



StorageGRID의 시스템 강화

StorageGRID software

NetApp
July 23, 2026

목차

StorageGRID의 시스템 강화	1
StorageGRID의 시스템 강화에 대해 알아보십시오	1
StorageGRID 소프트웨어 업그레이드를 위한 보안 강화 지침	1
StorageGRID 소프트웨어 업그레이드	1
외부 서비스 업그레이드	2
하이퍼바이저 업그레이드	2
Linux 노드 업그레이드	2
StorageGRID 네트워크 보안 강화 지침	2
그리드 네트워크 지침	2
관리자 네트워크 지침	3
클라이언트 네트워크 지침	3
StorageGRID 노드 보안 강화 지침	3
BMC에 대한 원격 IPMI 액세스 제어	3
방화벽 구성	3
사용하지 않는 서비스 비활성화	4
가상화, 컨테이너 및 공유 하드웨어	4
설치 중 노드 보호	4
하드웨어에 대한 물리적 액세스 제한	4
관리자 노드에 대한 지침	4
스토리지 노드에 대한 지침	5
게이트웨이 노드에 대한 지침	5
하드웨어 어플라이언스 노드에 대한 지침	6
StorageGRID의 TLS 및 SSH 강화 지침	7
인증서 강화 지침	7
TLS 및 SSH 정책 강화 지침	7
외부 SSH 액세스 관리	8
StorageGRID의 로그, 암호 및 감사 메시지에 대한 강화 지침	8
임시 설치 비밀번호	8
로그 및 감사 메시지	8
NetApp AutoSupport	8
CORS(Cross-Origin Resource Sharing)	9
외부 보안 장치	9
랜섬웨어 완화	9

StorageGRID의 시스템 강화

StorageGRID의 시스템 강화에 대해 알아보십시오

시스템 강화는 StorageGRID 시스템에서 가능한 한 많은 보안 위험을 제거하는 프로세스입니다.

StorageGRID를 설치하고 구성할 때 다음 지침을 활용하여 기밀성, 무결성 및 가용성에 대한 규정된 보안 목표를 달성하십시오.

이미 업계 표준 시스템 강화 모범 사례를 활용하고 있어야 합니다. 예를 들어, StorageGRID에 강력한 암호를 사용하고, HTTP 대신 HTTPS를 사용하며, 가능한 경우 인증서 기반 인증을 활성화해야 합니다. 이러한 모범 사례에는 물리적 접근을 제한하고 물리적 데이터 센터 및 지원 인프라를 보호하는 물리적 및 환경적 보안이 포함되어야 합니다. 또한 비즈니스 및 지역에 적용되는 모든 규제 표준 및 권장 사항을 참조해야 합니다.

StorageGRID는 "NetApp 취약점 처리 정책"을 따릅니다. 보고된 취약점은 제품 보안 사고 대응 프로세스에 따라 검증 및 처리됩니다.

StorageGRID 시스템의 보안을 강화할 때는 다음 사항을 고려하십시오.

- 구현한 세 가지 **StorageGRID** 네트워크 중 어떤 네트워크를 사용하고 있습니까. 모든 StorageGRID 시스템은 그리드 네트워크를 사용해야 하지만, 관리자 네트워크, 클라이언트 네트워크 또는 둘 다를 사용할 수도 있습니다. 각 네트워크에는 서로 다른 보안 고려 사항이 있습니다.
- StorageGRID 시스템의 개별 노드에 사용하는 *플랫폼 유형*입니다. StorageGRID 노드는 VMware 가상 머신, Linux 호스트의 컨테이너 엔진 또는 전용 하드웨어 어플라이언스에 배포할 수 있습니다. 각 플랫폼 유형에는 고유한 보안 강화 모범 사례가 있습니다.
- 테넌트 계정의 신뢰도. 신뢰할 수 없는 테넌트 계정을 사용하는 서비스 제공업체는 신뢰할 수 있는 사내 테넌트만 사용하는 경우와는 다른 보안 문제를 안게 됩니다.
- 귀사에서 준수하는 보안 요구 사항 및 규칙은 무엇입니까? 특정 규제 또는 회사 요구 사항을 준수해야 할 수도 있습니다.

StorageGRID 소프트웨어 업그레이드를 위한 보안 강화 지침

공격으로부터 시스템을 보호하려면 StorageGRID 시스템과 관련 서비스를 항상 최신 상태로 유지해야 합니다.

StorageGRID 소프트웨어 업그레이드

가능하면 StorageGRID 소프트웨어를 최신 주요 릴리스 또는 이전 주요 릴리스로 업그레이드하십시오.

StorageGRID를 최신 상태로 유지하면 알려진 취약점이 활성화되는 시간을 줄이고 전체 공격 표면을 축소하는 데 도움이 됩니다. 또한 최신 StorageGRID 릴리스에는 이전 릴리스에 포함되지 않은 보안 강화 기능이 있는 경우가 많습니다.

<https://imt.netapp.com/matrix/#welcome>["NetApp 상호 운용성 매트릭스 도구"^](IMT)에 문의하여 사용해야 할 StorageGRID 소프트웨어 버전을 확인하십시오. 핫픽스가 필요한 경우 NetApp은 최신 릴리스용 업데이트를 우선적으로 제공합니다. 일부 패치는 이전 릴리스와 호환되지 않을 수 있습니다.

- 최신 StorageGRID 릴리스 및 핫픽스를 다운로드하려면 "[NetApp 다운로드: StorageGRID](#)"로 이동하십시오.
- StorageGRID 소프트웨어를 업그레이드하려면 "[업그레이드 지침](#)"을 참조하십시오.
- 핫픽스를 적용하려면 "[StorageGRID 핫픽스 절차](#)"을 참조하십시오.

외부 서비스 업그레이드

외부 서비스에는 StorageGRID에 간접적으로 영향을 미치는 취약점이 있을 수 있습니다. StorageGRID가 의존하는 서비스를 최신 상태로 유지해야 합니다. 이러한 서비스에는 LDAP, KMS(또는 KMIP 서버), DNS, NTP가 포함됩니다.

지원되는 버전 목록은 "[NetApp 상호 운용성 매트릭스 도구](#)"을 참조하세요.

하이퍼바이저 업그레이드

StorageGRID 노드가 VMware 또는 다른 하이퍼바이저에서 실행 중인 경우 하이퍼바이저 소프트웨어 및 펌웨어가 최신 버전인지 확인해야 합니다.

지원되는 버전 목록은 "[NetApp 상호 운용성 매트릭스 도구](#)"을 참조하세요.

Linux 노드 업그레이드

StorageGRID 노드가 Linux 호스트 플랫폼을 사용하는 경우 호스트 운영 체제에 보안 업데이트 및 커널 업데이트가 적용되었는지 확인해야 합니다. 또한 취약한 하드웨어에 대한 펌웨어 업데이트가 제공되면 해당 업데이트를 적용해야 합니다.

지원되는 버전 목록은 "[NetApp 상호 운용성 매트릭스 도구](#)"을 참조하세요.

StorageGRID 네트워크 보안 강화 지침

StorageGRID 시스템은 그리드 노드당 최대 3개의 네트워크 인터페이스를 지원하므로 보안 및 액세스 요구 사항에 맞게 각 그리드 노드의 네트워킹을 개별적으로 구성할 수 있습니다.

StorageGRID 네트워크에 대한 자세한 내용은 "[StorageGRID 네트워크 유형](#)"을 참조하십시오.

그리드 네트워크 지침

모든 내부 StorageGRID 트래픽을 위해 그리드 네트워크를 구성해야 합니다. 모든 그리드 노드는 그리드 네트워크에 있으며, 다른 모든 노드와 통신할 수 있어야 합니다.

그리드 네트워크를 구성할 때는 다음 지침을 따르십시오.

- 개방형 인터넷상의 클라이언트와 같이 신뢰할 수 없는 클라이언트로부터 네트워크를 보호하십시오.
- 가능하면 그리드 네트워크는 내부 트래픽에만 사용하십시오. 관리자 네트워크와 클라이언트 네트워크 모두 외부에서 내부 서비스로의 트래픽 유입을 차단하는 추가 방화벽 제한이 적용됩니다. 외부 클라이언트 트래픽에 그리드 네트워크를 사용하는 것도 가능하지만, 이 경우 보안 수준이 낮아집니다.
- StorageGRID 배포가 여러 데이터 센터에 걸쳐 있는 경우, 내부 트래픽에 대한 추가 보호를 위해 그리드 네트워크에서 가상 사설망(VPN) 또는 이와 동등한 기능을 사용하십시오.
- 일부 유지 관리 절차에는 기본 관리 노드와 다른 모든 그리드 노드 간의 22번 포트에 대한 보안 셸(SSH) 액세스가

필요합니다. 외부 방화벽을 사용하여 신뢰할 수 있는 클라이언트로 SSH 액세스를 제한하십시오.

관리자 네트워크 지침

관리자 네트워크는 일반적으로 관리 작업(Grid Manager 또는 SSH를 사용하는 신뢰할 수 있는 직원) 및 LDAP, DNS, NTP 또는 KMS(또는 KMIP 서버)와 같은 기타 신뢰할 수 있는 서비스와의 통신에 사용됩니다. 그러나 StorageGRID는 내부적으로 이러한 사용을 강제하지 않습니다.

관리자 네트워크를 사용하는 경우 다음 지침을 따르십시오.

- 관리자 네트워크의 모든 내부 트래픽 포트를 차단하십시오. 자세한 내용은 "[내부 포트 목록](#)"을 참조하십시오.
- 신뢰할 수 없는 클라이언트가 관리 네트워크에 액세스할 수 있는 경우 외부 방화벽을 사용하여 관리 네트워크의 StorageGRID에 대한 액세스를 차단하십시오.

클라이언트 네트워크 지침

클라이언트 네트워크는 일반적으로 테넌트 및 CloudMirror 복제 서비스 또는 다른 플랫폼 서비스와 같은 외부 서비스와의 통신에 사용됩니다. 그러나 StorageGRID는 내부적으로 이러한 사용을 강제하지 않습니다.

클라이언트 네트워크를 사용하는 경우 다음 지침을 따르십시오.

- 클라이언트 네트워크의 모든 내부 트래픽 포트를 차단하십시오. "[내부 포트 목록](#)"을 참조하십시오.
- 명시적으로 구성된 엔드포인트에서만 수신 클라이언트 트래픽을 허용합니다. 자세한 내용은 "[방화벽 제어 관리](#)"에 대한 정보를 참조하십시오.

StorageGRID 노드 보안 강화 지침

StorageGRID 노드는 VMware 가상 머신, Linux 호스트의 컨테이너 엔진 또는 전용 하드웨어 어플라이언스에 배포할 수 있습니다. 각 플랫폼 유형과 노드 유형에는 각각 고유한 보안 강화 모범 사례가 있습니다.

BMC에 대한 원격 IPMI 액세스 제어

BMC가 포함된 모든 어플라이언스에 대해 원격 IPMI 액세스를 활성화하거나 비활성화할 수 있습니다. 원격 IPMI 인터페이스를 사용하면 BMC 계정과 암호를 가진 모든 사용자가 StorageGRID 어플라이언스의 하드웨어에 저수준으로 액세스할 수 있습니다. BMC에 대한 원격 IPMI 액세스가 필요하지 않은 경우 이 옵션을 비활성화하십시오.

- Grid Manager에서 BMC에 대한 원격 IPMI 액세스를 제어하려면 구성 > 보안 > 보안 설정 > *어플라이언스*로 이동하십시오.
 - 원격 **IPMI** 액세스 활성화 확인란의 선택을 취소하여 BMC에 대한 IPMI 액세스를 비활성화합니다.
 - 원격 **IPMI** 액세스 활성화 확인란을 선택하여 BMC에 대한 IPMI 액세스를 활성화합니다.

BMC 강화에 대한 추가 정보는 "[베이스보드 관리 컨트롤러 강화](#)" "[국가안보국\(NSA\)](#)"에서 제공하는 사이버 보안 정보 사이트와 "[사이버보안 및 인프라 보안국\(CISA\)](#)"을 참조하십시오.

방화벽 구성

시스템 보안 강화 과정의 일환으로 외부 방화벽 구성을 검토하고, 필요한 IP 주소와 포트에서만 트래픽이 허용되도록

수정해야 합니다.

StorageGRID는 각 노드에 내부 방화벽을 포함하여 노드에 대한 네트워크 액세스를 제어함으로써 그리드의 보안을 강화합니다. 특정 그리드 배포에 필요한 포트를 제외한 모든 포트에서 네트워크 액세스를 차단하려면 ["내부 방화벽 제어 관리"](#)해야 합니다. 방화벽 제어 페이지에서 변경한 구성은 각 노드에 적용됩니다.

구체적으로 다음과 같은 영역을 관리할 수 있습니다.

- 권한 있는 주소: 외부 액세스 관리 탭의 설정에 의해 닫힌 포트에 액세스할 수 있도록 선택한 IP 주소 또는 서브넷을 허용할 수 있습니다.
- 외부 액세스 관리: 기본적으로 열려 있는 포트를 닫거나 이전에 닫았던 포트를 다시 열 수 있습니다.
- 신뢰할 수 없는 클라이언트 네트워크: 노드가 클라이언트 네트워크에서 들어오는 트래픽을 신뢰할지 여부와 신뢰할 수 없는 클라이언트 네트워크가 구성된 경우 열어야 할 추가 포트를 지정할 수 있습니다.

이 내부 방화벽은 몇 가지 일반적인 위협에 대한 추가적인 보호 계층을 제공하지만, 외부 방화벽의 필요성을 없애는 것은 아닙니다.

StorageGRID에서 사용하는 모든 내부 및 외부 포트 목록은 ["StorageGRID 내부 포트"](#) 및 ["외부 통신에 사용되는 포트"](#)를 참조하십시오.

사용하지 않는 서비스 비활성화

모든 StorageGRID 노드에서 사용하지 않는 서비스에 대한 액세스를 비활성화하거나 차단해야 합니다. 예를 들어 DHCP를 사용하지 않을 계획이라면 Grid Manager를 사용하여 포트 68을 닫으십시오. 구성 > 방화벽 제어 > *외부 액세스 관리*를 선택합니다. 그런 다음 포트 68의 상태 토글을 *열림*에서 *닫힘*으로 변경합니다.

가상화, 컨테이너 및 공유 하드웨어

모든 StorageGRID 노드에서 신뢰할 수 없는 소프트웨어와 동일한 물리적 하드웨어에서 StorageGRID를 실행하지 마십시오. StorageGRID와 악성 소프트웨어가 동일한 물리적 하드웨어에 존재하는 경우 하이퍼바이저 보호 기능이 악성 소프트웨어의 StorageGRID 보호 데이터 액세스를 방지할 수 있다고 가정하지 마십시오. 예를 들어, Meltdown 및 Spectre 공격은 최신 프로세서의 심각한 취약점을 악용하여 동일한 컴퓨터의 메모리에서 데이터를 탈취합니다.

설치 중 노드 보호

StorageGRID 노드를 설치하는 동안 신뢰할 수 없는 사용자가 네트워크를 통해 노드에 액세스하지 못하도록 하십시오. 노드는 그리드에 연결될 때까지 완전히 안전하지 않습니다.

하드웨어에 대한 물리적 액세스 제한

StorageGRID 하드웨어 어플라이언스 노드뿐만 아니라 StorageGRID를 실행하는 VMware 가상 머신 호스트 및 Linux 호스트에 대한 물리적 액세스를 승인된 관리자만으로 제한해야 합니다. 물리적 접근 제어의 예로는 잠금 장치, 경비원, 물리적 장벽 및 비디오 감시 등이 있습니다.

하드웨어 어플라이언스 노드는 승인된 관리자만 설치 및 운영할 수 있도록 설계되었습니다. 승인되지 않은 관리자가 하드웨어 어플라이언스 노드에 접근하지 못하도록 하십시오.

관리자 노드에 대한 지침

관리자 노드는 시스템 구성, 모니터링 및 로깅과 같은 관리 서비스를 제공합니다. 그리드 관리자 또는 테넌트 관리자에

로그인하면 관리자 노드에 연결됩니다.

StorageGRID 시스템의 관리 노드를 안전하게 보호하려면 다음 지침을 따르십시오.

- 개방형 인터넷상의 클라이언트와 같은 신뢰할 수 없는 클라이언트로부터 모든 관리 노드를 보호하십시오. 신뢰할 수 없는 클라이언트가 그리드 네트워크, 관리 네트워크 또는 클라이언트 네트워크의 어떤 관리 노드에도 액세스할 수 없도록 하십시오.
- StorageGRID 그룹은 Grid Manager 및 Tenant Manager 기능에 대한 액세스를 제어합니다. 각 사용자 그룹에 역할에 필요한 최소한의 권한만 부여하고, 읽기 전용 액세스 모드를 사용하여 사용자가 구성을 변경하지 못하도록 합니다.
- StorageGRID 로드 밸런서 엔드포인트를 사용할 때는 신뢰할 수 없는 클라이언트 트래픽에 대해 관리 노드 대신 게이트웨이 노드를 사용하십시오.
- 신뢰할 수 없는 테넌트가 있는 경우, 해당 테넌트가 테넌트 관리자 또는 테넌트 관리 API에 직접 액세스하지 못하도록 하십시오. 대신, 신뢰할 수 없는 테넌트는 테넌트 관리 API와 연동되는 테넌트 포털 또는 외부 테넌트 관리 시스템을 사용하도록 하십시오.
- 선택적으로, 관리 노드에서 NetApp 지원으로의 AutoSupport 통신을 보다 세부적으로 제어하려면 관리 프록시를 사용하십시오. "[관리자 프록시 생성](#)"에 대한 단계를 참조하십시오.
- 선택적으로, 제한된 8443 및 9443 포트를 사용하여 Grid Manager와 Tenant Manager 간의 통신을 분리할 수 있습니다. 추가적인 보호를 위해 공유 포트인 443을 차단하고 테넌트 요청을 9443 포트에 제한하십시오.
- 선택적으로, 그리드 관리자와 테넌트 사용자를 위해 별도의 관리 노드를 사용할 수 있습니다.

더 자세한 내용은 "[StorageGRID 관리](#)"에 대한 지침을 참조하세요.

스토리지 노드에 대한 지침

스토리지 노드는 객체 데이터와 메타데이터를 관리하고 저장합니다. StorageGRID 시스템의 스토리지 노드를 안전하게 보호하려면 다음 지침을 따르십시오.

- 신뢰할 수 없는 클라이언트가 스토리지 노드에 직접 연결하지 못하도록 하십시오. 게이트웨이 노드 또는 타사 로드 밸런서에서 제공하는 로드 밸런서 엔드포인트를 사용하십시오.
- 신뢰할 수 없는 테넌트에 대해서는 아웃바운드 서비스를 활성화하지 마십시오. 예를 들어, 신뢰할 수 없는 테넌트의 계정을 생성할 때 테넌트가 자체 ID 소스를 사용하거나 플랫폼 서비스를 사용하도록 허용하지 마십시오. 자세한 단계는 "[테넌트 계정 생성](#)"을 참조하십시오.
- 신뢰할 수 없는 클라이언트 트래픽에는 타사 로드 밸런서를 사용하십시오. 타사 로드 밸런서는 더 많은 제어 권한과 공격에 대한 추가적인 보호 계층을 제공합니다.
- 선택적으로 스토리지 프록시를 사용하여 Cloud Storage Pool과 스토리지 노드에서 외부 서비스로의 플랫폼 서비스 통신을 더욱 세밀하게 제어할 수 있습니다. 자세한 단계는 "[스토리지 프록시 생성](#)"을 참조하십시오.
- 선택적으로 클라이언트 네트워크를 사용하여 외부 서비스에 연결할 수 있습니다. 그런 다음 구성 > 보안 > 방화벽 제어 > *신뢰할 수 없는 클라이언트 네트워크*를 선택하고 스토리지 노드의 클라이언트 네트워크를 신뢰할 수 없음으로 지정합니다. 그러면 스토리지 노드는 클라이언트 네트워크를 통한 수신 트래픽을 더 이상 허용하지 않지만 플랫폼 서비스에 대한 발신 요청은 계속 허용합니다.

게이트웨이 노드에 대한 지침

게이트웨이 노드는 클라이언트 애플리케이션이 StorageGRID에 연결하는 데 사용할 수 있는 선택적 로드 밸런싱 인터페이스를 제공합니다. StorageGRID 시스템의 게이트웨이 노드를 보호하려면 다음 지침을 따르십시오.

- 로드 밸런서 엔드포인트를 구성하고 사용합니다. "[로드 밸런싱 고려 사항](#)"을 참조하십시오.
- 신뢰할 수 없는 클라이언트 트래픽의 경우 클라이언트와 게이트웨이 노드 또는 스토리지 노드 사이에 타사 로드 밸런서를 사용하십시오. 타사 로드 밸런싱은 더 많은 제어 권한과 공격에 대한 추가적인 보호 계층을 제공합니다. 타사 로드 밸런서를 사용하는 경우에도 네트워크 트래픽이 내부 로드 밸런서 엔드포인트를 거치거나 스토리지 노드로 직접 전송되도록 선택적으로 구성할 수 있습니다.
- 로드 밸런싱 엔드포인트를 사용하는 경우, 클라이언트가 클라이언트 네트워크를 통해 연결하도록 설정할 수 있습니다. 그런 다음, 구성 > 보안 > 방화벽 제어 > *신뢰할 수 없는 클라이언트 네트워크*를 선택하고 게이트웨이 노드의 클라이언트 네트워크를 신뢰할 수 없는 네트워크로 지정합니다. 게이트웨이 노드는 로드 밸런서 엔드포인트로 명시적으로 구성된 포트에서만 수신 트래픽을 허용합니다.

하드웨어 어플라이언스 노드에 대한 지침

StorageGRID 하드웨어 어플라이언스는 StorageGRID 시스템에서 사용하도록 특별히 설계되었습니다. 일부 어플라이언스는 스토리지 노드로 사용할 수 있습니다. 다른 어플라이언스는 관리 노드 또는 게이트웨이 노드로 사용할 수 있습니다. 어플라이언스 노드와 소프트웨어 기반 노드를 조합하거나, 모든 어플라이언스로 구성된 완전 맞춤형 그리드를 구축할 수 있습니다.

StorageGRID 시스템의 하드웨어 어플라이언스 노드를 안전하게 보호하려면 다음 지침을 따르십시오.

- 어플라이언스가 스토리지 컨트롤러 관리에 SANtricity System Manager를 사용하는 경우, 신뢰할 수 없는 클라이언트가 네트워크를 통해 SANtricity System Manager에 액세스하지 못하도록 차단하십시오.
- 기기에 베이스보드 관리 컨트롤러(BMC)가 있는 경우, BMC 관리 포트를 통해 낮은 수준의 하드웨어 액세스가 가능하다는 점에 유의하십시오. BMC 관리 포트는 안전하고 신뢰할 수 있는 내부 관리 네트워크에만 연결하십시오.

VLAN을 설정하여 BMC 네트워크 연결을 격리하고 BMC 인터넷 액세스를 신뢰할 수 있는 네트워크로 제한할 수 있습니다. VLAN 분리 적용에 대한 자세한 내용은 "[베이스보드 관리 컨트롤러 강화](#)" 사이버 보안 정보 시트를 "[국가안보국\(NSA\)](#)" 및 "[사이버보안 및 인프라 보안국\(CISA\)](#)"에서 참조하십시오.

안전하고 신뢰할 수 있는 내부 관리 네트워크를 사용할 수 없는 경우 BMC 관리 포트를 연결하지 않거나 차단하십시오. 기술 지원 담당자가 지원 사례 처리 중에 임시 액세스 권한을 요청할 수 있습니다.

- 어플라이언스가 IPMI(Intelligent Platform Management Interface) 표준을 사용하여 이더넷을 통해 컨트롤러 하드웨어의 원격 관리를 지원하는 경우, 포트 623에서 신뢰할 수 없는 트래픽을 차단하십시오.



BMC가 포함된 모든 어플라이언스에 대해 원격 IPMI 액세스를 활성화하거나 비활성화할 수 있습니다. 원격 IPMI 인터페이스를 사용하면 BMC 계정과 암호를 가진 모든 사용자가 StorageGRID 어플라이언스에 대한 하위 수준의 하드웨어 액세스를 수행할 수 있습니다. BMC에 대한 원격 IPMI 액세스가 필요하지 않은 경우 다음 방법 중 하나를 사용하여 이 옵션을 비활성화하십시오. + Grid Manager에서 구성 > 보안 > 보안 설정 > 어플라이언스*로 이동하여 *원격 IPMI 액세스 활성화 확인란을 선택 해제합니다. + Grid 관리 API에서 비공개 엔드포인트를 사용합니다. PUT /private/bmc.

+ 또한 [원격 IPMI 액세스 비활성화](#)할 수도 있습니다.

- SANtricity System Manager로 관리하는 SED, FDE 또는 FIPS NL-SAS 드라이브가 포함된 어플라이언스 모델의 경우 "[SANtricity 드라이브 보안 활성화 및 구성](#)".
- StorageGRID Appliance Installer 및 Grid Manager를 사용하여 관리하는 SED 또는 FIPS NVMe SSD가 포함된 어플라이언스 모델의 경우, "[StorageGRID 드라이브 암호화 활성화 및 구성](#)".
- SED, FDE 또는 FIPS 드라이브가 없는 어플라이언스의 경우 키 관리 서버(KMS)를 사용하여 "[StorageGRID 소프트웨어 노드 암호화 활성화 및 구성](#)".

StorageGRID의 TLS 및 SSH 강화 지침

SSH 액세스를 제어하고, 기본 TLS 인증서를 교체하고, TLS 및 SSH 연결에 적합한 보안 정책을 선택해야 합니다.

인증서 강화 지침

설치 중에 생성된 기본 인증서를 사용자 지정 인증서로 교체해야 합니다.

많은 조직에서 StorageGRID 웹 액세스에 대한 자체 서명 디지털 인증서는 정보 보안 정책을 준수하지 않습니다. 운영 시스템에서는 StorageGRID 인증에 사용할 CA 서명 디지털 인증서를 설치해야 합니다.

구체적으로 말하자면, 이러한 기본 인증서 대신 사용자 지정 서버 인증서를 사용해야 합니다.

- 관리 인터페이스 인증서: 그리드 관리자, 테넌트 관리자, 그리드 관리 API 및 테넌트 관리 API에 대한 액세스를 보호하는 데 사용됩니다.
- **S3 API** 인증서: S3 클라이언트 애플리케이션이 객체 데이터를 업로드 및 다운로드하는 데 사용하는 스토리지 노드 및 게이트웨이 노드에 대한 액세스를 보호하는 데 사용됩니다.

자세한 내용 및 지침은 "[보안 인증서 관리](#)"를 참조하십시오.



StorageGRID는 로드 밸런서 엔드포인트에 사용되는 인증서를 별도로 관리합니다. 로드 밸런서 인증서를 구성하려면 "[로드 밸런서 엔드포인트 구성](#)"을 참조하십시오.

사용자 지정 서버 인증서를 사용할 때는 다음 지침을 따르십시오.

- 인증서에는 StorageGRID에 대한 DNS 항목과 일치하는 ``subjectAltName``이(가) 있어야 합니다. 자세한 내용은 "[RFC 5280: PKIX 인증서 및 CRL 프로필](#)"의 4.2.1.6절 "주체 대체 이름"을 참조하십시오.
- 가능하면 와일드카드 인증서 사용을 피하십시오. 단, 버킷 이름을 사전에 알 수 없는 경우 와일드카드 인증서가 필요한 S3 가상 호스팅 스타일 엔드포인트용 인증서는 예외입니다.
- 인증서에 와일드카드를 사용해야 하는 경우 위험을 줄이기 위해 추가적인 조치를 취해야 합니다.
`*.s3.example.com``와 같은 와일드카드 패턴을 사용하고 다른 애플리케이션에는 ``s3.example.com`` 접미사를 사용하지 마십시오. 이 패턴은 ``dc1-s1.s3.example.com/mybucket``와 같은 경로 스타일 S3 액세스에도 적용됩니다.
- 인증서 만료 기간을 짧게(예: 2개월) 설정하고, Grid Management API를 사용하여 인증서 순환을 자동화하십시오. 이는 특히 와일드카드 인증서에 중요합니다.

또한 클라이언트는 StorageGRID와 통신할 때 엄격한 호스트 이름 확인을 사용해야 합니다.

TLS 및 SSH 정책 강화 지침

보안 정책을 선택하여 클라이언트 애플리케이션과의 안전한 TLS 연결 및 내부 StorageGRID 서비스와의 안전한 SSH 연결을 설정하는 데 사용할 프로토콜과 암호화 방식을 결정할 수 있습니다.

보안 정책은 TLS 및 SSH를 사용하여 전송 중인 데이터를 암호화하는 방식을 제어합니다. 모범 사례로, 애플리케이션

호환성에 필요하지 않은 암호화 옵션은 비활성화하는 것이 좋습니다. 시스템이 Common Criteria, FIPS 140-2를 준수해야 하거나 다른 암호화 방식을 사용해야 하는 경우가 아니라면 기본값인 Modern 정책을 사용하십시오.

자세한 내용 및 지침은 ["TLS 및 SSH 정책 관리"](#)을 참조하십시오.

외부 SSH 액세스 관리

시스템 보안 강화를 위해 외부 SSH 접속은 기본적으로 차단되어 있습니다. 문제 해결과 같이 인바운드 SSH 접속이 필요한 작업에만 SSH 접속을 활성화하십시오. 자세한 내용 및 지침은 ["외부 SSH 액세스 관리"](#)을 참조하십시오.

StorageGRID의 로그, 암호 및 감사 메시지에 대한 강화 지침

StorageGRID 네트워크 및 노드에 대한 보안 강화 지침을 준수하는 것 외에도 StorageGRID 시스템의 다른 영역에 대한 보안 강화 지침도 준수해야 합니다.

임시 설치 비밀번호

StorageGRID 시스템 설치 보안을 강화하려면 StorageGRID 설치 UI 또는 설치 API의 임시 설치 암호 페이지에서 암호를 설정하십시오. 설정된 암호는 사용자 인터페이스, 설치 API 및 `configure-storagegrid.py` 스크립트를 포함한 StorageGRID 설치의 모든 방법에 적용됩니다.

자세한 내용은 다음을 참조하십시오.

- ["소프트웨어 기반 노드에 StorageGRID 설치"](#)
- ["StorageGRID 어플라이언스 설치"](#)

로그 및 감사 메시지

StorageGRID 로그 및 감사 메시지 출력은 항상 안전하게 보호해야 합니다. StorageGRID 로그 및 감사 메시지는 지원 및 시스템 가용성 측면에서 매우 중요한 정보를 제공합니다. 또한 StorageGRID 로그 및 감사 메시지 출력에 포함된 정보는 일반적으로 민감한 내용입니다.

StorageGRID 보안 이벤트를 외부 syslog 서버로 전송하도록 구성하십시오. syslog 내보내기를 사용하는 경우 전송 프로토콜로 TLS 및 RELP/TLS를 선택하십시오.

StorageGRID 로그에 대한 자세한 내용은 ["로그 파일 참조"](#)을 참조하십시오. StorageGRID 감사 메시지에 대한 자세한 내용은 ["감사 메시지"](#)을 참조하십시오.

NetApp AutoSupport

StorageGRID의 AutoSupport 기능을 사용하면 시스템의 상태를 사전에 모니터링하고 NetApp 지원 사이트, 조직의 내부 지원 팀 또는 지원 파트너에게 패키지를 자동으로 보낼 수 있습니다. 기본적으로 StorageGRID를 처음 구성할 때 NetApp로 AutoSupport 패키지를 보내는 기능이 활성화됩니다.

AutoSupport 기능을 비활성화할 수 있습니다. 그러나 StorageGRID 시스템에 문제가 발생할 경우 AutoSupport를 통해 문제를 신속하게 식별하고 해결할 수 있으므로 NetApp에서는 이 기능을 활성화할 것을 권장합니다.

AutoSupport는 전송 프로토콜로 HTTPS, HTTP 및 SMTP를 지원합니다. AutoSupport 패키지의 민감한 특성으로 인해 NetApp은 AutoSupport 패키지를 NetApp에 전송하기 위한 기본 전송 프로토콜로 HTTPS를 사용할 것을 강력히 권장합니다.

CORS(Cross-Origin Resource Sharing)

S3 버킷과 그 안에 있는 객체가 다른 도메인의 웹 애플리케이션에서 액세스 가능하도록 하려면 CORS(교차 출처 리소스 공유)를 구성할 수 있습니다. 일반적으로 CORS는 필요한 경우가 아니면 활성화하지 않는 것이 좋습니다. CORS가 필요한 경우, 신뢰할 수 있는 출처로 제한하십시오.

자세한 단계는 "[버킷 및 객체에 대한 CORS 구성](#)"을 참조하세요.

외부 보안 장치

완벽한 보안 강화 솔루션은 StorageGRID 외부의 보안 메커니즘을 다루어야 합니다. 추가 인프라 장치를 사용하여 StorageGRID에 대한 액세스를 필터링하고 제한하는 것은 강력한 보안 태세를 구축하고 유지하는 효과적인 방법입니다. 이러한 외부 보안 장치에는 방화벽, 침입 방지 시스템(IPS) 및 기타 보안 장치가 포함됩니다.

신뢰할 수 없는 클라이언트 트래픽에는 타사 로드 밸런서를 사용하는 것이 좋습니다. 타사 로드 밸런싱은 더 많은 제어 권한과 공격에 대한 추가적인 보호 계층을 제공합니다.

랜섬웨어 완화

다음 권장 사항을 준수하여 랜섬웨어 공격으로부터 객체 데이터를 보호하십시오 "[StorageGRID를 통한 랜섬웨어 방어](#)".

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 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.