vSphere 安全性

修改日期：2018 年 5 月 11 日
VMware vSphere 6.7
VMware ESXi 6.7
vCenter Server 6.7

vmware®

您可以在 VMware 網站上找到最新的技術說明文件，網址為:

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

如果您對此文件有何想法，請將您的回應意見提交至：

docfeedback@vmware.com

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

Copyright © 2009–2018 VMware, Inc. 版權所有。 版權和商標資訊。

內容

關於 vSphere 安全性

*vSphere 安全性*提供了有關確保 VMware® vCenter® Server 和 VMware ESXi 的 vSphere® 環境安全的資訊。

為了協助您保護 vSphere 環境，本說明文件說明可用的安全性功能，以及為使該環境免受攻擊可採取的措施。

表格 1. *vSphere 安全性* 要點

主題	內容要點
權限和使用者管理	■ 權限模型 (角色、群組、物件)。 ■ 建立自訂角色。 ■ 設定權限。 ■ 管理全域權限。
主機安全性功能	■ 鎖定模式以及其他安全性設定檔功能。 ■ 主機智慧卡驗證。 ■ vSphere Authentication Proxy。 ■ UEFI 安全開機。 ■ 信賴平台模組 (TPM)。
虛擬機器加密	■ 虛擬機器加密如何運作? ■ KMS 設定。 ■ 加密和解密虛擬機器。 ■ 疑難排解和最佳做法。
客體作業系統安全性	■ 虛擬信賴平台模組 (vTPM)。 ■ 虛擬式安全性 (VBS)。
管理 TLS 通訊協定組態	使用命令列公用程式變更 TLS 通訊協定組態。
安全性最佳做法和強化	VMware 安全性專家提出的最佳做法和建議。 ■ vCenter Server 安全性 ■ 主機安全性 ■ 虛擬機器安全性 ■ 網路安全性
vSphere 權限	此版本中支援的所有 vSphere 權限的完整清單。

相關說明文件

相關文件 *Platform Services Controller 管理*介紹如何使用 Platform Services Controller 服務，如用來管理使用 vCenter Single Sign-On 進行驗證，以及用來管理 vSphere 環境中的憑證。

除了這些文件，VMware 還發佈了適用於每個 vSphere 版本的*《強化指南》*，存取網址為：http://www.vmware.com/security/hardening-guides.html。*《強化指南》*是一份試算表，其中含有不同潛在安全性問題的項目。該指南包括三種不同風險設定檔的項目。本 *vSphere 安全性*文件不包括風險設定檔 1 (最高安全性環境，如最高機密的政府) 的資訊。

預定對象

該資訊適用於熟悉虛擬機器技術及資料中心作業的資深 Windows 或 Linux 系統管理員。

vSphere Web Client 和 vSphere Client (以 HTML5 為基礎的用戶端)

本指南中的工作指示以 vSphere Web Client 為基礎。您也可以使用 vSphere Client 執行本指南中的大部分工作。vSphere Client 使用者介面術語、拓撲和工作流程密切配合 vSphere Web Client 使用者介面的相同層面與元素。除非另有指示，否則您可以將 vSphere Web Client 指示套用到 vSphere Client。

備註 在 vSphere 6.7 中，會在 vSphere Client 中實作大部分 vSphere Web Client 功能。如需不支援功能的最新清單，請參閱《vSphere Client 的功能更新》。

更新的資訊

本《*vSphere 安全性*》文件會隨產品的每個版本更新或在必要時進行更新。

下表提供了《*vSphere 安全性*》說明文件的更新歷程記錄。

修訂版本	說明
2018 年 5 月 11 日	■ 在 vCenter Server 與 Platform Services Controller 所需的連接埠中更新了連接埠 80 和 443 的注意事項。 ■ 在為 ESXi 主機新增允許的 IP 位址中新增了有關使用 vCLI 命令的資訊。 ■ 在 ESXi ESXCLI 防火牆命令中新增了 VMware 知識庫文章 2008226 的連結。 ■ 在加密現有虛擬機器或虛擬磁碟和使用信賴平台模組保護 ESXi 主機中插入了視訊連結。 ■ 在使用信賴平台模組保護 ESXi 主機和疑難排解 ESXi 主機證明問題中新增了已由 vCenter Server 管理的 TPM 2.0 和 ESXi 主機的相關資訊。
2018 年 4 月 27 日	■ 在使用信賴平台模組保護 ESXi 主機中新增了必要的 ESXi 主機 BIOS 設定。 ■ 在附註和注意須知中新增了有關傳送郵件和 TLS 的注意須知。
2018 年 4 月 17 日	初始版本。

vSphere 環境中的安全性

1

vSphere 環境的元件會立即受到數種功能的保護，如驗證、授權、每個 ESXi 主機上的防火牆等。您可以多種方式修改預設設定。例如，您可以對 vCenter 物件設定權限、開啟防火牆連接埠，或變更預設憑證。您可以為 vCenter 物件階層中的不同物件 (例如，vCenter Server 系統、ESXi 主機、虛擬機器、網路和儲存區物件) 採取安全性措施。

對需要注意的 vSphere 不同區域的高層級概觀可協助您計劃安全性策略。您也可以從 VMware 網站的其他 vSphere 安全性資源中受益。

本章節討論下列主題:

保護 ESXi Hypervisor

ESXi Hypervisor 開始使用即受保護。您可以透過使用鎖定模式，以及其他內建功能，來進一步保護 ESXi 主機。針對一致性，您可以設定參考主機，並將所有主機與參考主機的主機設定檔保持同步。您也可以透過執行指令碼式管理保護您的環境，這會確保變更套用到所有主機。

您可以採取下列動作，增強對 vCenter Server 管理之 ESXi 主機的保護。如需背景和詳細資料，請參閱《*VMware vSphere Hypervisor 安全性*》白皮書。

限制 ESXi 存取

依預設，ESXi Shell 和 SSH 服務未在執行中，並且僅根使用者可以登入 Direct Console 使用者介面 (DCUI)。如果您決定啟用 ESXi 或 SSH 存取，可以設定逾時來限制未經授權存取的風險。

	可以存取 ESXi 主機的使用者必須具有管理主機的權限。您可以從管理主機的 vCenter Server 系統對主機物件設定權限。
使用具名使用者和最少的權限	依預設，根使用者可以執行許多工作。不允許管理員使用根使用者帳戶登入 ESXi 主機。而是從 vCenter Server 建立具名管理員使用者，並為這些使用者指派管理員角色。您也可以為這些使用者指派自訂角色。請參閱建立自訂角色。 如果您直接管理主機上的使用者，則會限制角色管理選項。請參閱 *vSphere 單一主機管理 - VMware Host Client* 說明文件。
將開啟的 ESXi 防火牆連接埠數目降至最低	依預設，僅在您啟動對應的服務時，ESXi 主機上的防火牆連接埠才處於開啟狀態。您可以使用 vSphere Web Client、ESXCLI 或 PowerCLI 命令來檢查並管理防火牆連接埠狀態。 請參閱 ESXi 防火牆組態。
自動化 ESXi 主機管理	由於同一資料中心中的不同主機處於同步狀態通常很重要，因此，請使用指令碼式安裝或 vSphere Auto Deploy 佈建主機。您可以使用指令碼管理主機。主機設定檔是指令碼式管理的替代。您可設定參考主機，匯出主機設定檔，並將主機設定檔套用到所有主機。您可以直接套用主機設定檔，或者做為使用 Auto Deploy 進行佈建的一部分。 如需有關 vSphere Auto Deploy 的資訊，請參閱使用指令碼管理主機組態設定和 *vCenter Server 安裝和設定*說明文件。
利用鎖定模式	在鎖定模式下，依預設僅能透過 vCenter Server 存取 ESXi 主機。從 vSphere 6.0 開始，您可以選取嚴格鎖定模式或一般鎖定模式。您可以定義例外使用者來允許直接存取服務帳戶 (如備份代理程式)。 請參閱鎖定模式。
檢查 VIB 套件完整性	每個 VIB 套件都具有相關聯的接受程度。僅當 VIB 的接受程度等同於或優於 ESXi 主機的接受程度時，才可以將此 VIB 新增至此主機。不得將接受程度為 CommunitySupported 或 PartnerSupported 的 VIB 新增至主機，除非您明確變更主機的接受程度。 請參閱管理主機和 VIB 的接受程度。
管理 ESXi 憑證	在 vSphere 6.0 及更新版本中，VMware Certificate Authority (VMCA) 使用依預設將 VMCA 做為根憑證授權機構的已簽署憑證佈建每台 ESXi 主機。如果公司原則需要，您可以將現有憑證取代為由第三方或企業 CA 簽署的憑證。 請參閱 ESXi 主機的憑證管理。
考量智慧卡驗證	從 vSphere 6.0 開始，ESXi 支援使用智慧卡驗證，而不是使用者名稱和密碼驗證。為增強安全性，您可以設定智慧卡驗證。vCenter Server 也支援雙重要素驗證。

請參閱設定用於 ESXi 的智慧卡驗證。

考量 ESXi 帳戶鎖定

從 vSphere 6.0 開始，支援透過 SSH 和 vSphere Web Services SDK 存取帳戶鎖定。依預設，最多 10 次嘗試失敗後，帳戶即會鎖定。依預設，帳戶會在兩分鐘後解除鎖定。

備註 Direct Console 介面 (DCUI) 和 ESXi Shell 不支援帳戶鎖定。

請參閱 ESXi 密碼及帳戶鎖定。

儘管獨立主機的管理工作可能有所不同，但其安全考量事項類似。請參閱 *vSphere 單一主機管理 - VMware Host Client* 說明文件。

保護 vCenter Server 系統和相關聯服務的安全

您的 vCenter Server 系統和相關聯的服務透過 vCenter Single Sign-On 進行驗證以及透過 vCenter Server 權限模型進行授權的方式受到保護。您可以修改預設行為，並採取其他步驟限制對您環境的存取。

請注意，在您保護 vSphere 環境時，也必須保護與 vCenter Server 執行個體相關聯的所有服務。在某些環境中，您可以要保護多個 vCenter Server 執行個體，以及一或多個 Platform Services Controller 執行個體。

強化所有 vCenter 主機

保護 vCenter 環境的第一步是強化 vCenter Server 或其相關聯服務執行所在的每部機器。類似的考量適用於實體機器或虛擬機器。始終安裝適用於您作業系統的最新安全性修補程式，並遵循業界標準最佳做法來保護主機電腦。

瞭解 vCenter 憑證模型

依預設，VMware Certificate Authority 會佈建環境中的每台 ESXi 主機、每台機器，以及具有 VMCA 所簽署憑證的每個解決方案使用者。環境可立即運作，但如果公司原則需要，您可以變更預設行為。如需詳細資料，請參閱 *Platform Services Controller 管理* 說明文件。

如需其他保護，請明確移除到期或撤銷的憑證及已失敗的安裝。

設定 vCenter Single Sign-On

vCenter Server 及其相關聯的服務受到 vCenter Single Sign-On 驗證架構的保護。當您首次安裝軟體時，請為 vCenter Single Sign-On 網域的管理員指定密碼，預設為 administrator@vsphere.local。僅該網域做為身分識別來源初始可用。您可以新增其他身分識別來源 (Active Directory 或 LDAP)，並設定預設身分識別來源。然後，可向其中一個身分識別來源進行驗證的使用者可以檢視物件並執行工作 (如果其有權執行這些作業)。如需詳細資料，請參閱 *Platform Services Controller 管理* 說明文件。

將角色指派給具名使用者或群組

為了更好地記錄，請將您授與物件的每個權限與具名使用者或群組，以及預先定義的角色或自訂角色相關聯。vSphere 6.0 權限模型提供很大的彈性，可透過多種方式為使用者或群組授權。請參閱瞭解 vSphere 中的授權和一般工作所需的權限。

限制管理員權限及管理員角色的使用。如果可能，請勿使用匿名管理員使用者。

設定 NTP

設定環境中每個節點的 NTP。憑證基礎結構需要準確的時間戳記，如果節點不同步，則無法正確運作。

請參閱同步 vSphere 網路上的時鐘。

確保虛擬機器安全

若要保護虛擬機器，請修補客體作業系統並保護您的環境，如同保護實體機器一樣。請考慮停用不必要的功能，儘量少用虛擬機器主控台，並遵循其他最佳做法。

保護客體作業系統

若要保護您的客體作業系統，請確保該系統使用最新的修補程式以及反間諜軟體和反惡意程式碼應用程式 (如果適用)。請參閱客體作業系統廠商提供的說明文件以及手冊或網際網路中可能提供的針對該作業系統的其他資訊。

停用不必要的功能

確認不必要的功能已停用，以盡可能地減少潛在攻擊點。依預設，許多不常使用的功能會處於停用狀態。移除不必要的硬體並停用某些功能，例如主機-客體檔案系統 (HFSG)，或者在虛擬機器與遠端主控台之間執行複製並貼上作業。

請參閱停用虛擬機器中不必要的功能。

使用範本和指令碼式管理

虛擬機器範本可讓您設定作業系統使其滿足您的需求，然後建立具有相同設定的其他虛擬機器。

若要在初始部署後變更虛擬機器設定，請考慮使用指令碼，例如 PowerCLI。本說明文件說明如何使用 GUI 執行工作。請考慮使用指令碼而非 GUI 以保持您的環境一致。在大型環境中，您可以將虛擬機器分組至各個資料夾，以最佳化指令碼。

如需範本的相關資訊，請參閱使用範本部署虛擬機器和 *vSphere 虛擬機器管理*。如需 PowerCLI 的相關資訊，請參閱 VMware PowerCLI 說明文件。

儘量少用虛擬機器主控台

虛擬機器主控台為虛擬機器提供的功能與實體伺服器上的監視器所提供的功能相同。有存取虛擬機器主控台權限的使用者可存取虛擬機器電源管理和卸除式裝置連線控制。因此，存取虛擬機器主控台可能造成對虛擬機器的惡意攻擊。

考量 UEFI 安全開機

從 vSphere 6.5 開始，您可以設定虛擬機器使用 UEFI 開機。如果作業系統支援安全 UEFI 開機，您可以為虛擬機器選取該選項以獲得額外的安全性。請參閱對虛擬機器啟用或停用 UEFI 安全開機。

保護虛擬網路層的安全

虛擬網路層包括虛擬網路介面卡、虛擬交換器、分散式虛擬交換器，以及連接埠和連接埠群組。ESXi 依賴虛擬網路層來支援虛擬機器與其使用者之間的通訊。此外，ESXi 可使用虛擬網路層與 iSCSI SAN 和 NAS 儲存區等進行通訊。

vSphere 包含安全網路基礎結構所需的完整陣列功能。您可以分別保護基礎結構的每個元素，例如虛擬交換器、分散式虛擬交換器和虛擬網路介面卡。此外，請考慮第 10 章確保 vSphere 網路安全中詳細介紹的準則。

隔離網路流量

隔離網路流量對於保護 ESXi 環境的安全至關重要。不同的網路需要不同的存取權和隔離層級。管理網路將用戶端流量、命令列介面 (CLI) 或 API 流量以及第三方軟體流量與一般流量隔離。確保此管理網路只能由系統、網路和安全管理員存取。

請參閱 ESXi 網路安全性建議。

使用防火牆保護虛擬網路元素的安全

您可以開啟和關閉防火牆連接埠，並分別保護虛擬網路中的每個元素。針對 ESXi 主機，防火牆規則將服務與對應的防火牆相關聯，從而可以根據服務狀態來開啟和關閉防火牆。請參閱 ESXi 防火牆組態。

您也可以明確開啟 Platform Services Controller 和 vCenter Server 執行個體上的連接埠。請參閱 vCenter Server 與 Platform Services Controller 所需的連接埠和其他 vCenter Server TCP 和 UDP 連接埠。

考量網路安全性原則

網路安全性原則可提供流量保護，防止 MAC 位址模擬和不需要的連接埠掃描。標準交換器或分散式交換器的安全性原則會在網路通訊協定堆疊的第 2 層 (資料連結層) 實作。安全性原則的三大要素分別是混合模式、MAC 位址變更和偽造的傳輸。

如需相關指示，請參閱 *vSphere 網路*說明文件。

保護虛擬機器網路的安全

您用於保護虛擬機器網路安全的方法取決於多個因素，包括：

- 安裝的客體作業系統。
- 虛擬機器是否在信任的環境中運作。

與其他一般的安全性措施 (例如，安裝防火牆) 搭配使用時，虛擬交換器和分散式虛擬交換器提供重要保護。

請參閱第 10 章確保 vSphere 網路安全。

考量使用 VLAN 來保護環境

ESXi 支援 IEEE 802.1q VLAN。VLAN 可讓您將實體網路分段。您可以使用 VLAN 來進一步保護虛擬機器網路或儲存區組態。當您使用 VLAN 時，同一實體網路中的兩個虛擬機器無法相互收發封包，除非位於相同的 VLAN 上。

請參閱透過 VLAN 保護虛擬機器的安全。

保護虛擬化儲存區的連線安全

虛擬機器會在虛擬磁碟上儲存作業系統檔案、程式檔案和其他資料。對於虛擬機器，每個虛擬磁碟都顯示為已連線至 SCSI 控制器的 SCSI 磁碟機。虛擬機器與儲存區詳細資料相互隔離，無法存取虛擬磁碟所在 LUN 的相關資訊。

虛擬機器檔案系統 (VMFS) 是為 ESXi 主機提供虛擬磁碟區的分散式檔案系統和磁碟區管理員。您將負責保護儲存區的連線安全。例如，如果您使用的是 iSCSI 儲存區，可以將環境設定為使用 CHAP。如果公司原則需要，您可以設定相互 CHAP。使用 vSphere Web Client 或 CLI 設定 CHAP。

	請參閱儲存區安全性最佳做法。
評估 IPSec 的使用情況	ESXi 支援針對 IPv6 使用 IPSec。您無法針對 IPv4 使用 IPSec。 請參閱網際網路通訊協定安全性。

此外，請評估 VMware NSX for vSphere 是否為保護環境中網路層的有效解決方案。

vSphere 環境中的密碼

vSphere 環境中的密碼限制、密碼到期和帳戶鎖定視使用者的目標系統、使用者的身分，以及原則的設定方式而有所不同。

ESXi 密碼

ESXi 密碼限制由 Linux PAM 模組 pam_passwdqc 決定。請參閱 Linux 手冊頁瞭解 `pam_passwdqc`，並參閱 ESXi 密碼及帳戶鎖定。

vCenter Server 及其他 vCenter 服務的密碼

vCenter Single Sign-On 會管理所有登入 vCenter Server 及其他 vCenter 服務的使用者驗證。密碼限制、密碼到期和帳戶鎖定視使用者的網域和使用者的身分而有所不同。

vCenter Single Sign-On 管理員	vCenter Single Sign-On 管理員的密碼預設為 administrator@vsphere.local，若您在安裝期間指定不同的網域，則密碼為 administrator@*mydomain*。此密碼不會到期。在所有其他方面，密碼必須遵循 vCenter Single Sign-On 密碼原則中設定的限制。如需詳細資料，請參閱 *Platform Services Controller 管理*。 如果您忘記了此使用者的密碼，請搜尋 VMware 知識庫系統，瞭解重設此密碼的相關資訊。重設需要其他權限，例如對 vCenter Server 系統的根存取權限。
其他 vCenter Single Sign-On 網域使用者	其他 vsphere.local 使用者或您在安裝期間指定之網域使用者的密碼，必須遵循由 vCenter Single Sign-On 密碼原則和鎖定原則所設定的限制。如需詳細資料，請參閱 *Platform Services Controller 管理*。依預設，這些密碼會於 90 天後到期。管理員可以將到期日做為密碼原則的一部分進行變更。 如果您忘記了自己的 vsphere.local 密碼，管理員使用者可以使用 `dir-cli` 命令重設密碼。
其他使用者	所有其他使用者的密碼限制、密碼到期和帳戶鎖定由使用者可進行驗證的網域 (身分識別來源) 決定。 vCenter Single Sign-On 支援一個預設的身分識別來源。使用者只能以包含其使用者名稱的 vSphere Web Client 登入對應網域。如果使用者希望登入非預設網域，他們可以加入網域名稱，即，指定 *user@domain* 或 *domain\user*。網域密碼參數可套用至每一個網域。

vCenter Server Appliance Direct Console 使用者介面使用者的密碼

vCenter Server Appliance 是預先設定之 Linux 系統的虛擬機器，已針對 Linux 上的執行中 vCenter Server 及相關聯的服務進行最佳化。

部署 vCenter Server Appliance 時可指定這些密碼。

- 應用裝置 Linux 作業系統的根使用者密碼。
- vCenter Single Sign-On 網域的管理員密碼 administrator@vsphere.local (預設)。

您可以從應用裝置主控台變更根使用者密碼，並執行其他 vCenter Server Appliance 本機使用者管理工作。請參閱 *vCenter Server Appliance 組態*。

安全性最佳做法和資源

如果遵循最佳做法，您的 ESXi 和 vCenter Server 可與不包含虛擬化的環境一樣安全，甚至更安全。

本手冊包括適用於 vSphere 基礎結構之不同元件的最佳做法。

表格 1-1. 安全性最佳做法

vSphere 元件	資源
ESXi 主機	第 3 章保護 ESXi 主機
vCenter Server 系統	vCenter Server 安全性最佳做法
虛擬機器	虛擬機器安全性最佳做法
vSphere 網路	vSphere 網路安全性最佳做法

本手冊僅為確保安全環境所需的來源之一。

Web 上提供了 VMware 安全性資源，包括安全性警示和下載。

表格 1-2. Web 上的 VMware 安全性資源

主題	資源
VMware 安全性原則、最新安全性警示、安全性下載及安全性主題的重點討論。	http://www.vmware.com/go/security
公司安全性回應原則	http://www.vmware.com/support/policies/security_response.html VMware 致力於協助維護安全的環境。安全性問題會及時更正。VMware 安全性回應原則中作出了解決產品中可能存在的漏洞之承諾。
第三方軟體支援原則	http://www.vmware.com/support/policies/ VMware 支援各種儲存區系統和軟體代理程式 (如備份代理程式、系統管理代理程式等)。可以透過在 http://www.vmware.com/vmtn/resources/ 上搜尋 ESXi 相容性指南，找到支援 ESXi 的代理程式、工具及其他軟體的清單。 VMware 不可能對此產業中的所有產品和組態進行測試。如果 VMware 未在相容性指南中列出某種產品或組態，技術支援將嘗試協助您解決任何問題，但不保證該產品或組態的可用性。請始終對不支援的產品或組態仔細進行安全性風險評估。
符合性和安全性標準，以及關於虛擬化和符合性的合作夥伴解決方案和深入內容	http://www.vmware.com/go/compliance

表格 1-2. Web 上的 VMware 安全性資源 (繼續)

主題	資源
針對不同版本 vSphere 元件的安全性憑證和驗證 (如 CCEVS 和 FIPS) 的資訊。	https://www.vmware.com/support/support-resources/certifications.html
不同版本的 vSphere 和其他 VMware 產品的強化指南。	https://www.vmware.com/support/support-resources/hardening-guides.html
《VMware vSphere Hypervisor 安全性》白皮書	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

vSphere 權限和使用者管理工作 2

驗證和授權管理存取。vCenter Single Sign-On 支援驗證，這表示它可以判斷使用者究竟是否可以存取 vSphere 元件。此外，必須授權每位使用者檢視或操縱 vSphere 物件。

vSphere 支援瞭解 vSphere 中的授權中所述的數個不同的授權機制。本節的資訊焦點為 vCenter Server 權限模型的工作方式和執行使用者管理工作的方式。

vCenter Server 允許透過權限和角色對授權進行良好的控制。將權限指派給 vCenter Server 物件階層中的某個物件時，您可以指定哪些使用者或群組對該物件擁有哪些權限。若要指定權限，請使用角色，即權限集。

一開始，僅授權 vCenter Single Sign-On 網域管理員使用者 (預設為 administrator@vsphere.local) 登入 vCenter Server 系統。接著，該使用者將以如下方式繼續進行：

1 將已定義使用者和群組的身分識別來源新增至 vCenter Single Sign-On。請參閱 *Platform Services Controller 管理*說明文件。

2 透過選取某個物件 (例如虛擬機器或 vCenter Server 系統) 並為某個使用者或群組指派該物件上的角色，可將權限指定給該使用者或群組。

角色、特殊權限與使用權限 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_roles_privileges_permissions_vsphere_web_client)

本章節討論下列主題:

- 瞭解 vSphere 中的授權
- 管理 vCenter 元件的權限
- 全域權限
- 使用角色指派權限
- 針對角色和權限的最佳做法
- 一般工作所需的權限

瞭解 vSphere 中的授權

vSphere 透過更為精細的控制支援數種模型，以決定是否允許使用者執行某項工作。vCenter Single Sign-On 使用 vCenter Single Sign-On 群組中的群組成員資格，決定允許您執行什麼操作。您對物件的角色或全域權限會決定是否允許您在 vSphere 中執行其他工作。

授權概觀

vSphere 6.0 及更新版本允許有權限的使用者授與其他使用者權限，以執行工作。您可以使用全域權限，或者您可以針對個別 vCenter Server 執行個體，使用本機 vCenter Server 權限授權其他使用者。

vCenter Server 權限

vCenter Server 系統的權限模型依賴於將權限指派到物件階層中的物件。每個權限會授予某個使用者或群組一組權限，即所選物件的角色。例如，您可以選取某個虛擬機器，然後選取**新增權限**以指派角色給您所選網域中的一組使用者。該角色可授與這些使用者在該虛擬機器上的對應權限。

全域權限

全域權限會套用到跨解決方案的全域根物件。例如，如果同時安裝了 vCenter Server 和 vRealize Orchestrator，則可以使用全域權限。例如，您可以授與使用者群組對兩個物件階層中所有物件的讀取權限。

全域權限會複寫到整個 vsphere.local 網域。全域權限不為透過 vsphere.local 群組管理的服務提供授權。請參閱全域權限。

vCenter Single Sign-On 群組中的群組成員資格

vsphere.local 群組成員可執行特定工作。例如，如果您是 LicenseService.Administrators 群組的成員，則可以執行授權管理。請參閱 *Platform Services Controller 管理*說明文件。

ESXi 本機主機權限

如果您管理不是由 vCenter Server 系統管理的獨立 ESXi 主機，可以將其中一個預先定義的角色指派給使用者。請參閱 *vSphere 單一主機管理 - VMware Host Client* 說明文件。

對於受管理的主機，將角色指派到 vCenter Server 詳細目錄中的 ESXi 主機物件。

瞭解物件層級權限模型

您可以透過使用物件上的權限，來授權使用者或群組在 vCenter 物件上執行工作。vSphere 權限模型端賴對 vSphere 物件階層中的物件所指派的權限。每個權限會針對某個使用者或群組指定一組權限，即所選物件的角色。例如，一組使用者可能在一個虛擬機器上具有唯讀角色，而在另一個虛擬機器上具有管理員角色。

下列概念很重要。

權限

vCenter Server 物件階層中的每個物件都擁有相關聯的權限。每個權限指定一個群組或使用者對物件擁有哪些權限。

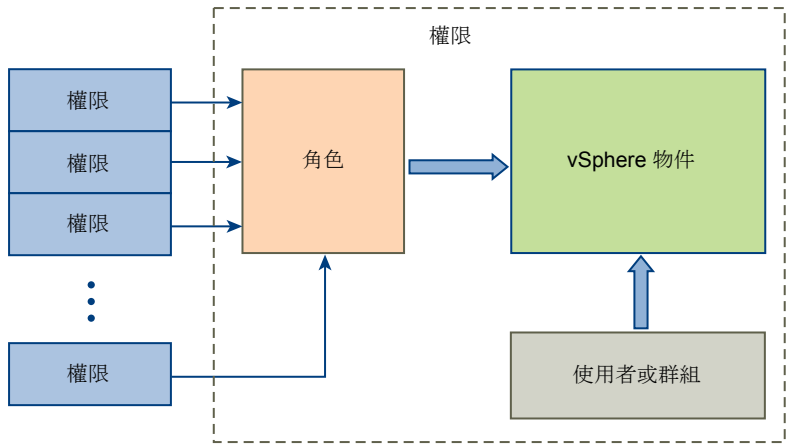
使用者和群組

在 vCenter Server 系統中，您只能將權限指派給已驗證使用者或已驗證使用者的群組。使用者將透過 vCenter Single Sign-On 進行驗證。必須在 vCenter Single Sign-On 用於驗證的身分識別來源中定義使用者和群組。使用身分識別來源中的工具 (例如 Active Directory) 定義使用者和群組。

權限 權限為細密的存取控制。您可以將這些權限群組到角色，然後將角色對應到使用者或群組。

角色 角色為權限集。角色讓您能夠根據使用者一般會執行的一組工作來指派物件的權限。vCenter Server 中已預先定義預設角色 (例如管理員) 且無法變更。其他角色 (例如資源集區管理員) 為預先定義的範例角色。您可以從頭開始建立自訂角色，也可以透過複製和修改範例角色來建立自訂角色。請參閱建立自訂角色。

圖 2-1 vSphere 權限



若要將權限指派給物件，請遵循以下步驟執行：

1 選取要將 vCenter 物件階層中的權限套用至的物件。

2 選取應擁有該物件權限的群組或使用者。

3 選取個別權限或角色，即群組或使用者應擁有的一組物件權限。

依預設，會散佈權限，即使用者或群組在所選物件及其子系物件上擁有所選角色。

vCenter Server 提供預先定義的角色，這些角色將合併常用權限集。您也可以透過合併一組角色來建立自訂角色。

通常必須在來源物件和目的地物件上同時定義權限。例如，如果您移動虛擬機器，則不僅需要該虛擬機器的權限，還需要目的地資料中心的權限。

請參閱下列資訊。

若要瞭解...	請參閱...
建立自訂角色。	建立自訂角色
所有權限和可套用權限的物件	第 13 章定義的權限
不同工作的不同物件上所需的權限集。	一般工作所需的權限

獨立 ESXi 主機的權限模型更為簡單。請參閱為 ESXi 主機指派權限。

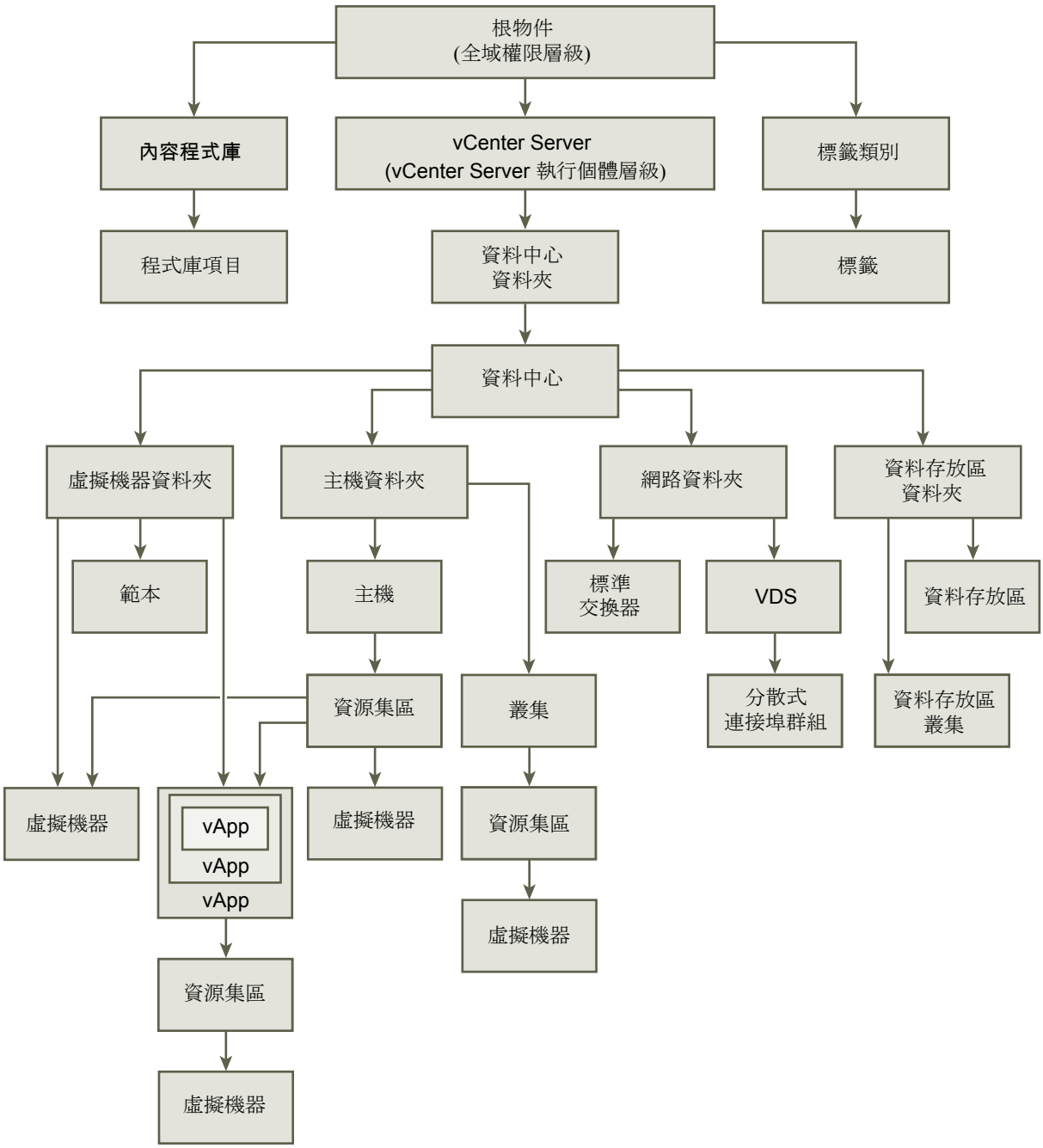
權限的階層式繼承

將權限指派給物件時，您可以選擇權限是否沿物件階層向下傳播。針對每個權限設定傳播方式。傳播並非普遍適用。為子系物件定義的權限永遠覆寫從父系物件傳播的權限。

此圖說明詳細目錄階層和權限可以傳播的路徑。

備註 全域權限支援從全域根物件跨解決方案指派權限。請參閱 全域權限。

圖 2-2 vSphere 詳細目錄階層



大多數詳細目錄物件會在階層中從單一父系物件繼承權限。例如，資料存放區會從其父系資料存放區資料夾或父系資料中心繼承權限。虛擬機器會同時從父系虛擬機器資料夾和父系主機、叢集或資源集區繼承權限。

例如，您可以為分散式交換器及其相關聯的分散式連接埠群組設定權限，方法是設定父系物件 (如資料夾或資料中心) 的權限。此外，您還必須選取用於將這些權限傳播到子系物件的選項。

權限在階層中採用數種形式：

受管理的實體

特權使用者可以定義受管理的實體的權限。

- 叢集
- 資料中心
- 資料存放區
- 資料存放區叢集
- 資料夾
- 主機
- 網路 (vSphere Distributed Switch 除外)
- 分散式連接埠群組
- 資源集區
- 範本
- 虛擬機器
- vSphere vApp

全域實體

您無法修改從根 vCenter Server 系統衍生權限的實體的權限。

- 自訂欄位
- 授權
- 角色
- 統計間隔
- 工作階段

多個權限設定

物件可能擁有多個權限，但是僅為每個使用者或群組指定一個權限。例如，有一個權限可能會指定群組 A 在某個物件上具有管理員權限。另一個權限可能會指定群組 B 在相同物件上具有虛擬機器管理員權限。

如果某物件繼承了來自兩個父系物件的權限，則一個物件的權限會新增到另一物件的權限。例如，假設虛擬機器位於虛擬機器資料夾中，並且也屬於資源集區。該虛擬機器會繼承來自虛擬機器資料夾和資源集區的所有權限設定。

在子系物件上套用的權限始終會覆寫在父系物件上套用的權限。請參閱範例 2：子權限覆寫父系權限。

如果對同一物件定義了多個群組權限，且使用者屬於這些群組中的兩個或多個群組，則可能出現下列兩種情況：

- 沒有直接在物件上定義使用者權限。在此情況下，使用者擁有群組在該物件上所擁有的權限。
- 已直接在物件上定義使用者權限。在此情況下，該使用者的權限優先於所有群組權限。

範例 1：多個權限繼承

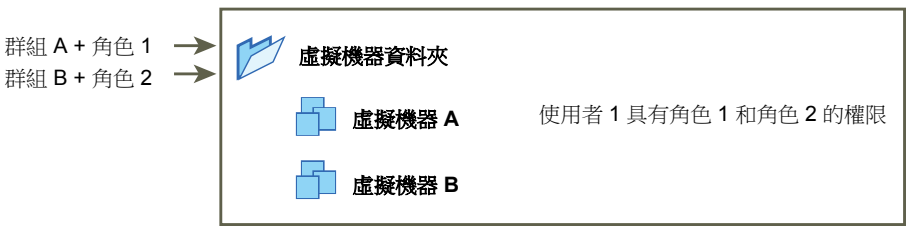
此範例說明物件如何從父系物件上授與權限的群組繼承多個權限。

在此範例中，將在同一物件上針對兩個不同的群組指派兩個權限。

- 角色 1 能夠開啟虛擬機器電源。
- 角色 2 可建立虛擬機器快照。
- 在虛擬機器資料夾上，將角色 1 授與群組 A，具備設定為可散佈到子物件的權限。
- 在虛擬機器資料夾上，將角色 2 授與群組 B，具備設定為可散佈到子物件的權限。
- 未向使用者 1 指派特定權限。

屬於群組 A 和 B 的使用者 1 登入。使用者 1 可為虛擬機器 A 和虛擬機器 B 開啟電源並建立快照。

圖 2-3 範例 1：多個權限繼承



範例 2：子權限覆寫父系權限

此範例說明子物件上指派的權限如何覆寫父系物件上指派的權限。可使用此覆寫行為限制使用者對詳細目錄的特定區域的存取。

在此範例中，權限將在兩個不同的物件上針對兩個不同的群組進行定義。

- 角色 1 能夠開啟虛擬機器電源。
- 角色 2 可建立虛擬機器快照。
- 在虛擬機器資料夾上，將角色 1 授與群組 A，具備設定為可散佈到子物件的權限。
- 在虛擬機器 B 上，將角色 2 授與群組 B。

屬於群組 A 和 B 的使用者 1 登入。由於角色 2 的指派位置在階層中比角色 1 略低，因此角色 2 會覆寫虛擬機器 B 上的角色 1。使用者 1 可開啟虛擬機器 A 的電源，但不能建立快照。使用者 1 可建立虛擬機器 B 的快照，但不能開啟它的電源。

圖 2-4 範例 2：子權限覆寫父系權限

範例 3：使用者角色覆寫群組角色

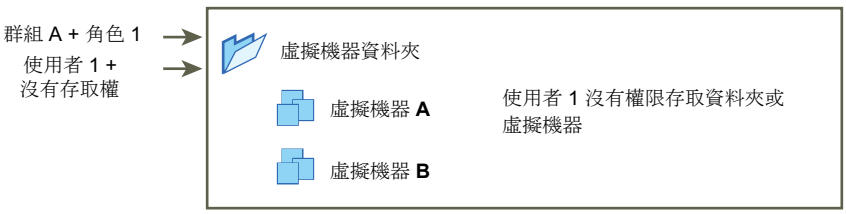
此範例說明了直接指派給個別使用者的角色如何覆寫與指派到群組之角色相關聯的權限。

在此範例中，將在相同物件上定義權限。某個權限會將群組與角色建立關聯，其他權限會將個別使用者與某個角色建立關聯。該使用者為群組成員。

- 角色 1 能夠開啟虛擬機器電源。
- 在虛擬機器資料夾上，將角色 1 授與群組 A。
- 在虛擬機器資料夾上，將無存取權角色授與使用者 1。

屬於群組 A 的使用者 1 登入。虛擬機器資料夾上被授與使用者 1 的無存取權角色會覆寫指派給群組的角色。使用者 1 無法存取虛擬機器資料夾或虛擬機器 A 與 B。

圖 2-5 範例 3：使用者權限覆寫群組權限



管理 vCenter 元件的權限

將在 vCenter 物件階層中的某個物件上設定權限。每個權限會將該物件與某個群組或使用者及該群組或使用者的存取角色建立關聯。例如，您可以選取某個虛擬機器物件，新增為群組 1 指定唯讀角色的權限，然後再新增為使用者 2 指定管理員角色的權限。

透過將不同角色指派給不同物件上的使用者群組，您可以控制使用者在 vSphere 環境中執行的工作。例如，若要允許群組設定主機的記憶體，請選取該主機並新增為該群組授與角色的權限 (包含**主機.組態.記憶體組態**權限)。

若要從 vSphere Web Client 管理權限，您需要瞭解以下概念：

權限	vCenter Server 物件階層中的每個物件都擁有相關聯的權限。每個權限指定一個群組或使用者對物件擁有哪些權限。
使用者和群組	在 vCenter Server 系統中，您只能將權限指派給已驗證使用者或已驗證使用者的群組。使用者將透過 vCenter Single Sign-On 進行驗證。必須在 vCenter Single Sign-On 用於驗證的身分識別來源中定義使用者和群組。使用身分識別來源中的工具 (例如 Active Directory) 定義使用者和群組。
權限	權限為細密的存取控制。您可以將這些權限群組到角色，然後將角色對應到使用者或群組。
角色	角色為權限集。角色讓您能夠根據使用者一般會執行的一組工作來指派物件的權限。vCenter Server 中已預先定義預設角色 (例如管理員) 且無法變更。其他角色 (例如資源集區管理員) 為預先定義的範例角色。您可以從頭開始建立自訂角色，也可以透過複製和修改範例角色來建立自訂角色。請參閱建立自訂角色。

您可以為階層之不同層級上的物件指派權限，例如，您可以為某個主機物件或包含所有主機物件的資料夾指派權限。請參閱 權限的階層式繼承。您還可以為某個全域根物件指派權限，以將權限套用到所有解決方案中的所有物件。請參閱 全域權限。

將權限新增到詳細目錄物件

在建立使用者和群組並定義角色後，您必須將使用者和群組及其角色指派給相關的詳細目錄物件。透過將物件移到資料夾並在資料夾上設定權限，您可以將相同的權限同時指派給多個物件。

當您從 vSphere Client 指派權限時，使用者和群組名稱必須準確符合 Active Directory (包括大小寫)。如果已從舊版 vSphere 進行升級，請在群組發生問題時檢查大小寫不一致情況。

先決條件

在要修改其權限的物件上，您必須具有包括**權限.修改權限**權限的角色。

程序

1. 在 vSphere Client 物件瀏覽器中，瀏覽到您想要為其指派權限的物件。
2. 按一下**權限**索引標籤。
3. 按一下 [新增] 圖示，然後按一下**新增**。
4. 選取將獲得由所選角色定義之權限的使用者或群組。
   a. 從**網域**下拉式功能表中，選取使用者或群組的網域。
   b. 在 [搜尋] 方塊中輸入名稱，或者從清單中選取名稱。

      系統便會搜尋使用者名稱、群組名稱和說明。
   c. 選取使用者或群組，然後按一下**新增**。

      即會將名稱新增到**使用者**或**群組**清單。

d (選擇性) 按一下**檢查名稱**，以確認身分識別來源中存在該使用者或群組。

e 按一下**確定**。

5 從**已指派的角色**下拉式功能表中選取角色。

指派給該物件的角色會顯示在功能表中。角色標題下方的區段中會列出角色所包含的權限。

6 (選擇性) 若要限制散佈，請取消選取**散佈到子系物件**核取方塊。

角色僅會套用到選取的物件，不會散佈到子系物件。

7 按一下**確定**以新增權限。

變更或移除權限

為詳細目錄物件設定使用者或群組，以及角色配對後，可以變更與使用者或群組配對的角色，或變更**散佈**核取方塊的設定。您也可以移除權限設定。

程序

1 在 vSphere Web Client 物件導覽器中瀏覽到物件。

2 按一下**權限**索引標籤。

3 按一下資料列以選取權限。

工作	步驟
變更權限	a 按一下**針對權限變更角色**圖示。 b 從**已指派的角色**下拉式功能表，為使用者或群組選取角色。 c 如果您想要變更權限繼承，請切換**散佈到子系**核取方塊。 d 按一下**確定**。
移除權限	按一下**移除權限**圖示。

變更使用者驗證設定

vCenter Server 會根據使用者目錄中的使用者和群組，定期驗證其使用者和群組清單。根據驗證結果，它會移除該網域中不再存在的使用者或群組。您可以停用驗證或變更兩次驗證之間的間隔。如果網域中有數千個使用者或群組，或者如果完成搜尋需要很長時間，則您可以考慮調整搜尋設定。

對於 vCenter Server5.0 之前的 vCenter Server 版本，這些設定會套用到與 vCenter Server 相關聯的 Active Directory。對於 vCenter Server5.0 及更新版本，這些設定會套用到 vCenter Single Sign-On 身分識別來源。

備註 此程序僅適用於 vCenter Server 使用者清單。您無法以相同的方式搜尋 ESXi 使用者清單。

程序

1 在 vSphere Web Client 物件導覽器中，瀏覽到 vCenter Server 系統。

2 選取**設定**，然後按一下**設定 > 一般**。

3 按一下**編輯**，然後選取**使用者目錄**。

4 視需要變更值，然後按一下**確定**。

選項	說明
使用者目錄逾時	連線到 Active Directory 伺服器的逾時間隔 (以秒為單位)。此值指定 vCenter Server 允許在所選網域上執行的搜尋時間量上限。搜尋大型網域可能需要很長時間。
查詢限制	選取此核取方塊，以設定 vCenter Server 顯示的使用者和群組數目上限。
查詢限制大小	所選網域中 vCenter Server 在**選取使用者或群組**對話方塊中顯示的使用者和群組數目上限。如果輸入 0 (零)，將出現所有使用者和群組。
驗證	取消選取核取方塊，停用驗證
驗證期間	指定 vCenter Server 驗證權限的頻率 (以分鐘為單位)。

全域權限

全域權限會套用到跨解決方案的全域根物件，例如 vCenter Server 和 vRealize Orchestrator。使用全域權限，將所有物件階層中所有物件的權限提供給使用者或群組。

每種解決方案自身的物件階層中都包含一個根物件。在所有解決方案中，全域根物件充當根物件的父系物件。您可以將全域權限指派給使用者或群組，並決定每個使用者或群組的角色。角色決定了使用者或群組針對階層中所有物件所具有的權限集。您可以指派預先定義的角色，或建立自訂角色。請參閱使用角色指派權限。區分 vCenter Server 權限和全域權限是十分重要的。

vCenter Server 權限

通常，您可將權限套用到 vCenter Server 詳細目錄物件，例如 ESXi 主機或虛擬機器。套用後，指定某使用者或群組具有一組權限，即該物件上的角色。

全域權限

全域權限會賦予使用者或群組檢視或管理您部署中每個詳細目錄階層上所有物件的權限。

如果您指派了全域權限且未選取 [散佈]，則此權限相關聯的使用者或群組將沒有存取階層中物件的權限。這些使用者或群組將只能存取部分全域功能 (例如建立角色)。

重要事項 請謹慎使用全域權限。確認您確實要將權限指派給所有詳細目錄階層中的所有物件。

新增全域權限

您可以使用全域權限為部署中所有詳細目錄階層的所有物件指定使用者或群組權限。

重要事項 請謹慎使用全域權限。確認您確實要將權限指派給所有詳細目錄階層中的所有物件。

先決條件

若要執行此工作，您必須擁有所有詳細目錄階層之根物件的**權限.修改權限**權限。

程序

1 在 [存取控制] 區域中，按一下**管理**並選取**全域權限**。

2 按一下**管理**，然後按一下**新增權限**圖示。

3 選取將獲得由所選角色定義之權限的使用者或群組。

a 從**網域**下拉式功能表中，選取使用者或群組的網域。

b 在 [搜尋] 方塊中輸入名稱，或者從清單中選取名稱。

系統便會搜尋使用者名稱、群組名稱和說明。

c 選取使用者或群組，然後按一下**新增**。

即會將名稱新增到**使用者**或**群組**清單。

d (選擇性) 按一下**檢查名稱**，以確認身分識別來源中存在該使用者或群組。

e 按一下**確定**。

4 從**已指派的角色**下拉式功能表中選取角色。

指派給該物件的角色會顯示在功能表中。角色標題下方的區段中會列出角色所包含的權限。

5 決定是否要將**散佈到子系**核取方塊保持選取狀態。

如果您指派了全域權限且未選取**散佈**，此權限相關聯的使用者或群組將沒有存取階層中物件的權限。這些使用者或群組將只能存取部分全域功能 (例如建立角色)。

6 按一下**確定**。

標籤物件的權限

在 vCenter Server 物件階層中，標籤物件不是 vCenter Server 的子系，但卻在 vCenter Server 根層級中建立。在包含多個 vCenter Server 執行個體的環境中，標籤物件在 vCenter Server 執行個體之間共用。標籤物件的權限與 vCenter Server 物件階層中其他物件的權限的運作方式有所不同。

僅全域權限或指派至標籤物件的權限適用

如果您授與 vCenter Server 詳細目錄物件 (例如虛擬機器) 的權限給使用者，該使用者可以執行與權限相關聯的工作。但是，使用者無法對物件執行標籤作業。

例如，如果您將**指派 vSphere 標籤**權限授與主機 TPA 上的使用者 Dana，該權限不會影響 Dana 是否可在主機 TPA 上指派標籤。Dana 必須擁有根層級的**指派 vSphere 標籤**權限，即全域權限；或必須擁有標籤物件的權限。

表格 2-1. 全域權限和標籤物件權限如何影響使用者可採取的動作

全域權限	標籤層級權限	vCenter Server 物件層級權限	有效權限
未指派標記權限。	Dana 擁有標籤的**指派或取消指派 vSphere 標籤**權限。	Dana 擁有 ESXi 主機 TPA 上的**刪除 vSphere 標籤**權限。	Dana 擁有標籤的**指派或取消指派 vSphere 標籤**權限。
Dana 擁有**指派或取消指派 vSphere 標籤**權限。	未針對標籤指派權限。	Dana 擁有 ESXi 主機 TPA 上的**刪除 vSphere 標籤**權限。	Dana 擁有**指派或取消指派 vSphere 標籤**全域權限。其包括標籤層級的權限。
未指派標記權限。	未針對標籤指派權限。	Dana 擁有 ESXi 主機 TPA 上的**指派或取消指派 vSphere 標籤**權限。	Dana 沒有任何物件 (包括主機 TPA) 的標記權限。

全域權限補充標籤物件權限

全域權限，即根物件上指派的權限，會在標籤物件上的權限限制較嚴格時補充標籤物件上的權限。vCenter Server 權限不會影響標籤物件。

例如，假定您透過使用全域權限將**刪除 vSphere 標籤**權限指派給位於根層級的使用者 Robin。對於標籤 [生產]，您沒有將**刪除 vSphere 標籤**權限指派給 Robin。在這種情況下，因 Robin 擁有全域權限，所以他擁有標籤 [生產] 的權限。除非您修改全域權限，否則您無法限制權限。

表格 2-2. 全域權限補充標籤層級權限

全域權限	標籤層級權限	有效權限
Robin 擁有**刪除 Robin vSphere 標籤**權限	Robin 沒有標籤的**刪除 vSphere 標籤**權限。	Robin 擁有**刪除 Robin vSphere 標籤**權限。
未指派標記權限	Robin 沒有針對標籤指派的**刪除 vSphere 標籤**權限。	Robin 沒有**刪除 vSphere 標籤**權限

標籤層級權限可延伸全域權限

您可以使用標籤層級權限來延伸全域權限。這表示使用者可同時擁有標籤的全域權限和標籤層級權限。

表格 2-3. 全域權限延伸標籤層級權限

全域權限	標籤層級權限	有效權限
Lee 擁有**指派或取消指派 vSphere 標籤**權限。	Lee 擁有**刪除 vSphere 標籤**權限。	Lee 擁有標籤的**指派 vSphere 標籤**權限以及**刪除 vSphere 標籤**權限。
未指派標記權限。	Lee 擁有針對標籤指派的**刪除 vSphere 標籤**權限。	Lee 擁有標籤的**刪除 vSphere 標籤**權限。

使用角色指派權限

角色是一組預先定義的權限。權限會定義執行動作和讀取內容的權限。例如，虛擬機器管理員角色允許使用者讀取並變更虛擬機器屬性。

指派權限時，將使用者或群組與角色配對，然後將該配對與詳細目錄物件相關聯。單一使用者或群組針對詳細目錄中的不同物件可能有不同角色。

例如，假設您的詳細目錄中有兩個資源集區 (集區 A 和集區 B)。您可以為群組 Sales 在集區 A 上指派虛擬機器使用者角色，而在集區 B 上指派唯讀角色。執行上述指派後，群組 Sales 中的使用者可以開啟集區 A 中的虛擬機器，但只能檢視集區 B 中的虛擬機器。

vCenter Server 預設會提供系統角色和範例角色。

系統角色 系統角色是永久的。無法編輯與這些角色關聯的權限。

範例角色 VMware 為某個頻繁執行的工作組合提供範例角色。您可複製、修改或移除這些角色。

備註 若要避免遺失範例角色中預先定義的設定，請先複製該角色，然後對複製品進行修改。無法將範例重設為預設設定。

如果使用者擁有的角色包含在建立工作時執行該工作的權限，則只能對工作進行排程。

備註 即使所涉及到的使用者已登入，對角色和權限的變更也會即時生效。但搜尋除外，在搜尋中，這些變更會在使用者登出再重新登入之後才生效。

vCenter Server 和 ESXi 中的自訂角色

可以為 vCenter Server 及其管理的所有物件，或為個別主機建立自訂角色。

vCenter Server 自訂角色 (建議) 可以使用 vSphere Web Client 中的角色編輯功能建立自訂角色，以建立符合您需求的權限集。

ESXi 自訂角色 可以透過使用 CLI 或 VMware Host Client 為個別主機建立自訂角色。請參閱 *vSphere 單一主機管理 - VMware Host Client* 說明文件。無法從 vCenter Server 存取自訂主機角色。

如果您透過 vCenter Server 管理 ESXi 主機，請勿同時在主機和 vCenter Server 中保留自訂角色。在 vCenter Server 層級定義角色。

使用 vCenter Server 管理主機時，與該主機相關聯的權限會透過 vCenter Server 建立並儲存在 vCenter Server 上。如果直接連線至主機，則只能使用直接在主機上建立的角色。

備註 新增自訂角色但不為其指派任何權限時，系統會將角色建立為擁有三個系統定義之權限的唯讀角色：**系統.匿名**、**系統.檢視**以及**系統.讀取**。

在 vSphere Web Client 中建立角色 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_creating_role_in_vsphere_webclient)

建立自訂角色

您可以根據環境的存取控制需求建立 vCenter Server 自訂角色。您可以從頭建立角色，或複製現有角色。

您可以在是與其他 vCenter Server 系統相同的 vCenter Single Sign-On 網域一部分的 vCenter Server 系統上建立或編輯角色。VMware Directory Service (vmdir) 會將您進行的角色變更傳播到群組中的所有其他 vCenter Server 系統。對特定使用者和物件的角色指派不會在 vCenter Server 系統上共用。

先決條件

確認您是否以具有管理員權限的使用者身分登入。

程序

1 登入 vCenter Server。

2 選取首頁，然後按一下**管理 > 角色**。

3 建立角色：

選項	說明
從頭建立角色	按一下**建立角色**按鈕。
透過複製建立角色	選取某個角色，然後按一下**複製角色**按鈕。

如需詳細資訊，請參閱 vCenter Server 系統角色。

4 輸入新角色的名稱。

5 選取和取消選取該角色的權限。

如需詳細資訊，請參閱第 13 章定義的權限。

6 按一下**確定**。

下一個

您現在可以透過選取某個物件，並將角色指派給該物件的使用者或群組來建立權限。

vCenter Server 系統角色

角色是一組預先定義的權限。當您將權限新增到物件時，同時也會將使用者或群組與角色進行配對。vCenter Server 包括數個系統角色，您無法變更這些角色。

vCenter Server 提供幾個預設角色。不能變更與預設角色關聯的權限。預設角色以階層方式進行組織整理。每個角色會繼承前一個角色的權限。例如，管理員角色會繼承唯讀角色的權限。

vCenter Server 角色階層還包括數個範例角色。您可以複製範例角色來建立類似的角色。

如果建立規則，它不會從任何系統角色繼承權限。

管理員角色

具有某物件之管理員角色的使用者，能夠檢視該物件並對其執行所有動作。此角色還包括唯讀角色中的所有權限。如果您具有某物件上的管理員角色，則可以將權限指派給個別使用者和群組。

如果您充當的是 vCenter Server 中的管理員角色，則可以將權限指派給預設 vCenter Single Sign-On 身分識別來源中的使用者和群組。支援的身分識別服務包括 Windows Active Directory 和 OpenLDAP 2.4。

	依預設，安裝完成後，administrator@vsphere.local 使用者會同時在 vCenter Single Sign-On 和 vCenter Server 上獲得管理員角色。此時，該使用者即可將其他使用者與 vCenter Server 上的管理員角色進行關聯。
唯讀角色	具有某物件之唯讀角色的使用者能夠檢視該物件的狀態和有關該物件的詳細資料。例如，具有此角色的使用者可檢視虛擬機器、主機以及資源集區屬性，但無法檢視主機的遠端主控台。透過功能表和工具列執行的所有動作均會遭到禁止。
無存取權角色	具有某物件之無存取權角色的使用者無法以任何方式檢視或變更該物件。依預設，新的使用者和群組會指派此角色。您可以逐物件地變更角色。 vCenter Single Sign-On 網域的管理員 (依預設為 administrator@vsphere.local)、根使用者以及 vpxuser 將依預設獲指派管理員角色。依預設，其他使用者將獲指派無存取權角色。
無密碼編譯管理員角色	具有某物件之無密碼編譯管理員角色的使用者擁有與具有管理員角色的使用者相同的權限，除了**密碼編譯作業**權限之外。這個角色允許管理員指定其他管理員，所指定管理員無法加密或解密虛擬機器，也無法存取已加密資料，但可執行所有其他管理工作。

最佳做法是在根層級建立使用者，並將管理員角色指派給該使用者。建立具有管理員權限的具名使用者後，您可從任何權限移除根使用者，或將其角色變更為無存取權。

針對角色和權限的最佳做法

遵循角色和權限的最佳做法，盡可能地提高 vCenter Server 環境的安全性和管理性。

在 vCenter Server 環境中設定角色和權限時，VMware 建議採用下列最佳做法：

- 可以的話，請將角色指派給群組，而不是個別使用者。
- 僅在有需要的物件上授與權限，並且僅將權限指派給必須具有這些權限的使用者或群組。使用最少權限數可以更輕鬆地瞭解和管理權限結構。
- 如果要為群組指派限制性角色，請確定該群組不包含管理員使用者或其他具有管理權限的使用者。否則，您可能無意中限制了詳細目錄階層組成部分 (已從中向該群組指派了限制性角色) 中管理員的權限。
- 使用資料夾將物件分組。例如，若要在一組主機上授與修改權限，而在另一組主機上授與檢視權限，請將每組主機置於一個資料夾中。
- 將權限新增到根 vCenter Server 物件時，請務必謹慎。具有根層級權限的使用者有權存取 vCenter Server 上的全域資料，如角色、自訂屬性、vCenter Server 設定。
- 當您將權限指派給物件時，請考慮啟用傳播。傳播可確保物件階層中的新物件繼承權限。例如，您可以為虛擬機器資料夾指派權限並啟用傳播，以確保此權限會套用至資料夾中的所有虛擬機器。
- 使用無存取權角色來遮罩階層的特定區域。無存取權角色會限制具有該角色的使用者或群組的存取權。

- 對授權的變更會按如下所示散佈：
  - 散佈到連結到相同 Platform Services Controller 的所有 vCenter Server 系統。
  - 散佈到相同 vCenter Single Sign-On 網域中的 Platform Services Controller 執行個體。
- 即使使用者沒有所有 vCenter Server 系統的權限，授權傳播仍會進行。

一般工作所需的權限

許多工作需要具有詳細目錄中多個物件的權限。如果嘗試執行工作的使用者只有一個物件的權限，則該工作無法成功完成。

下表列出了需要多個權限的一般工作。您可以透過將使用者與其中一個預先定義的角色或多個權限配對，來新增權限至詳細目錄物件。如果您希望指派一組權限多次，請建立自訂角色。

如果您要執行的工作不在此資料表中，下列規則會說明您必須指派權限才能允許特定作業的情況：

- 任何耗用儲存空間的作業，都需要有目標資料存放區的**資料存放區.配置空間**權限，以及自行執行作業的權限。例如，您在建立虛擬磁碟或建立快照時必須具有這些權限。
- 在詳細目錄階層中移動物件需要物件本身、來源父系物件 (如資料夾或叢集) 和目的地父系物件上的適當權限。
- 每個主機和叢集都擁有本身的隱含資源集區，集區中包含該主機或叢集的所有資源。將虛擬機器直接部署到主機或叢集，需要有**資源.將虛擬機器指派給資源集區**權限。

表格 2-4. 一般工作所需的權限

工作	所需權限	適當角色
建立虛擬機器	在目的地資料夾或資料中心上： ■ **虛擬機器.詳細目錄.新建** ■ **虛擬機器.組態.新增磁碟**(如果要建立新的虛擬磁碟) ■ **虛擬機器.組態.新增現有磁碟**(如果使用現有虛擬磁碟) ■ **虛擬機器.組態.原始裝置**(如果使用 RDM 或 SCSI 傳遞裝置)	管理員
	在目的地主機、叢集或資源集區上： **資源.將虛擬機器指派給資源集區**	資源集區管理員或管理員
	在目的地資料存放區或包含資料存放區的資料夾上： **資料存放區.配置空間**	資料存放區取用者或管理員
	在將虛擬機器指派到的網路上： **網路.指派網路**	網路取用者或管理員
開啟虛擬機器電源	在已部署虛擬機器的資料中心上： **虛擬機器.互動.開啟電源**	虛擬機器超級使用者或管理員
	在虛擬機器或虛擬機器資料夾上： **虛擬機器.互動.開啟電源**	
從範本部署虛擬機器	在目的地資料夾或資料中心上： ■ **虛擬機器.詳細目錄.從現有項目建立** ■ **虛擬機器.組態.新增磁碟**	管理員

表格 2-4. 一般工作所需的權限 (繼續)

工作	所需權限	適當角色
	在範本或範本資料夾上： **虛擬機器.佈建.部署範本**	管理員
	在目的地主機、叢集或資源集區上： **資源.將虛擬機器指派給資源集區**	管理員
	在目的地資料存放區或資料存放區資料夾上： **資料存放區.配置空間**	資料存放區取用者或管理員
	在將虛擬機器指派到的網路上： **網路.指派網路**	網路取用者或管理員
生成虛擬機器快照	在虛擬機器或虛擬機器資料夾上： **虛擬機器.快照管理.建立快照**	虛擬機器超級使用者或管理員
將虛擬機器移到資源集區中	在虛擬機器或虛擬機器資料夾上： ■ **資源.將虛擬機器指派給資源集區** ■ **虛擬機器.詳細目錄.移動**	管理員
	在目的地資源集區上： **資源.將虛擬機器指派給資源集區**	管理員
在虛擬機器上安裝客體作業系統	在虛擬機器或虛擬機器資料夾上： ■ **虛擬機器.互動.回答問題** ■ **虛擬機器.互動.主控台互動** ■ **虛擬機器.互動.裝置連線** ■ **虛擬機器.互動.關閉電源** ■ **虛擬機器.互動.開啟電源** ■ **虛擬機器.互動.重設** ■ **虛擬機器.互動.設定 CD 媒體**(如果從 CD 安裝) ■ **虛擬機器.互動.設定磁碟片媒體**(如果從磁碟片安裝) ■ **虛擬機器.互動 .VMware Tools 安裝**	虛擬機器超級使用者或管理員
	在包含安裝媒體 ISO 映像的資料存放區上： **資料存放區.瀏覽資料存放區**(如果從資料存放區上的 ISO 映像安裝) 在向其上傳安裝媒體 ISO 映像的資料存放區上： ■ **資料存放區.瀏覽資料存放區** ■ **資料存放區.低層級檔案作業**	虛擬機器超級使用者或管理員
透過 vMotion 移轉虛擬機器	在虛擬機器或虛擬機器資料夾上： ■ **資源.移轉已開啟電源的虛擬機器** ■ **資源.將虛擬機器指派給資源集區** (如果目的地資源集區與來源資源集區不同)	資源集區管理員或管理員
	在目的地主機、叢集或資源集區上 (如果與來源主機、叢集或資源集區不同)： **資源.將虛擬機器指派給資源集區**	資源集區管理員或管理員
冷移轉 (重新放置) 虛擬機器	在虛擬機器或虛擬機器資料夾上： ■ **資源.移轉已關閉電源的虛擬機器** ■ **資源.將虛擬機器指派給資源集區**(如果目的地資源集區與來源資源集區不同)	資源集區管理員或管理員

表格 2-4. 一般工作所需的權限 (繼續)

工作	所需權限	適當角色
	在目的地主機、叢集或資源集區上 (如果與來源主機、叢集或資源集區不同)： **資源.將虛擬機器指派給資源集區**	資源集區管理員或管理員
	在目的地資料存放區上 (如果與來源資料存放區不同)： **資料存放區.配置空間**	資料存放區取用者或管理員
透過 Storage vMotion 移轉虛擬機器	在虛擬機器或虛擬機器資料夾上： **資源.移轉已開啟電源的虛擬機器**	資源集區管理員或管理員
	在目的地資料存放區上： **資料存放區.配置空間**	資料存放區取用者或管理員
將主機移入叢集	在主機上： **主機.詳細目錄.新增主機至叢集**	管理員
	在目的地叢集上： **主機.詳細目錄.新增主機至叢集**	管理員
加密虛擬機器	只能在包含 vCenter Server 的環境中執行加密工作。此外，ESXi 主機必須為大多數加密工作啟用加密模式。執行此工作的使用者必須擁有適當的權限。一組**密碼編譯作業**權限允許進行更為精細的控制。請參閱加密工作的必要條件和所需權限。	管理員

保護 ESXi 主機

3

ESXi Hypervisor 架構具有許多內建安全性功能，如 CPU 隔離、記憶體隔離和裝置隔離。您可以設定其他功能，如鎖定模式、憑證取代與智慧卡驗證，以獲取增強的安全性。

ESXi 主機也受防火牆保護。您可以根據需要針對傳入和傳出流量開啟連接埠，但是應該限制對服務和連接埠的存取權。使用 ESXi 鎖定模式，並限制 ESXi Shell 的存取權，有助於進一步建立更安全的環境。從 vSphere 6.0 開始，ESXi 主機會加入憑證基礎結構。依預設，使用由 VMware Certificate Authority (VMCA) 簽署的憑證佈建主機。

如需有關 ESXi 安全性的其他資訊，請參閱 VMware 白皮書《*VMware vSphere Hypervisor 安全性*》。

本章節討論下列主題:

- ESXi 一般安全建議
- ESXi 主機的憑證管理
- 透過安全性設定檔自訂主機
- 為 ESXi 主機指派權限
- 使用 Active Directory 管理 ESXi 使用者
- 使用 vSphere Authentication Proxy
- 設定用於 ESXi 的智慧卡驗證
- 使用 ESXi Shell
- ESXi 主機的 UEFI 安全開機
- 使用信賴平台模組保護 ESXi 主機
- ESXi 記錄檔

ESXi 一般安全建議

若要避免 ESXi 主機遭到未經授權的入侵和不當使用，VMware 將對幾個參數、設定和活動強加限制。可以根據組態需求而放寬限制。若要放寬限制，請確定在受信任的環境中運作且採取了其他安全性措施。

內建安全性功能

開始使用時，主機的風險即降低，如下所示：

- 依預設，ESXi Shell 和 SSH 處於停用狀態。
- 依預設，僅有限數目的防火牆連接埠處於開啟狀態。您可以明確開啟與特定服務相關聯的其他防火牆連接埠。
- ESXi 僅執行管理其功能所必需的服務。散佈限制為執行 ESXi 所需的功能。
- 依預設，所有連接埠 (並非對主機進行管理存取所需) 均處於關閉狀態。請在需要其他服務時開啟連接埠。
- 依預設，將停用弱加密方式，並透過 SSL 保護來自用戶端的通訊。用於保護通道安全的精確演算法取決於 SSL 交握。建立於 ESXi 上的預設憑證，將具有 RSA 加密的 PKCS#1 SHA-256 用作簽章演算法。
- ESXi 在內部使用 Tomcat Web 服務來支援透過 Web Client 進行存取。此服務已經過修改，僅執行 Web Client 進行管理和監控所需的功能。因此，ESXi 不易遇到在更廣泛的應用中所報告的 Tomcat 安全性問題。
- VMware 將監控所有可能影響 ESXi 安全的安全性警示，並核發安全性修補程式 (如果需要)。
- 未安裝諸如 FTP 和 Telnet 之類的不安全服務，並且這些服務的連接埠預設為處於關閉狀態。由於 SSH 和 SFTP 之類較為安全的服務易於獲取，因此，請避免使用這些不安全的服務，並使用更為安全的替代方案。例如，如果 SSH 無法使用，而您必須使用 Telnet，請使用具有 SSL 的 Telnet 來存取虛擬序列埠。

  如果必須使用不安全的服務，且已為主機實作了充分的保護措施，則可以明確開啟相應連接埠以支援這些服務。
- 考慮對 ESXi 系統使用 UEFI 安全開機。請參閱 ESXi 主機的 UEFI 安全開機。

其他安全性措施

評估主機安全性和管理時，請考慮以下建議。

限制存取

如果您啟用對 Direct Console 使用者介面 (DCUI)、ESXi Shell 或 SSH 的存取，請強制執行嚴格的存取安全性原則。

ESXi Shell 具有對主機某些部分的存取權。只為受信任的使用者提供 ESXi Shell 登入存取權。

不直接存取受管理的主機

使用 vSphere Web Client 來管理受 vCenter Server 管理的 ESXi 主機。請勿使用 VMware Host Client 直接存取受管理的主機，也不要在 DCUI 中變更受管理的主機。

如果您使用指令碼式介面或 API 管理主機，請勿直接鎖定主機。而是鎖定管理主機的 vCenter Server 系統，然後指定主機名稱。

僅將 DCUI 用於疑難排解	僅為了疑難排解才以根使用者身分從 DCUI 或 ESXi Shell 存取主機。使用其中一個 GUI 用戶端或其中一個 VMware CLI 或 API 管理您的 ESXi 主機。如果您使用 ESXi Shell 或 SSH，請限制具有存取權的帳戶並設定逾時。
僅使用 VMware 來源以升級 ESXi 元件	主機執行多個第三方套件來支援管理介面或必須執行的工作。VMware 僅支援升級至這些來自 VMware 來源的套件。如果使用來自另一個來源的下載內容或修補程式，可能會危及管理介面的安全性或功能。檢查第三方廠商網站和 VMware 知識庫，取得安全性警示。

備註 請遵循以下位置的 VMware 安全性建議：http://www.vmware.com/security/。

利用主機設定檔設定 ESXi 主機

主機設定檔可讓您為 ESXi 主機設定標準組態，使主機自動遵循這些組態設定。主機設定檔可讓您控制主機組態的許多層面，包括記憶體、儲存區、網路等。

您可以從 vSphere Web Client 為參考主機設定主機設定檔，然後將主機設定檔套用至共用該參考主機特性的所有主機。您也可以使用主機設定檔來監控主機上的主機組態變更。請參閱 *vSphere 主機設定檔*說明文件。

您可以將主機設定檔附加至叢集，以將其套用至叢集中的所有主機。

程序

1. 設定參考主機的規格，然後建立主機設定檔。
2. 將設定檔附加至主機或叢集。
3. 將參考主機的主機設定檔套用至其他主機或叢集。

使用指令碼管理主機組態設定

在擁有多台主機的環境中，與從 vSphere Web Client 管理主機相比，使用指令碼管理主機更快速，產生的錯誤也更少。

vSphere 包含用於主機管理的多個指令碼語言。如需參考資訊和程式設計提示，請參閱《*vSphere 命令列說明文件*》和《*vSphere API/SDK 說明文件*》。如需有關指令碼式管理的其他提示，請參閱 VMware 社群。《vSphere 管理員》說明文件重點介紹如何使用 vSphere Web Client 進行管理。

vSphere PowerCLI	VMware vSphere PowerCLI 是 vSphere API 的 Windows PowerShell 介面。vSphere PowerCLI 包含用於管理 vSphere 元件的 PowerShell cmdlet。 vSphere PowerCLI 包含用於管理和自動化的 200 多個 cmdlet、範例指令碼集和函數程式庫。請參閱《*vSphere PowerCLI 說明文件*》。
vSphere Command-Line Interface (vCLI)	vCLI 包含用於管理 ESXi 主機和虛擬機器的命令集。該安裝程式執行 Windows 或 Linux 系統以及安裝 ESXCLI 命令、`vicfg-` 命令和一組其他 vCLI 命令，它也可安裝 vSphere SDK for Perl。請參閱《*vSphere Command-Line Interface 說明文件*》。

自 vSphere 6.0 起，您可以使用 vCloud Suite SDK 的其中一個指令碼介面，如 vCloud Suite SDK for Python。

程序

1 建立擁有限制權限的自訂角色。

例如，考慮建立具有一組管理主機的權限，但沒有管理虛擬機器、儲存區或網路的權限的角色。如果只想使用指令碼來擷取資訊，則可以建立擁有主機的唯讀權限的角色。

2 從 vSphere Web Client，建立服務帳戶，並為其指派自訂角色。

如果想要使對特定主機的存取權受到適當限制，則可以建立擁有不同層級存取權的多個自訂角色。

3 撰寫用於執行參數檢查或修改的指令碼，並執行這些指令碼。

例如，您可以按照如下方式檢查或設定主機的殼層互動式逾時：

語言	命令

vCLI (ESXCLI)	`esxcli <conn_options> system settings advanced get /UserVars/ESXiShellTimeOut`
	
	`esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /UserVars/ESXiShellTimeOut`

PowerCLI	`#List UserVars.ESXiShellInteractiveTimeOut for each host`
	`Get-VMHost | Select Name,`
	`@{N="UserVars.ESXiShellInteractiveTimeOut";E={$_`
	`| Get-AdvancedSetting -Name`
	`UserVars.ESXiShellInteractiveTimeOut`
	`| Select -ExpandProperty Value}}`
	
	`# Set UserVars.ESXiShellTimeOut to 900 on all hosts`
	`Get-VMHost`
	`| Foreach { Get-AdvancedSetting -Entity $_ -Name`
	`UserVars.ESXiShellInteractiveTimeOut | Set-AdvancedSetting -`
	`Value 900 }`

4 在大型環境中，建立擁有不同存取權限的角色，並根據要執行的工作將主機分組到資料夾中。然後從不同的服務帳戶針對不同的資料夾執行指令碼。

5 確認執行命令後的變更是所需變更。

ESXi 密碼及帳戶鎖定

對於 ESXi 主機，您必須使用符合預先定義需求的密碼。您可以使用 `Security.PasswordQualityControl` 進階選項來變更必要長度及字元類別需求或允許使用複雜密碼。

ESXi 使用 Linux PAM 模組 `pam_passwdqc` 進行密碼管理和控制。請參閱 `pam_passwdqc` 的手冊頁以瞭解詳細資訊。

備註 針對 ESXi 密碼的預設需求，可隨著版本不斷變更。您可以使用 `Security.PasswordQualityControl` 進階選項檢查並變更預設密碼限制。

ESXi 密碼

ESXi 會強制密碼必須符合需求，才能從 Direct Console 使用者介面、ESXi Shell、SSH 或 VMware Host Client 進行存取。

- 依預設，建立密碼時須包含以下四類字元的組合：小寫字母、大寫字母、數字和特殊字元 (如底線或破折號)。
- 依預設，密碼長度介於 7 到 40 個字元之間。
- 密碼不能包含字典字組或部分字典字組。

備註 密碼開頭的大寫字元不計入使用的字元類別數。密碼結尾的數字不計入使用的字元類別數。

ESXi 密碼範例

下列使用者輸入的密碼說明了潛在密碼 (如果選項以如下方式設定)。

```
retry=3 min=disabled,disabled,disabled,7,7
```

使用此設定時，由於前三個項目已停用，因此不允許使用包含一或兩類字元類別的密碼及複雜密碼。三類及四類字元類別的密碼需要七個字元。請參閱 `pam_passwdqc` 手冊頁以瞭解詳細資料。

使用這些設定時，允許使用下列密碼。

- xQaTEhb!：包含八個字元，由三類字元組成。
- xQaT3#A：包含七個字元，由四類字元組成。

下列使用者輸入的密碼不符合要求。

- Xqat3hi：以大寫字元開頭，將有效字元類別數目減少到兩種。最少需要三種類別的字元。
- xQaTEh2：以數字結尾，將有效字元類別數目減少到兩種。最少需要三種類別的字元。

ESXi 複雜密碼

除了密碼，您也可以使用複雜密碼，不過複雜密碼預設為停用。您可以透過使用 vSphere Web Client 的 `Security.PasswordQualityControl` 進階選項來變更此預設值或其他設定。

例如，您可將該選項變更為下列內容。

```
retry=3 min=disabled,disabled,16,7,7
```

此範例允許使用至少 16 個字元及 3 個字組 (以空格分隔) 的複雜密碼。

在舊版主機中仍然支援變更 `/etc/pamd/passwd` 檔案，但這在未來版本中會被取代。將改用 `Security.PasswordQualityControl` 進階選項。

變更預設密碼限制

您可以透過使用 ESXi 主機的 `Security.PasswordQualityControl` 進階選項來變更對密碼或複雜密碼的預設限制。請參閱 *vCenter Server 和主機管理* 說明文件瞭解有關設定 ESXi 進階選項的資訊。

您可以變更預設，例如要求最少 15 個字元且最少四個字，如下所示：

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

請參閱 `pam_passwdqc` 的手冊頁以瞭解詳細資料。

備註 並非所有可能的 `pam_passwdqc` 選項組合都已經過測試。在變更預設密碼設定後，執行其他測試。

ESXi 帳戶鎖定行為

從 vSphere 6.0 開始，支援透過 SSH 和 vSphere Web Services SDK 存取帳戶鎖定。Direct Console 介面 (DCUI) 和 ESXi Shell 不支援帳戶鎖定。依預設，最多十次嘗試失敗後，帳戶即會鎖定。依預設，帳戶會在兩分鐘後解除鎖定。

設定登入行為

您可以使用以下進階選項來設定 ESXi 主機的登入行為：

- `Security.AccountLockFailures`。使用者帳戶鎖定前的嘗試登入失敗次數上限。設為零會停用帳戶鎖定。
- `Security.AccountUnlockTime`。使用者被鎖定的秒數。

請參閱 *vCenter Server 和主機管理* 說明文件瞭解有關設定 ESXi 進階選項的資訊。

SSH 安全性

您可以使用 SSH 遠端登入 ESXi Shell，並針對主機執行疑難排解工作。

ESXi 中的 SSH 組態得到了增強，能夠提供較高的安全性層級。

第 1 版 SSH 通訊協定已停用	VMware 不再支援第 1 版 SSH 通訊協定，而是以獨佔方式使用第 2 版通訊協定。第 2 版消除了第 1 版中存在的某些安全性問題，且提供了安全的方式來與管理介面進行通訊。
提高了加密強度	SSH 對連線僅支援 256 位元和 128 位元 AES 加密。

這些設定旨在為透過 SSH 傳輸到管理介面的資料提供可靠保護。您不能變更這些設定。

ESXi SSH 金鑰

SSH 金鑰可限制、控制以及保護 ESXi 主機的存取權。SSH 金鑰可以讓受信任的使用者或指令碼在未指定密碼的情況下登入主機。

您可以使用 `vifs` vSphere CLI 命令將 SSH 金鑰複製到主機。如需安裝和使用 vSphere CLI 命令集的資訊，請參閱《vSphere Command-Line Interface 入門》。您也可以使用 HTTPS PUT 將 SSK 金鑰複製到主機。

您可以在 ESXi 主機上建立金輪並將其下載，而不是在外部產生金鑰然後將其上傳。請參閱 VMware 知識庫文章 1002866。

啟用 SSH 並將 SSH 金鑰新增到主機具有固有風險。根據擁有受信任金鑰的使用者受到入侵的風險，來衡量公開使用者名稱和密碼的潛在風險。

備註 若是 ESXi 5.0 及更早版本，即使主機處於鎖定模式，擁有 SSH 金鑰的使用者也可以存取主機。從 ESXi 5.1 開始，擁有 SSH 金鑰的使用者無法再存取處於鎖定模式的主機。

使用 vifs 命令上傳 SSH 金鑰

如果您決定想要使用授權金鑰登入具有 SSH 的主機，則可以使用 `vifs` 命令上傳授權金鑰。

備註 由於授權金鑰允許 SSH 存取且無需使用者驗證，請審慎考量是否要在您的環境中使用 SSH 金鑰。

授權金鑰可讓您驗證對主機的遠端存取。當使用者或指令碼嘗試透過 SSH 存取主機時，無需密碼，金鑰也能提供驗證。透過授權金鑰，您可以自動進行驗證，這在撰寫用於執行常式工作的指令碼時非常有用。

可以將以下類型的 SSH 金鑰上傳到主機。

- 根使用者的授權金鑰檔案
- RSA 金鑰
- RSA 公開金鑰

從 vSphere 6.0 Update 2 版本開始，DSS/DSA 金鑰不再受支援。

重要事項 請勿修改 `/etc/ssh/sshd_config` 檔案。如果您這麼做，主機精靈 (`hostd`) 將對您所做的變更一無所知。

程序

- 在命令列或管理伺服器上，使用 `vifs` 命令將 SSH 金鑰上傳到 ESXi 主機上的適當位置。

```
vifs --server hostname --username username --put filename /host/ssh_host_dsa_key_pub
```

金鑰類型	位置
根使用者的授權金鑰檔案	`/host/ssh_root_authorized keys` 您必須具有完整管理員權限，才可上傳此檔案。
RSA 金鑰	`/host/ssh_host_rsa_key`
RSA 公開金鑰	`/host/ssh_host_rsa_key_pub`

使用 HTTPS PUT 上傳 SSH 金鑰

您可以使用授權金鑰登入具有 SSH 的主機。您可以使用 HTTPS PUT 上傳授權金鑰。

授權金鑰可讓您驗證對主機的遠端存取。當使用者或指令碼嘗試透過 SSH 存取主機時，無需密碼，金鑰也能提供驗證。透過授權金鑰，您可以自動進行驗證，這在撰寫用於執行常式工作的指令碼時非常有用。

您可以使用 HTTPS PUT 將以下類型的 SSH 金鑰上傳到主機：

- 根使用者的授權金鑰檔案
- DSA 金鑰
- DSA 公開金鑰
- RSA 金鑰
- RSA 公開金鑰

重要事項 請勿修改 `/etc/ssh/sshd_config` 檔案。

程序

1. 在上傳應用程式中，請開啟金鑰檔案。
2. 將檔案發佈到下列位置。

金鑰類型	位置
根使用者的授權金鑰檔案	`https://hostname_or_IP_address/host/ssh_root_authorized_keys` 您必須對主機具有完整的管理員權限才可上傳此檔案。
DSA 金鑰	`https://hostname_or_IP_address/host/ssh_host_dsa_key`
DSA 公開金鑰	`https://hostname_or_IP_address/host/ssh_host_dsa_key_pub`
RSA 金鑰	`https://hostname_or_IP_address/host/ssh_host_rsa_key`
RSA 公開金鑰	`https://hostname_or_IP_address/host/ssh_host_rsa_key_pub`

PCI 和 PCIe 裝置和 ESXi

使用 VMware DirectPath I/O 功能來將 PCI 或 PCIe 裝置傳遞至虛擬機器，會導致潛在的安全性漏洞。該漏洞可能由錯誤或惡意程式碼觸發，例如，在客體作業系統中以特殊權限模式執行的裝置驅動程式。業界標準的硬體和韌體目前沒有足夠的錯誤抑制支援來保護 ESXi 主機不受漏洞侵害。

僅當虛擬機器由受信任的實體擁有並管理時，才使用 PCI 或 PCIe 傳遞至該虛擬機器。您必須確保此實體不會嘗試損壞或入侵虛擬機器的主機。

在以下情形下您的主機可能或受到影響。

- 客體作業系統也許會產生無法復原的 PCI 或 PCIe 錯誤。這個錯誤不會損毀資料，但是可以損壞 ESXi 主機。此類錯誤可能由正在傳遞的硬體裝置中的錯誤或不相容問題導致。其他錯誤原因包含客體作業系統中的驅動程式問題。
- 客體作業系統可能會產生直接記憶體存取 (DMA) 作業，這將會導致 IOMMU 頁面在 ESXi 主機上出錯。此作業可能是由於 DMA 作業將虛擬機器記憶體之外的地址做為目標導致的。在部分機器上，主機韌體會設定 IOMMU 錯誤來報告通過非遮罩式插斷 (NMI) 出現的嚴重錯誤。這個錯誤會導致 ESXi 主機損毀。該問題可能由客體作業系統中的驅動程式問題導致。
- 如果 ESXi 主機上的作業系統沒有使用插斷重新對應，則客體作業系統可能插入一個偽插斷至 ESXi 主機的任何向量上。ESXi 目前在其可用的 Intel 平台上使用中斷重新對應，中斷對應是 Intel VT-d 功能集的一部分。ESXi 在 AMD 平台上沒有使用插斷對應。錯誤的插斷可能會導致 ESXi 主機損毀。理論上，應該有其他方式可利用這些錯誤的插斷。

停用受管理物件瀏覽器

受管理物件瀏覽器 (MOB) 提供了深入瞭解 VMkernel 物件模型的方式。但是，由於可以使用 MOB 變更主機組態，因此攻擊者能夠使用此介面來執行惡意的組態變更或動作。將 MOB 僅用於偵錯，並確保已在生產系統中停用。

從 vSphere 6.0 開始，MOB 預設為停用狀態。但對於某些工作，例如從系統中擷取舊憑證時，您必須使用 MOB。您可以按如下方式啟用和停用 MOB。

程序

1 在 vSphere Web Client 中選取主機，然後前往**進階系統設定**。

2 檢查 **Config.HostAgent.plugins.solo.enableMob** 的值，然後視需要變更該值。

請勿透過 ESXi Shell 使用 `vim-cmd`。

ESXi 網路安全性建議

隔離網路流量對於保護 ESXi 環境的安全至關重要。不同的網路需要不同的存取權和隔離層級。

您的 ESXi 主機使用多個網路。針對每個網路使用適當的安全措施，並隔離特定應用程式和功能的流量。例如，確保 VMware vSphere vMotion® 流量不透過虛擬機器所在的網路進行傳輸。隔離可防止窺探。出於效能原因，建議也將網路隔離。

- vSphere 基礎結構網路用於如 vSphere vMotion、VMware vSphere Fault Tolerance 和儲存區等功能。針對其特定功能，隔離這些網路。通常不必要傳送這些單一實體伺服器機架外的網路。
- 管理網路將用戶端流量、命令列介面 (CLI) 或 API 流量以及第三方軟體流量與其他流量隔離。此網路只能從系統、網路和安全管理員存取。使用跳躍方塊或虛擬私人網路 (VPN) 安全存取管理網路。嚴格控制此網路內的存取。
- 虛擬機器流量可以流經一或多個網路。您可以透過使用在虛擬網路控制器上設定防火牆規則的虛擬防火牆解決方案來增強虛擬機器的隔離。當虛擬機器在 vSphere 環境中的主機之間移轉時，這些設定也會隨著虛擬機器移動。

修改 ESXi Web 代理設定

修改 Web 代理設定時，需要考慮若干加密和使用者安全性準則。

備註 對主機目錄或驗證機制做出任何變更之後重新啟動主機程序。

- 不要設定使用密碼或複雜密碼的憑證。ESXi 不支援使用密碼或複雜密碼 (也稱為加密的金鑰) 的 Web Proxy。如果設定了需要密碼或複雜密碼的 Web Proxy，ESXi 程序將無法正確啟動。
- 為了支援對使用者名稱、密碼和封包進行加密，vSphere Web Services SDK 連線的 SSL 預設為啟用。如果要設定這些連線以使它們不對傳輸進行加密，請將連線從 HTTPS 切換至 HTTP 以針對 vSphere Web Services SDK 連線停用 SSL。

  僅當為這些用戶端建立了完全受信任的環境時才可考慮停用 SSL，在這樣的環境中，安裝有防火牆，而且與主機之間的傳輸是完全隔離的。停用 SSL 可提高效能，因為避免了執行加密所需的額外負荷。
- 為了防止誤用 ESXi 服務，大多數內部 ESXi 服務只能透過連接埠 443 (用於 HTTPS 傳輸的連接埠) 來存取。連接埠 443 可充當 ESXi 的反向 Proxy。透過 HTTP 歡迎分頁可看到 ESXi 上的服務清單，但如果未經適當授權，則無法直接存取儲存裝置介面卡服務。

  可對此組態進行變更，以便可透過 HTTP 連線直接存取個別服務。除非是在完全受信任的環境中使用 ESXi，否則不要進行此變更。
- 在升級您的環境時，憑證仍然保留在原位。

vSphere Auto Deploy 安全考量

使用 vSphere Auto Deploy 時，請注意網路安全性、開機映像安全性，並小心不要讓密碼因主機設定檔而曝光，以便保護您的環境。

網路安全性

保護您的網路，就如您針對任何其他 PXE 型部署方法來保護網路一樣。vSphere Auto Deploy 透過 SSL 傳輸資料，可防止意外干擾和窺探。但是，在 PXE 開機期間不會檢查用戶端或 Auto Deploy 伺服器的真實性。

透過完全隔離使用 Auto Deploy 的網路，您可以大幅降低 Auto Deploy 的安全性風險。

開機映像和主機設定檔安全性

vSphere Auto Deploy 伺服器下載到電腦上的開機映像可以具有以下元件。

- 開機映像中永遠包括組成映像設定檔的 VIB 套件。
- 如果 Auto Deploy 規則是設定為使用主機設定檔或主機自訂來佈建主機，則開機映像中便包含主機設定檔和主機自訂。
  - 主機設定檔和主機自訂隨附的管理員 (root) 密碼和使用者密碼皆已進行 MD5 加密。
  - 與設定檔相關聯的任何其他密碼均採用明文形式。如果使用主機設定檔設定 Active Directory，則密碼不受保護。

    請使用 vSphere Authentication Proxy 來避免公開 Active Directory 密碼。如果使用主機設定檔設定 Active Directory，則密碼不會受到保護。
- 主機的公開和私密 SSL 金鑰和憑證都包含在開機映像中。

控制以 CIM 為基礎的硬體監控工具的存取

一般資訊模型 (CIM) 系統提供了一個介面，使得使用一組標準 API 能夠從遠端應用程式進行硬體層級管理。若要確保 CIM 介面安全，請僅為這些遠端應用程式提供必需的最小存取權限。如果以根或管理員帳戶佈建遠端應用程式，當該應用程式受破壞時，虛擬環境就可能會受破壞。

CIM 是一種開放式標準，其所定義的架構用於 ESXi 主機硬體資源的無代理程式、以標準為基礎的監控作業。該架構由一個 CIM 物件管理器 (通常稱為 [CIM Broker]) 和一組 CIM 提供者組成。

CIM 提供者支援對裝置驅動程式和基礎硬體進行管理存取。硬體廠商 (包括伺服器製造商和硬體裝置廠商) 可以撰寫監控和管理其裝置的提供者。VMware 會撰寫監控伺服器硬體、ESXi 儲存區基礎結構及虛擬化專屬資源的提供者。這些提供者在 ESXi 主機內執行，為輕量型且側重於特定管理工作。CIM Broker 會從所有 CIM 提供者獲得資訊，並使用標準 API 呈現給外界。最常見的 API 是 WS-MAN。

請勿為存取 CIM 介面的遠端應用程式提供根認證。而是應為這些應用程式建立服務帳戶。為在 ESXi 系統中定義的所有本機帳戶和在 vCenter Server 中定義的所有角色授與對 CIM 資訊的唯讀存取權限。

程序

1. 建立 CIM 應用程式的服務帳戶。
2. 為該服務帳戶授與對收集 CIM 資訊之 ESXi 主機的唯讀存取權限。
3. (選擇性) 如果應用程式需要寫入權限，請建立僅擁有兩項權限的角色。
   - **主機.組態.系統管理**

- **主機.CIM.CIM 互動**

4 對於您要監控的每台 ESXi 主機，建立可將自訂角色與服務帳戶進行配對的權限。

請參閱使用角色指派權限。

ESXi 主機的憑證管理

在 vSphere 6.0 及更新版本中，VMware Certificate Authority (VMCA) 會使用已簽署憑證 (VMCA 預設做為根憑證授權機構) 來佈建每個新的 ESXi 主機。當主機明確新增至 vCenter Server，或在安裝或升級至 ESXi 6.0 或更新版本的過程中新增時，會執行佈建。

可以透過 vSphere Web Client 及使用 vSphere Web Services SDK 中的 `vim.CertificateManager` API 來檢視和管理 ESXi 憑證。您無法透過用於管理 vCenter Server 憑證的憑證管理 CLI 來檢視或管理 ESXi 憑證。

vSphere 5.5 和 vSphere 6.x 中的憑證

ESXi 和 vCenter Server 通訊時，會將 TLS/SSL 用於幾乎所有管理流量。

在 vSphere 5.5 及更早版本中，僅透過使用者名稱、密碼和指紋的組合來保護 TLS/SSL 端點的安全。使用者可以將對應的自我簽署憑證取代為自己的憑證。請參閱 vSphere 5.5 說明文件中心。

在 vSphere 6.0 及更新版本中，vCenter Server 支援 ESXi 主機的下列憑證模式。

表格 3-1. ESXi 主機的憑證模式

憑證模式	說明
VMware Certificate Authority (預設)	如果 VMCA 做為頂層 CA 或中繼 CA 佈建所有 ESXi 主機，則使用此模式。 依預設，VMCA 會使用憑證佈建 ESXi 主機。 在此模式下，您可以透過 vSphere Web Client 重新整理和更新憑證。
自訂憑證授權機構	若要僅使用由第三方或企業 CA 簽署的自訂憑證，請使用此模式。 在此模式下，您負責管理憑證。無法透過 vSphere Web Client 重新整理和更新憑證。 **備註** 除非您將憑證模式變更為自訂憑證授權機構，否則 VMCA 可能會取代自訂憑證，例如，當您在 vSphere Web Client 中選取**更新**時。
指紋模式	vSphere 5.5 使用的是指紋模式，此模式仍以 vSphere 6.x 之後援選項的形式提供。在此模式中，vCenter Server 會檢查憑證是否已正確格式化，但不會檢查憑證的有效性。即使憑證已到期亦可接受。 除非您使用其他兩種模式時遇到無法解決的問題，否則請勿使用此模式。在指紋模式下，vCenter 6.x 及更新版本的某些服務可能無法正常運作。

憑證到期

從 vSphere 6.0 開始，您可以在 vSphere Web Client 中檢視由 VMCA 或第三方 CA 簽署之憑證的憑證到期相關資訊。您可以檢視 vCenter Server 管理之所有主機或個別主機的資訊。如果憑證處於**即將到期**狀態 (少於 8 個月)，則會引發黃色警示。如果憑證處於**即將到期**狀態 (少於 2 個月)，則會引發紅色警示。

ESXi 佈建和 VMCA

當您從安裝媒體將 ESXi 主機開機時，該主機一開始會有自動產生的憑證。將主機新增至 vCenter Server 系統後，會使用由 VMCA 簽署做為根 CA 的憑證進行佈建。

此程序類似於使用 Auto Deploy 佈建的主機。但是，由於這些主機並未儲存任何狀態，因此，已簽署憑證由 Auto Deploy 伺服器儲存在本機憑證存放區中。後續將 ESXi 主機開機時，會重複使用該憑證。Auto Deploy 伺服器是任何內嵌式部署或 vCenter Server 系統的一部分。

如果 VMCA 在 Auto Deploy 主機首次開機時不可用，則主機會先嘗試連線。如果主機無法連線，則會循環關閉和重新開機，直到 VMCA 變為可用且能夠透過已簽署憑證佈建主機為止。

ESXi 憑證管理所需的權限

您必須具有 **憑證.管理憑證** 權限，才能管理 ESXi 主機的憑證。您可以從 vSphere Web Client 設定該權限。

主機名稱和 IP 位址變更

在 vSphere 6.0 及更新版本中，主機名稱或 IP 位址變更可能會影響 vCenter Server 是否將主機憑證視為有效。將主機新增至 vCenter Server 的方式會影響是否需要手動介入。手動介入是指重新連線主機，或將主機從 vCenter Server 移除然後再次新增。

表格 3-2. 主機名稱或 IP 位址變更何時需要手動介入

透過下列方式將主機新增至 vCenter Server...	主機名稱變更	IP 位址變更
主機名稱	vCenter Server 連線問題。需要手動介入。	不需要介入。
IP 位址	不需要介入。	vCenter Server 連線問題。需要手動介入。

ESXi 憑證管理 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_esxi_certs_in_vsphere)

主機升級和憑證

如果您將 ESXi 主機升級到 ESXi 6.0 或更新版本，升級程序會將自我簽署 (指紋) 的憑證取代為 VMCA 簽署的憑證。如果 ESXi 主機使用自訂憑證，則升級程序會保留這些憑證，即使這些憑證已過期或無效也如此。

如果決定不將主機升級到 ESXi 6.0 或更新版本，則主機會保留其目前所使用的憑證，即使該主機由使用 VMCA 憑證的 vCenter Server 系統管理也如此。

建議的升級工作流程取決於目前的憑證。

使用指紋憑證佈建的主機

如果您的主機目前使用指紋憑證，則在升級過程中，它會自動獲指派 VMCA 憑證。

備註 您無法使用 VMCA 憑證佈建舊版主機。您必須將這些主機升級至 ESXi 6.0 或更新版本。

使用自訂憑證佈建的主機

如果您的主機使用自訂憑證 (通常是第三方 CA 簽署的憑證) 佈建，則在升級期間這些憑證會保留在原位。將憑證模式變更為**自訂**，以確保在稍後的憑證重新整理期間憑證不會被意外取代。

備註 如果您的環境處於 VMCA 模式下，並且您從 vSphere Web Client 重新整理憑證，則任何現有憑證都會取代為 VMCA 簽署的憑證。

然後，vCenter Server 會監控憑證，並在 vSphere Web Client 中顯示諸如憑證到期等資訊。

使用 Auto Deploy 佈建的主機

由 Auto Deploy 佈建的主機首次以 ESXi 6.0 或更新版本的軟體開機時，將一律獲指派新憑證。在您升級由 Auto Deploy 佈建的主機時，Auto Deploy 伺服器會針對該主機產生憑證簽署要求 (CSR) 並將其提交給 VMCA。VMCA 會為該主機儲存已簽署的憑證。當 Auto Deploy 伺服器佈建主機時，它會從 VMCA 擷取憑證，並將其納入佈建程序。

您可以搭配使用 Auto Deploy 與自訂憑證。

請參閱搭配使用自訂憑證與 Auto Deploy。

憑證模式切換工作流程

從 vSphere 6.0 開始，ESXi 主機預設會佈建 VMCA 提供的憑證。您可以改用自訂憑證模式，或傳統的指紋模式 (用於偵錯目的)。大多數情況下，模式切換具有破壞性，且無需執行。如果您確實需要模式切換，請在開始前檢閱潛在的影響。

在 vSphere 6.0 及更新版本中，vCenter Server 支援 ESXi 主機的下列憑證模式。

憑證模式	說明
VMware Certificate Authority (預設)	依預設，VMware Certificate Authority 用作 ESXi 主機憑證的 CA。依預設，VMCA 為根 CA，但可將其設定為其他 CA 的媒介 CA。在此模式下，使用者可從 vSphere Web Client 管理憑證。VMCA 為下層憑證時也會使用。
自訂憑證授權機構	某些客戶可能偏好管理其自己的外部憑證授權機構。在此模式下，由客戶負責管理憑證，無法從 vSphere Web Client 管理憑證。
指紋模式	vSphere 5.5 使用的是指紋模式，此模式仍以 vSphere 6.0 之後援選項的形式提供。除非您使用其他兩種模式時遇到無法解決的問題，否則請勿使用此模式。在指紋模式下，vCenter 6.0 及更新版本的某些服務可能無法正常運作。

使用自訂 ESXi 憑證

如果公司原則要求您使用 VMCA 以外的根 CA，您可以在仔細規劃後於環境中切換憑證模式。建議的工作流程如下所示。

1 取得您想要使用的憑證。

2 將一或多個主機置於維護模式，並將其與 vCenter Server 中斷連線。

3 將自訂 CA 的根憑證新增到 VECS。

4 將自訂 CA 憑證部署到每部主機，然後在該主機上重新啟動服務。

5 切換為 [自訂 CA] 模式。請參閱變更憑證模式。

6 將一或多個主機連線到 vCenter Server 系統。

從自訂 CA 模式切換為 VMCA 模式

如果您目前使用自訂 CA 模式，並判定環境中使用 VMCA 會運作更佳，可在仔細規劃後執行模式切換。建議的工作流程如下所示。

1 從 vCenter Server 系統移除所有主機。

2 在 vCenter Server 系統上，從 VECS 移除第三方 CA 的根憑證。

3 切換為 VMCA 模式。請參閱變更憑證模式。

4 將主機新增到 vCenter Server 系統。

備註 此模式切換的任何其他工作流程可能會導致無法預期的行為。

保留升級期間的指紋模式憑證

如果使用 VMCA 憑證時遇到問題，則可能必須從 VMCA 模式切換為指紋模式。在指紋模式下，vCenter Server 系統僅會檢查憑證是否存在以及是否正確格式化，而不會檢查憑證是否有效。如需指示，請參閱變更憑證模式。

從指紋模式切換為 VMCA 模式

如果您使用指紋模式，並且想開始使用 VMCA 簽署的憑證，則切換工作需要進行一些規劃。建議的工作流程如下所示。

1 從 vCenter Server 系統移除所有主機。

2 切換為 VMCA 憑證模式。請參閱變更憑證模式。

3 將主機新增到 vCenter Server 系統。

備註 此模式切換的任何其他工作流程可能會導致無法預期的行為。

從自訂 CA 模式切換為指紋模式

如果您在使用自訂 CA 模式時遇到問題，請考量暫時切換為指紋模式。如果您依照變更憑證模式中的指示執行，切換工作將會順暢完成。模式切換後，vCenter Server 系統僅會檢查憑證的格式，而不再檢查憑證本身的有效性。

從指紋模式切換為自訂 CA 模式

如果您在疑難排解期間將環境設定為指紋模式，並且想要開始使用自訂 CA 模式，必須先產生所需的憑證。建議的工作流程如下所示。

1 從 vCenter Server 系統移除所有主機。

2 在 vCenter Server 系統上，將自訂 CA 根憑證新增到 VECS 上的 TRUSTED_ROOTS 存放區。請參閱更新 vCenter Server TRUSTED_ROOTS 存放區 (自訂憑證)。

3 針對每部 ESXi 主機：

   a 部署自訂 CA 憑證和金鑰。

   b 重新啟動主機上的服務。

4 切換為自訂模式。請參閱變更憑證模式。

5 將主機新增到 vCenter Server 系統。

ESXi 憑證預設設定

主機新增到 vCenter Server 系統時，vCenter Server 會將該主機的憑證簽署要求 (CSR) 傳送到 VMCA。大多數預設值適用於許多情況，但公司的專屬資訊會有所變更。

可以使用 vSphere Web Client 來變更許多預設設定。請考慮變更組織及位置資訊。請參閱變更憑證預設設定。

表格 3-3. ESXi CSR 設定

參數	預設值	進階選項
金鑰大小	2048	不適用
金鑰演算法	RSA	不適用
憑證簽章演算法	sha256WithRSAEncryption	不適用
一般名稱	主機的名稱，如果主機依主機名稱新增至 vCenter Server。 主機的 IP 位址，如果主機依 IP 位址新增至 vCenter Server。	不適用
國家/地區	USA	vpxd.certmgmt.certs.cn.country
電子郵件地址	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
位置 (城市)	Palo Alto	vpxd.certmgmt.certs.cn.localityName
組織單位名稱	VMware 工程	vpxd.certmgmt.certs.cn.organizationalUnitName
組織名稱	VMware	vpxd.certmgmt.certs.cn.organizationName

表格 3-3. ESXi CSR 設定 (繼續)

參數	預設值	進階選項
省/市或州	加利福尼亞	vpxd.certmgmt.certs.cn.state
憑證有效天數。	1825	vpxd.certmgmt.certs.cn.daysValid
憑證到期的硬臨界值。如果達到此臨界值，vCenter Server 會引發紅色警示。	30 天	vpxd.certmgmt.certs.cn.hardThreshold
vCenter Server 憑證有效性檢查的輪詢間隔。	5 天	vpxd.certmgmt.certs.cn.pollIntervalDays
憑證到期的軟臨界值。如果達到此臨界值，vCenter Server 會引發事件。	240 天	vpxd.certmgmt.certs.cn.softThreshold
vCenter Server 使用者用來判定是否已取代現有憑證的模式。變更此模式以在升級期間保留自訂憑證。請參閱主機升級和憑證。	預設值為 vmca 也可以指定指紋或自訂。請參閱變更憑證模式。	vpxd.certmgmt.mode

變更憑證預設設定

主機新增到 vCenter Server 系統時，vCenter Server 會將該主機的憑證簽署要求 (CSR) 傳送到 VMCA。您可以在 vSphere Web Client 中使用 vCenter Server 進階設定來變更 CSR 中的某些預設設定。

如需預設設定的清單，請參閱 ESXi 憑證預設設定。無法變更某些預設值。

程序

1 在 vSphere Web Client 中，選取管理主機的 vCenter Server 系統。

2 按一下**設定**，然後按一下**進階設定**。

3 在 [篩選器] 方塊中，輸入 **certmgmt** 以僅顯示憑證管理參數。

4 變更現有參數的值以遵循公司原則，然後按一下**確定**。

下一次新增主機到 vCenter Server 時，新設定將用於 vCenter Server 傳送至 VMCA 的 CSR 以及指派給主機的憑證。

下一個

對憑證中繼資料的變更僅影響新憑證。如果您想變更已由 vCenter Server 系統管理的主機憑證，您可以中斷連線，然後重新連線主機或更新憑證。

檢視多個 ESXi 主機的憑證到期資訊

如果使用的是 ESXi 6.0 及更新版本，則可以檢視受 vCenter Server 系統管理的所有主機的憑證狀態。顯示內容可讓您判定是否有任何憑證即將到期。

您可以在 vSphere Web Client 中檢視使用 VMCA 模式及使用自訂模式之主機的憑證狀態資訊。您無法檢視處於指紋模式下的主機的憑證狀態資訊。

程序

1 在 vSphere Web Client 詳細目錄階層中瀏覽到主機。

依預設，主機顯示內容不包括憑證狀態。

2 在 [名稱] 欄位上按一下滑鼠右鍵，然後選取**顯示/隱藏資料行**。

3 選取**憑證有效期至**，按一下**確定**，然後向右側捲動 (如有必要)。

當憑證到期時，系統會顯示憑證資訊。

如果將某主機新增至 vCenter Server，或者在其中斷連線後重新連線，並且狀態為 [已到期]、[臨近到期]、[即將到期] 或 [立即到期]，則 vCenter Server 會更新憑證。如果憑證有效期少於八個月，則狀態為 [臨近到期]；如果有效期少於兩個月，則狀態為 [即將到期]；如果有效期少於一個月，則狀態為 [立即到期]。

4 (選擇性) 取消選取其他資料行，以便更容易看到您所感興趣的內容。

下一個

更新即將到期的憑證。請參閱 更新或重新整理 ESXi 憑證。

檢視單一 ESXi 主機的憑證詳細資料

對於處於 VMCA 模式或自訂模式的 ESXi 6.0 及更新版本的主機，可以從 vSphere Web Client 檢視憑證詳細資料。憑證的相關資訊對於偵錯可能很有用。

程序

1 在 vSphere Web Client 詳細目錄中瀏覽到主機。

2 選取**設定**。

3 在**系統**下，按一下**憑證**。

您可以檢查下列資訊。此資訊僅在單一主機視圖中提供。

欄位	說明	
主題	憑證產生期間使用的主題。	
簽發者	憑證的簽發者。	
有效期自	產生憑證的日期。	
有效期至	憑證到期的日期。	
狀態	憑證的狀態，為下列其中之一。	
	良好	一般作業。
	到期	憑證即將到期。
	即將到期	憑證將在 8 個月內到期 (預設)。
	即將到期	憑證將在 2 個月內到期 (預設)。
	已到期	憑證無效，因為已到期。

更新或重新整理 ESXi 憑證

如果 VMCA 將憑證指派給 ESXi 主機 (6.0 及更新版本)，您可以從 vSphere Web Client 更新這些憑證。也可以從與 vCenter Server 相關聯的 TRUSTED_ROOTS 存放區重新整理所有憑證。

如果憑證即將到期，或者基於其他原因要使用新憑證佈建主機，則可以更新您的憑證。如果憑證已到期，則必須中斷主機連線，然後重新連線。

依預設，每次將主機新增至詳細目錄或重新連線時，vCenter Server 會更新狀態為 [已到期]、[立即到期] 或 [即將到期] 的主機憑證。

程序

1. 在 vSphere Web Client 詳細目錄中瀏覽到主機。
2. 選取**設定**。
3. 在**系統**下，按一下**憑證**。

   您可以檢視有關所選主機之憑證的詳細資訊。
4. 按一下**更新**或**重新整理 CA 憑證**。

選項	說明
更新	從 VMCA 為主機擷取全新的已簽署憑證。
重新整理 CA 憑證	將 TRUSTED_ROOTS 存放區 (位於 vCenter Server VECS 存放區中) 中的所有憑證推送到主機。

5. 按一下**是**進行確認。

變更憑證模式

使用 VMCA 佈建您環境中的 ESXi 主機，除非公司規則需要您使用自訂憑證。若要使用含不同根 CA 的自訂憑證，您可以編輯 vCenter Server `vpxd.certmgmt.mode` 進階選項。變更後，主機不會在您重新整理憑證時使用 VMCA 憑證自動進行佈建。您負責您環境中的憑證管理。

您可以使用 vCenter Server 進階設定，以變更為指紋模式或自訂 CA 模式。將指紋模式僅用作後援選項。

程序

1. 選取管理主機的 vCenter Server，然後按一下**設定**。
2. 按一下**進階設定**，然後按一下**編輯**。
3. 在 [篩選器] 方塊中，輸入 **`certmgmt`** 以僅顯示憑證管理金鑰。
4. 如果您打算管理自己的憑證，請將 `vpxd.certmgmt.mode` 的值變更為**自訂**；如果您想暫時使用指紋模式，則變更為**指紋**，然後按一下**確定**。
5. 重新啟動 vCenter Server 服務。

取代 ESXi SSL 憑證和金鑰

您公司的安全性原則，可能要求您在每台主機上將預設 ESXi SSL 憑證，取代為第三方 CA 簽署的憑證。

依預設，vSphere 元件所使用的 VMCA 簽署的憑證和金鑰，均是於安裝過程中所建立。如果意外刪除了 VMCA 簽署的憑證，請從其 vCenter Server 系統中移除主機，然後再重新新增該主機。當您新增主機時，vCenter Server 會從 VMCA 申請新憑證並使用該憑證佈建主機。

將 VMCA 簽署的憑證取代為由受信任的 CA (商業 CA 或組織 CA) 簽署的憑證 (如果公司原則需要)。

預設憑證與 vSphere 5.5 憑證均位於相同位置。您可以使用多種方式將預設憑證取代為受信任的憑證。

備註 在 vSphere Web Services SDK 中，您也可以使用 `vim.CertificateManager` 和 `vim.host.CertificateManager` 受管理物件。請參閱 vSphere Web Services SDK 說明文件。

取代憑證之後，您必須在管理主機的 vCenter Server 系統上，更新 VECS 中的 TRUSTED_ROOTS 存放區，以確保 vCenter Server 和 ESXi 主機具有信任關係。

如需有關針對 ESXi 主機使用 CA 簽署憑證的詳細指示，請參閱 VMware 知識庫文章 https://kb.vmware.com/s/article/2113926。

- ESXi 憑證簽署要求的需求

  如果您要使用企業或第三方 CA 簽署憑證，則必須將憑證簽署要求 (CSR) 傳送到 CA。
- 取代 ESXi Shell 中的預設憑證和金鑰

  您可以取代 ESXi Shell 中的預設 VMCA 簽署 ESXi 憑證。
- 使用 vifs 命令取代預設憑證和金鑰

  可以使用 `vifs` 命令取代預設的 VMCA 簽署的 ESXi 憑證。
- 使用 HTTPS PUT 取代預設憑證

  可以使用第三方應用程式上傳憑證和金鑰。支援 HTTPS PUT 作業的應用程式與 ESXi 包含的 HTTPS 介面搭配使用。
- 更新 vCenter Server TRUSTED_ROOTS 存放區 (自訂憑證)

  如果將 ESXi 主機設定為使用自訂憑證，則必須更新管理主機之 vCenter Server 系統上的 TRUSTED_ROOTS 存放區。

ESXi 憑證簽署要求的需求

如果您要使用企業或第三方 CA 簽署憑證，則必須將憑證簽署要求 (CSR) 傳送到 CA。

使用具有下列特性的 CSR：

- 金鑰大小：2048 位元或以上 (PEM 編碼)
- PEM 格式。VMware 支援 PKCS8 和 PKCS1 (RSA 金鑰)。金鑰新增到 VECS 之後，會轉換為 PKCS8
- x509 第 3 版
- 若為根憑證，CA 延伸必須設為 true，憑證簽署必須位於需求清單中。

- SubjectAltName 必須包含 DNS Name=<machine_FQDN>
- CRT 格式
- 包含下列金鑰使用方法：數位簽章、不可否認性、金鑰編密
- 某天的開始時間早於目前時間
- CN (和 SubjectAltName) 設為 ESXi 主機在 vCenter Server 詳細目錄中所擁有的主機名稱 (或 IP 位址)。

取代 ESXi Shell 中的預設憑證和金鑰

您可以取代 ESXi Shell 中的預設 VMCA 簽署 ESXi 憑證。

先決條件

- 若要使用第三方 CA 簽署憑證，請產生憑證要求，將其傳送至憑證授權機構，然後在每台 ESXi 主機上儲存憑證。
- 如果需要，可從 vSphere Web Client 啟用 ESXi Shell 或啟用 SSH 流量。
- 所有的檔案傳輸和其他通訊均透過安全 HTTPS 工作階段進行。用於驗證工作階段的使用者必須在主機上擁有**主機.設定.進階設定**權限。

程序

1. 以具有管理員權限的使用者身分登入 ESXi Shell，可直接從 DCUI 登入，也可從 SSH 用戶端登入。
2. 在目錄 `/etc/vmware/ssl` 中，使用以下命令重新命名現有憑證。

   ```
   mv rui.crt orig.rui.crt
   mv rui.key orig.rui.key
   ```

3. 將要使用的憑證複製到 `/etc/vmware/ssl`。
4. 將新憑證和金鑰重新命名為 `rui.crt` 和 `rui.key`。
5. 安裝新憑證之後重新啟動主機。

   或者，您可以將主機置於維護模式、安裝新憑證、使用 Direct Console 使用者介面 (DCUI) 重新啟動管理代理程式，然後將主機設定為結束維護模式。

下一個

更新 vCenter Server TRUSTED_ROOTS 存放區。

使用 vifs 命令取代預設憑證和金鑰

可以使用 `vifs` 命令取代預設的 VMCA 簽署的 ESXi 憑證。

您執行 `vifs` 做為 vCLI 命令。請參閱 *vSphere Command-Line Interface 入門*。

先決條件

- 若要使用第三方 CA 簽署憑證，請產生憑證要求，將其傳送至憑證授權機構，然後在每台 ESXi 主機上儲存憑證。
- 如果需要，可從 vSphere Web Client 啟用 ESXi Shell 或啟用 SSH 流量。
- 所有的檔案傳輸和其他通訊均透過安全 HTTPS 工作階段進行。用於驗證工作階段的使用者必須在主機上擁有**主機.設定.進階設定**權限。

程序

1. 備份現有憑證。
2. 按照憑證授權單位的指示產生憑證要求。

   請參閱 ESXi 憑證簽署要求的需求。
3. 如果您擁有此憑證，可以使用 `vifs` 命令透過主機的 SSH 連線將憑證上傳到主機上的適當位置。

   ```
   vifs --server hostname --username username --put rui.crt /host/ssl_cert
   ```

   ```
   vifs --server hostname --username username --put rui.key /host/ssl_key
   ```
4. 重新啟動主機。

下一個

更新 vCenter ServerTRUSTED_ROOTS 存放區。請參閱更新 vCenter Server TRUSTED_ROOTS 存放區 (自訂憑證)。

使用 HTTPS PUT 取代預設憑證

可以使用第三方應用程式上傳憑證和金鑰。支援 HTTPS PUT 作業的應用程式與 ESXi 包含的 HTTPS 介面搭配使用。

先決條件

- 若要使用第三方 CA 簽署憑證，請產生憑證要求，將其傳送至憑證授權機構，然後在每台 ESXi 主機上儲存憑證。
- 如果需要，可從 vSphere Web Client 啟用 ESXi Shell 或啟用 SSH 流量。
- 所有的檔案傳輸和其他通訊均透過安全 HTTPS 工作階段進行。用於驗證工作階段的使用者必須在主機上擁有**主機.設定.進階設定**權限。

程序

1. 備份現有憑證。

2 在您的上傳應用程式中，按如下方式處理每個檔案：

a 開啟檔案。

b 將檔案發佈到以下其中一個位置。

選項	說明
憑證	`https://hostname/host/ssl_cert`
金鑰	`https://hostname/host/ssl_key`

位置 `/host/ssl_cert` 和 `host/ssl_key` 會連結到`/etc/vmware/ssl` 中的憑證檔案。

3 重新啟動主機。

下一個

更新 vCenter Server TRUSTED_ROOTS 存放區。請參閱 更新 vCenter Server TRUSTED_ROOTS 存放區 (自訂憑證)。

更新 vCenter Server TRUSTED_ROOTS 存放區 (自訂憑證)

如果將 ESXi 主機設定為使用自訂憑證，則必須更新管理主機之 vCenter Server 系統上的 TRUSTED_ROOTS 存放區。

先決條件

將每台主機上的憑證取代為自訂憑證。

程序

1 登入管理 ESXi 主機的 vCenter Server 系統。

登入軟體安裝所在的 Windows 系統，或是登入 vCenter Server Appliance shell。

2 執行 `vecs-cli` 以將新憑證新增到 TRUSTED_ROOTS 存放區，例如：

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --
cert /etc/vmware/ssl/custom1.crt
```

選項	說明
Linux	`/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt -- cert /etc/vmware/ssl/custom1.crt`
Windows	`C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert c:\ssl\custom1.crt`

下一個

將憑證模式設定為 [自訂]。如果憑證模式為 VMCA (預設值)，當您執行憑證重新整理時，您的自訂憑證將會取代為 VMCA 簽署的憑證。請參閱變更憑證模式。

搭配使用自訂憑證與 Auto Deploy

依預設，Auto Deploy 伺服器會使用由 VMCA 簽署的憑證佈建每台主機。可以將 Auto Deploy 伺服器設定為使用不是 VMCA 簽署的自訂憑證佈建所有主機。在此案例中，Auto Deploy 伺服器會變為第三方 CA 的下層憑證授權機構。

先決條件

- 向 CA 要求憑證。憑證必須符合這些需求。
  - 金鑰大小：2048 位元或以上 (PEM 編碼)
  - PEM 格式。VMware 支援 PKCS8 和 PKCS1 (RSA 金鑰)。金鑰新增到 VECS 之後，會轉換為 PKCS8
  - x509 第 3 版
  - 若為根憑證，CA 延伸必須設為 true，憑證簽署必須位於需求清單中。
  - SubjectAltName 必須包含 DNS Name=<machine_FQDN>
  - CRT 格式
  - 包含下列金鑰使用方法：數位簽章、不可否認性、金鑰編密
  - 某天的開始時間早於目前時間
  - CN (和 SubjectAltName) 設為 ESXi 主機在 vCenter Server 詳細目錄中所擁有的主機名稱 (或 IP 位址)。
- 將憑證和金鑰檔案命名為 `rbd-ca.crt` 和 `rbd-ca.key`。

程序

1. 備份預設 ESXi 憑證。

   憑證位於 `/etc/vmware-rbd/ssl/`。

2. 從 vSphere Web Client，停止 Auto Deploy 服務。
   a. 選取**管理**，然後在**部署**下按一下**系統組態**。
   b. 按一下**服務**。
   c. 在您要停止的服務上按一下滑鼠右鍵，然後選取**停止**。
3. 在 Auto Deploy 服務執行的系統上，將 `/etc/vmware-rbd/ssl/` 中的 `rbd-ca.crt` 和 `rbd-ca.key` 取代為您的自訂憑證和金鑰檔案。

4 在執行 Auto Deploy 服務的系統上，更新 VECS 中的 TRUSTED_ROOTS 存放區以使用新憑證。

選項	說明

Windows	`cd C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe`
	`vecs-cli entry delete --store TRUSTED_ROOTS --alias rbd_cert`
	`vecs-cli entry create --store TRUSTED_ROOTS --alias rbd_cert`
	`--cert /etc/vmware-rbd/ssl/rbd-ca.crt`

Linux	`cd /usr/lib/vmware-vmafd/bin/vecs-cli`
	`vecs-cli entry delete --store TRUSTED_ROOTS --alias`
	`rbd_cert`
	`vecs-cli entry create --store TRUSTED_ROOTS --alias`
	`rbd_cert`
	`--cert /etc/vmware-rbd/ssl/rbd-ca.crt`

5 建立可包含 TRUSTED_ROOTS 中內容的 `castore.pem` 檔案，然後將該檔案放置在 `/etc/vmware-rbd/ssl/` 目錄中。

在自訂模式中，您負責維護此檔案。

6 將 vCenter Server 系統的 ESXi 憑證模式變更為**自訂**。

請參閱變更憑證模式。

7 重新啟動 vCenter Server 服務，然後啟動 Auto Deploy 服務。

下一次您佈建已設定為使用 Auto Deploy 的主機時，Auto Deploy 伺服器會產生憑證。Auto Deploy 伺服器使用您剛剛新增至 TRUSTED_ROOTS 存放區的根憑證。

備註 如果您在取代憑證後使用 Auto Deploy 時遇到問題，請參閱 VMware 知識庫文章 2000988。

還原 ESXi 憑證和金鑰檔案

透過使用 vSphere Web Services SDK 取代 ESXi 主機上的憑證時，先前的憑證和金鑰將附加到 `.bak` 檔案。您可以透過將資訊從 `.bak` 檔案移到目前憑證和金鑰檔案，來還原先前的憑證。

主機憑證和金鑰位於 `/etc/vmware/ssl/rui.crt` 和 `/etc/vmware/ssl/rui.key`。透過使用 vSphere Web Services SDK `vim.CertificateManager` 管理的物件取代主機憑證和金鑰時，先前的金鑰和憑證將附加到檔案 `/etc/vmware/ssl/rui.bak`。

備註 如果透過使用 HTTP PUT、`vifs` 或從 ESXi Shell 取代憑證，則現有憑證將不會附加到 `.bak` 檔案。

程序

1 在 ESXi 主機上，尋找檔案 `/etc/vmware/ssl/rui.bak`。

檔案的格式如下。

```
#
# Host private key and certificate backup from 2014-06-20 08:02:49.961
#
```

```
-----BEGIN PRIVATE KEY-----
previous key
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
previous cert
-----END CERTIFICATE-----
```

2 將從 -----BEGIN PRIVATE KEY----- 到 -----END PRIVATE KEY----- 的文字複製到 /etc/vmware/ssl/rui.key 檔案。

   包含 -----BEGIN PRIVATE KEY----- 和 -----END PRIVATE KEY-----。

3 將 -----BEGIN CERTIFICATE----- 和 -----END CERTIFICATE----- 之間的文字複製到 /etc/vmware/ssl/rui.crt 檔案。

   包含 -----BEGIN CERTIFICATE----- 和 -----END CERTIFICATE-----。

4 重新啟動主機或將 ssl_reset 事件傳送到使用金鑰的所有服務。

   ```
   for s in /etc/init.d/*; do $s | grep ssl_reset > /dev/null; if [ $?== 0 ]; then
   $s ssl_reset; fi; done
   ```

透過安全性設定檔自訂主機

您可以透過 vSphere Web Client 中提供的 [安全性設定檔] 面板來為您的主機自訂多種基本的安全性設定。安全性設定檔對單一主機管理尤其有用。如果您要管理多台主機，請考慮使用 CLI 或 SDK 的其中一種，並考慮對自訂作業進行自動化。

ESXi 防火牆組態

ESXi 包含預設為啟用的防火牆。

在安裝時，ESXi 防火牆會設定為封鎖傳入和傳出流量 (主機安全性設定檔中已啟用之服務的流量除外)。

開啟防火牆上的連接埠時，請考慮不受限制地存取 ESXi 主機上執行的服務，會使主機遭受外部攻擊和未經授權的存取。將 ESXi 防火牆設定為僅允許從授權網路進行存取，可降低風險。

備註 防火牆還允許網際網路控制訊息通訊協定 (ICMP) Ping 及與 DHCP 和 DNS (僅 UDP) 用戶端的通訊。

您可以管理 ESXi 防火牆連接埠，說明如下：

- 在 vSphere Web Client 中為每部主機使用安全性設定檔。請參閱管理 ESXi 防火牆設定
- 從命令列或在指令碼中使用 ESXCLI 命令。請參閱 ESXi ESXCLI 防火牆命令。
- 如果要開啟的連接埠不在安全性設定檔中，請使用自訂 VIB。

使用 VMware Labs 中提供的 vibauthor 工具建立自訂 VIB。若要安裝自訂 VIB，您必須將 ESXi 主機的接受層級變更為 CommunitySupported。請參閱 VMware 知識庫文章 2007381。

備註 如果透過 VMware 技術支援調查安裝 CommunitySupported VIB 的 ESXi 主機上的問題，VMware 支援可能會要求執行疑難排解步驟，解除安裝此 CommunitySupported VIB，以判定該 VIB 是否與正在調查的問題相關。

ESXi 防火牆概念 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_esxi_firewall_concepts)

NFS 用戶端規則集 (`nfsClient`) 的行為與其他規則集不同。啟用 NFS 用戶端規則集後，會為允許的 IP 位址清單中的目的地主機開啟所有輸出 TCP 連接埠。如需詳細資訊，請參閱 NFS 用戶端防火牆行為。

管理 ESXi 防火牆設定

您可以從 vSphere Web Client 或命令列，為服務或管理代理程式設定傳入和傳出防火牆連線。

備註 如果不同的服務具有重疊的連接埠規則，則啟用一項服務時可能會隱式啟用其他服務。您可以指定允許存取主機上每個服務的 IP 位址，以避免發生此問題。

程序

1. 在 vSphere Web Client 詳細目錄中瀏覽到主機。
2. 按一下**設定**。
3. 在 [系統] 下，按一下**安全性設定檔**。

   vSphere Web Client 將顯示相應防火牆連接埠的作用中傳入和傳出連線清單。
4. 在 [防火牆] 區段中，按一下**編輯**。

   顯示器顯示了防火牆規則集，其中包括規則名稱及相關聯的資訊。
5. 選取要啟用的規則集，或取消選取要停用的規則集。

欄	說明
傳入連接埠和傳出連接埠	vSphere Web Client 針對服務開啟的連接埠
通訊協定	服務使用的通訊協定。
精靈	與服務相關聯的精靈狀態

6. 針對某些服務，您可以管理服務詳細資料。
   - 使用**開始**、**停止**或**重新啟動**按鈕，暫時變更服務狀態。
   - 變更啟動原則，讓服務根據主機或連接埠使用情況啟動。
7. 對於某些服務，您可以明確指定允許用以連線的 IP 位址。

   請參閱為 ESXi 主機新增允許的 IP 位址。
8. 按一下**確定**。

為 ESXi 主機新增允許的 IP 位址

依預設，每項服務的防火牆均允許存取所有 IP 位址。若要限制流量，請變更每項服務，以僅允許來自您的管理子網路的流量。如果您的環境不使用某些服務，您亦可取消選取這些服務。

可以使用 vSphere Web Client、vCLI 或 PowerCLI 更新服務的 [允許的 IP 位址] 清單。預設為允許服務的所有 IP 位址。此工作說明如何使用 vSphere Web Client。如需使用 vCLI 的指示，請參閱《*vSphere Command-Line Interface 概念和範例*》中有關管理防火牆的主題，網址為 https://code.vmware.com/。

將允許的 IP 位址新增到 ESXi 防火牆 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_adding_allowed_IP_to_esxi_firewall)

程序

1. 在 vSphere Web Client 詳細目錄中瀏覽到主機。
2. 按一下**設定**。
3. 在 [系統] 下，按一下**安全性設定檔**。
4. 在 [防火牆] 區段中，按一下**編輯**，然後從清單中選取服務。
5. 在 [允許的 IP 位址] 區段中，取消選取**允許從任何 IP 位址連線**，然後輸入允許連線到主機之網路的 IP 位址。

   使用逗點分隔 IP 位址。可以使用以下位址格式：

   - 192.168.0.0/24
   - 192.168.1.2, 2001::1/64
   - fd3e:29a6:0a81:e478::/64
6. 按一下**確定**。

ESXi 主機的傳入和傳出防火牆連接埠

vSphere Web Client 和 VMware Host Client 可讓您開啟和關閉每項服務的防火牆連接埠，或允許來自所選 IP 位址的流量。

下表列出了依預設安裝的服務的防火牆。如果您在主機上安裝其他 VIB，則其他服務和防火牆連接埠可能會可用。資訊主要是關於 vSphere Web Client 中可見的服務，但資料表還包含了一些其他連接埠。

表格 3-4. 傳入防火牆連線

連接埠	通訊協定	服務	說明
5988	TCP	CIM 伺服器	適用於 CIM (通用訊息模型) 的伺服器。
5989	TCP	CIM 安全伺服器	適用於 CIM 的安全伺服器。
427	TCP、UDP	CIM SLP	CIM 用戶端使用服務位置通訊協定第 2 版 (SLPv2) 尋找 CIM 伺服器。
546		DHCPv6	適用於 IPv6 的 DHCP 用戶端。

表格 3-4. 傳入防火牆連線 (繼續)

連接埠	通訊協定	服務	說明
8301, 8302	UDP	DVSSync	DVSSync 連接埠用於在已啟用 VMware FT 記錄/重新執行功能的主機之間同步分散式虛擬連接埠的狀態。只有執行主要或備份虛擬機器的主機才需要開啟這些連接埠。未使用 VMware FT 的主機則無需開啟這些連接埠。
902	TCP	NFC	網路檔案複製 (NFC) 可為 vSphere 元件提供檔案類型感知 FTP 服務。依預設，ESXi 將 NFC 用於在資料存放區之間複製和移動資料等作業。
12345, 23451	UDP	vSAN 叢集服務	VMware vSAN 叢集監控和成員資格目錄服務。使用以 UDP 為基礎的 IP 多點傳播來建立叢集成員並將 vSAN 中繼資料散佈至所有叢集成員。如果停用，vSAN 無法運作。
68	UDP	DHCP 用戶端	適用於 IPv4 的 DHCP 用戶端。
53	UDP	DNS 用戶端	DNS 用戶端。
8200, 8100, 8300	TCP、UDP	Fault Tolerance	主機之間用於 vSphere Fault Tolerance (FT) 的流量。
6999	UDP	NSX 分散式邏輯路由器服務	NSX 虛擬分散式路由器服務。安裝 NSX VIB 並建立 VDR 模組後，會開啟與此服務相關聯的防火牆連接埠。如果沒有與主機相關聯的 VDR 執行個體，則無需開啟此連接埠。 在舊版產品中，此服務稱為 NSX 分散式邏輯路由器。
2233	TCP	vSAN 傳輸	vSAN 可靠的資料包傳輸。此服務使用 TCP，且用於 vSAN Storage I/O。如果停用，vSAN 無法運作。
161	UDP	SNMP 伺服器	允許主機連線到 SNMP 伺服器。
22	TCP	SSH 伺服器	執行 SSH 存取時需要。
8000	TCP	vMotion	透過 vMotion 移轉虛擬機器時需要。ESXi 主機在來自遠端 ESXi 主機的 TCP 連線的連接埠 8000 上接聽 vMotion 流量。
902, 443	TCP	vSphere Web Client	用戶端連線
8080	TCP	vsanvp	vSAN VASA 廠商提供者。供屬於 vCenter 的儲存區管理服務 (SMS) 使用，以存取 vSAN 儲存區設定檔、功能和符合性的相關資訊。如果已停用，vSAN 儲存區設定檔型管理 (SPBM) 將無法運作。
80	TCP	vSphere Web Access	[歡迎] 頁面，包含不同介面的下載連結。
5900-5964	TCP	RFB 通訊協定	
80, 9000	TCP	vSphere Update Manager	

表格 3-5. 傳出防火牆連線

連接埠	通訊協定	服務	說明
427	TCP、UDP	CIM SLP	CIM 用戶端使用服務位置通訊協定第 2 版 (SLPv2) 尋找 CIM 伺服器。
547	TCP、UDP	DHCPv6	適用於 IPv6 的 DHCP 用戶端。

表格 3-5. 傳出防火牆連線 (繼續)

連接埠	通訊協定	服務	說明
8301, 8302	UDP	DVSSync	DVSSync 連接埠用於在已啟用 VMware FT 記錄/重新執行功能的主機之間同步分散式虛擬連接埠的狀態。只有執行主要或備份虛擬機器的主機才需要開啟這些連接埠。未使用 VMware FT 的主機則無需開啟這些連接埠。
44046, 31031	TCP	HBR	由 vSphere Replication 和 VMware Site Recovery Manager 用於目前的複寫流量。
902	TCP	NFC	網路檔案複製 (NFC) 可為 vSphere 元件提供檔案類型感知 FTP 服務。依預設，ESXi 將 NFC 用於在資料存放區之間複製和移動資料等作業。
9	UDP	WOL	透過網路喚醒使用。
12345 23451	UDP	vSAN 叢集服務	由 vSAN 使用的叢集監控、成員資格和目錄服務。
68	UDP	DHCP 用戶端	DHCP 用戶端。
53	TCP、UDP	DNS 用戶端	DNS 用戶端。
80, 8200, 8100, 8300	TCP、UDP	Fault Tolerance	支援 VMware Fault Tolerance。
3260	TCP	軟體 iSCSI 用戶端	支援軟體 iSCSI。
6999	UDP	NSX 分散式邏輯路由器服務	安裝 NSX VIB 並建立 VDR 模組後，會開啟與此服務相關聯的防火牆連接埠。如果沒有與主機相關聯的 VDR 執行個體，則無需開啟此連接埠。
5671	TCP	rabbitmqproxy	ESXi 主機上執行的 Proxy。此 Proxy 可讓虛擬機器內部執行的應用程式與 vCenter 網路網域中執行的 AMQP 代理進行通訊。 虛擬機器不一定要在網路中，即無需 NIC。確保傳出連線 IP 位址至少包含正在使用或以後使用的代理。您可以稍後按比例新增代理。
2233	TCP	vSAN 傳輸	用於 vSAN 節點之間的 RDT 流量 (單點傳播對等通訊)。
8000	TCP	vMotion	透過 vMotion 移轉虛擬機器時需要。
902	UDP	VMware vCenter Agent	vCenter Server 代理程式。
8080	TCP	vsanvp	用於 vSAN 廠商提供者流量。
9080	TCP	I/O 篩選器服務	由 I/O 篩選器儲存功能使用

表格 3-6. 依預設在 UI 中不可見的服務的防火牆連接埠

連接埠	通訊協定	服務	註解
5900-5964	TCP	RFB 通訊協定	RFB 通訊協定是適用於圖形式使用者介面的遠端存取的簡單通訊協定。
8889	TCP	OpenWSMAN 精靈	Web 服務管理 (WS-Management 是管理伺服器、裝置、應用程式和 Web 服務的 DMTF 開放式標準。

NFS 用戶端防火牆行為

NFS 用戶端防火牆規則集的行為方式與其他 ESXi 防火牆規則集不同。掛接或卸載 NFS 資料存放區時，ESXi 將設定 NFS 用戶端設定。不同 NFS 版本的行為有所不同。

新增、掛接或卸載 NFS 資料存放區時，所產生的行為取決於 NFS 的版本。

NFS v3 防火牆行為

新增或掛接 NFS v3 資料存放區時，ESXi 會檢查 NFS 用戶端 (`nfsClient`) 防火牆規則集的狀態。

- 如果已停用 `nfsClient` 規則集，則 ESXi 會啟用規則集，並透過將 `allowedAll` 旗標設定為 `FALSE` 來停用「允許所有 IP 位址」原則。NFS 伺服器的 IP 位址將新增到允許的傳出 IP 位址清單中。
- 如果已啟用 `nfsClient` 規則集，則規則集狀態和允許的 IP 位址原則不會變更。NFS 伺服器的 IP 位址將新增到允許的傳出 IP 位址清單中。

備註 如果手動啟用 `nfsClient` 規則集或手動設定「允許所有 IP 位址」原則，不論在 NFS v3 資料存放區新增到系統之前或之後，卸載最新 NFS v3 資料存放區時都將覆寫您的設定。卸載所有 NFS v3 資料存放區後，將停用 `nfsClient` 規則集。

移除或卸載 NFS v3 資料存放區時，ESXi 會執行下列其中一個動作。

- 如果剩餘的 NFS v3 資料存放區都沒有從正在卸載之資料存放區的伺服器進行掛接，則 ESXi 將從傳出 IP 位址清單中移除該伺服器的 IP 位址。
- 如果在卸載作業後沒有保留任何已掛接的 NFS v3 資料存放區，則 ESXi 會停用 `nfsClient` 防火牆規則集。

NFS v4.1 防火牆行為

當您掛接第一個 NFS v4.1 資料存放區時，ESXi 會啟用 `nfs41client` 規則集並將其 `allowedAll` 旗標設定為 TRUE。此動作將針對所有 IP 位址開啟連接埠 2049。卸載 NFS v4.1 資料存放區不會影響防火牆狀態。即，第一個 NFS v4.1 掛接會開啟連接埠 2049，且該連接埠會保持啟用狀態，除非您明確將其關閉。

ESXi ESXCLI 防火牆命令

如果您的環境包含多台 ESXi 主機，建議使用 ESXCLI 命令或 vSphere Web Services SDK 自動化防火牆組態。

防火牆命令參考

可以使用 ESXi Shell 或 vSphere CLI 命令，在命令列設定 ESXi 以自動化防火牆組態。請分別參閱 *vSphere Command-Line Interface 入門*和《*vSphere Command-Line Interface 概念和範例*》以瞭解相關簡介和使用 ESXCLI 操縱防火牆和防火牆規則的範例。如需建立自訂防火牆規則的相關資訊，請參閱 VMware 知識庫文章 2008226。

表格 3-7. 防火牆命令

命令	說明
`esxcli network firewall get`	傳回防火牆的啟用或停用狀態，並列出預設動作。
`esxcli network firewall set --default-action`	設定為 true 可設定要傳遞的預設動作。設定為 false 可設定要捨棄的預設動作。
`esxcli network firewall set --enabled`	啟用或停用 ESXi 防火牆。
`esxcli network firewall load`	載入防火牆模組和規則集組態檔。
`esxcli network firewall refresh`	如果已載入防火牆模組，則透過讀取規則集檔案來重新整理防火牆組態。
`esxcli network firewall unload`	損毀篩選器並卸載防火牆模組。
`esxcli network firewall ruleset list`	列出規則集資訊。
`esxcli network firewall ruleset set --allowed-all`	設定為 true 允許對所有 IP 具有完全存取權。設定為 false 可使用已允許的 IP 位址清單。
`esxcli network firewall ruleset set --enabled --ruleset-id=<string>`	將 enabled 設定為 true 可啟用指定規則集。將 enabled 設定為 false 可停用指定規則集。
`esxcli network firewall ruleset allowedip list`	列出指定規則集的允許 IP 位址。
`esxcli network firewall ruleset allowedip add`	允許從指定的 IP 位址或 IP 位址範圍存取規則集。
`esxcli network firewall ruleset allowedip remove`	從指定的 IP 位址或 IP 位址範圍移除對規則集的存取權。
`esxcli network firewall ruleset rule list`	列出防火牆中每個規則集的規則。

防火牆命令範例

下列範例來自 virtuallyGhetto 上的部落格文章。

1 驗證名為 virtuallyGhetto 的新規則集。

```
esxcli network firewall ruleset rule list | grep virtuallyGhetto
```

2 指定特定 IP 位址或 IP 範圍，以存取特定服務。下列範例停用 `allow all` 選項，並指定 virtuallyGhetto 服務的特定範圍。

```
esxcli network firewall ruleset set --allowed-all false --ruleset-id=virtuallyGhetto
esxcli network firewall ruleset allowedip add --ip-address=172.30.0.0/24 --ruleset-
id=virtuallyGhetto
```

透過安全性設定檔自訂 ESXi 服務

ESXi 主機包含數個依預設會執行的服務。您可以從安全性設定檔停用服務，或在公司原則允許時啟用服務。

使用 vSphere Web Client 啟用對 ESXi Shell 的存取是如何啟用服務的範例。

備註 啟用服務會影響主機的安全性。請勿啟用服務，除非完全必要。

可用服務視 ESXi 主機上安裝的 VIB 而定。不安裝 VIB，您將無法新增服務。一些 VMware 產品 (例如 vSphere HA) 在主機上安裝 VIB，使服務和對應的防火牆連接埠可用。

在預設安裝中，您可以從 vSphere Web Client 修改下列服務的狀態。

表格 3-8. 安全性設定檔中的 ESXi 服務

服務	預設值	說明
Direct Console UI	執行中	Direct Console 使用者介面 (DCUI) 服務允許您使用文字型功能表從本機主控台與 ESXi 主機進行互動。
ESXi Shell	已停止	ESXi Shell 可從 Direct Console 使用者介面取得，且包括一組完全支援的命令和一組用於疑難排解和修復的命令。您必須啟用從每個系統的 Direct Console 存取 ESXi Shell。您可以啟用存取本機 ESXi Shell 或透過 SSH 存取 ESXi Shell。
SSH	已停止	主機的 SSH 用戶端服務，允許透過安全殼層遠端連線。
以負載為基礎的整併精靈	執行中	以負載為基礎的整併。
Active Directory 服務	已停止	當您針對 Active Directory 設定 ESXi 時，此服務即啟動。
NTP 精靈	已停止	網路時間通訊協定精靈。
PC/SC 智慧卡精靈	已停止	啟用主機以進行智慧卡驗證時，將啟動此服務。請參閱設定用於 ESXi 的智慧卡驗證。
CIM 伺服器	執行中	可由通用訊息模型 (CIM) 應用程式使用的服務。
SNMP 伺服器	已停止	SNMP 精靈。如需有關設定 SNMP v1、v2 和 v3 的資訊，請參閱 *vSphere 監控和效能*。
Syslog 伺服器	已停止	Syslog 精靈。您可以在 vSphere Web Client 中從 [進階系統設定] 啟用 Syslog。請參閱 *vCenter Server 安裝和設定*。
VMware vCenter Agent	執行中	vCenter Server 代理程式。允許 vCenter Server 連線到 ESXi 主機。具體來說，vpxa 是主機精靈的通訊媒介，轉而與 ESXi 核心通訊。
X.Org 伺服器	已停止	X.Org 伺服器。針對虛擬機器，此選用功能僅內部用於 3D 圖形。

啟用或停用安全性設定檔中的服務

您可以從 vSphere Web Client 啟用或停用安全性設定檔中所列的其中一種服務。

安裝完成後，某些服務依預設處於執行中，而其他服務則會停止。在某些情況下，需要進行一些其他設定，服務才可用於 vSphere Web Client UI。例如，NTP 服務是取得準確時間資訊的一種方式，但此服務僅在防火牆中已開啟所需連接埠時運作。

先決條件

透過 vSphere Web Client 連線到 vCenter Server。

程序

1 在 vSphere Web Client 詳細目錄中瀏覽到主機，然後選取主機。

2 按一下**設定**。

3 在 [系統] 下，選取**安全性設定檔**，然後按一下**編輯**。

4 捲動到您要變更的服務。

5 在 [服務詳細資料] 窗格中，選取**啟動**、**停止**或**重新啟動**以對主機狀態進行一次性變更，或者從**啟動原則**功能表選取，以在重新開機過程中變更主機的狀態。

- **任一連接埠開啟時自動啟動，所有連接埠均關閉時停止**：這些服務的預設設定。如果任一連接埠開啟，則用戶端會嘗試連絡服務的網路資源。如果某些連接埠已開啟，而特定服務的連接埠卻關閉，則該嘗試將失敗。適用的傳出連接埠開啟時，此服務將開始完成其啟動。
- **隨主機一起啟動和停止**：服務在主機啟動後立即啟動，並在主機關閉之前不久關閉。此選項與**任一連接埠開啟時自動啟動，所有連接埠均關閉時停止**非常相似，都表示此服務會定期嘗試完成其工作，例如嘗試連絡指定的 NTP 伺服器。如果連接埠先是處於關閉狀態，但隨後又開啟，用戶端將在此後不久開始完成其工作。
- **手動啟動和停止**：無論連接埠開啟與否，主機都會保留使用者決定的服務設定。使用者啟動 NTP 服務後，只要主機電源開啟，該服務會一直執行。如果服務已啟動且主機已關閉，該服務將在關閉過程中停止，但是一旦主機電源開啟，該服務將再次啟動，保留使用者決定的狀態。

備註 這些設定僅適用於透過 vSphere Web Client 設定的服務設定，或使用 vSphere Web Services SDK 建立的應用程式。這些設定不會影響透過其他方式 (如 ESXi Shell) 或組態檔設定的組態。

鎖定模式

若要提高 ESXi 主機的安全性，您可以將主機置於鎖定模式。在鎖定模式下，依預設所有作業都必須透過 vCenter Server 執行。

從 vSphere 6.0 開始，您可以選取一般鎖定模式或嚴格鎖定模式，這兩者可提供不同的鎖定程度。vSphere 6.0 還推出了 [例外使用者] 清單。當主機進入鎖定模式時，例外使用者不會遺失他們的權限。主機處於鎖定模式時，使用 [例外使用者] 清單來新增需要直接存取主機之第三方解決方案和外部應用程式的帳戶。請參閱指定鎖定模式例外使用者。

vSphere 6 中的鎖定模式 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_lockdown_mode_vsphere)

鎖定模式行為

在鎖定模式下，部分服務會停用，而部分服務僅供特定使用者存取。

適用於不同使用者的鎖定模式服務

當主機執行時，可用服務取決於是否已啟用鎖定模式，以及鎖定模式的類型。

- 在嚴格及一般鎖定模式下，授權使用者可透過 vCenter Server、從 vSphere Web Client，或透過使用 vSphere Web Services SDK 來存取主機。
- Direct Console 介面行為針對嚴格鎖定模式和一般鎖定模式有所不同。
  - 在嚴格鎖定模式下，Direct Console 使用者介面 (DCUI) 服務會停用。

  - 在一般鎖定模式下，如果 [例外使用者] 清單上的帳戶擁有管理員權限，則可以存取 DCUI。此外，在 DCUI.Access 進階系統設定中指定的所有使用者都可存取 DCUI。
- 如果 ESXi Shell 或 SSH 已啟用，而主機處於鎖定模式下，則 [例外使用者] 清單中具有管理員權限的帳戶均可使用這些服務。對於所有其他使用者，ESXi Shell 或 SSH 存取會停用。從 vSphere 6.0 開始，針對無管理員權限之使用者的 ESXi 或 SSH 工作階段均會終止。

嚴格及一般鎖定模式下的所有存取均會得到記錄。

表格 3-9. 鎖定模式行為

服務	一般模式	一般鎖定模式	嚴格鎖定模式
vSphere Web Services API	所有使用者，根據權限	vCenter (vpxuser) 例外使用者，根據權限 vCloud Director (如果可用，則為 vslauser)	vCenter (vpxuser) 例外使用者，根據權限 vCloud Director (如果可用，則為 vslauser)
CIM 提供者	主機上具有管理員權限的使用者	vCenter (vpxuser) 例外使用者，根據權限。 vCloud Director (如果可用，則為 vslauser)	vCenter (vpxuser) 例外使用者，根據權限。 vCloud Director (如果可用，則為 vslauser)
Direct Console UI (DCUI)	主機上具有管理員權限的使用者，以及 DCUI.Access 進階選項中的使用者	在 DCUI.Access 進階選項中定義的使用者 主機上具有管理員權限的例外使用者	DCUI 服務已停止
ESXi Shell (如果啟用)	主機上具有管理員權限的使用者	在 DCUI.Access 進階選項中定義的使用者 主機上具有管理員權限的例外使用者	在 DCUI.Access 進階選項中定義的使用者 主機上具有管理員權限的例外使用者
SSH (如果啟用)	主機上具有管理員權限的使用者	在 DCUI.Access 進階選項中定義的使用者 主機上具有管理員權限的例外使用者	在 DCUI.Access 進階選項中定義的使用者 主機上具有管理員權限的例外使用者

啟用鎖定模式時登入 ESXi Shell 的使用者

使用者可能會登入 ESXi Shell，或透過 SSH 存取主機，然後鎖定模式才會啟用。在此情況下，位於 [例外使用者] 清單中且在主機上具有管理員權限的使用者會保持登入狀態。從 vSphere 6.0 開始，該工作階段會對所有其他使用者終止。此終止同時適用於一般及嚴格鎖定模式。

使用 vSphere Web Client 啟用鎖定模式

啟用鎖定模式，以要求所有組態變更均透過 vCenter Server 進行。vSphere 6.0 及更新版本支援一般鎖定模式和嚴格鎖定模式。

如果您想要完全禁止所有對主機的直接存取，您可以選取嚴格鎖定模式。在嚴格鎖定模式下，如果 vCenter Server 不可用，且 SSH 和 ESXi Shell 已停用，則無法存取主機。請參閱鎖定模式行為。

程序

1 在 vSphere Web Client 詳細目錄中瀏覽到主機。

2 按一下**設定**。

3 在 [系統] 下，選取**安全性設定檔**。

4 在 [鎖定模式] 面板中，按一下**編輯**。

5 按一下**鎖定模式**，然後選取其中一個鎖定模式選項。

選項	說明
正常	主機可透過 vCenter Server 存取。只有「例外使用者」清單中具有管理員權限的使用者才能登入 Direct Console 使用者介面。如果已啟用 SSH 或 ESXi Shell，才有可能進行存取。
嚴格	主機僅可透過 vCenter Server 存取。如果已啟用 SSH 或 ESXi Shell，則會保持執行 DCUI.Access 進階選項中的帳戶和具有管理員權限的例外使用者帳戶的工作階段。所有其他工作階段均會終止。

6 按一下**確定**。

使用 vSphere Web Client 停用鎖定模式

停用鎖定模式，以便使組態從直接連線變更為 ESXi 主機。保持啟用鎖定模式會實現更安全的環境。

在 vSphere 6.0 中，您可以按照以下方式停用鎖定模式：

從 vSphere Web Client 中	使用者可以從 vSphere Web Client 中停用一般鎖定模式和嚴格鎖定模式。
從 Direct Console 使用者介面中	若使用者能在 ESXi 主機上存取 Direct Console 使用者介面，即可停用一般鎖定模式。在嚴格鎖定模式下，Direct Console 介面服務會停止。

程序

1 在 vSphere Web Client 詳細目錄中瀏覽到主機。

2 按一下**設定**。

3 在 [系統] 下，選取**安全性設定檔**。

4 在 [鎖定模式] 面板中，按一下**編輯**。

5 按一下**鎖定模式**，然後選取**已停用**來停用鎖定模式。

系統會結束鎖定模式，vCenter Server 會顯示警示，並在稽核記錄中新增一個項目。

從 Direct Console 使用者介面啟用或停用一般鎖定模式

您可以從 Direct Console 使用者介面 (DCUI) 啟用和停用一般鎖定模式。您只能從 vSphere Web Client 啟用和停用嚴格鎖定模式。

當主機處於一般鎖定模式時，下列帳戶可存取 Direct Console 使用者介面：

- [例外使用者] 清單中擁有該主機的管理員權限的帳戶。[例外使用者] 清單適用於服務帳戶，例如備份代理程式。
- 該主機之 `DCUI.Access` 進階選項中定義的使用者。該選項可用於在發生災難性的失敗時啟用存取權。

針對 ESXi 6.0 及更新版本，啟用鎖定模式時，會保留使用者權限。從 Direct Console 介面停用鎖定模式時會還原使用者權限。

備註 如果將處於鎖定模式的主機在未結束鎖定模式的情況下升級為 ESXi 6.0 版，然後在升級後結束鎖定模式，則主機在進入鎖定模式前定義的所有權限都會遺失。系統會將管理員角色指派給 DCUI.Access 進階選項中找到的所有使用者，以保證主機仍可存取。

若要保留權限，請先從 vSphere Web Client 停用該主機的鎖定模式，然後再進行升級。

程序

1. 在主機的 Direct Console 使用者介面上，按 F2 並登入。
2. 捲動至**設定鎖定模式**設定並按 Enter 切換目前設定。
3. 按 Esc 直到返回 Direct Console 使用者介面的主功能表。

指定在鎖定模式下具有存取權限的帳戶

您可以指定可直接存取 ESXi 主機的服務帳戶，方式是將其新增到 [例外使用者] 清單。您可以指定在發生災難性 vCenter Server 失敗時可存取 ESXi 主機的單一使用者。

vSphere 版本決定啟用鎖定模式時不同帳戶預設執行的動作以及如何變更預設行為。

- 在 vSphere 5.0 及更早版本中，僅根使用者可以在處於鎖定模式的 ESXi 主機上登入 Direct Console 使用者介面。
- 在 vSphere 5.1 及更新版本中，您可以將某個使用者新增到每個主機的 DCUI.Access 進階系統設定中。該選項適用於 vCenter Server 的災難性故障。公司通常會將具有該存取權的使用者的密碼鎖定在安全位置中。DCUI.Access 清單中的使用者不需要擁有主機的完整管理權限。
- 在 vSphere 6.0 及更新版本中，仍支援 DCUI.Access 進階系統設定。此外，vSphere 6.0 及更新版本支援 [例外使用者] 清單，該清單適用於須直接登入主機的服務帳戶。[例外使用者] 清單中具有管理員權限的帳戶可登入 ESXi Shell。此外，這些使用者還可以在一般鎖定模式下登入主機的 DCUI 並結束鎖定模式。

  您可以從 vSphere Web Client 指定例外使用者。

  備註 例外使用者為主機的本機使用者，或具有針對 ESXi 主機本機定義之權限的 Active Directory 使用者。當主機處於鎖定模式時，身為 Active Directory 群組成員的使用者會遺失其權限。

將使用者新增至 DCUI.Access 進階選項

如果發生災難性的失敗，您無法從 vCenter Server 存取主機時，DCUI.Access 進階選項可用於結束鎖定模式。可從 vSphere Web Client 編輯主機的 [進階設定] 將使用者新增到清單。

備註 DCUI.Access 清單中的使用者可變更鎖定模式設定，無論其權限為何。變更鎖定模式功能可能會影響主機安全性。對於需要直接存取主機的服務帳戶，請考慮將使用者新增到 [例外使用者] 清單中。例外使用者只能執行擁有相應權限的工作。請參閱指定鎖定模式例外使用者。

程序

1 在 vSphere Web Client 物件導覽器中，瀏覽到主機。

2 按一下**設定**。

3 在 [系統] 下，按一下**進階系統設定**，然後按一下**編輯**。

4 DCUI 的篩選器。

5 在 **DCUI.Access** 文字方塊中，輸入本機 ESXi 使用者名稱，並以逗點分隔。

依預設，已包含根使用者。請考慮從 DCUI.Access 清單中移除 root 使用者並指定具名帳戶以更方便稽核。

6 按一下**確定**。

指定鎖定模式例外使用者

在 vSphere 6.0 及更新版本中，您可以從 vSphere Web Client 將使用者新增到 [例外使用者] 清單中。當主機進入鎖定模式時，這些使用者不會遺失他們的權限。因此，將服務帳戶 (例如備份代理程式) 新增到 [例外使用者] 清單很有必要。

當主機進入鎖定模式時，例外使用者不會遺失他們的權限。通常，這些帳戶代表需要在鎖定模式下繼續運作的第三方解決方案和外部應用程式。

備註 [例外使用者] 清單適用於執行極特定工作的服務帳戶，而不是管理員。將管理員使用者新增到 [例外使用者] 清單會讓鎖定模式的用途失效。

例外使用者為主機的本機使用者，或具有針對 ESXi 主機本機定義之權限的 Active Directory 使用者。他們不是 Active Directory 群組的成員，也不是 vCenter Server 使用者。這些使用者可根據其權限在主機上執行作業。這意味著，例如，唯讀使用者無法在主機上停用鎖定模式。

程序

1 在 vSphere Web Client 詳細目錄中瀏覽到主機。

2 按一下**設定**。

3 在 [系統] 下，選取**安全性設定檔**。

4 在 [鎖定模式] 面板中，按一下**編輯**。

5 按一下**例外使用者**，然後按一下加號新增例外使用者。

管理主機和 VIB 的接受程度

VIB 的接受程度視此 VIB 的憑證數量而定。主機的接受程度視最低 VIB 的層級而定。如果您想要允許較低層級的 VIB，可變更主機的接受程度。若要能夠變更主機接受程度，可移除 CommunitySupported VIB。

VIB 是包含 VMware 或 VMware 合作夥伴提供之簽章的軟體套件。若要保護 ESXi 主機的完整性，請禁止使用者安裝尚未簽署的 (社群支援的) VIB。未簽署的 VIB 包含未由 VMware 或其合作夥伴認證、接受或支援的程式碼。社群支援的 VIB 沒有數位簽章。

該主機的接受程度必須與要新增到該主機的任何 VIB 的接受程度相同或更低。例如，如果主機的接受程度為 VMwareAccepted，則您無法在 PartnerSupported 層級安裝 VIB。您可以使用 ESXCLI 命令來設定主機的接受程度。若要保護 ESXi 主機的安全性和完整性，請勿在生產系統的主機上安裝未簽署的 (CommunitySupported) VIB。

ESXi 主機的接受程度顯示在 vSphere Web Client 的**安全性設定檔**中。

支援以下接受程度。

VMwareCertified	VMwareCertified 接受程度具有最為嚴格的需求。此程度的 VIB 能夠完全通過全面測試，該測試相當於相同技術的 VMware 內部品質保證測試。今天，僅以此程度發佈 I/O Vendor Program (IOVP) 計畫驅動程式。VMware 受理此接受程度的 VIB 的支援致電。
VMwareAccepted	此接受程度的 VIB 雖然已通過驗證測試，但這些測試並非對軟體的每項功能進行全面測試。合作夥伴會執行測試並且 VMware 會驗證結果。現在，以此程度發佈的 VIB 包括 CIM 提供者和 PSA 外掛程式。VMware 會將此接受程度的 VIB 支援致電轉交給合作夥伴的支援組織。
PartnerSupported	接受程度為 PartnerSupported 的 VIB 是由 VMware 信任的合作夥伴發佈的。合作夥伴會執行所有測試。VMware 不會驗證結果。合作夥伴想要在 VMware 系統中啟用的新技術或非主流技術將使用此程度。現在，驅動程式 VIB 技術 (例如 Infiniband、ATAoE 和 SSD) 皆採用此程度，並具有非標準硬體驅動程式。VMware 會將此接受程度的 VIB 支援致電轉交給合作夥伴的支援組織。
CommunitySupported	CommunitySupported 接受程度適用於由未參與 VMware 合作夥伴計劃的個人或公司建立的 VIB。此程度的 VIB 尚未通過任何 VMware 核准的測試計劃，且不受 VMware 技術支援或 VMware 合作夥伴的支援。

程序

1 連線至每個 ESXi 主機，並執行以下命令來驗證是否已將接受程度設定為 VMwareCertified、VMwareAccepted 或 PartnerSupported。

```
esxcli software acceptance get
```

2 如果主機接受程度為 CommunitySupported，請執行以下命令來判定是否有任何 VIB 處於 CommunitySupported 層級。

```
esxcli software vib list
esxcli software vib get –n vibname
```

3 執行以下命令以移除任何 CommunitySupported VIB。

```
esxcli software vib remove ––vibname vib
```

4 使用以下其中一種方法變更主機的接受程度。

選項	說明
CLI 命令	`esxcli software acceptance set --level acceptance_level`
vSphere Client (以 HTML5 為基礎的用戶端) 或 vSphere Web Client	a 在詳細目錄中選取主機。 b 選取**設定**索引標籤。 c 展開**系統**，然後選取**安全性設定檔**。 d 針對主機映像設定檔接受程度按一下**編輯**按鈕，然後選擇接受程度。

為 ESXi 主機指派權限

在大多數情況下，您可授予權限給使用者，方法是將權限指派給受 vCenter Server 系統管理的 ESXi 主機物件。如果您正在使用獨立的 ESXi 主機，則可以直接指派權限。

將權限指派給 vCenter Server 管理的 ESXi 主機

如果您的 ESXi 主機受 vCenter Server 管理，請透過 vSphere Web Client 執行管理工作。

您可以從 vCenter Server 物件階層中選取 ESXi 主機物件，並將管理員角色指派給數量有限的使用者。然後，這些使用者可以在 ESXi 主機上執行直接管理。請參閱使用角色指派權限。

最佳做法是至少建立一個具名使用者帳戶，並為其指派對主機的完整管理權限，然後使用此帳戶取代根帳戶。為根帳戶設定一個非常複雜的密碼，並限制根帳戶的使用。請勿移除根帳戶。

將權限指派給獨立的 ESXi 主機

您可以新增本機使用者，並從 VMware Host Client 的 [管理] 索引標籤定義自訂角色。請參閱 *vSphere 單一主機管理 - VMware Host Client* 說明文件。

如需 ESXi 的所有版本，請參閱 `/etc/passwd` 檔案中的預先定義使用者清單。

會預先定義下列角色。

唯讀 允許使用者檢視與 ESXi 主機相關聯的物件，但請勿對物件做任何變更。

管理員 管理員角色。

無存取權 無存取權。此角色為預設角色。您可以覆寫預設角色。

透過使用直接連線至 ESXi 主機的 VMware Host Client，您可以管理本機使用者和群組，並將本機自訂角色新增至 ESXi 主機。請參閱 *vSphere 單一主機管理 - VMware Host Client* 說明文件。

從 vSphere 6.0 開始，您可以使用 ESXCLI 帳戶管理命令，來管理 ESXi 本機使用者帳戶。您可以使用 ESXCLI 權限管理命令，設定或移除 Active Directory 帳戶 (使用者和群組) 和 ESXi 本機帳戶 (僅使用者) 權限。

備註 如果透過直接連線至主機來針對 ESXi 主機定義使用者，並且 vCenter Server 中也存在相同名稱的使用者，則這些使用者會有所不同。如果將角色指派給 ESXi 使用者，則不會給 vCenter Server 使用者指派相同的角色。

預先定義的權限

如果您的環境不包含 vCenter Server 系統，則會預先定義下列使用者。

根使用者

依預設，每個 ESXi 主機擁有一個具有管理員角色的單一根使用者帳戶。該根使用者帳戶可用於本機管理並將主機連線到 vCenter Server。

指派根使用者權限可更輕易闖入 ESXi 主機，因為已經知道名稱。擁有一般根帳戶可讓符合使用者的動作更難。

為了更好地稽核，請建立具有管理員權限的個別帳戶。為根帳戶設定非常複雜的密碼，並限制根帳戶的使用，例如，新增主機至 vCenter Server 時使用。請勿移除根帳戶。

最佳做法是確保 ESXi 主機上具有管理員角色之任何帳戶指派給具名帳戶的特定使用者。請使用可讓您管理 Active Directory 認證的 ESXi Active Directory 功能。

重要事項 您可以移除根使用者的存取權限。但是，您必須首先在根層級 (擁有一個指派到管理員角色的不同使用者) 建立其他權限。

vpxuser 使用者

管理主機的活動時，vCenter Server 將使用 vpxuser 權限。

vCenter Server 管理員可以根使用者身分在主機上執行大多數相同的工作，亦可排程工作、使用範本等。然而，vCenter Server 管理員無法直接為主機建立、刪除或編輯本機使用者與群組。僅具有管理員權限的使用者才可以直接在主機上執行這些工作。

備註 您無法使用 Active Directory 管理 vpxuser。

警告 請勿以任何方式變更 vpxuser。請勿變更其密碼。請勿變更其權限。如果您執行了變更，可能會在透過 vCenter Server 使用主機時遇到問題。

dcui 使用者

dcui 使用者於主機上執行，並使用管理員權限。此使用者的主要用途為針對 Direct Console 使用者介面 (DCUI) 的鎖定模式設定主機。

此使用者可充當 Direct Console 的代理程式，且無法由互動式使用者修改或使用。

使用 Active Directory 管理 ESXi 使用者

可以將 ESXi 設定為使用 Active Directory 等目錄服務來管理使用者。

如果要在每台主機上都建立本機使用者帳戶，會面臨必須在多台主機間同步帳戶名稱和密碼的挑戰。若將 ESXi 主機加入到 Active Directory 網域中，就無需再建立和維護本機使用者帳戶。若使用 Active Directory 進行使用者驗證，可簡化 ESXi 主機組態，並降低可能導致未授權存取的組態問題風險。

使用 Active Directory 時，若將主機新增到網域，使用者會提供自己的 Active Directory 認證和 Active Directory 伺服器的網域名稱。

將主機設定為使用 Active Directory

可以設定主機，以使用目錄服務 (如 Active Directory) 管理使用者和群組。

將 ESXi 主機新增至 Active Directory 時，如果存在 DOMAIN 群組 **ESX Admins**，則為其指派對主機的完整管理存取權。如果不希望分配完整管理存取權，請參閱 VMware 知識庫文章 1025569 獲取因應措施。

如果使用 Auto Deploy 佈建主機，則無法在主機上儲存 Active Directory 認證。您可以使用 vSphere Authentication Proxy 將主機加入 Active Directory 網域。因為 vSphere Authentication Proxy 和主機之間存在信任鏈，Authentication Proxy 可以將主機加入 Active Directory 網域。請參閱使用 vSphere Authentication Proxy。

備註 在 Active Directory 中定義使用者帳戶設定時，可以按電腦名稱限制使用者能夠登入的電腦。依預設，未對使用者帳戶設定任何相關限制。如果設定了此限制，對使用者帳戶的 LDAP 繫結要求將失敗，並顯示訊息 LDAP 繫結失敗，即使該要求來自列出的電腦也是如此。透過將 Active Directory 伺服器的 netBIOS 名稱新增到使用者帳戶能夠登入的電腦清單，可避免此問題。

先決條件

- 確認您擁有 Active Directory 網域。請參閱目錄伺服器說明文件。
- 確認 ESXi 的主機名稱完全符合 Active Directory 樹系的網域名稱條件。

  fully qualified domain name = host_name.domain_name

程序

1. 使用 NTP 將 ESXi 和目錄服務系統的時間同步。

   如需如何使用 Microsoft 網域控制站同步 ESXi 時間的相關資訊，請參閱使 ESXi 時鐘與網路時間伺服器同步或 VMware 知識庫。

2. 確保為主機設定的 DNS 伺服器可以解析 Active Directory 控制站的主機名稱。
   a. 在 vSphere Web Client 物件導覽器中，瀏覽到主機。
   b. 按一下**設定**。

c 在 [網路] 下，按一下 **TCP/IP 組態**。

d 在 [TCP/IP 堆疊: 預設] 下，按一下 **DNS**，然後確認該主機的主機名稱和 DNS 伺服器資訊正確無誤。

下一個

使用 vSphere Web Client 加入目錄服務網域。請參閱將主機新增至目錄服務網域。對於使用 Auto Deploy 佈建的主機，請設定 vSphere Authentication Proxy。請參閱使用 vSphere Authentication Proxy。

將主機新增至目錄服務網域

若主機要使用目錄服務，必須先將主機加入目錄服務網域。

您可以使用下列兩種方式中的一種來輸入網域名稱：

- **`name.tld`** (例如，**`domain.com`**)：會在預設容器下建立帳戶。
- **`name.tld/container/path`** (例如，**`domain.com/OU1/OU2`**)：會在特定組織單位 (OU) 下建立帳戶。

若要使用 vSphere Authentication Proxy 服務，請參閱使用 vSphere Authentication Proxy。

程序

1 在 vSphere Web Client 詳細目錄中瀏覽到主機。

2 按一下**設定**。

3 在 [系統] 下，選取**驗證服務**。

4 按一下**加入網域**。

5 輸入網域。

使用 **`name.tld`** 或 **`name.tld/container/path`** 形式。

6 輸入有權將主機加入網域的目錄服務使用者的使用者名稱和密碼，然後按一下**確定**。

7 (選擇性) 如果您想要使用驗證 Proxy，請輸入 Proxy 伺服器 IP 位址。

8 按一下**確定**，關閉 [目錄服務組態] 對話方塊。

檢視目錄服務設定

您可以檢視目錄伺服器的類型 (如果有類型可檢視)，主機使用此類型來驗證使用者和目錄伺服器設定。

程序

1 在 vSphere Web Client 詳細目錄中瀏覽到主機。

2 按一下**設定**。

3 在 [系統] 下，選取**驗證服務**。

[驗證服務] 分頁將顯示目錄服務和網域設定。

使用 vSphere Authentication Proxy

您可透過使用 vSphere Authentication Proxy 將 ESXi 主機新增到 Active Directory 網域，而非將主機明確新增到 Active Directory 網域。

您只需設定主機，讓其瞭解 Active Directory 伺服器的網域名稱，以及 vSphere Authentication Proxy 的 IP 位址。啟用 vSphere Authentication Proxy 後，其會自動將使用 Auto Deploy 佈建的主機新增到 Active Directory 網域。您也可搭配使用 vSphere Authentication Proxy 與尚未使用 Auto Deploy 佈建的主機。

Auto Deploy

如果您是使用 Auto Deploy 佈建主機，則可設定指向 Authentication Proxy 的參考主機。之後，您可設定一個規則，該規則可將參考主機的設定檔套用至使用 Auto Deploy 佈建的任何 ESXi 主機。vSphere Authentication Proxy 將 Auto Deploy 使用 PXE 佈建之所有主機的 IP 位址儲存在其存取控制清單中。主機開機時，其將連絡 vSphere Authentication Proxy，之後 vSphere Authentication Proxy 會將已存在於其存取控制清單中的這些主機加入 Active Directory 網域。

即使您在使用 VMCA 或第三方憑證佈建之憑證的環境中使用 vSphere Authentication Proxy，只要您遵循搭配使用自訂憑證和 Auto Deploy 的指示，程序就會順利完成。

請參閱搭配使用自訂憑證與 Auto Deploy。

其他 ESXi 主機

如果您想要讓主機加入網域而不使用 Active Directory 認證，則您可將其他主機設定為使用 vSphere Authentication Proxy。也就是說，您無需將 Active Directory 認證傳輸到主機，且不將 Active Directory 認證儲存在主機設定檔中。

在這種情況下，您將主機的 IP 位址新增到 vSphere Authentication Proxy 存取控制清單，然後 vSphere Authentication Proxy 會依預設根據主機的 IP 位址進行授權。您可啟用用戶端驗證來讓 vSphere Authentication Proxy 檢查主機的憑證。

備註 您無法在只支援 IPv6 的環境下使用 vSphere Authentication Proxy。

啟用 vSphere Authentication Proxy

vSphere Authentication Proxy 服務在每個 vCenter Server 系統上均可用。依預設，此服務未執行。如果您想要在環境中使用 vSphere Authentication Proxy，可從 vSphere Web Client 或命令列啟動此服務。

vSphere Authentication Proxy 服務會繫結到 IPv4 位址與 vCenter Server 進行通訊，且不支援 IPv6。vCenter Server 執行個體可以位於僅 IPv4 或 IPv4/IPv6 混合模式網路環境中的主機機器上。但是，當您在 vSphere Web Client 中指定 vSphere Authentication Proxy 的位址時，必須指定 IPv4 位址。

先決條件

請確認您使用 vCenter Server 6.5 或更新版本。在舊版 vSphere 中，vSphere Authentication Proxy 是單獨安裝的。請參閱此舊版產品的說明文件以取得指示。

程序

1 使用 vSphere Web Client 連線到 vCenter Server 系統。

2 按一下**管理**，然後按一下**部署**下的**系統組態**。

3 按一下**服務**，然後按一下 **VMware vSphere Authentication Proxy** 服務。

4 在視窗頂端的功能表列中，按一下綠色的**啟動服務**圖示。

5 (選擇性) 服務啟動後，按一下**動作 > 編輯啟動類型**，然後按一下**自動**以自動啟動。

您現在可以設定 vSphere Authentication Proxy 網域。之後，vSphere Authentication Proxy 會處理使用 Auto Deploy 佈建的所有主機，並且您可以明確將主機新增至 vSphere Authentication Proxy。

使用 vSphere Web Client 將網域新增至 vSphere Authentication Proxy

您可以從 vSphere Web Client 或使用 `camconfig` 命令，將網域新增至 vSphere Authentication Proxy。

僅在啟用 Proxy 後，才能新增網域至 vSphere Authentication Proxy。新增網域後，vSphere Authentication Proxy 會將您使用 Auto Deploy 佈建的所有主機新增至該網域。對於其他主機，如果您不想授與這些主機網域權限，也可以使用 vSphere Authentication Proxy。

程序

1 使用 vSphere Web Client 連線到 vCenter Server 系統。

2 按一下**管理**，然後按一下**部署**下的**系統組態**。

3 依序按一下**服務**和 **VMware vSphere Authentication Proxy** 服務，然後按一下**編輯**。

4 輸入 vSphere Authentication Proxy 將在其中新增主機之網域的名稱，以及擁有 Active Directory 權限，可將主機新增至網域之使用者的名稱。

   此對話方塊中的其他欄位僅供參考。

5 按一下省略符號圖示，以新增並確認使用者的密碼，然後按一下**確定**。

使用 camconfig 命令，將網域新增至 vSphere Authentication Proxy

您可以從 vSphere Web Client 或使用 `camconfig` 命令，將網域新增至 vSphere Authentication。

僅在啟用 Proxy 後，才能新增網域至 vSphere Authentication Proxy。新增網域後，vSphere Authentication Proxy 會將您使用 Auto Deploy 佈建的所有主機新增至該網域。對於其他主機，如果您不想授與這些主機網域權限，也可以使用 vSphere Authentication Proxy。

程序

1 以具有管理員權限的使用者身分登入 vCenter Server Appliance 或 vCenter Server Windows 機器。

2 執行命令以啟用對 Bash shell 的存取。

```
shell
```

3 前往 **camconfig** 指令碼所在的目錄。

作業系統	位置
vCenter Server Appliance	`/usr/lib/vmware-vmcam/bin/`
vCenter Server Windows	`C:\Program Files\VMware\CIS\vmcamd\`

4 執行下列命令，將網域和使用者 Active Directory 認證新增至 Authentication Proxy 組態。

```
camconfig add-domain -d domain -u user
```

系統會提示您輸入密碼。

vSphere Authentication Proxy 會快取該使用者名稱和密碼。您可視需要移除和重新建立使用者。網域必須能夠透過 DNS 連線，但不必是 vCenter Single Sign-On 身分識別來源。

vSphere Authentication Proxy 將會使用 *user* 所指定的使用者名稱，在 Active Directory 中建立 ESXi 主機的帳戶，因此使用者必須具備權限，才能在您要在其中新增主機的 Active Directory 網域中建立帳戶。寫入此資訊時，Microsoft 知識庫文章 932455 具有帳戶建立權限的背景資訊。

5 如果您之後想要從 vSphere Authentication Proxy 移除網域和使用者資訊，請執行下列命令。

```
camconfig remove-domain -d domain
```

使用 vSphere Authentication Proxy 將主機新增到網域

Auto Deploy 伺服器將其佈建的所有主機新增至 vSphere Authentication Proxy，然後 vSphere Authentication Proxy 將這些主機新增至網域。如果您想要使用 vSphere Authentication Proxy 將其他主機新增至網域，您可明確將這些主機新增至 vSphere Authentication Proxy。隨後，vSphere Authentication Proxy 伺服器將這些主機新增至網域。因此，使用者提供的認證無需再傳輸至 vCenter Server 系統。

您可以使用下列兩種方式中的一種來輸入網域名稱：

- **`name.tld`** (例如，**`domain.com`**)：會在預設容器下建立帳戶。
- **`name.tld/container/path`** (例如，**`domain.com/OU1/OU2`**)：會在特定組織單位 (OU) 下建立帳戶。

先決條件

- 如果 ESXi 主機使用 VMCA 簽署憑證，請確認已將主機新增到 vCenter Server。否則，Authentication Proxy 服務無法信任 ESXi 主機。
- 如果 ESXi 使用 CA 簽署憑證，請確認已將 CA 簽署憑證新增到 vCenter Server 系統。請參閱 ESXi 主機的憑證管理。

程序

1 使用 vSphere Web Client 連線到 vCenter Server 系統。

2 瀏覽到 vSphere Web Client 中的主機，然後按一下**設定**。

3 在**設定**下，選取**驗證服務**。

4 按一下**加入網域**。

5 輸入網域。

使用表單 **name.tld** (例如 **mydomain.com**)，或 **name.tld/container/path** (例如 **mydomain.com/organizational_unit1/organizational_unit2**)。

6 選取**使用 Proxy 伺服器**。

7 輸入 Authentication Proxy 伺服器的 IP 位址，其始終與 vCenter Server 系統的 IP 位址相同。

8 按一下**確定**。

為 vSphere Authentication Proxy 啟用用戶端驗證

依預設，vSphere Authentication Proxy 可以新增存取控制清單中具有其 IP 位址的任何主機。為獲得額外的安全性，您可以啟用用戶端驗證。如果啟用用戶端驗證，vSphere Authentication Proxy 還會檢查主機的憑證。

先決條件

- 請確認 vCenter Server 系統是否信任此主機。依預設，當您將主機新增至 vCenter Server 時，系統會向此主機指派由 vCenter Server 信任的根 CA 簽署的憑證。vSphere Authentication Proxy 信任 vCenter Server 信任的根 CA。
- 如果您打算取代環境中的 ESXi 憑證，請在啟用 vSphere Authentication Proxy 之前進行取代。ESXi 主機上的憑證必須與主機登錄的憑證相符。

程序

1 以具有管理員權限的使用者身分登入 vCenter Server Appliance 或 vCenter Server Windows 機器。

2 執行命令以啟用對 Bash shell 的存取。

```
shell
```

3 前往 **camconfig** 指令碼所在的目錄。

作業系統	位置
vCenter Server Appliance	`/usr/lib/vmware-vmcam/bin/`
vCenter Server Windows	`C:\Program Files\VMware\CIS\vmcamd\`

4 執行以下命令以啟用用戶端驗證。

```
camconfig ssl-cliAuth -e
```

然後，vSphere Authentication Proxy 會檢查新增的每個主機的憑證。

5 如果您稍後想要再次停用用戶端驗證，請執行以下命令。

```
camconfig ssl-cliAuth -n
```

將 vSphere Authentication Proxy 憑證匯入 ESXi 主機

依預設，ESXi 主機要求對 vSphere Authentication Proxy 憑證進行明確驗證。如果您使用 vSphere Auto Deploy，Auto Deploy 服務會負責將憑證新增到其佈建的主機。至於其他主機，您必須明確新增憑證。

先決條件

- 將 vSphere Authentication Proxy 憑證上傳到 ESXi 主機。您可以在以下位置找到憑證。

vCenter Server Appliance	`/var/lib/vmware/vmcam/ssl/rui.crt`
vCenter Server Windows	`C:\ProgramData\VMware\vCenterServer\data\vmcamd\ssl\rui.crt`

- 確認 `UserVars.ActiveDirectoryVerifyCAMCertificate` ESXi 進階設定已設定為 1 (預設值)。

程序

1. 在 vSphere Web Client 中，選取 ESXi 主機，然後按一下**設定**。
2. 在**系統**下，選取**驗證服務**。
3. 按一下**匯入憑證**。
4. 遵循格式 `[datastore]/path/certname.crt` 輸入憑證檔案路徑，然後按一下**確定**。

為 vSphere Authentication Proxy 產生新的憑證

如果您想要產生使用 VMCA 佈建的新憑證，或是包含 VMCA 做為下層憑證的新憑證，請依照本主題中的步驟進行。

若要使用由第三方 CA 或企業 CA 簽署的自訂憑證，請參閱設定 vSphere Authentication Proxy 使用自訂憑證。

先決條件

您必須在 vSphere Authentication Proxy 執行所在的系統上具備根權限或管理員權限。

程序

1. 建立 `certool.cfg` 的複本。

```
cp /usr/lib/vmware-vmca/share/config/certool.cfg /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

2 編輯含關於您組織之一些資訊的複本，如下列範例所示。

```
Country = IE
Name = vmcam
Organization = VMware
OrgUnit = vTSU
State = Cork
Locality = Cork
Hostname = test-cam-1.test1.vmware.com
```

3 在 /var/lib/vmware/vmcam/ssl/ 中產生新的私密金鑰。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=/var/lib/vmware/vmcam/ssl/rui.key --
pubkey=/tmp/vmcam.pub --server=localhost
```

對於 *localhost*，提供 Platform Services Controller 的 FQDN。

4 使用您在步驟 1 和步驟 2 中建立的金鑰和 vmcam.cfg 檔案，在 /var/lib/vmware/vmcam/ssl/ 中產生新憑證。

```
/usr/lib/vmware-vmca/bin/certool --server=localhost --gencert --
privkey=/var/lib/vmware/vmcam/ssl/rui.key --cert=/var/lib/vmware/vmcam/ssl/rui.crt --
config=/var/lib/vmware/vmcam/ssl/vmcam.cfg
```

對於 *localhost*，提供 Platform Services Controller 的 FQDN。

設定 vSphere Authentication Proxy 使用自訂憑證

搭配使用自訂憑證和 vSphere Authentication Proxy 包含多個步驟。首先產生 CSR，並將其傳送到 CA 進行簽署。然後將簽署的憑證和金鑰檔案放置在 vSphere Authentication Proxy 可存取的位置。

依預設，vSphere Authentication Proxy 在首次開機期間會產生 CSR，然後要求 VMCA 簽署該 CSR。vSphere Authentication Proxy 使用該憑證向 vCenter Server 登錄。如果您將自訂憑證新增到 vCenter Server，便可以在自己的環境中使用這些憑證。

程序

1 為 vSphere Authentication Proxy 產生 CSR。

a 建立組態檔 `/var/lib/vmware/vmcam/ssl/vmcam.cfg`，如下列範例所示。

```
[ req ]
distinguished_name = req_distinguished_name
encrypt_key = no
prompt = no
string_mask = nombstr
req_extensions = v3_req
[ v3_req ]
basicConstraints = CA:false
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = DNS:olearyf-static-1.csl.vmware.com
[ req_distinguished_name ]
countryName = IE
stateOrProvinceName = Cork
localityName = Cork
0.organizationName = VMware
organizationalUnitName = vTSU
commonName = test-cam-1.test1.vmware.com
```

b 執行 `openssl` 以產生 CSR 檔案和金鑰檔案，並於組態檔中傳遞。

```
openssl req -new -nodes -out vmcam.csr -newkey rsa:2048 -
keyout /var/lib/vmware/vmcam/ssl/rui.key -config /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

2 備份儲存在下列位置的 `rui.crt` 憑證和 `rui.key` 檔案。

作業系統	位置
vCenter Server Appliance	`/var/lib/vmware/vmcam/ssl/rui.crt`
vCenter Server Windows	`C:\ProgramData\VMware\vCenterServer\data\vmcamd\ssl\rui.crt`

3 解除登錄 vSphere Authentication Proxy。

a 前往 `camregister` 指令碼所在的目錄。

作業系統	命令
vCenter Server Appliance	`/usr/lib/vmware-vmcam/bin`
vCenter Server Windows	`C:\ProgramData\VMware\vCenterServer\data\vmcamd\ssl\rui.crt`

b 執行下列命令。

```
camregister --unregister -a VC_address -u user
```

user 必須是擁有 vCenter Server 管理員權限的 vCenter Single Sign-On 使用者。

4 停止 vSphere Authentication Proxy 服務。

工具	步驟
vSphere Web Client	a 按一下**管理**，然後按一下**部署**下的**系統組態**。 b 按一下**服務**，接著按一下 **VMware vSphere Authentication Proxy** 服務，然後停止服務。
CLI	`service-control --stop vmcam`

5 將現有的 `rui.crt` 憑證和 `rui.key` 檔案取代為從 CA 收到的檔案。

6 重新啟動 vSphere Authentication Proxy 服務。

7 使用新憑證和金鑰向 vCenter Server 明確重新登錄 vSphere Authentication Proxy。

```
camregister --register -a VC_address -u user -c full_path_to_rui.crt -k full_path_to_rui.key
```

設定用於 ESXi 的智慧卡驗證

您可使用智慧卡驗證登入 ESXi Direct Console 使用者介面 (DCUI)，方法是使用個人身分驗證 (PIV)、通用存取卡 (CAC) 或 SC650 智慧卡，而非指定使用者名稱和密碼。

智慧卡是一張內嵌整合式電路晶片的小塑膠卡。許多政府機關及大型企業均採用以雙重要素驗證為基礎的智慧卡，以增強其系統的安全性並符合安全法規。

在 ESXi 主機上啟用智慧卡驗證時，DCUI 會提示提供智慧卡和 PIN 組合，而不是使用者名稱和密碼的預設提示。

1 當您將智慧卡插入智慧卡讀卡機時，ESXi 主機會讀取上面的認證。

2 ESXi DCUI 會顯示您的登入識別碼，並提示您輸入 PIN。

3 在您輸入 PIN 之後，ESXi 主機會將其與儲存在智慧卡上的 PIN 進行比對，並使用 Active Directory 驗證智慧卡上的憑證。

4 成功驗證智慧卡憑證之後，ESXi 會讓您登入 DCUI。

按 F3 即可從 DCUI 切換到使用者名稱和密碼驗證。

連續幾次輸入不正確的 PIN (通常為三次) 後，智慧卡上的晶片即會鎖定。如果智慧卡鎖定，只有特定人員才能將其解除鎖定。

啟用智慧卡驗證

啟用智慧卡驗證，以提示智慧卡和 PIN 組合登入 ESXi DCUI。

先決條件

- 設定基礎結構，以處理智慧卡驗證，如 Active Directory 網域中的帳戶、智慧卡讀卡機及智慧卡。
- 設定 ESXi 加入支援智慧卡驗證的 Active Directory 網域。如需詳細資訊，請參閱 使用 Active Directory 管理 ESXi 使用者。

- 使用 vSphere Web Client 新增根憑證。請參閱 ESXi 主機的憑證管理。

程序

1. 在 vSphere Web Client 中，瀏覽到主機。
2. 按一下**設定**。
3. 在 [系統] 下，選取**驗證服務**。

   您將看到目前的智慧卡驗證狀態和包含已匯入憑證的清單。
4. 在 [智慧卡驗證] 面板中，按一下**編輯**。
5. 在 [編輯智慧卡驗證] 對話方塊中，選取 [憑證] 頁面。
6. 新增受信任的憑證授權機構 (CA) 憑證，例如根 CA 憑證和中繼 CA 憑證。
7. 開啟 [智慧卡驗證] 頁面，選取**啟用智慧卡驗證**核取方塊，然後按一下**確定**。

停用智慧卡驗證

停用智慧卡驗證，以返回到用於 ESXi DCUI 登入的預設使用者名稱和密碼驗證。

程序

1. 在 vSphere Web Client 中，瀏覽到主機。
2. 按一下**設定**。
3. 在 [系統] 下，選取**驗證服務**。

   您將看到目前的智慧卡驗證狀態和包含已匯入憑證的清單。
4. 在 [智慧卡驗證] 面板中，按一下**編輯**。
5. 在 [智慧卡驗證] 頁面上，取消選取**啟用智慧卡驗證**核取方塊，然後按一下**確定**。

發生連線問題時，利用使用者名稱和密碼進行驗證

如果 Active Directory (AD) 網域伺服器無法連線，您可以藉由使用者名稱和密碼驗證登入 ESXi DCUI，以對主機執行緊急動作。

在例外情況下，因連線問題、網路中斷或災難而無法連線 AD 網域伺服器以對智慧卡進行使用者認證的驗證。在此情況下，您可以使用本機 ESXi 管理員使用者的認證，登入 ESXi DCUI。登入之後，您可以執行診斷或其他緊急動作。將記錄使用者名稱和密碼登入後援。至 AD 的連線已還原時，會再次啟用智慧卡驗證。

備註 如果 Active Directory (AD) 網域伺服器可用，則中斷與 vCenter Server 的網路連線不會影響智慧卡驗證。

在鎖定模式下使用智慧卡驗證

啟用後，ESXi 主機上的鎖定模式可提高主機的安全性並限制對 DCUI 的存取。鎖定模式可能會停用智慧卡驗證功能。

在一般鎖定模式下，僅 [例外使用者] 清單中具有管理員權限的使用者可以存取 DCUI。例外使用者為主機的本機使用者，或具有針對 ESXi 主機本機定義之權限的 Active Directory 使用者。如果要在一般鎖定模式下使用智慧卡驗證，必須從 vSphere Web Client 將使用者新增至 [例外使用者] 清單。當主機進入一般鎖定模式時，這些使用者不會遺失他們的權限，並且可以登入 DCUI。如需詳細資訊，請參閱 指定鎖定模式例外使用者。

在嚴格鎖定模式下，DCUI 服務會停止。因此，您無法使用智慧卡驗證存取主機。

使用 ESXi Shell

ESXi 主機上預設停用 ESXi Shell。如有必要，可以啟用對 Shell 的本機和遠端存取。

若要降低未授權存取的風險，請僅啟用 ESXi Shell 進行疑難排解。

ESXi Shell 獨立於鎖定模式之外。如果該功能已啟用，即使主機在鎖定模式下執行，您仍可登入 ESXi Shell。

ESXi Shell	啟用此服務可本機存取 ESXi Shell。
SSH	啟用此服務可使用 SSH 遠端存取 ESXi Shell。

根使用者和具有管理員角色的使用者可以存取 ESXi Shell。屬於 Active Directory 群組 ESX Admins 的使用者將自動指派有管理員角色。依預設，只有根使用者可使用 ESXi Shell 執行系統命令 (例如 `vmware -v`)。

備註 僅在實際需要存取時啟用 ESXi Shell。

- 使用 vSphere Web Client 啟用對 ESXi Shell 的存取

  可以使用 vSphere Web Client 啟用對 ESXi Shell 的本機和遠端 (SSH) 存取，以及設定閒置逾時和可用性逾時。

- 使用 Direct Console 使用者介面 (DCUI) 啟用對 ESXi Shell 的存取

  Direct Console 使用者介面 (DCUI) 允許您使用文字型功能表於本機與主機進行互動。請仔細評估您的環境安全性需求是否支援啟用 Direct Console 使用者介面。

- 登入 ESXi Shell 進行疑難排解

  使用 vSphere Web Client、vSphere CLI 或 vSphere PowerCLI 執行 ESXi 組態工作。登入 ESXi Shell (之前稱為技術支援模式或 TSM) 僅進行疑難排解。

使用 vSphere Web Client 啟用對 ESXi Shell 的存取

可以使用 vSphere Web Client 啟用對 ESXi Shell 的本機和遠端 (SSH) 存取，以及設定閒置逾時和可用性逾時。

備註 使用 vSphere Web Client、遠端命令列工具 (vCLI 和 PowerCLI) 和已發佈的 API 來存取主機。除非是在要求啟用 SSH 存取的特殊情況下，否則不要啟用使用 SSH 遠端存取主機的功能。

先決條件

如果要使用 SSH 授權金鑰，可以上傳該金鑰。請參閱 ESXi SSH 金鑰。

程序

1. 在 vSphere Web Client 詳細目錄中瀏覽到主機。
2. 按一下**設定**。
3. 在 [系統] 下，選取**安全性設定檔**。
4. 在 [服務] 面板中，按一下**編輯**。
5. 從清單中選取服務。
   - ESXi Shell
   - SSH
   - Direct Console UI
6. 按一下**服務詳細資料**，然後選取啟動原則**手動啟動和停止**。

   如果選取**手動啟動和停止**，則將主機重新開機時不會啟動服務。如果要在將主機重新開機時啟動服務，請選取**隨主機一起啟動和停止**。
7. 選取**啟動**來啟用該服務。
8. 按一下**確定**。

下一個

設定 ESXi Shell 的可用性和閒置逾時。請參閱在 vSphere Web Client 中為 ESXi Shell 可用性建立逾時和在 vSphere Web Client 中為閒置的 ESXi Shell 工作階段建立逾時

在 vSphere Web Client 中為 ESXi Shell 可用性建立逾時

依預設，ESXi Shell 處於停用狀態。您可為 ESXi Shell 設定可用性逾時，從而提高啟用 Shell 時的安全性。

可用性逾時設定是在啟用 ESXi Shell 之後和必須登入之前，可以經過的時間量。超過逾時期限後，該服務會停用，並且不允許使用者登入。

程序

1. 在 vSphere Web Client 詳細目錄中瀏覽到主機。
2. 按一下**設定**。
3. 在 [系統] 下，選取**進階系統設定**。
4. 選取 `UserVars.ESXiShellTimeOut`，然後按一下**編輯**。
5. 輸入閒置逾時設定。

   您必須重新啟動 SSH 服務和 ESXi Shell 服務，逾時才能生效。
6. 按一下**確定**。

如果您在逾時期限之內已登入，您的工作階段會存留下來。但是，在您登出或您的工作階段終止後，則不允許使用者登入。

在 vSphere Web Client 中為閒置的 ESXi Shell 工作階段建立逾時

如果使用者在主機上啟用了 ESXi Shell，但忘記登出工作階段，閒置工作階段將無限期保持連線狀態。開啟的連線會提高他人獲取主機存取權限的可能性。您可以透過為閒置工作階段設定逾時，防止出現此問題。

閒置逾時是使用者從閒置互動式工作階段登出之前可以經過的時間量。您可以從 Direct Console 介面 (DCUI) 或 vSphere Web Client 中控制本機和遠端 (SSH) 工作階段的時間量。

程序

1. 在 vSphere Web Client 詳細目錄中瀏覽到主機。
2. 按一下**設定**。
3. 在 [系統] 下，選取**進階系統設定**。
4. 選取 UserVars.ESXiShellInteractiveTimeOut，按一下**編輯**圖示，然後輸入逾時設定。
5. 重新啟動 ESXi Shell 服務和 SSH 服務，則此逾時生效。

如果該工作階段閒置，使用者將在逾時期限過後登出。

使用 Direct Console 使用者介面 (DCUI) 啟用對 ESXi Shell 的存取

Direct Console 使用者介面 (DCUI) 允許您使用文字型功能表於本機與主機進行互動。請仔細評估您的環境安全性需求是否支援啟用 Direct Console 使用者介面。

可以使用 Direct Console 使用者介面啟用對 ESXi Shell 的本機和遠端存取。

備註 使用 Direct Console 使用者介面、vSphere Web Client、ESXCLI 或其他管理工具對主機進行的變更，會每隔一小時或在正常關閉時提交到永久儲存區。如果在提交這些變更之前主機出現故障，則這些變更可能會遺失。

程序

1. 從 Direct Console 使用者介面中，按 F2 以存取 [系統自訂] 功能表。
2. 選取**疑難排解選項**並按 Enter。
3. 從 [疑難排解模式選項] 功能表中，選取要啟用的服務。
   - 啟用 ESXi Shell
   - 啟用 SSH
4. 按 Enter 啟用該服務。
5. 按 Esc 直到返回 Direct Console 使用者介面的主功能表。

下一個

設定 ESXi Shell 的可用性和閒置逾時。請參閱設定 ESXi Shell 的可用性逾時或閒置逾時。

設定 ESXi Shell 的可用性逾時或閒置逾時

依預設，ESXi Shell 處於停用狀態。若要提高啟用 Shell 時的安全性，您可以設定可用性逾時和/或閒置逾時。

兩種類型的逾時適用於不同的情況。

閒置逾時	如果使用者在主機上啟用了 ESXi Shell，但忘記登出工作階段，閒置工作階段將無限期保持連線狀態。開啟的連線會提高他人獲取主機存取權限的可能性。您可以透過為閒置工作階段設定逾時，防止出現此問題。
可用性逾時	可用性逾時決定在最初啟用 Shell 之後和登入之前，可以經過的時間量。如果等待更長的時間，服務會停用，並且您無法登入 ESXi Shell。

先決條件

啟用 ESXi Shell。請參閱使用 Direct Console 使用者介面 (DCUI) 啟用對 ESXi Shell 的存取。

程序

1. 登入 ESXi Shell。
2. 從 [疑難排解模式選項] 功能表中，選取**修改 ESXi Shell 和 SSH 逾時**，然後按 Enter。
3. 輸入閒置逾時 (以秒為單位) 或可用性逾時。

   您必須重新啟動 SSH 服務和 ESXi Shell 服務，逾時才能生效。
4. 按 Enter 並按 Esc，直到返回到 Direct Console 使用者介面的主功能表。
5. 按一下**確定**。

- 如果設定閒置逾時，使用者會在工作階段閒置指定的時間後登出。
- 如果設定可用性逾時，並且您在經過該逾時後沒有登入，便會再次停用登入。

登入 ESXi Shell 進行疑難排解

使用 vSphere Web Client、vSphere CLI 或 vSphere PowerCLI 執行 ESXi 組態工作。登入 ESXi Shell (之前稱為技術支援模式或 TSM) 僅進行疑難排解。

程序

1. 使用以下方式之一登入 ESXi Shell。
   - 如果可以直接存取主機，請在電腦的實體主控台上按 Alt+F1 開啟登入分頁。
   - 如果要遠端連線到主機，請使用 SSH 或其他遠端主控台連線，從而在主機上啟動工作階段。
2. 輸入由主機辨識的使用者名稱和密碼。

ESXi 主機的 UEFI 安全開機

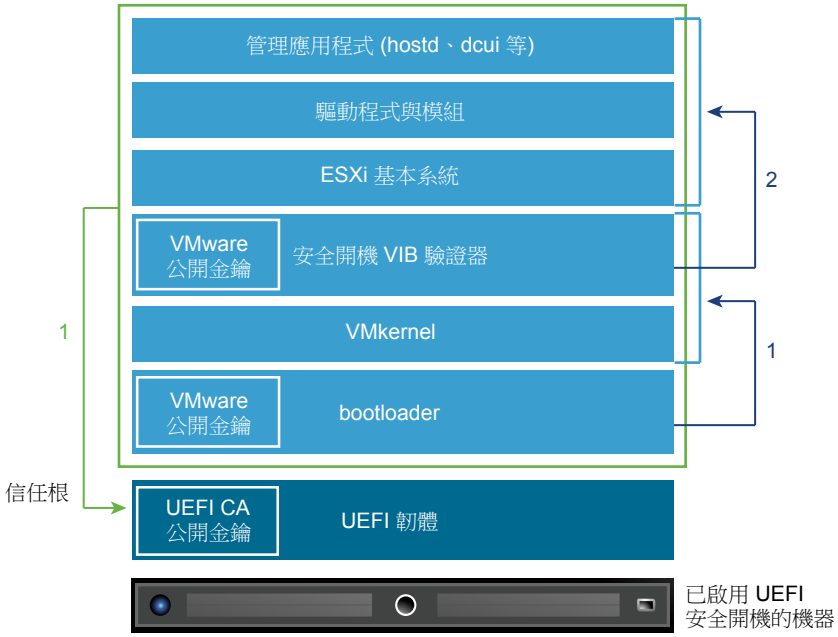
安全開機是 UEFI 韌體標準的一部分。啟用安全開機的情況下，除非作業系統開機載入器經密碼編譯簽署，否則機器將拒絕載入任何 UEFI 驅動程式或應用程式。從 vSphere 6.5 開始，ESXi 支援安全開機 (若已在硬體中啟用)。

UEFI 安全開機概觀

ESXi 6.5 版及更新版本支援在開機堆疊的每個層級上進行 UEFI 安全開機。

備註 在已升級至 ESXi 6.5 的主機上使用 UEFI 安全開機前，請遵循在升級的 ESXi 主機上執行安全開機驗證指令碼中的指示來檢查相容性。如果您透過使用 `esxcli` 命令來升級 ESXi 主機，則該升級不會更新開機載入器。在此情況下，您無法在該系統上執行安全開機。

圖 3-1 UEFI 安全開機



啟用安全開機的情況下，開機順序的執行方式如下。

1 從 vSphere 6.5 開始，ESXi 開機載入器包含 Vmware 公開金鑰。開機載入器使用此金鑰來驗證核心的簽章，以及一小部分包括安全開機 VIB 驗證器的系統。

2 VIB 驗證器驗證系統上安裝的每一個 VIB 套件。

此時，藉由屬於 UEFI 韌體之憑證中的信任根，整個系統完成開機。

UEFI 安全開機疑難排解

如果安全開機在開機順序的任意層級失敗，將會發生錯誤。

錯誤訊息取決於硬體廠商以及驗證失敗所屬的層級。

- 如果您嘗試使用尚未指派的或已遭竄改的開機載入器開機，則開機順序期間將發生錯誤。具體訊息取決於硬體廠商。該訊息可能類似如下錯誤，也可能不同。

  ```
  UEFI0073: Unable to boot PXE Device...because of the Secure Boot policy
  ```

- 如果核心已遭竄改，會發生類似如下的錯誤。

  ```
  Fatal error: 39 (Secure Boot Failed)
  ```

- 如果套件 (VIB 或驅動程式) 已遭竄改，則系統會出現紫色畫面，並顯示下列訊息。

  ```
  UEFI Secure Boot failed:
  Failed to verify signatures of the following vibs (XX)
  ```

若要解決安全開機的問題，請遵循這些步驟。

1 在安全開機停用的情況下將主機重新開機。

2 執行安全開機驗證指令碼 (請參閱在升級的 ESXi 主機上執行安全開機驗證指令碼)。

3 檢查 `/var/log/esxupdate.log` 檔案中的資訊。

在升級的 ESXi 主機上執行安全開機驗證指令碼

從不支援 UEFI 安全開機的舊版 ESXi 升級 ESXi 主機後，或許可以啟用安全開機。是否可以啟用安全開機取決於您如何執行升級，以及升級是否取代所有現有 VIB，或保留部分 VIB 不變。您可以在執行升級後執行驗證指令碼，以確定升級的安裝是否支援安全開機。

若要成功執行安全開機，每個已安裝的 VIB 的簽章必須在系統上可用。在安裝 VIB 時，較舊版本的 ESXi 不會儲存簽章。

- 如果您使用 ESXCLI 命令升級，則舊版 ESXi 會執行新的 VIB 安裝，因此不會儲存其簽章且不能安全開機。
- 如果您使用 ISO 升級，則新的 VIB 會儲存其簽章。此情況同樣適用於使用 ISO 的 vSphere Upgrade Manager 升級。
- 如果舊 VIB 保留在系統上，則這些 VIB 的簽章不可用且不能安全開機。
  - 如果系統使用第三方驅動程式，且 VMware 升級不包含新版驅動程式 VIB，則升級後舊 VIB 會保留在系統上。
  - 在少數情況下，VMware 可能會終止進行中的特定 VIB 的開發，而不提供將其取代或淘汰的新 VIB，因此升級後舊 VIB 會保留在系統上。

備註 UEFI 安全開機還需要使用最新的開機載入器。此指令碼不會檢查是否有最新的開機載入器。

先決條件

- 請確認硬體支援 UEFI 安全開機。

- 請確認所有 VIB 均在接受程度至少為 PartnerSupported 的情況下簽署。如果包含處於 CommunitySupported 程度的 VIB，則無法使用安全開機。

程序

1 升級 ESXi 並執行以下命令。

```
/usr/lib/vmware/secureboot/bin/secureBoot.py –c
```

2 檢查輸出。

輸出包含 `Secure boot can be enabled` 或 `Secure boot CANNOT be enabled`。

使用信賴平台模組保護 ESXi 主機

ESXi 可以使用信賴平台模組 (TPM) 晶片，這是安全的密碼處理器，可透過提供區別於軟體的硬體信任保證來增強主機安全性。

TPM 是安全密碼處理器的業界標準。TPM 晶片可在大多數現今電腦中找到，從筆記型電腦到桌上型電腦，再到伺服器。vSphere 6.7 支援 TPM 2.0 版。

TPM 2.0 晶片證明 ESXi 主機的身分。主機證明是驗證和證明在指定時間點主機軟體狀態的程序。UEFI 安全開機 (可確保在開機時僅載入簽署的軟體) 是成功證明的需求。TPM 2.0 晶片記錄並安全地儲存在系統中開機並由 vCenter Server 在遠端確認的軟體模組測量值。

遠端證明程序的高層級步驟如下：

1 建立遠端 TPM 的可信度，並在其上建立證明金鑰 (AK)。

將 ESXi 主機新增至 vCenter Server、從中重新開機該主機，或將該主機重新連線至它時，vCenter Server 會從主機要求 AK。部分 AK 建立程序也涉及驗證 TPM 硬體本身，以確保已知 (及受信任) 廠商已生產此硬體。

2 從主機擷取證明報告。

vCenter Server 要求主機傳送由 TPM 簽署的證明報告 (其中包含平台設定暫存器 (PCR) 的引述)，及其他簽署的主機二進位檔中繼資料。透過檢查被認定為受信任的組態對應資訊，vCenter Server 可識別先前不受信任的主機上的平台。

3 驗證主機的真實性。

vCenter Server 驗證已簽署引述的真實性、推斷軟體版本，並判斷前述軟體版本的可信度。如果 vCenter Server 判定已簽署引述無效，則遠端證明會失敗，並且主機不受信任。

若要使用 TPM 2.0 晶片，您的 vCenter Server 環境必須符合下列需求：

- vCenter Server6.7
- TPM 2.0 晶片已安裝在 ESXi6.7 主機中且已在 UEFI 中啟用
- 已啟用 UEFI 安全開機

確保在 ESXi 主機的 BIOS 中設定 TPM，以使用 SHA-256 雜湊演算法和 TIS/FIFO (先進先出) 介面，而非 CRB (命令回應緩衝)。如需設定這些必要 BIOS 選項的相關資訊，請參閱廠商說明文件。

在下列位置檢閱經過 VMware 認證的 TPM 2.0 晶片：

https://www.vmware.com/resources/compatibility/search.php

當您將已安裝 TPM 2.0 晶片的 ESXi 主機開機時，vCenter Server 會監控主機的證明狀態。vSphere Client 會在 vCenter Server 的**摘要**索引標籤的**安全性**下顯示硬體信任狀態，且顯示以下警示：

- 綠色：正常狀態，表示完全信任。
- 紅色：證明失敗。

備註 如果您將 TPM 2.0 晶片新增到已由 vCenter Server 管理的 ESXi 主機，必須先中斷主機連線，再重新連線。如需中斷連線和重新連線主機的相關資訊，請參閱 *vCenter Server 和主機管理*說明文件。

ESXi 和信賴平台模組 2.0 功能示範 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vm_67_esxi_tmp20)

檢視 ESXi 主機證明狀態

新增至 ESXi 主機時，信賴平台模組 2.0 相容晶片會證明平台的完整性。您可以在 vSphere Client 中檢視主機的證明狀態。

程序

1 透過使用 vSphere Client 連線至 vCenter Server。

2 導覽至資料中心，然後按一下**監控**索引標籤。

3 按一下**安全性**。

4 檢閱 [證明] 資料行中主機的狀態，並閱讀**訊息**資料行中隨附的訊息。

下一個

對於 [失敗] 或 [警告] 證明狀態，請參閱疑難排解 ESXi 主機證明問題。

疑難排解 ESXi 主機證明問題

當您在 ESXi 主機上安裝信賴平台模組 (TPM) 裝置時，主機可能無法通過證明。您可以疑難排解此問題的潛在原因。

程序

1 檢視 ESXi 主機警示狀態和隨附的錯誤訊息。請參閱檢視 ESXi 主機證明狀態。

2 如果錯誤訊息為主機安全開機已停用，您必須重新啟用安全開機來解決此問題。

3 如果主機的證明狀態為失敗，請查看 vCenter Server 記錄中的下列訊息：

```
No cached identity key, loading from DB
```

此訊息指出您正在將 TPM 2.0 晶片新增到已由 vCenter Server 管理的 ESXi 主機。您必須先中斷主機連線，再重新連線。如需中斷連線和重新連線主機的相關資訊，請參閱 *vCenter Server 和主機管理*說明文件。

4 如需所有其他錯誤訊息，請連絡客戶支援部門。

ESXi 記錄檔

記錄檔為對攻擊進行疑難排解和取得缺口相關資訊的一個重要元件。記錄到安全、集中的記錄伺服器，可協助防止記錄竄改。遠端記錄也能提供長期的稽核記錄。

若要提高主機的安全性，請採取下列措施

- 設定持續性記錄到資料存放區。依預設，ESXi 主機上的記錄儲存於記憶體中的檔案系統中。因此，當您將主機重新開機時，記錄將會遺失，並且僅儲存 24 小時的記錄資料。啟用持續性記錄時，您會有用於主機的專用活動記錄。
- 遠端記錄到中央主機可讓您收集中央主機上的記錄檔。您可從該主機使用單一工具監控所有主機、執行彙總分析和搜尋記錄資料。這種方法可協助監控，並顯示對多台主機的協調攻擊的相關資訊。
- 透過使用 CLI (如 vCLI 或 PowerCLI) 或透過使用 API 用戶端在 ESXi 主機上設定遠端安全 Syslog。
- 查詢 Syslog 組態，確保 Syslog 伺服器和連接埠有效。

如需有關 Syslog 設定的資訊以及 ESXi 記錄檔的其他相關資訊，請參閱 *vSphere 監控和效能*說明文件。

在 ESXi 主機上設定 Syslog

您可以使用 vSphere Web Client 或 `esxcli system syslog` vCLI 命令來設定 syslog 服務。

如需使用 `esxcli system syslog` 命令和其他 vCLI 命令的相關資訊，請參閱 *vSphere Command-Line Interface 入門*。

程序

1 在 vSphere Web Client 詳細目錄中，選取主機。

2 按一下**設定**。

3 在 [系統] 下，按一下**進階系統設定**。

4 篩選 **`syslog`**。

5 若要全域設定記錄，請選取要變更的設定，然後按一下**編輯**。

選項	說明
Syslog.global.defaultRotate	要保留的封存數目上限。可全域設定該數目，也可針對個別子記錄器進行設定。
Syslog.global.defaultSize	系統輪替記錄前記錄的預設大小 (以 KB 為單位)。可全域設定該數目，也可針對個別子記錄器進行設定。

選項	說明
Syslog.global.LogDir	儲存記錄的目錄。該目錄可能位於掛接的 NFS 或 VMFS 磁碟區中。只有本機檔案系統中的 `/scratch` 目錄在重新開機後仍會存在。將目錄指定為 [*datastorename*] *path_to_file*，其中路徑相對於支援資料存放區的磁碟區的根目錄路徑。例如，路徑 `[storage1] /systemlogs` 會對應到路徑 `/vmfs/volumes/storage1/systemlogs`。
Syslog.global.logDirUnique	若選取此選項，將會使用 ESXi 主機的名稱，在 **Syslog.global.LogDir** 指定的目錄下建立子目錄。如果有多個 ESXi 主機使用同一個 NFS 目錄，則唯一的目錄非常有用。
Syslog.global.LogHost	Syslog 訊息轉送到的遠端主機，以及該遠端主機接收 Syslog 訊息所在的連接埠。可以包含通訊協定和連接埠，例如 `ssl://hostName1:1514`。支援 UDP (僅位於連接埠 514 上)、TCP 和 SSL。遠端主機必須安裝並正確設定 Syslog，才能接收轉送的 Syslog 訊息。如需組態的相關資訊，請參閱遠端主機上所安裝 Syslog 服務的說明文件。

6 (選用) 覆寫任何記錄的預設記錄大小和記錄輪替。

a 按一下您要自訂的記錄的名稱。

b 按一下**編輯**，然後輸入所需的輪替次數和記錄大小。

7 按一下**確定**。

對 Syslog 選項進行的變更會立即生效。

ESXi 記錄檔位置

ESXi 透過使用 Syslog 功能，在記錄檔中記錄主機活動。

元件	位置	用途
VMkernel	`/var/log/vmkernel.log`	記錄與虛擬機器以及 ESXi 有關的活動。
VMkernel 警告	`/var/log/vmkwarning.log`	記錄與虛擬機器有關的活動。
VMkernel 摘要	`/var/log/vmksummary.log`	用於判定 ESXi 的運作時間和可用性統計資料 (以逗號分隔)。
ESXi 主機代理程式記錄	`/var/log/hostd.log`	包含管理和設定 ESXi 主機及其虛擬機器的代理程式的相關資訊。
vCenter 代理程式記錄	`/var/log/vpxa.log`	包含與 vCenter Server 通訊的代理程式的相關資訊 (如果主機由 vCenter Server 管理)。
Shell 記錄	`/var/log/shell.log`	包含輸入 ESXi Shell 的所有命令以及 Shell 事件 (例如，啟用 Shell) 的記錄。
驗證	`/var/log/auth.log`	包含與本機系統驗證相關的所有事件。

元件	位置	用途
系統訊息	`/var/log/syslog.log`	包含所有一般記錄訊息，並且可用來進行疑難排解。該資訊之前位於訊息記錄檔中。
虛擬機器	與受影響的虛擬機器的組態檔 (命名為 vmware.log 和 vmware*.log) 具有相同的目錄。例如，`/vmfs/volumes/datastore/virtual machine/vwmare.log`	包含虛擬機器電源事件、系統失敗資訊、工具狀態和活動、時間同步、虛擬硬體變更、vMotion 移轉和虛擬機器複製等。

確保 Fault Tolerance 記錄流量的安全

VMware Fault Tolerance (FT) 可擷取主要虛擬機器上發生的輸入和事件，並將這些輸入和事件傳送到正在另一台主機上執行的次要虛擬機器。

主要和次要虛擬機器之間的記錄流量未加密，並且包含客體網路和 Storage I/O 資料，以及客體作業系統的記憶體內容。此流量可能包含敏感資料，如純文字格式的密碼。若要避免此類資料的洩漏，請確保此網路的安全，特別是避免受到攔截式攻擊。例如，將私人網路用於 FT 記錄流量。

保護 vCenter Server 系統的安全

4

保護 vCenter Server 的安全包括：確認執行 vCenter Server 的主機的安全性、遵循指派權限和角色的最佳做法，以及確認連線到 vCenter Server 的用戶端完整性。

本章節討論下列主題:

vCenter Server 安全性最佳做法

遵循 vCenter Server 安全性最佳做法可協助確保 vSphere 環境的完整性。

vCenter Server 存取控制的最佳做法

嚴格控制不同 vCenter Server 元件的存取權，以提高系統的安全性。

下列準則可協助確保環境的安全性。

使用具名帳戶

- 如果目前本機 Windows 管理員帳戶具有 vCenter Server 的管理員角色，請移除該角色並將該角色指派給一或多個具名 vCenter Server 管理員帳戶。將管理員角色僅授與需要擁有該角色的管理員。對於擁有較多限制權限的管理員，您可以建立自訂角色或使用無密碼編譯管理員角色。請勿將此角色套用到其成員資格未受到嚴格控制的任何群組。

  備註 從 vSphere 6.0 開始，本機管理員預設不再具有 vCenter Server 的完整管理權限。

- 使用服務帳戶而不使用 Windows 帳戶安裝 vCenter Server。服務帳戶必須是本機電腦上的管理員。
- 確保應用程式在連線至 vCenter Server 系統時使用唯一服務帳戶。

監控 vCenter Server 管理員使用者的權限

並非所有管理員使用者都必須具有管理員角色。相反，可以建立具有一組適當權限的自訂角色，然後將其指派給其他管理員。

具有 vCenter Server 管理員角色的使用者擁有階層中所有物件的權限。例如，依預設，管理員角色可讓使用者與虛擬機器客體作業系統內的檔案和程式進行互動。將該角色指派給過多的使用者可能會降低虛擬機器資料的機密性、可用性或完整性。建立一個能夠為管理員提供所需權限，而不是移除部分虛擬機器管理權限的角色。

最小化存取權

請勿允許使用者直接登入 vCenter Server 主機。已登入 vCenter Server 主機的使用者可能會因更改設定和修改程序而有意或無意地造成傷害。這些使用者還可以存取 vCenter 認證，例如 SSL 憑證。僅允許要執行合法工作的使用者登入系統，並確保對這些登入事件進行稽核。

為 vCenter Server 資料庫使用者授與最低權限

資料庫使用者僅需要專屬於資料庫存取權的特定權限。

某些權限僅在安裝和升級時需要。您可以在安裝或升級 vCenter Server 後，從資料庫管理員移除這些權限。

限制資料存放區瀏覽器存取權

僅將**資料存放區.瀏覽資料存放區**權限指派給真正需要這些權限的使用者或群組。具有權限的使用者可以透過網頁瀏覽器或 vSphere Web Client 檢視、上傳或下載資料存放區上與 vSphere 部署相關聯的檔案。

限制使用者在虛擬機器中執行命令

依預設，具有 vCenter Server 管理員角色的使用者可與虛擬機器客體作業系統內的檔案和程式進行互動。若要降低破壞客體機密性、可用性或完整性的風險，請建立沒有**客體作業**權限的自訂非客體存取角色。請參閱限制使用者在虛擬機器中執行命令。

考量修改 vpxuser 的密碼原則

依預設，vCenter Server 每 30 天自動變更一次 vpxuser 密碼。請確保此設定符合公司原則，或設定 vCenter Server 密碼原則。請參閱設定 vCenter Server 密碼原則。

備註 確保密碼使用期限原則不會過短。

在 vCenter Server 重新啟動後檢查權限

重新啟動 vCenter Server 時應檢查權限重新指派。如果在重新啟動期間無法驗證在根資料夾上具有管理員角色的使用者或群組，則角色會從該使用者或群組中移除。vCenter Server 會改為將管理員角色授與 vCenter Single Sign-On 管理員 (依預設為 administrator@vsphere.local) 代替。此帳戶即可充當 vCenter Server 管理員。

重新建立具名管理員帳戶，然後將管理員角色指派給該帳戶以避免使用匿名 vCenter Single Sign-On 管理員帳戶 (依預設為 administrator@vsphere.local)。

使用高 RDP 加密層級

在基礎結構中的每台 Windows 電腦上，請確定已設定 [遠端桌面主機組態] 設定，以確保適用於環境的最高加密層級。

驗證 vSphere Web Client 憑證

指示其中一個 vSphere Web Client 或其他用戶端應用程式的使用者絕不忽略憑證驗證警告。在沒有憑證驗證的情況下，使用者可能會受到 MiTM 攻擊。

設定 vCenter Server 密碼原則

依預設，vCenter Server 每 30 天自動變更一次 vpxuser 密碼。您可以從 vSphere Web Client 中變更該值。

程序

1. 使用 vSphere Web Client 登入 vCenter Server 系統。
2. 在物件階層中，選取 vCenter Server 系統。
3. 按一下**設定**。
4. 按一下**進階設定**，然後在篩選器方塊中輸入 **VimPasswordExpirationInDays**。
5. 設定 `VirtualCenter.VimPasswordExpirationInDays` 以符合您的需求。

從失敗的安裝移除到期或撤銷的憑證和記錄

在 vCenter Server 系統上保留到期或撤銷的憑證，或保留已失敗安裝的 vCenter Server 安裝記錄可能會影響您的環境。

出於以下原因，需要移除到期或撤銷的憑證。

- 如果不從 vCenter Server 系統移除到期或撤銷的憑證，環境可能會受到 MiTM 攻擊
- 在某些情況下，如果 vCenter Server 安裝失敗，則會在系統上建立一個包含純文字資料庫密碼的記錄檔。闖入 vCenter Server 系統的攻擊者可能會存取此密碼，並同時存取 vCenter Server 資料庫。

保護 vCenter Server Windows 主機

透過盡可能地確保主機環境的安全，保護 vCenter Server 所執行的 Windows 主機使其免遭漏洞和攻擊。

- 為 vCenter Server 系統維護受支援的作業系統、資料庫和硬體。如果 vCenter Server 不是在受支援的作業系統上執行，則可能無法正常執行，從而使 vCenter Server 容易受到攻擊。
- 使 vCenter Server 系統得到正確修補。透過及時更新最新版本的作業系統修補程序，可讓 vCenter Server 不那麼容易受到攻擊。
- 在 vCenter Server 主機上提供作業系統保護。提供的保護包含防毒軟體和防惡意軟體。
- 在基礎結構中的每台 Windows 電腦上，請確保已按照業界標準的指導方針或內部指導方針設定了 [遠端桌面 (RDP) 主機組態] 設定，以保證最高層級的加密。

如需作業系統和資料庫相容性的資訊，請參閱《vSphere 相容性對照表》*vSphere 相容性矩陣圖*。

限制 vCenter Server 的網路連線

為提高安全性，請避免將 vCenter Server 系統置於管理網路之外的任何網路上，並確保 vSphere 管理流量位於受限制的網路。透過限制網路連線，可以限制特定類型的攻擊。

vCenter Server 僅需要存取管理網路。避免將 vCenter Server 系統置於其他網路 (如生產網路或儲存區網路) 或有權存取網際網路的任何網路。vCenter Server 不需要存取 vMotion 在其中運作的網路。

vCenter Server 需要與以下系統建立網路連線。

- 所有 ESXi 主機。
- vCenter Server 資料庫。
- 其他 vCenter Server 系統 (如果 vCenter Server 系統屬於用於複寫標籤、權限等的一般 vCenter Single Sign-On 網域)。
- 有權執行管理用戶端的系統。例如，vSphere Web Client，即您在其中使用 PowerCLI 的 Windows 系統，或任何其他以 SDK 為基礎的用戶端。
- 執行附加元件 (例如 VMware vSphere Update Manager) 的系統。
- 基礎結構服務，如 DNS、Active Directory 和 NTP。
- 執行對 vCenter Server 系統功能至關重要的元件的其他系統。

使用執行 vCenter Server 系統的 Windows 系統上的本機防火牆，或使用網路防火牆。包括以 IP 為基礎的存取限制，這樣只有必要的元件才能與 vCenter Server 系統通訊。

評估 Linux 用戶端搭配 CLI 和 SDK 的使用情況

依預設，用戶端元件與 vCenter Server 系統或 ESXi 主機之間的通訊由基於 SSL 的加密進行保護。這些元件的 Linux 版本不執行憑證驗證。請考慮限制這些用戶端的使用。

為提升安全性，您可以使用由企業或第三方 CA 簽署的憑證取代 vCenter Server 系統和 ESXi 主機上 VMCA 簽署的憑證。但是，與 Linux 用戶端的某些通訊可能仍然容易受到攔截式攻擊。以下元件在 Linux 作業系統上執行時容易受到攻擊。

- vCLI 命令
- vSphere SDK for Perl 指令碼
- 使用 vSphere Web Services SDK 撰寫的程式

如果強行執行適當的控制，則可放寬對使用 Linux 用戶端的限制。

- 僅限制管理網路對授權系統的存取。
- 使用防火牆確保僅允許授權主機存取 vCenter Server。
- 使用跳躍方塊系統確保 Linux 用戶端受跳躍限制。

檢查 vSphere Web Client 外掛程式

vSphere Web Client 延伸在與登入使用者相同的權限層級下執行。惡意延伸可以偽裝成有用的外掛程式並執行有害的作業，例如竊取認證或變更系統組態。若要增強安全性，請使用僅包括來自受信任來源的授權延伸的 vSphere Web Client 安裝。

vCenter 安裝包括 vSphere Web Client 可延伸性架構。您可以使用此架構透過功能表選取項目或工具列圖示來延伸 vSphere Web Client。延伸可提供對 vCenter 附加元件或外部以 Web 為基礎之功能的存取權。

使用可延伸性架構會導致引入誤用功能的風險。例如，如果管理員在 vSphere Web Client 的一個執行個體中安裝外掛程式，則該外掛程式可以使用該管理員的權限層級執行任意命令。

若要保護 vSphere Web Client 免受潛在的危害，請定期檢查所有已安裝的外掛程式，並確保所有外掛程式均來自受信任的來源。

先決條件

您必須具有存取 vCenter Single Sign-On 服務的權限。這些權限與 vCenter Server 權限不同。

程序

1. 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 權限的使用者身分登入 vSphere Web Client。
2. 在首頁上，選取**管理**，然後選取**解決方案**下的**用戶端外掛程式**
3. 檢查用戶端外掛程式清單。

vCenter Server Appliance 安全性最佳做法

請遵循所有最佳做法，以保護 vCenter Server 系統安全，從而保護您的 vCenter Server Appliance。額外步驟更有助於您保護應用裝置的安全。

設定 NTP	確保所有系統使用相同的相對時間來源。此時間來源必須與商定的時間標準 (如國際標準時間 (UTC)) 同步。同步的系統對於憑證驗證來說至關重要。NTP 還可讓您更輕鬆地追蹤記錄檔中的侵入者。不正確的時間設定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。請參閱將 vCenter Server Appliance 與 NTP 伺服器的時間同步。
限制 vCenter Server Appliance 網路存取	限制對與 vCenter Server Appliance 進行通訊所需元件的存取。封鎖來自不必要系統的存取可降低對作業系統發動攻擊的潛在可能性。請參閱 vCenter Server 與 Platform Services Controller 所需的連接埠和其他 vCenter Server TCP 和 UDP 連接埠。遵循 VMware 知識庫文章 https://kb.vmware.com/s/article/2047585 中的準則，使用與 DISA STIG 相符的防火牆設定來設定您的環境。

vCenter 密碼需求與鎖定行為

若要管理您的 vSphere 環境，您必須瞭解 vCenter Single Sign-On 密碼原則、vCenter Server 密碼以及鎖定行為。

本節討論 vCenter Single Sign-On 密碼。如需 ESXi 本機使用者的密碼的討論，請參閱 ESXi 密碼及帳戶鎖定。

vCenter Single Sign-On 管理員密碼

vCenter Single Sign-On 管理員 (預設為 administrator@vsphere.local) 的密碼由 vCenter Single Sign-On 密碼原則指定。依預設，此密碼必須符合下列需求：

- 至少 8 個字元
- 至少一個小寫字元
- 至少一個數字字元
- 至少一個特殊字元

該使用者的密碼長度不得超過 20 個字元。從 vSphere 6.0 開始，不允許使用非 ASCII 字元。管理員可以變更預設密碼原則。請參閱 *Platform Services Controller 管理*說明文件。

vCenter Server 密碼

在 vCenter Server 中，密碼需求由 vCenter Single Sign-On 或設定的身分識別來源決定，這些設定的身分識別來可以是 Active Directory 或 OpenLDAP。

vCenter Single Sign-On 鎖定行為

在連續嘗試失敗預設次數後，使用者會被鎖定。依預設，在三分鐘內連續嘗試失敗五次後，使用者會被鎖定，並且五分鐘後，系統會自動解除鎖定被鎖定的帳戶。您可以使用 vCenter Single Sign-On 鎖定原則變更這些預設值。請參閱 *Platform Services Controller 管理*說明文件。

從 vSphere 6.0 開始，vCenter Single Sign-On 網域管理員 (預設為 administrator@vsphere.local) 不會受鎖定原則影響。使用者受密碼原則影響。

密碼變更

如果您知道密碼，可以透過使用 `dir-cli password change` 命令變更密碼。如果您忘記密碼，vCenter Single Sign-On 管理員可以透過使用 `dir-cli password reset` 命令重設您的密碼。

如需有關不同版本 vSphere 中密碼到期及相關主題的資訊，請搜尋 VMware 知識庫。

驗證舊版 ESXi 主機的指紋

在 vSphere 6 及更新版本中，依預設會向主機指派 VMCA 憑證。如果您將憑證模式變更為指紋，則可以繼續針對舊版主機使用指紋模式。您可以在 vSphere Web Client 中驗證指紋。

備註 依預設，會在各升級中保留憑證。

程序

1. 在 vSphere Web Client 物件導覽器中，瀏覽到 vCenter Server 系統。
2. 按一下**設定**。
3. 在**設定**下，按一下**一般**。
4. 按一下**編輯**。
5. 按一下 **SSL 設定**。
6. 如果有需要手動驗證的 ESXi 5.5 或更早版本的主機，請比較主機列出的指紋和主機主控台中的指紋。

   若要取得主機憑證指紋，請使用 Direct Console 使用者介面 (DCUI)。

   a 登入 Direct Console 並按 F2，存取 [系統自訂] 功能表。

   b 選取**檢視支援資訊**。

   主機憑證指紋會出現在右側資料行中。
7. 如果指紋相符，則選取主機旁邊的**確認**核取方塊。

   按一下**確定**之後，未選取的主機將中斷連線。
8. 按一下**確定**。

確認已對網路檔案複製啟用 SSL 憑證驗證

網路檔案複製 (NFC) 可為 vSphere 元件提供檔案類型感知 FTP 服務。從 vSphere 5.5 開始，ESXi 預設會使用 NFC 執行作業，例如在資料存放區之間複製和移動資料，如果它處於停用狀態，您可能需要將其啟用。

如果 [透過 NFC 啟用 SSL] 已啟用，則透過 NFC 在 vSphere 元件之間建立的連線便能確保安全。此連線有助於防止資料中心內受到攔截式攻擊。

由於透過 SSL 使用 NFC 會造成效能降低，因此在某些開發環境中您可能會考慮停用此進階設定。

備註 如果正在使用指令碼檢查值，將此值明確設定為 true。

程序

1 使用 vSphere Web Client 連線到 vCenter Server。

2 按一下**設定**。

3 按一下**進階設定**，然後在對話方塊底部輸入下列金鑰和值。

欄位	值
索引鍵	config.nfc.useSSL
值	true

4 按一下**確定**。

vCenter Server 與 Platform Services Controller 所需的連接埠

位於 Windows 上和應用裝置中的 vCenter Server 系統必須能夠將資料傳送至每台受管理的主機，並接收來自 vSphere Web Client 和 Platform Services Controller 服務的資料。若要在受管理主機間啟用移轉和佈建活動，來源主機和目的地主機必須能夠彼此接收資料。

如果某個連接埠處於使用中狀態或被列入黑名單，vCenter Server 安裝程式會顯示一則錯誤訊息。您必須使用其他連接埠號碼才能繼續安裝。存在僅用於程序間通訊的內部連接埠。

VMware 使用指定的連接埠進行通訊。此外，受管理主機會在指定的連接埠上監控來自 vCenter Server 的資料。如果其中任何元素之間存在內建防火牆，則安裝程式會在執行安裝或升級程序期間開啟連接埠。對於自訂防火牆，您必須手動開啟所需的連接埠。如果您在兩台受管理主機之間設有防火牆，並且您想要在來源或目標主機上執行活動 (如移轉或複製)，則必須設定受管理主機接收資料的方式。

備註 在 Microsoft Windows Server 2008 及更新版本中，防火牆預設為啟用。

表格 4-1. 元件之間的通訊所需的連接埠

連接埠	通訊協定	說明	所需	用於節點到節點通訊
22	TCP	SSHD 的系統連接埠。	應用裝置部署 ■ vCenter Server ■ Platform Services Controller	否
53		DNS 服務	Platform Services Controller 的 Windows 安裝與應用裝置部署	否
80	TCP	vCenter Server 需要使用連接埠 80 進行直接 HTTP 連線。連接埠 80 會將要求重新導向到 HTTPS 連接埠 443。如果不小心使用了 http://server 而非 https://server，此重新導向會非常有用。 WS 管理 (也需要開啟連接埠 443)。 如果使用與 vCenter Server 儲存在同一虛擬機器或實體伺服器上的 Microsoft SQL 資料庫，SQL Reporting 服務會使用連接埠 80。安裝或升級 vCenter Server 時，安裝程式會提示您變更 vCenter Server 的 HTTP 連接埠。請將 vCenter ServerHTTP 連接埠變更為自訂值來確保成功安裝或升級。 **重要事項** 您只能在 vCenter Server 和 Platform Services Controller 安裝期間變更此連接埠號碼。	Windows 安裝與應用裝置部署 ■ vCenter Server ■ Platform Services Controller	否
88	TCP	Active Directory 伺服器。必須為要加入 Active Directory 的主機開啟此連接埠。如果您使用原生 Active Directory，vCenter Server 和 Platform Services Controller 均須開啟該連接埠。	Platform Services Controller 的 Windows 安裝與應用裝置部署	否
389	TCP/UDP	此連接埠在 vCenter Server 的本機和所有遠端執行個體上必須處於開啟狀態。這是 vCenter Server 群組之目錄服務的 LDAP 連接埠號碼。如果有其他服務在此連接埠上執行，最好移除該服務或將該服務的連接埠變更為其他連接埠。您可以在 1025 到 65535 之間的任一連接埠上執行 LDAP 服務。 如果此執行個體充當 Microsoft Windows Active Directory，請將連接埠號碼從 389 變更為 1025 到 65535 之間的任一可用連接埠。	Platform Services Controller 的 Windows 安裝與應用裝置部署	■ vCenter Server 至 Platform Services Controller ■ Platform Services Controller 至 Platform Services Controller

表格 4-1. 元件之間的通訊所需的連接埠 (繼續)

連接埠	通訊協定	說明	所需	用於節點到節點通訊
443	TCP	vCenter Server 系統用於接聽來自 vSphere Web Client 的連線的預設連接埠。若要使 vCenter Server 系統能夠從 vSphere Web Client 接收資料，請在防火牆中開啟連接埠 443。 vCenter Server 系統也使用連接埠 443 監控來自 SDK 用戶端的資料傳輸。 此連接埠也用於下列服務： ■ WS 管理 (也需要開啟連接埠 80) ■ 第三方網路管理用戶端與 vCenter Server 的連線 ■ 第三方網路管理用戶端對主機的存取 **重要事項** 您只能在 vCenter Server 和 Platform Services Controller 安裝期間變更此連接埠號碼。	Windows 安裝與應用裝置部署 ■ vCenter Server ■ Platform Services Controller	■ vCenter Server 至 vCenter Server ■ vCenter Server 至 Platform Services Controller ■ Platform Services Controller 至 vCenter Server
514	TCP/UDP	用於 Windows 上 vCenter Server 的 vSphere Syslog Collector 連接埠以及用於 vCenter Server Appliance 的 vSphere Syslog 服務連接埠 **重要事項** 在 Windows 上執行 vCenter Server 與 Platform Services Controller 安裝期間，可以變更此連接埠號碼。	Windows 安裝與應用裝置部署 ■ vCenter Server ■ Platform Services Controller	否
636	TCP	vCenter Single Sign-On LDAPS 僅與 vSphere 6.0 回溯相容。	Platform Services Controller 的 Windows 安裝與應用裝置部署	僅限從 vSphere 6.0 升級期間。 vCenter Server6.0 至 Platform Services Controller 6.5
902	TCP/UDP	vCenter Server 系統用於將資料傳送到受管理主機的預設連接埠。受管理的主機也會透過 UDP 連接埠 902 定期向 vCenter Server 系統傳送活動訊號。伺服器和主機之間或各主機之間的防火牆不得封鎖此連接埠。 不得在 VMware Host Client 和主機之間封鎖連接埠 902。VMware Host Client 使用此連接埠顯示虛擬機器主控台 **重要事項** 在 Windows 上執行 vCenter Server 安裝期間，可以變更此連接埠號碼。	vCenter Server 的 Windows 安裝與應用裝置部署	否

表格 4-1. 元件之間的通訊所需的連接埠 (繼續)

連接埠	通訊協定	說明	所需	用於節點到節點通訊
1514	TCP	用於 Windows 上 vCenter Server 的 vSphere Syslog Collector TLS 連接埠以及用於 vCenter Server Appliance 的 vSphere Syslog 服務 TLS 連接埠 **重要事項** 在 Windows 上執行 vCenter Server 與 Platform Services Controller 安裝期間，可以變更此連接埠號碼。	Windows 安裝與應用裝置部署 ■ vCenter Server ■ Platform Services Controller	否
2012	TCP	vCenter Single Sign-On 的控制介面 RPC	Platform Services Controller 的 Windows 安裝與應用裝置部署	■ vCenter Server 至 Platform Services Controller ■ Platform Services Controller 至 vCenter Server ■ Platform Services Controller 至 Platform Services Controller
2014	TCP	所有 VMCA (VMware Certificate Authority) API 的 RPC 連接埠 **重要事項** 在 Windows 上執行 Platform Services Controller 安裝期間，可以變更此連接埠號碼。	Platform Services Controller 的 Windows 安裝與應用裝置部署	■ vCenter Server 至 Platform Services Controller ■ Platform Services Controller 至 vCenter Server
2015	TCP	DNS 管理	Platform Services Controller 的 Windows 安裝與應用裝置部署	Platform Services Controller 至 Platform Services Controller
2020	TCP/UDP	驗證架構管理 **重要事項** 在 Windows 上執行 vCenter Server 與 Platform Services Controller 安裝期間，可以變更此連接埠號碼。	Windows 安裝與應用裝置部署 ■ vCenter Server ■ Platform Services Controller	■ vCenter Server 至 Platform Services Controller ■ Platform Services Controller 至 vCenter Server
5480	TCP	應用裝置管理介面 開啟透過 HTTPS 為所有 HTTPS、XMLRPS 和 JSON-RPC 要求提供服務的端點。	應用裝置部署 ■ vCenter Server ■ Platform Services Controller	否
6500	TCP/UDP	ESXi Dump Collector 連接埠 **重要事項** 在 Windows 上執行 vCenter Server 安裝期間，可以變更此連接埠號碼。	vCenter Server 的 Windows 安裝與應用裝置部署	否

表格 4-1. 元件之間的通訊所需的連接埠 (繼續)

連接埠	通訊協定	說明	所需	用於節點到節點通訊
6501	TCP	Auto Deploy 服務 **重要事項** 在 Windows 上執行 vCenter Server 安裝期間，可以變更此連接埠號碼。	vCenter Server 的 Windows 安裝與應用裝置部署	否
6502	TCP	Auto Deploy 管理 **重要事項** 在 Windows 上執行 vCenter Server 安裝期間，可以變更此連接埠號碼。	vCenter Server 的 Windows 安裝與應用裝置部署	否
7080、12721	TCP	安全 Token 服務 **備註** 內部連接埠	Platform Services Controller 的 Windows 安裝與應用裝置部署	否
7081	TCP	VMware Platform Services Controller Web 用戶端 **備註** 內部連接埠	Platform Services Controller 的 Windows 安裝與應用裝置部署	否
8200、8201、8300、8301	TCP	應用裝置管理 **備註** 內部連接埠	應用裝置部署 ■ vCenter Server ■ Platform Services Controller	否
8084	TCP	vSphere Update Manager SOAP 連接埠 vSphere Update Manager Client 外掛程式用於連線至 vSphere Update Manager SOAP Server 的連接埠。	vCenter Server 的應用裝置部署	否
9084	TCP	vSphere Update Manager Web 伺服器連接埠 ESXi 主機用於從 vSphere Update Manager 伺服器存取主機修補程式檔案的 HTTP 連接埠。	vCenter Server 的應用裝置部署	否
9087	TCP	vSphere Update Manager Web SSL 連接埠 vSphere Update Manager Client 外掛程式用於將主機升級檔案上傳至 vSphere Update Manager 伺服器的 HTTPS 連接埠。	vCenter Server 的應用裝置部署	否
9443	TCP	vSphere Web ClientHTTPS	vCenter Server 的 Windows 安裝與應用裝置部署	否

若要將 vCenter Server 系統設定為使用不同的連接埠來接收 vSphere Web Client 資料，請參閱 *vCenter Server 和主機管理*說明文件。

其他 vCenter Server TCP 和 UDP 連接埠

vCenter Server 可透過預先決定的 TCP 和 UDP 連接埠進行存取。若要從防火牆之外管理網路元件，您可能需要重新設定防火牆，允許在適當連接埠進行存取。

vCenter Server 與 Platform Services Controller 所需的連接埠會列出安裝程式所開啟的連接埠，做為預設安裝的一部分。部分服務需要一些其他連接埠，例如 NTP，或通常與 vCenter Server 一起安裝的應用程式。

除了這些連接埠之外，您可以根據需要設定其他連接埠。

表格 4-2. vCenter Server TCP 和 UDP 連接埠

連接埠	通訊協定	說明
123 (UDP)	UDP	NTP 用戶端。如果您要在 ESXi 主機上部署 vCenter Server Appliance，這兩者必須同步時間 (通常是透過 NTP 伺服器) 且開啟對應的連接埠。
135	UDP	對於 vCenter Server Appliance，此連接埠是針對 Active Directory 驗證而指定。 對於 vCenter Server Windows 安裝，此連接埠用於連結模式，連接埠 88 用於 Active Directory 驗證。
161	UDP	SNMP 伺服器。
636	TCP	vCenter Single Sign-On LDAPS (6.0 及更新版本)
8084, 9084, 9087	TCP	由 vSphere Update Manager 所使用。
8109	TCP	VMware Syslog Collector。如果您要集中記錄收集，則需要此服務。
15007, 15008	TCP	vService Manager (VSM)。此服務將登錄 vCenter Server 延伸。僅當您打算使用的延伸需要時，才會開啟此連接埠。
31031 、 44046 (預設)	TCP	vSphere Replication。
5355	UDP	systemd-resolve 程序會使用此連接埠，以解析網域名稱、IPv4 和 IPv6 位址、DNS 資源記錄和服務。

下列連接埠僅在內部使用。

表格 4-3. vCenter Server TCP 和 UDP 連接埠

連接埠	說明
5443	vCenter Server 圖形化使用者介面內部連接埠。
5444, 5432	用於監控 vPostgreSQL 的內部連接埠。
5090	vCenter Server 圖形化使用者介面內部連接埠。
7080	安全 Token 服務內部連接埠。
7081	Platform Services Controller 內部連接埠。
8000	ESXi Dump Collector 內部連接埠。
8006	用於 Virtual SAN 健全狀況監控。

表格 4-3. vCenter Server TCP 和 UDP 連接埠 (繼續)

連接埠	說明
8085	vCenter 服務 (vpxd) SDK 所使用的內部連接埠。
8095	VMware vCenter 服務摘要連接埠。
8098, 8099	由 VMware Image Builder Manager 所使用。
8190, 8191, 22000, 22100, 21100	VMware vSphere Profile-Driven Storage Service。
8200, 8201, 5480	應用裝置管理內部連接埠。
8300, 8301	應用裝置管理保留的連接埠。
8900	監控 API 內部連接埠。
9090	vSphere Web Client 的內部連接埠。
10080	Inventory Service 內部連接埠
10201	訊息匯流排組態服務內部連接埠。
11080	用於 HTTP 和啟動顯示畫面的 vCenter Server Appliance 內部連接埠。
12721	安全 Token 服務內部連接埠。
12080	授權服務內部連接埠。
12346, 12347, 4298	用於 VMware Cloud Management SDK (vAPI) 的內部連接埠。
13080, 6070	由效能圖服務在內部使用。
14080	由 Syslog 服務在內部使用。
15005, 15006	ESX Agent Manager 內部連接埠。
16666, 16667	內容程式庫連接埠。
18090	Content Manager 內部連接埠。
18091	Component Manager 內部連接埠。

此外，vCenter Server Appliance 針對 vPostgres 服務使用 32768 到 60999 之間的暫時連接埠。

vCenter High Availability (VCHA) 節點之間需要下列連接埠。

表格 4-4. VCHA 私人 IP 的防火牆連接埠需求

連接埠	通訊協定	節點	說明
22	TCP	在所有三個節點之間 (雙向)。	SSHD 的系統連接埠
5432	TCP	在主要和次要節點之間 (雙向)。	Postgres
8182	TCP	在所有三個節點之間 (雙向)。	Fault Domain Manager
8182	UDP	在所有三個節點之間 (雙向)。	Fault Domain Manager

確保虛擬機器安全

5

在虛擬機器中執行的客體作業系統會與實體系統一樣，遭遇相同的安全性風險。確保虛擬機器安全如同實體機器一樣，並遵循該文件和《*強化指南*》中論述的最佳做法。

本章節討論下列主題:

對虛擬機器啟用或停用 UEFI 安全開機

UEFI 安全開機是一種安全性標準，可協助確保您的電腦僅使用電腦製造商信任的軟體進行開機。對於某些虛擬機器硬體版本和作業系統，可以和實體機器一樣，為其啟用安全開機。

在支援 UEFI 安全開機的作業系統上，開機軟體的每個部分均已簽署，包括開機載入器、作業系統核心和作業系統驅動程式。虛擬機器的預設組態包括多個代碼簽署憑證。

- 僅用於將 Windows 開機的 Microsoft 憑證。
- 用於 Microsoft 簽署之第三方代碼的 Microsoft 憑證，例如 Linux 開機載入器。
- 僅用於將虛擬機器內的 ESXi 開機的 VMware 憑證。

虛擬機器的預設組態包含一個憑證，用於從虛擬機器內驗證修改安全開機組態 (包括安全開機撤銷清單) 的申請，它是一個 Microsoft KEK (金鑰交換金鑰) 憑證。

在幾乎所有情況下，沒有必要取代現有憑證。如果想要取代憑證，請參閱 VMware 知識庫系統。

對於使用 UEFI 安全開機的虛擬機器，需要 VMware Tools 10.1 版或更新版本。您可以將這些虛擬機器升級到較新版本的 VMware Tools (當其可用時)。

對於 Linux 虛擬機器，VMware 主機-客體檔案系統在安全開機模式下不受支援。請先從 VMware Tools 移除 VMware 主機-客體檔案系統，然後再啟用安全開機。

備註 如果您對虛擬機器開啟安全開機，則只能將已簽署的驅動程式載入該虛擬機器。

先決條件

僅在符合所有必要條件時，才能啟用安全開機。如果不符合必要條件，vSphere Client 中將不會顯示此核取方塊。

- 確認虛擬機器作業系統和韌體支援 UEFI 開機。
  - EFI 韌體
  - 虛擬硬體版本 13 或更新版本。
  - 支援 UEFI 安全開機的作業系統。

  備註 您無法將使用 BIOS 開機的虛擬機器升級到使用 UEFI 開機的虛擬機器。如果您將已使用 UEFI 開機的虛擬機器升級到支援 UEFI 安全開機的作業系統，則可以對此虛擬機器啟用安全開機。
- 關閉虛擬機器。如果虛擬機器正在執行，則此核取方塊會以灰色顯示。

程序

1. 在詳細目錄中的虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
2. 按一下**虛擬機器選項**索引標籤，然後展開**開機選項**。
3. 在**開機選項**下，確保韌體設為 **EFI**。
4. 選取您的工作。選取**安全開機**核取方塊以啟用安全開機。然後按一下**確定**。
   - 選取**安全開機**核取方塊以啟用安全開機。
   - 取消選取**安全開機**核取方塊以停用安全開機。

當虛擬機器開機時，僅允許具有有效簽章的元件。如果元件的簽章遺失或無效，開機程序將停止並顯示錯誤。

限制資訊訊息從虛擬機器流向 VMX 檔案

限制資訊訊息從虛擬機器流向 VMX 檔案，從而避免填滿資料存放區和導致拒絕服務 (DoS)。如果您不控制虛擬機器的 VMX 檔案的大小，並且資訊量超過資料存放區容量，則會造成 DoS。

依預設，虛擬機器組態檔 (VMX 檔案) 限制是 1 MB。通常，此容量足夠；如有必要，您也可變更此值。例如，如果您將大量自訂資訊儲存在檔案中，您可能需要增加限制。

備註 請審慎考量需要的資訊量。如果資訊量超過資料存放區容量，則會造成 DoS。

即使進階選項中未列出 `tools.setInfo.sizeLimit` 參數，也會套用預設限制 1 MB。

程序

1. 使用 vSphere Web Client 登入 vCenter Server 系統並尋找虛擬機器。
   a. 在導覽器中，選取**虛擬機器和範本**。
   b. 在階層中尋找虛擬機器。

2 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。

3 選取**虛擬機器選項**。

4 按一下**進階**，然後按一下**編輯組態**。

5 新增或編輯 `tools.setInfo.sizeLimit` 參數。

防止虛擬磁碟壓縮

客體作業系統中的非管理使用者能夠壓縮虛擬磁碟。壓縮虛擬磁碟將回收未使用的磁碟空間。但是，如果重複壓縮虛擬磁碟，磁碟會變得無法使用且會導致拒絕服務。若要避免這種情況，請停用壓縮虛擬磁碟的功能。

先決條件

- 關閉虛擬機器。
- 確認您在虛擬機器上具備根權限或管理員權限。

程序

1 使用 vSphere Client 登入 vCenter Server 系統。

2 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。

3 選取**虛擬機器選項**。

4 按一下**進階**，然後按一下**編輯組態**。

5 新增或編輯下列參數。

名稱	值
`isolation.tools.diskWiper.disable`	TRUE
`isolation.tools.diskShrink.disable`	TRUE

6 按一下**確定**。

如果停用此功能，在資料存放區空間不足時，您將無法壓縮虛擬機器磁碟。

虛擬機器安全性最佳做法

遵循虛擬機器安全性最佳做法可協助確保 vSphere 部署的完整性。

- 虛擬機器一般保護

  在大多數情況下，虛擬機器等同於實體伺服器。在虛擬機器中採用與實體系統相同的安全措施。

- 使用範本部署虛擬機器

  在虛擬機器上手動安裝客體作業系統和應用程式時，會帶來錯誤組態的風險。透過使用範本擷取未安裝任何應用程式的強化基礎作業系統映像，您可以確保透過已知的安全性基準層級，建立所有虛擬機器。

- 儘量少用虛擬機器主控台

  虛擬機器主控台為虛擬機器提供的功能與實體伺服器上的監視器所提供的功能相同。具有虛擬機器主控台存取權限的使用者可存取虛擬機器電源管理和卸除式裝置連線能力控制項。因此，主控台存取可能造成對虛擬機器的惡意攻擊。

- 防止虛擬機器接管資源

  當某個虛擬機器耗用過多主機資源，而使主機上的其他虛擬機器無法執行其預期功能時，可能會出現拒絕服務 (DoS)。為防止虛擬機器造成 DoS 問題，請使用主機資源管理功能，例如設定共用率和使用資源集區。

- 停用虛擬機器中不必要的功能

  在虛擬機器中執行的任何服務都有可能引發攻擊。透過停用不是支援系統上執行的應用程式或服務所必需的系統元件，可降低受到攻擊的可能性。

虛擬機器一般保護

在大多數情況下，虛擬機器等同於實體伺服器。在虛擬機器中採用與實體系統相同的安全措施。

請遵循以下最佳做法來保護您的虛擬機器：

修補程式和其他保護

保持所有安全措施最新，包括套用適當的修補程式。追蹤已關閉電源的休眠虛擬機器中的更新特別重要，因為這些虛擬機器常常會被忽略。例如，確保對您虛擬基礎結構中的每台虛擬機器均啟用防毒軟體、反間諜軟體、入侵偵測及其他保護措施。還應確保您具有足夠的空間來儲存虛擬機器記錄。

防毒掃描

由於每台虛擬機器都主控標準作業系統，因此必須安裝防毒軟體，避免感染病毒。根據虛擬機器的使用方式，可能還需要安裝軟體防火牆。

請錯開病毒掃描的排程，尤其是在具有大量虛擬機器的部署中。如果同時掃描所有虛擬機器，環境中的系統效能將大幅降低。因為軟體防火牆和防毒軟體需要佔用大量虛擬化資源，因此您可以根據虛擬機器效能平衡對這兩個安全措施的需求，尤其是在您確信虛擬機器處於完全受信任的環境中時。

序列埠

序列埠是用於連線周邊設備與虛擬機器的介面。它們通常用於實體系統，為伺服器主控台提供直接、低層級的連線，而虛擬序列埠允許對虛擬機器執行相同的存取。序列埠允許低層級存取，但通常不具有嚴格的控制，如記錄或權限。

使用範本部署虛擬機器

在虛擬機器上手動安裝客體作業系統和應用程式時，會帶來錯誤組態的風險。透過使用範本擷取未安裝任何應用程式的強化基礎作業系統映像，您可以確保透過已知的安全性基準層級，建立所有虛擬機器。

您可以使用包含已強化、修補且正確設定的作業系統的範本，來建立其他專屬於應用程式的範本，也可以使用應用程式範本來部署虛擬機器。

程序

- 提供包含已強化、修補且正確設定的作業系統部署的範本，來建立虛擬機器。

  如果可能，還可在範本中部署應用程式。請確保應用程式不仰賴於要部署的虛擬機器的專屬資訊。

下一個

如需有關範本的詳細資訊，請參閱 *vSphere 虛擬機器管理*說明文件。

儘量少用虛擬機器主控台

虛擬機器主控台為虛擬機器提供的功能與實體伺服器上的監視器所提供的功能相同。具有虛擬機器主控台存取權限的使用者可存取虛擬機器電源管理和卸除式裝置連線能力控制項。因此，主控台存取可能造成對虛擬機器的惡意攻擊。

程序

1. 請使用原生遠端管理服務 (如終端服務和 SSH) 與虛擬機器進行互動。

   請僅在需要時才授與對虛擬機器主控台的存取權限。

2. 限制與主控台的連線。

   例如，在高度安全的環境中，限制與一個主控台的連線。在某些環境中，若完成一般工作需要多個並行連線，您可增加限制。

防止虛擬機器接管資源

當某個虛擬機器耗用過多主機資源，而使主機上的其他虛擬機器無法執行其預期功能時，可能會出現拒絕服務 (DoS)。為防止虛擬機器造成 DoS 問題，請使用主機資源管理功能，例如設定共用率和使用資源集區。

依預設，ESXi 主機上的所有虛擬機器平均共用資源。您可以使用共用率和資源集區來防止出現拒絕服務攻擊，此攻擊會導致某台虛擬機器耗用過多主機資源，而使同一主機上的其他虛擬機器無法執行其預期功能。

請勿使用限制，除非您完全瞭解其影響。

程序

1. 使用適量的資源 (CPU 和記憶體) 佈建每台虛擬機器，以使其正常運作。
2. 使用共用率來保證將資源指派給重要的虛擬機器。
3. 根據類似的需求將虛擬機器分為多個資源集區。
4. 在每個資源集區中，將 [共用率] 設定保留為預設，以確保集區中每台虛擬機器的資源優先順序大致相同。

   透過此設定，單一虛擬機器使用的資源將無法多於資源集區中的其他虛擬機器。

下一個

如需共用率和限制的相關資訊，請參閱 *vSphere 資源管理*說明文件。

停用虛擬機器中不必要的功能

在虛擬機器中執行的任何服務都有可能引發攻擊。透過停用不是支援系統上執行的應用程式或服務所必需的系統元件，可降低受到攻擊的可能性。

通常，虛擬機器需要的服務或功能不像實體伺服器那樣多。對系統進行虛擬化時，請評估特定服務或功能是否必要。

程序

- 停用作業系統中未使用的服務。

  例如，如果系統執行檔案伺服器，則關閉所有 Web 服務。
- 中斷未使用的實體裝置 (如 CD/DVD 光碟機、軟碟機和 USB 介面卡) 的連線。
- 停用未使用的功能 (例如未使用的顯示功能)，或停用能向虛擬機器 (主機客體檔案系統) 共用主機檔案的 VMware 共用資料夾。
- 關閉螢幕保護程式。
- 除非必要，否則不要在 Linux、BSD 或 Solaris 客體作業系統上執行 X Window 系統。

移除不必要的硬體裝置

啟用或連線的任何裝置都可能代表潛在攻擊通道。虛擬機器上具有權限的使用者和程序可以連線或中斷連線硬體裝置 (如網路介面卡和 CD-ROM 光碟機)。攻擊者可利用該能力破壞虛擬機器安全性。移除不必要的硬體裝置可以協助防止攻擊。

具有虛擬機器存取權限的攻擊者可以連線已中斷連線的硬體裝置，並存取留存在硬體裝置中媒體上的敏感資訊。攻擊者可能會中斷網路介面卡的連線，將虛擬機器與其網路隔離，導致拒絕服務。

- 請勿將未經授權的裝置連線到虛擬機器。
- 移除不需要或未使用的硬體裝置。
- 從虛擬機器中停用不必要的虛擬裝置。
- 確保僅將所需的裝置連線到虛擬機器。虛擬機器很少使用序列埠或平行埠。一般來說，在軟體安裝期間，CD/DVD 磁碟機僅會暫時連線。

程序

1. 使用 vSphere Web Client 登入 vCenter Server 系統。
2. 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。
3. 停用不需要的硬體裝置。

   包括對下列裝置的檢查：

   - 軟碟機
   - 序列埠
   - 平行埠

- USB 控制器
- CD-ROM 光碟機

停用未使用的顯示功能

攻擊者可以將未使用的顯示功能用作向量，將惡意程式碼插入到您的環境。停用您環境中未使用的功能。

程序

1 使用 vSphere Web Client 登入 vCenter Server 系統並尋找虛擬機器。

a 在導覽器中，選取**虛擬機器和範本**。

b 在階層中尋找虛擬機器。

2 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。

3 選取**虛擬機器選項**。

4 按一下**進階**，然後按一下**編輯組態**。

5 如果適用，請新增或編輯下列參數。

選項	說明
svga.vgaonly	如果將此參數設定為 TRUE，則進階圖形功能將不再運作。將只有字元儲存格主控台模式可用。如果使用此設定，`mks.enable3d` 會不起作用。 **備註** 將此設定僅套用到不需要虛擬化視訊卡的虛擬機器。
mks.enable3d	在不需要 3D 功能的虛擬機器上將此參數設定為 FALSE。

停用未公開的功能

VMware 虛擬機器在 vSphere 環境中和主控虛擬化平台 (例如 VMware Workstation 和 VMware Fusion) 上都能運作。在 vSphere 環境中執行虛擬機器時，無需啟用某些虛擬機器參數。停用這些參數可降低出現漏洞的可能性。

先決條件

關閉虛擬機器。

程序

1 使用 vSphere Web Client 登入 vCenter Server 系統並尋找虛擬機器。

a 在導覽器中，選取**虛擬機器和範本**。

b 在階層中尋找虛擬機器。

2 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。

3 選取**虛擬機器選項**。

4 按一下**進階**，然後按一下**編輯組態**。

5 透過新增或編輯下列參數，將其設定為 TRUE。

- isolation.tools.unity.push.update.disable
- isolation.tools.ghi.launchmenu.change
- isolation.tools.memSchedFakeSampleStats.disable
- isolation.tools.getCreds.disable
- isolation.tools.ghi.autologon.disable
- isolation.bios.bbs.disable
- isolation.tools.hgfsServerSet.disable

6 按一下**確定**。

停用向虛擬機器共用主機檔案的 VMware 共用資料夾

在高安全性環境中，您可以停用某些元件，以最大程度地降低攻擊者使用主機客體檔案系統 (HGFS) 在客體作業系統內傳輸檔案的風險。

修改本節中所述的參數只會影響共用資料夾功能，不會影響在客體虛擬機器中做為工具一部分執行的 HGFS 伺服器。此外，這些參數不會影響使用工具之檔案傳輸的自動升級和 VIX 命令。

程序

1 使用 vSphere Web Client 登入 vCenter Server 系統並尋找虛擬機器。

a 在導覽器中，選取**虛擬機器和範本**。

b 在階層中尋找虛擬機器。

2 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。

3 選取**虛擬機器選項**。

4 按一下**進階**，然後按一下**編輯組態**。

5 確認 isolation.tools.hgfsServerSet.disable 參數已設定為 TRUE。

設定為 TRUE 可防止 VMX 程序從每個工具的服務、精靈或升級程式程序接收有關其 HGFS 伺服器功能的通知。

6 (選擇性) 確認 isolation.tools.hgfs.disable 參數已設定為 TRUE。

設定為 TRUE，將停用未使用的 VMware 共用資料夾功能，向虛擬機器共用主機檔案。

停用客體作業系統和遠端主控台之間的複製和貼上作業

依預設，系統會停用客體作業系統和遠端主控台之間的複製和貼上作業。為確保環境安全，請保留預設設定。如果需要複製和貼上作業，必須使用 vSphere Web Client 進行啟用。

這些選項依預設已設定為建議值。但是，如果您想要啟用稽核工具來檢查設定是否正確，必須將它們明確設定為 true。

先決條件

關閉虛擬機器。

程序

1 使用 vSphere Web Client 登入 vCenter Server 系統。

2 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。

3 按一下**虛擬機器選項**，然後按一下**編輯組態**。

4 確保 [名稱] 和 [值] 資料行中存在以下值，或按一下**新增列**進行新增。

名稱	建議的值
`isolation.tools.copy.disable`	`true`
`isolation.tools.paste.disable`	`true`
`isolation.tools.setGUIOptions.enable`	`false`

這些選項將覆寫在客體作業系統的 VMware Tools 控制台中做出的任何設定。

5 按一下**確定**。

6 (選擇性) 如果變更了組態參數，則要重新啟動虛擬機器。

限制曝光複製到剪貼簿中的敏感資料

依預設，系統已停用針對主機的複製和貼上作業，以防止曝光已複製到剪貼簿中的敏感資料。

在執行 VMware Tools 的虛擬機器上啟用複製和貼上時，可以在客體作業系統和遠端主控台之間執行複製和貼上作業。當主控台視窗取得焦點時，虛擬機器中執行的程序和無權限使用者可存取虛擬機器主控台剪貼簿。如果使用者在使用主控台前將敏感資訊複製到剪貼簿中，使用者就可以向虛擬機器曝光敏感資料。為防止出現此問題，預設會停用針對客體作業系統的複製和貼上作業。

必要時，可以為虛擬機器啟用複製和貼上作業。

限制使用者在虛擬機器中執行命令

依預設，具有 vCenter Server 管理員角色的使用者可與虛擬機器客體作業系統內的檔案和應用程式進行互動。若要降低破壞客體機密性、可用性或完整性的風險，請建立沒有**客體作業**權限的非客體存取角色。將該角色指派給不需要虛擬機器檔案存取的管理員。

出於安全性考慮，請嚴格限制對虛擬資料中心的存取，嚴格程度與限制對實體資料中心的存取相同。將停用客體存取的自訂角色套用至需要管理員權限但未授權與客體作業系統檔案和應用程式進行互動的使用者。

例如，某個組態可能在基礎結構中包括虛擬機器，該基礎結構帶有敏感資訊。

如果工作 (例如使用 vMotion 的移轉) 需要資料中心管理員可以存取虛擬機器，則停用一些遠端客體作業系統作業可確保這些管理員無法存取敏感資訊。

先決條件

確認您在將建立角色的 vCenter Server 系統擁有**管理員**權限。

程序

1 以使用者身分登入 vSphere Web Client，該使用者在將建立角色的 vCenter Server 系統擁有**管理員**權限。

2 按一下**管理**，然後選取**角色**。

3 按一下**建立角色動作**圖示，然後輸入角色的名稱。

例如，輸入**無客體存取權限的管理員**。

4 選取**所有權限**。

5 取消選取**所有權限.虛擬機器.客體作業**，從而移除一組客體作業權限。

6 按一下**確定**。

下一個

選取 vCenter Server 系統或主機，並指派可將應具有新權限的使用者或群組與新建立的角色進行配對的權限。從管理員角色中移除這些使用者。

防止虛擬機器使用者或程序中斷裝置的連線

虛擬機器內不具有根權限或管理員權限的使用者和程序能夠與裝置 (如網路介面卡和 CD-ROM 光碟機) 連線或中斷連線，還能夠修改裝置設定。若要提高虛擬機器的安全性，請移除這些裝置。如果您不希望移除裝置，您可以變更客體作業系統設定，以防止虛擬機器使用者或程序變更裝置狀態。

先決條件

關閉虛擬機器。

程序

1 使用 vSphere Web Client 登入 vCenter Server 系統並尋找虛擬機器。

a 在導覽器中，選取**虛擬機器和範本**。

b 在階層中尋找虛擬機器。

2 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。

3 選取**虛擬機器選項**。

4 按一下**進階**，然後按一下**編輯組態**。

5 請確認下列值是否位於 [名稱] 和 [值] 資料行中，或者按一下**新增列**，可新增這些值。

名稱	值
isolation.device.connectable.disable	true
isolation.device.edit.disable	true

這些選項將覆寫在客體作業系統的 VMware Tools 控制台中所做的任何設定。

6 按一下**確定**關閉 [組態參數] 對話方塊，然後再按一下**確定**。

阻止客體作業系統程序向主機傳送組態訊息

若要確保客體作業系統不會修改組態設定，您可以阻止這些程序將任何名稱值配對寫入到組態檔中。

先決條件

關閉虛擬機器。

程序

1 使用 vSphere Web Client 登入 vCenter Server 系統並尋找虛擬機器。

   a 在導覽器中，選取**虛擬機器和範本**。

   b 在階層中尋找虛擬機器。

2 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。

3 選取**虛擬機器選項**。

4 按一下**進階**，然後按一下**編輯組態**。

5 按一下**新增列**，並在 [名稱] 和 [值] 資料行中輸入下列值。

欄	值
名稱	`isolation.tools.setinfo.disable`
值	`true`

6 按一下**確定**關閉 [組態參數] 對話方塊，然後再按一下**確定**。

避免使用獨立非持續性磁碟

使用獨立非持續性磁碟時，成功的攻擊者可移除機器已受到系統關閉或重新開機影響的任何證據。若無虛擬機器上活動的持續記錄，管理員可能無法感知到攻擊。因此，您應避免使用獨立非持續性磁碟。

程序

- 請確保已在個別伺服器 (例如 syslog 伺服器或同等 Windows 系統的事件收集器) 上遠端記錄虛擬機器活動。

  如果還沒有為客體設定遠端記錄事件和活動，則 scsiX:Y.mode 應為下列其中一個設定：

  - 不存在
  - 未設為獨立非持續性

未啟用非持續性模式時，您無法將虛擬機器復原為重新啟動系統時的已知狀態。

虛擬機器加密

6

從 vSphere 6.5 開始，您可以利用虛擬機器加密。加密不僅可以保護虛擬機器，還可以保護虛擬機器磁碟和其他檔案。您可以在 vCenter Server 和金鑰管理伺服器 (KMS) 之間設定信任連線。vCenter Server 隨後便可視需要從 KMS 擷取金鑰。

您可以採用不同的方式管理虛擬機器加密的不同方面。

- 透過 vSphere Web Client 管理與 KMS 信任連線的設定，以及執行大多數加密工作流程。
- 透過 vSphere Web Services SDK 管理某些進階功能的自動化。請參閱 *vSphere Web Services SDK 程式設計指南*和 *VMware vSphere API 參考*。
- 針對某些特殊情況直接在 ESXi 主機上使用 `crypto-util` 命令列工具，例如，用來解密 `vm-support` 服務包中的核心傾印。

vSphere 虛擬機器加密概觀 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere_virtual_machine_encryption_overview)

本章節討論下列主題:

vSphere 虛擬機器加密 如何保護您的環境

透過 vSphere 虛擬機器加密，您可以建立加密的虛擬機器，以及加密現有虛擬機器。由於包含敏感資訊的所有虛擬機器檔案都會加密，因此會保護虛擬機器。僅具有加密權限的管理員可以執行加密和解密工作。

使用哪些金鑰

兩種類型的金鑰用於加密。

- ESXi 主機產生並使用內部金鑰來加密虛擬機器和磁碟。這些金鑰用作資料加密金鑰 (DEK) 且是 XTS-AES-256 金鑰。
- vCenter Server 從 KMS 申請金鑰。這些金鑰用作金鑰加密金鑰 (KEK) 且是 AES-256 金鑰。vCenter Server 僅儲存每個 KEK 的識別碼，但不儲存金鑰本身。
- ESXi 使用 KEK 加密內部金鑰，且在磁碟上儲存加密的內部金鑰。ESXi 不在磁碟上儲存 KEK。如果主機重新開機，vCenter Server 會從 KMS 申請具有對應識別碼的 KEK，且使其可供 ESXi 使用。然後，ESXi 可視需要解密內部金鑰。

加密哪些檔案

vSphere 虛擬機器加密支援加密虛擬機器檔案、虛擬磁碟檔案，以及核心傾印檔案。

虛擬機器檔案

會加密大多數虛擬機器檔案 (尤其是未儲存在 VMDK 檔案中的客體資料)。這組檔案包括但不限於 NVRAM、VSWP 和 VMSN 檔案。vCenter Server 從 KMS 擷取的金鑰將解除鎖定包含內部金鑰和其他密碼的 VMX 檔案中的加密服務包。

如果您正使用 vSphere Web Client 建立加密的虛擬機器，預設會加密所有虛擬磁碟。對於其他加密工作，如加密現有虛擬機器，您可以加密和解密獨立於虛擬機器檔案的虛擬磁碟。

備註 您無法將加密的虛擬磁碟與未加密的虛擬機器建立關聯。

虛擬磁碟檔案

加密的虛擬磁碟 (VMDK) 檔案中的資料永遠不會以純文字寫入儲存區或實體磁碟，且永遠不會以純文字透過網路傳輸。VMDK 描述元檔案通常為純文字，但包含 KEK 的金鑰識別碼和加密服務包中的內部金鑰 (DEK)。

您可以使用 vSphere API 透過新 KEK 執行淺層雙重加密作業或透過新內部金鑰執行深度雙重加密作業。

核心傾印

永遠加密已啟用加密模式的 ESXi 主機上的核心傾印。請參閱 vSphere 虛擬機器加密和核心傾印。

備註 不會加密 vCenter Server 系統上的核心傾印。務必保護對 vCenter Server 系統的存取權。

備註 如需 vSphere 虛擬機器加密可互通的裝置和功能相關的一些限制的相關資訊，請參閱虛擬機器加密互通性。

不加密哪些檔案

不加密或部分加密與虛擬機器相關聯的一些檔案。

記錄檔	不加密記錄檔，因為其不包含敏感資料。
虛擬機器組態檔	不加密 VMX 和 VMSD 檔案中儲存的大多數虛擬機器組態資訊。
虛擬磁碟描述元檔案	為了支援無金鑰的磁碟管理，不會加密大多數虛擬磁碟描述元檔案。

誰可以執行密碼編譯作業

僅指派了**密碼編譯作業**權限的使用者可以執行密碼編譯作業。權限集是精細的。請參閱密碼編譯作業權限。預設管理員系統角色包含所有**密碼編譯作業**權限。新角色「無密碼編譯管理員」支援所有管理員權限，**密碼編譯作業**權限除外。

您可以建立其他自訂角色，例如允許使用者群組加密虛擬機器但防止其解密虛擬機器。

如何執行密碼編譯作業

vSphere Web Client 支援許多密碼編譯作業。對於其他工作，您可以使用 vSphere API。

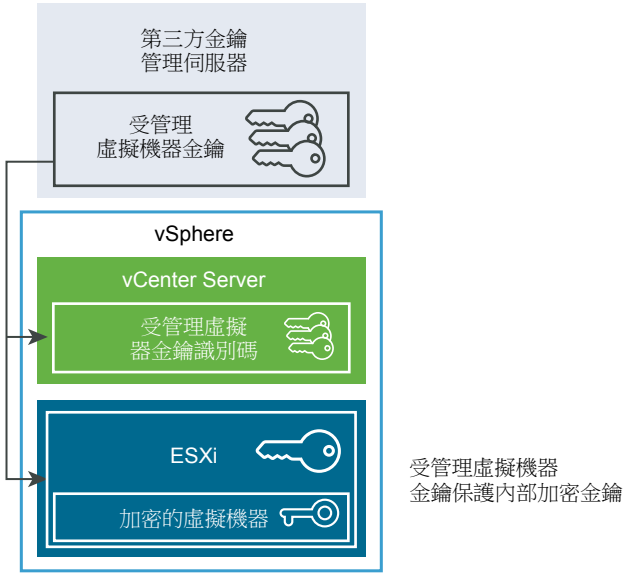
表格 6-1. 用於執行密碼編譯作業的介面

介面	作業	資訊
vSphere Web Client	建立加密的虛擬機器 加密和解密虛擬機器	本書。
vSphere Web Services SDK	建立加密的虛擬機器 加密和解密虛擬機器 執行虛擬機器的深度雙重加密 (使用不同的 DEK)。 執行虛擬機器的淺層雙重加密 (使用不同的 KEK)。	*vSphere Web Services SDK 程式設計指南* *VMware vSphere API 參考*
`crypto-util`	解密加密的核心傾印、檢查是否已加密檔案，以及在 ESXi 主機上直接執行其他管理工作。	命令列說明。 vSphere 虛擬機器加密和核心傾印

vSphere 虛擬機器加密 元件

外部 KMS、vCenter Server 系統及 ESXi 主機皆參與 vSphere 虛擬機器加密解決方案。

圖 6-1 vSphere 虛擬加密 架構



金鑰管理伺服器

vCenter Server 要求來自外部 KMS 的金鑰。KMS 會產生並儲存金鑰，然後將金鑰傳遞到 vCenter Server 進行發佈。

您可以使用 vSphere Web Client 或 vSphere API 將 KMS 執行個體的叢集新增至 vCenter Server 系統。如果您在一個叢集中使用多個 KMS 執行個體，所有執行個體都必須來自同一個廠商並且必須複寫金鑰。

如果您的環境使用不同環境中的不同 KMS 廠商，您可以針對每個 KMS 新增一個 KMS 叢集，並指定預設 KMS 叢集。新增的第一個叢集將成為預設叢集。您可以稍後明確指定預設值。

做為 KMIP 用戶端，vCenter Server 會使用金鑰管理互通協定 (KMIP)，可讓您輕鬆使用所選擇的 KMS。

vCenter Server

僅 vCenter Server 具有登入 KMS 的認證。ESXi 主機沒有這些認證。vCenter Server 會從 KMS 取得金鑰，並將其推送到 ESXi 主機。vCenter Server 不會儲存 KMS 金鑰，但會保留金鑰識別碼清單。

vCenter Server 會檢查執行密碼編譯作業的使用者的權限。您可以使用 vSphere Web Client 為使用者群組指派密碼編譯作業權限，或指派**無密碼編譯管理員**自訂角色。請參閱加密工作的必要條件和所需權限。

vCenter Server 會將密碼編譯事件新增至事件清單，您可以從 vSphere Web Client 事件主控台檢視和匯出這些事件。每個事件皆包含使用者、時間、金鑰識別碼及密碼編譯作業。

來自 KMS 的金鑰會用作金鑰加密金鑰 (KEK)。

ESXi 主機

ESXi 主機負責加密工作流程的多個方面。

- vCenter Server 會在主機需要金鑰時將金鑰推送到 ESXi 主機。主機必須已啟用加密模式。目前使用者的角色必須包含密碼編譯作業權限。請參閱加密工作的必要條件和所需權限和密碼編譯作業權限。

- 確保已加密虛擬機器的客體資料在儲存到磁碟時已加密。
- 確保已加密虛擬機器的客體資料不會在未加密的情況下透過網路傳送。

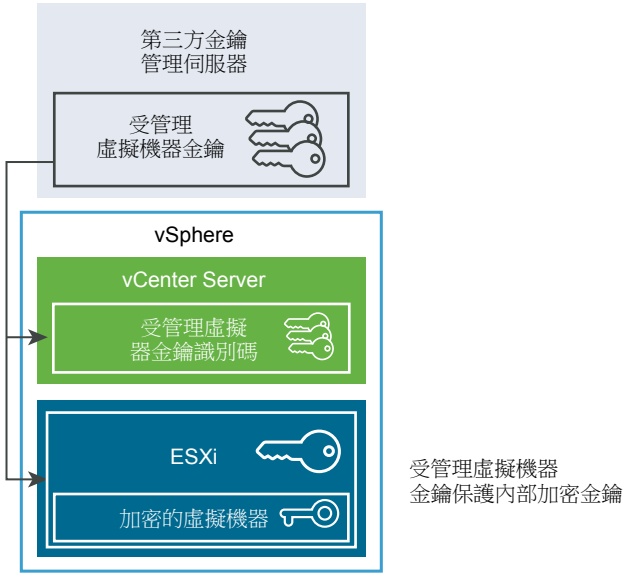
ESXi 主機所產生的金鑰在本文件中稱為內部金鑰。這些金鑰通常充當資料加密金鑰 (DEK)。

加密程序流程

vCenter Server 連線到 KMS 後，具有所需權限的使用者可以建立加密的虛擬機器和磁碟。這些使用者也可以執行其他加密工作，例如加密現有虛擬機器和解密已加密的虛擬機器。

程序流程包括 KMS、vCenter Server 和 ESXi 主機。

圖 6-2 vSphere 虛擬加密 架構



在執行加密程序期間，不同 vSphere 元件的相互影響如下。

1 當使用者執行加密工作 (例如建立加密的虛擬機器) 時，vCenter Server 會從預設 KMS 要求新金鑰。此金鑰會用作 KEK。

2 vCenter Server 會儲存金鑰識別碼並將此金鑰傳遞到 ESXi 主機。如果 ESXi 主機屬於某個叢集，則 vCenter Server 會將 KEK 傳送到此叢集中的每個主機。

   此金鑰本身不儲存在 vCenter Server 系統上。僅金鑰識別碼已知。

3 ESXi 主機會為虛擬機器及其磁碟產生內部金鑰 (DEK)。它僅將內部金鑰保留在記憶體中，並使用 KEK 加密內部金鑰。

   未加密內部金鑰永遠不會儲存在磁碟上。僅儲存已加密的資料。由於 KEK 來自 KMS，因此主機會繼續使用相同的 KEK。

4 ESXi 主機使用已加密的內部金鑰加密虛擬機器。

   任何擁有 KEK 以及可以存取已加密金鑰檔案的主機可以針對已加密虛擬機器或磁碟執行作業。

如果您稍後想要解密虛擬機器，可以變更其儲存區原則。您可以變更虛擬機器和所有磁碟的儲存區原則。如果您想要解密個別元件，請先解密所選磁碟，然後透過變更虛擬機器首頁的儲存區原則來解密虛擬機器。解密每個元件均需要兩個金鑰。

加密虛擬機器和磁碟 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_encrypting_vms_and_disks)

虛擬磁碟加密

當您從 vSphere Web Client 建立加密的虛擬機器時，所有虛擬磁碟均會加密。您可以稍後新增磁碟並設定其加密原則。您無法將已加密的磁碟新增至未加密的虛擬機器，並且如果虛擬機器未加密，您將無法加密磁碟。

虛擬機器及其磁碟的加密由儲存區原則控制。虛擬機器首頁的儲存區原則管理虛擬機器本身，並且每個虛擬磁碟都有一個相關聯的儲存區原則。

- 將虛擬機器首頁的儲存區原則設為僅加密虛擬機器本身的加密原則。
- 將虛擬機器首頁和所有磁碟的儲存區原則設為加密所有元件的加密原則。

請考慮下列使用案例。

表格 6-2. 虛擬磁碟加密使用案例

使用案例	詳細資訊
建立加密的虛擬機器。	如果您在建立加密的虛擬機器時新增磁碟，依預設會加密磁碟。您可以將此原則變更為不加密一或多個磁碟。 虛擬機器建立後，您可以明確變更每個磁碟的儲存區原則。請參閱變更虛擬磁碟的加密原則。
加密虛擬機器。	若要加密現有虛擬機器，請變更其儲存區原則。您可以變更虛擬機器和所有虛擬磁碟的儲存區原則。若要僅加密虛擬機器，您可以指定虛擬機器首頁的加密原則，然後為每個虛擬磁碟選取不同的儲存區原則，例如 [資料存放區預設值]。
將現有的未加密磁碟新增至已加密的虛擬機器 (加密儲存區原則)	失敗並顯示錯誤。您必須新增具有預設儲存區原則的磁碟，但稍後可以變更儲存區原則。
將現有的未加密磁碟新增至儲存區原則不包含加密 (例如 [資料存放區預設值]) 的已加密虛擬機器。	該磁碟使用預設儲存區原則。如果想要已加密的磁碟，您可以在新增磁碟後明確變更儲存區原則。
將已加密的磁碟新增至已加密的虛擬機器。虛擬機器首頁儲存區原則為 [加密]。	當您新增磁碟時，它會保持已加密狀態。vSphere Web Client 會顯示大小和其他屬性，包括加密狀態，但可能不會顯示正確的儲存區原則。為確保一致性，請變更儲存區原則。
將現有的已加密磁碟新增至未加密的虛擬機器	此使用案例不受支援。

加密工作的必要條件和所需權限

只能在包含 vCenter Server 的環境中執行加密工作。此外，ESXi 主機必須為大多數加密工作啟用加密模式。執行此工作的使用者必須擁有適當的權限。一組**密碼編譯作業**權限允許進行更為精細的控制。如果虛擬機器加密工作需要變更主機加密模式，則需要其他權限。

密碼編譯權限和角色

依預設，具有 vCenter Server 管理員角色的使用者擁有所有權限。**無密碼編譯管理員**角色沒有執行密碼編譯作業所需的下列權限。

- 新增**密碼編譯作業**權限。
- **全域.診斷**
- **主機.詳細目錄.新增主機至叢集**
- **主機.詳細目錄.新增獨立主機**
- **主機.本機作業.管理使用者群組**

您可以將**無密碼編譯管理員**角色指派給不需要**密碼編譯作業**權限的 vCenter Server 管理員。

若要進一步限制使用者可以執行的作業，您可以複製**無密碼編譯管理員**角色，並建立僅具有某些**密碼編譯作業**權限的自訂角色。例如，您可以建立允許使用者加密，但無法解密虛擬機器的角色。請參閱使用角色指派權限。

主機加密模式

僅在為 ESXi 主機啟用主機加密模式時，才可以加密虛擬機器。主機加密模式經常自動啟用，但其可以明確啟用。您可以從 vSphere Web Client 或透過使用 vSphere API 檢查並明確設定目前的主機加密模式。

如需相關指示，請參閱 明確啟用主機加密模式。

主機加密模式一經啟用，便不會輕易停用。請參閱停用主機加密模式。

當加密作業嘗試啟用主機加密模式時，會發生自動變更。例如，假設您將已加密的虛擬機器新增至獨立主機。主機加密模式未啟用。如果您在主機上擁有所需權限，則加密模式會變更為自動啟用。

假定叢集有三個 ESXi 主機：主機 A、B 和 C。您將已加密的虛擬機器新增至主機 A。發生的情況取決於多個因素。

- 如果主機 A、B 和 C 已啟用加密，則您只需**密碼編譯作業.加密新增項目**權限即可建立虛擬機器。
- 如果主機 A 和 B 已啟用加密，而主機 C 未啟用，則系統會以如下方式繼續進行。
  - 假設您在每台主機上擁有**密碼編譯作業.加密新增項目**和**密碼編譯作業.登錄主機**權限。在此情況下，虛擬機器建立程序會在主機 C 上啟用加密。加密程序在主機 C 上啟用主機加密模式，並將金鑰推送給叢集中的每台主機。

    對於這種情況，您也可以在主機 C 上明確啟用主機加密。
  - 假設您在虛擬機器或虛擬機器資料夾上僅擁有**密碼編譯作業.加密新增項目**權限。在此情況下，虛擬機器會成功建立，且金鑰在主機 A 和主機 B 上變得可用。主機 C 仍停用加密，且沒有虛擬機器金鑰。
- 如果所有主機皆未啟用加密，並且您在主機 A 上擁有**密碼編譯作業.登錄主機**權限，則虛擬機器建立程序會在該主機上啟用主機加密。否則會導致錯誤。

磁碟空間需求

加密現有虛擬機器時，您至少需要虛擬機器目前使用之空間兩倍的空間。

已加密的 vSphere vMotion

從 vSphere 6.5 開始，移轉已加密的虛擬機器時，vSphere vMotion 始終使用加密。對於未加密的虛擬機器，您可以選取其中一個已加密的 vSphere vMotion 選項。

已加密的 vSphere vMotion 保護使用 vSphere vMotion 傳輸之資料的機密性、完整性和真實性。

- 對於未加密的虛擬機器，支援已加密的 vSphere vMotion 的所有變體。在 vCenter Server 執行個體之間移轉需要共用儲存區。
- 對於已加密的虛擬機器，不支援在 vCenter Server 執行個體之間移轉。

加密什麼

對於已加密的磁碟，傳輸的資料會進行加密。對於未加密的磁碟，不支援 Storage vMotion 加密。

對於已加密的虛擬機器，透過 vSphere vMotion 移轉始終使用已加密的 vSphere vMotion。對於已加密的虛擬機器，您無法關閉已加密的 vSphere vMotion。

已加密的 vSphere vMotion 狀態

對於未加密的虛擬機器，您可以將已加密的 vSphere vMotion 設定為下列其中一種狀態。預設為 [隨機]。

已停用	請勿使用已加密的 vSphere vMotion。
隨機	如果來源主機和目的地主機支援，則使用已加密的 vSphere vMotion。僅 ESXi 6.5 版及更新版本使用已加密的 vSphere vMotion。
必要	僅允許已加密的 vSphere vMotion。如果來源主機或目的地主機不支援已加密的 vSphere vMotion，則不允許使用 vSphere vMotion 進行移轉。

當您加密虛擬機器時，虛擬機器會保留目前已加密的 vSphere vMotion 設定的記錄。如果您稍後停用虛擬機器加密，則已加密的 vMotion 設定會保留為 [必要]，直到您明確變更此設定。您可以使用**編輯設定**變更此設定。

如需針對未加密虛擬機器啟用和停用已加密 vSphere vMotion 的相關資訊，請參閱 *vCenter Server 和主機管理*說明文件。

加密最佳做法、注意須知和互通性

任何適用於實體機器加密的最佳做法和注意須知同樣適用於虛擬機器加密。虛擬機器加密架構會產生一些其他建議。在您規劃虛擬機器加密策略時，請考慮互通性限制。

虛擬機器加密最佳做法

請遵循虛擬機器加密最佳做法，以避免稍後 (例如產生 `vm-support` 服務包時) 發生問題。

一般最佳做法

請遵循下列一般最佳做法，以避免發生問題。

- 請勿加密任何 vCenter Server Appliance 虛擬機器。
- 如果 ESXi 主機當機，請儘快擷取支援服務包。主機金鑰必須可用於產生使用密碼的支援服務包或解密核心傾印。如果將主機重新開機，主機金鑰可能會發生變更。如果出現這種情況，您將無法再產生使用密碼的支援服務包或使用主機金鑰解密支援服務包中的核心傾印。
- 請謹慎管理 KMS 叢集名稱。如果已在使用中的 KMS 的 KMS 叢集名稱發生變更，使用來自該 KMS 的金鑰加密的虛擬機器在電源開啟或登錄期間會進入鎖定狀態。在這種情況下，請將該 KMS 從 vCenter Server 中移除並以最初使用的叢集名稱加以新增。
- 請勿編輯 VMX 檔案和 VMDK 描述元檔案。這些檔案包含加密服務包。您的變更可能會使虛擬機器無法復原，並且該復原問題無法修復。
- 加密程序會在主機上的資料寫入儲存區之前將其加密。後端儲存區功能 (例如重複資料刪除和壓縮) 可能對加密的虛擬機器無效。使用 vSphere 虛擬機器加密時，請考量儲存區權衡。
- 加密需要大量 CPU。AES-NI 顯著提升了加密效能。在 BIOS 中啟用 AES-NI。

已加密核心傾印的最佳做法

請遵循下列最佳做法，以避免在您想要檢查核心傾印以診斷問題時發生問題。

- 建立與核心傾印有關的原則。加密核心傾印是因為它們可能包含敏感資訊，例如金鑰。如果要解密核心傾印，請考慮敏感資訊。ESXi 核心傾印可能包含 ESXi 主機及其上虛擬機器的金鑰。在解密核心傾印之後，請考量變更主機金鑰並對已加密的虛擬機器進行雙重加密。您可以透過使用 vSphere API 來執行這兩項工作。

  如需詳細資料，請參閱 vSphere 虛擬機器加密和核心傾印。

- 在您收集 `vm-support` 服務包時，一律使用密碼。您可以在透過 vSphere Web Client 或使用 `vm-support` 命令產生支援服務包時指定密碼。

  該密碼會對使用內部金鑰的核心傾印進行雙重加密，以使用基於密碼的金鑰。您稍後可以使用該密碼來解密可能包含在支援服務包中的任何已加密核心傾印。透過使用密碼選項，未加密的核心傾印和記錄不會受到影響。

- vSphere 元件中不會保存您在 `vm-support` 服務包建立期間指定的密碼。您將負責追蹤支援服務包的密碼。
- 變更主機金鑰之前，請先產生使用密碼的 vm-support 服務包。您稍後可以使用密碼來存取可能已使用舊主機金鑰加密的任何核心傾印。

金鑰生命週期管理最佳做法

實作最佳做法不但可保證 KMS 可用性，而且能夠監控 KMS 上的金鑰。

- 您將負責建立用於保證 KMS 可用性的原則。

  如果 KMS 無法使用，需要 vCenter Server 要求來自 KMS 的金鑰的虛擬機器作業將無法進行。這意味著，執行中的虛擬機器會繼續執行，您可以對這些虛擬機器進行開啟電源、關閉電源和重新設定。但是，您無法將這些虛擬機器重新放置到不具金鑰資訊的主機。

  大多數 KMS 解決方案都包含高可用性功能。您可以使用 vSphere Web Client 或 API 來指定 KMS 叢集和相關聯的 KMS 伺服器。

- 您將負責追蹤金鑰，並在現有虛擬機器的金鑰未處於 [作用中] 狀態時執行修復。

  KMIP 標準定義了下列金鑰狀態。

  - 作用前
  - 作用中
  - 已停用
  - 已遭洩露
  - 已銷毀
  - 已銷毀並遭洩露

  vSphere 虛擬機器加密僅使用 [作用中] 金鑰進行加密。如果金鑰為 [作用前]，vSphere 虛擬機器加密會將其啟動。如果金鑰狀態為 [已停用]、[已遭洩露]、[已銷毀]、[已銷毀並遭洩露]，則無法使用該金鑰加密虛擬機器。

  對於處於其他狀態的金鑰，使用這些金鑰的虛擬機器會繼續運作。複製或移轉作業是否成功取決於其金鑰是否已存在於主機上。

  - 如果金鑰存在於目的地主機上，則表示作業成功執行，即使金鑰在 KMS 上不是 [作用中] 狀態。
  - 如果所需的虛擬機器和虛擬磁碟金鑰不在目的地主機上，則 vCenter Server 必須從 KMS 擷取金鑰。如果金鑰狀態為 [已停用]、[已遭洩露]、[已銷毀]、[已銷毀並遭洩露]，則 vCenter Server 會顯示錯誤，作業不會成功。

  如果金鑰已存在於主機上，則複製或移轉作業成功。如果 vCenter Server 必須從 KMS 提取金鑰，則作業失敗。

  如果金鑰不是 [作用中] 狀態，請使用 API 執行重設金鑰作業。請參閱*《vSphere Web Services SDK 程式設計指南》*。

備份和還原最佳做法

請設定有關備份和還原作業的原則。

- 並非所有備份架構皆受支援。請參閱虛擬機器加密互通性。
- 針對還原作業設定原則。因為備份一律採用純文字形式，所以請計劃在還原完成後立即加密虛擬機器。您可以指定加密虛擬機器做為還原作業的一部分。如果可能，請在還原程序過程中加密虛擬機器，以避免曝光敏感資訊。若要變更與虛擬機器相關聯的任何磁碟的加密原則，請變更磁碟的儲存區原則。

- 由於虛擬機器主檔案已加密，請確保加密金鑰在還原時可供使用。

效能最佳做法

- 加密效能取決於 CPU 和儲存區速度。
- 加密現有虛擬機器耗用的時間比在虛擬機器建立期間進行加密的時間要久。如果可能，請在建立虛擬機器時對其進行加密。

儲存區原則最佳做法

請勿修改配套虛擬機器加密範例儲存區原則。請改為複製原則並編輯複製品。

備註 不存在將虛擬機器加密原則恢復為其原始設定的自動化方式。

如需自訂儲存區原則的詳細資料，請參閱 *vSphere 儲存區* 說明文件。

虛擬機器加密注意須知

請檢閱虛擬機器加密注意須知，以避免稍後發生問題。

若要瞭解哪些裝置和功能不能與虛擬機器加密搭配使用，請參閱虛擬機器加密互通性。

限制

當您規劃虛擬機器加密策略時，請考慮下列注意須知。

- 複製加密的虛擬機器或執行 Storage vMotion 作業時，您可以嘗試變更磁碟格式。此類轉換不一定會成功。例如，如果複製虛擬機器並嘗試將磁碟格式從消極式歸零完整格式變更為精簡格式，虛擬機器磁碟會保留消極式歸零完整格式。
- 從虛擬機器卸除磁碟時，不會保留虛擬磁碟的儲存區原則資訊。
  - 如果虛擬磁碟已加密，您必須將儲存區原則明確設定為虛擬機器加密原則，或設定為包含加密的儲存區原則。
  - 如果虛擬磁碟未加密，您可以在將磁碟新增至虛擬機器時變更儲存區原則。

  如需詳細資料，請參閱虛擬磁碟加密。
- 先解密核心傾印，然後再將虛擬機器移到其他叢集。

  vCenter Server 不會儲存 KMS 金鑰，僅會追蹤金鑰識別碼。因此，vCenter Server 不會永久儲存 ESXi 主機金鑰。

  在某些情況下，例如將 ESXi 主機移到其他叢集並將主機重新開機時，vCenter Server 會為主機指派新的主機金鑰。您無法使用新的主機金鑰解密任何現有核心傾印。
- 加密的虛擬機器不支援 OVF 匯出。
- 不支援使用 VMware Host Client 登錄加密的虛擬機器。

虛擬機器鎖定狀態

如果虛擬機器金鑰或一或多個虛擬磁碟金鑰遺失，虛擬機器會進入鎖定狀態。在鎖定狀態下，無法執行虛擬機器作業。

- 從 vSphere Client 加密虛擬機器及其磁碟時，會為它們使用相同的金鑰。
- 使用 API 執行加密時，您可以針對虛擬機器和磁碟使用不同的加密金鑰。在這種情況下，如果您嘗試開啟虛擬機器電源並且其中一個磁碟金鑰遺失，開啟電源作業就會失敗。如果移除虛擬磁碟，就可以開啟虛擬機器電源。

如需疑難排解建議，請參閱解決遺失金鑰問題。

虛擬機器加密互通性

在 vSphere 6.5 及更新版本中，vSphere 虛擬機器加密就可與其互通的裝置和功能方面存在一些限制。

無法對加密的虛擬機器執行特定的工作。

- 對於大多數虛擬機器加密作業，必須關閉虛擬機器電源。您可以在虛擬機器電源開啟時複製加密的虛擬機器，並且可以執行淺層雙重加密。
- 您無法加密具有現有快照的虛擬機器。請在執行加密前整併所有現有的快照。

從 vSphere 6.7 開始，您可以從已加密虛擬機器的暫停狀態恢復，或還原為已加密機器的記憶體快照。您可以將在 ESXi 主機之間移轉具有記憶體快照和暫停狀態的已加密虛擬機器。

您可以純 IPv6 模式或混合模式下，使用 vSphere 虛擬機器加密。您可以使用 IPv6 位址設定 KMS。vCenter Server 和 KMS 只能設定 IPv6 位址。

某些功能無法與 vSphere 虛擬機器加密搭配使用。

- vSphere Fault Tolerance
- 視情況支援複製。
  - 支援完整複製。複製會繼承父系加密狀態 (包括金鑰)。您可以雙重加密完整複製以使用新金鑰，或解密完整複製。

    支援連結複製，並且複製會繼承父系加密狀態 (包括金鑰)。無法解密連結複製或使用不同金鑰雙重加密連結複製。
- vSphere ESXi Dump Collector
- 運用 vMotion 將加密的虛擬機器移轉至不同的 vCenter Server 執行個體。支援運用 vMotion 加密移轉未加密的虛擬機器。
- vSphere Replication
- 內容程式庫
- 並非所有使用 VMware vSphere Storage API - Data Protection (VADP) 進行虛擬磁碟備份的備份解決方案都受支援。
  - 不支援 VADP SAN 備份解決方案。

  - 如果廠商支援加密做為備份工作流程一部分建立的 Proxy 虛擬機器，則支援 VADP 熱新增備份解決方案。廠商必須具有權限**密碼編譯作業.加密虛擬機器**。
  - 支援 VADP NBD-SSL 備份解決方案。廠商應用程式必須具有權限**密碼編譯作業.直接存取**。
- 無法在其他 VMware 產品 (如 VMware Workstation) 上使用 vSphere 虛擬機器加密進行加密。
- 無法將輸出從加密的虛擬機器傳送至序列埠或平行埠。即使組態顯示成功，輸出仍傳送至檔案。

vSphere 虛擬機器加密不支援某些類型的虛擬機器磁碟組態。

- VMware vSphere Flash Read Cache。
- 與虛擬機器未關聯的具名虛擬磁碟，也稱為第一級磁碟。
- RDM (原始裝置對應)。
- 多重寫入器或共用磁碟 (MSCS、WSFC 或 Oracle RAC)。在虛擬磁碟已加密的情況下，如果您嘗試在虛擬機器的**編輯設定**頁面中選取多重寫入器，**確定**按鈕會停用。

在 vSphere 環境中使用加密

7

在 vSphere 環境中使用加密需要一些準備工作。在設定您的環境之後，您可以建立已加密的虛擬機器和虛擬磁碟，以及加密現有虛擬機器和磁碟。

您可以透過使用 API 和 `crypto-util` CLI 執行其他工作。請參閱 *vSphere Web Services SDK 程式設計指南*以取得 API 說明文件，以及參閱 `crypto-util` 命令列說明以取得有關此工具的詳細資料。

本章節討論下列主題:

設定金鑰管理伺服器叢集

在開始執行虛擬機器加密工作之前，您必須設定金鑰管理伺服器 (KMS) 叢集。該工作包括新增 KMS 以及與 KMS 建立信任。新增叢集時，系統會提示您將其設為預設值。您可以明確變更預設叢集。vCenter Server 會從預設叢集佈建金鑰。

KMS 必須支援金鑰管理互通協定 (KMIP) 1.1 標準。如需詳細資料，請參閱 *vSphere 相容性矩陣圖*。

您可以在《VMware 相容性指南》中的〈平台與運算〉下找到 VMware 認證的 KMS 廠商的相關資訊。如果選取《相容性指南》，您可以開啟《金鑰管理伺服器 (KMS) 相容性》說明文件。本說明文件會經常更新。

虛擬機器加密金鑰管理伺服器設定 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vm_KMS_vsphere67)

在 vSphere Client 中將 KMS 新增至 vCenter Server

您可以從 vSphere Client (以 HTML5 為基礎的用戶端) 或使用公開 API，將金鑰管理伺服器 (KMS) 新增至 vCenter Server 系統。

vSphere Client (以 HTML5 為基礎的用戶端) 提供將 KMS 新增至 vCenter Server 系統，以及建立 KMS 與 vCenter Server 之間的信任的精靈。

當您新增第一個 KMS 執行個體時，vCenter Server 會建立一個 KMS 叢集。

- vCenter Server 建立第一個叢集之後，您可以將相同廠商的 KMS 執行個體新增至叢集。
- 您僅能使用一個 KMS 執行個體設定叢集。
- 如果您的環境支援不同廠商的 KMS 解決方案，則可以新增多個 KMS 叢集。
- 如果您的環境含有多個 KMS 叢集，且您刪除預設叢集，則必須明確地設定其他預設值。

備註 下列步驟適用於 vCenter Server Appliance。針對 Windows 上的 vCenter Server，系統會提示您先讓 KMS 信任 vCenter Server，然後讓 vCenter Server 信任 KMS。

先決條件

- 確認金鑰伺服器位於*《適用於金鑰管理伺服器 (KMS) 的 VMware 相容性指南》*並與 KMIP 1.1 相容，而且可以是對稱金鑰 Foundry 和伺服器。
- 確認您具有所需權限：**密碼編譯作業.管理金鑰伺服器**。
- 您可以使用 IPv6 位址設定 KMS。
  - vCenter Server 和 KMS 只能設定 IPv6 位址。

程序

1. 使用 vSphere Client (以 HTML5 為基礎的用戶端) 登入 vCenter Server 系統。
2. 瀏覽詳細目錄清單，並選取 vCenter Server 執行個體。
3. 按一下**設定**，然後按一下**金鑰管理伺服器**。
4. 按一下**新增**，在精靈中指定 KMS 資訊，然後按一下**確定**。
5. 按一下**信任**。

   精靈會以綠色核取記號顯示 vCenter Server 信任 KMS。
6. 按一下**使 KMS 信任 vCenter**。

7 選取適合您伺服器的選項並完成這些步驟。

選項	請參閱
根 CA 憑證	使用 [根 CA 憑證] 選項建立信任連線。
憑證	使用憑證選項建立信任連線。
新增憑證簽署申請	使用新增憑證簽署要求選項建立信任連線。
上傳憑證和私密金鑰	使用上傳憑證和私密金鑰選項建立信任連線。

8 按一下**建立信任**。

精靈會以綠色核取記號顯示 KMS 信任 vCenter Server。

9 設定預設 KMS。

a 從**動作**功能表中，選取**變更預設叢集**。

b 選取 KMS 叢集，然後按一下**儲存**。

精靈會顯示 KMS 叢集為目前預設值。

在 vSphere Web Client 中將 KMS 新增至 vCenter Server

您可以從 vSphere Web Client 或使用公開 API，將 KMS 新增至 vCenter Server 系統。

當您新增第一個 KMS 執行個體時，vCenter Server 會建立一個 KMS 叢集。

- 新增 KMS 時，系統會提示您將此叢集設定為預設叢集。您之後可以明確地變更預設叢集。
- vCenter Server 建立第一個叢集之後，您可以將相同廠商的 KMS 執行個體新增至叢集。
- 您僅能使用一個 KMS 執行個體設定叢集。
- 如果您的環境支援不同廠商的 KMS 解決方案，則可以新增多個 KMS 叢集。
- 如果您的環境含有多個 KMS 叢集，且您刪除預設叢集，則必須明確地設定預設值。請參閱設定預設 KMS 叢集。

先決條件

- 確認金鑰伺服器位於 *vSphere 相容性矩陣圖* 並與 KMIP 1.1 相容，而且可以是對稱金鑰 Foundry 和伺服器。
- 確認您具有所需權限：**密碼編譯作業.管理金鑰伺服器**。
- 您可以使用 IPv6 位址設定 KMS。
- vCenter Server 和 KMS 只能設定 IPv6 位址。

程序

1 使用 vSphere Web Client 登入 vCenter Server 系統。

2 瀏覽詳細目錄清單，並選取 vCenter Server 執行個體。

3 按一下**設定**，然後按一下**金鑰管理伺服器**。

4 按一下**新增 KMS**，在精靈中指定 KMS 資訊，然後按一下**確定**。

選項	值
KMS 叢集	為新叢集選取**建立新叢集**。如果叢集存在，您可以選取該叢集。
叢集名稱	KMS 叢集的名稱。如果您的 vCenter Server 執行個體變成無法使用，您可能需要這個名稱才能連線至 KMS。
伺服器別名	KMS 的別名。如果您的 vCenter Server 執行個體變成無法使用，您可能需要這個別名才能連線至 KMS。
伺服器位址	KMS 的 IP 位址或 FQDN。
伺服器連接埠	vCenter Server 連線至 KMS 所在的連接埠。
Proxy 位址	連線至 KMS 選用的 Proxy 位址。
Proxy 連接埠	連線至 KMS 選用的 Proxy 連接埠。
使用者名稱	有些 KMS 廠商允許使用者透過指定使用者名稱和密碼，隔離不同使用者或群組所使用的加密金鑰。只有在 KMS 支援此功能，且您想要使用此功能時，才指定使用者名稱。
密碼	有些 KMS 廠商允許使用者透過指定使用者名稱和密碼，隔離不同使用者或群組所使用的加密金鑰。只有在 KMS 支援此功能，且您想要使用此功能時，才指定密碼。

透過交換憑證建立信任連線

將 KMS 新增至 vCenter Server 系統後，可以建立信任連線。確切程序取決於 KMS 接受的憑證以及公司原則。

先決條件

新增 KMS 叢集。

程序

1 登入 vSphere Web Client，然後選取 vCenter Server 系統。

2 按一下**設定**，然後選取**金鑰管理伺服器**。

3 選取想要與其建立信任連線的 KMS 執行個體。

4 按一下**與 KMS 建立信任**。

5 選取適合您伺服器的選項並完成這些步驟。

選項	請參閱
根 CA 憑證	使用 [根 CA 憑證] 選項建立信任連線。
憑證	使用憑證選項建立信任連線。
新增憑證簽署申請	使用新增憑證簽署要求選項建立信任連線。
上傳憑證和私密金鑰	使用上傳憑證和私密金鑰選項建立信任連線。

使用 [根 CA 憑證] 選項建立信任連線

部分 KMS 廠商 (例如，SafeNet) 會要求您將根 CA 憑證上傳到 KMS。之後，由您的根 CA 簽署的所有憑證會受此 KMS 信任。

vSphere 虛擬機器加密使用的根 CA 憑證是自我簽署的憑證，儲存於 vCenter Server 系統上 VMware Endpoint 憑證存放區 (VECS) 的獨立存放區中。

備註 僅在您想要取代現有憑證時，才產生根 CA 憑證。如果您產生該憑證，則由該 CA 簽署的其他憑證將變為無效。您可在此工作流程期間產生新的根 CA 憑證。

程序

1. 登入 vSphere Web Client，然後選取 vCenter Server 系統。
2. 按一下**設定**，然後選取**金鑰管理伺服器**。
3. 選取想要與其建立信任連線的 KMS 執行個體。
4. 選取**根 CA 憑證**，然後按一下**確定**。

   [下載根 CA 憑證] 對話方塊會填入 vCenter Server 用於加密的根憑證。此憑證儲存於 VECS 中。
5. 將憑證複製到剪貼簿，或將憑證下載為檔案。
6. 遵循 KMS 廠商提供的指示將憑證上傳到其系統。

   備註 部分 KMS 廠商 (例如，SafeNet) 會要求 KMS 廠商重新啟動 KMS 以獲取您上傳的根憑證。

下一個

完成憑證交換。請參閱完成信任設定。

使用憑證選項建立信任連線

部分 KMS 廠商 (例如 Vormetric) 會要求您將 vCenter Server 憑證上傳到 KMS。上傳後，KMS 會接受來自具有該憑證之系統的流量。

vCenter Server 會產生憑證來保護與 KMS 的連線。該憑證會儲存在 vCenter Server 系統上 VMware Endpoint 憑證存放區 (VECS) 的獨立金鑰存放區中。

程序

1. 登入 vSphere Web Client，然後選取 vCenter Server 系統。
2. 按一下**設定**，然後選取**金鑰管理伺服器**。
3. 選取想要與其建立信任連線的 KMS 執行個體。
4. 選取**憑證**，然後按一下**確定**。

   [下載憑證] 對話方塊會填入 vCenter Server 用於加密的根憑證。此憑證儲存於 VECS 中。

   備註 除非您想要取代現有憑證，否則請勿產生新憑證。

5 將憑證複製到剪貼簿中，或將其下載為檔案。

6 遵循 KMS 廠商提供的指示將憑證上傳到 KMS。

下一個

信任關係定案。請參閱 完成信任設定。

使用新增憑證簽署要求選項建立信任連線

部分 KMS 廠商 (例如 Thales) 會要求 vCenter Server 產生憑證簽署要求 (CSR) 並將該 CSR 傳送到 KMS。KMS 簽署 CSR 並傳回已簽署憑證。您可將已簽署憑證上傳到 vCenter Server。

使用**新增憑證簽署要求**選項的程序分為兩步。首先，產生 CSR 並將其傳送給 KMS 廠商。然後，將從 KMS 廠商接收的已簽署憑證上傳到 vCenter Server。

程序

1 登入 vSphere Web Client，然後選取 vCenter Server 系統。

2 按一下**設定**，然後選取**金鑰管理伺服器**。

3 選取想要與其建立信任連線的 KMS 執行個體。

4 選取**新增憑證簽署要求**，然後按一下**確定**。

5 在對話方塊中，將文字方塊中的完整憑證複製到剪貼簿，或將其下載為檔案，然後按一下**確定**。

僅在您明確想要產生 CSR 時，才使用對話方塊中的**產生新 CSR** 按鈕。使用該選項會使任何以舊 CSR 為基礎的已簽署憑證失效。

6 遵循 KMS 廠商提供的指示來提交 CSR。

7 從 KMS 廠商接收已簽署憑證時，再次按一下**金鑰管理伺服器**，然後再次選取**新增憑證簽署要求**。

8 將已簽署憑證貼至底部文字方塊中，或按一下**上傳檔案**來上傳檔案，然後按一下**確定**。

下一個

信任關係定案。請參閱 完成信任設定。

使用上傳憑證和私密金鑰選項建立信任連線

部分 KMS 廠商 (例如，HyTrust) 會要求您將 KMS 伺服器憑證和私密金鑰上傳到 vCenter Server 系統。

部分 KMS 廠商針對連線產生憑證和私密金鑰，並使其可供您使用。上傳檔案後，KMS 信任您的 vCenter Server 執行個體。

先決條件

- 從 KMS 廠商要求憑證和私密金鑰。檔案是採用 PEM 格式的 X509 檔案。

程序

1 登入 vSphere Web Client，然後選取 vCenter Server 系統。

2 按一下**設定**，然後選取**金鑰管理伺服器**。

3 選取想要與其建立信任連線的 KMS 執行個體。

4 選取**上傳憑證和私密金鑰**，然後按一下**確定**。

5 將您從 KMS 廠商接收的憑證貼至頂部文字方塊中，或按一下**上傳檔案**上傳憑證檔案。

6 將金鑰檔案貼至底部文字方塊中，或按一下**上傳檔案**上傳金鑰檔案。

7 按一下**確定**。

下一個

信任關係定案。請參閱完成信任設定。

設定預設 KMS 叢集

在下列情況下必須設定預設 KMS 叢集：沒有將第一個叢集設為預設叢集，或是您的環境使用多個叢集，而您移除了預設叢集。

先決條件

最佳做法是確認**金鑰管理伺服器**索引標籤中的 [連線狀態] 是否顯示 [正常] 和綠色核取記號。

程序

1 登入 vSphere Web Client，然後選取 vCenter Server 系統。

2 按一下**設定**索引標籤，然後按一下**更多**下的**金鑰管理伺服器**。

3 選取叢集，然後按一下**將 KMS 叢集設定為預設叢集**。

請勿選取伺服器。用於設定預設值的功能表僅適用於叢集。

4 按一下**是**。

叢集名稱旁會出現 `default` 字組。

完成信任設定

除非**新增伺服器**對話方塊提示您信任 KMS，否則您必須在憑證交換完成後明確建立信任。

可以透過信任 KMS 或上傳 KMS 憑證完成信任設定，即讓 vCenter Server 信任 KMS。您有兩個選項可供選擇：

- 使用**重新整理 KMS 憑證**選項明確信任憑證。
- 使用**上傳 KMS 憑證**選項，將 KMS 分葉憑證或 KMS CA 憑證上傳至 vCenter Server。

備註 如果您上傳根 CA 憑證或中繼 CA 憑證，vCenter Server 會信任由該 CA 簽署的所有憑證。為確保強大的安全性，請上傳 KMS 廠商控制的分葉憑證或中繼 CA 憑證。

程序

1 登入 vSphere Web Client，然後選取 vCenter Server 系統。

2 按一下**設定**，然後選取**金鑰管理伺服器**。

3 選取想要與其建立信任連線的 KMS 執行個體。

4 若要建立信任關係，請重新整理或上傳 KMS 憑證。

選項	動作
重新整理 KMS 憑證	a 按一下**所有動作**，然後選取**重新整理 KMS 憑證**。 b 在顯示的對話方塊中，按一下**信任**。
上傳 KMS 憑證	a 按一下**所有動作**，然後選取**上傳 KMS 憑證**。 b 在顯示的對話方塊中，按一下**上傳檔案**上傳憑證檔案，然後按一下**確定**。

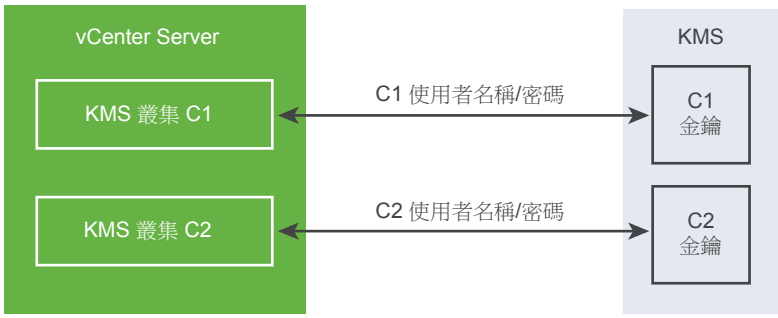
為不同使用者設定獨立的 KMS 叢集

您可以為相同 KMS 執行個體的不同使用者設定不同的 KMS 連線環境。有多個 KMS 連線非常有用，例如，如果您想授與公司的不同部門對不同 KMS 金鑰集的存取權限。

使用多個 KMS 叢集可讓您使用相同 KMS 來區隔金鑰。有不同的金鑰集對於使用案例 (如不同匯流排或不同客戶) 至關重要。

備註 並非所有 KMS 廠商都支援多個使用者。

圖 7-1 針對兩個不同使用者從 vCenter Server 連線至 KMS。



先決條件

設定與 KMS 的連線。請參閱設定金鑰管理伺服器叢集。

程序

1 在 KMS 上使用對應的使用者名稱和密碼建立兩個使用者，例如 C1 和 C2。

2 登入 vCenter Server 並建立第一個 KMS 叢集。

3 當提示輸入使用者名稱和密碼時，請提供第一個使用者的唯一資訊。

4 建立第二個 KMS 叢集並新增相同 KMS，但使用第二個使用者名稱和密碼 (C2)。

這兩個叢集獨立連線至 KMS，並使用不同的金鑰集。

建立加密儲存區原則

您必須先建立加密儲存區原則，然後才能建立加密的虛擬機器。建立一次儲存區原則後，每次加密虛擬機器或虛擬磁碟時都指派該原則。

如果想要將虛擬機器加密與其他 I/O 篩選器搭配使用，請參閱 *vSphere 儲存區* 說明文件以取得詳細資料。

先決條件

- 設定與 KMS 的連線。

  雖然可以在沒有 KMS 連線的情況下建立虛擬機器加密儲存區原則，但您在無法在建立與 KMS 伺服器的信任連線之前執行加密工作。
- 所需權限：**密碼編譯作業.管理加密原則**。

程序

1. 使用 vSphere Web Client 登入 vCenter Server。
2. 選取**首頁**，按一下**原則和設定檔**，然後按一下**虛擬機器儲存區原則**。
3. 按一下**建立虛擬機器儲存區原則**。
4. 指定儲存區原則值。
   a. 輸入儲存區原則名稱和選擇性說明，然後按**下一步**。
   b. 如果您對此精靈比較生疏，請先檢閱**原則結構**資訊，然後按**下一步**。
   c. 選取**使用虛擬機器儲存區原則中的一般規則**核取方塊。
   d. 按一下**新增元件**，選取**加密 > 預設加密內容**，然後按**下一步**。

      預設內容適合大多數情況。僅當您想要將加密和其他功能 (如快取或複寫) 結合使用時，才需要自訂原則。
   e. 取消選取**使用儲存區原則中的規則集**核取方塊，然後按**下一步**。
   f. 在**儲存區相容性**頁面上，保持 [相容] 為選取狀態，選擇資料存放區，然後按**下一步**。
   g. 檢閱資訊，然後按一下**完成**。

明確啟用主機加密模式

如果您想在 ESXi 主機上執行加密工作 (如建立加密的虛擬機器)，則必須啟用主機加密模式。在大多數情況下，當您執行加密工作時，會自動啟用主機加密模式。

在某些情況下，明確開啟加密模式是必要的。請參閱加密工作的必要條件和所需權限。

先決條件

所需權限：**Cryptographic operations.Register host**

程序

1 若要啟用主機加密模式，請遵循下列步驟。

2 透過使用 vSphere Web Client 連線至 vCenter Server。

3 選取 ESXi 主機，然後按一下**設定**。

4 在 [系統] 下，按一下**安全性設定檔**。

5 向下捲動至 [主機加密模式]，然後按一下**編輯**。

6 選取**已啟用**，然後按一下**確定**。

停用主機加密模式

當您執行加密工作時會自動啟用主機加密模式。啟用主機加密模式後，會加密所有核心傾印以避免敏感資訊洩漏給支援人員。如果您不再將虛擬機器加密用於 ESXi 主機，您可以停用加密模式。

程序

1 從主機解除登錄所有加密虛擬機器

2 從 vCenter Server 解除登錄。

3 將主機重新開機。

4 再次將主機登錄到 vCenter Server。

只要您不新增加密虛擬機器至主機，則主機加密模式會停用。

建立加密的虛擬機器

設定 KMS 後，您可以建立加密的虛擬機器。

此工作說明如何使用 vSphere Web Client 或 vSphere Client (以 HTML5 為基礎的用戶端) 建立已加密的虛擬機器。vSphere Client 會將儲存區原則篩選為包含虛擬機器加密的儲存區原則，從而便於建立已加密的虛擬機器。

備註 建立加密的虛擬機器比加密現有虛擬機器速度更快，且使用更少的儲存資源。如果可能，請在建立程序期間加密虛擬機器。

先決條件

- 建立與 KMS 的信任連線並選取預設 KMS。
- 建立加密儲存區原則，或使用綁定的範例「虛擬機器加密原則」。
- 確定虛擬機器已關閉電源。
- 確認您具有必要權限：
  - **密碼編譯作業.加密新增項目**
  - 如果主機加密模式未處於 [已啟用] 狀態，則還需要**密碼編譯作業.登錄主機**。

程序

1 透過使用 vSphere Client (以 HTML5 為基礎的用戶端) 或 vSphere Web Client 連線至 vCenter Server。

2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。

3 建立虛擬機器。

- vSphere Client：在物件上按一下滑鼠右鍵，然後選取**新增虛擬機器**。
- vSphere Web Client：在物件上按一下滑鼠右鍵，選取**新增虛擬機器 > 新增虛擬機器**。

4 依照提示建立已加密的虛擬機器。

選項	動作
選取建立類型	建立新的虛擬機器。
選取名稱和資料夾	指定虛擬機器的唯一名稱和目標位置。
選取運算資源	指定您有權限為其建立加密虛擬機器的物件。請參閱加密工作的必要條件和所需權限。
選取儲存區	vSphere Client：選取**加密此虛擬機器**核取方塊。將虛擬機器儲存區原則篩選為包含加密的儲存區原則。選取虛擬機器儲存區原則 (配套的範例為虛擬機器加密原則)，然後選取相容的資料存放區。 vSphere Web Client：選取使用加密的虛擬機器儲存區原則 (配套的範例為虛擬機器加密原則)。選取相容的資料存放區。
選取相容性	選取相容性。您只能將加密的虛擬機器移轉到含有相容性 ESXi 6.5 及更新版本的主機中。
選取客體作業系統	選取打算稍後安裝在虛擬機器上的客體作業系統。
自訂硬體	自訂硬體，例如，透過變更磁碟大小或 CPU。 vSphere Client：(選擇性) 選取**虛擬機器選項**索引標籤，然後開啟**加密**。選擇不進行加密的磁碟。當您取消選取磁碟時，僅加密虛擬機器首頁和任何其他選取的磁碟。 會加密您新增的所有新硬碟。您可稍後變更個別硬碟的儲存區原則。
即將完成	檢閱資訊，然後按一下**完成**。

複製加密的虛擬機器

複製加密的虛擬機器時，會使用相同的金鑰加密複製品。若要變更複製品的金鑰，請關閉虛擬機器的電源，並使用 API 對複製品執行雙重加密。請參閱 *vSphere Web Services SDK 程式設計指南*。

先決條件

- 建立與 KMS 的信任連線並選取預設 KMS。
- 建立加密儲存區原則，或使用綁定的範例「虛擬機器加密原則」。
- 必要權限：
  - **密碼編譯作業.複製**
  - 如果主機加密模式未處於 [已啟用] 狀態，則還需要**密碼編譯作業.登錄主機**權限。

程序

1 透過使用 vSphere Client (以 HTML5 為基礎的用戶端) 或 vSphere Web Client 連線至 vCenter Server。

2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。

3 若要建立已加密機器的複製品，請在虛擬機器上按一下滑鼠右鍵，然後依照提示操作。

選項	動作
選取名稱和資料夾	為複製品指定名稱和目標位置。
選取運算資源	指定您有權限為其建立加密虛擬機器的物件。請參閱加密工作的必要條件和所需權限。
選取儲存區	在**選取虛擬磁碟格式**功能表中進行選取，然後選取一個資料存放區。無法在複製作業進行時變更儲存區原則。
選取複製選項	按照 *vSphere 虛擬機器管理*說明文件中所述選取複製選項。
即將完成	檢閱資訊，然後按一下**完成**。

4 (選擇性) 變更已複製虛擬機器的金鑰。

依預設，會使用與父系相同的金鑰建立複製的虛擬機器。最佳做法是變更已複製虛擬機器的金鑰，以確保多部虛擬機器沒有相同的金鑰。

a 關閉虛擬機器電源。

b 使用 API 對複製品執行雙重加密。請參閱 *vSphere Web Services SDK 程式設計指南*。

若要使用不同的 DEK 和 KEK，請對已複製的虛擬機器執行深度雙重加密。若要使用不同的 KEK，請對已複製的虛擬機器執行淺層雙重加密。您可以在虛擬機器開啟電源時執行淺層雙重加密作業，除非虛擬機器已有快照存在。

加密現有虛擬機器或虛擬磁碟

您可以透過變更現有虛擬機器或虛擬磁碟的儲存區原則進行加密。您只能為已加密的虛擬機器加密虛擬磁碟。

此工作說明如何使用 vSphere Client (以 HTML5 為基礎的用戶端) 或 vSphere Web Client 加密現有的虛擬機器或虛擬磁碟。

虛擬機器加密功能示範 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vm_vsphere67_encryption)

先決條件

- 建立與 KMS 的信任連線並選取預設 KMS。
- 建立加密儲存區原則，或使用綁定的範例「虛擬機器加密原則」。
- 確定虛擬機器已關閉電源。
- 確認您具有必要權限：
  - **密碼編譯作業.加密新增項目**

- 如果主機加密模式未處於 [已啟用] 狀態，則還需要**密碼編譯作業.登錄主機**。

程序

1 透過使用 vSphere Client (以 HTML5 為基礎的用戶端) 或 vSphere Web Client 連線至 vCenter Server。

2 在想要變更的虛擬機器上按一下滑鼠右鍵，然後選取**虛擬機器原則 > 編輯虛擬機器儲存區原則**。

您可以設定虛擬機器檔案 (由虛擬機器首頁表示) 的儲存區原則，以及虛擬磁碟的儲存區原則。

3 選取儲存區原則。

- vSphere Client (以 HTML5 為基礎的用戶端)：
  - 若要加密虛擬機器及其硬碟，請選取加密儲存區原則，然後按一下**確定**。
  - 若要加密虛擬機器而不加密虛擬磁碟，請開啟**針對每個磁碟設定**，為虛擬機器首頁選取加密儲存區原則，並為虛擬磁碟選取其他儲存區原則，然後按一下**確定**。
- vSphere Web Client：
  - 若要加密虛擬機器及其硬碟，請選取加密儲存區原則，然後按一下**套用到全部**。
  - 若要加密虛擬機器而不加密虛擬磁碟，請為虛擬機器首頁選取加密儲存區原則，並為虛擬磁碟選取其他儲存區原則，然後按一下**套用**。

您無法加密未加密虛擬機器的虛擬磁碟。

4 如果您願意，可以從 vSphere Client 中的**編輯設定**功能表中加密虛擬機器或加密虛擬機器和磁碟。

a 在虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。

b 選取**虛擬機器選項**索引標籤，然後開啟**加密**。選擇加密原則。如果取消選取所有磁碟，則僅會加密虛擬機器首頁。

c 按一下**確定**。

解密已加密的虛擬機器或虛擬磁碟

您可以透過變更儲存區原則來解密虛擬機器和/或其磁碟。

此工作說明如何使用 vSphere Client (以 HTML5 為基礎的用戶端) 或 vSphere Web Client 解密已加密的虛擬機器。

所有已加密的虛擬機器均需要已加密的 vMotion。在虛擬機器解密期間，會保留 [已加密的 vMotion] 設定。若要變更此設定以不再使用 [已加密的 vMotion]，請明確變更此設定。

此工作說明如何使用儲存區原則執行解密。對於虛擬磁碟，您也可以使用**編輯設定**功能表執行解密。

先決條件

- 虛擬機器必須加密。
- 虛擬機器必須關閉電源或處於維護模式。
- 所需權限：**密碼編譯作業.解密**

程序

1 透過使用 vSphere Client (以 HTML5 為基礎的用戶端) 或 vSphere Web Client 連線至 vCenter Server。

2 在想要變更的虛擬機器上按一下滑鼠右鍵，然後選取**虛擬機器原則 > 編輯虛擬機器儲存區原則**。

您可以設定虛擬機器檔案 (由虛擬機器首頁表示) 的儲存區原則，以及虛擬磁碟的儲存區原則。

3 選取儲存區原則。

- vSphere Client (以 HTML5 為基礎的用戶端)：
  - 若要解密虛擬機器及其硬碟，請關閉**針對每個磁碟設定**，從下拉式功能表中選取儲存區原則，然後按一下**確定**。
  - 若要解密虛擬磁碟而不解密虛擬機器，請開啟**針對每個磁碟設定**，為虛擬機器首頁選取加密儲存區原則，並為虛擬磁碟選取其他儲存區原則，然後按一下**確定**。
- vSphere Web Client：
  - 若要解密虛擬機器及其硬碟，請從下拉式功能表中選取儲存區原則，按一下**全部套用**，然後按一下**確定**。
  - 若要解密虛擬磁碟而不解密虛擬機器，請從資料表中的下拉式功能表中選取虛擬磁碟的儲存區原則。請勿變更虛擬機器首頁的原則。按一下**確定**。

您無法解密虛擬機器並將磁碟保留為已加密。

4 如果您願意，可以使用 vSphere Client (以 HTML5 為基礎的用戶端)，從**編輯設定**功能表中解密虛擬機器和磁碟。

a 在虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。

b 選取**虛擬機器選項**索引標籤，然後展開**加密**。

c 若要解密虛擬機器及其硬碟，請從**加密虛擬機器**下拉式功能表中選擇**無**。

d 若要解密虛擬磁碟而不解密虛擬機器，請取消選取該磁碟。

e 按一下**確定**。

5 (選擇性) 可以變更 [已加密的 vMotion] 設定。

a 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。

b 按一下**虛擬機器選項**，然後開啟**加密**。

c 設定**已加密的 vMotion** 值。

變更虛擬磁碟的加密原則

從 vSphere Web Client 建立加密的虛擬機器時，會加密在虛擬機器建立期間新增的任何虛擬磁碟。您可以使用**編輯虛擬機器儲存區原則**選項解密虛擬磁碟。

備註 加密的虛擬機器可擁有未加密的虛擬磁碟。但是，未加密的虛擬機器不可擁有加密的虛擬磁碟。

請參閱虛擬磁碟加密。

此工作說明如何使用儲存區原則變更加密原則。您可以使用 vSphere Client (以 HTML5 為基礎的用戶端) 或 vSphere Web Client。您也可以使用**編輯設定**功能表進行此變更。

先決條件

- 您必須擁有**密碼編譯作業.管理加密原則**權限。
- 確定虛擬機器已關閉電源。

程序

1. 透過使用 vSphere Client (以 HTML5 為基礎的用戶端) 或 vSphere Web Client 連線至 vCenter Server。
2. 在虛擬機器上按一下滑鼠右鍵，然後選取**虛擬機器原則 > 編輯虛擬機器儲存區原則**。
3. 變更儲存區原則。
   - vSphere Client (以 HTML5 為基礎的用戶端)：
     - 若要變更虛擬機器及其硬碟的儲存區原則，請選取加密儲存區原則，然後按一下**確定**。
     - 若要加密虛擬機器而不加密虛擬磁碟，請開啟**針對每個磁碟設定**，為虛擬機器首頁選取加密儲存區原則，並為虛擬磁碟選取其他儲存區原則，然後按一下**確定**。
   - vSphere Web Client：
     - 若要變更虛擬機器及其硬碟的儲存區原則，請選取加密儲存區原則，然後按一下**全部套用**。
     - 若要加密虛擬機器而不加密虛擬磁碟，請為虛擬機器首頁選取加密儲存區原則，並為虛擬磁碟選取其他儲存區原則，然後按一下**套用**。

   您無法加密未加密虛擬機器的虛擬磁碟。
4. 如果您願意，可以從**編輯設定**功能表中變更儲存區原則。
   a. 在虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
   b. 選取**虛擬硬體**索引標籤，展開硬碟，然後從下拉式功能表中選擇加密原則。
   c. 按一下**確定**。

解決遺失金鑰問題

在某些情況下，ESXi 主機無法從 vCenter Server 取得已加密虛擬機器或已加密虛擬磁碟的金鑰 (KEK)。在這種情況下，您仍可以解除登錄或重新載入虛擬機器。然而，您無法執行其他虛擬機器作業，例如開啟虛擬機器的電源或刪除虛擬機器。當已加密的虛擬機器處於鎖定狀態時，vCenter Server 警示會通知您。在採取必要步驟使所需金鑰在 KMS 上可供使用後，可以使用 vSphere Client 解除鎖定已加密的虛擬機器。

如果虛擬機器金鑰無法使用，vSphere Web Client 中的虛擬機器狀態會顯示為無效。該虛擬機器無法開啟電源。如果虛擬機器金鑰可用，但是已加密磁碟的金鑰無法使用，則虛擬機器狀態不會顯示為無效。但是，虛擬機器無法開啟電源並產生下列錯誤：

```
The disk [/path/to/the/disk.vmdk] is encrypted and a required key was not found.
```

備註 下列程序說明會導致虛擬機器變為鎖定狀態的情況，顯示的對應警示和事件記錄，以及在每個案例中要執行的動作。

程序

1 如果 vCenter Server 系統和 KMS 之間的連線有問題，會產生虛擬機器警示並在事件記錄中顯示下列訊息：

由於 KMS 叢集錯誤，虛擬機器已鎖定。

必須手動檢查 KMS 叢集中的金鑰，然後還原與 KMS 叢集的連線。當 KMS 與金鑰可供使用時，解除鎖定已鎖定的虛擬機器。請參閱將鎖定的虛擬機器解除鎖定。也可以將主機重新開機並重新登錄虛擬機器，以便在還原連線後將其解除鎖定。

遺失與 KMS 的連線不會自動將虛擬機器鎖定。僅當滿足以下條件時，虛擬機器才會進入鎖定狀態：

- 該金鑰在 ESXi 主機上無法使用。
- vCenter Server 無法從 KMS 擷取金鑰。

每次重新開機後，ESXi 主機必須能夠連線 vCenter Server。vCenter Server 從 KMS 要求具有相應識別碼的金鑰，並使其可供 ESXi 使用。

如果在還原與 KMS 叢集的連線後虛擬機器保持鎖定狀態，請參閱將鎖定的虛擬機器解除鎖定。

2 如果連線已還原，請登錄虛擬機器。如果在嘗試登錄虛擬機器時產生錯誤，請確認您是否有 vCenter Server 系統的**密碼編譯作業.登錄虛擬機器**權限。

如果金鑰可用，則無需此權限即可開啟已加密虛擬機器的電源。如果必須擷取金鑰，則需要此權限來登錄虛擬機器。

3 如果 KMS 上的金鑰不再可用，會產生虛擬機器警示並在事件記錄中顯示下列訊息：

由於 KMS 叢集上的金鑰遺失，虛擬機器已鎖定。

要求 KMS 管理員還原金鑰。如果您要開啟電源的虛擬機器已從詳細目錄中移除並且很長時間未登錄，您可能會遇到非作用中金鑰。如果您將 ESXi 主機重新開機，而 KMS 不可用，也會發生此情況。

a 使用受管理物件瀏覽器 (MOB) 或 vSphere API 擷取金鑰識別碼。

從 `VirtualMachine.config.keyId.keyId` 擷取 `keyId`。

b 要求 KMS 管理員重新啟動與該金鑰識別碼相關聯的金鑰。

c 還原金鑰後，請參閱將鎖定的虛擬機器解除鎖定。

如果可在 KMS 上還原金鑰，則 vCenter Server 會擷取此金鑰，並在下次需要時將其推送至 ESXi 主機。

4 如果 KMS 可供存取且 ESXi 主機已開啟電源，但是 vCenter Server 系統無法使用，請遵循這些步驟解除鎖定虛擬機器。

   a 還原 vCenter Server 系統，或設定不同的 vCenter Server 系統，然後與 KMS 建立信任。

   您必須使用相同的 KMS 叢集名稱，但 KMS IP 位址可以不同。

   b 登錄所有鎖定的虛擬機器。

   新的 vCenter Server 執行個體會從 KMS 擷取金鑰，並且虛擬機器會解除鎖定。

5 如果只有 ESXi 主機上的金鑰遺失，會產生虛擬機器警示並在事件記錄中顯示下列訊息：

   由於主機上的金鑰遺失，虛擬機器已鎖定。

   vCenter Server 系統可以從 KMS 叢集擷取遺失金鑰。不需要手動復原金鑰。請參閱將鎖定的虛擬機器解除鎖定。

將鎖定的虛擬機器解除鎖定

當已加密的虛擬機器處於鎖定狀態時，vCenter Server 警示會通知您。在採取必要步驟使所需金鑰在 KMS 上可供使用後，可以使用 vSphere Client(以 HTML5 為基礎的用戶端) 解除鎖定已加密的虛擬機器。

先決條件

- 確認您具有所需權限：**密碼編譯作業.登錄虛擬機器**
- 執行選擇性工作可能需要其他權限，例如啟用主機加密。
- 解除鎖定已鎖定的虛擬機器之前，請查明鎖定原因，並嘗試手動修正此問題。請參閱解決遺失金鑰問題。

程序

1 透過使用 vSphere Client 連線至 vCenter Server。

2 導覽至虛擬機器的**摘要**索引標籤。

   當虛擬機器鎖定時，會顯示虛擬機器已鎖定警示。

3 決定是否要確認警示，還是將警示重設為綠色，但不立即解除鎖定虛擬機器。

   當您按一下**確認**或**重設為綠色**時，警示會消失，但虛擬機器會在解除鎖定之前保持鎖定狀態。

4 導覽至虛擬機器的**監控**索引標籤，然後按一下**事件**以取得有關為何鎖定虛擬機器的詳細資訊。

5 在解除鎖定虛擬機器之前執行建議的疑難排解。

6 導覽至虛擬機器的**摘要**索引標籤，然後按一下位於虛擬機器主控台下方的**解除鎖定虛擬機器**。

   此時會顯示一則訊息，警告加密金鑰資料已傳輸到主機。

7 按一下**是**。

解決 ESXi 主機加密模式問題

在某些情況下，ESXi 主機的加密模式會變為停用。

在包含任何已加密的虛擬機器的情況下，ESXi 主機需要啟用主機加密模式。如果主機偵測到其主機金鑰遺失，或如果 KMS 叢集不可用，則主機可能無法啟用加密模式。當無法啟用主機加密模式時，vCenter Server 會產生警示。

程序

1 如果 vCenter Server 系統和 KMS 叢集之間的連線有問題，會產生警示並在事件記錄中顯示下列訊息：

主機需要啟用加密模式，並且 KMS 叢集不可用。

您必須手動檢查 KMS 叢集中的金鑰，然後還原與 KMS 叢集的連線。

2 如果金鑰遺失，會產生警示並在事件記錄中顯示下列訊息：

主機需要啟用加密模式，並且金鑰在 KMS 叢集上不可用。

您必須將遺失的金鑰手動復原至 KMS 叢集。

下一個

還原與 KMS 叢集的連線或將金鑰手動復原至 KMS 叢集之後，如果主機加密模式仍保持停用，則重新啟用主機加密模式。請參閱重新啟用 ESXi 主機加密模式。

重新啟用 ESXi 主機加密模式

從 vSphere 6.7 開始，vCenter Server 警示會在 ESXi 主機的加密模式變為停用時通知您。在 vSphere 6.7 中，您可以重新啟用主機加密模式。

先決條件

- 確認您具有所需權限：**密碼編譯作業.登錄主機**。
- 重新啟用加密模式之前，請查明原因，並嘗試手動修正此問題。

程序

1 透過使用 vSphere Client 連線至 vCenter Server。

2 導覽至 ESXi 主機的**摘要**索引標籤。

停用加密模式時，會顯示 [主機需要啟用加密模式] 警示。

3 決定是否確認警示，還是將警示重設為綠色，但不立即重新啟用主機加密模式。

當您按一下**確認**或**重設為綠色**時，警示會消失，但主機加密模式會在重新啟用之前保持停用狀態。

4 導覽至 ESXi 主機的**監控**索引標籤，然後按一下**事件**以取得有關為何停用加密模式的詳細資訊。

執行建議的疑難排解，然後重新啟用加密模式。

5 在**摘要**索引標籤中，按一下**啟用主機加密模式**以重新啟用主機加密。

此時會顯示一則訊息，警告加密金鑰資料已傳輸到主機。

6 按一下**是**。

設定金鑰管理伺服器憑證到期臨界值

依預設，vCenter Server 會在金鑰管理伺服器 (KMS) 憑證到期前 30 天通知您。您可以變更此預設值。

KMS 憑證具有到期日期。達到到期日期的臨界值時，會顯示一則警示通知您。

vCenter Server 和 KMS 叢集交換兩種類型的憑證：伺服器和用戶端。vCenter Server 系統上的 VMware Endpoint Certificate Store (VECS) 會儲存伺服器憑證，並且每個 KMS 叢集儲存一個用戶端憑證。由於提供兩種憑證類型，因此每種憑證類型有兩個警示 (一個用於用戶端，一個用於伺服器)。

程序

1. 登入 vSphere Web Client，然後選取 vCenter Server 系統。
2. 按一下**設定**索引標籤。
3. 在**設定**下，按一下**進階系統設定**，然後按一下**編輯**。
4. 篩選或捲動至 `vpxd.kmscert.threshold` 組態參數。
5. 輸入您的值 (以天為單位)，然後按一下**確定**。

vSphere 虛擬機器加密和核心傾印

如果您的環境使用 vSphere 虛擬機器加密，且 ESXi 主機上發生錯誤，則產生的核心傾印會加密以保護客戶資料。此外，vm-support 套件中包含的核心傾印也會加密。

備註 核心傾印可能包含敏感資訊。處理核心傾印時，請遵循您組織的資料安全性和隱私權政策。

ESXi 主機上的核心傾印

當 ESXi 主機、使用者環境或虛擬機器出現當機時，會產生核心傾印，並且主機將重新開機。如果 ESXi 主機已啟用加密模式，會使用 ESXi 金鑰快取中的金鑰加密核心傾印。此金鑰來自 KMS。如需背景資訊，請參閱 vSphere 虛擬機器加密如何保護您的環境。

下表顯示依 vSphere 版本列出的用於每個核心傾印類型的加密金鑰。

表格 7-1. 核心傾印加密金鑰

核心傾印類型	加密金鑰 (ESXi 6.5)	加密金鑰 (ESXi 6.7 及更新版本)
ESXi 核心	主機金鑰	主機金鑰
使用者環境 (hostd)	主機金鑰	主機金鑰
加密的虛擬機器 (VM)	主機金鑰	虛擬機器金鑰

在 ESXi 主機重新開機後可執行的動作，視多個因素而定。

- 大多數情況下，vCenter Server 會為主機擷取來自 KMS 的金鑰，並在重新開機後嘗試將此金鑰推送給 ESXi 主機。如果此作業成功，您可以產生 vm-support 套件，並且可以解密或重新加密此核心傾印。請參閱解密或重新加密已加密的核心傾印。

- 如果 vCenter Server 無法連線至 ESXi 主機，您可能能夠擷取來自 KMS 的金鑰。請參閱解決遺失金鑰問題。
- 如果主機使用自訂金鑰，且該金鑰不同於 vCenter Server 推送給主機的金鑰，則您無法操縱核心傾印。請避免使用自訂金鑰。

核心傾印和 vm-support 套件

當您因嚴重錯誤連絡 VMware 技術支援時，您的支援代表通常會要求您產生 vm-support 套件。此套件包含記錄檔和其他資訊，包括核心傾印。如果支援代表無法透過查看記錄檔和其他資訊解決此問題，他們可能會要求您解密核心傾印並提供相關資訊。若要保護金鑰等敏感資訊，請遵循組織的安全性和隱私權政策。請參閱針對使用加密的 ESXi 主機收集 vm-support 套件。

vCenter Server 系統上的核心傾印

vCenter Server 系統上的核心傾印未加密。vCenter Server 已包含潛在的敏感資訊。至少確保 vCenter Server 執行所在的 Windows 系統或 vCenter Server Appliance 受到保護。請參閱第 4 章保護 vCenter Server 系統的安全。您也可以考慮關閉 vCenter Server 系統的核心傾印。記錄檔中的其他資訊可協助判定此問題。

針對使用加密的 ESXi 主機收集 vm-support 套件

如果已為 ESXi 啟用主機加密模式，則 `vm-support` 套件中的所有核心傾印皆已加密。您可以從 vSphere Web Client 收集套件，如果打算稍後解密核心傾印，您可以指定密碼。

`vm-support` 套件包含記錄檔、核心傾印檔案等。

先決條件

通知您的支援代表已針對 ESXi 主機啟用主機加密模式。您的支援代表可能會要求您解密核心傾印並擷取相關資訊。

備註 核心傾印可能包含敏感資訊。請遵循組織的安全性和隱私權政策以保護敏感資訊 (如主機金鑰)。

程序

1. 使用 vSphere Web Client 登入 vCenter Server 系統。
2. 按一下**主機和叢集**，然後在 ESXi 主機上按一下滑鼠右鍵。
3. 選取**匯出系統記錄**。
4. 在對話方塊中，選取**已加密核心傾印的密碼**，然後指定並確認密碼。
5. 其他選項保留預設值，或進行變更 (如果 VMware 技術支援要求)，然後按一下**完成**。
6. 指定檔案的位置。

7 如果您的支援代表要求您解密 vm-support 套件中的核心傾印，請登入任一 ESXi 主機並遵循下列步驟。

a 登入 ESXi 並連線至 vm-support 套件所在的目錄。

檔案名稱遵循 esx.date_and_time.tgz 模式。

b 確保有足夠的空間來儲存套件、未壓縮的套件和重新壓縮的套件，或移動套件。

c 將套件解壓縮到本機目錄。

```
vm-support -x *.tgz .
```

產生的檔案階層可能包含 ESXi 主機的核心傾印檔案 (通常位於 /var/core 中)，並且可能包含虛擬機器的多個核心傾印檔案。

d 分別解密每個加密的核心傾印檔案。

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

vm-support-incident-key-file 為您在目錄頂層找到的事件金鑰檔案。

encryptedZdump 為加密的核心傾印檔案的名稱。

decryptedZdump 為命令產生的檔案的名稱。讓該名稱與 *encryptedZdump* 名稱類似。

e 提供您在建立 vm-support 套件時所指定的密碼。

f 移除加密的核心傾印，並再次壓縮套件。

```
vm-support --reconstruct
```

8 移除包含機密資訊的任何檔案。

使用密碼匯出主機支援服務包 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_export_host_support_bundles_passwords)

解密或重新加密已加密的核心傾印

您可以透過使用 crypto-util CLI 解密或重新加密 ESXi 主機上的加密核心傾印。

您可以親自解密並檢查 vm-support 套件中的核心傾印。核心傾印可能包含敏感資訊。請遵循組織的安全性和隱私權政策以保護敏感資訊，例如金鑰。

如需有關重新加密 crypto-util 的核心傾印和其他功能的詳細資料，請參閱命令列說明。

備註 crypto-util 適用於進階使用者。

先決條件

用於加密核心傾印的金鑰必須在產生核心傾印的 ESXi 主機上可用。

程序

1 直接登入發生核心傾印的 ESXi 主機。

如果 ESXi 主機處於鎖定模式，或者如果 SSH 存取已停用，您可能必須首先啟用存取。

2 判斷核心傾印是否已加密。

選項	說明
監控核心傾印	`crypto-util envelope describe vmmcores.ve`
zdump 檔案	`crypto-util envelope describe --offset 4096 zdumpFile`

3 解密核心傾印 (視其類型而定)。

選項	說明
監控核心傾印	`crypto-util envelope extract vmmcores.ve vmmcores`
zdump 檔案	`crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted`

使用虛擬信賴平台模組保護虛擬機器

8

虛擬信賴平台模組 (vTPM) 功能可讓您將 TPM 2.0 虛擬密碼處理器新增至虛擬機器。

虛擬信賴平台模組概觀

vTPM 會在軟體中執行密碼編譯副處理器功能。新增至虛擬機器時，vTPM 可讓客體作業系統建立和儲存私有金鑰。這些金鑰不會向客體作業系統本身公開。因此，會減少虛擬機器攻擊面。通常，破壞客體作業系統會破壞其密碼，但啟用 vTPM 可大幅降低此風險。這些金鑰僅供客體作業系統用於加密或簽署。透過附加的 vTPM，第三方可遠端證明 (驗證) 韌體和客體作業系統的身分識別。

您可以將 vTPM 新增至新虛擬機器或現有的虛擬機器。vTPM 視虛擬機器加密來保護重要的 TPM 資料。當您設定 vTPM 時，虛擬機器加密會自動加密虛擬機器檔案，而不是磁碟。您可以選擇為虛擬機器及其磁碟明確新增加密。

您也可以備份已啟用 vTPM 的虛擬機器。備份必須包含所有虛擬機器資料，包括`*.nvram` 檔案。如果您的備份未包含`*.nvram` 檔案，則無法使用 vTPM 還原虛擬機器。此外，由於啟用 vTPM 之虛擬機器的虛擬機器主檔案已加密，請確保加密金鑰在還原時可供使用。

vTPM 不需要 ESXi 主機上存在實體信賴平台模組 (TPM) 2.0 晶片。但是，如果您想要執行主機證明，則需要 TPM 2.0 實體晶片等外部實體。請參閱使用信賴平台模組保護 ESXi 主機。

備註 依預設，沒有儲存區原則與已啟用 vTPM 的虛擬機器相關聯。僅加密虛擬機器檔案 (虛擬機器主檔案)。如果您願意，可以選擇為虛擬機器及其磁碟明確新增加密，但虛擬機器檔案已加密。

vTPM 的需求

若要使用 vTPM，您的 vSphere 環境必須符合下列需求：

- 虛擬機器需求：
  - EFI 韌體
  - 硬體版本 14
- 元件需求：
  - vCenter Server6.7。
  - 虛擬機器加密 (加密虛擬機器主檔案)。

  - 針對 vCenter Server 設定金鑰管理伺服器 (KMS) (虛擬機器加密取決於 KMS)。請參閱設定金鑰管理伺服器叢集。
- 客體作業系統支援：
  - Windows Server 2016 (64 位元)
  - Windows 10 (64 位元)

硬體 TPM 和虛擬 TPM 之間的差異

將硬體信賴平台模組 (TPM) 用作密碼編譯副處理器，以提供安全的認證或金鑰儲存區。vTPM 與 TPM 執行相同的功能，但在軟體中執行密碼編譯副處理器功能。vTPM 使用 `.nvram` 檔案做為其安全的儲存區，該檔案透過虛擬機器加密進行加密。

硬體 TPM 包含預先載入的金鑰，稱為簽署金鑰 (EK)。EK 具有私密和公開金鑰。EK 為 TPM 提供唯一的身分識別。對於 vTPM，將由 VMware Certificate Authority (VMCA) 或第三方憑證授權機構 (CA) 提供此金鑰。一旦 vTPM 使用金鑰，該金鑰通常不會變更，因為這樣做會導致 vTPM 中儲存的敏感資訊失效。vTPM 在任何時候都不會連線 CA。

本章節討論下列主題:

- 新增虛擬信賴平台模組到虛擬機器
- 為現有虛擬機器啟用虛擬信賴平台模組
- 從虛擬機器移除虛擬信賴平台模組
- 識別已啟用虛擬信賴平台的虛擬機器
- 檢視 vTPM 模組裝置憑證
- 匯出並取代 vTPM 模組裝置憑證

新增虛擬信賴平台模組到虛擬機器

您可以將虛擬信賴平台模組 (vTPM) 新增至虛擬機器，以增強客體作業系統的安全性。必須先設定 KMS，然後才能新增 vTPM。

您可以為 vSphere 6.7 及更新版本上執行的虛擬機器啟用 vTPM。VMware 虛擬 TPM 與 TPM 2.0 相容，並且會建立啟用 TPM 的虛擬晶片以供虛擬機器及其裝載的客體作業系統使用。

先決條件

- 確保針對虛擬機器加密設定您的 vSphere 環境。請參閱設定金鑰管理伺服器叢集。
- 您使用的客體作業系統必須為 Windows Server 2016 (64 位元) 或 Windows 10 (64 位元)。
- 您環境中執行的 ESXi 主機必須是 ESXi 6.7 或更新版本。
- 虛擬機器必須使用 EFI 韌體。

程序

1 透過使用 vSphere Client 連線至 vCenter Server。

2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。

3 在物件上按一下滑鼠右鍵，選取**新虛擬機器**，然後遵循提示來建立虛擬機器。

選項	動作
選取建立類型	建立新的虛擬機器。
選取名稱和資料夾	指定名稱和目標位置。
選取運算資源	指定您有權限為其建立虛擬機器的物件。請參閱加密工作的必要條件和所需權限。
選取儲存區	選取相容的資料存放區。
選取相容性	選取 **ESXi 6.7 及更新版本**。
選取客體作業系統	選取 Windows Server 2016 (64 位元) 或 Windows 10 (64 位元) 用做客體作業系統。
自訂硬體	按一下**新增裝置**，然後選取**信賴平台模組**。 您可以進一步自訂硬體，例如，透過變更磁碟大小或 CPU。
即將完成	檢閱資訊，然後按一下**完成**。

啟用 vTPM 的虛擬機器即顯示在您所指定的詳細目錄中。

為現有虛擬機器啟用虛擬信賴平台模組

您可以將虛擬信賴平台模組 (vTPM) 新增至現有虛擬機器，以增強客體作業系統的安全性。必須先設定 KMS，然後才能新增 vTPM。

您可以為 vSphere 6.7 及更新版本上執行的虛擬機器啟用 vTPM。VMware 虛擬 TPM 與 TPM 2.0 相容，並且會建立啟用 TPM 的虛擬晶片以供虛擬機器及其裝載的客體作業系統使用。

先決條件

- 確保針對虛擬機器加密設定您的 vSphere 環境。請參閱設定金鑰管理伺服器叢集。
- 您使用的客體作業系統必須為 Windows Server 2016 (64 位元) 或 Windows 10 (64 位元)。
- 確認已關閉虛擬機器。
- 您環境中執行的 ESXi 主機必須是 ESXi 6.7 或更新版本。
- 虛擬機器必須使用 EFI 韌體。

程序

1 透過使用 vSphere Client 連線至 vCenter Server。

2 在您想要修改的詳細目錄中的虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。

3 在 [**編輯設定**] 對話方塊中，按一下**新增裝置**，然後選取**信賴平台模組**。

4 按一下**確定**。

虛擬機器的**摘要**索引標籤的**虛擬機器硬體**窗格中現在會包括 [虛擬信賴平台模組]。

從虛擬機器移除虛擬信賴平台模組

您可以從虛擬機器移除虛擬信賴平台模組 (vTPM) 安全性。

移除 vTPM 會導致虛擬機器上的所有加密資訊變得無法復原。此外，移除 vTPM 會起始虛擬機器立即重新開機。從虛擬機器移除 vTPM 之前，停用使用 vTPM 的客體作業系統中的所有應用程式，例如 BitLocker。不執行此操作可能會導致虛擬機器無法開機。

程序

1. 透過使用 vSphere Client 連線至 vCenter Server。
2. 在您想要修改的詳細目錄中的虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
3. 在 [**編輯設定**] 對話方塊的**虛擬硬體**索引標籤中，找到信賴平台模組項目。
4. 將游標移至裝置上方，然後按一下**移除**圖示。

   只有可安全移除的虛擬硬體才會顯示此圖示。
5. 按一下**刪除**以確認您要移除裝置。

   vTPM 裝置已標記為移除。
6. 按一下**確定**。

   確認虛擬信賴平台模組項目不再顯示於虛擬機器的**摘要**索引標籤的**虛擬機器硬體**窗格中。

識別已啟用虛擬信賴平台的虛擬機器

您可以識別哪些虛擬機器能夠使用虛擬信賴平台模組 (vTPM)。

您可以產生詳細目錄中所有虛擬機器的清單，其中顯示虛擬機器名稱、作業系統和 vTPM 狀態。您也可以將此清單匯出至 CSV 檔案，以用於合規性稽核。

程序

1. 透過使用 vSphere Client 連線至 vCenter Server。
2. 選取 vCenter Server 執行個體、主機或叢集。
3. 按一下**虛擬機器**索引標籤，然後按一下**虛擬機器**。
4. 按一下任何虛擬機器資料行的功能表列，選取**顯示/隱藏資料行**，然後選取 **TPM**。

   TPM 資料行針對已啟用 TPM 的所有虛擬機器顯示為存在。未啟用 TPM 的虛擬機器會列為不存在。
5. 您可以將詳細目錄清單視圖的內容匯出至 CSV 檔案。
   a. 按一下清單視圖右下角的**匯出**。

      [匯出清單內容] 對話方塊隨即開啟，並列出 CSV 檔案中包含項目的可用選項。
   b. 選取是要將全部資料列還是目前所選的資料列列在 CSV 檔案中。

c 透過可用選項，選取要列在 CSV 檔案中的資料行。

d 按一下**匯出**。

CSV 檔案隨即產生且可供下載。

檢視 vTPM 模組裝置憑證

虛擬信賴平台模組 (vTPM) 裝置預先設定了可供您檢閱的預設憑證。

先決條件

您的環境中必須具有已啟用 vTPM 的虛擬機器。

程序

1 透過使用 vSphere Client 連線至 vCenter Server。

2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。

3 選取要檢視其憑證資訊的已啟用 vTPM 的虛擬機器。

4 按一下**設定**索引標籤。

5 在 **TPM** 下，選取**憑證**。

6 選取要檢視其資訊的憑證。

7 (選擇性) 若要匯出憑證資訊，請按一下**匯出**。

憑證會儲存到磁碟。

下一個

您可以使用第三方憑證授權機構 (CA) 核發的憑證取代預設憑證。請參閱匯出並取代 vTPM 模組裝置憑證。

匯出並取代 vTPM 模組裝置憑證

您可以取代虛擬信賴平台模組 (vTPM) 裝置隨附的預設憑證。

先決條件

您的環境中必須具有已啟用 vTPM 的虛擬機器。

程序

1 透過使用 vSphere Client 連線至 vCenter Server。

2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。

3 在想要取代其憑證資訊的詳細目錄中，選取已啟用 vTPM 的虛擬機器。

4 按一下**設定**索引標籤。

5 在 **TPM** 下，選取**簽署要求**。

6 選取憑證。

7 若要匯出憑證資訊，請按一下**匯出**。

憑證會儲存到磁碟。

8 根據匯出的憑證簽署要求 (CSR) 取得第三方憑證授權機構 (CA) 核發的憑證。

您可以使用 IT 環境中可能具有的任何測試 CA。

9 如果您有新的憑證，請取代現有憑證。

a 在您想要取代其憑證的詳細目錄中的虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。

b 在**編輯設定**對話方塊中，展開**信賴平台模組**。

將顯示憑證。

c 針對您想要取代的憑證，按一下**取代**。

將顯示**檔案上傳**對話方塊。

d 在您的本機機器上，找到新憑證並上傳。

新憑證會取代 vTPM 裝置隨附的預設憑證。

e 在虛擬機器的 **[摘要]** 索引標籤的**虛擬信賴平台模組**清單下，憑證名稱將會更新。

透過虛擬式安全性保護 Windows 客體作業系統

9

從 vSphere 6.7 開始，您可以在支援的 Windows 客體作業系統上啟用 Microsoft 虛擬式安全性 (VBS)。

關於虛擬式安全性

Microsoft VBS 是 Windows 10 和 Windows Server 2016 作業系統的一項功能，可使用硬體和軟體虛擬化透過建立隔離、受 Hypervisor 限制的專用子系統來增強系統安全性。

VBS 可讓您使用下列 Windows 安全性功能來強化系統，並隔離關鍵系統和使用者密碼使其不受影響：

- Credential Guard：旨在隔離和強化關鍵系統和使用者密碼使其不受影響。
- Device Guard：提供一組功能，旨在共同運作來防止及避免惡意程式碼在 Windows 系統上執行。
- 可設定的程式碼完整性：可確保只有受信任的程式碼可從開機載入器開始執行。

如需詳細資訊，請參閱 Microsoft 說明文件中有關虛擬式安全性的主題。

透過 vCenter Server 為虛擬機器啟用 VBS 之後，您可以在 Windows 客體作業系統內啟用 VBS。

本章節討論下列主題:

虛擬式安全性最佳做法

請遵循虛擬式安全性 (VBS) 的最佳做法，盡可能地提高 Windows 客體作業系統環境的安全性和管理性。

遵循這些最佳做法來避免出現問題。

VBS 硬體

針對 VBS 使用下列 Intel 硬體：

- Haswell CPU 或更新版本。為獲得最佳效能，請使用 Skylake-EP CPU 或更新版本。
- Ivybridge CPU 是可接受的。
- Sandybridge CPU 可能會導致部分效能降低。

並非所有 VBS 功能在 AMD CPU 上均可使用。如需詳細資訊，請參閱 VMware 知識庫文章 https://kb.vmware.com/s/article/53003。

Windows 客體作業系統相容性

在 vSphere 6.7 中，雖然版本 1607 及 1703 需要修補程式，Windows 10 和 Windows Server 2016 虛擬機器都支援 VBS。查看 Microsoft 說明文件以瞭解 ESXi 主機硬體相容性。

Windows 客體作業系統 RS1、RS2 和 RS3 中的 VBS 都需要 HyperV，才能在客體作業系統中啟用。如需詳細資訊，請參閱《*VMware vSphere 版本說明*》。

VBS 上不支援的 VMware 功能

啟用 VBS 時，虛擬機器不支援下列功能：

- Fault Tolerance
- PCI 傳遞
- CPU 或記憶體熱新增

VBS 的安裝和升級注意須知

設定 VBS 之前，請瞭解下列安裝和升級注意須知：

- 在低於版本 14 的硬體版本上針對 Windows 10 和 Windows Server 2016 設定的新虛擬機器，預設為使用舊版 BIOS 進行建立。將虛擬機器的韌體類型從舊版 BIOS 變更為 UEFI 後，您必須重新安裝客體作業系統。
- 如果您計劃將虛擬機器從舊版 vSphere 移轉至 vSphere 6.7 或更高版本，並且在虛擬機器上啟用 VBS，請使用 UEFI 來避免重新安裝作業系統。

在虛擬機器上啟用虛擬式安全性

建立虛擬機器的同時，可以為支援的 Windows 客體作業系統啟用 Microsoft 虛擬式安全性 (VBS)。

啟用 VBS 的程序涉及首先在虛擬機器中啟用 VBS，然後在 Windows 客體作業系統中啟用 VBS。

先決條件

建議使用 Intel 主機。如需可接受的 CPU，請參閱虛擬式安全性最佳做法。

建立使用硬體版本 14 或更新版本以及下列其中一個支援的客體作業系統的虛擬機器：

- Windows 10 (64 位元)
- Windows Server 2016 (64 位元)

程序

1 透過使用 vSphere Client 連線至 vCenter Server。

2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。

3 在物件上按一下滑鼠右鍵，選取**新虛擬機器**，然後遵循提示來建立虛擬機器。

選項	動作
選取建立類型	建立虛擬機器。
選取名稱和資料夾	指定名稱和目標位置。
選取運算資源	指定您有權限為其建立虛擬機器的物件。
選取儲存區	在虛擬機器儲存區原則中，選取儲存區原則。選取相容的資料存放區。
選取相容性	確保已選取 **ESXi 6.7 及更新版本**。
選取客體作業系統	選取 Windows 10 (64 位元) 或 Windows Server 2016 (64 位元)。選取**啟用 Windows 虛擬式安全性**核取方塊。
自訂硬體	自訂硬體，例如，透過變更磁碟大小或 CPU。
即將完成	檢閱資訊，然後按一下**完成**。

一旦建立虛擬機器，請確認其**摘要**索引標籤在客體作業系統說明中顯示「VBS true」。

下一個

請參閱在客體作業系統上啟用以虛擬化為基礎的安全性。

在現有虛擬機器上啟用以虛擬化為基礎的安全性

您可以為支援的 Windows 客體作業系統在現有虛擬機器上啟用 Microsoft 虛擬式安全性 (VBS)。

啟用 VBS 的程序涉及首先在虛擬機器中啟用 VBS，然後在客體作業系統中啟用 VBS。

備註 在低於版本 14 的硬體版本上針對 Windows 10 和 Windows Server 2016 設定的新虛擬機器，預設為使用舊版 BIOS 進行建立。如果將虛擬機器的韌體類型從舊版 BIOS 變更為 UEFI，您必須重新安裝客體作業系統。

先決條件

建議使用 Intel 主機。如需可接受的 CPU，請參閱虛擬式安全性最佳做法。

必須已使用硬體版本 14 或更新版本、UEFI 韌體，以及下列其中一個支援的客體作業系統建立虛擬機器：

- Windows 10 (64 位元)
- Windows Server 2016 (64 位元)

程序

1 在 vSphere Client 中，瀏覽到虛擬機器。

2 在虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。

3 按一下**虛擬機器選項**索引標籤。

4 針對虛擬式安全性勾選**啟用**核取方塊。

5 按一下**確定**。

請確認虛擬機器的**摘要**索引標籤在客體作業系統說明中顯示「VBS true」。

下一個

請參閱在客體作業系統上啟用以虛擬化為基礎的安全性。

在客體作業系統上啟用以虛擬化為基礎的安全性

您可以為支援的 Windows 客體作業系統啟用 Microsoft 虛擬式安全性 (VBS)。

從 Windows 客體作業系統內啟用 VBS。Windows 會透過群組原則物件 (GPO) 設定和強制執行 VBS。GPO 可讓您關閉和開啟各種服務，例如 VBS 提供的安全開機、Device Guard 和 Credential Guard。某些 Windows 版本還需要您執行啟用 Hyper-V 平台的其他步驟。

如需詳細資料，請參閱有關部署 Device Guard 以啟用虛擬式安全性的 Microsoft 說明文件。

先決條件

- 確定虛擬機器上已啟用虛擬式安全性。

程序

1 在 Microsoft Windows 中，編輯群組原則以開啟 VBS 並選擇其他與 VBS 相關的安全性選項。

2 (選擇性) 對於低於 Redstone 4 的 Microsoft Windows 版本，請在 Windows 功能控制台中啟用 Hyper-V 平台。

3 將客體作業系統重新開機。

停用以虛擬化為基礎的安全性

如果您無法再對虛擬機器使用虛擬式安全性 (VBS)，您可以停用 VBS。針對虛擬機器停用 VBS 時，Windows VBS 選項保持不變，但可能會引發效能問題。在虛擬機器上停用 VBS 之前，請停用 Windows 內的 VBS 選項。

先決條件

確定虛擬機器已關閉電源。

程序

1. 在 vSphere Client 中，瀏覽到已啟用 VBS 的虛擬機器。

   如需有關尋找已啟用 VBS 的虛擬機器的說明，請參閱識別已啟用 VBS 的虛擬機器。
2. 在虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
3. 按一下**虛擬機器選項**。
4. 針對虛擬式安全性取消選取**啟用**核取方塊。

   會出現訊息提醒您在客體作業系統中停用 VBS。
5. 按一下**確定**。
6. 請確認虛擬機器的**摘要**索引標籤不會再在客體作業系統說明中顯示「VBS true」。

識別已啟用 VBS 的虛擬機器

您可以識別哪些虛擬機器已啟用 VBS，用於進行報告和符合性。

程序

1. 透過使用 vSphere Client 連線至 vCenter Server。
2. 在詳細目錄中選取 vCenter Server 執行個體、資料中心或主機。
3. 按一下**虛擬機器**索引標籤，然後按一下**虛擬機器**。
4. 在虛擬機器的清單中，按一下資料行標頭中的向下箭頭，以顯示/隱藏資料行，然後選取 **VBS** 核取方塊。

   會顯示 **VBS** 資料行。
5. 掃描 **VBS** 資料行中是否存在。

確保 vSphere 網路安全

10

確保 vSphere 網路安全是保護環境的基礎部分。可以透過不同的方式確保不同 vSphere 元件的安全。如需 vSphere 環境中網路的詳細資訊，請參閱 *vSphere 網路*說明文件。

本章節討論下列主題:

vSphere 網路安全性簡介

vSphere 環境中的網路安全性不僅具有保護實體網路環境的許多特性，而且具有一些僅適用於虛擬機器的特性。

防火牆

為虛擬網路新增防火牆保護，方法是在其中的部分或所有虛擬機器上安裝和設定以主機為基礎的防火牆。

為提高效率，您可以設定私人虛擬機器乙太網路或虛擬網路。有了虛擬網路，您可以在虛擬網路最前面的虛擬機器上安裝以主機為基礎的防火牆。此防火牆可以用作實體網路介面卡和虛擬網路中剩餘虛擬機器之間的保護緩衝區。

以主機為基礎的防火牆可能會降低效能。請先根據效能目標平衡安全性需求，然後在虛擬網路中的其他虛擬機器上安裝以主機為基礎的防火牆。

請參閱使用防火牆確保網路安全。

分割

將主機中的不同虛擬機器區域置於不同網路區段。如果將每個虛擬機器區域隔離在各自的網路區段中，可以大大降低區域之間洩漏資料的風險。分割可防止多種威脅，包括位址解析通訊協定 (ARP) 詐騙。使用 ARP 詐騙，攻擊者可操縱 ARP 資料表以重新對應 MAC 和 IP 位址，從而存取進出主機的網路流量。攻擊者使用 ARP 詐騙產生攔截式 (MITM) 攻擊、執行拒絕服務 (DoS) 攻擊、劫持目標系統，並以其他方式破壞虛擬網路。

仔細規劃分割可減少虛擬機器區域之間封包傳輸的機會。因此，分割可防止嗅探攻擊 (嗅探攻擊需向受害者傳送網路流量)。此外，攻擊者無法使用一個虛擬機器區域中的不安全服務存取主機中的其他虛擬機器區域。可以使用兩種方法之一實作分割。

- 為虛擬機器區域使用單獨的實體網路介面卡，確保已將區域隔離。為虛擬機器區域使用單獨的實體網路介面卡可能是最安全的方法。在建立初始區段之後，此方法更不容易出現錯誤組態。
- 設定虛擬區域網路 (VLAN)，協助保護網路。VLAN 幾乎能夠提供實際實作單獨網路所具有的所有安全性優點，且不增加硬體額外負荷。VLAN 可為您節省部署和維護其他裝置、纜線等成本。請參閱透過 VLAN 保護虛擬機器的安全。

防止未經授權的存取

保護虛擬機器安全的需求通常與保護實體機器安全的需求相同。

- 如果將虛擬機器網路連線到實體網路，將會遭到破壞，就像由實體機器組成的網路一樣。
- 即使沒有將虛擬機器連線到實體網路，虛擬機器也可能會遭到其他虛擬機器攻擊。

虛擬機器之間相互隔離。一個虛擬機器無法讀取或寫入另一個虛擬機器的記憶體、無法存取其資料、無法使用其應用程式等等。但是，在網路中，任何虛擬機器或虛擬機器群組仍可能遭到其他虛擬機器的未經授權存取。保護您的虛擬機器免受此類未經授權的存取。

使用防火牆確保網路安全

安全性管理員使用防火牆，保護網路或網路中的選取元件不受到入侵。

防火牆可控制對保護範圍內裝置的存取，方法是關閉所有連接埠，管理員顯式或隱式指定的授權連接埠除外。管理員開啟的連接埠允許防火牆內外裝置間的流量。

重要事項 ESXi 5.5 及更新版本中的 ESXi 防火牆不允許每個網路篩選 vMotion 流量。因此，必須在外部防火牆上安裝規則，才能確認 vMotion 通訊端沒有傳入連線。

在虛擬機器環境中，您可以為元件之間的防火牆規劃配置。

- 實體機器 (如，vCenter Server 系統和 ESXi 主機) 之間的防火牆。

- 一個虛擬機器與另一個虛擬機器之間的防火牆 (例如，在做為外部 Web 伺服器的虛擬機器與連線到公司內部網路的虛擬機器之間)。
- 實體機器與虛擬機器之間的防火牆 (例如，將防火牆置於實體網路介面卡和虛擬機器之間)。

防火牆在 ESXi 組態中的使用方式，取決於您打算如何使用網路以及必須為特定的元件提供何等級別的安全。例如，如果在您建立的虛擬網路中，每個虛擬機器專用於執行同一部門的不同基準測試套件，那麼從一個虛擬機器對相鄰虛擬機器進行不需要的存取的風險最小。因此，防火牆存在於虛擬機器之間的組態不是必要的。但是，為了防止外部主機的測試執行中斷，您可以在虛擬網路的進入點設定防火牆來保護整個虛擬機器集。

如需取得防火牆連接埠的圖，請參閱 VMware 知識庫文章 2131180。

針對具有 vCenter Server 的組態設定防火牆

如果要透過 vCenter Server 存取 ESXi 主機，通常會使用防火牆來保護 vCenter Server。

必須在進入點佈設防火牆。防火牆可能位於用戶端和 vCenter Server 或 vCenter Server 之間，並且用戶端均可受防火牆保護。

如需 TCP 和 UDP 連接埠的完整清單，請參閱 vCenter Server 與 Platform Services Controller 所需的連接埠和其他 vCenter Server TCP 和 UDP 連接埠。

設定了 vCenter Server 的網路可透過 vSphere Web Client、其他 UI 用戶端或使用 vSphere API 的用戶端接收通訊。在一般作業期間，vCenter Server 會在指定的連接埠上接聽來自其受管理的主機和用戶端的資料。vCenter Server 還假定其受管理主機會在指定的連接埠上接聽來自 vCenter Server 的資料。如果在其中任一元素之間存在防火牆，必須確保防火牆中有開啟的連接埠可支援資料傳輸。

您可能還可以在網路中的其他存取點處佈設防火牆，具體取決於網路使用量及用戶端所需的安全性層級。根據網路組態的安全性風險，選取防火牆位置。通常使用以下防火牆位置。

- 在 vSphere Web Client 或第三方網路管理用戶端與 vCenter Server 之間。
- 在網頁瀏覽器與 ESXi 主機之間 (如果使用者透過網頁瀏覽器存取虛擬機器)。
- 在 vSphere Web Client 與 ESXi 主機之間 (如果使用者透過 vSphere Web Client 存取虛擬機器)。此連線是 vSphere Web Client 與 vCenter Server 之間連線的補充，它需要一個不同的連接埠。
- 在 vCenter Server 與 ESXi 主機之間。
- 在網路中的 ESXi 主機之間。儘管主機之間的流量通常被認為是受信任的，但是，如果您擔心電腦間存在安全性缺口，可以在主機間新增防火牆。

  如果要在 ESXi 主機間新增防火牆，並打算在這些主機間移轉虛擬機器，則在將來源主機和目標主機分隔開的任何防火牆中開啟連接埠。
- 在 ESXi 主機與網路儲存區 (如 NFS 或 iSCSI 儲存區) 之間。這些連接埠並非專屬於 VMware。可根據網路規格進行設定。

透過防火牆連線到 vCenter Server

在防火牆中開啟 TCP 連接埠 443，讓 vCenter Server 能夠接收資料。依預設，vCenter Server 使用 TCP 連接埠 443 來接聽其用戶端的資料。如果您在 vCenter Server 及其用戶端之間設有防火牆，必須設定可讓 vCenter Server 從用戶端接收資料的連線。

防火牆組態取決於您的站台所使用的內容，請連絡您的本機防火牆系統管理員以取得相關資訊。開啟連接埠的方式取決於您使用的是 vCenter Server Appliance 還是 vCenter Server Windows 安裝。

透過防火牆連線 ESXi 主機

如果您在 ESXi 主機及 vCenter Server 之間設有防火牆，請確保受管理的主機能夠接收資料。

若要設定用於接收資料的連線，請開啟用於 vSphere High Availability、vMotion、vSphere Fault Tolerance 等服務的流量的連接埠。如需組態檔、vSphere Web Client 存取權限，以及防火牆命令的討論，請參閱 ESXi 防火牆組態。如需連接埠清單，請參閱 ESXi 主機的傳入和傳出防火牆連接埠。

針對沒有 vCenter Server 的組態設定防火牆

如果您的環境不包含 vCenter Server，用戶端可以直接連線到 ESXi 網路。

您可以使用數種方式連線到獨立 ESXi 主機。

- VMware Host Client
- 其中一個 vSphere 命令列介面
- vSphere Web Services SDK 或 vSphere Automation SDK
- 第三方用戶端

獨立主機的防火牆需求與存在 vCenter Server 時的需求相似。

- 使用防火牆保護 ESXi 層，或保護用戶端及 ESXi 層，具體取決於您的組態。該防火牆可為網路提供基本保護。
- 此類組態中的授權是您在每個主機上安裝的 ESXi 套件的一部分。由於授權功能駐留在 ESXi 上，因此無需帶防火牆的單獨授權伺服器。

您可以使用 ESXCLI 或使用 VMware Host Client 設定防火牆連接埠。請參閱 *vSphere 單一主機管理 - VMware Host Client*。

透過防火牆連線到虛擬機器主控台

特定連接埠必須開啟，使用者和管理員才能與虛擬機器主控台通訊。必須開啟哪些連接埠會視虛擬機器主控台的類型，以及是透過包含 vSphere Web Client 的 vCenter Server 連線還是直接從 VMware Host Client 連線到 ESXi 主機而定。

透過 vSphere Web Client 連線到以瀏覽器為基礎的虛擬機器主控台

使用 vSphere Web Client 進行連線時，一律會連線到管理 ESXi 主機的 vCenter Server 系統，並從該處存取虛擬機器主控台。

如果使用 vSphere Web Client 並連線到以瀏覽器為基礎的虛擬機器主控台，則必須可進行下列存取：

- 防火牆必須允許 vSphere Web Client 在連接埠 9443 上存取 vCenter Server。
- 防火牆必須允許 vCenter Server 在連接埠 902 上存取 ESXi 主機。

透過 vSphere Web Client 連線到獨立式虛擬機器主控台

如果使用 vSphere Web Client 並連線到獨立式虛擬機器主控台，則必須可進行下列存取：

- 防火牆必須允許 vSphere Web Client 在連接埠 9443 上存取 vCenter Server。
- 防火牆必須允許獨立式虛擬機器主控台在連接埠 9443 上存取 vCenter Server，以及在連接埠 902 上存取 ESXi 主機。

使用 VMware Host Client 直接連線到 ESXi 主機

如果直接連線到 ESXi 主機，則可以使用 VMware Host Client 虛擬機器主控台。

備註　請勿使用 VMware Host Client 直接連線到由 vCenter Server 系統管理的主機。如果您透過 VMware Host Client 對此類主機進行變更，會導致環境不穩定。

防火牆必須允許在連接埠 443 和 902 上存取 ESXi 主機

VMware Host Client 使用連接埠 902 為虛擬機器上的客體作業系統 MKS 活動提供連線。使用者正是透過此連接埠，與虛擬機器的客體作業系統及應用程式進行互動。VMware 不支援為此功能設定不同的連接埠。

確保實體交換器安全

確保每個 ESXi 主機上實體交換器的安全，以防止攻擊者取得主機及其虛擬機器的存取權。

為了最好地保護主機，請確保實體交換器連接埠已設定為停用跨距樹狀目錄，並確保為外部實體交換器和虛擬交換器 (在虛擬交換器標記 (VST) 模式下) 之間的主幹連結設定了非交涉選項。

程序

1. 登入實體交換器並確保跨距樹狀目錄通訊協定已停用，或確保為連線到 ESXi 主機的所有實體交換器連接埠設定了 [連接埠快速] 。
2. 對於執行橋接或路由傳送的虛擬機器，定期檢查第一個上游實體交換器連接埠是否設定為停用 BPDU 防護和 [連接埠快速]，並啟用跨距樹狀目錄通訊協定。

   在 vSphere 5.1 及更新版本中，為了防止實體交換器受到潛在的拒絕服務 (DoS) 攻擊，可以在 ESXi 主機上開啟客體 BPDU 篩選器。
3. 登入實體交換器，並確保已連線 ESXi 主機的實體交換器連接埠上尚未啟用動態主幹連線通訊協定 (DTP)。
4. 如果實體交換器連接埠已連線到虛擬交換器 VLAN 主幹連線連接埠，則定期檢查實體交換器連接埠來確保它們已正確設定為主幹連接埠。

使用安全性原則確保標準交換器連接埠安全

標準交換器上的 VMkernel 連接埠群組或虛擬機器連接埠群組具有可設定的安全性原則。安全性原則決定您對虛擬機器強制執行的防模擬和截斷攻擊保護的強度。

與實體網路介面卡一樣，虛擬機器網路介面卡可以模擬另一台虛擬機器。模擬會造成安全性風險。

- 虛擬機器可以傳送可能來自不同電腦的畫面，以便其可以接收針對該電腦的網路畫面。
- 可以對虛擬機器網路介面卡加以設定，從而接收針對其他電腦的畫面。

在為標準交換器新增 VMkernel 連接埠群組或虛擬機器連接埠群組時，ESXi 會為群組中的連接埠設定安全性原則。可以使用此安全性原則確保主機能防止其虛擬機器的客體作業系統模擬網路中的其他電腦。可能會嘗試模擬的客體作業系統偵測不到模擬行為已被阻止。

安全性原則決定您對虛擬機器強制執行的防模擬和截斷攻擊保護的強度。若要正確使用安全性設定檔中的設定，請參閱 *vSphere 網路*文件中的〈安全性原則〉一節。本節說明：

- 虛擬機器網路介面卡如何控制傳輸。
- 此層級的攻擊如何進行。

保護 vSphere Standard Switch 的安全

您可以透過限制一些虛擬機器網路介面卡的 MAC 位址模式，來保護標準交換器流量不受第 2 層的攻擊。

每個虛擬機器網路介面卡均具有一個初始 MAC 位址和一個有效的 MAC 位址。

初始 MAC 位址	建立介面卡時將指派初始 MAC 位址。儘管可以從客體作業系統外部重新設定初始 MAC 位址，但客體作業系統無法變更初始 MAC 位址。
有效 MAC 位址	每個介面卡都具有一個有效 MAC 位址，可篩選出目的地 MAC 位址與有效 MAC 位址不同的傳入網路流量。客體作業系統負責設定有效 MAC 位址，且通常使有效 MAC 位址與初始 MAC 位址相符。

虛擬機器網路介面卡建立後，其有效 MAC 位址與初始 MAC 位址相同。客體作業系統可隨時將有效 MAC 位址更改為其他值。如果作業系統變更了有效 MAC 位址，其網路介面卡將接收傳送到新 MAC 位址的網路流量。

透過網路介面卡傳送封包時，客體作業系統通常會將其介面卡的有效 MAC 位址輸入乙太網路畫面的來源 MAC 位址欄位中。它還會將接收網路介面卡的 MAC 位址輸入目的地 MAC 位址欄位中。僅當封包中的目的地 MAC 位址與其自身有效的 MAC 位址相符時，接收介面卡才接受封包。

作業系統可傳送具有模擬來源 MAC 位址的畫面。因此作業系統可以模擬接收網路授權的網路介面卡，並且對網路中的裝置發起惡意攻擊。

透過在連接埠群組或連接埠上設定安全性原則，防止虛擬流量受到模擬和第 2 層攔截攻擊。

分散式連接埠群組和連接埠上的安全性原則包含下列選項：

- MAC 位址變更 (請參閱 MAC 位址變更)
- 混合模式 (請參閱混合模式作業)

- 偽造的傳輸 (請參閱偽造的傳輸)

您可以透過選取與 vSphere Web Client 中主機相關聯的虛擬交換器，來檢視與變更預設設定。請參閱 *vSphere 網路*說明文件。

MAC 位址變更

虛擬交換器的安全性原則包含一個 **MAC 位址變更**選項。此選項影響虛擬機器接收的流量。

當 **MAC 位址變更**選項設定為**接受**時，ESXi 接受將有效 MAC 位址變更為不同於初始 MAC 位址的其他位址的要求。

當 **MAC 位址變更**選項設定為**拒絕**時，ESXi 不接受將有效 MAC 位址變更為不同於初始 MAC 位址的不同位址的要求。此設定可以防止主機受到 MAC 模擬的威脅。虛擬機器介面卡用於傳送要求的連接埠將已停用，必須在有效 MAC 位址與初始 MAC 位址相符後，虛擬機器介面卡才能再接收框架。客體作業系統無法偵測到 MAC 位址變更要求已被拒絕。

備註 iSCSI 啟動器依賴於能夠從特定類型的儲存區取得 MAC 位址變更。如果將 ESXi iSCSI 與 iSCSI 儲存區搭配使用，請將 **MAC 位址變更**選項設定為**接受**。

有時，您可能確實需要多個介面卡在網路中使用同一 MAC 位址 (例如，在單點傳播模式中使用 Microsoft 網路負載平衡時)。在標準多點傳播模式中使用 Microsoft 網路負載平衡時，介面卡不能共用 MAC 位址。

偽造的傳輸

偽造的傳輸選項會影響從虛擬機器傳輸的流量。

當**偽造的傳輸**選項設定為**接受**時，ESXi 不會比較來源 MAC 位址和有效 MAC 位址。

若要防止 MAC 模擬，請將**偽造的傳輸**選項設定為**拒絕**。因此，主機會將客體作業系統傳輸的來源 MAC 位址與其虛擬機器介面卡的有效 MAC 位址進行比較，以確認是否相符。如果位址不相符，ESXi 主機將捨棄封包。

客體作業系統未偵測到其虛擬機器介面卡無法使用模擬 MAC 位址傳送封包。ESXi 主機會在具有模擬位址的任何封包傳遞之前將其攔截，而客體作業系統可能假設封包已被捨棄。

混合模式作業

混合模式會消除虛擬機器介面卡執行的任何接收篩選，因此客體作業系統將接收在網路上觀察到的所有流量。依預設，虛擬機器介面卡不能在混合模式中運作。

儘管混合模式對於追蹤網路活動很有用，但它是一種不安全的運作模式，因為混合模式中的任何介面卡均可存取封包，即使某些封包僅由特定的網路介面卡接收也是如此。這表示，虛擬機器中的管理員或根使用者可以檢視傳送至其他客體或主機作業系統的流量。

如需針對混合模式設定虛擬機器介面卡的相關資訊，請參閱 *vSphere 網路*說明文件。

備註 有時，您可能確實需要將標準虛擬交換器或分散式虛擬交換器設定為在混合模式中運作 (例如，執行網路入侵偵測軟體或封包嗅探器時)。

標準交換器保護和 VLAN

VMware 標準交換器可提供保護，以抵禦對 VLAN 安全性的特定威脅。標準交換器的設計方式可保護 VLAN 免受多種攻擊，其中包含 VLAN 跳躍。

具備此保護功能並不保證您的虛擬機器組態不容易遭受其他類型的攻擊。例如，標準交換器不會保護實體網路免受這些攻擊；標準交換器僅可保護虛擬網路。

標準交換器和 VLAN 可抵禦以下類型的攻擊。

MAC 洪水

透過含有標記為來自多個不同來源之 MAC 位址的封包以洪水攻擊交換器。許多交換器使用關聯記憶體資料表來瞭解和儲存每個封包的來源位址。當資料表已滿時，交換器就會進入完全開放狀態，其中的每個傳入封包便會在所有連接埠上廣播，讓攻擊者看見交換器的所有流量。此狀態可能會導致 VLAN 間的封包洩漏。

雖然 VMware 標準交換器會儲存 MAC 位址資料表，但是標準交換器不會從可觀察到的流量中取得 MAC 位址，而且不容易遭受此類型的攻擊。

802.1q 和 ISL 標記攻擊

透過讓交換器充當主幹並將流量廣播至其他 VLAN，以強制交換器將框架從某個 VLAN 重新導向至另一個 VLAN。

VMware 標準交換器不會執行此攻擊類型所需的動態主幹連線，因此不容易遭受此類攻擊。

雙重封裝攻擊

當攻擊者建立雙重封裝封包時發生，此類封包中內部標籤的 VLAN 識別碼與外部標籤的 VLAN 識別碼不同。為了回溯相容，原生 VLAN 會從已傳輸的封包去除外部標籤，除非另以其他方式設定。當原生 VLAN 交換器去除外部標籤時僅會剩下內部標籤，這個內部標籤會將封包路由至與在目前遺失的外部標籤中所識別到的不同 VLAN。

VMware 標準交換器會在針對特定 VLAN 設定的連接埠上，置放虛擬機器嘗試傳送的任何雙重封裝框架。因此，VMware 標準交換器不容易遭受此類型的攻擊。

多點傳送暴力密碼破解攻擊

與幾乎同時傳送大量多點傳送框架至已知的 VLAN 有關，這會使交換器超載，如此一來交換器便會錯誤地允許部分框架廣播至其他 VLAN。

VMware 標準交換器不允許框架離開其正確的廣播網域 (VLAN)，因此不容易遭受此類型的攻擊。

跨距樹狀目錄攻擊

以跨距樹狀目錄通訊協定 (STP) 為攻擊目標，此通訊協定通常用來控制 LAN 各部分間的橋接。攻擊者會傳送嘗試變更網路拓撲的橋接通訊協定資料單位 (BPDU) 封包，以將其自行建立為根橋接。建立為根橋接後，攻擊者便可窺探已傳輸框架的內容。

VMware 標準交換器不支援 STP，因此不容易遭受此類型的攻擊。

隨機框架攻擊

與傳送大量封包有關，封包中的來源和目的地位址保持不變，但欄位的長度、類型或內容卻隨機遭到變更。此攻擊的目標是強制交換器錯誤地將封包路由至不同的 VLAN。

VMware 標準交換器不容易遭受此類型的攻擊。

由於新的安全威脅會隨著時間不斷進化，因此請勿認為此表已詳盡列出所有攻擊。請定期檢查 Web 上的 VMware 安全性資源，以瞭解安全性、最新安全性警示，以及 VMware 安全性策略的相關資訊。

保護 vSphere Distributed Switch 和分散式連接埠群組安全

管理員可選擇多種方式來保護其 vSphere 環境中的 vSphere Distributed Switch 安全。

程序

1 對於具有靜態繫結的分散式連接埠群組，停用自動展開功能。

在 vSphere 5.1 及更新版本中，自動展開功能預設為啟用。

若要停用自動展開，請使用 vSphere Web Services SDK 或命令列介面，設定分散式連接埠群組下的 `autoExpand` 內容。請參閱《*vSphere Web Services SDK*》說明文件。

2 請確保已完整記錄所有 vSphere Distributed Switch 的全部私人 VLAN 識別碼。

3 如果您在 dvPortgroup 上使用 VLAN 標記，則 VLAN 識別碼必須對應於外部 VLAN 感知上游交換器上的識別碼。如果未正確地追蹤 VLAN 識別碼，錯誤地重複使用識別碼可能會允許非預期的流量。同樣地，錯誤或遺失的 VLAN 識別碼可能會讓流量不流經實體和虛擬機器。

4 請確保與 vSphere Distributed Switch 關聯的虛擬連接埠群組上不存在任何未使用的連接埠。

5 標記所有 vSphere Distributed Switch。

與 ESXi 主機相關聯的 vSphere Distributed Switch 需要交換器名稱所對應的文字方塊。此標籤用作交換器的功能性描述元，如同與實體交換器相關聯的主機名稱。vSphere Distributed Switch 上的標籤指示交換器的功能或 IP 子網路。例如，您可以將交換器標示為內部以指示其僅適用於虛擬機器之私人虛擬交換器上的內部網路。沒有任何流量通過實體網路介面卡。

6 如果未使用網路健全狀況檢查，請針對 vSphere Distributed Switch 將其停用。

依預設已停用網路健全狀況檢查。啟用後，健全狀況檢查封包將包含攻擊者可能會使用之主機、交換器及連接埠的相關資訊。僅將網路健全狀況檢查用於疑難排解，並在疑難排解完成後將其關閉。

7 透過在連接埠群組或連接埠上設定安全性原則，防止虛擬流量受到模擬和第 2 層攔截攻擊。

分散式連接埠群組和連接埠上的安全性原則包含下列選項：

- MAC 位址變更 (請參閱 MAC 位址變更)

- 混合模式 (請參閱混合模式作業)
- 偽造的傳輸 (請參閱偽造的傳輸)

透過從分散式交換器的右鍵功能表中選取**管理分散式連接埠群組**，然後在精靈中選取**安全性**，可以檢視和變更目前設定。請參閱 *vSphere 網路*說明文件。

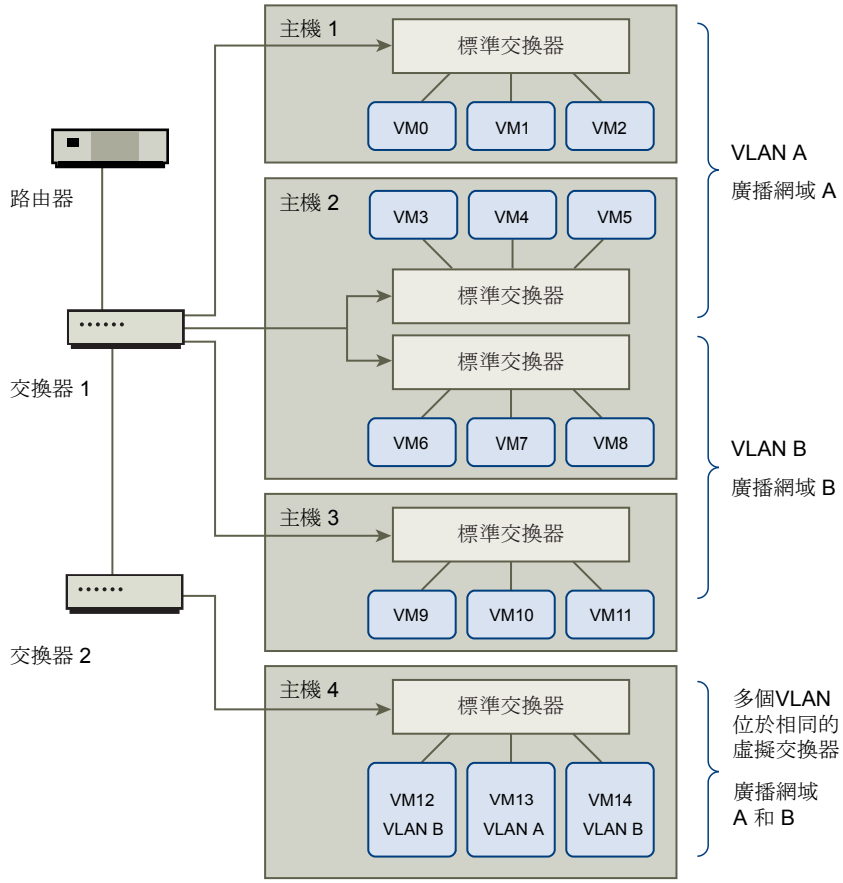
透過 VLAN 保護虛擬機器的安全

網路可能是任何系統中最薄弱的環節之一。虛擬機器網路需要的保護絲毫不少於實體網路。使用 VLAN 可以提高您環境的網路安全性。

VLAN 是一套 IEEE 標準網路配置組合，可透過特定的標記方式將封包的路由限制在 VLAN 中的連接埠內。正確設定後，VLAN 可提供保護一組虛擬機器免遭意外或惡意入侵的可靠方法。

VLAN 可讓您將實體網路分段，讓網路中的兩個虛擬機器無法相互傳輸封包，除非它們屬於相同 VLAN。例如，會計記錄和交易是一家公司最敏感的內部資訊。如果公司的銷售、貨運和會計員工均使用同一實體網路中的虛擬機器，則可透過設定 VLAN 來保護會計部門的虛擬機器。

圖 10-1 VLAN 配置範例



在此組態中，會計部門的所有員工均使用 VLAN A 中的虛擬機器，銷售部門的員工使用 VLAN B 中的虛擬機器。

路由器將包含會計資料的封包轉送到交換器。這些封包將被標記為僅散佈到 VLAN A。因此，資料將被限制在廣播網域 A 內，無法路由到廣播網域 B，除非對路由器如此設定。

此 VLAN 組態可防止銷售人員攔截要傳送到會計部門的封包。還能防止會計部門接收要傳送到銷售小組的封包。單個虛擬交換器可為不同 VLAN 中的虛擬機器服務。

VLAN 安全考量

如何設定 VLAN 來保護網路各部分的安全取決於很多因素，如客體作業系統以及網路設備的設定方式。

ESXi 配備了符合 IEEE 802.1q 標準的完整 VLAN 實作。VMware 不能對如何設定 VLAN 提出具體建議，但當您使用 VLAN 部署做為安全性強制執行原則一部分時，應考量一些因素。

安全 VLAN

管理員可使用數種選項，確保其 vSphere 環境中 VLAN 的安全。

程序

1 請確保連接埠群組未設定為由上游實體交換器保留的 VLAN 值

請勿將 VLAN 識別碼設定為保留供實體交換器使用的值。

2 請確保連接埠群組未設定為 VLAN 4095，除非您正在使用虛擬客體標記 (VGT)。

vSphere 中存在三種 VLAN 標記類型：

- 外部交換器標記 (EST)
- 虛擬交換器標記 (VST) - 虛擬交換器使用已設定的 VLAN 識別碼來標記傳入附加虛擬機器的流量，並移除從虛擬機器傳出的流量的標籤。若要設定 VST 模式，請指派 1 到 4095 之間的 VLAN 識別碼。
- 虛擬客體標記 (VGT) - 虛擬機器處理 VLAN 流量。若要啟動 VGT 模式，請將 VLAN 識別碼設定為 4095。在分散式交換器上，您還可以透過使用 **VLAN 主幹連線**選項，允許以 VLAN 為基礎的虛擬機器流量。

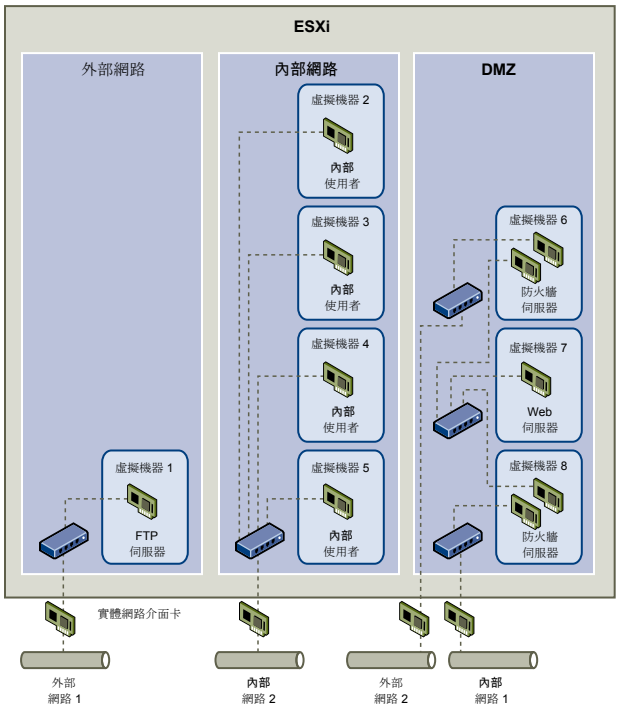
在標準交換器上，您可以在交換器或連接埠群組層級上設定 VLAN 網路模式，而在分散式交換器上，您可以在分散式連接埠群組或連接埠層級上設定。

3 請確保已完全記錄了每台虛擬交換器上的所有 VLAN，而且每台虛擬交換器有且僅有所需的 VLAN。

在單一 ESXi 主機內建立多個網路

ESXi 系統的設計可讓您將某些虛擬機器群組連線到內部網路，將其他虛擬機器群組連線到外部網路，並將其他虛擬機器群組同時連線到外部和內部網路，而這一切都在同一主機上進行。此功能是由對虛擬機器的基本隔離和對虛擬網路連線功能的有計劃使用組合而成的。

圖 10-2 單一 ESXi 主機上設定的外部網路、內部網路和 DMZ



在圖中，系統管理員已將主機設定到三個不同的虛擬機器區域：FTP 伺服器、內部虛擬機器和 DMZ。每個區域均提供唯一功能。

FTP 伺服器

虛擬機器 1 設定了 FTP 軟體，可用作從外部資源 (例如，由廠商當地語系化的表單和輔助材料) 傳出及向其傳送之資料的儲存區域。

此虛擬機器僅與外部網路相關聯。它自身擁有可用來與外部網路 1 連線的虛擬交換器和實體網路介面卡。此網路專用於公司在從外部來源接收資料時所使用的伺服器。例如，公司使用外部網路 1 從廠商接收 FTP 流量，並允許廠商透過 FTP 存取儲存在外部可用伺服器上的資料。除了用於虛擬機器 1 之外，外部網路 1 也用於在整個網站內不同 ESXi 主機上設定的 FTP 伺服器。

由於虛擬機器 1 不與主機上的任何虛擬機器共用虛擬交換器或實體網路介面卡，因此，其他駐留的虛擬機器無法透過虛擬機器 1 網路傳送和接收封包。此限制可防止嗅探攻擊 (嗅探攻擊需向受害者傳送網路流量)。更為重要的是，攻擊者再也無法使用 FTP 固有的漏洞來存取主機的任何其他虛擬機器。

內部虛擬機器

虛擬機器 2 到 5 保留供內部使用。這些虛擬機器用來處理和儲存公司機密資料 (例如，醫療記錄、法律裁決和欺詐調查)。因此，系統管理員必須確保為這些虛擬機器提供最高層級的保護。

這些虛擬機器透過其自身的虛擬交換器和網路介面卡，連線到內部網路 2。內部網路 2 保留供內部人員 (例如，索賠專員、內部律師或調解員) 使用。

虛擬機器 2 到 5 可透過虛擬交換器與另一個虛擬機器通訊，也可透過實體網路介面卡與內部網路 2 上其他位置的內部虛擬機器通訊。它們不能與對外電腦進行通訊。如同 FTP 伺服器一樣，這些虛擬機器不能透過其他虛擬機器網路傳送和接收封包。同樣，主機的其他虛擬機器不能透過虛擬機器 2 到 5 傳送和接收封包。

DMZ

虛擬機器 6 到 8 設定為可供營銷群組用於發佈公司外部網站的 DMZ。

此虛擬機器群組與外部網路 2 和內部網路 1 關聯。公司使用外部網路 2 來支援營銷部門和財務部門用來主控公司網站的 Web 伺服器及公司為外部使用者主控的其他 Web 設施。內部網路 1 是營銷部門用於向公司網站發佈內容、張貼下載內容及維護服務 (例如，使用者論壇) 的媒介。

由於這些網路與外部網路 1 和內部網路 2 隔離，因此虛擬機器無任何共用連絡點 (交換器或介面卡)，FTP 伺服器或內部虛擬機器群組也不存在任何攻擊風險。

透過利用虛擬機器隔離、正確設定虛擬交換器及維護網路分離，系統管理員可在同一 ESXi 主機上儲存所有三個虛擬機器區域，並完全不用擔心資料或資源流失。

公司使用多個內部和外部網路，並確保每個群組的虛擬交換器和實體網路介面卡與其他群組的虛擬交換器和實體網路介面卡完全分離，從而在虛擬機器群組中強制實作隔離。

由於沒有任何虛擬交換器橫跨虛擬機器區域，因此系統管理員可成功地消除虛擬機器區域之間的封包洩漏風險。虛擬機本身無法向另一個虛擬交換器直接洩漏封包。僅在以下情況下，封包才會在虛擬交換器之間移動：

- 這些虛擬交換器連線到同一實體 LAN。
- 這些虛擬交換器連線到可用於傳輸封包的一般虛擬機器。

這些條件均未出現在樣本組態中。如果系統管理員要確認不存在一般虛擬交換器路徑，可透過在 vSphere Web Client 中檢閱網路交換器配置，以檢查是否可能存在共用連絡點。

為了保護虛擬機器的資源，系統管理員為每台虛擬機器設定了資源保留區和限制，從而降低了 DoS 和 DDoS 攻擊的風險。系統管理員透過在 DMZ 的前後端安裝軟體防火牆，確保主機受到實體防火牆的保護，並設定了連線到網路的儲存資源以使每個資源均有自己的虛擬交換器，從而為 ESXi 主機和虛擬機器提供了進一步保護。

網際網路通訊協定安全性

網際網路通訊協定安全性 (IPsec) 可確保進出主機的 IP 通訊安全性。ESXi 主機支援使用 IPv6 的 IPsec。

在主機上設定 IPsec 時，可對傳入和傳出封包啟用驗證和加密。對 IP 流量進行加密的時間和方式，取決於如何設定系統的安全性關聯和安全性原則。

安全性關聯可判定系統對流量進行加密的方式。在建立安全性關聯時，可指定安全性關聯的來源和目的地、加密參數以及名稱。

安全性原則可判定系統應對流量進行加密的時間。安全性原則包含來源和目的地資訊、要加密之流量的通訊協定和方向、模式 (transport 或 tunnel) 以及要使用的安全性關聯。

列出可用的安全性關聯

ESXi 可提供可供安全性原則使用的所有安全性關聯的清單。該清單包含使用者建立的安全性關聯，以及 VMkernel 使用網際網路金鑰交換安裝的任何安全性關聯。

可以使用 `esxcli` vSphere CLI 命令取得可用安全性關聯的清單。

程序

- 在命令提示字元處，輸入命令 **`esxcli network ip ipsec sa list`**。

ESXi 將顯示所有可用安全性關聯的清單。

新增 IPsec 安全性關聯

新增安全性關聯來指定關聯 IP 流量的加密參數。

可以使用 `esxcli` vSphere CLI 命令新增安全性關聯。

程序

- 在命令提示字元下，使用下面一或多個選項輸入命令 **`esxcli network ip ipsec sa add`**。

選項	說明
`--sa-source=` ***來源位址***	必要。指定來源位址。
`--sa-destination=` ***目的地位址***	必要。指定目的地位址。
`--sa-mode=` ***模式***	必要。指定模式 `transport` 或 `tunnel`。
`--sa-spi=` ***安全性參數索引***	必要。指定安全性參數索引。安全性參數索引識別主機的安全性關聯。它必須是一個首碼為 0x 的十六進位值。所建立的每個安全性關聯都必須具有通訊協定和安全性參數索引的唯一組合。
`--encryption-algorithm=` ***加密演算法***	必要。使用以下其中一個參數指定加密演算法。 ■ `3des-cbc` ■ `aes128-cbc` ■ `null` (表示不提供任何加密)
`--encryption-key=` ***加密金鑰***	在指定加密演算法時為必要項。指定加密金鑰。可以使用 0x 首碼輸入 ASCII 文字或十六進位形式的金鑰。
`--integrity-algorithm=` ***驗證演算法***	必要。指定驗證演算法 `hmac-sha1` 或 `hmac-sha2-256`。
`--integrity-key=` ***驗證金鑰***	必要。指定驗證金鑰。可以使用 0x 首碼輸入 ASCII 文字或十六進位形式的金鑰。
`--sa-name=` ***名稱***	必要。提供安全性關聯名稱。

範例 10-1. 新安全性關聯命令

為方便讀取，下面的範例包含額外的換行符。

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
```

```
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x697076367265616479 6c6f676f33646573636362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x69707636726561647 96c6f67736861316f757432
--sa-name sa1
```

移除 IPsec 安全性關聯

您可以使用 ESXCLI vSphere CLI 命令移除安全性關聯。

先決條件

確認要使用的安全性關聯目前未在使用。如果嘗試移除正在使用的安全性關聯，則移除作業將失敗。

程序

- 在命令提示字元下，輸入命令
  esxcli network ip ipsec sa remove --sa-name *security_association_name*

列出可用的 IPsec 安全性原則

您可以使用 ESXCLI vSphere CLI 命令列出可用的安全性原則。

程序

- 在命令提示字元下，輸入命令 **esxcli network ip ipsec sp list**

主機將顯示所有可用安全性原則的清單。

建立 IPSec 安全性原則

建立安全性原則，可以判定何時使用在安全性關聯中設定的驗證和加密參數。您可以使用 ESXCLI vSphere CLI 命令新增安全性原則。

先決條件

在建立安全性原則之前，可按新增 IPsec 安全性關聯中所述，新增具有適當的驗證和加密參數的安全性關聯。

程序

- 在命令提示字元下輸入命令 **esxcli network ip ipsec sp add** ，並使用下列一或多個選項。

選項	說明
--sp-source= ***來源位址***	必要。指定來源 IP 位址和首碼長度。
--sp-destination= ***目的地位址***	必要。指定目的地位址和首碼長度。
--source-port= ***連接埠***	必要。指定來源連接埠。來源連接埠必須是介於 0 和 65535 之間的一個數字。
--destination-port= ***連接埠***	必要。指定目的地連接埠。來源連接埠必須是介於 0 和 65535 之間的一個數字。

選項	說明
--upper-layer-protocol= ***通訊協定***	使用下列參數之一指定上層通訊協定。 ■ tcp ■ udp ■ icmp6 ■ 任何
--flow-direction= ***方向***	使用 in 或 out 指定要監控流量的方向。
--action= ***動作***	使用下列參數之一指定在出現具有指定參數的流量時要採取的動作。 ■ none:不採取任何動作 ■ discard:不允許資料進出。 ■ ipsec:使用安全性關聯中提供的驗證和加密資訊來判定資料是否來自受信任的來源。
--sp-mode= ***模式***	指定模式 tunnel 或 transport。
--sa-name= ***安全性關聯名稱***	必要。為要使用的安全性原則提供安全性關聯名稱。
--sp-name= ***名稱***	必要。請為安全性原則提供名稱。

範例 10-2. 新安全性原則命令

為了方便閱讀，下列範例包含額外的分行符號。

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sa1
--sp-name=sp1
```

移除 IPsec 安全性原則

您可以使用 ESXCLI vSphere CLI 命令從 ESXi 主機移除安全性原則。

先決條件

確認要使用的安全性原則目前未在使用。如果嘗試移除正在使用的安全性原則，則移除作業將失敗。

程序

- 在命令提示字元下，輸入命令 **esxcli network ip ipsec sp remove --sa-name** ***security policy name***。

  若要移除所有安全性原則，請輸入命令 **esxcli network ip ipsec sp remove --remove-all**。

確保 SNMP 組態正確

如果未正確設定 SNMP，則監控資訊可能會被傳送到惡意主機。然後，惡意主機可能會使用此資訊計劃實施攻擊。

必須在每台 ESXi 主機上設定 SNMP。可以使用 vCLI、PowerCLI 或 vSphere Web Services SDK 進行設定。

如需 SNMP 3 的詳細設定資訊，請參閱*《監控與效能》*出版物。

程序

1 執行下列命令來判定目前是否正在使用 SNMP。

```
esxcli system snmp get
```

2 若要啟用 SNMP，請執行以下命令：

```
esxcli system snmp set --enable true
```

3 若要停用 SNMP，請執行以下命令：

```
esxcli system snmp set --disable true
```

vSphere 網路安全性最佳做法

遵循網路安全性最佳做法可協助確保 vSphere 部署的完整性。

一般網路安全性建議

遵循一般網路安全建議是保護網路環境安全的第一步。然後，您可以轉至特別區域，例如使用防火牆保護網路或使用 IPsec。

- 如果啟用跨距樹狀目錄，請確保實體交換器連接埠已設定 Portfast。由於 VMware 虛擬交換器不支援 STP，所以連線到 ESXi 主機的實體交換器連接埠必須已設定 Portfast，才能避免在實體交換器網路內迴圈。如果未設定 Portfast，則可能會出現效能和連線問題。
- 確保分散式虛擬交換器的 Netflow 流量僅傳送到授權的收集器 IP 位址。Netflow 匯出未加密且可能包含有關虛擬網路的資訊。此資訊會增加攔截式攻擊成功的可能性。如果需要 Netflow 匯出，請確認所有 Netflow 目標 IP 位址均正確無誤。
- 確保僅授權的管理員可以透過使用角色型存取控制來存取虛擬網路元件。例如，為虛擬機器管理員指定僅存取其虛擬機器所在連接埠群組的權限。為網路管理員指定存取所有虛擬網路元件的權限，但沒有虛擬機器的存取權。有限存取可降低錯誤組態 (無論是意外還是惡意) 的風險，並增強職責分離與最少權限的重要安全性概念。
- 請確保連接埠群組未設定為原生 VLAN 的值。實體交換器將 VLAN 1 用作其原生 VLAN。原生 VLAN 上的框架未加上標籤 1。ESXi 沒有原生 VLAN。在連接埠群組中指定含 VLAN 的框架有標籤，但未在連接埠群組中指定含 VLAN 的框架不會加上標籤。這可能會產生問題，因為具有標籤 1 的虛擬機器最終會屬於實體交換器的原生 VLAN。

例如，Cisco 實體交換器之 VLAN 1 的框架會取消標籤，因為 VLAN1 是該實體交換器的原生 VLAN。但是，ESXi 主機中指定為 VLAN 1 的框架會加上標籤 1。因此，傳送到原生 VLAN 的 ESXi 主機流量無法正確路由，因為該原生 VLAN 帶有標籤 1，而沒有取消標籤。來自原生 VLAN 的實體交換器流量不可見，因為原生 VLAN 未加上標籤。如果 ESXi 虛擬交換器連接埠群組使用原生 VLAN 識別碼，則來自該連接埠上的虛擬機器的流量對交換器上的原生 VLAN 不可見，因為交換器預期的是取消標籤的流量。

- 請確保連接埠群組未設定為由上游實體交換器保留的 VLAN 值。實體交換器保留某些 VLAN 識別碼用於內部用途，且通常禁止設定為這些值的流量。例如，Cisco Catalyst 交換器通常保留 VLAN 1001–1024 和 4094。使用保留的 VLAN 可能會導致網路上的拒絕服務。
- 請確保連接埠群組未設定為 VLAN 4095，虛擬客體標記 (VGT) 除外。將連接埠群組設定為 VLAN 4095 可啟動 VGT 模式。在此模式下，虛擬交換器會將所有網路框架傳遞到虛擬機器，不需要修改 VLAN 標籤，直接留給虛擬機器處理。
- 在分散式虛擬交換器上限制連接埠層級組態覆寫。連接埠層級組態覆寫預設為停用。啟用覆寫時，您可以使用除連接埠群組層級設定以外的其他虛擬機器安全性設定。某些虛擬機器需要唯一組態，但監控不可或缺。如果不監控覆寫，則可存取含危險分散式虛擬交換器組態之虛擬機器的任何人都可以嘗試利用該存取權。
- 確保分散式虛擬交換器連接埠鏡像流量僅傳送到授權的收集器連接埠或 VLAN。vSphere Distributed Switch 可以將流量從一個連接埠鏡像到另一個連接埠，以允許封包擷取裝置收集特定流量。連接埠鏡像以未加密格式傳送所有指定流量的複本。此鏡像流量包含擷取封包中的完整資料，如果方向錯誤，可能會完全損壞這些資料。如果需要連接埠鏡像，請確認所有連接埠鏡像目的地 VLAN、連接埠和上行識別碼皆正確無誤。

標記網路元件

識別網路架構的不同元件至關重要，有助於確保不會隨著網路不斷增長而引進任何錯誤。

遵循這些最佳做法：

- 確保連接埠群組設定有明確的網路標籤。這些標籤用作連接埠群組的功能性描述元，隨著網路變得日益複雜，協助您識別每個連接埠群組的功能。
- 確保每個 vSphere Distributed Switch 具有明確的網路標籤來指示交換器的功能或 IP 子網路。此標籤用作交換器的功能性描述元，如同實體交換器需要主機名稱。例如，您可以將交換器標示為「內部」以表明其用於內部網路。不可以變更標準虛擬交換器的標籤。

記錄及檢查 vSphere VLAN 環境

請定期檢查您的 VLAN 環境以避免問題發生。完整記錄 VLAN 環境，並確保 VLAN 識別碼僅使用一次。您的說明文件可協助進行疑難排解，且在您想要擴充環境時至關重要。

程序

1 請確保所有 vSwitch 和 VLANS 識別碼均已完整記錄

如果您在虛擬交換器上使用 VLAN 標記，則識別碼必須對應於外部 VLAN 感知上游交換器上的識別碼。如果未完整追蹤 VLAN 識別碼，錯誤地重複使用識別碼可能會允許錯誤的實體和虛擬機器之間的流量。同樣地，如果 VLAN 識別碼錯誤或遺失，則您想要流量通過的實體機器和虛擬機器之間的流量可能會遭到封鎖。

2 請確保已完整記錄用於所有分散式虛擬連接埠群組 (dvPortgroup 執行個體) 的 VLAN 識別碼。

如果您在 dvPortgroup 上使用 VLAN 標記，則識別碼必須對應於外部 VLAN 感知上游交換器上的識別碼。如果未完整追蹤 VLAN 識別碼，錯誤地重複使用識別碼可能會允許錯誤的實體和虛擬機器之間的流量。同樣地，如果 VLAN 識別碼錯誤或遺失，則您想要流量通過的實體機器和虛擬機器之間的流量可能會遭到封鎖。

3 請確保已完整記錄所有分散式虛擬交換器的私人 VLAN 識別碼。

分散式虛擬交換器的私人 VLAN (PVLAN) 需要主要和次要 VLAN 識別碼。這些識別碼對應於外部 PVLAN 感知上游交換器上的識別碼。如果未完整追蹤 VLAN 識別碼，錯誤地重複使用識別碼可能會允許錯誤的實體和虛擬機器之間的流量。同樣地，如果 PVLAN 識別碼錯誤或遺失，則您想要流量通過的實體機器和虛擬機器之間的流量可能會遭到封鎖。

4 確認 VLAN 主幹連結僅連線到當成主幹連結運作的實體交換器連接埠。

將虛擬交換器連線到 VLAN 主幹連接埠時，您必須在上行連接埠同時正確設定該虛擬交換器和實體交換器。如未正確設定實體交換器，則含 VLAN 802.1q 標頭的框架會轉送到不正確的交換器。

採用網路隔離做法

網路隔離做法可以大幅提高 vSphere 環境的網路安全性。

隔離管理網路

vSphere 管理網路提供在每個元件上存取 vSphere 管理介面的權限。在管理介面上執行的服務為攻擊者提供了獲取系統存取權限的機會。遠端攻擊可能會首先獲取此網路的存取權限。如果攻擊者獲得了管理網路的存取權限，它會提供暫存區域以進一步入侵。

以在 ESXi 主機或叢集上執行的最安全的虛擬機器安全性層級來保護管理網路，從而嚴格控制管理網路的存取權。無論管理網路的受限程度為何，管理員都必須具有此網路的存取權才能設定 ESXi 主機和 vCenter Server 系統。

將 vSphere 管理連接埠群組置於常用標準交換器上的專用 VLAN 中。如果生產虛擬機器未使用 vSphere 管理連接埠群組的 VLAN，生產 (虛擬機器) 流量可以共用標準交換器。

檢查網路區段是否未進行路由，路由至包含其他管理相關項目的網路除外。路由網路區段可能對 vSphere Replication 有意義。尤其確保生產虛擬機器流量無法路由到此網路。

使用下列其中一種方法，嚴格控制管理功能的存取權。

- 對於特別機密的環境，設定受控閘道或其他受控方法來存取管理網路。例如，需要管理員透過 VPN 連線至管理網路。僅允許受信任的管理員存取管理網路。

- 設定用於執行管理用戶端的跳躍方塊。

隔離儲存區流量

確保以 IP 為基礎的儲存區流量已隔離。以 IP 為基礎的儲存區包括 iSCSI 和 NFS。虛擬機器可能會與以 IP 為基礎的儲存區組態共用虛擬交換器和 VLAN。此類型的組態可能會向未經授權的虛擬機器使用者公開以 IP 為基礎的儲存區流量。

以 IP 為基礎的儲存區通常不會加密。任何對此網路具有存取權的人員都可以檢視以 IP 為基礎的儲存區流量。若要限制未經授權的使用者檢視以 IP 為基礎的儲存區流量，請以邏輯方式將以 IP 為基礎的儲存區網路流量與生產流量相區隔。從 VMkernel 管理網路的獨立 VLAN 或網路區段上設定以 IP 為基礎的儲存裝置介面卡，以限制未經授權的使用者檢視流量。

隔離 vMotion 流量

vMotion 移轉資訊以純文字格式進行傳輸。任何對此資訊流經的網路具有存取權的人員都可以進行檢視。潛在攻擊者可能會攔截 vMotion 流量以取得虛擬機器的記憶體內容。他們還可能會暫存移轉期間修改內容的 MiTM 攻擊。

在隔離網路上，將 vMotion 流量與生產流量相區隔。將網路設定為不可路由，即確保第 3 層路由器不會跨越此網路和其他網路，從而阻止從外部存取網路。

將常用標準交換器上的專用 VLAN 用於 vMotion 連接埠群組。如果生產虛擬機器不使用 vMotion 連接埠群組的 VLAN，則生產 (虛擬機器) 流量可以使用相同的標準交換器。

僅在需要時透過 vSphere Network Appliance API 使用虛擬交換器

不要將主機設定為傳送網路資訊到虛擬機器，除非您正在使用使用了 vSphere Network Appliance API (DvFilter) 的產品。如果 vSphere Network Appliance API 處於啟用狀態，則攻擊者可能會嘗試將虛擬機器連線到篩選器。此連線可能會導致存取主機上的其他虛擬機器網路。

如果您正在使用使用了此 API 的產品，請確認是否已正確設定主機。請參閱《開發和部署 vSphere 解決方案、vService 和 ESX 代理程式》中有關 DvFilter 的章節。如果您的主機設定為使用 API，請確保 `Net.DVFilterBindIpAddress` 參數的值與使用 API 的產品相符。

程序

1. 登入 vSphere Web Client。
2. 選取主機，然後按一下**設定**。
3. 在 [系統] 下，選取**進階系統設定**。
4. 向下捲動到 `Net.DVFilterBindIpAddress`，並確認該參數的值是否為空。

   參數的順序不是嚴格按字母順序排列的。在 [篩選器] 文字方塊中輸入 **`DVFilter`**，以顯示所有相關的參數。
5. 確認設定。
   - 如果未使用 DvFilter 設定，請確保值為空。

- 如果您使用 DvFilter 設定，請確定參數的值正確無誤。該值必須符合使用 DvFilter 之產品所使用的值。

有關多個 vSphere 元件的最佳做法

11

部分安全性最佳做法 (例如在環境中設定 NTP) 會影響多個 vSphere 元件。設定環境時請考慮這些建議。

如需相關資訊，請參閱第 3 章保護 ESXi 主機和第 5 章確保虛擬機器安全。

本章節討論下列主題:

- 同步 vSphere 網路上的時鐘
- 儲存區安全性最佳做法
- 確認已停用向客體傳送主機效能資料
- 設定 ESXi Shell 和 vSphere Web Client 的逾時

同步 vSphere 網路上的時鐘

確認 vSphere 網路上所有元件的時鐘均已同步。如果 vSphere 網路中機器的時鐘未同步，則在網路機器之間進行通訊時，無法將對時間敏感的 SSL 憑證 辨識為有效。

未同步的時鐘可能會導致驗證問題，從而使安裝失敗或使 vCenter Server Appliance vpxd 服務無法啟動。

請確認 vCenter Server 執行所在的任何 Windows 主機電腦與網路時間伺服器 (NTP) 伺服器同步。請參閱知識庫文章，網址為 http://kb.vmware.com/kb/1318。

若要將 ESXi 時鐘與 NTP 伺服器同步，您可以使用 VMware Host Client。如需編輯 ESXi 主機時間組態的相關資訊，請參閱《*vSphere 單一主機管理*》。

- 使 ESXi 時鐘與網路時間伺服器同步

  安裝 vCenter Server 或部署 vCenter Server Appliance 之前，請確保 vSphere 網路上所有機器的時鐘均已同步。

- 在 vCenter Server Appliance 中設定時間同步化設定

  您可在部署後變更 vCenter Server Appliance 中的時間同步化設定。

使 ESXi 時鐘與網路時間伺服器同步

安裝 vCenter Server 或部署 vCenter Server Appliance 之前，請確保 vSphere 網路上所有機器的時鐘均已同步。

此工作說明如何從 VMware Host Client 設定 NTP。您可改為使用 `vicfg-ntp` vCLI 命令。請參閱 *vSphere Command-Line Interface 參考*。

程序

1 啟動 VMware Host Client，然後連線至 ESXi 主機。

2 按一下**設定**。

3 在**系統**下，按一下**時間組態**，然後按一下**編輯**。

4 選取**使用網路時間通訊協定 (啟用 NTP 用戶端)**。

5 在 [新增 NTP 伺服器] 文字方塊中，輸入要與之同步的一或多部 NTP 伺服器的 IP 位址或完整網域名稱。

6 (選擇性) 設定啟動原則和服務狀態。

7 按一下**確定**。

主機即會與 NTP 伺服器同步。

在 vCenter Server Appliance 中設定時間同步化設定

您可在部署後變更 vCenter Server Appliance 中的時間同步化設定。

部署 vCenter Server Appliance 時，可使用 NTP 伺服器或 VMware Tools 選擇時間同步化方法。如果 vSphere 網路中的時間設定發生變更，您可以使用應用裝置 shell 中的命令編輯 vCenter Server Appliance 和設定時間同步化設定。

啟用定期時間同步化時，VMware Tools 會將客體作業系統的時間設定為與主機的時間相同。

執行時間同步化之後，VMware Tools 會每分鐘檢查一次，判定客體作業系統與主機上的時鐘是否仍然相符。如果不相符，則將同步客體作業系統上的時鐘以符合主機上的時鐘。

本機時間同步化軟體 (例如網路時間通訊協定 (NTP)) 通常比 VMware Tools 定期時間同步化更精確，因此更常使用。vCenter Server Appliance 中只能使用一種形式的定期時間同步化。如果您決定使用本機時間同步化軟體，vCenter Server Appliance VMware Tools 定期時間同步化會停用，反之亦然。

使用 VMware Tools 時間同步化

您可以將 vCenter Server Appliance 設定為使用 VMware Tools 時間同步化。

程序

1 存取應用裝置 shell 並以具有管理員或超級管理員角色的使用者身分登入。

具有超級管理員角色的預設使用者是根使用者。

2 執行下列命令以啟用 VMware Tools 時間同步化。

```
timesync.set --mode host
```

3 (選擇性) 執行下列命令以確認已成功套用 VMware Tools 時間同步化。

```
timesync.get
```

該命令傳回時間同步化處於主機模式。

應用裝置的時間已與 ESXi 主機的時間同步。

在 vCenter Server Appliance 組態中新增或取代 NTP 伺服器

若要設定 vCenter Server Appliance 以使用以 NTP 為基礎的時間同步化，您必須將 NTP 伺服器新增至 vCenter Server Appliance 組態。

程序

1 存取應用裝置 shell 並以具有管理員或超級管理員角色的使用者身分登入。

具有超級管理員角色的預設使用者是根使用者。

2 執行 `ntp.server.add` 命令，將 NTP 伺服器新增至 vCenter Server Appliance 組態。

例如，執行下列命令：

```
ntp.server.add --servers IP-addresses-or-host-names
```

在此，*IP-addresses-or-host-names* 是 NTP 伺服器的 IP 位址或主機名稱清單 (以逗點分隔)。

此命令可將 NTP 伺服器新增至組態。如果時間同步化以 NTP 伺服器為基礎，則 NTP 精靈會重新啟動以重新載入新的 NTP 伺服器。否則，此命令只會將新的 NTP 伺服器新增至現有 NTP 組態。

3 (選擇性) 若要刪除舊 NTP 伺服器並將新 NTP 伺服器新增至 vCenter Server Appliance 組態，請執行 `ntp.server.set` 命令。

例如，執行下列命令：

```
ntp.server.set --servers IP-addresses-or-host-names
```

在此，*IP-addresses-or-host-names* 是 NTP 伺服器的 IP 位址或主機名稱清單 (以逗點分隔)。

此命令可從組態刪除舊的 NTP 伺服器，並在組態中設定輸入 NTP 伺服器。如果時間同步化以 NTP 伺服器為基礎，則 NTP 精靈會重新啟動以重新載入新的 NTP 組態。否則，此命令只會使用您提供做為輸入的伺服器取代 NTP 組態中的伺服器。

4 (選擇性) 執行下列命令以確認您已成功套用新的 NTP 組態設定。

```
ntp.get
```

命令會傳回設定用於 NTP 同步之伺服器的空格分隔式清單。如果啟用 NTP 同步，則命令會傳回 NTP 組態處於 [啟動] 狀態。如果停用 NTP 同步，則命令會傳回 NTP 組態處於 [關閉] 狀態。

下一個

如果停用 NTP 同步，您可以將 vCenter Server Appliance 中的時間同步化設定設定為以 NTP 伺服器為基礎。請參閱 將 vCenter Server Appliance 與 NTP 伺服器的時間同步。

將 vCenter Server Appliance 與 NTP 伺服器的時間同步

您可以將 vCenter Server Appliance 中的時間同步化設定設定為以 NTP 伺服器為基礎。

先決條件

在 vCenter Server Appliance 組態中設定一或多部網路時間通訊協定 (NTP) 伺服器。請參閱 在 vCenter Server Appliance 組態中新增或取代 NTP 伺服器。

程序

1 存取應用裝置 shell 並以具有管理員或超級管理員角色的使用者身分登入。

具有超級管理員角色的預設使用者是根使用者。

2 執行下列命令以啟用以 NTP 為基礎的時間同步化。

```
timesync.set --mode NTP
```

3 (選擇性) 執行下列命令以確認已成功套用 NTP 同步化。

```
timesync.get
```

該命令傳回時間同步化處於 NTP 模式。

儲存區安全性最佳做法

遵循儲存區安全性提供者概略列出的儲存區安全性最佳做法。您還可以利用 CHAP 與相互 CHAP 來保護 iSCSI 儲存區、遮罩與區域 SAN 資源，並設定 NFS 4.1 的 Kerberos 認證。

另請參閱 *管理 VMware vSAN* 說明文件。

保護 iSCSI 儲存區安全

為主機設定的儲存區可能包括一或多個使用 iSCSI 的儲存區域網路 (SAN)。在主機上設定 iSCSI 時，可採取措施將安全性風險降到最低。

iSCSI 支援使用 TCP/IP 透過網路連接埠 (而非透過直接連線到 SCSI 裝置) 來存取 SCSI 裝置和交換資料。iSCSI 交易將原始 SCSI 資料區塊封裝在 iSCSI 記錄中，並將資料傳輸到要求資料的裝置或使用者。

iSCSI SAN 支援有效利用現有乙太網路基礎結構，為主機提供其可動態共用的儲存資源的存取權限。iSCSI SAN 是適用於依賴一般儲存區集區服務多個使用者之環境的經濟型儲存區解決方案。與任一網路系統一樣，iSCSI SAN 也可能會受到安全性破壞。

備註 用於保護 iSCSI SAN 安全的需求和程序，與和主機相關聯的硬體 iSCSI 介面卡和透過主機直接設定的 iSCSI 的需求和程序相似。

保護 iSCSI 裝置安全

若要保護 iSCSI 裝置，每當主機嘗試存取目標 LUN 上的資料時，都要求 ESXi 主機 (或啟動器) 向 iSCSI 裝置 (或目標) 進行驗證。

驗證可確保啟動器具有存取目標的權限。您可在 iSCSI 裝置上設定驗證時授與此權限。

對於 iSCSI，ESXi 不支援安全遠端通訊協定 (SRP) 或公開金鑰驗證方式。您只能搭配 NFS 4.1 使用 Kerberos。

ESXi 支援 CHAP 和相互 CHAP 驗證。*vSphere 儲存區*說明文件解釋如何選取適用於 iSCSI 裝置的最佳驗證方法，以及如何設定 CHAP。

確保 CHAP 密碼的唯一性。設定每台主機的不同相互驗證密碼。如果可能，請為連線至 ESXi 主機的每個用戶端設定不同的密碼。唯一的密碼可確保即使一個主機受到危害，攻擊者仍無法建立其他任意主機以及向儲存裝置進行驗證。使用共用密碼，一台主機受危害可能會使得攻擊者能夠向儲存裝置進行驗證。

保護 iSCSI SAN

計劃 iSCSI 組態時，應採取一些措施提高 iSCSI SAN 的整體安全性。iSCSI 組態是否安全性取決於 IP 網路，因此在設定網路時，強制執行良好的安全性標準可協助保護 iSCSI 儲存區。

下列是強制執行良好安全性標準的一些具體建議。

保護傳輸的資料

iSCSI SAN 中的一個主要安全性風險便是攻擊者會探查到傳輸的儲存資料。

採取其他措施，使攻擊者無法輕鬆看到 iSCSI 資料。無論是 iSCSI 硬體介面卡還是 ESXi iSCSI 啟動器，均不會對其傳輸到目標的資料和從目標接收的資料進行加密，這會造成資料更容易遭受探查攻擊。

若允許虛擬機器與 iSCSI 組態共用標準交換器和 VLAN，可能造成 iSCSI 流量遭到虛擬機器攻擊者的不當使用。若要協助確保侵入者無法接聽 iSCSI 傳輸，請確保任何虛擬機器都無法查看 iSCSI 儲存區網路。

如果您使用 iSCSI 硬體介面卡，若要達成此目標，您可以確保 iSCSI 介面卡和 ESXi 實體網路介面卡未透過共用交換器或其他某些方式，而不小心在主機外部連線。如果直接透過 ESXi 主機設定 iSCSI，若要達成此目標，您可以不與虛擬機器使用同一標準交換器，而改用不同的標準交換器來設定 iSCSI 儲存區。

除了透過提供專用標準交換器來保護 iSCSI SAN 之外，您還可以在 iSCSI SAN 自己的 VLAN 上進行設定來提高效能和安全性。將 iSCSI 組態置於獨立的 VLAN 上，可確保只有 iSCSI 介面卡能夠看到 iSCSI SAN 內的傳輸。同時，來自其他來源的網路壅塞不會影響 iSCSI 流量。

保護 iSCSI 連接埠安全

當執行 iSCSI 裝置時，ESXi 不會開啟任何接聽網路連線的連接埠。此措施可降低侵入者透過備用連接埠侵入 ESXi 並控制主機的機率。因此，執行 iSCSI 不會在連線的 ESXi 端產生任何額外的安全性風險。

您執行的任何 iSCSI 目標裝置都必須具有一或多個開啟的 TCP 連接埠可接聽 iSCSI 連線。如果 iSCSI 裝置軟體中存在任何安全性漏洞，則資料遭遇的風險並非 ESXi 所造成。若要降低此風險，請安裝儲存設備製造商提供的所有安全性修補程序，並限制連線到 iSCSI 網路的裝置。

遮罩 SAN 資源並進行分區

可以使用分區設定和 LUN 遮罩來區隔 SAN 活動，並限制對儲存裝置的存取。

透過對您的 SAN 資源使用分區設定和 LUN 遮罩，可以在 vSphere 環境中保護對儲存區的存取權。例如，可以管理為了在 SAN 中進行獨立測試而定義的區域，從而使其不會干擾生產區域中的活動。同樣，還可以針對不同的部門設定不同的區域。

設定區域時，請考慮已在 SAN 裝置上設定的任何主機群組。

每個 SAN 交換器和磁碟陣列的分區設定和遮罩功能以及用於管理 LUN 遮罩的工具，皆因廠商而異。

請參閱 SAN 廠商的說明文件和 *vSphere 儲存區*說明文件。

針對 NFS 4.1 使用 Kerberos

藉由 NFS 4.1 版，ESXi 支援 Kerberos 驗證機制。

RPCSEC_GSS Kerberos 機制是一種驗證服務。它可讓安裝在 ESXi 上的 NFS 4.1 用戶端在掛接 NFS 共用之前向 NFS 伺服器證明其身分。Kerberos 安全性使用密碼編譯在不安全的網路連線中運作。

針對 NFS 4.1，Kerberos 的 ESXi 實作提供兩種安全性模型 krb5 和 krb5i，這兩種模型提供不同的安全層級。

- 僅用於驗證的 Kerberos (krb5) 支援身分識別驗證。
- 用於驗證和資料完整性的 Kerberos (krb5i)，除身分識別驗證之外，還提供資料完整性服務。這些服務透過檢查資料封包是否存在任何潛在修改，協助保護 NFS 流量免遭竄改。

Kerberos 支援密碼編譯演算法，該演算法可防止未經授權的使用者取得 NFS 流量的存取權。ESXi 上的 NFS 4.1 用戶端會嘗試使用 AES256-CTS-HMAC-SHA1-96 或 AES128-CTS-HMAC-SHA1-96 演算法來存取 NAS 伺服器上的共用。在使用 NFS 4.1 資料存放區之前，請先確保 NAS 伺服器上已啟用 AES256-CTS-HMAC-SHA1-96 或 AES128-CTS-HMAC-SHA1-96。

下表比較了 ESXi 支援的 Kerberos 安全性層級。

表格 11-1. Kerberos 安全性類型

		ESXi 6.0	ESXi 6.5 及更新版本
僅用於驗證的 Kerberos (krb5)	RPC 標頭的完整性總和檢查碼	是 (採用 DES)	是 (採用 AES)
	RPC 資料的完整性總和檢查碼	否	否
用於驗證和資料完整性的 Kerberos (krb5i)	RPC 標頭的完整性總和檢查碼	否 (krb5i)	是 (採用 AES)
	RPC 資料的完整性總和檢查碼		是 (採用 AES)

當您使用 Kerberos 驗證時，需考量下列事項：

- ESXi 將 Kerberos 與 Active Directory 網域搭配使用。
- 做為 vSphere 管理員，您可指定 Active Directory 認證，為 NFS 使用者提供 NFS 4.1 Kerberos 資料存放區的存取權。單一認證集用於存取掛接在該主機上的所有 Kerberos 資料存放區。
- 當多個 ESXi 主機共用 NFS 4.1 資料存放區時，必須針對存取共用資料存放區的所有主機使用相同的 Active Directory 認證。若要自動化指派程序，請在主機設定檔中設定使用者並將設定檔套用至所有 ESXi 主機。
- 不能針對多台主機共用的同一個 NFS 4.1 資料存放區使用兩種安全機制 AUTH_SYS 和 Kerberos。

如需逐步指示，請參閱 *vSphere 儲存區* 說明文件。

確認已停用向客體傳送主機效能資料

在安裝了 VMware Tools 的 Windows 作業系統中，vSphere 會包括虛擬機器效能計數器。效能計數器允許虛擬機器擁有者在客體作業系統內進行準確的效能分析。依預設，vSphere 不會向客體虛擬機器公開主機資訊。

依預設，已停用向虛擬機器傳送主機效能資料的功能。此預設設定可防止虛擬機器取得有關實體主機的詳細資訊。如果虛擬機器受到安全性破壞，此設定可防止攻擊者取得主機資料。

備註 下列步驟說明了基本程序。考慮使用其中一個 vSphere 命令列介面 (vCLI、PowerCLI 等)，在所有主機上同時執行此工作。

程序

1 在主控虛擬機器的 ESXi 系統上，瀏覽到 VMX 檔案。

虛擬機器組態檔位於 `/vmfs/volumes/datastore` 目錄中，其中 *datastore* 是儲存虛擬機器檔案之儲存裝置的名稱。

2 在 VMX 檔案中，確認是否設定了下列參數。

```
tools.guestlib.enableHostInfo=FALSE
```

3 儲存並關閉該檔案。

您無法從客體虛擬機器中擷取有關主機的效能資訊。

設定 ESXi Shell 和 vSphere Web Client 的逾時

為了防止侵入者使用閒置工作階段，請務必設定 ESXi Shell 和 vSphere Web Client 的逾時。

ESXi Shell 逾時

對於 ESXi Shell，您可以從 vSphere Web Client 和 Direct Console 使用者介面 (DCUI) 來設定下列逾時。

可用性逾時 可用性逾時設定是在啟用 ESXi Shell 之後和必須登入之前，可以經過的時間量。超過逾時期限後，該服務會停用，並且不允許使用者登入。

閒置逾時 閒置逾時值是使用者從閒置互動式工作階段登出之前可以經過的時間量。對閒置逾時的變更會在下次使用者登入 ESXi Shell 時套用。變更不會影響現有工作階段。

vSphere Web Client 逾時

依預設，vSphere Web Client 工作階段會在閒置 120 分鐘後終止。如 *vCenter Server 和主機管理* 說明文件中所討論，您可以在 `webclient.properties` 檔案中變更此預設值。

透過 TLS Configurator 公用程式管理 TLS 通訊協定組態 12

從 vSphere 6.7 開始，預設僅啟用 TLS 1.2。預設為停用 TLS 1.0 和 TLS 1.1。無論是否執行全新安裝、升級或移轉，vSphere 6.7 都會停用 TLS 1.0 和 TLS 1.1。您可以使用 TLS Configurator 公用程式，在 vSphere 6.7 系統上暫時啟用舊版通訊協定。當所有連線均使用 TLS 1.2 之後，則可以停用較不安全的舊版。

備註 從 vSphere 6.7 開始，TLS Configurator 公用程式包含在該產品中。您不再需要單獨下載。

執行重新設定之前，請考量您的環境。根據您的環境需求和軟體版本，除了 TLS 1.2 以外，您可能還需要重新啟用 TLS 1.0 和 TLS 1.1 以維持互通性。關於 VMware 產品，請參閱 VMware 知識庫文章 2145796 以取得支援 TLS 1.2 的 VMware 產品清單。關於第三方整合，請參閱廠商說明文件。

本章節討論下列主題:

- 支援停用 TLS 版本的連接埠
- 在 vSphere 中啟用或停用 TLS 版本
- 執行選擇性手動備份
- 在 vCenter Server 系統上啟用或停用 TLS 版本
- 在 ESXi 主機上啟用或停用 TLS 版本
- 啟用或停用外部 Platform Services Controller 系統上的 TLS 版本
- 針對已啟用 TLS 的通訊協定掃描 vCenter Server
- 還原 TLS 組態變更
- 在 Windows 上的 vSphere Update Manager 上啟用或停用 TLS 版本

支援停用 TLS 版本的連接埠

當您在 vSphere 環境中執行 TLS Configurator 公用程式時，您可以在於 vCenter Server、Platform Services Controller 和 ESXi 主機上使用 TLS 的連接埠間停用 TLS。您可停用 TLS 1.0 或同時停用 TLS 1.0 和 TLS 1.1。

下表會列出 TLS 連接埠。如果有連接埠未包含在表格中，則表示其不受公用程式影響。

表格 12-1. 受 TLS Configurator 公用程式影響的 vCenter Server 和 Platform Services Controller

服務	Windows 系統的 vCenter Server	vCenter ServerVirtual Appliance	連接埠
VMware HTTP Reverse Proxy	rhttpproxy	vmware-rhttpproxy	443
VMware vCenter Server 服務	vpxd	vmware-vpxd	443
VMware Directory Service	VMWareDirectoryService	vmdird	636
VMware Syslog Collector	vmwaresyslogcollector	rsyslogd (*)	1514
VMware 應用裝置管理介面	不適用	vami-lighttp(*)	5480
vSphere Auto Deploy Waiter	vmware-autodeploy-waiter	vmware-rbd-watchdog	6501 6502
VMware Secure Token Service	VMwareSTS	vmware-stsd	7444
vSphere Authentication Proxy	VMWareCAMService	vmcam	7476
vSphere Update Manager 服務	vmware-ufad-vci	vmware-updatemgr(*)	8084 9087
vSphere Web Client	vspherewebclientsvc	vsphere-client	9443
VMware vSphere Profile-Driven Storage Service	vimPBSM	vmware-sps	大於 1024 的隨機連接埠

(*) 只能在 vCenter ServerVirtual Appliance 上重新設定這些服務。在 Windows 上的 vCenter Server 中，透過編輯組態檔重新設定 Update Manager 的 TLS 連接埠。請參閱在 Windows 上的 vSphere Update Manager 上啟用或停用 TLS 版本。

表格 12-2. 受 TLS Configurator 公用程式影響的 ESXi 連接埠

服務	服務名稱	連接埠
VMware HTTP 反向 Proxy 和主機精靈	Hostd	443
VMware vSAN VASA 廠商提供者	vSANVP	8080
VMware 容錯網域管理員	FDM	8182
適用於 IO 篩選器的 VMware vSphere API	ioFilterVPServer	9080
ESXiWBEM 服務	sfcbd-watchdog	5989
ESXivVold 用戶端服務	vvold	大於 1024 的隨機連接埠

附註和注意須知

- vCenter Server 目前不支援使用 TLSv1.0、TLSv1.1 或 TLSv1.2 連線到電子郵件伺服器。vCenter Server 使用純文字執行電子郵件功能。如需詳細資訊，請參閱 VMware 知識庫文章 2063147。

- 從 vSphere 6.7 開始，您可以使用 TLS 1.2 來加密 vCenter Server 與外部 Microsoft SQL Server 之間的連線。您無法僅使用 TLS 1.2 與外部 Oracle 資料庫連線。請參閱 VMware 知識庫文章 2149745。
- 請勿在 Windows Server 2008 上執行的 vCenter Server 或 Platform Services Controller 執行個體上停用 TLS 1.0。Windows 2008 僅支援 TLS 1.0。請參閱《*伺服器角色和技術指南*》中的 Microsoft TechNet 文章〈*TLS/SSL 設定*〉。
- 如果變更 TLS 通訊協定，則必須重新啟動 ESXi 主機以套用變更。即使使用主機設定檔在整個叢集組態中套用變更，也必須重新啟動主機。您可以選擇立即重新啟動主機，或將重新啟動延後到一個更加方便的時間。

在 vSphere 中啟用或停用 TLS 版本

停用 TLS 版本是一個多階段程序。以正確順序停用 TLS 版本可確保您的環境在執行程序期間保持正常運作。

1. 如果您的環境包含 Windows 上的 vSphere Update Manager，而且 vSphere Update Manager 位在獨立的系統，請透過編輯組態檔明確停用通訊協定。請參閱在 Windows 上的 vSphere Update Manager 上啟用或停用 TLS 版本。

   vCenter Server Appliance 上的 vSphere Update Manager 永遠隨附 vCenter Server 系統，該指令碼會更新對應的連接埠。
2. 在 vCenter Server 上執行該公用程式。
3. 在每部由 vCenter Server 管理的 ESXi 主機上執行該公用程式。您可以針對每部主機或叢集中的所有主機執行此工作。
4. 如果您的環境使用一或多個 Platform Services Controller 執行個體，請在每個執行個體上執行該公用程式。

先決條件

在您的環境中使用 TLS 有兩個選擇。

- 停用 TLS 1.0 並啟用 TLS 1.1 和 TLS 1.2。
- 停用 TLS 1.0 和 TLS 1.1 並啟用 TLS 1.2。

執行選擇性手動備份

TLS 組態公用程式會在每次指令碼於 vCenter Server Appliance 上修改 vCenter Server、Platform Services Controller 或 vSphere Update Manager 時執行備份。如果需要備份至特定目錄，您可以執行手動備份。

不支援備份 ESXi 組態。

對於 vCenter Server 或 Platform Services Controller，Windows 和應用裝置的預設目錄有所不同。

作業系統	備份目錄
Windows	c:\users*current_user*\appdata\local\temp*yearmonthday*T*time*
Linux	/tmp/*yearmonthday*T*time*

程序

1 將目錄變更為 VcTlsReconfigurator。

作業系統	命令
Windows	`cd %VMWARE_CIS_HOME%\TlsReconfigurator\VcTlsReconfigurator`
Linux	`cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`

2 若要備份至特定目錄，請執行下列命令。

作業系統	命令
Windows	*directory_path*\VcTlsReconfigurator> reconfigureVc backup -d *backup_directory_path*
Linux	*directory_path*/VcTlsReconfigurator> ./reconfigureVc backup -d *backup_directory_path*

3 確認您的備份已成功。

成功備份會與以下範例類似。

```
vCenter Transport Layer Security reconfigurator, version=6.7.0, build=8070195
For more information refer to the following article: https://kb.vmware.com/kb/2147469
Log file: "/var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log".
================= Backing up vCenter Server TLS configuration ==================
Using backup directory: /tmp/20180422T224804
Backing up: vmware-sps
Backing up: vmdird
Backing up: vmware-rbd-watchdog
Backing up: vmware-vpxd
Backing up: vmware-updatemgr
Backing up: vmcam
Backing up: vsphere-client
Backing up: vami-lighttp
Backing up: rsyslog
Backing up: vmware-rhttpproxy
Backing up: vmware-stsd
```

4 (選擇性) 如果您之後必須執行還原，您可以執行以下命令。

```
reconfigureVc restore -d optional_custom_backup_directory_path
```

在 vCenter Server 系統上啟用或停用 TLS 版本

您可以使用 TLS 組態公用程式，啟用或停用含外部 Platform Services Controller 之 vCenter Server 系統上以及含內嵌式 Platform Services Controller 之 vCenter Server 系統上的 TLS 版本。在執行該程序過程中，您可以停用 TLS 1.0 並啟用 TLS 1.1 和 TLS 1.2，也可以停用 TLS 1.0 和 TLS 1.1 並僅啟用 TLS 1.2。

先決條件

請確認 vCenter Server 所管理的主機和服務可使用仍保持啟用的 TLS 版本進行通訊。僅使用 TLS 1.0 通訊的產品將無法連線。

程序

1 使用 administrator@vsphere.local 的使用者名稱和密碼，或以可執行指令碼之 vCenter Single Sign-On 管理員群組的其他成員身分，來登入 vCenter Server 系統。

2 前往指令碼所在的目錄。

作業系統	命令
Windows	`cd %VMWARE_CIS_HOME%\TlsReconfigurator\VcTlsReconfigurator`
Linux	`cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`

3 根據您的作業系統以及要使用的 TLS 版本執行命令。

- 若要停用 TLS 1.0 並同時啟用 TLS 1.1 和 TLS 1.2，請執行以下命令。

作業系統	命令
Windows	*directory_path*`\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2`
Linux	*directory_path*`/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2`

- 若要停用 TLS 1.0 和 TLS 1.1 並僅啟用 TLS 1.2，請執行以下命令。

作業系統	命令
Windows	*directory_path*`\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2`
Linux	*directory_path*`/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2`

4 如果您的環境包含其他 vCenter Server 系統，請在每個 vCenter Server 系統上重複該程序。

5 請在每部 ESXi 主機和各個 Platform Services Controller 上重複設定該組態。

在 ESXi 主機上啟用或停用 TLS 版本

您可使用 TLS 組態公用程式來啟用或停用 ESXi 主機上的 TLS 版本。在執行該程序過程中，您可以停用 TLS 1.0 並啟用 TLS 1.1 和 TLS 1.2，也可以停用 TLS 1.0 和 TLS 1.1 並僅啟用 TLS 1.2。

對於 ESXi 主機，請使用與 vSphere 環境中的其他元件不同的公用程式。公用程式特定於版本，且無法用於先前版本。

先決條件

請確保與 ESXi 主機相關的任何產品或服務均可使用 TLS 1.1 或 TLS 1.2 進行通訊。僅使用 TLS 1.0 通訊的產品將失去連線功能。

此程序說明如何在單一主機上執行工作。您可以撰寫指令碼以設定多部主機。

程序

1 使用可執行指令碼之 vCenter Single Sign-On 使用者的使用者名稱和密碼，來登入 vCenter Server 系統。

2 前往指令碼所在的目錄。

作業系統	命令
Windows	`cd %VMWARE_CIS_HOME%\TlsReconfigurator\EsxTlsReconfigurator`
Linux	`cd /usr/lib/vmware-TlsReconfigurator/EsxTlsReconfigurator`

3 在屬於叢集一部分的主機上，執行以下其中一個命令。

- 若要在叢集中的所有主機上停用 TLS 1.0 並同時啟用 TLS 1.1 和 TLS 1.2，請執行以下命令。

作業系統	命令
Windows	`reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2`
Linux	`./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2`

- 若要在叢集中的所有主機上停用 TLS 1.0 和 TLS 1.1 並僅啟用 TLS 1.2，請執行以下命令。

作業系統	命令
Windows	`reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2`
Linux	`./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2`

4 在個別主機上，執行以下其中一個命令。

- 若要在個別主機上停用 TLS 1.0 並同時啟用 TLS 1.1 和 TLS 1.2，請執行以下命令。

作業系統	命令
Windows	`reconfigureEsx vCenterHost –h ESXi_Host_Name –u Administrative_User –p TLSv1.1 TLSv1.2`
Linux	`./reconfigureEsx vCenterHost –h ESXi_Host_Name –u Administrative_User –p TLSv1.1 TLSv1.2`

備註 若要重新設定獨立 ESXi 主機 (不屬於 vCenter Server 系統)，請使用 `ESXiHost –h HOST –u ESXi_USER` 選項。對於 *HOST* 選項，您可以指定單一 ESXi 主機 IP 位址或 FQDN，或一系列主機 IP 位址或 FQDN。例如，若要在兩個 ESXi 主機上啟用 TLS 1.1 和 TLS 1.2：

```
reconfigureEsx ESXiHost –h 198.51.100.2 198.51.100.3 –u root –p TLSv1.1 TLSv1.2
```

- 若要在個別主機上停用 TLS 1.0 和 TLS 1.1 並僅啟用 TLS 1.2，請執行以下命令。

作業系統	命令
Windows	`reconfigureEsx vCenterHost –h ESXi_Host_Name –u Administrative_User –p TLSv1.2`
Linux	`./reconfigureEsx vCenterHost –h ESXi_Host_Name –u Administrative_User –p TLSv1.2`

5 將 ESXi 主機重新開機以完成 TLS 通訊協定變更。

啟用或停用外部 Platform Services Controller 系統上的 TLS 版本

如果您的環境包含一或多個 Platform Services Controller 系統，您可以使用 TLS 組態公用程式來變更要支援的 TLS 版本。

如果您的環境僅使用內嵌式 Platform Services Controller，則之前已在 vCenter Server 程序期間完成此工作。請參閱在 vCenter Server 系統上啟用或停用 TLS 版本。

備註 僅在您確認每個 vCenter Server 系統都在執行相容的 TLS 版本後，再繼續進行此工作。

在執行該程序過程中，您可以停用 TLS 1.0 並啟用 TLS 1.1 和 TLS 1.2，也可以停用 TLS 1.0 和 TLS 1.1 並僅啟用 TLS 1.2。

先決條件

請確保連線到 Platform Services Controller 的應用程式、主機和服務合格，或設定為使用保持啟用的 TLS 版本進行通訊。由於 Platform Services Controller 負責處理驗證和憑證管理，請審慎考量哪些服務可能會受影響。僅使用不支援的通訊協定進行通訊的服務將無法連線。

程序

1 以可執行指令碼的使用者身分登入 Platform Services Controller，並前往指令碼所在的目錄。

作業系統	命令
Windows	`cd %VMWARE_CIS_HOME%\TlsReconfigurator\VcTlsReconfigurator`
Linux	`cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`

2 您可以在 Windows 上的 Platform Services Controller 或 Platform Services Controller 應用裝置上執行此工作。

- 若要停用 TLS 1.0 並同時啟用 TLS 1.1 和 TLS 1.2，請執行以下命令。

作業系統	命令
Windows	*directory_path*`\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2`
Linux	*directory_path*`\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2`

- 若要停用 TLS 1.0 和 TLS 1.1 並僅啟用 TLS 1.2，請執行以下命令。

作業系統	命令
Windows	*directory_path*`\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2`
Linux	*directory_path*`\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2`

3 如果您的環境包含其他 Platform Services Controller 系統，請重複該程序。

針對已啟用 TLS 的通訊協定掃描 vCenter Server

啟用或停用 vCenter Server 上的 TLS 版本後，您可以使用 TLS 組態公用程式來檢視變更。

TLS 組態公用程式 `scan` 選項會顯示各項服務已啟用的 TLS 版本。

程序

1 登入 vCenter Server 系統。

作業系統	程序
Windows	a 以具有管理員權限的使用者身分登入。 b 前往 `VcTlsReconfigurator` 目錄。 `cd %VMWARE_CIS_HOME%\TlsReconfigurator\VcTlsReconfigurator`

Linux	a 使用 SSH 連線應用裝置，並以具有執行指令碼權限的使用者身分登入。
	b 如果 Bash shell 目前尚未啟用，請執行以下命令。
	`shell.set --enabled true`
	`shell`
	c 前往 `VcTlsReconfigurator` 目錄。
	`cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`

2 若要顯示哪些服務已啟用 TLS 以及所使用的連接埠，請執行下列命令。

```
reconfigureVc scan
```

還原 TLS 組態變更

您可使用 TLS 組態公用程式來還原組態變更。當您還原變更時，系統會啟用您使用 TLS Configurator 公用程式停用的通訊協定。

您僅可在先前已備份組態的情況下才能執行復原。ESXi 主機不支援還原變更。

以此順序執行復原。

1 vSphere Update Manager。

   如果您的環境在 Windows 系統上執行個別的 vSphere Update Manager 執行個體，您必須先更新 vSphere Update Manager。

2 vCenter Server.

3 Platform Services Controller.

先決條件

還原變更之前，使用 vCenter Server Appliance 介面執行 Windows 機器或應用裝置的備份。

程序

1 連線至 Windows 機器或應用裝置。

2 登入您要還原變更的系統。

選項	說明
Windows	a 以具有管理員權限的使用者身分登入。 b 前往 `VcTlsReconfigurator` 目錄。 `cd %VMWARE_CIS_HOME%\TlsReconfigurator\VcTlsReconfigurator`

Linux	a 使用 SSH 連線應用裝置，並以具有執行指令碼權限的使用者身分登入。
	b 如果 Bash shell 目前尚未啟用，請執行以下命令。
	`shell.set --enabled true`
	`shell`
	c 前往 `VcTlsReconfigurator` 目錄。
	`cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`

3 檢閱先前備份。

選項	說明

Windows	`C:\ProgramData\VMware\vCenterServer\logs\vmware\vSphere-TlsReconfigurator\VcTlsReconfigurator.log`
	輸出與下列範例類似。
	`c:\users\username\appdata\local\temp\20161108T161539`
	`c:\users\username\appdata\local\temp\20161108T171539`

Linux	`grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log`
	輸出與下列範例類似。
	`2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920`
	`2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259`

4 執行以下其中一個命令以執行還原。

選項	說明

Windows	`reconfigureVc restore -d Directory_path_from_previous_step`
	例如：
	`reconfigureVc restore -d c:\users\username\appdata\local\temp\20161108T171539`

Linux	`reconfigureVc restore -d Directory_path_from_previous_step`
	例如：
	`reconfigureVc restore -d /tmp/20161117T172920`

5 請對任何其他 vCenter Server 執行個體重複該程序。

6 請對任何其他 Platform Services Controller 執行個體重複該程序。

在 Windows 上的 vSphere Update Manager 上啟用或停用 TLS 版本

在 vSphere Update Manager 6.7 中，預設為啟用 TLS 1.2。預設為停用 TLS 1.0 和 TLS 1.1。您可以啟用 TLS 版本 1.0 和 TLS 版本 1.1，但您無法停用 TLS 版本 1.2。

您可以使用 TLS 組態公用程式管理其他服務的 TLS 通訊協定組態。然而，針對 Windows 上的 vSphere Update Manager，您必須手動重新設定 TLS 通訊協定。

修改 TLS 通訊協定組態可能涉及以下任何工作。

- 停用 TLS 版本 1.0，但保持啟用 TLS 版本 1.1 和 TLS 版本 1.2。
- 停用 TLS 版本 1.0 和 TLS 版本 1.1，但保持啟用 TLS 版本 1.2。
- 重新啟用已停用的 TLS 通訊協定版本。

停用 Update Manager 連接埠 9087 的舊版 TLS

您可以透過修改 `jetty-vum-ssl.xml` 組態檔停用連接埠 9087 的舊版 TLS。該程序與連接埠 8084 不同。

備註 停用 TLS 版本前，請確保沒有服務使用該版本與 vSphere Update Manager 通訊。

先決條件

停止 vSphere Update Manager 服務。請參閱 *安裝與管理 VMware vSphere Update Manager* 說明文件。

程序

1 停止 vSphere Update Manager 服務。

2 導覽至 Update Manager 安裝目錄，這與 vSphere 6.0 和 vSphere 6.5 及更新版本不同。

版本	位置
vSphere 6.0	`C:\Program Files (x86)\VMware\Infrastructure\Update Manager`
vSphere 6.5 及更新版本	`C:\Program Files\VMware\Infrastructure\Update Manager`

3 備份 `jetty-vum-ssl.xml` 檔案並開啟檔案。

4 透過變更檔案停用舊版 TLS。

選項	說明

停用 TLS 1.0。保持啟用 TLS 1.1 和 TLS 1.2。	`<Set name="ExcludeProtocols">`
	`  <Array type="java.lang.String">`
	`  <Item>TLSv1</Item>`
	`  </Array>`
	`</Set>`

停用 TLS 1.0 和 TLS 1.1。保持啟用 TLS 1.2。	`<Set name="ExcludeProtocols">`
	`  <Array type="java.lang.String">`
	`  <Item>TLSv1</Item>`
	`  <Item>TLSv1.1</Item>`
	`  </Array>`
	`</Set>`

5 儲存檔案。

6 重新啟動 vSphere Update Manager 服務。

停用 Update Manager 連接埠 8084 的舊版 TLS

您可以透過修改 `vci-integrity.xml` 組態檔，停用連接埠 8084 的舊版 TLS。該程序與連接埠 9087 不同。

備註 停用 TLS 版本前，請確保沒有服務使用該版本與 vSphere Update Manager 通訊。

先決條件

停止 vSphere Update Manager 服務。請參閱 *安裝與管理 VMware vSphere Update Manager* 說明文件。

程序

1 停止 vSphere Update Manager 服務。

2 導覽至 Update Manager 安裝目錄，這與 6.0 和 6.5 及更新版本不同。

版本	位置
vSphere 6.0	`C:\Program Files (x86)\VMware\Infrastructure\Update Manager`
vSphere 6.5 及更新版本	`C:\Program Files\VMware\Infrastructure\Update Manager`

3 備份 `vci-integrity.xml` 檔案並開啟檔案。

4 編輯 vci-integrity.xml 檔案並新增 <protocols> 標籤。

```
<vmacore>
   <ssl>
      <handshakeTimeoutMs>120000</handshakeTimeoutMS>
      <protocols>protocols_value</protocols>
   </ssl>
</vmacore>
```

5 根據您要啟用的 TLS 版本，在 <procotols> 標籤中使用以下其中一個值。

要啟用的 TLS 版本	使用...
全部	tls1.0,tls1.1,tls1.2。
僅限 TLSv1.1 和 TLSv.1.2	tls.1.1,tls1.2。
僅限 TLSv1.2	tls1.2，或不包含 protocols 標籤。由於預設值是 TLS 1.2，因此 vmacore 中未顯示開頭為 protocols 標籤。

6 (選擇性) 從 vSphere 6.0 Update 2 開始，您可能具有 <sslOptions> 標籤。

如果是，請移除 <sslOptions> 標籤。

7 儲存 vci-integrity.xml 檔案。

8 重新啟動 vSphere Update Manager 服務。

重新啟用 Update Manager 連接埠 9087 停用的 TLS 版本

如果您停用 Update Manager 連接埠 9087 的 TLS 版本，但是遇到問題，您可以重新啟用該版本。該程序與重新啟用連接埠 8084 不同。

重新啟用舊版 TLS 會有安全疑慮。

程序

1 停止 vSphere Update Manager 服務。

2 導覽至 Update Manager 安裝目錄，這與 6.0 和 6.5 及更新版本不同。

版本	位置
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5 及更新版本	C:\Program Files\VMware\Infrastructure\Update Manager

3 備份 jetty-vum-ssl.xml 檔案並開啟檔案。

4 移除與您要啟用的 TLS 通訊協定版本對應的 TLS 標記。

例如，移除 jetty-vum-ssl.xml 檔案中的 <Item>TLSv1.1</Item> 以啟用 TLSv1.1。

5 儲存檔案。

6 重新啟動 vSphere Update Manager 服務。

重新啟用 Update Manager 連接埠 8084 停用的 TLS 版本

如果您停用 Update Manager 連接埠 8084 的 TLS 版本，但是遇到問題，您可以重新啟用該版本。該程序與連接埠 9087 不同。

重新啟用舊版 TLS 會有安全疑慮。

程序

1 停止 vSphere Update Manager 服務。

2 導覽至 Update Manager 安裝目錄，這與 6.0 和 6.5 及更新版本不同。

版本	位置
vSphere 6.0	`C:\Program Files (x86)\VMware\Infrastructure\Update Manager`
vSphere 6.5 及更新版本	`C:\Program Files\VMware\Infrastructure\Update Manager`

3 備份 `vci-integrity.xml` 檔案並開啟檔案。

4 編輯 `<protocols>` 標籤。

```
<vmacore>
   <ssl>
      <handshakeTimeoutMs>120000</handshakeTimeoutMS>
      <protocols>protocols_value</protocols>
   </ssl>
</vmacore>
```

5 根據您要啟用的 TLS 版本，在 `<procotols>` 標籤中使用以下其中一個值。

要啟用的 TLS 版本	使用...
全部	`tls1.0,tls1.1,tls1.2`。
僅限 TLSv1.1 和 TLSv.1.2	`tls.1.1,tls1.2`。
僅限 TLSv1.2	`tls1.2`，或不包含 `protocols` 標籤。由於預設值是 TLS 1.2，因此 `vmacore` 中未顯示開頭為 `protocols` 標籤。

6 儲存 `vci-integrity.xml` 檔案。

7 重新啟動 vSphere Update Manager 服務。

13 定義的權限

下列資料表列出了一些預設權限，為角色選取這些權限時，可以與使用者配對，也可以指派給物件。

在設定權限時，請確認對所有物件類型的每項特定動作均設定了適當的權限。除了要擁有對正操縱的物件的存取權限之外，部分作業需要有對根資料夾或父系資料夾的存取權限。部分作業還需要對父系資料夾及相關物件的存取權限或執行權限。

vCenter Server 延伸可能定義未在此處列出的其他權限。如需這些權限的詳細資訊，請參閱延伸說明文件。

本章節討論下列主題:

- 主機本機作業權限
- 主機 vSphere Replication 權限
- 主機設定檔權限
- 網路權限
- 效能權限
- 權限 (Permissions) 權限
- Profile-Driven Storage 權限
- 資源權限
- 排定的工作權限
- 工作階段權限
- 儲存區視圖權限
- 工作權限
- Transfer Service 權限
- 虛擬機器組態權限
- 虛擬機器客體作業權限
- 虛擬機器互動權限
- 虛擬機器詳細目錄權限
- 虛擬機器佈建權限
- 虛擬機器服務組態權限
- 虛擬機器快照管理權限
- 虛擬機器 vSphere Replication 權限
- dvPort 群組權限
- vApp 權限
- vServices 權限
- vSphere 標記權限

警示權限

警示權限控制在詳細目錄物件上建立、修改警示及回應警示的能力。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-1. 警示權限

權限名稱	說明	要求
警示.確認警示	允許在所有已觸發的警示上隱藏所有警示動作。	對其定義了警示的物件
警示.建立警示	允許建立新警示。 如果透過自訂動作建立警示，則在使用者建立警示時，將驗證執行動作的權限。	對其定義了警示的物件
警示.停用警示動作	允許在觸發警示之後阻止警示動作。此動作不會停用警示。	對其定義了警示的物件
警示.修改警示	允許變更警示的內容。	對其定義了警示的物件
警示.移除警示	允許刪除警示。	對其定義了警示的物件
警示.設定警示狀態	允許變更所設定的事件警示的狀態。狀態可以變更為**一般**、**警告**或**警示**。	對其定義了警示的物件

Auto Deploy 與映像設定檔權限

Auto Deploy 權限控制誰可以在 Auto Deploy 規則下執行不同的工作，以及誰可以關聯主機。Auto Deploy 權限還可讓您控制誰可以建立或編輯映像設定檔。

下表說明判定誰可以管理 Auto Deploy 規則和規則集以及誰可以建立和編輯映像設定檔的權限。請參閱 *vCenter Server 安裝和設定*。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-2. Auto Deploy 權限

權限名稱	說明	要求
Auto Deploy.主機.關聯機器	允許使用者將主機與機器關聯。	vCenter Server
Auto Deploy.映像設定檔.建立	允許建立映像設定檔。	vCenter Server
Auto Deploy.映像設定檔.編輯	允許編輯映像設定檔。	vCenter Server
Auto Deploy.規則.建立	允許建立 Auto Deploy 規則。	vCenter Server
Auto Deploy.規則.刪除	允許刪除 Auto Deploy 規則。	vCenter Server

表格 13-2. Auto Deploy 權限 (繼續)

權限名稱	說明	要求
Auto Deploy .規則.編輯	允許編輯 Auto Deploy 規則。	vCenter Server
Auto Deploy.規則集.啟用	允許啟動 Auto Deploy 規則集。	vCenter Server
Auto Deploy.規則集.編輯	允許編輯 Auto Deploy 規則集。	vCenter Server

憑證權限

憑證權限控制可管理 ESXi 憑證的使用者。

此權限決定可對 ESXi 主機執行憑證管理的使用者。如需 vCenter Server 憑證管理的相關資訊，請參閱 *Platform Services Controller 管理*說明文件中的「進行憑證管理作業所需的權限」。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-3. 主機憑證權限

權限名稱	說明	要求
憑證.管理憑證	允許對 ESXi 主機進行憑證管理。	vCenter Server

內容程式庫權限

內容程式庫會為虛擬機器範本和 vApp 提供簡單且有效的管理。內容程式庫權限會控制可檢視或管理內容程式庫不同方面的人選。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-4. 內容程式庫權限

權限名稱	說明	要求
內容程式庫.新增程式庫項目	允許在程式庫中新增項目。	程式庫
內容程式庫.建立本機程式庫	允許在指定的 vCenter Server 系統上建立本機程式庫。	vCenter Server
內容程式庫.建立已訂閱程式庫	允許建立已訂閱程式庫。	vCenter Server

表格 13-4. 內容程式庫權限 (繼續)

權限名稱	說明	要求
內容程式庫.刪除程式庫項目	允許刪除程式庫項目。	程式庫。將此權限設定為散佈到所有程式庫項目。
內容程式庫.刪除本機程式庫	允許刪除本機程式庫。	程式庫
內容程式庫.刪除已訂閱程式庫	允許刪除已訂閱程式庫。	程式庫
內容程式庫.下載檔案	允許從內容程式庫下載檔案。	程式庫
內容程式庫.收回程式庫項目	允許收回項目。已訂閱程式庫的內容可快取或無法快取。如果已快取內容，則您可以透過收回程式庫項目來將其釋放 (如果您擁有該權限)。	程式庫。將此權限設定為散佈到所有程式庫項目。
內容程式庫.收回已訂閱程式庫	允許收回已訂閱程式庫。已訂閱程式庫的內容可快取或無法快取。如果已快取內容，則您可以透過收回程式庫來將其釋放 (如果您擁有該權限)。	程式庫
內容程式庫.匯入儲存區	如果來源檔案 URL 以 `ds://` 或 `file://` 開頭，將允許使用者匯入程式庫項目。對於內容程式庫管理員，此權限預設為停用。因為從儲存區 URL 匯入即表示匯入內容，因此僅在必要時，並且將執行匯入的使用者存在安全性問題時，才會啟用此權限。	程式庫
內容程式庫.探查訂閱資訊	此權限可讓解決方案使用者和 API 探查遠端程式庫的訂閱資訊，其中包括 URL、SSL 憑證和密碼。產生的結構會介紹是否成功設定訂閱，或者是否存在諸如 SSL 錯誤的問題。	程式庫
內容程式庫.讀取儲存區	允許讀取內容程式庫儲存區。	程式庫
內容程式庫.同步程式庫項目	允許同步程式庫項目。	程式庫。將此權限設定為散佈到所有程式庫項目。
內容程式庫.同步已訂閱程式庫	允許同步已訂閱程式庫。	程式庫
內容程式庫.類型自我檢查	允許解決方案使用者或 API 自我檢查 Content Library Service 的類型支援外掛程式。	程式庫
內容程式庫.更新組態設定	允許更新組態設定。 沒有與此權限相關聯的 vSphere Web Client 使用者介面元素。	程式庫
內容程式庫.更新檔案	允許將內容上傳到內容程式庫中。此外，也允許從程式庫項目中移除檔案。	程式庫
內容程式庫.更新程式庫	允許更新內容程式庫。	程式庫
內容程式庫.更新程式庫項目	允許更新程式庫項目。	程式庫。將此權限設定為散佈到所有程式庫項目。
內容程式庫.更新本機程式庫	允許更新本機程式庫。	程式庫
內容程式庫.更新已訂閱程式庫	允許更新已訂閱程式庫的內容。	程式庫
內容程式庫.檢視組態設定	允許檢視組態設定。 沒有與此權限相關聯的 vSphere Web Client 使用者介面元素。	程式庫

密碼編譯作業權限

密碼編譯作業權限可控制對特定類型的物件執行特定類型密碼編譯作業的人員。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-5. 密碼編譯作業權限

權限名稱	說明	要求
密碼編譯作業.直接存取	允許使用者存取加密的資源。例如，使用者可以匯出虛擬機器、擁有虛擬機器的 NFC 存取權等。	虛擬機器、主機或資料存放區
密碼編譯作業.新增磁碟	允許使用者將磁碟新增到加密的虛擬機器。	虛擬機器
密碼編譯作業.複製	允許使用者複製加密的虛擬機器。	虛擬機器
密碼編譯作業.解密	允許使用者解密虛擬機器或磁碟。	虛擬機器
密碼編譯作業.加密	允許使用者加密虛擬機器或虛擬機器磁碟。	虛擬機器
密碼編譯作業.加密新增項目	允許使用者在建立虛擬機器期間加密虛擬機器，或在建立磁碟期間加密磁碟。	虛擬機器資料夾
密碼編譯作業.管理加密原則	允許使用者使用加密 IO 篩選器管理虛擬機器儲存區原則。依預設，使用加密儲存區原則的虛擬機器不會使用其他儲存區原則。	vCenter Server 根資料夾
密碼編譯作業.管理金鑰伺服器	允許使用者管理 vCenter Server 系統的金鑰管理伺服器。管理工作包括新增和移除 KMS 執行個體，以及建立與 KMS 的信任關係。	vCenter Server 系統。
密碼編譯作業.管理金鑰	允許使用者執行金鑰管理作業。vSphere Web Client 中不支援這些作業，但可以使用 `crypto-util` 或 API 來執行這些作業。	vCenter Server 根資料夾
密碼編譯作業.移轉	允許使用者將加密的虛擬機器移轉至其他 ESXi 主機。支援使用或不使用 vMotion 和 Storage vMotion 的移轉。不支援移轉至其他 vCenter Server 執行個體。	虛擬機器
密碼編譯作業.Recrypt	允許使用者使用不同金鑰對虛擬機器或磁碟進行雙重加密。深度和淺層雙重加密作業都需要此權限。	虛擬機器

表格 13-5. 密碼編譯作業權限 (繼續)

權限名稱	說明	要求
密碼編譯作業.登錄虛擬機器	允許使用者向 ESXi 主機登錄加密的虛擬機器。	虛擬機器資料夾
密碼編譯作業.登錄主機	允許使用者在主機上啟用加密。您可以在主機上明確啟用加密，虛擬機器建立程序也可以啟用加密。	獨立主機的主機資料夾、叢集中主機的叢集

資料中心權限

資料中心權限控制在 vSphere Web Client 詳細目錄中建立和編輯資料中心的能力。

所有資料中心權限僅用於 vCenter Server。在資料中心資料夾或根物件上定義**建立資料中心**權限。所有其他資料中心權限與資料中心、資料中心資料夾或根物件配對。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-6. 資料中心權限

權限名稱	說明	要求
資料中心.建立資料中心	允許建立新資料中心。	資料中心資料夾或根物件
資料中心.移動資料中心	允許移動資料中心。 權限必須同時存在於來源位置和目的地位置。	資料中心、來源和目的地
資料中心.網路通訊協定設定檔組態	允許為資料中心設定網路設定檔。	資料中心
資料中心.查詢 IP 集區配置	允許設定 IP 位址集區。	資料中心
資料中心.重新設定資料中心	允許重新設定資料中心。	資料中心
資料中心.釋放 IP 配置	允許為資料中心釋放已指派的 IP 配置。	資料中心
資料中心.移除資料中心	允許移除資料中心。 為了有執行此作業的權限，必須將此權限指派給該物件及其父系物件。	資料中心加父系物件
資料中心.重新命名資料中心	允許變更資料中心的名稱。	資料中心

資料存放區權限

資料存放區權限可控制在資料存放區上瀏覽、管理和配置空間的功能。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-7. 資料存放區權限

權限名稱	說明	要求
資料存放區.配置空間	允許在資料存放區上為虛擬機器、快照、複製或虛擬磁碟配置空間。	資料存放區
資料存放區.瀏覽資料存放區	允許在資料存放區上瀏覽檔案。	資料存放區
資料存放區.設定資料存放區	允許設定資料存放區。	資料存放區
資料存放區.低層級檔案作業	允許在資料存放區瀏覽器中執行讀取、寫入、刪除和重新命名作業。	資料存放區
資料存放區.移動資料存放區	允許在資料夾之間移動資料存放區。 權限必須存在於來源和目的地。	資料存放區、來源和目的地
資料存放區.移除資料存放區	允許移除資料存放區。 此權限已被取代。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	資料存放區
資料存放區.移除檔案	允許在資料存放區中刪除檔案。 此權限已被取代。指派**低層級檔案作業**權限。	資料存放區
資料存放區.重新命名資料存放區	允許重新命名資料存放區。	資料存放區
資料存放區.更新虛擬機器檔案	允許在資料存放區重新簽章之後，更新指向資料存放區中虛擬機器檔案的檔案路徑。	資料存放區
資料存放區.更新虛擬機器中繼資料	允許更新與資料存放區關聯的虛擬機器中繼資料。	資料存放區

資料存放區叢集權限

資料存放區叢集權限可控制 Storage DRS 資料存放區叢集的組態。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-8. 資料存放區叢集權限

權限名稱	說明	要求
資料存放區叢集.設定資料存放區叢集	允許建立和設定 Storage DRS 資料存放區叢集的設定。	資料存放區叢集

Distributed Switch 權限

Distributed Switch 權限控制執行與管理 Distributed Switch 執行個體相關的工作的能力。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-9. vSphere Distributed Switch 權限

權限名稱	說明	要求
Distributed Switch.建立	允許建立分散式交換器。	資料中心、網路資料夾
Distributed Switch.刪除	允許移除分散式交換器。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	分散式交換器
Distributed Switch.主機作業	允許變更分散式交換器的主機成員。	分散式交換器
Distributed Switch.修改	允許變更分散式交換器的組態。	分散式交換器
Distributed Switch.移動	允許將 vSphere Distributed Switch 移到其他資料夾。	分散式交換器
Distributed Switch.Network I/O Control 作業	允許變更 vSphere Distributed Switch 的資源設定。	分散式交換器
Distributed Switch.原則作業	允許變更 vSphere Distributed Switch 的原則。	分散式交換器
Distributed Switch.連接埠組態作業	允許變更 vSphere Distributed Switch 中連接埠的組態。	分散式交換器
Distributed Switch.連接埠設定作業	允許變更 vSphere Distributed Switch 中連接埠的設定。	分散式交換器
Distributed Switch.VSPAN 作業	允許變更 vSphere Distributed Switch 的 VSPAN 組態。	分散式交換器

ESX Agent Manager 權限

ESX Agent Manager 權限控制與 ESX Agent Manager 和代理程式虛擬機器相關的作業。ESX Agent Manager 是一項服務，可讓您安裝與主機關聯且不受 VMware DRS 或移轉虛擬機器之其他服務影響的管理虛擬機器。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-10. ESX Agent Manager

權限名稱	說明	要求
ESX Agent Manager.設定	允許在主機或叢集上部署代理程式虛擬機器。	虛擬機器
ESX Agent Manager.修改	允許修改代理程式虛擬機器，如關閉虛擬機器電源或刪除虛擬機器。	虛擬機器
ESX Agent View.檢視	允許檢視代理程式虛擬機器。	虛擬機器

延伸權限

延伸權限控制安裝和管理延伸的能力。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-11. 延伸權限

權限名稱	說明	要求
延伸.登錄延伸	允許延伸登錄 (外掛程式)。	根 vCenter Server
延伸.解除登錄延伸	允許取消登錄延伸 (外掛程式)。	根 vCenter Server
延伸.更新延伸	允許更新延伸 (外掛程式)。	根 vCenter Server

外部統計資料提供者權限

外部統計資料提供者權限可控制通知 vCenter Server 有關 Proactive Distributed Resource Scheduler (DRS) 統計資料的能力。

這些權限僅適用於 VMware 內部的 API。

資料夾權限

資料夾權限控制建立和管理資料夾的能力。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-12. 資料夾權限

權限名稱	說明	要求
資料夾.建立資料夾	允許建立新資料夾。	資料夾
資料夾.刪除資料夾	允許刪除資料夾。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	資料夾
資料夾.移動資料夾	允許移動資料夾。 權限必須同時存在於來源位置和目的地位置。	資料夾
資料夾.重新命名資料夾	允許變更資料夾的名稱。	資料夾

全域權限

全域權限控制與工作、指令碼和延伸相關的全域工作。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-13. 全域權限

權限名稱	說明	要求
全域.充當 vCenter Server	允許準備或啟動 vMotion 傳送作業或 vMotion 接收作業。	根 vCenter Server
全域.取消工作	允許取消執行中或已排入佇列的工作。	與工作相關的詳細目錄物件
全域.容量規劃	允許啟用容量規劃來規劃實體機器到虛擬機器的整併。	根 vCenter Server
全域.診斷	允許擷取診斷檔案、記錄檔標頭、二進位檔案或診斷服務包的清單。若要避免潛在的安全性缺口，請將此權限限制為 vCenter Server 管理員角色。	根 vCenter Server
全域.停用方法	允許 vCenter Server 延伸的伺服器對 vCenter Server 管理的物件停用某些作業。	根 vCenter Server
全域.啟用方法	允許 vCenter Server 延伸的伺服器對 vCenter Server 管理的物件啟用某些作業。	根 vCenter Server
全域.全域標籤	允許新增或移除全域標籤。	根主機或 vCenter Server
全域.健全狀況	允許檢視 vCenter Server 元件的健全狀況。	根 vCenter Server
全域.授權	允許檢視已安裝的授權並新增或移除授權。	根主機或 vCenter Server
全域.記錄事件	允許針對特定的受管理的實體記錄使用者定義的事件。	任何物件
全域.管理自訂屬性	允許新增、移除或重新命名自訂欄位定義。	根 vCenter Server
全域.Proxy	允許存取內部介面以將 Endpoint 新增至 Proxy 或從 Proxy 移除 Endpoint。	根 vCenter Server
全域.指令碼動作	允許排程與警示一起使用的指令碼動作。	任何物件
全域.服務管理員	允許在 vSphere CLI 中使用 `resxtop` 命令。	根主機或 vCenter Server
全域.設定自訂屬性	允許檢視、建立或移除受管理物件的自訂屬性。	任何物件
全域.設定	允許讀取並修改執行階段 vCenter Server 組態設定。	根 vCenter Server
全域.系統標籤	允許新增或移除系統標籤。	根 vCenter Server

健全狀況更新提供者權限

健全狀況更新提供者權限可控制硬體廠商通知 vCenter Server 有關 Proactive HA 事件的能力。

這些權限僅適用於 VMware 內部的 API。

主機 CIM 權限

主機 CIM 權限控制主機健全狀況監控的 CIM 使用。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-14. 主機 CIM 權限

權限名稱	說明	要求
主機.CIM.CIM 互動	允許用戶端取得用於 CIM 服務的票證。	主機

主機組態權限

主機組態權限控制設定主機的能力。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-15. 主機組態權限

權限名稱	說明	要求
主機.組態.進階設定	允許設定進階主機組態選項。	主機
主機.組態.驗證存放區	允許設定 Active Directory 驗證儲存。	主機
主機.組態.變更 PciPassthru 設定	允許變更主機的 PciPassthru 設定。	主機
主機.組態.變更 SNMP 設定	允許變更主機的 SNMP 設定。	主機
主機.組態.變更日期和時間設定	允許變更主機上的日期和時間設定。	主機
主機.組態.變更設定	允許在 ESXi 主機上設定鎖定模式。	主機
主機.組態.連線	允許變更主機的連線狀態 (連線或中斷連線)。	主機
主機.組態.韌體	允許更新 ESXi 主機的韌體。	主機
主機.組態.超執行緒	允許在主機 CPU 排程器中啟用和停用超執行緒。	主機
主機.組態.映像組態	允許變更與主機相關聯的映像。	
主機.組態.維護	允許使主機進入和退出維護模式，以及關閉和重新啟動主機。	主機
主機.組態.記憶體組態	允許修改主機組態。	主機
主機.組態.網路組態	允許設定網路、防火牆和 vMotion 網路。	主機
主機.組態.電源	允許設定主機電源管理設定。	主機
主機.組態.查詢修補程式	允許查詢可安裝的修補程序並將修補程序安裝在主機上。	主機
主機.組態.安全性設定檔和防火牆	允許設定網際網路服務 (如 SSH、Telnet、SNMP) 和主機防火牆。	主機
主機.組態.儲存區磁碟分割組態	允許管理 VMFS 資料存放區和診斷磁碟分割。具有此權限的使用者可以掃描新儲存裝置並管理 iSCSI。	主機

表格 13-15. 主機組態權限 (繼續)

權限名稱	說明	要求
主機.組態.系統管理	允許延伸，以操縱主機上的檔案系統。	主機
主機.組態.系統資源	允許更新系統資源階層的組態。	主機
主機.組態.虛擬機器自動啟動組態	允許變更單一主機上虛擬機器的自動啟動和自動停止順序。	主機

主機詳細目錄

主機詳細目錄權限控制向詳細目錄新增主機、向叢集新增主機以及在詳細目錄中移動主機等作業。

下表說明在詳細目錄中新增和移動主機和叢集所需的權限。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-16. 主機詳細目錄權限

權限名稱	說明	要求
主機.詳細目錄.新增主機至叢集	允許將主機新增到現有叢集。	叢集
主機.詳細目錄.新增獨立主機	允許新增獨立主機。	主機資料夾
主機.詳細目錄.建立叢集	允許建立新的叢集。	主機資料夾
主機.詳細目錄.修改叢集	允許變更叢集的內容。	叢集
主機.詳細目錄.移動叢集或獨立主機	允許在資料夾之間移動叢集或獨立主機。 權限必須同時存在於來源位置和目的地位置。	叢集
主機.詳細目錄.移動主機	允許將一組現有主機移入或移出叢集。 權限必須同時存在於來源位置和目的地位置。	叢集
主機.詳細目錄.移除叢集	允許刪除叢集或獨立主機。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	叢集、主機
主機.詳細目錄.移除主機	允許移除主機。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	主機加父系物件
主機.詳細目錄.重新命名叢集	允許重新命名叢集。	叢集

主機本機作業權限

當 VMware Host Client 直接連線到主機時執行的主機本機作業權限控制動作。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-17. 主機本機作業權限

權限名稱	說明	要求
主機.本機作業.新增主機至 vCenter	允許安裝和移除主機上的 vCenter 代理程式，如 vpxa 和 aam。	根主機
主機.本機作業.建立虛擬機器	允許在磁碟上從頭開始建立新的虛擬機器，而不在主機上登錄。	根主機
主機.本機作業.刪除虛擬機器	允許在磁碟上刪除虛擬機器。支援已登錄和解除登錄的虛擬機器。	根主機
主機.本機作業.管理使用者群組	允許在主機上管理本機帳戶。	根主機
主機.本機作業.重新設定虛擬機器	允許重新設定虛擬機器。	根主機

主機 vSphere Replication 權限

主機 vSphere Replication 權限控制 VMware vCenter Site Recovery Manager™ 對主機使用虛擬機器複寫的情況。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-18. 主機 vSphere Replication 權限

權限名稱	說明	要求
主機.vSphere Replication.管理複寫	允許管理此主機上的虛擬機器複寫。	主機

主機設定檔權限

主機設定檔權限可控制與建立和修改主機設定檔相關的作業。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-19. 主機設定檔權限

權限名稱	說明	要求
主機設定檔.清除	允許清除設定檔相關的資訊。	根 vCenter Server
主機設定檔.建立	允許建立主機設定檔。	根 vCenter Server
主機設定檔.刪除	允許刪除主機設定檔。	根 vCenter Server
主機設定檔.編輯	允許編輯主機設定檔。	根 vCenter Server
主機設定檔.匯出	允許匯出主機設定檔。	根 vCenter Server
主機設定檔.檢視	允許檢視主機設定檔。	根 vCenter Server

網路權限

網路權限控制與網路管理相關的工作。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-20. 網路權限

權限名稱	說明	要求
網路.指派網路	允許將網路指派到虛擬機器。	網路、虛擬機器
網路.設定	允許設定網路。	網路、虛擬機器
網路.移動網路	允許在資料夾之間移動網路。 權限必須同時存在於來源位置和目的地位置。	網路
網路.移除	允許移除網路。 此權限已被取代。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	網路

效能權限

效能權限可控制對效能統計資料設定的修改。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-21. 效能權限

權限名稱	說明	要求
效能.修改時間間隔	允許建立、移除和更新效能資料收集時間間隔。	根 vCenter Server

權限 (Permissions) 權限

權限 (Permissions) 權限控制角色和權限的指派。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-22. 權限 (Permissions) 權限

權限名稱	說明	要求
權限.修改權限	允許在實體上定義一或多個權限規則，或者如果實體上的特定使用者或群組已有規則，則更新規則。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	任何物件加父系物件
權限.修改權限	允許修改權限的群組或說明。 沒有與此權限相關聯的 vSphere Web Client 使用者介面元素。	
權限.修改角色	允許更新某個角色的名稱以及與該角色相關聯的權限。	任何物件
權限.重新指派角色權限	允許將某個角色的所有權限重新指派給另一個角色。	任何物件

Profile-Driven Storage 權限

Profile-Driven Storage 權限控制與儲存區設定檔相關的作業。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-23. Profile-Driven Storage 權限

權限名稱	說明	要求
Profile-Driven Storage.Profile-Driven Storage 更新	允許對儲存區設定檔做出變更，如建立和更新儲存區功能和虛擬機器儲存區設定檔。	根 vCenter Server
Profile-Driven Storage.Profile-Driven Storage 視圖	允許檢視定義的儲存區功能和儲存區設定檔。	根 vCenter Server

資源權限

資源權限控制資源集區的建立和管理，以及虛擬機器的移轉。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-24. 資源權限

權限名稱	說明	要求
資源.套用建議	允許接受伺服器提供的建議，以運用 vMotion 進行移轉。	叢集
資源.將 vApp 指派給資源集區	允許將 vApp 指派到資源集區。	資源集區
資源.將虛擬機器指派給資源集區	允許將虛擬機器指派到資源集區。	資源集區
資源.建立資源集區	允許建立資源集區。	資源集區, 叢集
資源.移轉已關閉電源的虛擬機器	允許將已關閉電源的虛擬機器移轉到不同的資源集區或主機。	虛擬機器

表格 13-24. 資源權限 (繼續)

權限名稱	說明	要求
資源.移轉已開啟電源的虛擬機器	允許運用 vMotion 將已開啟電源的虛擬機器移轉到不同的資源集區或主機。	
資源.修改資源集區	允許變更資源集區的配置。	資源集區
資源.移動資源集區	允許移動資源集區。 權限必須同時存在於來源位置和目的地位置。	資源集區
資源.查詢 vMotion	允許查詢虛擬機器與一組主機的一般 vMotion 相容性。	根 vCenter Server
資源.移除資源集區	允許刪除資源集區。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	資源集區
資源.重新命名資源集區	允許重新命名資源集區。	資源集區

排定的工作權限

排定的工作權限控制排定的工作的建立、編輯和移除。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-25. 排定的工作權限

權限名稱	說明	要求
排定的工作.建立工作	允許排定工作。在排定時，需要一定的權限來執行已排定的動作。	任何物件
排定的工作.修改工作	允許重新設定排定的工作的內容。	任何物件
排定的工作.移除工作	允許移除佇列中排定的工作。	任何物件
排定的工作.執行工作	允許立即執行排定的工作。 建立和執行排定的工作也需要執行關聯動作的權限。	任何物件

工作階段權限

工作階段權限控制延伸開啟 vCenter Server 系統上的工作階段的能力。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-26. 工作階段權限

權限名稱	說明	要求
工作階段.模擬使用者	允許模擬其他使用者。該功能由延伸使用。	根 vCenter Server
工作階段.訊息	允許設定全域登入訊息。	根 vCenter Server

表格 13-26. 工作階段權限 (繼續)

權限名稱	說明	要求
工作階段.驗證工作階段	允許驗證工作階段有效性。	根 vCenter Server
工作階段.檢視和停止工作階段	允許檢視工作階段和強制登出一或多個已登入的使用者。	根 vCenter Server

儲存區視圖權限

儲存區視圖權限控制儲存區監控服務 API 的權限。從 vSphere 6.0 開始，儲存區視圖會被取代，這些權限不再適用於它們。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-27. 儲存區視圖權限

權限名稱	說明	要求
儲存區視圖.設定服務	允許有特殊權限的使用者使用所有儲存區監控服務 API。將 **儲存區視圖.檢視** 用於儲存區監控服務 API 的唯讀權限。	根 vCenter Server
儲存區視圖.檢視	允許有特殊權限的使用者使用唯讀儲存區監控服務 API。	根 vCenter Server

工作權限

工作權限控制延伸在 vCenter Server 上建立和更新工作的能力。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-28. 工作權限

權限名稱	說明	要求
工作.建立工作	允許延伸建立使用者定義的工作。 沒有與此權限相關聯的 vSphere Web Client 使用者介面元素。	根 vCenter Server
工作.更新工作	允許延伸更新使用者定義的工作。 沒有與此權限相關聯的 vSphere Web Client 使用者介面元素。	根 vCenter Server

Transfer Service 權限

Transfer Service 權限為 VMware 內部權限。請勿使用這些權限。

虛擬機器組態權限

虛擬機器組態權限可控制設定虛擬機器選項和裝置的能力。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-29. 虛擬機器組態權限

權限名稱	說明	要求
虛擬機器.組態.新增現有磁碟	允許將現有的虛擬磁碟新增到虛擬機器。	虛擬機器
虛擬機器.組態.新增磁碟	允許建立要新增到虛擬機器的新虛擬磁碟。	虛擬機器
虛擬機器.組態.新增或移除裝置	允許新增或移除任何非磁碟裝置。	虛擬機器
虛擬機器.組態.進階	允許在虛擬機器的組態檔中新增或修改進階參數。	虛擬機器
虛擬機器.組態.變更 CPU 計數	允許變更虛擬 CPU 的數目。	虛擬機器
虛擬機器.組態.變更資源	允許在特定資源集區中變更一組虛擬機器節點的資源組態。	虛擬機器
虛擬機器.組態.設定 managedBy	允許延伸或解決方案將虛擬機器標記為由該延伸或解決方案管理。	虛擬機器
虛擬機器.組態.磁碟變更追蹤	允許啟用或停用虛擬機器的磁碟變更追蹤。	虛擬機器
虛擬機器.組態.磁碟租用	允許對虛擬機器執行磁碟租用作業。	虛擬機器
虛擬機器.組態.顯示連線設定	允許設定虛擬機器遠端主控台選項。	虛擬機器
虛擬機器.組態.擴充虛擬磁碟	允許擴充虛擬磁碟的大小。	虛擬機器
虛擬機器.組態.主機 USB 裝置	允許將主機式 USB 裝置連結到虛擬機器。	虛擬機器
虛擬機器.組態.記憶體	允許變更配置給虛擬機器的記憶體數量。	虛擬機器
虛擬機器.組態.修改裝置設定	允許變更現有裝置的內容。	虛擬機器
虛擬機器.組態.查詢 Fault Tolerance 相容性	允許檢查虛擬機器是否相容於 Fault Tolerance。	虛擬機器
虛擬機器.組態.查詢無人負責的檔案	允許查詢無人負責的檔案。	虛擬機器
虛擬機器.組態.原始裝置	允許新增或移除原始磁碟對應或 SCSI 傳遞裝置。 設定此參數會覆寫可用於修改原始裝置 (包括連線狀態) 的任何其他權限。	虛擬機器

表格 13-29. 虛擬機器組態權限 (繼續)

權限名稱	說明	要求
虛擬機器.組態.從路徑重新載入	允許變更虛擬機器組態路徑，同時保留虛擬機器的身分識別。諸如 VMware vCenter Site Recovery Manager 等解決方案使用此作業，在容錯移轉和容錯回復期間保留虛擬機器的身分識別。	虛擬機器
虛擬機器.組態.移除磁碟	允許移除虛擬磁碟裝置。	虛擬機器
虛擬機器.組態.重新命名	允許重新命名虛擬機器或修改虛擬機器的關聯說明。	虛擬機器
虛擬機器.組態.重設客體資訊	允許編輯虛擬機器的客體作業系統資訊。	虛擬機器
虛擬機器.組態.設定註解	允許新增或編輯虛擬機器註釋。	虛擬機器
虛擬機器.組態.設定	允許變更一般虛擬機器設定。	虛擬機器
虛擬機器.組態.分頁檔放置位置	允許變更虛擬機器的分頁檔放置原則。	虛擬機器
虛擬機器.組態.切換分支父系		
虛擬機器.組態.升級虛擬機器相容性	允許升級虛擬機器的虛擬機器相容性版本。	虛擬機器

虛擬機器客體作業權限

虛擬機器客體作業權限控制在虛擬機器的客體作業系統內部使用 API 與檔案和程式互動的能力。

如需這些作業的詳細資訊，請參閱《*VMware vSphere API 參考*》說明文件。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-30. 虛擬機器客體作業

權限名稱	說明	生效物件
虛擬機器.客體作業.客體作業別名修改	允許修改虛擬機器別名的虛擬機器客體作業。	虛擬機器
虛擬機器.客體作業.客體作業別名查詢	允許查詢虛擬機器別名的虛擬機器客體作業。	虛擬機器
虛擬機器.客體作業.客體作業修改	允許在虛擬機器中對客體作業系統進行修改的虛擬機器客體作業，如向虛擬機器傳輸檔案。 沒有與此權限相關聯的 vSphere Web Client 使用者介面元素。	虛擬機器

表格 13-30. 虛擬機器客體作業 (繼續)

權限名稱	說明	生效物件
虛擬機器.客體作業.客體作業程式執行	允許在虛擬機器中執行程式的虛擬機器客體作業。 沒有與此權限相關聯的 vSphere Web Client 使用者介面元素。	虛擬機器
虛擬機器.客體作業.客體作業查詢	允許對客體作業系統進行查詢的虛擬機器客體作業，如在客體作業系統中列出檔案。 沒有與此權限相關聯的 vSphere Web Client 使用者介面元素。	虛擬機器

虛擬機器互動權限

虛擬機器互動權限控制與虛擬機器主控台互動、設定媒體、執行電源作業和安裝 VMware Tools 的能力。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-31. 虛擬機器互動

權限名稱	說明	要求
虛擬機器.互動.回答問題	允許解決虛擬機器狀態轉換的問題或執行階段錯誤。	虛擬機器
虛擬機器.互動.虛擬機器上的備份作業	允許對虛擬機器執行備份作業。	虛擬機器
虛擬機器.互動.設定 CD 媒體	允許設定虛擬 DVD 或 CD-ROM 裝置。	虛擬機器
虛擬機器.互動.設定磁碟片媒體	允許設定虛擬磁碟片裝置。	虛擬機器

表格 13-31. 虛擬機器互動 (繼續)

權限名稱	說明	要求
虛擬機器.互動.主控台互動	允許與虛擬機器的虛擬滑鼠、鍵盤和螢幕互動。	虛擬機器
虛擬機器.互動.建立螢幕擷取畫面	允許建立虛擬機器螢幕快照。	虛擬機器
虛擬機器.互動.重組所有磁碟	允許對虛擬機器上的所有磁碟執行碎片重組作業。	虛擬機器
虛擬機器.互動.裝置連線	允許變更虛擬機器可斷開連線的虛擬裝置的連線狀態。	虛擬機器
虛擬機器.互動.拖放	允許在虛擬機器與遠端用戶端之間拖放檔案。	虛擬機器
虛擬機器.互動.透過 VIX API 管理客體作業系統	允許透過 VIX API 管理虛擬機器的作業系統。	虛擬機器
虛擬機器.互動.插入 USB HID 掃描碼	允許插入 USB HID 掃描碼。	虛擬機器

表格 13-31. 虛擬機器互動 (繼續)

權限名稱	說明	要求
虛擬機器.互動.暫停或取消暫停	允許暫停或取消暫停虛擬機器。	虛擬機器
虛擬機器.互動.執行抹除或壓縮作業	允許對虛擬機器執行抹除或壓縮作業。	虛擬機器
虛擬機器.互動.關閉電源	允許關閉已開啟電源的虛擬機器的電源。此作業將關閉客體作業系統的電源。	虛擬機器
虛擬機器.互動.開啟電源	允許開啟已關閉電源的虛擬機器的電源，以及繼續暫停的虛擬機器。	虛擬機器
虛擬機器.互動.記錄虛擬機器上的工作階段	允許記錄虛擬機器上的工作階段。	虛擬機器
虛擬機器.互動.重新執行虛擬機器上的工作階段	允許重新執行虛擬機器上已記錄的工作階段。	虛擬機器

表格 13-31. 虛擬機器互動 (繼續)

權限名稱	說明	要求
虛擬機器.互動.重設	允許重設虛擬機器並重新開機客體作業系統。	虛擬機器
虛擬機器.互動.繼續 Fault Tolerance	允許繼續執行虛擬機器的 Fault Tolerance 功能。	虛擬機器
虛擬機器.互動.暫停	允許暫停已開啟電源的虛擬機器。此作業將客體置於待命模式。	虛擬機器
虛擬機器.互動.暫停 Fault Tolerance	允許暫停虛擬機器的 Fault Tolerance 功能。	虛擬機器
虛擬機器.互動.測試容錯移轉	允許透過使次要虛擬機器成為主要虛擬機器，來測試 Fault Tolerance 容錯移轉。	虛擬機器

表格 13-31. 虛擬機器互動 (繼續)

權限名稱	說明	要求
虛擬機器.互動.測試重新啟動次要虛擬機器	允許終止使用 Fault Tolerance 的虛擬機器的次要虛擬機器。	虛擬機器
虛擬機器.互動.關閉 Fault Tolerance	允許關閉虛擬機器的 Fault Tolerance 功能。	虛擬機器
虛擬機器.互動.開啟 Fault Tolerance	允許開啟虛擬機器的 Fault Tolerance 功能。	虛擬機器
虛擬機器.互動 .VMware Tools 安裝	允許以 CD-ROM 形式為客體作業系統掛接和卸載 VMware Tools CD 安裝程式。	虛擬機器

虛擬機器詳細目錄權限

虛擬機器詳細目錄權限控制虛擬機器的新增、移動和移除。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-32. 虛擬機器詳細目錄權限

權限名稱	說明	要求
虛擬機器.詳細目錄.從現有項目建立	允許透過從範本複製或部署，以現有虛擬機器或範本為基礎建立虛擬機器。	叢集、主機、虛擬機器資料夾
虛擬機器.詳細目錄.新建	允許建立虛擬機器並為其執行配置資源。	叢集、主機、虛擬機器資料夾
虛擬機器.詳細目錄.移動	允許在階層中重新放置虛擬機器。 權限必須同時存在於來源位置和目的地位置。	虛擬機器
虛擬機器.詳細目錄.登錄	允許將現有虛擬機器新增到 vCenter Server 或主機詳細目錄。	叢集、主機、虛擬機器資料夾
虛擬機器.詳細目錄.移除	允許刪除虛擬機器。移除動作將從磁碟移除虛擬機器的基礎檔案。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	虛擬機器
虛擬機器.詳細目錄.解除登錄	允許從 vCenter Server 或主機詳細目錄中解除登錄虛擬機器。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	虛擬機器

虛擬機器佈建權限

虛擬機器佈建權限控制與部署和自訂虛擬機器相關的活動。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-33. 虛擬機器佈建權限

權限名稱	說明	要求
虛擬機器.佈建.允許磁碟存取	允許開啟虛擬機器上的磁碟，進行隨機的讀取和寫入權限。常用於遠端磁碟掛接。	虛擬機器
虛擬機器.佈建.允許檔案存取	允許在與虛擬機器關聯的檔案上執行作業，包括 vmx、磁碟、記錄和 nvram。	虛擬機器
虛擬機器.佈建.允許唯讀磁碟存取	允許開啟虛擬機器上的磁碟，進行隨機讀取存取。常用於遠端磁碟掛接。	虛擬機器
虛擬機器.佈建.允許虛擬機器下載	允許在與虛擬機器關聯的檔案上執行讀取作業，包括 vmx、磁碟、記錄和 nvram。	根主機或 vCenter Server
虛擬機器.佈建.允許虛擬機器檔案上傳	允許在與虛擬機器關聯的檔案上執行寫入作業，包括 vmx、磁碟、記錄和 nvram。	根主機或 vCenter Server
虛擬機器.佈建.複製範本	允許複製範本。	範本
虛擬機器.佈建.複製虛擬機器	允許複製現有的虛擬機器和配置資源。	虛擬機器
虛擬機器.佈建.從虛擬機器建立範本	允許從虛擬機器建立新範本。	虛擬機器
虛擬機器.佈建.自訂	允許自訂虛擬機器的客體作業系統，而不移動虛擬機器。	虛擬機器
虛擬機器.佈建.部署範本	允許從範本部署虛擬機器。	範本

表格 13-33. 虛擬機器佈建權限 (繼續)

權限名稱	說明	要求
虛擬機器.佈建.標記為範本	允許將現有已關閉電源的虛擬機器標記為範本。	虛擬機器
虛擬機器.佈建.標記為虛擬機器	允許將現有範本標記為虛擬機器。	範本
虛擬機器.佈建.修改自訂規格	允許建立、修改或刪除自訂規格。	根 vCenter Server
虛擬機器.佈建.升階磁碟	允許對虛擬機器的磁碟進行升階作業。	虛擬機器
虛擬機器.佈建.讀取自訂規格	允許讀取自訂規格。	虛擬機器

虛擬機器服務組態權限

虛擬機器服務組態權限控制可以對服務組態執行監控和管理工作的使用者。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

備註 在 vSphere 6.0 中，請勿使用 vSphere Web Client 指派或移除此權限。

表格 13-34. 虛擬機器服務組態權限

權限名稱	說明
虛擬機器.服務組態.允許通知	允許產生和使用有關服務狀態的通知。
虛擬機器.服務組態.允許輪詢全域事件通知	允許查詢是否存在任何通知。
虛擬機器.服務組態.管理服務組態	允許建立、修改和刪除虛擬機器服務。
虛擬機器.服務組態.修改服務組態	允許修改現有的虛擬機器服務組態。
虛擬機器.服務組態.查詢服務組態	允許擷取虛擬機器服務清單。
虛擬機器.服務組態.讀取服務組態	允許擷取現有的虛擬機器服務組態。

虛擬機器快照管理權限

虛擬機器快照管理權限控制執行、刪除、重新命名和還原快照的功能。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-35. 虛擬機器狀態權限

權限名稱	說明	要求
虛擬機器.快照管理.建立快照	允許按照虛擬機器的目前狀態建立快照。	虛擬機器
虛擬機器.快照管理.移除快照	允許從快照歷程記錄移除快照。	虛擬機器

表格 13-35. 虛擬機器狀態權限 (繼續)

權限名稱	說明	要求
虛擬機器.快照管理.重新命名快照	允許使用新的名稱、新的說明或兩者都使用以重新命名快照。	虛擬機器
虛擬機器.快照管理.還原為快照	允許將虛擬機器設定為在指定快照中所處的狀態。	虛擬機器

虛擬機器 vSphere Replication 權限

虛擬機器 vSphere Replication 權限控制 VMware vCenter Site Recovery Manager™ 對虛擬機器使用複寫的情況。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-36. 虛擬機器 vSphere Replication

權限名稱	說明	要求
虛擬機器.vSphere Replication.設定複寫	允許對虛擬機器進行複寫設定。	虛擬機器
虛擬機器.vSphere Replication.管理複寫	允許在複寫時觸發完整同步、線上同步或離線同步。	虛擬機器
虛擬機器.vSphere Replication.監控複寫	允許監控複寫。	虛擬機器

dvPort 群組權限

分散式虛擬連接埠群組權限控制建立、刪除和修改分散式虛擬連接埠群組的能力。

下表說明建立和設定分散式虛擬連接埠群組所需的權限。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-37. 分散式虛擬連接埠群組權限

權限名稱	說明	要求
dvPort 群組.建立	允許建立分散式虛擬連接埠群組。	虛擬連接埠群組
dvPort 群組.刪除	允許刪除分散式虛擬連接埠群組。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	虛擬連接埠群組
dvPort 群組.修改	允許修改分散式虛擬連接埠群組的組態。	虛擬連接埠群組
dvPort 群組.原則作業	允許設定分散式虛擬連接埠群組的原則。	虛擬連接埠群組
dvPort 群組.範圍作業	允許設定分散式虛擬連接埠群組的範圍。	虛擬連接埠群組

vApp 權限

vApp 權限控制與部署和設定 vApp 相關的作業。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-38. vApp 權限

權限名稱	說明	要求
vApp.新增虛擬機器	允許將虛擬機器新增到 vApp。	vApp
vApp.指派資源集區	允許將資源集區指派到 vApp。	vApp
vApp.指派 vApp	允許將一個 vApp 指派給另一個 vApp	vApp
vApp.複製	允許複製 vApp。	vApp
vApp.建立	允許建立 vApp。	vApp
vApp.刪除	允許刪除 vApp。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	vApp
vApp.匯出	允許從 vSphere 匯出 vApp。	vApp
vApp.匯入	允許將 vApp 匯入 vSphere。	vApp
vApp.移動	允許將 vApp 移動到新詳細目錄位置。	vApp
vApp.關閉電源	允許對 vApp 執行關閉電源作業。	vApp
vApp.開啟電源	允許對 vApp 執行開啟電源作業。	vApp
vApp.重新命名	允許重新命名 vApp。	vApp
vApp.暫停	允許暫停 vApp。	vApp
vApp.解除登錄	允許取消登錄 vApp。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	vApp
vApp.檢視 OVF 環境	允許在 vApp 中檢視已開啟電源的虛擬機器的 OVF 環境。	vApp
vApp.vApp 應用程式組態	允許修改 vApp 的內部結構，如產品資訊和內容。	vApp
vApp.vApp 執行個體組態	允許修改 vApp 的執行個體組態，如原則。	vApp
vApp.vApp managedBy 組態	允許延伸或解決方案將 vApp 標記為由該延伸或解決方案來管理。 沒有與此權限相關聯的 vSphere Web Client 使用者介面元素。	vApp
vApp.vApp 資源組態	允許修改 vApp 的資源組態。 若想擁有執行此作業的權限，使用者或群組必須將此權限指派給物件及其父系物件。	vApp

vServices 權限

vService 權限可控制建立、設定和更新虛擬機器與 vApp 之 vService 相依性的功能。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-39. vService

權限名稱	說明	要求
vService.建立相依性	允許建立虛擬機器或 vApp 的 vService 相依性。	vApp 和虛擬機器
vService.終結相依性	允許移除虛擬機器或 vApp 的 vService 相依性。	vApp 和虛擬機器
vService.重新設定相依性組態	允許重新設定相依性以更新提供者或繫結。	vApp 和虛擬機器
vService.更新相依性	允許更新相依性以設定名稱或說明。	vApp 和虛擬機器

vSphere 標記權限

vSphere 標記權限控制在 vCenter Server 詳細目錄物件上建立、刪除標籤與標籤類別，以及指派和移除標籤的能力。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表格 13-40. vSphere 標記權限

權限名稱	說明	要求
vSphere 標記.指派或取消指派 vSphere 標籤	允許對 vCenter Server 詳細目錄中的物件指派標籤或取消指派標籤。	任何物件
vSphere 標記.建立 vSphere 標籤	允許建立標籤。	任何物件
vSphere 標記.建立 vSphere 標籤類別	允許建立標籤類別。	任何物件
vSphere 標記.建立 vSphere 標籤範圍	允許建立標籤範圍。	任何物件
vSphere 標記.刪除 vSphere 標籤	允許刪除標籤類別。	任何物件
vSphere 標記.刪除 vSphere 標籤類別	允許刪除標籤類別。	任何物件
vSphere 標記.刪除 vSphere 標籤範圍	允許刪除標籤範圍。	任何物件
vSphere 標記.編輯 vSphere 標籤	允許編輯標籤。	任何物件
vSphere 標記.編輯 vSphere 標籤類別	允許編輯標籤類別。	任何物件
vSphere 標記.編輯 vSphere 標籤範圍	允許編輯標籤範圍。	任何物件
vSphere 標記.修改類別的 UsedBy 欄位	允許變更標籤類別的 UsedBy 欄位。	任何物件
vSphere 標記.修改標籤的 UsedBy 欄位	允許變更標籤的 UsedBy 欄位。	任何物件