

vSphere 安全性

Update 2

修改日期：2022 年 4 月 27 日

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

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

Copyright © 2009-2022 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

目錄

關於 vSphere 安全性 13

更新資訊 15

1 vSphere 環境中的安全性 17

保護 ESXi Hypervisor 17

保護 vCenter Server 系統和相關聯服務的安全 19

確保虛擬機器安全 20

保護虛擬網路層的安全 20

vSphere 環境中的密碼 22

安全性最佳做法和資源 23

2 使用 vCenter Single Sign-On 進行 vSphere 驗證 24

瞭解 vCenter Single Sign-On 25

如何使用 vCenter Single Sign-On 保護您的環境 25

vCenter Single Sign-On 元件 27

vCenter Single Sign-On 如何影響安裝 27

vCenter Single Sign-On 如何影響升級 28

將 vCenter Single Sign-On 與 vSphere 搭配使用 30

vsphere.local 網域中的群組 32

vCenter Server 密碼需求與鎖定行為 33

設定 vCenter Single Sign-On 身分識別來源 34

具有 vCenter Single Sign-On 的 vCenter Server 的身分識別來源 35

設定 vCenter Single Sign-On 的預設網域 36

新增 vCenter Single Sign-On 身分識別來源 36

Active Directory 身分識別來源設定 38

Active Directory LDAP Server 和 OpenLDAP Server 身分識別來源設定 39

編輯 vCenter Single Sign-On 身分識別來源 40

移除 vCenter Single Sign-On 身分識別來源 40

使用 vCenter Single Sign-On 進行 Windows 工作階段驗證 41

vCenter Server 雙因素驗證 41

設定用於 vCenter Single Sign-On 的智慧卡驗證 42

使用命令列設定智慧卡驗證 43

使用 Platform Services Controller Web 介面管理智慧卡驗證 46

設定智慧卡驗證的撤銷原則 48

設定 RSA SecurID 驗證 50

管理登入橫幅 52

針對其他服務提供者將 vCenter Single Sign-On 用做身分識別提供者	52
新增 SAML 服務提供者	53
安全性 Token 服務 STS	54
在應用裝置上產生新的 STS 簽署憑證	55
在 vCenter Windows 安裝上產生新 STS 簽署憑證	56
重新整理安全性 Token 服務憑證	58
判定 LDAPS SSL 憑證的到期日期	59
管理 vCenter Single Sign-On 原則	59
編輯 vCenter Single Sign-On 密碼原則	59
編輯 vCenter Single Sign-On 鎖定原則	60
編輯 vCenter Single Sign-On Token 原則	61
管理 vCenter Single Sign-On 使用者和群組	62
新增 vCenter Single Sign-On 使用者	63
停用和啟用 vCenter Single Sign-On 使用者	64
刪除 vCenter Single Sign-On 使用者	64
編輯 vCenter Single Sign-On 使用者	64
新增 vCenter Single Sign-On 群組	65
向 vCenter Single Sign-On 群組新增成員	66
從 vCenter Single Sign-On 群組中移除成員	66
刪除 vCenter Single Sign-On 解決方案使用者	67
變更 vCenter Single Sign-On 密碼	67
vCenter Single Sign-On 安全性最佳做法	68
vCenter Single Sign-On 疑難排解	68
判定 Lookup Service 錯誤的原因	68
無法使用 Active Directory 網域驗證登入	70
由於使用者帳戶被鎖定，vCenter Server 登入失敗	71
VMware 目錄服務複寫可能需要很長時間	71

3 vSphere 安全性憑證 73

不同解決方案路徑的憑證需求	74
憑證管理概觀	77
憑證取代概觀	79
vSphere 6.0 使用憑證所在位置	81
VMCA 和 VMware Core Identity Services	83
VMware Endpoint 憑證存放區概觀	83
管理憑證撤銷	85
大型部署中的憑證取代	85
使用 Platform Services Controller Web 介面管理憑證	87
從 Platform Services Controller Web 介面深入瞭解憑證存放區	87
從 Platform Services Controller Web 介面將憑證取代為新的 VMCA 簽署憑證	88
在 Platform Services Controller Web 介面中使 VMCA 成為中繼憑證授權機構	90

從 Platform Services Controller 將您的系統設定為使用自訂憑證	91
使用 vSphere Certificate Manager 產生憑證簽署要求 (自訂憑證)	91
將受信任的根憑證新增至憑證存放區	92
從 Platform Services Controller 新增自訂憑證	93
透過 vSphere Certificate Manager 公用程式管理憑證	94
重新發佈舊憑證以還原最後執行的作業	95
重設所有憑證	95
重新產生新的 VMCA 根憑證並取代所有憑證	96
使 VMCA 成為中繼憑證授權機構 (Certificate Manager)	97
使用 vSphere Certificate Manager 產生 CSR 並準備根憑證 (中繼 CA)	97
將 VMCA 根憑證取代為自訂簽署憑證並取代所有憑證	98
將機器 SSL 憑證取代為 VMCA 憑證 (中繼 CA)	99
將解決方案使用者憑證取代為 VMCA 憑證 (中繼 CA)	100
用自訂憑證取代所有憑證 (Certificate Manager)	101
使用 vSphere Certificate Manager 產生憑證簽署要求 (自訂憑證)	101
將機器 SSL 憑證取代為自訂憑證	102
將解決方案使用者憑證取代為自訂憑證	103
手動憑證取代	104
瞭解啟動和停止服務	104
用新的 VMCA 簽署憑證取代現有的 VMCA 簽署憑證	105
產生新的 VMCA 簽署根憑證	105
用 VMCA 簽署憑證取代機器 SSL 憑證	107
用新的 VMCA 簽署憑證取代解決方案使用者憑證	110
在混合模式環境中取代 VMware Directory Service 憑證	115
使用 VMCA 做為中繼憑證授權機構	116
取代根憑證 (中繼 CA)	117
取代機器 SSL 憑證 (中繼 CA)	119
取代解決方案使用者憑證 (中繼 CA)	122
取代 VMware 目錄服務憑證	127
在混合模式環境中取代 VMware Directory Service 憑證	128
將第三方憑證與 vSphere 搭配使用	129
要求憑證及匯入自訂根憑證	130
將機器 SSL 憑證取代為自訂憑證	131
將解決方案使用者憑證取代為自訂憑證	133
取代 VMware 目錄服務憑證	135
在混合模式環境中取代 VMware Directory Service 憑證	136
使用 CLI 命令管理憑證和服務	137
進行憑證管理作業所需的權限	137
變更 certool 組態	138
certool 初始化命令參考	139
certool 管理命令參考	142

vecs-cli 命令參考 144

dir-cli 命令參考 147

使用 vSphere Web Client 檢視 vCenter 憑證 152

設定 vCenter 憑證到期警告臨界值 152

4 vSphere 權限和使用者管理工作 154

瞭解 vSphere 中的授權 155

瞭解 vCenter Server 權限模型 155

權限的階層式繼承 157

多個權限設定 159

範例 1：多個權限繼承 160

範例 2：子權限覆寫父系權限 160

範例 3：使用者角色覆寫群組角色 161

管理 vCenter 元件的權限 161

將權限新增到詳細目錄物件 162

變更權限 163

移除權限 163

變更權限驗證設定 163

全域權限 164

新增全域權限 165

標籤物件的權限 165

使用角色指派權限 167

vCenter Server 系統角色 168

建立自訂角色 168

複製角色 169

編輯角色 169

針對角色和權限的最佳做法 170

一般工作所需的權限 170

5 保護 ESXi 主機 173

使用指令碼管理主機組態設定 174

利用主機設定檔設定 ESXi 主機 175

ESXi 一般安全建議 176

ESXi 密碼及帳戶鎖定 177

ESXi 網路安全性建議 179

停用受管理物件瀏覽器 (MOB) 179

停用授權 (SSH) 金鑰 179

ESXi 主機的憑證管理 180

主機升級和憑證 182

ESXi 憑證的預設設定 182

檢視多個 ESXi 主機的憑證到期資訊 183

檢視單一 ESXi 主機的憑證詳細資料	184
更新或重新整理 ESXi 憑證	185
變更憑證預設設定	186
瞭解憑證模式切換	186
變更憑證模式	188
取代 ESXi SSL 憑證和金鑰	188
ESXi 憑證簽署要求的需求	189
取代 ESXi Shell 中的預設憑證和金鑰	189
使用 vifs 命令取代預設憑證和金鑰	190
使用 HTTPS PUT 取代預設憑證	191
更新 vCenter Server TRUSTED_ROOTS 存放區 (自訂憑證)	191
透過 Auto Deploy 使用自訂憑證	192
還原 ESXi 憑證和金鑰檔案	194
透過安全性設定檔自訂主機	194
ESXi 防火牆組態	195
管理 ESXi 防火牆設定	195
為 ESXi 主機新增允許的 IP 位址	196
ESXi 主機的傳入和傳出防火牆連接埠	197
NFS 用戶端防火牆行為	199
ESXi ESXCLI 防火牆命令	199
透過安全性設定檔自訂 ESXi 服務	200
啟用或停用安全性設定檔中的服務	201
鎖定模式	202
鎖定模式行為	203
使用 vSphere Web Client 啟用鎖定模式	205
使用 vSphere Web Client 停用鎖定模式	205
從 Direct Console 使用者介面啟用或停用一般鎖定模式	206
指定在鎖定模式下具有存取權限的帳戶	206
檢查主機和 VIB 的接受程度	208
為 ESXi 指派權限	209
根使用者權限	210
vpxuser 權限	210
DCUI 使用者權限	210
使用 Active Directory 管理 ESXi 使用者	211
安裝或升級 vSphere Authentication Proxy	211
將主機設定為使用 Active Directory	212
將主機新增至目錄服務網域	213
檢視目錄服務設定	213
使用 vSphere Authentication Proxy	214
安裝或升級 vSphere Authentication Proxy	214
設定主機以使用 vSphere Authentication Proxy 進行驗證	215

設定 vSphere Authentication Proxy	216
匯出 vSphere Authentication Proxy 憑證	216
將 Proxy 伺服器憑證匯入到 ESXi	217
使用 vSphere Authentication Proxy 將主機新增到網域	218
取代 ESXi 主機的 Authentication Proxy 憑證	218
ESXi 安全性最佳做法	219
PCI 和 PCIe 裝置和 ESXi	220
設定用於 ESXi 的智慧卡驗證	220
啟用智慧卡驗證	221
停用智慧卡驗證	221
在發生連線問題的情況下驗證使用者認證	221
在鎖定模式下使用智慧卡驗證	222
ESXi SSH 金鑰	222
SSH 安全性	222
使用 vifs 命令上傳 SSH 金鑰	223
使用 HTTPS PUT 上傳 SSH 金鑰	223
使用 ESXi Shell	224
使用 vSphere Web Client 啟用對 ESXi Shell 的存取	225
在 vSphere Web Client 中為 ESXi Shell 可用性建立逾時	226
在 vSphere Web Client 中為閒置的 ESXi Shell 工作階段建立逾時	226
使用 Direct Console 使用者介面 (DCUI) 啟用對 ESXi Shell 的存取	227
在 Direct Console 使用者介面中為 ESXi Shell 可用性建立逾時	227
為閒置 ESXi Shell 工作階段建立逾時	228
登入 ESXi Shell 進行疑難排解	228
修改 ESXi Web 代理設定	228
vSphere Auto Deploy 安全考量	229
管理 ESXi 記錄檔	229
在 ESXi 主機上設定 Syslog	230
ESXi 記錄檔位置	231
確保 Fault Tolerance 記錄流量的安全	231

6 保護 vCenter Server 系統的安全 232

vCenter Server 安全性最佳做法	232
vCenter Server 存取控制的最佳做法	232
設定 vCenter Server 密碼原則	234
保護 vCenter Server Windows 主機	234
從失敗的安裝移除到期或撤銷的憑證和記錄	234
限制 vCenter Server 的網路連線	235
考慮限制 Linux 用戶端的使用	235
檢查已安裝的外掛程式	236
vCenter Server Appliance 安全性最佳做法	236

- 驗證舊版 ESXi 主機的指紋 236
- 確認已對網路檔案複製啟用 SSL 憑證驗證 237
- vCenter Server TCP 和 UDP 連接埠 238
- 控制以 CIM 為基礎的硬體監控工具存取 239

7 確保虛擬機器安全 241

- 限制資訊訊息從虛擬機器流向 VMX 檔案 241
- 防止虛擬磁碟壓縮 242
- 虛擬機器安全性最佳做法 242
 - 虛擬機器一般保護 243
 - 使用範本部署虛擬機器 243
 - 儘量少用虛擬機器主控台 244
 - 防止虛擬機器接管資源 244
 - 停用虛擬機器中不必要的功能 245
 - 移除不必要的硬體裝置 245
 - 停用未使用的顯示功能 246
 - 停用未公開的功能 246
 - 停用 HGFS 檔案傳輸 247
 - 停用客體作業系統和遠端主控台之間的複製和貼上作業 247
 - 限制曝光複製到剪貼簿中的敏感資料 248
 - 限制使用者在虛擬機器中執行命令 248
 - 防止虛擬機器使用者或程序中斷裝置的連線 249
 - 修改客體作業系統的可變記憶體限制 249
 - 阻止客體作業系統程序向主機傳送組態訊息 250
 - 避免使用獨立非持續性磁碟 250

8 確保 vSphere 網路安全 252

- vSphere 網路安全性簡介 252
- 使用防火牆確保網路安全 253
 - 針對具有 vCenter Server 的組態設定防火牆 254
 - 透過防火牆連線到 vCenter Server 254
 - 針對沒有 vCenter Server 的組態設定防火牆 255
 - 透過防火牆連線 ESXi 主機 255
 - 透過防火牆連線到虛擬機器主控台 255
- 確保實體交換器安全 256
- 使用安全性原則確保標準交換器連接埠安全 256
- 保護 vSphere Standard Switch 的安全 257
 - MAC 位址變更 258
 - 偽造的傳輸 258
 - 混合模式作業 258
- 保護 vSphere Distributed Switch 和分散式連接埠群組安全 258

透過 VLAN 保護虛擬機器的安全	259
VLAN 安全考量	260
安全 VLAN	260
在單一 ESXi 主機上建立網路 DMZ	261
在單一 ESXi 主機內建立多個網路	262
網際網路通訊協定安全性	264
列出可用的安全性關聯	264
新增 IPsec 安全性關聯	264
移除 IPsec 安全性關聯	265
列出可用的 IPsec 安全性原則	265
建立 IPsec 安全性原則	266
移除 IPsec 安全性原則	267
確保 SNMP 組態正確	267
僅在需要時透過 vSphere Network Appliance API 使用虛擬交換器	268
vSphere 網路安全性最佳做法	268
一般網路安全性建議	268
標記網路元件	269
記錄及檢查 vSphere VLAN 環境	269
採用音效網路隔離做法	270

9 有關多個 vSphere 元件的最佳做法 272

同步 vSphere 網路上的時鐘	272
使 ESXi 時鐘與網路時間伺服器同步	272
在 vCenter Server Appliance 中設定時間同步化設定	273
使用 VMware Tools 時間同步化	273
在 vCenter Server Appliance 組態中新增或取代 NTP 伺服器	274
將 vCenter Server Appliance 與 NTP 伺服器的時間同步	274
儲存區安全性最佳做法	275
保護 iSCSI 儲存區安全	275
保護 iSCSI 裝置安全	275
保護 iSCSI SAN	276
遮罩 SAN 資源並進行分區	276
針對 NFS 4.1 使用 Kerberos 認證	277
確認已停用向客體傳送主機效能資料	277
設定 ESXi Shell 和 vSphere Web Client 的逾時	278

10 透過 TLS 重新設定公用程式管理 TLS 通訊協定組態 279

支援停用 TLS 版本的連接埠	279
停用 vSphere 中的 TLS 版本	281
安裝 TLS 組態公用程式	281
執行選擇性手動備份	282

停用 vCenter Server 系統上的 TLS 版本	284
停用 ESXi 主機上的 TLS 版本	284
在 Platform Services Controller 系統上停用 TLS 版本	286
還原 TLS 組態變更	287
在 vSphere Update Manager 上停用 TLS 版本	289
停用 Update Manager 連接埠 9087 的舊版 TLS	289
停用 Update Manager 連接埠 8084 的舊版 TLS	290
重新啟用 Update Manager 連接埠 9087 停用的 TLS 版本	291
重新啟用 Update Manager 連接埠 8084 停用的 TLS 版本	291

11 定義的權限 293

警示權限	294
Auto Deploy 與映像設定檔權限	295
憑證權限	296
內容程式庫權限	296
資料中心權限	298
資料存放區權限	298
資料存放區叢集權限	299
Distributed Switch 權限	299
ESX Agent Manager 權限	300
延伸權限	301
資料夾權限	301
全域權限	302
主機 CIM 權限	302
主機組態權限	303
主機詳細目錄	304
主機本機作業權限	304
主機 vSphere Replication 權限	305
主機設定檔權限	305
Inventory Service 提供者權限	306
Inventory Service 標記權限	306
網路權限	307
效能權限	307
權限 (Permissions) 權限	308
Profile-Driven Storage 權限	308
資源權限	308
排定的工作權限	309
工作階段權限	309
儲存區視圖權限	310
工作權限	310
Transfer Service 權限	311

VRM 原則權限	311
虛擬機器組態權限	311
虛擬機器客體作業權限	312
虛擬機器互動權限	313
虛擬機器詳細目錄權限	318
虛擬機器佈建權限	319
虛擬機器服務組態權限	320
虛擬機器快照管理權限	320
虛擬機器 vSphere Replication 權限	321
dvPort 群組權限	321
vApp 權限	321
vServices 權限	323

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。

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 1-1. 《vSphere 安全性》要點

主題	內容要點
使用 vCenter Single Sign-On 進行驗證	<ul style="list-style-type: none">■ vCenter Single Sign-On 功能和服務。■ 新增和管理身分識別來源。■ vCenter Single Sign-On 原則。■ 使用者和群組。
權限和使用者管理	<ul style="list-style-type: none">■ 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。
憑證管理	<ul style="list-style-type: none">■ ESXi 憑證管理■ vCenter Server 和相關服務的憑證管理。<ul style="list-style-type: none">■ 使用 UI 進行憑證管理。■ 使用 Certificate Manager 公用程式進行憑證管理。■ 使用 CLI 進行手動憑證管理 (包括範例)。
主機安全性功能	<ul style="list-style-type: none">■ 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。
安全性最佳做法和強化	<p>VMware 安全性專家提出的最佳做法和建議。</p> <ul style="list-style-type: none">■ 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

除了本文件，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。

更新資訊

本《vSphere 安全性》說明文件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
2022 年 4 月 27 日	■ 對儲存區視圖權限進行輕微更新。
2021 年 11 月 05 日	■ 對 ESXi 安全性最佳做法進行輕微更新。 ■ 更正了停用 ESXi 主機上的 TLS 版本，以說明您應登入 vCenter Server。
2020 年 8 月 14 日	VMware 十分重視包容性。為了在我們的客戶、合作夥伴和內部社群之間提倡此原則，我們將取代內容中的一些術語。我們已更新此指南以移除非包容性語言的實例。 ■ 對確保虛擬機器安全進行輕微更新。
2017 年 10 月 4 日	■ 在瞭解憑證模式切換中說明了可接受將主機置於維護模式並中斷其連線，以執行模式切換。不需要移除主機。
ZH_TW-001949-07	■ 新增了詳細說明憑證需求的新主題不同解決方案路徑的憑證需求。移除了詳細資料較少的舊主題。 ■ 新增章節第 10 章 透過 TLS 重新設定公用程式管理 TLS 通訊協定組態。
ZH_TW-001949-06	■ 已更新使用命令列設定智慧卡驗證，以清楚地說明逗點分隔的憑證清單中不允許有空格。 ■ 包含了使用命令列設定智慧卡驗證中的指令碼位置。 ■ 釐清了將解決方案使用者憑證取代為自訂憑證中需要有完整的憑證鏈結。 ■ 修正了多個權限設定簡介的問題。
ZH_TW-001949-05	■ 已將驗證和驗證期間的資訊新增至變更權限驗證設定。
ZH_TW-001949-04	■ 已修正確認已對網路檔案複製啟用 SSL 憑證驗證中參數名稱的錯誤。 ■ 已將 Windows 上 service-control 命令的位置相關資訊新增至使用 CLI 命令管理憑證和服務。
ZH_TW-001949-03	■ 已在標籤物件的權限中新增標籤權限的相關資訊。 ■ 已釐清使用 vSphere Certificate Manager 產生 CSR 並準備根憑證 (中繼 CA) 中的憑證順序。
ZH_TW-001949-02	■ 已將關於使用 vSphere Client 登入的附註新增至第 2 章 使用 vCenter Single Sign-On 進行 vSphere 驗證。 ■ Active Directory 身分識別來源設定中的釐清資訊。必須將系統加入 Active Directory 名稱，並且網域名稱必須可透過 DNS 解析。

修訂版本	說明
ZH_TW-001949-01	<ul style="list-style-type: none"> ■ 已更正使用 vSphere Certificate Manager 產生 CSR 並準備根憑證 (中繼 CA) 中憑證的順序。 ■ 已更新 ESXi 密碼及帳戶鎖定。依預設，複雜密碼未啟用。 ■ 已更正存取使用命令列設定智慧卡驗證中應用裝置 shell 的步驟。 ■ 變更 vCenter Single Sign-On 密碼 的修正。如果您的密碼已到期，必須連絡管理員。 ■ 已更新使用指令碼管理主機組態設定中的 PowerCLI 指令碼。 ■ 已更新 vCenter Single Sign-On 如何影響安裝 中 vCenter Server 執行個體數目的相關資訊。 ■ 使用命令列設定智慧卡驗證、使用 Platform Services Controller Web 介面管理智慧卡驗證 和 設定 RSA SecurID 驗證 的多個更新。 ■ vCenter Server TCP 和 UDP 連接埠 中的更正。例如連接埠 903 和連接埠 5900-5964 在主機上使用，而不是在 vCenter Server 系統上使用，還有某些其他連接埠 (如 9090) 僅內部使用。 ■ 已從 使用 vifs 命令上傳 SSH 金鑰 移除 DSA 金鑰的相關資訊。 ■ 已更新 安全性 Token 服務 STS，以納入用於產生新 STS 簽署憑證的程序。
ZH_TW-001949-00	初始版本。

vSphere 環境中的安全性

1

vSphere 環境的元件會立即受到多種功能的保護，如憑證、驗證、每個 ESXi 上的防火牆、限制存取等。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。這可為保護 vCenter Server 系統、ESXi 主機，以及虛擬機器提供最大彈性。

您也可以進一步概覽需要注意的 vSphere 各個方面，有助於您規劃安全性策略。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](#)
- [保護 vCenter Server 系統和相關聯服務的安全](#)
- [確保虛擬機器安全](#)
- [保護虛擬網路層的安全](#)
- [vSphere 環境中的密碼](#)
- [安全性最佳做法和資源](#)

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。如果您設定了參考主機並對以該主機之主機設定檔為基礎的所有主機進行變更，或者如果您執行指令碼式管理，則透過保證變更套用到所有主機，可對您的環境提供進一步保護。

使用本指南中詳細論述的下列功能，增強受 vCenter Server 管理之 ESXi 主機的保護。另請參閱《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 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。您可以從 vCenter Server 權限管理介面將不同的主機組態權限套用到不同的具名使用者，而不是允許管理員使用根使用者帳戶登入 ESXi 主機。您可以建立自訂角

色，向該角色指派權限，以及將該角色與具名使用者及 vSphere Web Client 中的 ESXi 主機物件相關聯。

在只有一台主機的情況下，您直接管理使用者。請參閱《使用 vSphere Client 進行 vSphere 管理》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。可以使用主機設定檔替代指令碼式管理。設定參考主機，匯出主機設定檔，並將主機設定檔套用到您的主機。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《vSphere 安裝和設定》。

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，並且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，才可以將其新增至此主機。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 [檢查主機和 VIB 的接受程度](#)。

管理 ESXi 憑證

在 vSphere 6.0 及更新版本中，VMware 憑證授權機構 (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。根據公司原則需要，可以將現有憑證取代為由第三方 CA 簽署的憑證。

請參閱 [ESXi 主機的憑證管理](#)

智慧卡驗證

從 vSphere 6.0 開始，ESXi 支援智慧卡驗證，做為代替使用者名稱和密碼驗證的選項。。

請參閱 [設定用於 ESXi 的智慧卡驗證](#)。

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。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。

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《使用 vSphere Client 進行 vSphere 管理》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，並採取其他步驟保護對您環境的存取。

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 主機電腦

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 憑證授權機構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。請參閱 [第 3 章 vSphere 安全性憑證](#)。

如需其他保護，請確保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。第一次安裝軟體時，您可以指定 administrator@vsphere.local 使用者的密碼，只有該網域才能用作身分識別來源。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)。請參閱 [第 2 章 使用 vCenter Single Sign-On 進行 vSphere 驗證](#)。

為使用者或群組指派角色

為了更好地記錄，請將您授予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](#)。

確保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。

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、虛擬網路介面卡等。此外，請考慮[第 8 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。此網路只能從系統、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。防火牆規則將服務與對應的防火牆建立關聯，從而可以根據服務狀態來開啟和關閉 ESXi 防火牆。

請參閱 [ESXi 防火牆組態](#)。

考慮網路安全性原則

網路安全性原則可保護流量免受 MAC 位址模擬和有害連接埠掃描的威脅。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

這些用來保護虛擬機器網路安全的方式取決於所安裝的客體作業系統、虛擬機器是否在受信任環境中執行，以及其他各種因素。與其他一般的安全性措施 (例如，安裝防火牆) 搭配使用，可大大增強虛擬交換器和分散式虛擬交換器的保護作用。

請參閱 [第 8 章 確保 vSphere 網路安全](#)。

考慮使用 VLAN 來保護環境

ESXi 支援 IEEE 802.1q VLAN，可為虛擬機器網路或儲存區組態提供進一步保護。VLAN 可讓您將實體網路分段，以便讓同一實體網路中的兩台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，可透過 vSphere Web Client 或 CLI 將環境設定為使用 CHAP 和相互 CHAP (如果公司原則需要)。

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、鎖定和到期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 [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、鎖定和到期視使用者的網域和使用者的身分而有所不同。

administrator@vsphere.local

如果您在安裝期間選取了不同的網域，`administrator@vsphere.local` 使用者或 `administrator@mydomain` 使用者的密碼不會到期，且不會受到鎖定原則的限制。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。請參閱 [編輯 vCenter Single Sign-On 密碼原則](#)。

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。

其他 vsphere.local 使用者

其他 `vsphere.local` 使用者或您在安裝期間指定之本機網域使用者的密碼，必須遵循由 vCenter Single Sign-On 密碼原則和鎖定原則所設定的限制。請參閱 [編輯 vCenter Single Sign-On 密碼原則](#) 和 [編輯 vCenter Single Sign-On 鎖定原則](#)。依預設，這些密碼會於 90 天後到期，不過管理員可以將到期日做為密碼原則的一部分進行變更。

如果使用者忘記了自己的 `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、鎖定和到期視使用者進行驗證的網域 (身分識別來源) 而有所不同。

vCenter Single Sign-On 支援一個預設的身分識別來源，使用者只能以使用者名稱登入 vSphere Client。網域決定密碼參數。如果使用者希望在非預設網域中以使用者身分登入，他們可以加入網域名稱，即指定 `user@domain` 或 `domain\user`。網域密碼參數也適用於此情況。

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 上執行的 vCenter Server 及相關聯的服務進行最佳化。

部署 vCenter Server Appliance 時，為應用裝置 Linux 作業系統的根使用者和 `administrator@vsphere.local` 使用者指定密碼。您可以從 Direct Console 使用者介面變更根使用者密碼，以及執行其他 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 1-1. 安全性最佳做法

vSphere 元件	資源
ESXi 主機	ESXi 安全性最佳做法
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 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
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

使用 vCenter Single Sign-On 進行 vSphere 驗證

2

vCenter Single Sign-On 是一種驗證代理和安全性 Token 交換基礎結構。當使用者或解決方案使用者可以向 vCenter Single Sign-On 進行驗證時，該使用者會接收 SAML Token。接著，使用者可使用 SAML Token 向 vCenter 服務進行驗證。然後，使用者即可執行其有權執行的動作。

由於所有通訊的流量都會加密，並且只有經過驗證的使用者才能執行其有權執行的動作，因此您的環境很安全。

從 vSphere 6.0 開始，vCenter Single Sign-On 會包含在 Platform Services Controller 中。Platform Services Controller 包含支援 vCenter Server 和 vCenter Server 元件的共用服務。這些服務包括 vCenter Single Sign-On、VMware 憑證授權機構、授權服務和 Lookup Service。如需有關 Platform Services Controller 的詳細資料，請參閱《vSphere 安裝和設定》。

初始信號交換期間，會使用使用者名稱和密碼驗證使用者，使用憑證驗證解決方案使用者。如需取代解決方案使用者憑證的相關資訊，請參閱第 3 章 [vSphere 安全性憑證](#)。

透過 vCenter Single Sign-On 驗證使用者之後，您可以授權使用者執行特定工作。在大多數情況下，您會指派 vCenter Server 權限，但是 vSphere 包含其他權限模型。請參閱[瞭解 vSphere 中的授權](#)。

備註 如果要讓 Active Directory 使用者能夠透過使用 vSphere Client 搭配 SSPI 的方式登入 vCenter Server 執行個體，則必須將 vCenter Server 執行個體加入 Active Directory 網域。如需將含外部 Platform Services Controller 的 vCenter Server Appliance 加入 Active Directory 網域的相關資訊，請參閱 VMware 知識庫文章，網址為 <http://kb.vmware.com/kb/2118543>。

本章節討論下列主題：

- [瞭解 vCenter Single Sign-On](#)
- [設定 vCenter Single Sign-On 身分識別來源](#)
- [vCenter Server 雙因素驗證](#)
- [針對其他服務提供者將 vCenter Single Sign-On 用做身分識別提供者](#)
- [安全性 Token 服務 STS](#)
- [管理 vCenter Single Sign-On 原則](#)
- [管理 vCenter Single Sign-On 使用者和群組](#)
- [vCenter Single Sign-On 安全性最佳做法](#)
- [vCenter Single Sign-On 疑難排解](#)

瞭解 vCenter Single Sign-On

若要有有效管理 vCenter Single Sign-On，您需要瞭解基礎架構，以及它對安裝和升級有什麼影響。



vCenter Single Sign-On 6.0 網域與網站

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_y9pxac75/uiConfId/49694343/)

如何使用 vCenter Single Sign-On 保護您的環境

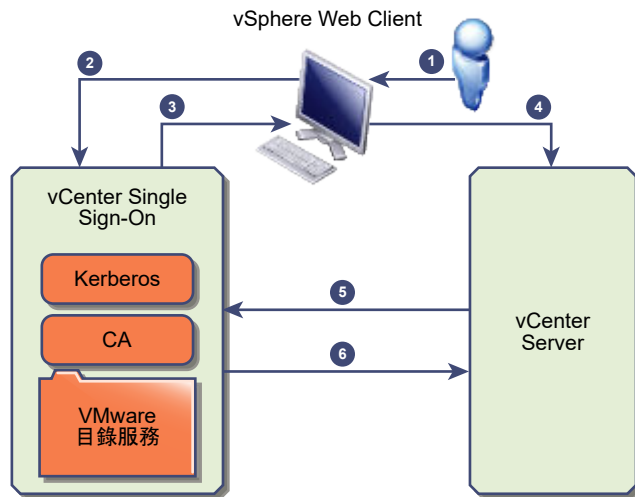
vCenter Single Sign-On 可讓 vSphere 元件透過安全的 Token 機制相互通訊，而不需要使用者分別驗證每個元件。

vCenter Single Sign-On 將 STS (安全性 Token 服務)、用於保護流量安全的 SSL、透過 Active Directory 或 OpenLDAP 的個人使用者驗證以及透過憑證的解決方案使用者驗證組合使用。

個人使用者的 vCenter Single Sign-On 信號交換

下圖顯示的是個人使用者的信號交換。

圖 2-1. 個人使用者的 vCenter Single Sign-On 信號交換



- 1 使用者透過使用者名稱和密碼登入 vSphere Web Client，以存取 vCenter Server 系統或其他 vCenter 服務。

使用者亦可不使用密碼，而是勾選使用 **Windows 工作階段驗證** 核取方塊登入。

- 2 vSphere Web Client 會將登入資訊傳遞到 vCenter Single Sign-On 服務，該服務將檢查 vSphere Web Client 的 SAML Token。如果 vSphere Web Client 的 Token 有效，vCenter Single Sign-On 隨後會檢查使用者是否位於已設定的身分識別來源中 (例如，Active Directory)。
 - 如果僅使用了使用者名稱，則 vCenter Single Sign-On 將在預設網域中檢查。
 - 如果使用者名稱中包含網域名稱 (*DOMAIN/user1* 或 *user1@DOMAIN*)，則 vCenter Single Sign-On 將檢查該網域。

- 3 如果使用者可驗證身分識別來源，則 vCenter Single Sign-On 會將表示該使用者的 Token 傳回到 vSphere Web Client。
- 4 vSphere Web Client 會將 Token 傳遞到 vCenter Server 系統。
- 5 vCenter Server 與 vCenter Single Sign-On 伺服器確認 Token 是否有效且未到期。
- 6 vCenter Single Sign-On 伺服器會將 Token 傳回到 vCenter Server 系統，以利用 vCenter Server 授權架構允許使用者存取。

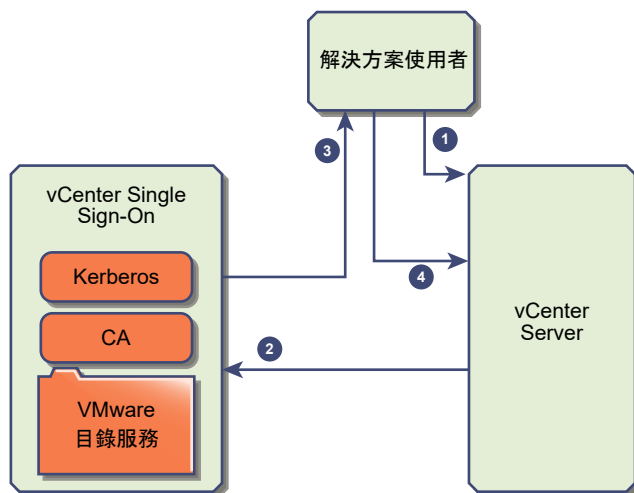
目前，使用者可以驗證、檢視並修改使用者角色對其擁有權限的任何物件。

備註 系統初始會向每個使用者指派「無存取權」的角色。vCenter Server 管理員必須至少為使用者指派「唯讀」角色，使用者才能登入。請參閱[將權限新增到詳細目錄物件](#)。

解決方案使用者的 vCenter Single Sign-On 信號交換

解決方案使用者是用於 vCenter Server 基礎結構的服務集，例如，vCenter Server 或 vCenter Server 延伸。VMware 延伸和潛在的第三方延伸可能也會驗證 vCenter Single Sign-On。

圖 2-2. 解決方案使用者的 vCenter Single Sign-On 信號交換



針對解決方案使用者，互動會按如下所示進行：

- 1 解決方案使用者會嘗試連線至 vCenter 服務，
- 2 解決方案使用者會重新導向到 vCenter Single Sign-On。如果該解決方案使用者對 vCenter Single Sign-On 來說是陌生的，則必須提供有效憑證。
- 3 如果憑證有效，則 vCenter Single Sign-On 會為解決方案使用者指派 SAML Token (Bearer Token)。此 Token 由 vCenter Single Sign-On 簽署。
- 4 然後，解決方案使用者會重新導向到 vCenter Single Sign-On，並且可以根據其權限執行相關工作。
- 5 下次解決方案使用者必須進行驗證，可使用 SAML Token 登入 vCenter Server。

依預設，由於啟動期間 VMCA 為解決方案使用者佈建有憑證，所以此信號交換會自動執行。如果公司原則需要第三方 CA 簽署的憑證，您可以用第三方 CA 簽署的憑證取代解決方案使用者憑證。如果這些憑證有效，則 vCenter Single Sign-On 會為解決方案使用者指派 SAML Token。請參閱 [將第三方憑證與 vSphere 搭配使用](#)。

vCenter Single Sign-On 元件

vCenter Single Sign-On 包括 Security Token Service (STS)、管理伺服器、vCenter Lookup Service 和 VMware 目錄服務 (vmdir)。VMware 目錄服務也可用於憑證管理。

在安裝期間，這些元件會做為內嵌式部署或 Platform Services Controller 的一部分進行部署。

STS (Security Token Service)

STS 服務會核發安全性聲明標記語言 (SAML) Token。這些安全性 Token 代表 vCenter Single Sign-On 支援的其中一種身分識別來源類型中的使用者身分識別。SAML Token 允許成功通過 vCenter Single Sign-On 驗證的個人使用者和解決方案使用者使用 vCenter Single Sign-On 支援的任何 vCenter 服務，無需再次向每項服務進行驗證。

vCenter Single Sign-On 服務使用簽署憑證簽署所有 Token，並將 Token 簽署憑證儲存在磁碟上。服務本身的憑證也儲存在磁碟上。

管理伺服器

管理伺服器允許具有 vCenter Single Sign-On 管理員權限的使用者，從 vSphere Web Client 設定 vCenter Single Sign-On 伺服器並管理使用者和群組。一開始，只有使用者 `administrator@your_domain_name` 具有這些權限。在 vSphere 5.5 中，此使用者是 `administrator@vsphere.local`。藉由 vSphere 6.0，您可以在使用新的 Platform Services Controller 安裝 vCenter Server 或部署 vCenter Server Appliance 時變更 vSphere 網域。請勿使用您的 Microsoft Active Directory 或 OpenLDAP 網域名稱命名此網域名稱。

VMware Directory Service (vmdir)

VMware Directory Service (vmdir) 與您安裝期間指定的網域相關聯，並包含於每個內嵌式部署及 Platform Services Controller 中。此服務是一種多承租人、對等複寫的目錄服務，可在連接埠 389 上提供 LDAP 目錄。服務仍使用連接埠 11711，以便與 vSphere 5.5 及更早版本的系統回溯相容。

如果您的環境包含多個 Platform Services Controller 執行個體，則一個 vmdir 執行個體中的 vmdir 內容更新將傳播到所有其他 vmdir 執行個體。

從 vSphere 6.0 開始，VMware Directory Service 不僅儲存 vCenter Single Sign-On 資訊，還會儲存憑證資訊。

Identity Management 服務

處理身分識別來源和 STS 驗證要求。

vCenter Single Sign-On 如何影響安裝

自 5.1 版起，vSphere 將包含 vCenter Single Sign-On 服務做為 vCenter Server 管理基礎結構的一部分。此變更會影響 vCenter Server 安裝。

使用 vCenter Single Sign-On 進行驗證會使 vSphere 更加安全，因為 vSphere 軟體元件透過安全的 Token 交換機制相互通訊，而其他所有使用者也透過 vCenter Single Sign-On 進行驗證。

自 vSphere 6.0 起，vCenter Single Sign-On 會包含在內嵌式部署中，或做為 Platform Services Controller 的一部分。Platform Services Controller 包含 vSphere 元件之間通訊所需的所有服務，包括 vCenter Single Sign-On、VMware Certificate Authority、VMware Lookup Service 及授權服務。

安裝順序非常重要。

第一次安裝

如果是分散式安裝，則必須先安裝 Platform Services Controller，再安裝 vCenter Server 或部署 vCenter Server Appliance。若是內嵌式部署，會自動以正確順序安裝。

後續安裝

若是大約有多達四個 vCenter Server 執行個體，一個 Platform Services Controller 可為整個 vSphere 環境提供服務。可以將新 vCenter Server 執行個體連線到同一個 Platform Services Controller。若是大約有四個以上 vCenter Server 執行個體，可以再額外安裝一個 Platform Services Controller，以提高效能。每個 Platform Services Controller 上的 vCenter Single Sign-On 服務會將驗證資料與其他所有執行個體同步。確切數目取決於使用 vCenter Server 執行個體的強度及其他因素。

vCenter Single Sign-On 如何影響升級

如果您將簡單安裝環境升級為 vCenter Server 6 內嵌式部署，升級可以順暢進行。如果您升級自訂安裝，升級之後，vCenter Single Sign-On 服務則屬於 Platform Services Controller 的一部分。升級後，哪些使用者可以登入 vCenter Server 視升級前的版本和部署組態而定。

在升級過程中，您可以定義其他 vCenter Single Sign-On 網域名稱，代替 vsphere.local 加以使用。

升級路徑

升級的結果取決於您選取的安裝選項以及要升級到的部署模型。

表 2-1. 升級路徑

來源	結果
vSphere 5.5 及更早版本的簡單安裝	含內嵌式 Platform Services Controller 的 vCenter Server。
vSphere 5.5 及更早版本的自訂安裝	<p>如果 vCenter Single Sign-On 和 vCenter Server 位於不同節點，會產生具有外部 Platform Services Controller 的環境。</p> <p>如果 vCenter Single Sign-On 和 vCenter Server 位於相同節點上，但其他服務位於不同節點上，會產生具有內嵌式 Platform Services Controller 的環境。</p> <p>如果自訂安裝包含多個複寫 vCenter Single Sign-On 伺服器，會產生具有多個複寫 Platform Services Controller 執行個體的環境。</p>

簡單安裝升級後可登入的對象

如果您要升級使用 [簡單安裝] 選項佈建的環境，則一律會產生含內嵌式 Platform Services Controller 的安裝。獲得授權登入的使用者取決於來源環境是否包含 vCenter Single Sign-On。

表 2-2. 簡單安裝環境升級後的登入權限

來源版本	登入存取權	附註
vSphere 5.0	本機作業系統使用者 administrator@vsphere.local	由於使用者存放區的變更，安裝期間系統可能會提示您輸入 vSphere 詳細目錄階層中根資料夾的管理員。 如果您先前的安裝支援 Active Directory 使用者，則可以將 Active Directory 網域新增為身分識別來源。
vSphere 5.1	本機作業系統使用者 administrator@vsphere.local Admin@SystemDomain	從 vSphere 5.5 開始，vCenter Single Sign-On 僅支援一個預設身分識別來源。 您可以設定預設身分識別來源。 非預設網域中的使用者可以在登入時指定網域 (<i>DOMAIN\user</i> 或 <i>user@DOMAIN</i>)。
vSphere 5.5	administrator@vsphere.local 或您於升級期間指定的網域管理員。 所有身分識別來源的所有使用者都能照常登入。	

如果您從未包含 vCenter Single Sign-On 的 vSphere 5.0 升級為包含 vCenter Single Sign-On 的版本，與目錄服務 (例如 Active Directory) 中的使用者相比，本機作業系統使用者會變得較不重要。因此，很難或甚至無法保留本機作業系統使用者做為經過驗證的使用者。

自訂安裝升級後可登入的對象

如果您要升級使用 [自訂安裝] 選項佈建的環境，結果會取決於初始選擇：

- 如果 vCenter Single Sign-On 和 vCenter Server 系統位於相同節點上，會產生含內嵌式 Platform Services Controller 的安裝。
- 如果 vCenter Single Sign-On 和 vCenter Server 系統位於不同節點上，會產生具有外部 Platform Services Controller 的安裝。
- 如果您從 vSphere 5.0 升級，可在升級程序期間選取外部或內嵌式 Platform Services Controller。

升級後的登入權限取決於多個因素。

表 2-3. 自訂安裝環境升級後的登入權限

來源版本	登入存取權	附註
vSphere 5.0	<p>vCenter Single Sign-On 會識別 Platform Services Controller 安裝所在機器的本機作業系統使用者，但不會識別 vCenter Server 安裝所在機器的本機作業系統使用者。</p> <p>備註 不建議使用本機作業系統使用者進行管理，聯合環境中尤其如此。</p> <p>administrator@vsphere.local 可以管理員使用者身分登入 vCenter Single Sign-On 與每個 vCenter Server 執行個體。</p>	如果您的 5.0 安裝支援 Active Directory 使用者，升級後這些使用者將不再具有存取權。您可以將 Active Directory 網域新增為身分識別來源。
vSphere 5.1 或 vSphere 5.5	<p>vCenter Single Sign-On 會識別 Platform Services Controller 安裝所在機器的本機作業系統使用者，但不會識別 vCenter Server 安裝所在機器的本機作業系統使用者。</p> <p>備註 不建議使用本機作業系統使用者進行管理，聯合環境中尤其如此。</p> <p>administrator@vsphere.local 可以管理員使用者身分登入 vCenter Single Sign-On 與每個 vCenter Server 執行個體。</p> <p>如果從 vSphere 5.1 升級，Admin@SystemDomain 將與 administrator@vsphere.local 具有相同的權限。</p>	<p>從 vSphere 5.5 開始，vCenter Single Sign-On 僅支援一個預設身分識別來源。</p> <p>您可以設定預設身分識別來源。</p> <p>非預設網域中的使用者可以在登入時指定網域 (<i>DOMAIN\user</i> 或 <i>user@DOMAIN</i>)。</p>

將 vCenter Single Sign-On 與 vSphere 搭配使用

當使用者登入 vSphere 元件，或當 vCenter Server 解決方案使用者存取另一個 vCenter Server 服務時，vCenter Single Sign-On 會執行驗證。使用者必須透過 vCenter Single Sign-On 進行驗證，並具有與 vSphere 物件互動所需的權限。

vCenter Single Sign-On 會驗證解決方案使用者和其他使用者。

- 解決方案使用者代表 vSphere 環境中的一組服務。依預設，VMCA 會在安裝期間為每個解決方案使用者指派憑證。解決方案使用者會使用該憑證向 vCenter Single Sign-On 進行驗證。vCenter Single Sign-On 會為解決方案使用者提供 SAML Token，然後解決方案使用者便可與環境中的其他服務互動。
- 當其他使用者登入環境時 (例如從 vSphere Web Client)，vCenter Single Sign-On 會提示輸入使用者名稱和密碼。如果 vCenter Single Sign-On 發現使用者的相應身分識別來源中具備這些認證，就會為該使用者指派 SAML Token。接著使用者就可以存取環境中的其他服務，而不會收到再次進行驗證的提示。

使用者可以檢視的物件，以及使用者可以執行的動作，通常是由 vCenter Server 權限設定決定。vCenter Server 管理員會從 vSphere Web Client 中的 **管理 > 權限** 介面指派這些權限，而不是透過 vCenter Single Sign-On。請參閱第 4 章 [vSphere 權限和使用者管理工作](#)。

vCenter Single Sign-On 和 vCenter Server 使用者

使用者可使用 vSphere Web Client，透過在 vSphere Web Client 登入頁面上輸入認證，向 vCenter Single Sign-On 進行驗證。連線到 vCenter Server 後，已驗證的使用者可以檢視所有 vCenter Server 執行個體，或其角色有權檢視的其他 vSphere 物件。無需進一步驗證。請參閱第 4 章 [vSphere 權限和使用者管理工作](#)。

安裝後，administrator@vsphere.local 使用者將擁有 vCenter Single Sign-On 和 vCenter Server 的管理員存取權。然後，該使用者可以新增身分識別來源、設定預設身分識別來源，以及管理 vCenter Single Sign-On 網域 (vsphere.local) 中的使用者和群組。

可向 vCenter Single Sign-On 進行驗證的所有使用者，只要記得密碼，都能進行密碼重設，即使密碼已過期也一樣。請參閱[變更 vCenter Single Sign-On 密碼](#)。只有 vCenter Single Sign-On 管理員能為遺失密碼的使用者重設密碼。

vCenter Single Sign-On 管理員使用者

可以從 vSphere Web Client 存取 vCenter Single Sign-On 管理介面。

若要設定 vCenter Single Sign-On 並管理 vCenter Single Sign-On 使用者和群組，使用者 administrator@vsphere.local 或 vCenter Single Sign-On 管理員群組中的使用者必須登入 vSphere Web Client。驗證後，該使用者可以從 vSphere Web Client 存取 vCenter Single Sign-On 管理介面並管理身分識別來源和預設網域、指定密碼原則，以及執行其他管理工作。請參閱[設定 vCenter Single Sign-On 身分識別來源](#)。

備註 您無法重新命名 administrator@vsphere.local 使用者。為提高安全性，請考量在 vsphere.local 網域中建立其他具名使用者，並為這些使用者指派管理權限。隨後即可停止使用 administrator@vsphere.local。

不同版本 vSphere 中的驗證

如果使用者連線到 vCenter Server 系統 5.0.x 或更早版本，vCenter Server 會根據 Active Directory 網域或本機作業系統使用者清單驗證使用者，從而對使用者進行驗證。在 vCenter Server 5.1 及更新版本中，使用者將透過 vCenter Single Sign-On 進行驗證。

備註 您無法使用 vSphere Web Client 管理 vCenter Server 5.0 或更早版本。將 vCenter Server 升級到 5.1 或更新版本。

ESXi 使用者

ESXi 未與 vCenter Single Sign-On 整合。將 ESXi 主機明確新增到 Active Directory 網域。請參閱[將主機設定為使用 Active Directory](#)。

您仍然可以使用 vSphere Client、vCLI 或 PowerCLI 建立本機 ESXi 使用者。vCenter Server 無法感知 ESXi 的本機使用者，且 ESXi 無法感知 vCenter Server 使用者。

備註 如果可能，請透過 vCenter Server 管理 ESXi 主機權限。

如何登入 vCenter Server 元件

使用者從 vSphere Web Client 登入 vCenter Server 系統時，登入行為視使用者是否位於預設網域 (即，設定為預設身分識別來源的網域) 而定。

- 預設網域中的使用者可以使用自己的使用者名稱和密碼登入。
- 若使用者位於已新增到 vCenter Single Sign-On 做為身分識別來源的網域，但未位於預設網域，可以登入 vCenter Server 但必須以下列其中一種方式指定網域。
 - 包括網域名稱前置詞，例如 MYDOMAIN\user1
 - 包括網域，例如 user1@mydomain.com
- 若使用者位於並非 vCenter Single Sign-On 身分識別來源的網域，則無法登入 vCenter Server。如果新增到 vCenter Single Sign-On 的網域是網域階層的一部分，則 Active Directory 會判斷階層中其他網域的使用者是否已進行驗證。

備註 如果您的環境包含 Active Directory 階層，請參閱 [VMware 知識庫文章 2064250](#) 以取得支援與不支援之設定的相關詳細資料。

vsphere.local 網域中的群組

vsphere.local 網域包含多個預先定義的群組。將使用者指派至其中一個群組，讓其可執行對應的動作。

對於 vCenter Server 階層中的所有物件，權限是透過將使用者和角色與物件配對來指派的。例如，您可以選取一個資源集區，並透過授予使用者群組對應的角色來授予其該資源集區的讀取權限。

對於不是由 vCenter Server 直接管理的某些服務，權限由其中一個 vCenter Single Sign-On 群組的成員資格決定。例如，身為管理員群組成員的使用者可以管理 vCenter Single Sign-On。身為 CAAdmins 群組成員的使用者可以管理 VMware 憑證授權機構，LicenseService.Administrators 群組中的使用者可以管理授權。

下列群組已在 vsphere.local 中預先定義。

備註 其中許多群組為 vsphere.local 的內部群組或授與使用者高層級的管理權限。請仔細考慮風險，然後再將使用者新增至任意群組。

備註 請勿刪除 vsphere.local 網域中的任何預先定義的群組。否則，可能會導致驗證或憑證佈建相關的錯誤。

表 2-4. vsphere.local 網域中的群組

權限	說明
使用者	vsphere.local 網域中的使用者。
SolutionUsers	解決方案使用者群組 vCenter 服務。每個解決方案使用者會使用憑證向 vCenter Single Sign-On 進行個別驗證。依預設，VMCA 會使用憑證佈建解決方案使用者。請勿明確向此群組新增成員。
CAAdmins	CAAdmins 群組的成員擁有 VMCA 的管理員權限。通常不建議向這些群組新增成員。

表 2-4. vsphere.local 網域中的群組 (續)

權限	說明
DCAdmins	DCAdmins 群組的成員可以對 VMware 目錄服務執行網域控制站管理員動作。 備註 請勿直接管理網域控制站。而是使用 <code>vmdir</code> CLI 或 vSphere Web Client 執行對應工作。
SystemConfiguration.BashShellAdministrators	此群組僅適用於 vCenter Server Appliance 部署。 此群組中的使用者可以啟用和停用對 BASH shell 的存取。依預設，使用 SSH 連線到 vCenter Server Appliance 的使用者只能存取受限制的 shell 中的命令。此群組中的使用者可以存取 BASH shell。
ActAsUsers	允許 Act-As Users 的成員從 vCenter Single Sign-On 取得 actas Token。
ExternalIPDUsers	vSphere 不使用此群組。此群組需要與 VMware vCloud Air 搭配使用。
SystemConfiguration.Administrators	SystemConfiguration.Administrators 群組的成員可以在 vSphere Web Client 中檢視和管理系統組態。這些使用者可檢視服務、啟動與重新啟動服務、對服務進行疑難排解，以及查看並管理可用節點。
DCClients	此群組供內部使用，允許管理節點對 VMware 目錄服務中的資料進行存取。 備註 請勿修改此群組。任何變更都可能影響憑證基礎結構。
ComponentManager.Administrators	ComponentManager.Administrators 群組的成員可以叫用登錄或解除登錄服務 (即，修改服務) 的 Component Manager API。取得此服務的讀取權限並不需要此群組的成員資格。
LicenseService.Administrators	LicenseService.Administrators 的成員擁有對所有授權相關資料的完整寫入權限，且可以針對在授權服務中登錄的所有產品資產新增、移除、指派以及解除指派序列金鑰。
管理員	VMware 目錄服務 (vmdir) 的管理員。此群組的成員可以執行 vCenter Single Sign-On 管理工作。通常不建議向此群組新增成員。

vCenter Server 密碼需求與鎖定行為

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

vCenter Single Sign-On 管理員密碼

administrator@vsphere.local 的密碼必須滿足下列需求：

- 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

administrator@vsphere.local 的密碼長度不得超過 20 個字元。僅允許使用可見的 ASCII 字元。這表示，您不得使用空格字元 (以此為例)。

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源可以是 Active Directory、OpenLDAP 或 vCenter Single Sign-On 伺服器的本機作業系統 (不建議)。

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。您可以使用鎖定原則變更這些預設值。請參閱[編輯 vCenter Single Sign-On 鎖定原則](#)。

從 vSphere 6.0 開始，依預設，系統網域管理員、administrator@vsphere.local 不會受鎖定原則的影響。

任何使用者都可以使用 `dir-cli password change` 命令變更其密碼。如果使用者忘記密碼，管理員可以使用 `dir-cli password reset` 命令重設密碼。

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](#)。

設定 vCenter Single Sign-On 身分識別來源

當使用者登入時，vCenter Single Sign-On 會於預設身分識別來源中檢查使用者能否進行驗證。您可以新增身分識別來源、移除身分識別來源，以及變更預設值。

可透過 vSphere Web Client 設定 vCenter Single Sign-On。若要設定 vCenter Single Sign-On，您必須擁有 vCenter Single Sign-On 管理員權限。vCenter Single Sign-On 管理員權限不同於 vCenter Server 或 ESXi 上的管理員角色。依預設，在全新安裝中，只有使用者 administrator@vsphere.local 具有 vCenter Single Sign-On 伺服器上的管理員權限。

- [具有 vCenter Single Sign-On 的 vCenter Server 的身分識別來源](#)

您可以使用身分識別來源將一或多個網域連結到 vCenter Single Sign-On。網域是使用者和群組的存放庫，vCenter Single Sign-On 伺服器可以用來進行使用者驗證。

- [設定 vCenter Single Sign-On 的預設網域](#)

每個 vCenter Single Sign-On 身分識別來源都與某個網域相關聯。vCenter Single Sign-On 使用預設網域驗證未使用網域名稱登入的使用者的身分。如果使用者所屬的網域不是預設網域，則在登入時必須包含網域名稱。

- [新增 vCenter Single Sign-On 身分識別來源](#)

僅當使用者位於已新增為 vCenter Single Sign-On 身分識別來源的網域中時，才可以登入 vCenter Server。vCenter Single Sign-On 管理員使用者可以從 vSphere Web Client 新增身分識別來源。

- [編輯 vCenter Single Sign-On 身分識別來源](#)

vSphere 使用者在身分識別來源中定義。您可以編輯與 vCenter Single Sign-On 相關聯的身分識別來源的詳細資料。

- [移除 vCenter Single Sign-On 身分識別來源](#)

vSphere 使用者在身分識別來源中定義。可從已登錄的身分識別來源清單中移除身分識別來源。

■ 使用 vCenter Single Sign-On 進行 Windows 工作階段驗證

您可以使用 vCenter Single Sign-On 進行 Windows 工作階段驗證 (SSPI)。必須先安裝用戶端整合外掛程式，然後才能讓登入頁面上的核取方塊可用。

具有 vCenter Single Sign-On 的 vCenter Server 的身分識別來源

您可以使用身分識別來源將一或多個網域連結到 vCenter Single Sign-On。網域是使用者和群組的存放庫，vCenter Single Sign-On 伺服器可以用來進行使用者驗證。

身分識別來源是使用者和群組資料的集合。使用者和群組資料儲存在 Active Directory、OpenLDAP 中，或在本機儲存到安裝有 vCenter Single Sign-On 的機器的作業系統。

安裝完成之後，vCenter Single Sign-On 的每個執行個體都會擁有身分識別來源 *your_domain_name*，例如 vsphere.local。此身分識別來源位於 vCenter Single Sign-On 內部。vCenter Single Sign-On 管理員可以新增身分識別來源、設定預設身分識別來源，以及在 vsphere.local 身分識別來源中建立使用者和群組。

身分識別來源類型

vCenter Server 5.1 版之前的版本支援將 Active Directory 和本機作業系統使用者做為使用者存放庫。因此，本機作業系統使用者可以一律向 vCenter Server 系統進行驗證。vCenter Server 5.1 版和 5.5 版使用 vCenter Single Sign-On 進行驗證。如需 vCenter Single Sign-On 5.1 支援的身分識別來源清單，請參閱 vSphere 5.1 說明文件。vCenter Single Sign-On 5.5 支援將下列類型的使用者存放庫做為身分識別來源，但僅支援一個預設身分識別來源。

- Active Directory 2003 及更新版本。在 vSphere Web Client 中顯示為 **Active Directory (整合式 Windows 驗證)**。vCenter Single Sign-On 可讓您將單一 Active Directory 網域指定為身分識別來源。該網域可包含子網域或做為樹系的根網域。VMware 知識庫文章 [2064250](#) 說明 vCenter Single Sign-On 支援的 Microsoft Active Directory 信任關係。
- Active Directory over LDAP。vCenter Single Sign-On 支援多個 Active Directory over LDAP 身分識別來源。包含這種身分識別來源類型旨在與 vSphere 5.1 隨附的 vCenter Single Sign-On 服務相容。在 vSphere Web Client 中顯示為**做為 LDAP 伺服器的 Active Directory**。
- OpenLDAP 2.4 及更新版本。vCenter Single Sign-On 支援多個 OpenLDAP 身分識別來源。在 vSphere Web Client 中顯示為 **OpenLDAP**。
- 本機作業系統使用者。本機作業系統使用者是執行 vCenter Single Sign-On 伺服器之作業系統的本機使用者。本機作業系統身分識別來源僅存在於基本 vCenter Single Sign-On 部署，在具有多個 vCenter Single Sign-On 執行個體的部署中無法使用。僅允許一個本機作業系統身分識別來源。在 vSphere Web Client 中顯示為 **localos**。

備註 如果 Platform Services Controller 與 vCenter Server 系統不在相同的機器上，請勿使用本機作業系統使用者。您可以在內嵌式部署中使用本機作業系統使用者，但不建議如此操作。

- vCenter Single Sign-On 系統使用者。每次安裝 vCenter Single Sign-On 時，只會建立一個名為 vsphere.local 的系統身分識別來源。在 vSphere Web Client 中顯示為 **vsphere.local**。

備註 在任何時候都僅存在一個預設網域。來自非預設網域的使用者在登入時必須新增網域名稱 (*DOMAIN\user*)，才能成功進行驗證。

vCenter Single Sign-On 身分識別來源由 vCenter Single Sign-On 管理員使用者管理。

您可以將身分識別來源新增到 vCenter Single Sign-On 伺服器執行個體。遠端身分識別來源僅限於 Active Directory 和 OpenLDAP 伺服器實作。

設定 vCenter Single Sign-On 的預設網域

每個 vCenter Single Sign-On 身分識別來源都與某個網域相關聯。vCenter Single Sign-On 使用預設網域驗證未使用網域名稱登入的使用者的身分。如果使用者所屬的網域不是預設網域，則在登入時必須包含網域名稱。

使用者從 vSphere Web Client 登入 vCenter Server 系統時，登入行為視使用者是否位於預設網域 (即，設定為預設身分識別來源的網域) 而定。

- 預設網域中的使用者可以使用自己的使用者名稱和密碼登入。
- 若使用者位於已新增到 vCenter Single Sign-On 做為身分識別來源的網域，但未位於預設網域，可以登入 vCenter Server 但必須以下列其中一種方式指定網域。
 - 包括網域名稱前置詞，例如 MYDOMAIN\user1
 - 包括網域，例如 user1@mydomain.com
- 若使用者位於並非 vCenter Single Sign-On 身分識別來源的網域，則無法登入 vCenter Server。如果新增到 vCenter Single Sign-On 的網域是網域階層的一部分，則 Active Directory 會判斷階層中其他網域的使用者是否已進行驗證。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。
具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。
- 2 瀏覽到 **管理 > Single Sign-On > 組態**。
- 3 在 **身分識別來源** 索引標籤上，選取一個身分識別來源，然後按一下 **設定為預設網域** 圖示。
在網域顯示中，預設網域顯示在 [網域] 欄中 (預設)。

新增 vCenter Single Sign-On 身分識別來源

僅當使用者位於已新增為 vCenter Single Sign-On 身分識別來源的網域中時，才可以登入 vCenter Server。vCenter Single Sign-On 管理員使用者可以從 vSphere Web Client 新增身分識別來源。

身分識別來源可以是原生 Active Directory (整合式 Windows 驗證) 網域，也可以是 OpenLDAP 目錄服務。為實現回溯相容性，做為 LDAP 伺服器的 Active Directory 也可供使用。請參閱[具有 vCenter Single Sign-On 的 vCenter Server 的身分識別來源](#)

完成安裝後，下列預設身分識別來源和使用者便立即可用：

localos

所有本機作業系統使用者。如果正在升級，已經可以驗證的使用者仍能夠繼續進行驗證。在使用 Platform Services Controller 的環境中，使用 localos 身分識別來源沒有意義。

vsphere.local

包含 vCenter Single Sign-On 內部使用者。

必要條件

想要新增為身分識別來源的網域必須可用於 vCenter Single Sign-On 執行所在的機器。如果使用 vCenter Server Appliance，請參閱《vCenter Server Appliance 組態》說明文件。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。
具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。
- 2 瀏覽到**管理 > Single Sign-On > 組態**。
- 3 在**身分識別來源**索引標籤上，按一下**新增身分識別來源**圖示。
- 4 選取身分識別來源的類型，然後輸入身分識別來源設定。

選項	說明
Active Directory (整合式 Windows 驗證)	對於原生 Active Directory 實作，請使用此選項。如果您想要使用此選項，則執行 vCenter Single Sign-On 服務所在的機器必須位於 Active Directory 網域。 請參閱 Active Directory 身分識別來源設定 。
做為 LDAP 伺服器的 Active Directory	此選項適用於回溯相容性。這需要您指定網域控制站和其他資訊。請參閱 Active Directory LDAP Server 和 OpenLDAP Server 身分識別來源設定 。
OpenLDAP	對於 OpenLDAP 身分識別來源，請使用此選項。請參閱 Active Directory LDAP Server 和 OpenLDAP Server 身分識別來源設定 。
LocalOS	使用此選項可新增本機作業系統做為身分識別來源。系統僅會提示您輸入本機作業系統的名稱。如果選取此選項，則 vCenter Single Sign-On 可看到指定機器上的所有使用者，即使這些使用者不屬於其他網域亦是如此。

備註 如果使用者帳戶已鎖定或停用，Active Directory 網域中的驗證以及群組和使用者搜尋會失敗。使用者帳戶必須具有使用者和群組 OU 的唯讀存取權，並且必須能夠讀取使用者和群組屬性。這是驗證權限的預設 Active Directory 網域組態。VMware 建議使用特殊服務使用者。

- 5 如果將 Active Directory 設定為 LDAP 伺服器或 OpenLDAP 身分識別來源，請按一下**測試連線**以確保您可以連線到身分識別來源。

6 按一下確定。

後續步驟

新增身分識別來源後，所有使用者皆可進行驗證但僅具有**無存取權**角色。具有 vCenter Server **修改權限**權限的使用者可向使用者或使用者群組指派權限，以便其能夠登入 vCenter Server 並檢視和管理物件。請參閱《vSphere 安全性》說明文件。

Active Directory 身分識別來源設定

如果選取 **Active Directory (整合式 Windows 驗證)** 身分識別來源類型，則可以使用本機機器帳戶做為 SPN (服務主體名稱) 或者明確指定 SPN。僅當 vCenter Single Sign-On 伺服器加入 Active Directory 網域時，您才能使用此選項。

使用 Active Directory 身分識別來源的必要條件

僅在身分識別來源可用的情況下，才能設定 vCenter Single Sign-On 使用該 Active Directory 身分識別來源。

- 對於 Windows 安裝，請將 Windows 機器加入 Active Directory 網域。
- 對於 vCenter Server Appliance，請遵循《vCenter Server Appliance 組態》說明文件中的指示進行操作。

備註 Active Directory (整合式 Windows 驗證) 一律使用 Active Directory 網域樹系的根。若要將您的整合式 Windows 驗證身分識別來源設定為 Active Directory 樹系內的子網域，請參閱 VMware 知識庫文章 [2070433](#)。

選取**使用機器帳戶**可加快組態速度。如果您打算重新命名執行 vCenter Single Sign-On 的本機機器，則最好明確指定 SPN。

備註 在 vSphere 5.5 中，即使您指定 SPN，vCenter Single Sign-On 也會使用機器帳戶。請參閱 VMware 知識庫文章 [2087978](#)。

表 2-5. 新增身分識別來源設定

文字方塊	說明
網域名稱	網域名稱的 FQDN，例如 mydomain.com。不提供 IP 位址。此網域名稱必須可由 vCenter Server 系統進行 DNS 解析。如果您使用 vCenter Server Appliance，請使用進行網路設定時使用的資訊來更新 DNS 伺服器設定。
使用機器帳戶	選取此選項可將本機機器帳戶用作 SPN。選取此選項時，應僅指定網域名稱。如果您打算重新命名此機器，請勿選取此選項。
使用服務主體名稱 (SPN)	如果您打算重新命名本機機器，請選取此選項。您必須指定 SPN、能夠透過身分識別來源進行驗證的使用者，以及該使用者的密碼。

表 2-5. 新增身分識別來源設定 (續)

文字方塊	說明
服務主體名稱 (SPN)	可協助 Kerberos 識別 Active Directory 服務的 SPN。請在名稱中包含網域，例如 STS/example.com。 SPN 在網域中必須是唯一的。執行 <code>setspn -S</code> 可檢查是否未建立任何重複項目。如需 <code>setspn</code> 的相關資訊，請參閱 Microsoft 說明文件。
使用者主體名稱 (UPN) 密碼	能夠透過此身分識別來源進行驗證之使用者的名稱和密碼。請使用電子郵件地址格式，例如 jchin@mydomain.com。您可以透過 Active Directory 服務介面編輯器 (ADSI 編輯) 來驗證使用者主體名稱。

Active Directory LDAP Server 和 OpenLDAP Server 身分識別來源設定

Active Directory 做為 LDAP 伺服器身分識別來源提供回溯相容性。對於需要較少輸入的設定，請使用 [Active Directory (整合式 Windows 驗證)] 選項。OpenLDAP 伺服器身分識別來源適用於使用 OpenLDAP 的環境。

如果要設定 OpenLDAP 身分識別來源，請參閱 VMware 知識庫文章 [2064977](#) 瞭解其他需求。

表 2-6. 做為 LDAP 伺服器的 Active Directory 和 OpenLDAP 設定

欄位	說明
名稱	身分識別來源的名稱。
使用者的基本 DN	使用者的基本辨別名稱。
網域名稱	網域的 FDQN，例如 example.com。請勿在此欄位中提供 IP 位址。
網域別名	對於 Active Directory 身分識別來源，網域的 NetBIOS 名稱。如果使用 SSPI 驗證，請將 Active Directory 網域的 NetBIOS 名稱新增為身分識別來源的別名。 對於 OpenLDAP 身分識別來源，如果沒有指定別名，則會新增大寫字母的網域名稱。
群組的基本 DN	群組的基本辨別名稱。
主要伺服器 URL	網域的網域主控站 LDAP 伺服器。 使用 <code>ldap://hostname:port</code> 或 <code>ldaps://hostname:port</code> 格式。連接埠通常為 389 (適用於 ldap:連線) 和 636 (適用於 ldaps:連線)。對於 Active Directory 多網域控制站部署，連接埠通常為 3268 (適用於 ldap:連線) 和 3269 (適用於 ldaps:連線)。 在主要或次要 LDAP URL 中使用 <code>ldaps://</code> 時，需要為 Active Directory 伺服器的 LDAPS 端點建立信任的憑證。
次要伺服器 URL	用於容錯移轉之次要網域控制站 LDAP 伺服器的位址。
選擇憑證	若要將 LDAP 用於 Active Directory LDAP 伺服器或 OpenLDAP 伺服器身分識別來源，則在 URL 欄位中輸入 <code>ldaps://</code> 後 [選擇憑證] 按鈕隨即變為可用。不需要次要 URL。

表 2-6. 做為 LDAP 伺服器的 Active Directory 和 OpenLDAP 設定 (續)

欄位	說明
使用者名稱	網域中使用者的識別碼，該使用者對使用者和群組的基本 DN 僅具有最小唯讀存取權。
密碼	[使用者名稱] 所指定使用者的密碼。

編輯 vCenter Single Sign-On 身分識別來源

vSphere 使用者在身分識別來源中定義。您可以編輯與 vCenter Single Sign-On 相關聯的身分識別來源的詳細資料。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。
具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。
- 2 瀏覽到 **管理 > Single Sign-On > 組態**。
- 3 按一下 **身分識別來源** 索引標籤。
- 4 在資料表中的身分識別來源上按一下滑鼠右鍵，然後選取 **編輯身分識別來源**。
- 5 編輯身分識別來源設定。可用選項取決於所選身分識別來源的類型。

選項	說明
Active Directory (整合式 Windows 驗證)	對於原生 Active Directory 實作，請使用此選項。如果您想要使用此選項，則執行 vCenter Single Sign-On 服務所在的機器必須位於 Active Directory 網域。 請參閱 Active Directory 身分識別來源設定 。
做為 LDAP 伺服器的 Active Directory	此選項適用於回溯相容性。這需要您指定網域控制站和其他資訊。請參閱 Active Directory LDAP Server 和 OpenLDAP Server 身分識別來源設定 。
OpenLDAP	對於 OpenLDAP 身分識別來源，請使用此選項。請參閱 Active Directory LDAP Server 和 OpenLDAP Server 身分識別來源設定 。
LocalOS	使用此選項可新增本機作業系統做為身分識別來源。系統僅會提示您輸入本機作業系統的名稱。如果選取此選項，則 vCenter Single Sign-On 可看到指定機器上的所有使用者，即使這些使用者不屬於其他網域亦是如此。

- 6 按一下 **測試連線**，確保可以連線到該身分識別來源。
- 7 按一下 **確定**。

移除 vCenter Single Sign-On 身分識別來源

vSphere 使用者在身分識別來源中定義。可從已登錄的身分識別來源清單中移除身分識別來源。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。

具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。

- 2 瀏覽到**管理 > Single Sign-On > 組態**。
- 3 在**身分識別來源**索引標籤上，選取一個身分識別來源，然後按一下**刪除身分識別來源**圖示。
- 4 出現確認提示時，請按一下**是**。

使用 vCenter Single Sign-On 進行 Windows 工作階段驗證

您可以使用 vCenter Single Sign-On 進行 Windows 工作階段驗證 (SSPI)。必須先安裝用戶端整合外掛程式，然後才能讓登入頁面上的核取方塊可用。

使用 SSPI，可為目前已登入電腦的使用者加快登入速度。

必要條件

必須正確設定 Windows 網域。請參閱 VMware 知識庫文章 [2064250](#)。

程序

- 1 導覽到 vSphere Web Client 登入頁面。
- 2 如果**使用 Windows 工作階段驗證**核取方塊無法使用，請按一下位於登入頁面底部的**下載用戶端整合外掛程式**。
- 3 如果瀏覽器透過發出憑證錯誤或執行快顯視窗封鎖程式來封鎖安裝，請依照瀏覽器的 [說明] 指示解決該問題。
- 4 如果系統提示您關閉其他瀏覽器，則執行此動作。

安裝之後，此外掛程式將適用於所有瀏覽器。如果您的瀏覽器需要，則必須允許將此外掛程式用於個別工作階段或所有工作階段。

- 5 結束並重新啟動瀏覽器。

重新啟動之後，您便可以選取**使用 Windows 工作階段驗證**核取方塊。

vCenter Server 雙因素驗證

vCenter Single Sign-On 可讓您透過以下兩種方式進行驗證：使用 vCenter Single Sign-On 已知的身分識別來源中的使用者名稱和密碼，或是對 Active Directory 身分識別來源使用 Windows 工作階段驗證。從 vSphere 6.0 Update 2 開始，您還可以使用智慧卡 (UPN 式通用存取卡，簡稱 CAC) 或 RSA SecurID Token 進行驗證。

雙因素驗證方法

政府機關或大型企業經常需要使用雙因素驗證方法。

通用存取卡 (CAC) 驗證

CAC 驗證僅為將實體卡片連接至所登入電腦之 USB 磁碟機的使用者提供存取權。如果部署 PKI，以使智慧卡憑證成為 CA 核發的唯一用戶端憑證，則只會向使用者提供智慧卡憑證。使用者選取憑證後，系統會提示其輸入 PIN。只有實體卡片和 PIN 都與憑證相符的使用者才能登入。

RSA SecurID 驗證

對於 RSA SecureID 驗證，必須正確設定您環境中的 RSA Authentication Manager。如果 Platform Services Controller 設定為指向 RSA 伺服器，且已啟用 RSA SecurID 驗證，則使用者可以使用其使用者名稱和 Token 登入。

備註 vCenter Single Sign-On 僅支援原生 SecurID，不支援 RADIUS 驗證。

指定非預設驗證方法

管理員可以從 Platform Services Controller Web 介面，或使用 `sso-config` 指令碼 (在 Windows 中使用 `sso-config.bat`，在應用裝置上使用 `sso-config.sh`) 來執行設定。

- 對於通用存取卡驗證，您可以使用 `sso-config` 指令碼設定網頁瀏覽器，並可從 Platform Services Controller Web 介面或使用 `sso-config` 執行 vCenter Single Sign-On 設定。設定包括啟用 CAC 驗證、設定驗證撤銷原則，以及設定登入橫幅。
- 對於 RSA SecureID，您可以使用 `sso-config` 指令碼設定網域的 RSA Authentication Manager，並啟用 RSA Token 驗證。驗證方法啟用後，會顯示在 Platform Services Controller Web 介面中，但您無法從 Web 介面設定 RSA SecureID 驗證。

組合使用不同的驗證方法

您可以使用 `sso-config` 單獨啟用或停用每種驗證方法。這可能十分有用，例如，當您測試其中一種雙因素驗證方法時，最初可以先讓使用者名稱和密碼驗證保持啟用狀態，然後只將一種驗證方法設為啟用。

設定用於 vCenter Single Sign-On 的智慧卡驗證

您可以將環境設定為在使用者透過 vSphere Web Client 連線到 vCenter Server 或相關聯的 Platform Services Controller 時必須進行智慧卡驗證。

智慧卡驗證登入

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通用存取卡 (CAC) 等智慧卡，以增強其系統的安全性並符合安全法規。在以下兩種環境中會使用通用存取卡：每個機器均隨附智慧卡讀卡機；管理通用存取卡的智慧卡硬體驅動程式通常已預先安裝。

設定用於 vCenter Single Sign-On 的智慧卡驗證時，登入 vCenter Server 或 Platform Services Controller 系統的使用者會收到透過智慧卡和 PIN 組合進行驗證的提示，具體如下：

- 1 使用者將智慧卡插入智慧卡讀卡機時，vCenter Single Sign-On 會讀取卡片上的憑證。

- 2 vCenter Single Sign-On 會提示使用者選取一個憑證，然後提示使用者使用該憑證對應的 PIN。
- 3 vCenter Single Sign-On 會檢查智慧卡上的憑證是否為已知且 PIN 是否正確。如果撤銷檢查已開啟，則 vCenter Single Sign-On 亦會檢查憑證是否已撤銷。
- 4 如果憑證已知，且不是撤銷的憑證，則表示使用者已經過驗證，然後便可以執行其有權執行的工作。

備註 大多數情況下，在測試期間將使用者名稱和密碼驗證保留為啟用狀態有其必要性。測試完成後，停用使用者名稱和密碼驗證並啟用智慧卡驗證。之後，vSphere Client 將僅允許智慧卡登入。僅在機器上擁有根或管理員權限的使用者才能透過直接登入 Platform Services Controller 來重新啟用使用者名稱和密碼。

使用命令列設定智慧卡驗證

您可以使用 `sso-config` 公用程式從命令列設定智慧卡驗證。該公用程式支援所有智慧卡組態工作。

從命令列設定智慧卡驗證時，您始終要先使用 `sso-config` 命令設定 Platform Services Controller。然後，您可以使用 Platform Services Controller Web 介面執行其他工作。

- 1 設定 Platform Services Controller，以便在使用者登入時網頁瀏覽器要求提交智慧卡憑證。
- 2 設定驗證原則。您可以使用 `sso-config` 指令碼或 Platform Services Controller Web 介面來設定原則。支援的驗證類型和撤銷設定的組態儲存在 VMware Directory Service 中，並於 vCenter Single Sign-On 網域中的所有 Platform Services Controller 執行個體之間複寫。

如果啟用了智慧卡驗證，並停用其他驗證方法，則系統會要求使用者使用智慧卡驗證登入。

如果無法從 vSphere Web Client 登入，且使用者名稱和密碼驗證已關閉，根使用者或管理員使用者可以從 Platform Services Controller 命令列執行以下命令來重新開啟使用者名稱和密碼驗證。該範例適用於 Windows；對於 Linux，請使用 `sso-config.sh`。

```
sso-config.bat -set_authn_policy -pwdAuthn true
```

您可以在以下位置找到 `sso-config` 指令碼：

Windows C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config.bat

Linux /opt/vmware/bin/sso-config.sh

必要條件

- 確認您的環境使用的是 Platform Services Controller 6.0 版 Update 2 或更新版本，且您使用的是 vCenter Server 6.0 或更新版本。將 5.5 版節點升級至 6.0 版。
- 確認環境中已設定企業公開金鑰基礎結構 (PKI)，並且憑證符合下列需求：
 - 使用者主體名稱 (UPN) 與主體別名 (SAN) 延伸中的 Active Directory 帳戶相對應。
 - 必須在憑證的 [應用程式原則] 或 [增強金鑰使用方法] 欄位中指定用戶端驗證，否則瀏覽器不會顯示該憑證。
- 確認 Platform Services Controller Web 介面憑證受使用者工作站信任；否則，瀏覽器不會嘗試驗證。

- 設定 Active Directory 身分識別來源，並將其新增至 vCenter Single Sign-On 做為身分識別來源。
- 將 vCenter Server 管理員角色指派給 Active Directory 身分識別來源中的一或多個使用者。隨後這些使用者即可執行驗證，因為他們處於 Active Directory 群組中，且具有 vCenter Server 管理員權限。administrator@vsphere.local 使用者無法執行智慧卡驗證。
- 如果您想要在環境中使用 Platform Services Controller HA 解決方案，請完成所有 HA 組態，然後再設定智慧卡驗證。請參閱 VMware 知識庫文章 [2112085](#) (Windows) 或 [2113315](#) (vCenter Server Appliance)。

程序

- 1 取得憑證，並將其複製到 sso-config 公用程式可存取的資料夾中。

選項	說明
Windows	登入 Platform Services Controller Windows 安裝，並使用 WinSCP 或類似的公用程式來複製檔案。
應用裝置	<ol style="list-style-type: none"> a 直接登入或使用 SSH 登入應用裝置主控台。 b 按如下方式啟用應用裝置 shell。 <pre>shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root</pre> c 使用 WinSCP 或類似公用程式將憑證複製到 Platform Services Controller 上的 /usr/lib/vmware-sso/vmware-sts/conf。 d 按如下方式選擇性地停用應用裝置 shell。 <pre>chsh -s "bin/appliancesh" root</pre>

2 在每個 Platform Services Controller 節點上，使用 sso-config CLI 設定智慧卡驗證設定。

- a 前往 sso-config 指令碼所在的目錄。

選項	說明
Windows	C:\Program Files\VMware\VCenter server\VMware Identity Services
應用裝置	/opt/vmware/bin

- b 執行下列命令：

```
sso-config.[bat|sh] -set_tc_cert_authn -switch true -cacerts
[FirstTrustedCA.cer,SecondTrustedCA.cer,...] -t tenant
```

例如：

```
sso-config.bat -set_tc_cert_authn -switch true -cacerts MySmartCA1.cer -t vsphere.local
```

- c 重新啟動虛擬或實體機器。

```
service-control --stop vmware-std
service-control --start vmware-std
```

3 若要針對 VMware Directory Service (vmdir) 啟用智慧卡驗證，請執行下列命令。

```
sso-config.[bat|sh] -set_authn_policy -certAuthn true -cacerts
first_trusted_cert.cer,second_trusted_cert.cer -t tenant
```

例如：

```
sso-config.[bat|sh] -set_authn_policy -certAuthn true -cacerts
MySmartCA1.cer,MySmartCA2.cer -t vsphere.local
```

如果您指定多個憑證，憑證間不允許有空格。

4 若要停用所有其他驗證方法，請執行以下命令。

```
sso-config.sh -set_authn_policy -pwdAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -winAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -securIDAuthn false -t vsphere.local
```

您可以使用這些命令視需要啟用和停用不同驗證方法。

5 (選擇性) 若要設定憑證原則允許清單，請執行以下命令。

```
sso-config.[bat|sh] -set_authn_policy -certPolicies policies
```

若要指定多個原則，請以命令分隔它們，例如：

```
sso-config.bat -set_authn_policy -certPolicies
2.16.840.1.101.2.1.11.9,2.16.840.1.101.2.1.11.19
```

該允許清單會指定在憑證的憑證原則延伸中允許的原則的物件識別碼。X509 憑證可以擁有憑證原則延伸。

6 (選擇性) 若要列出組態資訊，請執行以下命令。

```
sso-config.[bat|sh] -get_authn_policy -t tenantName
```

使用 Platform Services Controller Web 介面管理智慧卡驗證

您可以在 Platform Services Controller Web 介面中啟用和停用智慧卡驗證、自訂登入橫幅和設定撤銷原則。

從命令列設定智慧卡驗證時，您始終要先使用 `sso-config` 命令設定 Platform Services Controller。然後，您可以使用 Platform Services Controller Web 介面執行其他工作。

- 1 設定 Platform Services Controller，以便在使用者登入時網頁瀏覽器要求提交智慧卡憑證。
- 2 設定驗證原則。您可以使用 `sso-config` 指令碼或 Platform Services Controller Web 介面來設定原則。支援的驗證類型和撤銷設定的組態儲存在 VMware Directory Service 中，並於 vCenter Single Sign-On 網域中的所有 Platform Services Controller 執行個體之間複寫。

如果啟用了智慧卡驗證，並停用其他驗證方法，則系統會要求使用者使用智慧卡驗證登入。

如果無法從 vSphere Web Client 登入，且使用者名稱和密碼驗證已關閉，根使用者或管理員使用者可以從 Platform Services Controller 命令列執行以下命令來重新開啟使用者名稱和密碼驗證。該範例適用於 Windows；對於 Linux，請使用 `sso-config.sh`。

```
sso-config.bat -set_authn_policy -pwdAuthn true
```

必要條件

- 確認您的環境使用的是 Platform Services Controller 6.0 版 Update 2 或更新版本，且您使用的是 vCenter Server 6.0 或更新版本。將 5.5 版節點升級至 6.0 版。
- 確認環境中已設定企業公開金鑰基礎結構 (PKI)，並且憑證符合下列需求：
 - 使用者主體名稱 (UPN) 與主體別名 (SAN) 延伸中的 Active Directory 帳戶相對應。
 - 必須在憑證的 [應用程式原則] 或 [增強金鑰使用方法] 欄位中指定用戶端驗證，否則瀏覽器不會顯示該憑證。
- 確認 Platform Services Controller Web 介面憑證受使用者工作站信任；否則，瀏覽器不會嘗試驗證。
- 設定 Active Directory 身分識別來源，並將其新增至 vCenter Single Sign-On 做為身分識別來源。
- 將 vCenter Server 管理員角色指派給 Active Directory 身分識別來源中的一或多個使用者。隨後這些使用者即可執行驗證，因為他們處於 Active Directory 群組中，且具有 vCenter Server 管理員權限。administrator@vsphere.local 使用者無法執行智慧卡驗證。
- 如果您想要在環境中使用 Platform Services Controller HA 解決方案，請完成所有 HA 組態，然後再設定智慧卡驗證。請參閱 VMware 知識庫文章 [2112085](#) (Windows) 或 [2113315](#) (vCenter Server Appliance)。

程序

- 1 取得憑證，並將其複製到 `sso-config` 公用程式可存取的資料夾中。

選項	說明
Windows	登入 Platform Services Controller Windows 安裝，並使用 WinSCP 或類似的公用程式來複製檔案。
應用裝置	<ol style="list-style-type: none"> a 直接登入或使用 SSH 登入應用裝置主控台。 b 按如下方式啟用應用裝置 shell。 <pre>shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root</pre> c 使用 WinSCP 或類似公用程式將憑證複製到 Platform Services Controller 上的 <code>/usr/lib/vmware-sso/vmware-sts/conf</code>。 d 按如下方式選擇性地停用應用裝置 shell。 <pre>chsh -s "bin/appliancesh" root</pre>

- 2 在每個 Platform Services Controller 節點上，使用 `sso-config` CLI 設定智慧卡驗證設定。

- a 前往 `sso-config` 指令碼所在的目錄。

選項	說明
Windows	<code>C:\Program Files\VMware\VCenter server\VMware Identity Services</code>
應用裝置	<code>/opt/vmware/bin</code>

- b 執行下列命令：

```
sso-config.[bat|sh] -set_tc_cert_authn -switch true -cacerts
[FirstTrustedCA.cer,SecondTrustedCA.cer,...] -t tenant
```

例如：

```
sso-config.bat -set_tc_cert_authn -switch true -cacerts MySmartCA1.cer,MySmartCA2.cer
-t vsphere.local
```

使用逗點分隔多個憑證，但是不要在逗點後加空格。

- c 重新啟動虛擬或實體機器。

```
service-control --stop vmware-std
service-control --start vmware-std
```

- 3 從網頁瀏覽器中，透過指定以下 URL 來連線到 Platform Services Controller：

`https://psc_hostname_or_IP/psc`

在內嵌式部署中，Platform Services Controller 主機名稱或 IP 位址與 vCenter Server 主機名稱或 IP 位址相同。

- 4 指定 administrator@vsphere.local 或 vCenter Single Sign-On 管理員群組的其他成員的使用者名稱和密碼。

如果在安裝期間指定了其他網域，請以 administrator@mydomain 身分登入。

- 5 瀏覽到 **Single Sign-On > 組態**。
- 6 按一下**智慧卡組態**，然後選取**受信任的 CA 憑證**索引標籤。
- 7 若要新增一或多個可信任的憑證，請依序按一下**新增憑證**和**瀏覽**，並從受信任的 CA 中選取所有憑證，然後按一下**確定**。
- 8 若要指定驗證組態，請按一下**驗證組態**旁邊的**編輯**，然後選取或取消選取驗證方法。

您無法從此 Web 介面啟用或停用 RSA SecurID 驗證。但是，如果 RSA SecurID 已透過命令列啟用，則狀態會顯示在 Web 介面中。

設定智慧卡驗證的撤銷原則

您可以自訂憑證撤銷檢查，並可指定 vCenter Single Sign-On 在何處尋找已撤銷憑證的相關資訊。

您可以使用 Platform Services Controller Web 介面或 sso-config 指令碼自訂行為。您選取的設定部分取決於 CA 的支援情況。

- 如果停用撤銷檢查，vCenter Single Sign-On 將略過任何 CRL 或 OCSP 設定。
- 如果啟用撤銷檢查，則建議的設定取決於 PKI 設定。

僅使用 OCSP

如果核發 CA 支援 OCSP 回應程式，請啟用 OCSP 並停止使用 CRL 做為容錯移轉。

僅使用 CRL

如果核發 CA 不支援 OCSP，請啟用 CRL 檢查並停用 OCSP 檢查。

同時使用 OCSP 和 CRL

如果核發 CA 同時支援 OCSP 回應程式和 CRL，vCenter Single Sign-On 將先檢查 OCSP 回應程式。如果回應程式傳回未知狀態或無法使用，vCenter Single Sign-On 會檢查 CRL。在此情況下，請同時啟用 OCSP 檢查和 CRL 檢查，並啟用 CRL 做為 OCSP 的容錯移轉。

- 如果啟用撤銷檢查，進階使用者可以指定下列其他設定。

OCSP URL

依預設，vCenter Single Sign-On 將檢查正在接受驗證之憑證中所定義的 OCSP 回應程式的位置。如果憑證中不存在授權機構資訊存取延伸，或者您想要將其覆寫（例如，由於其無法在您的環境中使用），您可以明確指定位置。

使用來自憑證的 CRL

依預設，vCenter Single Sign-On 會檢查正在接受驗證之憑證中所定義的 CRL 的位置。當憑證中不存在 CRL 發佈點延伸，或者您想要覆寫預設值時，請停用此選項。

CRL 位置

如果您停用**使用來自憑證的 CRL**，並且想要指定 CRL 所在的位置 (檔案或 HTTP URL)，請使用此內容。

此外，您還可以透過新增憑證原則，進一步限制 vCenter Single Sign-On 接受的憑證。

必要條件

- 確認您的環境使用的是 Platform Services Controller 6.0 版 Update 2 或更新版本，且您使用的是 vCenter Server 6.0 版或更新版本。將 5.5 版節點升級至 6.0 版。
- 確認環境中已設定企業公開金鑰基礎結構 (PKI)，並且憑證符合下列需求：
 - 使用者主體名稱 (UPN) 與主體別名 (SAN) 延伸中的 Active Directory 帳戶相對應。
 - 必須在憑證的 [應用程式原則] 或 [增強金鑰使用方法] 欄位中指定用戶端驗證，否則瀏覽器不會顯示該憑證。
- 確認 Platform Services Controller Web 介面憑證受使用者工作站信任；否則，瀏覽器不會嘗試驗證。
- 設定 Active Directory 身分識別來源，並將其新增至 vCenter Single Sign-On 做為身分識別來源。
- 將 vCenter Server 管理員角色指派給 Active Directory 身分識別來源中的一或多個使用者。隨後這些使用者即可執行驗證，因為他們處於 Active Directory 群組中，且具有 vCenter Server 管理員權限。administrator@vsphere.local 使用者無法執行智慧卡驗證。
- 如果您想要在環境中使用 Platform Services Controller HA 解決方案，請完成所有 HA 組態，然後再設定智慧卡驗證。請參閱 VMware 知識庫文章 [2113085](#) (Windows) 或 [2113315](#) (vCenter Server Appliance)。

程序

- 1 從網頁瀏覽器中，透過指定以下 URL 來連線到 Platform Services Controller：

`https://psc_hostname_or_IP/psc`

在內嵌式部署中，Platform Services Controller 主機名稱或 IP 位址與 vCenter Server 主機名稱或 IP 位址相同。

- 2 指定 administrator@vsphere.local 或 vCenter Single Sign-On 管理員群組的其他成員的使用者名稱和密碼。

如果在安裝期間指定了其他網域，請以 administrator@mydomain 身分登入。

- 3 瀏覽到 **Single Sign-On > 組態**。
- 4 按一下**憑證撤銷設定**，然後啟用或停用撤銷檢查。
- 5 如果憑證原則已在您的環境中生效，您可以在**憑證原則已接受**窗格中新增原則。

設定 RSA SecurID 驗證

您可以將環境設為要求使用者使用 RSA SecurID Token (而非密碼) 登入。SecurID 僅支援透過命令列進行設定。

如需詳細資料，請參閱有關 [RSA SecurID 設定](#) 的兩篇 vSphere 部落格文章。

備註 RSA Authentication Manager 需要使用者 ID 為使用 1 至 255 ASCII 字元的唯一識別碼。不允許使用 & 符號 (&)、百分號 (%)、大於 (>)、小於 (<) 和單引號 (') 等字元。

必要條件

- 確認您的環境使用的是 Platform Services Controller 6.0 版 Update 2 或更新版本，且您使用的是 vCenter Server 6.0 版或更新版本。將 5.5 版節點升級至 6.0 版。
- 確認已正確設定您環境中的 RSA Authentication Manager，且使用者擁有 RSA Token。需要 RSA Authentication Manager 8.0 版或更新版本。
- 確認已將 RSA Manager 使用的身分識別來源新增至 vCenter Single Sign-On。請參閱[新增 vCenter Single Sign-On 身分識別來源](#)。
- 確認 RSA Authentication Manager 系統能夠解析 Platform Services Controller 主機名稱，並且 Platform Services Controller 系統能夠解析 RSA Authentication Manager 主機名稱。
- 透過選取 **存取 > 驗證代理程式 > 產生組態檔**，從 RSA Manager 匯出 `sdconf.rec` 檔案。解壓縮產生的 `AM_Config.zip` 檔案，以尋找 `sdconf.rec` 檔案。
- 將 `sdconf.rec` 檔案複製到 Platform Services Controller 節點。

程序

- 1 變更至 `sso-config` 指令碼所在的目錄。

選項	說明
Windows	C:\Program Files\VMware\VCenter server\VMware Identity Services
應用裝置	/opt/vmware/bin

- 2 若要啟用 RSA SecurID 驗證，請執行以下命令。

```
sso-config.[sh|bat] -t tenantName -set_authn_policy -securIDAuthn true
```

tenantName 是 vCenter Single Sign-On 網域的名稱，依預設為 `vsphere.local`。

- 3 (選擇性) 若要停用其他驗證方法，請執行以下命令。

```
sso-config.sh -set_authn_policy -pwdAuthn false -winAuthn false -certAuthn false -t vsphere.local
```

- 4 若要設定環境以使目前站台上的承租人使用 RSA 站台，請執行以下命令。

```
sso-config.[sh|bat] -set_rsa_site [-t tenantName] [-siteID Location] [-agentName Name] [-sdConfFile Path]
```

例如：

```
sso-config.sh -set_rsa_site -agentName SSO_RSA_AUTHSDK_AGENT -sdConfFile /tmp/sdconf.rec
```

您可以指定下列選項。

選項	說明
siteID	選擇性 Platform Services Controller 站台識別碼 Platform Services Controller 在每個站台上支援一個 RSA Authentication Manager 執行個體或叢集。如果您不明確指定此選項，則 RSA 組態會用於目前 Platform Services Controller 站台。僅在您新增其他站台時使用此選項。
agentName	在 RSA Authentication Manager 中定義。
sdConfFile	從 RSA Manager 下載，並包含諸如 IP 位址等 RSA Manager 組態資訊的 sdconf.rec 檔案複本。

- 5 (選擇性) 若要將承租人組態變更為非預設值，請執行下列命令。

```
sso-config.[sh|bat] -set_rsa_config [-t tenantName] [-logLevel Level] [-logFileSize Size] [-maxLogFileCount Count] [-connTimeOut Seconds] [-readTimeOut Seconds] [-encAlgList Alg1,Alg2,...]
```

預設值通常是適用的，例如：

```
sso-config.sh -set_rsa_config -t vsphere.local -logLevel DEBUG
```

- 6 (選擇性) 如果您的身分識別來源未使用使用者主體名稱做為使用者識別碼，請設定身分識別來源 userID 屬性。

userID 屬性可判定哪個 LDAP 屬性會用做 RSA userID。

```
sso-config.[sh|bat] -set_rsa_userid_attr_map [-t tenantName] [-idsName Name] [-ldapAttr AttrName] [-siteID Location]
```

例如：

```
sso-config.sh -set_rsa_userid_attr_map -t vsphere.local -idsName ssolabs.com -ldapAttr userPrincipalName
```

- 7 若要顯示目前設定，請執行下列命令。

```
sso-config.sh -t tenantName -get_rsa_config
```

結果

如果停用使用者名稱與密碼驗證並啟用 SecurID Token 驗證，則使用者必須使用其使用者名稱和 SecurID Token 登入。使用者名稱和密碼登入已無法繼續使用。

管理登入橫幅

從 vSphere 6.0 Update 2 開始，您可以在環境中加入登入橫幅。您可以顯示部分文字或者要求使用者按一下核取方塊 (例如，用以表示接受條款與條件)。您可以啟用和停用登入橫幅，也可以要求使用者按一下明確同意核取方塊。

程序

- 1 從網頁瀏覽器中，透過指定以下 URL 來連線到 Platform Services Controller：

`https://psc_hostname_or_IP/psc`

在內嵌式部署中，Platform Services Controller 主機名稱或 IP 位址與 vCenter Server 主機名稱或 IP 位址相同。

- 2 指定 administrator@vsphere.local 或 vCenter Single Sign-On 管理員群組的其他成員的使用者名稱和密碼。

如果在安裝期間指定了其他網域，請以 administrator@mydomain 身分登入。

- 3 在 Single Sign-On 下，選取**組態**，然後按一下**登入橫幅**索引標籤。
- 4 按一下**編輯**並設定登入橫幅。

選項	說明
狀態	按一下 已啟用 核取方塊，以啟用登入橫幅。除非按一下此核取方塊，否則無法變更其他欄位。
明確同意	按一下 明確同意 核取方塊，以要求使用者在登入前按一下核取方塊。也可以顯示不含核取方塊的訊息。
標題	橫幅的標題。依預設，登入橫幅文字為 I agree to the。您可以在其中新增 Terms and Conditions 等內容。
訊息	使用者按一下橫幅後看到的訊息。例如，條款與條件的文字。如果您使用明確同意，則該訊息為必填。

針對其他服務提供者將 vCenter Single Sign-On 用做身分識別提供者

vSphere Web Client 會以受信任的 SAML 2.0 服務提供者 (SP) 的身分自動登錄 vCenter Single Sign-On。您可以將其他受信任的服務提供者新增至充當 SAML 身分識別提供者 (IDP) 的 vCenter Single Sign-On 所在的識別身分同盟。服務提供者必須符合 SAML 2.0 通訊協定。在設定聯盟之後，如果使用者可以向 vCenter Single Sign-On 進行驗證，則服務提供者會授與該使用者存取權。

備註 vCenter Single Sign-On 可以為其他 SP 的 IDP。vCenter Single Sign-On 不能為使用其他 IDP 的 SP。

已登錄的 SAML 服務提供者可以授與已擁有即時工作階段的使用者 (即已登入身分識別提供者的使用者) 存取權。例如，vRealize Automation 7.0 及更新版本支援 vCenter Single Sign-On 做為身分識別提供者。您可以從 vCenter Single Sign-On 和 vRealize Automation 設定聯盟。在此之後，vCenter Single Sign-On 可以在您登入 vRealize Automation 時執行驗證。

若要將 SAML 服務提供者加入識別身分同盟，您必須透過在 SP 與 IDP 之間交換 SAML 中繼資料來設定它們之間的信任。

您必須同時對 vCenter Single Sign-On 及使用 vCenter Single Sign-On 的服務執行整合工作。

1 將 IDP 中繼資料匯出至檔案，然後將其匯入 SP。

2 匯出 SP 中繼資料並將其匯入 IDP。

您可以使用 vCenter Single Sign-On 的 vSphere Web Client 介面來匯出 IDP 中繼資料，並從 SP 匯入中繼資料。如果您是使用 vRealize Automation 做為 SP，請參閱 vRealize Automation 說明文件，以取得有關匯出 SP 中繼資料和匯入 IDP 中繼資料的詳細資料。

備註 服務必須完全支援 SAML 2.0 標準，否則整合將無法運作。

新增 SAML 服務提供者

您可以將 SAML 服務提供者新增至 vCenter Single Sign-On，並將 vCenter Single Sign-On 做為身分識別提供者新增至該服務。之後，當使用者登入服務提供者時，服務提供者會透過 vCenter Single Sign-On 對這些使用者進行驗證。

如果希望將 VMware vRealize Automation 7.0 及更新版本隨附的 Single Sign-On 解決方案與 vCenter Single Sign-On 身分識別提供者進行整合，或者如果正在使用其他外部 SAML 服務提供者，則可以使用該程序。

該程序涉及將 SAML 服務提供者的中繼資料匯入至 vCenter Single Sign-On，以及將 vCenter Single Sign-On 中繼資料匯入至 SAML 服務提供者，以使兩個提供者可以共用全部資料。

必要條件

目標服務必須完全支援 SAML 2.0 標準。

如果中繼資料沒有準確遵循 SAML 2.0 中繼資料架構，您可能必須在匯入前對架構進行編輯。例如，如果使用 Active Directory Federation Services (ADFS) SAML 服務提供者，則必須先編輯中繼資料，然後才能將其匯入。移除以下非標準元素：

```
fed:ApplicationServiceType
fed:SecurityTokenServiceType
```

目前無法從 vSphere Web Client 匯入 SAML IDP 中繼資料。

程序

1 將服務提供者的中繼資料匯出至檔案。

2 將服務提供者的中繼資料匯入 vCenter Single Sign-On。

- a 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。

具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。

- b 瀏覽到 **Single Sign-On > 組態**。
- c 選取 **SAML 服務提供者索引標籤**。
- d 在來自您的 **SAML 服務提供者**的中繼資料欄位中，按一下**匯入**，並在對話方塊中貼上 XML 字串，或者按一下**從檔案匯入**以匯入檔案，然後按一下**匯入**。

3 匯出 vCenter Single Sign-On 中繼資料。

- a 在您的 **SAML 服務提供者**的中繼資料欄位中，按一下**下載**。
- b 指定檔案位置。

4 前往 SAML 服務提供者 (例如 VMware vRealize Automation 7.0 或更新版本)，然後依照 SAML 服務提供者的指示，將 vCenter Single Sign-On 中繼資料新增至該服務提供者。

如需有關匯入中繼資料的詳細資料，請參閱 vRealize Automation 說明文件。

安全性 Token 服務 STS

vCenter Single Sign-On 安全性 Token 服務 (STS) 是一項核發、驗證和更新安全性 Token 的 Web 服務。

為取得 SAML Token，使用者可向 STS 介面出示其主要認證。主要認證取決於使用者的類型。

使用者

vCenter Single Sign-On 身分識別來源中可用的使用者名稱和密碼。

應用程式使用者

有效憑證。

STS 會根據主要認證對使用者進行驗證，並建構包含使用者屬性的 SAML Token。STS 會透過其 STS 簽署憑證來簽署 SAML Token，然後將 Token 指派給使用者。依預設，STS 簽署憑證由 VMCA 產生。您可以從 vSphere Web Client 取代預設的 STS 簽署憑證。除非您公司的安全性原則要求取代所有憑證，否則請勿取代 STS 簽署憑證。

使用者擁有 SAML Token 後，可能會透過各種 Proxy 將 SAML Token 做為該使用者 HTTP 要求的一部分進行傳送。只有預期收件者 (服務提供者) 才可以使用 SAML Token 中的資訊。

在應用裝置上產生新的 STS 簽署憑證

如果您想要取代預設 vCenter Single Sign-On Security Token Service (STS) 簽署憑證，則必須產生新憑證並將其新增至 Java 金鑰儲存區。此程序說明了內嵌式部署應用裝置或外部 Platform Services Controller 應用裝置的步驟。

備註 此憑證有效期為十年，且不是對外憑證。如果不是公司的安全政策要求，請勿取代此憑證。

如果您正在執行 Platform Services Controller Windows 安裝，請參閱在 [vCenter Windows 安裝上產生新 STS 簽署憑證](#)。

程序

- 1 建立頂層目錄以存放新憑證，並確認目錄的位置。

```
mkdir newsts
cd newsts
pwd
#resulting output: /root/newst
```

- 2 將 certtool.cfg 檔案複製到新目錄。

```
cp /usr/lib/vmware-vmca/share/config/certtool.cfg /root/newsts
```

- 3 開啟 certtool.cfg 檔案的複本，然後對其進行編輯以使用本機 Platform Services Controller IP 位址和主機名稱。

國家/地區是必要的，並且必須是兩個字元，如以下範例所示。

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

- 4 產生金鑰。

```
/usr/lib/vmware-vmca/bin/certtool --server localhost --genkey --privkey=/root/newsts/sts.key --pubkey=/root/newsts/sts.pub
```

5 產生憑證

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=/root/newsts/newsts.cer --privkey=/root/newsts/sts.key --config=/root/newsts/certool.cfg
```

6 將憑證轉換為 PK12 格式。

```
openssl pkcs12 -export -in /root/newsts/newsts.cer -inkey /root/newsts/sts.key -certfile /etc/vmware-sso/keys/ssoserverRoot.crt -name "newstssigning" -passout pass:changeme -out newsts.p12
```

7 將憑證新增到 Java 金鑰存放區 (JKS)。

```
/usr/java/jre-vmware/bin/keytool -v -importkeystore -srckeystore newsts.p12 -srcstoretype pkcs12 -srcstorepass changeme -srcalias newstssigning -destkeystore root-trust.jks -deststoretype JKS -deststorepass testpassword -destkeypass testpassword

/usr/java/jre-vmware/bin/keytool -v -importcert -keystore root-trust.jks -deststoretype JKS -storepass testpassword -keypass testpassword -file /etc/vmware-sso/keys/ssoserverRoot.crt -alias root-ca
```

8 當收到提示時，輸入 **Yes** 以接受新增至金鑰儲存區的憑證。

後續步驟

現在您可以匯入新憑證。請參閱[重新整理安全性 Token 服務憑證](#)。

在 vCenter Windows 安裝上產生新 STS 簽署憑證

如果想要取代預設 STS 簽署憑證，您必須先產生新憑證並將其新增到 Java 金鑰存放區。此程序會說明 Windows 安裝的步驟。

備註 此憑證有效期為十年，且不是對外憑證。如果不是公司的安全政策要求，請勿取代此憑證。

如果您正在使用虛擬應用裝置，請參閱[在應用裝置上產生新的 STS 簽署憑證](#)。

程序

1 建立新目錄以保存新憑證。

```
cd C:\ProgramData\VMware\vCenterServer\cfg\sso\keys\
mkdir newsts
cd newsts
```

2 建立 certool.cfg 檔案的複本，並將其放在新目錄中。

```
copy "C:\Program Files\VMware\vCenter Server\vmcad\certool.cfg" .
```


- 開啟 `certool.cfg` 檔案的複本，然後對其進行編輯以使用本機 Platform Services Controller IP 位址和主機名稱。

需要輸入國家/地區，並且必須為兩個字元。以下範例對此進行了說明。

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

- 產生金鑰。

```
"C:\Program Files\VMware\VCenter Server\vmcad\certool.exe" --server localhost --genkey --
privkey=sts.key --pubkey=sts.pub
```

- 產生憑證。

```
"C:\Program Files\VMware\VCenter Server\vmcad\certool.exe" --gencert --cert=newsts.cer --
privkey=sts.key --config=certool.cfg
```

- 將憑證轉換為 PK12 格式。

```
"C:\Program Files\VMware\VCenter Server\openSSL\openssl.exe" pkcs12 -export -in newsts.cer
-inkey sts.key -certfile ..\ssoserverRoot.crt -name "newstssigning" -passout pass:changeme
-out newsts.p12
```

- 將憑證新增到 Java 金鑰存放區 (JKS)。

```
"C:\Program Files\VMware\VCenter Server\jre\bin\keytool.exe" -v -importkeystore
-srckeystore newsts.p12 -srcstoretype pkcs12 -srcstorepass changeme -srcalias
newstssigning -destkeystore root-trust.jks -deststoretype JKS -deststorepass testpassword
-destkeypass testpassword
"C:\Program Files\VMware\VCenter Server\jre\bin\keytool.exe" -v -importcert -keystore root-
trust.jks -deststoretype JKS -storepass testpassword -keypass testpassword
-file ..\ssoserverRoot.crt -alias root-ca
```

後續步驟

現在您可以匯入新憑證。請參閱[重新整理安全性 Token 服務憑證](#)。

重新整理安全性 Token 服務憑證

vCenter Single Sign-On 伺服器包含安全性 Token 服務 (STS)。安全性 Token 服務是一項核發、驗證和續訂安全性 Token 的 Web 服務。當現有的安全性 Token 服務憑證到期或變更時，您可從 vSphere Web Client 手動重新整理。

若要取得 SAML Token，使用者需要為安全性 Token 服務 (STS) 提供主要認證。主要認證取決於使用者的類型：

解決方案使用者

有效憑證

其他使用者

vCenter Single Sign-On 身分識別來源中可用的使用者名稱和密碼。

STS 使用主要認證對使用者進行驗證，並建構包含使用者屬性的 SAML Token。STS 服務將透過其 STS 簽署憑證來簽署 SAML Token，然後將 Token 指派給使用者。依預設，STS 簽署憑證由 VMCA 產生。

使用者擁有 SAML Token 後，可能會透過各種 Proxy 將 SAML Token 做為該使用者 HTTP 要求的一部分進行傳送。只有預期收件者 (服務提供者) 才可以使用 SAML Token 中的資訊。

如果公司原則要求或者您想要更新到期的憑證，可取代現有 STS 簽署憑證 vSphere Web Client。

注意 請勿取代檔案系統中的檔案。如果取代，則會導致未預期及難以進行偵錯的錯誤。

備註 當取代憑證後，您必須重新啟動節點以同時重新啟動 vSphere Web Client 服務與 STS 服務。

必要條件

將剛從 Platform Services Controller 新增到 Java 金鑰儲存區的憑證複製到本機工作站。

Platform Services Controller 應用裝置

`certificate_location/keys/root-trust.jks` 例如：`/keys/root-trust.jks`

例如：

`/root/newsts/keys/root-trust.jks`

Windows 安裝

`certificate_location\root-trust.jks`

例如：

`C:\Program Files\VMware\vCenter Server\jre\bin\root-trust.jks`

程序

- 1 以 `administrator@vsphere.local` 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。

具有 vCenter Single Sign-On 管理員權限的使用者位於 `vsphere.local` 網域的管理員群組中。

- 2 依序選取**憑證**索引標籤和 **STS 簽署**子索引標籤，然後按一下**新增 STS 簽署憑證**圖示。
- 3 新增憑證。
 - a 按一下**瀏覽**可瀏覽到包含新憑證的金鑰存放區 JKS 檔案，然後按一下**開啟**。
 - b 收到提示時，輸入密碼。
 - c 按一下頂部的 STS 別名連結，然後按一下**確定**。
 - d 收到提示時，再次輸入密碼。
- 4 按一下**確定**。
- 5 重新啟動 Platform Services Controller 節點以同時啟動 STS 服務和 vSphere Web Client。
重新啟動前，驗證無法正確地工作，所以重新啟動是必要的。

判定 LDAPS SSL 憑證的到期日期

如果選取 Active Directory LDAP Server 和 OpenLDAP Server 身分識別來源並決定使用 LDAPS，則您可以為 LDAP 流量上傳 SSL 憑證。SSL 憑證在預先定義的週期之後到期。知道憑證何時到期，可讓您在到期日期之前取代或更新憑證。

僅在使用 Active Directory LDAP Server 和 OpenLDAP Server 並為伺服器指定 **ldaps://** URL 時，您才會看到到期資訊。對於其他類型的身分識別來源或 **ldap://** 流量，[身分識別來源信任存放區] 索引標籤會保持空白。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。
具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。
- 2 瀏覽到**管理 > Single Sign-On > 組態**。
- 3 按一下**憑證**索引標籤，然後按一下**身分識別來源信任存放區**子索引標籤。
- 4 找到憑證，並在**有效期至**文字方塊中驗證到期日期。
您可能會在索引標籤的頂部看到一則警告，指示憑證即將到期。

管理 vCenter Single Sign-On 原則

vCenter Single Sign-On 原則會在您的環境中強制執行安全性規則。您可以檢視並編輯預設的 vCenter Single Sign-On 密碼、鎖定原則以及 Token 原則。

編輯 vCenter Single Sign-On 密碼原則

vCenter Single Sign-On 密碼原則是有關 vCenter Single Sign-On 使用者密碼格式和到期時間的一組規則和限制。此密碼原則僅適用於 vCenter Single Sign-On 網域 (vsphere.local) 中的使用者。

依預設，vCenter Single Sign-On 密碼會在 90 天後到期。vSphere Web Client 會在密碼即將到期時提醒您。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。

具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。

- 2 瀏覽到 **管理 > Single Sign-On > 組態**。
- 3 按一下 **原則索引標籤**，然後選取 **密碼原則**。
- 4 按一下 **編輯**。
- 5 編輯密碼原則參數。

選項	說明
說明	密碼原則說明。
存留時間上限	使用者必須變更密碼前，密碼可存在的天數上限。
限制重複使用	無法選取之使用者先前密碼的數目。例如，如果使用者不能重複使用最後六個密碼中的任何一個，則輸入 6。
長度上限	允許密碼包含的字元數上限。
最小長度	密碼必須包含的最小字元數目。最小長度不得少於字母、數字和特殊字元需求的最小總和。
字元需求	<p>密碼必須包含的不同字元類型的最小數目。您可以按照以下方式指定每種類型字元的數目：</p> <ul style="list-style-type: none"> ■ 特殊字元：& # % ■ 字母：A b c D ■ 大寫：A B C ■ 小寫：a b c ■ 數字：1 2 3 <p>最小字母字元數不得少於大寫和小寫需求的總和。</p> <p>在 vSphere 6.0 及更新版本中，密碼支援使用非 ASCII 字元。在舊版 vCenter Single Sign-On 中，受支援的字元則存在限制。</p>
相同的相鄰字元	允許密碼包含的相同相鄰字元數的上限。該數值必須大於 0。例如，如果輸入 1，則不允許使用以下密碼：p@\$word。

- 6 按一下 **確定**。

編輯 vCenter Single Sign-On 鎖定原則

vCenter Single Sign-On 鎖定原則指定使用者的 vCenter Single Sign-On 帳戶鎖定條件，在使用者嘗試使用不正確的認證登入時，系統會依據這些條件鎖定使用者的帳戶。您可以編輯鎖定原則。

如果使用者多次嘗試使用錯誤的密碼登入 vsphere.local，則使用者將被鎖定。透過鎖定原則，您可以指定連續嘗試登入失敗的次數上限，以及兩次嘗試登入失敗之間的時間長。該原則還指定在自動解除鎖定帳戶之前必須經過的時間長。

備註 鎖定原則僅適用於使用者帳戶，而不適用於系統帳戶 (例如 administrator@vsphere.local)。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。

具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。

- 2 瀏覽到**管理 > Single Sign-On > 組態**。
- 3 按一下**原則索引標籤**，然後選取**鎖定原則**。
- 4 按一下**編輯**。
- 5 編輯參數。

選項	說明
說明	鎖定原則的選擇性說明。
嘗試登入失敗的次數上限	在鎖定帳戶之前允許的嘗試登入失敗次數上限。
兩次失敗之間的時間間隔	必須發生嘗試登入失敗才會觸發鎖定的期間。
解除鎖定時間	帳戶保持鎖定狀態的時間量。如果輸入 0，則管理員必須明確地解除鎖定帳戶。

- 6 按一下**確定**。

編輯 vCenter Single Sign-On Token 原則

vCenter Single Sign-On Token 原則指定時鐘容限、續訂計數以及其他 Token 內容。您可以編輯 vCenter Single Sign-On Token 原則，確保 Token 規格符合貴公司的安全性標準。

程序

- 1 登入 vSphere Web Client。
- 2 選取**系統管理 > Single Sign-On**，然後選取**組態**。
- 3 按一下**原則索引標籤**，然後選取**Token 原則**。

vSphere Web Client 將顯示目前的組態設定。如果您未修改預設設定，vCenter Single Sign-On 將使用這些設定。

- 4 編輯 Token 原則組態參數。

選項	說明
時鐘容限	vCenter Single Sign-On 容許用戶端時鐘與網域控制站時鐘之間存在的時間差異 (以毫秒為單位)。如果時間差異大於指定值，則 vCenter Single Sign-On 將宣告 Token 無效。
Token 續訂計數上限	可以續訂 Token 的數目上限。超過續訂嘗試數目上限後，需要使用新的安全性 Token。
Token 委派計數上限	可以將金鑰持有者 Token 委派給 vSphere 環境中的服務。使用所委派 Token 的服務將代表提供該 Token 的主體執行服務。Token 要求會指定 DelegateTo 身分。DelegateTo 值可以是解決方案 Token，也可以是對解決方案 Token 的參考。此值指定可以委派單一金鑰持有者 Token 的次數。

選項	說明
Bearer Token 存留時間上限	Bearer Token 僅根據 Token 的佔有情況提供驗證。Bearer Token 用於短期的單一作業。Bearer Token 不驗證傳送要求的使用者或實體的身分。此值在重新發出 Bearer Token 前指定該 Token 的存留時間值。
金鑰持有者 Token 存留時間上限	金鑰持有者 Token 根據 Token 中的內嵌式安全性構件提供驗證。金鑰持有者 Token 可用於委派。用戶端可以取得金鑰持有者 Token 並將該 Token 委派給其他實體。該 Token 包含用於識別建立方和委派方的聲明。在 vSphere 環境中，vCenter Server 系統會代表使用者取得委派的 Token，並使用這些 Token 執行作業。 此值決定在將金鑰持有者 Token 標記為無效前該 Token 的存留時間。

5 按一下確定。

管理 vCenter Single Sign-On 使用者和群組

vCenter Single Sign-On 管理員使用者可以從 vSphere Web Client 管理 vsphere.local 網域中的使用者和群組。

vCenter Single Sign-On 管理員使用者可以執行以下工作。

■ 新增 vCenter Single Sign-On 使用者

vSphere Web Client 的**使用者**索引標籤中列出的使用者在 vCenter Single Sign-On 內部，屬於 vsphere.local 網域。

■ 停用和啟用 vCenter Single Sign-On 使用者

如果停用 vCenter Single Sign-On 使用者帳戶，則使用者無法登入 vCenter Single Sign-On 伺服器，除非管理員啟用該帳戶。可以從 vSphere Web Client 介面停用和啟用使用者。

■ 刪除 vCenter Single Sign-On 使用者

您可以從 vCenter Single Sign-On 刪除 vsphere.local 網域中的使用者。無法從 vSphere Web Client 刪除本機作業系統使用者或其他網域中的使用者。

■ 編輯 vCenter Single Sign-On 使用者

您可以從 vSphere Web Client 中變更 vCenter Single Sign-On 使用者的密碼或其他詳細資料。您無法在 vsphere.local 網域中重新命名使用者。換句話說，您無法重新命名 administrator@vsphere.local。

■ 新增 vCenter Single Sign-On 群組

在 vCenter Single Sign-On 中，**群組**索引標籤上列出的群組位於 vCenter Single Sign-On 內部。透過群組可以為一系列群組成員 (主體) 建立容器。

■ 向 vCenter Single Sign-On 群組新增成員

vCenter Single Sign-On 群組的成員可以是來自一或多個身分識別來源的使用者或其他群組。您可以從 vSphere Web Client 中新增成員。

■ 從 vCenter Single Sign-On 群組中移除成員

您可以透過 vSphere Web Client 從 vCenter Single Sign-On 群組中移除成員。從本機群組中移除成員 (使用者或群組) 並不會將該成員從系統中刪除。

■ 刪除 vCenter Single Sign-On 解決方案使用者

vCenter Single Sign-On 會顯示解決方案使用者。解決方案使用者是服務的集合。已預先定義多個 vCenter Server 解決方案使用者，並會在安裝過程中向 vCenter Single Sign-On 驗證。例如，在進行疑難排解時，如果解除安裝未徹底完成，可從 vSphere Web Client 刪除個別解決方案使用者。

■ 變更 vCenter Single Sign-On 密碼

本機網域中的使用者 (依預設為 vsphere.local) 可以從 Web 介面變更其 vCenter Single Sign-On 密碼。其他網域中的使用者變更其密碼時應遵循對應網域的規則。

新增 vCenter Single Sign-On 使用者

vSphere Web Client 的**使用者索引**標籤中列出的使用者在 vCenter Single Sign-On 內部，屬於 vsphere.local 網域。

您可以選取其他網域並檢視這些網域中使用者的相關資訊，但是，您無法從 vSphere Web Client 的 vCenter Single Sign-On 管理介面將使用者新增到其他網域。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。

具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。

- 2 按一下**首頁**，然後瀏覽到**管理 > Single Sign-On > 使用者和群組**。
- 3 如果 vsphere.local 不是目前選取的網域，請從下拉式功能表中選取此網域。

您不能將使用者新增到其他網域。

- 4 在**使用者索引**標籤上，按一下**新增使用者**圖示。

- 5 輸入新使用者的使用者名稱和密碼。

建立使用者後，將不能變更使用者名稱。

密碼必須符合系統的密碼原則需求。

- 6 (選擇性) 輸入新使用者的名字和姓氏。
- 7 (選擇性) 輸入此使用者的電子郵件地址和說明。
- 8 按一下**確定**。

結果

新增使用者時，該使用者最初沒有執行管理作業的權限。

後續步驟

將使用者新增至 vsphere.local 網域中的群組，例如，可管理 VMCA (CAAdmins) 的使用者群組或可管理 vCenter Single Sign-On (管理員) 的使用者群組。請參閱[向 vCenter Single Sign-On 群組新增成員](#)。

停用和啟用 vCenter Single Sign-On 使用者

如果停用 vCenter Single Sign-On 使用者帳戶，則使用者無法登入 vCenter Single Sign-On 伺服器，除非管理員啟用該帳戶。可以從 vSphere Web Client 介面停用和啟用使用者。

停用的使用者帳戶在 vCenter Single Sign-On 系統中仍可用，但是使用者無法在伺服器上登入或執行作業。具有管理員權限的使用者可從 vCenter [使用者和群組] 頁面中停用和啟用使用者。

必要條件

您必須是 vCenter Single Sign-On 管理員群組的成員，才能停用和啟用 vCenter Single Sign-On 使用者。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。

具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。

- 2 按一下**首頁**，然後瀏覽到**管理 > Single Sign-On > 使用者和群組**。
- 3 選取使用者，按一下**停用**圖示，然後在系統提示時按一下**是**。
- 4 若要再次啟用該使用者，請在該使用者上按一下滑鼠右鍵，選取**啟用**，然後在系統提示時按一下**是**。

刪除 vCenter Single Sign-On 使用者

您可以從 vCenter Single Sign-On 刪除 vsphere.local 網域中的使用者。無法從 vSphere Web Client 刪除本機作業系統使用者或其他網域中的使用者。

注意 如果您刪除了 vsphere.local 網域中的管理員使用者，則將無法再登入 vCenter Single Sign-On。請重新安裝 vCenter Server 及其元件。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。

具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。

- 2 按一下**首頁**，然後瀏覽到**管理 > Single Sign-On > 使用者和群組**。
- 3 選取**使用者索引標籤**，然後選取 vsphere.local 網域。
- 4 在使用者清單中，選取要刪除的使用者，然後按一下**刪除**圖示。

請謹慎執行作業。您無法復原此動作。

編輯 vCenter Single Sign-On 使用者

您可以從 vSphere Web Client 中變更 vCenter Single Sign-On 使用者的密碼或其他詳細資料。您無法在 vsphere.local 網域中重新命名使用者。換句話說，您無法重新命名 administrator@vsphere.local。

您可以建立權限與 administrator@vsphere.local 相同的其他使用者。

vCenter Single Sign-On 使用者儲存在 vCenter Single Sign-On vsphere.local 網域中。

您可以從 vSphere Web Client 中檢閱 vCenter Single Sign-On 密碼原則。以 administrator@vsphere.local 身分登入，並選取**組態 > 原則 > 密碼原則**。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。

具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。

- 2 按一下**首頁**，然後瀏覽到**管理 > Single Sign-On > 使用者和群組**。
- 3 按一下**使用者**索引標籤。
- 4 在使用者上按一下滑鼠右鍵，然後選取**編輯使用者**。

- 5 對使用者進行變更。

您無法變更使用者名稱。

密碼必須符合系統的密碼原則需求。

- 6 按一下**確定**。

新增 vCenter Single Sign-On 群組

在 vCenter Single Sign-On 中，**群組**索引標籤上列出的群組位於 vCenter Single Sign-On 內部。透過群組可以為一系列群組成員 (主體) 建立容器。

從 vCenter Single Sign-On 管理介面新增 vSphere Web Client 群組時，該群組將新增到 vsphere.local 網域。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。

具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。

- 2 按一下**首頁**，然後瀏覽到**管理 > Single Sign-On > 使用者和群組**。
- 3 選取**群組**索引標籤上，然後按一下**新增群組**圖示。
- 4 輸入群組的名稱與說明。

建立群組後，將不能變更群組名稱。

- 5 按一下**確定**。

後續步驟

- 向群組新增成員。

向 vCenter Single Sign-On 群組新增成員

vCenter Single Sign-On 群組的成員可以是來自一或多個身分識別來源的使用者或其他群組。您可以從 vSphere Web Client 中新增成員。

您可以將 Microsoft Active Directory 或 OpenLDAP 群組的成員新增到 vCenter Single Sign-On 群組。您無法將群組從外部身分識別來源新增到 vCenter Single Sign-On 群組。

vSphere Web Client 中群組索引標籤上列出的群組屬於 vsphere.local 網域。請參閱 [vsphere.local 網域中的群組](#)。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。

具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。

- 2 按一下**首頁**，然後瀏覽到**管理 > Single Sign-On > 使用者和群組**。
- 3 按一下**群組**索引標籤，然後按一下群組 (例如 [管理員])。
- 4 在 [群組成員] 區域中，按一下**新增成員**圖示。
- 5 選取包含要新增到群組之成員的身分識別來源。
- 6 (選擇性) 輸入搜尋詞彙，然後按一下**搜尋**。
- 7 選取成員，然後按一下**新增**。

您可以同時新增多個成員。

- 8 按一下**確定**。

從 vCenter Single Sign-On 群組中移除成員

您可以透過 vSphere Web Client 從 vCenter Single Sign-On 群組中移除成員。從本機群組中移除成員 (使用者或群組) 並不會將該成員從系統中刪除。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。

具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。

- 2 按一下**首頁**，然後瀏覽到**管理 > Single Sign-On > 使用者和群組**。
- 3 選取**群組**索引標籤，然後按一下群組。
- 4 在群組成員清單中，選取要移除的使用者或群組，然後按一下**移除成員**圖示。
- 5 按一下**確定**。

結果

使用者從群組中移除，但在系統中仍然可用。

刪除 vCenter Single Sign-On 解決方案使用者

vCenter Single Sign-On 會顯示解決方案使用者。解決方案使用者是服務的集合。已預先定義多個 vCenter Server 解決方案使用者，並會在安裝過程中向 vCenter Single Sign-On 驗證。例如，在進行疑難排解時，如果解除安裝未徹底完成，可從 vSphere Web Client 刪除個別解決方案使用者。

當您從環境中移除與某個 vCenter Server 解決方案使用者或第三方解決方案使用者相關聯的服務集時，會顯示已從 vSphere Web Client 移除的解決方案使用者。如果您強制移除某個應用程式，或者如果當解決方案使用者仍在系統中時系統變為無法復原，您可以從 vSphere Web Client 中明確移除此解決方案使用者。

重要 如果您刪除某個解決方案使用者，對應服務將無法再向 vCenter Single Sign-On 驗證。

程序

- 1 以 administrator@vsphere.local 或擁有 vCenter Single Sign-On 管理員權限的其他使用者身分登入 vSphere Web Client。
具有 vCenter Single Sign-On 管理員權限的使用者位於 vsphere.local 網域的管理員群組中。
- 2 按一下**首頁**，然後瀏覽到**管理 > Single Sign-On > 使用者和群組**。
- 3 按一下**解決方案使用者**索引標籤，然後按一下解決方案使用者名稱。
- 4 按一下**刪除解決方案使用者**圖示。
- 5 按一下**是**。

結果

與此解決方案使用者相關聯的服務無法再存取 vCenter Server，並且無法做為 vCenter Server 服務運作。

變更 vCenter Single Sign-On 密碼

本機網域中的使用者 (依預設為 vsphere.local) 可以從 Web 介面變更其 vCenter Single Sign-On 密碼。其他網域中的使用者變更其密碼時應遵循對應網域的規則。

vCenter Single Sign-On 鎖定原則會決定密碼的到期時間。依預設，vCenter Single Sign-On 使用者密碼會在 90 天後到期，但是管理員密碼 (例如 administrator@vsphere.local 的密碼) 不會到期。vCenter Single Sign-On 管理介面會在密碼即將到期時顯示警告。

備註 您僅可在密碼未到期時變更密碼。

如果密碼已到期，本機網域的管理員 (依預設為 administrator@vsphere.local) 可以使用 `dir-cli password reset` 命令重設密碼。僅 vCenter Single Sign-On 網域的管理員群組成員可以重設密碼。

程序

- 1 從網頁瀏覽器中，透過指定以下 URL 來連線到 Platform Services Controller：

`https://psc_hostname_or_IP/psc`

在內嵌式部署中，Platform Services Controller 主機名稱或 IP 位址與 vCenter Server 主機名稱或 IP 位址相同。

- 2 指定 administrator@vsphere.local 或 vCenter Single Sign-On 管理員群組的其他成員的使用者名稱和密碼。

如果在安裝期間指定了其他網域，請以 administrator@mydomain 身分登入。

- 3 在上方的導覽窗格中 [說明] 功能表的左側，按一下您的使用者名稱以彈出下拉式功能表。

此外，還可以選取 **Single Sign-On > 使用者和群組**，然後從右鍵功能表中選取**編輯使用者**。

- 4 選取**變更密碼**，然後輸入您目前的密碼。

- 5 輸入新密碼並確認。

該密碼必須符合密碼原則。

- 6 按一下**確定**。

vCenter Single Sign-On 安全性最佳做法

請遵循 vCenter Single Sign-On 安全性最佳做法來保護 vSphere 環境。

vSphere 6.0 驗證和憑證基礎結構可提升 vSphere 環境的安全性。若要確保基礎結構不受破壞，請遵循 vCenter Single Sign-On 最佳做法。

檢查密碼到期

預設 vCenter Single Sign-On 密碼原則的密碼存留時間為 90 天。90 天後密碼到期，登入能力將受到限制。檢查到期並及時重新整理密碼。

設定 NTP

確保所有系統使用相同的相對時間來源 (包括相關的當地語系化偏移)，並且相對時間來源可與商定的時間標準相關聯 (如國際標準時間-UTC)。同步的系統對 vCenter Single Sign-On 憑證有效性以及其他 vSphere 憑證的有效性至關重要。

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。

vCenter Single Sign-On 疑難排解

設定 vCenter Single Sign-On 的程序可能很複雜。

以下主題提供 vCenter Single Sign-On 疑難排解的起點。如需其他指示，請搜尋此說明文件中心和 VMware 知識庫系統。

判定 Lookup Service 錯誤的原因

vCenter Single Sign-On 安裝顯示有關 vCenter Server 或 vSphere Web Client 的錯誤。

問題

vCenter Server 和 Web Client 安裝程式顯示錯誤無法連絡 Lookup Service。請檢查 VM_ssoreg.log...

原因

導致該問題的原因有多種，包括主機電腦上的時鐘未同步、防火牆封鎖以及必須啟動的服務未啟動等。

解決方案

- 1 確認執行 vCenter Single Sign-On、vCenter Server 和 Web Client 之主機電腦上的時鐘同步。
- 2 檢視錯誤訊息中找到的特定記錄檔。

在該訊息中，系統暫存資料夾指的是 %TEMP%。

- 3 在記錄檔中，搜尋以下訊息。

該記錄檔包含所有安裝嘗試的輸出內容。找到最後一條訊息，其中顯示 Initializing registration provider...

訊息	原因和解決方案
java.net.ConnectException:Connection timed out:connect	IP 位址不正確、防火牆封鎖了對 vCenter Single Sign-On 的存取，或者 vCenter Single Sign-On 超載。 確保防火牆未封鎖 vCenter Single Sign-On 連接埠 (預設為 7444)，並且安裝有 vCenter Single Sign-On 的電腦擁有足夠的可用 CPU、I/O 及 RAM 容量。
java.net.ConnectException:Connection refused:connect	IP 位址或 FQDN 不正確，並且 vCenter Single Sign-On 服務未啟動或曾經啟動過，但當前已停止運作。 透過檢查 vCenter Single Sign-On 服務 (Windows) 和 vmware-ssso 精靈 (Linux) 的狀態，確認 vCenter Single Sign-On 運作正常。 重新啟動服務。如果這未能解決問題，請參閱《vSphere 疑難排解指南》的「復原」一節。
Unexpected status code:404. SSO Server failed during initialization	重新啟動 vCenter Single Sign-On。如果這未能解決問題，請參閱《vSphere 疑難排解指南》的「復原」一節。
The error shown in the UI begins with Could not connect to vCenter Single Sign-on.	您還會看到傳回代碼 SslHandshakeFailed。這種錯誤並不常見。它表示所提供的解析為 vCenter Single Sign-On 主機的 IP 位址或 FQDN，不是安裝 vCenter Single Sign-On 時所使用的 IP 位址或 FQDN。 在 %TEMP%\VM_ssoreg.log 中，找到包含以下訊息的行。 host name in certificate did not match:<install-configured FQDN or IP> != <A> or or <C>，其中 A 表示您在 vCenter Single Sign-On 安裝期間輸入的 FQDN，B 和 C 表示系統產生的允許替代值。 將組態更正為使用該記錄檔中 != 符號右側的 FQDN。在大多數情況下，使用在 vCenter Single Sign-On 安裝期間指定的 FQDN。 如果這些替代值均不適用於您的網路組態，請復原您的 vCenter Single Sign-On SSL 組態。

無法使用 Active Directory 網域驗證登入

您可以從 vSphere Web Client 登入 vCenter Server 元件。使用您的 Active Directory 使用者名稱和密碼。驗證失敗。

問題

您可以將 Active Directory 身分識別來源新增到 vCenter Single Sign-On，但使用者無法登入 vCenter Server。

原因

使用者可使用各自的使用者名稱和密碼登入預設網域。對於所有其他網域，使用者必須包括網域名稱 (user@domain 或 DOMAIN\user)。

如果使用的是 vCenter Server Appliance，則可能存在其他問題。

解決方案

對於所有 vCenter Single Sign-On 部署，您可以變更預設身分識別來源。執行此變更後，使用者只能使用使用者名稱和密碼來登入預設身分識別來源。

若要將您的整合式 Windows 驗證身分識別來源設定為 Active Directory 樹系內的子網域，請參閱 VMware 知識庫文章 [2070433](#)。依預設，整合式 Windows 驗證會使用 Active Directory 樹系的根網域。

如果使用的是 vCenter Server Appliance，且變更預設身分識別來源未能解決此問題，則執行以下額外的疑難排解步驟。

- 1 同步 vCenter Server Appliance 和 Active Directory 網域控制器之間的時鐘。
- 2 確認每個網域控制站在 Active Directory 網域 DNS 服務中是否均有指標記錄 (PTR)，並確認 PTR 記錄資訊與控制器的 DNS 名稱是否相符。使用 vCenter Server Appliance 時，可以執行以下命令來執行此工作：
 - a 若要列出網域控制器，請執行以下命令：

```
# dig SRV _ldap._tcp.my-ad.com
```

相關位址位於回答區段，如以下範例中所示：

```
;; ANSWER SECTION:
_ldap._tcp.my-ad.com. (...) my-controller.my-ad.com
...
```

- b 對於每個網域控制站，請執行以下命令來驗證正向和反向解析：

```
# dig my-controller.my-ad.com
```

相關位址位於回答區段，如以下範例中所示：

```
;; ANSWER SECTION:
my-controller.my-ad.com (...) IN A controller IP address
...

# dig -x <controller IP address>
```

相關位址位於回答區段，如以下範例中所示：

```
;; ANSWER SECTION:
IP-in-reverse.in-addr.arpa. (...) IN PTR my-controller.my-ad.com
...
```

- 3 如果執行上述步驟未能解決問題，請從 Active Directory 網域中移除 vCenter Server Appliance，然後重新加入網域。請參閱《vCenter Server Appliance 組態》說明文件。
- 4 關閉所有連線到 vCenter Server Appliance 的瀏覽器工作階段，然後重新啟動所有服務。

```
/bin/service-control --restart --all
```

由於使用者帳戶被鎖定，vCenter Server 登入失敗

從 vSphere Web Client 登入頁面登入 vCenter Server 時出現錯誤，指示帳戶被鎖定。

問題

多次嘗試均失敗之後，您將無法使用 vCenter Single Sign-On 登入到 vSphere Web Client。您會看到一則訊息，指示您的帳戶被鎖定。

原因

您已超過嘗試登入失敗的次數上限。

解決方案

- ◆ 如果您做為系統網域 (vsphere.local) 中的使用者登入，請要求您的 vCenter Single Sign-On 管理員解除鎖定您的帳戶。或者，如果在密碼原則中將此鎖定設定為到期，則可以等待帳戶解除鎖定。vCenter Single Sign-On 管理員可以使用 CLI 命令來解除鎖定您的帳戶。
- ◆ 如果您做為 Active Directory 或 LDAP 網域中的使用者身分登入，請要求您的 Active Directory 或 LDAP 管理員解除鎖定您的帳戶。

VMware 目錄服務複寫可能需要很長時間

如果您的環境包含多個 Platform Services Controller 執行個體，而當其中一個 Platform Services Controller 執行個體無法使用時，您的環境會繼續正常運作。當 Platform Services Controller 重新恢復可用時，使用者資料及其他資訊通常會於 60 秒內複寫。但是，在某些特定情況下，複寫可能需要很長時間。

問題

例如，在某些情況下，當您的環境包含多個位於不同位置的 Platform Services Controller 執行個體，並且您在某個 Platform Services Controller 無法使用時進行了重大變更，則跨 VMware 目錄服務執行個體的複寫不會立即開始。例如，在複寫完成之前，新增到可用 Platform Services Controller 執行個體的新使用者不會出現在另一個執行個體中。

原因

在一般作業期間，於某個 Platform Services Controller 執行個體 (節點) 中對 VMware 目錄服務 (vmdir) 執行個體所做的變更，會於約 60 秒內顯示在其直接複寫合作夥伴中。視複寫拓撲而定，某個節點中的變更可能必須透過中繼節點傳播，才能到達每個節點中的各個 vmdir 執行個體。複寫的資訊包括使用 VMware VMotion 建立、複製或移轉之虛擬機器的使用者資訊、憑證資訊、授權資訊及更多資訊。

當複寫連結中斷 (例如因為網路中斷或節點無法使用) 時，聯盟中的變更不會聚合。還原無法使用的節點後，每個節點會嘗試完成所有變更。最終，所有 vmdir 執行個體會聚合為一致狀態，但如果某個節點無法使用時發生了許多變更，可能需要一段時間才能達到這種一致狀態。

解決方案

複寫進行時，您的環境會正常運作。除非問題持續存在超過一個小時，否則請勿嘗試解決。

vSphere 安全性憑證

3

vSphere 元件會使用 SSL 於彼此間以及與 ESXi 安全地進行通訊。SSL 通訊可以確保資料的機密性和完整性。資料會受到保護，只要在傳輸期間對其修改，就將被偵測到。

vCenter Server 服務，例如 vSphere Web Client，也使用憑證向 vCenter Single Sign-On 進行初始驗證。vCenter Single Sign-On 會為每個元件提供日後可用於驗證的 SAML Token。

在 vSphere 6.0 及更新版本中，VMware Certificate Authority (VMCA) 會使用預設由 VMCA 簽署的憑證佈建每台 ESXi 主機及每個 vCenter Server 服務。

您可以用新的 VMCA 簽署的憑證取代現有憑證，使 VMCA 做為下層授權機構，或使用自訂憑證取代所有憑證。您有多個選項可供選擇：

表 3-1. 不同的憑證取代方法

選項	請參閱
使用 Platform Services Controller Web 介面 (vSphere 6.0 Update 1 及更新版本)。	使用 Platform Services Controller Web 介面管理憑證
從命令列使用 vSphere Certificate Manager 公用程式。	透過 vSphere Certificate Manager 公用程式管理憑證
使用 CLI 命令來手動取代憑證。	使用 CLI 命令管理憑證和服務



vSphere 憑證管理

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_ejp3dqkt/uiConfId/49694343/)

本章節討論下列主題：

- [不同解決方案路徑的憑證需求](#)
- [憑證管理概觀](#)
- [使用 Platform Services Controller Web 介面管理憑證](#)
- [透過 vSphere Certificate Manager 公用程式管理憑證](#)
- [手動憑證取代](#)
- [使用 CLI 命令管理憑證和服務](#)
- [使用 vSphere Web Client 檢視 vCenter 憑證](#)
- [設定 vCenter 憑證到期警告臨界值](#)

不同解決方案路徑的憑證需求

視您是否將 VMCA 做為中繼 CA 使用或您使用的為自訂憑證而定，憑證需求會有所不同。機器憑證和解決方案使用者憑證的需求也不盡相同。

登入前，請確保您環境中所有節點的時間均已同步。

所有匯入憑證的需求

- 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)。將金鑰新增到 VECS 之後，系統會將其轉換為 PKCS8。
- x509 第 3 版
- 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。
- 用戶端驗證和伺服器驗證無法在 [增強金鑰使用方法] 下顯示。

VMCA 不支援以下憑證。

- 含有萬用字元的憑證
- 不建議使用的演算法包括 md2WithRSAEncryption 1.2.840.113549.1.1.2、md5WithRSAEncryption 1.2.840.113549.1.1.4 和 sha1WithRSAEncryption 1.2.840.113549.1.1.5。
- 不支援 OID 為 1.2.840.113549.1.1.10 的演算法 RSASSA-PSS。

符合 RFC 2253 的憑證

憑證必須符合 RFC 2253。

如果您不使用 Certificate Manager 產生 CSR，請確保 CSR 包含以下欄位。

字串	X.500 屬性類型
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName
STREET	streetAddress
DC	domainComponent
UID	userid

如果您使用 Certificate Manager 產生 CSR，系統會提示您輸入以下資訊，而且 Certificate Manager 會將對應欄位新增至 CSR 檔案。

- administrator@vsphere.local 使用者的密碼，或您要連線的 vCenter Single Sign-On 網域的管理員密碼。
- 如果您是使用外部 Platform Services Controller 在環境中產生 CSR，系統會提示您輸入 Platform Services Controller 的主機名稱或 IP 位址。
- Certificate Manager 儲存在 `certtool.cfg` 檔案中的資訊。對於大部分的欄位，您可以接受預設值，或提供站台專屬值。機器的 FQDN 為必填。
 - administrator@vsphere.local 的密碼。
 - 兩個字母形式的國碼
 - 公司名稱
 - 組織名稱
 - 組織單位
 - 狀態
 - 位置
 - IP 位址 (選用)
 - 電子郵件
 - 主機名稱，即要進行憑證取代之機器的完整網域名稱。如果主機名稱與 FQDN 不相符，憑證取代就無法正確完成，而您的環境可能會最終處於不穩定狀態。
 - Platform Services Controller 的 IP 位址 (如果您在 vCenter Server 管理節點上執行命令)

將 VMCA 作為中繼 CA 使用時的需求

當您將 VMCA 作為中繼 CA 使用時，憑證必須符合以下需求。

憑證類型	憑證需求
根憑證	<ul style="list-style-type: none"> ■ 您可以使用 vSphere Certificate Manager 建立 CSR。請參閱使用 vSphere Certificate Manager 產生 CSR 並準備根憑證 (中繼 CA) ■ 如果您偏好手動建立 CSR，則傳送要求簽署的憑證必須符合下列需求： <ul style="list-style-type: none"> ■ 金鑰大小：2048 位元或以上 ■ 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 ■ 若使用自訂憑證，CA 延伸必須設為 true (若為根憑證)，且憑證簽署必須位於需求清單中。 ■ 必須啟用 CRL 簽署。 ■ [增強金鑰使用方法] 不得包含 [用戶端驗證] 或 [伺服器驗證]。 ■ 對憑證鏈結的長度無明確限制。VMCA 預設使用 OpenSSL (為 10 個憑證)。 ■ 不支援含萬用字元或多個 DNS 名稱的憑證。 ■ 您無法建立 VMCA 的附屬 CA。 <p>如需 Microsoft 憑證授權機構的使用範例，請參閱 VMware 知識庫文章 2112009，建立 Microsoft 憑證授權機構範本，用於在 vSphere 6.0 中建立 SSL 憑證。</p>
機器 SSL 憑證	<p>您可以使用 vSphere Certificate Manager 建立 CSR 或手動建立 CSR。</p> <p>如果您手動建立 CSR，則其必須符合上述所有匯入憑證的需求中所列的需求。您也必須指定主機的 FQDN。</p>
解決方案使用者憑證	<p>您可以使用 vSphere Certificate Manager 建立 CSR 或手動建立 CSR。</p> <p>備註 每位解決方案使用者必須使用不同的名稱。如果您手動產生憑證，則主體下可能顯示為 CN，視您使用的工具而定。</p> <p>如果您使用 vSphere Certificate Manager，則工具會提示您輸入每位解決方案使用者的憑證資訊。vSphere Certificate Manager 會將資訊儲存在 <code>certtool.cfg</code> 中。請參閱 Certificate Manager 提示輸入的資訊。</p>

自訂憑證的需求

當您要使用自訂憑證時，憑證必須符合以下需求。

憑證類型	憑證需求
機器 SSL 憑證	<p>每個節點上的機器 SSL 憑證必須具有與第三方或企業 CA 不同的獨立憑證。</p> <ul style="list-style-type: none"> ■ 您可以使用 vSphere Certificate Manager 產生 CSR，也可以手動建立 CSR。CSR 必須符合上述所有匯入憑證的需求中所列的需求。 ■ 如果您使用 vSphere Certificate Manager，則工具會提示您輸入每位解決方案使用者的憑證資訊。vSphere Certificate Manager 會將資訊儲存在 <code>certtool.cfg</code> 中。請參閱 Certificate Manager 提示輸入的資訊。 ■ 對於大部分的欄位，您可以接受預設值，或提供站台專屬值。機器的 FQDN 為必填。
解決方案使用者憑證	<p>各節點上的每個解決方案使用者必須具有與第三方或企業 CA 不同的獨立憑證。</p> <ul style="list-style-type: none"> ■ 您可以使用 vSphere Certificate Manager 產生 CSR，也可以自行準備 CSR。CSR 必須符合上述所有匯入憑證的需求中所列的需求。 ■ 如果您使用 vSphere Certificate Manager，則工具會提示您輸入每位解決方案使用者的憑證資訊。vSphere Certificate Manager 會將資訊儲存在 <code>certtool.cfg</code> 中。請參閱 Certificate Manager 提示輸入的資訊。 <p>備註 每位解決方案使用者必須使用不同的名稱。如果您手動產生憑證，則主體下可能顯示為 CN，視您使用的工具而定。</p> <p>之後當您使用自訂憑證取代解決方案使用者憑證時，請提供第三方 CA 的完整簽署憑證鏈結。</p>
<p>備註 請勿在任何自訂憑證中使用 CRL 發佈點、授權資訊存取或憑證範本資訊。</p>	

憑證管理概觀

新憑證基礎結構的影響具體取決於您環境的需求、執行全新安裝還是升級，以及考慮使用 ESXi 還是 vCenter Server。

未取代 VMware 憑證的管理員

如果您身為管理員且目前並未取代 VMware 憑證，VMCA 能夠為您處理所有憑證管理事項。VMCA 使用以 VMCA 做為根憑證授權機構的憑證佈建 vCenter Server 元件和 ESXi 主機。如果您要從舊版 vSphere 升級為 vSphere 6，所有自我簽署的憑證都會取代為 VMCA 簽署的憑證。

將 VMware 憑證取代為自訂憑證的管理員

對於全新安裝，管理員可以選擇公司原則需要由第三方或企業憑證授權機構簽署的憑證，還是需要自訂憑證資訊。

- 將 VMCA 根憑證取代為 CA 簽署憑證。在此情況下，VMCA 憑證為此第三方 CA 的中繼憑證。VMCA 使用包含完整憑證鏈結的憑證佈建 vCenter Server 元件和 ESXi 主機。

- 如果公司原則不允許鏈結中存在中繼憑證，您必須明確取代這些憑證。您可以使用 vSphere Certificate Manager 公用程式，或使用憑證管理 CLI 執行手動憑證取代。

升級使用自訂憑證的環境時，您可以保留部分憑證。

- ESXi 主機會在升級期間保留其自訂憑證。確定 vCenter Server 升級程序會將所有相關根憑證新增到 vCenter Server 上 VECS 中的 TRUSTED_ROOTS 存放區。

vCenter Server 升級後，管理員可以將憑證模式設為自訂 (請參閱[變更憑證模式](#))。如果憑證模式為 VMCA (預設值)，且使用者從 vSphere Web Client 執行憑證重新整理，則 VMCA 簽署憑證會取代自訂憑證。

- 對於 vCenter Server 元件，發生的情況取決於現有環境。
 - 如果您將簡單安裝升級為內嵌式部署，vCenter Server 自訂憑證會保留。升級後，您的環境將會如往常一般正常運作。
 - 如果您為多站台部署進行升級，該部署的 vCenter Single Sign-On 和其他 vCenter Server 元件位於不同的機器上，升級程序會建立包含一個 Platform Services Controller 節點及一或多個管理節點的多節點部署。

在此情況下，現有的 vCenter Server 和 vCenter Single Sign-On 憑證會保留並用做機器 SSL 憑證。VMCA 會將 VMCA 簽署憑證指派給每個解決方案使用者 (vCenter 服務集合)。解決方案使用者僅使用此憑證向 vCenter Single Sign-On 進行驗證，因此可能不需要取代解決方案使用者憑證。

您無法繼續使用過去可用於 vSphere 5.5 安裝的 vSphere 5.5 憑證取代工具，因為新的架構導致服務散佈與放置不同。新的命令列公用程式 vSphere Certificate Manager 可供大部分憑證管理工作使用。

vCenter 憑證介面

對於 vCenter Server，您可以使用下列工具和介面檢視與取代憑證。

vSphere Certificate Manager 公用程式

從命令列執行所有一般憑證取代工作。

憑證管理 CLI

使用 `dir-cli`、`certool` 和 `vecs-cli` 執行所有憑證管理工作。

vSphere Web Client 憑證管理

檢視憑證，包括到期資訊。

對於 ESXi，您可以從 vSphere Web Client 執行憑證管理。憑證會由 VMCA 佈建，並僅會本機儲存於 ESXi 主機，而不會儲存在 vmdir 或 VECS 中。請參閱[ESXi 主機的憑證管理](#)。

支援的 vCenter 憑證

對於 vCenter Server、Platform Services Controller 以及相關的機器與服務，支援下列憑證：

- 由 VMware 憑證授權機構 (VMCA) 產生及簽署的憑證。

- 自訂憑證。
 - 產生自您自己的內部 PKI 的企業憑證。
 - 由外部 PKI (例如 Verisign、GoDaddy 等) 產生的第三方 CA 簽署憑證。

使用 OpenSSL 建立的自我簽署憑證，支援全部現有根 CA。

憑證取代概觀

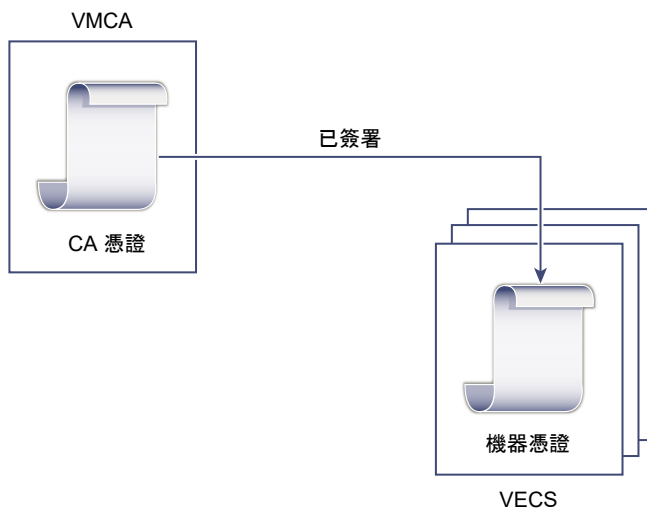
根據公司原則以及要設定之系統的需求，您可以執行不同類型的憑證取代。可以透過 vSphere 憑證管理員公用程式或使用安裝隨附的 CLI 手動執行每個取代。

可以取代預設憑證。對於 vCenter Server 元件，您可以使用包含在安裝中的一組命令列工具。您可以有多個選項。

用 VMCA 簽署的憑證取代

如果您的 VMCA 憑證到期或出於其他原因想將其取代，則可使用憑證管理 CLI 執行該程序。依預設，VMCA 根憑證會在十年後到期，而 VMCA 簽署的所有憑證都會在根憑證到期時到期 (即最多十年期限)。

圖 3-1. VMCA 簽署的憑證儲存在 VECS 中

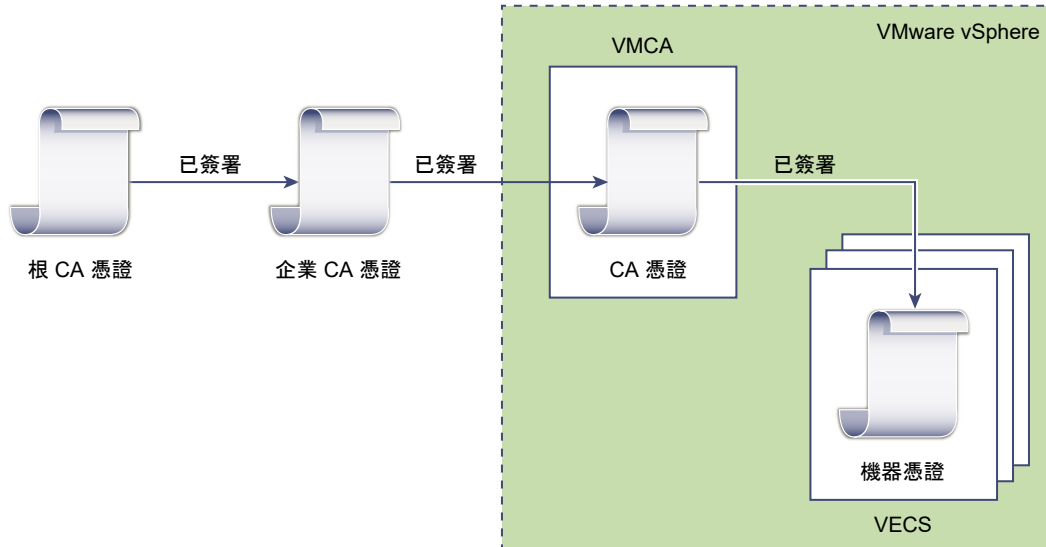


使 VMCA 成為中繼 CA

可以將 VMCA 根憑證取代為企業 CA 或第三方 CA 簽署的憑證。VMCA 每次佈建憑證時都可以簽署自訂根憑證，使 VMCA 成為中繼 CA。

備註 如果執行的全新安裝中包含外部 Platform Services Controller，請先安裝 Platform Services Controller 並取代 VMCA 根憑證。接著，安裝其他服務或將 ESXi 主機新增至您的環境。如果執行的全新安裝中包含內嵌式 Platform Services Controller，則在新增 ESXi 主機之前取代 VMCA 根憑證。這樣一來，所有憑證將由整個鏈結簽署，且不需要產生新憑證。

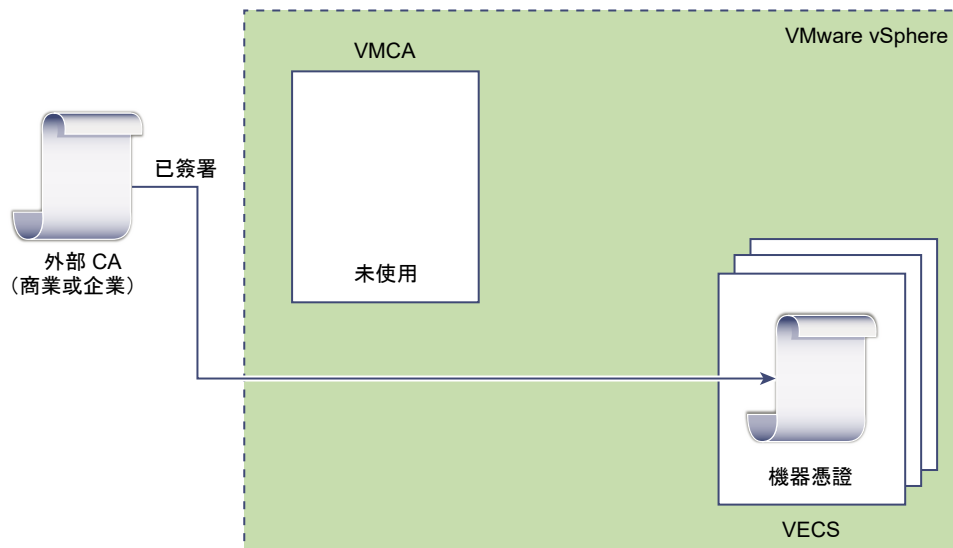
圖 3-2. 第三方或企業 CA 簽署的憑證使用 VMCA 做為中繼 CA



用自訂憑證而非 VMCA 進行佈建

可以使用自訂憑證取代現有的 VMCA 簽署的憑證。如果使用该方法，您將負責佈建和監控所有憑證。

圖 3-3. 外部憑證直接儲存在 VECS 中



混合部署

可以讓 VMCA 提供一些憑證，並針對基礎結構的其他部分使用自訂憑證。例如，由於解決方案使用者憑證僅用於向 vCenter Single Sign-On 進行驗證，因此，請考慮讓 VMCA 佈建這些憑證。將機器 SSL 憑證取代為自訂憑證以確保所有 SSL 流量安全。

ESXi 憑證取代

對於 ESXi 主機，您可以透過 vSphere Web Client 變更憑證佈建行為。

VMware 憑證授權機構模式 (預設)

從 vSphere Web Client 更新憑證時，VMCA 會核發用於主機的憑證。如果您將 VMCA 根憑證變更為包含憑證鏈結，則主機憑證會包含完整鏈結。

自訂憑證授權機構模式

允許您手動更新和使用並非由 VMCA 簽署或核發的憑證。

指紋模式

可用於在重新整理期間保留 5.5 憑證。將此模式僅暫時用於偵錯情況。

vSphere 6.0 使用憑證所在位置

在 vSphere 6.0 及更新版本中，VMware 憑證授權機構 (VMCA) 會使用憑證佈建您的環境。這包括用於安全連線的機器 SSL 憑證、用於向 vCenter Single Sign-On 進行驗證的解決方案使用者憑證，以及用於新增到 vCenter Server 之 ESXi 主機的憑證。

使用中的憑證如下。

表 3-2. vSphere 6.0 中的憑證

憑證	佈建者	儲存位置
ESXi 憑證	VMCA (預設)	本機儲存於 ESXi 主機
機器 SSL 憑證	VMCA (預設)	VECS
解決方案使用者憑證	VMCA (預設)	VECS
vCenter Single Sign-On SSL 簽署憑證	於安裝期間佈建。	在 vSphere Web Client 中管理這個憑證。 警告 請勿在檔案系統中變更此憑證，否則可能導致無法預期的行為。
VMware 目錄服務 (vmdir) SSL 憑證	於安裝期間佈建。	在某些極端情況下，您可能必須取代此憑證。請參閱 取代 VMware 目錄服務憑證 。

ESXi

ESXi 憑證會本機儲存於每台主機的 `/etc/vmware/ssl` 目錄中。ESXi 憑證預設由 VMCA 佈建，但是您可以改為使用自訂憑證。ESXi 憑證會在主機首次新增到 vCenter Server 以及主機重新連線時佈建。

機器 SSL 憑證

每個節點的機器 SSL 憑證用於在 SSL 用戶端所連線的伺服器端建立 SSL 通訊端。此憑證用於進行伺服器驗證以及安全通訊 (例如 HTTPS 或 LDAPS)。

所有服務都會透過反向 Proxy 進行通訊。為確保相容性，舊版 vSphere 中提供的服務也會使用特定連接埠。例如，vpxd 服務使用 MACHINE_SSL_CERT 公開其端點。

每個節點 (內嵌式部署、管理節點或 Platform Services Controller) 都擁有自己的機器 SSL 憑證。在該節點上執行的所有服務都會使用此機器 SSL 憑證公開其 SSL 端點。

機器 SSL 憑證的使用方式如下：

- 透過每個 Platform Services Controller 節點上的反向 Proxy 服務。與個別 vCenter 服務的 SSL 連線一律經過反向 Proxy。流量並不會進入服務本身。
- 透過管理節點和內嵌式節點上的 vCenter 服務 (vpxd)。
- 透過基礎結構節點和內嵌式節點上的 VMware 目錄服務 (vmdir)。

VMware 產品使用標準 X.509 第 3 版 (X.509v3) 憑證來加密工作階段資訊，此工作階段資訊是透過元件之間的 SSL 傳送。

解決方案使用者憑證

解決方案使用者會封裝一或多個 vCenter Server 服務，並使用憑證透過 SAML Token 交換向 vCenter Single Sign-On 進行驗證。每個解決方案使用者都必須向 vCenter Single Sign-On 進行驗證。

解決方案使用者憑證用於向 vCenter Single Sign-On 進行驗證。解決方案使用者會在首次驗證時、重新開機後以及逾時結束後，向 vCenter Single Sign-On 出示憑證。逾時 (金鑰持有者逾時) 可以從 vSphere Web Client 進行設定，預設為 2592000 秒 (30 天)。

例如，vpxd 解決方案使用者會在連線至 vCenter Single Sign-On 時，向 vCenter Single Sign-On 出示其憑證。vpxd 解決方案使用者會從 vCenter Single Sign-On 收到 SAML Token，然後便可以使用該 Token 向其他解決方案使用者和服務進行驗證。

每個管理節點和每個內嵌式部署上的 VECS 中包含下列解決方案使用者憑證存放區：

- 機器：由 Component Manager、授權伺服器及記錄服務所使用。

備註 機器解決方案使用者憑證與機器的 SSL 憑證毫無關聯。機器解決方案使用者憑證用於進行 SAML Token 交換；機器的 SSL 憑證用於對機器進行安全 SSL 連線。

- vpxd：vCenter 服務精靈 (vpxd) 存放區位於管理節點和內嵌式部署中。vpxd 會使用此存放區中儲存的解決方案使用者憑證向 vCenter Single Sign-On 進行驗證。
- vpxd-extensions：vCenter 延伸存放區。包含 Auto Deploy 服務、Inventory Service 及不屬於其他解決方案使用者的其他服務。
- vsphere-webclient：vSphere Web Client 存放區。還包括一些其他服務，例如效能圖服務。

每個 Platform Services Controller 節點中也包含機器存放區。

vCenter Single Sign-On 憑證

vCenter Single Sign-On 憑證不是儲存在 VECS 中，並且不使用憑證管理工具進行管理。按規則，並不需要進行變更，但在特殊情況下，您可以取代這些憑證。

vCenter Single Sign-On 簽署憑證

vCenter Single Sign-On 服務包含身分識別提供者服務，該服務會核發在 vSphere 中用於驗證的 SAML Token。SAML Token 表示使用者的身分，同時還包含群組成員資格資訊。vCenter Single Sign-On 核發 SAML Token 時，將使用其簽署憑證簽署每個 Token，讓 vCenter Single Sign-On 用戶端可以驗證 SAML Token 是否來自受信任來源。

vCenter Single Sign-On 會核發金鑰持有者 SAML Token 給解決方案使用者，並核發 Bearer Token 給以使用者名稱和密碼登入的其他使用者。

您可以從 vSphere Web Client 中取代此憑證。請參閱 [重新整理安全性 Token 服務憑證](#)。

VMware 目錄服務 SSL 憑證

如果您使用的是自訂憑證，可能必須明確取代 VMware 目錄服務 SSL 憑證。請參閱 [取代 VMware 目錄服務憑證](#)。

VMCA 和 VMware Core Identity Services

Core Identity Services 是每個內嵌式部署和每個平台服務節點的一部分。VMCA 是每個 VMware Core Identity Services 群組的一部分。請使用管理 CLI 和 vSphere Web Client 與這些服務進行互動。

VMware Core Identity Services 包含數個元件。

表 3-3. Core Identity Services

服務	描述	包含於
VMware 目錄服務 (vmdir)	結合 vCenter Single Sign-On 處理 SAML 憑證管理以進行驗證。	Platform Services Controller 內嵌式部署
VMware 憑證授權機構 (VMCA)	核發 VMware 解決方案使用者憑證、執行服務之機器的機器憑證，以及 ESXi 主機憑證。VMCA 可用於原本用途，也可以做為中繼憑證授權機構。 VMCA 只會對相同網域中能向 vCenter Single Sign-On 進行驗證的用戶端核發憑證。	Platform Services Controller 內嵌式部署
VMware 驗證架構精靈 (VMAFD)	包含 VMware Endpoint 憑證存放區 (VECS) 和數個其他驗證服務。VMware 管理員會與 VECS 互動；其他服務則會於內部使用。	Platform Services Controller vCenter Server 內嵌式部署

VMware Endpoint 憑證存放區概觀

VMware Endpoint 憑證存放區 (VECS) 用作儲存憑證、私密金鑰及其他可儲存於金鑰儲存區之憑證資訊的本機 (用戶端) 存放庫。您可以決定不使用 VMCA 做為憑證授權機構和憑證簽署者，但您必須使用 VECS 儲存所有 vCenter 憑證、金鑰等等。ESXi 憑證會本機儲存於每台主機，而不會儲存於 VECS 中。

VECS 會於 VMware 驗證架構精靈 (VMAFD) 一併執行。VECS 會在每個內嵌式部署、Platform Services Controller 節點及管理節點上執行，且具有包含憑證與金鑰的金鑰儲存區。

VECS 會定期輪詢 VMware 目錄服務 (vmdir) 以查看 TRUSTED_ROOTS 存放區是否有任何更新。您也可以使用 `vecs-cli` 命令明確管理 VECS 中的憑證和金鑰。請參閱 [vecs-cli 命令參考](#)。

VECS 包含下列存放區。

表 3-4. VECS 中的存放區

存放區	描述
機器的 SSL 存放區 (MACHINE_SSL_CERT)	<ul style="list-style-type: none"> ■ 由每個 vSphere 節點上反向 Proxy 服務所使用。 ■ 供內嵌式部署和每個 Platform Services Controller 節點上的 VMware 目錄服務 (vmdir) 使用。 <p>vSphere 6.0 中的所有服務都會透過使用機器 SSL 憑證的反向 Proxy 進行通訊。為確保回溯相容性，5.x 服務仍會使用特定的連接埠。因此，部分服務 (例如 vpxd) 仍會將自己的連接埠維持開啟。</p>
受信任的根存放區 (TRUSTED_ROOTS)	包含所有受信任的根憑證。
解決方案使用者存放區 <ul style="list-style-type: none"> ■ machine ■ vpxd ■ vpxd-extensions ■ vsphere-webclient 	<p>對於每個解決方案使用者，VECS 包含一個存放區。每個解決方案使用者憑證的主旨必須是唯一的，例如，機器憑證不能與 vpxd 憑證的主旨相同。</p> <p>解決方案使用者憑證用於透過 vCenter Single Sign-On 進行驗證。vCenter Single Sign-On 會檢查憑證是否有效，但不會檢查其他憑證屬性。在內嵌式部署中，所有解決方案使用者憑證均位於同一系統中。</p> <p>每個管理節點和每個內嵌式部署上的 VECS 中包含下列解決方案使用者憑證存放區：</p> <ul style="list-style-type: none"> ■ 機器：由 Component Manager、授權伺服器及記錄服務所使用。 <p>備註 機器解決方案使用者憑證與機器的 SSL 憑證毫無關聯。機器解決方案使用者憑證用於進行 SAML Token 交換；機器的 SSL 憑證用於對機器進行安全 SSL 連線。</p> <ul style="list-style-type: none"> ■ vpxd：vCenter 服務精靈 (vpxd) 存放區位於管理節點和內嵌式部署中。vpxd 會使用此存放區中儲存的解決方案使用者憑證向 vCenter Single Sign-On 進行驗證。 ■ vpxd-extensions：vCenter 延伸存放區。包含 Auto Deploy 服務、Inventory Service 及不屬於其他解決方案使用者的其他服務。 ■ vsphere-webclient：vSphere Web Client 存放區。還包括一些其他服務，例如效能圖服務。 <p>每個 Platform Services Controller 節點中也包含機器存放區。</p>
vSphere Certificate Manager 公用程式備份存放區 (BACKUP_STORE)	由 VMCA (VMware Certificate Manager) 用於支援憑證還原。只有最新狀態會儲存為備份，您無法還原一個以上的步驟。
其他存放區	<p>其他存放區可能由解決方案新增。例如，虛擬磁碟區解決方案將新增一個 SMS 存放區。除非 VMware 說明文件或 VMware 知識庫文章指示您修改這些存放區中的憑證，否則請勿這麼做。</p> <p>備註 vSphere 6.0 不支援 CRLS，然而，刪除 TRUSTED_ROOTS_CRLS 存放區可能會破壞憑證基礎結構。請勿刪除或修改 TRUSTED_ROOTS_CRLS 存放區。</p>

vCenter Single Sign-On 服務會將 Token 簽署憑證及其 SSL 憑證儲存於磁碟中。您可以從 vSphere Web Client 變更 Token 簽署憑證。

備註 除非 VMware 說明文件或知識庫文章做出相關指示，否則請勿變更磁碟上的任何憑證檔案。否則可能導致發生無法預期的行為。

部分憑證會在啟動期間暫時或永久儲存在檔案系統中。請勿變更檔案系統中的憑證。請使用 `vecs-cli` 對 VECS 中儲存的憑證執行作業。

管理憑證撤銷

如果您懷疑其中一個憑證已損毀，請取代所有現有的憑證，包括 VMCA 根憑證。

對於 ESXi 主機或 vCenter Server 系統，vSphere 6.0 支援取代憑證但不會強制憑證撤銷。

從所有節點移除撤銷的憑證。如果您沒有移除撤銷的憑證，他人可能得以透過使用帳戶認證模擬來進行攔截式攻擊造成破壞。

大型部署中的憑證取代

包含多個管理節點及一或多個 Platform Services Controller 節點的部署中的憑證取代與內嵌式部署中的取代類似。在這兩種情況下，您都可以使用 vSphere 憑證管理公用程式，或以手動方式取代憑證。有一些最佳做法可引導您進行取代程序。

包含負載平衡器之高可用性環境中的憑證取代

在使用少於八個 vCenter Server 系統的環境中，VMware 通常建議使用單一 Platform Services Controller 執行個體與相關聯的 vCenter Single Sign-On 服務。在大型環境中，請考慮使用多個受網路負載平衡器保護的 Platform Services Controller 執行個體。VMware 網站上的白皮書《vCenter Server 6.0 部署指南》說明了此設定。

具有多個管理節點之環境中的機器 SSL 憑證取代

如果您的環境包含多個管理節點以及單一 Platform Services Controller，您可以使用 vSphere Certificate Manager 公用程式取代憑證，或使用 vSphere CLI 命令以手動方式取代。

vSphere Certificate Manager

在每台機器上執行 vSphere Certificate Manager。在管理節點上，系統會提示您輸入 Platform Services Controller 的 IP 位址。視您所執行的工作而定，系統也會提示您輸入憑證資訊。

手動憑證取代

對於手動憑證取代，您需要在每台機器上執行憑證取代命令。在管理節點上，您必須使用 `--server` 參數指定 Platform Services Controller。如需詳細資訊，請參閱下列主題：

- [用 VMCA 簽署憑證取代機器 SSL 憑證](#)
- [取代機器 SSL 憑證 \(中繼 CA\)](#)
- [將機器 SSL 憑證取代為自訂憑證](#)

具有多個管理節點之環境中的解決方案使用者憑證取代

如果您的環境包含多個管理節點和單一 Platform Services Controller，請遵循下列步驟進行憑證取代。

備註 當您列出大型部署中的解決方案使用者憑證時，`dir-cli list` 的輸出會包含所有節點上的所有解決方案使用者。執行 `vmafd-cli get-machine-id --server-name localhost` 以找出每台主機的本機機器識別碼。每個解決方案使用者名稱都包含機器識別碼。

vSphere Certificate Manager

在每台機器上執行 vSphere Certificate Manager。在管理節點上，系統會提示您輸入 Platform Services Controller 的 IP 位址。視您所執行的工作而定，系統也會提示您輸入憑證資訊。

手動憑證取代

- 產生或要求憑證。您需要下列憑證：
 - Platform Services Controller 上機器解決方案使用者的憑證。
 - 每個管理節點上機器解決方案使用者的憑證。
 - 每個管理節點上的下列每個解決方案使用者的憑證：
 - vpxd 解決方案使用者
 - vpxd-extension 解決方案使用者
 - vsphere-webclient 解決方案使用者
- 取代每個節點上的憑證。確切程序會視您所執行的憑證取代類型而定。請參閱[透過 vSphere Certificate Manager 公用程式管理憑證](#)

如需詳細資訊，請參閱下列主題：

- [用新的 VMCA 簽署憑證取代解決方案使用者憑證](#)
- [取代解決方案使用者憑證 \(中繼 CA\)](#)
- [將解決方案使用者憑證取代為自訂憑證](#)

如果公司原則需要您取代所有憑證，您也必須取代 Platform Services Controller 上的 VMware 目錄服務 (vmmdir) 憑證。請參閱 [取代 VMware 目錄服務憑證](#)。

包含外部解決方案之環境中的憑證取代

某些諸如 VMware vCenter Site Recovery Manager 或 VMware vSphere Replication 的解決方案一律會安裝在與 vCenter Server 系統或 Platform Services Controller 不同的機器上。如果您取代 vCenter Server 系統或 Platform Services Controller 上的預設機器 SSL 憑證，則當解決方案嘗試連線到 vCenter Server 系統時會產生連線錯誤。

您可以執行 `ls_update_certs` 指令碼來解決此問題。如需詳細資料，請參閱 [VMware 知識庫文章 2109074](#)。

使用 Platform Services Controller Web 介面管理憑證

您可以登入 Platform Services Controller Web 介面來檢視及管理憑證。您可以透過 vSphere Certificate Manager 公用程式或使用此 Web 介面執行許多憑證管理工作。

Platform Services Controller Web 介面可讓您執行以下管理工作。

- 檢視目前的憑證存放區，然後新增和移除憑證存放區項目。
- 檢視與這個 Platform Services Controller 相關聯的 VMware Certificate Authority (VMCA) 執行個體。
- 檢視 VMware Certificate Authority 產生的憑證。
- 更新現有憑證或取代憑證。

大部分的憑證取代工作流程完全可從 Platform Services Controller Web 介面進行。若要產生 CSR，您可以使用 vSphere Certificate Manager 公用程式。

支援的工作流程

依預設，Platform Services Controller 安裝完成後，該節點上的 VMware Certificate Authority 會使用憑證佈建環境中的所有其他節點。您可以使用下列其中一個工作流程來更新或取代憑證。

更新憑證

您可以從 Platform Services Controller Web 介面讓 VMCA 產生新的根憑證，並更新您環境中的所有憑證。

使 VMCA 成為中繼 CA

您可以使用 vSphere Certificate Manager 公用程式產生 CSR，編輯從 CSR 收到的憑證以將 VMCA 新增到鏈結，然後將憑證鏈結與私密金鑰新增到您的環境中。當您接著更新所有憑證時，VMCA 會使用由完整鏈結簽署的憑證來佈建所有機器和解決方案使用者。

將憑證取代為自訂憑證

如果您不希望使用 VMCA，則可以針對您要取代的憑證產生 CSR。CA 會針對每個 CSR 傳回根憑證及已簽署憑證。您可以從 Platform Services Controller 上傳根憑證及自訂憑證。

如果您必須取代 VMware Directory Service (vmdir) 根憑證，或公司原則要求您取代混合模式環境中的 vCenter Single Sign-On 憑證，則可以在取代其他憑證之後使用 CLI 命令取代這些憑證。請參閱 [取代 VMware 目錄服務憑證](#) 和 [在混合模式環境中取代 VMware Directory Service 憑證](#)。

從 Platform Services Controller Web 介面深入瞭解憑證存放區

每個 Platform Services Controller 節點和每個 vCenter Server 節點上均包含 VMware Endpoint 憑證存放區 (VECS) 執行個體。您可以從 Platform Services Controller Web 介面深入瞭解 VMware Endpoint 憑證存放區內的不同存放區。

如需有關 VECS 內不同存放區的詳細資料，請參閱 [VMware Endpoint 憑證存放區概觀](#)。

必要條件

就大多數管理工作而言，您必須具有本機網域管理員帳戶 (administrator@vsphere.local) 的密碼，或其他網域 (如果您在安裝期間變更了網域) 的管理員密碼。

程序

- 1 從網頁瀏覽器中，透過指定以下 URL 來連線到 Platform Services Controller：

`https://psc_hostname_or_IP/psc`

在內嵌式部署中，Platform Services Controller 主機名稱或 IP 位址與 vCenter Server 主機名稱或 IP 位址相同。

- 2 指定 administrator@vsphere.local 或 vCenter Single Sign-On 管理員群組的其他成員的使用者名稱和密碼。

如果在安裝期間指定了其他網域，請以 administrator@mydomain 身分登入。

- 3 在 [憑證] 下，按一下 **憑證存放區**，然後深入瞭解存放區。

- 4 從下拉式功能表選取 VMware Endpoint 憑證存放區 (VECS) 內您想要深入瞭解的存放區。

[VMware Endpoint 憑證存放區概觀](#)會說明個別存放區內的項目。

- 5 若要檢視憑證的詳細資料，請選取該憑證，然後按一下 **顯示詳細資料** 圖示。

- 6 若要從所選存放區中刪除項目，請按一下 **刪除項目** 圖示。

例如，如果您取代現有憑證，稍後可以移除舊的根憑證。請務必確定憑證已不再使用，才將其移除。

從 Platform Services Controller Web 介面將憑證取代為新的 VMCA 簽署憑證

您可以使用新的 VMCA 簽署的憑證取代所有 VMCA 簽署的憑證；此程序稱為更新憑證。您可以從 Platform Services Controller Web 介面更新所選憑證或您環境中的所有憑證。

必要條件

要管理憑證，您必須提供本機網域管理員 (預設為 administrator@vsphere.local) 的密碼。如果要為 vCenter Server 系統更新憑證，您還必須為在 vCenter Server 系統上具有管理員權限的使用者提供 vCenter Single Sign-On 認證。

程序

- 1 從網頁瀏覽器中，透過指定以下 URL 來連線到 Platform Services Controller：

`https://psc_hostname_or_IP/psc`

在內嵌式部署中，Platform Services Controller 主機名稱或 IP 位址與 vCenter Server 主機名稱或 IP 位址相同。

- 2 指定 administrator@vsphere.local 或 vCenter Single Sign-On 管理員群組的其他成員的使用者名稱和密碼。

如果在安裝期間指定了其他網域，請以 administrator@mydomain 身分登入。

- 3 在 [憑證] 下，選取**憑證管理**，並指定 Platform Services Controller 的 IP 位址或主機名稱，以及本機網域管理員 (預設為 administrator@vsphere.local) 的使用者名稱和密碼，然後按一下**提交**。
- 4 更新本機系統的機器 SSL 憑證。
 - a 按一下**機器憑證索引**標籤。
 - b 選取憑證，按一下**更新**，然後在出現提示時回答**是**。
- 5 (選擇性) 更新本機系統的解決方案使用者憑證。
 - a 按一下**解決方案使用者憑證索引**標籤。
 - b 選取憑證並按一下**更新**以更新個別選取的憑證，或按一下**全部更新**以更新所有解決方案使用者憑證。
 - c 在出現提示時回答**是**。
- 6 如果您的環境包含外部 Platform Services Controller，則您可為每個 vCenter Server 系統更新憑證。
 - a 在 [憑證管理] 面板中按一下**登出**按鈕。
 - b 當系統提示時，指定 vCenter Server 系統的 IP 位址或 FQDN，以及可向 vCenter Single Sign-On 驗證的 vCenter Server 管理員的使用者名稱和密碼。
 - c 在 vCenter Server 上更新機器 SSL 憑證，並選擇性地更新每個解決方案使用者憑證。
 - d 如果您的環境中具有多個 vCenter Server 系統，請為每個系統重複以上程序。

後續步驟

重新啟動 Platform Services Controller 上的服務。您可以重新啟動 Platform Services Controller，也可以從命令列執行下列命令：

Windows

在 Windows 上，服務控制命令位於 `VCENTER_INSTALL_PATH\bin`。

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

在 Platform Services Controller Web 介面中使 VMCA 成為中繼憑證授權機構

您可以使用由其他 CA 簽署的 VMCA 憑證，以便 VMCA 成為中繼 CA，然後，VMCA 產生的所有憑證都將包含完整鏈結。

您可透過使用 vSphere Certificate Manager 公用程式、CLI 或從 Platform Services Controller Web 介面執行此設定。

必要條件

- 1 產生 CSR。
- 2 編輯您接收的憑證，並將目前 VMCA 根憑證置於底部。

使用 [vSphere Certificate Manager 產生 CSR 並準備根憑證 \(中繼 CA\)](#) 說明了這兩個步驟。

程序

- 1 從網頁瀏覽器中，透過指定以下 URL 來連線到 Platform Services Controller：

`https://psc_hostname_or_IP/psc`

在內嵌式部署中，Platform Services Controller 主機名稱或 IP 位址與 vCenter Server 主機名稱或 IP 位址相同。

- 2 指定 administrator@vsphere.local 或 vCenter Single Sign-On 管理員群組的其他成員的使用者名稱和密碼。

如果在安裝期間指定了其他網域，請以 administrator@mydomain 身分登入。

- 3 若要將現有憑證取代為鏈結的憑證，請遵循下列步驟：

- a 在 [憑證] 下，按一下 **憑證授權機構**，然後選取 **根憑證** 索引標籤。
- b 按一下 **取代憑證**。新增私密金鑰檔案和憑證檔案 (完整鏈結)，然後按一下 **確定**。
- c 在 **取代根憑證** 對話方塊中，按一下 **瀏覽** 並選取私密金鑰，然後再次按一下 **瀏覽** 並選取憑證，最後按一下 **確定**。

接著，VMCA 會簽署其核發的所有憑證以及新鏈結的根憑證。

- 4 更新本機系統的機器 SSL 憑證。

- a 在 [憑證] 下，按一下 **憑證管理**，然後按一下 **機器憑證** 索引標籤。
- b 選取憑證，按一下 **更新**，然後在出現提示時回答是。

VMCA 將用由新 CA 簽署的憑證取代機器 SSL 憑證。

- 5 (選擇性) 更新本機系統的解決方案使用者憑證。

- a 按一下 **解決方案使用者憑證** 索引標籤。
- b 選取憑證並按一下 **更新** 來更新個別選取的憑證，或按一下 **全部更新** 來取代所有憑證並在出現提示時回答是。

VMCA 將用由新 CA 簽署的憑證取代解決方案使用者憑證或所有解決方案使用者憑證。

- 6 如果您的環境包含外部 Platform Services Controller，則您可為每個 vCenter Server 系統更新憑證。
 - a 在 [憑證管理] 面板中按一下**登出**按鈕。
 - b 當系統提示時，指定 vCenter Server 系統的 IP 位址或 FQDN，以及可向 vCenter Single Sign-On 驗證的 vCenter Server 管理員的使用者名稱和密碼。
 - c 在 vCenter Server 上更新機器 SSL 憑證，並選擇性地更新每個解決方案使用者憑證。
 - d 如果您的環境中具有多個 vCenter Server 系統，請為每個系統重複以上程序。

後續步驟

重新啟動 Platform Services Controller 上的服務。您可以重新啟動 Platform Services Controller，也可以從命令列執行下列命令：

Windows

在 Windows 上，服務控制命令位於 `VCENTER_INSTALL_PATH\bin`。

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

從 Platform Services Controller 將您的系統設定為使用自訂憑證

您可以使用 Platform Services Controller 將環境設定為使用自訂憑證。

您可以使用 Certificate Manager 公用程式針對每個機器和每個解決方案使用者產生憑證簽署要求 (CSR)。將 CSR 提交給您的內部或第三方 CA 後，CA 會傳回已簽署憑證和根憑證。您可以從 Platform Services Controller UI 上傳根憑證和已簽署憑證。

使用 vSphere Certificate Manager 產生憑證簽署要求 (自訂憑證)

您可以使用 vSphere Certificate Manager 產生可隨後與企業 CA 搭配使用或傳送到外部憑證授權機構的憑證簽署要求 (CSR)。您可以將憑證與不同的受支援憑證取代程序搭配使用。

您可以從命令列執行 Certificate Manager 工具，如下所示：

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

必要條件

vSphere Certificate Manager 會提示您輸入資訊。這些提示取決於您的環境和想要取代的憑證類型。

- 每次要產生 CSR 時，系統都會提示您輸入 administrator@vsphere.local 使用者的密碼，或所連線之 vCenter Single Sign-On 網域的管理員。
- 如果您是使用外部 Platform Services Controller 在環境中產生 CSR，系統會提示您輸入 Platform Services Controller 的主機名稱或 IP 位址。
- 若要產生機器 SSL 憑證的 CSR，系統會提示您輸入憑證內容，這些內容儲存在 certtool.cfg 檔案中。對於大部分的欄位，您可以接受預設值，或提供站台專屬值。機器的 FQDN 為必填。

程序

- 1 在您環境中的每台機器上，啟動 vSphere Certificate Manager，然後選取選項 1。
- 2 提供密碼以及 Platform Services Controller IP 位址或主機名稱 (如果出現此提示)。
- 3 選取選項 1 以產生 CSR，回應提示並結束 Certificate Manager。

在程序過程中，您必須提供目錄。Certificate Manager 會將憑證和金鑰檔案放置於目錄中。

- 4 如果還希望取代所有解決方案使用者憑證，請重新啟動 Certificate Manager。
- 5 選取選項 5。
- 6 提供密碼以及 Platform Services Controller IP 位址或主機名稱 (如果出現此提示)。
- 7 選取選項 1 以產生 CSR，回應提示並結束 Certificate Manager。

在程序過程中，您必須提供目錄。Certificate Manager 會將憑證和金鑰檔案放置於目錄中。

在每個 Platform Services Controller 節點上，Certificate Manager 會產生一個憑證和金鑰配對。在每個 vCenter Server 節點上，Certificate Manager 會產生四個憑證和金鑰配對。

後續步驟

執行憑證取代。

將受信任的根憑證新增至憑證存放區

如果要在環境中使用第三方憑證，必須將受信任的根憑證新增至憑證存放區。

必要條件

從第三方或內部 CA 取得自訂根憑證。

程序

- 1 從網頁瀏覽器中，透過指定以下 URL 來連線到 Platform Services Controller：

`https://psc_hostname_or_IP/psc`

在內嵌式部署中，Platform Services Controller 主機名稱或 IP 位址與 vCenter Server 主機名稱或 IP 位址相同。

- 2 指定 administrator@vsphere.local 或 vCenter Single Sign-On 管理員群組的其他成員的使用者名稱和密碼。

如果在安裝期間指定了其他網域，請以 administrator@mydomain 身分登入。

- 3 在 [憑證] 下，選取**憑證管理**，並指定 Platform Services Controller 的 IP 位址或主機名稱，以及本機網域管理員 (預設為 administrator@vsphere.local) 的使用者名稱和密碼，然後按一下**提交**。

- 4 選取**受信任的根憑證**，然後按一下**新增憑證**。

- 5 按一下**瀏覽**，然後選取憑證鏈結的位置。

您可以使用以下檔案類型：CER、PEM 或 CRT。

後續步驟

將機器 SSL 憑證及解決方案使用者憑證 (後者可選) 取代為由此 CA 簽署的憑證。

從 Platform Services Controller 新增自訂憑證

您可以從 Platform Services Controller 將自訂機器 SSL 憑證及自訂解決方案使用者憑證新增至憑證存放區。

大多數情況下，取代每個元件的機器 SSL 憑證就已足夠。解決方案使用者憑證保持在 Proxy 後方。

必要條件

針對您要取代的每個憑證產生憑證簽署要求 (CSR)。您可以透過 Certificate Manager 公用程式來產生 CSR。將憑證和私密金鑰放置到 Platform Services Controller 可存取的位置。

程序

- 1 從網頁瀏覽器中，透過指定以下 URL 來連線到 Platform Services Controller：

`https://psc_hostname_or_IP/psc`

在內嵌式部署中，Platform Services Controller 主機名稱或 IP 位址與 vCenter Server 主機名稱或 IP 位址相同。

- 2 指定 administrator@vsphere.local 或 vCenter Single Sign-On 管理員群組的其他成員的使用者名稱和密碼。

如果在安裝期間指定了其他網域，請以 administrator@mydomain 身分登入。

- 3 在 [憑證] 下，選取**憑證管理**，並指定 Platform Services Controller 的 IP 位址或主機名稱，以及本機網域管理員 (預設為 administrator@vsphere.local) 的使用者名稱和密碼，然後按一下**提交**。
- 4 若要取代機器憑證，請遵循下列步驟：
 - a 選取**機器憑證**索引標籤，然後按一下要取代的憑證。
 - b 依序按一下**取代**和**瀏覽**以取代憑證鏈結，然後按一下**瀏覽**以取代私密金鑰。
- 5 若要取代解決方案使用者憑證，請遵循下列步驟：
 - a 選取**解決方案使用者憑證**索引標籤，然後針對某個元件按一下四個憑證中的第一個憑證，例如**機器**。
 - b 依序按一下**取代**和**瀏覽**以取代憑證鏈結，然後按一下**瀏覽**以取代私密金鑰。
 - c 針對同一元件的其他三個憑證重複上述程序。

後續步驟

重新啟動 Platform Services Controller 上的服務。您可以重新啟動 Platform Services Controller，也可以從命令列執行下列命令：

Windows

在 Windows 上，服務控制命令位於 `VCENTER_INSTALL_PATH\bin`。

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

透過 vSphere Certificate Manager 公用程式管理憑證

vSphere Certificate Manager 公用程式可讓您使用命令列以互動方式執行大部分憑證管理工作。vSphere Certificate Manager 會提示您輸入要執行的工作、憑證位置及其他資訊 (視需要)，接著為您進行停止和啟動服務以及取代憑證。

如果使用 vSphere Certificate Manager，您並不需要將憑證置於 VECS (VMware Endpoint 憑證存放區)，也不需要啟動和停止服務。

執行 vSphere Certificate Manager 之前，確保您瞭解取代程序，並取得要使用的憑證。

注意 vSphere Certificate Manager 支援一個還原層級。如果您執行了 vSphere Certificate Manager 兩次，之後發現無意間造成環境損毀，工具將無法還原到第一次執行前的狀態。

您可以在命令列上執行工具，如下所示：

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

程序

1 重新發佈舊憑證以還原最後執行的作業

使用 vSphere Certificate Manager 執行憑證管理作業時，在憑證遭到取代之前，目前的憑證狀態會儲存於 VECS 的 BACKUP_STORE 存放區中。您可以還原最後執行的作業並恢復為先前的狀態。

2 重設所有憑證

如果您希望將全部現有 vCenter 憑證取代為由 VMCA 簽署的憑證，請使用重設所有憑證選項。

3 重新產生新的 VMCA 根憑證並取代所有憑證

您可以重新產生 VMCA 根憑證，並將本機機器 SSL 憑證和本機解決方案使用者憑證取代為 VMCA 簽署憑證。在多節點部署中，於 Platform Services Controller 上使用此選項執行 vSphere Certificate Manager，接著於所有其他節點上再次執行公用程式，並選取用 VMCA 憑證取代機器 SSL 憑證和用 VMCA 憑證取代解決方案使用者憑證。

4 使 VMCA 成為中繼憑證授權機構 (Certificate Manager)

您可以遵循 Certificate Manager 公用程式中的提示，使 VMCA 成為中繼 CA。完成此程序後，VMCA 會簽署所有具有完整鏈結的新憑證。如果需要，您可以使用 Certificate Manager 將所有現有憑證取代為新的 VMCA 簽署的憑證。

5 用自訂憑證取代所有憑證 (Certificate Manager)

您可使用 vSphere Certificate Manager 公用程式來用自訂憑證取代所有憑證。在您啟動此程序之前，必須將 CSR 傳送給您的 CA。您可使用 Certificate Manager 來產生 CSR。

重新發佈舊憑證以還原最後執行的作業

使用 vSphere Certificate Manager 執行憑證管理作業時，在憑證遭到取代之前，目前的憑證狀態會儲存於 VECS 的 BACKUP_STORE 存放區中。您可以還原最後執行的作業並恢復為先前的狀態。

備註 還原作業會還原目前 BACKUP_STORE 中的內容。如果您使用兩個不同選項執行 vSphere Certificate Manager，並接著嘗試還原，將只能還原上一個作業。

重設所有憑證

如果您希望將全部現有 vCenter 憑證取代為由 VMCA 簽署的憑證，請使用重設所有憑證選項。

使用此選項時，會覆寫目前 VECS 中的所有自訂憑證。

- 在 Platform Services Controller 節點上，vSphere Certificate Manager 可以重新產生根憑證，並取代機器 SSL 憑證和機器解決方案使用者憑證。
- 在管理節點上，vSphere Certificate Manager 可以取代機器 SSL 憑證和所有解決方案使用者憑證。
- 在內嵌式部署中，vSphere Certificate Manager 可以取代所有憑證。

取代的憑證取決於您選擇的選項。

重新產生新的 VMCA 根憑證並取代所有憑證

您可以重新產生 VMCA 根憑證，並將本機機器 SSL 憑證和本機解決方案使用者憑證取代為 VMCA 簽署憑證。在多節點部署中，於 Platform Services Controller 上使用此選項執行 vSphere Certificate Manager，接著於所有其他節點上再次執行公用程式，並選取用 VMCA 憑證取代機器 SSL 憑證和用 VMCA 憑證取代解決方案使用者憑證。

執行此命令時，vSphere Certificate Manager 會提示您輸入密碼及憑證資訊，並將密碼以外的所有資訊儲存於 `certtool.cfg` 檔案中。之後，會自動進行停止服務、取代所有憑證及重新啟動程序。系統會提示您輸入下列資訊：

- administrator@vsphere.local 的密碼。
- 兩個字母形式的國碼
- 公司名稱
- 組織名稱
- 組織單位
- 狀態
- 位置
- IP 位址 (選用)
- 電子郵件
- 主機名稱，即要進行憑證取代之機器的完整網域名稱
- Platform Services Controller 的 IP 位址 (如果您是在管理節點上執行命令)

必要條件

對於要產生新 VMCA 簽署憑證的機器，您必須知道其 FQDN。所有其他內容都會預設為預先定義的值。IP 位址為選用。

後續步驟

在多節點部署中取代根憑證之後，您必須在含外部 Platform Services Controller 節點的所有 vCenter Server 上重新啟動服務。

使 VMCA 成為中繼憑證授權機構 (Certificate Manager)

您可以遵循 Certificate Manager 公用程式中的提示，使 VMCA 成為中繼 CA。完成此程序後，VMCA 會簽署所有具有完整鏈結的新憑證。如果需要，您可以使用 Certificate Manager 將所有現有憑證取代為新的 VMCA 簽署的憑證。

使用 vSphere Certificate Manager 產生 CSR 並準備根憑證 (中繼 CA)

您可以使用 vSphere Certificate Manager 產生憑證簽署要求 (CSR)。然後將這些 CSR 提交至企業 CA 或外部憑證授權機構進行簽署。您可以將簽署的憑證與其他受支援憑證取代程序搭配使用。

- 您可以使用 vSphere Certificate Manager 建立 CSR。
- 如果您偏好手動建立 CSR，則傳送要求簽署的憑證必須符合下列需求：
 - 金鑰大小：2048 位元或以上
 - 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
 - 若使用自訂憑證，CA 延伸必須設為 true (若為根憑證)，且憑證簽署必須位於需求清單中。
 - 必須啟用 CRL 簽署。
 - [增強金鑰使用方法] 不得包含 [用戶端驗證] 或 [伺服器驗證]。
 - 對憑證鏈結的長度無明確限制。VMCA 預設使用 OpenSSL (為 10 個憑證)。
 - 不支援含萬用字元或多個 DNS 名稱的憑證。
 - 您無法建立 VMCA 的附屬 CA。

如需 Microsoft 憑證授權機構的使用範例，請參閱 VMware 知識庫文章 2112009，建立 Microsoft 憑證授權機構範本，用於在 vSphere 6.0 中建立 SSL 憑證。

必要條件

vSphere Certificate Manager 會提示您輸入資訊。這些提示取決於您的環境和想要取代的憑證類型。

每次要產生 CSR 時，系統都會提示您輸入 administrator@vsphere.local 使用者的密碼，或所連線之 vCenter Single Sign-On 網域的管理員。

程序

- 1 啟動 vSphere Certificate Manager 並選取選項 2。

剛開始時您可以使用此選項產生 CSR，而不是取代憑證。

- 2 提供密碼以及 Platform Services Controller IP 位址或主機名稱 (如果出現此提示)。
- 3 選取選項 1 來產生 CSR 並回應提示。

在程序過程中，您必須提供目錄。Certificate Manager 會將待簽署的憑證 (*.csr 檔案) 及對應的金鑰檔案 (*.key 檔案) 存放在目錄中。

- 4 將憑證發送至 CA 以簽署至企業或外部 CA，並將檔案命名為 `root_signing_cert.cer`。
- 5 在文字編輯器中，按以下方式合併憑證。

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

- 6 將檔案儲存為 `root_signing_chain.cer`。

後續步驟

將現有根憑證取代為鏈結的根憑證。請參閱[將 VMCA 根憑證取代為自訂簽署憑證並取代所有憑證](#)。

將 VMCA 根憑證取代為自訂簽署憑證並取代所有憑證

您可以將 VMCA 根憑證取代為憑證鏈結中包含 VMCA 做為中繼憑證的 CA 簽署憑證。然後，VMCA 產生的所有憑證都會包含完整鏈結。

您可以在內嵌式安裝或外部 Platform Services Controller 上執行 vSphere Certificate Manager，將 VMCA 根憑證取代為自訂簽署憑證。

vSphere Certificate Manager 會提示您輸入下列資訊：

必要條件

- 產生 CSR。
 - 您可以使用 vSphere Certificate Manager 建立 CSR。請參閱[使用 vSphere Certificate Manager 產生 CSR 並準備根憑證 \(中繼 CA\)](#)
 - 如果您偏好手動建立 CSR，則傳送要求簽署的憑證必須符合下列需求：
 - 金鑰大小：2048 位元或以上
 - 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
 - 若使用自訂憑證，CA 延伸必須設為 true (若為根憑證)，且憑證簽署必須位於需求清單中。
 - 必須啟用 CRL 簽署。
 - [增強金鑰使用方法] 不得包含 [用戶端驗證] 或 [伺服器驗證]。
 - 對憑證鏈結的長度無明確限制。VMCA 預設使用 OpenSSL (為 10 個憑證)。
 - 不支援含萬用字元或多個 DNS 名稱的憑證。
 - 您無法建立 VMCA 的附屬 CA。

如需 Microsoft 憑證授權機構的使用範例，請參閱 VMware 知識庫文章 2112009，建立 Microsoft 憑證授權機構範本，用於在 vSphere 6.0 中建立 SSL 憑證。

- 在從第三方或企業 CA 收到憑證後，將它與初始 VMCA 根憑證合併來產生完整鏈結，底部為 VMCA 根憑證。請參閱 [使用 vSphere Certificate Manager 產生 CSR 並準備根憑證 \(中繼 CA\)](#)。
- 收集所需的資訊。
 - administrator@vsphere.local 的密碼。
 - 有效的自訂根憑證 (.crt 檔案)。
 - 有效的自訂根使用者金鑰 (.key 檔案)。

程序

- 1 在內嵌式安裝或外部 Platform Services Controller 上啟動 vSphere Certificate Manager，然後選取選項 2。
- 2 選取選項 2 以啟動憑證取代並回應提示。
 - a 出現提示時，指定根憑證的完整路徑。
 - b 如果是第一次取代憑證，系統會提示您輸入用於機器 SSL 憑證的資訊。
此資訊包含所需的機器 FQDN 並儲存於 certool.cfg 檔案中。
- 3 如果在多節點部署中取代根憑證，您必須在所有 vCenter Server 上重新啟動服務。
- 4 在多節點部署中，使用選項 3 (將機器 SSL 憑證取代為 VMCA 憑證) 和 6 (將解決方案使用者憑證取代為 VMCA 憑證)，在每個 vCenter Server 執行個體上重新產生所有憑證。

當您取代憑證時，VMCA 會以完整鏈結簽署。

後續步驟

視您的環境而定，可能必須明確取代其他憑證。

- 如果公司原則要求您取代所有憑證，請取代 vmdir 根憑證。請參閱 [取代 VMware 目錄服務憑證](#)
- 如果要從 vSphere 5.x 環境升級，您可能必須取代 vmdir 內的 vCenter Single Sign-On 憑證。請參閱 [在混合模式環境中取代 VMware Directory Service 憑證](#)

將機器 SSL 憑證取代為 VMCA 憑證 (中繼 CA)

在使用 VMCA 作為中繼 CA 的多節點部署中，您必須明確取代機器 SSL 憑證。先取代 Platform Services Controller 節點上的 VMCA 根憑證，然後取代 vCenter Server 節點上的憑證，以便使用完整鏈結簽署憑證。您亦可使用該選項來取代已損壞或即將到期的機器 SSL 憑證。

將現有機器 SSL 憑證取代為新的 VMCA 簽署憑證時，vSphere Certificate Manager 會提示您輸入資訊並將所有值 (除了 Platform Services Controller 的密碼及 IP 位址) 輸入 certool.cfg 檔案。

- administrator@vsphere.local 的密碼。
- 兩個字母形式的國碼
- 公司名稱

- 組織名稱
- 組織單位
- 狀態
- 位置
- IP 位址 (選用)
- 電子郵件
- 主機名稱，即要進行憑證取代之機器的完整網域名稱。如果主機名稱與 FQDN 不相符，憑證取代就無法正確完成，而您的環境可能會最終處於不穩定狀態。
- Platform Services Controller 的 IP 位址 (如果您是在管理節點上執行命令)

必要條件

- 如果已在多節點部署中取代 VMCA 根憑證，請明確重新啟動所有 vCenter Server 節點。
- 您必須瞭解以下資訊以使用此選項執行 Certificate Manager。
 - administrator@vsphere.local 的密碼。
 - 您希望產生新 VMCA 簽署憑證之機器的 FQDN。所有其他內容都會預設為預先定義的值，但您可以變更這些值。
 - 在含有外部 Platform Services Controller 的 vCenter Server 系統上執行時，Platform Services Controller 的主機名稱或 IP 位址。

程序

- 1 啟動 vSphere Certificate Manager 並選取選項 3。
- 2 對提示做出回應。

Certificate Manager 在 `certtool.cfg` 檔案中儲存資訊。

結果

vSphere Certificate Manager 取代機器 SSL 憑證。

將解決方案使用者憑證取代為 VMCA 憑證 (中繼 CA)

在將 VMCA 用作中繼 CA 的多節點上，您必須明確取代解決方案使用者憑證。先取代 Platform Services Controller 節點上的 VMCA 根憑證，然後取代 vCenter Server 節點上的憑證，以便使用完整鏈結簽署憑證。您亦可使用該選項來取代已損壞或即將到期的解決方案使用者憑證。

必要條件

- 如果已在多節點部署中取代 VMCA 根憑證，請明確重新啟動所有 vCenter Server 節點。
- 您必須瞭解以下資訊以使用此選項執行 Certificate Manager。
 - administrator@vsphere.local 的密碼。

- 在含有外部 Platform Services Controller 的 vCenter Server 系統上執行時，Platform Services Controller 的主機名稱或 IP 位址。

程序

- 1 啟動 vSphere Certificate Manager 並選取選項 6。
- 2 對提示做出回應。

結果

vSphere Certificate Manager 將取代所有解決方案使用者憑證。

用自訂憑證取代所有憑證 (Certificate Manager)

您可使用 vSphere Certificate Manager 公用程式來用自訂憑證取代所有憑證。在您啟動此程序之前，必須將 CSR 傳送給您的 CA。您可使用 Certificate Manager 來產生 CSR。

一個選項只能取代機器 SSL 憑證，並使用 VMCA 佈建的解決方案使用者憑證。解決方案使用者憑證僅用於 vSphere 元件之間的通訊。

當您使用自訂憑證時，您負責佈建新增至具有自訂憑證之環境的每個節點。VMCA 仍然使用 VMCA 簽署的憑證佈建，您負責取代這些憑證。您可使用 vSphere Certificate Manager 公用程式或使用 CLI 來取代手動憑證。憑證存儲在 VECS 中。

使用 vSphere Certificate Manager 產生憑證簽署要求 (自訂憑證)

您可以使用 vSphere Certificate Manager 產生可隨後與企業 CA 搭配使用或傳送到外部憑證授權機構的憑證簽署要求 (CSR)。您可以將憑證與不同的受支援憑證取代程序搭配使用。

您可以從命令列執行 Certificate Manager 工具，如下所示：

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

必要條件

vSphere Certificate Manager 會提示您輸入資訊。這些提示取決於您的環境和想要取代的憑證類型。

- 每次要產生 CSR 時，系統都會提示您輸入 administrator@vsphere.local 使用者的密碼，或所連線之 vCenter Single Sign-On 網域的管理員。
- 如果您是使用外部 Platform Services Controller 在環境中產生 CSR，系統會提示您輸入 Platform Services Controller 的主機名稱或 IP 位址。
- 若要產生機器 SSL 憑證的 CSR，系統會提示您輸入憑證內容，這些內容儲存在 certtool.cfg 檔案中。對於大部分的欄位，您可以接受預設值，或提供站台專屬值。機器的 FQDN 為必填。

程序

- 1 在您環境中的每台機器上，啟動 vSphere Certificate Manager，然後選取選項 1。
- 2 提供密碼以及 Platform Services Controller IP 位址或主機名稱 (如果出現此提示)。
- 3 選取選項 1 以產生 CSR，回應提示並結束 Certificate Manager。

在程序過程中，您必須提供目錄。Certificate Manager 會將憑證和金鑰檔案放置於目錄中。

- 4 如果還希望取代所有解決方案使用者憑證，請重新啟動 Certificate Manager。
- 5 選取選項 5。
- 6 提供密碼以及 Platform Services Controller IP 位址或主機名稱 (如果出現此提示)。
- 7 選取選項 1 以產生 CSR，回應提示並結束 Certificate Manager。

在程序過程中，您必須提供目錄。Certificate Manager 會將憑證和金鑰檔案放置於目錄中。

在每個 Platform Services Controller 節點上，Certificate Manager 會產生一個憑證和金鑰配對。在每個 vCenter Server 節點上，Certificate Manager 會產生四個憑證和金鑰配對。

後續步驟

執行憑證取代。

將機器 SSL 憑證取代為自訂憑證

機器 SSL 憑證是由每個管理節點、Platform Services Controller 以及內嵌式部署上的反向 Proxy 服務所使用。每台機器必須具有機器 SSL 憑證，以便與其他服務進行安全通訊。您可以將每個節點上的憑證取代為自訂憑證。

必要條件

開始前，您需要環境中每台機器的 CSR。您可以使用 vSphere Certificate Manager 或明確地產生 CSR。

- 1 若要使用 vSphere Certificate Manager 產生 CSR，請參閱[使用 vSphere Certificate Manager 產生憑證簽署要求 \(自訂憑證\)](#)。
- 2 若要明確產生 CSR，請向第三方或企業 CA 要求每台機器的憑證。憑證必須符合以下需求：
 - 金鑰大小：2048 位元或以上 (PEM 編碼)
 - CRT 格式
 - x509 第 3 版
 - SubjectAltName 必須包含 DNS Name=<machine_FQDN>
 - 包含下列金鑰使用方法：數位簽章、不可否認性、金鑰編密

另請參閱 VMware 知識庫文章 [2112014](#)，從 Microsoft 憑證授權機構取得 vSphere 憑證。

程序

- 1 啟動 vSphere Certificate Manager 並選取選項 1。

2 選取選項 2 以啟動憑證取代並回應提示。

vSphere Certificate Manager 會提示您輸入下列資訊：

- administrator@vsphere.local 的密碼。
- 有效的機器 SSL 自訂憑證 (.crt 檔案)。
- 有效的機器 SSL 自訂金鑰 (.key 檔案)。
- 用於自訂機器 SSL 憑證 (.crt 檔案) 的有效簽署憑證。
- 如果您在多節點部署中的管理節點上執行命令，需要 Platform Services Controller 的 IP 位址。

後續步驟

視您的環境而定，可能必須明確取代其他憑證。

- 如果公司原則要求您取代所有憑證，請取代 vmdir 根憑證。請參閱[取代 VMware 目錄服務憑證](#)
- 如果要從 vSphere 5.x 環境升級，您可能必須取代 vmdir 內的 vCenter Single Sign-On 憑證。請參閱[在混合模式環境中取代 VMware Directory Service 憑證](#)

將解決方案使用者憑證取代為自訂憑證

許多公司僅要求您取代可從外部存取之服務的憑證。但 Certificate Manager 也支援取代解決方案使用者憑證。解決方案使用者是多種服務的集合，例如與 vSphere Web Client 相關聯的所有服務。在多節點部署中，取代 Platform Services Controller 上的機器解決方案使用者憑證，以及每個管理節點上的一組完整解決方案使用者。

如果系統提示您使用解決方案使用者憑證，請提供第三方 CA 的完整簽署憑證鏈結。

格式應類似以下內容。

```
-----BEGIN CERTIFICATE-----
Signing certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

必要條件

開始前，您需要環境中每台機器的 CSR。您可以使用 vSphere Certificate Manager 或明確地產生 CSR。

- 1 若要使用 vSphere Certificate Manager 產生 CSR，請參閱[使用 vSphere Certificate Manager 產生憑證簽署要求 \(自訂憑證\)](#)。
- 2 向第三方或企業 CA 為每個節點上的每個解決方案使用者要求憑證。您可以使用 vSphere Certificate Manager 產生 CSR，也可以手動準備。CSR 必須符合以下需求：
 - 金鑰大小：2048 位元或以上 (PEM 編碼)

- CRT 格式
- x509 第 3 版
- SubjectAltName 必須包含 DNS Name=<machine_FQDN>
- 每個解決方案使用者憑證必須具有不同的 Subject。例如，您可以考慮加入解決方案使用者名稱 (例如 vpxd) 或其他唯一識別碼。
- 包含下列金鑰使用方法：數位簽章、不可否認性、金鑰編密

另請參閱 VMware 知識庫文章 [2112014](#)，從 Microsoft 憑證授權機構取得 vSphere 憑證。

程序

- 1 啟動 vSphere Certificate Manager 並選取選項 5。
- 2 選取選項 2 以啟動憑證取代並回應提示。

vSphere Certificate Manager 會提示您輸入下列資訊：

- administrator@vsphere.local 的密碼。
- 機器解決方案使用者的憑證與金鑰。
- 如果您在 Platform Services Controller 節點上執行 vSphere Certificate Manager，系統會提示您提供機器解決方案使用者的憑證與金鑰 (vpxd.crt 和 vpxd.key)。
- 如果您在管理節點或內嵌式部署中執行 vSphere Certificate Manager，系統會提示您提供所有解決方案使用者的一組完整憑證與金鑰 (vpxd.crt 和 vpxd.key)。

後續步驟

如果要從 vSphere 5.x 環境升級，您可能必須取代 vmdir 內的 vCenter Single Sign-On 憑證。請參閱在 [混合模式環境中取代 VMware Directory Service 憑證](#)。

手動憑證取代

在某些特殊情況下 (例如，若您希望只取代一個類型的解決方案使用者憑證)，不能使用 vSphere Certificate Manager 公用程式。在此情況下，您可以使用隨附於安裝的 CLI 進行憑證取代。

瞭解啟動和停止服務

對於手動憑證取代的某些部分，您必須停止所有服務，接著僅啟動管理憑證基礎結構的服務。如果您僅在需要時停止服務，可最大程度地縮短停機時間。

遵循下列經驗法則：

- 請勿停止服務以產生新的公開/私密金鑰配對或新憑證。
- 如果您是唯一的管理員，當您新增根憑證時，不需要停止服務。舊的根憑證仍然可用，所有服務仍可以使用該憑證進行驗證。新增根憑證後，請將所有服務停止並立即重新啟動，以避免主機發生問題。
- 如果您的環境包含多個管理員，請在新增根憑證前停止服務，並於新增憑證後重新啟動服務。

- 請在執行下列工作前停止服務：
 - 刪除機器 SSL 憑證或 VECS 中的任何解決方案使用者憑證。
 - 取代 vmdir (VMware 目錄服務) 中的解決方案使用者憑證。

用新的 VMCA 簽署憑證取代現有的 VMCA 簽署憑證

如果 VMCA 根憑證將於近期到期，或您基於其他理由希望取代該憑證，您可以產生新的根憑證，並將其新增到 VMware 目錄服務中。接著，您可以使用新的根憑證，產生新的機器 SSL 憑證和解決方案使用者憑證。

在大部分情況下，您可以使用 vSphere Certificate Manager 公用程式取代憑證。

如果您需要進行更為精細的控制，此案例提供了使用 CLI 命令取代一組完整憑證的詳細逐步指示。您也可以使用對應工作中的程序，僅取代個別憑證。

必要條件

只有 administrator@vsphere.local 或 CAAdmins 群組中的其他使用者能夠執行憑證管理工作。請參閱 [向 vCenter Single Sign-On 群組新增成員](#)。

程序

1 產生新的 VMCA 簽署根憑證

您可以使用 `certool` CLI 產生新的 VMCA 簽署憑證，並將憑證發佈到 vmdir。

2 用 VMCA 簽署憑證取代機器 SSL 憑證

產生新的 VMCA 簽署根憑證後，您可以取代環境中的所有機器 SSL 憑證。

3 用新的 VMCA 簽署憑證取代解決方案使用者憑證

取代機器 SSL 憑證後，您可以取代所有解決方案使用者憑證。解決方案使用者憑證必須有效 (即並未到期)，但憑證基礎結構並不會使用憑證中的任何其他資訊。

4 在混合模式環境中取代 VMware Directory Service 憑證

在升級期間，您的環境可能會暫時同時包含 vCenter Single Sign-On 5.5 版本和 vCenter Single Sign-On 6.x 版本。這種情況下，如果您取代 vCenter Single Sign-On 服務執行所在節點的 SSL 憑證，必須執行額外步驟以取代 VMware Directory Service SSL 憑證。

產生新的 VMCA 簽署根憑證

您可以使用 `certool` CLI 產生新的 VMCA 簽署憑證，並將憑證發佈到 vmdir。

在多節點部署中，您需要在 Platform Services Controller 上執行根憑證產生命令。

程序

1 產生新的自我簽署憑證和私密金鑰。

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config
<config_file>
```

2 將現有根憑證取代為新的憑證。

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

命令會產生憑證、將憑證新增至 vmdir 及 VECS。

3 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

Windows 和 vCenter Server Appliance 上的服務名稱並不相同。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

4 (選擇性) 將新的根憑證發佈到 vmdir。

```
dir-cli trustedcert publish --cert newRoot.crt
```

當您執行此命令時，所有 vmdir 執行個體都會立即更新。否則，傳播到所有執行個體可能需要一些時間。

5 重新啟動所有服務。

```
service-control --start --all
```

範例：產生新的 VMCA 簽署根憑證

下列範例會顯示確認目前根 CA 資訊以及重新產生根憑證的一組完整步驟。

1 (選用) 列出 VMCA 根憑證以確定其位於憑證存放區。

- 在 Platform Services Controller 節點或內嵌式安裝中：

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --getrootca
```

- 在管理節點 (外部安裝) 上：

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --getrootca --server=<psc-  
ip-or-fqdn>
```

輸出會類似下列內容：

```
output:
Certificate:
Data:
Version:3 (0x2)
Serial Number:
cf:2d:ff:49:88:50:e5:af
...
```

- 2 (選用) 列出 VECS TRUSTED_ROOTS 存放區並比較此處憑證序號與步驟 1 的輸出內容。

此命令在 Platform Services Controller 和管理節點上都有效，因為 VECS 會輪詢 vmdir。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry list --store TRUSTED_ROOTS
--text
```

在只有一個根憑證的最單純情況下，輸出會類似下列內容：

```
Number of entries in store :    1
Alias :960d43f31eb95211ba3a2487ac840645a02894bd
Entry type :Trusted Cert
Certificate:
Data:
Version:3 (0x2)
Serial Number:
cf:2d:ff:49:88:50:e5:af
```

- 3 產生新的 VMCA 根憑證。憑證會新增到 VECS 中的 TRUSTED_ROOTS 存放區以及 vmdir (VMware 目錄服務)。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --selfca --config="C:\Program
Files\VMware\vCenter Server\vmcad\certool.cfg"
```

在 Windows 上，--config 為選用選項，因為該命令使用預設的 certool.cfg 檔案。

用 VMCA 簽署憑證取代機器 SSL 憑證

產生新的 VMCA 簽署根憑證後，您可以取代環境中的所有機器 SSL 憑證。

每台機器必須具有機器 SSL 憑證，以便與其他服務進行安全通訊。在多節點部署中，您必須在每個節點上執行機器 SSL 憑證產生命令。使用 --server 參數從含外部 Platform Services Controller 的 vCenter Server 指向 Platform Services Controller。

必要條件

準備好停止所有服務，並啟動用於處理憑證傳播和儲存的服務。

程序

- 1 為每部需要新憑證的機器製作一份 certtool.cfg 的複本。

您可以在以下位置找到 certtool.cfg：

作業系統	路徑
Windows	C:\Program Files\VMware\vCenter Server\vmcad
Linux	/usr/lib/vmware-vmca/share/config/

- 2 編輯每台機器的自訂組態檔以納入該機器的 FDQN。

按照機器的 IP 位址執行 NSLookup，以查看 DNS 的名稱清單，然後在檔案中為 [主機名稱] 欄位使用該名稱。

- 3 為每個檔案產生公開/私密金鑰檔案配對和憑證，並於您先前自訂的組態檔中傳遞。

例如：

```
certtool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certtool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --
config machine1.cfg
```

- 4 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

Windows 和 vCenter Server Appliance 上的服務名稱並不相同。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

- 5 新增憑證到 VECS。

所有機器都需要使用本機憑證存放區中的新憑證，以透過 SSL 進行通訊。您需要先刪除現有項目，接著再新增項目。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.crt
--key machine1.priv
```


6 重新啟動所有服務。

```
service-control --start --all
```

範例：將機器憑證取代為 VMCA 簽署憑證

- 1 為 SSL 憑證建立組態檔，命名為 `ssl-config.cfg` 並儲存於當前目錄中。

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

- 2 為機器 SSL 憑證產生金鑰配對。在每個管理節點和 Platform Services Controller 節點上執行此命令；不需要使用 `--server` 選項。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

`ssl-key.priv` 和 `ssl-key.pub` 檔案均在當前目錄中建立。

- 3 產生新的機器 SSL 憑證。此憑證是由 VMCA 簽署的。如果您將 VMCA 根憑證取代為自訂憑證，VMCA 會簽署所有具有完整鏈結的憑證。

- 在 Platform Services Controller 節點或內嵌式安裝中：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- 在 vCenter Server (外部安裝) 上：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

`new-vmca-ssl.crt` 檔案於當前目錄中建立。

- 4 (選用) 列出 VECS 的內容。

```
"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli store list
```

- Platform Services Controller 上的輸出：

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- vCenter Server 上的輸出：

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

- 5 將 VECS 中的機器 SSL 憑證取代為新的機器 SSL 憑證。--store 和 --alias 值必須與預設名稱完全相符。

- 在 Platform Services Controller 上，執行下列命令以更新 MACHINE_SSL_CERT 存放區中的機器 SSL 憑證。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- 在每個管理節點或內嵌式部署中，執行下列命令以更新 MACHINE_SSL_CERT 存放區中的機器 SSL 憑證。您必須為每台機器個別更新憑證，因為每台機器的 FQDN 都不相同。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

後續步驟

您也可以取代 ESXi 主機的憑證。請參閱《vSphere 安全性》出版物。

在多節點部署中取代根憑證之後，您必須在含外部 Platform Services Controller 節點的所有 vCenter Server 上重新啟動服務。

用新的 VMCA 簽署憑證取代解決方案使用者憑證

取代機器 SSL 憑證後，您可以取代所有解決方案使用者憑證。解決方案使用者憑證必須有效 (即並未到期)，但憑證基礎結構並不會使用憑證中的任何其他資訊。

您會在每個管理節點與每個 Platform Services Controller 節點上取代機器解決方案使用者憑證。您只會在每個管理節點上取代其他解決方案使用者憑證。在包含外部 Platform Services Controller 的管理節點上執行命令時，請使用 --server 參數指向 Platform Services Controller。

備註 當您列出大型部署中的解決方案使用者憑證時，dir-cli list 的輸出會包含所有節點上的所有解決方案使用者。執行 vmafd-cli get-machine-id --server-name localhost 以找出每台主機的本機機器識別碼。每個解決方案使用者名稱都包含機器識別碼。

必要條件

準備好停止所有服務，並啟動用於處理憑證傳播和儲存的服務。

程序

- 1 製作一份 `certool.cfg` 的複本，移除名稱、IP 位址、DNS 名稱和電子郵件欄位，然後重新命名該檔案 (例如重新命名為 `sol_usr.cfg`)。

做為產生過程的一部分，您可以從命令列重新命名憑證。解決方案使用者無需其他資訊。如果保留預設資訊，所產生的憑證可能會造成混淆。

- 2 為每個解決方案使用者產生公開/私密金鑰檔案配對和憑證，並於您先前自訂的組態檔中傳遞。

例如：

```
certool --genkey --privkey=vpzd.priv --pubkey=vpzd.pub
certool --gencert --privkey=vpzd.priv --cert vpzd.crt --Name=VPXD_1 --config sol_usr.cfg
```

- 3 找到每個解決方案使用者的名稱。

```
dir-cli service list
```

您可以使用取代憑證時返回的唯一識別碼。輸入和輸出內容可能如下。

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpzd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpzd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

當您列出多節點部署中的解決方案使用者憑證時，`dir-cli list` 的輸出會包含所有節點上的所有解決方案使用者。請執行 `vmafd-cli get-machine-id --server-name localhost` 以找出每台主機的本機機器識別碼。每個解決方案使用者名稱都包含機器識別碼。

- 4 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

Windows 和 vCenter Server Appliance 上的服務名稱並不相同。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 針對每個解決方案使用者，先後取代 vmdir 和 VECS 中的現有憑證。

下列範例說明如何取代 vpxd 服務的憑證。

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

備註 如果您不取代 vmdir 中的憑證，解決方案使用者就無法向 vCenter Single Sign-On 進行驗證。

6 重新啟動所有服務。

```
service-control --start --all
```

範例：使用 VMCA 簽署解決方案使用者憑證

- 1 為每個解決方案使用者產生公開/私密金鑰配對。其中包括一組為每個 Platform Services Controller 和每個管理節點上機器解決方案使用者提供的配對，以及一組為每個管理節點上每個其他解決方案使用者 (vpxd、vpxd-extension、vsphere-webclient) 提供的配對。

- a 為內嵌式部署的機器解決方案使用者或 Platform Services Controller 的機器解決方案使用者產生金鑰配對。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-
key.priv --pubkey=machine-key.pub
```

- b (選用) 針對包含外部 Platform Services Controller 的部署，為每個管理節點上的機器解決方案使用者產生金鑰配對。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-
key.priv --pubkey=machine-key.pub
```

- c 為每個管理節點上的 vpxd 解決方案使用者產生金鑰配對。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-
key.priv --pubkey=vpxd-key.pub
```

- d 為每個管理節點上的 vpxd-extension 解決方案使用者產生金鑰配對。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-
extension-key.priv --pubkey=vpxd-extension-key.pub
```

- e 為每個管理節點上的 vsphere-webclient 解決方案使用者產生金鑰配對。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-
webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

- 2 為每個 Platform Services Controller 和每個管理節點上的機器解決方案使用者，以及每個管理節點上的每個其他解決方案使用者 (vpxd、vpxd-extension、vsphere-webclient)，產生由新 VMCA 根憑證簽署的解決方案使用者憑證。

備註 --Name 參數必須是唯一的。包含解決方案使用者存放區的名稱 (例如 vpxd 或 vpxd-extension)，可讓您輕鬆辨識憑證與解決方案使用者之間的對應關係。

- a 在 Platform Services Controller 節點上執行下列命令，為該節點上的機器解決方案使用者產生解決方案使用者憑證。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

- b 為每個管理節點上的機器解決方案使用者產生憑證。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

- c 為每個管理節點上的 vpxd 解決方案使用者產生憑證。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

- d 為每個管理節點上的 vpxd-extensions 解決方案使用者產生憑證。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

- e 執行下列命令，為每個管理節點上的 vsphere-webclient 解決方案使用者產生憑證。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

- 3 將 VECS 中的解決方案使用者憑證取代為新的解決方案使用者憑證。

備註 --store 和 --alias 參數必須與預設服務名稱完全相符。

- a 在 Platform Services Controller 節點上，執行下列命令以取代機器解決方案使用者憑證：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b 取代每個管理節點上的機器解決方案使用者憑證：

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vmadfs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vmadfs-cli entry create --store
machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- c 取代每個管理節點上的 vpxd 解決方案使用者憑證：

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vmadfs-cli entry delete --store vpxd
--alias vpxd
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vmadfs-cli entry create --store vpxd
--alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

- d 取代每個管理節點上的 vpxd-extension 解決方案使用者憑證：

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vmadfs-cli entry delete --store vpxd-
extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vmadfs-cli entry create --store vpxd-
extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-
key.priv
```

- e 取代每個管理節點上的 vsphere-webclient 解決方案使用者憑證。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vmadfs-cli entry delete --store
vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vmadfs-cli entry create --store
vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key
vsphere-webclient-key.priv
```

- 4 使用新的解決方案使用者憑證更新 VMware 目錄服務 (vmdir)。系統會提示您輸入 vCenter Single Sign-On 管理員密碼。

- a 執行 `dir-cli service list`，為每個解決方案使用者取得唯一的服務識別碼尾碼。您可以在 Platform Services Controller 或 vCenter Server 系統上執行此命令。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vmadfs-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

備註 當您列出大型部署中的解決方案使用者憑證時，`dir-cli list` 的輸出會包含所有節點上的所有解決方案使用者。執行 `vmadfs-cli get-machine-id --server-name localhost` 以找出每台主機的本機機器識別碼。每個解決方案使用者名稱都包含機器識別碼。

- b 取代 Platform Services Controller 上 vmdir 中的機器憑證。例如，如果 machine-29a45d00-60a7-11e4-96ff-00505689639a 是 Platform Services Controller 上的機器解決方案使用者，請執行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

- c 取代每個管理節點上 vmdir 中的機器憑證。例如，如果 machine-6fd7f140-60a9-11e4-9e28-005056895a69 是 vCenter Server 上的機器解決方案使用者，請執行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

- d 取代每個管理節點上 vmdir 中的 vpxd 解決方案使用者憑證。例如，如果 vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 是 vpxd 解決方案使用者識別碼，請執行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

- e 取代每個管理節點上 vmdir 中的 vpxd-extension 解決方案使用者憑證。例如，如果 vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 是 vpxd-extension 解決方案使用者識別碼，請執行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

- f 取代每個管理節點上的 vsphere-webclient 解決方案使用者憑證。例如，如果 vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 是 vsphere-webclient 解決方案使用者識別碼，請執行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

後續步驟

在每個 Platform Services Controller 節點和每個管理節點上重新啟動所有服務。

在混合模式環境中取代 VMware Directory Service 憑證

在升級期間，您的環境可能會暫時同時包含 vCenter Single Sign-On 5.5 版本和 vCenter Single Sign-On 6.x 版本。這種情況下，如果您取代 vCenter Single Sign-On 服務執行所在節點的 SSL 憑證，必須執行額外步驟以取代 VMware Directory Service SSL 憑證。

vmdir 會使用 VMware Directory Service SSL 憑證，在執行 vCenter Single Sign-On 複寫的 Platform Services Controller 節點之間進行信號交換。

包含 vSphere 6.0 和 vSphere 6.5 節點的混合模式環境無需這些步驟。只有在下列情況中才需要進行這些步驟：

- 您的環境同時包含 vCenter Single Sign-On 5.5 和 vCenter Single Sign-On 6.x 服務。
- vCenter Single Sign-On 服務已設定為複寫 vmdir 資料。
- 您計劃在執行 vCenter Single Sign-On 6.x 服務的節點上將預設的 VMCA 簽署憑證取代為自訂憑證。

備註 最佳做法為，在重新啟動服務前升級整個環境。一般不建議取代 VMware Directory Service 憑證。

程序

- 1 在執行 vCenter Single Sign-On 6.x 服務的節點上，取代 vmdir SSL 憑證和金鑰。
請參閱[取代 VMware 目錄服務憑證](#)。
- 2 在執行 vCenter Single Sign-On 5.5 服務的節點上進行環境設定，使 vCenter Single Sign-On 6.x 服務成為已知服務。
 - a 備份 C:\ProgramData\VMware\CIS\cfg\vmdir 中的所有檔案。
 - b 在 6.x 節點上建立 vmDirCert.pem 檔案的複本，並將其重新命名為 <sso_node2.domain.com>.pem，其中 <sso_node2.domain.com> 是 6.x 節點的 FQDN。
 - c 將重新命名後的憑證複製到 C:\ProgramData\VMware\CIS\cfg\vmdir，以取代現有的複寫憑證。
- 3 在所有已取代憑證的機器上重新啟動 VMware Directory Service。
您可以從 vSphere Web Client 或使用 service-control 命令重新啟動服務。

使用 VMCA 做為中繼憑證授權機構

您可以將 VMCA 根憑證取代為憑證鏈結中包含 VMCA 的第三方 CA 簽署憑證。然後，VMCA 產生的所有憑證都會包含完整鏈結。您可以將現有憑證取代為新產生的憑證。此方法結合了第三方 CA 簽署憑證的安全性，以及自動憑證管理的便利性。

程序

- 1 [取代根憑證 \(中繼 CA\)](#)
將 VMCA 憑證取代為自訂憑證的第一個步驟，是產生 CSR 並新增做為根憑證傳回給 VMCA 的憑證。
- 2 [取代機器 SSL 憑證 \(中繼 CA\)](#)
從 CA 收到簽署憑證並將其用做 VMCA 根憑證之後，您可以取代所有機器 SSL 憑證。
- 3 [取代解決方案使用者憑證 \(中繼 CA\)](#)
取代機器 SSL 憑證後，您可以取代解決方案使用者憑證。

4 取代 VMware 目錄服務憑證

如果您決定使用新的 VMCA 根憑證，並解除發佈當初佈建環境時使用的 VMCA 根憑證，則您必須取代機器 SSL 憑證、解決方案使用者憑證，以及部分內部服務的憑證。

5 在混合模式環境中取代 VMware Directory Service 憑證

在升級期間，您的環境可能會暫時同時包含 vCenter Single Sign-On 5.5 版本和 vCenter Single Sign-On 6.x 版本。這種情況下，如果您取代 vCenter Single Sign-On 服務執行所在節點的 SSL 憑證，必須執行額外步驟以取代 VMware Directory Service SSL 憑證。

取代根憑證 (中繼 CA)

將 VMCA 憑證取代為自訂憑證的第一個步驟，是產生 CSR 並新增做為根憑證傳回給 VMCA 的憑證。

傳送要求簽署的憑證必須符合下列需求：

- 金鑰大小：2048 位元或以上
- 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
- 若使用自訂憑證，CA 延伸必須設為 true (若為根憑證)，且憑證簽署必須位於需求清單中。
- 必須啟用 CRL 簽署。
- [增強金鑰使用方法] 不得包含 [用戶端驗證] 或 [伺服器驗證]。
- 對憑證鏈結的長度無明確限制。VMCA 預設使用 OpenSSL (為 10 個憑證)。
- 不支援含萬用字元或多個 DNS 名稱的憑證。
- 您無法建立 VMCA 的附屬 CA。

如需 Microsoft 憑證授權機構的使用範例，請參閱 VMware 知識庫文章 2112009，建立 Microsoft 憑證授權機構範本，用於在 vSphere 6.0 中建立 SSL 憑證。

當您取代根憑證時，VMCA 會驗證下列憑證屬性：

- 金鑰大小 2048 位元或以上
- 金鑰使用方式:憑證簽署
- 基本限制：主體類型 CA

程序

- 1 產生 CSR 並將其傳送至您的 CA。

依照 CA 指示進行。

- 2 準備包含已簽署之 VMCA 憑證以及第三方 CA 或企業 CA 之完整 CA 鏈結的憑證檔案，並儲存此檔案 (例如，儲存為 rootcal.crt)。

您可以將所有 PEM 格式的 CA 憑證複製到單一檔案，以完成此項作業。您必須從 VMCA 根憑證開始複製，並於根 CA PEM 憑證結束複製。例如：

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

- 3 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

Windows 和 vCenter Server Appliance 上的服務名稱並不相同。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

- 4 取代現有的 VMCA 根 CA。

```
certool --rootca --cert=rootcal.crt --privkey=root1.key
```

當您執行此命令時，會執行下列動作：

- 將新的自訂根憑證新增到檔案系統中的憑證位置。
- 將自訂根憑證附加到 VECS 中的 TRUSTED_ROOTS 存放區 (過一段時間)。
- 將自訂根憑證新增到 vmdir (過一段時間)。

- 5 (選擇性) 如果要將變更傳播到所有 vmdir (VMware 目錄服務) 執行個體，請將新的根憑證發佈到 vmdir，並提供每個檔案的完整檔案路徑。

例如：

```
dir-cli trustedcert publish --cert rootcal.crt
```

vmdir 節點間的複寫每隔 30 秒會進行一次。您不需要明確將根憑證新增到 VECS，因為 VECS 會每隔 5 分鐘輪詢 vmdir 是否有新的根憑證檔案。

- 6 (選擇性) 如有必要，您可以強制重新整理 VECS。

```
vecs-cli force-refresh
```

- 7 重新啟動所有服務。

```
service-control --start --all
```

範例：取代根憑證

使用 certool 命令與 `--rootca` 選項，將 VMCA 根憑證取代為自訂 CA 根憑證。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\certool" --rootca --cert=C:\custom-  
certs\root.pem --privkey=C:\custom-certs\root.key
```

當您執行此命令時，會執行下列動作：

- 將新的自訂根憑證新增到檔案系統中的憑證位置。
- 將自訂根憑證附加到 VECS 中的 TRUSTED_ROOTS 存放區。
- 將自訂根憑證新增到 vmdir。

後續步驟

如果公司原則需要，您可以從憑證存放區移除原始的 VMCA 根憑證。如果進行移除，您必須重新整理這些內部憑證：

- 取代 vCenter Single Sign-On 簽署憑證。請參閱 [重新整理安全性 Token 服務憑證](#)。
- 取代 VMware 目錄服務憑證。請參閱 [取代 VMware 目錄服務憑證](#)。

取代機器 SSL 憑證 (中繼 CA)

從 CA 收到簽署憑證並將其用做 VMCA 根憑證之後，您可以取代所有機器 SSL 憑證。

這些步驟與取代使用 VMCA 做為憑證授權機構之憑證的步驟基本相同。不過，在此情況下，VMCA 會簽署所有具有完整鏈結的憑證。

每台機器必須具有機器 SSL 憑證，以便與其他服務進行安全通訊。在多節點部署中，您必須在每個節點上執行機器 SSL 憑證產生命令。使用 `--server` 參數從含外部 Platform Services Controller 的 vCenter Server 指向 Platform Services Controller。

必要條件

對於每個機器 SSL 憑證，SubjectAltName 必須包含 `DNS Name=<Machine FQDN>`。

程序

- 1 為每部需要新憑證的機器製作一份 `certtool.cfg` 的複本。

您可以在以下位置找到 `certtool.cfg`：

Windows

`C:\Program Files\VMware\vCenter Server\vmcad`

Linux

`/usr/lib/vmware-vmca/share/config/`

- 2 編輯每台機器的自訂組態檔以納入該機器的 FDQN。

按照機器的 IP 位址執行 `NSLookup`，以查看 DNS 的名稱清單，然後在檔案中為 [主機名稱] 欄位使用該名稱。

- 3 為每台機器產生公開/私密金鑰檔案配對和憑證，並於您先前自訂的組態檔中傳遞。

例如：

```
certtool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certtool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --
config machine1.cfg
```

- 4 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

Windows 和 vCenter Server Appliance 上的服務名稱並不相同。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

- 5 新增憑證到 VECS。

所有機器都需要使用本機憑證存放區中的新憑證，以透過 SSL 進行通訊。您需要先刪除現有項目，接著再新增項目。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

6 重新啟動所有服務。

```
service-control --start --all
```

範例：取代機器 SSL 憑證 (VMCA 為中繼 CA)

- 1 為 SSL 憑證建立組態檔，命名為 `ssl-config.cfg` 並儲存於當前目錄中。

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

- 2 為機器 SSL 憑證產生金鑰配對。在每個管理節點和 Platform Services Controller 節點上執行此命令；不需要使用 `--server` 選項。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

`ssl-key.priv` 和 `ssl-key.pub` 檔案均在當前目錄中建立。

- 3 產生新的機器 SSL 憑證。此憑證是由 VMCA 簽署的。如果您將 VMCA 根憑證取代為自訂憑證，VMCA 會簽署所有具有完整鏈結的憑證。

- 在 Platform Services Controller 節點或內嵌式安裝中：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- 在 vCenter Server (外部安裝) 上：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

`new-vmca-ssl.crt` 檔案於當前目錄中建立。

- 4 (選用) 列出 VECS 的內容。

```
"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli store list
```

- Platform Services Controller 上的輸出：

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- vCenter Server 上的輸出：

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

- 5 將 VECS 中的機器 SSL 憑證取代為新的機器 SSL 憑證。--store 和 --alias 值必須與預設名稱完全相符。

- 在 Platform Services Controller 上，執行下列命令以更新 MACHINE_SSL_CERT 存放區中的機器 SSL 憑證。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- 在每個管理節點或內嵌式部署中，執行下列命令以更新 MACHINE_SSL_CERT 存放區中的機器 SSL 憑證。您必須為每台機器個別更新憑證，因為每台機器的 FQDN 都不相同。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

後續步驟

您也可以取代 ESXi 主機的憑證。請參閱《vSphere 安全性》出版物。

在多節點部署中取代根憑證之後，您必須在含外部 Platform Services Controller 節點的所有 vCenter Server 上重新啟動服務。

取代解決方案使用者憑證 (中繼 CA)

取代機器 SSL 憑證後，您可以取代解決方案使用者憑證。

您會在每個管理節點與每個 Platform Services Controller 節點上取代機器解決方案使用者憑證。您只會在每個管理節點上取代其他解決方案使用者憑證。在包含外部 Platform Services Controller 的管理節點上執行命令時，請使用 --server 參數指向 Platform Services Controller。

備註 當您列出大型部署中的解決方案使用者憑證時，dir-cli list 的輸出會包含所有節點上的所有解決方案使用者。執行 vmafd-cli get-machine-id --server-name localhost 以找出每台主機的本機機器識別碼。每個解決方案使用者名稱都包含機器識別碼。

必要條件

每個解決方案使用者憑證必須具有不同的 Subject。例如，您可以考慮加入解決方案使用者名稱 (例如 vpxd) 或其他唯一識別碼。

程序

- 1 製作一份 certtool.cfg 的複本，移除名稱、IP 位址、DNS 名稱和電子郵件欄位，然後重新命名該檔案 (例如重新命名為 sol_usr.cfg)。

做為產生過程的一部分，您可以從命令列重新命名憑證。解決方案使用者無需其他資訊。如果保留預設資訊，所產生的憑證可能會造成混淆。

- 2 為每個解決方案使用者產生公開/私密金鑰檔案配對和憑證，並於您先前自訂的組態檔中傳遞。

例如：

```
certtool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certtool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

- 3 找到每個解決方案使用者的名稱。

```
dir-cli service list
```

您可以使用取代憑證時返回的唯一識別碼。輸入和輸出內容可能如下。

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

當您列出多節點部署中的解決方案使用者憑證時，dir-cli list 的輸出會包含所有節點上的所有解決方案使用者。請執行 vmafd-cli get-machine-id --server-name localhost 以找出每台主機的本機機器識別碼。每個解決方案使用者名稱都包含機器識別碼。

- 4 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

Windows 和 vCenter Server Appliance 上的服務名稱並不相同。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdir
service-control --start vmcad
```

- 5 先後取代 vmdir 和 VECS 中的現有憑證。

對於解決方案使用者，您必須以此順序新增憑證。例如：

```
dir-cli service update --name <vpzd-xxxx-xxx-7c7b769cd9f4> --cert ./vpzd.crt
vecs-cli entry delete --store vpzd --alias vpzd
vecs-cli entry create --store vpzd --alias vpzd --cert vpzd.crt --key vpzd.priv
```

備註 如果您不取代 vmdir 中的憑證，解決方案使用者就無法登入 vCenter Single Sign-On。

- 6 重新啟動所有服務。

```
service-control --start --all
```

範例：取代解決方案使用者憑證 (中繼 CA)

- 1 為每個解決方案使用者產生公開/私密金鑰配對。其中包括一組為每個 Platform Services Controller 和每個管理節點上機器解決方案使用者提供的配對，以及一組為每個管理節點上每個其他解決方案使用者 (vpzd、vpzd-extension、vsphere-webclient) 提供的配對。
 - a 為內嵌式部署的機器解決方案使用者或 Platform Services Controller 的機器解決方案使用者產生金鑰配對。

```
C:\>"C:\Program Files\VMware\VCServer\vmcad\"certool --genkey --privkey=machine-
key.priv --pubkey=machine-key.pub
```

- b (選用) 針對包含外部 Platform Services Controller 的部署，為每個管理節點上的機器解決方案使用者產生金鑰配對。

```
C:\>"C:\Program Files\VMware\VCServer\vmcad\"certool --genkey --privkey=machine-
key.priv --pubkey=machine-key.pub
```


- c 為每個管理節點上的 vpxd 解決方案使用者產生金鑰配對。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub"
```

- d 為每個管理節點上的 vpxd-extension 解決方案使用者產生金鑰配對。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub"
```

- e 為每個管理節點上的 vsphere-webclient 解決方案使用者產生金鑰配對。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub"
```

- 2 為每個 Platform Services Controller 和每個管理節點上的機器解決方案使用者，以及每個管理節點上的每個其他解決方案使用者 (vpxd、vpxd-extension、vsphere-webclient)，產生由新 VMCA 根憑證簽署的解決方案使用者憑證。

備註 --Name 參數必須是唯一的。包含解決方案使用者存放區的名稱 (例如 vpxd 或 vpxd-extension)，可讓您輕鬆辨識憑證與解決方案使用者之間的對應關係。

- a 在 Platform Services Controller 節點上執行下列命令，為該節點上的機器解決方案使用者產生解決方案使用者憑證。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine"
```

- b 為每個管理節點上的機器解決方案使用者產生憑證。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>"
```

- c 為每個管理節點上的 vpxd 解決方案使用者產生憑證。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>"
```

- d 為每個管理節點上的 vpxd-extensions 解決方案使用者產生憑證。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>"
```

- e 執行下列命令，為每個管理節點上的 vsphere-webclient 解決方案使用者產生憑證。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>"
```

3 將 VECS 中的解決方案使用者憑證取代為新的解決方案使用者憑證。

備註 --store 和 --alias 參數必須與預設服務名稱完全相符。

- a 在 Platform Services Controller 節點上，執行下列命令以取代機器解決方案使用者憑證：

```
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry create --store
machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b 取代每個管理節點上的機器解決方案使用者憑證：

```
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry create --store
machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- c 取代每個管理節點上的 vpxd 解決方案使用者憑證：

```
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry delete --store vpxd
--alias vpxd
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry create --store vpxd
--alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

- d 取代每個管理節點上的 vpxd-extension 解決方案使用者憑證：

```
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry delete --store vpxd-
extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry create --store vpxd-
extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-
key.priv
```

- e 取代每個管理節點上的 vsphere-webclient 解決方案使用者憑證。

```
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry delete --store
vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\VCServer\vmaddd\vecs-cli entry create --store
vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key
vsphere-webclient-key.priv
```

4 使用新的解決方案使用者憑證更新 VMware 目錄服務 (vmmdir)。系統會提示您輸入 vCenter Single Sign-On 管理員密碼。

- a 執行 `dir-cli service list`，為每個解決方案使用者取得唯一的服務識別碼尾碼。您可以在 Platform Services Controller 或 vCenter Server 系統上執行此命令。

```
C:\>"C:\Program Files\VMware\VCServer\vmaddd\dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
```

```

2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69

```

備註 當您列出大型部署中的解決方案使用者憑證時，`dir-cli list` 的輸出會包含所有節點上的所有解決方案使用者。執行 `vmafd-cli get-machine-id --server-name localhost` 以找出每台主機的本機機器識別碼。每個解決方案使用者名稱都包含機器識別碼。

- b 取代 Platform Services Controller 上 `vmdir` 中的機器憑證。例如，如果 `machine-29a45d00-60a7-11e4-96ff-00505689639a` 是 Platform Services Controller 上的機器解決方案使用者，請執行此命令：

```

C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt

```

- c 取代每個管理節點上 `vmdir` 中的機器憑證。例如，如果 `machine-6fd7f140-60a9-11e4-9e28-005056895a69` 是 vCenter Server 上的機器解決方案使用者，請執行此命令：

```

C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt

```

- d 取代每個管理節點上 `vmdir` 中的 `vpxd` 解決方案使用者憑證。例如，如果 `vpxd-6fd7f140-60a9-11e4-9e28-005056895a69` 是 `vpxd` 解決方案使用者識別碼，請執行此命令：

```

C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt

```

- e 取代每個管理節點上 `vmdir` 中的 `vpxd-extension` 解決方案使用者憑證。例如，如果 `vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69` 是 `vpxd-extension` 解決方案使用者識別碼，請執行此命令：

```

C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\"dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt

```

- f 取代每個管理節點上的 `vsphere-webclient` 解決方案使用者憑證。例如，如果 `vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69` 是 `vsphere-webclient` 解決方案使用者識別碼，請執行此命令：

```

C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\"dir-cli service update --name
vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt

```

取代 VMware 目錄服務憑證

如果您決定使用新的 VMCA 根憑證，並解除發佈當初佈建環境時使用的 VMCA 根憑證，則您必須取代機器 SSL 憑證、解決方案使用者憑證，以及部分內部服務的憑證。

如果您解除發佈 VMCA 根憑證，必須取代由 vCenter Single Sign-On 所使用的 SSL 簽署憑證。請參閱 [重新整理安全性 Token 服務憑證](#)。您也必須取代 VMware 目錄服務 (vmdir) 憑證。

必要條件

向第三方或企業 CA 為 vmdir 要求憑證。

程序

- 1 停止 vmdir。

Linux

```
service-control --stop vmdird
```

Windows

```
service-control --stop VMWareDirectoryService
```

- 2 將剛剛產生的憑證和金鑰複製到 vmdir 位置。

Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

- 3 從 vSphere Web Client 或使用 service-control 命令重新啟動 vmdir。

Linux

```
service-control --start vmdird
```

Windows

```
service-control --start VMWareDirectoryService
```

在混合模式環境中取代 VMware Directory Service 憑證

在升級期間，您的環境可能會暫時同時包含 vCenter Single Sign-On 5.5 版本和 vCenter Single Sign-On 6.x 版本。這種情況下，如果您取代 vCenter Single Sign-On 服務執行所在節點的 SSL 憑證，必須執行額外步驟以取代 VMware Directory Service SSL 憑證。

vmdir 會使用 VMware Directory Service SSL 憑證，在執行 vCenter Single Sign-On 複寫的 Platform Services Controller 節點之間進行信號交換。

包含 vSphere 6.0 和 vSphere 6.5 節點的混合模式環境無需這些步驟。只有在下列情況中才需要進行這些步驟：

- 您的環境同時包含 vCenter Single Sign-On 5.5 和 vCenter Single Sign-On 6.x 服務。
- vCenter Single Sign-On 服務已設定為複寫 vmdir 資料。
- 您計劃在執行 vCenter Single Sign-On 6.x 服務的節點上將預設的 VMCA 簽署憑證取代為自訂憑證。

備註 最佳做法為，在重新啟動服務前升級整個環境。一般不建議取代 VMware Directory Service 憑證。

程序

- 1 在執行 vCenter Single Sign-On 6.x 服務的節點上，取代 vmdir SSL 憑證和金鑰。
請參閱[取代 VMware 目錄服務憑證](#)。
- 2 在執行 vCenter Single Sign-On 5.5 服務的節點上進行環境設定，使 vCenter Single Sign-On 6.x 服務成為已知服務。
 - a 備份 C:\ProgramData\VMware\CIS\cfg\vmdir 中的所有檔案。
 - b 在 6.x 節點上建立 vmdircert.pem 檔案的複本，並將其重新命名為 <sso_node2.domain.com>.pem，其中 <sso_node2.domain.com> 是 6.x 節點的 FQDN。
 - c 將重新命名後的憑證複製到 C:\ProgramData\VMware\CIS\cfg\vmdir，以取代現有的複寫憑證。
- 3 在所有已取代憑證的機器上重新啟動 VMware Directory Service。
您可以從 vSphere Web Client 或使用 service-control 命令重新啟動服務。

將第三方憑證與 vSphere 搭配使用

如果公司原則需要，您可以將 vSphere 中使用的所有憑證取代為第三方 CA 簽署憑證。如果您執行這項作業，VMCA 不在您的憑證鏈結中，但所有 vCenter 憑證都必須儲存於 VECS 中。

您可以取代所有憑證，或使用混合解決方案。例如，考量取代所有用於網路流量的憑證，但保留 VMCA 簽署解決方案使用者憑證。解決方案使用者憑證僅用於就地向 vCenter Single Sign-On 進行驗證。

備註 如果您不希望使用 VMCA，就需要自行負責取代所有憑證、使用憑證佈建新的元件，以及追蹤憑證到期。

程序

- 1 [要求憑證及匯入自訂根憑證](#)
如果公司原則不允許使用中繼 CA，則 VMCA 無法為您產生憑證。您可以使用來自企業或第三方 CA 的自訂憑證。
- 2 [將機器 SSL 憑證取代為自訂憑證](#)
收到自訂憑證後，您可以取代每個機器憑證。

3 將解決方案使用者憑證取代為自訂憑證

取代機器 SSL 憑證後，您可以將 VMCA 簽署的解決方案使用者憑證取代為第三方或企業憑證。

4 取代 VMware 目錄服務憑證

如果您決定使用新的 VMCA 根憑證，並解除發佈當初佈建環境時使用的 VMCA 根憑證，則您必須取代機器 SSL 憑證、解決方案使用者憑證，以及部分內部服務的憑證。

5 在混合模式環境中取代 VMware Directory Service 憑證

在升級期間，您的環境可能會暫時同時包含 vCenter Single Sign-On 5.5 版本和 vCenter Single Sign-On 6.x 版本。這種情況下，如果您取代 vCenter Single Sign-On 服務執行所在節點的 SSL 憑證，必須執行額外步驟以取代 VMware Directory Service SSL 憑證。

要求憑證及匯入自訂根憑證

如果公司原則不允許使用中繼 CA，則 VMCA 無法為您產生憑證。您可以使用來自企業或第三方 CA 的自訂憑證。

必要條件

憑證必須符合以下需求：

- 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)。

程序

1 將下列憑證的 CSR 傳送給您的企業或第三方憑證提供者。

- 每台機器有一個機器 SSL 憑證。對於機器 SSL 憑證，SubjectAltName 欄位必須包含完整網域名稱 (DNS NAME=*machine_FQDN*)。
- 或是，每個內嵌式系統或管理節點有四個解決方案使用者憑證。解決方案使用者憑證不應包含 IP 位址、主機名稱或電子郵件地址。每個憑證必須具有不同的憑證主體。

一般來說，會為信任鏈結產生 PEM 檔案，並為每個 Platform Services Controller 或管理節點產生已簽署的 SSL 憑證。

2 列出 TRUSTED_ROOTS 和機器 SSL 存放區。

```
vecs-cli store list
```

- a 確認目前的根憑證和所有機器 SSL 憑證都經 VMCA 簽署。
- b 記下序號、簽發者以及主體 CN 欄位。
- c (選擇性) 使用網頁瀏覽器開啟將進行憑證取代之節點的 HTTPS 連線，檢查憑證資訊並確認其與機器 SSL 憑證相符。

3 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

Windows 和 vCenter Server Appliance 上的服務名稱並不相同。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

4 發佈自訂根憑證 (來自第三方 CA 的簽署憑證)。

```
dir-cli trustedcert publish --cert <my_custom_root>
```

如果您未在命令列上指定使用者名稱和密碼，系統會提示您指定。

5 重新啟動所有服務。

```
service-control --start --all
```

後續步驟

如果公司原則需要，您可以從憑證存放區移除原始的 VMCA 根憑證。如果進行移除，您必須重新整理這些內部憑證：

- 取代 vCenter Single Sign-On 簽署憑證。請參閱 [重新整理安全性 Token 服務憑證](#)。
- 取代 VMware 目錄服務憑證。請參閱 [取代 VMware 目錄服務憑證](#)。

將機器 SSL 憑證取代為自訂憑證

收到自訂憑證後，您可以取代每個機器憑證。

每台機器必須具有機器 SSL 憑證，以便與其他服務進行安全通訊。在多節點部署中，您必須在每個節點上執行機器 SSL 憑證產生命令。使用 `--server` 參數從含外部 Platform Services Controller 的 vCenter Server 指向 Platform Services Controller。

在開始取代憑證之前，您必須準備好下列資訊：

- administrator@vsphere.local 的密碼。
- 有效的機器 SSL 自訂憑證 (.crt 檔案)。
- 有效的機器 SSL 自訂金鑰 (.key 檔案)。
- 有效的自訂根憑證 (.crt 檔案)。
- 如果您在多節點部署中於含外部 Platform Services Controller 的 vCenter Server 上執行命令，需要 Platform Services Controller 的 IP 位址。

必要條件

您一定已收到第三方或企業憑證授權機構核發給每台機器的憑證。

- 金鑰大小：2048 位元或以上 (PEM 編碼)
- CRT 格式
- x509 第 3 版
- SubjectAltName 必須包含 DNS Name=<machine_FQDN>
- 包含下列金鑰使用方法：數位簽章、不可否認性、金鑰編密

程序

- 1 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

Windows 和 vCenter Server Appliance 上的服務名稱並不相同。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```


2 登入每個節點，並將從 CA 收到的新機器憑證新增到 VECS 中。

所有機器都需要使用本機憑證存放區中的新憑證，以透過 SSL 進行通訊。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-path>
--key <key-file-path>
```

3 重新啟動所有服務。

```
service-control --start --all
```

範例：將機器 SSL 憑證取代為自訂憑證

您可以在每個節點上以相同方式取代機器 SSL 憑證。

1 首先，刪除 VECS 中的現有憑證。

```
"C:\Program Files\VMware\VMware Server\vmaddd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
```

2 接著，新增替代憑證。

```
"C:\Program Files\VMware\VMware Server\vmaddd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-wl-
vim-cat-dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-
cat-dhcp-1128.vmware.com.priv
```

後續步驟

您也可以取代 ESXi 主機的憑證。請參閱《vSphere 安全性》出版物。

在多節點部署中取代根憑證之後，您必須在含外部 Platform Services Controller 節點的所有 vCenter Server 上重新啟動服務。

將解決方案使用者憑證取代為自訂憑證

取代機器 SSL 憑證後，您可以將 VMCA 簽署的解決方案使用者憑證取代為第三方或企業憑證。

解決方案使用者僅會使用憑證向 vCenter Single Sign-On 進行驗證。如果憑證有效，vCenter Single Sign-On 會為解決方案使用者指派 SAML Token，解決方案使用者使用 SAML Token 向其他 vCenter 元件進行驗證。

考量您的環境中是否需要進行解決方案使用者憑證取代。由於解決方案使用者位於 Proxy 伺服器的後方，且使用機器 SSL 憑證保護 SSL 流量安全，因此解決方案使用者憑證可能比較沒有安全之憂。

您會在每個管理節點與每個 Platform Services Controller 節點上取代機器解決方案使用者憑證。您只會在每個管理節點上取代其他解決方案使用者憑證。在包含外部 Platform Services Controller 的管理節點上執行命令時，請使用 `--server` 參數指向 Platform Services Controller。

備註 當您列出大型部署中的解決方案使用者憑證時，`dir-cli list` 的輸出會包含所有節點上的所有解決方案使用者。執行 `vmafd-cli get-machine-id --server-name localhost` 以找出每台主機的本機機器識別碼。每個解決方案使用者名稱都包含機器識別碼。

必要條件

- 金鑰大小：2048 位元或以上 (PEM 編碼)
- CRT 格式
- x509 第 3 版
- SubjectAltName 必須包含 DNS Name=<machine_FQDN>
- 每個解決方案使用者憑證必須具有不同的 Subject。例如，您可以考慮加入解決方案使用者名稱 (例如 vpxd) 或其他唯一識別碼。
- 包含下列金鑰使用方法：數位簽章、不可否認性、金鑰編密

程序

- 1 停止所有服務，並啟動用於處理憑證建立、傳播和儲存的服務。

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmca
```

- 2 找到每個解決方案使用者的名稱。

```
dir-cli service list
```

您可以使用取代憑證時返回的唯一識別碼。輸入和輸出內容可能如下。

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

當您列出多節點部署中的解決方案使用者憑證時，`dir-cli list` 的輸出會包含所有節點上的所有解決方案使用者。請執行 `vmafd-cli get-machine-id --server-name localhost` 以找出每台主機的本機機器識別碼。每個解決方案使用者名稱都包含機器識別碼。

3 針對每個解決方案使用者，先後取代 VECS 和 vmdir 中的現有憑證。

您必須以此順序新增憑證。

```
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
dir-cli service update --name <vpxd-xxxx-xxx-xxxxxx> --cert vpxd.crt
```

備註 如果您不取代 vmdir 中的憑證，解決方案使用者就無法向 vCenter Single Sign-On 進行驗證。

4 重新啟動所有服務。

```
service-control --start --all
```

取代 VMware 目錄服務憑證

如果您決定使用新的 VMCA 根憑證，並解除發佈當初佈建環境時使用的 VMCA 根憑證，則您必須取代機器 SSL 憑證、解決方案使用者憑證，以及部分內部服務的憑證。

如果您解除發佈 VMCA 根憑證，必須取代由 vCenter Single Sign-On 所使用的 SSL 簽署憑證。請參閱 [重新整理安全性 Token 服務憑證](#)。您也必須取代 VMware 目錄服務 (vmdir) 憑證。

必要條件

向第三方或企業 CA 為 vmdir 要求憑證。

程序

1 停止 vmdir。

Linux

```
service-control --stop vmkdir
```

Windows

```
service-control --stop VMWardirectoryService
```

2 將剛剛產生的憑證和金鑰複製到 vmdir 位置。

Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmkdir\vmldircert.pem
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmkdir\vmldirkey.pem
```

- 3 從 vSphere Web Client 或使用 `service-control` 命令重新啟動 `vmmdir`。

Linux

```
service-control --start vmmdir
```

Windows

```
service-control --start VMWareDirectoryService
```

在混合模式環境中取代 VMware Directory Service 憑證

在升級期間，您的環境可能會暫時同時包含 vCenter Single Sign-On 5.5 版本和 vCenter Single Sign-On 6.x 版本。這種情況下，如果您取代 vCenter Single Sign-On 服務執行所在節點的 SSL 憑證，必須執行額外步驟以取代 VMware Directory Service SSL 憑證。

`vmmdir` 會使用 VMware Directory Service SSL 憑證，在執行 vCenter Single Sign-On 複寫的 Platform Services Controller 節點之間進行信號交換。

包含 vSphere 6.0 和 vSphere 6.5 節點的混合模式環境無需這些步驟。只有在下列情況中才需要進行這些步驟：

- 您的環境同時包含 vCenter Single Sign-On 5.5 和 vCenter Single Sign-On 6.x 服務。
- vCenter Single Sign-On 服務已設定為複寫 `vmmdir` 資料。
- 您計劃在執行 vCenter Single Sign-On 6.x 服務的節點上將預設的 VMCA 簽署憑證取代為自訂憑證。

備註 最佳做法為，在重新啟動服務前升級整個環境。一般不建議取代 VMware Directory Service 憑證。

程序

- 1 在執行 vCenter Single Sign-On 6.x 服務的節點上，取代 `vmmdir` SSL 憑證和金鑰。
請參閱[取代 VMware 目錄服務憑證](#)。
- 2 在執行 vCenter Single Sign-On 5.5 服務的節點上進行環境設定，使 vCenter Single Sign-On 6.x 服務成為已知服務。
 - a 備份 `C:\ProgramData\VMware\CIS\cfg\vmmdir` 中的所有檔案。
 - b 在 6.x 節點上建立 `vmdircert.pem` 檔案的複本，並將其重新命名為 `<sso_node2.domain.com>.pem`，其中 `<sso_node2.domain.com>` 是 6.x 節點的 FQDN。
 - c 將重新命名後的憑證複製到 `C:\ProgramData\VMware\CIS\cfg\vmmdir`，以取代現有的複寫憑證。
- 3 在所有已取代憑證的機器上重新啟動 VMware Directory Service。
您可以從 vSphere Web Client 或使用 `service-control` 命令重新啟動服務。

使用 CLI 命令管理憑證和服務

有一組 CLI 可讓您管理 VMCA (VMware Certificate Authority)、VECS (VMware Endpoint 憑證存放區) 以及 VMware Directory Service (vmdir)。vSphere Certificate Manager 公用程式也支援多項相關工作，但手動憑證管理需要使用 CLI。

表 3-5. 用於管理憑證和相關聯服務的 CLI 工具

CLI	說明	請參閱
certool	產生與管理憑證及金鑰。屬於 VMCA 的一部分。	certool 初始化命令參考
vecs-cli	管理 VMware 憑證存放區執行個體的內容。屬於 VMAFD 的一部分。	vecs-cli 命令參考
dir-cli	建立與更新 VMware Directory Service 中的憑證。屬於 VMAFD 的一部分。	dir-cli 命令參考
service-control	啟動或停止服務，例如做為憑證取代工作流程的一部分	

憑證管理工具位置

依預設，您可以在每個節點上的下列位置找到工具。

Windows

```
C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe
C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe
C:\Program Files\VMware\vCenter Server\vmcad\certool.exe
VCENTER_INSTALL_PATH\bin\service-control
```

Linux

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
```

在 Linux 上，service-control 命令不需要您指定路徑。

如果您從具有外部 Platform Services Controller 的管理節點執行命令，可以使用 `--server` 參數指定 Platform Services Controller。

進行憑證管理作業所需的權限

您必須身為 vsphere.local 網域中 CAAdmins 群組的成員，才能進行大多數的 vCenter 憑證管理作業。administrator@vsphere.local 使用者是 CAAdmins 群組的成員。部分作業是所有使用者都可以進行的。

如果您執行 vCenter Certificate Manager 公用程式，系統會提示您輸入 administrator@vsphere.local 的密碼。如果您以手動方式取代憑證，不同憑證管理 CLI 的不同選項會需要不同的權限。

dir-cli

您必須是 vsphere.local 網域中 CAAdmins 群組的成員。每次執行 dir-cli 命令時，系統會提示您輸入使用者名稱及密碼。

vecs-cli

一開始，只有存放區擁有者具有存放區的存取權。在 Windows 系統上，存放區擁有者是管理員使用者，在 Linux 系統上則是根使用者。存放區擁有者可以將存取權提供給其他使用者。

MACHINE_SSL_CERT 和 TRUSTED_ROOTS 存放區是特殊存放區。只有根使用者或管理員使用者 (視安裝類型而定) 具有完整的存取權。

certool

大部分的 certool 命令都只有 CAAdmins 群組中的使用者才能使用。administrator@vsphere.local 使用者是 CAAdmins 群組的成員。所有使用者都可以執行的命令如下：

- genselfcacert
- initscr
- getdc
- waitVMDIR
- waitVMCA
- genkey
- viewcert

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。

變更 certool 組態

執行 certool --gencert 及某些其他憑證初始化或管理命令時，CLI 會從組態檔讀取所有值。您可以編輯現有檔案、使用 --config=<file name> 選項覆寫預設組態檔 (certool.cfg)，或覆寫命令列上的不同值。

組態檔中有數個欄位，預設值如下：

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
```

```
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

您可以變更組態中的值，方式如下：

- 為組態檔建立備份，然後編輯檔案。如果您使用的是預設組態檔，則不需要加以指定。否則，舉例來說，如果您變更了組態檔名稱，請使用 `--config` 命令列選項。
- 使用命令列覆寫組態檔值。例如，如果要覆寫位置，請執行此命令：

```
certool --gencert --privkey=private.key --Locality="Mountain View"
```

指定 `--Name` 以取代憑證主體名稱的 CN 欄位。

- 對於解決方案使用者憑證，慣例上名稱會是 `<sol_user name>@<domain>`，但如果您環境中採用的慣例有所不同，可以變更名稱。
- 對於機器 SSL 憑證，會使用機器的 FQDN，因為 SSL 用戶端會在確認機器的主機名稱時，檢查憑證主體名稱的 CN 欄位。由於機器可以使用多個別名，憑證擴充了 [主體別名] 欄位，您可以在此指定其他名稱 (DNS 名稱、IP 位址等)。然而，VMCA 僅允許使用一個 `DNSName` (在 `Hostname` 欄位中) 且不得使用其他別名。如果 IP 位址是由使用者指定，也會儲存在 `SubAltName` 中。

`--Hostname` 參數用於指定憑證 `SubAltName` 的 `DNSName`。

certool 初始化命令參考

`certool` 初始化命令可讓您產生憑證簽署要求、檢視和產生由 VMCA 簽署的憑證和金鑰、匯入根憑證以及執行其他憑證管理作業。

在許多情況下，您將組態檔傳遞到 `certool` 命令。請參閱 [變更 certool 組態](#)。如需使用量範例，請參閱 [新的 VMCA 簽署憑證取代現有的 VMCA 簽署憑證](#)。

certool --initcsr

產生憑證簽署要求 (CSR)。該命令產生 PKCS10 檔案和私密金鑰。

選項	描述
<code>--initcsr</code>	產生 CSR 時需要。
<code>--privkey <key_file></code>	私密金鑰檔案的名稱。
<code>--pubkey <key_file></code>	公開金鑰檔案的名稱。
<code>--csrfile <csr_file></code>	要傳送到 CA 提供者的 CSR 檔案的檔案名稱。
<code>--config <config_file></code>	組態檔的選用名稱。預設值為 <code>certool.cfg</code> 。

例如：

```
certool --initcsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

certool --selfca

建立自我簽署的憑證並使用自我簽署的根 CA 佈建 VMCA 伺服器。使用此選項為佈建 VMCA 伺服器最簡單的方式之一。您可以改為使用第三方根憑證佈建 VMCA 伺服器，以讓 VMCA 成為中繼 CA。請參閱 [使用 VMCA 做為中繼憑證授權機構](#)。

此命令會提早 3 天產生憑證，以避免時區衝突。

選項	描述
--selfca	產生自我簽署的憑證時需要。
--predate <number_of_minutes>	可讓您將根憑證的 [有效起始時間] 欄位設定為目前時間之前的指定分鐘數。此選項可協助對潛在時區問題進行說明。上限為 3 天。
--config <config_file>	組態檔的選用名稱。預設值為 certool.cfg。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

例如：

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280 --selfca --server=
192.0.2.24 --srp-upn=administrator@vsphere.local
```

certool --rootca

匯入根憑證。將指定憑證和私密金鑰新增到 VMCA。VMCA 一律使用最新根憑證進行簽署，但是其他根憑證仍可用。這意味著，您可以一次執行一個步驟來更新基礎結構，最後才刪除不再使用的憑證。

選項	描述
--rootca	匯入根 CA 時需要。
--cert <certfile>	組態檔的選用名稱。預設值為 certool.cfg。
--privkey <key_file>	私密金鑰檔案的名稱。此檔案必須為 PEM 編碼格式。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

例如：

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

certool --getdc

傳回由 vmdir 使用的預設網域名稱。

選項	描述
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。
--port <port_num>	選用的連接埠號碼。預設值為連接埠 389。

例如：

```
certool --getdc
```

certool --waitVMDIR

請等待，直到 VMware 目錄服務正在執行或 `--wait` 指定的逾時結束為止。搭配使用此選項和其他選項可排程某些工作，例如傳回預設網域名稱。

選項	描述
<code>--wait</code>	要等待的選用分鐘數。預設值為 3。
<code>--server <server></code>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。
<code>--port <port_num></code>	選用的連接埠號碼。預設值為連接埠 389。

例如：

```
certool --waitVMDIR --wait 5
```

certool --waitVMCA

請等待，直到 VMCA 服務正在執行或指定的逾時結束為止。搭配使用此選項和其他選項可排程某些工作，例如產生憑證。

選項	描述
<code>--wait</code>	要等待的選用分鐘數。預設值為 3。
<code>--server <server></code>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。
<code>--port <port_num></code>	選用的連接埠號碼。預設值為連接埠 389。

例如：

```
certool --waitVMCA --selfca
```

certool --publish-roots

強制更新根憑證。此命令需要管理權限。

選項	描述
<code>--server <server></code>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

例如：

```
certool --publish-roots
```

certool 管理命令參考

certool 管理命令可讓您檢視、產生與撤銷憑證，以及檢視有關憑證的資訊。

certool --genkey

產生私密和公開金鑰配對。然後，可使用這些檔案產生 VMCA 簽署的憑證。您可以使用該憑證佈建機器或解決方案使用者。

選項	描述
--genkey	產生私密和公開金鑰時所需的選項。
--privkey <keyfile>	私密金鑰檔案的名稱。
--pubkey <keyfile>	公開金鑰檔案的名稱。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

例如：

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

certool --gencert

從 VMCA 伺服器產生憑證。此命令會使用 certool.cfg 或指定組態檔中的資訊。

選項	描述
--gencert	產生憑證時所需的選項。
--cert <certfile>	憑證檔案的名稱。此檔案必須為 PEM 編碼格式。
--privkey <keyfile>	私密金鑰檔案的名稱。此檔案必須為 PEM 編碼格式。
--config <config_file>	組態檔的選用名稱。預設值為 certool.cfg。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

例如：

```
certool --gencert --privkey=<filename> --cert=<filename>
```

certool --getrootca

以人類可讀的形式列印目前的根 CA 憑證。如果您正在從管理節點執行此命令，請使用 Platform Services Controller 節點的機器名稱來擷取根 CA。此輸出不可做為憑證使用，而會變更為人類可讀的內容。

選項	描述
--getrootca	列印根憑證時所需的選項。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

例如：

```
certool --getrootca --server=remoteserver
```

certool --viewcert

以人類可讀的形式列印憑證中的所有欄位。

選項	描述
--viewcert	檢視憑證時所需的選項。
--cert <certfile>	組態檔的選用名稱。預設值為 certool.cfg。

例如：

```
certool --viewcert --cert=<filename>
```

certool --enumcert

列出 VMCA 伺服器知曉的所有憑證。必要的篩選器選項可讓您列出所有憑證或僅列出撤銷的、作用中或到期的憑證。

選項	描述
--enumcert	列出所有憑證時所需的選項。
--filter [all active]	必要篩選器。指定所有或作用中的選項。目前不支援已撤銷和到期的選項。

例如：

```
certool --enumcert --filter=active
```

certool --status

將指定憑證傳送給 VMCA 伺服器，以檢查哪些憑證已撤銷。如果憑證已撤銷，則列印 [憑證: 已撤銷]，否則，列印 [憑證: 作用中]。

選項	描述
--status	檢查憑證狀態時所需的選項。
--cert <certfile>	組態檔的選用名稱。預設值為 certool.cfg。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

例如：

```
certool --status --cert=<filename>
```

certool --genselfcacert

根據組態檔中的值，產生自我簽署的憑證。此命令會提早 3 天產生憑證，以避免時區衝突。

選項	描述
--genselfcacert	產生自我簽署的憑證時需要。
--outcert <cert_file>	憑證檔案的名稱。此檔案必須為 PEM 編碼格式。
--outprivkey <key_file>	私密金鑰檔案的名稱。此檔案必須為 PEM 編碼格式。
--config <config_file>	組態檔的選用名稱。預設值為 certool.cfg。

例如：

```
certool --genselfcacert --privkey=<filename> --cert=<filename>
```

vecs-cli 命令參考

vecs-cli 命令集可讓您管理 VMware 憑證存放區 (VECS) 執行個體。將這些命令與 dir-cli 和 certool 搭配使用，以管理您的憑證基礎結構。

vecs-cli store create

建立憑證存放區。

選項	描述
--name <name>	憑證存放區的名稱。

例如：

```
vecs-cli store create --name <store>
```

vecs-cli store delete

刪除憑證存放區。您無法刪除系統預先定義的憑證存放區。

選項	描述
--name <name>	要刪除的憑證存放區的名稱。

例如：

```
vecs-cli store delete --name <store>
```

vecs-cli store list

列出憑證存放區。

VECS 包含下列存放區。

表 3-6. VECS 中的存放區

存放區	描述
機器的 SSL 存放區 (MACHINE_SSL_CERT)	<ul style="list-style-type: none"> ■ 由每個 vSphere 節點上反向 Proxy 服務所使用。 ■ 供內嵌式部署和每個 Platform Services Controller 節點上的 VMware 目錄服務 (vmdir) 使用。 <p>vSphere 6.0 中的所有服務都會透過使用機器 SSL 憑證的反向 Proxy 進行通訊。為確保回溯相容性，5.x 服務仍會使用特定的連接埠。因此，部分服務 (例如 vpxd) 仍會將自己的連接埠維持開啟。</p>
受信任的根存放區 (TRUSTED_ROOTS)	包含所有受信任的根憑證。
解決方案使用者存放區 <ul style="list-style-type: none"> ■ machine ■ vpxd ■ vpxd-extensions ■ vsphere-webclient 	<p>對於每個解決方案使用者，VECS 包含一個存放區。每個解決方案使用者憑證的主旨必須是唯一的，例如，機器憑證不能與 vpxd 憑證的主旨相同。</p> <p>解決方案使用者憑證用於透過 vCenter Single Sign-On 進行驗證。vCenter Single Sign-On 會檢查憑證是否有效，但不會檢查其他憑證屬性。在內嵌式部署中，所有解決方案使用者憑證均位於同一系統中。</p> <p>每個管理節點和每個內嵌式部署上的 VECS 中包含下列解決方案使用者憑證存放區：</p> <ul style="list-style-type: none"> ■ 機器：由 Component Manager、授權伺服器及記錄服務所使用。 <p>備註 機器解決方案使用者憑證與機器的 SSL 憑證毫無關聯。機器解決方案使用者憑證用於進行 SAML Token 交換；機器的 SSL 憑證用於對機器進行安全 SSL 連線。</p> <ul style="list-style-type: none"> ■ vpxd：vCenter 服務精靈 (vpxd) 存放區位於管理節點和內嵌式部署中。vpxd 會使用此存放區中儲存的解決方案使用者憑證向 vCenter Single Sign-On 進行驗證。 ■ vpxd-extensions：vCenter 延伸存放區。包含 Auto Deploy 服務、Inventory Service 及不屬於其他解決方案使用者的其他服務。 ■ vsphere-webclient：vSphere Web Client 存放區。還包括一些其他服務，例如效能圖服務。 <p>每個 Platform Services Controller 節點中也包含機器存放區。</p>
vSphere Certificate Manager 公用程式備份存放區 (BACKUP_STORE)	由 VMCA (VMware Certificate Manager) 用於支援憑證還原。只有最新狀態會儲存為備份，您無法還原一個以上的步驟。
其他存放區	<p>其他存放區可能由解決方案新增。例如，虛擬磁碟區解決方案將新增一個 SMS 存放區。除非 VMware 說明文件或 VMware 知識庫文章指示您修改這些存放區中的憑證，否則請勿這麼做。</p> <p>備註 vSphere 6.0 不支援 CRLS，然而，刪除 TRUSTED_ROOTS_CRLS 存放區可能會破壞憑證基礎結構。請勿刪除或修改 TRUSTED_ROOTS_CRLS 存放區。</p>

例如：

```
vecs-cli store list
```

vecs-cli store permissions

授與或撤銷儲存權限。使用 `--grant` 或 `--revoke` 選項。

存放區的擁有者擁有其存放區的所有控制權，包括授與和撤銷權限。管理員擁有所有存放區上的所有權限，包括授與和撤銷權限。

您可以使用 `vecs-cli get-permissions --name <store-name>` 擷取存放區的目前設定。

選項	描述
<code>--name <name></code>	憑證存放區的名稱。
<code>--user <username></code>	為其授與權限的使用者的唯一名稱。
<code>--grant [read write]</code>	授與讀取或寫入權限。
<code>--revoke [read write]</code>	撤銷讀取或寫入權限。目前不支援。

vecs-cli entry create

在 VECS 中建立一個項目。使用此命令新增私密金鑰或憑證到存放區。

選項	描述
<code>--store <NameOfStore></code>	憑證存放區的名稱。
<code>--alias <Alias></code>	憑證的選用別名。受信任的根存放區將忽略此選項。
<code>--cert <certificate_file_path></code>	憑證檔案的完整路徑。
<code>--key <key-file-path></code>	對應於憑證之金鑰的完整路徑。 選擇性。

vecs-cli entry list

列出指定存放區中的所有項目。

選項	描述
<code>--store <NameOfStore></code>	憑證存放區的名稱。
<code>--text</code>	顯示人類看得懂的憑證版本。

vecs-cli entry getcert

從 VECS 擷取憑證。您可以將憑證傳送到輸出檔案，或將其顯示為人類看得懂的文字。

選項	描述
<code>--store <NameOfStore></code>	憑證存放區的名稱。
<code>--alias <Alias></code>	憑證的別名。

選項	描述
<code>--output <output_file_path></code>	要將憑證寫入的檔案。
<code>--text</code>	顯示人類看得懂的憑證版本。

vecs-cli entry getkey

擷取儲存在 VECS 中的金鑰。您可以將憑證傳送到輸出檔案，或將其顯示為人類看得懂的文字。

選項	描述
<code>--store <NameOfStore></code>	憑證存放區的名稱。
<code>--alias <Alias></code>	金鑰的別名。
<code>--output <output_file_path></code>	要將金鑰寫入的輸出檔案。
<code>--text</code>	顯示人類看得懂的金鑰版本。

vecs-cli entry delete

刪除憑證存放區中的項目。如果您刪除 VECS 中的項目，則會將其從 VECS 永久移除。唯一的例外是目前的根憑證。VECS 會輪詢 vmdir 是否有根憑證。

選項	描述
<code>--store <NameOfStore></code>	憑證存放區的名稱。
<code>--alias <Alias></code>	您想要刪除之項目的別名。

vecs-cli force-refresh

強制重新整理 vecs-cli。發生此情況時，vecs-cli 會更新為使用 vmdir 中的最新資訊。依預設，VECS 會每隔 5 分隔輪詢 vmdir 是否有新根憑證檔案。使用此命令可從 vmdir 立即更新 VECS。

dir-cli 命令參考

dir-cli 公用程式可讓您在 vmdir 中建立和更新解決方案使用者、建立其他使用者帳戶以及管理憑證和密碼。將此公用程式與 vecs-cli 和 certool 搭配使用，以管理您的憑證基礎結構。

dir-cli service create

建立解決方案使用者。主要供第三方解決方案使用。

選項	描述
<code>--name <name></code>	要建立的解決方案使用者的名稱。
<code>--cert <cert file></code>	憑證檔案的路徑。可以是 VMCA 簽署的憑證或第三方憑證。

選項	描述
<code>--login <admin_user_id></code>	依預設為 administrator@vsphere.local。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
<code>--password <admin_password></code>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli service list

列出 dir-cli 知道的解決方案使用者。

選項	描述
<code>--login <admin_user_id></code>	依預設為 administrator@vsphere.local。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
<code>--password <admin_password></code>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli service delete

刪除 vmdir 中的解決方案使用者。刪除解決方案使用者時，使用 vmdir 的這一執行個體的所有管理節點都無法使用所有相關聯的服務。

選項	描述
<code>--name</code>	要刪除的解決方案使用者的名稱。
<code>--login <admin_user_id></code>	依預設為 administrator@vsphere.local。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
<code>--password <admin_password></code>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli service update

更新指定解決方案使用者的憑證 (即服務集合)。執行此命令後，VECS 會在 5 分鐘後提取變更，您也可以使用 `vecs-cli force-refresh` 強制執行重新整理。

選項	描述
<code>--name <name></code>	要更新的解決方案使用者的名稱。
<code>--cert <cert_file></code>	要指派給服務的憑證的名稱。
<code>--login <admin_user_id></code>	依預設為 administrator@vsphere.local。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
<code>--password <admin_password></code>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli user create

在 vmdir 內建立一般使用者。此命令可用於透過使用者名稱和密碼向 vCenter Single Sign-On 進行驗證的個人使用者。僅在原型設計期間使用此命令。

選項	描述
--account <name>	要建立的 vCenter Single Sign-On 使用者的名稱。
--user-password <password>	使用者的初始密碼。
--first-name <name>	使用者的名字。
--last-name <name>	使用者的姓氏。
--login <admin_user_id>	依預設為 administrator@vsphere.local。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
--password <admin_password>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli user delete

刪除 vmdir 內的指定使用者。

選項	描述
--account <name>	要刪除的 vCenter Single Sign-On 使用者的名稱。
--login <admin_user_id>	依預設為 administrator@vsphere.local。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
--password <admin_password>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli group modify

將使用者或群組新增至現有的群組。

選項	描述
--name <name>	vmdir 中群組的名稱。
--add <user_or_group_name>	要新增的使用者或群組的名稱。
--login <admin_user_id>	依預設為 administrator@vsphere.local。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
--password <admin_password>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli group list

列出指定的 vmdir 群組。

選項	描述
<code>--name <name></code>	vmdir 中群組的選擇性名稱。此選項可讓您檢查某個群組是否存在。
<code>--login <admin_user_id></code>	依預設為 administrator@vsphere.local。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
<code>--password <admin_password></code>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli trustedcert publish

將信任的根憑證發佈到 vmdir。

選項	描述
<code>--cert <file></code>	憑證檔案的路徑。
<code>--login <admin_user_id></code>	依預設為 administrator@vsphere.local。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
<code>--password <admin_password></code>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli trustedcert unpublish

解除發佈目前 vmdir 中信任的根憑證。例如，如果您已將其他根憑證新增到 vmdir (目前為環境中所有其他憑證的根憑證)，請使用此命令。強化環境的過程中，會解除發佈目前不再使用的憑證。

選項	描述
<code>--cert-file <file></code>	要解除發佈的憑證檔案的路徑
<code>--crl <file></code>	與此憑證相關聯的 CRL 檔案的路徑。目前未使用。
<code>--login <admin_user_id></code>	依預設為 administrator@vsphere.local。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
<code>--password <admin_password></code>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli trustedcert list

列出所有信任的根憑證及其對應的識別碼。您需要憑證識別碼才能使用 `dir-cli trustedcert get` 擷取憑證。

選項	描述
<code>--login <admin_user_id></code>	依預設為 administrator@vsphere.local。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
<code>--password <admin_password></code>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli trustedcert get

從 vmdir 擷取信任的根憑證，然後將其寫入指定的檔案。

選項	描述
--id <cert_ID>	要擷取的憑證的識別碼。此識別碼顯示在 <code>dir-cli trustedcert list</code> 命令中。
--outcert <path>	憑證檔案的寫入路徑。
--outcrl <path>	CRL 檔案的寫入路徑。目前未使用。
--login <admin_user_id>	依預設為 <code>administrator@vsphere.local</code> 。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
--password <admin_password>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli password create

建立符合密碼需求的隨機密碼。此命令可供第三方解決方案使用者使用。

選項	描述
--login <admin_user_id>	依預設為 <code>administrator@vsphere.local</code> 。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
--password <admin_password>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli password reset

可讓管理員重設使用者的密碼。如果您是管理員使用者，但想重設密碼，請改用 `dir-cli password change`。

選項	描述
--account	為其指派新密碼的帳戶的名稱。
--new	指定使用者的新密碼。
--login <admin_user_id>	依預設為 <code>administrator@vsphere.local</code> 。該管理員能夠將其他使用者新增到 CAAdmins vCenter Single Sign-On 群組以授與他們管理員權限。
--password <admin_password>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli password change

可讓使用者變更其密碼。您必須是擁有帳戶的使用者，才能做出此變更。管理員可使用 `dir-cli password reset` 重設任何密碼。

選項	描述
--account	帳戶名稱。
--current	擁有帳戶之使用者的目前密碼。
--new	擁有帳戶之使用者的新密碼。

使用 vSphere Web Client 檢視 vCenter 憑證

您可以檢視 vCenter 憑證授權機構 (VMCA) 可識別的憑證，查看作用中憑證是否即將到期、檢查到期的憑證，以及查看根憑證的狀態。您可以使用憑證管理 CLI 執行所有憑證管理工作。

您可以檢視內嵌式部署或 Platform Services Controller 隨附之 VMCA 執行個體的相關聯憑證。憑證資訊會跨 VMware 目錄服務 (vmdir) 執行個體複寫。

嘗試檢視 vSphere Web Client 中的憑證時，系統會提示您輸入使用者名稱和密碼。請指定具有 VMware 憑證授權機構相關權限之使用者 (即 CAAdmins vCenter Single Sign-On 群組中的使用者) 的使用者名稱和密碼。

程序

- 1 以 administrator@vsphere.local 或 CAAdmins vCenter Single Sign-On 群組中另一位使用者的身分登入 vCenter Server。
- 2 選取**管理**，按一下**部署**，然後按一下**系統組態**。
- 3 按一下**節點**，然後選取要檢視或管理其憑證的節點。
- 4 按一下**管理索引標籤**，然後按一下**憑證授權單位**。
- 5 按一下要檢視憑證資訊的憑證類型。

選項	描述
作用中憑證	顯示作用中憑證，包括憑證的驗證資訊。綠色的「有效期至」圖示會在接近憑證到期日時發生變更。
已撤銷的憑證	顯示已撤銷憑證的清單。此版本不支援此功能。
到期的憑證	列出到期的憑證。
根憑證	顯示此 vCenter 憑證授權機構執行個體可用的根憑證。

- 6 選取憑證並按一下**顯示憑證詳細資料**按鈕，檢視憑證詳細資料。

詳細資料包括主體名稱、簽發者、有效性和演算法。

設定 vCenter 憑證到期警告臨界值

從 vSphere 6.0 開始，vCenter Server 會監控 VMware Endpoint 憑證存放區 (VECS) 中的所有憑證，並在距離憑證到期 30 天或更短時間時發出警示。您可以使用 `vpzd.cert.threshold` 進階選項來變更收到警告的時間。

程序

- 1 登入 vSphere Web Client。
- 2 選取 vCenter Server 物件，接著選取**管理**索引標籤和**設定**子索引標籤。
- 3 按一下**進階設定**，選取**編輯**，並篩選臨界值。
- 4 將 vpxd.cert.threshold 的設定變更為所需的值，然後按一下**確定**。

vSphere 權限和使用者管理工作

4

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，只有使用者 administrator@vsphere.local 被授權登入 vCenter Server 系統。接著，該使用者將以如下方式繼續進行：

- 1 將已定義其他使用者和群組的身分識別來源新增至 vCenter Single Sign-On。請參閱[新增 vCenter Single Sign-On 身分識別來源](#)。
- 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

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8vla7txu/uiConfId/49694343/)

本章節討論下列主題：

- [瞭解 vSphere 中的授權](#)
- [瞭解 vCenter Server 權限模型](#)
- [權限的階層式繼承](#)
- [多個權限設定](#)
- [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

在 vSphere 中授權給使用者或群組的主要方式為授予 vCenter Server 權限。視要執行的工作而定，您可能需要其他授權。

vSphere 6.0 及更新版本允許擁有權限的使用者授予其他使用者權限，讓其能以下列方式執行工作。這些方式大部分互斥，不過，您可以針對所有解決方案，為使用者指派可授權給特定使用者的全域權限。您也可以針對個別 vCenter Server 系統，為使用者指派可授權給其他使用者的本機 vCenter Server 權限。

vCenter Server 權限

vCenter Server 系統的權限模型依賴於將權限指派到該 vCenter Server 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 ESXi 主機並將角色指派給使用者群組，授予這些使用者在該主機上的對應權限。

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，如果安裝了 vCenter Server 和 vCenter Orchestrator，您可以使用全域權限將權限授予兩個物件階層中的所有物件。

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](#)。

vsphere.local 群組中的群組成員資格

使用者 administrator@vsphere.local 可以執行與 Platform Services Controller 隨附之服務相關聯的工作。此外，vsphere.local 群組的成員可以執行對應的工作。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 [vsphere.local 網域中的群組](#)。

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《使用 vSphere Client 進行 vSphere 管理》說明文件。

瞭解 vCenter Server 權限模型

vCenter Server 系統的權限模型依賴於將權限指派到 vSphere 物件階層中的物件。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。

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。

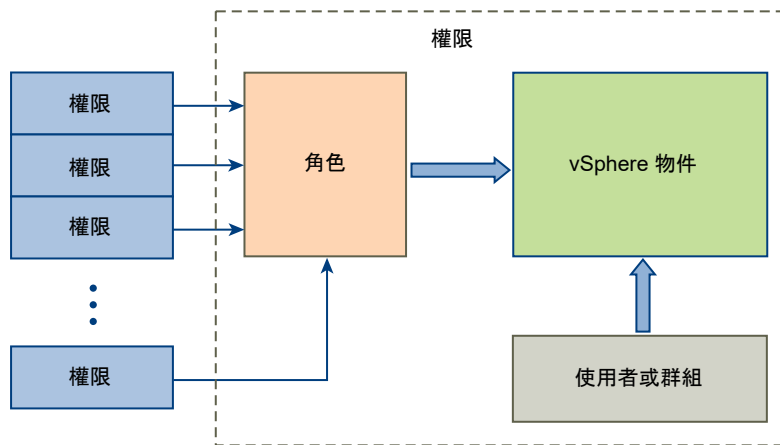
角色

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。

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。

圖 4-1. vSphere 權限



若要將權限指派給物件，請遵循以下步驟執行：

- 1 在 vCenter 物件階層中選取要套用權限的物件。
- 2 選取應擁有該物件權限的群組或使用者。
- 3 選取角色，即群組或使用者應擁有的物件權限集。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。

權限模型透過提供預先定義的角色，使工作效率得到大幅提高。您還可以合併權限，以建立自訂角色。如需所有權限和可將權限套用至其中的物件的相關參考，請參閱第 11 章 [定義的權限](#)。如需執行這些工作所需權限集的一些範例，請參閱 [一般工作所需的權限](#)。

在許多情況下，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部分權限，還需要目的地資料中心的權限。

獨立 ESXi 主機的權限模型更為簡單。請參閱 [為 ESXi 指派權限](#)

vCenter Server 使用者驗證

使用目錄服務的 vCenter Server 系統將根據使用者目錄網域定期驗證使用者和群組。系統將根據 vCenter Server 設定中指定的固定間隔執行驗證。例如，如果在數個物件上為使用者 Smith 指派了某個角色並在網域中將使用者名稱變更為 Smith2，則在下次驗證時，主機會認為 Smith 已不存在並從 vSphere 物件中移除與該使用者關聯的權限。

同樣地，如果將使用者 Smith 從網域中移除，則下次進行驗證時與該使用者關聯的所有權限都會遭到移除。如果在下次進行驗證之前將新使用者 Smith 新增至網域，則新使用者 Smith 會取代舊使用者 Smith 對任何物件具有的權限。

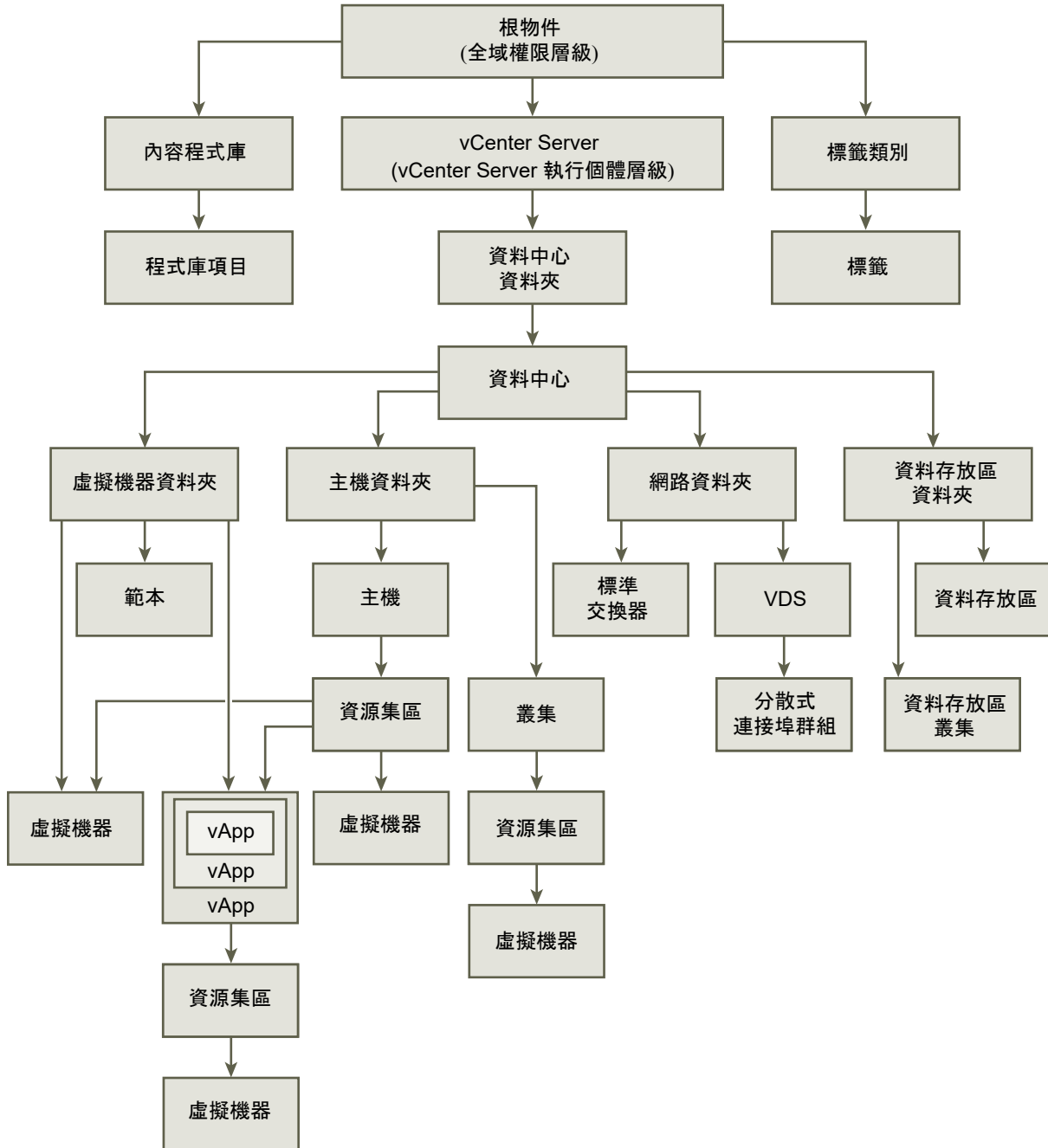
權限的階層式繼承

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 4-2. 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，如果某一虛擬機器位於虛擬機器資料夾中且同時屬於資源集區，則該虛擬機器會同時繼承來自虛擬機器資料夾和資源集區的權限設定。

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：

- 如果沒有為使用者定義對該物件的權限，則使用者將獲得指派給該物件的群組的一組權限。
- 如果為使用者定義了對該物件的權限，則該使用者權限將優先於所有群組權限。

範例 1：多個權限繼承

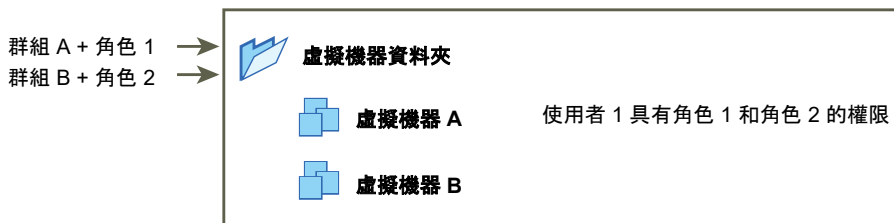
此範例說明物件如何從父系物件上授與權限的群組繼承多個權限。

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 4-3. 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 4-4. 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

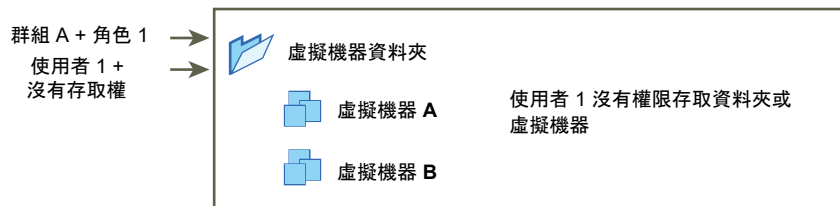
此範例說明了直接指派給個別使用者的角色如何覆寫與指派到群組之角色相關聯的權限。

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 4-5. 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。

角色

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。

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。

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](#)。您還可以为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 Web 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。

必要條件

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 Web 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 **管理索引** 標籤，然後選取 **權限**。
- 3 按一下 [新增] 圖示，然後按一下 **新增**。
- 4 識別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，選取使用者或群組所在的網域。
 - 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**管理索引**標籤，然後選取**權限**。
- 3 按一下行項目，選取使用者或群組，以及角色配對。
- 4 按一下**針對權限變更角色**。
- 5 從**已指派的角色**下拉式功能表，為使用者或群組選取角色。
- 6 若要將權限散佈到指派的詳細目錄物件的子物件，請按一下**散佈**核取方塊，然後按一下**確定**。

移除權限

您可以在物件階層中針對個別使用者或群組移除某物件的權限。當您執行此動作時，使用者將不再具有與該物件上角色相關聯的權限。

程序

- 1 在 vSphere Web Client 物件導覽器中瀏覽到物件。
- 2 按一下**管理索引**標籤，然後選取**權限**。
- 3 按一下適當的行項目，選取使用者和角色配對或群組和角色配對。
- 4 按一下**移除權限**。

結果

vCenter Server 會移除權限設定。

變更權限驗證設定

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 Server 5.0 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 Server 5.0 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。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**管理**索引標籤，然後按一下**設定**。
- 3 依序按一下**一般**和**編輯**。
- 4 選取**使用者目錄**。
- 5 視需要變更值。

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	在 選取使用者或群組 對話方塊中指定 vCenter Server 顯示的所選網域中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)。

- 6 按一下**確定**。

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 vCenter 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。全域根物件會充當每個解決方案物件的父系物件。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。角色決定了該組中的權限。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

大多數情況下，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]，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 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上的所有物件。

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。

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上的所有物件。

必要條件

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 識別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，選取使用者或群組所在的網域。
 - 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 在大多數情況下，請將 [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

如果您將權限授與 vCenter Server 詳細目錄物件上的使用者，例如 ESXi 主機或虛擬機器，則該使用者無法在該物件上執行標籤作業。

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 4-1. 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，Robin 甚至擁有標籤 [生產] 的權限。除非您修改全域權限，否則您無法限制權限。

表 4-2. 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 4-3. 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包含讀取內容和一組執行動作的權限。該角色允許使用者讀取和變更虛擬機器屬性。

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，如果詳細目錄中有兩個資源集區 (集區 A 和集區 B)，可以為特定使用者在集區 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，該使用者可以開啟集區 A 中的虛擬機器，而只能檢視集區 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。可以複製、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

可以使用 CLI 或 vSphere Client 為個別主機建立自訂角色。請參閱《使用 vSphere Client 進行 vSphere 管理》說明文件。無法從 vCenter Server 存取自訂主機角色。

如果透過 vCenter Server 管理 ESXi 主機，則在主機和 vCenter Server 中維護自訂角色可能會導致混淆和誤用。在大多數情況下，建議定義 vCenter Server 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 如果您新增了自訂角色，且未指派任何權限給該角色，則該角色將會建立為唯讀角色，並具有以下三個系統定義的權限：**System.Anonymous**、**System.View** 和 **System.Read**。



在 vSphere Web Client 中建立角色

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_egsyxkp4/uiConfId/49694343/)

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 系統角色

vCenter Server 提供少量預設角色。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。您建立的角色不會繼承任何系統角色的權限。

管理員角色

指派某物件之管理員角色的使用者，能夠檢視並執行該物件上的所有動作。此角色還包括唯讀角色中的所有固有權限。如果您充當的是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。

無存取權角色

指派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。

依預設，administrator@vsphere.local 使用者、根使用者和 vpxuser 是僅有幾個不會指派無存取權角色的使用者。相反，他們會指派管理員角色。只要您先在根層級上以管理員角色建立替代權限，並將此權限與其他使用者關聯，即可從任何權限移除根使用者，或將其角色變更為無存取權。

唯讀角色

指派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。使用者可使用此角色來檢視虛擬機器、主機和資源集區屬性。該使用者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。

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。

如果在屬於與其他 vCenter Server 系統相同的 vCenter Single Sign-On 網域的 vCenter Server 系統上建立或編輯角色，VMware 目錄服務 (vmdir) 會將您所做的變更散佈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。

必要條件

確認您是否以具有管理員權限的使用者身分登入。

程序

- 1 使用 vSphere Web Client 登入 vCenter Server。
- 2 選取 [首頁]，按一下**管理**，然後按一下**角色**。
- 3 按一下**建立角色動作** (+) 按鈕。
- 4 輸入新角色的名稱。
- 5 為該角色選取權限，然後按一下**確定**。

複製角色

可複製現有角色、重新命名以及編輯該角色。進行複製時，新角色不會套用到任何使用者或群組以及物件。您必須將該角色指派給使用者或群組以及物件。

如果在屬於與其他 vCenter Server 系統相同的 vCenter Single Sign-On 網域的 vCenter Server 系統上建立或編輯角色，VMware 目錄服務 (vmdir) 會將您所做的變更散佈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。

必要條件

確認您是否以具有管理員權限的使用者身分登入。

程序

- 1 使用 vSphere Web Client 登入 vCenter Server。
- 2 選取 [首頁]，按一下**管理**，然後按一下**角色**。
- 3 選取某一角色，然後按一下**複製角色動作**圖示。
- 4 輸入複製角色的名稱。
- 5 為該角色選取或取消選取權限，然後按一下**確定**。

編輯角色

編輯角色時，您可以變更為該角色選取的權限。完成後，這些權限將套用於指派了編輯後角色的任一使用者或群組。

如果在屬於與其他 vCenter Server 系統相同的 vCenter Single Sign-On 網域的 vCenter Server 系統上建立或編輯角色，VMware 目錄服務 (vmdir) 會將您所做的變更散佈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。

必要條件

確認您是否以具有管理員權限的使用者身分登入。

程序

- 1 使用 vSphere Web Client 登入 vCenter Server。
- 2 選取 [首頁]，按一下**管理**，然後按一下**角色**。
- 3 選取某個角色，然後按一下**編輯角色動作**按鈕。
- 4 為該角色選取或取消選取權限，然後按一下**確定**。

針對角色和權限的最佳做法

使用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：

- 如有可能，請將角色指派給群組而不是個別使用者，以便將權限授與該群組。
- 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，如果您想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。
- 大多數情況下，請在將權限指派給某物件時啟用傳播。這樣可確保在向詳細目錄階層中插入新物件時，這些物件會繼承權限並且可供使用者存取。
- 如果不希望特定使用者或群組擁有該部分物件階層中之物件的存取權，請使用無存取權角色來遮罩階層的特定區域。
- 即使使用者沒有所有 vCenter Server 系統的權限，對授權的變更也會散佈到連結到相同 Platform Services Controller 或相同 vCenter Single Sign-On 網域中 Platform Services Controller 的所有 vCenter Server 系統。

一般工作所需的權限

許多工作需要針對詳細目錄中多個物件的權限。您可以檢閱執行工作所需的權限以及適當的範例角色。

下表列出了需要多個權限的一般工作。可透過將某位使用者與其中一個預先定義的角色配對來新增權限至詳細目錄物件，或建立具有預期使用多次之權限集的自訂角色。

如果您要執行的工作不在此資料表中，下列規則可協助您確定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 (例如建立虛擬磁碟或建立快照)，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。

- 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 4-4. 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： <ul style="list-style-type: none"> ■ 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
	在包含資料存放區的目的地資料存放區或資料夾上： 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
從範本部署虛擬機器	在目的地資料夾或資料中心上： <ul style="list-style-type: none"> ■ 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
	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： <ul style="list-style-type: none"> ■ 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

表 4-4. 一般工作所需的權限 (續)

工作	所需權限	適當角色
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： <ul style="list-style-type: none"> ■ 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： <ul style="list-style-type: none"> ■ 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： <ul style="list-style-type: none"> ■ 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： <ul style="list-style-type: none"> ■ 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
	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

保護 ESXi 主機

5

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 憑證授權機構 (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：

- [使用指令碼管理主機組態設定](#)
- [利用主機設定檔設定 ESXi 主機](#)
- [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 指派權限](#)
- [使用 Active Directory 管理 ESXi 使用者](#)
- [使用 vSphere Authentication Proxy](#)
- [ESXi 安全性最佳做法](#)
- [設定用於 ESXi 的智慧卡驗證](#)
- [ESXi SSH 金鑰](#)
- [使用 ESXi Shell](#)
- [修改 ESXi Web 代理設定](#)
- [vSphere Auto Deploy 安全考量](#)
- [管理 ESXi 記錄檔](#)

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)	<pre>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</pre>
PowerCLI	<pre>#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 }</pre>

- 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。

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。

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足夠的其他安全性措施，可以保護整個網路以及連線到主機的裝置。

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（並非專用於對主機進行管理存取）均處於關閉狀態。如果需要其他服務，則必須專門開啟適當的連接埠。
- 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 在內部曾使用 Tomcat Web 服務來支援 Web Client 進行存取。Tomcat Web 服務經過修改後，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，以支援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。

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

如果您決定啟用對 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。請勿透過 vSphere Client 直接存取受管理的主機，且不要從主機的 DCUI 變更受管理主機。

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。

使用 vSphere Client 或 VMware CLI 或者 API 管理獨立 ESXi 主機

使用 vSphere Client、其中一個 VMware CLI 或 API 管理您的 ESXi 主機。僅為了疑難排解才以根使用者身分從 DCUI 或 ESXi Shell 存取主機。如果您決定使用 ESXi Shell，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。

主機執行各種第三方套件來支援管理介面或必須執行的工作。VMware 不支援從 VMware 來源以外的任何其他來源升級這些套件。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。定期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/>。

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 vSphere 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)。

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。

密碼不能包含字典字組或部分字典字組。

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` 的手冊頁以瞭解詳細資訊。

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訊。

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。

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 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，建議隔離網路。

- vSphere 基礎結構網路用於如 VMware vSphere vMotion®、VMware vSphere Fault Tolerance 和儲存區等功能。為了實現這些網路的特定功能，會考慮隔離這些網路，並且通常不會在伺服器機架的單一實體集外部路由傳遞這些網路。
- 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一般流量隔離。只能從系統、網路和安全管理員存取此網路。使用跳躍方塊或虛擬私人網路 (VPN) 安全存取管理網路。在此網路內嚴格控制對惡意程式碼潛在來源的存取。
- 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。這些設定會與虛擬機器一起傳輸，因為虛擬機器在 vSphere 環境內的主機之間進行移轉。

停用受管理物件瀏覽器 (MOB)

受管理物件瀏覽器提供了深入瞭解 VMkernel 物件型號的方式。但是，由於您可以使用受管理物件瀏覽器變更主機組態，因此攻擊者將使用此介面執行惡意的組態變更或動作。將受管理物件瀏覽器僅用於偵錯，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。

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。

不再建議透過 ESXi Shell 使用 `vim-cmd`。

停用授權 (SSH) 金鑰

透過授權金鑰，您可以在無需使用者驗證的情況下，透過 SSH 啟用對 ESXi 主機的存取。若要提高主機安全性，請不要允許使用者使用授權金鑰存取主機。

如果某個使用者的公開金鑰位於主機上的 `/etc/ssh/keys-root/authorized_keys` 檔案中，則會被視為受信任的使用者。允許受信任的遠端使用者在不提供密碼的情況下存取主機。

程序

- ◆ 對於日常作業，請停用 ESXi 主機上的 SSH。
- ◆ 即使暫時啟用了 SSH，也要監控 `/etc/ssh/keys-root/authorized_keys` 檔案的內容，確保未允許任何使用者在未進行適當驗證的情況下存取主機。

- ◆ 監控 `/etc/ssh/keys-root/authorized_keys` 檔案，驗證其是否為空且未將任何 SSH 金鑰新增到該檔案中。
- ◆ 如果發現 `/etc/ssh/keys-root/authorized_keys` 檔案不為空，請移除所有金鑰。

結果

停用透過授權金鑰的遠端存取，可能會限制您在不提供有效登入認證的情況下，在主機上遠端執行命令的能力。例如，這會使您無法執行自動的遠端指令碼。

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 來檢視和管理這些憑證。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 6.0 中的憑證

ESXi 和 vCenter Server 通訊時，會將 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 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 5-1. ESXi 主機的憑證模式

憑證模式	說明
VMware Certificate Authority (預設)	<p>如果 VMCA 做為頂層 CA 或媒介 CA 佈建所有 ESXi 主機，則使用此模式。</p> <p>依預設，VMCA 會使用憑證佈建 ESXi 主機。</p> <p>在此模式下，您可以透過 vSphere Web Client 重新整理和更新憑證。</p>
自訂憑證授權機構	<p>若要僅使用由第三方 CA 簽署的自訂憑證，請使用此模式。</p> <p>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。</p> <p>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。</p>
指紋模式	<p>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。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。</p> <p>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。</p>

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。後續開機 ESXi 主機時，會重複使用該憑證。Auto Deploy 伺服器是任何內嵌式部署或管理節點的一部分。

如果 VMCA 在 Auto Deploy 主機首次開機時不可用，則該主機會首先嘗試連線，然後進入關閉和重新開機的循環中，直到 VMCA 變為可用且主機能夠透過已簽署憑證進行佈建。

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 5-2. 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

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_vkuyp3rf/uiConfId/49694343/)

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的憑證取代為 VMCA 簽署的憑證。該程序會保留自訂憑證，即使這些憑證已過期或無效也如此。

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。必須升級到 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，則這些憑證會保留在原位。將憑證模式變更為 [自訂]，確保這些憑證不會意外遭到取代。

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。

如果決定不將主機升級到 vSphere 6.0 或更新版本，則主機會保留其目前所使用的憑證，即使該主機受管於使用 VMCA 憑證的 vCenter Server 系統也如此。

由 Auto Deploy 佈建的主機首次以 ESXi 6.0 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。

ESXi 憑證的預設設定

當 vCenter Server 從 ESXi 主機申請憑證簽署要求 (CSR) 時，會使用預設設定。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。

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

表 5-3. 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 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
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

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。

後續步驟

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 按一下**管理索引標籤**，然後按一下**設定**。

- 3 選取**系統**，然後按一下**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	描述
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。

欄位	描述
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。
	<p>良好</p> <p>一般作業。</p> <p>到期</p> <p>憑證即將到期。</p> <p>即將到期</p> <p>憑證將在 8 個月內到期 (預設)。</p> <p>即將到期</p> <p>憑證將在 2 個月內到期 (預設)。</p> <p>已到期</p> <p>憑證無效，因為已到期。</p>

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 按一下**管理索引標籤**，然後按一下**設定**。
- 3 選取**系統**，然後按一下**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	描述
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。

變更公司專屬的預設憑證設定。如需預設設定的完整清單，請參閱 [ESXi 憑證的預設設定](#)。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**管理索引標籤**，然後按一下**設定**。
- 3 按一下**進階設定**，然後按一下**編輯**。
- 4 在 [篩選器] 方塊中，輸入 `certmgmt` 以僅顯示憑證管理參數。
- 5 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。

後續步驟

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。

瞭解憑證模式切換

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。

表 5-4. ESXi 主機的憑證模式

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。

變更憑證模式

在大多數情況下，使用 VMCA 佈建環境中的 ESXi 主機是最佳解決方案。如果公司原則要求使用含不同根 CA 的自訂憑證，您可以編輯 vCenter Server 進階選項，以便主機不會在您重新整理憑證時使用 VMCA 憑證自動進行佈建。然後，您負責管理環境中的憑證。

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 `vpdx.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

您的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 元件使用在安裝過程中建立的 VMCA 簽署的憑證和金鑰。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。

- **ESXi 憑證簽署要求的需求**

如果要使用第三方 CA 簽署的憑證 (VMCA 做為下層授權機構或者自訂憑證授權機構)，必須向 CA 傳送憑證簽署要求 (CSR)。

- **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

如果要使用第三方 CA 簽署的憑證 (VMCA 做為下層授權機構或者自訂憑證授權機構)，必須向 CA 傳送憑證簽署要求 (CSR)。

使用具有下列特性的 CSR：

- 2048 位元
- PKCS1
- 無萬用字元
- 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。

必要條件

- 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。如需啟用對 ESXi Shell 的存取的相關資訊，請參閱《vSphere 安全性》出版物。

- 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。如需透過角色指派權限的相關資訊，請參閱《vSphere 安全性》出版物。

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。

後續步驟

更新 vCenter Server TRUSTED_ROOTS 存放區。請參閱 [更新 vCenter Server TRUSTED_ROOTS 存放區 \(自訂憑證\)](#)。

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。

必要條件

- 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。如需啟用對 ESXi Shell 的存取的相關資訊，請參閱《vSphere 安全性》出版物。
- 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。如需透過角色指派權限的相關資訊，請參閱《vSphere 安全性》出版物。

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。
- 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。

後續步驟

更新 vCenter Server TRUSTED_ROOTS 存放區。請參閱 [更新 vCenter Server TRUSTED_ROOTS 存放區 \(自訂憑證\)](#)。

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。

必要條件

- 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。如需啟用對 ESXi Shell 的存取的相關資訊，請參閱《vSphere 安全性》出版物。
- 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。如需透過角色指派權限的相關資訊，請參閱《vSphere 安全性》出版物。

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。

後續步驟

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。

必要條件

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

後續步驟

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](#)。

透過 Auto Deploy 使用自訂憑證

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。

必要條件

- 從 CA 申請滿足您需求的憑證。
 - 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 在執行 Auto Deploy 服務的系統上，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。

```
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
```

Windows

`C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe`

Linux

`/usr/lib/vmware-vmafd/bin/vecs-cli`

- 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。

結果

下次佈建設定為使用 Auto Deploy 的主機時，Auto Deploy 伺服器會使用剛剛新增至 TRUSTED_ROOTS 存放區的根憑證來產生憑證。

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

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8qp59yqe/uiConfId/49694343/)

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[管理索引標籤](#)，然後按一下[設定](#)。
- 3 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。



將允許的 IP 位址新增到 ESXi 防火牆

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_Ougsspa2/uiConfId/49694343/)

程序

- 1 在 vSphere Web Client 詳細目錄中瀏覽到主機。
- 2 按一下**管理索引標籤**，然後按一下**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 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。

下表列出了通常為服務安裝的防火牆。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。

表 5-5. 傳入防火牆連線

服務	連接埠	註解
CIM 伺服器	5988 (TCP)	適用於 CIM (通用訊息模型) 的伺服器。
CIM 安全伺服器	5989 (TCP)	適用於 CIM 的安全伺服器。
CIM SLP	427 (TCP、UDP)	CIM 用戶端使用服務位置通訊協定第 2 版 (SLPv2) 尋找 CIM 伺服器。
DHCPv6	546 (TCP、UDP)	適用於 IPv6 的 DHCP 用戶端。
DVSSync	8301、8302 (UDP)	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。
NFC	902 (TCP)	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。
Virtual SAN 叢集服務	12345、23451 (UDP)	Virtual SAN 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 Virtual SAN 中繼資料散佈至所有叢集成員。如果已停用，Virtual SAN 將無法運作。
DHCP 用戶端	68 (UDP)	適用於 IPv4 的 DHCP 用戶端。
DNS 用戶端	53 (UDP)	DNS 用戶端。
Fault Tolerance	8200、8100、8300 (TCP、UDP)	主機之間用於 vSphere Fault Tolerance (FT) 的流量。
NSX 分散式邏輯路由器服務	6999 (UDP)	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。
Virtual SAN 傳輸	2233 (TCP)	Virtual SAN 可靠的資料包傳輸。此服務使用 TCP，且用於 Virtual SAN Storage I/O。如果已停用，Virtual SAN 將無法運作。
SNMP 伺服器	161 (UDP)	允許主機連線到 SNMP 伺服器。
SSH 伺服器	22 (TCP)	執行 SSH 存取時需要。
vMotion	8000 (TCP)	透過 vMotion 移轉虛擬機器時需要。
vSphere Web Client	902、443 (TCP)	用戶端連線

表 5-5. 傳入防火牆連線 (續)

服務	連接埠	註解
vsanvp	8080 (TCP)	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 Virtual SAN 儲存區設定檔、功能和符合性的相關資訊。如果已停用，Virtual SAN 以儲存區設定檔為基礎的管理 (SPBM) 將無法運作。
vSphere Web Access	80 (TCP)	[歡迎] 頁面，包含不同介面的下載連結。
RFB 通訊協定	5900-5964 (TCP)	由管理工具 (如 VNC) 使用。

表 5-6. 傳出防火牆連線

服務	連接埠	註解
CIM SLP	427 (TCP、UDP)	CIM 用戶端使用服務位置通訊協定第 2 版 (SLPv2) 尋找 CIM 伺服器。
DHCPv6	547 (TCP、UDP)	適用於 IPv6 的 DHCP 用戶端。
DVSSync	8301、8302 (UDP)	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。
HBR	44046、31031 (TCP)	由 vSphere Replication 和 VMware Site Recovery Manager 用於目前的複寫流量。
NFC	902 (TCP)	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。
WOL	9 (UDP)	透過網路喚醒使用。
Virtual SAN 叢集服務	12345 23451 (UDP)	由 Virtual SAN 使用的叢集監控、成員資格和目錄服務。
DHCP 用戶端	68 (UDP)	DHCP 用戶端。
DNS 用戶端	53 (TCP、UDP)	DNS 用戶端。
Fault Tolerance	80、8200、8100、8300 (TCP、UDP)	支援 VMware Fault Tolerance。
軟體 iSCSI 用戶端	3260 (TCP)	支援軟體 iSCSI。
NSX 分散式邏輯路由服務	6999 (UDP)	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。
rabbitmqproxy	5671 (TCP)	在 ESXi 主機上執行的 Proxy，允許應用程式在虛擬機器內執行，以便與 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。Proxy 將連線到 vCenter 網路網域中的代理。因此，傳出連線 IP 位址應至少包含目前正在使用中的或未來的代理。如果客戶想要擴充，可新增代理。

表 5-6. 傳出防火牆連線 (續)

服務	連接埠	註解
Virtual SAN 傳輸	2233 (TCP)	用於 Virtual SAN 節點之間的 RDT 流量 (單點傳播對等通訊)。
vMotion	8000 (TCP)	透過 vMotion 移轉虛擬機器時需要。
VMware vCenter Agent	902 (UDP)	vCenter Server 代理程式。
vsanvp	8080 (TCP)	用於 Virtual SAN 廠商提供者流量。

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。

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 命令列介面概念和範例》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。

表 5-7. 防火牆命令

命令	說明
<code>esxcli network firewall get</code>	傳回防火牆的啟用或停用狀態，並列出預設動作。
<code>esxcli network firewall set --default-action</code>	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。
<code>esxcli network firewall set --enabled</code>	啟用或停用 ESXi 防火牆。
<code>esxcli network firewall load</code>	載入防火牆模組和規則集組態檔。
<code>esxcli network firewall refresh</code>	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。
<code>esxcli network firewall unload</code>	損毀篩選器並卸載防火牆模組。
<code>esxcli network firewall ruleset list</code>	列出規則集資訊。
<code>esxcli network firewall ruleset set --allowed-all</code>	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。
<code>esxcli network firewall ruleset set --enabled --ruleset-id=<string></code>	將 enabled 設定為 true 或 false，可啟用或停用指定的規則集。
<code>esxcli network firewall ruleset allowedip list</code>	列出指定規則集的允許 IP 位址。
<code>esxcli network firewall ruleset allowedip add</code>	允許從指定的 IP 位址或 IP 位址範圍存取規則集。
<code>esxcli network firewall ruleset allowedip remove</code>	從指定的 IP 位址或 IP 位址範圍移除對規則集的存取權。
<code>esxcli network firewall ruleset rule list</code>	列出防火牆中每個規則集的規則。

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。其他服務 (例如 SSH) 均包含在主機的安全性設定檔中。如果公司原則允許，您可以根據需要啟用和停用這些服務。

[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 5-8. 安全性設定檔中的 ESXi 服務

服務	預設值	描述
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。
本機安全性驗證伺服器 (Active Directory 服務)	已停止	Active Directory 服務的一部分。當您針對 Active Directory 設定 ESXi 時，此服務即啟動。
I/O 重新導向器 (Active Directory 服務)	已停止	Active Directory 服務的一部分。當您針對 Active Directory 設定 ESXi 時，此服務即啟動。
網路登入伺服器 (Active Directory 服務)	已停止	Active Directory 服務的一部分。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。
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《vSphere 安裝和設定》。
vSphere High Availability Agent	已停止	支援 vSphere High Availability 功能。
vProbe 精靈	已停止	vProbe 精靈。
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。

必要條件

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**管理索引標籤**，然後按一下**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，並在主機關機之前不久關閉。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

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_zg4ylgu0/uiConfId/49694343/)

一般鎖定模式和嚴格鎖定模式

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。

一般鎖定模式

在一般鎖定模式下，不會停止 DCUI 服務。如果 vCenter Server 系統的連線中斷，且無法再透過 vSphere Web Client 進行存取，具有權限的帳戶可以登入 ESXi 主機的 Direct Console 介面並結束鎖定模式。只有下列帳戶可以存取 Direct Console 使用者介面：

- 鎖定模式的 [例外使用者] 清單中擁有該主機之管理權限的帳戶。[例外使用者] 清單適用於執行極特定工作的服務帳戶。將 ESXi 管理員新增到此清單會讓鎖定模式的用途失效。
- 該主機之 DCUI.Access 進階選項中定義的使用者。此選項用於在 vCenter Server 連線中斷的情況下緊急存取 Direct Console 介面。這些使用者不需要該主機的管理權限。

嚴格鎖定模式

嚴格鎖定模式是 vSphere 6.0 中的新增模式，這種模式下會停止 DCUI 服務。如果 vCenter Server 的連線中斷，且無法再使用 vSphere Web Client，則 ESXi 主機將無法使用，除非啟用 ESXi Shell 和 SSH 服務並定義「例外使用者」。如果您無法還原 vCenter Server 系統的連線，則必須重新安裝該主機。

鎖定模式以及 ESXi Shell 與 SSH 服務

嚴格鎖定模式會停止 DCUI 服務。不過，ESXi Shell 和 SSH 服務不受鎖定模式的影響。如果要讓鎖定模式成為有效的安全性措施，請確保同樣停用 ESXi Shell 和 SSH 服務。這些服務預設為停用狀態。

主機處於鎖定模式時，如果 [例外使用者] 清單中的使用者擁有主機的管理員角色，則可以從 ESXi Shell 並透過 SSH 存取該主機。即使處於嚴格鎖定模式，仍然可存取主機。保持停用 ESXi Shell 服務和 SSH 服務是最安全的選擇。

備註 [例外使用者] 清單適用於執行特定工作 (例如，主機備份) 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。

啟用和停用鎖定模式

具有權限的使用者可以透過下列多種方式啟用鎖定模式：

- 使用**新增主機精靈**將主機新增到 vCenter Server 系統時。
- 使用 vSphere Web Client。請參閱[使用 vSphere Web Client 啟用鎖定模式](#)。您可以從 vSphere Web Client 中啟用一般鎖定模式和嚴格鎖定模式。
- 使用 Direct Console 使用者介面 (DCUI)。請參閱從 [Direct Console 使用者介面啟用或停用一般鎖定模式](#)。

具有權限的使用者可以從 vSphere Web Client 停用鎖定模式。他們可從 Direct Console 介面停用一般鎖定模式，但是無法從 Direct Console 介面停用嚴格鎖定模式。

備註 如果使用 Direct Console 使用者介面來啟用或停用鎖定模式，則會捨棄主機上使用者和群組的權限。若要保留這些權限，您必須使用 vSphere Web Client 啟用和停用鎖定模式。

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，「例外使用者」清單中具有管理員權限的帳戶和 DCUI.Access 進階系統設定中指定的使用者均可存取 Direct Console 介面。
- 如果 ESXi Shell 或 SSH 已啟用，而主機處於嚴格或一般鎖定模式下，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 5-9. 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，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

在啟用鎖定模式前，如果使用者已登入 ESXi Shell 或透過 SSH 存取主機，則「例外使用者」清單中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。這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。

若要完全禁止所有對主機的直接存取，則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**管理**索引標籤，然後按一下**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

能夠在 ESXi 主機上存取 Direct Console 使用者介面的使用者可以停用一般鎖定模式。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**管理**索引標籤，然後按一下**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**無**來停用鎖定模式。

結果

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。

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

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。

如果已啟用鎖定模式，不同帳戶預設執行的動作以及如何變更預設行為，取決於 vSphere 環境的版本。

- 在 vSphere 5.1 版之前的 vSphere 版本中，僅根使用者可以在處於鎖定模式的 ESXi 主機上登入到 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。該選項適用於災難性的 vCenter Server 失敗，並且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

DCUI.Access 進階選項的主要用途為，當發生災難性的失敗時，如果無法從 vCenter Server 存取主機，可讓您結束鎖定模式。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。這可能會影響您主機的安全性。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**管理索引標籤**，然後選取**設定**。
- 3 按一下**進階系統設定**，然後選取 **DCUI.Access**。
- 4 按一下**編輯**，輸入使用者名稱，並以逗號分隔。

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

- 5 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**管理索引標籤**，然後按一下**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。

檢查主機和 VIB 的接受程度

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。

您可以使用 ESXCLI 命令來設定主機的接受程度。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。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。

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。現在，僅 IOVP 驅動程式是以此程度發佈的。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 或 VMwareAccepted。

```
esxcli software acceptance get
```

- 2 如果主機的接受程度不是 VMwareCertified 或 VMwareAccepted，請執行以下命令判定是否有 VIB 的接受程度不是 VMwareCertified 或 VMwareAccepted。

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

- 3 執行以下命令移除接受程度為 PartnerSupported 或 CommunitySupported 的任何 VIB。

```
esxcli software vib remove --vibname vib
```

- 4 執行以下命令變更主機的接受程度。

```
esxcli software acceptance set --level acceptance_level
```

為 ESXi 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。

將權限指派給受 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。

您可以在 vCenter Server 物件階層中選取 ESXi 主機物件，並將管理員角色指派給有限數目的使用者，這些使用者可能會對 ESXi 主機執行直接管理。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

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。請參閱[根使用者權限](#)。
- vpxuser。請參閱[vpxuser 權限](#)。
- dcui 使用者。請參閱[DCUI 使用者權限](#)。

您可以新增本機使用者，並從 vSphere Client 的 [管理] 索引標籤中定義自訂角色。

如需 ESXi 的全部版本，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。此項為預設。可以適當覆寫預設值。

透過使用直接連線至 ESXi 主機的 vSphere 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。

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。如果將角色指派給其中一個使用者，則不會給其他使用者指派相同的角色。

根使用者權限

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。

這個一般根帳戶可更輕易闖入 ESXi 主機，並且難以比對特定管理員的動作。

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。在 vSphere 5.1 及更新版本中，僅允許具有管理員角色的根使用者 (不允許其他具名使用者) 新增主機到 vCenter Server。

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。如果可能，請使用可讓您管理 Active Directory 認證的 ESXi Active Directory 功能。

重要 如果您移除根使用者的存取權限，則必須首先在根層級 (擁有一個指派到管理員角色的不同使用者) 建立其他權限。

vpuser 權限

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

vCenter Server 在它所管理的主機上擁有管理員權限。例如，vCenter Server 可將虛擬機器移到主機或從主機移動，並執行所需的組態變更以支援虛擬機器。

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。僅限擁有管理員權限的使用者直接在每台主機上執行這些工作。

備註 您無法使用 Active Directory 管理 vpuser。

注意 請勿以任何方式變更 vpuser。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 使用者權限

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。

安裝或升級 vSphere Authentication Proxy

安裝 vSphere Authentication Proxy 可讓 ESXi 主機無需使用 Active Directory 認證即可加入網域。由於不需要在主機組態中儲存 Active Directory 認證，因此 vSphere Authentication Proxy 可提高 PXE 開機的主機和使用 Auto Deploy 佈建的主機的安全性。

如果系統中安裝有舊版 vSphere Authentication Proxy，則此程序會將 vSphere Authentication Proxy 升級到目前版本。

您可以在相關聯的 vCenter Server 所在的機器上安裝 vSphere Authentication Proxy，或在具有 vCenter Server 網路連線的其他機器上進行安裝。vCenter Server 5.0 及更新版本支援 vSphere Authentication Proxy。

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 執行個體可以位於純 IPv4、IPv4/IPv6 混合模式或純 IPv6 網路環境中的主機上，但透過 vSphere Web Client 連線到 vCenter Server 的機器必須具有 IPv4 位址，vSphere Authentication Proxy 服務才能運作。

必要條件

- 在要安裝 vSphere Authentication Proxy 的機器上，安裝 Microsoft .NET Framework 3.5。
- 確認您具有管理員權限。
- 確認主機電腦具有受支援的處理器和作業系統。
- 確認主機電腦具有有效的 IPv4 位址。您可以在純 IPv4 網路環境或 IPv4/IPv6 混合模式網路環境中的電腦上安裝 vSphere Authentication Proxy，但無法在純 IPv6 環境中的電腦上安裝 vSphere Authentication Proxy。
- 如果要將 vSphere Authentication Proxy 安裝到 Windows Server 2008 R2 主機電腦上，請從 support.microsoft.com 網站下載 Windows 知識庫文章 981506 中所述的 Windows Hotfix 並進行安裝。如果未安裝此 Hotfix，則 vSphere Authentication Proxy 介面卡將無法進行初始化。發生此問題的同時還會在 `camadapter.log` 中顯示類似於無法將 CAM 網站與 CTL 繫結和無法初始化 CAMAdapter 的錯誤訊息。
- 下載 vCenter Server 安裝程式。

收集下列資訊來完成安裝或升級：

- vSphere Authentication Proxy 的安裝位置 (如果未使用預設位置)。

- vSphere Authentication Proxy 將連線到的 vCenter Server 的位址和認證：IP 位址或名稱、HTTP 連接埠、使用者名稱和密碼。
- 用於在網路上識別 vSphere Authentication Proxy 的主機名稱或 IP 位址。

程序

- 1 將要安裝 Authentication Proxy 服務的主機電腦新增到網域。
- 2 使用網域管理員帳戶登入該主機電腦。
- 3 在軟體安裝程式目錄中，按兩下 `autorun.exe` 檔案以啟動安裝程式。
- 4 選取 **VMware vSphere Authentication Proxy**，然後按一下**安裝**。
- 5 依照精靈提示完成安裝或升級。

在安裝期間，驗證服務會向已登錄 Auto Deploy 的 vCenter Server 執行個體進行登錄。

結果

安裝 vSphere Authentication Proxy 服務時，安裝程式會建立具有適當權限的網域帳戶來執行 Authentication Proxy 服務。帳戶名稱以前置詞 `CAM-` 開頭，並且會隨機產生 32 個字元的密碼與其相關聯。密碼設定為永不到期。請勿變更帳戶設定。

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**，則將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。

必要條件

- 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 依序按一下**管理索引標籤**和**網路**。
 - c 按一下 [DNS]，並確認主機的名稱與 DNS 伺服器資訊是正確的。

後續步驟

使用 vSphere Web Client 加入目錄服務網域。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`)：系統會在預設容器下建立該帳戶。
- `name.tld/container/path` (例如，`domain.com/OU1/OU2`)：系統會在特定組織單位 (OU) 下建立該帳戶。

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**管理索引標籤**，然後按一下**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**管理**索引標籤，然後按一下**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

使用 vSphere Authentication Proxy 時，無需將 Active Directory 認證傳輸到主機。使用者將主機新增至網域時，會提供 Active Directory 伺服器的網域名稱和 Authentication Proxy 伺服器的 IP 位址。

vSphere Authentication Proxy 在與 Auto Deploy 搭配使用時尤其有用。可以設定指向 Authentication Proxy 的參考主機，並設定將參考主機的設定檔套用到任何使用 Auto Deploy 佈建之 ESXi 主機的規則。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，該程序仍會順暢完成。請參閱[透過 Auto Deploy 使用自訂憑證](#)。

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

安裝或升級 vSphere Authentication Proxy

安裝 vSphere Authentication Proxy 可讓 ESXi 主機無需使用 Active Directory 認證即可加入網域。由於不需要在主機組態中儲存 Active Directory 認證，因此 vSphere Authentication Proxy 可提高 PXE 開機的主機和使用 Auto Deploy 佈建的主機的安全性。

如果系統中安裝有舊版 vSphere Authentication Proxy，則此程序會將 vSphere Authentication Proxy 升級到目前版本。

您可以在相關聯的 vCenter Server 所在的機器上安裝 vSphere Authentication Proxy，或在具有 vCenter Server 網路連線的其他機器上進行安裝。vCenter Server 5.0 及更新版本支援 vSphere Authentication Proxy。

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 執行個體可以位於純 IPv4、IPv4/IPv6 混合模式或純 IPv6 網路環境中的主機上，但透過 vSphere Web Client 連線到 vCenter Server 的機器必須具有 IPv4 位址，vSphere Authentication Proxy 服務才能運作。

必要條件

- 在要安裝 vSphere Authentication Proxy 的機器上，安裝 Microsoft .NET Framework 3.5。
- 確認您具有管理員權限。
- 確認主機電腦具有受支援的處理器和作業系統。
- 確認主機電腦具有有效的 IPv4 位址。您可以在純 IPv4 網路環境或 IPv4/IPv6 混合模式網路環境中的電腦上安裝 vSphere Authentication Proxy，但無法在純 IPv6 環境中的電腦上安裝 vSphere Authentication Proxy。

- 如果要將 vSphere Authentication Proxy 安裝到 Windows Server 2008 R2 主機電腦上，請從 support.microsoft.com 網站下載 Windows 知識庫文章 981506 中所述的 Windows Hotfix 並進行安裝。如果未安裝此 Hotfix，則 vSphere Authentication Proxy 介面卡將無法進行初始化。發生此問題的同時還會在 camadapter.log 中顯示類似於無法將 CAM 網站與 CTL 繫結和無法初始化 CAMAdapter 的錯誤訊息。
- 下載 vCenter Server 安裝程式。

收集下列資訊來完成安裝或升級：

- vSphere Authentication Proxy 的安裝位置 (如果未使用預設位置)。
- vSphere Authentication Proxy 將連線到的 vCenter Server 的位址和認證：IP 位址或名稱、HTTP 連接埠、使用者名稱和密碼。
- 用於在網路上識別 vSphere Authentication Proxy 的主機名稱或 IP 位址。

程序

- 1 將要安裝 Authentication Proxy 服務的主機電腦新增到網域。
- 2 使用網域管理員帳戶登入該主機電腦。
- 3 在軟體安裝程式目錄中，按兩下 autorun.exe 檔案以啟動安裝程式。
- 4 選取 **VMware vSphere Authentication Proxy**，然後按一下**安裝**。
- 5 依照精靈提示完成安裝或升級。

在安裝期間，驗證服務會向已登錄 Auto Deploy 的 vCenter Server 執行個體進行登錄。

結果

安裝 vSphere Authentication Proxy 服務時，安裝程式會建立具有適當權限的網域帳戶來執行 Authentication Proxy 服務。帳戶名稱以前置詞 CAM- 開頭，並且會隨機產生 32 個字元的密碼與其相關聯。密碼設定為永不到期。請勿變更帳戶設定。

設定主機以使用 vSphere Authentication Proxy 進行驗證

安裝 vSphere Authentication Proxy 服務 (CAM 服務) 後，必須設定主機，使用 Authentication Proxy 伺服器對使用者進行驗證。

必要條件

在主機上安裝 vSphere Authentication Proxy 服務 (CAM 服務)。請參閱 [安裝或升級 vSphere Authentication Proxy](#)。

程序

1 使用主機上的 IIS 管理員設定 DHCP 範圍。

透過設定範圍，在管理網路中使用 DHCP 的主機可以使用 Authentication Proxy 服務。

選項	動作
對於 IIS 6	<ul style="list-style-type: none"> a 瀏覽到電腦帳戶管理網站。 b 在虛擬目錄 CAM ISAPI 上按一下滑鼠右鍵。 c 選取內容 > 目錄安全性 > 編輯 IP 位址和網域名稱限制 > 新增電腦群組。
對於 IIS 7	<ul style="list-style-type: none"> a 瀏覽到電腦帳戶管理網站。 b 在左窗格中按一下 CAM ISAPI 虛擬目錄，然後開啟 IPv4 位址和網域限制。 c 選取新增允許項目 > IPv4 位址範圍。

2 如果 Auto Deploy 未佈建某個主機，請將預設 SSL 憑證變更為自我簽署憑證或由商業憑證授權單位 (CA) 簽署的憑證。

選項	說明
VMCA 憑證	<p>如果使用預設 VMCA 簽署的憑證，您必須確保 Authentication Proxy 主機信任此 VMCA 憑證。</p> <ul style="list-style-type: none"> a 將 VMCA 憑證手動新增至受信任的根憑證授權機構憑證存放區。 b 將 VMCA 簽署的憑證 (root.cer) 新增至本機信任憑證存放區，該存放區位於 Authentication Proxy 服務安裝所在的系統上。您可在 C:\ProgramData\VMware\CIS\data\vmca 中找到該檔案。 c 重新啟動 vSphere Authentication Proxy 服務。
第三方 CA 簽署的憑證	<p>將 CA 簽署的憑證 (DER 編碼) 新增到本機信任憑證存放區，該存放區位於 Authentication Proxy 服務安裝所在的系統上，然後重新啟動 vSphere Authentication Proxy 服務。</p> <ul style="list-style-type: none"> ■ 針對 Windows 2003，將憑證檔案複製到 C:\Documents and Settings\All Users\Application Data\VMware\vsphere Authentication Proxy\trust。 ■ 針對 Windows 2008，將憑證檔案複製到 C:\Program Data\VMware\vsphere Authentication Proxy\trust。

設定 vSphere Authentication Proxy

若 ESXi 主機具有 Authentication Proxy 憑證資訊，則可以使用 vSphere Authentication Proxy。

您只需驗證伺服器一次。

備註 ESXi 和 Authentication Proxy 伺服器必須能夠進行驗證。請確保始終啟用此驗證功能。如果必須停用驗證功能，您可以使用 [進階設定] 對話方塊，將 UserVars.ActiveDirectoryVerifyCAMCertificate 屬性設定為 0。

匯出 vSphere Authentication Proxy 憑證

若要向 ESXi 驗證 vSphere Authentication Proxy，必須為 ESXi 提供 Proxy 伺服器憑證。

必要條件

在主機上安裝 vSphere Authentication Proxy (CAM 服務)。請參閱 [安裝或升級 vSphere Authentication Proxy](#)。

程序

- 1 在 Authentication Proxy 伺服器系統上，使用 IIS Manager 匯出憑證。

選項	動作
對於 IIS 6	<ol style="list-style-type: none"> a 在電腦帳戶管理網站上按一下滑鼠右鍵。 b 選取內容 > 目錄安全性 > 檢視憑證。
對於 IIS 7	<ol style="list-style-type: none"> a 按一下左窗格中的電腦帳戶管理網站。 b 選取繫結以開啟 [站台繫結] 對話方塊。 c 選取 https 繫結。 d 選取編輯 > 檢視 SSL 憑證。

- 2 選取詳細資料 > 複製到檔案。
- 3 選取不要匯出私密金鑰和 Base-64 編碼 X.509 (.CER)選項。

後續步驟

將憑證匯入到 ESXi。

將 Proxy 伺服器憑證匯入到 ESXi

若要向 ESXi 驗證 vSphere Authentication Proxy 伺服器，請將 Proxy 伺服器憑證上傳到 ESXi。

您可以使用 vSphere Web Client 使用者介面，將 vSphere Authentication Proxy 伺服器憑證上傳到 ESXi 主機。

必要條件

在主機上安裝 vSphere Authentication Proxy 服務 (CAM 服務)。請參閱 [安裝或升級 vSphere Authentication Proxy](#)。

匯出 vSphere Authentication Proxy 伺服器憑證 (如[匯出 vSphere Authentication Proxy 憑證](#)中所述)。

程序

- 1 瀏覽到主機，按一下管理索引標籤，然後依序按一下設定和驗證服務。
- 2 按一下匯入憑證。
- 3 輸入主機上 Authentication Proxy 伺服器憑證檔案的完整路徑和 Authentication Proxy 伺服器的 IP 位址。
使用 [datastore name] file path 形式輸入 Proxy 伺服器的路徑。
- 4 按一下確定。

使用 vSphere Authentication Proxy 將主機新增到網域

將主機加入目錄服務網域時，可以使用 vSphere Authentication Proxy 伺服器進行驗證，而不傳輸使用者提供的 Active Directory 認證。

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

必要條件

- 使用 vSphere Web Client 連線到 vCenter Server 系統。
- 如果 ESXi 設定了 DHCP 位址，請設定 DHCP 範圍。
- 如果 ESXi 設定了靜態 IP 位址，請確認其相關聯設定檔已設為使用 vSphere Authentication Proxy 服務來加入網域，因此 Authentication Proxy 伺服器可以信任 ESXi IP 位址。
- 如果 ESXi 使用 VMCA 簽署憑證，請確認已將主機新增到 vCenter Server。如此可使 Authentication Proxy 伺服器信任 ESXi。
- 如果 ESXi 正使用 CA 簽署的憑證，且未經 Auto Deploy 佈建，請確認 CA 憑證已新增到 Authentication Proxy 伺服器的本機信任憑證儲存區 (如 [設定主機以使用 vSphere Authentication Proxy 進行驗證](#) 中所述)。
- 向主機驗證 vSphere Authentication Proxy 伺服器。

程序

- 1 在 vSphere Web Client 中瀏覽到主機，然後按一下**管理索引標籤**。
- 2 按一下**設定**，然後選取**驗證服務**。
- 3 按一下**加入網域**。
- 4 輸入網域。
使用 `name.tld` 或 `name.tld/container/path` 形式。
- 5 選取**使用 Proxy 伺服器**。
- 6 輸入 Authentication Proxy 伺服器的 IP 位址。
- 7 按一下**確定**。

取代 ESXi 主機的 Authentication Proxy 憑證

您可以匯入 vSphere Web Client 中受信任憑證授權單位所核發的憑證

必要條件

- 將 Authentication Proxy 憑證檔案上傳到 ESXi 主機。

程序

- 1 在 vSphere Web Client 中選取 ESXi 主機。
- 2 在設定索引標籤中，選取系統區域內的驗證服務。
- 3 按一下匯入憑證。
- 4 輸入 SSL 憑證路徑和 vSphere Authentication Proxy 伺服器。

ESXi 安全性最佳做法

遵循 ESXi 安全性最佳做法可確保 vSphere 部署的完整性。如需其他資訊，請參閱《強化指南》。

確認安裝媒體

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

下載媒體後，請使用 MD5 總和值確認下載的完整性。將 MD5 總和輸出值與 VMware 網站上公佈的值加以比較。每個作業系統有不同的方法和工具可供檢查 MD5 總和值。對於 Linux，請使用 md5sum 命令。對於 Microsoft Windows，您可以下載附加元件產品。

手動檢查 CRL

依預設，ESXi 主機不支援 CRL 檢查。您必須手動搜尋並移除撤銷的憑證。這些憑證通常是來自公司 CA 或第三方 CA 的自訂產生的憑證。許多公司使用指令碼尋找並取代 ESXi 主機上撤銷的 SSL 憑證。

監控 ESX Admins Active Directory 群組

vSphere 使用的 Active Directory 群組由 `plugins.hostsvc.esxAdminsGroup` 進階系統設定定義。依預設，將此選項設定為 ESX Admins。將為 ESX Admins 群組的所有成員授與網域中所有 ESXi 主機的完整管理存取權。針對這個群組的建立監控 Active Directory，並將成員資格限制為高度信任的使用者和群組。

監控組態檔

雖然大多數 ESXi 組態設定使用 API 加以控制，僅有限數目的組態檔直接影響主機。這些檔案透過 vSphere 檔案傳輸 API (使用 HTTPS) 公開。如果您對這些檔案做出變更，則您也必須執行對應的管理動作，例如變更組態。

備註 請勿嘗試監控未透過此檔案傳輸 API 公開的檔案。

使用 vmkfstool 清除敏感資料

刪除含敏感資料的 VMDK 檔案時，請關閉或停止虛擬機器，然後對該檔案發出 vCLI 命令 `vmkfstools --writezeros`。然後，您可以從資料存放區刪除檔案。

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可使 ESXi 完全關閉漏洞。

僅在虛擬機器由受信任的實體擁有並管理時，VMware 才建議您使用 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。這個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，或者由客體作業系統中的驅動程式問題導致。
- 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，例如，如果 DMA 作業虛擬機器將記憶體之外的地址作為目標。在某些機器上，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 主機的任意向量上。ESXi 目前在其可用的 Intel 平台上使用插斷重新對應，插斷對應是 Intel VT-d 功能集的一部分。ESXi 在 AMD 平台上沒有使用插斷對應。偽插斷很有可能導致 ESXi 主機損毀，但是理論上也可能有其他方式可利用這些插斷。

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，而不使用使用者名稱和密碼的預設提示。

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因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 會提示您輸入有效的智慧卡和 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。

必要條件

- 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**管理索引標籤**，然後按一下**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**管理索引標籤**，然後按一下**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**。

在發生連線問題的情況下驗證使用者認證

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。如果已中斷與 AD 伺服器的連線，您可以使用本機 ESXi 使用者的認證登入 ESXi DCUI。如此您便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。

ESXi SSH 金鑰

您可以使用 SSH 金鑰來限制、控制以及保護 ESXi 主機的存取權限。透過使用 SSH 金鑰，您可以允許受信任的使用者或指令碼在不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 命令列介面入門》。也可以使用 HTTPS PUT 將 SSH 金鑰複製到主機。

您可以在 ESXi 主機上建立金鑰並將其下載，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，建議不在強化環境中執行此作業。請參閱 [停用授權 \(SSH\) 金鑰](#)。

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。ESXi 5.1 版本已修正此問題。

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。

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 請勿修改 `/etc/ssh/sshd_config` 檔案。

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 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	<code>https://hostname_or_IP_address/host/ssh_root_authorized_keys</code> 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	<code>https://hostname_or_IP_address/host/ssh_host_dsa_key</code>
DSA 公開金鑰	<code>https://hostname_or_IP_address/host/ssh_host_dsa_key_pub</code>
RSA 金鑰	<code>https://hostname_or_IP_address/host/ssh_host_rsa_key</code>
RSA 公開金鑰	<code>https://hostname_or_IP_address/host/ssh_host_rsa_key_pub</code>

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。

請參閱《vSphere 安全性》。

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。

必要條件

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**管理索引標籤**，然後按一下**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**。

後續步驟

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**管理**索引標籤，然後按一下**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**圖示。
- 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**。

結果

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**管理**索引標籤，然後按一下**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。

結果

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。

後續步驟

設定 ESXi Shell 的可用性和閒置逾時。請參閱在 [Direct Console 使用者介面中為 ESXi Shell 可用性建立逾時](#)和為閒置 [ESXi Shell 工作階段建立逾時](#)。

在 Direct Console 使用者介面中為 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 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。
- 2 輸入可用性逾時。
您必須重新啟動 SSH 服務和 ESXi Shell 服務，逾時才能生效。
- 3 按 Enter 並按 Esc，直到返回到 Direct Console 使用者介面的主功能表。
- 4 按一下**確定**。

結果

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。

為閒置 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。

閒置逾時值是使用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，不會影響現有工作階段。

您可以從 Direct Console 使用者介面指定逾時 (以秒為單位)，或從 vSphere Web Client 指定逾時 (以分鐘為單位)。

程序

- 1 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。
- 2 輸入閒置逾時 (以秒為單位)。

您必須重新啟動 SSH 服務和 ESXi Shell 服務，逾時才能生效。

- 3 按 Enter 並按 Esc，直到返回到 Direct Console 使用者介面的主功能表。

結果

如果該工作階段閒置，使用者將在逾時期限過後登出。

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。

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

若要最有效地保護您的環境，請注意 Auto Deploy 與主機設定檔搭配使用時可能存在的安全性風險。

網路安全性

保護您的網路，就像其他任何 PXE 式部署方式一樣。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。

藉由完全隔離使用 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 規則設定為使用主機設定檔或主機自訂設定佈建主機，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 Service 來設定 Active Directory，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。

管理 ESXi 記錄檔

記錄檔為對攻擊進行疑難排解和取得有關主機安全性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。

採取下列措施來提高主機的安全性。

- 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。當啟用持續性記錄時，您會有用於主機的專用伺服器活動記錄。

- 遠端記錄到中央主機，可讓您將記錄檔收集到中央主機，在中央主機上您可以使用單一工具監控所有主機。您也可以執行彙總分析和記錄資料搜尋，這可能會洩露某些資訊，例如對多台主機的協調攻擊。
- 使用遠端命令列 (如 vCLI 或 PowerCLI) 或使用 API 用戶端，在 ESXi 主機上設定遠端安全 Syslog。
- 查詢 Syslog 組態，確保已設定有效的 Syslog 伺服器 (包括正確的連接埠)。

在 ESXi 主機上設定 Syslog

所有 ESXi 主機均執行 Syslog 服務 (vmsyslogd)，該服務會將來自 VMkernel 和其他系統元件的訊息記錄到記錄檔中。

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

如需有關使用 vCLI 命令的詳細資訊，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**管理索引**標籤。
- 3 在 [系統] 面板中，按一下**進階系統設定**。
- 4 尋找 [進階系統設定] 清單中的 **Syslog** 區段。
- 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] 圖示。

選項	說明
Syslog.global.defaultRotate	設定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	設定系統輪替記錄前的記錄預設大小 (KB)。可全域設定該數目，也可針對個別子記錄器進行設定。
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 <code>/scratch</code> 目錄在重新開機後仍會存在。目錄應指定為 <code>[datastorename] path_to_file</code> ，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 <code>[storage1] /systemlogs</code> 會對應到路徑 <code>/vmfs/volumes/storage1/systemlogs</code> 。
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 <code>ssl://hostName1:1514</code> 。支援 UDP (預設)、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 按一下要自訂的記錄的名稱。
 - b 按一下 [編輯] 圖示，然後輸入所需的輪替次數和記錄大小。
- 7 按一下**確定**。

結果

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/vmwarning.log	記錄與虛擬機器有關的活動。
VMkernel 摘要	/var/log/vmksmmary.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。
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

當啟用 Fault Tolerance (FT) 時，VMware vLockstep 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。此流量可以包含敏感資料，如純文字格式的密碼。若要避免此類資料的泄漏，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

6

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
- 驗證舊版 ESXi 主機的指紋
- 確認已對網路檔案複製啟用 SSL 憑證驗證
- vCenter Server TCP 和 UDP 連接埠
- 控制以 CIM 為基礎的硬體監控工具存取

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 的完整管理權限，請移除這些存取權限並將這些權限授與一或多個具名 vCenter Server 管理員帳戶。僅可將完整管理權限授與需要該權限的管理員。請勿將該權限授與其成員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。不建議使用本機作業系統使用者。

- 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。

最小化存取權

避免允許使用者直接登入 vCenter Server 主機。已登入 vCenter Server 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。

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。

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。此外，某些權限僅在安裝和升級時需要。在安裝或升級產品之後，可以移除這些權限。

限制資料存放區瀏覽器存取權

資料存放區瀏覽器功能可讓具有適當權限的使用者透過網頁瀏覽器或 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。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。

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](#)。

驗證 vpxuser 的密碼原則

依預設，vCenter Server 每 30 天自動變更一次 vpxuser 密碼。確保此設定符合您的原則，或設定原則以符合您公司的密碼使用期限原則。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。如果在根資料夾上指派了管理員角色的使用者或使用者群組無法在重新啟動期間被驗證為有效的使用者或群組，則角色會從該使用者或群組中移除。在其位置上，vCenter Server 會將管理員角色授與 vCenter Single Sign-On 帳戶 administrator@vsphere.local。然後，此帳戶即可充當管理員。

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 administrator@vsphere.local 帳戶。

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 在 vSphere Web Client 物件階層中，選取 vCenter Server。
- 2 按一下**管理索引標籤**和**設定子索引標籤**。
- 3 按一下**進階設定**，然後在篩選器方塊中輸入 **VimPasswordExpirationInDays**。
- 4 設定 **VirtualCenter.VimPasswordExpirationInDays** 以符合您的需求。

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。

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。

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。

考慮限制 Linux 用戶端的使用

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。

即使您已將 vCenter Server 系統和 ESXi 主機上的 VMCA 簽署憑證取代為由第三方 CA 簽署的憑證，但與 Linux 用戶端的某些通訊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。

檢查已安裝的外掛程式

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，該架構可用於透過功能表選取項目或工具列圖示 (可用於存取 vCenter 附加元件或外部以 Web 為基礎的功能) 延伸 vSphere Web Client。此彈性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，可以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。

必要條件

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**系統管理**，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環境的安全。

設定 NTP

確保所有系統使用相同的相對時間來源 (包括相關的當地語系化偏移)，並且相對時間來源可與商定的時間標準相關聯 (如國際標準時間-UTC)。同步的系統對於憑證有效性來說至關重要。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

僅限制對這些與 vCenter Server Appliance 進行通訊所需的基礎元件的存取。封鎖來自不必要系統的存取可降低對作業系統發動一般攻擊的潛在可能性。僅限制對這些基礎元件的存取即可將風險降到最低。

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 選取**管理**索引標籤，然後依序按一下**設定**和**一般**。
- 3 按一下**編輯**。
- 4 按一下 **SSL 設定**。
- 5 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。
- 6 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。
- 7 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 選取**設定**索引標籤，然後按一下**進階設定**。
- 3 按一下**編輯**。
- 4 在對話方塊的底部，輸入以下金鑰和值。

欄位	值
索引鍵	config.nfc.useSSL
值	true

- 5 按一下**確定**。

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。

下面的資料表列出了 TCP 和 UDP 連接埠，以及每個連接埠的用途和類型。在安裝時預設為開啟的連接埠由 (預設值) 進行指示。如需不同版本 vSphere 的所有 vSphere 元件的最新連接埠清單，請參閱 [VMware 知識庫文章 1012382](#)。

表 6-1. vCenter Server TCP 和 UDP 連接埠

連接埠	用途
80 (預設值)	HTTP 存取 vCenter Server 需要使用連接埠 80 進行直接 HTTP 連線。連接埠 80 將要求重新導向到 HTTPS 連接埠 443。如果不小心使用 http://server 而非 https://server，則此重新導向將非常有用 WS 管理 (也需要開啟連接埠 443)
88, 2013	Kerberos 的控制介面 RPC，由 vCenter Single Sign-On 使用。
123	NTP 用戶端
135 (預設值)	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 (預設)	SNMP 伺服器。此為 ESXi 主機和 vCenter Server Appliance 上的預設連接埠。
389	vCenter Single Sign-On LDAP (6.0 及更新版本)
636	vCenter Single Sign-On LDAPS (6.0 及更新版本)
443 (預設)	vCenter Server 系統使用連接埠 443 來監控從 SDK 用戶端傳輸的資料。 此連接埠也用於下列服務： <ul style="list-style-type: none"> ■ 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
2012	VMware Directory Service (vmdir) 的 RPC 連接埠。
2014	VMware Certificate Authority (VMCA) 服務的 RPC 連接埠。
2020	VMware Authentication Framework 服務 (vmafd) 的 RPC 連接埠。
31031、44046 (預設值)	vSphere Replication
7444	vCenter Single Sign-On HTTPS。
8093	用戶端整合外掛程式會使用本機回送主機名稱，並使用連接埠 8093 和範圍在 50100 到 60099 之間的隨機連接埠。用戶端整合外掛程式會僅使用連接埠 8093 進行本機通訊。該連接埠可能會受到防火牆的持續封鎖。
8109	VMware Syslog Collector。
9443	vSphere Web Client 對 ESXi 主機的 HTTP 存取。
10080	Inventory Service。

表 6-1. vCenter Server TCP 和 UDP 連接埠 (續)

連接埠	用途
11711	vCenter Single Sign-On LDAP (從 vSphere 5.5 升級的環境)
11712	vCenter Single Sign-On LDAPS (從 vSphere 5.5 升級的環境)
12721	VMware Identity Management Service。
15005	ESX Agent Manager (EAM)。ESX Agent 可以是虛擬機器或選用的 VIB。該代理程式可延伸 ESXi 主機的功能，以提供 vSphere 解決方案 (如 NSX-v 或 vRealize Automation) 所需的其他服務。
15007	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。
50100-60099	用戶端整合外掛程式會使用本機回送主機名稱，並使用連接埠 8093 和範圍在 50100 到 60099 之間的隨機連接埠。用戶端整合外掛程式僅會使用此範圍內的連接埠進行本機通訊。該連接埠可能會受到防火牆的持續封鎖。

除了這些連接埠之外，您可以根據需要設定其他連接埠。

控制以 CIM 為基礎的硬體監控工具存取

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，請僅為這些應用程式提供必需的最小存取權限。如果某個應用程式已佈建有根或完整管理員帳戶，且該應用程式受到影響，則整個虛擬環境就可能會受到影響。

CIM 是一種開放式標準，其所定義的架構用於 ESXi 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 提供者用作機制，提供對裝置驅動程式和基礎硬體的管理存取權限。硬體廠商 (包括伺服器製造商和特定硬體裝置廠商) 可寫入提供者，從而對其特定裝置進行監控和管理。VMware 也可以寫入一些提供者，用於實作監控伺服器硬體、ESXi 儲存區基礎結構和虛擬化專屬資源。這些提供者在 ESXi 系統內執行，因此設計為極其輕量且側重於特定管理工作。CIM Broker 從所有 CIM 提供者獲得資訊，並透過標準 API (最常見的一個是 WS-MAN) 呈現給外界。

請勿為遠端應用程式提供存取 CIM 介面的根認證。而是應該建立這些應用程式專屬的服務帳戶，並為 ESXi 系統上定義的所有本機帳戶以及 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 建立專屬於 CIM 應用程式的服務帳戶。
- 2 為在 ESXi 系統中定義的所有本機帳戶以及在 vCenter Server 中定義的所有角色授與對 CIM 資訊的唯讀存取權限。
- 3 (選擇性) 如果應用程式需要對 CIM 介面的寫入權限，請建立一個要套用於服務帳戶的角色，使其僅擁有以下兩項權限：
 - 主機.組態.系統管理
 - 主機.CIM.CIM 互動

視監控應用程式的工作方式而定，該角色可以是主機的本機角色，也可以在 vCenter Server 中集中定義。

結果

使用者使用您為 CIM 應用程式建立的服務帳戶登入主機時，該使用者僅擁有**系統管理**和 **CIM 互動**權限，或唯讀存取權限。

確保虛擬機器安全

7

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。請像保護實體電腦一樣確保虛擬機器的安全。

本章節討論下列主題：

- 限制資訊訊息從虛擬機器流向 VMX 檔案
- 防止虛擬磁碟壓縮
- 虛擬機器安全性最佳做法

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 VMX 的資訊量超過資料存放區的容量，則會造成拒絕服務。

依預設，包含資訊名稱值配對的組態檔將限制為 1 MB。此容量在大多數情況下是足夠的，但是在必要時可以變更此值。例如，如果組態檔中儲存的自訂資訊過多，可以增加該限制。

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的容量，則可能會造成拒絕服務。

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 在 vSphere Web Client 詳細目錄中尋找虛擬機器。
 - a 選取資料中心、資料夾、叢集、資源集區或主機。
 - b 按一下**相關物件索引標籤**，然後按一下**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。

必要條件

- 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 在 vSphere Web Client 詳細目錄中尋找虛擬機器。
 - a 選取資料中心、資料夾、叢集、資源集區或主機。
 - b 按一下**相關物件**索引標籤，然後按一下**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 新增或編輯下列參數。

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

- 6 按一下**確定**。

結果

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

虛擬機器中執行的任何服務都有可能引發攻擊。透過停用不必要的系統元件 (即，不是支援系統上執行的應用程式或服務所必需的)，可減少會受到攻擊的元件數目。

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。

後續步驟

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，如有必要，連線越少越好。

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，您可以根據完成一般工作所需的並行連線數目來增加限制。

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。

後續步驟

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

虛擬機器中執行的任何服務都有可能引發攻擊。透過停用不必要的系統元件 (即，不是支援系統上執行的應用程式或服務所必需的)，可減少會受到攻擊的元件數目。

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 HGFS (主機客體檔案系統)。
- ◆ 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。虛擬機器上不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禦攻擊。

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，並存取遺留在磁碟機中媒體上的敏感資訊，或者中斷連線網路介面卡，將虛擬機器與其網路隔離，從而導致拒絕服務。

- 確保不與未經授權的裝置連線，並移除所有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。
- 確保不會將任何非必要的裝置連線到虛擬機器。序列埠和平行埠很少在資料中心中用於虛擬機器，而 CD/DVD 光碟機通常僅在軟體安裝期間暫時連線。

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 檢查每個硬體裝置，並確保您希望其保持連線狀態。

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 在 vSphere Web Client 詳細目錄中尋找虛擬機器。
 - a 選取資料中心、資料夾、叢集、資源集區或主機。
 - b 按一下**相關物件索引標籤**，然後按一下**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 如果適當，請根據需要新增或編輯下列參數來加以設定。

選項	描述
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 系統與主控虛擬化平台 (例如 Workstation 和 Fusion) 上都能運作。在 vSphere 系統上執行虛擬機器時，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。

必要條件

關閉虛擬機器。

程序

- 1 在 vSphere Web Client 詳細目錄中尋找虛擬機器。
 - a 選取資料中心、資料夾、叢集、資源集區或主機。
 - b 按一下**相關物件索引標籤**，然後按一下**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 HGFS 檔案傳輸

某些作業 (例如，自動化工具升級) 使用 Hypervisor 中名為主機客體檔案系統 (HGFS) 的元件。在高安全性環境中，您可以停用此元件，以最大程度地降低攻擊者使用 HGFS 在客體作業系統內傳輸檔案的風險。

程序

- 1 在 vSphere Web Client 詳細目錄中尋找虛擬機器。
 - a 選取資料中心、資料夾、叢集、資源集區或主機。
 - b 按一下**相關物件索引標籤**，然後按一下**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。

結果

進行此項變更時，VMX 程序不會再回應來自工具程序的命令。使用 HGFS 將檔案傳入和傳出客體作業系統的 API (例如某些 VIX 命令或 VMware Tools 自動升級公用程式) 將無法正常運作。

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。

必要條件

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。主控台視窗獲得焦點時，虛擬機器中執行的無權限使用者和程序均可以存取虛擬機器主控台的剪貼簿。如果使用者在使用主控台前將敏感資訊複製到剪貼簿中，就可能在無意中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。

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。若要避免授與使用者完整管理員存取權限，請建立可停用客體存取的自訂角色，並將該角色套用於需要管理員權限，但是無權與客體作業系統內的檔案和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。使用 vMotion 和 Storage vMotion 進行移轉等工作會要求 IT 角色有權存取該虛擬機器。在此案例中，停用客體作業系統內的部分遠端作業，以確保該 IT 角色無法存取敏感資訊。

必要條件

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**。

後續步驟

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。從預設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使用者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。如果不想永久移除裝置，您可以阻止虛擬機器使用者或程序在客體作業系統中與裝置連線或中斷連線。

必要條件

關閉虛擬機器。

程序

- 1 在 vSphere Web Client 詳細目錄中尋找虛擬機器。
 - a 選取資料中心、資料夾、叢集、資源集區或主機。
 - b 按一下**相關物件索引標籤**，然後按一下**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**。

修改客體作業系統的可變記憶體限制

如果組態檔中儲存的自訂資訊較多，則可以增加客體作業系統的可變記憶體限制。

必要條件

關閉虛擬機器。

程序

- 1 在 vSphere Web Client 詳細目錄中尋找虛擬機器。
 - a 選取資料中心、資料夾、叢集、資源集區或主機。
 - b 按一下**相關物件**索引標籤，然後按一下**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 > 進階**，然後按一下**編輯組態**。
- 4 新增或編輯參數 `tools.setInfo.sizeLimit`，並將值設定為位元組數。
- 5 按一下**確定**。

阻止客體作業系統程序向主機傳送組態訊息

您可以阻止客體將任何名稱值配對寫入到組態檔中。這在必須防止客體作業系統的組態設定遭修改的情況下，是適當的。

必要條件

關閉虛擬機器。

程序

- 1 在 vSphere Web Client 詳細目錄中尋找虛擬機器。
 - a 選取資料中心、資料夾、叢集、資源集區或主機。
 - b 按一下**相關物件**索引標籤，然後按一下**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。
 - 在 [名稱] 欄中：`isolation.tools.setinfo.disable`
 - 在 [值] 欄中：`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

結果

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。

確保 vSphere 網路安全

8

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
- 使用防火牆確保網路安全
- 確保實體交換器安全
- 使用安全性原則確保標準交換器連接埠安全
- 保護 vSphere Standard Switch 的安全
- 保護 vSphere Distributed Switch 和分散式連接埠群組安全
- 透過 VLAN 保護虛擬機器的安全
- 在單一 ESXi 主機上建立網路 DMZ
- 在單一 ESXi 主機內建立多個網路
- 網際網路通訊協定安全性
- 確保 SNMP 組態正確
- 僅在需要時透過 vSphere Network Appliance API 使用虛擬交換器
- vSphere 網路安全性最佳做法

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。

由於以主機為基礎的防火牆會降低效能，因此請先根據效能目標平衡安全性需求，然後再決定是否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，可以大大降低虛擬機器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，即攻擊者操縱 ARP 資料表重新對應 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。

仔細規劃分割可降低虛擬機器區域間傳輸封包的幾率，從而防止嗅探攻擊 (此類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。每種方法具有不同的優點。

- 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，並且更不容易在建立初始區段之後出現錯誤組態。
- 設定虛擬區域網路 (VLAN)，協助保護網路。VLAN 幾乎能夠提供實體實作單獨網路所具有的所有安全性優點，且不增加硬體額外開支，可為您節省部署和維護其他裝置、纜線等硬體的コスト，是一種可行的解決方案。請參閱[透過 VLAN 保護虛擬機器的安全](#)。

防止未經授權的存取

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。即使虛擬機器網路已與任何實體網路隔離，虛擬機器也可能遭到網路中其他虛擬機器的攻擊。用於確保虛擬機器安全的需求通常與確保實體機器安全的需求相同。

虛擬機器是相互獨立的。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，因此可能需要透過外部方法加強保護。

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 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。該防火牆可為網路提供基本保護。

防火牆可能位於用戶端和 vCenter Server 之間。或者，根據您的部署情況，vCenter Server 和用戶端可能均受防火牆保護。重點是確保在您認為的系統進入點處存在防火牆。

如需 TCP 和 UDP 連接埠的完整清單 (包括用於 vSphere vMotion™ 和 vSphere Fault Tolerance 的連接埠)，請參閱 [vCenter Server TCP 和 UDP 連接埠](#)。

設定了 vCenter Server 的網路可以透過 vSphere Web Client 或第三方網路管理用戶端接收通訊，這些用戶端使用 SDK 與主機相連。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。

根據您計劃如何使用網路以及各種裝置所需的安全性層級，您可能還需要在網路中的許多其他存取點處建立防火牆。根據為網路組態辨別的安全性風險，選取防火牆位置。下列是 ESXi 實作中常用防火牆位置的清單。

- 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。

如果在 ESXi 主機間新增防火牆，並打算在伺服器間移轉虛擬機器、執行複製操作或使用 vMotion，您還必須在用來將來源主機和目標主機分隔開的防火牆中開啟連接埠，以便來源主機與目標主機進行通訊。

- 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，您可以根據網路規格進行設定。

透過防火牆連線到 vCenter Server

vCenter Server 使用 TCP 連接埠 443 來接聽從其用戶端傳輸的資料。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。

在防火牆中開啟 TCP 連接埠 443，讓 vCenter Server 能夠從 vSphere Web Client 接收資料。防火牆組態取決於您的網站所使用的內容，請連絡當地的防火牆系統管理員以取得相關資訊。

如果您不希望使用連接埠 443 做為 vSphere Web Client 與 vCenter Server 通訊使用的連接埠，您可以從 vSphere Web Client 變更 vCenter Server 設定，以切換到另一個連接埠。請參閱《vCenter Server 和主機管理》說明文件。

如果您仍然使用 vSphere Client，請參閱《使用 vSphere Client 進行 vSphere 管理》說明文件。

針對沒有 vCenter Server 的組態設定防火牆

可以將用戶端直接連線到 ESXi 網路，而不使用 vCenter Server。

如果未設定 vCenter Server，網路會透過 vSphere Client、任一 vSphere 命令列介面、vSphere Web Services SDK 或第三方用戶端來接收通訊。在多數情況下，防火牆需求與設定有 vCenter Server 的情況基本相同，但存在幾個重要差異。

- 與包含 vCenter Server 的組態一樣，應確保有防火牆來保護 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伺服器上，因此無需單獨的授權伺服器。這就消除了授權伺服器與 ESXi 網路間設定防火牆的需要。

您可以透過 ESXCLI、vSphere Client 或防火牆規則來設定防火牆連接埠。請參閱 [ESXi 防火牆組態](#)。

透過防火牆連線 ESXi 主機

如果在兩台 ESXi 主機間有防火牆，並想要允許主機間的交易或使用 vCenter Server 執行任何來源或目標活動，例如 vSphere High Availability (vSphere HA) 流量、移轉、複製或 vMotion，則必須設定一個可供受管理主機接收資料的連線。

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](#)。有關設定連接埠的其他資訊，請洽詢防火牆系統管理員。

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 vSphere 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。

透過 vSphere Client 直接連線到 ESXi 主機

如果直接連線到 ESXi 主機，則可以使用 vSphere Client 虛擬機器主控台。

備註 請勿使用 vSphere Client 直接連線到由 vCenter Server 系統管理的主機。如果您透過 vSphere 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

vSphere 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

對於實體網路介面卡，虛擬機器網路介面卡可以傳送可能來自不同電腦的畫面，或者模擬另一台電腦，從而接收針對該電腦的網路畫面。同樣，與實體網路介面卡相同，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。這兩種案例都具有一定的安全性風險。

為網路建立標準交換器時，會在 vSphere Web Client 中新增連接埠群組，為連結到該交換器上的虛擬機器和 VMkernel 介面卡強制執行系統流量原則。

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的過程中，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。實作此安全性功能的目的是在於負責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。為了正確使用安全性設定檔中的設定，必須瞭解虛擬機器網路介面卡如何控制傳輸及此層級的攻擊如何進行。請參閱《vSphere 網路》文件中的「安全性原則」一節。

保護 vSphere Standard Switch 的安全

使用交換器的安全性設定，您可以透過限制一些 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。這意味著，作業系統可透過模擬接收網路授權的網路介面卡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：

- 混合模式 (請參閱[混合模式作業](#))
- MAC 位址變更 (請參閱[MAC 位址變更](#))
- 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。

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)。

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，確認已停用自動展開功能。

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。如果未完整追蹤 VLAN 識別碼，錯誤地重複使用識別碼可能會允許不適當的實體和虛擬機器之間的流量。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。

ESXi 主機相關聯的 vSphere Distributed Switch 需要交換器名稱所對應的欄位。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，您可以將交換器標記為內部以指示其僅適用於虛擬機器之私人虛擬交換器之間的內部網路，且未繫結任何實體網路介面卡。

- 6 如果未使用 Network Healthcheck，請針對 vSphere Distributed Switch 將其停用。

Network Healthcheck 預設為停用。啟用後，Healthcheck 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 Network Healthcheck 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：

- 混合模式 (請參閱[混合模式作業](#))
- MAC 位址變更 (請參閱[MAC 位址變更](#))
- 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。

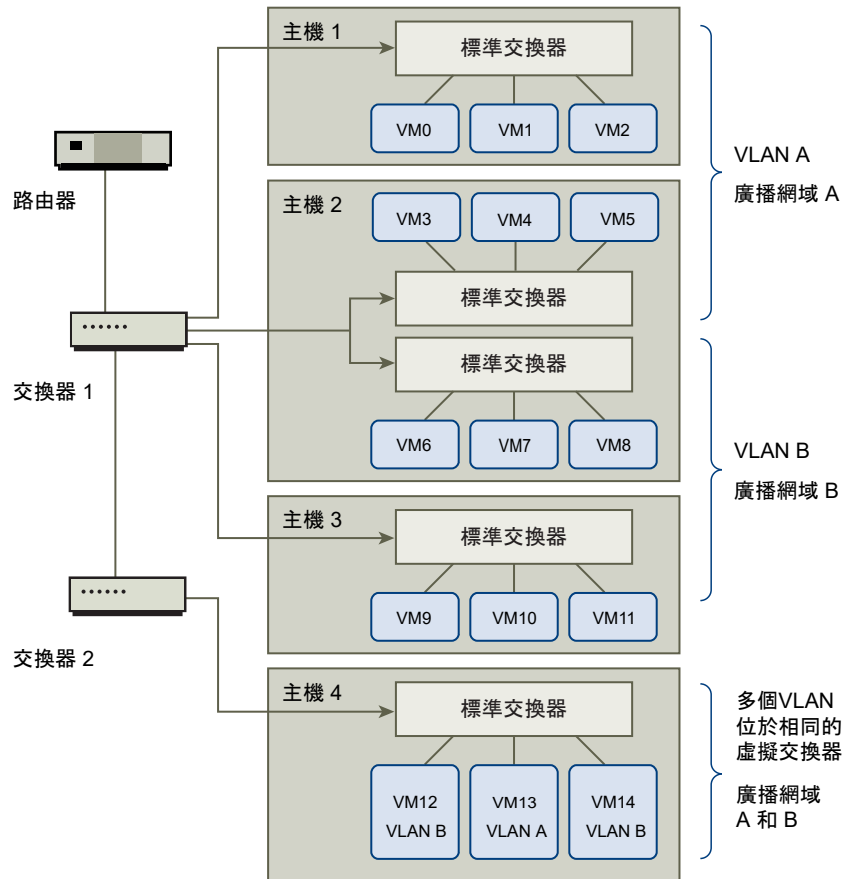
透過 VLAN 保護虛擬機器的安全

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 8-1. 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。

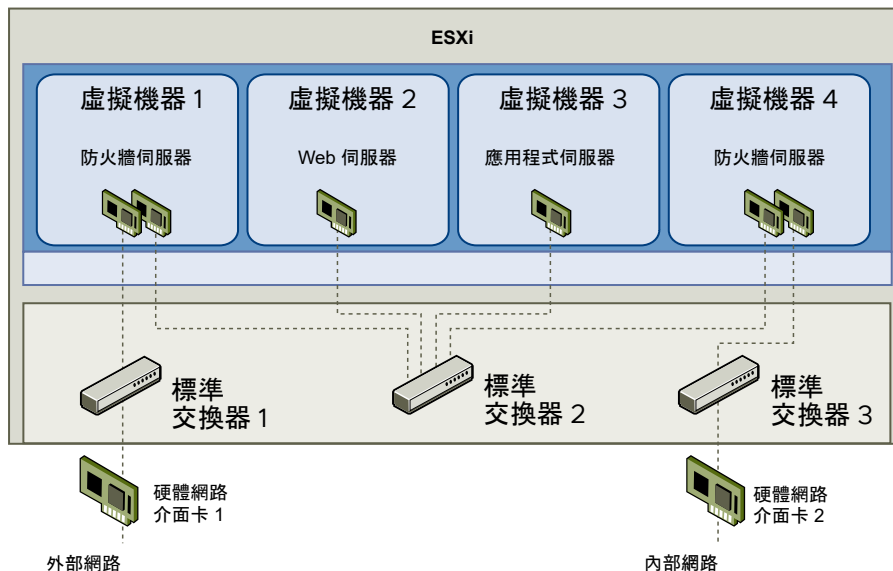
在標準交換器上，您可以在交換器或連接埠群組層級上設定 VLAN 網路模式，而在分散式交換器上，您可以在分散式連接埠群組或連接埠層級上設定。

- 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 主機上建立網路 DMZ

在單一主機上建立網路非軍事區域 (DMZ) 是使用 ESXi 隔離和虛擬網路功能設定安全環境的一個範例。

圖 8-2. 在單一 ESXi 主機上設定的 DMZ



在此範例中，將四個虛擬機器設定為在標準交換器 2 上建立虛擬 DMZ：

- 虛擬機器 1 和虛擬機器 4 執行防火牆，並透過標準交換器連線到實體網路介面卡。這兩個虛擬機器均使用多個交換器。

- 虛擬機器 2 執行 Web 伺服器，同時虛擬機器 3 做為應用程式伺服器執行。這兩個虛擬機器均連線到一個虛擬交換器。

Web 伺服器和應用程式伺服器佔用兩個防火牆之間的 DMZ。這些元素之間的媒介是用來連線防火牆和伺服器的標準交換器 2。此交換器未與 DMZ 之外的任何元素進行直接連線，且透過兩個防火牆與外部流量相隔離。

從運作角度來看，外部流量透過硬體網路介面卡 1 (由標準交換器 1 路由) 從網際網路進入虛擬機器 1，並由此虛擬機器上安裝的防火牆進行驗證。如果經防火牆授權，流量可路由到 DMZ 中的標準交換器，即標準交換器 2。由於 Web 伺服器和應用程式伺服器也連線到此交換器，因此，它們可以滿足外部要求。

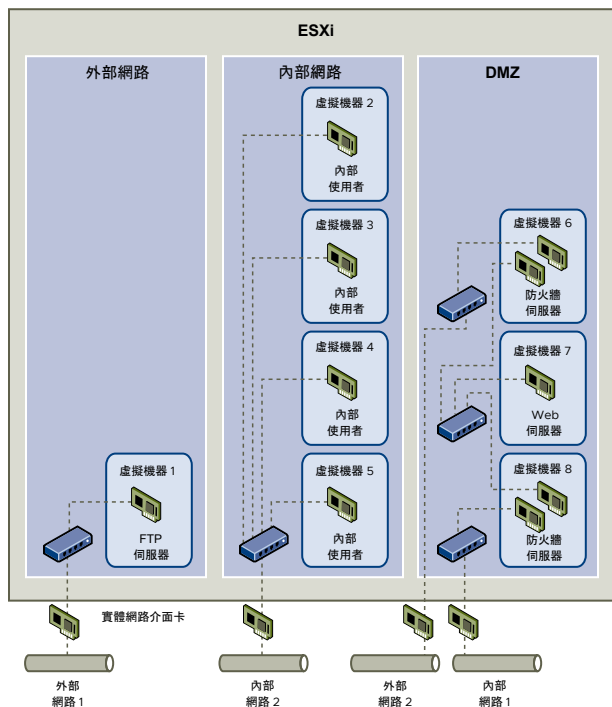
標準交換器 2 還與虛擬機器 4 相連線。此虛擬機器在 DMZ 和內部公司網路之間提供防火牆。此防火牆對來自 Web 伺服器和應用程式伺服器的封包進行篩選。驗證後的封包將透過標準交換器 3 路由到硬體網路介面卡 2。硬體網路介面卡 2 與內部公司網路相連線。

在單一主機上建立 DMZ 時，可使用相當輕量的防火牆。雖然此組態中的虛擬機器無法直接控制其他虛擬機器或存取其記憶體，但是所有虛擬機器仍然透過虛擬網路處於連線狀態。此網路可能會傳播病毒，或成為其他類型攻擊的對象。DMZ 中虛擬機器的安全性等同於連線到同一網路的獨立實體機器。

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 8-3. 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結點。

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`。

結果

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
<code>--sa-source= 來源位址</code>	必要。指定來源位址。
<code>--sa-destination= 目的地位址</code>	必要。指定目的地位址。
<code>--sa-mode= 模式</code>	必要。指定模式 <code>transport</code> 或 <code>tunnel</code> 。

選項	說明
<code>--sa-spi=</code> 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。
<code>--encryption-algorithm=</code> 加密演算法	必要。使用以下其中一個參數指定加密演算法。 <ul style="list-style-type: none"> ■ 3des-cbc ■ aes128-cbc ■ null (表示不提供任何加密)
<code>--encryption-key=</code> 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。
<code>--integrity-algorithm=</code> 驗證演算法	必要。指定驗證演算法 <code>hmac-sha1</code> 或 <code>hmac-sha2-256</code> 。
<code>--integrity-key=</code> 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。
<code>--sa-name=</code> 名稱	必要。提供安全性關聯名稱。

範例：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 0x6970763672656164796c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sal
```

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。

必要條件

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`

結果

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。

必要條件

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
<code>--sp-source= 來源位址</code>	必要。指定來源 IP 位址和首碼長度。
<code>--sp-destination= 目的地位址</code>	必要。指定目的地位址和首碼長度。
<code>--source-port= 連接埠</code>	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。
<code>--destination-port= 連接埠</code>	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。
<code>--upper-layer-protocol= 通訊協定</code>	使用下列參數之一指定上層通訊協定。 <ul style="list-style-type: none"> ■ tcp ■ udp ■ icmp6 ■ 任何
<code>--flow-direction= 方向</code>	使用 in 或 out 指定要監控流量的方向。
<code>--action= 動作</code>	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。 <ul style="list-style-type: none"> ■ 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。
<code>--sp-mode= 模式</code>	指定模式 tunnel 或 transport。
<code>--sa-name= 安全性關聯名稱</code>	必要。為要使用的安全性原則提供安全性關聯名稱。
<code>--sp-name= 名稱</code>	必要。請為安全性原則提供名稱。

範例：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=sal
--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。

必要條件

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。

程序

- 1 執行 `esxcli system snmp get` 來判定目前是否已使用 SNMP。
- 2 如果您的系統確實需要 SNMP，請透過執行 `esxcli system snmp set --enable true` 命令確保其正在執行。
- 3 如果您的系統使用 SNMP，請參閱《監控和效能》出版品獲取 SNMP 3 的設定資訊。
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。

僅在需要時透過 vSphere Network Appliance API 使用虛擬交換器

如果您未使用使用了 vSphere Network Appliance API (DvFilter) 的產品，請勿將主機設定為向虛擬機器傳送網路資訊。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 若要確保 `Net.DVFilterBindIpAddress` 核心參數的值正確，請使用 vSphere Web Client 找到該參數。
 - a 選取主機，然後按一下**管理索引標籤**。
 - b 在 [系統] 下，選取**進階系統設定**。
 - c 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] 欄位中輸入 **DVFilter**，以顯示所有相關的參數。
- 2 如果未使用 DvFilter 設定，請確保值為空。
- 3 如果使用 DvFilter 設定，請確保該參數的值與使用 DvFilter 的產品所使用的值相符。

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，如果停用跨距樹狀目錄以避免在實體交換器網路內迴圈，則連線到 ESXi 主機的實體交換器連接埠必須已設定 Portfast。如果 Portfast 未設定，則可能會出現潛在的效能和連線問題。
- 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，從而增加了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，虛擬機器管理員應只有權存取其虛擬機器所在的連接埠群組。網路管理員應具有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。啟用後，覆寫允許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。

採用音效網路隔離做法

採用音效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 主機或叢集上執行之最安全的虛擬機器的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 vSwitch 上的專用 VLAN 中。只要生產虛擬機器未使用 vSphere 管理連接埠群組的 VLAN，vSwitch 就能與生產 (虛擬機器) 流量共用。檢查網路區段是否未進行路由 (可能路由至包含其他管理相關項目的網路除外)，例如與 vSphere Replication 一起使用。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，以嚴格控制的方式啟用管理功能的存取權。

- 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，要求管理員透過 VPN 連線到管理網路，並且只允許受信任的管理員進行存取。
- 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；任何具有此網路存取權的人員都可以進行檢視。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。

VMotion 連結埠群組應位於常用 vSwitch 上的專用 VLAN 中。只要生產虛擬機器未使用 VMotion 連接埠群組的 VLAN，vSwitch 就能與生產 (虛擬機器) 流量共用。

有關多個 vSphere 元件的最佳做法

9

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 5 章 保護 ESXi 主機和第 7 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

確保 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，則在網路機器相互通訊時，可能會將對時間敏感的 SSL 憑證視為無效。

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。

請確定 vCenter 元件執行所在的任何 Windows 主機電腦均已與 NTP 伺服器同步。請參閱知識庫文章，網址為 <http://kb.vmware.com/kb/1318>。

- 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 vSphere 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 vSphere Client，然後連線至 ESXi 主機。
- 2 在**組態**索引標籤上，按一下**時間組態**。
- 3 按一下**內容**，然後按一下**選項**。
- 4 選取 **NTP 設定**。
- 5 按一下**新增**。
- 6 在 [新增 NTP 伺服器] 對話方塊，輸入要與之同步的 NTP 伺服器的 IP 位址或完整網域名稱。
- 7 按一下**確定**。

主機時間即會與 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。

結果

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。

後續步驟

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。

必要條件

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 Virtual SAN》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，可採取幾種措施將安全性風險降到最低。

iSCSI 是一種使用 TCP/IP 協議透過網路連接埠 (而非透過直接連線到 SCSI 裝置) 來存取 SCSI 裝置和交換資料記錄的方法。在 iSCSI 交易中，原始 SCSI 資料區塊被封裝在 iSCSI 記錄中並傳輸到要求資料的裝置或使用者。

iSCSI SAN 可讓您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 可為依賴一般儲存區集區服務多個使用者的環境提供經濟的儲存解決方案。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，與可用於主機的 iSCSI 硬體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

確保 iSCSI 裝置免遭不利入侵的一種方法就是，每當主機嘗試存取目標 LUN 上的資料時，都要求 iSCSI 裝置 (或目標) 對主機 (或啟動器) 進行驗證。

驗證的目的是證明啟動器具有存取目標的權限，這是在您設定驗證時授與的權限。

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 Storage》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。每台主機的相互驗證密碼應有所不同；如果可能，每個用戶端向伺服器進行驗證的密碼也應有所不同。這樣可確保若單一主機受到危害，攻擊者無法建立其他任意主機以及驗證儲存裝置。使用單一共用密碼，一台主機受危害會使得攻擊者能夠驗證儲存裝置。

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 遮罩來分隔 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 Storage》說明文件。

針對 NFS 4.1 使用 Kerberos 認證

藉由 NFS 4.1 版，ESXi 支援 Kerberos 驗證機制。

Kerberos 是一種驗證服務，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 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 vSphere 實作僅支援為用戶端和伺服器識別驗證，但不提供資料完整性或機密性服務。

當您使用 Kerberos 驗證時，需考量下列事項：

- ESXi 會對 Active Directory 網域和金鑰發佈中心 (KDC) 使用 Kerberos 第 5 版。
- 做為 vSphere 管理員，您可指定 Active Directory 認證，為 NFS 使用者提供對 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 主機共用同一個 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。透過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，即可自動化此作業。
- NFS 4.1 不支援同時掛接 AUTH_SYS 與 Kerberos。
- 使用 Kerberos 的 NFS 4.1 不支援 IPv6。僅支援 IPv4。

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，已停用向客體虛擬機器傳送主機效能資料的功能。此預設設定將阻止虛擬機器取得有關實體主機的詳細資訊，並且在虛擬機器安全性遭到破壞時，使主機資料不可用。

備註 下列步驟說明了基本程序。改用 vSphere 或其中一個 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的儲存裝置的名稱。

- 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。

結果

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，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 重新設定公用程式管理 TLS 通訊協定組態

10

您可以使用 TLS 重新設定公用程式啟用或停用 TLS 通訊協定版本。您可以在 vSphere 環境中停用 TLS 1.0，或者您可以同時停用 TLS 1.0 和 TLS 1.1。從 vSphere 6.5 開始，TLS 通訊協定版本 1.0、1.1 以及 1.2 依預設會啟用。

如需重新設定，環境中的 vCenter Server、Platform Services Controller、vSphere Update Manager 和 ESXi 主機必須執行允許停用的軟體版本。請參閱 VMware 知識庫文章 [2145796](#)，以取得支援停用 TLS 1.0 的 VMware 產品清單。

停用 TLS 1.0 前，您也必須確保其他 VMware 產品和第三方產品支援啟用的 TLS 通訊協定。視您的組態而定，這可以是 TLS 1.2 或同時是 TLS 1.1 和 TLS 1.2。

本章節討論下列主題：

- [支援停用 TLS 版本的連接埠](#)
- [停用 vSphere 中的 TLS 版本](#)
- [安裝 TLS 組態公用程式](#)
- [執行選擇性手動備份](#)
- [停用 vCenter Server 系統上的 TLS 版本](#)
- [停用 ESXi 主機上的 TLS 版本](#)
- [在 Platform Services Controller 系統上停用 TLS 版本](#)
- [還原 TLS 組態變更](#)
- [在 vSphere Update Manager 上停用 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 10-1. 受 TLS Configurator 公用程式影響的 vCenter Server 和 Platform Services Controller

服務	在 Windows 上的名稱	在 Linux 上的名稱	連接埠
VMware HTTP Reverse Proxy	rhttpproxy	vmware-rhttpproxy	443
VMware Directory Service	VMwareDirectoryService	vmldird	636
VMware Syslog Collector (*)	vmwaresyslogcollector (*)	rsyslogd	1514
vSphere Auto Deploy Waiter	vmware-autodeploy-waiter	vmware-rbd-watchdog	6501 6502
VMware Secure Token Service	VMwareSTS	vmware-stsd	7444
vSphere Update Manager Service (**)	vmware-ufad-vci (**)	vmware-updatemgr	8084 9087
vSphere Web Client	vspherewebclientsvc	vsphere-client	9443
VMware Directory Service	VMwareDirectoryService	vmldird	11712

(*) TLS 由這些服務的加密清單所控制。您無法進行細微管理。僅 TLS 1.2 或所有 TLS 1.x 版本受到支援。

(**) 在 vCenter Server Appliance 上，vSphere Update Manager 與 vCenter Server 位於相同的系統。在 Windows 上的 vCenter Server，您可透過編輯組態檔設定 TLS。請參閱在 [vSphere Update Manager 上停用 TLS 版本](#)。

表 10-2. 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
VMware 授權精靈	vmware-authd	902

附註和注意須知

- 請確保受 vCenter Server 管理的舊版 ESXi 主機支援啟用的 TLS 版本，無論是 TLS 1.1 和 TLS 1.2，或僅支援 TLS 1.2。當您在 vCenter Server 6.5 停用 TLS 版本時，vCenter Server 將無法再管理舊版 ESXi 5.x 主機和 6.0 主機。請將這些主機升級至支援 TLS 1.1 或 TLS 1.2 的版本。
- 您無法僅使用 TLS 1.2 與外部 Microsoft SQL Server 或外部 Oracle 資料庫連線。
- 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〉。

- 在下列情況下，您必須先重新啟動主機服務，再套用 TLS 組態變更。
 - 如果您要直接將變更套用至 ESXi 主機。
 - 如果您使用主機設定檔透過叢集組態套用變更。

停用 vSphere 中的 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 [vSphere Update Manager 上停用 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 和 Platform Services Controller 上安裝 TLS 組態公用程式。如果您的環境使用內嵌式 Platform Services Controller，您僅可以在 vCenter Server 上安裝該公用程式。
- 3 在 vCenter Server 上執行該公用程式。
- 4 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。
- 5 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。

必要條件

若要在執行 vSphere 6.0 U3 的系統上以及執行 vSphere 6.5 的系統上執行此組態，您有兩個選擇。

- 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。

安裝 TLS 組態公用程式

您可從 MyVMware.com 下載 TLS 組態公用程式並將其安裝在您的本機機器上。安裝後，您可使用兩個指令碼。一個指令碼用於設定 vCenter Server 和 Platform Services Controller，另一個用於設定 ESXi。

在 vCenter Server Appliance 上，vSphere Update Manager 連接埠會由該指令碼更新。在 vCenter Server 上，您可編輯 vSphere Update Manager 組態檔。請參閱在 [vSphere Update Manager 上停用 TLS 版本](#)。

必要條件

您需要 MyVMware 帳戶才能下載指令碼。

程序

- 1 登入您的 MyVMware 帳戶並前往 vSphere。

- 2 尋找您獲得授權的產品和產品版本，選取 VMware vCenter Server，接著按一下**前往下載**。
- 3 選取 VMware vSphere TLS Configurator 並下載以下檔案。

作業系統	檔案
Windows	VMware-vSphereTlsReconfigurator-version-build_number.x86_64.msi
Linux	VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm

- 4 上傳檔案至 vCenter Server 並安裝指令碼。

在含外部 Platform Services Controller 的環境中，您也可以將檔案上傳至 Platform Services Controller。

作業系統	程序
Windows	<ol style="list-style-type: none"> 以具有管理員權限的使用者身分登入。 複製您剛下載的 VMware-vSphereTlsReconfigurator-version-build_number.x86_64.msi 檔案。 安裝該 MSI 檔案。
Linux	<ol style="list-style-type: none"> 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。 將 VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm 檔案複製到使用 SCP 用戶端的應用裝置。 如果 Bash shell 目前尚未啟用，請執行以下命令。 <div data-bbox="681 1087 999 1138" data-label="Text"> <pre>shell.set --enabled true shell</pre> </div> 前往上傳的 rpm 檔案所在的目錄並執行以下命令。 <div data-bbox="681 1226 1324 1276" data-label="Text"> <pre>rpm -Uvh VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm</pre> </div>

結果

安裝完成後，您會在以下位置找到指令碼。

作業系統	位置
Windows	<ul style="list-style-type: none"> ■ C:\Program Files\VMware\CIS\vSphereTLSReconfigurator\VcTlsReconfigurator ■ C:\Program Files\VMware\CIS\vSphereTLSReconfigurator\EsxTlsReconfigurator
Linux	<ul style="list-style-type: none"> ■ /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator ■ /usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator

執行選擇性手動備份

TLS 組態公用程式會在每次指令碼修改 vCenter Server、Platform Services Controller 或 vSphere Update Manager 時執行備份。如果需要備份特定目錄，您可以執行手動備份。

Windows 和應用裝置的預設目錄不同。

作業系統	備份目錄
Windows	<code>c:\users\current_user\appdata\local\temp\yearmonthdayTtime</code>
Linux	<code>/tmp/yearmonthdayTtime</code>

程序

- 1 將目錄變更至 vSphereTlsReconfigurator，然後變更至 VcTlsReconfigurator 子目錄。

作業系統	命令
Windows	<code>C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\ cd VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vsphereTlsReconfigurator/ cd VcTlsReconfigurator</code>

- 2 執行以下命令以備份特定目錄。

作業系統	命令
Windows	<code>directory_path\VcTlsReconfigurator> reconfigureVc backup -d backup_directory_path</code>
Linux	<code>directory_path/VcTlsReconfigurator> ./ reconfigureVc backup -d backup_directory_path</code>

- 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=6.0.0, build=8482376
For more information, refer to the following article: https://kb.vmware.com/kb/2148819"
Log file: "C:\ProgramData\VMware\vmCenterServer\logs\vmware\vsphere-
TlsReconfigurator\VcTlsReconfigurator.log".
===== Backing up vCenter Server TLS configuration =====
Using backup directory: c:\users\admini~1\appdata\local\temp\1\20170202T054311
Backing up: vmsyslogcollector
Backing up: vspherewebclientsvc
Backing up: vmware-autodeploy-waiter
Backing up: rhttpproxy
Backing up: VMwareSTS
Backing up: VMwareDirectoryService
```

- 4 (選擇性) 如果您之後必須執行還原，您可以執行以下命令。

```
reconfigure restore -d tmp directory or custom backup directory path
```

停用 vCenter Server 系統上的 TLS 版本

您可使用 TLS 組態公用程式來停用 vCenter Server 系統上的 TLS 版本。在執行該程序過程中，您可同時啟用 TLS 1.1 和 TLS 1.2，或僅啟用 TLS 1.2。

必要條件

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 請以可執行指令碼的使用者身分登入 vCenter Server 系統，並前往指令碼所在的目錄。

作業系統	命令
------	----

Windows	<code>cd C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</code>
---------	--

Linux	<code>cd /usr/lib/vmware-vsphereTlsReconfigurator/VcTlsReconfigurator</code>
-------	--

- 2 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	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2</code>
---------	---

Linux	<code>directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2</code>
-------	---

- 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	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2</code>
---------	---

Linux	<code>directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2</code>
-------	---

- 3 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。
- 4 請在每部 ESXi 主機和各個 Platform Services Controller 上重複設定該組態。

停用 ESXi 主機上的 TLS 版本

您可使用 TLS 組態公用程式來停用 ESXi 主機上的 TLS 版本。在執行該程序過程中，您可同時啟用 TLS 1.1 和 TLS 1.2，或僅啟用 TLS 1.2。

對於 ESXi 主機，請使用與 vSphere 環境中的其他元件不同的指令碼。

備註 該指令碼會同時停用 TLS 1.0 和 TLS 1.1，除非您另行指定 `-p` 選項。

必要條件

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。

程序

- 1 請以可執行指令碼的使用者身分登入 vCenter Server 主機，並前往指令碼所在的目錄。

作業系統	命令
Windows	<code>C:\Program Files\VMware\CIS\vsphereTLSReconfigurator\EsxTlsReconfigurator</code>
Linux	<code>/usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator</code>

- 2 若要在叢集中的所有主機上停用 TLS，請執行以下命令之一。

- 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	<code>reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2</code>

- 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	<code>reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2</code>

- 3 若要在個別主機上停用 TLS，請執行以下命令之一。

- 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	<code>reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.1 TLSv1.2</code>

- 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	<code>reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.2</code>

- 4 將 ESXi 主機重新開機以完成 TLS 通訊協定變更。

在 Platform Services Controller 系統上停用 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，則您無須執行此工作。

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。如果 vCenter Server 6.0.x 或 5.5.x 的執行個體已連線至 vCenter Server，則當您停用 TLS 版本時，那些執行個體會停止與 Platform Services Controller 通訊。

您可以停用 TLS 1.0 和 TLS 1.1 並保持啟用 TLS 1.2，或者您可以僅停用 TLS 1.0 並保持啟用 TLS 1.1 和 TLS 1.2。

必要條件

請確保 Platform Services Controller 連線的主機和服務可使用支援的通訊協定進行通訊。由於驗證和憑證管理會由 Platform Services Controller 處理，因此請審慎考量哪些服務會受到影響。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	<code>cd C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</code>

- 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	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2</code>
Linux	<code>directory_path\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2</code>

- 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	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2</code>
Linux	<code>directory_path\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2</code>

- 3 如果您的環境包含其他 Platform Services Controller 系統，請重複該程序。

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

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。

作業系統	程序
Windows	<ol style="list-style-type: none"> 1 以具有管理員權限的使用者身分登入。 2 前往 <code>VcTlsReconfigurator</code> 目錄。 <pre>cd C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</pre>
Linux	<ol style="list-style-type: none"> 1 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。 2 如果 Bash shell 目前尚未啟用，請執行以下命令。 <pre>shell.set --enabled true shell</pre> <ol style="list-style-type: none"> 3 前往 <code>VcTlsReconfigurator</code> 目錄。 <pre>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</pre>

3 檢閱先前備份。

作業系統	程序
Windows	<pre>C:\ProgramData\VMware\vCenterServer\logs\vsphere-TlsReconfigurator\VcTlsReconfigurator.log</pre> <p>輸出與下列範例類似。</p> <pre>c:\users\username\appdata\local\temp\20161108T161539 c:\users\username\appdata\local\temp\20161108T171539</pre>
Linux	<pre>grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log</pre> <p>輸出與下列範例類似。</p> <pre>2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920 2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259</pre>

4 執行以下其中一個命令以執行還原。

作業系統	程序
Windows	<pre>reconfigureVc restore -d Directory_path_from_previous_step</pre> <p>例如</p> <pre>reconfigureVc restore -d c:\users\username\appdata\local\temp\20161108T171539</pre>
Linux	<pre>reconfigureVc restore -d Directory_path_from_previous_step</pre> <p>例如</p> <pre>reconfigureVc restore -d /tmp/20161117T172920</pre>

- 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 vSphere Update Manager 上停用 TLS 版本

在 vSphere Update Manager 6.0 Update 3 及更新版本中，TLS 通訊協定版本 1.0、1.1 以及 1.2 依預設會啟用。您可以停用 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 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。

必要條件

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 版本不同。

版本	位置
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	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。	<pre><Set name="ExcludeProtocols"> <Array type="java.lang.String"> <Item>TLSv1</Item> </Array> </Set></pre>
停用 TLS 1.0 和 TLS 1.1。保持啟用 TLS 1.2。	<pre><Set name="ExcludeProtocols"> <Array type="java.lang.String"> <Item>TLSv1</Item> <Item>TLSv1.1</Item> </Array> </Set></pre>

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。

必要條件

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 版本不同。

版本	位置
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 備份 `vci-integrity.xml` 檔案並開啟檔案。
- 4 在 `vci-integrity.xml` 檔案中新增 `<sslOptions>` 標記。

```
<ssl>
  <handshakeTimeoutMs>120000</handshakeTimeoutMS>
  <sslOptions>sslOptions_value</sslOptions>
</ssl>
```

```
<ssl>
  <privateKey>ssl/rui.key</privateKey>
  <certificate>ssl/rui.crt</certificate>
  <sslOptions>sslOptions_value</sslOptions>
</ssl>
```

5 根據您要停用的 TLS 版本，在 <sslOptions> 標記中使用以下十進位值。

- 若要僅停用 TLSv1.0，請使用十進位值 117587968。
- 若要停用 TLSv1.0 和 TLSv1.1，請使用十進位值 386023424

6 儲存檔案。

7 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 版本不同。

版本	位置
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	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 版本不同。

版本	位置
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 備份 vci-integrity.xml 檔案並開啟檔案。
- 4 變更 <sslOptions> 標記中使用的十進位值，或刪除該標記以允許所有 TLS 版本。
 - 若要啟用 TLS 1.1，但保持停用 TLS 1.0，請使用十進位值 117587968。
 - 若要同時重新啟用 TLS 1.1 和 TLS 1.0，請移除標記。
- 5 儲存檔案。
- 6 重新啟動 vSphere Update Manager 服務。

定義的權限

11

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。此附錄中的資料表使用 VC 指示 vCenter Server，使用 HC 指示主機用戶端 (一個獨立的 ESXi 或 Workstation 主機)。

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：

- 警示權限
- Auto Deploy 與映像設定檔權限
- 憑證權限
- 內容程式庫權限
- 資料中心權限
- 資料存放區權限
- 資料存放區叢集權限
- Distributed Switch 權限
- ESX Agent Manager 權限
- 延伸權限
- 資料夾權限
- 全域權限
- 主機 CIM 權限
- 主機組態權限
- 主機詳細目錄
- 主機本機作業權限
- 主機 vSphere Replication 權限

- 主機設定檔權限
- Inventory Service 提供者權限
- Inventory Service 標記權限
- 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
- VRM 原則權限
- 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

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 11-1. 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《vSphere 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 11-2. 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

表 11-2. Auto Deploy 權限 (續)

權限名稱	說明	要求
Auto Deploy.規則.刪除	允許刪除 Auto Deploy 規則。	vCenter Server
Auto Deploy.規則.編輯	允許編輯 Auto Deploy 規則。	vCenter Server
Auto Deploy.規則集.啟動	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[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 11-3. 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 11-4. 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
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:// or 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

表 11-4. 內容程式庫權限 (續)

權限名稱	說明	要求
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

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 11-5. 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 11-6. 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 11-7. 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 11-8. 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 11-9. ESX Agent Manager

權限名稱	說明	要求
ESX Agent Manager.組態	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 11-10. 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

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 11-11. 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 11-12. 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.啟用方式	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 <code>resxtp</code> 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

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 11-13. 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 11-14. 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 11-14. 主機組態權限 (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 11-15. 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

主機本機作業權限控制當 vSphere Client 直接連線到主機時執行的動作。

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 11-16. 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.擷取 NVRAM 內容	允許擷取主機的 NVRAM 內容。	
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.本機作業.重新配置快照	允許變更虛擬機器快照的配置。	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 11-17. 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 11-18. 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

Inventory Service 提供者權限

Inventory Service 提供者權限僅供內部使用。請勿使用。

Inventory Service 標記權限

Inventory Service 標記權限控制在 vSphere 詳細目錄物件上建立、刪除標籤與標籤類別，以及指派、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 11-19. vCenter Inventory Service 權限

權限名稱	說明	要求
Inventory Service.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
Inventory Service.vSphere 標記.建立 vSphere 標籤	允許建立標籤。	任何物件
Inventory Service.vSphere 標記.建立 vSphere 標籤類別	允許建立標籤類別。	任何物件
Inventory Service.vSphere 標記.建立 vSphere 標籤範圍	允許建立標籤範圍。	任何物件
Inventory Service.vSphere 標記.刪除 vSphere 標籤	允許刪除標籤類別。	任何物件
Inventory Service.vSphere 標記.刪除 vSphere 標籤類別	允許刪除標籤類別。	任何物件
Inventory Service.vSphere 標記.刪除 vSphere 標籤範圍	允許刪除標籤範圍。	任何物件
Inventory Service.vSphere 標記.編輯 vSphere 標籤	允許編輯標籤。	任何物件

表 11-19. vCenter Inventory Service 權限 (續)

權限名稱	說明	要求
Inventory Service.vSphere 標記.編輯 vSphere 標籤類別	允許編輯標籤類別。	任何物件
Inventory Service.vSphere 標記.編輯 vSphere 標籤範圍	允許編輯標籤範圍。	任何物件
Inventory Service.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
Inventory Service.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

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 11-20. 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 11-21. 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 11-22. 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 11-23. 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 11-24. 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.移轉已關閉電源之虛擬機器	允許將已關閉電源之虛擬機器移轉到不同的資源集區或主機。	虛擬機器
資源.移轉已開啟電源之虛擬機器	允許運用 vMotion 將已開啟電源之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 11-25. 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 11-26. 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	允許在訊息中設定全域記錄。	根 vCenter Server
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。

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 11-27. 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 11-28. 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。

VRM 原則權限

VRM 原則權限為 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 11-29. 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

表 11-29. 虛擬機器組態權限 (續)

權限名稱	說明	要求
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
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.解除鎖定虛擬機器	允許對虛擬機器解密。	虛擬機器
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 11-30. 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

表 11-30. 虛擬機器客體作業 (續)

權限名稱	說明	生效物件
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
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 11-31. 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.備份虛擬機器上的作業	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 11-31. 虛擬機器互動 (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.停用 Fault Tolerance	允許停用使用 Fault Tolerance 的虛擬機器的次要虛擬機器。	虛擬機器
虛擬機器.互動.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

表 11-31. 虛擬機器互動 (續)

權限名稱	說明	要求
虛擬機器.互動.啟用 Fault Tolerance	允許啟用使用 Fault Tolerance 的虛擬機器的次要虛擬機器。	虛擬機器
虛擬機器.互動.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
虛擬機器.互動.暫停/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

表 11-31. 虛擬機器互動 (續)

權限名稱	說明	要求
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
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

表 11-31. 虛擬機器互動 (續)

權限名稱	說明	要求
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
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

表 11-31. 虛擬機器互動 (續)

權限名稱	說明	要求
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 11-32. 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

表 11-32. 虛擬機器詳細目錄權限 (續)

權限名稱	說明	要求
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 11-33. 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
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 11-34. 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 11-35. 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
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 11-36. 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 11-37. 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 11-38. 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 11-39. 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