系統強化
StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/storagegrid-116/harden/index.html on October 03, 2025. Always check docs.netapp.com for the latest.

目錄

系統強化 1
- 系統強化：總覽 1
  - 強化StorageGRID 功能的一般考量 1
- 強化軟體升級準則 1
  - 升級StorageGRID 至更新版軟體 1
  - 升級至外部服務 2
  - 升級至Hypervisor 2
  - 升級至**Linux**節點 2
- 強化有關資訊網路的準則StorageGRID 2
  - Grid Network準則 2
  - 管理網路準則 3
  - 用戶端網路準則 3
- 強化有關節點的準則StorageGRID 3
  - 防火牆組態 3
  - 虛擬化、容器和共享硬體 4
  - 停用未使用的服務 4
  - 在安裝期間保護節點 4
  - 管理節點準則 4
  - 儲存節點準則 4
  - 閘道節點準則 5
  - 硬體應用裝置節點準則 5
- 伺服器憑證的強化準則 6
- 其他強化準則 6
  - 記錄與稽核訊息 7
  - NetApp AutoSupport 7
  - 跨來源資源共享（CORS） 7
  - 外部安全裝置 7

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。

以下是_NetApp弱點處理原則_。StorageGRID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。

相關資訊

"弱點處理原則"

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StorageGRID 、最新版的功能往往包含舊版不含的安全強化功能。

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StorageGRID 最新的版本資訊和即時修補程式、請前往StorageGRID 「更新版本」下載頁面。如需升級StorageGRID 版更新版的逐步說明、請參閱升級StorageGRID 版的說明。如需套用修補程式的指示、請參閱還原與維護指示。

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互通性對照表工具取得支援版本的清單。

相關資訊

"NetApp下載StorageGRID"

升級軟體

恢復與維護

"NetApp 互通性對照表工具"

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

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。請參閱平台安裝指南中的內部連接埠清單。
- 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。請參閱平台安裝指南中的內部連接埠清單。
- 只接受明確設定的端點上的傳入用戶端流量。請參閱 管理不受信任的用戶端網路。

相關資訊

網路準則

網格入門指南

管理StorageGRID

安裝Red Hat Enterprise Linux或CentOS

安裝Ubuntu或DEBIAN

安裝VMware

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。

使用自動管理的內部防火牆。StorageGRID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 所有供列舉的內部和外部連接埠清單、請參閱適用於您平台的安裝指南。

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 實體硬體上同時存在著不受保護的物件和惡意軟體、請勿假設Hypervisor保護功能可防止惡意軟體存取受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。

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存取CIFS或NFS的稽核共用、請封鎖或停用這些服務的存取。

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StorageGRID 網路存取節點。節點必須先加入網格、才會完全安全無虞。

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、請勿讓他們直接存取租戶管理程式或租戶管理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。
- 您也可以選擇使用管理Proxy、以更有效地控制AutoSupport 從管理節點到NetApp支援的各項功能通訊。如需管理StorageGRID 功能的說明、請參閱建立管理Proxy的步驟。
- 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《關於管理StorageGRID 功能的說明》。

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。

- 請勿讓不受信任的用戶端直接連線至儲存節點。使用閘道節點或協力廠商負載平衡器所服務的負載平衡器端點。
- 請勿為不受信任的租戶啟用傳出服務。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。請參閱管理StorageGRID 功能介紹中的建立租戶帳戶步驟。

- 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。如需管理StorageGRID 功能的說明、請參閱建立儲存Proxy的步驟。
- 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*>*網路*>*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：

- 在閘道節點上設定及使用負載平衡器端點、而非使用CLB服務。請參閱《管理StorageGRID VMware知識》中的管理負載平衡步驟。

  CLB服務已過時。

- 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。然後選取*組態*>*網路*>*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。
- 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。
- 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StorageGRID 您的不支援硬體應用裝置的安裝與維護說明。

相關資訊

- 安裝Red Hat Enterprise Linux或CentOS

- 安裝Ubuntu或DEBIAN
- 安裝VMware
- 管理StorageGRID
- 使用租戶帳戶
- SG100與SG1000服務應用裝置
- SG5600儲存設備
- SG5700儲存設備
- SG6000儲存設備

伺服器憑證的強化準則

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。

> 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、請參閱管理StorageGRID 指令中的設定負載平衡器端點步驟。

使用自訂伺服器憑證時、請遵循下列準則：

- 憑證應該有一個與DNS項目相符StorageGRID 的「*bectAltName*」、以供觀賞。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、如果儲存區名稱事先不知道、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。請使用萬用字元模式、例如「*.s3.example.com」、不要將「3.example.com」字尾用於其他應用程式。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。

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傳輸協定。

如需StorageGRID 更多有關資訊、請參閱監控和疑難排解的指示。請參閱稽核訊息的指示、以取得StorageGRID 更多有關不景稽核訊息的資訊。

NetApp AutoSupport

利用支援功能、您可以主動監控系統的健全狀況、並自動將訊息和詳細資料傳送給NetApp技術支援、貴組織的內部支援團隊或支援合作夥伴。AutoSupport StorageGRID根據預設、AutoSupport 第一次設定使用者支援時、會啟用向NetApp技術支援發出的功能性訊息StorageGRID 。

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由於資訊內容敏感、NetApp強烈建議使用HTTPS作為預設傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸協定、以將資訊傳送給NetApp支援部門。AutoSupport AutoSupport

或者、您可以設定管理Proxy、以便更有效地控制AutoSupport 從管理節點到NetApp技術支援之間的各種通訊。如需管理StorageGRID 功能的說明、請參閱建立管理Proxy的步驟。

跨來源資源共享（CORS）

如果您想要讓其他網域中的Web應用程式能夠存取S3儲存區中的儲存區和物件、可以設定S3儲存區的跨來源資源共享（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。

請參閱使用租戶帳戶說明中的「設定跨來源資源共用（CORS）的步驟」。

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。

相關資訊

監控及疑難排解

檢閱稽核記錄

使用租戶帳戶

管理StorageGRID

版權資訊

Copyright © 2025 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。