



StorageGRID 的系統強化

StorageGRID software

NetApp
February 12, 2026

目錄

StorageGRID 的系統強化	1
了解 StorageGRID 的系統強化	1
StorageGRID 軟體升級的強化準則	1
升級StorageGRID 至更新版軟體	1
升級至外部服務	1
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	2
用戶端網路準則	3
強化有關節點的準則StorageGRID	3
控制遠端 IPMI 對BMC的訪問	3
防火牆組態	3
停用未使用的服務	4
虛擬化、容器和共享硬體	4
在安裝期間保護節點	4
限制對硬體的實體訪問	4
管理節點準則	4
儲存節點準則	5
閘道節點準則	5
硬體應用裝置節點準則	5
StorageGRID 中 TLS 和 SSH 的強化準則	6
證書強化準則	6
TLS 和 SSH 原則的強化準則	7
管理外部 SSH 訪問	7
StorageGRID 中日誌、密碼和稽核訊息的強化準則	7
暫時安裝密碼	7
記錄與稽核訊息	7
NetApp AutoSupport	8
跨來源資源共享（CORS）	8
外部安全裝置	8
勒索軟體緩解	8

StorageGRID 的系統強化

了解 StorageGRID 的系統強化

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。

在您安裝和設定 StorageGRID 時、請使用這些準則來協助您達成任何指定的機密性、完整性和可用度安全目標。

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。這些最佳實踐必須包括限制實體存取以及保護實體資料中心和支援基礎設施的實體和環境安全。您還必須參考適用於您的業務和地理位置的任何適用監管標準和建議。

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 系統時、請考慮下列事項：

- * 您已實作三個 StorageGRID 網路 * 中的哪一個。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 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。
- * 租戶帳戶的信任程度 *。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。

StorageGRID 軟體升級的強化準則

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）以判斷您應該使用的 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

外部服務可能存在間接影響StorageGRID 的漏洞。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。

如需支援版本的清單，請參閱 ["NetApp 互通性對照表工具"](#)。

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。

如需支援版本的清單，請參閱 ["NetApp 互通性對照表工具"](#)。

* 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。

如需支援版本的清單，請參閱 ["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

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。請參閱的相關資訊["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。

控制遠端 IPMI 對BMC的訪問

您可以為所有包含 BMC 的應用裝置啟用或停用遠端 IPMI 存取。遠端 IPMI 介面可讓任何擁有 BMC 帳戶和密碼的人、對您的 StorageGRID 應用裝置進行低階硬體存取。如果不需要對 BMC 進行遠端 IPMI 存取、請停用此選項。

- 若要控制 Grid Manager 中對BMC 的遠端 IPMI 訪問，請前往 配置 > 安全性 > 安全設定 > 裝置：
 - 清除 * 啟用遠端 IPMI 存取 * 核取方塊、以停用對 BMC 的 IPMI 存取。
 - 選中 **Enable remote IPMI access**（啟用遠程 IPMI 訪問 *）複選框以啟用對 BMC 的 IPMI 訪問。

有關BMC強化的更多信息，請參閱 ["強化基板管理控制器"](#)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

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、藉此增強網絡的安全性。除了特定網絡部署所需的連接埠之外、您應該["管理內部防火牆控制"](#)防止所有連接埠上的網路存取。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。

有關StorageGRID使用的所有內部和外部連接埠的列表，請參閱["內部連接埠StorageGRID"](#)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 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Specter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。

限制對硬體的實體訪問

您必須將對StorageGRID硬體設備節點以及執行StorageGRID 的VMware 虛擬機器主機和 Linux 主機的實體存取權限制為僅限授權管理員。實體存取控制的一些範例包括鎖、警衛、實體屏障和視訊監控。

硬體設備節點設計為僅由授權管理員安裝和操作。不允許未經授權的管理員存取硬體設備節點。

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。
- 您也可以選擇使用管理 Proxy 、以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，請參閱的說明["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 、以更有效地控制雲端儲存池、以及從儲存節點到外部服務的平台服務通訊。請參閱的步驟["建立儲存 Proxy"](#)。
- 或者，使用客戶端網路連線到外部服務。然後，選擇*設定*>*安全*>*防火牆控制*>*不受信任的用戶端網路*，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。

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，則可以選擇讓用戶端透過用戶端網路連線。然後，選擇*設定*>*安全*>*防火牆控制*>*不受信任的用戶端網路*，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。

硬體應用裝置節點準則

用作作業系統的各種硬體應用。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絡。

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。

您可以建立 VLAN 來隔離BMC網路連線並限制BMC對受信任網路的網際網路存取。有關強制 VLAN 分離的更多信息，請參閱 ["強化基板管理控制器"](#)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阻塞狀態。技術支援可能會在支援案例期間請求臨時存取權限。

- 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。

+ 您還可以[停用遠端 IPMI 存取](#)。

- 對於包含 SED、FDE 或 FIPS NL-SAS 磁碟機的應用裝置機型、您可以使用 SANtricity System Manager 來管理 ["啟用和設定 SANtricity 磁碟機安全性"](#)。
- 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，["啟用及設定 StorageGRID 磁碟機加密"](#)。
- 對於沒有 SED、FDE 或 FIPS 磁碟機的設備，請使用金鑰管理伺服器 (KMS) ["啟用並配置StorageGRID軟體節點加密"](#)。

相關資訊

["了解SANtricity System Manager 中的磁碟機安全性"](#)

StorageGRID 中 TLS 和 SSH 的強化準則

您應該控制 SSH 訪問，替換預設 TLS 證書，並為 TLS 和 SSH 連線選擇適當的安全策略。

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 API 憑證 *：用於保護儲存節點和閘道節點的存取安全、S3 用戶端應用程式會使用這些節點來上傳和下載物件資料。

如需詳細資訊和指示、請參閱["管理安全性憑證"](#)。



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` 符合 StorageGRID DNS 項目的。如需詳細資訊、請參閱中的第 4.2.1.6 節「主旨替代名稱」["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。請使用萬用字元模式、例如 `*.s3.example.com`、而不要 `s3.example.com`、將後置字元用於其他應用程式。此模式也適用於路徑樣式的 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、符合 FIPS 140-2，或您需要使用其他密碼

如需詳細資訊和指示、請參閱["管理 TLS 和 SSH 原則"](#)。

管理外部 SSH 訪問

為了增強系統安全性，預設會阻止外部 SSH 存取。僅當需要執行需要入站 SSH 存取的任務（例如故障排除）時才啟用 SSH 存取。參考["管理外部 SSH 訪問"](#)了解詳細資訊和說明。

StorageGRID 中日誌、密碼和稽核訊息的強化準則

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。

暫時安裝密碼

若要在安裝期間保護 StorageGRID 系統、請在 StorageGRID 安裝 UI 或安裝 API 的暫存安裝程式密碼頁面上設定密碼。設定此密碼時、會套用至所有安裝 StorageGRID 的方法、包括使用者介面、安裝 API 和 ``configure-storagegrid.py`` 指令碼。

如需詳細資訊、請參閱：

- ["在基於軟體的節點上安裝StorageGRID"](#)
- ["安裝 StorageGRID 應用裝置"](#)

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。

如需 StorageGRID 記錄的詳細資訊、請參閱["記錄檔參考"](#)。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、貴組織的內部支援團隊或支援合作夥伴。根據預設、第一次設定 StorageGRID 時、會啟用傳送 AutoSupport 套件至 NetApp。

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協定。AutoSupport由於 AutoSupport 套件的敏感性質、NetApp 強烈建議使用 HTTPS 做為傳送 AutoSupport 套件至 NetApp 的預設傳輸通訊協定。

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["為儲存桶和物件配置 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

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"](#)。

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。