管理叢集安全目標

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

目錄

管理叢集安全目標 1
正在評估哪些安全性準則 1
不符合法規的意義 5
檢視叢集和儲存VM的安全狀態 5
檢視可能需要軟體或韌體更新的安全性事件 7
檢視如何在所有叢集上管理使用者驗證 7
檢視所有磁碟區的加密狀態 8
檢視所有磁碟區和儲存VM的勒索軟體狀態 8
檢視所有作用中的安全事件 9
新增安全性事件的警示 9
停用特定的安全性事件 10
安全事件 10

管理叢集安全目標

Unified Manager提供儀表板、可根據ONTAP 《_ NetApp ONTAP 資訊安全強化指南》（英文）中所定義的各項建議、識別您的叢集、儲存虛擬機器（SVM）和磁碟區的安全程度。

安全儀表板的目標是顯示ONTAP 任何不符合NetApp建議準則的領域、以便您修正這些潛在問題。在大多數情況ONTAP 下、您都會使用「功能不全系統管理程式」或ONTAP 「功能不全的CLI」來修正問題。您的組織可能不會遵循所有建議、因此在某些情況下、您不需要進行任何變更。

請參閱 "《NetApp ONTAP 資訊安全強化指南》（英文）9" （TR-4569）、以取得詳細建議與解決方案。

除了報告安全狀態之外、Unified Manager也會針對任何違反安全性的叢集或SVM產生安全性事件。您可以在「事件管理」資源清冊頁面中追蹤這些問題、也可以設定這些事件的警示、以便在發生新的安全事件時通知儲存管理員。

如需詳細資訊、請參閱 "正在評估哪些安全性準則"。

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
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

參數	說明	建議	影響叢集規範
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
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

參數	說明	建議	影響叢集規範
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
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

參數	說明	建議	影響**SVM**法規遵循
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。

不符合法規的意義

如果未ONTAP 符合根據《_ NetApp資訊安全強化指南》（英文）中所定義的各項建議來評估的任何安全性條件、則叢集與儲存虛擬機器（SVM）將視為不符合法規要求。此外、當任何SVM被標示為不相容時、叢集也會被視為不相容。

安全卡中的狀態圖示與其法規遵循相關、具有下列意義：

- -參數設定為建議。
- -參數未依建議進行設定。
- -叢集上未啟用此功能、或參數未依建議進行設定、但此參數並不影響物件的符合性。

請注意、磁碟區加密狀態並不會影響叢集或SVM是否符合法規要求。

檢視叢集和儲存**VM**的安全狀態

利用此功能、您可以從介面中的不同點、檢視環境中儲存物件的安全狀態。Active IQ Unified Manager您可以根據定義的參數來收集及分析資訊和報告、並偵測受監控叢集和儲存VM上的可疑行為或未獲授權的系統變更。

如需安全性建議、請參閱 "《NetApp ONTAP 資訊安全強化指南》（英文）9"

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 （安全性）頁面、在ONTAP 資料中心和站台層級、清楚掌握各個叢集和儲存VM的安全性強度。支援的物件包括叢集、儲存VM和Volume。請遵循下列步驟：

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狀態而定、請選取*所有叢集*或從下拉式功能表中選取單一叢集。
3. 按一下「安全性」面板中的向右箭頭。隨即顯示「安全性」頁面。

按一下橫條圖、計數和 `View Reports` 連結會帶您前往「Volumes（磁碟區）」、「Clusterss（叢集）」或「Storage VMs（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」頁面會顯示下列面板：

- 叢集法規遵循：資料中心內所有叢集的安全狀態（符合或不符合法規的叢集數目）
- 儲存虛擬機器法規遵循：資料中心內所有儲存虛擬機器的安全狀態（相容或不相容的儲存虛擬機器數量）
- * Volume Encryption*：環境中所有磁碟區的磁碟區加密狀態（加密或未加密的磁碟區數目）
- * Volume反勒索軟體狀態*：環境中所有磁碟區的安全狀態（啟用或停用反勒索軟體的磁碟區數量）
- 叢集驗證與憑證：使用各種驗證方法（例如SAML、Active Directory）或透過憑證與本機驗證的叢集數目。面板也會顯示憑證已過期或即將在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」詳細資料頁面可讓您檢視叢集層級的安全性法規遵循狀態。

步驟

1. 在左導覽窗格中、按一下*儲存>叢集*。
2. 選取*檢視>安全性>所有叢集*。

預設安全參數、例如Global FIPS、Telnet、不安全SSH設定、登入橫幅、網路時間傳輸協定、 顯示「支援HTTPS傳輸」、以及叢集憑證過期狀態。AutoSupport

您可以按一下 ⋮ 「更多選項」按鈕、然後選擇在Unified Manager * Security （安全性）頁面或System Manager上檢視安全性詳細資料。您應該擁有有效的認證資料、以便在System Manager上檢視詳細資料。

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System Manager（9.10.1及更新版本）續約。您無法按一下 `expired` 如果System Manager執行個體的版本早於9.10.1。

從「儲存**VM**」頁面檢視所有叢集的安全詳細資料

「儲存**VM** /安全性」詳細資料頁面可讓您檢視儲存VM層級的安全性法規遵循狀態。

步驟

1. 在左導覽窗格中、按一下*儲存設備>儲存設備VM*。
2. 選取*檢視>安全性>所有儲存VM*。隨即顯示具有安全參數的叢集清單。

您可以檢查安全參數、例如儲存VM、叢集、登入橫幅、稽核記錄和不安全的SSH設定、以預設檢視儲存VM的安全性法規遵循。

您可以按一下 ⋮ 「更多選項」按鈕、然後選擇在Unified Manager * Security （安全性）頁面或System Manager上檢視安全性詳細資料。您應該擁有有效的認證資料、以便在System Manager上檢視詳細資料。

如需磁碟區和儲存VM的反勒索軟體安全性詳細資料、請參閱 "檢視所有磁碟區和儲存VM的勒索軟體狀態"。

檢視可能需要軟體或韌體更新的安全性事件

有些安全事件會影響「升級」的影響範圍。這些事件是Active IQ 從支援中心平台報告、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（如需安全性建議）。

您需要的是什麼

您必須具有「操作員」、「應用程式管理員」或「儲存管理員」角色。

您可能想要針對其中的某些問題立即採取修正行動、但其他問題可能需要等到下次排定的維護作業才會發生。您可以檢視所有這些事件、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性升級事件的通知、此清單可協助您識別這些事件、以便停用這些事件。

步驟

1. 在左側導覽窗格中、按一下*事件管理*。

   依預設、所有作用中（新增和已確認）事件都會顯示在「事件管理」目錄頁面上。

2. 從「View（檢視）」功能表中選取*「Upgrade events（升級事件）」*。

   此頁面會顯示所有作用中的升級安全性事件。

檢視如何在所有叢集上管理使用者驗證

「安全性」頁面會顯示驗證每個叢集上使用者的類型、以及使用每種類型存取叢集的使用者數量。這可讓您確認使用者驗證是否已依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. 在儀表板頂端、從下拉式功能表中選取*所有叢集*。
3. 按一下「安全性」面板中的向右箭頭、就會顯示「安全性」頁面。
4. 查看*叢集驗證*卡、查看使用每種驗證類型存取系統的使用者人數。
5. 檢視*叢集安全性*卡、以檢視驗證每個叢集上使用者的驗證機制。

如果有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、您可以停用此方法。

檢視所有磁碟區的加密狀態

您可以檢視所有磁碟區及其目前加密狀態的清單、以便判斷您磁碟區上的資料是否受到適當保護、不受未獲授權的使用者存取。

您需要的是什麼

您必須具有「操作員」、「應用程式管理員」或「儲存管理員」角色。

可套用至磁碟區的加密類型包括：

- 軟體：使用NetApp Volume Encryption（NVE）或NetApp Aggregate Encryption（NAE）軟體加密解決方案進行保護的磁碟區。
- 硬體：使用NetApp儲存加密（NSE）硬體加密保護的磁碟區。
- 軟體與硬體：受軟體與硬體加密保護的磁碟區。
- 無-未加密的磁碟區。

步驟

1. 在左導覽窗格中、按一下「儲存設備>*磁碟區*」。
2. 在「檢視」功能表中、選取「健全狀況」>「磁碟區加密」
3. 在「健全狀況：**Volume Encryption**」（磁碟區加密）檢視中、依*加密類型*欄位排序、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」）。

檢視所有磁碟區和儲存**VM**的勒索軟體狀態

您可以檢視所有磁碟區和儲存VM（SVM）的清單、以及它們目前的反勒索軟體狀態、以便判斷您的磁碟區和SVM上的資料是否受到足夠的保護、免受勒索軟體攻擊。

您需要的是什麼

您必須具有「操作員」、「應用程式管理員」或「儲存管理員」角色。

如需不同勒索軟體狀態的詳細資訊、請參閱 "支援勒索軟體ONTAP"。

利用勒索軟體偵測功能檢視所有磁碟區的安全詳細資料

步驟

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

離線磁碟區、受限磁碟區、SnapLock VMware Volume、FlexGroup FlexCache SAN專用磁碟區、停止儲存VM的磁碟區、儲存VM的根磁碟區或資料保護磁碟區。

透過勒索軟體偵測功能、檢視所有儲存**VM**的安全詳細資料

步驟

1. 在左導覽窗格中、按一下*儲存設備>儲存設備VM*。
2. 選取*檢視>安全性>勒索軟體*。隨即顯示具有勒索軟體狀態的SVM清單。

未啟用NAS傳輸協定的儲存VM不支援勒索軟體監控。

檢視所有作用中的安全事件

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可以解決問題的使用者。此外、如果您不想接收某些安全性事件、此清單可協助您識別要停用的事件。

您需要的是什麼

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*。

   依預設、「事件管理」目錄頁會顯示「新增」和「已確認」事件。

2. 從「View（檢視）」功能表中、選取「* Active Security events（*作用中的安全事件

   此頁面會顯示過去7天內產生的所有「新增」和「已確認的安全性」事件。

新增安全性事件的警示

您可以設定個別安全事件的警示、就像Unified Manager收到的任何其他事件一樣。此外、如果您想要處理所有安全事件、並將電子郵件傳送給同一位人員、您可以建立單一警示、在觸發任何安全事件時通知您。

您需要的是什麼

您必須具有應用程式管理員或儲存管理員角色。

以下範例說明如何為「已啟用的Telnet傳輸協定」安全性事件建立警示。如果將遠端存取設定為遠端管理存取、則會傳送警示至叢集。您可以使用相同的方法為所有安全性事件建立警示。

步驟

1. 在左導覽窗格中、按一下*儲存管理*>*警示設定*。
2. 在「警示設定」頁面中、按一下「新增」。
3. 在「新增警示」對話方塊中、按一下「名稱」、然後輸入警示的名稱和說明。
4. 按一下*資源*、然後選取您要啟用此警示的叢集或叢集。
5. 按一下「事件」並執行下列動作：

a. 在「事件嚴重性」清單中、選取*警告*。

b. 在「Matching Event（相符事件）」清單中、選取「* Telnet* Protocol Enabled*（*啟用的

6. 按一下「動作」、然後在「警示這些使用者」欄位中選取接收警示電子郵件的使用者名稱。
7. 設定此頁面上的任何其他選項、以取得通知頻率、發出SNMP點選及執行指令碼。
8. 按一下「 * 儲存 * 」。

停用特定的安全性事件

預設會啟用所有事件。您可以停用特定事件、以防止為環境中不重要的事件產生通知。如果您想要繼續接收已停用的事件通知、您可以啟用這些事件。

您需要的是什麼

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會標示為已過時、且不會觸發針對這些事件所設定的警示。當您啟用停用的事件時、這些事件的通知會從下一個監控週期開始產生。

步驟

1. 在左導覽窗格中、按一下*儲存管理*>*事件設定*。
2. 在「*事件*設定」頁面中、選擇下列其中一個選項來停用或啟用事件：

如果您想要...	然後執行此動作...
停用事件	a. 按一下*停用*。 b. 在「停用事件」對話方塊中、選取*警告*嚴重性。這是所有安全事件的類別。 c. 在「Matching Event（符合事件）」欄中、選取您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. 按一下*儲存並關閉*。 e. 確認您停用的事件顯示在「事件設定」頁面的清單檢視中。
啟用事件	a. 從停用事件清單中、選取您要重新啟用的事件或事件核取方塊。 b. 按一下「啟用」。

安全事件

安全事件可根據ONTAP 《_ NetApp ONTAP 資訊安全強化指南》（英文）中定義的參數、提供有關VMware叢集、儲存虛擬機器（SVM）和磁碟區安全狀態的資訊。這些事件會通知您潛在的問題、以便您評估其嚴重性、並在必要時修正問題。

安全性事件會依來源類型分組、包括事件和陷阱名稱、影響層級和嚴重性。這些事件會出現在叢集和儲存VM事件類別中。

版權資訊

商標資訊