



## 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 .....	1
叢集規範類別 .....	1
儲存VM法規遵循類別 .....	3
Volume法規遵循類別 .....	4

# 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。

## 版權資訊

Copyright © 2023 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。