管理叢集安全性目標

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/active-iq-unified-manager-918/health-checker/concept_manage_cluster_security_objectives.html on November 13, 2026. Always check docs.netapp.com for the latest.

目錄

管理叢集安全性目標 . . . 1
在 Active IQ Unified Manager 中管理叢集安全性目標 . . . 1
正在評估哪些安全性標準 . . . 1
了解 Active IQ Unified Manager 如何評估安全性標準 . . . 1
了解 Active IQ Unified Manager 中的叢集法規遵循類別 . . . 1
了解 Active IQ Unified Manager 中的儲存 VM 法規遵循類別 . . . 3
了解 Active IQ Unified Manager 中的 Volume 法規遵循類別 . . . 4
了解 Active IQ Unified Manager 中的叢集和 SVM 法規遵循狀態 . . . 5
在 Active IQ Unified Manager 中檢視叢集和儲存虛擬機器的安全性狀態 . . . 5
在「安全性」頁面上檢視物件層級的安全性狀態 . . . 5
在「叢集」頁面上檢視所有叢集的安全性詳細資料 . . . 6
從儲存設備虛擬機器頁面檢視所有叢集的安全性詳細資料 . . . 6
在 Active IQ Unified Manager 中檢視可能需要軟體或韌體更新的安全性事件 . . . 6
在 Active IQ Unified Manager 中檢視叢集如何管理所有叢集上的使用者身分驗證 . . . 7
在 Active IQ Unified Manager 中檢視所有 Volume 的加密狀態 . . . 7
在 Active IQ Unified Manager 中查看所有 Volume 和儲存設備 VM 的反勒索軟體狀態 . . . 8
檢視所有具備反勒索軟體偵測功能之 Volume 的安全性詳細資料 . . . 8
檢視所有具有反勒索軟體偵測功能的儲存設備 VM 的安全性詳細資料 . . . 8
在 Active IQ Unified Manager 中查看所有作用中安全性事件 . . . 8
在 Active IQ Unified Manager 中新增安全性事件警報 . . . 9
在 Active IQ Unified Manager 中停用特定安全性事件 . . . 9
在 Active IQ Unified Manager 中檢視安全性事件 . . . 10

管理叢集安全性目標

在 **Active IQ Unified Manager** 中管理叢集安全性目標

Unified Manager 提供了一個儀表板，根據 *NetApp Security Hardening Guide for ONTAP 9* 中定義的建議，識別您的 ONTAP 叢集、儲存虛擬機器（SVM）和 Volume 的安全性。

安全性儀表板的目標是顯示 ONTAP 叢集中任何不遵守 NetApp 建議準則的地方，以便您可以修復這些潛力問題。大多數情況下，您可以使用 ONTAP System Manager 或 ONTAP CLI 來解決這些問題。您的組織可能不會遵循所有建議，因此在某些情況下，您無需進行任何變更。

如需詳細建議與解決方案，請參閱 "NetApp ONTAP 9 安全性強化指南"（TR-4569）。

除了報告安全性狀態外，Unified Manager 還會為任何有安全性違規的叢集或 SVM 產生安全性事件。您可以在「事件管理」清單頁面中追蹤這些問題，並可設定這些事件的警報，以便在發生新的安全性事件時通知您的儲存管理員。

如需詳細資訊，請參閱 "正在評估哪些安全性標準"。

正在評估哪些安全性標準

了解 **Active IQ Unified Manager** 如何評估安全性標準

一般而言，您的 ONTAP 叢集、儲存設備虛擬機器（SVM）和 Volume 的安全性標準，是根據 *NetApp Security Hardening Guide for ONTAP 9* 中定義的建議進行評估。

部分安全性檢查措施包括：

- 叢集是否使用安全的身分驗證方法，例如 SAML
- 對等叢集的通訊是否加密
- 儲存 VM 是否已啟用稽核日誌
- 您的 Volume 是否已啟用軟體或硬體加密

請參閱有關法規遵循類別與 "NetApp ONTAP 9 安全性強化指南"的主題，以取得詳細資訊。

> 從 Active IQ 平台報告的升級事件也被視為安全性事件。這些事件識別出的問題，需要您升級 ONTAP 軟體、節點韌體或作業系統軟體（針對安全性公告）才能解決。這些事件不會顯示在「安全性」面板中，但可以從「事件管理」清單頁面查看。

如需詳細資訊，請參閱 "管理叢集安全性目標"。

了解 **Active IQ Unified Manager** 中的叢集法規遵循類別

此表說明 Unified Manager 評估的叢集安全性法規遵循參數、NetApp 建議，以及該參數是否會影響叢集是否符合法規的整體判定。

叢集上存在不符合法規的 SVM 會影響叢集的法規遵循值。因此，在某些情況下，您可能需要先修復 SVM 的安全性問題，叢集的安全性才會被視為符合法規。

請注意，並非以下列出的所有參數都會在所有安裝中顯示。例如，如果您沒有對等叢集，或者您已在叢集上停用 AutoSupport，則您將不會在使用者介面頁面中看到「叢集對等」或「AutoSupport HTTPS 傳輸」項目。

參數	說明	建議	影響叢集法規遵循
全球 FIPS	指示是否啟用或停用全球 FIPS（聯邦資訊處理標準）140-2 法規遵循模式。啟用 FIPS 時，會停用 TLSv1 和 SSLv3，僅允許使用 TLSv1.1 和 TLSv1.2。	已啟用	是的
Telnet	指示是否啟用或停用對系統的 Telnet 存取。NetApp 建議使用 Secure Shell (SSH) 進行安全的遠端存取。	已停用	是的
不安全的 SSH 設定	指示 SSH 是否使用不安全的密碼，例如以 *cbc 開頭的密碼。	否	是的
登入橫幅	指示是否為存取系統的使用者啟用或停用登入橫幅。	已啟用	是的
叢集對等互連	指示對等叢集之間的通訊是加密或未加密。若要使此參數符合法規，來源和目的地叢集都必須設定加密。	加密	是的
網路時間協定	指示叢集是否設定了一個或多個 NTP 伺服器。為了實現備援和最佳服務，NetApp 建議您至少將三個 NTP 伺服器與叢集關聯。	已設定	是的
OCSP	從 9.14.1 開始，Active IQ Unified Manager 在儲存設備虛擬機器（SVM，以前稱為 Vserver）層級提供線上憑證狀態協定（OCSP）狀態資訊。這表示 OCSP 驗證會套用至與 SVM 建立的所有 SSL/TLS 連線，並確保這些連線中所使用憑證的完整性與有效性。	已啟用	否
遠端稽核日誌	指示日誌轉送（Syslog）是否加密。	加密	是的

參數	說明	建議	影響叢集法規遵循
AutoSupport HTTPS 傳輸	指示是否使用 HTTPS 作為傳送 AutoSupport 訊息至 NetApp 支援的預設傳輸協定。	已啟用	是的
預設管理員使用者	指示預設管理員使用者（內建）是否已啟用或停用。NetApp 建議鎖定（停用）任何不需要的內建帳戶。	已停用	是的
SAML 使用者	指出是否已設定 SAML。SAML 可讓您將多因素驗證（MFA）設定為單一登入的登入方法。	否	否
Active Directory 使用者	指出是否已設定 Active Directory。Active Directory 和 LDAP 是使用者存取叢集的首選驗證機制。	否	否
LDAP 使用者	指示是否已設定 LDAP。對於管理叢集的使用者而言，Active Directory 和 LDAP 是比本機使用者更首選的驗證機制。	否	否
憑證使用者	指示是否已設定憑證使用者登入叢集。	否	否
本機使用者	指示是否已設定本機使用者登入叢集。	否	否
遠端 Shell	指示是否啟用 RSH。基於安全性考量，應停用 RSH。建議使用 Secure Shell（SSH）進行安全的遠端存取。	已停用	是的
使用中的 MD5	指示 ONTAP 使用者帳戶是否使用安全性較低的 MD5 雜湊函數。建議將使用 MD5 雜湊的使用者帳戶移轉至更安全的加密雜湊函數，例如 SHA-512。	否	是的
憑證發行者類型	指示所使用的數位憑證類型。	CA 簽署	否

了解 **Active IQ Unified Manager** 中的儲存 **VM** 法規遵循類別

此表描述了 Unified Manager 評估的儲存設備虛擬機器（SVM）安全性法規遵循標準、NetApp 建議，以及該參數是否會影響 SVM 是否符合法規遵循的整體判定。

參數	說明	建議	影響 **SVM** 法規遵循
稽核記錄	指示是否啟用或停用稽核記錄。	已啟用	是的
不安全的 SSH 設定	指示 SSH 是否使用不安全的密碼，例如以 `cbc*`開頭的密碼。	否	是的
登入橫幅	指示是否為存取系統上 SVM 的使用者啟用或停用登入橫幅。	已啟用	是的
LDAP 加密	指示 LDAP 加密是否已啟用或停用。	已啟用	否
NTLM 驗證	指示 NTLM 驗證是否已啟用或停用。	已啟用	否
LDAP 有效負載簽章	指出 LDAP 有效負載簽章是否已啟用或停用。	已啟用	否
CHAP 設定	指示 CHAP 是否已啟用或停用。	已啟用	否
Kerberos V5	指示 Kerberos V5 驗證是否已啟用或停用。	已啟用	否
NIS 驗證	指出是否已設定使用 NIS 驗證。	已停用	否
FPolicy 狀態作用中	指示是否已建立 FPolicy。	是的	否
已啟用 SMB 加密	指示 SMB 簽章和密封是否未啟用。	是的	否
已啟用 SMB 簽章	指示是否未啟用 SMB 簽章。	是的	否

了解 **Active IQ Unified Manager** 中的 **Volume** 法規遵循類別

此表描述了 Unified Manager 評估的 Volume 加密參數，以確定 Volume 上的資料是否得到充分保護，防止未經授權的使用者存取。

請注意，Volume 加密參數不會影響叢集或儲存設備虛擬機器是否被視為符合法規。

參數	說明
軟體加密	顯示使用 NetApp Volume 加密 (NVE) 或 NetApp Aggregate 加密 (NAE) 軟體加密解決方案保護的 Volume 數量。
硬體加密	顯示使用 NetApp 儲存加密（NSE）硬體加密保護的 Volume 數量。
軟體和硬體加密	顯示受軟體和硬體加密雙重保護的 Volume 數量。
未加密	顯示未加密的 Volume 數量。

了解 Active IQ Unified Manager 中的叢集和 SVM 法規遵循狀態

當叢集和儲存設備虛擬機器（SVM）未能滿足根據《NetApp ONTAP 9 安全強化指南》中定義的建議所評估的任何安全性標準時，即被視為不符合法規。此外，當任何 SVM 被標記為不符合法規時，叢集也會被視為不符合法規。

安全性卡中的狀態圖示在法規遵循方面具有以下含義：

- - 此參數已依建議設定。
- - 此參數未依建議設定。
- - 叢集上未啟用該功能，或是未依建議設定參數，但此參數不影響物件的法規遵循。

請注意，Volume 加密狀態與叢集或 SVM 是否被視為符合法規無關。

在 Active IQ Unified Manager 中檢視叢集和儲存虛擬機器的安全性狀態

Active IQ Unified Manager 可讓您從介面的不同位置檢視環境中儲存設備物件的安全性狀態。您可以根據定義的參數收集和分析資訊及報告，並偵測受監控叢集和儲存設備虛擬機器上的可疑行為或未經授權的系統變更。

有關安全性建議，請參閱 "NetApp ONTAP 9 安全性強化指南"

在「安全性」頁面上檢視物件層級的安全性狀態

身為系統管理員，您可以使用 **Security** 頁面來取得資料中心和站台層級的 ONTAP 叢集和儲存設備虛擬機器安全性強度的可見度。支援的物件包括叢集、儲存設備虛擬機器和 Volume。請依照下列步驟操作：

步驟

1. 在左側導覽窗格中，按一下 儀表板。
2. 視您要檢視所有受監控叢集或單一叢集的安全性狀態而定，請選擇 所有叢集 或從下拉式選單中選擇單一叢集。
3. 點選 安全性 面板中的右箭頭。隨即顯示「安全性」頁面。

按一下長條圖、計數和 `View Reports`連結，即可進入 Volume 、叢集或儲存 VM 頁面，以便視需要檢視對應的詳細資料或產生報告。

「安全性」頁面顯示下列面板：

- 叢集法規遵循：資料中心內所有叢集的安全性狀態（符合法規或不符合法規的叢集數量）
- **Storage VM** 法規遵循：資料中心內所有 Storage VM 的安全性狀態（符合法規或不符合法規的 Storage VM 數量）
- **Volume Encryption**：您環境中所有 Volume 的 Volume 加密狀態（已加密或未加密的 Volume 數量）
- **Volume** 反勒索軟體狀態：環境中所有 Volume 的安全性狀態（已啟用或已停用反勒索軟體的 Volume 數量

）

- 叢集身分驗證和憑證：使用每種身分驗證方法（例如 SAML、Active Directory 或透過憑證和本機驗證）的叢集數量。此面板還會顯示憑證已過期或將在 60 天內過期的叢集數量。

在「叢集」頁面上檢視所有叢集的安全性詳細資料

叢集 / 安全性 詳細資訊頁面可讓您檢視叢集層級的安全性法規遵循狀態。

步驟

1. 在左側導覽窗格中，按一下 儲存設備 > 叢集。
2. 選擇 檢視 > 安全性 > 所有叢集。

顯示預設安全性參數，例如全域 FIPS、Telnet、不安全的 SSH 設定、登入橫幅、網路時間協定、AutoSupport HTTPS 傳輸以及叢集憑證過期狀態。

您可以點選 ⋮ 「更多選項」按鈕，選擇在 Unified Manager 的 安全性 頁面或 System Manager 中檢視安全性詳情。您需要擁有有效的憑證才能在 System Manager 中檢視詳情。

> ⓘ 如果叢集的憑證已過期，您可以按一下 **Cluster Certificate Validity** 下方的 `expired`，然後從 System Manager（9.10.1 及更新版本）將其續約。如果 System Manager 執行個體的版本早於 9.10.1，則無法按一下 `expired`。

從儲存設備虛擬機器頁面檢視所有叢集的安全性詳細資料

儲存虛擬機器 / 安全性 詳細資訊頁面可讓您檢視儲存虛擬機器層級的安全性法規遵循狀態。

步驟

1. 在左側導覽窗格中，按一下 儲存設備 > 儲存 **VM**。
2. 選擇 檢視 > 安全性 > 所有儲存虛擬機器。此時將顯示包含安全性參數的叢集清單。

您可以透過檢查安全性參數（例如儲存設備虛擬機器、叢集、登入橫幅、稽核日誌和不安全的 SSH 設定）來取得儲存設備虛擬機器安全性法規遵循的預設檢視。

您可以點選 ⋮ 「更多選項」按鈕，選擇在 Unified Manager 的 安全性 頁面或 System Manager 中檢視安全性詳情。您需要擁有有效的憑證才能在 System Manager 中檢視詳情。

如需 Volume 和儲存設備虛擬機器的反勒索軟體安全性詳細資訊，請參閱 "檢視所有 Volume 和 Storage VM 的反勒索軟體狀態"。

在 Active IQ Unified Manager 中檢視可能需要軟體或韌體更新的安全性事件

某些安全性事件的影響範圍為 “Upgrade”。這些事件由 Active IQ 平台報告，它們指出需要升級 ONTAP 軟體、節點韌體或作業系統軟體（針對安全性公告）才能解決的問題。

開始之前

您必須擁有操作員、應用程式管理員或儲存管理員角色。

對於某些問題，您可能需要立即採取修正行動，而其他問題則可以等到下次計劃維護再處理。您可以檢視所有這些事件，並將其指派給能夠解決問題的使用者。此外，如果您不想收到某些安全性升級事件的通知，此清單可以幫助您識別這些事件，以便您可以將其停用。

步驟

1. 在左側導覽窗格中，按一下 事件管理。

   預設情況下，所有作用中（新增和已確認）事件都會顯示在事件管理清單頁面上。

2. 從檢視功能表中，選擇 升級事件。

   該頁面顯示所有作用中的升級安全性事件。

在 Active IQ Unified Manager 中檢視叢集如何管理所有叢集上的使用者身分驗證

「安全性」頁面會顯示每個叢集上用來驗證使用者的驗證類型，以及使用每種類型存取叢集的使用者人數。這可讓您驗證使用者身分驗證是否按照組織定義的安全方式執行。

步驟

1. 在左側導覽窗格中，按一下 儀表板。
2. 在儀表板頂部，從下拉式選單中選擇 所有叢集。
3. 按一下 安全性 面板中的右箭頭，即會顯示 安全性 頁面。
4. 檢視 叢集驗證 卡，以查看使用每種驗證類型存取系統的使用者數量。
5. 檢視 叢集安全性 卡片，以檢視每個叢集上用於驗證使用者的驗證機制。

如果某些使用者使用不安全的方法，或使用 NetApp 不建議的方法存取系統，您可以停用該方法。

在 Active IQ Unified Manager 中檢視所有 Volume 的加密狀態

您可以檢視所有 Volume 及其目前加密狀態的清單，以便確定 Volume 上的資料是否得到充分保護，防止未經授權的使用者存取。

開始之前

您必須擁有操作員、應用程式管理員或儲存管理員角色。

可應用於 Volume 的加密類型有：

- 軟體 - 使用 NetApp Volume 加密（NVE）或 NetApp 彙總加密（NAE）軟體加密解決方案保護的 Volume。
- 硬體 - 使用 NetApp 儲存加密（NSE）硬體加密保護的 Volume。
- 軟體和硬體 - 受軟體和硬體加密雙重保護的 Volume。
- 無 - 未加密的 Volume。

步驟

1. 在左側導覽窗格中，按一下 儲存設備 > **Volume**。
2. 在「檢視」功能表中，選擇 健全狀況 > **Volume** 加密
3. 在 健全狀況：**Volume** 加密 檢視中，依 加密類型 欄位排序，或使用篩選器來顯示具有特定加密類型的 Volume，或是未加密的 Volume（加密類型為 “None”）。

在 **Active IQ Unified Manager** 中查看所有 **Volume** 和儲存設備 **VM** 的反勒索軟體狀態

您可以檢視所有 Volume 和儲存設備虛擬機器（SVM）的清單及其目前的防勒索軟體狀態，以便確定 Volume 和 SVM 上的資料是否得到充分保護，免受勒索軟體攻擊。

開始之前

您必須擁有操作員、應用程式管理員或儲存管理員角色。

有關不同反勒索軟體狀態的更多資訊，請參閱 "ONTAP：啟用反勒索軟體"。

檢視所有具備反勒索軟體偵測功能之 **Volume** 的安全性詳細資料

步驟

1. 在左側導覽窗格中，按一下 儲存設備 > **Volume**。
2. 在「檢視」功能表中，選擇 健全狀況 > 安全性 > 反勒索軟體
3. 在 安全性：反勒索軟體 檢視中，您可以依各種欄位排序或使用篩選器。

離線 Volume、受限 Volume、SnapLock Volume、FlexGroup Volume、FlexCache® Volume、僅限 SAN 的 Volume、已停止儲存設備虛擬機器的 Volume、儲存設備虛擬機器的根目錄 Volume，或資料保護 Volume，不支援反勒索軟體。

檢視所有具有反勒索軟體偵測功能的儲存設備 **VM** 的安全性詳細資料

步驟

1. 在左側導覽窗格中，按一下 儲存設備 **>** 儲存 **VM**。
2. 選取 檢視 **>** 安全性 **>** 反勒索軟體。此時將顯示具有反勒索軟體狀態的 SVM 清單。

未啟用 NAS 傳輸協定的儲存設備虛擬機器不支援反勒索軟體監控。

在 **Active IQ Unified Manager** 中查看所有作用中安全性事件

您可以檢視所有作用中的安全性事件，然後將每個事件指派給能夠解決問題的使用者。此外，如果您不想接收某些安全性事件，此清單可以幫助您識別要停用的事件。

開始之前

您必須擁有操作員、應用程式管理員或儲存管理員角色。

步驟

1. 在左側導覽窗格中，按一下 事件管理。

   預設情況下，新事件和已確認事件會顯示在事件管理清單頁面上。

2. 從「檢視」功能表中，選擇 作用中安全性事件。

   此頁面顯示過去 7 天內產生的所有新安全性事件與已確認的安全性事件。

在 Active IQ Unified Manager 中新增安全性事件警報

您可以像設定 Unified Manager 接收的任何其他事件一樣，為個別安全性事件設定警報。此外，如果您希望將所有安全性事件一視同仁，並將電子郵件傳送給同一個人，您可以建立單一警報，以便在觸發任何安全性事件時通知您。

開始之前

您必須擁有應用程式系統管理員或儲存系統管理員角色。

以下範例展示如何為 “Telnet Protocol Enabled” 安全性事件建立警報。如果已設定 Telnet 存取以進行叢集的遠端管理存取，這將會傳送警報。您可以使用相同的方法為所有安全性事件建立警報。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 警示設定。
2. 在 警報設定 頁面中，按一下 新增。
3. 在 新增警報 對話方塊中，按一下 名稱，然後輸入警報的名稱和執行摘要。
4. 按一下 資源，然後選擇要啟用此警報的叢集或叢集。
5. 按一下 事件 並執行下列動作：
   a. 在事件嚴重性清單中，選擇 警告。
   b. 在符合事件清單中，選擇 已啟用 **Telnet** 協定。
6. 按一下 動作 ，然後在 警示這些使用者 欄位中選取將收到警示電子郵件的使用者名稱。
7. 在此頁面上設定通知頻率、發出 SNMP taps 及執行指令碼的任何其他選項。
8. 按一下 **Save** 。

在 Active IQ Unified Manager 中停用特定安全性事件

所有事件預設啟用。您可以停用特定事件，以防止產生與您的環境無關的事件通知。如果您希望恢復接收已停用事件的通知，可以重新啟用這些事件。

開始之前

您必須擁有應用程式系統管理員或儲存系統管理員角色。

停用事件後，系統中先前產生的事件將被標記為過時，並且不會觸發針對這些事件設定的警報。啟用已停用的事件後，這些事件的通知將從下一個監控週期開始產生。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 事件設定。
2. 在 事件 設定頁面中，選擇下列選項之一來停用或啟用事件：

如果您想要.....	然後這樣做.....
停用事件	a. 按一下 **Disable** 。 b. 在「停用事件」對話方塊中，選擇 警告 嚴重程度。這是所有安全性事件的類別。 c. 在「符合事件」欄中，選擇要停用的安全性事件，然後按一下右箭頭將這些事件移至「停用事件」欄。 d. 點選 儲存並關閉。 e. 確認您已停用的事件是否顯示在「事件設定」頁面的清單檢視中。
啟用事件	a. 從已停用事件清單中，選取要重新啟用之事件的核取方塊。 b. 按一下 **Enable** 。

在 **Active IQ Unified Manager** 中檢視安全性事件

安全性事件會根據 *NetApp Security Hardening Guide for ONTAP 9* 中定義的參數，為您提供有關 ONTAP 叢集、儲存設備虛擬機器 (SVM) 和 Volume 的安全性狀態資訊。這些事件會通知您潛力問題，以便您評估其嚴重性並在必要時修復問題。

安全性事件按來源類型分組，包括事件和設陷名稱、影響層級和嚴重性。這些事件會出現在叢集和儲存設備虛擬機器事件類別中。

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。