

安全組態

2020 年 11 月 20 日

vRealize Operations Manager 7.5

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/>

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

Copyright © 2021 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

目錄

安全組態 6

1 vRealize Operations Manager 安全性狀態 7

2 保護 vRealize Operations Manager 部署的安全 8

驗證安裝媒體的完整性 8

強化已部署軟體基礎架構 8

強化 VMware vSphere 環境 9

檢閱已安裝與不支援的軟體 9

驗證第三方軟體 9

VMware 安全性諮詢與修補 9

3 vRealize Operations Manager 的安全組態 10

確保 vRealize Operations Manager 主控台安全 11

變更根密碼 11

管理密碼有效期限 11

管理安全殼層、管理員帳戶和主控台存取 12

啟用或停用 vRealize Operations Manager 節點的安全殼層 13

為安全殼層建立本機管理員帳戶 13

限制安全殼層存取 14

維護安全殼層金鑰檔案權限 14

強化安全殼層伺服器組態 15

強化安全殼層用戶端組態 15

停用以根使用者身分直接登入 16

停用 Admin 使用者帳戶的 SSH 存取權 16

設定開機載入器驗證 17

單一使用者或維護模式驗證 17

監控基本必要使用者帳戶 17

監控基本必要群組 18

重設 vRealize Operations Manager 管理員密碼 (Linux) 19

設定 VMware 應用裝置的 NTP 19

在 Linux 上停用 TCP 時間戳記回應 19

啟用 FIPS 140-2 模式 20

為傳遞中的資料使用 TLS 20

為 vRealize Operations Manager 設定強式通訊協定 20

設定 vRealize Operations Manager 使用強式加密方式 22

針對 Localhost 連線啟用 TLS 23

使用 OpenSSL 產生或提供您自己的自我簽署憑證	24
為 PostgreSQL 安裝憑證	24
針對 PostgreSQL 啟用 TLS	24
必須保護的應用程式資源	24
Apache 組態	26
停用 Web 目錄瀏覽	26
移除 Apache2 伺服器的範例程式碼	26
驗證 Apache2 伺服器的伺服器 Token	26
停用 Apache2 伺服器的 Trace 方法	27
停用組態模式	27
管理不重要的軟體元件	27
保護 USB 大型存放處理常式的安全	27
保護藍牙通訊協定處理常式的安全	27
保護串流控制傳輸通訊協定的安全	28
保護資料包壅塞控制通訊協定的安全	28
保護可靠資料包通訊端通訊協定通訊協定的安全	29
保護透明程序間通訊通訊協定的安全	29
保護網際網路封包交換通訊協定的安全	29
保護 AppleTalk 通訊協定的安全	29
保護 DECnet 通訊協定的安全	30
保護 Firewire 模組的安全	30
核心訊息記錄	30
End Point Operations Management 代理程式	31
執行 End Point Operations Management 代理程式的最佳安全性做法	31
執行代理程式功能所需的最低必要權限	31
開啟代理程式主機上的連接埠	34
撤銷代理程式	34
代理程式憑證撤銷與憑證更新	36
End Point Operations Management 代理程式的修補與更新	36
其他安全組態活動	36
確認伺服器使用者帳戶設定	36
刪除並停用不必要的應用程式	37
停用不必要的連接埠與服務	37

4 網路安全性與安全通訊 38

為虛擬應用程式安裝進行網路設定	38
防止使用者控制網路介面	38
設定 TCP 待處理項目的佇列大小	38
拒絕 ICMPv4 廣播位址回應	39
設定主機系統以停用 IPv4 Proxy ARP	39
設定主機系統以忽略 IPv4 ICMP 重新導向訊息	40

設定主機系統以忽略 IPv6 ICMP 重新導向訊息	40
設定主機系統以拒絕 IPv4 ICMP 重新導向	40
設定主機系統以記錄 IPv4 Martian 封包	41
設定主機系統以使用 IPv4 反向路徑篩選	41
設定主機系統以拒絕 IPv4 轉送	42
設定主機系統拒絕 IPv4 來源路由封包的轉送	42
設定主機系統以拒絕 IPv6 轉送	43
設定主機系統使用 IPv4 TCP SYN Cookie	43
設定主機系統以拒絕 IPv6 路由器公告	43
設定主機系統以拒絕 IPv6 路由器邀請	44
設定主機系統以拒絕路由器邀請中的 IPv6 路由器喜好設定	44
設定主機系統以拒絕 IPv6 路由器前置詞	45
設定主機系統以拒絕 IPv6 路由器公告躍點限制設定	45
設定主機系統以拒絕 IPv6 路由器公告 Autoconf 設定	46
設定主機系統以拒絕 IPv6 芳鄰邀請	46
設定主機系統來限制 IPv6 位址數上限	46
設定連接埠和通訊協定	47
最低要求的預設傳入連接埠	47

5 vRealize Operations Manager 系統上的稽核與記錄 49

保護遠端記錄伺服器	49
使用獲授權的 NTP 伺服器	49
用戶端瀏覽器考量事項	49

安全組態

「安全組態」的說明文件可作為 vRealize Operations Manager 部署的安全基準。如果您是使用系統監控工具，確保持續監控和維護安全基準組態，以得知意外的變更，那麼請參閱本文件。

非預設設定的強化活動可以手動執行。

預定對象

這些資訊適合 vRealize Operations Manager 的管理員閱讀。

vRealize Operations Manager 安全性狀態

1

vRealize Operations Manager 的安全性狀態是根據系統與網路組態、組織安全性原則及最佳做法，造就一個完整的安全環境。很重要的是，您必須根據組織的安全性原則與最佳做法來執行強化活動。

本文件分為以下三節：

- 安全部署
- 安全組態
- 網路安全性
- 通訊

本指南將詳述虛擬應用程式的安裝。

若要確保系統能夠安全地強化，請檢閱建議事項，並根據您組織的安全性原則與風險曝險程度來評估建議事項。

保護 vRealize Operations Manager 部署的安全

2

在安裝產品之前，必須先確認安裝媒體的完整性，以確保下載檔案的真確性。

本章節討論下列主題：

- 驗證安裝媒體的完整性
- 強化已部署軟體基礎架構
- 檢閱已安裝與不支援的軟體
- VMware 安全性諮詢與修補

驗證安裝媒體的完整性

下載媒體之後，請使用 MD5/SHA1 總合檢查碼的值來確認下載的完整性。下載 ISO、離線服務包或修補程式後，請務必確認 MD5/SHA1 雜湊，以確保所下載檔案的完整性及真確性。如果您是從 VMware 取得實體媒體，而安全封裝已遭到破壞，請將軟體退回 VMware，以更換新品。

程序

- ◆ 比較 MD5/SHA1 雜湊輸出與 VMware 網站上張貼的值。

SHA1 或 MD5 雜湊應該相符。

備註 vRealize Operations Manager 6.x-x.pak/7.x-x.pak 檔案是由 VMware 軟體發佈憑證所簽署。vRealize Operations Manager 會在安裝前先驗證 PAK 檔案的簽名。

強化已部署軟體基礎架構

在強化程序中，您必須強化支援 VMware 系統的已部署軟體基礎架構。

在強化 VMware 系統前，請先在支援軟體基礎架構中檢閱並處理安全性缺陷，以建立完全強化且安全的環境。要考量的軟體基礎架構元素包括作業系統元件、支援軟體和資料庫軟體。請依據製造商的建議和其他相關安全性通訊協定，處理這些元件和其他元件中的安全性考量。

強化 VMware vSphere 環境

vRealize Operations Manager 仰賴安全的 VMware vSphere 環境來獲得最大的好處和安全的基礎架構。

評估 VMware vSphere 環境，確認已強制執行和維持適當程度的 vSphere 強化指導方針。

如需強化的詳細指導方針，請參閱 <http://www.vmware.com/security/hardening-guides.html>。

檢閱已安裝與不支援的軟體

不使用之軟體中的漏洞有可能會增加未經授權存取系統和可用性中斷的風險。請檢閱安裝在 VMware 主機機器上的軟體，並評估其使用率。

請不要在 vRealize Operations Manager 節點主機上，安裝非系統安全作業所必需的軟體。不使用或不重要的軟體，請一律解除安裝。

在 vRealize Operations Manager 等基礎結構產品上安裝不受支援、未經測試或未經核准的軟體，會對基礎結構造成威脅。

若要盡量降低對基礎結構的威脅，請不要在 VMware 提供的主機上，安裝或使用 VMware 不支援的任何第三方軟體。

請評估您的 vRealize Operations Manager 部署和已安裝產品的詳細目錄，確認未安裝不受支援的軟體。

如需第三方產品支援原則的詳細資訊，請參閱 VMware 支援資訊：<http://www.vmware.com/security/hardening-guides.html>。

驗證第三方軟體

請勿使用 VMware 不支援的第三方軟體。請確認所有第三方軟體皆遵循第三方廠商的指導方針，具備完善的安全性設定和修補程式。

VMware 主機機器上所安裝第三方軟體的不可靠、不安全或未修補漏洞，可能會讓系統蒙受未經授權存取及可用性中斷的風險。VMware 不提供的所有軟體都必須受到妥善的保護並套用修補程式。

如果您必須使用 VMware 不支援的第三方軟體，請向第三方廠商詢問安全組態和修補需求。

VMware 安全性諮詢與修補

VMware 偶而會針對產品發佈安全性諮詢。留意這些安全性諮詢可以確保您擁有最安全的基本產品，而且該產品不容易受到已知威脅的侵害。

請評估 vRealize Operations Manager 安裝、修補和升級歷程記錄，並確認已遵循及強制執行發佈的 VMware 安全性諮詢。

建議您一律採用最新的 vRealize Operations Manager 版本，因為其中也會包含最新的安全性修正。

如需最新 VMware 安全性諮詢的詳細資訊，請參閱 <http://www.vmware.com/security/advisories/>。

vRealize Operations Manager 的安全組態

3

最佳安全性做法是保護 vRealize Operations Manager 主控台的安全，並管理安全殼層 (SSH)、管理員帳戶和主控台存取。請確保系統部署有安全傳輸通道。

另外，在執行 End Point Operations Management 代理程式時，也必須遵守一定的最佳安全性做法。

本章節討論下列主題：

- 確保 vRealize Operations Manager 主控台安全
- 變更根密碼
- 管理安全殼層、管理員帳戶和主控台存取
- 設定開機載入器驗證
- 單一使用者或維護模式驗證
- 監控基本必要使用者帳戶
- 監控基本必要群組
- 重設 vRealize Operations Manager 管理員密碼 (Linux)
- 設定 VMware 應用裝置的 NTP
- 在 Linux 上停用 TCP 時間戳記回應
- 啟用 FIPS 140-2 模式
- 為傳遞中的資料使用 TLS
- 針對 Localhost 連線啟用 TLS
- 必須保護的應用程式資源
- Apache 組態
- 停用組態模式
- 管理不重要的軟體元件
- End Point Operations Management 代理程式
- 其他安全組態活動

確保 vRealize Operations Manager 主控台安全

安裝 vRealize Operations Manager 後，您必須進行第一次登入，並確保叢集中每個節點主控台的安全。

必要條件

安裝 vRealize Operations Manager。

程序

- 1 在 vCenter 中找到節點主控台，或是直接存取節點主控台。
在 vCenter 中，按下 **Alt+F1** 存取登入提示。基於安全考量，依預設會停用 vRealize Operations Manager 遠端終端機工作階段。
- 2 以根使用者身分登入。
在您建立根密碼之前，vRealize Operations Manager 不會允許您存取命令提示字元。
- 3 看到密碼提示時按下 **Enter**。
- 4 看到舊密碼提示時按下 **Enter**。
- 5 系統提示您輸入新密碼時，輸入您要的根密碼，並記下以供日後參考。
- 6 重新輸入根密碼。
- 7 登出主控台。

變更根密碼

您可以使用主控台，隨時變更任何 vRealize Operations Manager 主要或資料節點的根密碼。

根使用者可略過 `etc/pam.d/common-password` 中的 `pam_cracklib` 模組密碼複雜度檢查。所有強化應用裝置都可為 `enforce_for_root` 模組啟用 `etc/pam.d/common-password` 檔案中的 `pw_history` 模組。系統預設會記住最後使用的五個密碼。每個使用者的舊密碼都會儲存在 `/etc/security/opasswd` 檔案中。

必要條件

確認應用裝置的根密碼符合組織的公司密碼複雜度要求。如果帳戶密碼是以 `6` 開頭，表示是使用 `sha512` 雜湊。這是所有強化應用裝置的標準雜湊。

程序

- 1 在應用裝置的根殼層執行 `# passwd` 命令。
- 2 若要驗證根密碼的雜湊，請以根使用者的身分登入，然後執行 `# more /etc/shadow` 命令。
隨後便會出現雜湊資訊。
- 3 如果根密碼不含 `sha512` 雜湊，請執行 `passwd` 命令變更根密碼。

管理密碼有效期限

您可以根據組織的安全性原則，設定所有帳戶的密碼有效期限。

依預設，所有強化的 VMware 應用裝置一律採用 60 天的密碼有效期限。在大部分的強化應用裝置上，根帳戶的密碼有效期限都是設定為 365 天。最佳做法是確認所有帳戶的有效期限都符合安全性與作業需求標準。

根密碼一旦過期，就不能恢復。因此您必須實作站台專屬的原則，防止管理員密碼與根密碼過期。

程序

- 1 請以根使用者身分登入您的虛擬應用裝置機器，然後執行 `# more /etc/shadow` 命令，確認所有帳戶的密碼有效期限。
- 2 若要修改根帳戶的有效期限，請執行 `# passwd -x 365 root` 命令。

在這個命令中，365 代表密碼的有效天數。請使用同一個命令來修改任何使用者，將 `root` 換成特定的帳戶，並且配合組織的有效期限標準來更改天數。

依預設，根密碼的有效期限是設定為 365 天。

管理安全殼層、管理員帳戶和主控台存取

針對遠端連線，所有強化的應用裝置都會包含安全殼層 (SSH) 通訊協定。依預設，強化應用裝置上會停用 SSH。

SSH 是互動式的命令列環境，支援遠端連線至 vRealize Operations Manager 節點。SSH 要求使用高權限的使用者帳戶認證。SSH 活動通常會略過角色型存取控制 (RBAC)，並且稽核 vRealize Operations Manager 節點的控制。

最佳做法是在生產環境中停用 SSH，只在診斷或疑難排解無法以其他方式解決的問題時才啟用。除非出於某個特定目的，以及配合組織的安全性原則，否則不要保持在啟用狀態。如果要啟用 SSH，請確保防護完善不會受到攻擊，而且僅在必要時啟用。您可以根據您的 vSphere 組態，在部署開放虛擬化格式 (OVF) 範本時，啟用或停用 SSH。

若要判斷機器上的 SSH 是否啟用，最簡單的測試方法是使用 SSH 來開啟連線。如果連線開啟並要求認證，表示 SSH 已啟用且可用於連線。

安全殼層根使用者

由於 VMware 應用裝置不含預先設定的預設使用者帳戶，因此依預設，根帳戶可以使用 SSH 直接登入。請以根使用者的身分立即停用 SSH。

為滿足符合性標準以確立不可否認性，所有強化應用裝置上的 SSH 伺服器都會預先設定 `AllowGroups wheel` 項目，限制 SSH 存取權僅授於次要群組 `wheel`。若要區分責任，您可以修改 `/etc/ssh/sshd_config` 檔案中的 `AllowGroups wheel` 項目，改用另一個群組 (例如 `sshd`)。

`wheel` 群組是以 `pam_wheel` 模組啟用，目的是取得 `superuser` 存取權，好讓 `wheel` 群組的成員能使用 `su-root` 命令 (使用此命令必須具備根密碼)。群組區分可讓使用者使用 SSH 存取用應用裝置，但無法使用 `su` 命令以根使用者的身分登入。請不要移除或修改 `AllowGroups` 欄位中的其他項目，以確保應用裝置正常運作。變更後，請執行 `# service sshd restart` 命令，重新啟動 SSH 常駐程式。

啟用或停用 vRealize Operations Manager 節點的安全殼層

您可以啟用 vRealize Operations Manager 節點的安全殼層 (SSH) 來進行疑難排解。例如，若要對伺服器進行疑難排解，可能需要該伺服器透過 SSH 的主控制台存取權。若為一般作業，則停用 vRealize Operations Manager 節點的 SSH。

程序

- 1 從 vCenter 存取 vRealize Operations Manager 節點的主控制台。
- 2 按下 Alt + F1 取得登入提示，然後登入。
- 3 執行 `#chkconfig` 命令。
- 4 若 SSHD 服務已關閉，請執行 `#chkconfig sshd on` 命令。
- 5 執行 `#service sshd start` 命令以啟動 SSHD 服務。
- 6 執行 `#service sshd stop` 命令以停止 SSHD 服務。

您也可以從 vRealize Operations Manager 管理介面的 **SSH 狀態** 資料行中，啟用或停用 Secure Shell。

為安全殼層建立本機管理員帳戶

您必須建立本機管理員帳戶，使其可使用安全殼層 (SSH) 並是次要 `wheel` 群組的成員，之後才能移除根 SSH 存取。

在停用直接根存取前，請使用 `AllowGroups` 來測試授權管理員是否可以存取 SSH，而且可以使用 `Wheel` 群組和 `su` 命令，以根使用者的身分登入。

程序

- 1 以根使用者身分登入並執行下列命令。

```
# useradd -d /home/vropsuser -g users -G wheel -m
# passwd username
```

`Wheel` 是針對 SSH 存取，在 `AllowGroups` 中指定的群組。若要新增多個次要群組，請使用 `-G wheel,sshd`。

- 2 切換為該使用者並提供新密碼，以確定執行密碼複雜度檢查。

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

若密碼達到密碼複雜度，便會更新。若密碼未達到密碼複雜度，便會還原為原始密碼，您必須重新執行密碼命令。

在您建立登入帳戶以允許 SSH 遠端存取，並且使用 `su` 命令與 `wheel` 存取權以根使用者身分登入後，便可以移除 SSH 直接登入的根帳戶。

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

後續步驟

停用以根使用者身分直接登入。依預設，強化後的應用裝置允許透過主控台直接登入根使用者。在您建立管理員帳戶以確立不可否認性，並測試帳戶的 `wheel` 存取權 (`su-root`) 後，請以根使用者的身分編輯 `/etc/securetty` 檔案，並以 `console` 取代 `tty1`，藉此停用直接根登入。

限制安全殼層存取

您可以在系統強化的程序中，在所有 VMware 虛擬應用裝置主機機器上適當設定 `tcp_wrappers` 套件，來限制安全殼層 (SSH) 存取權。同時也請維護這些應用裝置上的必要 SSH 金鑰檔案權限。

所有的 VMware 虛擬應用裝置都含有 `tcp_wrappers` 套件，以允許支援 `tcp` 的常駐程式控制能存取 `libwrap` 常駐程式的網路子網路。依預設，`/etc/hosts.allow` 檔案包含一個一般項目 (`sshd: ALL : ALLOW`)，可允許所有人存取安全殼層。請視情況為您的組織限制此存取權。

程序

- 1 在虛擬應用裝置主機機器上，使用文字編輯器開啟 `/etc/hosts.allow` 檔案。
- 2 將生產環境中的一般項目變更為只包含本機主機項目和管理網路子網路，以維護作業的安全。

```
sshd:127.0.0.1 : ALLOW
sshd: [::1] : ALLOW
sshd: 10.0.0.0 :ALLOW
```

在此範例中，可以使用所有本機主機連線，以及用戶端在 10.0.0.0 子網路上建立的連線。

- 3 新增所有適當的機器識別資訊，例如主機名稱、IP 位址、完整網域名稱 (FQDN) 及回送。
- 4 儲存並關閉檔案。

維護安全殼層金鑰檔案權限

若要維護適當的安全性等級，請設定安全殼層 (SSH) 金鑰檔案權限。

程序

- 1 檢視位於 `/etc/ssh/*key.pub` 的公用主機金鑰檔案。
- 2 確認這些檔案是由根使用者擁有、群組是由根使用者擁有，以及檔案的權限設定為 `0644`。
權限為 (`-rw-r--r--`)。
- 3 關閉所有檔案。
- 4 檢視位於 `/etc/ssh/*key` 的私人主機金鑰檔案。
- 5 確認根使用者擁有這些檔案和群組，以及檔案的權限設定為 `0600`。
權限為 (`-rw-----`)。
- 6 關閉所有檔案。

強化安全殼層伺服器組態

在可行的情況下，虛擬應用程式安裝 (OVF) 都有預設的強化組態。使用者可以檢驗組態檔案中全域選項區段中的伺服器及用戶端服務，來確認其組態已適當強化。

可能的話，請將 SSH 伺服器的使用限制在 `/etc/hosts.allow` 檔案中的管理子網路。

程序

- 1 開啟 `/etc/ssh/sshd_config` 伺服器組態檔案，確認設定都正確無誤。

設定	狀態
伺服器常駐程式通訊協定	Protocol 2
加密方式	Ciphers aes256-ctr,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	使用 AllowGroups 欄位，針對可使用服務的使用者，指定獲允許可存取次要群組及新增成員至其中的群組。
GSSAPI 驗證	GSSAPIAuthentication no (若未使用此設定)
Kerberos 驗證	KerberosAuthentication no (若未使用此設定)
本機變數 (AcceptEnv 全域選項)	設定為停用 (註解掉) 或 啟用 (僅限 LC_* 或 LANG 變數)
通道組態	PermitTunnel no
網路工作階段	MaxSessions 1
嚴格模式檢查	Strict Modes yes
權限區別	UsePrivilegeSeparation yes
rhosts RSA 驗證	RhostsRSAAuthentication no
壓縮	Compression delayed 或 Compression no
訊息驗證碼	MACs hmac-sha1
使用者存取限制	PermitUserEnvironment no

- 2 儲存變更並關閉檔案。

強化安全殼層用戶端組態

在系統強化監控程序的步驟中，請檢驗虛擬應用裝置主機機器上的 SSH 用戶端組態檔案，確保其設定都遵循 VMware 的方針，進而確認 SSH 用戶端的強化。

程序

- 1 開啟 SSH 用戶端組態檔案 (/etc/ssh/ssh_config)，然後確認全域選項區段中的設定正確無誤。

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)	僅提供 LC_* 或 LANG 變數
CBC 加密方式	Ciphers aes256-ctr,aes128-ctr
訊息驗證碼	僅在 MACs hmac-sha1 項目中使用

- 2 儲存變更並關閉檔案。

停用以根使用者身分直接登入

依預設，強化後的應用裝置允許您以根使用者的身分，使用主控台直接登入。最佳安全性做法就是建立管理員帳戶以確立不可否認性、使用 `su-root` 命令測試帳戶的 `wheel` 存取權，然後再停用直接登入。

必要條件

- 完成[為安全殼層建立本機管理員帳戶](#)這個主題中的步驟。
- 在停用直接根登入之前，先確認您已測試使用管理員身分存取系統。

程序

- 1 以根使用者的身分登入，然後瀏覽至 /etc/securetty 檔案。

您可以從命令提示字元存取這個檔案。

- 2 將 `tty1` 項目改為 `console`。

停用 Admin 使用者帳戶的 SSH 存取權

為了安全起見，最佳做法是停用 Admin 使用者帳戶的 SSH 存取權。vRealize Operations Manager 管理員帳戶和 Linux 管理員帳戶共用相同的密碼。停用 Admin 使用者的 SSH 存取權可確保所有 SSH 使用者均先使用與 vRealize Operations Manager 管理員帳戶不同的密碼登入權限較低的服務帳戶，之後再將使用者切換到管理員或根使用者等較高的權限，藉此強制執行深度防禦機制。

程序

- 1 編輯 /etc/ssh/sshd_config 檔案。

您可以從命令提示字元存取這個檔案。

- 2 請將 `DenyUsers admin` 項目新增到檔案中的任何位置，然後儲存檔案。
- 3 若要重新啟動 sshd 伺服器，請執行 `service sshd restart` 命令。

設定開機載入器驗證

若要提供適當的安全性等級，請在 VMware 虛擬應用裝置上設定開機載入器驗證。如果系統開機載入器不需要驗證，對於系統具有主控台存取權的使用者，也許就能夠變更系統開機組態，或將系統開機到單一使用者或維護模式，導致阻斷服務或未經授權的系統存取。

由於開機載入器驗證並非 VMware 虛擬應用裝置上的預設設定，因此您必須建立 GRUB 密碼才能設定。

程序

- 1 在虛擬應用裝置上的 `/boot/grub/menu.lst` 檔案中，找到 `password --md5 <password-hash>` 這一行，確認是否有開機密碼。
- 2 如果沒有密碼，請在虛擬應用裝置上執行 `# /usr/sbin/grub-md5-crypt` 命令。
隨後就會產生一個 MD5 密碼，且該命令會提供 md5 雜湊輸出。
- 3 執行 `# password --md5 <hash from grub-md5-crypt>` 命令，將密碼附加至 `menu.lst` 檔案。

單一使用者或維護模式驗證

如果系統不要求您提供有效的根驗證，就直接開機到單一使用者或維護模式，則任何人只要叫用單一使用者或維護模式，都會獲得系統上所有檔案的特殊存取權。

程序

- ◆ 檢閱 `/etc/inittab` 檔案，確認出現以下兩行：`ls:S:wait:/etc/init.d/rc S` 和 `~~:S:respawn:/sbin/sulogin`。

監控基本必要使用者帳戶

您必須監控現有的使用者帳戶，並確保移除任何不必要的使用者帳戶。

程序

- ◆ 您可以執行 `host:~ # cat /etc/passwd` 命令，確認基本必要使用者帳戶：

```
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
haldaemon:x:101:102:User for haldaemon:/var/run/hald:/bin/false
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:100:101:User for D-Bus:/var/run/dbus:/bin/false
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
ntp:x:74:106:NTP daemon:/var/lib/ntp:/bin/false
polkituser:x:103:104:PolicyKit:/var/run/PolicyKit:/bin/false
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
root:x:0:0:root:/root:/bin/bash
sshd:x:71:65:SSH daemon:/var/lib/ssh:/bin/false
suse-ncc:x:104:107:Novell Customer Center User:/var/lib/YaST2/suse-ncc-fakehome:/bin/bash
```

```

uuid:x:102:103:User for uuid:/var/run/uuid:/bin/false
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
admin:x:1000:1003:./home/admin:/bin/bash
postgres:x:1002:100:./var/vmware/vpostgres/9.3:/bin/bash

```

監控基本必要群組

您必須監控現有的群組和成員，以確保移除任何不必要的群組或群組存取權。

程序

- ◆ 您可以執行 `<host>:~ # cat /etc/group` 命令，來確認基本必要群組和群組成員資格。

```

audio:x:17:
bin:x:1:daemon
cdrom:x:20:
console:x:21:
daemon:x:2:
dialout:x:16:u1,tcserver,postgres
disk:x:6:
floppy:x:19:
haldaemon:!:102:
kmem:x:9:
mail:x:12:
man:x:62:
messagebus:!:101:
modem:x:43:
nobody:x:65533:
nogroup:x:65534:nobody
ntp:!:106:
polkituser:!:105:
public:x:32:
root:x:0:admin
shadow:x:15:
sshd:!:65:
suse-ncc:!:107:
sys:x:3:
tape:!:103:
trusted:x:42:
tty:x:5:
utmp:x:22:
uuid:!:104:
video:x:33:u1,tcserver,postgres
wheel:x:10:root,admin
www:x:8:
xok:x:41:
maildrop:!:1001:
postfix:!:51:
users:x:100:
vami:!:1002:root
nginx:!:108:
admin:!:1003:

```

重設 vRealize Operations Manager 管理員密碼 (Linux)

最佳安全性做法是在 Linux 叢集上，針對 vApp 或 Linux 安裝重設 vRealize Operations Manager 密碼。

程序

- 1 以根使用者的身分登入主要節點的遠端主控台。
- 2 輸入以下命令，然後依照提示執行：`$VMWARE_PYTHON_BIN $VCOPS_BASE/../../vmware-vcopsuite/utilities/sliceConfiguration/bin/vcopsSetAdminPassword.py --reset`。

設定 VMware 應用裝置的 NTP

針對重要的時間來源，在 VMware 應用裝置上停用主機時間同步化，並且使用網路時間通訊協定 (NTP)。您必須設定受信任的遠端 NTP 伺服器，以進行時間同步化。NTP 伺服器必須是授權時間伺服器，或者至少要與授權時間伺服器同步化。

VMware 虛擬應用裝置上的 NTP 常駐程式會提供同步的時間服務。NTP 預設為停用，因此您需要手動設定。如果可以，請在生產環境中使用 NTP，透過精確的稽核與記錄，來追蹤使用者動作及偵測潛在的惡意攻擊和入侵。如需 NTP 安全性通知的相關資訊，請參閱 NTP 網站。

NTP 組態檔案位於每個應用裝置上的 `/etc/ntp.conf` 檔案中。

程序

- 1 導覽至虛擬應用裝置主機機器上的 `/etc/ntp.conf` 組態檔案。
- 2 將檔案擁有權設為 **root:root**。
- 3 將權限設定為 **0640**。
- 4 若要在 NTP 服務上減緩阻斷服務擴大攻擊的風險，請開啟 `/etc/ntp.conf` 檔案，確保 `restrict` 行出現在檔案中。

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

- 5 儲存任何變更並關閉檔案。

如需 NTP 安全性通知的相關資訊，請參閱 <http://support.ntp.org/bin/view/Main/SecurityNotice>。

在 Linux 上停用 TCP 時間戳記回應

TCP 時間戳記回應可用於預估遠端主機的運作時間，並在未來的攻擊中提供協助。此外，部分作業系統可依其 TCP 時間戳記行為來辨識出指紋。

程序

- ◆ 在 Linux 上停用 TCP 時間戳記回應。
 - a 若要將 `net.ipv4.tcp_timestamps` 的值設定為 0，請執行 `sysctl -w net.ipv4.tcp_timestamps=0` 命令。
 - b 在預設的 `sysctl.conf` 檔案中新增 `ipv4.tcp_timestamps=0` 值。

啟用 FIPS 140-2 模式

vRealize Operations Manager 6.3 和更新版本隨附的 OpenSSL 版本經認證符合 FIPS 140-2。不過 FIPS 模式依預設不會啟用。

如果有安全性符合性的需求而必須啟用 FIPS 模式，並使用經認證符合 FIPS 的密碼編譯演算法，則可啟用 FIPS 模式。

程序

- 1 若要更換 `mod_ssl.so` 檔案，請執行以下命令：

```
cd /usr/lib64/apache2-prefork/  
cp mod_ssl.so mod_ssl.so.old  
cp mod_ssl.so.FIPSON.openssl1.0.2 mod_ssl.so
```

- 2 請編輯 `/etc/apache2/ssl-global.conf` 檔案來修改 Apache2 組態。
- 3 搜尋 `<IfModule mod_ssl.c>` 行，並在該行下方加上 `SSLFIPS on` 指令。
- 4 若要重設 Apache 組態，請執行 `service apache2 restart` 命令。

為傳遞中的資料使用 TLS

最佳安全性做法是確保系統部署有安全傳輸通道。

為 vRealize Operations Manager 設定強式通訊協定

一般不再將 SSLv2 及 SSLv3 等通訊協定視為是安全的。此外，TLS 1.0 和 TLS 1.1 也已停用，並依預設僅會啟用 TLS 1.2。

備註 當您將 vRealize Operations Manager 執行個體升級至 7.5 版時，會在所有 vRealize Operations Manager 節點上停用 TLS 1.0 和 TLS 1.1。TLS 1.2 是依預設支援的唯一通訊協定。但是，如果您想要降低安全性的標準並啟用 TLS 1.0 和 1.1 版，請參閱下列知識庫文章：[67108](#)。

驗證在 Apache HTTPD 中正確使用通訊協定

vRealize Operations Manager 預設會停用 SSLv2、SSLv3、TLSv1 和 TLSv1.1。您必須先停用所有負載平衡器上不安全的通訊協定，才能將系統投入生產。

程序

- 1 從命令提示字元執行 `grep SSLProtocol /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf | grep -v '#'` 命令，驗證 SSLv2、SSLv3、TLSv1 和 TLSv1.1 已經停用。
如果通訊協定已經停用，該命令就會傳回以下輸出：SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1。
- 2 如果要重新啟動 Apache2 伺服器，請從命令提示字元執行 `/etc/init.d/apache2 restart` 命令。

驗證在 GemFire TLS 處理常式中正確使用通訊協定

vRealize Operations Manager 預設會停用 SSLv3、TLS 1.0 和 TLS 1.1。您必須先停用所有負載平衡器上不安全的通訊協定，才能將系統投入生產。

程序

- 1 驗證通訊協定已停用。若要驗證通訊協定已停用，請在每個節點執行下列命令：

```
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.properties | grep -v '#'
```

預期會有下列結果：

```
cluster-ssl-protocols=TLSv1.2
```

```
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.native.properties | grep -v '#'
```

預期會有下列結果：

```
cluster-ssl-protocols=TLSv1.2
```

```
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties | grep -v '#'
```

預期會有下列結果：

```
cluster-ssl-protocols=TLSv1.2
```

- 2 重新啟用 TLS 1.0 和 TLS 1.1。
 - a 導覽至管理員使用者介面，讓叢集離線：url/admin。
 - b 按一下**離線**。
 - c 若要確保啟用 TLS 1.0 和 TLS 1.1，請執行下列命令：

```
sed -i "/^[^#]*cluster-ssl-protocol/ c\cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1" /usr/lib/vmware-vcops/user/conf/gemfire.properties
sed -i "/^[^#]*cluster-ssl-protocol/ c\cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1" /usr/lib/vmware-vcops/user/conf/gemfire.native.properties
sed -i "/^[^#]*cluster-ssl-protocol/ c\cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1" /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties
```

為每個節點重複這個步驟。

- d 導覽至管理員使用者介面，讓叢集上線。
- e 按一下上線。

設定 vRealize Operations Manager 使用強式加密方式

為獲得最高的安全性，您必須設定 vRealize Operations Manager 元件使用強式加密方式。為確保僅選用強式加密方式，請停用弱式加密方式。將伺服器設定為僅支援強式加密方式，並且使用夠大的金鑰大小。此外，加密方式必須依適當的順序設定。

vRealize Operations Manager 依預設會停用以 DHE 金鑰交換使用加密套件的功能。請務必先在所有負載平衡器上停用相同的不安全加密套件，再將系統投入生產。

使用強式加密方式

伺服器與瀏覽器之間交涉的加密方式，決定了 TLS 工作階段中所使用的金鑰交換方法和加密強度。

驗證在 Apache HTTPD 中正確使用加密套件

為盡量提升安全性，請驗證在 Apache Httpd 中正確使用加密套件。

程序

- 1 若要驗證在 Apache Httpd 中正確使用加密套件，請從命令提示字元執行 `grep SSLCipherSuite /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf | grep -v '#'` 命令。

如果 Apache httpd 使用正確的加密套件，命令會傳回下列輸出：SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH

- 2 若要設定正確使用加密套件，請從命令提示字元執行 `sed -i "/^[^#]*SSLCipherSuite/ c \SSLCipherSuite HIGH:\!aNULL\!ADH:\!EXP:\!MD5:\!3DES:\!CAMELLIA:\!PSK:\!SRP:\!DH:@STRENGTH" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` 命令。

如果步驟 1 的輸出不如預期，請執行這個命令。

這個命令會停用所有使用 DH 和 DHE 金鑰交換方法的加密套件。

- 3 從命令提示字元執行 `/etc/init.d/apache2 restart` 命令，重新啟動 Apache2 伺服器。
- 4 若要重新啟用 DH，請從命令提示字元執行 `sed -i "/^[^#]*SSLCipherSuite/ c \SSLCipherSuite HIGH:\!aNULL\!ADH:\!EXP:\!MD5:\!3DES:\!CAMELLIA:\!PSK:\!SRP:@STRENGTH" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` 命令，移除加密套件的 !DH。
- 5 從命令提示字元執行 `/etc/init.d/apache2 restart` 命令，重新啟動 Apache2 伺服器。

驗證在 GemFire TLS 處理常式中正確使用加密套件

為盡量提升安全性，請驗證在 GemFire TLS 處理常式中正確使用加密套件。

程序

- 1 若要驗證加密套件已啟用，請在每個節點執行下列命令，驗證通訊協定已經啟用：

```
grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.properties |
grep -v '#'

grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/
gemfire.native.properties | grep -v '#'

grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/
gemfire.locator.properties | grep -v '#'
```

- 2 設定正確的加密套件。

- a 導覽至管理員使用者介面，其位於 *URL/admin*。
- b 若要讓叢集離線，請按一下 **離線**。
- c 若要設定正確的加密套件，請執行下列命令：

```
sed -i "/^[^#]*cluster-ssl-ciphers/ c\cluster-ssl-
ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" /usr/lib/vmware-vcops/user/conf/
gemfire.properties

sed -i "/^[^#]*cluster-ssl-ciphers/ c\cluster-ssl-
ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" /usr/lib/vmware-vcops/user/conf/
gemfire.native.properties

sed -i "/^[^#]*cluster-ssl-ciphers/ c\cluster-ssl-
ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" /usr/lib/vmware-vcops/user/conf/
gemfire.locator.properties
```

為每個節點重複這個步驟。

- d 導覽至管理員使用者介面，其位於 *URL/admin*。
- e 按一下 **上線**。

針對 Localhost 連線啟用 TLS

依預設，連至 PostgreSQL 資料庫的 localhost 連線不會使用 TLS。若要啟用 TLS，您必須使用 OpenSSL 產生自我簽署憑證，或者提供您自己的憑證。

若要針對連至 PostgreSQL 的 localhost 連線啟用 TLS，請完成下列步驟：

- 1 使用 [OpenSSL](#) 產生或提供您自己的自我簽署憑證
- 2 為 [PostgreSQL](#) 安裝憑證
- 3 針對 [PostgreSQL](#) 啟用 TLS

使用 OpenSSL 產生或提供您自己的自我簽署憑證

連至 PostgreSQL 資料庫的 localhost 連線不會使用 TLS。若要啟用 TLS，您可以使用 OpenSSL 產生您自己的自我簽署憑證，或者提供您自己的憑證。

- 若要使用 OpenSSL 產生自我簽署憑證，請執行下列命令：

```
openssl req -new -text -out cert.req openssl rsa -in privkey.pem -out cert.pem openssl req -x509 -in cert.req -text -key cert.pem -out cert.cert
```

- 若要提供您自己的憑證，請完成下列步驟：

- 將 CAcerts.crt 檔案的擁有權修改為 postgres。
- 編輯 postgresql.conf 檔案以包含指令 `ssl_ca_file = 'CAcerts.crt'`。

如果您使用有 CA 鏈結的憑證，則必須將包含中繼和根 CA 憑證的 CAcerts.crt 檔案新增到相同目錄中。

為 PostgreSQL 安裝憑證

針對連至 PostgreSQL 的 localhost 連線啟用 TLS 時，必須為 PostgreSQL 安裝憑證。

程序

- 1 將 cert.pem 檔案複製到 `/storage/db/vcops/vpostgres/data/server.key`。
- 2 將 cert.cert 檔案複製到 `/storage/db/vcops/vpostgres/data/server.crt`。
- 3 執行 `chmod 600 /storage/db/vcops/vpostgres/data/server.key` 命令。
- 4 執行 `chmod 600 /storage/db/vcops/vpostgres/data/server.crt` 命令。
- 5 執行 `chown postgres /storage/db/vcops/vpostgres/data/server.key` 及 `chown postgres /storage/db/vcops/vpostgres/data/server.crt` 命令，以將 server.crt 和 server.key 檔案的擁有權從 root 變更為 postgres。

針對 PostgreSQL 啟用 TLS

您必須編輯 postgresql.conf 檔案，才能在針對連至 PostgreSQL 的 localhost 連線上啟用 TLS。

程序

- ◆ 編輯位於 `/storage/db/vcops/vpostgres/data/` 的 postgresql.conf 檔案，並進行下列變更：
 - a 設定 `ssl = on`。
 - b 設定 `ssl_cert_file = 'server.crt'`。
 - c 設定 `ssl_key_file = 'server.key'`。

必須保護的應用程式資源

最佳安全性做法是確保應用程式資源受到保護。

請執行以下步驟，確保應用程式資源受到保護。

程序

- 1 執行 `Find / -path /proc -prune -o -type f -perm +6000 -ls` 指令，驗證檔案已設定定義完善的 SUID 及 GUID 位集。

您會看到以下清單：

```

354131  24 -rwsr-xr-x  1 polkituser root 23176 /usr/lib/PolicyKit/polkit-set-default-helper
354126  20 -rwxr-sr-x  1 root    polkituser  19208 /usr/lib/PolicyKit/polkit-grant-helper
354125  20 -rwxr-sr-x  1 root    polkituser  19008 /usr/lib/PolicyKit/polkit-explicit-grant-
helper
354130  24 -rwxr-sr-x  1 root    polkituser  23160 /usr/lib/PolicyKit/polkit-revoke-helper
354127  12 -rwsr-x---  1 root    polkituser  10744 /usr/lib/PolicyKit/polkit-grant-helper-pam
354128  16 -rwxr-sr-x  1 root    polkituser  14856 /usr/lib/PolicyKit/polkit-read-auth-helper
73886   84 -rwsr-xr-x  1 root    shadow    77848 /usr/bin/chsh
73888   88 -rwsr-xr-x  1 root    shadow    85952 /usr/bin/gpasswd
73887   20 -rwsr-xr-x  1 root    shadow    19320 /usr/bin/expiry
73890   84 -rwsr-xr-x  1 root    root      81856 /usr/bin/passwd
73799  240 -rwsr-xr-x  1 root    root     238488 /usr/bin/sudo
73889   20 -rwsr-xr-x  1 root    root     19416 /usr/bin/newgrp
73884   92 -rwsr-xr-x  1 root    shadow    86200 /usr/bin/chage
73885   88 -rwsr-xr-x  1 root    shadow    82472 /usr/bin/chfn
73916   40 -rwsr-x---  1 root    trusted   40432 /usr/bin/crontab
296275  28 -rwsr-xr-x  1 root    root     26945 /usr/lib64/pt_chown
353804  816 -r-xr-sr-x  1 root    mail     829672 /usr/sbin/sendmail
278545  36 -rwsr-xr-x  1 root    root     35792 /bin/ping6
278585  40 -rwsr-xr-x  1 root    root     40016 /bin/su
278544  40 -rwsr-xr-x  1 root    root     40048 /bin/ping
278638  72 -rwsr-xr-x  1 root    root     69240 /bin/umount
278637 100 -rwsr-xr-x  1 root    root     94808 /bin/mount
475333  48 -rwsr-x---  1 root    messagebus 47912 /lib64/dbus-1/dbus-daemon-launch-helper
41001   36 -rwsr-xr-x  1 root    shadow    35688 /sbin/unix_chkpwd
41118   12 -rwsr-xr-x  1 root    shadow    10736 /sbin/unix2_chkpwd

```

- 2 執行 `find / -path */proc -prune -o -nouser -o -nogroup` 命令，確認 vApp 中所有的檔案都有擁有者。

如果沒有出現任何結果，表示所有檔案都有擁有者。

- 3 執行 `find / -name "*. *" -type f -perm -a+w | xargs ls -ldb` 命令，檢閱 vApp 上所有檔案的權限，確認這些檔案都不是任何人都能寫入的。

Others 不應具有寫入權限。這些檔案的權限應為 `##4` 或 `##5`，其中 `#` 等於擁有者和群組的預設權限，例如 `6` 或 `7`。

- 4 執行 `find / -path */proc -prune -o ! -user root -o -user admin -print` 命令，確認這些檔案的擁有者都是正確的使用者。

如果沒有出現任何結果，表示所有檔案都屬於 `root` 或 `admin`。

- 5 執行 `find /usr/lib/vmware-casa/ -type f -perm -o=w` 命令，確保 `/usr/lib/vmware-casa/` 目錄中的檔案不是任何人都能寫入的。

執行完畢後不應出現任何結果。

- 6 執行 `find /usr/lib/vmware-vcops/ -type f -perm -o=w` 命令，確保 `/usr/lib/vmware-vcops/` 目錄中的檔案不是任何人都能寫入的。

執行完畢後不應出現任何結果。

- 7 執行 `find /usr/lib/vmware-vcopssuite/ -type f -perm -o=w` 命令，確保 `/usr/lib/vmware-vcopssuite/` 目錄中的檔案不是任何人都能寫入的。

執行完畢後不應出現任何結果。

Apache 組態

停用 Web 目錄瀏覽

安全性最佳做法是確保使用者無法瀏覽目錄，因為這可能會增加受到目錄周遊攻擊的風險。

程序

- ◆ 確認停用所有目錄的 Web 目錄瀏覽。
 - a 在文字編輯器中開啟 `/etc/apache2/default-server.conf` 和 `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` 檔案。
 - b 針對每個列出的 `<Directory>`，確認 `Options` 行中已省略相關標記的 `Indexes` 選項。

移除 Apache2 伺服器的範例程式碼

Apache 包含兩個範例通用閘道介面 (CGI) 指令碼：`printenv` 和 `test-cgi`。生產 Web 伺服器只能包含在運作時必須用到的元件。這些元件有可能會洩露重要的系統資訊給攻擊者。

最佳的安全性做法是從 `cgi-bin` 目錄刪除 CGI 指令碼。

程序

- ◆ 若要移除 `test-cgi` 和 `prinenv` 指令碼，請執行 `rm /usr/share/doc/packages/apache2/test-cgi` 和 `rm /usr/share/doc/packages/apache2/printenv` 命令。

驗證 Apache2 伺服器的伺服器 Token

系統強化程序包括了驗證 Apache2 伺服器的伺服器 Token。HTTP 回應的 Web 伺服器回應標頭可能包含數個欄位的資訊。這些資訊包含要求的 HTML 頁面、Web 伺服器類型與版本、作業系統與版本，以及與 Web 伺服器相關聯的連接埠。這些資訊都會提供重要資訊給惡意使用者，而無需透過延伸工具。

指令 `ServerTokens` 必須設定為 `Prod`。例如，`ServerTokens Prod`。這個指令控制了傳回用戶端的伺服器回應標頭欄位是否包含作業系統的說明，以及編入模組的相關資訊。

程序

- 1 若要驗證伺服器 Token，請執行 `cat /etc/apache2/sysconfig.d/global.conf | grep ServerTokens` 命令。
- 2 若要將 `ServerTokens OS` 修改為 `ServerTokens Prod`，請執行 `sed -i 's/\(ServerTokens\s\+\)\sOS/\1Prod/g' /etc/apache2/sysconfig.d/global.conf` 命令。

停用 Apache2 伺服器的 Trace 方法

在標準生產作業中，可運用診斷找出尚未發現又足以導致資料外洩的漏洞。若要防止資料遭到濫用，請停用 HTTP Trace 方法。

程序

- 1 若要驗證 Apache2 伺服器的 Trace 方法，請執行以下命令：`grep TraceEnable /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf`。
- 2 若要停用 Apache2 伺服器的 Trace 方法，請執行以下命令：`sed -i "/^[^#]*TraceEnable/ c \TraceEnable off" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf`。

停用組態模式

最佳做法是在安裝、設定或維護 vRealize Operations Manager 時，修改組態或設定，以便為安裝執行疑難排解和偵錯。

為您所做的每個變更製作目錄並稽核，以確保變更都受到適當的保護。若您不確定組態變更正確受到保護，請勿放入生產環境。

管理不重要的軟體元件

為盡量降低安全性風險，請從 vRealize Operations Manager 主機機器移除或設定不重要的軟體。

請根據製造商建議和安全性最佳做法，設定所有您未移除的軟體，將造成安全性漏洞的可能性降到最低。

保護 USB 大型存放處理常式的安全

請保護 USB 大型存放處理常式的安全，確保 vRealize 應用裝置預設不載入，並且不作為 vRealize 應用裝置的 USB 裝置處理常式。潛在攻擊者可能會利用這個處理常式安裝惡意軟體。

程序

- 1 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。
- 2 確保檔案中出現 `install usb-storage /bin/true` 這一行。
- 3 儲存並關閉檔案。

保護藍牙通訊協定處理常式的安全

請保護 vRealize 應用裝置上的藍牙通訊協定處理常式，避免遭到潛在攻擊者的利用。

將藍牙通訊協定繫結到網路堆疊不僅沒有必要，還會擴大主機的受攻擊面。請確保 vRealize 應用裝置預設不載入藍牙通訊協定處理常式模組。

程序

- 1 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。
- 2 確保檔案中出現 `install bluetooth /bin/true` 這一行。
- 3 儲存並關閉檔案。

保護串流控制傳輸通訊協定的安全

請確保 vRealize 應用裝置預設不載入串流控制傳輸通訊協定 (Stream Control Transmission Protocol, SCTP)。潛在攻擊者可能會利用這個通訊協定入侵您的系統。

請將系統設定為除非絕對有必要，否則不會載入 SCTP 模組。SCTP 是尚未正式使用的 IETF 標準傳輸層通訊協定。若將此通訊協定繫結到網路堆疊，會擴大主機的受攻擊面。無權限的本機程序可能會使用此通訊協定開啟通訊端，促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 確保檔案中出現下列這行。

```
install sctp /bin/true
```
- 3 儲存並關閉檔案。

保護資料包壅塞控制通訊協定的安全

您可以在進行系統強化活動時，確保 vRealize 應用裝置預設不載入資料包壅塞控制通訊協定 (Datagram Congestion Control Protocol, DCCP)。潛在攻擊者可能會利用這個通訊協定入侵您的系統。

除非絕對有必要，否則切勿載入 DCCP 模組。DCCP 是尚在提議的傳輸層通訊協定，並未正式使用。若將此通訊協定繫結到網路堆疊，會擴大主機的受攻擊面。無權限的本機程序可能會使用此通訊協定開啟通訊端，促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。

保護可靠資料包通訊端通訊協定的安全

您可以在進行系統強化活動時，確保 vRealize 應用裝置預設不載入可靠資料包通訊端 (Reliable Datagram Sockets, RDS) 通訊協定。潛在攻擊者可能會利用這個通訊協定入侵您的系統。

若將 RDS 通訊協定繫結到網路堆疊，會擴大主機的受攻擊面。無權限的本機程序可能會使用此通訊協定開啟通訊端，促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 確保檔案中出現 `install rds /bin/true` 這一行。
- 3 儲存並關閉檔案。

保護透明程序間通訊通訊協定的安全

您可以在進行系統強化活動時，確保您的虛擬應用裝置主機機器預設不載入透明程序間通訊 (Transparent Inter-Process Communication, TIPC) 通訊協定。潛在攻擊者可能會利用這個通訊協定入侵您的系統。

若將 TIPC 通訊協定繫結到網路堆疊，會擴大主機的受攻擊面。無權限的本機程序可能會使用此通訊協定開啟通訊端，促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 確保檔案中出現 `install tipc /bin/true` 這一行。
- 3 儲存並關閉檔案。

保護網際網路封包交換通訊協定的安全

請確保 vRealize 應用裝置預設不載入網際網路封包交換 (IPX) 通訊協定。潛在攻擊者可能會利用這個通訊協定入侵您的系統。

除非絕對有必要，否則切勿載入 IPX 通訊協定模組。IPX 通訊協定是過時的網路層通訊協定。若將此通訊協定繫結到網路堆疊，會擴大主機的受攻擊面。無權限的本機程序可能會使用此通訊協定開啟通訊端，促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 確保檔案中出現 `install ipx /bin/true` 這一行。
- 3 儲存並關閉檔案。

保護 AppleTalk 通訊協定的安全

請確保 vRealize 應用裝置預設不載入 AppleTalk 通訊協定。潛在攻擊者可能會利用這個通訊協定入侵您的系統。

除非有必要，否則切勿載入 AppleTalk 通訊協定模組。若將此通訊協定繫結到網路堆疊，會擴大主機的受攻擊面。無權限的本機程序可能會使用此通訊協定開啟通訊端，促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 確保檔案中出現 `install appletalk /bin/true` 這一行。
- 3 儲存並關閉檔案。

保護 DECnet 通訊協定的安全

請確保您的系統預設不載入 DECnet 通訊協定。潛在攻擊者可能會利用這個通訊協定入侵您的系統。

除非絕對有必要，否則切勿載入 DECnet 通訊協定模組。若將此通訊協定繫結到網路堆疊，會擴大主機的受攻擊面。無權限的本機程序可能會使用此通訊協定開啟通訊端，促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 確保檔案中出現 `install decnet /bin/true` 這一行。
- 3 儲存並關閉檔案。

保護 Firewire 模組的安全

請確保 vRealize 應用裝置預設不載入 Firewire 模組。潛在攻擊者可能會利用這個通訊協定入侵您的系統。

除非絕對有必要，否則切勿載入 Firewire 模組。

程序

- 1 在文字編輯器中開啟 `/etc/modprobe.conf.local` 檔案。
- 2 確保檔案中出現 `install ieee1394 /bin/true` 這一行。
- 3 儲存並關閉檔案。

核心訊息記錄

`/etc/sysctl.conf` 檔案中的 `kernel.printk` 規格指定了核心列印記錄規格。

指定的值有 4 個：

- `console loglevel`. 列印到主控台之訊息的最低優先順序。
- `default loglevel`. 無特定記錄等級之訊息的最低等級。
- 主控台記錄等級的最低等級。
- 主控台記錄等級的預設值。

每個值有八個可能項目。

- `define KERN_EMERG "<0>" /* system is unusable */`
- `define KERN_ALERT "<1>" /* action must be taken immediately */`
- `define KERN_CRIT "<2>" /* critical conditions */`
- `define KERN_ERR "<3>" /* error conditions */`
- `define KERN_WARNING "<4>" /* warning conditions */`
- `define KERN_NOTICE "<5>" /* normal but significant condition */`
- `define KERN_INFO "<6>" /* informational */`
- `define KERN_DEBUG "<7>" /* debug-level messages */`

將 `kernel.printk` 值設定為 **3 4 1 7**，並確保 `/etc/sysctl.conf` 檔案中有 `kernel.printk=3 4 1 7` 這行。

End Point Operations Management 代理程式

End Point Operations Management 代理程式會新增以代理程式為基礎的探索與監控功能至 vRealize Operations Manager。

End Point Operations Management 代理程式會直接安裝在主機上，而且信任等級可能不一定與 End Point Operations Management 伺服器相同。因此，您必須確認代理程式已確實安裝。

執行 End Point Operations Management 代理程式的最佳安全性做法

使用使用者帳戶時，必須遵照一定的最佳安全性做法。

- 執行無訊息安裝時，請移除 `AGENT_HOME/conf/agent.properties` 檔案中儲存的任何認證與伺服器憑證指紋。
- 使用特別為 End Point Operations Management 代理程式註冊作業所保留的 vRealize Operations Manager 使用者帳戶。如需詳細資訊，請參閱 vRealize Operations Manager 說明中的〈vRealize Operations Manager 中的角色和權限〉主題。
- 安裝結束後，請停用您用於代理程式註冊的 vRealize Operations Manager 使用者帳戶。您必須啟用使用者對代理程式管理活動的存取權。如需詳細資訊，請參閱 vRealize Operations Manager 說明中的〈在 vRealize Operations Manager 中設定使用者和群組〉主題。
- 如果執行代理程式的系統遭到入侵，您可以使用 vRealize Operations Manager 使用者介面移除代理程式資源，以撤銷代理程式憑證。如需詳細資訊，請參閱〈撤銷代理程式〉一節。

執行代理程式功能所需的最低必要權限

您必須具備安裝和修改服務的權限。如果您要探索執行程序，則您執行代理程式所用的使用者帳戶，也必須具備這些程序與程式的存取權。如果您要安裝在 Windows 作業系統上，必須具備安裝與修改服務的權限。如果您要安裝在 Linux 上，而且如果您是使用 RPM 安裝程式來安裝代理程式，則必須具備將代理程式安裝為服務的權限。

若要向 vRealize Operations Manager 伺服器註冊代理程式，所需的最低認證是獲授予 Agent Manager 角色的使用者認證，無需在系統內部對物件做任何指派。

Linux 平台檔案與權限

安裝 End Point Operations Management 代理程式後，擁有者就是安裝該代理程式的使用者。

當安裝 End Point Operations Management 代理程式的使用者解壓縮 TAR 檔案或安裝 RPM 時，安裝目錄與檔案權限 (例如 600 和 700) 會設定給擁有者。

備註 當您解壓縮 ZIP 檔案時，權限可能不會正確套用。請驗證並確保權限正確。

所有由代理程式建立及寫入的所有檔案，都會獲得 700 權限，且擁有者就是執行該代理程式的使用者。

表 3-1. Linux 檔案與權限

目錄或檔案	權限	群組或使用者	讀取	寫入	執行
<i>agent directory/bin</i>	700	擁有者	是	是	是
		群組	否	否	否
		全部	否	否	否
<i>agent directory/conf</i>	700	擁有者	是	是	是
		群組	否	否	否
		全部	否	否	否
<i>agent directory/log</i>	700	擁有者	是	是	否
		群組	否	否	否
		全部	否	否	否
<i>agent directory/data</i>	700	擁有者	是	是	是
		群組	否	否	否
		全部	否	否	否
<i>agent directory/bin/ep-agent.bat</i>	600	擁有者	是	是	否
		群組	否	否	否
		全部	否	否	否
<i>agent directory/bin/ep-agent.sh</i>	700	擁有者	是	是	是
		群組	否	否	否
		全部	否	否	否
<i>agent directory/conf/*</i> (<i>conf</i> 目錄中的所有檔案)	600	擁有者	是	是	是
		群組	否	否	否
		全部	否	否	否
<i>agent directory/log/*</i> (<i>log</i> 目錄中的所有檔案)	600	擁有者	是	是	否
		群組	否	否	否
		全部	否	否	否
<i>agent directory/data/*</i>	600	擁有者	是	是	否

表 3-1. Linux 檔案與權限 (續)

目錄或檔案	權限	群組或使用者	讀取	寫入	執行
(data 目錄中的所有檔案)		群組	否	否	否
		全部	否	否	否

Windows 平台檔案與權限

若要將 End Point Operations Management 代理程式安裝在 Windows 上，安裝代理程式的使用者必須具備安裝與修改服務的權限。

安裝 End Point Operations Management 代理程式後，安裝資料夾 (包括所有子目錄和檔案) 應僅能由系統、管理員群組和安裝使用者存取。使用 `ep-agent.bat` 安裝 End Point Operations Management 代理程式時，請確保強化程序順利完成。如果您是安裝代理程式的使用者，建議您記下任何錯誤訊息。如果強化程序失敗，使用者可以手動套用這些權限。

表 3-2. Windows 檔案與權限

目錄或檔案	群組或使用者	完整控制	修改	讀取和執行	讀取	寫入
<agent directory>/bin	系統	是	-	-	-	-
	管理員	是	-	-	-	-
	安裝使用者	是	-	-	-	-
	使用者		-	-	-	-
<agent directory>/conf	系統	是	-	-	-	-
	管理員	是	-	-	-	-
	安裝使用者	是	-	-	-	-
	使用者		-	-	-	-
<agent directory>/log	系統	是	-	-	-	-
	管理員	是	-	-	-	-
	安裝使用者	是	-	-	-	-
	使用者		-	-	-	-
<agent directory>/data	系統	是	-	-	-	-
	管理員	是	-	-	-	-
	安裝使用者	是	-	-	-	-
	使用者		-	-	-	-
<agent directory>/bin/hq-agent.bat	系統	是	-	-	-	-
	管理員	是	-	-	-	-
	安裝使用者	是	-	-	-	-
	使用者		-	-	-	-
<agent directory>/bin/hq-	系統	是	-	-	-	-

表 3-2. Windows 檔案與權限 (續)

目錄或檔案	群組或使用者	完整控制	修改	讀取和執行	讀取	寫入
agent.sh	管理員	是	-	-	-	-
	安裝使用者	是	-	-	-	-
	使用者	-	-	-	-	-
<agent directory>/conf/* (conf 目錄中的所有檔案)	系統	是	-	-	-	-
	管理員	是	-	-	-	-
	安裝使用者	是	-	-	-	-
	使用者	-	-	-	-	-
<agent directory>/log/* (log 目錄中的所有檔案)	系統	是	-	-	-	-
	管理員	是	-	-	-	-
	安裝使用者	是	-	-	-	-
	使用者	-	-	-	-	-
<agent directory>/data/* (data 目錄中的所有檔案)	系統	是	-	-	-	-
	管理員	是	-	-	-	-
	安裝使用者	是	-	-	-	-
	使用者	-	-	-	-	-

開啟代理程式主機上的連接埠

代理程式程序會在 127.0.0.1:2144 和 127.0.0.1:32000 這兩個可以設定的連接埠上接聽命令。這兩個連接埠可能是任意指派，因此確實的連接埠號碼可能會不同。代理程式不會開啟外部介面上的連接埠。

表 3-3. 最低要求的連接埠

連接埠	通訊協定	方向	註解
443	TCP	傳出	代理程式用於透過 HTTP、TCP 或 ICMP 進行傳出連線。
2144	TCP	接聽	僅限向內。可以設定。用於代理程式與載入和設定該代理程式之命令列間的程序間通訊。代理程式程序會在這個連接埠上接聽。 備註 連接埠號碼是任意指派，因此可能會不同。
32000	TCP	接聽	僅限向內。可以設定。用於代理程式與載入和設定該代理程式之命令列間的程序間通訊。代理程式程序會在這個連接埠上接聽。 備註 連接埠號碼是任意指派，因此可能會不同。

撤銷代理程式

如果您因故必須撤銷代理程式，例如有執行中代理程式的系統遭到入侵，可以刪除系統上的代理程式資源。任何後續要求都會驗證失敗。

您可以運用 vRealize Operations Manager 使用者介面，以移除代理程式資源的方式撤銷代理程式憑證。如需詳細資訊，請參閱 [移除代理程式資源](#)。

待系統再次安全後，就可以恢復代理程式。如需詳細資訊，請參閱 [恢復代理程式資源](#)。

移除代理程式資源

您可以使用 vRealize Operations Manager 移除代理程式資源，以撤銷代理程式憑證。

必要條件

若要保留資源與先前記錄之度量資料的連續性，請記錄資源詳細資料中顯示的 End Point Operations Management 代理程式 Token。

程序

- 1 瀏覽到 vRealize Operations Manager 使用者介面中的**詳細目錄**頁面。
- 2 開啟 [介面卡類型] 樹狀結構。
- 3 開啟 [EP Ops 介面卡] 清單。
- 4 選取 **EP Ops 代理程式 - *主機 DNS 名稱***。
- 5 按一下**編輯物件**。
- 6 記錄代理程式識別碼，也就是代理程式 Token 字串。
- 7 關閉 [編輯物件] 對話方塊。
- 8 選取 **EP Ops 代理程式 - *主機 DNS 名稱***，然後按一下**刪除物件**。

恢復代理程式資源

系統的安全狀態復原後，您就可以恢復撤銷的代理程式。這可確保代理程式繼續針對相同的資源提出報告，而不會遺失歷史資料。若要這麼做，您必須使用移除代理程式資源前所記錄的相同 Token，來建立新的 End Point Operations Management Token 檔案。請參閱〈移除代理程式資源〉一節。

必要條件

- 確定您有記錄 End Point Operations Management Token 字串。
- 使用從 vRealize Operations Manager 伺服器移除代理程式資源前所記錄的資源 Token。
- 確定您具有「管理代理程式」權限。

程序

- 1 以執行代理程式的使用者身分，建立代理程式 Token 檔案。

例如，執行命令來建立包含 123-456-789 Token 的 Token 檔案。

- Linux:


```
echo 123-456-789 > /etc/epops/epops-token
```
- Windows:


```
echo 123-456-789 > %PROGRAMDATA%\VMware\Ep Ops Agent\epops-token
```

在此範例中，Token 檔案會寫入該平台的預設 Token 位置

- 2 安裝新的代理程式，並向 vRealize Operations Manager 伺服器註冊。請確定代理程式載入您在 Token 檔案中插入的 Token。

您必須具備「管理代理程式」權限，才能執行這個動作。

代理程式憑證撤銷與憑證更新

重新核發流程是使用 `setup` 命令列引數從代理程式啟動。如果已註冊的代理程式使用 `setup` 命令列引數 `ep-agent.sh setup` 並填入要求的認證時，新的 `registerAgent` 命令就會傳送到伺服器。

伺服器會偵測到代理程式已經註冊，並傳送新的用戶端憑證給代理程式，而不會另外建立代理程式資源。在代理程式端，新的用戶端憑證會取代舊的。若伺服器憑證遭到修改，那麼當您執行 `ep-agent.sh setup` 指令時，會看到一則訊息要求您信任新憑證。您也可以在此 `agent.properties` 檔案中提供新的伺服器憑證指紋，再執行 `ep-agent.sh setup` 指令，讓過程中不會出現訊息。

必要條件

「管理代理程式」權限，以撤銷和更新憑證。

程序

- ◆ 在 Linux 作業系統上，於代理程式主機上執行 `ep-agent.sh setup` 命令。在 Windows 作業系統，請執行 `ep-agent.bat setup` 命令。

如果代理程式偵測到伺服器憑證已經修改，就會顯示一則訊息。如果您信任新憑證，而且該憑證有效，那麼請接受。

End Point Operations Management 代理程式的修補與更新

如有需要，新的 End Point Operations Management 代理程式服務包可另外提供 (獨立於 vRealize Operations Manager 版本之外)。

End Point Operations Management 代理程式不提供修補程式或更新。您必須安裝可用的最新版代理程式，其中便會包含最新的安全性修正。重要的安全性修正將會依 VMware 安全性諮詢指導方針的規定告知您。請參閱安全性諮詢中的主題。

其他安全組態活動

驗證伺服器使用者帳戶，並從主機伺服器刪除非必要的應用程式。封鎖非必要的連接埠，並停用主機伺服器上執行的非必要服務。

確認伺服器使用者帳戶設定

建議您確認本機和網域使用者帳戶與設定沒有不必要的使用者帳戶。

您可以將與應用程式運作無關的任何使用者帳戶，限制為管理、維護和疑難排解所用的帳戶。網域使用者帳戶的遠端存取權，可以限制成維護伺服器所需的最低必要權限。請嚴格控制與稽核這些帳戶。

刪除並停用不必要的應用程式

從主機伺服器刪除不必要的應用程式。每個額外及不必要的應用程式都會有未知或未修補的弱點，因而增加曝險。

停用不必要的連接埠與服務

針對允許流量通過之開放連接埠的清單，確認主機伺服器的防火牆。

若連接埠未在本文件[設定連接埠和通訊協定](#)一節中列為 vRealize Operations Manager 的最低要求，或不是必要的，全部都封鎖。此外，請稽核在主機伺服器上執行的服務，並停用不是必要的服務。

網路安全性與安全通訊

4

最佳安全性做法是檢閱和編輯 VMware 虛擬應用裝置和主機機器的網路通訊設定。您也必須為 vRealize Operations Manager 設定最低要求的傳入和傳出連接埠。

本章節討論下列主題：

- 為虛擬應用程式安裝進行網路設定
- 設定連接埠和通訊協定

為虛擬應用程式安裝進行網路設定

若要確保您的 VMware 虛擬應用裝置及主機機器僅允許安全且必要的通訊，請檢閱並編輯其網路通訊設定。

防止使用者控制網路介面

最佳安全性做法是只允許有特殊權限的使用者變更網路介面設定。如果使用者能操控網路介面，可能會導致略過網路安全性機制或阻斷服務。因此請確保網路介面未設定為由使用者控制。

程序

- 1 若要確認使用者控制設定，請執行 `#grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*` 命令。
- 2 務必將每個介面設定為 NO。

設定 TCP 待處理項目的佇列大小

最佳安全性做法是在 VMware 應用裝置主機機器上，設定預設的 TCP 待處理項目佇列大小。若要減緩 TCP 阻斷服務攻擊，請為 TCP 待處理項目佇列大小設定適當的預設大小。建議的預設設定是 1280。

程序

- 1 在每一部 VMware 應用裝置主機機器上，執行 `# cat /proc/sys/net/ipv4/tcp_max_syn_backlog` 命令。

2 設定 TCP 待處理項目的佇列大小

- a 在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。
- b 在檔案中新增以下項目，設定預設的 TCP 待處理項目佇列大小。

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

- c 儲存變更並關閉檔案。

拒絕 ICMPv4 廣播位址回應

若對廣播網際網路控制訊息通訊協定 (Internet Control Message Protocol, ICMP) 回應傳送回應，就會為擴大攻擊提供攻擊媒介，並可能有助於惡意代理程式執行網路對應。將系統設定為忽略 ICMPv4 回應後，便能防衛此類攻擊。

程序

- 1 執行 `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` 命令，確認系統不會針對 ICMP 廣播位址回應要求傳送回應。
- 2 設定主機系統，使其拒絕 ICMPv4 廣播位址回應要求。
 - a 在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。
 - b 若此項目的值未設定為 1，請新增項目 `net.ipv4.icmp_echo_ignore_broadcasts=1`。
 - c 儲存變更並關閉檔案。

設定主機系統以停用 IPv4 Proxy ARP

IPv4 Proxy ARP 會允許系統代表已連線至某個介面的主機，針對另一個介面的 ARP 要求傳送回應。您必須停用 IPv4 Proxy ARP，以避免未經授權的資訊共用。停用此設定可避免在連接網路區段間洩漏位址資訊。

程序

- 1 執行 `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | egrep "default|all"` 命令，驗證 Proxy ARP 是否已停用。
- 2 設定主機系統以停用 IPv4 Proxy ARP。
 - a 在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。
 - b 若值未設定為 0，請新增該項目或相對應地更新現有項目。將值設定為 0。

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

- c 儲存任何變更並關閉檔案。

設定主機系統以忽略 IPv4 ICMP 重新導向訊息

最佳安全性做法就是確認主機系統會忽略 IPv4 網際網路控制訊息通訊協定 (ICMP) 重新導向訊息。惡意的 ICMP 重新導向訊息可能會允許攔截式攻擊。路由器會使用 ICMP 重新導向訊息，通知主機目的地有更直接的路由。這些訊息會修改主機的路由表，而且未通過驗證。

程序

- 1 在主機系統上執行 `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` 命令，檢查主機系統是否忽略 IPv4 重新導向訊息。
- 2 設定主機系統以忽略 IPv4 ICMP 重新導向訊息。
 - a 開啟 `/etc/sysctl.conf` 檔案。
 - b 若值未設定為 0，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 0。

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

- c 儲存變更並關閉檔案。

設定主機系統以忽略 IPv6 ICMP 重新導向訊息

最佳安全性做法就是確認主機系統會忽略 IPv6 網際網路控制訊息通訊協定 (ICMP) 重新導向訊息。惡意的 ICMP 重新導向訊息可能會允許攔截式攻擊。路由器會使用 ICMP 重新導向訊息，告知主機目的地有更直接的路由。這些訊息會修改主機的路由表，而且未通過驗證。

程序

- 1 在主機系統上執行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` 命令，檢查是否忽略 IPv6 重新導向訊息。
- 2 設定主機系統以忽略 IPv6 ICMP 重新導向訊息。
 - a 開啟 `/etc/sysctl.conf` 設定主機系統，使其忽略 IPv6 重新導向訊息。
 - b 若值未設定為 0，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 0。

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

- c 儲存變更並關閉檔案。

設定主機系統以拒絕 IPv4 ICMP 重新導向

最佳安全性做法就是確認主機系統會拒絕 IPv4 網際網路控制訊息通訊協定 (ICMP) 重新導向。路由器會使用 ICMP 重新導向訊息，告知伺服器特定目的地有直接路由。這些訊息包含了來自於系統路由表的資訊，可能會透露部分網路拓撲。

程序

- 1 在主機系統上執行 `# grep [01] /proc/sys/net/ipv4/conf/*/send_redirects|egrep "default|all"`，確認系統是否拒絕 IPv4 ICMP 重新導向。
- 2 設定主機系統以拒絕 IPv4 ICMP 重新導向。
 - a 開啟 `/etc/sysctl.conf` 檔案以設定主機系統。
 - b 若值未設定為 0，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 0。

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

- c 儲存變更並關閉檔案。

設定主機系統以記錄 IPv4 Martian 封包

最佳安全性做法就是確認主機系統記錄 IPv4 Martian 封包。Martian 封包內含系統已知無效的位址。請設定讓主機系統記錄訊息，好讓您找出組態錯誤或進行中的攻擊。

程序

- 1 執行 `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians|egrep "default|all"` 命令，檢查主機是否有記錄 IPv4 Martian 封包。
- 2 設定讓主機系統記錄 IPv4 Martian 封包。
 - a 開啟 `/etc/sysctl.conf` 檔案以設定主機系統。
 - b 若值未設定為 1，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 1。

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

- c 儲存變更並關閉檔案。

設定主機系統以使用 IPv4 反向路徑篩選

最佳安全性做法就是設定主機機器，使其使用 IPv4 反向路徑篩選。反向路徑篩選可讓系統捨棄來源位址沒有路由的封包，或是路由未指向原始介面的封包，以保護系統不受詐騙來源位址的侵害。

設定系統以儘可能使用反向路徑篩選。視系統角色而定，反向路徑篩選可能會造成合法流量遭到捨棄。在此類情況下，您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 在主機系統上執行 `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"` 命令，檢查系統是否使用 IPv4 反向路徑篩選。

2 設定主機系統以使用 IPv4 反向路徑篩選。

- a 開啟 `/etc/sysctl.conf` 檔案以設定主機系統。
- b 若值未設定為 1，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 1。

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

- c 儲存變更並關閉檔案。

設定主機系統以拒絕 IPv4 轉送

最佳安全性做法就是確認主機系統會拒絕 IPv4 轉送。若系統設定成可進行 IP 轉送，而且不是指定的路由器，就可能會遭到利用，提供網路裝置不會篩選的通訊路徑來繞過網路安全性措施。

程序

- 1 執行 `# cat /proc/sys/net/ipv4/ip_forward` 命令，確認主機是否拒絕 IPv4 轉送。
- 2 設定主機系統以拒絕 IPv4 轉送。
 - a 開啟 `/etc/sysctl.conf` 以設定主機系統。
 - b 若值未設定為 0，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 0。

```
net.ipv4.ip_forward=0
```

- c 儲存變更並關閉檔案。

設定主機系統拒絕 IPv4 來源路由封包的轉送

來源路由封包可允許封包來源指示路由器以異於路由器設定的路徑來轉送封包，而這可用來繞過網路安全性措施。

此項要求僅適用於來源路由流量的轉送，例如當已啟用 IPv4 轉送且系統作為路由器運作時。

程序

- 1 執行 `# grep [01] /proc/sys/net/ipv4/conf/*/accept_source_route | egrep "default|all"` 命令，以確認系統是否不使用 IPv4 來源路由封包
- 2 設定主機系統以拒絕 IPv4 來源路由封包的轉送。
 - a 在文字編輯器中開啟 `/etc/sysctl.conf` 檔案。
 - b 若值未設定成 0，請確保 `net.ipv4.conf.all.accept_source_route=0` 及 `net.ipv4.conf.default.accept_source_route=0` 都設定成 0。
 - c 儲存並關閉該檔案。

設定主機系統以拒絕 IPv6 轉送

最佳安全性做法就是確認主機系統會拒絕 IPv6 轉送。若系統設定成可進行 IP 轉送，而且不是指定的路由器，就可能會遭到利用，提供網路裝置不會篩選的通訊路徑來繞過網路安全性措施。

程序

- 1 執行 `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding | egrep "default|all"` 命令，確認主機是否拒絕 IPv6 轉送。

- 2 設定主機系統以拒絕 IPv6 轉送。

- a 開啟 `/etc/sysctl.conf` 以設定主機系統。
- b 若值未設定為 0，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 0。

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

- c 儲存變更並關閉檔案。

設定主機系統使用 IPv4 TCP SYN Cookie

安全性最佳做法是確認主機系統使用 IPv4 傳輸控制通訊協定 (TCP) SYN Cookie。TCP SYN 洪水攻擊可能會在系統的 TCP 連線表填入 SYN_RCVD 狀態的連線，導致阻斷服務。而使用 SYN Cookie 的目的是，在收到後續的 ACK、確認起始者嘗試發有效連線，而不是洪水來源前，不追蹤連線。

這項技術並不是完全符合標準的運作，只有在偵測到洪水狀況時才啟用，而且允許系統在防禦的同時繼續為有效要求服務。

程序

- 1 執行 `# cat /proc/sys/net/ipv4/tcp_syncookies` 指令，確認主機系統是否使用 IPv4 TCP SYN Cookie。

- 2 設定主機系統使用 IPv4 TCP SYN Cookie。

- a 開啟 `/etc/sysctl.conf` 以設定主機系統。
- b 若值未設定為 1，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 1。

```
net.ipv4.tcp_syncookies=1
```

- c 儲存變更並關閉檔案。

設定主機系統以拒絕 IPv6 路由器公告

最佳安全性做法就是確認主機系統除非有必要，否則會拒絕接受路由器公告及網際網路控制訊息通訊協定 (ICMP) 重新導向。IPv6 的特色之一是系統能如何地自動使用網路資訊來設定其網路裝置。從安全性的觀點來看，建議手動設定重要的組態資訊，而非未經驗證便接受來自於網路的資訊。

程序

- 1 在主機系統上執行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"` 命令，確認系統是否除非有必要，否則會拒絕接受路由器公告及 ICMP 重新導向。
- 2 設定主機系統以拒絕 IPv6 路由器公告。
 - a 開啟 `/etc/sysctl.conf` 檔案。
 - b 若值未設定為 0，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 0。

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

- c 儲存變更並關閉檔案。

設定主機系統以拒絕 IPv6 路由器邀請

最佳安全性做法就是確認主機系統除非有必要，否則會拒絕 IPv6 路由器邀請。路由器邀請設定決定了在啟動介面時會傳送多少路由器邀請。若位址為靜態指派，就不需要傳送任何邀請。

程序

- 1 執行 `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations | egrep "default|all"` 命令，確認主機系統是否除非有必要，否則會拒絕 IPv6 路由器邀請。
- 2 設定主機系統以拒絕 IPv6 路由器邀請。
 - a 開啟 `/etc/sysctl.conf`。
 - b 若值未設定為 0，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 0。

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

- c 儲存變更並關閉檔案。

設定主機系統以拒絕路由器邀請中的 IPv6 路由器喜好設定

最佳安全性做法就是確認主機系統除非有必要，否則會拒絕 IPv6 路由器邀請。邀請設定中的路由器喜好設定決定了路由器喜好設定。若位址為靜態指派，就不需要接收邀請的任何路由器喜好設定。

程序

- 1 在主機系統上執行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"` 命令，確認主機系統是否拒絕 IPv6 路由器邀請。

2 設定主機系統以拒絕路由器邀請中的 IPv6 路由器喜好設定。

- a 開啟 `/etc/sysctl.conf` 檔案。
- b 若值未設定為 0，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 0。

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

- c 儲存變更並關閉檔案。

設定主機系統以拒絕 IPv6 路由器前置詞

最佳安全性做法就是確認主機系統除非有必要，否則會拒絕 IPv6 路由器前置詞資訊。`accept_ra_pinfo` 設定控制了系統是否接受來自於路由器的前置詞資訊。若位址為靜態指派，系統就不接收任何路由器前置詞資訊。

程序

- 1 執行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | egrep "default|all"`，確認系統是否拒絕 IPv6 路由器前置詞資訊。
- 2 設定主機系統以拒絕 IPv6 路由器前置詞。
 - a 開啟 `/etc/sysctl.conf` 檔案。
 - b 若值未設定為 0，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 0。

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

- c 儲存變更並關閉檔案。

設定主機系統以拒絕 IPv6 路由器公告躍點限制設定

最佳安全性做法是除非有必要，否則確定主機系統會拒絕路由器公告中的 IPv6 路由器公告躍點限制設定。`accept_ra_defrtr` 設定可控制系統是否接受路由器公告中的躍點限制設定。若設定為 0，可防止路由器變更傳出封包的預設 IPv6 躍點限制。

程序

- 1 執行 `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` 命令，確認主機系統拒絕 IPv6 路由器躍點限制設定。
- 2 如果這些值不是設定為 0，請將主機系統設定為拒絕 IPv6 路由器公告躍點限制設定。
 - a 開啟 `/etc/sysctl.conf` 檔案。
 - b 若值未設定為 0，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 0。

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

- c 儲存變更並關閉檔案。

設定主機系統以拒絕 IPv6 路由器公告 Autoconf 設定

最佳安全性做法就是確認主機系統會拒絕 IPv6 路由器公告 autoconf 設定。autoconf 設定控制了路由器公告是否能使系統指派全域單點傳播位址至介面。

程序

- 1 執行 `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf|egrep "default|all"` 命令，確認主機系統是否拒絕 IPv6 路由器公告 autoconf 設定。
- 2 若值未設定為 0，請設定主機系統，使其拒絕 IPv6 路由器公告 autoconf 設定。
 - a 開啟 `/etc/sysctl.conf` 檔案。
 - b 若值未設定為 0，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 0。

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

- c 儲存變更並關閉檔案。

設定主機系統以拒絕 IPv6 芳鄰邀請

最佳安全性做法就是確認主機系統除非有必要，否則會拒絕 IPv6 芳鄰邀請。dad_transmits 設定決定了在您啟動介面以確定所需位址在網路中都是唯一時，每一位址傳送多少芳鄰邀請 (包括全域及 Link-local)。

程序

- 1 執行 `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits|egrep "default|all"` 命令，確認主機系統是否拒絕 IPv6 芳鄰邀請。
- 2 若值未設定為 0，請設定主機系統，使其拒絕 IPv6 芳鄰邀請。
 - a 開啟 `/etc/sysctl.conf` 檔案。
 - b 若值未設定為 0，請新增下列項目至檔案，或相對應地更新現有項目。將值設定為 0。

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

- c 儲存變更並關閉檔案。

設定主機系統來限制 IPv6 位址數上限

最佳安全性做法是確認主機有限制可指派的 IPv6 位址數上限。位址數上限設定可決定能指派多少全域單點傳播 IPv6 位址給每個介面。預設值是 16，但是您必須將此數字設定為需要的靜態設定全域位址。

程序

- 1 執行 `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses|egrep "default|all"` 命令，確認主機系統是否限制可指派的 IPv6 位址數上限。

2 如果這些值不是設定為 1，請設定主機系統，使其限制可指派的 IPv6 位址數上限。

- a 開啟 `/etc/sysctl.conf` 檔案。
- b 在檔案中加入下列項目或更新現有項目。將值設定為 1。

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

- c 儲存變更並關閉檔案。

設定連接埠和通訊協定

最佳安全性做法就是停用所有非必要的連接埠和通訊協定。

請依最低要求為 vRealize Operations Manager 元件設定傳入及傳出連接埠，以便重要系統元件能在生產環境中運作。

最低要求的預設傳入連接埠

最佳安全性做法是設定必要的傳入連接埠，以便 vRealize Operations Manager 能在生產環境中運作。

表 4-1. 最低要求的傳入連接埠

連接埠	通訊協定	註解
443	TCP	用於存取 vRealize Operations Manager 使用者介面及 vRealize Operations Manager 管理員介面。
123	UDP	由 vRealize Operations Manager 用於網路時間通訊協定 (NTP) 同步至主要節點。
5433	TCP	在啟用高可用性時，主要和複本節點用來複寫全域資料庫 (vPostgreSQL)。
7001	TCP	Cassandra 用以確保節點間叢集通訊安全。 請勿將此連接埠暴露到網際網路。請將此連接埠新增至防火牆。
9042	TCP	Cassandra 用來進行確保與用戶端相關的節點間通訊安全。 請勿將此連接埠暴露到網際網路。請將此連接埠新增至防火牆。
6061	TCP	供用戶端連線至 GemFire Locator 以取得分散式系統中伺服器的連線資訊。同時監控伺服器負載，以便將用戶端傳送到負載最小的伺服器。
10000-10010	TCP 與 UDP	用於在對等分散式系統中進行單點傳播 UDP 傳訊與 TCP 失敗偵測的 GemFire 伺服器暫時連接埠範圍。
20000-20010	TCP 與 UDP	用於在對等分散式系統中進行單點傳播 UDP 傳訊與 TCP 失敗偵測的 GemFire 定位器暫時連接埠範圍。

表 4-2. 選用傳入連接埠

連接埠	通訊協定	註解
22	TCP	選用。安全殼層 (SSH)。在生產環境中，必須停用在連接埠 22 或在任何其他連接埠接聽的 SSH 服務，而且必須關閉連接埠 22。
80	TCP	選用。重新導向至 443。
3091-3101	TCP	安裝 Horizon View 時，用來從 Horizon View 存取 vRealize Operations Manager 的資料。

vRealize Operations Manager 系統 上的稽核與記錄

5

最佳安全性做法就是在 vRealize Operations Manager 系統上設定稽核與記錄功能。

稽核與記錄的詳細實作未涵蓋在此文件的範圍內。

從遠端將記錄存放至中央記錄主機的方式，為記錄提供了一個安全的存放區。將記錄檔案收集至中央主機後，只要使用單一工具便能輕鬆監控環境。此外，您還可以在基礎架構中的多個實體上，執行彙總分析及搜尋有組織的攻擊。將記錄存放在安全集中式的記錄伺服器，不但可避免記錄遭到竄改，也可以提供長期的稽核記錄。

本章節討論下列主題：

- [保護遠端記錄伺服器](#)
- [使用獲授權的 NTP 伺服器](#)
- [用戶端瀏覽器考量事項](#)

保護遠端記錄伺服器

最佳安全性做法就是確保只有獲授權的使用者可以設定遠端記錄伺服器，而且遠端記錄伺服器是安全的。

侵害您主機機器安全性的攻擊者，可能會搜尋並嘗試竄改記錄檔案，以掩飾其行蹤並在不被發現的情況下保有控制權。

使用獲授權的 NTP 伺服器

請確定所有主機系統都使用相同的相對時間來源，包括相關的當地語系化偏移。您可以將相對時間來源關聯到一個商定的時間標準，例如國際標準時間 (UTC)。

您可以在檢閱相關記錄檔案時，輕鬆追蹤並關聯入侵者的動作。如果時間設定不正確，很可能會讓您難以檢查和關聯記錄檔案來偵測攻擊，也會使稽核不準確。您可以使用至少三個來自外部時間來源的 NTP 伺服器，或者在受信任的網路上，設定幾個本機 NTP 伺服器，並使其從至少三個外部時間來源取得時間。

用戶端瀏覽器考量事項

最佳安全性做法是不要使用來自不受信任或未修補的用戶端，或使用瀏覽器擴充功能之用戶端提供的 vRealize Operations Manager。