安全組態指南

2019 年 10 月 24 日

vRealize Automation 7.5

vmware®

您可以在 VMware 網站上找到最新的技術文件，網址如下：

https://docs.vmware.com/tw/

如果您對於本文件有任何意見，歡迎寄至：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

目錄

安全組態

1

安全組態可協助使用者評估和最佳化 vRealize Automation 部署的安全組態。

安全組態針對一般 vRealize Automation 環境說明安全部署的驗證和組態，以及提供資訊和程序來協助使用者在安全組態方面做出正確的選擇。

適合對象

此資訊適用於 vRealize Automation 系統管理員和負責系統安全維護和設定的其他使用者。

VMware 技術出版品詞彙表

VMware 技術出版品提供您可能不熟悉的專有詞彙表。如需 VMware 技術說明文件中所用專有詞彙的定義，請前往 http://www.vmware.com/support/pubs。

vRealize Automation 安全基準概觀

2

VMware 提供了全面性建議來協助您確認和設定 vRealize Automation 系統的安全基準。

使用 VMware 指定的適當工具和程序，確認和維護 vRealize Automation 系統強化的安全基準組態。某些 vRealize Automation 元件雖然是在已強化或半強化狀態下安裝的，但您應依照 VMware 安全性建議、公司安全性原則和已知威脅來檢閱並確認每個元件的組態。

vRealize Automation 安全性狀態

vRealize Automation 的安全性狀態假設整體安全環境基於系統和網路組態、組織安全性原則和安全性最佳做法。

在確認和設定 vRealize Automation 系統的強化時，請考量 VMware 強化建議所指明的下列各個方面。

- 安全部署
- 安全組態
- 網路安全性

為確保安全強化系統，請考量 VMware 建議和您的本機安全性原則，因為它們與這些概念領域都息息相關。

系統元件

考量 vRealize Automation 系統的強化和安全組態時，請確保您瞭解所有元件以及這些元件如何共同運作來支援系統功能。

規劃和實作安全系統時，請考量下列元件。

- vRealize Automation 應用裝置
- IaaS 元件

若要熟悉 vRealize Automation 元件以及這些元件如何共同運作，請參閱 VMware vRealize Automation 說明文件中心中的《基礎和概念》。如需一般 vRealize Automation 部署和架構的相關資訊，請參閱《參考架構》。

確認安裝媒體的完整性

3

使用者應務必在安裝 VMware 產品前確認安裝媒體的完整性。

請務必於下載 ISO、離線服務包或修補程式後確認 SHA1 雜湊，以確保下載檔案的完整性和真實性。如果您從 VMware 取得實體媒體，而安全封條已損壞，請將軟體退回 VMware 進行更換。

下載媒體後，請使用 MD5/SHA1 總和值確認下載的完整性。將 MD5/SHA1 雜湊輸出與 VMware 網站上公佈的值進行比較。SHA1 或 MD5 雜湊應與之相符。

如需有關確認安裝媒體完整性的詳細資訊，請參閱 http://kb.vmware.com/kb/1537。

強化 VMware 系統軟體基礎結構

4

在強化過程中，請對所部署來支援您 VMware 系統的軟體基礎結構進行評估，確認其符合 VMware 強化準則。

強化您的 VMware 系統之前，請先檢閱支援軟體基礎結構的安全缺陷並加以解決，以便建立完全強化且安全的環境。需要考量的軟體基礎結構元素包括作業系統元件、支援軟體，以及資料庫軟體。請根據製造商的建議及其他相關安全性通訊協定，解決這些元件與其他元件中的安全性問題。

本章節討論下列主題：

強化 VMware vSphere ® 環境

評估 VMware vSphere ® 環境，並確認已強制執行並維護適當層級的 vSphere 強化指引。

如需更多強化指引，請參閱 http://www.vmware.com/security/hardening-guides.html 。

在全面強化的環境中，VMware vSphere ® 基礎結構必須符合 VMware 所定義的安全性準則。

強化基礎結構即服務主機

請確認您的基礎結構即服務 Microsoft Windows 主機已根據 VMware 準則進行強化。

請檢閱適當 Microsoft Windows 強化與安全最佳做法準則中的建議，並確保您的 Windows Server 主機已適當進行強化。不遵循強化建議，可能會暴露 Windows 版本中不安全元件的已知安全性漏洞。

若要確認您的版本是否受支援，請參閱《vRealize Automation 支援對照表》。

請連絡您的 Microsoft 廠商，瞭解有關 Microsoft 產品強化做法的正確指引。

強化 Microsoft SQL Server

請確認 Microsoft SQL Server 資料庫符合 Microsoft 和 VMware 所建立的安全性準則。

請檢閱適當 Microsoft SQL Server 強化與安全最佳做法準則中的建議。請檢閱所有 Microsoft 資訊安全佈告欄，瞭解有關所安裝 Microsoft SQL Server 版本的資訊。不遵循強化建議，可能會暴露 Microsoft SQL Server 版本中不安全元件的已知安全性漏洞。

若要確認您的 Microsoft SQL Server 版本是否受支援，請參閱《vRealize Automation 支援對照表》。

如需 Microsoft 產品強化做法的指引，請連絡您的 Microsoft 廠商。

強化 Microsoft .NET

在全面強化的環境中，Microsoft .NET 必須符合 Microsoft 和 VMware 所提供的安全性準則。

請檢閱適當 .NET 強化與安全最佳做法準則中提供的建議。另外，亦請檢閱所有 Microsoft 資訊安全佈告欄，瞭解有關所使用 Microsoft SQL Server 版本的資訊。不遵循強化建議，可能會暴露不安全 Microsoft.NET 元件的已知安全性漏洞。

若要確認您的 Microsoft.NET 版本是否受支援，請參閱《vRealize Automation 支援對照表》。

如需 Microsoft 產品強化做法的指引，請連絡您的 Microsoft 廠商。

強化 Microsoft Internet Information Services (IIS)

請確認您的 Microsoft Internet Information Services (IIS) 符合所有的 Microsoft 和 VMware 安全性準則。

請檢閱適當 Microsoft IIS 強化與安全最佳做法準則中提供的建議。另外，亦請檢閱所有 Microsoft 資訊安全佈告欄，瞭解有關所使用 IIS 版本的資訊。不遵循強化建議，可能會暴露已知安全性漏洞。

若要確認您的版本是否受支援，請參閱《vRealize Automation 支援對照表》。

如需 Microsoft 產品強化做法的指引，請連絡您的 Microsoft 廠商。

檢閱安裝的軟體

5

因為第三方軟體和未使用軟體中的漏洞會增加未經授權的系統存取和中斷可用性的風險，所以檢閱 VMware 主機上安裝的所有軟體並對其使用情況進行評估非常重要。

請勿在 VMware 主機上安裝系統安全作業不需要的軟體。解除安裝未使用或無關的軟體。

清查已安裝的不受支援軟體

評估 VMware 部署和已安裝產品的詳細目錄，確認未安裝任何無關的不受支援軟體。

如需有關第三方產品支援原則的詳細資訊，請參閱 VMware 支援文章，網址為 https://www.vmware.com/support/policies/thirdparty.html。

確認第三方軟體

VMware 不支援亦不建議安裝未經測試和驗證的第三方軟體。在 VMware 主機上安裝不安全、未修補或未經驗證的第三方軟體，可能會使系統遭受未經授權的存取和中斷可用性風險。如果必須使用不受支援的第三方軟體，請諮詢第三方廠商以瞭解安全組態和修補需求。

VMware 安全性建議和修補程式

6

為維護系統的最大安全性，請遵循 VMware 安全性建議並套用所有相關修補程式。

VMware 發行了產品的安全性建議。請關注這些建議，以確保您的產品可抵禦已知威脅。

評估 vRealize Automation 安裝、修補和升級歷程記錄，確認已遵循並強制執行發行的 VMware 安全性建議。

如需有關最新 VMware 安全性建議的詳細資訊，請參閱 http://www.vmware.com/security/advisories/。

安全組態

7

視系統組態需要，確認並更新 vRealize Automation 虛擬應用裝置和基礎結構即服務元件的安全性設定。此外，還請確認並更新其他元件和應用程式的組態。

安全地設定 vRealize Automation 安裝涉及個別處理每個元件的組態，以及處理元件共同運作時的組態。請考量所有系統元件共同運作的組態，以達成合理的安全基準。

本章節討論下列主題：

保護 vRealize Automation 應用裝置

根據您的系統組態，視需要驗證並更新 vRealize Automation 應用裝置的安全性設定。

設定虛擬應用裝置及其主機作業系統的安全性設定。此外，也請設定或驗證其他相關元件與應用程式的組態。在某些情況下，您需要驗證現有設定，而在其他情況下，您必須變更或新增設定以便達成適當的組態。

變更根密碼

您可以變更 vRealize Automation 應用裝置的根密碼。

程序

1 以根使用者身分登入 vRealize Automation 應用裝置管理介面。

https://*vrealize-automation-appliance-FQDN*:5480

2 按一下**管理**索引標籤。

3 按一下**管理**子功能表。

4 在**目前管理員密碼**文字方塊中輸入現有密碼。

5 在**新管理員密碼**文字方塊中輸入新密碼。

6 在**重新輸入新管理員密碼**文字方塊中輸入新密碼。

7 按一下**儲存設定**。

確認根密碼雜湊和複雜性

確認根密碼符合貴組織的公司密碼複雜性需求。

需要驗證根密碼複雜性，因為根使用者可以略過套用到使用者帳戶的 pam_cracklib 模組密碼複雜性檢查。

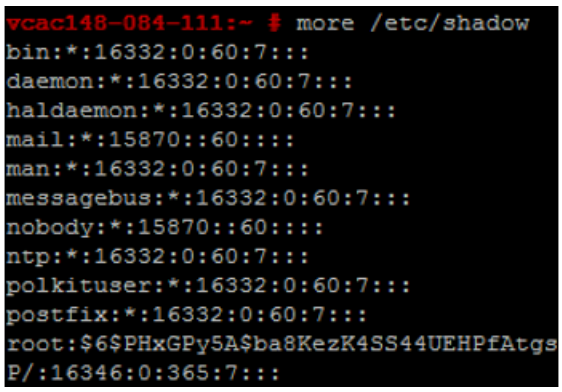
帳戶密碼必須以表示 SHA512 雜湊的 6 開頭。這是所有已強化應用裝置的標準雜湊。

程序

1 若要確認根密碼的雜湊，請以根使用者身分登入並執行 `# more /etc/shadow` 命令。

此時會顯示雜湊資訊。

圖 7-1. 密碼雜湊結果



2 如果根密碼不包含 SHA512 雜湊，請執行 `passwd` 命令進行變更。

所有已強化的應用裝置都針對 `pw_history` 模組啟用了 `enforce_for_root`，可在 `/etc/pam.d/common-password` 檔案中找到。依預設，系統會記住最後五個密碼。每個使用者的舊密碼皆儲存在 `/etc/securetty/passwd` 檔案中。

確認根密碼歷程記錄

確認對根帳戶強制執行密碼歷程記錄。

所有已強化的應用裝置都針對 pw_history 模組啟用了 `enforce_for_root`，可在 `/etc/pam.d/common-password` 檔案中找到。依預設，系統會記住最後五個密碼。每個使用者的舊密碼皆儲存在 `/etc/securetty/passwd` 檔案中。

程序

1 執行下列命令：

```
cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so
```

2 確保傳回的結果中出現 `enforce_for_root`。

```
password required pam_pwhistory.so enforce_for_root remember=5 retry=3
```

管理密碼到期

依據組織的安全性原則設定所有帳戶密碼到期。

依預設，所有強化的 VMware 虛擬應用裝置帳戶使用 60 天密碼到期。在大多數強化的應用裝置上，根帳戶設為 365 天密碼到期。最佳做法是確認所有帳戶的到期符合安全性和作業需求標準。

如果根密碼到期，您無法恢復。您必須實作站台專屬原則，以防止管理和根密碼到期。

程序

1 以根使用者身分登入虛擬應用裝置機器，然後執行下列命令以確認所有帳戶的密碼到期。

```
# cat /etc/shadow
```

密碼到期是陰影檔案的第五個欄位 (欄位以冒號分隔)。根到期以天數設定。

圖 7-2. 密碼到期欄位

2 若要修改根帳戶的到期，請執行下列格式的命令。

```
# passwd –x 365 root
```

在此命令中，365 指定密碼到期前的天數。使用相同命令修改任何使用者、以特定帳戶替代「根」，並取代天數以滿足組織的到期標準。

管理安全殼層和管理帳戶

對於遠端連線，所有強化的應用裝置包含安全殼層 (SSH) 通訊協定。僅在必要時使用 SSH，並且適當地管理 SSH 以維持系統安全性。

SSH 是支援遠端連線至 VMware 虛擬應用裝置的互動式命令列環境。依預設，SSH 存取需要高權限使用者帳戶認證。根使用者 SSH 活動通常會略過角色型存取控制 (RBAC) 並稽核虛擬應用裝置的控制。

最佳做法是在生產環境中停用 SSH，然後將其啟用，以僅疑難排解您無法透過其他方法解決的問題。僅當需要用於特定目的並依據組織的安全性原則時，將其維持在啟用狀態。vRealize Automation 應用裝置上預設會停用 SSH。視 vSphere 組態而定，當您部署開放虛擬化格式 (OVF) 範本時可能會啟用或停用 SSH。

判定機器上是否已啟用 SSH 的簡單測試是嘗試使用 SSH 開啟連線。如果連線開啟並要求認證，則 SSH 會啟用且可用於連線。

安全殼層根使用者帳戶

因為 VMware 應用裝置不包含預先設定的使用者帳戶，依預設，根帳戶可以使用 SSH 直接登入。儘快以根使用者身分停用 SSH。

為符合不可否認性的符合性標準，所有強化的應用裝置上的 SSH 伺服器都預先設定 AllowGroups wheel 項目，以限制 SSH 存取次要群組 wheel。針對職責分離，您可以修改 `/etc/ssh/sshd_config` 檔案中的 AllowGroups wheel 項目以使用其他群組 (如 sshd)。

針對超級使用者存取，已使用 `pam_wheel` 模組啟用 wheel 群組，因此 wheel 群組的成員可以將使用者切換為根使用者，其中需要根密碼。群組分離可讓使用者透過 SSH 連線至應用裝置，但是不可以將使用者切換為根使用者。請勿在 AllowGroups 欄位中移除或修改其他項目，這可確保適當的應用裝置功能。進行變更後，您必須透過執行命令 `# service sshd restart` 重新啟動 SSH 精靈。

啟用或停用 vRealize Automation 應用裝置上的安全殼層

僅在進行疑難排解時，才啟用 vRealize Automation 應用裝置上的安全殼層 (SSH)。在正常生產運作期間，請停用這些元件上的 SSH。

您可以使用 vRealize Automation 應用裝置管理介面，啟用或停用 vRealize Automation 應用裝置上的 SSH。

程序

1 以根使用者身分登入 vRealize Automation 應用裝置管理介面。

https://*vrealize-automation-appliance-FQDN*:5480

2 按一下**管理**索引標籤。

3 按一下**管理**子功能表。

4 選取 **SSH 服務啟用**核取方塊來啟用 SSH，或取消選取該核取方塊來停用 SSH。

5 按一下**儲存設定**儲存變更。

為安全殼層建立本機管理員帳戶

安全性最佳做法是在虛擬應用裝置主機上為安全殼層 (SSH) 建立並設定本機管理帳戶。此外，在建立適當的帳戶後，移除根 SSH 存取權。

為 SSH 或次要 wheel 群組成員 (或兩者) 建立本機管理帳戶。停用直接根存取權前，請先測試獲授權管理員能否使用 AllowGroups 存取 SSH，以及能否使用 wheel 群組將使用者切換為根使用者。

程序

1 透過適當的使用者名稱，以根使用者身分登入虛擬應用裝置並執行下列命令。

```
# useradd –g users <username> –G wheel –m –d /home/username
             # passwd username
```

Wheel 是 AllowGroups 中為 SSH 存取指定的群組。若要新增多個次要群組，請使用 `–G wheel,sshd`。

2 切換至使用者並提供新密碼，以強制執行密碼複雜性檢查。

```
# su -username
    # username@hostname:~>passwd
```

如果符合密碼複雜性，密碼便會更新。如果不符合密碼複雜性，密碼會還原為原始密碼，您必須重新執行密碼命令。

3 若要移除對 SSH 的直接登入，請修改 `/etc/ssh/sshd_config` 檔案，將 `(#)PermitRootLogin yes` 取代為 `PermitRootLogin no`。

或者，您也可以在虛擬應用裝置管理介面 (VAMI) 中，透過選取或取消選取**管理員**索引標籤上的**已啟用管理員 SSH 登入**核取方塊，來啟用/停用 SSH。

後續步驟

停用以根使用者身分直接登入。依預設，強化的應用裝置允許透過主控台直接登入至根目錄。在您建立不可否認的管理帳戶並測試其 su-root wheel 存取權後，請以根使用者身分編輯 `/etc/security` 檔案，將 `tty1` 項目取代為 `console`，以停用直接根登入。

1 在文字編輯器中開啟 `/etc/securetty` 檔案。

2 找到 `tty1` 並將其取代為 `console`。

3 儲存並關閉檔案。

強化安全殼層伺服器組態

只要可以，所有 VMware 應用裝置都有已強化的預設組態。使用者可以透過在組態檔的全域選項區段中檢查伺服器與用戶端服務設定，來確認其組態是否經過適當強化。

程序

1 在 VMware 應用裝置上開啟 `/etc/ssh/sshd_config` 伺服器組態檔，並確認其中設定均正確無誤。

設定	狀態
伺服器精靈通訊協定	Protocol 2
CBC 加密	aes256-ctr 和 aes128-ctr
TCP 轉送	AllowTCPForwarding no
伺服器閘道連接埠	Gateway Ports no
X11 轉送	X11Forwarding no
SSH 服務	請使用 AllowGroups 欄位並指定允許的群組存取權。請新增適當成員至此群組。
GSSAPI 驗證	如果未使用，則為 GSSAPIAuthentication no
Keberos 驗證	如果未使用，則為 KeberosAuthentication no
本機變數 (AcceptEnv 全域選項)	請設定為 `disabled by commenting out` 或 `enabled for LC_* or LANG variables`

設定	狀態
通道組態	PermitTunnel no
網路工作階段	MaxSessions 1
使用者並行連線	對於根使用者與任何其他使用者，設定為 1。 `/etc/security/limits.conf` 檔案也需要以相同設定進行設定。
嚴格模式檢查	Strict Modes yes
權限分離	UsePrivilegeSeparation yes
rhosts RSA 驗證	RhostsESAAuthentication no
壓縮	Compression delayed 或 Compression no
訊息驗證代碼	MACs hmac-sha1
使用者存取限制	PermitUserEnvironment no

2 儲存變更並關閉此檔案。

強化安全殼層用戶端組態

在系統強化過程中，請確認 SSH 用戶端經過強化，方法是檢查虛擬應用裝置主機上的 SSH 用戶端組態檔，確定其設定符合 VMware 準則。

程序

1 開啟 SSH 用戶端組態檔 `/etc/ssh/ssh_config`，並確認全域選項區段內的設定均正確無誤。

設定	狀態
用戶端通訊協定	Protocol 2
用戶端閘道連接埠	Gateway Ports no
GSSAPI 驗證	GSSAPIAuthentication no
本機變數 (SendEnv 全域選項)	請僅提供 LC_* 或 LANG 變數
CBC 加密	只有 aes256-ctr 和 aes128-ctr
訊息驗證代碼	僅在 `MACs hmac-sha1` 項目中使用

2 儲存變更並關閉此檔案。

確認安全殼層金鑰檔案權限

為了盡可能減少惡意攻擊，請維護虛擬應用裝置主機上的關鍵 SSH 金鑰檔案權限。

在設定或更新 SSH 組態後，請務必確認下列 SSH 金鑰檔案權限未發生變更。

- 位於 `/etc/ssh/*key.pub` 的公開主機金鑰檔案由根使用者擁有且權限設定為 0644 (-rw-r--r--)。
- 位於 `/etc/ssh/*key` 的私密主機金鑰檔案由根使用者擁有且權限設定為 0600 (-rw------)。

確認 SSH 金鑰檔案權限

確認 SSH 權限同時適用於公開和私密金鑰檔案。

程序

1 透過執行以下命令檢查 SSH 公開金鑰檔案：`ls –l /etc/ssh/*key.pub`

2 確認擁有者為根使用者、群組擁有者為根使用者，以及檔案權限設為 0644 (-rw-r--r--)。

3 透過執行以下命令修正任何問題。

```
chown root /etc/ssh/*key.pub

chgrp root /etc/ssh/*key.pub

chmod 644 /etc/ssh/*key.pub
```

4 透過執行以下命令檢查 SSH 私密金鑰檔案：`ls –l /etc/ssh/*key`

5 確認擁有者為根使用者、群組擁有者為根使用者，以及檔案權限設為 0600 (-rw-------)。透過執行以下命令修正任何問題。

```
chown root /etc/ssh/*key

chgrp root /etc/ssh/*key

chmod 600 /etc/ssh/*key
```

變更虛擬應用裝置管理介面使用者

您可以在虛擬應用裝置管理介面上新增和刪除使用者，以建立適當的安全性層級。

虛擬應用裝置管理介面的根使用者帳戶使用 PAM 進行驗證，因此 PAM 設定的剪輯層級同樣適用。如果您未適當隔離虛擬應用裝置管理介面，則可能會在攻擊者嘗試暴力密碼破解登入時鎖定系統根帳戶。此外，如果根帳戶被視為不足以在您的組織中提供多個不可否認的人員，您可能需要選擇變更管理介面的 Admin 使用者。

必要條件

程序

1 執行以下命令來建立新使用者，並將其新增至虛擬應用裝置管理介面群組。

```
useradd –G vami,root user
```

2 為使用者建立密碼。

```
passwd user
```

3 (選擇性) 執行以下命令以在虛擬應用裝置管理介面上停用根存取權。

```
usermod –R vami root
```

> **備註** 停用對虛擬應用裝置管理介面的根存取權，亦會停用從 [管理] 索引標籤更新管理員或根使用者的密碼功能。

設定開機載入器驗證

若要提供適當的安全性層級，請設定 VMware 虛擬應用裝置上的開機載入器驗證。

如果系統的開機載入器不需要驗證，具有系統主控台存取權的使用者就可以更改系統開機組態或將系統開機至單一使用者或維護模式，這會導致拒絕服務或未經授權的系統存取。由於 VMware 虛擬應用裝置上預設未設定開機載入器驗證，因此您必須建立 GRUB 密碼以進行設定。

程序

1 確認開機密碼是否存在，方法是在虛擬應用裝置上的 `/boot/grub/menu.lst` 檔案中尋找 `password --md5 <password-hash>` 行。

2 如果該密碼不存在，請在虛擬應用裝置上執行 `# /usr/sbin/grub-md5-crypt` 命令。

此時會產生 MD5 密碼，並且命令會提供 md5 雜湊輸出。

3 執行 `# password --md5 <hash from grub-md5-crypt>` 命令，將該密碼附加至 `menu.lst` 檔案。

設定 NTP

對於重要的時間來源，應停用主機時間同步化並在 vRealize Automation 應用裝置上使用網路時間通訊協定 (NTP)。

vRealize Automation 應用裝置上的 NTP 精靈可提供同步時間服務。NTP 依預設為停用，所以您需要手動對其進行設定。請盡可能在生產環境使用 NTP，透過準確的稽核和記錄保存來追蹤使用者動作以及偵測潛在的惡意攻擊和入侵。如需 NTP 安全性注意事項的相關資訊，請參閱 NTP 網站。

NTP 組態檔案位於每個應用裝置的 `/etc/` 資料夾中。您可為 vRealize Automation 應用裝置啟用 NTP 服務，並在虛擬應用裝置管理介面的**管理員**索引標籤上新增時間伺服器。

程序

1 使用文字編輯器開啟虛擬應用裝置主機上的 `/etc/ntp.conf` 組態檔。

2 將檔案擁有權設定為 **`root:root`**。

3 將權限設定為 **`0640`**。

4 為了降低對 NTP 服務進行拒絕服務放大攻擊的風險，請開啟 `/etc/ntp.conf` 檔案並確保檔案中存在 restrict 行。

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

5 儲存所有變更並關閉檔案。

為 vRealize Automation 應用裝置傳輸中的資料設定 TLS

確保您的 vRealize Automation 部署使用強式 TLS 通訊協定來保護 vRealize Automation 應用裝置元件的傳輸通道。

基於效能考量，某些應用程式服務之間的 localhost 連線不會啟用 TLS。但若希望獲得深度防禦，請在所有 localhost 通訊上啟用 TLS。

重要 如果您在負載平衡器上終止 TLS，請停用所有負載平衡器上不安全的通訊協定，例如 SSLv2、SSLv3 和 TLS 1.0。

對 Localhost 組態啟用 TLS

依預設，部分 localhost 通訊並不會使用 TLS。您可以對所有 localhost 連線啟用 TLS 以增強安全性。

程序

1 使用 SSH 連線至 vRealize Automation 應用裝置。

2 透過執行下列命令來為 vcac 金鑰儲存區設定權限。

```
usermod –A vco,coredump,pivotal vco
chown vcac.pivotal /etc/vcac/vcac.keystore
chmod 640 /etc/vcac/vcac.keystore
```

3 更新 HAProxy 組態。

a 開啟位於 `/etc/haproxy/conf.d` 的 HAProxy 組態檔，然後選擇 20-vcac.cfg 服務。

b 找到含有下列字串的行：

`server local 127.0.0.1…` 並將下列內容新增到此類行的結尾：`ssl verify none`

此區段還包含類似以下的其他行：

backend-horizon	backend-vro
backend-vra	backend-artifactory
backend-vra-health	

c 將 backend-horizon 的連接埠從 8080 變更為 8443。

4 取得 keystorePass 的密碼。

a 在 `/etc/vcac/security.properties` 檔案中找到內容 `certificate.store.password`。

例如，`certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

b 使用下列命令將值解密：

`vcac–config prop–util –d ––p VALUE`

例如，`vcac–config prop–util –d ––p s2enc~iom0GXATG+RB8ff7Wdm4Bg==`

5 設定 vRealize Automation 服務

a 開啟 `/etc/vcac/server.xml` 檔案。

b 將下列屬性新增至 [連接器] 標記，其中的 certificate.store.password 要以 `etc/vcac/security.properties` 中的憑證存放區密碼值取代。

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS" keystoreFile="/etc/vcac/
vcac.keystore" keyAlias="apache" keystorePass="certificate.store.password"
```

6 設定 vRealize Orchestrator 服務。

a 開啟 `/etc/vco/app-server.xml` 檔案

b 將下列屬性新增至 [連接器] 標記，其中的 certificate.store.password 要以 `etc/vcac/security.properties` 中的憑證存放區密碼值取代。

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS" keystoreFile="/etc/vcac/
vcac.keystore" keyAlias="apache" keystorePass="certificate.store.password"
```

7 重新啟動 vRealize Orchestrator、vRealize Automation 與 haproxy 服務。

```
service vcac-server restart
service vco-server restart
service haproxy restart
```

備註 如果無法重新啟動 vco-server，請將主機電腦重新開機。

8 設定虛擬應用裝置管理介面。

您可以在 vRealize Automation 虛擬應用裝置上執行下列命令以列出服務的狀態。

```
curl -ks -H "Content-Type: application/json" https://localhost/component-registry/services/status/
current?limit=200 | jq -re '.content[]|"\(.serviceStatus.serviceName) \
(.serviceStatus.serviceInitializationStatus)"'
```

備註 如果您在虛擬應用裝置管理介面上啟用 SSL，[服務] 索引標籤無法列出 vRealize Automation 服務的狀態。

a 開啟 `/opt/vmware/share/htdocs/service/café-services/services.py` 檔案。

b 將 `conn = httplib.HTTP()` 行變更為 `conn = httplib.HTTPS()` 以增強安全性。

啟用聯邦資訊處理標準 (FIPS) 140-2 符合性

vRealize Automation 應用裝置現在會對所有輸入與輸出網路流量中正在透過 TLS 傳輸的資料，使用聯邦資訊處理標準 (FIPS) 140-2 認證版本的 OpenSSL。

您可以在 vRealize Automation 應用裝置管理介面啟用或停用 FIPS 模式。您也可以在以根使用者身分登入的情況下，在命令列使用下列命令來設定 FIPS：

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

啟用 FIPS 後，連接埠 443 上的輸入與輸出 vRealize Automation 應用裝置網路流量會使用符合 FIPS 140–2 的加密。無論 FIPS 設定為何，vRealize Automation 都會使用 AES–256 來保護儲存在 vRealize Automation 應用裝置上的安全資料。

備註 目前 vRealize Automation 僅會部分啟用 FIPS 符合性，因為某些內部元件尚未使用認證的密碼編譯模組。在尚未實作認證模組的案例中，所有密碼編譯演算法中都會使用 AES–256 型加密。

備註 當您更改組態時，下列程序會將實體機器重新開機。

程序

1 以根使用者身分登入 vRealize Automation 應用裝置管理介面。

https://*vrealize-automation-appliance-FQDN*:5480

2 選取 **vRA > 主機設定**。

3 按一下右上方 [動作] 標題下的按鈕以啟用或停用 FIPS。

4 按一下**是**重新啟動 vRealize Automation 應用裝置

確認 SSLv3、TLS 1.0 和 TLS 1.1 已停用

做為強化程序的一部分，請確保已部署的 vRealize Automation 應用裝置 使用安全的傳輸通道。

備註 停用 TLS 1.0/1.1 並啟用 TLS 1.2 之後，無法執行加入叢集作業

必要條件

完成對 Localhost 組態啟用 TLS。

程序

1 確認 SSLv3、TLS 1.0 和 TLS 1.1 已在 vRealize Automation 應用裝置 上的 HAProxy https 處理常式中停用。

檢閱此檔案	確保存在以下內容	所在的適當行如下所示
/etc/haproxy/conf.d/20-vcac.cfg	no-sslv3 no-tlsv10 no-tls11 force-tls12	bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tlsv11
/etc/haproxy/conf.d/30-vro-config.cfg	no-sslv3 no-tlsv10 no-tls11 force-tls12	bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tlsv11

2 重新啟動服務。

```
service haproxy restart
```

3 開啟 /opt/vmware/etc/lighttpd/lighttpd.conf 檔案，確認出現正確的停用項目。

備註 沒有可在 Lighttpd 中停用 TLS 1.0 或 TLS 1.1 的指令。透過強制 OpenSSL 不使用 TLS 1.0 和 TLS 1.1 的加密套件，可部分減少 TLS 1.0 和 TLS 1.1 的使用限制。

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
```

4 確認已針對 vRealize Automation 應用裝置 上的主控台 Proxy 停用 SSLv3、TLS 1.0 和 TLS 1.1。

a 新增或修改以下行，對 /etc/vcac/security.properties 檔案進行編輯：

```
consoleproxy.ssl.server.protocols = TLSv1.2
```

b 透過執行下列命令重新啟動伺服器：

```
service vcac-server restart
```

5 確認已針對 vCO 服務停用 SSLv3、TLS 1.0 和 TLS 1.1。

a 找到 /etc/vco/app-server/server.xml 檔案中的 <Connector> 標記，然後新增以下屬性：

```
sslEnabledProtocols = "TLSv1.2"
```

b 透過執行下列命令重新啟動 vCO 服務。

```
service vco-server restart
```

6 確認已針對 vRealize Automation 服務停用 SSLv3、TLS 1.0 和 TLS 1.1。

a 在 /etc/vcac/server.xml 檔案的 <Connector> 標記中新增下列屬性

```
sslEnabledProtocols = "TLSv1.2"
```

b 透過執行下列命令重新啟動 vRealize Automation 服務：

```
service vcac-server restart
```

7 確認已針對 RabbitMQ 停用 SSLv3、TLS 1.0 和 TLS 1.1。

開啟 /etc/rabbitmq/rabbitmq.config 檔案，確認 ssl 和 ssl_options 區段中僅存在 {versions, ['tlsv1.2']}。

```
[
  {ssl, [
      {versions, ['tlsv1.2']},
      {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
   {rabbit, [
      {tcp_listeners, [{"127.0.0.1", 5672}]},
      {frame_max, 262144},
      {ssl_listeners, [5671]},
      {ssl_options, [
```

```
         {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
         {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
         {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
         {versions, ['tlsv1.2']},
         {ciphers, ["AES256-SHA", "AES128-SHA"]},
         {verify, verify_peer},
         {fail_if_no_peer_cert, false}
      ]},
      {mnesia_table_loading_timeout,600000},
      {cluster_partition_handling, autoheal},
      {heartbeat, 600}
   ]},
   {kernel, [{net_ticktime,  120}]}
].
```

8 重新啟動 RabbitMQ 伺服器。

```
# service rabbitmq-server restart
```

9 確認已針對 vIDM 服務停用 SSLv3、TLS 1.0 和 TLS 1.1。

針對包含 `SSLEnabled="true"` 的每個連接器執行個體，開啟 `/opt/vmware/horizon/workspace/conf/server.xml` 檔案並確認存在以下行。

```
sslEnabledProtocols="TLSv1.2"
```

為 vRealize Automation 元件設定 TLS 加密套件

為達到最大的安全性，您必須將 vRealize Automation 元件設定為使用強式密碼。

加密密碼會在伺服器和瀏覽器之間交涉，判斷 TLS 工作階段使用的加密強度。

為了確保僅選取強式密碼，請在 vRealize Automation 元件中停用弱式密碼。將伺服器設定為僅支援強式密碼，以及使用足夠大的金鑰大小。此外，也請依照適當順序設定所有加密。

停用未提供驗證的加密套件，例如 NULL 加密套件、aNULL 或 eNULL。也請停用匿名 Diffie-Hellman 金鑰交換 (ADH)、匯出層級加密 (EXP，包含 DES 的加密)、小於 128 位元用於加密裝載流量的金鑰大小、針對裝載流量使用 MD5 做為雜湊機制、IDEA 加密套件，以及 RC4 加密套件。同時，務請停用使用 Diffie-Hellman (DHE) 金鑰交換的加密套件

在 HA Proxy 中停用弱式密碼

對照可接受的密碼清單檢閱 vRealize Automation 應用裝置 HA Proxy 服務密碼，並停用視為弱式密碼的所有密碼。

停用未提供驗證的加密套件，例如 NULL 加密套件、aNULL 或 eNULL。也請停用匿名 Diffie-Hellman 金鑰交換 (ADH)、匯出層級加密 (EXP，包含 DES 的加密)、小於 128 位元用於加密裝載流量的金鑰大小、針對裝載流量使用 MD5 做為雜湊機制、IDEA 加密套件，以及 RC4 加密套件。

程序

1 檢閱繫結指令的 `/etc/haproxy/conf.d/20-vcac.cfg` 檔案密碼項目，並停用視為弱式密碼的所有密碼。

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tlsv11
```

2 檢閱繫結指令的 `/etc/haproxy/conf.d/30-vro-config.cfg` 檔案密碼項目，並停用視為弱式密碼的所有密碼。

```
bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tlsv11
```

在 vRealize Automation 應用裝置 vRealize Automation 應用裝置主控台 Proxy 服務中停用弱式密碼

對照可接受的密碼清單檢閱 vRealize Automation 應用裝置主控台 Proxy 服務密碼，並停用視為弱式密碼的所有密碼。

停用未提供驗證的加密套件，例如 NULL 加密套件、aNULL 或 eNULL。也請停用匿名 Diffie-Hellman 金鑰交換 (ADH)、匯出層級加密 (EXP，包含 DES 的加密)、小於 128 位元用於加密裝載流量的金鑰大小、針對裝載流量使用 MD5 做為雜湊機制、IDEA 加密套件，以及 RC4 加密套件。

程序

1 在文字編輯器中開啟 `/etc/vcac/security.properties` 檔案。

2 在該檔案中新增一行以停用不需要的密碼套件。

對下列行進行適當變化：

```
consoleproxy.ssl.ciphers.disallowed=cipher_suite_1, cipher_suite_2,etc
```

例如，若要停用 AES 128 和 AES 256 加密套件，請新增下列行：

```
consoleproxy.ssl.ciphers.disallowed=TLS_DH_DSS_WITH_AES_128_CBC_SHA,
TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

3 使用下列命令重新啟動伺服器。

```
service vcac-server restart
```

在 vRealize Automation 應用裝置 vCO 服務中停用弱式密碼

對照可接受的密碼清單檢閱 vRealize Automation 應用裝置 vCO 服務密碼，並停用視為弱式密碼的所有密碼。

停用未提供驗證的加密套件，例如 NULL 加密套件、aNULL 或 eNULL。也請停用匿名 Diffie-Hellman 金鑰交換 (ADH)、匯出層級加密 (EXP，包含 DES 的加密)、小於 128 位元用於加密裝載流量的金鑰大小、針對裝載流量使用 MD5 做為雜湊機制、IDEA 加密套件，以及 RC4 加密套件。

程序

1 找到 /etc/vco/app-server/server.xml 檔案中的 <Connector> 標籤。

2 編輯或新增密碼屬性，以使用所需的密碼套件。

請參閱下列範例：

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_E
CDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GC
M_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_R
SA_WITH_AES_256_CBC_SHA384”
```

在 vRealize Automation 應用裝置 RabbitMQ 服務中停用弱式密碼

對照可接受的密碼清單檢閱 vRealize Automation 應用裝置 RabbitMQ 服務密碼，並停用視為弱式密碼的所有密碼。

停用未提供驗證的加密套件，例如 NULL 加密套件、aNULL 或 eNULL。也請停用匿名 Diffie-Hellman 金鑰交換 (ADH)、匯出層級加密 (EXP，包含 DES 的加密)、小於 128 位元用於加密裝載流量的金鑰大小、針對裝載流量使用 MD5 做為雜湊機制、IDEA 加密套件，以及 RC4 加密套件。

程序

1 透過執行 # /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites().' 命令評估支援的密碼套件。

以下範例中傳回的密碼僅代表支援的密碼。RabbitMQ 伺服器不會使用或通告這些密碼，除非 rabbitmq.config 檔案中有所設定。

```
["ECDHE-ECDSA-AES256-GCM-SHA384","ECDHE-RSA-AES256-GCM-SHA384",
 "ECDHE-ECDSA-AES256-SHA384","ECDHE-RSA-AES256-SHA384",
 "ECDH-ECDSA-AES256-GCM-SHA384","ECDH-RSA-AES256-GCM-SHA384",
 "ECDH-ECDSA-AES256-SHA384","ECDH-RSA-AES256-SHA384",
 "DHE-RSA-AES256-GCM-SHA384","DHE-DSS-AES256-GCM-SHA384",
 "DHE-RSA-AES256-SHA256","DHE-DSS-AES256-SHA256","AES256-GCM-SHA384",
 "AES256-SHA256","ECDHE-ECDSA-AES128-GCM-SHA256",
 "ECDHE-RSA-AES128-GCM-SHA256","ECDHE-ECDSA-AES128-SHA256",
 "ECDHE-RSA-AES128-SHA256","ECDH-ECDSA-AES128-GCM-SHA256",
 "ECDH-RSA-AES128-GCM-SHA256","ECDH-ECDSA-AES128-SHA256",
 "ECDH-RSA-AES128-SHA256","DHE-RSA-AES128-GCM-SHA256",
 "DHE-DSS-AES128-GCM-SHA256","DHE-RSA-AES128-SHA256","DHE-DSS-AES128-SHA256",
 "AES128-GCM-SHA256","AES128-SHA256","ECDHE-ECDSA-AES256-SHA",
 "ECDHE-RSA-AES256-SHA","DHE-RSA-AES256-SHA","DHE-DSS-AES256-SHA",
 "ECDH-ECDSA-AES256-SHA","ECDH-RSA-AES256-SHA","AES256-SHA",
 "ECDHE-ECDSA-DES-CBC3-SHA","ECDHE-RSA-DES-CBC3-SHA","EDH-RSA-DES-CBC3-SHA",
 "EDH-DSS-DES-CBC3-SHA","ECDH-ECDSA-DES-CBC3-SHA","ECDH-RSA-DES-CBC3-SHA",
 "DES-CBC3-SHA","ECDHE-ECDSA-AES128-SHA","ECDHE-RSA-AES128-SHA",
 "DHE-RSA-AES128-SHA","DHE-DSS-AES128-SHA","ECDH-ECDSA-AES128-SHA",
 "ECDH-RSA-AES128-SHA","AES128-SHA"]
```

2 選取符合您組織安全性需求的受支援密碼。

例如，若要僅允許使用 ECDHE-ECDSA-AES128-GCM-SHA256 & ECDHE-ECDSA-AES256-GCM-SHA384，請檢閱 /etc/rabbitmq/rabbitmq.config 檔案並將以下行新增至 ssl 和 ssl_options。

```
{ciphers, ["ECDHE-ECDSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-GCM-SHA384"]}
```

3 使用下列命令重新啟動 RabbitMQ 伺服器。

```
service rabbitmq-server restart
```

確認靜態資料的安全性

確認與 vRealize Automation 搭配使用的資料庫使用者和帳戶的安全性。

Postgres 使用者

Postgres Linux 使用者帳戶繫結至 Postgres 資料庫超級使用者帳戶角色，依預設是鎖定的帳戶。這是此使用者最安全的組態，因為只能透過根使用者帳戶進行存取。請勿解除鎖定此使用者帳戶。

資料庫使用者帳戶角色

預設 Postgres 使用者帳戶角色不應用於應用程式功能之外的用途。若要支援非預設資料庫檢閱或報告活動，應建立其他帳戶並適當保護密碼。

在命令列中執行以下指令碼：

```
vcac-vami add-db-user newUsername newPassword
```

這將新增使用者和受該使用者保護的密碼。

備註 在已設定主從式 HA Postgres 設定的情況下，必須針對主 Postgres 資料庫執行此指令碼。

設定 PostgreSQL 用戶端驗證

確保 vRealize Automation 應用裝置 PostgreSQL 資料庫未設定本機信任驗證。此組態允許任何本機使用者 (包括資料庫超級使用者) 以任何 PostgreSQL 使用者身分連線 (無需密碼)。

備註 Postgres 超級使用者帳戶應該保持做為本機信任。

建議使用 md5 驗證方法，因為其會傳送加密密碼。

用戶端驗證組態設定位於 `/storage/db/pgdata/pg_hba.conf` 檔案。

```
# TYPE  DATABASE        USER              ADDRESS          METHOD

# "local" is for Unix domain socket connections only
local      all              postgres                            trust
# IPv4 local connections:
#host    all              all               127.0.0.1/32     md5
hostssl    all              all               127.0.0.1/32     md5
# IPv6 local connections:
#host    all              all               ::1/128          md5
hostssl    all              all               ::1/128          md5

# Allow remote connections for VCAC user.
#host    vcac             vcac              0.0.0.0/0        md5
hostssl    vcac             vcac              0.0.0.0/0        md5
hostssl    vcac             vcac              ::0/0        md5
```

```
# Allow remote connections for VCAC replication user.
#host    vcac             vcac_replication   0.0.0.0/0        md5
hostssl    vcac          vcac_replication   0.0.0.0/0        md5
hostssl    vcac          vcac_replication   ::0/0        md5
# Allow replication connections by a user with the replication privilege.
#host    replication      vcac_replication   0.0.0.0/0        md5
hostssl    replication      vcac_replication   0.0.0.0/0        md5
hostssl    replication      vcac_replication   ::0/0        md5
```

如果您編輯 pg_hba.conf 檔案，在變更生效之前必須透過執行下列命令重新啟動 Postgres 伺服器。

```
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

設定 vRealize Automation 應用程式資源

檢閱 vRealize Automation 應用程式資源和限制檔案權限。

程序

1 執行以下命令，以確認含有 SUID 和 GUID 位元集的檔案已明確定義。

```
find / -path /proc -prune -o -type f -perm +6000 -ls
```

下列清單應該會出現。

```
2197357   24 -rwsr-xr-x   1 polkituser root        23176 Mar 31  2015 /usr/lib/PolicyKit/polkit-
set-default-helper
2197354   16 -rwxr-sr-x   1 root     polkituser    14856 Mar 31  2015 /usr/lib/PolicyKit/polkit-
read-auth-helper
2197353   12 -rwsr-x---   1 root     polkituser    10744 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper-pam
2197352   20 -rwxr-sr-x   1 root     polkituser    19208 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper
2197351   20 -rwxr-sr-x   1 root     polkituser    19008 Mar 31  2015 /usr/lib/PolicyKit/polkit-
explicit-grant-helper
2197356   24 -rwxr-sr-x   1 root     polkituser    23160 Mar 31  2015 /usr/lib/PolicyKit/polkit-
revoke-helper
2188203  460 -rws--x--x   1 root     root       465364 Apr 21 22:38 /usr/lib64/ssh/ssh-keysign
2138858   12 -rwxr-sr-x   1 root     tty         10680 May 10  2010 /usr/sbin/utempter
2142482  144 -rwsr-xr-x   1 root     root       142890 Sep 15  2015 /usr/bin/passwd
2142477  164 -rwsr-xr-x   1 root     shadow     161782 Sep 15  2015 /usr/bin/chage
2142467  156 -rwsr-xr-x   1 root     shadow     152850 Sep 15  2015 /usr/bin/chfn
1458298  364 -rwsr-xr-x   1 root     root       365787 Jul 22  2015 /usr/bin/sudo
2142481   64 -rwsr-xr-x   1 root     root        57776 Sep 15  2015 /usr/bin/newgrp
1458249   40 -rwsr-x---   1 root     trusted     40432 Mar 18  2015 /usr/bin/crontab
2142478  148 -rwsr-xr-x   1 root     shadow     146459 Sep 15  2015 /usr/bin/chsh
2142480  156 -rwsr-xr-x   1 root     shadow     152387 Sep 15  2015 /usr/bin/gpasswd
2142479   48 -rwsr-xr-x   1 root     shadow      46967 Sep 15  2015 /usr/bin/expiry
311484   48 -rwsr-x---   1 root     messagebus    47912 Sep 16  2014 /lib64/dbus-1/dbus-daemon-
launch-helper
876574   36 -rwsr-xr-x   1 root     shadow      35688 Apr 10  2014 /sbin/unix_chkpwd
876648   12 -rwsr-xr-x   1 root     shadow      10736 Dec 16  2011 /sbin/unix2_chkpwd
 49308   68 -rwsr-xr-x   1 root     root        63376 May 27  2015 /opt/likewise/bin/ksu
```

```
1130552   40 -rwsr-xr-x   1 root     root        40016 Apr 16  2015 /bin/su
1130511   40 -rwsr-xr-x   1 root     root        40048 Apr 15  2011 /bin/ping
1130600  100 -rwsr-xr-x   1 root     root        94808 Mar 11  2015 /bin/mount
1130601   72 -rwsr-xr-x   1 root     root        69240 Mar 11  2015 /bin/umount
1130512   36 -rwsr-xr-x   1 root     root        35792 Apr 15  2011 /bin/ping6  2012 /lib64/
dbus-1/dbus-daemon-launch-helper
```

2 執行以下命令，以確認虛擬應用裝置上的所有檔案都有擁有者。

```
find / -path /proc -prune -o -nouser -o -nogroup
```

3 透過執行下列命令，檢閱虛擬應用裝置之所有檔案的權限，以確認沒有檔案可全域寫入。

```
find / -name "*.*" -type f -perm -a+w | xargs ls -ldb
```

4 執行以下命令，以確認僅 vcac 使用者擁有正確檔案。

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" | egrep -v -e "*/
vmware-vcac/*"
```

如果沒有顯示結果，則所有正確檔案僅由 vcac 使用者擁有。

5 確認僅 vcac 使用者可寫入下列檔案。

```
/etc/vcac/vcac/security.properties
/etc/vcac/vcac/solution-users.properties
/etc/vcac/vcac/sso-admin.properties
/etc/vcac/vcac/vcac.keystore
/etc/vcac/vcac/vcac.properties
```

另請確認下列檔案及其子目錄

```
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

6 確認僅 vcac 或根使用者可以讀取下列目錄及其子目錄中的正確檔案。

```
/etc/vcac/*
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

7 確認正確檔案僅由 vco 或根使用者擁有，如下列目錄及其子目錄所示。

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
/var/cache/vco/*
```

8 確認正確檔案僅可由 vco 或根使用者寫入，如下列目錄及其子目錄所示。

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
/var/cache/vco/*
```

9 確認正確檔案僅可由 vco 或根使用者讀取，如下列目錄及其子目錄所示。

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
/var/cache/vco/*
```

自訂主控台 Proxy 組態

您可為 vRealize Automation 自訂遠端主控台組態，以利疑難排解與實施組織做法。

當您安裝、設定或維護 vRealize Automation 時，可變更某些設定來啟用安裝的疑難排解與偵錯。記載並稽核您進行的每項變更，可確保適用元件皆根據其必要用途適當受保護。若不確定您的組態變更是否已正確受保護，請勿繼續進行至生產階段。

自訂 VMware Remote Console 票證到期

您可自訂用於建立 VMware Remote Console 連線之遠端主控台票證的有效期限。

當使用者進行 VMware Remote Console 連線時，系統會建立並傳回單次認證，用於建立連往虛擬機器的特定連線。您可將票證到期時間設定為指定的時間範圍 (以分鐘為單位)。

程序

1 在文字編輯器中開啟 `/etc/vcac/security.properties` 檔案。

2 新增此形式的行 `consoleproxy.ticket.validitySec=30` 至檔案。

在此行中，數值指定票證到期前的分鐘數。

3 儲存並關閉檔案。

4 使用命令 `/etc/init.d/vcac-server restart` 重新啟動 vcac-server。

票證到期值會重設為指定的時間範圍 (以分鐘為單位)。

自訂主控台 Proxy 伺服器連接埠

您可自訂 VMware Remote Console 主控台 Proxy 用於接聽訊息的連接埠。

程序

1 在文字編輯器中開啟 `/etc/vcac/security.properties` 檔案。

2 新增此形式的行 `consoleproxy.service.port=8445` 至檔案。

數值指定主控台 Proxy 服務連接埠號碼，在此案例中是 8445。

3 儲存並關閉檔案。

4 使用命令 `/etc/init.d/vcac-server restart` 重新啟動 vcac-server。

Proxy 服務連接埠會變更為指定的連接埠號碼。

設定 X-XSS-Protection 回應標頭

新增 X-XSS-Protection 回應標頭至 haproxy 組態檔。

程序

1 開啟 `/etc/haproxy/conf.d/20-vcac.cfg` 以便編輯。

2 將下列幾行新增至前端區段：

```
rspdel X-XSS-Protection:\ 1;\ mode=block
              rspadd X-XSS-Protection:\ 1;\ mode=block
```

3 使用下列命令重新載入 HAProxy 組態。

```
/etc/init.d/haproxy reload
```

設定 X-Content-Type-Options 回應標頭

將 X-Content-Type-Options 回應標頭新增至 HAProxy 組態。

程序

1 開啟 `/etc/haproxy/conf.d/20-vcac.cfg` 以便編輯。

2 將下列幾行新增至前端區段：

```
http-response set-header X-Content-Type-Options nosniff
```

3 使用下列命令重新載入 HAProxy 組態。

```
/etc/init.d/haproxy reload
```

設定 HTTP 強制安全傳輸技術回應標頭

新增 HTTP 強制安全傳輸技術 (HSTS) 回應標頭至 HAProxy 組態。

程序

1 開啟 `/etc/haproxy/conf.d/20-vcac.cfg` 以便編輯。

2 將下列幾行新增至前端區段：

```
rspdel Strict-Transport-Security:\ max-age=31536000
        rspadd Strict-Transport-Security:\ max-age=31536000
```

3 使用下列命令重新載入 HAProxy 組態。

```
/etc/init.d/haproxy reload
```

設定 X-Frame-Options 回應標頭

在某些情況下，X-Frame-Options 回應標頭可能會出現兩次。

由於 vIDM 服務將此標頭新增至後端以及 HAProxy，所以 X-Frame-Options 回應標頭可能會出現兩次。您可使用適當的組態，防止此標頭出現兩次。

程序

1 開啟 `/etc/haproxy/conf.d/20-vcac.cfg` 以便編輯。

2 在前端區段中找到下列行：

```
rspadd X-Frame-Options:\ SAMEORIGIN
```

3 將下列幾行新增至您於上一步驟中找到的該行之前。

```
rspdel X-Frame-Options:\ SAMEORIGIN
```

4 使用下列命令重新載入 HAProxy 組態。

```
/etc/init.d/haproxy reload
```

設定伺服器回應標頭

安全性最佳做法是設定您的 vRealize Automation 系統，以限制可供潛在攻擊者利用的資訊。

請儘量減少共用的系統身分識別和版本資訊數量。駭客和惡意執行者可以利用這些資訊對您的 Web 伺服器或版本發動鎖定攻擊。

設定 Lighttpd 伺服器回應標頭

最佳做法是為 vRealize Automation 應用裝置 lighttpd 伺服器建立空白伺服器標頭。

程序

1 在文字編輯器中開啟 `/opt/vmware/etc/lighttpd/lighttpd.conf` 檔案。

2 新增 `server.tag = " "` 至檔案。

3 儲存變更並關閉此檔案。

4 執行 `# /opt/vmware/etc/init.d/vami-lighttp restart` 命令，重新啟動 lighttpd 伺服器。

為 vRealize Automation 應用裝置設定 TCServer 回應標頭

最佳做法是為搭配 vRealize Automation 應用裝置使用的 TCServer 回應標頭建立自訂空白伺服器標頭，以限制惡意攻擊者取得寶貴資訊的可能性。

程序

1 在文字編輯器中開啟 `/etc/vco/app-server/server.xml` 檔案。

2 在每個 <Connector> 元素中新增 server=" ".

例如：<Connector protocol="HTTP/1.1" server="" .... />

3 儲存變更並關閉此檔案。

4 使用下列命令重新啟動伺服器。

```
service vco-server restart
```

設定網際網路資訊服務伺服器回應標頭

最佳做法是為搭配 Identity Appliance 使用的網際網路資訊服務 (IIS) 伺服器建立自訂空白伺服器標頭，限制惡意攻擊者取得寶貴資訊的可能性。

程序

1 在文字編輯器中開啟 C:\Windows\System32\inetsrv\urlscan\UrlScan.ini 檔案。

2 搜尋 RemoveServerHeader=0 並將其變更為 RemoveServerHeader=1.

3 儲存變更並關閉此檔案。

4 透過執行 iisreset 命令重新啟動伺服器。

後續步驟

從 [IIS 管理員] 主控台的清單中移除 HTTP 回應標頭，以便停用 IIS X-Powered By 標頭。

1 開啟 [IIS 管理員] 主控台。

2 開啟 [HTTP 回應標頭] 並從清單中將其移除。

3 透過執行 iisreset 命令重新啟動伺服器。

設定 vRealize Automation 應用裝置 工作階段逾時

根據公司安全性原則，設定 vRealize Automation 應用裝置 上的工作階段逾時設定。

vRealize Automation 應用裝置針對使用者閒置的預設工作階段逾時為 30 分鐘。若要調整此逾時值以符合組織的安全性原則，請編輯 vRealize Automation 應用裝置主機上的 web.xml 檔案。

程序

1 在文字編輯器中開啟 /usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml 檔案。

2 找到 session-config 並設定工作階段逾時值。請參閱以下程式碼範例。

```
<!-- 30 minutes session expiration time -->
  <session-config>
         <session-timeout>30</session-timeout>
         <tracking-mode>COOKIE</tracking-mode>
         <cookie-config>
                <path>/</path>
         </cookie-config>
  </session-config>
```

3 透過執行下列命令重新啟動伺服器。

```
service vcac-server restart
```

管理非必要軟體

為了將安全性風險降至最低，請從 vRealize Automation 主機移除或設定非必要軟體。

依據製造商建議和安全性最佳做法，設定所有您不移除的軟體，以將其建立安全性漏洞的可能性降至最低。

保護 USB 大型儲存裝置處理常式

保護 USB 大型儲存裝置處理常式，防止將其做為 USB 裝置處理常式與 VMware 虛擬應用裝置主機搭配使用。潛在攻擊者可能會利用此處理常式危害系統。

程序

1 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。

2 確保該檔案中出現 `install usb-storage /bin/true` 行。

3 儲存並關閉檔案。

保護藍牙通訊協定處理常式

保護虛擬應用裝置主機上的藍牙通訊協定處理常式安全，以防止其遭到攻擊者利用。

將藍牙通訊協定繫結到網路堆疊不但沒必要，而且還會增大主機攻擊面。

程序

1 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。

2 確保此檔案中出現以下行。

```
install bluetooth /bin/true
```

3 儲存並關閉檔案。

保護串流控制傳輸通訊協定

依預設會阻止將串流控制傳輸通訊協定 (SCTP) 載入到系統。潛在攻擊者可能會利用此通訊協定危害系統。

除非絕對必要，否則請將系統設定為阻止載入串流控制傳輸通訊協定 (SCTP) 模組。SCTP 是一種未使用的 IETF 標準化傳輸層通訊協定。將此通訊協定繫結到網路堆疊會增大主機攻擊面。透過使用該通訊協定開啟通訊端，無權限的本機程序可能會使核心動態載入通訊協定處理常式。

程序

1 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。

2 確保此檔案中出現以下行。

```
install sctp /bin/true
```

3 儲存並關閉檔案。

保護資料包壅塞通訊協定

做為系統強化活動的一部分，依預設會阻止將資料包壅塞通訊協定 (DCCP) 載入到虛擬應用裝置主機。潛在攻擊者可能會利用此通訊協定危害系統。

除非絕對必要，否則請避免載入資料包壅塞控制通訊協定 (DCCP) 模組。DCCP 是一種建議的傳輸層通訊協定，並沒有使用。將此通訊協定繫結到網路堆疊會增大主機攻擊面。透過使用該通訊協定開啟通訊端，無權限的本機程序可能會使核心動態載入通訊協定處理常式。

程序

1 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。

2 確保該檔案中出現 DCCP 行。

```
install dccp/bin/true
 install dccp_ipv4/bin/true
 install dccp_ipv6/bin/true
```

3 儲存並關閉檔案。

保護網路橋接

依預設會阻止將網路橋接模組載入到系統。潛在攻擊者可能會利用它危害系統。

除非絕對必要，否則請將系統設定為阻止載入網路橋接。潛在攻擊者可能會利用它略過網路磁碟分割和安全性檢查。

程序

1 在所有 VMware 虛擬應用裝置主機上執行以下命令。

```
# rmmod bridge
```

2 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。

3 確保此檔案中出現以下行。

```
install bridge /bin/false
```

4 儲存並關閉檔案。

保護可靠資料包通訊端通訊協定

做為系統強化活動的一部分，依預設會阻止將可靠資料包通訊端 (RDS) 通訊協定載入到虛擬應用裝置主機。潛在攻擊者可能會利用此通訊協定危害系統。

將可靠資料包通訊端 (RDS) 通訊協定繫結到網路堆疊會增大主機攻擊面。透過使用該通訊協定開啟通訊端，無權限的本機程序可能會使系統動態載入通訊協定處理常式。

程序

1 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。

2 確保此檔案中出現 `install rds /bin/true` 行。

3 儲存並關閉檔案。

保護透明處理序間通訊協定

做為系統強化活動的一部分，依預設會阻止將透明處理序間通訊協定 (TIPC) 載入到虛擬應用裝置主機。潛在攻擊者可能會利用此通訊協定危害系統。

將透明處理序間通訊協定 (TIPC) 繫結到網路堆疊會增大主機攻擊面。透過使用該通訊協定開啟通訊端，無權限的本機程序可能會使核心動態載入通訊協定處理常式。

程序

1 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。

2 確保此檔案中出現 `install tipc /bin/true` 行。

3 儲存並關閉檔案。

保護網際網路封包交換通訊協定

依預設會阻止將網際網路封包交換 (IPX) 通訊協定載入到系統。潛在攻擊者可能會利用此通訊協定危害系統。

除非絕對必要，否則請避免載入網際網路封包交換 (IPX) 通訊協定模組。IPX 通訊協定是一種過時的網路層通訊協定。將此通訊協定繫結到網路堆疊會增大主機攻擊面。透過使用該通訊協定開啟通訊端，無權限的本機程序可能會使系統動態載入通訊協定處理常式。

程序

1 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。

2 確保此檔案中出現以下行。

```
install ipx /bin/true
```

3 儲存並關閉檔案。

保護 AppleTalk 通訊協定安全

依預設會阻止將 AppleTalk 通訊協定載入到系統。潛在攻擊者可能會利用此通訊協定危害系統。

除非絕對必要，否則請避免載入 AppleTalk 通訊協定模組。將此通訊協定繫結到網路堆疊會增大主機攻擊面。透過使用該通訊協定開啟通訊端，無權限的本機程序可能會使系統動態載入通訊協定處理常式。

程序

1 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。

2 確保此檔案中出現以下行。

```
install appletalk /bin/true
```

3 儲存並關閉檔案。

保護 DECnet 通訊協定

依預設會阻止將 DECnet 通訊協定載入到系統。潛在攻擊者可能會利用此通訊協定危害系統。

除非絕對必要，否則請避免載入 DECnet 通訊協定模組。將此通訊協定繫結到網路堆疊會增大主機攻擊面。透過使用該通訊協定開啟通訊端，無權限的本機程序可能會使系統動態載入通訊協定處理常式。

程序

1 在文字編輯器中開啟 DECnet 通訊協定 `/etc/modprobe.conf.local` 檔案。

2 確保此檔案中出現以下行。

```
install decnet /bin/true
```

3 儲存並關閉檔案。

保護 FireWire 模組

依預設會阻止將 FireWire 模組載入到系統。潛在攻擊者可能會利用此通訊協定危害系統。

除非絕對必要，否則請避免載入 FireWire 模組。

程序

1 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。

2 確保此檔案中出現以下行。

```
install ieee1394 /bin/true
```

3 儲存並關閉檔案。

保護基礎結構即服務元件

在強化系統時，請保護 vRealize Automation 基礎結構即服務 (IaaS) 元件及其主機，以防止其遭到潛在攻擊者利用。

必須針對 vRealize Automation 基礎結構即服務 (IaaS) 元件及該元件所在的主機進行安全性設定。必須設定或確認其他相關元件和應用程式的組態。在某些情況下，您可以確認現有設定，但其他情況下必須變更或新增設定才能取得適當的組態。

設定 NTP

安全性最佳做法是在 vRealize Automation 生產環境中使用授權的時間伺服器，而非主機時間同步化。

在生產環境中，請停用主機時間同步化並使用授權的時間伺服器，以支援透過稽核與記錄，準確追蹤使用者動作以及識別潛在的惡意攻擊與入侵。

為基礎結構即服務傳輸中的資料設定 TLS

確定您的 vRealize Automation 部署使用強式 TLS 通訊協定來保護基礎結構即服務元件的傳輸通道。

安全通訊端層 (SSL) 與最近開發的傳輸層安全性 (TLS) 是密碼編譯式通訊協定，可協助確保在不同的系統元件之間進行網路通訊時的系統安全。由於 SSL 是較舊的標準，其許多實作已無法再針對潛在攻擊提供足夠的安全防範。舊版 SSL 通訊協定 (包括 SSLv2 和 SSLv3) 已被識別出嚴重的弱點。這些通訊協定已被視為不夠安全。

視貴組織的安全性原則而定，您可能也會想停用 TLS 1.0。

備註 在負載平衡器上終止 TLS 時，請視需要一併停用弱式通訊協定，例如 SSLv2、SSLv3 以及 TLS 1.0 和 1.1。

針對 IaaS 啟用 TLS 1.1 和 1.2 通訊協定

在裝載 IaaS 元件的所有虛擬機器上啟用並強制使用 TLS 1.1 和 1.2 通訊協定。

程序

1 按一下**開始**和**執行**。

2 輸入 Regedit，然後按一下**確定**。

3 找到並開啟下列登錄子機碼。

```
HKEY LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols
```

4 確認下列項目並根據需要建立新項目。

- 如果通訊協定下方沒有名稱為 TLS 1.1 的子機碼，請建立一個。
- 如果 TLS 1.1 下方沒有名稱為 Client 的子機碼，請建立一個。
- 如果 Client 子機碼中沒有名稱為 DisabledByDefault 的機碼，請建立一個類型為 DWORD 的機碼。
- 在 DisabledByDefault 上按一下滑鼠右鍵，選取 [修改]，然後將其值設定為 0。
- 如果 Client 子機碼中沒有名稱為 Enabled 的機碼，請建立一個類型為 DWORD 的機碼。
- 在 Enabled 上按一下滑鼠右鍵，選取 [修改]，然後將其值設定為 1。
- 如果 TLS 1.1 下方沒有名稱為 Server 的子機碼，請建立一個。
- 如果 Server 子機碼中沒有名稱為 DisabledByDefault 的機碼，請建立一個類型為 DWORD 的機碼。
- 在 DisabledByDefault 上按一下滑鼠右鍵，選取 [修改]，然後將其值設定為 0。
- 如果 Server 子機碼中沒有名稱為 Enabled 的機碼，請建立一個類型為 DWORD 的機碼。
- 在 Enabled 上按一下滑鼠右鍵，選取 [修改]，然後將其值設定為 1。

5 針對 TLS 1.2 通訊協定重複前述步驟。

備註 若要強制使用 TLS 1.1 和 1.2，則需要後續步驟中所述的其他設定。

6 找到並開啟下列登錄子機碼。

```
HKEY LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFrmework\v4.0.30319
```

7 確認下列項目並根據需要建立新項目。

- 如果沒有名稱為 SchUseStrongCrypto 的 DWORD 項目，請建立一個並將其值設定為 1。
- 如果沒有名稱為 SystemDefaultTlsVersions 的 DWORD 項目，請建立一個並將其值設定為 1。

8 找到並開啟下列登錄子機碼。

```
HKEY LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFrmework\v4.0.30319
```

9 確認下列項目並根據需要建立新項目。

- 如果沒有名稱為 SchUseStrongCrypto 的 DWORD 項目，請建立一個並將其值設定為 1。
- 如果沒有名稱為 SystemDefaultTlsVersions 的 DWORD 項目，請建立一個並將其值設定為 1。

針對 IaaS 停用 SSL 3.0 和 TLS 1.0

針對 IaaS 元件停用 SSL 3.0 和已過時的 TLS 1.0 通訊協定。

程序

1 按一下**開始**和**執行**。

2 輸入 `Regedit`，然後按一下**確定**。

3 找到並開啟下列登錄子機碼。

```
HKEY LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols
```

4 確認下列項目並根據需要建立新項目。

- 如果通訊協定的 SSL 3.0 下方沒有帶名稱的子機碼，請建立一個。
- 如果 SSL 3.0 下方沒有名稱為 Client 的子機碼，請建立一個。
- 如果 Client 子機碼中沒有名稱為 DisabledByDefault 的機碼，請建立一個類型為 DWORD 的機碼。
- 在 DisabledByDefault 上按一下滑鼠右鍵，選取 [修改]，然後將其值設定為 1。
- 在 Enabled 上按一下滑鼠右鍵，選取 [修改]，然後將其值設定為 0。
- 如果 SSL 3.0 下方沒有名稱為 Server 的子機碼，請建立一個。
- 如果 Server 子機碼中沒有名稱為 DisabledByDefault 的機碼，請建立一個類型為 DWORD 的機碼。
- 在 DisabledByDefault 上按一下滑鼠右鍵，選取 [修改]，然後將其值設定為 1。
- 如果 Server 中沒有名稱為 Enabled 的機碼，請建立一個類型為 DWORD 的機碼。
- 在 Enabled 上按一下滑鼠右鍵，選取 [修改]，然後將其值設定為 0。

5 針對 TLS 1.0 通訊協定重複前述步驟。

針對 IaaS 停用 TLS 1.0

為提供最高安全性，請將 IaaS 設定為使用集區並停用 TLS 1.0。

如需詳細資訊，請參閱 Microsoft 知識庫文章，網址為 https://support.microsoft.com/en-us/kb/245030。

程序

1 將 IaaS 設定為使用集區而非 Web 通訊端。

a 在 <appSettings> 區段中新增以下值，以更新 Manager Services 組態檔 `C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config`

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```

b 重新啟動 Manager Service (VMware vCloud Automation Center 服務)。

2 確認 TLS 1.0 在 IaaS 伺服器上已停用。

a 以管理員身分執行登錄編輯器。

b 在登錄視窗中導覽到 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\`

c 在 Protocols 上按一下滑鼠右鍵，選取**新增 > 機碼**，然後輸入 **`TLS 1.0`**。

d 在導覽樹狀結構中，在剛建立的 TLS 1.0 機碼上按一下滑鼠右鍵，然後在快顯功能表中選取**新增 > 機碼**並輸入 **`Client`**。

e 在導覽樹狀結構中，在剛建立的 TLS 1.0 機碼上按一下滑鼠右鍵，然後在快顯功能表中選取**新增 > 機碼**並輸入 **`Server`**。

f 在導覽樹狀結構中的 TLS 1.0 下方，在 **Client** 上按一下滑鼠右鍵，然後按一下**新增 > DWORD (32-位元) 值**並輸入 **`DisabledByDefault`**。

g 在導覽樹狀結構中的 TLS 1.0 下方，選取 **Client**，然後在右窗格中按兩下 **DisabledByDefault** DWORD 並輸入 **`1`**。

h 在導覽樹狀結構中的 TLS 1.0 下方，在 **Server** 上按一下滑鼠右鍵，然後選取**新增 > DWORD (32-位元) 值**並輸入 **`Enabled`**。

i 在導覽樹狀結構中的 TLS 1.0 下方，選取 **Server**，然後在右窗格中按兩下 **Enabled** DWORD 並輸入 **`0`**。

j 重新啟動 Windows Server。

設定 TLS 加密套件

為達到最大的安全性，您必須將 vRealize Automation 元件設定為使用強式密碼。加密密碼會在伺服器和瀏覽器之間交涉，判斷 TLS 工作階段使用的加密強度。為了確保僅選取強式密碼，請在 vRealize Automation 元件中停用弱式密碼。將伺服器設定為僅支援強式密碼，以及使用足夠大的金鑰大小。此外，也請依照適當順序設定所有加密。

不接受的加密套件

停用未提供驗證的加密套件，例如 NULL 加密套件、aNULL 或 eNULL。也請停用匿名 Diffie-Hellman 金鑰交換 (ADH)、匯出層級加密 (EXP，包含 DES 的加密)、小於 128 位元用於加密裝載流量的金鑰大小、針對裝載流量使用 MD5 做為雜湊機制、IDEA 加密套件，以及 RC4 加密套件。同時，務請停用使用 Diffie-Hellman (DHE) 金鑰交換的加密套件。

如需在 vRealize Automation 中停用靜態金鑰加密的相關資訊，請參閱知識庫文章 71094。

確認主機伺服器安全性

安全性最佳做法是確認基礎結構即服務 (IaaS) 主機伺服器機器的安全性組態。

Microsoft 提供了數種工具來協助您確認主機伺服器機器的安全性。請連絡您的 Microsoft 廠商，以取得有關這些工具最適當的使用方式指引。

確認主機伺服器安全基準

執行 Microsoft Baseline Security Analyzer (MBSA) 以快速確認您的伺服器是否具有最新的更新或 Hotfix。您可以依照 Microsoft 安全性建議，使用 MBSA 安裝缺少的 Microsoft 安全性修補程式，以使伺服器保持最新狀態。

從 Microsoft 網站下載最新版本的 MBSA 工具。

確認主機伺服器安全性組態

使用 Windows 安全性設定精靈 (SCW) 和 Microsoft Security Compliance Manager (SCM) 工具組來確認主機伺服器是否已安全設定。

從 Windows 伺服器的系統管理工具中執行 SCW。此工具可識別伺服器角色和已安裝的功能 (包括網路功能、Windows 防火牆和登錄設定)。將報告與來自 Windows 伺服器之相關 SCM 的最新強化指引進行比較。您可以根據結果微調每項功能 (如網路服務、帳戶設定和 Windows 防火牆) 的安全性設定，並將這些設定套用至伺服器。

您可以在 Microsoft Technet 網站上尋找有關 SCW 工具的詳細資訊。

保護應用程式資源

安全性最佳做法是確保所有相關基礎結構即服務檔案都擁有適當權限。

針對您的基礎結構即服務安裝檢閱基礎結構即服務檔案。在大多數情況下，每個資料夾的子資料夾和檔案應該具有與資料夾相同的設定。

目錄或檔案	群組或使用者	完全控制	修改	讀取和執行	讀取	寫入
VMware\vCAC\Agents \<agent_name> \logs	系統	X	X	X	X	X
	管理員	X	X	X	X	X
	管理員	X	X	X	X	X
VMware\vCAC\Agents\ <agent_name> \temp	系統	X	X	X	X	X
	管理員	X	X	X	X	X

目錄或檔案	群組或使用者	完全控制	修改	讀取和執行	讀取	寫入
	管理員	X	X	X	X	X
VMware\vCAC\Agents\	系統	X	X	X	X	X
	管理員	X	X	X	X	X
	使用者			X	X	
VMware\vCAC\Distributed Execution Manager\	系統	X	X	X	X	X
	管理員	X	X	X	X	X
	使用者			X	X	
VMware\vCAC\Distributed Execution Manager\DEM\Logs	系統	X	X	X	X	X
	管理員	X	X	X	X	X
	管理員	X	X	X	X	X
VMware\vCAC\Distributed Execution Manager\DEO\Logs	系統	X	X	X	X	X
	管理員	X	X	X	X	X
	管理員	X	X	X	X	X
VMware\vCAC\Management Agent\	系統	X	X	X	X	X
	管理員	X	X	X	X	X
	使用者			X	X	
VMware\vCAC\Server\	系統	X	X	X	X	X
	管理員	X	X	X	X	X
	使用者			X	X	
VMware\vCAC\Web API	系統	X	X	X	X	X
	管理員	X	X	X	X	X
	使用者			X	X	

保護基礎結構即服務主機的安全

安全性最佳做法是，檢閱基礎結構即服務 (IaaS) 主機的基本設定，確保其符合安全準則。

保護基礎結構即服務 (IaaS) 主機上的其他帳戶、應用程式、連接埠以及服務的安全。

確認伺服器使用者帳戶設定

確認不存在不必要的本機和網域使用者帳戶及設定。將與應用程式功能無關的所有使用者帳戶限制為進行管理、維護和疑難排解所需的功能。將網域使用者帳戶的遠端存取權限制為維護伺服器所需的最低權限。嚴格控制和稽核這些帳戶。

刪除不必要的應用程式

從主機伺服器中刪除所有不必要的應用程式。不必要的應用程式由於具備未知或未修補的漏洞，會提高暴露風險。

停用不必要的連接埠和服務

檢閱主機伺服器防火牆的開啟連接埠清單。封鎖對 IaaS 元件或關鍵系統作業非必要的所有連接埠。請參閱設定連接埠和通訊協定。稽核對主機伺服器執行的服務，並停用不需要的服務。

8 設定主機網路安全性

為了針對已知的安全性威脅提供最強的防禦，請在所有 VMware 主機上進行網路介面與通訊的設定。

在全面的安全性計劃中，請根據既定的安全性準則，針對 VMware 虛擬應用裝置以及基礎結構即服務元件進行網路介面安全性設定。

本章節討論下列主題：

為 VMware 應用裝置進行網路設定

為了確保您的 VMware 虛擬應用裝置主機僅支援安全的基本通訊，請檢閱並編輯其網路通訊設定。

根據安全性準則，檢查 VMware 主機的網路 IP 通訊協定組態，以及進行網路設定。停用所有非必要的通訊協定。

阻止使用者控制網路介面

安全性最佳做法是允許使用者僅具有在 VMware 應用裝置主機上完成其工作所需的系統權限。

允許具有權限的使用者帳戶操縱網路介面會導致略過網路安全性機制或拒絕服務。限制具有權限的使用者變更網路介面設定的能力。

程序

1 在每個 VMware 應用裝置主機上執行下列命令。

```
# grep –i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*
```

2 請確保每個介面都設為 NO。

設定 TCP 待處理項目佇列大小

若要針對惡意攻擊提供一定程度的防禦，請在 VMware 應用裝置主機上設定預設 TCP 待處理項目佇列大小。

將 TCP 待處理項目佇列大小設定為適當的預設大小，以降低 TCP 拒絕服務攻擊的風險。建議的預設設定為 1280。

程序

1 在每個 VMware 應用裝置主機上執行以下命令。

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```

2 在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 透過將以下項目新增至該檔案來設定預設 TCP 待處理項目佇列大小。

```
net.ipv4.tcp_max_syn_backlog=1280
```

4 儲存變更並關閉此檔案。

拒絕 ICMPv4 廣播位址回應

安全性最佳做法是確認您的 VMware 應用裝置主機忽略 ICMP 廣播位址回應要求。

對廣播網際網路控制訊息通訊協定 (ICMP) 回應進行回應會為放大攻擊提供攻擊媒介，並且可能會讓惡意代理程式更容易進行網路對應。將您的應用裝置主機設定為忽略 ICMPv4 回應，可以抵禦此類攻擊。

程序

1 在 VMware 虛擬應用裝置主機上執行 `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` 命令，以確認這些主機拒絕 IPv4 廣播位址回應要求。

如果主機設定為拒絕 IPv4 重新導向，則此命令會針對 `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` 傳回值 0。

2 若要將虛擬應用裝置主機設定為拒絕 ICMPv4 廣播位址回應要求，請在 Windows 主機的文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 找到內容為 `net.ipv4.icmp_echo_ignore_broadcasts=0` 的項目。如果該項目的值未設定為零或是該項目不存在，請新增該項目或相應地更新現有項目。

4 儲存變更並關閉檔案。

停用 IPv4 Proxy ARP

確認 IPv4 Proxy ARP 已停用，以防未經授權的資訊共用 (除非您的 VMware 應用裝置主機有其他要求)。

IPv4 Proxy ARP 允許系統代表連線至一個介面的主機傳送對另一個介面上 ARP 要求的回應。如果不需要防止附加網路區段之間的定址資訊洩漏，請將其停用。

程序

1 在 VMware 虛擬應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp| egrep "default|all"` 命令，以確認 IPv4 Proxy ARP 已停用。

如果在主機上停用 IPv6 Proxy ARP，此命令將傳回值 0。

```
/proc/sys/net/ipv4/conf/all/proxy_arp:0
/proc/sys/net/ipv4/conf/default/proxy_arp:0
```

如果主機已正確設定，則無需進行進一步動作。

2 如果需要在主機上設定 IPv6 Proxy ARP，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 檢查下列項目。

```
net.ipv4.conf.default.proxy_arp=0
net.ipv4.conf.all.proxy_arp=0
```

如果這些項目不存在或是其值未設定為零，請新增這些項目或相應地更新現有項目。

4 儲存您進行的任何變更並關閉檔案。

拒絕 IPv4 ICMP 重新導向訊息

安全性最佳做法是確認您的 VMware 虛擬應用裝置主機拒絕 IPv4 ICMP 重新導向訊息。

路由器使用 ICMP 重新導向訊息來通知主機，目的地存在更直接的路由器。惡意的 ICMP 重新導向訊息容易產生攔截式攻擊。這些訊息會修改主機的路由器資料表且未經驗證。如果不需要這些訊息，請確保您的系統設定為忽略這些訊息。

程序

1 在 VMware 應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep "default|all"` 命令，以確認這些主機拒絕 IPv4 重新導向訊息。

如果主機設定為拒絕 IPv4 重新導向，則此命令會傳回下列內容：

`/proc/sys/net/ipv4/conf/all/accept_reidrects:0`

`/proc/sys/net/ipv4/conf/default/accept_redirects:0`

2 如果需要將虛擬應用裝置主機設定為拒絕 IPv4 重新導向訊息，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 查看開頭為 `net.ipv4.conf` 的幾行的值。

如果以下項目的值未設定為零或是這些項目不存在，請新增至檔案或相應地更新現有項目。

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

4 儲存您進行的任何變更並關閉檔案。

拒絕 IPv6 ICMP 重新導向訊息

安全性最佳做法是確認您的 VMware 虛擬應用裝置主機會拒絕 IPv6 ICMP 重新導向訊息。

路由器使用 ICMP 重新導向訊息來通知主機，目的地存在更直接的路由器。惡意的 ICMP 重新導向訊息容易產生攔截式攻擊。這些訊息會修改主機的路由器資料表且未經驗證。若無其他必要用途，請務必將您的系統設定為忽略這些訊息。

程序

1 在 VMware 虛擬應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects| egrep "default|all"` 命令，確認這些主機會拒絕 IPv6 重新導向訊息。

如果主機設定為拒絕 IPv6 重新導向，則此命令會傳回下列結果：

`/proc/sys/net/ipv6/conf/all/accept_redirects:0`

`/proc/sys/net/ipv6/conf/default/accept_redirects:0`

2 若要將虛擬應用裝置主機設定為拒絕 IPv4 重新導向訊息，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 查看開頭為 `net.ipv6.conf` 的幾行的值。

如果下列項目的值未設為零，或是下列項目不存在，請將下列項目新增至檔案，或相應更新現有項目。

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

4 儲存變更並關閉檔案。

記錄 IPv4 Martian 封包

安全性最佳做法是確認您的 VMware 虛擬應用裝置主機會記錄 IPv4 Martian 封包。

Martian 封包包含系統已知無效的位址。請將主機設定為記錄這些訊息，讓您能夠識別錯誤組態或進行中的攻擊。

程序

1 在 VMware 應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians|egrep "default|all"` 命令，確認這些主機會記錄 IPv4 Martian 封包。

如果虛擬機器已設定為記錄 Martian 封包，則會傳回下列結果：

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/default/log_martians:1
```

如果主機已正確設定，則無需進行進一步動作。

2 如果您需要將虛擬機器設定為記錄 IPv4 Martian 封包，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 查看開頭為 `net.ipv4.conf` 的幾行的值。

如果下列項目的值未設為 1，或是下列項目不存在，請將下列項目新增至檔案，或是相應更新現有項目。

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

4 儲存變更並關閉此檔案。

使用 IPv4 反向路徑篩選

安全性最佳做法是確認您的 VMware 虛擬應用裝置主機使用 IPv4 反向路徑篩選。

反向路徑篩選可以透過讓系統捨棄來源位址不具有路由或路由不指向原始介面的封包，來抵禦偽造的來源位址。請盡可能將您的主機設定為使用反向路徑篩選。在某些情況下，取決於系統角色，反向路徑篩選可能會導致系統捨棄合法流量。如果您遇到此類問題，可能需要使用更寬鬆的模式或是完全停用反向路徑篩選。

程序

1 在 VMware 虛擬應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"` 命令，確認這些機器使用 IPv4 反向路徑篩選。

如果虛擬機器使用 IPv4 反向路徑篩選，此命令會傳回下列內容：

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/re_filter:1
```

如果虛擬機器的設定正確，則無需執行進一步的動作。

2 如果需要在主機上設定 IPv4 反向路徑篩選，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 查看開頭為 `net.ipv4.conf` 的幾行的值。

如果下列項目的值不是設為 1 或者項目不存在，請新增這些項目至檔案或相應地更新現有項目。

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

4 儲存變更並關閉檔案。

拒絕 IPv4 轉送

確認您的 VMware 應用裝置主機拒絕 IPv4 轉送。

如果系統已針對 IP 轉送進行設定但不是指定的路由器，則攻擊者可能會透過為網路裝置未篩選的通訊提供路徑，利用此系統來略過網路安全性。請將您的虛擬應用裝置主機設定為拒絕 IPv4 轉送來避免這一風險。

程序

1 在 VMware 應用裝置主機上執行 `# cat /proc/sys/net/ipv4/ip_forward` 命令，以確認這些主機拒絕 IPv4 轉送。

如果主機設定為拒絕 IPv4 轉送，則此命令會針對 `/proc/sys/net/ipv4/ip_forward` 傳回值 0。如果虛擬機器已正確設定，則無需進行進一步動作。

2 若要將虛擬應用裝置主機設定為拒絕 IPv4 轉送，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 找到內容為 `net.ipv4.ip_forward=0` 的項目。如果該項目的值目前未設定為零或是該項目不存在，請新增該項目或相應地更新現有項目。

4 儲存任何變更並關閉檔案。

拒絕 IPv6 轉送

安全性最佳做法是確認您的 VMware 應用裝置主機系統拒絕 IPv6 轉送。

如果系統已針對 IP 轉送進行設定但不是指定的路由器，則攻擊者可能會透過為網路裝置未篩選的通訊提供路徑，利用此系統來略過網路安全性。請將您的虛擬應用裝置主機設定為拒絕 IPv6 轉送來避免這一風險。

程序

1 在 VMware 應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding|egrep "default|all"` 命令，以確認這些主機拒絕 IPv6 轉送。

如果主機設定為拒絕 IPv6 轉送，則此命令會傳回下列內容：

```
/proc/sys/net/ipv6/conf/all/forwarding:0
/proc/sys/net/ipv6/conf/default/forwarding:0
```

如果主機已正確設定，則無需進行進一步動作。

2 如果需要將主機設定為拒絕 IPv6 轉送，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 查看開頭為 `net.ipv6.conf` 的幾行的值。

如果以下項目的值未設定為零或是這些項目不存在，請新增這些項目或相應地更新現有項目。

```
                net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

4 儲存您進行的任何變更並關閉檔案。

使用 IPv4 TCP Syncookie

確認您的 VMware 應用裝置主機使用 IPv4 TCP Syncookie。

透過用 SYN_RCVD 狀態的連線填滿系統的 TCP 連線表，TCP SYN 洪水攻擊可能會導致拒絕服務。Syncookie 可阻止追蹤連線，直到收到後續 ACK 並確認啟動器正嘗試有效連線且不是洪水來源為止。此技術的運作方式雖然不完全符合標準，但僅在出現洪水攻擊情況時啟用，並且可在防護系統的同時繼續為有效要求提供服務。

程序

1 在 VMware 應用裝置主機上執行 `# cat /proc/sys/net/ipv4/tcp_syncookies` 命令，以確認這些主機是否使用 IPv4 TCP Syncookie。

如果主機設定為拒絕 IPv4 轉送，此命令會針對 `/proc/sys/net/ipv4/tcp_syncookies` 傳回值 1。如果虛擬機器已正確設定，則無需進行進一步動作。

2 如果需要將虛擬應用裝置設定為使用 IPv4 TCP Syncookie，請在文字編輯器中開啟 `/etc/sysctl.conf`。

3 找到內容為 `net.ipv4.tcp_syncookies=1` 的項目。

如果此項目的值目前未設定為 1 或其不存在，請新增該項目或相應地更新現有項目。

4 儲存您進行的任何變更並關閉檔案。

拒絕 IPv6 路由器通告

確認 VMware 主機拒絕接受路由器通告和 ICMP 重新導向 (除非系統運作需要接受)。

IPv6 可讓系統透過自動使用網路中的資訊來設定其網路裝置。從安全性角度而言，與以未經驗證的方式接受網路中的資訊相比，手動設定重要組態資訊更為可取。

程序

1 在 VMware 應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra|egrep "default|all"` 命令，以確認這些主機拒絕路由器通告。

如果主機設定為拒絕 IPv6 路由器通告，則此命令會傳回值 0：

```
/proc/sys/net/ipv6/conf/all/accept_ra:0
/proc/sys/net/ipv6/conf/default/accept_ra:0
```

如果主機已正確設定，則無需進行進一步動作。

2 如果需要將主機設定為拒絕 IPv6 路由器通告，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 檢查下列項目。

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

如果這些項目不存在或是其值未設定為零，請新增這些項目或相應地更新現有項目。

4 儲存您進行的任何變更並關閉檔案。

拒絕 IPv6 路由器請求

安全性最佳做法是確認您的 VMware 應用裝置主機拒絕 IPv6 路由器請求 (除非系統運作需要接受)。

路由器請求設定可決定啟動介面時傳送的路由器請求數量。如果已靜態指派位址，則無需傳送任何請求。

程序

1 在 VMware 應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations|egrep "default|all"` 命令，以確認這些主機拒絕 IPv6 路由器請求。

如果主機設定為拒絕 IPv6 路由器通告，則此命令會傳回下列內容：

```
/proc/sys/net/ipv6/conf/all/router_solicitations:0
/proc/sys/net/ipv6/conf/default/router_solicitations:0
```

如果主機已正確設定，則無需進行進一步動作。

2 如果需要將主機設定為拒絕 IPv6 路由器請求，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 檢查下列項目。

```
net.ipv6.conf.all.router_solicitations=0
net.ipv6.conf.default.router_solicitations=0
```

如果這些項目不存在或是其值未設定為零，請新增這些項目或相應地更新現有項目。

4 儲存任何變更並關閉檔案。

拒絕路由器請求中的 IPv6 路由器喜好設定

確認您的 VMware 應用裝置主機拒絕 IPv6 路由器請求 (除非系統運作需要接受)。

請求設定中的路由器喜好設定可決定路由器的喜好設定。如果已靜態指派位址，則無需接收請求中的任何路由器喜好設定。

程序

1 在 VMware 應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref|egrep "default|all"` 命令，以確認這些主機拒絕 IPv6 路由器請求。

如果主機設定為拒絕 IPv6 路由器通告，則此命令會傳回下列內容：

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

如果主機已正確設定，則無需進行進一步動作。

2 如果需要將主機設定為拒絕 IPv6 路由器請求，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 檢查下列項目。

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

如果這些項目不存在或是其值未設定為零，請新增這些項目或相應地更新現有項目。

4 儲存您進行的任何變更並關閉檔案。

拒絕 IPv6 路由器前置詞

確認您的 VMware 應用裝置主機拒絕 IPv6 路由器前置詞資訊 (除非系統運作需要接受)。

`accept_ra_pinfo` 設定可控制系統是否接受路由器的前置詞資訊。如果已靜態指派位址，則無需接收任何路由器前置詞資訊。

程序

1 在 VMware 應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo|egrep "default|all"` 命令，以確認這些主機拒絕 IPv6 路由器前置詞資訊。

如果主機設定為拒絕 IPv6 路由器通告，則此命令會傳回下列內容。

```
/proc/sys/net/ipv6/conf/all/accept_ra_pinfo:0
/proc/sys/net/ipv6/conf/default/accept_ra_pinfo:0
```

如果主機已正確設定，則無需進行進一步動作。

2 如果需要將主機設定為拒絕 IPv6 路由器前置詞資訊，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 檢查下列項目。

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

如果這些項目不存在或是其值未設定為零，請新增這些項目或相應地更新現有項目。

4 儲存任何變更並關閉檔案。

拒絕 IPv6 路由器通告躍點限制設定

確認您的 VMware 應用裝置主機拒絕 IPv6 路由器躍點限制設定 (除非有必要)。

`accept_ra_defrtr` 設定可控制系統是否接受路由器通告的躍點限制設定。將其設定為零可防止路由器變更傳出封包的預設 IPv6 躍點限制。

程序

1 在 VMware 應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr|egrep "default|all"` 命令，以確認這些主機拒絕 IPv6 路由器躍點限制設定。

如果主機設定為拒絕 IPv6 路由器躍點限制設定，則此命令會傳回值 0。

```
/proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
/proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
```

如果主機已正確設定，則無需進行進一步動作。

2 如果需要將主機設定為拒絕 IPv6 路由器躍點限制設定，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 檢查下列項目。

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

如果這些項目不存在或是其值未設定為零，請新增這些項目或相應地更新現有項目。

4 儲存您進行的任何變更並關閉檔案。

拒絕 IPv6 路由器通告自動組態設定

確認您的 VMware 應用裝置主機拒絕 IPv6 路由器自動組態設定 (除非有必要)。

`autoconf` 設定可控制路由器通告是否能夠使系統向介面指派全域單點傳播位址。

程序

1 在 VMware 應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf|egrep "default|all"` 命令，以確認這些主機拒絕 IPv6 路由器自動組態設定。

如果主機設定為拒絕 IPv6 路由器自動組態設定，則此命令會傳回值 0。

```
/proc/sys/net/ipv6/conf/all/autoconf:0
/proc/sys/net/ipv6/conf/default/autoconf:0
```

如果主機已正確設定，則無需進行進一步動作。

2 如果需要將主機設定為拒絕 IPv6 路由器自動組態設定，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 檢查下列項目。

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

如果這些項目不存在或是其值未設定為零，請新增這些項目或相應地更新現有項目。

4 儲存您進行的任何變更並關閉檔案。

拒絕 IPv6 芳鄰請求

確認您的 VMware 應用裝置主機拒絕 IPv6 芳鄰請求 (除非有必要)。

`dad_transmits` 設定可決定啟動介面時每個位址 (全域及連結-本機) 傳送的芳鄰請求數量，以確保所需位址在網路中的唯一性。

程序

1 在 VMware 應用裝置主機上執行 `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits| egrep "default|all"` 命令，以確認這些主機拒絕 IPv6 芳鄰請求。

如果主機設定為拒絕 IPv6 芳鄰請求，則此命令會傳回值 0。

```
/proc/sys/net/ipv6/conf/all/dad_transmits:0
/proc/sys/net/ipv6/conf/default/dad_transmits:0
```

如果主機已正確設定，則無需進行進一步動作。

2 如果需要將主機設定為拒絕 IPv6 芳鄰請求，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 檢查下列項目。

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

如果這些項目不存在或是其值未設定為零，請新增這些項目或相應地更新現有項目。

4 儲存您進行的任何變更並關閉檔案。

限制 IPv6 位址數目上限

確認 VMware 應用裝置主機將 IPv6 位址數目上限設定為系統作業所需的最小值。

位址數目上限決定每個介面可用的全域單點傳播 IPv6 位址數目。雖然預設值為 16，但應將其精確設定為系統所需的靜態設定全域位址數目。

程序

1 在 VMware 應用裝置主機上執行 `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses| egrep "default|all"` 命令，確認這些主機正確限制 IPv6 位址數目上限。

如果已設定主機以限制 IPv6 位址數目上限，此命令將傳回值 1。

```
/proc/sys/net/ipv6/conf/all/max_addresses:1
/proc/sys/net/ipv6/conf/default/max_addresses:1
```

如果主機已正確設定，則無需進行進一步動作。

2 如果需要設定主機上的 IPv6 位址數目上限，請在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。

3 檢查下列項目。

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

如果這些項目不存在或它們的值未設定為 1，請新增這些項目或相應地更新現有項目。

4 儲存您進行的任何變更並關閉檔案。

為基礎結構即服務主機進行網路設定

安全性最佳做法是根據 VMware 需求與準則，在 VMware 基礎結構即服務 (IaaS) 元件主機上進行網路通訊設定。

設定基礎結構即服務 (IaaS) 主機的網路組態，以透過適當的安全性來支援完整的 vRealize Automation 功能。

請參閱保護基礎結構即服務元件。

設定連接埠和通訊協定

安全性最佳做法是依據 VMware 準則為所有 vRealize Automation 應用裝置和元件設定連接埠和通訊協定。

視需要為 vRealize Automation 元件設定傳入和傳出連接埠，供關鍵系統元件在生產中運作。停用所有不需要的連接埠和通訊協定。請參閱 VMware vRealize Automation 說明文件中的《vRealize Automation 參考架構》。

「連接埠和通訊協定」工具

「連接埠和通訊協定」工具可讓您在單一儀表板上檢視各種 VMware 產品及其組合的連接埠資訊。您也可以從工具中匯出所選資料以供離線存取。連接埠和通訊協定工具目前支援：

- vSphere
- vSAN
- NSX for vSphere
- vRealize Network Insight
- vRealize Operations Manager
- vRealize Automation

此工具可在 https://ports.vmware.com/ 上取得。

使用者所需的連接埠

安全性最佳做法是根據 VMware 準則來設定 vRealize Automation 使用者連接埠。

僅在安全的網路上公開必要的連接埠。

伺服器	連接埠
vRealize Automation 應用裝置	443、8443

管理員必要的連接埠

安全性最佳做法是根據 VMware 準則來設定 vRealize Automation 管理員連接埠。

僅在安全的網路上公開必要的連接埠。

伺服器	連接埠
vRealize Application Services 伺服器	5480

vRealize Automation 應用裝置連接埠

安全性最佳做法是根據 VMware 建議設定 vRealize Automation 應用裝置 的傳入和傳出連接埠。

傳入連接埠

設定 vRealize Automation 應用裝置 所需的傳入連接埠數下限。請視系統組態需要設定選擇性連接埠。

表 8-1. 所需的最少傳入連接埠

連接埠	通訊協定	註解
443	TCP	存取 vRealize Automation 主控台及 API 呼叫。
8443	TCP	VMware Remote Console Proxy。
5480	TCP	存取 vRealize Automation 應用裝置管理介面。
5488, 5489	TCP	內部。由 vRealize Automation 應用裝置 用於更新。
5672	TCP	RabbitMQ 訊息傳送。 **備註** 叢集 vRealize Automation 應用裝置 執行個體時，您可能需要設定開啟連接埠 4369 和 25672。
40002	TCP	vIDM 服務的所需項。在 HA 組態中新增該項後，將封鎖所有外部流量 (來自其他 vRealize Automation 應用裝置 節點的流量除外)。

視需要設定選擇性傳入連接埠。

表 8-2. 選擇性傳入連接埠

連接埠	通訊協定	註解
22	TCP	(選擇性) SSH。在生產環境中，在連接埠 22 上停用接聽 SSH 服務，並關閉連接埠 22。
80	TCP	(選擇性) 重新導向至 443。

傳出連接埠

設定所需的傳出連接埠。

表 8-3. 所需的最少傳出連接埠

連接埠	通訊協定	註解
25、587	TCP、UDP	傳送輸出通知電子郵件的 SMTP。
53	TCP、UDP	DNS。
67, 68, 546, 547	TCP、UDP	DHCP。
110, 995	TCP、UDP	接收輸入通知電子郵件的 POP。
143, 993	TCP、UDP	接收輸入通知電子郵件的 IMAP。
443	TCP	透過 HTTPS 的基礎結構即 Service Manager 服務。

視需要設定選擇性傳出連接埠。

表 8-4. 選擇性的傳出連接埠

連接埠	通訊協定	註解
80	TCP	(選擇性) 供提取軟體更新。您可以個別下載並套用更新。
123	TCP、UDP	(選擇性) 供直接連線至 NTP，而非使用主機時間。

「連接埠和通訊協定」工具

「連接埠和通訊協定」工具可讓您在單一儀表板上檢視各種 VMware 產品及其組合的連接埠資訊。您也可以從工具中匯出所選資料以供離線存取。連接埠和通訊協定工具目前支援：

- vSphere
- vSAN
- NSX for vSphere
- vRealize Network Insight
- vRealize Operations Manager
- vRealize Automation

這些工具可在 https://ports.vmware.com/ 上取得。

基礎結構即服務連接埠

安全性最佳做法是根據 VMware 準則，為基礎結構即服務 (IaaS) 元件設定傳入與傳出連接埠。

傳入連接埠

請為 IaaS 元件設定所需的最少傳入連接埠。

表 8-5. 所需的最少傳入連接埠

元件	連接埠	通訊協定	註解
Manager Service	443	TCP	透過 HTTPS 來與 IaaS 元件及 vRealize Automation 應用裝置通訊。任何受 Proxy 代理程式管理的虛擬化主機也都必須開放 TCP 連接埠 443，以供接收傳入流量

傳出連接埠

請為 IaaS 元件設定所需的最少傳出連接埠。

表 8-6. 所需的最少傳出連接埠

元件	連接埠	通訊協定	註解
全部	53	TCP、UDP	DNS。
全部		TCP、UDP	DHCP。
Manager Service	443	TCP	透過 HTTPS 與 vRealize Automation 應用裝置通訊。
網站	443	TCP	透過 HTTPS 與 Manager Service 通訊。
Distributed Execution Manager	443	TCP	透過 HTTPS 與 Manager Service 通訊。
Proxy 代理程式	443	TCP	透過 HTTPS 來與 Manager Service 及虛擬化主機通訊。
客體代理程式	443	TCP	透過 HTTPS 與 Manager Service 通訊。
Manager Service、網站	1433	TCP	MSSQL。

如有需要，設定選擇性的傳出連接埠。

表 8-7. 選擇性的傳出連接埠

元件	連接埠	通訊協定	註解
全部	123	TCP、UDP	NTP 是選擇性的。

稽核與記錄

9

安全性最佳做法是按照 VMware 的建議，在您的 vRealize Automation 系統上設定稽核與記錄。

遠端記錄至中央記錄主機，可為記錄檔提供安全的存放區。透過將記錄檔收集至中央主機，您可以使用單一工具來監控環境。此外，您也可以執行彙總分析，以及在基礎結構中的多個項目上搜尋協調式攻擊之類的威脅證據。記錄至安全的集中式記錄伺服器，有助於防止記錄遭篡改，並能提供長期稽核記錄。

確保遠端記錄伺服器安全無虞

攻擊者破壞主機的安全性後，通常都會嘗試搜尋並篡改記錄檔，以遮掩他們的行蹤，並在不被發現的情況下繼續控制主機。適當地保護遠端記錄伺服器，有助於阻止記錄遭篡改。

使用獲授權的 NTP 伺服器

確保所有主機使用相同的相對時間來源，包括相關的當地語系化時差，並確保您可將相對時間來源關聯至商定的時間標準，例如國際標準時間 (UTC)。有原則地管理時間來源，可讓您在檢閱相關記錄檔時，迅速追蹤並關聯入侵者的動作。不正確的時間設定會讓您難以檢查和關聯要偵測攻擊的記錄檔，且會導致稽核不準確。

請至少使用外部時間來源的三個 NTP 伺服器，或者在信任的網路上設定幾個本機 NTP 伺服器，然後再從至少三個外部時間來源取得時間。