系統強化
StorageGRID 11.7

NetApp
April 12, 2024

目錄

系統強化

系統強化：總覽

系統強化是消除StorageGRID 儘可能多的安全風險的程序、因為這個系統是由一個系統來強化的。

本文件概述StorageGRID 具體針對具體功能的強化準則。這些準則是業界標準系統強化最佳實務做法的補充說明。例如、這些準則假設您使用強式密碼來StorageGRID 執行功能、使用HTTPS而非HTTP、並在可行的情況下啟用憑證型驗證。

安裝和設定StorageGRID 功能時、您可以使用這些準則來協助您達成任何規定的資訊系統機密性、完整性和可用度安全目標。

StorageGRID 遵循 "NetApp 弱點處理原則"。報告的弱點會根據產品安全性事件回應程序進行驗證和解決。

強化**StorageGRID** 功能的一般考量

強化StorageGRID 功能時、您必須考量下列事項：

- 您已實作的StorageGRID 三個不實網路中、有哪一個。所有StorageGRID 的支援系統都必須使用Grid Network、但您也可能使用管理網路、用戶端網路或兩者。每個網路都有不同的安全考量。
- 您用於StorageGRID 您的作業系統中個別節點的平台類型。可在VMware虛擬機器、Linux主機上的容器引擎內或專屬硬體設備上部署支援節點。StorageGRID每種平台都有自己的強化最佳實務做法。
- 租戶帳戶的可信程度。如果您是具有不受信任租戶帳戶的服務供應商、您的安全考量會與僅使用受信任的內部租戶不同。
- 貴組織遵循哪些安全要求和慣例。您可能需要遵守特定的法規或企業要求。

強化軟體升級準則

您必須保持StorageGRID 更新的不中斷系統和相關服務、才能抵禦攻擊。

升級**StorageGRID** 至更新版軟體

只要可能、您就應該將StorageGRID 更新版的更新版更新為最新的重大版本或先前的重大版本。保持更新有助於縮短已知弱點的作用時間、並減少整體攻擊範圍。StorageGRID此外、最新版的 StorageGRID 通常包含舊版中未包含的安全性強化功能。

請參閱 "NetApp 互通性對照表工具" （ IMT ）來判斷您應該使用的 StorageGRID 軟體版本。當需要修補程式時、NetApp會優先為最新版本建立更新。某些修補程式可能與舊版不相容。

- 若要下載最新的 StorageGRID 版本和 Hotfix 、請前往 "NetApp下載StorageGRID"。
- 若要升級 StorageGRID 軟體、請參閱 "升級指示"。
- 若要套用 Hotfix 、請參閱 "修復程序StorageGRID"。

升級至外部服務

外部服務可能會有間接影響StorageGRID 到非功能性的弱點。您應確保StorageGRID 仰賴的服務保持最新狀態。這些服務包括LDAP、KMS（或KMIP伺服器）、DNS和NTP。

使用 "NetApp 互通性對照表工具" 以取得支援版本的清單。

升級至**Hypervisor**

如果StorageGRID 您的VMware節點或其他Hypervisor上執行、則必須確保Hypervisor軟體和韌體為最新版本。

使用 "NetApp 互通性對照表工具" 以取得支援版本的清單。

* 升級至 **Linux** 節點 *

如果StorageGRID 您的支援節點使用Linux主機平台、則必須確保安全性更新和核心更新已套用至主機作業系統。此外、您必須在有更新可用時、將韌體更新套用至易受影響的硬體。

使用 "NetApp 互通性對照表工具" 以取得支援版本的清單。

強化有關資訊網路的準則**StorageGRID**

此支援每個網格節點最多三個網路介面、可讓您針對每個個別網格節點設定網路、以符合您的安全性和存取需求。StorageGRID

如需 StorageGRID 網路的詳細資訊、請參閱 "網路類型StorageGRID"。

Grid Network準則

您必須為所有內部StorageGRID 的資訊流量設定Grid Network。所有的網格節點都位於網格網路上、而且必須能夠與所有其他節點交談。

設定Grid Network時、請遵循下列準則：

- 確保網路受到不受信任用戶端的保護、例如開放式網際網路上的用戶端。
- 如有可能、請將Grid Network專用於內部流量。管理網路和用戶端網路都有額外的防火牆限制、可封鎖外部的內部服務流量。支援將Grid Network用於外部用戶端流量、但這種使用方式可提供較少的保護層。
- 如果StorageGRID 此功能跨越多個資料中心、請使用Grid Network上的虛擬私有網路（VPN）或同等網路、為內部流量提供額外的保護。
- 有些維護程序需要在主要管理節點和所有其他網格節點之間的連接埠22上進行安全Shell（SSH）存取。使用外部防火牆限制SSH存取信任的用戶端。

管理網路準則

管理網路通常用於管理工作（使用Grid Manager或SSH的信任員工）、以及與其他信任的服務（例如LDAP、DNS、NTP或KMS（或KMIP伺服器）通訊。不過StorageGRID 、內部不強制使用此功能。

如果您使用的是管理網路、請遵循下列準則：

- 封鎖管理網路上的所有內部流量連接埠。請參閱 "內部連接埠清單"。
- 如果不受信任的用戶端可以存取管理網路、請使用StorageGRID 外部防火牆封鎖對管理網路上的功能。

用戶端網路準則

用戶端網路通常用於租戶及與外部服務（例如CloudMirror複寫服務或其他平台服務）通訊。不過StorageGRID、內部不強制使用此功能。

如果您使用的是用戶端網路、請遵循下列準則：

- 封鎖用戶端網路上的所有內部流量連接埠。請參閱 "內部連接埠清單"。
- 只接受明確設定的端點上的傳入用戶端流量。請參閱相關資訊 "管理防火牆控制"。

強化有關節點的準則StorageGRID

可在VMware虛擬機器、Linux主機上的容器引擎內或專屬硬體設備上部署支援節點。StorageGRID每種類型的平台和每種類型的節點都有自己的強化最佳實務做法。

防火牆組態

在系統強化程序中、您必須檢閱外部防火牆組態並加以修改、以便只接受來自IP位址和嚴格需要的連接埠的流量。

StorageGRID 在每個節點上都包含內部防火牆、可讓您控制對節點的網路存取、藉此增強網格的安全性。您應該 "管理內部防火牆控制" 防止網路存取所有連接埠、但您的特定網格部署所需的連接埠除外。您在「防火牆控制」頁面上所做的組態變更會部署到每個節點。

具體而言、您可以管理以下領域：

- * 貴賓位址 * ：您可以允許選取的 IP 位址或子網路存取「管理外部存取」索引標籤上的設定所關閉的連接埠。
- * 管理外部存取 * ：您可以關閉預設開啟的連接埠、或重新開啟先前關閉的連接埠。
- * 不受信任的用戶端網路 * ：您可以指定節點是否信任來自用戶端網路的傳入流量、以及在設定不受信任的用戶端網路時、您要開啟的其他連接埠。

雖然此內部防火牆提供額外的保護層來抵禦某些常見的威脅、但它並不免除外部防火牆的需求。

如需 StorageGRID 使用的所有內部和外部連接埠清單、請參閱 "網路連接埠參考"。

停用未使用的服務

對於所有StorageGRID 的支援節點、您應該停用或封鎖未使用服務的存取。例如、如果您不打算設定用戶端對 NFS 稽核共用的存取、請封鎖或停用對這些服務的存取。

虛擬化、容器和共享硬體

對於所有StorageGRID 的物件節點、請避免在StorageGRID 不受信任的軟體所在的實體硬體上執行不可靠的功能。如果 StorageGRID 和惡意軟體位於同一實體硬體上、請勿假設 Hypervisor 保護措施可防止惡意軟體存取

StorageGRID 保護的資料。例如、Meltdown和Spetter攻擊會利用現代處理器的重大弱點、讓程式在同一部電腦的記憶體中竊取資料。

在安裝期間保護節點

安裝節點時、請勿允許不受信任的使用者透過網路存取 StorageGRID 節點。節點必須先加入網格、才能完全安全無虞。

管理節點準則

管理節點提供系統組態、監控及記錄等管理服務。當您登入Grid Manager或租戶管理程式時、即連線至管理節點。

請遵循以下準則、將管理節點安全地存放在StorageGRID 您的一套系統上：

- 保護不受信任用戶端（例如開放式網際網路上的用戶端）的所有管理節點。確保任何不受信任的用戶端都無法存取Grid Network、管理網路或用戶端網路上的任何管理節點。
- 可控制Grid Manager和Tenant Manager功能的存取權限。StorageGRID授予每個使用者群組其角色所需的最低權限、並使用唯讀存取模式來防止使用者變更組態。
- 使用StorageGRID 動態負載平衡器端點時、請針對不受信任的用戶端流量、使用閘道節點而非管理節點。
- 如果您有不受信任的租戶、請勿允許他們直接存取租戶管理器或租戶管理 API 。而是讓任何不受信任的租戶使用與租戶管理API互動的租戶入口網站或外部租戶管理系統。
- 或者、您也可以使用管理 Proxy 來更有效地控制從管理節點到 NetApp 支援的 AutoSupport 通訊。請參閱的步驟 "建立管理 Proxy"。
- 您也可以選擇使用受限的843和9443連接埠來分隔Grid Manager和Tenant Manager通訊。封鎖共享連接埠443、並將租戶要求限制為連接埠9443以提供額外保護。
- 您也可以為網格管理員和租戶使用者使用個別的管理節點。

如需詳細資訊、請參閱的指示 "管理StorageGRID"。

儲存節點準則

儲存節點可管理及儲存物件資料和中繼資料。請遵循以下準則、將儲存節點固定在StorageGRID 您的一套系統上。

- 請勿允許不受信任的用戶端直接連線至儲存節點。使用由閘道節點或協力廠商負載平衡器提供服務的負載平衡器端點。
- 請勿為不受信任的租戶啟用外傳服務。例如、為不受信任的租戶建立帳戶時、請勿允許租戶使用自己的身分識別來源、也不允許使用平台服務。請參閱的步驟 "建立租戶帳戶"。
- 針對不受信任的用戶端流量使用協力廠商負載平衡器。第三方負載平衡可提供更多控制能力、並提供額外的層級保護、防止攻擊。
- 您也可以選擇使用儲存Proxy、以更有效地控制從儲存節點到外部服務的雲端儲存資源池及平台服務通訊。請參閱的步驟 "建立儲存代理伺服器"。
- 您也可以選擇使用用戶端網路連線至外部服務。然後，選擇 * 組態 * > * 安全性 * > * 防火牆控制 * > * 不受信任的用戶端網路 * ，並指出儲存節點上的用戶端網路不受信任。儲存節點不再接受用戶端網路上的任何傳入流量、而是繼續允許平台服務的傳出要求。

閘道節點準則

閘道節點提供選用的負載平衡介面、用戶端應用程式可用來連接StorageGRID 到VMware。請遵循下列準則、保護StorageGRID 您的整個作業系統中的任何閘道節點：

- 設定及使用負載平衡器端點。請參閱 "負載平衡考量"。
- 對於不受信任的用戶端流量、請在用戶端與閘道節點或儲存節點之間使用協力廠商負載平衡器。第三方負載平衡可提供更多控制能力、並提供額外的層級保護、防止攻擊。如果您確實使用協力廠商負載平衡器、網路流量仍可選擇性地設定為透過內部負載平衡器端點、或直接傳送至儲存節點。
- 如果您使用負載平衡器端點、可選擇讓用戶端透過用戶端網路連線。然後，選擇 * 組態 * > * 安全性 * > * 防火牆控制 * > * 不受信任的用戶端網路 * ，並指出閘道節點上的用戶端網路不受信任。閘道節點僅接受明確設定為負載平衡器端點之連接埠上的傳入流量。

硬體應用裝置節點準則

用作作業系統的各種硬體應用。StorageGRID StorageGRID有些應用裝置可做為儲存節點。其他應用裝置可做為管理節點或閘道節點。您可以將應用裝置節點與軟體型節點結合使用、或是部署設計完善的全應用裝置網格。

請遵循下列準則、確保StorageGRID 您的整個作業系統中的任何硬體應用裝置節點安全無虞：

- 如果應用SANtricity 程式使用NetApp系統管理程式來管理儲存控制器、請避免不受信任的用戶端SANtricity透過網路存取《系統管理程式》。
- 如果應用裝置有基板管理控制器（BMC）、請注意BMC管理連接埠允許低階硬體存取。僅將BMC管理連接埠連接至安全、受信任的內部管理網路。如果沒有此類網路可用、請將BMC管理連接埠保持未連線或封鎖狀態、除非技術支援部門要求BMC連線。
- 如果應用裝置使用智慧型平台管理介面（IPMI）標準、支援透過乙太網路遠端管理控制器硬體、請封鎖連接埠623上不受信任的流量。

> ⓘ 您可以使用管理 API 私有端點（ Put /Private / bmc ）來啟用或停用包含 BMC 的所有應用裝置的遠端 IPMI 存取。

- 如果應用裝置中的儲存控制器包含FDE或FIPS磁碟機、且已啟用磁碟機安全功能、請使用SANtricity 支援功能來設定磁碟機安全金鑰。請參閱 "設定 SANtricity 系統管理員（ SG6000 和 SG5700 ）"。
- 對於沒有FDE或FIPS磁碟機的設備、請使用金鑰管理伺服器（KMS）啟用節點加密。請參閱 "選用：啟用節點加密"。

TLS 和 SSH 的強化準則

您應該取代安裝期間建立的預設憑證、並為 TLS 和 SSH 連線選取適當的安全性原則。

證書強化準則

您應該使用自己的自訂憑證來取代安裝期間建立的預設憑證。

對於許多組織而言StorageGRID 、自我簽署的數位憑證不符合其資訊安全政策。在正式作業系統上、您應該安裝CA簽署的數位憑證、以用於驗證StorageGRID 功能。

具體而言、您應該使用自訂伺服器憑證、而非下列預設憑證：

- 管理介面認證：用於安全存取Grid Manager、租戶管理程式、Grid Management API及租戶管理API。
- * S3和Swift API認證*：用於保護儲存節點和閘道節點的存取安全、S3和Swift用戶端應用程式可用來上傳和下載物件資料。

請參閱 "管理安全性憑證" 以取得詳細資料和指示。

> 可分別管理負載平衡器端點所使用的憑證。StorageGRID若要設定負載平衡器憑證、請參閱 "設定負載平衡器端點"。

使用自訂伺服器憑證時、請遵循下列準則：

- 憑證應具有 *subjectAltName* 這與DNS項目相符StorageGRID 。如需詳細資料、請參閱第4.2.1.6節「Subject Alternative Name」（主題替代名稱）、請參閱 "RFC 5280：PKIX憑證與CRL設定檔"。
- 如有可能、請避免使用萬用字元憑證。此準則的例外情況是 S3 虛擬託管樣式端點的憑證、如果庫位名稱事先不清楚、則需要使用萬用字元。
- 當您必須在憑證中使用萬用字元時、應採取其他步驟來降低風險。使用萬用字元模式、例如 `*.s3.example.com`、請勿使用 `s3.example.com` 其他應用程式的字尾。此模式也適用於路徑樣式S3存取、例如 `dc1-s1.s3.example.com/mybucket`。
- 將憑證到期時間設為短（例如2個月）、然後使用Grid Management API自動執行憑證輪替。這對萬用字元憑證特別重要。

此外、用戶端在與StorageGRID NetApp通訊時、應使用嚴格的主機名稱檢查。

TLS 和 SSH 原則的強化準則

您可以選取安全性原則、以決定使用哪些通訊協定和加密程式來建立與用戶端應用程式的安全 TLS 連線、以及安全的 SSH 連線至內部 StorageGRID 服務。

安全性原則控制 TLS 和 SSH 如何加密移動中的資料。最佳做法是停用應用程式相容性不需要的加密選項。請使用預設的現代化原則、除非您的系統需要符合一般準則、或您需要使用其他密碼。

請參閱 "管理 TLS 和 SSH 原則" 以取得詳細資料和指示。

其他強化準則

除了遵循StorageGRID 有關「不二網」和「節點」的強化準則、您還應遵循StorageGRID「不二網」系統其他區域的強化準則。

記錄與稽核訊息

請務必StorageGRID 以安全的方式保護不間斷記錄和稽核訊息輸出。從支援和系統可用度的觀點來看、支援記錄和稽核訊息可提供寶貴的資訊。StorageGRID此外StorageGRID 、包含在「資訊記錄」和「稽核訊息」輸出中的資訊和詳細資料、通常屬於敏感性質。

設定StorageGRID 將安全事件傳送至外部syslog伺服器。如果使用syslog匯出、請選取TLS和RELP/TLS做為傳輸傳輸傳輸傳輸傳輸傳輸協定。

請參閱 "記錄檔參考" 如需 StorageGRID 記錄的詳細資訊、請參閱。請參閱 "稽核訊息" 如需 StorageGRID 稽核

訊息的詳細資訊、請參閱。

NetApp AutoSupport

StorageGRID 的 AutoSupport 功能可讓您主動監控系統的健全狀況、並自動傳送訊息和詳細資料給 NetApp 技術支援、貴組織的內部支援團隊或支援合作夥伴。根據預設、首次設定 StorageGRID 時、會啟用 AutoSupport 訊息給 NetApp 技術支援。

可停用此功能。AutoSupport不過、NetApp建議您啟用此功能、因為AutoSupport 當StorageGRID 您的作業系統發生問題時、支援使用支援功能來加速問題識別與解決。

支援HTTPS、HTTP和SMTP傳輸傳輸傳輸傳輸傳輸傳輸協定。AutoSupport由於 AutoSupport 訊息的敏感性質、NetApp 強烈建議使用 HTTPS 做為傳送 AutoSupport 訊息給 NetApp 支援的預設傳輸協定。

跨來源資源共享（ CORS ）

如果您想讓其他網域中的 Web 應用程式能夠存取 S3 貯體中的貯體和物件、則可以為 S3 貯體設定跨來源資源共享（ CORS ）。一般而言、除非需要、否則請勿啟用 CORS 。如果需要CORS、請將其限制在信任的來源。

請參閱的步驟 "設定跨來源資源共享（ CORS ）"。

外部安全裝置

完整的強化解決方案必須能解決StorageGRID 不屬於其他功能的安全機制問題。使用額外的基礎架構裝置來篩選及限制StorageGRID 存取功能、是建立及維持嚴苛安全態勢的有效方法。這些外部安全裝置包括防火牆、入侵防禦系統（IPS）和其他安全裝置。

不受信任的用戶端流量建議使用協力廠商負載平衡器。第三方負載平衡可提供更多控制能力、並提供額外的層級保護、防止攻擊。

勒索軟體緩解

請遵循中的建議、協助保護物件資料免遭勒索軟體攻擊 "使用 StorageGRID 進行勒索軟體防禦"。