系統強化
StorageGRID software

NetApp
May 29, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/storagegrid-119/harden/index.html on May 29, 2026. Always check docs.netapp.com for the latest.

目錄

系統強化

系統強化的一般考慮

系統強化是盡可能消除StorageGRID系統中的安全風險的過程。

在安裝和設定StorageGRID時，請使用這些準則來協助您滿足機密性、完整性和可用性的任何規定的安全目標。

您應該已經在使用行業標準的最佳實踐來強化系統。例如，您對StorageGRID使用強密碼，使用 HTTPS 而不是 HTTP，並在可用的情況下啟用基於憑證的驗證。

StorageGRID遵循 "NetApp漏洞處理政策"。報告的漏洞將依照產品安全事件回應流程進行驗證和處理。

強化StorageGRID系統時，請考慮以下事項：

- 您實作了*三個StorageGRID網路中的哪一個*。所有StorageGRID系統都必須使用網格網絡，但您可能也會使用管理網路、客戶端網路或兩者。每個網路都有不同的安全考量。
- 您在StorageGRID系統中用於各個節點的*平台類型*。 StorageGRID節點可部署在 VMware 虛擬機器上、Linux 主機上的容器引擎內或作為專用硬體設備。每種類型的平台都有自己的一套強化最佳實踐。
- 租戶帳戶的可信度。如果您是擁有不受信任的租用戶帳戶的服務提供者，那麼您將面臨與僅使用受信任的內部租戶不同的安全問題。
- 您的組織遵循*哪些安全要求和慣例*。您可能需要遵守特定的監管或公司要求。

軟體升級強化指南

您必須保持StorageGRID系統和相關服務為最新版本以防禦攻擊。

StorageGRID軟體升級

只要有可能，您就應該將StorageGRID軟體升級到最新的主要版本或之前的主要版本。保持StorageGRID為最新狀態有助於減少已知漏洞的活躍時間並減少整體攻擊面。此外， StorageGRID的最新版本通常包含早期版本中未包含的安全性增強功能。

諮詢 "NetApp互通性表工具"（IMT）來決定您應該使用哪個版本的StorageGRID軟體。當需要修補程式時，NetApp會優先為最新版本建立更新。某些補丁可能與早期版本不相容。

- 要下載最新的StorageGRID版本和修補程序，請訪問 "NetApp下載： StorageGRID"。
- 若要升級StorageGRID軟體，請參閱"升級說明"。
- 若要套用修補程序，請參閱"StorageGRID修補程式程序"。

外部服務升級

外部服務可能存在間接影響StorageGRID 的漏洞。您應該確保StorageGRID所依賴的服務保持最新。這些服務包括 LDAP、KMS（或 KMIP 伺服器）、DNS 和 NTP。

有關受支援版本的列表，請參閱 "NetApp互通性表工具"。

升級虛擬機器管理程序

如果您的StorageGRID節點在 VMware 或其他虛擬機器管理程式上執行，則必須確保虛擬機器管理程式軟體和韌體是最新的。

有關受支援版本的列表，請參閱 "NetApp互通性表工具"。

升級到 **Linux** 節點

如果您的StorageGRID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，當這些更新可用時，您必須將韌體更新套用至易受攻擊的硬體。

有關受支援版本的列表，請參閱 "NetApp互通性表工具"。

StorageGRID網路強化指南

StorageGRID系統每個網格節點最多支援三個網路接口，可讓您為每個單獨的網格節點配置網路以滿足您的安全性和存取要求。

有關StorageGRID網路的詳細信息，請參閱"StorageGRID網路類型"。

網格網路指南

您必須為所有內部StorageGRID流量配置一個網格網路。所有網格節點都在網格網路上，並且它們必須能夠與所有其他節點通訊。

配置網格網路時，請遵循下列準則：

- 確保網路安全，免受不受信任的用戶端（例如開放網路上的用戶端）的攻擊。
- 如果可能的話，請將網格網路專門用於內部流量。管理網路和客戶端網路都有額外的防火牆限制，可以阻止外部流量流向內部服務。支援使用網格網路進行外部客戶端流量，但這種使用方式提供的保護層較少。
- 如果StorageGRID部署跨越多個資料中心，請在網格網路上使用虛擬私人網路 (VPN) 或等效網路為內部流量提供額外保護。
- 某些維護程序需要在主管理節點和所有其他網格節點之間的連接埠 22 上進行安全外殼 (SSH) 存取。使用外部防火牆限制對受信任用戶端的 SSH 存取。

管理網路指南

管理網路通常用於管理任務（使用網格管理器或 SSH 的受信任員工）以及與其他受信任服務（如 LDAP、DNS、NTP 或 KMS（或 KMIP 伺服器））進行通訊。但是， StorageGRID內部並不會強制執行這種用法。

如果您使用管理網絡，請遵循以下準則：

- 阻止管理網路上的所有內部流量連接埠。查看"內部連接埠列表"。
- 如果不受信任的用戶端可以存取管理網絡，請使用外部防火牆阻止對管理網路上的StorageGRID的存取。

客戶網路指南

客戶端網路通常用於租戶和與外部服務（例如 CloudMirror 複製服務或其他平台服務）進行通訊。但是，StorageGRID內部並不會強制執行這種用法。

如果您使用客戶端網絡，請遵循以下準則：

- 阻止客戶端網路上的所有內部流量連接埠。查看"內部連接埠列表"。
- 僅在明確配置的端點上接受入站用戶端流量。查看有關"管理防火牆控制"。

StorageGRID節點的強化指南

StorageGRID節點可部署在 VMware 虛擬機器上、Linux 主機上的容器引擎內或作為專用硬體設備。每種類型的平台和每種類型的節點都有自己的一套強化最佳實踐。

控制遠端 **IPMI** 對**BMC**的存取

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帳戶和密碼的人對您的StorageGRID設備進行低階硬體存取。如果您不需要遠端 IPMI 存取BMC，請停用此選項。

- 要控制 Grid Manager 中對BMC 的遠端 IPMI 訪問，請前往 **CONFIGURATION** > **Security** > **Security settings** > **Appliances**：
  - 清除「啟用遠端 IPMI 存取」複選框以停用 IPMI 對BMC的存取。
  - 勾選「啟用遠端 IPMI 存取」複選框以啟用對BMC 的IPMI 存取。

防火牆配置

作為系統強化過程的一部分，您必須檢查外部防火牆配置並進行修改，以便僅接受來自嚴格需要的 IP 位址和連接埠的流量。

StorageGRID在每個節點上都包含一個內部防火牆，透過讓您能夠控制對節點的網路存取來增強網格的安全性。你應該"管理內部防火牆控制"阻止除特定網格部署所需連接埠之外的所有連接埠上的網路存取。您在防火牆控制頁面上所做的設定變更將部署到每個節點。

具體來說，您可以管理以下領域：

- 特權位址：您可以允許選定的 IP 位址或子網路存取「管理外部存取」標籤上的設定已關閉的連接埠。
- 管理外部存取：您可以關閉預設開啟的端口，或重新開啟先前關閉的端口。
- 不受信任的客戶端網路：您可以指定節點是否信任來自客戶端網路的入站流量，以及在配置不受信任的客戶端網路時要開啟的其他連接埠。

雖然此內部防火牆針對一些常見威脅提供了額外的保護層，但它並不能消除對外部防火牆的需求。

有關StorageGRID使用的所有內部和外部連接埠的列表，請參閱"網路連接埠參考"。

禁用未使用的服務

對於所有StorageGRID節點，您應該停用或封鎖對未使用的服務的存取。例如，如果您不打算使用 DHCP，請

使用網格管理員關閉連接埠 68。選擇*設定* > 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、容器和共享硬體

對於所有StorageGRID節點，避免在與不受信任的軟體相同的實體硬體上執行StorageGRID 。如果StorageGRID和惡意軟體都存在於同一個實體硬體上，請不要假設虛擬機器管理程式保護將阻止惡意軟體存取受StorageGRID保護的資料。例如，Meltdown 和 Spectre 攻擊利用現代處理器中的關鍵漏洞，並允許程式竊取同一台電腦記憶體中的資料。

在安裝期間保護節點

安裝節點時，不允許不受信任的使用者透過網路存取StorageGRID節點。節點只有在加入電網後才會完全安全。

管理節點指南

管理節點提供系統設定、監控和日誌記錄等管理服務。當您登入網格管理器或租戶管理器時，您正在連線到管理節點。

請遵循下列準則來保護StorageGRID系統中的管理節點：

- 保護所有管理節點免受不受信任的用戶端（例如開放網路上的用戶端）的攻擊。確保不受信任的用戶端無法存取網格網路、管理網路或用戶端網路上的任何管理節點。
- StorageGRID群組控制對網格管理器和租用戶管理器功能的存取。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配置。
- 使用StorageGRID負載平衡器端點時，對於不受信任的用戶端流量，請使用網關節點而非管理節點。
- 如果您有不受信任的租用戶，請不要允許他們直接存取租用戶管理器或租用戶管理 API。相反，讓任何不受信任的租用戶使用租用戶入口網站或外部租用戶管理系統，與租用戶管理 API 進行互動。
- 或者，使用管理代理來更好地控制從管理節點到NetApp支援的AutoSupport通訊。請參閱"建立管理代理"。
- 或者，使用受限的 8443 和 9443 連接埠來分離網格管理器和租戶管理器通訊。封鎖共用連接埠 443 並將租用戶要求限製到連接埠 9443 以獲得額外保護。
- 或者，為網格管理員和租用戶使用者使用單獨的管理節點。

欲了解更多信息，請參閱"管理StorageGRID"。

儲存節點指南

儲存節點管理和儲存物件資料和元資料。遵循這些準則來保護StorageGRID系統中的儲存節點。

- 不允許不受信任的客戶端直接連接到儲存節點。使用由網關節點或第三方負載平衡器提供服務的負載平衡器端點。
- 不要為不受信任的租戶啟用出站服務。例如，為不受信任的租用戶建立帳戶時，不允許租用戶使用自己的身分來源，也不允許使用平台服務。請參閱"建立租用戶帳戶"。
- 對於不受信任的用戶端流量，請使用第三方負載平衡器。第三方負載平衡提供了更多的控制和額外的防禦攻擊層。
- 或者，使用儲存代理程式來更好地控制雲端儲存池和從儲存節點到外部服務的平台服務通訊。請參閱"建立儲存代理"。

- 或者，使用客戶端網路連線到外部服務。然後，選擇 **CONFIGURATION** > **Security** > **Firewall control** > **Untrusted Client Networks** 並指示儲存節點上的用戶端網路不受信任。儲存節點不再接受客戶端網路上的任何傳入流量，但它繼續允許平台服務的出站請求。

網關指南

網關節點提供可選的負載平衡接口，客戶端應用程式可以使用它來連接到StorageGRID。請遵循以下準則來保護StorageGRID系統中的任何網關節點：

- 配置和使用負載平衡器端點。看"負載平衡的注意事項" 。
- 對於不受信任的用戶端流量，在用戶端和網關節點或儲存節點之間使用第三方負載平衡器。第三方負載平衡提供了更多的控制和額外的防禦攻擊層。如果您確實使用第三方負載平衡器，仍然可以選擇將網路流量配置為透過內部負載平衡器端點或直接傳送到儲存節點。
- 如果您使用負載平衡器端點，則可以選擇讓用戶端透過用戶端網路連線。然後，選擇 **CONFIGURATION** > **Security** > **Firewall control** > **Untrusted Client Networks** 並指示網關節點上的用戶端網路不受信任。網關節點僅接受明確配置為負載平衡器端點的連接埠上的入站流量。

硬體設備節點指南

StorageGRID硬體設備專為在StorageGRID系統中使用而設計。一些設備可以用作儲存節點。其他設備可用作管理節點或網關節點。您可以將設備節點與基於軟體的節點結合起來，或部署完全工程化的全設備網格。

請遵循下列準則來保護StorageGRID系統中的任何硬體設備節點：

- 如果設備使用SANtricity System Manager 進行儲存控制器管理，則應防止不受信任的用戶端透過網路存取SANtricity System Manager。
- 如果設備具有基板管理控制器 (BMC)，請注意BMC管理連接埠允許低階硬體存取。僅將BMC管理連接埠連接到安全、可信任的內部管理網路。如果沒有可用的網絡，請將BMC管理連接埠保持未連線或阻塞狀態，除非技術支援要求BMC連線。
- 如果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件，請封鎖連接埠 623 上不受信任的流量。

> ⓘ 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帳戶和密碼的人對您的StorageGRID設備進行低階硬體存取。如果您不需要遠端 IPMI 存取BMC，請使用下列方法之一停用此選項：+ 在 Grid Manager 中，前往 設定 > 安全 > 安全設定 > 裝置，然後清除 *啟用遠端 IPMI 存取*複選框。+ 在網格管理 API 中，使用私有端點： `PUT /private/bmc` 。

- 對於包含使用SANtricity System Manager 管理的 SED、FDE 或 FIPS NL-SAS 磁碟機的設備型號， "啟用並配置SANtricity Drive Security" 。
- 對於包含使用StorageGRID Appliance Installer 和 Grid Manager 管理的 SED 或 FIPS NVMe SSD 的裝置型號， "啟用並配置StorageGRID磁碟機加密" 。
- 對於沒有 SED、FDE 或 FIPS 磁碟機的設備，啟用並設定StorageGRID軟體節點加密 "使用金鑰管理伺服器（KMS）"。

TLS 和 SSH 強化指南

您應該替換安裝期間建立的預設證書，並為 TLS 和 SSH 連線選擇適當的安全性原則。

證書強化指南

您應該用自己的自訂憑證取代安裝期間建立的預設憑證。

對於許多組織來說， StorageGRID網路存取的自簽名數位憑證不符合其資訊安全政策。在生產系統上，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：用於安全存取網格管理員、租用戶管理員、網格管理 API 和租用戶管理 API。
- **S3 API** 憑證：用於保護對儲存節點和網關節點的訪問，S3 用戶端應用程式使用這些憑證來上傳和下載物件資料。

看"管理安全證書"了解詳細資訊和說明。

> StorageGRID單獨管理用於負載平衡器端點的憑證。若要設定負載平衡器證書，請參閱"配置負載平衡器端點"。

使用自訂伺服器憑證時，請遵循下列準則：

- 證書應該有 `*subjectAltName*`與StorageGRID 的DNS 條目相符。有關詳細信息，請參閱第 4.2.1.6 節“主題備用名稱” "RFC 5280：PKIX 憑證和 CRL 設定檔" 。
- 盡可能避免使用通配符憑證。此指南的例外是 S3 虛擬託管樣式端點的證書，如果事先不知道儲存桶名稱，則需要使用萬用字元。
- 當您必須在憑證中使用通配符時，您應該採取額外措施來降低風險。使用通配符模式，例如 `*.s3.example.com`，並且不要使用 `s3.example.com`其他應用程式的後綴。此模式也適用於路徑式 S3 訪問，例如 `dc1-s1.s3.example.com/mybucket`。
- 將憑證到期時間設定為較短（例如 2 個月），並使用網格管理 API 自動進行憑證輪替。這對於通配符證書尤其重要。

此外，客戶端在與StorageGRID通訊時應使用嚴格的主機名稱檢查。

TLS 和 SSH 策略強化指南

您可以選擇安全性原則來決定使用哪些協定和密碼與用戶端應用程式建立安全的 TLS 連線以及與內部StorageGRID服務建立安全的 SSH 連線。

安全性策略控制 TLS 和 SSH 如何加密傳輸中的資料。作為最佳實踐，您應該停用應用程式相容性不需要的加密選項。使用預設的現代策略，除非您的系統需要符合通用標準或您需要使用其他密碼。

看"管理 TLS 和 SSH 策略"了解詳細資訊和說明。

其他強化指南

除了遵循StorageGRID網路和節點的強化指南外，您還應遵循StorageGRID系統其他區域的強化指南。

臨時安裝密碼

為了在安裝期間保護StorageGRID系統的安全，請在StorageGRID安裝 UI 或安裝 API 中的臨時安裝程式密碼頁面上設定密碼。設定後，此密碼適用於安裝StorageGRID 的所有方法，包括使用者介面、安裝 API 和 `configure-storagegrid.py`腳本。

有關詳細信息，請參閱：

- "在 Red Hat Enterprise Linux 上安裝StorageGRID"
- "在 Ubuntu 或 Debian 上安裝StorageGRID"
- "在 VMware 上安裝StorageGRID"
- "安裝StorageGRID設備"

日誌和審計訊息

始終以安全的方式保護StorageGRID日誌和稽核訊息輸出。從支援和系統可用性的角度來看， StorageGRID日誌和稽核訊息提供了寶貴的資訊。此外， StorageGRID日誌和稽核訊息輸出中包含的資訊和詳細資訊通常具有敏感性質。

設定StorageGRID以將安全事件傳送到外部系統日誌伺服器。如果使用 syslog 匯出，請選擇 TLS 和 RELP/TLS 作為傳輸協定。

查看"日誌檔參考"有關StorageGRID日誌的詳細資訊。看"審計訊息"有關StorageGRID審計訊息的詳細資訊。

NetAppAutoSupport

StorageGRID的AutoSupport功能可讓您主動監控系統的健康狀況，並自動將軟體包傳送至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，首次配置StorageGRID時會啟用將AutoSupport套件傳送至NetApp 。

可停用AutoSupport功能。但是， NetApp建議啟用它，因為如果StorageGRID系統出現問題， AutoSupport有助於加快問題識別和解決速度。

AutoSupport支援 HTTPS、HTTP 和 SMTP 作為傳輸協定。由於AutoSupport軟體包的敏感性， NetApp強烈建議使用 HTTPS 作為向NetApp發送AutoSupport軟體包的預設傳輸協定。

跨域資源共享（CORS）

如果您希望其他網域中的 Web 應用程式可以存取 S3 儲存桶及其中的對象，則可以為該儲存桶配置跨網域資源共用 (CORS)。一般來說，除非有必要，否則不要啟用 CORS。如果需要 CORS，請將其限制為受信任的來源。

請參閱"配置跨域資源共享（CORS）"。

外部安全設備

完整的強化解決方案必須解決StorageGRID以外的安全機制。使用額外的基礎設施設備來過濾和限制對StorageGRID 的存取是建立和維護嚴格安全態勢的有效方法。這些外部安全設備包括防火牆、入侵防禦系統 (IPS) 和其他安全設備。

對於不受信任的客戶端流量，建議使用第三方負載平衡器。第三方負載平衡提供了更多的控制和額外的防禦攻擊層。

勒索軟體緩解

遵循以下建議，協助保護您的物件資料免受勒索軟體攻擊 "使用StorageGRID防禦勒索軟體"。

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。