된 것처럼 그리드 페더레이션 연결을 만드는 작업은 두 그리드 모두에 대한 단계를 포함합니다. 한 그리드에 연결을 추가하고 다른 그리드에서 연결을 완료합니다. 두 눈금 중 하나에서 시작할 수 있습니다.



시작하기 전에

- 그리드 페더레이션 연결을 구성하기 위해 을 검토했습니다. "[고려 사항 및 요구 사항](#)"
- IP 또는 VIP 주소 대신 각 그리드에 대해 FQDN(정규화된 도메인 이름)을 사용하려는 경우 사용할 이름을 알고 각 그리드의 DNS 서버에 적절한 항목이 있는지 확인합니다.
- 을 사용하고 "[지원되는 웹 브라우저](#)"입니다.
- 두 그리드 모두에 대한 루트 액세스 권한과 프로비저닝 암호가 있습니다.

연결을 추가합니다

두 StorageGRID 시스템 중 하나에서 다음 단계를 수행합니다.

단계

- 두 그리드 중 하나의 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
- 구성 > 시스템 > *그리드 연합*을 선택합니다.
- 연결 추가 * 를 선택합니다.
- 연결에 대한 세부 정보를 입력합니다.

필드에 입력합니다	설명
연결 이름입니다	이 연결을 쉽게 인식할 수 있는 고유한 이름(예: "그리드 1 - 그리드 2")
이 그리드의 FQDN 또는 IP입니다	<p>다음 중 하나:</p> <ul style="list-style-type: none"> 현재 로그인한 그리드의 FQDN입니다 이 그리드에서 HA 그룹의 VIP 주소입니다 이 그리드에 있는 관리 노드 또는 게이트웨이 노드의 IP 주소입니다. IP는 대상 그리드가 연결할 수 있는 모든 네트워크에 있을 수 있습니다.

필드에 입력합니다	설명
포트	<p>이 연결에 사용할 포트입니다. 사용하지 않는 포트 번호는 23000에서 23999까지 입력할 수 있습니다.</p> <p>이 연결의 두 그리드는 동일한 포트를 사용합니다. 두 그리드 중 어떤 노드도 다른 연결에 이 포트를 사용하지 않도록 해야 합니다.</p>
이 그리드에 대한 인증서 유효 일일입니다	<p>연결에서 이 그리드에 대한 보안 인증서를 유효하게 만들 일 수입니다. 기본값은 730일(2년)이지만 1일에서 762일 사이의 값을 입력할 수 있습니다.</p> <p>StorageGRID는 연결을 저장할 때 각 그리드에 대해 클라이언트 및 서버 인증서를 자동으로 생성합니다.</p>
이 그리드에 대한 프로비저닝 암호입니다	로그인한 그리드의 프로비저닝 암호입니다.
다른 그리드의 FQDN 또는 IP입니다	<p>다음 중 하나:</p> <ul style="list-style-type: none"> • 연결할 그리드의 FQDN입니다 • 다른 그리드에서 HA 그룹의 VIP 주소입니다 • 다른 그리드에 있는 관리 노드 또는 게이트웨이 노드의 IP 주소입니다. IP는 소스 그리드가 연결할 수 있는 모든 네트워크에 있을 수 있습니다.

5. Save and continue * 를 선택합니다.

6. 다운로드 확인 파일 단계에서 * 확인 파일 다운로드 * 를 선택합니다.

다른 그리드에서 연결이 완료된 후에는 두 그리드 중 하나에서 확인 파일을 더 이상 다운로드할 수 없습니다.

7. 다운로드한 파일을 찾아 (`connection-name.grid-federation` 안전한 위치에 저장합니다.



이 파일에는 비밀(마스킹된 AS) 및 기타 민감한 정보가 포함되어 * 있으므로 안전하게 저장하고 전송해야 합니다.

8. 그리드 페더레이션 페이지로 돌아가려면 * 닫기 * 를 선택합니다.

9. 새 연결이 표시되고 해당 * 연결 상태 * 가 * 연결 대기 * 인지 확인합니다.

10. `connection-name.grid-federation` 다른 그리드의 그리드 관리자에게 파일을 제공합니다.

연결을 완료합니다

연결 중인 StorageGRID 시스템(다른 그리드)에서 다음 단계를 수행합니다.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인합니다.

2. 구성 > 시스템 > *그리드 연합*을 선택합니다.

3. 업로드 페이지에 액세스하려면 * 검증 파일 업로드 * 를 선택합니다.
4. 검증 파일 업로드 * 를 선택합니다. 그런 다음 첫 번째 그리드에서 다운로드한 파일을 찾아 (`connection-name.grid-federation` 선택합니다).

연결에 대한 세부 정보가 표시됩니다.

5. 필요에 따라 이 그리드의 보안 인증서에 대해 다른 유효 일수를 입력합니다. 인증서 유효 일 * 항목은 기본적으로 첫 번째 그리드에 입력한 값으로 설정되지만 각 그리드에는 서로 다른 만료 날짜를 사용할 수 있습니다.

일반적으로 연결의 양쪽에 있는 인증서에 대해 동일한 일 수를 사용합니다.



연결 끝 중 하나의 인증서가 만료되면 연결이 중지되고 인증서가 업데이트될 때까지 복제가 보류됩니다.

6. 현재 로그인한 그리드의 프로비저닝 암호를 입력합니다.
7. Save and test * 를 선택합니다.

인증서가 생성되고 연결이 테스트됩니다. 연결이 유효한 경우 성공 메시지가 나타나고 새 연결이 그리드 페더레이션 페이지에 나열됩니다. 연결 상태 * 는 * 연결됨 * 이 됩니다.

오류 메시지가 나타나면 문제를 해결하십시오. 을 ["그리드 통합 오류 문제 해결"](#) 참조하십시오.

8. 첫 번째 그리드의 그리드 페더레이션 페이지로 이동하여 브라우저를 새로 고칩니다. 연결 상태 * 가 지금 * 연결됨 * 인지 확인합니다.
9. 연결이 설정되면 확인 파일의 모든 복사본을 안전하게 삭제합니다.

이 연결을 편집하면 새 확인 파일이 생성됩니다. 원본 파일을 다시 사용할 수 없습니다.

작업을 마친 후

- 에 대한 고려 사항을 ["허용된 테넌트 관리"](#) 검토합니다.
- ["하나 이상의 새 테넌트 계정을 생성합니다"](#) 을 클릭하고 * 그리드 페더레이션 연결 사용 * 권한을 할당하고 새 연결을 선택합니다.
- ["연결을 관리합니다"](#) 필요한 경우. 연결 값을 편집하거나, 연결을 테스트하거나, 연결 인증서를 회전하거나, 연결을 제거할 수 있습니다.
- ["연결을 모니터링합니다"](#) 를 일반적인 StorageGRID 모니터링 활동의 일부로 활용합니다.
- ["연결 문제를 해결합니다"](#) 계정 클론 및 교차 그리드 복제와 관련된 경고 및 오류 해결을 포함합니다.

그리드 페더레이션 연결을 관리합니다

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

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인되어 ["지원되는 웹 브라우저"](#) 있습니다.
- 로그인한 그리드에 대한 가 ["루트 액세스 권한"](#) 있습니다.

[[EDIT_GRID_FED_CONNECTION]] 그리드 페더레이션 연결을 편집합니다

연결의 두 그리드 중 하나에서 기본 관리 노드에 로그인하여 그리드 페더레이션 연결을 편집할 수 있습니다. 첫 번째 그리드를 변경한 후에는 새 검증 파일을 다운로드하여 다른 그리드에 업로드해야 합니다.



연결을 편집하는 동안 계정 클론 또는 교차 그리드 복제 요청은 기존 연결 설정을 계속 사용합니다. 첫 번째 격자에 대한 편집 내용은 로컬에 저장되지만 두 번째 격자에 업로드되고 저장 및 테스트될 때까지 사용되지 않습니다.

연결 편집을 시작합니다

단계

1. 두 그리드 중 하나의 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
2. *노드*를 선택하고 시스템의 다른 모든 관리 노드가 온라인인지 확인하세요.



그리드 페더레이션 연결을 편집할 때 StorageGRID는 첫 번째 그리드의 모든 관리 노드에 "대상 구성" 파일을 저장하려고 시도합니다. 이 파일을 모든 관리 노드에 저장할 수 없는 경우 * 저장 및 테스트 *를 선택하면 경고 메시지가 나타납니다.

3. 구성 > 시스템 > *그리드 연합*을 선택합니다.
4. 그리드 페더레이션 페이지의 * 작업 * 메뉴 또는 특정 연결에 대한 세부 정보 페이지를 사용하여 연결 세부 정보를 편집합니다. 입력할 항목은 ["그리드 페더레이션 연결을 만듭니다"](#) 참조하십시오.

작업 메뉴

- a. 연결에 사용할 라디오 버튼을 선택합니다.
- b. Actions * > * Edit *를 선택합니다.
- c. 새 정보를 입력합니다.

세부 정보 페이지

- a. 세부 정보를 표시할 연결 이름을 선택합니다.
- b. 편집 *를 선택합니다.
- c. 새 정보를 입력합니다.

5. 로그인한 그리드의 프로비저닝 암호를 입력합니다.

6. Save and continue *를 선택합니다.

새 값은 저장되지만 다른 그리드에 새 검증 파일을 업로드하기 전에는 연결에 적용되지 않습니다.

7. 검증 파일 다운로드 *를 선택합니다.

나중에 이 파일을 다운로드하려면 연결에 대한 세부 정보 페이지로 이동합니다.

8. 다운로드한 파일을 찾아 (`connection-name.grid-federation` 안전한 위치에 저장합니다).



확인 파일에는 비밀이 포함되어 있으며 안전하게 저장하고 전송해야 합니다.

9. 그리드 페더레이션 페이지로 돌아가려면 * 닫기 * 를 선택합니다.

10. 연결 상태 * 가 * 편집 보류 * 인지 확인합니다.



연결 편집을 시작할 때 연결 상태가 * 연결됨 * 이 아닌 경우 * 편집 보류 * 로 변경되지 않습니다.

11. `connection-name.grid-federation` 다른 그리드의 그리드 관리자에게 파일을 제공합니다.

연결 편집을 마칩니다

다른 그리드에 확인 파일을 업로드하여 연결 편집을 마칩니다.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인합니다.

2. 구성 > 시스템 > *그리드 연합*을 선택합니다.

3. 업로드 페이지에 액세스하려면 * 검증 파일 업로드 * 를 선택합니다.

4. 검증 파일 업로드 * 를 선택합니다. 그런 다음 첫 번째 그리드에서 다운로드한 파일을 찾아 선택합니다.

5. 현재 로그인한 그리드의 프로비저닝 암호를 입력합니다.

6. Save and test * 를 선택합니다.

편집한 값을 사용하여 연결을 설정할 수 있으면 성공 메시지가 나타납니다. 그렇지 않으면 오류 메시지가 나타납니다. 메시지를 검토하고 문제를 해결합니다.

7. 마법사를 닫고 그리드 페더레이션 페이지로 돌아갑니다.

8. 연결 상태 * 가 * 연결됨 * 인지 확인합니다.

9. 첫 번째 그리드의 그리드 페더레이션 페이지로 이동하여 브라우저를 새로 고칩니다. 연결 상태 * 가 지금 * 연결됨 * 인지 확인합니다.

10. 연결이 설정되면 확인 파일의 모든 복사본을 안전하게 삭제합니다.

[[TEST_GRID_FED_CONNECTION]] 그리드 페더레이션 연결을 테스트합니다

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인합니다.

2. 구성 > 시스템 > *그리드 연합*을 선택합니다.

3. 그리드 페더레이션 페이지의 * 작업 * 메뉴 또는 특정 연결에 대한 세부 정보 페이지를 사용하여 연결을 테스트합니다.

작업 메뉴

- a. 연결에 사용할 라디오 버튼을 선택합니다.
- b. Actions * > * Test * 를 선택합니다.

세부 정보 페이지

- a. 세부 정보를 표시할 연결 이름을 선택합니다.
- b. Test connection * 을 선택합니다.

4. 연결 상태를 검토합니다.

연결 상태입니다	설명
연결되었습니다	두 그리드 모두 연결되어 있고 정상적으로 통신하고 있습니다.
오류	연결이 오류 상태입니다. 예를 들어 인증서가 만료되었거나 구성 값이 더 이상 유효하지 않습니다.
편집 보류 중	이 그리드에서 연결을 편집했지만 연결이 여전히 기존 구성 사용하고 있습니다. 편집을 완료하려면 새 검증 파일을 다른 그리드에 업로드합니다.
연결 대기 중입니다	이 그리드에서 연결을 구성했지만 다른 그리드에서 연결이 완료되지 않았습니다. 이 그리드에서 확인 파일을 다운로드하여 다른 그리드에 업로드합니다.
알 수 없음	네트워크 문제 또는 오프라인 노드로 인해 연결이 알 수 없는 상태입니다.

5. 연결 상태가 * 오류 * 인 경우 모든 문제를 해결하십시오. 그런 다음 * Test connection * 을 다시 선택하여 문제가 해결되었는지 확인합니다.

연결 인증서를 회전합니다

각 그리드 페더레이션 연결은 자동으로 생성된 4개의 SSL 인증서를 사용하여 연결을 보호합니다. 각 그리드의 만료 날짜 근처에 두 개의 인증서가 있으면 * 그리드 페더레이션 인증서 만료 * 알림이 인증서를 회전하도록 알려 줍니다.



연결 끝 중 하나의 인증서가 만료되면 연결이 중지되고 인증서가 업데이트될 때까지 복제가 보류됩니다.

단계

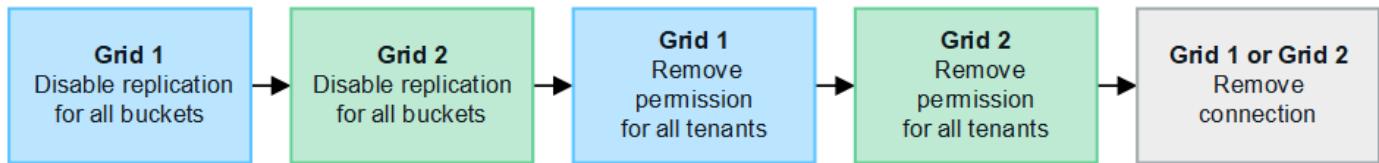
1. 두 그리드 중 하나의 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
2. 구성 > 시스템 > *그리드 연합*을 선택합니다.
3. Grid Federation(그리드 통합) 페이지의 어느 탭에서든 세부 정보를 표시할 연결 이름을 선택합니다.
4. 인증서 * 탭을 선택합니다.
5. 인증서 회전 * 을 선택합니다.
6. 새 인증서가 유효해야 하는 일 수를 지정합니다.

7. 로그인한 그리드의 프로비저닝 암호를 입력합니다.
8. 인증서 회전 * 을 선택합니다.
9. 필요에 따라 연결의 다른 격자에서 이 단계를 반복합니다.

일반적으로 연결의 양쪽에 있는 인증서에 대해 동일한 일 수를 사용합니다.

그리드 페더레이션 연결을 제거합니다

연결의 각 그리드에서 그리드 페더레이션 연결을 제거할 수 있습니다. 그림에 표시된 것처럼 두 그리드에 대해 선행 단계를 수행하여 두 그리드 중 하나의 테넌트에서 연결이 사용되고 있지 않은지 확인해야 합니다.



연결을 제거하기 전에 다음 사항에 유의하십시오.

- 연결을 제거해도 그리드 간에 이미 복사된 항목은 삭제되지 않습니다. 예를 들어, 테넌트의 권한이 제거되면 두 그리드에 있는 테넌트 사용자, 그룹 및 객체가 두 그리드 모두에서 삭제되지 않습니다. 이러한 항목을 삭제하려면 두 그리드 모두에서 수동으로 삭제해야 합니다.
- 연결을 제거하면 대기 중인 복제(수집되었지만 아직 다른 그리드에 복제되지 않은) 객체가 영구적으로 복제되지 않습니다.

모든 테넌트 버킷에 대한 복제를 비활성화합니다

단계

1. 두 그리드 중 하나에서 시작하여 기본 관리 노드에서 그리드 관리자에 로그인합니다.
2. 구성 > 시스템 > *그리드 연합*을 선택합니다.
3. 세부 정보를 표시할 연결 이름을 선택합니다.
4. 허용된 테넌트 * 탭에서 테넌트가 연결을 사용 중인지 확인합니다.
5. 테넌트가 나열되면 모든 테넌트가 연결의 두 그리드에 있는 모든 버킷에 대해 에 지시합니다. "["크로스 그리드 복제를 비활성화합니다"](#)"



테넌트 버킷에 교차 그리드 복제가 활성화된 경우 * 그리드 통합 연결 사용 * 권한을 제거할 수 없습니다. 각 테넌트 계정은 양쪽 그리드의 해당 버킷에 대해 교차 그리드 복제를 비활성화해야 합니다.

각 테넌트에 대한 권한을 제거합니다

모든 테넌트 버킷에 대해 교차 그리드 복제를 비활성화한 후 두 그리드의 모든 테넌트에서 * 그리드 통합 사용 권한 * 을 제거합니다.

단계

1. 구성 > 시스템 > *그리드 연합*을 선택합니다.
2. 세부 정보를 표시할 연결 이름을 선택합니다.

- 허용된 테넌트 * 탭의 각 테넌트에 대해 각 테넌트에서 * 그리드 페더레이션 연결 사용 * 권한을 제거합니다. 을 "허용된 테넌트 관리" 참조하십시오.
- 다른 그리드에서 허용된 테넌트에 대해 이 단계를 반복합니다.

연결을 제거합니다

단계

- 두 그리드 중 어느 한 테넌트가 연결을 사용하고 있지 않으면 * 제거 * 를 선택합니다.
- 확인 메시지를 검토하고 * 제거 * 를 선택합니다.
 - 연결을 제거할 수 있는 경우 성공 메시지가 표시됩니다. 그리드 페더레이션 연결이 이제 두 그리드에서 제거됩니다.
 - 연결을 제거할 수 없는 경우(예: 여전히 사용 중이거나 연결 오류가 있는 경우) 오류 메시지가 표시됩니다. 다음 중 하나를 수행할 수 있습니다.
 - 오류를 해결합니다(권장). 을 "그리드 통합 오류 문제 해결" 참조하십시오.
 - 강제로 연결을 제거합니다. 다음 섹션을 참조하십시오.

그리드 페더레이션 연결을 강제로 제거합니다

필요한 경우 * Connected * 상태가 없는 연결을 강제로 제거할 수 있습니다.

강제 제거는 로컬 격자에서 연결을 삭제만 합니다. 연결을 완전히 제거하려면 두 그리드에서 동일한 단계를 수행합니다.

단계

- 확인 대화 상자에서 * 강제 제거 * 를 선택합니다.

성공 메시지가 나타납니다. 이 그리드 페더레이션 연결은 더 이상 사용할 수 없습니다. 그러나 테넌트 버킷은 여전히 교차 그리드 복제를 사용하고 일부 오브젝트 복사본은 연결의 그리드 간에 이미 복제되었을 수 있습니다.
- 연결의 다른 그리드에서 기본 관리 노드에서 그리드 관리자에 로그인합니다.
- 구성 > 시스템 > *그리드 연합*을 선택합니다.
- 세부 정보를 표시할 연결 이름을 선택합니다.
- 제거 * 및 * 예 * 를 선택합니다.
- 이 그리드에서 연결을 제거하려면 * 강제 제거 * 를 선택합니다.

그리드 페더레이션을 위해 허용된 테넌트를 관리합니다

S3 테넌트 계정에서 두 StorageGRID 시스템 간의 그리드 페더레이션 연결을 사용하도록 허용할 수 있습니다. 테넌트가 연결을 사용할 수 있는 경우 테넌트 세부 정보를 편집하거나 연결을 사용할 테넌트의 권한을 영구적으로 제거하려면 특별한 단계가 필요합니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인되어 "지원되는 웹 브라우저" 있습니다.
- 로그인한 그리드에 대한 가 "루트 액세스 권한" 있습니다.
- "그리드 페더레이션 연결을 만들었습니다" 두 그리드 사이에 있습니다.

- 및에 대한 워크플로를 검토했습니다."[계정 클론](#)""[교차 그리드 복제](#)"
- 필요한 경우 이미 SSO(Single Sign-On)를 구성했거나 연결의 두 그리드에 대한 페더레이션을 식별했습니다. 을 "[계정 클론이란 무엇입니까](#)"참조하십시오.

허용된 테넌트를 생성합니다

새 테넌트 계정이나 기존 테넌트 계정에서 계정 클론 생성 및 교차 그리드 복제에 그리드 페더레이션 연결을 사용하도록 허용하려면 또는 "[테넌트 계정을 편집합니다](#)"의 일반 지침을 "[새 S3 테넌트를 생성합니다](#)"따르고 다음 사항에 유의하십시오.

- 연결의 두 그리드 중 하나에서 테넌트를 생성할 수 있습니다. 테넌트가 생성되는 그리드는 _ 테넌트의 소스 그리드 _ 입니다.
- 연결 상태는 * 연결됨 * 이어야 합니다.
- 테넌트를 만들거나 편집하여 * 그리드 페더레이션 연결 사용 * 권한을 활성화한 다음 첫 번째 그리드에 저장하면 동일한 테넌트가 자동으로 다른 그리드에 복제됩니다. 테넌트가 복제되는 그리드는 _ 테넌트의 대상 그리드 _ 입니다.
- 두 그리드의 테넌트는 동일한 20자리 계정 ID, 이름, 설명, 할당량 및 권한을 갖습니다. 선택적으로 * Description * 필드를 사용하여 소스 테넌트와 대상 테넌트를 식별할 수 있습니다. 예를 들어 그리드 1에서 생성된 테넌트에 대한 이 설명은 그리드 2에 복제된 테넌트에 대해서도 나타납니다. "이 테넌트는 그리드 1에 생성되었습니다."
- 보안상의 이유로 로컬 루트 사용자의 암호는 대상 그리드에 복사되지 않습니다.



로컬 루트 사용자가 대상 그리드에서 복제된 테넌트에 로그인하려면 먼저 해당 그리드의 그리드 관리자가 있어야 "[로컬 루트 사용자의 암호를 변경합니다](#)"합니다.

- 두 그리드 모두에서 새 테넌트 또는 편집된 테넌트를 사용할 수 있게 되면 테넌트 사용자는 다음 작업을 수행할 수 있습니다.
 - 테넌트의 소스 그리드에서 그룹과 로컬 사용자를 생성합니다. 이 그룹은 테넌트의 대상 그리드에 자동으로 복제됩니다. 을 "[클론 테넌트 그룹 및 사용자](#)"참조하십시오.
 - 필요에 따라 테넌트의 대상 그리드에 클론 복제할 수 있는 새 S3 액세스 키를 생성합니다. 을 "[API를 사용하여 S3 액세스 키의 클론을 생성합니다](#)"참조하십시오.
 - 연결의 두 그리드에 동일한 버킷을 생성하고 한 방향 또는 양쪽 방향에서 크로스 그리드 복제를 가능하게 합니다. 을 "[교차 그리드 복제 관리](#)"참조하십시오.

허용된 테넌트를 봅니다

그리드 페더레이션 연결을 사용하도록 허용된 테넌트에 대한 세부 정보를 볼 수 있습니다.

단계

1. *세입자*를 선택하세요.
2. 테넌트 페이지에서 테넌트 이름을 선택하여 테넌트 세부 정보 페이지를 표시합니다.

테넌트의 소스 그리드(즉, 테넌트가 이 그리드에 생성된 경우)인 경우 테넌트가 다른 그리드에 클론 생성되었다는 배너가 나타납니다. 이 테넌트를 편집하거나 삭제하면 변경 내용이 다른 눈금에 동기화되지 않습니다.

tenant A for grid federation

Tenant ID:	0899 6970 1700 0930 0009	<input type="checkbox"/>	Quota	—
Protocol:	S3		utilization:	
Object count:	0		Logical space used:	0 bytes
			Quota:	—

Description: this tenant was created on Grid 1

[Sign in](#)

[Edit](#)

[Actions ▾](#)



This tenant has been cloned to another grid. If you edit or delete this tenant, your changes will not be synced to the other grid.

[Space breakdown](#)

[Allowed features](#)

[Grid federation](#)

[Remove permission](#)

[Clear error](#)

[Search...](#)



Displaying one result

Connection name

Connection status

Remote grid hostname

Last error



Grid 1 to Grid 2

Connected

10.96.106.230

[Check for errors](#)

3. 필요에 따라 * Grid Federation * 탭을 선택합니다."그리드 페더레이션 연결을 모니터링합니다".

허용된 테넌트를 편집합니다

그리드 페더레이션 연결 사용* 권한이 있는 테넌트를 편집해야 하는 경우에 대한 일반 지침을 "[테넌트 계정 편집](#)"따르고 다음 사항에 유의하십시오.

- 테넌트에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 연결의 각 그리드에서 테넌트 세부 정보를 편집할 수 있습니다. 그러나 변경한 내용은 다른 눈금에 복사되지 않습니다. 테넌트 세부 정보를 그리드 간에 동기화된 상태로 유지하려면 두 그리드에 대해 동일한 편집 작업을 수행해야 합니다.
- 테넌트를 편집할 때 * 그리드 페더레이션 연결 사용 * 권한을 지울 수 없습니다.
- 테넌트를 편집할 때는 다른 그리드 페더레이션 연결을 선택할 수 없습니다.

허용된 테넌트를 삭제합니다

그리드 페더레이션 연결 사용* 권한이 있는 테넌트를 제거해야 하는 경우에 대한 일반 지침을 "[테넌트 계정을 삭제하는 중입니다](#)"따르고 다음 사항에 유의하십시오.

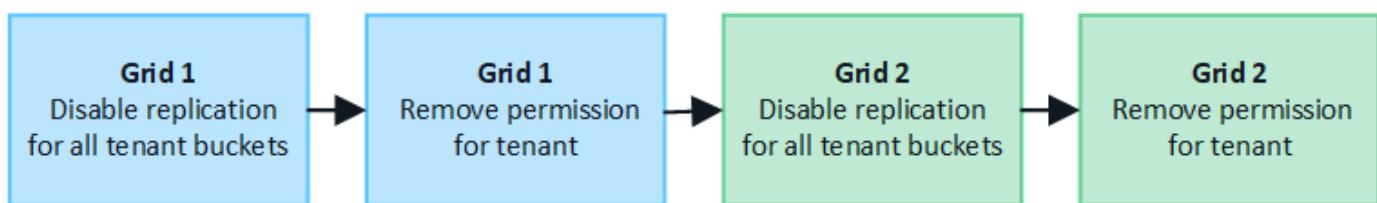
- 소스 그리드에서 원래 테넌트를 제거하려면 먼저 소스 그리드에서 해당 계정에 대한 모든 버킷을 제거해야 합니다.

- 대상 그리드에서 복제된 테넌트를 제거하려면 먼저 대상 그리드에서 계정에 대한 모든 버킷을 제거해야 합니다.
- 원래 테넌트 또는 복제된 테넌트를 제거하면 해당 계정을 더 이상 교차 그리드 복제에 사용할 수 없습니다.
- 소스 그리드에서 원래 테넌트를 제거하는 경우 대상 그리드에 클론 복제된 테넌트 그룹, 사용자 또는 키는 영향을 받지 않습니다. 클론 생성된 테넌트를 삭제하거나 해당 테넌트가 자신의 그룹, 사용자, 액세스 키 및 버킷을 관리하도록 허용할 수 있습니다.
- 대상 그리드에서 복제된 테넌트를 제거하는 경우 새 그룹 또는 사용자가 원래 테넌트에 추가되면 클론 오류가 발생합니다.

이러한 오류를 방지하려면 이 그리드에서 테넌트를 삭제하기 전에 그리드 페더레이션 연결을 사용하도록 테넌트의 권한을 제거합니다.

그리드 페더레이션 연결 사용 권한을 제거합니다

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



그리드 페더레이션 연결을 사용하는 테넌트의 권한을 제거하기 전에 다음 사항에 유의하십시오.

- 테넌트의 버킷에서 교차 그리드 복제가 활성화된 경우 * 그리드 페더레이션 연결 사용 * 권한을 제거할 수 없습니다. 테넌트 계정은 먼저 모든 버킷에 대해 교차 그리드 복제를 비활성화해야 합니다.
- 그리드 통합 연결 사용 * 권한을 제거해도 그리드 간에 이미 복제된 항목은 삭제되지 않습니다. 예를 들어, 테넌트의 사용 권한이 제거되면 두 그리드에 있는 테넌트 사용자, 그룹 및 객체가 두 그리드 모두에서 삭제되지 않습니다. 이러한 항목을 삭제하려면 두 그리드 모두에서 수동으로 삭제해야 합니다.
- 동일한 그리드 페더레이션 연결을 사용하여 이 권한을 다시 활성화하려면 먼저 대상 그리드에서 이 테넌트를 삭제하십시오. 그렇지 않으면 이 권한을 다시 설정하면 오류가 발생합니다.



그리드 페더레이션 연결 사용 * 권한을 다시 활성화하면 로컬 그리드가 소스 그리드로 바뀌고 선택한 그리드 페더레이션 연결에 지정된 원격 그리드에 대한 복제가 트리거됩니다. 테넌트 계정이 이미 원격 그리드에 있는 경우 클론 생성으로 인해 충돌 오류가 발생합니다.

시작하기 전에

- 을 사용하고 "지원되는 웹 브라우저"입니다.
- 두 그리드 모두에 대한 가 "루트 액세스 권한"입니다.

테넌트 버킷에 대한 복제를 비활성화합니다

첫 번째 단계로 모든 테넌트 버킷에 대해 교차 그리드 복제를 비활성화합니다.

단계

1. 두 그리드 중 하나에서 시작하여 기본 관리 노드에서 그리드 관리자에 로그인합니다.
2. 구성 > 시스템 > *그리드 연합*을 선택합니다.

3. 세부 정보를 표시할 연결 이름을 선택합니다.
4. 허용된 테넌트 * 탭에서 테넌트가 연결을 사용 중인지 확인합니다.
5. 테넌트가 나열되면 연결의 두 그리드에 있는 모든 버킷을 에 대해 으로 "[크로스 그리드 복제를 비활성화합니다](#)"안내합니다.



테넌트 버킷에 교차 그리드 복제가 활성화된 경우 * 그리드 통합 연결 사용 * 권한을 제거할 수 없습니다. 테넌트는 두 그리드의 해당 버킷에 대해 교차 그리드 복제를 비활성화해야 합니다.

테넌트에 대한 권한을 제거합니다

테넌트 버킷에 대해 교차 그리드 복제를 비활성화한 후 그리드 페더레이션 연결을 사용할 수 있는 테넌트의 권한을 제거할 수 있습니다.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
2. 그리드 페더레이션 페이지 또는 테넌트 페이지에서 권한을 제거합니다.

그리드 페더레이션 페이지

- a. 구성 > 시스템 > *그리드 연합*을 선택합니다.
- b. 세부 정보 페이지를 표시하려면 연결 이름을 선택합니다.
- c. 허용된 테넌트 * 탭에서 테넌트에 대한 라디오 버튼을 선택합니다.
- d. 권한 제거 * 를 선택합니다.

Tenants 페이지

- a. *세입자*를 선택하세요.
- b. 세부 정보 페이지를 표시하려면 테넌트 이름을 선택합니다.
- c. Grid Federation * (그리드 통합 *) 탭에서 연결에 대한 라디오 버튼을 선택합니다.
- d. 권한 제거 * 를 선택합니다.

3. 확인 대화 상자에서 경고를 검토하고 * 제거 * 를 선택합니다.
 - 권한을 제거할 수 있는 경우 세부 정보 페이지로 돌아가며 성공 메시지가 표시됩니다. 이 테넌트는 더 이상 그리드 페더레이션 연결을 사용할 수 없습니다.
 - 하나 이상의 테넌트 버킷에서 교차 그리드 복제가 활성화된 경우 오류가 표시됩니다.

⚠ Remove permission to use grid federation connection

X

Are you sure you want to prevent **Tenant A** from performing account sync and cross-grid replication using grid federation connection **Grid 1-Grid 2**?

- Removing this permission does not delete any items that have already been copied to the other grid.
- After removing this permission for the tenant on this grid, go to the other grid and remove the permission for the corresponding tenant account.

✖ Connection '5427cbf8-0dd0-4b83-a2c8-e5e23cc49cc5' is used by bucket 'my-cgr-bucket' for cross-grid replication, so it can't be removed. From Tenant Manager, remove the cross-grid configuration from the tenant bucket and retry.

⚠ Using **Force remove** removes the tenant's permission to use the grid federation connection even if tenant buckets still have cross-grid replication enabled. When the permission is removed, data in these buckets can no longer be copied between the grids.

Cancel

Force remove

Remove

다음 중 하나를 수행할 수 있습니다.

- (권장) 테넌트 관리자에 로그인하고 각 테넌트의 버킷에 대한 복제를 비활성화합니다. 을 "교차 그리드 복제 관리"참조하십시오. 그런 다음 단계를 반복하여 * 그리드 연결 사용 * 권한을 제거합니다.
- 권한을 강제로 제거합니다. 다음 섹션을 참조하십시오.

4. 다른 그리드로 이동하여 이 단계를 반복하여 다른 그리드에서 동일한 테넌트에 대한 권한을 제거합니다.

권한을 강제로 제거합니다

필요한 경우 테넌트 버킷에 교차 그리드 복제가 활성화되어 있는 경우에도 테넌트의 권한 제거를 통해 그리드 페더레이션 연결을 사용하도록 할 수 있습니다.

테넌트의 권한을 강제로 제거하기 전에 에 대한 일반적인 고려 사항 및 다음과 같은 추가 고려 사항에 **권한을 제거합니다**유의하십시오.

- 그리드 페더레이션 연결 사용 * 권한을 강제로 제거하면 다른 그리드(수집되었지만 아직 복제되지 않음)로 복제 보류 중인 모든 객체가 계속 복제됩니다. 이러한 처리 중인 객체가 대상 버킷에 도달하지 않도록 하려면 다른 그리드에 대한 테넌트의 권한도 제거해야 합니다.

- 그리드 통합 연결 사용 * 권한을 제거한 후 소스 버킷으로 인제된 모든 오브젝트는 대상 버킷에 복제되지 않습니다.

단계

1. 기본 관리자 노드에서 그리드 관리자에 로그인합니다.
2. 구성 > 시스템 > *그리드 연합*을 선택합니다.
3. 세부 정보 페이지를 표시하려면 연결 이름을 선택합니다.
4. 허용된 테넌트 * 탭에서 테넌트에 대한 라디오 버튼을 선택합니다.
5. 권한 제거 * 를 선택합니다.
6. 확인 대화 상자에서 경고를 검토하고 * 강제 제거 * 를 선택합니다.

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

7. 필요한 경우 다른 그리드로 이동하여 이 단계를 반복하여 다른 그리드에서 동일한 테넌트 계정에 대한 권한을 강제로 제거합니다. 예를 들어, 다른 그리드에서 이 단계를 반복하여 처리 중인 오브젝트가 대상 버킷에 도달하지 못하게 해야 합니다.

그리드 통합 오류 문제 해결

그리드 페더레이션 연결, 계정 클론 및 교차 그리드 복제와 관련된 경고 및 오류를 해결해야 할 수 있습니다.

그리드 페더레이션 연결 경고 및 오류

그리드 페더레이션 연결에서 경고를 받거나 오류가 발생할 수 있습니다.

연결 문제를 해결하기 위해 변경한 후 연결을 테스트하여 연결 상태가 * 연결됨 * 으로 돌아가는지 확인합니다. 자세한 내용은 ["그리드 페더레이션 연결을 관리합니다"](#) 참조하십시오.

그리드 페더레이션 연결 실패 알림

문제

그리드 페더레이션 연결 실패 * 경고가 트리거되었습니다.

세부 정보

이 알림은 그리드 간의 그리드 페더레이션 연결이 작동하지 않음을 나타냅니다.

권장 조치

1. 두 그리드에 대한 Grid Federation(그리드 통합) 페이지의 설정을 검토합니다. 모든 값이 올바른지 확인합니다. 을 ["그리드 페더레이션 연결을 관리합니다"](#) 참조하십시오.
2. 연결에 사용되는 인증서를 검토합니다. 만료된 그리드 페더레이션 인증서에 대한 알림이 없고 각 인증서에 대한 세부 정보가 유효한지 확인합니다. 에서 연결 인증서 회전에 대한 지침을 ["그리드 페더레이션 연결을 관리합니다"](#) 참조하십시오.
3. 양쪽 그리드의 모든 관리자 및 게이트웨이 노드가 온라인 상태이고 사용 가능한지 확인합니다. 이러한 노드에 영향을 줄 수 있는 알림을 모두 해결한 후 다시 시도하십시오.
4. 로컬 또는 원격 그리드에 대해 FQDN(정규화된 도메인 이름)을 제공한 경우 DNS 서버가 온라인 상태이고 사용 가능한지 확인합니다. 네트워킹, IP 주소 및 DNS 요구 사항은 ["그리드 페더레이션은 무엇입니까?"](#) 참조하십시오.

그리드 페더레이션 인증서 알림의 만료

문제

그리드 페더레이션 인증서 만료 * 알림이 트리거되었습니다.

세부 정보

이 알림은 하나 이상의 그리드 페더레이션 인증서가 곧 만료됨을 나타냅니다.

권장 조치

에서 연결 인증서 회전에 대한 지침을 "[그리드 페더레이션 연결을 관리합니다](#)" 참조하십시오.

그리드 페더레이션 연결을 편집하는 동안 오류가 발생했습니다

문제

그리드 페더레이션 연결을 편집할 때 * 저장 및 테스트 * 를 선택하면 "하나 이상의 노드에서 대상 구성 파일을 만들지 못했습니다."라는 경고 메시지가 표시됩니다.

세부 정보

그리드 페더레이션 연결을 편집할 때 StorageGRID는 첫 번째 그리드의 모든 관리 노드에 "대상 구성" 파일을 저장하려고 시도합니다. 관리 노드가 오프라인이기 때문에 이 파일을 모든 관리 노드에 저장할 수 없는 경우 경고 메시지가 나타납니다.

권장 조치

1. 연결을 편집하는 데 사용하는 그리드에서 *노드*를 선택합니다.
2. 해당 그리드의 모든 관리 노드가 온라인 상태인지 확인합니다.
3. 노드가 오프라인인 경우 노드를 다시 온라인 상태로 전환하고 연결을 다시 편집하십시오.

계정 클론 오류입니다

복제된 테넌트 계정에 로그인할 수 없습니다

문제

복제된 테넌트 계정에 로그인할 수 없습니다. Tenant Manager 로그인 페이지의 오류 메시지는 "이 계정에 대한 자격 증명이 잘못되었습니다. 다시 시도하십시오."

세부 정보

보안상의 이유로 테넌트 계정의 클론을 테넌트의 소스 그리드에서 테넌트의 대상 그리드로 생성할 때 테넌트의 로컬 루트 사용자에 대해 설정한 암호는 복제되지 않습니다. 마찬가지로 테넌트가 소스 그리드에 로컬 사용자를 생성할 때 로컬 사용자 암호가 대상 그리드에 복제되지 않습니다.

권장 조치

루트 사용자가 테넌트의 대상 그리드에 로그인하려면 먼저 그리드 관리자가 대상 그리드에서 로그인해야 "[로컬 루트 사용자의 암호를 변경합니다](#)" 합니다.

복제된 로컬 사용자가 테넌트의 대상 그리드에 로그인하려면 먼저 복제된 테넌트의 루트 사용자가 대상 그리드에서 해당 사용자의 비밀번호를 추가해야 합니다. 지침은 다음을 참조하세요. "[사용자 관리](#)" 테넌트 관리자 사용에 대한 지침에서.

클론 없이 테넌트가 생성되었습니다

문제

Use GRID Federation connection * 권한으로 새 테넌트를 생성한 후 "클론 없이 테넌트가 생성됨"이라는 메시지가 표시됩니다.

세부 정보

이 문제는 연결 상태 업데이트가 지연되어 상태가 불량한 연결이 * 연결됨 * 으로 나열되는 경우에 발생할 수 있습니다.

권장 조치

1. 오류 메시지에 나열된 이유를 검토하고 연결이 작동하지 않을 수 있는 네트워킹 또는 기타 문제를 해결합니다. 을 [그리드 페더레이션 연결 경고 및 오류 참조](#)하십시오.
2. 지침에 따라 에서 그리드 페더레이션 연결을 "[그리드 페더레이션 연결을 관리합니다](#)" 테스트하여 문제가 해결되었는지 확인합니다.
3. 테넌트의 소스 그리드에서 *테넌트*를 선택합니다.
4. 클론 생성에 실패한 테넌트 계정을 찾습니다.
5. 테넌트 이름을 선택하여 세부 정보 페이지를 표시합니다.
6. 계정 클론 재시도 * 를 선택합니다.

The screenshot shows the Grid interface with a tenant named 'test'. The tenant details are as follows:

Tenant ID:	0040 2213 8117 4859 6503	Protocol:	S3	Object count:	0	Quota utilization:	—
				Logical space used:	0 bytes	Quota:	—

Below the tenant details are three buttons: 'Sign in', 'Edit', and 'Actions ▾'.

A red error message box contains the following text:

✖ Tenant account could not be cloned to the other grid.
Reason: Internal server error. The server encountered an error and could not complete your request. Try again. If the problem persists, contact support. Internal Server Error

[Retry account clone](#)

오류가 해결된 경우 테넌트 계정은 이제 다른 그리드에 복제됩니다.

교차 그리드 복제 경고 및 오류

연결 또는 테넌트에 대해 마지막 오류가 표시됩니다

문제

"[그리드 페더레이션 연결 보기](#)" 연결 세부 정보 페이지의 * 마지막 오류 * 열에 오류가 있는 경우(또는 연결 시 "[허용된 테넌트 관리](#)") 예를 들면 다음과 같습니다.

Grid 1 - Grid 2

Local hostname (this grid): 10.115.96.170
Port: 23000
Remote hostname (other grid): 10.115.96.175
Connection status:  Connected

[Edit](#) [Download file](#) [Test connection](#) [Remove](#)

[Permitted tenants](#) [Certificates](#)

[Remove permission](#) [Clear error](#) 

Displaying one result

Tenant name	Last error
Tenant A	2025-03-13 15:45:59 PDT Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-bucket' to destination bucket 'my-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled. (logID 13371653720226059496)

[Check for errors](#)

세부 정보

각 그리드 연합 연결의 마지막 오류 열에는 테넌트의 데이터가 다른 그리드로 복제될 때 발생한 가장 최근의 오류(있는 경우)가 표시됩니다. 이 열에는 마지막으로 발생한 그리드 간 복제 오류만 표시되며, 이전에 발생했을 수 있는 오류는 표시되지 않습니다. 이 열의 오류는 다음과 같은 이유 중 하나로 발생할 수 있습니다.

- 소스 개체 버전을 찾을 수 없습니다.
- 소스 버킷을 찾을 수 없습니다.
- 대상 버킷이 삭제되었습니다.
- 대상 버킷이 다른 계정에 의해 다시 생성되었습니다.
- 대상 버킷에 버전 관리가 일시 중지되었습니다.
- 대상 버킷은 동일한 계정으로 다시 생성되었지만 현재는 버전이 지정되지 않았습니다.
- 소스 개체에 대상 그리드의 테넌트 수준 보존 설정을 준수하지 않는 S3 개체 잠금 설정이 있습니다.
- 소스 객체에는 S3 객체 잠금 설정이 있고, 대상 버킷에서는 S3 객체 잠금이 비활성화되어 있습니다.

권장 조치

마지막 오류 * 열에 오류 메시지가 나타나면 다음 단계를 수행하십시오.

1. 메시지 텍스트를 검토합니다.
2. 권장되는 작업을 수행합니다. 예를 들어 교차 그리드 복제를 위해 대상 버킷에서 버전 관리가 일시 중단된 경우 해당 버킷의 버전 관리를 다시 사용하도록 설정합니다.
3. 테이블에서 접속 또는 테넌트 계정을 선택합니다.
4. Clear error * 를 선택합니다.
5. 메시지를 지우고 시스템 상태를 업데이트하려면 * 예 * 를 선택하십시오.
6. 5-6분 정도 기다린 다음 새 오브젝트를 버킷에 넣습니다. 오류 메시지가 다시 나타나지 않는지 확인합니다.



오류 메시지가 지워졌는지 확인하려면 새 개체를 수신하기 전에 메시지의 타임스탬프가 나타난 후 5분 이상 기다립니다.



오류를 지운 후 오류가 있는 다른 버킷에서 오브젝트를 섭취할 경우 새 * 마지막 오류 * 가 나타날 수 있습니다.

7. 버킷 오류로 인해 객체를 복제하지 못했는지 확인하려면 을 참조하십시오."실패한 복제 작업을 식별하고 다시 시도하십시오"

교차 그리드 복제 영구 실패 알림

문제

Cross-grid replication permanent failure * 알림이 트리거되었습니다.

세부 정보

이 알림은 사용자가 해결해야 하는 이유 때문에 두 그리드의 버킷 간에 테넌트 객체를 복제할 수 없음을 나타냅니다. 이 알림은 일반적으로 소스 또는 대상 버킷의 변경으로 인해 발생합니다.

권장 조치

1. 경고가 트리거된 그리드에 로그인합니다.
2. 구성 > 시스템 > *그리드 연합*으로 이동하여 알림에 나열된 연결 이름을 찾습니다.
3. 허용된 테넌트 탭에서 * 마지막 오류 * 열을 확인하여 오류가 있는 테넌트 계정을 확인합니다.
4. 오류에 대한 자세한 내용은 의 지침을 "[그리드 페더레이션 연결을 모니터링합니다](#)"참조하여 교차 그리드 복제 메트릭을 검토하십시오.
5. 영향을 받는 각 테넌트 계정에 대해 다음을 수행합니다.
 - a. 테넌트가 교차 그리드 복제를 위해 대상 그리드에서 할당량을 초과하지 않았는지 확인하려면 의 지침을 "[테넌트 작업을 모니터링합니다](#)"참조하십시오.
 - b. 필요에 따라 새 객체를 저장할 수 있도록 대상 그리드에 대한 테넌트 할당량을 늘리십시오.
6. 영향을 받는 각 테넌트의 경우 두 그리드의 테넌트 관리자에 로그인하여 버킷 목록을 비교할 수 있습니다.
7. 교차 그리드 복제가 활성화된 각 버킷에 대해 다음을 확인합니다.
 - 다른 그리드에 동일한 테넌트의 해당 버킷이 있습니다(정확한 이름을 사용해야 함).
 - 두 버킷에는 모두 개체 버전 관리가 활성화되어 있습니다(두 그리드 중 하나에서 버전 관리를 중단할 수 없음).
 - 버킷이 * 오브젝트 삭제: 읽기 전용 * 상태에 있지 않습니다.
8. 문제가 해결되었는지 확인하려면 의 지침을 "[그리드 페더레이션 연결을 모니터링합니다](#)"참조하여 교차 그리드 복제 메트릭을 검토하거나 다음 단계를 수행하십시오.
 - a. 그리드 페더레이션 페이지로 돌아갑니다.
 - b. 영향을 받는 테넌트를 선택하고 * Last error * (마지막 오류 *) 열에서 * Clear Error * (오류 지우기 *)를 선택합니다.
 - c. 메시지를 지우고 시스템 상태를 업데이트하려면 * 예 * 를 선택하십시오.
 - d. 5-6분 정도 기다린 다음 새 오브젝트를 버킷에 넣습니다. 오류 메시지가 다시 나타나지 않는지 확인합니다.



오류 메시지가 지워졌는지 확인하려면 새 개체를 수신하기 전에 메시지의 타임스탬프가 나타난 후 5분 이상 기다립니다.



알림이 해결된 후 지우는 데 하루 정도 걸릴 수 있습니다.

- a. 로 "[실패한 복제 작업을 식별하고 다시 시도하십시오](#)"이동하여 다른 그리드로 복제되지 않은 개체를 식별하거나 마커를 삭제하고 필요에 따라 복제를 다시 시도하십시오.

교차 그리드 복제 리소스를 사용할 수 없음 경고

문제

Cross-grid replication resource unavailable * 경고가 트리거되었습니다.

세부 정보

이 알림은 리소스를 사용할 수 없기 때문에 교차 그리드 복제 요청이 보류 중임을 나타냅니다. 예를 들어, 네트워크 오류가 있을 수 있습니다.

권장 조치

1. 알림을 모니터링하여 문제가 자체적으로 해결되는지 확인합니다.
2. 문제가 지속되면 동일한 연결에 대해 * 그리드 페더레이션 연결 실패 * 경고가 있는지 또는 노드에 대한 * 노드 * 경고와 통신할 수 없는지 확인합니다. 이 경고는 이러한 경고를 해결할 때 해결될 수 있습니다.
3. 오류에 대한 자세한 내용은 의 지침을 "[그리드 페더레이션 연결을 모니터링합니다](#)"참조하여 교차 그리드 복제 메트릭을 검토하십시오.
4. 알림을 해결할 수 없는 경우 기술 지원 팀에 문의하십시오.

문제가 해결된 후에는 교차 그리드 복제가 정상적으로 진행됩니다.

실패한 복제 작업을 식별하고 다시 시도하십시오

Cross-grid replication permanent failure * 경고를 해결한 후에는 어떤 개체나 삭제 표식을 다른 그리드에 복제하지 못했는지 확인해야 합니다. 그런 다음 이러한 객체를 다시 수집하거나 Grid Management API를 사용하여 복제를 다시 시도할 수 있습니다.

Cross-grid replication permanent failure * 알림은 사용자 개입이 필요한 이유로 두 그리드의 버킷 간에 테넌트 객체를 복제할 수 없음을 나타냅니다. 이 알림은 일반적으로 소스 또는 대상 버킷의 변경으로 인해 발생합니다. 자세한 내용은 [을 참조하십시오 "그리드 통합 오류 문제 해결"](#).

복제하지 못한 개체가 있는지 확인합니다

개체 또는 삭제 표식이 다른 그리드에 복제되지 않았는지 확인하려면 감사 로그에서 메시지를 검색할 "[CGRR\(Cross-Grid Replication Request\)](#)"수 있습니다. 이 메시지는 StorageGRID가 대상 버킷에 오브젝트, 다중 파트 오브젝트 또는 삭제 마커를 복제하지 못할 때 로그에 추가됩니다.

을 사용하여 결과를 읽기 쉬운 형식으로 변환할 수 "[감사 - 설명 도구](#)"있습니다.

시작하기 전에

- 루트 액세스 권한이 있습니다.

- `Passwords.txt` 파일이 있습니다.
- 기본 관리 노드의 IP 주소를 알고 있습니다.

단계

1. 기본 관리자 노드에 로그인합니다.
 - a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
 - b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
 - c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
 - d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 \$ 로 '#' 변경됩니다.

2. `audit.log`에서 CGRR 메시지를 검색하고 감사 설명 도구를 사용하여 결과를 포맷합니다.

예를 들어 이 명령은 지난 30분 동안 모든 CGRR 메시지에 대해 `greps`를 수행하고 감사 설명 도구를 사용합니다.

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date {
print }' audit.log | grep CGRR | audit-explain
```

명령의 결과는 이 예와 같이 되며, 이 예제에는 6개의 CGRR 메시지에 대한 항목이 있습니다. 이 예에서는 모든 크로스 그리드 복제 요청이 객체를 복제할 수 없기 때문에 일반 오류를 반환했습니다. 처음 세 가지 오류는 "객체 복제" 작업이고, 마지막 세 가지 오류는 "마커 복제" 작업용입니다.

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error

CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error

CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error

CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

각 항목에는 다음 정보가 포함되어 있습니다.

필드에 입력합니다	설명
CGRR 교차 그리드 복제 요청	요청 이름입니다
테넌트	테넌트의 계정 ID입니다
연결	그리드 패더레이션 연결의 ID입니다
작동	시도 중인 복제 작업의 유형: <ul style="list-style-type: none">• 오브젝트 복제• 삭제 마커를 복제합니다• 다중 파트 개체를 복제합니다
버킷	버킷 이름입니다
오브젝트	개체 이름입니다
버전	객체의 버전 ID입니다
오류	오류 유형입니다. 크로스 그리드 복제에 실패한 경우 오류는 "일반 오류"입니다.

실패한 복제를 다시 시도하십시오

객체 목록을 생성하고 대상 버킷에 복제되지 않은 마커를 삭제하고 기본 문제를 해결한 후 다음 두 가지 방법 중 하나로 복제를 재시도할 수 있습니다.

- 각 오브젝트를 소스 버킷으로 재수집하십시오.
- 그리드 관리 전용 API를 사용합니다(설명 참조).

단계

1. Grid Manager 상단에서 도움말 아이콘을 선택하고 * API documentation * 을 선택합니다.
2. 전용 API 문서로 이동 * 을 선택합니다.



"비공개"로 표시된 StorageGRID API 끝점은 예고 없이 변경될 수 있습니다. StorageGRID 전용 엔드포인트도 요청의 API 버전을 무시합니다.

3. Cross-grid-replication-advanced * 섹션에서 다음 끝점을 선택합니다.

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

4. 체험하기 * 를 선택합니다.
5. body * 텍스트 상자에서 * versionID * 의 예제 항목을 실패한 교차 그리드 복제 요청에 해당하는 audit.log 의 버전 ID로 바꿉니다.

문자열 주위에 큰따옴표를 붙여야 합니다.

6. Execute * 를 선택합니다.
7. 서버 응답 코드가 * 204 * 인지 확인합니다. 이는 개체 또는 삭제 마커가 다른 그리드에 교차 그리드 복제를 위해 보류 중으로 표시되었음을 나타냅니다.



보류 중 은 교차 그리드 복제 요청이 처리를 위해 내부 대기열에 추가되었음을 의미합니다.

복제 재시도를 모니터링합니다

복제 재시도 작업을 모니터링하여 작업이 완료되었는지 확인해야 합니다.



개체 또는 삭제 마커를 다른 그리드에 복제하려면 몇 시간 이상이 걸릴 수 있습니다.

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

- S3 사용 "[HeadObject 를 선택합니다](#)" 또는 "[GetObject 를 참조하십시오](#)" 요청 응답에는 다음 값 중 하나가 있는 StorageGRID 관련 x-ntap-sg-cgr-replication-status 응답 헤더가 포함됩니다.

그리드	복제 상태입니다
출처	<ul style="list-style-type: none">• * 완료됨 *: 복제가 성공했습니다.• * 보류 중 *: 객체가 아직 복제되지 않았습니다.• * 실패 *: 영구적인 장애로 인해 복제에 실패했습니다. 사용자가 오류를 해결해야 합니다.
목적지	<ul style="list-style-type: none">• replica *: 객체가 소스 그리드에서 복제되었습니다.

- 그리드 관리 전용 API를 사용합니다(설명 참조).

단계

1. 전용 API 설명서의 * cross-grid-replication-advanced * 섹션에서 다음 끝점을 선택합니다.

```
GET /private/cross-grid-replication-object-status/{id}
```

2. 체험하기 * 를 선택합니다.
3. 매개 변수 섹션에서 요청에 사용한 버전 ID를 cross-grid-replication-retry-failed 입력합니다.
4. Execute * 를 선택합니다.
5. 서버 응답 코드가 * 200 * 인지 확인합니다.
6. 다음 중 하나인 복제 상태를 검토합니다.
 - * 보류 중 *: 객체가 아직 복제되지 않았습니다.
 - * 완료됨 *: 복제가 성공했습니다.
 - * 실패 *: 영구적인 장애로 인해 복제에 실패했습니다. 사용자가 오류를 해결해야 합니다.

보안 관리

보안 관리

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

암호화 관리

StorageGRID는 데이터 암호화를 위한 여러 옵션을 제공합니다. "사용 가능한 암호화 방법을 검토합니다" 데이터 보호 요구사항을 충족하는 솔루션을 결정해야 합니다.

인증서를 관리합니다

HTTP 연결이나 서버에 대한 클라이언트 또는 사용자 ID를 인증하는 데 사용되는 클라이언트 인증서에 사용할 수 "서버 인증서를 구성하고 관리합니다" 있습니다.

키 관리 서버를 구성합니다

를 "키 관리 서버입니다" 사용하면 어플라이언스를 데이터 센터에서 제거할 경우에도 StorageGRID 데이터를 보호할 수 있습니다. 어플라이언스 볼륨이 암호화된 후에는 노드에서 KMS와 통신할 수 없는 한 어플라이언스의 데이터에 액세스할 수 없습니다.



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

프록시 설정을 관리합니다

S3 플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 스토리지 노드와 외부 S3 엔드 포인트 간에 를 구성할 수 "스토리지 프록시 서버입니다" 있습니다. HTTPS 또는 HTTP를 사용하여 AutoSupport 패키지를 보내는 경우 관리 노드와 기술 지원 간에 를 구성할 수 있습니다"관리 프록시 서버".

방화벽을 제어합니다

시스템 보안을 강화하기 위해 에서 특정 포트를 열거나 닫아 StorageGRID 관리 노드에 대한 액세스를 제어할 수 있습니다"외부 방화벽". 또한 노드를 구성하여 각 노드에 대한 네트워크 액세스를 제어할 수도 "내부 방화벽" 있습니다. 배포에 필요한 포트를 제외한 모든 포트에 대한 액세스를 차단할 수 있습니다.

StorageGRID 암호화 방법을 검토합니다

StorageGRID는 데이터 암호화를 위한 여러 옵션을 제공합니다. 사용 가능한 방법을 검토하여 데이터 보호 요구 사항을 충족하는 방법을 결정해야 합니다.

이 표는 StorageGRID에서 사용할 수 있는 암호화 방법에 대한 상위 수준의 요약을 제공합니다.

암호화 옵션	작동 방식	적용 대상
Grid Manager의 키 관리 서버(KMS)	<p>"키 관리 서버를 구성합니다" "StorageGRID 사이트 및 "어플라이언스에 대해 노드 암호화를 활성화합니다"의 경우 그런 다음 어플라이언스 노드가 KMS에 연결하여 키 암호화 키(KEK)를 요청합니다. 이 키는 각 볼륨의 DEK(데이터 암호화 키)를 암호화하고 해독합니다.</p>	<p>설치 중에 * 노드 암호화 * 가 활성화된 어플라이언스 노드 어플라이언스의 모든 데이터는 물리적 손실이나 데이터 센터에서 제거되는 것을 방지합니다.</p> <ul style="list-style-type: none"> 참고 *: KMS를 사용한 암호화 키 관리는 스토리지 노드 및 서비스 어플라이언스에서만 지원됩니다.
StorageGRID 어플라이언스 설치 프로그램의 드라이브 암호화 페이지	<p>어플라이언스에 하드웨어 암호화를 지원하는 드라이브가 포함된 경우 설치 중에 드라이브 암호를 설정할 수 있습니다. 드라이브 암호를 설정하면 암호를 모르는 경우 시스템에서 제거된 드라이브에서 유효한 데이터를 복구할 수 없습니다. 설치를 시작하기 전에 * 하드웨어 구성 * > * 드라이브 암호화 *로 이동하여 노드의 모든 StorageGRID에서 관리하는 자체 암호화 드라이브에 적용되는 드라이브 암호를 설정하십시오.</p>	<p>자체 암호화 드라이브를 포함하는 어플라이언스: 보안 드라이브의 모든 데이터는 데이터 센터에서 물리적 손실 또는 제거로부터 보호됩니다.</p> <p>드라이브 암호화는 SANtricity에서 관리하는 드라이브에는 적용되지 않습니다. 자체 암호화 드라이브와 SANtricity 컨트롤러가 포함된 스토리지 어플라이언스가 있는 경우 SANtricity에서 드라이브 보안을 활성화할 수 있습니다.</p>
SANtricity 시스템 관리자의 드라이브 보안	<p>StorageGRID 어플라이언스에 드라이브 보안 기능이 활성화된 경우를 사용하여 보안 키를 생성하고 관리할 수 "SANtricity 시스템 관리자" 있습니다. 보안 드라이브의 데이터에 액세스하려면 키가 필요합니다.</p>	<p>FDE(전체 디스크 암호화) 드라이브 또는 자체 암호화 드라이브를 사용하는 스토리지 어플라이언스 보안 드라이브의 모든 데이터는 데이터 센터에서 물리적 손실 또는 제거로부터 보호됩니다. 일부 스토리지 어플라이언스나 서비스 어플라이언스와 함께 사용할 수 없습니다.</p>
저장된 오브젝트 암호화	<p>"저장된 오브젝트 암호화" 그리드 관리자에서 옵션을 활성화합니다. 이 기능을 사용하도록 설정하면 버킷 레벨이나 오브젝트 레벨에서 암호화되지 않은 새로운 모든 객체가 수집 중에 암호화됩니다.</p>	<p>새로 수집된 S3 오브젝트 데이터 저장된 기존 객체는 암호화되지 않습니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다.</p>
S3 버킷 암호화	<p>버킷에 대한 암호화를 사용하도록 설정하기 위한 PutBucketEncryption 요청을 발행합니다. 오브젝트 레벨에서 암호화되지 않은 새로운 모든 오브젝트는 수집 중에 암호화됩니다.</p>	<p>새로 수집된 S3 오브젝트 데이터만 버킷에 대해 암호화를 지정해야 합니다. 기존 버킷 객체는 암호화되지 않습니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다.</p> <p>"버킷 작업"</p>

암호화 옵션	작동 방식	적용 대상
S3 오브젝트 서버 측 암호화(SSE)	S3 요청을 실행하여 객체를 저장하고 x-amz-server-side- encryption 요청 헤더를 포함합니다.	새로 수집된 S3 오브젝트 데이터만 객체에 대해 암호화를 지정해야 합니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다. StorageGRID가 키를 관리합니다. "서버측 암호화를 사용합니다"
고객이 제공한 키(SSE-C)를 사용한 S3 오브젝트 서버 측 암호화	S3 요청을 발급하여 오브젝트를 저장하고 세 개의 요청 헤더를 포함시킵니다. <ul style="list-style-type: none"> • x-amz-server-side- encryption-customer- algorithm • x-amz-server-side- encryption-customer-key • x-amz-server-side- encryption-customer- key-MD5 	새로 수집된 S3 오브젝트 데이터만 객체에 대해 암호화를 지정해야 합니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다. 키는 StorageGRID 외부에서 관리됩니다. "서버측 암호화를 사용합니다"
외부 볼륨 또는 데이터 저장소 암호화	구축 플랫폼에서 지원하는 경우 StorageGRID 외부의 암호화 방법을 사용하여 전체 볼륨 또는 데이터 저장소를 암호화합니다.	모든 볼륨 또는 데이터 저장소가 암호화되었다고 가정할 때 모든 오브젝트 데이터, 메타데이터 및 시스템 구성 데이터입니다. 외부 암호화 방법을 사용하면 암호화 알고리즘 및 키를 보다 강력하게 제어할 수 있습니다. 나열된 다른 방법과 결합할 수 있습니다.
StorageGRID 외부에서 개체 암호화	StorageGRID 외부에서 암호화 방법을 사용하여 오브젝트 데이터 및 메타데이터를 StorageGRID에 수집하기 전에 암호화합니다.	오브젝트 데이터 및 메타데이터만 (시스템 구성 데이터는 암호화되지 않음). 외부 암호화 방법을 사용하면 암호화 알고리즘 및 키를 보다 강력하게 제어할 수 있습니다. 나열된 다른 방법과 결합할 수 있습니다. "Amazon Simple Storage Service - 사용자 가이드: 클라이언트 측 암호화를 사용하여 데이터 보호"

여러 암호화 방법을 사용합니다

요구 사항에 따라 한 번에 두 가지 이상의 암호화 방법을 사용할 수 있습니다. 예를 들면 다음과 같습니다.

- KMS를 사용하여 어플라이언스 노드를 보호하고 SANtricity 시스템 관리자의 드라이브 보안 기능을 사용하여 동일한 어플라이언스에 있는 자체 암호화 드라이브의 데이터를 "이중 암호화"할 수 있습니다.
- KMS를 사용하여 어플라이언스 노드의 데이터를 보호할 수 있으며 저장된 개체 암호화 옵션을 사용하여 수집될 때 모든 개체를 암호화할 수 있습니다.

오브젝트의 일부 부분만 암호화해야 하는 경우 대신 버킷 또는 개별 오브젝트 수준에서 암호화를 제어하는 것이 좋습니다. 여러 수준의 암호화를 사용하면 추가 성능 비용이 듭니다.

관련 정보

["FIPS 인증 암호화 옵션에 대해 알아보세요"](#)

인증서를 관리합니다

보안 인증서를 관리합니다

보안 인증서는 StorageGRID 구성 요소와 StorageGRID 구성 요소 및 외부 시스템 간에 안전하고 신뢰할 수 있는 연결을 만드는 데 사용되는 작은 데이터 파일입니다.

StorageGRID는 두 가지 유형의 보안 인증서를 사용합니다.

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

클라이언트가 HTTPS를 사용하여 서버에 연결하면 서버는 공개 키가 포함된 서버 인증서로 응답합니다. 클라이언트는 서버 서명을 인증서 사본의 서명과 비교합니다. 서명이 일치하면 클라이언트는 동일한 공개 키를 사용하여 서버와 세션을 시작합니다.

StorageGRID는 로드 밸런서 끝점과 같은 일부 연결에 대한 서버 또는 CloudMirror 복제 서비스와 같은 다른 연결에 대한 클라이언트로 작동합니다.

- 기본 그리드 CA 인증서 *

StorageGRID에는 시스템 설치 중에 내부 Grid CA 인증서를 생성하는 내장 인증 기관(CA)이 있습니다. Grid CA 인증서는 기본적으로 내부 StorageGRID 트래픽을 보호하는데 사용됩니다. 외부 인증 기관(CA)은 조직의 정보 보안 정책을 완벽하게 준수하는 맞춤형 인증서를 발급할 수 있습니다.

비생산 환경에서는 Grid CA 인증서를 사용하세요. 생산의 경우 외부 인증 기관에서 서명한 사용자 정의 인증서를 사용하세요. 인증서가 없는 보안되지 않은 연결은 지원되지만 권장되지는 않습니다.

- 사용자 지정 CA 인증서는 내부 인증서를 제거하지 않지만 사용자 지정 인증서는 서버 연결을 확인하기 위해 지정된 인증서여야 합니다.
- 모든 사용자 지정 인증서는 를 충족해야 ["서버 인증서에 대한 시스템 강화 지침"](#)합니다.
- StorageGRID는 CA의 인증서를 단일 파일(CA 인증서 번들이라고 함)로 번들링하는 것을 지원합니다.



StorageGRID에는 모든 그리드에서 동일한 운영 체제 CA 인증서도 포함됩니다. 프로덕션 환경에서는 운영 체제 CA 인증서 대신 외부 인증 기관에서 서명한 사용자 지정 인증서를 지정해야 합니다.

서버 및 클라이언트 인증서 유형의 변형은 여러 가지 방법으로 구현됩니다. 시스템을 구성하기 전에 특정 StorageGRID 구성에 필요한 모든 인증서를 준비해야 합니다.

보안 인증서에 액세스합니다

각 인증서의 구성 워크플로 링크와 함께 모든 StorageGRID 인증서에 대한 정보에 액세스할 수 있습니다.

단계

1. Grid Manager에서 구성 > 보안 > *인증서*를 선택합니다.

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Name	Description	Type	Expiration date
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. 인증서 페이지에서 탭을 선택하여 각 인증서 범주에 대한 정보를 확인하고 인증서 설정에 액세스합니다. 가 있는 경우 탭에 액세스할 수 "적절한 권한"입니다.

- * 글로벌 *: 웹 브라우저 및 외부 API 클라이언트에서 StorageGRID 액세스를 보호합니다.
- * 그리드 CA *: 내부 StorageGRID 트래픽을 보호합니다.
- * 클라이언트 *: 외부 클라이언트와 StorageGRID Prometheus 데이터베이스 간의 연결을 보호합니다.
- * 로드 밸런서 엔드포인트 *: S3 클라이언트와 StorageGRID 로드 밸런서 간의 연결을 보호합니다.
- * 테넌트 *: ID 페더레이션 서버 또는 플랫폼 서비스 끝점에서 S3 스토리지 리소스에 대한 연결을 보호합니다.
- * 기타 *: 특정 인증서가 필요한 StorageGRID 연결을 보호합니다.

각 탭은 아래에 추가 인증서 세부 정보에 대한 링크와 함께 설명되어 있습니다.

글로벌

글로벌 인증서는 웹 브라우저 및 외부 S3 API 클라이언트에서 StorageGRID 액세스를 보호합니다. 두 개의 글로벌 인증서는 처음에 설치 중에 StorageGRID 인증 기관에서 생성합니다. 프로덕션 환경의 모범 사례는 외부 인증 기관에서 서명한 사용자 지정 인증서를 사용하는 것입니다.

- [관리 인터페이스 인증서입니다](#): StorageGRID 관리 인터페이스에 대한 클라이언트 웹 브라우저 연결의 보안을 유지합니다.
- [S3 API 인증서](#): S3 클라이언트 애플리케이션이 오브젝트 데이터를 업로드 및 다운로드하는 데 사용하는 스토리지 노드, 관리 노드 및 게이트웨이 노드에 대한 클라이언트 API 연결을 보호합니다.

설치된 글로벌 인증서에 대한 정보는 다음과 같습니다.

- * 이름 *: 인증서 관리 링크가 있는 인증서 이름입니다.
- * 설명 *
- * 유형 *: 사용자 정의 또는 기본값 + 그리드 보안을 강화하기 위해 항상 사용자 지정 인증서를 사용해야 합니다.
- * 만료 날짜 *: 기본 인증서를 사용하는 경우 만료 날짜가 표시되지 않습니다.

다음을 수행할 수 있습니다.

- 기본 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 교체하여 그리드 보안 강화:
 - ["기본 StorageGRID 생성 관리 인터페이스 인증서를 교체합니다"](#) Grid Manager 및 Tenant Manager 연결에 사용됩니다.
 - ["S3 API 인증서를 교체합니다"](#) 스토리지 노드 및 로드 밸런서 엔드포인트(선택 사항) 연결에 사용됩니다.
- ["기본 관리 인터페이스 인증서를 복원합니다"](#)..
- ["기본 S3 API 인증서를 복원합니다"](#)..
- ["스크립트를 사용하여 자체 서명된 새 관리 인터페이스 인증서를 생성합니다"](#)..
- 또는 을 복사하거나 ["관리 인터페이스 인증서입니다""S3 API 인증서"](#)다운로드합니다.

그리드 CA

[Grid CA 인증서](#)StorageGRID 설치 중에 StorageGRID 인증 기관에서 생성한 는 모든 내부 StorageGRID 트래픽을 보호합니다.

인증서 정보에는 인증서 만료 날짜 및 인증서 내용이 포함됩니다.

"[Grid CA 인증서를 복사하거나 다운로드합니다](#)"변경할 수는 있지만 변경할 수는 없습니다.

클라이언트

[클라이언트 인증서](#)외부 인증 기관에서 생성한 로 외부 모니터링 도구와 StorageGRID Prometheus 데이터베이스 간의 연결을 보호합니다.

인증서 테이블에는 구성된 각 클라이언트 인증서에 대한 행이 있으며 인증서 만료 날짜와 함께 인증서를 Prometheus 데이터베이스 액세스에 사용할 수 있는지 여부를 나타냅니다.

다음을 수행할 수 있습니다.

- "새 클라이언트 인증서를 업로드하거나 생성합니다."
- 인증서 이름을 선택하면 다음 작업을 수행할 수 있는 인증서 세부 정보가 표시됩니다.
 - "클라이언트 인증서 이름을 변경합니다."
 - "Prometheus 액세스 권한을 설정합니다."
 - "클라이언트 인증서를 업로드하고 교체합니다."
 - "클라이언트 인증서를 복사하거나 다운로드합니다."
 - "클라이언트 인증서를 제거합니다."
- 작업 * 을 선택하여 빠르게 "편집" 또는 "첨부" "제거" 클라이언트 인증서를 선택합니다. 클라이언트 인증서를 최대 10개까지 선택하고 * Actions * > * Remove * 를 사용하여 한 번에 제거할 수 있습니다.

부하 분산 장치 엔드포인트

[로드 밸런서 끝점 인증서](#) 게이트웨이 노드 및 관리 노드에서 S3 클라이언트와 StorageGRID 로드 밸런서 서비스 간의 연결을 보호합니다.

로드 밸런서 끝점 테이블에는 구성된 각 로드 밸런서 끝점에 대한 행이 있으며, 글로벌 S3 API 인증서나 사용자 지정 로드 밸런서 끝점 인증서가 끝점에 사용되고 있는지 여부를 나타냅니다. 각 인증서의 만료 날짜도 표시됩니다.



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

다음을 수행할 수 있습니다.

- "로드 밸런서 끝점을 봅니다" 인증서 세부 정보가 포함됩니다.
- "FabricPool에 대한 로드 밸런서 끝점 인증서를 지정합니다."
- "글로벌 S3 API 인증서를 사용합니다" 새 로드 밸런서 엔드포인트 인증서를 생성하는 대신

테넌트

테넌트는 또는 [플랫폼 서비스 끝점 인증서](#) 를 사용하여 StorageGRID과의 연결을 보호할 수 [ID 페더레이션 서버 인증서](#)입니다.

테넌트 테이블에는 각 테넌트에 대한 행이 있으며 각 테넌트가 자체 ID 소스 또는 플랫폼 서비스를 사용할 수 있는 권한이 있는지 여부를 나타냅니다.

다음을 수행할 수 있습니다.

- "테넌트 관리자에 로그인할 테넌트 이름을 선택합니다"
- "테넌트 이름을 선택하여 테넌트 ID 페더레이션 세부 정보를 봅니다"
- "테넌트 이름을 선택하여 테넌트 플랫폼 서비스 세부 정보를 봅니다"
- "엔드포인트 생성 중에 플랫폼 서비스 끝점 인증서를 지정합니다"

기타

StorageGRID는 특정 목적으로 다른 보안 인증서를 사용합니다. 이러한 인증서는 기능 이름으로 나열됩니다. 기타 보안 인증서에는 다음이 포함됩니다.

- [클라우드 스토리지 폴 인증서](#)

- 이메일 경고 알림 인증서
- 외부 syslog 서버 인증서
- 그리드 페더레이션 연결 인증서
- ID 페더레이션 인증서
- KMS(키 관리 서버) 인증서
- SSO(Single Sign-On) 인증서

정보는 함수에 사용되는 인증서 유형과 해당 서버 및 클라이언트 인증서 만료 날짜를 나타냅니다. 기능 이름을 선택하면 인증서 세부 정보를 보고 편집할 수 있는 브라우저 탭이 열립니다.



가 있는 경우에만 다른 인증서의 정보를 보고 액세스할 수 "적절한 권한"있습니다.

다음을 수행할 수 있습니다.

- "S3, C2S S3 또는 Azure에 대한 클라우드 스토리지 풀 인증서를 지정합니다"
- "경고 e-메일 알림에 사용할 인증서를 지정합니다"
- "외부 syslog 서버에 인증서를 사용합니다"
- "그리드 페더레이션 연결 인증서를 회전합니다"
- "ID 페더레이션 인증서를 보고 편집합니다"
- "KMS(키 관리 서버) 서버 및 클라이언트 인증서를 업로드합니다"
- "신뢰할 수 있는 당사자 트러스트를 위해 SSO 인증서를 수동으로 지정합니다"

보안 인증서 세부 정보입니다

각 보안 인증서 유형은 구현 지침에 대한 링크와 함께 아래에 설명되어 있습니다.

관리 인터페이스 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	<p>클라이언트 웹 브라우저와 StorageGRID 관리 인터페이스 간의 연결을 인증하여 사용자가 보안 경고 없이 그리드 관리자 및 테넌트 관리자에 액세스할 수 있도록 합니다.</p> <p>또한 이 인증서는 Grid Management API 및 테넌트 관리 API 연결을 인증합니다.</p> <p>설치 중에 생성된 기본 인증서를 사용하거나 사용자 지정 인증서를 업로드할 수 있습니다.</p>	구성 > 보안 > 인증서*에서 *전역 탭을 선택한 다음 *관리 인터페이스 인증서*를 선택합니다.	" 관리 인터페이스 인증서를 구성합니다 "

S3 API 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	스토리지 노드 및 로드 밸런서 앤드포인트에 대한 보안 S3 클라이언트 연결을 인증합니다(선택 사항).	구성 > 보안 > 인증서*에서 *글로벌 탭을 선택한 다음 *S3 API 인증서*를 선택합니다.	" S3 API 인증서를 구성합니다 "

Grid CA 인증서

를 [기본 그리드 CA 인증서 설명입니다](#) 참조하십시오.

관리자 클라이언트 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
클라이언트	<p>각 클라이언트에 설치되어 StorageGRID에서 외부 클라이언트 액세스를 인증할 수 있습니다.</p> <ul style="list-style-type: none"> 권한이 있는 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있습니다. 외부 도구를 사용하여 StorageGRID를 안전하게 모니터링할 수 있습니다. 	구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.	"클라이언트 인증서를 구성합니다"

로드 밸런서 끝점 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	<p>게이트웨이 노드 및 관리 노드에서 S3 클라이언트와 StorageGRID 로드 밸런서 서비스 간의 연결을 인증합니다. 로드 밸런서 끝점을 구성할 때 로드 밸런서 인증서를 업로드하거나 생성할 수 있습니다. 클라이언트 응용 프로그램은 StorageGRID에 연결할 때 로드 밸런서 인증서를 사용하여 개체 데이터를 저장하고 검색합니다.</p> <p>전역 인증서의 사용자 지정 버전을 사용하여 부하 분산 서비스에 대한 연결을 인증할 수도 S3 API 인증서입니다. 글로벌 인증서를 사용하여 로드 밸런서 연결을 인증하는 경우 각 로드 밸런서 끝점에 대해 별도의 인증서를 업로드하거나 생성할 필요가 없습니다.</p> <ul style="list-style-type: none"> 참고: * 로드 밸런서 인증에 사용되는 인증서는 일반적인 StorageGRID 작업 중에 가장 많이 사용되는 인증서입니다. 	구성 > 네트워크 > 로드 밸런서 엔드포인트	<ul style="list-style-type: none"> "로드 밸런서 엔드포인트를 구성합니다" "FabricPool용 로드 밸런서 끝점을 만듭니다"

Cloud Storage Pool 엔드포인트 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	<p>StorageGRID 클라우드 스토리지 풀에서 S3 Glacier 또는 Microsoft Azure Blob 스토리지와 같은 외부 스토리지 위치로 연결을 인증합니다. 각 클라우드 공급자 유형에는 다른 인증서가 필요합니다.</p>	ILM * > * 스토리지 풀 *	"클라우드 스토리지 풀을 생성합니다"

이메일 경고 알림 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버 및 클라이언트	<p>SMTP 이메일 서버와 알림 알림에 사용되는 StorageGRID 간의 연결을 인증합니다.</p> <ul style="list-style-type: none"> SMTP 서버와의 통신에 TLS(Transport Layer Security)가 필요한 경우 전자 메일 서버 CA 인증서를 지정해야 합니다. SMTP 전자 메일 서버에 인증을 위해 클라이언트 인증서가 필요한 경우에만 클라이언트 인증서를 지정합니다. 	알림 > 이메일 설정	" 알림에 대한 이메일 알림을 설정합니다 "

외부 syslog 서버 인증서입니다

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	<p>StorageGRID에서 이벤트를 기록하는 외부 syslog 서버 간의 TLS 또는 RELP/TLS 연결을 인증합니다.</p> <ul style="list-style-type: none"> 참고: * 외부 syslog 서버에 대한 TCP, RELP/TCP 및 UDP 연결에는 외부 syslog 서버 인증서가 필요하지 않습니다. 	구성 > 모니터링 > 감사 및 시스템 로그 서버	" 외부 syslog 서버를 사용합니다 "

그리드 페더레이션 연결 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버 및 클라이언트	그리드 페더레이션 연결에서 현재 StorageGRID 시스템과 다른 그리드 간에 전송된 정보를 인증하고 암호화합니다.	구성 > 시스템 > 그리드 연합	<ul style="list-style-type: none"> "그리드 페더레이션 연결을 만듭니다" "연결 인증서를 회전합니다"

ID 페더레이션 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	Active Directory, OpenLDAP 또는 Oracle Directory Server와 같은 외부 ID 공급자와 StorageGRID 간의 연결을 인증합니다. ID 페더레이션에 사용됩니다. 이 페더레이션을 사용하면 외부 시스템에서 관리 그룹 및 사용자를 관리할 수 있습니다.	구성 > 액세스 제어 > ID 페더레이션	"ID 페더레이션을 사용합니다"

KMS(키 관리 서버) 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버 및 클라이언트	StorageGRID와 StorageGRID 어플라이언스 노드에 암호화 키를 제공하는 외부 키 관리 서버(KMS) 간의 연결을 인증합니다.	구성 > 보안 > 키 관리 서버	"KMS(키 관리 서버) 추가"

플랫폼 서비스 끝점 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	StorageGRID 플랫폼 서비스에서 S3 스토리지 리소스에 대한 연결을 인증합니다.	• 테넌트 관리자 * > * 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 *	"플랫폼 서비스 끝점을 만듭니다" "플랫폼 서비스 끝점을 편집합니다"

SSO(Single Sign-On) 인증서

인증서 유형입니다	설명	내비게이션 위치	세부 정보
서버	AD FS(Active Directory Federation Services)와 같은 ID 페더레이션 서비스와 SSO(Single Sign-On) 요청에 사용되는 StorageGRID 간의 연결을 인증합니다.	구성 > 액세스 제어 > 단일 로그인	"Single Sign-On 구성"

인증서 예

예 1: 부하 분산 서비스

이 예에서 StorageGRID는 서버 역할을 합니다.

1. 로드 밸런서 끝점을 구성하고 StorageGRID에서 서버 인증서를 업로드하거나 생성합니다.
2. 로드 밸런서 끝점에 대한 S3 클라이언트 연결을 구성하고 동일한 인증서를 클라이언트에 업로드합니다.
3. 클라이언트가 데이터를 저장하거나 검색하려는 경우 HTTPS를 사용하여 로드 밸런서 끝점에 연결합니다.
4. StorageGRID는 공개 키가 포함된 서버 인증서와 개인 키를 기반으로 하는 서명으로 응답합니다.
5. 클라이언트는 서버 서명을 인증서 사본의 서명과 비교합니다. 서명이 일치하면 클라이언트는 동일한 공개 키를 사용하여 세션을 시작합니다.
6. 클라이언트가 StorageGRID로 개체 데이터를 보냅니다.

예 2: 외부 키 관리 서버(KMS)

이 예에서 StorageGRID는 클라이언트 역할을 합니다.

1. 외부 키 관리 서버 소프트웨어를 사용하면 StorageGRID를 KMS 클라이언트로 구성하고 CA 서명된 서버 인증서, 공용 클라이언트 인증서 및 클라이언트 인증서에 대한 개인 키를 얻을 수 있습니다.
2. Grid Manager를 사용하여 KMS 서버를 구성하고 서버 및 클라이언트 인증서와 클라이언트 개인 키를 업로드합니다.
3. StorageGRID 노드에 암호화 키가 필요한 경우, 이 노드는 인증서의 데이터와 개인 키를 기반으로 하는 서명을 포함하는 KMS 서버에 요청합니다.
4. KMS 서버는 인증서 서명의 유효성을 검사하고 StorageGRID를 신뢰할 수 있는지 결정합니다.
5. KMS 서버는 검증된 연결을 사용하여 응답합니다.

지원되는 서버 인증서 유형입니다

StorageGRID 시스템은 RSA 또는 ECDSA(Elliptic Curve Digital Signature Algorithm)로 암호화된 사용자 지정 인증서를 지원합니다.

보안 정책의 암호화 유형은 서버 인증서 유형과 일치해야 합니다. 예를 들어, RSA cipherer는 RSA 인증서가 필요하며, ECDSA cipherer는 ECDSA 인증서가 필요합니다. 을 "보안 인증서를 관리합니다" "참조하십시오. 서버 인증서와 호환되지 않는 사용자 지정 보안 정책을 구성할 수 "일시적으로 기본 보안 정책으로 돌아갑니다" 있습니다.

StorageGRID가 클라이언트 연결을 보호하는 방법에 대한 자세한 내용은 을 참조하십시오 "[S3 클라이언트에 대한 보안](#)".

관리 인터페이스 인증서를 구성합니다

기본 관리 인터페이스 인증서를 단일 사용자 지정 인증서로 대체하면 보안 경고가 발생하지 않고 사용자가 Grid Manager 및 Tenant Manager에 액세스할 수 있습니다. 기본 관리 인터페이스 인증서로 되돌리거나 새 인증서를 생성할 수도 있습니다.

이 작업에 대해

기본적으로 모든 관리 노드에는 그리드 CA에서 서명한 인증서가 발급됩니다. 이러한 CA 서명 인증서는 단일 공통 사용자 지정 관리 인터페이스 인증서 및 해당 개인 키로 대체할 수 있습니다.

모든 관리 노드에 하나의 사용자 지정 관리 인터페이스 인증서가 사용되므로 클라이언트가 Grid Manager 및 Tenant Manager에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 사용자 지정 인증서를 정의하여 그리드의 모든 관리 노드와 일치시킵니다.

서버에서 구성은 완료해야 하며 사용 중인 루트 인증 기관(CA)에 따라 사용자가 그리드 관리자 및 테넌트 관리자에 액세스하는 데 사용할 웹 브라우저에 그리드 CA 인증서를 설치해야 할 수도 있습니다.

 실패한 서버 인증서로 인해 작업이 중단되지 않도록 하기 위해 이 서버 인증서가 만료되려고 할 때 관리 인터페이스에 대한 서버 인증서 만료 알림이 트리거됩니다. 필요에 따라 구성 > 보안 > *인증서*를 선택하고 글로벌 탭에서 관리 인터페이스 인증서의 만료 날짜를 확인하여 현재 인증서가 만료되는 시기를 확인할 수 있습니다.

 IP 주소 대신 도메인 이름을 사용하여 Grid Manager 또는 Tenant Manager에 액세스하는 경우, 다음 중 하나가 발생할 경우 브라우저에 인증서 오류가 표시되지 않고 무시하도록 옵션이 표시되지 않습니다.

- 사용자 지정 관리 인터페이스 인증서가 만료됩니다.
- 여러분 [사용자 지정 관리 인터페이스 인증서에서 기본 서버 인증서로 되돌립니다](#),

사용자 지정 관리 인터페이스 인증서를 추가합니다

사용자 지정 관리 인터페이스 인증서를 추가하려면 고유한 인증서를 제공하거나 Grid Manager를 사용하여 인증서를 생성할 수 있습니다.

단계

- 구성 > 보안 > *인증서*를 선택합니다.
- 글로벌 * 탭에서 * 관리 인터페이스 인증서 * 를 선택합니다.
- 사용자 정의 인증서 사용 * 을 선택합니다.
- 인증서를 업로드하거나 생성합니다.

인증서를 업로드합니다

필요한 서버 인증서 파일을 업로드합니다.

- a. 인증서 업로드 * 를 선택합니다.
- b. 필요한 서버 인증서 파일을 업로드합니다.
 - * 서버 인증서 *: 사용자 정의 서버 인증서 파일(PEM 인코딩).
 - * 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일(.key).



EC 개인 키는 224비트 이상이어야 합니다. RSA 개인 키는 2048비트 이상이어야 합니다.

- * CA 번들 *: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 선택적 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.
- c. 업로드한 각 인증서의 메타데이터를 보려면 * 인증서 세부 정보 * 를 확장합니다. 선택적 CA 번들을 업로드한 경우 각 인증서는 자체 탭에 표시됩니다.
 - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택하고 인증서 번들을 저장하려면 * CA 번들 다운로드 * 를 선택합니다.

인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 .pem 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

- 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 또는 * CA 번들 PEM * 복사 를 선택합니다.
- d. 저장 * 을 선택합니다. + 사용자 지정 관리 인터페이스 인증서는 Grid Manager, Tenant Manager, Grid Manager API 또는 Tenant Manager API에 대한 이후의 모든 새 연결에 사용됩니다.

인증서를 생성합니다

서버 인증서 파일을 생성합니다.



프로덕션 환경의 모범 사례는 외부 인증 기관에서 서명한 사용자 지정 관리 인터페이스 인증서를 사용하는 것입니다.

- a. 인증서 생성 * 을 선택합니다.
- b. 인증서 정보를 지정합니다.

필드에 입력합니다	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
IP	인증서에 포함할 하나 이상의 IP 주소입니다.

필드에 입력합니다	설명
제목(선택 사항)	X.509 인증서 소유자의 주체 또는 고유 이름(DN)입니다. 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 CN(Subject Common Name)으로 사용합니다.
일 유효	인증서가 만료된 후 경과한 일 수입니다.
키 사용 확장을 추가합니다	이 옵션을 선택하면(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다. 이러한 확장은 인증서에 포함된 키의 용도를 정의합니다. • 참고 *: 인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

- c. Generate * 를 선택합니다.
- d. 생성된 인증서의 메타데이터를 보려면 * 인증서 세부 정보 * 를 선택합니다.
 - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 .pem 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

- 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.
- e. 저장 * 을 선택합니다. + 사용자 지정 관리 인터페이스 인증서는 Grid Manager, Tenant Manager, Grid Manager API 또는 Tenant Manager API에 대한 이후의 모든 새 연결에 사용됩니다.

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.



새 인증서를 업로드하거나 생성한 후에는 관련 인증서 만료 알림을 지울 수 있도록 최대 하루 동안 기다립니다.

6. 사용자 지정 관리 인터페이스 인증서를 추가하면 관리 인터페이스 인증서 페이지에 사용 중인 인증서에 대한 자세한 인증서 정보가 표시됩니다. + 필요에 따라 인증서 PEM을 다운로드하거나 복사할 수 있습니다.

기본 관리 인터페이스 인증서를 복원합니다

Grid Manager 및 Tenant Manager 연결에 기본 관리 인터페이스 인증서를 사용하도록 되돌릴 수 있습니다.

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 글로벌 * 탭에서 * 관리 인터페이스 인증서 * 를 선택합니다.
3. 기본 인증서 사용 * 을 선택합니다.

기본 관리 인터페이스 인증서를 복원하면 구성한 사용자 지정 서버 인증서 파일이 삭제되고 시스템에서 복구할 수 없습니다. 이후의 모든 새 클라이언트 연결에 기본 관리 인터페이스 인증서가 사용됩니다.

4. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

스크립트를 사용하여 자체 서명된 새 관리 인터페이스 인증서를 생성합니다

엄격한 호스트 이름 확인이 필요한 경우 스크립트를 사용하여 관리 인터페이스 인증서를 생성할 수 있습니다.

시작하기 전에

- 있습니다. ["특정 액세스 권한"](#)
- `Passwords.txt` 파일이 있습니다.

이 작업에 대해

프로덕션 환경의 모범 사례는 외부 인증 기관에서 서명한 인증서를 사용하는 것입니다.

단계

1. 각 관리 노드의 FQDN(정규화된 도메인 이름)을 얻습니다.

2. 기본 관리자 노드에 로그인합니다.

- a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
- b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
- c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
- d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 \$로 `#`로 변경됩니다.

3. 자체 서명된 새 인증서를 사용하여 StorageGRID를 구성합니다.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- 의 경우 --domains 모든 관리 노드의 정규화된 도메인 이름을 나타내는 와일드카드를 사용합니다. 예를 들어,에서는 `*.ui.storagegrid.example.com` 와일드카드를 사용하여 `admin1.ui.storagegrid.example.com` 및 `admin2.ui.storagegrid.example.com`를 나타냅니다.
- --type `Grid Manager` 및 Tenant Manager에서 사용하는 관리 인터페이스 인증서를 구성하려면 `management` 설정합니다.
- 기본적으로 생성된 인증서는 1년(365일) 동안 유효하며 만료되기 전에 다시 만들어야 합니다. 인수를 사용하여 기본 유효 기간을 재정의할 수 `--days` 있습니다.



인증서의 유효 기간은 가 실행될 때 `make-certificate` 시작됩니다. 관리 클라이언트가 StorageGRID와 동일한 시간 소스와 동기화되어 있는지 확인해야 합니다. 그렇지 않으면 클라이언트가 인증서를 거부할 수 있습니다.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 720
```

결과 출력에는 관리 API 클라이언트에 필요한 공용 인증서가 포함됩니다.

4. 인증서를 선택하고 복사합니다.

선택 항목에 BEGIN 및 END 태그를 포함합니다.

5. 명령 셸에서 로그아웃합니다. `$ exit`

6. 인증서가 구성되었는지 확인합니다.

a. 그리드 관리자에 액세스합니다.

b. 구성 > 보안 > *인증서*를 선택하세요.

c. 글로벌 * 탭에서 * 관리 인터페이스 인증서 * 를 선택합니다.

7. 복사한 공용 인증서를 사용하도록 관리 클라이언트를 구성합니다. BEGIN 및 END Tags를 포함합니다.

관리 인터페이스 인증서를 다운로드하거나 복사합니다

다른 곳에서 사용할 관리 인터페이스 인증서 내용을 저장하거나 복사할 수 있습니다.

단계

1. 구성 > 보안 > *인증서*를 선택합니다.

2. 글로벌 * 탭에서 * 관리 인터페이스 인증서 * 를 선택합니다.

3. 서버 * 또는 * CA 번들 * 탭을 선택한 다음 인증서를 다운로드하거나 복사합니다.

인증서 파일 또는 CA 번들을 다운로드합니다

인증서 또는 CA 번들 .pem 파일을 다운로드합니다. 선택적 CA 번들을 사용하는 경우 번들의 각 인증서가 자체 하위 탭에 표시됩니다.

- 인증서 다운로드 * 또는 * CA 번들 다운로드 * 를 선택합니다.

CA 번들을 다운로드하는 경우 CA 번들 보조 탭의 모든 인증서가 단일 파일로 다운로드됩니다.

- 인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 .pem 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

인증서 또는 CA 번들 PEM을 복사합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다. 선택적 CA 번들을 사용하는 경우 번들의 각 인증서가 자체 하위 탭에 표시됩니다.

- Copy certificate pem * 또는 * Copy CA bundle pem * 을 선택합니다.

CA 번들을 복사하는 경우 CA 번들 보조 탭의 모든 인증서가 함께 복사됩니다.

- 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.
- 텍스트 파일을 확장자로 `.pem` 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

S3 API 인증서를 구성합니다

스토리지 노드에 대한 S3 클라이언트 연결이나 로드 밸런서 끝점에 사용되는 서버 인증서를 교체하거나 복원할 수 있습니다. 교체 사용자 지정 서버 인증서는 조직에 따라 다릅니다.



이 버전의 문서 사이트에서 Swift 세부 정보가 제거되었습니다. 을 "StorageGRID 11.8: S3 및 Swift API 인증서를 구성합니다" 참조하십시오.

이 작업에 대해

기본적으로 모든 스토리지 노드에는 그리드 CA에서 서명한 X.509 서버 인증서가 발급됩니다. 이러한 CA 서명 인증서는 하나의 공통 사용자 지정 서버 인증서 및 해당 개인 키로 대체할 수 있습니다.

단일 사용자 지정 서버 인증서가 모든 스토리지 노드에 사용되므로 클라이언트가 스토리지 끝점에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 사용자 지정 인증서를 정의하여 그리드의 모든 스토리지 노드와 일치시킵니다.

서버에서 구성을 완료한 후 사용하는 루트 CA(인증 기관)에 따라 시스템에 액세스하는 데 사용할 S3 API 클라이언트에 그리드 CA 인증서를 설치해야 할 수도 있습니다.



실패한 서버 인증서로 인해 작업이 중단되지 않도록 하기 위해 루트 서버 인증서가 만료되려고 할 때 **S3 API**에 대한 글로벌 서버 인증서 만료 알림이 트리거됩니다. 필요에 따라 구성 > 보안 > *인증서*를 선택하고 글로벌 탭에서 S3 API 인증서의 만료 날짜를 확인하여 현재 인증서가 만료되는 시점을 확인할 수 있습니다.

사용자 지정 S3 API 인증서를 업로드하거나 생성할 수 있습니다.

사용자 지정 **S3 API** 인증서를 추가합니다

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 글로벌 * 탭에서 * S3 API 인증서 * 를 선택합니다.
3. 사용자 정의 인증서 사용 * 을 선택합니다.
4. 인증서를 업로드하거나 생성합니다.

인증서를 업로드합니다

필요한 서버 인증서 파일을 업로드합니다.

- a. 인증서 업로드 * 를 선택합니다.
- b. 필요한 서버 인증서 파일을 업로드합니다.
 - * 서버 인증서 *: 사용자 정의 서버 인증서 파일(PEM 인코딩).
 - * 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일(.key).



EC 개인 키는 224비트 이상이어야 합니다. RSA 개인 키는 2048비트 이상이어야 합니다.

- * CA 번들 *: 각 중간 발급 인증 기관의 인증서를 포함하는 단일 선택적 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.
- c. 인증서 세부 정보를 선택하여 업로드된 각 사용자 지정 S3 API 인증서의 메타데이터 및 PEM을 표시합니다. 선택적 CA 번들을 업로드한 경우 각 인증서는 자체 탭에 표시됩니다.
 - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택하고 인증서 번들을 저장하려면 * CA 번들 다운로드 * 를 선택합니다.

인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 .pem 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

- 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 또는 * CA 번들 PEM * 복사 를 선택합니다.
- d. 저장 * 을 선택합니다.

사용자 지정 서버 인증서는 이후의 새 S3 클라이언트 연결에 사용됩니다.

인증서를 생성합니다

서버 인증서 파일을 생성합니다.

- a. 인증서 생성 * 을 선택합니다.
- b. 인증서 정보를 지정합니다.

필드에 입력합니다	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
IP	인증서에 포함할 하나 이상의 IP 주소입니다.

필드에 입력합니다	설명
제목(선택 사항)	X.509 인증서 소유자의 주체 또는 고유 이름(DN)입니다. 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 CN(Subject Common Name)으로 사용합니다.
일 유효	인증서가 만료된 후 경과한 일 수입니다.
키 사용 확장을 추가합니다	이 옵션을 선택하면(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다. 이러한 확장은 인증서에 포함된 키의 용도를 정의합니다. • 참고 *: 인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

- c. Generate * 를 선택합니다.
- d. 생성된 사용자 지정 S3 API 인증서의 메타데이터와 PEM을 표시하려면 * Certificate Details * 를 선택하십시오.
- 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 .pem 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

- 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.

- e. 저장 * 을 선택합니다.

사용자 지정 서버 인증서는 이후의 새 S3 클라이언트 연결에 사용됩니다.

5. 탭을 선택하여 기본 StorageGRID 서버 인증서, 업로드된 CA 서명 인증서 또는 생성된 사용자 지정 인증서의 메타데이터를 표시합니다.



새 인증서를 업로드하거나 생성한 후에는 관련 인증서 만료 알림을 지울 수 있도록 최대 하루 동안 기다립니다.

6. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.
7. 사용자 지정 S3 API 인증서를 추가하면 S3 API 인증서 페이지에 사용 중인 사용자 지정 S3 API 인증서에 대한 자세한 인증서 정보가 표시됩니다. + 필요에 따라 인증서 PEM을 다운로드하거나 복사할 수 있습니다.

기본 S3 API 인증서를 복원합니다

스토리지 노드에 대한 S3 클라이언트 연결에 기본 S3 API 인증서를 사용하도록 되돌릴 수 있습니다. 그러나 부하 분산 끝점에 기본 S3 API 인증서를 사용할 수는 없습니다.

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 글로벌 * 탭에서 * S3 API 인증서 * 를 선택합니다.
3. 기본 인증서 사용 * 을 선택합니다.

글로벌 S3 API 인증서의 기본 버전을 복원하면 구성한 사용자 지정 서버 인증서 파일이 삭제되어 시스템에서 복구할 수 없습니다. 기본 S3 API 인증서는 스토리지 노드에 대한 이후 새 S3 클라이언트 연결에 사용됩니다.

4. 경고를 확인하고 기본 S3 API 인증서를 복원하려면 * 확인 * 을 선택하십시오.

루트 액세스 권한이 있고 사용자 지정 S3 API 인증서가 부하 분산 장치 끝점 연결에 사용된 경우 기본 S3 API 인증서를 사용하여 더 이상 액세스할 수 없는 로드 밸런서 끝점의 목록이 표시됩니다. [로드 밸런서 엔드포인트를 구성합니다](#) 이동하여 영향을 받는 끝점을 편집하거나 제거합니다.

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

S3 API 인증서를 다운로드하거나 복사합니다

다른 곳에서 사용할 S3 API 인증서 콘텐츠를 저장하거나 복사할 수 있습니다.

단계

1. 구성 > 보안 > *인증서*를 선택합니다.
2. 글로벌 * 탭에서 * S3 API 인증서 * 를 선택합니다.
3. 서버 * 또는 * CA 번들 * 탭을 선택한 다음 인증서를 다운로드하거나 복사합니다.

인증서 파일 또는 **CA** 번들을 다운로드합니다

인증서 또는 CA 번들 .pem 파일을 다운로드합니다. 선택적 CA 번들을 사용하는 경우 번들의 각 인증서가 자체 하위 탭에 표시됩니다.

- a. 인증서 다운로드 * 또는 * CA 번들 다운로드 * 를 선택합니다.

CA 번들을 다운로드하는 경우 CA 번들 보조 탭의 모든 인증서가 단일 파일로 다운로드됩니다.

- b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 .pem 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

인증서 또는 **CA** 번들 **PEM**을 복사합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다. 선택적 CA 번들을 사용하는 경우 번들의 각 인증서가 자체 하위 탭에 표시됩니다.

- a. Copy certificate pem * 또는 * Copy CA bundle pem * 을 선택합니다.

CA 번들을 복사하는 경우 CA 번들 보조 탭의 모든 인증서가 함께 복사됩니다.

- b. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.
- c. 텍스트 파일을 확장자로 `.pem` 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

관련 정보

- "[S3 REST API 사용](#)"
- "[S3 끝점 도메인 이름을 구성합니다](#)"

Grid CA 인증서를 복사합니다

StorageGRID는 내부 CA(인증 기관)를 사용하여 내부 트래픽을 보호합니다. 인증서를 업로드해도 이 인증서는 변경되지 않습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."[지원되는 웹 브라우저](#)"
- 있습니다. "[특정 액세스 권한](#)"

이 작업에 대해

사용자 지정 서버 인증서가 구성된 경우 클라이언트 응용 프로그램은 사용자 지정 서버 인증서를 사용하여 서버를 확인해야 합니다. StorageGRID 시스템에서 CA 인증서를 복사해서는 안 됩니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 ***Grid CA** 탭을 선택합니다.
2. 인증서 PEM * 섹션에서 인증서를 다운로드하거나 복사합니다.

인증서 파일을 다운로드합니다

인증서 .pem 파일을 다운로드합니다.

a. 인증서 다운로드 * 를 선택합니다.

b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 .pem 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

인증서 **PEM**을 복사합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다.

a. 인증서 PEM 복사 * 를 선택합니다.

b. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.

c. 텍스트 파일을 확장자로 `.pem` 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

FabricPool용 StorageGRID 인증서를 구성합니다

엄격한 호스트 이름 유효성 검사를 수행하고 FabricPool을 사용하는 ONTAP 클라이언트와 같은 엄격한 호스트 이름 유효성 검사 비활성화를 지원하지 않는 S3 클라이언트의 경우 로드 밸런서 끝점을 구성할 때 서버 인증서를 생성하거나 업로드할 수 있습니다.

시작하기 전에

- 있습니다. "[특정 액세스 권한](#)"
- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"

이 작업에 대해

로드 밸런서 끝점을 만들 때 자체 서명된 서버 인증서를 생성하거나 알려진 CA(인증 기관)에서 서명한 인증서를 업로드할 수 있습니다. 프로덕션 환경에서는 알려진 CA가 서명한 인증서를 사용해야 합니다. CA에서 서명한 인증서는 중단 없이 회전할 수 있습니다. 또한 중간자 공격에 대한 보호 기능이 강화되어 보안이 더욱 강화되고 있습니다.

다음 단계에서는 FabricPool을 사용하는 S3 클라이언트에 대한 일반 지침을 제공합니다. 자세한 정보 및 절차는 ["FabricPool용 StorageGRID를 구성합니다"](#) 참조하십시오.

단계

1. 선택적으로 FabricPool에서 사용할 고가용성(HA) 그룹을 구성합니다.
2. FabricPool에서 사용할 S3 로드 밸런서 끝점을 만듭니다.

HTTPS 로드 밸런서 끝점을 만들면 서버 인증서, 인증서 개인 키 및 선택적 CA 번들을 업로드하라는 메시지가 표시됩니다.

3. StorageGRID를 ONTAP의 클라우드 계층으로 연결

로드 밸런서 끝점 포트와 업로드한 CA 인증서에 사용된 정규화된 도메인 이름을 지정합니다. 그런 다음 CA 인증서를 제공합니다.



중간 CA에서 StorageGRID 인증서를 발급한 경우 중간 CA 인증서를 제공해야 합니다.
StorageGRID 인증서가 루트 CA에서 직접 발급된 경우 루트 CA 인증서를 제공해야 합니다.

클라이언트 인증서를 구성합니다

클라이언트 인증서를 사용하면 권한이 있는 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있으므로 외부 도구에서 StorageGRID를 모니터링하는 안전한 방법이 제공됩니다.

외부 모니터링 도구를 사용하여 StorageGRID에 액세스해야 하는 경우 그리드 관리자를 사용하여 클라이언트 인증서를 업로드하거나 생성하고 인증서 정보를 외부 도구에 복사해야 합니다.

"보안 인증서를 관리합니다" 및 을 "사용자 지정 서버 인증서를 구성합니다" 참조하십시오.



실패한 서버 인증서로 인해 작업이 중단되지 않도록, 이 서버 인증서가 만료되려고 할 때 인증서 페이지에서 구성된 클라이언트 인증서 만료 알림이 트리거됩니다. 필요에 따라 구성 > 보안 > *인증서 *를 선택하고 클라이언트 탭에서 클라이언트 인증서의 만료 날짜를 확인하여 현재 인증서가 만료되는 시점을 확인할 수 있습니다.



KMS(키 관리 서버)를 사용하여 특수하게 구성된 어플라이언스 노드의 데이터를 보호하는 경우에 대한 특정 정보를 참조하십시오 "[KMS 클라이언트 인증서 업로드](#)".

시작하기 전에

- 루트 액세스 권한이 있습니다.
- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 클라이언트 인증서를 구성하려면 다음을 따르십시오.
 - 관리 노드의 IP 주소 또는 도메인 이름이 있습니다.
 - StorageGRID 관리 인터페이스 인증서를 구성한 경우 관리 인터페이스 인증서를 구성하는 데 사용되는 CA, 클라이언트 인증서 및 개인 키가 있습니다.
 - 인증서를 업로드하려면 로컬 컴퓨터에서 인증서의 개인 키를 사용할 수 있습니다.
 - 개인 키는 생성 시 저장 또는 기록되어야 합니다. 원래 개인 키가 없으면 새 개인 키를 만들어야 합니다.
- 클라이언트 인증서를 편집하려면 다음을 따르십시오.
 - 관리 노드의 IP 주소 또는 도메인 이름이 있습니다.
 - 자체 인증서 또는 새 인증서를 업로드하려면 로컬 컴퓨터에서 개인 키, 클라이언트 인증서 및 CA(사용되는 경우)를 사용할 수 있습니다.

클라이언트 인증서를 추가합니다

클라이언트 인증서를 추가하려면 다음 절차 중 하나를 사용합니다.

- 관리 인터페이스 인증서가 이미 구성되어 있습니다

- CA 발급 클라이언트 인증서
- Grid Manager에서 인증서를 생성했습니다

관리 인터페이스 인증서가 이미 구성되어 있습니다

고객이 제공한 CA, 클라이언트 인증서 및 개인 키를 사용하여 관리 인터페이스 인증서가 이미 구성된 경우 이 절차를 사용하여 클라이언트 인증서를 추가합니다.

단계

1. 그리드 관리자에서 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.
2. 추가 * 를 선택합니다.
3. 인증서 이름을 입력합니다.
4. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
5. Continue * 를 선택합니다.
6. 인증서 첨부 * 단계의 경우 관리 인터페이스 인증서를 업로드합니다.
 - a. 인증서 업로드 * 를 선택합니다.
 - b. 찾아보기 * 를 선택하고 관리 인터페이스 인증서 파일을 (`.pem`선택합니다.)
 - 인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.
 - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.
 - c. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

새 인증서가 클라이언트 탭에 나타납니다.

7. 외부 모니터링 툴을 구성합니다

CA 발급 클라이언트 인증서

관리 인터페이스 인증서가 구성되어 있지 않고 CA에서 발급한 클라이언트 인증서 및 개인 키를 사용하는 Prometheus에 대한 클라이언트 인증서를 추가하려는 경우 이 절차를 사용하여 관리자 클라이언트 인증서를 추가하십시오.

단계

1. 의 단계를 "관리 인터페이스 인증서를 구성합니다"수행합니다.
2. 그리드 관리자에서 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.
3. 추가 * 를 선택합니다.
4. 인증서 이름을 입력합니다.
5. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
6. Continue * 를 선택합니다.
7. 인증서 첨부 * 단계의 경우 클라이언트 인증서, 개인 키 및 CA 번들 파일을 업로드합니다.
 - a. 인증서 업로드 * 를 선택합니다.
 - b. 찾아보기 * 를 선택하고 클라이언트 인증서, 개인 키 및 CA 번들 파일을 (`.pem`선택합니다).

- 인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 *를 선택합니다.
 - 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사를 선택합니다.
- c. Grid Manager에 인증서를 저장하려면 * Create *를 선택합니다.

새 인증서가 클라이언트 탭에 나타납니다.

8. 외부 모니터링 툴을 구성합니다

Grid Manager에서 인증서를 생성했습니다

관리 인터페이스 인증서가 구성되어 있지 않고 Grid Manager에서 인증서 생성 기능을 사용하는 Prometheus에 대한 클라이언트 인증서를 추가하려는 경우 이 절차를 사용하여 관리자 클라이언트 인증서를 추가하십시오.

단계

1. 그리드 관리자에서 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.
2. 추가 *를 선택합니다.
3. 인증서 이름을 입력합니다.
4. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus *를 선택합니다.
5. Continue *를 선택합니다.
6. 인증서 첨부 * 단계에서 * 인증서 생성 *를 선택합니다.
7. 인증서 정보를 지정합니다.
 - * subject * (선택 사항): X.509 주체 또는 인증서 소유자의 고유 이름(DN).
 - 유효한 * 일 수 *: 생성된 인증서가 생성된 시점부터 생성된 유효 일 수입니다.
 - * 키 사용 확장 추가 *: 선택한 경우(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다.

이러한 확장은 인증서에 포함된 키의 용도를 정의합니다.



인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트에 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

8. Generate *를 선택합니다.
9. [[CLIENT_CERT_DETAILS]] 인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 *를 선택합니다.



대화 상자를 닫은 후에는 인증서 개인 키를 볼 수 없습니다. 키를 안전한 위치에 복사하거나 다운로드합니다.

- 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사를 선택합니다.
- 인증서 파일을 저장하려면 * 인증서 다운로드 *를 선택합니다.

인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 .pem 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

◦ 다른 곳에 붙여넣을 인증서 개인 키를 복사하려면 * 개인 키 복사 * 를 선택합니다.

◦ 개인 키를 파일로 저장하려면 * 개인 키 다운로드 * 를 선택합니다.

개인 키 파일 이름과 다운로드 위치를 지정합니다.

10. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

새 인증서가 클라이언트 탭에 나타납니다.

11. 그리드 관리자에서 구성 > 보안 > 인증서*를 선택한 다음 *전역 탭을 선택합니다.

12. Management Interface certificate * 를 선택합니다.

13. 사용자 정의 인증서 사용 * 을 선택합니다.

14. 단계에서 certificate.pem 및 private_key.pem 파일을 업로드합니다.[클라이언트 인증서 세부 정보입니다](#) CA 번들을 업로드할 필요가 없습니다.

a. 인증서 업로드 * 를 선택한 다음 * 계속 * 을 선택합니다.

b. 각 인증서 파일 업로드(.pem).

c. 인증서를 Grid Manager에 저장하려면 * 저장 * 을 선택합니다.

새 인증서가 관리 인터페이스 인증서 페이지에 나타납니다.

15. [외부 모니터링 툴을 구성합니다](#) 그레파나와 같은

외부 모니터링 툴을 설정한다

단계

1. Grafana와 같은 외부 모니터링 도구에서 다음 설정을 구성합니다.

a. * 이름 *: 연결 이름을 입력합니다.

StorageGRID에는 이 정보가 필요하지 않지만 연결을 테스트하려면 이름을 입력해야 합니다.

b. * URL *: 관리자 노드의 도메인 이름 또는 IP 주소를 입력합니다. HTTPS 및 포트 9091을 지정합니다.

예를 들면 다음과 같습니다. `https://admin-node.example.com:9091`

c. TLS 클라이언트 인증 * 및 * CA 인증 * 을 활성화합니다.

d. TLS/SSL 인증 세부 정보에서 다음을 복사하여 붙여 넣습니다.

▪ CA 인증서** 에 대한 관리 인터페이스 CA 인증서입니다

▪ 클라이언트 인증서**

▪ 클라이언트 키에 대한 개인 키입니다

e. * ServerName *: 관리 노드의 도메인 이름을 입력합니다.

servername은 관리 인터페이스 인증서에 표시된 도메인 이름과 일치해야 합니다.

2. StorageGRID 또는 로컬 파일에서 복사한 인증서 및 개인 키를 저장하고 테스트합니다.

이제 외부 모니터링 툴을 사용하여 StorageGRID에서 Prometheus 메트릭에 액세스할 수 있습니다.

메트릭에 대한 자세한 내용은 를 참조하십시오 "[StorageGRID 모니터링 지침](#)".

클라이언트 인증서를 편집합니다

관리자 클라이언트 인증서를 편집하여 이름을 변경하거나, Prometheus 액세스를 활성화 또는 비활성화하거나, 현재 인증서가 만료되면 새 인증서를 업로드할 수 있습니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.

인증서 만료 날짜 및 Prometheus 액세스 권한이 표에 나열되어 있습니다. 인증서가 곧 만료되거나 이미 만료된 경우 테이블에 메시지가 나타나고 경고가 트리거됩니다.

2. 편집할 인증서를 선택합니다.
3. 편집 * 을 선택한 다음 * 이름 및 권한 편집 * 을 선택합니다
4. 인증서 이름을 입력합니다.
5. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 * Prometheus * 를 선택합니다.
6. Grid Manager에 인증서를 저장하려면 * Continue * 를 선택합니다.

업데이트된 인증서가 클라이언트 탭에 표시됩니다.

새 클라이언트 인증서를 연결합니다

현재 인증서가 만료되면 새 인증서를 업로드할 수 있습니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.

인증서 만료 날짜 및 Prometheus 액세스 권한이 표에 나열되어 있습니다. 인증서가 곧 만료되거나 이미 만료된 경우 테이블에 메시지가 나타나고 경고가 트리거됩니다.

2. 편집할 인증서를 선택합니다.
3. 편집 * 을 선택한 다음 편집 옵션을 선택합니다.

인증서를 업로드합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다.

- a. 인증서 업로드 * 를 선택한 다음 * 계속 * 을 선택합니다.

- b. 클라이언트 인증서 이름을 업로드합니다.(. pem

인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.

- 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 . pem 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

- 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.

- c. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

업데이트된 인증서가 클라이언트 탭에 표시됩니다.

인증서를 생성합니다

다른 곳에 붙여 넣을 인증서 텍스트를 생성합니다.

- a. 인증서 생성 * 을 선택합니다.

- b. 인증서 정보를 지정합니다.

- * subject * (선택 사항): X.509 주체 또는 인증서 소유자의 고유 이름(DN).

- 유효한 * 일 수 *: 생성된 인증서가 생성된 시점부터 생성된 유효 일 수입니다.

- * 키 사용 확장 추가 *: 선택한 경우(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다.

이러한 확장은 인증서에 포함된 키의 용도를 정의합니다.



인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트에 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

- c. Generate * 를 선택합니다.

- d. 인증서 메타데이터와 인증서 PEM을 표시하려면 * 클라이언트 인증서 세부 정보 * 를 선택합니다.



대화 상자를 닫은 후에는 인증서 개인 키를 볼 수 없습니다. 키를 안전한 위치에 복사하거나 다운로드합니다.

- 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.

- 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 . pem 저장합니다.

예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

- 다른 곳에 붙여넣을 인증서 개인 키를 복사하려면 * 개인 키 복사 * 를 선택합니다.
- 개인 키를 파일로 저장하려면 * 개인 키 다운로드 * 를 선택합니다.

개인 키 파일 이름과 다운로드 위치를 지정합니다.

- e. Grid Manager에 인증서를 저장하려면 * Create * 를 선택합니다.

새 인증서가 클라이언트 탭에 나타납니다.

클라이언트 인증서를 다운로드하거나 복사합니다

다른 곳에서 사용할 클라이언트 인증서를 다운로드하거나 복사할 수 있습니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.
2. 복사 또는 다운로드할 인증서를 선택합니다.
3. 인증서를 다운로드하거나 복사합니다.

인증서 파일을 다운로드합니다

인증서 `.pem` 파일을 다운로드합니다.

- a. 인증서 다운로드 * 를 선택합니다.
- b. 인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 `.pem` 저장합니다.

예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

인증서를 복사합니다

인증서 텍스트를 복사하여 다른 곳에 붙여 넣습니다.

- a. 인증서 PEM 복사 * 를 선택합니다.
- b. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.
- c. 텍스트 파일을 확장자로 `'pem'`저장합니다.

예를 들면 다음과 같습니다. `storagegrid_certificate.pem`

클라이언트 인증서를 제거합니다

더 이상 관리자 클라이언트 인증서가 필요하지 않으면 제거할 수 있습니다.

단계

1. 구성 > 보안 > 인증서*를 선택한 다음 *클라이언트 탭을 선택합니다.

- 제거할 인증서를 선택합니다.
- 삭제 * 를 선택한 다음 확인합니다.



최대 10개의 인증서를 제거하려면 클라이언트 탭에서 제거할 각 인증서를 선택한 다음 * 작업 * > * 삭제 * 를 선택합니다.

인증서가 제거된 후에는 인증서를 사용한 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스하기 위해 새 클라이언트 인증서를 지정해야 합니다.

보안 설정을 구성합니다

TLS 및 SSH 정책을 관리합니다

TLS 및 SSH 정책은 클라이언트 응용 프로그램과 보안 TLS 연결을 설정하고 내부 StorageGRID 서비스에 대한 보안 SSH 연결을 설정하는 데 사용되는 프로토콜과 암호를 결정합니다.

보안 정책은 TLS 및 SSH가 이동 중인 데이터를 암호화하는 방법을 제어합니다. 일반적으로 시스템이 일반 조건 호환이거나 다른 암호를 사용해야 하는 경우가 아니면 최신 호환성(기본값) 정책을 사용합니다.



이러한 정책에서 암호를 사용하도록 일부 StorageGRID 서비스가 업데이트되지 않았습니다.

시작하기 전에

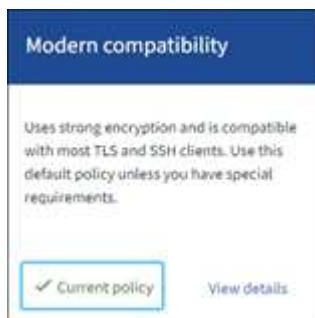
- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 이 "[루트 액세스 권한](#)"입니다.

보안 정책을 선택합니다

단계

- 구성 > 보안 > *보안 설정*을 선택합니다.

TLS 및 SSH 정책 * 탭에는 사용 가능한 정책이 표시됩니다. 현재 활성 정책은 정책 타일에 녹색 확인 표시로 표시됩니다.



- 사용 가능한 정책에 대해 알아보려면 탭을 검토하세요.

최신 호환성(기본값)

강력한 암호화가 필요하고 특별한 요구 사항이 없는 경우 기본 정책을 사용하세요. 이 정책은 대부분의 TLS 및 SSH 클라이언트와 호환됩니다.

레거시 호환성

이전 클라이언트에 대한 추가 호환성 옵션이 필요한 경우 레거시 호환성 정책을 사용하세요. 이 정책의 추가 옵션으로 인해 최신 호환성 정책보다 보안성이 떨어질 수 있습니다.

일반 조건

Common Criteria 인증이 필요한 경우 Common Criteria 정책을 사용하세요.

FIPS 엄격한

Common Criteria 인증이 필요하고 외부 클라이언트가 로드 밸런서 엔드포인트, 테넌트 관리자 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 엄격한 정책을 사용하세요. 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 간 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 간 TLS 연결
 - SSE-S3, SSE-C 및 저장된 개체 암호화 설정에 대한 개체 콘텐츠 암호화
 - SSH 연결

자세한 내용은 NIST 암호화 알고리즘 검증 프로그램을 참조하세요.["인증서 #4838"](#).

- NetApp StorageGRID 커널 암호화 API 모듈

NetApp StorageGRID Kernel Crypto API 모듈은 VM 및 StorageGRID 어플라이언스 플랫폼에만 있습니다.

- 엔트로피 수집
- 노드 암호화

자세한 내용은 NIST 암호화 알고리즘 검증 프로그램을 참조하세요.["인증서 #A6242부터 #A6257까지"](#) 그리고["엔트로피 인증서 #E223"](#).

참고: 이 정책을 선택한 후, ["롤링 재부팅을 수행하다"](#) 모든 노드가 NCSM을 활성화합니다. 재부팅을 시작하고 모니터링하려면 유지 관리 > *롤링 재부팅*을 사용하세요.

맞춤형

자신의 암호를 적용해야 하는 경우 사용자 지정 정책을 만듭니다.

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 사용합니다.

- a. 설정하다 `fipsMode` 매개변수 `true` .
 - b. 메시지가 표시되면, "룰링 재부팅을 수행하다" 모든 노드가 암호화 모듈을 활성화합니다. 재부팅을 시작하고 모니터링하려면 유지 관리 > *룰링 재부팅*을 사용하세요.
 - c. 지원 > *진단*을 선택하여 활성 FIPS 모듈 버전을 확인하세요.

- 각 정책의 암호화, 프로토콜 및 알고리즘에 대한 세부 정보를 보려면 * 상세 정보 보기 * 를 선택합니다.
 - 현재 정책을 변경하려면 * 정책 사용 * 을 선택합니다.

정책 타일에서 * 현재 정책 * 옆에 녹색 확인 표시가 나타납니다.

사용자 지정 보안 정책을 만듭니다

사용자 고유의 암호를 적용해야 하는 경우 사용자 지정 정책을 만들 수 있습니다.

단계

1. 만들려는 사용자 지정 정책과 가장 유사한 정책 타일에서 * 세부 정보 보기 *를 선택합니다.
 2. 클립보드로 복사 *를 선택한 다음 * 죄소 *를 선택합니다.



3. 사용자 정의 정책 * 타일에서 * 구성 및 사용 * 을 선택합니다.
 4. 복사한 JSON을 붙여 넣고 필요한 내용을 변경합니다.
 5. Use policy * 를 선택합니다.

사용자 지정 정책 타일의 * 현재 정책 * 옆에 놀색 확인 표시가 나타납니다

6. 필요에 따라 * 구성 평집 * 을 선택하여 새 사용자 지정 정책을 더 많이 변경합니다.

일시적으로 기본 보안 정책으로 돌아갑니다

사용자 지정 보안 정책을 구성한 경우 구성된 TLS 정책이 과 호환되지 않으면 그리드 관리자에 로그인하지 못할 수 "구성된 서버 인증서입니다"입니다.

일시적으로 기본 보안 정책으로 되돌릴 수 있습니다.

단계

1. 관리자 노드에 로그인:

- a. 다음 명령을 입력합니다. `ssh admin@Admin_Node_IP`
- b. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.
- c. 다음 명령을 입력하여 루트로 전환합니다. `su -`
- d. 파일에 나열된 암호를 `Passwords.txt` 입력합니다.

루트로 로그인하면 프롬프트가 에서 \$ 로 '#' 변경됩니다.

2. 다음 명령을 실행합니다.

```
restore-default-cipher-configurations
```

3. 웹 브라우저에서 동일한 관리 노드의 그리드 관리자에 액세스합니다.

4. 의 단계에 따라 [보안 정책을 선택합니다](#)정책을 다시 구성합니다.

네트워크 및 개체 보안을 구성합니다

네트워크 및 개체 보안을 구성하여 저장된 개체를 암호화하거나, 특정 S3 요청을 방지하거나, 스토리지 노드에 대한 클라이언트 연결이 HTTPS 대신 HTTP를 사용하도록 할 수 있습니다.

저장된 오브젝트 암호화

저장된 오브젝트 암호화를 통해 S3를 통해 수집된 모든 오브젝트 데이터를 암호화할 수 있습니다. 기본적으로 저장된 개체는 암호화되지 않지만 AES - 128 또는 AES - 256 암호화 알고리즘을 사용하여 개체를 암호화하도록 선택할 수 있습니다. 이 설정을 활성화하면 새로 수집된 모든 객체가 암호화되지만 기존 저장된 객체는 변경되지 않습니다. 암호화를 사용하지 않도록 설정하면 현재 암호화된 개체는 암호화된 상태로 유지되지만 새로 수집된 개체는 암호화되지 않습니다.

저장된 오브젝트 암호화 설정은 버킷 레벨 또는 오브젝트 레벨 암호화로 암호화되지 않은 S3 오브젝트에만 적용됩니다.

StorageGRID 암호화 방법에 대한 자세한 내용은 ["StorageGRID 암호화 방법을 검토합니다"](#)참조하십시오.

클라이언트 수정을 방지합니다

클라이언트 수정 방지 는 시스템 전체 설정입니다. 클라이언트 수정 방지 * 옵션을 선택하면 다음 요청이 거부됩니다.

S3 REST API

- DeleteBucket 요청
- 기존 오브젝트의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태그 지정을 수정하는 요청

스토리지 노드 연결에 대해 **HTTP**를 설정합니다

기본적으로 클라이언트 애플리케이션은 스토리지 노드에 대한 직접 연결에 HTTPS 네트워크 프로토콜을 사용합니다. 비프로덕션 그리드를 테스트할 때와 같이 이러한 연결에 대해 HTTP를 선택적으로 활성화할 수 있습니다.

S3 클라이언트가 스토리지 노드에 직접 HTTP 연결을 만들어야 하는 경우에만 스토리지 노드 연결에 HTTP를 사용합니다. HTTPS 연결만 사용하는 클라이언트 또는 부하 분산 서비스에 연결하는 클라이언트(HTTP 또는 HTTPS를 사용할 수 있으므로)에는 이 옵션을 사용할 필요가 없습니다."각 로드 밸런서 엔드포인트를 구성합니다"

HTTP 또는 HTTPS를 사용하여 스토리지 노드에 연결할 때 S3 클라이언트가 사용하는 포트에 대해 알아보려면 를 참조하십시오"[요약: 클라이언트 연결을 위한 IP 주소 및 포트](#)".

옵션을 선택합니다

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."[지원되는 웹 브라우저](#)"
- 루트 액세스 권한이 있습니다.

단계

1. 구성 > 보안 > *보안 설정*을 선택합니다.
2. Network and objects * 탭을 선택합니다.
3. 저장된 개체 암호화의 경우 저장된 개체를 암호화하지 않으려면 * 없음 * (기본값) 설정을 사용하거나 * AES-128 * 또는 * AES-256 * 을 선택하여 저장된 개체를 암호화합니다.
4. 필요에 따라 S3 클라이언트가 특정 요청을 하지 못하도록 하려면 * 클라이언트 수정 방지 * 를 선택합니다.



이 설정을 변경하면 새 설정을 적용하는 데 약 1분이 걸립니다. 구성된 값이 성능 및 확장을 위해 캐싱됩니다.

5. 클라이언트가 스토리지 노드에 직접 접속하고 HTTP 연결을 사용하려는 경우 선택적으로 * 스토리지 노드 연결에 HTTP 사용 * 을 선택합니다.



요청이 암호화되지 않은 상태로 전송되므로 프로덕션 그리드에 대해 HTTP를 설정할 때는 주의해야 합니다.

6. 저장 * 을 선택합니다.

인터페이스 보안 설정을 변경합니다

인터페이스 보안 설정을 사용하면 사용자가 지정된 시간 이상 비활성 상태인 경우 로그아웃할지 여부 및 스택 추적이 API 오류 응답에 포함되는지 여부를 제어할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."[지원되는 웹 브라우저](#)"
- 있습니다. "[루트 액세스 권한](#)"

이 작업에 대해

보안 설정 * 페이지에는 * 브라우저 비활성 시간 제한 * 및 * 관리 API 스택 추적 * 설정이 포함됩니다.

브라우저 비활성 시간 초과

사용자가 로그아웃되기 전까지 사용자의 브라우저가 비활성화될 수 있는 시간을 나타냅니다. 기본값은 15분입니다.

브라우저 비활성 시간 초과는 다음과 같은 방법으로 제어됩니다.

- 시스템 보안을 위해 포함되어 있는 별도의 구성 불가능한 StorageGRID 타이머입니다. 각 사용자의 인증 토큰은 사용자가 로그인한 후 16시간 후에 만료됩니다. 사용자의 인증이 만료되면 브라우저 비활성 시간 제한이 비활성화되거나 브라우저 시간 제한 값에 도달하지 않은 경우에도 해당 사용자는 자동으로 로그아웃됩니다. 토큰을 갱신하려면 사용자가 다시 로그인해야 합니다.
- StorageGRID에 대해 SSO(Single Sign-On)가 활성화된 경우 ID 공급자에 대한 시간 제한 설정입니다.

SSO가 활성화되어 있고 사용자 브라우저의 시간이 초과되면 사용자는 StorageGRID 다시 액세스하려면 SSO 자격 증명을 다시 입력해야 합니다. 보다 "[SSO 작동 방식](#)".

관리 API 스택 추적

Grid Manager 및 Tenant Manager API 오류 응답에서 스택 추적이 반환되는지 여부를 제어합니다.

이 옵션은 기본적으로 비활성화되어 있지만 테스트 환경에서 이 기능을 사용할 수 있습니다. 일반적으로 API 오류가 발생할 때 내부 소프트웨어 세부 정보가 노출되지 않도록 프로덕션 환경에서 스택 추적을 비활성화해야 합니다.

단계

- 구성 > 보안 > *보안 설정*을 선택합니다.
- 인터페이스 * 탭을 선택합니다.
- 브라우저 비활성 시간 초과 설정을 변경하려면:
 - 아코디언을 확장합니다.
 - 제한 시간을 변경하려면 60초에서 7일 사이의 값을 지정합니다. 기본 시간 제한은 15분입니다.
 - 이 기능을 비활성화하려면 확인란을 선택 취소합니다.
 - 저장 * 을 선택합니다.
- 새 설정은 현재 로그인한 사용자에게는 영향을 주지 않습니다. 새 시간 초과 설정을 적용하려면 사용자가 다시 로그인하거나 브라우저를 새로 고쳐야 합니다.
- 관리 API 스택 추적 설정을 변경하려면 다음을 수행합니다.
 - 아코디언을 확장합니다.
 - Grid Manager 및 Tenant Manager API 오류 응답에서 스택 추적을 반환하려면 확인란을 선택합니다.



API 오류가 발생할 때 내부 소프트웨어 세부 정보가 노출되지 않도록 프로덕션 환경에서 스택 추적을 비활성화하십시오.

- 저장 * 을 선택합니다.

외부 SSH 액세스 관리

외부 액세스를 차단하거나 허용하여 그리드로 들어오는 트래픽에 대한 SSH 액세스를 관리합니다. SSH 외부 액세스를 관리해도 그리드 내 노드 간 트래픽에는 영향을 미치지

않습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 있습니다. "[루트 액세스 권한](#)"

이 작업에 대해

시스템 보안을 강화하기 위해 기본적으로 외부 SSH 액세스는 차단됩니다. 문제 해결 등 인바운드 SSH 액세스가 필요한 작업을 수행해야 하는 경우 일시적으로 외부 액세스를 허용합니다. 작업을 완료하면 외부 접근을 차단하세요.

단계

1. 구성 > 보안 > *보안 설정*을 선택합니다.
2. **SSH** 차단 탭을 선택합니다.
3. 외부 SSH 액세스를 관리하려면 인바운드 **SSH** 액세스 차단 옵션을 사용하세요.
 - a. 접근을 차단하려면 확인란을 선택하세요(기본값).
 - b. 접근을 허용하려면 체크박스의 선택을 해제하세요.



서비스 노트북과 다른 모든 그리드 노드 간에는 포트 22에서 액세스가 필요합니다. 유지 관리 작업을 완료하면 포트 22에 대한 액세스를 제거하세요.

4. 저장 * 을 선택합니다.

키 관리 서버를 구성합니다

KMS(키 관리 서버)란 무엇입니까?

KMS(Key Management Server)는 KMIP(Key Management Interoperability Protocol)를 사용하여 관련 StorageGRID 사이트의 StorageGRID 어플라이언스 노드에 암호화 키를 제공하는 외부 타사 시스템입니다.

StorageGRID는 특정 키 관리 서버만 지원합니다. 지원되는 제품 및 버전 목록을 보려면 을 "[NetApp 상호 운용성 매트릭스 툴\(IMT\)](#)" 사용합니다.

하나 이상의 키 관리 서버를 사용하여 설치 중에 * 노드 암호화 * 설정이 활성화된 모든 StorageGRID 어플라이언스 노드에 대한 노드 암호화 키를 관리할 수 있습니다. 이러한 어플라이언스 노드에 키 관리 서버를 사용하면 어플라이언스를 데이터 센터에서 제거하더라도 데이터를 보호할 수 있습니다. 어플라이언스 볼륨이 암호화된 후에는 노드에서 KMS와 통신할 수 없는 한 어플라이언스의 데이터에 액세스할 수 없습니다.



StorageGRID는 어플라이언스 노드를 암호화하고 해독하는 데 사용되는 외부 키를 생성하거나 관리하지 않습니다. 외부 키 관리 서버를 사용하여 StorageGRID 데이터를 보호하려는 경우 해당 서버를 설정하는 방법을 이해하고 암호화 키를 관리하는 방법을 이해해야 합니다. 주요 관리 작업을 수행하는 것은 이 지침의 범위를 벗어납니다. 도움이 필요한 경우 키 관리 서버 설명서를 참조하거나 기술 지원 부서에 문의하십시오.

KMS 및 어플라이언스 구성

KMS(키 관리 서버)를 사용하여 어플라이언스 노드에서 StorageGRID 데이터를 보호하려면 먼저 하나 이상의 KMS 서버 설정 및 어플라이언스 노드에 대한 노드 암호화 활성화라는 두 가지 구성 작업을 완료해야 합니다. 이러한 두 구성 작업이 완료되면 키 관리 프로세스가 자동으로 수행됩니다.

이 순서도는 KMS를 사용하여 어플라이언스 노드의 StorageGRID 데이터를 보호하는 상위 단계를 보여 줍니다.

순서도는 KMS 설정 및 어플라이언스 설정이 병렬로 이루어지지만, 요구 사항에 따라 새 어플라이언스 노드에 대한 노드 암호화를 활성화하기 전이나 후에 키 관리 서버를 설정할 수 있습니다.

KMS(키 관리 서버) 설정

키 관리 서버를 설정하는 단계는 다음과 같습니다.

단계	을 참조하십시오
KMS 소프트웨어에 액세스하고 각 KMS 또는 KMS 클러스터에 StorageGRID용 클라이언트를 추가합니다.	" KMS에서 StorageGRID를 클라이언트로 구성합니다 "
KMS에서 StorageGRID 클라이언트에 필요한 정보를 얻습니다.	" KMS에서 StorageGRID를 클라이언트로 구성합니다 "
KMS를 Grid Manager에 추가하고, 단일 사이트 또는 기본 사이트 그룹에 할당하고, 필요한 인증서를 업로드하고, KMS 구성을 저장합니다.	" KMS(키 관리 서버) 추가 "

제품을 설치합니다

KMS 사용을 위해 어플라이언스 노드를 설정하는 단계는 다음과 같습니다.

1. 어플라이언스 설치 시 하드웨어 구성 단계에서 StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스에 대한 * 노드 암호화 * 설정을 활성화합니다.



어플라이언스를 그리드에 추가한 후에는 * 노드 암호화 * 설정을 활성화할 수 없으며 노드 암호화가 활성화되지 않은 어플라이언스의 경우 외부 키 관리를 사용할 수 없습니다.

2. StorageGRID 어플라이언스 설치 프로그램을 실행합니다. 설치 중에 각 어플라이언스 볼륨에 DEK(임의 데이터 암호화 키)가 다음과 같이 할당됩니다.
 - DEK는 각 볼륨의 데이터를 암호화하는 데 사용됩니다. 이러한 키는 어플라이언스 OS에서 LUKS(Linux Unified Key Setup) 디스크 암호화를 사용하여 생성되며 변경할 수 없습니다.
 - 각 개별 DEK는 마스터 키 암호화 키(KEK)로 암호화됩니다. 초기 KEK는 어플라이언스가 KMS에 연결할 수 있을 때까지 DEK를 암호화하는 임시 키입니다.
3. 어플라이언스 노드를 StorageGRID에 추가합니다.

자세한 내용은 ["노드 암호화를 설정합니다"](#) 참조하십시오.

키 관리 암호화 프로세스(자동으로 발생)

키 관리 암호화에는 자동으로 수행되는 다음과 같은 높은 수준의 단계가 포함됩니다.

1. 노드 암호화가 활성화된 어플라이언스를 그리드에 설치하는 경우 StorageGRID는 새 노드가 포함된 사이트에 대해 KMS 구성이 존재하는지 여부를 결정합니다.
 - KMS가 사이트에 대해 이미 구성된 경우 어플라이언스는 KMS 구성을 받습니다.
 - KMS가 사이트에 대해 아직 구성되지 않은 경우 사이트에 대해 KMS를 구성하고 어플라이언스가 KMS 구성을 받을 때까지 어플라이언스의 데이터는 임시 KEK에 의해 계속 암호화됩니다.
2. 이 어플라이언스는 KMS 구성을 사용하여 KMS에 연결하고 암호화 키를 요청합니다.
3. KMS는 암호화 키를 어플라이언스에 보냅니다. KMS의 새 키는 임시 KEK를 대체하며, 이제 어플라이언스 볼륨의 DEK를 암호화하고 해독하는 데 사용됩니다.



암호화된 어플라이언스 노드가 구성된 KMS에 연결하기 전에 존재하는 모든 데이터는 임시 키로 암호화됩니다. 그러나 임시 키를 KMS 암호화 키로 교체할 때까지 어플라이언스 볼륨을 데이터 센터에서 제거하지 않도록 보호해서는 안 됩니다.

4. 제품의 전원이 켜져 있거나 재부팅된 경우 KMS에 다시 연결하여 키를 요청합니다. 휘발성 메모리에 저장된 키는 전원 손실이나 재부팅 시에도 계속 유지될 수 없습니다.

키 관리 서버 사용에 대한 고려 사항 및 요구 사항

외부 키 관리 서버(KMS)를 구성하기 전에 고려 사항 및 요구 사항을 이해해야 합니다.

지원되는 **KMIP** 버전은 무엇입니까?

StorageGRID는 KMIP 버전 1.4를 지원합니다.

["키 관리 상호 운용성 프로토콜 사양 버전 1.4"](#)

네트워크 고려 사항은 무엇입니까?

네트워크 방화벽 설정을 통해 각 어플라이언스 노드가 KMIP(Key Management Interoperability Protocol) 통신에 사용되는 포트를 통해 통신할 수 있어야 합니다. 기본 KMIP 포트는 5696입니다.

노드 암호화를 사용하는 각 어플라이언스 노드에서 사이트에 대해 구성한 KMS 또는 KMS 클러스터에 대한 네트워크 액세스 권한이 있는지 확인해야 합니다.

지원되는 **TLS** 버전은 무엇입니까?

어플라이언스 노드와 구성된 KMS 간의 통신은 보안 TLS 연결을 사용합니다. StorageGRID는 KMS가 지원하는 것과 사용 중인 것에 따라 KMS 또는 KMS 클러스터에 KMIP 연결을 설정할 때 TLS 1.2 또는 TLS 1.3 프로토콜을 지원할 수 있습니다."TLS 및 SSH 정책".

StorageGRID 연결을 만들 때 KMS와 프로토콜 및 암호(TLS 1.2) 또는 암호 그룹(TLS 1.3)을 협상합니다. 사용 가능한 프로토콜 버전 및 암호/암호 모음을 확인하려면 다음을 검토하세요. `tlsOutbound` 그리드의 활성 TLS 및 SSH 정책 섹션(구성 > 보안 보안 설정).

어떤 어플라이언스가 지원됩니까?

KMS(키 관리 서버)를 사용하여 * 노드 암호화 * 설정이 활성화된 그리드에 있는 StorageGRID 어플라이언스의 암호화 키를 관리할 수 있습니다. 이 설정은 StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스 설치의 하드웨어 구성 단계에서만 활성화할 수 있습니다.



어플라이언스를 그리드에 추가한 후에는 노드 암호화를 활성화할 수 없으며 노드 암호화가 활성화되지 않은 어플라이언스에는 외부 키 관리를 사용할 수 없습니다.

구성된 KMS for StorageGRID 어플라이언스 및 어플라이언스 노드를 사용할 수 있습니다.

다음을 포함하여 소프트웨어 기반(비어플라이언스) 노드에 대해 구성된 KMS를 사용할 수 없습니다.

- 가상 머신(VM)으로 구축된 노드
- Linux 호스트의 컨테이너 엔진 내에 구축된 노드

이러한 다른 플랫폼에 구축된 노드는 StorageGRID 외부의 데이터 저장소 또는 디스크 레벨에서 암호화를 사용할 수 있습니다.

키 관리 서버는 언제 구성해야 합니까?

새 설치의 경우 일반적으로 테넌트를 생성하기 전에 Grid Manager에서 하나 이상의 키 관리 서버를 설정해야 합니다. 이 순서를 사용하면 오브젝트 데이터가 노드에 저장되기 전에 노드가 보호됩니다.

어플라이언스 노드를 설치하기 전이나 설치한 후에 Grid Manager에서 키 관리 서버를 구성할 수 있습니다.

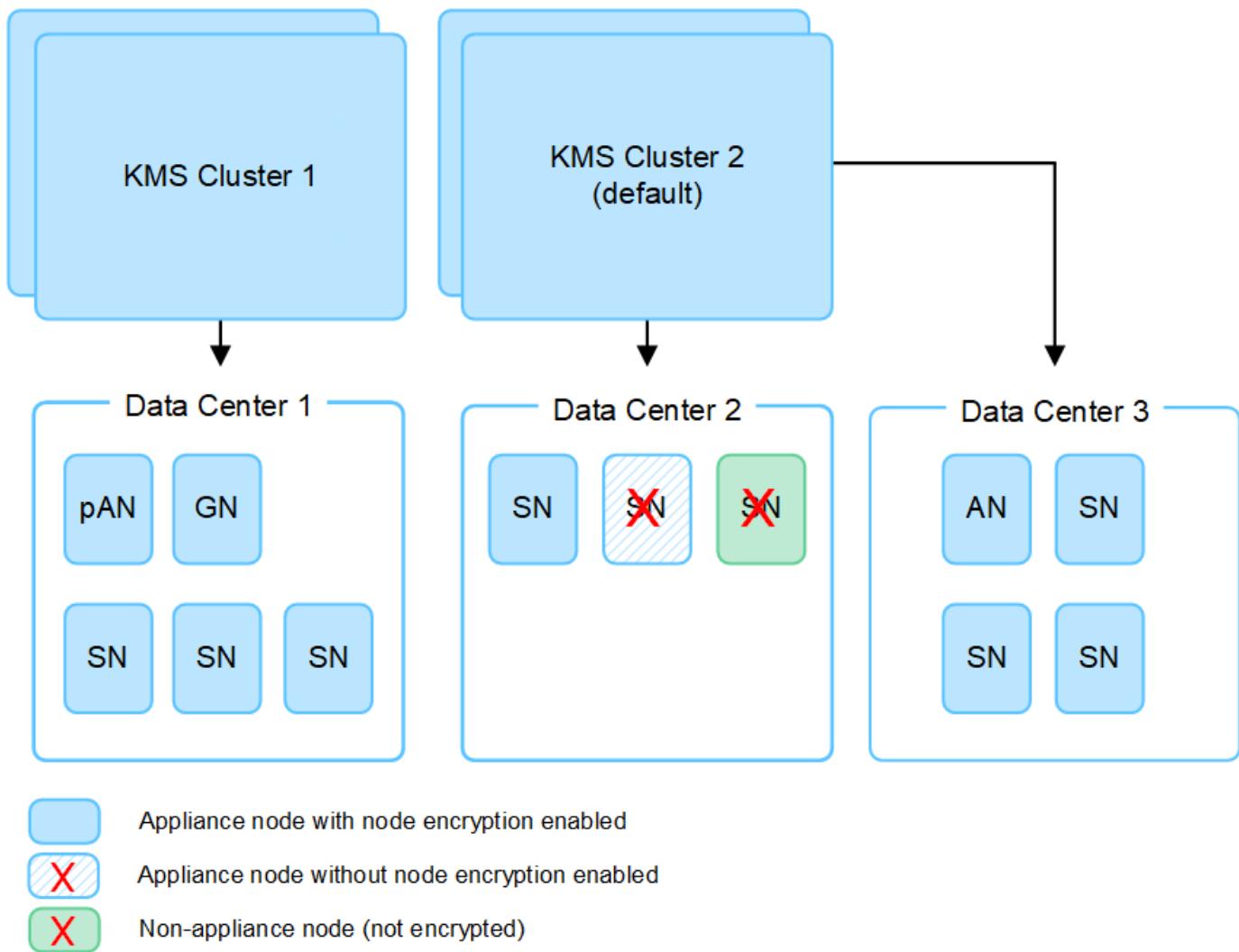
몇 개의 키 관리 서버가 필요합니까?

StorageGRID 시스템의 어플라이언스 노드에 암호화 키를 제공하도록 하나 이상의 외부 키 관리 서버를 구성할 수 있습니다. 각 KMS는 단일 사이트 또는 사이트 그룹의 StorageGRID 어플라이언스 노드에 단일 암호화 키를 제공합니다.

StorageGRID는 KMS 클러스터 사용을 지원합니다. 각 KMS 클러스터에는 구성 설정 및 암호화 키를 공유하는 여러 개의 복제된 키 관리 서버가 포함되어 있습니다. KMS 클러스터를 사용하여 키 관리를 수행하는 것이 좋습니다. KMS 클러스터는 고가용성 구성의 장애 조치 기능을 개선하므로 이 기능을 사용하는 것이 좋습니다.

예를 들어, StorageGRID 시스템에 데이터 센터 사이트가 3개 있다고 가정합니다. 다른 모든 사이트의 모든 어플라이언스 노드에 키를 제공하도록 하나의 KMS 클러스터를 구성하여 Data Center 1의 모든 어플라이언스 노드와 두 번째 KMS 클러스터에 키를 제공할 수 있습니다. 두 번째 KMS 클러스터를 추가하면 데이터 센터 2 및 데이터 센터 3에 대한 기본 KMS를 구성할 수 있습니다.

비어플라이언스 노드나 설치 중에 * 노드 암호화 * 설정이 활성화되지 않은 어플라이언스 노드에 대해 KMS를 사용할 수 없습니다.



키를 회전하면 어떻게 됩니까?

보안 모범 사례로서, 구성된 각 KMS에서 주기적으로 사용해야 ["암호화 키를 회전합니다"](#)합니다.

새 키 버전을 사용할 수 있는 경우:

- KMS와 관련된 사이트 또는 사이트의 암호화된 어플라이언스 노드에 자동으로 배포됩니다. 키는 회전된 후 1시간 내에 분포되어야 합니다.
- 새 키 버전이 배포될 때 암호화된 어플라이언스 노드가 오프라인이면 재부팅되는 즉시 새 키가 노드에 수신됩니다.
- 새 키 버전을 사용하여 어플라이언스 볼륨을 암호화할 수 없는 경우 어플라이언스 노드에 대해 * KMS 암호화 키 회전 실패 * 경고가 트리거됩니다. 이 경고를 해결하려면 기술 지원 부서에 문의해야 할 수도 있습니다.

어플라이언스 노드를 암호화한 후 다시 사용할 수 있습니까?

암호화된 어플라이언스를 다른 StorageGRID 시스템에 설치해야 하는 경우 오브젝트 데이터를 다른 노드로 이동하려면 먼저 그리드 노드를 해제해야 합니다. 그런 다음 StorageGRID 어플라이언스 설치 프로그램을 사용하여 연결할 수 ["KMS 구성을 지웁니다"](#) 있습니다. KMS 구성은 * 노드 암호화 * 설정이 비활성화되고 StorageGRID 사이트에 대한 어플라이언스 노드와 KMS 구성 간의 연결이 제거됩니다.



KMS 암호화 키에 액세스할 수 없으므로 어플라이언스에 남아 있는 데이터는 더 이상 액세스할 수 없으며 영구적으로 잠깁니다.

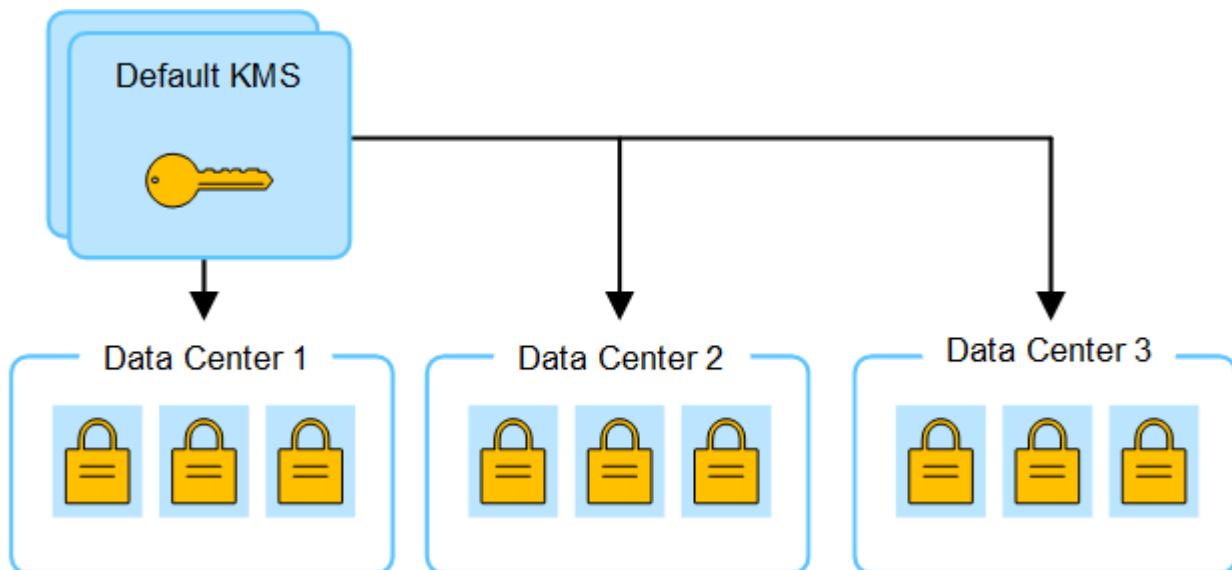
사이트의 KMS를 변경할 때의 고려 사항

각 KMS(Key Management Server) 또는 KMS 클러스터는 단일 사이트 또는 사이트 그룹의 모든 어플라이언스 노드에 암호화 키를 제공합니다. 사이트에 사용되는 KMS를 변경해야 하는 경우 암호화 키를 한 KMS에서 다른 KMS로 복사해야 할 수 있습니다.

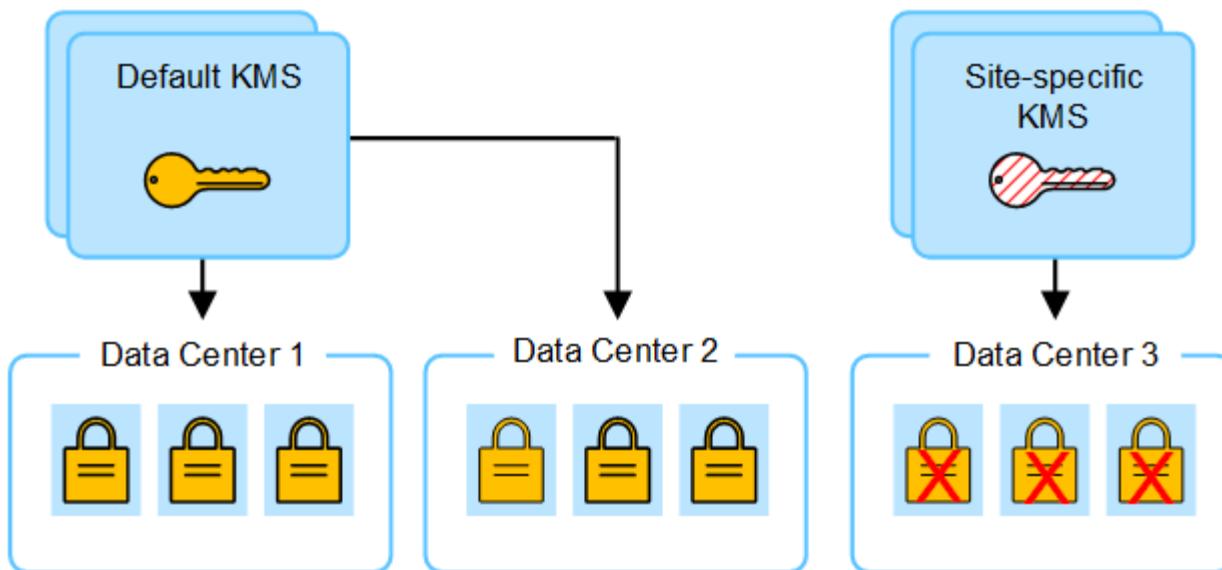
사이트에 사용되는 KMS를 변경하는 경우 해당 사이트에서 이전에 암호화된 어플라이언스 노드를 새 KMS에 저장된 키를 사용하여 해독할 수 있는지 확인해야 합니다. 경우에 따라 기존 KMS에서 새 KMS로 최신 버전의 암호화 키를 복사해야 할 수도 있습니다. KMS가 사이트에서 암호화된 어플라이언스 노드를 해독할 수 있는 올바른 키를 가지고 있는지 확인해야 합니다.

예를 들면 다음과 같습니다.

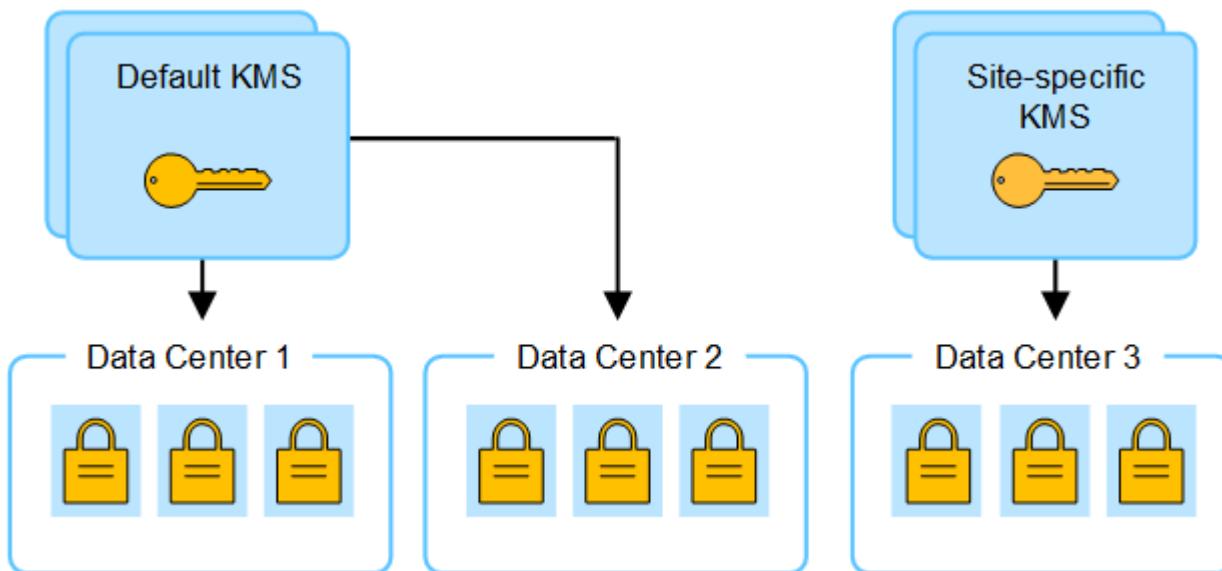
1. 처음에는 전용 KMS가 없는 모든 사이트에 적용되는 기본 KMS를 구성합니다.
2. KMS가 저장되면 * 노드 암호화 * 설정이 활성화된 모든 어플라이언스 노드가 KMS에 연결하여 암호화 키를 요청합니다. 이 키는 모든 사이트에서 어플라이언스 노드를 암호화하는 데 사용됩니다. 이러한 어플라이언스의 암호를 해독하는 데에도 이 동일한 키를 사용해야 합니다.



3. 한 사이트에 대해 사이트별 KMS를 추가하기로 결정합니다(그림의 데이터 센터 3). 그러나 어플라이언스 노드는 이미 암호화되어 있으므로 사이트별 KMS에 대한 구성을 저장하려고 하면 유효성 검사 오류가 발생합니다. 이 오류는 사이트별 KMS에 해당 사이트의 노드를 해독할 수 있는 올바른 키가 없기 때문에 발생합니다.



4. 이 문제를 해결하려면 기본 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사합니다. (원칙적으로 원래 키를 동일한 별칭이 있는 새 키에 복사합니다. 원래 키는 새 키의 이전 버전이 됩니다.) 사이트별 KMS에는 이제 데이터 센터 3에서 어플라이언스 노드를 해독하는 올바른 키가 있으므로 StorageGRID에 저장할 수 있습니다.



사이트에 사용되는 **KMS**를 변경하는 사용 사례

이 표에는 사이트에 대한 KMS를 변경하는 가장 일반적인 경우를 위한 필수 단계가 요약되어 있습니다.

사이트의 KMS를 변경하는 사용 사례	필요한 단계
하나 이상의 사이트별 KMS 항목이 있으며 이 중 하나를 기본 KMS로 사용하려고 합니다.	사이트별 KMS를 편집합니다. [에 대한 키 관리] 필드에서 * 다른 KMS에 의해 관리되지 않는 사이트(기본 KMS) * 를 선택합니다. 이제 사이트별 KMS가 기본 KMS로 사용됩니다. 이 내용은 전용 KMS가 없는 사이트에 적용됩니다. "KMS(키 관리 서버) 편집"

사이트의 KMS를 변경하는 사용 사례	필요한 단계
기본 KMS가 있으며 확장 시 새 사이트를 추가합니다. 새 사이트에 기본 KMS를 사용하지 않으려는 경우	<ol style="list-style-type: none"> 새 사이트의 어플라이언스 노드가 기본 KMS에 의해 이미 암호화된 경우 KMS 소프트웨어를 사용하여 기본 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사합니다. Grid Manager를 사용하여 새 KMS를 추가하고 사이트를 선택합니다. <p>"KMS(키 관리 서버) 추가"</p>
사이트의 KMS가 다른 서버를 사용하도록 해야 합니다.	<ol style="list-style-type: none"> 사이트의 어플라이언스 노드가 기존 KMS에 의해 이미 암호화된 경우 KMS 소프트웨어를 사용하여 기존 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사합니다. Grid Manager를 사용하여 기존 KMS 구성을 편집하고 새 호스트 이름 또는 IP 주소를 입력합니다. <p>"KMS(키 관리 서버) 추가"</p>

KMS에서 StorageGRID를 클라이언트로 구성합니다

KMS를 StorageGRID에 추가하려면 각 외부 키 관리 서버 또는 KMS 클러스터에 대해 StorageGRID를 클라이언트로 구성해야 합니다.



이러한 지침은 Thales CipherTrust Manager 및 Hashicorp Vault에 적용됩니다. 지원되는 제품 및 버전 목록을 보려면 ["NetApp 상호 운용성 매트릭스 툴\(IMT\)"](#) 사용합니다.

단계

1. KMS 소프트웨어에서 사용하려는 각 KMS 또는 KMS 클러스터에 대해 StorageGRID 클라이언트를 만듭니다.

각 KMS는 단일 사이트 또는 사이트 그룹에서 StorageGRID 어플라이언스 노드에 대한 단일 암호화 키를 관리합니다.

2. 다음 두 가지 방법 중 하나를 사용하여 키를 만듭니다.
 - KMS 제품의 키 관리 페이지를 사용합니다. 각 KMS 또는 KMS 클러스터에 대해 AES 암호화 키를 생성합니다.

암호화 키는 2,048비트 이상이어야 하며 내보낼 수 있어야 합니다.

- StorageGRID에서 키를 생성하도록 합니다. 테스트 후 저장하면 메시지가 ["클라이언트 인증서를 업로드하는 중입니다"](#) 표시됩니다.

3. 각 KMS 또는 KMS 클러스터에 대해 다음 정보를 기록합니다.

KMS를 StorageGRID에 추가할 때 다음 정보가 필요합니다.

- 각 서버의 호스트 이름 또는 IP 주소입니다.
- KMS에서 KMIP 포트를 사용합니다.
- KMS의 암호화 키에 대한 키 별칭입니다.

4. 각 KMS 또는 KMS 클러스터에 대해 CA(인증 기관)가 서명한 서버 인증서 또는 인증서 체인 순서에 따라 연결된

PEM 인코딩된 CA 인증서 파일이 들어 있는 인증서 번들을 받습니다.

서버 인증서를 사용하면 외부 KMS가 StorageGRID에 자신을 인증할 수 있습니다.

- 인증서는 PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식을 사용해야 합니다.
- 각 서버 인증서의 주체 대체 이름(SAN) 필드에는 StorageGRID가 연결할 정규화된 도메인 이름(FQDN) 또는 IP 주소가 포함되어야 합니다.



StorageGRID에서 KMS를 구성할 때 * 호스트 이름 * 필드에 동일한 FQDN 또는 IP 주소를 입력해야 합니다.

- 서버 인증서는 KMS의 KMIP 인터페이스에서 사용하는 인증서와 일치해야 하며, 일반적으로 포트 5696을 사용합니다.

5. 외부 KMS 및 클라이언트 인증서의 개인 키로 StorageGRID에 발급된 공용 클라이언트 인증서를 얻습니다.

클라이언트 인증서를 사용하면 StorageGRID가 KMS에 대한 인증을 받을 수 있습니다.

KMS(키 관리 서버) 추가

StorageGRID 키 관리 서버 마법사를 사용하여 각 KMS 또는 KMS 클러스터를 추가합니다.

시작하기 전에

- 를 검토했습니다.["키 관리 서버 사용에 대한 고려 사항 및 요구 사항"](#)
- ["KMS에서 StorageGRID를 클라이언트로 구성했습니다"](#)각 KMS 또는 KMS 클러스터에 필요한 정보가 있습니다.
- 을 사용하여 그리드 관리자에 로그인되어 있습니다.["지원되는 웹 브라우저"](#)
- 이 ["루트 액세스 권한"](#)있습니다.

이 작업에 대해

가능하면 다른 KMS에서 관리하지 않는 모든 사이트에 적용되는 기본 KMS를 구성하기 전에 사이트별 키 관리 서버를 구성하십시오. 기본 KMS를 먼저 만들면 그리드의 모든 노드 암호화 어플라이언스는 기본 KMS로 암호화됩니다. 나중에 사이트별 KMS를 만들려면 먼저 기본 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사해야 합니다. 자세한 내용은 ["사이트의 KMS를 변경할 때의 고려 사항"](#) 참조하십시오.

1단계: KMS 세부 정보

KMS(Key Management Server 추가) 마법사의 1단계(KMS 세부 정보)에서 KMS 또는 KMS 클러스터에 대한 세부 정보를 제공합니다.

단계

1. 구성 > 보안 > *키 관리 서버*를 선택합니다.

구성 세부 정보 탭이 선택된 키 관리 서버 페이지가 나타납니다.

2. Create * 를 선택합니다.

키 관리 서버 추가 마법사의 1단계(KMS 세부 정보)가 나타납니다.

3. KMS에 구성한 KMS 및 StorageGRID 클라이언트에 대한 다음 정보를 입력합니다.

필드에 입력합니다	설명
KMS 이름	이 KMS를 식별하는 데 도움이 되는 설명 이름입니다. 1자에서 64자 사이여야 합니다.
키 이름	KMS에서 StorageGRID 클라이언트에 대한 정확한 키 별칭입니다. 1자에서 255자 사이여야 합니다. <ul style="list-style-type: none"> • 참고 *: KMS 제품을 사용하여 키를 만들지 않은 경우 StorageGRID에서 키를 만들라는 메시지가 표시됩니다.
의 키를 관리합니다	이 KMS와 관련된 StorageGRID 사이트입니다. 가능하면 다른 KMS에서 관리하지 않는 모든 사이트에 적용되는 기본 KMS를 구성하기 전에 사이트별 키 관리 서버를 구성해야 합니다. <ul style="list-style-type: none"> • 이 KMS가 특정 사이트의 어플라이언스 노드에 대한 암호화 키를 관리하는 경우 사이트를 선택합니다. • 전용 KMS가 없는 사이트와 후속 확장에 추가한 사이트에 적용되는 기본 KMS를 구성하려면 * 다른 KMS(기본 KMS)에서 관리하지 않는 사이트 *를 선택합니다. <ul style="list-style-type: none"> ◦ 참고: * KMS 구성을 저장하면 검증 오류가 발생합니다. KMS 기본 KMS에 의해 이전에 암호화된 사이트를 선택했지만 새 KMS에 원본 암호화 키의 현재 버전을 제공하지 않은 경우 KMS 구성을 저장하면 오류가 발생합니다.
포트	KMS 서버가 KMIP(Key Management Interoperability Protocol) 통신에 사용하는 포트입니다. 기본값은 5696으로, KMIP 표준 포트입니다.
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. <ul style="list-style-type: none"> • 참고: * 서버 인증서의 주체 대체 이름(SAN) 필드에는 여기에 입력한 FQDN 또는 IP 주소가 포함되어야 합니다. 그렇지 않으면 StorageGRID는 KMS 또는 KMS 클러스터의 모든 서버에 연결할 수 없습니다.

4. KMS 클러스터를 구성하는 경우 * 다른 호스트 이름 추가 * 를 선택하여 클러스터의 각 서버에 대한 호스트 이름을 추가합니다.
5. Continue * 를 선택합니다.

2단계: 서버 인증서를 업로드합니다

키 관리 서버 추가 마법사의 2단계(서버 인증서 업로드)에서 KMS에 대한 서버 인증서(또는 인증서 번들)를 업로드합니다. 서버 인증서를 사용하면 외부 KMS가 StorageGRID에 자신을 인증할 수 있습니다.

단계

1. 2단계(서버 인증서 업로드) * 에서 저장된 서버 인증서 또는 인증서 번들의 위치를 찾습니다.
2. 인증서 파일을 업로드합니다.

서버 인증서 메타데이터가 나타납니다.



인증서 번들을 업로드한 경우 각 인증서의 메타데이터가 해당 탭에 표시됩니다.

3. Continue * 를 선택합니다.

】 3단계: 클라이언트 인증서 업로드

키 관리 서버 추가 마법사의 3단계(클라이언트 인증서 업로드)에서 클라이언트 인증서와 클라이언트 인증서 개인 키를 업로드합니다. 클라이언트 인증서를 사용하면 StorageGRID가 KMS에 대한 인증을 받을 수 있습니다.

단계

1. 3단계(클라이언트 인증서 업로드) * 에서 클라이언트 인증서 위치를 찾습니다.
2. 클라이언트 인증서 파일을 업로드합니다.

클라이언트 인증서 메타데이터가 나타납니다.

3. 클라이언트 인증서의 개인 키 위치를 찾습니다.
4. 개인 키 파일을 업로드합니다.
5. 테스트 및 저장 * 을 선택합니다.

키가 없으면 StorageGRID에서 키를 만들라는 메시지가 표시됩니다.

키 관리 서버와 어플라이언스 노드 간의 연결은 테스트를 거칩니다. 모든 연결이 올바르고 KMS에서 올바른 키를 찾으면 키 관리 서버 페이지의 표에 새 키 관리 서버가 추가됩니다.



KMS를 추가한 직후 키 관리 서버 페이지의 인증서 상태는 알 수 없음으로 표시됩니다. 각 인증서의 실제 상태를 가져오는 데 30분 정도 StorageGRID 걸릴 수 있습니다. 현재 상태를 보려면 웹 브라우저를 새로 고쳐야 합니다.

6. 테스트 및 저장 * 을 선택할 때 오류 메시지가 나타나면 메시지 세부 정보를 검토한 다음 * 확인 * 을 선택합니다.

예를 들어 연결 테스트에 실패한 경우 422:처리할 수 없는 엔터티 오류가 발생할 수 있습니다.

7. 외부 연결을 테스트하지 않고 현재 구성을 저장해야 하는 경우 * 강제 저장 * 을 선택합니다.



강제 저장 * 을 선택하면 KMS 구성이 저장되지만 각 제품에서 해당 KMS로의 외부 연결은 테스트되지 않습니다. 구성에 문제가 있을 경우 해당 사이트에서 노드 암호화가 활성화된 어플라이언스 노드를 재부팅하지 못할 수 있습니다. 문제가 해결될 때까지 데이터에 액세스하지 못할 수 있습니다.

8. 확인 경고를 검토하고 구성을 강제 저장하려면 * OK * 를 선택합니다.

KMS 구성은 저장되지만 KMS에 대한 연결은 테스트되지 않습니다.

KMS를 관리합니다

KMS(키 관리 서버) 관리에는 세부 정보 보기 또는 편집, 인증서 관리, 암호화된 노드 보기, KMS

제거 등이 포함됩니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 이 "[필수 액세스 권한](#)"입니다.

KMS 세부 정보 보기

키 세부 정보, 서버 및 클라이언트 인증서의 현재 상태 등 StorageGRID 시스템의 각 KMS(키 관리 서버)에 대한 정보를 볼 수 있습니다.

단계

- 구성 > 보안 > *키 관리 서버*를 선택합니다.

키 관리 서버 페이지가 나타나고 다음 정보가 표시됩니다.

- 구성 세부 정보 탭에는 구성된 모든 키 관리 서버가 나열됩니다.
- 암호화된 노드 탭에는 노드 암호화가 활성화된 모든 노드가 나열됩니다.

- 특정 KMS에 대한 세부 정보를 보고 해당 KMS에 대한 작업을 수행하려면 KMS의 이름을 선택합니다. KMS의 세부 정보 페이지에는 다음 정보가 나열됩니다.

필드에 입력합니다	설명
의 키를 관리합니다	KMS와 관련된 StorageGRID 사이트 이 필드에는 특정 StorageGRID 사이트 또는 다른 KMS(기본 KMS)가 관리하지 않는 사이트의 이름이 표시됩니다.*
호스트 이름	KMS의 정규화된 도메인 이름 또는 IP 주소입니다. 두 개의 키 관리 서버로 구성된 클러스터가 있는 경우 두 서버의 정규화된 도메인 이름 또는 IP 주소가 나열됩니다. 클러스터에 키 관리 서버가 두 개 이상 있는 경우 첫 번째 KMS의 정규화된 도메인 이름 또는 IP 주소가 클러스터에 있는 추가 키 관리 서버의 수와 함께 나열됩니다. 예 10.10.10.10 and 10.10.10.11: 또는 10.10.10.10 and 2 others. 클러스터의 모든 호스트 이름을 보려면 KMS를 선택하고 * 편집 * 또는 * 작업 * > * 편집 * 을 선택합니다.

- KMS 세부 정보 페이지에서 탭을 선택하여 다음 정보를 봅니다.

탭을 클릭합니다	필드에 입력합니다	설명
키 세부 정보	키 이름	KMS에서 StorageGRID 클라이언트의 키 별칭입니다.

탭을 클릭합니다	필드에 입력합니다	설명
키 UID	최신 버전의 키에 대한 고유 식별자입니다.	마지막 수정
키의 최신 버전 날짜 및 시간입니다.	서버 인증서	메타데이터
인증서의 메타데이터 (예: 일련 번호, 만료 날짜 및 시간, 인증서 PEM)	인증서 PEM	인증서에 대한 PEM(개인 정보 보호 강화 메일) 파일의 내용입니다.
클라이언트 인증서	메타데이터	인증서의 메타데이터(예: 일련 번호, 만료 날짜 및 시간, 인증서 PEM)

4.] 조직의 보안 관행에 필요한 만큼 * Rotate key * 를 선택하거나 KMS 소프트웨어를 사용하여 새 버전의 키를 만듭니다.

키 회전이 성공하면 키 UID 및 마지막으로 수정된 필드가 업데이트됩니다.

KMS 소프트웨어를 사용하여 암호화 키를 회전하는 경우 마지막으로 사용한 키 버전에서 동일한 키의 새 버전으로 회전합니다. 완전히 다른 키로 회전하지 마십시오.



KMS의 키 이름(별칭)을 변경하여 키를 회전하려고 하지 마십시오. StorageGRID를 사용하려면 KMS에서 동일한 키 별칭을 사용하여 이전에 사용한 모든 키 버전과 향후 모든 키 버전에 액세스할 수 있어야 합니다. 구성된 KMS의 키 별칭을 변경하면 StorageGRID에서 데이터의 암호를 해독하지 못할 수 있습니다.

인증서를 관리합니다

모든 서버 또는 클라이언트 인증서 문제를 즉시 해결합니다. 가능하면 만료되기 전에 인증서를 교체하십시오.



데이터 액세스를 유지하려면 가능한 한 빨리 인증서 문제를 해결해야 합니다.

단계

1. 구성 > 보안 > *키 관리 서버*를 선택합니다.
2. 표에서 각 KMS에 대한 인증서 만료 값을 확인합니다.
3. KMS에 대한 인증서 만료가 알 수 없는 경우 최대 30분 정도 기다린 다음 웹 브라우저를 새로 고칩니다.
4. 인증서 만료 열에 인증서가 만료되었거나 만료가 임박했음을 나타내는 경우 KMS를 선택하여 KMS 세부 정보 페이지로 이동합니다.
 - a. 서버 인증서 * 를 선택하고 "만료 날짜" 필드에 대한 값을 확인합니다.
 - b. 인증서를 교체하려면 * 인증서 편집 * 을 선택하여 새 인증서를 업로드합니다.
 - c. 이 하위 단계를 반복하고 서버 인증서 대신 * 클라이언트 인증서 * 를 선택합니다.

5. KMS CA 인증서 만료 * , * KMS 클라이언트 인증서 만료 * 및 * KMS 서버 인증서 만료 * 알림이 트리거되면 각 경고에 대한 설명을 기록하고 권장 조치를 수행합니다.

인증서 만료에 대한 업데이트를 받는 데 30분 정도 걸릴 수 StorageGRID 있습니다. 현재 값을 보려면 웹 브라우저를 새로 고치십시오.



서버 인증서 상태가 알 수 없음 * 인 경우 KMS에서 클라이언트 인증서 없이도 서버 인증서를 받을 수 있도록 허용하는지 확인합니다.

암호화된 노드를 봅니다

노드 암호화 * 설정이 활성화된 StorageGRID 시스템의 어플라이언스 노드에 대한 정보를 볼 수 있습니다.

단계

1. 구성 > 보안 > *키 관리 서버*를 선택합니다.

키 관리 서버 페이지가 나타납니다. 구성 세부 정보 탭에는 구성된 모든 키 관리 서버가 표시됩니다.

2. 페이지 상단에서 *암호화된 노드 * 탭을 선택합니다.

암호화된 노드 탭에는 * 노드 암호화 * 설정이 활성화된 StorageGRID 시스템의 어플라이언스 노드가 나열됩니다.

3. 각 어플라이언스 노드에 대해 표의 정보를 검토합니다.

열	설명
노드 이름	어플라이언스 노드의 이름입니다.
노드 유형입니다	노드 유형: 스토리지, 관리자 또는 게이트웨이
사이트	노드가 설치된 StorageGRID 사이트의 이름입니다.
KMS 이름	노드에 사용된 KMS의 설명 이름입니다. KMS가 나열되지 않으면 구성 세부 정보 탭을 선택하여 KMS를 추가합니다. "KMS(키 관리 서버) 추가"
키 UID	어플라이언스 노드에서 데이터를 암호화하고 해독하는 데 사용되는 암호화 키의 고유 ID입니다. 전체 키 UID를 보려면 텍스트를 선택합니다. 대시(--)는 어플라이언스 노드와 KMS 사이의 연결 문제로 인해 키 UID를 알 수 없음을 나타냅니다.

열	설명
상태	<p>KMS와 어플라이언스 노드 간의 연결 상태입니다. 노드가 연결되어 있으면 타임스탬프가 30분마다 업데이트됩니다. KMS 구성이 변경된 후 연결 상태를 업데이트하는 데 몇 분 정도 걸릴 수 있습니다.</p> <ul style="list-style-type: none"> 참고: * 새 값을 보려면 웹 브라우저를 새로 고치십시오.

4. 상태 열에 KMS 문제가 표시되면 즉시 문제를 해결하십시오.

KMS가 정상적으로 작동하는 동안 KMS*에 연결됨 상태로 표시됩니다. 노드가 그리드에서 연결이 끊어지면 노드 연결 상태가 표시됩니다(관리자 다운 또는 알 수 없음).

다른 상태 메시지는 이름이 같은 StorageGRID 알림에 해당합니다.

- KMS 구성은 로드하지 못했습니다
- KMS 연결 오류입니다
- KMS 암호화 키 이름을 찾을 수 없습니다
- KMS 암호화 키 회전이 실패했습니다
- 킬로미터 키가 어플라이언스 볼륨을 해독하지 못했습니다
- KMS가 구성되지 않았습니다

이러한 경고에 대해 권장되는 작업을 수행합니다.



데이터를 완벽하게 보호하려면 모든 문제를 즉시 해결해야 합니다.

KMS를 편집합니다

예를 들어 인증서가 곧 만료될 경우 키 관리 서버의 구성을 편집해야 할 수 있습니다.

시작하기 전에

- KMS에 대해 선택한 사이트를 업데이트할 계획이 있는 경우를 검토한 ["사이트의 KMS를 변경할 때의 고려 사항"](#) 것입니다.
- 을 사용하여 그리드 관리자에 로그인되어 있습니다. ["지원되는 웹 브라우저"](#)
- 이 ["루트 액세스 권한"](#)입니다.

단계

1. 구성 > 보안 > *키 관리 서버*를 선택합니다.

키 관리 서버 페이지가 나타나고 구성된 모든 키 관리 서버가 표시됩니다.

2. 편집할 KMS를 선택하고 * Actions * > * Edit * 를 선택합니다.

KMS 세부 정보 페이지에서 KMS 이름을 선택하고 * 편집 * 을 선택하여 KMS를 편집할 수도 있습니다.

3. 선택적으로 키 관리 서버 편집 마법사의 * 1단계(KMS 세부 정보) * 에 있는 세부 정보를 업데이트합니다.

필드에 입력합니다	설명
KMS 이름	이 KMS를 식별하는 데 도움이 되는 설명 이름입니다. 1자에서 64자 사이여야 합니다.
키 이름	<p>KMS에서 StorageGRID 클라이언트에 대한 정확한 키 별칭입니다. 1자에서 255자 사이여야 합니다.</p> <p>키 이름은 드문 경우지만 편집하면 됩니다. 예를 들어, KMS에서 별칭의 이름이 바뀌거나 이전 키의 모든 버전이 새 별칭의 버전 기록으로 복사된 경우 키 이름을 편집해야 합니다.</p>
의 키를 관리합니다	<p>사이트별 KMS를 편집하고 있고 기본 KMS가 아직 없는 경우 선택적으로 * 다른 KMS(기본 KMS)에서 관리하지 않는 사이트 * 를 선택합니다. 이 항목을 선택하면 사이트별 KMS가 기본 KMS로 변환되며, 이 KMS는 전용 KMS가 없는 모든 사이트와 확장 시 추가된 사이트에 적용됩니다.</p> <ul style="list-style-type: none"> 참고: * 사이트별 KMS를 편집하는 경우 다른 사이트를 선택할 수 없습니다. 기본 KMS를 편집하는 경우 특정 사이트를 선택할 수 없습니다.
포트	KMS 서버가 KMIP(Key Management Interoperability Protocol) 통신에 사용하는 포트입니다. 기본값은 5696으로, KMIP 표준 포트입니다.
호스트 이름	<p>KMS의 정규화된 도메인 이름 또는 IP 주소입니다.</p> <ul style="list-style-type: none"> 참고: * 서버 인증서의 주체 대체 이름(SAN) 필드에는 여기에 입력한 FQDN 또는 IP 주소가 포함되어야 합니다. 그렇지 않으면 StorageGRID는 KMS 또는 KMS 클러스터의 모든 서버에 연결할 수 없습니다.

4. KMS 클러스터를 구성하는 경우 * 다른 호스트 이름 추가 * 를 선택하여 클러스터의 각 서버에 대한 호스트 이름을 추가합니다.
 5. Continue * 를 선택합니다.
 6. 키 관리 서버 편집 마법사의 2단계(서버 인증서 업로드)가 나타납니다.
 7. 서버 인증서를 교체해야 하는 경우 * 찾아보기 * 를 선택하고 새 파일을 업로드합니다.
 8. Continue * 를 선택합니다.
 9. 키 관리 서버 편집 마법사의 3단계(클라이언트 인증서 업로드)가 나타납니다.
 10. 클라이언트 인증서와 클라이언트 인증서 개인 키를 교체해야 하는 경우 * 찾아보기 * 를 선택하고 새 파일을 업로드합니다.
 11. 테스트 및 저장 * 을 선택합니다.
- 영향을 받는 사이트에서 키 관리 서버와 모든 노드 암호화 어플라이언스 노드 간의 연결을 테스트합니다. 모든 노드 연결이 유효하고 KMS에서 올바른 키를 찾으면 키 관리 서버가 키 관리 서버 페이지의 테이블에 추가됩니다.
12. 오류 메시지가 나타나면 메시지 세부 정보를 검토하고 * OK * 를 선택합니다.

예를 들어, 이 KMS에 대해 선택한 사이트가 다른 KMS에 의해 이미 관리되고 있거나 연결 테스트에 실패한 경우 422:처리할 수 없는 엔터티 오류가 발생할 수 있습니다.

11. 연결 오류를 해결하기 전에 현재 설정을 저장해야 하는 경우 * 강제 저장 * 을 선택합니다.



강제 저장 * 을 선택하면 KMS 구성이 저장되지만 각 제품에서 해당 KMS로의 외부 연결은 테스트되지 않습니다. 구성에 문제가 있을 경우 해당 사이트에서 노드 암호화가 활성화된 어플라이언스 노드를 재부팅하지 못할 수 있습니다. 문제가 해결될 때까지 데이터에 액세스하지 못할 수 있습니다.

KMS 구성이 저장됩니다.

12. 확인 경고를 검토하고 구성을 강제 저장하려면 * OK * 를 선택합니다.

KMS 구성이 저장되지만 KMS에 대한 연결은 테스트되지 않습니다.

KMS(키 관리 서버) 제거

경우에 따라 키 관리 서버를 제거할 수 있습니다. 예를 들어 사이트를 해체한 경우 사이트별 KMS를 제거할 수 있습니다.

시작하기 전에

- 를 검토했습니다.["키 관리 서버 사용에 대한 고려 사항 및 요구 사항"](#)
- 을 사용하여 그리드 관리자에 로그인되어 있습니다.["지원되는 웹 브라우저"](#)
- 이 ["루트 액세스 권한"](#)있습니다.

이 작업에 대해

다음과 같은 경우 KMS를 제거할 수 있습니다.

- 사이트를 폐기했거나 사이트에 노드 암호화가 활성화된 어플라이언스 노드가 없는 경우 사이트별 KMS를 제거할 수 있습니다.
- 노드 암호화가 활성화된 어플라이언스 노드가 있는 각 사이트에 대해 사이트별 KMS가 이미 있는 경우 기본 KMS를 제거할 수 있습니다.

단계

1. 구성 > 보안 > *키 관리 서버*를 선택합니다.

키 관리 서버 페이지가 나타나고 구성된 모든 키 관리 서버가 표시됩니다.

2. 제거할 KMS를 선택하고 * Actions * > * Remove * 를 선택합니다.

KMS 세부 정보 페이지에서 KMS 이름을 선택하고 * Remove * 를 선택하여 KMS를 제거할 수도 있습니다.

3. 다음 내용이 맞는지 확인합니다.

- 노드 암호화가 활성화된 어플라이언스 노드가 없는 사이트에 대한 사이트별 KMS를 제거하고 있습니다.
- 기본 KMS를 제거하고 있지만 노드 암호화를 사용하는 각 사이트에 대해 사이트별 KMS가 이미 있습니다.

4. 예 * 를 선택합니다.

KMS 구성이 제거되었습니다.

프록시 설정을 관리합니다

스토리지 프록시를 구성합니다

플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 스토리지 노드와 외부 S3 엔드포인트 간에 투명하지 않은 프록시를 구성할 수 있습니다. 예를 들어, 플랫폼 서비스 메시지를 인터넷의 끝점과 같은 외부 끝점으로 보내려면 투명하지 않은 프록시가 필요할 수 있습니다.



구성된 스토리지 프록시 설정은 Kafka 플랫폼 서비스 엔드포인트에 적용되지 않습니다.

시작하기 전에

- 있습니다. "[특정 액세스 권한](#)"
- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"

이 작업에 대해

단일 스토리지 프록시에 대한 설정을 구성할 수 있습니다.

단계

1. 구성 > 보안 > *프록시 설정*을 선택합니다.
2. Storage * 탭에서 * Enable storage proxy * 확인란을 선택합니다.
3. 스토리지 프록시의 프로토콜을 선택합니다.
4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. 필요에 따라 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.

프로토콜의 기본 포트(HTTP의 경우 80, SOCKS5의 경우 1080)를 사용하려면 이 필드를 비워 둡니다.

6. 저장 * 을 선택합니다.

스토리지 프록시가 저장된 후 플랫폼 서비스 또는 클라우드 스토리지 풀의 새 엔드포인트를 구성하고 테스트할 수 있습니다.



프록시 변경 사항이 적용되려면 최대 10분이 소요될 수 있습니다.

7. 프록시 서버의 설정을 확인하여 StorageGRID의 플랫폼 서비스 관련 메시지가 차단되지 않는지 확인합니다.
8. 스토리지 프록시를 비활성화해야 하는 경우 확인란을 선택 취소하고 * 저장 * 을 선택합니다.

관리자 프록시 설정을 구성합니다

HTTP 또는 HTTPS를 사용하여 AutoSupport 패키지를 보내는 경우 관리 노드와 기술 지원(AutoSupport) 간에 비투명 프록시 서버를 구성할 수 있습니다.

AutoSupport에 대한 자세한 내용은 을 "[AutoSupport를 구성합니다](#)" 참조하십시오.

시작하기 전에

- 있습니다. "[특정 액세스 권한](#)"

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."[지원되는 웹 브라우저](#)"

이 작업에 대해

단일 관리자 프록시에 대한 설정을 구성할 수 있습니다.

단계

1. 구성 > 보안 > *프록시 설정*을 선택합니다.

프록시 설정 페이지가 나타납니다. 기본적으로 탭 메뉴에서 스토리지가 선택되어 있습니다.

2. 관리 * 탭을 선택합니다.
3. 관리자 프록시 사용 * 확인란을 선택합니다.
4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.
6. 필요한 경우 프록시 서버의 사용자 이름과 암호를 입력합니다.

프록시 서버에 사용자 이름 또는 암호가 필요하지 않은 경우 이 필드를 비워 둡니다.

7. 다음 중 하나를 선택합니다.

- 관리자 프록시에 대한 연결을 보호하려면 * 프록시 인증서 확인 * 을 선택합니다. CA 번들을 업로드하여 관리 프록시 서버에서 제공하는 SSL 인증서의 신뢰성을 확인합니다.



프록시 인증서가 확인된 경우 AutoSupport on Demand, StorageGRID를 통한 E-Series AutoSupport 및 StorageGRID 업그레이드 페이지의 업데이트 경로 확인이 작동하지 않습니다.

CA 번들을 업로드하면 해당 메타데이터가 나타납니다.

- 관리자 프록시 서버와 통신할 때 인증서의 유효성을 검사하지 않으려면 * 프록시 인증서 확인 안 함 * 을 선택합니다.

8. 저장 * 을 선택합니다.

관리자 프록시가 저장된 후 관리 노드와 기술 지원 간의 프록시 서버가 구성됩니다.



프록시 변경 사항이 적용되려면 최대 10분이 소요될 수 있습니다.

9. 관리자 프록시를 비활성화해야 하는 경우 * 관리자 프록시 사용 * 확인란의 선택을 취소한 다음 * 저장 * 을 선택합니다.

방화벽을 제어합니다

외부 방화벽에서 액세스를 제어합니다

외부 방화벽에서 특정 포트를 열거나 닫을 수 있습니다.

외부 방화벽에서 특정 포트를 열거나 닫아 StorageGRID 관리 노드의 사용자 인터페이스 및 API에 대한 액세스를 제어할 수 있습니다. 예를 들어, 테넌트가 다른 방법을 사용하여 시스템 액세스를 제어하는 것 외에도 방화벽에서 Grid Manager에 연결할 수 없도록 할 수 있습니다.

StorageGRID 내부 방화벽을 구성하려면 를 참조하십시오 "[내부 방화벽을 구성합니다](#)".

포트	설명	포트가 열려 있는 경우...
443	관리 노드의 기본 HTTPS 포트	<p>웹 브라우저 및 관리 API 클라이언트는 Grid Manager, Grid Management API, Tenant Manager 및 Tenant Management API에 액세스할 수 있습니다.</p> <ul style="list-style-type: none">참고: * 포트 443은 일부 내부 트래픽에도 사용됩니다.
8443	관리 노드의 제한된 그리드 관리자 포트	<ul style="list-style-type: none">웹 브라우저 및 관리 API 클라이언트는 HTTPS를 사용하여 그리드 관리자 및 그리드 관리 API에 액세스할 수 있습니다.웹 브라우저 및 관리 API 클라이언트는 테넌트 관리자 또는 테넌트 관리 API에 액세스할 수 없습니다.내부 콘텐츠 요청은 거부됩니다.
9443	관리 노드의 제한된 테넌트 관리자 포트	<ul style="list-style-type: none">웹 브라우저 및 관리 API 클라이언트는 HTTPS를 사용하여 테넌트 관리자 및 테넌트 관리 API에 액세스할 수 있습니다.웹 브라우저 및 관리 API 클라이언트는 그리드 관리자 또는 그리드 관리 API에 액세스할 수 없습니다.내부 콘텐츠 요청은 거부됩니다.



제한된 Grid Manager 또는 테넌트 관리자 포트에서는 SSO(Single Sign-On)를 사용할 수 없습니다. 사용자가 SSO(Single Sign-On)로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다.

관련 정보

- "[Grid Manager에 로그인합니다](#)"
- "[테넌트 계정을 생성합니다](#)"
- "[외부 통신](#)"

내부 방화벽 제어를 관리합니다

StorageGRID에는 노드에 대한 네트워크 액세스를 제어할 수 있도록 함으로써 그리드의 보안을 강화하는 각 노드에 대한 내부 방화벽이 포함되어 있습니다. 방화벽을 사용하여 특정 그리드 구축에 필요한 포트를 제외한 모든 포트의 네트워크 액세스를 방지합니다. 방화벽 제어 페이지에서 변경한 구성은 각 노드에 배포됩니다.

방화벽 제어 페이지의 세 가지 탭을 사용하여 그리드에 필요한 액세스를 사용자 지정합니다.

- * 특별 권한 주소 목록 *: 이 탭을 사용하면 닫힌 포트에 대한 선택된 액세스를 허용할 수 있습니다. 외부 액세스 관리 탭을 사용하여 닫은 포트에 액세스할 수 있는 IP 주소 또는 서브넷을 CIDR 표시법으로 추가할 수 있습니다.
- * 외부 액세스 관리 *: 이 탭을 사용하여 기본적으로 열려 있는 포트를 닫거나 이전에 닫은 포트를 다시 열 수 있습니다.

- * 신뢰할 수 없는 클라이언트 네트워크 *: 노드가 클라이언트 네트워크의 인바운드 트래픽을 신뢰하는지 여부를 지정하려면 이 탭을 사용합니다.

이 탭의 설정은 외부 액세스 관리 탭의 설정보다 우선합니다.

- 신뢰할 수 없는 클라이언트 네트워크가 있는 노드는 해당 노드에 구성된 로드 밸런서 엔드포인트 포트(글로벌, 노드 인터페이스 및 노드 유형 바운드 엔드포인트)의 연결만 받아들입니다.
- 부하 분산 장치 엔드포인트 포트 는(는) 신뢰할 수 없는 클라이언트 네트워크에서 외부 네트워크 관리 탭의 설정에 관계없이 열려 있는 유일한 포트입니다.
- 신뢰할 수 있는 경우 외부 액세스 관리 탭에서 열린 모든 포트와 클라이언트 네트워크에 열려 있는 모든 로드 밸런서 끝점에 액세스할 수 있습니다.



한 탭에서 설정한 내용은 다른 탭의 액세스 변경에 영향을 줄 수 있습니다. 모든 탭의 설정을 확인하여 네트워크가 예상한 대로 작동하는지 확인하십시오.

내부 방화벽 제어를 구성하려면 를 참조하십시오 "[방화벽 제어를 구성합니다](#)".

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 을 "[외부 방화벽에서 액세스를 제어합니다](#)" 참조하십시오.

특별 권한 주소 목록 및 외부 액세스 관리 탭

특별 권한 주소 목록 탭을 사용하면 닫힌 그리드 포트에 대한 액세스 권한이 부여된 하나 이상의 IP 주소를 등록할 수 있습니다. 외부 액세스 관리 탭을 사용하면 선택한 외부 포트 또는 열려 있는 모든 외부 포트에 대한 외부 액세스를 닫을 수 있습니다(외부 포트는 기본적으로 비 그리드 노드가 액세스할 수 있는 포트입니다). 이러한 두 탭을 함께 사용하여 그리드에 필요한 정확한 네트워크 액세스를 사용자 지정할 수 있습니다.



권한이 있는 IP 주소는 기본적으로 내부 그리드 포트 액세스를 갖지 않습니다.

예 1: 유지 보수 작업에 점프 호스트를 사용합니다

네트워크 관리에 점프 호스트(보안 강화 호스트)를 사용하려는 경우를 가정해 보겠습니다. 다음과 같은 일반 단계를 사용할 수 있습니다.

1. 특별 권한 주소 목록 탭을 사용하여 점프 호스트의 IP 주소를 추가합니다.
2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단합니다.



포트 443 및 8443을 차단하기 전에 권한이 있는 IP 주소를 추가합니다. 사용자를 포함하여 현재 차단된 포트에 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다.

구성을 저장하면 이동 호스트를 제외한 모든 호스트에 대해 그리드의 관리 노드에 있는 모든 외부 포트가 차단됩니다. 그런 다음 점프 호스트를 사용하여 그리드에 대한 유지 관리 작업을 보다 안전하게 수행할 수 있습니다.

예 2: 민감한 포트를 잠금니다

민감한 포트와 해당 포트의 서비스를 잠그고 싶다고 가정해 보겠습니다. 다음과 같은 일반적인 단계를 사용할 수 있습니다.

1. 특별 권한 주소 목록 탭을 사용하여 서비스에 액세스해야 하는 호스트에만 액세스 권한을 부여합니다.

2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단합니다.



Grid Manager 및 Tenant Manager 액세스에 할당된 포트에 대한 액세스를 차단하기 전에 권한 있는 IP 주소를 추가합니다(사전 설정된 포트는 443 및 8443). 사용자를 포함하여 현재 차단된 포트에 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다.

구성을 저장한 후에는 민감한 포트와 해당 포트의 서비스를 특권 주소 목록에 있는 호스트에서 사용할 수 있습니다. 요청이 어떤 인터페이스에서 왔는지에 관계없이 다른 모든 호스트는 서비스에 대한 액세스가 거부됩니다.

예 3: 사용하지 않는 서비스에 대한 액세스를 비활성화합니다

네트워크 수준에서는 사용하지 않을 일부 서비스를 사용하지 않도록 설정할 수 있습니다. 예를 들어 HTTP S3 클라이언트 트래픽을 차단하려면 외부 액세스 관리 탭의 토글을 사용하여 포트 18084를 차단할 수 있습니다.

신뢰할 수 없는 클라이언트 네트워크 탭

클라이언트 네트워크를 사용하는 경우 명시적으로 구성된 끝점에서만 인바운드 클라이언트 트래픽을 허용하여 악의적인 공격으로부터 StorageGRID를 보호할 수 있습니다.

기본적으로 각 그리드 노드의 클라이언트 네트워크는 _trusted_ 입니다. 즉, 기본적으로 StorageGRID는 모든 의 각 그리드 노드에 대한 인바운드 연결을 신뢰합니다. ["사용 가능한 외부 포트"](#)

각 노드의 클라이언트 네트워크가 _untrusted_로 지정함으로써 StorageGRID 시스템에 대한 악의적인 공격의 위협을 줄일 수 있습니다. 노드의 클라이언트 네트워크를 신뢰할 수 없는 경우 노드는 로드 밸런서 끝점으로 명시적으로 구성된 포트의 인바운드 연결만 허용합니다. ["로드 밸런서 엔드포인트를 구성합니다"](#) 및 ["방화벽 제어를 구성합니다"](#) ["참조하십시오."](#)

예 1: 게이트웨이 노드는 **HTTPS S3** 요청만 허용합니다

게이트웨이 노드가 HTTPS S3 요청을 제외한 클라이언트 네트워크의 모든 인바운드 트래픽을 거부하도록 한다고 가정합니다. 다음과 같은 일반 단계를 수행합니다.

1. ["부하 분산 장치 엔드포인트"](#)페이지에서 포트 443에서 HTTPS를 통한 S3에 대한 로드 밸런서 끝점을 구성합니다.
2. 방화벽 제어 페이지에서 신뢰할 수 없음을 선택하여 게이트웨이 노드의 클라이언트 네트워크를 신뢰할 수 없도록 지정합니다.

구성을 저장한 후 게이트웨이 노드의 클라이언트 네트워크의 모든 인바운드 트래픽은 포트 443 및 ICMP 에코(ping) 요청의 HTTPS S3 요청을 제외하고 삭제됩니다.

예 2: 스토리지 노드가 **S3 플랫폼** 서비스 요청을 전송합니다

스토리지 노드에서 아웃바운드 S3 플랫폼 서비스 트래픽을 활성화하되 클라이언트 네트워크의 해당 스토리지 노드에 대한 인바운드 연결을 차단하려는 경우를 가정해 봅니다. 이 일반 단계를 수행합니다.

- 방화벽 제어 페이지의 신뢰할 수 없는 클라이언트 네트워크 탭에서 스토리지 노드의 클라이언트 네트워크를 신뢰할 수 없음을 나타냅니다.

구성을 저장한 후 스토리지 노드는 더 이상 클라이언트 네트워크에서 들어오는 트래픽을 허용하지 않지만 구성된 플랫폼 서비스 대상에 대한 아웃바운드 요청은 계속 허용합니다.

예 3: 그리드 관리자에 대한 액세스를 서브넷으로 제한

특정 서브넷에서만 Grid Manager 액세스를 허용한다고 가정합니다. 다음 단계를 수행합니다.

1. 관리 노드의 클라이언트 네트워크를 서브넷에 연결합니다.
2. 신뢰할 수 없는 클라이언트 네트워크 탭을 사용하여 클라이언트 네트워크를 신뢰할 수 없음으로 구성합니다.
3. 관리 인터페이스 로드 밸런서 엔드포인트를 생성할 때 port를 입력하고 포트가 액세스할 관리 인터페이스를 선택합니다.
4. 신뢰할 수 없는 클라이언트 네트워크에 대해 * 예 * 를 선택합니다.
5. 외부 액세스 관리 탭을 사용하여 모든 외부 포트(해당 서브넷 외부의 호스트에 대해 설정된 권한이 있는 IP 주소 포함 또는 제외)를 차단합니다.

구성을 저장한 후에는 지정한 서브넷의 호스트만 Grid Manager에 액세스할 수 있습니다. 다른 호스트는 모두 차단됩니다.

내부 방화벽을 구성합니다

StorageGRID 노드의 특정 포트에 대한 네트워크 액세스를 제어하도록 StorageGRID 방화벽을 구성할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다.["지원되는 웹 브라우저"](#)
- 있습니다. ["특정 액세스 권한"](#)
- 및 의 정보를 검토했습니다.["방화벽 제어 관리""네트워킹 지침"](#)
- 관리자 노드 또는 게이트웨이 노드가 명시적으로 구성된 끝점에서만 인바운드 트래픽을 수락하도록 하려면 로드 밸런서 끝점을 정의해야 합니다.



클라이언트 네트워크의 구성을 변경할 때 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

이 작업에 대해

StorageGRID에는 그리드의 노드에서 일부 포트를 열거나 닫을 수 있도록 각 노드에 대한 내부 방화벽이 포함되어 있습니다. 방화벽 제어 탭을 사용하여 그리드 네트워크, 관리자 네트워크 및 클라이언트 네트워크에서 기본적으로 열려 있는 포트를 열거나 닫을 수 있습니다. 닫힌 그리드 포트에 액세스할 수 있는 권한이 있는 IP 주소 목록을 만들 수도 있습니다. 클라이언트 네트워크를 사용하는 경우 노드가 클라이언트 네트워크의 인바운드 트래픽을 신뢰하는지 여부를 지정하고 클라이언트 네트워크의 특정 포트에 대한 액세스를 구성할 수 있습니다.

그리드 외부의 IP 주소에 열려 있는 포트 수를 절대적으로 필요한 포트로만 제한하면 그리드의 보안이 향상됩니다. 세 개의 방화벽 제어 탭 각각에서 설정을 사용하여 필요한 포트만 열도록 합니다.

예를 비롯한 방화벽 제어 사용에 대한 자세한 내용은 [을 참조하십시오 "방화벽 제어 관리"](#).

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 [을 "외부 방화벽에서 액세스를 제어합니다" 참조하십시오.](#)

방화벽 컨트롤에 액세스합니다

단계

1. 구성 > 보안 > *방화벽 제어*를 선택합니다.

이 페이지의 세 가지 탭은 예 "[방화벽 제어 관리](#)" 설명되어 있습니다.

2. 탭을 선택하여 방화벽 컨트롤을 구성합니다.

이러한 탭은 순서에 상관없이 사용할 수 있습니다. 한 탭에서 설정한 구성은 다른 탭에서 수행할 수 있는 작업을 제한하지 않지만 한 탭에서 변경한 구성은 다른 탭에 구성된 포트의 동작을 변경할 수 있습니다.

특별 권한 주소 목록

특별 권한 주소 목록 탭을 사용하여 외부 액세스 관리 탭의 설정에 따라 기본적으로 닫히거나 닫힌 포트에 대한 호스트 액세스 권한을 부여할 수 있습니다.

권한이 있는 IP 주소 및 서브넷에는 기본적으로 내부 그리드 액세스가 없습니다. 또한 외부 액세스 관리 탭에서 차단된 경우에도 권한이 있는 주소 목록 탭에서 열린 로드 밸런서 끝점과 추가 포트에 액세스할 수 있습니다.



권한이 있는 주소 목록 탭의 설정은 신뢰할 수 없는 클라이언트 네트워크 탭의 설정을 재정의할 수 없습니다.

단계

- 특별 권한 주소 목록 탭에서 닫힌 포트에 대한 액세스를 허용할 주소 또는 IP 서브넷을 입력합니다.
- 선택적으로 * CIDR 표기법 * 으로 다른 IP 주소 또는 서브넷 추가를 선택하여 권한이 있는 클라이언트를 추가합니다.



가능한 한 적은 수의 주소를 권한 있는 목록에 추가합니다.

- 선택적으로 * 권한이 있는 IP 주소가 StorageGRID 내부 포트에 액세스하도록 허용 * 을 선택합니다. 을 "[StorageGRID 내부 포트](#)" 참조하십시오.



이 옵션은 내부 서비스에 대한 일부 보호를 제거합니다. 가능한 경우 비활성화 상태로 됩니다.

- 저장 * 을 선택합니다.

외부 액세스를 관리합니다

외부 액세스 관리 탭에서 포트가 닫힌 경우 권한이 있는 주소 목록에 IP 주소를 추가하지 않으면 비 그리드 IP 주소로 포트에 액세스할 수 없습니다. 기본적으로 열려 있는 포트만 닫을 수 있으며 닫은 포트만 열 수 있습니다.



외부 액세스 관리 탭의 설정은 신뢰할 수 없는 클라이언트 네트워크 탭의 설정을 재정의할 수 없습니다. 예를 들어, 노드가 신뢰할 수 없는 경우 외부 액세스 관리 탭에 열려 있어도 클라이언트 네트워크에서 포트 SSH/22가 차단됩니다. 신뢰할 수 없는 클라이언트 네트워크 탭의 설정은 클라이언트 네트워크의 닫힌 포트(예: 443, 8443, 9443)를 재정의합니다.

단계

- 외부 액세스 관리 * 를 선택합니다. 이 탭에는 그리드의 노드에 대해 모든 외부 포트(기본적으로 비 그리드 노드가 액세스할 수 있는 포트)가 포함된 테이블이 표시됩니다.
- 다음 옵션을 사용하여 열고 닫을 포트를 구성합니다.

- 각 포트 옆의 토글을 사용하여 선택한 포트를 열거나 닫습니다.
- 표시된 모든 포트 열기 * 를 선택하여 표에 나열된 모든 포트를 엽니다.
- 표에 나열된 모든 포트를 닫으려면 * 표시된 모든 포트 닫기 * 를 선택합니다.



Grid Manager 포트 443 또는 8443을 닫으면 사용자를 포함하여 차단된 포트에 현재 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다.



테이블 오른쪽에 있는 스크롤 막대를 사용하여 사용 가능한 모든 포트를 확인합니다. 검색 필드를 사용하여 포트 번호를 입력하여 외부 포트의 설정을 찾습니다. 일부 포트 번호를 입력할 수 있습니다. 예를 들어 * 2 * 를 입력하면 이름에 문자열 "2"가 포함된 모든 포트가 표시됩니다.

3. 저장 * 을 선택합니다

신뢰할 수 없는 클라이언트 네트워크

노드의 클라이언트 네트워크를 신뢰할 수 없는 경우 노드는 로드 밸런서 끝점으로 구성된 포트의 인바운드 트래픽만 허용하고 선택적으로 이 탭에서 선택하는 추가 포트만 허용합니다. 이 탭을 사용하여 확장에 추가된 새 노드의 기본 설정을 지정할 수도 있습니다.



로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

신뢰할 수 없는 클라이언트 네트워크* 탭에서 변경한 구성은 * 외부 액세스 관리 * 탭의 설정보다 우선합니다.

단계

1. 신뢰할 수 없는 클라이언트 네트워크 * 를 선택합니다.
2. 새 노드 기본값 설정 섹션에서 확장 절차에서 그리드에 새 노드를 추가할 때 기본 설정을 지정합니다.

- * 신뢰 * (기본값): 확장 시 노드를 추가하면 해당 클라이언트 네트워크가 신뢰됩니다.
- * 신뢰할 수 없음 *: 확장 시 노드가 추가되면 해당 클라이언트 네트워크를 신뢰할 수 없습니다.

필요에 따라 이 탭으로 돌아가 특정 새 노드의 설정을 변경할 수 있습니다.



이 설정은 StorageGRID 시스템의 기존 노드에는 영향을 주지 않습니다.

3. 다음 옵션을 사용하여 명시적으로 구성된 로드 밸런싱 장치 엔드포인트 또는 추가 선택 포트에서만 클라이언트 연결을 허용할 노드를 선택합니다.
 - 표시된 노드에서 신뢰 해제 * 를 선택하여 테이블에 표시된 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가합니다.
 - 표시된 노드의 신뢰 * 를 선택하여 신뢰할 수 없는 클라이언트 네트워크 목록에서 표에 표시된 모든 노드를 제거합니다.
 - 각 노드 옆의 토글을 사용하여 선택한 노드에 대해 클라이언트 네트워크를 신뢰할 수 있는 또는 신뢰할 수 없는 것으로 설정합니다.

예를 들어 표시된 노드에서 * 언트러스트 * 를 선택하여 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가한 다음 개별 노드 옆의 토글을 사용하여 해당 단일 노드를 신뢰할 수 있는 클라이언트 네트워크

목록에 추가할 수 있습니다.



테이블 오른쪽에 있는 스크롤 막대를 사용하여 사용 가능한 모든 노드를 확인합니다. 검색 필드를 사용하여 노드 이름을 입력하여 노드 설정을 찾습니다. 부분 이름을 입력할 수 있습니다. 예를 들어 * GW * 를 입력하면 이름에 "GW" 문자열이 포함된 모든 노드가 표시됩니다.

4. 저장 * 을 선택합니다.

새 방화벽 설정이 즉시 적용되고 적용됩니다. 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

테넌트 관리

테넌트 계정이란 무엇입니까?

테넌트 계정을 사용하면 S3(Simple Storage Service) REST API를 사용하여 StorageGRID 시스템에 오브젝트를 저장하고 검색할 수 있습니다.



이 버전의 문서 사이트에서 Swift 세부 정보가 제거되었습니다. 을 ["StorageGRID 11.8: 테넌트 관리"](#) 참조하십시오.

그리드 관리자는 S3 클라이언트가 오브젝트를 저장하고 검색하는 데 사용하는 테넌트 계정을 만들고 관리합니다.

각 테넌트 계정에는 페더레이션 또는 로컬 그룹, 사용자, S3 버킷 및 오브젝트가 있습니다.

테넌트 계정은 저장된 객체를 다른 엔터티로 분리하는 데 사용할 수 있습니다. 예를 들어, 다음과 같은 사용 사례에서 여러 테넌트 계정을 사용할 수 있습니다.

- * 기업 활용 사례: * 엔터프라이즈 애플리케이션에서 StorageGRID 시스템을 관리하는 경우 조직의 여러 부서에서 그리드의 객체 스토리지를 분리할 수 있습니다. 이 경우 마케팅 부서, 고객 지원 부서, 인사 부서 등에 대한 테넌트 계정을 만들 수 있습니다.



S3 클라이언트 프로토콜을 사용하면 S3 버킷과 버킷 정책을 사용하여 기업 내 부서 간에 객체를 분리할 수 있습니다. 세입자 계정을 사용할 필요가 없습니다. 구현에 대한 지침을 참조하세요. ["S3 버킷 및 버킷 정책"](#) 자세한 내용은.

- * 서비스 공급자 활용 사례: * StorageGRID 시스템을 서비스 공급자로 관리하는 경우 그리드의 객체 스토리지를 그리드의 스토리지를 임대할 다른 엔터티로 분리할 수 있습니다. 이 경우 회사 A, 회사 B, 회사 C 등에 대한 테넌트 계정을 생성합니다.

자세한 내용은 을 ["테넌트 계정을 사용합니다"](#) 참조하십시오.

테넌트 계정은 어떻게 생성합니까?

그리드 관리자를 사용하여 테넌트 계정을 생성합니다. 테넌트 계정을 생성할 때 다음 정보를 지정합니다.

- 테넌트 이름, 클라이언트 유형(S3) 및 선택적 스토리지 할당량을 포함한 기본 정보입니다.
- 테넌트 계정에서 S3 플랫폼 서비스를 사용할 수 있는지 여부, 해당 ID 소스를 구성할 수 있는지 여부, S3 Select를 사용할 것인지, 그리드 페더레이션 연결을 사용할 수 있는지 여부 등의 테넌트 계정에 대한 사용 권한

- StorageGRID 시스템에서 로컬 그룹 및 사용자, ID 페더레이션 또는 SSO(Single Sign-On)를 사용하는지 여부에 따라 테넌트의 초기 루트 액세스입니다.

또한 S3 테넌트 계정이 규정 요구 사항을 준수해야 하는 경우 StorageGRID 시스템에 대해 S3 오브젝트 잠금 설정을 활성화할 수 있습니다. S3 오브젝트 잠금이 활성화된 경우 모든 S3 테넌트 계정에서 호환 버킷을 생성하고 관리할 수 있습니다.

테넌트 관리자는 무엇에 사용됩니까?

테넌트 계정을 생성한 후 테넌트 사용자는 테넌트 관리자에 로그인하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 페더레이션 설정(ID 소스가 그리드와 공유되지 않는 경우)
- 그룹 및 사용자를 관리합니다
- 계정 클론 및 교차 그리드 복제에 그리드 페더레이션을 사용합니다
- S3 액세스 키를 관리합니다
- S3 버킷을 생성하고 관리합니다
- S3 플랫폼 서비스 사용
- S3 Select를 사용합니다
- 스토리지 사용량을 모니터링합니다

 S3 테넌트 사용자는 테넌트 관리자를 사용하여 S3 액세스 키와 버킷을 생성하고 관리할 수 있지만, S3 클라이언트 애플리케이션을 사용하여 오브젝트를 수집 및 관리해야 합니다. 자세한 내용은 ["S3 REST API 사용"](#) 참조하십시오.

테넌트 계정을 생성합니다

StorageGRID 시스템의 스토리지에 대한 액세스를 제어하려면 하나 이상의 테넌트 계정을 생성해야 합니다.

테넌트 계정을 만드는 단계는 다음에 따라 다릅니다. ["ID 제휴"](#) 그리고 ["SSO\(Single Sign-On\)"](#) 구성되었는지 여부와 테넌트 계정을 만드는 데 사용하는 Grid Manager 계정이 루트 액세스 권한이 있는 관리자 그룹에 속하는지 여부입니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. ["지원되는 웹 브라우저"](#)
- 이 ["루트 액세스 또는 테넌트 계정 권한"](#) 있습니다.
- 테넌트 계정에서 Grid Manager에 대해 구성된 ID 소스를 사용하고 테넌트 계정에 대한 루트 액세스 권한을 통합 그룹에 부여하려는 경우 해당 통합 그룹을 Grid Manager로 가져온 것입니다. 이 관리 그룹에 그리드 관리자 권한을 할당할 필요가 없습니다. 을 ["관리 그룹을 관리합니다"](#) 참조하십시오.
- S3 테넌트가 계정 데이터를 복제하고 그리드 통합 연결을 사용하여 버킷 오브젝트를 다른 그리드에 복제하도록 허용하려면
 - 있습니다. ["그리드 페더레이션 연결을 구성했습니다"](#)
 - 연결 상태는 * 연결됨 * 입니다.
 - 루트 액세스 권한이 있습니다.

- 에 대한 고려 사항을 검토했습니다. "[그리드 페더레이션에 허용된 테넌트 관리](#)"
- 테넌트 계정에서 Grid Manager용으로 구성된 ID 소스를 사용할 경우 동일한 통합 그룹을 두 그리드의 Grid Manager로 가져왔습니다.

테넌트를 생성할 때 소스 및 대상 테넌트 계정에 대한 초기 루트 액세스 권한을 가지려면 이 그룹을 선택합니다.



이 관리 그룹이 테넌트를 생성하기 전에 두 그리드에 없는 경우 테넌트는 대상에 복제되지 않습니다.

마법사에 액세스합니다

단계

1. *세입자*를 선택하세요.
2. Create * 를 선택합니다.

세부 정보를 입력합니다

단계

1. 테넌트에 대한 세부 정보를 입력합니다.

필드에 입력합니다	설명
이름	테넌트 계정의 이름입니다. 테넌트 이름은 고유해야 할 필요가 없습니다. 테넌트 계정이 생성되면 고유한 20자리 계정 ID를 받습니다.
설명(선택 사항)	테넌트를 식별하는 데 도움이 되는 설명입니다. 그리드 페더레이션 연결을 사용할 테넌트를 생성하는 경우 이 필드를 사용하여 소스 테넌트인지 대상 테넌트인지 확인할 수 있습니다. 예를 들어 그리드 1에서 생성된 테넌트에 대한 이 설명은 그리드 2에 복제된 테넌트에 대해서도 나타납니다. "이 테넌트는 그리드 1에 생성되었습니다."
클라이언트 유형입니다	S3 * 여야 합니다.
스토리지 할당량(선택 사항)	이 테넌트에 스토리지 할당량을 사용하려면 할당량과 유닛에 대한 숫자 값입니다.

2. Continue * 를 선택합니다.

권한을 선택합니다

단계

1. 필요에 따라 이 테넌트에 부여할 기본 권한을 선택합니다.



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

권한	선택한 경우...
플랫폼 서비스를 허용합니다	테넌트는 CloudMirror와 같은 S3 플랫폼 서비스를 사용할 수 있습니다. 을 " S3 테넌트 계정에 대한 플랫폼 서비스 관리 " 참조하십시오.
고유 ID 소스를 사용합니다	테넌트는 연합된 그룹과 사용자에 대한 자체 ID 소스를 구성하고 관리할 수 있습니다. 이 옵션은 다음 경우 비활성화됩니다. " SSO를 구성했습니다 " StorageGRID 시스템용.
S3 선택 허용	테넌트는 오브젝트 데이터를 필터링하고 검색하기 위해 S3 SelectObjectContent API 요청을 실행할 수 있습니다. 을 " 관리 S3 테넌트 계정에 대해 선택 " 참조하십시오.
	<ul style="list-style-type: none"> 중요 *: SelectObjectContent 요청은 모든 S3 클라이언트 및 모든 테넌트의 로드 밸런서 성능을 감소시킬 수 있습니다. 신뢰할 수 있는 테넌트에만 필요한 경우에만 이 기능을 사용하도록 설정합니다.

2. 필요에 따라 이 테넌트에 부여할 고급 권한을 선택합니다.

권한	선택한 경우...
그리드 페더레이션 연결	<p>테넌트는 다음과 같은 그리드 페더레이션 연결을 사용할 수 있습니다.</p> <ul style="list-style-type: none"> 이 테넌트 및 계정에 추가된 모든 테넌트 그룹 및 사용자가 이 그리드(<i>source grid</i>)에서 선택한 연결의 다른 그리드(<i>destination grid</i>)로 복제되도록 합니다. 이 테넌트가 각 그리드의 해당 버킷 간에 교차 그리드 복제를 구성할 수 있도록 허용합니다. <p>을 "그리드 페더레이션을 위해 허용된 테넌트를 관리합니다" 참조하십시오.</p>
S3 오브젝트 잠금	<p>테넌트가 S3 오브젝트 잠금의 특정 기능을 사용하도록 허용:</p> <ul style="list-style-type: none"> * 최대 보존 기간 설정 * 이 버킷에 추가된 새 객체가 수집된 시점부터 유지되는 기간을 정의합니다. * Allow compliance mode * 는 사용자가 보존 기간 동안 보호된 객체 버전을 덮어쓰거나 삭제할 수 없도록 합니다.

3. Continue * 를 선택합니다.

루트 액세스를 정의하고 테넌트를 생성합니다

단계

- StorageGRID 시스템에서 ID 페더레이션, SSO(Single Sign-On) 또는 둘 다를 사용하는지 여부에 따라 테넌트 계정에 대한 루트 액세스를 정의합니다.

옵션을 선택합니다	이렇게 하십시오
ID 페더레이션이 활성화되지 않은 경우	테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.

옵션을 선택합니다	이렇게 하십시오
ID 페더레이션이 활성화된 경우	<p>a. 테넌트에 대한 루트 액세스 권한이 있는 기존 통합 그룹을 선택합니다.</p> <p>b. 필요에 따라 테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.</p>
ID 페더레이션 및 SSO(Single Sign-On)가 모두 활성화된 경우	테넌트에 대한 루트 액세스 권한이 있는 기존 통합 그룹을 선택합니다. 로컬 사용자는 로그인할 수 없습니다.

2. 테넌트 생성 * 을 선택합니다.

성공 메시지가 나타나고 새 테넌트가 테넌트 페이지에 나열됩니다. 테넌트 세부 정보를 보고 테넌트 활동을 모니터링하는 방법에 대한 자세한 내용은 [을 참조하십시오 "테넌트 작업을 모니터링합니다"](#).



네트워크 연결, 노드 상태 및 Cassandra 작업에 따라 그리드 전체에 테넌트 설정을 적용하는 데 15분 이상이 걸릴 수 있습니다.

3. 테넌트에 대해 * 그리드 페더레이션 연결 사용 * 권한을 선택한 경우:

- a. 동일한 테넌트가 연결의 다른 그리드에 복제되었는지 확인합니다. 두 그리드의 테넌트는 동일한 20자리 계정 ID, 이름, 설명, 할당량 및 권한을 갖습니다.



"Tenant created without a clone"이라는 오류 메시지가 나타나면 [의 지침을 참조하십시오 "그리드 통합 오류 문제 해결"](#).

- b. 복제된 테넌트에 대해 루트 액세스를 정의할 때 로컬 루트 사용자 암호를 제공한 경우 ["로컬 루트 사용자의 암호를 변경합니다"](#)



로컬 루트 사용자는 암호가 변경될 때까지 대상 그리드의 테넌트 관리자에 로그인할 수 없습니다.

테넌트에 로그인(선택 사항)

필요에 따라 새 테넌트에 지금 로그인하여 구성을 완료하거나 나중에 테넌트에 로그인할 수 있습니다. 로그인 단계는 기본 포트(443) 또는 제한된 포트를 사용하여 Grid Manager에 로그인했는지 여부에 따라 달라집니다. [을 "외부 방화벽에서 액세스를 제어합니다" 참조하십시오](#).

지금 로그인하십시오

사용 중인 경우...	수행할 작업...
포트 443을 사용하여 로컬 루트 사용자의 암호를 설정합니다	<p>1. root로 로그인 * 을 선택합니다. 로그인하면 버킷, ID 통합, 그룹 및 사용자를 구성하기 위한 링크가 나타납니다.</p> <p>2. 테넌트 계정을 구성할 링크를 선택합니다. 각 링크는 테넌트 관리자에서 해당 페이지를 엽니다. 페이지를 완료하려면 을 참조하십시오 "테넌트 계정 사용 지침".</p>
포트 443을 사용하고 로컬 루트 사용자의 암호를 설정하지 않았습니다	로그인 * 을 선택하고 루트 액세스 통합 그룹에 사용자의 자격 증명을 입력합니다.
제한된 포트	<p>1. 마침 * 을 선택합니다</p> <p>2. 테넌트 테이블에서 * 제한 * 을 선택하여 이 테넌트 계정에 액세스하는 방법에 대해 자세히 알아보십시오.</p> <p>테넌트 관리자의 URL 형식은 다음과 같습니다.</p> <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> <ul style="list-style-type: none"> ◦ FQDN or Admin Node IP 은 관리자 노드의 정규화된 도메인 이름 또는 IP 주소입니다 ◦ port 는 테넌트 전용 포트입니다 ◦ 20-digit-account-id 테넌트의 고유 계정 ID입니다

나중에 로그인하십시오

사용 중인 경우...	다음 중 하나를 수행합니다.
포트 443	<ul style="list-style-type: none"> • 그리드 관리자에서 *테넌트*를 선택하고 테넌트 이름 오른쪽에 있는 * Sign in*을 선택합니다. • 웹 브라우저에 테넌트의 URL을 입력합니다. <pre>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> <ul style="list-style-type: none"> ◦ FQDN or Admin Node IP 은 관리자 노드의 정규화된 도메인 이름 또는 IP 주소입니다 ◦ 20-digit-account-id 테넌트의 고유 계정 ID입니다

사용 중인 경우...	다음 중 하나를 수행합니다.
제한된 포트	<ul style="list-style-type: none"> 그리드 관리자에서 *테넌트*를 선택하고 *제한됨*을 선택합니다. 웹 브라우저에 테넌트의 URL을 입력합니다. <p><code>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</code></p> <ul style="list-style-type: none"> <i>FQDN_or_Admin_Node_IP</i>은 관리자 노드의 정규화된 도메인 이름 또는 IP 주소입니다 <i>port</i>는 테넌트 전용 제한된 포트입니다 <i>20-digit-account-id</i> 테넌트의 고유 계정 ID입니다

테넌트를 구성합니다

의 지침에 따라 "[테넌트 계정을 사용합니다](#)" 테넌트 그룹 및 사용자, S3 액세스 키, 버킷, 플랫폼 서비스, 계정 클론 및 그리드 간 복제를 관리합니다.

테넌트 계정을 편집합니다

테넌트 계정을 편집하여 표시 이름, 스토리지 할당량 또는 테넌트 권한을 변경할 수 있습니다.



테넌트에 * 그리드 페더레이션 연결 사용 * 권한이 있는 경우 연결의 각 그리드에서 테넌트 세부 정보를 편집할 수 있습니다. 그러나 연결의 한 그리드에서 변경한 내용은 다른 그리드로 복사되지 않습니다. 테넌트 세부 정보를 그리드 간에 정확하게 동기화하려면 두 그리드에 동일한 편집 작업을 수행합니다. 을 ["그리드 페더레이션 연결에 대해 하용된 테넌트를 관리합니다"](#) 참조하십시오.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. ["지원되는 웹 브라우저"](#)
- 이 ["루트 액세스 또는 테넌트 계정 권한"](#) 있습니다.



네트워크 연결, 노드 상태 및 Cassandra 작업에 따라 그리드 전체에 테넌트 설정을 적용하는 데 15분 이상이 걸릴 수 있습니다.

단계

- *세입자*를 선택하세요.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div style="width: 10%;">10%</div>	20.00 GB	100	→ Copy URL
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%;">85%</div>	100.00 GB	500	→ Copy URL
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%;">50%</div>	1.00 PB	10,000	→ Copy URL
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%;">95%</div>	500.00 TB	50,000	→ Copy URL
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	→ Copy URL

2. 편집할 테넌트 계정을 찾습니다.

검색 상자를 사용하여 이름 또는 테넌트 ID로 테넌트를 검색합니다.

3. 테넌트를 선택합니다. 다음 중 하나를 수행할 수 있습니다.

- 테넌트에 대한 확인란을 선택하고 * Actions * > * Edit * 를 선택합니다.
- 테넌트 이름을 선택하여 세부 정보 페이지를 표시하고 * Edit * 를 선택합니다.

4. 필요에 따라 다음 필드의 값을 변경합니다.

- * 이름 *
- * 설명 *
- * 스토리지 할당량 *

5. Continue * 를 선택합니다.

6. 테넌트 계정에 대한 권한을 선택하거나 지웁니다.

- 이미 사용 중인 테넌트에 대해 * 플랫폼 서비스 * 를 비활성화하면 해당 S3 버킷에 대해 구성된 서비스가 작동을 멈춥니다. 테넌트에 오류 메시지가 전송되지 않습니다. 예를 들어, 테넌트가 S3 버킷에 대해 CloudMirror 복제를 구성한 경우 버킷에 오브젝트를 저장할 수 있지만 해당 오브젝트의 복사본은 더 이상 엔드포인트로 구성된 외부 S3 버킷에서 생성할 수 없습니다. 을 ["S3 테넌트 계정에 대한 플랫폼 서비스 관리"](#)참조하십시오.
- 테넌트 계정에서 그리드 관리자를 위해 구성된 ID 소스 또는 고유한 ID 소스를 사용할지 여부를 결정하려면 * 고유한 ID 소스 사용 * 의 설정을 변경합니다.

고유한 ID 소스 사용 * 이 다음과 같은 경우:

- 비활성화되었으며 이 옵션을 선택하면 테넌트가 이미 자체 ID 소스를 사용하도록 설정되어 있습니다. 테넌트는 그리드 관리자에 대해 구성된 ID 소스를 사용하기 전에 해당 ID 소스를 비활성화해야 합니다.
- 비활성화되었으며 선택되지 않았습니다. StorageGRID 시스템에 대해 SSO가 활성화됩니다. 테넌트는 Grid Manager에 대해 구성된 ID 소스를 사용해야 합니다.
- 필요한 경우 * Allow S3 Select * (S3 선택 * 허용) 권한을 선택하거나 지웁니다. 을 ["관리 S3 테넌트 계정에](#)

대해 선택"참조하십시오.

- 그리드 페더레이션 연결 사용 * 권한을 제거하려면 다음을 수행합니다.
 - i. Grid Federation * 탭을 선택합니다.
 - ii. 권한 제거 * 를 선택합니다.
- 그리드 페더레이션 연결 사용 * 권한을 추가하려면
 - i. Grid Federation * 탭을 선택합니다.
 - ii. Use grid federation connection * 확인란을 선택합니다.
 - iii. 필요에 따라 * 기존 로컬 사용자 및 그룹 복제 * 를 선택하여 원격 그리드에 복제합니다. 필요한 경우 마지막 클론 작업이 완료된 후 일부 로컬 사용자 또는 그룹의 클론이 생성되지 않은 경우 클론 생성을 중지하거나 복제를 다시 시도할 수 있습니다.
- 최대 보존 기간을 설정하거나 규정 준수 모드를 허용하려면



이 설정을 사용하려면 먼저 그리드에서 S3 오브젝트 잠금을 활성화해야 합니다.

- i. S3 오브젝트 잠금 * 탭을 선택합니다.
- ii. Set maximum retention period * 에 값을 입력하고 풀다운 메뉴에서 기간을 선택합니다.
- iii. Allow compliance mode *에서 확인란을 선택합니다.

테넌트의 로컬 루트 사용자에 대한 암호를 변경합니다

루트 사용자가 계정에서 잠겨 있는 경우 테넌트의 로컬 루트 사용자의 암호를 변경해야 할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 있습니다. "[특정 액세스 권한](#)"

이 작업에 대해

StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 로컬 루트 사용자는 테넌트 계정에 로그인할 수 없습니다. 루트 사용자 작업을 수행하려면 사용자가 테넌트에 대한 루트 액세스 권한이 있는 통합 그룹에 속해야 합니다.

단계

1. *세입자*를 선택하세요.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div style="width: 10%;">10%</div>	20.00 GB	100	→ Copy URL
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%;">85%</div>	100.00 GB	500	→ Copy URL
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%;">50%</div>	1.00 PB	10,000	→ Copy URL
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%;">95%</div>	500.00 TB	50,000	→ Copy URL
<input type="checkbox"/>	Tenant 05	5.00 GB	—	—	500	→ Copy URL

2. 테넌트 계정을 선택합니다. 다음 중 하나를 수행할 수 있습니다.

- 테넌트 확인란을 선택하고 * 작업 * > * 루트 암호 변경 * 을 선택합니다.
- 세부 정보 페이지를 표시하려면 테넌트 이름을 선택하고 * 작업 * > * 루트 암호 변경 * 을 선택합니다.

3. 테넌트 계정의 새 암호를 입력합니다.

4. 저장 * 을 선택합니다.

테넌트 계정을 삭제합니다

테넌트의 시스템 액세스를 영구적으로 제거하려면 테넌트 계정을 삭제할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다.["지원되는 웹 브라우저"](#)
- 있습니다. ["특정 액세스 권한"](#)
- 테넌트 계정과 연결된 모든 S3 버킷 및 오브젝트를 제거했습니다.
- 테넌트가 그리드 페더레이션 연결을 사용하도록 허용된 경우에 대한 고려 사항을 검토했습니다. ["그리드 페더레이션 연결 사용 권한이 있는 테넌트 삭제"](#)

단계

1. *세입자*를 선택하세요.
2. 삭제할 테넌트 계정 또는 계정을 찾습니다.

검색 상자를 사용하여 이름 또는 테넌트 ID로 테넌트를 검색합니다.

3. 여러 테넌트를 삭제하려면 확인란을 선택하고 * Actions * > * Delete * 를 선택합니다.
4. 단일 테넌트를 삭제하려면 다음 중 하나를 수행합니다.
 - 확인란을 선택하고 * Actions * > * Delete * 를 선택합니다.

- 테넌트 이름을 선택하여 세부 정보 페이지를 표시한 다음 * 작업 * > * 삭제 * 를 선택합니다.
5. 예 * 를 선택합니다.

플랫폼 서비스 관리

플랫폼 서비스란 무엇입니까?

플랫폼 서비스에는 CloudMirror 복제, 이벤트 알림 및 검색 통합 서비스가 포함됩니다.

S3 테넌트 계정에 대해 플랫폼 서비스를 설정하는 경우 테넌트가 이러한 서비스를 사용하는 데 필요한 외부 리소스에 액세스할 수 있도록 그리드를 구성해야 합니다.

플랫폼 서비스는 지원되지 않습니다. ["가지 버킷"](#).

CloudMirror 복제

StorageGRID CloudMirror 복제 서비스는 StorageGRID 버킷에서 지정된 외부 대상으로 특정 오브젝트를 미러링하는데 사용됩니다.

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

CloudMirror 복제는 교차 그리드 복제 기능과 몇 가지 중요한 유사점과 차이점이 있습니다. 자세한 내용은 [을 참조하십시오"교차 그리드 복제와 CloudMirror 복제를 비교합니다"](#).



소스 버킷에 S3 개체 잠금이 활성화된 경우 CloudMirror 복제가 지원되지 않습니다.

알림

버킷별 이벤트 알림은 객체에서 수행된 특정 작업에 대한 알림을 지정된 외부 Kafka 클러스터, 웹훅 엔드포인트 또는 Amazon Simple Notification Service로 보내는 데 사용됩니다.

예를 들어, 버킷에 추가된 각 오브젝트에 대해 관리자에게 경고가 전송되도록 구성할 수 있습니다. 여기서 객체는 중요한 시스템 이벤트와 연결된 로그 파일을 나타냅니다.



S3 오브젝트 잠금이 활성화된 버킷에서 이벤트 알림을 구성할 수 있지만 오브젝트의 S3 오브젝트 잠금 메타데이터(마지막 보존 날짜 및 법적 보류 상태 포함)는 알림 메시지에 포함되지 않습니다.

검색 통합 서비스

검색 통합 서비스는 S3 오브젝트 메타데이터를 지정된 Elasticsearch 인덱스로 전송하는 데 사용되며, 여기에서 외부 서비스를 사용하여 메타데이터를 검색 또는 분석할 수 있습니다.

예를 들어, S3 오브젝트 메타데이터를 원격 Elasticsearch 서비스로 전송하도록 버킷을 구성할 수 있습니다. 그런 다음 Elasticsearch를 사용하여 버킷에 대한 검색을 수행하고 객체 메타데이터에 있는 패턴에 대한 정교한 분석을 수행할 수 있습니다.



S3 오브젝트 잠금이 활성화된 버킷에서 Elasticsearch 통합을 구성할 수 있지만 오브젝트의 S3 오브젝트 잠금 메타데이터(보존 기한 및 법적 보류 상태 포함)는 알림 메시지에 포함되지 않습니다.

플랫폼 서비스를 통해 테넌트는 외부 스토리지 리소스, 알림 서비스 및 데이터에 대한 검색 또는 분석 서비스를 사용할 수 있습니다. 플랫폼 서비스의 대상 위치는 일반적으로 StorageGRID 배포 외부에 있으므로 테넌트가 이러한 서비스를 사용하도록 허용할지 여부를 결정해야 합니다. 이 경우 테넌트 계정을 만들거나 편집할 때 플랫폼 서비스 사용을 활성화해야 합니다. 또한 테넌트가 생성하는 플랫폼 서비스 메시지가 대상에 도달할 수 있도록 네트워크를 구성해야 합니다.

플랫폼 서비스 사용을 위한 권장 사항

플랫폼 서비스를 사용하기 전에 다음 권장 사항을 숙지하십시오.

- StorageGRID 시스템의 S3 버킷에서 버전 관리 및 CloudMirror 복제가 모두 활성화된 경우 대상 엔드포인트에 대해 S3 버킷 버전 관리를 활성화해야 합니다. 이를 통해 CloudMirror 복제가 엔드포인트에 비슷한 개체 버전을 생성할 수 있습니다.
- CloudMirror 복제, 알림 및 검색 통합이 필요한 S3 요청이 있는 100개 이상의 활성 테넌트를 사용해서는 안 됩니다. 활성 테넌트가 100개 이상인 경우 S3 클라이언트 성능이 저하될 수 있습니다.
- 완료할 수 없는 엔드포인트에 대한 요청은 최대 500,000개의 요청에 대해 대기됩니다. 이 제한은 활성 테넌트 간에 동일하게 공유됩니다. 새 테넌트는 이 500,000개 제한을 일시적으로 초과할 수 있으므로 새로 생성된 테넌트가 불공평하게 처벌되지 않습니다.

관련 정보

- ["플랫폼 서비스 관리"](#)
- ["스토리지 프록시 설정을 구성합니다"](#)
- ["StorageGRID 모니터링"](#)

플랫폼 서비스를 위한 네트워크 및 포트

S3 테넌트가 플랫폼 서비스를 사용할 수 있도록 허용하는 경우 플랫폼 서비스 메시지가 대상으로 전달될 수 있도록 그리드에 대한 네트워킹을 구성해야 합니다.

테넌트 계정을 생성하거나 업데이트할 때 S3 테넌트 계정에 대해 플랫폼 서비스를 활성화할 수 있습니다. 플랫폼 서비스가 설정된 경우 테넌트는 CloudMirror 복제, 이벤트 알림 또는 S3 버킷에서 통합 메시지를 검색할 대상으로 사용되는 엔드포인트를 생성할 수 있습니다. 이러한 플랫폼 서비스 메시지는 ADC 서비스를 실행하는 스토리지 노드에서 대상 끝점으로 전송됩니다.

예를 들어, 테넌트는 다음과 같은 유형의 대상 엔드포인트를 구성할 수 있습니다.

- 로컬로 호스팅되는 Elasticsearch 클러스터입니다
- Amazon Simple Notification Service 메시지 수신을 지원하는 로컬 애플리케이션입니다
- 로컬에서 호스팅되는 Kafka 클러스터
- HTTP POST 알림 요청을 지원하는 외부 또는 로컬로 호스팅되는 웹훅 엔드포인트입니다.

이 엔드포인트는 Fluentd와 같은 다양한 웹 서버, 프레임워크 또는 데이터 처리 도구에서 호스팅될 수 있습니다.

- StorageGRID의 동일한 인스턴스 또는 다른 인스턴스에서 로컬로 호스팅되는 S3 버킷
- Amazon Web Services의 엔드포인트와 같은 외부 엔드포인트입니다.

플랫폼 서비스 메시지가 전달될 수 있도록 ADC 스토리지 노드가 포함된 네트워크를 구성해야 합니다. 다음 포트를 사용하여 플랫폼 서비스 메시지를 대상 끝점에 보낼 수 있는지 확인해야 합니다.

기본적으로 플랫폼 서비스 메시지는 다음 포트로 전송됩니다.

- **80**: http로 시작하는 끝점 URI(대부분의 끝점)용
- *443 *: https로 시작하는 끝점 URI(대부분의 끝점)
- * 9092 *: http 또는 https로 시작하는 엔드포인트 URI(Kafka 엔드포인트만 해당)

테넌트는 끝점을 만들거나 편집할 때 다른 포트를 지정할 수 있습니다.



StorageGRID 배포를 CloudMirror 복제의 대상으로 사용하는 경우 80 또는 443 이외의 포트에서 복제 메시지를 받을 수 있습니다. 대상 StorageGRID 배포에서 S3에 사용 중인 포트가 끝점에 지정되었는지 확인합니다.

투명하지 않은 프록시 서버를 사용하는 경우 인터넷의 끝점과 같은 외부 끝점으로 메시지를 보낼 수 있도록 허용해야 "[스토리지 프록시 설정을 구성합니다](#)"합니다.

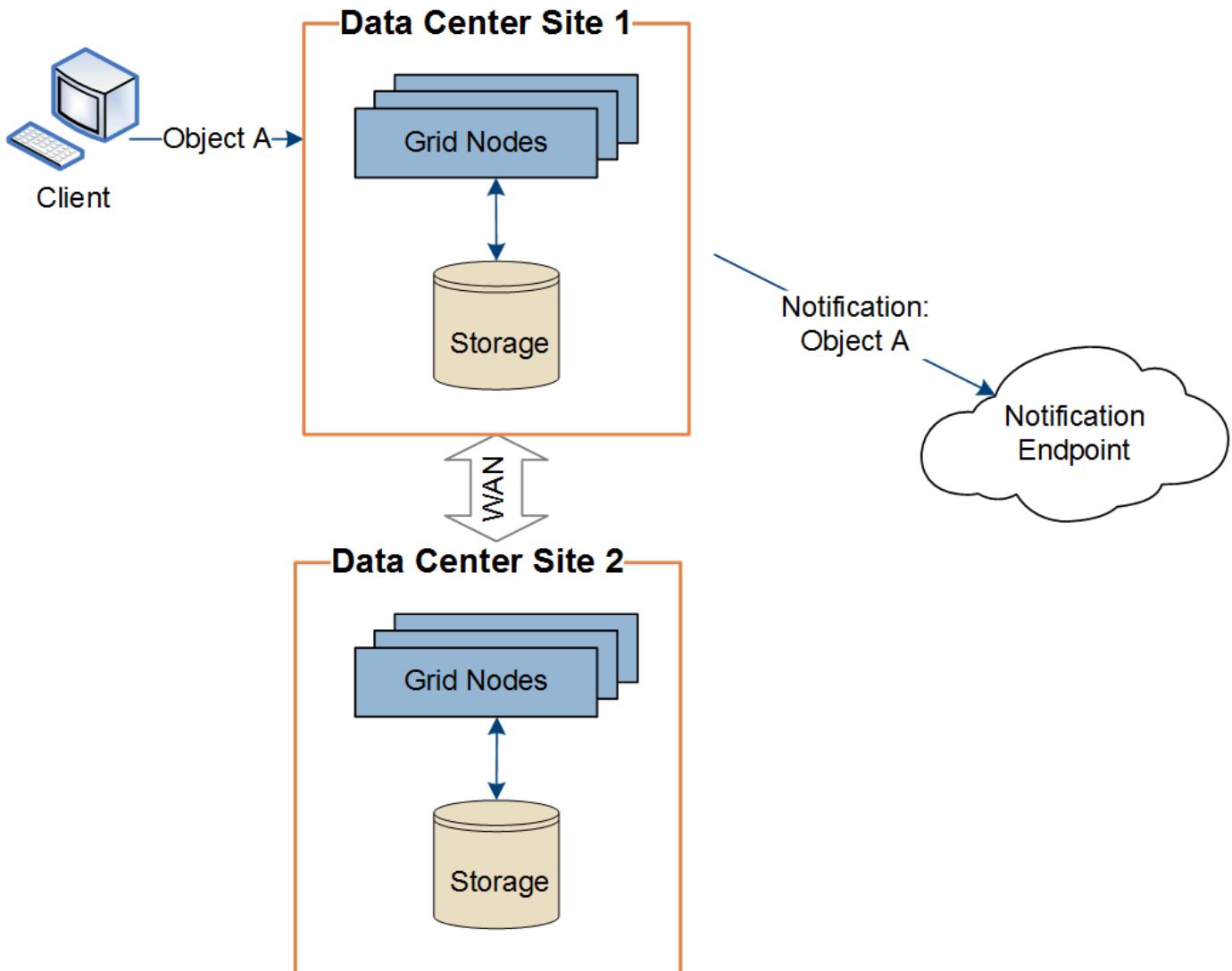
관련 정보

["테넌트 계정을 사용합니다"](#)

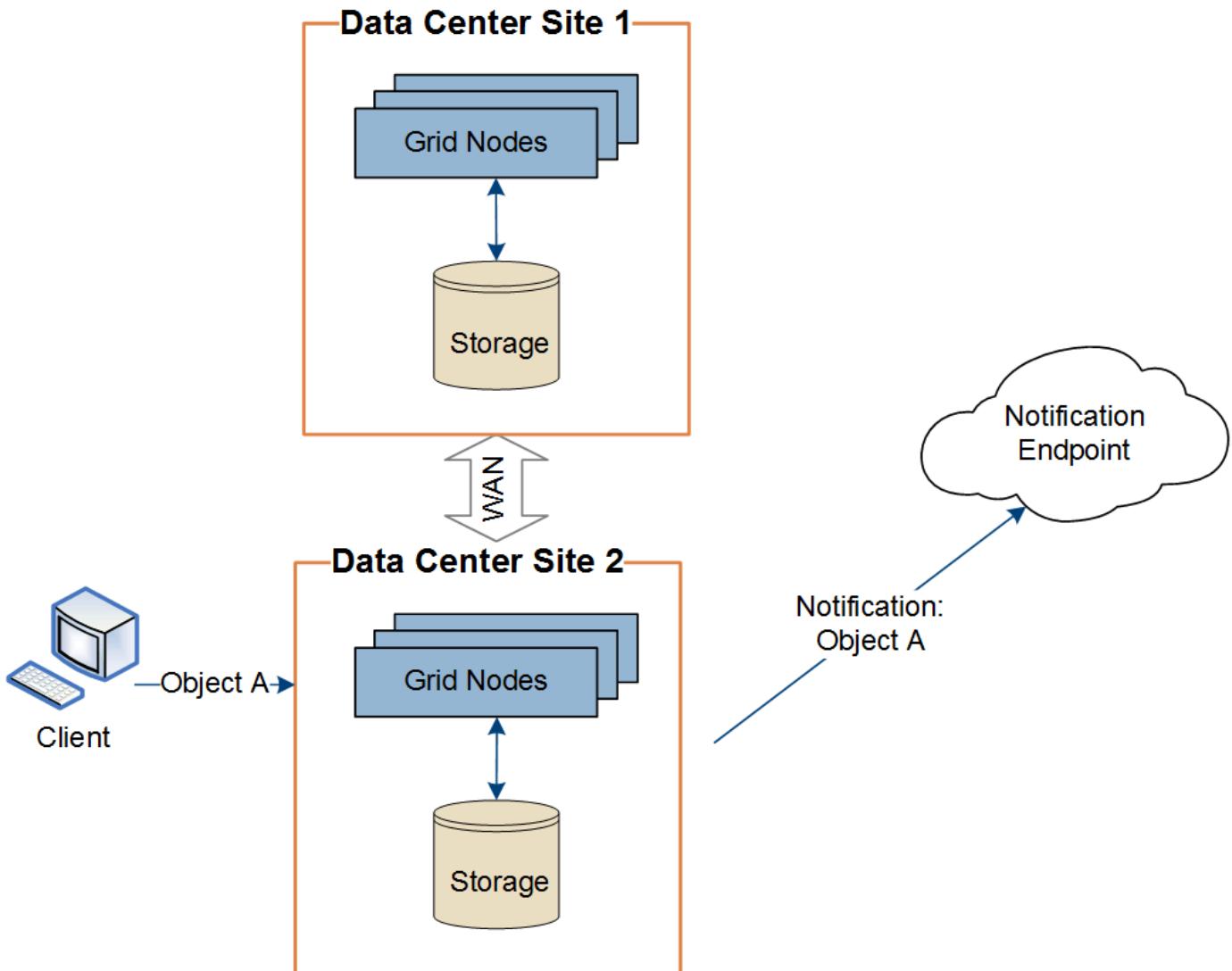
플랫폼 서비스 메시지를 사이트별로 전달

모든 플랫폼 서비스 작업은 사이트별로 수행됩니다.

즉, 테넌트가 클라이언트를 사용하여 데이터 센터 사이트 1의 게이트웨이 노드에 연결하여 오브젝트에 대해 S3 API 생성 작업을 수행하는 경우 해당 작업에 대한 알림이 트리거되고 데이터 센터 사이트 1에서 전송됩니다.



이후에 클라이언트가 데이터 센터 사이트 2에서 동일한 개체에 대해 S3 API 삭제 작업을 수행하면 삭제 작업에 대한 알림이 트리거되어 데이터 센터 사이트 2에서 전송됩니다.



각 사이트의 네트워킹이 플랫폼 서비스 메시지를 해당 대상에 전달할 수 있도록 구성되어 있는지 확인합니다.

플랫폼 서비스 문제 해결

플랫폼 서비스에 사용되는 엔드포인트는 테넌트 관리자의 테넌트 사용자가 생성 및 유지 관리합니다. 그러나 테넌트에 플랫폼 서비스를 구성하거나 사용하는 데 문제가 있는 경우 Grid Manager를 사용하여 문제를 해결할 수 있습니다.

새 끝점에 문제가 있습니다

테넌트가 플랫폼 서비스를 사용하려면 먼저 테넌트 관리자를 사용하여 하나 이상의 엔드포인트를 생성해야 합니다. 각 엔드포인트는 StorageGRID S3 버킷, Amazon Web Services 버킷, Amazon Simple Notification Service 주제, Kafka 주제 또는 로컬 또는 AWS에서 호스팅되는 Elasticsearch 클러스터와 같이 단일 플랫폼 서비스에 대한 외부 대상을 나타냅니다. 각 끝점에는 외부 리소스의 위치와 해당 리소스에 액세스하는 데 필요한 자격 증명이 모두 포함됩니다.

테넌트가 끝점을 만들 때 StorageGRID 시스템은 끝점이 있는지, 그리고 지정된 자격 증명을 사용하여 해당 끝점에 도달할 수 있는지 검증합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

끝점 유효성 검사에 실패하면 끝점 유효성 검사가 실패한 이유를 설명하는 오류 메시지가 표시됩니다. 테넌트 사용자가

문제를 해결한 다음 엔드포인트를 다시 생성해 보십시오.



테넌트 계정에 플랫폼 서비스가 활성화되어 있지 않으면 엔드포인트 생성이 실패합니다.

기존 엔드포인트에 문제가 있습니다

StorageGRID가 기존 끝점에 도달하려고 할 때 오류가 발생하면 테넌트 관리자의 대시보드에 메시지가 표시됩니다.



One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

테넌트 사용자는 끝점 페이지로 이동하여 각 끝점에 대한 가장 최근의 오류 메시지를 검토하고 오류가 발생한 시간을 확인할 수 있습니다. 마지막 오류 * 열은 각 끝점에 대한 가장 최근 오류 메시지를 표시하고 오류가 발생한 시간을 나타냅니다. 아이콘이 포함된 오류는 지난 7일 내에 발생했습니다.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.



One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints

[Create endpoint](#)

[Delete endpoint](#)

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-2	2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3	3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
<input type="checkbox"/>	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



마지막 오류 * 열에 있는 일부 오류 메시지에는 괄호 안에 로그 ID가 포함될 수 있습니다. 그리드 관리자 또는 기술 지원에서는 이 ID를 사용하여 `broadcast.log`의 오류에 대한 자세한 정보를 찾을 수 있습니다.

프록시 서버와 관련된 문제

구성한 경우 "스토리지 프록시" 스토리지 노드와 플랫폼 서비스 엔드포인트 사이에서 프록시 서비스가 StorageGRID 의 메시지를 허용하지 않으면 오류가 발생할 수 있습니다. 이러한 문제를 해결하려면 프록시 서버 설정을 확인하여 플랫폼 서비스 관련 메시지가 차단되지 않는지 확인하세요.

오류가 발생했는지 확인합니다

지난 7일 이내에 엔드포인트 오류가 발생한 경우 테넌트 관리자의 대시보드에 경고 메시지가 표시됩니다. 끝점 페이지로 이동하여 오류에 대한 자세한 정보를 볼 수 있습니다.

클라이언트 작업이 실패했습니다

일부 플랫폼 서비스 문제로 인해 S3 버킷의 클라이언트 작업이 실패할 수 있습니다. 예를 들어 RSM(Internal Replicated State Machine) 서비스가 중지되거나 너무 많은 플랫폼 서비스 메시지가 배달 대기 중인 경우 S3 클라이언트 작업이 실패합니다.

서비스 상태를 확인하려면

1. 노드 > 사이트 > 스토리지 노드 > *개요*를 선택합니다.
2. 알림 표에서 활성 알림을 확인하세요.
3. 모든 활성 알림을 해결합니다. 필요한 경우 기술 지원팀에 문의하세요.

복구할 수 없는 끝점 오류입니다

엔드포인트가 생성된 후 다양한 이유로 플랫폼 서비스 요청 오류가 발생할 수 있습니다. 일부 오류는 사용자 개입으로 복구할 수 있습니다. 예를 들어 다음과 같은 이유로 복구 가능한 오류가 발생할 수 있습니다.

- 사용자의 자격 증명이 삭제되었거나 만료되었습니다.
- 대상 버킷이 존재하지 않습니다.
- 알림을 전송할 수 없습니다.

StorageGRID에서 복구 가능한 오류가 발생하면 성공할 때까지 플랫폼 서비스 요청이 재시도됩니다.

다른 오류는 복구할 수 없습니다. 예를 들어, 다음과 같은 이유로 복구할 수 없는 오류가 발생할 수 있습니다.

- 엔드포인트가 삭제되었습니다.
- 웹후크 엔드포인트 대상은 알림 요청에 응답합니다. 400 Bad Request 오류.

StorageGRID에서 복구할 수 없는 끝점 오류가 발생하는 경우:

- Grid Manager에서 * 지원 * > * 툴 * > * 메트릭 * > * Grafana * > * 플랫폼 서비스 개요 *로 이동하여 오류 세부 정보를 확인하십시오.
- 테넌트 관리자에서 * 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 *로 이동하여 오류 세부 정보를 확인합니다.
- /var/local/log/bycast-err.log 관련된 오류가 있는지 확인합니다. ADC 서비스가 있는 스토리지 노드에는 이 로그 파일이 포함되어 있습니다.

플랫폼 서비스 메시지를 전달할 수 없습니다

대상에서 플랫폼 서비스 메시지를 수락하지 못하게 하는 문제가 발생하면 버킷에 대한 클라이언트 작업은 성공하지만 플랫폼 서비스 메시지는 전달되지 않습니다. 예를 들어, 대상에서 자격 증명이 업데이트되어 StorageGRID 더 이상 대상 서비스를 인증할 수 없는 경우 이 오류가 발생할 수 있습니다.

관련 경고를 확인합니다.

플랫폼 서비스 요청에 대한 성능 저하

요청이 전송되는 속도가 대상 엔드포인트에서 요청을 수신할 수 있는 속도를 초과하는 경우 StorageGRID 소프트웨어는 버킷에 대한 수신 S3 요청을 스로틀할 수 있습니다. 임계치 조절은 대상 끝점으로 보내려고 기다리는 요청의 백로그가 있는 경우에만 발생합니다.

단, 들어오는 S3 요청의 실행 시간이 더 오래 걸린다는 점을 알 수 있습니다. 속도가 현저히 느린 성능을 감지하기 시작하는 경우 수집 속도를 줄이거나 용량이 더 큰 엔드포인트를 사용해야 합니다. 요청 백로그가 계속 증가하는 경우 PUT 요청과 같은 클라이언트 S3 작업이 결국 실패합니다.

CloudMirror 요청은 일반적으로 검색 통합 또는 이벤트 알림 요청보다 더 많은 데이터 전송을 포함하므로 대상 엔드포인트의 성능에 영향을 받을 가능성이 더 높습니다.

플랫폼 서비스 요청에 실패했습니다

플랫폼 서비스에 대한 요청 실패율을 보려면

1. *노드*를 선택하세요.
2. _site * > * 플랫폼 서비스 * 를 선택합니다.
3. 요청 오류율 차트를 봅니다.

Network Storage Objects ILM Platform services Load balancer

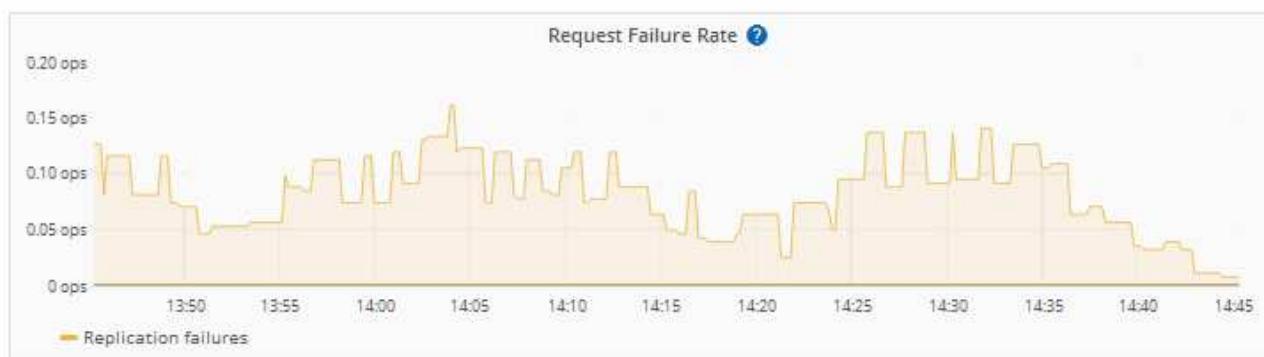
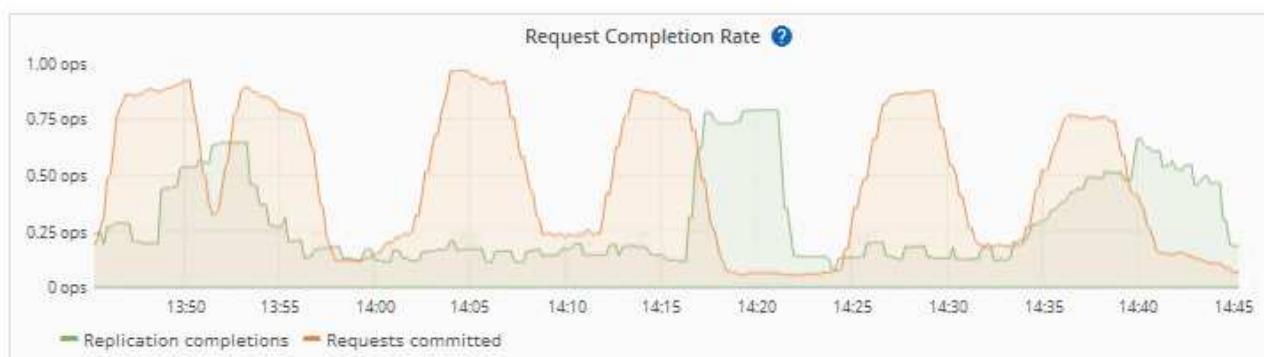
1 hour

1 day

1 week

1 month

Custom



플랫폼 서비스를 사용할 수 없음 경고

플랫폼 서비스 사용 불가 * 경고는 RSM 서비스가 실행 중이거나 사용 가능한 스토리지 노드가 너무 적어서 사이트에서 플랫폼 서비스 작업을 수행할 수 없음을 나타냅니다.

RSM 서비스는 플랫폼 서비스 요청이 각 끝점으로 전송되도록 합니다.

이 경고를 해결하려면 사이트에서 RSM 서비스를 포함하는 스토리지 노드를 확인합니다. (RSM 서비스는 ADC 서비스도 포함하는 스토리지 노드에 있습니다.) 그런 다음 이러한 스토리지 노드 중 일부만 실행되고 사용 가능한지 확인합니다.



사이트에서 RSM 서비스를 포함하는 스토리지 노드가 두 개 이상 장애가 발생하면 해당 사이트에 대한 보류 중인 플랫폼 서비스 요청이 손실됩니다.

플랫폼 서비스 끝점에 대한 추가 문제 해결 지침

자세한 내용은 ["테넌트 계정 및 GT 사용, 플랫폼 서비스 끝점 문제 해결"](#) 참조하십시오.

관련 정보

["StorageGRID 시스템 문제를 해결합니다"](#)

관리 **S3** 테넌트 계정에 대해 선택

특정 S3 테넌트가 S3 선택을 사용하여 개별 오브젝트에 SelectObjectContent 요청을 발급하도록 허용할 수 있습니다.

S3 Select를 사용하면 데이터베이스와 관련 리소스를 배치하지 않고도 대량의 데이터를 효율적으로 검색할 수 있습니다. 또한, 데이터를 검색하는 데 드는 비용과 대기 시간도 줄어듭니다.

S3 Select란 무엇입니까?

S3 Select를 사용하면 S3 클라이언트가 SelectObjectContent 요청을 사용하여 오브젝트에서 필요한 데이터만 필터링 및 검색할 수 있습니다. S3 Select의 StorageGRID 구현에는 S3 Select 명령 및 기능의 하위 집합이 포함됩니다.

S3 Select 사용에 대한 고려 사항 및 요구 사항

그리드 관리 요구 사항

그리드 관리자는 테넌트에 S3 Select 기능을 부여해야 합니다. 또는 를 선택하면 * Allow S3 Select * ["테넌트 생성"](#) ["테넌트 편집"](#)가 선택됩니다.

오브젝트 형식 요구사항

쿼리할 객체는 다음 형식 중 하나여야 합니다.

- CSV *. GZIP 또는 BZIP2 보관 파일로 압축하거나 그대로 사용할 수 있습니다.
- * 파케 *. Parquet 객체에 대한 추가 요구 사항:
 - S3 Select는 GZIP 또는 Snappy를 사용한 컬럼 압축만 지원합니다. S3 Select는 Parquet 오브젝트에 대한 전체 오브젝트 압축을 지원하지 않습니다.
 - S3 Select는 Parquet 출력을 지원하지 않습니다. 출력 형식을 CSV 또는 JSON으로 지정해야 합니다.
 - 압축되지 않은 최대 행 그룹 크기는 512MB입니다.
 - 개체의 스키마에 지정된 데이터 형식을 사용해야 합니다.
 - 간격, JSON, 목록, 시간 또는 UUID 논리적 유형은 사용할 수 없습니다.

엔드포인트 요구 사항

SelectObjectContent 요청을 보내야 ["StorageGRID 로드 밸런서 엔드포인트"](#)합니다.

끝점에서 사용하는 관리자 및 게이트웨이 노드는 다음 중 하나여야 합니다.

- 서비스 어플라이언스 노드입니다
- VMware 기반 소프트웨어 노드입니다
- cgroup v2가 활성화된 커널을 실행하는 베어 메탈 노드

일반 고려 사항

쿼리를 스토리지 노드로 직접 보낼 수 없습니다.



SelectObjectContent 요청은 모든 S3 클라이언트 및 모든 테넌트의 로드 밸런서 성능을 줄일 수 있습니다. 신뢰할 수 있는 테넌트에만 필요한 경우에만 이 기능을 사용하도록 설정합니다.

를 "[S3 Select 사용에 대한 지침](#)" 참조하십시오.

보려면 "[Grafana 차트](#)" S3 Select의 경우 시간 경과에 따른 작업을 확인하려면 그리드 관리자에서 지원 > 도구 > *메트릭*을 선택하세요.

클라이언트 연결을 구성합니다

S3 클라이언트 연결을 구성합니다

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



이 버전의 문서 사이트에서 Swift 세부 정보가 제거되었습니다. 을 "[StorageGRID 11.8: S3 및 Swift 클라이언트 연결 구성](#)" 참조하십시오.

구성 작업

1. 클라이언트 응용 프로그램이 StorageGRID에 연결되는 방법에 따라 StorageGRID에서 필수 작업을 수행합니다.

필수 작업

다음 정보를 얻어야 합니다.

- IP 주소
- 도메인 이름
- SSL 인증서

선택적 태스크입니다

필요에 따라 다음을 구성합니다.

- ID 제휴
- SSO

1. StorageGRID를 사용하여 응용 프로그램이 그리드에 연결하는 데 필요한 값을 얻습니다. S3 설정 마법사를 사용하거나 각 StorageGRID 엔터티를 수동으로 구성할 수 있습니다. 를 누릅니다

S3 설정 마법사를 사용합니다

S3 설정 마법사의 단계를 따릅니다.

수동으로 구성합니다

1. 고가용성 그룹을 생성합니다
2. 로드 밸런서 끝점을 만듭니다
3. 테넌트 계정을 생성합니다
4. 버킷 및 액세스 키를 생성합니다
5. ILM 규칙 및 정책을 구성합니다

1. S3 애플리케이션을 사용하여 StorageGRID에 대한 연결을 완료합니다. DNS 항목을 만들어 사용하려는 도메인 이름에 IP 주소를 연결합니다.

필요에 따라 추가 애플리케이션 설정을 수행합니다.

2. 애플리케이션 및 StorageGRID에서 지속적인 작업을 수행하여 시간에 따라 오브젝트 스토리지를 관리하고 모니터링합니다.

StorageGRID를 클라이언트 애플리케이션에 연결하는 데 필요한 정보입니다

StorageGRID를 S3 클라이언트 응용 프로그램에 연결하려면 먼저 StorageGRID에서 구성 단계를 수행하고 특정 값을 얻어야 합니다.

어떤 가치가 필요합니까?

다음 표에는 StorageGRID에서 구성해야 하는 값과 S3 응용 프로그램 및 DNS 서버에서 이러한 값을 사용하는 위치가 나와 있습니다.

값	값이 구성된 위치	값이 사용되는 위치
가상 IP(VIP) 주소입니다	StorageGRID > HA 그룹을 선택합니다	DNS 항목
포트	StorageGRID > 부하 분산 장치 끝점	클라이언트 응용 프로그램
SSL 인증서	StorageGRID > 부하 분산 장치 끝점	클라이언트 응용 프로그램
서버 이름(FQDN)	StorageGRID > 부하 분산 장치 끝점	<ul style="list-style-type: none">• 클라이언트 응용 프로그램• DNS 항목
S3 액세스 키 ID 및 비밀 액세스 키	StorageGRID > 테넌트 및 버킷	클라이언트 응용 프로그램
버킷/컨테이너 이름입니다	StorageGRID > 테넌트 및 버킷	클라이언트 응용 프로그램

이러한 값을 얻으려면 어떻게 해야 합니까?

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

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



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

- * 를 사용합니다 "[FabricPool 설정 마법사](#)". S3 설정 마법사와 마찬가지로 FabricPool 설정 마법사를 사용하면 필요한 값을 빠르게 구성하고ONTAP에서 FabricPool 클라우드 계층을 구성할 때 사용할 수 있는 파일을 출력할 수 있습니다.



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

- * 항목을 수동으로 구성 *. S3 응용 프로그램에 연결하는 경우 S3 설정 마법사를 사용하지 않으려면 수동으로 구성을 수행하여 필요한 값을 얻을 수 있습니다. 다음 단계를 수행하십시오.
 - S3 애플리케이션에 사용할 고가용성(HA) 그룹을 구성합니다. 을 "[고가용성 그룹을 구성합니다](#)"참조하십시오.
 - S3 애플리케이션에서 사용할 로드 밸런서 끝점을 생성합니다. 을 "[로드 밸런서 엔드포인트를 구성합니다](#)"참조하십시오.
 - S3 응용 프로그램에서 사용할 테넌트 계정을 만듭니다. 을 "[테넌트 계정을 생성합니다](#)"참조하십시오.
 - S3 테넌트의 경우 테넌트 계정에 로그인하고 응용 프로그램에 액세스할 각 사용자에 대한 액세스 키 ID 및 비밀 액세스 키를 생성합니다. 을 "[사용자 고유의 액세스 키를 생성합니다](#)"참조하십시오.
 - 테넌트 계정 내에 하나 이상의 S3 버킷을 생성합니다. S3의 경우 을 "[S3 버킷을 생성합니다](#)"참조하십시오.
 - 새 테넌트 또는 버킷/컨테이너에 속한 개체에 대한 특정 배치 지침을 추가하려면 새 ILM 규칙을 생성하고 해당 규칙을 사용하도록 새 ILM 정책을 활성화합니다. "[ILM 규칙을 생성합니다](#)"및 을 "[ILM 정책을 생성합니다](#)"참조하십시오.

S3 클라이언트에 대한 보안

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

요약

다음 목록에는 S3 REST API에 대해 보안이 구현되는 방식이 요약되어 있습니다.

연결 보안

TLS

서버 인증

시스템 CA에서 서명한 X.509 서버 인증서 또는 관리자가 제공한 사용자 지정 서버 인증서입니다

클라이언트 인증

S3 계정 액세스 키 ID 및 비밀 액세스 키

클라이언트 인증

버킷 소유권 및 모든 적용 가능한 액세스 제어 정책

StorageGRID가 클라이언트 응용 프로그램에 보안을 제공하는 방법

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

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

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

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

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

HTTPS가 기본값이며 권장됩니다.

HTTP는 보안이 약하고 암호화되지 않은 통신을 제공하지만 비운영 또는 테스트 그리드의 경우 선택적으로 사용할 수 ["활성화됨"](#) 있습니다.

- StorageGRID와 클라이언트 간의 통신은 TLS를 사용하여 암호화됩니다.
- 로드 밸런서 끝점이 HTTP 또는 HTTPS 연결을 허용하도록 구성되었는지 여부에 관계없이 그리드 내의 로드 밸런서 서비스와 스토리지 노드 간의 통신이 암호화됩니다.
- 클라이언트가 REST API 작업을 수행하려면 StorageGRID에 을 제공해야 ["HTTP 인증 헤더"](#)합니다.

보안 인증서 및 클라이언트 응용 프로그램

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

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

을 ["로드 균형 조정에 대한 고려 사항"](#)참조하십시오.

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

클라이언트가 TLS 연결을 설정하는 데 사용하는 인증서를 신뢰하도록 구성해야 합니다.

TLS 라이브러리에 대해 지원되는 해시 및 암호화 알고리즘

StorageGRID 시스템은 클라이언트 애플리케이션이 TLS 세션을 설정할 때 사용할 수 있는 일련의 암호 그룹을 지원합니다. 암호를 구성하려면 구성 > 보안 > *보안 설정*으로 이동하여 *TLS 및 SSH 정책*을 선택하세요.

지원되는 **TLS** 버전입니다

StorageGRID는 TLS 1.2 및 TLS 1.3을 지원합니다.



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

S3 설정 마법사를 사용합니다

S3 설정 마법사 고려 사항 및 요구 사항을 사용합니다

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

S3 설정 마법사를 사용하는 경우

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

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

마법사를 사용하기 전에

마법사를 사용하기 전에 이러한 사전 요구 사항을 완료했는지 확인합니다.

IP 주소를 얻고 **VLAN** 인터페이스를 설정합니다

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

가상 LAN을 사용하여 S3 애플리케이션의 트래픽을 분리할 계획이라면 이미 VLAN 인터페이스를 구성한 것입니다. 을 "[VLAN 인터페이스를 구성합니다](#)" 참조하십시오.

ID 페더레이션 및 **SSO**를 구성합니다

StorageGRID 시스템에 ID 페더레이션이나 SSO(Single Sign-On)를 사용하려는 경우 이러한 기능을 활성화해야 합니다. 또한 S3 애플리케이션이 사용할 테넌트 계정에 대해 루트 액세스 권한이 있는 페더레이션 그룹이 어느 것인지도 알고 있습니다. 보다 "[ID 페더레이션을 사용합니다](#)" 그리고 "[Single Sign-On 구성](#)".

도메인 이름 가져오기 및 구성

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

S3 가상 호스팅 방식의 요청을 사용하려는 경우 가 있어야 "[S3 끝점 도메인 이름을 구성했습니다](#)" 합니다. 가상 호스팅 방식의 요청을 사용하는 것이 좋습니다.

로드 밸런서 및 보안 인증서 요구 사항을 검토합니다

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

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

인증서가 있어야 합니다.

모든 그리드 페더레이션 연결을 구성합니다

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

- 있습니다. "[그리드 페더레이션 연결을 구성했습니다](#)"
- 연결 상태는 * 연결됨 * 입니다.
- 루트 액세스 권한이 있습니다.

S3 설정 마법사를 액세스하고 완료합니다

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

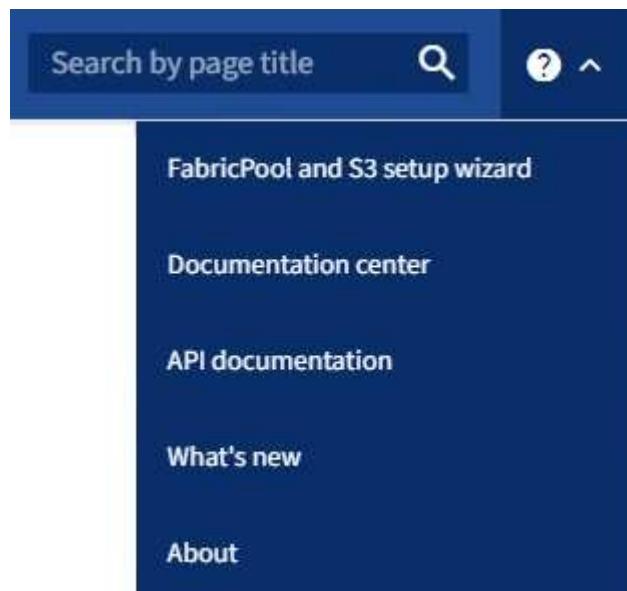
시작하기 전에

- 이 "[루트 액세스 권한](#)"입니다.
- 마법사 사용을 위해 을 검토했습니다."[고려 사항 및 요구 사항](#)"

마법사에 액세스합니다

단계

1. 을 사용하여 그리드 관리자에 "[지원되는 웹 브라우저](#)"로그인합니다.
2. 대시보드에 * FabricPool and S3 setup wizard * 배너가 나타나면 배너에서 링크를 선택합니다. 배너가 더 이상 나타나지 않으면 그리드 관리자의 머리글 표시줄에서 도움말 아이콘을 선택하고 * FabricPool and S3 setup wizard * 를 선택합니다.



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

단계 1/6: HA 그룹 구성

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

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

이 작업에 대한 자세한 내용은 ["고가용성 그룹을 관리합니다"](#) 참조하십시오.

단계

1. 외부 로드 밸런서를 사용할 계획이라면 HA 그룹을 생성할 필요가 없습니다. 이 단계 건너뛰기 *를 선택하고 로 이동합니다[6단계 중 2단계: 로드 밸런서 끝점을 구성합니다](#).
2. StorageGRID 로드 밸런서를 사용하려면 새 HA 그룹을 생성하거나 기존 HA 그룹을 사용할 수 있습니다.

HA 그룹을 생성합니다

- 새 HA 그룹을 생성하려면 * Create HA group * 을 선택합니다.
- Enter details * (세부 정보 입력) 단계에 대해 다음 필드를 작성합니다.

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

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

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

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

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

행을 드래그하여 * Priority order * 열의 값을 변경합니다.

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

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

- IP 주소 입력 * 단계에 대해 다음 필드를 입력합니다.

필드에 입력합니다	설명
서브넷 CIDR	CIDR 표기법 —의 VIP 서브넷 주소, IPv4 주소, 슬래시 및 서브넷 길이(0-32). 네트워크 주소에는 호스트 비트가 설정되어 있지 않아야 합니다. '192.16.0.0/22' 예를 들어,
게이트웨이 IP 주소(선택 사항)	StorageGRID 액세스에 사용되는 S3 IP 주소가 StorageGRID VIP 주소와 동일한 서브넷에 없는 경우 StorageGRID VIP 로컬 게이트웨이 IP 주소를 입력합니다. 로컬 게이트웨이 IP 주소는 VIP 서브넷 내에 있어야 합니다.

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

- f. HA 그룹 생성 * 을 선택한 다음 * 마침 * 을 선택하여 S3 설정 마법사로 돌아갑니다.
- g. 로드 밸런서 단계로 이동하려면 * 계속 * 을 선택합니다.

기존 HA 그룹 사용

- a. 기존 HA 그룹을 사용하려면 * HA 그룹 선택 *에서 HA 그룹 이름을 선택합니다.
- b. 로드 밸런서 단계로 이동하려면 * 계속 * 을 선택합니다.

6단계 중 2단계: 로드 밸런서 끝점을 구성합니다

StorageGRID는 로드 밸런서를 사용하여 클라이언트 애플리케이션에서 워크로드를 관리합니다. 로드 밸런싱은 여러 스토리지 노드에서 속도와 연결 용량을 극대화합니다.

모든 게이트웨이 및 관리 노드에 있는 StorageGRID 로드 밸런서 서비스를 사용하거나 외부(타사) 로드 밸런서에 연결할 수 있습니다. StorageGRID 로드 밸런서를 사용하는 것이 좋습니다.

이 작업에 대한 자세한 내용은 ["로드 균형 조정에 대한 고려 사항"](#) 참조하십시오.

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

끝점 작성

단계

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

필드에 입력합니다	설명
이름	끝점에 대한 설명 이름입니다.
포트	<p>로드 밸런싱에 사용할 StorageGRID 포트입니다. 이 필드는 처음 생성한 엔드포인트에 대해 기본적으로 10433으로 설정되지만 사용하지 않는 외부 포트는 입력할 수 있습니다. 80 또는 443을 입력하면 해당 포트가 관리 노드에 예약되기 때문에 끝점이 게이트웨이 노드에서만 구성됩니다.</p> <p>참고: 다른 그리드 서비스에서 사용하는 포트는 허용되지 않습니다. 보다 "StorageGRID 내부 포트".</p>
클라이언트 유형입니다	S3 * 여야 합니다.
네트워크 프로토콜	<p>HTTPS * 를 선택합니다.</p> <ul style="list-style-type: none">참고 *: TLS 암호화 없이 StorageGRID와 통신하는 것은 지원되지만 권장되지 않습니다.

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

모드를 선택합니다	설명
글로벌(기본값)	<p>클라이언트는 게이트웨이 노드 또는 관리 노드의 IP 주소, 네트워크에 있는 HA 그룹의 가상 IP(VIP) 주소 또는 해당 FQDN을 사용하여 끝점에 액세스할 수 있습니다.</p> <p>이 끝점의 접근성을 제한할 필요가 없는 경우 * Global * (글로벌 *) 설정(기본값)을 사용합니다.</p>
HA 그룹의 가상 IP입니다	<p>클라이언트는 HA 그룹의 가상 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다.</p> <p>이 바인딩 모드의 엔드포인트는 엔드포인트에 대해 선택한 HA 그룹이 겹치지 않는 한 모두 동일한 포트 번호를 사용할 수 있습니다.</p>
노드 인터페이스	클라이언트는 선택한 노드 인터페이스의 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다.

모드를 선택합니다	설명
노드 유형입니다	선택한 노드 유형에 따라 클라이언트는 관리 노드의 IP 주소(또는 해당 FQDN)나 게이트웨이 노드의 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다.

4. 테넌트 액세스 단계에서 다음 중 하나를 선택합니다.

필드에 입력합니다	설명
모든 테넌트 허용(기본값)	모든 테넌트 계정은 이 엔드포인트를 사용하여 해당 버킷에 액세스할 수 있습니다.
선택한 테넌트 허용	선택한 테넌트 계정만 이 끝점을 사용하여 해당 버킷을 액세스할 수 있습니다.
선택한 테넌트 차단	선택한 테넌트 계정은 이 끝점을 사용하여 해당 버킷을 액세스할 수 없습니다. 다른 모든 테넌트는 이 끝점을 사용할 수 있습니다.

5. 인증서 연결 * 단계에서 다음 중 하나를 선택합니다.

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

6. S3 설정 마법사로 돌아가려면 * 마침 * 을 선택합니다.

7. 테넌트 및 버킷 단계로 이동하려면 * 계속 * 을 선택합니다.



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

기존 로드 밸런서 끝점을 사용합니다

단계

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

외부 로드 밸런서를 사용합니다

단계

- 외부 로드 밸런서를 사용하려면 다음 필드를 완료합니다.

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

- 테넌트 및 버킷 단계로 이동하려면 * 계속 * 을 선택합니다.

6단계 중 3단계: 테넌트 및 버킷을 생성합니다

테넌트는 S3 애플리케이션을 사용하여 StorageGRID에 오브젝트를 저장하고 검색할 수 있는 엔터티입니다. 각 테넌트에는 자체 사용자, 액세스 키, 버킷, 오브젝트 및 특정 기능 세트가 있습니다.

버킷은 테넌트의 오브젝트 및 오브젝트 메타데이터를 저장하는 데 사용되는 컨테이너입니다. 테넌트에 버킷이 많을 수도 있지만 마법사를 사용하면 가장 빠르고 쉽게 테넌트와 버킷을 만들 수 있습니다. 나중에 버킷을 추가하거나 옵션을 설정해야 하는 경우 Tenant Manager를 사용할 수 있습니다.

이 작업에 대한 자세한 내용은 ["테넌트 계정을 생성합니다"](#) 및 ["S3 버킷을 생성합니다"](#)을 참조하십시오.

단계

- 테넌트 계정의 이름을 입력합니다.

- 테넌트 이름은 고유해야 할 필요가 없습니다. 테넌트 계정이 생성되면 고유한 숫자 계정 ID를 받습니다.
- StorageGRID 시스템에서 사용하는지 여부에 따라 테넌트 계정에 대한 루트 액세스를 정의합니다.["ID 제휴"](#), ["SSO\(Single Sign-On\)"](#), 또는 둘 다.

옵션을 선택합니다	이렇게 하십시오
ID 페더레이션이 활성화되지 않은 경우	테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.
ID 페더레이션이 활성화된 경우	<p>a. 테넌트에 대해 가질 기존 페더레이션 그룹을 "루트 액세스 권한" 선택합니다.</p> <p>b. 필요에 따라 테넌트에 로컬 루트 사용자로 로그인할 때 사용할 암호를 지정합니다.</p>
ID 페더레이션 및 SSO(Single Sign-On)가 모두 활성화된 경우	테넌트에 대해 가질 기존 페더레이션 그룹을 "루트 액세스 권한" 선택합니다. 로컬 사용자는 로그인할 수 없습니다.

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

테넌트의 유일한 사용자가 루트 사용자인 경우 이 옵션을 선택합니다. 다른 사용자가 이 테넌트를 사용할 경우 "Tenant Manager를 사용합니다" 키와 권한을 구성합니다.

4. 지금 이 테넌트에 대한 버킷을 생성하려면 * 이 테넌트에 대한 버킷 생성 * 을 선택합니다.



그리드에 S3 오브젝트 잠금이 활성화된 경우 이 단계에서 생성한 버킷에 S3 오브젝트 잠금이 활성화되지 않습니다. 이 S3 애플리케이션에 S3 오브젝트 잠금 버킷을 사용해야 하는 경우 지금 버킷을 생성하도록 선택하지 마십시오. 대신 나중에 테넌트 관리자를 "버킷을 생성합니다" 사용하십시오.

- S3 애플리케이션에서 사용할 버킷의 이름을 입력합니다. `s3-bucket` 예를 들어,

버킷을 생성한 후에는 버킷 이름을 변경할 수 없습니다.

- 이 버킷의 * 지역 * 을 선택합니다.

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

5. Create and continue * 를 선택합니다.

단계 4 / 6: 데이터 다운로드

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

단계

- 루트 사용자 S3 액세스 키 자동 생성 * 을 선택한 경우 다음 중 하나 또는 모두를 수행합니다.
 - 테넌트 계정 이름, 액세스 키 ID 및 비밀 액세스 키가 포함된 파일을 다운로드하려면 * 액세스 키 다운로드 * 를 선택합니다 .csv.
 - 복사 아이콘 (복사 아이콘)을 선택하여 액세스 키 ID 및 비밀 액세스 키를 클립보드에 복사합니다.
- 부하 분산 장치 끝점, 테넌트, 버킷 및 루트 사용자에 대한 설정이 포함된 파일을 다운로드하려면 * 구성 값 다운로드 * 를 선택합니다 .txt.
- 이 정보를 안전한 위치에 저장합니다.



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

4. 메시지가 나타나면 확인란을 선택하여 키를 다운로드하거나 복사했는지 확인합니다.

5. ILM 규칙 및 정책 단계로 이동하려면 * 계속 * 을 선택합니다.

단계 6 중 5: S3에 대한 ILM 규칙 및 ILM 정책을 검토합니다

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

단계

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

6단계 중 6단계: 요약 검토

단계

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

HA 그룹 관리

고가용성(HA) 그룹이란?

HA(고가용성) 그룹은 S3 클라이언트를 위한 고가용성 데이터 연결과 Grid Manager 및 Tenant Manager에 대한 고가용성 연결을 제공합니다.

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

각 HA 그룹은 선택한 노드의 공유 서비스에 대한 액세스를 제공합니다.

- 게이트웨이 노드, 관리 노드 또는 둘 모두를 포함하는 HA 그룹은 S3 클라이언트에 고가용성 데이터 연결을 제공합니다.
- 관리 노드만 포함하는 HA 그룹은 Grid Manager 및 테넌트 관리자에 대한 고가용성 연결을 제공합니다.
- 서비스 어플라이언스와 VMware 기반 소프트웨어 노드만 포함하는 HA 그룹은 용 고가용성 연결을 제공할 수 있습니다. "[S3 Select를 사용하는 S3 테넌트](#)" S3 Select를 사용할 때는 HA 그룹을 사용하는 것이 좋지만 반드시 필요한 것은 아닙니다.

HA 그룹을 어떻게 생성합니까?

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



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

2. 하나의 인터페이스를 기본 인터페이스로 지정합니다. Primary 인터페이스는 장애가 발생하지 않는 한 Active 인터페이스입니다.

- 모든 백업 인터페이스의 우선 순위 순서를 결정합니다.
- 그룹에 가상 IP(VIP) 주소를 10개까지 할당할 수 있습니다. 클라이언트 응용 프로그램은 이러한 VIP 주소를 사용하여 StorageGRID에 연결할 수 있습니다.

자세한 내용은 ["고가용성 그룹을 구성합니다"](#) 참조하십시오.

액티브 인터페이스란 무엇입니까?

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

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

노드의 현재 **HA** 그룹 상태를 봅니다

노드가 HA 그룹에 할당되었는지 확인하고 현재 상태를 확인하려면 노드 > *노드*를 선택하세요.

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

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

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

DC1-ADM1 (Primary Admin Node) 

Overview **Hardware** **Network** **Storage** **Load balancer** **Tasks**

Node information 

Name:	DC1-ADM1
Type:	Primary Admin Node
ID:	ce00d9c8-8a79-4742-bdef-c9c658db5315
Connection state:	 Connected
Software version:	11.6.0 (build 20211207.1804.614bc17)
HA groups:	Admin clients (Active) FabricPool clients (Backup)
IP addresses:	172.16.1.225 - eth0 (Grid Network) 10.224.1.225 - eth1 (Admin Network) 47.47.0.2, 47.47.1.225 - eth2 (Client Network)
Show additional IP addresses 	

활성 인터페이스가 실패하면 어떻게 됩니까?

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

페일오버는 다음과 같은 이유로 트리거될 수 있습니다.

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



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

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

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

HA 그룹은 어떻게 사용됩니까?

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

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

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

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

HA 그룹의 용도	이 유형의 노드를 HA 그룹에 추가합니다
Grid Manager에 액세스합니다	<ul style="list-style-type: none">• 기본 관리 노드(* 기본 *)• 운영 관리자 노드가 아닌 노드• 참고: * 기본 관리 노드는 기본 인터페이스여야 합니다. 일부 유지 보수 절차는 기본 관리 노드에서만 수행할 수 있습니다.
테넌트 관리자에 대한 액세스만 가능합니다	<ul style="list-style-type: none">• 운영 또는 비운영 관리 노드
S3 클라이언트 액세스—로드 밸런서 서비스	<ul style="list-style-type: none">• 관리자 노드• 게이트웨이 노드
에 대한 S3 클라이언트 액세스 " S3를 선택합니다 "	<ul style="list-style-type: none">• 서비스 어플라이언스• VMware 기반 소프트웨어 노드입니다• 참고 *: S3 Select를 사용할 때는 HA 그룹을 사용하는 것이 좋지만 반드시 필요한 것은 아닙니다.

Grid Manager 또는 Tenant Manager에 HA 그룹을 사용할 때의 제한 사항

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

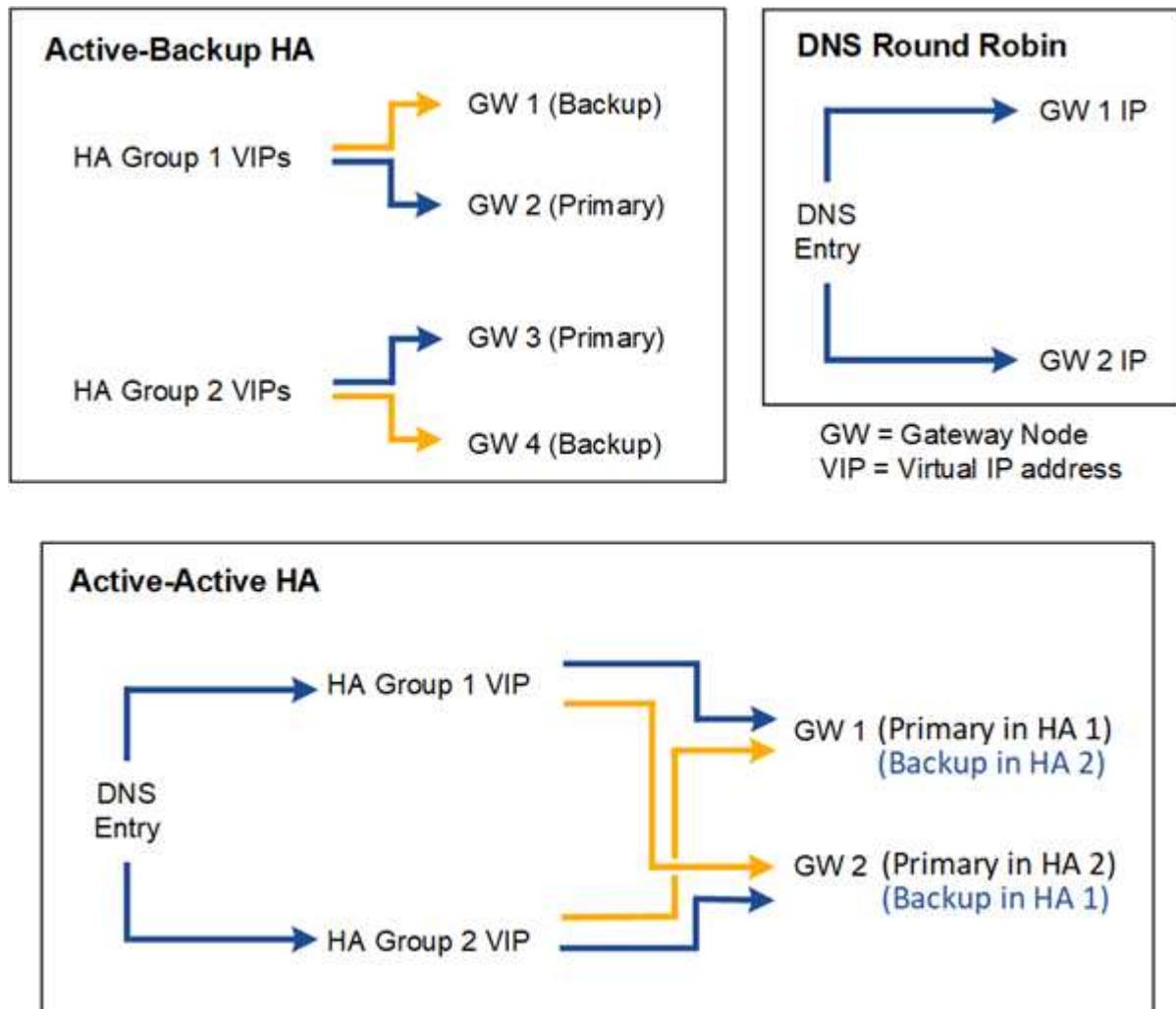
폐일오버가 발생했을 때 Grid Manager 또는 Tenant Manager에 로그인한 경우, 로그아웃되면 작업을 재개하려면 다시 로그인해야 합니다.

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

HA 그룹에 대한 구성 옵션

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

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



이 표에는 다이어그램에 표시된 각 HA 구성의 이점이 요약되어 있습니다.

구성	장점	단점
Active-Backup HA를 참조하십시오	<ul style="list-style-type: none"> 외부 종속성 없이 StorageGRID에서 관리 빠른 페일오버. 	<ul style="list-style-type: none"> HA 그룹에서 하나의 노드만 활성화됩니다. HA 그룹당 최소 하나의 노드가 유휴 상태가 됩니다.
DNS 라운드 로빈	<ul style="list-style-type: none"> 총 처리량 향상: 유휴 호스트가 없습니다. 	<ul style="list-style-type: none"> 느린 페일오버 - 클라이언트 동작에 따라 달라질 수 있습니다. StorageGRID 외부에서 하드웨어를 구성해야 합니다. 고객이 구현한 상태 점검이 필요합니다.

구성	장점	단점
액티브-액티브 HA	<ul style="list-style-type: none"> 트래픽이 여러 HA 그룹에 분산됩니다. HA 그룹 수에 따라 확장 가능한 높은 애그리게이트 처리량입니다. 빠른 폐일오버. 	<ul style="list-style-type: none"> 구성이 더 복잡합니다. StorageGRID 외부에서 하드웨어를 구성해야 합니다. 고객이 구현한 상태 점검이 필요합니다.

고가용성 그룹을 구성합니다

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



StorageGRID 시스템은 최대 255개의 HA 그룹을 가질 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 이 "[루트 액세스 권한](#)"입니다.
- HA 그룹에서 VLAN 인터페이스를 사용하려는 경우 VLAN 인터페이스를 만들었습니다. 을 "[VLAN 인터페이스를 구성합니다](#)" 참조하십시오.
- HA 그룹의 노드에 액세스 인터페이스를 사용하려는 경우 인터페이스를 생성했습니다.
 - Linux**(노드 설치 전): "[노드 구성 파일을 생성합니다](#)"
 - 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 배포를 의미합니다. 지원되는 버전 목록은 다음을 참조하세요. "[NetApp 상호 운용성 매트릭스 툴\(IMT\)](#)" .

고가용성 그룹을 생성합니다

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

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

마법사에 액세스합니다

단계

- 구성 > 네트워크 > *고가용성 그룹*을 선택합니다.
- Create * 를 선택합니다.

HA 그룹에 대한 세부 정보를 입력합니다

단계

1. HA 그룹에 고유한 이름을 제공하십시오.
2. 필요에 따라 HA 그룹에 대한 설명을 입력합니다.
3. Continue * 를 선택합니다.

HA 그룹에 인터페이스를 추가합니다

단계

1. 이 HA 그룹에 추가할 인터페이스를 하나 이상 선택하십시오.

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

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

<input type="text" value="Search..."/>		Total interface count: 4		
Node	Interface	Site	IPv4 subnet	Node type
<input type="checkbox"/> DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
<input type="checkbox"/> DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
<input type="checkbox"/> DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
<input type="checkbox"/> DC2-ADM1-104-103	eth2	DC2	—	Admin Node

0 interfaces selected

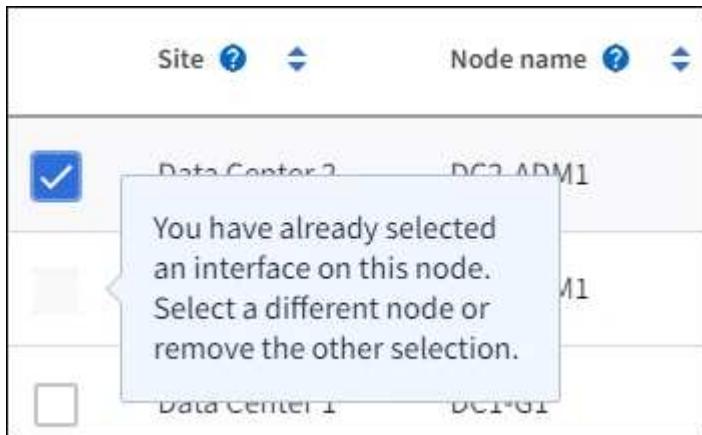


VLAN 인터페이스를 생성한 후 새 인터페이스가 테이블에 나타날 때까지 최대 5분 정도 기다립니다.

인터넷페이스 선택을 위한 지침

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

- 인터페이스를 선택할 수 없는 경우 해당 확인란이 비활성화됩니다. 자세한 내용은 툴 팁을 참조하십시오.



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

2. Continue * 를 선택합니다.

우선 순위 순서를 결정합니다

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

단계

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

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

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order ?	Node	Interface ?	Node type ?
1 (Primary interface)	DC1-ADM1-104-96	eth2	Primary Admin Node
2	DC2-ADM1-104-103	eth2	Admin Node



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

2. Continue * 를 선택합니다.

IP 주소를 입력합니다

단계

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

네트워크 주소에는 호스트 비트가 설정되어 있지 않아야 합니다. `192.16.0.0/22` 예를 들어,



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

Enter details for the HA group

Subnet CIDR ?

Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

Gateway IP address (optional) ?

Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

Virtual IP address ?

Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

1.2.3.4

[Add another IP address](#)

- 원하는 경우 S3 관리 또는 테넌트 클라이언트가 다른 서브넷에서 이러한 VIP 주소에 액세스하는 경우 * 게이트웨이 IP 주소 * 를 입력합니다. 게이트웨이 주소는 VIP 서브넷 내에 있어야 합니다.

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

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

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

- HA 그룹 생성 * 을 선택하고 * 마침 * 을 선택합니다.

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

다음 단계

이 HA 그룹을 로드 밸런싱에 사용하려면 로드 밸런서 엔드포인트를 생성하여 포트 및 네트워크 프로토콜을 결정하고

필요한 인증서를 연결합니다. 을 "[로드 밸런서 엔드포인트를 구성합니다](#)" 참조하십시오.

High Availability 그룹을 편집합니다

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

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

단계

1. 구성 > 네트워크 > *고가용성 그룹*을 선택합니다.

고가용성 그룹 페이지에는 기존의 모든 HA 그룹이 표시됩니다.

2. 편집할 HA 그룹의 확인란을 선택합니다.
3. 업데이트할 항목을 기준으로 다음 중 하나를 실행합니다.

- VIP 주소를 추가하거나 제거하려면 * Actions * > * Edit virtual IP address * 를 선택합니다.
- 작업 * > * HA 그룹 편집 * 을 선택하여 그룹의 이름 또는 설명을 업데이트하거나, 인터페이스를 추가 또는 제거하거나, 우선 순위 순서를 변경하거나, VIP 주소를 추가 또는 제거합니다.

4. Edit virtual IP address * 를 선택한 경우:

- a. HA 그룹의 가상 IP 주소를 업데이트합니다.
- b. 저장 * 을 선택합니다.
- c. 마침 * 을 선택합니다.

5. HA 그룹 편집 * 을 선택한 경우:

- a. 필요에 따라 그룹의 이름 또는 설명을 업데이트합니다.
- b. 선택적으로 확인란을 선택하거나 선택 취소하여 인터페이스를 추가하거나 제거합니다.



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

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

High Availability 그룹을 제거합니다

HA(고가용성) 그룹을 한 번에 하나 이상 제거할 수 있습니다.



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

클라이언트 중단을 방지하려면 HA 그룹을 제거하기 전에 영향을 받는 S3 클라이언트 애플리케이션을 모두 업데이트하십시오. 다른 IP 주소(예: 다른 HA 그룹의 가상 IP 주소 또는 설치 중 인터페이스에 대해 구성된 IP 주소)를

사용하여 연결할 각 클라이언트를 업데이트합니다.

단계

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

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

로드 밸런싱 관리

로드 균형 조정에 대한 고려 사항

로드 밸런싱을 사용하여 S3 클라이언트에서 수집 및 검색 워크로드를 처리할 수 있습니다.

로드 밸런싱이란 무엇입니까?

클라이언트 애플리케이션이 StorageGRID 시스템에서 데이터를 저장하거나 검색할 때 StorageGRID는 로드 밸런서를 사용하여 수집 및 검색 워크로드를 관리합니다. 로드 밸런싱은 여러 스토리지 노드에 워크로드를 분산하여 속도와 연결 용량을 극대화합니다.

StorageGRID 로드 밸런서 서비스는 모든 관리 노드 및 모든 게이트웨이 노드에 설치되며 계층 7 로드 밸런싱을 제공합니다. 클라이언트 요청에 대한 TLS(Transport Layer Security) 종료를 수행하고 요청을 검사하며 스토리지 노드에 대한 새로운 보안 연결을 설정합니다.

각 노드의 로드 밸런서 서비스는 클라이언트 트래픽을 스토리지 노드로 전달할 때 독립적으로 작동합니다. 로드 밸런서 서비스는 가중 프로세스를 통해 더 많은 요청을 CPU 사용성이 높은 스토리지 노드로 라우팅합니다.



StorageGRID 로드 밸런서 서비스가 권장되는 로드 밸런싱 메커니즘이기는 하지만 대신 타사 로드 밸런서를 통합하는 것이 좋을 수도 있습니다. 자세한 내용은 NetApp 계정 담당자에게 문의하거나 다음을 참조하세요. "[StorageGRID 와 함께 타사 로드 밸런서를 사용하세요](#)".

몇 개의 로드 밸런싱 노드가 필요합니까?

일반적으로 StorageGRID 시스템의 각 사이트에는 부하 분산 서비스가 있는 두 개 이상의 노드가 포함되어야 합니다. 예를 들어 사이트에는 두 개의 게이트웨이 노드 또는 관리 노드와 게이트웨이 노드가 모두 포함될 수 있습니다. 서비스 어플라이언스, 베어 메탈 노드 또는 가상 머신(VM) 기반 노드를 사용하는지에 관계없이 각 로드 밸런싱 노드에 적절한 네트워킹, 하드웨어 또는 가상화 인프라가 있어야 합니다.

로드 밸런서 엔드포인트란 무엇입니까?

로드 밸런서 끝점은 들어오는 클라이언트 응용 프로그램 요청과 나가는 클라이언트 응용 프로그램이 로드 밸런서 서비스를 포함하는 노드에 액세스하는 데 사용할 포트 및 네트워크 프로토콜(HTTPS 또는 HTTP)을 정의합니다. 또한 엔드포인트는 클라이언트 유형(S3), 바인딩 모드 및 허용되는 테넌트 또는 차단된 테넌트 목록을 정의합니다.

로드 밸런서 엔드포인트를 생성하려면 Grid Manager를 사용하거나 S3 설정 및 FabricPool 마법사를 완료하세요.

- ["로드 밸런서 엔드포인트를 구성합니다"](#)
- ["S3 설정 마법사를 사용합니다"](#)
- ["FabricPool 설정 마법사를 사용합니다"](#)

로드 밸런서 캐싱에 대한 고려 사항

작업 부하가 데이터의 하위 집합에서 작동하고 개체에 여러 번 액세스할 때 캐싱을 사용하면 성능이 크게 향상됩니다. 또한 캐싱은 전체 그리드 배포 없이도 개체 스토리지에 대한 원격 액세스를 제공합니다. 로드 밸런서 캐싱은 게이트웨이 노드에서만 사용할 수 있습니다.

로드 밸런서 엔드포인트를 생성할 때:

- 캐시 가능한 작업에 대해서만 캐싱을 활성화합니다. 캐시된 데이터보다 캐시되지 않은 데이터에 더 자주 액세스하는 워크로드는 캐시에서 서비스되지 않는 경우보다 성능이 떨어집니다. 어떤 경우에는 덮어쓰기 및 제거 비율이 높은 작업 부하가 보증된 드라이브 쓰기 내구성을 초과할 수도 있습니다.
- 캐싱에 적합한 개별 워크로드를 캐싱하기 위해 추가 엔드포인트나 노드를 추가하는 것을 고려하세요.
- 캐시 가능한 워크로드와 캐시 불가능한 워크로드에 대해 서로 다른 엔드포인트를 사용합니다. 이러한 분리를 통해 캐싱 메커니즘이 적절하게 적용되고 캐시할 수 없는 데이터 처리를 방해하지 않습니다.
- 캐시가 가능한 잠재적인 작업 부하를 캐시가 활성화된 엔드포인트로 전달하여 평가합니다. 캐싱에 대한 워크로드의 적합성을 판단하기 위해 캐시 적중률을 모니터링하고 검증합니다. 이러한 평가는 성능을 최적화하고 캐시 리소스의 효율적인 사용을 보장하는 데 도움이 됩니다.
- ["감사 로그를 검토합니다"](#)기준 작업 부하가 캐싱에 적합한지 여부를 확인합니다. 주어진 기간 동안 GET 중 고유한 객체에 대한 비율이 얼마인지 확인합니다. 캐싱에 적합하려면 이 값이 50% 미만이어야 합니다.

캐싱에 적합한 후보가 될 수 있는 작업 부하의 예

- 데이터 레이크
- 고성능 컴퓨팅(HPC)
- AI/ML 훈련
- 콘텐츠 배포 네트워크(CDN)
- 미디어 자산 관리
- 영상 제작

- 여러 개의 객체 버전을 캐시할 수 있습니다.
- 범위 읽기 작업이 지원됩니다.



캐싱에 적합하지 않은 작업 부하의 예

- 패브릭 풀
- 백업 애플리케이션
- 스토리지 계층화



캐시에서 제공하는 콘텐츠에 저장 중 암호화가 필요한 경우 "[노드 또는 드라이브 암호화 활성화](#)" 캐시 노드에서.

캐시되지 않는 객체 및 요청 유형

- 그만큼 response-content-encoding 쿼리 매개변수
- 그만큼 partNumber 쿼리 매개변수
- 조건부 헤더
 - If-Match
 - If-Modified-Since
 - If-None-Match
 - If-Unmodified-Since
- 다음 중 하나로 암호화된 요청:
 - SSE(StorageGRID 관리 키를 사용한 서버 측 암호화)
 - SSE-C(고객 제공 키를 사용한 서버 측 암호화)
 - 저장된 오브젝트 암호화

캐시되지 않은 모든 요청은 캐시가 활성화되지 않은 것처럼 업스트림 LDR로 전달됩니다.

관련 정보

- "[로드 밸런서 캐싱 문제 해결](#)"
- 로드 밸런서 캐싱에 대한 자세한 내용은 기술 지원팀에 문의하세요.

포트에 대한 고려 사항

로드 밸런서 끝점의 포트는 사용자가 만든 첫 번째 끝점의 경우 기본적으로 10433으로 설정되지만 사용하지 않는 외부 포트는 1에서 65535 사이로 지정할 수 있습니다. 포트 80 또는 443을 사용하는 경우 엔드포인트는 게이트웨이 노드에서만 로드 밸런서 서비스를 사용합니다. 이러한 포트는 관리 노드에 예약되어 있습니다. 두 개 이상의 끝점에 동일한 포트를 사용하는 경우 각 끝점에 대해 다른 바인딩 모드를 지정해야 합니다.

다른 그리드 서비스에서 사용하는 포트는 허용되지 않습니다. 보다 "[StorageGRID 내부 포트](#)".

네트워크 프로토콜에 대한 고려 사항

대부분의 경우 클라이언트 응용 프로그램과 StorageGRID 간의 연결은 TLS(전송 계층 보안) 암호화를 사용해야 합니다. TLS 암호화 없이 StorageGRID에 연결하는 것은 지원되지만 특히 프로덕션 환경에서는 권장되지 않습니다. StorageGRID 로드 밸런서 끝점에 대한 네트워크 프로토콜을 선택할 때 * HTTPS *를 선택해야 합니다.

로드 밸런서 끝점 인증서에 대한 고려 사항

로드 밸런서 끝점의 네트워크 프로토콜로 * HTTPS * 를 선택한 경우 보안 인증서를 제공해야 합니다. 로드 밸런서 끝점을 만들 때 다음 세 가지 옵션 중 하나를 사용할 수 있습니다.

- * 서명된 인증서 업로드(권장) *. 이 인증서는 공개적으로 신뢰할 수 있거나 개인 인증 기관(CA)에서 서명할 수 있습니다. 공개적으로 신뢰할 수 있는 CA 서버 인증서를 사용하여 연결을 보호하는 것이 가장 좋습니다. 생성된 인증서와 달리 CA에서 서명한 인증서는 중단 없이 회전할 수 있으므로 만료 문제를 방지하는 데 도움이 됩니다.

로드 밸런서 끝점을 만들기 전에 다음 파일을 얻어야 합니다.

- 사용자 지정 서버 인증서 파일입니다.
 - 사용자 지정 서버 인증서 개인 키 파일입니다.
 - 선택적으로 각 중간 발급 인증 기관의 인증서 CA 번들.
- * 자체 서명된 인증서 생성 *.
 - * 글로벌 StorageGRID S3 인증서를 사용하십시오 *. 로드 밸런서 끝점에 대해 인증서를 선택하려면 먼저 이 인증서의 사용자 지정 버전을 업로드하거나 생성해야 합니다. 을 "[S3 API 인증서를 구성합니다](#)" 참조하십시오.

어떤 가치가 필요합니까?

인증서를 만들려면 S3 클라이언트 응용 프로그램이 끝점에 액세스하는 데 사용할 모든 도메인 이름과 IP 주소를 알고 있어야 합니다.

인증서의 * 주체 DN * (고유 이름) 항목에는 클라이언트 응용 프로그램이 StorageGRID에 사용할 정규화된 도메인 이름이 포함되어야 합니다. 예를 들면 다음과 같습니다.

Subject DN:
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com

필요에 따라 인증서는 와일드카드를 사용하여 로드 밸런서 서비스를 실행하는 모든 관리 노드 및 게이트웨이 노드의 정규화된 도메인 이름을 나타낼 수 있습니다. 예를 들어,에서는 * .storagegrid.example.com * 와일드카드를 사용하여 adm1.storagegrid.example.com 및 `gn1.storagegrid.example.com`를 나타냅니다.

S3 가상 호스팅 스타일 요청을 사용하려는 경우 인증서에는 와일드카드 이름을 포함하여 구성한 각 항목에 대해 * Alternative Name * 항목도 포함되어야 "[S3 끝점 도메인 이름입니다](#)" 합니다. 예를 들면 다음과 같습니다.

Alternative Name: DNS:*.s3.storagegrid.example.com



도메인 이름에 와일드카드를 사용하는 경우 을 "[서버 인증서에 대한 강화 지침](#)" 검토합니다.

보안 인증서의 각 이름에 대한 DNS 항목도 정의해야 합니다.

만료 예정인 인증서를 관리하려면 어떻게 해야 합니까?



S3 응용 프로그램과 StorageGRID 간의 연결을 보호하는 데 사용되는 인증서가 만료되면 응용 프로그램이 StorageGRID에 대한 액세스를 일시적으로 상실할 수 있습니다.

인증서 만료 문제를 방지하려면 다음 모범 사례를 따르십시오.

- 로드 밸런서 엔드포인트 인증서 만료 * 및 * S3 API용 글로벌 서버 인증서 만료 * 경고와 같이 인증서 만료 날짜가 다가올 경우 경고를 주의 깊게 모니터링하십시오.
- 항상 StorageGRID 및 S3 애플리케이션 버전의 인증서를 동기화된 상태로 유지합니다. 로드 밸런서 끝점에 사용되는 인증서를 교체하거나 갱신하는 경우 S3 애플리케이션에서 사용하는 동등한 인증서를 교체하거나 갱신해야 합니다.
- 공개적으로 서명된 CA 인증서를 사용합니다. CA에서 서명한 인증서를 사용하는 경우 만료 예정 인증서를 중단 없이 교체할 수 있습니다.
- 자체 서명된 StorageGRID 인증서를 생성했으며 인증서가 곧 만료될 경우 기존 인증서가 만료되기 전에 StorageGRID 및 S3 응용 프로그램 모두에서 수동으로 인증서를 교체해야 합니다.

바인딩 모드에 대한 고려 사항

바인딩 모드를 사용하면 로드 밸런서 끝점에 액세스하는 데 사용할 수 있는 IP 주소를 제어할 수 있습니다. 끝점에서 바인딩 모드를 사용하는 경우 클라이언트 응용 프로그램은 허용된 IP 주소 또는 해당 FQDN(정규화된 도메인 이름)을 사용하는 경우에만 끝점에 액세스할 수 있습니다. 다른 IP 주소 또는 FQDN을 사용하는 클라이언트 응용 프로그램은 끝점에 액세스할 수 없습니다.

다음 바인딩 모드 중 하나를 지정할 수 있습니다.

- * 글로벌 * (기본값): 클라이언트 응용 프로그램은 게이트웨이 노드 또는 관리 노드의 IP 주소, 네트워크의 모든 HA 그룹의 가상 IP(VIP) 주소 또는 해당 FQDN을 사용하여 끝점에 액세스할 수 있습니다. 끝점의 접근성을 제한할 필요가 없는 경우 이 설정을 사용합니다.
- * HA 그룹의 가상 IP *. 클라이언트 애플리케이션은 HA 그룹의 가상 IP 주소(또는 해당 FQDN)를 사용해야 합니다.
- * 노드 인터페이스 *. 클라이언트는 선택한 노드 인터페이스의 IP 주소(또는 해당 FQDN)를 사용해야 합니다.
- * 노드 유형 *. 선택한 노드 유형에 따라 클라이언트는 관리 노드의 IP 주소(또는 해당 FQDN)나 게이트웨이 노드의 IP 주소(또는 해당 FQDN)를 사용해야 합니다.

테넌트 액세스에 대한 고려 사항

테넌트 액세스는 어떤 StorageGRID 테넌트 계정에서 로드 밸런서 끝점을 사용하여 해당 버킷을 액세스할 수 있는지 제어할 수 있는 선택적 보안 기능입니다. 모든 테넌트가 끝점(기본값)에 액세스하도록 허용하거나 각 끝점에 대해 허용 또는 차단된 테넌트 목록을 지정할 수 있습니다.

이 기능을 사용하여 테넌트와 해당 끝점 간의 보안 격리를 향상시킬 수 있습니다. 예를 들어, 이 기능을 사용하여 한 테넌트가 소유한 기밀 자료 또는 기밀 자료를 다른 테넌트에서 완전히 액세스할 수 없도록 할 수 있습니다.



액세스 제어를 위해 테넌트는 클라이언트 요청에 사용된 액세스 키로 결정되며, 요청의 일부로 액세스 키가 제공되지 않은 경우(예: 익명 액세스) 버킷 소유자가 테넌트를 결정하는 데 사용됩니다.

테넌트 액세스 예

이 보안 기능의 작동 방식을 이해하려면 다음 예제를 고려해 보십시오.

1. 다음과 같이 두 개의 로드 밸런서 엔드포인트를 생성했습니다.

- * 공개 * 엔드포인트: 포트 10443을 사용하고 모든 테넌트에 대한 액세스를 허용합니다.
- * 상위 비밀 * 엔드포인트: 포트 10444를 사용하며 * 상위 비밀 * 테넌트에만 액세스할 수 있습니다. 다른 모든

테넌트는 이 끝점에 액세스할 수 없습니다.

2. 는 top-secret.pdf * Top secret * 테넌트가 소유한 버킷에 있습니다.

에 액세스하려면 top-secret.pdf * Top secret * 테넌트의 사용자가 GET 요청을 할 수

<https://w.x.y.z:10444/top-secret.pdf> 있습니다. 이 테넌트는 10444 엔드포인트를 사용할 수 있으므로 사용자가 개체에 액세스할 수 있습니다. 그러나 다른 테넌트에 속한 사용자가 동일한 URL에 동일한 요청을 보내면 즉시 액세스 거부 메시지가 표시됩니다. 자격 증명과 서명이 유효하더라도 액세스가 거부됩니다.

CPU 사용성

각 관리자 노드 및 게이트웨이 노드의 로드 밸런서 서비스는 S3 트래픽을 스토리지 노드로 전달할 때 독립적으로 작동합니다. 로드 밸런서 서비스는 가중 프로세스를 통해 더 많은 요청을 CPU 사용성이 높은 스토리지 노드로 라우팅합니다. 노드 CPU 로드 정보는 몇 분마다 업데이트되지만 가중치는 더 자주 업데이트될 수 있습니다. 모든 스토리지 노드에는 최소 기본 가중치 값이 할당됩니다. 이는 노드에서 100% 사용률을 보고하거나 사용률을 보고하지 않는 경우에도 마찬가지입니다.

경우에 따라 CPU 사용성에 대한 정보는 로드 밸런서 서비스가 있는 사이트로 제한됩니다.

로드 밸런서 엔드포인트를 구성합니다

로드 밸런서 엔드포인트는 게이트웨이 및 관리 노드의 StorageGRID 로드 밸런서에 연결할 때 S3 클라이언트가 사용할 수 있는 포트 및 네트워크 프로토콜을 결정합니다. 끝점을 사용하여 그리드 관리자, 테넌트 관리자 또는 둘 다에 액세스할 수도 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. ["지원되는 웹 브라우저"](#)
- 이 ["루트 액세스 권한"](#)입니다.
- 를 검토했습니다. ["로드 균형 조정에 대한 고려 사항"](#)
- 로드 밸런서 끝점에 사용할 포트를 이전에 다시 매핑한 경우 이 있는 ["포트 재맵을 제거했습니다"](#) 것입니다.
- 사용할 고가용성(HA) 그룹을 만들었습니다. HA 그룹이 권장되지만 필수는 아닙니다. 을 ["고가용성 그룹을 관리합니다"](#) 참조하십시오.
- 에서 로드 밸런서 엔드포인트를 사용할 경우 ["S3 테넌트를 선택합니다"](#) 베어 메탈 노드의 IP 주소 또는 FQDN을 사용하지 않아야 합니다. S3 Select에 사용되는 로드 밸런서 엔드포인트에 서비스 어플라이언스 및 VMware 기반 소프트웨어 노드만 허용됩니다.
- 사용할 VLAN 인터페이스를 구성했습니다. 을 ["VLAN 인터페이스를 구성합니다"](#) 참조하십시오.
- HTTPS 끝점을 만드는 경우(권장) 서버 인증서에 대한 정보가 있습니다.



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

- 인증서를 업로드하려면 서버 인증서, 인증서 개인 키 및 선택적으로 CA 번들이 필요합니다.
- 인증서를 생성하려면 S3 클라이언트가 끝점에 액세스하는 데 사용할 모든 도메인 이름과 IP 주소가 필요합니다. 제목(고유 이름)도 알아야 합니다.
- StorageGRID S3 API 인증서(스토리지 노드에 직접 연결하는 데 사용할 수도 있음)를 사용하려는 경우 이미 기본 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 대체한 것입니다. 을 ["S3 API 인증서를 구성합니다"](#) 참조하십시오.

로드 밸런서 끝점을 만듭니다

각 S3 클라이언트 로드 밸런서 엔드포인트는 포트, 클라이언트 유형(S3), 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 클라이언트에 대한 엔드포인트를 생성하려면 **S3** 클라이언트 탭을 선택합니다.
3. Grid Manager, Tenant Manager 또는 둘 다에 액세스하기 위한 끝점을 만들려면 * Management interface * 탭을 선택합니다.
4. Create * 를 선택합니다.

끝점 세부 정보를 입력합니다

단계

1. 만들려는 끝점 유형에 대한 세부 정보를 입력하려면 적절한 지침을 선택합니다.

S3 클라이언트

필드에 입력합니다	설명
이름	Load Balancer Endpoints(분산 장치 끝점 로드) 페이지의 테이블에 표시되는 끝점에 대한 설명 이름입니다.
포트	<p>로드 밸런싱에 사용할 StorageGRID 포트입니다. 이 필드의 기본값은 첫 번째 끝점에서 10433이지만 사용하지 않는 외부 포트는 1에서 65535까지 입력할 수 있습니다.</p> <p>80 * 또는 * 8443 * 을 입력하면 포트 8443을 해제하지 않는 한 엔드포인트는 게이트웨이 노드에서만 구성됩니다. 그런 다음 포트 8443을 S3 엔드포인트로 사용할 수 있으며 포트가 게이트웨이 및 관리 노드 모두에서 구성됩니다.</p>
클라이언트 유형입니다	S3 * 여야 합니다.
네트워크 프로토콜	<p>클라이언트가 이 끝점에 연결할 때 사용할 네트워크 프로토콜입니다.</p> <ul style="list-style-type: none"> TLS 암호화 보안 통신을 위해 * HTTPS * 를 선택합니다(권장). 끝점을 저장하려면 먼저 보안 인증서를 연결해야 합니다. 보안이 취약한 암호화되지 않은 통신을 위해 * HTTP * 를 선택합니다. 비 프로덕션 그리드에만 HTTP를 사용합니다.
캐싱 활성화	<p>활성화 또는 비활성화 "게이트웨이 노드의 캐싱" 이 로드 밸런서 엔드포인트에 대해.</p> <p>캐싱에 문제가 발생하면 다음을 참조하세요. "로드 밸런서 캐싱 문제 해결".</p>

관리 인터페이스

필드에 입력합니다	설명
이름	Load Balancer Endpoints(분산 장치 끝점 로드) 페이지의 테이블에 표시되는 끝점에 대한 설명 이름입니다.
포트	<p>그리드 관리자, 테넌트 관리자 또는 둘 모두에 액세스하는 데 사용할 StorageGRID 포트입니다.</p> <ul style="list-style-type: none"> 그리드 관리자: * 8443 * 테넌트 관리자: * 9443 * 그리드 관리자와 테넌트 관리자 모두: * 443 * <p>참고: 이 사전 설정 포트나 기타 사용 가능한 포트를 사용할 수 있습니다.</p>
인터페이스 유형입니다	이 엔드포인트를 사용하여 액세스할 StorageGRID 인터페이스의 라디오 버튼을 선택합니다.

필드에 입력합니다	설명
신뢰할 수 없는 클라이언트 네트워크	<p>신뢰할 수 없는 클라이언트 네트워크에서 이 끝점에 액세스할 수 있어야 하는 경우 * 예 * 를 선택합니다. 그렇지 않으면 * 아니요 * 를 선택합니다.</p> <p>예 * 를 선택하면 포트가 모든 신뢰할 수 없는 클라이언트 네트워크에서 열립니다.</p> <p>참고: 로드 밸런서 끝점을 만들 때만 신뢰할 수 없는 클라이언트 네트워크에 대해 포트를 열거나 닫도록 구성할 수 있습니다.</p>

1. Continue * 를 선택합니다.

바인딩 모드를 선택합니다

단계

1. 엔드포인트에 대한 바인딩 모드를 선택하여 모든 IP 주소를 사용하거나 특정 IP 주소 및 네트워크 인터페이스를 사용하여 엔드포인트에 액세스하는 방법을 제어합니다.

일부 바인딩 모드는 클라이언트 끝점 또는 관리 인터페이스 끝점에 사용할 수 있습니다. 두 끝점 유형의 모든 모드가 여기에 나열됩니다.

모드를 선택합니다	설명
글로벌(클라이언트 끝점의 기본값)	<p>클라이언트는 게이트웨이 노드 또는 관리 노드의 IP 주소, 네트워크에 있는 HA 그룹의 가상 IP(VIP) 주소 또는 해당 FQDN을 사용하여 끝점에 액세스할 수 있습니다.</p> <p>이 끝점의 접근성을 제한할 필요가 없는 경우 * 글로벌 * 설정을 사용하십시오.</p>
HA 그룹의 가상 IP입니다	<p>클라이언트는 HA 그룹의 가상 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다.</p> <p>이 바인딩 모드의 엔드포인트는 엔드포인트에 대해 선택한 HA 그룹이 겹치지 않는 한 모두 동일한 포트 번호를 사용할 수 있습니다.</p>
노드 인터페이스	클라이언트는 선택한 노드 인터페이스의 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다.
노드 유형(클라이언트 엔드포인트만 해당)	선택한 노드 유형에 따라 클라이언트는 관리 노드의 IP 주소(또는 해당 FQDN)나 게이트웨이 노드의 IP 주소(또는 해당 FQDN)를 사용하여 이 끝점에 액세스해야 합니다.
모든 관리 노드(관리 인터페이스 엔드포인트의 기본값)	클라이언트는 이 끝점에 액세스하려면 관리자 노드의 IP 주소(또는 해당 FQDN)를 사용해야 합니다.

둘 이상의 끝점에서 동일한 포트를 사용하는 경우 StorageGRID는 이 우선 순위 순서를 사용하여 사용할 끝점을 결정합니다. * HA 그룹의 가상 IP * > * 노드 인터페이스 * > * 노드 유형 * > * 글로벌 *.

관리 인터페이스 앤드포인트를 생성하는 경우 관리 노드만 허용됩니다.

2. HA 그룹의 가상 IP * 를 선택한 경우 하나 이상의 HA 그룹을 선택합니다.

관리 인터페이스 끝점을 생성하는 경우 관리 노드에만 연결된 VIP를 선택합니다.

3. 노드 인터페이스 * 를 선택한 경우 이 끝점과 연결할 각 관리 노드 또는 게이트웨이 노드에 대해 하나 이상의 노드 인터페이스를 선택합니다.
4. 노드 유형 * 을 선택한 경우 기본 관리 노드와 비기본 관리 노드 또는 게이트웨이 노드를 모두 포함하는 관리자 노드 중 하나를 선택합니다.

테넌트 액세스를 제어합니다



관리 인터페이스 끝점은 끝점에 가 있는 경우에만 테넌트 액세스를 제어할 수 [Tenant Manager의 인터페이스 유형입니다](#) 있습니다.

단계

1. Tenant access * 단계에서 다음 중 하나를 선택합니다.

필드에 입력합니다	설명
모든 테넌트 허용(기본값)	모든 테넌트 계정은 이 엔드포인트를 사용하여 해당 버킷에 액세스할 수 있습니다. 테넌트 계정을 아직 생성하지 않은 경우 이 옵션을 선택해야 합니다. 테넌트 계정을 추가한 후 로드 밸런서 끝점을 편집하여 특정 계정을 허용하거나 차단할 수 있습니다.
선택한 테넌트 허용	선택한 테넌트 계정만 이 끝점을 사용하여 해당 버킷을 액세스할 수 있습니다.
선택한 테넌트 차단	선택한 테넌트 계정은 이 끝점을 사용하여 해당 버킷을 액세스할 수 없습니다. 다른 모든 테넌트는 이 끝점을 사용할 수 있습니다.

2. HTTP* 끝점을 만드는 경우에는 인증서를 첨부할 필요가 없습니다. 새 로드 밸런서 끝점을 추가하려면 * Create * 를 선택합니다. 그런 다음 로 이동합니다[작업을 마친 후](#). 그렇지 않으면 * 계속 * 을 선택하여 인증서를 첨부하십시오.

인증서를 첨부합니다

단계

1. HTTPS* 끝점을 만드는 경우 끝점에 연결할 보안 인증서 유형을 선택합니다.

인증서는 관리자 노드 또는 게이트웨이 노드에서 S3 클라이언트와 로드 밸런서 서비스 간의 연결을 보호합니다.

- * 인증서 업로드 *. 업로드할 사용자 지정 인증서가 있는 경우 이 옵션을 선택합니다.
- * 인증서 생성 *. 사용자 지정 인증서를 생성하는 데 필요한 값이 있는 경우 이 옵션을 선택합니다.
- * StorageGRID S3 인증서 사용 *. 스토리지 노드에 대한 직접 연결에도 사용할 수 있는 글로벌 S3 API 인증서를 사용하려면 이 옵션을 선택합니다.

그리드 CA에서 서명한 기본 S3 API 인증서를 외부 인증 기관에서 서명한 사용자 지정 인증서로 대체하지 않는 한 이 옵션을 선택할 수 없습니다. 을 "[S3 API 인증서를 구성합니다](#)" 참조하십시오.

- * 관리 인터페이스 인증서 사용 *. 관리 노드에 대한 직접 연결에도 사용할 수 있는 글로벌 관리 인터페이스 인증서를 사용하려면 이 옵션을 선택합니다.

2. StorageGRID S3 인증서를 사용하지 않는 경우 인증서를 업로드하거나 생성합니다.

인증서를 업로드합니다

- 인증서 업로드 * 를 선택합니다.
- 필요한 서버 인증서 파일을 업로드합니다.
 - * 서버 인증서 *: PEM 인코딩의 사용자 정의 서버 인증서 파일.
 - * 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일(.key).



EC 개인 키는 224비트 이상이어야 합니다. RSA 개인 키는 2048비트 이상이어야 합니다.

- * CA 번들 *: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 선택적 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.
- 업로드한 각 인증서의 메타데이터를 보려면 * 인증서 세부 정보 * 를 확장합니다. 선택적 CA 번들을 업로드한 경우 각 인증서는 자체 탭에 표시됩니다.
 - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택하고 인증서 번들을 저장하려면 * CA 번들 다운로드 * 를 선택합니다.

인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 .pem 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

- 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 또는 * CA 번들 PEM * 복사 를 선택합니다.
- Create * 를 선택합니다. + 로드 밸런서 끝점이 생성됩니다. 사용자 지정 인증서는 S3 클라이언트 또는 관리 인터페이스와 끝점 간의 모든 후속 새 연결에 사용됩니다.

인증서를 생성합니다

- 인증서 생성 * 을 선택합니다.
- 인증서 정보를 지정합니다.

필드에 입력합니다	설명
도메인 이름	인증서에 포함할 하나 이상의 정규화된 도메인 이름입니다. 여러 도메인 이름을 나타내는 와일드카드로 * 를 사용합니다.
IP	인증서에 포함할 하나 이상의 IP 주소입니다.
제목(선택 사항)	X.509 인증서 소유자의 주체 또는 고유 이름(DN)입니다. 이 필드에 값을 입력하지 않으면 생성된 인증서는 첫 번째 도메인 이름 또는 IP 주소를 CN(Subject Common Name)으로 사용합니다.
일 유효	인증서가 만료된 후 경과한 일 수입니다.

필드에 입력합니다	설명
키 사용 확장을 추가합니다	<p>이 옵션을 선택하면(기본값 및 권장) 키 사용 및 확장 키 사용 확장이 생성된 인증서에 추가됩니다.</p> <p>이러한 확장은 인증서에 포함된 키의 용도를 정의합니다.</p> <ul style="list-style-type: none"> 참고 *: 인증서에 이러한 확장자가 포함되어 있을 때 이전 클라이언트와의 연결 문제가 발생하지 않는 한 이 확인란을 선택된 상태로 둡니다.

- Generate * 를 선택합니다.
- 생성된 인증서의 메타데이터를 보려면 * 인증서 세부 정보 * 를 선택합니다.
 - 인증서 파일을 저장하려면 * 인증서 다운로드 * 를 선택합니다.

인증서 파일 이름 및 다운로드 위치를 지정합니다. 확장자를 사용하여 파일을 .pem 저장합니다.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

- 다른 곳에 붙여넣을 인증서 내용을 복사하려면 * 인증서 PEM * 복사 를 선택합니다.

- Create * 를 선택합니다.

로드 밸런서 끝점이 생성됩니다. 사용자 지정 인증서는 S3 클라이언트 또는 관리 인터페이스와 이 끝점 간의 모든 후속 새 연결에 사용됩니다.

작업을 마친 후

단계

- DNS를 사용하는 경우 DNS에 StorageGRID FQDN(정규화된 도메인 이름)을 클라이언트가 연결에 사용할 각 IP 주소에 연결하는 레코드가 포함되어 있는지 확인합니다.

DNS 레코드에 입력하는 IP 주소는 로드 밸런싱 노드의 HA 그룹을 사용하는지 여부에 따라 달라집니다.

- HA 그룹을 구성한 경우 클라이언트는 해당 HA 그룹의 가상 IP 주소에 연결됩니다.
- HA 그룹을 사용하지 않는 경우 클라이언트는 게이트웨이 노드 또는 관리 노드의 IP 주소를 사용하여 StorageGRID 로드 밸런서 서비스에 연결됩니다.

또한 DNS 레코드가 와일드카드 이름을 포함하여 필요한 모든 끝점 도메인 이름을 참조하는지 확인해야 합니다.

- S3 클라이언트에 엔드포인트에 연결하는 데 필요한 정보 제공:

- 포트 번호입니다
- 정규화된 도메인 이름 또는 IP 주소입니다
- 필요한 인증서 세부 정보입니다

로드 밸런서 끝점을 보고 편집합니다

보안 끝점의 인증서 메타데이터를 포함하여 기존 로드 밸런서 끝점에 대한 세부 정보를 볼 수 있습니다. 끝점의 특정 설정을 변경할 수 있습니다.

- 모든 로드 밸런서 끝점에 대한 기본 정보를 보려면 부하 분산 끝점 페이지의 표를 검토하십시오.
- 인증서 메타데이터를 포함하여 특정 끝점에 대한 모든 세부 정보를 보려면 테이블에서 끝점 이름을 선택합니다. 표시되는 정보는 엔드포인트 유형 및 구성 방법에 따라 다릅니다.

S3 load balancer endpoint

Port:	10443
Client type:	S3
Network protocol:	HTTPS
Binding mode:	Global
Endpoint ID:	3d02c126-9437-478c-8b24-08384401d3cb

[Remove](#)

[Edit binding mode](#)

Binding mode Certificate Tenant access (2 allowed)

You can select a different binding mode or change IP addresses for the current binding mode.

Binding mode: Global

 This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

- 끝점을 편집하려면 로드 밸런서 끝점 페이지의 * 작업 * 메뉴를 사용하십시오.



관리 인터페이스 끝점의 포트를 편집하는 동안 Grid Manager에 액세스할 수 없는 경우 URL 및 포트를 업데이트하여 다시 액세스합니다.



끝점을 편집한 후 변경 내용이 모든 노드에 적용될 때까지 최대 15분 정도 기다려야 할 수 있습니다.

작업	작업 메뉴	세부 정보 페이지
끝점 이름을 편집합니다	<ul style="list-style-type: none"> a. 끝점의 확인란을 선택합니다. b. 작업 * > * 끝점 이름 편집 * 을 선택합니다. c. 새 이름을 입력합니다. d. 저장 * 을 선택합니다. 	<ul style="list-style-type: none"> a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. 편집 아이콘을 선택합니다 . c. 새 이름을 입력합니다. d. 저장 * 을 선택합니다.
엔드포인트 포트를 편집합니다	<ul style="list-style-type: none"> a. 끝점의 확인란을 선택합니다. b. Actions * > * Edit Endpoint port * 를 선택합니다 c. 유효한 포트 번호를 입력하십시오. d. 저장 * 을 선택합니다. 	n/a
끝점 바인딩 모드를 편집합니다	<ul style="list-style-type: none"> a. 끝점의 확인란을 선택합니다. b. 작업 * > * 끝점 바인딩 모드 편집 * 을 선택합니다. c. 필요에 따라 바인딩 모드를 업데이트합니다. d. 변경 내용 저장 * 을 선택합니다. 	<ul style="list-style-type: none"> a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. 바인딩 모드 편집 * 을 선택합니다. c. 필요에 따라 바인딩 모드를 업데이트합니다. d. 변경 내용 저장 * 을 선택합니다.
끝점 인증서를 편집합니다	<ul style="list-style-type: none"> a. 끝점의 확인란을 선택합니다. b. 작업 * > * 끝점 인증서 편집 * 을 선택합니다. c. 필요에 따라 새 사용자 지정 인증서를 업로드 또는 생성하거나 글로벌 S3 인증서를 사용합니다. d. 변경 내용 저장 * 을 선택합니다. 	<ul style="list-style-type: none"> a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. Certificate * 탭을 선택합니다. c. 인증서 편집 * 을 선택합니다. d. 필요에 따라 새 사용자 지정 인증서를 업로드 또는 생성하거나 글로벌 S3 인증서를 사용합니다. e. 변경 내용 저장 * 을 선택합니다.
테넌트 액세스를 편집합니다	<ul style="list-style-type: none"> a. 끝점의 확인란을 선택합니다. b. 작업 * > * 테넌트 액세스 편집 * 을 선택합니다. c. 다른 액세스 옵션을 선택하거나 목록에서 테넌트를 선택하거나 제거하거나 둘 모두를 수행합니다. d. 변경 내용 저장 * 을 선택합니다. 	<ul style="list-style-type: none"> a. 세부 정보를 표시할 끝점 이름을 선택합니다. b. Tenant access * 탭을 선택합니다. c. Edit tenant access * 를 선택합니다. d. 다른 액세스 옵션을 선택하거나 목록에서 테넌트를 선택하거나 제거하거나 둘 모두를 수행합니다. e. 변경 내용 저장 * 을 선택합니다.

로드 밸런서 끝점을 제거합니다

Actions * 메뉴를 사용하여 하나 이상의 끝점을 제거하거나 세부 정보 페이지에서 단일 끝점을 제거할 수 있습니다.

 클라이언트 중단을 방지하려면 로드 밸런서 엔드포인트를 제거하기 전에 영향을 받는 S3 클라이언트 애플리케이션을 모두 업데이트하십시오. 다른 로드 밸런서 끝점에 할당된 포트를 사용하여 연결할 각 클라이언트를 업데이트합니다. 필요한 인증서 정보도 업데이트해야 합니다.

 관리 인터페이스 끝점을 제거하는 동안 그리드 관리자에 액세스할 수 없는 경우 URL을 업데이트합니다.

- 하나 이상의 끝점을 제거하려면:

- 부하 분산 장치 페이지에서 제거할 각 끝점에 대한 확인란을 선택합니다.
- Actions * > * Remove * 를 선택합니다.
- OK * 를 선택합니다.

- 세부 정보 페이지에서 끝점 하나를 제거하려면 다음을 수행합니다.

- 부하 분산 페이지에서 끝점 이름을 선택합니다.
- 세부 정보 페이지에서 * 제거 * 를 선택합니다.
- OK * 를 선택합니다.

S3 끝점 도메인 이름을 구성합니다

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

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

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 있습니다. "[특정 액세스 권한](#)"
- 그리드 업그레이드가 진행 중이 아닌 것을 확인했습니다.

 그리드 업그레이드가 진행 중일 때는 도메인 이름 구성을 변경하지 마십시오.

이 작업에 대해

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

- 그리드 관리자를 사용하여 StorageGRID 시스템에 S3 끝점 도메인 이름을 추가합니다.
- 클라이언트가 필요로 하는 모든 도메인 이름에 대해 에 "[클라이언트가 StorageGRID에 대한 HTTPS 연결에 사용하는 인증서입니다](#)" 서명되어 있는지 확인합니다.

예를 들어, 끝점이 인 경우 HTTPS 연결에 사용되는 인증서에 끝점과 끝점의 와일드카드 SAN(Subject Alternative Name) *.s3.company.com 이 `s3.company.com 포함되어 있는지 확인해야 s3.company.com 합니다.

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



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

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

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



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

S3 엔드포인트 도메인 이름을 추가합니다

단계

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

결과

이제 클라이언트가 끝점을 사용하면 `bucket.s3.company.com` DNS 서버가 올바른 끝점으로 확인되고 인증서가 예상대로 끝점을 인증합니다.

S3 끝점 도메인 이름 바꾸기

S3 애플리케이션에서 사용하는 이름을 변경하면 가상 호스팅 스타일 요청이 실패합니다.

단계

- 구성 > 네트워크 > *S3 엔드포인트 도메인 이름*을 선택합니다.
- 편집할 도메인 이름 필드를 선택하고 필요한 내용을 변경합니다.
- 저장 * 을 선택합니다.
- 예 * 를 선택하여 변경 사항을 확인합니다.

S3 끝점 도메인 이름을 삭제합니다

S3 애플리케이션에서 사용하는 이름을 제거하면 가상 호스팅 스타일 요청이 실패합니다.

단계

- 구성 > 네트워크 > *S3 엔드포인트 도메인 이름*을 선택합니다.
- 도메인 이름 옆에 있는 삭제 아이콘을 선택합니다.
- 예 * 를 선택하여 삭제를 확인합니다.

관련 정보

- "[S3 REST API 사용](#)"
- "[IP 주소를 봅니다](#)"
- "[고가용성 그룹을 구성합니다](#)"

요약: 클라이언트 연결을 위한 IP 주소 및 포트

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

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

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

연결 위치	클라이언트가 연결하는 서비스입니다	IP 주소입니다	포트
HA 그룹	로드 밸런서	HA 그룹의 가상 IP 주소입니다	로드 밸런서 끝점에 할당된 포트입니다
관리자 노드	로드 밸런서	관리 노드의 IP 주소입니다	로드 밸런서 끝점에 할당된 포트입니다
게이트웨이 노드	로드 밸런서	게이트웨이 노드의 IP 주소입니다	로드 밸런서 끝점에 할당된 포트입니다
스토리지 노드	LDR	스토리지 노드의 IP 주소입니다	기본 S3 포트: <ul style="list-style-type: none">HTTPS: 18082HTTP: 18084

URL의 예

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

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

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

`https://192.0.2.5:10443`

IP 주소를 찾을 위치

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

클라이언트 응용 프로그램에서 목록의 IP 주소로의 연결을 설정할 수 있습니다.

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



관리 노드 또는 게이트웨이 노드를 보고 있고 고가용성 그룹의 활성 노드인 경우 HA 그룹의 가상 IP 주소가 eth2에 표시됩니다.

3. 고가용성 그룹의 가상 IP 주소를 찾으려면 다음을 수행합니다.
 - a. 구성 > 네트워크 > *고가용성 그룹*을 선택합니다.
 - b. 표에서 HA 그룹의 가상 IP 주소를 확인합니다.
4. 로드 밸런서 끝점의 포트 번호를 찾으려면 다음을 수행합니다.
 - a. 구성 > 네트워크 > *로드 밸런서 엔드포인트*를 선택합니다.
 - b. 사용할 끝점의 포트 번호를 확인합니다.



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

- c. 테이블에서 끝점 이름을 선택합니다.
- d. 클라이언트 유형 * (S3)이 끝점을 사용할 클라이언트 응용 프로그램과 일치하는지 확인합니다.

네트워크 및 연결을 관리합니다

네트워크 설정을 구성합니다

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

VLAN 인터페이스를 구성합니다

보안, 유연성 및 성능을 위해 트래픽을 격리하고 파티셔닝할 수 ["VLAN\(Virtual LAN\) 인터페이스를 생성합니다"](#) 있습니다. 각 VLAN 인터페이스는 관리 노드 및 게이트웨이 노드에서 하나 이상의 상위 인터페이스와 연결됩니다. HA 그룹 및 로드 밸런서 끝점에서 VLAN 인터페이스를 사용하여 클라이언트 또는 관리 트래픽을 애플리케이션 또는 테넌트별로 분리할 수 있습니다.

트래픽 분류 정책

를 사용하면 특정 버킷, 테넌트, 클라이언트 서브넷 또는 로드 밸런서 끝점과 관련된 트래픽을 포함하여 다양한 유형의 네트워크 트래픽을 식별하고 처리할 수 ["트래픽 분류 정책"](#) 있습니다. 이러한 정책은 트래픽 제한 및 모니터링을 지원할 수 있습니다.

StorageGRID 네트워크 지침

그리드 관리자를 사용하여 StorageGRID 네트워크 및 연결을 구성하고 관리할 수 있습니다.

S3 클라이언트 연결 방법은 ["S3 클라이언트 연결을 구성합니다"](#) 참조하십시오.

기본 StorageGRID 네트워크

기본적으로 StorageGRID는 그리드 노드당 세 개의 네트워크 인터페이스를 지원하므로 각 개별 그리드 노드에 대한 네트워킹을 보안 및 액세스 요구 사항에 맞게 구성할 수 있습니다.

네트워크 토플로지에 대한 자세한 내용은 ["네트워킹 지침"](#) 참조하십시오.

그리드 네트워크

필수 요소입니다. 그리드 네트워크는 모든 내부 StorageGRID 트래픽에 사용됩니다. 그리드에서 모든 사이트 및 서브넷의 모든 노드 간에 연결을 제공합니다.

관리자 네트워크

선택 사항. 관리 네트워크는 일반적으로 시스템 관리 및 유지 보수에 사용됩니다. 클라이언트 프로토콜 액세스에도 사용할 수 있습니다. 관리 네트워크는 일반적으로 사설 네트워크이며 사이트 간에 라우팅할 필요가 없습니다.

클라이언트 네트워크

선택 사항. 클라이언트 네트워크는 일반적으로 S3 클라이언트 응용 프로그램에 대한 액세스를 제공하는 데 사용되는 개방형 네트워크이므로 그리드 네트워크를 격리하고 보호할 수 있습니다. 클라이언트 네트워크는 로컬 게이트웨이를 통해 연결할 수 있는 모든 서브넷과 통신할 수 있습니다.

지침

- 각 StorageGRID 노드에는 할당된 각 네트워크에 대해 전용 네트워크 인터페이스, IP 주소, 서브넷 마스크 및 게이트웨이가 필요합니다.
- 그리드 노드는 네트워크에 둘 이상의 인터페이스를 가질 수 없습니다.
- 네트워크 당, 그리드 노드별로 단일 게이트웨이가 지원되며 노드와 동일한 서브넷에 있어야 합니다. 필요한 경우 게이트웨이에서 보다 복잡한 라우팅을 구현할 수 있습니다.
- 각 노드에서 각 네트워크는 특정 네트워크 인터페이스에 매핑됩니다.

네트워크	인터페이스 이름입니다
그리드	eth0
관리자(선택 사항)	eth1
클라이언트(선택 사항)	윤리2

- 노드가 StorageGRID 어플라이언스에 연결된 경우 각 네트워크에 대해 특정 포트가 사용됩니다. 자세한 내용은 어플라이언스 설치 지침을 참조하십시오.
- 기본 라우트는 노드당 자동으로 생성됩니다. eth2가 활성화된 경우 0.0.0.0/0 은 eth2의 클라이언트 네트워크를 사용합니다. eth2가 활성화되지 않은 경우 0.0.0.0/0 은 eth0의 그리드 네트워크를 사용합니다.
- 그리드 노드가 그리드에 가입될 때까지 클라이언트 네트워크가 작동하지 않습니다
- 그리드 노드를 구축하는 동안 관리 네트워크를 구성하여 그리드를 완전히 설치하기 전에 설치 사용자 인터페이스에 액세스할 수 있습니다.

선택적 인터페이스

선택적으로 노드에 인터페이스를 추가할 수 있습니다. 예를 들어, 트렁크 인터페이스를 관리자 또는 게이트웨이 노드에 추가하여 를 서로 다른 애플리케이션 또는 테넌트에 속한 트래픽을 분리할 수 ["VLAN 인터페이스"](#)있습니다. 또는 에서 사용할 액세스 인터페이스를 추가할 수도 ["고가용성\(HA\) 그룹"](#)있습니다.

트렁크 또는 액세스 인터페이스를 추가하려면 다음을 참조하십시오.

- * VMware(노드 설치 후) *: ["VMware: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다"](#)
 - Linux(노드 설치 전): ["노드 구성 파일을 생성합니다"](#)
 - Linux(노드 설치 후): ["노드에 트렁크 또는 액세스 인터페이스 추가"](#)



"Linux"는 RHEL, Ubuntu 또는 Debian 배포를 의미합니다. 지원되는 버전 목록은 다음을 참조하세요.
["NetApp 상호 운용성 매트릭스 툴\(IMT\)"](#).

IP 주소를 봅니다

StorageGRID 시스템의 각 그리드 노드에 대한 IP 주소를 볼 수 있습니다. 그런 다음 이 IP 주소를 사용하여 명령줄에서 그리드 노드에 로그인하고 다양한 유지보수 절차를 수행할 수 있습니다.

시작하기 전에

을 사용하여 그리드 관리자에 로그인되어 있습니다. "지원되는 웹 브라우저"

이 작업에 대해

IP 주소 변경에 대한 자세한 내용은 를 "IP 주소를 구성합니다" 참조하십시오.

단계

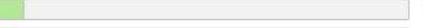
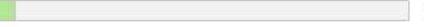
- 노드 > 그리드 노드 > *개요*를 선택합니다.
- IP 주소 제목 오른쪽에 있는 * 더 보기 *를 선택합니다.

해당 그리드 노드의 IP 주소가 테이블에 나열됩니다.

DC2-SGA-010-096-106-021 (Storage Node) 

Overview Hardware Network Storage Objects ILM Tasks

Node information 

Name:	DC2-SGA-010-096-106-021		
Type:	Storage Node		
ID:	f0890e03-4c72-401f-ae92-245511a38e51		
Connection state:	 Connected		
Storage used:	Object data	 7%	
	Object metadata	 5%	
Software version:	11.6.0 (build 20210915.1941.afce2d9)		
IP addresses:	10.96.106.21 - eth0 (Grid Network)		

[Hide additional IP addresses](#) 

Interface	IP address
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

Alerts

Alert name	Severity	Time triggered	Current values
ILM placement unachievable 	 Major	2 hours ago 	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

VLAN 인터페이스를 구성합니다

관리 노드와 게이트웨이 노드에 가상 LAN(VLAN) 인터페이스를 만들고 HA 그룹과 로드 밸런서 엔드포인트에서 이를 사용하여 트래픽을 분리하고 분할하여 보안, 유연성, 성능을 향상시킵니다. HA 그룹에서 선택된 노드는 VLAN 인터페이스를 사용하여 최대 10개의 가상 IP 주소를 공유할 수 있으므로 노드가 다운되면 다른 노드가 가상 IP 주소와의 트래픽을 인계받습니다.

VLAN 인터페이스에 대한 고려 사항

- VLAN ID를 입력하고 하나 이상의 노드에서 상위 인터페이스를 선택하여 VLAN 인터페이스를 생성합니다.
- 상위 인터페이스는 스위치에서 트렁크 인터페이스로 구성되어야 합니다.
- 상위 인터페이스는 Grid Network(eth0), Client Network(eth2) 또는 VM 또는 베어 메탈 호스트(예: ens256)용 추가 트렁크 인터페이스가 될 수 있습니다.
- 각 VLAN 인터페이스에 대해 특정 노드에 대해 하나의 상위 인터페이스만 선택할 수 있습니다. 예를 들어 동일한 VLAN에 대한 상위 인터페이스와 동일한 게이트웨이 노드에서 그리드 네트워크 인터페이스와 클라이언트 네트워크 인터페이스를 모두 사용할 수 없습니다.
- VLAN 인터페이스가 그리드 관리자 및 테넌트 관리자와 관련된 트래픽을 포함하는 관리 노드 트래픽용 VLAN인 경우 관리 노드에서만 인터페이스를 선택합니다.
- VLAN 인터페이스가 S3 클라이언트 트래픽용 인터페이스인 경우 관리 노드 또는 게이트웨이 노드에서 인터페이스를 선택합니다.
- 트렁크 인터페이스를 추가해야 하는 경우 자세한 내용은 다음을 참조하십시오.
 - * VMware(노드 설치 후) *: "[VMware: 노드에 트렁크 또는 액세스 인터페이스를 추가합니다](#)"
 - [Linux\(노드 설치 전\): "노드 구성 파일을 생성합니다"](#)
 - [Linux\(노드 설치 후\): "노드에 트렁크 또는 액세스 인터페이스 추가"](#)



"Linux"는 RHEL, Ubuntu 또는 Debian 배포를 의미합니다. 지원되는 버전 목록은 다음을 참조하세요. ["NetApp 상호 운용성 매트릭스 툴\(IMT\)"](#).

VLAN 인터페이스를 생성합니다

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. ["지원되는 웹 브라우저"](#)
- 이 ["루트 액세스 권한"](#)입니다.
- 트렁크 인터페이스가 네트워크에서 구성되었으며 VM 또는 Linux 노드에 연결되었습니다. 트렁크 인터페이스의 이름을 알고 있습니다.
- 구성하려는 VLAN의 ID를 알고 있습니다.

이 작업에 대해

네트워크 관리자가 하나 이상의 트렁크 인터페이스와 하나 이상의 VLAN을 구성하여 다른 애플리케이션이나 테넌트에 속한 클라이언트 또는 관리 트래픽을 분리했을 수 있습니다. 각 VLAN은 숫자 ID 또는 태그로 식별됩니다. 예를 들어 네트워크에서 FabricPool 트래픽에는 VLAN 100을 사용하고 아카이브 애플리케이션에는 VLAN 200을 사용할 수 있습니다.

그리드 관리자를 사용하여 클라이언트가 특정 VLAN에서 StorageGRID에 액세스할 수 있도록 하는 VLAN

인터페이스를 생성할 수 있습니다. VLAN 인터페이스를 생성할 때 VLAN ID를 지정하고 하나 이상의 노드에서 상위(트렁크) 인터페이스를 선택합니다.

마법사에 액세스합니다

단계

1. 구성 > 네트워크 > *VLAN 인터페이스*를 선택합니다.
2. Create * 를 선택합니다.

VLAN 인터페이스에 대한 세부 정보를 입력합니다

단계

1. 네트워크에 있는 VLAN의 ID를 지정합니다. 1에서 4094 사이의 값을 입력할 수 있습니다.

VLAN ID는 고유하지 않아도 됩니다. 예를 들어 한 사이트의 관리 트래픽에는 VLAN ID 200을 사용하고 다른 사이트의 클라이언트 트래픽에는 동일한 VLAN ID를 사용할 수 있습니다. 각 사이트에서 서로 다른 상위 인터페이스 집합을 사용하여 별도의 VLAN 인터페이스를 만들 수 있습니다. 그러나 동일한 ID를 가진 두 VLAN 인터페이스가 노드에서 동일한 인터페이스를 공유할 수 없습니다. 이미 사용된 ID를 지정하면 메시지가 나타납니다.

2. 선택적으로 VLAN 인터페이스에 대한 간단한 설명을 입력합니다.
3. Continue * 를 선택합니다.

상위 인터페이스를 선택합니다

표에는 그리드의 각 사이트에 있는 모든 관리 노드 및 게이트웨이 노드에 대해 사용 가능한 인터페이스가 나열됩니다. 관리 네트워크(eth1) 인터페이스는 상위 인터페이스로 사용할 수 없으며 표시되지 않습니다.

단계

1. 이 VLAN을 연결할 상위 인터페이스를 하나 이상 선택하십시오.

예를 들어, 게이트웨이 노드 및 관리 노드에 대한 클라이언트 네트워크(eth2) 인터페이스에 VLAN을 연결할 수 있습니다.

Parent interfaces

Select one or more parent interfaces for this VLAN interface. You can only select one parent interface on each node for each VLAN interface.

Site	Node name	Interface	Description	Node type	Attached VLANs
Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
<input checked="" type="checkbox"/> Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
<input checked="" type="checkbox"/> Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
<input type="checkbox"/> Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected. [Previous](#) [Continue](#)

2. Continue * 를 선택합니다.

설정을 확인합니다

단계

1. 구성은 검토하고 변경합니다.
 - VLAN ID 또는 설명을 변경해야 하는 경우 페이지 맨 위에서 * VLAN 세부 정보 입력 * 을 선택합니다.
 - 상위 인터페이스를 변경해야 하는 경우 페이지 맨 위에서 * 상위 인터페이스 선택 * 을 선택하거나 * 이전 * 을 선택합니다.
 - 상위 인터페이스를 제거해야 하는 경우 휴지통을  선택합니다.
2. 저장 * 을 선택합니다.
3. 고가용성 그룹 페이지에 새 인터페이스가 선택 항목으로 나타나고 노드의 네트워크 인터페이스 표(노드 > 부모 인터페이스 노드 > 네트워크)에 나열될 때까지 최대 5분 정도 기다립니다.

VLAN 인터페이스를 편집합니다

VLAN 인터페이스를 편집할 때 다음과 같은 유형의 변경을 수행할 수 있습니다.

- VLAN ID 또는 설명을 변경합니다.
- 부모 인터페이스를 추가하거나 제거합니다.

예를 들어, 연결된 노드의 서비스를 해제하려는 경우 VLAN 인터페이스에서 상위 인터페이스를 제거할 수 있습니다.

다음 사항에 유의하십시오.

- VLAN 인터페이스가 HA 그룹에서 사용되는 경우 VLAN ID를 변경할 수 없습니다.

- 상위 인터페이스가 HA 그룹에서 사용되는 경우에는 상위 인터페이스를 제거할 수 없습니다.

예를 들어, VLAN 200이 노드 A 및 B의 상위 인터페이스에 연결되어 있다고 가정합니다. HA 그룹이 노드 A의 VLAN 200 인터페이스와 노드 B의 eth2 인터페이스를 사용하는 경우 노드 B의 사용되지 않는 상위 인터페이스를 제거할 수는 있지만 노드 A에서 사용된 상위 인터페이스를 제거할 수는 없습니다

단계

- 구성 > 네트워크 > *VLAN 인터페이스*를 선택합니다.
- 편집할 VLAN 인터페이스의 확인란을 선택합니다. 그런 다음 * Actions * > * Edit * 를 선택합니다.
- 필요에 따라 VLAN ID 또는 설명을 업데이트합니다. 그런 다음 * 계속 * 을 선택합니다.

VLAN이 HA 그룹에서 사용되는 경우 VLAN ID를 업데이트할 수 없습니다.

- 필요에 따라 확인란을 선택하거나 선택 취소하여 부모 인터페이스를 추가하거나 사용하지 않는 인터페이스를 제거합니다. 그런 다음 * 계속 * 을 선택합니다.
- 구성을 검토하고 변경합니다.
- 저장 * 을 선택합니다.

VLAN 인터페이스를 제거합니다

하나 이상의 VLAN 인터페이스를 제거할 수 있습니다.

VLAN 인터페이스가 현재 HA 그룹에서 사용되고 있으면 제거할 수 없습니다. VLAN 인터페이스를 제거하려면 먼저 HA 그룹에서 VLAN 인터페이스를 제거해야 합니다.

클라이언트 트래픽의 중단을 방지하려면 다음 중 하나를 수행하는 것이 좋습니다.

- 이 VLAN 인터페이스를 제거하기 전에 HA 그룹에 새 VLAN 인터페이스를 추가하십시오.
- 이 VLAN 인터페이스를 사용하지 않는 새 HA 그룹을 생성합니다.
- 제거하려는 VLAN 인터페이스가 현재 활성 인터페이스인 경우 HA 그룹을 편집합니다. 제거하려는 VLAN 인터페이스를 우선 순위 목록의 맨 아래로 이동합니다. 새 기본 인터페이스에 통신이 설정될 때까지 기다린 다음 HA 그룹에서 이전 인터페이스를 제거합니다. 마지막으로 해당 노드에서 VLAN 인터페이스를 삭제합니다.

단계

- 구성 > 네트워크 > *VLAN 인터페이스*를 선택합니다.
- 제거할 각 VLAN 인터페이스의 확인란을 선택합니다. 그런 다음 * 작업 * > * 삭제 * 를 선택합니다.
- 예 * 를 선택하여 선택을 확인합니다.

선택한 모든 VLAN 인터페이스가 제거됩니다. VLAN 인터페이스 페이지에 녹색 성공 배너가 나타납니다.

관리 인터페이스에 StorageGRID CORS 활성화

그리드 관리자는 StorageGRID 에 대한 관리 API 요청에 대해 CORS(교차 출처 리소스 공유)를 활성화하여 다른 도메인의 관리 API를 사용하여 StorageGRID 의 데이터에 액세스할 수 있도록 할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 그만큼 "[루트 액세스 권한](#)" 모든 CORS 구성 요청에 대한 액세스를 제공합니다.

이 작업에 대해

CORS는 한 도메인의 클라이언트 웹 애플리케이션이 다른 도메인의 리소스에 액세스할 수 있도록 하는 보안 메커니즘입니다. 예를 들어, 도메인에서 StorageGRID에 대한 모니터링 대시보드를 구축하려고 한다고 가정해 보겠습니다. <http://www.example.com>. StorageGRID에서 CORS를 활성화하여 <http://www.example.com> 그리고 "Grid Manager", StorageGRID 도메인은 Grid Management API 요청에 응답합니다. <http://www.example.com>.

관리 API(mgmt-api) 요청 application/json 또는 multipart/formdata 요청 Content-Type CORS가 지원됩니다.

단계

1. Grid Manager에서 구성 > 네트워크 > *관리 인터페이스 CORS 설정*으로 이동합니다.
2. 그리드 관리자, 테넌트 관리자 또는 두 옵션을 모두 선택하세요.
 - 그리드 관리자: 크로스 도메인 그리드 관리 API 요청에 대해 CORS를 활성화합니다.
 - 테넌트 관리자: 크로스 도메인 테넌트 관리 API 요청에 대해 CORS를 활성화합니다.
3. 도메인 필드에 다른 도메인의 URL을 입력합니다.

StorageGRID에서 두 개 이상의 도메인에 대해 CORS를 활성화하려면 *다른 도메인 추가*를 선택하세요.

4. 저장 * 을 선택합니다.

관련 정보

["버킷 및 객체에 대한 StorageGRID CORS 구성"](#)

트래픽 분류 정책을 관리합니다

트래픽 분류 정책이란 무엇입니까?

트래픽 분류 정책을 사용하면 다양한 유형의 네트워크 트래픽을 식별하고 모니터링할 수 있습니다. 이러한 정책은 트래픽 제한 및 모니터링을 지원하여 QoS(Quality-of-Service) 서비스를 향상시킬 수 있습니다.

트래픽 분류 정책은 게이트웨이 노드 및 관리 노드에 대한 StorageGRID 로드 밸런서 서비스의 끝점에 적용됩니다. 트래픽 분류 정책을 생성하려면 로드 밸런서 엔드포인트를 이미 생성해야 합니다.

일치하는 규칙

각 트래픽 분류 정책에는 다음 항목 중 하나 이상에 관련된 네트워크 트래픽을 식별하기 위한 하나 이상의 일치하는 규칙이 포함되어 있습니다.

- 버킷
- 서브넷

- 테넌트
- 부하 분산 장치 엔드포인트

StorageGRID는 규칙의 목적에 따라 정책 내의 규칙과 일치하는 트래픽을 모니터링합니다. 정책에 대한 규칙과 일치하는 모든 트래픽은 해당 정책에 의해 처리됩니다. 반대로, 지정된 엔터티를 제외한 모든 트래픽에 일치시키는 규칙을 설정할 수 있습니다.

트래픽 제한

필요에 따라 다음 제한 유형을 정책에 추가할 수 있습니다.

- 애그리게이트 대역폭
- 요청 당 대역폭
- 동시 요청
- 요청 속도

제한 값은 부하 분산 장치별로 적용됩니다. 트래픽이 여러 부하 분산 장치에 동시에 분산되는 경우 총 최대 속도는 사용자가 지정한 속도 제한의 배수입니다.



정책을 생성하여 애그리게이트 대역폭을 제한하거나 요청당 대역폭을 제한할 수 있습니다. 그러나 StorageGRID는 두 가지 유형의 대역폭을 동시에 제한할 수 없습니다. 애그리게이트 대역폭 제한은 제한 없는 트래픽에 약간의 성능 영향을 줄 수 있습니다.

애그리게이트 또는 요청별 대역폭 제한의 경우 요청은 사용자가 설정한 속도로 스트림 인 또는 아웃됩니다.

StorageGRID는 단 하나의 속도만 적용할 수 있으므로 가장 구체적인 정책 매칭은 매처 유형별로 적용됩니다. 요청에 사용된 대역폭은 총 대역폭 제한 정책을 포함하는 비교적 덜 특정한 다른 정책에 포함되지 않습니다. 다른 모든 제한 유형의 경우 클라이언트 요청이 250밀리초 지연되고 일치하는 정책 제한을 초과하는 요청에 대해 503 느린 응답 응답을 수신합니다.

Grid Manager에서 트래픽 차트를 보고 정책이 기대하는 트래픽 제한을 적용하고 있는지 확인할 수 있습니다.

SLA와 함께 트래픽 분류 정책을 사용합니다

용량 제한 및 데이터 보호와 함께 트래픽 분류 정책을 사용하여 용량, 데이터 보호 및 성능에 대한 세부 정보를 제공하는 서비스 수준 계약(SLA)을 적용할 수 있습니다.

다음 예에서는 SLA의 세 가지 계층을 보여 줍니다. 트래픽 분류 정책을 작성하여 각 SLA 계층의 성능 목표를 달성할 수 있습니다.

서비스 수준 계층	용량	데이터 보호	최대 성능이 허용됩니다	비용
골드	1PB의 스토리지가 허용됩니다	ILM 규칙 3개 복사	초당 25K 요청 5GB/sec(40Gbps) 대역폭	\$\$/월

서비스 수준 계층	용량	데이터 보호	최대 성능이 허용됩니다	비용
실버	250TB 스토리지 허용	ILM 규칙 2개 복사	초당 10K 요청 1.25GB/sec(10Gbps) 대역폭	\$\$/월
브론즈	100TB 스토리지 허용	ILM 규칙 2개 복사	초당 5K 요청 1 GB/sec(8Gbps) 대역폭	\$/월

트래픽 분류 정책을 생성합니다

트래픽 분류 정책을 생성하고 버킷, 버킷 regex, CIDR, 부하 분산 단말 장치 또는 테넌트별로 네트워크 트래픽을 선택적으로 제한할 수 있습니다. 필요에 따라 대역폭, 동시 요청 수 또는 요청 속도를 기준으로 정책에 대한 제한을 설정할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 이 "[루트 액세스 권한](#)"입니다.
- 일치시킬 로드 밸런서 끝점을 만들었습니다.
- 일치시킬 테넌트를 만들었습니다.

단계

1. 구성 > 네트워크 > *트래픽 분류*를 선택합니다.
2. Create * 를 선택합니다.
3. 정책의 이름과 설명(선택 사항)을 입력하고 * Continue * 를 선택합니다.

예를 들어, 이 트래픽 분류 정책이 적용되는 대상 및 제한할 내용에 대해 설명하십시오.

4. 규칙 추가 * 를 선택하고 다음 세부 정보를 지정하여 정책에 일치하는 규칙을 하나 이상 만듭니다. 생성하는 모든 정책에는 하나 이상의 일치하는 규칙이 있어야 합니다. Continue * 를 선택합니다.

필드에 입력합니다	설명
유형	일치하는 규칙이 적용되는 트래픽 유형을 선택합니다. 트래픽 유형은 버킷, 버킷 regex, CIDR, 부하 분산 단말 장치 및 테넌트입니다.

필드에 입력합니다	설명
일치 값	<p>선택한 유형과 일치하는 값을 입력합니다.</p> <ul style="list-style-type: none"> 버킷: 하나 이상의 버킷 이름을 입력합니다. 버킷 정규식: 버킷 이름 집합과 일치하는 데 사용되는 하나 이상의 정규식을 입력합니다. <p>정규식이 고정 해제됩니다. ^anchor를 사용하여 버킷 이름의 시작 부분에 일치시키고 \$ anchor를 사용하여 이름 끝에 일치시킵니다. 정규식 일치는 PCRE(Perl 호환 정규식) 구문의 하위 집합을 지원합니다.</p> <ul style="list-style-type: none"> CIDR: 원하는 서브넷과 일치하는 하나 이상의 IPv4 서브넷을 CIDR 표기법으로 입력합니다. 로드 밸런서 끝점: 끝점 이름을 선택합니다. 예상 정의한 로드 밸런서 엔드포인트입니다. "로드 밸런서 엔드포인트를 구성합니다" 테넌트: 테넌트 일치는 액세스 키 ID를 사용합니다. 요청에 액세스 키 ID(예: 익명 액세스)가 없으면 액세스한 버킷의 소유권이 테넌트를 결정하는 데 사용됩니다.
역일치	<p>방금 정의한 유형 및 일치 값과 일치하는 모든 network traffic_except_traffic을 일치시키려면 * 역일치 * 확인란을 선택합니다. 그렇지 않으면 확인란을 선택하지 않은 상태로 듭니다.</p> <p>예를 들어, 이 정책이 로드 밸런서 끝점 중 하나를 제외한 모든 항목에 적용되도록 하려면 제외할 로드 밸런서 끝점을 지정하고 * 역일치 *를 선택합니다.</p> <p>하나 이상의 교자가 역마쳐인 여러 마치를 포함하는 정책의 경우 모든 요청과 일치하는 정책을 만들지 않도록 주의하십시오.</p>

5. 필요에 따라 * 제한 추가 *를 선택하고 다음 세부 정보를 선택하여 규칙에 일치하는 네트워크 트래픽을 제어하는 하나 이상의 제한을 추가합니다.



StorageGRID는 제한을 추가하지 않아도 메트릭을 수집하므로 트래픽 추세를 파악할 수 있습니다.

필드에 입력합니다	설명
유형	<p>규칙에 일치하는 네트워크 트래픽에 적용할 제한 유형입니다. 예를 들어, 대역폭 또는 요청 속도를 제한할 수 있습니다.</p> <ul style="list-style-type: none"> 참고 *: 정책을 작성하여 총 대역폭을 제한하거나 요청 당 대역폭을 제한할 수 있습니다. 그러나 StorageGRID는 두 가지 유형의 대역폭을 동시에 제한할 수 없습니다. 애그리게이트 대역폭이 사용 중인 경우 요청당 대역폭을 사용할 수 없습니다. 반대로, 요청 당 대역폭이 사용 중일 때는 총 대역폭을 사용할 수 없습니다. 애그리게이트 대역폭 제한은 제한 없는 트래픽에 약간의 성능 영향을 줄 수 있습니다. <p>대역폭 제한에 대해 StorageGRID는 설정된 제한 유형과 가장 일치하는 정책을 적용합니다. 예를 들어, 트래픽을 한 방향으로만 제한하는 정책이 있는 경우 대역폭 제한이 있는 추가 정책과 일치하는 트래픽이 있더라도 반대 방향의 트래픽은 무제한입니다. StorageGRID는 대역폭 제한에 대해 다음 순서로 "가장 적합한" 일치 항목을 구현합니다.</p> <ul style="list-style-type: none"> 정확한 IP 주소(/32 마스크) 정확한 버킷 이름입니다 버킷 regex 테넌트 엔드포인트 일치하지 않는 CIDR 일치(NOT/32) 역 일치
적용 대상	이 제한이 클라이언트 읽기 요청(GET 또는 HEAD) 또는 쓰기 요청(PUT, POST 또는 DELETE)에 적용될지 여부를 나타냅니다.
값	<p>선택한 장치에 따라 네트워크 트래픽이 로 제한됩니다. 예를 들어, 10을 입력하고 MiB/s를 선택하면 이 규칙에 일치하는 네트워크 트래픽이 10MiB/s를 초과하지 않습니다</p> <ul style="list-style-type: none"> 참고 *: 단위 설정에 따라 사용 가능한 단위는 2진수(예: GiB) 또는 10진수(예: GB)가 됩니다. 단위 설정을 변경하려면 그리드 관리자 오른쪽 상단의 사용자 드롭다운을 선택한 다음 * 사용자 기본 설정 * 을 선택합니다.
단위	입력한 값을 설명하는 단위입니다.

예를 들어, SLA 계층에 대해 4GB/s 대역폭 제한을 생성하려면 GET/HEAD(4GB/s) 및 PUT/POST/DELETE(4GB/s)의 두 가지 집계 대역폭 제한을 생성합니다.

6. Continue * 를 선택합니다.
7. 트래픽 분류 정책을 읽고 검토하십시오. Previous * (이전 *) 버튼을 사용하여 돌아가서 필요에 따라 변경합니다. 정책에 만족하면 * Save and continue * 를 선택합니다.

이제 S3 클라이언트 트래픽이 트래픽 분류 정책에 따라 처리됩니다.

작업을 마친 후

"네트워크 트래픽 메트릭을 확인합니다" 정책이 예상한 트래픽 제한을 적용하고 있는지 확인합니다.

트래픽 분류 정책을 편집합니다

트래픽 분류 정책을 편집하여 이름 또는 설명을 변경하거나 정책에 대한 규칙 또는 제한을 생성, 편집 또는 삭제할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "지원되는 웹 브라우저"
- 이 "루트 액세스 권한" 있습니다.

단계

1. 구성 > 네트워크 > *트래픽 분류*를 선택합니다.

트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

2. 작업 메뉴 또는 세부 정보 페이지를 사용하여 정책을 편집합니다. 입력할 항목은 ["트래픽 분류 정책을 생성합니다"](#) 참조하십시오.

작업 메뉴

- 정책 확인란을 선택합니다.
- Actions * > * Edit * 를 선택합니다.

세부 정보 페이지

- 정책 이름을 선택합니다.
- 정책 이름 옆의 * Edit * 버튼을 선택합니다.

- Enter policy name(정책 이름 입력) 단계에서 필요에 따라 정책 이름 또는 설명을 편집하고 * Continue *(계속 *)를 선택합니다.
- 일치하는 규칙 추가 단계에서는 필요에 따라 규칙을 추가하거나 기존 규칙의 * 유형 * 및 * 일치 값 * 을 편집하고 * 계속 * 을 선택합니다.
- Set limits(제한 설정) 단계에서 필요에 따라 제한을 추가, 편집 또는 삭제하고 * Continue *(계속 *)를 선택합니다.
- 업데이트된 정책을 검토하고 * Save and continue * 를 선택합니다.

정책 변경 사항이 저장되고 이제 트래픽 분류 정책에 따라 네트워크 트래픽이 처리됩니다. 트래픽 차트를 보고 정책이 기대하는 트래픽 제한을 적용하고 있는지 확인할 수 있습니다.

트래픽 분류 정책을 삭제합니다

더 이상 필요하지 않은 경우 트래픽 분류 정책을 삭제할 수 있습니다. 삭제 시 정책을 검색할 수 없으므로 올바른 정책을 삭제해야 합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"

- 이 "루트 액세스 권한"있습니다.

단계

1. 구성 > 네트워크 > *트래픽 분류*를 선택합니다.

트래픽 분류 정책 페이지가 테이블에 나열된 기존 정책과 함께 나타납니다.

2. 작업 메뉴 또는 세부 정보 페이지를 사용하여 정책을 삭제합니다.

작업 메뉴

- a. 정책 확인란을 선택합니다.
- b. Actions * > * Remove * 를 선택합니다.

정책 세부 정보 페이지

- a. 정책 이름을 선택합니다.
- b. 정책 이름 옆의 * 제거 * 버튼을 선택합니다.

3. 예 * 를 선택하여 정책을 삭제할 것임을 확인합니다.

정책이 삭제됩니다.

네트워크 트래픽 메트릭을 확인합니다

트래픽 분류 정책 페이지에서 사용할 수 있는 그래프를 보고 네트워크 트래픽을 모니터링할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 이 "루트 액세스 또는 테넌트 계정 권한"있습니다.

이 작업에 대해

기존 트래픽 분류 정책에 대해 로드 밸런서 서비스에 대한 메트릭을 확인하여 정책이 네트워크 전체의 트래픽을 성공적으로 제한하고 있는지 확인할 수 있습니다. 그래프의 데이터를 통해 정책을 조정해야 하는지 여부를 결정할 수 있습니다.

트래픽 분류 정책에 대해 설정된 제한이 없더라도 메트릭이 수집되고 그래프는 트래픽 추세를 이해하는 데 유용한 정보를 제공합니다.

단계

1. 구성 > 네트워크 > *트래픽 분류*를 선택합니다.

트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

2. 메트릭을 보려는 트래픽 분류 정책 이름을 선택합니다.

3. 메트릭 * 탭을 선택합니다.

트래픽 분류 정책 그래프가 나타납니다. 그래프에는 선택한 정책과 일치하는 트래픽에 대한 메트릭만 표시됩니다.

다음 그래프가 페이지에 포함되어 있습니다.

- 요청 속도: 이 그래프는 모든 로드 밸런싱 장치가 처리하는 이 정책과 일치하는 대역폭을 제공합니다. 수신된 데이터에는 모든 요청에 대한 요청 헤더와 본문 데이터가 있는 응답에 대한 본문 데이터 크기가 포함됩니다. 보낸 편지에는 모든 요청에 대한 응답 헤더와 응답에 본문 데이터가 포함된 요청에 대한 응답 본문 데이터 크기가 포함됩니다.



요청이 완료되면 이 차트는 대역폭 사용량만 표시합니다. 오브젝트 요청이 느리거나 큰 경우 실제 순간 대역폭은 이 그래프에 보고된 값과 다를 수 있습니다.

- 오류 응답 속도: 이 그래프는 이 정책과 일치하는 요청이 클라이언트에 오류(HTTP 상태 코드 ≥ 400)를 반환하는 대략적인 속도를 제공합니다.
- 평균 요청 기간(오류 없음): 이 그래프는 이 정책과 일치하는 성공적인 요청의 평균 기간을 제공합니다.
- 정책 대역폭 사용량: 이 그래프는 모든 로드 밸런싱 장치가 처리하는 이 정책과 일치하는 대역폭을 제공합니다. 수신된 데이터에는 모든 요청에 대한 요청 헤더와 본문 데이터가 있는 응답에 대한 본문 데이터 크기가 포함됩니다. 보낸 편지에는 모든 요청에 대한 응답 헤더와 응답에 본문 데이터가 포함된 요청에 대한 응답 본문 데이터 크기가 포함됩니다.

4. 커서를 선 그래프 위에 놓으면 그래프의 특정 부분에 값 팝업이 표시됩니다.

5. 메트릭 제목 바로 아래에 있는 * Grafana 대시보드 * 를 선택하여 정책에 대한 모든 그래프를 봅니다. Metrics * 탭의 네 가지 그래프 외에도 두 개의 그래프를 더 볼 수 있습니다.

- 객체 크기별 쓰기 요청 비율: 이 정책과 일치하는 PUT/POST/DELETE 요청 비율. 개별 셀에 위치하면 초당 비율이 표시됩니다. 호버 보기에 표시된 속도는 정수 수로 잘리고 버켓에 0이 아닌 요청이 있을 경우 0으로 보고할 수 있습니다.
- 객체 크기별 읽기 요청 비율: 이 정책과 일치하는 GET/HEAD 요청의 비율 개별 셀에 위치하면 초당 비율이 표시됩니다. 호버 보기에 표시된 속도는 정수 수로 잘리고 버켓에 0이 아닌 요청이 있을 경우 0으로 보고할 수 있습니다.

6. 또는 지원 메뉴에서 그래프에 접근하세요.

- 지원 > 도구 > *측정항목*을 선택하세요.
- Grafana * 섹션에서 * 트래픽 분류 정책 * 을 선택합니다.
- 페이지 왼쪽 상단의 메뉴에서 정책을 선택합니다.
- 그래프 위에 커서를 놓으면 샘플의 날짜 및 시간, 개수로 집계된 개체 크기 및 해당 기간 동안 초당 요청 수를 보여 주는 팝업이 표시됩니다.

트래픽 분류 정책은 ID로 식별됩니다. 정책 ID는 트래픽 분류 정책 페이지에 나열되어 있습니다.

7. 그래프를 분석하여 정책에 따라 트래픽이 제한되는 빈도와 정책을 조정해야 하는지 여부를 결정합니다.

발신 TLS 연결에 지원되는 암호

StorageGRID 시스템은 ID 페더레이션 및 클라우드 스토리지 풀에 사용되는 외부 시스템에 대한 TLS(Transport Layer Security) 연결을 위한 제한된 암호화 그룹 세트를 지원합니다.

지원되는 TLS 버전입니다

StorageGRID는 ID 페더레이션 및 클라우드 스토리지 폴에 사용되는 외부 시스템에 대한 연결을 위해 TLS 1.2 및 TLS 1.3을 지원합니다.

외부 시스템에서 사용할 수 있는 TLS 암호는 다양한 외부 시스템과의 호환성을 보장하기 위해 선택되었습니다. 이 목록은 S3 클라이언트 애플리케이션에서 사용할 수 있는 암호 목록보다 큽니다. 암호를 구성하려면 구성 > 보안 > *보안 설정*으로 이동하여 *TLS 및 SSH 정책*을 선택하세요.



프로토콜 버전, 암호, 키 교환 알고리즘 및 MAC 알고리즘과 같은 TLS 구성 옵션은 StorageGRID에서 구성할 수 없습니다. 이러한 설정에 대한 구체적인 요청이 있을 경우 NetApp 어카운트 담당자에게 문의하십시오.

활성, 유휴 및 동시 HTTP 연결의 이점

HTTP 연결을 구성하는 방법은 StorageGRID 시스템의 성능에 영향을 줄 수 있습니다. 구성은 HTTP 연결이 활성 상태인지 유휴 상태인지 또는 여러 개의 동시 연결이 있는지 여부에 따라 달라집니다.

다음과 같은 유형의 HTTP 연결에 대한 성능 이점을 확인할 수 있습니다.

- 유휴 HTTP 연결
- 활성 HTTP 연결
- 동시 HTTP 연결

유휴 HTTP 연결을 열어 두면 얻을 수 있는 이점

클라이언트 애플리케이션이 유휴 상태일 때에도 HTTP 연결을 열어두면 나중에 트랜잭션을 수행할 수 있습니다. 최대 10분 동안 유휴 HTTP 연결을 열어 둡니다. StorageGRID 10분 이상 열려 있고 유휴 상태인 HTTP 연결을 자동으로 닫을 수 있습니다.

개방 및 유휴 HTTP 연결은 다음과 같은 이점을 제공합니다.

- StorageGRID 시스템이 HTTP 트랜잭션을 수행해야 한다고 결정하는 시간부터 StorageGRID 시스템이 트랜잭션을 수행할 수 있는 시간까지 지연 시간을 줄였습니다

지연 시간 감소는 특히 TCP/IP 및 TLS 연결을 설정하는 데 필요한 시간의 주요 장점입니다.

- 이전에 수행된 전송을 사용하여 TCP/IP 저속 시작 알고리즘을 프라이밍하여 데이터 전송 속도를 높였습니다
- 클라이언트 응용 프로그램과 StorageGRID 시스템 간의 연결을 종단하는 여러 가지 장애 조건에 대한 즉각적인 알림

느린 시작의 이점과 리소스 할당의 균형을 맞춰 유휴 연결을 얼마나 오랫동안 열어둘지 결정합니다.

활성 HTTP 연결의 이점

스토리지 노드에 직접 연결하는 경우 HTTP 연결이 지속적으로 트랜잭션을 수행하더라도 활성 HTTP 연결 기간을 최대 10분으로 제한해야 합니다.

연결을 열어 두어야 하는 최대 기간을 결정하는 것은 연결 지속성의 이점과 내부 시스템 리소스에 대한 연결을

이상적으로 할당하는 것입니다.

스토리지 노드에 대한 클라이언트 연결의 경우 활성 HTTP 연결을 제한하면 다음과 같은 이점이 있습니다.

- StorageGRID 시스템 전체에서 최적의 로드 밸런싱을 지원합니다.

시간이 지남에 따라 부하 분산 요구 사항이 변경되어 HTTP 연결이 더 이상 최적이 아닐 수 있습니다. 시스템은 클라이언트 애플리케이션이 각 트랜잭션에 대해 별도의 HTTP 연결을 설정할 때 최상의 부하 분산을 수행하지만, 이 방법은 지속적인 연결과 관련된 귀중한 이점을 무효화합니다.

- 클라이언트 응용 프로그램이 사용 가능한 공간이 있는 LDR 서비스로 HTTP 트랜잭션을 보낼 수 있도록 합니다.
- 유지보수 절차를 시작할 수 있습니다.

일부 유지 관리 절차는 진행 중인 모든 HTTP 연결이 완료된 후에만 시작됩니다.

부하 분산 서비스에 대한 클라이언트 연결의 경우 일부 유지 관리 절차를 즉시 시작할 수 있도록 개방 연결 기간을 제한하는 것이 유용할 수 있습니다. 클라이언트 연결 기간이 제한되지 않으면 활성 연결이 자동으로 종료되는 데 몇 분이 걸릴 수 있습니다.

동시 HTTP 연결의 이점

병렬 처리를 허용하도록 StorageGRID 시스템에 대한 여러 TCP/IP 연결을 열린 상태로 유지하여 성능을 향상시켜야 합니다. 최적의 병렬 연결 수는 다양한 요인에 따라 달라집니다.

동시 HTTP 연결은 다음과 같은 이점을 제공합니다.

- 지연 시간 단축

다른 트랜잭션이 완료될 때까지 기다리지 않고 즉시 트랜잭션을 시작할 수 있습니다.

- 처리량 향상

StorageGRID 시스템은 병렬 트랜잭션을 수행하고 총 트랜잭션 처리량을 늘릴 수 있습니다.

클라이언트 응용 프로그램은 여러 HTTP 연결을 설정해야 합니다. 클라이언트 응용 프로그램은 트랜잭션을 수행해야 하는 경우 트랜잭션을 현재 처리하지 않는 설정된 연결을 선택하여 즉시 사용할 수 있습니다.

각 StorageGRID 시스템의 토플로지는 동시 트랜잭션과 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 종종 여러 클라이언트 애플리케이션을 지원합니다. 동시 연결의 최대 수를 결정할 때 이 점을 명심하세요. 클라이언트 애플리케이션이 StorageGRID 시스템에 각각 연결을 설정하는 여러 소프트웨어 엔터티로 구성된 경우 엔터티 간의 모든 연결을 더합니다. 다음과 같은 상황에서는 동시 연결의 최대 수를 조정해야 할 수도 있습니다.

- StorageGRID 시스템의 토플로지는 시스템에서 지원할 수 있는 최대 동시 트랜잭션 및 연결 수에 영향을 줍니다.
- 대역폭이 제한된 네트워크에서 StorageGRID 시스템과 상호 작용하는 클라이언트 응용 프로그램은 개별 트랜잭션이 적절한 시간 내에 완료되도록 동시성 정도를 줄여야 할 수 있습니다.
- 많은 클라이언트 응용 프로그램이 StorageGRID 시스템을 공유하는 경우 시스템의 제한을 초과하지 않도록 동시성 정도를 줄여야 할 수 있습니다.

읽기 및 쓰기 작업을 위한 HTTP 연결 풀 분리

읽기 및 쓰기 작업에 별도의 HTTP 연결 풀을 사용하고 각 풀에 사용할 풀 수를 제어할 수 있습니다. 별도의 HTTP 연결 풀을 통해 트랜잭션을 보다 효율적으로 제어하고 로드 밸런싱을 수행할 수 있습니다.

클라이언트 애플리케이션은 검색 가능(읽기) 또는 저장 가능(쓰기) 부하를 생성할 수 있습니다. 읽기 및 쓰기 트랜잭션을 위한 별도의 HTTP 연결 풀을 사용하여 읽기 또는 쓰기 트랜잭션에 사용할 각 풀의 양을 조정할 수 있습니다.

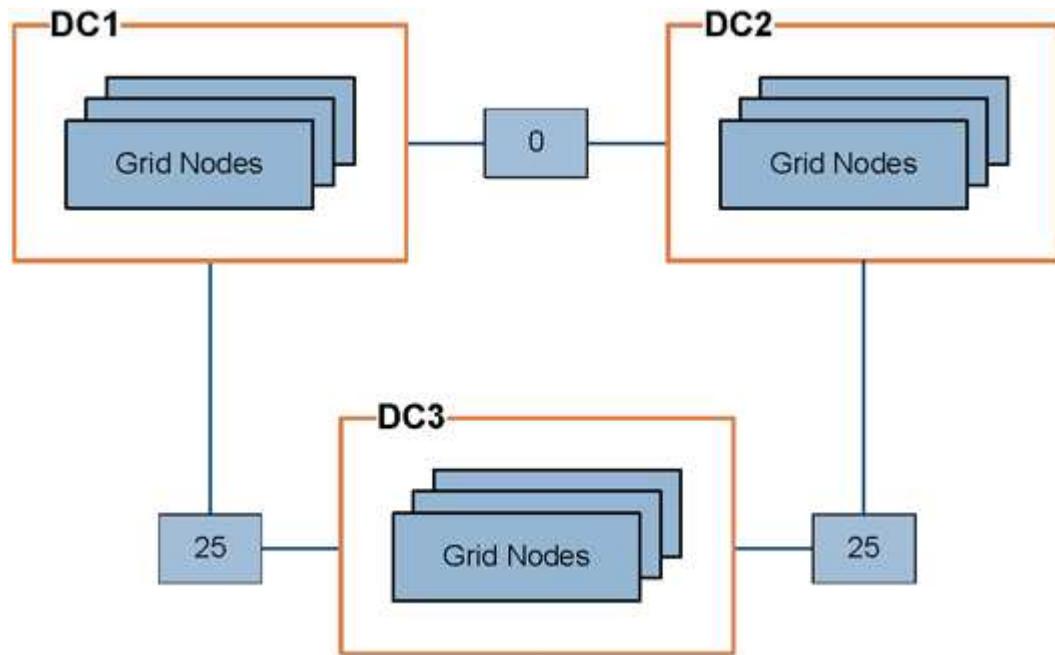
링크 비용 관리

링크 비용을 사용하면 둘 이상의 데이터 센터 사이트가 있을 때 요청된 서비스를 제공하는 데이터 센터 사이트의 우선 순위를 지정할 수 있습니다. 링크 비용을 조정하여 사이트 간 지연 시간을 반영할 수 있습니다.

링크 비용이란 무엇입니까?

- 링크 비용은 오브젝트 검색을 수행하는 데 사용되는 오브젝트 복사본의 우선 순위를 지정하는 데 사용됩니다.
- 링크 비용은 그리드 관리 API 및 테넌트 관리 API에서 사용할 내부 StorageGRID 서비스를 결정하는 데 사용됩니다.
- 링크 비용은 관리 노드 및 게이트웨이 노드의 부하 분산 서비스에서 클라이언트 연결을 연결하는 데 사용됩니다. 을 ["로드 균형 조정에 대한 고려 사항"](#)참조하십시오.

다이어그램에는 사이트 간에 구성된 링크 비용이 있는 세 개의 사이트 표가 표시됩니다.



- 관리 노드 및 게이트웨이 노드의 부하 분산 서비스는 동일한 데이터 센터 사이트의 모든 스토리지 노드 및 링크 비용이 0인 모든 데이터 센터 사이트에 클라이언트 연결을 균등하게 분산합니다.

이 예에서는 데이터 센터 사이트 1(DC1)의 게이트웨이 노드가 DC1의 스토리지 노드 및 DC2의 스토리지 노드로 클라이언트 접속을 균등하게 분산합니다. DC3의 게이트웨이 노드는 DC3의 스토리지 노드에만 클라이언트 접속을 전송합니다.

- 여러 개의 복제된 복제본으로 존재하는 객체를 검색할 때 StorageGRID는 가장 낮은 링크 비용을 가진 데이터 센터에서 복제본을 검색합니다.

이 예제에서 DC2의 클라이언트 응용 프로그램이 DC1과 DC3에 모두 저장된 개체를 검색할 경우 DC1에서 DC2로의 링크 비용은 DC3에서 DC2로의 링크 비용(25)보다 낮은 0이므로 DC1에서 개체를 검색합니다.

링크 비용은 특정 측정 단위가 없는 임의의 상대 숫자입니다. 예를 들어 링크 비용 50은 링크 비용 25보다 우선적으로 사용됩니다. 이 표에는 일반적으로 사용되는 링크 비용이 나와 있습니다.

링크	링크 비용	참고
데이터를 안전하게 보호	25(기본값)	WAN 링크로 연결된 데이터 센터
동일한 물리적 위치의 논리적 데이터 센터 사이트 간	0	LAN으로 연결된 동일한 물리적 건물 또는 캠퍼스의 논리적 데이터 센터

링크 비용을 업데이트합니다

사이트 간 지연 시간을 반영하기 위해 데이터 센터 사이트 간의 링크 비용을 업데이트할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"
- 당신은 가지고 있다"다른 그리드 구성 권한" .

단계

- 지원 > 기타 > *링크 비용*을 선택하세요.

Site Names (1 - 3 of 3)		
Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	
30	Data Center 3	

Link Costs				
		Link Destination		
Link Source	10	20	30	Actions
Data Center 1	0	25	25	

2. 링크 원본 *에서 사이트를 선택하고 * 링크 대상 *에서 0에서 100 사이의 비용 값을 입력합니다.

소스가 대상과 동일한 경우 링크 비용을 변경할 수 없습니다.

변경 사항을  취소하려면 * 복원 * 을 선택합니다.

3. Apply Changes * 를 선택합니다.

AutoSupport를 사용합니다

AutoSupport란 무엇입니까?

AutoSupport 기능을 사용하면 StorageGRID에서 상태 패키지를 NetApp 기술 지원으로 보낼 수 있습니다.

AutoSupport 사용하면 문제를 더 빨리 해결하는 데 도움이 됩니다. 기술 지원팀은 시스템의 저장 공간 요구 사항을 모니터링하고 새로운 노드나 사이트를 추가해야 하는지 여부를 결정하는 데 도움을 줍니다. 선택적으로 AutoSupport 패키지를 하나의 추가 목적으로 보낼 수 있습니다.

StorageGRID에는 두 가지 유형의 AutoSupport가 있습니다.

- * StorageGRID AutoSupport * 는 StorageGRID 소프트웨어 문제를 보고합니다. StorageGRID를 처음 설치할 때 기본적으로 사용됩니다. 필요한 경우 수행할 수 ["기본 AutoSupport 구성과 변경합니다"](#) 있습니다.



StorageGRID AutoSupport 활성화되어 있지 않으면 Grid Manager 대시보드에 메시지가 나타납니다. 해당 메시지에는 AutoSupport 구성 페이지에 대한 링크가 포함되어 있습니다. 메시지를 닫으면 AutoSupport 비활성화된 경우에도 브라우저 캐시가 지워질 때까지 메시지가 다시 나타나지 않습니다.

- * 어플라이언스 하드웨어 AutoSupport * 는 StorageGRID 어플라이언스 문제를 보고합니다. 반드시 해야 ["각 어플라이언스에 하드웨어 AutoSupport를 구성합니다"](#) 합니다.

Active IQ란 무엇입니까?

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

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

"Active IQ 디지털 자문 문서"

AutoSupport 패키지에 포함된 정보입니다

AutoSupport 패키지에는 다음과 같은 파일과 세부 정보가 들어 있습니다.

파일 이름입니다	필드를 선택합니다	설명
autosupport-history.xml	이 AutoSupport에 대한 AutoSupport 시퀀스 번호 + 대상 + 전달 상태 + 전송 시도 + AutoSupport 제목 + 전송 URI + 마지막 오류 + AutoSupport 파일 이름 + 생성 시간 + AutoSupport 압축 크기 + AutoSupport 압축 해제 크기 + 총 수집 시간(ms)	AutoSupport 기록 파일.
AutoSupport.xml을 참조하십시오	지원 문의 지원 + HTTP/HTTPS에 대한 지원 URL + 지원 주소 + AutoSupport OnDemand 상태 + AutoSupport OnDemand 서버 URL + AutoSupport OnDemand 폴링 간격	AutoSupport 상태 파일. 사용된 프로토콜, 기술 지원 URL 및 주소, 폴링 간격 및 활성화 또는 비활성화한 경우 OnDemand AutoSupport에 대한 자세한 내용은 에 나와 있습니다.
버킷.xml	버킷 ID + 계정 ID + 빌드 버전 + 위치 제약 구성 + 규정 준수 활성화 + 규정 준수 구성 + S3 오브젝트 잠금 활성화 + S3 오브젝트 잠금 구성 + 일관성 구성 + CORS 활성화 + CORS 구성 + 마지막 액세스 시간 활성화 + 정책 활성화 + 정책 구성 + 알림 설정 + 클라우드 미러 구성 + 활성화 검색 + 검색 구성 + 버킷 태깅 지원	버킷 수준의 구성 세부 정보 및 통계를 제공합니다. 버킷 구성의 예로는 플랫폼 서비스, 규정 준수 및 버킷 일관성이 있습니다.
그리드-설정.xml	특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	그리드 전체의 구성 정보 파일입니다. 그리드 인증서, 메타데이터 예약 공간, 그리드 전체 구성 설정(규정 준수, S3 오브젝트 잠금, 오브젝트 압축, 경고, syslog 및 ILM 구성), 삭제 코딩 프로필 세부 정보, DNS 이름 및 ILM 구성 등에 대한 정보가 포함되어 있습니다 " NMS 이름 ".
그리드 사양 XML	그리드 사양, 원시 XML	StorageGRID 구성 및 배포에 사용됩니다. 그리드 사양, NTP 서버 IP, DNS 서버 IP, 네트워크 토플로지 및 노드의 하드웨어 프로필을 포함합니다.
그리드 - tasks.xml	노드 + 서비스 경로 + 특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	그리드 작업(유지보수 절차) 상태 파일입니다. 그리드의 활성, 종료, 완료, 실패 및 보류 중인 작업에 대한 세부 정보를 제공합니다.

파일 이름입니다	필드를 선택합니다	설명
그리드.JSON	그리드 + 개정 + 소프트웨어 버전 + 설명 + 라이센스 + 암호 + DNS + NTP + 사이트 + 노드	그리드 정보
ILM-configuration.xml을 참조하십시오	특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	ILM 구성에 대한 특성 목록입니다.
ILM-STATUS.xml입니다	노드 + 서비스 경로 + 특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	ILM 메트릭 정보 파일 각 노드에 대한 ILM 평가율과 그리드 전체 메트릭에 대한 ILM 평가율이 포함되어 있습니다.
ILM.xml을 참조하십시오	ILM 원시 XML	ILM 활성 정책 파일 스토리지 폴 ID, 수집 동작, 필터, 규칙 및 설명과 같은 활성 ILM 정책에 대한 세부 정보를 제공합니다.
Log.TGZ(로그 TGZ)	n/a	로그 파일을 다운로드할 수 있습니다. 각 노드에서 및 servermanager.log 을 bycast- err.log 포함합니다.
매니페스트.xml	이 데이터에 대한 수집 순서 + AutoSupport 콘텐츠 파일 이름 + 이 데이터 항목에 대한 설명 + 수집된 바이트 수 + 수집에 소요된 시간 + 이 데이터 항목의 상태 + 이 데이터에 대한 AutoSupport 콘텐츠 형식 설명	AutoSupport 메타데이터와 모든 AutoSupport 파일에 대한 간략한 설명을 포함합니다.
nms-entities.xml입니다	속성 인덱스 + 엔터티 OID + 노드 ID + 장치 모델 ID + 장치 모델 버전 + 엔터티 이름	의 그룹 및 서비스 엔티티 " NMS 트리 " 그리드 토플로지 세부 정보를 제공합니다. 노드는 노드에서 실행되는 서비스를 기반으로 확인할 수 있습니다.
개체 - 상태 .xml	노드 + 서비스 경로 + 특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	배경 스캔 상태, 활성 전송, 전송 속도, 총 전송, 삭제 속도, 손상된 조각, 손실된 개체, 누락된 개체, 복구 시도, 스캔 속도, 예상 스캔 기간 및 복구 완료 상태를 포함한 개체 상태.
서버 상태 .xml	노드 + 서비스 경로 + 특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	서버 구성. 각 노드에 대한 세부 정보가 포함됩니다. 플랫폼 유형, 운영 체제, 설치된 메모리, 사용 가능한 메모리, 스토리지 연결, 스토리지 어플라이언스 새시 일련 번호, 스토리지 컨트롤러 오류 드라이브 수, 컴퓨팅 컨트롤러 새시 온도, 컴퓨팅 하드웨어, 컴퓨팅 컨트롤러 일련 번호, 전원 공급 장치, 드라이브 크기, 드라이브 유형.

파일 이름입니다	필드를 선택합니다	설명
서비스 상태 .xml	노드 + 서비스 경로 + 특성 ID + 특성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	서비스 노드 정보 파일입니다. 할당된 테이블 공간, 사용 가능한 테이블 공간, 데이터베이스의 Reaper 메트릭, 세그먼트 복구 기간, 복구 작업 기간, 자동 작업 재시작 및 자동 작업 종료와 같은 세부 정보가 포함됩니다.
저장 - 등급 .xml	스토리지 등급 ID + 스토리지 등급 이름 + 스토리지 노드 ID + 스토리지 노드 경로입니다	각 스토리지 노드에 대한 스토리지 등급 정의 파일입니다.
요약 - attributes.xml	그룹 OID + 그룹 경로 + 요약 속성 ID + 요약 속성 이름 + 값 + 인덱스 + 테이블 ID + 테이블 이름	StorageGRID 사용 정보를 요약하는 상위 수준의 시스템 상태 데이터입니다. 그리드 이름, 사이트 이름, 그리드당 및 사이트당 스토리지 노드 수, 라이센스 유형, 라이센스 용량 및 사용, 소프트웨어 지원 조건, S3 작업 세부 정보와 같은 세부 정보를 제공합니다.
System-alerts.xml을 참조하십시오	이름 + 심각도 + 노드 이름 + 경고 상태 + 사이트 이름 + 경고 트리거 시간 + 경고 해결 시간 + 규칙 ID + 노드 ID + 사이트 ID + 해제 + 기타 주석 + 기타 레이블	StorageGRID 시스템의 잠재적 문제를 나타내는 현재 시스템 알림입니다.
USERAGENTS.xml을 참조하십시오	사용자 에이전트 + 일 수 + 총 HTTP 요청 수 + 수집된 총 바이트 수 + 검색된 총 바이트 수 + 검색된 총 바이트 수 + 요청 가져오기 + 요청 가져오기 + 헤더 요청 + POST 요청 + 옵션 요청 + 평균 요청 시간(ms) + 평균 수신 요청 시간(ms) + 평균 삭제 요청 시간(ms) + 평균 헤드 요청 시간(ms) + 평균 POST 요청 시간(ms) + 평균 POST 요청 시간(ms) + 평균 요청 시간(ms)	애플리케이션 사용자 에이전트를 기준으로 한 통계입니다. 예를 들어, 사용자 에이전트당 Put/get/delete/head 작업 수와 각 작업의 총 바이트 크기입니다.
X-헤더-데이터	X-NetApp-ASUP-Generated-on+X-NetApp-ASUP-hostname+X-NetApp-ASUP-OS-버전+X-NetApp-ASUP-serial-num+X-NetApp-ASUP-subject+X-NetApp-ASUP-system-id+X-NetApp-ASUP-MODEL-NAME+	AutoSupport 헤더 데이터

AutoSupport를 구성합니다

기본적으로 StorageGRID AutoSupport 기능은 StorageGRID를 처음 설치할 때 활성화됩니다. 그러나 각 어플라이언스에서 하드웨어 AutoSupport를 구성해야 합니다. 필요에 따라 AutoSupport 구성을 변경할 수 있습니다.

StorageGRID AutoSupport의構성을 변경하려면 기본 관리자 노드에서만 변경하십시오. 반드시 각 제품에 부착해야 하드웨어 AutoSupport를 구성합니다합니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다.["지원되는 웹 브라우저"](#)
- 이 ["루트 액세스 권한"](#)있습니다.
- AutoSupport 패키지를 보내기 위해 HTTPS를 사용할 경우, 직접 또는 (인바운드 연결 필요 없음) 기본 관리자 노드에 대한 아웃바운드 인터넷 액세스를 제공한 ["프록시 서버 사용"](#)것입니다.
- StorageGRID AutoSupport 페이지에서 HTTP를 선택한 경우 AutoSupport 패키지를 HTTPS로 전달해야 ["프록시 서버를 구성했습니다"](#)합니다. NetApp의 AutoSupport 서버는 HTTP를 사용하여 전송된 패키지를 거부합니다.
- SMTP를 AutoSupport 패키지의 프로토콜로 사용할 경우 SMTP 메일 서버를 구성한 것입니다.

이 작업에 대해

다음 옵션 중 원하는 옵션을 조합하여 AutoSupport 패키지를 기술 지원으로 보낼 수 있습니다.

- * 매주 *: 매주 AutoSupport 패키지를 자동으로 발송합니다. 기본 설정: 사용.
- * 이벤트 트리거 *: 매 시간마다 또는 중요한 시스템 이벤트가 발생할 때 자동으로 AutoSupport 패키지를 전송합니다. 기본 설정: 사용.
- * 온디맨드 *: 기술 지원 부서에서 StorageGRID 시스템에서 AutoSupport 패키지를 자동으로 보내도록 요청하도록 허용합니다. 이는 문제가 활발하게 발생할 때 유용합니다(HTTPS AutoSupport 전송 프로토콜 필요). 기본 설정: 사용 안 함
- * 사용자 트리거 * : 언제든지 수동으로 AutoSupport 패키지를 보내십시오.
- 로그 수집:["수동으로 로그 파일과 시스템 데이터를 수집하고 AutoSupport 패키지를 보냅니다."](#) .

AutoSupport 패키지의 프로토콜을 지정합니다

다음 프로토콜을 사용하여 AutoSupport 패키지를 보낼 수 있습니다.

- * HTTPS *: 새 설치에 대한 기본 권장 설정입니다. 이 프로토콜은 포트 443을 사용합니다. 원하는 경우 [AutoSupport 온디맨드 기능을 활성화합니다](#) 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 포트 80을 사용합니다.
- **SMTP:** AutoSupport 패키지를 이메일로 보내려면 이 옵션을 사용하십시오.

설정한 프로토콜은 모든 유형의 AutoSupport 패키지를 보내는 데 사용됩니다.

단계

1. 지원 > 도구 > * AutoSupport* > *설정*을 선택하세요.

2. AutoSupport 패키지를 보내는 데 사용할 프로토콜을 선택합니다.
3. HTTPS * 를 선택한 경우 NetApp 지원 인증서(TLS 인증서)를 사용하여 기술 지원 서버에 대한 연결을 보호할지 여부를 선택합니다.
 - * 인증서 확인 * (기본값): AutoSupport 패키지 전송이 안전한지 확인합니다. NetApp 지원 인증서는 StorageGRID 소프트웨어와 함께 이미 설치되어 있습니다.
 - 인증서 확인 안 함 *: 인증서에 일시적인 문제가 있는 경우와 같이 인증서 유효성 검사를 사용하지 않는 것이 좋은 경우에만 이 옵션을 선택합니다.
4. 저장 * 을 선택합니다. 모든 주간, 사용자 트리거 및 이벤트 트리거 패키지는 선택한 프로토콜을 사용하여 전송됩니다.

Weekly AutoSupport를 비활성화합니다

기본적으로 StorageGRID 시스템은 일주일에 한 번 AutoSupport 패키지를 기술 지원부로 보내도록 구성되어 있습니다.

주간 AutoSupport 패키지의 전송 시기를 결정하려면 * AutoSupport * > * 결과 * 탭으로 이동하십시오. Weekly AutoSupport * 섹션에서 * 다음 예약 시간 * 의 값을 확인합니다.

언제든지 주간 AutoSupport 패키지의 자동 전송을 비활성화할 수 있습니다.

단계

1. 지원 > 도구 > * AutoSupport* > *설정*을 선택하세요.
2. Weekly AutoSupport * 활성화 확인란의 선택을 취소합니다.
3. 저장 * 을 선택합니다.

이벤트가 트리거된 **AutoSupport**를 비활성화합니다

기본적으로 StorageGRID 시스템은 한 시간마다 AutoSupport 패키지를 기술 지원으로 보내도록 구성되어 있습니다.

이벤트에 의해 트리거되는 AutoSupport는 언제든지 비활성화할 수 있습니다.

단계

1. 지원 > 도구 > * AutoSupport* > *설정*을 선택하세요.
2. 이벤트 트리거 AutoSupport* 활성화 확인란의 선택을 취소합니다.
3. 저장 * 을 선택합니다.

AutoSupport 온디맨드 를 활성화합니다

AutoSupport On Demand는 기술 지원이 활발하게 진행 중인 문제를 해결하는 데 도움이 될 수 있습니다.

기본적으로 AutoSupport On Demand는 비활성화되어 있습니다. 이 기능을 사용하도록 설정하면 기술 지원 부서에서 StorageGRID 시스템에 AutoSupport 패키지를 자동으로 보내도록 요청할 수 있습니다. 기술 지원 부서에서는 AutoSupport 주문형 쿼리에 대한 폴링 시간 간격을 설정할 수도 있습니다.

기술 지원 부서에서 AutoSupport On Demand를 활성화하거나 비활성화할 수 없습니다.

단계

1. 지원 > 도구 > * AutoSupport* > *설정*을 선택하세요.
2. 프로토콜에 대해 * HTTPS * 를 선택합니다.
3. Weekly AutoSupport * 활성화 확인란을 선택합니다.
4. AutoSupport On Demand * 확인란을 선택합니다.
5. 저장 * 을 선택합니다.

AutoSupport On Demand가 활성화되어 있으면 기술 지원 부서에서 AutoSupport On Demand 요청을 StorageGRID로 보낼 수 있습니다.

소프트웨어 업데이트 확인을 비활성화합니다

기본적으로 StorageGRID은 NetApp에 문의하여 사용 가능한 소프트웨어 업데이트가 있는지 확인합니다. StorageGRID 핫픽스 또는 새 버전을 사용할 수 있는 경우 새 버전이 StorageGRID 업그레이드 페이지에 표시됩니다.

필요에 따라 소프트웨어 업데이트 확인을 비활성화할 수도 있습니다. 예를 들어 시스템에 WAN 액세스가 없는 경우 다운로드 오류를 방지하려면 검사를 비활성화해야 합니다.

단계

1. 지원 > 도구 > * AutoSupport* > *설정*을 선택하세요.
2. 소프트웨어 업데이트 확인 * 확인란의 선택을 취소합니다.
3. 저장 * 을 선택합니다.

AutoSupport 대상을 추가합니다

AutoSupport를 활성화하면 상태 패키지와 상태 패키지가 기술 지원으로 전송됩니다. 모든 AutoSupport 패키지에 대해 하나의 추가 대상을 지정할 수 있습니다.

AutoSupport 패키지 전송에 사용되는 프로토콜을 확인하거나 변경하려면 에 있는 지침을 참조하십시오 [AutoSupport 패키지의 프로토콜을 지정합니다](#).



SMTP 프로토콜을 사용하여 AutoSupport 패키지를 추가 대상으로 보낼 수 없습니다.

단계

1. 지원 > 도구 > * AutoSupport* > *설정*을 선택하세요.
2. AutoSupport 대상 추가 활성화 * 를 선택합니다.
3. 다음을 지정합니다.

호스트 이름

추가 AutoSupport 대상 서버의 서버 호스트 이름 또는 IP 주소입니다.



하나의 추가 대상만 입력할 수 있습니다.

포트

추가 AutoSupport 대상 서버에 연결하는 데 사용되는 포트입니다. 기본값은 HTTP의 경우 포트 80, HTTPS의 경우 포트 443입니다.

인증서 검증

TLS 인증서를 사용하여 추가 대상에 대한 연결을 보호할지 여부를 나타냅니다.

- 인증서 유효성 검사를 사용하려면 * 인증서 확인 * 을 선택합니다.
- 인증서 확인 없이 AutoSupport 패키지를 보내려면 * 인증서 확인 안 함 * 을 선택합니다.

인증서에 일시적인 문제가 있는 경우와 같이 인증서 유효성 검사를 사용하지 않는 좋은 이유가 있는 경우에만 이 옵션을 선택합니다.

4. 인증서 확인 * 을 선택한 경우 다음을 수행합니다.

- a. CA 인증서의 위치를 찾습니다.
- b. CA 인증서 파일을 업로드합니다.

CA 인증서 메타데이터가 나타납니다.

5. 저장 * 을 선택합니다.

향후의 모든 주간, 이벤트 트리거 및 사용자 트리거 AutoSupport 패키지가 추가 대상으로 전송됩니다.

어플라이언스에 대해 AutoSupport를 구성합니다

어플라이언스용 AutoSupport가 StorageGRID 하드웨어 문제를 보고하며 StorageGRID AutoSupport은 StorageGRID 소프트웨어 문제를 보고하지만, SGF6112의 경우 StorageGRID AutoSupport에서 하드웨어 및 소프트웨어 문제를 모두 보고합니다. 추가 구성이 필요하지 않은 SGF6112를 제외하고 각 어플라이언스에서 AutoSupport를 구성해야 합니다. AutoSupport는 서비스 어플라이언스와 스토리지 어플라이언스에 대해 서로 다르게 구현됩니다.

SANtricity를 사용하여 각 스토리지 어플라이언스에 대해 AutoSupport를 사용하도록 설정할 수 있습니다. 초기 어플라이언스 설정 중 또는 어플라이언스 설치 후 SANtricity AutoSupport를 구성할 수 있습니다.

- SG6000 및 SG5700 어플라이언스의 경우, "[SANtricity 시스템 관리자에서 AutoSupport를 구성합니다](#)"

에서 AutoSupport 제공을 프록시 구성하는 경우 E-Series 어플라이언스의 AutoSupport 패키지를 StorageGRID AutoSupport에 포함할 수 "[SANtricity 시스템 관리자](#)"입니다.

StorageGRID AutoSupport은 DIMM 또는 HIC(호스트 인터페이스 카드) 오류와 같은 하드웨어 문제를 보고하지 않습니다. 하지만 일부 구성 요소 장애가 트리거될 수 "[하드웨어 경고](#)"입니다. BMC(베이스보드 관리 컨트롤러)가 있는 StorageGRID 어플라이언스의 경우 e-메일 및 SNMP 트랩을 구성하여 하드웨어 오류를 보고할 수 있습니다.

- "[BMC 알림에 대한 이메일 알림을 설정합니다](#)"
- "[BMC에 대한 SNMP 설정을 구성합니다](#)"

관련 정보

["NetApp 지원"](#)

AutoSupport 패키지를 수동으로 트리거합니다

StorageGRID 시스템 관련 문제 해결에 대한 기술 지원을 지원하기 위해 AutoSupport 패키지를

수동으로 전송할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."[지원되는 웹 브라우저](#)"
- 루트 액세스 권한 또는 기타 그리드 구성 권한이 있습니다.

단계

- 지원 > 도구 > * AutoSupport*를 선택하세요.
- 작업 * 탭에서 * 사용자 트리거 AutoSupport 전송 * 을 선택합니다.

StorageGRID NetApp 지원 사이트로 AutoSupport 패키지를 보내려고 시도합니다. 시도가 성공하면 결과 탭의 최근 결과 및 마지막 성공 시간 값이 업데이트됩니다. 문제가 있는 경우 최근 결과 값이 "실패"로 업데이트되고 StorageGRID AutoSupport 패키지를 다시 보내지 않습니다.

- 1분 후, 브라우저에서 AutoSupport 페이지를 새로 고쳐 최신 결과에 액세스하세요.



또한, 당신은 할 수 있습니다"[더 광범위한 로그 파일과 시스템 데이터를 수집합니다.](#)" NetApp 지원 사이트로 보내주세요.

AutoSupport 패키지 문제 해결

AutoSupport 패키지를 보내려는 시도가 실패하면 StorageGRID 시스템은 AutoSupport 패키지 유형에 따라 다른 조치를 취합니다. 지원 > 도구 > * AutoSupport * > *결과*를 선택하여 AutoSupport 패키지의 상태를 확인할 수 있습니다.

AutoSupport 패키지를 전송하지 못했으면 * AutoSupport * 페이지의 * 결과 * 탭에 "실패"가 표시됩니다.



AutoSupport 패키지를 NetApp에 전달하도록 프록시 서버를 구성한 경우"프록시 서버 구성 설정이 올바른지 확인합니다",

주별 AutoSupport 패키지 오류

주별 AutoSupport 패키지를 전송하지 못한 경우 StorageGRID 시스템은 다음 작업을 수행합니다.

- 가장 최근의 결과 속성을 다시 시도하도록 업데이트합니다.
- AutoSupport 패키지를 1시간 동안 4분마다 15회 재전송합니다.
- 전송 실패 1시간 후는 가장 최근의 결과 속성을 실패로 업데이트합니다.
- 다음 예약 시간에 AutoSupport 패키지 전송을 다시 시도합니다.
- NMS 서비스를 이용할 수 없어 패키지가 실패하는 경우, 7일 전에 패키지가 발송되는 경우, AutoSupport 스케줄을 정기적으로 유지
- NMS 서비스를 다시 사용할 수 있게 되면는 패키지를 7일 이상 보내지 않은 경우 즉시 AutoSupport 패키지를 보냅니다.

사용자가 트리거하거나 이벤트가 트리거된 AutoSupport 패키지 오류입니다

사용자가 트리거하거나 이벤트가 트리거된 AutoSupport 패키지를 전송하지 못하는 경우 StorageGRID 시스템은 다음

작업을 수행합니다.

1. 오류가 알려진 경우 오류 메시지를 표시합니다. 예를 들어, 사용자가 올바른 이메일 구성 설정을 제공하지 않고 SMTP 프로토콜을 선택하면 다음 오류가 표시됩니다. AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.
2. 패키지를 다시 보내지 않습니다.
3. 에 오류를 nms.log 기록합니다.

오류가 발생하고 SMTP가 선택된 프로토콜인 경우 StorageGRID 시스템의 이메일 서버가 올바르게 구성되었고 이메일 서버가 실행 중인지 확인하세요(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.

의 방법을 "[이메일 서버 설정을 구성합니다](#)" 알아보십시오.

AutoSupport 패키지 오류를 해결합니다

오류가 발생하고 SMTP가 선택한 프로토콜인 경우 StorageGRID 시스템의 이메일 서버가 올바르게 구성되어 있고 이메일 서버가 실행 중인지 확인합니다. AutoSupport 페이지에 다음과 같은 오류 메시지가 나타날 수 있습니다. AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.

StorageGRID를 통해 E-Series AutoSupport 패키지를 전송합니다

E-Series SANtricity System Manager AutoSupport 패키지는 스토리지 어플라이언스의 관리 포트가 아니라 StorageGRID 관리자 노드를 통해 기술 지원으로 보낼 수 있습니다.

E-Series 어플라이언스와 함께 AutoSupport 사용에 대한 자세한 내용은 ["E-Series 하드웨어 AutoSupport"](#) 참조하십시오.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인됩니다."지원되는 웹 브라우저"
- 이 "[스토리지 어플라이언스 관리자 또는 루트 액세스 권한](#)"있습니다.
- SANtricity AutoSupport를 구성했습니다.
 - SG6000 및 SG5700 어플라이언스의 경우, "[SANtricity 시스템 관리자에서 AutoSupport를 구성합니다](#)"



그리드 관리자를 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 펌웨어 8.70 이상이 있어야 합니다.

이 작업에 대해

E-Series AutoSupport 패키지는 스토리지 하드웨어에 대한 세부 정보를 포함하며 StorageGRID 시스템에서 보내는 다른 AutoSupport 패키지보다 구체적입니다.

SANtricity 시스템 관리자에서 어플라이언스의 관리 포트를 사용하지 않고 StorageGRID 관리자 노드를 통해 AutoSupport 패키지를 전송하도록 특수 프록시 서버 주소를 구성할 수 있습니다. 이러한 방식으로 전송된 AutoSupport 패키지는에서 전송하며 "[기본 설정 보낸 사람 관리자 노드](#)" "[관리자 프록시 설정](#)" 그리드 관리자에서 구성된 패키지를 사용합니다.

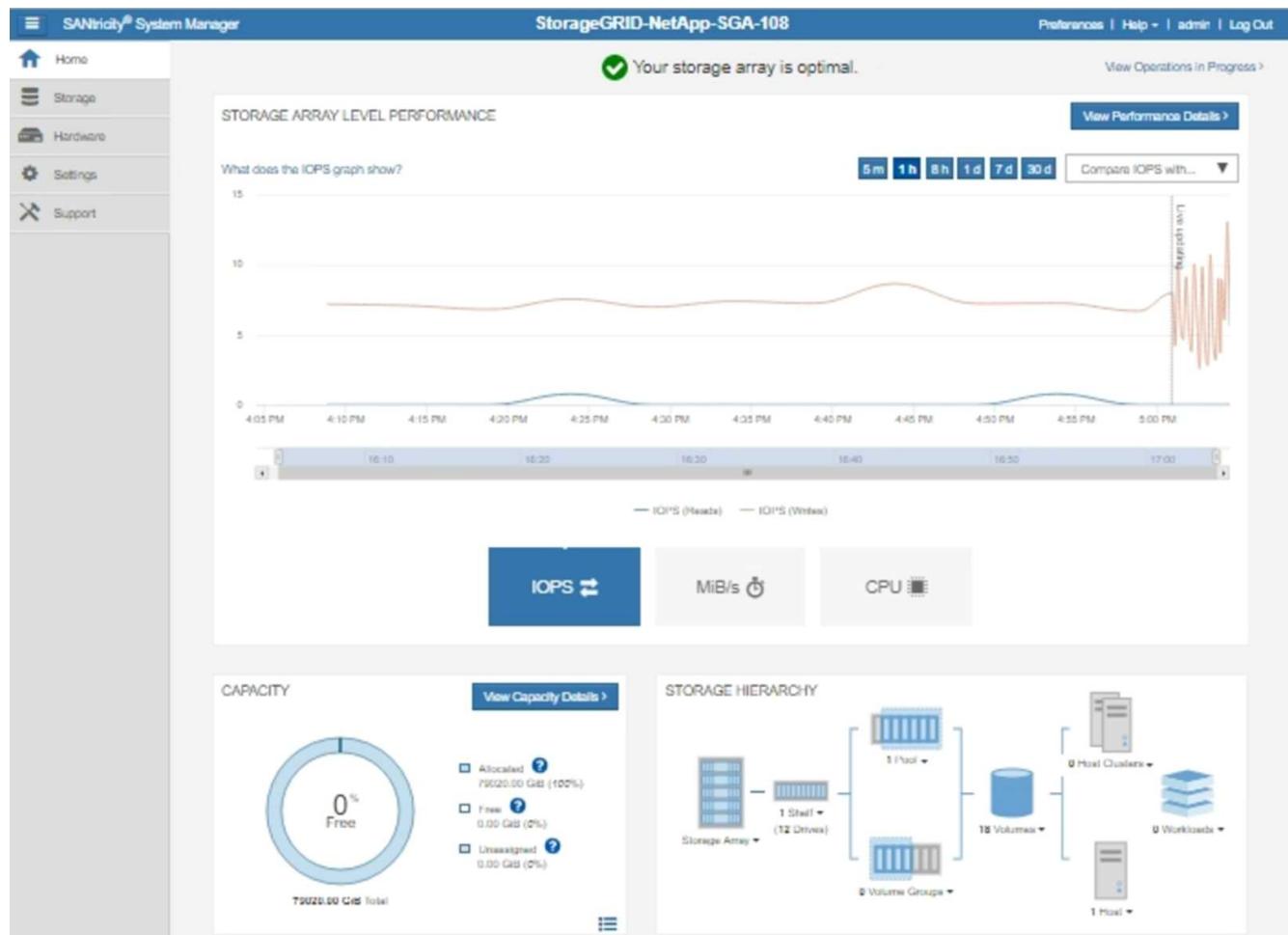


이 절차는 E-Series AutoSupport 패키지용 StorageGRID 프록시 서버를 구성하는 경우에만 적용됩니다. E-Series AutoSupport 구성에 대한 자세한 내용은을 참조하십시오 "[NetApp E-Series 및 SANtricity 문서](#)".

단계

1. 그리드 관리자에서 *노드*를 선택합니다.
2. 왼쪽의 노드 목록에서 구성할 스토리지 어플라이언스 노드를 선택합니다.
3. SANtricity 시스템 관리자 * 를 선택합니다.

SANtricity 시스템 관리자 홈 페이지가 나타납니다.



4. 지원 > 지원 센터 > * AutoSupport*를 선택하세요.

AutoSupport 작업 페이지가 나타납니다.

Support Resources

Diagnostics

AutoSupport

AutoSupport operations

AutoSupport status: Enabled

Enable/Disable AutoSupport Features

AutoSupport proactively monitors the health of your storage array and automatically sends support data ("dispatches") to the support team.

Configure AutoSupport Delivery Method

Connect to the support team via HTTPS, HTTP or Mail (SMTP) server delivery methods.

Schedule AutoSupport Dispatches

AutoSupport dispatches are sent daily at 03:06 PM UTC and weekly at 07:39 AM UTC on Thursday.

Send AutoSupport Dispatch

Automatically sends the support team a dispatch to troubleshoot system issues without waiting for periodic dispatches.

View AutoSupport Log

The AutoSupport log provides information about status, dispatch history, and errors encountered during delivery of AutoSupport dispatches.

Enable AutoSupport Maintenance Window

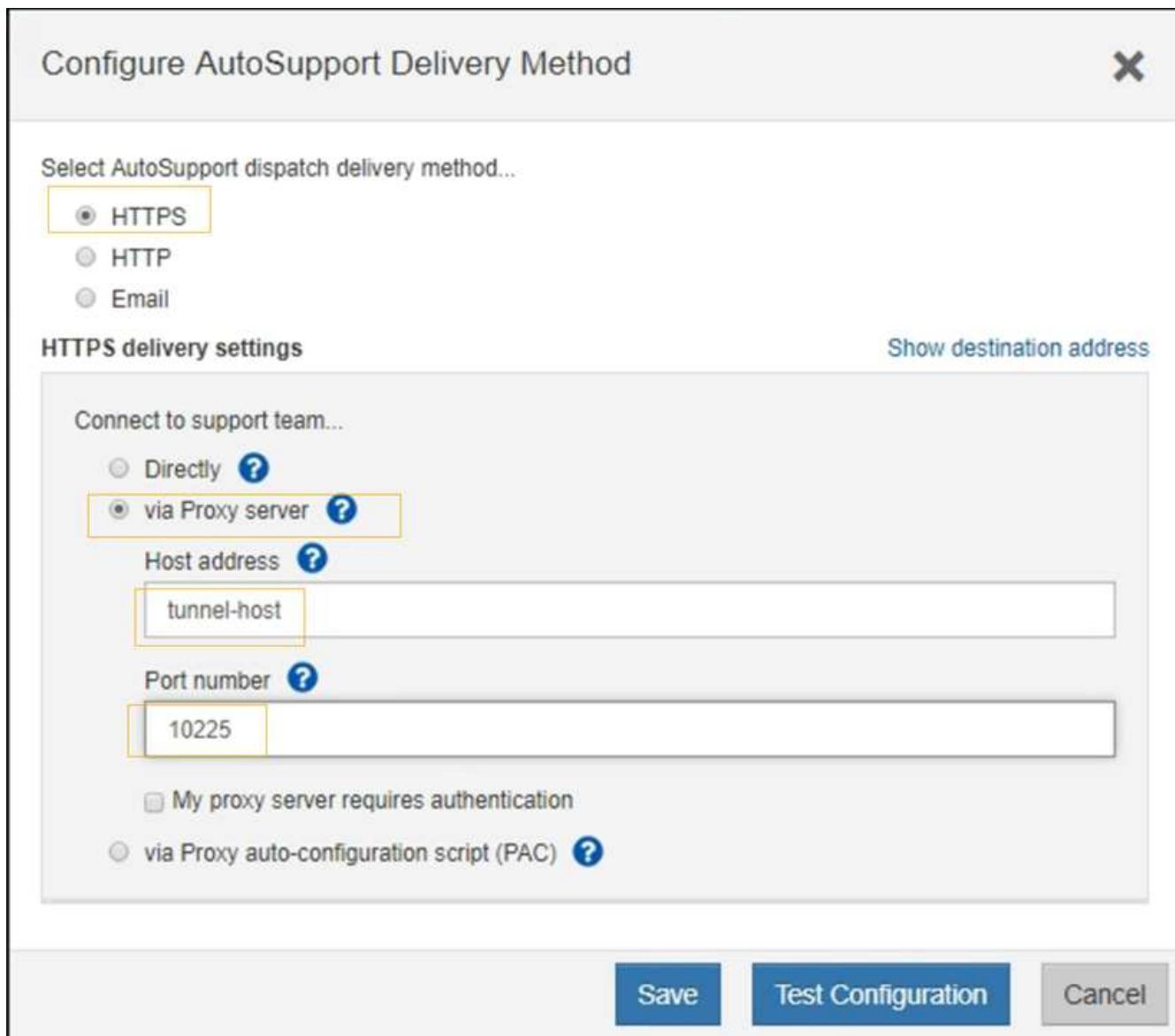
Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

Disable AutoSupport Maintenance Window

Disable AutoSupport Maintenance window to allow the storage array to generate support cases on component failures and other destructive actions.

5. AutoSupport 제공 방법 구성 * 을 선택합니다.

AutoSupport 배달 방법 구성 페이지가 나타납니다.



6. 전달 방법으로 * HTTPS * 를 선택합니다.



HTTPS를 활성화하는 인증서가 미리 설치되어 있습니다.

7. 프록시 서버를 통해 * 를 선택합니다.

8. 호스트 주소 * 에 대해 터널-호스트 입력합니다.

터널-호스트은 관리자 노드를 사용하여 E-Series AutoSupport 패키지를 전송하기 위한 특수 주소입니다.

9. 포트 번호 * 에 대해 10225 입력합니다.

10225은 어플라이언스의 E-Series 컨트롤러에서 AutoSupport 패키지를 수신하는 StorageGRID 프록시 서버의 포트 번호입니다.

10. AutoSupport 프록시 서버의 라우팅 및 구성을 테스트하려면 * 구성 테스트 * 를 선택합니다.

올바른 경우 녹색 배너에 "AutoSupport 구성이 확인되었습니다."라는 메시지가 나타납니다.

테스트에 실패하면 빨간색 배너에 오류 메시지가 나타납니다. StorageGRID DNS 설정 및 네트워킹을 확인하고 가 NetApp 지원 사이트에 연결할 수 있는지 "[기본 설정 보낸 사람 관리자 노드](#)" 확인한 후 테스트를 다시 시도하십시오.

11. 저장 * 을 선택합니다.

구성이 저장되고 "AutoSupport 배달 방법이 구성되었습니다."라는 확인 메시지가 나타납니다.

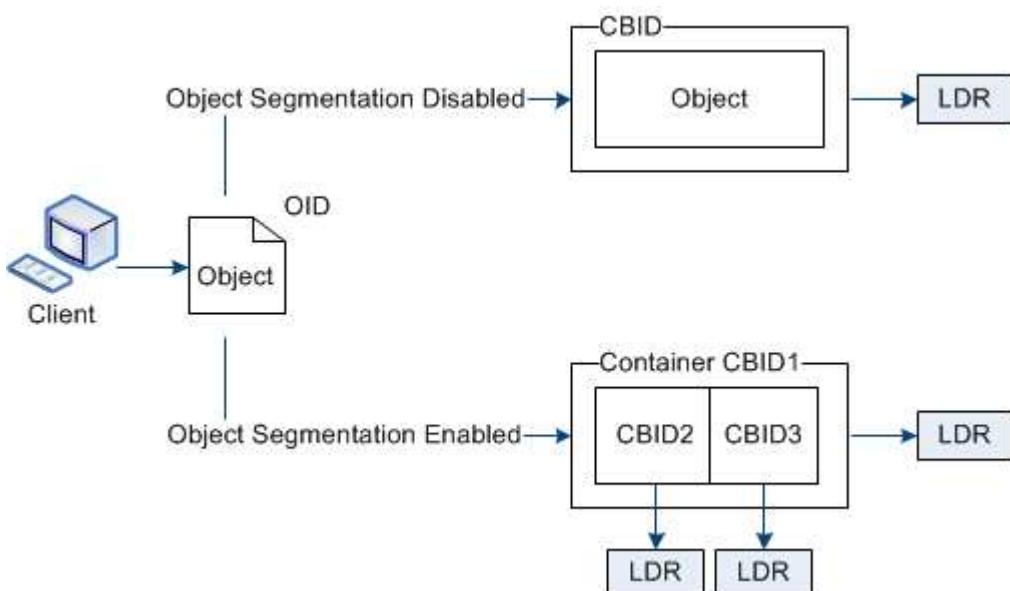
스토리지 노드 관리

스토리지 옵션을 사용합니다

객체 분할이란 무엇입니까?

객체 분할은 객체를 더 작은 고정 크기 객체 컬렉션으로 분할하여 큰 객체에 대한 스토리지 및 리소스 사용을 최적화하는 프로세스입니다. S3 다중 파트 업로드는 또한 각 파트를 나타내는 오브젝트와 함께 분할된 오브젝트를 만듭니다.

개체가 StorageGRID 시스템으로 수집되면 LDR 서비스는 개체를 세그먼트로 분할하고 모든 세그먼트의 헤더 정보를 내용으로 나열하는 세그먼트 컨테이너를 만듭니다.



세그먼트 컨테이너를 검색할 때 LDR 서비스는 세그먼트에서 원래 개체를 어셈블하고 개체를 클라이언트에 반환합니다.

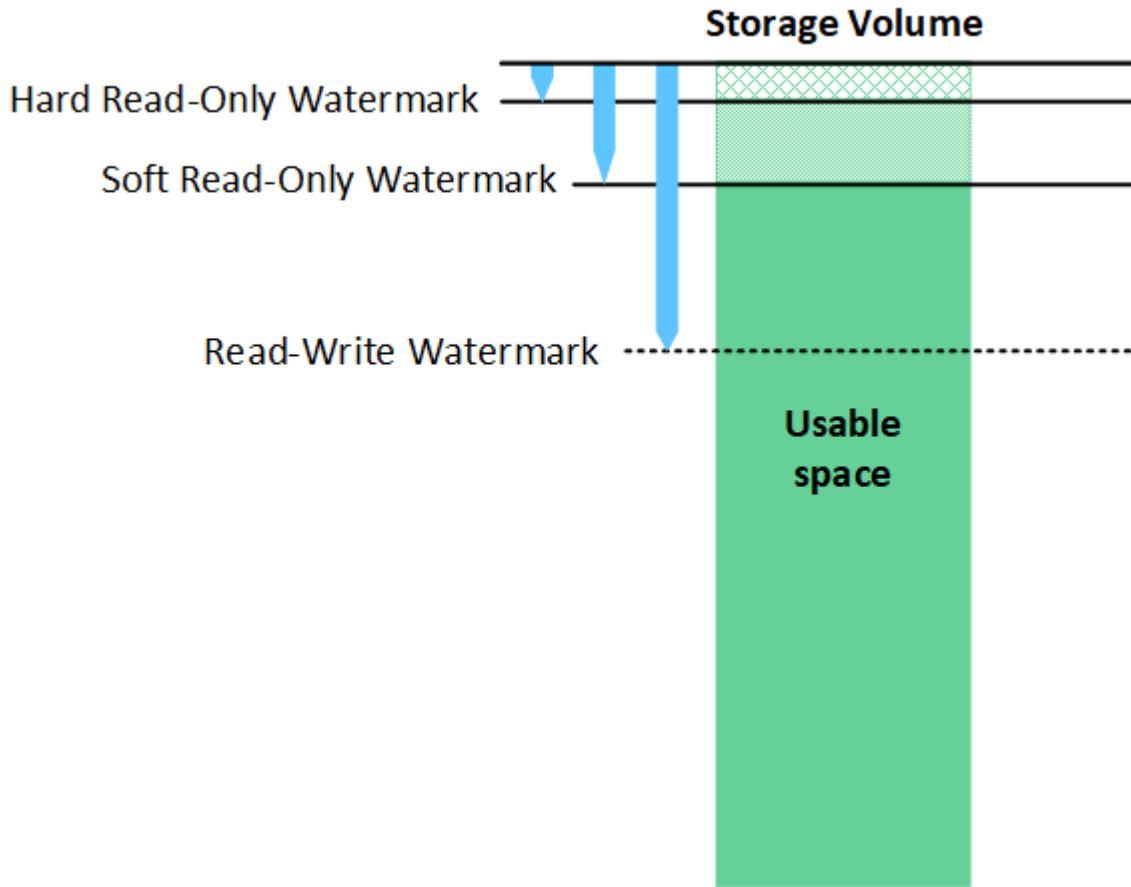
컨테이너와 세그먼트가 반드시 동일한 스토리지 노드에 저장되지는 않습니다. 컨테이너 및 세그먼트는 ILM 규칙에 지정된 스토리지 폴 내의 모든 스토리지 노드에 저장할 수 있습니다.

각 세그먼트는 StorageGRID 시스템에 의해 독립적으로 처리되고 관리되는 개체 및 저장된 개체와 같은 특성의 카운트에 기여합니다. 예를 들어, StorageGRID 시스템에 저장된 객체가 두 세그먼트로 분할되면 다음과 같이 수집 완료 후 관리 객체 값이 3씩 증가합니다.

```
segment container + segment 1 + segment 2 = three stored objects
```

스토리지 볼륨 워터마크란 무엇입니까?

StorageGRID는 세 개의 스토리지 볼륨 워터마크를 사용하여 공간이 매우 부족하기 전에 스토리지 노드가 읽기 전용 상태로 안전하게 전환되도록 하고 읽기 전용 상태로 전환된 스토리지 노드가 다시 읽기-쓰기로 전환되도록 합니다.



i 스토리지 볼륨 워터마크는 복제되고 삭제 코딩 오브젝트 데이터에 사용되는 공간에만 적용됩니다. 볼륨 0의 오브젝트 메타데이터용으로 예약된 공간에 대한 자세한 내용은 ["오브젝트 메타데이터 스토리지 관리"](#)를 참조하십시오.

소프트 읽기 전용 워터마크란 무엇입니까?

스토리지 볼륨 소프트 읽기 전용 워터마크 * 는 객체 데이터에 대한 스토리지 노드의 가용 공간이 가득 차있음을 나타내는 첫 번째 워터마크입니다.

스토리지 노드의 각 볼륨에 사용 가능한 공간이 해당 볼륨의 소프트 읽기 전용 워터마크보다 적은 경우 스토리지 노드는 `_READ-ONLY MODE`로 전환됩니다. 읽기 전용 모드는 스토리지 노드가 나머지 StorageGRID 시스템에 읽기 전용 서비스를 알리는 반면 보류 중인 모든 쓰기 요청을 처리하는 것을 의미합니다.

예를 들어 스토리지 노드의 각 볼륨에 10GB의 소프트 읽기 전용 워터마크가 있다고 가정합니다. 각 볼륨의 사용 가능한 공간이 10GB 미만이면 스토리지 노드가 소프트 읽기 전용 모드로 전환됩니다.

하드 읽기 전용 워터마크란 무엇입니까?

스토리지 볼륨 하드 읽기 전용 워터마크 * 는 오브젝트 데이터에 대한 노드의 사용 가능한 공간이 가득 차있음을

나타내는 다음 워터마크입니다.

볼륨의 여유 공간이 해당 볼륨의 하드 읽기 전용 워터마크보다 작으면 볼륨에 대한 쓰기가 실패합니다. 그러나 다른 볼륨에 대한 쓰기는 해당 볼륨의 여유 공간이 하드 읽기 전용 워터마크보다 작아질 때까지 계속될 수 있습니다.

예를 들어 스토리지 노드의 각 볼륨에 하드 읽기 전용 워터마크가 5GB라고 가정합니다. 각 볼륨의 사용 가능한 공간이 5GB 미만이면 스토리지 노드가 더 이상 쓰기 요청을 수락하지 않습니다.

하드 읽기 전용 워터마크는 항상 소프트 읽기 전용 워터마크보다 작습니다.

읽기-쓰기 워터마크란 무엇입니까?

스토리지 볼륨 읽기/쓰기 워터마크 * 는 읽기 전용 모드로 전환된 스토리지 노드에만 적용됩니다. 노드가 다시 읽기-쓰기가 될 수 있는 시기를 결정합니다. 스토리지 노드에 있는 스토리지 볼륨 중 하나의 사용 가능한 공간이 해당 볼륨의 읽기-쓰기 워터마크보다 크면 노드는 자동으로 읽기-쓰기 상태로 전환됩니다.

예를 들어 스토리지 노드가 읽기 전용 모드로 전환되었다고 가정해 보겠습니다. 또한 각 볼륨에 30GB의 읽기-쓰기 워터마크가 있다고 가정합니다. 볼륨의 사용 가능한 공간이 30GB로 증가하는 즉시 노드는 다시 읽기-쓰기가 됩니다.

읽기-쓰기 워터마크는 항상 소프트 읽기 전용 워터마크와 하드 읽기 전용 워터마크보다 큽니다.

스토리지 볼륨 워터마크를 봅니다

현재 워터마크 설정 및 시스템 최적화 값을 볼 수 있습니다. 최적화된 워터마크를 사용하지 않는 경우 설정을 조정할 수 있는지 또는 조정할 수 있는지 여부를 결정할 수 있습니다.

시작하기 전에

- StorageGRID 11.6 이상으로 업그레이드를 완료했습니다.
- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 이 "[루트 액세스 권한](#)"있습니다.

현재 워터마크 설정을 봅니다

그리드 관리자에서 현재 스토리지 워터마크 설정을 볼 수 있습니다.

단계

1. 지원 > 기타 > *저장소 워터마크*를 선택하세요.
 2. 스토리지 워터마크 페이지에서 최적화된 값 사용 확인란을 확인합니다.
 - 이 확인란을 선택하면 스토리지 노드의 크기와 볼륨의 상대적 용량에 따라 모든 스토리지 노드의 모든 스토리지 볼륨에 대해 세 개의 워터마크가 모두 최적화됩니다.
- 이 설정이 기본값이며 권장 설정입니다. 이 값을 업데이트하지 마십시오. 선택적으로, 할 수 [최적화된 스토리지 워터마크를 봅니다](#)있습니다.
- 최적화된 값 사용 확인란이 선택되어 있지 않으면 사용자 지정(최적화되지 않은) 워터마크가 사용됩니다. 사용자 지정 배경무늬 설정은 사용하지 않는 것이 좋습니다. 의 지침에 "[낮은 읽기 전용 배경무늬 재정의 알림 문제 해결](#)"따라 설정을 조정할 수 있는지 또는 조정할 수 있는지 결정합니다.

사용자 지정 워터마크 설정을 지정할 때는 0보다 큰 값을 입력해야 합니다.

최적화된 스토리지 워터마크를 봅니다

StorageGRID는 두 가지 Prometheus 메트릭을 사용하여 스토리지 볼륨 소프트 읽기 전용 워터마크에 대해 계산된 최적화된 값을 표시합니다. 그리드의 각 스토리지 노드에 대해 최적화된 최소 및 최대 값을 볼 수 있습니다.

1. 지원 > 도구 > *측정항목*을 선택하세요.
2. Prometheus 섹션에서 Prometheus 사용자 인터페이스에 액세스할 링크를 선택합니다.
3. 권장되는 최소 소프트 읽기 전용 워터마크를 보려면 다음 Prometheus 메트릭을 입력하고 * Execute * 를 선택합니다.

```
storagegrid_storage_volume_minimum_optimized_soft_READONLY_watermark
```

마지막 열에는 각 스토리지 노드의 모든 스토리지 볼륨에 대한 소프트 읽기 전용 워터마크의 최소화된 값이 표시됩니다. 이 값이 스토리지 볼륨 소프트 읽기 전용 워터마크에 대한 사용자 지정 설정보다 크면 스토리지 노드에 대해 * 낮은 읽기 전용 워터마크 무시 * 경고가 트리거됩니다.

4. 권장되는 최대 소프트 읽기 전용 워터마크를 보려면 다음 Prometheus 메트릭을 입력하고 * Execute * 를 선택합니다.

```
storagegrid_storage_volume_maximum_optimized_soft_READONLY_watermark
```

마지막 열에는 각 스토리지 노드의 모든 스토리지 볼륨에 대한 소프트 읽기 전용 워터마크의 최대 최적화 값이 표시됩니다.

오브젝트 메타데이터 스토리지 관리

StorageGRID 시스템의 오브젝트 메타데이터 용량은 해당 시스템에 저장할 수 있는 최대 오브젝트 수를 제어합니다. StorageGRID 시스템에 새 개체를 저장할 충분한 공간이 있는지 확인하려면 StorageGRID에서 개체 메타데이터를 저장하는 위치와 방법을 알아야 합니다.

오브젝트 메타데이터란?

개체 메타데이터는 개체를 설명하는 정보입니다. StorageGRID는 오브젝트 메타데이터를 사용하여 그리드 전체의 모든 오브젝트의 위치를 추적하고 각 오브젝트의 라이프사이클 관리를 제공합니다.

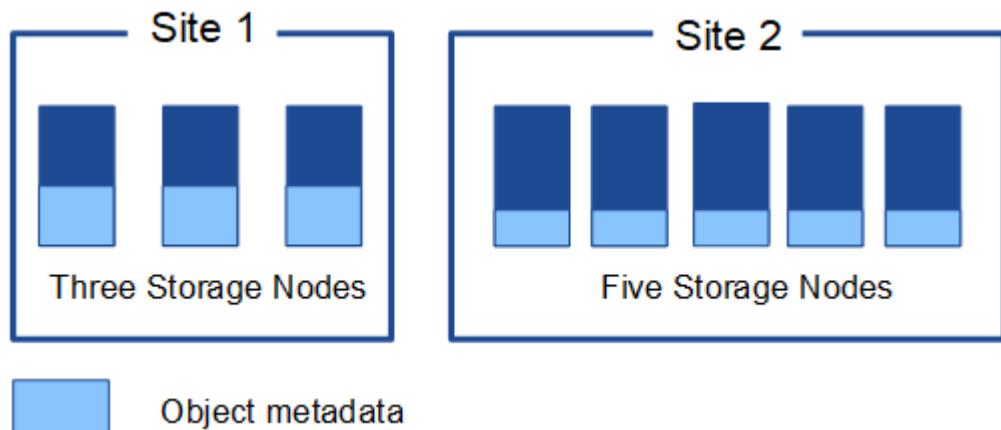
StorageGRID의 개체에 대한 개체 메타데이터에는 다음 유형의 정보가 포함됩니다.

- 각 오브젝트의 고유 ID(UUID), 오브젝트 이름, S3 버킷의 이름, 테넌트 계정 이름 또는 ID, 오브젝트의 논리적 크기, 오브젝트를 처음 생성한 날짜와 시간, 오브젝트를 마지막으로 수정한 날짜와 시간이 포함된 시스템 메타데이터
- 객체와 연결된 모든 사용자 메타데이터 키 값 쌍입니다.
- S3 오브젝트의 경우 오브젝트와 연결된 오브젝트 태그 키 값 쌍이 됩니다.
- 복제된 오브젝트 복사본의 경우 각 복제본의 현재 스토리지 위치입니다.
- 삭제 코딩 오브젝트 복사본의 경우 각 분절의 현재 스토리지 위치입니다.
- 클라우드 스토리지 풀의 오브젝트 복사본의 경우 외부 버킷의 이름 및 오브젝트의 고유 식별자를 비롯한 오브젝트의 위치가 포함됩니다.
- 분할된 오브젝트 및 다중 파트 오브젝트의 경우 세그먼트 식별자 및 데이터 크기가 사용됩니다.

오브젝트 메타데이터는 어떻게 저장됩니까?

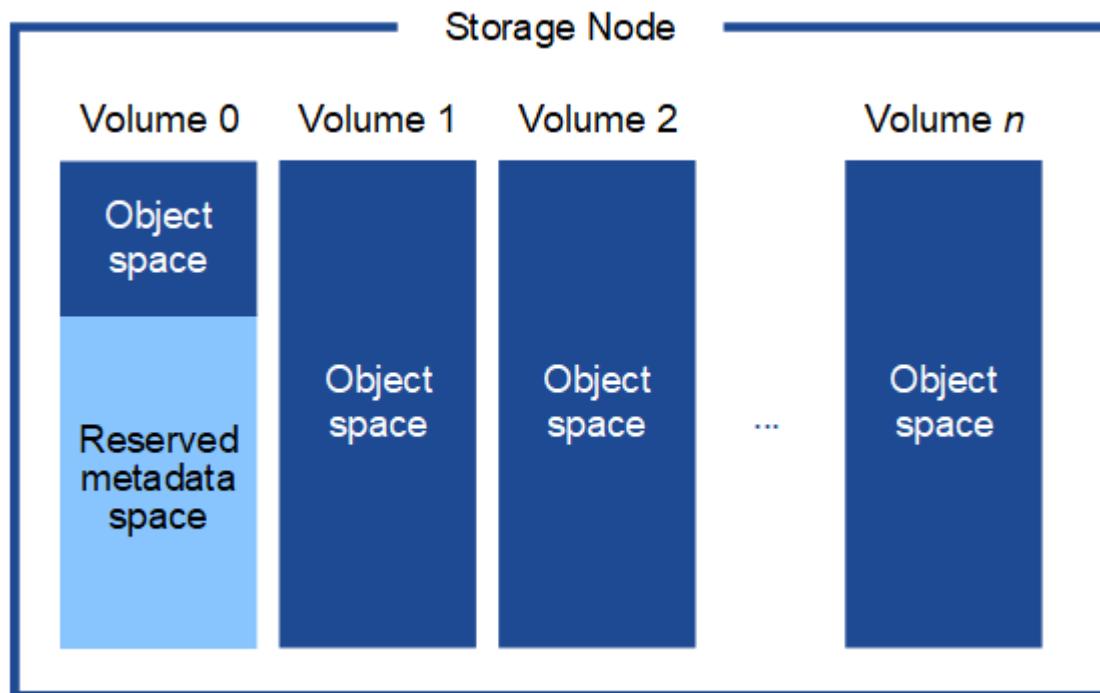
StorageGRID는 오브젝트 메타데이터를 Cassandra 데이터베이스에 유지하며, 이 데이터베이스는 오브젝트 데이터와 독립적으로 저장됩니다. 이중화를 제공하고 개체 메타데이터를 손실로부터 보호하기 위해 StorageGRID는 각 사이트의 시스템 모든 개체에 대한 메타데이터 복사본을 3개 저장합니다.

이 그림은 두 사이트의 스토리지 노드를 나타냅니다. 각 사이트에는 동일한 양의 오브젝트 메타데이터가 있으며 각 사이트의 메타데이터는 해당 사이트의 모든 스토리지 노드 간에 세분됩니다.



오브젝트 메타데이터는 어디에 저장됩니까?

이 그림은 단일 스토리지 노드의 스토리지 볼륨을 나타냅니다.



그림에 나와 있는 것처럼 StorageGRID는 각 스토리지 노드의 스토리지 볼륨 0에 객체 메타데이터를 위한 공간을 예약합니다. 이 경우 예약된 공간을 사용하여 오브젝트 메타데이터를 저장하고 중요한 데이터베이스 작업을 수행합니다. 스토리지 볼륨 0 및 스토리지 노드의 다른 모든 스토리지 볼륨의 나머지 공간은 오브젝트 데이터(복제된 복사본 및 삭제 코딩 단편)에만 사용됩니다.

특정 스토리지 노드의 개체 메타데이터에 예약된 공간의 양은 아래에 설명된 여러 요인에 따라 달라집니다.

메타데이터 예약 공간 설정입니다

Metadata Reserved space_는 모든 스토리지 노드의 볼륨 0에서 메타데이터로 예약될 공간의 양을 나타내는 시스템 차원의 설정입니다. 표에 나와 있는 것처럼 이 설정의 기본값은 다음을 기반으로 합니다.

- StorageGRID를 처음 설치할 때 사용한 소프트웨어 버전입니다.
- 각 스토리지 노드의 RAM 용량입니다.

초기 StorageGRID 설치에 사용되는 버전입니다	스토리지 노드의 RAM 크기입니다	기본 메타데이터 예약 공간 설정입니다
11.5에서 12.0까지	그리드의 각 스토리지 노드에 128GB 이상	8TB(8,000GB)
	그리드의 스토리지 노드에서 128GB 미만	3TB(3,000GB)
11.1 - 11.4	한 사이트의 각 스토리지 노드에 128GB 이상	4TB(4,000GB)
	각 사이트의 스토리지 노드에 128GB 미만	3TB(3,000GB)
11.0 이전 버전	금액	2TB(2,000GB)

메타데이터 예약 공간 설정을 봅니다

StorageGRID 시스템의 메타데이터 예약 공간 설정을 보려면 다음 단계를 수행하십시오.

단계

1. 구성 > 시스템 > *저장소 설정*을 선택합니다.
2. 저장소 설정 페이지에서 * 메타데이터 예약 공간 * 섹션을 확장합니다.

StorageGRID 11.8 이상의 경우 메타데이터 예약 공간 값은 100GB 이상 1PB 이하여야 합니다.

각 스토리지 노드에 128GB 이상의 RAM이 있는 새로운 StorageGRID 11.6 이상 설치의 기본 설정은 8,000GB(8TB)입니다.

메타데이터의 실제 예약 공간입니다

시스템 차원 메타데이터 예약 공간 설정과 달리 각 스토리지 노드에 대해 _actual reserved space_for object 메타데이터가 결정됩니다. 지정된 스토리지 노드에 대해 메타데이터의 실제 예약된 공간은 노드의 볼륨 0 크기 및 시스템 차원의 메타데이터 예약 공간 설정에 따라 달라집니다.

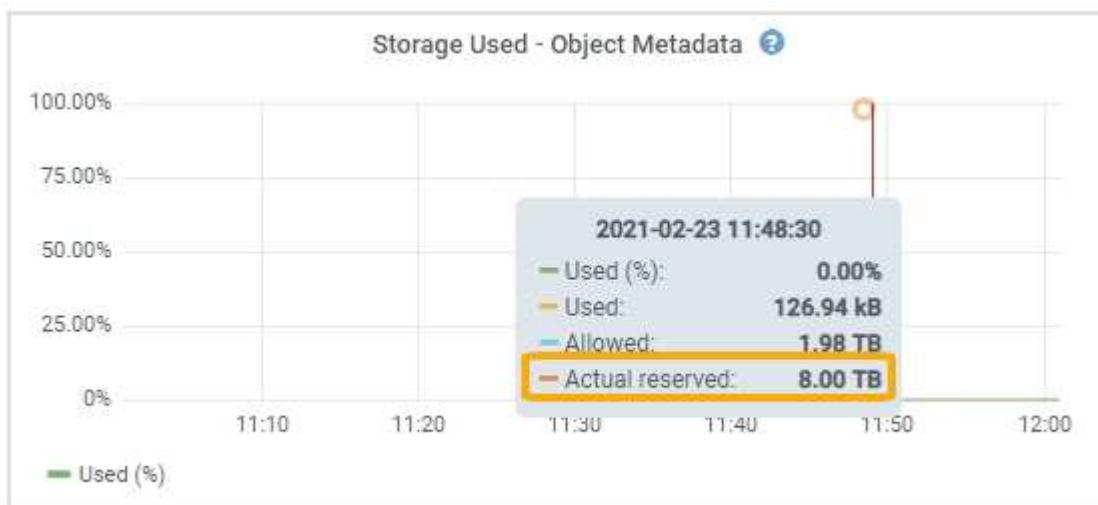
노드에 대한 볼륨 0의 크기입니다	메타데이터의 실제 예약 공간입니다
500GB 미만(비운영 용도)	볼륨 0의 10%
500GB 이상 + 또는 + 메타데이터 전용 스토리지 노드	다음 값 중 더 작은 값: <ul style="list-style-type: none">• 볼륨 0• 메타데이터 예약 공간 설정입니다• 참고 *: 메타데이터 전용 스토리지 노드에는 하나의 rangedb만 필요합니다.

메타데이터에 대한 실제 예약 공간을 봅니다

특정 스토리지 노드의 메타데이터에 대한 실제 예약 공간을 보려면 다음 단계를 따르십시오.

단계

1. 그리드 관리자에서 노드 > *스토리지 노드*를 선택합니다.
2. Storage * 탭을 선택합니다.
3. 커서를 Storage Used - Object Metadata 차트 위에 놓고 * Actual Reserved * 값을 찾습니다.



스크린샷에서 * Actual Reserved * 값은 8TB입니다. 이 스크린샷은 새 StorageGRID 11.6 설치의 대규모 스토리지 노드에 대한 것입니다. 이 스토리지 노드의 시스템 차원 메타데이터 예약 공간 설정이 볼륨 0보다 작기 때문에 이 노드의 실제 예약 공간은 메타데이터 예약 공간 설정과 같습니다.

실제 예약 메타데이터 공간의 예

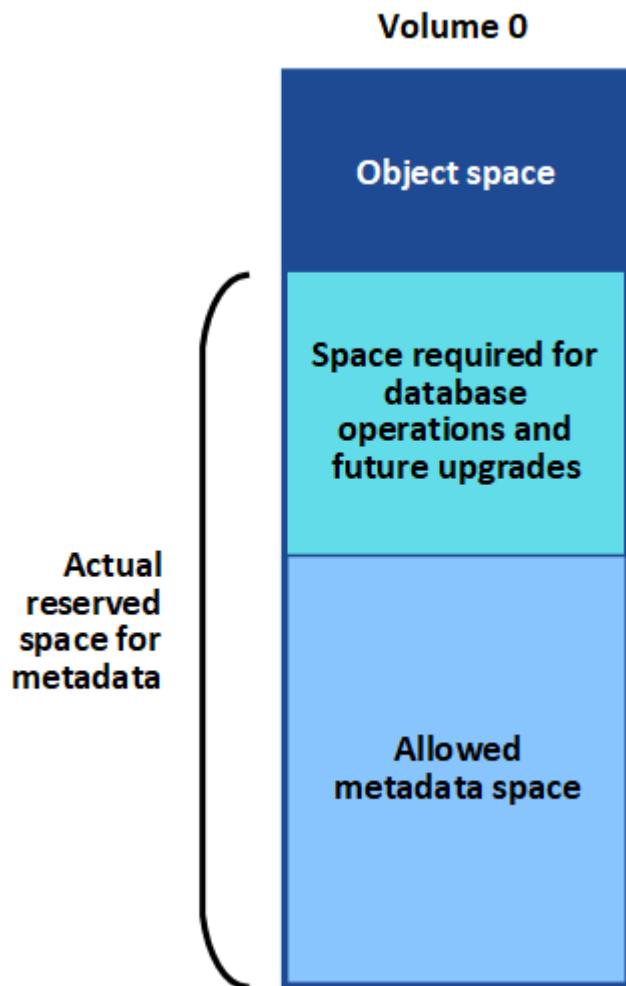
버전 11.7 이상을 사용하여 새 StorageGRID 시스템을 설치한다고 가정합니다. 이 예에서는 각 스토리지 노드에 128MB 이상의 RAM이 있고 SN1(Storage Node 1)의 볼륨 0이 6TB라고 가정합니다. 다음 값을 기준으로 합니다.

- 시스템 전체 * 메타데이터 예약 공간 * 이 8TB로 설정되어 있습니다. (각 스토리지 노드에 128GB RAM이 넘는 경우 새 StorageGRID 11.6 이상 설치의 기본값입니다.)
- SN1의 메타데이터에 대한 실제 예약 공간은 6TB입니다. (볼륨 0이 * Metadata Reserved space * 설정보다 작기

때문에 전체 볼륨이 예약됩니다.)

허용된 메타데이터 공간입니다

각 스토리지 노드의 실제 메타데이터 예약 공간은 오브젝트 메타데이터(*allowed metadata space*)에 사용할 수 있는 공간과 필수 데이터베이스 작업(예: 컴팩션 및 복구)에 필요한 공간, 향후 하드웨어 및 소프트웨어 업그레이드로 세분화됩니다. 허용되는 메타데이터 공간은 전체 오브젝트 용량을 관리합니다.



다음 표에서는 StorageGRID가 노드에 대한 메모리 양과 메타데이터에 대한 실제 예약된 공간을 기준으로 서로 다른 스토리지 노드에 대해 * 허용된 메타데이터 공간 * 을 계산하는 방법을 보여 줍니다.

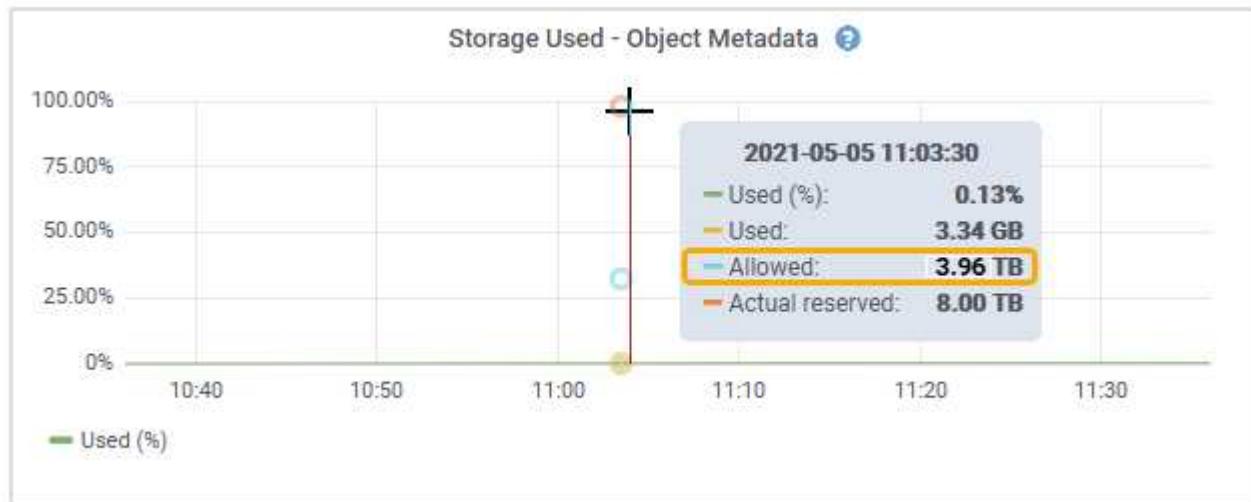
		• 스토리지 노드의 메모리 양 *	
	lt; 128GB(&L)	GT; = 128GB(&G)	• 메타데이터에 대한 실제 예약 공간 *
lt; = 4 TB.&L	메타데이터를 위해 실제 예약된 공간의 60%, 최대 1.32TB	메타데이터를 위해 실제 예약된 공간의 60%, 최대 1.98TB	GT, 4TB(&G)

허용된 메타데이터 공간을 봅니다

스토리지 노드에 대해 허용되는 메타데이터 공간을 보려면 다음 단계를 따르십시오.

단계

1. 그리드 관리자에서 *노드*를 선택합니다.
2. 스토리지 노드를 선택합니다.
3. Storage * 탭을 선택합니다.
4. 커서를 Storage Used-object 메타데이터 차트 위에 놓고 * Allowed * 값을 찾습니다.



스크린샷에서 * Allowed * 값은 3.96TB로, 메타데이터에 대한 실제 예약된 공간이 4TB를 초과하는 스토리지 노드의 최대값입니다.

허용 * 값은 다음 Prometheus 메트릭에 해당합니다.

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

허용되는 메타데이터 공간의 예

버전 11.6를 사용하여 StorageGRID 시스템을 설치한다고 가정합니다. 이 예에서는 각 스토리지 노드에 128MB 이상의 RAM이 있고 SN1(Storage Node 1)의 볼륨 0이 6TB라고 가정합니다. 다음 값을 기준으로 합니다.

- 시스템 전체 * 메타데이터 예약 공간 * 이 8TB로 설정되어 있습니다. (각 스토리지 노드에 128GB RAM이 넘는 경우 StorageGRID 11.6 이상의 기본값입니다.)
- SN1의 메타데이터에 대한 실제 예약 공간은 6TB입니다. (볼륨 0이 * Metadata Reserved space * 설정보다 작기 때문에 전체 볼륨이 예약됩니다.)
- SN1의 메타데이터에 허용되는 공간은 3TB이며 [메타데이터에 허용되는 공간에 대한 테이블입니다](#), 이 계산 결과는 메타데이터 -1TB의 실제 예약된 공간) × 60%(최대 3.96TB)입니다.

서로 다른 크기의 스토리지 노드가 오브젝트 용량에 미치는 영향

위에서 설명한 것처럼 StorageGRID는 각 사이트의 스토리지 노드에 오브젝트 메타데이터를 균등하게 분산합니다. 따라서 사이트에 크기가 다른 스토리지 노드가 있는 경우 사이트의 가장 작은 노드가 사이트의 메타데이터 용량을

결정합니다.

다음 예제를 고려해 보십시오.

- 크기가 다른 세 개의 스토리지 노드가 포함된 단일 사이트 그리드가 있습니다.
- 메타데이터 예약 공간 * 설정은 4TB입니다.
- 스토리지 노드에는 실제 예약된 메타데이터 공간과 허용되는 메타데이터 공간에 대해 다음 값이 있습니다.

스토리지 노드	볼륨 0의 크기입니다	실제 예약된 메타데이터 공간입니다	허용된 메타데이터 공간입니다
SN1을 참조하십시오	2.2TB	2.2TB	1.32TB
에스엔2	5TB	4TB	1.98TB
SN3을 참조하십시오	6TB	4TB	1.98TB

개체 메타데이터는 사이트의 스토리지 노드에 균등하게 분산되므로 이 예제의 각 노드는 1.32TB의 메타데이터만 보유할 수 있습니다. sn2 및 SN3에 대해 허용되는 추가 0.66TB의 메타데이터 공간은 사용할 수 없습니다.



마찬가지로, StorageGRID는 각 사이트에서 StorageGRID 시스템의 모든 개체 메타데이터를 유지하므로 StorageGRID 시스템의 전체 메타데이터 용량은 가장 작은 사이트의 개체 메타데이터 용량에 따라 결정됩니다.

또한 오브젝트 메타데이터 용량은 최대 오브젝트 수를 제어하므로 한 노드에 메타데이터 용량이 부족한 경우 이 그리드는 효과적으로 가득 차게 됩니다.

관련 정보

- 각 스토리지 노드의 오브젝트 메타데이터 용량을 모니터링하는 방법은 의 지침을 참조하십시오.["StorageGRID 모니터링"](#)
- 새 스토리지 노드를 추가하여 시스템의 오브젝트 메타데이터 용량을 ["그리드를 확장합니다"](#) 늘립니다.

메타데이터 예약 공간 증가 설정을 사용합니다

스토리지 노드가 RAM 및 사용 가능한 공간에 대한 특정 요구 사항을 충족할 경우 메타데이터 예약 공간 시스템 설정을 늘릴 수 있습니다.

필요한 것

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."지원되는 웹 브라우저"

- 당신은 가지고있다"루트 액세스 권한 또는 기타 그리드 구성 권한" .

이 작업에 대해

시스템 전체의 메타데이터 예약 공간 설정을 수동으로 최대 8TB까지 늘릴 수 있습니다.

다음 두 문이 모두 참인 경우에만 시스템 전체의 메타데이터 예약된 공간 설정 값을 늘릴 수 있습니다.

- 시스템의 모든 사이트에 있는 스토리지 노드에는 각각 128GB 이상의 RAM이 있습니다.
- 시스템의 모든 사이트에 있는 스토리지 노드에는 스토리지 볼륨 0에 사용 가능한 공간이 충분합니다.

이 설정을 높이는 경우 모든 스토리지 노드의 스토리지 볼륨 0에서 오브젝트 스토리지에 사용할 수 있는 공간을 동시에 줄일 수 있습니다. 따라서 메타데이터 예약 공간을 예상 오브젝트 메타데이터 요구 사항에 따라 8TB 미만의 값으로 설정하는 것이 좋습니다.



일반적으로 더 낮은 값 대신 더 높은 값을 사용하는 것이 좋습니다. 메타데이터 예약 공간 설정이 너무 큰 경우 나중에 줄일 수 있습니다. 반대로 값을 나중에 증가해도 시스템에서 공간을 확보하기 위해 오브젝트 데이터를 이동해야 할 수 있습니다.

메타데이터 예약 공간 설정이 특정 스토리지 노드에서 개체 메타데이터 저장소에 허용되는 공간에 미치는 영향에 대한 자세한 설명은 을 참조하십시오."오브젝트 메타데이터 스토리지 관리"

단계

1. 현재 메타데이터 예약 공간 설정을 확인합니다.
 - a. 구성 > 시스템 > *저장소 설정*을 선택합니다.
 - b. *메타데이터 예약 공간*의 값을 확인하세요.
2. 각 스토리지 노드의 스토리지 볼륨 0에 이 값을 늘릴 수 있는 충분한 공간이 있는지 확인합니다.
 - a. *노드*를 선택하세요.
 - b. 그리드에서 첫 번째 스토리지 노드를 선택합니다.
 - c. Storage 탭을 선택합니다.
 - d. Volumes 섹션에서 * /var/local/rangedb/0 * 항목을 찾습니다.
 - e. 사용할 수 있는 값이 사용하려는 새 값과 현재 메타데이터 예약된 공간 값의 차이와 같거나 큰지 확인합니다.
3. 예를 들어 메타데이터 예약 공간 설정이 현재 4TB이고 이 설정을 6TB로 늘리려면 사용 가능한 값이 2TB 이상이어야 합니다.
 - f. 모든 스토리지 노드에 대해 이 단계를 반복합니다.
 - 하나 이상의 스토리지 노드에 사용 가능한 공간이 충분하지 않으면 메타데이터 예약 공간 값을 늘릴 수 없습니다. 이 절차를 계속 진행하지 마십시오.
 - 각 스토리지 노드에 볼륨 0에 사용 가능한 공간이 충분한 경우 다음 단계로 이동합니다.
 3. 각 스토리지 노드에 128MB 이상의 RAM이 있는지 확인합니다.
 - a. *노드*를 선택하세요.
 - b. 그리드에서 첫 번째 스토리지 노드를 선택합니다.

- c. 하드웨어 * 탭을 선택합니다.
 - d. 메모리 사용량 차트 위에 커서를 놓습니다. 총 메모리 * 가 128GB 이상인지 확인합니다.
 - e. 모든 스토리지 노드에 대해 이 단계를 반복합니다.
 - 하나 이상의 스토리지 노드에 사용 가능한 총 메모리가 충분하지 않으면 메타데이터 예약 공간 값을 늘릴 수 없습니다. 이 절차를 계속 진행하지 마십시오.
 - 각 스토리지 노드에 총 메모리가 최소 128GB인 경우 다음 단계로 이동합니다.
4. 메타데이터 예약 공간 설정을 업데이트합니다.
- a. 구성 > 시스템 > *저장소 설정*을 선택합니다.
 - b. *메타데이터 예약 공간*을 선택하세요.
 - c. 새 값을 입력합니다.
- 예를 들어, 지원되는 최대 값인 8TB를 입력하려면 * 8000000000000 * (8, 0이 12개 있음)을 입력합니다.
- d. 저장 * 을 선택합니다.

저장된 객체를 압축합니다

오브젝트 압축을 활성화하여 StorageGRID에 저장된 오브젝트 크기를 줄일 수 있으므로 오브젝트가 더 적은 스토리지를 소비하도록 할 수 있습니다.

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다. "[지원되는 웹 브라우저](#)"
- 있습니다. "[특정 액세스 권한](#)"

이 작업에 대해

기본적으로 오브젝트 압축은 비활성화되어 있습니다. 압축을 설정하면 StorageGRID는 무손실 압축을 사용하여 저장할 때 각 개체의 압축을 시도합니다.



이 설정을 변경하면 새 설정을 적용하는 데 약 1분이 걸립니다. 구성된 값이 성능 및 확장을 위해 캐싱됩니다.

오브젝트 압축을 설정하기 전에 다음 사항을 숙지하십시오.

- 저장 중인 데이터가 압축될 수 있다는 것을 모를 경우 * Compress stored objects * 를 선택하면 안 됩니다.
- 개체를 StorageGRID에 저장하는 응용 프로그램은 개체를 저장하기 전에 압축할 수 있습니다. 클라이언트 응용 프로그램이 개체를 StorageGRID에 저장하기 전에 이미 압축한 경우 이 옵션을 선택하면 개체의 크기가 더 작아지지 않습니다.
- StorageGRID에서 NetApp FabricPool를 사용하는 경우 * 저장된 오브젝트 압축 * 을 선택하지 마십시오.
- 저장된 개체 압축 * 을 선택하면 S3 클라이언트 응용 프로그램에서 반환되는 바이트 범위를 지정하는 GetObject 작업을 수행하지 않도록 해야 합니다. 이러한 "범위 읽기" 작업은 StorageGRID에서 요청된 바이트에 액세스하기 위해 개체의 압축을 효과적으로 해제해야 하기 때문에 비효율적입니다. 매우 큰 개체에서 작은 범위의 바이트를 요청하는 GetObject 작업은 특히 비효율적입니다. 예를 들어, 50GB의 압축된 개체에서 10MB 범위를 읽는 것은 비효율적입니다.

압축된 개체에서 범위를 읽으면 클라이언트 요청이 시간 초과될 수 있습니다.



개체를 압축해야 하고 클라이언트 응용 프로그램에서 범위 읽기를 사용해야 하는 경우 응용 프로그램의 읽기 시간 초과를 늘리십시오.

단계

- 구성 > 시스템 > 저장소 설정 > *개체 압축*을 선택합니다.
- 저장된 객체 압축 * 확인란을 선택합니다.
- 저장 * 을 선택합니다.

전체 스토리지 노드 관리

스토리지 노드가 용량에 도달하면 새 스토리지를 추가하여 StorageGRID 시스템을 확장해야 합니다. 스토리지 볼륨 추가, 스토리지 확장 웰프 추가, 스토리지 노드 추가의 세 가지 옵션을 사용할 수 있습니다.

스토리지 볼륨을 추가합니다

각 스토리지 노드는 최대 개수의 스토리지 볼륨을 지원합니다. 정의된 최대값은 플랫폼에 따라 다릅니다. 스토리지 노드에 최대 스토리지 볼륨 수보다 적은 수의 볼륨이 포함된 경우 볼륨을 추가하여 용량을 늘릴 수 있습니다. 의 지침을 "[StorageGRID 시스템 확장](#)" 참조하십시오.

스토리지 확장 웰프를 추가합니다

SG6060 또는 SG6160 같은 일부 StorageGRID 어플라이언스 스토리지 노드는 추가 스토리지 웰프를 지원할 수 있습니다. 최대 용량으로 아직 확장되지 않은 확장 기능을 갖춘 StorageGRID 어플라이언스를 사용하는 경우 스토리지 웰프를 추가하여 용량을 늘릴 수 있습니다. 의 지침을 "[StorageGRID 시스템 확장](#)" 참조하십시오.

스토리지 노드 추가

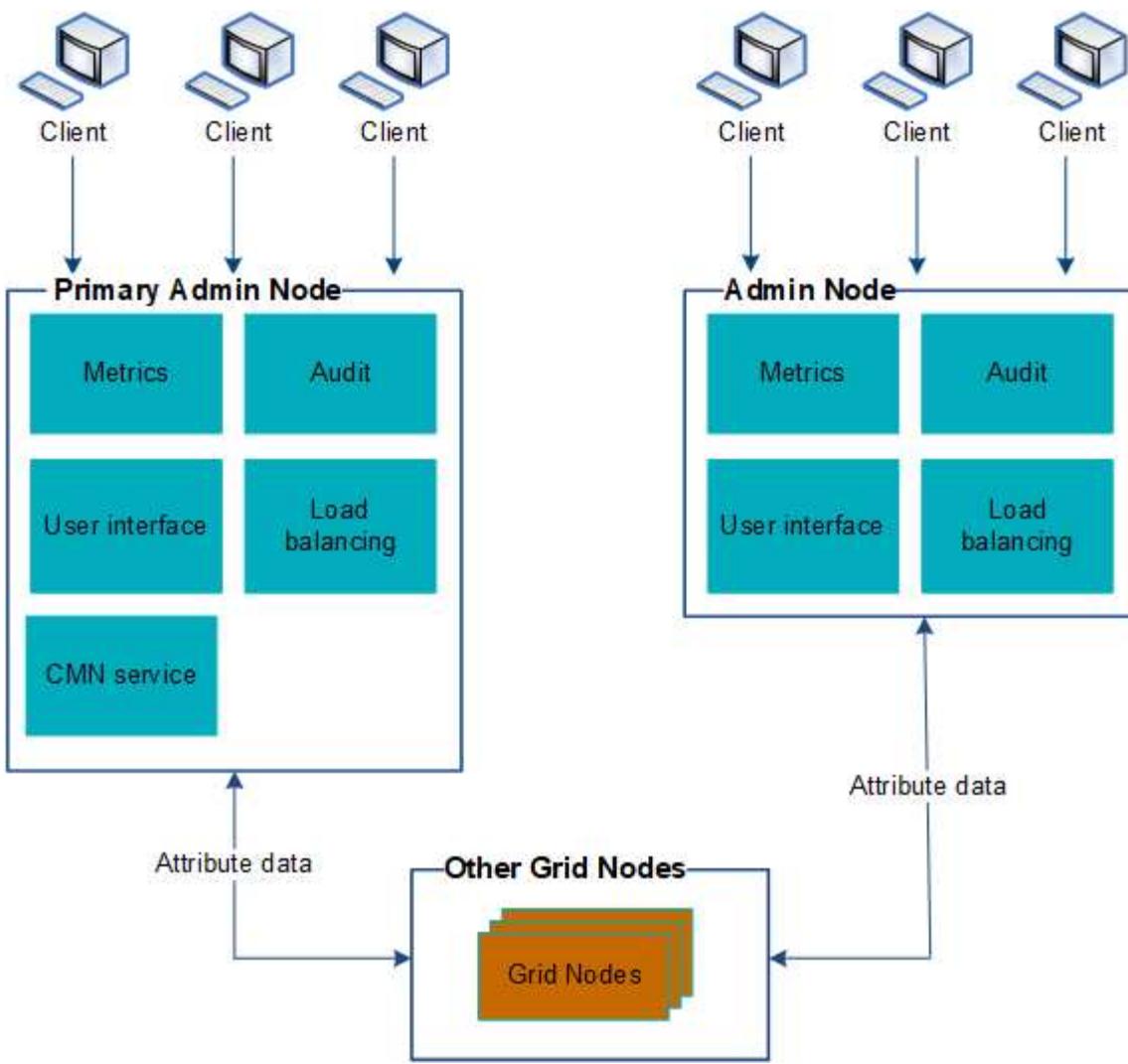
스토리지 노드를 추가하여 스토리지 용량을 늘릴 수 있습니다. 스토리지를 추가할 때 현재 활성 상태인 ILM 규칙 및 용량 요구 사항을 신중하게 고려해야 합니다. 의 지침을 "[StorageGRID 시스템 확장](#)" 참조하십시오.

관리 노드 관리

여러 관리자 노드 사용

StorageGRID 시스템에는 여러 관리 노드가 포함되어 있어 하나의 관리 노드에 장애가 발생하더라도 StorageGRID 시스템을 지속적으로 모니터링하고 구성할 수 있습니다.

관리자 노드를 사용할 수 없게 되면 속성 처리가 계속되고 알림이 계속 트리거되며 이메일 알림 및 AutoSupport 패키지가 계속 전송됩니다. 그러나 관리 노드가 여러 개인 경우에는 알림 및 AutoSupport 패키지를 제외한 페일오버 보호 기능을 제공하지 않습니다.



관리 노드에 장애가 발생할 경우 StorageGRID 시스템을 계속 보고 구성할 수 있는 두 가지 옵션이 있습니다.

- 웹 클라이언트는 사용 가능한 다른 관리 노드에 다시 연결할 수 있습니다.
- 시스템 관리자가 고가용성 관리 노드 그룹을 구성한 경우 웹 클라이언트는 HA 그룹의 가상 IP 주소를 사용하여 그리드 관리자 또는 테넌트 관리자에 계속 액세스할 수 있습니다. 을 ["고가용성 그룹을 관리합니다"](#) 참조하십시오.



HA 그룹을 사용하는 경우 활성 관리 노드에 장애가 발생하면 액세스가 중단됩니다. 사용자는 HA 그룹의 가상 IP 주소가 그룹의 다른 관리 노드로 폐일오버된 후 다시 로그인해야 합니다.

일부 유지 보수 작업은 기본 관리 노드를 통해서만 수행할 수 있습니다. 기본 관리 노드에 장애가 발생할 경우 StorageGRID 시스템이 다시 정상적으로 작동하기 전에 해당 노드를 복구해야 합니다.

기본 관리 노드를 식별합니다

기본 관리자 노드는 비기본 관리자 노드보다 더 많은 기능을 제공합니다. 예를 들어, 일부 유지 보수 절차는 기본 관리자 노드를 사용하여 수행해야 합니다.

관리 노드에 대한 자세한 내용은 을 참조하십시오 ["관리자 노드란 무엇입니까"](#).

시작하기 전에

- 을 사용하여 그리드 관리자에 로그인되어 있습니다."[지원되는 웹 브라우저](#)"

- 있습니다. "[특정 액세스 권한](#)"

단계

1. *노드*를 선택하세요.
2. 검색 상자에 * primary * 를 입력합니다.

검색 결과에서 유형 열에 "기본 관리자 노드"가 표시된 노드를 확인합니다. 하나의 기본 관리자 노드가 나열되어야 합니다.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그레픽, 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 있으며 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/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.