



# StorageGRID 관리

## StorageGRID 11.5

NetApp  
April 11, 2024

# 목차

StorageGRID 관리 .....	1
StorageGRID 시스템 관리 .....	1
StorageGRID에 대한 관리자 액세스 제어 .....	29
키 관리 서버 구성 .....	71
테넌트 관리 .....	101
S3 및 Swift 클라이언트 연결 구성 .....	123
StorageGRID 네트워크 및 연결 관리 .....	154
AutoSupport 구성 .....	182
스토리지 노드 관리 .....	198
관리 노드 관리 .....	221
아카이브 노드 관리 .....	243
StorageGRID로 데이터 마이그레이션 .....	265

# StorageGRID 관리

StorageGRID 시스템을 구성하는 방법에 대해 알아봅니다.

- ["StorageGRID 시스템 관리"](#)
- ["StorageGRID에 대한 관리자 액세스 제어"](#)
- ["키 관리 서버 구성"](#)
- ["테넌트 관리"](#)
- ["S3 및 Swift 클라이언트 연결 구성"](#)
- ["StorageGRID 네트워크 및 연결 관리"](#)
- ["AutoSupport 구성"](#)
- ["스토리지 노드 관리"](#)
- ["관리 노드 관리"](#)
- ["아카이브 노드 관리"](#)
- ["StorageGRID로 데이터 마이그레이션"](#)

## StorageGRID 시스템 관리

다음 지침에 따라 StorageGRID 시스템을 구성하고 관리합니다.

이 지침은 그리드 관리자를 사용하여 그룹 및 사용자를 설정하고, S3 및 Swift 클라이언트 애플리케이션이 오브젝트를 저장 및 검색하고, StorageGRID 네트워크를 구성 및 관리하고, AutoSupport를 구성하고, 노드 설정을 관리하는 등의 작업을 수행할 수 있도록 테넌트 계정을 생성하는 방법을 설명합니다.



ILM(정보 수명 주기 관리) 규칙 및 정책이 있는 개체를 관리하기 위한 지침이 로 옮겨졌습니다"ILM을 사용하여 개체를 관리합니다".

이 지침은 StorageGRID 시스템을 설치한 후 구성, 관리 및 지원할 기술 담당자를 위한 것입니다.

필요한 것

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

웹 브라우저 요구 사항

지원되는 웹 브라우저를 사용해야 합니다.

웹 브라우저	최소 지원 버전
Google Chrome	87
Microsoft Edge를 참조하십시오	87

웹 브라우저	최소 지원 버전
Mozilla Firefox	84

브라우저 창을 권장 너비로 설정해야 합니다.

브라우저 폭	픽셀
최소	1024
최적	1280

## Grid Manager에 로그인합니다

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

필요한 것

- 로그인 자격 증명이 있어야 합니다.
- 그리드 관리자의 URL이 있어야 합니다.
- 지원되는 웹 브라우저를 사용하고 있어야 합니다.
- 웹 브라우저에서 쿠키를 활성화해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

각 StorageGRID 시스템에는 1개의 기본 관리 노드와 1차 관리자가 아닌 노드 수가 포함되어 있습니다. 관리자 노드의 그리드 관리자에 로그인하여 StorageGRID 시스템을 관리할 수 있습니다. 그러나 관리 노드는 정확히 동일하지 않습니다.

- 한 관리 노드에서 이루어진 알람 승인(레거시 시스템)은 다른 관리 노드에 복사되지 않습니다. 이러한 이유로 알람에 대해 표시되는 정보는 각 관리 노드에서 동일하지 않을 수 있습니다.
- 일부 유지 보수 절차는 기본 관리 노드에서만 수행할 수 있습니다.

HA(고가용성) 그룹에 관리 노드가 포함된 경우 HA 그룹의 가상 IP 주소 또는 가상 IP 주소에 매핑되는 정규화된 도메인 이름을 사용하여 연결합니다. 기본 관리 노드를 그룹의 기본 마스터로 선택해야 그리드 관리자에 액세스할 때 기본 관리 노드를 사용할 수 없는 경우를 제외하고 기본 관리 노드에서 액세스할 수 있습니다.

단계

1. 지원되는 웹 브라우저를 실행합니다.
2. 브라우저의 주소 표시줄에 Grid Manager의 URL을 입력합니다.

`https://FQDN_or_Admin_Node_IP/`

위치 `FQDN_or_Admin_Node_IP`는 관리자 노드의 정규화된 도메인 이름 또는 IP 주소 또는 관리 노드의 HA 그룹의 가상 IP 주소입니다.

HTTPS의 표준 포트(443)가 아닌 포트에서 Grid Manager에 액세스해야 하는 경우 다음 위치를 입력합니다  
*FQDN\_or\_Admin\_Node\_IP*는 정규화된 도메인 이름 또는 IP 주소이고 *port*는 포트 번호입니다.

`https://FQDN_or_Admin_Node_IP:port/`

3. 보안 경고 메시지가 나타나면 브라우저의 설치 마법사를 사용하여 인증서를 설치합니다.

4. Grid Manager에 로그인:

◦ SSO(Single Sign-On)를 StorageGRID 시스템에 사용하지 않는 경우:

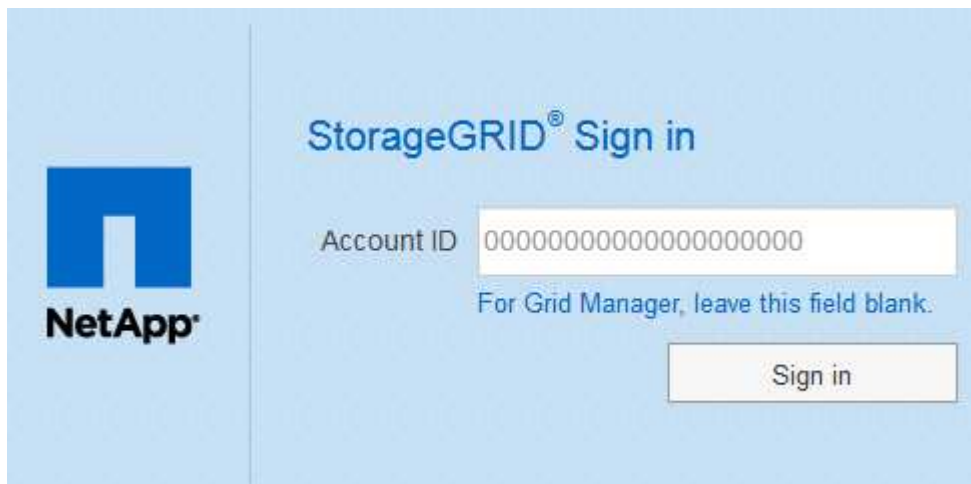
- i. Grid Manager의 사용자 이름과 암호를 입력합니다.
- ii. 로그인 \* 을 클릭합니다.



The image shows the StorageGRID Grid Manager login page. On the left is the NetApp logo. The main heading is "StorageGRID® Grid Manager". Below the heading are two input fields: "Username" and "Password". At the bottom right is a "Sign in" button.

◦ StorageGRID 시스템에서 SSO가 활성화되어 있고 이 브라우저에서 URL에 처음 액세스한 경우:

- i. 로그인 \* 을 클릭합니다. 계정 ID 필드는 비워 둘 수 있습니다.



The image shows the StorageGRID Sign in page. On the left is the NetApp logo. The main heading is "StorageGRID® Sign in". Below the heading is an "Account ID" input field with the placeholder text "00000000000000000000". Below the input field is the text "For Grid Manager, leave this field blank." At the bottom right is a "Sign in" button.

- ii. 조직의 SSO 로그인 페이지에 표준 SSO 자격 증명을 입력합니다. 예를 들면 다음과 같습니다.

Sign in with your organizational account

someone@example.com

Password

Sign in

◦ StorageGRID 시스템에 대해 SSO가 활성화되어 있고 이전에 그리드 관리자 또는 테넌트 계정에 액세스한 경우:

i. 다음 중 하나를 수행합니다.

- 0 \* (Grid Manager의 계정 ID)을 입력하고 \* 로그인 \* 을 클릭합니다.
- 최근 계정 목록에 나타나는 경우 \* Grid Manager \* 를 선택하고 \* Sign In \* 을 클릭합니다.

StorageGRID<sup>®</sup> Sign in

Recent Grid Manager

Account ID 0

Sign in

ii. 조직의 SSO 로그인 페이지에서 표준 SSO 자격 증명을 사용하여 로그인합니다. 로그인하면 대시보드가 포함된 그리드 관리자의 홈 페이지가 나타납니다. 제공되는 정보에 대한 자세한 내용은 StorageGRID 모니터링 및 문제 해결 설명서의 "대시보드 보기"를 참조하십시오.

Dashboard

**Health**

✔

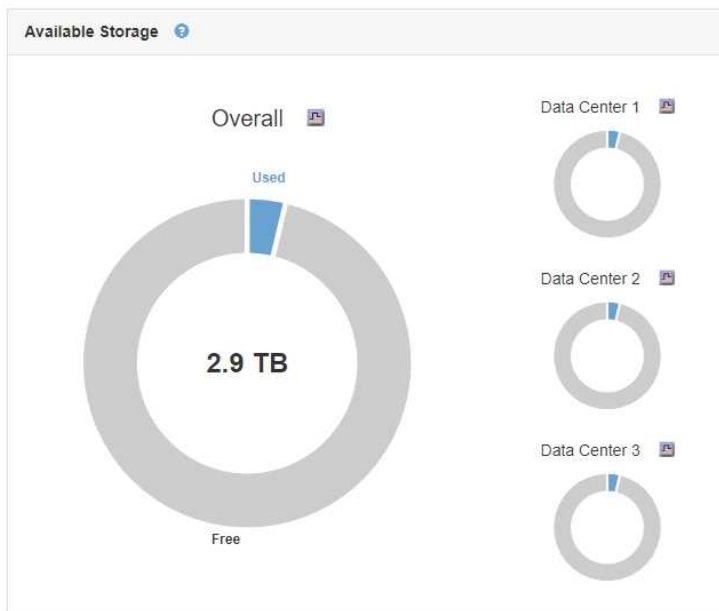
No current alerts. All grid nodes are connected.

**Information Lifecycle Management (ILM)**

Awaiting - Client	0 objects	📊
Awaiting - Evaluation Rate	0 objects / second	📊
Scan Period - Estimated	0 seconds	📊

**Protocol Operations**

S3 rate	0 operations / second	📊
Swift rate	0 operations / second	📊



5. 다른 관리자 노드에 로그인하려면:

옵션을 선택합니다	단계
SSO가 활성화되지 않았습니다	<p>a. 브라우저의 주소 표시줄에 다른 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력합니다. 필요에 따라 포트 번호를 포함시킵니다.</p> <p>b. Grid Manager의 사용자 이름과 암호를 입력합니다.</p> <p>c. 로그인 * 을 클릭합니다.</p>
SSO가 활성화되었습니다	<p>브라우저의 주소 표시줄에 다른 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력합니다.</p> <p>한 관리 노드에 로그인한 경우 다시 로그인하지 않고도 다른 관리 노드에 액세스할 수 있습니다. 그러나 SSO 세션이 만료되면 자격 증명을 다시 입력하라는 메시지가 표시됩니다.</p> <ul style="list-style-type: none"> <li>참고: * SSO는 제한된 Grid Manager 포트에서 사용할 수 없습니다. 사용자가 SSO(Single Sign-On)로 인증하도록하려면 기본 HTTPS 포트 (443)를 사용해야 합니다.</li> </ul>

관련 정보

["웹 브라우저 요구 사항"](#)

["방화벽을 통한 액세스 제어"](#)

"서버 인증서를 구성하는 중입니다"

"Single Sign-On 구성"

"관리 그룹 관리"

"고가용성 그룹 관리"

"테넌트 계정을 사용합니다"

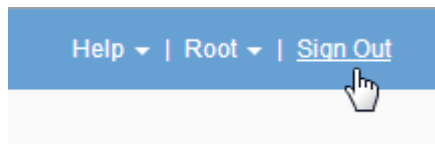
"모니터링 및 문제 해결"

## 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. 사용자 인터페이스의 오른쪽 상단 모서리에 있는 \* 로그아웃 \* 링크를 찾습니다.



2. 로그아웃 \* 을 클릭합니다.

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

관련 정보

"Single Sign-On 구성"

"테넌트 계정을 사용합니다"



## 암호 변경

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

### 필요한 것

지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

### 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 클릭합니다.

## 프로비저닝 암호 변경

StorageGRID 프로비저닝 암호를 변경하려면 다음 절차를 따르십시오. 복구, 확장 및 유지 보수 절차에 필요한 암호 문구입니다. 또한 StorageGRID 시스템의 그리드 토폴로지 정보와 암호화 키가 포함된 복구 패키지 백업을 다운로드하려면 암호문이 필요합니다.

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.
- 현재 프로비저닝 암호가 있어야 합니다.

### 이 작업에 대해

프로비저닝 암호는 많은 설치 및 유지 관리 절차와 복구 패키지 다운로드에 필요합니다. 프로비저닝 암호가 에 나와 있지 않습니다 Passwords.txt 파일. 프로비저닝 암호를 문서화하고 안전한 장소에 보관해야 합니다.

### 단계

1. Configuration \* > \* Access Control \* > \* Grid Passwords \* 를 선택합니다.

Grid Passwords

Change the provisioning passphrase and other passwords for your StorageGRID system.

Change Provisioning Passphrase

The provisioning passphrase is required for any installation, expansion, or maintenance procedure that makes changes to the grid topology. This passphrase is also required to download backups of the grid topology information and encryption keys for the StorageGRID system. After changing the provisioning passphrase, you must download a new Recovery Package.

Current Provisioning Passphrase

New Provisioning Passphrase

Confirm New Provisioning Passphrase

2. 현재 프로비저닝 암호를 입력합니다.
3. 새 passWindows를 입력하십시오. 암호는 8자 이상이어야 하며 32자 이하여야 합니다. 암호는 대/소문자를 구분합니다.



새 프로비저닝 암호를 안전한 위치에 저장합니다. 설치, 확장 및 유지보수 절차에 필요합니다.

4. 새 암호를 다시 입력하고 \* Save \* 를 클릭합니다.

프로비저닝 암호 변경이 완료되면 녹색 성공 배너가 표시됩니다. 변경 작업은 1분 이내에 이루어져야 합니다.

Grid Passwords

Change the provisioning passphrase and other passwords for your StorageGRID system.

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

Change Provisioning Passphrase

The provisioning passphrase is required for any installation, expansion, or maintenance procedure that makes changes to the grid topology. This passphrase is also required to download backups of the grid topology information and encryption keys for the StorageGRID system. After changing the provisioning passphrase, you must download a new Recovery Package.

Current Provisioning Passphrase

New Provisioning Passphrase

Confirm New Provisioning Passphrase

5. 성공 배너 내에서 \* 복구 패키지 페이지 \* 링크를 선택합니다.
6. Grid Manager에서 새 복구 패키지를 다운로드합니다. 유지보수 \* > \* 복구 패키지 \* 를 선택하고 새 프로비저닝 암호를 입력합니다.



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

## 브라우저 세션 시간 초과 변경

특정 시간 이상 사용하지 않는 경우 Grid Manager 및 Tenant Manager 사용자가 로그아웃되는지 여부를 제어할 수 있습니다.

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

### 이 작업에 대해

GUI 비활성 시간 초과 기본값은 900초(15분)입니다. 사용자의 브라우저 세션이 이 시간 동안 활성 상태가 아니면 세션 시간이 초과됩니다.

필요한 경우 GUI 비활성 시간 초과 표시 옵션을 설정하여 시간 초과 기간을 늘리거나 줄일 수 있습니다.

SSO(Single Sign-On)가 활성화되어 있고 사용자의 브라우저 세션 시간이 초과되면 사용자가 \* 로그아웃 \* 수동으로 클릭하는 것처럼 시스템이 작동합니다. 사용자가 SSO 자격 증명을 다시 입력하여 StorageGRID에 다시 액세스해야 합니다.

사용자 세션 시간 초과는 다음을 통해서도 제어할 수 있습니다.



- 시스템 보안을 위해 포함되어 있는 별도의 구성 불가능한 StorageGRID 타이머입니다. 기본적으로 각 사용자의 인증 토큰은 사용자가 로그인 한 후 16시간 후에 만료됩니다. 사용자의 인증이 만료되면 GUI 비활성 시간 제한 값에 도달하지 않았더라도 해당 사용자는 자동으로 로그아웃됩니다. 토큰을 갱신하려면 사용자가 다시 로그인해야 합니다.
- StorageGRID에 대해 SSO가 활성화된 경우 ID 공급자에 대한 시간 제한 설정

### 단계

1. 구성 \* > \* 시스템 설정 \* > \* 표시 옵션 \* 을 선택합니다.
2. GUI 비활성 시간 초과 \* 의 경우 시간 초과 기간을 60초 이상으로 입력합니다.

이 기능을 사용하지 않으려면 이 필드를 0으로 설정합니다. 사용자는 로그인 후 16시간 후에 인증 토큰이 만료되었을 때 로그아웃됩니다.



## Display Options

Updated: 2017-03-09 20:36:53 MST

Current Sender	ADMIN-DC1-ADM1
Preferred Sender	ADMIN-DC1-ADM1
GUI Inactivity Timeout	900
Notification Suppress All	<input type="checkbox"/>

Apply Changes

3. 변경 내용 적용 \* 을 클릭합니다.

새 설정은 현재 로그인한 사용자에게는 영향을 주지 않습니다. 사용자는 다시 로그인하거나 브라우저를 새로 고쳐야 새 시간 초과 설정을 적용할 수 있습니다.

관련 정보

["Single Sign-On의 작동 방식"](#)

["테넌트 계정을 사용합니다"](#)

### StorageGRID 라이선스 정보 보기

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

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

이 작업에 대해

이 StorageGRID 시스템의 소프트웨어 라이선스에 문제가 있는 경우 대시보드의 상태 패널에 라이선스 상태 아이콘과 \* 라이선스 \* 링크가 포함됩니다. 이 숫자는 라이선스 관련 문제가 얼마나 많은가를 나타냅니다.

### Dashboard

The screenshot shows a 'Health' dashboard section. At the top left, it says 'Health' with a question mark icon. In the center, there is a large orange warning icon (exclamation mark inside a circle) above the text 'License Status'. Below that, the number '1' is displayed in a large font. At the bottom, there is a blue link labeled 'License'.

단계

라이센스를 보려면 다음 중 하나를 수행합니다.

- 대시보드의 상태 패널에서 라이선스 상태 아이콘 또는 \* 라이선스 \* 링크를 클릭합니다. 이 링크는 라이선스에 문제가 있는 경우에만 나타납니다.
- 유지 관리 \*\* 시스템 \* 라이선스 \* 를 선택합니다.

라이선스 페이지가 나타나고 현재 라이선스에 대한 다음과 같은 읽기 전용 정보가 제공됩니다.

- StorageGRID 시스템 ID로, 이 StorageGRID 설치의 고유 식별 번호입니다
- 라이선스 일련 번호입니다
- 그리드의 라이선스가 부여된 스토리지 용량입니다
- 소프트웨어 라이선스 종료 날짜입니다
- 지원 서비스 계약 종료 날짜입니다
- 라이선스 텍스트 파일의 내용입니다



StorageGRID 10.3 이전에 발급된 라이선스의 경우 라이선스 저장 용량은 라이선스 파일에 포함되지 않으며 값 대신 "사용권 계약 참조" 메시지가 표시됩니다.

## StorageGRID 라이선스 정보를 업데이트하는 중입니다

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

필요한 것

- StorageGRID 시스템에 적용하려면 새 라이선스 파일이 있어야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 프로비저닝 암호가 있어야 합니다.

단계

1. 유지 관리 \*\* 시스템 \* 라이선스 \* 를 선택합니다.
2. Provisioning Passphrase \* 텍스트 상자에 StorageGRID 시스템의 프로비저닝 암호를 입력합니다.
3. 찾아보기 \* 를 클릭합니다.
4. 열기 대화 상자에서 새 라이선스 파일을 찾아 선택합니다 (.txt)를 클릭하고 \* 열기 \* 를 클릭합니다.

새 라이선스 파일의 유효성을 검사한 후 표시합니다.

5. 저장 \* 을 클릭합니다.

## Grid Management API 사용

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 엔티티를 더 빠르게 생성할 수 있습니다.

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.

## 최고 수준의 리소스

Grid Management API는 다음과 같은 최상위 리소스를 제공합니다.

- `/grid`: 액세스는 Grid Manager 사용자로 제한되며 구성된 그룹 권한을 기반으로 합니다.
- `/org`: 테넌트 계정의 로컬 또는 통합 LDAP 그룹에 속한 사용자만 액세스할 수 있습니다. 자세한 내용은 테넌트 계정 사용에 대한 정보를 참조하십시오.
- `/private`: 액세스는 Grid Manager 사용자로 제한되며 구성된 그룹 권한을 기반으로 합니다. 이러한 API는 내부용으로만 사용해야 하며 공개적으로 문서화되지 않았습니다. 또한 이러한 API는 사전 통보 없이 변경될 수 있습니다.

## 관련 정보

["테넌트 계정을 사용합니다"](#)

["Prometheus: 쿼리 기본 사항"](#)

## Grid Management API 작업

Grid Management API는 사용 가능한 API 작업을 다음 섹션으로 구성합니다.

- **\* ACCOUNT \*** — 새 계정 생성 및 지정된 계정의 스토리지 사용량 검색을 포함하여 스토리지 테넌트 계정을 관리하는 작업입니다.
- **\* ALARMS \*** — 현재 경고(레거시 시스템)를 나열하고, 현재 경고와 노드 연결 상태 요약에 포함하여 그리드의 상태에 대한 정보를 반환하는 작업.
- **\* alert-history \*** — 해결된 경고에 대한 작업.
- **알림 메시지 수신자 \*** — 경고 알림 수신자(이메일)에 대한 작업.
- **\* alert-rules \*** — 경고 규칙에 대한 작업.
- **\* alert-silences \*** — 경고 작동 중.
- **\* 경고 \*** — 경고 작업.
- **\* 감사 \*** — 감사 구성을 나열하고 업데이트하는 작업.
- **\* auth \*** — 사용자 세션 인증을 수행하기 위한 작업.

Grid Management API는 Bearer Token Authentication Scheme을 지원한다. 로그인하려면 인증 요청의 JSON 본문에 사용자 이름 및 암호를 입력합니다(즉, `POST /api/v3/authorize`)를 클릭합니다. 사용자가 성공적으로 인증되면 보안 토큰이 반환됩니다. 이 토큰은 후속 API 요청 헤더("Authorization:Bearer\_token\_")에 제공되어야 합니다.



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

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

- \* client-certificates \* — 외부 모니터링 도구를 사용하여 StorageGRID에 안전하게 액세스할 수 있도록 클라이언트 인증서를 구성하는 작업.
- \* config \* — 그리드 관리 API 제품 릴리스 및 버전과 관련된 작업. 제품 릴리스 버전과 해당 릴리스에서 지원하는 Grid Management API의 주요 버전을 나열할 수 있으며 더 이상 사용되지 않는 API 버전을 사용하지 않도록 설정할 수 있습니다.
- \* deactivated - features \* — 비활성화된 기능을 보기 위한 작업.
- \* DNS-서버 \* — 구성된 외부 DNS 서버를 나열하고 변경하는 작업.
- **endpoint-domain-names** — 끝점 도메인 이름을 나열하고 변경하는 작업.
- \* 삭제 코딩 \* — 삭제 코딩 프로파일에서 작업.
- \* 확장 \* — 확장 작업(절차 수준).
- \* expansion-nodes \* — 확장 시 작업(노드 레벨).
- \* 확장 사이트 \* — 확장 시 운영(사이트 레벨)
- \* GRID-NETWORKS \* — 그리드 네트워크 목록을 나열하고 변경하는 작업.
- \* GRID-Passwords \* — 그리드 암호 관리 작업.
- \* 그룹 \* — 로컬 그리드 관리자 그룹을 관리하고 외부 LDAP 서버에서 통합 그리드 관리자 그룹을 검색하는 작업.
- \* identity-source \* — 외부 ID 소스를 구성하고 통합 그룹 및 사용자 정보를 수동으로 동기화하는 작업.
- \* ILM \* — 정보 수명 주기 관리(ILM)에 대한 운영.
- \* license \* — StorageGRID 라이선스를 검색하고 업데이트하는 작업.
- \* 로그 \* — 로그 파일을 수집하고 다운로드하기 위한 작업.
- \* 메트릭 \* — 일정 기간 동안 단일 시점 및 범위 메트릭 쿼리에 대한 즉석 메트릭 쿼리를 비롯한 StorageGRID 메트릭의 운영 Grid Management API는 Prometheus 시스템 모니터링 도구를 백엔드 데이터 소스로 사용합니다. Prometheus 쿼리 구성에 대한 자세한 내용은 Prometheus 웹 사이트를 참조하십시오.



다음에 포함된 메트릭 *private* 해당 이름은 내부용으로만 사용해야 합니다. 이러한 메트릭은 사전 통지 없이 StorageGRID 릴리스 간에 변경될 수 있습니다.

- \* 노드 상태 \* — 노드 상태에 대한 작업
- \* NTP-서버 \* — 외부 NTP(Network Time Protocol) 서버를 나열하거나 업데이트하는 작업.
- \* 오브젝트 \* — 오브젝트 및 오브젝트 메타데이터 작업
- \* 복구 \* — 복구 절차를 위한 작업.
- \* recovery-package \* — 복구 패키지를 다운로드하기 위한 작업.
- \* 지역 \* — 영역을 보고 작성하는 작업.
- \* S3-오브젝트 잠금 \* — 글로벌 S3 오브젝트 잠금 설정에서 작업.
- \* server-certificate \* — Grid Manager 서버 인증서를 보고 업데이트하는 작업.
- \* SNMP \* — 현재 SNMP 구성에 대한 작업.
- \* traffic-classes \* — 트래픽 분류 정책을 위한 운영.

- \* 신뢰할 수 없는 클라이언트-네트워크 \* — 신뢰할 수 없는 클라이언트 네트워크 구성에서의 작업.
- \* 사용자 \* — 그리드 관리자 사용자를 보고 관리하는 작업.

## API 요청을 발급하는 중입니다

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

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.



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

### 단계

1. Grid Manager 헤더에서 \* Help \* > \* API Documentation \* 을 선택합니다.
2. 원하는 작업을 선택합니다.

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

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



GET /grid/groups Lists Grid Administrator Groups
🔒

Try it out

Name	Description
type string <small>(query)</small>	filter by group type Available values : local, federated <div style="border: 1px solid #ccc; padding: 2px; width: 100px; margin-top: 5px;">--</div>
limit integer <small>(query)</small>	maximum number of results Default value : 25 <div style="border: 1px solid #ccc; padding: 2px; width: 100px; margin-top: 5px;">25</div>
marker string <small>(query)</small>	marker-style pagination offset (value is Group's URN) <div style="border: 1px solid #ccc; padding: 2px; width: 100%; margin-top: 5px;">marker - marker-style pagination offset (value</div>
includeMarker boolean <small>(query)</small>	if set, the marker element is also returned <div style="border: 1px solid #ccc; padding: 2px; width: 100px; margin-top: 5px;">--</div>
order string <small>(query)</small>	pagination order (desc requires marker) Available values : asc, desc <div style="border: 1px solid #ccc; padding: 2px; width: 100px; margin-top: 5px;">--</div>

Responses
Response content type application/json ▼

Code	Description
200	successfully retrieved Example Value   Model <div style="background-color: #2e3436; color: #eeeeec; padding: 10px; font-family: monospace; font-size: 0.9em; margin-top: 5px;"> <pre> {   "responseTime": "2021-03-29T14:22:19.673Z",   "status": "success",   "apiVersion": "3.3",   "deprecated": false,   "data": [     {       "displayName": "Developers", </pre> </div>

4. 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.
5. 예제 요청 본문을 수정해야 하는지 확인합니다. 이 경우 \* Model \* 을 클릭하여 각 필드의 요구 사항을 확인할 수 있습니다.
6. 체험하기 \* 를 클릭합니다.
7. 필요한 매개 변수를 제공하거나 요청 본문을 필요에 따라 수정합니다.
8. Execute \* 를 클릭합니다.
9. 응답 코드를 검토하여 요청이 성공했는지 확인합니다.

## Grid Management API 버전 관리

Grid Management API는 버전 관리를 사용하여 무중단 업그레이드를 지원합니다.

예를 들어 이 요청 URL은 API의 버전 3을 지정합니다.

```
https://hostname_or_ip_address/api/v3/authorize
```

테넌트 관리 API의 주요 버전은 이전 버전과 \* \_호환되지 않는\_ \* 변경 사항이 있을 때 충돌합니다. 테넌트 관리 API의 부 버전은 \* \_이(가) 이전 버전과 호환된다는 변경 사항이 있을 때 충돌합니다. 호환 가능한 변경 사항에는 새 끝점 또는 새 속성 추가가 포함됩니다. 다음 예제에서는 변경 유형에 따라 API 버전을 충돌하는 방법을 보여 줍니다.

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

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



Grid Management API를 사용하여 지원되는 버전을 구성할 수 있습니다. 자세한 내용은 Swagger API 설명서의 ""구성"" 섹션을 참조하십시오. 최신 버전을 사용하도록 모든 Grid Management API 클라이언트를 업데이트한 후에는 이전 버전에 대한 지원을 비활성화해야 합니다.

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

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

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

현재 릴리즈에서 지원되는 **API** 버전 확인

다음 API 요청을 사용하여 지원되는 API 주요 버전 목록을 반환합니다.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

요청에 대한 **API** 버전을 지정합니다

path 매개 변수를 사용하여 API 버전을 지정할 수 있습니다 (/api/v3) 또는 머리글 (Api-Version: 3)를 클릭합니다. 두 값을 모두 제공하면 헤더 값이 경로 값을 재정의합니다.

```
curl https://[IP-Address]/api/v3/grid/accounts
curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

사이트 간 요청 위조(**CSRF**)로부터 보호

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

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

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

기능을 활성화하려면 를 설정합니다 csrfToken 매개 변수 대상 true 인증 중. 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"
```

참이면 A입니다 GridCsrfToken 쿠키는 Grid Manager 및 에 대한 로그인의 임의 값으로 설정됩니다

AccountCsrfToken 쿠키는 테넌트 관리자에 대한 로그인에 대한 임의 값으로 설정됩니다.

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

- 를 클릭합니다 x-Csrf-Token CSRF 토큰 쿠키의 값으로 설정된 헤더.
- 폼 인코딩된 바디를 수용하는 끝점의 경우: A csrfToken 폼 인코딩된 요청 본문 매개 변수입니다.

추가 예제 및 세부 정보는 온라인 API 설명서를 참조하십시오.



CSRF 토큰 쿠키 세트가 있는 요청도 를 적용합니다 "Content-Type: application/json" JSON 요청 본문을 CSRF 공격에 대한 추가 보호 기능으로 기대하는 모든 요청의 헤더입니다.

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

StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 표준 인증 API 요청을 사용하여 그리드 관리 API 또는 테넌트 관리 API에 로그인하고 로그아웃할 수 없습니다.

**SSO(Single Sign-On)**가 활성화된 경우 **API**에 로그인합니다

SSO(Single Sign-On)가 활성화된 경우 그리드 관리 API 또는 테넌트 관리 API에 유효한 AD FS에서 인증 토큰을 얻기 위해 일련의 API 요청을 실행해야 합니다.

필요한 것

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

이 작업에 대해

인증 토큰을 얻으려면 다음 예 중 하나를 사용할 수 있습니다.

- 를 클릭합니다 storagegrid-ssoauth.py StorageGRID 설치 파일 디렉터리에 있는 Python 스크립트 (./rpms Red Hat Enterprise Linux 또는 CentOS의 경우 ./debs Ubuntu 또는 Debian, 및 의 경우 ./vsphere VMware의 경우).
- curl 요청의 워크플로 예

컬을 너무 느리게 수행하면 컬링 작업 시간이 초과될 수 있습니다. 이 응답에 유효한 SubjectConfirmation을 찾을 수 없습니다. 오류가 표시될 수 있습니다.



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

URL 인코딩 문제가 있는 경우 Unsupported SAML version(지원되지 않는 SAML 버전) 오류가 표시될 수 있습니다.

단계

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

2. 을(를) 사용하려는 경우 `storagegrid-ssoauth.py` 스크립트에서 Python 인터프리터로 스크립트를 전달하고 스크립트를 실행합니다.

프롬프트가 표시되면 다음 인수에 대한 값을 입력합니다.

- SSO 사용자 이름입니다
- StorageGRID가 설치된 도메인입니다
- StorageGRID의 주소입니다
- 테넌트 관리 API에 액세스하려면 테넌트 계정 ID를 입력합니다. 를

```
python3 /tmp/storagegrid-ssoauth.py
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-af0b-5c6cacfb25e7
```

누릅니다

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

3. curl 요청을 사용하려면 다음 절차를 따르십시오.

- a. 로그인에 필요한 변수를 선언합니다.

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



Grid Management API에 액세스하려면 0 As를 사용합니다 TENANTACCOUNTID.

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

이 예는 에 대한 서명된 인증 URL에 대한 POST 요청을 보여 줍니다 TENANTACCOUNTID. 결과는 `python-mjson.tool`에 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://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
  sS1%2BfQ33cvfwA%3D&RelayState=12345",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

c. 를 저장합니다 SAMLRequest 후속 명령에 사용할 응답에 따라.

```
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=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
  nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. 응답에서 클라이언트 요청 ID를 저장합니다.

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

f. 이전 응답에서 양식 작업으로 자격 증명을 보냅니다.

```
curl -X POST
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --data
"UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMPLPASSWORD&AuthMethod=For
msAuthentication" --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=fZHRTomwFIZfhh...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. 를 저장합니다 MSISAuth 응답에서 받은 쿠키입니다.

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

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

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

응답 헤더에는 나중에 로그아웃 사용을 위한 AD FS 세션 정보가 포함되며 응답 본문에는 숨겨진 양식 필드에 SALMLResponse가 포함됩니다.

```

HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bk11MnFuUSUzZCUzZCYmJiYmXze3MjAyZTA5LTNmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMj01OVpcMQ==;
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="PHNhbWxwOlJlc3Bvb2N...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />

```

i. 를 저장합니다 SAMLResponse 숨겨진 필드에서:

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb2N...1scDpSZXNwb25zZT4='
```

j. 저장된 를 사용합니다 SAMLResponse, StorageGRID을 만듭니다/api/saml-response StorageGRID 인증 토큰 생성 요청.

용 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 다른 이름으로 저장합니다 MYTOKEN.

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

이제 를 사용할 수 있습니다 MYTOKEN 다른 요청에서는 SSO가 사용되지 않는 경우 API를 사용하는 방법과 유사합니다.

**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 작업에 대해

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

단계

1. 서명된 로그아웃 요청을 생성하려면 통과하십시오 cookie "sso=true" SLO API로

```
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://ads.example.com/ads/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=fZDNboMwEI
RfhZ...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. If(경우 cookie "sso=true" 이(가) 제공되지 않으면 사용자가 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
```

A 204 No Content 응답 - 사용자가 로그아웃되었음을 나타냅니다.

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

## StorageGRID 보안 인증서 사용

보안 인증서는 StorageGRID 구성 요소와 StorageGRID 구성 요소 및 외부 시스템 간에 안전하고 신뢰할 수 있는 연결을 만드는 데 사용되는 작은 데이터 파일입니다.

StorageGRID는 두 가지 유형의 보안 인증서를 사용합니다.

- HTTPS 연결을 사용할 때는 \* 서버 인증서 \* 가 필요합니다. 서버 인증서는 클라이언트와 서버 간의 보안 연결을 설정하고, 클라이언트에 대한 서버 ID를 인증하고, 데이터에 대한 보안 통신 경로를 제공하는 데 사용됩니다. 서버와

클라이언트마다 인증서의 복사본이 있습니다.

- \* 클라이언트 인증서 \* 는 서버에 대한 클라이언트 또는 사용자 ID를 인증하여 암호만 사용하는 것보다 더 안전한 인증을 제공합니다. 클라이언트 인증서는 데이터를 암호화하지 않습니다.

클라이언트가 HTTPS를 사용하여 서버에 연결하면 서버는 공개 키가 포함된 서버 인증서로 응답합니다. 클라이언트는 서버 서명을 인증서 사본의 서명과 비교하여 이 인증서를 확인합니다. 서명이 일치하면 클라이언트는 동일한 공개 키를 사용하여 서버와 세션을 시작합니다.

StorageGRID는 로드 밸런서 끝점과 같은 일부 연결에 대한 서버 또는 CloudMirror 복제 서비스와 같은 다른 연결에 대한 클라이언트로 작동합니다.

외부 CA(인증 기관)는 조직의 정보 보안 정책을 완벽하게 준수하는 사용자 지정 인증서를 발급할 수 있습니다. StorageGRID에는 시스템 설치 중에 내부 CA 인증서를 생성하는 CA(인증 기관)도 내장되어 있습니다. 이러한 내부 CA 인증서는 기본적으로 내부 StorageGRID 트래픽을 보호하기 위해 사용됩니다. 비프로덕션 환경에 내부 CA 인증서를 사용할 수 있지만 프로덕션 환경에 가장 적합한 방법은 외부 인증 기관에서 서명한 사용자 지정 인증서를 사용하는 것입니다. 인증서가 없는 비보안 연결도 지원되지만 권장되지 않습니다.

- 사용자 지정 CA 인증서는 내부 인증서를 제거하지 않지만 사용자 지정 인증서는 서버 연결을 확인하기 위해 지정된 인증서여야 합니다.
- 모든 사용자 지정 인증서는 서버 인증서에 대한 시스템 강화 지침을 충족해야 합니다.

#### "시스템 강화"

- 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.

인증서	인증서 유형입니다	설명	내비게이션 위치	세부 정보
관리자 클라이언트 인증서입니다	클라이언트	<p>각 클라이언트에 설치되어 StorageGRID에서 외부 클라이언트 액세스를 인증할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• 권한이 있는 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있습니다.</li> <li>• 외부 도구를 사용하여 StorageGRID를 안전하게 모니터링할 수 있습니다.</li> </ul>	<ul style="list-style-type: none"> <li>• 구성 * &gt; * 액세스 제어 * &gt; * 클라이언트 인증서 *</li> </ul>	"관리자 클라이언트 인증서를 구성하는 중입니다"
ID 페더레이션 인증서	서버	StorageGRID와 외부 Active Directory, OpenLDAP 또는 Oracle Directory 서버 간의 연결을 인증합니다. ID 페더레이션에 사용되며, 이 ID 페더레이션은 관리 그룹 및 사용자를 외부 시스템에서 관리할 수 있도록 합니다.	<ul style="list-style-type: none"> <li>• 구성 * &gt; * 액세스 제어 * &gt; * ID 페더레이션 *</li> </ul>	"ID 페더레이션 사용"
SSO(Single Sign-On) 인증서	서버	SSO(Single Sign-On) 요청에 사용되는 AD FS(Active Directory Federation Services)와 StorageGRID 간의 연결을 인증합니다.	<ul style="list-style-type: none"> <li>• 구성 * &gt; * 액세스 제어 * &gt; * 단일 사인온 *</li> </ul>	"Single Sign-On 구성"
KMS(키 관리 서버) 인증서	서버 및 클라이언트	StorageGRID와 StorageGRID 어플라이언스 노드에 암호화 키를 제공하는 외부 키 관리 서버(KMS) 간의 연결을 인증합니다.	<ul style="list-style-type: none"> <li>• 구성 * &gt; * 시스템 설정 * &gt; * 키 관리 서버 *</li> </ul>	"KMS(키 관리 서버) 추가"

인증서	인증서 유형입니다	설명	내비게이션 위치	세부 정보
이메일 경고 알림 인증서입니다	서버 및 클라이언트	<p>SMTP 이메일 서버와 알림 알림에 사용되는 StorageGRID 간의 연결을 인증합니다.</p> <ul style="list-style-type: none"> <li>SMTP 서버와의 통신에 TLS(Transport Layer Security)가 필요한 경우 전자 메일 서버 CA 인증서를 지정해야 합니다.</li> <li>SMTP 전자 메일 서버에 인증을 위해 클라이언트 인증서가 필요한 경우에만 클라이언트 인증서를 지정합니다.</li> </ul>	<ul style="list-style-type: none"> <li>경고 * &gt; * 이메일 설정 *</li> </ul>	"모니터링 및 문제 해결"
로드 밸런서 끝점 인증서	서버	<p>게이트웨이 노드 또는 관리 노드에서 S3 또는 Swift 클라이언트와 StorageGRID 로드 밸런서 서비스 간의 연결을 인증합니다. 로드 밸런서 끝점을 구성할 때 로드 밸런서 인증서를 업로드하거나 생성합니다. 클라이언트 응용 프로그램은 StorageGRID에 연결할 때 로드 밸런서 인증서를 사용하여 개체 데이터를 저장하고 검색합니다.</p> <ul style="list-style-type: none"> <li>참고: * 로드 밸런서 인증서는 일반적인 StorageGRID 작업 중에 가장 많이 사용되는 인증서입니다.</li> </ul>	<ul style="list-style-type: none"> <li>구성 * &gt; * 네트워크 설정 * &gt; * 로드 밸런서 엔드포인트 *</li> </ul>	<ul style="list-style-type: none"> <li>"부하 분산 장치 엔드포인트 구성"</li> <li>FabricPool용 로드 밸런서 끝점 생성</li> <li>"FabricPool용 StorageGRID를 구성합니다"</li> </ul>

인증서	인증서 유형입니다	설명	내비게이션 위치	세부 정보
관리 인터페이스 서버 인증서	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>내부 CA 인증서를 사용하거나 사용자 지정 인증서를 업로드할 수 있습니다.</p>	<ul style="list-style-type: none"> <li>구성 * &gt; * 네트워크 설정 * &gt; * 서버 인증서 *</li> </ul>	<ul style="list-style-type: none"> <li>"서버 인증서를 구성하는 중입니다"</li> <li>"Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성"</li> </ul>
Cloud Storage Pool 엔드포인트 인증서입니다	서버	<p>StorageGRID 클라우드 스토리지 풀에서 외부 스토리지 위치(예: S3 Glacier 또는 Microsoft Azure Blob 저장소)로 연결을 인증합니다. 각 클라우드 공급자 유형에는 다른 인증서가 필요합니다.</p>	<ul style="list-style-type: none"> <li>ILM * &gt; * 스토리지 풀 *</li> </ul>	"ILM을 사용하여 개체를 관리합니다"
플랫폼 서비스 끝점 인증서	서버	<p>StorageGRID 플랫폼 서비스에서 S3 스토리지 리소스에 대한 연결을 인증합니다.</p>	<ul style="list-style-type: none"> <li>테넌트 관리자 * &gt; * 스토리지(S3) * &gt; * 플랫폼 서비스 엔드포인트 *</li> </ul>	"테넌트 계정을 사용합니다"
객체 스토리지 API 서비스 엔드포인트 서버 인증서입니다	서버	<p>스토리지 노드의 LDR(Local Distribution Router) 서비스 또는 게이트웨이 노드의 더 이상 사용되지 않는 CLB(Connection Load Balancer) 서비스에 대한 보안 S3 또는 Swift 클라이언트 연결을 인증합니다.</p>	<ul style="list-style-type: none"> <li>구성 * &gt; * 네트워크 설정 * &gt; * 로드 밸런서 엔드포인트 *</li> </ul>	"스토리지 노드 또는 CLB 서비스에 연결하기 위한 사용자 지정 서버 인증서 구성"

## 예 1: 부하 분산 서비스

이 예에서 StorageGRID는 서버 역할을 합니다.

1. 로드 밸런서 끝점을 구성하고 StorageGRID에서 서버 인증서를 업로드하거나 생성합니다.
2. 로드 밸런서 끝점에 S3 또는 Swift 클라이언트 연결을 구성하고 동일한 인증서를 클라이언트에 업로드합니다.
3. 클라이언트가 데이터를 저장하거나 검색하려는 경우 HTTPS를 사용하여 로드 밸런서 끝점에 연결합니다.
4. StorageGRID는 공개 키가 포함된 서버 인증서와 개인 키를 기반으로 하는 서명으로 응답합니다.
5. 클라이언트는 서버 서명을 인증서 사본의 서명과 비교하여 이 인증서를 확인합니다. 서명이 일치하면 클라이언트는 동일한 공개 키를 사용하여 세션을 시작합니다.
6. 클라이언트가 StorageGRID로 개체 데이터를 보냅니다.

## 예 2: 외부 키 관리 서버(KMS)

이 예에서 StorageGRID는 클라이언트 역할을 합니다.

1. 외부 키 관리 서버 소프트웨어를 사용하면 StorageGRID를 KMS 클라이언트로 구성하고 CA 서명된 서버 인증서, 공용 클라이언트 인증서 및 클라이언트 인증서에 대한 개인 키를 얻을 수 있습니다.
2. Grid Manager를 사용하여 KMS 서버를 구성하고 서버 및 클라이언트 인증서와 클라이언트 개인 키를 업로드합니다.
3. StorageGRID 노드에 암호화 키가 필요한 경우, 이 노드는 인증서의 데이터와 개인 키를 기반으로 하는 서명을 포함하는 KMS 서버에 요청합니다.
4. KMS 서버는 인증서 서명의 유효성을 검사하고 StorageGRID를 신뢰할 수 있는지 결정합니다.
5. KMS 서버는 검증된 연결을 사용하여 응답합니다.

# StorageGRID에 대한 관리자 액세스 제어

방화벽 포트를 열거나 닫거나, 관리 그룹 및 사용자를 관리하고, SSO(Single Sign-On)를 구성하고, StorageGRID 메트릭에 대한 안전한 외부 액세스를 허용하는 클라이언트 인증서를 제공하여 StorageGRID 시스템에 대한 관리자 액세스를 제어할 수 있습니다.

- "방화벽을 통한 액세스 제어"
- "ID 페더레이션 사용"
- "관리 그룹 관리"
- "로컬 사용자 관리"
- "StorageGRID용 SSO(Single Sign-On) 사용"
- "관리자 클라이언트 인증서를 구성하는 중입니다"

## 방화벽을 통한 액세스 제어

방화벽을 통해 액세스를 제어하려면 외부 방화벽에서 특정 포트를 열거나 닫습니다.

## 외부 방화벽에서 액세스 제어

외부 방화벽에서 특정 포트를 열거나 닫아 StorageGRID 관리 노드의 사용자 인터페이스 및 API에 대한 액세스를 제어할 수 있습니다. 예를 들어, 테넌트가 다른 방법을 사용하여 시스템 액세스를 제어하는 것 외에도 방화벽에서 Grid Manager에 연결할 수 없도록 할 수 있습니다.

포트	설명	포트가 열려 있는 경우...
443	관리 노드의 기본 HTTPS 포트	<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"> <li>참고: * 포트 443은 일부 내부 트래픽에도 사용됩니다.</li> </ul>
8443	관리 노드의 제한된 그리드 관리자 포트	<ul style="list-style-type: none"> <li>웹 브라우저 및 관리 API 클라이언트는 HTTPS를 사용하여 그리드 관리자 및 그리드 관리 API에 액세스할 수 있습니다.</li> <li>웹 브라우저 및 관리 API 클라이언트는 테넌트 관리자 또는 테넌트 관리 API에 액세스할 수 없습니다.</li> <li>내부 콘텐츠 요청은 거부됩니다.</li> </ul>
9443	관리 노드의 제한된 테넌트 관리자 포트	<ul style="list-style-type: none"> <li>웹 브라우저 및 관리 API 클라이언트는 HTTPS를 사용하여 테넌트 관리자 및 테넌트 관리 API에 액세스할 수 있습니다.</li> <li>웹 브라우저 및 관리 API 클라이언트는 그리드 관리자 또는 그리드 관리 API에 액세스할 수 없습니다.</li> <li>내부 콘텐츠 요청은 거부됩니다.</li> </ul>



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"](#)

["StorageGRID에서 SSO를 사용하지 않는 경우 테넌트 계정 생성"](#)

["요약: 클라이언트 연결을 위한 IP 주소 및 포트"](#)

["신뢰할 수 없는 클라이언트 네트워크 관리"](#)

["Ubuntu 또는 Debian을 설치합니다"](#)

["VMware를 설치합니다"](#)

["Red Hat Enterprise Linux 또는 CentOS를 설치합니다"](#)



## ID 페더레이션 사용

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

### ID 페더레이션을 구성하는 중입니다

관리 그룹 및 사용자를 Active Directory, OpenLDAP 또는 Oracle Directory Server와 같은 다른 시스템에서 관리하도록 하려면 ID 페더레이션을 구성할 수 있습니다.

#### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- SSO(Single Sign-On)를 사용하려는 경우 통합 ID 소스로 Active Directory를 사용하고 ID 공급자로 AD FS를 사용해야 합니다. Single Sign-On 사용 요건 참조
- ID 공급자로 Active Directory, OpenLDAP 또는 Oracle Directory Server를 사용하고 있어야 합니다.



목록에 없는 LDAP v3 서비스를 사용하려면 기술 지원 부서에 문의해야 합니다.

- LDAP 서버와의 통신에 TLS(Transport Layer Security)를 사용하려는 경우 ID 공급자는 TLS 1.2 또는 1.3을 사용해야 합니다.

#### 이 작업에 대해

다음과 같은 유형의 통합 그룹을 가져오려면 그리드 관리자의 ID 소스를 구성해야 합니다.

- 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.

#### 단계

1. Configuration \* > \* Access Control \* > \* Identity Federation \* 을 선택합니다.
2. ID 페더레이션 사용 \* 을 선택합니다.

LDAP 서버 구성 필드가 나타납니다.

3. LDAP 서비스 유형 섹션에서 구성할 LDAP 서비스 유형을 선택합니다.

Active Directory \*, \* OpenLDAP \* 또는 \* 기타 \* 를 선택할 수 있습니다.



OpenLDAP \* 를 선택한 경우 OpenLDAP 서버를 구성해야 합니다. OpenLDAP 서버 구성 지침을 참조하십시오.



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

4. 기타 \* 를 선택한 경우 LDAP 속성 섹션의 필드를 작성합니다.

- \* 사용자 고유 이름 \*: LDAP 사용자의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 과 같습니다 sAMAccountName Active Directory 및 의 경우 uid OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 uid.
- \* 사용자 UUID \*: LDAP 사용자의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 과 같습니다 objectGUID Active Directory 및 의 경우 entryUUID OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 nsuniqueid. 지정된 속성에 대한 각 사용자의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.
- \* 그룹 고유 이름 \*: LDAP 그룹의 고유 식별자가 포함된 속성의 이름입니다. 이 속성은 과 같습니다 sAMAccountName Active Directory 및 의 경우 cn OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 cn.
- \* 그룹 UUID \*: LDAP 그룹의 영구 고유 식별자가 포함된 특성의 이름입니다. 이 속성은 과 같습니다 objectGUID Active Directory 및 의 경우 entryUUID OpenLDAP의 경우. Oracle Directory Server를 구성하는 경우 를 입력합니다 nsuniqueid. 지정된 속성에 대한 각 그룹의 값은 16바이트 또는 문자열 형식의 32자리 16진수 숫자여야 하며, 하이픈은 무시됩니다.

5. LDAP 서버 구성 섹션에서 필요한 LDAP 서버 및 네트워크 연결 정보를 입력합니다.

- \* 호스트 이름 \*: LDAP 서버의 서버 호스트 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 로그인 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
- \* 암호 \*: 사용자 이름과 연결된 암호입니다.
- \* Group base DN \*: 그룹을 검색할 LDAP 하위 트리에 대한 DN(고유 이름)의 전체 경로입니다. Active Directory 예제(아래)에서 고유 이름이 기본 DN(DC=StorageGrid, DC=example, DC=com)과 관련된 모든 그룹을 통합 그룹으로 사용할 수 있습니다.



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

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



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

6. TLS(Transport Layer Security) \* 섹션에서 보안 설정을 선택합니다.

- \* STARTTLS 사용(권장) \*: STARTTLS를 사용하여 LDAP 서버와의 통신을 보호합니다. 이 옵션을 선택하는 것이 좋습니다.
- \* LDAPS \* 사용: LDAPS(LDAP over SSL) 옵션은 TLS를 사용하여 LDAP 서버에 연결합니다. 이 옵션은 호환성을 위해 지원됩니다.
- \* TLS \* 사용 안 함: StorageGRID 시스템과 LDAP 서버 간의 네트워크 트래픽은 보호되지 않습니다.



Active Directory 서버가 LDAP 서명을 적용하는 경우 \* TLS 사용 안 함 \* 옵션을 사용할 수 없습니다. STARTTLS 또는 LDAPS를 사용해야 합니다.

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

- \* 운영 체제 CA 인증서 사용 \*: 운영 체제에 설치된 기본 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.

8. 선택적으로 \* 연결 테스트 \* 를 선택하여 LDAP 서버에 대한 연결 설정을 확인합니다.

연결이 유효한 경우 페이지의 오른쪽 상단에 확인 메시지가 나타납니다.

9. 연결이 유효하면 \* 저장 \* 을 선택합니다.

다음 스크린샷은 Active Directory를 사용하는 LDAP 서버의 구성 값 예를 보여 줍니다.

## LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

OpenLDAP

Other

## Configure LDAP server (All fields are required)

Hostname

my-active-directory.example.com

Port

389

Username

MyDomain\Administrator

Password

●●●●●●●●

Group Base DN

DC=storagegrid,DC=example,DC=com

User Base DN

DC=storagegrid,DC=example,DC=com

관련 정보

["발신 TLS 연결에 지원되는 암호"](#)

["Single Sign-On 사용에 대한 요구 사항"](#)

["테넌트 계정을 생성하는 중입니다"](#)

["테넌트 계정을 사용합니다"](#)

**OpenLDAP** 서버 구성 지침

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

## MemberOf 및 구체화 오버레이

MemberOf 및 구체화 오버레이를 활성화해야 합니다. 자세한 내용은 OpenLDAP용 관리자 안내서 에서 역방향 그룹 구성원 유지 관리 지침을 참조하십시오.

### 인덱싱

지정된 인덱스 키워드를 사용하여 다음 OpenLDAP 속성을 구성해야 합니다.

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

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

OpenLDAP용 관리자 안내서 에서 역방향 그룹 구성원 유지 관리에 대한 정보를 참조하십시오.

### 관련 정보

["OpenLDAP 설명서: 버전 2.4 관리자 가이드"](#)

## ID 소스와 동기화 수행

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

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- ID 소스를 활성화해야 합니다.

### 단계

1. Configuration \* > \* Access Control \* > \* Identity Federation \* 을 선택합니다.

ID 페더레이션 페이지가 나타납니다. 동기화 \* 버튼은 페이지 하단에 있습니다.

#### Synchronize

StorageGRID periodically synchronizes federated groups and users from the configured LDAP server. Clicking the button below will immediately start the synchronization process against the saved LDAP server.

Synchronize

2. 동기화 \* 를 클릭합니다.

동기화가 성공적으로 시작되었다는 확인 메시지가 표시됩니다. 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 사용하지 않도록 설정합니다

그룹 및 사용자에 대한 ID 페더레이션을 일시적으로 또는 영구적으로 비활성화할 수 있습니다. ID 페더레이션을 사용하지 않도록 설정하면 StorageGRID와 ID 소스 간에 통신이 이루어지지 않습니다. 그러나 구성된 설정은 그대로 유지되므로 나중에 ID 페더레이션을 쉽게 다시 사용할 수 있습니다.

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

### 이 작업에 대해

ID 페더레이션을 사용하지 않도록 설정하기 전에 다음 사항을 확인해야 합니다.

- 페더레이션 사용자는 로그인할 수 없습니다.
- 현재 로그인한 페더레이션 사용자는 세션이 만료될 때까지 StorageGRID 시스템에 대한 액세스 권한을 유지하지만 세션이 만료된 후에는 로그인할 수 없습니다.
- StorageGRID 시스템과 ID 소스 간의 동기화는 수행되지 않으며 동기화되지 않은 계정에 대해 알림 또는 경보가 발생하지 않습니다.
- SSO(Single Sign-On)가 \* Enabled \* 또는 \* Sandbox Mode \* 로 설정된 경우 \* Enable Identity Federation \*(ID 페더레이션 사용 \*) 확인란이 비활성화됩니다. ID 페더레이션을 비활성화하려면 Single Sign-On 페이지의 SSO 상태가 \* 사용 안 함 \* 이어야 합니다.

### 단계

1. Configuration \* > \* Access Control \* > \* Identity Federation \* 을 선택합니다.
2. ID 페더레이션 사용 \* 확인란의 선택을 취소합니다.
3. 저장 \* 을 클릭합니다.

### 관련 정보

["SSO\(Single Sign-On\) 비활성화"](#)

## 관리 그룹 관리

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

### 관리 그룹 생성 중

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

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

- 특정 액세스 권한이 있어야 합니다.
- 통합 그룹을 가져오려면 ID 페더레이션을 구성해야 하며 통합 그룹은 구성된 ID 소스에 이미 있어야 합니다.

단계

1. Configuration \* \* \* Access Control \* \* Admin Groups \* 를 선택합니다.

관리 그룹 페이지가 나타나고 기존 관리 그룹이 나열됩니다.

### Admin Groups

Add and manage local and federated user groups, allowing member users to sign in to the Grid Manager. Set group permissions to control access to specific pages and features.

<input type="button" value="+ Add"/> <input type="button" value="Clone"/> <input type="button" value="Edit"/> <input type="button" value="x Remove"/>				
	Name	ID	Group Type ?	Access Mode ?
<input checked="" type="radio"/>	Flintstone	264083d0-23b5-3046-9bd4-88b7097731ab	Federated	Read-write
<input type="radio"/>	Simpson	cc8ad11f-68d0-f84a-af29-e7a6fcdc63a2	Federated	Read-only
<input type="radio"/>	ILM (read-only group)	88446141-9599-4543-b183-9c227ce7767a	Local	Read-only
<input type="radio"/>	API Developers	974b2faa-f9a1-4cfc-b364-914cdba2905f	Local	Read-write
<input type="radio"/>	ILM Admins (read-write)	a528c0c2-2417-4559-86ed-f0d2e31da820	Local	Read-write
<input type="radio"/>	Maintenance Users	7e3400ec-de8c-45a7-8bb8-e1496b362a8d	Local	Read-write

Group Type: All ▾ Show 20 ▾ rows per page

2. 추가 \* 를 선택합니다.

그룹 추가 대화 상자가 나타납니다.

## Add Group

Create a new local group or import a group from the external identity source.

Group Type  Local  Federated

Display Name

Unique Name

Access Mode  Read-write  Read-only

### Management Permissions

- |  |   |
|--|---|
| <input type="checkbox"/> Root Access                 | <input type="checkbox"/> Manage Alerts                    |
| <input type="checkbox"/> Acknowledge Alarms          | <input type="checkbox"/> Grid Topology Page Configuration |
| <input type="checkbox"/> Other Grid Configuration    | <input type="checkbox"/> Tenant Accounts                  |
| <input type="checkbox"/> Change Tenant Root Password | <input type="checkbox"/> Maintenance                      |
| <input type="checkbox"/> Metrics Query               | <input type="checkbox"/> ILM                              |
| <input type="checkbox"/> Object Metadata Lookup      | <input type="checkbox"/> Storage Appliance Administrator  |

Cancel

Save

- 그룹 유형 에서 StorageGRID 내에서만 사용할 그룹을 만들려면 \* 로컬 \* 을 선택하고, ID 소스에서 그룹을 가져오려면 \* 통합 \* 을 선택합니다.
- Local \* 을 선택한 경우 그룹의 표시 이름을 입력합니다. 표시 이름은 그리드 관리자에 나타나는 이름입니다. 예를 들어, "유지 보수 사용자" 또는 ""ILM 관리자""가 있습니다.
- 그룹의 고유한 이름을 입력합니다.
  - \* 로컬 \*: 원하는 고유한 이름을 입력합니다. 예: ""ILM 관리자""
  - \* Federated \*: 구성된 ID 소스에 표시된 대로 그룹의 이름을 정확하게 입력합니다.
- 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.

- 하나 이상의 관리 권한을 선택합니다.



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

8. 저장 \* 을 선택합니다.

새 그룹이 생성됩니다. 로컬 그룹인 경우 하나 이상의 사용자를 추가할 수 있습니다. 통합 그룹인 경우 ID 소스는 그룹에 속한 사용자를 관리합니다.

관련 정보

["로컬 사용자 관리"](#)

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 Manager에 로그인할 수 없습니다.

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

- Grid Manager에 로그인합니다
- 대시보드 보기
- 노드 페이지를 봅니다
- 그리드 토폴로지를 모니터링합니다
- 현재 및 해결된 경고를 봅니다
- 현재 및 과거 알람 보기(레거시 시스템)
- 자신의 암호 변경(로컬 사용자만 해당)
- 구성 및 유지 관리 페이지에서 특정 정보를 봅니다

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.

알림 관리

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

알람 확인(레거시 시스템)

이 권한을 통해 알람(레거시 시스템)을 확인하고 이에 대응할 수 있습니다. 로그인한 모든 사용자는 현재 및 과거 알람을 볼 수 있습니다.

사용자가 그리드 토폴로지를 모니터링하고 알람을 확인하려면 이 권한을 할당해야 합니다.

## 그리드 토폴로지 페이지 구성

이 권한을 통해 다음 메뉴 옵션에 액세스할 수 있습니다.

- 지원 \*\* 도구 \* 그리드 토폴로지 \* 의 페이지에서 사용할 수 있는 구성 탭.
- \* 노드 \*\* 이벤트 \* 탭에서 이벤트 카운트 \* 링크를 재설정합니다.

## 기타 그리드 구성

이 권한은 추가 그리드 구성 옵션에 대한 액세스를 제공합니다.



이러한 추가 옵션을 보려면 그리드 토폴로지 페이지 구성 권한도 있어야 합니다.

- 알람 \* (레거시 시스템):
  - 전체 알람
  - 레거시 이메일 설정
- \* ILM \*:
  - 스토리지 풀
  - 보관 등급
- \* 구성 \*\* 네트워크 설정 \*
  - 링크 비용
- \* 구성 \*\* 시스템 설정 \*:
  - 표시 옵션
  - 그리드 옵션
  - 스토리지 옵션
- \* 구성 \*\* 모니터링 \*:
  - 이벤트
- \* 지원 \*:
  - AutoSupport

## 테넌트 계정

이 권한은 \* Tenants \*\* \* Tenant Accounts \* 페이지에 대한 액세스를 제공합니다.



Grid Management API 버전 1(더 이상 사용되지 않음)에서는 이 권한을 사용하여 테넌트 그룹 정책을 관리하고, Swift 관리자 암호를 재설정하고, 루트 사용자 S3 액세스 키를 관리합니다.

## 테넌트 루트 암호를 변경합니다

이 권한은 테넌트 계정 페이지의 \* 루트 암호 변경 \* 옵션에 대한 액세스를 제공하므로 테넌트의 로컬 루트 사용자에게 대한 암호를 변경할 수 있는 사용자를 제어할 수 있습니다. 이 권한이 없는 사용자는 \* 루트 암호 변경 \* 옵션을 볼 수 없습니다.



이 권한을 할당하려면 먼저 그룹에 테넌트 계정 권한을 할당해야 합니다.

#### 유지 관리

이 권한을 통해 다음 메뉴 옵션에 액세스할 수 있습니다.

- \* 구성 \* \* 시스템 설정 \* :
  - 도메인 이름 \*
  - 서버 인증서 \*
- \* 구성 \* \* 모니터링 \* :
  - 감사 \*
- \* 구성 \* \* 액세스 제어 \* :
  - 그리드 암호
- \* 유지보수 \* \* 유지보수 태스크 \*
  - 서비스 해제
  - 확장
  - 복구
- \* 유지보수 \* \* 네트워크 \* :
  - DNS 서버 \*
  - 그리드 네트워크 \*
  - NTP 서버 \*
- \* 유지보수 \* \* 시스템 \* :
  - 라이선스 \*
  - 복구 패키지
  - 소프트웨어 업데이트
- \* 지원 \* \* 툴 \* :
  - 로그
- 유지 관리 권한이 없는 사용자는 별표가 표시된 페이지를 볼 수는 있지만 편집할 수는 없습니다.

#### 메트릭 쿼리

이 권한은 \* 지원 \* \* 도구 \* 메트릭 \* 페이지에 대한 액세스를 제공합니다. 이 권한은 또한 Grid Management API의 \* Metrics \* 섹션을 사용하여 맞춤형 Prometheus 메트릭 쿼리에 대한 액세스를 제공합니다.

#### ILM을 참조하십시오

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

- \* 삭제 코딩 \*
- \* 규칙 \*

• \* 정책 \*

• \* 지역 \*



ILM \*\*\* 스토리지 풀 \* 및 \* ILM \*\* 스토리지 등급 \* 메뉴 옵션에 대한 액세스는 다른 그리드 구성 및 그리드 토폴로지 페이지 구성 권한에 의해 제어됩니다.

개체 메타데이터 조회

이 권한은 \* ILM \*\* 개체 메타데이터 조회 \* 메뉴 옵션에 대한 액세스를 제공합니다.

스토리지 어플라이언스 관리자

이 권한은 그리드 관리자를 통해 스토리지 어플라이언스에서 E-Series SANtricity System Manager에 대한 액세스를 제공합니다.

사용 권한과 액세스 모드 간의 상호 작용

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

**Grid Management API**에서 기능 비활성화

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 액세스 권한이 있는 관리자 그룹에 속한 루트 사용자나 사용자가 해당 기능을 사용할 수 없도록 하는 유일한 방법은 기능을 비활성화하는 것입니다.

이 기능이 어떻게 유용한지 이해하려면 다음 시나리오를 고려해 보십시오.

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

\_회사 A는 그리드 관리 API에서 기능 비활성화 시스템을 사용하여 이 목표를 달성할 수 있습니다. 그리드 관리자(UI 및 API 모두)에서 \* 테넌트 루트 암호 변경 \* 기능을 완전히 비활성화함으로써 회사 A는 루트 액세스 권한이 있는 그룹에 속하는 루트 사용자 및 루트 사용자를 포함한 관리자 사용자가 테넌트 계정의 루트 사용자에 대한 암호를 변경할 수 없도록 할 수 있습니다

비활성화된 피처를 다시 활성화합니다

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



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

자세한 내용은 S3 또는 Swift 클라이언트 애플리케이션 구현 지침을 참조하십시오.

#### 단계

1. Grid Management API에 대한 Swagger 문서에 액세스합니다.
2. 기능 비활성화 끝점을 찾습니다.
3. 테넌트 루트 암호 변경 \* 과 같은 기능을 비활성화하려면 다음과 같이 API로 본문을 보냅니다.

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

요청이 완료되면 테넌트 루트 암호 변경 기능이 비활성화됩니다. 테넌트 루트 암호 변경 관리 권한이 사용자 인터페이스에 더 이상 나타나지 않으며 테넌트의 루트 암호를 변경하려고 시도하는 모든 API 요청이 "403 사용 금지"로 실패합니다.

4. 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, Change Tenant Root Password 기능을 다시 활성화하고 Alarm Acknowledgement 기능을 계속 비활성화하려면 다음 Put 요청을 보냅니다.

```
{ "grid": { "alarmAcknowledgment": true } }
```

#### 관련 정보

##### ["Grid Management API 사용"](#)

#### 관리 그룹 수정

admin 그룹을 수정하여 그룹과 연결된 권한을 변경할 수 있습니다. 로컬 관리자 그룹의 경우 표시 이름을 업데이트할 수도 있습니다.

#### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

#### 단계

1. Configuration \* \* \* Access Control \* \* Admin Groups \* 를 선택합니다.
2. 그룹을 선택합니다.

시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 그런 다음 브라우저의 찾기 기능을 사용하여 현재 표시된 행에서 특정 항목을 검색할 수 있습니다.

3. 편집 \* 을 클릭합니다.
4. 또는 로컬 그룹의 경우 사용자에게 표시할 그룹 이름(예: "유지보수 사용자")을 입력합니다.

내부 그룹 이름인 고유한 이름은 변경할 수 없습니다.

5. 선택적으로 그룹의 액세스 모드를 변경합니다.
  - \* 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.

6. 필요에 따라 그룹 권한을 추가하거나 제거합니다.

관리자 그룹 권한에 대한 정보를 봅니다.

7. 저장 \* 을 선택합니다.

#### 관련 정보

#### [관리자 그룹 권한](#)

#### 관리 그룹 삭제

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

#### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

#### 이 작업에 대해

그룹을 삭제하면 다른 그룹에 의해 권한을 부여하지 않는 한 해당 그룹에 할당된 사용자는 그리드 관리자에 대한 모든 액세스 권한을 잃게 됩니다.

#### 단계

1. Configuration \* \* \* Access Control \* \* Admin Groups \* 를 선택합니다.
2. 그룹 이름을 선택합니다.

시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 그런 다음 브라우저의 찾기 기능을 사용하여 현재 표시된 행에서 특정 항목을 검색할 수 있습니다.

3. 제거 \* 를 선택합니다.
4. OK \* 를 선택합니다.

## 로컬 사용자 관리

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

Grid Manager에는 ""root""라는 이름의 미리 정의된 로컬 사용자가 하나 있습니다. 로컬 사용자를 추가 및 제거할 수는 있지만 루트 사용자는 제거할 수 없습니다.



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

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

### 로컬 사용자 생성

로컬 관리자 그룹을 생성한 경우 하나 이상의 로컬 사용자를 생성하고 각 사용자를 하나 이상의 그룹에 할당할 수 있습니다. 그룹의 권한은 사용자가 액세스할 수 있는 Grid Manager 기능을 제어합니다.

#### 이 작업에 대해

로컬 사용자만 생성할 수 있으며 이러한 사용자는 로컬 관리자 그룹에만 할당할 수 있습니다. 통합 사용자 및 통합 그룹은 외부 ID 소스를 사용하여 관리됩니다.

#### 단계

1. Configuration \* > \* Access Control \* > \* Admin Users \* 를 선택합니다.
2. Create \* 를 클릭합니다.
3. 사용자의 표시 이름, 고유 이름 및 암호를 입력합니다.
4. 액세스 권한을 제어하는 하나 이상의 그룹에 사용자를 할당합니다.

그룹 이름 목록은 그룹 테이블에서 생성됩니다.

5. 저장 \* 을 클릭합니다.

#### 관련 정보

["관리 그룹 관리"](#)

### 로컬 사용자 계정 수정

로컬 관리자 사용자 계정을 수정하여 사용자의 표시 이름 또는 그룹 구성원을 업데이트할 수 있습니다. 또한 사용자가 일시적으로 시스템에 액세스하지 못하도록 할 수도 있습니다.

#### 이 작업에 대해

로컬 사용자만 편집할 수 있습니다. 통합 사용자 세부 정보는 외부 ID 소스와 자동으로 동기화됩니다.

#### 단계

1. Configuration \* > \* Access Control \* > \* Admin Users \* 를 선택합니다.
2. 편집할 사용자를 선택합니다.

시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 그런 다음 브라우저의 찾기 기능을 사용하여 현재 표시된 행에서 특정 항목을 검색할 수 있습니다.

3. 편집 \* 을 클릭합니다.
4. 필요에 따라 이름 또는 그룹 구성원을 변경합니다.
5. 선택적으로 사용자가 시스템에 일시적으로 액세스하지 못하게 하려면 \* 액세스 거부 \* 를 선택합니다.
6. 저장 \* 을 클릭합니다.

다음 번에 사용자가 로그아웃한 다음 그리드 관리자에 다시 로그인할 때 새 설정이 적용됩니다.

## 로컬 사용자 계정을 삭제하는 중입니다

더 이상 Grid Manager에 액세스할 필요가 없는 로컬 사용자의 계정을 삭제할 수 있습니다.

### 단계

1. Configuration \* > \* Access Control \* > \* Admin Users \* 를 선택합니다.
2. 삭제할 로컬 사용자를 선택합니다.



사전 정의된 루트 로컬 사용자는 삭제할 수 없습니다.

시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 그런 다음 브라우저의 찾기 기능을 사용하여 현재 표시된 행에서 특정 항목을 검색할 수 있습니다.

3. 제거 \* 를 클릭합니다.
4. 확인 \* 을 클릭합니다.

## 로컬 사용자 암호 변경

로컬 사용자는 Grid Manager 배너의 \* Change Password \* 옵션을 사용하여 자신의 암호를 변경할 수 있습니다. 또한 관리자 사용자 페이지에 액세스할 수 있는 사용자는 다른 로컬 사용자의 암호를 변경할 수 있습니다.

### 이 작업에 대해

로컬 사용자의 암호만 변경할 수 있습니다. 통합 사용자는 외부 ID 원본에서 자신의 암호를 변경해야 합니다.

### 단계

1. Configuration \* > \* Access Control \* > \* Admin Users \* 를 선택합니다.
2. 사용자 페이지에서 사용자를 선택합니다.

시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 그런 다음 브라우저의 찾기 기능을 사용하여 현재 표시된 행에서 특정 항목을 검색할 수 있습니다.

3. 암호 변경 \* 을 클릭합니다.
4. 암호를 입력 및 확인하고 \* 저장 \* 을 클릭합니다.



## StorageGRID용 SSO(Single Sign-On) 사용

StorageGRID 시스템은 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용하여 SSO(Single Sign-On)를 지원합니다. SSO가 활성화된 경우 모든 사용자는 Grid Manager, Tenant Manager, Grid Management API 또는 Tenant Management API에 액세스하기 전에 외부 ID 공급자에 의해 인증되어야 합니다. 로컬 사용자는 StorageGRID에 로그인할 수 없습니다.

- "Single Sign-On의 작동 방식"
- "Single Sign-On 사용에 대한 요구 사항"
- "Single Sign-On 구성"

### Single Sign-On의 작동 방식

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

SSO가 활성화되어 있을 때 로그인합니다

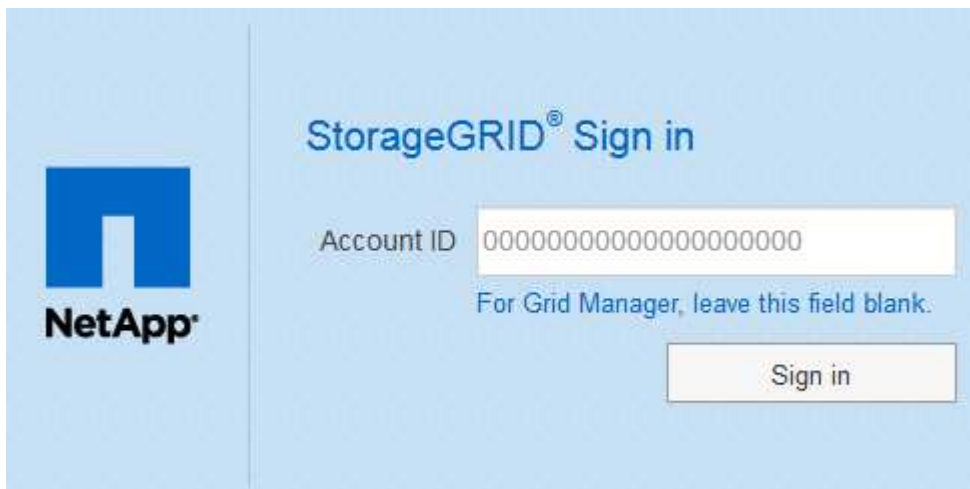
SSO가 활성화되어 있고 StorageGRID에 로그인하면 조직의 SSO 페이지로 리디렉션되어 자격 증명을 검증합니다.

단계

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

StorageGRID 로그인 페이지가 나타납니다.

- 이 브라우저에서 URL에 처음 액세스한 경우 계정 ID를 입력하라는 메시지가 표시됩니다.

A screenshot of the StorageGRID Sign in page. On the left is the NetApp logo. The main content area has the title "StorageGRID® Sign in". Below the title is a form with a label "Account ID" and a text input field containing "00000000000000000000". Below the input field is the text "For Grid Manager, leave this field blank." At the bottom right of the form is a "Sign in" button.

- 이전에 Grid Manager 또는 Tenant Manager에 액세스한 경우, 최근 계정을 선택하거나 계정 ID를 입력하라는 메시지가 나타납니다.



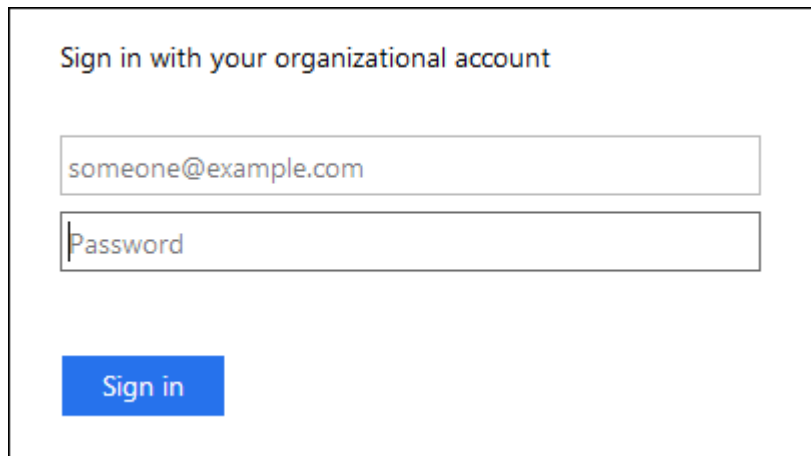
테넌트 계정의 전체 URL(즉, 정규화된 도메인 이름 또는 IP 주소 뒤에 오는)을 입력하면 StorageGRID 로그인 페이지가 표시되지 않습니다 `/?accountId=20-digit-account-id` )를 클릭합니다. 대신 조직의 SSO 로그인 페이지로 즉시 리디렉션됩니다. 여기에서 해당 페이지로 이동할 수 있습니다 [SSO 자격 증명으로 로그인합니다](#).

2. 그리드 관리자 또는 테넌트 관리자에 액세스할지 여부를 지정합니다.

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

3. 로그인 \* 을 클릭합니다

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 적절한 액세스 권한이 있는 통합 그룹에 속해 있는 경우 선택한 계정에 따라 Grid Manager

또는 Tenant Manager에 로그인됩니다.

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

SSO 자격 증명을 다시 입력하지 않아도 됩니다.

#### SSO가 활성화된 경우 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 클릭합니다.

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

에 로그인한 경우...	에서 로그아웃합니다.	에서 로그아웃되었습니다...
하나 이상의 관리 노드에서 그리드 관리자	모든 관리 노드의 그리드 관리자	모든 관리 노드의 그리드 관리자
하나 이상의 관리 노드에서 테넌트 관리자	모든 관리 노드의 테넌트 관리자	모든 관리 노드의 테넌트 관리자
Grid Manager와 Tenant Manager 모두	그리드 관리자	그리드 관리자 전용. SSO에서 로그아웃하려면 테넌트 관리자에서 로그아웃해야 합니다.



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

#### Single Sign-On 사용에 대한 요구 사항

StorageGRID 시스템에 대해 SSO(Single Sign-On)를 활성화하기 전에 이 섹션의 요구 사항을 검토하십시오.



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.

#### ID 공급자 요구 사항

SSO의 ID 공급자(IDP)는 다음 요구 사항을 충족해야 합니다.

- 다음 AD FS(Active Directory Federation Service) 버전 중 하나:

- AD FS 4.0, Windows Server 2016에 포함되어 있습니다



Windows Server 2016에서 을 사용해야 합니다 "KB3201845 업데이트"또는 그 이상.

- AD FS 3.0, Windows Server 2012 R2 업데이트 이상에 포함되어 있습니다.

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

#### 서버 인증서 요구 사항

StorageGRID는 각 관리 노드의 관리 인터페이스 서버 인증서를 사용하여 그리드 관리자, 테넌트 관리자, 그리드 관리 API 및 테넌트 관리 API에 대한 액세스를 보호합니다. AD FS에서 StorageGRID에 대한 SSO 기반 당사자 트러스트를 구성하는 경우 서버 인증서를 AD FS에 대한 StorageGRID 요청에 대한 서명 인증서로 사용합니다.

관리 인터페이스에 대한 사용자 지정 서버 인증서를 아직 설치하지 않았다면 지금 설치해야 합니다. 사용자 지정 서버 인증서를 설치하면 모든 관리 노드에 사용되며 모든 StorageGRID 사용 상대 트러스트에 사용할 수 있습니다.



AD FS 기반 당사자 신뢰에서 관리 노드의 기본 서버 인증서를 사용하는 것은 권장되지 않습니다. 노드가 실패하고 복구되면 새로운 기본 서버 인증서가 생성됩니다. 복구된 노드에 로그인하려면 먼저 AD FS의 기반 당사자 신뢰를 새 인증서로 업데이트해야 합니다.

노드의 명령 셸에 로그인하고 로 이동하여 관리 노드의 서버 인증서에 액세스할 수 있습니다 `/var/local/mgmt-api` 디렉토리. 사용자 지정 서버 인증서의 이름이 지정됩니다 `custom-server.crt`. 노드의 기본 서버 인증서 이름은 `server.crt`.

#### 관련 정보

["방화벽을 통한 액세스 제어"](#)

["Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성"](#)

#### Single Sign-On 구성

SSO(Single Sign-On)가 활성화된 경우 사용자는 조직에서 구현한 SSO 로그인 프로세스를 사용하여 자격 증명이 승인된 경우에만 Grid Manager, Tenant Manager, Grid Management API 또는 Tenant Management API에 액세스할 수 있습니다.

- ["페더레이션 사용자가 로그인할 수 있는지 확인합니다"](#)
- ["sandbox 모드 사용"](#)
- ["AD FS에서 기반 당사자 신뢰를 생성합니다"](#)
- ["신뢰할 수 있는 당사자 신뢰 테스트"](#)
- ["SSO\(Single Sign-On\) 활성화"](#)
- ["SSO\(Single Sign-On\) 비활성화"](#)
- ["하나의 관리 노드에 대해 SSO\(Single Sign-On\)를 일시적으로 비활성화 및 다시 활성화합니다"](#)

페더레이션 사용자가 로그인할 수 있는지 확인합니다

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

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 통합 ID 소스로 Active Directory를 사용하고 ID 공급자로 AD FS를 사용하고 있습니다.

["Single Sign-On 사용에 대한 요구 사항"](#)

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.

- 각 테넌트 계정의 테넌트 관리자에 로그인합니다.
  - 액세스 제어 \* > \* ID 페더레이션 \* 을 선택합니다.
  - ID 페더레이션 사용 \* 확인란이 선택되지 않았는지 확인합니다.
  - 이 경우 이 테넌트 계정에 사용 중인 모든 통합 그룹이 더 이상 필요하지 않은지 확인하고 확인란의 선택을 취소하고 \* Save \* 를 클릭합니다.
2. 통합 사용자가 Grid Manager에 액세스할 수 있는지 확인합니다.
- Grid Manager에서 \* 구성 \* > \* 액세스 제어 \* > \* 관리 그룹 \* 을 선택합니다.
  - Active Directory ID 소스에서 하나 이상의 통합 그룹을 가져오고 루트 액세스 권한이 할당되었는지 확인합니다.
  - 로그아웃합니다.
  - 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.
- Grid Manager에서 \* Tenants \* 를 선택합니다.
  - 테넌트 계정을 선택하고 \* 계정 편집 \* 을 클릭합니다.
  - [고유 ID 소스 사용] \* 확인란을 선택한 경우 상자의 선택을 취소하고 [저장]을 클릭합니다.

## Edit Tenant Account

### Tenant Details

Display Name

Uses Own Identity Source

Allow Platform Services

Storage Quota (optional)

Cancel

Save

테넌트 계정 페이지가 나타납니다.

- 테넌트 계정을 선택하고 \* 로그인 \* 을 클릭한 다음 테넌트 계정에 로컬 루트 사용자로 로그인합니다.
- 테넌트 관리자에서 \* 액세스 제어 \* > \* 그룹 \* 을 클릭합니다.
- Grid Manager에서 하나 이상의 통합 그룹에 이 테넌트에 대한 루트 액세스 권한이 할당되었는지 확인합니다.
- 로그아웃합니다.
- 통합 그룹의 사용자로 테넌트에 다시 로그인할 수 있는지 확인합니다.

관련 정보

["Single Sign-On 사용에 대한 요구 사항"](#)

["관리 그룹 관리"](#)

["테넌트 계정을 사용합니다"](#)

**sandbox** 모드 사용

StorageGRID 사용자에게 대해 SSO(Single Sign-On)를 적용하기 전에 샌드박스 모드를 사용하여 AD FS(Active Directory Federation Services) 기반 당사자 트러스트를 구성 및 테스트할 수 있습니다. SSO를 사용하도록 설정한 후 샌드박스 모드를 다시 활성화하여 새로운 신뢰할 수 있는 기존 및 기존의 트러스트를 구성하거나 테스트할 수 있습니다. sandbox 모드를 다시 활성화하면 StorageGRID 사용자에게 대해 SSO가 일시적으로 비활성화됩니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

SSO가 활성화되어 있고 사용자가 관리자 노드에 로그인을 시도하면 StorageGRID는 AD FS에 인증 요청을 보냅니다. 그런 다음 AD FS는 인증 요청을 성공했는지 여부를 나타내는 인증 응답을 StorageGRID로 다시 보냅니다. 요청에 성공하려면 사용자의 UUID(Universally Unique Identifier)가 응답에 포함됩니다.

StorageGRID(서비스 공급자) 및 AD FS(ID 공급자)가 사용자 인증 요청에 대해 안전하게 통신할 수 있도록 하려면 StorageGRID에서 특정 설정을 구성해야 합니다. 그런 다음 AD FS를 사용하여 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 만들어야 합니다. 마지막으로 StorageGRID로 돌아가서 SSO를 활성화해야 합니다.

sandbox 모드를 사용하면 SSO를 활성화하기 전에 이 전면과 후면을 간편하게 구성하고 모든 설정을 테스트할 수 있습니다.



sandbox 모드를 사용하는 것이 좋지만 반드시 필요한 것은 아닙니다. StorageGRID에서 SSO를 구성한 직후 AD FS 기반 당사자 트러스트를 생성할 준비가 되었으면 또한 각 관리 노드에 대해 SSO 및 단일 로그아웃(SLO) 프로세스를 테스트할 필요가 없습니다. \* Enabled \* 를 클릭하고 StorageGRID 설정을 입력한 다음 AD FS의 각 관리 노드에 대한 신뢰할 수 있는 파티 트러스트 를 생성한 다음 \* Save \* 를 클릭하여 SSO를 활성화합니다.

단계

1. Configuration \* \* \* Access Control \* \* Single Sign-On \* 을 선택합니다.

단일 사인온 페이지가 나타나고 \* 비활성화 \* 옵션이 선택됩니다.

#### Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status  Disabled  Sandbox Mode  Enabled

Save



SSO 상태 옵션이 나타나지 않으면 Active Directory를 통합 ID 소스로 구성했는지 확인합니다. Single Sign-On 사용 요건 참조

2. Sandbox 모드 \* 옵션을 선택합니다.

ID 공급자 및 공급자 설정이 나타납니다. ID 공급자 섹션에서 \* 서비스 유형 \* 필드는 읽기 전용입니다. 사용 중인 ID 페더레이션 서비스 유형(예: Active Directory)이 표시됩니다.

3. ID 공급자 섹션에서 다음을 수행합니다.

- a. AD FS에 표시되는 대로 페더레이션 서비스 이름을 입력합니다.



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

- b. ID 공급자가 StorageGRID 요청에 대한 응답으로 SSO 구성 정보를 보낼 때 TLS(전송 계층 보안)를 사용하여 연결을 보호할지 여부를 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 인증서를 복사하여 \* CA 인증서 \* 텍스트 상자에 붙여 넣습니다.

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

4. 신뢰할 수 있는 당사자 섹션에서 신뢰할 수 있는 상대 트러스트를 구성할 때 StorageGRID 관리 노드에 사용할 신뢰할 수 있는 당사자 식별자를 지정합니다.

- 예를 들어 그리드에 관리 노드가 하나뿐이고 나중에 관리 노드를 더 추가할 예정이 없는 경우 를 입력합니다 sg 또는 StorageGRID.
- 그리드에 둘 이상의 관리 노드가 포함된 경우 문자열을 포함합니다 [HOSTNAME] 를 입력합니다. 예를 들면, 다음과 같습니다. SG-[HOSTNAME]. 이렇게 하면 노드의 호스트 이름을 기반으로 각 관리 노드에 대한 기반 당사자 식별자가 포함된 테이블이 생성됩니다. +참고: 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.

5. 저장 \* 을 클릭합니다.

- 몇 초 동안 \* Save \* (저장 \*) 버튼에 녹색 확인 표시가 나타납니다.



- Sandbox 모드 확인 알림이 나타나고 Sandbox 모드가 이제 활성화되었음을 확인합니다. AD FS를 사용하는 동안 이 모드를 사용하여 각 관리 노드에 대한 의존적인 당사자 신뢰를 구성하고 SSO(Single Sign-In) 및 SLO(Single Logout) 프로세스를 테스트할 수 있습니다.

### Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status    Disabled    Sandbox Mode    Enabled

#### Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

관련 정보

"Single Sign-On 사용에 대한 요구 사항"

AD FS에서 기반 당사자 신뢰를 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.

## Windows PowerShell을 사용하여 신뢰할 수 있는 사용자 신뢰 생성

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

### 필요한 것

- StorageGRID에서 SSO를 구성했으며 시스템의 각 관리 노드에 대한 정규화된 도메인 이름(또는 IP 주소)과 관련 당사자 식별자를 알고 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.

### 이 작업에 대해

이러한 지침은 Windows Server 2016에 포함된 AD FS 4.0에 적용됩니다. Windows 2012 R2에 포함된 AD FS 3.0을 사용하는 경우 절차에 약간의 차이가 있습니다. 질문이 있는 경우 Microsoft AD FS 설명서를 참조하십시오.

### 단계

- Windows 시작 메뉴에서 PowerShell 아이콘을 마우스 오른쪽 단추로 클릭하고 \* 관리자 권한으로 실행 \* 을 선택합니다.
- PowerShell 명령 프롬프트에서 다음 명령을 입력합니다.

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

- 용 `Admin_Node_Identifier``에서 관리 노드에 대한 기반 당사자 식별자를 단일 사인온 페이지에 표시된 대로 정확하게 입력합니다. 예를 들면, 다음과 같습니다. ``SG-DC1-ADM1.`
- 용 ``Admin_Node_FQDN``에서 동일한 관리 노드에 대해 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)

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

AD FS 관리 도구가 나타납니다.

- AD FS \* > \* 기반 당사자 신뢰 \* 를 선택합니다.

신뢰할 수 있는 당사자 목록이 나타납니다.

- 새로 만든 신뢰할 수 있는 상대 신뢰에 액세스 제어 정책 추가:

- 방금 만든 신뢰할 수 있는 상대자를 찾습니다.
- 트러스트를 마우스 오른쪽 단추로 클릭하고 \* 액세스 제어 정책 편집 \* 을 선택합니다.

- c. 액세스 제어 정책을 선택합니다.
  - d. 적용 \* 을 클릭하고 \* 확인 \* 을 클릭합니다
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 클릭합니다.
  - d. 규칙 템플릿 선택 페이지의 목록에서 \* 청구로 LDAP 속성 보내기 \* 를 선택하고 \* 다음 \* 을 클릭합니다.
  - e. 규칙 구성 페이지에서 이 규칙의 표시 이름을 입력합니다.

예를 들어, 이름 ID\*에 대한 \* objectGUID.

- f. 특성 저장소의 경우 \* Active Directory \* 를 선택합니다.
  - g. 매핑 테이블의 LDAP 속성 열에 \* objectGUID \* 를 입력합니다.
  - h. 매핑 테이블의 발신 클레임 유형 열에서 드롭다운 목록에서 \* 이름 ID \* 를 선택합니다.
  - i. 마침 \* 을 클릭하고 \* 확인 \* 을 클릭합니다.
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 및 로 돌아갑니다 "모든 신뢰할 수 있는 당사자 테스트" 올바르게 구성되었는지 확인합니다.

### 페더레이션 메타데이터를 가져와 사용 가능한 상대 신뢰 만들기

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

#### 필요한 것

- StorageGRID에서 SSO를 구성했으며 시스템의 각 관리 노드에 대한 정규화된 도메인 이름(또는 IP 주소)과 관련 당사자 식별자를 알고 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.

#### 이 작업에 대해

이러한 지침은 Windows Server 2016에 포함된 AD FS 4.0에 적용됩니다. Windows 2012 R2에 포함된 AD FS 3.0을 사용하는 경우 절차에 약간의 차이가 있습니다. 질문이 있는 경우 Microsoft AD FS 설명서를 참조하십시오.

## 단계

1. Windows Server Manager에서 \* Tools \* 를 클릭한 다음 \* AD FS Management \* 를 선택합니다.
2. 작업에서 \* 신뢰할 수 있는 당사자 신뢰 추가 \* 를 클릭합니다.
3. 시작 페이지에서 \* 클레임 인식 \* 을 선택하고 \* 시작 \* 을 클릭합니다.
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`

용 `Admin\_Node\_FQDN`에서 동일한 관리 노드에 대해 정규화된 도메인 이름을 입력합니다. (필요한 경우 노드의 IP 주소를 대신 사용할 수 있습니다. 그러나 여기에 IP 주소를 입력한 경우에는 해당 IP 주소가 변경될 경우 이 신뢰할 수 있는 사용자 신뢰를 업데이트하거나 다시 만들어야 합니다.)

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



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

## 7. 청구 규칙 추가:

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

예를 들어, 이름 ID\*에 대한 \* objectGUID.

- e. 특성 저장소의 경우 \* Active Directory \* 를 선택합니다.
- f. 매핑 테이블의 LDAP 속성 열에 \* objectGUID \* 를 입력합니다.
- g. 매핑 테이블의 발신 클레임 유형 열에서 드롭다운 목록에서 \* 이름 ID \* 를 선택합니다.
- h. 마침 \* 을 클릭하고 \* 확인 \* 을 클릭합니다.

## 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 및 로 돌아갑니다 "모든 신뢰할 수 있는 당사자 테스트" 올바르게 구성되었는지 확인합니다.

수동으로 신뢰할 수 있는 상대 만들기

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

필요한 것

- StorageGRID에서 SSO를 구성했으며 시스템의 각 관리 노드에 대한 정규화된 도메인 이름(또는 IP 주소)과 관련 당사자 식별자를 알고 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.

- StorageGRID 관리 인터페이스를 위해 업로드된 사용자 지정 인증서가 있거나 명령 셸에서 관리자 노드에 로그인하는 방법을 알고 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.

이 작업에 대해

이러한 지침은 Windows Server 2016에 포함된 AD FS 4.0에 적용됩니다. Windows 2012 R2에 포함된 AD FS 3.0을 사용하는 경우 절차에 약간의 차이가 있습니다. 질문이 있는 경우 Microsoft AD FS 설명서를 참조하십시오.

단계

1. Windows Server Manager에서 \* Tools \* 를 클릭한 다음 \* AD FS Management \* 를 선택합니다.
2. 작업에서 \* 신뢰할 수 있는 당사자 신뢰 추가 \* 를 클릭합니다.
3. 시작 페이지에서 \* 클레임 인식 \* 을 선택하고 \* 시작 \* 을 클릭합니다.
4. [의지하는 사용자에 대한 데이터 입력]을 선택하고 \* [다음]을 클릭합니다.
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. 예를 들면, 다음과 같습니다. SG-DC1-ADM1.

- b. 선택적 토큰 암호화 인증서를 구성하려면 단계를 건너뛵니다.
- 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
```

용 `Admin\_Node\_FQDN`에서 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
```

용 `Admin Node Identifier`에서 관리 노드에 대한 기반 당사자 식별자를 단일 사인온 페이지에 표시된 대로 정확하게 입력합니다. 예를 들면, 다음과 같습니다. `SG-DC1-ADM1`.

- 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 클릭합니다.

- a. 규칙 템플릿 선택 페이지의 목록에서 \*청구로 LDAP 속성 보내기\* 를 선택하고 \*다음\* 을 클릭합니다.
- b. 규칙 구성 페이지에서 이 규칙의 표시 이름을 입력합니다.

예를 들어, 이름 ID\*에 대한 \*objectGUID

- c. 특성 저장소의 경우 \*Active Directory\* 를 선택합니다.
- d. 매핑 테이블의 LDAP 속성 열에 \*objectGUID\* 를 입력합니다.
- e. 매핑 테이블의 발신 클레임 유형 열에서 드롭다운 목록에서 \*이름 ID\* 를 선택합니다.
- f. 마침\* 을 클릭하고 \*확인\* 을 클릭합니다.

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 클릭합니다.
- 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`

용 `Admin_Node_FQDN`에서 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. 확인\* 을 클릭합니다.

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 관리 노드에 로그인하고 로 이동합니다 `/var/local/mgmt-api` Admin Node의 디렉토리로 이동한 후 를 추가합니다 `custom-server.crt` 인증서 파일.
  - 참고: \* 관리자 노드의 기본 인증서 사용 (`server.crt`)는 권장되지 않습니다. 관리자 노드에 장애가 발생하면 노드를 복구할 때 기본 인증서가 다시 생성되고, 신뢰할 수 있는 상대 트러스트를 업데이트해야 합니다.

b. 적용 \* 을 클릭하고 \* 확인 \* 을 클릭합니다.

종속된 당사자 속성이 저장되고 닫힙니다.

10. 이 단계를 반복하여 StorageGRID 시스템의 모든 관리 노드에 대한 신뢰할 수 있는 상대 트러스트를 구성합니다.
11. 완료되면 StorageGRID 및 로 돌아갑니다 "모든 신뢰할 수 있는 당사자 테스트" 올바르게 구성되었는지 확인합니다.

신뢰할 수 있는 당사자 신뢰 테스트

StorageGRID에 SSO(Single Sign-On)를 사용하도록 강제하기 전에 SSO(Single Sign-On)와 SLO(Single Logout)가 올바르게 구성되었는지 확인합니다. 각 관리 노드에 대해 종속된 당사자 신뢰를 생성한 경우 각 관리 노드에 대해 SSO 및 SLO를 사용할 수 있는지 확인합니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- AD FS에서 하나 이상의 기반 당사자 트러스트를 구성했습니다.

단계

1. Configuration \* \* \* Access Control \* \* Single Sign-On \* 을 선택합니다.

단일 사인온 페이지가 나타나고 \* Sandbox 모드 \* 옵션이 선택됩니다.

2. sandbox 모드에 대한 지침에서 ID 공급자의 로그인 페이지에 대한 링크를 찾습니다.

URL은 \* Federated Service Name \* 필드에 입력한 값에서 파생됩니다.

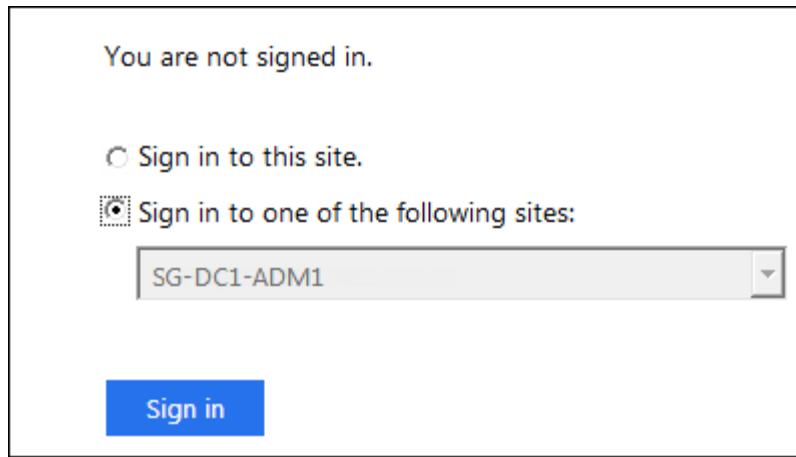
### Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

3. ID 공급자의 로그인 페이지에 액세스하려면 링크를 클릭하거나 URL을 복사하여 브라우저에 붙여 넣으십시오.
4. 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 클릭합니다.



사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.

5. 통합 사용자 이름과 암호를 입력합니다.

- SSO 로그인 및 로그아웃 작업이 성공하면 성공 메시지가 나타납니다.

✔ Single sign-on authentication and logout test completed successfully.

- SSO 작업이 실패하면 오류 메시지가 나타납니다. 문제를 해결하고 브라우저의 쿠키를 삭제한 후 다시 시도하십시오.

6. 이전 단계를 반복하여 다른 관리 노드에 로그인할 수 있는지 확인합니다.

모든 SSO 로그인 및 로그아웃 작업이 성공하면 SSO를 활성화할 수 있습니다.

### SSO(Single Sign-On) 활성화

sandbox 모드를 사용하여 모든 StorageGRID 기반 당사자 트러스트를 테스트한 후에는 SSO(Single Sign-On)를 사용할 수 있습니다.

#### 필요한 것

- ID 소스에서 하나 이상의 통합 그룹을 가져오고 그룹에 할당된 루트 액세스 관리 권한을 가져와야 합니다. 하나 이상의 통합 사용자가 그리드 관리자 및 기존 테넌트 계정에 대한 테넌트 관리자에 대한 루트 액세스 권한을 가지고 있는지 확인해야 합니다.
- 샌드박스 모드를 사용하여 모든 신뢰할 수 있는 파티 트러스트를 수행해야 합니다.

#### 단계

1. Configuration \* \* \* Access Control \* \* Single Sign-On \* 을 선택합니다.

단일 사인온 페이지가 \* Sandbox 모드 \* 가 선택된 상태로 나타납니다.

2. SSO 상태를 \* Enabled \* 로 변경합니다.

3. 저장 \* 을 클릭합니다.

경고 메시지가 나타납니다.

## ⚠ Warning

### Enable single sign-on

After you enable SSO, no local users—including the root user—will be able to sign in to the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API.

Before proceeding, confirm the following:

- You have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts.
- You have tested all relying party trusts using sandbox mode.

Are you sure you want to enable single sign-on?

Cancel

OK

4. 경고를 검토하고 \* OK \* 를 클릭합니다.

이제 SSO(Single Sign-On)가 활성화됩니다.



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.

### SSO(Single Sign-On) 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.

#### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

#### 단계

1. Configuration \* \* \* Access Control \* \* Single Sign-On \* 을 선택합니다.

단일 사인온 페이지가 나타납니다.

2. 사용 안 함 \* 옵션을 선택합니다.

3. 저장 \* 을 클릭합니다.

로컬 사용자가 로그인할 수 있음을 나타내는 경고 메시지가 나타납니다.



## ⚠ Warning

### Disable single sign-on

After you disable SSO or switch to sandbox mode, local users will be able to sign in. Are you sure you want to proceed?

Cancel

OK

#### 4. 확인 \* 을 클릭합니다.

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

하나의 관리 노드에 대해 **SSO(Single Sign-On)**를 일시적으로 비활성화 및 다시 활성화합니다

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

#### 필요한 것

- 특정 액세스 권한이 있어야 합니다.
- 에 가 있어야 합니다 Passwords.txt 파일.
- 로컬 루트 사용자의 암호를 알아야 합니다.

#### 이 작업에 대해

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



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

#### 단계

##### 1. 관리자 노드에 로그인:

- 다음 명령을 입력합니다. `ssh admin@Admin_Node_IP`
- 에 나열된 암호를 입력합니다 Passwords.txt 파일.
- 루트로 전환하려면 다음 명령을 입력합니다. `su -`
- 에 나열된 암호를 입력합니다 Passwords.txt 파일.

루트로 로그인하면 프롬프트가 `에`서 변경됩니다 `$` 를 선택합니다 `#`.

##### 2. 다음 명령을 실행합니다.disable-saml

명령이 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

3. SSO를 비활성화할지 확인합니다.

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

4. 웹 브라우저에서 동일한 관리 노드의 그리드 관리자에 액세스합니다.

이제 SSO가 비활성화되어 Grid Manager 로그인 페이지가 표시됩니다.

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

6. SSO 구성을 수정해야 하므로 SSO를 일시적으로 비활성화한 경우:

- a. Configuration \* \* \* Access Control \* \* Single Sign-On \* 을 선택합니다.
- b. 잘못된 또는 오래된 SSO 설정을 변경합니다.
- c. 저장 \* 을 클릭합니다.

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

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

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

- 다음 명령을 실행합니다. `enable-saml`

명령이 이 관리 노드에만 적용된다는 메시지가 표시됩니다.

SSO를 활성화할지 확인합니다.

노드에서 Single Sign-On이 설정되었음을 나타내는 메시지가 표시됩니다.

- 그리드 노드를 재부팅합니다. `reboot`

8. 웹 브라우저에서 동일한 관리 노드에서 그리드 관리자에 액세스합니다.

9. StorageGRID 로그인 페이지가 나타나고 그리드 관리자에 액세스하려면 SSO 자격 증명을 입력해야 합니다.

관련 정보

["Single Sign-On 구성"](#)

## 관리자 클라이언트 인증서를 구성하는 중입니다

클라이언트 인증서를 사용하여 권한이 있는 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있도록 허용할 수 있습니다. 클라이언트 인증서는 외부 도구를 사용하여 StorageGRID를 모니터링하는 안전한 방법을 제공합니다.

외부 모니터링 도구를 사용하여 StorageGRID에 액세스해야 하는 경우 그리드 관리자를 사용하여 클라이언트 인증서를 업로드하거나 생성하고 인증서 정보를 외부 도구에 복사해야 합니다.

관리자 클라이언트 인증서를 추가하는 중입니다

클라이언트 인증서를 추가하려면 고유한 인증서를 제공하거나 Grid Manager를 사용하여 인증서를 생성할 수 있습니다.

필요한 것

- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 관리 노드의 IP 주소 또는 도메인 이름을 알아야 합니다.
- StorageGRID 관리 인터페이스 서버 인증서를 구성하고 해당 CA 번들을 가지고 있어야 합니다
- 인증서를 업로드하려면 인증서의 공개 키와 개인 키를 로컬 컴퓨터에서 사용할 수 있어야 합니다.

단계

1. 그리드 관리자에서 \* 구성 \* > \* 액세스 제어 \* > \* 클라이언트 인증서 \* 를 선택합니다.

클라이언트 인증서 페이지가 나타납니다.

#### Client Certificates

You can upload or generate one or more client certificates to allow StorageGRID to authenticate external client access.

+ Add   ✎ Edit   ✕ Remove		
Name	Allow Prometheus	Expiration Date
No client certificates configured.		

2. 추가 \* 를 선택합니다.

인증서 업로드 페이지가 나타납니다.

#### Upload Certificate

Name

Allow Prometheus

---

#### Certificate Details

Upload the public key for the client certificate.

3. 인증서의 이름을 1자에서 32자 사이로 입력합니다.
4. 외부 모니터링 도구를 사용하여 Prometheus 메트릭에 액세스하려면 \* Prometheus \* 허용 확인란을 선택합니다.
5. 인증서 업로드 또는 생성:
  - a. 인증서를 업로드하려면 [으로 이동합니다](#) [여기](#).
  - b. 인증서를 생성하려면 [으로 이동합니다](#) [여기](#).
6. 인증서를 업로드하려면

a. 클라이언트 인증서 업로드 \* 를 선택합니다.

b. 인증서의 공개 키를 찾습니다.

인증서의 공개 키를 업로드하면 \* 인증서 메타데이터 \* 및 \* 인증서 PEM \* 필드가 채워집니다.

### Upload Certificate

Name

Allow Prometheus

#### Certificate Details

Upload the public key for the client certificate.

Uploaded file name: client (1).crt

Certificate metadata

```
Subject DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Serial Number: 0D:0E:FC:16:75:B8:BE:3E:7D:47:4D:05:49:08:F3:7B:E8:4A:71:90
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Issued On: 2020-06-19T22:11:56.000Z
Expires On: 2021-06-19T22:11:56.000Z
SHA-1 Fingerprint: 13:AA:D6:06:2B:90:FE:B7:7B:EB:1A:83:BE:C3:62:39:B7:A6:E7:F0
SHA-256 Fingerprint: 5C:29:06:6B:CF:81:50:B8:4F:A9:56:F7:A7:AB:3C:36:FA:3D:B7:32:A4:C9:74:85:2C:8D:E6:67:37:C3:AC:60
```

Certificate PEM

```
-----BEGIN CERTIFICATE-----
MIIDmzCCRoOgAwIBAgIUUDQ78FnW4vj59R00FSQjze+hKcZAwDQYJKoZIhvcNAQEL
BQAwDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbgG1mb3JuaWEuEjAQBgNVBAcM
CVN1bm55dmFsZTEUMBIGA1UECgwLRXhhbXBsZSBDbj4xZzA5BGNVBAeMAk1UMRkw
FwYDVQDDBAQLnMzLmV4YW1wbGUuY29tMjYyOTIwMDYxOTIyMTE1N1oXDTIxMDYx
OTIyMTE1N1owDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbgG1mb3JuaWEuEjAQB
BgNVBAcMCVN1bm55dmFsZTEUMBIGA1UECgwLRXhhbXBsZSBDbj4xZzA5BGNVBAeM
Ak1UMRkwFwYDVQDDBAQLnMzLmV4YW1wbGUuY29tMjYyOTIwMDYxOTIyMTE1N1oXDT
AAOCAQ8AMIIBCgKCAQEA5Vqq2MNjvVotLeGtq1Co4coJmsQ2ygRhuwSza0bgMnjf
cwUgHNVFXGuG1zY/TL37r3Dk5bu2fyGyAeJ6mqbQA6cE3ypOp5Hx7Cm/AWJknFw6
-----END CERTIFICATE-----
```

a. 클립보드로 인증서 복사 \* 를 선택하고 외부 모니터링 도구에 인증서를 붙여 넣습니다.

b. 편집 도구를 사용하여 개인 키를 복사하여 외부 모니터링 도구에 붙여 넣습니다.

c. 인증서를 Grid Manager에 저장하려면 \* 저장 \* 을 선택합니다.

7. 인증서를 생성하려면:

a. 클라이언트 인증서 생성 \* 을 선택합니다.

b. 관리자 노드의 도메인 이름 또는 IP 주소를 입력합니다.

c. 선택적으로 DN(고유 이름)이라고도 하는 X.509 제목을 입력하여 인증서를 소유한 관리자를 식별합니다.

d. 원하는 경우 인증서가 유효한 일 수를 선택합니다. 기본값은 730일입니다.

e. Generate \* 를 선택합니다.

인증서 메타데이터 \*, \* 인증서 PEM \* 및 \* 인증서 개인 키 \* 필드가 채워집니다.

## Upload Certificate

Name

Allow Prometheus

### Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Certificate metadata

```
Subject DN: /CN=test.com
Serial Number: 08:F8:FB:76:B2:13:E4:DF:54:83:3D:35:56:0F:2A:03:53:B0:E2:0
A
Issuer DN: /CN=test.com
Issued On: 2020-11-20T22:44:46.000Z
Expires On: 2022-11-20T22:44:46.000Z
SHA-1 Fingerprint: 6E:DB:8C:F8:3E:20:88:E4:C6:42:52:5F:32:7E:E7:93:66:89:F3:3
D
SHA-256 Fingerprint: 73:D3:51:83:ED:D3:89:AD:7B:89:4C:AF:AE:34:76:B6:42:FE:0D:
EF:78:C0:A4:66:C2:EB:65:64:C3:D4:7A:B0
```

Certificate PEM

```
-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUUCFj7dxITSN9Ugs01Vm8qA1Ow4gowDQYJKoZIhvcNAQEL
BQAwEwERMA8GA1UEAwIgdGVudC5jb20wHhcNMjIwMjI0MjI0NDQ2WzBcMjIwMjI0
MjI0NDQ2WzATMREwDwYDVQQDDAh0ZXN0LmNvbTCCASAwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAR02dS9mx2jFrGuBb22Mjcidf/tCkKtL8Gm+4vIwt1gvrR
XgHZ31B9YIQn/Vo729R2mNKKyBwkyQTkGCO2Ixvv0STBLEIWFb8S+TgcIeMyt1V1F
OseBWy402xxjnR3/X+AX+6s2WZIsVe+3CDjGu4ie0V/uVQxx4yA1T9SoKnjBmOa
LCVjL6iVnkUGB8GbkYUPeOaoMjsL6TN1QsoFv9VEB0xBKCP4D7FDbaIy2f9Ng8rS
FEOQoLN=N+XCasLO4D7j2qFqOVUpFJ3M0oh1x0n5pQ78Z5KEYwV=DKg6v52P8UBM
1o6GeuoFaW+dbpLZKp09N1V=PhghXe9AxxN8s+kCAwEAAaMXMBUwEwYDVR0RBAAw

```


Copy certificate to clipboard

Certificate private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEArT20H2bHaM+sa4Fv2kyNyJ1/+1NwzEu0Eab7i8jC2KWC/BFe
AdneUH1ghCf9Wjvb1HaY0orIHCTJBOQYI5kjG+/RjMEb4h29eKxOBwiczK2VWUU7
OwF2jPg7bPGoOrf9f4Bf7n1ZkixV75IICMa7iJaRX+5VDPHjIDVP1KggelMGYSos
JWmVqJWeRQYFI2uTJQ946qgyOwvpm2VDOgW/1UQHTEEoKngFpUNtojLZ/02DmtJ8
QSCgs202x0JxMe7gFuNmoWe5hSkUncw6iHXHSfm1Dvxnkp9jBw0MqDm/nY/xQEeW
jw266h9pb51ukt2k703VW0WGCfD7GDPE2yyQQIDAQABoIBAQCfEUfY4pE0Hqtv
2uEL6De4yXMTwg/3Gn+W3mvtgdgQB4xWEGQrk1kEUG+HTYrFJen6XX0vACDYAC/
Hh1Q67xDPVpRjdpuK0ctr1W3ervzEmpBx99MqH9Y2UGx6Yub3UBJaqfDvja4Nvaon
MxaYJRFBLvAR7f2z2xXVY3b0zRPA+rn0YCrz1Ler5Y0K79e0G8naTmwIdm2YM6EE

```

Copy private key to clipboard

 You will not be able to view the certificate private key after you close this dialog. To save the keys for future reference, copy and paste the values to another location.

Cancel

Save

a. 클립보드로 인증서 복사 \* 를 선택하고 외부 모니터링 도구에 인증서를 붙여 넣습니다.

b. Copy private key to clipboard \* 를 선택하고 키를 외부 모니터링 도구에 붙여 넣습니다.



대화 상자를 닫은 후에는 개인 키를 볼 수 없습니다. 키를 안전한 위치에 복사합니다.

c. 인증서를 Grid Manager에 저장하려면 \* 저장 \* 을 선택합니다.

8. Grafana와 같은 외부 모니터링 도구에서 다음 설정을 구성합니다.

Grafana 예제는 다음 스크린샷에 나와 있습니다.

The screenshot shows the Grafana configuration interface for a data source named 'sg-prometheus'. The 'Name' field is 'sg-prometheus' and the 'Default' toggle is turned on. Under the 'HTTP' section, the 'URL' is 'https://admin-node.example.com:9091'. The 'Access' dropdown is set to 'Server (default)'. Under the 'Auth' section, 'Basic auth' is disabled, 'With Credentials' is disabled, 'TLS Client Auth' is enabled, 'With CA Cert' is enabled, 'Skip TLS Verify' is disabled, and 'Forward OAuth Identity' is disabled. Under the 'TLS/SSL Auth Details' section, the 'CA Cert' field is highlighted with a yellow box and contains the text 'Begins with ---BEGIN CERTIFICATE---'. The 'ServerName' field is highlighted with a yellow box and contains 'admin-node.example.com'. The 'Client Cert' field is highlighted with a yellow box and contains the text 'Begins with ---BEGIN CERTIFICATE---'.

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. 관리 인터페이스 서버 인증서 또는 CA 번들을 TLS/SSL 인증 세부 정보 아래의 **CA Cert**에 복사하여 붙여 넣습니다.
- e. \* `ServerName` \*: 관리 노드의 도메인 이름을 입력합니다.

`servername`은 관리 인터페이스 서버 인증서에 표시된 도메인 이름과 일치해야 합니다.

- f. StorageGRID 또는 로컬 파일에서 복사한 인증서 및 개인 키를 저장하고 테스트합니다.

이제 외부 모니터링 툴을 사용하여 StorageGRID에서 Prometheus 메트릭에 액세스할 수 있습니다.

메트릭에 대한 자세한 내용은 StorageGRID 모니터링 및 문제 해결 지침을 참조하십시오.

## 관련 정보

["StorageGRID 보안 인증서 사용"](#)

["Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성"](#)

["모니터링 및 문제 해결"](#)

## 관리자 클라이언트 인증서를 편집하는 중입니다

인증서를 편집하여 이름을 변경하거나, Prometheus 액세스를 활성화 또는 비활성화하거나, 현재 인증서가 만료되면 새 인증서를 업로드할 수 있습니다.

## 필요한 것

- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 관리 노드의 IP 주소 또는 도메인 이름을 알아야 합니다.
- 새 인증서 및 개인 키를 업로드하려면 로컬 컴퓨터에서 사용할 수 있어야 합니다.

## 단계

1. 구성 \* > \* 액세스 제어 \* > \* 클라이언트 인증서 \* 를 선택합니다.

클라이언트 인증서 페이지가 나타납니다. 기존 인증서가 나열됩니다.

인증서 만료 날짜가 표에 나열되어 있습니다. 인증서가 곧 만료되거나 이미 만료된 경우 테이블에 메시지가 나타나고 경고가 트리거됩니다.

	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. 편집할 인증서 왼쪽에 있는 라디오 단추를 선택합니다.

3. 편집 \* 을 선택합니다.

인증서 편집 대화 상자가 나타납니다.

Edit Certificate test-certificate-generate

Name

Allow Prometheus

**Certificate Details**

Upload the public key for the client certificate.

**Certificate metadata**

Subject DN: /CN=test.com  
Serial Number: 0C:11:87:6C:1E:FD:13:16:F3:F2:06:D9:DA:6D:BC:CE:2A:A9:C3:53  
Issuer DN: /CN=test.com  
Issued On: 2020-11-23T15:53:33.000Z  
Expires On: 2022-11-23T15:53:33.000Z  
SHA-1 Fingerprint: AE:E6:70:A7:D3:C3:39:7A:09:F9:62:9B:81:8A:87:CD:43:16:89:A7  
SHA-256 Fingerprint: 63:07:BF:FF:08:1E:84:F1:D4:67:C6:16:B0:35:26:00:C6:A3:13:11:7E:5E:90:EC:7A:7B:EF:23:14:55:3D:56

**Certificate PEM**

```
-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUDBGHbB79Exbz8gbZ2m28ziqpw1MwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwIdGVzdC5jb20wHhcNMjAwMTIzMTU1MzE1MzE1LjEzMTIz
MTU1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1
ggEPADCCAQoCggEBAKdgEeneCDFDsLjvLnX9ow6oPrdU7m2EN6SS6xdVI155sCH+
hkwO5a2Mym7EhbNxfwOt2nMjQkcaKIrk8QAmutRgG6N1N12FIW0gY0uzFQ0QddLq
n7ymFx6w8a9zYSu7bLp84Yn0/LSDPk+h3Jic7Mrt2X70It5ZDRwFmbLNvEvYEtIS
h+FbNh885AIRO2eLxvC0IRijlbySe76wK+Wmc97HdxRSgyxIWk6BD47XC+dOrv55
wvtjc/41qc5xsE6XmJs2yJg4VARz10y8Icwa9fr00+xPwIdCQnwxkpWJKeBnCoKx
YcQxbWz1z+iVLJqLTMxUsrTTI30rUgN00M82GJUcAwEAAaMKMBUwEwYDVR0RBAAw
-----END CERTIFICATE-----
```

4. 원하는 대로 인증서를 변경합니다.

5. 인증서를 Grid Manager에 저장하려면 \* 저장 \* 을 선택합니다.

6. 새 인증서를 업로드한 경우:

- 외부 모니터링 도구에 인증서를 붙여넣으려면 \* 클립보드로 인증서 복사 \* 를 선택합니다.
- 편집 도구를 사용하여 새 개인 키를 복사하여 외부 모니터링 도구에 붙여 넣습니다.
- 외부 모니터링 도구에서 인증서와 개인 키를 저장하고 테스트합니다.

7. 새 인증서를 생성한 경우:

- 외부 모니터링 도구에 인증서를 붙여넣으려면 \* 클립보드로 인증서 복사 \* 를 선택합니다.
- 인증서를 외부 모니터링 도구에 붙여넣으려면 \* 클립보드로 개인 키 복사 \* 를 선택합니다.



대화 상자를 닫은 후에는 개인 키를 보거나 복사할 수 없습니다. 키를 안전한 위치에 복사합니다.



c. 외부 모니터링 도구에서 인증서와 개인 키를 저장하고 테스트합니다.

관리자 클라이언트 인증서를 제거하는 중입니다

인증서가 더 이상 필요하지 않으면 제거할 수 있습니다.

필요한 것

- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

단계

1. 구성 \* > \* 액세스 제어 \* > \* 클라이언트 인증서 \* 를 선택합니다.

클라이언트 인증서 페이지가 나타납니다. 기존 인증서가 나열됩니다.

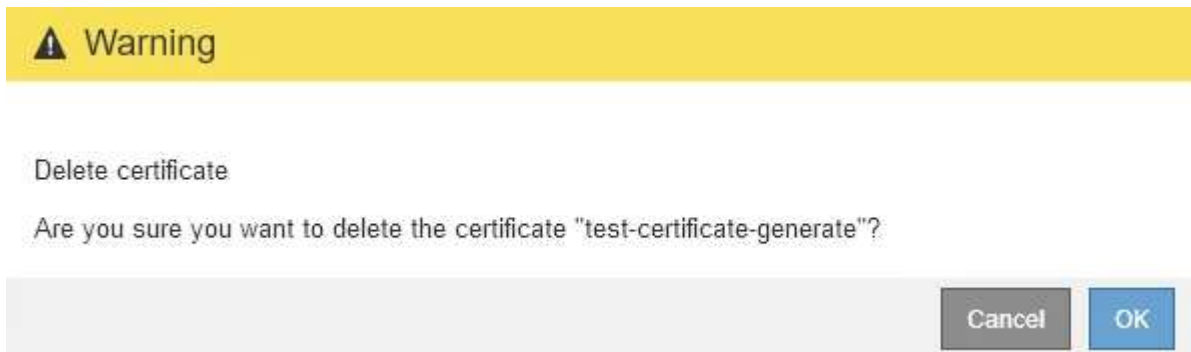
	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. 제거할 인증서 왼쪽에 있는 라디오 단추를 선택합니다.

3. 제거 \* 를 선택합니다.

확인 대화 상자가 나타납니다.



4. OK \* 를 선택합니다.

인증서가 제거됩니다.

## 키 관리 서버 구성

특별히 구성된 어플라이언스 노드의 데이터를 보호하도록 하나 이상의 외부 키 관리 서버 (KMS)를 구성할 수 있습니다.

## KMS(키 관리 서버)란 무엇입니까?

KMS(Key Management Server)는 KMIP(Key Management Interoperability Protocol)를 사용하여 관련 StorageGRID 사이트의 StorageGRID 어플라이언스 노드에 암호화 키를 제공하는 외부 타사 시스템입니다.

하나 이상의 키 관리 서버를 사용하여 설치 중에 \* 노드 암호화 \* 설정이 활성화된 모든 StorageGRID 어플라이언스 노드에 대한 노드 암호화 키를 관리할 수 있습니다. 이러한 어플라이언스 노드에 키 관리 서버를 사용하면 어플라이언스를 데이터 센터에서 제거하더라도 데이터를 보호할 수 있습니다. 어플라이언스 볼륨이 암호화된 후에는 노드에서 KMS와 통신할 수 없는 한 어플라이언스의 데이터에 액세스할 수 없습니다.



StorageGRID는 어플라이언스 노드를 암호화하고 해독하는 데 사용되는 외부 키를 생성하거나 관리하지 않습니다. 외부 키 관리 서버를 사용하여 StorageGRID 데이터를 보호하려는 경우 해당 서버를 설정하는 방법을 이해하고 암호화 키를 관리하는 방법을 이해해야 합니다. 주요 관리 작업을 수행하는 것은 이 지침의 범위를 벗어납니다. 도움이 필요한 경우 키 관리 서버 설명서를 참조하거나 기술 지원 부서에 문의하십시오.

## StorageGRID 암호화 방법 검토

StorageGRID는 데이터 암호화를 위한 다양한 옵션을 제공합니다. 사용 가능한 방법을 검토하여 데이터 보호 요구 사항을 충족하는 방법을 결정해야 합니다.

이 표는 StorageGRID에서 사용할 수 있는 암호화 방법에 대한 상위 수준의 요약を提供합니다.

암호화 옵션	작동 방식	적용 대상
Grid Manager의 키 관리 서버(KMS)	StorageGRID 사이트(* 구성*>* 시스템 설정*>* 키 관리 서버*)에 대한 키 관리 서버를 구성하고 어플라이언스에 대한 노드 암호화를 활성화합니다. 그런 다음 어플라이언스 노드가 KMS에 연결하여 키 암호화 키(KEK)를 요청합니다. 이 키는 각 볼륨의 DEK(데이터 암호화 키)를 암호화하고 해독합니다.	설치 중에 * 노드 암호화 * 가 활성화된 어플라이언스 노드 어플라이언스의 모든 데이터는 물리적 손실이나 데이터 센터에서 제거되는 것을 방지합니다. 일부 StorageGRID 스토리지 및 서비스 어플라이언스와 함께 사용할 수 있습니다.

암호화 옵션	작동 방식	적용 대상
SANtricity 시스템 관리자의 드라이브 보안	스토리지 어플라이언스에 대해 드라이브 보안 기능이 설정된 경우 SANtricity 시스템 관리자를 사용하여 보안 키를 생성하고 관리할 수 있습니다. 보안 드라이브의 데이터에 액세스하려면 키가 필요합니다.	<p>FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브를 사용하는 스토리지 어플라이언스 보안 드라이브의 모든 데이터는 데이터 센터에서 물리적 손실 또는 제거로부터 보호됩니다. 일부 스토리지 어플라이언스 또는 서비스 어플라이언스와 함께 사용할 수 없습니다.</p> <p>"SG6000 스토리지 어플라이언스"</p> <p>"SG5700 스토리지 어플라이언스"</p> <p>"SG5600 스토리지 어플라이언스"</p>
저장 객체 암호화 그리드 옵션	저장된 개체 암호화 * 옵션은 그리드 관리자(* 구성 * > * 시스템 설정 * > * 그리드 옵션 *)에서 활성화할 수 있습니다. 활성화되면 버킷 레벨 또는 오브젝트 레벨에서 암호화되지 않은 새로운 객체는 수집 중에 암호화됩니다.	<p>새로 수집된 S3 및 Swift 오브젝트 데이터. 기존 저장된 오브젝트는 암호화되지 않습니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다.</p> <p>"저장된 오브젝트 암호화 구성"</p>
S3 버킷 암호화	버킷에 대한 암호화를 활성화하기 위해 Put Bucket 암호화 요청을 발급합니다. 오브젝트 레벨에서 암호화되지 않은 새로운 모든 오브젝트는 수집 중에 암호화됩니다.	<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>"S3을 사용합니다"</p>
S3 오브젝트 서버 측 암호화(SSE)	오브젝트를 저장하고 을 포함하기 위한 S3 요청을 실행합니다 x-amz-server-side-encryption 요청 헤더.	<p>새로 수집된 S3 오브젝트 데이터만 해당. 객체에 대해 암호화를 지정해야 합니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다.</p> <p>StorageGRID가 키를 관리합니다.</p> <p>"S3을 사용합니다"</p>

암호화 옵션	작동 방식	적용 대상
고객이 제공한 키(SSE-C)를 사용한 S3 오브젝트 서버 측 암호화	<p>S3 요청을 발급하여 오브젝트를 저장하고 세 개의 요청 헤더를 포함시킵니다.</p> <ul style="list-style-type: none"> <li>• x-amz-server-side-encryption-customer-algorithm</li> <li>• x-amz-server-side-encryption-customer-key</li> <li>• x-amz-server-side-encryption-customer-key-MD5</li> </ul>	<p>새로 수집된 S3 오브젝트 데이터만 해당. 객체에 대해 암호화를 지정해야 합니다. 오브젝트 메타데이터 및 기타 중요한 데이터는 암호화되지 않습니다.</p> <p>키는 StorageGRID 외부에서 관리됩니다.</p> <p>"S3을 사용합니다"</p>
외부 볼륨 또는 데이터 저장소 암호화	<p>구축 플랫폼에서 지원하는 경우 StorageGRID 외부의 암호화 방법을 사용하여 전체 볼륨 또는 데이터 저장소를 암호화합니다.</p>	<p>모든 볼륨 또는 데이터 저장소가 암호화되었다고 가정할 때 모든 오브젝트 데이터, 메타데이터 및 시스템 구성 데이터입니다.</p> <p>외부 암호화 방법을 사용하면 암호화 알고리즘 및 키를 보다 강력하게 제어할 수 있습니다. 나열된 다른 방법과 결합할 수 있습니다.</p>
StorageGRID 외부에서 개체 암호화	<p>StorageGRID 외부에서 암호화 방법을 사용하여 오브젝트 데이터 및 메타데이터를 StorageGRID에 수집하기 전에 암호화합니다.</p>	<p>오브젝트 데이터 및 메타데이터만 (시스템 구성 데이터는 암호화되지 않음).</p> <p>외부 암호화 방법을 사용하면 암호화 알고리즘 및 키를 보다 강력하게 제어할 수 있습니다. 나열된 다른 방법과 결합할 수 있습니다.</p> <p>"Amazon Simple Storage Service - 개발자 가이드: 클라이언트측 암호화를 사용하여 데이터 보호"</p>

## 여러 암호화 방법 사용

요구 사항에 따라 한 번에 두 가지 이상의 암호화 방법을 사용할 수 있습니다. 예를 들면 다음과 같습니다.

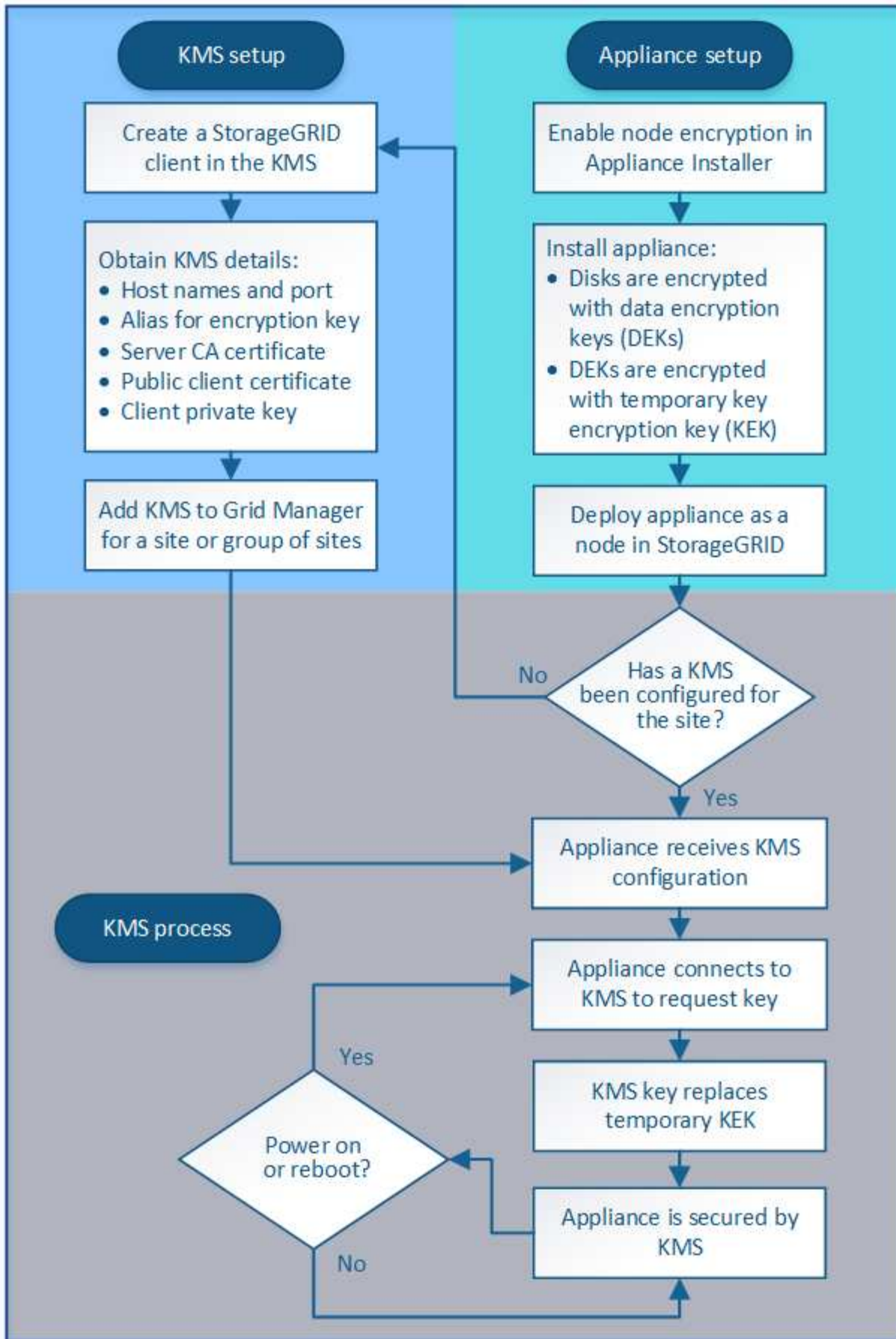
- KMS를 사용하여 어플라이언스 노드를 보호하고 SANtricity 시스템 관리자의 드라이브 보안 기능을 사용하여 동일한 어플라이언스에 있는 자체 암호화 드라이브의 데이터를 "이중 암호화"할 수 있습니다.
- KMS를 사용하여 어플라이언스 노드의 데이터를 보호하고 저장된 개체 암호화 그리드 옵션을 사용하여 모든 개체를 인제스트할 때 암호화할 수 있습니다.

오브젝트의 일부 부분만 암호화해야 하는 경우 대신 버킷 또는 개별 오브젝트 수준에서 암호화를 제어하는 것이 좋습니다. 여러 수준의 암호화를 사용하면 추가 성능 비용이 듭니다.

## **KMS** 및 어플라이언스 구성 개요

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 클라이언트로 StorageGRID 구성"
KMS에서 StorageGRID 클라이언트에 필요한 정보를 얻습니다.	"KMS에서 클라이언트로 StorageGRID 구성"
KMS를 Grid Manager에 추가하고, 단일 사이트 또는 기본 사이트 그룹에 할당하고, 필요한 인증서를 업로드하고, KMS 구성을 저장합니다.	"KMS(키 관리 서버) 추가"

## 제품 설치

KMS 사용을 위해 어플라이언스 노드를 설정하는 단계는 다음과 같습니다.

1. 어플라이언스 설치 시 하드웨어 구성 단계에서 StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스에 대한 \* 노드 암호화 \* 설정을 활성화합니다.



어플라이언스를 그리드에 추가한 후에는 \* 노드 암호화 \* 설정을 활성화할 수 없으며 노드 암호화가 활성화되지 않은 어플라이언스의 경우 외부 키 관리를 사용할 수 없습니다.

2. StorageGRID 어플라이언스 설치 프로그램을 실행합니다. 설치 중에 각 어플라이언스 볼륨에 DEK(임의 데이터 암호화 키)가 다음과 같이 할당됩니다.
  - DEK는 각 볼륨의 데이터를 암호화하는 데 사용됩니다. 이러한 키는 어플라이언스 OS에서 LUKS(Linux Unified Key Setup) 디스크 암호화를 사용하여 생성되며 변경할 수 없습니다.
  - 각 개별 DEK는 마스터 키 암호화 키(KEK)로 암호화됩니다. 초기 KEK는 어플라이언스가 KMS에 연결할 수 있을 때까지 DEK를 암호화하는 임시 키입니다.
3. 어플라이언스 노드를 StorageGRID에 추가합니다.

자세한 내용은 다음을 참조하십시오.

- "SG100 및 AMP, SG1000 서비스 어플라이언스"
- "SG6000 스토리지 어플라이언스"
- "SG5700 스토리지 어플라이언스"
- "SG5600 스토리지 어플라이언스"

## 키 관리 암호화 프로세스(자동으로 발생)

키 관리 암호화에는 자동으로 수행되는 다음과 같은 높은 수준의 단계가 포함됩니다.

1. 노드 암호화가 활성화된 어플라이언스를 그리드에 설치하는 경우 StorageGRID는 새 노드가 포함된 사이트에 대해 KMS 구성이 존재하는지 여부를 결정합니다.
  - KMS가 사이트에 대해 이미 구성된 경우 어플라이언스는 KMS 구성을 받습니다.
  - KMS가 사이트에 대해 아직 구성되지 않은 경우 사이트에 대해 KMS를 구성하고 어플라이언스가 KMS 구성을 받을 때까지 어플라이언스의 데이터는 임시 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.

### KMIP 요구사항은 무엇입니까?

StorageGRID는 KMIP 버전 1.4를 지원합니다.

#### "키 관리 상호 운용성 프로토콜 사양 버전 1.4"

어플라이언스 노드와 구성된 KMS 간의 통신은 보안 TLS 연결을 사용합니다. StorageGRID는 KMIP에 대해 다음 TLS v1.2 암호를 지원합니다.

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

노드 암호화를 사용하는 각 어플라이언스 노드에서 사이트에 대해 구성한 KMS 또는 KMS 클러스터에 대한 네트워크 액세스 권한이 있는지 확인해야 합니다.

네트워크 방화벽 설정을 통해 각 어플라이언스 노드가 KMIP(Key Management Interoperability Protocol) 통신에 사용되는 포트를 통해 통신할 수 있어야 합니다. 기본 KMIP 포트는 5696입니다.

### 어떤 어플라이언스가 지원됩니까?

KMS(키 관리 서버)를 사용하여 \* 노드 암호화 \* 설정이 활성화된 그리드에 있는 StorageGRID 어플라이언스의 암호화 키를 관리할 수 있습니다. 이 설정은 StorageGRID 어플라이언스 설치 프로그램을 사용하여 어플라이언스 설치의 하드웨어 구성 단계에서만 활성화할 수 있습니다.



어플라이언스를 그리드에 추가한 후에는 노드 암호화를 활성화할 수 없으며 노드 암호화가 활성화되지 않은 어플라이언스의 경우 외부 키 관리를 사용할 수 없습니다.

다음 StorageGRID 어플라이언스 및 어플라이언스 노드에 대해 구성된 KMS를 사용할 수 있습니다.



어플라이언스	노드 유형입니다
SG1000 서비스 어플라이언스	관리자 노드 또는 게이트웨이 노드
SG100 서비스 어플라이언스	관리자 노드 또는 게이트웨이 노드
SG6000 스토리지 어플라이언스	스토리지 노드
SG5700 스토리지 어플라이언스	스토리지 노드
SG5600 스토리지 어플라이언스	스토리지 노드

다음은 포함하여 소프트웨어 기반(비어플라이언스) 노드에 대해 구성된 KMS를 사용할 수 없습니다.

- 가상 머신(VM)으로 구축된 노드
- Linux 호스트의 Docker 컨테이너 내에 구축된 노드

이러한 다른 플랫폼에 구축된 노드는 StorageGRID 외부의 데이터 저장소 또는 디스크 레벨에서 암호화를 사용할 수 있습니다.

키 관리 서버는 언제 구성해야 합니까?

새 설치의 경우 일반적으로 테넌트를 생성하기 전에 Grid Manager에서 하나 이상의 키 관리 서버를 설정해야 합니다. 이 순서를 사용하면 오브젝트 데이터가 노드에 저장되기 전에 노드가 보호됩니다.

어플라이언스 노드를 설치하기 전이나 설치한 후에 Grid Manager에서 키 관리 서버를 구성할 수 있습니다.

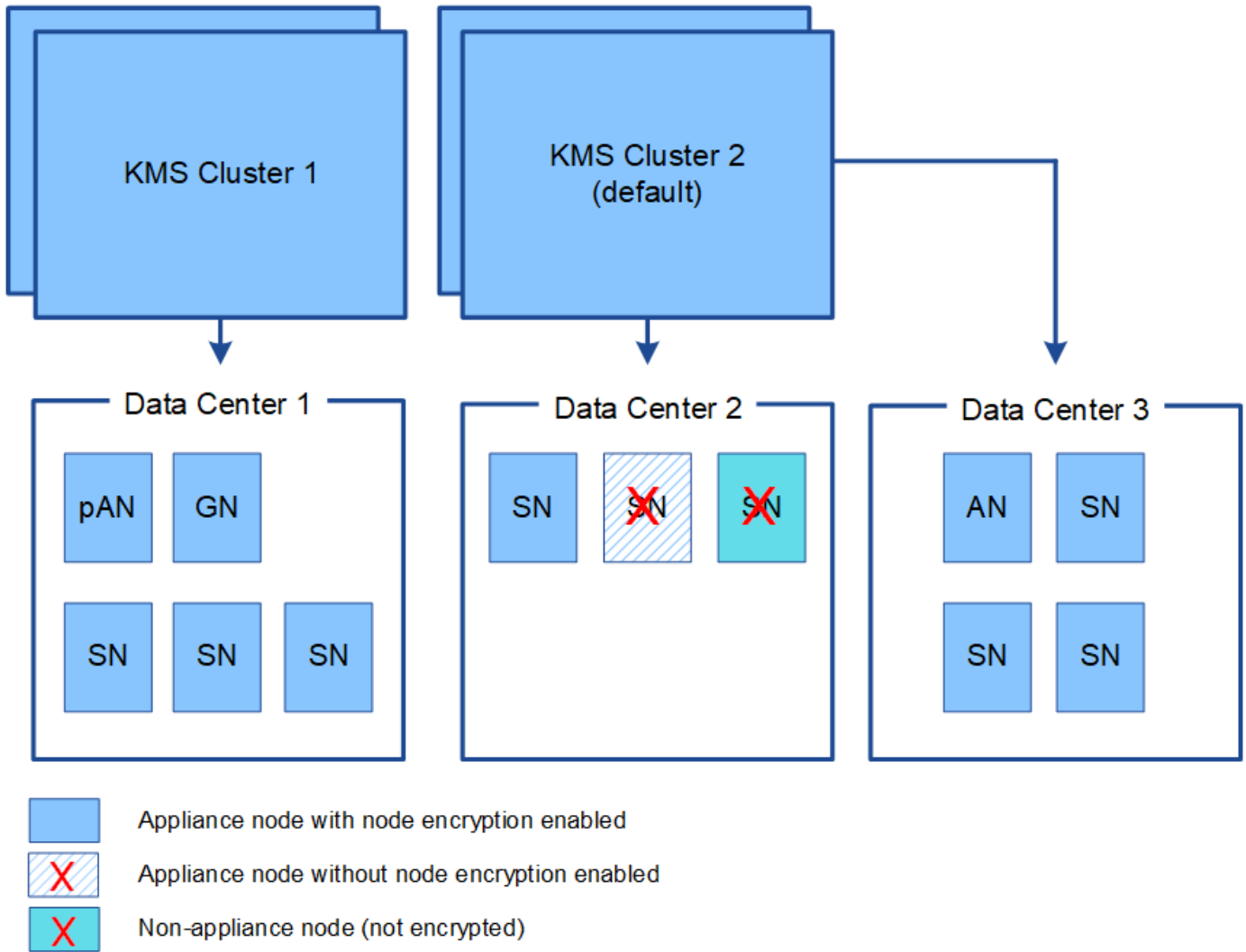
몇 개의 키 관리 서버가 필요합니까?

StorageGRID 시스템의 어플라이언스 노드에 암호화 키를 제공하도록 하나 이상의 외부 키 관리 서버를 구성할 수 있습니다. 각 KMS는 단일 사이트 또는 사이트 그룹의 StorageGRID 어플라이언스 노드에 단일 암호화 키를 제공합니다.

StorageGRID는 KMS 클러스터 사용을 지원합니다. 각 KMS 클러스터에는 구성 설정 및 암호화 키를 공유하는 여러 개의 복제된 키 관리 서버가 포함되어 있습니다. KMS 클러스터를 사용하여 키 관리를 수행하는 것이 좋습니다. KMS 클러스터는 고가용성 구성의 장애 조치 기능을 개선하므로 이 기능을 사용하는 것이 좋습니다.

예를 들어, StorageGRID 시스템에 데이터 센터 사이트가 3개 있다고 가정합니다. 다른 모든 사이트의 모든 어플라이언스 노드에 키를 제공하도록 하나의 KMS 클러스터를 구성하여 Data Center 1의 모든 어플라이언스 노드와 두 번째 KMS 클러스터에 키를 제공할 수 있습니다. 두 번째 KMS 클러스터를 추가하면 데이터 센터 2 및 데이터 센터 3에 대한 기본 KMS를 구성할 수 있습니다.

비어플라이언스 노드나 설치 중에 \* 노드 암호화 \* 설정이 활성화되지 않은 어플라이언스 노드에 대해 KMS를 사용할 수 없습니다.



키를 회전하면 어떻게 됩니까?

보안 모범 사례로서 구성된 각 KMS에서 사용하는 암호화 키를 주기적으로 순환시켜야 합니다.

암호화 키를 회전할 때 KMS 소프트웨어를 사용하여 마지막으로 사용된 키 버전에서 동일한 키의 새 버전으로 회전합니다. 완전히 다른 키로 회전하지 마십시오.



Grid Manager에서 KMS의 키 이름(별칭)을 변경하여 키를 회전하려고 하지 마십시오. 대신 KMS 소프트웨어의 키 버전을 업데이트하여 키를 돌리십시오. 이전 키에 사용된 것과 동일한 키 별칭을 새 키에 사용합니다. 구성된 KMS의 키 별칭을 변경하면 StorageGRID에서 데이터의 암호를 해독하지 못할 수 있습니다.

새 키 버전을 사용할 수 있는 경우:

- KMS와 관련된 사이트 또는 사이트의 암호화된 어플라이언스 노드에 자동으로 배포됩니다. 키는 회전된 후 1시간 내에 분포되어야 합니다.
- 새 키 버전이 배포될 때 암호화된 어플라이언스 노드가 오프라인이면 재부팅되는 즉시 새 키가 노드에 수신됩니다.
- 새 키 버전을 사용하여 어플라이언스 볼륨을 암호화할 수 없는 경우 어플라이언스 노드에 대해 \* KMS 암호화 키 회전 실패 \* 경고가 트리거됩니다. 이 경고를 해결하려면 기술 지원 부서에 문의해야 할 수도 있습니다.

어플라이언스 노드를 암호화한 후 다시 사용할 수 있습니까?

암호화된 어플라이언스를 다른 StorageGRID 시스템에 설치해야 하는 경우 오브젝트 데이터를 다른 노드로 이동하려면 먼저 그리드 노드를 해제해야 합니다. 그런 다음 StorageGRID 어플라이언스 설치 프로그램을 사용하여 KMS 구성을 지울 수 있습니다. KMS 구성을 지우면 \* 노드 암호화 \* 설정이 비활성화되고 StorageGRID 사이트에 대한 어플라이언스 노드와 KMS 구성 간의 연결이 제거됩니다.



KMS 암호화 키에 액세스할 수 없으므로 어플라이언스에 남아 있는 데이터는 더 이상 액세스할 수 없으며 영구적으로 잠깁니다.

"SG100 및 AMP, SG1000 서비스 어플라이언스"

"SG6000 스토리지 어플라이언스"

"SG5700 스토리지 어플라이언스"

"SG5600 스토리지 어플라이언스"

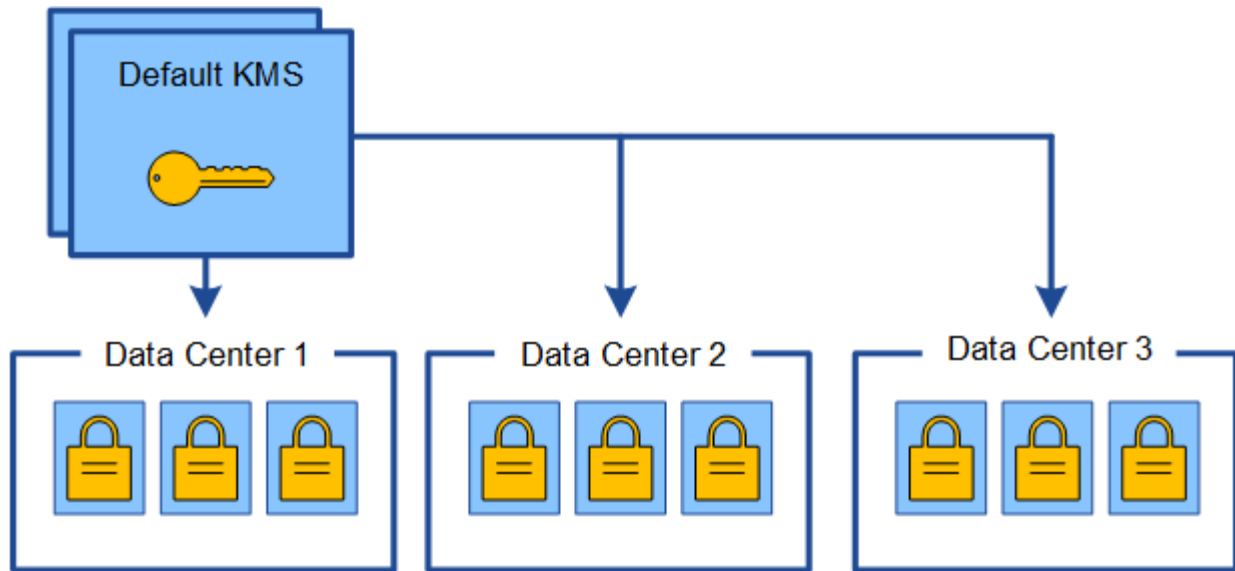
사이트의 **KMS**를 변경할 때의 고려 사항

각 KMS(Key Management Server) 또는 KMS 클러스터는 단일 사이트 또는 사이트 그룹의 모든 어플라이언스 노드에 암호화 키를 제공합니다. 사이트에 사용되는 KMS를 변경해야 하는 경우 암호화 키를 한 KMS에서 다른 KMS로 복사해야 할 수 있습니다.

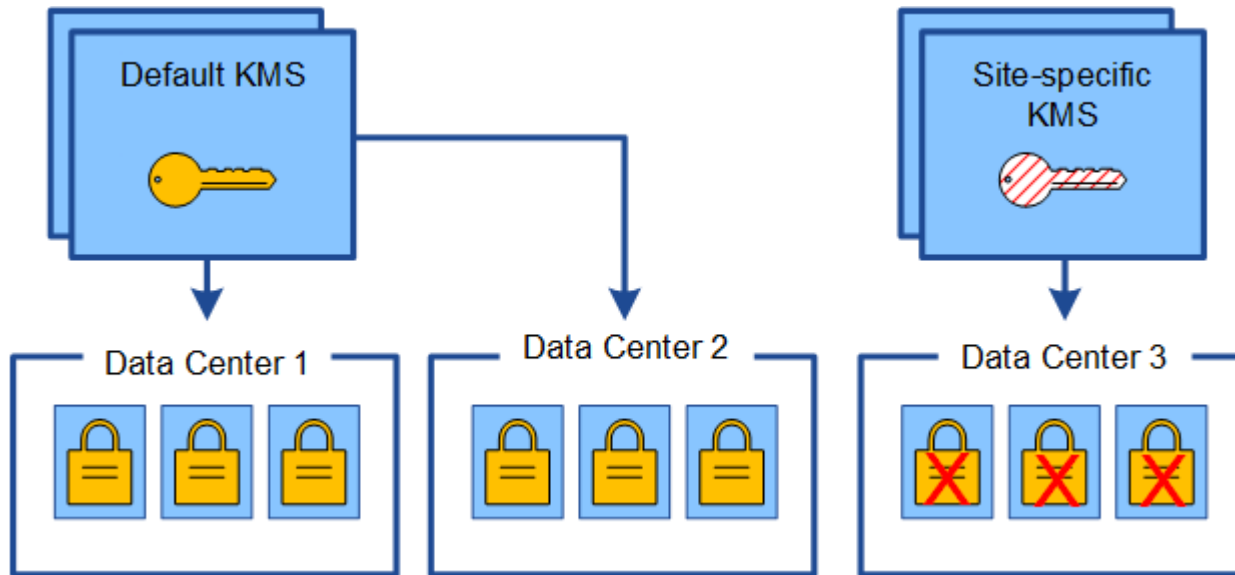
사이트에 사용되는 KMS를 변경하는 경우 해당 사이트에서 이전에 암호화된 어플라이언스 노드를 새 KMS에 저장된 키를 사용하여 해독할 수 있는지 확인해야 합니다. 경우에 따라 기존 KMS에서 새 KMS로 최신 버전의 암호화 키를 복사해야 할 수도 있습니다. KMS가 사이트에서 암호화된 어플라이언스 노드를 해독할 수 있는 올바른 키를 가지고 있는지 확인해야 합니다.

예를 들면 다음과 같습니다.

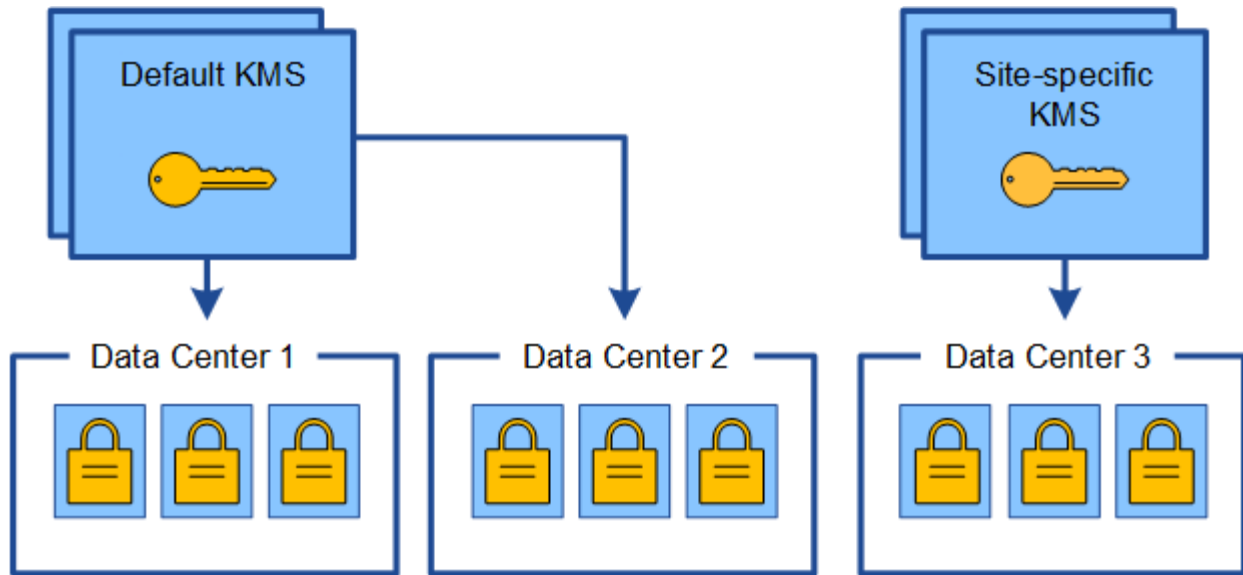
1. 처음에는 전용 KMS가 없는 모든 사이트에 적용되는 기본 KMS를 구성합니다.
2. KMS가 저장되면 \* 노드 암호화 \* 설정이 활성화된 모든 어플라이언스 노드가 KMS에 연결하여 암호화 키를 요청합니다. 이 키는 모든 사이트에서 어플라이언스 노드를 암호화하는 데 사용됩니다. 이러한 어플라이언스의 암호를 해독하는 데에도 이 동일한 키를 사용해야 합니다.



3. 한 사이트에 대해 사이트별 KMS를 추가하기로 결정합니다(그림의 데이터 센터 3). 그러나 어플라이언스 노드는 이미 암호화되어 있으므로 사이트별 KMS에 대한 구성을 저장하려고 하면 유효성 검사 오류가 발생합니다. 이 오류는 사이트별 KMS에 해당 사이트의 노드를 해독할 수 있는 올바른 키가 없기 때문에 발생합니다.



4. 이 문제를 해결하려면 기본 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사합니다. (원칙적으로 원래 키를 동일한 별칭이 있는 새 키에 복사합니다. 원래 키는 새 키의 이전 버전이 됩니다.) 이제 사이트별 KMS에는 데이터 센터 3의 어플라이언스 노드를 해독하는 올바른 키가 있으므로 StorageGRID에 저장할 수 있습니다.



사이트에 사용되는 **KMS**를 변경하는 사용 사례

이 표에는 사이트에 대한 KMS를 변경하는 가장 일반적인 경우를 위한 필수 단계가 요약되어 있습니다.

사이트의 <b>KMS</b> 를 변경하는 사용 사례	필요한 단계
하나 이상의 사이트별 KMS 항목이 있으며 이 중 하나를 기본 KMS로 사용하려고 합니다.	<p>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.</p> <p>"KMS(키 관리 서버) 편집"</p>
기본 KMS가 있으며 확장 시 새 사이트를 추가합니다. 새 사이트에 기본 KMS를 사용하지 않으려는 경우	<ol style="list-style-type: none"> <li>1. 새 사이트의 어플라이언스 노드가 기본 KMS에 의해 이미 암호화된 경우 KMS 소프트웨어를 사용하여 기본 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사합니다.</li> <li>2. Grid Manager를 사용하여 새 KMS를 추가하고 사이트를 선택합니다.</li> </ol> <p>"KMS(키 관리 서버) 추가"</p>
사이트의 KMS가 다른 서버를 사용하도록 해야 합니다.	<ol style="list-style-type: none"> <li>1. 사이트의 어플라이언스 노드가 기존 KMS에 의해 이미 암호화된 경우 KMS 소프트웨어를 사용하여 기존 KMS에서 새 KMS로 암호화 키의 현재 버전을 복사합니다.</li> <li>2. Grid Manager를 사용하여 기존 KMS 구성을 편집하고 새 호스트 이름 또는 IP 주소를 입력합니다.</li> </ol> <p>"KMS(키 관리 서버) 추가"</p>

## KMS에서 클라이언트로 StorageGRID 구성

KMS를 StorageGRID에 추가하려면 각 외부 키 관리 서버 또는 KMS 클러스터에 대해 StorageGRID를 클라이언트로 구성해야 합니다.

이 작업에 대해

이러한 지침은 Thales CipherTrust Manager k170v, 버전 2.0, 2.1 및 2.2에 적용됩니다. StorageGRID에서 다른 키 관리 서버를 사용하는 방법에 대한 질문이 있는 경우 기술 지원 부서에 문의하십시오.

### "Thales CipherTrust 관리자"

단계

1. KMS 소프트웨어에서 사용하려는 각 KMS 또는 KMS 클러스터에 대해 StorageGRID 클라이언트를 만듭니다.

각 KMS는 단일 사이트 또는 사이트 그룹에서 StorageGRID 어플라이언스 노드에 대한 단일 암호화 키를 관리합니다.

2. KMS 소프트웨어에서 각 KMS 또는 KMS 클러스터에 대한 AES 암호화 키를 만듭니다.

암호화 키를 내보낼 수 있어야 합니다.

3. 각 KMS 또는 KMS 클러스터에 대해 다음 정보를 기록합니다.

KMS를 StorageGRID에 추가할 때 이 정보가 필요합니다.

- 각 서버의 호스트 이름 또는 IP 주소입니다.
- KMS에서 KMIP 포트를 사용합니다.
- KMS의 암호화 키에 대한 키 별칭입니다.



암호화 키는 KMS에 이미 있어야 합니다. StorageGRID는 KMS 키를 만들거나 관리하지 않습니다.

4. 각 KMS 또는 KMS 클러스터에 대해 CA(인증 기관)가 서명한 서버 인증서 또는 인증서 체인 순서에 따라 연결된 PEM 인코딩된 CA 인증서 파일이 들어 있는 인증서 번들을 받습니다.

서버 인증서를 사용하면 외부 KMS가 StorageGRID에 자신을 인증할 수 있습니다.

- 인증서는 PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식을 사용해야 합니다.
- 각 서버 인증서의 주체 대체 이름(SAN) 필드에는 StorageGRID가 연결할 정규화된 도메인 이름(FQDN) 또는 IP 주소가 포함되어야 합니다.



StorageGRID에서 KMS를 구성할 때 \* 호스트 이름 \* 필드에 동일한 FQDN 또는 IP 주소를 입력해야 합니다.

- 서버 인증서는 KMS의 KMIP 인터페이스에서 사용하는 인증서와 일치해야 하며, 일반적으로 포트 5696을 사용합니다.

5. 외부 KMS 및 클라이언트 인증서의 개인 키로 StorageGRID에 발급된 공용 클라이언트 인증서를 얻습니다.

클라이언트 인증서를 사용하면 StorageGRID가 KMS에 대한 인증을 받을 수 있습니다.

## KMS(키 관리 서버) 추가

StorageGRID 키 관리 서버 마법사를 사용하여 각 KMS 또는 KMS 클러스터를 추가합니다.

필요한 것

- 을(를) 검토해야 합니다 "[키 관리 서버 사용에 대한 고려 사항 및 요구 사항](#)".
- 이(가) 있어야 합니다 "[KMS에서 StorageGRID를 클라이언트로 구성했습니다](#)" 또한 각 KMS 또는 KMS 클러스터에 필요한 정보가 있어야 합니다
- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

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.

["사이트의 KMS를 변경할 때의 고려 사항"](#)

단계

1. "[1단계: KMS 세부 정보를 입력합니다](#)"
2. "[2단계: 서버 인증서 업로드](#)"
3. "[3단계: 클라이언트 인증서 업로드](#)"

**1단계: KMS** 세부 정보를 입력합니다

키 관리 서버 추가 마법사의 1단계(KMS 세부 정보 입력)에서 KMS 또는 KMS 클러스터에 대한 세부 정보를 제공합니다.

단계

1. 구성 \* \* 시스템 설정 \* 키 관리 서버 \* 를 선택합니다.

구성 세부 정보 탭이 선택된 상태로 키 관리 서버 페이지가 나타납니다.

## Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create
✎ Edit
🗑 Remove

KMS Display Name	Key Name	Manages keys for	Hostname	Certificate Status
No key management servers have been configured. Select Create.				

2. Create \* 를 선택합니다.

키 관리 서버 추가 마법사의 1단계(KMS 세부 정보 입력)가 나타납니다.

### Add a Key Management Server

1  
**Enter KMS  
Details**

2  
**Upload  
Server  
Certificate**

3  
**Upload Client  
Certificates**

Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster, select + to add a hostname for each server in the cluster.

KMS Display Name

Key Name

Manages keys for

-- Choose One --

Port

Hostname

+

Cancel
Next

3. KMS에 구성된 KMS 및 StorageGRID 클라이언트에 대한 다음 정보를 입력합니다.

필드에 입력합니다	설명
KMS 표시 이름	이 KMS를 식별하는 데 도움이 되는 설명 이름입니다. 1자에서 64자 사이여야 합니다.



필드에 입력합니다	설명
키 이름	KMS에서 StorageGRID 클라이언트에 대한 정확한 키 별칭입니다. 1자에서 255자 사이여야 합니다.
의 키를 관리합니다	<p>이 KMS와 관련된 StorageGRID 사이트입니다. 가능하면 다른 KMS에서 관리하지 않는 모든 사이트에 적용되는 기본 KMS를 구성하기 전에 사이트별 키 관리 서버를 구성해야 합니다.</p> <ul style="list-style-type: none"> <li>• 이 KMS가 특정 사이트의 어플라이언스 노드에 대한 암호화 키를 관리하는 경우 사이트를 선택합니다.</li> <li>• 다른 KMS(기본 KMS)에서 관리하지 않는 사이트 * 를 선택하여 전용 KMS가 없는 사이트 및 이후 확장에 추가한 사이트에 적용되는 기본 KMS를 구성합니다. <ul style="list-style-type: none"> <li>◦ 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.</li> </ul> </li> </ul>
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"> <li>• 참고: * 서버 인증서의 SAN 필드에는 여기에 입력한 FQDN 또는 IP 주소가 포함되어야 합니다. 그렇지 않으면 StorageGRID는 KMS 또는 KMS 클러스터의 모든 서버에 연결할 수 없습니다.</li> </ul>

4. KMS 클러스터를 사용하는 경우 더하기 기호를 선택합니다 + 클러스터에 있는 각 서버의 호스트 이름을 추가합니다.

5. 다음 \* 을 선택합니다.

키 관리 서버 추가 마법사의 2단계(서버 인증서 업로드)가 나타납니다.

## 2단계: 서버 인증서 업로드

키 관리 서버 추가 마법사의 2단계(서버 인증서 업로드)에서 KMS에 대한 서버 인증서(또는 인증서 번들)를 업로드합니다. 서버 인증서를 사용하면 외부 KMS가 StorageGRID에 자신을 인증할 수 있습니다.

### 단계

1. 2단계(서버 인증서 업로드) \* 에서 저장된 서버 인증서 또는 인증서 번들의 위치를 찾습니다.

## Add a Key Management Server



Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate 

Cancel

Back

Next

2. 인증서 파일을 업로드합니다.

서버 인증서 메타데이터가 나타납니다.

## Add a Key Management Server



Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ⓘ  k170vCA.pem

### Server Certificate Metadata

```
Server DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Serial Number: 71:CD:6D:72:53:B5:6D:0A:8C:69:13:0D:4D:D7:81:0E
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T21:12:45.000Z
Expires On: 2030-10-13T21:12:45.000Z
SHA-1 Fingerprint: EE:E4:6E:17:86:DF:56:B4:F5:AF:A2:3C:BD:56:6B:10:DB:B2:5A:79
```

Cancel

Back

Next



인증서 번들을 업로드한 경우 각 인증서의 메타데이터가 해당 탭에 표시됩니다.

3. 다음 \* 을 선택합니다.

키 관리 서버 추가 마법사의 3단계(클라이언트 인증서 업로드)가 나타납니다.

### 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.

## Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate 

Client Certificate Private Key 

Cancel

Back

Save

2. 클라이언트 인증서 파일을 업로드합니다.

클라이언트 인증서 메타데이터가 나타납니다.

3. 클라이언트 인증서의 개인 키 위치를 찾습니다.

4. 개인 키 파일을 업로드합니다.

클라이언트 인증서 및 클라이언트 인증서 개인 키에 대한 메타데이터가 나타납니다.

## Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate  k170vClientCert.pem

```
Server DN: /CN=admin/UID=  
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB  
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA  
Issued On: 2020-10-15T23:31:49.000Z  
Expires On: 2022-10-15T23:31:49.000Z  
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69
```

Client Certificate Private Key  k170vClientKey.pem

Cancel

Back

Save

5. 저장 \* 을 선택합니다.

키 관리 서버와 어플라이언스 노드 간의 연결은 테스트를 거칩니다. 모든 연결이 올바르고 KMS에서 올바른 키를 찾으면 키 관리 서버 페이지의 표에 새 키 관리 서버가 추가됩니다.



KMS를 추가한 직후 키 관리 서버 페이지의 인증서 상태는 알 수 없음으로 표시됩니다. 각 인증서의 실제 상태를 가져오는 데 30분 정도 StorageGRID 걸릴 수 있습니다. 현재 상태를 보려면 웹 브라우저를 새로 고쳐야 합니다.

6. 저장 \* 을 선택할 때 오류 메시지가 나타나면 메시지 세부 정보를 검토한 다음 \* 확인 \* 을 선택합니다.

예를 들어 연결 테스트에 실패한 경우 422:처리할 수 없는 엔터티 오류가 발생할 수 있습니다.

7. 외부 연결을 테스트하지 않고 현재 구성을 저장해야 하는 경우 \* 강제 저장 \* 을 선택합니다.

## Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ⓘ  k170vClientCert.pem

Server DN: /CN=admin/UID=  
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB  
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA  
Issued On: 2020-10-15T23:31:49.000Z  
Expires On: 2022-10-15T23:31:49.000Z  
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ⓘ  k170vClientKey.pem

Select **Force Save** to save this KMS without testing the external connections. If there is an issue with the configuration, you might not be able to reboot any FDE-enabled appliance nodes at the affected site, and you might lose access to your data.

Cancel

Back

Force Save

Save



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.

### Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

KMS 구성은 저장되지만 KMS에 대한 연결은 테스트되지 않습니다.

## KMS 세부 정보 보기

서버 및 클라이언트 인증서의 현재 상태를 포함하여 StorageGRID 시스템의 각 키 관리 서버(KMS)에 대한 정보를 볼 수 있습니다.

단계

1. 구성 \*\* 시스템 설정 \* 키 관리 서버 \* 를 선택합니다.

키 관리 서버 페이지가 나타납니다. 구성 세부 정보 탭에는 구성된 모든 키 관리 서버가 표시됩니다.

### Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name	Key Name	Manages keys for	Hostname	Certificate Status
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

2. 각 KMS에 대한 표의 정보를 검토합니다.

필드에 입력합니다	설명
KMS 표시 이름	KMS의 설명 이름입니다.
키 이름	KMS에서 StorageGRID 클라이언트의 키 별칭입니다.
의 키를 관리합니다	KMS와 관련된 StorageGRID 사이트  이 필드에는 특정 StorageGRID 사이트 또는 다른 KMS(기본 KMS)가 관리하지 않는 사이트의 이름이 표시됩니다.*

필드에 입력합니다	설명
호스트 이름	<p>KMS의 정규화된 도메인 이름 또는 IP 주소입니다.</p> <p>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.</p> <p>예를 들면 다음과 같습니다. 10.10.10.10 and 10.10.10.11 또는 10.10.10.10 and 2 others.</p> <p>클러스터의 모든 호스트 이름을 보려면 KMS를 선택한 다음 * 편집 * 을 선택합니다.</p>
인증서 상태입니다	<p>서버 인증서, 선택적 CA 인증서 및 클라이언트 인증서의 현재 상태: 유효, 만료, 만료 임박 또는 알 수 없음.</p> <ul style="list-style-type: none"> <li>참고: * StorageGRID 인증서 상태를 업데이트하는데 30분 정도 걸릴 수 있습니다. 현재 값을 보려면 웹 브라우저를 새로 고쳐야 합니다.</li> </ul>

3. 인증서 상태가 알 수 없음 인 경우 최대 30분 동안 기다린 다음 웹 브라우저를 새로 고칩니다.



KMS를 추가한 직후 키 관리 서버 페이지의 인증서 상태는 알 수 없음으로 표시됩니다. 각 인증서의 실제 상태를 가져오는 데 30분 정도 StorageGRID 걸릴 수 있습니다. 실제 상태를 보려면 웹 브라우저를 새로 고쳐야 합니다.

4. 인증서 상태 열에 인증서가 만료되었거나 만료 시기가 임박했다는 메시지가 표시되면 가능한 한 빨리 문제를 해결하십시오.

StorageGRID 모니터링 및 문제 해결에 대한 지침은 \* KMS CA 인증서 만료 \*, \* KMS 클라이언트 인증서 만료 \* 및 \* KMS 서버 인증서 만료 \* 경고에 대한 권장 조치를 참조하십시오.



데이터 액세스를 유지하려면 가능한 한 빨리 인증서 문제를 해결해야 합니다.

관련 정보

["모니터링 및 문제 해결"](#)

[암호화된 노드 보기](#)

노드 암호화 \* 설정이 활성화된 StorageGRID 시스템의 어플라이언스 노드에 대한 정보를 볼 수 있습니다.

단계



1. 구성 \* \* 시스템 설정 \* 키 관리 서버 \* 를 선택합니다.

키 관리 서버 페이지가 나타납니다. 구성 세부 정보 탭에는 구성된 모든 키 관리 서버가 표시됩니다.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details **Encrypted Nodes**

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

2. 페이지 상단에서 \* 암호화된 노드 \* 탭을 선택합니다.

Key Management Server

If your StorageGRID system includes appliance nodes with Full Disk Encryption (FDE) enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID data at rest.

Configuration Details **Encrypted Nodes**

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

암호화된 노드 탭에는 \* 노드 암호화 \* 설정이 활성화된 StorageGRID 시스템의 어플라이언스 노드가 나열됩니다.

Configuration Details **Encrypted Nodes**

Review the KMS status for all appliance nodes that have node encryption enabled. Address any issues immediately to ensure your data is fully protected. If no KMS exists for a site, select Configuration Details and add a KMS.

**Nodes with Encryption Enabled**

Node Name	Node Type	Site	KMS Display Name ?	Key UID ?	Status ?
SGA-010-096-104-67	Storage Node	Data Center 1	Default KMS	41b0...5c57	✓ Connected to KMS (2021-03-12 10:59:32 MST)

3. 각 어플라이언스 노드에 대해 표의 정보를 검토합니다.

열	설명
노드 이름	어플라이언스 노드의 이름입니다.

이름	설명
노드 유형	노드 유형: 스토리지, 관리자 또는 게이트웨이
사이트	노드가 설치된 StorageGRID 사이트의 이름입니다.
KMS 표시 이름	<p>노드에 사용된 KMS의 설명 이름입니다.</p> <p>KMS가 나열되지 않은 경우 구성 세부 정보 탭을 선택하여 KMS를 추가합니다.</p> <p><a href="#">"KMS(키 관리 서버) 추가"</a></p>
키 UID	<p>어플라이언스 노드에서 데이터를 암호화하고 해독하는 데 사용되는 암호화 키의 고유 ID입니다. 전체 키 UID를 보려면 셀 위로 커서를 이동합니다.</p> <p>대시(-- )는 어플라이언스 노드와 KMS 사이의 연결 문제로 인해 키 UID를 알 수 없음을 나타냅니다.</p>
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"> <li>참고: * 새 값을 보려면 웹 브라우저를 새로 고쳐야 합니다.</li> </ul>

#### 4. 상태 옆에 KMS 문제가 표시되면 즉시 문제를 해결하십시오.

KMS가 정상적으로 작동하는 동안 KMS\*에 연결된 상태로 표시됩니다. 노드가 그리드에서 연결이 끊어지면 노드 연결 상태가 표시됩니다(관리자 다운 또는 알 수 없음).

다른 상태 메시지는 이름이 같은 StorageGRID 알림에 해당합니다.

- KMS 구성을 로드하지 못했습니다
- KMS 연결 오류입니다
- KMS 암호화 키 이름을 찾을 수 없습니다
- KMS 암호화 키 회전이 실패했습니다
- 킬로미터 키가 어플라이언스 볼륨을 해독하지 못했습니다
- KMS가 구성되지 않았습니다. StorageGRID 모니터링 및 문제 해결에 대한 지침에서 이러한 경고에 대한 권장 조치를 참조하십시오.



데이터를 완벽하게 보호하려면 모든 문제를 즉시 해결해야 합니다.

관련 정보

["모니터링 및 문제 해결"](#)

## KMS(키 관리 서버) 편집

예를 들어 인증서가 곧 만료될 경우 키 관리 서버의 구성을 편집해야 할 수 있습니다.

필요한 것

- 을(를) 검토해야 합니다 "키 관리 서버 사용에 대한 고려 사항 및 요구 사항".
- KMS에 대해 선택한 사이트를 업데이트할 계획이라면 을 검토해야 합니다 "사이트의 KMS를 변경할 때의 고려 사항".
- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

단계

1. 구성 \* \* 시스템 설정 \* 키 관리 서버 \* 를 선택합니다.

Key Management Server 페이지가 나타나고 구성된 모든 키 관리 서버가 표시됩니다.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:


- Ensure that the KMS is KMP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

KMS Display Name	Key Name	Manages keys for	Hostname	Certificate Status
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

2. 편집할 KMS를 선택하고 \* 편집 \* 을 선택합니다.
3. 필요한 경우 키 관리 서버 편집 마법사의 \* 1단계(KMS 세부 정보 입력) \* 에 있는 세부 정보를 업데이트합니다.

필드에 입력합니다	설명
KMS 표시 이름	이 KMS를 식별하는 데 도움이 되는 설명 이름입니다. 1자에서 64자 사이여야 합니다.

필드에 입력합니다	설명
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> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;">  <p>KMS의 키 이름(별칭)을 변경하여 키를 회전하려고 하지 마십시오. 대신 KMS 소프트웨어의 키 버전을 업데이트하여 키를 돌리십시오. StorageGRID를 사용하려면 KMS에서 동일한 키 별칭을 사용하여 이전에 사용한 모든 키 버전과 향후 모든 키 버전에 액세스할 수 있어야 합니다. 구성된 KMS의 키 별칭을 변경하면 StorageGRID에서 데이터의 암호를 해독하지 못할 수 있습니다.</p> <p><b>"키 관리 서버 사용에 대한 고려 사항 및 요구 사항"</b></p> </div>
의 키를 관리합니다	<p>사이트별 KMS를 편집하고 있고 기본 KMS가 아직 없는 경우 선택적으로 * 다른 KMS에 의해 관리되지 않는 사이트(기본 KMS) * 를 선택합니다. 이 항목을 선택하면 사이트별 KMS가 기본 KMS로 변환되며, 이 KMS는 전용 KMS가 없는 모든 사이트와 확장 시 추가된 사이트에 적용됩니다.</p> <ul style="list-style-type: none"> <li>참고: * 사이트별 KMS를 편집하는 경우에는 다른 사이트를 선택할 수 없습니다. 기본 KMS를 편집하는 경우 특정 사이트를 선택할 수 없습니다.</li> </ul>
포트	<p>KMS 서버가 KMIP(Key Management Interoperability Protocol) 통신에 사용하는 포트입니다. 기본값은 5696으로, KMIP 표준 포트입니다.</p>
호스트 이름	<p>KMS의 정규화된 도메인 이름 또는 IP 주소입니다.</p> <ul style="list-style-type: none"> <li>참고: * 서버 인증서의 SAN 필드에는 여기에 입력한 FQDN 또는 IP 주소가 포함되어야 합니다. 그렇지 않으면 StorageGRID는 KMS 또는 KMS 클러스터의 모든 서버에 연결할 수 없습니다.</li> </ul>

4. KMS 클러스터를 구성하는 경우 더하기 기호를 선택합니다 **+** 클러스터에 있는 각 서버의 호스트 이름을 추가합니다.

5. 다음 \* 을 선택합니다.

키 관리 서버 편집 마법사의 2단계(서버 인증서 업로드)가 나타납니다.

6. 서버 인증서를 교체해야 하는 경우 \* 찾아보기 \* 를 선택하고 새 파일을 업로드합니다.

7. 다음 \* 을 선택합니다.

키 관리 서버 편집 마법사의 3단계(클라이언트 인증서 업로드)가 나타납니다.

8. 클라이언트 인증서와 클라이언트 인증서 개인 키를 교체해야 하는 경우 \* 찾아보기 \* 를 선택하고 새 파일을

업로드합니다.

9. 저장 \* 을 선택합니다.

영향을 받는 사이트에서 키 관리 서버와 모든 노드 암호화 어플라이언스 노드 간의 연결을 테스트합니다. 모든 노드 연결이 유효하고 KMS에서 올바른 키를 찾으면 키 관리 서버가 키 관리 서버 페이지의 테이블에 추가됩니다.

10. 오류 메시지가 나타나면 메시지 세부 정보를 검토하고 \* OK \* 를 선택합니다.

예를 들어, 이 KMS에 대해 선택한 사이트가 다른 KMS에 의해 이미 관리되고 있거나 연결 테스트에 실패한 경우 422:처리할 수 없는 엔터티 오류가 발생할 수 있습니다.

11. 연결 오류를 해결하기 전에 현재 설정을 저장해야 하는 경우 \* 강제 저장 \* 을 선택합니다.



강제 저장 \* 을 선택하면 KMS 구성이 저장되지만 각 제품에서 해당 KMS로의 외부 연결은 테스트되지 않습니다. 구성에 문제가 있을 경우 해당 사이트에서 노드 암호화가 활성화된 어플라이언스 노드를 재부팅하지 못할 수 있습니다. 문제가 해결될 때까지 데이터에 액세스하지 못할 수 있습니다.

KMS 구성이 저장됩니다.

12. 확인 경고를 검토하고 구성을 강제 저장하려면 \* OK \* 를 선택합니다.

**Warning**

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel OK

KMS 구성은 저장되지만 KMS에 대한 연결은 테스트되지 않습니다.

## KMS(키 관리 서버) 제거

경우에 따라 키 관리 서버를 제거할 수 있습니다. 예를 들어 사이트를 해체한 경우 사이트별 KMS를 제거할 수 있습니다.

필요한 것

- 을(를) 검토해야 합니다 "[키 관리 서버 사용에 대한 고려 사항 및 요구 사항](#)".
- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

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 \* \* 시스템 설정 \* 키 관리 서버 \* 를 선택합니다.

Key Management Server 페이지가 나타나고 구성된 모든 키 관리 서버가 표시됩니다.

#### Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
<input checked="" type="radio"/> Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

2. 제거할 KMS의 라디오 단추를 선택하고 \* 제거 \* 를 선택합니다.
3. 경고 대화 상자에서 고려 사항을 검토합니다.

### Warning

#### Delete KMS Configuration

You can only remove a KMS in these cases:

- You are removing a site-specific KMS for a site that has no appliance nodes with node encryption enabled.
- You are removing the default KMS, but a site-specific KMS already exists for each site with node encryption.

Are you sure you want to delete the Default KMS KMS configuration?

Cancel

OK

4. OK \* 를 선택합니다.

KMS 구성이 제거되었습니다.

## 테넌트 관리

그리드 관리자는 S3 및 Swift 클라이언트가 StorageGRID 시스템을 사용하여 오브젝트를 저장 및 검색하고, 스토리지 사용량을 모니터링하고, 클라이언트가 수행할 수 있는 작업을 관리하는 데 사용하는 테넌트 계정을 생성하고 관리합니다.

### 테넌트 계정이란 무엇입니까

테넌트 계정을 사용하면 S3(Simple Storage Service) REST API 또는 Swift REST API를 사용하는 클라이언트 애플리케이션이 StorageGRID에 개체를 저장하고 검색할 수 있습니다.

각 테넌트 계정은 계정을 생성할 때 지정하는 단일 프로토콜 사용을 지원합니다. 두 프로토콜을 모두 사용하는 StorageGRID 시스템에 오브젝트를 저장하고 검색하려면 S3 버킷 및 오브젝트, Swift 컨테이너 및 오브젝트, 두 개의 테넌트 계정을 만들어야 합니다. 각 테넌트 계정에는 고유한 계정 ID, 인증된 그룹 및 사용자, 버킷 또는 컨테이너 및 객체가 있습니다.

필요에 따라 시스템에 저장된 객체를 다른 엔터티로 분리하려는 경우 추가 테넌트 계정을 생성할 수 있습니다. 예를 들어, 다음과 같은 사용 사례에서 여러 테넌트 계정을 설정할 수 있습니다.

- \* 기업 활용 사례: \* 엔터프라이즈 애플리케이션에서 StorageGRID 시스템을 관리하는 경우 조직의 여러 부서에서 그리드의 객체 스토리지를 분리할 수 있습니다. 이 경우 마케팅 부서, 고객 지원 부서, 인사 부서 등에 대한 테넌트 계정을 만들 수 있습니다.



S3 클라이언트 프로토콜을 사용하는 경우 S3 버킷 및 버킷 정책을 사용하여 엔터프라이즈의 부서 간에 오브젝트를 분리할 수 있습니다. 테넌트 계정은 사용할 필요가 없습니다. 자세한 내용은 S3 클라이언트 애플리케이션 구현 지침을 참조하십시오.

- \* 서비스 공급자 활용 사례: \* StorageGRID 시스템을 서비스 공급자로 관리하는 경우 그리드의 객체 스토리지를 그리드의 스토리지를 임대할 다른 엔터티로 분리할 수 있습니다. 이 경우 회사 A, 회사 B, 회사 C 등에 대한 테넌트 계정을 생성합니다.

### 테넌트 계정 생성 및 구성

테넌트 계정을 생성할 때 다음 정보를 지정합니다.

- 테넌트 계정의 표시 이름입니다.
- 테넌트 계정(S3 또는 Swift)에서 사용할 클라이언트 프로토콜입니다.
- S3 테넌트 계정의 경우: 테넌트 계정에 S3 버킷을 포함하는 플랫폼 서비스를 사용할 수 있는 권한이 있는지 여부  
테넌트 계정에서 플랫폼 서비스를 사용하도록 허용하는 경우 해당 사용자의 사용을 지원하도록 그리드가 구성되어 있는지 확인해야 합니다. "플랫폼 서비스"를 참조하십시오.
- 필요한 경우 테넌트 계정의 스토리지 할당량 — 테넌트의 객체에 사용할 수 있는 최대 GB, 테라바이트 또는 PB입니다. 할당량이 초과되면 테넌트가 새 객체를 생성할 수 없습니다.



테넌트의 스토리지 할당량은 물리적 크기(디스크 크기)가 아닌 논리적 양(오브젝트 크기)을 나타냅니다.

- StorageGRID 시스템에 대해 ID 페더레이션이 설정된 경우 테넌트 계정을 구성할 수 있는 루트 액세스 권한이 있는 통합 그룹입니다.
- StorageGRID 시스템에서 SSO(Single Sign-On)를 사용하지 않는 경우 테넌트 계정이 자체 ID 소스를 사용할지 또는 그리드의 ID 소스를 공유할지 여부 및 테넌트의 로컬 루트 사용자의 초기 암호를 공유할지 여부

테넌트 계정이 생성된 후 다음 작업을 수행할 수 있습니다.

- \* GRID용 플랫폼 서비스 관리 \*: 테넌트 계정에 대해 플랫폼 서비스를 사용하는 경우, 플랫폼 서비스 메시지가 전달되는 방법과 StorageGRID 배포에서 플랫폼 서비스를 사용하는 데 필요한 네트워킹 요구 사항을 이해해야 합니다.
- \* 테넌트 계정의 스토리지 사용량 모니터링 \*: 테넌트가 해당 계정을 사용하기 시작한 후 Grid Manager를 사용하여 각 테넌트가 사용하는 스토리지 양을 모니터링할 수 있습니다.

테넌트에 대해 할당량을 설정한 경우 \* 테넌트 할당량 사용량 높음 \* 알림을 설정하여 테넌트가 할당량을 사용하고 있는지 확인할 수 있습니다. 활성화된 경우 테넌트가 할당량의 90%를 사용한 경우 이 경고가 트리거됩니다. 자세한 내용은 StorageGRID 모니터링 및 문제 해결 설명서의 경고 참조를 참조하십시오.

- \* 클라이언트 작업 구성 \*: 일부 클라이언트 작업이 금지되는지 여부를 구성할 수 있습니다.

### S3 테넌트 구성 중

S3 테넌트 계정이 생성된 후 테넌트 사용자는 테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 통합을 설정하고(ID 소스를 그리드와 공유하지 않는 경우) 로컬 그룹 및 사용자를 생성합니다
- S3 액세스 키 관리
- S3 버킷 생성 및 관리
- 스토리지 사용량 모니터링
- 플랫폼 서비스 사용(활성화된 경우)



S3 테넌트 사용자는 테넌트 관리자를 사용하여 S3 액세스 키 및 버킷을 생성 및 관리할 수 있지만, S3 클라이언트 애플리케이션을 사용하여 오브젝트를 수집 및 관리해야 합니다.

### Swift 테넌트 구성 중

Swift 테넌트 계정이 생성된 후 테넌트의 루트 사용자는 테넌트 관리자에 액세스하여 다음과 같은 작업을 수행할 수 있습니다.

- ID 통합을 설정하고(ID 소스를 그리드와 공유하지 않는 경우) 로컬 그룹 및 사용자를 만듭니다
- 스토리지 사용량 모니터링



Swift 사용자는 테넌트 관리자에 액세스하려면 루트 액세스 권한이 있어야 합니다. 그러나 루트 액세스 권한은 사용자가 Swift REST API에 인증하여 컨테이너를 생성하고 객체를 수집하는 것을 허용하지 않습니다. 사용자는 Swift REST API에 인증할 수 있는 Swift 관리자 권한이 있어야 합니다.

관련 정보

["테넌트 계정을 사용합니다"](#)



## 테넌트 계정을 생성하는 중입니다

StorageGRID 시스템의 스토리지에 대한 액세스를 제어하려면 하나 이상의 테넌트 계정을 생성해야 합니다.

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

### 단계

1. Tenants \* 를 선택합니다.

테넌트 계정 페이지가 나타나고 기존 테넌트 계정이 나열됩니다.

#### Tenant Accounts

View information for each tenant account.

**Note:** 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 and select **View Details**.



The screenshot shows a web interface for managing Tenant Accounts. At the top, there are buttons for '+ Create', 'View details', 'Edit', 'Actions', and 'Export to CSV'. A search bar on the right is labeled 'Search by Name/ID'. Below the buttons is a table header with columns: 'Display Name', 'Space Used', 'Quota Utilization', 'Quota', 'Object Count', and 'Sign in'. The table body is empty, with the text 'No results found.' displayed. At the bottom right, there is a 'Show 20 rows per page' dropdown menu.

2. Create \* 를 선택합니다.

Create Tenant Account 페이지가 나타납니다. 페이지에 포함된 필드는 StorageGRID 시스템에서 SSO(Single Sign-On)를 활성화했는지 여부에 따라 달라집니다.

- SSO를 사용하지 않는 경우 Create Tenant Account 페이지는 다음과 같습니다.

## Create Tenant Account

### Tenant Details

Display Name

Protocol  S3  Swift

Storage Quota (optional)

### Authentication [?](#)

Configure how the tenant account will be accessed.

Uses Own Identity Source

Specify a password for the tenant's local root user.

Username root

Password

Confirm Password

Cancel

Save

- SSO가 활성화된 경우 Create Tenant Account 페이지는 다음과 같습니다.

## Create Tenant Account

### Tenant Details

Display Name

Protocol  S3  Swift

Allow Platform Services

Storage Quota (optional)

### Authentication

Because single sign-on is enabled, the tenant must use the Grid Manager's identity federation service, and no local users can sign in. You must select an existing federated group to have the initial Root Access permission for the tenant.

Uses Own Identity Source

Single sign-on is enabled. The tenant cannot use its own identity source.

Root Access Group

Cancel

Save

관련 정보

["ID 페더레이션 사용"](#)

["Single Sign-On 구성"](#)

**StorageGRID**에서 **SSO**를 사용하지 않는 경우 테넌트 계정 생성

테넌트 계정을 생성할 때 이름, 클라이언트 프로토콜 및 선택적으로 스토리지 할당량을 지정합니다. StorageGRID에서 SSO(Single Sign-On)를 사용하지 않는 경우 테넌트 계정에서 자체 ID 소스를 사용할지 여부를 지정하고 테넌트의 로컬 루트 사용자에게 대한 초기 암호를 구성해야 합니다.

이 작업에 대해

테넌트 계정에서 Grid Manager에 대해 구성된 ID 소스를 사용하고 테넌트 계정에 대한 루트 액세스 권한을 통합 그룹에 부여하려면 해당 통합 그룹을 Grid Manager로 가져와야 합니다. 이 관리 그룹에 그리드 관리자 권한을 할당할 필요는 없습니다. 의 지침을 참조하십시오 ["관리 그룹 관리"](#).

단계

1. Display Name \* (표시 이름 \*) 텍스트 상자에 이 테넌트 계정의 표시 이름을 입력합니다.

표시 이름은 고유하지 않아도 됩니다. 테넌트 계정이 생성되면 고유한 숫자 계정 ID를 받습니다.

- 이 테넌트 계정에서 사용할 클라이언트 프로토콜을 \* S3 \* 또는 \* Swift \* 로 선택합니다.
- S3 테넌트 계정의 경우 이 테넌트에서 S3 버킷을 위한 플랫폼 서비스를 사용하지 않도록 하려면 \* 플랫폼 서비스 허용 \* 확인란을 선택한 상태로 유지합니다.

플랫폼 서비스가 설정된 경우 테넌트는 외부 서비스에 액세스하는 CloudMirror 복제와 같은 기능을 사용할 수 있습니다. 이러한 기능을 사용하지 않도록 설정하여 테넌트가 사용하는 네트워크 대역폭 또는 기타 리소스의 양을 제한할 수 있습니다. "플랫폼 서비스"를 참조하십시오.

- 스토리지 할당량 \* 텍스트 상자에 원하는 경우 이 테넌트의 개체에 사용할 수 있도록 설정할 최대 기가바이트, 테라바이트 또는 페타 바이트 수를 입력합니다. 그런 다음 드롭다운 목록에서 단위를 선택합니다.

이 테넌트에 무제한 할당량을 사용하려면 이 필드를 비워 둡니다.



테넌트의 스토리지 할당량은 물리적 크기(디스크 크기)가 아닌 논리적 양(오브젝트 크기)을 나타냅니다. ILM 복사본 및 삭제 코딩은 사용된 할당량에 영향을 주지 않습니다. 할당량이 초과되면 테넌트 계정에서 새 객체를 생성할 수 없습니다.



각 테넌트 계정의 스토리지 사용량을 모니터링하려면 \* Usage \* 를 선택합니다. 또한 테넌트 계정은 테넌트 관리자의 대시보드 또는 테넌트 관리 API를 통해 자신의 스토리지 사용량을 모니터링할 수 있습니다. 노드가 그리드의 다른 노드로부터 격리되면 테넌트의 스토리지 사용량 값이 최신 상태가 아닐 수 있습니다. 네트워크 연결이 복원되면 합계가 업데이트됩니다.

- 테넌트가 자체 그룹 및 사용자를 관리하는 경우 다음 단계를 수행합니다.
  - 고유 ID 소스 사용 \* 확인란을 선택합니다(기본값).



이 확인란을 선택하고 테넌트 그룹 및 사용자에 대해 ID 페더레이션을 사용하려면 테넌트가 자체 ID 소스를 구성해야 합니다. 테넌트 계정 사용 지침을 참조하십시오.

- 테넌트의 로컬 루트 사용자에 대한 암호를 지정합니다.

- 테넌트가 Grid Manager에 대해 구성된 그룹 및 사용자를 사용하는 경우 다음 단계를 수행합니다.

- 고유 ID 소스 사용 \* 확인란의 선택을 취소합니다.

- 다음 중 하나 또는 모두를 수행합니다.

- 루트 액세스 그룹 필드의 그리드 관리자에서 테넌트에 대한 초기 루트 액세스 권한이 있어야 하는 기존 통합 그룹을 선택합니다.



적절한 권한이 있는 경우 필드를 클릭하면 그리드 관리자의 기존 통합 그룹이 나열됩니다. 그렇지 않으면 그룹의 고유 이름을 입력합니다.

- 테넌트의 로컬 루트 사용자에 대한 암호를 지정합니다.

- 저장 \* 을 클릭합니다.

테넌트 계정이 생성됩니다.

- 필요에 따라 새 테넌트에 액세스합니다. 그렇지 않으면 의 단계로 이동합니다 [나중에 테넌트에 액세스하는 중입니다](#).

만약...	수행할 작업...
제한된 포트에서 그리드 관리자 액세스	<p>이 테넌트 계정에 액세스하는 방법에 대한 자세한 내용을 보려면 * 제한 * 을 클릭하십시오.</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"> <li>• <i>FQDN_or_Admin_Node_IP</i> 은(는) 관리자 노드의 정규화된 도메인 이름 또는 IP 주소입니다</li> <li>• <i>port</i> 테넌트 전용 포트입니다</li> <li>• <i>20-digit-account-id</i> 테넌트의 고유 계정 ID입니다</li> </ul>
포트 443에서 그리드 관리자에 액세스하지만 로컬 루트 사용자에게 대한 암호를 설정하지 않았습니다	로그인 * 을 클릭하고 루트 액세스 통합 그룹에 사용자의 자격 증명을 입력합니다.
포트 443에서 그리드 관리자에 액세스하고 로컬 루트 사용자의 암호를 설정합니다	의 다음 단계로 이동합니다 <a href="#">루트로 로그인합니다</a> .

9. 테넌트에 루트로 로그인합니다.

a. Configure Tenant Account 대화 상자에서 \* Sign in as root \* 버튼을 클릭합니다.

### Configure Tenant Account

✓ Account S3 tenant created successfully.

If you are ready to configure this tenant account, sign in as the tenant's root user. Then, click the links below.

Sign in as root

- [Buckets](#) - Create and manage buckets.
- [Groups](#) - Manage user groups, and assign group permissions.
- [Users](#) - Manage local users, and assign users to groups.

Finish

버튼에 녹색 확인 표시가 나타나 현재 테넌트 계정에 루트 사용자로 로그인했음을 나타냅니다.

a. 링크를 클릭하여 테넌트 계정을 구성합니다.

각 링크는 테넌트 관리자에서 해당 페이지를 엽니다. 이 페이지를 완료하려면 테넌트 계정 사용 지침을 참조하십시오.

b. 마침 \* 을 클릭합니다.

10. 테넌트에 나중에 액세스하려면:

사용 중인 경우...	다음 중 하나를 수행합니다.
포트 443	<ul style="list-style-type: none"> <li>• Grid Manager에서 * Tenants * 를 선택하고 테넌트 이름 오른쪽에 있는 * 로그인 * 을 클릭합니다.</li> <li>• 웹 브라우저에 테넌트의 URL을 입력합니다.</li> </ul> <p><code>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</code></p> <ul style="list-style-type: none"> <li>◦ <i>FQDN_or_Admin_Node_IP</i> 은(는) 관리자 노드의 정규화된 도메인 이름 또는 IP 주소입니다</li> <li>◦ <i>20-digit-account-id</i> 테넌트의 고유 계정 ID입니다</li> </ul>
제한된 포트	<ul style="list-style-type: none"> <li>• Grid Manager에서 * Tenants * 를 선택하고 * Restricted * 를 클릭합니다.</li> <li>• 웹 브라우저에 테넌트의 URL을 입력합니다.</li> </ul> <p><code>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</code></p> <ul style="list-style-type: none"> <li>◦ <i>FQDN_or_Admin_Node_IP</i> 은(는) 관리자 노드의 정규화된 도메인 이름 또는 IP 주소입니다</li> <li>◦ <i>port</i> 테넌트 전용 제한 포트입니다</li> <li>◦ <i>20-digit-account-id</i> 테넌트의 고유 계정 ID입니다</li> </ul>

관련 정보

["방화벽을 통한 액세스 제어"](#)

["S3 테넌트 계정에 대한 플랫폼 서비스 관리"](#)

["테넌트 계정을 사용합니다"](#)

**SSO**가 활성화된 경우 테넌트 계정을 생성합니다

테넌트 계정을 생성할 때 이름, 클라이언트 프로토콜 및 선택적으로 스토리지 할당량을 지정합니다. StorageGRID에 대해 SSO(Single Sign-On)를 사용하도록 설정한 경우 테넌트

계정을 구성할 루트 액세스 권한이 있는 통합 그룹도 지정합니다.

단계

1. Display Name \* (표시 이름 \*) 텍스트 상자에 이 테넌트 계정의 표시 이름을 입력합니다.

표시 이름은 고유하지 않아도 됩니다. 테넌트 계정이 생성되면 고유한 숫자 계정 ID를 받습니다.

2. 이 테넌트 계정에서 사용할 클라이언트 프로토콜을 \* S3 \* 또는 \* Swift \* 로 선택합니다.
3. S3 테넌트 계정의 경우 이 테넌트에서 S3 버킷을 위한 플랫폼 서비스를 사용하지 않도록 하려면 \* 플랫폼 서비스 허용 \* 확인란을 선택한 상태로 유지합니다.

플랫폼 서비스가 설정된 경우 테넌트는 외부 서비스에 액세스하는 CloudMirror 복제와 같은 기능을 사용할 수 있습니다. 이러한 기능을 사용하지 않도록 설정하여 테넌트가 사용하는 네트워크 대역폭 또는 기타 리소스의 양을 제한할 수 있습니다. "플랫폼 서비스"를 참조하십시오.

4. 스토리지 할당량 \* 텍스트 상자에 원하는 경우 이 테넌트의 개체에 사용할 수 있도록 설정할 최대 기가바이트, 테라바이트 또는 페타 바이트 수를 입력합니다. 그런 다음 드롭다운 목록에서 단위를 선택합니다.

이 테넌트에 무제한 할당량을 사용하려면 이 필드를 비워 둡니다.



테넌트의 스토리지 할당량은 물리적 크기(디스크 크기)가 아닌 논리적 양(오브젝트 크기)을 나타냅니다. ILM 복사본 및 삭제 코딩은 사용된 할당량에 영향을 주지 않습니다. 할당량이 초과되면 테넌트 계정에서 새 객체를 생성할 수 없습니다.



각 테넌트 계정의 스토리지 사용량을 모니터링하려면 \* Usage \* 를 선택합니다. 또한 테넌트 계정은 테넌트 관리자의 대시보드 또는 테넌트 관리 API를 통해 자신의 스토리지 사용량을 모니터링할 수 있습니다. 노드가 그리드의 다른 노드로부터 격리되면 테넌트의 스토리지 사용량 값이 최신 상태가 아닐 수 있습니다. 네트워크 연결이 복원되면 합계가 업데이트됩니다.

5. [고유 ID 소스 사용] 확인란이 선택 취소되어 비활성화되어 있습니다.

SSO가 활성화되어 있기 때문에 테넌트는 Grid Manager에 대해 구성된 ID 소스를 사용해야 합니다. 로컬 사용자는 로그인할 수 없습니다.

6. [루트 액세스 그룹] \* 필드의 그리드 관리자에서 기존 통합 그룹을 선택하여 테넌트에 대한 초기 루트 액세스 권한을 가집니다.



적절한 권한이 있는 경우 필드를 클릭하면 그리드 관리자의 기존 통합 그룹이 나열됩니다. 그렇지 않으면 그룹의 고유 이름을 입력합니다.

7. 저장 \* 을 클릭합니다.

테넌트 계정이 생성됩니다. 테넌트 계정 페이지가 나타나고 새 테넌트에 대한 행이 포함됩니다.

8. 루트 액세스 그룹의 사용자인 경우 필요에 따라 새 테넌트에 대한 \* 로그인 \* 링크를 클릭하여 테넌트 관리자를 즉시 액세스하고 테넌트를 구성할 수 있습니다. 그렇지 않으면 \* 로그인 \* 링크의 URL을 테넌트 계정의 관리자에게 제공하십시오. (테넌트의 URL은 관리자 노드의 정규화된 도메인 이름 또는 IP 주소이며 그 뒤에 가 있습니다 `?accountid=20-digit-account-id` 참조)



로그인 \* 을 클릭했지만 테넌트 계정의 루트 액세스 그룹에 속하지 않은 경우 액세스 거부 메시지가 표시됩니다.

관련 정보

["Single Sign-On 구성"](#)

["S3 테넌트 계정에 대한 플랫폼 서비스 관리"](#)

["테넌트 계정을 사용합니다"](#)

## 테넌트의 로컬 루트 사용자에게 대한 암호 변경

루트 사용자가 계정에서 잠겨 있는 경우 테넌트의 로컬 루트 사용자의 암호를 변경해야 할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

StorageGRID 시스템에서 SSO(Single Sign-On)가 활성화된 경우 로컬 루트 사용자는 테넌트 계정에 로그인할 수 없습니다. 루트 사용자 작업을 수행하려면 사용자가 테넌트에 대한 루트 액세스 권한이 있는 통합 그룹에 속해야 합니다.

단계

1. Tenants \* 를 선택합니다.

테넌트 계정 페이지가 나타나고 모든 기존 테넌트 계정이 나열됩니다.

### Tenant Accounts

View information for each tenant account.

**Note:** 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 and select **View Details**.

	Display Name  	Space Used  	Quota Utilization  	Quota  	Object Count  	Sign in 
<input checked="" type="radio"/>	Account01	500.00 KB	0.00%	20.00 GB	100	
<input type="radio"/>	Account02	2.50 MB	0.01%	30.00 GB	500	
<input type="radio"/>	Account03	605.00 MB	4.03%	15.00 GB	31,000	
<input type="radio"/>	Account04	1.00 GB	10.00%	10.00 GB	200,000	
<input type="radio"/>	Account05	0 bytes	—	Unlimited	0	

Show  rows per page

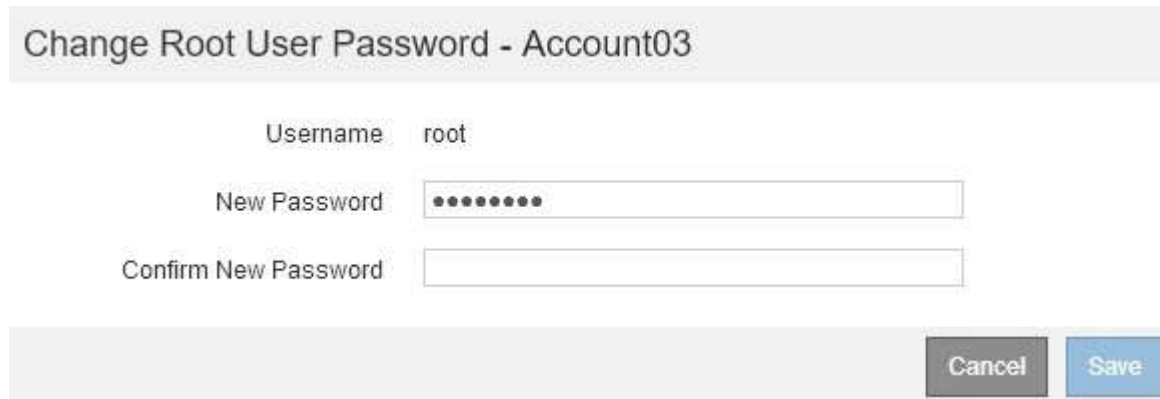
2. 편집할 테넌트 계정을 선택합니다.



시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 검색 상자를 사용하여 표시 이름 또는 테넌트 ID로 테넌트 계정을 검색합니다.

세부 정보 보기, 편집 및 작업 단추가 활성화됩니다.

3. Actions \* 드롭다운에서 \* Change Root Password \* 를 선택합니다.



Change Root User Password - Account03

Username root

New Password ●●●●●●

Confirm New Password

Cancel Save

4. 테넌트 계정의 새 암호를 입력합니다.

5. 저장 \* 을 선택합니다.

관련 정보

["StorageGRID에 대한 관리자 액세스 제어"](#)

## 테넌트 계정 편집

테넌트 계정을 편집하여 표시 이름을 변경하거나, ID 소스 설정을 변경하거나, 플랫폼 서비스를 허용 또는 금지하거나, 스토리지 할당량을 입력할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

단계

















1. Tenants \* 를 선택합니다.

테넌트 계정 페이지가 나타나고 모든 기존 테넌트 계정이 나열됩니다.

## Tenant Accounts

View information for each tenant account.

**Note:** 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 and select **View Details**.

	Display Name  	Space Used  	Quota Utilization  	Quota  	Object Count  	Sign in 
<input checked="" type="radio"/>	Account01	500.00 KB	0.00%	20.00 GB	100	
<input type="radio"/>	Account02	2.50 MB	0.01%	30.00 GB	500	
<input type="radio"/>	Account03	605.00 MB	4.03%	15.00 GB	31,000	
<input type="radio"/>	Account04	1.00 GB	10.00%	10.00 GB	200,000	
<input type="radio"/>	Account05	0 bytes	—	Unlimited	0	

Show  rows per page

2. 편집할 테넌트 계정을 선택합니다.

시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 검색 상자를 사용하여 표시 이름 또는 테넌트 ID로 테넌트 계정을 검색합니다.

3. 편집 \* 을 선택합니다.

Edit Tenant Account 페이지가 나타납니다. 이 예제는 SSO(Single Sign-On)를 사용하지 않는 그리드에 대한 것입니다. 이 테넌트 계정은 자체 ID 소스를 구성하지 않았습니다.

### Edit Tenant Account

#### Tenant Details

Display Name

Allow Platform Services

Storage Quota (optional)

Uses Own Identity Source

4. 필요에 따라 필드의 값을 변경합니다.

a. 이 테넌트 계정의 표시 이름을 변경합니다.

b. 플랫폼 서비스 허용 \* 확인란의 설정을 변경하여 테넌트 계정에서 S3 버킷을 위한 플랫폼 서비스를 사용할 수 있는지 여부를 확인합니다.



이미 사용 중인 테넌트에 대해 플랫폼 서비스를 사용하지 않도록 설정하면 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.

- c. 스토리지 할당량 \* 의 경우 이 테넌트의 개체에 사용할 수 있는 최대 기가바이트, 테라바이트 또는 페타 바이트 수를 변경하거나, 이 테넌트에 무제한 할당량을 사용하려면 필드를 비워 둡니다.

테넌트의 스토리지 할당량은 물리적 크기(디스크 크기)가 아닌 논리적 양(오브젝트 크기)을 나타냅니다. ILM 복사본 및 삭제 코딩은 사용된 할당량에 영향을 주지 않습니다.



각 테넌트 계정의 스토리지 사용량을 모니터링하려면 \* Usage \* 를 선택합니다. 테넌트 계정은 테넌트 관리자의 대시보드 또는 테넌트 관리 API를 통해 자신의 사용량을 모니터링할 수도 있습니다. 노드가 그리드의 다른 노드로부터 격리되면 테넌트의 스토리지 사용량 값이 최신 상태가 아닐 수 있습니다. 네트워크 연결이 복원되면 합계가 업데이트됩니다.

- d. 사용자 지정 ID 소스 사용 \* 확인란의 설정을 변경하여 테넌트 계정에서 자체 ID 소스를 사용할지 또는 Grid Manager용으로 구성된 ID 소스를 사용할지 여부를 결정합니다.



고유 ID 소스 사용 \* 확인란이 다음과 같은 경우:

- 비활성화된 후 선택한 경우 테넌트는 이미 자체 ID 소스를 사용하도록 설정되어 있습니다. 테넌트는 그리드 관리자에 대해 구성된 ID 소스를 사용하기 전에 해당 ID 소스를 비활성화해야 합니다.
- 비활성화되고 선택 취소되며 StorageGRID 시스템에 대해 SSO가 활성화됩니다. 테넌트는 Grid Manager에 대해 구성된 ID 소스를 사용해야 합니다.

5. 저장 \* 을 선택합니다.

관련 정보

["S3 테넌트 계정에 대한 플랫폼 서비스 관리"](#)

["테넌트 계정을 사용합니다"](#)

## 테넌트 계정을 삭제하는 중입니다

테넌트의 시스템 액세스를 영구적으로 제거하려면 테넌트 계정을 삭제할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 테넌트 계정과 연결된 모든 버킷(S3), 컨테이너(Swift) 및 개체를 제거해야 합니다.

단계

1. Tenants \* 를 선택합니다.
2. 삭제할 테넌트 계정을 선택합니다.

시스템에 20개 이상의 항목이 포함된 경우 각 페이지에 한 번에 표시되는 행 수를 지정할 수 있습니다. 검색 상자를

사용하여 표시 이름 또는 테넌트 ID로 테넌트 계정을 검색합니다.

3. 작업 \* 드롭다운에서 \* 제거 \* 를 선택합니다.
4. OK \* 를 선택합니다.

관련 정보

["StorageGRID에 대한 관리자 액세스 제어"](#)

### S3 테넌트 계정에 대한 플랫폼 서비스 관리

S3 테넌트 계정에 대해 플랫폼 서비스를 설정하는 경우 테넌트가 이러한 서비스를 사용하는 데 필요한 외부 리소스에 액세스할 수 있도록 그리드를 구성해야 합니다.

- ["어떤 플랫폼 서비스인지 확인하십시오"](#)
- ["플랫폼 서비스를 위한 네트워킹 및 포트"](#)
- ["플랫폼 서비스 메시지를 사이트별로 전달"](#)
- ["플랫폼 서비스 문제 해결"](#)

어떤 플랫폼 서비스인지 확인하십시오

플랫폼 서비스에는 CloudMirror 복제, 이벤트 알림 및 검색 통합 서비스가 포함됩니다.

이러한 서비스를 통해 테넌트는 자신의 S3 버킷에서 다음 기능을 사용할 수 있습니다.

- \* CloudMirror 복제 \*: StorageGRID CloudMirror 복제 서비스는 StorageGRID 버킷에서 지정된 외부 대상으로 특정 객체를 미러링하는 데 사용됩니다.

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



소스 버킷에 S3 오브젝트 잠금이 설정된 경우 CloudMirror 복제가 지원되지 않습니다.

- \* 알림 \*: 버킷당 이벤트 알림은 지정된 외부 SNS(Amazon Simple Notification Service ™)에 객체에서 수행된 특정 작업에 대한 알림을 보내는 데 사용됩니다.

예를 들어, 버킷에 추가된 각 오브젝트에 대해 관리자에게 경고가 전송되도록 구성할 수 있습니다. 여기서 객체는 중요한 시스템 이벤트와 연결된 로그 파일을 나타냅니다.



S3 오브젝트 잠금이 활성화된 버킷에서 이벤트 알림을 구성할 수 있지만 오브젝트의 S3 오브젝트 잠금 메타데이터(마지막 보존 날짜 및 법적 보류 상태 포함)는 알림 메시지에 포함되지 않습니다.

- \* 검색 통합 서비스 \*: 검색 통합 서비스는 외부 서비스를 사용하여 메타데이터를 검색하거나 분석할 수 있는 지정된 Elasticsearch 인덱스에 S3 오브젝트 메타데이터를 전송하는 데 사용됩니다.

예를 들어, S3 오브젝트 메타데이터를 원격 Elasticsearch 서비스로 전송하도록 버킷을 구성할 수 있습니다. 그런 다음 Elasticsearch를 사용하여 버킷에 대한 검색을 수행하고 객체 메타데이터에 있는 패턴에 대한 정교한 분석을 수행할 수 있습니다.



S3 오브젝트 잠금이 활성화된 버킷에서 Elasticsearch 통합을 구성할 수 있지만 오브젝트의 S3 오브젝트 잠금 메타데이터(보존 기한 및 법적 보류 상태 포함)는 알림 메시지에 포함되지 않습니다.

플랫폼 서비스를 통해 테넌트는 외부 스토리지 리소스, 알림 서비스 및 데이터에 대한 검색 또는 분석 서비스를 사용할 수 있습니다. 플랫폼 서비스의 대상 위치는 일반적으로 StorageGRID 배포 외부에 있으므로 테넌트가 이러한 서비스를 사용하도록 허용할지 여부를 결정해야 합니다. 이 경우 테넌트 계정을 만들거나 편집할 때 플랫폼 서비스 사용을 활성화해야 합니다. 또한 테넌트가 생성하는 플랫폼 서비스 메시지가 대상에 도달할 수 있도록 네트워크를 구성해야 합니다.

플랫폼 서비스 사용을 위한 권장 사항

플랫폼 서비스를 사용하기 전에 다음 권장 사항을 숙지해야 합니다.

- 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.
- 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.

관련 정보

["테넌트 계정을 사용합니다"](#)

["스토리지 프록시 설정을 구성하는 중입니다"](#)

["모니터링 및 문제 해결"](#)

플랫폼 서비스를 위한 네트워킹 및 포트

S3 테넌트가 플랫폼 서비스를 사용할 수 있도록 허용하는 경우 플랫폼 서비스 메시지가 대상으로 전달될 수 있도록 그리드에 대한 네트워킹을 구성해야 합니다.

테넌트 계정을 생성하거나 업데이트할 때 S3 테넌트 계정에 대해 플랫폼 서비스를 활성화할 수 있습니다. 플랫폼 서비스가 설정된 경우 테넌트는 CloudMirror 복제, 이벤트 알림 또는 S3 버킷에서 통합 메시지를 검색할 대상으로 사용되는 엔드포인트를 생성할 수 있습니다. 이러한 플랫폼 서비스 메시지는 ADC 서비스를 실행하는 스토리지 노드에서 대상 끝점으로 전송됩니다.

예를 들어, 테넌트는 다음과 같은 유형의 대상 엔드포인트를 구성할 수 있습니다.

- 로컬로 호스팅되는 Elasticsearch 클러스터입니다
- SNS(Simple Notification Service) 메시지 수신을 지원하는 로컬 애플리케이션입니다
- StorageGRID의 동일한 인스턴스 또는 다른 인스턴스에서 로컬로 호스팅되는 S3 버킷
- Amazon Web Services의 엔드포인트와 같은 외부 엔드포인트입니다.

플랫폼 서비스 메시지가 전달될 수 있도록 ADC 스토리지 노드가 포함된 네트워크를 구성해야 합니다. 다음 포트를 사용하여 플랫폼 서비스 메시지를 대상 끝점에 보낼 수 있는지 확인해야 합니다.

기본적으로 플랫폼 서비스 메시지는 다음 포트로 전송됩니다.

- \* 80 \*: http로 시작하는 끝점 URI입니다

- \* 443 \*: https로 시작하는 끝점 URI의 경우

테넌트는 끝점을 만들거나 편집할 때 다른 포트를 지정할 수 있습니다.



StorageGRID 배포를 CloudMirror 복제의 대상으로 사용하는 경우 80 또는 443 이외의 포트에서 복제 메시지를 받을 수 있습니다. 대상 StorageGRID 배포에서 S3에 사용 중인 포트가 끝점에 지정되었는지 확인합니다.

투명하지 않은 프록시 서버를 사용하는 경우에는 인터넷 끝점과 같은 외부 끝점으로 메시지를 보낼 수 있도록 스토리지 프록시 설정도 구성해야 합니다.

관련 정보

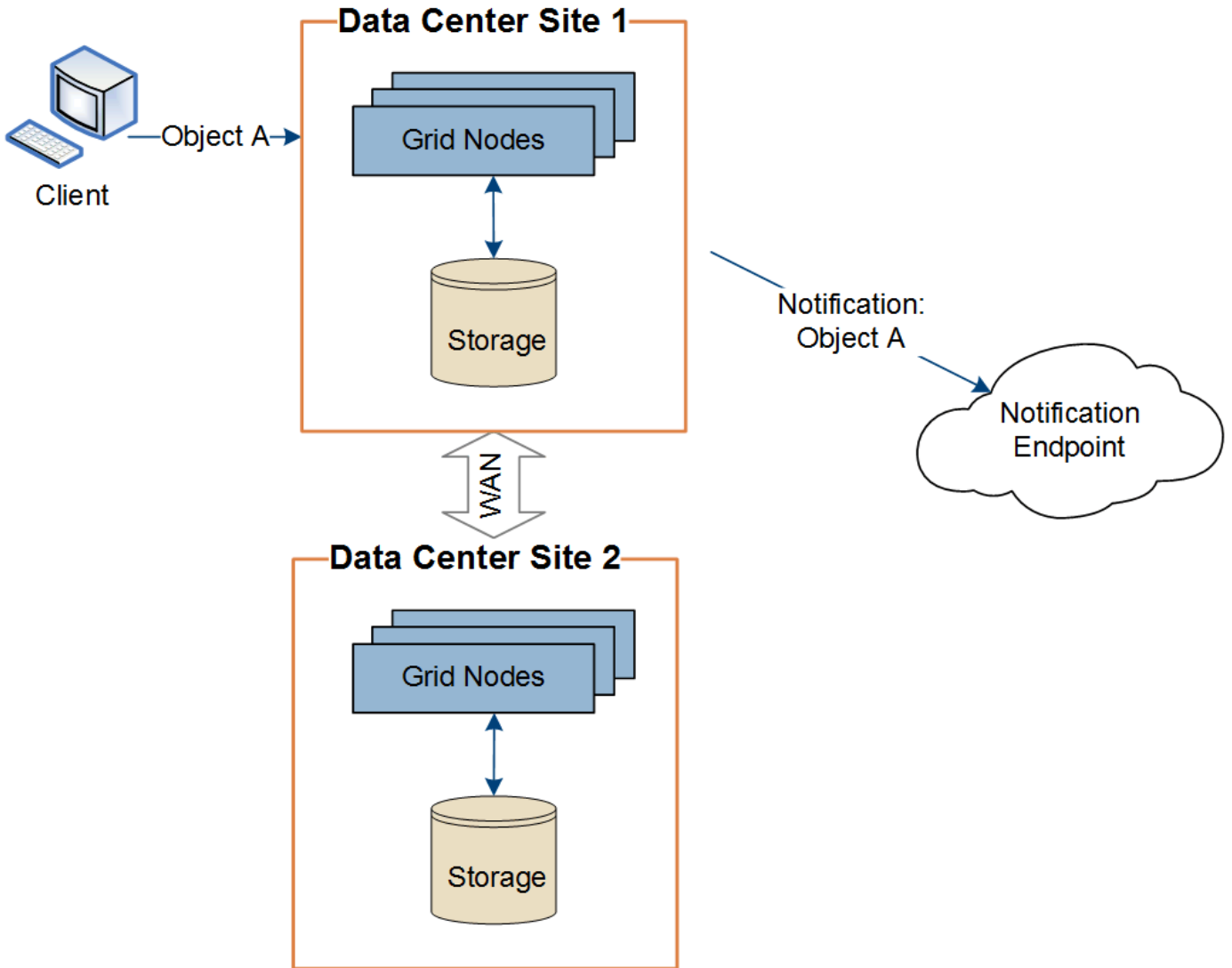
["스토리지 프록시 설정을 구성하는 중입니다"](#)

["테넌트 계정을 사용합니다"](#)

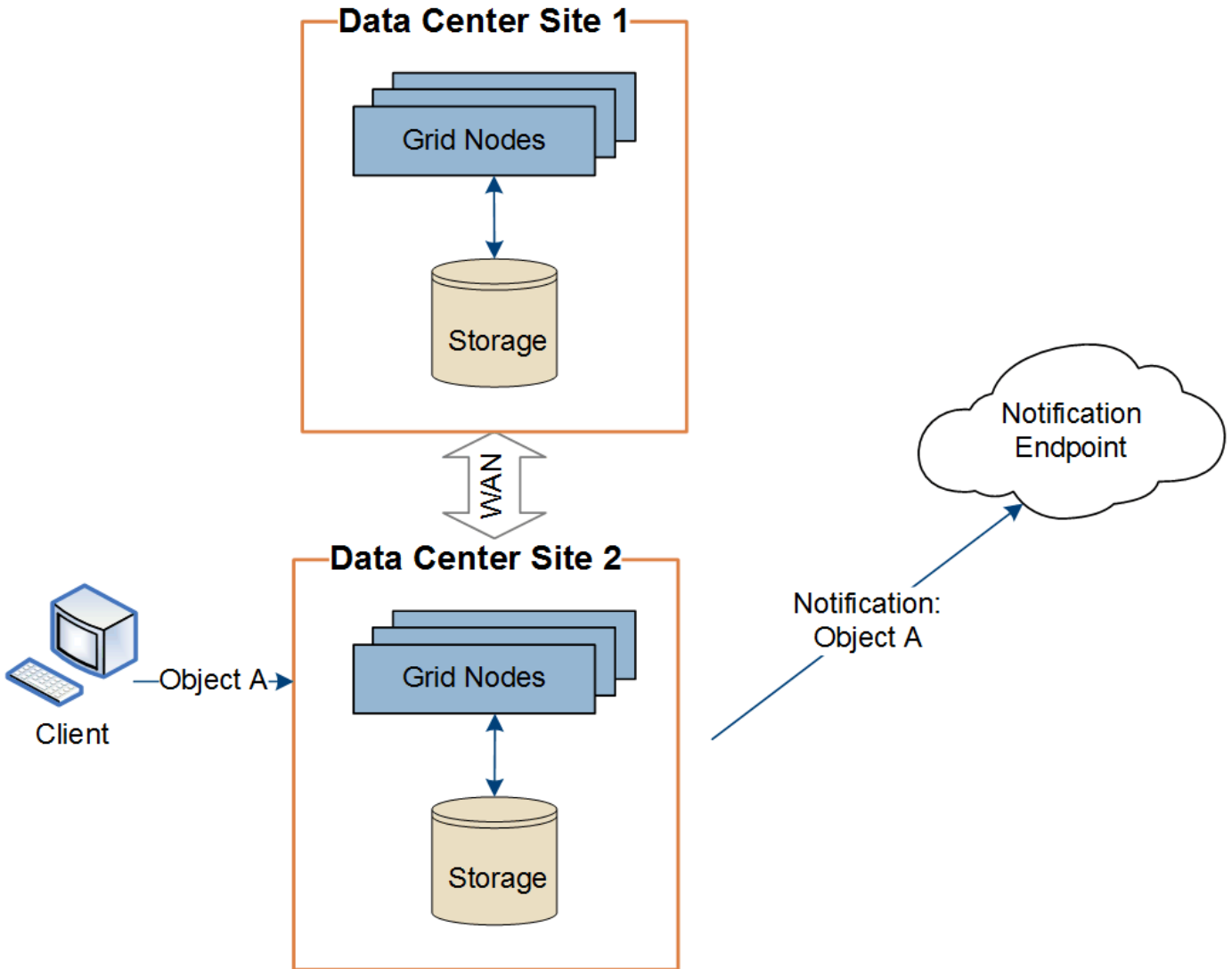
플랫폼 서비스 메시지를 사이트별로 전달

모든 플랫폼 서비스 작업은 사이트별로 수행됩니다.

즉, 테넌트가 클라이언트를 사용하여 데이터 센터 사이트 1의 게이트웨이 노드에 연결하여 오브젝트에 대해 S3 API 생성 작업을 수행하는 경우 해당 작업에 대한 알림이 트리거되고 데이터 센터 사이트 1에서 전송됩니다.



이후에 클라이언트가 데이터 센터 사이트 2에서 동일한 개체에 대해 S3 API 삭제 작업을 수행하면 삭제 작업에 대한 알림이 트리거되어 데이터 센터 사이트 2에서 전송됩니다.



각 사이트의 네트워킹이 플랫폼 서비스 메시지를 해당 대상에 전달할 수 있도록 구성되어 있는지 확인합니다.

#### 플랫폼 서비스 문제 해결

플랫폼 서비스에 사용되는 엔드포인트는 테넌트 관리자의 테넌트 사용자가 생성 및 유지 관리합니다. 그러나 테넌트에 플랫폼 서비스를 구성하거나 사용하는 데 문제가 있는 경우 Grid Manager를 사용하여 문제를 해결할 수 있습니다.

#### 새 끝점에 문제가 있습니다

테넌트가 플랫폼 서비스를 사용하려면 먼저 테넌트 관리자를 사용하여 하나 이상의 엔드포인트를 생성해야 합니다. 각 엔드포인트는 StorageGRID S3 버킷, Amazon 웹 서비스 버킷, 간단한 알림 서비스 주제 또는 로컬 또는 AWS에서 호스팅되는 Elasticsearch 클러스터와 같은 단일 플랫폼 서비스의 외부 대상을 나타냅니다. 각 끝점에는 외부 리소스의 위치와 해당 리소스에 액세스하는 데 필요한 자격 증명이 모두 포함됩니다.

테넌트가 끝점을 만들 때 StorageGRID 시스템은 끝점이 있는지, 그리고 지정된 자격 증명을 사용하여 해당 끝점에 도달할 수 있는지 검증합니다. 엔드포인트에 대한 연결은 각 사이트의 한 노드에서 검증됩니다.

끝점 유효성 검사에 실패하면 끝점 유효성 검사가 실패한 이유를 설명하는 오류 메시지가 표시됩니다. 테넌트 사용자가 문제를 해결한 다음 엔드포인트를 다시 생성해 보십시오.





테넌트 계정에 대해 플랫폼 서비스가 활성화되어 있지 않으면 엔드포인트 생성이 실패합니다.

기존 엔드포인트에 문제가 있습니다

StorageGRID가 기존 엔드포인트에 도달하려고 할 때 오류가 발생하면 테넌트 관리자의 대시보드에 메시지가 표시됩니다.

One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

테넌트 사용자는 끝점 페이지로 이동하여 각 끝점에 대한 가장 최근의 오류 메시지를 검토하고 오류가 발생한 시간을 확인할 수 있습니다. 마지막 오류 \* 열은 각 끝점에 대한 가장 최근 오류 메시지를 표시하고 오류가 발생한 시간을 나타냅니다. \*에 포함된 오류 지난 7일 내에 아이콘이 발생했습니다.

## 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 bycast.log의 오류에 대한 자세한 정보를 찾을 수 있습니다.

프록시 서버와 관련된 문제

스토리지 노드와 플랫폼 서비스 엔드포인트 간에 스토리지 프록시를 구성한 경우 프록시 서비스에서 StorageGRID의 메시지를 허용하지 않으면 오류가 발생할 수 있습니다. 이러한 문제를 해결하려면 프록시 서버의 설정을 확인하여 플랫폼 서비스 관련 메시지가 차단되지 않았는지 확인합니다.

오류가 발생했는지 확인합니다

지난 7일 이내에 엔드포인트 오류가 발생한 경우 테넌트 관리자의 대시보드에 경고 메시지가 표시됩니다. 끝점 페이지로 이동하여 오류에 대한 자세한 정보를 볼 수 있습니다.

클라이언트 작업이 실패했습니다

일부 플랫폼 서비스 문제로 인해 S3 버킷의 클라이언트 작업이 실패할 수 있습니다. 예를 들어 RSM(Internal Replicated State Machine) 서비스가 중지되거나 너무 많은 플랫폼 서비스 메시지가 배달 대기 중인 경우 S3 클라이언트 작업이 실패합니다.

서비스 상태를 확인하려면

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. site\_ \* > \*Storage Node \* > \* SSM \* > \* Services \* 를 선택합니다.

복구할 수 없는 끝점 오류입니다

엔드포인트가 생성된 후 다양한 이유로 플랫폼 서비스 요청 오류가 발생할 수 있습니다. 일부 오류는 사용자 개입으로 복구할 수 있습니다. 예를 들어 다음과 같은 이유로 복구 가능한 오류가 발생할 수 있습니다.

- 사용자의 자격 증명이 삭제되었거나 만료되었습니다.
- 대상 버킷이 없습니다.
- 알림을 전달할 수 없습니다.

StorageGRID에서 복구 가능한 오류가 발생하면 성공할 때까지 플랫폼 서비스 요청이 재시도됩니다.

다른 오류는 복구할 수 없습니다. 예를 들어, 끝점이 삭제되면 복구할 수 없는 오류가 발생합니다.

StorageGRID에서 복구할 수 없는 끝점 오류가 발생하면 그리드 관리자에서 SMTT(Total Events) 경보가 트리거됩니다. Total Events(총 이벤트) 알람을 보려면

1. 노드 \* 를 선택합니다.
2. site\_ \* > \*GRID node \* > \* Events \* 를 선택합니다.
3. 테이블 상단의 마지막 이벤트 보기

이벤트 메시지는 에도 나열됩니다 `/var/local/log/bycast-err.log`.

4. SMTT 알람 내용물에 제공된 지침을 따라 문제를 해결하십시오.
5. Reset event counts \* 를 클릭합니다.
6. 플랫폼 서비스 메시지가 전달되지 않은 객체를 테넌트에 알립니다.
7. 테넌트에게 객체의 메타데이터 또는 태그를 업데이트하여 실패한 복제 또는 알림을 다시 트리거하도록 지시합니다.

테넌트는 불필요한 변경을 방지하기 위해 기존 값을 다시 제출할 수 있습니다.

플랫폼 서비스 메시지를 전달할 수 없습니다

대상에 플랫폼 서비스 메시지를 수락하지 못하는 문제가 발생하면 버킷에 대한 클라이언트 작업은 성공하지만 플랫폼

서비스 메시지는 전달되지 않습니다. 예를 들어, StorageGRID가 더 이상 대상 서비스에 인증할 수 없도록 대상에서 자격 증명이 업데이트되는 경우 이 오류가 발생할 수 있습니다.

복구할 수 없는 오류로 인해 플랫폼 서비스 메시지를 전달할 수 없는 경우 그리드 관리자에서 SMTT(Total Events) 경보가 트리거됩니다.

플랫폼 서비스 요청에 대한 성능 저하

요청이 전송되는 속도가 대상 엔드포인트에서 요청을 수신할 수 있는 속도를 초과하는 경우 StorageGRID 소프트웨어는 버킷에 대한 수신 S3 요청을 스로틀할 수 있습니다. 임계치 조절은 대상 끝점으로 보내려고 기다리는 요청의 백로그가 있는 경우에만 발생합니다.

단, 들어오는 S3 요청의 실행 시간이 더 오래 걸린다는 점을 알 수 있습니다. 속도가 현저히 느린 성능을 감지하기 시작하는 경우 수집 속도를 줄이거나 용량이 더 큰 엔드포인트를 사용해야 합니다. 요청 백로그가 계속 증가하는 경우 PUT 요청과 같은 클라이언트 S3 작업이 결국 실패합니다.

CloudMirror 요청은 일반적으로 검색 통합 또는 이벤트 알림 요청보다 더 많은 데이터 전송을 포함하므로 대상 엔드포인트의 성능에 영향을 받을 가능성이 더 높습니다.

플랫폼 서비스 요청에 실패했습니다

플랫폼 서비스에 대한 요청 실패율을 보려면

1. 노드 \* 를 선택합니다.
2. `_site * > * 플랫폼 서비스 *` 를 선택합니다.
3. 요청 실패율 차트를 봅니다.

## Data Center 1



플랫폼 서비스를 사용할 수 없음 경고

플랫폼 서비스 사용 불가 \* 경고는 RSM 서비스가 실행 중이거나 사용 가능한 스토리지 노드가 너무 적어서 사이트에서 플랫폼 서비스 작업을 수행할 수 없음을 나타냅니다.

RSM 서비스는 플랫폼 서비스 요청이 각 끝점으로 전송되도록 합니다.

이 경고를 해결하려면 사이트에서 RSM 서비스를 포함하는 스토리지 노드를 확인합니다. (RSM 서비스는 ADC 서비스도 포함하는 스토리지 노드에 있습니다.) 그런 다음 이러한 스토리지 노드 중 대부분이 실행 중이고 사용 가능한지 확인합니다.



사이트에서 RSM 서비스를 포함하는 스토리지 노드가 두 개 이상 장애가 발생하면 해당 사이트에 대한 보류 중인 플랫폼 서비스 요청이 손실됩니다.

플랫폼 서비스 끝점에 대한 추가 문제 해결 지침

플랫폼 서비스 엔드포인트 문제 해결에 대한 자세한 내용은 테넌트 계정 사용 지침을 참조하십시오.

["테넌트 계정을 사용합니다"](#)

관련 정보

["모니터링 및 문제 해결"](#)

["스토리지 프록시 설정을 구성하는 중입니다"](#)

## S3 및 Swift 클라이언트 연결 구성

그리드 관리자는 S3 및 Swift 테넌트가 클라이언트 애플리케이션을 StorageGRID 시스템에 연결하여 데이터를 저장 및 검색하는 방법을 제어하는 구성 옵션을 관리합니다. 다양한 클라이언트 및 테넌트 요구 사항을 충족하는 여러 가지 옵션이 있습니다.

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

- 관리 노드 또는 게이트웨이 노드의 부하 분산 서비스 또는 선택적으로 관리 노드 또는 게이트웨이 노드의 고가용성(HA) 그룹의 가상 IP 주소입니다
- 게이트웨이 노드의 CLB 서비스 또는 게이트웨이 노드의 고가용성 그룹의 가상 IP 주소(선택 사항)입니다



CLB 서비스는 더 이상 사용되지 않습니다. StorageGRID 11.3 릴리스 전에 구성된 클라이언트는 게이트웨이 노드에서 CLB 서비스를 계속 사용할 수 있습니다. 로드 밸런싱을 제공하기 위해 StorageGRID에 의존하는 다른 모든 클라이언트 애플리케이션은 로드 밸런서 서비스를 사용하여 연결해야 합니다.

- 외부 로드 밸런서가 있거나 없는 스토리지 노드

StorageGRID 시스템에서 다음 기능을 선택적으로 구성할 수 있습니다.

- **\* 로드 밸런서 서비스 \***: 클라이언트가 클라이언트 연결을 위한 로드 밸런서 끝점을 만들어 로드 밸런서 서비스를 사용할 수 있도록 합니다. 로드 밸런서 끝점을 만들 때 끝점에서 HTTP 또는 HTTPS 연결을 허용하는지 여부, 끝점을 사용할 클라이언트 유형(S3 또는 Swift) 및 HTTPS 연결에 사용할 인증서(해당하는 경우)를 포트 번호로 지정합니다.
- **\* 신뢰할 수 없는 클라이언트 네트워크 \***: 클라이언트 네트워크를 신뢰할 수 없음으로 구성하여 보안을 강화할 수 있습니다. 클라이언트 네트워크를 신뢰할 수 없는 경우 클라이언트는 로드 밸런서 끝점만 사용하여 연결할 수 있습니다.
- **\* 고가용성 그룹 \***: 게이트웨이 노드 또는 관리 노드의 HA 그룹을 생성하여 액티브 백업 구성을 생성하거나 라운드 로빈 DNS 또는 타사 로드 밸런서 및 여러 HA 그룹을 사용하여 액티브-액티브 구성을 수행할 수 있습니다. HA 그룹의 가상 IP 주소를 사용하여 클라이언트 연결이 이루어집니다.

또한 StorageGRID에 직접 연결하는 클라이언트나 CLB 서비스(사용되지 않음)를 사용하는 클라이언트에 대해 HTTP를 사용하도록 설정할 수 있으며 S3 클라이언트에 대해 S3 API 엔드포인트 도메인 이름을 구성할 수 있습니다.

**요약: 클라이언트 연결을 위한 IP 주소 및 포트**

클라이언트 애플리케이션은 그리드 노드의 IP 주소와 해당 노드에 있는 서비스의 포트 번호를 사용하여 StorageGRID에 연결할 수 있습니다. HA(고가용성) 그룹이 구성되어 있는 경우 클라이언트 애플리케이션은 HA 그룹의 가상 IP 주소를 사용하여 연결할 수 있습니다.

이 작업에 대해

이 표에는 클라이언트가 StorageGRID에 연결할 수 있는 다양한 방법과 각 연결 유형에 사용되는 IP 주소 및 포트가 요약되어 있습니다. 이 지침은 로드 밸런서 끝점과 HA(고가용성) 그룹이 이미 구성되어 있는 경우 그리드 관리자에서 이 정보를 찾는 방법을 설명합니다.

연결 위치	클라이언트가 연결하는 서비스입니다	IP 주소입니다	포트
HA 그룹	로드 밸런서	HA 그룹의 가상 IP 주소입니다	<ul style="list-style-type: none"> <li>로드 밸런서 엔드포인트 포트</li> </ul>
HA 그룹	CLB <ul style="list-style-type: none"> <li>참고: * CLB 서비스는 더 이상 사용되지 않습니다.</li> </ul>	HA 그룹의 가상 IP 주소입니다	기본 S3 포트: <ul style="list-style-type: none"> <li>HTTPS: 8082</li> <li>HTTP: 8084</li> </ul> 기본 Swift 포트: <ul style="list-style-type: none"> <li>HTTPS: 8083</li> <li>HTTP: 8085</li> </ul>
관리자 노드	로드 밸런서	관리 노드의 IP 주소입니다	<ul style="list-style-type: none"> <li>로드 밸런서 엔드포인트 포트</li> </ul>
게이트웨이 노드	로드 밸런서	게이트웨이 노드의 IP 주소입니다	<ul style="list-style-type: none"> <li>로드 밸런서 엔드포인트 포트</li> </ul>
게이트웨이 노드	CLB <ul style="list-style-type: none"> <li>참고: * CLB 서비스는 더 이상 사용되지 않습니다.</li> </ul>	게이트웨이 노드의 IP 주소입니다 <ul style="list-style-type: none"> <li>참고: * 기본적으로 CLB 및 LDR용 HTTP 포트는 사용되지 않습니다.</li> </ul>	기본 S3 포트: <ul style="list-style-type: none"> <li>HTTPS: 8082</li> <li>HTTP: 8084</li> </ul> 기본 Swift 포트: <ul style="list-style-type: none"> <li>HTTPS: 8083</li> <li>HTTP: 8085</li> </ul>

연결 위치	클라이언트가 연결하는 서비스입니다	IP 주소입니다	포트
스토리지 노드	LDR	스토리지 노드의 IP 주소입니다	기본 S3 포트: <ul style="list-style-type: none"> <li>• HTTPS: 18082</li> <li>• HTTP: 18084</li> </ul> 기본 Swift 포트: <ul style="list-style-type: none"> <li>• HTTPS: 18083</li> <li>• HTTP: 18085</li> </ul>

예

S3 클라이언트를 게이트웨이 노드 HA 그룹의 로드 밸런서 끝점에 연결하려면 아래와 같이 구조화된 URL을 사용합니다.

- `https://VIP-of-HA-group:LB-endpoint-port`

예를 들어 HA 그룹의 가상 IP 주소가 192.0.2.5이고 S3 로드 밸런서 끝점의 포트 번호가 10443인 경우 S3 클라이언트는 다음 URL을 사용하여 StorageGRID에 연결할 수 있습니다.

- `https://192.0.2.5:10443`

Swift 클라이언트를 게이트웨이 노드 HA 그룹의 로드 밸런서 끝점에 연결하려면 아래와 같이 구조화된 URL을 사용합니다.

- `https://VIP-of-HA-group:LB-endpoint-port`

예를 들어 HA 그룹의 가상 IP 주소가 192.0.2.6이고 Swift 로드 밸런서 끝점의 포트 번호가 10444인 경우 Swift 클라이언트는 다음 URL을 사용하여 StorageGRID에 연결할 수 있습니다.

- `https://192.0.2.6:10444`

클라이언트가 StorageGRID에 연결하는 데 사용하는 IP 주소에 대한 DNS 이름을 구성할 수 있습니다. 로컬 네트워크 관리자에게 문의하십시오.

단계

1. 지원되는 브라우저를 사용하여 Grid Manager에 로그인합니다.
2. 그리드 노드의 IP 주소를 찾으려면
  - a. 노드 \* 를 선택합니다.
  - b. 연결할 관리 노드, 게이트웨이 노드 또는 스토리지 노드를 선택합니다.
  - c. 개요 \* 탭을 선택합니다.
  - d. 노드 정보 섹션에서 노드의 IP 주소를 확인합니다.
  - e. IPv6 주소 및 인터페이스 매핑을 보려면 \* 더 보기 \* 를 클릭합니다.

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.

- 구성 \* > \* 네트워크 설정 \* > \* 고가용성 그룹 \* 을 선택합니다.
- 표에서 HA 그룹의 가상 IP 주소를 확인합니다.

4. 로드 밸런서 끝점의 포트 번호를 찾으려면 다음을 수행합니다.

- 구성 \* > \* 네트워크 설정 \* > \* 로드 밸런서 엔드포인트 \* 를 선택합니다.

로드 밸런서 끝점 페이지가 나타나고 이미 구성된 끝점 목록이 표시됩니다.

- 끝점을 선택하고 \* 끝점 편집 \* 을 클릭합니다.

끝점 편집 창이 열리고 끝점에 대한 추가 세부 정보가 표시됩니다.

- 선택한 끝점이 올바른 프로토콜(S3 또는 Swift)과 함께 사용하도록 구성되었는지 확인한 후 \* Cancel \* (취소 \*)을 클릭합니다.
- 클라이언트 연결에 사용할 끝점의 포트 번호를 확인합니다.



포트 번호가 80 또는 443이면 해당 포트가 관리 노드에 예약되므로 끝점이 게이트웨이 노드에서만 구성됩니다. 다른 모든 포트는 게이트웨이 노드와 관리 노드 모두에서 구성됩니다.

## 로드 밸런싱 관리

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

다음과 같은 방법으로 StorageGRID 시스템에서 로드 밸런싱을 수행할 수 있습니다.

- 관리 노드 및 게이트웨이 노드에 설치된 로드 밸런서 서비스를 사용합니다. 로드 밸런서 서비스는 계층 7 로드 밸런싱을 제공하고 클라이언트 요청에 대한 TLS 종료를 수행하고 요청을 검사하며 스토리지 노드에 대한 새로운 보안 연결을 설정합니다. 이것은 권장되는 로드 밸런싱 메커니즘입니다.
- 게이트웨이 노드에만 설치된 CLB(연결 로드 밸런서) 서비스를 사용합니다. CLB 서비스는 계층 4 로드 밸런싱을 제공하고 링크 비용을 지원합니다.



CLB 서비스는 더 이상 사용되지 않습니다.

- 타사 로드 밸런서를 통합합니다. 자세한 내용은 NetApp 어카운트 담당자에게 문의하십시오.



## 로드 밸런싱 작동 방식 - 로드 밸런서 서비스

로드 밸런서 서비스는 들어오는 네트워크 연결을 클라이언트 애플리케이션에서 스토리지 노드로 배포합니다. 로드 밸런싱을 사용하려면 Grid Manager를 사용하여 부하 분산 엔드포인트를 구성해야 합니다.

이러한 노드 유형에는 로드 밸런서 서비스가 포함되어 있으므로 관리 노드 또는 게이트웨이 노드에 대해서만 로드 밸런서 끝점을 구성할 수 있습니다. 스토리지 노드 또는 아카이브 노드의 끝점은 구성할 수 없습니다.

각 로드 밸런서 끝점은 포트, 프로토콜(HTTP 또는 HTTPS), 서비스 유형(S3 또는 Swift) 및 바인딩 모드를 지정합니다. HTTPS 엔드포인트에는 서버 인증서가 필요합니다. 바인딩 모드를 사용하면 엔드포인트 포트의 액세스를 다음과 같이 제한할 수 있습니다.

- 특정 HA(고가용성) 가상 IP 주소(VIP)
- 특정 노드의 특정 네트워크 인터페이스

### 포트 고려 사항

클라이언트는 로드 밸런서 서비스를 실행하는 노드에서 구성된 모든 끝점에 액세스할 수 있습니다. 단, 포트 80과 443은 관리 노드에 예약되므로 이러한 포트에 구성된 끝점은 게이트웨이 노드에서만 로드 밸런싱 작업을 지원합니다.

포트를 다시 매핑한 경우 동일한 포트를 사용하여 로드 밸런서 끝점을 구성할 수 없습니다. 다시 매핑된 포트를 사용하여 끝점을 만들 수 있지만 이러한 끝점은 로드 밸런서 서비스가 아닌 원래 CLB 포트 및 서비스에 다시 매핑됩니다. 포트 재매핑을 제거하기 위한 복구 및 유지 관리 지침의 단계를 따릅니다.



CLB 서비스는 더 이상 사용되지 않습니다.

### CPU 가용성

각 관리 노드와 게이트웨이 노드의 로드 밸런서 서비스는 S3 또는 Swift 트래픽을 스토리지 노드로 전달할 때 독립적으로 작동합니다. 로드 밸런서 서비스는 가중 프로세스를 통해 더 많은 요청을 CPU 가용성이 높은 스토리지 노드로 라우팅합니다. 노드 CPU 로드 정보는 몇 분마다 업데이트되지만 가중치는 더 자주 업데이트될 수 있습니다. 모든 스토리지 노드에는 최소 기본 가중치 값이 할당됩니다. 이는 노드에서 100% 사용률을 보고하거나 사용률을 보고하지 않는 경우에도 마찬가지입니다.

경우에 따라 CPU 가용성에 대한 정보는 로드 밸런서 서비스가 있는 사이트로 제한됩니다.

### 관련 정보

["유지 및 복구"](#)

### 부하 분산 장치 엔드포인트 구성

부하 분산 엔드포인트를 생성, 편집 및 제거할 수 있습니다.

### 로드 밸런서 끝점을 만듭니다

각 로드 밸런서 끝점은 포트, 네트워크 프로토콜(HTTP 또는 HTTPS) 및 서비스 유형(S3 또는 Swift)을 지정합니다. HTTPS 끝점을 만드는 경우 서버 인증서를 업로드하거나 생성해야 합니다.

### 필요한 것

- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 로드 밸런서 서비스에 사용할 포트를 이전에 다시 매핑한 경우 리맵을 제거해야 합니다.



포트를 다시 매핑한 경우 동일한 포트를 사용하여 로드 밸런서 끝점을 구성할 수 없습니다. 다시 매핑된 포트를 사용하여 끝점을 만들 수 있지만 이러한 끝점은 로드 밸런서 서비스가 아닌 원래 CLB 포트 및 서비스에 다시 매핑됩니다. 포트 재맵을 제거하기 위한 복구 및 유지 관리 지침의 단계를 따릅니다.



CLB 서비스는 더 이상 사용되지 않습니다.

## 단계

1. 구성 \* > \* 네트워크 설정 \* > \* 로드 밸런서 엔드포인트 \* 를 선택합니다.

부하 분산 엔드포인트 페이지가 나타납니다.

### Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

**i** Changes to endpoints can take up to 15 minutes to be applied to all nodes.

**+** Add endpoint port   **✎** Edit endpoint   **✕** Remove endpoint port

Display name	Port	Using HTTPS
<i>No endpoints configured.</i>		

2. 끝점 추가 \* 를 선택합니다.

끝점 만들기 대화 상자가 나타납니다.

### Create Endpoint

Display Name

Port

10443

Protocol

HTTP

HTTPS

Endpoint Binding Mode

Global

HA Group VIPs

Node Interfaces

Cancel

Save

3. 로드 밸런서 끝점 페이지의 목록에 표시될 끝점의 표시 이름을 입력합니다.
4. 포트 번호를 입력하거나 미리 채워진 포트 번호를 그대로 둡니다.

포트 번호 80 또는 443을 입력하면 엔드포인트는 게이트웨이 노드에서만 구성됩니다. 이러한 포트는 관리 노드에

예약되기 때문입니다.



다른 그리드 서비스에서 사용하는 포트는 허용되지 않습니다. 내부 및 외부 통신에 사용되는 포트 목록은 네트워킹 지침을 참조하십시오.

5. 이 끝점의 네트워크 프로토콜을 지정하려면 \* HTTP \* 또는 \* HTTPS \* 를 선택합니다.

6. 끝점 바인딩 모드를 선택합니다.

- \* 글로벌 \* (기본값): 엔드포인트는 지정된 포트 번호의 모든 게이트웨이 노드 및 관리 노드에서 액세스할 수 있습니다.

#### Create Endpoint

Display Name

Port

Protocol  HTTP  HTTPS

Endpoint Binding Mode  Global  HA Group VIPs  Node Interfaces

**i** This endpoint is currently bound globally. All nodes will use this endpoint unless an endpoint with an overriding binding mode exists for a specific port.

Cancel Save

- \* HA 그룹 VIP \*: 끝점은 선택한 HA 그룹에 대해 정의된 가상 IP 주소를 통해서만 액세스할 수 있습니다. 이 모드에서 정의된 엔드포인트는 해당 엔드포인트에서 정의된 HA 그룹이 서로 겹치지 않는 한 동일한 포트 번호를 재사용할 수 있습니다.

끝점을 표시할 가상 IP 주소가 있는 HA 그룹을 선택합니다.

#### Create Endpoint

Display Name

Port

Protocol  HTTP  HTTPS

Endpoint Binding Mode  Global  HA Group VIPs  Node Interfaces

Name	Description	Virtual IP Addresses	Interfaces
<input type="checkbox"/> Group1		192.168.5.163	CO-REF-DC1-ADM1:eth0 (preferred Master)
<input type="checkbox"/> Group2		47.47.5.162	CO-REF-DC1-ADM1:eth2 (preferred Master)

Displaying 2 HA groups.

**⚠** No HA groups selected. You must select one or more HA Groups; otherwise, this endpoint will act as a globally bound endpoint.

Cancel Save

- \* 노드 인터페이스 \*: 끝점은 지정된 노드와 네트워크 인터페이스에서만 액세스할 수 있습니다. 이 모드에서 정의된 끝점은 인터페이스가 서로 겹치지 않는 한 동일한 포트 번호를 다시 사용할 수 있습니다.

끝점을 표시할 노드 인터페이스를 선택합니다.

### Create Endpoint


Display Name

Port

Protocol  HTTP  HTTPS

Endpoint Binding Mode  Global  HA Group VIPs  Node Interfaces

Node	Interface
<input type="checkbox"/> CO-REF-DC1-ADM1	eth0
<input type="checkbox"/> CO-REF-DC1-ADM1	eth1
<input type="checkbox"/> CO-REF-DC1-ADM1	eth2
<input type="checkbox"/> CO-REF-DC1-GW1	eth0
<input type="checkbox"/> CO-REF-DC2-ADM1	eth0
<input type="checkbox"/> CO-REF-DC2-GW1	eth0

 No node interfaces selected. You must select one or more node interfaces; otherwise, this endpoint will act as a globally bound endpoint.

Cancel

Save

7. 저장 \* 을 선택합니다.

끝점 편집 대화 상자가 나타납니다.

8. S3 \* 또는 \* Swift \* 를 선택하여 이 끝점에서 지원하는 트래픽 유형을 지정합니다.

### Edit Endpoint Unsecured Port A (port 10449)

#### Endpoint Service Configuration

Endpoint service type  S3  Swift

9. HTTP \* 를 선택한 경우 \* Save \* 를 선택합니다.

보안되지 않은 끝점이 만들어집니다. 부하 분산 끝점 페이지의 표에는 끝점의 표시 이름, 포트 번호, 프로토콜 및 끝점 ID가 나열됩니다.

10. HTTPS \* 를 선택하고 인증서를 업로드하려면 \* 인증서 업로드 \* 를 선택합니다.

## Load Certificate

Upload the PEM-encoded custom certificate, private key, and CA bundle files.

Server Certificate

Certificate Private Key

CA Bundle

Cancel

Save

- a. 서버 인증서와 인증서 개인 키를 찾습니다.

S3 클라이언트가 S3 API 엔드포인트 도메인 이름을 사용하여 연결할 수 있도록 하려면 클라이언트가 그리드에 연결하는 데 사용할 수 있는 모든 도메인 이름과 일치하는 다중 도메인 또는 와일드카드 인증서를 사용합니다. 예를 들어 서버 인증서에서 도메인 이름을 사용할 수 있습니다 \*.example.com.

### "S3 API 엔드포인트 도메인 이름 구성"

- a. 선택적으로 CA 번들을 찾습니다.
- b. 저장 \* 을 선택합니다.

끝점에 대한 PEM 인코딩된 인증서 데이터가 나타납니다.

11. HTTPS \* 를 선택하고 인증서를 생성하려면 \* 인증서 생성 \* 을 선택합니다.

## Generate Certificate

Domain 1  +

IP 1  +

Subject

Days valid

Cancel

Generate

- a. 도메인 이름 또는 IP 주소를 입력합니다.

와일드카드를 사용하여 로드 밸런서 서비스를 실행하는 모든 관리 노드 및 게이트웨이 노드의 정규화된 도메인 이름을 나타낼 수 있습니다. 예를 들면, 다음과 같습니다. \*.sgws.foo.com 와일드카드를 사용하여 나타냅니다 gn1.sgws.foo.com 및 gn2.sgws.foo.com.

## "S3 API 엔드포인트 도메인 이름 구성"

a. 를 선택합니다 + 다른 도메인 이름 또는 IP 주소를 추가합니다.

HA(고가용성) 그룹을 사용하는 경우 HA 가상 IP의 도메인 이름 및 IP 주소를 추가합니다.

b. 필요한 경우 인증서를 소유하는 사용자를 식별하기 위해 DN(고유 이름)이라고도 하는 X.509 제목을 입력합니다.

c. 원하는 경우 인증서가 유효한 일 수를 선택합니다. 기본값은 730일입니다.

d. Generate \* 를 선택합니다.

끝점에 대한 인증서 메타데이터 및 PEM 인코딩된 인증서 데이터가 나타납니다.

12. 저장 \* 을 클릭합니다.

끝점이 작성됩니다. 부하 분산 끝점 페이지의 표에는 끝점의 표시 이름, 포트 번호, 프로토콜 및 끝점 ID가 나열됩니다.

관련 정보

["유지 및 복구"](#)

["네트워크 지침"](#)

["고가용성 그룹 관리"](#)

["신뢰할 수 없는 클라이언트 네트워크 관리"](#)

로드 밸런서 끝점 편집

비보안(HTTP) 끝점의 경우 S3 및 Swift 간에 끝점 서비스 유형을 변경할 수 있습니다. 보안(HTTPS) 엔드포인트의 경우 엔드포인트 서비스 유형을 편집하고 보안 인증서를 보거나 변경할 수 있습니다.

필요한 것

- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

단계

1. 구성 \* > \* 네트워크 설정 \* > \* 로드 밸런서 엔드포인트 \* 를 선택합니다.

부하 분산 엔드포인트 페이지가 나타납니다. 기존 끝점이 테이블에 나열됩니다.

인증서가 곧 만료되는 끝점이 표에 나와 있습니다.

## Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

+ Add endpoint
✎ Edit endpoint
✕ Remove endpoint

	Display name	Port	Using HTTPS
<input type="radio"/>	Unsecured Endpoint 5	10444	No
<input checked="" type="radio"/>	Secured Endpoint 1	10443	Yes

Displaying 2 endpoints.

2. 편집할 끝점을 선택합니다.
3. 끝점 편집 \* 을 클릭합니다.

끝점 편집 대화 상자가 나타납니다.

비보안(HTTP) 끝점의 경우 대화 상자의 끝점 서비스 구성 섹션만 나타납니다. 보안(HTTPS) 끝점의 경우 다음 예제와 같이 대화 상자의 끝점 서비스 구성 및 인증서 섹션이 나타납니다.

### Endpoint Service Configuration

Endpoint service type  S3  Swift

### Certificates

Upload Certificate

Generate Certificate

Server **CA**

Certificate metadata

```

Subject DN: /C=CA/ST=British Columbia/O=NetApp, Inc./OU=SGQA/CN=*.mraymond-grid-a.sgqa.eng.netapp.com
Serial Number: 1C:FD:27:8B:E6:A5:BA:30:45:A9:16:4F:DC:77:3E:C6:80:7D:AF:E9
Issuer DN: /C=CA/ST=British Columbia/O=EqualSign, Inc./OU=IT/CN=EqualSign Issuing CA
Issued On: 2000-01-01T00:00:00.000Z
Expires On: 3000-01-01T00:00:00.000Z
SHA-1 Fingerprint: 60:3D:5A:8C:62:C5:B8:49:DC:9A:B3:F7:B9:0B:5B:0E:D2:A2:7E:C7
SHA-256 Fingerprint: AF:75:7F:44:C6:86:A4:84:B2:7D:11:DE:9F:49:D3:F6:2A:7E:D9:4D:2A:1B:8A:0B:B3:7E:23:0F:B3:CB:84:89
Alternative Names: DNS:*.mraymond-grid-a.sgqa.eng.netapp.com
DNS:*.99-140-dc1-g1.mraymond-grid-a.sgqa.eng.netapp.com
DNS:*.99-142-dc1-s1.mraymond-grid-a.sgqa.eng.netapp.com
    
```

Certificate PEM

```

-----BEGIN CERTIFICATE-----
MIIHfDCCBWSgAwIBAgIUHP0ni+alujBFqRZP3Hc+xoB9r+kwDQYJKoZIhvcNAQEL
BQAwbjELMAkGA1UEBhMCQ0ExGTAXBgNVBAgMEEJyaXRpc2ggQ29sdWliaWExGDAW
BgNVBAoMD0VxdWFeU2lnbiwgSW5jLjELMAkGA1UECwwCSVQxHTAbBgNVBAMMFVx
dWFeU2lnbiBjc3N1aW5nIENBMCAxDTAwMDEwMTAwMDAwMDAwMDAwMDAwMDAwMDAw
MDAwWjB+MQswCQYDVQQGEwJDQTEZMBcGA1UECAwQbnJpdG1zaCBDb2x1bWJpYTEV
MEMGA1UECgwMTmV0QXBwLW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50
LmlyYX1tb25kLWdyYWQtcYSS5zZ3FhLmVuzY5uZXRhcHAuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEaonUkwkFg/BlU1Y+bIR8OMaVJSC+R7Sfz102V
Hz4rSnrYCh/WURCT+fznmxzaGs2RRUDinNLnX1Yk+QUPAdIFZ+S1dr6HirYTF/NK
-----END CERTIFICATE-----
    
```

4. 끝점을 원하는 대로 변경합니다.

비보안(HTTP) 엔드포인트의 경우 다음을 수행할 수 있습니다.

- S3 및 Swift 간에 엔드포인트 서비스 유형을 변경합니다.

- 끝점 바인딩 모드를 변경합니다. 보안(HTTPS) 엔드포인트의 경우 다음을 수행할 수 있습니다.
- S3 및 Swift 간에 엔드포인트 서비스 유형을 변경합니다.
- 끝점 바인딩 모드를 변경합니다.
- 보안 인증서를 봅니다.
- 현재 인증서가 만료되거나 만료될 때 새 보안 인증서를 업로드하거나 생성합니다.

기본 StorageGRID 서버 인증서 또는 업로드된 CA 서명 인증서에 대한 자세한 정보를 표시하려면 탭을 선택합니다.



예를 들어, HTTP에서 HTTPS로 같은 기존 끝점의 프로토콜을 변경하려면 새 끝점을 만들어야 합니다. 로드 밸런서 끝점을 만들기 위한 지침에 따라 원하는 프로토콜을 선택합니다.

5. 저장 \* 을 클릭합니다.

관련 정보

[로드 밸런서 끝점을 만듭니다](#)

로드 밸런서 끝점을 제거하는 중입니다

로드 밸런서 끝점이 더 이상 필요하지 않으면 제거할 수 있습니다.

필요한 것

- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

단계

1. 구성 \* > \* 네트워크 설정 \* > \* 로드 밸런서 엔드포인트 \* 를 선택합니다.

부하 분산 엔드포인트 페이지가 나타납니다. 기존 끝점이 테이블에 나열됩니다.

### Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

<input type="button" value="+ Add endpoint"/> <input type="button" value="✎ Edit endpoint"/> <input type="button" value="✕ Remove endpoint"/>			
	Display name	Port	Using HTTPS
<input type="radio"/>	Unsecured Endpoint 5	10444	No
<input checked="" type="radio"/>	Secured Endpoint 1	10443	Yes

Displaying 2 endpoints.

2. 제거할 끝점 왼쪽에 있는 라디오 단추를 선택합니다.

3. 끝점 제거 \* 를 클릭합니다.

확인 대화 상자가 나타납니다.



## Warning

Remove Endpoint

Are you sure you want to remove endpoint 'Secured Endpoint 1'?

Cancel

OK

4. 확인 \* 을 클릭합니다.

끝점이 제거됩니다.

### 로드 균형 조정 작동 방식 - CLB 서비스

게이트웨이 노드의 CLB(연결 로드 밸런서) 서비스는 더 이상 사용되지 않습니다. 이제 로드 밸런서 서비스가 권장되는 로드 밸런싱 메커니즘입니다.

CLB 서비스는 Layer 4 로드 밸런싱을 사용하여 클라이언트 응용 프로그램에서 들어오는 TCP 네트워크 연결을 가용성, 시스템 로드 및 관리자 구성 링크 비용에 따라 최적의 스토리지 노드로 배포합니다. 최적의 스토리지 노드를 선택하면 CLB 서비스는 양방향 네트워크 연결을 설정하고 선택한 노드로 트래픽을 전달합니다. CLB는 들어오는 네트워크 연결을 연결할 때 그리드 네트워크 구성을 고려하지 않습니다.

CLB 서비스에 대한 정보를 보려면 \* 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택한 다음 \* CLB \* 와 그 아래 옵션을 선택할 수 있을 때까지 게이트웨이 노드를 확장합니다.

The screenshot shows the StorageGRID WebScale Deployment interface. On the left, the 'Grid Topology' view displays a tree structure of data centers and nodes. The 'Data Center 1' section is expanded, showing nodes like 'DC1-ADM1-98-160', 'DC1-G1-98-161', 'SSM', 'CLB', 'HTTP', 'Events', and 'Resources'. The 'DC1-G1-98-161' node is highlighted with a blue box. On the right, the 'Overview Summary - DC1-G1-98-161' page is displayed, showing a 'Storage Capacity' table with various metrics and their values.

Storage Capacity	
Storage Nodes Installed:	N/A
Storage Nodes Readable:	N/A
Storage Nodes Writable:	N/A
Installed Storage Capacity:	N/A
Used Storage Capacity:	N/A
Used Storage Capacity for Data:	N/A
Used Storage Capacity for Metadata:	N/A
Usable Storage Capacity:	N/A

CLB 서비스를 사용하도록 선택한 경우 StorageGRID 시스템에 대한 링크 비용을 구성하는 것이 좋습니다.

관련 정보

"링크 비용은 얼마입니까"

"링크 비용을 업데이트하는 중입니다"

## 신뢰할 수 없는 클라이언트 네트워크 관리

클라이언트 네트워크를 사용하는 경우 명시적으로 구성된 끝점에서만 인바운드 클라이언트 트래픽을 허용하여 악의적인 공격으로부터 StorageGRID를 보호할 수 있습니다.

기본적으로 각 그리드 노드의 클라이언트 네트워크는 `_trusted_`입니다. 즉, 기본적으로 StorageGRID는 사용 가능한 모든 외부 포트의 각 그리드 노드에 대한 인바운드 연결을 신뢰합니다(네트워크 지침의 외부 통신 정보 참조).

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.

### 예 1: 게이트웨이 노드는 HTTPS S3 요청만 허용합니다

게이트웨이 노드가 HTTPS S3 요청을 제외한 클라이언트 네트워크의 모든 인바운드 트래픽을 거부하도록 한다고 가정합니다. 다음과 같은 일반 단계를 수행합니다.

1. 로드 밸런서 엔드포인트 페이지에서 포트 443에서 HTTPS를 통해 S3에 대한 로드 밸런서 끝점을 구성합니다.
2. 신뢰할 수 없는 클라이언트 네트워크 페이지에서 게이트웨이 노드의 클라이언트 네트워크를 신뢰할 수 없도록 지정합니다.

구성을 저장한 후 게이트웨이 노드의 클라이언트 네트워크의 모든 인바운드 트래픽은 포트 443 및 ICMP 에코(ping) 요청의 HTTPS S3 요청을 제외하고 삭제됩니다.

### 예 2: 스토리지 노드가 S3 플랫폼 서비스 요청을 전송합니다

스토리지 노드에서 아웃바운드 S3 플랫폼 서비스 트래픽을 활성화하되 클라이언트 네트워크의 해당 스토리지 노드에 대한 인바운드 연결을 차단하려는 경우를 가정해 봅니다. 이 일반 단계를 수행합니다.

- 신뢰할 수 없는 클라이언트 네트워크 페이지에서 스토리지 노드의 클라이언트 네트워크를 신뢰할 수 없음을 나타냅니다.

구성을 저장한 후 스토리지 노드는 더 이상 클라이언트 네트워크에서 들어오는 트래픽을 허용하지 않지만 Amazon Web Services에 대한 아웃바운드 요청은 계속 허용합니다.

## 관련 정보

["네트워크 지침"](#)

["부하 분산 장치 엔드포인트 구성"](#)

노드의 클라이언트 네트워크를 지정하는 것은 신뢰할 수 없습니다

클라이언트 네트워크를 사용하는 경우 각 노드의 클라이언트 네트워크를 신뢰할 수 있는지 신뢰할 수 없는지 여부를 지정할 수 있습니다. 또한 확장에 추가된 새 노드의 기본 설정을 지정할 수도 있습니다.

## 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

- 관리자 노드 또는 게이트웨이 노드가 명시적으로 구성된 끝점에서만 인바운드 트래픽을 수락하도록 하려면 로드 밸런서 끝점을 정의해야 합니다.



로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

## 단계

1. 구성 \* \* 네트워크 설정 \* 신뢰할 수 없는 클라이언트 네트워크 \* 를 선택합니다.

신뢰할 수 없는 클라이언트 네트워크 페이지가 나타납니다.

이 페이지에는 StorageGRID 시스템의 모든 노드가 나열됩니다. 노드의 클라이언트 네트워크를 신뢰할 수 있어야 하는 경우 사용할 수 없는 이유 열에 항목이 포함됩니다.

### Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

#### Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network Default  Trusted  Untrusted

#### Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	

Client Network untrusted on 0 nodes.

Save

2. 새 노드 기본값 설정 \* 섹션에서 확장 절차에서 그리드에 새 노드를 추가할 때 기본 설정을 지정합니다.

- \* 신뢰 \*: 확장 시 노드가 추가되면 해당 클라이언트 네트워크를 신뢰할 수 있습니다.
- \* 신뢰할 수 없음 \*: 확장 시 노드가 추가되면 해당 클라이언트 네트워크를 신뢰할 수 없습니다. 필요에 따라 이 페이지로 돌아가 특정 새 노드의 설정을 변경할 수 있습니다.



이 설정은 StorageGRID 시스템의 기존 노드에는 영향을 주지 않습니다.

3. 신뢰할 수 없는 클라이언트 네트워크 노드 선택 \* 섹션에서 명시적으로 구성된 로드 밸런서 끝점에서만 클라이언트 연결을 허용할 노드를 선택합니다.

제목에서 확인란을 선택하거나 선택 취소하여 모든 노드를 선택하거나 선택 취소할 수 있습니다.

#### 4. 저장 \* 을 클릭합니다.

새 방화벽 규칙이 즉시 추가되고 적용됩니다. 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

관련 정보

["부하 분산 장치 엔드포인트 구성"](#)

## 고가용성 그룹 관리

고가용성(HA) 그룹을 사용하여 S3 및 Swift 클라이언트에 고가용성 데이터 연결을 제공할 수 있습니다. HA 그룹을 사용하여 Grid Manager 및 Tenant Manager에 대한 고가용성 연결을 제공할 수도 있습니다.

- ["HA 그룹이란"](#)
- ["HA 그룹 사용 방법"](#)
- ["HA 그룹에 대한 구성 옵션"](#)
- ["고가용성 그룹 생성"](#)
- ["고가용성 그룹 편집"](#)
- ["고가용성 그룹을 제거하는 중입니다"](#)

### HA 그룹이란

고가용성 그룹은 가상 IP 주소(VIP)를 사용하여 게이트웨이 노드 또는 관리 노드 서비스에 대한 액티브 백업 액세스를 제공합니다.

HA 그룹은 관리 노드 및 게이트웨이 노드에 있는 하나 이상의 네트워크 인터페이스로 구성됩니다. HA 그룹을 생성할 때 Grid Network(eth0) 또는 Client Network(eth2)에 속하는 네트워크 인터페이스를 선택합니다. HA 그룹의 모든 인터페이스는 동일한 네트워크 서브넷 내에 있어야 합니다.

HA 그룹은 그룹의 활성 인터페이스에 추가된 하나 이상의 가상 IP 주소를 유지합니다. 활성 인터페이스를 사용할 수 없게 되면 가상 IP 주소가 다른 인터페이스로 이동합니다. 이 장애 조치 프로세스는 일반적으로 몇 초 밖에 걸리지 않으며 클라이언트 응용 프로그램에 거의 영향을 주지 않고 정상적인 재시도 동작에 의존하여 작업을 계속할 수 있을 정도로 빠릅니다.

HA 그룹의 활성 인터페이스가 Master로 지정됩니다. 다른 모든 인터페이스는 백업으로 지정됩니다. 이러한 지정을 보려면 \* 노드 \* > \*노드 \* > \* 개요 \* 를 선택합니다.

Overview

Hardware

Network

Storage

Load Balancer

Events

Tasks

## Node Information ⓘ

Name	DC1-ADM1
Type	Admin Node
ID	711b7b9b-8d24-4d9f-877a-be3fa3ac27e8
Connection State	✔ Connected
Software Version	11.4.0 (build 20200515.2346.8edcbbf)
HA Groups	Fabric Pools, Master
IP Addresses	192.168.2.208, 10.224.2.208, 47.47.2.208, 47.47.4.219 <a href="#">Show more</a> ▼

HA 그룹을 생성할 때 기본 마스터가 될 인터페이스를 하나 지정합니다. 장애가 발생하여 VIP 주소가 백업 인터페이스에 재할당되지 않는 한 기본 마스터는 활성 인터페이스입니다. 장애가 해결되면 VIP 주소가 자동으로 기본 마스터로 다시 이동됩니다.

페일오버는 다음과 같은 이유로 트리거될 수 있습니다.

- 인터페이스가 구성된 노드가 다운됩니다.
- 인터페이스가 구성된 노드는 다른 모든 노드와의 연결이 2분 이상 끊어집니다
- 활성 인터페이스가 다운됩니다.
- 로드 밸런서 서비스가 중지됩니다.
- High Availability 서비스가 중지됩니다.



활성 인터페이스를 호스팅하는 노드 외부의 네트워크 장애로 인해 페일오버가 트리거되지 않을 수 있습니다. 마찬가지로, 페일오버는 CLB 서비스 장애(더 이상 사용되지 않음) 또는 Grid Manager 또는 테넌트 관리자에 대한 서비스에 의해 트리거되지 않습니다.

HA 그룹에 2개 이상의 노드의 인터페이스가 포함된 경우 페일오버 중에 액티브 인터페이스가 다른 노드의 인터페이스로 이동할 수 있습니다.

### HA 그룹 사용 방법

여러 가지 이유로 고가용성(HA) 그룹을 사용할 수 있습니다.

- HA 그룹은 Grid Manager 또는 Tenant Manager에 대한 고가용성 관리 연결을 제공할 수 있습니다.
- HA 그룹은 S3 및 Swift 클라이언트에 고가용성 데이터 연결을 제공할 수 있습니다.
- 인터페이스가 하나만 포함된 HA 그룹을 사용하면 많은 VIP 주소를 제공하고 IPv6 주소를 명시적으로 설정할 수 있습니다.

그룹에 포함된 모든 노드가 동일한 서비스를 제공하는 경우에만 HA 그룹이 고가용성을 제공할 수 있습니다. HA 그룹을

생성할 때 필요한 서비스를 제공하는 노드 유형의 인터페이스를 추가합니다.

- \* 관리 노드 \*: 로드 밸런서 서비스를 포함하고 그리드 관리자 또는 테넌트 관리자에 대한 액세스를 활성화합니다.
- \* 게이트웨이 노드 \*: 로드 밸런서 서비스 및 CLB 서비스(더 이상 사용되지 않음)를 포함합니다.

HA 그룹의 용도	이 유형의 노드를 HA 그룹에 추가합니다
Grid Manager에 액세스합니다	<ul style="list-style-type: none"> <li>• 기본 관리자 노드(* 기본 마스터 *)</li> <li>• 운영 관리자 노드가 아닌 노드</li> <li>• 참고: * 기본 관리 노드는 기본 마스터여야 합니다. 일부 유지 보수 절차는 기본 관리 노드에서만 수행할 수 있습니다.</li> </ul>
테넌트 관리자에 대한 액세스만 가능합니다	<ul style="list-style-type: none"> <li>• 운영 또는 비운영 관리 노드</li> </ul>
S3 또는 Swift 클라이언트 액세스 — 로드 밸런서 서비스	<ul style="list-style-type: none"> <li>• 관리자 노드</li> <li>• 게이트웨이 노드</li> </ul>
S3 또는 Swift 클라이언트 액세스 — CLB 서비스  • 참고: * CLB 서비스는 더 이상 사용되지 않습니다.	<ul style="list-style-type: none"> <li>• 게이트웨이 노드</li> </ul>

#### Grid Manager 또는 Tenant Manager에 HA 그룹을 사용할 때의 제한 사항

Grid Manager 또는 테넌트 관리자에 대한 서비스 장애가 HA 그룹 내에서 페일오버를 트리거하지 않습니다.

페일오버가 발생했을 때 Grid Manager 또는 Tenant Manager에 로그인한 경우, 로그아웃되며 작업을 재개하려면 다시 로그인해야 합니다.

기본 관리 노드를 사용할 수 없는 경우 일부 유지 관리 절차를 수행할 수 없습니다. 장애 조치 중에 그리드 관리자를 사용하여 StorageGRID 시스템을 모니터링할 수 있습니다.

#### CLB 서비스에 HA 그룹 사용 제한

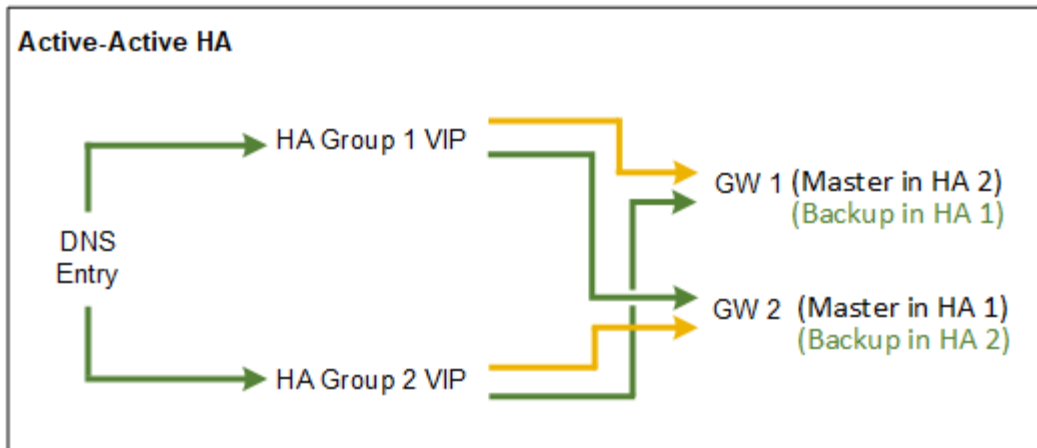
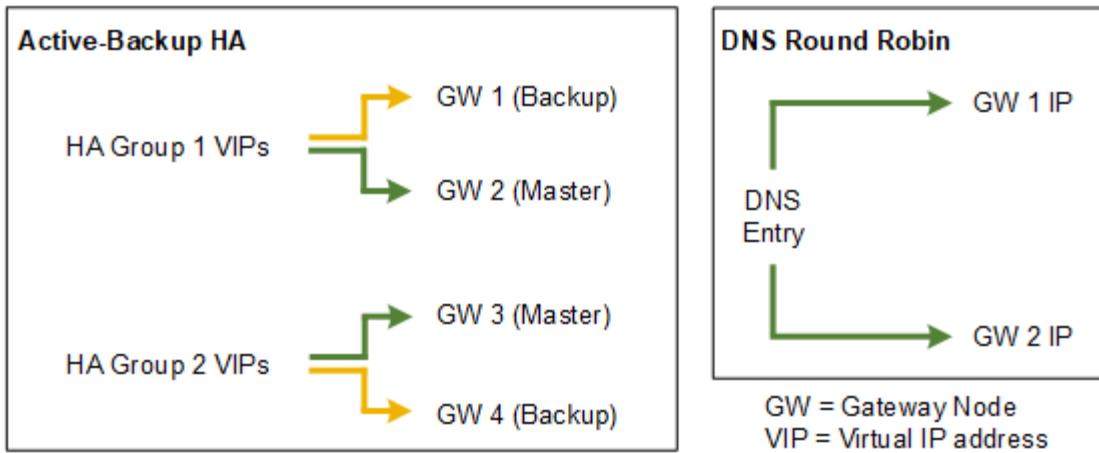
CLB 서비스가 실패해도 HA 그룹 내에서 대체 작동이 트리거되지 않습니다.



CLB 서비스는 더 이상 사용되지 않습니다.

#### HA 그룹에 대한 구성 옵션

다음 다이어그램에서는 HA 그룹을 구성할 수 있는 다양한 방법의 예를 제공합니다. 각 옵션에는 장단점이 있습니다.



Active-Active HA 예에서와 같이 여러 개의 중복 HA 그룹을 생성할 때 총 처리량은 노드 수와 HA 그룹으로 확장됩니다. 3개 이상의 노드와 3개 이상의 HA 그룹을 사용하면 노드를 오프라인으로 전환해야 하는 유지보수 절차 중에도 VIP를 사용하여 작업을 계속할 수 있습니다.

이 표에는 다이어그램에 표시된 각 HA 구성의 이점이 요약되어 있습니다.

구성	장점	단점
Active-Backup HA를 참조하십시오	<ul style="list-style-type: none"> <li>외부 종속성 없이 StorageGRID에서 관리</li> <li>빠른 페일오버.</li> </ul>	<ul style="list-style-type: none"> <li>HA 그룹에서 하나의 노드만 활성화됩니다. HA 그룹당 최소 하나의 노드가 유휴 상태가 됩니다.</li> </ul>
DNS 라운드 로빈	<ul style="list-style-type: none"> <li>총 처리량 향상:</li> <li>유휴 호스트가 없습니다.</li> </ul>	<ul style="list-style-type: none"> <li>느린 페일오버 - 클라이언트 동작에 따라 달라질 수 있습니다.</li> <li>StorageGRID 외부에서 하드웨어를 구성해야 합니다.</li> <li>고객이 구현한 상태 점검이 필요합니다.</li> </ul>

구성	장점	단점
액티브-액티브	<ul style="list-style-type: none"> <li>트래픽이 여러 HA 그룹에 분산됩니다.</li> <li>HA 그룹 수에 따라 확장 가능한 높은 애그리게이트 처리량입니다.</li> <li>빠른 페일오버.</li> </ul>	<ul style="list-style-type: none"> <li>구성이 더 복잡합니다.</li> <li>StorageGRID 외부에서 하드웨어를 구성해야 합니다.</li> <li>고객이 구현한 상태 점검이 필요합니다.</li> </ul>

## 고가용성 그룹 생성

하나 이상의 고가용성(HA) 그룹을 생성하여 관리 노드 또는 게이트웨이 노드의 서비스에 대한 고가용성 액세스를 제공할 수 있습니다.

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

### 이 작업에 대해

HA 그룹에 포함할 인터페이스는 다음 조건을 충족해야 합니다.

- 인터페이스는 게이트웨이 노드 또는 관리 노드여야 합니다.
- 인터페이스는 Grid Network(eth0) 또는 Client Network(eth2)에 속해야 합니다.
- 인터페이스는 DHCP가 아닌 고정 또는 고정 IP 주소 지정으로 구성해야 합니다.

### 단계

- 구성 \* > \* 네트워크 설정 \* > \* 고가용성 그룹 \* 을 선택합니다.

High Availability Groups 페이지가 나타납니다.

#### High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.



- Create \* 를 클릭합니다.

High Availability Group 생성 대화 상자가 나타납니다.

- 이름을 입력하고 원하는 경우 HA 그룹에 대한 설명을 입력합니다.
- Select Interfaces \* 를 클릭합니다.

High Availability Group에 인터페이스 추가 대화 상자가 나타납니다. 이 표에는 적합한 노드, 인터페이스 및 IPv4 서브넷이 나와 있습니다.



## Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
	g140-g1	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g1	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g3	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g3	eth2	192.168.0.0/21	
	g140-g4	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

Cancel

Apply

DHCP에서 IP 주소를 할당한 경우 인터페이스가 목록에 나타나지 않습니다.

### 5. HA 그룹에 추가 \* 열에서 HA 그룹에 추가할 인터페이스의 확인란을 선택합니다.

인터페이스 선택에 대한 다음 지침을 참조하십시오.

- 인터페이스를 하나 이상 선택해야 합니다.
- 둘 이상의 인터페이스를 선택하는 경우 모든 인터페이스가 그리드 네트워크(eth0) 또는 클라이언트 네트워크(eth2)에 있어야 합니다.
- 모든 인터페이스는 동일한 서브넷 또는 공통 접두사가 있는 서브넷에 있어야 합니다.

IP 주소는 가장 작은 서브넷(접두사가 가장 큰 서브넷)으로 제한됩니다.

- 다른 노드 유형의 인터페이스를 선택하고 페일오버가 발생하는 경우 선택한 노드에 공통되는 서비스만 가상 IP에서 사용할 수 있습니다.
  - Grid Manager 또는 Tenant Manager의 HA 보호를 위해 두 개 이상의 관리 노드를 선택합니다.
  - 로드 밸런서 서비스의 HA 보호를 위해 두 개 이상의 관리 노드, 게이트웨이 노드 또는 둘 다를 선택합니다.
  - CLB 서비스의 HA 보호를 위해 둘 이상의 게이트웨이 노드를 선택합니다.



CLB 서비스는 더 이상 사용되지 않습니다.

## Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
<input checked="" type="checkbox"/>	DC1-ADM1	eth0	10.96.100.0/23	
<input checked="" type="checkbox"/>	DC1-G1	eth0	10.96.100.0/23	
<input checked="" type="checkbox"/>	DC2-ADM1	eth0	10.96.100.0/23	

There are 3 interfaces selected.

**Attention:** You have selected nodes of different types that run different services. If a failover occurs, only the services common to all node types will be available on the virtual IPs.

Cancel

Apply

6. 적용 \* 을 클릭합니다.

선택한 인터페이스가고가용성 그룹 생성 페이지의 인터페이스 섹션에 나열됩니다. 기본적으로 목록의 첫 번째 인터페이스가 기본 설정 마스터로 선택됩니다.

## Create High Availability Group

### High Availability Group

Name

Description

### Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Select Interfaces

Node Name	Interface	IPv4 Subnet	Preferred Master
g140-g1	eth2	47.47.0.0/21	<input checked="" type="radio"/>
g140-g2	eth2	47.47.0.0/21	<input type="radio"/>

Displaying 2 interfaces.

### Virtual IP Addresses

Virtual IP Subnet: 47.47.0.0/21. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1



Cancel

Save

7. 다른 인터페이스를 기본 마스터로 사용하려면 \* Preferred Master \* 열에서 해당 인터페이스를 선택합니다.

장애가 발생하여 VIP 주소가 백업 인터페이스에 재할당되지 않는 한 기본 마스터는 활성 인터페이스입니다.



HA 그룹이 그리드 관리자에 대한 액세스를 제공하는 경우 기본 관리 노드에서 기본 마스터로 사용할 인터페이스를 선택해야 합니다. 일부 유지 보수 절차는 기본 관리 노드에서만 수행할 수 있습니다.

8. 페이지의 가상 IP 주소 섹션에서 HA 그룹에 대한 가상 IP 주소를 1~10개 입력합니다. 더하기 기호(+)

IPv4 주소를 하나 이상 입력해야 합니다. 선택적으로 추가 IPv4 및 IPv6 주소를 지정할 수 있습니다.

IPv4 주소는 모든 멤버 인터페이스에서 공유하는 IPv4 서브넷 내에 있어야 합니다.

9. 저장 \* 을 클릭합니다.

HA 그룹이 생성되고 이제 구성된 가상 IP 주소를 사용할 수 있습니다.

관련 정보

["Red Hat Enterprise Linux 또는 CentOS를 설치합니다"](#)

["VMware를 설치합니다"](#)

["Ubuntu 또는 Debian을 설치합니다"](#)

["로드 밸런싱 관리"](#)

고가용성 그룹 편집

HA(고가용성) 그룹을 편집하여 이름과 설명을 변경하거나, 인터페이스를 추가 또는 제거하거나, 가상 IP 주소를 추가 또는 업데이트할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

이 작업에 대해

HA 그룹을 편집하는 몇 가지 이유는 다음과 같습니다.

- 기존 그룹에 인터페이스 추가 인터페이스 IP 주소는 그룹에 이미 할당된 다른 인터페이스와 동일한 서브넷 내에 있어야 합니다.
- HA 그룹에서 인터페이스 제거 예를 들어 그리드 네트워크 또는 클라이언트 네트워크에 대한 노드의 인터페이스가 HA 그룹에서 사용되는 경우 사이트 또는 노드 서비스 해제 절차를 시작할 수 없습니다.

단계

1. 구성 \* > \* 네트워크 설정 \* > \* 고가용성 그룹 \* 을 선택합니다.

High Availability Groups 페이지가 나타납니다.

### High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

	Name	Description	Virtual IP Addresses	Interfaces
<input type="radio"/>	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
<input type="radio"/>	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

2. 편집할 HA 그룹을 선택하고 \* 편집 \* 을 클릭합니다.

High Availability Group 편집 대화 상자가 나타납니다.

- 필요에 따라 그룹의 이름 또는 설명을 업데이트합니다.
- 필요에 따라 \* 인터페이스 선택 \* 을 클릭하여 HA 그룹의 인터페이스를 변경합니다.

High Availability Group에 인터페이스 추가 대화 상자가 나타납니다.

### Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
	g140-g1	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g1	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g3	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g3	eth2	192.168.0.0/21	
	g140-g4	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

DHCP에서 IP 주소를 할당한 경우 인터페이스가 목록에 나타나지 않습니다.

- 확인란을 선택하거나 선택 취소하여 인터페이스를 추가하거나 제거합니다.

인터페이스 선택에 대한 다음 지침을 참조하십시오.

- 인터페이스를 하나 이상 선택해야 합니다.
- 둘 이상의 인터페이스를 선택하는 경우 모든 인터페이스가 그리드 네트워크(eth0) 또는 클라이언트 네트워크(eth2)에 있어야 합니다.
- 모든 인터페이스는 동일한 서브넷 또는 공통 접두사가 있는 서브넷에 있어야 합니다.

IP 주소는 가장 작은 서브넷(접두사가 가장 큰 서브넷)으로 제한됩니다.

- 다른 노드 유형의 인터페이스를 선택하고 페일오버가 발생하는 경우 선택한 노드에 공통되는 서비스만 가상 IP에서 사용할 수 있습니다.
  - Grid Manager 또는 Tenant Manager의 HA 보호를 위해 두 개 이상의 관리 노드를 선택합니다.
  - 로드 밸런서 서비스의 HA 보호를 위해 두 개 이상의 관리 노드, 게이트웨이 노드 또는 둘 다를 선택합니다.
  - CLB 서비스의 HA 보호를 위해 둘 이상의 게이트웨이 노드를 선택합니다.



CLB 서비스는 더 이상 사용되지 않습니다.

- 적용 \* 을 클릭합니다.

선택한 인터페이스가 페이지의 인터페이스 섹션에 나열됩니다. 기본적으로 목록의 첫 번째 인터페이스가 기본 설정 마스터로 선택됩니다.

### Edit High Availability Group 'HA Group - Admin Nodes'

#### High Availability Group

Name:

Description:

#### Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Node Name	Interface	IPv4 Subnet	Preferred Master
DC1-ADM1	eth0	10.96.100.0/23	<input checked="" type="radio"/>
DC2-ADM1	eth0	10.96.100.0/23	<input type="radio"/>

Displaying 2 interfaces.

#### Virtual IP Addresses

Virtual IP Subnet: 10.96.100.0/23. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1:

7. 다른 인터페이스를 기본 마스터로 사용하려면 \* Preferred Master \* 열에서 해당 인터페이스를 선택합니다.

장애가 발생하여 VIP 주소가 백업 인터페이스에 재할당되지 않는 한 기본 마스터는 활성 인터페이스입니다.



HA 그룹이 그리드 관리자에 대한 액세스를 제공하는 경우 기본 관리 노드에서 기본 마스터로 사용할 인터페이스를 선택해야 합니다. 일부 유지 보수 절차는 기본 관리 노드에서만 수행할 수 있습니다.

8. 필요에 따라 HA 그룹의 가상 IP 주소를 업데이트합니다.

IPv4 주소를 하나 이상 입력해야 합니다. 선택적으로 추가 IPv4 및 IPv6 주소를 지정할 수 있습니다.

IPv4 주소는 모든 멤버 인터페이스에서 공유하는 IPv4 서브넷 내에 있어야 합니다.

9. 저장 \* 을 클릭합니다.

HA 그룹이 업데이트됩니다.

고가용성 그룹을 제거하는 중입니다

더 이상 사용하지 않는 고가용성(HA) 그룹을 제거할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

이 작업을 시작합니다

HA 그룹을 제거하면 그룹의 가상 IP 주소 중 하나를 사용하도록 구성된 S3 또는 Swift 클라이언트가 더 이상 StorageGRID에 연결할 수 없습니다. 클라이언트 종단을 방지하려면 HA 그룹을 삭제하기 전에 영향을 받는 모든 S3 또는 Swift 클라이언트 애플리케이션을 업데이트해야 합니다. 다른 IP 주소(예: 다른 HA 그룹의 가상 IP 주소 또는 설치 중 또는 DHCP를 사용하는 동안 인터페이스에 구성된 IP 주소)를 사용하여 연결할 각 클라이언트를 업데이트합니다.

단계

1. 구성 \* > \* 네트워크 설정 \* > \* 고가용성 그룹 \* 을 선택합니다.

High Availability Groups 페이지가 나타납니다.

### High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

<input type="button" value="+ Create"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>				
	Name	Description	Virtual IP Addresses	Interfaces
<input type="radio"/>	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
<input type="radio"/>	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

2. 제거할 HA 그룹을 선택하고 \* 제거 \* 를 클릭합니다.

High Availability Group 삭제 경고가 나타납니다.

## Warning

### Delete High Availability Group

Are you sure you want to delete High Availability Group 'HA group 1'?

Cancel

OK

3. 확인 \* 을 클릭합니다.

HA 그룹이 제거됩니다.

## S3 API 엔드포인트 도메인 이름 구성

S3 가상 호스팅 스타일 요청을 지원하려면 Grid Manager를 사용하여 S3 클라이언트가 연결하는 끝점 도메인 이름 목록을 구성해야 합니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 그리드 업그레이드가 진행 중이 아닌 것을 확인해야 합니다.



그리드 업그레이드가 진행 중일 때는 도메인 이름 구성을 변경하지 마십시오.

이 작업에 대해

클라이언트가 S3 엔드 포인트 도메인 이름을 사용하도록 설정하려면 다음 작업을 모두 수행해야 합니다.

- 그리드 관리자를 사용하여 StorageGRID 시스템에 S3 끝점 도메인 이름을 추가합니다.
- 클라이언트가 StorageGRID에 대한 HTTPS 연결에 사용하는 인증서가 클라이언트에 필요한 모든 도메인 이름에 서명되었는지 확인합니다.

예를 들어, 끝점이 인 경우 `s3.company.com`HTTPS 연결에 사용되는 인증서에 가 포함되어 있는지 확인해야 합니다 `s3.company.com 끝점 및 끝점의 와일드카드 주체 대체 이름(SAN): *.s3.company.com.`

- 클라이언트가 사용하는 DNS 서버를 구성합니다. 클라이언트가 연결하는 데 사용하는 IP 주소에 대한 DNS 레코드를 포함하고 와일드카드 이름을 포함하여 레코드가 필요한 모든 끝점 도메인 이름을 참조하는지 확인합니다.



클라이언트는 게이트웨이 노드, 관리 노드 또는 스토리지 노드의 IP 주소를 사용하거나고가용성 그룹의 가상 IP 주소에 연결하여 StorageGRID에 연결할 수 있습니다. DNS 레코드에 올바른 IP 주소를 포함하도록 클라이언트 응용 프로그램이 그리드에 연결하는 방법을 이해해야 합니다.

클라이언트가 HTTPS 연결에 사용하는 인증서는 클라이언트가 그리드에 연결하는 방식에 따라 달라집니다.

- 클라이언트가 로드 밸런서 서비스를 사용하여 연결하는 경우 이 클라이언트는 특정 로드 밸런서 끝점에 대한



인증서를 사용합니다.



각 로드 밸런서 끝점마다 고유한 인증서가 있으며 각 끝점이 서로 다른 끝점 도메인 이름을 인식하도록 구성할 수 있습니다.

- 클라이언트가 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 접속하는 경우 클라이언트는 필요한 모든 끝점 도메인 이름을 포함하도록 업데이트된 그리드 사용자 지정 서버 인증서를 사용합니다.



CLB 서비스는 더 이상 사용되지 않습니다.

단계

1. 구성 > \* 네트워크 설정 > \* 도메인 이름 \* 을 선택합니다.

끝점 도메인 이름 페이지가 나타납니다.

Endpoint Domain Names

#### Virtual Hosted-Style Requests

Enable support of S3 virtual hosted-style requests by specifying API endpoint domain names. Support is disabled if this list is empty. Examples: s3.example.com, s3.example.co.uk, s3-east.example.com

Endpoint 1	<input type="text" value="s3.example.com"/>	✕
Endpoint 2	<input type="text"/>	+ ✕
<input type="button" value="Save"/>		

2. (+) 아이콘을 사용하여 추가 필드를 추가하려면 \* Endpoint \* 필드에 S3 API 끝점 도메인 이름 목록을 입력합니다.

이 목록이 비어 있으면 S3 가상 호스팅 스타일 요청에 대한 지원이 비활성화됩니다.

3. 저장 \* 을 클릭합니다.
4. 클라이언트가 사용하는 서버 인증서가 필요한 끝점 도메인 이름과 일치하는지 확인합니다.
  - 로드 밸런서 서비스를 사용하는 클라이언트의 경우 클라이언트가 연결하는 로드 밸런서 끝점과 연결된 인증서를 업데이트합니다.
  - 스토리지 노드에 직접 접속하거나 게이트웨이 노드에서 CLB 서비스를 사용하는 클라이언트의 경우 그리드의 사용자 지정 서버 인증서를 업데이트합니다.
5. 엔드포인트 도메인 이름 요청을 확인하는 데 필요한 DNS 레코드를 추가합니다.

결과

이제 클라이언트가 끝점을 사용할 때 `bucket.s3.company.com` DNS 서버가 올바른 끝점으로 확인되고 인증서는 끝점을 예상대로 인증합니다.

관련 정보

["S3을 사용합니다"](#)

["IP 주소 보기"](#)

"고가용성 그룹 생성"

"스토리지 노드 또는 CLB 서비스에 연결하기 위한 사용자 지정 서버 인증서 구성"

"부하 분산 장치 엔드포인트 구성"

## 클라이언트 통신을 위해 HTTP 활성화

기본적으로 클라이언트 응용 프로그램은 스토리지 노드에 대한 모든 연결 또는 게이트웨이 노드의 더 이상 사용되지 않는 CLB 서비스에 대해 HTTPS 네트워크 프로토콜을 사용합니다. 비프로덕션 그리드를 테스트할 때와 같이 이러한 연결에 대해 HTTP를 선택적으로 활성화할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

S3 및 Swift 클라이언트가 HTTP를 스토리지 노드 또는 게이트웨이 노드의 더 이상 사용되지 않는 CLB 서비스에 직접 연결해야 하는 경우에만 이 작업을 완료합니다.

HTTPS 연결만 사용하는 클라이언트 또는 로드 밸런서 서비스에 연결된 클라이언트에 대해서는 이 작업을 완료할 필요가 없습니다. 각 로드 밸런서 끝점에서 HTTP 또는 HTTPS를 사용하도록 구성할 수 있기 때문입니다. 자세한 내용은 로드 밸런서 엔드포인트 구성에 대한 정보를 참조하십시오.

을 참조하십시오. ["요약: 클라이언트 연결을 위한 IP 주소 및 포트"](#) 스토리지 노드에 연결할 때 또는 HTTP 또는 HTTPS를 사용하여 더 이상 사용되지 않는 CLB 서비스에 연결할 때 사용하는 S3 및 Swift 포트에 대해 알아보십시오



요청이 암호화되지 않은 상태로 전송되므로 프로덕션 그리드에 대해 HTTP를 설정할 때는 주의해야 합니다.

단계

1. 구성 \*\* 시스템 설정 \* 그리드 옵션 \* 을 선택합니다.
2. 네트워크 옵션 섹션에서 \* HTTP 연결 사용 \* 확인란을 선택합니다.

### Network Options



3. 저장 \* 을 클릭합니다.

관련 정보

"부하 분산 장치 엔드포인트 구성"

"S3을 사용합니다"

"Swift를 사용합니다"

허용되는 클라이언트 작업을 제어합니다

클라이언트 수정 방지 그리드 옵션을 선택하여 특정 HTTP 클라이언트 작업을 거부할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

클라이언트 수정 방지 는 시스템 전체 설정입니다. 클라이언트 수정 방지 옵션을 선택하면 다음 요청이 거부됩니다.

- \* S3 REST API \*
  - 버킷 요청을 삭제합니다
  - 기존 오브젝트의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태그 지정을 수정하는 요청



이 설정은 버전 관리가 활성화된 버킷에는 적용되지 않습니다. 버전 관리를 사용하면 이미 개체 데이터, 사용자 정의 메타데이터 및 개체 태그 지정을 수정할 수 없습니다.

- \* Swift REST API \*
  - 컨테이너 요청을 삭제합니다
  - 기존 객체 수정 요청. 예를 들어, 덮어쓰기, 삭제, 메타데이터 업데이트 등의 작업이 거부됩니다.

단계

1. 구성 \*\* 시스템 설정 \* 그리드 옵션 \* 을 선택합니다.
2. 네트워크 옵션 섹션에서 \* 클라이언트 수정 방지 \* 확인란을 선택합니다.

### Network Options

Prevent Client Modification

Enable HTTP Connection

Network Transfer Encryption  AES128-SHA  AES256-SHA

3. 저장 \* 을 클릭합니다.

## StorageGRID 네트워크 및 연결 관리

그리드 관리자를 사용하여 StorageGRID 네트워크 및 연결을 구성하고 관리할 수 있습니다.

을 참조하십시오 ["S3 및 Swift 클라이언트 연결 구성"](#) S3 또는 Swift 클라이언트를 연결하는 방법에 대해 알아보십시오.

- ["StorageGRID 네트워크 지침"](#)
- ["IP 주소 보기"](#)
- ["발신 TLS 연결에 지원되는 암호"](#)
- ["네트워크 전송 암호화를 변경하는 중입니다"](#)
- ["서버 인증서를 구성하는 중입니다"](#)
- ["스토리지 프록시 설정을 구성하는 중입니다"](#)
- ["관리자 프록시 설정을 구성합니다"](#)
- ["트래픽 분류 정책 관리"](#)
- ["링크 비용은 얼마입니까"](#)

### StorageGRID 네트워크 지침

StorageGRID는 그리드 노드당 최대 3개의 네트워크 인터페이스를 지원하므로 각 개별 그리드 노드의 네트워킹을 보안 및 액세스 요구 사항에 맞게 구성할 수 있습니다.



그리드 노드의 네트워크를 수정하거나 추가하려면 복구 및 유지 관리 지침을 참조하십시오. 네트워크 토폴로지에 대한 자세한 내용은 네트워킹 지침을 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 및 Swift 클라이언트 애플리케이션에 대한 액세스를 제공하는 데 사용되는 개방형 네트워크이므로 그리드 네트워크를 격리하고 보호할 수 있습니다. 클라이언트 네트워크는 로컬 게이트웨이를 통해 연결할 수 있는 모든 서브넷과 통신할 수 있습니다.

#### 지침

- 각 StorageGRID 그리드 노드에는 할당된 각 네트워크에 대한 전용 네트워크 인터페이스, IP 주소, 서브넷 마스크

및 게이트웨이가 필요합니다.

- 그리드 노드는 네트워크에 둘 이상의 인터페이스를 가질 수 없습니다.
- 네트워크 당, 그리드 노드별로 단일 게이트웨이가 지원되며 노드와 동일한 서브넷에 있어야 합니다. 필요한 경우 게이트웨이에서 보다 복잡한 라우팅을 구현할 수 있습니다.
- 각 노드에서 각 네트워크는 특정 네트워크 인터페이스에 매핑됩니다.

네트워크	인터페이스 이름입니다
그리드	eth0
관리자(선택 사항)	eth1
클라이언트(선택 사항)	eth2

- 노드가 StorageGRID 어플라이언스에 연결된 경우 각 네트워크에 대해 특정 포트가 사용됩니다. 자세한 내용은 어플라이언스 설치 지침을 참조하십시오.
- 기본 라우트는 노드당 자동으로 생성됩니다. eth2가 활성화된 경우 0.0.0.0/0 은 eth2의 클라이언트 네트워크를 사용합니다. eth2가 활성화되지 않은 경우 0.0.0.0/0 은 eth0의 그리드 네트워크를 사용합니다.
- 그리드 노드가 그리드에 가입될 때까지 클라이언트 네트워크가 작동하지 않습니다
- 그리드 노드를 구축하는 동안 관리 네트워크를 구성하여 그리드를 완전히 설치하기 전에 설치 사용자 인터페이스에 액세스할 수 있습니다.

관련 정보

["유지 및 복구"](#)

["네트워크 지침"](#)

## IP 주소 보기

StorageGRID 시스템의 각 그리드 노드에 대한 IP 주소를 볼 수 있습니다. 그런 다음 이 IP 주소를 사용하여 명령줄에서 그리드 노드에 로그인하고 다양한 유지보수 절차를 수행할 수 있습니다.

필요한 것

지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

이 작업에 대해

IP 주소 변경에 대한 자세한 내용은 복구 및 유지 관리 지침을 참조하십시오.

단계

1. 노드 \* > \*GRID node \* > \* Overview \* 를 선택합니다.
2. IP 주소 제목 오른쪽에 있는 \* 더 보기 \* 를 클릭합니다.

해당 그리드 노드의 IP 주소가 테이블에 나열됩니다.

**Node Information** ⓘ

**Name** SGA-lab11  
**Type** Storage Node  
**ID** 0b583829-6659-4c6e-b2d0-31461d22ba67

**Connection State** ✔ Connected  
**Software Version** 11.4.0 (build 20200527.0043.61839a2)  
**IP Addresses** 192.168.4.138, 10.224.4.138, 169.254.0.1 [Show less](#) ▲

Interface	IP Address
eth0	192.168.4.138
eth0	fd20:331:331:0:2a0:98ff:fea1:831d
eth0	fe80::2a0:98ff:fea1:831d
eth1	10.224.4.138
eth1	fd20:327:327:0:280:e5ff:fe43:a99c
eth1	fd20:8b1e:b255:8154:280:e5ff:fe43:a99c
eth1	fe80::280:e5ff:fe43:a99c
hic2	192.168.4.138
hic4	192.168.4.138
mtc1	10.224.4.138
mtc2	169.254.0.1

관련 정보

["유지 및 복구"](#)

## 발신 TLS 연결에 지원되는 암호

StorageGRID 시스템은 ID 페더레이션 및 클라우드 스토리지 풀에 사용되는 외부 시스템에 대한 TLS(Transport Layer Security) 연결을 위한 제한된 암호화 그룹 세트를 지원합니다.

지원되는 TLS 버전입니다

StorageGRID는 ID 페더레이션 및 클라우드 스토리지 풀에 사용되는 외부 시스템에 대한 연결을 위해 TLS 1.2 및 TLS 1.3을 지원합니다.

외부 시스템과 호환되도록 외부 시스템에 사용할 수 있도록 지원되는 TLS 암호가 선택되었습니다. 이 목록은 S3 또는 Swift 클라이언트 애플리케이션에서 사용할 수 있도록 지원되는 암호화 목록보다 큽니다.



프로토콜 버전, 암호, 키 교환 알고리즘 및 MAC 알고리즘과 같은 TLS 구성 옵션은 StorageGRID에서 구성할 수 없습니다. 이러한 설정에 대한 구체적인 요청이 있을 경우 NetApp 어카운트 담당자에게 문의하십시오.

지원되는 TLS 1.2 암호 그룹

지원되는 TLS 1.2 암호 제품군은 다음과 같습니다.

- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_with\_CHACH20\_POLY1305
- TLS\_ECDHE\_ECDSA\_WITH\_CHACH20\_POLY1305
- TLS\_RSA\_with\_AES\_128\_GCM\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

지원되는 **TLS 1.3** 암호 그룹

지원되는 TLS 1.3 암호 제품군은 다음과 같습니다.

- TLS\_AES\_256\_GCM\_SHA384
- TLS\_CHACH20\_POLY1305\_SHA256
- TLS\_AES\_128\_GCM\_SHA256

네트워크 전송 암호화를 변경하는 중입니다

StorageGRID 시스템은 TLS(Transport Layer Security)를 사용하여 그리드 노드 간의 내부 제어 트래픽을 보호합니다. 네트워크 전송 암호화 옵션은 TLS가 그리드 노드 간의 제어 트래픽을 암호화하는 데 사용하는 알고리즘을 설정합니다. 이 설정은 데이터 암호화에 영향을 주지 않습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

기본적으로 네트워크 전송 암호화는 AES256-SHA 알고리즘을 사용합니다. AES128-SHA 알고리즘을 사용하여 제어 트래픽을 암호화할 수도 있습니다.

단계

1. 구성 \* \* 시스템 설정 \* 그리드 옵션 \* 을 선택합니다.
2. 네트워크 옵션 섹션에서 네트워크 전송 암호화를 \* AES128-SHA \* 또는 \* AES256-SHA \* (기본값)로 변경합니다.

### Network Options



3. 저장 \* 을 클릭합니다.

## 서버 인증서를 구성하는 중입니다

StorageGRID 시스템에서 사용하는 서버 인증서를 사용자 지정할 수 있습니다.

StorageGRID 시스템은 다음과 같은 여러 가지 목적으로 보안 인증서를 사용합니다.

- 관리 인터페이스 서버 인증서: 그리드 관리자, 테넌트 관리자, 그리드 관리 API 및 테넌트 관리 API에 대한 액세스를 보호하는 데 사용됩니다.
- 스토리지 API 서버 인증서: API 클라이언트 애플리케이션이 객체 데이터를 업로드 및 다운로드하는 데 사용하는 스토리지 노드 및 게이트웨이 노드에 대한 액세스를 보호하는 데 사용됩니다.

설치 중에 생성된 기본 인증서를 사용하거나 이러한 기본 인증서 유형 중 하나 또는 둘 다를 사용자 지정 인증서로 바꿀 수 있습니다.

### 지원되는 유형의 사용자 지정 서버 인증서

StorageGRID 시스템은 RSA 또는 ECDSA(Elliptic Curve Digital Signature Algorithm)로 암호화된 사용자 지정 서버 인증서를 지원합니다.

StorageGRID가 REST API용 클라이언트 연결을 보호하는 방법에 대한 자세한 내용은 S3 또는 Swift 구현 가이드를 참조하십시오.

### 로드 밸런서 끝점용 인증서

StorageGRID는 로드 밸런서 끝점에 사용되는 인증서를 별도로 관리합니다. 로드 밸런서 인증서를 구성하려면 로드 밸런서 끝점을 구성하는 지침을 참조하십시오.

### 관련 정보

["S3을 사용합니다"](#)

["Swift를 사용합니다"](#)

["부하 분산 장치 엔드포인트 구성"](#)

### Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성

기본 StorageGRID 서버 인증서를 단일 사용자 지정 서버 인증서로 교체하여 보안 경고가 발생하지 않고 사용자가 그리드 관리자 및 테넌트 관리자에 액세스할 수 있도록 할 수 있습니다.

#### 이 작업에 대해

기본적으로 모든 관리 노드에는 그리드 CA에서 서명한 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 관리 노드에 사용되므로 클라이언트가 Grid Manager 및 Tenant Manager에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 사용자 지정 인증서를 정의하여 그리드의 모든 관리 노드와 일치시킵니다.

서버에서 구성을 완료해야 하며 사용 중인 루트 CA(인증 기관)에 따라 사용자가 그리드 관리자 및 테넌트 관리자에 액세스하는 데 사용할 웹 브라우저에 루트 CA 인증서를 설치해야 할 수도 있습니다.





실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 이 서버 인증서가 만료될 때 \* Management Interface \* 용 서버 인증서 만료 알림과 레거시 관리 인터페이스 인증서 만료(MCEP) 경보가 모두 트리거됩니다. 필요에 따라 \* 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택하여 현재 서비스 인증서가 만료될 때까지 일 수를 확인할 수 있습니다. 그런 다음 \*기본 관리 노드 \* > \* CMN \* > \* 리소스 \* 를 선택합니다.



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 서버 인증서가 만료됩니다.
- 사용자 지정 관리 인터페이스 서버 인증서를 기본 서버 인증서로 되돌립니다.

#### 단계

1. 구성 \* > \* 네트워크 설정 \* > \* 서버 인증서 \* 를 선택합니다.
2. 관리 인터페이스 서버 인증서 섹션에서 \* 사용자 정의 인증서 설치 \* 를 클릭합니다.
3. 필요한 서버 인증서 파일을 업로드합니다.
  - \* 서버 인증서 \*: 사용자 정의 서버 인증서 파일 (.crt)를 클릭합니다.
  - \* 서버 인증서 개인 키 \*: 사용자 지정 서버 인증서 개인 키 파일입니다 (.key)를 클릭합니다.



EC 개인 키는 224비트 이상이어야 합니다. RSA 개인 키는 2048비트 이상이어야 합니다.

- \* CA 번들 \*: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.

4. 저장 \* 을 클릭합니다.

사용자 지정 서버 인증서는 이후의 모든 새 클라이언트 연결에 사용됩니다.

기본 StorageGRID 서버 인증서 또는 업로드된 CA 서명 인증서에 대한 자세한 정보를 표시하려면 탭을 선택합니다.



새 인증서를 업로드한 후 관련 인증서 만료 알림(또는 레거시 알람)이 지워지도록 최대 1일을 허용합니다.

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

#### Grid Manager 및 Tenant Manager에 대한 기본 서버 인증서 복원

Grid Manager 및 Tenant Manager에 대한 기본 서버 인증서를 사용하도록 되돌릴 수 있습니다.

#### 단계

1. 구성 \* > \* 네트워크 설정 \* > \* 서버 인증서 \* 를 선택합니다.
2. 인터페이스 서버 인증서 관리 섹션에서 \* 기본 인증서 사용 \* 을 클릭합니다.
3. 확인 대화 상자에서 \* 확인 \* 을 클릭합니다.

기본 서버 인증서를 복원하면 구성된 사용자 지정 서버 인증서 파일이 삭제되고 시스템에서 복구할 수 없습니다.

이후의 모든 새 클라이언트 연결에 기본 서버 인증서가 사용됩니다.

4. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

스토리지 노드 또는 **CLB** 서비스에 연결하기 위한 사용자 지정 서버 인증서 구성

스토리지 노드에 대한 S3 또는 Swift 클라이언트 연결에 사용되는 서버 인증서 또는 게이트웨이 노드의 CLB 서비스(더 이상 사용되지 않음)를 교체할 수 있습니다. 교체 사용자 지정 서버 인증서는 조직에 따라 다릅니다.

이 작업에 대해

기본적으로 모든 스토리지 노드에는 그리드 CA에서 서명한 X.509 서버 인증서가 발급됩니다. 이러한 CA 서명 인증서는 하나의 공통 사용자 지정 서버 인증서 및 해당 개인 키로 대체할 수 있습니다.

단일 사용자 지정 서버 인증서가 모든 스토리지 노드에 사용되므로 클라이언트가 스토리지 끝점에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 사용자 지정 인증서를 정의하여 그리드의 모든 스토리지 노드와 일치시킵니다.

서버에서 구성을 완료한 후 사용하는 루트 CA(인증 기관)에 따라 시스템에 액세스하는 데 사용할 S3 또는 Swift API 클라이언트에 루트 CA 인증서를 설치해야 할 수도 있습니다.



실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 \* Storage API Endpoints \* 용 서버 인증서 만료 알림과 레거시 Storage API Service Endpoints 인증서 만료(SCEP) 경보가 모두 루트 서버 인증서가 만료될 때 트리거됩니다. 필요에 따라 \* Support \*\*\* Tools \*\* Grid Topology \* 를 선택하여 현재 서비스 인증서가 만료될 때까지 일 수를 확인할 수 있습니다. 그런 다음 \*기본 관리 노드 \*\* CMN \* 리소스 \* 를 선택합니다.

사용자 지정 인증서는 클라이언트가 게이트웨이 노드에서 더 이상 사용되지 않는 CLB 서비스를 사용하여 StorageGRID에 연결하거나 스토리지 노드에 직접 연결하는 경우에만 사용됩니다. 관리 노드 또는 게이트웨이 노드에서 로드 밸런서 서비스를 사용하여 StorageGRID에 연결하는 S3 또는 Swift 클라이언트는 로드 밸런서 끝점에 대해 구성된 인증서를 사용합니다.



곧 만료되는 로드 밸런서 끝점에 대해 \* 로드 밸런서 끝점 인증서 만료 \* 경고가 트리거됩니다.

단계

1. 구성 \* > \* 네트워크 설정 \* > \* 서버 인증서 \* 를 선택합니다.
2. 개체 스토리지 API 서비스 끝점 서버 인증서 섹션에서 \* 사용자 지정 인증서 설치 \* 를 클릭합니다.
3. 필요한 서버 인증서 파일을 업로드합니다.
  - \* 서버 인증서 \*: 사용자 정의 서버 인증서 파일 (.crt)를 클릭합니다.
  - \* 서버 인증서 개인 키 \*: 사용자 지정 서버 인증서 개인 키 파일입니다 (.key)를 클릭합니다.



EC 개인 키는 224비트 이상이어야 합니다. RSA 개인 키는 2048비트 이상이어야 합니다.

- \* CA 번들 \*: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.
4. 저장 \* 을 클릭합니다.

사용자 지정 서버 인증서는 이후의 모든 새 API 클라이언트 연결에 사용됩니다.

기본 StorageGRID 서버 인증서 또는 업로드된 CA 서명 인증서에 대한 자세한 정보를 표시하려면 탭을 선택합니다.



새 인증서를 업로드한 후 관련 인증서 만료 알림(또는 레거시 알림)이 지워지도록 최대 1일을 허용합니다.

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

관련 정보

["S3을 사용합니다"](#)

["Swift를 사용합니다"](#)

["S3 API 엔드포인트 도메인 이름 구성"](#)

**S3 및 Swift REST API 엔드포인트에 대한 기본 서버 인증서 복원**

S3 및 Swift REST API 엔드포인트에 대한 기본 서버 인증서를 사용하여 로 되돌릴 수 있습니다.

단계

1. 구성 \* > \* 네트워크 설정 \* > \* 서버 인증서 \* 를 선택합니다.
2. 개체 스토리지 API 서비스 끝점 서버 인증서 섹션에서 \* 기본 인증서 사용 \* 을 클릭합니다.
3. 확인 대화 상자에서 \* 확인 \* 을 클릭합니다.

객체 저장소 API 끝점에 대한 기본 서버 인증서를 복원하면 구성된 사용자 지정 서버 인증서 파일이 삭제되고 시스템에서 복구할 수 없습니다. 이후의 모든 새 API 클라이언트 연결에 기본 서버 인증서가 사용됩니다.

4. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

**StorageGRID 시스템의 CA 인증서를 복사하는 중입니다**

StorageGRID는 내부 CA(인증 기관)를 사용하여 내부 트래픽을 보호합니다. 인증서를 업로드해도 이 인증서는 변경되지 않습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

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

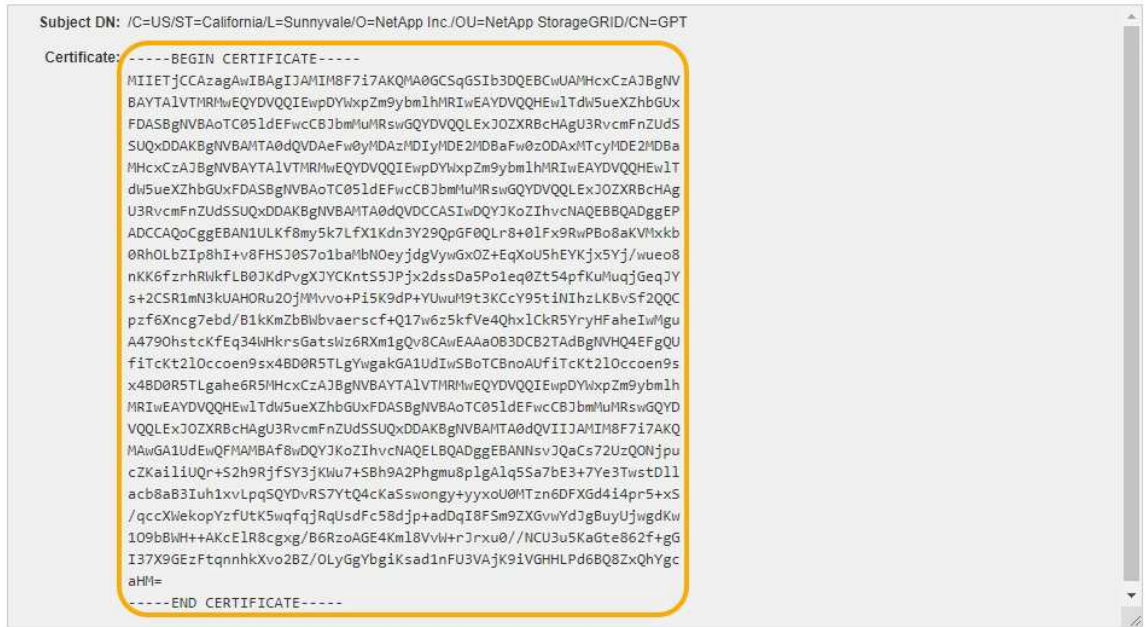
1. 구성 \* > \* 네트워크 설정 \* > \* 서버 인증서 \* 를 선택합니다.
2. 내부 CA 인증서 \* 섹션에서 모든 인증서 텍스트를 선택합니다.

반드시 포함해야 합니다 -----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 선택합니다.

### Internal CA Certificate

StorageGRID uses an internal Certificate Authority (CA) to secure internal traffic. This certificate does not change if you upload your own certificates.

To export the internal CA certificate, copy all of the certificate text (starting with -----BEGIN CERTIFICATE and ending with END CERTIFICATE-----), and save it as a .pem file.



3. 선택한 텍스트를 마우스 오른쪽 단추로 클릭하고 \* 복사 \* 를 선택합니다.
4. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.
5. 파일을 확장자로 저장합니다 .pem.

예를 들면 다음과 같습니다. storagegrid\_certificate.pem

### FabricPool용 StorageGRID 인증서 구성

엄격한 호스트 이름 유효성 검사를 수행하고 FabricPool를 사용하는 ONTAP 클라이언트와 같은 엄격한 호스트 이름 유효성 검사를 사용하지 않는 S3 클라이언트의 경우 로드 밸런서 끝점을 구성할 때 서버 인증서를 생성하거나 업로드할 수 있습니다.

#### 필요한 것

- 특정 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

#### 이 작업에 대해

로드 밸런서 끝점을 만들 때 자체 서명된 서버 인증서를 생성하거나 알려진 CA(인증 기관)에서 서명한 인증서를 업로드할 수 있습니다. 프로덕션 환경에서는 알려진 CA가 서명한 인증서를 사용해야 합니다. CA에서 서명한 인증서는 중단 없이 회전할 수 있습니다. 또한 중간자 공격에 대한 보호 기능이 강화되어 보안이 더욱 강화되고 있습니다.

다음 단계에서는 FabricPool를 사용하는 S3 클라이언트에 대한 일반 지침을 제공합니다. 자세한 내용과 절차는 StorageGRID for FabricPool 구성 지침을 참조하십시오.



게이트웨이 노드의 별도의 CLB(연결 로드 밸런서) 서비스는 더 이상 사용되지 않으며 FabricPool에서 더 이상 사용하지 않는 것이 좋습니다.

#### 단계

1. 선택적으로 FabricPool에서 사용할 고가용성(HA) 그룹을 구성합니다.
2. FabricPool에서 사용할 S3 로드 밸런서 끝점을 만듭니다.

HTTPS 로드 밸런서 끝점을 만들면 서버 인증서, 인증서 개인 키 및 CA 번들을 업로드하라는 메시지가 표시됩니다.

3. StorageGRID을 ONTAP의 클라우드 계층으로 연결

로드 밸런서 끝점 포트와 업로드한 CA 인증서에 사용된 정규화된 도메인 이름을 지정합니다. 그런 다음 CA 인증서를 제공합니다.



중간 CA에서 StorageGRID 인증서를 발급한 경우 중간 CA 인증서를 제공해야 합니다. StorageGRID 인증서가 루트 CA에서 직접 발급된 경우 루트 CA 인증서를 제공해야 합니다.

#### 관련 정보

["FabricPool용 StorageGRID를 구성합니다"](#)

관리 인터페이스에 대해 자체 서명된 서버 인증서를 생성하는 중입니다

스크립트를 사용하여 엄격한 호스트 이름 확인이 필요한 관리 API 클라이언트용 자체 서명된 서버 인증서를 생성할 수 있습니다.

#### 필요한 것

- 특정 액세스 권한이 있어야 합니다.
- 에 가 있어야 합니다 Passwords.txt 파일.

#### 이 작업에 대해

프로덕션 환경에서는 알려진 CA(인증 기관)에서 서명한 인증서를 사용해야 합니다. CA에서 서명한 인증서는 중단 없이 회전할 수 있습니다. 또한 중간자 공격에 대한 보호 기능이 강화되어 보안이 더욱 강화되고 있습니다.

#### 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. 에 나열된 암호를 입력합니다 Passwords.txt 파일.
  - c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
  - d. 에 나열된 암호를 입력합니다 Passwords.txt 파일.

루트로 로그인하면 프롬프트가 에서 변경됩니다 \$ 를 선택합니다 #.

3. 자체 서명된 새 인증서를 사용하여 StorageGRID를 구성합니다.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- 용 `--domains``에서 와일드카드를 사용하여 모든 관리 노드의 정규화된 도메인 이름을 나타냅니다. 예를 들면, 다음과 같습니다. ``*.ui.storagegrid.example.com` 와일드카드를 사용하여 나타냅니다 `admin1.ui.storagegrid.example.com` 및 `admin2.ui.storagegrid.example.com`.
- 설정 `--type` 를 선택합니다 `management` Grid Manager 및 Tenant Manager에서 사용하는 인증서를 구성합니다.
- 기본적으로 생성된 인증서는 1년(365일) 동안 유효하며 만료되기 전에 다시 만들어야 합니다. 를 사용할 수 있습니다 `--days` 기본 유효 기간을 재정의하는 인수입니다.



인증서의 유효 기간은 언제 시작됩니다 `make-certificate` 가 실행됩니다. 관리 API 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 365
```

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 `** 서버 인증서 * 관리 인터페이스 서버 인증서 *` 를 선택합니다.

#### 7. 복사한 공용 인증서를 사용하도록 관리 API 클라이언트를 구성합니다. BEGIN 및 END Tags를 포함합니다.

### 스토리지 프록시 설정을 구성하는 중입니다

플랫폼 서비스 또는 클라우드 스토리지 풀을 사용하는 경우 스토리지 노드와 외부 S3 엔드포인트 간에 투명하지 않은 프록시를 구성할 수 있습니다. 예를 들어, 플랫폼 서비스 메시지를 인터넷의 끝점과 같은 외부 끝점으로 보내려면 투명하지 않은 프록시가 필요할 수 있습니다.

#### 필요한 것

- 특정 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

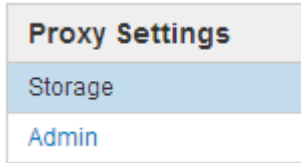
#### 이 작업에 대해

단일 스토리지 프록시에 대한 설정을 구성할 수 있습니다.

#### 단계

1. 구성 \* \* \* 네트워크 설정 \* \* 프록시 설정 \* 을 선택합니다.

스토리지 프록시 설정 페이지가 나타납니다. 기본적으로 보조 아이콘 메뉴에서 \* 스토리지 \* 가 선택됩니다.



2. 스토리지 프록시 사용 \* 확인란을 선택합니다.

스토리지 프록시 구성에 대한 필드가 나타납니다.

### Storage Proxy Settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy

Protocol  HTTP  SOCKS5

Hostname

Port (optional)

3. 투명하지 않은 스토리지 프록시에 대한 프로토콜을 선택합니다.

4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.

5. 필요에 따라 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.

프로토콜의 기본 포트(HTTP의 경우 80, SOCKS5의 경우 1080)를 사용하는 경우 이 필드를 비워 둘 수 있습니다.

6. 저장 \* 을 클릭합니다.

스토리지 프록시를 저장한 후 플랫폼 서비스 또는 클라우드 스토리지 풀의 새 엔드포인트를 구성 및 테스트할 수 있습니다.



프록시 변경 사항이 적용하려면 최대 10분이 소요될 수 있습니다.

7. 프록시 서버의 설정을 확인하여 StorageGRID의 플랫폼 서비스 관련 메시지가 차단되지 않는지 확인합니다.

작업을 마친 후

스토리지 프록시를 비활성화해야 하는 경우 \* 스토리지 프록시 사용 \* 확인란의 선택을 취소하고 \* 저장 \* 을 클릭합니다.

관련 정보

["플랫폼 서비스를 위한 네트워킹 및 포트"](#)

["ILM을 사용하여 개체를 관리합니다"](#)

## 관리자 프록시 설정을 구성합니다

HTTP 또는 HTTPS를 사용하여 AutoSupport 메시지를 보내는 경우 관리자 노드와 기술 지원(AutoSupport) 간에 투명하지 않은 프록시 서버를 구성할 수 있습니다.

### 필요한 것

- 특정 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

### 이 작업에 대해

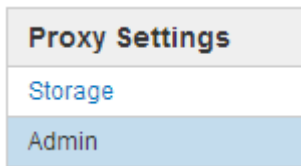
단일 관리 프록시에 대한 설정을 구성할 수 있습니다.

### 단계

1. 구성 \* \* \* 네트워크 설정 \* \* 프록시 설정 \* 을 선택합니다.

관리자 프록시 설정 페이지가 나타납니다. 기본적으로 보조 아이콘 메뉴에서 \* 스토리지 \* 가 선택됩니다.

2. 측면 표시줄 메뉴에서 \* Admin \* 을 선택합니다.



3. 관리자 프록시 사용 \* 확인란을 선택합니다.

### Admin Proxy Settings

If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy

Hostname

Port

Username (optional)

Password (optional)

4. 프록시 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. 프록시 서버에 연결하는 데 사용되는 포트를 입력합니다.
6. 필요에 따라 프록시 사용자 이름을 입력합니다.

프록시 서버에 사용자 이름이 필요하지 않은 경우 이 필드를 비워 둡니다.



7. 필요에 따라 프록시 암호를 입력합니다.

프록시 서버에 암호가 필요하지 않은 경우 이 필드를 비워 둡니다.

8. 저장 \* 을 클릭합니다.

관리자 프록시가 저장되면 관리 노드와 기술 지원 사이의 프록시 서버가 구성됩니다.



프록시 변경 사항이 적용되려면 최대 10분이 소요될 수 있습니다.

9. 프록시를 비활성화해야 하는 경우 \* 관리자 프록시 사용 \* 확인란의 선택을 취소하고 \* 저장 \* 을 클릭합니다.

관련 정보

["AutoSupport 메시지에 대한 프로토콜 지정"](#)

## 트래픽 분류 정책 관리

서비스 품질(QoS) 오퍼링을 향상하기 위해 트래픽 분류 정책을 생성하여 다양한 유형의 네트워크 트래픽을 식별 및 모니터링할 수 있습니다. 이러한 정책은 트래픽 제한 및 모니터링을 지원할 수 있습니다.

트래픽 분류 정책은 게이트웨이 노드 및 관리 노드에 대한 StorageGRID 로드 밸런서 서비스의 끝점에 적용됩니다. 트래픽 분류 정책을 생성하려면 로드 밸런서 엔드포인트를 이미 생성해야 합니다.

규칙 및 옵션 제한 일치

각 트래픽 분류 정책에는 다음 항목 중 하나 이상에 관련된 네트워크 트래픽을 식별하기 위한 하나 이상의 일치하는 규칙이 포함되어 있습니다.

- 버킷
- 테넌트
- 서브넷(클라이언트가 포함된 IPv4 서브넷)
- 엔드포인트(로드 밸런서 엔드포인트)

StorageGRID는 규칙의 목적에 따라 정책 내의 규칙과 일치하는 트래픽을 모니터링합니다. 정책에 대한 규칙과 일치하는 모든 트래픽은 해당 정책에 의해 처리됩니다. 반대로, 지정된 엔터티를 제외한 모든 트래픽에 일치시키는 규칙을 설정할 수 있습니다.

필요에 따라 다음 매개 변수를 기반으로 정책에 대한 제한을 설정할 수 있습니다.

- 총 대역폭
- 총 대역폭 출력
- 동시 읽기 요청
- 동시 쓰기 요청
- 요청 당 대역폭
- 요청 당 대역폭 출력

- 읽기 요청 속도
- 쓰기 요청 속도



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.

### 트래픽 제한

트래픽 분류 정책을 만들면 설정한 규칙 및 제한 유형에 따라 트래픽이 제한됩니다. 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 매치 유형별로 적용됩니다. 다른 모든 제한 유형의 경우 클라이언트 요청이 250밀리초 지연되고 일치하는 정책 제한을 초과하는 요청에 대해 503 느린 응답 응답을 수신합니다.

Grid Manager에서 트래픽 차트를 보고 정책이 기대하는 트래픽 제한을 적용하고 있는지 확인할 수 있습니다.

### SLA와 함께 트래픽 분류 정책을 사용합니다

용량 제한 및 데이터 보호와 함께 트래픽 분류 정책을 사용하여 용량, 데이터 보호 및 성능에 대한 세부 정보를 제공하는 서비스 수준 계약(SLA)을 적용할 수 있습니다.

트래픽 분류 제한은 부하 분산 장치에 따라 구현됩니다. 트래픽이 여러 부하 분산 장치에 동시에 분산되는 경우 총 최대 속도는 사용자가 지정한 속도 제한의 배수입니다.

다음 예에서는 SLA의 세 가지 계층을 보여 줍니다. 트래픽 분류 정책을 작성하여 각 SLA 계층의 성능 목표를 달성할 수 있습니다.

서비스 수준 계층	용량	데이터 보호	성능	비용
골드	1PB의 스토리지가 허용됩니다	3 ILM 규칙을 복사합니다	초당 25K 요청  5GB/sec(40Gbps) 대역폭	\$\$/월
실버	250TB 저장 가능	2 ILM 규칙을 복사합니다	초당 10K 요청  1.25GB/sec(10Gbps) 대역폭	\$\$/월
브론즈	100TB 스토리지 허용	2 ILM 규칙을 복사합니다	초당 5K 요청  1 GB/sec(8Gbps) 대역폭	\$/월

트래픽 분류 정책을 생성하는 중입니다

버킷, 테넌트, IP 서브넷 또는 로드 밸런서 끝점별로 네트워크 트래픽을 모니터링하고 선택적으로 제한하려는 경우 트래픽 분류 정책을 생성합니다. 필요에 따라 대역폭, 동시 요청 수 또는 요청 속도를 기준으로 정책에 대한 제한을 설정할 수 있습니다.

## 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.
- 일치시킬 로드 밸런서 끝점을 만들어야 합니다.
- 일치시킬 테넌트를 모두 만들어야 합니다.

## 단계

1. 구성 \* > \* 네트워크 설정 \* > \* 트래픽 분류 \* 를 선택합니다.

교통 분류 정책 페이지가 나타납니다.

### Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.




The screenshot shows a user interface for managing traffic classification policies. At the top, there are four buttons: '+ Create', 'Edit', 'Remove', and 'Metrics'. Below these buttons is a table with three columns: 'Name', 'Description', and 'ID'. The table is currently empty, and the text 'No policies found.' is displayed below it.

2. Create \* 를 클릭합니다.

트래픽 분류 정책 생성 대화 상자가 나타납니다.

## Create Traffic Classification Policy



### Policy

Name 

Description

### Matching Rules

Traffic that matches any rule is included in the policy.

Type	Inverse Match	Match Value
------	---------------	-------------

*No matching rules found.*

### Limits (Optional)

Type	Value	Units
------	-------	-------

*No limits found.*

Cancel

Save

- 이름 \* 필드에 정책의 이름을 입력합니다.

정책을 인식할 수 있도록 설명 이름을 입력합니다.

- 필요에 따라 \* Description \* (설명 \*) 필드에 정책에 대한 설명을 추가합니다.

예를 들어, 이 트래픽 분류 정책이 적용되는 대상 및 제한할 내용에 대해 설명하십시오.

- 정책에 일치하는 규칙을 하나 이상 생성합니다.



일치 규칙은 이 트래픽 분류 정책의 영향을 받을 엔터티를 제어합니다. 예를 들어 특정 테넌트의 네트워크 트래픽에 이 정책을 적용하려면 Tenant를 선택합니다. 또는 이 정책을 특정 로드 밸런싱 장치 끝점의 네트워크 트래픽에 적용하려면 끝점을 선택합니다.


- 일치 규칙 \* 섹션에서 \* 만들기 \* 를 클릭합니다.


일치 규칙 만들기 대화 상자가 나타납니다.



## Create Matching Rule

### Matching Rules

Type  -- Choose One -- 

Match Value  Choose type before providing match value

Inverse Match 

b. Type \* 드롭다운에서 일치하는 규칙에 포함할 요소의 유형을 선택합니다.

c. 일치 값 \* 필드에 선택한 요소의 유형에 따라 일치 값을 입력합니다.

- 버킷: 버킷 이름을 입력합니다.

- Bucket Regex: 버킷 이름 집합과 일치시키는 데 사용할 정규식을 입력합니다.

정규식이 고정 해제됩니다. {캐럿} 앵커를 사용하여 버킷 이름의 시작 부분에 일치시키고 \$ 앵커를 사용하여 이름 끝에 일치시킵니다.

- CIDR: 원하는 서브넷과 일치하는 IPv4 서브넷을 CIDR 표기법으로 입력합니다.

- 끝점: 기존 끝점 목록에서 끝점을 선택합니다. 로드 밸런서 엔드포인트 페이지에서 정의한 로드 밸런서 엔드포인트입니다.

- 테넌트: 기존 테넌트 목록에서 테넌트를 선택합니다. 테넌트 일치는 액세스 중인 버킷의 소유권을 기반으로 합니다. 버킷에 대한 익명 액세스는 버킷을 소유하는 테넌트와 일치합니다.

d. 방금 정의한 유형 및 일치 값과 일치하는 모든 `network traffic_except_traffic`을 일치시키려면 \* Inverse \* 확인란을 선택합니다. 그렇지 않으면 확인란을 선택하지 않은 상태로 둡니다.

예를 들어, 이 정책이 로드 밸런서 끝점 중 하나를 제외한 모든 항목에 적용되도록 하려면 제외할 로드 밸런서 끝점을 지정하고 \* Inverse \* 를 선택합니다.



하나 이상의 교자가 역마쳐인 여러 마처를 포함하는 정책의 경우 모든 요청과 일치하는 정책을 만들지 않도록 주의하십시오.

e. 적용 \* 을 클릭합니다.

규칙이 만들어지고 일치하는 규칙 테이블에 나열됩니다.

+ Create   Edit   Remove		
Type	Inverse Match	Match Value
• Bucket Regex	✓	control-ld+

Displaying 1 matching rule.

### Limits (Optional)

+ Create   Edit   Remove			
Type	Value	Type	Units
No limits found.			

Cancel   Save

a. 정책에 대해 생성할 각 규칙에 대해 이 단계를 반복합니다.

**i** 모든 규칙과 일치하는 트래픽은 정책에 의해 처리됩니다.

6. 필요에 따라 정책에 대한 제한을 생성합니다.

**i** 제한을 만들지 않더라도 StorageGRID는 정책과 일치하는 네트워크 트래픽을 모니터링할 수 있도록 메트릭을 수집합니다.

a. Limits \* 섹션에서 \* Create \* 를 클릭합니다.

Create Limit 대화상자가 나타납니다.

### Create Limit

#### Limits (Optional)

Type **?**

Aggregate rate limits in use. Per-request rate limits are not available. **?**

Value **?**

Cancel   Apply

b. Type \* 드롭다운에서 정책에 적용할 제한 유형을 선택합니다.

다음 목록에서 \* in \* 은 S3 또는 Swift 클라이언트에서 StorageGRID 로드 밸런서로의 트래픽을 나타내고 \*

out \* 은 로드 밸런서에서 S3 또는 Swift 클라이언트로 보내는 트래픽을 나타냅니다.

- 총 대역폭
- 총 대역폭 출력
- 동시 읽기 요청
- 동시 쓰기 요청
- 요청 당 대역폭
- 요청 당 대역폭 출력
- 읽기 요청 속도
- 쓰기 요청 속도



정책을 생성하여 애그리게이트 대역폭을 제한하거나 요청당 대역폭을 제한할 수 있습니다. 그러나 StorageGRID는 두 가지 유형의 대역폭을 동시에 제한할 수 없습니다. 애그리게이트 대역폭 제한은 제한 없는 트래픽에 약간의 성능 영향을 줄 수 있습니다.

대역폭 제한에 대해 StorageGRID는 설정된 제한 유형과 가장 일치하는 정책을 적용합니다. 예를 들어, 트래픽을 한 방향으로만 제한하는 정책이 있는 경우 대역폭 제한이 있는 추가 정책과 일치하는 트래픽이 있더라도 반대 방향의 트래픽은 무제한입니다. StorageGRID는 대역폭 제한에 대해 다음 순서로 ""가장 적합한"" 일치 항목을 구현합니다.

- 정확한 IP 주소(/32 마스크)
- 정확한 버킷 이름입니다
- 버킷 regex
- 테넌트
- 엔드포인트
- 일치하지 않는 CIDR 일치(NOT/32)
- 역 일치

c. 값 \* 필드에 선택한 제한 유형의 숫자 값을 입력합니다.

한계를 선택하면 예상 단위가 표시됩니다.

d. 적용 \* 을 클릭합니다.

제한이 생성되고 Limits 테이블에 나열됩니다.

Type	Inverse Match	Match Value
<input checked="" type="radio"/> Bucket Regex	<input checked="" type="checkbox"/>	control-ld+

Displaying 1 matching rule.

#### Limits (Optional)

Type	Value	Units
<input checked="" type="radio"/> Aggregate Bandwidth Out	10000000000	Bytes/Second

Displaying 1 limit.

Cancel Save

e. 정책에 추가할 각 제한에 대해 이 단계를 반복합니다.

예를 들어, SLA 계층에 대해 40Gbps 대역폭 제한을 생성하려면 한도 내의 총 대역폭 및 총 대역폭 제한을 생성하고 각 대역폭을 40Gbps로 설정합니다.



초당 메가바이트를 초당 기가비트 수로 변환하려면 8을 곱합니다. 예를 들어, 125MB/s는 1,000Mbps 또는 1Gbps와 동일합니다.

7. 규칙 및 제한 만들기를 마치면 \* 저장 \* 을 클릭합니다.

정책이 저장되고 트래픽 분류 정책 표에 나열됩니다.

#### Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

이제 S3 및 Swift 클라이언트 트래픽이 트래픽 분류 정책에 따라 처리됩니다. 트래픽 차트를 보고 정책이 기대하는 트래픽 제한을 적용하고 있는지 확인할 수 있습니다.

관련 정보

["로드 밸런싱 관리"](#)

["네트워크 트래픽 메트릭 보기"](#)



## 트래픽 분류 정책 편집

트래픽 분류 정책을 편집하여 이름 또는 설명을 변경하거나 정책에 대한 규칙 또는 제한을 생성, 편집 또는 삭제할 수 있습니다.

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

### 단계

1. 구성 \* > \* 네트워크 설정 \* > \* 트래픽 분류 \* 를 선택합니다.

트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

#### Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

	Name	Description	ID
<input type="radio"/>	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/>	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

2. 편집할 정책 왼쪽의 라디오 버튼을 선택합니다.
3. 편집 \* 을 클릭합니다.

트래픽 분류 정책 편집 대화 상자가 나타납니다.

## Edit Traffic Classification Policy "Fabric Pools"

### Policy

Name 



Fabric Pools

Description (optional)

Monitor Fabric Pools

### Matching Rules

Traffic that matches any rule is included in the policy.

 Create	 Edit	 Remove
Type	Inverse Match	Match Value
<input checked="" type="checkbox"/> CIDR		10.10.152.0/24
Displaying 1 matching rule.		

### Limits (Optional)

 Create	 Edit	 Remove
Type	Value	Units
No limits found.		

Cancel

Save

- 필요에 따라 일치하는 규칙 및 제한을 생성, 편집 또는 제거합니다.
  - 일치하는 규칙 또는 제한을 만들려면 \* 만들기 \* 를 클릭하고 규칙을 만들거나 제한을 만드는 방법에 대한 지침을 따릅니다.
  - 일치하는 규칙 또는 제한을 편집하려면 규칙 또는 제한에 대한 라디오 단추를 선택하고 \* 일치 규칙 \* 섹션 또는 \* 제한 \* 섹션에서 \* 편집 \* 을 클릭한 다음 규칙 만들기 또는 제한 만들기 지침을 따릅니다.
  - 일치하는 규칙 또는 제한을 제거하려면 규칙 또는 제한에 대한 라디오 단추를 선택하고 \* 제거 \* 를 클릭합니다. 그런 다음 \* 확인 \* 을 클릭하여 규칙 또는 제한을 제거할 것인지 확인합니다.
- 규칙 또는 제한을 만들거나 편집한 후에는 \* 적용 \* 을 클릭합니다.
- 정책 편집이 완료되면 \* 저장 \* 을 클릭합니다.

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 삭제하는 중입니다

트래픽 분류 정책이 더 이상 필요하지 않으면 삭제할 수 있습니다.

## 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

## 단계

1. 구성 \* > \* 네트워크 설정 \* > \* 트래픽 분류 \* 를 선택합니다.

트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

### Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddd894b

Displaying 2 traffic classification policies.

2. 삭제할 정책의 왼쪽에 있는 라디오 버튼을 선택합니다.
3. 제거 \* 를 클릭합니다.

경고 대화 상자가 나타납니다.



4. 확인 \* 을 클릭하여 정책 삭제를 확인합니다.

정책이 삭제됩니다.

## 네트워크 트래픽 메트릭 보기

트래픽 분류 정책 페이지에서 사용할 수 있는 그래프를 보고 네트워크 트래픽을 모니터링할 수 있습니다.

## 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

이 작업에 대해

기존 트래픽 분류 정책에 대해 로드 밸런서 서비스에 대한 메트릭을 확인하여 정책이 네트워크 전체의 트래픽을 성공적으로 제한하고 있는지 확인할 수 있습니다. 그래프의 데이터를 통해 정책을 조정해야 하는지 확인할 수 있습니다.

트래픽 분류 정책에 대해 설정된 제한이 없더라도 메트릭이 수집되고 그래프는 트래픽 추세를 이해하는 데 유용한 정보를 제공합니다.

단계

1. 구성 > \* 네트워크 설정 > \* 트래픽 분류 \* 를 선택합니다.

트래픽 분류 정책 페이지가 나타나고 기존 정책이 표에 나열됩니다.

### Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

<span>+ Create</span> <span>✎ Edit</span> <span>✕ Remove</span> <span>📊 Metrics</span>		
Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

2. 메트릭을 보려는 정책 왼쪽의 라디오 버튼을 선택합니다.
3. 메트릭 \* 을 클릭합니다.

새 브라우저 창이 열리고 트래픽 분류 정책 그래프가 나타납니다. 그래프에는 선택한 정책과 일치하는 트래픽에 대한 메트릭만 표시됩니다.

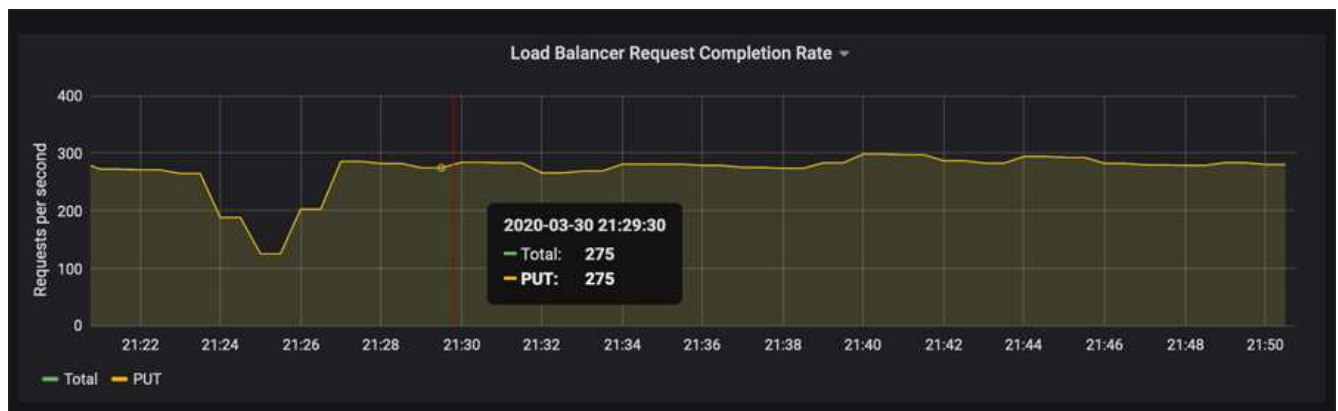
policy \* 폴다운을 사용하여 확인할 다른 정책을 선택할 수 있습니다.



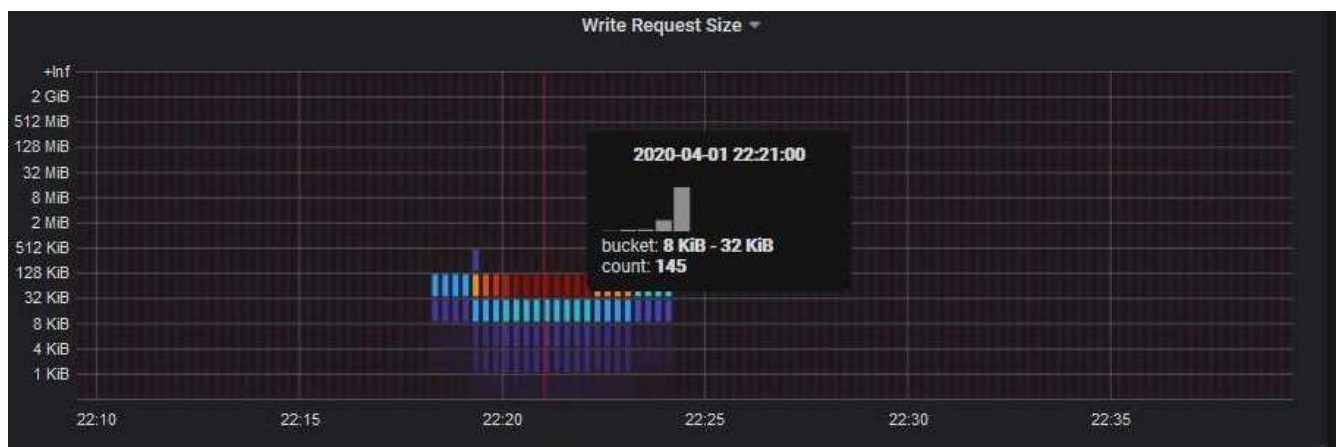
다음 그래프는 웹 페이지에 포함되어 있습니다.

- 로드 밸런서 요청 트래픽: 이 그래프는 로드 밸런서 끝점과 요청을 하는 클라이언트 간에 전송되는 데이터 처리량의 3분 이동 평균을 초당 비트 수로 제공합니다.
- 부하 분산 요청 완료율: 이 그래프는 초당 완료된 요청 수(GET, PUT, HEAD 및 DELETE)에 대한 3분의 이동 평균을 요청 유형별로 제공합니다. 이 값은 새 요청의 헤더가 검증되면 업데이트됩니다.
- 오류 응답 속도: 이 그래프는 오류 응답 코드로 분리된 초당 클라이언트에 반환된 오류 응답 수의 이동 평균을 3분으로 제공합니다.
- 평균 요청 기간(오류 없음): 이 그래프는 요청 유형(GET, PUT, HEAD, DELETE)별로 분류되는 요청 지속 시간의 3분 이동 평균을 제공합니다. 각 요청 기간은 부하 분산 서비스에서 요청 헤더를 구문 분석할 때 시작되어 완전한 응답 본문이 클라이언트로 반환될 때 종료됩니다.
- 개체 크기별 쓰기 요청 속도: 이 히트맵은 개체 크기에 따라 쓰기 요청이 완료되는 속도의 이동 평균을 3분으로 제공합니다. 이 컨텍스트에서 쓰기 요청은 PUT 요청에만 참조됩니다.
- 개체 크기별 읽기 요청 속도: 이 히트맵은 개체 크기에 따라 읽기 요청이 완료되는 속도에 대한 3분의 이동 평균을 제공합니다. 이 컨텍스트에서 읽기 요청은 요청 가져오기만 참조합니다. 히트맵의 색상은 개별 그래프 내의 개체 크기의 상대적 주파수를 나타냅니다. 차가운 색(예: 자주색 및 파란색)은 상대적으로 낮은 비율을 나타내고 따뜻한 색(예: 주황색 및 빨간색)은 상대적으로 높은 비율을 나타냅니다.

4. 커서를 선 그래프 위로 이동하면 그래프의 특정 부분에 있는 값의 팝업이 표시됩니다.



5. Heatmap 위로 커서를 이동하면 샘플의 날짜 및 시간, 카운트로 집계된 개체 크기 및 해당 기간 동안 초당 요청 수를 보여주는 팝업이 표시됩니다.



6. 왼쪽 상단의 \* 정책 \* 폴다운을 사용하여 다른 정책을 선택합니다.

선택한 정책에 대한 그래프가 나타납니다.

7. 또는 \* Support \* (지원 \*) 메뉴에서 그래프에 액세스하십시오.
  - a. 지원 \* > \* 도구 \* > \* 메트릭 \* 을 선택합니다.
  - b. 페이지의 \* Grafana \* 섹션에서 \* 트래픽 분류 정책 \* 을 선택합니다.
  - c. 페이지 왼쪽 상단의 풀다운 메뉴에서 정책을 선택합니다.

트래픽 분류 정책은 ID로 식별됩니다. 정책 ID는 트래픽 분류 정책 페이지에 나열되어 있습니다.

8. 그래프를 분석하여 정책에 따라 트래픽이 제한되는 빈도와 정책을 조정해야 하는지 여부를 결정합니다.

관련 정보

["모니터링 및 문제 해결"](#)

## 링크 비용은 얼마입니까

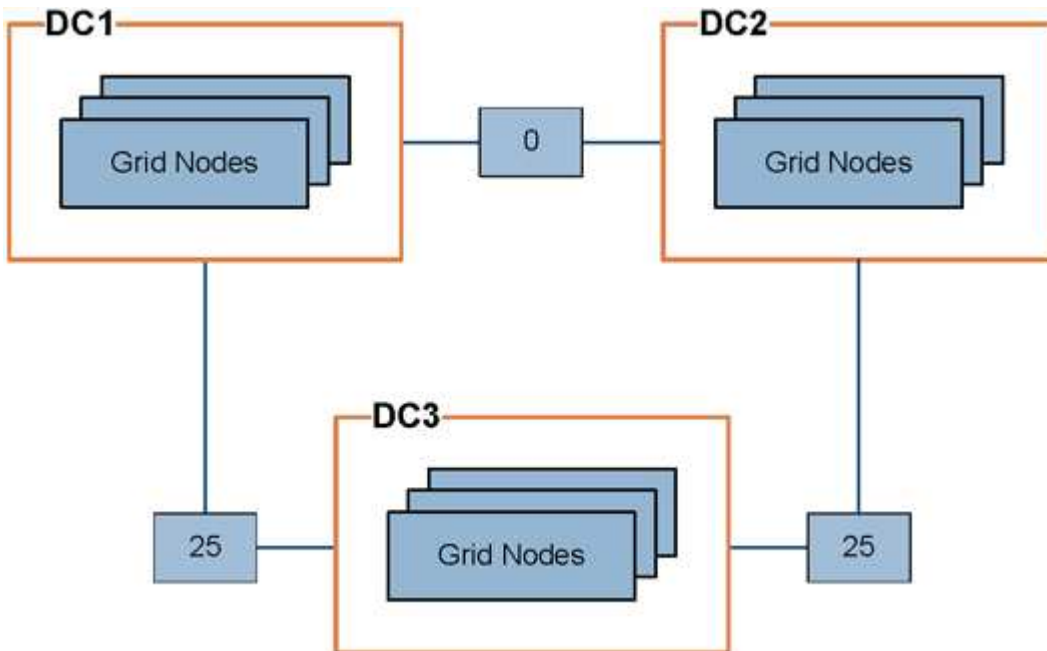
링크 비용을 사용하면 둘 이상의 데이터 센터 사이트가 있을 때 요청된 서비스를 제공하는 데이터 센터 사이트의 우선 순위를 지정할 수 있습니다. 링크 비용을 조정하여 사이트 간 지연 시간을 반영할 수 있습니다.

- 링크 비용은 오브젝트 검색을 수행하는 데 사용되는 오브젝트 복사본의 우선 순위를 지정하는 데 사용됩니다.
- 링크 비용은 그리드 관리 API 및 테넌트 관리 API에서 사용할 내부 StorageGRID 서비스를 결정하는 데 사용됩니다.
- 링크 비용은 게이트웨이 노드의 CLB 서비스에서 클라이언트 연결을 연결하는 데 사용됩니다.



CLB 서비스는 더 이상 사용되지 않습니다.

다이어그램에는 사이트 간에 구성된 링크 비용이 있는 세 개의 사이트 표가 표시됩니다.



- 게이트웨이 노드의 CLB 서비스는 동일한 데이터 센터 사이트의 모든 스토리지 노드 및 링크 비용이 0인 모든

데이터 센터 사이트에 클라이언트 연결을 균등하게 분산합니다.

이 예에서는 데이터 센터 사이트 1(DC1)의 게이트웨이 노드가 DC1의 스토리지 노드 및 DC2의 스토리지 노드로 클라이언트 접속을 균등하게 분산합니다. DC3의 게이트웨이 노드는 DC3의 스토리지 노드에만 클라이언트 접속을 전송합니다.

- 여러 개의 복제된 복제본으로 존재하는 객체를 검색할 때 StorageGRID는 가장 낮은 링크 비용을 가진 데이터 센터에서 복제본을 검색합니다.

이 예제에서 DC2의 클라이언트 응용 프로그램이 DC1과 DC3에 둘 다 저장된 객체를 검색할 경우 DC1에서 D2까지의 링크 비용은 DC3에서 DC2로 링크 비용보다 낮은 0이므로 DC2의 클라이언트 응용 프로그램이 DC1에서 객체를 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

관련 정보

["로드 균형 조정 작동 방식 - CLB 서비스"](#)

링크 비용을 업데이트하는 중입니다

사이트 간 지연 시간을 반영하기 위해 데이터 센터 사이트 간의 링크 비용을 업데이트할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 그리드 토폴로지 페이지 구성 권한이 있어야 합니다.

단계

1. 구성 \* > \* 네트워크 설정 \* > \* 링크 비용 \* 을 선택합니다.



## Link Cost

Updated: 2021-03-29 12:28:41 EDT

Site Names (1 - 2 of 2)

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	

Show  Records Per Page  Previous « 1 » Next

### Link Costs

Link Source	Link Destination	Actions
<input type="text" value="10"/>	<input type="text" value="20"/>	

2. 링크 원본 \* 에서 사이트를 선택하고 \* 링크 대상 \* 에서 0에서 100 사이의 비용 값을 입력합니다.

소스가 대상과 동일한 경우 링크 비용을 변경할 수 없습니다.

변경 사항을 취소하려면 를 클릭합니다 \* 되돌리기 \*.

3. 변경 내용 적용 \* 을 클릭합니다.

## AutoSupport 구성

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

### AutoSupport 메시지에 포함된 정보입니다

AutoSupport 메시지는 다음과 같은 정보가 포함됩니다.


- StorageGRID 소프트웨어 버전입니다
- 운영 체제 버전입니다
- 시스템 레벨 및 위치 레벨 속성 정보
- 최근 알림 및 알람(기존 시스템)
- 내역 데이터를 포함하여 모든 그리드 작업의 현재 상태입니다
- 이벤트 정보는 \* 노드 \* \* Grid Node \* \* 이벤트 \* 페이지에 나열되어 있습니다
- 관리 노드 데이터베이스 사용



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

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

The AutoSupport feature is disabled. You should enable AutoSupport to allow StorageGRID to send health and status messages to technical support for proactive monitoring and troubleshooting.

"x" 기호를 선택할 수 있습니다  을 눌러 메시지를 닫습니다. AutoSupport가 비활성화된 경우에도 브라우저 캐시가 지워질 때까지 메시지가 다시 나타나지 않습니다.

## Active IQ 사용

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 설정에 액세스하는 중입니다

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

## AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings Results

---

### Protocol Details

Protocol ?  HTTPS  HTTP  SMTP

NetApp Support Certificate Validation ?

---

### AutoSupport Details

Enable Weekly AutoSupport ?

Enable Event-Triggered AutoSupport ?

Enable AutoSupport on Demand ?

---

### Additional AutoSupport Destination

Enable Additional AutoSupport Destination ?

## AutoSupport 메시지를 보내는 프로토콜입니다

다음 세 가지 프로토콜 중 하나를 선택하여 AutoSupport 메시지를 보낼 수 있습니다.

- HTTPS
- HTTP
- SMTP

HTTPS 또는 HTTP를 사용하여 AutoSupport 메시지를 보내는 경우 관리자 노드와 기술 지원 간에 투명하지 않은 프록시 서버를 구성할 수 있습니다.

AutoSupport 메시지의 프로토콜로 SMTP를 사용하는 경우 SMTP 메일 서버를 구성해야 합니다.

## AutoSupport 옵션

다음 옵션을 조합하여 기술 지원 부서에 AutoSupport 메시지를 보낼 수 있습니다.

- \* Weekly \*: AutoSupport 메시지를 매주 한 번씩 자동으로 전송합니다. 기본 설정: 사용.
- \* 이벤트 트리거 \*: 1시간마다 또는 중요한 시스템 이벤트가 발생할 때 AutoSupport 메시지를 자동으로 전송합니다. 기본 설정: 사용.
- \* 주문형 \*: 기술 지원 부서에서 StorageGRID 시스템에서 AutoSupport 메시지를 자동으로 보내도록 요청할 수 있습니다. 이 메시지는 문제가 활발하게 발생하는 경우 유용합니다(HTTPS AutoSupport 전송 프로토콜 필요). 기본 설정: 사용 안 함
- \* 사용자 트리거 \*: 언제든지 수동으로 AutoSupport 메시지를 보냅니다.

## AutoSupport 메시지에 대한 프로토콜 지정

세 가지 프로토콜 중 하나를 사용하여 AutoSupport 메시지를 보낼 수 있습니다.

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 또는 기타 그리드 구성 권한이 있어야 합니다.
- AutoSupport 메시지를 보내는 데 HTTPS 또는 HTTP 프로토콜을 사용할 경우, 직접 또는 프록시 서버를 사용하여 기본 관리자 노드에 대한 아웃바운드 인터넷 액세스를 제공해야 합니다(인바운드 연결은 필요하지 않음).
- HTTPS 또는 HTTP 프로토콜을 사용하고 프록시 서버를 사용하려는 경우 관리자 프록시 서버를 구성해야 합니다.
- AutoSupport 메시지의 프로토콜로 SMTP를 사용하려면 SMTP 메일 서버를 구성해야 합니다. 알람 이메일 알림(레거시 시스템)에 동일한 메일 서버 구성이 사용됩니다.

### 이 작업에 대해

AutoSupport 메시지는 다음 프로토콜을 사용하여 보낼 수 있습니다.

- \* HTTPS \*: 새 설치에 대한 기본 권장 설정입니다. HTTPS 프로토콜은 포트 443을 사용합니다. AutoSupport 온디맨드 기능을 활성화하려면 HTTPS 프로토콜을 사용해야 합니다.
- \* HTTP \*: 인터넷을 통해 데이터를 전송할 때 프록시 서버가 HTTPS로 변환되는 신뢰할 수 있는 환경에서 사용되지 않는 한 이 프로토콜은 안전하지 않습니다. HTTP 프로토콜은 포트 80을 사용합니다.
- \* SMTP : **AutoSupport** 메시지를 이메일로 보내려면 이 옵션을 사용합니다. **AutoSupport** 메시지의 프로토콜로 **SMTP**를 사용하는 경우 레거시 전자 메일 설정 페이지(지원 \* 알람(레거시) \* \* 레거시 전자 메일 설정 \* )에서 SMTP 메일 서버를 구성해야 합니다.



SMTP는 StorageGRID 11.2 릴리스 이전에 AutoSupport 메시지에 사용할 수 있는 유일한 프로토콜이었습니다. 처음에 이전 버전의 StorageGRID를 설치한 경우 SMTP가 선택된 프로토콜일 수 있습니다.

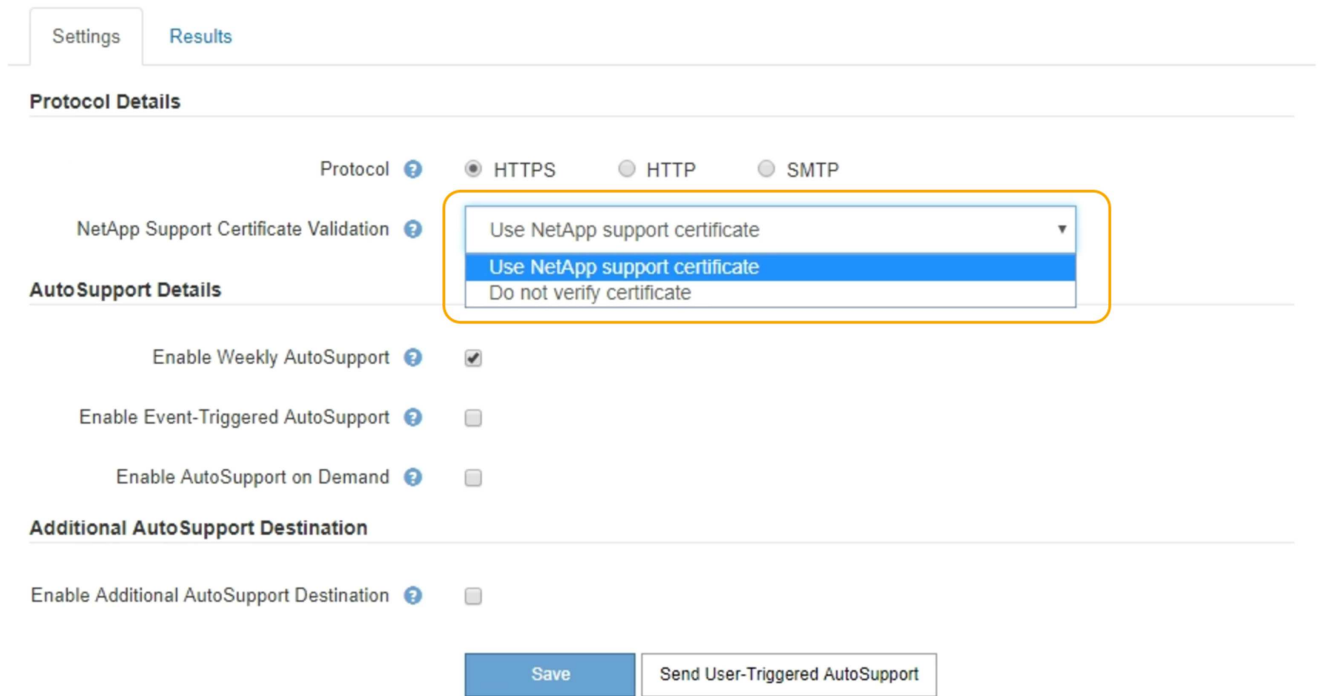
설정한 프로토콜은 모든 유형의 AutoSupport 메시지를 전송하는 데 사용됩니다.

### 단계

1. 지원 \* > \* 도구 \* > \* AutoSupport \* 를 선택합니다.

AutoSupport 페이지가 나타나고 \* 설정 \* 탭이 선택됩니다.

2. AutoSupport 메시지를 보내는 데 사용할 프로토콜을 선택합니다.



3. NetApp 지원 인증서 검증 \* 에 대한 항목을 선택하십시오.

- NetApp 지원 인증서 사용(기본값): 인증서 검증으로 AutoSupport 메시지를 안전하게 전송할 수 있습니다. NetApp 지원 인증서는 StorageGRID 소프트웨어와 함께 이미 설치되어 있습니다.
- 인증서 확인 안 함: 인증서에 일시적인 문제가 있는 경우와 같이 인증서 유효성 검사를 사용하지 않는 좋은 이유가 있는 경우에만 이 옵션을 선택합니다.

4. 저장 \* 을 선택합니다.

매주, 사용자 트리거 및 이벤트 트리거 메시지는 선택한 프로토콜을 사용하여 전송됩니다.

관련 정보

["관리자 프록시 설정을 구성합니다"](#)

## AutoSupport 온디맨드 를 지원합니다

AutoSupport On Demand는 기술 지원이 활발하게 진행 중인 문제를 해결하는 데 도움이 될 수 있습니다. AutoSupport On Demand를 활성화하면 기술 지원 부서에서 사용자의 개입 없이 AutoSupport 메시지를 보내도록 요청할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 또는 기타 그리드 구성 권한이 있어야 합니다.
- 주간 AutoSupport 메시지를 사용하도록 설정해야 합니다.
- 전송 프로토콜을 HTTPS로 설정해야 합니다.

이 작업에 대해

이 기능을 활성화하면 기술 지원 부서에서 StorageGRID 시스템에 AutoSupport 메시지를 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 \* 를 선택합니다.

AutoSupport 페이지가 나타나고 \* 설정 \* 탭이 선택됩니다.

2. 페이지의 \* 프로토콜 세부 정보 \* 섹션에서 HTTPS 라디오 버튼을 선택합니다.

The screenshot shows the 'Settings' tab for AutoSupport configuration. Under 'Protocol Details', the 'Protocol' is set to 'HTTPS'. Under 'AutoSupport Details', 'Enable Weekly AutoSupport' and 'Enable AutoSupport on Demand' are checked. Under 'Additional AutoSupport Destination', 'Enable Additional AutoSupport Destination' is unchecked. There are 'Save' and 'Send User-Triggered AutoSupport' buttons at the bottom.

3. Weekly AutoSupport \* 활성화 확인란을 선택합니다.
4. AutoSupport On Demand \* 활성화 확인란을 선택합니다.
5. 저장 \* 을 선택합니다.

AutoSupport On Demand가 활성화되어 있으면 기술 지원 부서에서 AutoSupport On Demand 요청을 StorageGRID로 보낼 수 있습니다.

## 주간 **AutoSupport** 메시지 비활성화

기본적으로 StorageGRID 시스템은 AutoSupport 메시지를 일주일에 한 번 NetApp Support에 보내도록 구성됩니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 또는 기타 그리드 구성 권한이 있어야 합니다.

이 작업에 대해

Weekly AutoSupport 메시지 전송 시기를 확인하려면 \* AutoSupport \* > \* Results \* 페이지의 \* Weekly AutoSupport \* 에서 \* Next Scheduled Time \* 을 참조하십시오.

Settings Results

**Weekly AutoSupport**

Next Scheduled Time ? 2021-02-12 00:20:00 EST

Most Recent Result ? Idle (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

언제든지 AutoSupport 메시지 자동 전송을 사용하지 않도록 설정할 수 있습니다.

단계

1. 지원 \* > \* 도구 \* > \* AutoSupport \* 를 선택합니다.  
AutoSupport 페이지가 나타나고 \* 설정 \* 탭이 선택됩니다.
2. Weekly AutoSupport \* 활성화 확인란의 선택을 취소합니다.

Settings Results

**Protocol Details**

Protocol ?  HTTPS  HTTP  SMTP

NetApp Support Certificate Validation ? Use NetApp support certificate

**AutoSupport Details**

Enable Weekly AutoSupport ?

Enable Event-Triggered AutoSupport ?

AutoSupport On Demand can only be enabled when the protocol is HTTPS and Weekly AutoSupport is enabled. When you enable AutoSupport on Demand, technical support can request that your StorageGRID system send AutoSupport messages automatically.

**Additional AutoSupport Destination**

Enable Additional AutoSupport Destination ?

Save Send User-Triggered AutoSupport

3. 저장 \* 을 선택합니다.

## 이벤트 트리거 **AutoSupport** 메시지 비활성화

기본적으로 StorageGRID 시스템은 중요한 알림 또는 기타 중요한 시스템 이벤트가 발생할 경우 NetApp 지원에 AutoSupport 메시지를 보내도록 구성됩니다.

## 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 또는 기타 그리드 구성 권한이 있어야 합니다.

## 이 작업에 대해

언제든지 이벤트 트리거 AutoSupport 메시지를 사용하지 않도록 설정할 수 있습니다.



e-메일 알림 시스템 전체를 억제하면 이벤트 트리거 AutoSupport 메시지도 표시되지 않습니다. (\* 구성 \* 시스템 설정 \* 디스플레이 옵션 \* 을 선택합니다. 그런 다음 \* 알림 모두 표시 안 함 \* 을 선택합니다.)

## 단계

1. 지원 \* > \* 도구 \* > \* AutoSupport \* 를 선택합니다.

AutoSupport 페이지가 나타나고 \* 설정 \* 탭이 선택됩니다.

2. 이벤트 트리거 AutoSupport\* 활성화 확인란의 선택을 취소합니다.

Settings Results

**Protocol Details**

Protocol ?  HTTPS  HTTP  SMTP

NetApp Support Certificate Validation ? Use NetApp support certificate ▼

**AutoSupport Details**

Enable Weekly AutoSupport ?

Enable Event-Triggered AutoSupport ?

AutoSupport On Demand can only be enabled when the protocol is HTTPS and Weekly AutoSupport is enabled. When you enable AutoSupport on Demand, technical support can request that your StorageGRID system send AutoSupport messages automatically.

**Additional AutoSupport Destination**

Enable Additional AutoSupport Destination ?

Save Send User-Triggered AutoSupport

3. 저장 \* 을 선택합니다.

## 수동으로 **AutoSupport** 메시지 트리거

StorageGRID 시스템 관련 문제 해결에 대한 기술 지원을 받으려면 AutoSupport 메시지를 수동으로 전송할 수 있습니다.

## 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

- 루트 액세스 또는 기타 그리드 구성 권한이 있어야 합니다.

#### 단계

1. 지원 \* > \* 도구 \* > \* AutoSupport \* 를 선택합니다.

AutoSupport 페이지가 나타나고 \* 설정 \* 탭이 선택됩니다.

2. Send User-triggered AutoSupport \* 를 선택합니다.

StorageGRID는 기술 지원 부서에 AutoSupport 메시지를 보내려고 시도합니다. 시도가 성공하면 \* Results \* 탭의 \* Most Recent Result \* 및 \* Last Successful Time \* 값이 업데이트됩니다. 문제가 있는 경우 \* 가장 최근의 결과 \* 값이 "실패"로 업데이트되고 StorageGRID는 AutoSupport 메시지를 다시 전송하지 않습니다.



사용자 트리거 AutoSupport 메시지를 보낸 후 1분 후 브라우저에서 AutoSupport 페이지를 새로 고쳐 가장 최근 결과에 액세스합니다.

## AutoSupport 대상을 추가하는 중입니다

AutoSupport를 활성화하면 상태 및 상태 메시지가 NetApp 지원으로 전송됩니다. 모든 AutoSupport 메시지에 대해 하나의 추가 대상을 지정할 수 있습니다.

#### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 또는 기타 그리드 구성 권한이 있어야 합니다.

#### 이 작업에 대해

AutoSupport 메시지를 보내는 데 사용되는 프로토콜을 확인하거나 변경하려면 AutoSupport 프로토콜 지정 지침을 참조하십시오.



SMTP 프로토콜을 사용하여 AutoSupport 메시지를 추가 대상으로 보낼 수는 없습니다.

### "AutoSupport 메시지에 대한 프로토콜 지정"

#### 단계

1. 지원 \* > \* 도구 \* > \* AutoSupport \* 를 선택합니다.

AutoSupport 페이지가 나타나고 \* 설정 \* 탭이 선택됩니다.

2. 추가 AutoSupport 대상 사용 \* 을 선택합니다.

추가 AutoSupport 대상 필드가 나타납니다.



### Additional AutoSupport Destination

Enable Additional AutoSupport Destination

Hostname

Port

Certificate Validation

You are not using a TLS certificate to secure the connection to the additional AutoSupport destination.

Save

Send User-Triggered AutoSupport

3. 추가 AutoSupport 대상 서버의 서버 호스트 이름 또는 IP 주소를 입력합니다.



하나의 추가 대상만 입력할 수 있습니다.

4. 추가 AutoSupport 대상 서버에 연결하는 데 사용되는 포트를 입력합니다. 기본값은 HTTP의 경우 포트 80, HTTPS의 경우 포트 443입니다.

5. 인증서 유효성 검사와 함께 AutoSupport 메시지를 보내려면 \* 인증서 유효성 검사 \* 드롭다운에서 \* 사용자 지정 CA 번들 사용 \* 을 선택합니다. 그런 다음 다음 다음 중 하나를 수행합니다.

- 편집 도구를 사용하여 인증서 체인 순서대로 연결된 \* CA 번들 \* 필드에 PEM 인코딩된 각 CA 인증서 파일의 모든 내용을 복사하여 붙여 넣습니다. 반드시 포함해야 합니다 -----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 선택합니다.

### Additional AutoSupport Destination

Enable Additional AutoSupport Destination

Hostname

Port

Certificate Validation

CA Bundle

Browse

- 찾아보기 \* 를 선택하고 인증서가 포함된 파일을 찾은 다음 \* 열기 \* 를 선택하여 파일을 업로드합니다. 인증서 유효성 검사를 통해 AutoSupport 메시지를 안전하게 전송할 수 있습니다.

6. 인증서 유효성 검사 없이 AutoSupport 메시지를 보내려면 \* 인증서 유효성 검사 \* 드롭다운에서 \* 인증서 확인 안 함 \* 을 선택합니다.

인증서에 일시적인 문제가 있는 경우와 같이 인증서 유효성 검사를 사용하지 않는 좋은 이유가 있는 경우에만 이 옵션을 선택합니다.

"추가 AutoSupport 대상에 대한 연결을 보호하기 위해 TLS 인증서를 사용하고 있지 않습니다."라는 메시지가 나타납니다.

7. 저장 \* 을 선택합니다.

향후 모든 주별, 이벤트 트리거 및 사용자 트리거 AutoSupport 메시지가 추가 대상으로 전송됩니다.

## StorageGRID를 통해 E-Series AutoSupport 메시지 전송

스토리지 어플라이언스의 관리 포트가 아닌 StorageGRID 관리 노드를 통해 E-Series SANtricity 시스템 관리자 AutoSupport 메시지를 기술 지원 부서에 보낼 수 있습니다.

필요한 것

- 지원되는 웹 브라우저를 사용하여 Grid Manager에 로그인했습니다.
- 스토리지 어플라이언스 관리자 권한이나 루트 액세스 권한이 있습니다.



그리드 관리자를 사용하여 SANtricity 시스템 관리자에 액세스하려면 SANtricity 펌웨어 8.70 이상이 있어야 합니다.

이 작업에 대해

E-Series AutoSupport 메시지에는 스토리지 하드웨어의 세부 정보가 포함되어 있으며 StorageGRID 시스템에서 보내는 다른 AutoSupport 메시지보다 더 구체적으로 나타납니다.

어플라이언스의 관리 포트를 사용하지 않고 StorageGRID 관리 노드를 통해 AutoSupport 메시지가 전송되도록 SANtricity 시스템 관리자에서 특수 프록시 서버 주소를 구성합니다. 이렇게 전송되는 AutoSupport 메시지는 그리드 관리자에서 구성되었을 수 있는 기본 설정 보낸 사람 및 관리자 프록시 설정을 기준으로 합니다.

Grid Manager에서 Admin 프록시 서버를 구성하려면 관리 프록시 설정 구성 지침을 참조하십시오.

### "관리자 프록시 설정을 구성합니다"



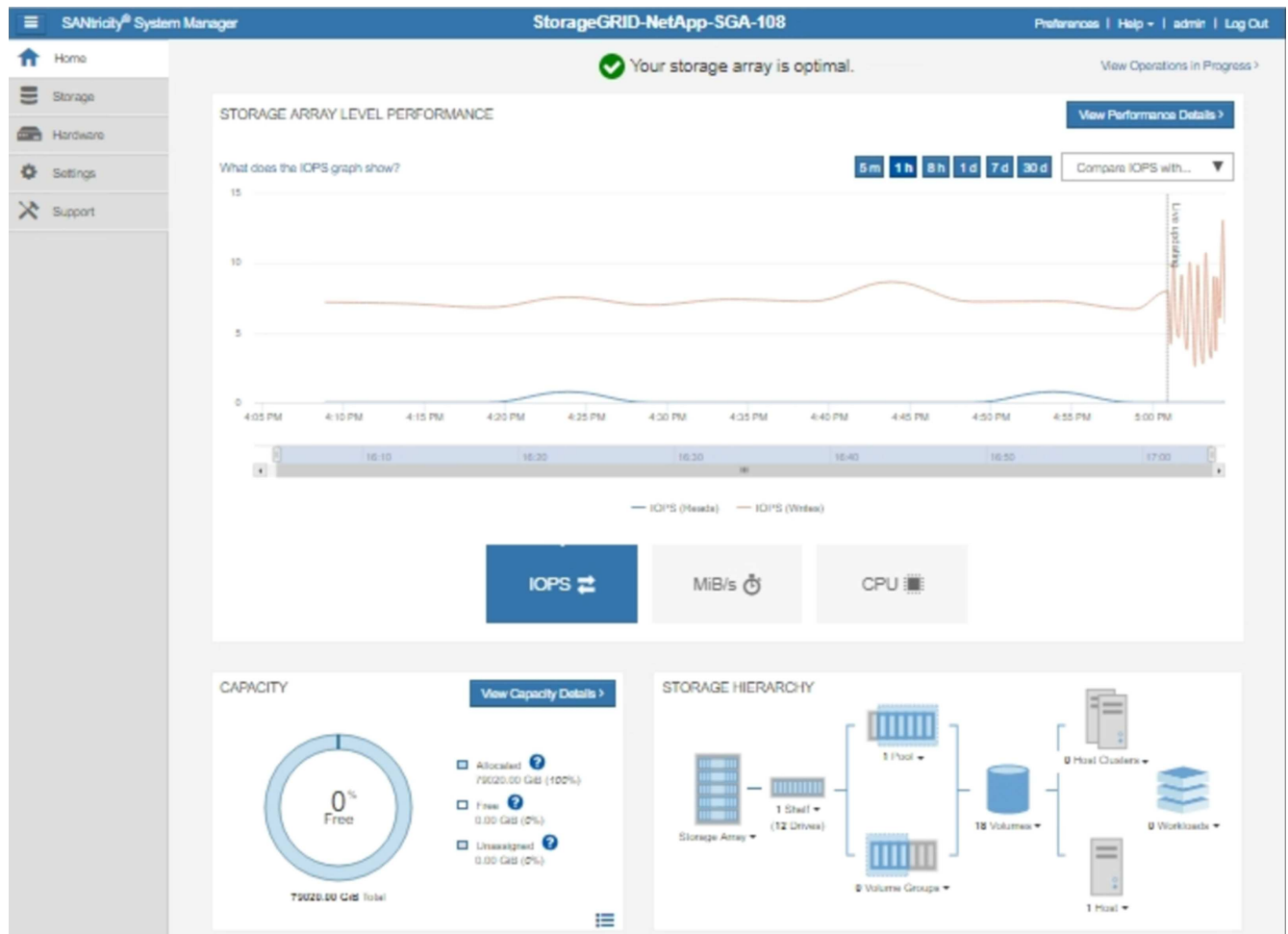
이 절차는 E-Series AutoSupport 메시지용으로 StorageGRID 프록시 서버를 구성하는 경우에만 적용됩니다. E-Series AutoSupport 구성 정보에 대한 자세한 내용은 E-Series 문서 센터를 참조하십시오.

["NetApp E-Series 시스템 설명서 센터 를 참조하십시오"](#)

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 선택합니다.

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.

## Configure AutoSupport Delivery Method ✕

Select AutoSupport dispatch delivery method...

HTTPS  
 HTTP  
 Email

**HTTPS delivery settings** Show destination address

Connect to support team...

Directly ?  
 via Proxy server ?

Host address ?

Port number ?

My proxy server requires authentication  
 via Proxy auto-configuration script (PAC) ?

6. 전달 방법으로 \* HTTPS \* 를 선택합니다.



HTTPS 프로토콜을 활성화하는 인증서가 미리 설치되어 있습니다.

7. 프록시 서버를 통해 \* 를 선택합니다.

8. 를 입력합니다 tunnel-host 호스트 주소 \* 용.

tunnel-host 는 관리 노드를 사용하여 E-Series AutoSupport 메시지를 보내는 특수 주소입니다.

9. 를 입력합니다 10225 포트 번호 \*.

10225 은 어플라이언스의 E-Series 컨트롤러에서 AutoSupport 메시지를 수신하는 StorageGRID 프록시 서버의 포트 번호입니다.

10. AutoSupport 프록시 서버의 라우팅 및 구성을 테스트하려면 \* 구성 테스트 \* 를 선택합니다.

올바른 경우 녹색 배너에 "Your AutoSupport configuration has been verified(사용자의 구성이 확인되었습니다)" 메시지가 나타납니다.

테스트에 실패하면 빨간색 배너에 오류 메시지가 나타납니다. StorageGRID DNS 설정 및 네트워킹을 확인하고 기본 센터 관리자 노드가 NetApp Support 사이트에 연결할 수 있는지 확인한 다음 테스트를 다시 시도하십시오.

11. 저장 \* 을 선택합니다.

구성이 저장되고 "AutoSupport delivery method has been configured(전달 방법이 구성되었습니다)" 확인 메시지가 나타납니다.

## AutoSupport 메시지 문제 해결

AutoSupport 메시지 전송 시도가 실패하면 StorageGRID 시스템은 AutoSupport 메시지 유형에 따라 다른 작업을 수행합니다. 지원 \* \* 도구 \* AutoSupport \* \* 결과 \* 를 선택하여 AutoSupport 메시지의 상태를 확인할 수 있습니다.



e-메일 알림 시스템 전체를 억제하면 이벤트 트리거 AutoSupport 메시지가 표시되지 않습니다. (\* 구성 \* 시스템 설정 \* 디스플레이 옵션 \* 을 선택합니다. 그런 다음 \* 알림 모두 표시 안 함 \* 을 선택합니다.)

AutoSupport 메시지가 전송되지 않으면 \* AutoSupport \* 페이지의 \* 결과 \* 탭에 ""실패""가 나타납니다.

## AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings

Results

### Weekly AutoSupport

Next Scheduled Time ? 2020-12-11 23:30:00 EST

Most Recent Result ? Idle (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

### Event-Triggered AutoSupport

Most Recent Result ? N/A (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

### User-Triggered AutoSupport

Most Recent Result ? Failed (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

### AutoSupport On Demand

AutoSupport On Demand messages are only sent to NetApp Support.

Most Recent Result ? N/A (NetApp Support)

Last Successful Time ? N/A (NetApp Support)

## Weekly AutoSupport 메시지 실패

Weekly AutoSupport 메시지가 전송되지 않으면 StorageGRID 시스템에서 다음 작업을 수행합니다.

1. 가장 최근의 결과 속성을 다시 시도하도록 업데이트합니다.
2. 1시간 동안 4분마다 15회 AutoSupport 메시지를 재전송하려고 시도합니다.
3. 전송 실패 1시간 후 는 가장 최근의 결과 속성을 실패 로 업데이트합니다.
4. 다음에 예약된 시간에 AutoSupport 메시지를 다시 보내려고 시도합니다.
5. NMS 서비스를 사용할 수 없어 메시지 실패 시, 7일 이전에 메시지를 보낸 경우, 정규 AutoSupport 일정을 유지 관리합니다.
6. NMS 서비스를 다시 사용할 수 있는 경우 7일 이상 메시지를 보내지 않은 경우 에서 즉시 AutoSupport 메시지를 보냅니다.

사용자가 트리거하거나 이벤트가 트리거된 **AutoSupport** 메시지 오류입니다

사용자 트리거 또는 이벤트 트리거 AutoSupport 메시지가 전송되지 않으면 StorageGRID 시스템에서 다음 작업을 수행합니다.

1. 오류가 알려진 경우 오류 메시지를 표시합니다. 예를 들어, 사용자가 올바른 이메일 구성 설정을 제공하지 않고 SMTP 프로토콜을 선택하면 다음 오류가 표시됩니다. AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.
2. 메시지를 다시 보내지 않습니다.
3. 에 오류를 기록합니다 nms.log.

오류가 발생하고 SMTP가 선택된 프로토콜인 경우, StorageGRID 시스템의 이메일 서버가 올바르게 구성되어 있고 이메일 서버가 실행 중인지 확인하십시오(\* 지원 \* 알람(레거시) \*\* 레거시 이메일 설정 \*). AutoSupport 페이지에 다음과 같은 오류 메시지가 나타날 수 있습니다. AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.

에서 전자 메일 서버 설정을 구성하는 방법에 대해 알아보십시오 ["모니터 램프; 문제 해결 지침"](#).

### AutoSupport 메시지 오류 해결

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 messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.

관련 정보

["모니터링 및 문제 해결"](#)

## 스토리지 노드 관리

스토리지 노드는 디스크 스토리지 용량 및 서비스를 제공합니다. 스토리지 노드를 관리하려면 각 노드에서 사용 가능한 공간의 양을 모니터링하고, 워터마크 설정을 사용하고, 스토리지 노드 구성 설정을 적용해야 합니다.

- ["스토리지 노드 정의"](#)
- ["스토리지 옵션 관리"](#)
- ["오브젝트 메타데이터 스토리지 관리"](#)
- ["저장된 개체에 대한 전역 설정 구성"](#)
- ["스토리지 노드 구성 설정입니다"](#)
- ["전체 스토리지 노드 관리"](#)

### 스토리지 노드 정의

스토리지 노드: 오브젝트 데이터 및 메타데이터를 관리하고 저장합니다. 각 StorageGRID 시스템에는 3개 이상의 스토리지 노드가 있어야 합니다. 여러 사이트가 있는 경우 StorageGRID 시스템 내의 각 사이트에도 3개의 스토리지 노드가 있어야 합니다.



스토리지 노드에는 디스크에서 오브젝트 데이터와 메타데이터를 저장, 이동, 확인 및 검색하는 데 필요한 서비스와 프로세스가 포함되어 있습니다. 노드 \* 페이지에서 스토리지 노드에 대한 자세한 정보를 볼 수 있습니다.

## ADC 서비스의 정의

ADC(관리 도메인 컨트롤러) 서비스는 그리드 노드와 상호 연결을 인증합니다. ADC 서비스는 사이트의 처음 세 스토리지 노드 각각에 호스팅됩니다.

ADC 서비스는 서비스의 위치 및 가용성을 포함한 토폴로지 정보를 유지합니다. 그리드 노드에 다른 그리드 노드의 정보가 필요하거나 다른 그리드 노드에서 작업을 수행해야 하는 경우 ADC 서비스에 문의하여 요청을 처리할 최적의 그리드 노드를 찾습니다. 또한 ADC 서비스는 StorageGRID 배포의 구성 번들의 복사본을 유지하여 그리드 노드가 현재 구성 정보를 검색할 수 있도록 합니다. 그리드 토폴로지 페이지(\* 지원 \* 그리드 토폴로지 \*)에서 스토리지 노드에 대한 ADC 정보를 볼 수 있습니다.

분산 및 분산 작업을 용이하게 하기 위해 각 ADC 서비스는 인증서, 구성 번들 및 서비스 및 토폴로지에 대한 정보를 StorageGRID 시스템의 다른 ADC 서비스와 동기화합니다.

일반적으로 모든 그리드 노드는 하나 이상의 ADC 서비스에 대한 연결을 유지합니다. 이렇게 하면 그리드 노드가 항상 최신 정보에 액세스할 수 있습니다. 그리드 노드가 연결되면 다른 그리드 노드 "" 인증서를 캐시하여 ADC 서비스를 사용할 수 없는 경우에도 시스템이 알려진 그리드 노드를 계속 사용할 수 있도록 합니다. 새 그리드 노드는 ADC 서비스를 통해서만 연결을 설정할 수 있습니다.

ADC 서비스는 각 그리드 노드의 연결을 통해 토폴로지 정보를 수집할 수 있습니다. 이 그리드 노드 정보에는 CPU 로드, 사용 가능한 디스크 공간(스토리지가 있는 경우), 지원되는 서비스 및 그리드 노드의 사이트 ID가 포함됩니다. 다른 서비스에서는 ADC 서비스에 토폴로지 쿼리를 통한 토폴로지 정보를 요청합니다. ADC 서비스는 StorageGRID 시스템에서 수신한 최신 정보로 각 쿼리에 응답합니다.

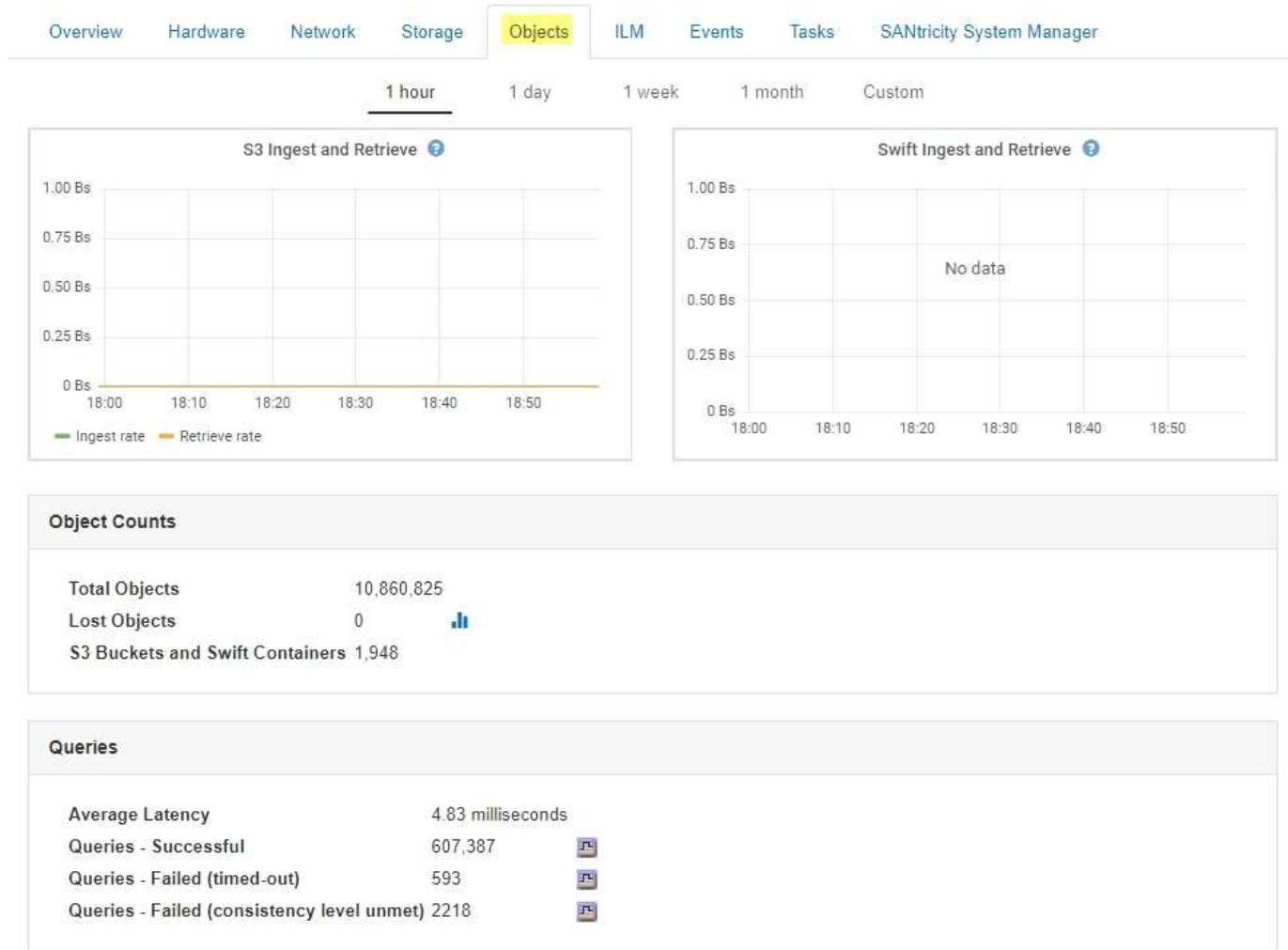
## DDS 서비스란 무엇입니까

스토리지 노드에서 호스팅되는 DDS(Distributed Data Store) 서비스는 Cassandra 데이터베이스와 상호 작용하여 StorageGRID 시스템에 저장된 객체 메타데이터에 대한 백그라운드 작업을 수행합니다.

개체 수

DDS 서비스는 StorageGRID 시스템으로 수집된 총 객체 수와 시스템의 지원되는 인터페이스(S3 또는 Swift)를 통해 수집된 총 객체 수를 추적합니다.

스토리지 노드의 노드 페이지 오브젝트 탭에서 총 오브젝트 수를 확인할 수 있습니다.



쿼리

특정 DDS 서비스를 통해 메타데이터 저장소에 대한 쿼리를 실행하는 데 걸리는 평균 시간, 성공한 총 쿼리 수 및 제한 시간 문제로 인해 실패한 총 쿼리 수를 확인할 수 있습니다.

쿼리 정보를 검토하여 메타데이터 저장소, Cassandra의 상태를 모니터링할 수 있으며, 이는 시스템의 수집 및 검색 성능에 영향을 줍니다. 예를 들어, 평균 쿼리의 지연 시간이 느리고 시간 초과로 인해 실패한 쿼리의 수가 많은 경우 메타데이터 저장소의 로드가 높거나 다른 작업을 수행해야 할 수 있습니다.

일관성 오류로 인해 실패한 총 쿼리 수를 볼 수도 있습니다. 정합성 보장 레벨 오류는 특정 DDS 서비스를 통해 쿼리를 수행할 때 사용 가능한 메타데이터 저장소의 수가 부족하기 때문에 발생합니다.

진단 페이지를 사용하여 그리드의 현재 상태에 대한 추가 정보를 얻을 수 있습니다. 을 참조하십시오 ["진단 프로그램 실행 중"](#).

일관성 보장 및 제어

StorageGRID는 새로 생성된 개체에 대해 쓰기 후 읽기 일관성을 보장합니다. 성공적으로 완료된 PUT 작업 이후의 모든 GET 작업은 새로 작성된 데이터를 읽을 수 있습니다. 기존 오브젝트, 메타데이터 업데이트 및 삭제를 덮어쓰더라도 결국 일관성이 유지됩니다.

## LDR 서비스의 정의

각 스토리지 노드에 의해 호스팅되는 LDR(Local Distribution Router) 서비스는 StorageGRID 시스템의 콘텐츠 전송을 처리합니다. 콘텐츠 전송에는 데이터 저장, 라우팅 및 요청 처리를 비롯한 다양한 작업이 포함됩니다. LDR 서비스는 데이터 전송 로드 및 데이터 트래픽 기능을 처리하여 StorageGRID 시스템의 대부분의 작업을 수행합니다.

LDR 서비스는 다음 작업을 처리합니다.

- 쿼리
- ILM(정보 수명 주기 관리) 작업
- 개체 삭제
- 오브젝트 데이터 스토리지
- 다른 LDR 서비스(스토리지 노드)에서 오브젝트 데이터 전송
- 데이터 스토리지 관리
- 프로토콜 인터페이스(S3 및 Swift)

또한 LDR 서비스는 StorageGRID 시스템이 수집된 각 오브젝트에 할당하는 고유 "UUID(Content Handles)"(UUID)에 S3 및 Swift 객체의 매핑을 관리합니다.

### 쿼리

LDR 쿼리에는 검색 및 아카이브 작업 중 개체 위치에 대한 쿼리가 포함됩니다. 쿼리를 실행하는 데 걸리는 평균 시간, 성공한 쿼리의 총 수 및 제한 시간 문제로 인해 실패한 쿼리의 총 수를 확인할 수 있습니다.

쿼리 정보를 검토하여 메타데이터 저장소의 상태를 모니터링하여 시스템의 수집 및 검색 성능에 영향을 줄 수 있습니다. 예를 들어, 평균 쿼리의 지연 시간이 느리고 시간 초과로 인해 실패한 쿼리의 수가 많은 경우 메타데이터 저장소의 로드가 높거나 다른 작업을 수행해야 할 수 있습니다.

일관성 오류로 인해 실패한 총 쿼리 수를 볼 수도 있습니다. 정합성 보장 수준 오류는 특정 LDR 서비스를 통해 쿼리를 수행할 때 사용 가능한 메타데이터 저장소의 수가 부족하여 발생합니다.

진단 페이지를 사용하여 그리드의 현재 상태에 대한 추가 정보를 얻을 수 있습니다. 을 참조하십시오 ["진단 프로그램 실행 중"](#).

### ILM 활동

ILM(정보 수명 주기 관리) 메트릭을 통해 ILM 구현을 위해 개체가 평가되는 속도를 모니터링할 수 있습니다. 이러한 메트릭은 대시보드 또는 각 스토리지 노드의 노드 페이지 ILM 탭에서 확인할 수 있습니다.

### 오브젝트 저장소

LDR 서비스의 기본 데이터 스토리지는 고정된 수의 오브젝트 저장소(스토리지 볼륨이라고도 함)로 나뉩니다. 각 오브젝트 저장소는 별도의 마운트 지점입니다.

노드 페이지 스토리지 탭에서 스토리지 노드에 대한 오브젝트 저장소를 확인할 수 있습니다.

Object Stores						
ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health
0000	4.40 TB	1.35 TB	43.99 GB	0 bytes	1.00%	No Errors
0001	1.97 TB	1.57 TB	44.76 GB	351.14 GB	20.09%	No Errors
0002	1.97 TB	1.46 TB	43.29 GB	465.20 GB	25.81%	No Errors
0003	1.97 TB	1.70 TB	43.51 GB	223.98 GB	13.58%	No Errors
0004	1.97 TB	1.92 TB	44.03 GB	0 bytes	2.23%	No Errors
0005	1.97 TB	1.46 TB	43.67 GB	463.36 GB	25.73%	No Errors
0006	1.97 TB	1.92 TB	43.10 GB	1.61 GB	2.27%	No Errors
0007	1.97 TB	1.35 TB	46.05 GB	575.24 GB	31.53%	No Errors
0008	1.97 TB	1.81 TB	46.00 GB	112.84 GB	8.06%	No Errors
0009	1.97 TB	1.57 TB	43.91 GB	352.72 GB	20.13%	No Errors
000A	1.97 TB	1.70 TB	44.31 GB	226.81 GB	13.76%	No Errors
000B	1.97 TB	1.92 TB	43.17 GB	780.07 MB	2.23%	No Errors
000C	1.97 TB	1.58 TB	44.32 GB	339.56 GB	19.48%	No Errors
000D	1.97 TB	1.82 TB	44.47 GB	107.34 GB	7.70%	No Errors
000E	1.97 TB	1.68 TB	43.07 GB	241.70 GB	14.45%	No Errors
000F	2.03 TB	1.50 TB	44.57 GB	475.47 GB	25.67%	No Errors

스토리지 노드의 오브젝트 저장소는 002F의 16진수 번호로 식별되며 볼륨 ID라고도 합니다. Cassandra 데이터베이스의 오브젝트 메타데이터에 대한 첫 번째 오브젝트 저장소(볼륨 0)에 공간이 예약되며, 해당 볼륨의 나머지 공간은 오브젝트 데이터에 사용됩니다. 다른 모든 오브젝트 저장소는 복제된 복사본 및 삭제 코딩 조각이 포함된 오브젝트 데이터에만 사용됩니다.

복제된 복사본에 대한 공간 사용이 고르게 되도록 지정된 개체의 개체 데이터는 사용 가능한 스토리지 공간을 기반으로 한 하나의 개체 저장소에 저장됩니다. 하나 이상의 오브젝트 저장소에서 용량을 채우는 경우, 나머지 오브젝트 저장소는 스토리지 노드에 더 이상 공간이 없을 때까지 오브젝트를 계속 저장합니다.

#### 메타데이터 보호

오브젝트 메타데이터는 오브젝트 수정 시간 또는 저장 위치와 같은 오브젝트의 설명이나 이와 관련된 정보입니다. StorageGRID는 LDR 서비스와 상호 작용하는 Cassandra 데이터베이스에 개체 메타데이터를 저장합니다.

이중화를 보장하고 손실을 방지하기 위해 각 사이트에 오브젝트 메타데이터의 복사본 3개가 유지됩니다. 각 사이트의 모든 스토리지 노드에 복사본이 균등하게 분산됩니다. 이 복제는 구성이 불가능하며 자동으로 수행됩니다.

#### "오브젝트 메타데이터 스토리지 관리"

#### 스토리지 옵션 관리

그리드 관리자의 구성 메뉴를 사용하여 스토리지 옵션을 보고 구성할 수 있습니다. 스토리지 옵션에는 객체 세분화 설정과 스토리지 워터마크에 대한 현재 값이 포함됩니다. 또한 게이트웨이 노드에서 더 이상 사용되지 않는 CLB 서비스와 스토리지 노드의 LDR 서비스에서 사용하는 S3 및 Swift 포트를 볼 수 있습니다.

포트 할당에 대한 자세한 내용은 을 참조하십시오 "[요약: 클라이언트 연결을 위한 IP 주소 및 포트](#)".



### Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

### Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

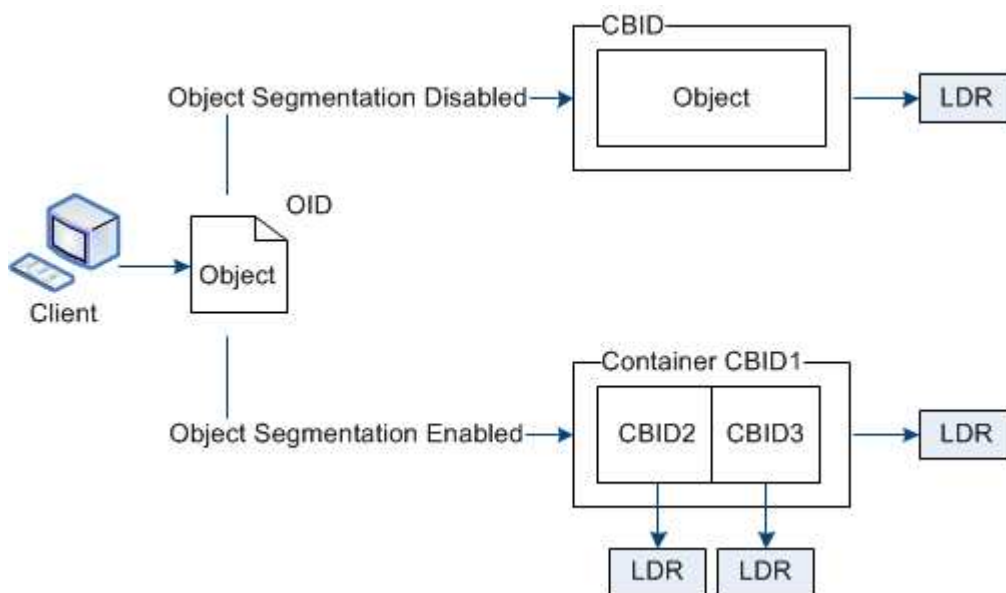
### Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

개체 분할이란 무엇입니까

객체 분할은 큰 객체에 대한 스토리지 및 리소스 사용을 최적화하기 위해 객체를 작은 고정 크기 객체 컬렉션으로 분할하는 프로세스입니다. S3 다중 파트 업로드는 또한 각 파트를 나타내는 오브젝트와 함께 분할된 오브젝트를 만듭니다.

개체가 StorageGRID 시스템으로 수집되면 LDR 서비스는 개체를 세그먼트로 분할하고 모든 세그먼트의 헤더 정보를 내용으로 나열하는 세그먼트 컨테이너를 만듭니다.



StorageGRID 시스템에 타겟 유형이 클라우드 계층화인 아카이브 노드가 포함되어 있고 타겟 아카이브 스토리지 시스템이 AWS(Amazon Web Services)인 경우 최대 세그먼트 크기는 4.5GiB(4,8338,208바이트)보다 작거나 같아야 합니다. 이 상한은 AWS가 5GB의 한도를 초과하지 않도록 합니다. 이 값을 초과하는 AWS 요청은 실패했습니다.

세그먼트 컨테이너를 검색할 때 LDR 서비스는 세그먼트에서 원래 개체를 어셈블하고 개체를 클라이언트에 반환합니다.

컨테이너와 세그먼트가 반드시 동일한 스토리지 노드에 저장되지는 않습니다. 컨테이너와 세그먼트는 모든 스토리지 노드에 저장될 수 있습니다.

각 세그먼트는 StorageGRID 시스템에 의해 독립적으로 처리되고 관리되는 개체 및 저장된 개체와 같은 특성의 카운트에 기여합니다. 예를 들어, StorageGRID 시스템에 저장된 객체가 두 세그먼트로 분할되면 다음과 같이 수집 완료 후 관리 객체 값이 3씩 증가합니다.

세그먼트 컨테이너 + 세그먼트 1 + 세그먼트 2 = 저장된 오브젝트 3개

다음과 같은 방법으로 큰 물체를 다룰 때 성능을 향상시킬 수 있습니다.

- 각 게이트웨이 및 스토리지 노드에는 필요한 처리량을 위한 충분한 네트워크 대역폭이 있습니다. 예를 들어 10Gbps 이더넷 인터페이스에서 별도의 그리드 및 클라이언트 네트워크를 구성합니다.
- 필요한 처리량에 대해 충분한 게이트웨이 및 스토리지 노드가 구축됩니다.
- 각 스토리지 노드에는 필요한 처리량을 위한 충분한 디스크 입출력 성능이 있습니다.

스토리지 볼륨 워터마크는 무엇입니까

StorageGRID에서는 스토리지 볼륨 워터마크를 사용하여 스토리지 노드에서 사용 가능한 공간의 양을 모니터링할 수 있습니다. 노드에서 사용 가능한 공간의 양이 구성된 워터마크 설정보다 작은 경우 SSTS(스토리지 상태) 경보가 트리거되어 스토리지 노드를 추가해야 하는지 여부를 확인할 수 있습니다.

스토리지 볼륨 워터마크에 대한 현재 설정을 보려면 \* 구성 \*\* 스토리지 옵션 \*\* 개요 \* 를 선택합니다.



## Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

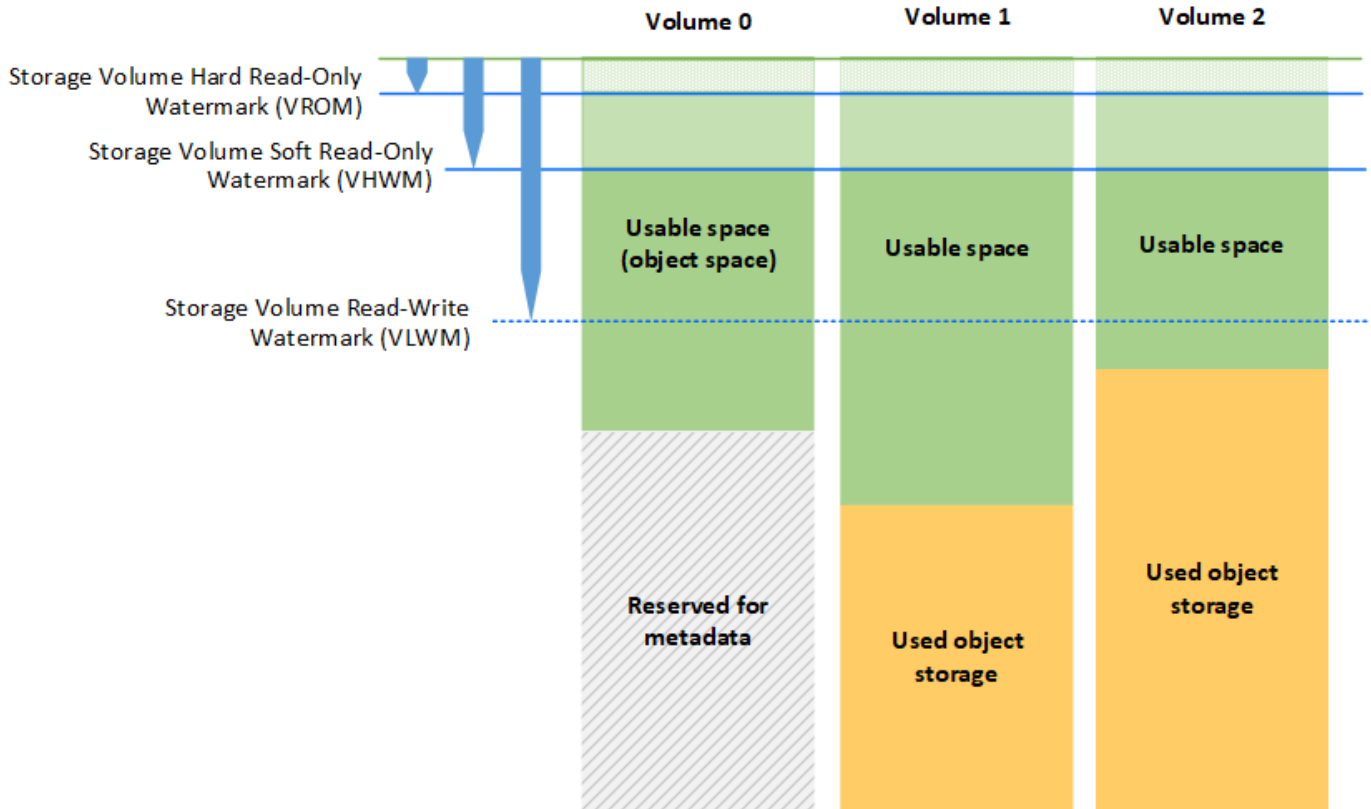
### Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

### Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

다음 그림은 세 개의 볼륨이 있고 세 개의 스토리지 볼륨 워터마크의 상대적 위치를 보여 주는 스토리지 노드를 나타냅니다. 각 스토리지 노드 내에서 StorageGRID는 오브젝트 메타데이터를 위해 볼륨 0의 공간을 예약하며, 해당 볼륨의 나머지 공간은 오브젝트 데이터에 사용됩니다. 다른 모든 볼륨은 복제된 복사본 및 삭제 코딩 조각이 포함된 오브젝트 데이터에만 사용됩니다.



스토리지 볼륨 워터마크는 StorageGRID가 노드의 읽기-쓰기 동작을 변경하거나 경보를 트리거하지 않도록 스토리지 노드의 각 볼륨에 필요한 최소 여유 공간을 나타내는 시스템 전체의 기본값입니다. StorageGRID가 작업을 수행하기 전에 모든 볼륨이 워터마크에 도달해야 합니다. 일부 볼륨의 여유 공간이 필요한 최소 용량을 초과하는 경우 알람이 트리거되지 않고 노드의 읽기-쓰기 동작이 변경되지 않습니다.

#### 스토리지 볼륨 소프트 읽기 전용 워터마크(VHWM)

스토리지 볼륨 소프트 읽기 전용 워터마크는 오브젝트 데이터에 대해 노드의 사용 가능한 공간이 가득 차있음을 나타내는 첫 번째 워터마크입니다. 이 배경무늬는 노드가 "소프트 읽기 전용 모드"로 전환되는 것을 방지하기 위해 스토리지 노드의 모든 볼륨에 얼마나 많은 여유 공간이 있어야 하는지를 나타냅니다. 소프트 읽기 전용 모드는 스토리지 노드가 나머지 StorageGRID 시스템에 읽기 전용 서비스를 알리는 한편 보류 중인 모든 쓰기 요청을 처리하는 것을 의미합니다.

각 볼륨의 여유 공간이 이 배경무늬의 설정보다 작은 경우 SSTS(Storage Status) 알람이 알림 수준에서 트리거되고 스토리지 노드가 소프트 읽기 전용 모드로 전환됩니다.

예를 들어 스토리지 볼륨 소프트 읽기 전용 워터마크가 기본값인 10GB로 설정되어 있다고 가정합니다. 스토리지 노드의 각 볼륨에 10GB보다 작은 여유 공간이 남아 있는 경우, SSTS 알람은 알림 수준에서 트리거되고 스토리지 노드는 소프트 읽기 전용 모드로 전환됩니다.

#### 스토리지 볼륨 하드 읽기 전용 워터마크(VROM)

스토리지 볼륨 하드 읽기 전용 워터마크는 노드의 사용 가능한 오브젝트 데이터 공간이 가득 차있음을 나타내는 다음 워터마크입니다. 이 배경무늬는 노드가 "하드 읽기 전용 모드"로 전환되는 것을 방지하기 위해 스토리지 노드의 모든

볼륨에 얼마나 많은 여유 공간이 있어야 하는지를 나타냅니다. 하드 읽기 전용 모드는 스토리지 노드가 읽기 전용이며 더 이상 쓰기 요청을 수락하지 않음을 의미합니다.

스토리지 노드의 모든 볼륨에서 사용 가능한 공간의 양이 이 배경무늬의 설정보다 작은 경우 SSTS(Storage Status) 알람이 주요 레벨에서 트리거되고 스토리지 노드가 하드 읽기 전용 모드로 전환됩니다.

예를 들어 스토리지 볼륨 하드 읽기 전용 워터마크가 기본값인 5GB로 설정되어 있다고 가정합니다. 스토리지 노드의 각 스토리지 볼륨에 5GB 미만의 여유 공간이 남아 있는 경우 주요 레벨에서 SSTS 경보가 트리거되고 스토리지 노드가 하드 읽기 전용 모드로 전환됩니다.

스토리지 볼륨 하드 읽기 전용 배경무늬 값은 스토리지 볼륨 소프트웨어 읽기 전용 배경무늬 값보다 작아야 합니다.

#### 스토리지 볼륨 읽기-쓰기 워터마크(VLWM)

스토리지 볼륨 읽기-쓰기 워터마크가 읽기 전용 모드로 전환된 스토리지 노드에만 적용됩니다. 이 배경무늬는 스토리지 노드가 다시 읽기/쓰기가 허용되는 시기를 결정합니다.

예를 들어, 스토리지 노드가 하드 읽기 전용 모드로 전환되었다고 가정해 보겠습니다. 스토리지 볼륨 읽기-쓰기 워터마크가 30GB(기본값)로 설정된 경우 스토리지 노드의 모든 스토리지 볼륨에서 사용 가능한 공간이 5GB에서 30GB로 증가해야 노드가 다시 읽기/쓰기가 가능합니다.

스토리지 볼륨 읽기-쓰기 배경무늬 값은 스토리지 볼륨 소프트웨어 읽기 전용 배경무늬 값보다 커야 합니다.

관련 정보

["전체 스토리지 노드 관리"](#)

## 오브젝트 메타데이터 스토리지 관리

StorageGRID 시스템의 오브젝트 메타데이터 용량은 해당 시스템에 저장할 수 있는 최대 오브젝트 수를 제어합니다. StorageGRID 시스템에 새 개체를 저장할 충분한 공간이 있는지 확인하려면 StorageGRID에서 개체 메타데이터를 저장하는 위치와 방법을 알아야 합니다.

### 오브젝트 메타데이터란?

개체 메타데이터는 개체를 설명하는 정보입니다. StorageGRID는 오브젝트 메타데이터를 사용하여 그리드 전체의 모든 오브젝트의 위치를 추적하고 각 오브젝트의 라이프사이클 관리를 제공합니다.

StorageGRID의 개체에 대한 개체 메타데이터에는 다음 유형의 정보가 포함됩니다.

- 각 개체의 고유 ID(UUID), 개체 이름, S3 버킷 또는 Swift 컨테이너의 이름, 테넌트 계정 이름 또는 ID, 개체의 논리적 크기, 개체를 처음 만든 날짜 및 시간을 포함한 시스템 메타데이터 및 객체가 마지막으로 수정된 날짜 및 시간입니다.
- 객체와 연결된 모든 사용자 메타데이터 키 값 쌍입니다.
- S3 오브젝트의 경우 오브젝트와 연결된 오브젝트 태그 키 값 쌍이 됩니다.
- 복제된 오브젝트 복사본의 경우 각 복제본의 현재 스토리지 위치입니다.
- 삭제 코딩 오브젝트 복사본의 경우 각 분절의 현재 스토리지 위치입니다.
- 클라우드 스토리지 풀의 오브젝트 복사본의 경우 외부 버킷의 이름 및 오브젝트의 고유 식별자를 비롯한 오브젝트의 위치가 포함됩니다.

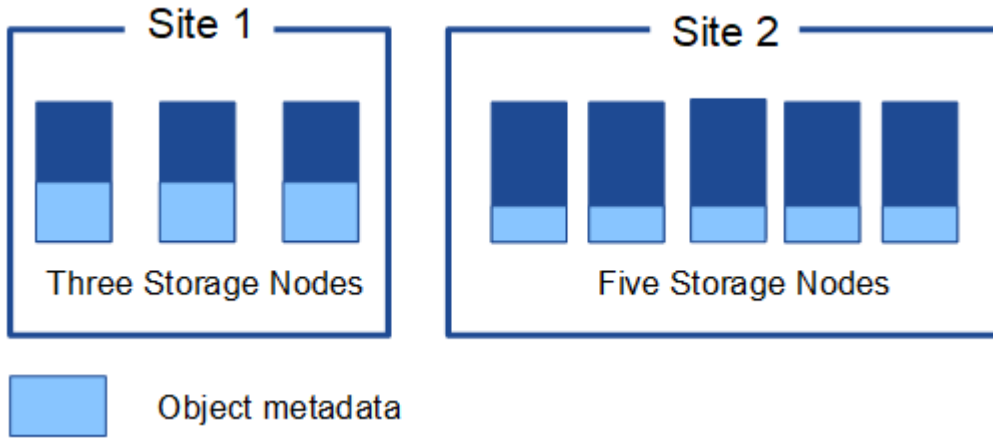


- 분할된 오브젝트 및 다중 파트 오브젝트의 경우 세그먼트 식별자 및 데이터 크기가 사용됩니다.

오브젝트 메타데이터는 어떻게 저장됩니까?

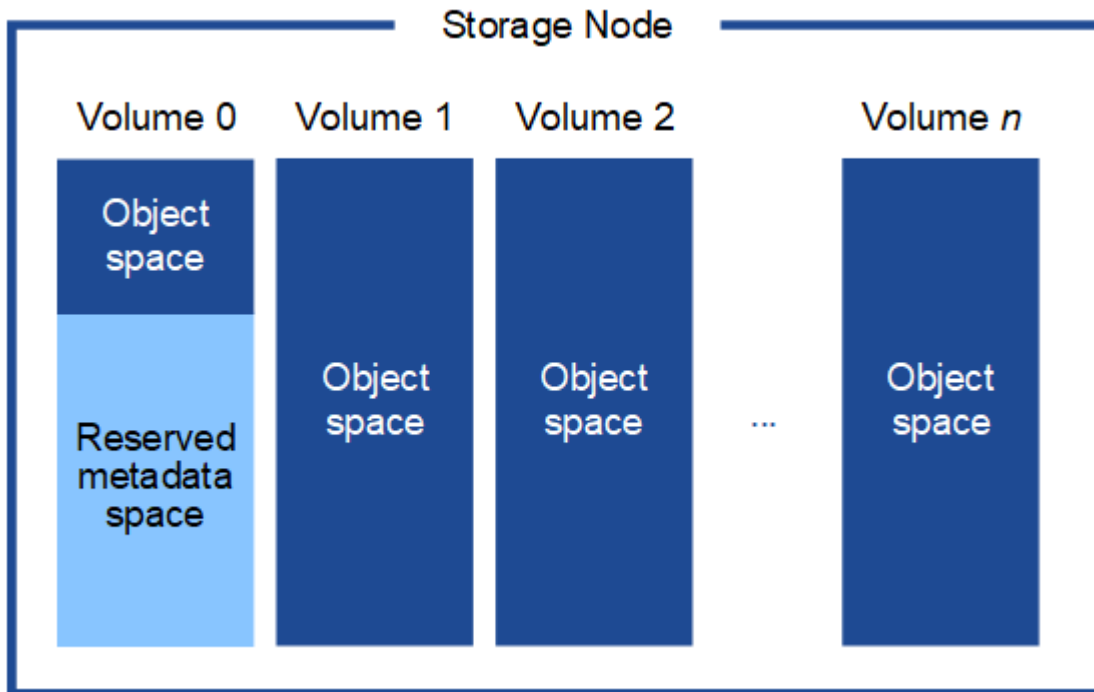
StorageGRID는 오브젝트 메타데이터를 Cassandra 데이터베이스에 유지하며, 이 데이터베이스는 오브젝트 데이터와 독립적으로 저장됩니다. 이중화를 제공하고 개체 메타데이터를 손실로부터 보호하기 위해 StorageGRID는 각 사이트의 시스템 모든 개체에 대한 메타데이터 복사본을 3개 저장합니다. 오브젝트 메타데이터의 복사본 3개는 각 사이트의 모든 스토리지 노드에 균등하게 분산됩니다.

이 그림은 두 사이트의 스토리지 노드를 나타냅니다. 각 사이트에는 동일한 양의 오브젝트 메타데이터가 있으며, 이 메타데이터는 해당 사이트의 스토리지 노드 전체에 균등하게 분산됩니다.



오브젝트 메타데이터는 어디에 저장됩니까?

이 그림은 단일 스토리지 노드의 스토리지 볼륨을 나타냅니다.



그림에 나와 있는 것처럼 StorageGRID는 각 스토리지 노드의 스토리지 볼륨 0에 객체 메타데이터를 위한 공간을 예약합니다. 이 경우 예약된 공간을 사용하여 오브젝트 메타데이터를 저장하고 중요한 데이터베이스 작업을 수행합니다.

스토리지 볼륨 0 및 스토리지 노드의 다른 모든 스토리지 볼륨의 나머지 공간은 오브젝트 데이터(복제된 복사본 및 삭제 코딩 단편)에만 사용됩니다.

특정 스토리지 노드에서 오브젝트 메타데이터에 예약된 공간의 양은 아래에 설명된 여러 요인에 따라 달라집니다.

메타데이터 예약 공간 설정입니다

Metadata Reserved Space\_는 모든 스토리지 노드의 볼륨 0에 있는 메타데이터에 예약된 공간의 양을 나타내는 시스템 전체 설정입니다. 표에서 볼 수 있듯이 StorageGRID 11.5에 대한 이 설정의 기본값은 다음과 같습니다.

- StorageGRID를 처음 설치할 때 사용한 소프트웨어 버전입니다.
- 각 스토리지 노드의 RAM 용량입니다.

초기 <b>StorageGRID</b> 설치에 사용되는 버전입니다	스토리지 노드의 <b>RAM</b> 크기입니다	<b>StorageGRID 11.5</b> 의 기본 메타데이터 예약 공간 설정
11.5	그리드의 각 스토리지 노드에 128GB 이상	8TB(8,000GB)
	그리드의 스토리지 노드에서 128GB 미만	3TB(3,000GB)
11.1 ~ 11.4	한 사이트의 각 스토리지 노드에 128GB 이상	4TB(4,000GB)
	각 사이트의 스토리지 노드에 128GB 미만	3TB(3,000GB)
11.0 이전 버전	금액	2TB(2,000GB)

StorageGRID 시스템에 대한 메타데이터 예약 공간 설정을 보려면

1. 구성 \* > \* 시스템 설정 \* > \* 스토리지 옵션 \* 을 선택합니다.
2. Storage Watermarks 테이블에서 \* Metadata Reserved Space \* 를 찾습니다.



## Storage Options Overview

Updated: 2021-02-23 11:58:33 MST

### Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

### Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	8,000 GB

스크린샷에서 \* Metadata Reserved Space \* 값은 8,000GB(8TB)입니다. 각 스토리지 노드에 128GB 이상의 RAM이 있는 새 StorageGRID 11.5 설치의 기본 설정입니다.

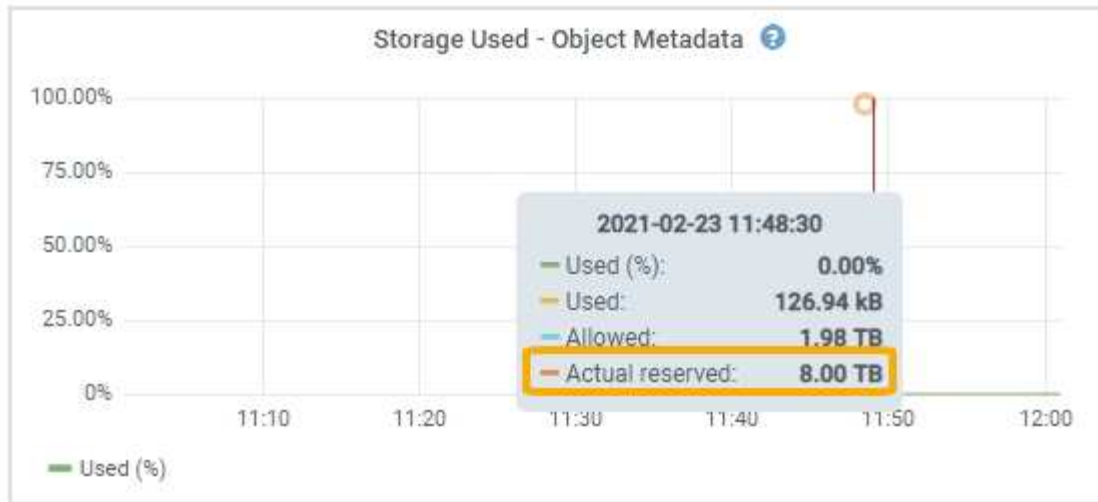
메타데이터의 실제 예약 공간입니다

시스템 전체의 메타데이터 예약 공간 설정과 달리, 객체 메타데이터에 대한 \_실제 예약된 공간\_은 각 스토리지 노드에 대해 결정됩니다. 특정 스토리지 노드에 대해 메타데이터에 대한 실제 예약된 공간은 노드에 대한 볼륨 0의 크기 및 시스템 전반의 \* 메타데이터 예약 공간 \* 설정에 따라 달라집니다.

노드에 대한 볼륨 0의 크기입니다	메타데이터의 실제 예약 공간입니다
500GB 미만(비운영 용도)	볼륨 0의 10%
500GB 이상	다음 값 중 더 작은 값: <ul style="list-style-type: none"> <li>• 볼륨 0</li> <li>• 메타데이터 예약 공간 설정입니다</li> </ul>

특정 스토리지 노드의 메타데이터에 대한 실제 예약 공간을 보려면 다음을 따르십시오.

1. Grid Manager에서 \* Nodes \* > \*Storage Node \* 를 선택합니다.
2. Storage \* 탭을 선택합니다.
3. 커서를 Storage Used — Object Metadata 차트 위에 놓고 \* Actual Reserved \* 값을 찾습니다.



스크린샷에서 \* Actual Reserved \* 값은 8TB입니다. 이 스크린샷은 새 StorageGRID 11.5 설치의 대규모 스토리지 노드에 대한 것입니다. 시스템 전체의 메타데이터 예약 공간 설정이 이 스토리지 노드의 볼륨 0보다 작기 때문에 이 노드에 대한 실제 예약 공간은 메타데이터 예약 공간 설정과 같습니다.

실제 예약 \* 값은 다음 Prometheus 메트릭에 해당합니다.

```
storagegrid_storage_utilization_metadata_reserved_bytes
```

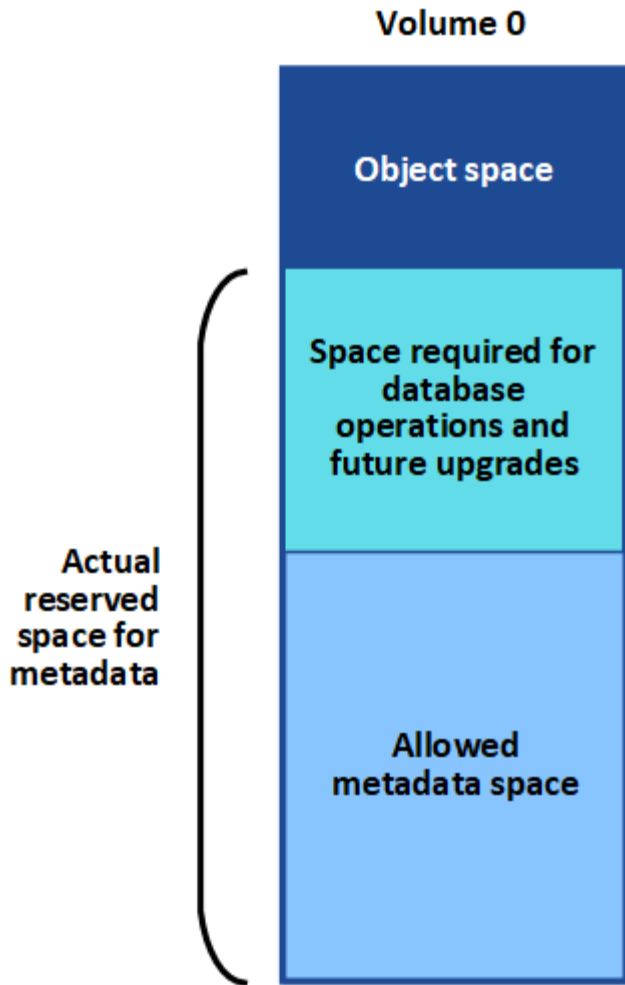
### 실제 예약 메타데이터 공간의 예

버전 11.5를 사용하여 새 StorageGRID 시스템을 설치한다고 가정합니다. 이 예에서는 각 스토리지 노드에 128MB 이상의 RAM이 있고 SN1(Storage Node 1)의 볼륨 0이 6TB라고 가정합니다. 다음 값을 기준으로 합니다.

- 시스템 전체 \* 메타데이터 예약 공간 \* 은 8TB로 설정됩니다. 각 스토리지 노드에 128GB RAM이 넘는 경우 새 StorageGRID 11.5 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 표에는 StorageGRID가 스토리지 노드에 대해 허용되는 메타데이터 공간 값을 결정하는 방법이 요약되어 있습니다.

메타데이터의 실제 예약 공간입니다	허용된 메타데이터 공간입니다
4TB 이하	메타데이터를 위해 실제 예약된 공간의 60%, 최대 1.98TB
4TB 초과	(메타데이터의 실제 예약 공간 - 1TB) × 60%, 최대 2.64TB



StorageGRID 시스템이 어떤 스토리지 노드에도 2.64TB 이상의 메타데이터를 저장(또는 저장할 것으로 예상되는 경우)하는 경우, 허용되는 메타데이터 공간을 늘릴 수 있습니다. 스토리지 노드 각각에 128GB 이상의 RAM이 있고 스토리지 볼륨 0에 사용 가능한 공간이 있는 경우 NetApp 고객 담당자에게 문의하십시오. NetApp에서 요구사항을 검토하고 가능한 경우 각 스토리지 노드에 대해 허용된 메타데이터 공간을 늘립니다.

스토리지 노드에 대해 허용되는 메타데이터 공간을 보려면 다음을 따르십시오.

1. Grid Manager에서 \* Node \* > \* Storage Node \* 를 선택합니다.
2. Storage \* 탭을 선택합니다.

3. 커서를 Storage Used — Object Metadata 차트 위에 놓고 \* Allowed \* 값을 찾습니다.



스크린샷에서 \* Allowed \* 값은 2.64TB이며, 이는 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 11.5를 사용하여 StorageGRID 시스템을 설치한다고 가정합니다. 이 예에서는 각 스토리지 노드에 128MB 이상의 RAM이 있고 SN1(Storage Node 1)의 볼륨 0이 6TB라고 가정합니다. 다음 값을 기준으로 합니다.

- 시스템 전체 \* 메타데이터 예약 공간 \* 은 8TB로 설정됩니다. 각 스토리지 노드에 128GB RAM이 넘는 경우 StorageGRID 11.5의 기본값입니다.
- SN1의 메타데이터에 대한 실제 예약 공간은 6TB입니다. (볼륨 0이 \* Metadata Reserved Space \* 설정보다 작기 때문에 전체 볼륨이 예약됩니다.)
- SN1의 메타데이터에 허용되는 공간은 2.64TB입니다. (이 값은 실제 예약 공간의 최대값입니다.)

서로 다른 크기의 스토리지 노드가 오브젝트 용량에 미치는 영향

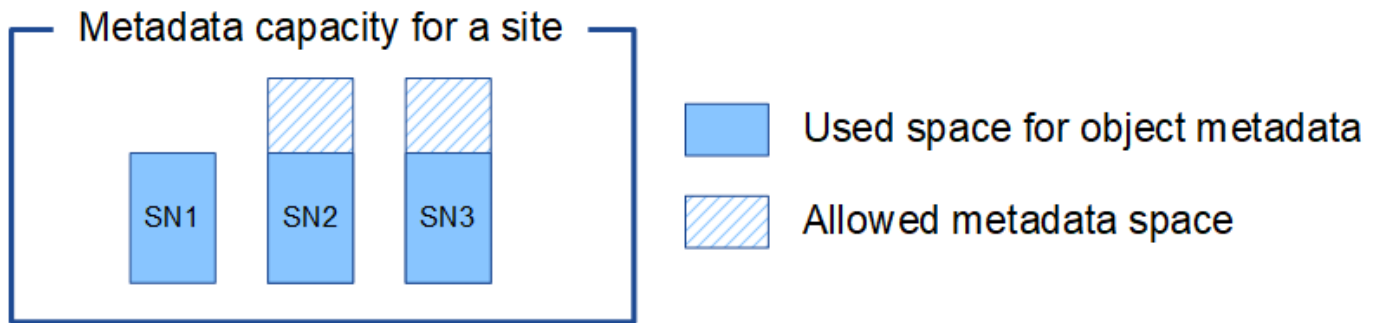
위에서 설명한 것처럼 StorageGRID는 각 사이트의 스토리지 노드에 오브젝트 메타데이터를 균등하게 분산합니다. 따라서 사이트에 크기가 다른 스토리지 노드가 있는 경우 사이트의 가장 작은 노드가 사이트의 메타데이터 용량을 결정합니다.

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
SN1	2.2TB	2.2TB	1.32TB
Sn2	5TB	4TB	1.98TB
SN3	6TB	4TB	1.98TB

개체 메타데이터는 사이트의 스토리지 노드에 균등하게 분산되므로 이 예제의 각 노드는 1.32TB의 메타데이터만 보유할 수 있습니다. sn2 및 SN3에 대해 허용되는 추가 0.66TB의 메타데이터 공간은 사용할 수 없습니다.



마찬가지로, StorageGRID는 각 사이트에서 StorageGRID 시스템의 모든 개체 메타데이터를 유지하므로 StorageGRID 시스템의 전체 메타데이터 용량은 가장 작은 사이트의 개체 메타데이터 용량에 따라 결정됩니다.

또한 오브젝트 메타데이터 용량은 최대 오브젝트 수를 제어하므로 한 노드에 메타데이터 용량이 부족한 경우 이 그리드는 효과적으로 가득 차게 됩니다.

#### 관련 정보

- 각 스토리지 노드의 객체 메타데이터 용량을 모니터링하는 방법에 대해 알아보려면 다음을 수행합니다.

["모니터링 및 문제 해결"](#)

- 시스템의 오브젝트 메타데이터 용량을 늘리려면 새 스토리지 노드를 추가해야 합니다.

["그리드를 확장합니다"](#)

#### 저장된 개체에 대한 전역 설정 구성

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

- ["저장된 객체 압축 구성"](#)
- ["저장된 오브젝트 암호화 구성"](#)
- ["저장된 객체 해싱을 구성합니다"](#)

## 저장된 객체 압축 구성

저장된 개체 압축 그리드 옵션을 사용하여 StorageGRID에 저장된 개체의 크기를 줄여 개체가 더 적은 스토리지를 사용하도록 할 수 있습니다.

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

### 이 작업에 대해

저장된 개체 그리드 압축 옵션은 기본적으로 비활성화되어 있습니다. 이 옵션을 활성화하면 StorageGRID는 무손실 압축을 사용하여 저장할 때 각 개체의 압축을 시도합니다.



이 설정을 변경하면 새 설정을 적용하는 데 약 1분이 걸립니다. 구성된 값이 성능 및 확장을 위해 캐싱됩니다.

이 옵션을 활성화하기 전에 다음 사항에 유의하십시오.

- 저장되는 데이터가 압축 가능한지 여부를 모를 경우 압축을 사용해서는 안 됩니다.
- 개체를 StorageGRID에 저장하는 응용 프로그램은 개체를 저장하기 전에 압축할 수 있습니다. 클라이언트 응용 프로그램에서 개체를 StorageGRID에 저장하기 전에 이미 압축한 경우 저장된 개체 압축을 설정하면 개체의 크기가 더 작아지지 않습니다.
- StorageGRID에서 NetApp FabricPool를 사용하는 경우 압축을 활성화하지 마십시오.
- Compress Stored Objects(저장된 오브젝트 압축) 그리드 옵션이 활성화된 경우 S3 및 Swift 클라이언트 애플리케이션은 바이트 범위를 지정하는 Get Object(오브젝트 가져오기) 작업을 수행하지 않아야 합니다. 이러한 ""범위 읽기"" 작업은 StorageGRID가 요청된 바이트에 액세스하기 위해 개체의 압축을 효과적으로 해제해야 하기 때문에 비효율적입니다. 매우 큰 개체에서 작은 바이트 범위를 요청하는 Get Object 작업은 특히 비효율적입니다. 예를 들어, 50GB의 압축 개체에서 10MB 범위를 읽는 것은 비효율적입니다.

압축된 개체에서 범위를 읽으면 클라이언트 요청이 시간 초과될 수 있습니다.



개체를 압축해야 하고 클라이언트 응용 프로그램에서 범위 읽기를 사용해야 하는 경우 응용 프로그램의 읽기 시간 초과를 늘리십시오.

### 단계

1. 구성 \*\* 시스템 설정 \* 그리드 옵션 \* 을 선택합니다.
2. 저장 개체 옵션 구역에서 저장된 개체 압축 \* 확인란을 선택합니다.



## Stored Object Options

Compress Stored Objects  

Stored Object Encryption   None  AES-128  AES-256

Stored Object Hashing   SHA-1  SHA-256

3. 저장 \* 을 클릭합니다.

### 저장된 오브젝트 암호화 구성

개체 저장소가 손상된 경우 읽을 수 있는 형식으로 데이터를 검색할 수 없도록 하려면 저장된 개체를 암호화할 수 있습니다. 기본적으로 객체는 암호화되지 않습니다.

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

### 이 작업에 대해

저장된 오브젝트 암호화를 사용하면 S3 또는 Swift를 통해 수집되는 모든 오브젝트 데이터를 암호화할 수 있습니다. 이 설정을 활성화하면 새로 수집된 모든 객체가 암호화되지만 기존 저장된 객체는 변경되지 않습니다. 암호화를 사용하지 않도록 설정하면 현재 암호화된 개체는 암호화된 상태로 유지되지만 새로 수집된 개체는 암호화되지 않습니다.



이 설정을 변경하면 새 설정을 적용하는 데 약 1분이 걸립니다. 구성된 값이 성능 및 확장을 위해 캐시됩니다.

저장된 오브젝트는 AES - 128 또는 AES - 256 암호화 알고리즘을 사용하여 암호화할 수 있습니다.

저장된 오브젝트 암호화 설정은 버킷 레벨 또는 오브젝트 레벨 암호화로 암호화되지 않은 S3 오브젝트에만 적용됩니다.

### 단계

1. 구성 \* \* 시스템 설정 \* 그리드 옵션 \* 을 선택합니다.
2. 저장된 개체 옵션 섹션에서 저장된 개체 암호화를 \* 없음 \* (기본값), \* AES-128 \* 또는 \* AES-256 \* 으로 변경합니다.

## Stored Object Options

Compress Stored Objects  

Stored Object Encryption   None  AES-128  AES-256

Stored Object Hashing   SHA-1  SHA-256

3. 저장 \* 을 클릭합니다.

저장된 객체 해싱을 구성합니다

저장된 개체 해싱 옵션은 개체 무결성을 확인하는 데 사용되는 해시 알고리즘을 지정합니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

기본적으로 오브젝트 데이터는 SHA - 1 알고리즘을 사용하여 해시됩니다. SHA-256 알고리즘에는 추가 CPU 리소스가 필요하며 일반적으로 무결성 검증에 권장되지 않습니다.



이 설정을 변경하면 새 설정을 적용하는 데 약 1분이 걸립니다. 구성된 값이 성능 및 확장을 위해 캐시됩니다.

단계

1. 구성 \*\* 시스템 설정 \* 그리드 옵션 \* 을 선택합니다.
2. 저장된 개체 옵션 섹션에서 저장된 개체 해시를 \* SHA-1 \* (기본값) 또는 \* SHA-256 \* 로 변경합니다.

#### Stored Object Options



3. 저장 \* 을 클릭합니다.

스토리지 노드 구성 설정입니다

각 스토리지 노드는 여러 가지 구성 설정 및 카운터를 사용합니다. 현재 설정을 보거나 카운터를 재설정하여 알람을 소거해야 할 수 있습니다(기존 시스템).



설명서에 구체적으로 명시된 경우를 제외하고 스토리지 노드 구성 설정을 수정하기 전에 기술 지원 부서에 문의해야 합니다. 필요에 따라 이벤트 카운터를 재설정하여 기존 알람을 지울 수 있습니다.

스토리지 노드의 구성 설정 및 카운터에 액세스하려면 다음을 수행합니다.

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. 사이트 \_ \* > \* \_ 스토리지 노드 \_ \* 를 선택합니다.
3. 스토리지 노드를 확장하고 서비스 또는 구성 요소를 선택합니다.

4. Configuration \* 탭을 선택합니다.

다음 표에는 스토리지 노드 구성 설정이 요약되어 있습니다.

**LDR**

속성 이름	코드	설명
HTTP 상태	HSTE	<p>S3, Swift 및 기타 내부 StorageGRID 트래픽에 대한 HTTP 프로토콜의 현재 상태:</p> <ul style="list-style-type: none"> <li>오프라인: 작업이 허용되지 않으며 LDR 서비스에 대한 HTTP 세션을 열려고 하는 모든 클라이언트 응용 프로그램에서 오류 메시지가 표시됩니다. 활성 세션이 정상적으로 닫힙니다.</li> <li>Online(온라인): 작업이 정상적으로 계속됩니다</li> </ul>
HTTP를 자동으로 시작합니다	HTAS	<ul style="list-style-type: none"> <li>이 옵션을 선택하면 재시작 시 시스템 상태는 * LDR * &gt; * 스토리지 * 구성 요소의 상태에 따라 달라집니다. 재시작 시 * LDR * &gt; * 스토리지 * 구성 요소가 읽기 전용인 경우 HTTP 인터페이스도 읽기 전용입니다. LDR * &gt; * 스토리지 * 구성 요소가 온라인인 경우 HTTP도 온라인입니다. 그렇지 않으면 HTTP 인터페이스가 오프라인 상태로 유지됩니다.</li> <li>선택되지 않은 경우 HTTP 인터페이스는 명시적으로 활성화될 때까지 오프라인 상태로 유지됩니다.</li> </ul>

**LDR > 데이터 저장소 를 선택합니다**

속성 이름	코드	설명
손실된 개체 수를 재설정합니다	RCOR	이 서비스의 손실된 개체 수에 대한 카운터를 재설정합니다.

**LDR > 스토리지**

속성 이름	코드	설명
Storage State — 원하는 상태입니다	SSD를 지원합니다	<p>스토리지 구성 요소의 원하는 상태에 대해 사용자가 구성할 수 있는 설정입니다. LDR 서비스는 이 값을 읽고 이 속성에 표시된 상태와 일치시킵니다. 이 값은 다시 시작할 때 영구적으로 유지됩니다.</p> <p>예를 들어 사용 가능한 저장 공간이 충분한 경우에도 이 설정을 사용하여 저장소를 읽기 전용으로 만들 수 있습니다. 이는 문제 해결에 유용할 수 있습니다.</p> <p>특성은 다음 값 중 하나를 사용할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• 오프라인: 원하는 상태가 오프라인이면 LDR 서비스에서 * LDR * &gt; * 스토리지 * 구성 요소를 오프라인으로 전환합니다.</li> <li>• 읽기 전용: 원하는 상태가 읽기 전용인 경우 LDR 서비스는 스토리지 상태를 읽기 전용으로 이동하고 새 콘텐츠 수신을 중지합니다. 열려 있는 세션이 닫힐 때까지 콘텐츠가 잠시 동안 스토리지 노드에 계속 저장될 수 있습니다.</li> <li>• Online(온라인): 일반 시스템 작업 중에 값을 Online(온라인)으로 유지합니다. 스토리지 구성 요소의 스토리지 상태 — 현재 상태는 LDR 서비스의 상태(예: 사용 가능한 오브젝트 스토리지 공간)를 기준으로 서비스에 의해 동적으로 설정됩니다. 공간이 부족하면 구성 요소가 읽기 전용이 됩니다.</li> </ul>
상태 점검 시간 초과	SHCT	<p>스토리지 볼륨이 양호한 것으로 간주되려면 상태 점검 테스트를 완료해야 하는 시간 제한(초)입니다. 지원 부서에서 이 값을 변경하도록 지시하는 경우에만 이 값을 변경하십시오.</p>

#### LDR > 확인 을 누릅니다

속성 이름	코드	설명
누락된 개체 수를 재설정합니다	VCMI	<p>감지된 누락된 개체 수(OMIS)를 재설정합니다. 전경 확인이 완료된 후에만 사용합니다. 누락된 복제 객체 데이터는 StorageGRID 시스템에 의해 자동으로 복구됩니다.</p>
확인합니다	FVOV	<p>전경 검증을 수행할 오브젝트 저장소를 선택합니다.</p>
검증 비율	VPRI	<p>백그라운드 검증이 실행되는 속도를 설정합니다. 백그라운드 검증 비율 구성에 대한 자세한 내용은 을 참조하십시오.</p>

속성 이름	코드	설명
손상된 개체 수를 재설정합니다	VCCR	백그라운드 확인 중에 발견된 손상된 복제된 개체 데이터에 대한 카운터를 재설정합니다. 이 옵션은 손상된 물체 감지(OCOR) 알람 조건을 지우는 데 사용할 수 있습니다. 자세한 내용은 StorageGRID 모니터링 및 문제 해결 지침을 참조하십시오.
격리된 개체 삭제	합니다	격리 디렉터리에서 손상된 개체를 삭제하고, 격리된 개체의 수를 0으로 재설정하고, 격리된 개체 감지(OQRT) 경보를 지웁니다. 이 옵션은 손상된 개체가 StorageGRID 시스템에 의해 자동으로 복구된 후에 사용됩니다.  개체 손실 경보가 트리거되면 기술 지원 부서에서 격리된 개체에 액세스하려고 할 수 있습니다. 경우에 따라 격리된 개체는 데이터 복구나 손상된 개체 복사본을 발생시킨 기본 문제를 디버깅하는 데 유용할 수 있습니다.

#### LDR > 삭제 코딩

속성 이름	코드	설명
쓰기 실패 횟수를 재설정합니다	RSWF	삭제 코딩 오브젝트 데이터의 쓰기 실패에 대한 카운터를 스토리지 노드로 재설정합니다.
재설정 읽기 실패 횟수	SRF	스토리지 노드에서 삭제 코딩 오브젝트 데이터의 읽기 실패에 대한 카운터를 재설정합니다.
재설정 실패 횟수를 삭제합니다	RSDF	스토리지 노드에서 삭제 코딩 오브젝트 데이터의 삭제 실패에 대한 카운터를 재설정합니다.
손상된 복제본 감지 수를 재설정합니다	RSCC	스토리지 노드에서 삭제 코딩 오브젝트 데이터의 손상된 복제본 수에 대한 카운터를 재설정합니다.
손상된 조각 감지됨 카운트 재설정	RSCCD를 참조하십시오	스토리지 노드에서 삭제 코딩 오브젝트 데이터의 손상된 조각에 대한 카운터를 재설정합니다.
누락된 조각 감지 횟수를 재설정합니다	RSMD	스토리지 노드에서 삭제 코딩 오브젝트 데이터의 누락된 조각에 대한 카운터를 재설정합니다. 전경 확인이 완료된 후에만 사용합니다.

#### LDR > 복제

속성 이름	코드	설명
인바운드 복제 실패 수를 재설정합니다	RICR	인바운드 복제 실패에 대한 카운터를 재설정합니다. RIRF(Inbound Replication - - Failed) 경보를 지우는 데 사용할 수 있습니다.

속성 이름	코드	설명
아웃바운드 복제 실패 수를 재설정합니다	ROCR	아웃바운드 복제 실패에 대한 카운터를 재설정합니다. RORF(아웃바운드 복제 -- 실패) 경보를 지우는 데 사용할 수 있습니다.
인바운드 복제를 비활성화합니다	DSIR	유지 관리 또는 테스트 절차의 일부로 인바운드 복제를 사용하지 않도록 설정하려면 선택합니다. 정상 작동 중에 선택하지 않은 상태로 둡니다.  인바운드 복제를 비활성화하면 StorageGRID 시스템의 다른 위치로 복사하기 위해 스토리지 노드에서 객체를 검색할 수 있지만 다른 위치에서는 이 스토리지 노드에 객체를 복사할 수 없습니다. 즉, LDR 서비스는 읽기 전용입니다.
아웃바운드 복제를 비활성화합니다	DSOR	유지 관리 또는 테스트 절차의 일부로 아웃바운드 복제(HTTP 검색을 위한 콘텐츠 요청 포함)를 사용하지 않도록 설정하려면 선택합니다. 정상 작동 중에 선택하지 않은 상태로 둡니다.  아웃바운드 복제를 사용하지 않도록 설정하면 객체를 이 스토리지 노드에 복제할 수 있지만 StorageGRID 시스템의 다른 위치로 복제할 스토리지 노드에서 객체를 검색할 수는 없습니다. LDR 서비스는 쓰기 전용입니다.

#### 관련 정보

["모니터링 및 문제 해결"](#)

## 전체 스토리지 노드 관리

스토리지 노드가 용량에 도달하면 새 스토리지를 추가하여 StorageGRID 시스템을 확장해야 합니다. 스토리지 볼륨 추가, 스토리지 확장 쉘프 추가, 스토리지 노드 추가의 세 가지 옵션을 사용할 수 있습니다.

### 스토리지 볼륨 추가

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. StorageGRID 시스템 확장 지침을 참조하십시오.

### 스토리지 확장 쉘프 추가

SG6060과 같은 일부 StorageGRID 어플라이언스 스토리지 노드는 추가 스토리지 쉘프를 지원할 수 있습니다. 최대 용량으로 아직 확장되지 않은 확장 기능을 갖춘 StorageGRID 어플라이언스를 사용하는 경우 스토리지 쉘프를 추가하여 용량을 늘릴 수 있습니다. StorageGRID 시스템 확장 지침을 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. StorageGRID 시스템 확장 지침을 참조하십시오.

관련 정보

["그리드를 확장합니다"](#)

## 관리 노드 관리

StorageGRID 배포의 각 사이트에는 하나 이상의 관리 노드가 있을 수 있습니다.

- ["관리 노드의 정의"](#)
- ["여러 관리 노드 사용"](#)
- ["기본 관리자 노드 식별"](#)
- ["기본 설정 발신자 선택"](#)
- ["알림 상태 및 대기열 보기"](#)
- ["관리자 노드가 확인된 경보를 표시하는 방법\(레거시 시스템\)"](#)
- ["감사 클라이언트 액세스 구성"](#)

### 관리 노드의 정의

관리 노드는 시스템 구성, 모니터링 및 로깅과 같은 관리 서비스를 제공합니다. 각 그리드에는 1개의 기본 관리 노드가 있어야 하며 이중화를 위해 여러 개의 비기본 관리 노드가 있을 수 있습니다.

그리드 관리자 또는 테넌트 관리자에 로그인할 때 관리 노드에 연결됩니다. 모든 관리 노드에 연결할 수 있으며 각 관리 노드에는 StorageGRID 시스템의 유사한 보기가 표시됩니다. 그러나 기본 관리 노드를 사용하여 유지 관리 절차를 수행해야 합니다.

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

관리 노드는 다음 서비스를 호스팅합니다.

- AMS 서비스
- CMN 서비스
- NMS 서비스
- Prometheus 서비스
- 로드 밸런서 및 고가용성 서비스(S3 및 Swift 클라이언트 트래픽 지원)

관리 노드는 그리드 관리 API 및 테넌트 관리 API의 요청을 처리하는 관리 애플리케이션 프로그램 인터페이스(mgmt-API)도 지원합니다.

## AMS 서비스의 정의

AMS(Audit Management System) 서비스는 시스템 활동 및 이벤트를 추적합니다.

## CMN 서비스의 정의

CMN(Configuration Management Node) 서비스는 모든 서비스에 필요한 시스템 전반의 연결 및 프로토콜 기능을 관리합니다. 또한 CMN 서비스는 그리드 작업을 실행하고 모니터링하는 데 사용됩니다. StorageGRID 배포당 하나의 CMN 서비스만 있습니다. CMN 서비스를 호스팅하는 관리 노드를 기본 관리 노드라고 합니다.

## NMS 서비스의 정의

NMS(네트워크 관리 시스템) 서비스는 StorageGRID 시스템의 브라우저 기반 인터페이스인 그리드 관리자를 통해 표시되는 모니터링, 보고 및 구성 옵션을 강화합니다.

## Prometheus 서비스의 정의

Prometheus 서비스는 모든 노드의 서비스에서 시계열 메트릭을 수집합니다.

관련 정보

["Grid Management API 사용"](#)

["테넌트 계정을 사용합니다"](#)

["로드 밸런싱 관리"](#)

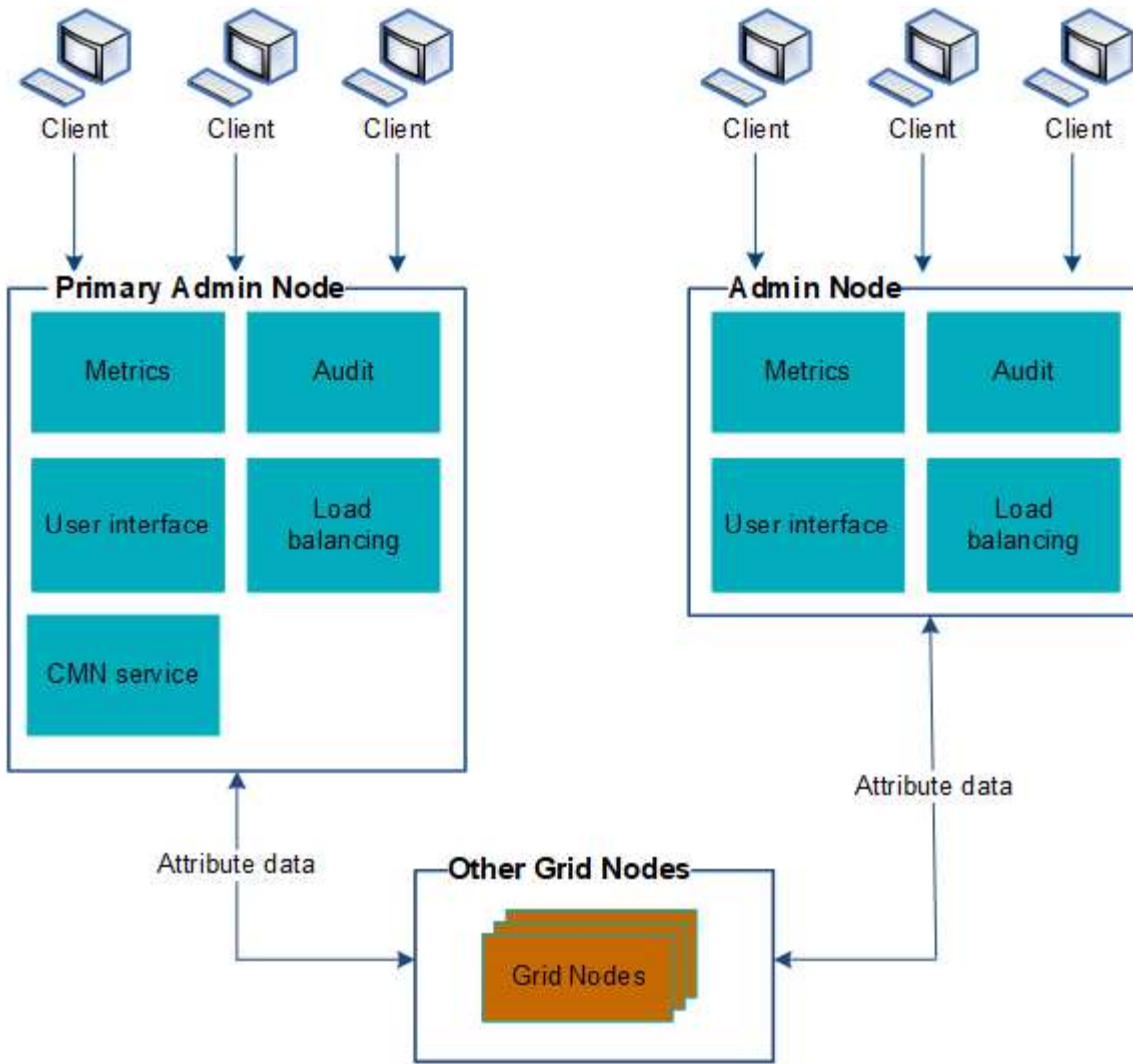
["고가용성 그룹 관리"](#)

## 여러 관리 노드 사용

StorageGRID 시스템에는 여러 관리 노드가 포함되어 있어 하나의 관리 노드에 장애가 발생하더라도 StorageGRID 시스템을 지속적으로 모니터링하고 구성할 수 있습니다.

관리 노드를 사용할 수 없게 되면 속성 처리가 계속되고 경고 및 경보(레거시 시스템)가 계속 트리거되며 이메일 알림 및 AutoSupport 메시지가 계속 전송됩니다. 그러나 여러 개의 관리 노드가 있으면 알림 및 AutoSupport 메시지를 제외한 페일오버 보호가 제공되지 않습니다. 특히 한 관리 노드에서 발생한 알람 확인응답을 다른 관리 노드로 복사하지 않습니다.





관리 노드에 장애가 발생할 경우 StorageGRID 시스템을 계속 보고 구성할 수 있는 두 가지 옵션이 있습니다.

- 웹 클라이언트는 사용 가능한 다른 관리 노드에 다시 연결할 수 있습니다.
- 시스템 관리자가 고가용성 관리 노드 그룹을 구성한 경우 웹 클라이언트는 HA 그룹의 가상 IP 주소를 사용하여 그리드 관리자 또는 테넌트 관리자에 계속 액세스할 수 있습니다.



HA 그룹을 사용하는 경우 마스터 관리자 노드에 장애가 발생하면 액세스가 중단됩니다. 사용자는 HA 그룹의 가상 IP 주소가 그룹의 다른 관리 노드로 페일오버된 후 다시 로그인해야 합니다.

일부 유지 보수 작업은 기본 관리 노드를 통해서만 수행할 수 있습니다. 기본 관리 노드에 장애가 발생할 경우 StorageGRID 시스템이 다시 정상적으로 작동하기 전에 해당 노드를 복구해야 합니다.

관련 정보

["고가용성 그룹 관리"](#)

## 기본 관리자 노드 식별

기본 관리 노드는 CMN 서비스를 호스팅합니다. 일부 유지 관리 절차는 기본 관리 노드를 사용해서만 수행할 수 있습니다.

## 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

## 단계

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. site\_ \* \* \* Admin Node \* 를 선택한 다음 를 클릭합니다 + 토폴로지 트리를 확장하고 이 관리 노드에서 호스팅되는 서비스를 표시합니다.  
  
기본 관리 노드는 CMN 서비스를 호스팅합니다.
3. 이 관리 노드가 CMN 서비스를 호스팅하지 않는 경우 다른 관리 노드를 확인합니다.

## 기본 설정 발신자 선택

StorageGRID 배포에 여러 관리 노드가 포함된 경우 알림을 보내는 기본 설정 관리자 노드를 선택할 수 있습니다. 기본적으로 기본 관리 노드가 선택되지만 모든 관리 노드가 기본 설정 송신자가 될 수 있습니다.

## 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

## 이 작업에 대해

Configuration \* \* \* System Settings \* \* Display Options \* 페이지에는 현재 기본 설정 발신인으로 선택된 관리 노드가 표시됩니다. 기본 관리 노드는 기본적으로 선택됩니다.

정상적인 시스템 작업에서 기본 설정 보낸 사람만이 다음 알림을 보냅니다.

- AutoSupport 메시지
- SNMP 알림
- 경고 이메일
- 알람 이메일(기존 시스템)

그러나 다른 모든 관리 노드(대기 보낸 사람)는 기본 설정 보낸 사람을 모니터링합니다. 문제가 감지되면 대기 보낸 사람이 이러한 알림을 보낼 수도 있습니다.

다음과 같은 경우 기본 발신자와 대기 발신자는 모두 알림을 보낼 수 있습니다.

- 관리 노드가 서로 "isfand"가 되면 기본 발신자와 대기 보낸 사람 모두 알림 전송을 시도하며 여러 개의 알림 복사본이 수신될 수 있습니다.
- 대기 보낸 사람이 기본 설정 보낸 사람과 관련된 문제를 감지하고 알림을 보내기 시작하면 기본 설정 보낸 사람이 알림을 다시 보낼 수 있습니다. 이 경우 중복 알림이 전송될 수 있습니다. 대기 보낸 사람이 더 이상 기본 설정 보낸 사람의 오류를 감지하지 않으면 알림 전송을 중지합니다.



알림 알림 및 AutoSupport 메시지를 테스트할 때 모든 관리 노드가 테스트 이메일을 보냅니다. 알림 알림을 테스트할 때는 모든 관리 노드에 로그인하여 연결을 확인해야 합니다.

#### 단계

1. 구성 \* > \* 시스템 설정 \* > \* 표시 옵션 \* 을 선택합니다.
2. 표시 옵션 메뉴에서 \* 옵션 \* 을 선택합니다.
3. 드롭다운 목록에서 기본 설정 발신자로 설정할 관리 노드를 선택합니다.



### Display Options

Updated: 2017-08-30 16:31:10 MDT

Current Sender	ADMIN-DC1-ADM1
Preferred Sender	ADMIN-DC1-ADM1
GUI Inactivity Timeout	900
Notification Suppress All	<input type="checkbox"/>

Apply Changes

4. 변경 내용 적용 \* 을 클릭합니다.

관리 노드는 알림의 기본 보낸 사람으로 설정됩니다.

#### 알림 상태 및 대기열 보기

관리 노드의 NMS 서비스는 메일 서버에 알림을 보냅니다. 인터페이스 엔진 페이지에서 NMS 서비스의 현재 상태와 해당 알림 대기열의 크기를 볼 수 있습니다.



인터페이스 엔진 페이지에 액세스하려면 \* 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다. 마지막으로 \* site \* > \* Admin Node \* > \* NMS \* > \* Interface Engine \* 을 선택합니다.



Overview | Alarms | Reports | Configuration

Main



**Overview: NMS (170-176) - Interface Engine**  
Updated: 2009-03-09 10:12:17 PDT



---

NMS Interface Engine Status: Connected  



Connected Services: 15  



**E-mail Notification Events**



E-mail Notifications Status: No Errors  

E-mail Notifications Queued: 0  

**Database Connection Pool**

Maximum Supported Capacity: 100  

Remaining Capacity: 95 %  

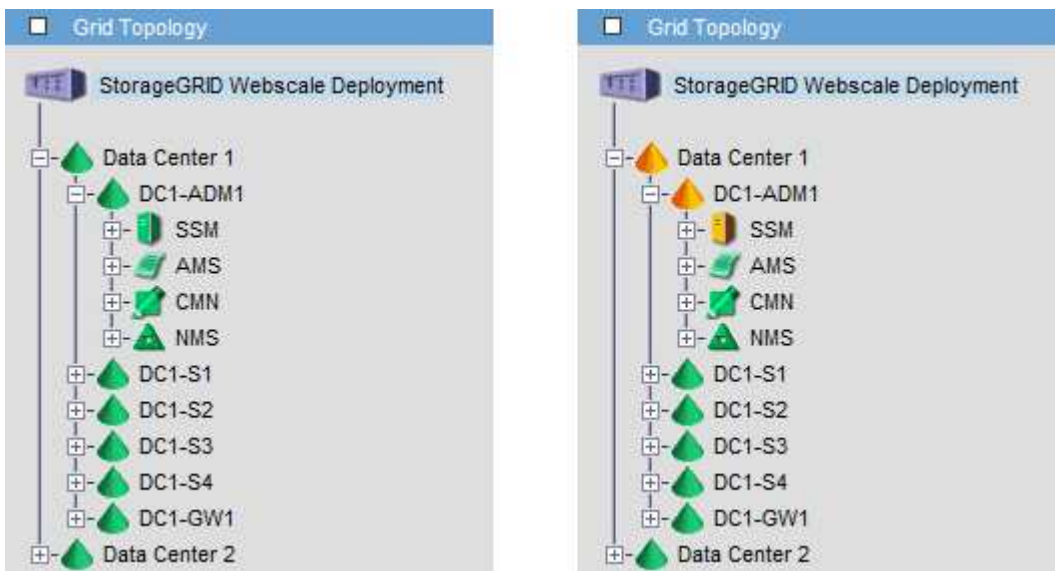
Active Connections: 5  

알림은 이메일 알림 대기열을 통해 처리되며, 트리거된 순서대로 하나씩 메일 서버로 전송됩니다. 네트워크 연결 오류 등의 문제가 있고 메일 서버를 사용할 수 없는 경우 알림 전송을 시도할 때 메일 서버에 알림을 다시 보내려는 최선의 노력을 60초 동안 계속합니다. 60초 후에 메일 서버로 알림이 전송되지 않으면 알림 대기열에서 알림이 삭제되어 대기열의 다음 알림을 보내려고 시도합니다. 알림을 보내지 않고 알림 대기열에서 놓을 수 있으므로 알림을 보내지 않고 경보를 트리거할 수 있습니다. 알림이 전송되지 않고 대기열에서 삭제된 경우 Minor(분)(이메일 알림 상태) 경보가 트리거됩니다.

### 관리자 노드가 확인된 경보를 표시하는 방법(레거시 시스템)

한 관리 노드에서 알람을 확인하면 확인된 알람이 다른 관리 노드에 복사되지 않습니다. 승인 내용이 다른 관리 노드에 복사되지 않기 때문에 그리드 토폴로지 트리거가 각 관리 노드에 대해 동일하게 보이지 않을 수 있습니다.

이 차이는 웹 클라이언트를 연결할 때 유용할 수 있습니다. 웹 클라이언트는 관리자 요구에 따라 StorageGRID 시스템에 대한 다양한 보기를 가질 수 있습니다.



알림은 확인이 발생하는 관리 노드에서 전송됩니다.

## 감사 클라이언트 액세스 구성

AMS(감사 관리 시스템) 서비스를 통해 관리 노드는 감사 공유를 통해 사용 가능한 로그 파일에 모든 감사 시스템 이벤트를 기록하며, 이 로그 파일은 설치 시 각 관리 노드에 추가됩니다. 감사 로그에 쉽게 액세스할 수 있도록 CIFS 및 NFS 모두에 대한 감사 공유에 대한 클라이언트 액세스를 구성할 수 있습니다.

StorageGRID 시스템은 감사 메시지를 로그 파일에 쓰기 전에 손실을 방지하기 위해 긍정 승인을 사용합니다. AMS 서비스 또는 중간 감사 릴레이 서비스가 해당 제어 권한을 확인할 때까지 메시지는 서비스 대기 상태로 유지됩니다.

자세한 내용은 감사 메시지 이해를 위한 지침을 참조하십시오.



CIFS 또는 NFS를 사용할 수 있는 옵션이 있으면 NFS를 선택합니다.



CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

관련 정보

["관리 노드의 정의"](#)

["감사 로그를 검토합니다"](#)

["소프트웨어 업그레이드"](#)

### CIFS에 대한 감사 클라이언트 구성

감사 클라이언트를 구성하는 절차는 Windows Workgroup 또는 Windows AD(Active Directory)의 인증 방법에 따라 다릅니다. 추가된 감사 공유는 읽기 전용 공유로 자동 설정됩니다.



CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

관련 정보

["소프트웨어 업그레이드"](#)

### Workgroup에 대한 감사 클라이언트 구성

감사 메시지를 검색할 StorageGRID 배포의 각 관리자 노드에 대해 이 절차를 수행합니다.

필요한 것

- 예 가 있어야 합니다 Passwords.txt 루트/관리자 계정 암호가 있는 파일(해당 패키지에서 사용 가능).
- 예 가 있어야 합니다 Configuration.txt 파일(해당 패키지에서 사용 가능).

이 작업에 대해

CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

단계

1. 기본 관리자 노드에 로그인합니다.

- a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
- b. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
- c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
- d. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.

루트로 로그인하면 프롬프트가 `에서` 변경됩니다 `$` 를 선택합니다 `#`.

2. 모든 서비스가 실행 중 또는 확인됨 상태인지 확인합니다. `storagegrid-status`

모든 서비스가 실행 중이거나 확인되지 않은 경우 계속하기 전에 문제를 해결하십시오.

3. 명령줄로 돌아가 \* `Ctrl` \* + \* `C` \* 를 누릅니다.

4. CIFS 구성 유틸리티를 시작합니다. `config_cifs.rb`

```

-----
| Shares                | Authentication          | Config                  |
-----
| add-audit-share       | set-authentication      | validate-config        |
| enable-disable-share  | set-netbios-name        | help                   |
| add-user-to-share     | join-domain             | exit                   |
| remove-user-from-share | add-password-server     |                         |
| modify-group          | remove-password-server  |                         |
|                       | add-wins-server         |                         |
|                       | remove-wins-server     |                         |
-----

```

5. Windows Workgroup에 대한 인증을 설정합니다.

인증이 이미 설정된 경우 권고 메시지가 나타납니다. 인증이 이미 설정된 경우 다음 단계로 이동합니다.

- a. 입력: `set-authentication`
- b. Windows Workgroup 또는 Active Directory 설치를 묻는 메시지가 나타나면 다음을 입력합니다. `workgroup`
- c. 메시지가 나타나면 워크그룹 이름을 입력합니다. `workgroup_name`
- d. 메시지가 표시되면 다음과 같이 의미 있는 NetBIOS 이름을 만듭니다. `netbios_name`

또는

관리자 노드의 호스트 이름을 NetBIOS 이름으로 사용하려면 \* `Enter` \* 를 누릅니다.

이 스크립트는 Samba 서버를 다시 시작하고 변경 사항이 적용됩니다. 이 작업은 1분 이내에 수행해야 합니다. 인증을 설정한 후 감사 클라이언트를 추가합니다.

- a. 메시지가 표시되면 \* `Enter` \* 를 누릅니다.

CIFS 구성 유틸리티가 표시됩니다.

6. 감사 클라이언트 추가:

a. 입력: `add-audit-share`



공유는 자동으로 읽기 전용으로 추가됩니다.

b. 메시지가 표시되면 사용자 또는 그룹을 추가합니다. `user`

c. 메시지가 표시되면 감사 사용자 이름을 입력합니다. `audit_user_name`

d. 메시지가 표시되면 감사 사용자의 암호를 입력합니다. `password`

e. 메시지가 나타나면 동일한 암호를 다시 입력하여 확인합니다. `password`

f. 메시지가 표시되면 \* Enter \* 를 누릅니다.

CIFS 구성 유틸리티가 표시됩니다.



디렉토리를 입력할 필요가 없습니다. 감사 디렉토리 이름이 미리 정의되어 있습니다.

7. 둘 이상의 사용자 또는 그룹이 감사 공유에 액세스할 수 있는 경우 추가 사용자를 추가합니다.

a. 입력: `add-user-to-share`

활성화된 공유의 번호 매기기 목록이 표시됩니다.

b. 메시지가 표시되면 감사 내보내기 공유의 번호를 입력합니다. `share_number`

c. 메시지가 표시되면 사용자 또는 그룹을 추가합니다. `user`

또는 `group`

d. 메시지가 표시되면 감사 사용자 또는 그룹의 이름을 입력합니다. `audit_user or audit_group`

e. 메시지가 표시되면 \* Enter \* 를 누릅니다.

CIFS 구성 유틸리티가 표시됩니다.

f. 감사 공유에 대한 액세스 권한이 있는 추가 사용자 또는 그룹에 대해 이러한 하위 단계를 반복합니다.

8. 필요에 따라 구성을 확인합니다. `validate-config`

서비스가 확인 및 표시됩니다. 다음 메시지는 무시해도 됩니다.

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. 메시지가 표시되면 \* Enter \* 를 누릅니다.

감사 클라이언트 구성이 표시됩니다.

b. 메시지가 표시되면 \* Enter \* 를 누릅니다.

CIFS 구성 유틸리티가 표시됩니다.

9. CIFS 구성 유틸리티를 닫습니다. `exit`

10. Samba 서비스 시작: `service smb start`

11. StorageGRID 배포가 단일 사이트인 경우 다음 단계로 이동합니다.

또는

필요한 경우 StorageGRID 배포에 다른 사이트의 관리자 노드가 포함된 경우 필요에 따라 다음 감사 공유를 활성화합니다.

a. 사이트의 관리 노드에 원격으로 로그인:

i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

ii. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.

iii. 루트로 전환하려면 다음 명령을 입력합니다. `su -`

iv. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.

b. 각 추가 관리 노드에 대한 감사 공유를 구성하려면 단계를 반복합니다.

c. 원격 관리 노드에 대한 원격 보안 셸 로그인을 닫습니다. `exit`

12. 명령 셸에서 로그아웃합니다. `exit`

관련 정보

["소프트웨어 업그레이드"](#)

**Active Directory**에 대한 감사 클라이언트 구성

감사 메시지를 검색할 StorageGRID 배포의 각 관리자 노드에 대해 이 절차를 수행합니다.

필요한 것

- 에 가 있어야 합니다 `Passwords.txt` 루트/관리자 계정 암호가 있는 파일(해당 패키지에서 사용 가능).
- CIFS Active Directory 사용자 이름과 암호가 있어야 합니다.
- 에 가 있어야 합니다 `Configuration.txt` 파일(해당 패키지에서 사용 가능).



CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

단계

1. 기본 관리자 노드에 로그인합니다.

a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`



- b. 에 나열된 암호를 입력합니다 Passwords.txt 파일.
- c. 루트로 전환하려면 다음 명령을 입력합니다. su -
- d. 에 나열된 암호를 입력합니다 Passwords.txt 파일.

루트로 로그인하면 프롬프트가 에서 변경됩니다 \$ 를 선택합니다 #.

2. 모든 서비스가 실행 중 또는 확인됨 상태인지 확인합니다. storagegrid-status  
모든 서비스가 실행 중이거나 확인되지 않은 경우 계속하기 전에 문제를 해결하십시오.
3. 명령줄로 돌아가 \* Ctrl \* + \* C \* 를 누릅니다.
4. CIFS 구성 유틸리티를 시작합니다. config\_cifs.rb

```

-----
| Shares                | Authentication          | Config                  |
-----
| add-audit-share       | set-authentication      | validate-config        |
| enable-disable-share  | set-netbios-name        | help                   |
| add-user-to-share     | join-domain             | exit                   |
| remove-user-from-share| add-password-server     |                         |
| modify-group          | remove-password-server  |                         |
|                       | add-wins-server         |                         |
|                       | remove-wins-server     |                         |
-----

```

5. Active Directory에 대한 인증 설정: set-authentication

대부분의 배포에서는 감사 클라이언트를 추가하기 전에 인증을 설정해야 합니다. 인증이 이미 설정된 경우 권고 메시지가 나타납니다. 인증이 이미 설정된 경우 다음 단계로 이동합니다.

- a. Workgroup 또는 Active Directory 설치를 묻는 메시지가 나타나면 다음을 수행합니다. ad
- b. 메시지가 표시되면 AD 도메인 이름(짧은 도메인 이름)을 입력합니다.
- c. 메시지가 표시되면 도메인 컨트롤러의 IP 주소 또는 DNS 호스트 이름을 입력합니다.
- d. 메시지가 표시되면 전체 도메인 영역 이름을 입력합니다.

대문자를 사용합니다.

- e. winbind 지원을 활성화하라는 메시지가 나타나면 \* y \* 를 입력합니다.

Winbind는 AD 서버에서 사용자 및 그룹 정보를 확인하는 데 사용됩니다.

- f. 메시지가 표시되면 NetBIOS 이름을 입력합니다.
- g. 메시지가 표시되면 \* Enter \* 를 누릅니다.

CIFS 구성 유틸리티가 표시됩니다.

## 6. 도메인 가입:

- a. 아직 시작하지 않은 경우 CIFS 구성 유틸리티를 시작합니다. `config_cifs.rb`
- b. 도메인 가입: `join-domain`
- c. 관리자 노드가 현재 도메인의 유효한 구성원인지 테스트하라는 메시지가 표시됩니다. 이 관리자 노드가 이전에 도메인에 가입하지 않은 경우 다음을 입력합니다. `no`
- d. 메시지가 표시되면 관리자의 사용자 이름을 입력합니다. `administrator_username`

위치 `administrator_username` CIFS Active Directory 사용자 이름이며 StorageGRID 사용자 이름이 아닙니다.

- e. 메시지가 표시되면 관리자 암호를 입력합니다. `administrator_password`

있습니다 `administrator_password` CIFS Active Directory 사용자 이름이며 StorageGRID 암호가 아닙니다.

- f. 메시지가 표시되면 \* Enter \* 를 누릅니다.

CIFS 구성 유틸리티가 표시됩니다.

## 7. 도메인에 올바르게 가입했는지 확인합니다.

- a. 도메인 가입: `join-domain`
- b. 서버가 현재 도메인의 유효한 구성원인지 테스트하라는 메시지가 나타나면 다음을 입력합니다. `y`

"Join is OK"라는 메시지가 표시되면 도메인에 성공적으로 참가한 것입니다. 이 응답이 없으면 인증을 설정하고 도메인에 다시 가입해 보십시오.

- c. 메시지가 표시되면 \* Enter \* 를 누릅니다.

CIFS 구성 유틸리티가 표시됩니다.

## 8. 감사 클라이언트 추가: `add-audit-share`

- a. 사용자 또는 그룹을 추가하라는 메시지가 나타나면 다음을 입력합니다. `user`
- b. 감사 사용자 이름을 입력하라는 메시지가 나타나면 감사 사용자 이름을 입력합니다.
- c. 메시지가 표시되면 \* Enter \* 를 누릅니다.

CIFS 구성 유틸리티가 표시됩니다.

## 9. 둘 이상의 사용자 또는 그룹이 감사 공유에 액세스할 수 있는 경우, 사용자를 추가합니다. `add-user-to-share`

활성화된 공유의 번호 매기기 목록이 표시됩니다.

- a. 감사 내보내기 공유의 번호를 입력합니다.
- b. 사용자 또는 그룹을 추가하라는 메시지가 나타나면 다음을 입력합니다. `group`

감사 그룹 이름을 묻는 메시지가 표시됩니다.

- c. 감사 그룹 이름을 묻는 메시지가 표시되면 감사 사용자 그룹의 이름을 입력합니다.

d. 메시지가 표시되면 \* Enter \* 를 누릅니다.

CIFS 구성 유틸리티가 표시됩니다.

e. 감사 공유에 액세스할 수 있는 추가 사용자 또는 그룹에 대해 이 단계를 반복합니다.

10. 필요에 따라 구성을 확인합니다. `validate-config`

서비스가 확인 및 표시됩니다. 다음 메시지는 무시해도 됩니다.

- 포함 파일을 찾을 수 없습니다 `/etc/samba/includes/cifs-interfaces.inc`
- 포함 파일을 찾을 수 없습니다 `/etc/samba/includes/cifs-filesystem.inc`
- 포함 파일을 찾을 수 없습니다 `/etc/samba/includes/cifs-interfaces.inc`
- 포함 파일을 찾을 수 없습니다 `/etc/samba/includes/cifs-custom-config.inc`
- 포함 파일을 찾을 수 없습니다 `/etc/samba/includes/cifs-shares.inc`
- `rlimit_max`: `rlimit_max(1024)`를 최소 윈도우 한계(16384)로 증가



'보안 = 광고' 설정을 '암호 서버' 매개변수와 결합하지 마십시오. (기본적으로 Samba는 자동으로 연락할 올바른 DC를 검색합니다.)

- i. 메시지가 표시되면 \* Enter \* 를 눌러 감사 클라이언트 구성을 표시합니다.
- ii. 메시지가 표시되면 \* Enter \* 를 누릅니다.

CIFS 구성 유틸리티가 표시됩니다.

11. CIFS 구성 유틸리티를 닫습니다. `exit`

12. StorageGRID 배포가 단일 사이트인 경우 다음 단계로 이동합니다.

또는

필요에 따라 StorageGRID 구축에 다른 사이트의 관리 노드가 포함되는 경우 필요에 따라 다음 감사 공유를 활성화합니다.

a. 사이트의 관리 노드에 원격으로 로그인:

- i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
- ii. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
- iii. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
- iv. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.

b. 각 관리 노드에 대한 감사 공유를 구성하려면 다음 단계를 반복합니다.

c. 관리자 노드에 대한 원격 보안 셸 로그인을 닫습니다. `exit`

13. 명령 셸에서 로그아웃합니다. `exit`

관련 정보

["소프트웨어 업그레이드"](#)

## AD 인증과 통합된 CIFS 감사 공유에 사용자 또는 그룹을 추가할 수 있습니다.

### 필요한 것

- 에 가 있어야 합니다 Passwords.txt 루트/관리자 계정 암호가 있는 파일(해당 패키지에서 사용 가능).
- 에 가 있어야 합니다 Configuration.txt 파일(해당 패키지에서 사용 가능).

### 이 작업에 대해

다음 절차는 AD 인증과 통합된 감사 공유에 대한 것입니다.



CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

### 단계

1. 기본 관리자 노드에 로그인합니다.

- 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
- 에 나열된 암호를 입력합니다 Passwords.txt 파일.
- 루트로 전환하려면 다음 명령을 입력합니다. `su -`
- 에 나열된 암호를 입력합니다 Passwords.txt 파일.

루트로 로그인하면 프롬프트가 에서 변경됩니다 \$ 를 선택합니다 #.

2. 모든 서비스의 상태가 실행 중 또는 확인인지 확인합니다. 입력: `storagegrid-status`

모든 서비스가 실행 중이거나 확인되지 않은 경우 계속하기 전에 문제를 해결하십시오.

3. 명령줄로 돌아가 \* Ctrl \* + \* C \* 를 누릅니다.

4. CIFS 구성 유틸리티를 시작합니다. `config_cifs.rb`

```
-----  
| Shares                | Authentication          | Config                |  
-----  
| add-audit-share      | set-authentication      | validate-config      |  
| enable-disable-share | set-netbios-name        | help                  |  
| add-user-to-share    | join-domain             | exit                  |  
| remove-user-from-share | add-password-server     |                       |  
| modify-group         | remove-password-server  |                       |  
|                       | add-wins-server         |                       |  
|                       | remove-wins-server      |                       |  
-----
```

5. 사용자 또는 그룹 추가 시작: `add-user-to-share`

구성된 감사 공유의 번호가 매겨진 목록이 표시됩니다.

6. 메시지가 표시되면 감사 공유(감사-내보내기) 번호를 입력합니다. `audit_share_number`

사용자 또는 그룹에 이 감사 공유에 대한 액세스 권한을 부여할지 묻는 메시지가 표시됩니다.

7. 메시지가 표시되면 사용자 또는 그룹을 추가합니다. `user` 또는 `group`

8. 이 AD 감사 공유에 대한 사용자 또는 그룹 이름을 묻는 메시지가 나타나면 이름을 입력합니다.

사용자 또는 그룹은 서버의 운영 체제와 CIFS 서비스 모두에서 감사 공유에 대해 읽기 전용으로 추가됩니다. 사용자 또는 그룹이 감사 클라이언트 공유에 액세스할 수 있도록 Samba 구성이 다시 로드됩니다.

9. 메시지가 표시되면 \* Enter \* 를 누릅니다.

CIFS 구성 유틸리티가 표시됩니다.

10. 감사 공유에 액세스할 수 있는 각 사용자 또는 그룹에 대해 이 단계를 반복합니다.

11. 필요에 따라 구성을 확인합니다. `validate-config`

서비스가 확인 및 표시됩니다. 다음 메시지는 무시해도 됩니다.

- include 파일 `/etc/samba/include/cifs-interfaces.in` c를 찾을 수 없습니다
- include 파일 `/etc/samba/include/cifs-filesystem.in` c를 찾을 수 없습니다
- include 파일 `/etc/samba/include/cifs-custom-config.in` c를 찾을 수 없습니다
- include 파일 `/etc/samba/include/cifs-shares.in` c를 찾을 수 없습니다
  - i. 메시지가 표시되면 \* Enter \* 를 눌러 감사 클라이언트 구성을 표시합니다.
  - ii. 메시지가 표시되면 \* Enter \* 를 누릅니다.

12. CIFS 구성 유틸리티를 닫습니다. `exit`

13. 다음과 같이 추가 감사 공유를 설정해야 하는지 확인합니다.

- StorageGRID 배포가 단일 사이트인 경우 다음 단계로 이동합니다.
- StorageGRID 구축에 다른 사이트의 관리 노드가 포함되는 경우 필요에 따라 다음 감사 공유를 활성화합니다.
  - i. 사이트의 관리 노드에 원격으로 로그인:
    - A. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
    - B. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
    - C. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
    - D. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
  - ii. 각 관리 노드에 대한 감사 공유를 구성하려면 다음 단계를 반복합니다.
  - iii. 원격 관리 노드에 대한 원격 보안 셸 로그인을 닫습니다. `exit`

14. 명령 셸에서 로그아웃합니다. `exit`

감사 공유에 액세스할 수 있는 마지막 사용자 또는 그룹은 제거할 수 없습니다.

필요한 것

- 에 가 있어야 합니다 Passwords.txt 루트 계정 암호가 있는 파일(해당 패키지에서 사용 가능).
- 에 가 있어야 합니다 Configuration.txt 파일(해당 패키지에서 사용 가능).

이 작업에 대해

CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

단계

1. 기본 관리자 노드에 로그인합니다.

- 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
- 에 나열된 암호를 입력합니다 Passwords.txt 파일.
- 루트로 전환하려면 다음 명령을 입력합니다. `su -`
- 에 나열된 암호를 입력합니다 Passwords.txt 파일.

루트로 로그인하면 프롬프트가 에서 변경됩니다 \$ 를 선택합니다 #.

2. CIFS 구성 유틸리티를 시작합니다. `config_cifs.rb`

```
-----  
| Shares                | Authentication          | Config                  |  
-----  
| add-audit-share       | set-authentication      | validate-config        |  
| enable-disable-share  | set-netbios-name       | help                   |  
| add-user-to-share     | join-domain            | exit                   |  
| remove-user-from-share| add-password-server    |                         |  
| modify-group          | remove-password-server |                         |  
|                       | add-wins-server        |                         |  
|                       | remove-wins-server     |                         |  
-----
```

3. 사용자 또는 그룹 제거 시작: `remove-user-from-share`

관리 노드에 대해 사용 가능한 감사 공유 목록이 번호가 매겨진 형식으로 표시됩니다. 감사 공유는 `audit-export`로 표시됩니다.

4. 감사 공유의 번호를 입력합니다. `audit_share_number`

5. 사용자 또는 그룹을 제거하라는 메시지가 나타나면 다음을 수행합니다. `user` 또는 `group`

감사 공유의 사용자 또는 그룹 번호가 매겨진 목록이 표시됩니다.

6. 제거할 사용자 또는 그룹에 해당하는 번호를 입력합니다. `number`

감사 공유가 업데이트되고 사용자 또는 그룹이 더 이상 감사 공유에 액세스할 수 없습니다. 예를 들면 다음과 같습니다.

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
 1. audituser
 2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. CIFS 구성 유틸리티를 닫습니다. `exit`
8. StorageGRID 배포에 다른 사이트의 관리자 노드가 포함된 경우 필요에 따라 각 사이트에서 감사 공유를 비활성화합니다.
9. 구성이 완료되면 각 명령 셸에서 로그아웃합니다. `exit`

관련 정보

["소프트웨어 업그레이드"](#)

**CIFS** 감사 공유 사용자 또는 그룹 이름 변경

새 사용자 또는 그룹을 추가한 다음 이전 사용자 또는 그룹을 삭제하여 CIFS 감사 공유의 사용자 또는 그룹 이름을 변경할 수 있습니다.

이 작업에 대해

CIFS/Samba를 통한 감사 내보내기는 더 이상 사용되지 않으며 향후 StorageGRID 릴리즈에서 제거될 예정입니다.

단계

1. 업데이트된 이름이 있는 새 사용자 또는 그룹을 감사 공유에 추가합니다.
2. 이전 사용자 또는 그룹 이름을 삭제합니다.

관련 정보

["소프트웨어 업그레이드"](#)

["CIFS 감사 공유에 사용자 또는 그룹 추가"](#)

["CIFS 감사 공유에서 사용자 또는 그룹 제거"](#)

**CIFS** 감사 통합을 확인하는 중입니다

감사 공유는 읽기 전용입니다. 로그 파일은 컴퓨터 응용 프로그램에서 읽기 위한 것이며 파일

열기에 대한 확인은 포함되지 않습니다. 감사 로그 파일이 Windows 탐색기 창에 표시된다는 것은 충분한 검증으로 간주됩니다. 연결 확인 후 모든 창을 닫습니다.

## NFS에 대한 감사 클라이언트 구성

감사 공유는 읽기 전용 공유로 자동 설정됩니다.

필요한 것

- 에 가 있어야 합니다 Passwords.txt 루트/관리자 암호가 있는 파일(해당 패키지에서 사용 가능).
- 에 가 있어야 합니다 Configuration.txt 파일(해당 패키지에서 사용 가능).
- 감사 클라이언트는 NFS 버전 3(NFSv3)을 사용해야 합니다.

이 작업에 대해

감사 메시지를 검색할 StorageGRID 배포의 각 관리자 노드에 대해 이 절차를 수행합니다.

단계

1. 기본 관리자 노드에 로그인합니다.
  - a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
  - b. 에 나열된 암호를 입력합니다 Passwords.txt 파일.
  - c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
  - d. 에 나열된 암호를 입력합니다 Passwords.txt 파일.

루트로 로그인하면 프롬프트가 에서 변경됩니다 \$ 를 선택합니다 #.
2. 모든 서비스의 상태가 실행 중 또는 확인인지 확인합니다. 입력: `storagegrid-status`  
실행 중 또는 확인으로 나열되지 않은 서비스가 있는 경우 계속하기 전에 문제를 해결합니다.
3. 명령줄로 돌아갑니다. `Ctrl * + * C *` 를 누릅니다.
4. NFS 구성 유틸리티를 시작합니다. 입력: `config_nfs.rb`

```
-----  
| Shares                | Clients                | Config                |  
-----  
| add-audit-share      | add-ip-to-share       | validate-config      |  
| enable-disable-share | remove-ip-from-share  | refresh-config       |  
|                       |                       | help                 |  
|                       |                       | exit                 |  
-----
```

5. 감사 클라이언트를 추가합니다. `add-audit-share`
  - a. 메시지가 표시되면 감사 공유의 감사 클라이언트의 IP 주소 또는 IP 주소 범위를 입력합니다.  
`client_IP_address`



- b. 메시지가 표시되면 \* Enter \* 를 누릅니다.
6. 둘 이상의 감사 클라이언트가 감사 공유에 액세스할 수 있는 경우 추가 사용자의 IP 주소를 추가합니다. `add-ip-to-share`
- a. 감사 공유의 번호를 입력합니다. `audit_share_number`
  - b. 메시지가 표시되면 감사 공유의 감사 클라이언트의 IP 주소 또는 IP 주소 범위를 입력합니다. `client_IP_address`
  - c. 메시지가 표시되면 \* Enter \* 를 누릅니다.

NFS 구성 유틸리티가 표시됩니다.

- d. 감사 공유에 대한 액세스 권한이 있는 각 추가 감사 클라이언트에 대해 이러한 하위 단계를 반복합니다.
7. 필요한 경우 구성을 확인합니다.
- a. 다음을 입력합니다. `validate-config`
- 서비스가 확인 및 표시됩니다.
- b. 메시지가 표시되면 \* Enter \* 를 누릅니다.
- NFS 구성 유틸리티가 표시됩니다.
- c. NFS 구성 유틸리티를 닫습니다. `exit`

8. 다른 사이트에서 감사 공유를 사용하도록 설정해야 하는지 확인합니다.
- StorageGRID 배포가 단일 사이트인 경우 다음 단계로 이동합니다.
  - StorageGRID 구축에 다른 사이트의 관리 노드가 포함되는 경우 필요에 따라 다음 감사 공유를 활성화합니다.
    - i. 사이트의 관리 노드에 원격으로 로그인:
      - A. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
      - B. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
      - C. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
      - D. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
    - ii. 이 단계를 반복하여 각 추가 관리 노드에 대한 감사 공유를 구성합니다.
    - iii. 원격 관리 노드에 대한 원격 보안 셸 로그인을 닫습니다. 입력: `exit`

9. 명령 셸에서 로그아웃합니다. `exit`

NFS 감사 클라이언트는 IP 주소를 기반으로 감사 공유에 대한 액세스 권한이 부여됩니다. 공유에 IP 주소를 추가하여 새 NFS 감사 클라이언트에 감사 공유에 대한 액세스 권한을 부여하거나 IP 주소를 제거하여 기존 감사 클라이언트를 제거합니다.

#### 감사 공유에 **NFS** 감사 클라이언트 추가

NFS 감사 클라이언트는 IP 주소를 기반으로 감사 공유에 대한 액세스 권한이 부여됩니다. 감사 공유에 IP 주소를 추가하여 새 NFS 감사 클라이언트에 감사 공유에 대한 액세스 권한을 부여합니다.

## 필요한 것

- 에 가 있어야 합니다 Passwords.txt 루트/관리자 계정 암호가 있는 파일(해당 패키지에서 사용 가능).
- 에 가 있어야 합니다 Configuration.txt 파일(해당 패키지에서 사용 가능).
- 감사 클라이언트는 NFS 버전 3(NFSv3)을 사용해야 합니다.

## 단계

### 1. 기본 관리자 노드에 로그인합니다.

- a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
- b. 에 나열된 암호를 입력합니다 Passwords.txt 파일.
- c. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
- d. 에 나열된 암호를 입력합니다 Passwords.txt 파일.

루트로 로그인하면 프롬프트가 에서 변경됩니다 \$ 를 선택합니다 #.

### 2. NFS 구성 유틸리티를 시작합니다. config\_nfs.rb

```
-----  
| Shares                | Clients                | Config                |  
-----  
| add-audit-share      | add-ip-to-share       | validate-config      |  
| enable-disable-share | remove-ip-from-share  | refresh-config       |  
|                       |                       | help                 |  
|                       |                       | exit                 |  
-----
```

### 3. 입력: add-ip-to-share

관리 노드에 설정된 NFS 감사 공유 목록이 표시됩니다. 감사 공유는 다음과 같이 나열됩니다.  
`/var/local/audit/export`

### 4. 감사 공유의 번호를 입력합니다. `audit_share_number`

### 5. 메시지가 표시되면 감사 공유의 감사 클라이언트의 IP 주소 또는 IP 주소 범위를 입력합니다. `client_IP_address`

감사 클라이언트가 감사 공유에 추가됩니다.

### 6. 메시지가 표시되면 \* Enter \* 를 누릅니다.

NFS 구성 유틸리티가 표시됩니다.

### 7. 감사 공유에 추가해야 하는 각 감사 클라이언트에 대해 이 단계를 반복합니다.

### 8. 필요에 따라 구성을 확인합니다. `validate-config`

서비스가 확인 및 표시됩니다.

a. 메시지가 표시되면 \* Enter \* 를 누릅니다.

NFS 구성 유틸리티가 표시됩니다.

9. NFS 구성 유틸리티를 닫습니다. `exit`

10. StorageGRID 배포가 단일 사이트인 경우 다음 단계로 이동합니다.

그렇지 않으면 StorageGRID 구축에 다른 사이트의 관리 노드가 포함되는 경우 필요에 따라 다음 감사 공유를 활성화합니다.

a. 사이트의 관리 노드에 원격으로 로그인:

i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`

ii. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.

iii. 루트로 전환하려면 다음 명령을 입력합니다. `su -`

iv. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.

b. 각 관리 노드에 대한 감사 공유를 구성하려면 다음 단계를 반복합니다.

c. 원격 관리 노드에 대한 원격 보안 셸 로그인을 닫습니다. `exit`

11. 명령 셸에서 로그아웃합니다. `exit`

**NFS 감사 통합을 확인하는 중입니다**

감사 공유를 구성하고 NFS 감사 클라이언트를 추가한 후에는 감사 클라이언트 공유를 마운트하고 감사 공유에서 해당 파일을 사용할 수 있는지 확인할 수 있습니다.

단계

1. AMS 서비스를 호스팅하는 관리 노드의 클라이언트 측 IP 주소를 사용하여 연결(또는 클라이언트 시스템의 변형)을 확인합니다. 입력: `ping IP_address`

서버가 응답하여 연결을 나타내는지 확인합니다.

2. 클라이언트 운영 체제에 적합한 명령을 사용하여 감사 읽기 전용 공유를 마운트합니다. Linux 명령의 예는 다음과 같습니다(한 줄에 입력).

```
mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export  
myAudit
```

AMS 서비스를 호스팅하는 관리 노드의 IP 주소와 감사 시스템에 대해 미리 정의된 공유 이름을 사용합니다. 마운트 지점은 클라이언트에서 선택한 모든 이름일 수 있습니다(예: `myAudit` 이전 명령에서).

3. 감사 공유에서 파일을 사용할 수 있는지 확인합니다. 입력: `ls myAudit /*`

위치 `myAudit` 감사 공유의 마운트 지점입니다. 하나 이상의 로그 파일이 나열되어야 합니다.

감사 공유에서 **NFS** 감사 클라이언트 제거

NFS 감사 클라이언트는 IP 주소를 기반으로 감사 공유에 대한 액세스 권한이 부여됩니다. IP

주소를 제거하여 기존 감사 클라이언트를 제거할 수 있습니다.

필요한 것

- 에 가 있어야 합니다 Passwords.txt 루트/관리자 계정 암호가 있는 파일(해당 패키지에서 사용 가능).
- 에 가 있어야 합니다 Configuration.txt 파일(해당 패키지에서 사용 가능).

이 작업에 대해

감사 공유에 액세스할 수 있는 마지막 IP 주소는 제거할 수 없습니다.

단계

1. 기본 관리자 노드에 로그인합니다.

- 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`
- 에 나열된 암호를 입력합니다 Passwords.txt 파일.
- 루트로 전환하려면 다음 명령을 입력합니다. `su -`
- 에 나열된 암호를 입력합니다 Passwords.txt 파일.

루트로 로그인하면 프롬프트가 에서 변경됩니다 \$ 를 선택합니다 #.

2. NFS 구성 유틸리티를 시작합니다. `config_nfs.rb`

```
-----  
| Shares                | Clients                | Config                |  
-----  
| add-audit-share       | add-ip-to-share       | validate-config      |  
| enable-disable-share  | remove-ip-from-share  | refresh-config       |  
|                       |                       | help                 |  
|                       |                       | exit                 |  
-----
```

3. 감사 공유에서 IP 주소를 제거합니다. `remove-ip-from-share`

서버에 구성된 감사 공유의 번호가 매겨진 목록이 표시됩니다. 감사 공유는 다음과 같이 나열됩니다.  
`/var/local/audit/export`

4. 감사 공유에 해당하는 번호를 입력합니다. `audit_share_number`

감사 공유에 액세스할 수 있는 번호가 매겨진 IP 주소 목록이 표시됩니다.

5. 제거할 IP 주소에 해당하는 번호를 입력합니다.

감사 공유가 업데이트되며 이 IP 주소를 가진 감사 클라이언트에서 더 이상 액세스가 허용되지 않습니다.

6. 메시지가 표시되면 \* Enter \* 를 누릅니다.

NFS 구성 유틸리티가 표시됩니다.

7. NFS 구성 유틸리티를 닫습니다. `exit`
8. StorageGRID 배포가 다른 사이트에 추가 관리 노드가 있는 다중 데이터 센터 사이트 배포인 경우 필요에 따라 다음 감사 공유를 비활성화합니다.
  - a. 각 사이트의 관리자 노드에 원격으로 로그인:
    - i. 다음 명령을 입력합니다. `ssh admin@grid_node_IP`
    - ii. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
    - iii. 루트로 전환하려면 다음 명령을 입력합니다. `su -`
    - iv. 에 나열된 암호를 입력합니다 `Passwords.txt` 파일.
  - b. 이 단계를 반복하여 각 추가 관리 노드에 대한 감사 공유를 구성합니다.
  - c. 원격 관리 노드에 대한 원격 보안 셸 로그인을 닫습니다. `exit`
9. 명령 셸에서 로그아웃합니다. `exit`

#### NFS 감사 클라이언트의 IP 주소 변경

1. 기존 NFS 감사 공유에 새 IP 주소를 추가합니다.
2. 원래 IP 주소를 제거합니다.

#### 관련 정보

["감사 공유에 NFS 감사 클라이언트 추가"](#)

["감사 공유에서 NFS 감사 클라이언트 제거"](#)

## 아카이브 노드 관리

선택적으로 StorageGRID 시스템의 각 데이터 센터 사이트를 아카이브 노드와 함께 구축할 수 있습니다. 그러면 TSM(Tivoli Storage Manager)과 같은 타겟 외부 아카이브 스토리지 시스템에 연결할 수 있습니다.

외부 타겟에 대한 접속을 구성한 후 TSM 성능을 최적화하도록 아카이브 노드를 구성하고, TSM 서버가 용량 또는 사용 불가 상태에 근접할 때 아카이브 노드를 오프라인으로 전환하고, 복제 및 검색 설정을 구성할 수 있습니다. 아카이브 노드에 대한 사용자 지정 알람을 설정할 수도 있습니다.

- ["아카이브 노드의 정의"](#)
- ["아카이브 스토리지에 대한 아카이브 노드 연결 구성"](#)
- ["보관 노드에 대한 사용자 정의 경보 설정"](#)
- ["Tivoli Storage Manager 통합"](#)

### 아카이브 노드의 정의

아카이브 노드는 객체 데이터의 장기 저장을 위해 외부 아카이브 스토리지 시스템을 대상으로 지정할 수 있는 인터페이스를 제공합니다. 또한 아카이브 노드는 이 연결과 StorageGRID 시스템과 대상 외부 아카이브 스토리지 시스템 간의 개체 데이터 전송을 모니터링합니다.

**Overview: ARC (DC1-ARC1-98-165) - ARC**  
Updated: 2015-09-30 10:29:18 PDT

ARC State:	Online	
ARC Status:	No Errors	
Tivoli Storage Manager State:	Online	
Tivoli Storage Manager Status:	No Errors	
Store State:	Online	
Store Status:	No Errors	
Retrieve State:	Online	
Retrieve Status:	No Errors	
Inbound Replication Status:	No Errors	
Outbound Replication Status:	No Errors	

**Node Information**

Device Type:	Archive Node
Version:	10.2.0
Build:	20150928.2133.a27b3ab
Node ID:	19002524
Site ID:	10

삭제할 수 없지만 정기적으로 액세스하지 않는 오브젝트 데이터는 언제든지 스토리지 노드의 회전식 디스크에서 벗어나 클라우드 또는 테이프와 같은 외부 아카이브 스토리지로 이동할 수 있습니다. 이러한 오브젝트 데이터 아카이빙은 데이터 센터 사이트의 아카이브 노드 구성과 이 아카이브 노드가 콘텐츠 배치 지침을 위한 "대상"으로 선택된 ILM 규칙 구성을 통해 수행됩니다. 아카이브 노드는 아카이빙된 객체 데이터 자체를 관리하지 않으며, 이는 외부 아카이브 디바이스가 수행합니다.



오브젝트 메타데이터는 아카이빙되지 않지만 스토리지 노드에 유지됩니다.

## ARC 서비스의 정의

아카이브 노드의 아카이브(ARC) 서비스는 TSM 미들웨어를 통해 테이프와 같은 외부 아카이브 스토리지에 대한 연결을 구성하는 데 사용할 수 있는 관리 인터페이스를 제공합니다.

이 서비스는 외부 아카이브 스토리지 시스템과 상호 작용하여 니어라인 스토리지에 대한 오브젝트 데이터를 전송하고 클라이언트 애플리케이션이 아카이빙된 객체를 요청할 때 검색을 수행하는 ARC 서비스입니다. 클라이언트 애플리케이션이 아카이빙된 객체를 요청하면 스토리지 노드는 ARC 서비스에서 객체 데이터를 요청합니다. ARC 서비스는 외부 아카이브 스토리지 시스템에 요청을 하여 요청된 객체 데이터를 검색하여 ARC 서비스로 전송합니다. ARC 서비스는 객체 데이터를 확인하고 이를 스토리지 노드로 전달하여 객체를 요청한 클라이언트 애플리케이션으로 반환합니다.

TSM 미들웨어를 통해 테이프로 아카이빙된 오브젝트 데이터에 대한 요청은 검색 효율성을 위해 관리됩니다. 테이프에 순차적으로 저장된 객체가 동일한 순서로 요청되도록 요청을 주문할 수 있습니다. 그런 다음 요청이 스토리지 디바이스에 제출될 때까지 대기합니다. 아카이브 장치에 따라 서로 다른 볼륨에 있는 개체에 대한 여러 요청을 동시에 처리할 수 있습니다.

## 아카이브 스토리지에 대한 아카이브 노드 연결 구성

아카이브 노드를 외부 아카이브와 연결하도록 구성할 때 대상 유형을 선택해야 합니다.

StorageGRID 시스템은 S3 인터페이스를 통해 오브젝트 데이터를 클라우드에 아카이빙하거나 TSM(Tivoli Storage Manager) 미들웨어를 통해 테이프로 아카이빙할 수 있도록 지원합니다.



아카이브 노드에 대해 아카이브 타겟의 유형을 구성한 후에는 타겟 유형을 변경할 수 없습니다.

- "S3 API를 통해 클라우드에 아카이빙"
- "TSM 미들웨어를 통해 테이프에 아카이빙"
- "아카이브 노드 검색 설정을 구성합니다"
- "아카이브 노드 복제 구성"

### S3 API를 통해 클라우드에 아카이빙

아카이브 노드를 구성하여 AWS(Amazon Web Services)에 직접 연결하거나 S3 API를 통해 StorageGRID 시스템에 연결할 수 있는 다른 시스템에 연결할 수 있습니다.



S3 API를 통해 아카이브 노드에서 외부 아카이브 스토리지 시스템으로 오브젝트를 이동한 후 ILM 클라우드 스토리지 풀로 대체되었으며 더 많은 기능을 제공합니다. Cloud Tiering - S3(Simple Storage Service) \* 옵션은 계속 지원되지만 Cloud Storage Pool을 대신 구현하는 것이 좋습니다.

현재 \* Cloud Tiering - Simple Storage Service(S3) \* 옵션과 함께 아카이브 노드를 사용 중인 경우 오브젝트를 클라우드 스토리지 풀로 마이그레이션하는 것을 고려해 보십시오. 정보 수명 주기 관리를 사용하여 개체를 관리하는 방법에 대한 지침을 참조하십시오.

### 관련 정보

["ILM을 사용하여 개체를 관리합니다"](#)

### S3 API에 대한 연결 설정 구성

S3 인터페이스를 사용하여 아카이브 노드에 연결하는 경우 S3 API에 대한 연결 설정을 구성해야 합니다. 이러한 설정이 구성될 때까지 ARC 서비스는 외부 아카이브 스토리지 시스템과 통신할 수 없기 때문에 주요 알람 상태를 유지합니다.



S3 API를 통해 아카이브 노드에서 외부 아카이브 스토리지 시스템으로 오브젝트를 이동한 후 ILM 클라우드 스토리지 풀로 대체되었으며 더 많은 기능을 제공합니다. Cloud Tiering - S3(Simple Storage Service) \* 옵션은 계속 지원되지만 Cloud Storage Pool을 대신 구현하는 것이 좋습니다.

현재 \* Cloud Tiering - Simple Storage Service(S3) \* 옵션과 함께 아카이브 노드를 사용 중인 경우 오브젝트를 클라우드 스토리지 풀로 마이그레이션하는 것을 고려해 보십시오. 정보 수명 주기 관리를 사용하여 개체를 관리하는 방법에 대한 지침을 참조하십시오.

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 타겟 아카이브 스토리지 시스템에 버킷을 생성해야 합니다.
  - 버킷은 단일 아카이브 노드 전용이어야 합니다. 다른 아카이브 노드 또는 다른 응용 프로그램에서는 사용할 수 없습니다.
  - 버킷은 해당 위치에 적합한 영역을 선택해야 합니다.
  - 버킷을 버전 관리가 일시 중지되도록 구성해야 합니다.

- 오브젝트 분할이 활성화되어 있어야 하며 최대 세그먼트 크기는 4.5GiB(4,831,838,208바이트) 이하여야 합니다. S3를 외부 아카이브 스토리지 시스템으로 사용하면 이 값을 초과하는 S3 API 요청이 실패합니다.

단계

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. Archive Node \* \* \* ARC \* Target \* 을 선택합니다.
3. Configuration \* > \* Main \* 을 선택합니다.

4. Target Type 드롭다운 목록에서 \* Cloud Tiering - Simple Storage Service (S3) \* 를 선택합니다.



대상 유형을 선택할 때까지 구성 설정을 사용할 수 없습니다.

5. 아카이브 노드가 타겟 외부 S3 지원 아카이브 스토리지 시스템에 연결하는 데 사용할 클라우드 계층화(S3) 계정을 구성합니다.

이 페이지의 대부분의 필드는 설명이 필요 없습니다. 다음은 지침이 필요한 필드에 대한 설명입니다.

- \* 지역 \*: \* AWS 사용 \* 이 선택된 경우에만 사용할 수 있습니다. 선택한 지역은 버킷 지역과 일치해야 합니다.
- \* 엔드포인트 \* 및 \* AWS 사용 \*: AWS(Amazon Web Services)의 경우 \* AWS 사용 \* 을 선택합니다. 그러면 \* Endpoint \* 가 버킷 이름 및 영역 속성에 따라 끝점 URL로 자동으로 채워집니다. 예를 들면 다음과 같습니다.

`https://bucket.region.amazonaws.com`

비 AWS 타겟의 경우 포트 번호를 포함하여 버킷을 호스팅하는 시스템의 URL을 입력합니다. 예를 들면 다음과



같습니다.

https://system.com:1080

- \* 엔드포인트 인증 \*: 기본적으로 사용됩니다. 외부 아카이브 스토리지 시스템에 대한 네트워크를 신뢰할 수 있는 경우 확인란을 선택 취소하여 대상 외부 아카이브 스토리지 시스템에 대한 엔드포인트 SSL 인증서 및 호스트 이름 확인을 비활성화할 수 있습니다. StorageGRID 시스템의 다른 인스턴스가 대상 아카이브 스토리지 디바이스이고 시스템에서 공개적으로 서명된 인증서를 구성한 경우 확인란을 선택한 상태로 유지할 수 있습니다.
- \* 스토리지 클래스 \*: 일반 스토리지로 \* 표준(기본값) \* 을 선택합니다. 쉽게 다시 만들 수 있는 개체에 대해서만 \* Reduced Redundancy \* 를 선택합니다. \* 감소된 중복 \* 은 낮은 신뢰성을 통해 저렴한 저장 공간을 제공합니다. 대상 아카이브 스토리지 시스템이 StorageGRID 시스템의 또 다른 인스턴스인 경우 \* 스토리지 클래스 \* 는 오브젝트가 인제스트될 때 이중 커밋이 사용되는 경우 대상 시스템에서 인제스트할 때 오브젝트의 중간 복제본 수를 제어합니다.

6. 변경 내용 적용 \* 을 클릭합니다.

지정된 구성 설정이 검증되어 StorageGRID 시스템에 적용됩니다. 구성이 완료되면 타겟을 변경할 수 없습니다.

관련 정보

["ILM을 사용하여 개체를 관리합니다"](#)

S3 API에 대한 연결 설정을 수정합니다

S3 API를 통해 아카이브 노드가 외부 아카이브 스토리지 시스템에 연결되도록 구성된 후 연결이 변경될 경우 일부 설정을 수정할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

Cloud Tiering(S3) 계정을 변경하는 경우 이전에 아카이브 노드에서 버킷으로 수집했던 모든 오브젝트를 비롯하여 사용자 액세스 자격 증명이 버킷에 대한 읽기/쓰기 액세스를 가져야 합니다.

단계

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. Archive Node\_ \* \* \* ARC \* \* Target \* 을 선택합니다.
3. Configuration \* > \* Main \* 을 선택합니다.

Target Type: Cloud Tiering - Simple Storage Service (S3)

**Cloud Tiering (S3) Account**

Bucket Name: name

Region: Virginia or Pacific Northwest (us-east-1)


Endpoint: https://10.10.10.123:8082  Use AWS

Endpoint Authentication:

Access Key: ABCD123EFG45AB

Secret Access Key: ●●●●●●

Storage Class: Standard (Default)

**Apply Changes** 

4. 필요에 따라 계정 정보를 수정합니다.

스토리지 클래스를 변경하면 새 오브젝트 데이터가 새 스토리지 클래스에 저장됩니다. 기존 객체는 인제스트할 때 스토리지 클래스 세트 아래에 계속 저장됩니다.



버킷 이름, 지역 및 종점, AWS 값을 사용하며 변경할 수 없습니다.

5. 변경 내용 적용 \* 을 클릭합니다.

#### Cloud Tiering Service 상태 수정

Cloud Tiering Service의 상태를 변경하여 S3 API를 통해 연결되는 타겟 외부 아카이브 스토리지 시스템에 대한 아카이브 노드의 읽기 및 쓰기 기능을 제어할 수 있습니다.

#### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 아카이브 노드를 구성해야 합니다.

#### 이 작업에 대해

Cloud Tiering Service State를 \* Read-Write Disabled \* 로 변경하면 아카이브 노드를 효과적으로 오프라인 상태로 전환할 수 있습니다.

#### 단계

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. Archive Node\_ \* > \* ARC \* 를 선택합니다.
3. Configuration \* > \* Main \* 을 선택합니다.

4. Cloud Tiering Service State \* 를 선택합니다.
5. 변경 내용 적용 \* 을 클릭합니다.

#### S3 API 연결에 대한 저장소 실패 횟수 재설정

아카이브 노드가 S3 API를 통해 아카이브 스토리지 시스템에 연결된 경우 ARVF(Store Failure Count) 경보를 지우는 데 사용할 수 있는 저장소 오류 카운트를 재설정할 수 있습니다.

#### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

#### 단계

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. Archive Node\_ \* \* \* ARC \* \* Store \* 를 선택합니다.
3. Configuration \* > \* Main \* 을 선택합니다.

4. Reset Store Failure Count \* 를 선택합니다.

5. 변경 내용 적용 \* 을 클릭합니다.

Store Failures 속성이 0으로 재설정됩니다.

Cloud Tiering-S3에서 클라우드 스토리지 풀로 오브젝트 마이그레이션

현재 \* Cloud Tiering - S3(Simple Storage Service) \* 기능을 사용하여 오브젝트 데이터를 S3 버킷으로 계층화하려는 경우 대신 오브젝트를 Cloud Storage Pool로 마이그레이션하는 것을 고려해 보십시오. 클라우드 스토리지 풀은 StorageGRID 시스템의 모든 스토리지 노드를 활용하는 확장 가능한 접근 방식을 제공합니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- Cloud Tiering에 구성된 S3 버킷에 오브젝트를 이미 저장했습니다.



오브젝트 데이터를 마이그레이션하기 전에 NetApp 고객 담당자에게 연락하여 관련 비용을 파악하고 관리하십시오.

이 작업에 대해

ILM 관점에서 Cloud Storage Pool은 스토리지 풀과 유사합니다. 그러나 스토리지 풀은 StorageGRID 시스템 내의 스토리지 노드 또는 아카이브 노드로 구성되지만, 클라우드 스토리지 풀은 외부 S3 버킷으로 구성됩니다.

Cloud Tiering-S3에서 클라우드 스토리지 풀로 오브젝트를 마이그레이션하기 전에 먼저 S3 버킷을 생성한 다음 StorageGRID에서 클라우드 스토리지 풀을 생성해야 합니다. 그런 다음 새 ILM 정책을 생성하고 Cloud Tiering 버킷에 오브젝트를 저장하는 데 사용되는 ILM 규칙을 Cloud Storage Pool에 동일한 오브젝트를 저장하는 클론 생성된 ILM 규칙으로 대체할 수 있습니다.



오브젝트를 클라우드 스토리지 풀에 저장할 경우 해당 오브젝트의 복사본도 StorageGRID 내에 저장할 수 없습니다. 현재 Cloud Tiering에 사용 중인 ILM 규칙이 개체를 동시에 여러 위치에 저장하도록 구성된 경우 해당 기능이 손실되므로 이 선택적 마이그레이션을 계속 수행할지 여부를 고려하십시오. 이 마이그레이션을 계속할 경우 기존 규칙을 복제하는 대신 새 규칙을 만들어야 합니다.

단계

1. 클라우드 스토리지 풀을 생성합니다.

Cloud Storage Pool에 새로운 S3 버킷을 사용하여 Cloud Storage Pool에서 관리하는 데이터만 포함되도록 합니다.

2. 활성 ILM 정책에서 객체가 Cloud Tiering 버킷에 저장되도록 하는 ILM 규칙을 찾습니다.

3. 이러한 각 규칙을 복제합니다.

4. 클론 복제된 규칙에서 배치 위치를 새 Cloud Storage Pool로 변경합니다.

5. 복제된 규칙을 저장합니다.

6. 새 규칙을 사용하는 새 정책을 만듭니다.

7. 새 정책을 시뮬레이션하고 활성화합니다.

새 정책이 활성화되어 ILM 평가가 발생하면 Cloud Tiering에 구성된 S3 버킷에서 Cloud Storage Pool에 구성된 S3 버킷으로 오브젝트가 이동됩니다. 그리드의 사용 가능한 공간은 영향을 받지 않습니다. 오브젝트를 Cloud Storage Pool로 이동한 후 Cloud Tiering 버킷에서 제거됩니다.

## 관련 정보

["ILM을 사용하여 개체를 관리합니다"](#)

## TSM 미들웨어를 통해 테이프 아카이빙

테이프 라이브러리를 포함하여 랜덤 또는 순차 액세스 스토리지 디바이스에 오브젝트 데이터를 저장하고 검색하기 위한 논리 인터페이스를 제공하는 TSM(Tivoli Storage Manager) 서버를 대상으로 아카이브 노드를 구성할 수 있습니다.

아카이브 노드의 ARC 서비스는 TSM 서버에 대한 클라이언트 역할을 하며 Tivoli Storage Manager를 아카이빙 스토리지 시스템과 통신하는 미들웨어로 사용됩니다.

## TSM 관리 클래스

TSM 미들웨어에 의해 정의된 관리 클래스는 TSM의 백업 및 아카이브 작업이 작동하는 방식을 요약하고 TSM 서버에 의해 적용되는 콘텐츠에 대한 규칙을 지정하는 데 사용할 수 있습니다. 이러한 규칙은 StorageGRID 시스템의 ILM 정책과 독립적으로 작동하며, 객체가 영구적으로 저장되고 아카이브 노드에서 검색할 수 있도록 항상 사용 가능한 StorageGRID 시스템의 요구 사항과 일치해야 합니다. 아카이브 노드에서 TSM 서버로 객체 데이터를 전송한 후 TSM 서버에서 관리하는 테이프에 객체 데이터를 저장하는 동안 TSM 수명주기 및 보존 규칙이 적용됩니다.

TSM 관리 클래스는 아카이브 노드에서 TSM 서버로 객체가 전송된 후 데이터 위치 또는 보존에 대한 규칙을 적용하기 위해 TSM 서버에서 사용됩니다. 예를 들어, 데이터베이스 백업으로 식별된 객체(최신 데이터로 덮어쓸 수 있는 임시 콘텐츠)는 애플리케이션 데이터(무기한으로 보존되어야 하는 고정 콘텐츠)와 다르게 처리될 수 있습니다.

## TSM 미들웨어에 대한 연결 구성

아카이브 노드가 TSM(Tivoli Storage Manager) 미들웨어와 통신하려면 먼저 여러 설정을 구성해야 합니다.

## 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

## 이 작업에 대해

이러한 설정이 구성될 때까지 ARC 서비스는 Tivoli Storage Manager와 통신할 수 없기 때문에 주요 알람 상태를 유지합니다.

## 단계

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. Archive Node\_ \* \* \* ARC \* \* Target \* 을 선택합니다.
3. Configuration \* > \* Main \* 을 선택합니다.



## Configuration: ARC (DC1-ARC1-98-165) - Target

Updated: 2015-09-28 09:56:36 PDT

Target Type:

Tivoli Storage Manager State:

### Target (TSM) Account

Server IP or Hostname:

Server Port:

Node Name:

User Name:

Password:

Management Class:

Number of Sessions:

Maximum Retrieve Sessions:

Maximum Store Sessions:

Apply Changes

4. Target Type \* 드롭다운 목록에서 \* TSM(Tivoli Storage Manager) \* 을 선택합니다.
5. Tivoli Storage Manager State \* 의 경우 \* Offline \* 을 선택하여 TSM 미들웨어 서버에서 검색을 방지합니다.

기본적으로 Tivoli Storage Manager State는 Online으로 설정되어 있으므로 Archive Node는 TSM 미들웨어 서버에서 객체 데이터를 검색할 수 있습니다.

6. 다음 정보를 입력합니다.
  - \* 서버 IP 또는 호스트 이름 \*: ARC 서비스에서 사용하는 TSM 미들웨어 서버의 IP 주소 또는 정규화된 도메인 이름을 지정합니다. 기본 IP 주소는 127.0.0.1입니다.
  - \* 서버 포트\*: TSM 미들웨어 서버에서 ARC 서비스가 연결할 포트 번호를 지정합니다. 기본값은 1500입니다.
  - \* 노드 이름 \*: 아카이브 노드의 이름을 지정합니다. TSM 미들웨어 서버에 등록된 이름(arc - user)을 입력해야 합니다.
  - \* 사용자 이름 \*: ARC 서비스가 TSM 서버에 로그인하는 데 사용하는 사용자 이름을 지정합니다. 아카이브 노드에 대해 지정한 기본 사용자 이름(arc - user) 또는 관리 사용자를 입력합니다.
  - \* 암호 \*: ARC 서비스가 TSM 서버에 로그인하기 위해 사용하는 암호를 지정합니다.
  - \* 관리 클래스 \*: 객체가 StorageGRID 시스템에 저장될 때 관리 클래스가 지정되지 않았거나 지정된 관리 클래스가 TSM 미들웨어 서버에 정의되지 않은 경우 사용할 기본 관리 클래스를 지정합니다.
  - \* Number of Sessions \*: 아카이브 노드 전용 TSM 미들웨어 서버의 테이프 드라이브 수를 지정합니다. 아카이브 노드는 마운트 지점당 최대 1개의 세션을 동시에 생성하고 적은 수의 추가 세션(5개 미만)을 생성합니다.

보관 노드를 등록 또는 업데이트할 때 MAXNUMMP(최대 탑재 지점 수)에 대해 설정된 값과 같도록 이 값을

변경해야 합니다. (설정된 값이 없는 경우 REGISTER 명령에서 사용되는 MAXNUMMP의 기본값은 1입니다.)

또한 TSM 서버에 대한 MAXSESSIONS 값을 최소한 ARC 서비스에 대해 설정된 세션 수 만큼 큰 숫자로 변경해야 합니다. TSM 서버의 MAXSESSIONS 기본값은 25입니다.

- \* Maximum Retrieve Sessions \*: ARC 서비스가 검색 작업을 위해 TSM 미들웨어 서버에 열 수 있는 최대 세션 수를 지정합니다. 대부분의 경우 적절한 값은 세션 수에서 최대 저장소 세션을 뺀 수입니다. 저장 및 검색을 위해 하나의 테이프 드라이브를 공유해야 하는 경우 세션 수와 동일한 값을 지정하십시오.
- \* Maximum Store Sessions \*: 아카이브 작업을 위해 ARC 서비스가 TSM 미들웨어 서버에 열 수 있는 최대 동시 세션 수를 지정합니다.

타겟 아카이브 스토리지 시스템이 딱 차고 검색할 수만 있는 경우를 제외하고 이 값은 1로 설정해야 합니다. 검색을 위해 모든 세션을 사용하려면 이 값을 0으로 설정합니다.

7. 변경 내용 적용 \* 을 클릭합니다.

#### TSM 미들웨어 세션에 대한 아카이브 노드 최적화

아카이브 노드의 세션을 구성하여 TSM(Tivoli Server Manager)에 연결되는 아카이브 노드의 성능을 최적화할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

일반적으로 아카이브 노드가 TSM 미들웨어 서버에 열려 있는 동시 세션 수는 TSM 서버가 아카이브 노드 전용으로 사용하는 테이프 드라이브 수로 설정됩니다. 나머지 테이프 드라이브는 검색을 위해 할당되는 동안 보관을 위해 하나의 테이프 드라이브가 할당됩니다. 그러나 스토리지 노드가 아카이브 노드 복제본에서 재구축되거나 아카이브 노드가 읽기 전용 모드로 작동하는 경우 최대 검색 세션 수를 동시 세션 수와 같도록 설정하여 TSM 서버 성능을 최적화할 수 있습니다. 그 결과, 모든 드라이브를 동시에 검색할 수 있으며, 해당하는 경우 이들 드라이브 중 하나를 스토리지에도 사용할 수 있습니다.

단계

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. Archive Node\_ \* \* \* ARC \* \* Target \* 을 선택합니다.
3. Configuration \* > \* Main \* 을 선택합니다.
4. 최대 검색 세션 \* 을 \* 세션 수 \* 와 동일하게 변경합니다.



## Configuration: ARC (DC1-ARC1-98-165) - Target

Updated: 2015-09-28 09:56:36 PDT

Target Type:

Tivoli Storage Manager State:

### Target (TSM) Account

Server IP or Hostname:

Server Port:

Node Name:

User Name:

Password:

Management Class:

Number of Sessions:

Maximum Retrieve Sessions:

Maximum Store Sessions:

Apply Changes

5. 변경 내용 적용 \* 을 클릭합니다.

#### TSM에 대한 아카이브 상태 및 카운터 구성

아카이브 노드가 TSM 미들웨어 서버에 연결된 경우 아카이브 노드의 아카이브 저장소 상태를 온라인 또는 오프라인으로 구성할 수 있습니다. 또한 아카이브 노드가 처음 시작될 때 아카이브 저장소를 비활성화하거나 관련 알람에 대해 추적 중인 실패 수를 재설정할 수 있습니다.

#### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.


#### 단계

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. Archive Node\_ \* \* \* ARC \* \* Store \* 를 선택합니다.
3. Configuration \* > \* Main \* 을 선택합니다.



Overview Alarms Reports **Configuration**

Main Alarms


 **Configuration: ARC (DC1-ARC1-98-165) - Store**  
Updated: 2015-09-29 17:10:12 PDT

---

Store State

Archive Store Disabled on Startup

Reset Store Failure Count

**Apply Changes** 

4. 필요에 따라 다음 설정을 수정합니다.

- Store State(상태 저장): 구성 요소 상태를 다음 중 하나로 설정합니다.
  - 온라인: 아카이브 노드는 스토리지의 객체 데이터를 아카이브 스토리지 시스템에 처리하는 데 사용할 수 있습니다.
  - 오프라인: 아카이브 노드는 스토리지의 객체 데이터를 아카이브 스토리지 시스템에 처리하는 데 사용할 수 없습니다.
- 시작할 때 아카이브 저장소 사용 안 함: 이 옵션을 선택하면 아카이브 저장소 구성 요소는 다시 시작할 때 읽기 전용 상태로 유지됩니다. 대상 아카이브 스토리지 시스템에 대한 스토리지를 영구적으로 해제하는 데 사용됩니다. 대상 아카이브 스토리지 시스템에서 콘텐츠를 수락할 수 없는 경우에 유용합니다.
- Reset Store Failure Count(저장 실패 카운트 재설정): 저장소 오류에 대한 카운터를 재설정합니다. ARVF(Store Failure) 알람을 소거하는 데 사용할 수 있습니다.

5. 변경 내용 적용 \* 을 클릭합니다.

관련 정보

["TSM 서버가 용량에 도달할 때 아카이브 노드 관리"](#)

**TSM** 서버가 용량에 도달할 때 아카이브 노드 관리

TSM 서버에서 관리하는 TSM 데이터베이스나 아카이브 미디어 스토리지가 용량에 근접하는 경우 TSM 서버에서 아카이브 노드를 알릴 수 없습니다. 아카이브 노드는 TSM 서버가 새 콘텐츠 수신을 중지한 후에도 TSM 서버로 전송하기 위한 객체 데이터를 계속 수락합니다. 이 콘텐츠는 TSM 서버에서 관리하는 미디어에 쓸 수 없습니다. 이 경우 알람이 트리거됩니다. TSM 서버의 사전 모니터링을 통해 이러한 상황을 방지할 수 있습니다.

필요한 것

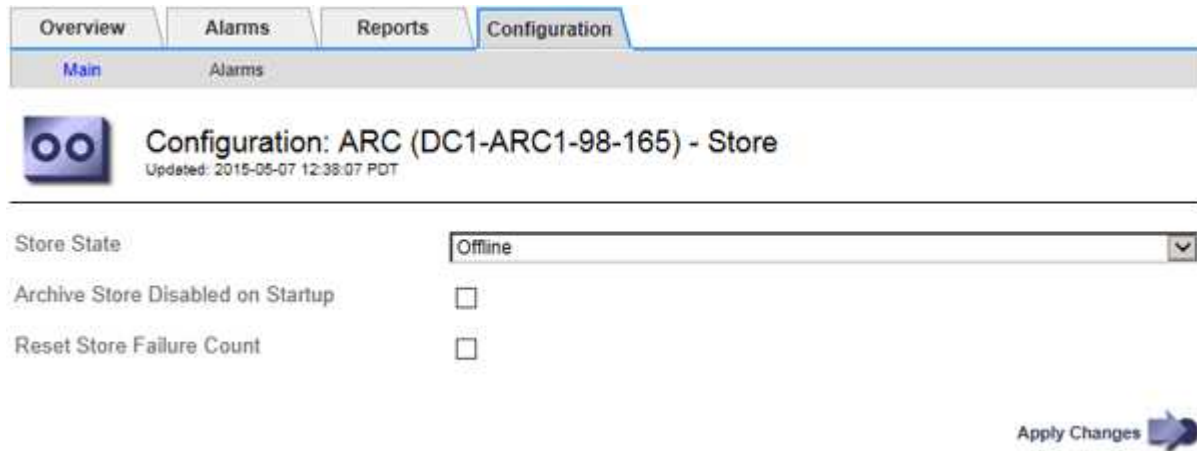
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

ARC 서비스가 TSM 서버로 추가 콘텐츠를 전송하지 않도록 하려면 \* ARC \* \* \* Store \* 구성 요소를 오프라인으로 전환하여 아카이브 노드를 오프라인으로 전환할 수 있습니다. 이 절차는 TSM 서버를 유지 보수할 수 없는 경우 알람을 방지하는 데에도 유용할 수 있습니다.

단계

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. Archive Node\_ \* \* \* ARC \* \* Store \* 를 선택합니다.
3. Configuration \* > \* Main \* 을 선택합니다.



4. Store State \* 를 로 변경합니다 Offline.
5. 시작 시 \* 아카이브 저장소 사용 안 함 \* 을 선택합니다.
6. 변경 내용 적용 \* 을 클릭합니다.

**TSM** 미들웨어가 용량에 도달하면 아카이브 노드를 읽기 전용으로 설정합니다

대상 TSM 미들웨어 서버가 용량에 도달하면 아카이브 노드를 최적화하여 검색을 수행할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

단계

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. Archive Node\_ \* \* \* ARC \* \* Target \* 을 선택합니다.
3. Configuration \* > \* Main \* 을 선택합니다.
4. 최대 검색 세션을 세션 수에 나열된 동시 세션 수와 동일하게 변경합니다.
5. 최대 저장 세션을 0으로 변경합니다.



아카이브 노드가 읽기 전용인 경우 최대 저장소 세션을 0으로 변경할 필요가 없습니다. 저장 세션이 생성되지 않습니다.

6. 변경 내용 적용 \* 을 클릭합니다.

아카이브 노드 검색 설정을 구성합니다

아카이브 노드의 검색 설정을 구성하여 상태를 온라인 또는 오프라인으로 설정하거나 관련 알람에 대해 추적되는 실패 수를 재설정할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

단계

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. Archive Node \* \* \* ARC \* Retrieve \* 를 선택합니다.
3. Configuration \* > \* Main \* 을 선택합니다.

Configuration: ARC (DC1-ARC1-98-165) - Retrieve  
Updated: 2015-05-07 12:24:45 PDT

Retrieve State	Online
Reset Request Failure Count	<input type="checkbox"/>
Reset Verification Failure Count	<input type="checkbox"/>

Apply Changes

4. 필요에 따라 다음 설정을 수정합니다.

- \* 상태 검색 \*: 구성 요소 상태를 다음 중 하나로 설정합니다.
  - 온라인: 그리드 노드를 사용하여 보관 미디어 장치에서 오브젝트 데이터를 검색할 수 있습니다.
  - 오프라인: 그리드 노드를 사용하여 오브젝트 데이터를 검색할 수 없습니다.
- Reset Request Failures Count(요청 실패 카운트 재설정): 요청 실패에 대한 카운터를 재설정하려면 확인란을 선택합니다. ARRF(Request Failures) 알람을 소거하는 데 사용할 수 있습니다.
- 검증 실패 카운트 재설정: 체크 박스를 선택하면 검색된 개체 데이터에 대한 검증 실패 시 카운터가 재설정됩니다. 이는 ARRV (Verification Failures) 알람을 지우는 데 사용할 수 있습니다.

5. 변경 내용 적용 \* 을 클릭합니다.

아카이브 노드 복제 구성

아카이브 노드에 대한 복제 설정을 구성하고 인바운드 및 아웃바운드 복제를 비활성화하거나 관련 알람에 대해 추적되는 실패 수를 재설정할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

단계

1. 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택합니다.
2. Archive Node\_ \* > \* ARC \* > \* Replication \* 을 선택합니다.
3. Configuration \* > \* Main \* 을 선택합니다.

Configuration: ARC (DC1-ARC1-98-165) - Replication  
Updated: 2015-05-07 12:21:53 PDT

Reset Inbound Replication Failure Count

Reset Outbound Replication Failure Count

**Inbound Replication**

Disable Inbound Replication

**Outbound Replication**

Disable Outbound Replication

Apply Changes

4. 필요에 따라 다음 설정을 수정합니다.

- \* 인바운드 복제 실패 횟수 재설정 \*: 인바운드 복제 실패에 대한 카운터를 재설정하려면 선택합니다. RIRF(인바운드 복제 - - 실패) 경보를 지우는 데 사용할 수 있습니다.
- \* 아웃바운드 복제 실패 횟수 재설정 \*: 아웃바운드 복제 실패에 대한 카운터를 재설정하려면 선택합니다. RORF(아웃바운드 복제 - - 실패) 경보를 지우는 데 사용할 수 있습니다.
- \* 인바운드 복제 비활성화 \*: 유지 관리 또는 테스트 절차의 일부로 인바운드 복제를 비활성화하려면 선택합니다. 정상 작동 중에 선택을 취소합니다.

인바운드 복제가 비활성화된 경우 StorageGRID 시스템의 다른 위치로 복제하기 위해 ARC 서비스에서 개체 데이터를 검색할 수 있지만 다른 시스템 위치에서 이 ARC 서비스로 개체를 복제할 수는 없습니다. ARC 서비스는 읽기 전용입니다.

- \* 아웃바운드 복제 비활성화 \*: 유지 관리 또는 테스트 절차의 일환으로 아웃바운드 복제(HTTP 검색을 위한 콘텐츠 요청 포함)를 비활성화하려면 이 확인란을 선택합니다. 정상 작동 중에 선택하지 않은 상태로 둡니다.

아웃바운드 복제를 비활성화하면 개체 데이터를 이 ARC 서비스로 복사하여 ILM 규칙을 충족할 수 있지만, StorageGRID 시스템의 다른 위치로 복제하기 위해 ARC 서비스에서 개체 데이터를 검색할 수는 없습니다. ARC 서비스는 쓰기 전용입니다.

5. 변경 내용 적용 \* 을 클릭합니다.

## 보관 노드에 대한 사용자 정의 경고 설정

아카이브 노드에서 아카이브 스토리지 시스템의 객체 데이터 검색 속도와 효율성을 모니터링하는 데 사용되는 ARQL 및 ARRL 속성에 대한 사용자 지정 경보를 설정해야 합니다.

- ARQL: 평균 대기열 길이. 오브젝트 데이터가 아카이브 스토리지 시스템에서 검색을 위해 대기할 때까지 걸리는 평균 시간(마이크로초)입니다.
- ARRL: 평균 요청 지연 시간 아카이브 노드에서 아카이브 스토리지 시스템의 오브젝트 데이터를 검색하는 데 필요한 평균 시간(마이크로초)입니다.

이러한 속성에 허용되는 값은 아카이브 스토리지 시스템의 구성 및 사용 방식에 따라 달라집니다. (\* ARC \* > \* Retrieve \* > \* Overview \* > \* Main \* 로 이동합니다.) 요청 시간 초과 및 검색 요청에 사용할 수 있는 세션 수에 대해 설정된 값은 특히 영향을 줍니다.

통합이 완료된 후 아카이브 노드의 오브젝트 데이터 검색을 모니터링하여 일반적인 검색 시간 및 대기열 길이 값을 설정합니다. 그런 다음 비정상적인 작동 조건이 발생할 경우 트리거되는 ARQL 및 ARRL에 대한 사용자 지정 알람을 생성합니다.

관련 정보

["모니터링 및 문제 해결"](#)

## Tivoli Storage Manager 통합

이 섹션에는 TSM 서버 구성에 영향을 미치는 아카이브 노드 운영 세부 정보를 비롯하여 아카이브 노드를 TSM(Tivoli Storage Manager) 서버와 통합하기 위한 Best Practice 및 설정 정보가 포함되어 있습니다.

- ["아카이브 노드 구성 및 작업"](#)
- ["구성 모범 사례"](#)
- ["아카이브 노드 설정을 완료합니다"](#)

아카이브 노드 구성 및 작업

StorageGRID 시스템은 아카이브 노드를 무기한으로 저장되고 항상 액세스할 수 있는 위치로 관리합니다.

오브젝트가 수집되면 StorageGRID 시스템에 정의된 ILM(정보 수명 주기 관리) 규칙에 따라 아카이브 노드를 비롯한 모든 필요한 위치에 복사본이 만들어집니다. 아카이브 노드는 TSM 서버에 대한 클라이언트 역할을 하며 TSM 클라이언트 라이브러리는 StorageGRID 소프트웨어 설치 프로세스에 의해 아카이브 노드에 설치됩니다. 스토리지의 아카이브 노드에 대한 객체 데이터는 수신된 TSM 서버에 직접 저장됩니다. 아카이브 노드는 TSM 서버에 저장하기 전에 객체 데이터를 스테이징하지 않으며 객체 집계를 수행하지 않습니다. 그러나 데이터 속도가 필요한 경우 아카이브 노드는 하나의 트랜잭션에서 TSM 서버에 여러 복제본을 제출할 수 있습니다.

아카이브 노드가 TSM 서버에 객체 데이터를 저장한 후 TSM 서버에서 해당 수명주기/보존 정책을 사용하여 객체 데이터를 관리합니다. 이러한 보존 정책은 아카이브 노드의 작업과 호환되도록 정의해야 합니다. 즉, 아카이브 노드에서 저장한 개체 데이터는 보관 노드에서 삭제하지 않는 한 영구적으로 저장해야 하며 항상 아카이브 노드에서 액세스할 수 있어야 합니다.

StorageGRID 시스템의 ILM 규칙과 TSM 서버의 수명주기/보존 정책 간에는 연결이 없습니다. 각 개체는 서로 독립적으로 작동하지만, 각 개체는 StorageGRID 시스템으로 수집되므로 TSM 관리 클래스를 할당할 수 있습니다. 이 관리 클래스는 객체 데이터와 함께 TSM 서버로 전달됩니다. 여러 객체 유형에 서로 다른 관리 클래스를 할당하면 TSM 서버가 서로 다른 스토리지 풀에 객체 데이터를 배치하도록 구성하거나 필요에 따라 다른 마이그레이션 또는 보존 정책을 적용하도록 구성할 수 있습니다. 예를 들어 데이터베이스 백업으로 식별된 개체(최신 데이터로 덮어쓸 수 있는 임시 콘텐츠)는 응용 프로그램 데이터(영구적으로 보존해야 하는 고정 콘텐츠)와 다르게 처리될 수 있습니다.

아카이브 노드는 새 TSM 서버 또는 기존 TSM 서버와 통합할 수 있으며 전용 TSM 서버가 필요하지 않습니다. TSM 서버의 크기가 최대 예상 로드에게 적절히 지정되면 TSM 서버를 다른 클라이언트와 공유할 수 있습니다. TSM은 아카이브 노드와 분리된 서버 또는 가상 머신에 설치해야 합니다.

동일한 TSM 서버에 쓰기 위해 아카이브 노드를 두 개 이상 구성할 수 있지만 아카이브 노드가 서로 다른 데이터 세트를 TSM 서버에 쓰는 경우에만 이 구성이 권장됩니다. 각 아카이브 노드가 동일한 객체 데이터의 복제본을 아카이브에 쓸 때 동일한 TSM 서버에 쓰기 위해 아카이브 노드를 두 개 이상 구성하는 것은 권장되지 않습니다. 두 복제본 모두 독립적인 중복 객체 데이터 복제본에 대해 단일 장애 지점(TSM 서버)에 해당합니다.

아카이브 노드는 TSM의 HSM(Hierarchical Storage Management) 구성 요소를 사용하지 않습니다.

#### 구성 모범 사례

TSM 서버를 사이징하고 구성할 때는 아카이브 노드와 함께 작동하도록 최적화하기 위해 이를 최적화하는 모범 사례를 적용해야 합니다.

TSM 서버를 사이징하고 구성할 때는 다음 요소를 고려해야 합니다.

- 아카이브 노드는 TSM 서버에 저장하기 전에 객체를 집계하지 않기 때문에 아카이브 노드에 기록될 모든 객체에 대한 참조를 보유할 수 있도록 TSM 데이터베이스의 크기를 조정해야 합니다.
- 아카이브 노드 소프트웨어는 테이프 또는 기타 이동식 미디어에 직접 개체를 쓰는 데 수반되는 지연 시간을 허용할 수 없습니다. 따라서 이동식 미디어를 사용할 때마다 아카이브 노드에서 저장한 데이터의 초기 스토리지를 위해 TSM 서버를 디스크 스토리지 풀로 구성해야 합니다.
- 이벤트 기반 보존을 사용하려면 TSM 보존 정책을 구성해야 합니다. 아카이브 노드는 생성 기반 TSM 보존 정책을 지원하지 않습니다. 보존 정책에서 `retmin=0` 및 `retver=0`의 권장 설정을 사용합니다. 보존 정책은 보관 노드가 보존 이벤트를 트리거할 때 보존이 시작되고 그 후 0일 동안 유지됨을 나타냅니다. 그러나 `retmin` 및 `retver`에 대한 이러한 값은 선택 사항입니다.

데이터를 테이프 풀로 마이그레이션하도록 디스크 풀을 구성해야 합니다. 즉, 테이프 풀은 디스크 풀의 NXTSTOOL이어야 합니다. 테이프 풀은 두 풀에 동시에 쓰는 디스크 풀의 복제 풀로 구성해서는 안 됩니다. 즉, 테이프 풀은 디스크 풀의 COPYSTGPOOL이 될 수 없습니다. 아카이브 노드 데이터를 포함하는 테이프의 오프라인 복사본을 생성하려면 아카이브 노드 데이터에 사용되는 테이프 풀의 복사본 풀인 두 번째 테이프 풀을 사용하여 TSM 서버를 구성합니다.

아카이브 노드 설정을 완료합니다

설치 프로세스를 완료한 후에는 아카이브 노드가 작동하지 않습니다. StorageGRID 시스템에서 TSM 아카이브 노드에 객체를 저장하려면 먼저 TSM 서버의 설치 및 구성을 완료하고 TSM 서버와 통신하도록 아카이브 노드를 구성해야 합니다.

TSM 검색 및 저장 세션 최적화에 대한 자세한 내용은 아카이브 스토리지 관리에 대한 정보를 참조하십시오.

- ["아카이브 노드 관리"](#)

StorageGRID 시스템에서 아카이브 노드와 통합되도록 TSM 서버를 준비할 때 필요한 경우 다음 IBM 설명서를 참조하십시오.

- ["IBM 테이프 장치 드라이버 설치 및 사용 설명서"](#)
- ["IBM 테이프 장치 드라이버 프로그래밍 참조"](#)

새 TSM 서버를 설치합니다

아카이브 노드를 새 TSM 서버 또는 기존 TSM 서버와 통합할 수 있습니다. 새 TSM 서버를 설치하는 경우 TSM 설명서의 지침에 따라 설치를 완료합니다.



아카이브 노드는 TSM 서버와 함께 호스팅할 수 없습니다.

### TSM 서버 구성

이 섹션에서는 TSM Best Practice에 따라 TSM 서버를 준비하는 방법에 대한 샘플 지침을 제공합니다.

다음 지침은 의 프로세스를 안내합니다.

- TSM 서버에서 디스크 스토리지 풀 및 테이프 스토리지 풀(필요한 경우) 정의
- 아카이브 노드에서 저장된 데이터에 대해 TSM 관리 클래스를 사용하는 도메인 정책을 정의하고 이 도메인 정책을 사용하도록 노드를 등록합니다

이 지침은 참조용으로만 제공됩니다. TSM 설명서를 교체하거나 모든 구성에 적합한 완전하고 포괄적인 지침을 제공하기 위한 지침은 아닙니다. 자세한 요구 사항 및 전체 TSM 서버 설명서를 모두 숙지한 TSM 관리자가 배포별 지침을 제공해야 합니다.

### TSM 테이프 및 디스크 스토리지 풀 정의

아카이브 노드는 디스크 스토리지 풀에 씩니다. 콘텐츠를 테이프에 아카이빙하려면 테이프 스토리지 풀로 콘텐츠를 이동하도록 디스크 스토리지 풀을 구성해야 합니다.

이 작업에 대해

TSM 서버의 경우 Tivoli Storage Manager 내에서 테이프 스토리지 풀과 디스크 스토리지 풀을 정의해야 합니다. 디스크 풀을 정의한 후 디스크 볼륨을 생성하여 디스크 풀에 할당합니다. TSM 서버에서 디스크 전용 스토리지를 사용하는 경우에는 테이프 풀이 필요하지 않습니다.

테이프 스토리지 풀을 생성하려면 TSM 서버에서 여러 단계를 완료해야 합니다. 테이프 라이브러리와 테이프 라이브러리에 하나 이상의 드라이브를 만듭니다. 서버에서 라이브러리까지, 서버에서 드라이브까지 경로를 정의한 다음 드라이브의 디바이스 클래스를 정의합니다.) 이러한 단계에 대한 자세한 내용은 사이트의 하드웨어 구성 및 스토리지 요구 사항에 따라 다를 수 있습니다. 자세한 내용은 TSM 설명서를 참조하십시오.

다음 지침은 프로세스를 보여 줍니다. 사이트 요구 사항은 배포 요구 사항에 따라 다를 수 있습니다. 구성 세부 정보 및 지침은 TSM 설명서를 참조하십시오.



관리자 권한으로 서버에 로그인하고 dsmadm 도구 사용하여 다음 명령을 실행해야 합니다.

단계

1. 테이프 라이브러리를 생성합니다.

```
define library tapelibrary libtype=scsi
```

위치 *tapelibrary* 테이프 라이브러리에 대해 선택한 임의 이름이며 의 값입니다 libtype 테이프 라이브러리의 유형에 따라 달라질 수 있습니다.

2. 서버에서 테이프 라이브러리의 경로를 정의합니다.

```
define path servername tapelibrary srctype=server desttype=library device=lib-  
devicename
```

- *servername* TSM 서버의 이름입니다
- *tapelibrary* 정의한 테이프 라이브러리 이름입니다
- *lib-devicename* 테이프 라이브러리의 디바이스 이름입니다

3. 라이브러리의 드라이브를 정의합니다.

```
define drive tapelibrary drivename
```

- *drivename* 드라이브에 지정할 이름입니다
- *tapelibrary* 정의한 테이프 라이브러리 이름입니다

하드웨어 구성에 따라 추가 드라이브 또는 드라이브를 구성할 수 있습니다. 예를 들어 TSM 서버가 테이프 라이브러리에서 두 개의 입력이 있는 Fibre Channel 스위치에 연결되어 있는 경우 각 입력에 대해 드라이브를 정의할 수 있습니다.

4. 서버에서 정의한 드라이브까지의 경로를 정의합니다.

```
define path servername drivename srctype=server desttype=drive  
library=tapelibrary device=drive-dname
```

- *drive-dname* 드라이브의 장치 이름입니다
- *tapelibrary* 정의한 테이프 라이브러리 이름입니다

테이프 라이브러리에 대해 정의한 각 드라이브에 대해 별도의 를 사용하여 이 과정을 반복합니다 *drivename* 및 *drive-dname* 각 드라이브에 대해.

5. 드라이브의 디바이스 클래스를 정의합니다.

```
define devclass DeviceClassName devtype=lto library=tapelibrary  
format=tape
```

- *DeviceClassName* 디바이스 클래스의 이름입니다
- *lto* 서버에 연결된 드라이브 유형입니다
- *tapelibrary* 정의한 테이프 라이브러리 이름입니다
- *tape* 은 테이프 유형입니다(예: ul3um3)

6. 라이브러리의 인벤토리에 테이프 볼륨을 추가합니다.

```
checkin libvolume tapelibrary
```

*tapelibrary* 정의한 테이프 라이브러리 이름입니다.

7. 운영 테이프 스토리지 풀을 생성합니다.



```
define stgpool SGWSTapePool DeviceClassName description=description
collocate=filesystem maxxscratch=XX
```

- *SGWSTapePool* 아카이브 노드의 테이프 스토리지 풀의 이름입니다. 이름이 TSM 서버에서 예상하는 구문 규칙을 사용하는 경우 테이프 스토리지 풀의 이름을 선택할 수 있습니다.
- *DeviceClassName* 테이프 라이브러리의 디바이스 클래스 이름입니다.
- *description* 은 를 사용하여 TSM 서버에 표시할 수 있는 스토리지 풀에 대한 설명입니다 query stgpool 명령. 예: ""아카이브 노드의 테이프 스토리지 풀""
- *collocate=filesystem* TSM 서버가 동일한 파일 공간의 객체를 단일 테이프에 기록하도록 지정합니다.
- xx 다음 중 하나입니다.
  - 테이프 라이브러리의 빈 테이프 수(라이브러리를 사용하는 유일한 애플리케이션인 경우)
  - StorageGRID 시스템에서 사용하도록 할당된 테이프 수(테이프 라이브러리가 공유되는 경우)

## 8. TSM 서버에서 디스크 스토리지 풀을 생성합니다. TSM 서버의 관리 콘솔에서 를 입력합니다

```
define stgpool SGWSDiskPool disk description=description
maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
lowmig=percent_low
```

- *SGWSDiskPool* 아카이브 노드의 디스크 풀의 이름입니다. 이름이 TSM에서 예상하는 구문 규칙을 사용하는 경우 디스크 스토리지 풀의 이름을 선택할 수 있습니다.
- *description* 은 를 사용하여 TSM 서버에 표시할 수 있는 스토리지 풀에 대한 설명입니다 query stgpool 명령. 예: "아카이브 노드의 경우 디스크 스토리지 풀"
- *maximum\_file\_size* 디스크 풀에 캐시되지 않고 이 크기보다 큰 오브젝트를 테이프에 직접 기록합니다. 를 설정하는 것이 좋습니다 *maximum\_file\_size* 10GB로 설정합니다.
- *nextstgpool=SGWSTapePool* 디스크 스토리지 풀을 아카이브 노드에 대해 정의된 테이프 스토리지 풀로 나타냅니다.
- *percent\_high* 디스크 풀의 내용을 테이프 풀로 마이그레이션하기 시작하는 값을 설정합니다. 를 설정하는 것이 좋습니다 *percent\_high* 0으로 지정하면 데이터 마이그레이션이 즉시 시작됩니다
- *percent\_low* 테이프 풀로의 마이그레이션이 중지되는 값을 설정합니다. 를 설정하는 것이 좋습니다 *percent\_low* 를 0으로 눌러 디스크 풀을 지웁니다.

## 9. TSM 서버에서 디스크 볼륨(또는 볼륨)을 생성하여 디스크 풀에 할당합니다.

```
define volume SGWSDiskPool volume_name formsize=size
```

- *SGWSDiskPool* 디스크 풀 이름입니다.
- *volume\_name* 볼륨 위치에 대한 전체 경로입니다(예: /var/local/arc/stage6.dsm) TSM 서버에서 테이프 전송을 준비하기 위해 디스크 풀의 내용을 기록합니다.
- *size* 디스크 볼륨의 크기(MB)입니다.

예를 들어, 디스크 풀의 콘텐츠가 단일 테이프를 채우도록 단일 디스크 볼륨을 생성하려면 테이프 볼륨의 용량이 200GB인 경우 크기 값을 200000으로 설정합니다.

그러나 TSM 서버가 디스크 풀의 각 볼륨에 쓸 수 있으므로 더 작은 크기의 여러 디스크 볼륨을 생성하는 것이 좋습니다. 예를 들어 테이프 크기가 250GB인 경우 각각 10GB(10000)의 크기로 25개의 디스크 볼륨을

생성합니다.

TSM 서버는 디스크 볼륨의 디렉토리에 공간을 사전 할당합니다. 완료하는 데 시간이 걸릴 수 있습니다(200GB 디스크 볼륨의 경우 3시간 이상).

## 도메인 정책 정의 및 노드 등록

아카이브 노드에서 저장된 데이터에 대해 TSM 관리 클래스를 사용하는 도메인 정책을 정의한 다음 이 도메인 정책을 사용하도록 노드를 등록해야 합니다.



TSM(Tivoli Storage Manager)의 아카이브 노드에 대한 클라이언트 암호가 만료되면 아카이브 노드 프로세스에서 메모리가 누수될 수 있습니다. 아카이브 노드의 클라이언트 사용자 이름/암호가 만료되지 않도록 TSM 서버가 구성되어 있는지 확인합니다.

아카이브 노드를 사용하거나 기존 노드를 업데이트하기 위해 TSM 서버에 노드를 등록할 때 MAXNUMMP 매개 변수를 REGISTER NODE 명령에 지정하여 쓰기 작업에 사용할 수 있는 마운트 지점의 수를 지정해야 합니다. 마운트 지점의 수는 일반적으로 아카이브 노드에 할당된 테이프 드라이브 헤드의 수와 같습니다. TSM 서버의 MAXNUMMP에 지정된 숫자는 최소한 \* ARC \* > \* Target \* > \* Configuration \* > \* Main \* > \* Maximum Store Sessions \* 에 설정된 값보다 큰 값이어야 합니다. 동시 저장소 세션은 아카이브 노드에서 지원되지 않으므로 0 또는 1 값으로 설정됩니다.

TSM 서버에 대해 설정된 MAXSESSIONS 값은 모든 클라이언트 애플리케이션이 TSM 서버에 열 수 있는 최대 세션 수를 제어합니다. TSM에 지정된 MAXSESSIONS 값은 아카이브 노드의 Grid Manager에서 \* ARC \* > \* Target \* > \* Configuration \* > \* Main \* > \* Number of Sessions \* 에 지정된 값보다 크거나 같아야 합니다. 아카이브 노드는 마운트 지점당 최대 하나의 세션과 작은 수의(<5) 추가 세션을 동시에 생성합니다.

아카이브 노드에 할당된 TSM 노드는 사용자 지정 도메인 정책을 사용합니다 tsm-domain. 를 클릭합니다 tsm-domain 도메인 정책은 테이프에 기록하고 아카이브 대상이 StorageGRID 시스템의 스토리지 풀로 설정된 "표준" 도메인 정책의 수정된 버전입니다 (SGWSDiskPool)를 클릭합니다.



관리자 권한으로 TSM 서버에 로그인하고 dsmadm 도구 사용하여 도메인 정책을 생성하고 활성화해야 합니다.

## 도메인 정책 생성 및 활성화

아카이브 노드에서 전송된 데이터를 저장하도록 TSM 서버를 구성하려면 도메인 정책을 생성한 다음 활성화해야 합니다.

### 단계

1. 도메인 정책을 생성합니다.

```
copy domain standard tsm-domain
```

2. 기존 관리 클래스를 사용하지 않는 경우 다음 중 하나를 입력합니다.

```
define policyset tsm-domain standard
```

```
define mgmtclass tsm-domain standard default
```

*default* 는 배포의 기본 관리 클래스입니다.

3. 적절한 스토리지 풀에 카피그룹을 생성합니다. 입력(한 줄에):

```
define copygroup tsm-domain standard default type=archive
destination=SGWSDiskPool retinit=event retmin=0 retver=0
```

*default* 아카이브 노드의 기본 관리 클래스입니다. 의 값 *retinit*, *retmin*, 및 *retver* 아카이브 노드에서 현재 사용하는 보존 동작을 반영하도록 선택되었습니다



설정하지 마십시오 *retinit* 를 선택합니다 *retinit=create*. 설정 *retinit=create* TSM 서버에서 콘텐츠를 제거하는 데 보존 이벤트가 사용되므로 아카이브 노드가 콘텐츠를 삭제하지 못하도록 차단합니다.

4. 관리 클래스를 기본값으로 할당합니다.

```
assign defmgmtclass tsm-domain standard default
```

5. 새 정책 세트를 활성으로 설정합니다.

```
activate policyset tsm-domain standard
```

*activate* 명령을 입력할 때 나타나는 ""백업 복사 그룹 없음"" 경고는 무시하십시오.

6. TSM 서버에 설정된 새 정책을 사용하려면 노드를 등록합니다. TSM 서버에서 (한 줄에) 다음을 입력합니다.

```
register node arc-user arc-password passexp=0 domain=tsm-domain
MAXNUMMP=number-of-sessions
```

*arc-user* 및 *arc-password*는 Archive Node에서 정의한 클라이언트 노드 이름 및 암호와 동일하며, *MAXNUMMP* 값은 Archive Node store 세션에 예약된 테이프 드라이브 수로 설정됩니다.



기본적으로 노드를 등록하면 노드에 대해 정의된 암호를 사용하여 클라이언트 소유자 권한에 관리 사용자 ID가 생성됩니다.

## StorageGRID로 데이터 마이그레이션

대량의 데이터를 StorageGRID 시스템으로 마이그레이션하는 동시에 일상적인 작업을 위해 StorageGRID 시스템을 사용할 수 있습니다.

다음 섹션에서는 대량의 데이터를 StorageGRID 시스템으로 마이그레이션하는 방법을 이해하고 계획하는 방법을 안내합니다. 이 가이드는 데이터 마이그레이션의 일반적인 가이드가 아니며 마이그레이션을 수행하기 위한 자세한 단계는 포함되어 있지 않습니다. 이 섹션의 지침과 지침을 따라 일상적인 작업을 방해하지 않으면서 데이터가 StorageGRID 시스템으로 효율적으로 마이그레이션되고 마이그레이션된 데이터가 StorageGRID 시스템에서 적절하게 처리되도록 하십시오.

- "StorageGRID 시스템의 용량 확인"
- "마이그레이션된 데이터에 대한 ILM 정책 결정"
- "마이그레이션이 운영에 미치는 영향"
- "데이터 마이그레이션 예약"

- ["데이터 마이그레이션 모니터링"](#)
- ["마이그레이션 알람에 대한 사용자 지정 알림을 생성합니다"](#)

## StorageGRID 시스템의 용량 확인

대량의 데이터를 StorageGRID 시스템으로 마이그레이션하기 전에 StorageGRID 시스템에 예상되는 볼륨을 처리할 수 있는 디스크 용량이 있는지 확인하십시오.

StorageGRID 시스템에 아카이브 노드가 포함되어 있고 마이그레이션된 객체의 복제본이 니어라인 스토리지(예: 테이프)에 저장된 경우 아카이브 노드의 스토리지가 마이그레이션된 데이터의 예상 볼륨에 충분한 용량을 가지고 있는지 확인하십시오.

용량 평가의 일환으로 마이그레이션할 객체의 데이터 프로파일을 살펴보고 필요한 디스크 용량을 계산합니다. StorageGRID 시스템의 디스크 용량을 모니터링하는 방법에 대한 자세한 내용은 StorageGRID 모니터링 및 문제 해결 지침을 참조하십시오.

관련 정보

["모니터링 및 문제 해결"](#)

["스토리지 노드 관리"](#)

## 마이그레이션된 데이터에 대한 ILM 정책 결정

StorageGRID 시스템의 ILM 정책은 복사본 수, 복사본이 저장되는 위치 및 복사본 보유 기간을 결정합니다. ILM 정책은 시간 경과에 따라 개체를 필터링하고 개체 데이터를 관리하는 방법을 설명하는 ILM 규칙 집합으로 구성되어 있습니다.

마이그레이션된 데이터의 사용 방법과 마이그레이션된 데이터의 요구 사항에 따라 일상적인 작업에 사용되는 ILM 규칙과 다른 마이그레이션 데이터에 대한 고유한 ILM 규칙을 정의할 수 있습니다. 예를 들어, 마이그레이션에 포함된 데이터에 대한 규정 요구사항과 일상적인 데이터 관리에 대한 규정 요구사항이 서로 다른 경우 다른 등급의 스토리지에 마이그레이션된 데이터의 복사본을 여러 개 만들어야 할 수 있습니다.

마이그레이션된 데이터와 일상적인 작업과 저장된 오브젝트 데이터를 고유하게 구분할 수 있는 경우 마이그레이션된 데이터에만 적용되는 규칙을 구성할 수 있습니다.

메타데이터 기준 중 하나를 사용하여 데이터 유형을 안정적으로 구분할 수 있는 경우, 이 기준을 사용하여 마이그레이션된 데이터에만 적용되는 ILM 규칙을 정의할 수 있습니다.

데이터 마이그레이션을 시작하기 전에 StorageGRID 시스템의 ILM 정책과 마이그레이션 데이터에 적용되는 방법을 이해하고 ILM 정책에 대한 모든 변경 사항을 적용 및 테스트해야 합니다.



잘못 지정된 ILM 정책으로 인해 복구할 수 없는 데이터 손실이 발생할 수 있습니다. ILM 정책을 활성화하기 전에 변경한 모든 내용을 주의 깊게 검토하여 정책이 의도한 대로 작동하는지 확인합니다.

관련 정보

["ILM을 사용하여 개체를 관리합니다"](#)

## 마이그레이션이 운영에 미치는 영향

StorageGRID 시스템은 오브젝트 스토리지 및 검색을 위한 효율적인 작업을 제공하고 오브젝트 데이터 및 메타데이터의 중복 복사본을 지속적으로 생성하여 데이터 손실로부터 데이터를 완벽하게 보호하도록 설계되었습니다.

그러나 일상적인 시스템 운영에 영향을 주지 않도록 이 장의 지침에 따라 데이터 마이그레이션을 주의 깊게 관리해야 합니다. 그렇지 않을 경우, 극단적인 경우 StorageGRID 시스템에 장애가 발생할 경우 데이터가 손실될 위험이 있습니다.

대량의 데이터를 마이그레이션하면 시스템에 추가 부하가 걸린 것입니다. StorageGRID 시스템이 로드가 많은 경우 객체를 저장하고 검색하는 요청에 더 느리게 응답합니다. 이로 인해 일상적인 작업에 필수적인 저장 및 검색 요청이 방해받을 수 있습니다. 마이그레이션으로 인해 다른 운영 문제가 발생할 수도 있습니다. 예를 들어, 스토리지 노드의 용량이 거의 다 되면 배치 수집으로 인한 과중한 간헐적 로드로 인해 스토리지 노드가 읽기 전용과 읽기-쓰기 간에 순환되어 알림을 생성할 수 있습니다.

로드가 많은 경우 큐는 StorageGRID 시스템에서 수행하는 다양한 작업에 대해 개발되어 오브젝트 데이터 및 메타데이터의 완전한 이중화를 보장할 수 있습니다.

마이그레이션 중에 StorageGRID 시스템을 안전하고 효율적으로 운영할 수 있도록 이 문서의 지침에 따라 데이터 마이그레이션을 신중하게 관리해야 합니다. 데이터를 마이그레이션할 때는 오브젝트를 일괄적으로 수집하거나 지속적으로 스로틀로 인제스트합니다. 그런 다음 StorageGRID 시스템을 지속적으로 모니터링하여 다양한 속성 값을 초과하지 않는지 확인합니다.

## 데이터 마이그레이션 예약

핵심 운영 시간 중에는 데이터 마이그레이션을 하지 마십시오. 시스템 사용량이 적은 야간, 주말 및 기타 시간으로 데이터 마이그레이션을 제한합니다.

가능한 경우 활동이 많은 기간 동안에는 데이터 마이그레이션을 예약하지 마십시오. 그러나 높은 활동 기간을 완전히 피하는 것이 실용적이지 않은 경우에는 관련 특성을 면밀히 모니터링하고 허용 가능한 값을 초과하는 경우 조치를 취하는 한 계속 진행하는 것이 안전합니다.

### 관련 정보

["데이터 마이그레이션 모니터링"](#)

## 데이터 마이그레이션 모니터링

필요한 기간 내에 ILM 정책에 따라 데이터를 배치할 수 있도록 데이터 마이그레이션을 모니터링하고 조정해야 합니다.

이 표에는 데이터 마이그레이션 중에 모니터링해야 하는 속성과 이러한 특성이 나타내는 문제가 나열되어 있습니다.

트래픽 분류 정책을 사용하여 수집 임계치를 조절할 경우, 다음 표에 설명된 통계와 함께 관찰된 비율을 모니터링하고 필요한 경우 제한을 줄일 수 있습니다.

모니터링	설명
ILM 평가를 기다리는 개체의 수입니다	<ol style="list-style-type: none"> <li>1. 지원 * &gt; * 도구 * &gt; * 그리드 토폴로지 * 를 선택합니다.</li> <li>2. 배포 _ ** 개요 ** 주 * 를 선택합니다.</li> <li>3. ILM 활동 섹션에서 다음 특성에 대해 표시된 개체 수를 모니터링합니다. <ul style="list-style-type: none"> <li>◦ * Awaiting-all(XQUZ) *: ILM 평가를 기다리는 총 개체 수.</li> <li>◦ * Awaiting-Client(XCQZ) *: 클라이언트 작업에서 ILM 평가를 기다리는 총 오브젝트 수(예: 수집).</li> </ul> </li> <li>4. 이러한 속성 중 하나에 대해 표시되는 오브젝트 수가 100,000개를 초과할 경우 개체의 수집 속도를 조절하여 StorageGRID 시스템의 로드를 줄입니다.</li> </ol>
타겟 아카이브 시스템의 스토리지 용량	ILM 정책이 마이그레이션된 데이터의 복사본을 대상 아카이브 스토리지 시스템(테이프 또는 클라우드)에 저장하는 경우 대상 아카이브 스토리지 시스템의 용량을 모니터링하여 마이그레이션된 데이터에 충분한 용량이 있는지 확인하십시오.
• 보관 노드 ** ARC ** 저장 *	ARVF(Store Failures) * 속성에 대한 알람이 트리거되면 대상 아카이브 스토리지 시스템의 용량이 한계에 도달했을 수 있습니다. 대상이 되는 아카이브 스토리지 시스템을 확인하고 알람을 트리거한 문제를 모두 해결합니다.

## 마이그레이션 알람에 대한 사용자 지정 알람을 생성합니다

특정 값이 권장 임계값을 초과할 경우 마이그레이션을 모니터링하는 시스템 관리자에게 StorageGRID에서 알림 또는 알람(레거시 시스템) 알람을 보낼 수 있습니다.

### 필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 경고(또는 알람) 알람에 대한 이메일 설정을 구성해야 합니다.

### 단계

1. 데이터 마이그레이션 중에 모니터링하려는 각 Prometheus 메트릭 또는 StorageGRID 속성에 대해 사용자 지정 알람 규칙 또는 글로벌 사용자 지정 알람을 생성합니다.

알림은 Prometheus 메트릭 값을 기준으로 트리거됩니다. 알람은 특성 값에 따라 트리거됩니다. 자세한 내용은 StorageGRID 모니터링 및 문제 해결 지침을 참조하십시오.

2. 데이터 마이그레이션이 완료된 후 사용자 지정 알람 규칙 또는 글로벌 사용자 지정 알람을 비활성화합니다.

전역 사용자 정의 알람은 기본 알람보다 우선합니다.

### 관련 정보

["모니터링 및 문제 해결"](#)

## 저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 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 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 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 라이선스는 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.