StorageGRID 的系統強化

StorageGRID software

NetApp
July 23, 2026

目錄

StorageGRID 的系統強化

了解 StorageGRID 的系統強化

系統強化是指從 StorageGRID 系統中消除盡可能多的安全性風險的過程。

在安裝和設定 StorageGRID 時，請使用這些準則來協助您達成任何規定的機密性、完整性和可用度安全性目標。

您應該已經採用業界標準的系統強化最佳實務做法。例如，您為 StorageGRID 使用強式密碼、使用 HTTPS 而非 HTTP，並在可用時啟用憑證型驗證。這些最佳實務做法必須包含實體和環境安全性，以限制實體存取並保護實體資料中心和支援基礎架構。您還必須參考適用於您業務和所在地區的任何監管標準和建議。

StorageGRID 遵循相關規定 "NetApp 漏洞處理原則"。已報告的漏洞將根據產品安全性事件回應流程進行驗證和處理。

在強化 StorageGRID 系統時，請考慮以下事項：

- 您已實作 StorageGRID 的哪三種網路。所有 StorageGRID 系統都必須使用網格網路，但您也可能同時使用管理網路、用戶端網路或兩者。每種網路的安全性考量各不相同。
- *您在 StorageGRID 系統中各節點所使用的平台類型。*StorageGRID 節點可部署在 VMware 虛擬機器上、Linux 主機上的 Container 引擎中，或作為專用硬體應用裝置部署。每種平台類型都有其自身的一套強化最佳實務做法。
- 租戶帳戶的可信度。如果您是服務供應商，且租戶帳戶不受信任，那麼您面臨的安全性問題將與僅使用受信任的公司內部租戶帳戶的情況有所不同。
- 貴組織遵循哪些安全性要求和規範。您可能需要遵守特定的監管或公司要求。

StorageGRID 軟體升級的強化準則

為了抵禦攻擊，您必須保持 StorageGRID 系統及相關服務的更新。

StorageGRID 軟體升級

只要條件允許，就應該將 StorageGRID 軟體升級到最新主要版本或上一個主要版本。維持 StorageGRID 更新有助於減少已知漏洞的活躍時間，並縮小整體攻擊面。此外，最新版本的 StorageGRID 通常包含早期版本所沒有的安全性強化功能。

請查閱 "NetApp 互通性矩陣工具"（IMT）以確定您應該使用的 StorageGRID 軟體版本。如果需要 Hotfix，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，請造訪 "NetApp 下載：StorageGRID"。
- 若要升級 StorageGRID 軟體，請參閱"升級說明"。
- 若要套用 Hotfix，請參閱"StorageGRID Hotfix 程序"。

外部服務升級

外部服務可能有漏洞，間接影響 StorageGRID。請確保 StorageGRID 所依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。

有關支援的版本列表，請參閱 "NetApp 互通性矩陣工具"。

Hypervisor 升級

如果您的 StorageGRID 節點在 VMware 或其他 Hypervisor 上執行，則必須確保 Hypervisor 軟體和韌體是最新的。

有關支援的版本列表，請參閱 "NetApp 互通性矩陣工具"。

升級至 Linux 節點

如果您的 StorageGRID 節點使用 Linux 主機平台，則必須確保主機作業系統已套用安全性更新和核心更新。此外，當韌體更新可用時，您必須將韌體更新套用至存在漏洞的硬體。

有關支援的版本列表，請參閱 "NetApp 互通性矩陣工具"。

StorageGRID 網路強化準則

StorageGRID 系統每個網格節點最多支援三個網路介面，可讓您為每個個別的網格節點設定連網，以符合您的安全性和存取需求。

有關 StorageGRID 網路的詳細資訊，請參閱"StorageGRID 網路類型"。

Grid 網路準則

您必須為所有內部 StorageGRID 流量設定網格網路。所有網格節點都位於網格網路上，且必須能夠與其他所有節點通訊。

設定 Grid 網路時，請遵循以下準則：

- 確保網路安全，防止來自不受信任的用戶端（例如來自開放網際網路的用戶端）的存取。
- 盡可能僅使用 Grid Network 進行內部流量傳輸。Admin Network 和 Client Network 都設有額外的防火牆限制，會封鎖外部流量存取內部服務。雖然支援使用 Grid Network 傳輸外部用戶端流量，但這種做法提供的保護階層數較少。
- 如果 StorageGRID 部署跨越多個資料中心，請使用 Grid Network 上的虛擬私人網路 （VPN） 或等效技術，為內部流量提供額外的保護。
- 某些維護作業需要透過主管理節點與所有其他網格節點之間的連接埠 22 進行安全殼層 (SSH) 存取。請使用外部防火牆將 SSH 存取限制為受信任的用戶端。

管理員網路指南

管理網路通常用於執行管理任務（受信任的員工使用 Grid Manager 或 SSH）以及與其他受信任的服務（例如 LDAP、DNS、NTP 或 KMS（或 KMIP 伺服器））通訊。但是，StorageGRID 內部並不會強制執行此用途。

如果您要使用管理網路，請遵循以下準則：

- 封鎖管理網路上的所有內部流量連接埠。請參閱"內部連接埠列表"。
- 如果不受信任的用戶端可以存取管理網路，請使用外部防火牆封鎖管理網路上對 StorageGRID 的存取。

用戶端網路指南

用戶端網路通常用於租戶以及與外部服務（例如 CloudMirror 複寫服務或其他平台服務）通訊。但是，StorageGRID 內部並不會強制執行此用法。

如果您正在使用用戶端網路，請遵循以下準則：

- 封鎖用戶端網路上的所有內部流量連接埠。請參閱"內部連接埠列表"。
- 僅允許透過明確設定的端點接受傳入用戶端流量。請參閱相關資訊 "管理防火牆控制"。

StorageGRID 節點強化準則

StorageGRID 節點可部署在 VMware 虛擬機器上、Linux 主機上的 Container 引擎中，或作為專用硬體設備部署。每種平台和每種節點都有其自身的一套強化最佳實務做法。

控制對 BMC 的遠端 IPMI 存取

您可以為所有包含 BMC 的裝置啟用或停用遠端 IPMI 存取。遠端 IPMI 介面允許任何擁有 BMC 帳戶和密碼的使用者對您的 StorageGRID 設備進行底層硬體存取。如果您不需要對 BMC 進行遠端 IPMI 存取，請停用此選項。

- 若要在 Grid Manager 中控制對 BMC 的遠端 IPMI 存取，請前往 **Configuration** > **Security** > **Security settings** > **Appliances**：
  - 清除「啟用遠端 IPMI 存取」核取方塊，即可停用對 BMC 的 IPMI 存取。
  - 勾選「啟用遠端 IPMI 存取」核取方塊，即可啟用對 BMC 的 IPMI 存取。

如需 BMC 強化的其他資訊，請參閱 "強化基板管理控制器"的網路安全資訊表 "國家安全局（NSA）"和 "網路安全與基礎設施安全局（CISA）"。

防火牆組態

作為系統強化程序的一部分，您必須審查外部防火牆組態並加以修改，以便僅接受來自嚴格需要的 IP 位址和連接埠的流量。

StorageGRID 在每個節點上內建了內部防火牆，透過控制節點的網路存取來增強網格的安全性。您應該"管理內部防火牆控制"以防止除特定網格部署所需連接埠之外的所有連接埠進行網路存取。您在防火牆控制頁面上所做的組態變更將部署到每個節點。

具體來說，您可以管理以下幾個方面：

- 特權位址：您可以允許選定的 IP 位址或子網路存取在「管理外部存取」標籤上的設定中關閉的連接埠。
- 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要開啟的其他連接埠。

雖然此內部防火牆可針對某些常見威脅提供額外的保護階層，但並不能取代外部防火牆的需求。

如需 StorageGRID 使用的所有內部和外部連接埠清單，請參閱 "StorageGRID 內部連接埠" 和 "用於外部通訊的連接埠"。

停用未使用的服務

對於所有 StorageGRID 節點，您應停用或封鎖對未使用服務的存取。例如，如果您不打算使用 DHCP，請使用 Grid Manager 關閉連接埠 68。選取 組態 > 防火牆控制 > 管理外部存取。然後將連接埠 68 的狀態切換從 開啟 變更為 關閉。

虛擬化、**Container** 和共享的硬體

對於所有 StorageGRID 節點，請避免將 StorageGRID 與不受信任的軟體運行在同一實體硬體上。如果 StorageGRID 和惡意軟體都存在於同一實體硬體上，請勿假設 Hypervisor 的防護措施能夠阻止惡意軟體存取受 StorageGRID 保護的資料。例如，Meltdown 和 Spectre 攻擊利用了現代處理器中的關鍵漏洞，允許程式竊取同一台電腦上記憶體容量中的資料。

安裝期間保護節點

在 StorageGRID 節點安裝過程中，禁止未經信任的使用者透過網路存取這些節點。節點只有加入網格後才能完全安全。

限制對硬體的實體存取

您必須將對 StorageGRID 硬體應用裝置節點、VMware 虛擬機器主機以及執行 StorageGRID 的 Linux 主機的實體存取限制為僅限授權管理員。實體存取控制措施的範例包括鎖具、保全、實體屏障和視訊監控。

硬體應用裝置節點的設計初衷是僅由授權管理員安裝和操作。請勿允許未經授權的管理員存取硬體應用裝置節點。

管理節點指南

管理節點提供系統組態、監控和記錄等管理服務。當您登入 Grid Manager 或 Tenant Manager 時，您連接的就是一個管理節點。

請遵循下列準則，以保護 StorageGRID 系統中的管理節點安全性：

- 保護所有管理節點免受不受信任用戶端（例如開放網際網路上的用戶端）的存取。確保任何不受信任的用戶端都無法存取網格網路、管理網路或用戶端網路上的任何管理節點。
- StorageGRID 群組控制對 Grid Manager 和 Tenant Manager 功能的存取。授予每個使用者群組與其角色相符的最低必要權限，並使用唯讀存取模式以防止使用者變更組態。
- 使用 StorageGRID 負載平衡器端點時，對於不受信任的用戶端流量，請使用 Gateway Nodes 而非 Admin Nodes。
- 如果您有不受信任的租戶，請不要允許他們直接存取 Tenant Manager 或 Tenant Management API。相反，應讓所有不受信任的租戶使用租戶入口網站或與 Tenant Management API 互動的外部租戶管理系統。
- （選用）使用管理 Proxy，以針對從管理節點到 NetApp 支援的 AutoSupport 通訊進行更多控制。請參閱 "建立管理員 Proxy" 的步驟。
- （選用）使用受限連接埠 8443 和 9443 來分隔 Grid Manager 和 Tenant Manager 的通訊。為了進一步保護

，請封鎖共享連接埠 443，並將租戶要求限制在連接埠 9443。

- （可選）為網格管理員和租戶使用者使用分隔的管理節點。

如需更多資訊，請參閱 "管理 StorageGRID" 的說明。

儲存節點指南

儲存節點管理和儲存物件資料和中繼資料。請遵循下列準則來保護 StorageGRID 系統中的儲存節點。

- 不要允許不受信任的用戶端直接連線至儲存節點。請使用由 Gateway Node 或協力廠商負載平衡器提供的負載平衡端點。
- 不要為不受信任的租戶啟用傳出服務。例如，在為不受信任的租戶建立帳戶時，不要允許該租戶使用其自身的身分來源，也不要允許其使用平台服務。請參閱相關步驟 "建立租戶帳戶"。
- 對不受信任的用戶端流量使用協力廠商負載平衡器。協力廠商負載平衡提供更多控制，以及額外的攻擊防護層。
- 您也可以選擇使用儲存設備 Proxy，以便更有效地控制雲端儲存池以及儲存節點與外部服務之間的平台服務通訊。請參閱相關步驟"建立儲存設備 Proxy"。
- （可選）使用用戶端網路連線至外部服務。然後，選取 **Configuration** > **Security** > **Firewall control** > **Untrusted Client Networks**，並將儲存節點上的用戶端網路設定為不受信任。儲存節點將不再接受用戶端網路上的任何傳入流量，但仍允許對平台服務的傳出請求。

閘道節點準則

閘道節點提供選用的負載平衡介面，用戶端應用程式可使用該介面連線至 StorageGRID。請遵循以下準則，以保護 StorageGRID 系統中的所有閘道節點：

- 設定及使用負載平衡端點。請參閱"負載平衡的考慮因素"。
- 對於不受信任的用戶端流量，請在用戶端與 Gateway Node 或 Storage Nodes 之間使用協力廠商負載平衡器。協力廠商負載平衡可提供更精細的控制和額外的保護層，有效抵禦攻擊。即使使用協力廠商負載平衡器，您仍可選擇將網路流量設定為先經過內部負載平衡器端點，或直接傳送至 Storage Nodes。
- 如果您使用負載平衡器端點，可以選擇讓用戶端透過用戶端網路連線。然後，選取 **Configuration** > **Security** > **Firewall control** > **Untrusted Client Networks**，並將 Gateway 節點上的用戶端網路設定為不受信任。Gateway 節點僅接受明確設定為負載平衡器端點的連接埠上的傳入流量。

硬體應用裝置節點指南

StorageGRID 硬體應用裝置專為 StorageGRID 系統設計。部分應用裝置可用作儲存節點。其他應用裝置可用作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組合使用，也可以部署完全由應用裝置組成的整合網格。

請遵循下列準則，以保護 StorageGRID 系統中的所有硬體應用裝置節點：

- 如果應用裝置使用 SANtricity System Manager 進行儲存控制器管理，請阻止不受信任的用戶端透過網路存取 SANtricity System Manager。
- 如果應用裝置具有底板管理控制器 （BMC），請注意 BMC 管理連接埠允許底層硬體存取。請僅將 BMC 管理連接埠連接到安全的、可信任的內部管理網路。

  您可以建立 VLAN 來隔離 BMC 網路連線，並將 BMC 的網際網路存取限制在受信任的網路。如需強制執行

VLAN 隔離的其他資訊，請參閱 "強化基板管理控制器"的網路安全資訊表 "國家安全局（NSA）"和 "網路安全與基礎設施安全局（CISA）"。

如果沒有安全、可信任的內部管理網路，請將 BMC 管理連接埠保持未連接或封鎖狀態。技術支援人員可能會在支援案例期間要求暫時存取。

- 如果應用裝置支援使用智慧型平台管理介面 (IPMI) 標準透過乙太網路遠端管理控制器硬體，請封鎖連接埠 623 上的不受信任流量。

> ⓘ 您可以為所有包含 BMC 的裝置啟用或停用遠端 IPMI 存取。遠端 IPMI 介面允許任何擁有 BMC 帳戶和密碼的使用者對您的 StorageGRID 設備進行底層硬體存取。如果您不需要對 BMC 進行遠端 IPMI 存取，請使用下列方法之一停用此選項：+ 在 Grid Manager 中，前往 **Configuration** > **Security** > **Security settings** > **Appliances**，然後清除 **Enable remote IPMI access** 核取方塊。+ 在 Grid 管理 API 中，使用私有端點： `PUT /private/bmc`。

+ 您也可以停用遠端 IPMI 存取。

- 對於包含 SED、FDE 或 FIPS NL-SAS 磁碟機且使用 SANtricity System Manager 管理的應用裝置型號 "啟用並設定 SANtricity 磁碟機安全性"。
- 對於包含 SED 或 FIPS NVMe SSD 的應用裝置型號，您可以使用 StorageGRID 應用裝置安裝程式和 Grid Manager 進行管理 "啟用並設定 StorageGRID 磁碟機加密"。
- 對於沒有 SED、FDE 或 FIPS 磁碟機的應用裝置，請使用金鑰管理伺服器 (KMS) 來 "啟用並設定 StorageGRID 軟體節點加密"。

相關資訊

"了解 SANtricity System Manager 中的磁碟機安全功能"

StorageGRID 中 TLS 和 SSH 的強化準則

您應該控制 SSH 存取，替換預設的 TLS 憑證，並為 TLS 和 SSH 連線選擇適當的安全性原則。

憑證強化準則

您應該將安裝過程中建立的預設憑證替換為您自己的自訂憑證。

對於許多組織而言，用於 StorageGRID 網路存取的自簽章數位憑證不符合其資訊安全性原則。在正式作業系統中，您應該安裝 CA 簽署的數位憑證，以用於驗證 StorageGRID。

具體來說，您應該使用自訂伺服器憑證，而不是這些預設憑證：

- 管理介面憑證：用於保護對 Grid Manager、Tenant Manager、網格管理 API 和 Tenant Management API 的存取。
- **S3 API** 憑證：用於保護對儲存節點和 Gateway 節點的存取，S3 用戶端應用程式使用這些節點上傳和下載物件資料。

如需詳細資訊和說明，請參閱 "管理安全性證書"。

StorageGRID 單獨管理負載平衡器端點所使用的憑證。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*`與 StorageGRID 的 DNS 項目相符的屬性。如需詳細資訊，請參閱 "RFC 5280：PKIX 憑證和 CRL 設定檔"中的第 4.2.1.6 節「Subject Alternative Name」。
- 盡可能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，如果事先不知道儲存貯體名稱，則必須使用萬用字元憑證。
- 當必須在憑證中使用萬用字元時，應採取額外措施來降低風險。使用類似 `*.s3.example.com`的萬用字元模式，且不要將 `s3.example.com`後綴用於其他應用程式。此模式也適用於路徑式 `S3` 存取，例如 `dc1-s1.s3.example.com/mybucket`。
- 將憑證過期時間設定得較短（例如 2 個月），並使用 Grid Management API 自動化憑證輪替。這對於萬用字元憑證尤其重要。

此外，用戶端在與 StorageGRID 通訊時應使用嚴格的主機名稱檢查。

TLS 和 SSH 原則強化指南

您可以選擇安全性原則來決定使用哪些協定和密碼，以建立與用戶端應用程式的安全 TLS 連線，以及與內部 StorageGRID 服務的安全 SSH 連線。

安全性原則控制 TLS 和 SSH 如何加密傳輸中的資料。最佳實務做法是停用應用程式相容性不需要的加密選項。除非您的系統需要符合通用準則 （Common Criteria）、FIPS 140-2 符合法規，或您需要使用其他加密演算法，否則請使用預設的「現代」原則。

如需詳細資訊和說明，請參閱 "管理 TLS 和 SSH 原則"。

管理外部 SSH 存取

為增強系統安全性，預設會封鎖外部 SSH 存取。僅在需要執行需要傳入 SSH 存取的任務（例如疑難排解）時，才啟用 SSH 存取。如需詳細資訊和說明，請參閱 "管理外部 SSH 存取"。

StorageGRID 中日誌、密碼和稽核訊息的強化準則

除了遵循 StorageGRID 網路和節點的強化準則外，您還應遵循 StorageGRID 系統其他區域的強化準則。

臨時安裝密碼

為確保安裝期間 StorageGRID 系統的安全性，請在 StorageGRID 安裝介面或安裝 API 的臨時安裝程式密碼頁面上設定密碼。設定後，此密碼將套用於所有 StorageGRID 安裝方法，包括使用者介面、安裝 API 和 `configure-storagegrid.py`指令碼。

如需更多資訊，請參閱：

- "在基於軟體的節點上安裝 StorageGRID"
- "安裝 StorageGRID 應用裝置"

日誌和稽核訊息

務必以安全的方式保護 StorageGRID 日誌和稽核訊息輸出。StorageGRID 日誌和稽核訊息從支援和系統可用度的角度來看提供了寶貴的資訊。此外，StorageGRID 日誌和稽核訊息輸出中包含的資訊和細節通常較為敏感。

設定 StorageGRID 將安全性事件傳送到外部 syslog 伺服器。如果使用 syslog 匯出，請選擇 TLS 和 RELP/TLS 作為傳輸協定。

如需 StorageGRID 記錄的詳細資訊，請參閱 "日誌檔參考"。如需 StorageGRID 稽核訊息的詳細資訊，請參閱 "稽核訊息"。

NetApp AutoSupport

StorageGRID 的 AutoSupport 功能可讓您主動監控系統健全狀況，並自動將套件傳送至 NetApp 支援網站、您組織的內部支援團隊或支援合作夥伴。預設情況下，首次設定 StorageGRID 時，即會啟用將 AutoSupport 套件傳送至 NetApp 的功能。

此 AutoSupport 功能可以停用。但是，NetApp 建議啟用此功能，因為當 StorageGRID 系統發生問題時，AutoSupport 有助於加速問題的識別與解決。

AutoSupport 支援 HTTPS、HTTP 和 SMTP 作為傳輸協定。由於 AutoSupport 套件的敏感性，NetApp 強烈建議使用 HTTPS 作為將 AutoSupport 套件傳送至 NetApp 的預設傳輸協定。

跨來源資源共享（CORS）

如果您希望其他網域中的 Web 應用程式能夠存取 S3 儲存桶及其中的物件，則可以為該儲存桶設定跨來源資源共用 (CORS)。一般而言，除非必要，否則請勿啟用 CORS。如果必須使用 CORS，請將其限制為受信任的來源。

請參閱以下步驟"為儲存桶和物件設定 CORS"。

外部安全性設備

一套完整的安全加固方案必須涵蓋 StorageGRID 以外的安全性機制。使用額外的基礎架構設備來過濾和限制對 StorageGRID 的存取，是建立和維護嚴苛安全性態勢的有效方法。這些外部安全性設備包括防火牆、入侵防禦系統 (IPS) 和其他安全性設備。

對於不受信任的用戶端流量，建議使用協力廠商負載平衡器。協力廠商負載平衡可提供更多控制及額外的保護層，以抵禦攻擊。

勒索軟體緩解

遵循 "使用 StorageGRID 進行勒索軟體防禦"中的建議，協助保護您的物件資料免受勒索軟體攻擊。

版權資訊

商標資訊