TR-4645 ：安全功能

StorageGRID solutions and resources

NetApp
December 12, 2025

目錄

TR-4645 ：安全功能

保護物件存放區中的 StorageGRID 資料和中繼資料安全

探索 StorageGRID 物件儲存解決方案的整合式安全功能。

這是NetApp® StorageGRID® 中眾多安全功能的概述，涵蓋資料存取、物件和元資料、管理存取和平台安全。它已更新，包含StorageGRID 12.0 發布的最新功能。

安全性是 NetApp StorageGRID 物件儲存解決方案不可或缺的一部分。安全性特別重要、因為許多適合物件儲存的豐富內容資料類型、本質上也很敏感、而且必須遵守法規與法規。隨著 StorageGRID 功能不斷進化、軟體提供許多安全功能、對於保護組織的安全狀態和協助組織遵循業界最佳實務實務非常寶貴。

本文概述了StorageGRID 12.0 中的眾多安全功能，分為五類：

- 資料存取安全功能
- 物件和中繼資料安全功能
- 系統管理安全功能
- 平台安全功能
- 雲端整合

本文旨在成為一份安全資料表——它沒有詳細說明如何配置系統以支援其中列舉的預設未配置的安全功能。這"StorageGRID 強化指南"可在官方 "StorageGRID 文件"頁。

除了本報告中所述的功能外， StorageGRID 還遵循 "NetApp 產品安全性弱點回應與通知原則"。報告的弱點會根據產品安全性事件回應程序進行驗證及回應。

NetApp StorageGRID 為要求嚴苛的企業物件儲存使用案例提供進階安全功能。

何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- NetApp StorageGRID ： SEC 17a-4(f) 、 FINRA 4511 （ c ）和 CFTC 1.31 （ c ） - （ d ）法規遵循評估 https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- NetApp StorageGRID NIST FIPS 140-3 核心加密認證 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5097
- NetApp StorageGRID NIST SP 800-90B 熵認證 https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/223
- NetApp StorageGRID加拿大網路安全中心通用準則認證 https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/565-LSS%20CT%20v1.0.pdf
- StorageGRID文件頁面https://docs.netapp.com/us-en/storagegrid/[]
- NetApp 產品文件 https://www.netapp.com/support-and-training/documentation/

詞彙與縮寫

本節提供文件中所用術語的定義。

術語或縮寫	定義
S3	簡易儲存服務：
用戶端	可透過 S3 傳輸協定與 StorageGRID 進行資料存取的應用程式、或是用於管理的 HTTP 傳輸協定。
租戶管理	StorageGRID 租戶帳戶的管理員
租戶使用者	StorageGRID 租戶帳戶中的使用者
TLS	傳輸層安全性
ILM	資訊生命週期管理
LAN	區域網路
網格管理員	StorageGRID 系統管理員
網格	StorageGRID 系統
鏟斗	儲存在 S3 中的物件容器
LDAP	輕量型目錄存取傳輸協定
秒	證券交易委員會；規範交易所成員、經紀商或交易商
FINRA	金融產業監管局；遵守 SEC 法規 17a-4(f) 的格式與媒體要求
CFTC	商品期貨交易佣金；規範商品期貨交易
NIST	國家標準和技術研究所

資料存取安全功能

瞭解 StorageGRID 的資料存取安全功能。

功能	功能	影響	法規遵循
可設定的傳輸層安全性（ TLS ）	TLS 會為用戶端與 StorageGRID 閘道節點、儲存節點或負載平衡器端點之間的通訊建立信號交換傳輸協定。 StorageGRID 支援下列 TLS 加密套件： • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • TLS_AES_256_GCM_SHA384 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • AES128-GCM-SHA256 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 支援 TLS v1.2 與 1.3 。 不支援 SSLv3、TLS v1.1 及更早版本。	讓用戶端和 StorageGRID 能夠識別和驗證彼此、並與機密性和資料完整性進行通訊。確保使用最新的 TLS 版本。密碼現在可在組態 / 安全性設定下進行設定	—

功能	功能	影響	法規遵循
可設定的伺服器憑證（負載平衡器端點）	網格管理員可以設定負載平衡器端點來產生或使用伺服器憑證。	可讓使用由其標準信任憑證授權單位（ CA ）簽署的數位憑證、針對每個負載平衡器端點、在網格和用戶端之間驗證物件 API 作業。	—
可設定的伺服器憑證（ API 端點）	網格管理員可以集中設定所有 StorageGRID API 端點、以使用組織信任 CA 簽署的伺服器憑證。	啟用使用由標準信任 CA 簽署的數位憑證、以驗證用戶端與網格之間的物件 API 作業。	—
多租戶	StorageGRID 每個網格都支援多個租戶、每個租戶都有自己的命名空間。租戶提供 S3 傳輸協定；根據預設、只有帳戶內的使用者才能存取貯體 / 容器和物件。租戶可以有一位使用者（例如、每位使用者都有自己的帳戶的企業部署）或多位使用者（例如、服務供應商部署、其中每個帳戶都是公司和服務供應商的客戶）。使用者可以是本機或同盟使用者；同盟使用者是由 Active Directory 或輕量型目錄存取通訊協定（ LDAP ）所定義。StorageGRID 提供個別租戶儀表板、讓使用者使用其本機或同盟帳戶認證登入。使用者可以根據網格管理員指派的配額、存取租戶使用量的視覺化報告、包括儲存於儲存區的資料和物件中的使用資訊。具有管理權限的使用者可以執行租戶層級的系統管理工作、例如管理使用者、群組和存取金鑰。	可讓 StorageGRID 管理員在隔離租戶存取的同時、託管來自多個租戶的資料、並透過與外部身分識別提供者（例如 Active Directory 或 LDAP ）聯合使用者來建立使用者身分識別。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
存取認證的不可否認性	每個 S3 作業都會以唯一的租戶帳戶、使用者和存取金鑰來識別和記錄。	允許 Grid 系統管理員建立哪些個人執行哪些 API 動作。	—
停用匿名存取	根據預設、 S3 帳戶的匿名存取已停用。要求者必須擁有有效的存取認證、才能存取帳戶中的貯體、容器或物件。可以使用明確的 IAM 原則來啟用對 S3 儲存區或物件的匿名存取。	允許 Grid 管理員停用或控制對貯體 / 容器和物件的匿名存取。	—

功能	功能	影響	法規遵循
法規遵循 WORM	專為符合 SEC 法規 17a-4(f) 的要求而設計、並由 Cohasset 驗證。客戶可以在貯體層級實現法規遵循。保留可延長、但絕不會減少。 資訊生命週期管理（ ILM ）規則可強制執行最低的資料保護層級。	允許具有法規資料保留要求的租戶、在儲存的物件和物件中繼資料上啟用 WORM 保護。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
WORM	網格管理員可啟用「停用用戶端修改」選項、以啟用全網格 WORM 、避免用戶端覆寫或刪除所有租戶帳戶中的物件或物件中繼資料。 S3 租戶管理員也可以透過指定 IAM 原則、依租戶、貯體或物件首碼來啟用 WORM 、其中包括自訂 S3 ：物件和中繼資料覆寫的 PutOverwriteObject 權限。	允許 Grid 管理員和租戶管理員控制儲存物件和物件中繼資料上的 WORM 保護。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
KMS 主機伺服器加密金鑰管理	網格管理員可以在網格管理程式中設定一或多個外部金鑰管理伺服器（ KMS ）、為 StorageGRID 服務和儲存設備提供加密金鑰。每個 KMS 主機伺服器或 KMS 主機伺服器叢集都使用金鑰管理互通性通訊協定（ KMIP ）、為相關 StorageGRID 站台的應用裝置節點提供加密金鑰。	資料靜止加密已完成。應用裝置磁碟區加密後、除非節點可以與 KMS 主機伺服器通訊、否則您無法存取應用裝置上的任何資料。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
自動容錯移轉	StorageGRID 提供內建的備援功能和自動容錯移轉功能。即使有多個故障、從磁碟或節點到整個站台、仍可繼續存取租戶帳戶、貯體和物件。StorageGRID 可識別資源、並自動將要求重新導向至可用的節點和資料位置。StorageGRID 站台甚至可以在著陸模式下運作；如果 WAN 中斷會中斷站台與系統其餘部分的連線、則讀取和寫入作業可以繼續使用本機資源、並在 WAN 恢復時自動恢復複寫作業。	讓 Grid 管理員能夠處理正常運作時間、 SLA 及其他合約義務、並實作業務持續性計畫。	—

功能	功能	影響	法規遵循
• S3 特有的資料存取安全功能 *	AWS 簽名第 2 版和第 4 版	簽署 API 要求可為 S3 API 作業提供驗證。Amazon 支援兩個版本的簽名版本 2 和版本 4 。簽署程序會驗證要求者的身分、保護傳輸中的資料、並防範可能的重播攻擊。	符合 AWS 對簽名版本 4 的建議、並可與舊版應用程式與簽名版本 2 向下相容。
—	S3物件鎖定	StorageGRID 中的 S3 物件鎖定功能是一種物件保護解決方案、相當於 Amazon S3 中的 S3 物件鎖定。	允許租戶建立啟用 S3 物件鎖定的貯體、以符合規定、要求特定物件保留一段固定時間或無限期。
SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)	S3 認證的安全儲存	S3 存取金鑰是以受密碼雜湊功能（ SHA-2 ）保護的格式儲存。	結合金鑰長度（ 10^{31} 隨機產生的數字）和密碼雜湊演算法、可安全儲存存取金鑰。
—	有時間限制的 S3 存取金鑰	為使用者建立 S3 存取金鑰時、客戶可以設定存取金鑰的到期日和時間。	讓 Grid 系統管理員可以選擇配置暫存 S3 存取金鑰。
—	每個使用者帳戶有多個存取金鑰	StorageGRID 可為使用者帳戶建立多個存取金鑰、並同時啟用多個存取金鑰。由於每個 API 動作都會以租戶使用者帳戶和存取金鑰記錄、因此即使多個金鑰處於作用中狀態、仍會保留不可否認性。	讓用戶端能夠不中斷地旋轉存取金鑰、並讓每個用戶端都擁有自己的金鑰、從而阻止用戶端之間的金鑰共用。
—	S3 IAM 存取原則	StorageGRID 支援 S3 IAM 原則、可讓 Grid 管理員依租戶、貯體或物件首碼指定精細的存取控制。StorageGRID 也支援 IAM 原則條件和變數、允許更多動態存取控制原則。	允許 Grid 系統管理員依整個租戶的使用者群組指定存取控制、也可讓租戶使用者指定自己的貯體和物件的存取控制。
—	S3 安全性令牌服務 API AssumeRole	StorageGRID支援 S3 STS API AssumeRole 提供具有縮小範圍的權限和有限持續時間的臨時安全憑證（存取金鑰 ID、秘密存取金鑰、會話令牌）。作為 AssumeRole API 的一部分，支援內嵌會話策略來進一步限制會話期間的權限。	允許租用戶管理員提供對對象資料的安全臨時存取。

功能	功能	影響	法規遵循
—	簡單通知服務	StorageGRID支援在物件存取時發送通知。支援以下事件類型： • s3：物件創建： • s3：物件創建：放置 • s3：物件創建：發布 • s3：物件創建：複製 • s3：物件創建：完成分段上傳 • s3：物件已移除： • s3：物件已移除：刪除 • s3：物件已移除：刪除標記已建立 • s3：對象恢復：發布	允許租用戶管理員監控對象的存取
—	使用 StorageGRID 託管金鑰（ SSE ）進行伺服器端加密	StorageGRID 支援 SSE 、可透過 StorageGRID 管理的加密金鑰、為靜止的資料提供多租戶保護。	可讓租戶加密物件。寫入和擷取這些物件需要加密金鑰。
SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)	使用客戶提供的加密金鑰（ SSE-C ）進行伺服器端加密	StorageGRID 支援 SSE-C 、可透過用戶端管理的加密金鑰、為靜止的資料提供多租戶保護。 雖然 StorageGRID 管理所有物件加密和解密作業、但使用 SSE-C 時、用戶端必須自行管理加密金鑰。	可讓用戶端使用其控制的金鑰來加密物件。寫入和擷取這些物件需要加密金鑰。

物件和中繼資料安全性

探索 StorageGRID 中的物件和中繼資料安全功能。

功能	功能	影響	法規遵循
進階加密標準（AES）伺服器端物件加密	StorageGRID 提供以 AES 128 和 AES 256 為基礎的伺服器端物件加密。網格管理員可以啟用加密作為全域預設設定。StorageGRID 也支援 S3 x-amz-server-Side 加密標頭、可針對每個物件啟用或停用加密。啟用時、物件會在儲存或在網格節點之間傳輸時加密。	有助於保護物件的儲存和傳輸、不受基礎儲存硬體的影響。	SEC 規則 17a-4(f) CTFC 1.31(c) - （d）（FINRA）規則 4511(c)
內建金鑰管理	啟用加密時、每個物件都會以隨機產生的唯一對稱金鑰進行加密、此金鑰會儲存在 StorageGRID 內部、而不會有外部存取。	無需外部金鑰管理即可加密物件。	
符合聯邦資訊處理標準（FIPS） 140-2 標準的加密磁碟	SG5812 、 SG5860 、 SG6160 和 SGF6024 StorageGRID 應用裝置提供 FIPS 140-2 相容加密磁碟的選項。磁碟的加密金鑰可由外部 KMIP 伺服器選擇性管理。	可安全儲存系統資料、中繼資料和物件。也提供 StorageGRID 軟體型物件加密、可保護物件的儲存和傳輸。	SEC 規則 17a-4(f) CTFC 1.31(c) - （d）（FINRA）規則 4511(c)
符合聯邦資訊處理標準 (FIPS) 140-3 的節點加密	SG5812、SG5860、SG6160、SGF6112、SG1100 和 SG110 StorageGRID設備提供符合 FIPS 140-3 的節點加密選項。節點的加密金鑰由外部 KMIP 伺服器管理。	可安全儲存系統資料、中繼資料和物件。也提供 StorageGRID 軟體型物件加密、可保護物件的儲存和傳輸。	SEC 規則 17a-4(f) CTFC 1.31(c) - （d）（FINRA）規則 4511(c)
背景完整性掃描與自我修復	StorageGRID 在物件和子物件層級使用雜湊、校驗和循環備援檢查（CRC）的互鎖機制、以防止物件在儲存和傳輸時發生資料不一致、竄改或修改。StorageGRID 會自動偵測毀損和竄改的物件並加以取代、同時隔離變更的資料並向管理員發出警示。	讓 Grid 管理員能夠滿足 SLA 、法規及其他資料耐用性相關義務。協助客戶偵測試圖加密、竄改或修改資料的勒索軟體或病毒。	SEC 規則 17a-4(f) CTFC 1.31(c) - （d）（FINRA）規則 4511(c)

功能	功能	影響	法規遵循
原則型物件放置與保留	StorageGRID 可讓 Grid 系統管理員設定 ILM 規則、以指定物件保留、放置、保護、轉換和到期。網格管理員可以設定 StorageGRID 、依其中繼資料篩選物件、並在各種精細度層級套用規則、包括網格範圍、租戶、貯體、金鑰首碼、 以及使用者定義的中繼資料金鑰值配對。StorageGRID 有助於確保物件在整個生命週期內都依照 ILM 規則儲存、除非用戶端明確刪除。	協助強制執行資料放置、保護及保留。協助客戶達成 SLA 、以確保持久性、可用度和效能。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
背景中繼資料掃描	StorageGRID 會定期掃描背景中的物件中繼資料、以套用 ILM 指定的物件資料放置或保護變更。	協助探索毀損的物件。	
可調一致性	租戶可以在貯體層級選擇一致性層級、以確保多站台連線等資源可用。	提供選項、只有在必要數量的站台或資源可用時、才會將寫入內容提交至網格。	

系統管理安全功能

探索 StorageGRID 的管理安全功能。

功能	功能	影響	法規遵循
伺服器憑證（網格管理介面）	Grid 系統管理員可以設定 Grid Management Interface 使用組織信任 CA 簽署的伺服器憑證。	使用由標準信任 CA 簽署的數位憑證、驗證管理用戶端和網格之間的管理 UI 和 API 存取。	—
管理使用者驗證	系統管理使用者會使用使用者名稱和密碼進行驗證。系統管理使用者和群組可以是本機或同盟的、從客戶的 Active Directory 或 LDAP 匯入。本機帳戶密碼以受 bcrypt 保護的格式儲存；命令列密碼以 SHA-2 保護的格式儲存。	驗證管理 UI 和 API 的管理存取權。	—

功能	功能	影響	法規遵循
SAML 支援	StorageGRID 支援使用安全聲明標記語言 2.0 （ SAML 2.0 ）標準的單一登入（ SSO ）。啟用SSO時、所有使用者必須先經過外部身分識別供應商的驗證、才能存取Grid Manager、租戶管理程式、Grid Management API或租戶管理API。本機使用者無法登入StorageGRID 到無法使用的功能。	為網格和租戶管理員提供更高層級的安全性、例如 SSO 和多因素驗證（ MFA ）。	NIST SP800-63
精細的權限控制	網格管理員可以將權限指派給角色、並將角色指派給管理使用者群組、以強制執行管理用戶端可以同時使用管理 UI 和 API 來執行的工作。	允許 Grid 管理員管理管理員使用者和群組的存取控制。	—
分散式稽核記錄	StorageGRID 提供內建的分散式稽核記錄基礎架構、可擴充至多達 16 個站台的數百個節點。StorageGRID 軟體節點會產生稽核訊息、這些訊息會透過備援稽核轉送系統傳輸、最後會擷取到一或多個稽核記錄儲存庫中。稽核訊息會擷取物件層級精細度的事件、例如用戶端啟動的 S3 API 作業、 ILM 的物件生命週期事件、背景物件健全狀況檢查、以及從管理 UI 或 API 所做的組態變更。 審計日誌可以透過 syslog 匯出，從而允許 Splunk 和 ELK 等工具挖掘審計訊息。審計訊息有四種類型： • 系統稽核訊息 • 物件儲存稽核訊息 • HTTP 傳輸協定稽核訊息 • 管理稽核訊息 審計日誌可以儲存在 S3 儲存桶中，以便長期保留和應用程式存取。	為 Grid 管理員提供經過實證且可擴充的稽核服務、讓他們能夠為各種目標挖掘稽核資料。這類目標包括疑難排解、稽核 SLA 效能、用戶端資料存取 API 作業、以及管理組態變更。	—

功能	功能	影響	法規遵循
系統稽核	系統稽核訊息會擷取與系統相關的事件、例如網格節點狀態、毀損的物件偵測、根據 ILM 規則在所有指定位置提交的物件、以及全系統維護工作的進度（網格工作）。	協助客戶疑難排解系統問題、並提供依據其 SLA 儲存物件的證明。SLA 是由 StorageGRID ILM 規則實作、並受到完整性保護。	—
物件儲存稽核	物件儲存稽核訊息會擷取物件 API 交易和生命週期相關事件。這些事件包括物件儲存和擷取、網格節點對網格節點傳輸和驗證。	協助客戶透過系統稽核資料進度、以及是否提供指定為 StorageGRID ILM 的 SLA 。	—
HTTP 傳輸協定稽核	HTTP 傳輸協定稽核訊息會擷取與用戶端應用程式和 StorageGRID 節點相關的 HTTP 傳輸協定互動。此外、客戶可以擷取特定的 HTTP 要求標頭（例如 X 轉寄的 for 和使用者中繼資料 [x-amz-meta-*] ）進行稽核。	協助客戶稽核用戶端與 StorageGRID 之間的資料存取 API 作業、並追蹤個別使用者帳戶和存取金鑰的動作。客戶也可以將使用者中繼資料登入稽核、並使用 Splunk 或 elk 等記錄採礦工具來搜尋物件中繼資料。	—
管理稽核	管理稽核訊息會將管理使用者要求記錄到管理 UI （ Grid Management Interface ）或 API 。並非取得API或取得API要求的每個要求、都會以使用者名稱、IP和API要求類型來記錄回應。	協助 Grid 管理員建立系統組態變更記錄、記錄使用者在何時從哪個來源 IP 和目的地 IP 所做的變更。	—
TLS 1.3 支援管理 UI 和 API 存取	TLS 會為管理用戶端和 StorageGRID 管理節點之間的通訊建立信號交換傳輸協定。	可讓管理用戶端和 StorageGRID 識別及驗證彼此、並與機密性和資料完整性通訊。	—
StorageGRID 監控用的 SNMPv3	SNMPv3 同時提供強大的驗證和資料加密功能來保護隱私、進而提供安全性。在 v3 中、傳輸協定資料單元會使用 CBC-DES 進行加密、以用於加密傳輸協定。 傳送傳輸協定資料單元的使用者驗證是由 HMAC-SHA 或 HMAC-MD5 驗證傳輸協定提供。 仍支援 SNMPv2 和 v1 。	在管理節點上啟用 SNMP 代理程式、協助 Grid 管理員監控 StorageGRID 系統。	—

功能	功能	影響	法規遵循
Prometheus計量匯出的用戶端憑證	網格管理員可以上傳或產生用戶端憑證、這些憑證可用於提供對 StorageGRID Prometheus 資料庫的安全、驗證存取。	網格管理員可以使用用戶端憑證、使用 Grafana 等應用程式從外部監控 StorageGRID 。	—

平台安全功能

瞭解 StorageGRID 的平台安全功能。

功能	功能	影響	法規遵循
內部公開金鑰基礎架構（ PKI ）、節點憑證和 TLS	StorageGRID 使用內部 PKI 和節點憑證來驗證和加密節點間通訊。節點間通訊受到 TLS 的保護。	協助保護 LAN 或 WAN 上的系統流量、特別是在多站台部署中。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
節點防火牆	StorageGRID 會自動設定 IP 表格和防火牆規則、以控制傳入和傳出網路流量、以及關閉未使用的連接埠。	協助保護 StorageGRID 系統、資料和中繼資料、防範來路不明的網路流量。	—
作業系統強化	強化 StorageGRID 實體應用裝置和虛擬節點的基礎作業系統；移除不相關的軟體套件。	有助於將潛在的攻擊面降至最低。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
定期更新平台和軟體	StorageGRID 提供包括作業系統、應用程式二進位檔和軟體更新的一般軟體版本。	協助 StorageGRID 系統以最新的軟體和應用程式二進位檔進行更新。	—
停用透過安全 Shell （ SSH ）的根登入	在所有 StorageGRID 節點上、都會停用透過 SSH 的根登入。SSH 存取使用憑證驗證。	協助客戶防範 root 登入的潛在遠端密碼破解。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
自動時間同步	StorageGRID 會自動將每個節點的系統時鐘與多個外部時間網路時間傳輸協定（ NTP ）伺服器同步。至少需要四個階層 3 或更新版本的 NTP 伺服器。	確保所有節點的時間參照相同。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
獨立的網路、用於用戶端、管理和內部網格流量	StorageGRID 軟體節點和硬體應用裝置支援多個虛擬和實體網路介面、讓客戶可以在不同的網路上分隔用戶端、管理和內部網格流量。	允許 Grid 管理員隔離內部和外部網路流量、並透過不同 SLA 的網路提供流量。	—

功能	功能	影響	法規遵循
多個虛擬 LAN （ VLAN ）介面	StorageGRID 支援在 StorageGRID 用戶端和網格網路上設定 VLAN 介面。	允許 Grid 管理員分割和隔離應用程式流量、以確保安全性、靈活度和效能。	
不受信任的用戶端網路	不受信任的用戶端網路介面只接受已明確設定為負載平衡器端點的連接埠上的傳入連線。	確保暴露於不受信任網路的介面受到保護。	—
可設定的防火牆	管理管理、網格和用戶端網路的開放和封閉連接埠。	允許網格管理員控制連接埠的存取、並管理核准的裝置對連接埠的存取。	
增強的 SSH 行為	安裝前預設禁用 SSH。在預設狀態下，僅在連結本機管理連接埠位址上啟用 SSH 存取。管理者和 root 使用者密碼設定為裝置計算控制器序號。僅允許在序列控制台和圖形控制台（BMC KVM）上登入。任何網路連接埠上的 SSH 均已停用。	增強網路存取保護。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)
節點加密	作為 KMS 主機伺服器加密新功能的一部分、 StorageGRID 應用裝置安裝程式會新增節點加密設定。	此設定必須在裝置安裝的硬體組態階段啟用。	SEC 規則 17a-4(f) CTFC 1.31(c) - （ d ）（ FINRA ）規則 4511(c)

雲端整合

瞭解 StorageGRID 如何與雲端服務整合。

功能	功能	影響
以通知為基礎的病毒掃描	StorageGRID 平台服務支援事件通知。事件通知可與外部雲端運算服務搭配使用、以觸發資料上的病毒掃描工作流程。	可讓租戶管理員使用外部雲端運算服務觸發資料的病毒掃描。

版權資訊

商標資訊