# 管理叢集安全目標

## Active IQ Unified Manager

NetApp
October 15, 2025

# 目錄

# 管理叢集安全目標

Unified Manager 提供了一個儀表板，可根據《NetApp ONTAP 9 安全強化指南》中定義的建議來確定ONTAP叢集、儲存虛擬機器 (SVM) 和磁碟區的安全性。

安全儀表板的目標是顯示ONTAP叢集與NetApp建議指南不一致的任何區域，以便您可以修復這些潛在問題。大多數情況下，您可以使用ONTAP System Manager 或ONTAP CLI 來解決問題。您的組織可能不會遵循所有建議，因此在某些情況下您不需要進行任何更改。

查看 "NetApp ONTAP 9 安全強化指南"（TR-4569）以獲取詳細的建議和解決方案。

除了報告安全狀態之外，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。您可以在事件管理庫存頁面中追蹤這些問題，並且可以為這些事件配置警報，以便在發生新的安全事件時通知您的儲存管理員。

有關詳細信息，請參閱 "正在評估哪些安全標準"。

# 正在評估哪些安全標準

一般來說，您的ONTAP叢集、儲存虛擬機器 (SVM) 和磁碟區的安全標準將根據《NetApp ONTAP 9 安全強化指南》中定義的建議進行評估。

一些安全檢查包括：

- 叢集是否使用安全性身份驗證方法，例如 SAML
- 對等集群的通訊是否加密
- 儲存虛擬機器是否啟用了稽核日誌
- 您的磁碟區是否啟用了軟體或硬體加密

請參閱合規類別和 "NetApp ONTAP 9 安全強化指南"了解詳細資訊。

Active IQ平台報告的升級事件也被視為安全事件。這些事件標識了需要您升級ONTAP軟體、節點韌體或作業系統軟體（以取得安全公告）才能解決的問題。這些事件不會顯示在安全面板中，但可從事件管理庫存頁面取得。

有關詳細信息，請參閱 "管理叢集安全目標"。

## 集群合規性類別

此表描述了 Unified Manager 評估的叢集安全性合規性參數、 NetApp建議以及該參數是否影響叢集合規性的整體判定。

叢集上存在不合規的 SVM 將影響叢集的合規性值。因此在某些情況下，您可能需要先修復 SVM 的安全性問題，然後叢集安全性才被視為合規。

請注意，以下列出的每個參數並非都會出現在所有安裝中。例如，如果您沒有對等集群，或者您在集群上停用了AutoSupport ，那麼您將不會在 UI 頁面中看到 Cluster Peering 或AutoSupport HTTPS Transport 項目。

| 範圍 | 描述 | 推薦 | 影響集群合規性 |
| --- | --- | --- | --- |
| 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 合規模式。啟用 FIPS 時，TLSv1 和 SSLv3 被停用，並且只允許使用 TLSv1.1 和 TLSv1.2。 | 已啟用 | 是的 |
| 遠端登入 | 指示是否啟用或停用 Telnet 系統存取。NetApp 建議使用安全外殼 (SSH) 進行安全遠端存取。 | 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。 | 不 | 是的 |
| 登入橫幅 | 指示是否對存取系統的使用者啟用或停用登入橫幅。 | 已啟用 | 是的 |
| 集群對等連接 | 指示對等集群之間的通訊是否加密或未加密。必須在來源叢集和目標叢集上配置加密，此參數才被視為合規。 | 加密 | 是的 |
| 網路時間協定 | 指示叢集是否已配置一個或多個 NTP 伺服器。為了實現冗餘和最佳服務，NetApp建議您將至少三個 NTP 伺服器與叢集關聯。 | 已配置 | 是的 |
| OCSP | 從 9.14.1 開始， Active IQ Unified Manager在儲存虛擬機器（SVM，以前稱為 Vserver）層級提供線上憑證狀態協定 (OCSP) 狀態資訊。這意味著 OCSP 驗證適用於與 SVM 建立的所有 SSL/TLS 連接，並確保這些連接中使用的憑證的完整性和有效性。 | 已啟用 | 不 |
| 遠端審計日誌 | 指示日誌轉送（Syslog）是否加密。 | 加密 | 是的 |

| 範圍 | 描述 | 推薦 | 影響集群合規性 |
| --- | --- | --- | --- |
| AutoSupport HTTPS 傳輸 | 指示是否使用 HTTPS 作為向NetApp支援發送AutoSupport訊息的預設傳輸協定。 | 已啟用 | 是的 |
| 預設管理員用戶 | 指示預設管理員使用者（內建）是否啟用或停用。NetApp建議鎖定（停用）任何不必要的內建帳戶。 | 已停用 | 是的 |
| SAML 用戶 | 指示是否配置了 SAML。SAML 可讓您將多重驗證 (MFA) 設定為單一登入的登入方法。 | 不 | 不 |
| Active Directory 用戶 | 指示是否配置了 Active Directory。 Active Directory 和 LDAP 是使用者存取叢集的首選驗證機制。 | 不 | 不 |
| LDAP 用戶 | 指示是否配置了 LDAP。對於管理叢集的使用者而非本機使用者來說，Active Directory 和 LDAP 是首選的驗證機制。 | 不 | 不 |
| 憑證用戶 | 指示是否配置了憑證使用者來登入叢集。 | 不 | 不 |
| 本地用戶 | 指示是否配置本機使用者登入叢集。 | 不 | 不 |
| 遠端 Shell | 指示 RSH 是否啟用。出於安全原因，應停用 RSH。首選使用安全外殼 (SSH) 進行安全遠端存取。 | 已停用 | 是的 |
| MD5 使用中 | 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 MD5 Hashed 使用者帳戶遷移到更安全的加密雜湊函數（如 SHA-512）。 | 不 | 是的 |

| 範圍 | 描述 | 推薦 | 影響集群合規性 |
| --- | --- | --- | --- |
| 證書頒發者類型 | 指示使用的數位憑證的類型。 | CA簽名 | 不 |

## 儲存虛擬機器合規性類別

此表描述了 Unified Manager 評估的儲存虛擬機器 (SVM) 安全性合規性標準、 NetApp建議以及該參數是否會影響 SVM 是否符合規定的整體判斷。

| 範圍 | 描述 | 推薦 | 影響 **SVM** 合規性 |
| --- | --- | --- | --- |
| 審計日誌 | 指示審計日常記錄是否啟用或停用。 | 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*`。 | 不 | 是的 |
| 登入橫幅 | 指示是否為存取系統上的 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 加密是否啟用或停用。 | 已啟用 | 不 |
| NTLM 身份驗證 | 指示 NTLM 驗證是否啟用或停用。 | 已啟用 | 不 |
| LDAP 有效負載簽名 | 指示 LDAP 有效負載簽章是否啟用或停用。 | 已啟用 | 不 |
| CHAP 設定 | 指示 CHAP 是啟用還是停用。 | 已啟用 | 不 |
| Kerberos V5 | 指示是否啟用或停用 Kerberos V5 驗證。 | 已啟用 | 不 |
| NIS 身份驗證 | 指示是否配置了使用 NIS 身份驗證。 | 已停用 | 不 |
| FPolicy 狀態有效 | 指示是否創建了 FPolicy。 | 是的 | 不 |
| 已啟用 SMB 加密 | 指示是否未啟用 SMB-Signing & Sealing。 | 是的 | 不 |

| 範圍 | 描述 | 推薦 | 影響 **SVM** 合規性 |
| --- | --- | --- | --- |
| 已啟用 SMB 簽名 | 指示是否未啟用 SMB 簽章。 | 是的 | 不 |

### 容量合規性類別

下表描述了 Unified Manager 評估的捲加密參數，以確定磁碟區上的資料是否受到充分保護，以免被未經授權的使用者存取。

請注意，卷加密參數不會影響叢集或儲存虛擬機器是否被視為合規。

| 範圍 | 描述 |
| --- | --- |
| 軟體加密 | 顯示使用NetApp磁碟區加密 (NVE) 或NetApp聚合加密 (NAE) 軟體加密解決方案保護的磁碟區的數量。 |
| 硬體加密 | 顯示使用NetApp儲存加密 (NSE) 硬體加密保護的捲數。 |
| 軟體和硬體加密 | 顯示受軟體和硬體加密保護的捲的數量。 |
| 未加密 | 顯示未加密的捲數。 |

## 不合規意味著什麼

如果根據《NetApp ONTAP 9 安全強化指南》中定義的建議評估的任何安全標準未滿足，則叢集和儲存虛擬機器 (SVM) 被視為不合規。此外，當任何 SVM 被標記為不合規時，該叢集被視為不合規。

安全卡中的狀態圖示與其合規性有以下含義：

- - 參數配置符合建議要求。
- - 參數未依建議配置。
- - 叢集上未啟用此功能，或未依照建議配置該參數，但此參數對物件的合規性沒有貢獻。

請注意，磁碟區加密狀態不會影響叢集或 SVM 是否合規。

## 查看叢集和儲存虛擬機器的安全狀態

Active IQ Unified Manager可讓您從介面中的不同點檢視環境中儲存物件的安全狀態。您可以根據定義的參數收集和分析資訊和報告，並偵測受監控叢集和儲存虛擬機器上的可疑行為或未經授權的系統變更。

有關安全建議，請參閱 "NetApp ONTAP 9 安全強化指南"

## 在「安全性」頁面上查看物件層級的安全狀態

身為系統管理員，您可以使用「安全性」頁面來了解資料中心和網站層級的ONTAP叢集和儲存虛擬機器的安全強度。支援的物件是叢集、儲存虛擬機器和磁碟區。請依照以下步驟操作：

步驟

1. 在左側導覽窗格中，按一下「儀表板」。
2. 根據您是否要查看所有受監控叢集或單一叢集的安全狀態，選擇「所有叢集」或從下拉式選單中選擇單一叢集。
3. 按一下“安全性”面板中的右箭頭。將顯示“安全”頁面。

點擊條形圖、計數和 `View Reports`連結將帶您進入磁碟區、叢集或儲存虛擬機器頁面，以便您根據需要查看相應的詳細資訊或產生報告。

安全頁面顯示以下面板：

- 集群合規性：資料中心內所有集群的安全狀態（合規或不合規的集群數量）
- 儲存虛擬機器合規性：資料中心內所有儲存虛擬機器的安全狀態（合規或不合規的儲存虛擬機器數量）
- 磁碟區加密：您環境中所有磁碟區的磁碟區加密狀態（已加密或未加密的磁碟區數）
- 捲反勒索軟體狀態：您環境中所有磁碟區的安全狀態（啟用或停用反勒索軟體的捲數）
- 叢集身分驗證和憑證：使用每種驗證方法的叢集數量，例如 SAML、Active Directory 或透過憑證和本機驗證。此面板還顯示證書已過期或即將在 60 天內過期的群集數量。

## 在叢集頁面查看所有叢集的安全詳情

透過「叢集/安全」詳細資訊頁面，您可以查看叢集層級的安全合規性狀態。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「叢集」。
2. 選擇“檢視”>“安全性”>“所有叢集”。

顯示預設安全參數，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 傳輸和叢集憑證過期狀態。

您可以點選⋮更多選項按鈕並選擇在 Unified Manager 的 安全 頁面或系統管理員上查看安全性詳細資訊。您應該擁有有效的憑證才能查看系統管理員上的詳細資訊。

如果叢集的憑證已過期，您可以按一下 `expired`在*叢集憑證有效性*下，並從系統管理員（9.10.1 及更高版本）更新它。您無法點擊 `expired`如果系統管理員實例的版本早於 9.10.1。

## 從儲存虛擬機器頁面查看所有叢集的安全詳細信息

透過「儲存虛擬機器/安全」詳細資訊頁面，您可以查看儲存虛擬機器層級的安全合規性狀態。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「儲存虛擬機器」。

2. 選擇「檢視」>「安全性」>「所有儲存虛擬機器」。顯示具有安全參數的群集清單。

您可以透過檢查安全性參數（例如儲存虛擬機器、叢集、登入橫幅、稽核日誌和不安全的 SSH 設定）來預設了解儲存虛擬機器的安全性合規性。

您可以點選⋮更多選項按鈕並選擇在 Unified Manager 的 安全 頁面或系統管理員上查看安全性詳細資訊。您應該擁有有效的憑證才能查看系統管理員上的詳細資訊。

有關捲和存儲虛擬機的反勒索軟體安全詳細信息，請參閱"查看所有磁碟區和儲存虛擬機器的反勒索軟體狀態"。

# 查看可能需要軟體或韌體更新的安全性事件

## 某些安全事件的影響範圍為「升級」。這些事件由Active IQ平台報告，它們識別需要升級ONTAP軟體、節點韌體或作業系統軟體（用於安全公告）才能解決的問題。

開始之前

您必須具有操作員、應用程式管理員或儲存管理員角色。

您可能希望立即對其中一些問題採取糾正措施，而其他問題可能要等到下次預定的維護時再解決。您可以查看所有這些事件並將其指派給可以解決問題的使用者。此外，如果您不想收到某些安全升級事件的通知，此清單可以幫助您識別這些事件，以便您可以停用它們。

步驟

1. 在左側導覽窗格中，按一下「事件管理」。

   預設情況下，所有活動（新事件和已確認）事件都會顯示在事件管理庫存頁面上。

2. 從「檢視」功能表中，選擇「升級事件」。

   此頁面顯示所有活動的升級安全事件。

# 查看所有叢集上使用者身份驗證的管理方式

## 安全性頁面顯示用於對每個叢集上的使用者進行身份驗證的身份驗證類型，以及使用每種類型存取叢集的使用者數量。這使您能夠驗證使用者身份驗證是否按照組織的定義安全地執行。

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“所有集群”。
3. 按一下「安全」面板中的右箭頭，將顯示「安全」頁面。
4. 查看*群集身份驗證*卡片，以了解使用每種驗證類型存取系統的使用者數量。
5. 查看「叢集安全」卡以查看用於對每個叢集上的使用者進行身份驗證的身份驗證機制。

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

# 查看所有磁碟區的加密狀態

您可以查看所有磁碟區及其目前加密狀態的列表，以便確定磁碟區上的資料是否受到充分保護，以免被未經授權的使用者存取。

開始之前

您必須具有操作員、應用程式管理員或儲存管理員角色。

可以應用於卷的加密類型有：

- 軟體 - 使用NetApp磁碟區加密 (NVE) 或NetApp聚合加密 (NAE) 軟體加密解決方案保護的磁碟區。
- 硬體 - 使用NetApp儲存加密 (NSE) 硬體加密保護的磁碟區。
- 軟體和硬體 - 受軟體和硬體加密保護的捲。
- 無 - 未加密的捲。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在“檢視”選單中，選擇“健康”>“卷加密”
3. 在*健康：卷加密*視圖中，按*加密類型*欄位進行排序，或使用篩選器顯示具有特定加密類型或未加密的磁碟區（加密類型為「無」）。

# 查看所有磁碟區和儲存虛擬機器的反勒索軟體狀態

您可以查看所有磁碟區和儲存虛擬機器 (SVM) 及其目前反勒索軟體狀態的列表，以便確定磁碟區和 SVM 上的資料是否受到充分保護，免受勒索軟體攻擊。

開始之前

您必須具有操作員、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信息，請參閱"ONTAP：啟用反勒索軟體"。

## 查看所有具有反勒索軟體檢測功能的捲的安全詳細信息

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在“檢視”功能表中，選擇“健康”>“安全性”>“反勒索軟體”
3. 在*安全：反勒索軟體*視圖中，您可以按各個欄位進行排序或使用篩選器。

> 離線磁碟區、受限磁碟區、 SnapLock磁碟區、 FlexGroup磁碟區、 FlexCache磁碟區、僅 SAN 磁碟區、已停止的儲存虛擬機器的磁碟區、儲存虛擬機器的根磁碟區或資料保護磁碟區則不支援反勒索軟體。

### 查看所有具有反勒索軟體檢測功能的儲存虛擬機器的安全性詳細信息

步驟

1. 在左側導覽窗格中，按一下「儲存」>「儲存虛擬機器」。
2. 選擇「檢視」>「安全性」>「反勒索軟體」。顯示具有反勒索軟體狀態的 SVM 清單。

未啟用 NAS 協定的儲存虛擬機器不支援反勒索軟體監控。

# 查看所有活動的安全事件

您可以查看所有活動的安全事件，然後將每個事件指派給可以解決問題的使用者。此外，如果您不想接收某些安全事件，此清單可以幫助您識別要停用的事件。

開始之前

您必須具有操作員、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顯示在事件管理庫存頁面上。

2. 從「檢視」功能表中，選擇「活動安全事件」。

   此頁面顯示過去 7 天內產生的所有新的和已確認的安全事件。

# 新增安全事件警報

您可以為單一安全事件設定警報，就像 Unified Manager 收到的任何其他事件一樣。此外，如果您想平等對待所有安全事件並將電子郵件發送給同一個人，您可以建立單一警報，在觸發任何安全事件時通知您。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

下面的範例顯示如何為「`Telnet` **協定已啟用**」安全事件建立警報。如果配置了 Telnet 存取以對叢集進行遠端管理訪問，則將發送警報。您可以使用相同的方法為所有安全事件建立警報。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「警報設定」。
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描述。
4. 按一下*資源*並選擇要啟用此警報的叢集或叢集。
5. 按一下“事件”並執行以下操作：
   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*Telnet 協定已啟用*。

6. 按一下“操作”，然後在“警告這些使用者”欄位中選擇將接收警報電子郵件的使用者的姓名。
7. 配置此頁面上的任何其他選項，包括通知頻率、發出 SNMP tap 和執行腳本。
8. 點選“儲存”。

# 禁用特定安全事件

預設情況下，所有事件均啟用。您可以停用特定事件以防止產生那些在您的環境中不重要的事件的通知。如果您想要恢復接收已停用的事件的通知，您可以啟用它們。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

當您停用事件時，系統中先前產生的事件將被標記為過時，並且不會觸發為這些事件配置的警報。當您啟用已停用的事件時，將從下一個監控週期開始產生這些事件的通知。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「事件設定」。
2. 在「*事件*設定」頁面中，透過選擇以下選項之一來停用或啟用事件：

| 如果你想... | 然後這樣做... |
| --- | --- |
| 禁用事件 | a. 按一下“禁用”。<br>b. 在「停用事件」對話方塊中，選擇「警告」嚴重性。這是所有安全事件的類別。<br>c. 在「符合事件」列中，選擇要停用的安全性事件，然後按一下向右箭頭將這些事件移至「停用事件」列。<br>d. 按一下“儲存並關閉”。<br>e. 驗證您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，選取要重新啟用的一個或多個事件的複選框。<br>b. 按一下“啟用”。 |

# 安全事件

安全事件根據《NetApp ONTAP 9 安全性強化指南》中定義的參數，為您提供有關ONTAP叢集、儲存虛擬機器 (SVM) 和磁碟區的安全狀態的資訊。這些事件會通知您潛在的問題，以便您評估其嚴重性並在必要時解決問題。

安全事件按來源類型分組，包括事件和陷阱名稱、影響等級和嚴重性。這些事件出現在叢集和儲存虛擬機器事件

類別中。

## 版權資訊



## 商標資訊