# 正在評估哪些安全性準則

## Active IQ Unified Manager 9.13

NetApp
December 18, 2023

# 目錄

# 正在評估哪些安全性準則

一般而ONTAP 言、我們會根據《_ NetApp資訊安全強化指南ONTAP 》（英文）中所定義的各項建議、評估您的VMware叢集、儲存虛擬機器（SVM）和磁碟區的安全性條件。

部分安全性檢查包括：

- 叢集是否使用安全驗證方法、例如SAML
- 對等叢集的通訊是否已加密
- 儲存VM是否已啟用稽核記錄
- 您的磁碟區是否已啟用軟體或硬體加密

請參閱法規遵循類別和的主題 "《NetApp ONTAP 資訊安全強化指南》（英文）9" 以取得詳細資訊。

> 從該平台回報的升級事件Active IQ 也被視為安全事件。這些事件可識別解決方案需要您升級ONTAP 的問題、包括軟體、節點韌體或作業系統軟體（如需安全性摘要報告）。這些事件不會顯示在「安全性」面板中、但可從「事件管理」目錄頁取得。

如需詳細資訊、請參閱 "管理叢集安全目標"。

# 叢集規範類別

此表說明Unified Manager評估的叢集安全性法規遵循參數、NetApp建議、以及此參數是否會影響要抱怨或不抱怨的叢集整體判斷。

在叢集上使用不相容的SVM、將會影響叢集的法規遵循值。因此在某些情況下、您可能需要先修正SVM的安全性問題、然後才能將叢集安全性視為相容。

請注意、並非所有安裝都會顯示下列每個參數。例如、如果您沒有對等的叢集、或是在AutoSupport 叢集上停用了某些功能、AutoSupport 您就不會在UI頁面中看到叢集對等或是物件式HTTPS傳輸項目。

| 參數 | 說明 | 建議 | 影響叢集規範 |
| --- | --- | --- | --- |
| 全球FIPS | 指出是否已啟用或停用全域FIPS（聯邦資訊處理標準）140-2相容模式。啟用FIPS時、會停用TLSv1和SSLv3、而且只允許使用TLSv1.1和TLSv1.2。 | 已啟用 | 是的 |
| 遠端登入 | 表示是否已啟用或停用對系統的遠端登入存取。NetApp建議使用安全Shell（SSH）進行安全遠端存取。 | 已停用 | 是的 |

| 參數 | 說明 | 建議 | 影響叢集規範 |
| --- | --- | --- | --- |
| 不安全的SSH設定 | 指出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 | 表示存取系統的使用者是否已啟用或停用登入橫幅。 | 已啟用 | 是的 |
| 叢集對等 | 指出對等叢集之間的通訊是否已加密或未加密。必須在來源叢集和目的地叢集上設定加密、此參數才視為符合法規。 | 加密 | 是的 |
| 網路時間傳輸協定 | 指出叢集是否有一個或多個已設定的NTP伺服器。為了提供備援和最佳服務、NetApp建議您將至少三部NTP伺服器與叢集建立關聯。 | 已設定 | 是的 |
| OCSP | 指出ONTAP 在功能不適用OCSP（線上憑證狀態傳輸協定）的情況下、是否有應用程式在功能不適用的情況下進行通訊。列出不相容的應用程式。 | 已啟用 | 否 |
| 遠端稽核記錄 | 表示記錄轉送（Syslog）是否已加密或未加密。 | 加密 | 是的 |
| 支援HTTPS傳輸AutoSupport | 表示HTTPS是否作為預設傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸協定、以傳送AutoSupport 不支援的消息給NetApp。 | 已啟用 | 是的 |
| 預設管理使用者 | 指出預設的管理使用者（內建）是啟用還是停用。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 | 表示是否已設定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 |

| 參數 | 說明 | 建議 | 影響叢集規範 |
| --- | --- | --- | --- |
| Active Directory使用者 | 指出是否已設定Active Directory。Active Directory和LDAP是存取叢集的使用者偏好的驗證機制。 | 否 | 否 |
| LDAP 使用者 | 指出是否已設定 LDAP 。Active Directory和LDAP是管理叢集的使用者優先使用的驗證機制、而不使用本機使用者。 | 否 | 否 |
| 憑證使用者 | 指出是否已將憑證使用者設定為登入叢集。 | 否 | 否 |
| 本機使用者 | 指出本機使用者是否已設定登入叢集。 | 否 | 否 |
| 遠端Shell | 表示是否已啟用RSH。基於安全考量、應停用RSH。建議使用安全Shell（SSH）進行安全遠端存取。 | 已停用 | 是的 |
| 使用中的MD5 | 表示ONTAP 不安全的使用者帳戶是否使用不安全的MD5雜湊功能。建議使用將使用者帳戶的密碼編譯雜湊功能（如SHA-512）移轉至更安全的密碼編譯雜湊功能。 | 否 | 是的 |
| 憑證發卡行類型 | 指出所使用的數位憑證類型。 | CA簽署 | 否 |

# 儲存**VM**法規遵循類別

本表說明Unified Manager評估的儲存虛擬機器（SVM）安全性法規遵循條件、NetApp建議、以及此參數是否影響SVM的整體判斷是否符合申訴。

| 參數 | 說明 | 建議 | 影響**SVM**法規遵循 |
| --- | --- | --- | --- |
| 稽核記錄 | 表示稽核記錄已啟用或停用。 | 已啟用 | 是的 |

| 參數 | 說明 | 建議 | 影響**SVM**法規遵循 |
| --- | --- | --- | --- |
| 不安全的SSH設定 | 指出SSH是否使用不安全的密碼、例如開頭為的密碼 `cbc*`。 | 否 | 是的 |
| 登入橫幅 | 指出是否為存取系統上SVM的使用者啟用或停用登入橫幅。 | 已啟用 | 是的 |
| LDAP 加密 | 指出LDAP加密是啟用還是停用。 | 已啟用 | 否 |
| NTLM驗證 | 表示是否已啟用或停用NTLM驗證。 | 已啟用 | 否 |
| LDAP有效負載簽署 | 指出LDAP有效負載簽署是否已啟用或停用。 | 已啟用 | 否 |
| CHAP 設定 | 指出CHAP是否已啟用或停用。 | 已啟用 | 否 |
| Kerberos V5 | 指出是否已啟用或停用Kerberos V5驗證。 | 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 | 指出是否已建立FPolicy。 | 是的 | 否 |
| SMB加密已啟用 | 表示SMB簽署與密封是否未啟用。 | 是的 | 否 |
| SMB簽署已啟用 | 表示SMB簽署是否未啟用。 | 是的 | 否 |

# Volume法規遵循類別

下表說明Unified Manager評估的Volume加密參數、以判斷您磁碟區上的資料是否受到未獲授權使用者的適當保護。

請注意、磁碟區加密參數不會影響叢集或儲存VM是否符合法規要求。

| 參數 | 說明 |
| --- | --- |
| 軟體加密 | 顯示使用NetApp Volume Encryption（NVE）或NetApp Aggregate Encryption（NAE）軟體加密解決方案保護的磁碟區數量。 |
| 硬體加密 | 顯示使用NetApp儲存加密（NSE）硬體加密保護的磁碟區數量。 |
| 軟體與硬體已加密 | 顯示受軟體和硬體加密保護的磁碟區數目。 |
| 未加密 | 顯示未加密的磁碟區數目。 |