시스템 강화

StorageGRID 11.8

NetApp
March 19, 2024

목차

시스템 강화

시스템 강화: 개요

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

이 문서에서는 StorageGRID와 관련된 강화 지침에 대해 간략하게 설명합니다. 이 지침은 시스템 강화를 위한 업계 표준 모범 사례를 보완합니다. 예를 들어, 이 지침에서는 StorageGRID에 강력한 암호를 사용하고 HTTP 대신 HTTPS를 사용하고 가능한 경우 인증서 기반 인증을 활성화한다고 가정합니다.

StorageGRID를 설치 및 구성할 때 이 지침을 사용하여 정보 시스템의 기밀성, 무결성 및 가용성에 대해 규정된 모든 보안 목표를 충족할 수 있습니다.

StorageGRID는 을 따릅니다 "NetApp 취약성 처리 정책". 보고된 취약점은 제품 보안 사고 대응 프로세스에 따라 확인 및 해결됩니다.

StorageGRID 시스템 강화를 위한 일반 고려 사항

StorageGRID 시스템을 강화하려면 다음 사항을 고려해야 합니다.

- 구현한 3개의 StorageGRID 네트워크는 무엇입니까? 모든 StorageGRID 시스템은 그리드 네트워크를 사용해야 하지만 관리자 네트워크, 클라이언트 네트워크 또는 둘 다를 사용할 수도 있습니다. 각 네트워크마다 서로 다른 보안 고려 사항이 있습니다.
- StorageGRID 시스템의 개별 노드에 사용하는 플랫폼 유형입니다. StorageGRID 노드는 VMware 가상 머신, Linux 호스트의 컨테이너 엔진 내부 또는 전용 하드웨어 어플라이언스에 구축할 수 있습니다. 각 플랫폼 유형에는 강화 모범 사례가 자체적으로 있습니다.
- 테넌트 계정의 신뢰성. 신뢰할 수 없는 테넌트 계정을 사용하는 서비스 공급자라면 신뢰할 수 있는 내부 테넌트만 사용하는 것과 보안 문제가 다릅니다.
- 조직의 보안 요구 사항 및 규약 뒤에 오는 것은 무엇입니까? 특정 규정 또는 기업 요구 사항을 준수해야 할 수 있습니다.

소프트웨어 업그레이드 강화 지침

공격을 방어하려면 StorageGRID 시스템 및 관련 서비스를 최신 상태로 유지해야 합니다.

StorageGRID 소프트웨어로 업그레이드합니다

가능하면 StorageGRID 소프트웨어를 최신 주요 릴리즈나 이전 주요 릴리즈로 업그레이드해야 합니다. StorageGRID를 최신 상태로 유지하면 알려진 취약점이 활성화되는 시간을 줄이고 전체 공격 노출 영역을 줄일 수 있습니다. 또한 최신 버전의 StorageGRID에는 이전 릴리즈에 포함되지 않은 보안 강화 기능이 포함되어 있는 경우가 많습니다.

을 참조하십시오 "NetApp 상호 운용성 매트릭스 툴" (IMT) 을 클릭하여 사용해야 하는 StorageGRID 소프트웨어 버전을 확인합니다. 핫픽스가 필요한 경우 NetApp은 가장 최근 릴리즈에 대한 업데이트를 만드는 데 우선 순위를 지정합니다. 일부 패치는 이전 릴리스와 호환되지 않을 수 있습니다.

- 최신 StorageGRID 릴리스 및 핫픽스를 다운로드하려면 로 이동하십시오 "NetApp 다운로드: StorageGRID".

- StorageGRID 소프트웨어를 업그레이드하려면 를 참조하십시오 "업그레이드 지침".
- 핫픽스를 적용하려면 를 참조하십시오 "StorageGRID 핫픽스 절차".

외부 서비스로 업그레이드

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

지원되는 버전 목록은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

하이퍼바이저로 업그레이드

StorageGRID 노드가 VMware 또는 다른 하이퍼바이저에서 실행 중인 경우 하이퍼바이저 소프트웨어 및 펌웨어를 최신 상태로 유지해야 합니다.

지원되는 버전 목록은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

* Linux 노드로 업그레이드 *

StorageGRID 노드가 Linux 호스트 플랫폼을 사용하는 경우 보안 업데이트 및 커널 업데이트가 호스트 OS에 적용되었는지 확인해야 합니다. 또한 이러한 업데이트를 사용할 수 있게 되면 취약한 하드웨어에 펌웨어 업데이트를 적용해야 합니다.

지원되는 버전 목록은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

StorageGRID 네트워크에 대한 강화 지침

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

StorageGRID 네트워크에 대한 자세한 내용은 를 참조하십시오 "StorageGRID 네트워크 유형입니다".

그리드 네트워크 지침

모든 내부 StorageGRID 트래픽에 대해 그리드 네트워크를 구성해야 합니다. 모든 그리드 노드는 그리드 네트워크에 있으며 다른 모든 노드와 통신할 수 있어야 합니다.

그리드 네트워크를 구성할 때 다음 지침을 따르십시오.

- 네트워크가 인터넷에 있는 클라이언트와 같이 신뢰할 수 없는 클라이언트로부터 보호되는지 확인합니다.
- 가능한 경우 내부 트래픽에만 그리드 네트워크를 사용합니다. 관리 네트워크와 클라이언트 네트워크 모두 내부 서비스에 대한 외부 트래픽을 차단하는 추가 방화벽 제한이 있습니다. 외부 클라이언트 트래픽에 그리드 네트워크 사용이 지원되지만, 이러한 사용은 보호 계층의 수를 줄입니다.
- StorageGRID 구축이 여러 데이터 센터에 걸쳐 있는 경우, 내부 트래픽을 추가로 보호하기 위해 VPN(가상 사설망) 또는 이와 동등한 그리드 네트워크를 사용합니다.
- 일부 유지 관리 절차에서는 기본 관리 노드와 다른 모든 그리드 노드 사이의 포트 22에서 SSH(Secure Shell) 액세스가 필요합니다. 외부 방화벽을 사용하여 신뢰할 수 있는 클라이언트에 대한 SSH 액세스를 제한합니다.

관리 네트워크 지침

관리 네트워크는 일반적으로 관리 작업(Grid Manager 또는 SSH를 사용하는 신뢰할 수 있는 직원)과 LDAP, DNS, NTP 또는 KMS(또는 KMIP 서버)와 통신하는 데 사용됩니다. 그러나 StorageGRID에서는 이 사용을 내부적으로 적용하지 않습니다.

관리자 네트워크를 사용하는 경우 다음 지침을 따르십시오.

- 관리 네트워크의 모든 내부 트래픽 포트를 차단합니다. 를 참조하십시오 "내부 포트 목록입니다".
- 신뢰할 수 없는 클라이언트가 관리자 네트워크에 액세스할 수 있는 경우 외부 방화벽을 사용하여 관리자 네트워크의 StorageGRID에 대한 액세스를 차단합니다.

클라이언트 네트워크 지침

클라이언트 네트워크는 일반적으로 테넌트에 사용되며 CloudMirror 복제 서비스 또는 다른 플랫폼 서비스와 같은 외부 서비스와 통신하는 데 사용됩니다. 그러나 StorageGRID에서는 이 사용을 내부적으로 적용하지 않습니다.

클라이언트 네트워크를 사용하는 경우 다음 지침을 따르십시오.

- 클라이언트 네트워크의 모든 내부 트래픽 포트를 차단합니다. 를 참조하십시오 "내부 포트 목록입니다".
- 명시적으로 구성된 끝점에서만 인바운드 클라이언트 트래픽을 허용합니다. 에 대한 정보를 참조하십시오 "방화벽 제어 관리".

StorageGRID 노드에 대한 강화 지침

StorageGRID 노드는 VMware 가상 머신, Linux 호스트의 컨테이너 엔진 내부 또는 전용 하드웨어 어플라이언스에 구축할 수 있습니다. 각 플랫폼 유형과 각 노드 유형에는 강화 모범 사례가 포함되어 있습니다.

BMC에 대한 원격 IPMI 액세스를 제어합니다

BMC를 포함하는 모든 어플라이언스에 대해 원격 IPMI 액세스를 활성화 또는 비활성화할 수 있습니다. 원격 IPMI 인터페이스를 사용하면 BMC 계정 및 암호를 가진 모든 사용자가 StorageGRID 어플라이언스에 낮은 수준의 하드웨어 액세스를 할 수 있습니다. BMC에 대한 원격 IPMI 액세스가 필요하지 않으면 이 옵션을 비활성화합니다.

- Grid Manager에서 BMC에 대한 원격 IPMI 액세스를 제어하려면 * configuration * > * Security * > * Security settings * > * Appliances *:
  - BMC에 대한 IPMI 액세스를 비활성화하려면 * 원격 IPMI 액세스 활성화 * 확인란을 선택 취소합니다.
  - BMC에 대한 IPMI 액세스를 활성화하려면 * 원격 IPMI 액세스 활성화 * 확인란을 선택합니다.

방화벽 구성

시스템 강화 프로세스의 일환으로 외부 방화벽 구성을 검토하고 트래픽이 IP 주소 및 해당 IP 주소가 반드시 필요한 포트에서만 허용되도록 수정해야 합니다.

StorageGRID에는 노드에 대한 네트워크 액세스를 제어할 수 있도록 함으로써 그리드의 보안을 강화하는 각 노드에 대한 내부 방화벽이 포함되어 있습니다. 당신은 해야 한다 "내부 방화벽 제어를 관리합니다" 특정 그리드 구축에 필요한 포트를 제외한 모든 포트에 대한 네트워크 액세스를 방지합니다. 방화벽 제어 페이지에서 변경한 구성은 각 노드에

배포됩니다.

특히, 다음과 같은 영역을 관리할 수 있습니다.

- * 특별 권한 주소 *: 선택한 IP 주소 또는 서브넷이 외부 액세스 관리 탭의 설정으로 닫힌 포트에 액세스하도록 허용할 수 있습니다.
- * 외부 액세스 관리 *: 기본적으로 열려 있는 포트를 닫거나 이전에 닫은 포트를 다시 열 수 있습니다.
- * 신뢰할 수 없는 클라이언트 네트워크 *: 노드가 클라이언트 네트워크의 인바운드 트래픽을 신뢰하는지 여부와 신뢰할 수 없는 클라이언트 네트워크가 구성될 때 열려는 추가 포트를 트러스트할지 여부를 지정할 수 있습니다.

이 내부 방화벽은 일부 일반적인 위협에 대한 추가 보호 계층을 제공하지만 외부 방화벽의 필요성을 제거하지 않습니다.

StorageGRID에서 사용하는 모든 내부 및 외부 포트 목록은 를 참조하십시오 "네트워크 포트 참조".

사용하지 않는 서비스를 비활성화합니다

모든 StorageGRID 노드에 대해 사용하지 않는 서비스에 대한 액세스를 비활성화하거나 차단해야 합니다. 예를 들어, NFS에 대한 감사 공유에 대한 클라이언트 액세스를 구성하지 않을 경우 이러한 서비스에 대한 액세스를 차단하거나 해제합니다.

가상화, 컨테이너 및 공유 하드웨어

모든 StorageGRID 노드의 경우 신뢰할 수 없는 소프트웨어와 동일한 물리적 하드웨어에서 StorageGRID를 실행하지 마십시오. StorageGRID와 맬웨어가 모두 동일한 물리적 하드웨어에 존재할 경우 하이퍼바이저 보호를 통해 맬웨어가 StorageGRID로 보호되는 데이터에 액세스하지 못할 것이라고 가정하지 마십시오. 예를 들어 멜트다운 및 스펙터 공격은 최신 프로세서의 중요한 취약점을 악용하고 프로그램이 동일한 컴퓨터의 메모리에 있는 데이터를 훔칠 수 있도록 합니다.

설치하는 동안 노드를 보호합니다

노드가 설치될 때 신뢰할 수 없는 사용자가 네트워크를 통해 StorageGRID 노드에 액세스하도록 허용하지 않습니다. 노드가 그리드에 가입될 때까지 완전히 보안되지 않습니다.

관리 노드에 대한 지침

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

다음 지침에 따라 StorageGRID 시스템의 관리 노드를 보호합니다.

- 인터넷에 있는 클라이언트와 같이 신뢰할 수 없는 클라이언트의 모든 관리 노드를 보호합니다. 신뢰할 수 없는 클라이언트가 그리드 네트워크, 관리 네트워크 또는 클라이언트 네트워크의 관리 노드에 액세스할 수 있는지 확인합니다.
- StorageGRID 그룹은 그리드 관리자 및 테넌트 관리자 기능에 대한 액세스를 제어합니다. 각 사용자 그룹에 역할에 필요한 최소 권한을 부여하고 읽기 전용 액세스 모드를 사용하여 사용자가 구성을 변경하지 못하도록 합니다.
- StorageGRID 로드 밸런서 끝점을 사용할 때는 신뢰할 수 없는 클라이언트 트래픽에 관리자 노드 대신 게이트웨이 노드를 사용합니다.
- 신뢰할 수 없는 테넌트가 있는 경우 테넌트 관리자 또는 테넌트 관리 API에 직접 액세스할 수 없도록 허용해서는 안 됩니다. 대신 신뢰할 수 없는 테넌트가 테넌트 관리 API와 상호 작용하는 테넌트 포털 또는 외부 테넌트 관리

시스템을 사용하도록 합니다.

- 필요한 경우 관리자 프록시를 사용하여 관리 노드에서 NetApp 지원으로의 AutoSupport 통신을 더욱 강력하게 제어할 수 있습니다. 의 단계를 참조하십시오 "관리자 프록시를 만드는 중입니다".
- 필요에 따라 제한된 8443 및 9443 포트를 사용하여 Grid Manager 및 Tenant Manager 통신을 분리합니다. 추가 보호를 위해 공유 포트 443을 차단하고 테넌트 요청을 포트 9443으로 제한합니다.
- 선택적으로 그리드 관리자 및 테넌트 사용자에 대해 별도의 관리 노드를 사용합니다.

자세한 내용은 의 지침을 참조하십시오 "StorageGRID 관리".

스토리지 노드 지침

스토리지 노드: 오브젝트 데이터 및 메타데이터를 관리하고 저장합니다. 다음 지침에 따라 StorageGRID 시스템의 스토리지 노드를 보호합니다.

- 신뢰할 수 없는 클라이언트가 스토리지 노드에 직접 연결하도록 허용하지 않습니다. 게이트웨이 노드 또는 타사 로드 밸런서가 제공하는 로드 밸런서 끝점을 사용합니다.
- 신뢰할 수 없는 테넌트에 대해 아웃바운드 서비스를 활성화하지 마십시오. 예를 들어, 신뢰할 수 없는 테넌트의 계정을 생성할 때 테넌트가 자신의 ID 소스를 사용하도록 허용하지 않고 플랫폼 서비스의 사용을 허용하지 않습니다. 의 단계를 참조하십시오 "테넌트 계정을 생성하는 중입니다".
- 신뢰할 수 없는 클라이언트 트래픽에 타사 로드 밸런서를 사용합니다. 타사 로드 밸런싱은 더 많은 제어 기능과 공격에 대한 추가적인 보호 계층을 제공합니다.
- 필요한 경우 스토리지 프록시를 사용하여 스토리지 노드에서 외부 서비스로의 클라우드 스토리지 풀 및 플랫폼 서비스 통신을 더욱 강력하게 제어할 수 있습니다. 의 단계를 참조하십시오 "스토리지 프록시 생성".
- 선택적으로 클라이언트 네트워크를 사용하여 외부 서비스에 연결합니다. 그런 다음 * 구성 * > * 보안 * > * 방화벽 제어 * > * 신뢰할 수 없는 클라이언트 네트워크 * 를 선택하고 스토리지 노드의 클라이언트 네트워크를 신뢰할 수 없음을 표시합니다. 스토리지 노드는 더 이상 클라이언트 네트워크에서 들어오는 트래픽을 허용하지 않지만 플랫폼 서비스에 대한 아웃바운드 요청은 계속 허용합니다.

게이트웨이 노드에 대한 지침

게이트웨이 노드는 클라이언트 애플리케이션이 StorageGRID에 연결하는 데 사용할 수 있는 선택적 로드 밸런싱 인터페이스를 제공합니다. 다음 지침에 따라 StorageGRID 시스템의 게이트웨이 노드를 보호합니다.

- 로드 밸런서 엔드포인트를 구성하고 사용합니다. 을 참조하십시오 "로드 균형 조정에 대한 고려 사항".
- 신뢰할 수 없는 클라이언트 트래픽에 대해 클라이언트와 게이트웨이 노드 또는 스토리지 노드 간에 타사 로드 밸런서를 사용합니다. 타사 로드 밸런싱은 더 많은 제어 기능과 공격에 대한 추가적인 보호 계층을 제공합니다. 타사 로드 밸런서를 사용하는 경우에도 내부 로드 밸런서 엔드포인트를 통과하도록 네트워크 트래픽을 선택적으로 구성하거나 스토리지 노드로 직접 보내도록 구성할 수 있습니다.
- 부하 분산 엔드포인트를 사용하는 경우 선택적으로 클라이언트가 클라이언트 네트워크를 통해 접속하도록 합니다. 그런 다음 * 구성 * > * 보안 * > * 방화벽 제어 * > * 신뢰할 수 없는 클라이언트 네트워크 * 를 선택하고 게이트웨이 노드의 클라이언트 네트워크를 신뢰할 수 없음을 표시합니다. 게이트웨이 노드는 로드 밸런서 끝점으로 명시적으로 구성된 포트의 인바운드 트래픽만 허용합니다.

하드웨어 어플라이언스 노드에 대한 지침입니다

StorageGRID 하드웨어 어플라이언스는 StorageGRID 시스템에서 사용하도록 특별히 설계되었습니다. 일부 어플라이언스는 스토리지 노드로 사용할 수 있습니다. 다른 어플라이언스를 관리 노드 또는 게이트웨이 노드로 사용할

수 있습니다. 어플라이언스 노드를 소프트웨어 기반 노드와 결합하거나 완전히 엔지니어링된 모든 어플라이언스 그리드를 구축할 수 있습니다.

StorageGRID 시스템에서 하드웨어 어플라이언스 노드를 보호하려면 다음 지침을 따르십시오.

- 어플라이언스가 스토리지 컨트롤러 관리에 SANtricity System Manager를 사용하는 경우 신뢰할 수 없는 클라이언트가 네트워크를 통해 SANtricity System Manager에 액세스하지 못하도록 합니다.
- 어플라이언스에 BMC(베이스보드 관리 컨트롤러)가 있는 경우 BMC 관리 포트가 낮은 수준의 하드웨어 액세스를 허용한다는 점에 유의하십시오. BMC 관리 포트는 안전하고 신뢰할 수 있는 내부 관리 네트워크에만 연결합니다. 이러한 네트워크를 사용할 수 없는 경우 기술 지원 부서에서 BMC 연결을 요청하지 않는 한 BMC 관리 포트는 연결되지 않거나 차단된 상태로 둡니다.
- 어플라이언스가 IPMI(Intelligent Platform Management Interface) 표준을 사용하여 이더넷을 통한 컨트롤러 하드웨어의 원격 관리를 지원하는 경우 포트 623에서 신뢰할 수 없는 트래픽을 차단합니다.

> BMC를 포함하는 모든 어플라이언스에 대해 원격 IPMI 액세스를 활성화 또는 비활성화할 수 있습니다. 원격 IPMI 인터페이스를 사용하면 BMC 계정 및 암호를 가진 모든 사용자가 StorageGRID 어플라이언스에 낮은 수준의 하드웨어 액세스를 할 수 있습니다. BMC에 대한 원격 IPMI 액세스가 필요하지 않으면 다음 방법 중 하나를 사용하여 이 옵션을 비활성화합니다 Grid Manager에서 * configuration * > * Security * > * Security settings * > * Appliances * 로 이동하고 * Enable remote IPMI access * 확인란을 선택 취소합니다. 를 누릅니다 그리드 관리 API에서 전용 엔드포인트를 사용합니다. `PUT /private/bmc`.

- SANtricity System Manager로 관리하는 SED, FDE 또는 FIPS NL-SAS 드라이브를 포함한 어플라이언스 모델의 경우, "SANtricity 드라이브 보안을 활성화하고 구성합니다".
- StorageGRID 어플라이언스 설치 프로그램 및 그리드 관리자를 사용하여 관리하는 SED 또는 FIPS NVMe SSD를 포함한 어플라이언스 모델의 경우, "StorageGRID 드라이브 암호화를 설정하고 구성합니다".
- SED, FDE 또는 FIPS 드라이브가 없는 어플라이언스의 경우 StorageGRID 소프트웨어 노드 암호화를 활성화하고 구성합니다 "KMS(키 관리 서버) 사용".

TLS 및 SSH에 대한 강화 지침

설치 중에 생성된 기본 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 액세스를 위한 자체 서명된 디지털 인증서가 정보 보안 정책을 준수하지 않습니다. 프로덕션 시스템에서는 StorageGRID 인증에 사용할 CA 서명 디지털 인증서를 설치해야 합니다.

특히 다음과 같은 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 및 Swift API 인증서 *: S3 및 Swift 클라이언트 애플리케이션이 오브젝트 데이터를 업로드 및 다운로드하는 데 사용하는 스토리지 노드 및 게이트웨이 노드에 대한 액세스를 보호하는 데 사용됩니다.

을 참조하십시오 "보안 인증서를 관리합니다" 자세한 내용 및 지침은 을 참조하십시오.

> StorageGRID는 로드 밸런서 끝점에 사용되는 인증서를 별도로 관리합니다. 로드 밸런서 인증서를 구성하려면 를 참조하십시오 "로드 밸런서 엔드포인트를 구성합니다".

사용자 지정 서버 인증서를 사용하는 경우 다음 지침을 따르십시오.

- 인증서에 가 있어야 합니다 *subjectAltName* StorageGRID의 DNS 항목과 일치합니다. 자세한 내용은 의 4.2.1.6절 "주체 대체 이름"을 참조하십시오 "RFC 5280: PKIX 인증서 및 CRL 프로필".
- 가능한 경우 와일드카드 인증서를 사용하지 마십시오. 이 지침의 예외는 S3 가상 호스팅 스타일 엔드포인트에 대한 인증서이며, 버킷 이름을 미리 모르는 경우 와일드카드를 사용해야 합니다.
- 인증서에 와일드카드를 사용해야 하는 경우 위험을 줄이기 위해 추가 단계를 수행해야 합니다. 과 같은 와일드카드 패턴을 사용합니다 `*.s3.example.com`를 사용하지 마십시오 `s3.example.com` 기타 응용 프로그램용 접미사. 이 패턴은 과 같은 경로 스타일 S3 액세스에서도 사용할 수 있습니다 `dc1-s1.s3.example.com/mybucket`.
- 인증서 만료 시간을 짧게(예: 2개월) 설정하고 그리드 관리 API를 사용하여 인증서 회전을 자동화합니다. 이것은 와일드카드 인증서에 특히 중요합니다.

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

TLS 및 SSH 정책 강화 지침

보안 정책을 선택하여 클라이언트 응용 프로그램과 보안 TLS 연결을 설정하고 내부 StorageGRID 서비스에 대한 SSH 연결을 보안하는 데 사용되는 프로토콜과 암호를 결정할 수 있습니다.

보안 정책은 TLS 및 SSH가 이동 중인 데이터를 암호화하는 방법을 제어합니다. 가장 좋은 방법은 응용 프로그램 호환성에 필요하지 않은 암호화 옵션을 비활성화하는 것입니다. 시스템이 공통 기준 호환이거나 다른 암호를 사용해야 하는 경우가 아니면 기본 최신 정책을 사용합니다.

을 참조하십시오 "TLS 및 SSH 정책을 관리합니다" 자세한 내용 및 지침은 을 참조하십시오.

기타 강화 지침

StorageGRID 네트워크 및 노드에 대한 강화 지침을 따르는 것 외에도 StorageGRID 시스템의 다른 영역에 대한 강화 지침을 따라야 합니다.

로그 및 감사 메시지

항상 안전한 방법으로 StorageGRID 로그 및 감사 메시지 출력을 보호합니다. StorageGRID 로그 및 감사 메시지는 지원 및 시스템 가용성의 관점에서 중요한 정보를 제공합니다. 또한 StorageGRID 로그 및 감사 메시지 출력에 포함된 정보와 세부 정보는 일반적으로 민감한 특성을 가지고 있습니다.

보안 이벤트를 외부 syslog 서버로 보내도록 StorageGRID를 구성합니다. syslog 내보내기를 사용하는 경우 전송 프로토콜에 대해 TLS 및 RELP/TLS를 선택합니다.

를 참조하십시오 "로그 파일 참조" StorageGRID 로그에 대한 자세한 내용은 를 참조하십시오. 을 참조하십시오 "감사 메시지" StorageGRID 감사 메시지에 대한 자세한 내용은

NetApp AutoSupport를 참조하십시오

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

AutoSupport 기능을 비활성화할 수 있습니다. 하지만 AutoSupport는 StorageGRID 시스템에서 문제가 발생할 경우 문제를 빠르게 식별하고 해결할 수 있도록 하므로 NetApp에서 이 기능을 사용하도록 권장합니다.

AutoSupport는 전송 프로토콜을 위해 HTTPS, HTTP 및 SMTP를 지원합니다. AutoSupport 패키지는 매우 민감하므로 NetApp에서 AutoSupport 패키지를 NetApp에 전송하기 위한 기본 전송 프로토콜로 HTTPS를 사용하는 것이 좋습니다.

CORS(Cross-Origin Resource Sharing)

다른 도메인의 웹 애플리케이션에서 해당 버킷의 버킷 및 오브젝트에 액세스할 수 있도록 하려면 S3 버킷에 대해 CORS(Cross-Origin Resource Sharing)를 구성할 수 있습니다. 일반적으로 CORS가 필요한 경우가 아니면 활성화하지 마십시오. CORS가 필요한 경우 신뢰할 수 있는 오리진으로 제한합니다.

의 단계를 참조하십시오 "CORS(Cross-Origin Resource Sharing) 구성".

외부 보안 장치

완벽한 강화 솔루션은 StorageGRID 외부의 보안 메커니즘을 해결해야 합니다. StorageGRID에 대한 액세스를 필터링하고 제한하는 데 추가 인프라 장치를 사용하는 것은 엄격한 보안 상태를 설정하고 유지하는 효과적인 방법입니다. 이러한 외부 보안 장치에는 방화벽, IPS(침입 방지 시스템) 및 기타 보안 장치가 포함됩니다.

신뢰할 수 없는 클라이언트 트래픽에는 타사 로드 밸런서가 권장됩니다. 타사 로드 밸런싱은 더 많은 제어 기능과 공격에 대한 추가적인 보호 계층을 제공합니다.

랜섬웨어 완화

의 권장 사항을 따르면 랜섬웨어 공격으로부터 오브젝트 데이터를 보호할 수 있습니다 "StorageGRID를 통한 랜섬웨어 방어".