TR-4645: 보안 기능

How to enable StorageGRID in your environment

NetApp
July 05, 2024

목차

TR-4645: 보안 기능

오브젝트 저장소에서 StorageGRID 데이터와 메타데이터의 보안 유지

StorageGRID 오브젝트 스토리지 솔루션의 핵심 보안 기능에 대해 알아보십시오.

데이터 액세스, 개체 및 메타데이터, 관리 액세스, 플랫폼 보안을 다루는 NetApp ® StorageGRID ® 의 다양한 보안 기능에 대한 개요입니다. StorageGRID 11.8과 함께 릴리즈된 최신 기능을 포함하도록 업데이트되었습니다.

보안은 NetApp StorageGRID 오브젝트 스토리지 솔루션의 핵심 부분입니다. 오브젝트 스토리지에 적합한 다양한 유형의 다양한 콘텐츠 데이터 또한 본질적으로 민감하고 규정 및 규정 준수를 충족해야 하기 때문에 보안은 특히 중요합니다. StorageGRID의 기능이 계속해서 발전함에 따라 소프트웨어는 조직의 보안 입지를 보호하고 조직이 업계 모범 사례를 준수하도록 지원하는 데 매우 중요한 여러 보안 기능을 사용할 수 있습니다.

이 문서에서는 StorageGRID 11.8의 다양한 보안 기능에 대해 다음과 같은 다섯 가지 범주로 나뉩니다.

- 데이터 액세스 보안 기능
- 오브젝트 및 메타데이터 보안 기능
- 관리 보안 기능
- 플랫폼 보안 기능
- 클라우드 통합

이 문서는 보안 데이터시트로 작성되었으며 기본적으로 구성되지 않은 내에서 열거된 보안 기능을 지원하도록 시스템을 구성하는 방법에 대해서는 자세히 설명하지 않습니다. 는 "StorageGRID 강화 가이드 를 참조하십시오" 공식 페이지에서 사용할 수 "StorageGRID 설명서" 있습니다.

이 보고서에 설명된 기능 외에도 StorageGRID는 를 "NetApp 제품 보안 취약성 대응 및 알림 정책"따릅니다. 보고된 취약성은 제품 보안 사고 대응 프로세스에 따라 확인 및 대응됩니다.

NetApp StorageGRID는 매우 까다로운 엔터프라이즈 오브젝트 스토리지 사용 사례를 위한 고급 보안 기능을 제공합니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- NetApp StorageGRID: SEC 17a-4(f), FINRA 4511(c) 및 CFTC 1.31(c)-(d) 준수 평가 https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- StorageGRID 11.8 설명서 페이지 https://docs.netapp.com/us-en/storagegrid-118/
- StorageGRID 문서 리소스 페이지 https://www.netapp.com/data-storage/storagegrid/documentation/
- NetApp 제품 설명서 https://www.netapp.com/support-and-training/documentation/

용어 및 약어

이 섹션에서는 문서에 사용된 용어에 대한 정의를 제공합니다.

용어 또는 약어	정의
S3를 참조하십시오	간단한 스토리지 서비스.
클라이언트	데이터 액세스를 위한 S3 프로토콜 또는 관리를 위한 HTTP 프로토콜을 통해 StorageGRID와 인터페이스할 수 있는 애플리케이션.
테넌트 관리자	StorageGRID 테넌트 계정의 관리자입니다
테넌트 사용자입니다	StorageGRID 테넌트 계정 내의 사용자입니다
TLS	전송 계층 보안
ILM을 참조하십시오	정보 수명 주기 관리
LAN을 선택합니다	LAN(Local Area Network)을 선택합니다
그리드 관리자	StorageGRID 시스템의 관리자입니다
그리드	StorageGRID 시스템
버킷	S3에 저장된 오브젝트의 컨테이너입니다
LDAP를 지원합니다	Lightweight Directory Access Protocol의 약어입니다
초	증권거래위원회; 교환원, 중개인 또는 딜러를 규제합니다
FINRA/핀라	금융 업계 규제 당국. SEC Rule 17a-4(f)의 형식 및 미디어 요구 사항을 준수합니다.
CFTC의 약어입니다	상품 선물 거래 위원회; 상품 선물 거래를 규제합니다
NIST	미국 표준 기술 연구소

데이터 액세스 보안 기능

StorageGRID의 데이터 액세스 보안 기능에 대해 알아보십시오.

피처	기능	영향	규정 준수
구성 가능한 TLS(Transport Layer Security)	TLS는 클라이언트와 StorageGRID 게이트웨이 노드, 스토리지 노드 또는 로드 밸런서 끝점 간의 통신을 위한 핸드셰이크 프로토콜을 설정합니다. StorageGRID는 TLS에 대해 다음 암호화 제품군을 지원합니다. • TLS_AES_256_GCM_SHA384를 참조하십시오 • TLS_AES_128_GCM_SHA256를 참조하십시오 • ECDHE-ECDSA-AES256-GCM-SHA384를 참조하십시오 • ECDHE-RSA-AES256-GCM-SHA384를 참조하십시오 • ECDHE-ECDSA-AES128-GCM-SHA256를 참조하십시오 • ECDHE-RSA-AES128-GCM-SHA256를 참조하십시오 • TLS_AES_256_GCM_SHA384를 참조하십시오 • DHE-RSA-AES128-GCM-SHA256를 참조하십시오 • DHE-RSA-AES256-GCM-SHA384를 참조하십시오 • AES256-GCM-SHA384를 참조하십시오 • AES128-GCM-SHA256를 참조하십시오 • TLS_CHACHA20_POLY1305_SHA256를 참조하십시오 • ECDHE-ECDSA-CHACHA20-POLY1305를 참조하십시오 • ECDHE-RSA-CHACHA20-POLY1305를 참조하십시오 TLS v1.2 및 1.3이 지원됩니다. SSLv3, TLS v1.1 및 이전 버전은 더 이상 지원되지 않습니다.	클라이언트와 StorageGRID가 서로를 식별 및 인증하고 기밀성 및 데이터 무결성을 유지할 수 있도록 합니다. 최신 TLS 버전 사용을 보장합니다. 이제 구성 /보안 설정에서 암호를 구성할 수 있습니다	—

피처	기능	영향	규정 준수
구성 가능한 서버 인증서(로드 밸런서 끝점)	그리드 관리자는 서버 인증서를 생성하거나 사용하도록 부하 분산 엔드포인트를 구성할 수 있습니다.	표준 CA(신뢰할 수 있는 인증 기관)에서 서명한 디지털 인증서를 사용하여 로드 밸런서 엔드포인트별 그리드와 클라이언트 간 개체 API 작업을 인증할 수 있습니다.	—
구성 가능한 서버 인증서(API 끝점)	그리드 관리자는 조직의 신뢰할 수 있는 CA에서 서명한 서버 인증서를 사용하도록 모든 StorageGRID API 끝점을 중앙에서 구성할 수 있습니다.	신뢰할 수 있는 표준 CA에서 서명한 디지털 인증서를 사용하여 클라이언트와 그리드 간의 개체 API 작업을 인증할 수 있습니다.	—
멀티 테넌시	StorageGRID는 그리드당 여러 테넌트를 지원하며 각 테넌트에는 자체 네임스페이스가 있습니다. 테넌트는 S3 프로토콜을 제공합니다. 기본적으로 버킷/컨테이너 및 오브젝트에 대한 액세스가 계정 내의 사용자로 제한됩니다. 테넌트는 한 명의 사용자(예: 각 사용자가 자신의 계정을 가지고 있는 엔터프라이즈 배포) 또는 여러 사용자(예: 각 계정이 회사 및 서비스 공급자의 고객인 서비스 공급자 구축)를 가질 수 있습니다. 사용자는 로컬 또는 페더레이션될 수 있으며 페더레이션 사용자는 Active Directory 또는 LDAP(Lightweight Directory Access Protocol)로 정의됩니다. StorageGRID는 사용자가 로컬 또는 페더레이션 계정 자격 증명을 사용하여 로그인할 수 있는 테넌트별 대시보드를 제공합니다. 사용자는 데이터 및 버킷에 의해 저장된 개체의 사용 정보를 포함하여 그리드 관리자가 할당한 할당량에 대해 테넌트 사용량에 대한 시각화 보고서에 액세스할 수 있습니다. 관리 권한이 있는 사용자는 사용자, 그룹 및 액세스 키 관리와 같은 테넌트 수준 시스템 관리 작업을 수행할 수 있습니다.	StorageGRID 관리자는 테넌트 액세스를 격리하면서 여러 테넌트의 데이터를 호스팅할 수 있으며, Active Directory 또는 LDAP와 같은 외부 ID 공급자와 사용자를 연합하여 사용자 ID를 설정할 수 있습니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
액세스 자격 증명 거부 안 함	모든 S3 작업은 고유한 테넌트 계정, 사용자 및 액세스 키로 식별되고 기록됩니다.	그리드 관리자가 어떤 API 작업이 어떤 개인에 의해 수행되는지 설정할 수 있습니다.	—

피처	기능	영향	규정 준수
익명 액세스를 사용할 수 없습니다	기본적으로 S3 계정에 대해서는 익명 액세스가 비활성화됩니다. 요청자는 테넌트 계정의 유효한 사용자에 대한 유효한 액세스 자격 증명이 있어야 계정 내의 버킷, 컨테이너 또는 개체에 액세스할 수 있습니다. 명시적 IAM 정책을 통해 S3 버킷 또는 오브젝트에 대한 익명 액세스를 활성화할 수 있습니다.	그리드 관리자가 버킷/컨테이너 및 객체에 대한 익명 액세스를 비활성화하거나 제어할 수 있습니다.	—
규정 준수 WORM	SEC Rule 17a-4(f)의 요구 사항을 충족하도록 설계되었으며 Cohasset에 의해 검증되었습니다. 고객은 버킷 수준의 규정 준수를 지원할 수 있습니다. 보존은 연장할 수 있지만 줄일 수는 없습니다. 정보 수명 주기 관리(ILM) 규칙은 최소 데이터 보호 수준을 적용합니다.	규정 데이터 보존 요구사항이 있는 테넌트에서 저장된 오브젝트 및 오브젝트 메타데이터에 대해 WORM 보호를 지원할 수 있습니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
웜	그리드 관리자는 클라이언트 수정 비활성화 옵션을 활성화하여 그리드 전체에서 WORM을 설정할 수 있습니다. 이렇게 하면 클라이언트가 모든 테넌트 계정에서 객체 또는 객체 메타데이터를 덮어쓰거나 삭제하지 못하게 됩니다. S3 테넌트 관리자는 IAM 정책을 지정하여 오브젝트 및 메타데이터 덮어쓰기에 대한 사용자 지정 S3:PutOverwriteObject 권한이 포함된 테넌트, 버킷 또는 오브젝트 접두사로 WORM을 활성화할 수도 있습니다.	그리드 관리자 및 테넌트 관리자가 저장된 오브젝트 및 오브젝트 메타데이터에 대한 WORM 보호를 제어할 수 있도록 합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)

피처	기능	영향	규정 준수
KMS 호스트 서버 암호화 키 관리	그리드 관리자는 그리드 관리자에서 하나 이상의 외부 키 관리 서버(KMS)를 구성하여 StorageGRID 서비스 및 스토리지 어플라이언스에 암호화 키를 제공할 수 있습니다. 각 KMS 호스트 서버 또는 KMS 호스트 서버 클러스터는 KMIP(Key Management Interoperability Protocol)를 사용하여 관련 StorageGRID 사이트의 어플라이언스 노드에 암호화 키를 제공합니다.	유휴 데이터 암호화를 달성합니다. 어플라이언스 볼륨이 암호화된 후에는 노드가 KMS 호스트 서버와 통신할 수 없는 한 어플라이언스의 모든 데이터에 액세스할 수 없습니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
구현할 수 있습니다	StorageGRID는 내장 이중화 및 자동 페일오버 기능을 제공합니다. 디스크 또는 노드에서 전체 사이트에 이르기까지 여러 번의 장애가 발생하더라도 테넌트 계정, 버킷 및 오브젝트에 계속 액세스할 수 있습니다. StorageGRID는 리소스를 인식하며 요청을 가용 노드 및 데이터 위치로 자동으로 리디렉션합니다. StorageGRID 사이트는 island 모드에서도 작동할 수 있습니다. WAN 중단 시 사이트의 나머지 시스템 연결이 끊어지면 로컬 리소스를 사용하여 읽기 및 쓰기를 계속할 수 있으며 WAN이 복구될 때 복제가 자동으로 재개됩니다.	그리드 관리자는 가동 시간, SLA 및 기타 계약상의 의무를 해결하고 비즈니스 연속성 계획을 구현할 수 있습니다.	—
• S3 전용 데이터 액세스 보안 기능 *	AWS 서명 버전 2 및 버전 4	API 요청 서명은 S3 API 작업에 대한 인증을 제공합니다. 아마존은 두 가지 버전의 서명 버전 2와 버전 4를 지원합니다. 서명 프로세스는 요청자의 신원을 확인하고 전송 중인 데이터를 보호하며 잠재적인 재생 공격을 방지합니다.	Signature Version 4에 대한 AWS 권장 사항과 일치하며 Signature Version 2의 이전 버전과의 호환성을 지원합니다.
—	S3 오브젝트 잠금	StorageGRID의 S3 오브젝트 잠금 기능은 Amazon S3의 S3 오브젝트 잠금에 상응하는 오브젝트 보호 솔루션입니다.	테넌트가 S3 오브젝트 잠금이 설정된 상태에서 버킷을 생성하여 특정 오브젝트를 일정 시간 동안 또는 무기한으로 보존해야 하는 규정을 준수할 수 있습니다.

피처	기능	영향	규정 준수
SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)	S3 자격 증명의 안전한 스토리지	S3 액세스 키는 SHA-2(암호 해싱 기능)로 보호되는 형식으로 저장됩니다.	키 길이(10도 31의 임의 생성 번호)와 암호 해시 알고리즘을 조합하여 액세스 키를 안전하게 저장할 수 있습니다.
—	시간이 제한된 S3 액세스 키	사용자에 대한 S3 액세스 키를 생성할 때 고객은 액세스 키에서 만료 날짜 및 시간을 설정할 수 있습니다.	그리드 관리자가 임시 S3 액세스 키를 프로비저닝할 수 있는 옵션을 제공합니다.
—	사용자 계정당 여러 개의 액세스 키	StorageGRID를 사용하면 사용자 계정에 대해 여러 개의 액세스 키를 생성하고 동시에 활성화할 수 있습니다. 각 API 작업은 테넌트 사용자 계정 및 액세스 키로 기록되므로 여러 키가 활성 상태에서도 거부 안 됨(Nonrepudiation)이 유지됩니다.	클라이언트가 액세스 키를 중단 없이 회전할 수 있도록 하며 각 클라이언트가 자체 키를 가질 수 있도록 하여 클라이언트 간에 키를 공유하지 않도록 합니다.
—	S3 IAM 액세스 정책	StorageGRID는 S3 IAM 정책을 지원하므로 그리드 관리자가 테넌트, 버킷 또는 오브젝트 접두사를 기준으로 세분화된 액세스 제어를 지정할 수 있습니다. 또한 StorageGRID는 IAM 정책 조건 및 변수를 지원하여 보다 동적인 액세스 제어 정책을 지원합니다.	그리드 관리자가 전체 테넌트에 대해 사용자 그룹별로 액세스 제어를 지정할 수 있도록 허용하며, 테넌트 사용자가 자신의 버킷 및 객체에 대한 액세스 제어를 지정할 수도 있습니다.
—	StorageGRID에서 관리하는 키(SSE)를 사용한 서버측 암호화	StorageGRID는 SSE를 지원하므로 StorageGRID에서 관리하는 암호화 키로 유휴 데이터의 멀티 테넌트 보호가 가능합니다.	테넌트가 오브젝트를 암호화할 수 있도록 합니다. 이러한 개체를 쓰고 검색하려면 암호화 키가 필요합니다.
SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)	고객이 제공한 암호화 키(SSE-C)를 사용한 서버측 암호화	StorageGRID는 SSE-C를 지원하여 클라이언트가 관리하는 암호화 키를 사용하여 저장된 데이터를 멀티 테넌트(Multi-tenant) 보호할 수 있습니다. StorageGRID가 모든 개체 암호화 및 암호 해독 작업을 관리하지만 SSE-C를 사용하여 클라이언트는 암호화 키 자체를 관리해야 합니다.	클라이언트가 제어하는 키를 사용하여 개체를 암호화할 수 있습니다. 이러한 개체를 쓰고 검색하려면 암호화 키가 필요합니다.

오브젝트 및 메타데이터 보안

StorageGRID의 개체 및 메타데이터 보안 기능을 살펴봅니다.

피처	기능	영향	규정 준수
AES(Advanced Encryption Standard) 서버측 개체 암호화	StorageGRID는 AES 128 및 AES 256 기반의 서버측 오브젝트 암호화를 제공합니다. 그리드 관리자는 암호화를 전역 기본 설정으로 활성화할 수 있습니다. 또한 StorageGRID는 S3 x-amz-server-side 암호화 헤더를 지원하여 오브젝트별로 암호화를 활성화하거나 비활성화할 수 있습니다. 이 기능을 활성화하면 저장 또는 그리드 노드 간에 전송 중인 객체가 암호화됩니다.	기본 스토리지 하드웨어에 관계없이 안전하게 개체를 저장하고 전송할 수 있습니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
내장된 키 관리	암호화가 활성화되면 각 오브젝트가 무작위로 생성된 고유 대칭 키로 암호화되며 외부 액세스 없이 StorageGRID 내에 저장됩니다.	외부 키 관리 없이도 개체 암호화 가능	
FIPS(Federal Information Processing Standard) 140-2 준수 암호화 디스크	SG5712, SG5760, SG6060 및 SGF6024 StorageGRID 어플라이언스는 FIPS 140-2 준수 암호화 디스크의 옵션을 제공합니다. 선택적으로 외부 KMIP 서버를 통해 디스크의 암호화 키를 관리할 수 있습니다.	시스템 데이터, 메타데이터 및 오브젝트의 안전한 스토리지 지원 또한 StorageGRID 소프트웨어 기반 오브젝트 암호화를 제공하여 오브젝트의 저장 및 전송을 보호합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
백그라운드 무결성 검사 및 자가 복구	StorageGRID는 오브젝트 및 하위 오브젝트 수준에서 해시, 체크섬, 순환 중복 검사(CRC)의 인터잠금 메커니즘을 사용하여 오브젝트가 스토리지에 있을 때와 전송 중일 때 데이터 비일관성, 변조 또는 수정으로부터 보호합니다. StorageGRID는 손상되거나 무단 변경된 오브젝트를 자동으로 감지하여 교체하는 한편, 변경된 데이터를 격리하고 관리자에게 경고합니다.	그리드 관리자는 데이터 내구성과 관련된 SLA, 규정 및 기타 의무를 충족할 수 있습니다. 고객이 데이터를 암호화, 변조 또는 수정하려는 랜섬웨어 또는 바이러스를 감지하는 데 도움이 됩니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)

피처	기능	영향	규정 준수
정책 기반 오브젝트 배치 및 보존	StorageGRID를 통해 그리드 관리자는 객체 보존, 배치, 보호, 전환 및 만료가 지정된 ILM 규칙을 구성할 수 있습니다. 그리드 관리자는 StorageGRID 메타데이터로 오브젝트를 필터링하고 그리드 전체, 테넌트, 버킷, 키 접두사, 및 사용자 정의 메타데이터 키-값 쌍 StorageGRID는 클라이언트에서 명시적으로 삭제하지 않는 한, 라이프사이클 전반에서 ILM 규칙에 따라 오브젝트를 저장할 수 있도록 도와줍니다.	데이터 배치, 보호 및 보존을 적용할 수 있도록 지원 고객이 내구성, 가용성, 성능에 대한 SLA를 달성할 수 있도록 지원합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
백그라운드 메타데이터 검사	StorageGRID은 주기적으로 백그라운드에서 오브젝트 메타데이터를 검사하여 ILM에서 지정한 대로 오브젝트 데이터 배치 또는 보호 변경 사항을 적용합니다.	손상된 개체를 찾는 데 도움이 됩니다.	
일관성 조정 가능	테넌트는 버킷 수준의 일관성 수준을 선택하여 다중 사이트 연결과 같은 리소스를 사용할 수 있도록 할 수 있습니다.	필요한 수의 사이트 또는 리소스를 사용할 수 있는 경우에만 그리드에 쓰기를 커밋하는 옵션을 제공합니다.	

관리 보안 기능

StorageGRID의 관리 보안 기능에 대해 알아봅니다.

피처	기능	영향	규정 준수
서버 인증서(그리드 관리 인터페이스)	그리드 관리자는 조직의 신뢰할 수 있는 CA에서 서명한 서버 인증서를 사용하도록 그리드 관리 인터페이스를 구성할 수 있습니다.	신뢰할 수 있는 표준 CA에서 서명한 디지털 인증서를 사용하여 관리 클라이언트와 그리드 간의 관리 UI 및 API 액세스를 인증할 수 있습니다.	—

피처	기능	영향	규정 준수
관리 사용자 인증	관리 사용자는 사용자 이름과 암호를 사용하여 인증됩니다. 관리 사용자 및 그룹은 로컬 또는 페더레이션될 수 있으며 고객의 Active Directory 또는 LDAP에서 가져올 수 있습니다. 로컬 계정 암호는 bcrypt로 보호되는 형식으로 저장되고 명령줄 암호는 SHA-2로 보호되는 형식으로 저장됩니다.	관리 UI 및 API에 대한 관리 액세스를 인증합니다.	—
SAML 지원	StorageGRID는 SAML 2.0(Security Assertion Markup Language 2.0) 표준을 사용하는 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.	SSO 및 다단계 인증(MFA)과 같은 그리드 및 테넌트 관리자를 위한 추가 보안 수준 지원	NIST SP800-63 를 참조하십시오
세분화된 권한 제어	그리드 관리자는 역할에 권한을 할당하고 관리 사용자 그룹에 역할을 할당할 수 있습니다. 그러면 관리 UI와 API를 모두 사용하여 관리 클라이언트가 수행할 수 있는 작업이 적용됩니다.	그리드 관리자가 관리자 및 그룹에 대한 액세스 제어를 관리할 수 있습니다.	—

피처	기능	영향	규정 준수
분산 감사 로깅	StorageGRID는 최대 16개 사이트에서 수백 개의 노드로 확장할 수 있는 분산형 감사 로깅 인프라를 내장하고 있습니다. StorageGRID 소프트웨어 노드는 중복 감사 릴레이 시스템을 통해 전송되어 하나 이상의 감사 로그 저장소에 캡처되는 감사 메시지를 생성합니다. 감사 메시지는 클라이언트 실행형 S3 API 작업, ILM을 통한 오브젝트 라이프사이클 이벤트, 백그라운드 오브젝트 상태 점검, 관리 UI 또는 API를 통한 구성 변경 등과 같이 오브젝트 레벨에서 세분화된 이벤트를 캡처합니다. 감사 로그를 CIFS 또는 NFS를 통해 관리 노드에서 내보낼 수 있으므로 Splunk 및 elk와 같은 툴을 통해 감사 메시지를 마이닝할 수 있습니다. 감사 메시지에는 네 가지 유형이 있습니다. • 시스템 감사 메시지 • 오브젝트 스토리지 감사 메시지 • HTTP 프로토콜 감사 메시지 • 관리 감사 메시지	그리드 관리자는 검증되고 확장 가능한 감사 서비스를 제공하며 다양한 목표에 대한 감사 데이터를 마이닝할 수 있습니다. 이러한 목표에는 문제 해결, SLA 성능 감사, 클라이언트 데이터 액세스 API 작업, 관리 구성 변경 등이 포함됩니다.	—
시스템 감사	시스템 감사 메시지는 그리드 노드 상태, 손상된 개체 감지, ILM 규칙에 따라 지정된 모든 위치에 커밋된 개체, 시스템 차원의 유지 관리 작업(그리드 작업)의 진행률과 같은 시스템 관련 이벤트를 캡처합니다.	고객이 시스템 문제를 해결하도록 지원하고 SLA에 따라 개체가 저장된다는 증거를 제공합니다. SLA는 StorageGRID ILM 규칙을 통해 구현되며 무결성이 보호됩니다.	—
오브젝트 스토리지 감사	오브젝트 스토리지 감사 메시지는 오브젝트 API 트랜잭션 및 라이프사이클 관련 이벤트를 캡처합니다. 이러한 이벤트에는 오브젝트 스토리지 및 검색, 그리드 노드에서 그리드 노드로 전송 및 검증이 포함됩니다.	고객이 시스템을 통해 데이터의 진행 상황과 StorageGRID ILM으로 지정된 SLA 제공 여부를 감사하는 데 도움이 됩니다.	—

피처	기능	영향	규정 준수
HTTP 프로토콜 감사	HTTP 프로토콜 감사 메시지는 클라이언트 응용 프로그램 및 StorageGRID 노드와 관련된 HTTP 프로토콜 상호 작용을 캡처합니다. 또한 고객은 특정 HTTP 요청 헤더(예: X-Forwarded-For 및 사용자 메타데이터[x-amz-meta- *])를 감사에 캡처할 수 있습니다.	고객이 클라이언트와 StorageGRID 간의 데이터 액세스 API 작업을 감사하고 개별 사용자 계정 및 액세스 키에 대한 작업을 추적할 수 있도록 도와줍니다. 또한 고객은 사용자 메타데이터를 감사에 로그인하고 Splunk 또는 elk와 같은 로그 마이닝 툴을 사용하여 오브젝트 메타데이터를 검색할 수 있습니다.	—
관리 감사	관리 감사 메시지는 관리 UI(그리드 관리 인터페이스) 또는 API에 관리자 사용자 요청을 기록합니다. API에 대한 GET 또는 HEAD 요청이 아닌 모든 요청은 API에 대한 사용자 이름, IP 및 요청 유형을 사용하여 응답을 기록합니다.	그리드 관리자가 소스 IP와 대상 IP를 어느 시점에 어느 사용자가 변경했는지에 대한 시스템 구성 변경 기록을 설정할 수 있도록 도와줍니다.	—
관리 UI 및 API 액세스를 위한 TLS 1.3 지원	TLS는 관리 클라이언트와 StorageGRID 관리 노드 간의 통신을 위한 핸드셰이크 프로토콜을 설정합니다.	관리 클라이언트와 StorageGRID가 서로 식별 및 인증하고 기밀성 및 데이터 무결성을 유지할 수 있도록 합니다.	—
StorageGRID 모니터링용 SNMPv3	SNMPv3는 개인 정보 보호를 위해 강력한 인증 및 데이터 암호화를 제공하여 보안을 제공합니다. v3에서는 암호화 프로토콜에 CBC-DES를 사용하여 프로토콜 데이터 유닛이 암호화됩니다. 프로토콜 데이터 단위를 보낸 사람의 사용자 인증은 HMAC-SHA 또는 HMAC-MD5 인증 프로토콜을 통해 제공됩니다. SNMPv2 및 v1은 계속 지원됩니다.	그리드 관리자가 관리자 노드에서 SNMP 에이전트를 활성화하여 StorageGRID 시스템을 모니터링할 수 있도록 합니다.	—
Prometheus 메트릭스 내보내기용 클라이언트 인증서	그리드 관리자는 StorageGRID Prometheus 데이터베이스에 대한 안전하고 인증된 액세스를 제공하는 데 사용할 수 있는 클라이언트 인증서를 업로드하거나 생성할 수 있습니다.	그리드 관리자는 클라이언트 인증서를 사용하여 Grafana와 같은 애플리케이션을 사용하여 외부에서 StorageGRID를 모니터링할 수 있습니다.	—

플랫폼 보안 기능

StorageGRID의 플랫폼 보안 기능에 대해 알아봅니다.

피처	기능	영향	규정 준수
내부 PKI(공개 키 인프라), 노드 인증서 및 TLS	StorageGRID는 내부 PKI 및 노드 인증서를 사용하여 노드 간 통신을 인증하고 암호화합니다. 노드 간 통신은 TLS에 의해 보호됩니다.	LAN 또는 WAN을 통한 시스템 트래픽 보안, 특히 다중 사이트 구축 시 유용합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
노드 방화벽	StorageGRID는 IP 테이블 및 방화벽 규칙을 자동으로 구성하여 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 제어하고 사용되지 않는 포트를 닫습니다.	StorageGRID 시스템, 데이터 및 메타데이터를 원치 않는 네트워크 트래픽으로부터 보호합니다.	—
OS 강화	StorageGRID 물리적 어플라이언스 및 가상 노드의 기본 운영 체제가 강화되며 관련 없는 소프트웨어 패키지가 제거됩니다.	잠재적인 공격 대상을 최소화합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
주기적인 플랫폼 및 소프트웨어 업데이트	StorageGRID는 운영 체제, 응용 프로그램 바이너리 및 소프트웨어 업데이트를 포함하는 정기적인 소프트웨어 릴리즈를 제공합니다.	StorageGRID 시스템을 최신 소프트웨어 및 응용 프로그램 바이너리로 업데이트하는 데 도움이 됩니다.	—
SSH(Secure Shell)를 통한 루트 로그인 비활성화	모든 StorageGRID 노드에서 SSH를 통한 루트 로그인이 비활성화됩니다. SSH 액세스에서는 인증서 인증을 사용합니다.	고객이 루트 로그인의 잠재적인 원격 암호 크래킹으로부터 보호할 수 있습니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
자동 시간 동기화	StorageGRID는 여러 외부 시간 네트워크 시간 프로토콜(NTP) 서버에 대해 각 노드의 시스템 클록을 자동으로 동기화합니다. Stratum 3 이상의 NTP 서버가 4개 이상 필요합니다.	모든 노드에서 동일한 시간 참조를 보장합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
클라이언트, 관리자 및 내부 그리드 트래픽을 위한 별도의 네트워크	StorageGRID 소프트웨어 노드 및 하드웨어 어플라이언스는 여러 가상 및 물리적 네트워크 인터페이스를 지원하므로 고객이 여러 네트워크에서 클라이언트, 관리 및 내부 그리드 트래픽을 분리할 수 있습니다.	그리드 관리자는 내부 및 외부 네트워크 트래픽을 분리하고 서로 다른 SLA를 가진 네트워크를 통해 트래픽을 전달할 수 있습니다.	—

피처	기능	영향	규정 준수
다중 VLAN(Virtual LAN) 인터페이스	StorageGRID는 StorageGRID 클라이언트 및 그리드 네트워크에서 VLAN 인터페이스 구성을 지원합니다.	그리드 관리자는 보안, 유연성 및 성능을 위해 애플리케이션 트래픽을 분할하고 격리할 수 있습니다.	
신뢰할 수 없는 클라이언트 네트워크	신뢰할 수 없는 클라이언트 네트워크 인터페이스는 로드 밸런서 끝점으로 명시적으로 구성된 포트에 대해서만 인바운드 연결을 허용합니다.	신뢰할 수 없는 네트워크에 노출된 인터페이스의 보안을 보장합니다.	—
구성 가능한 방화벽	관리, 그리드 및 클라이언트 네트워크에 대한 열린 포트 및 닫힌 포트를 관리합니다.	그리드 관리자가 포트에 대한 액세스를 제어하고 포트에 대한 승인된 장치 액세스를 관리할 수 있습니다.	
향상된 SSH 동작	노드를 StorageGRID 11.5로 업그레이드할 때 새로운 SSH 호스트 인증서 및 호스트 키가 생성됩니다.	중간자 공격 보호 기능을 강화합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)
노드 암호화	새로운 KMS 호스트 서버 암호화 기능의 일부로 새로운 노드 암호화 설정이 StorageGRID 어플라이언스 설치 프로그램에 추가됩니다.	이 설정은 어플라이언스 설치의 하드웨어 구성 단계에서 활성화해야 합니다.	SEC 규정 17a-4(f) CTFC 1.31(c) -(d)(FINRA) 규칙 4511(c)

클라우드 통합

StorageGRID를 클라우드 서비스와 통합하는 방식 이해

피처	기능	영향
알림 기반 바이러스 검사	StorageGRID 플랫폼 서비스는 이벤트 알림을 지원합니다. 이벤트 알림을 외부 클라우드 컴퓨팅 서비스와 함께 사용하여 데이터에 대한 바이러스 검사 워크플로우를 트리거할 수 있습니다.	테넌트 관리자가 외부 클라우드 컴퓨팅 서비스를 사용하여 데이터의 바이러스 검사를 트리거할 수 있습니다.

저작권 정보

상표 정보