StorageGRID 시스템 관리

StorageGRID

NetApp
October 03, 2025

목차

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
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.

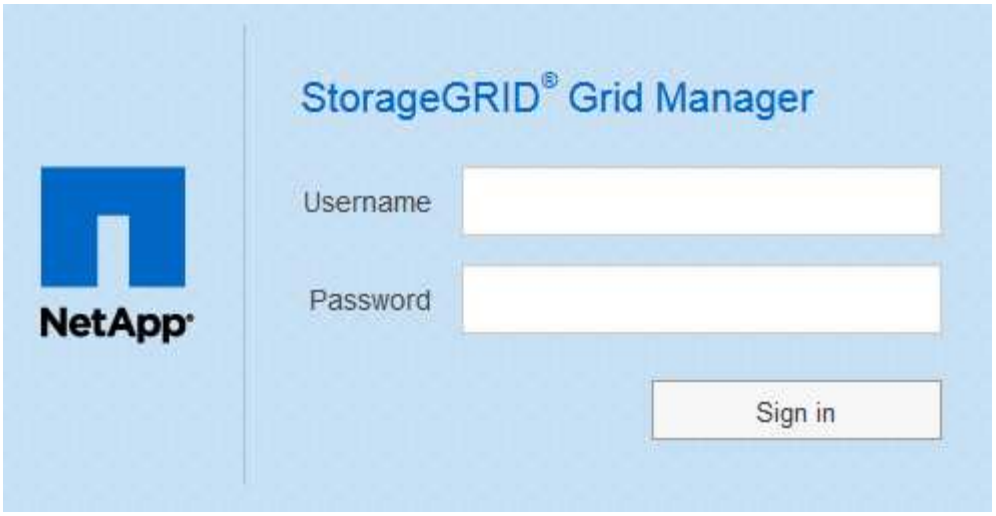
   `https://FQDN_or_Admin_Node_IP/`

   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/`

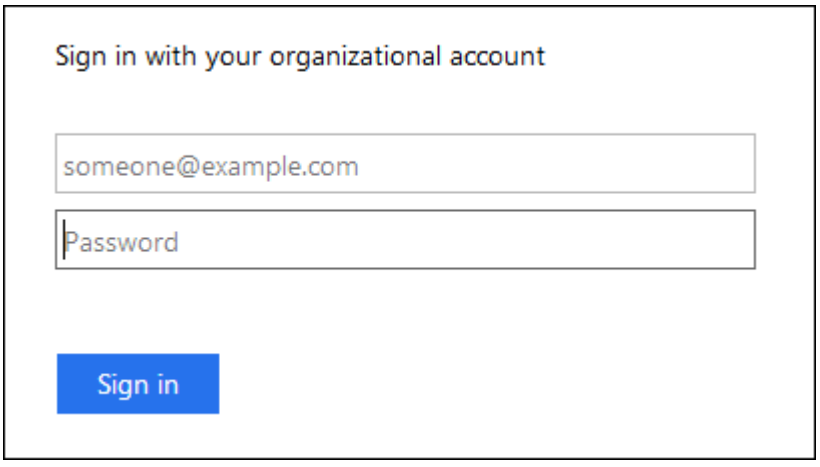
3. 보안 경고 메시지가 나타나면 브라우저의 설치 마법사를 사용하여 인증서를 설치합니다.
4. Grid Manager에 로그인:
   - SSO(Single Sign-On)를 StorageGRID 시스템에 사용하지 않는 경우:
     i. Grid Manager의 사용자 이름과 암호를 입력합니다.
     ii. 로그인 * 을 클릭합니다.



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

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

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

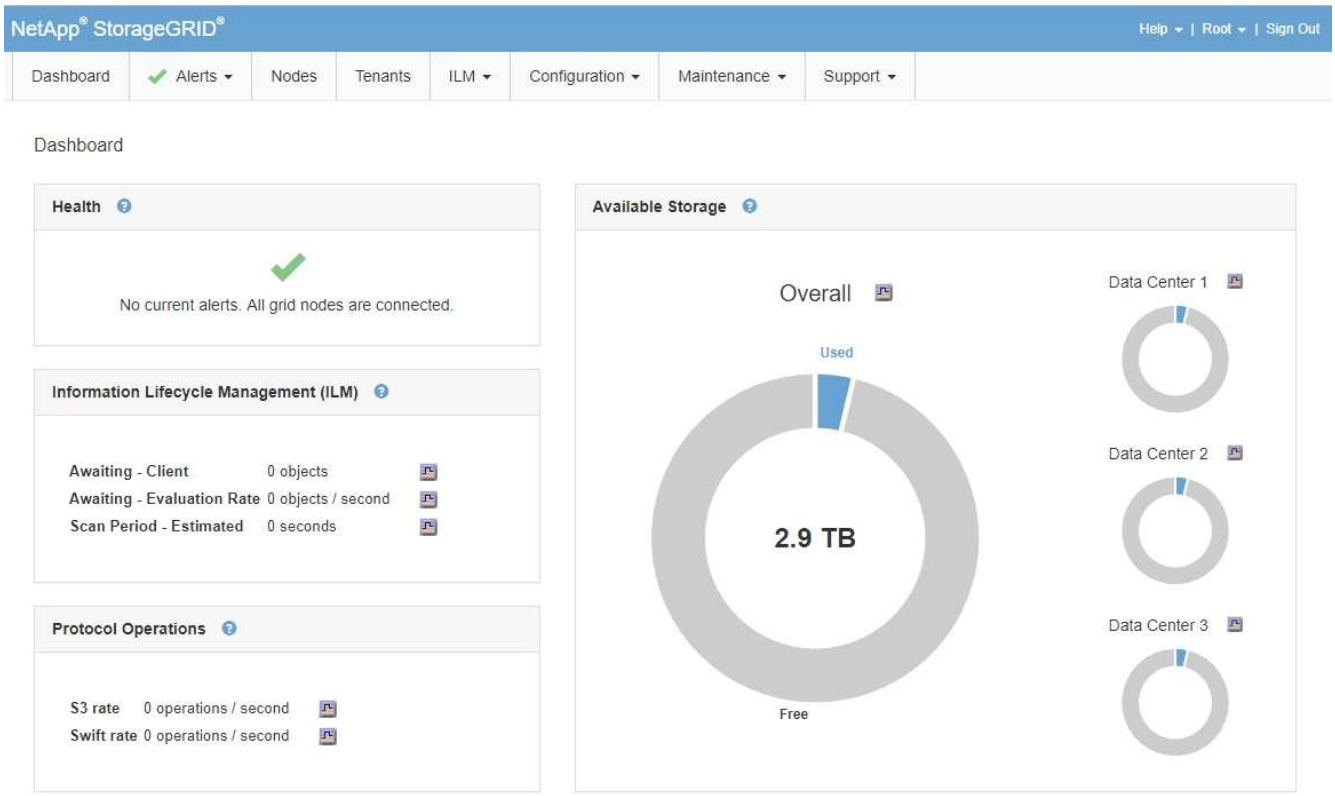


◦ StorageGRID 시스템에 대해 SSO가 활성화되어 있고 이전에 그리드 관리자 또는 테넌트 계정에 액세스한 경우:

i. 다음 중 하나를 수행합니다.

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

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.



5. 다른 관리자 노드에 로그인하려면:

옵션을 선택합니다	단계
SSO가 활성화되지 않았습니다	a. 브라우저의 주소 표시줄에 다른 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력합니다. 필요에 따라 포트 번호를 포함시킵니다. b. Grid Manager의 사용자 이름과 암호를 입력합니다. c. 로그인 * 을 클릭합니다.
SSO가 활성화되었습니다	브라우저의 주소 표시줄에 다른 관리 노드의 정규화된 도메인 이름 또는 IP 주소를 입력합니다. 한 관리 노드에 로그인한 경우 다시 로그인하지 않고도 다른 관리 노드에 액세스할 수 있습니다. 그러나 SSO 세션이 만료되면 자격 증명을 다시 입력하라는 메시지가 표시됩니다. • 참고: * SSO는 제한된 Grid Manager 포트에서 사용할 수 없습니다. 사용자가 SSO(Single Sign-On)로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다.

관련 정보

"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"

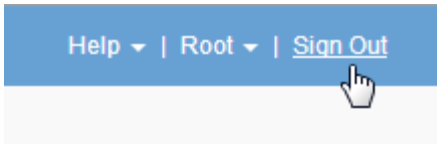
"모니터링 및 문제 해결"

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. • 참고: * 둘 이상의 관리자 노드에 로그인한 경우 각 노드에서 로그아웃해야 합니다.
SSO가 활성화되었습니다	액세스 중인 모든 관리 노드에서 로그아웃되었습니다. StorageGRID 로그인 페이지가 표시됩니다. * 그리드 관리자 * 는 * 최근 계정 * 드롭다운에 기본값으로 나열되고 * 계정 ID * 필드는 0으로 표시됩니다. • 참고: * SSO가 활성화되어 있고 테넌트 관리자에도 로그인한 경우, SSO에서 로그아웃하려면 테넌트 계정에서도 로그아웃해야 합니다.

관련 정보

"Single Sign-On 구성"

"테넌트 계정을 사용합니다"

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

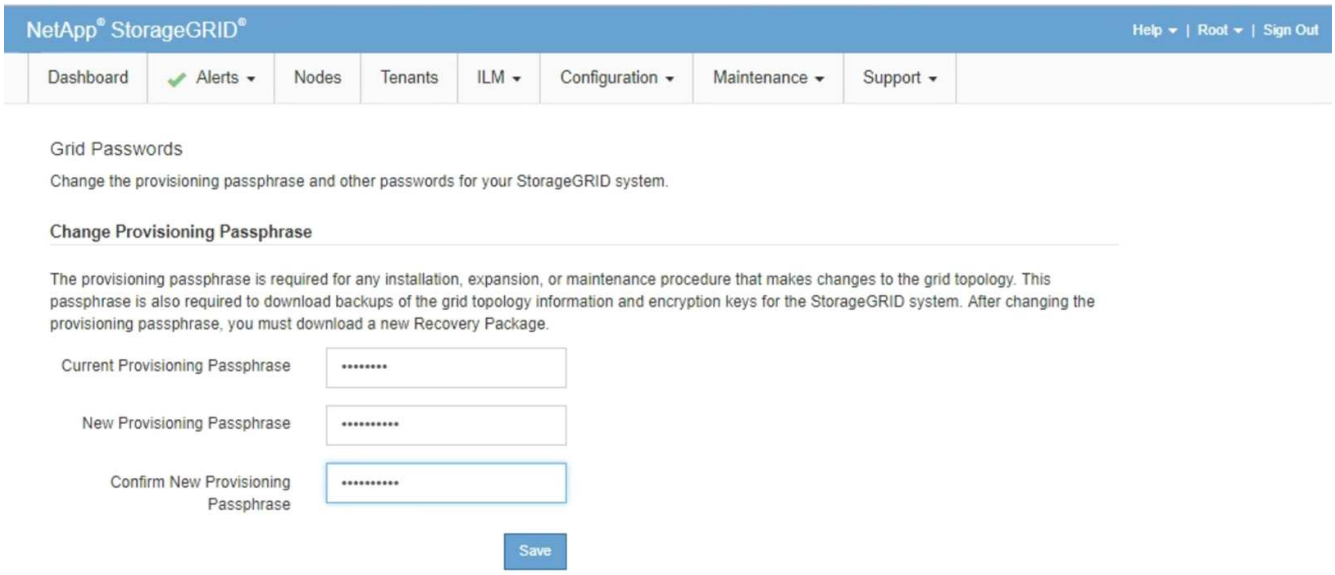
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 유지 관리 또는 루트 액세스 권한이 있어야 합니다.
- 현재 프로비저닝 암호가 있어야 합니다.

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.

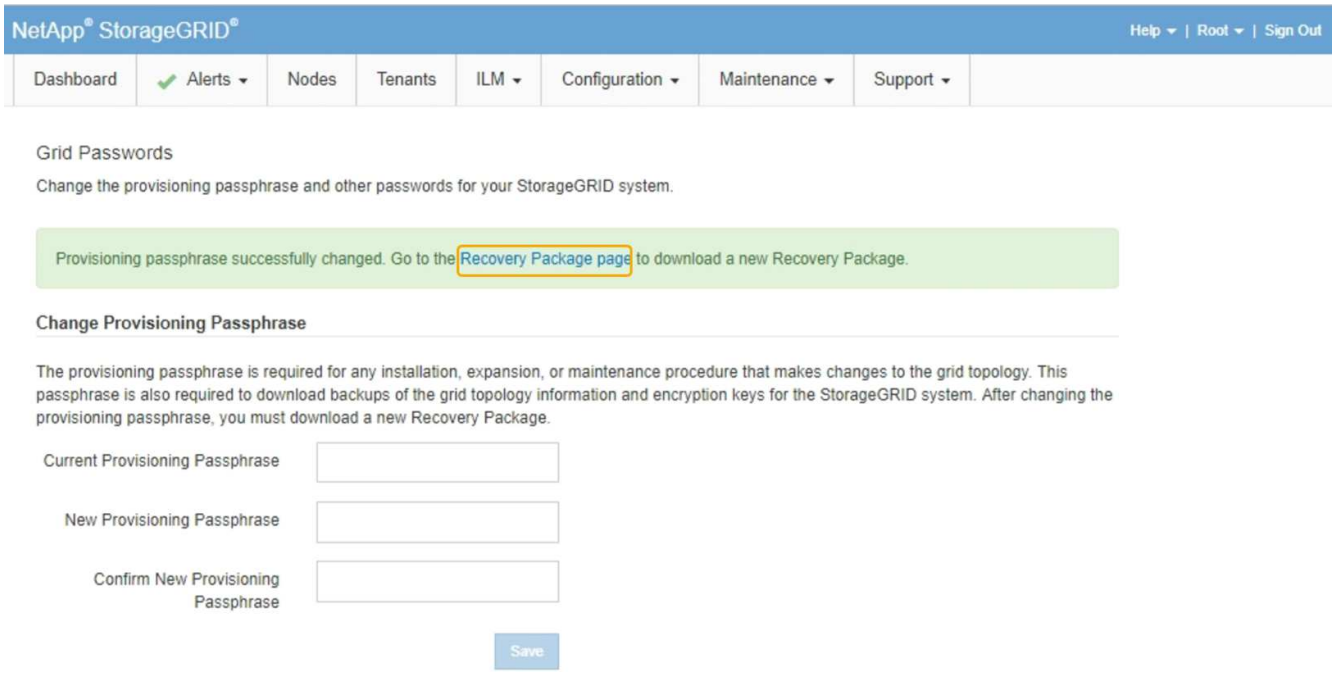


2. 현재 프로비저닝 암호를 입력합니다.
3. 새 passWindows를 입력하십시오. 암호는 8자 이상이어야 하며 32자 이하여야 합니다. 암호는 대/소문자를 구분합니다.

> 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.



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.

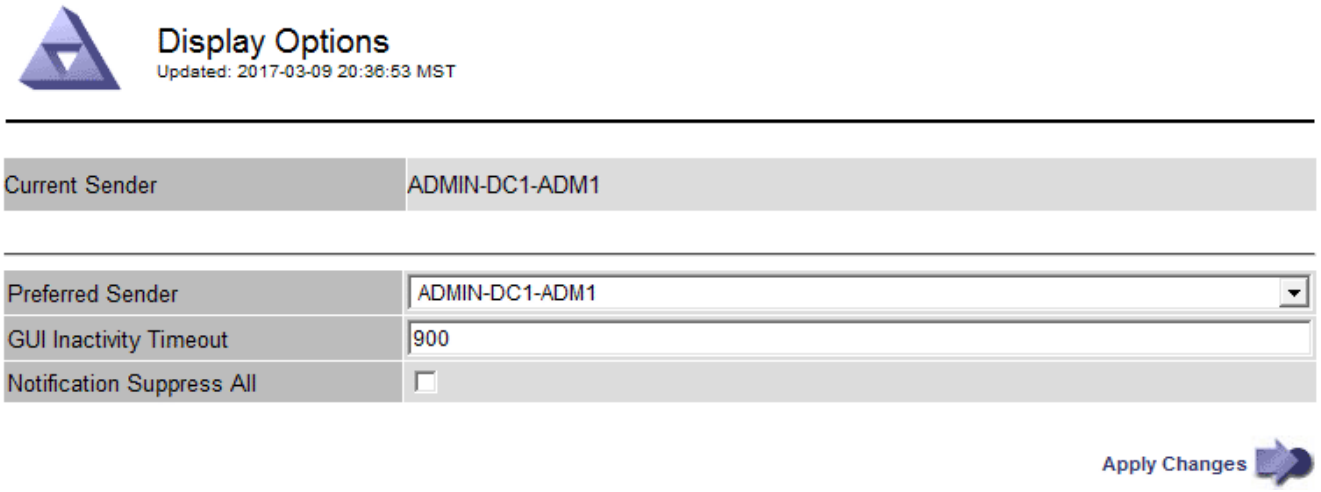
사용자 세션 시간 초과는 다음을 통해서도 제어할 수 있습니다.

- 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.



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 라이센스 정보 보기

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

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

이 작업에 대해

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

단계

라이센스를 보려면 다음 중 하나를 수행합니다.

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

라이센스 페이지가 나타나고 현재 라이센스에 대한 다음과 같은 읽기 전용 정보가 제공됩니다.

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

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

StorageGRID 라이센스 정보를 업데이트하는 중입니다

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

필요한 것

- StorageGRID 시스템에 적용하려면 새 라이센스 파일이 있어야 합니다.
- 특정 액세스 권한이 있어야 합니다.

- 프로비저닝 암호가 있어야 합니다.

단계

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

   새 라이센스 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 엔터티를 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 경보(레거시 시스템)를 나열하고, 현재 경고와 노드 연결 상태 요약을 포함하여 그리드의 상태에 대한 정보를 반환하는 작업.

- * alert-history * — 해결된 경고에 대한 작업.
- 알림 메시지 수신자 * — 경고 알림 수신자(이메일)에 대한 작업.
- * alert-rules * — 경고 규칙에 대한 작업.
- * alert-silences * — 경고 작동 중.
- * 경고 * — 경고 작업.
- * 감사 * — 감사 구성을 나열하고 업데이트하는 작업.
- * auth * — 사용자 세션 인증을 수행하기 위한 작업.

  Grid Management API는 Bearer Token Authentication Scheme을 지원한다. 로그인하려면 인증 요청의 JSON 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 라이센스를 검색하고 업데이트하는 작업.
- * 로그 * — 로그 파일을 수집하고 다운로드하기 위한 작업.
- * 메트릭 * — 일정 기간 동안 단일 시점 및 범위 메트릭 쿼리에 대한 즉석 메트릭 쿼리를 비롯한 StorageGRID 메트릭의 운영 Grid Management API는 Prometheus 시스템 모니터링 도구를 백엔드 데이터 소스로 사용합니다. Prometheus 쿼리 구성에 대한 자세한 내용은 Prometheus 웹 사이트를 참조하십시오.

다음을 포함한 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.

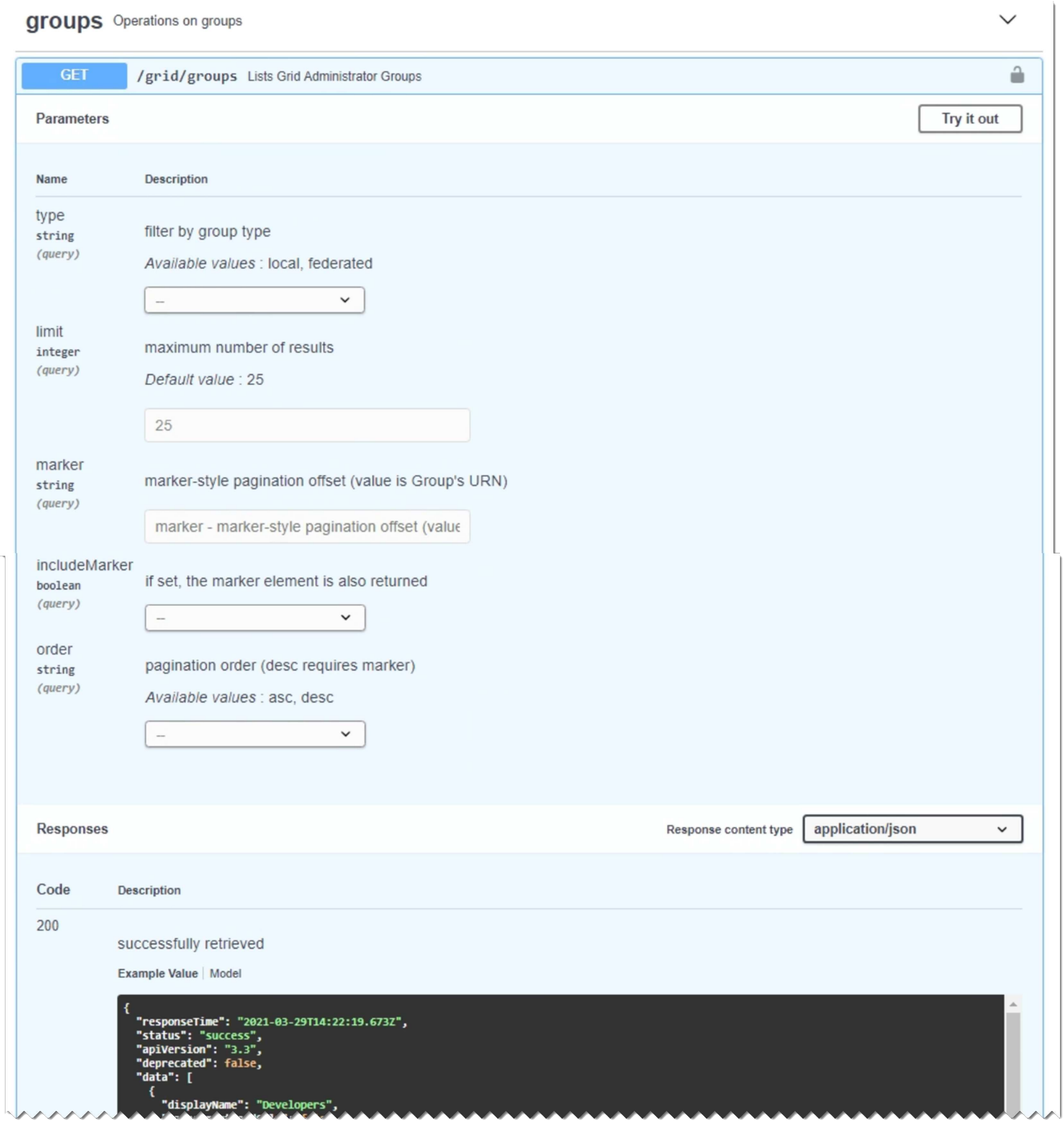
API Docs 웹 페이지를 사용하여 수행하는 모든 API 작업은 라이브 작업입니다. 실수로 구성 데이터나 기타 데이터를 작성, 업데이트 또는 삭제하지 않도록 주의하십시오.

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.



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 API를 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 API에 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

   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-m json.tool에 전달되어 JSON 인코딩을 제거합니다.

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

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

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%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...sSl%2BfQ33cvfwA%3D'
```

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

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

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

응답에는 클라이언트 요청 ID:

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

e. 응답에서 클라이언트 요청 ID를 저장합니다.

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

f. 이전 응답에서 양식 작업으로 자격 증명을 보냅니다.

```
curl -X POST
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --data
"UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMLPASSWORD&AuthMethod=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=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. 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
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. 를 저장합니다 `SAMLResponse` 숨겨진 필드에서:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...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://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. 로그아웃 URL을 저장합니다.

```
export
LOGOUT_REQUEST='https://adfs.example.com/adfs/ls/?SAMLRequest=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: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. StorageGRID bearer token을 삭제한다.

StorageGRID 베어러 토큰을 삭제하는 것은 SSO를 사용하지 않는 것과 동일한 방식으로 작동합니다. 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	각 클라이언트에 설치되어 StorageGRID에서 외부 클라이언트 액세스를 인증할 수 있습니다. • 권한이 있는 외부 클라이언트가 StorageGRID Prometheus 데이터베이스에 액세스할 수 있습니다. • 외부 도구를 사용하여 StorageGRID를 안전하게 모니터링할 수 있습니다.	• 구성 * > * 액세스 제어 * > * 클라이언트 인증서 *	"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.	• 구성 * > * 액세스 제어 * > * ID 페더레이션 *	"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.	• 구성 * > * 액세스 제어 * > * 단일 사인온 *	"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.	• 구성 * > * 시스템 설정 * > * 키 관리 서버 *	"KMS(키 관리 서버) 추가"

인증서	인증서 유형입니다	설명	내비게이션 위치	세부 정보
이메일 경고 알림 인증서입니다	서버 및 클라이언트	SMTP 이메일 서버와 알림 알림에 사용되는 StorageGRID 간의 연결을 인증합니다. • SMTP 서버와의 통신에 TLS(Transport Layer Security)가 필요한 경우 전자 메일 서버 CA 인증서를 지정해야 합니다. • SMTP 전자 메일 서버에 인증을 위해 클라이언트 인증서가 필요한 경우에만 클라이언트 인증서를 지정합니다.	• 경고 * > * 이메일 설정 *	"모니터링 및 문제 해결"
로드 밸런서 끝점 인증서	서버	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. • 참고: * 로드 밸런서 인증서는 일반적인 StorageGRID 작업 중에 가장 많이 사용되는 인증서입니다.	• 구성 * > * 네트워크 설정 * > * 로드 밸런서 엔드포인트 *	• "부하 분산 장치 엔드포인트 구성" • FabricPool용 로드 밸런서 끝점 생성 "FabricPool용 StorageGRID를 구성합니다"

인증서	인증서 유형입니다	설명	내비게이션 위치	세부 정보
관리 인터페이스 서버 인증서	서버	클라이언트 웹 브라우저와 StorageGRID 관리 인터페이스 간의 연결을 인증하여 사용자가 보안 경고 없이 그리드 관리자 및 테넌트 관리자에 액세스할 수 있도록 합니다. 또한 이 인증서는 Grid Management API 및 테넌트 관리 API 연결을 인증합니다. 내부 CA 인증서를 사용하거나 사용자 지정 인증서를 업로드할 수 있습니다.	• 구성 * > * 네트워크 설정 * > * 서버 인증서 *	• "서버 인증서를 구성하는 중입니다" • "Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성"
Cloud Storage Pool 엔드포인트 인증서입니다	서버	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.	• ILM * > * 스토리지 풀 *	"ILM을 사용하여 개체를 관리합니다"
플랫폼 서비스 끝점 인증서	서버	StorageGRID 플랫폼 서비스에서 S3 스토리지 리소스에 대한 연결을 인증합니다.	• 테넌트 관리자 * > * 스토리지(S3) * > * 플랫폼 서비스 엔드포인트 *	"테넌트 계정을 사용합니다"
객체 스토리지 API 서비스 엔드포인트 서버 인증서입니다	서버	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.	• 구성 * > * 네트워크 설정 * > * 로드 밸런서 엔드포인트 *	"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.