

vSphere 安全性

修改日期：2022 年 11 月 23 日

VMware vSphere 8.0

VMware ESXi 8.0

vCenter Server 8.0

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 14

更新的資訊 16

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 21

確保 vSphere 環境中密碼的安全 23

vCenter Server 和 ESXi 安全性最佳做法與資源 24

2 vSphere 權限和使用者管理工作 26

瞭解 vSphere 中的授權 27

vSphere 中的權限階層式繼承 30

多個權限設定在 vSphere 中如何運作 33

範例 1：從多個群組繼承權限 33

範例 2：子權限覆寫父系權限 34

範例 3：使用者角色覆寫群組角色 34

管理 vCenter Server 元件的權限 35

將權限新增到詳細目錄物件 35

變更或移除詳細目錄物件的權限 36

變更 vCenter Server 使用者驗證設定 36

使用 vCenter Server 全域權限 37

新增全域權限 37

標籤物件的 vCenter Server 權限 38

使用 vCenter Server 角色指派權限 40

建立 vCenter Server 自訂角色 42

針對 vCenter Server 角色和權限的最佳做法 43

一般工作所需的 vCenter Server 權限 43

3 保護 ESXi 主機 47

ESXi 一般安全建議 48

ESXi 進階系統設定 49

利用主機設定檔設定 ESXi 主機 51

使用指令碼管理 ESXi 主機組態設定 52

ESXi 密碼及帳戶鎖定 53

ESXi 產生密碼編譯金鑰	55
ESXi 中的 SSH 安全性	56
使用 HTTPS PUT 上傳 SSH 金鑰	57
PCI 和 PCIe 裝置和 ESXi	58
停用 vSphere 受管理物件瀏覽器	58
ESXi 網路安全性建議	59
修改 ESXi Web 代理設定	59
vSphere Auto Deploy 安全考量	59
控制以 CIM 為基礎的硬體監控工具的存取	60
vSphere Distributed Services Engine 安全性最佳做法	61
控制 ESXi 熵	61
管理 ESXi 主機的憑證	63
ESXi 主機升級和憑證	65
ESXi 憑證模式切換工作流程	66
ESXi 憑證預設設定	68
變更 ESXi 憑證預設設定	68
檢視 ESXi 主機的憑證到期資訊	69
更新或重新整理 ESXi 憑證	70
變更 ESXi 憑證模式	71
取代 ESXi SSL 憑證和金鑰	72
ESXi 憑證簽署要求的需求	72
取代 ESXi Shell 中的預設憑證和金鑰	73
使用 HTTPS PUT 取代預設憑證	74
更新 vCenter Server TRUSTED_ROOTS 存放區 (自訂憑證)	75
將 Auto Deploy 設為下層憑證授權機構	75
透過 Auto Deploy 使用自訂憑證	77
還原 ESXi 憑證和金鑰檔案	81
自訂 ESXi 主機安全性	81
設定 ESXi 防火牆	82
管理 ESXi 防火牆設定	82
為 ESXi 主機新增允許的 IP 位址	83
ESXi 主機的傳入和傳出防火牆連接埠	83
NFS 用戶端防火牆行為	84
使用 ESXCLI 防火牆命令設定 ESXi 行為	84
啟用或停用 ESXi 服務	85
在 ESXi 主機上設定和管理鎖定模式	87
鎖定模式行為	87
從 vSphere Client 啟用鎖定模式	89
從 vSphere Client 停用鎖定模式	89
從 Direct Console 使用者介面啟用或停用一般鎖定模式	90
指定在鎖定模式下具有存取權限的帳戶	90

使用 vSphere 安裝服務包執行安全更新	91
管理 ESXi 主機和 vSphere 安裝服務包的接受程度	92
為 ESXi 主機指派權限	94
使用 Active Directory 管理 ESXi 使用者	96
將 ESXi 主機設定為使用 Active Directory	96
將 ESXi 主機新增至目錄服務網域	97
檢視 ESXi 主機的目錄服務設定	98
使用 vSphere Authentication Proxy	98
啟動 vSphere Authentication Proxy 服務	99
使用 vSphere Client 將網域新增至 vSphere Authentication Proxy	100
使用 camconfig 命令，將網域新增至 vSphere Authentication Proxy	100
使用 vSphere Authentication Proxy 將主機新增到網域	101
為 vSphere Authentication Proxy 啟用用戶端驗證	102
將 vSphere Authentication Proxy 憑證匯入 ESXi 主機	103
為 vSphere Authentication Proxy 產生新的憑證	103
設定 vSphere Authentication Proxy 使用自訂憑證	104
設定和管理用於 ESXi 的智慧卡驗證	105
啟用智慧卡驗證	106
停用智慧卡驗證	106
發生連線問題時，利用使用者名稱和密碼進行驗證	107
在鎖定模式下使用智慧卡驗證	107
使用 ESXi Shell	107
使用 vSphere Client 設定 ESXi Shell 的閒置逾時	108
使用 vSphere Client 設定 ESXi Shell 的可用性逾時	109
使用 DCUI 設定 ESXi Shell 的可用性逾時或閒置逾時	109
使用 vSphere Client 啟用對 ESXi Shell 的存取	110
使用 DCUI 啟用對 ESXi Shell 的存取	111
登入 ESXi Shell 進行疑難排解	111
ESXi 主機的 UEFI 安全開機	112
在升級的 ESXi 主機上執行安全開機驗證指令碼	113
使用信賴平台模組保護 ESXi 主機	114
檢視 ESXi 主機證明狀態	115
疑難排解 ESXi 主機證明問題	116
ESXi 記錄檔	116
在 ESXi 主機上設定 Syslog	117
ESXi Syslog 選項	117
ESXi 記錄檔位置	121
確保 Fault Tolerance 記錄流量的安全	121
啟用 Fault Tolerance 加密	122
管理 ESXi 稽核記錄	123
保護 ESXi 組態安全	123

管理安全 ESXi 組態	126
列出安全 ESXi 組態復原金鑰的內容	126
輪替安全 ESXi 組態復原金鑰	126
安全 ESXi 組態的疑難排解和復原	127
復原安全 ESXi 組態	127
啟用或停用安全開機強制執行以確保安全的 ESXi 組態	128
啟用或停用 execInstalledOnly 強制執行以確保安全的 ESXi 組態	130
停用 execInstalledOnly 進階組態執行階段選項	133

4 保護 vCenter Server 系統的安全 134

vCenter Server 存取控制的最佳做法	134
設定 vCenter Server 密碼原則	136
從失敗的安裝移除到期或撤銷的憑證和記錄	136
限制 vCenter Server 的網路連線	136
評估 Linux 用戶端搭配 CLI 和 SDK 的使用情況	137
檢查 vSphere Client 外掛程式	137
vCenter Server 安全性最佳做法	138
vCenter 密碼需求與鎖定行為	138
驗證舊版 ESXi 主機的指紋	139
vCenter Server 所需的連接埠	140

5 確保虛擬機器安全 141

對虛擬機器啟用或停用 UEFI 安全開機	141
限制資訊訊息從虛擬機器流向 VMX 檔案	143
虛擬機器安全性最佳做法	143
虛擬機器一般保護	144
使用範本部署虛擬機器	144
儘量少用虛擬機器主控台	144
防止虛擬機器接管資源	145
停用虛擬機器中不必要的功能	145
從虛擬機器中移除不必要的硬體裝置	146
停用虛擬機器上未使用的顯示功能	147
停用客體作業系統和遠端主控台之間的複製和貼上作業	147
限制公開複製到虛擬機器主控台剪貼簿中的敏感資料	148
限制使用者在虛擬機器中執行命令	148
防止虛擬機器使用者或程序中斷裝置的連線	149
阻止客體作業系統程序向主機傳送組態訊息	149
避免使用獨立非持續性磁碟	150
使用 Intel 軟體防護延伸保護虛擬機器	150
vSGX 入門	151
在虛擬機器上啟用 vSGX	152

- 在現有虛擬機器上啟用 vSGX 152
- 從虛擬機器移除 vSGX 153
- 使用 AMD 安全加密虛擬化-加密狀態保護虛擬機器 153
 - vSphere 和 AMD 安全加密虛擬化-加密狀態 154
 - 使用 vSphere Client 將 AMD 安全加密虛擬化-加密狀態新增至虛擬機器 154
 - 將 AMD 安全加密虛擬化-加密狀態新增至虛擬機器 156
 - 使用 vSphere Client 在現有虛擬機器上啟用 AMD 安全加密虛擬化-加密狀態 157
 - 在現有虛擬機器上啟用 AMD 安全加密虛擬化-加密狀態 158
 - 使用 vSphere Client 在虛擬機器停用 AMD 安全加密虛擬化-加密狀態 159
 - 在虛擬機器上停用 AMD 安全加密虛擬化-加密狀態 159

6 虛擬機器加密 160

- vSphere 金鑰提供者的比較 161
- vSphere 虛擬機器加密如何保護您的環境 163
- vSphere 虛擬機器加密元件 166
- 加密程序流程 168
- 虛擬磁碟加密 170
- 虛擬機器加密錯誤 171
- 虛擬機器加密工作的必要條件和所需權限 172
- 已加密的 vSphere vMotion 173
- 虛擬機器加密最佳做法 176
- 虛擬機器加密注意須知 178
- 虛擬機器加密互通性 179
- ESXi 主機上的 vSphere 金鑰持續性 182

7 設定和管理標準金鑰提供者 184

- 標準金鑰提供者概觀 184
- 設定標準金鑰提供者 185
 - 使用 vSphere Client 新增標準金鑰提供者 185
 - 透過交換憑證建立標準金鑰提供者信任連線 186
 - 使用根 CA 憑證選項建立標準金鑰提供者信任連線 187
 - 使用憑證選項建立標準金鑰提供者信任連線 187
 - 使用上傳憑證和私密金鑰選項建立標準金鑰提供者信任連線 188
 - 使用新增憑證簽署要求選項建立標準金鑰提供者信任連線 189
 - 完成標準金鑰提供者的信任設定 189
 - 為不同使用者設定獨立的金鑰提供者 190

8 設定和管理 vSphere Native Key Provider 191

- vSphere Native Key Provider 概觀 191
- vSphere Native Key Provider 程序流程 194
- 設定 vSphere Native Key Provider 194

備份 vSphere Native Key Provider	196
在增強型連結模式組態中匯入 vSphere Native Key Provider	197
復原 vSphere Native Key Provider	198
使用 vSphere Client 還原 vSphere Native Key Provider	198
更新 vSphere Native Key Provider	199
刪除 vSphere Native Key Provider	200

9 vSphere Trust Authority 201

vSphere Trust Authority 概念和功能	201
vSphere Trust Authority 如何保護環境	201
受信任基礎結構概觀	204
vSphere Trust Authority 程序流程	207
vSphere Trust Authority 拓撲	210
vSphere Trust Authority 的必要條件和必要權限	210
vSphere Trust Authority 最佳做法、注意須知和互通性	212
vSphere Trust Authority 生命週期	213
設定 vSphere Trust Authority	215
設定工作站以設定 vSphere Trust Authority	217
啟用 Trust Authority 管理員	218
啟用 Trust Authority 狀態	218
收集要信任的 ESXi 主機和 vCenter Server 的相關資訊	220
匯出和匯入 TPM 簽署金鑰憑證	225
將受信任主機資訊匯入至 Trust Authority 叢集	230
在 Trust Authority 叢集上建立金鑰提供者	233
上傳用戶端憑證以建立受信任金鑰提供者信任連線	238
上傳憑證和私密金鑰以建立受信任金鑰提供者信任連線	239
建立憑證簽署要求以建立受信任金鑰提供者信任連線	241
匯出 Trust Authority 叢集資訊	242
將 Trust Authority 叢集資訊匯入至受信任的主機	244
使用 vSphere Client 為受信任的主機設定受信任金鑰提供者	248
使用命令列為受信任的主機設定受信任金鑰提供者	249
在 vSphere 環境中管理 vSphere Trust Authority	250
啟動、停止和重新啟動 vSphere Trust Authority 服務	251
檢視 Trust Authority 主機	251
檢視 vSphere Trust Authority 叢集狀態	251
重新啟動受信任主機服務	252
新增和移除 vSphere Trust Authority 主機	252
使用 vSphere Client 將主機新增到受信任叢集	252
使用 CLI 將主機新增到受信任叢集	253
從受信任叢集中解除委任受信任的主機	254
備份 vSphere Trust Authority 組態	255

- 變更受信任金鑰提供者的主要金鑰 255
- 受信任主機證明報告 256
 - 檢視受信任叢集證明狀態 257
- 對受信任主機證明問題進行疑難排解 258
- 檢查和修復受信任叢集健全狀況 258
 - 檢查受信任叢集健全狀況 259
 - 修復受信任叢集 260

10 在 vSphere 環境中使用加密 262

- 建立加密儲存區原則 263
- 明確啟用主機加密模式 263
- 使用 API 停用主機加密模式 264
- 建立加密的虛擬機器 265
- 複製加密的虛擬機器 266
- 加密現有虛擬機器或虛擬磁碟 269
- 解密已加密的虛擬機器或虛擬磁碟 269
- 變更虛擬磁碟的加密原則 270
- 解決缺少加密金鑰問題 271
- 將鎖定的虛擬機器解除鎖定 273
- 解決 ESXi 主機加密模式問題 274
- 重新啟用 ESXi 主機加密模式 274
- 設定金鑰伺服器憑證到期臨界值 275
- vSphere 虛擬機器加密和核心傾印 275
 - 針對使用加密的 ESXi 主機收集 vm-support 套件 276
 - 解密或重新加密已加密的核心傾印 277
- 在 ESXi 主機上啟用和停用金鑰持續性 278
- 使用 vSphere Client 對加密虛擬機器進行重設金鑰 279
- 使用 vSphere Client 設定預設金鑰提供者 279
- 使用 CLI 設定預設金鑰提供者 280

11 使用虛擬信賴平台模組保護虛擬機器 282

- 什麼是虛擬信賴平台模組 282
- 使用虛擬信賴平台模組建立虛擬機器 284
- 為現有虛擬機器新增虛擬信賴平台模組 285
- 從虛擬機器移除虛擬信賴平台模組 286
- 識別已啟用虛擬信賴平台模組的虛擬機器 286
- 檢視虛擬信賴平台模組裝置憑證 287
- 匯出並取代虛擬信賴平台模組裝置憑證 288

12 透過虛擬式安全性保護 Windows 客體作業系統 289

- vSphere 虛擬式安全性最佳做法 289

- 在虛擬機器上啟用虛擬式安全性 290
- 在現有虛擬機器上啟用以虛擬化為基礎的安全性 291
- 在客體作業系統上啟用以虛擬化為基礎的安全性 292
- 停用以虛擬化為基礎的安全性 293
- 識別已啟用 VBS 的虛擬機器 293

13 確保 vSphere 網路安全 294

- 使用防火牆確保網路安全 295
 - 針對具有 vCenter Server 的組態設定防火牆 296
 - 透過防火牆連線到 vCenter Server 297
 - 透過防火牆連線 ESXi 主機 297
 - 針對沒有 vCenter Server 的組態設定防火牆 297
 - 透過防火牆連線到虛擬機器主控台 297
- 確保實體交換器安全 298
- 使用安全性原則確保標準交換器連接埠安全 299
- 保護 vSphere Standard Switch 的安全 299
 - MAC 位址變更 300
 - 偽造的傳輸 300
 - 混合模式作業 301
- 標準交換器保護和 VLAN 301
- 保護 vSphere Distributed Switch 和分散式連接埠群組安全 302
- 透過 VLAN 保護虛擬機器的安全 303
 - VLAN 安全考量 304
 - 安全 VLAN 304
- 在單一 ESXi 主機內建立多個網路 305
- 在 ESXi 主機上使用網際網路通訊協定安全性 307
 - 列出可用的安全性關聯 308
 - 新增 IPsec 安全性關聯 308
 - 移除 IPsec 安全性關聯 309
 - 列出可用的 IPsec 安全性原則 309
 - 建立 IPsec 安全性原則 309
 - 移除 IPsec 安全性原則 310
- 確保 SNMP 組態正確 311
- vSphere 網路安全性最佳做法 311
 - 一般 vSphere 網路安全性建議 311
 - 標記 vSphere 網路元件 313
 - 記錄及檢查 vSphere VLAN 環境 313
 - 在 vSphere 中採用網路隔離做法 313
 - 僅在需要時透過 vSphere Network Appliance API 使用虛擬交換器 315

14 有關多個 vSphere 元件的最佳做法 316

- 同步 vSphere 網路上的時鐘 316
 - 使 ESXi 時鐘與網路時間伺服器同步 317
 - 在 vCenter Server 中設定時間同步化設定 317
 - 使用 VMware Tools 時間同步化 318
 - 在 vCenter Server 組態中新增或取代 NTP 伺服器 318
 - 將 vCenter Server 與 NTP 伺服器的時間同步 319
- 儲存區安全性最佳做法 319
 - 保護 iSCSI 儲存區安全 319
 - 保護 iSCSI 裝置安全 320
 - 保護 iSCSI SAN 320
 - 遮罩 SAN 資源並進行分區 321
 - 針對 NFS 4.1 使用 Kerberos 321
- 確認已停用向客體傳送主機效能資料 322
- 設定 ESXi Shell 和 vSphere Client 的逾時 322

15 透過 TLS Configurator 公用程式管理 vSphere TLS 通訊協定組態 324

- 執行選擇性 vCenter Server TLS 手動備份 325
- 在 vCenter Server 系統上啟用或停用 TLS 版本 326
- 針對 TLS 通訊協定掃描 vCenter Server 326
- 還原 vCenter Server TLS 組態變更 327

16 定義的權限 329

- 警示權限 332
- Auto Deploy 與映像設定檔權限 332
- 憑證權限 333
- 憑證授權機構權限 333
- 憑證管理權限 334
- Cns 權限 334
- 計算原則權限 335
- 內容程式庫權限 335
- 密碼編譯作業權限 338
- dvPort 群組權限 341
- Distributed Switch 權限 341
- 資料中心權限 342
- 資料存放區權限 343
- 資料存放區叢集權限 344
- ESX Agent Manager 權限 345
- 延伸權限 345
- 外部統計資料提供者權限 345
- 資料夾權限 346
- 全域權限 346

混合連結模式權限	347
健全狀況更新提供者權限	348
主機 CIM 權限	348
主機組態權限	348
主機熵集區權限	350
主機的 Intel Software Guard Extensions 權限	350
主機詳細目錄權限	351
主機本機作業權限	351
主機統計資料權限	352
主機信賴平台模組權限	352
主機 vSphere Replication 權限	353
主機設定檔權限	353
vCenter Server 設定檔權限	353
vSphere with Tanzu 權限	354
網路權限	355
NSX 權限	355
VMware 可觀察性權限	355
OvfManager 權限	356
與合作夥伴 REST 精靈互動權限	356
效能權限	356
外掛程式權限	356
權限 (Permissions) 權限	357
資源權限	357
排定的工作權限	358
工作階段權限	359
虛擬機器儲存區原則權限	359
儲存區視圖權限	359
主管服務權限	360
工作權限	360
承租人管理權限	361
Transfer Service 權限	361
VcTrusts/VcIdentity 權限	361
受信任基礎結構管理員權限	362
vApp 權限	363
VcIdentityProviders 權限	364
VMware vSphere Lifecycle Manager 組態權限	365
VMware vSphere Lifecycle Manager ESXi 健全狀況透視圖權限	365
VMware vSphere Lifecycle Manager 一般權限	366
VMware vSphere Lifecycle Manager 硬體相容性權限	366
VMware vSphere Lifecycle Manager 映像權限	366
VMware vSphere Lifecycle Manager 映像修復權限	367

VMware vSphere Lifecycle Manager 設定權限	368
VMware vSphere Lifecycle Manager 管理基準權限	368
VMware vSphere Lifecycle Manager 管理修補程式和升級權限	369
VMware vSphere Lifecycle Manager 上傳檔案權限	369
虛擬機器變更組態權限	370
虛擬機器客體作業權限	372
虛擬機器互動權限	373
虛擬機器編輯詳細目錄權限	375
虛擬機器佈建權限	376
虛擬機器服務組態權限	377
虛擬機器快照管理權限	378
虛擬機器 vSphere Replication 權限	378
虛擬機器類別權限	379
vSAN 權限	379
vSphere 區域權限	379
vService 權限	380
vSphere 標記權限	380
vSphere Client 權限	381

17 瞭解 vSphere 強化與符合性 382

vSphere 環境中的安全性與符合性	382
瞭解 vSphere 安全性組態指南	384
關於國家標準與技術研究院	385
關於 DISA STIG	385
關於 VMware 安全性開發生命週期	385
vSphere 中的稽核記錄	386
Single Sign-On 稽核事件	386
瞭解安全性與合規性後續步驟	387
vCenter Server 和 FIPS	388
FIPS 模組	388
在 vCenter Server Appliance 上啟用和停用 FIPS	389
使用 FIPS 時的考量事項	389

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。

VMware 十分重視包含性。為了在我們的客戶、合作夥伴和內部社群中貫徹這一原則，我們將使用包含性語言建立內容。

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
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。
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。■ UEFI 安全開機。■ 信賴平台模組 (TPM)。■ VMware® vSphere Trust Authority™。■ 安全 ESXi 組態和組態封裝
虛擬機器加密	<ul style="list-style-type: none">■ VMware vSphere® Native Key Provider™。■ 虛擬機器加密如何運作？■ KMS 設定。■ 加密和解密虛擬機器。■ 疑難排解和最佳做法。
客體作業系統安全性	<ul style="list-style-type: none">■ 虛擬信賴平台模組 (vTPM)。■ 虛擬式安全性 (VBS)。
管理 TLS 通訊協定組態	使用命令列公用程式變更 TLS 通訊協定組態。
安全性最佳做法和強化	VMware 安全性專家提出的最佳做法和建議。 <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

相關文件 vSphere 驗證說明了如何使用驗證服務來管理使用 vCenter Single Sign-On 進行的驗證以及管理 vSphere 環境中的憑證等。

除了這些文件，VMware 還發佈了適用於每個 vSphere 版本的《vSphere 安全性組態指南》(以前稱為《強化指南》)，存取網址為 <https://core.vmware.com/security>。《vSphere 安全性組態指南》包含客戶可以或應該設定的安全性設定的準則，而且客戶應該稽核 VMware 提供的安全性設定，以確保其設定為預設值。

Platform Services Controller 發生了什麼情況

從 vSphere 7.0 開始，部署新的 vCenter Server 或升級至 vCenter Server 7.0 需要使用 vCenter Server Appliance (已針對執行 vCenter Server 而最佳化的預先設定的虛擬機器)。新的 vCenter Server 包含所有 Platform Services Controller 服務，保留了功能和工作流程，其中包括驗證、憑證管理、標籤和授權。不再需要部署和使用外部 Platform Services Controller，也無法再進行部署和使用。所有 Platform Services Controller 服務已合併至 vCenter Server，並且簡化了部署和管理。

由於這些服務現在是 vCenter Server 的一部分，因此不再將其描述為 Platform Services Controller 的一部分。在 vSphere 7.0 中，vSphere 驗證出版物會取代 Platform Services Controller 管理 出版物。新的出版物包含有關驗證和憑證管理的完整資訊。如需從使用現有外部 Platform Services Controller 的 vSphere 6.5 和 6.7 部署升級或移轉至使用 vCenter Server Appliance 的 vSphere 7.0 的相關資訊，請參閱 vSphere 升級說明文件。

預定對象

該資訊適用於熟悉虛擬機器技術和資料中心作業且富有經驗的系統管理員。

認證

VMware 會發佈已完成通用準則認證的 VMware 產品的公開清單。若要確認特定 VMware 產品版本是否已通過認證，請參閱「通用準則評估和驗證」網頁，網址為：<https://www.vmware.com/security/certifications/common-criteria.html>。

更新的資訊

本 vSphere 安全性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 11 月 23 日	<ul style="list-style-type: none">■ 對使用 vCenter Server 角色指派權限 進行輕微更新。■ 更新了 ESXi 主機上的 vSphere 金鑰持續性和在 ESXi 主機上啟用和停用金鑰持續性，新增了有關 vSphere Native Key Provider 的其他資訊。■ 對安全 VLAN 進行輕微更新。■ 在第 16 章 定義的權限 一章中新增了主題。
2022 年 10 月 27 日	<ul style="list-style-type: none">■ 對使用命令列為受信任的主機設定受信任金鑰提供者進行輕微更新。■ 對使用 vSphere Client 設定預設金鑰提供者進行輕微更新。■ 新增了使用 CLI 設定預設金鑰提供者。■ 在第 16 章 定義的權限 一章中新增了多個主題。
2022 年 10 月 13 日	<ul style="list-style-type: none">■ 對 vSphere 虛擬式安全性最佳做法、在虛擬機器上啟用虛擬式安全性和在現有虛擬機器上啟用以虛擬化為基礎的安全性進行了輕微更新。■ 移除了對 <code>vifs</code> 命令的參考。請參閱 VMware 知識庫文章，網址為 https://kb.vmware.com/article/78473。
2022 年 10 月 11 日	初始版本。

vSphere 環境中的安全性

1

vSphere 環境的元件會立即受到數種功能的保護，如驗證、授權、每個 ESXi 主機上的防火牆等。您可以透過多種方式修改預設設定。例如，您可以設定 vCenter Server 物件的權限、開啟防火牆連接埠或變更預設憑證。可以針對不同 vSphere 物件採取安全性措施，例如，vCenter Server 系統、ESXi 主機、虛擬機器以及網路和儲存區物件。

對需要注意的 vSphere 不同區域的高層級概觀可協助您計劃安全性策略。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](#)
- [確保 vSphere 環境中密碼的安全](#)
- [vCenter Server 和 ESXi 安全性最佳做法與資源](#)

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。針對一致性，您可以設定參考主機，並將所有主機與參考主機的主機設定檔保持同步。您也可以透過執行指令碼式管理保護您的環境，這會確保變更套用到所有主機。

您可以採取下列動作，增強對 vCenter Server 管理之 ESXi 主機的保護。儘管獨立主機的管理工作可能有所不同，但其安全考量事項類似。請參閱 vSphere 單一主機管理 - VMware Host Client 說明文件。

限制 ESXi 存取

依預設，ESXi Shell 和 SSH 服務未在執行中，並且僅根使用者可以登入 Direct Console 使用者介面 (DCUI)。如果您決定啟用 ESXi 或 SSH 存取，可以設定逾時來限制未經授權存取的風險。可以存取 ESXi 主機的使用者必須具有管理主機的權限。您可以從管理主機的 vCenter Server 系統對主機物件設定權限。

請參閱[使用 ESXi Shell](#)。

使用具名使用者和最少的權限

依預設，根使用者可以執行許多工作。不允許管理員使用根使用者帳戶登入 ESXi 主機。而是從 vCenter Server 建立具名管理員使用者，並為這些使用者指派管理員角色。您也可以為這些使用者指派自訂角色。請參閱[建立 vCenter Server 自訂角色](#)。

如果您直接管理主機上的使用者，則會限制角色管理選項。請參閱 [vSphere 單一主機管理 - VMware Host Client 說明文件](#)。

將開啟的 ESXi 防火牆連接埠數目降至最低

依預設，僅在您啟動對應的服務時，ESXi 主機上的防火牆連接埠才處於開啟狀態。您可以使用 vSphere Client、ESXCLI 或 PowerCLI 命令來檢查並管理防火牆連接埠狀態。

請參閱[設定 ESXi 防火牆](#)。

自動化 ESXi 主機管理

由於同一資料中心中的不同主機處於同步狀態通常很重要，因此，請使用指令碼式安裝或 vSphere Auto Deploy 佈建主機。您可以使用指令碼管理主機。主機設定檔是指令碼式管理的替代。您可設定參考主機，匯出主機設定檔，並將主機設定檔套用到所有主機。您可以直接套用主機設定檔，或者做為使用 Auto Deploy 進行佈建的一部分。

如需有關 vSphere Auto Deploy 的資訊，請參閱[使用指令碼管理 ESXi 主機組態設定](#)和 vCenter Server 安裝和設定說明文件。

利用 ESXi 鎖定模式

在鎖定模式下，依預設僅能透過 vCenter Server 存取 ESXi 主機。您可以選取嚴格鎖定模式或一般鎖定模式。您可以定義例外使用者，以允許直接存取備份代理程式等服務帳戶。

請參閱[在 ESXi 主機上設定和管理鎖定模式](#)。

檢查 VIB 套件完整性

每個 vSphere 安裝服務包 (VIB) 套件都具有相關聯的接受程度。僅當 VIB 的接受程度等同於或優於 ESXi 主機的接受程度時，才可以將此 VIB 新增至此主機。不得將接受程度為 CommunitySupported 或 PartnerSupported 的 VIB 新增至主機，除非您明確變更主機的接受程度。

請參閱[管理 ESXi 主機和 vSphere 安裝服務包的接受程度](#)。

管理 ESXi 憑證

VMware Certificate Authority (VMCA) 預設會使用將 VMCA 做為根憑證授權機構的已簽署憑證佈建每台 ESXi 主機。如果公司原則需要，您可以將現有憑證取代為由第三方或企業憑證授權機構簽署的憑證。

請參閱[管理 ESXi 主機的憑證](#)。

考量為 ESXi 使用智慧卡驗證

ESXi 支援使用智慧卡驗證，而不是使用者名稱和密碼驗證。vCenter Server 也支援雙因素驗證。您可以同時設定使用者名稱和密碼驗證及智慧卡驗證。

請參閱[設定和管理用於 ESXi 的智慧卡驗證](#)。

考量 ESXi 帳戶鎖定

支援透過 SSH 和 vSphere Web Services SDK 存取帳戶鎖定。依預設，最多 5 次嘗試失敗後，帳戶即會鎖定。依預設，帳戶會在 15 分鐘後解除鎖定。

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

請參閱[ESXi 密碼及帳戶鎖定](#)。

保護 vCenter Server 系統和相關聯服務的安全

透過 vCenter Single Sign-On 進行驗證並透過 vCenter Server 權限模型進行授權，可保護 vCenter Server 系統和關聯的服務。您可以修改預設行為，並採取步驟限制對您環境的存取。

請注意，在您保護 vSphere 環境時，也必須保護與 vCenter Server 執行個體相關聯的所有服務。在一些環境中，您可以保護數個 vCenter Server 執行個體。

vCenter Server 使用加密通訊

依預設（「即時可用」），vCenter Server 系統與其他 vSphere 元件之間的所有資料通訊均已加密。在某些情況下，根據環境的設定方式，一些流量可能未加密。例如，可以為電子郵件警示設定未加密的 SMTP，為監控設定未加密的 SNMP。DNS 流量也未加密。vCenter Server 會接聽連接埠 80 (TCP) 和連接埠 443 (TCP)。連接埠 443 (TCP) 是業界標準的 HTTPS (安全 HTTP) 連接埠，並使用 TLS 1.2 加密進行保護。連接埠 80 (TCP) 是業界標準的 HTTP 連接埠，不使用加密。連接埠 80 的用途是將請求從連接埠 80 重新導向到連接埠 443，以確保這些請求的安全。

強化 vCenter Server 系統

保護 vCenter Server 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 vSphere 憑證模型

依預設，VMware Certificate Authority (VMCA) 會使用 VMCA 所簽署的憑證在環境中佈建每台 ESXi 主機和每個機器。如果您的公司原則需要，可以變更預設行為。如需詳細資料，請參閱 vSphere 驗證說明文件。

如需其他保護，請明確移除到期或撤銷的憑證及已失敗的安裝。

設定 vCenter Single Sign-On

vCenter Server 及其相關聯的服務受到 vCenter Single Sign-On 驗證架構的保護。當您首次安裝軟體時，請為 vCenter Single Sign-On 網域的管理員指定密碼，預設為 administrator@vsphere.local。僅該網域做為身分識別來源初始可用。您可以新增外部身分識別提供者，例如 Microsoft Active Directory Federation Services (AD FS)，以進行同盟驗證。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。能夠向其中一個身分識別來源進行驗證的使用者可以檢視物件並執行工作 (如果有權執行這些作業)。如需詳細資料，請參閱 vSphere 驗證說明文件。

為使用者或群組指派 vCenter Server 角色

为了更好地記錄，請將您授與物件的每個權限與具名使用者或群組，以及預先定義的角色或自訂角色相關聯。vSphere 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 vCenter Server 權限](#)。

限制管理員權限及管理員角色的使用。如果可能，請勿使用匿名管理員使用者。

設定精確時間通訊協定或網路時間通訊協定

為環境中的每個節點設定精確時間通訊協定 (PTP) 或網路時間通訊協定 (NTP)。vSphere 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虛擬環境，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。

停用不必要的虛擬機器功能

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 (HGFS)，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](#)。

使用虛擬機器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 PowerCLI 指令碼。本說明文件主要介紹如何使用 vSphere Client 執行工作。請考慮使用指令碼而非 vSphere Client 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 虛擬機器管理說明文件。如需 PowerCLI 的相關資訊，請參閱 VMware PowerCLI 說明文件。

儘量少用虛擬機器主控台

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

考慮虛擬機器的 UEFI 安全開機

可以將虛擬機器設定為使用 UEFI 開機。如果該作業系統支援安全 UEFI 開機，您可以針對其他安全性為虛擬機器選取該選項。請參閱[對虛擬機器啟用或停用 UEFI 安全開機](#)。

考慮使用 Carbon Black Cloud Workload

您可以安裝並使用 Carbon Black Cloud 工作負載，以識別風險、防止攻擊，以及偵測異常活動。憑藉內建於 Carbon Black Cloud 平台的 AppDefense 功能，Carbon Black Cloud 工作負載是 AppDefense 的接替產品。

保護虛擬網路層的安全

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

vSphere 包含安全網路基礎結構所需的完整陣列功能。您可以分別保護基礎結構的每個元素，例如虛擬交換器、分散式虛擬交換器和虛擬網路介面卡。此外，請考慮[第 13 章 確保 vSphere 網路安全](#)中詳細介紹的準則。

隔離網路流量

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

請參閱[ESXi 網路安全性建議](#)。

使用防火牆保護虛擬網路元素的安全

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

您也可以明確開啟 vCenter Server 執行個體上的連接埠。

如需 VMware 產品 (包括 vSphere 和 vSAN) 中所有支援的連接埠和通訊協定的清單，請參閱 VMware Ports and Protocols Tool™，網址為 <https://ports.vmware.com/>。可以依 VMware 產品搜尋連接埠、建立自訂連接埠清單，以及列印或儲存連接埠清單。

考慮網路安全性原則

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

如需相關指示，請參閱 vSphere 網路說明文件。

保護虛擬機器網路的安全

您用於保護虛擬機器網路安全的方法取決於多個因素，包括：

- 安裝的客體作業系統
- 虛擬機器是否在信任的環境中運作

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

請參閱 [第 13 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。VLAN 可讓您將實體網路分段。您可以使用 VLAN 來進一步保護虛擬機器網路或儲存區組態。當您使用 VLAN 時，同一實體網路中的兩台虛擬機器無法相互收發封包，除非位於相同的 VLAN 上。

請參閱 [透過 VLAN 保護虛擬機器的安全](#)。

保護虛擬化儲存區的連線安全

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

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

請參閱 [儲存區安全性最佳做法](#)。

評估網際網路通訊協定安全性的使用

ESXi 透過 IPv6 支援網際網路通訊協定安全性 (IPSec)。您無法針對 IPv4 使用 IPSec。

請參閱 [在 ESXi 主機上使用網際網路通訊協定安全性](#)。

確保 vSphere 環境中密碼的安全

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

ESXi 密碼限制由某些需求決定。請參閱 [ESXi 密碼及帳戶鎖定](#)。

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

vCenter Single Sign-On 管理員的密碼

administrator@vsphere.local 使用者或 administrator@mydomain 使用者 (如果您在安裝期間選取了不同的網域) 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。如需詳細資料，請參閱 vSphere 驗證說明文件。

如果您忘記了此使用者的密碼，請搜尋 VMware 知識庫系統，瞭解重設此密碼的相關資訊。重設需要其他權限，例如對 vCenter Server 系統的根存取權限。

其他 vCenter Single Sign-On 網域使用者的密碼

其他 vsphere.local 使用者或您在安裝期間指定之網域使用者的密碼，必須遵循由 vCenter Single Sign-On 密碼原則和鎖定原則所設定的限制。如需詳細資料，請參閱 vSphere 驗證說明文件。依預設，這些密碼會於 90 天後到期。管理員可以將到期日做為密碼原則的一部分進行變更。

如果您忘記了自己的 vsphere.local 密碼，管理員使用者可以使用 `dir-cli` 命令重設密碼。

其他身分識別來源中使用者的密碼

所有其他使用者的密碼限制、密碼到期和帳戶鎖定由使用者可進行驗證的網域 (身分識別來源) 決定。

vCenter Single Sign-On 支援一個預設身分識別來源。使用者可以使用 vSphere Client 及其使用者名稱登入對應的網域。如果使用者希望登入非預設網域，他們可以加入網域名稱，即，指定 `user@domain` 或 `domain\user`。網域密碼參數可套用至每一個網域。

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

vCenter Server Appliance 是預先設定的針對執行中 vCenter Server 及相關聯服務進行最佳化的虛擬機器。

部署 vCenter Server 時可指定這些密碼。

- root 使用者的密碼。
- vCenter Single Sign-On 網域的管理員密碼 administrator@vsphere.local (預設)。

您可以從 vCenter Server 管理介面變更根使用者密碼，並執行其他 vCenter Server 本機使用者管理工作。請參閱 vCenter Server 組態說明文件。

vCenter Server 和 ESXi 安全性最佳做法與資源

如果遵循最佳做法，您的 ESXi 主機和 vCenter Server 系統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。本手冊僅為確保安全環境必須使用的來源之一。

vSphere 安全性資源

若要進一步瞭解 vSphere 安全性的特定方面，請使用本手冊中的以下內容。

表 1-1. 安全性最佳做法

vSphere 元件	資源
ESXi 主機	第 3 章 保護 ESXi 主機
vCenter Server 系統	第 4 章 保護 vCenter Server 系統的安全
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

Web 上的 VMware 安全性資源

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
有關 ESXi 和 vCenter Server 安全性和作業的資訊，包括安全組態和 Hypervisor 安全性。	https://core.vmware.com/security
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	https://core.vmware.com/compliance

表 1-2. Web 上的 VMware 安全性資源 (續)

主題	資源
針對不同版本 vSphere 元件的安全性憑證和驗證 (如 CCEVS 和 FIPS) 的資訊。	https://www.vmware.com/support/support-resources/certifications.html
適用於不同版本 vSphere 和其他 VMware 產品的《安全性組態指南》(以前稱為《強化指南》)。	https://core.vmware.com/security-configuration-guide
《VMware vSphere Hypervisor 安全性》白皮書	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

vSphere 權限和使用者管理工作

2

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

如需有關使用 vSphere Client 指派角色和權限的概觀，請觀看以下視訊。



(使用 vSphere Client 指派角色和權限)

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

一開始，僅授權 vCenter Single Sign-On 網域的管理員使用者登入 vCenter Server 系統。預設網域為 vsphere.local，預設管理員為 administrator@vsphere.local。可以在 vSphere 安裝期間變更預設網域。身為管理員使用者，您可以：

- 1 將已定義使用者和群組的身分識別來源新增至 vCenter Single Sign-On。請參閱 vSphere 驗證說明文件。
- 2 透過選取某個物件 (例如虛擬機器或 vCenter Server 系統) 並為某個使用者或群組指派該物件上的角色，可將權限指定給該使用者或群組。

本章節討論下列主題：

- 瞭解 vSphere 中的授權
- 多個權限設定在 vSphere 中如何運作
- 管理 vCenter Server 元件的權限
- 使用 vCenter Server 全域權限
- 使用 vCenter Server 角色指派權限
- 針對 vCenter Server 角色和權限的最佳做法
- 一般工作所需的 vCenter Server 權限

瞭解 vSphere 中的授權

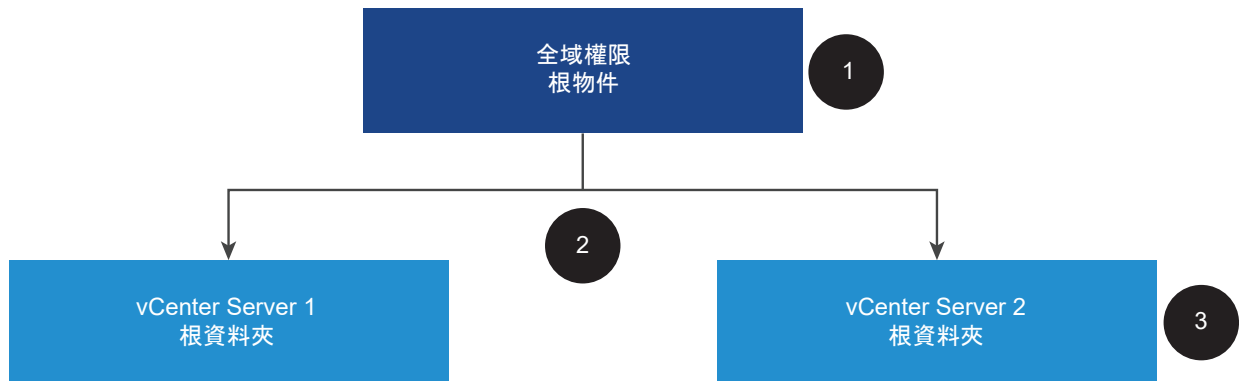
vSphere 支援使用數種模型來確定是否允許使用者執行某項工作。vCenter Single Sign-On 群組中的群組成員資格決定了允許您執行的操作。您對物件的角色或全域權限將決定是否允許您執行其他工作。

權限在 vSphere 中如何運作

vSphere 允許有權限的使用者授與其他使用者執行工作的權限。您可以使用全域權限，或者您可以針對個別 vCenter Server 執行個體，使用本機 vCenter Server 權限授權其他使用者。

下圖說明了全域權限和本機權限的運作方式。

圖 2-1. 全域權限和本機權限



在此圖中：

- 1 在根物件層級上指派全域權限並選取「散佈到子系」。
- 2 vCenter Server 將權限散佈到環境中的 vCenter Server 1 和 vCenter Server 2 物件階層。
- 3 vCenter Server 2 上的根資料夾的本機權限會取代全域權限。

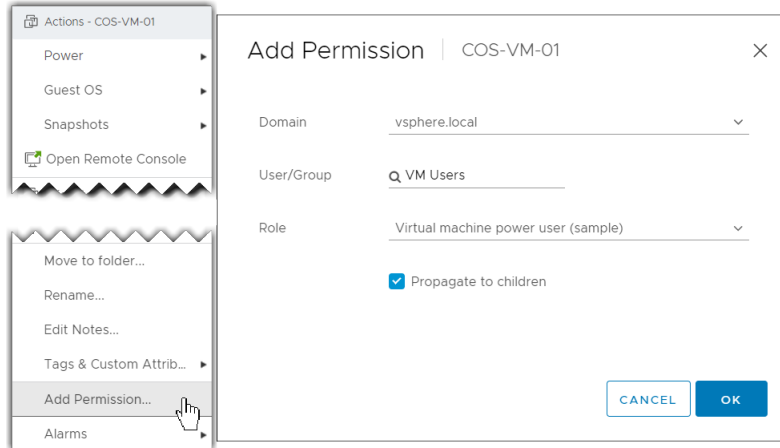
vCenter Server 權限

vCenter Server 系統的權限模型依賴於將權限指派到物件階層中的物件。使用者會按下列方式取得權限。

- 來自使用者的特定權限或來自使用者所屬的群組
- 來自物件的權限或透過父系物件的權限繼承

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。您可以使用 vSphere Client 新增權限。例如，可以在虛擬機器上按一下滑鼠右鍵，選取**新增權限**，然後完成向一組使用者指派角色的對話方塊。該角色可授與這些使用者在虛擬機器上的對應權限。

圖 2-2. 使用 vSphere Client 將權限新增到虛擬機器



全域權限

全域權限會賦予使用者或群組檢視或管理部署中解決方案的每個詳細目錄階層中所有物件的權限。也就是說，全域權限會應用至跨解決方案詳細目錄階層的全域根物件。(解決方案包括 vCenter Server、vRealize Orchestrator 等。)全域權限也適用於標籤和內容程式庫等全域物件。例如，假設一個部署包含兩個解決方案，即 vCenter Server 和 vRealize Orchestrator。您可以使用全域權限向一組使用者指派角色，這些使用者對 vCenter Server 和 vRealize Orchestrator 物件階層中的所有物件具有唯讀權限。

將跨 vCenter Single Sign-On 網域 (vsphere.local by default) 複寫全域權限。全域權限不為透過 vCenter Single Sign-On 網域群組管理的服務提供授權。請參閱[使用 vCenter Server 全域權限](#)。

vCenter Single Sign-On 群組中的群組成員資格

vCenter Single Sign-On 網域群組的成員可以執行特定工作。例如，如果您是 LicenseService.Administrators 群組的成員，則可以執行授權管理。請參閱 vSphere 驗證說明文件。

ESXi 本機主機權限

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

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

瞭解物件層級權限模型

您可以透過使用物件上的權限來授權使用者或群組在 vCenter Server 物件上執行工作。就程式設計而言，當使用者嘗試執行作業時，即會執行 API 方法。vCenter Server 會檢查該方法的權限，以確認使用者是否有權執行作業。例如，當使用者嘗試新增主機時，會叫用 AddStandaloneHost_Task 方法。此方法要求使用者的角色具有 Host.Inventory.AddStandaloneHost 權限。如果該檢查找不到此權限，則使用者新增主機的權限會遭到拒絕。

下列概念很重要。

權限

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

使用者和群組

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

權限

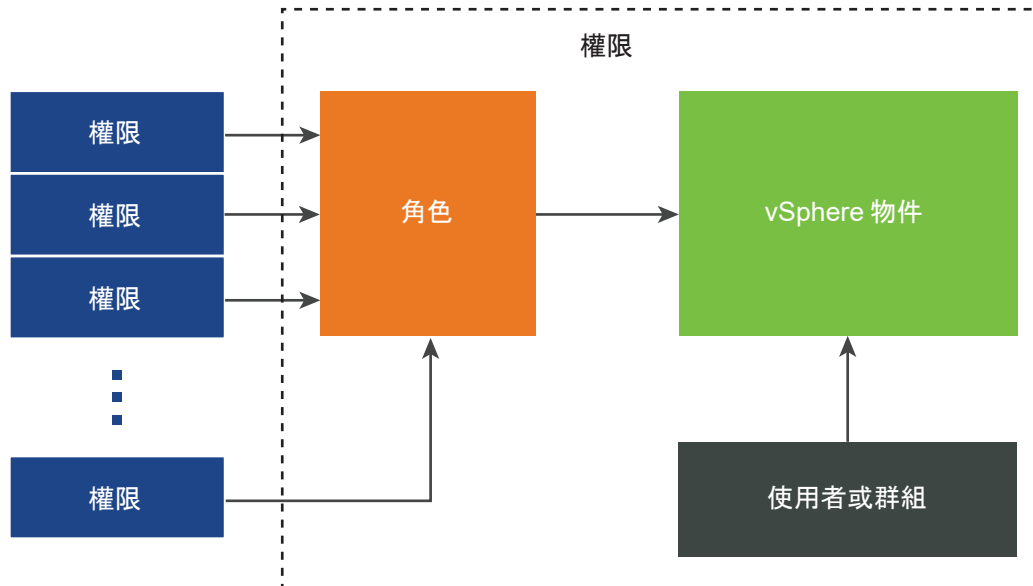
權限為細密的存取控制。您可以將這些權限分組到角色，然後將角色對應到使用者或群組。

角色

角色為權限集。角色讓您能夠根據使用者一般會執行的一組工作來指派物件的權限。vCenter Server 中已預先定義系統角色 (例如管理員) 且無法變更。vCenter Server 還提供了一些可修改的預設範例角色，例如資源集區管理員。您可以從頭開始建立自訂角色，也可以透過複製和修改範例角色來建立自訂角色。請參閱[建立 vCenter Server 自訂角色](#)。

下圖說明了如何透過特殊權限和角色建構權限，以及如何將權限指派給 vSphere 物件的使用者或群組。

圖 2-3. vSphere 權限



若要將權限指派給物件，請遵循以下步驟執行：

- 1 選取要將 vCenter Server 物件階層中的權限套用到的物件。
- 2 選取應擁有該物件權限的群組或使用者。
- 3 選取個別權限或角色，即群組或使用者應擁有的一組物件權限。

依預設，不會選取 [散佈到子系]。必須選取該核取方塊，使用者或群組才能對所選物件及其子物件擁有所選角色。

vCenter Server 提供了範例角色，這些角色將合併常用的權限集。您也可以透過合併一組角色來建立自訂角色。

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

請參閱下列資訊。

若要瞭解...	請參閱...
建立自訂角色。	建立 vCenter Server 自訂角色
所有權限和可套用權限的物件	第 16 章 定義的權限
不同工作的不同物件上所需的權限集。	一般工作所需的 vCenter Server 權限

獨立 ESXi 主機的權限模型更為簡單。請參閱[為 ESXi 主機指派權限](#)。

什麼是 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，假設在數個物件上為使用者 Smith 指派了某個角色。網域管理員將名稱變更為 Smith2。下次進行驗證時，主機會認為 Smith 已不存在，並從 vSphere 物件中移除與該使用者相關聯的權限。

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。

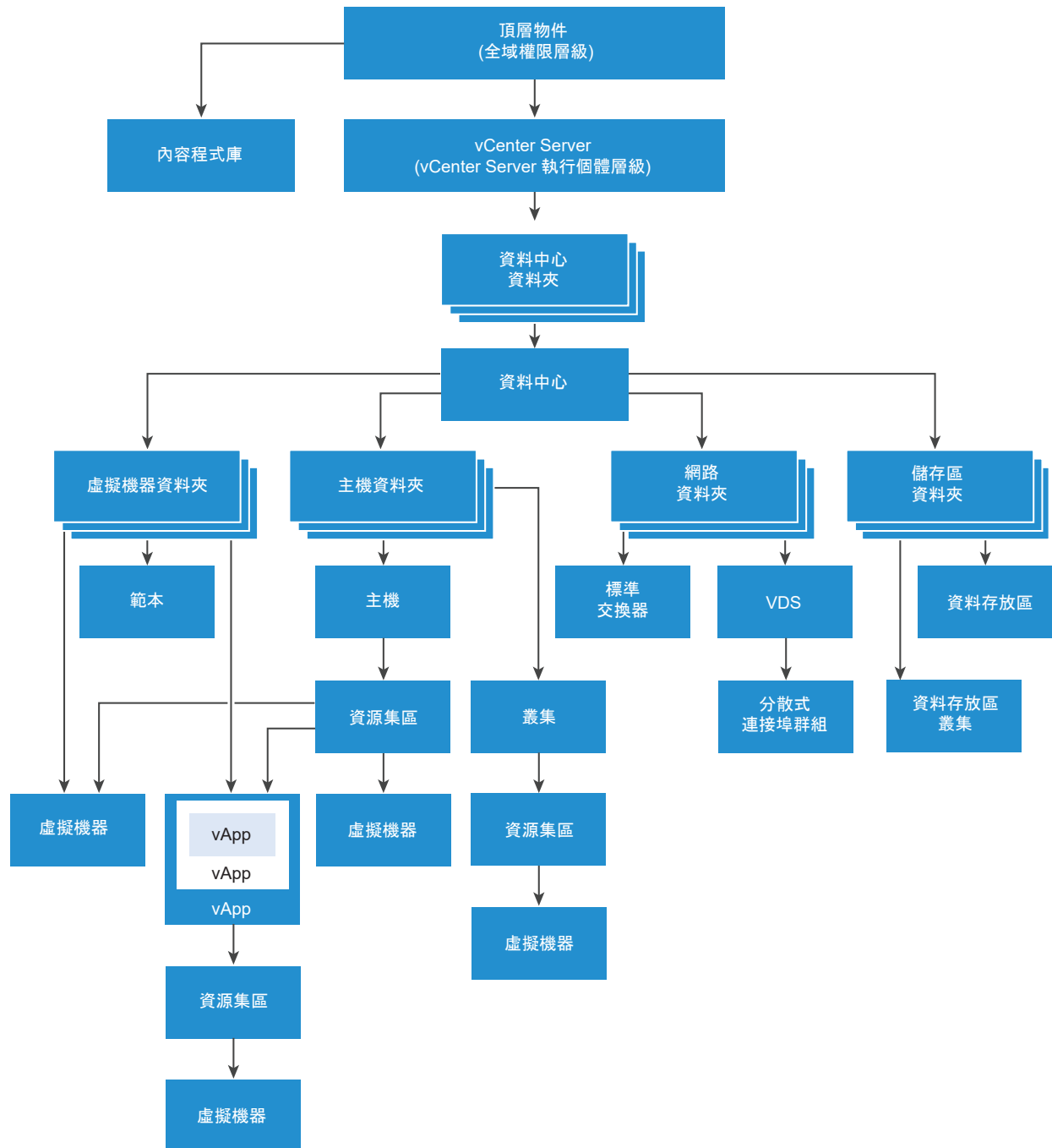
vSphere 中的權限階層式繼承

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。

下圖說明了詳細目錄階層和權限的散佈路徑。

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[使用 vCenter Server 全域權限](#)。

圖 2-4. vSphere 詳細目錄階層



關於此圖：

- 您無法在虛擬機器、主機、網路和儲存區資料夾上設定直接權限。也就是說，這些資料夾將充當容器，因此對使用者不可見。
- 您無法設定標準交換器的權限。

備註 為了能夠設定權限並將其散佈到 vSphere Distributed Switch (VDS) 上的子系，交換器物件必須位於在資料中心上建立的網路資料夾中。

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

受管理實體指的是下列 vSphere 物件。受管理實體可提供視實體類型而異的特定作業。特權使用者可以定義受管理的實體的權限。如需有關 vSphere 物件、內容和方法的詳細資訊，請參閱 vSphere API 說明文件。

- 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

多個權限設定在 vSphere 中如何運作

物件可能擁有多個權限，但是每個使用者或群組只能有一個權限。例如，一種權限必須指定 GroupAdmin 對某個物件具有管理員角色。另一種權限必須指定 GroupVMAdmin 對同一物件具有虛擬機器管理員角色。但是，GroupVMAdmin 群組不能對此物件具有同一 GroupVMAdmin 的其他權限。

如果父系的散佈內容設定為 true，則子物件會繼承其父系物件的權限。直接在子物件上設定的權限會覆寫父系物件中的權限。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角色，且使用者屬於這些群組中的兩個或多個群組，則可能出現下列兩種情況：

- 沒有直接在物件上定義使用者權限。在此情況下，使用者將獲得群組對該物件具有的權限聯集。
- 已直接在物件上定義使用者權限。在此情況下，該使用者的權限優先於所有群組權限。

範例 1：從多個群組繼承權限

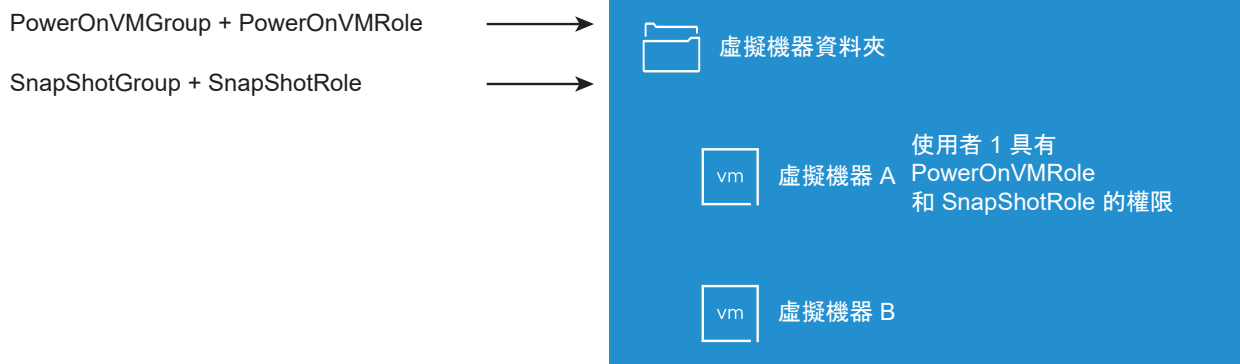
此範例說明物件如何從父系物件上授與權限的群組繼承多個權限。

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。

- PowerOnVMRole 可以開啟虛擬機器電源。
- SnapShotRole 可以建立虛擬機器快照。
- 在虛擬機器資料夾上為 PowerOnVMGroup 授與 PowerOnVMRole，並將權限設定為散佈到子物件。
- 在虛擬機器資料夾上為 SnapShotGroup 授與 SnapShotRole，並將權限設定為散佈到子物件。
- 未向使用者 1 指派特定權限。

同時屬於 PowerOnVMGroup 和 SnapShotGroup 的使用者 1 登入。使用者 1 可同時為虛擬機器 A 和虛擬機器 B 開啟電源並建立快照。

圖 2-5. 範例 1：從多個群組繼承權限



範例 2：子權限覆寫父系權限

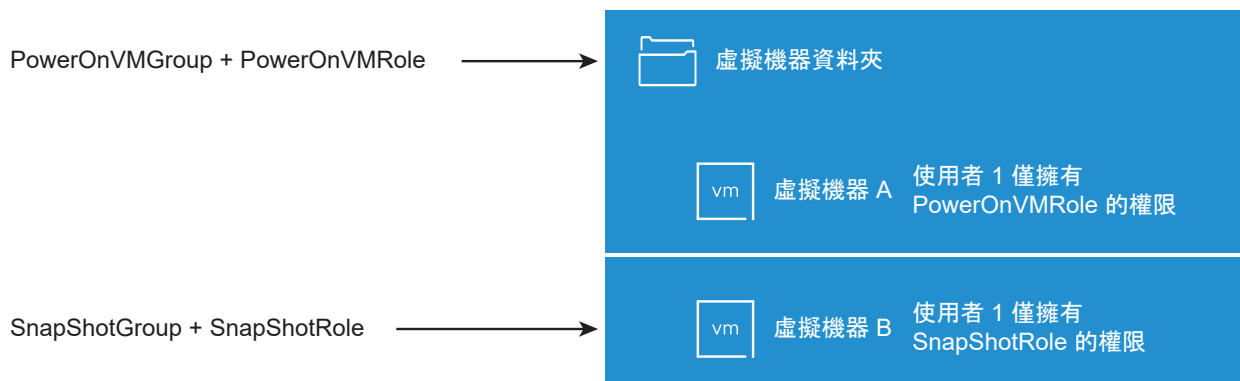
此範例說明子物件上指派的權限如何覆寫父系物件上指派的權限。可使用此覆寫行為限制使用者對詳細目錄的特定區域的存取。

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。

- PowerOnVMRole 可以開啟虛擬機器電源。
- SnapShotRole 可以建立虛擬機器快照。
- 在虛擬機器資料夾上為 PowerOnVMGroup 授與 PowerOnVMRole，並將權限設定為散佈到子物件。
- 在虛擬機器 B 上為 SnapShotGroup 授與 SnapShotRole。

同時屬於 PowerOnVMGroup 和 SnapShotGroup 的使用者 1 登入。由於在階層中，SnapShotRole 的指派位置比 PowerOnVMRole 略低，因此 SnapShotRole 會覆寫虛擬機器 B 上的 PowerOnVMRole。使用者 1 可開啟虛擬機器 A 的電源，但不能建立快照。使用者 1 可建立虛擬機器 B 的快照，但不能開啟它的電源。

圖 2-6. 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

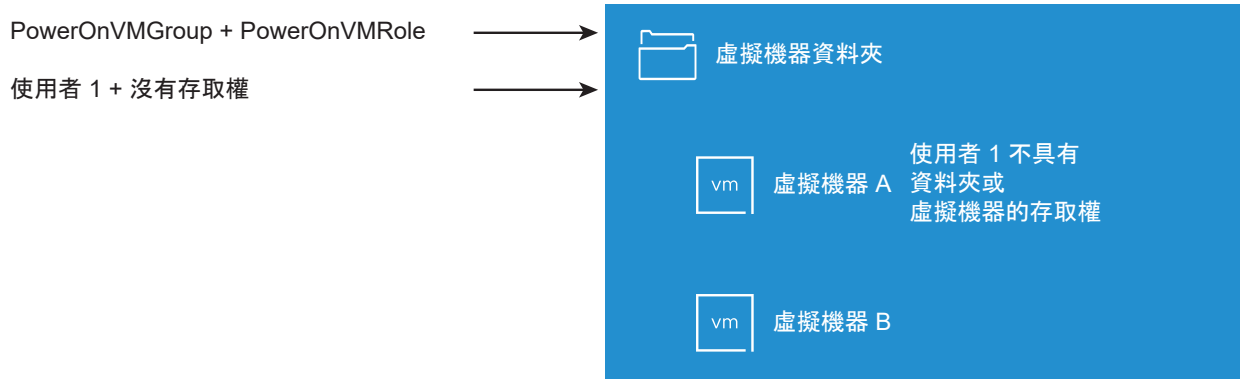
此範例說明了直接指派給個別使用者的角色如何覆寫與指派到群組之角色相關聯的權限。

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。

- PowerOnVMRole 可以開啟虛擬機器電源。
- 在虛擬機器資料夾上為 PowerOnVMGroup 授與 PowerOnVMRole。
- 在虛擬機器資料夾上為使用者 1 授與 NoAccess 角色。

屬於 PowerOnVMGroup 的使用者 1 登入。虛擬機器資料夾上為使用者 1 授與的 NoAccess 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 和 B。在階層中，使用者 1 看不到虛擬機器 A 和 B。

圖 2-7. 範例 3：使用者權限覆寫群組權限



管理 vCenter Server 元件的權限

將在 vCenter Server 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)。

如需有關權限的概念資訊，請參閱[瞭解物件層級權限模型](#)中的討論。

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[vSphere 中的權限階層式繼承](#)。您還可以为某個全域根物件指派散佈權限，以將權限套用到所有解決方案中的所有物件。請參閱[使用 vCenter Server 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。透過將物件移至資料夾並在資料夾上設定權限，您可以將相同的散佈權限同時指派給多個物件。

當您指派權限時，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 Client 物件瀏覽器中，瀏覽到您想要為其指派權限的物件。
- 2 按一下**權限**索引標籤。
- 3 按一下**新增**。
- 4 (選擇性) 如果您已設定外部身分識別提供者進行同盟驗證，則可在**網域**下拉式功能表中選取該身分識別提供者的網域。

- 5 選取將獲得由所選角色定義之權限的使用者或群組。
 - a 從**網域**下拉式功能表中，選取使用者或群組的網域。
 - b 在 [搜尋] 方塊中輸入名稱。
系統會搜尋使用者和群組名稱。
 - c 選取使用者或群組。
- 6 從**角色**下拉式功能表中選取角色。
- 7 (選擇性) 若要散佈權限，選取**散佈到子系核取方塊**。
角色僅會套用到選取的物件，並散佈到子系物件。
- 8 按一下**確定**。

變更或移除詳細目錄物件的權限

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**散佈到子系核取方塊**的設定。您也可以移除權限設定。

程序

- 1 在 vSphere Client 物件導覽器中瀏覽到物件。
- 2 按一下**權限**索引標籤。
- 3 按一下資料列以選取權限。

工作	步驟
變更權限	<ol style="list-style-type: none"> a 按一下編輯。 b 從角色下拉式功能表，為使用者或群組選取角色。 c 切換散佈到子系核取方塊以變更權限繼承。 d 按一下確定。
移除權限	<ol style="list-style-type: none"> a 按一下刪除。 b 按一下移除。

變更 vCenter Server 使用者驗證設定

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

這些設定適用於 vCenter Single Sign-On 身分識別來源，而不是可能與 vCenter Server 相關聯的外部身分識別來源，例如 Active Directory。

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

程序

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

- 2 選取**設定**，然後按一下**設定 > 一般**。
- 3 按一下**編輯**，然後選取**使用者目錄**。
- 4 視需要變更值，然後按一下**儲存**。

選項	說明
使用者目錄逾時	搜尋此 vCenter Server 安裝的逾時間隔 (以秒為單位)。
查詢限制	開啟以設定 vCenter Server 顯示的使用者和群組數目上限。
查詢限制大小	所選網域中 vCenter Server 在 選取使用者或群組 對話方塊中顯示的使用者和群組數目上限。如果輸入 0 (零)，將出現所有使用者和群組。

使用 vCenter Server 全域權限

在 vCenter Server 中，全域權限會套用到跨 VMware 解決方案的全域根物件。在內部部署 SDDC 中，全域權限可能會跨越 vCenter Server 和 vRealize Orchestrator。但對於任何 vSphere SDDC，全域權限適用於標籤和內容程式庫等全域物件。

您可以將全域權限指派給使用者或群組，並決定每個使用者或群組的角色。角色決定了使用者或群組針對階層中所有物件所具有的權限集。您可以指派預先定義的角色，或建立自訂角色。請參閱[使用 vCenter Server 角色指派權限](#)。

區分 vCenter Server 權限和全域權限是十分重要的。

表 2-1. vCenter Server 權限與全域權限之間的差異

權限類型	說明
vCenter Server	vCenter Server 權限適用於詳細目錄階層中的特定物件，如主機、虛擬機器、資料存放區等。指派 vCenter Server 權限後，指定某使用者或群組具有該物件上的角色 (一組權限)。
全域	<p>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。全域權限也適用於標籤和內容程式庫等全域物件。請參閱標籤物件的 vCenter Server 權限。</p> <p>如果您指派了全域權限且未選取 [散佈]，則此權限相關聯的使用者或群組將沒有存取階層中物件的權限。這些使用者或群組將只能存取部分全域功能 (例如建立角色)。</p>

新增全域權限

您可以使用全域權限為部署中所有詳細目錄階層的所有物件指定使用者或群組權限。

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

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 使用 vSphere Client 登入 vCenter Server。
- 2 在 [存取控制] 區域中，選取**管理**並按一下**全域權限**。
- 3 從**權限提供者**下拉式功能表中選取網域。
- 4 (選擇性) 如果您已設定外部身分識別提供者進行同盟驗證，則可在**網域**下拉式功能表中選取該身分識別提供者的網域。
- 5 按一下**新增**。
- 6 選取將獲得由所選角色定義之權限的使用者或群組。
 - a 從**網域**下拉式功能表中，選取使用者或群組的網域。
 - b 在 [搜尋] 方塊中輸入名稱。
系統會搜尋使用者和群組名稱。
 - c 選取使用者或群組。
- 7 從**角色**下拉式功能表中選取角色。
- 8 決定是否要選取**散佈到子系**核取方塊來散佈權限。
如果您指派了全域權限且未選取**散佈到子系**，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)。
- 9 按一下**確定**。

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

僅全域權限或指派至標籤物件的權限適用

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

例如，如果您將**指派 vSphere 標籤**權限授與主機 TPA 上的使用者 Dana，該權限不會影響 Dana 是否可在主機 TPA 上指派標籤。Dana 必須擁有頂層的**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 2-2. 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，即頂層物件上指派的權限，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頂層的使用者 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，Robin 擁有標籤 [生產] 的權限，因為他擁有從頂層散佈的全域權限。除非您修改全域權限，否則您無法限制權限。

表 2-3. 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。

備註 此行為不同於繼承 vCenter Server 權限的方式。在 vCenter Server 中，為子物件定義的權限一律覆寫從父系物件散佈的權限。

表 2-4. 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 vCenter Server 角色指派權限

在 vCenter Server 中，角色是一組預先定義的權限，用於定義執行動作和讀取內容的權限。透過將角色指派給物件的使用者或群組來建立權限。vCenter Server 預設會提供系統角色和範例角色。也可建立自訂角色。

在 vCenter Server 中指派權限

在 vCenter Server 中指派權限時，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。例如，可以使用虛擬機器使用者範例角色允許使用者讀取和變更虛擬機器屬性。

單一使用者或群組針對詳細目錄中的不同物件可能有不同角色。例如，假設您的詳細目錄中有兩個資源集區 (集區 A 和集區 B)。您可以為群組 Sales 在集區 A 上指派虛擬機器使用者範例角色，而在集區 B 上指派唯讀角色。執行上述指派後，群組 Sales 中的使用者可以開啟集區 A 中的虛擬機器，但只能檢視集區 B 中的虛擬機器。

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。

什麼是預先定義的 vCenter Server 角色

如下表所示，vCenter Server 提供預先定義的角色。

表 2-5. 預先定義的 vCenter Server 角色

角色類型	角色名稱	說明
系統	管理員、唯讀和無存取權。	系統角色是永久的。您無法刪除系統角色，也無法編輯與這些角色關聯的權限。系統角色按階層進行組織。每個角色都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。如需有關系統角色的更多詳細資料，請參閱以下一節。
範例	vSphere 提供了許多範例角色，例如 AutoUpdateUser、資源集區管理員和虛擬機器使用者。	vSphere 為某個頻繁執行的工作組合提供範例角色。您可複製、修改或移除這些角色。 備註 若要避免遺失範例角色中預先定義的設定，請先複製該角色，然後對複製品進行修改。無法將範例重設為預設設定。

若要檢視與某個角色相關聯的權限，請在 vSphere Client 中導覽到該角色 (**功能表 > 系統管理 > 角色**)，然後按一下**權限索引**標籤。

若要檢視所有 vSphere 權限和說明，請參閱第 16 章 **定義的權限**。

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 系統角色

無法更改或刪除系統角色。

管理員角色

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

如果您充當的是 vCenter Server 中的管理員角色，則可以將權限指派給預設 vCenter Single Sign-On 身分識別來源中的使用者和群組。如需支援的身分識別服務，請參閱 vSphere 驗證說明文件。

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。

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

唯讀角色

具有某物件之唯讀角色的使用者能夠檢視該物件的狀態和有關該物件的詳細資料。例如，具有此角色的使用者可檢視虛擬機器、主機以及資源集區屬性，但無法檢視主機的遠端主控台。透過功能表和工具列執行的所有動作均會遭到禁止。

無存取權角色

具有某物件之無存取權角色的使用者無法以任何方式檢視或變更該物件。依預設，新的使用者和群組會指派此角色。您可以逐物件地變更角色。

vCenter Single Sign-On 網域的管理員 (依預設為 administrator@vsphere.local)、根使用者以及 vpxuser 將依預設獲指派管理員角色。依預設，其他使用者將獲指派無存取權角色。

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 Client 中的角色編輯功能建立自訂角色，以建立符合您需求的權限集。

ESXi 自訂角色

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

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

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

備註 新增自訂角色但不為其指派任何權限時，系統會將角色建立為擁有三個系統定義之權限的唯讀角色：**系統.匿名**、**系統.檢視**以及**系統.讀取**。這些權限不會顯示在資料 vSphere Client 中，但將用來讀取某些受管理物件的特定內容。vCenter Server 中所有預先定義的角色都包含這三個系統定義的權限。如需詳細資訊，請參閱 vSphere Web Services API 說明文件。

建立 vCenter Server 自訂角色

為了滿足環境的存取控制需求，可以建立 vCenter Server 自訂角色。您可以建立角色，或複製現有角色。

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

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 使用 vSphere Client 登入 vCenter Server。
- 2 選取**管理**，然後按一下**存取控制**區域中的**角色**。
- 3 建立角色。

選項	說明
建立角色	<ol style="list-style-type: none"> 按一下新增。 輸入新角色的名稱。 選取和取消選取該角色的權限。 捲動權限類別，然後為該類別選取所有權限或一部分權限。可以顯示所有、已選取或未選取的類別。還可以顯示所有、已選取或未選取的權限。如需詳細資訊，請參閱第 16 章 定義的權限。 按一下建立。
透過複製建立角色	<ol style="list-style-type: none"> 選取角色，然後按一下複製。 輸入角色的名稱。 按一下確定。 <p>備註 在建立複製角色時，您無法變更權限。若要變更權限，請選取複製的角色，然後按一下編輯。</p>

後續步驟

您現在可以透過選取某個物件，並將角色指派給該物件的使用者或群組來建立權限。

針對 vCenter Server 角色和權限的最佳做法

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

在 vCenter Server 環境中設定角色和權限時，請遵循下列最佳做法：

- 可以的話，請將角色指派給群組，而不是個別使用者。
- 僅在有需要的物件上授與權限，並且僅將權限指派給必須具有這些權限的使用者或群組。使用最少權限數可以更輕鬆地瞭解和管理權限結構。
- 如果要為群組指派限制性角色，請確定該群組不包含管理員使用者或其他具有管理權限的使用者。否則，您可能無意中限制了詳細目錄階層組成部分 (已從中向該群組指派了限制性角色) 中管理員的權限。
- 將物件分組到資料夾中，以便更輕鬆地指派權限。例如，若要在某一組主機上授與修改權限，而在另一組主機上授與檢視權限，請將每組主機置於一個資料夾中。
- 將權限新增到根 vCenter Server 物件時，請務必謹慎。具有根層級權限的使用者有權存取 vCenter Server 上的全域資料，如角色、自訂屬性、vCenter Server 設定。
- 當您將權限指派給物件時，請考慮啟用傳播。傳播可確保物件階層中的新物件繼承權限。例如，您可以為虛擬機器資料夾指派權限並啟用傳播，以確保此權限會套用於資料夾中的所有虛擬機器。
- 使用無存取權角色來遮罩階層的特定區域。無存取權角色會限制具有該角色的使用者或群組的存取權。
- 對授權的變更會傳播到相同 vCenter Single Sign-On 網域中的所有連結 vCenter Server 系統。
- 即使使用者沒有所有 vCenter Server 系統的權限，授權傳播仍會進行。

一般工作所需的 vCenter Server 權限

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

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

若要瞭解 vSphere Client 使用者介面中的作業如何與 API 呼叫相對應以及執行作業需要哪些權限，請參閱《vSphere Web Services API 參考》說明文件。例如，AddHost_Task(addHost) 方法對應的 API 說明文件規定，向叢集新增主機需要擁有 Host.Inventory.AddHostToCluster 權限。

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

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

表 2-6. 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.編輯詳細目錄.新建 ■ 虛擬機器.變更組態.新增磁碟(如果要建立新的虛擬磁碟) ■ 虛擬機器.變更組態.新增現有磁碟(如果使用現有虛擬磁碟) ■ 虛擬機器.組態.設定原始裝置(如果使用 RDM 或 SCSI 傳遞裝置) 	管理員
	在目的地主機、叢集或資源集區上： 資源.將虛擬機器指派給資源集區	資源集區管理員 或管理員
	在目的地資料存放區或包含資料存放區的資料夾上： 資料存放區.配置空間	資料存放區取用 者或管理員
	在將虛擬機器指派到的網路上： 網路.指派網路	網路取用者或管 理員
開啟虛擬機器電源	在已部署虛擬機器的資料中心上： 虛擬機器.互動.開啟電源	虛擬機器超級使 用者或管理員
	在虛擬機器或虛擬機器資料夾上： 虛擬機器.互動.開啟電源	
從範本部署虛擬機器	在目的地資料夾或資料中心上： <ul style="list-style-type: none"> ■ 虛擬機器.編輯詳細目錄.從現有項目建立 ■ 虛擬機器.變更組態.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： <ul style="list-style-type: none"> ■ 資源.將虛擬機器指派給資源集區 ■ vApp.匯入 	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
	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.編輯詳細目錄.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 2-6. 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： <ul style="list-style-type: none"> ■ 主機.詳細目錄.新增主機至叢集 ■ 主機.詳細目錄.修改叢集 	管理員

表 2-6. 一般工作所需的權限 (續)

工作	所需權限	適當角色
使用 vSphere Client 將單一主機新增到資料中心，或使用 PowerCLI 或 API (利用 addHost API) 將單一主機新增到叢集	在主機上： 主機.詳細目錄.新增主機至叢集	管理員
	在叢集上： ■ 主機.詳細目錄.修改叢集 ■ 主機.詳細目錄.新增主機至叢集	管理員
	在資料中心上： 主機.詳細目錄.新增獨立主機	管理員
將多個主機新增至叢集	在叢集上： ■ 主機.詳細目錄.修改叢集 ■ 主機.詳細目錄.新增主機至叢集	管理員
	在叢集 (具有散佈權限) 的父系資料中心上： ■ 主機.詳細目錄.新增獨立主機 ■ 主機.詳細目錄.移動主機 ■ 主機.詳細目錄.修改叢集 ■ 主機.組態.維護	管理員
加密虛擬機器	只能在包含 vCenter Server 的環境中執行加密工作。此外，ESXi 主機必須為大多數加密工作啟用加密模式。執行此工作的使用者必須擁有適當的權限。一組 密碼編譯作業 權限允許進行更為精細的控制。請參閱 虛擬機器加密工作的必要條件和所需權限 。	管理員
保護虛擬機器 (如果使用 vSphere+ 保護虛擬機器)	在已部署虛擬機器的資料中心上： ■ vSphere 標記.指派或取消指派 vSphere 標籤	管理員

保護 ESXi 主機

3

ESXi Hypervisor 架構具有許多內建安全性功能，包括 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，但一般而言，會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。ESXi 主機參與了憑證基礎結構。依預設，VMware Certificate Authority (VMCA) 會使用將 VMCA 做為根憑證授權機構的已簽署憑證佈建每台新的 ESXi 主機。

備註 ESXi 並非基於 Linux 核心或商用 Linux 發行版建立。它使用自己的 VMware 專用及專屬的核心與軟體工具，以獨立單位形式提供，且不包含 Linux 發行版中的應用程式和元件。

本章節討論下列主題：

- [ESXi 一般安全建議](#)
- [管理 ESXi 主機的憑證](#)
- [自訂 ESXi 主機安全性](#)
- [為 ESXi 主機指派權限](#)
- [使用 Active Directory 管理 ESXi 使用者](#)
- [使用 vSphere Authentication Proxy](#)
- [設定和管理用於 ESXi 的智慧卡驗證](#)
- [使用 ESXi Shell](#)
- [ESXi 主機的 UEFI 安全開機](#)
- [使用信賴平台模組保護 ESXi 主機](#)
- [ESXi 記錄檔](#)
- [確保 Fault Tolerance 記錄流量的安全](#)
- [管理 ESXi 稽核記錄](#)
- [保護 ESXi 組態安全](#)
- [停用 execInstalledOnly 進階組態執行階段選項](#)

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。若要滿足組態需求，可以放寬限制。若要放寬限制，請確定在受信任的環境中運作且採取了其他安全性措施。

什麼是 ESXi 內建安全性功能？

如下所示，ESXi 可降低主機的風險：

- 依預設，ESXi Shell 介面和 SSH 介面處於停用狀態。除非執行疑難排解或支援活動，否則，請將這些介面保持停用狀態。對於日常活動，請使用 vSphere Client，其中活動受到角色型存取控制和現代存取控制方法的約束。
- 依預設，僅部分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防火牆連接埠。
- 依預設，所有連接埠（並非對主機進行管理存取所需）均處於關閉狀態。請在需要其他服務時開啟連接埠。
- 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，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 交換。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 使用內部 Web 服務來支援透過 Web Client 進行存取。此服務已經過修改，僅執行 Web Client 進行管理和監控所需的功能。因此，ESXi 不易遇到在更廣泛的應用中所報告的 Web 服務安全性問題。
- 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）。您可以訂閱 VMware 安全性摘要報告和安全性警示郵寄清單，以接收安全性警示。請參閱網頁，網址為 <http://lists.vmware.com/mailman/listinfo/security-announce>。
- 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。
- 若要防止主機載入未經密碼編譯簽署的驅動程式和應用程式，請使用 UEFI 安全開機。將在系統 BIOS 中完成啟用安全開機的操作。ESXi 主機上不需要額外的組態變更，例如，磁碟分割。請參閱 [ESXi 主機的 UEFI 安全開機](#)。
- 如果您的 ESXi 主機具有 TPM 2.0 晶片，則在系統 BIOS 中啟用並設定該晶片。TPM 2.0 與安全開機一起運作，可增強安全性和提供硬體信任保證。請參閱 [使用信賴平台模組保護 ESXi 主機](#)。

採取更多 ESXi 安全性措施

評估主機安全性和管理時，請考慮以下建議。

限制對 ESXi 主機的存取

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

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

不直接存取受管理的 ESXi 主機

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

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

僅將 DCUI 用於疑難排解

僅為了疑難排解才以根使用者身分從 DCUI 或 ESXi Shell 存取主機。若要管理 ESXi 主機，請使用 vSphere Client (或 VMware Host Client) 或其中一個 VMware CLI 或 API。請參閱 ESXCLI 概念和範例，網址為 <https://code.vmware.com/>。如果您使用 ESXi Shell 或 SSH，請限制具有存取權的帳戶並設定逾時。

僅使用 VMware 來源以升級 ESXi 元件

主機執行多個第三方套件來支援管理介面或必須執行的工作。VMware 僅支援升級至這些來自 VMware 來源的套件。如果使用來自另一個來源的下載內容或修補程式，可能會危及管理介面的安全性或功能。檢查第三方廠商網站和 VMware 知識庫，取得安全性警示。

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

ESXi 進階系統設定

進階系統設定控制 ESXi 行為的各個方面，例如記錄、系統資源和安全性。

下表展示了安全性方面的一些重要 ESXi 進階系統設定。若要檢視所有進階系統設定，請查看 vSphere Client (主機 > 設定 > 系統 > 進階系統設定) 或適用於指定版本的 API。

表 3-1. 安全性進階系統設定部分清單

進階系統設定	說明	預設值
Annotations.WelcomeMessage	在 Host Client 中登入之前顯示歡迎訊息，或者在 DCUI 中的預設螢幕上顯示歡迎訊息。在 DCUI 中，歡迎訊息會取代某些文字，例如主機 IP 位址。	(空白)
Config.Etc.issue	在 SSH 登入工作階段期間顯示橫幅。可使用後置換行符號以實現最佳效果。	(空白)
Config.Etc.motd	在 SSH 登入時顯示當天的訊息。	(空白)
Config.HostAgent.vmacore.soap.sessionTimeout	設定系統自動登出 VIM API 之前的閒置時間 (以分鐘為單位)。值為 0 (零) 表示停用閒置時間。此設定僅適用於新工作階段。	30 (分鐘)

表 3-1. 安全性進階系統設定部分清單 (續)

進階系統設定	說明	預設值
Mem.MemEagerZero	在虛擬機器結束後，啟用 VMkernel 作業系統 (包括 VMM 程序) 中的使用者環境和客體記憶體頁面歸零。預設值 (0) 表示使用消極式歸零。值為 1 表示使用積極式歸零。	0 (已停用)
Security.AccountLockFailures	<p>設定系統鎖定使用者帳戶之前的失敗登入嘗試次數上限。例如，若要在第五次登入失敗時鎖定帳戶，請將此值設定為 4。值為 0 (零) 表示停用帳戶鎖定。</p> <p>出於實作原因，某些登入機制會意外計數：</p> <ul style="list-style-type: none"> ■ VIM 登入 (包括 VMware Host Client) 和 ESXCLI 反映確切的失敗登入次數。 ■ 在顯示密碼提示時，SSH 連線計為一次登入嘗試，在成功登入時復原該計數。此行為在查問和回應通訊中正常。 ■ CGI 登入重複計算登入失敗次數。 <p>注意 由於此問題，使用 CGI 介面時，使用者鎖定的速度可能比失敗登入次數更快。</p>	5
Security.AccountUnlockTime	設定使用者被鎖定的秒數。指定鎖定逾時內的任何登入嘗試將重新啟動鎖定逾時。	900 (15 分鐘)
Security.PasswordHistory	設定需記住用於每個使用者的密碼數目。此設定可防止重複或類似的密碼。	0
Security.PasswordMaxDays	設定兩次變更密碼之間的天數上限。	99999

表 3-1. 安全性進階系統設定部分清單 (續)

進階系統設定	說明	預設值
Security.PasswordQualityControl	<p>在 Pam_passwdqc 組態中變更所需長度 and 字元類別需求，或允許使用複雜密碼。可以在密碼中使用特殊字元。密碼長度可以至少為 15 個字元。預設設定需要三類字元，且最小長度為七個字元。</p> <p>如果實作 DoD Annex，可以結合使用 similar=deny 選項與最小密碼長度，以強制執行密碼完全不同的需求。僅對透過 VIM LocalAccountManager.changePassword API 變更的密碼強制執行密碼歷程記錄設定。若要變更密碼，則要求使用者具有管理員權限。PasswordQualityControl 設定和 PasswordMaxDays 設定滿足 DoD Annex 的需求：</p> <pre>min=disabled,disabled,disabled,disabled,15 similar=deny</pre>	<p>retry=3</p> <p>min=disabled,disabled,disabled,7,7</p>
UserVars.DcuiTimeOut	設定系統自動登出 DCUI 之前的閒置時間 (以秒為單位)。值為 0 (零) 表示停用逾時。	600 (10 分鐘)
UserVars.ESXiShellInteractiveTimeOut	設定系統自動登出互動式 shell 之前的閒置時間 (以秒為單位)。此設定僅對新工作階段生效。值為 0 (零) 表示停用閒置時間。同時適用於 DCUI 和 SSH shell。	0
UserVars.ESXiShellTimeOut	設定登入 shell 等待登入的時間 (以秒為單位)。值為 0 (零) 表示停用逾時。同時適用於 DCUI 和 SSH shell。	0
UserVars.HostClientSessionTimeout	設定系統自動登出 Host Client 之前的閒置時間 (以秒為單位)。值為 0 (零) 表示停用閒置時間。	900 (15 分鐘)
UserVars.HostClientWelcomeMessage	在 Host Client 中登入時顯示歡迎訊息。該訊息在登入後以「提示」形式加以顯示。	(空白)

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。

主機設定檔為主機組態和組態符合性提供一種自動化的集中管理機制。主機設定檔可以減少對重複性的手動工作的依賴，提高效率。主機設定檔會擷取預先設定和驗證的參考主機組態，將該組態儲存為受管理物件，並使用其中包含的參數目錄來設定網路、儲存區、安全性及其他主機層級的參數。

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

您可以將主機設定檔附加至叢集，以將其套用至叢集中的所有主機。

程序

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

使用指令碼管理 ESXi 主機組態設定

在擁有多台 ESXi 主機的環境中，與從 vSphere 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 包括用於 ESXi 主機管理的指令碼語言。VMware PowerCLI 是 vSphere API 的 Windows PowerShell 介面，包含用於管理 vSphere 元件的 PowerShell cmdlet。ESXCLI 包含用於管理 ESXi 主機和虛擬機器的命令集。如需參考資訊和程式設計提示，請參閱 <https://developer.vmware.com>。

《vSphere 管理員》說明文件重點介紹如何使用 vSphere Client 進行管理。

您也可以使用 vSphere Automation SDK 的其中一個指令碼介面，如 vSphere Automation SDK for Python。

程序

- 1 建立擁有限制權限的自訂角色。

請參閱[建立 vCenter Server 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 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
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。

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` 進階系統設定變更必要長度及字元類別需求或允許使用複雜密碼。還可以使用 `Security.PasswordHistory` 進階系統設定來設定需記住用於每個使用者的密碼數目。

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` 進階系統設定檢查並變更預設密碼限制。

ESXi 密碼

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

- 依預設，建立密碼時，必須包括以下四類字元中至少三類字元的組合：小寫字母、大寫字母、數字和特殊字元 (如底線或破折號)。
- 依預設，密碼長度至少為 7 個字元，且少於 40 個字元。
- 密碼不得包含字典字組或部分字典字組。

- 密碼不得包含使用者名稱或部分使用者名稱。

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。密碼內使用的字典字組可降低整體密碼強度。

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，如果新密碼的強度不夠或兩次未正確輸入密碼，則會提示使用者最多輸入三次 (retry=3)。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。如需有關其他選項 (例如 max、passphrase 等) 的詳細資料，請參閱 `pam_passwdqc` 手冊頁。

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

還可以使用複雜密碼代替密碼。但是，複雜密碼預設為停用。您可以使用 vSphere Client 的 `Security.PasswordQualityControl` 進階系統設定變更預設設定和其他設定。

例如，您可將該選項變更為下列內容。

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

此範例允許至少使用 16 個字元及 3 個字組的複雜密碼。

在舊版主機中仍然支援變更 `/etc/pam.d/passwd` 檔案，但這在未來版本中會被取代。而是使用 `Security.PasswordQualityControl` 進階系統設定。

變更預設密碼限制

您可以使用 ESXi 主機的 `Security.PasswordQualityControl` 進階系統設定變更對密碼或複雜密碼的預設限制。如需變更 ESXi 進階系統設定的相關資訊，請參閱 vCenter Server 和主機管理說明文件。

您可以變更預設值，例如要求至少 15 個字元且至少四個字組 (passphrase=4)，如下所示：

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

請參閱 `pam_passwdqc` 的手冊頁以瞭解詳細資料。

備註 並非所有可能的密碼選項組合都已經過測試。在變更預設密碼設定後執行測試。

以下範例設定了密碼複雜性需求，要求使用四類字元中的 8 個字元並強制顯著的密碼差異、記住五個密碼的歷程記錄以及 90 天輪替原則：

```
min=disabled,disabled,disabled,disabled,8 similar=deny
```

將 `Security.PasswordHistory` 選項設定為 5，並將 `Security.PasswordMaxDays` 選項設定為 90。

ESXi 帳戶鎖定行為

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 5 次嘗試失敗後，帳戶即會鎖定。依預設，帳戶會在 15 分鐘後解除鎖定。

設定登入行為

您可以使用以下進階系統設定來設定 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。零表示停用帳戶鎖定。
- `Security.AccountUnlockTime`. 使用者被鎖定的秒數。
- `Security.PasswordHistory`. 需記住用於每個使用者的密碼數目。零表示停用密碼歷程記錄。

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 產生密碼編譯金鑰

ESXi 會針對一般作業產生多個非對稱金鑰。傳輸層安全性 (TLS) 金鑰使用 TLS 通訊協定保護與 ESXi 主機的通訊。SSH 金鑰使用 SSH 通訊協定保護與 ESXi 主機的通訊。

傳輸層安全性金鑰

傳輸層安全性 (TLS) 金鑰使用 TLS 通訊協定保護與主機的通訊。首次開機時，ESXi 主機會以 2048 位元 RSA 金鑰的形式產生 TLS 金鑰。目前，ESXi 不為 TLS 自動產生 ECDSA 金鑰。TLS 私密金鑰不由管理員進行維護。

TLS 金鑰位於以下非持續性位置：

```
/etc/vmware/ssl/rui.key
```

TLS 公開金鑰 (包括中繼憑證授權機構) 作為 X.509 v3 憑證位於以下非持續性位置：

```
/etc/vmware/ssl/rui.crt
```

將 vCenter Server 與 ESXi 主機搭配使用時，vCenter Server 會自動產生 CSR，使用 VMware Certificate Authority (VMCA) 對其進行簽署，並產生憑證。將 ESXi 主機新增到 vCenter Server 時，vCenter Server 會在該 ESXi 主機上安裝所產生的憑證。

預設 TLS 憑證是自我簽署憑證，且 subjectAltName 欄位與安裝時主機名稱相符。可以安裝不同的憑證，以便使用不同的 subjectAltName 或在驗證鏈結中包含特定的憑證授權機構 (CA) 等。請參閱[取代 ESXi SSL 憑證和金鑰](#)。

還可以使用 VMware Host Client 取代憑證。請參閱 [vSphere 單一主機管理 - VMware Host Client](#)。

SSH 金鑰

SSH 金鑰使用 SSH 通訊協定保護與 ESXi 主機的通訊。首次開機時，系統會產生 nistp256 ECDSA 金鑰，並以 2048 位元 RSA 金鑰的形式產生 SSH 金鑰。依預設，SSH 伺服器處於停用狀態。SSH 存取主要用於疑難排解目的。SSH 金鑰不由管理員進行維護。透過 SSH 登入需要相當於完全主機控制的管理權限。若要啟用 SSH 存取，請參閱[使用 vSphere Client 啟用對 ESXi Shell 的存取](#)。

SSH 公開金鑰位於以下位置：

```
/etc/ssh/ssh_host_rsa_key.pub
```

```
/etc/ssh/ssh_host_ecdsa_key.pub
```

SSH 私密金鑰位於以下位置：

```
/etc/ssh/ssh_host_rsa_key
```

```
/etc/ssh/ssh_host_ecdsa_key
```

TLS 密碼編譯金鑰建立

TLS 密碼編譯金鑰建立的組態由所選 TLS 加密套件進行管理，這些加密套件選取以 RSA 為基礎的金鑰傳輸 (如 NIST 特刊 800-56B 中所指定) 或使用暫時 Elliptic Curve Diffie Hellman (ECDH) 的以 ECC 為基礎的金鑰合約 (如 NIST 特刊 800-56A 中所指定) 之一。

SSH 密碼編譯金鑰建立

SSH 密碼編譯金鑰建立的組態由 SSHD 組態管理。ESXi 提供了一項預設組態，該組態允許以 RSA 為基礎的金鑰傳輸 (如 NIST 特刊 800-56B 中所指定)、暫時 Diffie Hellman (DH) (如 NIST 特刊 800-56A 中所指定) 金鑰合約和暫時 Elliptic Curve Diffie Hellman (ECDH) (如 NIST 特刊 800-56A 中所指定)。SSHD 組態不由管理員進行維護。

ESXi 中的 SSH 安全性

依預設，ESXi Shell 介面和 SSH 介面處於停用狀態。除非執行疑難排解或支援活動，否則，請將這些介面保持停用狀態。對於定期活動，請使用 vSphere Client，其中活動受到角色型存取控制和現代存取控制方法的約束。

ESXi 中的 SSH 組態

ESXi 中的 SSH 組態使用下列設定。

第 1 版 SSH 通訊協定已停用

VMware 不再支援第 1 版 SSH 通訊協定，而是以獨佔方式使用第 2 版通訊協定。第 2 版消除了第 1 版中存在的某些安全性問題，且提供了安全的方式來與管理介面進行通訊。

提高了加密強度

SSH 對連線僅支援 256 位元和 128 位元 AES 加密。

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

ESXi SSH 金鑰

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

您可以使用 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，網址為 <http://kb.vmware.com/kb/1002866>。

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

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>

金鑰類型	位置
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>

PCI 和 PCIe 裝置和 ESXi

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

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

在以下情形下您的主機可能或受到影響。

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

停用 vSphere 受管理物件瀏覽器

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

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

程序

- 1 在 vSphere Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在 [系統] 下，按一下**進階系統設定**。
- 4 檢查 `Config.HostAgent.plugins.solo.enableMob` 的值，然後按一下**編輯**以視情況進行變更。

請勿透過 ESXi Shell 使用 `vim-cmd`。

ESXi 網路安全性建議

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

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

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

修改 ESXi Web 代理設定

修改 Web 代理設定時，需要考慮若干加密和使用者安全性準則。

備註 對主機目錄或驗證機制做出任何變更之後重新啟動主機程序。

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

僅當為這些用戶端建立了完全受信任的環境時才可考慮停用 SSL，在這樣的環境中，安裝有防火牆，而且與主機之間的傳輸是完全隔離的。停用 SSL 可提高效能，因為避免了執行加密所需的額外負荷。

- 為了防止誤用 ESXi 服務，大多數內部 ESXi 服務只能透過連接埠 443 (用於 HTTPS 傳輸的連接埠) 來存取。連接埠 443 可充當 ESXi 的反向 Proxy。透過 HTTP 歡迎分頁可看到 ESXi 上的服務清單，但如果未經適當授權，則無法直接存取儲存裝置介面卡服務。

可對此組態進行變更，以便可透過 HTTP 連線直接存取個別服務。除非是在完全受信任的環境中使用 ESXi，否則不要進行此變更。

- 在升級您的環境時，憑證仍然保留在原位。

vSphere Auto Deploy 安全考量

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

網路安全性

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

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

開機映像和主機設定檔安全性

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

- 開機映像中永遠包括組成映像設定檔的 VIB 套件。
- 如果 Auto Deploy 規則是設定為使用主機設定檔或主機自訂來佈建主機，則開機映像中便包含主機設定檔和主機自訂。
 - 主機設定檔和主機自訂隨附的管理員 (根) 密碼和使用者密碼已使用 SHA-512 進行雜湊處理。
 - 與設定檔相關聯的任何其他密碼均採用明文形式。如果使用主機設定檔設定 Active Directory，則密碼不受保護。

請使用 vSphere Authentication Proxy 來避免公開 Active Directory 密碼。如果使用主機設定檔設定 Active Directory，則密碼不會受到保護。

- 主機的公開和私密 SSL 金鑰和憑證都包含在開機映像中。

控制以 CIM 為基礎的硬體監控工具的存取

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

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

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

請勿為存取 CIM 介面的遠端應用程式提供根認證。相反，為這些應用程式建立權限較低的 vSphere 使用者帳戶，並使用 VIM API 票證功能將 sessionId (稱為「票證」) 核發至此權限較低的使用者帳戶以向 CIM 進行驗證。如果帳戶已被授與取得 CIM 票證的權限，VIM API 會向 CIM 提供票證。然後，這些票證會做為使用者識別碼和密碼提供給任何 CIM-XML API 呼叫。如需詳細資訊，請參閱

AcquireCimServicesTicket() 方法。

安裝第三方 CIM VIB 時會啟動 CIM 服務，例如，當您執行 `esxcli software vib install -n VIBname` 命令時。

如果您必須手動啟用 CIM 服務，請執行下列命令：

```
esxcli system wbem set -e true
```


如有必要，您可以停用 wsman (WSManagement 服務)，以便只有 CIM 服務正在執行：

```
esxcli system wbem set -W false
```

若要確認 wsman 已停用，請執行下列命令：

```
esxcli system wbem get
...
WSManagement PID: 0
WSManagement Service: false
```

如需有關 ESXCLI 命令的詳細資訊，請參閱 ESXCLI 說明文件。如需有關啟用 CIM 服務的詳細資訊，請參閱 VMware 知識庫文章，網址為：<https://kb.vmware.com/kb/1025757>。

程序

- 1 為 CIM 應用程式建立 vSphere 非 root 使用者帳戶。

請參閱 vSphere 驗證中有關新增 vCenter Single Sign-On 使用者的主題。使用者帳戶所需的 vSphere 權限為 **Host.CIM.Interaction**。

- 2 使用您所選擇的 vSphere API SDK 向 vCenter Server 驗證使用者帳戶。然後，使用 CIM-XML 連接埠 5989 或 WS-Man 連接埠 433 API，以管理員層級帳戶的身分呼叫

`AcquireCimServicesTicket()` 傳回票證以向 ESXi 進行驗證。

如需詳細資訊，請參閱《vSphere Web Services API 參考》。

- 3 視需要每兩分鐘更新一次票證。

vSphere Distributed Services Engine 安全性最佳做法

為了盡可能地提高 ESXi 環境的安全性，請遵循 vSphere Distributed Services Engine 的最佳做法。

從 vSphere 8.0 開始，vSphere Distributed Services Engine 支援將基礎結構功能從主機或伺服器的 CPU 卸載到資料處理裝置 (DPU，也稱為 SmartNIC)，從而釋放 CPU 週期來為應用程式提供服務。如需 vSphere Distributed Services Engine 的相關介紹，請參閱 VMware ESXi 安裝和設定說明文件。如需有關 vSphere Distributed Services Engine 的詳細資訊，請參閱管理主機和叢集生命週期說明文件。

通常，請像保護 ESXi 環境那樣處理 vSphere Distributed Services Engine 的安全方面。

- 依預設，vSphere Distributed Services Engine 的 ESXi Shell 介面和 SSH 介面處於停用狀態。除非執行疑難排解或支援活動，否則，請將這些介面保持停用狀態。
- 對於 vSphere Distributed Services Engine 的日常管理活動，請使用 vSphere Client，其中活動受到角色型存取控制和現代存取控制方法的約束。

控制 ESXi 熵

從 vSphere 8.0 開始，ESXi 熵實作支援 FIPS 140-3 和 EAL4 憑證。核心開機選項可控制要在 ESXi 主機上啟用哪些熵來源。

在計算中，「熵」這個詞彙是指收集用於加密的隨機字元和資料，例如產生加密金鑰以確保透過網路傳輸的資料的安全性。在產生金鑰並透過網路進行安全通訊時，需要熵來確保安全性。熵通常是從系統上的各種來源收集的。

如果滿足以下條件，則 FIPS 熵處理是預設行為。

- 1 硬體支援 RDSEED。
- 2 disableHwrng VMkernel 開機選項不存在或為 FALSE。
- 3 entropySources VMkernel 開機選項不存在、為 0 (零) 或為 4。

可以使用以下 VMkernel 開機選項設定 ESXi Entropy 子系統：

表 3-2. ESXi Entropy VMkernel 開機選項

VMkernel 開機選項	選項類型	說明	預設值
disableHwrng (在 vSphere 8.0 之前可用)	布林值	設定為 TRUE (覆寫「entropySources」) 時停用 RDRAND 和 RDSEED 熵來源。	FALSE 啟用硬體隨機數字產生器熵來源 (如果存在)。
entropySources (從 vSphere 8.0 開始可用)	整數，位元遮罩	指定要啟用的熵來源。 ■ 0=全部 ■ 1=中斷 ■ 2=rdrand ■ 4=rdseed ■ 8=使用者空間 (已啟用 EAL4 熵處理) 指定 entropySources=9 會啟用中斷和使用者空間熵來源，並停用 rdrand 和 rdseed 熵來源。	0 (零) 啟用所有可用的熵來源。

備註 在做出變更以僅使用 RDRAND、RDSEED 或同時使用兩個熵來源之前，請查看廠商說明文件，確保 ESXi 主機支援這些組態。如果主機不支援這些組態，vCenter Server 會顯示一則警示通知您，並且主機會回復為使用中斷和使用者空間熵來源。

必要條件

您必須在 ESXi 主機上具有根存取權。

程序

- 1 使用 SSH 或其他遠端主控台連線，以啟動 ESXi 主機上的工作階段。
- 2 以 root 身分登入。

3 設定所需的熵 VMkernel 開機選項。

- a 若要為 disableHwrng 停用 RDRAND 和 RDSEED 熵來源，請執行以下作業：

```
esxcli system settings kernel set -s disableHwrng -v TRUE
```

- b 若要設定熵來源，請執行以下作業：

```
esxcli system settings kernel set -s entropySources -v entropy_source_value
```

如需可為 entropySources 設定的值，請參閱上述資料表。

管理 ESXi 主機的憑證

VMware Certificate Authority (VMCA) 預設會使用將 VMCA 做為根憑證授權機構的已簽署憑證佈建每台新的 ESXi 主機。當主機明確新增至 vCenter Server，或在安裝或升級至 ESXi 的過程中新增時，會執行佈建。

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

vSphere 中的憑證

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

vCenter Server 支援 ESXi 主機的以下憑證模式。

表 3-3. 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 或中繼 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 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或企業 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 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 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.x 之後援選項的形式提供。在此模式中，vCenter Server 會檢查憑證是否已正確格式化，但不會檢查憑證的有效性。即使憑證已到期亦可接受。</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 Server 6.x 及更新版本的某些服務可能無法正常運作。</p>

ESXi 憑證到期

您可以在 vSphere 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 佈建和憑證

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。

您還可以將第三方或企業 CA 簽署的自訂憑證用於 ESXi 主機。

Auto Deploy 中的 ESXi 佈建和憑證

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

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

您可以將 Auto Deploy 設為第三方憑證授權機構的下層憑證授權機構。在此情況下，產生的憑證會使用 Auto Deploy SSL 金鑰進行簽署。請參閱[將 Auto Deploy 設為下層憑證授權機構](#)。

從 8.0 開始，您可以將自訂憑證 (憑證授權機構簽署的憑證) 與 Auto Deploy 搭配使用。主機啟動時，Auto Deploy 會將自訂憑證與 ESXi 主機的 MAC 位址或 BIOS UUID 相關聯。請參閱[透過 Auto Deploy 使用自訂憑證](#)。

ESXi 憑證管理所需的權限

使用者需要擁有 **憑證.管理憑證** 權限才能管理 ESXi 主機憑證。

ESXi 主機名稱和 IP 位址變更

ESXi 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 ESXi 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 3-4. 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 ESXi 主機新增至 vCenter Server...	ESXi 主機名稱變更	ESXi 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 主機升級和憑證

如果您將 ESXi 主機升級到 ESXi 6.5 或更新版本，升級程序會將自我簽署 (指紋) 的憑證取代為 VMCA 簽署的憑證。如果 ESXi 主機使用自訂憑證，則升級程序會保留這些憑證，即使這些憑證已過期或無效也如此。

建議的升級工作流程取決於目前的憑證。

使用指紋憑證佈建的主機

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

備註 您無法使用 VMCA 憑證佈建舊版主機。您必須將這些主機升級至 ESXi 6.5 或更新版本。

使用自訂憑證佈建的主機

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

備註 如果您的環境處於 VMCA 模式下，並且您從 vSphere 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 Client 中顯示諸如憑證到期等資訊。

使用 Auto Deploy 佈建的主機

由 Auto Deploy 佈建的主機首次以 ESXi 6.5 或更新版本的軟體開機時，將一律獲指派新憑證。在您升級由 Auto Deploy 佈建的主機時，Auto Deploy 伺服器會針對該主機產生憑證簽署要求 (CSR) 並將其提交給 VMCA。VMCA 會為該主機儲存已簽署的憑證。當 Auto Deploy 伺服器佈建主機時，它會從 VMCA 擷取憑證，並將其納入佈建程序。

您可以搭配使用 Auto Deploy 與自訂憑證。

請參閱 [將 Auto Deploy 設為下層憑證授權機構](#) 和 [透過 Auto Deploy 使用自訂憑證](#)。

ESXi 憑證模式切換工作流程

依預設，VMware Certificate Authority (VMCA) 使用憑證佈建 ESXi。您可以改用自訂憑證模式，或傳統的指紋模式 (用於偵錯目的)。大多數情況下，模式切換具有破壞性，且無需執行。如果您確實需要模式切換，請在開始前檢閱潛在的影響。

vCenter Server 支援 ESXi 主機的以下憑證模式。

憑證模式	說明
VMware Certificate Authority (預設)	依預設，VMware Certificate Authority 用作 ESXi 主機憑證的憑證授權機構 (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 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 Client 管理憑證。
指紋模式	vSphere 5.5 使用的是指紋模式，且此模式仍可做為 vSphere 6.0 的後援選項提供，用於回溯相容性。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 Server 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。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 VMware Endpoint 憑證存放區 (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 ESXi 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。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 中移除第三方 CA 的根憑證。

- 3 切換為 VMCA 模式。請參閱[變更 ESXi 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 ESXi 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。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 ESXi 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 ESXi 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。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 ESXi 憑證模式](#)。
- 5 將主機新增到 vCenter Server 系統。

ESXi 憑證預設設定

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

可以使用 vSphere Client 來變更許多預設設定。請考慮變更組織及位置資訊。請參閱[變更 ESXi 憑證預設設定](#)。

表 3-5. ESXi CSR 設定

參數	預設值	進階選項
金鑰大小	2048	不適用
金鑰演算法	RSA	不適用
憑證簽章演算法	sha256WithRSAEncryption	不適用
一般名稱	主機的名稱，如果主機依主機名稱新增至 vCenter Server。 主機 IP 位址，如果主機依 IP 位址新增至 vCenter Server。	不適用
國家/地區	USA	vpzd.certmgmt.certs.cn.country
電子郵件地址	vmca@vmware.com	vpzd.certmgmt.certs.cn.email
位置 (城市)	Palo Alto	vpzd.certmgmt.certs.cn.localityName
組織單位名稱	VMware 工程	vpzd.certmgmt.certs.cn.organizationalUnitName
組織名稱	VMware	vpzd.certmgmt.certs.cn.organizationName
省/市或州	加利福尼亞	vpzd.certmgmt.certs.cn.state
憑證有效天數。	1825	vpzd.certmgmt.certs.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	vpzd.certmgmt.certs.cn.hardThreshold
vCenter Server 憑證有效性檢查的輪詢間隔。	5 天	vpzd.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	vpzd.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 ESXi 主機升級和憑證 。	vmca 也可以指定指紋或自訂。請參閱 變更 ESXi 憑證模式 。	vpzd.certmgmt.mode

變更 ESXi 憑證預設設定

ESXi 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 Client 中使用 vCenter Server 進階設定來變更 CSR 中的某些預設設定。

請參閱上一個資料表中的預設設定清單。無法變更某些預設值。

程序

- 1 在 vSphere Client 中，選取管理主機的 vCenter Server 系統。
- 2 按一下**設定**，然後按一下**進階設定**。
- 3 按一下**編輯設定**。
- 4 按一下 [名稱] 資料行中的**篩選器**圖示，然後在 [篩選器] 方塊中輸入 `vpzd.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**儲存**。

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，然後重新連線主機或更新憑證。

檢視 ESXi 主機的憑證到期資訊

對於處於 VMCA 模式或自訂模式的 ESXi 主機，可以從 vSphere Client 檢視憑證詳細資料。透過憑證資訊，您可以確定任何憑證是否即將到期。您還可以使用此資訊偵錯憑證問題。

您無法檢視處於指紋模式下的 ESXi 主機的憑證狀態資訊。您可以檢視多個 ESXi 主機或單一 ESXi 主機的資訊。多主機視圖僅顯示「憑證有效期結束日期」資訊。

程序

- 1 使用 vSphere Client 登入 vCenter Server。
- 2 瀏覽詳細目錄清單，並選取 vCenter Server 執行個體。
- 3 取得憑證資訊。

單一主機或多個主機	步驟
Single	<ol style="list-style-type: none"> a 瀏覽到 ESXi 主機。 b 按一下設定。 c 在系統下，按一下憑證。
倍數	<ol style="list-style-type: none"> a 選取主機與叢集 > 主機。 依預設，主機顯示內容不包括憑證狀態。 b 若要顯示或隱藏資料行，請按一下左下角的三列資料行選取器。 c 選取憑證有效期至核取方塊，然後向右側捲動 (如有必要) 以檢視新增的資料行。 當憑證到期時，系統會顯示憑證資訊。 d (可選) 取消選取其他資料行，以便更容易看到您所感興趣的內容。

4 檢閱憑證資訊。

以下資訊僅在單一主機視圖中提供。

欄位	說明
主題	憑證產生期間使用的主題。
簽發者	憑證的簽發者。
有效期自	產生憑證的日期。
有效期至	憑證到期的日期。
狀態	憑證的狀態，為下列其中之一。 <div> <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> </div>

備註 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]。

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](#)。

更新或重新整理 ESXi 憑證

在 ESXi 6.0 及更新版本中，如果 VMware Certificate Authority (VMCA) 向主機指派憑證，您可以從 vSphere 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。如果在憑證到期之前未更新憑證，則中斷主機連線後又將其重新連線時，會使 vCenter Server 更新憑證。將主機重新新增到 vCenter Server 會重新建立信任，並使 vCenter Server 無條件地簽發更新的憑證。

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。

必要條件

確認以下內容：

- ESXi 主機已連線到 vCenter Server 系統。
- vCenter Server 系統和 ESXi 主機之間存在適當的時間同步。
- 可在 vCenter Server 系統和 ESXi 主機之間進行 DNS 解析。
- vCenter Server 系統的 MACHINE_SSL_CERT 和 Trusted_Root 憑證是有效的，且尚未到期。請參閱 VMware 知識庫文章，網址為 <https://kb.vmware.com/s/article/2111411>。
- ESXi 主機未處於維護模式。

程序

1 在 vSphere Client 詳細目錄中瀏覽到主機。

2 按一下**設定**。

3 在**系統**下，按一下**憑證**。

您可以檢視有關所選主機的憑證的詳細資料。

4 按一下**更新或重新整理 CA 憑證**。

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

5 按一下**是**。

變更 ESXi 憑證模式

使用 VMware Certificate Authority (VMCA) 佈建您環境中的 ESXi 主機，除非公司原則要求使用自訂憑證。若要使用含不同根 CA 的自訂憑證，可以編輯 vCenter Server 進階設定 `vpzd.certmgmt.mode`。變更後，主機不再於重新整理憑證時使用 VMCA 憑證自動進行佈建。您負責您環境中的憑證管理。

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

程序

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

2 按一下**設定**，然後按一下 [設定] 下的**進階設定**。

3 按一下**編輯設定**。

4 按一下 [名稱] 資料行中的**篩選器**圖示，然後在 [篩選器] 方塊中輸入 `vpzd.certmgmt` 以僅顯示憑證管理參數。

5 如果您打算管理自己的憑證，請將 `vpzd.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**儲存**。

6 重新啟動 vCenter Server 服務。

如需重新啟動服務的相關資訊，請參閱 vCenter Server 組態說明文件。

取代 ESXi SSL 憑證和金鑰

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

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

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

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

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

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

如需有關針對 ESXi 主機使用 CA 簽署憑證的詳細指示，請參閱 [ESXi 憑證模式切換工作流程](#)。

備註 如果您要取代屬於 vSAN 叢集一部分的 ESXi 主機上的 SSL 憑證，請遵循 VMware 知識庫文章中的步驟進行操作，網址為：<https://kb.vmware.com/s/article/56441>。

■ ESXi 憑證簽署要求的需求

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

■ 取代 ESXi Shell 中的預設憑證和金鑰

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

■ 使用 HTTPS PUT 取代預設憑證

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

■ 更新 vCenter Server TRUSTED_ROOTS 存放區 (自訂憑證)

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

ESXi 憑證簽署要求的需求

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

使用具有下列特性的 CSR：

- 金鑰大小：2048 位元 (下限) 至 16384 位元 (上限) (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、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)。

vSphere 不支援以下憑證。

- 具有萬用字元的憑證。
- 不支援演算法 md2WithRSAEncryption、md5WithRSAEncryption、RSASSA-PSS、dsaWithSHA1、ecdsa_with_SHA1 和 sha1WithRSAEncryption。

如需產生 CSR 的相關資訊，請參閱 VMware 知識庫文章，網址為：<https://kb.vmware.com/s/article/2113926>。

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 Client 啟用 ESXi Shell 或啟用 SSH 流量。
- 所有的檔案傳輸和其他通訊均透過安全 HTTPS 工作階段進行。用於驗證工作階段的使用者必須在主機上擁有主機.設定.進階設定權限。

程序

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

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

- 3 將要使用的憑證複製到 /etc/vmware/ssl。
- 4 將新憑證和金鑰重新命名為 rui.crt 和 rui.key。

5 安裝新憑證之後重新啟動主機。

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

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 Client 啟用 ESXi Shell 或啟用 SSH 流量。
- 所有的檔案傳輸和其他通訊均透過安全 HTTPS 工作階段進行。用於驗證工作階段的使用者必須在主機上擁有主機.設定.進階設定權限。

程序

- 1 備份現有憑證。
- 2 在您的上傳應用程式中，按如下方式處理每個檔案：
 - a 開啟檔案。
 - b 將檔案發佈到以下其中一個位置。

選項	說明
憑證	<code>https://hostname/host/ssl_cert</code>
金鑰	<code>https://hostname/host/ssl_key</code>

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

3 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 \(自訂憑證\)](#)。

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。

備註 如果 vCenter Server 系統也在執行時使用 ESXi 主機上安裝的相同 CA 核發的自訂憑證，則不需要執行此步驟。

程序

1 登入管理 ESXi 主機的 vCenter Server 系統的 vCenter Server shell。

2 若要將新憑證新增到 TRUSTED_ROOTS 存放區，請執行 `dir-cli`，例如：

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_RootCA
```

3 出現提示時，請提供 Single Sign-On 管理員認證。

4 如果您的自訂憑證由中繼 CA 核發，還必須將中繼 CA 新增至 vCenter Server 上的 TRUSTED_ROOTS 存放區，例如：

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_intermediateCA
```

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 ESXi 憑證模式](#)。

將 Auto Deploy 設為下層憑證授權機構

依預設，Auto Deploy 伺服器會使用 VMware Certificate Authority (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憑證授權機構 (CA) 的下層憑證授權機構。

必要條件

- 向 CA 要求憑證。憑證必須符合這些需求。
 - 金鑰大小：2048 位元 (下限) 至 16384 位元 (上限) (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、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/` 目錄中。

2 停止 vSphere Authentication Proxy 服務。

工具	步驟
vCenter Server 管理介面	a 在網頁瀏覽器中，移至 vCenter Server 管理介面 (https://vcenter-IP-address-or-FQDN:5480)。 b 以 root 身分登入。 預設根密碼為部署 vCenter Server 時設定的密碼。 c 按一下 服務 ，然後按一下 VMware vSphere Authentication Proxy 服務 。 d 按一下 停止 。
CLI	<code>service-control --stop vmcam</code>

3 在 Auto Deploy 服務執行的系統上，將 `/etc/vmware-rbd/ssl/` 中的 `rbd-ca.crt` 和 `rbd-ca.key` 取代為您的自訂憑證和金鑰檔案。

4 在執行 Auto Deploy 服務的系統上，執行下列命令更新 VMware Endpoint 憑證存放區 (VECS) 內的 TRUSTED_ROOTS 存放區以使用新憑證。

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert /etc/vmware-rbd/ssl/rbd-ca.crt
/usr/lib/vmware-vmafd/bin/vecs-cli force-refresh
```

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

在自訂模式中，您負責維護此檔案。

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

請參閱變更 [ESXi 憑證模式](#)。

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

結果

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

備註 如果您在取代憑證後使用 Auto Deploy 時遇到問題，請參閱 VMware 知識庫文章，網址為 <http://kb.vmware.com/kb/2000988>。

透過 Auto Deploy 使用自訂憑證

從 vSphere 8.0 開始，您可以將 Auto Deploy 伺服器設定為使用第三方憑證授權機構 (CA) 或您自己的內部 CA 簽署的自訂憑證佈建 ESXi 主機。依預設，Auto Deploy 伺服器會使用 VMware Certificate Authority (VMCA) 簽署的憑證佈建 ESXi 主機。

在 vSphere 8.0 之前，使用 Auto Deploy 管理憑證的選項包括：

- 使用 vCenter Server 和內建 VMware Certificate Authority (預設)。
- 將 Auto Deploy 設為第三方 CA 的下層 CA。在這種情況下，Auto Deploy SSL 金鑰會對憑證進行簽署。

從 vSphere 8.0 開始，您可以將第三方 CA 或您自己的內部 CA 簽署的自訂憑證上傳到 Auto Deploy。Auto Deploy 將自訂憑證與 ESXi 主機的 MAC 位址或 BIOS UUID 相關聯。每次 Auto Deploy 主機啟動時，Auto Deploy 都會檢查自訂憑證。如果 Auto Deploy 找到自訂憑證，則將使用該憑證，而不是透過 VMCA 產生一個憑證。

此工作的高層級步驟包括：

- 1 為第三方 CA 或您自己的內部 CA 產生自訂憑證請求。
- 2 取得簽署的自訂憑證 (金鑰和憑證) 並將其儲存在本機。
- 3 如果使用的是第三方 CA，並且之前未曾使用，請確保將 CA 的根憑證上傳到 vCenter Server 上的 TRUSTED_ROOTS 存放區。
- 4 將自訂憑證上傳到 Auto Deploy 並將憑證與 ESXi 主機的 MAC 位址或 BIOS UUID 相關聯。
- 5 將 ESXi 主機開機。

將自訂憑證指派給 ESXi 主機時，Auto Deploy 會在下次從 Auto Deploy 開機時將該憑證推送到主機。

使用自訂憑證和 Auto Deploy 時，請注意以下考量事項。

- 您必須使用 PowerCLI `Add-CustomCertificate`、`Remove-CustomCertificate` 和 `List-CustomCertificate` cmdlet 來管理與 Auto Deploy 一起使用的自訂憑證。管理自訂憑證的功能在 vSphere Client 中不可用。
- 若要重新整理用於 Auto Deploy 的自訂憑證，必須再次執行 `Add-CustomCertificate` cmdlet。
- 請務必檢查自訂憑證是否存在潛在錯誤。Auto Deploy 僅驗證自訂憑證是否符合 X.509 憑證標準，以及憑證的到期臨界值是否設定為至少 240 天。Auto Deploy 不會執行任何其他憑證驗證或檢查。若要變更憑證臨界值，可以執行 `Set-DeployOption -Key certificate-refresh-threshold` cmdlet。

- 如果稍後使用 `Remove-CustomCertificate cmdlet` 從 ESXi 主機中移除自訂憑證，必須重新啟動該主機才能使變更生效。

如需有關自訂憑證和 Auto Deploy 的詳細資訊，請參閱 VMware ESXi 安裝和設定說明文件。

必要條件

確保您具有以下內容：

- 向憑證授權機構要求憑證。憑證必須符合這些需求。
 - 金鑰大小：2048 位元 (下限) 至 16384 位元 (上限) (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
 - CRT 格式
 - 設定為 true 的 CA 延伸
 - 憑證簽署的金鑰使用方法
 - 某天的開始時間早於目前時間
- ESXi 主機 MAC 位址或 BIOS UUID。評估哪種方法最適合您的環境。BIOS UUID 比 MAC 位址更穩定，更不受變更的影響。如果變更 ESXi 主機中的網路介面卡，MAC 位址將發生變更。但是，MAC 位址可能更易於使用，並且比 BIOS UUID 更易於取得。
- 至少為 PowerCLI 版本 12.6.0。如需有關 Auto Deploy PowerCLI cmdlet 的詳細資訊，請參閱 VMware ESXi 安裝和設定說明文件中的「Auto Deploy PowerCLI Cmdlet 概觀」主題。

確保您具有下列權限：

- 新增自訂憑證：**Autodeploy.規則.建立**
- 取得自訂憑證資訊：**系統.讀取**

程序

1 產生憑證請求。

- a 使用之前列出的憑證請求需求，建立組態檔 (.cfg)。
- b 若要產生 CSR 檔案和金鑰檔案，請執行 `openssl req` 命令，同時傳入組態檔 (.cfg)。

例如：

```
openssl req -new -config custom_cert.cfg -days 4200 -sha256 -keyout rui.key -out rui.csr
```

在該命令中：

- `-new` 產生新的憑證請求。
- `-config custom_cert.cfg` 指定自訂 .cfg 檔案。
- `-days 4200` 指定憑證認證時間為 4200 天。
- `-sha256` 指定簽署請求所需的訊息摘要。
- `-keyout rui.key` 指定要將新建立的私密金鑰寫入的檔案。
- `-out rui.csr` 指定要寫入的輸出檔案。

2 將憑證請求傳送給第三方 CA，或者，如果您為自己的憑證簽署，請執行 `openssl x509 -req` 命令，從 `rui.csr` 檔案產生自訂憑證。

例如：

```
openssl x509 -req -in rui.csr -CA "/etc/vmware-rbd/ssl/rbd-ca.crt" -CAkey \
"/etc/vmware-rbd/ssl/rbd-ca.key" -extfile \
openssl.cfg -extensions x509 -CAserial "/etc/vmware-rbd/ssl/rbd-ca.srl" -days \
4200 -sha256 -out signed_rui.crt
```

在該命令中：

- `-in rui.csr` 指定輸入檔案。
- `-CA "/etc/vmware-rbd/ssl/rbd-ca.crt"` 指定用於伺服器憑證驗證的目錄。
- `-CAkey "/etc/vmware-rbd/ssl/rbd-ca.key"` 設定用於簽署憑證的 CA 私密金鑰。
- `-extfile openssl.cfg` 指定要從中讀取憑證延伸的其他可選組態檔。
- `-extensions x509` 指定使用 x509 憑證延伸。
- `-CAserial "/etc/vmware-rbd/ssl/rbd-ca.srl"` 使用 `rbd-ca.srl` 中的序號對憑證進行簽署。
- `-days 4200` 指定憑證認證時間為 4200 天。
- `-sha256` 指定簽署請求所需的訊息摘要。
- `-out signed_rui.crt` 指定要寫入的輸出檔案。

- 3 (選擇性) 如果之前未將簽署憑證授權機構的憑證上傳到 VMware Endpoint 憑證存放區 (VECS) 內的 TRUSTED_ROOTS 存放區，請在執行 Auto Deploy 服務的 vCenter Server 上執行以下步驟。

- a 使用 WinSCP 等工具將憑證複製到 vCenter Server。
- b 使用 SSH 登入 vCenter Server 並執行以下命令。

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_ca_certificate
```

- 4 取得 ESXi 主機 MAC 位址或 BIOS UUID。

- 5 執行以下步驟將自訂憑證新增到 Auto Deploy。

- a 若要連線到 vCenter Server，請執行 Connect-VIServer cmdlet。

```
Connect-VIServer -server VC_ip_address -User administrator_user -Password 'password'
```

- b (選擇性) 若要檢視現有的自訂憑證，請執行 Get-CustomCertificates cmdlet。

首次新增自訂憑證時，不會看到此 cmdlet 傳回的任何憑證。

- c 若要將自訂憑證與 ESXi 主機關聯，請執行 Add-CustomCertificate cmdlet。

```
Add-CustomCertificate -HostID [MAC_Address | BIOS_UUID] -Certificate  
"path_to_custom_cert" -Key "path_to_custom_cert_key"
```

您可以指定主機的 MAC 位址或 BIOS UUID。Auto Deploy 將自訂憑證上傳到主機。

- d 若要驗證憑證是否已上傳，請執行 Get-CustomCertificates cmdlet。

您會看到類似下列內容的輸出：

```
Name:      CustomHostCert-1  
CertificateId:      1  
HostId:      02:08:b0:8e:18:a2  
ExpirationTime: 1   2/28/2033 10:45:50 AM  
TimeCreated:      9/29/2022 7:40:28 AM  
LastModified:      9/29/2022 7:40:28 AM  
AssociatedHostName:
```

AssociatedHostName 目前為空。啟動主機後，輸出將反映與自訂憑證關聯的 ESXi 主機的名稱。

- 6 啟動 ESXi 主機。

- 7 若要驗證自訂憑證是否與 vCenter Server 相關聯，請再次執行 Get-CustomCertificates cmdlet。

您會看到類似下列內容的輸出。

```
Name:      CustomHostCert-1  
CertificateId:      1  
HostId:      02:08:b0:8e:18:a2  
ExpirationTime: 1   2/28/2033 10:45:50 AM  
TimeCreated:      9/29/2022 7:40:28 AM  
LastModified:      9/29/2022 7:40:28 AM  
AssociatedHostName: host1.example.com
```

現在，AssociatedHostName 包含 ESXi 主機的名稱。

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 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 ESXi 主機。

或者，您可以將主機置於維護模式並使用 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。

自訂 ESXi 主機安全性

您可以透過 vSphere Client 中提供的 [防火牆]、[服務] 和 [安全性設定檔] 面板來為您的 ESXi 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 VMware CLI 或 SDK 的其中一種，並考慮對自訂作業進行自動化。

設定 ESXi 防火牆

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)。可以使用 vSphere Client、CLI 和 API 管理防火牆。

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 防火牆設定為僅從授權網路啟用存取，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：

- 針對 vSphere Client 中的每台主機，使用**設定 > 防火牆**。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[使用 ESXCLI 防火牆命令設定 ESXi 行為](#)。
- 如果要開啟的連接埠不在安全性設定檔中，請使用自訂 VIB。

若要安裝自訂 VIB，您必須將 ESXi 主機的接受層級變更為 CommunitySupported。

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 支援可能會要求解除安裝此 VIB。這類要求是疑難排解步驟，用於判定該 VIB 是否與正在調查的問題相關。

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 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。

此工作說明如何使用 vSphere Client 設定 ESXi 防火牆設定。可以使用 ESXi Shell 或 ESXCLI 命令，在命令列設定 ESXi 以自動化防火牆組態。如需使用 ESXCLI 操縱防火牆和防火牆規則的相關範例，請參閱[使用 ESXCLI 防火牆命令設定 ESXi 行為](#)。

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 使用 vSphere Client 登入 vCenter Server。
- 2 在詳細目錄中瀏覽到主機。
- 3 按一下**設定**，然後按一下**系統下的防火牆**。
可以透過按一下**傳入**和**傳出**，在傳入和傳出連線之間切換。
- 4 在 [防火牆] 區段中，按一下**編輯**。
- 5 從以下三個服務群組中選取一個：**未分組**、**安全殼層**和**簡易網路管理通訊協定**。
- 6 選取要啟用的規則集，或取消選取要停用的規則集。

- 7 對於某些服務，也可以透過導覽至**系統**下的**設定 > 服務**來管理服務詳細資料。

如需有關啟動、停止和重新啟動服務的詳細資訊，請參閱[啟用或停用 ESXi 服務](#)。

- 8 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](#)。

- 9 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。

若要更新服務的 [允許的 IP] 清單，可以使用 vSphere Client、ESXCLI 或 PowerCLI。此工作說明如何使用 vSphere Client。如需使用 ESXCLI 的相關指示，請參閱 ESXCLI 概念和範例中的[管理 ESXi 防火牆](#)。

程序

- 1 使用 vSphere Client 登入 vCenter Server。
- 2 瀏覽到 ESXi 主機。
- 3 按一下**設定**，然後按一下**系統**下的**防火牆**。
可以透過按一下**傳入**和**傳出**，在傳入和傳出連線之間切換。
- 4 在 [防火牆] 區段中，按一下**編輯**。
- 5 從以下三個服務群組中選取一個：**未分組**、**安全殼層**和**簡易網路管理通訊協定**。
- 6 若要顯示 [允許的 IP 位址] 區段，請展開一個服務。
- 7 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

- 8 確保選取服務本身。
- 9 按一下**確定**。
- 10 驗證服務的**允許的 IP 位址**資料行中的變更。

ESXi 主機的傳入和傳出防火牆連接埠

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

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)。如需 ESXi 防火牆中支援的連接埠和通訊協定的清單，請參閱 VMware Ports and Protocols Tool™，網址為 <https://ports.vmware.com/>。

VMware Ports and Protocols Tool 會列出依預設安裝之服務的連接埠資訊。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。該資訊主要是關於 vSphere Client 中可見的服務，但 VMware Ports and Protocols Tool 還包含了一些其他連接埠。

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。

使用 ESXCLI 防火牆命令設定 ESXi 行為

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

防火牆命令參考

可以使用 ESXi Shell 或 ESXCLI 命令，在命令列設定 ESXi 以自動化防火牆組態。若要操縱防火牆和防火牆規則，請參閱 ESXCLI 入門瞭解相關簡介，參閱《ESXCLI 概念和範例》瞭解使用 ESXCLI 的範例。

在 ESXi 7.0 及更新版本中，已限制對用於建立自訂防火牆規則的 `service.xml` 檔案進行存取。如需使用 `/etc/rc.local.d/local.sh` 檔案建立自訂防火牆規則的相關資訊，請參閱 VMware 知識庫文章 [2008226](#)。

表 3-6. 防火牆命令

命令	說明
<code>esxcli network firewall get</code>	傳回防火牆的狀態並列出預設動作。
<code>esxcli network firewall set --default-action</code>	設定為 <code>true</code> 可設定要傳遞的預設動作。設定為 <code>false</code> 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 <code>true</code> 允許對所有 IP 具有完全存取權。設定為 <code>false</code> 可使用已允許的 IP 位址清單。
<code>esxcli network firewall ruleset set --enabled --ruleset-id=<string></code>	將 <code>enabled</code> 設定為 <code>true</code> 可啟用指定規則集。將 <code>enabled</code> 設定為 <code>false</code> 可停用指定規則集。
<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。

啟用或停用 ESXi 服務

可以從 vSphere Client 啟用或停用 ESXi 服務。

ESXi 主機包含數個依預設會執行的服務。如果您的公司原則允許，則可以從安全性設定檔停用服務或啟用服務。

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。

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。有時，需要進行一些其他設定，服務才可用於 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。

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 Client 修改下列服務的狀態。

表 3-7. 安全性設定檔中的 ESXi 服務

服務	預設值	說明
Direct Console UI	執行中	Direct Console 使用者介面 (DCUI) 服務允許您使用文字型功能表從本機主控台與 ESXi 主機進行互動。
ESXi Shell	已停止	ESXi Shell 可從 Direct Console 使用者介面取得，且包括一組完全支援的命令和一組用於疑難排解和修復的命令。您必須啟用從每個系統的 Direct Console 存取 ESXi Shell。您可以啟用存取本機 ESXi Shell 或透過 SSH 存取 ESXi Shell。
SSH	已停止	主機上的 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。
attestd	已停止	vSphere Trust Authority 證明服務。
kmxd	已停止	vSphere Trust Authority 金鑰提供者服務。
Active Directory 服務	已停止	當您針對 Active Directory 設定 ESXi 時，此服務即啟動。
NTP 精靈	已停止	網路時間通訊協定精靈。
PC/SC 智慧卡精靈	已停止	啟用主機以進行智慧卡驗證時，將啟動此服務。請參閱 設定和管理用於 ESXi 的智慧卡驗證 。
CIM 伺服器	執行中	可由通用訊息模型 (CIM) 應用程式使用的服務。
SNMP 伺服器	已停止	SNMP 精靈。如需有關設定 SNMP v1、v2 和 v3 的資訊，請參閱 vSphere 監控和效能 說明文件。
Syslog 伺服器	已停止	Syslog 精靈。您可以在 vSphere Client 中從 [進階系統設定] 啟用 Syslog。請參閱 vCenter Server 安裝和設定說明文件。
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。

必要條件

透過 vSphere Client 連線到 vCenter Server。

程序

- 1 在詳細目錄中瀏覽到 ESXi 主機。
- 2 按一下**設定**，然後按一下**系統下的服務**。

3 選取您想要變更的服務。

- a 選取**重新啟動、啟動或停止**以對主機狀態進行一次性變更。
- b 若要在重新開機過程中變更主機的狀態，請按一下**編輯啟動原則**，然後選取原則。
 - **隨主機一起啟動和停止**：服務在主機啟動後立即啟動，並在主機關閉之前不久關閉。此選項與**根據連接埠使用情況啟動和停止**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，但之後又開啟，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，如果主機電源開啟，該服務會一直執行。如果服務已啟動且主機已關閉電源，則該服務將在關閉過程中停止。當主機開啟電源時，該服務將再次啟動，以保留使用者確定的狀態。
 - **根據連接埠使用情況啟動和停止**：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。

備註 這些設定僅適用於透過 UI 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。

4 按一下確定。

在 ESXi 主機上設定和管理鎖定模式

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。

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。也可以使用 [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。

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，有特殊權限的使用者可透過 vCenter Server、從 vSphere Client，或透過使用 vSphere Web Services SDK 來存取主機。
- Direct Console 介面行為針對嚴格鎖定模式和一般鎖定模式有所不同。
 - 在嚴格鎖定模式下，Direct Console 使用者介面 (DCUI) 服務會停用。
 - 在一般鎖定模式下，如果 [例外使用者] 清單上的帳戶擁有管理員權限，則可以存取 DCUI。此外，在 `DCUI.Access` 進階系統設定中指定的所有使用者都可存取 DCUI。

- 如果 ESXi Shell 或 SSH 已啟用，而主機處於鎖定模式下，則 [例外使用者] 清單中具有管理員權限的帳戶均可使用這些服務。對於所有其他使用者，ESXi Shell 或 SSH 存取會停用。針對無管理員權限之使用者的 ESXi 或 SSH 工作階段均會關閉。

嚴格及一般鎖定模式下的所有存取均會得到記錄。

表 3-8. 鎖定模式行為

服務	一般模式	一般鎖定模式	嚴格鎖定模式
vSphere Web Services API	所有使用者，根據權限	vCenter (vpxuser) 例外使用者，根據權限 vCloud Director (如果可用，則為 vslauser)	vCenter (vpxuser) 例外使用者，根據權限 vCloud Director (如果可用，則為 vslauser)
CIM 提供者	主機上具有管理員權限的使用者	vCenter (vpxuser) 例外使用者，根據權限 vCloud Director (如果可用，則為 vslauser)	vCenter (vpxuser) 例外使用者，根據權限 vCloud Director (如果可用，則為 vslauser)
Direct Console UI (DCUI)	主機上具有管理員權限的使用者，以及 DCUI.Access 進階系統設定中的使用者	DCUI.Access 進階系統設定中定義的使用者 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) 和 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	DCUI.Access 進階系統設定中定義的使用者 主機上具有管理員權限的例外使用者

在啟用鎖定模式時登入 ESXi Shell 的使用者的鎖定模式行為

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

如何停用鎖定模式

您可以停用鎖定模式，如下所示。

從 vSphere Client 中

使用者可以從 vSphere Client 中停用一般鎖定模式和嚴格鎖定模式。請參閱[從 vSphere Client 停用鎖定模式](#)。

從 Direct Console 使用者介面中

若使用者能在 ESXi 主機上存取 Direct Console 使用者介面，即可停用一般鎖定模式。在嚴格鎖定模式下，Direct Console 介面服務會停止。請參閱[從 Direct Console 使用者介面啟用或停用一般鎖定模式](#)。

從 vSphere Client 啟用鎖定模式

選取鎖定模式，要求所有組態變更都透過 vCenter Server 進行。vSphere 支援一般鎖定模式和嚴格鎖定模式。

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

程序

- 1 在 vSphere Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在 [系統] 下，選取**安全性設定檔**。
- 4 在 [鎖定模式] 面板中，按一下**編輯**。
- 5 按一下**鎖定模式**，然後選取其中一個鎖定模式選項。

選項	說明
正常	主機可透過 vCenter Server 存取。只有「例外使用者」清單中具有管理員權限的使用者才能登入 Direct Console 使用者介面。如果已啟用 SSH 或 ESXi Shell，才有可能進行存取。
嚴格	主機僅可透過 vCenter Server 存取。如果已啟用 SSH 或 ESXi Shell，則會保持執行 DCUI.Access 進階系統設定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關閉。

- 6 按一下**確定**。

從 vSphere 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。

使用者可以從 vSphere Client 中停用一般鎖定模式和嚴格鎖定模式。

程序

- 1 在 vSphere Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在 [系統] 下，選取**安全性設定檔**。
- 4 在 [鎖定模式] 面板中，按一下**編輯**。
- 5 按一下**鎖定模式**，然後選取已停用來停用鎖定模式。
- 6 按一下**確定**。

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 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故障時啟用存取權。

啟用鎖定模式時，會保留使用者權限。從 Direct Console 介面停用鎖定模式時會還原使用者權限。

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

若要保留權限，請先從 vSphere 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。

當 vSphere 處於鎖定模式時帳戶可以執行的作業

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

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

您可以從 vSphere 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。

將使用者新增到 DCUI.Access 進階系統設定

發生災難性故障時，如果無法從 vCenter Server 存取主機，可以透過 DCUI.Access 進階系統設定結束鎖定模式。可從 vSphere Client 編輯主機的 [進階設定] 將使用者新增到清單。

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

- 1 在 vSphere Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在 [系統] 下，按一下**進階系統設定**，然後按一下**編輯**。
- 4 DCUI 的篩選器。
- 5 在 **DCUI.Access** 文字方塊中，輸入本機 ESXi 使用者名稱，並以逗點分隔。
依預設，已包含根使用者。請考慮從 DCUI.Access 清單中移除 root 使用者並指定具名帳戶以更方便稽核。
- 6 按一下**確定**。

指定鎖定模式例外使用者

您可以從 vSphere 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。例如，這意味著唯讀使用者無法在主機上停用鎖定模式。

- 1 在 vSphere Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在 [系統] 下，選取**安全性設定檔**。
- 4 在 [鎖定模式] 面板中，按一下**編輯**。
- 5 按一下**例外使用者**，然後按一下**新增使用者**圖示以新增例外使用者。
- 6 按一下**確定**。

使用 vSphere 安裝服務包執行安全更新

使用 ESXCLI 升級 ESXi 時，需要瞭解 vSphere 安裝服務包、映像設定檔和軟體存放庫。

ESXi 包含映像設定檔，該設定檔描述了一組包含實際軟體的 vSphere 安裝服務包 (VIB)。VIB 是表示系統元件的簽署 ramdisk，大致類似於 Linux 系統上的 RPM 或 DEB。映像設定檔是 VIB 的集合。軟體存放庫是 VIB 和映像設定檔的集合。ESXi 修補程式和存放庫包含由一組通用 VIB 組成的更新映像設定檔。

可以使用 `esxcli software` 命令在獨立主機上安裝 ESXi 更新。如需詳細資訊，請參閱 VMware ESXi 升級說明文件。

備註 通常，在 vSphere 7.0 及更新版本的環境中，可以使用 VMware vSphere® vSphere Lifecycle Manager 對 ESXi 主機進行生命週期管理。

若要列出所有已安裝的 VIB 及其目前版本或目前映像設定檔，您可以使用以下 ESXCLI 命令。

- `esxcli software vib list`
- `esxcli software profile get`

通常，可以使用以下高層級步驟安全地升級 ESXi：

- 將 ESXi 主機置於維護模式
- 執行 `esxcli software profile update` 命令，該命令指向 URL 或透過 SSH 傳輸到主機的 ZIP 檔案
- 重新啟動 ESXi 主機

由於 VMware 會對 VIB 進行密碼編譯簽署，因此不需要安全傳輸 VIB 或整個存放庫，更新程序會驗證這些簽章。

管理 ESXi 主機和 vSphere 安裝服務包的接受程度

vSphere 安裝服務包 (VIB) 的接受程度視此 VIB 的憑證數量而定。ESXi 主機的接受程度視最低 VIB 的層級而定。如果您要允許較低層級的 VIB，可以變更主機的接受程度。若要能夠變更主機接受程度，可移除 CommunitySupported VIB。

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

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

ESXi 主機的接受程度顯示在 vSphere Client 的安全性設定檔中。

支援以下接受程度。

VMwareCertified

VMwareCertified 接受程度具有最為嚴格的需求。此程度的 VIB 能夠完全通過全面測試，該測試相當於相同技術的 VMware 內部品質保證測試。今天，僅以此程度發佈 I/O Vendor Program (IOVP) 計畫驅動程式。VMware 受理此接受程度的 VIB 的支援致電。

VMwareAccepted

此接受程度的 VIB 雖然已通過驗證測試，但這些測試並非對軟體的每項功能進行全面測試。合作夥伴會執行測試並且 VMware 會驗證結果。現在，以此程度發佈的 VIB 包括 CIM 提供者和 PSA 外掛程式。VMware 會將此接受程度的 VIB 支援致電的客戶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 支援致電的客戶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 使用 SSH 連線至每個 ESXi 主機。
- 2 透過執行以下命令來驗證是否已將接受程度設定為 VMwareCertified、VMwareAccepted 或 PartnerSupported。

```
esxcli software acceptance get
```

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

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

- 4 執行以下命令以移除任何 CommunitySupported VIB。

```
esxcli software vib remove --vibname vib
```

5 使用以下其中一種方法變更主機的接受程度。

選項	說明
CLI 命令	<pre>esxcli software acceptance set --level level</pre> <p><code>level</code> 為必要參數，用於指定要設定的接受程度。應為以下內容之一： VMwareCertified、VMwareAccepted、PartnerSupported 或 CommunitySupported。如需詳細資訊，請參閱 ESXCLI 參考。</p>
vSphere Client	<ol style="list-style-type: none"> 在詳細目錄中選取主機。 按一下設定。 在 [系統] 下，選取安全性設定檔。 針對主機映像設定檔接受程度按一下編輯，然後選擇接受程度。

結果

新的接受程度已生效。

備註 ESXi 對受接受程度約束的 VIB 執行完整性檢查。可以使用 `VMkernel.Boot.execInstalledOnly` 設定指示 ESXi 僅執行主機上安裝的有效 VIB 所產生的二進位檔。此設定與安全開機結合使用時，可確保在 ESXi 主機上執行的每個程序都是已簽署、允許且符合預期的程序。在 vSphere 7 中，預設會停用 `VMkernel.Boot.execInstalledOnly` 設定以實現合作夥伴相容性。儘量啟用此設定以提高安全性。如需有關為 ESXi 設定進階選項的詳細資訊，請參閱 VMware 知識庫文章，網址為 <https://kb.vmware.com/kb/1038578>。

為 ESXi 主機指派權限

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

將權限指派給 vCenter Server 管理的 ESXi 主機

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

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

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

將權限指派給獨立的 ESXi 主機

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

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

會預先定義下列角色。

唯讀

允許使用者檢視與 ESXi 主機相關聯的物件，但請勿對物件做任何變更。

管理員

管理員角色。

無存取權

無存取權。此角色為預設角色。您可以覆寫預設角色。

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

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

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

預先定義的 ESXi 使用者和權限

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

根使用者

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

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

為了更好地稽核，請建立具有管理員權限的個別帳戶。為根帳戶設定非常複雜的密碼，並限制根帳戶的使用，例如，新增主機至 vCenter Server 時使用。請勿移除根帳戶。如需有關針對 ESXi 主機指派給使用者權限的詳細資訊，請參閱 vSphere 單一主機管理 - VMware Host Client 說明文件。

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

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

vpxuser 使用者

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

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

您無法使用 Active Directory 管理 vpxuser 使用者。

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

dcui 使用者

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

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

停用非根 ESXi 使用者的殼層存取

從 vSphere 8.0 開始，可以使用 API 或 ESXCLI 停用 vpxuser 使用者和 dcui 使用者的殼層存取。您還可以使用 API 或 ESXCLI 防止 vpxuser 使用者變更其他使用者的密碼。做出此類變更時，請確認它們不會中斷現有的第三方工作流程。如需詳細資訊，請參閱 API 或 ESXCLI 說明文件。

使用 Active Directory 管理 ESXi 使用者

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

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

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

將 ESXi 主機設定為使用 Active Directory

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

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

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

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

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 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 Client 詳細目錄中瀏覽到主機。
- b 按一下**設定**。
- c 在[網路]下，按一下**TCP/IP 組態**。
- d 在[TCP/IP 堆疊: 預設]下，按一下**DNS**，然後確認該主機的主機名稱和 DNS 伺服器資訊正確無誤。

後續步驟

將主機加入目錄服務網域。請參閱[將 ESXi 主機新增至目錄服務網域](#)。對於使用 Auto Deploy 佈建的主機，請設定 vSphere Authentication Proxy。請參閱[使用 vSphere Authentication Proxy](#)。您可以設定權限，以便加入的 Active Directory 網域中的使用者和群組可以存取 vCenter Server 元件。如需有關管理權限的資訊，請參閱[將權限新增到詳細目錄物件](#)。

將 ESXi 主機新增至目錄服務網域

若 ESXi 主機要使用目錄服務，必須先將主機加入目錄服務網域。

您可以使用下列兩種方式中的一種來輸入網域名稱：

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

若要使用 vSphere Authentication Proxy 服務，請參閱[使用 vSphere Authentication Proxy](#)。

程序

- 1 在 vSphere Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在 [系統] 下，選取**驗證服務**。
- 4 按一下**加入網域**。
- 5 輸入網域。
使用 `name.tld` 或 `name.tld/container/path` 形式。
- 6 輸入有權將主機加入網域的目錄服務使用者的使用者名稱和密碼，然後按一下**確定**。
- 7 (選擇性) 如果您想要使用驗證 Proxy，請輸入 Proxy 伺服器 IP 位址。
- 8 按一下**確定**，關閉 [目錄服務組態] 對話方塊。

後續步驟

您可以設定權限，以便加入的 Active Directory 網域中的使用者和群組可以存取 vCenter Server 元件。如需有關管理權限的資訊，請參閱[將權限新增到詳細目錄物件](#)。

檢視 ESXi 主機的目錄服務設定

您可以檢視目錄伺服器的類型 (如果有類型可檢視)，ESXi 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 Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在 [系統] 下，選取**驗證服務**。

[驗證服務] 分頁將顯示目錄服務和網域設定。

後續步驟

您可以設定權限，以便加入的 Active Directory 網域中的使用者和群組可以存取 vCenter Server 元件。如需有關管理權限的資訊，請參閱[將權限新增到詳細目錄物件](#)。

使用 vSphere Authentication Proxy

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

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

請參閱 [vCenter Server 所需的連接埠](#)，取得有關 vSphere Authentication Proxy 所使用的 TCP 連接埠的資訊。

Auto Deploy

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

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

請參閱將 [Auto Deploy 設為下層憑證授權機構](#)。

其他 ESXi 主機

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

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

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

啟動 vSphere Authentication Proxy 服務

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

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

必要條件

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

程序

1 啟動 VMware vSphere Authentication Proxy 服務。

選項	說明
vCenter Server 管理介面	<ol style="list-style-type: none"> 在網頁瀏覽器中，移至 vCenter Server 管理介面 (https://vcenter-IP-address-or-FQDN:5480)。 以 root 身分登入。 預設根密碼為部署 vCenter Server 時設定的密碼。 按一下 服務，然後按一下 VMware vSphere Authentication Proxy 服務。 按一下 開始。 (選擇性) 服務啟動後，按一下 設定啟動類型，然後按一下 自動 以自動啟動。
CLI	<pre>service-control --start vmcam</pre>

2 確認服務已成功啟動。

結果

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

使用 vSphere Client 將網域新增至 vSphere Authentication Proxy

可以從 vSphere Client 將網域新增至 vSphere Authentication Proxy。

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

程序

- 1 使用 vSphere Client 連線到 vCenter Server 系統。
- 2 選取 vCenter Server，然後按一下 **設定**。
- 3 按一下 **Authentication Proxy**，然後按一下 **編輯**。
- 4 輸入 vSphere Authentication Proxy 將在其中新增主機之網域的名稱，以及擁有 Active Directory 權限，可將主機新增至網域之使用者的名稱和密碼。
- 5 按一下 **儲存**。

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

您可以使用 `camconfig` 命令，將網域新增至 vSphere 驗證。

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

程序

- 1 以具有管理員權限的使用者身分登入 vCenter Server 系統。
- 2 執行命令以啟用對 Bash shell 的存取。

```
shell
```

- 3 前往 **camconfig** 指令碼所在的 `/usr/lib/vmware-vmcam/bin/` 目錄。
- 4 若要將網域和使用 Active Directory 認證新增到 Authentication Proxy 組態，請執行下列命令。

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

系統會提示您輸入密碼。

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

vSphere Authentication Proxy 使用由 *使用者* 指定的使用者名稱來為 Active Directory 中的 ESXi 主機建立帳戶。使用者必須具有權限，才能在新增主機的 Active Directory 網域中建立帳戶。寫入此資訊時，Microsoft 知識庫文章 932455 具有帳戶建立權限的背景資訊。

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

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

使用 vSphere Authentication Proxy 將主機新增到網域

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

您可以使用下列兩種方式中的一種來輸入網域名稱：

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

必要條件

- 如果 ESXi 主機使用 VMCA 簽署憑證，請確認已將主機新增到 vCenter Server。否則，Authentication Proxy 服務無法信任 ESXi 主機。
- 如果 ESXi 主機使用的是 root CA 簽署憑證，請確認已將適當的 root CA 簽署憑證新增到 vCenter Server 系統。請參閱[管理 ESXi 主機的憑證](#)。

程序

- 1 在 vSphere Client 詳細目錄中瀏覽到主機。

- 2 按一下**設定**。
- 3 在**系統**下，選取**驗證服務**。
- 4 按一下**加入網域**。
- 5 輸入網域。
使用表單 `name.tld` (例如 `mydomain.com`)，或 `name.tld/container/path` (例如 `mydomain.com/organizational_unit1/organizational_unit2`)。
- 6 選取**使用 Proxy 伺服器**。
- 7 輸入 Authentication Proxy 伺服器的 IP 位址，其始終與 vCenter Server 系統的 IP 位址相同。
- 8 按一下**確定**。

為 vSphere Authentication Proxy 啟用用戶端驗證

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

必要條件

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

程序

- 1 以具有管理員權限的使用者身分登入 vCenter Server 系統。
- 2 若要啟用對 Bash shell 的存取，請執行 `shell` 命令。
- 3 前往 **camconfig** 指令碼所在的 `/usr/lib/vmware-vmcam/bin/` 目錄。
- 4 若要啟用用戶端驗證，請執行以下命令。

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

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

- 5 如果您稍後想要再次停用用戶端驗證，請執行以下命令。

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

將 vSphere Authentication Proxy 憑證匯入 ESXi 主機

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

必要條件

- 將 vSphere Authentication Proxy 憑證上傳到 ESXi 主機可存取的資料存放區。使用 SFTP 應用程式 (例如 WinSCP)，您可以從 vCenter Server 主機的以下位置下載憑證。

```
/var/lib/vmware/vmcam/ssl/rui.crt
```

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

程序

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

為 vSphere Authentication Proxy 產生新的憑證

您可以產生使用 VMware Certificate Authority (VMCA) 佈建的新憑證，或是包含 VMCA 作為下層憑證的新憑證。

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

必要條件

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

程序

- 1 建立 `certtool.cfg` 的複本。

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

- 2 編輯含關於您組織之一些資訊的複本，如下列範例所示。

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

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

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

對於 *localhost*，提供 vCenter Server 的 FQDN。

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

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

對於 *localhost*，提供 vCenter Server 的 FQDN。

設定 vSphere Authentication Proxy 使用自訂憑證

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

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

程序

1 為 vSphere Authentication Proxy 產生 CSR。

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

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

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

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

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

```
/var/lib/vmware/vmcam/ssl/rui.crt
```

- 3 解除登錄 vSphere Authentication Proxy。

- a 前往 `camregister` 指令碼所在的 `/usr/lib/vmware-vmcam/bin` 目錄。
- b 執行下列命令。

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

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

- 4 停止 vSphere Authentication Proxy 服務。

工具	步驟
vCenter Server 組態管理介面	<ol style="list-style-type: none"> a 在網頁瀏覽器中，移至 vCenter Server 組態管理介面 (https://vcenter-IP-address-or-FQDN:5480)。 b 以 root 身分登入。 預設根密碼為部署 vCenter Server 時設定的密碼。 c 按一下服務，然後按一下 VMware vSphere Authentication Proxy 服務。 d 按一下停止。
CLI	<pre>service-control --stop vmcam</pre>

- 5 將現有的 `rui.crt` 憑證和 `rui.key` 檔案取代為從 CA 收到的檔案。
- 6 重新啟動 vSphere Authentication Proxy 服務。
- 7 使用新憑證和金鑰向 vCenter Server 明確重新登錄 vSphere Authentication Proxy。

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

設定和管理用於 ESXi 的智慧卡驗證

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

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

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

- 1 當您將智慧卡插入智慧卡讀卡機時，ESXi 主機會讀取上面的認證。
- 2 ESXi DCUI 會顯示您的登入識別碼，並提示您輸入 PIN。
- 3 在您輸入 PIN 之後，ESXi 主機會將其與儲存在智慧卡上的 PIN 進行比對，並使用 Active Directory 驗證智慧卡上的憑證。

4 成功驗證智慧卡憑證之後，ESXi 會讓您登入 DCUI。

按 F3 即可從 DCUI 切換到使用者名稱和密碼驗證。

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

啟用智慧卡驗證

啟用智慧卡驗證，以提示智慧卡和 PIN 組合登入 ESXi DCUI。

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 Client 新增根憑證。請參閱[管理 ESXi 主機的憑證](#)。

程序

- 1 在 vSphere Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在 [系統] 下，選取**驗證服務**。
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。
憑證必須採用 PEM 格式。
- 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 Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在 [系統] 下，選取**驗證服務**。
您將看到目前的智慧卡驗證狀態和包含已匯入憑證的清單。
- 4 在 [智慧卡驗證] 面板中，按一下**編輯**。
- 5 在 [智慧卡驗證] 頁面上，取消選取**啟用智慧卡驗證**核取方塊，然後按一下**確定**。

發生連線問題時，利用使用者名稱和密碼進行驗證

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

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

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

在鎖定模式下使用智慧卡驗證

啟用後，ESXi 主機上的鎖定模式可提高主機的安全性並限制對 DCUI 的存取。鎖定模式可能會導致智慧卡驗證不再起作用。

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 Client 將使用者新增至 [例外使用者] 清單。當主機進入一般鎖定模式時，這些使用者不會遺失他們的權限，並且可以登入 DCUI。如需詳細資訊，請參閱 [指定鎖定模式例外使用者](#)。

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

使用 ESXi Shell

ESXi Shell 提供基本維護命令，依預設，在 ESXi 主機上處於停用狀態。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。

適用服務如下所示。

ESXi Shell

啟用此服務可本機存取 ESXi Shell。

SSH

啟用此服務可使用 SSH 遠端存取 ESXi Shell。

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

備註 僅在實際需要存取時啟用 ESXi Shell。

- **使用 vSphere Client 設定 ESXi Shell 的閒置逾時**

如果您在主機上啟用了 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。可以透過為閒置工作階段設定逾時來防止出現此問題。

- **使用 vSphere Client 設定 ESXi Shell 的可用性逾時**

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。

- **使用 DCUI 設定 ESXi Shell 的可用性逾時或閒置逾時**

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

- **使用 vSphere Client 啟用對 ESXi Shell 的存取**

依預設，ESXi Shell 和 SSH 介面處於停用狀態。除非執行疑難排解或支援活動，否則，請將這些介面保持停用狀態。對於日常活動，請使用 vSphere Client，其中活動受到角色型存取控制和現代存取控制方法的約束。

- **使用 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 Client、ESXCLI 或 VMware 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 Client 設定 ESXi Shell 的閒置逾時

如果您在主機上啟用了 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。可以透過為閒置工作階段設定逾時來防止出現此問題。

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 Client 中控制本機和遠端 (SSH) 工作階段的時間量。

程序

- 1 在 vSphere Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在 [系統] 下，選取**進階系統設定**。

- 4 按一下**編輯**，選取 `UserVars.ESXiShellInteractiveTimeOut`，然後輸入逾時設定。
若值為零 (0)，則會停用閒置時間。
- 5 重新啟動 ESXi Shell 服務和 SSH 服務，則此逾時生效。
 - a 移至**系統 > 服務**。
 - b 依序選取 ESXi Shell 和 SSH，然後按一下**重新啟動**。

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 vSphere Client 設定 ESXi Shell 的可用性逾時

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 Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在 [系統] 下，選取**進階系統設定**。
- 4 按一下**編輯**，然後選取 `UserVars.ESXiShellTimeOut`。
- 5 輸入閒置逾時設定。
- 6 按一下**確定**。
- 7 重新啟動 ESXi Shell 服務和 SSH 服務，則此逾時生效。
 - a 移至**系統 > 服務**。
 - b 依序選取 ESXi Shell 和 SSH，然後按一下**重新啟動**。

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。

使用 DCUI 設定 ESXi Shell 的可用性逾時或閒置逾時

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

兩種類型的逾時適用於不同的情況。

ESXi Shell 閒置逾時

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

ESXi Shell 可用性逾時

可用性逾時決定在最初啟用 Shell 之後和登入之前，可以經過的時間量。如果等待更長的時間，服務會停用，並且您無法登入 ESXi Shell。

必要條件

啟用 ESXi Shell。請參閱[使用 DCUI 啟用對 ESXi Shell 的存取](#)。

程序

- 1 登入 ESXi Shell。
- 2 從 [疑難排解模式選項] 功能表中，選取**修改 ESXi Shell 和 SSH 逾時**，然後按 Enter。
- 3 輸入閒置逾時 (以秒為單位) 或可用性逾時。
- 4 按 Enter 並按 Esc，直到返回到 Direct Console 使用者介面的主功能表。
- 5 按一下**確定**。
- 6 重新啟動 ESXi Shell 服務和 SSH 服務，則此逾時生效。
 - a 在 vSphere Client 中，選取主機，然後移至**設定 > 系統 > 服務**。
 - b 依序選取 ESXi Shell 和 SSH，然後按一下**重新啟動**。

結果

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

使用 vSphere Client 啟用對 ESXi Shell 的存取

依預設，ESXi Shell 和 SSH 介面處於停用狀態。除非執行疑難排解或支援活動，否則，請將這些介面保持停用狀態。對於日常活動，請使用 vSphere Client，其中活動受到角色型存取控制和現代存取控制方法的約束。

備註 使用 vSphere Client、遠端命令列工具 (ESXCLI 和 PowerCLI) 和已發佈的 API 來存取主機。除非是在特殊情況下，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 在詳細目錄中瀏覽到主機。
- 2 按一下**設定**，然後按一下 [系統] 下的**服務**。

3 管理 ESXi、SSH 或 Direct Console UI 服務。

- a 在 [服務] 窗格中，選取服務。
- b 按一下 **編輯啟動原則**，然後選取啟動原則 **手動啟動和停止**。
- c 若要啟用服務，按一下 **啟動**。

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**。

後續步驟

設定 ESXi Shell 的可用性和閒置逾時。請參閱 [使用 vSphere Client 設定 ESXi Shell 的可用性逾時](#) 和 [使用 vSphere Client 設定 ESXi Shell 的閒置逾時](#)。

使用 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 (DCUI) 啟用對 ESXi Shell 的本機和遠端存取。您可以從連結到主機的實體主控台存取 Direct Console 使用者介面。當主機重新開機並載入 ESXi 後，按 F2 以登入 DCUI。輸入您在安裝 ESXi 時建立的認證。

備註 使用 Direct Console 使用者介面、vSphere 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。如果在認可變更之前主機發生故障，則變更可能會遺失。

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 [使用 DCUI 設定 ESXi Shell 的可用性逾時或閒置逾時](#)。

登入 ESXi Shell 進行疑難排解

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

程序

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

ESXi 主機的 UEFI 安全開機

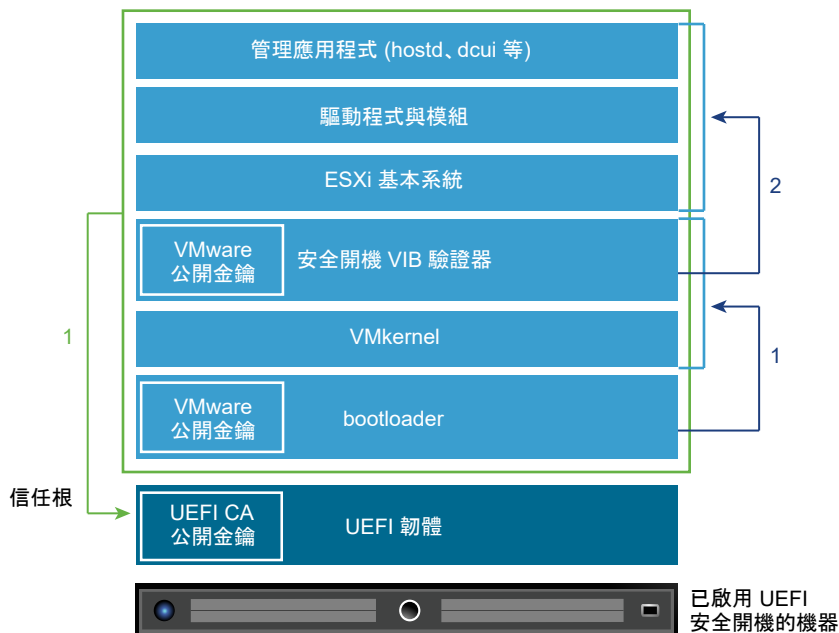
安全開機是 UEFI 韌體標準的一部分。當安全開機正在使用中時，除非作業系統開機載入器經密碼編譯簽署，否則機器將拒絕載入任何 UEFI 驅動程式或應用程式。在 vSphere 6.5 及更新版本中，ESXi 支援安全開機 (若已在硬體中啟用)。

ESXi 如何使用 UEFI 安全開機

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

備註 在已升級的主機上使用 UEFI 安全開機前，請遵循在升級的 ESXi 主機上執行安全開機驗證指令碼中的指示來檢查相容性。

圖 3-1. UEFI 安全開機



安全開機正在使用中時，開機順序的執行方式如下。

- 1 在 vSphere 6.5 及更新版本中，ESXi 開機載入器包含 VMware 公開金鑰。開機載入器使用此金鑰來驗證核心的簽章，以及一小部分包括安全開機 VIB 驗證器的系統。
- 2 VIB 驗證器驗證系統上安裝的每一個 VIB 套件。

此時，藉由屬於 UEFI 韌體之憑證中的信任根，整個系統完成開機。

備註 當您安裝或升級至 vSphere 7.0 Update 2 或更新版本，並且 ESXi 主機具有 TPM 時，TPM 會根據 UEFI 安全開機的 PCR 值透過 TPM 原則封裝敏感資訊。如果滿足此原則，將在後續重新開機期間載入此值。若要在 vSphere 7.0 Update 2 和更新版本中停用或啟用 UEFI 安全開機，請參閱[啟用或停用安全開機強制執行以確保安全的 ESXi 組態](#)。

UEFI 安全開機疑難排解

如果安全開機在開機順序的任意層級失敗，將會發生錯誤。

錯誤訊息取決於硬體廠商以及驗證失敗所屬的層級。

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

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

- 如果核心已遭篡改，會發生類似如下的錯誤。

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

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

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

若要解決安全開機的問題，請遵循這些步驟。

- 1 在安全開機停用的情況下將主機重新開機。
- 2 執行安全開機驗證指令碼 (請參閱[在升級的 ESXi 主機上執行安全開機驗證指令碼](#))。
- 3 檢查 `/var/log/esxupdate.log` 檔案中的資訊。

在升級的 ESXi 主機上執行安全開機驗證指令碼

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

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

- 如果您使用 `ESXCLI` 命令升級，則舊版 ESXi 會執行新的 VIB 安裝，因此不會儲存其簽章且不能安全開機。
- 如果您使用 ISO 升級，則新的 VIB 會儲存其簽章。此情況同樣適用於使用 ISO 的 vSphere Lifecycle Manager 升級。

- 如果舊 VIB 保留在系統上，則這些 VIB 的簽章不可用且不能安全開機。
 - 如果系統使用第三方驅動程式，且 VMware 升級不包含新版驅動程式 VIB，則升級後舊 VIB 會保留在系統上。
 - 在少數情況下，VMware 可能會終止進行中的特定 VIB 的開發，而不提供將其取代或淘汰的新 VIB，因此升級後舊 VIB 會保留在系統上。

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

必要條件

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

程序

- 1 升級 ESXi 並執行以下命令。

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

- 2 檢查輸出。

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

使用信賴平台模組保護 ESXi 主機

ESXi 主機可以使用信賴平台模組 (TPM) 晶片，這是安全的密碼處理器，可透過提供以硬體 (而非軟體) 為基礎的信任保證來增強主機安全性。



(ESXi 和信賴平台模組 2.0 功能示範)

什麼是 TPM

TPM 是安全密碼處理器的業界標準。如今，大多數電腦 (從筆記型電腦到桌上型電腦，再到伺服器) 中都含 TPM 晶片。vSphere 6.7 及更新版本支援 TPM 2.0 版。

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

遠端證明程序的高層級步驟如下：

- 1 建立遠端 TPM 的可信度，並在其上建立證明金鑰 (AK)。

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

- 2 從主機擷取證明報告。

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

3 驗證主機的真實性。

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

使用 TPM 時有哪些 vSphere 需求？

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

- vCenter Server 6.7 或更新版本
- 已在 UEFI 中安裝並啟用 TPM 2.0 晶片的 ESXi 6.7 或更新版本主機
- 已啟用 UEFI 安全開機

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

在下列位置檢閱經過 VMware 認證的 TPM 2.0 晶片：

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

使用 TPM 開機主機時會發生什麼情況？

將已安裝 TPM 2.0 晶片的 ESXi 主機開機時，vCenter Server 將監控主機的證明狀態。若要檢視硬體信任狀態，請在 vSphere Client 中選取 vCenter Server，然後選取**安全性**下的**摘要索引**標籤。硬體信任狀態有以下幾種：

- 綠色：正常狀態，表示完全信任。
- 紅色：證明失敗。

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

在 vSphere 7.0 及更新版本中，VMware® vSphere Trust Authority™ 為 ESXi 主機使用遠端證明功能。請參閱[什麼是 vSphere Trust Authority 證明服務](#)。

檢視 ESXi 主機證明狀態

新增至 ESXi 主機時，信賴平台模組 2.0 相容晶片會證明平台的完整性。您可以在 vSphere Client 中檢視主機的證明狀態。您也可以檢視 Intel Trusted Execution Technology (TXT) 狀態。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 導覽至資料中心，然後按一下**監控索引**標籤。
- 3 按一下**安全性**。

- 4 檢閱 [證明] 資料行中主機的狀態，並閱讀**訊息**資料行中隨附的訊息。
- 5 如果此主機是受信任的主機，請參閱**檢視受信任叢集證明狀態**以取得詳細資訊。

後續步驟

對於 [失敗] 或 [警告] 證明狀態，請參閱**疑難排解 ESXi 主機證明問題**。對於受信任的主機，請參閱**對受信任主機證明問題進行疑難排解**。

疑難排解 ESXi 主機證明問題

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

程序

- 1 檢視 ESXi 主機警示狀態和隨附的錯誤訊息。請參閱**檢視 ESXi 主機證明狀態**。
- 2 如果錯誤訊息為主機安全開機已停用，您必須重新啟用安全開機來解決此問題。
- 3 如果主機的證明狀態為失敗，請查看 vCenter Server vpxd.log 檔案中的下列訊息：

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

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

如需有關 vCenter Server 記錄檔 (包括位置和記錄輪替) 的詳細資訊，請參閱 VMware 知識庫文章，網址為 <https://kb.vmware.com/s/article/1021804>。

- 4 如需所有其他錯誤訊息，請連絡客戶支援部門。

ESXi 記錄檔

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

若要提高主機的安全性，請採取下列措施。

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

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

在 ESXi 主機上設定 Syslog

您可以使用 vSphere Client、VMware Host Client 或 `esxcli system syslog` 命令來設定 syslog 服務。

如需使用 `esxcli system syslog` 命令和其他 ESXCLI 命令的相關資訊，請參閱 ESXCLI 入門。如需有關如何為每個遠端主機規格中指定的連接埠開啟 ESXi 防火牆的詳細資料，請參閱[設定 ESXi 防火牆](#)。

程序

- 1 在 vSphere Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在**系統**下，按一下**進階系統設定**。
- 4 按一下**編輯**。
- 5 篩選 **syslog**。
- 6 若要全域設定記錄並設定各種進階設定，請參閱[ESXi Syslog 選項](#)。
- 7 (選擇性) 覆寫任何記錄的預設記錄大小和記錄輪替：
 - a 按一下您要自訂的記錄的名稱。
 - b 輸入所需的輪替次數和記錄大小。
- 8 按一下**確定**。

結果

對 Syslog 選項進行的變更將生效。

備註 使用 vSphere Client 或 VMware Host Client 定義的 Syslog 參數設定將立即生效。但是，使用 ESXCLI 定義的大多數設定都需要額外命令才能生效。如需詳細資料，請參閱[ESXi Syslog 選項](#)。

ESXi Syslog 選項

可以使用一組 syslog 選項定義 ESXi syslog 檔案和傳輸的行為。

除了基本設定 (如 `Syslog.global.logHost`) 之外，從 ESXi 7.0 Update 1 開始，還提供了用於自訂和 NIAP 符合性的進階選項清單。

備註 所有稽核記錄設定 (以 `Syslog.global.auditRecord` 開頭) 會立即生效。但是，對於使用 ESXCLI 定義的其他設定，請確保執行 `esxcli system syslog reload` 命令以啟用變更。

表 3-9. 舊版 Syslog 選項

選項	ESXCLI 命令	說明
Syslog.global.logHost	esxcli system syslog config set --loghost=<str>	定義用於訊息傳輸的遠端主機及規格清單 (以逗號分隔)。如果 loghost=<str> 欄位為空，則不會轉送任何記錄。雖然對接收 Syslog 訊息的遠端主機數量沒有硬限制，但最好將遠端主機的數量保持在 5 個或以下。遠端主機規格的格式為： protocol://hostname ipv4 ['ipv6'][:port]。該通訊協定必須為 TCP、UDP 或 SSL 之一。連接埠值可以是介於 1 到 65535 之間的任何十進位數字。如果未提供連接埠，則 SSL 和 TCP 將使用 1514。UDP 使用 514。例如：ssl://hostname:1514。
Syslog.global.defaultRotate	esxcli system syslog config set --default-rotate=<long>	要保留的舊記錄檔的最大數目。可全域設定該數目，也可針對個別子記錄器進行設定 (請參閱 Syslog.global.defaultSize)。
Syslog.global.defaultSize	esxcli system syslog config set --default-size=<long>	記錄檔的預設大小 (以 KiB 為單位)。檔案達到預設大小後，syslog 服務會建立一個新檔案。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	esxcli system syslog config set --logdir=<str>	記錄所在的目錄。該目錄可能位於掛接的 NFS 或 VMFS 磁碟區中。只有本機檔案系統中的 /scratch 目錄在重新開機後仍會存在。將目錄指定為 [datastorename] path_to_file，其中路徑相對於支援資料存放區的磁碟區的根目錄路徑。例如，路徑 [storage1] / systemlogs 會對應到路徑 /vmfs/volumes/storage1/systemlogs。
Syslog.global.logDirUnique	esxcli system syslog config set --logdir-unique=<bool>	指定要與 Syslog.global.logDir 值相連接的 ESXi 主機名稱。當多個 ESXi 主機登入共用檔案系統時，啟用此設定至關重要。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.certificate.checkSSLCerts	esxcli system syslog config set --check-ssl-certs=<bool>	將訊息傳輸至遠端主機時強制檢查 SSL 憑證。

表 3-10. 從 ESXi 7.0 Update 1 開始可用的 Syslog 選項

選項	ESXCLI 命令	說明
Syslog.global.auditRecord.storageCapacity	esxcli system auditrecords local set --size=<long>	指定位於 ESXi 主機上的稽核記錄儲存目錄的容量 (以 MiB 為單位)。無法減少稽核記錄儲存的容量。可以在啟用稽核記錄儲存之前或之後 (請參閱 Syslog.global.auditRecord.storageEnable) 增加容量。
Syslog.global.auditRecord.remoteEnable	esxcli system auditrecords remote enable	允許將稽核記錄傳送到遠端主機。遠端主機透過使用 Syslog.global.logHost 參數指定。
Syslog.global.auditRecord.storageDirectory	esxcli system auditrecords local set --directory=<dir>	指定稽核記錄儲存目錄的位置。啟用稽核記錄儲存 (請參閱 Syslog.global.auditRecord.storageEnable) 後，無法變更稽核記錄儲存目錄。
Syslog.global.auditRecord.storageEnable	esxcli system auditrecords local enable	在 ESXi 主機上啟用稽核記錄儲存。如果稽核記錄儲存目錄不存在，則使用 Syslog.global.auditRecord.storageCapacity 指定的容量建立該目錄。
Syslog.global.certificate.checkCRL	esxcli system syslog config set --crl-check=<bool>	啟用對 SSL 憑證鏈結中所有憑證的撤銷狀態檢查。 啟用 X.509 CRL 驗證，依預設不會根據產業慣例檢查這些 CRL。經過 NIAP 驗證的組態需要進行 CRL 檢查。由於實作限制，如果啟用了 CRL 檢查，則憑證鏈結中的所有憑證都必須提供 CRL 連結。 不要為與認證無關的安裝啟用 crl-check 選項，因為很難正確設定使用 CRL 檢查的環境。
Syslog.global.certificate.strictX509Compliance	esxcli system syslog config set --x509-strict=<bool>	啟用與 X.509 的嚴格符合性。在驗證期間，對 CA 根憑證執行額外的有效性檢查。通常不會執行這些檢查，因為 CA 根本來就受信任，並且可能會導致與現有設定錯誤的 CA 根不相容。經過 NIAP 驗證的組態甚至需要 CA 根來通過驗證。 不要為與認證無關的安裝啟用 x509-strict 選項，因為很難正確設定使用 CRL 檢查的環境。
Syslog.global.droppedMsgs.fileRotate	esxcli system syslog config set --drop-log-rotate=<long>	指定要保留的舊的已捨棄訊息記錄檔數。
Syslog.global.droppedMsgs.fileSize	esxcli system syslog config set --drop-log-size=<long>	指定切換到新訊息記錄檔之前每個捨棄的訊息記錄檔大小 (以 KiB 為單位)。

表 3-10. 從 ESXi 7.0 Update 1 開始可用的 Syslog 選項 (續)

選項	ESXCLI 命令	說明
Syslog.global.logCheckSSLCerts	esxcli system syslog config set --check-ssl-certs=<bool>	將訊息傳輸至遠端主機時強制檢查 SSL 憑證。 備註 已被取代。在 ESXi 7.0 Update 1 及更新版本中使用 Syslog.global.certificate.checkSSLCerts。
Syslog.global.logFilters	esxcli system syslog logfile [add remove set] ...	指定一或多個記錄篩選規格。每個記錄篩選器必須用雙分隔號「 」分隔。記錄篩選器的格式為：numLogs ident logRegexp。numLogs 設定所指定記錄訊息的記錄項目數目上限。達到此數目後，就會篩選並忽略指定的記錄訊息。ident 指定一或多個系統元件，以將篩選器套用於這些元件所產生的記錄訊息。logRegexp 以 Python 規則運算式語法指定區分大小寫的片語，以依內容篩選記錄訊息。
Syslog.global.logFiltersEnable		允許使用記錄篩選器。
Syslog.global.logLevel	esxcli system config set --log-level=<str>	指定記錄篩選層級。僅當對 syslog 精靈問題進行疑難排解時，才必須變更此參數。可以使用值 debug 表示最詳細層級，使用 info 表示預設詳細層級，使用 warning 表示僅警告或錯誤，使用 error 表示僅錯誤。
Syslog.global.msgQueueDropMark	esxcli system syslog config --queue-drop-mark=<long>)	指定佔訊息佇列容量的百分比，達到此值後捨棄訊息。
Syslog.global.remoteHost.connectRetryDelay	esxcli system syslog config set --default-timeout=<long>	指定連線嘗試失敗後重試連線到遠端主機之前的延遲 (以秒為單位)。
Syslog.global.remoteHost.maxMsgLen	esxcli system syslog config set --remote-host-max-msg-len=<long>	對於 TCP 和 SSL 通訊協定，此參數指定截斷發生之前 syslog 傳輸的最大長度 (以位元組為單位)。遠端主機訊息的預設最大長度為 1 KiB。可以將最大訊息長度增加到多達 16 KiB。但是，將此值提高到 1 KiB 以上不能確保長傳輸到達 syslog 收集器時未被截斷。例如，發出訊息的 syslog 基礎結構位於 ESXi 外部時。RFC 5426 將 UDP 通訊協定的最大訊息傳輸長度設定為 480 位元組 (IPV4) 和 1180 位元組 (IPV6)。
Syslog.global.vsanBacking	esxcli system syslog config set --vsan-backing=<bool>	允許將記錄檔和稽核記錄儲存目錄放置在 vSAN 叢集上。但是，啟用此參數可能會導致 ESXi 主機變得無回應。

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。

表 3-11. ESXi 記錄檔位置

元件	位置	用途
驗證	/var/log/auth.log	包含與本機系統驗證相關的所有事件。
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。
Shell 記錄	/var/log/shell.log	包含在 ESXi 中輸入的所有命令以及 Shell 事件 (例如，啟用 Shell) 的記錄。
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。
vCenter Server 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)。
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/vmware.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。
VMkernel	/var/log/vmkernel.log	記錄與虛擬機器以及 ESXi 有關的活動。
VMkernel 摘要	/var/log/vmksummary.log	用於判定 ESXi 的運作時間和可用性統計資料 (以逗號分隔)。
VMkernel 警告	/var/log/vmkwarning.log	記錄與虛擬機器有關的活動。
快速開機	/var/log/loadESX.log	包含與透過「快速開機」重新啟動 ESXi 主機相關的所有事件。
受信任基礎結構代理程式	/var/run/log/kmxa.log	記錄與 ESXi 受信任主機上的用戶端服務相關的活動。
金鑰提供者服務	/var/run/log/kmxd.log	記錄與 vSphere Trust Authority 金鑰提供者服務相關的活動。
證明服務	/var/run/log/attestd.log	記錄與 vSphere Trust Authority 證明服務相關的活動。
ESX Token 服務	/var/run/log/esxtokend.log	記錄與 vSphere Trust Authority ESX Token 服務相關的活動。
ESX API 轉寄站	/var/run/log/esxapiadapter.log	記錄與 vSphere Trust Authority API 轉寄站相關的活動。

確保 Fault Tolerance 記錄流量的安全

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

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

啟用 Fault Tolerance 加密

您可以加密 Fault Tolerance 記錄流量。

vSphere Fault Tolerance 在主要虛擬機器和次要虛擬機器之間頻繁執行檢查，以便次要虛擬機器可以從上次成功的檢查點快速恢復。檢查點包含自上一個檢查點以來已修改的虛擬機器狀態。您可以加密 Fault Tolerance 記錄流量。

開啟 Fault Tolerance 時，FT 加密預設為**隨機**，這表示僅在主要和次要主機均支援加密時啟用加密。如果您需要手動變更 FT 加密模式，請遵循此程序。

備註 Fault Tolerance 支援 vSphere 7.0 Update 2 及更新版本的 vSphere 虛擬機器加密。客體內和陣列式加密不依賴或干擾虛擬機器加密。擁有多個加密層會使用其他計算資源，這可能會影響虛擬機器效能。影響因硬體以及 I/O 的數量和類型而異，但對於大多數工作負載而言，整體效能影響可以忽略不計。重複資料刪除、壓縮和複寫等後端儲存功能的有效性和相容性也可能會受到虛擬機器加密的影響。

必要條件

FT 加密需要 SMP-FT。不支援對舊版 FT (記錄-重新執行 FT) 進行加密。

程序

- 1 選取虛擬機器，然後選擇**編輯設定**。
- 2 在**虛擬機器選項**下選取已加密 FT 下拉式功能表。
- 3 選取下列其中一個選項：

選項	說明
已停用	請勿開啟加密的 Fault Tolerance 記錄。
隨機	僅在雙方均支援時開啟加密。允許 Fault Tolerance 虛擬機器移到不支援加密的 Fault Tolerance 記錄的 ESXi 主機。
必要	為 Fault Tolerance 主要和次要主機選擇同時支援已加密 FT 記錄的主機。

備註 啟用虛擬機器加密時，FT 加密模式依預設會設定為**必要**且無法修改。

當 FT 加密模式設定為**必要**時：

- 開啟 FT 時，針對 FT 次要主機的放置，僅會列出支援 FT 加密的主機。
- FT 容錯移轉只能在支援 FT 加密的主機上執行。

- 4 按一下**確定**。

管理 ESXi 稽核記錄

稽核記錄符合 RFC 5424，且包含與事項相關的事件的資訊，例如針對 ESXi 主機上發生的事件記錄的時間、狀態、說明和使用者資訊。本機和遠端稽核記錄保留均可用。依預設，稽核記錄保留處於停用狀態。您必須手動啟用本機和遠端稽核模式。

本機 ESXi 稽核記錄作為包含近期稽核訊息的固定大小緩衝區執行。訊息填滿緩衝區後，新記錄將覆寫最早的記錄。遠端稽核記錄以標準 syslog 格式 (RFC 3164) 將相同的稽核記錄串流轉送到遠端伺服器，未加密或加密 (RFC 5425) 形式均可。稽核訊息符合 RFC 5424，但一般 syslog 訊息僅符合 RFC 3164。系統將產生的稽核訊息同時傳送到本機存放區和遠端存放區。

在主機與遠端存放區之間連線中斷期間，遠端存放區會捨棄產生的任何稽核訊息。重新連線後，系統會產生一條稽核訊息，指示可能存在訊息遺失情況。

設定稽核記錄

可以使用 ESXCLI 設定本機稽核記錄保留。如需詳細資訊，請參閱 ESXCLI 參考，網址為 <https://code.vmware.com/>。

檢視稽核記錄

您可以按如下方式檢視稽核記錄。

- 本機：使用 ESXi `/bin/viewAudit` 應用程式。
- 遠端：使用 ESXCLI 設定遠端稽核伺服器。

此外，還可以使用 `FetchAuditRecords` API (在 `DiagnosticsManager` 受管理物件中) 檢視稽核記錄。

保護 ESXi 組態安全

在 vSphere 7.0 Update 2 及更新版本中，將透過加密保護 ESXi 組態。

什麼是安全 ESXi 組態

許多 ESXi 服務將密碼儲存在其組態檔中。這些組態以封存檔形式保存在 ESXi 主機的開機區中。在 vSphere 7.0 Update 2 之前，已封存的 ESXi 組態檔未加密。在 vSphere 7.0 Update 2 及更新版本中，將會加密已封存的組態檔。因此，攻擊者無法直接讀取或更改此檔案，即使他們具有 ESXi 主機儲存區的實際存取權。

除了防止攻擊者存取密碼之外，將安全 ESXi 組態與 TPM 搭配使用時，還可以在重新開機期間儲存虛擬機器加密金鑰。當 ESXi 主機設有 TPM 時，會使用 TPM 將組態「封裝」到主機，從而保證了強大的安全性。因此，加密的工作負載能夠在金鑰伺服器無法使用或無法連線時繼續運作。請參閱 [ESXi 主機上的 vSphere 金鑰持續性](#)。

無需手動啟用 ESXi 組態加密。安裝或升級至 vSphere 7.0 Update 2 或更新版本時，將會加密已封存的 ESXi 組態檔。

如需瞭解與安全 ESXi 組態關聯的工作，請參閱 [管理安全 ESXi 組態](#)。

vSphere 7.0 Update 2 之前的 ESXi 組態檔概觀

ESXi 主機組態包括在主機上執行的每個服務的組態檔。組態檔通常位於 `/etc/` 目錄中，但它們也可以位於其他命名空間中。組態檔包含有關服務狀態的執行階段資訊。隨著時間推移，組態檔中的預設值可能會變更，例如，當您變更 ESXi 主機上的設定時。cron 工作會定期備份 ESXi 組態檔、在 ESXi 正常關閉時備份或根據需要進行備份，並在開機區中建立已封存的組態檔。當 ESXi 重新開機後，它會讀取已封存的組態檔，並重新建立 ESXi 在備份建立時所處的狀態。在 vSphere 7.0 Update 2 之前，已封存的組態檔是未加密的。因此，可以存取實體 ESXi 儲存區的攻擊者能夠在系統離線時讀取並更改此檔案。

如何實作安全 ESXi 組態

在將 ESXi 主機安裝或升級至 vSphere 7.0 Update 2 或更新版本後首次開機期間，會發生下列情況：

- 如果 ESXi 主機具有 TPM，且在韌體中已啟用，則已封存的組態檔會透過儲存在 TPM 中的加密金鑰進行加密。自此之後，主機組態將由 TPM 封裝。
- 如果 ESXi 主機沒有 TPM，ESXi 會使用金鑰衍生功能 (KDF) 為已封存的組態檔產生安全的組態加密金鑰。KDF 的輸入將儲存在磁碟的 `encryption.info` 檔案中。

備註 當 ESXi 主機具有已啟用 TPM 的裝置時，您將獲得額外的保護。

當 ESXi 主機在首次開機後重新開機時，會發生下列情況：

- 如果 ESXi 主機具有 TPM，則主機必須從 TPM 取得該特定主機的加密金鑰。如果 TPM 度量滿足建立加密金鑰時所使用的封裝原則，則主機會從 TPM 取得加密金鑰。
- 如果 ESXi 主機沒有 TPM，則 ESXi 會從 `encryption.info` 檔案讀取資訊以解除鎖定安全組態。

安全 ESXi 組態需求

- ESXi 7.0 Update 2 或更新版本
- TPM 2.0，用於組態加密並且能夠使用封裝原則

安全 ESXi 組態復原金鑰

安全 ESXi 組態包括復原金鑰。如果您必須復原 ESXi 安全組態，請使用您輸入其內容作為命令列開機選項的復原金鑰。可以列出復原金鑰以建立復原金鑰備份。此外，作為安全性需求的一部分，還可以輪替復原金鑰。

建立復原金鑰備份是管理安全 ESXi 組態的一個重要部分。vCenter Server 會產生一個警示，提醒您備份復原金鑰。

安全 ESXi 組態復原金鑰警示

建立復原金鑰備份是管理安全 ESXi 組態的一個重要部分。每當 TPM 模式下的 ESXi 主機連線到或重新連線到 vCenter Server 時，vCenter Server 都會產生一個警示，提醒您備份復原金鑰。重設警示後，除非條件變更，否則不會再次觸發該警示。

安全 ESXi 組態的最佳做法

請遵循以下關於安全 ESXi 復原金鑰的最佳做法：

- 列出復原金鑰時，該金鑰會暫時顯示在不受信任的環境中，並且位於記憶體中。移除金鑰追蹤。
 - 將主機重新開機會移除記憶體中的剩餘金鑰。
 - 為了增強保護，您可以在主機上啟用加密模式。請參閱[明確啟用主機加密模式](#)。
- 執行復原時：
 - 若要消除復原金鑰在不受信任的環境中的任何追蹤，請將主機重新開機。
 - 為了增強安全性，請在金鑰復原一次後，輪替復原金鑰以使用新金鑰。

什麼是 TPM 封裝原則

TPM 可使用平台設定暫存器 (PCR) 度量來實作用於限制對機密資料進行未經授權存取的原則。將具有 TPM 的 ESXi 主機安裝或升級至 vSphere 7.0 Update 2 及更新版本時，TPM 會使用涵蓋安全開機設定的原則來封裝敏感資訊。此原則會在首次使用 TPM 封裝資料時確認是否已啟用安全開機，然後，在後續開機過程中嘗試解除封裝資料時，安全開機仍必須處於啟用狀態。

安全開機是 UEFI 韌體標準的一部分。啟用 UEFI 安全開機的情況下，除非作業系統開機載入器具有有效的數位簽章，否則主機將拒絕載入任何 UEFI 驅動程式或應用程式。

您可以選擇停用或啟用 UEFI 安全開機強制執行。請參閱[啟用或停用安全開機強制執行以確保安全的 ESXi 組態](#)。

備註 如果在安裝或升級至 vSphere 7.0 Update 2 或更新版本時未啟用 TPM，可以稍後使用下列命令執行此操作。

```
esxcli system settings encryption set --mode=TPM
```

啟用 TPM 後，便無法復原設定。

即使為主機啟用了 TPM，`esxcli system settings encryption set` 命令也會在某些 TPM 上失敗。

- 在 vSphere 7.0 Update 2 中：來自 NationZ (NTZ) 的 TPM、來自 Infineon Technologies (IFX) 的 TPM 以及來自 Nuvoton Technologies Corporation (NTC) 的某些新型號 (例如 NPCT75x)
- 在 vSphere 7.0 Update 3 中：來自 NationZ (NTZ) 的 TPM

如果安裝或升級 vSphere 7.0 Update 2 或更新版本在首次開機期間無法使用 TPM，則安裝或升級將繼續，並且模式預設為 [無] (即，`--mode=NONE`)。由此產生的行為就像未啟用 TPM 一樣。

TPM 也可以在封裝原則中強制執行 `execInstalledOnly` 開機選項的設定。`execInstalledOnly` 強制執行是一個進階 ESXi 開機選項，可保證 VMkernel 僅執行作為 VIB 一部分進行正確封裝和簽署的二進位檔案。`execInstalledOnly` 開機選項依賴於安全開機選項。必須啟用安全開機強制執行，然後才能在封裝原則中強制執行 `execInstalledOnly` 開機選項。請參閱[啟用或停用 `execInstalledOnly` 強制執行以確保安全的 ESXi 組態](#)。

管理安全 ESXi 組態

可以使用 ESXCLI 命令列出安全 ESXi 組態復原金鑰、輪替復原金鑰，以及變更 TPM 原則 (例如，強制執行 UEFI 安全開機)。

列出安全 ESXi 組態復原金鑰的內容

可以使用 ESXCLI 顯示安全 ESXi 組態復原金鑰的內容。

此工作僅適用於具有 TPM 的 ESXi 主機。一般而言，可以列出安全 ESXi 組態復原金鑰的內容以建立備份，或作為輪替復原金鑰的一部分。

必要條件

- 可以存取 ESXCLI 命令集。您可以遠端執行 ESXCLI 命令，或在 ESXi Shell 中執行。
- 使用 ESXCLI 獨立版本或透過 PowerCLI 的所需權限：**主機.組態.設定**

程序

- 1 在 ESXi 主機上執行下列命令。

```
esxcli system settings encryption recovery list
```

- 2 如果您必須復原安全組態，請將輸出儲存在安全的遠端位置作為備份。

結果

此時會顯示復原金鑰識別碼和金鑰。

範例：列出安全 ESXi 組態復原金鑰

```
[root@host1] esxcli system settings encryption recovery list

Recovery ID                                Key
-----
{2DDD5424-7F3F-406A-8DA8-D62630F6C8BC}
478269-039194-473926-430939-686855-231401-642208-184477-602511
-225586-551660-586542-338394-092578-687140-267425
```

輪替安全 ESXi 組態復原金鑰

可以使用 ESXCLI 輪替安全 ESXi 組態復原金鑰。

此工作僅適用於具有 TPM 的 ESXi 主機。在安全性最佳做法中，您可以輪替 ESXi 安全組態復原金鑰。

必要條件

- 可以存取 ESXCLI 命令集。您可以遠端執行 ESXCLI 命令，或在 ESXi Shell 中執行。
- 使用 ESXCLI 獨立版本或透過 PowerCLI 的所需權限：**主機.組態.設定**

程序

1 列出復原金鑰。

請參閱[列出安全 ESXi 組態復原金鑰的內容](#)。

2 執行下列命令。

```
esxcli system settings encryption recovery rotate [-k keyID] -u uuid
```

在此命令中，選擇性 *keyID* 是 VMkernel 金鑰快取中的金鑰識別碼，而 *uuid* 是復原識別碼 (透過 `esxcli system settings encryption recovery list` 命令取得)。如果不提供選擇性金鑰識別碼，ESXi 會將舊復原金鑰取代為隨機產生的新復原金鑰。

結果

如果提供，則復原金鑰現已設定為金鑰識別碼所參考金鑰的內容。否則，ESXi 提供新的金鑰識別碼。

安全 ESXi 組態的疑難排解和復原

您可以對可能遇到的安全 ESXi 組態的開機問題進行疑難排解和復原。

如果清除 TPM (即重設 TPM 中的種子值)，或如果 TPM 出現故障，您必須採取步驟來復原 ESXi 安全組態。您必須具有復原金鑰，才能復原組態。在復原組態之前，ESXi 主機將無法開機。請參閱[復原安全 ESXi 組態](#)。

雖然此情況並不常見，但 ESXi 主機可能無法還原或解密安全組態，從而使主機無法開機。可能的情況包括：

- 變更為安全開機設定 (或其他原則)
- 實際竄改
- 復原金鑰無法使用

若要對這些狀況進行疑難排解，請參閱 VMware 知識庫文章，網址為 <https://kb.vmware.com/kb/81446>。

復原安全 ESXi 組態

如果 TPM 出現故障或如果您清除 TPM，則必須復原安全 ESXi 組態。在復原組態之前，ESXi 主機將無法開機。

復原安全 ESXi 組態指的是下列情況：

- 已清除 TPM (即，TPM 中的種子已重設)。
- TPM 出現了故障。

若要對其他安全 ESXi 組態問題進行疑難排解，請參閱 VMware 知識庫文章，網址為 <https://kb.vmware.com/kb/81446>。

手動執行復原。請勿在執行安裝或升級指令碼的過程中進行復原。

必要條件

取得復原金鑰。您先前應已列出並儲存復原金鑰。請參閱[列出安全 ESXi 組態復原金鑰的內容](#)。

程序

- 1 (選擇性) 如果 TPM 出現故障，請將磁碟 (具有開機區) 移至具有 TPM 的另一個主機。
- 2 啟動 ESXi 主機。
- 3 出現 ESXi 安裝程式視窗時，按 Shift+O 即可編輯開機選項。
- 4 在命令提示字元中，輸入開機選項以復原組態。

```
encryptionRecoveryKey=recovery_key
```

安全 ESXi 組態隨即復原，並且 ESXi 主機開機。

- 5 若要保留變更，請輸入以下命令：

```
/sbin/auto-backup.sh
```

後續步驟

輸入復原金鑰時，該金鑰會暫時顯示在不受信任的環境中，並且位於記憶體中。儘管並非必要，但最佳做法是透過將主機重新開機從記憶體中移除金鑰的殘留痕跡。或者，可以輪替金鑰。請參閱[輪替安全 ESXi 組態復原金鑰](#)。

啟用或停用安全開機強制執行以確保安全的 ESXi 組態

您可以選擇啟用 UEFI 安全開機強制執行，或停用先前啟用的 UEFI 安全開機強制執行。必須使用 ESXCLI，才能變更 ESXi 主機上 TPM 中的設定。

此工作僅適用於具有 TPM 的 ESXi 主機。UEFI 安全開機是一種韌體設定，用於確保由韌體啟動的軟體受到信任。每次開機後，都可以使用 TPM 強制啟用 UEFI 安全開機。

必要條件

- 可以存取 ESXCLI 命令集。您可以遠端執行 ESXCLI 命令，或在 ESXi Shell 中執行。
- 使用 ESXCLI 獨立版本或透過 PowerCLI 的所需權限：**主機.組態.設定**

程序

- 1 列出 ESXi 主機上的目前設定。

```
esxcli system settings encryption get
Mode: TPM
Require Executables Only From Installed VIBs: false
Require Secure Boot: true
```

如果安全開機強制執行已啟用，則 [需要安全開機] 會顯示為 true。如果安全開機強制執行已停用，則 [需要安全開機] 會顯示為 false。

如果模式顯示為 NONE，您必須在主機的韌體中啟用 TPM，並透過執行以下命令設定模式：

```
esxcli system settings encryption set --mode=TPM
```

2 啟用或停用安全開機強制執行。

選項	說明
啟動	a 正常關閉主機。 例如，在 vSphere Client 中的 ESXi 主機上按一下滑鼠右鍵，然後選取 電源 > 關閉 。
	b 在主機的韌體中啟用安全開機。 請參閱特定的廠商硬體說明文件。
	c 重新啟動主機。
	d 執行下列 ESXCLI 命令。 <pre>esxcli system settings encryption set --require-secure-boot=T</pre>
	e 驗證變更。 <pre>esxcli system settings encryption get Mode: TPM Require Executables Only From Installed VIBs: false Require Secure Boot: true</pre> 確認 [需要安全開機] 顯示為 true。
	f 若要儲存設定，請執行下列命令。 <pre>/sbin/auto-backup.sh</pre>
停用	a 執行下列 ESXCLI 命令。 <pre>esxcli system settings encryption set --require-secure-boot=F</pre>
	b 驗證變更。 <pre>esxcli system settings encryption get Mode: TPM Require Executables Only From Installed VIBs: false Require Secure Boot: false</pre> 確認 [需要安全開機] 顯示為 false。
	c 若要儲存設定，請執行下列命令。 <pre>/sbin/auto-backup.sh</pre> 您可以選擇在主機的韌體中停用安全開機，但此時無法再設定韌體設定和 TPM 強制執行之間的相依性。

結果

ESXi 主機會在啟用或停用安全開機強制執行的情況下執行，視您的選擇而定。

備註 如果在安裝或升級至 vSphere 7.0 Update 2 或更新版本時未啟用 TPM，可以稍後使用下列命令執行此操作。

```
esxcli system settings encryption set --mode=TPM
```

啟用 TPM 後，便無法復原設定。

即使為主機啟用了 TPM，`esxcli system settings encryption set` 命令也會在某些 TPM 上失敗。

- 在 vSphere 7.0 Update 2 中：來自 NationZ (NTZ) 的 TPM、來自 Infineon Technologies (IFX) 的 TPM 以及來自 Nuvoton Technologies Corporation (NTC) 的某些新型號 (例如 NPCT75x)
- 在 vSphere 7.0 Update 3 中：來自 NationZ (NTZ) 的 TPM

如果安裝或升級 vSphere 7.0 Update 2 或更新版本在首次開機期間無法使用 TPM，則安裝或升級將繼續，並且模式預設為 [無] (即，`--mode=NONE`)。由此產生的行為就像未啟用 TPM 一樣。

啟用或停用 `execInstalledOnly` 強制執行以確保安全的 ESXi 組態

您可以選擇啟用 `execInstalledOnly` 強制執行，或停用先前啟用的 `execInstalledOnly` 強制執行。必須使用 ESXCLI，才能變更 ESXi 主機上 TPM 中的設定。必須先啟用 UEFI 安全開機強制執行，然後才能啟用 `execInstalledOnly` 強制執行。

此工作僅適用於具有 TPM 的 ESXi 主機。`execInstalledOnly` 進階 ESXi 開機選項設定為 TRUE 時，可保證 VMkernel 僅執行作為 VIB 一部分進行封裝和簽署的二進位檔案。每次開機後，都可以使用 TPM 強制啟用此開機選項。

必要條件

- 若要啟用 `execInstalledOnly` 強制執行，您必須先啟用 UEFI 安全開機強制執行。`execInstalledOnly` 強制執行建立於 UEFI 安全開機強制執行之上。請參閱[啟用或停用安全開機強制執行以確保安全的 ESXi 組態](#)。
- 可以存取 ESXCLI 命令集。您可以遠端執行 ESXCLI 命令，或在 ESXi Shell 中執行。
- 使用 ESXCLI 獨立版本或透過 PowerCLI 的所需權限：**主機.組態.設定**

程序

- 1 列出 ESXi 主機上的目前設定。

```
esxcli system settings encryption get
Mode: TPM
Require Executables Only From Installed VIBs: false
Require Secure Boot: true
```

如果 `execInstalledOnly` 強制執行已啟用，則 `Require Executables Only From Installed VIBs` 會顯示為 `true`。如果 `execInstalledOnly` 強制執行已停用，則 `Require Executables Only From Installed VIBs` 會顯示為 `false`。若要啟用 `execInstalledOnly` 強制執行，則安全開機強制執行必須處於啟用狀態，並且 `Require Secure Boot` 在此案例中顯示為 `true`。

如果模式顯示為 `NONE`，您必須在主機的韌體中啟用 TPM，並透過執行以下命令設定模式：

```
esxcli system settings encryption set --mode=TPM
```

此外，如果 [需要安全開機] 顯示為 `False`，請參閱[啟用或停用安全開機強制執行以確保安全的 ESXi 組態](#)以啟用實作。

2 啟用或停用 execInstalledOnly 強制執行。

選項	說明
啟動	<p>a 確認已啟用安全開機選項。</p> <pre>esxcli system settings encryption get Mode: TPM Require Executables Only From Installed VIBs: false Require Secure Boot: true</pre> <p>確認 Require Secure Boot 顯示為 true。若非如此，請參閱啟用或停用安全開機強制執行以確保安全的 ESXi 組態。</p>
	<p>b 若要將 execInstalledOnly 開機選項的執行階段值設定為 TRUE，請執行下列 ESXCLI 命令。</p> <pre>esxcli system settings kernel set -s execInstalledOnly -v TRUE</pre>
	<p>c 正常關閉主機。</p> <p>例如，在 vSphere Client 中的 ESXi 主機上按一下滑鼠右鍵，然後選取電源 > 關閉。</p>
	<p>d 重新啟動主機。</p>
	<p>e 若要設定 execInstalledOnly 強制執行，請執行下列 ESXCLI 命令。</p> <pre>esxcli system settings encryption set --require-exec-installed-only=T</pre>
	<p>f 驗證變更。</p> <pre>esxcli system settings encryption get Mode: TPM Require Executables Only From Installed VIBs: true Require Secure Boot: true</pre> <p>確認 Require Executables Only From Installed VIBs 顯示為 true。</p>
	<p>g 若要儲存設定，請執行下列命令。</p> <pre>/sbin/auto-backup.sh</pre>
停用	<p>a 執行下列 ESXCLI 命令。</p> <pre>esxcli system settings encryption set --require-exec-installed-only=F</pre>
	<p>b 驗證變更。</p> <pre>esxcli system settings encryption get Mode: TPM Require Executables Only From Installed VIBs: false Require Secure Boot: true</pre> <p>確認 Require Executables Only From Installed VIBs 顯示為 false。</p>
	<p>c 若要儲存設定，請執行下列命令。</p> <pre>/sbin/auto-backup.sh</pre>

選項	說明
	TPM 不再強制執行 execInstalledOnly 開機選項。

結果

ESXi 主機會在啟用或停用 execInstalledOnly 強制執行的情況下執行，視您的選擇而定。

停用 execInstalledOnly 進階組態執行階段選項

安裝或升級到 ESXi 8.0 時，依預設會在主機上啟用 execInstalledOnly 進階組態執行階段選項。此選項有助於保護主機免受惡意軟體攻擊。如果 ESXi 8.0 主機仍執行來自外部來源的非 VIB 二進位檔，則可以停用 execInstalledOnly 進階組態執行階段選項。

execInstalledOnly 選項可確保 VMkernel 僅執行已作為有效 VIB 一部分進行正確封裝和簽署的二進位檔案，從而幫助保護主機免受惡意軟體攻擊。

execInstalledOnly 選項既是開機選項，也是執行階段選項。execInstalledOnly 開機選項 (也稱為核心選項) 是在 ESXi 5.5 中引入的。依預設，execInstalledOnly 開機選項處於停用狀態。從 vSphere 7.0 Update 2 開始，可以在每次使用 TPM 開機時強制執行 execInstalledOnly 開機選項。如需詳細資訊，請參閱 [啟用或停用 execInstalledOnly 強制執行以確保安全的 ESXi 組態](#)。

依預設，ESXi 8.0 中新增的 execInstalledOnly 進階組態執行階段選項在主機上處於啟用狀態。依預設，execInstalledOnly 開機選項會繼續處於停用狀態，但先前啟用的 execInstalledOnly 開機選項會在您設定了這兩個選項時覆寫執行階段選項。

備註 execInstalledOnly 選項獨立於安全開機之外。安全開機會檢查所有已安裝的 VIB 是否已簽署。如需詳細資訊，請參閱 [ESXi 主機的 UEFI 安全開機](#)。

停用 execInstalledOnly 執行階段選項後，會針對主機顯示 vCenter Server 警告。

必要條件

若要停用 execInstalledOnly 選項，您必須對 ESXi 主機擁有根存取權。可以使用 ESXCLI、PowerCLI 或 API。接下來的工作使用 ESXCLI。

注意 停用 execInstalledOnly 進階組態執行階段選項會讓您更容易受到攻擊。

程序

- 1 使用 SSH 連線至 ESXi 主機。
- 2 若要停用 execInstalledOnly 執行階段選項，請輸入以下 ESXCLI 命令。

```
esxcli system settings advanced set -o /User/execInstalledOnly -i 0
```

保護 vCenter Server 系統的安全

4

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

本章節討論下列主題：

- vCenter Server 存取控制的最佳做法
- 限制 vCenter Server 的網路連線
- vCenter Server 安全性最佳做法
- vCenter 密碼需求與鎖定行為
- 驗證舊版 ESXi 主機的指紋
- vCenter Server 所需的連接埠

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。

使用具名帳戶存取 vCenter Server

- 將管理員角色僅授與需要擁有該角色的管理員。對於擁有較多限制權限的管理員，您可以建立自訂角色或使用無密碼編譯管理員角色。請勿將此角色套用到其成員資格未受到嚴格控制的任何群組。
- 確保應用程式在連線至 vCenter Server 系統時使用唯一服務帳戶。

監控 vCenter Server 管理員使用者的權限

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

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

最大程度地減少對 vCenter Server Appliance 的存取

請勿允許使用者直接登入 vCenter Server Appliance。已登入 vCenter Server Appliance 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 Server 認證，例如 SSL 憑證。僅允許要執行合法工作的使用者登入系統，並確保對這些登入事件進行稽核。

為資料庫使用者授與最低權限

資料庫使用者僅需要專屬於資料庫存取權的特定權限。

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

限制資料存放區瀏覽器存取權

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

限制使用者在虛擬機器中執行命令

依預設，具有管理員角色的使用者可以與虛擬機器內客體作業系統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 **虛擬機器.客體作業** 權限的自訂非客體存取角色。請參閱 [限制使用者在虛擬機器中執行命令](#)。

考量修改 vpxuser 的密碼原則

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

備註 確保密碼使用期限原則不會過短。

重新啟動 vCenter Server 後檢查權限

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

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

對遠端桌面通訊協定使用高加密層級

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

驗證 vSphere Client 憑證

指示 vSphere Client 或其他用戶端應用程式的使用者留意憑證驗證警告。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 Client 中變更該值。

程序

- 1 使用 vSphere Client 登入 vCenter Server 系統。
- 2 在物件階層中，選取 vCenter Server 系統。
- 3 按一下**設定**。
- 4 按一下**進階設定**，然後按一下**編輯設定**。
- 5 按一下**篩選器**圖示，然後輸入 `VimPasswordExpirationInDays`。
- 6 設定 `VirtualCenter.VimPasswordExpirationInDays` 以符合您的需求。

從失敗的安裝移除到期或撤銷的憑證和記錄

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

出於以下原因，需要移除到期或撤銷的憑證。

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

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 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。

- 基礎結構服務，例如 DNS、Active Directory 以及 PTP 或 NTP。
- 執行對 vCenter Server 系統功能至關重要的元件的其他系統。

在 vCenter Server 上使用防火牆。包括以 IP 為基礎的存取限制，這樣只有必要的元件才能與 vCenter Server 系統通訊。

評估 Linux 用戶端搭配 CLI 和 SDK 的使用情況

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

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

- ESXCLI 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。
- 使用堡壘主機 (跳轉盒系統) 確保 Linux 用戶端受「跳轉」限制。

檢查 vSphere Client 外掛程式

vSphere 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安裝。

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

使用可延伸性架構會導致引入誤用功能的風險。例如，如果管理員在 vSphere 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 Client 免受潛在的危害，請定期檢查所有已安裝的外掛程式，並確保所有外掛程式均來自受信任的來源。

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 Client。
- 2 在首頁上，選取**管理**，然後選取**解決方案**下的**用戶端外掛程式**。

3 檢查用戶端外掛程式清單。

vCenter Server 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。採取額外步驟更有助於提高 vCenter Server 的安全性。

設定精確時間通訊協定或網路時間通訊協定

確保所有系統使用相同的相對時間來源。此時間來源必須與商定的時間標準 (如國際標準時間 (UTC)) 同步。同步的系統對於憑證驗證來說至關重要。精確時間通訊協定 (PTP) 和網路時間通訊協定 (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 與 NTP 伺服器的時間同步](#)。

限制 vCenter Server 網路存取

限制對與 vCenter Server 進行通訊所需元件的存取。封鎖來自不必要系統的存取可降低對作業系統發動攻擊的潛在可能性。

如需 VMware 產品 (包括 vSphere 和 vSAN) 中所有支援的連接埠和通訊協定的清單，請參閱 VMware Ports and Protocols Tool™，網址為 <https://ports.vmware.com/>。可以依 VMware 產品搜尋連接埠、建立自訂連接埠清單，以及列印或儲存連接埠清單。

設定 Bastion 主機

若要幫助保護資產，請設定 bastion 主機 (也稱為跳轉盒) 以執行提升的管理工作。Bastion 主機是一種專用電腦，可主控最低數量的管理應用程式。將移除所有其他不必要的服務。主機通常位於管理網路上。Bastion 主機透過將登入限制為主要個人、要求防火牆規則登入以及使用稽核工具新增監控來提高資產的保護。

vCenter 密碼需求與鎖定行為

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

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

vCenter Single Sign-On 管理員密碼需求

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

- 至少 8 個字元
- 至少一個小寫字元
- 至少一個數字字元

- 至少一個特殊字元

該使用者的密碼長度不得超過 20 個字元。允許使用非 ASCII 字元。管理員可以變更預設密碼原則。請參閱 vSphere 驗證說明文件。

vCenter Server 密碼需求

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

vCenter Single Sign-On 鎖定行為

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

vCenter Single Sign-On 網域管理員 (預設為 administrator@vsphere.local) 不受鎖定原則的影響。使用者受密碼原則影響。

vCenter Server 密碼變更

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

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

驗證舊版 ESXi 主機的指紋

在 vSphere 6.0 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 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 Client 詳細目錄中，瀏覽到 vCenter Server。
- 2 按一下**設定**。
- 3 在**設定**底下，按一下**一般**。
- 4 按一下**編輯**。
- 5 按一下**SSL 設定**。
- 6 如果有需要手動驗證的 ESXi 5.5 或更早版本的主機，請比較主機列出的指紋和主機主控台下的指紋。
若要取得主機憑證指紋，請使用 Direct Console 使用者介面 (DCUI)。
 - a 登入 Direct Console 並按 F2，存取 [系統自訂] 功能表。
 - b 選取**檢視支援資訊**。

主機憑證指紋會出現在右側資料行中。

7 如果指紋相符，則選取主機旁邊的**確認**核取方塊。

按一下**確定**之後，未選取的主機將中斷連線。

8 按一下**儲存**。

vCenter Server 所需的連接埠

vCenter Server 系統必須能夠將資料傳送到每台受管理主機，並從 vSphere Client 接收資料。若要在受管理主機之間啟用移轉和佈建活動，來源主機和目的地主機之間必須能夠透過預先決定的 TCP 和 UDP 連接埠來接收資料。

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。如需 vSphere 中所有支援的連接埠和通訊協定的清單，請參閱 VMware Ports and Protocols Tool™，網址為 <https://ports.vmware.com>。

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

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

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

確保虛擬機器安全

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。如實體機器一樣保護虛擬機器安全，並遵循本文件和《安全性組態指南》(以前稱為《強化指南》) 中所述的最佳做法。

《安全性組態指南》的網址為 <https://core.vmware.com/security>。

本章節討論下列主題：

- 對虛擬機器啟用或停用 UEFI 安全開機
- 限制資訊訊息從虛擬機器流向 VMX 檔案
- 虛擬機器安全性最佳做法
- 使用 Intel 軟體防護延伸保護虛擬機器
- 使用 AMD 安全加密虛擬化-加密狀態保護虛擬機器

對虛擬機器啟用或停用 UEFI 安全開機

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

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

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

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

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

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

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

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

此工作說明如何使用 vSphere Client 來啟用和停用虛擬機器的安全開機。您也可以撰寫指令碼來管理虛擬機器設定。例如，您可以使用下列 PowerCLI 程式碼，自動將虛擬機器的韌體從 BIOS 變更為 EFI：

```
$vm = Get-VM TestVM

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]::efi
$vm.ExtensionData.ReconfigVM($spec)
```

如需詳細資訊，請參閱《VMware PowerCLI 使用者指南》。

必要條件

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

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

備註 部分客體作業系統不支援在不修改客體作業系統的情況下，從 BIOS 開機變更為 UEFI 開機。變更為 UEFI 開機之前，請參閱您的客體作業系統說明文件。如果您將已使用 UEFI 開機的虛擬機器升級到支援 UEFI 安全開機的作業系統，則可以對該虛擬機器啟用安全開機。

- 關閉虛擬機器。如果虛擬機器正在執行，則此核取方塊會以灰色顯示。

程序

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

結果

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

限制資訊訊息從虛擬機器流向 VMX 檔案

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

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

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

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

程序

- 1 在 vSphere Client 詳細目錄中，瀏覽至虛擬機器。
- 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。

虛擬機器安全性最佳做法

遵循虛擬機器安全性最佳做法可協助確保 vSphere 部署的完整性。

■ 虛擬機器一般保護

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

■ 使用範本部署虛擬機器

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

■ 儘量少用虛擬機器主控台

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

■ 防止虛擬機器接管資源

當某個虛擬機器耗用過多主機資源，而使主機上的其他虛擬機器無法執行其預期功能時，可能會出現拒絕服務 (DoS)。為防止虛擬機器造成 DoS 問題，請使用主機資源管理功能，例如設定共用率和使用資源集區。

■ 停用虛擬機器中不必要的功能

在虛擬機器中執行的任何服務都有可能引發攻擊。透過停用不是支援系統上執行的應用程式或服務所必需的系統元件，可降低受到攻擊的可能性。

虛擬機器一般保護

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

請遵循以下最佳做法來保護您的虛擬機器。如需有關其他資訊，請參閱《vSphere 安全性組態指南》，網址為 <https://core.vmware.com/security-configuration-guide>。

修補虛擬機器

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，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。

掃描虛擬機器中的病毒

由於每台虛擬機器都主控標準作業系統，因此必須安裝防毒軟體，避免感染病毒。根據虛擬機器的使用方式，可能還需要安裝軟體防火牆。

請錯開病毒掃描的排程，尤其是在具有大量虛擬機器的部署中。如果同時掃描所有虛擬機器，環境中的系統效能將大幅降低。因為軟體防火牆和防毒軟體需要佔用大量虛擬化資源，因此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。

停用虛擬機器上的序列埠

序列埠是用於連線周邊設備與虛擬機器的介面。管理員通常使用序列埠提供與伺服器主控台的直接、低層級的連線。虛擬序列埠允許對虛擬機器執行相同的存取。因為序列埠允許低層級存取，但不具有嚴格的控制 (如記錄或權限)，所以請在虛擬機器上將其保留為停用。

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，主控台存取可能造成對虛擬機器的惡意攻擊。

程序

- 1 請使用原生遠端管理服務 (如終端服務和 SSH) 與虛擬機器進行互動。

請僅在需要時才授與對虛擬機器主控台的存取權限。

- 2 限制與虛擬機器主控台的連線。

例如，在高度安全的環境中，限制與一個主控台的連線。在某些環境中，若完成一般工作需要多個並行連線，您可增加限制。

- a 在 vSphere Client 中，關閉虛擬機器的電源。
- b 在虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
- c 按一下**虛擬機器選項索引**標籤，然後展開 **VMware 遠端主控台選項**。
- d 輸入工作階段的數目上限，例如 2。
- e 按一下**確定**。

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。

在完全瞭解影響之前，請勿設定限制或使用資源集區。

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

在虛擬機器中執行的任何服務都有可能引發攻擊。透過停用不是支援系統上執行的應用程式或服務所必需的系統元件，可降低受到攻擊的可能性。

通常，虛擬機器需要的服務或功能不像實體伺服器那樣多。對系統進行虛擬化時，請評估特定服務或功能是否必要。

備註 可能的話，請使用「最小」或「核心」安裝模式安裝客體作業系統，以減少客體作業系統的大小、複雜性和攻擊面。

程序

- ◆ 停用作業系統中未使用的服務。
例如，如果系統執行檔案伺服器，則關閉所有 Web 服務。
- ◆ 中斷未使用的實體裝置 (如 CD/DVD 光碟機、軟碟機和 USB 介面卡) 的連線。
- ◆ 停用未使用的功能 (例如未使用的顯示功能)，或停用能向虛擬機器 (主機客體檔案系統) 共用主機檔案的 VMware 共用資料夾。
- ◆ 關閉螢幕保護程式。
- ◆ 除非必要，否則不要在 Linux、BSD 或 Solaris 客體作業系統上執行 X Window 系統。

從虛擬機器中移除不必要的硬體裝置

虛擬機器中的任何啟用或連線的裝置都表示潛在的攻擊通道。虛擬機器上具有權限的使用者和程序可以連線或中斷連線硬體裝置 (如網路介面卡和 CD-ROM 光碟機)。攻擊者可利用該能力破壞虛擬機器安全性。移除不必要的硬體裝置可以協助防止攻擊。

具有虛擬機器存取權限的攻擊者可以連線已中斷連線的硬體裝置，並存取留存在硬體裝置中媒體上的敏感資訊。攻擊者可能會中斷網路介面卡的連線，將虛擬機器與其網路隔離，導致拒絕服務。

- 請勿將未經授權的裝置連線到虛擬機器。
- 移除不需要或未使用的硬體裝置。
- 從虛擬機器中停用不必要的虛擬裝置。
- 確保僅將所需的裝置連線到虛擬機器。虛擬機器很少使用序列埠或平行埠。一般來說，在軟體安裝期間，CD/DVD 磁碟機僅會暫時連線。

程序

- 1 在 vSphere Client 詳細目錄中，瀏覽至虛擬機器。
- 2 在虛擬機器上按一下滑鼠右鍵，然後按一下 **編輯設定**。
- 3 停用不需要的硬體裝置。

包括對下列裝置的檢查：

- 序列埠
- 平行埠
- USB 控制器

■ CD-ROM 光碟機

備註 您必須使用 PowerCLI 命令管理 vSphere 7.0 及更新版本中的軟碟機裝置。

停用虛擬機器上未使用的顯示功能

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。

必要條件

關閉虛擬機器電源。

程序

- 1 在 vSphere Client 詳細目錄中，瀏覽至虛擬機器。
- 2 在虛擬機器上按一下滑鼠右鍵，然後按一下 **編輯設定**。
- 3 選取**虛擬機器選項**。
- 4 按一下**進階**，然後按一下**編輯組態**。
- 5 如果適用，請新增或編輯下列參數。

選項	說明
<code>svga.vgaonly</code>	如果將此參數設定為 TRUE，則進階圖形功能將不再運作。對於現代客體作業系統，不要將此參數設定為 TRUE，因為它們無法正常運作。如果 <code>svga.vgaonly</code> 設定為 TRUE，則只有字元儲存格主控台模式可用。如果使用此設定， <code>mks.enable3d</code> 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。
<code>mks.enable3d</code>	在不需要 3D 功能的虛擬機器上將此參數設定為 FALSE。

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 Client 進行啟用。

為了確保安全環境，這些選項會設有預設值。但是，如果要使稽核工具能夠檢查設定是否正確，則必須將它們明確設定為 true。

必要條件

關閉虛擬機器。

程序

- 1 在 vSphere Client 詳細目錄中，瀏覽至虛擬機器。
- 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 確保 [名稱] 和 [值] 資料行中存在以下值，或新增這些值。

名稱	值
<code>isolation.tools.copy.disable</code>	<code>true</code>
<code>isolation.tools.paste.disable</code>	<code>true</code>
<code>isolation.tools.setGUIOptions.enable</code>	<code>false</code>

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。

- 6 按一下**確定**。
- 7 (選擇性) 如果變更了組態參數，則要重新啟動虛擬機器。

限制公開複製到虛擬機器主控台剪貼簿中的敏感資料

依預設，系統已停用針對主機的複製和貼上作業，以防止曝光已複製到剪貼簿中的敏感資料。

在執行 VMware Tools 的虛擬機器上啟用複製和貼上時，可以在客體作業系統和遠端主控台之間執行複製和貼上作業。當主控台視窗取得焦點時，虛擬機器中執行的程序和無權限使用者可存取虛擬機器主控台剪貼簿。如果使用者在使用主控台前將敏感資訊複製到剪貼簿中，使用者就可以向虛擬機器曝光敏感資料。為防止出現此問題，預設會停用針對客體作業系統的複製和貼上作業。

必要時，可以為虛擬機器啟用複製和貼上作業。

限制使用者在虛擬機器中執行命令

依預設，具有 vCenter Server 管理員角色的使用者可與虛擬機器客體作業系統內的檔案和應用程式進行互動。若要降低破壞客體機密性、可用性或完整性的風險，請建立不包括**虛擬機器.客體作業**權限的非客體存取角色。將該角色指派給不需要虛擬機器檔案存取的管理員。

出於安全性考慮，請嚴格限制對虛擬資料中心的存取，嚴格程度與限制對實體資料中心的存取相同。將不包括**虛擬機器.客體作業**權限的自訂角色套用至需要管理員權限但未授權與客體作業系統檔案和應用程式進行互動的使用者。

例如，某個組態可能在基礎結構中包括虛擬機器，該基礎結構帶有敏感資訊。

如果 vMotion 移轉等工作要求資料中心管理員可以存取虛擬機器，則停用一些遠端客體作業系統作業可確保這些管理員無法存取敏感資訊。

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 Client，該使用者在您要建立角色的 vCenter Server 系統擁有**管理員**權限。
- 2 選取**管理**，然後按一下**角色**。
- 3 按一下**管理員**角色，然後按一下**複製**。

- 輸入角色名稱和說明，然後按一下**確定**。

例如，輸入**無客體存取權限的管理員**。

- 選取複製的角色，然後按一下**編輯**。
- 在**虛擬機器**權限下，取消選取 [客體作業]。
- 按一下**儲存**。

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。從管理員角色中移除這些使用者。

防止虛擬機器使用者或程序中斷裝置的連線

虛擬機器內不具有根權限或管理員權限的使用者和程序能夠與裝置 (如網路介面卡和 CD-ROM 光碟機) 連線或中斷連線，還能夠修改裝置設定。若要提高虛擬機器的安全性，請移除這些裝置。

可以透過變更虛擬機器的進階設定，防止客體作業系統中的虛擬機器使用者以及在客體作業系統中執行的程序對裝置進行任何變更。

必要條件

關閉虛擬機器。

程序

- 在 vSphere Client 詳細目錄中，瀏覽至虛擬機器。
- 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。
- 按一下**進階參數**索引標籤。
- 請確認 [名稱] 和 [值] 資料行中存在以下值，否則新增該值。

名稱	值
isolation.device.connectable.disable	true

此設定不會影響 vSphere 管理員連線或中斷連線已連結到虛擬機器的裝置的能力。

- 按一下**確定**。

阻止客體作業系統程序向主機傳送組態訊息

若要確保客體作業系統不會修改組態設定，您可以阻止這些程序將任何名稱值配對寫入到組態檔中。

必要條件

關閉虛擬機器。

程序

- 在 vSphere Client 詳細目錄中，瀏覽至虛擬機器。

- 2 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。
- 3 按一下**進階參數索引**標籤。
- 4 請確認 [名稱] 和 [值] 資料行中存在以下值，否則新增該值。

欄	值
名稱	isolation.tools.setinfo.disable
值	true

- 5 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。

使用 Intel 軟體防護延伸保護虛擬機器

vSphere 可讓您為虛擬機器設定虛擬 Intel® 軟體防護延伸 (vSGX)。使用 vSGX 可以為工作負載提供額外的安全性。

某些新型 Intel CPU 會執行稱為 Intel® 軟體防護延伸 (Intel® SGX) 的安全性延伸。Intel SGX 是一種特定於處理器的技術，適用於致力於保護特定代碼和資料免遭洩漏或修改的應用程式開發人員。Intel SGX 允許使用者層級代碼定義記憶體的私有區域 (稱為 Enclave)。Enclave 內容受到保護，因此，在 Enclave 外部執行的代碼無法存取 Enclave 內容。

vSGX 允許虛擬機器使用 Intel SGX 技術 (如果在硬體上可用)。若要使用 vSGX，ESXi 主機必須安裝在支援 SGX 的 CPU 上，並且必須在 ESXi 主機的 BIOS 中啟用 SGX。您可以使用 vSphere Client 為虛擬機器啟用 SGX。

從 vSphere 8.0 開始，可以對已啟用 vSGX 的虛擬機器使用遠端證明。Intel SGX 遠端證明是一種安全機制，允許您與受信任的遠端實體建立經過驗證的安全通訊通道。若要對使用 SGX Enclave 的虛擬機器使用遠端證明，具有單一 CPU 通訊端的主機不需要 Intel 登錄。若要在具有多個 CPU 通訊端的主機中執行的虛擬機器上啟用遠端證明，必須先向 Intel 登錄伺服器登錄該主機。如果具有多個 CPU 通訊端且支援 SGX 的主機未向 Intel 登錄伺服器登錄，則只能開啟不需要遠端證明且已啟用 vSGX 的虛擬機器的電源。

如需有關向 Intel 登錄伺服器登錄多通訊端 ESXi 主機的詳細資訊，請參閱 vCenter Server 和主機管理說明文件。

vSGX 入門

虛擬機器可使用 Intel SGX 技術 (如果在硬體上可用)。

vSGX 對 vSphere 的需求

若要使用 vSGX，您的 vSphere 環境必須符合下列需求：

- 虛擬機器需求：
 - EFI 韌體
 - 硬體版本 17 或更新版本
 - 若要啟用遠端證明，請使用硬體版本 20 或更新版本
- 元件需求：
 - vCenter Server 7.0 及更新版本
 - ESXi 7.0 及更新版本
 - ESXi 主機必須安裝在支援 SGX 的 CPU 上，並且必須在 ESXi 主機的 BIOS 中啟用 SGX。
 - 若要為主機啟用遠端證明，請向 Intel 登錄伺服器登錄主機。這樣一來，在主機上執行的虛擬機器就可以使用遠端證明。如需有關如何登錄多通訊端 ESXi 的詳細資訊，請參閱 vCenter Server 和主機管理說明文件。
- 客體作業系統支援：
 - Linux
 - Windows Server 2016 (64 位元) 及更新版本
 - Windows 10 (64 位元) 及更新版本

vSGX 支援的 Intel 硬體

如需適用於 vSGX 的受支援的 Intel 硬體，請參閱位於 <https://www.vmware.com/resources/compatibility/search.php> 的《vSphere 相容性指南》。

您可能需要在某些 CPU 上關閉超執行緒，以在 ESXi 主機上啟用 SGX。如需詳細資訊，請參閱 VMware 知識庫文章，網址為 <https://kb.vmware.com/s/article/71367>。

vSGX 上不支援的 VMware 功能

啟用 vSGX 時，虛擬機器不支援下列功能：

- vMotion/DRS 移轉
- 虛擬機器暫停和繼續
- 虛擬機器快照 (如果不建立虛擬機器記憶體快照，則支援虛擬機器快照)。

- Fault Tolerance
- 客體完整性 (GI, VMware AppDefense™ 1.0 的平台基礎)

備註 由於 Intel SGX 架構的運作方式，這些 VMware 功能不受支援。並非由 VMware 弊端所致。

在虛擬機器上啟用 vSGX

您可以在建立虛擬機器的同時，在虛擬機器上啟用 vSGX。

必要條件

請參閱 [vSGX 對 vSphere 的需求](#)。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。
- 3 在物件上按一下滑鼠右鍵，選取**新虛擬機器**，然後遵循提示來建立虛擬機器。
- 4 在**自訂硬體**頁面上，按一下**虛擬硬體**索引標籤，然後展開**安全性裝置**。
- 5 若要啟用 SGX，請選取**啟用核取方塊**。
- 6 在**Enclave 頁面快取大小 (MB)** 文字方塊中，輸入快取大小 (以 MB 為單位)。

備註 Enclave 頁面快取大小必須為 2 MB 的倍數。

- 7 若要防止虛擬機器開啟不支援 SGX 遠端證明的主機 (如解除登錄的多通訊端 SGX 主機) 的電源，請選取**遠端證明**核取方塊。
- 8 從**啟動控制組態**下拉式功能表中，選取適當模式。

選項	動作
已解除鎖定	此選項可啟用客體作業系統的啟動 Enclave 組態。
已鎖定	<p>此選項可讓您設定啟動 Enclave。</p> <ol style="list-style-type: none"> a 選取啟動 Enclave 公開金鑰雜湊選項。 b 若要使用主機上設定的其中一個公開金鑰，請選取從主機使用，然後從下拉式功能表中選取公開金鑰雜湊。 c 若要手動輸入公開金鑰，請選取手動輸入，然後輸入有效的 SHA256 雜湊 (64 字元金鑰)。

- 9 按一下**確定**。

在現有虛擬機器上啟用 vSGX

您可以在現有虛擬機器上啟用 vSGX。

必要條件

請參閱 [vSGX 對 vSphere 的需求](#)。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在您想要修改的詳細目錄中的虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
- 3 在**虛擬硬體**索引標籤上，展開**安全性裝置**。
- 4 若要啟用 SGX，請選取**啟用核取方塊**。
- 5 在 **Enclave 頁面快取大小 (MB)** 文字方塊中，輸入快取大小 (以 MB 為單位)。

備註 Enclave 頁面快取大小必須為 2 MB 的倍數。

- 6 若要防止虛擬機器開啟不支援 SGX 遠端證明的主機 (如解除登錄的多通訊端 SGX 主機) 的電源，請選取**遠端證明核取方塊**。
- 7 從**啟動控制組態**下拉式功能表中，選取適當模式。

選項	動作
已解除鎖定	此選項可啟用客體作業系統的啟動 Enclave 組態。
已鎖定	<p>此選項可讓您設定啟動 Enclave。</p> <ol style="list-style-type: none"> a 選取啟動 Enclave 公開金鑰雜湊選項。 b 若要使用主機上設定的其中一個公開金鑰，請選取從主機使用，然後從下拉式功能表中選取公開金鑰雜湊。 c 若要手動輸入公開金鑰，請選取手動輸入，然後輸入有效的 SHA256 雜湊 (64) 字元金鑰。

- 8 按一下**確定**。

從虛擬機器移除 vSGX

您可以從虛擬機器中移除 vSGX。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在您想要修改的詳細目錄中的虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
- 3 在**編輯設定**對話方塊的**安全性裝置**下，針對 SGX 取消選取**啟用核取方塊**。
- 4 按一下**確定**。

確認 vSGX 項目不再顯示於虛擬機器之**虛擬機器硬體**窗格中的**摘要**索引標籤上。

使用 AMD 安全加密虛擬化-加密狀態保護虛擬機器

安全加密虛擬化-加密狀態 (SEV-ES) 是一種在最新 AMD CPU 中啟用的硬體功能，可保持客體作業系統的記憶體和暫存器狀態為已加密，從而防止 Hypervisor 對其進行存取。

您可以將 SEV-ES 新增至虛擬機器，作為額外的安全性增強功能。SEV-ES 可防止 CPU 暫存器將暫存器中的資訊洩漏給 Hypervisor 之類的元件。SEV-ES 還可以偵測到對 CPU 暫存器狀態進行的惡意修改。

vSphere 和 AMD 安全加密虛擬化-加密狀態

在 vSphere 7.0 Update 1 及更新版本中，您可以在支援的 AMD CPU 和客體作業系統上啟用安全加密虛擬化-加密狀態 (SEV-ES)。

目前，SEV-ES 僅支援 AMD EPYC 7xx2 CPU (名為「Rome」的代碼) 及更新版本的 CPU，以及僅支援包含對 SEV-ES 的特定支援的 Linux 核心版本。

SEV-ES 元件和架構

SEV-ES 架構由以下元件所組成。

- AMD CPU，尤其是管理加密金鑰和處理加密的平台安全性處理器 (PSP)。
- 啟發性的作業系統，也就是對 Hypervisor 使用客體起始呼叫的作業系統。
- 虛擬機器監控器 (VMM) 和虛擬機器可執行檔 (VMX)，用於在開啟虛擬機器電源期間初始化已加密的虛擬機器狀態，並同時處理來自客體作業系統的呼叫。
- VMkernel 驅動程式，用於在 Hypervisor 與客體作業系統之間傳遞未加密的資料。

在 ESXi 上執行和管理 SEV-ES

必須先在系統的 BIOS 組態中啟用 SEV-ES。如需有關存取 BIOS 組態的詳細資訊，請參閱所用系統的說明文件。在系統的 BIOS 中啟用 SEV-ES 後，可以將 SEV-ES 新增到虛擬機器。

可以使用 vSphere Client (從 vSphere 7.0 Update 2 開始) 或 PowerCLI 命令在虛擬機器上啟用和停用 SEV-ES。可以使用 SEV-ES 建立新虛擬機器，或在現有虛擬機器上啟用 SEV-ES。管理啟用了 SEV-ES 的虛擬機器的權限與管理一般虛擬機器的權限相同。

SEV-ES 上不支援的 VMware 功能

在啟用了 SEV-ES 的情況下，不支援以下功能。

- 系統管理模式
- vMotion
- 已開啟電源的快照 (但支援無記憶體體的快照)
- 熱新增或熱移除 CPU 或記憶體
- 暫停/繼續
- VMware Fault Tolerance
- 複製和即時複製
- 客體完整性
- UEFI 安全開機

使用 vSphere Client 將 AMD 安全加密虛擬化-加密狀態新增至虛擬機器

在 vSphere 7.0 Update 2 及更新版本中，可以使用 vSphere Client 將 SEV-ES 新增至虛擬機器，以增強客體作業系統的安全性。

您可以將 SEV-ES 新增至 ESXi 7.0 Update 1 或更新版本上執行的虛擬機器。

必要條件

- 系統必須安裝有 AMD EPYC 7xx2 (名為「Rome」的代碼) 或更新版本的 CPU 及支援 BIOS。
- 必須在 BIOS 中啟用 SEV-ES。
- 每台 ESXi 主機的 SEV-ES 虛擬機器數目受 BIOS 控制。在 BIOS 中啟用 SEV-ES 時，輸入的**最小 SEV 非 ES ASID** 設定值等於 SEV-ES 虛擬機器數目加上 1。例如，如果要同時執行的虛擬機器數目為 12，則輸入 13。

備註 vSphere 7.0 Update 1 支援每台 ESXi 主機有 16 個啟用了 SEV-ES 的虛擬機器。在 BIOS 中使用較高的設定不會阻止 SEV-ES 正常運作，但是，限制值 16 仍適用。vSphere 7.0 Update 2 支援每台 ESXi 主機有 480 個啟用了 SEV-ES 的虛擬機器。

- 您環境中執行的 ESXi 主機必須是 ESXi 7.0 Update 1 或更新版本。
- vCenter Server 必須為 vSphere 7.0 Update 2 或更新版本。
- 客體作業系統必須支援 SEV-ES。
目前，僅支援具有對 SEV-ES 的特定支援的 Linux 核心。
- 虛擬機器必須具有硬體版本 18 或更新版本。
- 虛擬機器必須已啟用**保留所有客體記憶體**選項，否則開啟電源會失敗。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。
- 3 在物件上按一下滑鼠右鍵，選取**新虛擬機器**，然後遵循提示來建立虛擬機器。

選項	動作
選取建立類型	建立虛擬機器。
選取名稱和資料夾	指定名稱和目標位置。
選取運算資源	指定您有權限為其建立虛擬機器的物件。
選取儲存區	在虛擬機器儲存區原則中，選取儲存區原則。選取相容的資料存放區。
選取相容性	確保已選取 ESXi 7.0 及更新版本 。
選取客體作業系統	選取 Linux，然後選取具有 SEV-ES 之特定支援的 Linux 版本。
自訂硬體	在 虛擬機器選項 > 開機選項 > 韌體 下，請確保已選取 EFI。在 虛擬機器選項 > 加密 下，選取 AMD SEV-ES 的 啟用核取方塊 。
即將完成	檢閱資訊，然後按一下 完成 。

結果

虛擬機器是使用 SEV-ES 建立的。

將 AMD 安全加密虛擬化-加密狀態新增至虛擬機器

您可以將 SEV-ES 新增至虛擬機器，以增強客體作業系統的安全性。

您可以將 SEV-ES 新增至 ESXi 7.0 Update 1 或更新版本上執行的虛擬機器。

必要條件

- 系統必須安裝有 AMD EPYC 7xx2 (名為「Rome」的代碼) 或更新版本的 CPU 及支援 BIOS。
- 必須在 BIOS 中啟用 SEV-ES。
- 每台 ESXi 主機的 SEV-ES 虛擬機器數目受 BIOS 控制。在 BIOS 中啟用 SEV-ES 時，輸入的**最小 SEV 非 ES ASID** 設定值等於 SEV-ES 虛擬機器數目加上 1。例如，如果要同時執行的虛擬機器數目為 12，則輸入 13。

備註 vSphere 7.0 Update 1 支援每台 ESXi 主機有 16 個啟用了 SEV-ES 的虛擬機器。在 BIOS 中使用較高的設定不會阻止 SEV-ES 正常運作，但是，限制值 16 仍適用。vSphere 7.0 Update 2 支援每台 ESXi 主機有 480 個啟用了 SEV-ES 的虛擬機器。

- 您環境中執行的 ESXi 主機必須是 ESXi 7.0 Update 1 或更新版本。
- 客體作業系統必須支援 SEV-ES。
目前，僅支援具有對 SEV-ES 的特定支援的 Linux 核心。
- 虛擬機器必須具有硬體版本 18 或更新版本。
- 虛擬機器必須已啟用**保留所有客體記憶體**選項，否則開啟電源會失敗。
- 必須在具有環境存取權的系統上安裝 PowerCLI 12.1.0 或更新版本。

程序

- 1 在 PowerCLI 工作階段中，執行 `Connect-VIServer` cmdlet，以管理員身分連線至管理 ESXi 主機 (您要在其中新增具有 SEV-ES 的虛擬機器) 的 vCenter Server。

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

- 2 使用 `New-VM` cmdlet 建立虛擬機器，並指定 `-SEVEnabled $true`。

例如，先將主機資訊指派給一個變數，然後再建立虛擬機器。

```
$vmhost = Get-VMHost -Name 10.193.25.83
New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
```

如果必須指定虛擬硬體版本，請將 `New-VM` cmdlet 與 `-HardwareVersion vmx-18` 參數搭配執行。例如：

```
New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
-HardwareVersion vmx-18
```


結果

虛擬機器是使用 SEV-ES 建立的。

使用 vSphere Client 在現有虛擬機器上啟用 AMD 安全加密虛擬化-加密狀態

在 vSphere 7.0 Update 2 及更新版本中，可以使用 vSphere Client 將 SEV-ES 新增至現有虛擬機器，以增強客體作業系統的安全性。

您可以將 SEV-ES 新增至 ESXi 7.0 Update 1 或更新版本上執行的虛擬機器。

必要條件

- 系統必須安裝有 AMD EPYC 7xx2 (名為「Rome」的代碼) 或更新版本的 CPU 及支援 BIOS。
- 必須在 BIOS 中啟用 SEV-ES。
- 每台 ESXi 主機的 SEV-ES 虛擬機器數目受 BIOS 控制。在 BIOS 中啟用 SEV-ES 時，輸入的**最小 SEV 非 ES ASID** 設定值等於 SEV-ES 虛擬機器數目加上 1。例如，如果要同時執行的虛擬機器數目為 12，則輸入 13。

備註 vSphere 7.0 Update 1 支援每台 ESXi 主機有 16 個啟用了 SEV-ES 的虛擬機器。在 BIOS 中使用較高的設定不會阻止 SEV-ES 正常運作，但是，限制值 16 仍適用。vSphere 7.0 Update 2 支援每台 ESXi 主機有 480 個啟用了 SEV-ES 的虛擬機器。

- 您環境中執行的 ESXi 主機必須是 ESXi 7.0 Update 1 或更新版本。
- vCenter Server 必須為 vSphere 7.0 Update 2 或更新版本。
- 客體作業系統必須支援 SEV-ES。
目前，僅支援具有對 SEV-ES 的特定支援的 Linux 核心。
- 虛擬機器必須具有硬體版本 18 或更新版本。
- 虛擬機器必須選中**保留所有客體記憶體**選項，否則開啟電源會失敗。
- 確定虛擬機器已關閉電源。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在您想要修改的詳細目錄中的虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
- 3 在**虛擬機器選項 > 開機選項 > 韌體**下，請確保已選取 EFI。
- 4 在**編輯設定對話方塊的虛擬機器選項 > 加密**下，選取 AMD SEV-ES 的**啟用核取方塊**。
- 5 按一下**確定**。

結果

SEV-ES 已新增至虛擬機器。

在現有虛擬機器上啟用 AMD 安全加密虛擬化-加密狀態

您可以將 SEV-ES 新增至現有虛擬機器，以增強客體作業系統的安全性。

您可以將 SEV-ES 新增至 ESXi 7.0 Update 1 或更新版本上執行的虛擬機器。

必要條件

- 系統必須安裝有 AMD EPYC 7xx2 (名為「Rome」的代碼) 或更新版本的 CPU 及支援 BIOS。
- 必須在 BIOS 中啟用 SEV-ES。
- 每台 ESXi 主機的 SEV-ES 虛擬機器數目受 BIOS 控制。在 BIOS 中啟用 SEV-ES 時，輸入的**最小 SEV 非 ES ASID** 設定值等於 SEV-ES 虛擬機器數目加上 1。例如，如果要同時執行的虛擬機器數目為 12，則輸入 13。

備註 vSphere 7.0 Update 1 支援每台 ESXi 主機有 16 個啟用了 SEV-ES 的虛擬機器。在 BIOS 中使用較高的設定不會阻止 SEV-ES 正常運作，但是，限制值 16 仍適用。vSphere 7.0 Update 2 支援每台 ESXi 主機有 480 個啟用了 SEV-ES 的虛擬機器。

- 您環境中執行的 ESXi 主機必須是 ESXi 7.0 Update 1 或更新版本。
- 客體作業系統必須支援 SEV-ES。
目前，僅支援具有對 SEV-ES 的特定支援的 Linux 核心。
- 虛擬機器必須具有硬體版本 18 或更新版本。
- 虛擬機器必須選中**保留所有客體記憶體**選項，否則開啟電源會失敗。
- 必須在具有環境存取權的系統上安裝 PowerCLI 12.1.0 或更新版本。
- 確定虛擬機器已關閉電源。

程序

- 1 在 PowerCLI 工作階段中，執行 Connect-VIServer cmdlet，以管理員身分連線至管理 ESXi 主機 (具有要新增 SEV-ES 的虛擬機器) 的 vCenter Server。

例如：

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

- 2 使用 Set-VM cmdlet 將 SEV-ES 新增至虛擬機器，並指定 -SEVENabled \$true。

例如：

```
$vmhost = Get-VMHost -Name 10.193.25.83
Set-VM -Name MyVM2 $vmhost -SEVENabled $true
```

如果必須指定虛擬硬體版本，請將 Set-VM cmdlet 與 -HardwareVersion vmx-18 參數搭配執行。例如：

```
Set-VM -Name MyVM2 $vmhost -SEVENabled $true -HardwareVersion vmx-18
```

結果

SEV-ES 已新增至虛擬機器。

使用 vSphere Client 在虛擬機器停用 AMD 安全加密虛擬化-加密狀態

在 vSphere 7.0 Update 2 及更新版本中，您可以使用 vSphere Client 在虛擬機器上停用 SEV-ES。

必要條件

- 確定虛擬機器已關閉電源。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在您想要修改的詳細目錄中的虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
- 3 在**編輯設定**對話方塊的**虛擬機器選項 > 加密**下，取消選取 AMD SEV-ES 的**啟用核取方塊**。
- 4 按一下**確定**。

結果

此虛擬機器上已停用 SEV-ES。

在虛擬機器上停用 AMD 安全加密虛擬化-加密狀態

您可以在虛擬機器上停用 SEV-ES。

必要條件

- 確定虛擬機器已關閉電源。
- 必須在具有環境存取權的系統上安裝 PowerCLI 12.1.0 或更新版本。

程序

- 1 在 PowerCLI 工作階段中，執行 `Connect-VIServer` cmdlet，以管理員身分連線至管理 ESXi 主機 (具有要從中移除 SEV-ES 的虛擬機器) 的 vCenter Server。

例如：

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

- 2 使用 `Set-VM` cmdlet 在虛擬機器上停用 SEV-ES，並指定 `-SEVEnabled $false`。

例如，先將主機資訊指派給一個變數，然後對虛擬機器停用 SEV-ES。

```
$vmhost = Get-VMHost -Name 10.193.25.83
Set-VM -Name MyVM2 $vmhost -SEVEnabled $false
```

結果

此虛擬機器上已停用 SEV-ES。

透過使用 vSphere 虛擬機器加密，可以更安全的方式加密敏感工作負載。可以將加密金鑰的存取權設為以 ESXi 主機處於受信任狀態為條件。

在開始執行虛擬機器加密工作之前，您必須設定金鑰提供者。以下金鑰提供者類型可用。

表 6-1. vSphere 金鑰提供者

金鑰提供者	說明	瞭解詳細資訊
標準金鑰提供者	標準金鑰提供者在 vSphere 6.5 及更新版本中可用，該提供者使用 vCenter Server 從外部金鑰伺服器請求金鑰。金鑰伺服器會產生並儲存金鑰，然後將金鑰傳遞到 vCenter Server 進行散佈。	請參閱第 7 章 設定和管理標準金鑰提供者 。
受信任金鑰提供者	vSphere Trust Authority 受信任金鑰提供者在 vSphere 7.0 及更新版本中可用，該提供者以工作負載叢集的證明狀態為條件來存取加密金鑰。vSphere Trust Authority 需要外部金鑰伺服器。	請參閱第 9 章 vSphere Trust Authority 。
VMware vSphere® Native Key Provider™	在 vSphere 7.0 Update 2 及更新版本中，vSphere Native Key Provider 已包含在所有 vSphere 版本中，且不需要外部金鑰伺服器。	請參閱第 8 章 設定和管理 vSphere Native Key Provider 。

本章節討論下列主題：

- [vSphere 金鑰提供者的比較](#)
- [vSphere 虛擬機器加密如何保護您的環境](#)
- [vSphere 虛擬機器加密元件](#)
- [加密程序流程](#)
- [虛擬磁碟加密](#)
- [虛擬機器加密錯誤](#)
- [虛擬機器加密工作的必要條件和所需權限](#)
- [已加密的 vSphere vMotion](#)
- [虛擬機器加密最佳做法](#)

- [虛擬機器加密注意須知](#)
- [虛擬機器加密互通性](#)
- [ESXi 主機上的 vSphere 金鑰持續性](#)

vSphere 金鑰提供者的比較

您可以關注 vSphere 金鑰提供者功能的高層級概觀，這有助於規劃加密策略。

一般而言，金鑰提供者每日作業在功能或產品支援方面幾乎沒有區別。儘管金鑰提供者的外觀與行為類似，但是在選擇金鑰提供者時可能需要考慮一些需求和規範，如下表所示。

表 6-2. 金鑰提供者考量事項

金鑰提供者	是否需要外部金鑰伺服器？	執行快速設定？	僅適用於 vSphere？
標準金鑰提供者	是	否	否
受信任金鑰提供者	是	否	否
vSphere Native Key Provider	否	是	是

加密功能

每個金鑰提供者類型均支援以下加密功能。

- 使用同一金鑰提供者或其他金鑰提供者重設金鑰
- 輪替金鑰
- 虛擬信賴平台模組 (vTPM)
- 磁碟加密
- vSphere 虛擬機器加密
- 與其他金鑰提供者共存
- 升級為其他金鑰提供者

vSphere 功能

以下說明了對某些重要 vSphere 功能的金鑰提供者支援。

- 已加密的 vSphere vMotion：受所有金鑰提供者類型支援。目的地主機上必須存在相同的金鑰提供者。請參閱[已加密的 vSphere vMotion](#)。
- vCenter Server 以檔案為基礎的備份和還原：標準金鑰提供者和 vSphere Native Key Provider 支援 vCenter Server 以檔案為基礎的備份和還原。由於大多數 vSphere Trust Authority 組態資訊儲存在 ESXi 主機上，因此，vCenter Server 以檔案為基礎的備份機制不會備份此資訊。若要確保已儲存 vSphere Trust Authority 部署的組態資訊，請參閱[備份 vSphere Trust Authority 組態](#)。

VMware 產品

下表比較了對某些 VMware 產品的金鑰提供者支援。

表 6-3. VMware 產品支援比較

金鑰提供者	vSAN	Site Recovery Manager	vSphere Replication
標準金鑰提供者	是	是	是
受信任金鑰提供者	是	是 如果在復原端有相同的 vSphere Trust Authority 服務組態，則支援使用陣列式複寫的 SRM。	否
vSphere Native Key Provider	是	是	是

所需硬體

下表比較了一些最低金鑰提供者硬體需求。

表 6-4. 所需硬體的比較

金鑰提供者	ESXi 主機上的 TPM
標準金鑰提供者	非必要
受信任金鑰提供者	在受信任主機 (受信任叢集中的主機) 上是必要的。 備註 目前，Trust Authority 叢集中的 ESXi 主機不需要 TPM。但是，最佳做法是考慮安裝帶有 TPM 的全新 ESXi 主機。
vSphere Native Key Provider	非必要 vSphere Native Key Provider 可用性可以選擇性地限制為具有 TPM 的主機。

金鑰提供者命名

vSphere 使用金鑰提供者名稱查詢金鑰識別碼。如果兩個金鑰提供者具有相同的名稱，vSphere 會假定它們是等效的並且可以存取相同的金鑰。每個邏輯金鑰提供者 (無論其類型為標準、可信任還是本機) 都必須在所有 vCenter Server 系統中具有唯一的名稱。

在少數情況下，您可以跨多個 vCenter Server 系統設定同一個金鑰提供者，例如：

- 在 vCenter Server 系統之間移轉加密的虛擬機器
- 將 vCenter Server 設定為災難復原站台

vSphere 虛擬機器加密如何保護您的環境

無論使用哪個金鑰提供者，都可以透過 vSphere 虛擬機器加密建立加密的虛擬機器並加密現有虛擬機器。由於包含敏感資訊的所有虛擬機器檔案都會加密，因此會保護虛擬機器。僅具有加密權限的管理員可以執行加密和解密工作。

vSphere 虛擬機器加密支援的儲存區

vSphere 虛擬機器加密可與任何支援的儲存區類型 (NFS、iSCSI、光纖通道、直接連結儲存區等) 搭配使用，包括 VMware vSAN。如需有關在 vSAN 叢集中使用加密的詳細資訊，請參閱管理 VMware vSAN 說明文件。

vSphere 虛擬機器加密和 vSAN 使用相同的加密程式庫，但具有不同的設定檔。虛擬機器加密是依虛擬機器的加密，vSAN 是資料存放區層級的加密。

vSphere 加密金鑰和金鑰提供者

vSphere 以金鑰加密金鑰 (KEK) 和資料加密金鑰 (DEK) 的形式使用兩級加密。簡單來說，ESXi 主機產生 DEK，用於加密虛擬機器和磁碟。KEK 由金鑰伺服器提供，對 DEK 進行加密 (或「封裝」)。KEK 使用 AES256 演算法進行加密，DEK 使用 XTS-AES-256 演算法進行加密。根據金鑰提供者的類型，使用不同的方法建立及管理 DEK 和 KEK。

標準金鑰提供者的運作方式如下。

- 1 ESXi 主機產生並使用內部金鑰來加密虛擬機器和磁碟。這些金鑰用作 DEK。
- 2 vCenter Server 會從金鑰伺服器 (KMS) 請求金鑰。這些金鑰用作 KEK。vCenter Server 僅儲存每個 KEK 的識別碼，但不儲存金鑰本身。
- 3 ESXi 使用 KEK 加密內部金鑰，且在磁碟上儲存加密的內部金鑰。ESXi 不在磁碟上儲存 KEK。如果主機重新開機，vCenter Server 會從金鑰伺服器請求具有對應識別碼的 KEK，且使其可供 ESXi 使用。然後，ESXi 可視需要解密內部金鑰。

vSphere Trust Authority 受信任金鑰提供者的運作方式如下所示。

- 1 受信任叢集的 vCenter Server 會檢查即將建立加密虛擬機器的 ESXi 主機是否可存取預設的受信任金鑰提供者。
- 2 受信任叢集的 vCenter Server 會將受信任的金鑰提供者新增至虛擬機器 ConfigSpec。
- 3 虛擬機器建立申請將會傳送至 ESXi 主機。
- 4 如果證明 Token 尚未可供 ESXi 主機使用，則會從證明服務申請一個。
- 5 金鑰提供者服務會驗證證明 Token，並建立要傳送至 ESXi 主機的 KEK。將使用金鑰提供者上設定的主要金鑰封裝 (加密) KEK。KEK 加密文字和 KEK 純文字將傳回到受信任的主機。
- 6 ESXi 主機產生 DEK，對虛擬機器磁碟進行加密。
- 7 此 KEK 用於封裝 ESXi 主機所產生的 DEK，而金鑰提供者中的加密文字會與加密資料一起儲存。

8 虛擬機器已加密並寫入儲存區。

備註 如果刪除或解除登錄已加密的虛擬機器，則 ESXi 主機和叢集會從快取中移除 KEK。ESXi 主機無法再使用 KEK。對於標準金鑰提供者和受信任金鑰提供者，此行為是相同的。

vSphere Native Key Provider 的運作方式如下所示。

- 1 建立金鑰提供者時，vCenter Server 會產生主要金鑰並將其推送至叢集中的 ESXi 主機。(不涉及外部金鑰伺服器。)
- 2 ESXi 主機按需產生 DEK。
- 3 執行加密活動時，會使用 DEK 加密資料。
加密的 DEK 將與加密的資料一起儲存。
- 4 解密資料時，會使用主要金鑰先解密 DEK，然後再解密資料。

vSphere 虛擬機器加密可以對哪些元件加密

vSphere 虛擬機器加密支援加密虛擬機器檔案、虛擬磁碟檔案，以及核心傾印檔案。

虛擬機器檔案

會加密大多數虛擬機器檔案 (尤其是未儲存在 VMDK 檔案中的客體資料)。這組檔案包括但不限於 NVRAM、VSWP 和 VMSN 檔案。來自金鑰提供者的金鑰將解除鎖定包含內部金鑰和其他密碼的 VMX 檔案中的加密服務包。根據金鑰提供者的不同，金鑰擷取工作如下所示：

- 標準金鑰提供者：vCenter Server 管理來自金鑰伺服器的金鑰，並且 ESXi 無法直接存取金鑰提供者。主機等待 vCenter Server 推送金鑰。
- 受信任金鑰提供者和 vSphere Native Key Provider：ESXi 主機直接存取金鑰提供者，因此可以直接從 vSphere Trust Authority 服務或從 vSphere Native Key Provider 擷取請求的金鑰。

如果使用 vSphere Client 建立加密的虛擬機器，可以加密和解密獨立於虛擬機器檔案的虛擬磁碟。依預設，所有虛擬磁碟均已加密。對於其他加密工作，如加密現有虛擬機器，您可以加密和解密獨立於虛擬機器檔案的虛擬磁碟。

備註 您無法將加密的虛擬磁碟與未加密的虛擬機器建立關聯。

虛擬磁碟檔案

加密的虛擬磁碟 (VMDK) 檔案中的資料永遠不會以純文字寫入儲存區或實體磁碟，且永遠不會以純文字透過網路傳輸。VMDK 描述元檔案通常為純文字，但包含 KEK 的金鑰識別碼和加密服務包中的內部金鑰 (DEK)。

您可以使用 vSphere Client 或 vSphere API 透過新的 KEK 執行淺層雙重加密作業，或者使用 vSphere API 透過新的內部金鑰執行深層雙重加密作業。

核心傾印

永遠加密已啟用加密模式的 ESXi 主機上的核心傾印。請參閱 [vSphere 虛擬機器加密和核心傾印](#)。不會加密 vCenter Server 系統上的核心傾印。保護 vCenter Server 系統的存取權。

備註 如需 vSphere 虛擬機器加密可互通的裝置和功能相關的一些限制的相關資訊，請參閱 [虛擬機器加密互通性](#)。

vSphere 虛擬機器加密不對哪些元件加密

不加密或部分加密與虛擬機器相關聯的一些檔案。

記錄檔

不加密記錄檔，因為其不包含敏感資料。

虛擬機器組態檔

不加密 VMX 和 VMDS 檔案中儲存的大多數虛擬機器組態資訊。

虛擬磁碟描述元檔案

為了支援無金鑰的磁碟管理，不會加密大多數虛擬磁碟描述元檔案。

如何執行密碼編譯作業

僅指派了密碼編譯作業權限的使用者可以執行密碼編譯作業。權限集是精細的。預設管理員系統角色包含所有密碼編譯作業權限。「無密碼編譯管理員」角色支援所有管理員權限，密碼編譯作業權限除外。

除了使用 `Cryptographer.*` 權限之外，vSphere Native Key Provider 還可以使用 `Cryptographer.ReadKeyServersInfo` 權限，這是 vSphere Native Key Provider 的專屬權限。

如需詳細資訊，請參閱 [密碼編譯作業權限](#)。

您可以建立其他自訂角色，例如允許使用者群組加密虛擬機器但防止其解密虛擬機器。

如何執行密碼編譯作業

vSphere Client 支援許多密碼編譯作業。對於其他工作，您可以使用 PowerCLI 或 vSphere API。

表 6-5. 用於執行密碼編譯作業的介面

介面	作業	資訊
vSphere Client	建立加密的虛擬機器 加密和解密虛擬機器 執行虛擬機器的淺層雙重加密 (使用不同的 KEK)	本書
PowerCLI	建立加密的虛擬機器 加密和解密虛擬機器 設定 vSphere Trust Authority	VMware PowerCLI Cmdlet 參考

表 6-5. 用於執行密碼編譯作業的介面 (續)

介面	作業	資訊
vSphere Web Services SDK	建立加密的虛擬機器 加密和解密虛擬機器 執行虛擬機器的深度雙重加密 (使用不同的 DEK) 執行虛擬機器的淺層雙重加密 (使用不同的 KEK)	vSphere Web Services SDK 程式設計指南 vSphere Web Services API 參考
crypto-util	解密已加密的核心傾印 確認檔案是否已加密 直接在 ESXi 主機上執行其他管理工作	命令列說明 vSphere 虛擬機器加密和核心傾印

如何對虛擬機器雙重加密

您可以使用新金鑰對虛擬機器進行雙重加密 (亦稱為重設金鑰)，以防金鑰到期或遭到破解。可用選項如下。

- 深度雙重加密，會取代磁碟加密金鑰 (DEK) 和金鑰加密金鑰 (KEK)
- 淺層雙重加密，僅取代 KEK

可以使用 vSphere Client 或 API 對虛擬機器執行雙重加密。請參閱[使用 vSphere Client 對加密虛擬機器進行重設金鑰](#)和 vSphere Web Services SDK 程式設計指南。

深度雙重加密要求虛擬機器已關閉電源且不包含任何快照。您可以在虛擬機器開啟電源且虛擬機器已有快照存在時執行淺層雙重加密作業。僅允許在單一快照分支 (磁碟鏈結) 上對具有快照的加密虛擬機器進行淺層雙重加密。不支援多個快照分支。此外，在虛擬機器或磁碟的連結複製上不支援淺層雙重加密。如果淺層雙重加密在使用新 KEK 更新鏈結中的所有連結之前失敗，您仍可以存取加密的虛擬機器 (如果有舊 KEK 和新 KEK)。但是，最好在執行任何快照作業之前重新發出淺層雙重加密作業。

vSphere 虛擬機器加密元件

根據所使用的金鑰提供者，外部金鑰伺服器、vCenter Server 系統和 ESXi 主機可能會影像加密解決方案。

下列元件包括 vSphere 虛擬機器加密：

- 外部金鑰伺服器，也稱為 KMS (vSphere Native Key Provider 不需要此項)
- vCenter Server
- ESXi 主機

金鑰伺服器在 vSphere 虛擬機器加密中是什麼角色

金鑰伺服器是與金鑰提供者相關聯的金鑰管理互通協定 (KMIP) 管理伺服器。標準金鑰提供者和受信任的金鑰提供者需要金鑰伺服器。vSphere Native Key Provider 不需要金鑰伺服器。下表說明了金鑰提供者和金鑰伺服器互動之間的差異。

表 6-6. 金鑰提供者和金鑰伺服器互動

金鑰提供者	與金鑰伺服器的互動
標準金鑰提供者	標準金鑰提供者使用 vCenter Server 從金鑰伺服器請求金鑰。金鑰伺服器會產生並儲存金鑰，然後將金鑰傳遞到 vCenter Server 以散佈到 ESXi 主機。
受信任金鑰提供者	受信任的金鑰提供者使用金鑰提供者服務，該服務支援受信任的 ESXi 主機直接擷取金鑰。請參閱 什麼是 vSphere Trust Authority 金鑰提供者服務 。
vSphere Native Key Provider	vSphere Native Key Provider 不需要金鑰伺服器。vCenter Server 產生主要金鑰並將其推送至 ESXi 主機。然後，ESXi 主機產生資料加密金鑰 (即使未連線至 vCenter Server)。請參閱 vSphere Native Key Provider 概觀 。

您可以使用 vSphere Client 或 vSphere API 將金鑰提供者執行個體新增至 vCenter Server 系統。如果您使用多個金鑰提供者執行個體，則所有執行個體都必須來自同一個廠商並且必須複寫金鑰。

如果您的環境使用不同環境中的不同金鑰伺服器廠商，則可以針對每個金鑰伺服器新增一個金鑰提供者，並指定預設金鑰提供者。您新增的第一個金鑰提供者將成為預設金鑰提供者。您可以稍後明確指定預設值。

作為 KMIP 用戶端，vCenter Server 會使用金鑰管理互通協定 (KMIP)，可讓您輕鬆使用所選擇的金鑰伺服器。

vCenter Server 在 vSphere 虛擬機器加密中是什麼角色

下表說明了 vCenter Server 在加密程序中的角色。

表 6-7. 金鑰提供者和 vCenter Server

金鑰提供者	vCenter Server 的角色	如何檢查權限
標準金鑰提供者	僅 vCenter Server 具有登入金鑰伺服器的認證。ESXi 主機沒有這些認證。 vCenter Server 會從金鑰伺服器取得金鑰，並將其推送到 ESXi 主機。vCenter Server 不會儲存金鑰伺服器金鑰，但會保留金鑰識別碼清單。	vCenter Server 會檢查執行密碼編譯作業的使用者的權限。
受信任金鑰提供者	透過 vSphere Trust Authority，vCenter Server 不再需要從金鑰伺服器請求金鑰，並且以工作負載叢集的證明狀態為條件來存取加密金鑰。必須針對受信任叢集和 Trust Authority 叢集使用不同的 vCenter Server 系統。	vCenter Server 會檢查執行密碼編譯作業的使用者的權限。只有屬於 TrustedAdmins SSO 群組的使用者可以執行管理作業。
vSphere Native Key Provider	vCenter Server 會產生金鑰。	vCenter Server 會檢查執行密碼編譯作業的使用者的權限。

您可以使用 vSphere Client 為使用者群組指派密碼編譯作業權限，或指派無密碼編譯管理員自訂角色。請參閱[虛擬機器加密工作的必要條件和所需權限](#)。

vCenter Server 會將密碼編譯事件新增至事件清單，您可以從 vSphere Client 事件主控台檢視和匯出這些事件。每個事件皆包含使用者、時間、金鑰識別碼及密碼編譯作業。

來自金鑰伺服器的金鑰會用作金鑰加密金鑰 (KEK)。

ESXi 主機在 vSphere 虛擬機器加密中是什麼角色

ESXi 主機負責加密工作流程的多個方面。

表 6-8. 金鑰提供者 and ESXi 主機

金鑰提供者	ESXi 主機方面
標準金鑰提供者	<ul style="list-style-type: none"> ■ vCenter Server 會在主機需要金鑰時將金鑰推送到 ESXi 主機。主機必須已啟用加密模式。 ■ 確保已加密虛擬機器的客體資料在儲存到磁碟時已加密。 ■ 確保已加密虛擬機器的客體資料不會在未加密的情況下透過網路傳送。
受信任金鑰提供者	ESXi 主機會執行 vSphere Trust Authority 服務，具體取決於這些主機是受信任主機還是 Trust Authority 主機。受信任的 ESXi 主機會執行工作負載虛擬機器，這些虛擬機器可以使用 Trust Authority 主機發佈的金鑰提供者進行加密。請參閱 受信任基礎結構概觀 。
vSphere Native Key Provider	ESXi 主機會直接從 vSphere Native Key Provider 擷取金鑰。

ESXi 主機所產生的金鑰在本文件中稱為內部金鑰。這些金鑰通常充當資料加密金鑰 (DEK)。

加密程序流程

設定金鑰提供者後，具有所需權限的使用者可以建立加密的虛擬機器和磁碟。這些使用者也可以加密現有虛擬機器、解密已加密的虛擬機器，以及將虛擬信賴平台模組 (vTPM) 新增到虛擬機器。

根據金鑰提供者類型，程序流程可能涉及金鑰伺服器、vCenter Server 以及 ESXi 主機。

標準金鑰提供者加密程序流程

在執行加密程序期間，不同 vSphere 元件的相互影響如下。

- 1 當使用者執行加密工作 (例如建立加密的虛擬機器) 時，vCenter Server 會從預設金鑰伺服器請求新金鑰。此金鑰會用作 KEK。
- 2 vCenter Server 會儲存金鑰識別碼並將此金鑰傳遞到 ESXi 主機。如果 ESXi 主機屬於某個叢集，則 vCenter Server 會將 KEK 傳送到此叢集中的每個主機。
此金鑰本身不儲存在 vCenter Server 系統上。僅金鑰識別碼已知。
- 3 ESXi 主機為虛擬機器及其磁碟產生內部金鑰 (DEK)。它僅將內部金鑰保留在記憶體中，並使用 KEK 加密內部金鑰。
未加密內部金鑰永遠不會儲存在磁碟上。僅儲存已加密的資料。由於 KEK 來自金鑰伺服器，因此主機會繼續使用相同的 KEK。

4 ESXi 主機使用已加密的內部金鑰加密虛擬機器。

任何擁有 KEK 以及可以存取已加密金鑰檔案的主機可以針對已加密虛擬機器或磁碟執行作業。

受信任金鑰提供者加密程序流程

vSphere Trust Authority 加密程序流程包括 vSphere Trust Authority 服務、受信任的金鑰提供者、vCenter Server 以及 ESXi 主機。

使用受信任金鑰提供者加密虛擬機器，與使用標準金鑰提供者時的虛擬機器加密使用者體驗類似。vSphere Trust Authority 下的虛擬機器加密會繼續依賴虛擬機器加密儲存區原則或 vTPM 裝置是否存在，以決定何時加密虛擬機器。從 vSphere Client 加密虛擬機器時，仍可以使用預設設定的金鑰提供者 (在 vSphere 6.5 和 6.7 中稱為 KMS 叢集)。此外，仍可以類似方式使用 API 來手動指定金鑰提供者。為 vSphere 6.5 新增的現有密碼編譯權限在 vSphere 7.0 中仍與 vSphere Trust Authority 相關。

受信任金鑰提供者的加密程序與標準金鑰提供者之間有一些重要差異：

- Trust Authority 管理員在設定 vCenter Server 執行個體的金鑰伺服器時不會直接指定資訊，且不會建立金鑰伺服器信任。而是 vSphere Trust Authority 發佈受信任主機可使用的受信任金鑰提供者。
- vCenter Server 不再將金鑰推送到 ESXi 主機，而是將每個受信任的金鑰提供者視為單一頂層金鑰。
- 僅受信任的主機可從 Trust Authority 主機申請加密作業。

vSphere Native Key Provider 加密程序流程

從 7.0 Update 2 版本開始，vSphere 中將會包含 vSphere Native Key Provider。設定 vSphere Native Key Provider 時，vCenter Server 將主要金鑰推送至叢集中的所有 ESXi 主機。同樣地，如果更新或刪除 vSphere Native Key Provider，則會將變更推送至叢集中的主機。加密程序流程類似於受信任金鑰提供者的工作方式。不同之處在於，vSphere Native Key Provider 會產生金鑰並使用主要金鑰進行封裝，然後將其交還以執行加密。

金鑰伺服器的自訂屬性

金鑰管理互通性通訊協定 (KMIP) 支援新增用於廠商特定目的的自訂屬性。自訂屬性可讓您更明確地識別金鑰伺服器中儲存的金鑰。vCenter Server 會為虛擬機器金鑰和主機金鑰新增下列自訂屬性。

表 6-9. 虛擬機器加密自訂屬性

自訂屬性	值
x-Vendor	VMware, Inc.
x-Product	VMware vSphere
x-Product_Version	vCenter Server 版本
x-Component	虛擬機器
x-Name	虛擬機器名稱 (從 ConfigInfo 或 ConfigSpec 收集)
x-Identifier	虛擬機器的執行個體 UUID (從 ConfigInfo 或 ConfigSpec 收集)

表 6-10. 主機加密自訂屬性

自訂屬性	值
x-Vendor	VMware, Inc.
x-Product	VMware vSphere
x-Product_Version	vCenter Server 版本
x-Component	ESXi 伺服器
x-Name	主機名稱
x-Identifier	主機的硬體 UUID

當金鑰伺服器建立金鑰時，vCenter Server 會新增 `x-Vendor`、`x-Product` 和 `x-Product_Version` 屬性。使用金鑰加密虛擬機器或主機時，vCenter Server 會設定 `x-Component`、`x-Identifier` 和 `x-Name` 屬性。您可以在金鑰伺服器使用者介面中檢視這些自訂屬性。請洽詢您的金鑰伺服器廠商。

主機金鑰和虛擬機器金鑰都具有六個自訂屬性。兩個金鑰的 `x-Vendor`、`x-Product` 和 `x-Product_Version` 可能相同。這些屬性會在金鑰產生時進行設定。根據金鑰是用於虛擬機器還是主機，它可能會附加 `x-Component`、`x-Identifier` 和 `x-Name` 屬性。

金鑰錯誤

如果將金鑰從金鑰伺服器傳送至 ESXi 主機時發生錯誤，vCenter Server 會在事件記錄中針對下列事件產生訊息：

- 由於主機連線或主機支援問題，將金鑰新增至 ESXi 主機失敗。
- 由於金鑰伺服器中遺失金鑰，從金鑰伺服器取得金鑰失敗。
- 由於金鑰伺服器連線，從金鑰伺服器取得金鑰失敗。

解密已加密的虛擬機器

如果您稍後想要解密已加密的虛擬機器，可以變更其儲存區原則。您可以變更虛擬機器和所有磁碟的儲存區原則。如果您想要解密個別元件，請先解密所選磁碟，然後透過變更虛擬機器首頁的儲存區原則來解密虛擬機器。解密每個元件均需要兩個金鑰。請參閱[解密已加密的虛擬機器或虛擬磁碟](#)。

虛擬磁碟加密

當您從 vSphere Client 建立已加密的虛擬機器時，可以決定不進行加密的磁碟。您可以稍後新增磁碟並設定其加密原則。您無法將已加密的磁碟新增至未加密的虛擬機器，並且如果虛擬機器未加密，您將無法加密磁碟。

虛擬機器及其磁碟的加密由儲存區原則控制。虛擬機器首頁的儲存區原則管理虛擬機器本身，並且每個虛擬磁碟都有一個相關聯的儲存區原則。

- 將虛擬機器首頁的儲存區原則設為僅加密虛擬機器本身的加密原則。
- 將虛擬機器首頁和所有磁碟的儲存區原則設為加密所有元件的加密原則。

請考慮下列使用案例。

表 6-11. 虛擬磁碟加密使用案例

使用案例	詳細資料
建立加密的虛擬機器。	如果您在建立加密的虛擬機器時新增磁碟，依預設會加密磁碟。您可以將此原則變更為不加密一或多個磁碟。 虛擬機器建立後，您可以明確變更每個磁碟的儲存區原則。請參閱 變更虛擬磁碟的加密原則 。
加密虛擬機器。	若要加密現有虛擬機器，請變更其儲存區原則。您可以變更虛擬機器和所有虛擬磁碟的儲存區原則。若要僅加密虛擬機器，您可以指定虛擬機器首頁的加密原則，然後為每個虛擬磁碟選取不同的儲存區原則，例如 [資料存放區預設值]。請參閱 建立加密的虛擬機器 。
將現有的未加密磁碟新增至已加密的虛擬機器 (加密儲存區原則)。	失敗並顯示錯誤。您必須新增具有預設儲存區原則的磁碟，但稍後可以變更儲存區原則。請參閱 變更虛擬磁碟的加密原則 。
將現有的未加密磁碟新增至儲存區原則不包含加密 (例如 [資料存放區預設值]) 的已加密虛擬機器。	該磁碟使用預設儲存區原則。如果想要已加密的磁碟，您可以在新增磁碟後明確變更儲存區原則。請參閱 變更虛擬磁碟的加密原則 。
將已加密的磁碟新增至已加密的虛擬機器。虛擬機器首頁儲存區原則為 [加密]。	當您新增磁碟時，它會保持已加密狀態。vSphere Client 會顯示大小和其他屬性，包括加密狀態。
將現有的已加密磁碟新增至未加密的虛擬機器。	此使用案例不受支援。
登錄已加密的虛擬機器。	如果從 vCenter Server 移除已加密的虛擬機器，但未從磁碟中將其刪除，則可以透過登錄虛擬機器的虛擬機器組態 (vmx) 檔案將其傳回至 vCenter Server 詳細目錄。若要登錄已加密的虛擬機器，使用者必須具有 密碼編譯作業.登錄虛擬機器 權限。 如果已使用標準金鑰提供者加密虛擬機器，則在登錄已加密的虛擬機器時，vCenter Server 會將所需金鑰推送到 ESXi 主機。 如果登錄虛擬機器的使用者不具有 密碼編譯作業.登錄虛擬機器 權限，則 vCenter Server 會在登錄時鎖定虛擬機器，並且在解除鎖定之前無法使用該虛擬機器。 如果已使用受信任金鑰提供者或 vSphere Native Key Provider 加密虛擬機器，則在登錄已加密的虛擬機器時，vCenter Server 不再將金鑰推送到 ESXi 主機，而是在登錄虛擬機器時從主機中擷取金鑰。如果登錄虛擬機器的使用者不具有 密碼編譯作業.登錄虛擬機器 權限，則 vCenter Server 不允許執行此作業。

虛擬機器加密錯誤

如果 vCenter Server 偵測到虛擬機器加密發生嚴重錯誤，則會建立一個事件。您可以檢視這些事件，以協助疑難排解和解決加密錯誤。

vCenter Server 會針對下列虛擬機器加密嚴重錯誤建立事件。

- 無法產生 KEK。
- 資料存放區上的磁碟空間不足，無法建立加密的虛擬機器。
- 使用者權限不足，無法起始加密作業。

- 金鑰提供者上的指定金鑰遺失，因此使用新金鑰更新 ESXi 主機金鑰。
- 具有指定金鑰的金鑰提供者發生錯誤，因此使用新金鑰更新 ESXi 主機金鑰。

虛擬機器加密工作的必要條件和所需權限

只能在包含 vCenter Server 的環境中執行虛擬機器加密工作。此外，ESXi 主機必須為大多數加密工作啟用加密模式。執行此工作的使用者必須擁有適當的權限。一組**密碼編譯作業**權限允許進行更為精細的控制。如果虛擬機器加密工作需要變更主機加密模式，則需要其他權限。

備註 vSphere Trust Authority 具有額外的必要條件和必要權限。請參閱 [vSphere Trust Authority 的必要條件和必要權限](#)。

使用密碼編譯權限和角色

依預設，具有 vCenter Server 管理員角色的使用者擁有所有權限，包括密碼編譯作業權限。**無密碼編譯管理員**角色沒有執行密碼編譯作業所需的下列權限。

- 新增**密碼編譯作業**權限。
- **全域.診斷**
- **主機.詳細目錄.新增主機至叢集**
- **主機.詳細目錄.新增獨立主機**
- **主機.本機作業.管理使用者群組**

您可以將**無密碼編譯管理員**角色指派給不需要**密碼編譯作業**權限的 vCenter Server 管理員。

若要進一步限制使用者可以執行的作業，您可以複製**無密碼編譯管理員**角色，並建立僅具有某些**密碼編譯作業**權限的自訂角色。例如，您可以建立允許使用者加密，但無法解密虛擬機器的角色。請參閱[使用 vCenter Server 角色指派權限](#)。

什麼是主機加密模式

主機加密模式可確定 ESXi 主機是否準備好接受密碼編譯資料，用於加密虛擬機器和虛擬磁碟。必須啟用主機加密模式，才能在主機上執行任何密碼編譯作業。主機加密模式通常在需要時自動設定，但您可以明確設定。您可以從 vSphere Client 或透過使用 vSphere API 檢查並明確設定目前的主機加密模式。

啟用主機加密模式時，vCenter Server 會在主機上安裝主機金鑰，這可確保主機已經過密碼編譯，「安全無憂」。就地使用主機金鑰，可以繼續執行其他密碼編譯作業，包括 vCenter Server 從金鑰提供者取得金鑰和將其推送到 ESXi 主機。

在「安全」模式下，使用者環境 (即 hostd) 和加密的虛擬機器具有加密的核心傾印。未加密的虛擬機器沒有加密的核心傾印。

如需有關加密的核心傾印和 VMware 技術支援如何使用它們的詳細資訊，請參閱 VMware 知識庫文章，網址為 <http://kb.vmware.com/kb/2147388>。

如需相關指示，請參閱 [明確啟用主機加密模式](#)。

主機加密模式一經設定，便不會輕易停用。請參閱[使用 API 停用主機加密模式](#)。

當加密作業嘗試設定主機加密模式時，會發生自動變更。例如，假設您將已加密的虛擬機器新增至獨立主機。主機加密模式未設定。如果您在主機上擁有所需權限，則加密模式會變更為自動設定。

假定叢集有三台 ESXi 主機：主機 A、B 和 C。您在主機 A 上建立已加密的虛擬機器。發生的情況取決於多個因素。

- 如果主機 A、B 和 C 已設定主機加密模式，則您只需**密碼編譯作業.加密新增項目**權限即可建立虛擬機器。
- 如果主機 A 和 B 已設定主機加密，而主機 C 未設定，則系統會以如下方式繼續進行。
 - 假設您在每台主機上擁有**密碼編譯作業.加密新增項目**和**密碼編譯作業.登錄主機**權限。在這種情況下，加密程序會在主機 C 上設定主機加密模式，並將金鑰推送到叢集中的每台主機。
對於這種情況，您也可以在主機 C 上明確設定主機加密模式。
 - 假設您在虛擬機器或虛擬機器資料夾上僅擁有**密碼編譯作業.加密新增項目**權限。在此情況下，虛擬機器會成功建立，且金鑰在主機 A 和主機 B 上變得可用。主機 C 仍停用加密，且沒有虛擬機器金鑰。
- 如果所有主機皆未設定主機加密模式，並且您在主機 A 上擁有**密碼編譯作業.登錄主機**權限，則虛擬機器建立程序會在該主機上設定主機加密模式。否則，主機 B 和 C 會產生錯誤。
- 也可以使用 vSphere API 將叢集的加密模式設定為「強制啟用」。強制啟用會導致叢集中的所有主機均「安全無憂」，即 vCenter Server 已在主機上安裝主機金鑰。請參閱 vSphere Web Services SDK 程式設計指南。

加密虛擬機器時的磁碟空間需求

加密現有虛擬機器時，您至少需要虛擬機器目前使用之空間兩倍的空間。

已加密的 vSphere vMotion

vSphere vMotion 始終在移轉已加密的虛擬機器時使用加密。對於未加密的虛擬機器，您可以選取其中一個已加密的 vSphere vMotion 選項。

已加密的 vSphere vMotion 保護使用 vSphere vMotion 傳輸之資料的機密性、完整性和真實性。

vSphere 支援對 vCenter Server 執行個體之間未加密和已加密的虛擬機器執行加密 vMotion。

加密哪些檔案

對於已加密的磁碟，在所有情況下，傳輸的資料會進行加密。對於未加密的磁碟，將適用於以下情況：

- 如果在主機內傳輸磁碟資料，即不變更主機，僅變更資料存放區，則傳輸未加密。
- 如果在主機之間傳輸磁碟資料並使用加密 vMotion，則傳輸將加密。如果未使用加密 vMotion，則傳輸未加密。

對於已加密的虛擬機器，透過 vSphere vMotion 移轉始終使用已加密的 vSphere vMotion。對於已加密的虛擬機器，您無法關閉已加密的 vSphere vMotion。

已加密的 vSphere vMotion 狀態

對於未加密的虛擬機器，您可以將已加密的 vSphere vMotion 設定為下列其中一種狀態。預設為 [隨機]。

已停用

請勿使用已加密的 vSphere vMotion。

隨機

如果來源主機和目的地主機支援，則使用已加密的 vSphere vMotion。僅 ESXi 6.5 版及更新版本使用已加密的 vSphere vMotion。

必要

僅允許已加密的 vSphere vMotion。如果來源主機或目的地主機不支援已加密的 vSphere vMotion，則不允許使用 vSphere vMotion 進行移轉。

當您加密虛擬機器時，虛擬機器會保留目前已加密的 vSphere vMotion 設定的記錄。如果您稍後停用虛擬機器加密，則已加密的 vMotion 設定會保留為 [必要]，直到您明確變更此設定。您可以使用 [編輯設定變更](#) 此設定。

如需針對未加密虛擬機器啟用和停用已加密 vSphere vMotion 的相關資訊，請參閱 vCenter Server 和主機管理說明文件。

備註 目前，您必須使用 vSphere API 在 vCenter Server 執行個體之間移轉或複製加密的虛擬機器。請參閱 vSphere Web Services SDK 程式設計指南和《vSphere Web Services API 參考》。

在 vCenter Server 執行個體之間移轉或複製已加密的虛擬機器

vSphere vMotion 支援在 vCenter Server 執行個體之間移轉和複製已加密的虛擬機器。

在 vCenter Server 執行個體之間移轉或複製已加密的虛擬機器時，必須將來源和目的地 vCenter Server 執行個體設定為共用用於加密虛擬機器的金鑰提供者。此外，來源和目的地 vCenter Server 執行個體上的金鑰提供者名稱必須相同，並且具有下列特性：

- 標準金鑰提供者：金鑰提供者中必須具有一個相同的金鑰伺服器 (或多個金鑰伺服器)。
- 受信任金鑰提供者：在目的地主機上必須設定相同的 vSphere Trust Authority 服務。
- vSphere Native Key Provider：必須具有相同的 KDK。

備註 無論來源主機是否位於叢集中，都無法將使用 vSphere Native Key Provider 加密的虛擬機器複製或移轉到獨立主機。

目的地 vCenter Server 可確保目的地 ESXi 主機已設定加密模式，從而確保主機「安全無憂」。

使用 vSphere vMotion 在 vCenter Server 執行個體之間移轉或複製已加密的虛擬機器時，需要具備下列權限。

- 移轉：虛擬機器上的 **密碼編譯作業.移轉** 權限
- 複製：虛擬機器上的 **密碼編譯作業.複製** 權限

此外，目的地 vCenter Server 還必須具有**密碼編譯作業.EncryptNew** 權限。如果目的地 ESXi 主機未處於「安全」模式，則目的地 vCenter Server 還必須具有**密碼編譯作業.RegisterHost** 權限。

在同一 vCenter Server 或跨 vCenter Server 執行個體移轉虛擬機器 (未加密或加密) 時，不允許執行某些工作。

- 無法變更虛擬機器儲存區原則。
- 無法執行金鑰變更。

備註 可以在複製虛擬機器時變更虛擬機器儲存區原則。

在 vCenter Server 執行個體之間移轉或複製已加密的虛擬機器的最低需求

使用 vSphere vMotion 在 vCenter Server 執行個體之間移轉或複製標準金鑰提供者的已加密虛擬機器的最低版本需求如下：

- 來源和目的地 vCenter Server 執行個體都必須為版本 7.0 或更新版本。
- 來源和目的地 ESXi 主機都必須為版本 6.7 或更新版本。

使用 vSphere vMotion 在 vCenter Server 執行個體之間移轉或複製受信任金鑰提供者的已加密虛擬機器的最低版本需求如下：

- 必須針對目的地主機設定 vSphere Trust Authority 服務，並且必須證明目的地主機。
- 在移轉時無法變更加密。例如，將虛擬機器移轉到新儲存區時，無法加密未加密的磁碟。
- 您可以將標準的已加密虛擬機器移轉至受信任的主機。來源和目的地 vCenter Server 執行個體上的金鑰提供者名稱必須相同。
- 無法將 vSphere Trust Authority 加密虛擬機器移轉至不受信任的主機。

受信任金鑰提供者 vMotion 和跨 vCenter Server 執行 vMotion

受信任金鑰提供者完全支援跨 ESXi 主機執行 vMotion。

支援跨 vCenter Server 執行 vMotion，但具有以下限制。

- 1 必須在目的地主機上設定所需的受信任服務，並且必須證明目的地主機。
- 2 在移轉時無法變更加密。例如，將虛擬機器移轉到新儲存區時，無法加密磁碟。

跨 vCenter Server 執行 vMotion 時，vCenter Server 會檢查受信任金鑰提供者在目的地主機上是否可用，以及主機是否有權存取該金鑰提供者。

vSphere Native Key Provider vMotion 和跨 vCenter Server 執行 vMotion

vSphere Native Key Provider 支援 vMotion 和跨 ESXi 主機的加密 vMotion。如果在目的地主機上已設定 vSphere Native Key Provider，則支援跨 vCenter Server 執行 vMotion。

虛擬機器加密最佳做法

請遵循虛擬機器加密最佳做法，以避免稍後 (例如產生 `vm-support` 服務包時) 發生問題。

入門最佳做法

若要避免在使用虛擬機器加密時出現問題，請遵循以下一般最佳做法。

- 請勿加密任何 vCenter Server Appliance 虛擬機器。
- 如果 ESXi 主機失敗，請儘快擷取支援服務包。主機金鑰必須可用於產生使用密碼的支援服務包或解密核心傾印。如果將主機重新開機，主機金鑰可能會發生變更。如果出現這種情況，您將無法再產生使用密碼的支援服務包或使用主機金鑰解密支援服務包中的核心傾印。
- 請謹慎管理金鑰提供者名稱。如果已在使用中的金鑰伺服器的金鑰提供者名稱發生變更，使用來自該金鑰伺服器的金鑰進行加密的虛擬機器在電源開啟或登錄期間會進入鎖定狀態。在這種情況下，請將該金鑰伺服器從 vCenter Server 中移除並以最初使用的金鑰提供者名稱加以新增。
- 請勿編輯 VMX 檔案和 VMDK 描述元檔案。這些檔案包含加密服務包。您的變更可能會使虛擬機器無法復原，並且該復原問題無法修復。
- vSphere 虛擬機器加密程序會先對主機上的資料進行加密，然後再將資料寫入儲存區。以這種方式加密虛擬機器時，後端儲存區功能 (例如重複資料刪除、壓縮、複寫等) 的有效性可能會受到影響。
- 如果使用多層加密，例如，vSphere 虛擬機器加密和客體內加密 (BitLocker、dm-crypt 等)，則虛擬機器的整體性能可能會受到影響，因為加密程序會使用額外的 CPU 和記憶體資源。
- 確保使用 vSphere 虛擬機器加密進行加密之虛擬機器的複寫複本有權在復原站台存取加密金鑰。對於標準金鑰提供者，在 vSphere 外部作為金鑰管理系統設計的一部分進行處理。對於 vSphere Native Key Provider，請確保存在原生金鑰提供者金鑰的備份複本，並受到保護以防遺失。如需詳細資訊，請參閱 [備份 vSphere Native Key Provider](#)。
- 加密需要大量 CPU。AES-NI 顯著提升了加密效能。在 BIOS 中啟用 AES-NI。

已加密核心傾印的最佳做法

請遵循下列最佳做法，以避免在您想要檢查核心傾印以診斷問題時發生問題。

- 建立與核心傾印有關的原則。加密核心傾印是因為它們可能包含敏感資訊，例如金鑰。如果要解密核心傾印，請考慮敏感資訊。ESXi 核心傾印可能包含 ESXi 主機及其上虛擬機器的金鑰。在解密核心傾印之後，請考量變更主機金鑰並對已加密的虛擬機器進行雙重加密。您可以透過使用 vSphere API 來執行這兩項工作。

如需詳細資料，請參閱 [vSphere 虛擬機器加密和核心傾印](#)。

- 在您收集 `vm-support` 服務包時，一律使用密碼。您可以在透過 vSphere Client 或使用 `vm-support` 命令產生支援服務包時指定密碼。

該密碼會對使用內部金鑰的核心傾印進行雙重加密，以使用基於密碼的金鑰。您稍後可以使用該密碼來解密可能包含在支援服務包中的任何已加密核心傾印。透過使用密碼選項，未加密的核心傾印和記錄不會受到影響。

- vSphere 元件中不會保存您在 vm-support 服務包建立期間指定的密碼。您將負責追蹤支援服務包的密碼。
- 變更主機金鑰之前，請先產生使用密碼的 vm-support 服務包。您稍後可以使用密碼來存取可能已使用舊主機金鑰加密的任何核心傾印。

金鑰生命週期管理的最佳做法

實作最佳做法不但可保證金鑰伺服器可用性，而且能夠監控金鑰伺服器上的金鑰。

- 您負責實作可保證金鑰伺服器可用性的原則。

如果金鑰伺服器無法使用，則要求 vCenter Server 從金鑰伺服器請求金鑰的虛擬機器作業將無法進行。這意味著，執行中的虛擬機器會繼續執行，您可以對這些虛擬機器進行開啟電源、關閉電源和重新設定。但是，您無法將這些虛擬機器重新放置到不具金鑰資訊的主機。

大多數金鑰伺服器解決方案都包括高可用性功能。您可以使用 vSphere Client 或 API 來指定金鑰提供者和相關聯的金鑰伺服器。

備註 從 7.0 Update 2 版本開始，加密的虛擬機器和虛擬 TPM 可以繼續運作，即使金鑰伺服器暫時離線或無法使用也是如此。ESXi 主機可保存加密金鑰以繼續執行加密和 vTPM 作業。請參閱 [ESXi 主機上的 vSphere 金鑰持續性](#)。

- 您將負責追蹤金鑰，並在現有虛擬機器的金鑰未處於 [作用中] 狀態時執行修復。

KMIP 標準定義了下列金鑰狀態。

- 作用前
- 作用中
- 已停用
- 已遭洩露
- 已銷毀
- 已銷毀並遭洩露

vSphere 虛擬機器加密僅使用 [作用中] 金鑰進行加密。如果金鑰為 [作用前]，vSphere 虛擬機器加密會將其啟動。如果金鑰狀態為 [已停用]、[已遭洩露]、[已銷毀]、[已銷毀並遭洩露]，則無法使用該金鑰加密虛擬機器。

對於處於其他狀態的金鑰，使用這些金鑰的虛擬機器會繼續運作。複製或移轉作業是否成功取決於其金鑰是否已存在於主機上。

- 如果金鑰存在於目的地主機上，則表示作業成功執行，即使金鑰在金鑰伺服器上不是 [作用中] 狀態。
- 如果所需的虛擬機器和虛擬磁碟金鑰不在目的地主機上，則 vCenter Server 必須從金鑰伺服器擷取金鑰。如果金鑰狀態為 [已停用]、[已遭洩露]、[已銷毀]、[已銷毀並遭洩露]，則 vCenter Server 會顯示錯誤，作業不會成功。

如果金鑰已存在於主機上，則複製或移轉作業成功。如果 vCenter Server 必須從金鑰伺服器提取金鑰，則作業失敗。

如果金鑰不是 [作用中] 狀態，請使用 API 執行重設金鑰作業。請參閱《vSphere Web Services SDK 程式設計指南》。

- 制定金鑰輪替原則，使金鑰在特定時間後淘汰並變換。
 - 受信任金鑰提供者：變更受信任金鑰提供者的主要金鑰。
 - vSphere Native Key Provider：變更 vSphere Native Key Provider 的 `key_id`。

備份和還原的最佳做法

請設定有關備份和還原作業的原則。

- 並非所有備份架構皆受支援。請參閱[虛擬機器加密互通性](#)。
- 針對還原作業設定原則。因為備份一律採用純文字形式，所以請計劃在還原完成後立即加密虛擬機器。您可以指定加密虛擬機器做為還原作業的一部分。如果可能，請在還原程序過程中加密虛擬機器，以避免曝光敏感資訊。若要變更與虛擬機器相關聯的任何磁碟的加密原則，請變更磁碟的儲存區原則。
- 由於虛擬機器主檔案已加密，請確保加密金鑰在還原時可供使用。

效能的最佳做法

- 加密效能取決於 CPU 和儲存區速度。
- 加密現有虛擬機器耗用的時間比在虛擬機器建立期間進行加密的時間要久。如果可能，請在建立虛擬機器時對其進行加密。

範例儲存區原則的最佳做法

請勿修改配套虛擬機器加密範例儲存區原則。請改為複製原則並編輯複製品。

備註 不存在將虛擬機器加密原則恢復為其原始設定的自動化方式。

如需自訂儲存區原則的詳細資料，請參閱 vSphere 儲存區說明文件。

移除加密金鑰的最佳做法

若要確保加密金鑰已從某個叢集移除，請在已加密的虛擬機器刪除、解除登錄或移至另一個 vCenter Server 後，將叢集中的 ESXi 主機重新開機。

虛擬機器加密注意須知

請檢閱虛擬機器加密注意須知，以避免稍後發生問題。

若要瞭解哪些裝置和功能不能與虛擬機器加密搭配使用，請參閱[虛擬機器加密互通性](#)。

加密虛擬機器限制

當您規劃虛擬機器加密策略時，請考慮下列注意須知。

- 複製加密的虛擬機器或執行 Storage vMotion 作業時，您可以嘗試變更磁碟格式。此類轉換不一定會成功。例如，如果複製虛擬機器並嘗試將磁碟格式從消極式歸零完整格式變更為精簡格式，虛擬機器磁碟會保留消極式歸零完整格式。
- 從虛擬機器卸除磁碟時，不會保留虛擬磁碟的儲存區原則資訊。
 - 如果虛擬磁碟已加密，您必須將儲存區原則明確設定為虛擬機器加密原則，或設定為包含加密的儲存區原則。
 - 如果虛擬磁碟未加密，您可以在將磁碟新增至虛擬機器時變更儲存區原則。

如需詳細資料，請參閱[虛擬磁碟加密](#)。

- 先解密核心傾印，然後再將虛擬機器移到其他叢集。

vCenter Server 不會儲存金鑰伺服器金鑰，僅會追蹤金鑰識別碼。因此，vCenter Server 不會永久儲存 ESXi 主機金鑰。但是，在 vSphere 7.0 Update 2 及更新版本中，即使對金鑰伺服器的存取已中斷，加密的裝置仍可運作。請參閱 [ESXi 主機上的 vSphere 金鑰持續性](#)。

在某些情況下，例如將 ESXi 主機移到其他叢集並將主機重新開機時，vCenter Server 會為主機指派新的主機金鑰。您無法使用新的主機金鑰解密任何現有核心傾印。

- 加密的虛擬機器不支援 OVF 匯出。
- 不支援使用 VMware Host Client 登錄加密的虛擬機器。

虛擬機器鎖定狀態

如果虛擬機器金鑰或一或多個虛擬磁碟金鑰遺失，虛擬機器會進入鎖定狀態。在鎖定狀態下，無法執行虛擬機器作業。

- 從 vSphere Client 加密虛擬機器及其磁碟時，會為它們使用相同的金鑰。
- 使用 API 執行加密時，您可以針對虛擬機器和磁碟使用不同的加密金鑰。在這種情況下，如果您嘗試開啟虛擬機器電源並且其中一個磁碟金鑰遺失，開啟電源作業就會失敗。如果移除虛擬磁碟，就可以開啟虛擬機器電源。

如需疑難排解建議，請參閱[解決缺少加密金鑰問題](#)。

虛擬機器加密互通性

vSphere 虛擬機器加密就可與其互通的裝置和功能方面存在一些限制。

以下限制和備註適用於使用 vSphere 虛擬機器加密的情況。如需有關使用 vSAN 加密的類似資訊，請參閱管理 VMware vSAN 說明文件。

關於特定加密工作的限制

在加密的虛擬機器上執行某些任務時，會有一些限制。

- 無法在已開啟電源的虛擬機器上執行大多數加密作業。必須關閉虛擬機器的電源。您可以在虛擬機器電源開啟時複製加密的虛擬機器，並且可以執行淺層雙重加密。
- 無法在具有快照的虛擬機器上執行深度雙重加密。您可以在具有快照的虛擬機器上執行淺層雙重加密。

虛擬信賴平台模組裝置和 vSphere 虛擬機器加密

虛擬信賴平台模組 (vTPM) 是實體信賴平台模組 2.0 晶片的基於軟體的表示。您可以將 vTPM 新增至新虛擬機器或現有的虛擬機器。若要將 vTPM 新增至虛擬機器，必須在 vSphere 環境中設定金鑰提供者。設定 vTPM 時，將對虛擬機器的「主」檔案 (記憶體交換、NVRAM 檔案等) 進行加密。磁碟檔案或 VMDK 檔案不會自動加密。可以選擇為虛擬機器磁碟明確新增加密。

注意 複製虛擬機器將複製整個虛擬機器，包括 vTPM 等虛擬裝置。儲存在 vTPM 中的資訊 (包括軟體可用於確定系統身分識別的 vTPM 內容) 也會進行複製。

從 vSphere 8.0 開始，在複製包含 vTPM 的虛擬機器時，會從一個新的空白 vTPM 開始，該 vTPM 將取得自己的密碼和身分識別。

vSphere 虛擬機器加密以及暫停狀態和快照

您可以從已加密虛擬機器的暫停狀態恢復，或還原為已加密機器的記憶體快照。您可以將在 ESXi 主機之間移轉具有記憶體快照和暫停狀態的已加密虛擬機器。

vSphere 虛擬機器加密和 IPv6

在純 IPv6 模式或混合模式下，可以使用 vSphere 虛擬機器加密。您可以使用 IPv6 位址設定金鑰伺服器。可以僅使用 IPv6 位址設定 vCenter Server 和金鑰伺服器。

vSphere 虛擬機器加密中的複製限制

對於所有金鑰提供者類型，支援複製需要滿足一定的條件。您可以在複製時變更加密金鑰。某些複製功能無法與 vSphere 虛擬機器加密搭配使用。

- 支援完整複製。複製會繼承父系加密狀態 (包括金鑰)。您可以加密完整複製、雙重加密完整複製以使用新金鑰，或解密完整複製。

支援連結複製，並且複製會繼承父系加密狀態 (包括金鑰)。無法解密連結複製或使用不同金鑰雙重加密連結複製。

備註 確認其他應用程式支援連結複製。例如，VMware Horizon® 7 支援完整複製和即時複製，但不支援連結複製。

- 所有金鑰提供者類型都支援即時複製，但在複製時無法變更加密金鑰。
- 您可以從加密的虛擬機器建立連結複製虛擬機器。連結複製虛擬機器包含相同的金鑰。您可以對連結複製的加密虛擬機器「首頁」檔案重設金鑰，但無法對磁碟重設金鑰。

vSphere Native Key Provider 的限制

vSphere Native Key Provider 不支援某些作業。

- 無法使用 vSphere Native Key Provider 對獨立主機上的虛擬機器進行加密。主機必須位於叢集中才能使用 vSphere Native Key Provider。
- 無法將包含使用 vSphere Native Key Provider 加密的虛擬機器的主機移至其他叢集，除非目標叢集包含相同的 vSphere Native Key Provider。(當加密金鑰不存在且目標叢集不具有相同的 vSphere Native Key Provider 時，將會鎖定已移動主機上的加密虛擬機器。)
- 由於不支援 vSphere Native Key Provider，無法將 vSphere Native Key Provider 加密的虛擬機器登錄到舊版主機。
- 由於要求獨立主機位於叢集中，無法將 vSphere Native Key Provider 加密的虛擬機器登錄到獨立主機。

vSphere 虛擬機器加密不支援的磁碟組態

vSphere 虛擬機器加密不支援某些類型的虛擬機器磁碟組態。

- RDM (原始裝置對應)。但是，支援 vSphere Virtual Volumes (vVols)。
- 多重寫入器或共用磁碟 (MSCS、WSFC 或 Oracle RAC)。多寫入器磁碟支援加密虛擬機器的「主」檔案。多重寫入器磁碟不支援加密虛擬磁碟。如果嘗試在具有加密虛擬磁碟的虛擬機器的編輯設定頁面中選取多重寫入器，則會停用確定按鈕。

vSphere 虛擬機器加密中的其他限制

無法與 vSphere 虛擬機器加密搭配使用的其他功能包括下列各項。

- vSphere ESXi Dump Collector
- 內容程式庫
 - 內容程式庫支援兩種類型的範本，即 OVF 範本類型和虛擬機器範本類型。無法將加密虛擬機器匯出為 OVF 範本類型。OVF Tool 不支援加密虛擬機器。可以使用虛擬機器範本類型建立加密虛擬機器範本。從 vSphere 8.0 開始，ovftool 命令包含將 vTPM 預留位置新增到 OVF 描述元檔案的選項。從此類範本部署虛擬機器時，vCenter Server 在目的地虛擬機器上建立具有唯一密碼的 vTPM。請參閱《vSphere 虛擬機器管理》說明文件。
- 用於備份加密虛擬磁碟的軟體必須使用 VMware vSphere Storage API - Data Protection (VADP) 在熱新增模式或啟用了 SSL 的 NBD 模式下備份磁碟。但是，並非所有使用 VADP 進行虛擬磁碟備份的備份解決方案都受支援。有關詳細資料，請洽詢您的備份廠商。
 - 不支援使用 VADP SAN 傳輸模式解決方案備份加密虛擬磁碟。
 - 加密虛擬磁碟支援 VADP 熱新增解決方案。備份軟體必須支援對在熱新增備份工作流中使用的 Proxy 虛擬機器進行加密。廠商必須具有密碼編譯作業.加密虛擬機器權限。
 - 備份加密虛擬磁碟時，支援使用 NBD-SSL 傳輸模式的備份解決方案。廠商應用程式必須具有密碼編譯作業.直接存取權限。

- 無法將輸出從加密的虛擬機器傳送至序列埠或平行埠。即使組態顯示成功，輸出仍傳送至檔案。
- VMware Cloud on AWS 中不支援 vSphere 虛擬機器加密。請參閱《管理 VMware Cloud on AWS 資料中心》說明文件。

ESXi 主機上的 vSphere 金鑰持續性

在 vSphere 7.0 Update 2 及更新版本中，即使金鑰伺服器暫時離線或無法使用，加密的虛擬機器和虛擬 TPM 仍可繼續運作 (可選)。ESXi 主機可保存加密金鑰以繼續執行加密和 vTPM 作業。

在 vSphere 7.0 Update 2 之前，加密的虛擬機器和 vTPM 要求金鑰伺服器始終可以運作。在 vSphere 7.0 Update 2 及更新版本中，即使對金鑰伺服器的存取已中斷，加密的裝置仍可運作。

從 vSphere 7.0 Update 3 開始，即使對金鑰提供者的存取已中斷，加密 vSAN 叢集也可以正常運作。

備註 使用 vSphere Native Key Provider 時，不需要金鑰持續性。vSphere Native Key Provider 設計為立即可用，無需存取金鑰伺服器即可執行。請參閱以下章節：「金鑰持續性和 vSphere Native Key Provider」。

ESXi 主機上的金鑰持續性的運作方式

使用標準金鑰提供者時，ESXi 主機依賴 vCenter Server 管理加密金鑰。使用受信任金鑰提供者時，ESXi 主機直接依賴 Trust Authority 主機取得金鑰，並未涉及 vCenter Server。vSphere Native Key Provider 處理金鑰的方式不同。如需詳細資訊，請參閱下一節。

無論金鑰提供者的類型為何，ESXi 主機會從一開始取得金鑰並將其保留在金鑰快取中。如果 ESXi 主機重新開機，將會失去其金鑰快取。然後，ESXi 主機從金鑰伺服器 (標準金鑰提供者) 或 Trust Authority 主機 (受信任的金鑰提供者) 再次請求金鑰。當 ESXi 主機嘗試取得金鑰且金鑰伺服器已離線或無法連線時，vTPM 和工作負載加密將無法運作。對於 Edge 式部署 (金鑰伺服器通常未部署在站台中)，與金鑰伺服器中斷連線可能會導致加密的工作負載出現不必要的停機時間。

在 vSphere 7.0 Update 2 及更新版本中，即使金鑰伺服器已離線或無法連線，加密的工作負載仍可繼續運作。如果 ESXi 主機具有 TPM，則加密金鑰將在重新開機過程中一直保存於 TPM 中。因此，即使 ESXi 主機重新開機，該主機也不需要請求加密金鑰。此外，當金鑰伺服器無法使用時，加密和解密作業也可繼續進行，因為這些金鑰一直保存在 TPM 中。本質上來說，當金鑰伺服器或 Trust Authority 主機無法使用時，您可以繼續以「無金鑰伺服器」方式執行加密的工作負載，具體取決於金鑰提供者。此外，即使金鑰伺服器無法連線，vTPM 也可繼續運作。

金鑰持續性和 vSphere Native Key Provider

使用 vSphere Native Key Provider 時，vSphere 會產生加密金鑰，並且不需要金鑰伺服器。ESXi 主機取得金鑰衍生金鑰 (KDK)，可用來衍生其他金鑰。收到 KDK 並產生其他金鑰後，ESXi 主機不需要存取 vCenter Server，即可執行加密作業。本質上來說，vSphere Native Key Provider 始終以「無金鑰伺服器」方式執行。

依預設，即使 ESXi 主機重新開機，甚至 vCenter Server 在主機重新開機後不可用時，KDK 仍會保留在主機上。

您可以使用 vSphere Native Key Provider 啟用金鑰持續性，但通常無需執行此操作。ESXi 主機可完全存取 vSphere Native Key Provider，因此額外的金鑰持續性是冗餘的。使用 vSphere Native Key Provider 啟用金鑰持續性的一個使用案例是，同時設定了標準金鑰提供者 (外部 KMIP 伺服器) 的情況。

如何設定金鑰持續性

若要啟用或停用金鑰持續性，請參閱 [在 ESXi 主機上啟用和停用金鑰持續性](#)。

設定和管理標準金鑰提供者

7

在 vSphere 環境中使用標準金鑰提供者需要做一些準備。在設定您的環境之後，您可以建立已加密的虛擬機器和虛擬磁碟，以及加密現有虛擬機器和磁碟。

針對標準金鑰提供者設定您的環境之後，您可以使用 vSphere Client 建立已加密的虛擬機器和虛擬磁碟，以及加密現有虛擬機器和磁碟。請參閱第 10 章 [在 vSphere 環境中使用加密](#)。

您可以透過使用 API 和 crypto-util CLI 執行其他工作。請參閱 vSphere Web Services SDK 程式設計指南以取得 API 說明文件，以及參閱 crypto-util 命令列說明以取得有關此工具的詳細資料。

本章節討論下列主題：

- [標準金鑰提供者概觀](#)
- [設定標準金鑰提供者](#)
- [為不同使用者設定獨立的金鑰提供者](#)

標準金鑰提供者概觀

可以使用標準金鑰提供者執行虛擬機器加密工作。

什麼是標準金鑰提供者？

在 vSphere 中，標準金鑰提供者可直接從金鑰伺服器取得加密金鑰，然後 vCenter Server 將金鑰散佈到資料中心內所需的 ESXi 主機。

您可以為不同的使用者新增單獨的標準金鑰提供者，並設定預設標準金鑰提供者。

vSphere 標準金鑰提供者需求

- vSphere 6.5 或更新版本
- 外部金鑰伺服器 (KMS)

金鑰伺服器必須支援金鑰管理互通協定 (KMIP) 1.1 標準。如需詳細資料，請參閱 vSphere 相容性對照表。

您可以在《[VMware 相容性指南](#)》中的〈平台與運算〉下找到 VMware 認證的金鑰伺服器 (KMS) 廠商的相關資訊。如果選取《相容性指南》，您可以開啟《金鑰管理伺服器 (KMS) 相容性》說明文件。本說明文件會經常更新。

標準金鑰提供者權限

標準金鑰提供者使用 **Cryptographer.*** 權限。請參閱[密碼編譯作業權限](#)。

設定標準金鑰提供者

在開始執行虛擬機器加密工作之前，您必須設定標準金鑰提供者。

設定標準金鑰提供者包括新增金鑰提供者以及建立與金鑰伺服器的信任。新增金鑰提供者時，系統會提示您將其設為預設值。您可以明確變更預設金鑰提供者。vCenter Server 會從預設金鑰提供者佈建金鑰。

備註 先前在 vSphere 6.5 和 6.7 中稱為金鑰管理伺服器叢集，現在稱為金鑰提供者。

使用 vSphere Client 新增標準金鑰提供者

您可以從 vSphere Client 或使用公開 API，將標準金鑰提供者新增至 vCenter Server 系統。

透過 vSphere Client，可以將標準金鑰提供者新增到 vCenter Server 系統，並在金鑰伺服器和 vCenter Server 之間建立信任。

- 您可以新增來自同一廠商的多個金鑰伺服器。
- 如果您的環境支援不同廠商提供的解決方案，則可以新增多個金鑰提供者。
- 如果您的環境包含多個金鑰提供者，且刪除了預設金鑰提供者，則必須明確設定其他預設值。
- 您可以使用 IPv6 位址設定金鑰伺服器。
 - vCenter Server 系統和金鑰伺服器都可以僅設定 IPv6 位址。

必要條件

- 確認金鑰伺服器 (KMS) 位於《適用於金鑰管理伺服器 (KMS) 的 VMware 相容性指南》並與 KMIP 1.1 相容，而且可以是對稱金鑰 Foundry 和伺服器。
- 確認您具有所需權限：[密碼編譯作業.管理金鑰伺服器](#)。
- 確保金鑰伺服器具有高可用性。中斷與金鑰伺服器的連線 (例如，在斷電或災難復原事件期間)，會導致加密的虛擬機器無法存取。

備註 從 vSphere 7.0 Update 2 開始，即使金鑰伺服器暫時離線或無法使用，加密的虛擬機器和虛擬 TPM 仍可繼續運作。請參閱[ESXi 主機上的 vSphere 金鑰持續性](#)。

- 請仔細考慮您的基礎結構對金鑰伺服器的相依性。某些 KMS 解決方案會做為虛擬應用裝置提供，可讓您建立相依性迴圈或其他關於無法放置 KMS 應用裝置的可用性問題。

程序

- 1 使用 vSphere Client 登入 vCenter Server 系統。
- 2 瀏覽詳細目錄清單，並選取 vCenter Server 執行個體。
- 3 按一下**設定**，然後按一下**安全性**下的**金鑰提供者**。

4 按一下**新增標準金鑰提供者**，然後輸入金鑰提供者資訊。

選項	值
名稱	金鑰提供者的名稱。 每個邏輯金鑰提供者 (無論其類型為標準、可信任還是本機) 都必須在所有 vCenter Server 系統中具有唯一的名稱。 如需詳細資訊，請參閱 金鑰提供者命名 。
KMS	金鑰伺服器 (KMS) 的別名。
位址	金鑰伺服器的 IP 位址或 FQDN。
連接埠	vCenter Server 連線至金鑰伺服器所在的連接埠。
Proxy 伺服器	用於連線至金鑰伺服器的選用 Proxy 伺服器位址。
Proxy 連接埠	用於連線至金鑰伺服器的選用 Proxy 連接埠。
使用者名稱	有些金鑰伺服器廠商允許使用者透過指定使用者名稱和密碼，隔離不同使用者或群組所使用的加密金鑰。只有在金鑰伺服器支援此功能，且您想要使用此功能時，才指定使用者名稱。
密碼	有些金鑰伺服器廠商允許使用者透過指定使用者名稱和密碼，隔離不同使用者或群組所使用的加密金鑰。只有在金鑰伺服器支援此功能，且您想要使用此功能時，才指定密碼。

您可以按一下**新增 KMS**，以新增更多金鑰伺服器。

5 按一下**新增金鑰提供者**。

6 按一下**信任**。

vCenter Server 會新增金鑰提供者，並將狀態顯示為 [已連線]。

後續步驟

請參閱[透過交換憑證建立標準金鑰提供者信任連線](#)。

透過交換憑證建立標準金鑰提供者信任連線

將標準金鑰提供者新增至 vCenter Server 系統後，可以建立信任連線。確切程序取決於金鑰提供者接受的憑證以及您的公司原則。

必要條件

新增標準金鑰提供者。

程序

- 1 導覽到 vCenter Server。
- 2 按一下**設定**，然後選取**安全性**下的**金鑰提供者**。
- 3 選取金鑰提供者。
隨即顯示金鑰提供者的 KMS。
- 4 選取 KMS。

- 5 從**建立信任**下拉式功能表中，選取**使 KMS 信任 vCenter**。
- 6 選取適合您伺服器的選項，並依照下列步驟進行操作。

選項	請參閱
vCenter Server 根 CA 憑證	使用根 CA 憑證選項建立標準金鑰提供者信任連線。
vCenter Server 憑證	使用憑證選項建立標準金鑰提供者信任連線。
上傳憑證和私密金鑰	使用上傳憑證和私密金鑰選項建立標準金鑰提供者信任連線。
新增憑證簽署申請	使用新增憑證簽署要求選項建立標準金鑰提供者信任連線。

使用根 CA 憑證選項建立標準金鑰提供者信任連線

某些金鑰管理伺服器 (KMS) 廠商會要求您將根 CA 憑證上傳到 KMS。之後，由您的根 CA 簽署的所有憑證會受此 KMS 信任。

vSphere 虛擬機器加密使用的根 CA 憑證是自我簽署的憑證，儲存於 vCenter Server 系統上 VMware Endpoint 憑證存放區 (VECS) 的獨立存放區中。

備註 僅在您想要取代現有憑證時，才產生根 CA 憑證。如果您產生該憑證，則由該 CA 簽署的其他憑證將變為無效。您可在此工作流程期間產生新的根 CA 憑證。

程序

- 1 導覽到 vCenter Server。
- 2 按一下**設定**，然後選取**安全性下的金鑰提供者**。
- 3 選取想要與其建立信任連線的金鑰提供者。
隨即顯示金鑰提供者的金鑰伺服器 (KMS)。
- 4 從**建立信任**下拉式功能表中，選取**使 KMS 信任 vCenter**。
- 5 選取 **vCenter 根 CA 憑證**，然後按**下一步**。
[下載根 CA 憑證] 對話方塊會填入 vCenter Server 用於加密的根憑證。此憑證儲存於 VECS 中。
- 6 將憑證複製到剪貼簿，或將憑證下載為檔案。
- 7 遵循 KMS 廠商提供的指示將憑證上傳到其系統。

備註 部分 KMS 廠商會要求 KMS 廠商重新啟動 KMS 以獲取您上傳的根憑證。

後續步驟

完成憑證交換。請參閱[完成標準金鑰提供者的信任設定](#)。

使用憑證選項建立標準金鑰提供者信任連線

某些金鑰管理伺服器 (KMS) 廠商會要求您將 vCenter Server 憑證上傳到 KMS。上傳後，KMS 會接受來自具有該憑證之系統的流量。

vCenter Server 會產生憑證來保護與 KMS 的連線。該憑證會儲存在 vCenter Server 系統上 VMware Endpoint 憑證存放區 (VECS) 的獨立金鑰存放區中。

程序

- 1 導覽到 vCenter Server。
- 2 按一下**設定**，然後選取**安全性下的金鑰提供者**。
- 3 選取想要與其建立信任連線的金鑰提供者。
隨即顯示金鑰提供者的金鑰伺服器 (KMS)。
- 4 從**建立信任**下拉式功能表中，選取**使 KMS 信任 vCenter**。
- 5 選取 **vCenter 憑證**，然後按下一步。

[下載憑證] 對話方塊會填入 vCenter Server 用於加密的根憑證。此憑證儲存於 VECS 中。

備註 除非您想要取代現有憑證，否則請勿產生新憑證。

- 6 將憑證複製到剪貼簿中，或將其下載為檔案。
- 7 遵循 KMS 廠商提供的指示將憑證上傳到 KMS。

後續步驟

信任關係定案。請參閱[完成標準金鑰提供者的信任設定](#)。

使用上傳憑證和私密金鑰選項建立標準金鑰提供者信任連線

某些金鑰管理伺服器 (KMS) 廠商會要求您將 KMS 伺服器憑證和私密金鑰上傳到 vCenter Server 系統。

部分 KMS 廠商針對連線產生憑證和私密金鑰，並使其可供您使用。上傳檔案後，KMS 信任您的 vCenter Server 執行個體。

必要條件

- 從 KMS 廠商要求憑證和私密金鑰。檔案是採用 PEM 格式的 X509 檔案。

程序

- 1 導覽到 vCenter Server。
- 2 按一下**設定**，然後選取**安全性下的金鑰提供者**。
- 3 選取想要與其建立信任連線的金鑰提供者。
隨即顯示金鑰提供者的金鑰伺服器 (KMS)。
- 4 從**建立信任**下拉式功能表中，選取**使 KMS 信任 vCenter**。
- 5 選取 **KMS 憑證和私密金鑰**，然後按下一步。
- 6 將您從 KMS 廠商接收的憑證貼至頂部文字方塊中，或按一下**上傳檔案**上傳憑證檔案。
- 7 將金鑰檔案貼至底部文字方塊中，或按一下**上傳檔案**上傳金鑰檔案。

8 按一下**建立信任**。

後續步驟

信任關係定案。請參閱[完成標準金鑰提供者的信任設定](#)。

使用新增憑證簽署要求選項建立標準金鑰提供者信任連線

某些金鑰管理伺服器 (KMS) 廠商會要求 vCenter Server 產生憑證簽署要求 (CSR) 並將該 CSR 傳送到 KMS。KMS 簽署 CSR 並傳回已簽署憑證。您可將已簽署憑證上傳到 vCenter Server。

使用**新增憑證簽署要求**選項的程序分為兩步。首先，產生 CSR 並將其傳送給 KMS 廠商。然後，將從 KMS 廠商接收的已簽署憑證上傳到 vCenter Server。

程序

- 1 導覽到 vCenter Server。
- 2 按一下**設定**，然後選取**安全性下的金鑰提供者**。
- 3 選取想要與其建立信任連線的金鑰提供者。
隨即顯示金鑰提供者的金鑰伺服器 (KMS)。
- 4 從**建立信任**下拉式功能表中，選取**使 KMS 信任 vCenter**。
- 5 選取**新增憑證簽署要求 (CSR)**，然後按下一步。
- 6 在對話方塊中，將文字方塊中的完整憑證複製到剪貼簿，或以檔案形式將其下載。
僅在您明確想要產生 CSR 時，才使用對話方塊中的**產生新 CSR** 按鈕。
- 7 遵循 KMS 廠商提供的指示來提交 CSR。
- 8 當您從 KMS 廠商收到已簽署的憑證時，請再次按一下**金鑰提供者**，選取金鑰提供者，然後從**建立信任**下拉式功能表中，選取**上傳已簽署的 CSR 憑證**。
- 9 將已簽署憑證貼至底部文字方塊中，或按一下**上傳檔案**來上傳檔案，然後按一下**上傳**。

後續步驟

信任關係定案。請參閱[完成標準金鑰提供者的信任設定](#)。

完成標準金鑰提供者的信任設定

除非**新增標準金鑰提供者**對話方塊提示您信任 KMS，否則您必須在憑證交換完成後明確建立信任。

可以透過信任 KMS 或上傳 KMS 憑證完成信任設定，即讓 vCenter Server 信任 KMS。您有兩個選項可供選擇：

- 使用**上傳 KMS 憑證**選項明確信任憑證。
- 使用**使 vCenter 信任 KMS**選項，將 KMS 分葉憑證或 KMS CA 憑證上傳至 vCenter Server。

備註 如果您上傳根 CA 憑證或中繼 CA 憑證，vCenter Server 會信任由該 CA 簽署的所有憑證。為確保強大的安全性，請上傳 KMS 廠商控制的分葉憑證或中繼 CA 憑證。

程序

- 1 導覽到 vCenter Server。
- 2 按一下**設定**，然後選取**安全性**下的**金鑰提供者**。
- 3 選取想要與其建立信任連線的金鑰提供者。
隨即顯示金鑰提供者的金鑰伺服器 (KMS)。
- 4 選取 KMS。
- 5 從**建立信任**下拉式功能表中，選取下列其中一個選項。

選項	動作
使 vCenter 信任 KMS	在顯示的對話方塊中，按一下 信任 。
上傳 KMS 憑證	<ol style="list-style-type: none"> a 在出現的對話方塊中，貼上憑證，或按一下上傳檔案並瀏覽至憑證檔案。 b 按一下上傳。

為不同使用者設定獨立的金鑰提供者

您可以設定同一 KMS 執行個體的不同使用者具有不同金鑰提供者的環境。有多個金鑰提供者非常有用，例如，如果您想授與公司的不同部門對不同加密金鑰集的存取權限。

可以對同一個 KMS 使用多個金鑰提供者來分隔金鑰。有不同的金鑰集對於使用案例 (如不同匯流排或不同客戶) 至關重要。

備註 並非所有 KMS 廠商都支援多個使用者。

必要條件

設定與 KMS 的連線。

程序

- 1 在 KMS 上使用對應的使用者名稱和密碼建立兩個使用者，例如 C1 和 C2。
- 2 登入 vCenter Server 並建立第一個金鑰提供者。
- 3 當提示輸入使用者名稱和密碼時，請提供第一個使用者的唯一資訊。
- 4 建立第二個金鑰提供者並新增相同 KMS，但使用第二個使用者名稱和密碼 (C2)。

結果

這兩個金鑰提供者獨立連線至 KMS，並使用不同的金鑰集。

設定和管理 vSphere Native Key Provider

8

在 vSphere 環境中使用 VMware vSphere® Native Key Provider™ 需要做一些準備。設定 vSphere Native Key Provider 之後，您可以在虛擬機器上建立虛擬信賴平台模組 (vTPM)。

針對 vSphere Native Key Provider 設定環境後，可以使用 vSphere Client 和 API 建立 vTPM。如果購買的是 VMware vSphere® Enterprise Plus 版本™，還可以加密虛擬機器和虛擬磁碟，以及加密現有的虛擬機器和磁碟。



(設定 vSphere Native Key Provider)

本章節討論下列主題：

- [vSphere Native Key Provider 概觀](#)
- [vSphere Native Key Provider 程序流程](#)
- [設定 vSphere Native Key Provider](#)
- [備份 vSphere Native Key Provider](#)
- [在增強型連結模式組態中匯入 vSphere Native Key Provider](#)
- [復原 vSphere Native Key Provider](#)
- [更新 vSphere Native Key Provider](#)
- [刪除 vSphere Native Key Provider](#)

vSphere Native Key Provider 概觀

在 vSphere 7.0 Update 2 及更新版本中，您可以使用內建 vSphere Native Key Provider 來啟用加密技術，如虛擬 TPM (vTPM)。

vSphere Native Key Provider 已包含在所有 vSphere 版本中，且不需要外部金鑰伺服器 (業內也稱為金鑰管理伺服器 (KMS))。也可以將 vSphere Native Key Provider 用於 vSphere 虛擬機器加密，但必須購買 VMware vSphere® Enterprise Plus 版本™。

什麼是 vSphere Native Key Provider

使用標準金鑰提供者或受信任金鑰提供者時，您必須設定外部金鑰伺服器。在標準金鑰提供者的設定過程中，vCenter Server 從外部金鑰伺服器擷取金鑰並將其散佈到 ESXi 主機。在受信任金鑰提供者 (vSphere Trust Authority) 的設定過程中，受信任的 ESXi 主機直接擷取金鑰。

通過 vSphere Native Key Provider，不再需要外部金鑰伺服器。vCenter Server 會產生一個稱為金鑰衍生金鑰 (KDK) 的主要金鑰，並將其推送至叢集中的所有 ESXi 主機。然後，ESXi 主機產生資料加密金鑰 (即使未連線到 vCenter Server)，以啟用 vTPM 等安全性功能。所有 vSphere 版本均包含 vTPM 功能。若要將 vSphere Native Key Provider 用於 vSphere 虛擬機器加密，則必須購買 vSphere Enterprise Plus 版本。vSphere Native Key Provider 可以與現有的金鑰伺服器基礎結構共存。

vSphere Native Key Provider：

- 允許使用 vTPM、vSphere 虛擬機器加密和 vSAN 靜態資料加密 (如果不需要或不想使用外部金鑰伺服器)。
- 僅適用於 VMware 基礎結構產品。
- 不提供外部互通性、KMIP 支援、硬體安全性模組或傳統的第三方外部金鑰伺服器為實現互通性或符合法規而提供的其他功能。如果您的組織需要將此功能用於非 VMware 產品和元件，請安裝傳統的第三方金鑰伺服器。
- 幫助滿足了無法使用外部金鑰伺服器或不想使用外部金鑰伺服器的組織需求。
- 改進了資料整理和系統重複使用做法，允許在難以整理的媒體 (如 Flash 和 SSD) 上早些使用加密技術。
- 提供金鑰提供者之間的轉換路徑。vSphere Native Key Provider 與 VMware 標準金鑰提供者和 vSphere Trust Authority 受信任金鑰提供者相容。
- 可用於使用增強型連結模式組態或 vCenter Server High Availability 組態的多個 vCenter Server 系統。
- 可用於在所有版本的 vSphere 中啟用 vTPM 以及對虛擬機器進行加密 (但需要購買包含 vSphere 虛擬機器加密的 vSphere Enterprise Plus 版本)。vSphere 虛擬機器加密適用於 vSphere Native Key Provider，就像適用於 VMware 標準金鑰提供者和受信任金鑰提供者一樣。
- 可用於通過使用適當的 vSAN 授權啟用 vSAN 靜態資料加密。
- 可使用信賴平台模組 (TPM) 2.0 提高安全性 (如果 ESXi 主機中安裝了 TPM)。還可以將 vSphere Native Key Provider 設定為僅對安裝了 TPM 2.0 的主機可用。

備註 ESXi 主機不需要 TPM 2.0 即可使用 vSphere Native Key Provider。不過，TPM 2.0 確實增強了安全性。

與所有安全性解決方案一樣，請考慮系統設計、實作考量事項和使用 Native Key Provider 的權衡。例如，ESXi 金鑰持續性避免了要求金鑰伺服器始終可用的相依性。但是，由於金鑰持續性將 Native Key Provider 密碼編譯資訊儲存在叢集主機上，因此，如果惡意操作者竊取 ESXi 主機本身，您仍會面臨風險。由於環境各不相同，因此請根據您所在組織的法規和安全性需求、運作需求以及風險承受能力來評估和實作安全性控制。

如需有關 vSphere Native Key Provider 的詳細概觀資訊，請參閱 <https://core.vmware.com/native-key-provider>。

vSphere Native Key Provider 需求

若要使用 vSphere Native Key Provider，您必須：

- 確保 vCenter Server 系統和 ESXi 主機均執行 vSphere 7.0 Update 2 或更高版本。
- 在叢集中設定 ESXi 主機。儘管不是必需要求，但最好使用盡可能相同的 ESXi 主機，包括 TPM。叢集主機相同時，叢集管理和功能啟用要容易得多。
- 設定 vCenter Server 以檔案為基礎的備份，並安全地還原和儲存備份，因為它們包含金鑰衍生金鑰。請參閱 vCenter Server 安裝和設定說明文件中有關 vCenter Server 備份和還原的主題。

若要使用 vSphere Native Key Provider 執行 vSphere 虛擬機器加密或 vSAN 加密，必須購買包含適當授權的產品版本。

vSphere Native Key Provider 和增強型連結模式

可以設定一個 vSphere Native Key Provider 並使其可在增強型連結模式組態下設定的 vCenter Server 系統之間共用。此案例中的高層級步驟包括：

- 1 在一個 vCenter Server 系統上建立 vSphere Native Key Provider
- 2 在建立 Native Key Provider 的 vCenter Server 上備份 Native Key Provider
- 3 匯出 Native Key Provider
- 4 將 Native Key Provider 匯入到增強型連結模式組態中的其他 vCenter Server 系統

請參閱[在增強型連結模式組態中匯入 vSphere Native Key Provider](#)。

vSphere Native Key Provider 權限

對於標準和受信任金鑰提供者，vSphere Native Key Provider 會使用 **Cryptographer.*** 權限。此外，vSphere Native Key Provider 還會使用 **Cryptographer.ReadKeyServersInfo** 權限 (vSphere Native Key Provider 專屬權限) 來列出 vSphere Native Key Provider。請參閱[密碼編譯作業權限](#)。

vSphere Native Key Provider 警示

您必須備份 vSphere Native Key Provider。如果未備份 vSphere Native Key Provider，vCenter Server 會產生一個警示。當您備份已產生警示的 vSphere Native Key Provider 時，vCenter Server 會重設該警示。依預設，vCenter Server 每天檢查已備份的 vSphere Native Key Provider 一次。您可以透過修改 `vpzd.KMS.backupCheckInterval` 選項來變更檢查間隔。

vSphere Native Key Provider 定期修復檢查

vCenter Server 會定期檢查 vCenter Server 和 ESXi 主機上的 vSphere Native Key Provider 組態是否相符。當主機狀態變更時 (例如，將主機新增到叢集時)，叢集上的金鑰提供者組態會偏離主機上的組態。如果主機上的組態 (keyID) 有所不同，vCenter Server 會自動更新主機組態。不需要手動介入。

依預設，vCenter Server 每 5 分鐘檢查一次組態。可以透過使用 `vpzd.KMS.remediationInterval` 選項修改間隔。

將 vSphere Native Key Provider 用於災難復原站台

可以將 vSphere Native Key Provider 用於備份災難復原站台。透過將 vSphere Native Key Provider 備份從主要 vCenter Server 匯入災難復原站台的 vCenter Server 備份中，該叢集能夠解密並執行加密的虛擬機器。

始終測試 DR 解決方案。絕對不要以為您的解決方案可正常執行，無需嘗試復原。確保 DR 站台也可以使用 vSphere Native Key Provider 備份的複本。

vSphere Native Key Provider 程序流程

瞭解 vSphere Native Key Provider 程序流程對於瞭解如何設定和管理 vSphere Native Key Provider 非常重要。

您可以使用內建的 vSphere Native Key Provider 支援以加密為基礎的虛擬 TPM (vTPM)。vSphere Native Key Provider 已包含在所有 vSphere 版本中，且不需要外部金鑰伺服器 (KMS)。若要將 vSphere Native Key Provider 用於 vSphere 虛擬機器加密，則必須購買 vSphere Enterprise+ 版本。

設定 vSphere Native Key Provider

設定 vSphere Native Key Provider 的程序涉及以下基本作業：

- 1 具有適當管理權限的使用者使用 vSphere Client 在 vCenter Server 上建立 vSphere Native Key Provider。
- 2 然後，vCenter Server 為 ESXi 主機的所有叢集設定 vSphere Native Key Provider。
在此步驟中，vCenter Server 將主要金鑰推送至叢集中的所有 ESXi 主機。同樣地，如果更新或刪除 vSphere Native Key Provider，則會將變更推送至叢集中的主機。
- 3 具有適當密碼編譯權限的使用者建立 vTPM 和加密的虛擬機器 (假設您已購買 vSphere Enterprise+ 版本)。

請參閱第 11 章 [使用虛擬信賴平台模組保護虛擬機器](#) 和第 10 章 [在 vSphere 環境中使用加密](#)。

vSphere Native Key Provider 加密程序流程

若要瞭解不同元件如何互動以使用 vSphere Native Key Provider 執行加密，請參閱 [vSphere Native Key Provider 加密程序流程](#)。

設定 vSphere Native Key Provider

執行加密工作需要金鑰提供者。您可以使用 vSphere Client 在 vCenter Server 上設定 vSphere Native Key Provider。

vSphere 7.0 Update 2 及更新版本包含稱為 vSphere Native Key Provider 的金鑰提供者。vSphere Native Key Provider 支援與加密相關的功能，而不需要外部金鑰伺服器 (KMS)。一開始，vCenter Server 未設定 vSphere Native Key Provider。您必須手動設定 vSphere Native Key Provider。

ESXi 主機不需要 TPM 2.0 即可使用 vSphere Native Key Provider。不過，TPM 2.0 確實增強了安全性。

備註 設定 vSphere Native Key Provider 時，金鑰提供者在其設定所在的 vCenter Server 的所有叢集上均可供使用。因此，連結至 vCenter Server 的所有主機可存取您設定的所有 vSphere Native Key Provider。

必要條件

所需權限：**密碼編譯作業.管理金鑰伺服器**

程序

- 1 使用 vSphere Client 登入 vCenter Server 系統。
- 2 瀏覽詳細目錄清單，並選取 vCenter Server 執行個體。
- 3 按一下**設定**，然後按一下**安全性下的金鑰提供者**。
- 4 按一下**新增**，然後按一下**新增原生金鑰提供者**。
- 5 輸入 vSphere Native Key Provider 的名稱。

每個邏輯金鑰提供者 (無論其類型為標準、可信任還是本機) 都必須在所有 vCenter Server 系統中具有唯一的名稱。

如需詳細資訊，請參閱 [金鑰提供者命名](#)。

- 6 如果希望此 vSphere Native Key Provider 僅由具有 TPM 2.0 的主機使用，請選取**僅對受 TPM 保護的 ESXi 主機使用金鑰提供者**核取方塊。

如果已啟用，則 vSphere Native Key Provider 僅在具有 TPM 2.0 的主機上可用。

- 7 按一下**新增金鑰提供者**。

備註 資料中心內的所有叢集化 ESXi 主機取得金鑰提供者以及 vCenter Server 更新其快取大約需要五分鐘的時間。由於資訊的散佈方式，您可能必須等待幾分鐘，才能在某些主機上將金鑰提供者用於金鑰作業。

結果

vSphere Native Key Provider 將會新增並出現在**金鑰提供者**窗格中。此時，vSphere Native Key Provider 尚未備份。您必須先備份 vSphere Native Key Provider，然後才能使用它。

後續步驟

請參閱[備份 vSphere Native Key Provider](#)。

備份 vSphere Native Key Provider

如果必須還原金鑰提供者組態，必須備份 vSphere Native Key Provider，這是災難復原情況的一部分。您可以使用 vSphere Client、PowerCLI 或 API 備份 vSphere Native Key Provider。

將在 vCenter Server 之以檔案為基礎的備份過程中備份 vSphere Native Key Provider。但是，必須至少備份 vSphere Native Key Provider 一次，然後才能使用它。在建立 vSphere Native Key Provider 時，不會對其進行備份。

如果您必須還原組態，則備份是必要的。若要還原 vSphere Native Key Provider，請參閱[使用 vSphere Client 還原 vSphere Native Key Provider](#)。

將備份檔案保留在安全的位置。您可以在建立備份時對備份進行密碼保護。備份檔案採用 PKCS#12 格式。

如果 vSphere Native Key Provider 尚未備份，則 vCenter Server 會建立一個警示。您可以確認該警示，但它會每 24 小時重新顯示一次，直到 vSphere Native Key Provider 備份完成。

必要條件

所需權限：[密碼編譯作業](#)、[管理金鑰伺服器](#)

備註 在增強型連結模式組態中，必須在金鑰提供者所屬的 vCenter Server 上執行備份。

程序

- 1 使用 vSphere Client 登入 vCenter Server 系統。
- 2 瀏覽詳細目錄清單，並選取 vCenter Server 執行個體。
- 3 按一下**設定**，然後按一下**安全性下的金鑰提供者**。
- 4 選取想要備份的 vSphere Native Key Provider。
對於尚未備份的金鑰提供者，會顯示「未備份」狀態。
- 5 按一下**備份**。
- 6 若要對備份進行密碼保護，請勾選**使用密碼保護原生金鑰提供者資料方塊**。
 - a 輸入密碼，並將其儲存在安全的位置。
 - b 勾選**我已將密碼儲存在安全的位置方塊**，表示您已將密碼儲存至安全位置。
- 7 按一下**備份金鑰提供者**。
備份檔案採用 PKCS#12 格式。
- 8 將備份檔案儲存在安全的位置。

結果

vSphere Native Key Provider 狀態會從 [未備份] 變更為 [警告]、[作用中]。[警告] 表示 vCenter Server 仍在將資訊推送至資料中心中的所有 ESXi 主機。[作用中] 表示資訊已推送到所有主機。

後續步驟

若要將 vTPM 新增至 ESXi 主機，請參閱第 11 章 [使用虛擬信賴平台模組保護虛擬機器](#)。若要加密虛擬機器，請參閱第 10 章 [在 vSphere 環境中使用加密](#)。

在增強型連結模式組態中匯入 vSphere Native Key Provider

在增強型連結模式組態中的一個 vCenter Server 上建立 vSphere Native Key Provider 後，可以使用 vSphere Client 將其匯入到組態中的另一個 vCenter Server。

可以設定一個 vSphere Native Key Provider 並使其可在增強型連結模式組態下設定的 vCenter Server 系統之間共用。可以在增強型連結模式組態中的一個 vCenter Server 系統上建立 vSphere Native Key Provider，然後使用**還原**功能將加密金鑰檔案匯入到其他 ELM 連線的 vCenter Server 系統。

必要條件

- 所需權限：**密碼編譯作業.管理金鑰伺服器**
- 在增強型連結模式組態中的一個 vCenter Server 系統上建立 vSphere Native Key Provider。請參閱 [設定 vSphere Native Key Provider](#)。
- 備份 vSphere Native Key Provider 並下載備份加密金鑰檔案。請參閱[備份 vSphere Native Key Provider](#)。將備份加密金鑰檔案放置在匯入時可以存取的安全位置。

程序

- 1 使用 vSphere Client，登入到增強型連結模式組態中要匯入 vSphere Native Key Provider 的一個 vCenter Server。
- 2 瀏覽詳細目錄清單，並選取 vCenter Server 執行個體。
- 3 按一下**設定**，然後按一下**安全性**下的**金鑰提供者**。
- 4 按一下**還原**。
- 5 流覽到儲存 vSphere Native Key Provider 備份加密金鑰檔案的檔案位置。
檔案以 PKCS#12 格式儲存。
- 6 選取檔案。
- 7 (選擇性) 如果檔案受密碼保護，請輸入密碼。
- 8 按下一步。
- 9 (選擇性) 如果您決定僅對受 TPM 保護的 ESXi 主機使用此金鑰提供者，請選取此核取方塊。
- 10 按一下**完成**。

結果

vSphere Native Key Provider 隨即匯入至 vCenter Server。若要使用 vSphere Native Key Provider 執行加密工作，請確保先在**金鑰提供者**窗格中選取它，然後按一下**設定為預設值**。

後續步驟

對增強型連結模式組態中要新增 vSphere Native Key Provider 的其他 vCenter Server 系統重複這些步驟。

復原 vSphere Native Key Provider

您可以透過 vSphere Client 或從 vCenter Server Appliance 備份復原 vSphere Native Key Provider。

必要時，可以使用下列方式復原 vSphere Native Key Provider。

- 1 如果不需要重建 vCenter Server Appliance，則使用 vSphere Client 還原金鑰提供者。請參閱[使用 vSphere Client 還原 vSphere Native Key Provider](#)。
- 2 如果必須重建 vCenter Server Appliance，則必須從 vCenter Server Appliance 備份還原金鑰提供者。執行 vCenter Server Appliance 備份時，將會儲存原生金鑰提供者。如需從備份還原 vCenter Server Appliance 的相關資訊，請參閱 <https://blogs.vmware.com/vsphere/2018/05/vcenter-server-appliance-6-7-file-based-backup-and-restore-walkthroughs.html>。

使用 vSphere Client 還原 vSphere Native Key Provider

您可以使用 vSphere Client 還原 vSphere Native Key Provider。

在原生金鑰提供者遭到意外刪除或您必須執行災難復原的情況下，可以還原原生金鑰提供者。

還原 vSphere Native Key Provider 時，不需要再次備份金鑰提供者。執行初始備份即可。繼續將備份檔案維持在安全的位置。

必要條件

- 所需權限：**密碼編譯作業.管理金鑰伺服器**
- 金鑰提供者備份檔案。
- 金鑰提供者檔案的密碼 (如果您在備份金鑰提供者時輸入了密碼)。

程序

- 1 使用 vSphere Client 登入 vCenter Server 系統。
- 2 瀏覽詳細目錄清單，並選取 vCenter Server 執行個體。
- 3 按一下**設定**，然後按一下**安全性下的金鑰提供者**。
- 4 選取 vSphere Native Key Provider，然後按一下**還原**。
- 5 瀏覽至檔案位置，然後選取備份加密的金鑰檔案。
檔案以 PKCS#12 格式儲存。
- 6 (選擇性) 如果檔案受密碼保護，請輸入密碼。
- 7 按**下一步**。
- 8 (選擇性) 如果您決定僅對受 TPM 保護的 ESXi 主機使用此金鑰提供者，請選取此核取方塊。

9 按一下完成。

結果

vSphere Native Key Provider 已還原。

更新 vSphere Native Key Provider

作為定期金鑰輪替計劃的一部分，可以使用 PowerCLI 更新 vSphere Native Key Provider。

如果您有金鑰輪替原則，則可以更新 vSphere Native Key Provider 並為使用該金鑰提供者加密的虛擬機器重設金鑰。必須使用 PowerCLI 更新 vSphere Native Key Provider。此外，也可以在不更新金鑰提供者的情況下為已經加密的虛擬機器重設金鑰。在這種情況下，僅更改虛擬機器金鑰。若要為虛擬機器重設金鑰，請參閱[使用 vSphere Client 對加密虛擬機器進行重設金鑰](#)。

必要條件

- 所需權限：[密碼編譯作業.管理金鑰伺服器](#)
- PowerCLI 12.3.0

程序

- 1 在 PowerCLI 工作階段中，執行 `Connect-VIServer` cmdlet 以管理員使用者身分連線到設定了要更新的 vSphere Native Key Provider 的 vCenter Server。

```
Connect-VIServer -server VC_ip_address -User admin_user -Password 'password'
```

- 2 若要取得 vSphere Native Key Provider 名稱，請使用可選的 `Type` 參數執行 `Get-KeyProvider` cmdlet。

```
Get-KeyProvider -Type NativeKeyProvider
```

- 3 若要更新金鑰提供者，請在指定金鑰提供者名稱和 GUID 的情況下執行 `Set-KeyProvider` cmdlet。可以透過執行 `New-Guid` cmdlet 產生要使用的 GUID。

```
Set-KeyProvider -KeyProvider KeyProvider_name -KeyId Guid
```

此時將顯示一則有關備份組態的警告。

- 4 若要備份金鑰提供者，請執行 `Export-KeyProvider` cmdlet。

```
Export-KeyProvider -KeyProvider KeyProvider_name -FilePath path_file_name
```

還可以使用 vSphere Client 備份金鑰提供者。請參閱[備份 vSphere Native Key Provider](#)。

結果

更新金鑰提供者後，其狀態將變更為 [未備份]。備份金鑰提供者後，其狀態將更改為 [作用中]。

刪除 vSphere Native Key Provider

可以使用 vSphere Client 從 vCenter Server 中刪除 vSphere Native Key Provider。

刪除 vSphere Native Key Provider 後，具有 vTPM 的虛擬機器或已加密的虛擬機器會繼續執行。如果將 ESXi 主機重新開機，其加密虛擬機器會進入鎖定狀態。將這些虛擬機器解除登錄後，如果您嘗試重新登錄，則這些虛擬機器會進入鎖定狀態。將虛擬機器解除鎖定的唯一方式是還原先前的 vSphere Native Key Provider。

必要條件

所需權限：**密碼編譯作業.管理金鑰伺服器**

刪除 vSphere Native Key Provider 之前，將使用該金鑰提供者加密的任何加密虛擬機器和資料存放區重設金鑰至其他金鑰提供者。請參閱[使用 vSphere Client 對加密虛擬機器進行重設金鑰](#)。

此外，保留 vSphere Native Key Provider 的備份，以防您在刪除金鑰提供者後必須將加密的虛擬機器重設金鑰。

程序

- 1 使用 vSphere Client 登入 vCenter Server 系統。
- 2 瀏覽詳細目錄清單，並選取 vCenter Server 執行個體。
- 3 按一下**設定**，然後按一下**安全性下的金鑰提供者**。
- 4 選取要刪除的金鑰提供者。
- 5 按一下**刪除**。
- 6 閱讀警告訊息，然後將滑桿一直向右滑動。
- 7 按一下**刪除**。

結果

vSphere Native Key Provider 隨即從 vCenter Server 中移除。

vSphere Trust Authority

9

在 vSphere 7.0 及更新版本中，您可以利用 VMware® vSphere Trust Authority™。vSphere Trust Authority 是一項可增強工作負載安全性的基礎技術。vSphere Trust Authority 透過將 ESXi 主機的硬體信任根關聯至工作負載本身，以在您的組織中建立更高的信任層級。

本章節討論下列主題：

- [vSphere Trust Authority 概念和功能](#)
- [設定 vSphere Trust Authority](#)
- [在 vSphere 環境中管理 vSphere Trust Authority](#)

vSphere Trust Authority 概念和功能

vSphere Trust Authority 將受信任運算基礎的可信度延伸到您組織的整個運算基礎結構，從而保護 SDDC 抵禦惡意攻擊。vSphere Trust Authority 使用遠端證明和對進階密碼編譯功能的控制存取權。

vSphere Trust Authority 是一組滿足高安全性需求的服務。透過 vSphere Trust Authority，您可以設定並維護一個安全的基礎結構。您可以確保敏感工作負載僅在已證明啟動了正版軟體的 ESXi 主機上執行。

vSphere Trust Authority 如何保護環境

您可以設定 vSphere Trust Authority 服務來證明 ESXi 主機，如此便能夠執行信任的密碼編譯作業。

vSphere Trust Authority 針對 ESXi 主機使用遠端證明，以證明其開機軟體的真確性。證明將驗證 ESXi 主機正在執行可靠的 VMware 軟體，還是 VMware 簽署的合作夥伴軟體。證明依賴於在 ESXi 主機中安裝的信賴平台模組 (TPM) 2.0 晶片中的度量。在 vSphere Trust Authority 中，ESXi 只能在證明後存取加密金鑰並僅執行密碼編譯作業。

vSphere Trust Authority 詞彙

vSphere Trust Authority 介紹對於理解非常重要的特定詞彙和定義。

表 9-1. vSphere Trust Authority 詞彙

詞彙	定義
VMware vSphere® Trust Authority™	指定一組可啟用受信任基礎結構的服務。它負責確保 ESXi 主機執行的是受信任的軟體，並且僅向受信任的 ESXi 主機發佈加密金鑰。
vSphere Trust Authority 元件	vSphere Trust Authority 元件包括： <ul style="list-style-type: none"> ■ 證明服務 ■ 金鑰提供者服務
證明服務	證明遠端 ESXi 主機的狀態。使用 TPM 2.0 建立硬體信任根，並對照管理員核准的 ESXi 版本清單驗證軟體度量。
金鑰提供者服務	封裝一或多個金鑰伺服器，並公開加密虛擬機器時可指定的受信任金鑰提供者。目前，金鑰伺服器僅限於 KMIP 通訊協定。
受信任的基礎結構	受信任的基礎結構包括： <ul style="list-style-type: none"> ■ Trust Authority vCenter Server ■ 工作負載 vCenter Server ■ 至少一個 vSphere Trust Authority 叢集 (設定為 Trust Authority vCenter Server 的一部分) ■ 至少一個受信任叢集 (設定為工作負載 vCenter Server 的一部分) ■ 在受信任叢集中執行的加密工作負載虛擬機器 ■ 至少一個符合 KMIP 的金鑰管理伺服器 <p>備註 您必須針對 Trust Authority 叢集和受信任叢集使用不同的 vCenter Server 系統。</p>
Trust Authority 叢集	由執行 vSphere Trust Authority 元件 (證明服務和金鑰提供者服務) 之 ESXi 主機的 vCenter Server 叢集組成。
Trust Authority 主機	執行 vSphere Trust Authority 元件 (證明服務和金鑰提供者服務) 的 ESXi 主機。
受信任叢集	由 Trust Authority 叢集遠端證明的受信任 ESXi 主機的 vCenter Server 叢集組成。雖然不是嚴格要求，但設定的金鑰提供者服務可以大大增加受信任叢集所提供的價值。
受信任主機	其軟體已由 Trust Authority 叢集證明服務驗證的 ESXi 主機。此主機會執行工作負載虛擬機器，這些虛擬機器可使用 Trust Authority 叢集金鑰提供者服務發佈的金鑰提供者進行加密。
vSphere 虛擬機器加密	透過 vSphere 虛擬機器加密，您可以建立加密的虛擬機器並加密現有虛擬機器。vSphere 6.5 中引入了 vSphere 虛擬機器加密。如需瞭解金鑰提供者處理加密金鑰的方式差異，請參閱 vSphere 加密金鑰和金鑰提供者 。
受信任金鑰提供者	在金鑰伺服器上封裝單一加密金鑰的金鑰提供者。存取加密金鑰需要證明服務確認已在受信任的主機上驗證 ESXi 軟體。
標準金鑰提供者	可直接從金鑰伺服器取得加密金鑰，並將金鑰散佈到資料中心內的所需主機的金鑰提供者。先前在 vSphere 中稱為 KMS 叢集。
金鑰伺服器	與金鑰提供者相關聯的 KMIP 金鑰管理伺服器 (KMS)。
工作負載 vCenter Server	負責管理並用於設定一或多個受信任叢集的 vCenter Server。

vSphere Trust Authority 基礎

藉由 vSphere Trust Authority，您可以：

- 為 ESXi 主機提供硬體信任根及遠端證明功能

- 透過僅向已證明的 ESXi 主機發佈金鑰來限制加密金鑰管理
- 建立更安全的管理環境以管理信任
- 集中管理多個金鑰伺服器
- 繼續在虛擬機器上執行密碼編譯作業，但具有增強的加密金鑰管理層級

在 vSphere 6.5 和 6.7 中，虛擬機器加密相依於 vCenter Server 從金鑰伺服器取得加密金鑰，並視需要將其推送至 ESXi 主機。vCenter Server 使用用戶端和伺服器憑證 (儲存在 VMware Endpoint 憑證存放區 (VECS) 中) 向金鑰伺服器進行驗證。從金鑰伺服器傳送的加密金鑰會透過 vCenter Server 記憶體傳送至所需的 ESXi 主機 (TLS 透過連線提供資料加密)。此外，vSphere 還依賴 vCenter Server 中的權限檢查以驗證使用者權限並強制執行金鑰伺服器存取限制。雖然此架構是安全的，但無法解決出現遭破解的 vCenter Server、惡意 vCenter Server 管理員，或可能會導致密碼洩露或遭竊的管理或設定錯誤的可能性。

從 vSphere 7.0 開始，vSphere Trust Authority 解決了這些問題。您可以建立受信任的運算基礎，其中包含一組安全、可管理的 ESXi 主機。vSphere Trust Authority 針對您要信任的 ESXi 主機執行遠端證明服務。此外，vSphere Trust Authority 會在 TPM 2.0 證明支援 (從 6.7 版開始新增至 vSphere) 的情況下改進，以對加密金鑰執行存取限制，以便更好地保護虛擬機器工作負載密碼。此外，vSphere Trust Authority 僅允許授權的 Trust Authority 管理員設定 vSphere Trust Authority 服務以及設定 Trust Authority 主機。Trust Authority 管理員可以是與 vSphere 管理員使用者相同的使用者，也可以是不同的使用者。

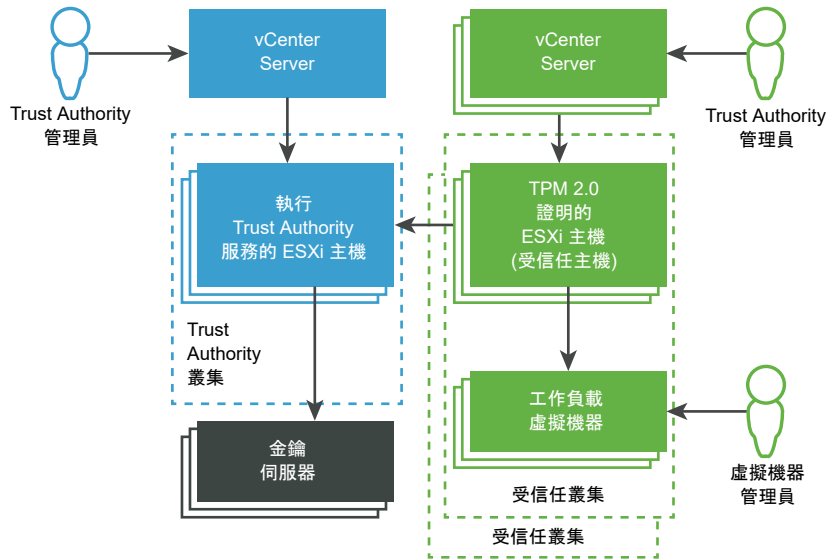
最後，vSphere Trust Authority 可讓您透過以下方式在更安全的環境中執行工作負載：

- 偵測竄改
- 禁止未經授權的變更
- 防止惡意軟體和修改
- 限制敏感工作負載僅在已驗證、安全的硬體和軟體堆疊上執行

vSphere Trust Authority 架構

下圖顯示 vSphere Trust Authority 架構的簡化視圖。

圖 9-1. vSphere Trust Authority 架構



在此圖中：

1 vCenter Server 系統

由不同的 vCenter Server 系統管理 Trust Authority 叢集和受信任叢集。

2 Trust Authority 叢集

由執行 vSphere Trust Authority 元件的 ESXi 主機所組成。

3 金鑰伺服器

在執行加密作業時，儲存金鑰提供者服務所使用的加密金鑰。主要伺服器位於 vSphere Trust Authority 的外部。

4 受信任叢集

由 ESXi 受信任主機組成，這些主機已透過 TPM 進行遠端證明，並且執行加密的工作負載。

5 Trust Authority 管理員

屬於 vCenter Server TrustedAdmins 群組成員的管理員，負責設定受信任的基礎結構。

vSphere Trust Authority 可讓您靈活地選擇指定 Trust Authority 管理員的方式。圖中的 Trust Authority 管理員可以是不同的使用者。此外，Trust Authority 管理員也可以是同一個使用者（使用跨 vCenter Server 系統連結的認證）。在此情況下，是同一個使用者和同一個 TrustedAdmins 群組。

6 虛擬機器管理員

已被授與在受信任主機上管理加密工作負載虛擬機器的權限的管理員。

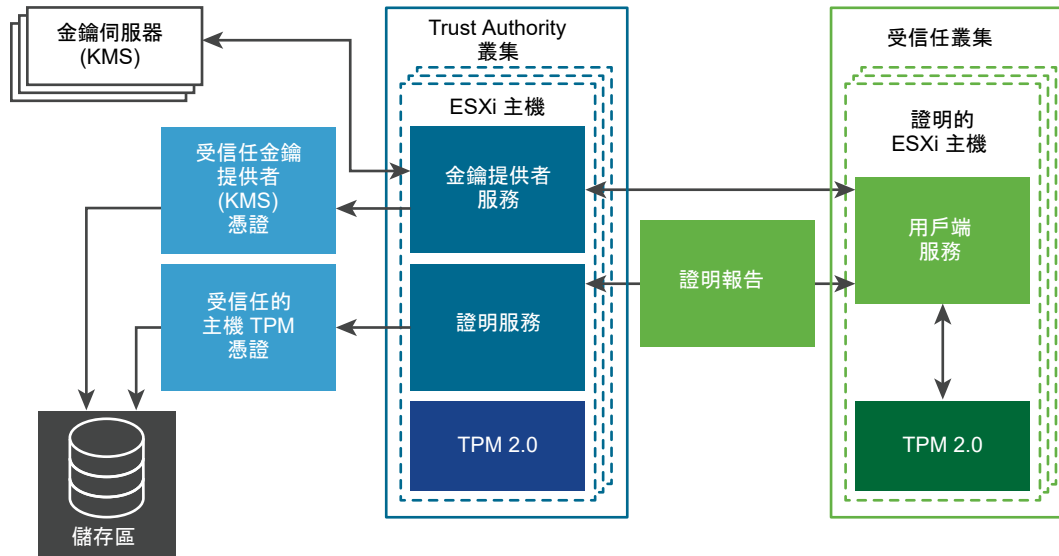
受信任基礎結構概觀

以下內容構成了受信任基礎結構：vSphere Trust Authority 服務、至少一個符合 KMIP 的外部金鑰伺服器、vCenter Server 系統和您的 ESXi 主機。

什麼是受信任基礎結構

受信任基礎結構包含至少一個 vSphere Trust Authority 叢集、至少一個受信任叢集，以及至少一個符合 KMIP 的外部金鑰伺服器。每個叢集包含執行特定 vSphere Trust Authority 服務的 ESXi 主機，如下圖所示。

圖 9-2. vSphere Trust Authority 服務



設定 Trust Authority 叢集可啟用兩項服務：

- 證明服務
- 金鑰提供者服務

當您設定 vSphere Trust Authority 時，受信任叢集中的 ESXi 主機會與證明服務進行通訊。金鑰提供者服務介於受信任主機與一或多個受信任金鑰提供者之間。

備註 目前，Trust Authority 叢集中的 ESXi 主機不需要 TPM。但是，最佳做法是考慮安裝帶有 TPM 的全新 ESXi 主機。

什麼是 vSphere Trust Authority 證明服務

證明服務會產生一個已簽署的文件，其中包含說明了受信任叢集中遠端 ESXi 主機的二進位和組態狀態的判斷提示。證明服務會使用信賴平台模組 (TPM) 2.0 晶片做為軟體測量和報告的基礎，以證明 ESXi 主機的狀態。遠端 ESXi 主機上的 TPM 會測量軟體堆疊，並將組態資料傳送到證明服務。證明服務會驗證軟體測量簽章是否可歸於先前設定的受信任 TPM 簽署金鑰 (EK)。證明服務也可確保軟體測量與一組先前賦予的 ESXi 映像中的其中一個相符。證明服務會簽署向 ESXi 主機發出的 JSON Web Token (JWT)，以提供有關 ESXi 主機的身分識別、有效性和組態的判斷提示。

什麼是 vSphere Trust Authority 金鑰提供者服務

透過金鑰提供者服務，vCenter Server 和 ESXi 主機不再需要直接金鑰伺服器認證。在 vSphere Trust Authority 中，若要讓 ESXi 主機具有加密金鑰的存取權，必須透過金鑰提供者服務進行驗證。

若要讓金鑰提供者服務連線到金鑰伺服器，Trust Authority 管理員必須進行信任設定。對於大多數符合 KMIP 的伺服器，信任設定涉及用戶端和伺服器憑證設定。

為了確保金鑰僅發行到 ESXi 受信任主機，金鑰提供者服務將充當金鑰伺服器的閘道管理員。金鑰提供者服務使用受信任金鑰提供者概念，對其餘資料中心軟體堆疊隱藏金鑰伺服器的特性。每個受信任的金鑰提供者都有一個已設定的主要加密金鑰，並參考一或多個金鑰伺服器。金鑰提供者服務可以有多個已設定的受信任金鑰提供者。例如，您可能想要針對組織中的每個部門設定單獨的受信任金鑰提供者。每個受信任的金鑰提供者使用不同的主要金鑰，但可以參考同一個支援金鑰伺服器。

建立受信任金鑰提供者後，金鑰提供者服務可接受來自 ESXi 受信任主機的申請，以針對該受信任金鑰提供者執行密碼編譯作業。

當 ESXi 受信任主機對受信任金鑰提供者申請作業時，金鑰提供者服務會確定嘗試取得加密金鑰的 ESXi 主機已經過證明。通過所有檢查後，ESXi 受信任主機從金鑰提供者服務收到加密金鑰。

vSphere Trust Authority 使用哪些連接埠

vSphere Trust Authority 服務接聽 ESXi 主機反向 Proxy 後方的連線。所有通訊都在連接埠 443 上透過 HTTPS 進行。

什麼是 vSphere Trust Authority 受信任主機

ESXi 受信任主機設定為使用受信任金鑰提供者來執行密碼編譯作業。ESXi 受信任主機透過與金鑰提供者服務和證明服務進行通訊來執行金鑰作業。若要進行驗證和授權，ESXi 受信任主機會使用從證明服務取得的 Token。若要取得有效的 Token，ESXi 受信任主機必須成功地向證明服務進行證明。Token 包含特定的宣告，用於決定 ESXi 受信任主機是否有權存取受信任金鑰提供者。

vSphere Trust Authority 和金鑰伺服器需求

vSphere Trust Authority 需要使用至少一個金鑰伺服器。在舊版 vSphere 中，金鑰伺服器稱為金鑰管理伺服器或 KMS。目前，vSphere 虛擬機器加密支援符合 KMIP 1.1 的金鑰伺服器。

vSphere Trust Authority 如何儲存組態和狀態資訊

vCenter Server 通常是用於 vSphere Trust Authority 組態和狀態資訊的傳遞服務。大多數 vSphere Trust Authority 組態和狀態資訊會儲存在 ConfigStore 資料庫中的 ESXi 主機上。某些狀態資訊也會儲存在 vCenter Server 資料庫中。

備註 由於大多數 vSphere Trust Authority 組態資訊儲存在 ESXi 主機上，因此，vCenter Server 以檔案為基礎的備份機制不會備份此資訊。若要確保已儲存 vSphere Trust Authority 部署的組態資訊，請參閱 [備份 vSphere Trust Authority 組態](#)。

vSphere Trust Authority 如何與 vCenter Server 整合

您可以設定單獨的 vCenter Server 執行個體，以管理 Trust Authority 叢集和受信任叢集。請參閱 [設定 vSphere Trust Authority](#)。

在受信任叢集中，vCenter Server 會管理 Trust Authority API 呼叫，並將其傳遞至 ESXi 主機。vCenter Server 將在受信任叢集中的所有 ESXi 主機之間複寫 API 呼叫。

最初設定 vSphere Trust Authority 之後，可以在 Trust Authority 叢集或受信任叢集中新增或移除 ESXi 主機。請參閱[新增和移除 vSphere Trust Authority 主機](#)。

vSphere Trust Authority 程序流程

瞭解 vSphere Trust Authority 程序流程對於學習如何設定和管理受信任基礎結構至關重要。

如何設定 vSphere Trust Authority？

依預設，不會啟用 vSphere Trust Authority。必須在環境中手動設定 vSphere Trust Authority。請參閱[設定 vSphere Trust Authority](#)。

設定 vSphere Trust Authority 時，您必須指定證明服務接受的 ESXi 軟體版本，以及哪些信賴平台模組 (TPM) 值得信任。

TPM 和證明

本指南在討論 TPM 和證明時使用下列定義。

表 9-2. TPM 和證明詞彙表

詞彙	定義
簽署金鑰 (EK)	TPM 使用內置於硬體的 RSA 公開/私密金鑰配對 (稱為簽署金鑰 (EK)) 進行製造。EK 對於特定 TPM 是唯一的。
EK 公開金鑰	EK 金鑰配對的公開部分。
EK 私密金鑰	EK 金鑰配對的私密部分。
EK 憑證	用簽章封裝的 EK 公開金鑰。EK 憑證是由使用其憑證授權機構私密金鑰簽署 EK 公開金鑰的 TPM 製造商所建立。並非所有 TPM 都包含 EK 憑證。在此情況下，不會簽署 EK 公開金鑰。
TPM 證明	證明服務驗證在遠端主機上所執行軟體的能力。TPM 證明透過 TPM 在遠端主機啟動時所進行的密碼編譯度量完成，並根據要求轉送至證明服務。證明服務透過 EK 公開金鑰或 EK 憑證在 TPM 中建立信任。

在受信任主機上設定 TPM 信任

ESXi 受信任主機必須包含 TPM。TPM 使用內置於硬體的公開/私密金鑰配對 (稱為簽署金鑰 (EK)) 進行製造。雖然 TPM 2.0 允許使用許多金鑰/憑證配對，但最常見的是 RSA-2048 金鑰配對。當 TPM EK 公開金鑰由 CA 簽署時，會產生 EK 憑證。TPM 製造商通常會預先產生至少一個 EK，使用憑證授權機構簽署公開金鑰，並將簽署的憑證嵌入 TPM 的非揮發性記憶體中。

您可以將證明服務設定為信任 TPM，如下所示：

- 信任製造商用來簽署 TPM 的所有 CA 憑證 (EK 公開金鑰)。證明服務的預設設定為信任 CA 憑證。在此方法中，相同的 CA 憑證涵蓋許多 ESXi 主機，因此可降低管理額外負荷。
- 信任 ESXi 主機的 TPM CA 憑證和 EK 公開金鑰。後者可以是 EK 憑證或 EK 公開金鑰。雖然此方法可提供更高安全性，但需要您設定每個受信任主機的相關資訊。
- 某些 TPM 不包含 EK 憑證。在此情況下，信任 EK 公開金鑰。

決定信任所有 TPM CA 憑證在操作上較為方便。僅當您將新的硬體類別新增至資料中心時，才需要設定新憑證。透過信任個別 EK 憑證，您可以限制對特定 ESXi 主機的存取權。

也可以決定不信任 TPM CA 憑證。儘管此情況不常見，但是當 CA 未簽署 EK 時可使用此組態。目前未完全實現此功能。

備註 某些 TPM 不包含 EK 憑證。如果您想要信任個別 ESXi 主機，TPM 必須包含 EK 憑證。

證明 TPM

受信任叢集中的 ESXi 受信任主機會將預先設定的 EK 公開金鑰和 EK 憑證傳送至 Trust Authority 叢集上的證明服務，以開始證明程序。當證明服務收到要求時，會查詢其組態中的 EK，它可能是 EK 公開金鑰或 EK 憑證，或兩者（視組態而定）。如果任何情況都無效，證明服務會拒絕證明申請。

EK 不直接用於簽署，因此會交涉證明金鑰 (AK 或 AIK)。交涉通訊協定可確保新建立的 AK 繫結到先前已驗證的 EK，從而防止發生攔截情況或假冒情況。交涉 AK 後，它會在未來的證明申請中重複使用，而不是每次都產生一個新 AK。

ESXi 受信任主機會從 TPM 讀取引用和 PCR 值。此引用由 AK 簽署。ESXi 受信任主機也會讀取 TCG 事件記錄，其中包括導致目前 PCR 狀態的所有事件。此 TPM 資訊將會傳送至證明服務以進行驗證。證明服務會使用事件記錄來驗證 PCR 值。

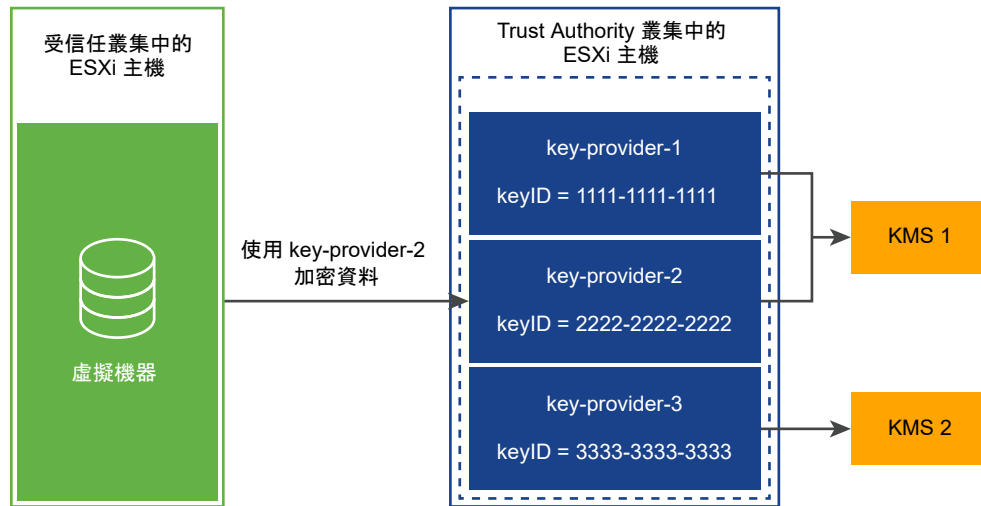
金鑰提供者如何使用金鑰伺服器？

金鑰提供者服務使用受信任金鑰提供者的概念，對其餘資料中心軟體隱藏金鑰伺服器的特性。每個受信任的金鑰提供者都有一個已設定的主要加密金鑰，並參考一或多個金鑰伺服器。主要加密金鑰存在於金鑰伺服器中。在設定 vSphere Trust Authority 的過程中，必須將主要金鑰佈建為單獨的活動，然後將其啟用。金鑰提供者服務可以有多个已設定的受信任金鑰提供者。每個受信任的金鑰提供者使用不同的主要金鑰，但可以參考同一個支援金鑰伺服器。

新增受信任金鑰提供者後，Trust Authority 管理員必須在該金鑰伺服器上指定金鑰伺服器和現有的金鑰識別碼。

下圖顯示了金鑰提供者服務與金鑰伺服器之間的關係。

圖 9-3. 金鑰提供者和金鑰伺服器



為受信任的叢集設定受信任金鑰提供者後，金鑰提供者服務可接受針對該受信任金鑰提供者執行密碼編譯作業的要求。例如，在此圖中，設定了三個受信任的金鑰提供者，兩個用於 KMS-1，一個用於 KMS-2。受信任主機針對 key-provider-2 申請加密作業。受信任主機要求產生並傳回加密金鑰，並使用此加密金鑰執行加密作業。

金鑰提供者服務使用 key-provider-2 所引用的主要金鑰，以加密指定的純文字資料並傳回對應的加密文字。稍後，受信任主機可以為解密作業提供相同的加密文字，並取回原始純文字。

vSphere Trust Authority 驗證和授權

vSphere Trust Authority 管理作業需要屬於 TrustedAdmins 群組成員的使用者。僅擁有 Trust Authority 管理員權限不足以執行涉及 ESXi 主機的所有管理作業。如需詳細資訊，請參閱 [vSphere Trust Authority 的必要條件和必要權限](#)。

將受信任主機新增至受信任叢集

[設定 vSphere Trust Authority](#) 中說明了一開始將 ESXi 主機新增至受信任叢集的步驟。

稍後，如果要將 ESXi 主機新增至受信任叢集，則工作流程會有所不同。請參閱 [新增和移除 vSphere Trust Authority 主機](#)。

一開始將 ESXi 主機新增至受信任叢集時，您必須收集下列資訊：

- 叢集中每種硬體類型的 TPM 憑證
- 叢集中每個 ESXi 版本的 ESXi 映像
- vCenter Server 主體資訊

如果稍後將 ESXi 主機新增至受信任叢集，則可能需要收集一些其他資訊。也就是說，如果新 ESXi 主機的硬體或 ESXi 版本與原始主機不同，則必須收集新的 ESXi 主機資訊並將其匯入至 Trust Authority 叢集。每個 vCenter Server 系統只需收集一次 vCenter Server 主體資訊。

vSphere Trust Authority 拓撲

vSphere Trust Authority 需要將不同的 vCenter Server 系統用於 Trust Authority 叢集和受信任叢集。

Trust Authority 叢集在獨立、隔離的 vCenter Server 上進行設定和管理。Trust Authority 叢集的 vCenter Server 也不能是受信任叢集的 vCenter Server。受信任叢集必須擁有其自己的獨立 vCenter Server。單一 vCenter Server 可管理多個受信任的叢集。受信任叢集的多個 vCenter Server 系統可加入增強型連結模式。Trust Authority 叢集的 vCenter Server 不能與其他 Trust Authority 叢集 vCenter Server 系統或受信任叢集 vCenter Server 系統一起加入增強型連結模式。

Trust Authority 管理員將 Trust Authority 叢集及其相關聯的 vCenter Server 與其他 vCenter Server 執行個體單獨進行管理，因為這種方法可提供最佳的安全性隔離。

Trust Authority 管理員可記錄或發佈受信任叢集管理員用來設定其叢集的主機名稱和 SSL 憑證。此外，Trust Authority 管理員還會為組織及其部門或甚至個別管理員佈建受信任金鑰提供者。

無法直接在工作負載 vCenter Server 所管理的受信任叢集上部署 vSphere Trust Authority 服務，因為工作負載管理員擁有 ESXi 主機的高權限存取權。此類型的部署無法實現滿足 vSphere Trust Authority 安全性目標所需的必要角色分離。

vSphere Trust Authority 的必要條件和必要權限

設定 vSphere Trust Authority 時，必須考慮硬體和軟體需求。您必須設定密碼編譯權限和角色才能使用加密。執行 vSphere Trust Authority 工作的使用者必須擁有適當的權限。

vSphere Trust Authority 的需求

若要使用 vSphere Trust Authority，您的 vSphere 環境必須符合下列需求：

- ESXi 受信任主機的硬體需求：
 - TPM 2.0
 - 必須啟用安全開機
 - EFI 韌體
- 元件需求：
 - vCenter Server 7.0 或更新版本
 - 專用於 vSphere Trust Authority 叢集和 ESXi 主機的 vCenter Server 系統
 - 單獨用於受信任叢集和 ESXi 受信任叢集的 vCenter Server 系統
 - 金鑰伺服器 (在先前的 vSphere 版本中稱為金鑰管理伺服器或 KMS)
- 虛擬機器需求：
 - EFI 韌體
 - 已啟用安全開機

備註 開始設定 vSphere Trust Authority 之前，請先確定您為 Trust Authority 叢集和受信任叢集設定了 vCenter Server 系統，並將 ESXi 主機新增到每個叢集。

vSphere Trust Authority 和密碼編譯權限

vSphere Trust Authority 不會引入任何新的密碼編譯權限。[使用密碼編譯權限和角色](#)中所述的相同密碼編譯權限適用於 vSphere Trust Authority。

vSphere Trust Authority 和主機加密模式

vSphere Trust Authority 不會引入在 ESXi 受信任主機上啟用主機加密模式的任何新需求。如需有關主機加密模式的詳細資訊，請參閱[虛擬機器加密工作的必要條件和所需權限](#)。

使用 vSphere Trust Authority 角色和 TrustedAdmins 群組

vSphere Trust Authority 作業需要屬於 TrustedAdmins 群組成員的使用者。此使用者稱為 Trust Authority 管理員。vSphere 管理員必須將自己新增至 TrustedAdmins 群組，或將其他使用者新增至群組，以取得「受信任基礎結構管理員」角色。vCenter Server 授權需要「受信任基礎結構管理員」角色。在做為受信任基礎結構一部分的 ESXi 主機上進行驗證時，需要 TrustedAdmins 群組。在 ESXi 主機上具有密碼編譯作業、登錄主機權限的使用者可以管理受信任的叢集。vCenter Server 不會散佈至 Trust Authority 主機，而是僅散佈至受信任的主機。僅 TrustedAdmins 群組的成員會被授與 Trust Authority 主機的權限。群組成員資格會在 ESXi 主機本身上進行驗證。

備註 vSphere 管理員和管理員群組的成員會指派有「受信任基礎結構管理員」角色，但此角色本身不允許使用者執行 vSphere Trust Authority 作業。此外，還需要 TrustedAdmins 群組中的成員資格。

啟用 vSphere Trust Authority 後，Trust Authority 管理員可將受信任的金鑰提供者指派給受信任主機。然後，這些受信任的主機可以使用受信任的金鑰提供者來執行密碼編譯工作。

除了「受信任基礎結構管理員」角色之外，vSphere Trust Authority 還提供「無受信任基礎結構管理員」角色，該角色包含 vCenter Server 中的所有權限，但呼叫 vSphere Trust Authority API 的權限除外。

vSphere Trust Authority 群組、角色和使用者的運作方式如下：

- 首次開機時，vSphere 授與 TrustedAdmins 群組具有全域權限的「受信任基礎結構管理員」角色。
- 「受信任基礎結構管理員」角色是一種系統角色，具有呼叫 vSphere Trust Authority API (`TrustedAdmin.*`) 所需的權限，以及用於檢視詳細目錄物件的系統權限 **System.Read**、**System.View** 和 **System.Anonymous**。
- 「無受信任基礎結構管理員」角色是一種包含 vCenter Server 中所有權限 (除了呼叫 vSphere Trust Authority API 的權限以外) 的系統角色。將新權限新增至 vCenter Server 也會將其新增至「無受信任基礎結構管理員」角色。(「無受信任基礎結構管理員」角色類似於「無密碼編譯管理員」角色)。
- vSphere Trust Authority 權限 (`TrustedAdmin.*` API) 不包括在「無密碼編譯管理員」角色中，會防止具有此角色的使用者設定受信任基礎結構或執行密碼編譯作業。

這些使用者、群組和角色的使用案例如下表所示。

表 9-3. vSphere Trust Authority 使用者、群組和角色

使用者、群組或角色	可以呼叫 vSphere Trust Authority vCenter Server API (包括對 vSphere Trust Authority ESXi API 的呼叫)	可以呼叫 vSphere Trust Authority vCenter Server API (不包括對 vSphere Trust Authority ESXi API 的呼叫)	可在不與 vSphere Trust Authority 相關的叢集中執行主機作業	註解
同時在 Administrators@system.domain 群組和 TrustedAdmins@system.domain 群組中的使用者	是	是	是	NA
僅在 TrustedAdmins@system.domain 群組中的使用者	是	是	否	此類使用者無法執行定期叢集管理作業。
僅在 Administrators@system.domain 群組中的使用者	是	否	是	NA
具有「受信任基礎結構管理員」角色但不在 TrustedAdmins@system.domain 群組中的使用者	是	否	否	ESXi 主機會檢查使用者的群組成員資格以授與權限。
僅具有「無受信任基礎結構管理員」角色的使用者	否	否	是	此類使用者類似於無法執行 vSphere Trust Authority 作業的管理員。

vSphere Trust Authority 最佳做法、注意須知和互通性

vSphere Trust Authority 架構會產生一些其他建議。在您規劃 vSphere Trust Authority 策略時，請考慮互通性限制。

受信任基礎結構互通性

對於 ESXi 版本，證明服務會向後和向前相容。例如，可以在 vSphere Trust Authority 叢集中具有執行 ESXi 7.0 的 ESXi 主機的叢集，並將受信任叢集中的 ESXi 主機升級或修補至較新的 ESXi 版本。同樣地，您可以升級或修補 Trust Authority 叢集中的 ESXi 主機，同時將受信任叢集中的 ESXi 主機保持在目前版本。

不能讓某個叢集同時充當 Trust Authority 叢集和受信任叢集。此組態不受支援。

受信任叢集的組態限制

只能為每個工作負載 vCenter Server 設定一個受信任叢集。不能將受信任叢集設定為參考多個 Trust Authority 叢集。

支援的功能

vSphere Trust Authority 支援下列內容：

- vCenter High Availability (vCenter HA)
- VMware vSphere High Availability
- DRS
- DPM
- SRM，需瞭解以下幾點：
 - 如果在復原端有相同的 vSphere Trust Authority 服務組態，則支援使用陣列式複寫的 SRM。
 - SPPG
- VADP
 - 支援與標準加密相同。支援熱新增和 NFC 模式，但不支援 SAN 模式。備份已解密。VADP 合作夥伴可選擇使用與原始虛擬機器相同的加密金鑰來復原已備份的虛擬機器。
- vSAN
 - 在 vSAN 上完全支援虛擬機器加密。
- OVF
 - 無法將加密的虛擬機器匯出至 OVF。但是，從 OVF 匯入虛擬機器時，可以對其進行加密。
- vVol

不支援的功能

目前，vSphere Trust Authority 不支援下列內容：

- vSAN 加密
- 第一級磁碟 (FCD) 加密
- vSphere Replication
- vSphere 主機設定檔

vSphere Trust Authority 生命週期

vSphere Trust Authority 服務會做為基礎 ESXi 映像的一部分進行封裝和安裝。

啟動和停止 vSphere Trust Authority 服務

在 vSphere Client 中，您可以啟動、停止及重新啟動在 ESXi 主機上執行的 vSphere Trust Authority 服務。您可在組態變更時或出現可疑的運作或效能問題時重新啟動服務。若要重新啟動 ESXi 受信任主機上的服務，您必須登入主機本身以重新啟動服務。請參閱[啟動、停止和重新啟動 vSphere Trust Authority 服務](#)。

升級和修補 vSphere Trust Authority

每次升級或修補 ESXi 受信任主機時，必須以新的 ESXi 版本資訊來更新 vSphere Trust Authority 叢集。執行此操作的一種方法是升級或修補測試 ESXi 主機、匯出 ESXi 基礎映像資訊、將映像檔案匯入至 Trust Authority 叢集，然後升級或修補 ESXi 受信任主機。

vSphere Trust Authority 升級的最佳做法

升級 vSphere Trust Authority 基礎結構的最佳做法是先升級 Trust Authority vCenter Server 和 Trust Authority 主機。透過這種方式，您可以從最新的 vSphere Trust Authority 功能中獲得最大益處。但是，您可以對 vCenter Server 和 ESXi 主機執行個別的獨立升級，以符合特定的業務原因。

一般而言，請遵循此順序來升級您的 vSphere Trust Authority 基礎結構：

- 1 升級 Trust Authority 叢集 vCenter Server。
- 2 升級 Trust Authority 主機。
- 3 升級受信任叢集 vCenter Server。
- 4 升級受信任主機。

為確保程序順暢執行，請逐步升級 Trust Authority 主機和受信任主機，一次一個。

對 vSphere Trust Authority 升級問題進行疑難排解

如果 Trust Authority 主機升級出現失敗，請執行下列步驟。

- 1 從受信任叢集中移除 Trust Authority 主機。
- 2 還原為先前版本的 ESXi。
- 3 按照 VMware 知識庫文章 (網址為 <https://kb.vmware.com/s/article/77234>) 中所述，將 Trust Authority 主機重新新增至叢集。
- 4 確認 Trust Authority 主機的組態與 Trust Authority 叢集中的其他 Trust Authority 主機一致。請參閱 [檢查受信任叢集健全狀況](#)。

使用新的 ESXi 基礎映像資訊更新 Trust Authority 叢集之前，如果在受信任主機上升級到新版本的 ESXi，則證明會失敗。這是預期的行為。無法再加密虛擬機器或使用升級前已加密的現有虛擬機器，直到您修正問題為止。證明錯誤訊息會顯示在 vSphere Client **最近的工作**窗格以及 `attestd.log`、`kmsa.log` 和 `vpxd.log` 檔案中。

若要更正問題，請遵循下列步驟。

- 1 執行 `Export-VMHostImageDb cmdlet` 以重新匯出 ESXi 基礎映像。請參閱 [收集要信任的 ESXi 主機和 vCenter Server 的相關資訊](#) 中的步驟 5。
- 2 執行 `New-TrustAuthorityVMHostBaseImage cmdlet`，以將新的基礎映像重新匯入至 Trust Authority 叢集的 vCenter Server。請參閱 [將受信任主機資訊匯入至 Trust Authority 叢集](#) 中的步驟 8。

- 3 如果您不再需要證明較舊版本的 ESXi (已升級所有受信任的主機)，請執行 `Remove-TrustAuthorityVMHostBaseImage` cmdlet 以移除版本。例如：

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
$baseImages = Get-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
Remove-TrustAuthorityVMHostBaseImage -VMHostBaseImage $baseImages
```

備份 vSphere Trust Authority 組態

由於大多數 vSphere Trust Authority 組態資訊儲存在 ESXi 主機上，因此，vCenter Server 備份不會備份此 vSphere Trust Authority 資訊。請參閱[備份 vSphere Trust Authority 組態](#)。

設定 vSphere Trust Authority

依預設，不會啟用 vSphere Trust Authority。必須先設定 vSphere Trust Authority 的環境，然後才能開始使用。

請在專用的 vCenter Server 叢集 (稱為 vSphere Trust Authority 叢集) 上啟用 vSphere Trust Authority 服務。Trust Authority 叢集可充當集中式安全管理平台。然後，啟用工作負載 vCenter Server 叢集以做為受信任的叢集。受信任叢集包含 ESXi 受信任主機。

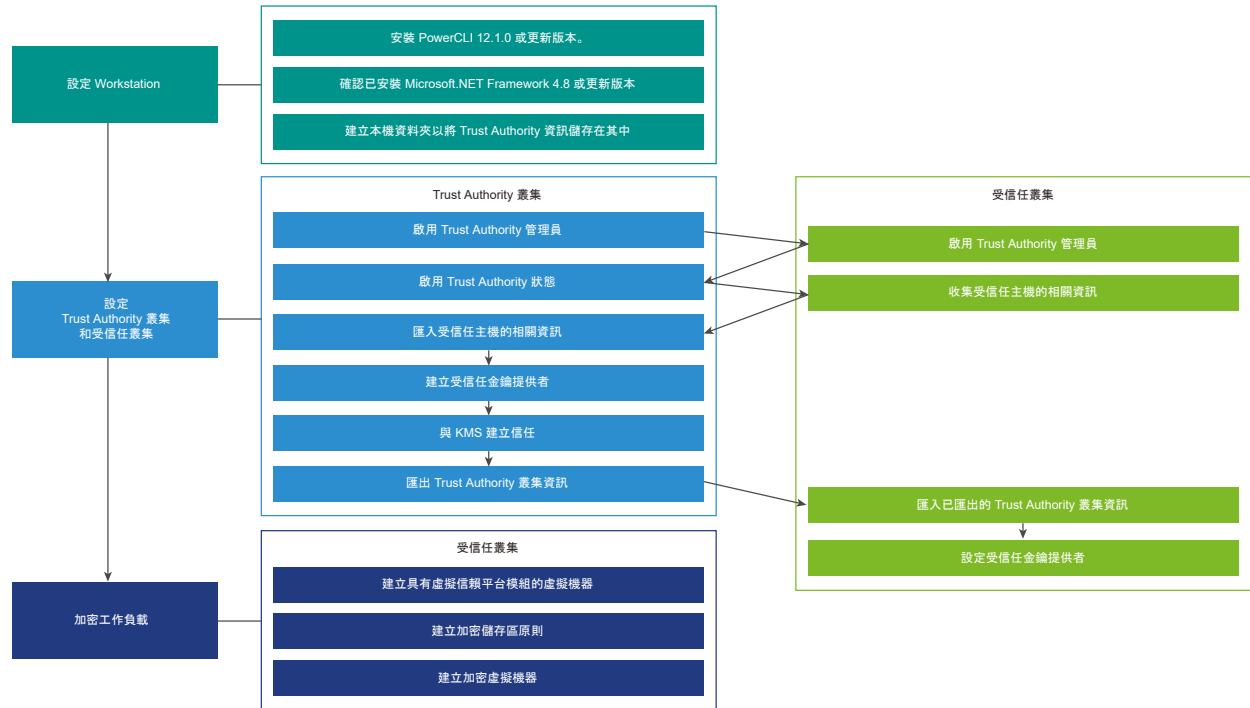
Trust Authority 叢集會從遠端證明受信任叢集中的 ESXi 主機。Trust Authority 叢集僅向受信任叢集中被證明的 ESXi 主機釋放加密金鑰，以使用受信任金鑰提供者加密虛擬機器和虛擬磁碟。

開始設定 vSphere Trust Authority 之前，請參閱[vSphere Trust Authority 的必要條件和必要權限](#)，以瞭解 vCenter Server 系統和 ESXi 主機所需設定的相關資訊。

可以使用下列方式管理 vSphere Trust Authority 的不同方面。

- 使用 PowerCLI cmdlet 或 vSphere API 設定 vSphere Trust Authority 服務和信任連線。請參閱《VMware PowerCLI Cmdlet 參考》和《vSphere Automation SDK 程式設計指南》。
- 使用 PowerCLI cmdlet 或從 vSphere Client 管理受信任金鑰提供者的組態。
- 使用 vSphere Client 和 API 執行加密工作流程，如同在先前 vSphere 版本中一樣。

圖 9-4. vSphere Trust Authority 工作流程



若要設定和管理 vSphere Trust Authority，可以使用 VMware PowerCLI，但是可以在 vSphere Client 中獲得某些功能。

當您設定 vSphere Trust Authority 時，必須在 Trust Authority 叢集和受信任叢集上完成設定工作。其中部分工作是特定於順序的。使用本指南中列出的工作順序。

備註 在完成初始 vSphere Trust Authority 設定後將更多 ESXi 主機新增至受信任叢集時，您可能需要再次匯出並匯入受信任主機資訊。也就是說，如果新 ESXi 主機與原始主機不同，則必須收集新的 ESXi 主機資訊並將其匯入至 Trust Authority 叢集。請參閱[新增和移除 vSphere Trust Authority 主機](#)。

程序

1 設定工作站以設定 vSphere Trust Authority

若要設定 vSphere Trust Authority 部署，必須先準備具有必要軟體和設定的工作站。

2 啟用 Trust Authority 管理員

若要啟用 vSphere Trust Authority，您必須將使用者新增至 vSphere TrustedAdmins 群組。此使用者將成為 Trust Authority 管理員。您可以使用 Trust Authority 管理員來執行大多數 vSphere Trust Authority 組態工作。

3 啟用 Trust Authority 狀態

將 vCenter Server 叢集變為 vSphere Trust Authority 叢集 (也稱為啟用 Trust Authority 狀態)，會在叢集中的 ESXi 主機上啟動所需的 Trust Authority 服務。

4 收集要信任的 ESXi 主機和 vCenter Server 的相關資訊

若要建立信任，vSphere Trust Authority 叢集需要有關受信任叢集的 ESXi 主機和 vCenter Server 的資訊。以檔案形式匯出此資訊，以匯入到 Trust Authority 叢集中。務必確保這些檔案的機密性並安全地進行傳輸。

5 將受信任主機資訊匯入至 Trust Authority 叢集

您可以將匯出的 ESXi 主機和 vCenter Server 資訊匯入 vSphere Trust Authority 叢集中，以便 Trust Authority 叢集知道它可以證明哪些主機。

6 在 Trust Authority 叢集上建立金鑰提供者

為了讓金鑰提供者服務連線到金鑰提供者，必須建立受信任金鑰提供者，然後在 vSphere Trust Authority 叢集與金鑰伺服器 (KMS) 之間進行信任設定。對於大多數符合 KMIP 的金鑰伺服器，此設定程序包括設定用戶端和伺服器憑證。

7 匯出 Trust Authority 叢集資訊

為了讓受信任叢集連線至 vSphere Trust Authority 叢集，您必須以檔案形式匯出 Trust Authority 叢集的服務資訊，然後將該檔案匯入至受信任叢集中。務必確保此檔案的機密性並安全地進行傳輸。

8 將 Trust Authority 叢集資訊匯入至受信任的主機

將 vSphere Trust Authority 叢集資訊匯入至受信任的叢集後，受信任主機會透過 Trust Authority 叢集啟動證明程序。

9 使用 vSphere Client 為受信任的主機設定受信任金鑰提供者

您可以使用 vSphere Client 設定受信任的金鑰提供者。

10 使用命令列為受信任的主機設定受信任金鑰提供者

您可以使用命令列設定受信任的金鑰提供者。可以為 vCenter Server 設定預設受信任金鑰提供者，或在 vCenter 物件階層中的叢集或叢集資料夾層級設定。

設定工作站以設定 vSphere Trust Authority

若要設定 vSphere Trust Authority 部署，必須先準備具有必要軟體和設定的工作站。

在有權存取 vSphere Trust Authority 環境的工作站上執行以下步驟。

程序

- 1 安裝 PowerCLI 12.1.0 或更新版本。請參閱《PowerCLI 使用者指南》。
- 2 確認已安裝 Microsoft .NET Framework 4.8 或更新版本。
- 3 建立本機資料夾，用於儲存以檔案形式匯出的 Trust Authority 資訊。

後續步驟

繼續啟用 Trust Authority 管理員。

啟用 Trust Authority 管理員

若要啟用 vSphere Trust Authority，您必須將使用者新增至 vSphere TrustedAdmins 群組。此使用者將成為 Trust Authority 管理員。您可以使用 Trust Authority 管理員來執行大多數 vSphere Trust Authority 組態工作。

使用 vCenter Server 管理員以外的其他使用者做為 Trust Authority 管理員。擁有單獨的使用者可增強環境的安全性。必須為 Trust Authority 叢集和受信任叢集同時啟用 Trust Authority 管理員。

必要條件

可以建立使用者或識別現有使用者，使其成為 Trust Authority 管理員。

程序

- 1 使用 vSphere Client 連線至 Trust Authority 叢集的 vCenter Server。
- 2 以管理員身分登入。
- 3 從首頁功能表中，選取**管理**。
- 4 在 **Single Sign On** 下，按一下**使用者和群組**。
- 5 按一下**群組**，然後按一下 **TrustedAdmins** 群組。

如果 TrustedAdmins 群組在一開始並未顯示，請使用**篩選器**圖示進行篩選，或按一下窗格底部的向右箭頭以瀏覽各個群組。

- 6 在**群組成員**區域中，按一下**新增成員**。

確保已選取本機身分識別來源 (vsphere.local 為預設值，但您可能在安裝期間選取了其他網域)，然後搜尋要新增至群組以做為 Trust Authority 管理員的成員 (使用者)。

- 7 選取成員。
- 8 按一下**儲存**。
- 9 針對受信任叢集的 vCenter Server 重複步驟 1 至 8。

後續步驟

繼續[啟用 Trust Authority 狀態](#)。

啟用 Trust Authority 狀態

將 vCenter Server 叢集變為 vSphere Trust Authority 叢集 (也稱為啟用 Trust Authority 狀態)，會在叢集中的 ESXi 主機上啟動所需的 Trust Authority 服務。

必要條件

- [啟用 Trust Authority 管理員](#)。

程序

- 1 在 PowerCLI 工作階段中，執行 `Connect-VIServercmdlet`，以 Trust Authority 管理員使用者身分連線至 Trust Authority 叢集的 vCenter Server。

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 2 若要檢查叢集的目前狀態，請執行 `Get-TrustAuthorityClustercmdlet`。

例如，此命令會顯示叢集、vTA Cluster，並顯示其狀態為 [已停用]。

```
Get-TrustAuthorityCluster

Name                State                Id
----                -
vTA Cluster         Disabled            TrustAuthorityCluster-domain-c8
```

在 [狀態] 資料行中，會針對找到的每個叢集顯示輸出為 [已停用] 或 [已啟用]。[已停用] 表示 Trust Authority 服務不在執行中。

- 3 若要啟用 Trust Authority 叢集，請執行 `Set-TrustAuthorityClustercmdlet`。

例如，此命令會啟用叢集 vTA Cluster。

```
Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA Cluster' -State Enabled
```

系統會用確認提示作出回應。

```
Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to
proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

- 4 出現確認提示時按 Enter。(預設值為 **y**。)

輸出會顯示叢集的狀態。例如，以下內容顯示叢集 vTA Cluster 已啟用：

```
Name                State                Id
----                -
vTA Cluster         Enabled            TrustAuthorityCluster-domain-c8
```

結果

將在 Trust Authority 叢集中的 ESXi 主機上啟動兩項服務：證明服務和金鑰提供者服務。

範例：在 Trust Authority 叢集上啟用受信任狀態

此範例顯示如何使用 PowerCLI 在 Trust Authority 叢集上啟用服務。下表顯示了所使用的範例元件和值。

表 9-4. vSphere Trust Authority 設定範例

元件	值
Trust Authority 叢集的 vCenter Server	192.168.210.22
Trust Authority 叢集名稱	vTA 叢集
Trust Authority 管理員	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                               Port  User
----                               -
192.168.210.22                     443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustAuthorityCluster

Name                State                Id
----                -
vTA Cluster         Disabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA
Cluster' -State Enabled

Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                State                Id
----                -
vTA Cluster         Enabled              TrustAuthorityCluster-domain-c8
```

後續步驟

繼續收集要信任的 ESXi 主機和 vCenter Server 的相關資訊。

收集要信任的 ESXi 主機和 vCenter Server 的相關資訊

若要建立信任，vSphere Trust Authority 叢集需要有關受信任叢集的 ESXi 主機和 vCenter Server 的資訊。以檔案形式匯出此資訊，以匯入到 Trust Authority 叢集中。務必確保這些檔案的機密性並安全地進行傳輸。

您可以使用 vSphere Trust AuthorityPowerCLI cmdlet，以檔案形式從受信任叢集中的 ESXi 主機匯出下列資訊，以便 Trust Authority 叢集瞭解要信任的軟體和硬體。

- ESXi 版本
- TPM 製造商 (CA 憑證)

- (選用) 個別 TPM (EK 憑證)

備註 將這些匯出的檔案儲存在安全的位置，以防您必須還原 vSphere Trust Authority 組態。

如果您主機的類型和廠商相同，並且該主機在相同的時間範圍和位置製造，則可以僅取得其中一個 TPM 的 CA 憑證來信任所有 TPM。若要信任個別 TPM，您需要取得該 TPM 的 EK 憑證。

同時，必須從受信任叢集的 vCenter Server 中取得主體資訊。主體資訊包含 vpxd 解決方案使用者及其憑證鏈結。憑藉主體資訊，受信任叢集的 vCenter Server 能夠探索在 Trust Authority 叢集上設定的可用受信任金鑰提供者。

若要一開始設定 vSphere Trust Authority，則必須收集 ESXi 版本和 TPM 資訊。此外，還必須在每次部署新版本的 ESXi 後 (包括升級或套用修補程式時) 收集 ESXi 版本。

每個 vCenter Server 系統僅收集一次 vCenter Server 主體資訊。

必要條件

- 識別受信任叢集中的 ESXi 版本和 TPM 硬體類型，以及您要信任所有 TPM 硬體類型、僅特定的 TPM 硬體類型還是個別主機。
- 在執行 PowerCLI cmdlet 的機器上，建立用於儲存以檔案形式匯出之資訊的本機資料夾。
- [啟用 Trust Authority 管理員](#)。
- [啟用 Trust Authority 狀態](#)。

程序

- 1 在 PowerCLI 工作階段中，執行下列命令，中斷任何目前連線並以根使用者身分連線至受信任叢集中的其中一個 ESXi 主機。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

- 2 執行 `Get-VMHost` cmdlet 以確認 ESXi 主機。

```
Get-VMHost
```

隨即顯示主機資訊。

- 3 將 `Get-VMHost` 指派給變數。

例如：

```
$vmhost = Get-VMHost
```


4 執行 Export-Tpm2CACertificatecmdlet 以匯出指定 TPM 製造商的 CA 憑證。

- a 將 Get-Tpm2EndorsementKey -VMHost \$vmhost 指派給變數。

例如，此命令會將 \$tpm2 指派給變數 Get-Tpm2EndorsementKey -VMHost \$vmhost。

```
$tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
```

- b 執行 Export-Tpm2CACertificatecmdlet。

例如，此命令會將 TPM 憑證匯出至 cacert.zip 檔案。請在執行此命令之前確認目的地目錄已存在。

```
Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip
```

隨即建立該檔案。

- c 針對您要信任的叢集中的每個 TPM 硬體類型重複以上操作。針對每個 TMP 硬體類型使用不同的檔案名稱，以便您不會覆寫先前匯出的檔案。

5 執行 Export-VMHostImageDbcmdlet，以匯出軟體的 ESXi 主機說明 (ESXi 映像)。

例如，此命令會將資訊匯出至 image.tgz 檔案。請在執行此命令之前確認目的地目錄已存在。

```
Export-VMHostImageDb -VMHost $vmhost -FilePath C:\vta\image.tgz
```

備註 如果您偏好登入受信任叢集的 vCenter Server，則 Export-VMHostImageDb cmdlet 也會起作用。

隨即建立該檔案。

針對您要信任的叢集中的每個 ESXi 版本重複以上操作。針對每個版本使用不同的檔案名稱，以便您不會覆寫先前匯出的檔案。

6 匯出受信任叢集的 vCenter Server 主體資訊。

- a 中斷與 ESXi 主機的連線。

```
Disconnect-VIServer -server * -Confirm:$false
```

- b 使用 Trust Authority 管理員使用者連線至受信任叢集的 vCenter Server。(也可以使用具有管理員權限的使用者。)

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'
```

- c 若要匯出受信任叢集的 vCenter Server 主體資訊，請執行 Export-TrustedPrincipal cmdlet。

例如，此命令會將資訊匯出至 principal.json 檔案。請在執行此命令之前確認目的地目錄已存在。

```
Export-TrustedPrincipal -FilePath C:\vta\principal.json
```

隨即建立該檔案。

7 (選擇性) 如果您想要信任個別主機，則必須匯出 TPM EK 公開金鑰憑證。

請參閱[匯出和匯入 TPM 簽署金鑰憑證](#)。

結果

將建立下列檔案：

- TPM CA 憑證檔案 (.zip 副檔名)
- ESXi 映像檔案 (.tgz 副檔名)
- vCenter Server 主體檔案 (json 副檔名)

範例：收集要信任的 ESXi 主機和 vCenter Server 的相關資訊

此範例顯示如何使用 PowerCLI 匯出 ESXi 主機資訊和 vCenter Server 主體。下表顯示了所使用的範例元件和值。

表 9-5. vSphere Trust Authority 設定範例

元件	值
受信任叢集中的 ESXi 主機	192.168.110.51
受信任叢集的 vCenter Server	192.168.110.22
變數 \$vmhost	Get-VMHost
變數 \$tpm2	Get-Tpm2EndorsementKey -VMHost \$vmhost

表 9-5. vSphere Trust Authority 設定範例 (續)

元件	值
Trust Authority 管理員	trustedadmin@vsphere.local
包含輸出檔案的本機目錄	C:\vta

```
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.51 -User root -Password 'VMware1!'
```

Name	Port	User
-----	----	----
192.168.110.51	443	root

```
PS C:\Users\Administrator.CORP> Get-VMHost
```

Name	ConnectionState	PowerState	NumCpu	CpuUsageMhz	CpuTotalMhz	MemoryUsageGB	MemoryTotalGB	Version
-----	-----	-----	-----	-----	-----	-----	-----	-----
192.168.110.51	Connected	PoweredOn	4	200	9576			
1.614	7.999	7.0.0						

```
PS C:\Users\Administrator.CORP> $vmhost = Get-VMHost
```

```
PS C:\Users\Administrator.CORP> $tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
```

```
PS C:\> Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip
```

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	10/8/2019 6:55 PM	1004	cacert.zip

```
PS C:\Users\Administrator.CORP> Export-VMHostImageDb -VMHost $vmhost -FilePath C:\vta\image.tgz
```

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	10/8/2019 11:02 PM	2391	image.tgz

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
```

```
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User trustedadmin@vsphere.local -Password 'VMware1!'
```

Name	Port	User
-----	----	----
192.168.110.22	443	VSPHERE.LOCAL\trustedadmin

```
PS C:\Users\Administrator.CORP> Export-TrustedPrincipal -FilePath C:\vta\principal.json
```

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	10/8/2019 11:14 PM	1873	principal.json

後續步驟

繼續將受信任主機資訊匯入至 Trust Authority 叢集。

匯出和匯入 TPM 簽署金鑰憑證

您可以從 ESXi 主機匯出 TPM 簽署金鑰 (EK) 憑證，然後將其匯入至 vSphere Trust Authority 叢集。當您想要信任受信任叢集中的個別 ESXi 主機時，請執行此動作。

若要將 TPM EK 憑證匯入至 Trust Authority 叢集中，必須變更 Trust Authority 叢集的預設證明類型以接受 EK 憑證。預設證明類型接受 TPM 憑證授權機構 (CA) 憑證。某些 TPM 不包含 EK 憑證。如果您想要信任個別 ESXi 主機，TPM 必須包含 EK 憑證。

備註 將匯出的 EK 憑證檔案儲存在安全的位置，以防您必須還原 vSphere Trust Authority 組態。

必要條件

- 啟用 Trust Authority 管理員。
- 啟用 Trust Authority 狀態。

程序

- 1 確保以 Trust Authority 管理員身分連線至 Trust Authority 叢集的 vCenter Server。

例如，您可以輸入 `$global:defaultviservers` 來顯示所有已連線的伺服器。

- 2 (選擇性) 如有必要，您可以執行下列命令，以確保您已連線至 Trust Authority 叢集的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 變更 Trust Authority 叢集的證明類型：

- a 執行 `Get-TrustAuthorityCluster` cmdlet，以顯示此 vCenter Server 管理的叢集。

```
Get-TrustAuthorityCluster
```

叢集隨即顯示。

- b 將 `Get-TrustAuthorityCluster` 資訊指派給變數。

例如，此命令會將名為 `vTA Cluster` 的叢集指派給變數 `$vTA`。

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

- c 將 `Get-TrustAuthorityTpm2AttestationSettings` 資訊指派給變數。

例如，此命令會將資訊指派給變數 `$tpm2Settings`。

```
$tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA
```

- d 執行 `Set-TrustAuthorityTpm2AttestationSettings` cmdlet，以指定 `RequireEndorsementKey` 和/或 `RequireCertificateValidation`。

例如，此命令會指定 `RequireEndorsementKey`。

```
Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings $tpm2Settings
-RequireEndorsementKey
```

系統會使用類似下列內容的確認提示進行回應。

```
Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-
c8' with the following parameters:
  RequireCertificateValidation: False
  RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

- e 出現確認提示時按 Enter。(預設值為 **Y**。)

輸出針對指定的設定顯示狀態為 True。例如，此狀態顯示 [需要簽署金鑰] 為 True，[需要憑證驗證] 為 False。

```
Name                                     RequireEndorsementKey
RequireCertificateValidation  Health
----
-----
TrustAuthorityTpm2AttestationSettings... True
False                               Ok
```

4 匯出 TPM EK 憑證：

- a 與 Trust Authority 叢集的 vCenter Server 中斷連線。

```
Disconnect-VIServer -server * -Confirm:$false
```

- b 執行 `Connect-VIServer` cmdlet，以根使用者身分連線至受信任叢集中的其中一個 ESXi 主機。

```
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

- c 執行 `Get-VMHost` cmdlet 以確認 ESXi 主機。

```
Get-VMHost
```

隨即顯示主機資訊。

- d 將 `Get-VMHost` 指派給變數。

例如：

```
$vmhost = Get-VMHost
```

- e 執行 `Export-Tpm2EndorsementKey cmdlet` 以匯出 ESXi 主機的 EK 憑證。

例如，此命令會將 EK 憑證匯出至 `tpm2ek.json` 檔案。

```
Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath C:\vta\tpm2ek.json
```

隨即建立該檔案。

5 匯入 TPM EK：

- a 與受信任叢集中的 ESXi 主機中斷連線。

```
Disconnect-VIServer -server * -Confirm:$false
```

- b 使用 Trust Authority 管理員使用者連線至 Trust Authority 叢集的 vCenter Server。

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user  
-Password 'password'
```

- c 執行 `Get-TrustAuthorityCluster cmdlet`。

```
Get-TrustAuthorityCluster
```

隨即顯示 Trust Authority 叢集中的叢集。

- d 將 `Get-TrustAuthorityCluster` '*cluster*' 資訊指派給變數。

例如，此命令會將叢集 `vTA Cluster` 的資訊指派給變數 `$vTA`。

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

- e 執行 `New-TrustAuthorityTpm2EndorsementKey cmdlet`。

例如，此命令使用先前在步驟 4 中匯出的 `tpm2ek.json` 檔案。

```
New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA -FilePath  
C:\vta\tpm2ek.json
```

此時會顯示已匯入的簽署金鑰資訊。

結果

Trust Authority 叢集的證明類型已變更為接受 EK 憑證。EK 憑證會從受信任叢集中匯出並匯入至 Trust Authority 叢集。

範例：匯出和匯入 TPM EK 憑證

此範例顯示如何使用 PowerCLI 將 Trust Authority 叢集的預設證明類型變更為接受 EK 憑證，從受信任叢集中的 ESXi 主機匯出 TPM EK 憑證，然後將其匯入至 Trust Authority 叢集。下表顯示了所使用的範例元件和值。

表 9-6. vSphere Trust Authority 設定範例

元件	值
Trust Authority 叢集的 vCenter Server	192.168.210.22
變數 \$vTA	Get-TrustAuthorityCluster 'vTA Cluster'
變數 \$tpm2Settings	Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster \$vTA
變數 \$vmhost	Get-VMHost
受信任叢集中的 ESXi 主機	192.168.110.51
Trust Authority 管理員	trustedadmin@vsphere.local
包含輸出檔案的本機目錄	C:\vta

```
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                                Port  User
----                                -
192.168.210.22                      443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                State           Id
----                -
vTA Cluster         Enabled         TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'

PS C:\Users\Administrator> $tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings
-TrustAuthorityCluster $vTA

PS C:\Users\Administrator> Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings
$tpm2Settings -RequireEndorsementKey

Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-c8' with
the following parameters:
  RequireCertificateValidation: False
  RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                                RequireEndorsementKey
RequireCertificateValidation  Health
----                                -
```



```

-----
TrustAuthorityTpm2AttestationSettings... True
False                               Ok

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                               Port  User
----                               -
192.168.110.51                     443   root

PS C:\Users\Administrator> Get-VMHost

Name                               ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz
MemoryUsageGB MemoryTotalGB Version
-----
-----
192.168.110.51 Connected      PoweredOn    4      55      9576
1.230      7.999  7.0.0

PS C:\Users\Administrator> $vmhost = Get-VMHost
PS C:\Users\Administrator> Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath
C:\vta\tpm2ek.json

Mode                               LastWriteTime           Length Name
----                               -
-a----      12/3/2019  10:16 PM           2391 tpm2ek.json

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                               Port  User
----                               -
192.168.210.22                     443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                               State           Id
----                               -
vTA Cluster      Enabled        TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'
PS C:\Users\Administrator> New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA
-FilePath C:\vta\tpm2ek.json

TrustAuthorityClusterId           Name                               Health
-----
TrustAuthorityCluster-domain-c8  1a520e42-4db8-1cbb-6dd7-f493fd921ccb  Ok

```

後續步驟

繼續將受信任主機資訊匯入至 [Trust Authority 叢集](#)。

將受信任主機資訊匯入至 Trust Authority 叢集

您可以將匯出的 ESXi 主機和 vCenter Server 資訊匯入 vSphere Trust Authority 叢集中，以便 Trust Authority 叢集知道它可以證明哪些主機。

如果按順序執行這些工作，則仍會連線至 Trust Authority 叢集的 vCenter Server。

必要條件

- 啟用 Trust Authority 管理員。
- 啟用 Trust Authority 狀態。
- 收集要信任的 ESXi 主機和 vCenter Server 的相關資訊。

程序

- 1 確保以 Trust Authority 管理員身分連線至 Trust Authority 叢集的 vCenter Server。

例如，您可以輸入 `$global:defaultviservers` 來顯示所有已連線的伺服器。

- 2 (選擇性) 如有必要，您可以執行下列命令，以確保您已連線至 Trust Authority 叢集的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 若要顯示此 vCenter Server 管理的叢集，請執行 `Get-TrustAuthorityCluster` cmdlet。

```
Get-TrustAuthorityCluster
```

叢集隨即顯示。

- 4 將 `Get-TrustAuthorityCluster` '*cluster*' 資訊指派給變數。

例如，此命令會將叢集 `vTA Cluster` 的資訊指派給變數 `$vTA`。

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

- 5 若要將受信任叢集的 vCenter Server 主體資訊匯入至 Trust Authority 叢集，請執行 `New-TrustAuthorityPrincipal` cmdlet。

例如，下列命令會匯入先前在 [收集要信任的 ESXi 主機和 vCenter Server 的相關資訊](#) 中匯出的 `principal.json` 檔案。

```
New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA -FilePath C:\vta\principal.json
```

此時會顯示 `TrustAuthorityPrincipal` 資訊。

- 6 若要確認匯入，請執行 `Get-TrustAuthorityPrincipal` cmdlet。

例如：

```
Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
```

此時會顯示已匯入的 `TrustAuthorityPrincipal` 資訊。

- 7 若要匯入信賴平台模組 (TPM) CA 憑證資訊，請執行 `New-TrustAuthorityTpm2CACertificate` cmdlet。

例如，下列命令會從先前在[收集要信任的 ESXi 主機和 vCenter Server 的相關資訊](#)中匯出的 `cacert.zip` 檔案匯入 TPM CA 憑證資訊。

```
New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster $vTA -FilePath C:\vta\cacert.zip
```

此時會顯示已匯入的憑證資訊。

- 8 若要匯入 ESXi 主機基礎映像資訊，請執行 `New-TrustAuthorityVMHostBaseImage` cmdlet。

例如，下列命令會從先前在[收集要信任的 ESXi 主機和 vCenter Server 的相關資訊](#)中匯出的 `image.tgz` 檔案匯入映像資訊。

```
New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA -FilePath C:\vta\image.tgz
```

此時會顯示已匯入的映像資訊。

結果

Trust Authority 叢集瞭解可遠端證明的 ESXi 主機，以及可信任的主機。

範例：將受信任主機資訊匯入至 Trust Authority 叢集

此範例顯示如何使用 PowerCLI 將受信任叢集的 vCenter Server 主體資訊和受信任主機資訊檔案匯入至 Trust Authority 叢集。假設您以 Trust Authority 管理員身分連線至 Trust Authority 叢集的 vCenter Server。下表顯示了所使用的範例元件和值。

表 9-7. vSphere Trust Authority 設定範例

元件	值
變數 <code>\$vTA</code>	<code>Get-TrustAuthorityCluster 'vTA Cluster1'</code>
Trust Authority 叢集的 vCenter Server	192.168.210.22
Trust Authority 叢集名稱	vTA Cluster1 (已啟用) vTA Cluster2 (已停用)
主體資訊檔案	<code>C:\vta\principal.json</code>
TPM 憑證檔案	<code>C:\vta\cacert.cer</code>

表 9-7. vSphere Trust Authority 設定範例 (續)

元件	值
ESXi 主機基礎映像檔案	C:\vta\image.tgz
Trust Authority 管理員	trustedadmin@vsphere.local

```

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                                Port  User
----                                -
192.168.210.22                      443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                State          Id
----                -
vTA Cluster1        Enabled        TrustAuthorityCluster-domain-c8
vTA Cluster2        Disabled      TrustAuthorityCluster-domain-c26

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster1'

PS C:\Users\Administrator.CORP> New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
-FilePath C:\vta\principal.json

Name                                Domain          Type
TrustAuthorityClusterId
----                                -
-----
vpxd-de207929-0601-43ef-9616-47d0cee0302f  vsphere.local  STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA

Name                                Domain          Type
TrustAuthorityClusterId
----                                -
-----
vpxd-de207929-0601-43ef-9616-47d0cee0302f  vsphere.local  STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster
$vTA -FilePath C:\vta\cacert.cer

TrustAuthorityClusterId              Name                                Health
-----
TrustAuthorityCluster-domain-c8      52BDB7B4B2F55C925C047257DED4588A7767D961 Ok

PS C:\Users\Administrator.CORP> New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
-FilePath C:\vta\image.tgz

TrustAuthorityClusterId              VMHostVersion              Health
-----

```

TrustAuthorityCluster-domain-c8-----
ESXi 7.0.0-0.0.14828939-----
Ok

後續步驟

繼續在 [Trust Authority 叢集上建立金鑰提供者](#)。

在 Trust Authority 叢集上建立金鑰提供者

為了讓金鑰提供者服務連線到金鑰提供者，必須建立受信任金鑰提供者，然後在 vSphere Trust Authority 叢集與金鑰伺服器 (KMS) 之間進行信任設定。對於大多數符合 KMIP 的金鑰伺服器，此設定程序包括設定用戶端和伺服器憑證。

之前在 vSphere 6.7 中稱為 KMS 叢集，現在在 vSphere 7.0 中稱為金鑰提供者。如需有關金鑰提供者的詳細資訊，請參閱[什麼是 vSphere Trust Authority 金鑰提供者服務](#)。

在生產環境中，您可以建立多個金鑰提供者。透過建立多個金鑰提供者，您可以解決如何根據公司組織、不同的業務單位或客戶等管理部署的問題。

如果按順序執行這些工作，則仍會連線至 vSphere Trust Authority 叢集的 vCenter Server。

必要條件

- [啟用 Trust Authority 管理員](#)。
- [啟用 Trust Authority 狀態](#)。
- [收集要信任的 ESXi 主機和 vCenter Server 的相關資訊](#)。
- [將受信任主機資訊匯入至 Trust Authority 叢集](#)。
- 在金鑰伺服器上建立並啟用金鑰，以用作受信任金鑰提供者的主要金鑰。此金鑰會包裝此受信任金鑰提供者所使用的其他金鑰和密碼。如需有關建立金鑰的詳細資訊，請參閱金鑰伺服器廠商說明文件。

程序

- 1 確保您已連線至 Trust Authority 叢集的 vCenter Server。例如，您可以輸入 `$global:defaultviservers` 來顯示所有已連線的伺服器。
- 2 (選擇性) 如有必要，您可以執行下列命令，以確保您已連線至 Trust Authority 叢集的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 若要建立受信任金鑰提供者，請執行 `New-TrustAuthorityKeyProvider` cmdlet。

例如，此命令對 `PrimaryKeyId` 使用 1，並使用名稱 `clkp`。如果按順序執行這些工作，則先前已將 `Get-TrustAuthorityCluster` 資訊指派給變數 (例如 `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`)。

```
New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA -PrimaryKeyId 1 -Name clkp
-KmipServerAddress ip_address
```

`PrimaryKeyId` 通常是來自金鑰伺服器的金鑰識別碼 (採用 UUID 形式)。請勿將金鑰名稱用於 `PrimaryKeyId`。`PrimaryKeyId` 值取決於廠商。請參閱金鑰伺服器說明文件。`New-TrustAuthorityKeyProvider` cmdlet 可以採用其他選項，例如 `KmipServerPort`、`ProxyAddress` 和 `ProxyPort`。如需詳細資訊，請參閱 `New-TrustAuthorityKeyProvider` 說明系統。

每個邏輯金鑰提供者 (無論其類型為標準、可信任還是本機) 都必須在所有 vCenter Server 系統中具有唯一的名稱。

如需詳細資訊，請參閱 [金鑰提供者命名](#)。

備註 若要將多個金鑰伺服器新增至金鑰提供者，請使用 `Add-TrustAuthorityKeyProviderServer` cmdlet。

隨即顯示金鑰提供者資訊。

- 4 建立信任連線，使金鑰伺服器信任受信任金鑰提供者。確切程序取決於金鑰伺服器接受的憑證以及您的公司原則。選取適合您伺服器的選項，然後完成下列步驟。

選項	請參閱
上傳用戶端憑證	上傳用戶端憑證以建立受信任金鑰提供者信任連線。
上傳 KMS 憑證和私密金鑰	上傳憑證和私密金鑰以建立受信任金鑰提供者信任連線。
新增憑證簽署申請	建立憑證簽署要求以建立受信任金鑰提供者信任連線。

5 透過上傳金鑰伺服器憑證完成信任設定，以便受信任金鑰提供者信任金鑰伺服器。

- a 將 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 資訊指派給變數。

例如：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

此變數會取得指定 Trust Authority 叢集中受信任的金鑰提供者，在此案例中為 `$vTA`。

備註 如果您有多個受信任金鑰提供者，請使用類似下列內容的命令根據需要進行選取：

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

使用 `Select-Object -Last 1` 會選取清單中的最後一個受信任金鑰提供者。

- b 若要取得金鑰伺服器的伺服器憑證，請執行 `Get-TrustAuthorityKeyProviderServerCertificate` 命令。

例如：

```
Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
```

隨即顯示伺服器憑證資訊。一開始，憑證不受信任，因此受信任狀態為 `False`。如果您已設定多個金鑰伺服器，將會傳回一份憑證清單。使用下列指示驗證並新增每個憑證。

- c 信任憑證之前，請將 `Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers` 資訊指派給變數 (例如 `cert`)，然後執行 `$cert.Certificate.ToString()` 命令並確認輸出。

例如：

```
$cert = Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
$cert.Certificate.ToString()
```

隨即顯示憑證資訊，包括主旨、簽發者和其他資訊。

- d 若要將 KMIP 伺服器憑證新增至受信任的金鑰提供者，請執行 `Add-TrustAuthorityKeyProviderServerCertificate`。

例如：

```
Add-TrustAuthorityKeyProviderServerCertificate -ServerCertificate $cert
```

此時會顯示憑證資訊，且現在受信任狀態為 `True`。

6 驗證金鑰提供者的狀態。

- a 若要重新整理金鑰提供者狀態，請重新指派 \$kp 變數。

例如：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

備註 如果您有多個受信任金鑰提供者，請使用類似下列內容的命令根據需要進行選取：

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

使用 `Select-Object -Last 1` 會選取清單中的最後一個受信任金鑰提供者。

- b 執行 \$kp.Status 命令以取得金鑰提供者狀態。

例如：

```
$kp.Status
```

備註 可能需要幾分鐘的時間才會重新整理狀態。若要檢視狀態，請重新指派 \$kp 變數，並重新執行 \$kp.Status 命令。

健全狀況狀態為 [正常] 表示金鑰提供者正在正常執行。

結果

受信任金鑰提供者隨即建立，並與金鑰伺服器建立了信任。

範例：在 Trust Authority 叢集上建立金鑰提供者

此範例顯示如何使用 PowerCLI 在 Trust Authority 叢集上建立受信任的金鑰提供者。假設您以 Trust Authority 管理員身分連線至 Trust Authority 叢集的 vCenter Server。在向廠商提交 CSR 後，它還使用金鑰伺服器廠商簽署的憑證。

下表顯示了所使用的範例元件和值。

表 9-8. vSphere Trust Authority 設定範例

元件	值
變數 \$vTA	Get-TrustAuthorityCluster 'vTA Cluster'
變數 \$kp	Get-TrustAuthorityKeyProvider -TrustAuthorityCluster \$vTA
變數 \$cert	Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer \$kp.KeyProviderServers
Trust Authority 叢集的 vCenter Server	192.168.210.22
符合 KMIP 的金鑰伺服器	192.168.110.91

表 9-8. vSphere Trust Authority 設定範例 (續)

元件	值
符合 KMIP 的金鑰伺服器使用者	vcqekmip
Trust Authority 叢集名稱	vTA 叢集
Trust Authority 管理員	trustedadmin@vsphere.local

```

PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
-PrimaryKeyId 8 -Name clkp -KmipServerAddress 192.168.110.91
Name                PrimaryKeyId      Type            TrustAuthorityClusterId
----                -
clkp                8                KMIP            TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProviderClientCertificate -KeyProvider
$kp
<Export the client certificate when you need to use it.>
PS C:\Users\Administrator.CORP> Export-TrustAuthorityKeyProviderClientCertificate
-KeyProvider $kp -FilePath clientcert.pem

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers

Certificate                Trusted      KeyProviderServerId      KeyProviderId
-----                -
[Subject]...              False      domain-c8-clkp:192.16.... domain-c8-clkp

PS C:\WINDOWS\system32> $cert.Certificate.ToString()
[Subject]
    E=<domain>, CN=<IP address>, OU=VMware Engineering, O=VMware, L=Palo Alto, S=California,
    C=US

[Issuer]
    O=<host>.eng.vmware.com, C=US, DC=local, DC=vsphere, CN=CA

[Serial Number]
    00CEF192BBF9D80C9F

[Not Before]
    8/10/2015 4:16:12 PM

[Not After]
    8/9/2020 4:16:12 PM

[Thumbprint]
    C44068C124C057A3D07F51DCF18720E963604B70

```

```
PS C:\Users\Administrator.CORP> $cert = Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers
PS C:\Users\Administrator.CORP> Add-TrustAuthorityKeyProviderServerCertificate
-ServerCertificate $cert
```

Certificate	Trusted	KeyProviderServerId	KeyProviderId
-----	-----	-----	-----
[Subject]...	True		domain-c8-clkp

```
PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> $kp.Status
```

KeyProviderId	Health	HealthDetails	ServerStatus
-----	-----	-----	-----
domain-c8-kp4	Ok	{}	{192.168.210.22}

後續步驟

繼續匯出 [Trust Authority 叢集資訊](#)。

上傳用戶端憑證以建立受信任金鑰提供者信任連線

某些金鑰伺服器 (KMS) 廠商會要求您將受信任金鑰提供者的用戶端憑證上傳到金鑰伺服器。上傳後，金鑰伺服器會接受來自受信任金鑰提供者的流量。

必要條件

- [啟用 Trust Authority 管理員](#)。
- [啟用 Trust Authority 狀態](#)。
- [收集要信任的 ESXi 主機和 vCenter Server 的相關資訊](#)。
- [將受信任主機資訊匯入至 Trust Authority 叢集](#)。
- [在 Trust Authority 叢集上建立金鑰提供者](#)。

程序

- 1 確保您已連線至 Trust Authority 叢集的 vCenter Server。例如，您可以輸入 `$global:defaultviservers` 來顯示所有已連線的伺服器。
- 2 (選擇性) 如有必要，您可以執行下列命令，以確保您已連線至 Trust Authority 叢集的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 將 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 資訊指派給變數。

例如：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

如果按順序執行這些工作，則先前已將 `Get-TrustAuthorityCluster` 資訊指派給變數 (例如 `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`)。

此變數會取得指定 Trust Authority 叢集中受信任的金鑰提供者，在此案例中為 `$vTA`。

備註 如果您有多個受信任金鑰提供者，請使用類似下列內容的命令根據需要進行選取：

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

使用 `Select-Object -Last 1` 會選取清單中的最後一個受信任金鑰提供者。

- 4 若要建立受信任金鑰提供者用戶端憑證，請執行 `New-TrustAuthorityKeyProviderClientCertificate` cmdlet。

例如：

```
New-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp
```

隨即顯示指紋。

- 5 若要匯出金鑰提供者用戶端憑證，請執行 `Export-TrustAuthorityKeyProviderClientCertificate` cmdlet。

例如：

```
Export-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -FilePath clientcert.pem
```

憑證即會匯出至檔案。

- 6 將憑證檔案上傳到金鑰伺服器。

如需詳細資訊，請參閱金鑰伺服器說明文件。

結果

受信任金鑰提供者已與金鑰伺服器建立信任。

上傳憑證和私密金鑰以建立受信任金鑰提供者信任連線

某些金鑰伺服器 (KMS) 廠商會要求您使用金鑰伺服器提供的用戶端憑證和私密金鑰來設定受信任金鑰提供者。設定受信任金鑰提供者後，金鑰伺服器會接受來自受信任金鑰提供者的流量。

必要條件

- 啟用 Trust Authority 管理員。
- 啟用 Trust Authority 狀態。
- 收集要信任的 ESXi 主機和 vCenter Server 的相關資訊。
- 將受信任主機資訊匯入至 Trust Authority 叢集。
- 在 Trust Authority 叢集上建立金鑰提供者。

- 從金鑰伺服器廠商請求採用 PEM 格式的憑證和私密金鑰。如果以 PEM 以外的格式傳回憑證，請將其轉換為 PEM。如果私密金鑰受密碼保護，請在移除密碼的情況下建立 PEM 檔案。您可以針對兩項作業使用 `openssl` 命令。例如：

- 將憑證從 CRT 轉換為 PEM 格式：

```
openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
```

- 將憑證從 DER 轉換為 PEM 格式：

```
openssl x509 -inform DER -in clientcert.der -out clientcert.pem
```

- 從私密金鑰移除密碼：

```
openssl rsa -in key.pem -out keynopassword.pem
Enter pass phrase for key.pem:
writing RSA key
```

程序

- 1 確保您已連線至 Trust Authority 叢集的 vCenter Server。例如，您可以輸入 `$global:defaultviservers` 來顯示所有已連線的伺服器。
- 2 (選擇性) 如有必要，您可以執行下列命令，以確保您已連線至 Trust Authority 叢集的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 將 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 資訊指派給變數。

例如：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

如果按順序執行這些工作，則先前已將 `Get-TrustAuthorityCluster` 資訊指派給變數 (例如 `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`)。

`$kp` 變數會取得指定 Trust Authority 叢集中受信任的金鑰提供者，在此案例中為 `$vTA`。

備註 如果您有多個受信任金鑰提供者，請使用類似下列內容的命令根據需要進行選取：

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

使用 `Select-Object -Last 1` 會選取清單中的最後一個受信任金鑰提供者。

4 使用 Set-TrustAuthorityKeyProviderClientCertificate 命令上傳憑證和私密金鑰。

例如：

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/to/certfile.pem> -PrivateKeyFilePath <path/to/privatekey.pem>
```

結果

受信任金鑰提供者已與金鑰伺服器建立信任。

建立憑證簽署要求以建立受信任金鑰提供者信任連線

某些金鑰伺服器 (KMS) 廠商會要求產生憑證簽署要求 (CSR) 並將該 CSR 傳送到金鑰伺服器廠商。金鑰伺服器廠商簽署 CSR 並傳回已簽署憑證。將此簽署憑證設定為受信任金鑰提供者的用戶端憑證後，金鑰伺服器會接受來自受信任金鑰提供者的流量。

此工作分為兩個步驟。首先，產生 CSR 並將其傳送給金鑰伺服器廠商。然後，上傳從金鑰伺服器廠商收到的簽署憑證。

必要條件

- 啟用 Trust Authority 管理員。
- 啟用 Trust Authority 狀態。
- 收集要信任的 ESXi 主機和 vCenter Server 的相關資訊。
- 將受信任主機資訊匯入至 Trust Authority 叢集。
- 在 Trust Authority 叢集上建立金鑰提供者。

程序

- 1 確保您已連線至 Trust Authority 叢集的 vCenter Server。例如，您可以輸入 `$global:defaultviservers` 來顯示所有已連線的伺服器。
- 2 (選擇性) 如有必要，您可以執行下列命令，以確保您已連線至 Trust Authority 叢集的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 將 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 資訊指派給變數。

例如：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

如果按順序執行這些工作，則先前已將 `Get-TrustAuthorityCluster` 資訊指派給變數 (例如 `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`)。

此變數會取得指定 Trust Authority 叢集中受信任的金鑰提供者，在此案例中為 \$vTA。

備註 如果您有多個受信任金鑰提供者，請使用類似下列內容的命令根據需要進行選取：

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

使用 `Select-Object -Last 1` 會選取清單中的最後一個受信任金鑰提供者。

- 4 若要產生 CSR，請使用 `New-TrustAuthorityKeyProviderClientCertificateCSR` cmdlet。

例如：

```
New-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp
```

隨即顯示 CSR。您也可以使用 `Get-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp` cmdlet 來取得 CSR。

- 5 若要取得已簽署的憑證，請將 CSR 提交至金鑰伺服器廠商。

憑證必須採用 PEM 格式。如果以 PEM 以外的格式傳回憑證，請使用 `openssl` 命令將其轉換為 PEM。例如：

- 將憑證從 CRT 轉換為 PEM 格式：

```
openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
```

- 將憑證從 DER 轉換為 PEM 格式：

```
openssl x509 -inform DER -in clientcert.der -out clientcert.pem
```

- 6 當您從金鑰伺服器廠商收到已簽署的憑證時，請使用 `Set-TrustAuthorityKeyProviderClientCertificate` cmdlet 將憑證上傳至金鑰伺服器。

例如：

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/tp/certfile.pem>
```

結果

受信任金鑰提供者已與金鑰伺服器建立信任。

匯出 Trust Authority 叢集資訊

為了讓受信任叢集連線至 vSphere Trust Authority 叢集，您必須以檔案形式匯出 Trust Authority 叢集的服務資訊，然後將該檔案匯入至受信任叢集中。務必確保此檔案的機密性並安全地進行傳輸。

如果按順序執行這些工作，則仍會連線至 Trust Authority 叢集的 vCenter Server。

備註 將匯出的服務資訊檔案儲存在安全的位置，以防您必須還原 vSphere Trust Authority 組態。

必要條件

- 啟用 Trust Authority 管理員。
- 啟用 Trust Authority 狀態。
- 收集要信任的 ESXi 主機和 vCenter Server 的相關資訊。
- 將受信任主機資訊匯入至 Trust Authority 叢集。
- 在 Trust Authority 叢集上建立金鑰提供者。

程序

- 1 確保您已連線至 Trust Authority 叢集的 vCenter Server。例如，您可以輸入 `$global:defaultviservers` 來顯示所有已連線的伺服器。
- 2 (選擇性) 如有必要，您可以執行下列命令，以確保您已連線至 Trust Authority 叢集的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 若要匯出 Trust Authority 叢集的證明服務和金鑰提供者服務資訊，請執行 `Export-TrustAuthorityServicesInfo cmdlet`。

例如，此命令會將服務資訊匯出至 `clsettings.json` 檔案。如果按順序執行這些工作，則先前已將 `Get-TrustAuthorityCluster` 資訊指派給變數 (例如 `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`)。

```
Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA -FilePath
C:\vta\clsettings.json
```

隨即建立該檔案。

結果

隨即建立包含 Trust Authority 叢集資訊的檔案。

範例：匯出 Trust Authority 叢集資訊

此範例顯示如何使用 PowerCLI 匯出 Trust Authority 叢集服務資訊。下表顯示了所使用的範例元件和值。

表 9-9. vSphere Trust Authority 設定範例

元件	值
變數 \$vTA	Get-TrustAuthorityCluster 'vTA Cluster'
Trust Authority 叢集的 vCenter Server	192.168.210.22
Trust Authority 管理員	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA
-FilePath C:\vta\clsettings.json

Mode                LastWriteTime         Length Name
----                -
-a----          10/16/2019   9:59 PM           8177 clsettings.json
```

後續步驟

繼續將 Trust Authority 叢集資訊匯入至受信任的主機。

將 Trust Authority 叢集資訊匯入至受信任的主機

將 vSphere Trust Authority 叢集資訊匯入至受信任的叢集後，受信任主機會透過 Trust Authority 叢集啟動證明程序。

必要條件

- 啟用 Trust Authority 管理員。
- 啟用 Trust Authority 狀態。
- 收集要信任的 ESXi 主機和 vCenter Server 的相關資訊。
- 將受信任主機資訊匯入至 Trust Authority 叢集。
- 在 Trust Authority 叢集上建立金鑰提供者。
- 匯出 Trust Authority 叢集資訊。

程序

- 1 確保以 Trust Authority 管理員身分連線至受信任叢集的 vCenter Server。

例如，您可以輸入 `$global:defaultviservers` 來顯示所有已連線的伺服器。

- 2 (選擇性) 如有必要，您可以執行下列命令，以確保您已連線至受信任叢集的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

備註 也可以啟動另一個 PowerCLI 工作階段來連線至受信任叢集的 vCenter Server。

- 3 確認受信任叢集的狀態為 [已停用]。

```
Get-TrustedCluster
```

狀態會顯示為 [已停用]。

- 4 將 Get-TrustedCluster 資訊指派給變數。

例如，此命令會將叢集 Trusted Cluster 的資訊指派給變數 \$TC。

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

- 5 透過回應來驗證變數的值。

例如：

```
$TC
```

隨即顯示 Get-TrustedCluster 資訊。

- 6 若要將 Trust Authority 叢集資訊匯入至 vCenter Server，請執行 Import-TrustAuthorityServicesInfo cmdlet。

例如，此命令會從先前在匯出 Trust Authority 叢集資訊中匯出的 clsettings.json 檔案匯入服務資訊。

```
Import-TrustAuthorityServicesInfo -FilePath C:\vta\clsettings.json
```

系統會用確認提示作出回應。

```
Confirmation
Importing the TrustAuthorityServicesInfo into Server 'ip_address'. Do you want to proceed?

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):
```

- 7 出現確認提示時按 Enter。(預設值為 **Y**。)

隨即顯示 Trust Authority 叢集中主機的服務資訊。

- 8 若要啟用受信任叢集，請執行 Set-TrustedCluster cmdlet。

例如：

```
Set-TrustedCluster -TrustedCluster $TC -State Enabled
```

系統會用確認提示作出回應。

```
Confirmation
Setting TrustedCluster 'cluster' with new TrustedState 'Enabled'. Do you want to proceed?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):
```

如果受信任叢集處於狀況不良的狀態，則會顯示下列警告訊息，然後再顯示確認訊息：

```
WARNING: The TrustedCluster 'cluster' is not healthy in its TrustedClusterAppliedStatus.
This cmdlet will automatically remediate the TrustedCluster.
```

9 出現確認提示時按 Enter。(預設值為 **y**。)

受信任的叢集隨即啟用。

備註 也可以透過單獨啟用證明服務和金鑰提供者服務來啟用受信任的叢集。使用 `Add-TrustedClusterAttestationServiceInfo` 與 `Add-TrustedClusterKeyProviderServiceInfo` 命令。例如，下列命令一次針對具有兩個金鑰提供者服務和兩個證明服務的叢集 `Trusted Cluster` 啟用一個服務。

```
Add-TrustedClusterAttestationServiceInfo -TrustedCluster 'Trusted Cluster'
-AttestationServiceInfo (Get-AttestationServiceInfo | Select-Object -index 0,1)
Add-TrustedClusterKeyProviderServiceInfo -TrustedCluster 'Trusted Cluster'
-KeyProviderServiceInfo (Get-KeyProviderServiceInfo | Select-Object -index 0,1)
```

10 確認受信任叢集中已設定證明服務和金鑰提供者服務。

a 將 `Get-TrustedCluster` 資訊指派給變數。

例如，此命令會將叢集 `Trusted Cluster` 的資訊指派給變數 `$TC`。

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

b 確認已設定證明服務。

```
$tc.AttestationServiceInfo
```

即會顯示證明服務資訊。

c 確認已設定金鑰提供者服務。

```
$tc.KeyProviderServiceInfo
```

即會顯示金鑰提供者服務資訊。

結果

受信任叢集中的 ESXi 受信任主機會透過 `Trust Authority` 叢集啟動證明程序。

範例：將 `Trust Authority` 叢集資訊匯入至受信任的主機

此範例顯示如何將 `Trust Authority` 叢集服務資訊匯入至受信任叢集。下表顯示了所使用的範例元件和值。

表 9-10. vSphere Trust Authority 設定範例

元件	值
受信任叢集的 vCenter Server	192.168.110.22
Trust Authority 管理員	trustedadmin@vsphere.local
受信任叢集名稱	受信任叢集
Trust Authority 叢集中的 ESXi 主機	192.168.210.51 和 192.168.210.52
變數 \$TC	Get-TrustedCluster -Name 'Trusted Cluster'

```

PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                                Port  User
----                                -
192.168.110.22                     443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustedCluster

Name                State          Id
----                -
Trusted Cluster     Disabled       TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $TC

Name                State          Id
----                -
Trusted Cluster     Disabled       TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> Import-TrustAuthorityServicesInfo -FilePath
C:\vta\clsettings.json

Confirmation
Importing the TrustAuthorityServicesInfo into Server '192.168.110.22'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

ServiceAddress      ServicePort      ServiceGroup
-----
192.168.210.51      443              host-13:86f7ab6c-ad6f-4606-...
192.168.210.52      443              host-16:86f7ab6c-ad6f-4606-...
192.168.210.51      443              host-13:86f7ab6c-ad6f-4606-...
192.168.210.52      443              host-16:86f7ab6c-ad6f-4606-...

PS C:\Users\Administrator.CORP> Set-TrustedCluster -TrustedCluster $TC -State Enabled

Confirmation
Setting TrustedCluster 'Trusted Cluster' with new TrustedState 'Enabled'. Do you want to
proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):

```

```

Name                State                Id
----                -
Trusted Cluster     Enabled              TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $tc.AttestationServiceInfo

ServiceAddress      ServicePort          ServiceGroup
-----
192.168.210.51      443                  host-13:dc825986-73d2-463c-...
192.168.210.52      443                  host-16:dc825986-73d2-463c-...

PS C:\Users\Administrator.CORP> $tc.KeyProviderServiceInfo

ServiceAddress      ServicePort          ServiceGroup
-----
192.168.210.51      443                  host-13:dc825986-73d2-463c-...
192.168.210.52      443                  host-16:dc825986-73d2-463c-...

```

後續步驟

繼續使用 vSphere Client 為受信任的主機設定受信任金鑰提供者或使用命令列為受信任的主機設定受信任金鑰提供者。

使用 vSphere Client 為受信任的主機設定受信任金鑰提供者

您可以使用 vSphere Client 設定受信任的金鑰提供者。

必要條件

- 啟用 Trust Authority 管理員。
- 啟用 Trust Authority 狀態。
- 收集要信任的 ESXi 主機和 vCenter Server 的相關資訊。
- 將受信任主機資訊匯入至 Trust Authority 叢集。
- 在 Trust Authority 叢集上建立金鑰提供者。
- 匯出 Trust Authority 叢集資訊。
- 將 Trust Authority 叢集資訊匯入至受信任的主機。

程序

- 1 使用 vSphere Client 連線到受信任叢集的 vCenter Server。
- 2 以 vCenter Server 管理員身分或具有密碼編譯作業、管理金鑰伺服器權限的管理員身分登入。
- 3 選取 vCenter Server，然後選取設定。
- 4 在安全性下，選取金鑰提供者。

5 選取新增受信任的金鑰提供者。

可用的受信任金鑰提供者會顯示 [已連線] 狀態。

6 選取受信任的金鑰提供者，然後按一下**新增金鑰提供者**。

受信任的金鑰提供者會顯示為 [受信任且已連線]。如果這是您新增的第一個受信任金鑰提供者，則會將其標記為預設提供者。

備註 片刻之後，所有主機才能取得金鑰提供者，vCenter Server 才會更新快取。由於資訊的散佈方式，您可能必須等待幾分鐘，才能在某些主機上將金鑰提供者用於金鑰作業。

結果

ESXi 受信任的主機現在可以執行密碼編譯作業，例如建立已加密的虛擬機器。

後續步驟

使用受信任的金鑰提供者加密虛擬機器，與第一次在 vSphere 6.5 中提供的虛擬機器加密使用者體驗類似。請參閱第 10 章 [在 vSphere 環境中使用加密](#)。

使用命令列為受信任的主機設定受信任金鑰提供者

您可以使用命令列設定受信任的金鑰提供者。可以為 vCenter Server 設定預設受信任金鑰提供者，或在 vCenter 物件階層中的叢集或叢集資料夾層級設定。

必要條件

- [啟用 Trust Authority 管理員](#)。
- [啟用 Trust Authority 狀態](#)。
- [收集要信任的 ESXi 主機和 vCenter Server 的相關資訊](#)。
- [將受信任主機資訊匯入至 Trust Authority 叢集](#)。
- [在 Trust Authority 叢集上建立金鑰提供者](#)。
- [匯出 Trust Authority 叢集資訊](#)。
- [將 Trust Authority 叢集資訊匯入至受信任的主機](#)。

在受信任叢集中，您必須擁有包含 [密碼編譯作業.管理 KMS 權限](#) 的角色。

程序

1 確保以管理員身分連線至受信任叢集的 vCenter Server。

例如，您可以輸入 `$global:defaultviservers` 來顯示所有已連線的伺服器。

2 (選擇性) 如有必要，您可以執行下列命令，以確保您已連線至受信任叢集的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustedCluster_VC_ip_address -User admin_user -Password 'password'
```

3 取得受信任的金鑰提供者。

```
Get-KeyProvider
```

您可以使用 `-Name keyprovider` 選項來指定單一受信任金鑰提供者。

4 將 `Get-KeyProvider` 受信任金鑰提供者資訊指派給變數。

例如，此命令會將資訊指派給變數 `$workload_kp`。

```
$workload_kp = Get-KeyProvider
```

如果您有多個受信任的金鑰提供者，可以使用 `Select-Object` 選取其中一個。

```
$workload_kp = Get-KeyProvider | Select-Object -Index 0
```

5 登錄受信任的金鑰提供者。

```
Register-KeyProvider -KeyProvider $workload_kp
```

若要登錄其他受信任的金鑰提供者，請重複步驟 4 和步驟 5。

備註 片刻之後，所有主機才能取得金鑰提供者，vCenter Server 才會更新快取。由於資訊的散佈方式，您可能必須等待幾分鐘，才能在某些主機上將金鑰提供者用於金鑰作業。

6 設定要使用的預設受信任金鑰提供者。

- a 若要在 vCenter Server 層級設定預設金鑰提供者，請執行下列命令。

```
Set-KeyProvider -KeyProvider $workload_kp -DefaultForSystem
```

- b 若要在叢集層級設定金鑰提供者，請執行下列命令。

例如，此命令為叢集 `Trusted Cluster` 設定金鑰提供者。

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'Trusted Cluster'
```

- c 若要在叢集資料夾層級設定金鑰提供者，請執行下列命令。

例如，此命令會為在 `workLoad` 資料中心建立的叢集資料夾 `TC Folder` 設定金鑰提供者。

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'TC Folder'
```

後續步驟

使用受信任的金鑰提供者加密虛擬機器，與第一次在 vSphere 6.5 中提供的虛擬機器加密使用者體驗類似。請參閱第 10 章在 [vSphere 環境中使用加密](#)。

在 vSphere 環境中管理 vSphere Trust Authority

設定 vSphere Trust Authority 後，您可以執行其他作業，例如停止和啟動服務、將主機新增至叢集，以及檢視 Trust Authority 叢集的狀態。

您可以使用 vSphere Client、API 和 PowerCLI cmdlet 來執行工作。請參閱 vSphere Web Services SDK 程式設計指南、VMware PowerCLI 說明文件，以及《VMware PowerCLI Cmdlet 參考》說明文件。

啟動、停止和重新啟動 vSphere Trust Authority 服務

您可以使用 vSphere Client 來啟動、停止和重新啟動 vSphere Trust Authority 服務。

構成 vSphere Trust Authority 的服務包括證明服務 (attestd) 和金鑰提供者服務 (kmsd)。

程序

- 1 使用 vSphere Client 連線至 vSphere Trust Authority 叢集的 vCenter Server。
- 2 以管理員身分登入。
- 3 瀏覽至 Trust Authority 叢集中的 ESXi 主機。
- 4 選取**設定**，然後按一下**系統**下的**服務**。
- 5 找到 attestd 服務和 kmsd 服務。
- 6 視情況選取**重新啟動**、**啟動**或**停止**作業。

檢視 Trust Authority 主機

可以使用 vSphere Client 檢視為受信任叢集設定的 vSphere Trust Authority 主機。

程序

- 1 使用 vSphere Client 連線到受信任叢集的 vCenter Server。
- 2 以管理員身分登入。
- 3 選取 vCenter Server 執行個體。
- 4 按一下**設定**索引標籤，然後選取**安全性**下的 **Trust Authority**。
隨即顯示為受信任叢集設定的 Trust Authority 叢集中的 ESXi 主機。

檢視 vSphere Trust Authority 叢集狀態

您可以使用 vSphere Client 檢視 vSphere Trust Authority 叢集的狀態。狀態為 [已啟用] 或 [已停用]。

當 Trust Authority 叢集狀態為 [已啟用] 時，受信任叢集中的受信任主機可與證明服務和金鑰提供者服務進行通訊。

程序

- 1 使用 vSphere Client 連線至 Trust Authority 叢集的 vCenter Server。
- 2 以管理員身分登入。
- 3 在物件階層中選取 Trust Authority 叢集。

- 按一下**設定索引標籤**，然後選取 **Trust Authority** 下的 **Trust Authority 叢集**。

狀態會顯示為 [已啟用] 或 [已停用]。

重新啟動受信任主機服務

您可以重新啟動在受信任主機上執行的服務。

服務 **kmxa** 會在 ESXi 受信任主機上執行。

必要條件

必須啟用對 ESXi shell 的存取。請參閱[使用 vSphere Client 啟用對 ESXi Shell 的存取](#)。

程序

- 使用 SSH 或其他遠端主控台連線，以啟動 ESXi 受信任主機上的工作階段。
- 以 root 身分登入。
- 執行下列命令。

```
/etc/init.d/kmxa restart
```

新增和移除 vSphere Trust Authority 主機

您可以使用 VMware 提供的指令碼，在 vSphere Trust Authority 叢集中新增和移除 ESXi 主機。

在 vSphere 7.0 中，您可以使用 VMware 提供的指令碼，在現有 vSphere Trust Authority 叢集或受信任叢集中新增和移除 ESXi 主機。在 vSphere 7.0 Update 1 及更新版本中，可以使用修復功能將 ESXi 主機新增至現有受信任叢集。請參閱[使用 vSphere Client 將主機新增到受信任叢集](#)和[使用 CLI 將主機新增到受信任叢集](#)。

在 vSphere 7.0 Update 1 及更新版本中，仍必須使用指令碼將 ESXi 主機新增至現有 Trust Authority 叢集。請參閱 VMware 知識庫文章，網址為 <https://kb.vmware.com/s/article/77234> 和 <https://kb.vmware.com/s/article/77146>。

使用 vSphere Client 將主機新增到受信任叢集

可以使用 vSphere Client 將 ESXi 主機新增至現有的受信任叢集。

最初設定了受信任叢集後，您可能想要新增更多 ESXi 主機。但是，將主機新增至受信任叢集時，必須採取額外的修復步驟。修復受信任叢集時，請確保其所需組態狀態與其套用的組態相符。

在 vSphere 7.0 中發行的第一個版本的 vSphere Trust Authority 中，執行指令碼以將主機新增至現有的受信任叢集。在 vSphere 7.0 Update 1 及更新版本中，可以使用修復功能將主機新增至受信任叢集。在 vSphere 7.0 Update 1 及更新版本中，仍必須使用指令碼將主機新增至現有的 Trust Authority 叢集。請參閱[新增和移除 vSphere Trust Authority 主機](#)。

必要條件

適用於受信任叢集的 vCenter Server 必須執行 vSphere 7.0 Update 1 或更新版本。

如果您要新增的 ESXi 主機的 ESXi 版本或 TPM 硬體類型與您最初為受信任叢集設定的值不同，則需要執行其他步驟。必須將此資訊匯出後再匯入 vSphere Trust Authority 叢集。請參閱[收集要信任的 ESXi 主機和 vCenter Server 的相關資訊](#)和將受信任主機資訊匯入至 Trust Authority 叢集。

所需權限：請參閱[一般工作所需的 vCenter Server 權限](#)中的「新增主機」工作。

程序

- 1 使用 vSphere Client 連線到受信任叢集的 vCenter Server。
- 2 以 Trust Authority 管理員身分登入。
- 3 導覽至受信任叢集。
- 4 在設定索引標籤上，選取組態 > 快速入門。
- 5 按一下新增主機卡中的新增。
- 6 依照提示進行操作。
- 7 在 Trust Authority 索引標籤上，按一下修復。
- 8 若要確認受信任叢集狀況良好，請按一下檢查健全狀況。

使用 CLI 將主機新增到受信任叢集

可以使用命令列將 ESXi 主機新增至現有的受信任叢集。

最初設定了受信任叢集後，您可能想要新增更多 ESXi 主機。但是，將主機新增至受信任叢集時，必須採取額外的修復步驟。修復受信任叢集時，請確保其所需組態狀態與其套用的組態相符。

在 vSphere 7.0 中發行的第一個版本的 vSphere Trust Authority 中，執行指令碼以將主機新增至現有的受信任叢集。在 vSphere 7.0 Update 1 及更新版本中，可以使用修復功能新增受信任主機。在 vSphere 7.0 Update 1 及更新版本中，仍必須使用指令碼將主機新增至現有的 Trust Authority 叢集。請參閱[新增和移除 vSphere Trust Authority 主機](#)。

必要條件

- 適用於受信任叢集的 vCenter Server 必須執行 vSphere 7.0 Update 1 或更新版本。
- 需要 PowerCLI 12.1.0 或更新版本。
- 所需權限：請參閱[一般工作所需的 vCenter Server 權限](#)中的「新增主機」工作。

程序

- 1 使用您通常執行的任何步驟，將 ESXi 主機新增至受信任叢集。
- 2 在 PowerCLI 工作階段中，執行 Connect-VIServer cmdlet，以 Trust Authority 管理員身分連線至受信任叢集的 vCenter Server。

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'
```

- 若要檢查受信任叢集的狀態，請執行 `Get-TrustedClusterAppliedStatus` PowerCLI cmdlet。

```
Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
```

- 如果受信任叢集狀況不良，請將 `Set-TrustedCluster` cmdlet 與 `-Remediate` 參數搭配執行。

```
Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate
```

- 若要確認受信任叢集狀況良好，請重新執行 `Get-TrustedClusterAppliedStatus` cmdlet。

```
Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
```

從受信任叢集中解除委任受信任的主機

您可以從受信任叢集中移除或解除委任受信任的主機。根據具體案例，您可以從受信任叢集中解除委任一台受信任主機或所有受信任主機。

解除委任受信任的主機時，修復功能會將受信任主機的所需狀態設定為將其移到的非受信任叢集的所需狀態。解除委任的受信任主機會變成一般主機。受信任叢集 (從中移動了受信任主機) 會繼續擁有其所需的狀態組態，並且仍作為受信任叢集運作。

從受信任叢集中移除所有受信任主機時，會解除委任受信任叢集。從受信任主機和受信任叢集中移除所需的狀態組態和已套用的組態，然後將所有受信任主機移至非受信任叢集。

您可以在環境中重複使用已解除委任的受信任主機。例如，可以重複使用非受信任的基礎結構容量中的主機或作為 vSphere Trust Authority 主機重複使用。您可以使用相同 vCenter Server 或不同 vCenter Server 中已解除委任的主機。

如需有關受信任叢集組態和健全狀況的詳細資訊，請參閱[檢查和修復受信任叢集健全狀況](#)。

必要條件

- 適用於受信任叢集的 vCenter Server 必須執行 vSphere 7.0 Update 1 或更新版本。
- 如果使用 PowerCLI，則需要 12.1.0 或更新版本。

程序

- 使用 vSphere Client 連線到受信任叢集的 vCenter Server。
- 以 Trust Authority 管理員身分登入。
- 導覽至受信任叢集。

4 決定如何從受信任叢集中解除委任受信任主機。

工作	步驟
保留受信任叢集和其餘受信任主機的所需組態狀態	<p>a 將主機置於維護模式，並將其移至新的空白叢集 (即叢集不包含任何主機)。</p> <p>b 在主機上結束維護模式。</p> <p>c 對於新的空白叢集 (非受信任叢集)，請在 Trust Authority 索引標籤上，按一下 修復。</p> <p>修復會從已移動的主機中移除受信任的組態。受信任叢集會保留其所需的狀態組態。</p>
移除所有受信任主機的所需組態狀態和已套用的組態狀態	<p>a 在 PowerCLI 工作階段中，執行 <code>Connect-VIServer</code> cmdlet，以 Trust Authority 管理員身分連線至受信任叢集的 vCenter Server。</p> <pre>Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'</pre> <p>b 執行 <code>Set-TrustedCluster</code> cmdlet，例如：</p> <pre>Set-TrustedCluster -TrustedCluster 'TrustedCluster' -State Disabled</pre> <p>將從所有受信任主機中移除受信任基礎結構組態，並且受信任叢集已移除其所需的狀態組態。</p> <p>c 將所有主機置於維護模式，並將其移至其他叢集。</p> <p>d 在主機上結束維護模式。</p>

5 若要確認受信任叢集狀況良好，請在受信任叢集的 **Trust Authority** 索引標籤上按一下 **檢查健全狀況**。

後續步驟

如果您不再打算從解除委任的 ESXi 主機證明特定版本的 ESXi 或 TPM 硬體，請更新 Trust Authority 叢集的組態以實現最佳安全性。請參閱 VMware 知識庫文章，網址為 <https://kb.vmware.com/s/article/77146>。

備份 vSphere Trust Authority 組態

使用設定 vSphere Trust Authority 時匯出的檔案做為 Trust Authority 備份。您可以使用這些檔案還原 Trust Authority 部署。確保這些組態檔的機密性並安全地進行傳輸。

大多數 vSphere Trust Authority 組態和狀態資訊會儲存在 ConfigStore 資料庫中的 ESXi 主機上。用於備份 vCenter Server 執行個體的 vCenter Server 管理介面不會備份 vSphere Trust Authority 的組態資訊。如果您儲存並安全地存放設定 vSphere Trust Authority 環境時所匯出的組態檔，將會有還原 vSphere Trust Authority 組態所需的資訊。若您必須產生此資訊，請參閱 [收集要信任的 ESXi 主機和 vCenter Server 的相關資訊](#)。

變更受信任金鑰提供者的主要金鑰

您可以變更受信任金鑰提供者的主要金鑰，例如，當您想要輪替所使用的主要金鑰時。

如需有關金鑰生命週期的指引，請參閱 [虛擬機器加密最佳做法](#)。

必要條件

在金鑰伺服器 (KMS) 上建立並啟用金鑰，以用作受信任金鑰提供者的新主要金鑰。此金鑰會包裝此受信任金鑰提供者所使用的其他金鑰和密碼。如需有關建立金鑰的詳細資訊，請參閱 KMS 廠商說明文件。

程序

- 1 執行 `Set-TrustAuthorityKeyProvider` 命令。

例如：

```
Set-TrustAuthorityKeyProvider -MasterKeyId Key-ID
```

- 2 驗證金鑰提供者的狀態。

- a 將 `Get-TrustAuthorityCluster` 資訊指派給變數。

例如：

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

- b 將 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 資訊指派給變數。

例如：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

- c 透過執行 `$kp.Status` 驗證金鑰提供者的狀態。

例如：

```
$kp.Status

KeyProviderId Health HealthDetails ServerStatus
-----
domain-c8-kp4    Ok {} {IP_address}
```

健全狀況狀態為 [正常] 表示金鑰提供者正在正常執行。

結果

新的主要金鑰將用於任何新的加密作業。使用舊的主要金鑰加密的資料仍會使用舊金鑰進行解密。

受信任主機證明報告

在 vSphere Trust Authority 中，vCenter Server 驗證並報告受信任主機的證明狀態。您可以使用 vSphere Client 來檢視受信任主機的證明狀態。

什麼是 vSphere Trust Authority 證明報告

vSphere Trust Authority 針對受信任主機使用遠端證明，以證明其開機軟體的真確性。證明將驗證受信任主機正在執行正版 VMware 軟體，還是 VMware 簽署的合作夥伴軟體。受信任叢集的 vCenter Server 會與受信任主機進行通訊，以取得內部證明報告。證明報告會指出受信任主機是否已透過 Trust Authority 叢集上執行的證明服務進行證明。如果受信任主機尚未證明，則證明報告還會指定錯誤訊息。vSphere Client 顯示受信任主機的證明狀態，以及 vSphere Trust Authority 或 vCenter Server 是否證明了主機。

已通過證明狀態

已通過證明狀態表示受信任主機已透過 vSphere Trust Authority 證明服務進行證明，並且向 vCenter Server 提供了內部證明報告。

未通過證明狀態

未通過證明狀態表示受信任主機無法透過任何 vSphere Trust Authority 證明服務進行證明。vCenter Server 內部證明報告包含由受信任主機嘗試證明所用的證明服務所報告的錯誤。

處理未證明的受信任主機

如果受信任主機未經證明，則受信任主機上執行的虛擬機器 (包括已加密的虛擬機器) 仍可繼續存取。無法將未證明的受信任主機上的虛擬機器開啟電源。但是，仍可以新增未加密的虛擬機器。如果受信任主機未經證明，請採取步驟來解決證明問題。請參閱[對受信任主機證明問題進行疑難排解](#)。

多個 Trust Authority 主機和證明報告

如果已設定多個 Trust Authority 主機，則各個主機可能會提供多個可用的證明報告。報告狀態時，vSphere Client 會顯示第一個「證明」報告中所找到的狀態。如果沒有「證明」報告，vSphere Client 會顯示第一個「未證明」報告中所找到的錯誤。

即使已設定多個 Trust Authority 主機，vSphere Client 仍會僅顯示一個證明報告中的狀態，並且可能會顯示錯誤訊息。

檢視受信任叢集證明狀態

您可以使用 vSphere Client 來檢視受信任主機的證明狀態。

必要條件

- 受信任主機和 vSphere Trust Authority 主機都必須執行 ESXi 7.0 Update 1 或更新版本。
- 適用於個別叢集的 vCenter Server 主機必須執行 vSphere 7.0 Update 1 或更新版本。

程序

- 1 使用 vSphere Client 連線到受信任叢集的 vCenter Server。
- 2 以管理員身分登入。
可以 Trust Authority 管理員或 vSphere 管理員身分登入。
- 3 導覽至資料中心，然後按一下**監控索引**標籤。
- 4 按一下**安全性**。

5 檢閱 [證明] 資料行中受信任主機的狀態，並讀取 [訊息] 資料行中隨附的訊息。

後續步驟

如果發生錯誤，請參閱[對受信任主機證明問題進行疑難排解](#)。

對受信任主機證明問題進行疑難排解

vSphere Trust Authority 證明報告提供了對受信任主機證明錯誤進行疑難排解的起點。

程序

- 1 檢視受信任叢集證明狀態。
- 2 使用下表來疑難排解和解決錯誤。

Error	原因和解決方案
未設定證明服務。	尚未設定證明服務。透過使用 [修復] 動作，將受信任主機設定為使用證明服務。請參閱 修復受信任叢集 。
沒有可用的 TPM2 裝置。	安裝受信任主機並將其設定為使用信賴平台模組 (TPM)。請參閱廠商說明文件。
無法擷取 TPM2 簽署公開金鑰或憑證。	請檢查 TPM 是否受支援，以及是否具有有效的簽署金鑰。您可能需要連絡 VMware 支援。
證明報告不可用。	受信任主機可能尚未完成證明。請等待幾分鐘，然後重新檢查證明狀態。
證明服務版本與請求不相容。	將執行證明服務的 Trust Authority 主機更新為 vSphere 7.0 Update 1 或更新版本。
由於未啟用安全開機，證明失敗。	檢查受信任主機是否已設定為使用安全開機。請參閱 ESXi 主機的 UEFI 安全開機 。
證明無法識別遠端軟體版本。	將受信任主機的基礎映像資訊匯入至證明服務。請參閱 將受信任主機資訊匯入至 Trust Authority 叢集 。
由於需要 TPM 憑證，證明失敗。	檢查 TPM 是否受支援。或者，執行下列 PowerCLI cmdlet 來修改 <code>com.vmware.esx.attestation.tpm2.settings</code> ，以將 <code>requireCertificateValidation</code> 設定為 <code>false</code> 。 <pre>Set-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster TrustedCluster -RequireCertificateValidation:\$false -RequireEndorsementKey:\$true</pre>
由於 TPM 未知，證明失敗。	將 TPM 簽署金鑰匯入至證明服務。請參閱 將受信任主機資訊匯入至 Trust Authority 叢集 。
錯誤: vapi.send.failed。	kmxa 服務可能未在受信任主機上執行，或 kmxa 服務無法連絡證明服務。確保 kmxa 服務已啟動。此外，請檢查證明服務是否正在執行。請參閱 重新啟動受信任主機服務 。

檢查和修復受信任叢集健全狀況

您可以檢查並驗證受信任叢集的健全狀況。如果受信任叢集的組態狀況不良，您必須解決這些組態不一致問題。可以透過修復受信任叢集來執行此操作。修復受信任叢集時，請確保受信任叢集中的所有受信任主機都具有相同的受信任組態。

受信任叢集由受信任 ESXi 主機的 vCenter Server 叢集組成，這些主機將由 Trust Authority 叢集遠端證明。最初設定 vSphere Trust Authority 時，您必須將 Trust Authority 叢集中的 Trust Authority 服務資訊匯入至受信任叢集中。受信任叢集將使用元件的組態，以與 Trust Authority 叢集上執行的金鑰提供者服務和證明服務進行連絡。如需有關設定受信任叢集這方面的詳細資訊，請參閱[將 Trust Authority 叢集資訊匯入至受信任的主機](#)。設定受信任叢集後，您可以檢查並修復其健全狀況。

檢查受信任叢集健全狀況

檢查受信任叢集的健全狀況取決於以下內容。

所需狀態組態

所需狀態組態是以匯入至受信任叢集中的 Trust Authority 服務資訊為基礎。所需狀態組態是受信任叢集的「實際來源」。將所需狀態組態視為設定受信任叢集時最初建立的內容。

已套用組態

已套用組態是指登錄為其設定了受信任叢集的特定證明服務和金鑰提供者服務。已套用組態是受信任叢集目前正在執行的內容。您可以將已套用組態視為「執行階段」組態。所需狀態組態應與已套用組態相符。但是，如果已套用組態與所需狀態組態不一致，則會將受信任叢集視為「狀況不良」。狀況不良的受信任叢集可能會出現效能降級或根本無法運作的情況。

此健全狀況檢查不是受信任叢集或 vSphere Trust Authority 基礎結構的整體健全狀況的指示器。健全狀況檢查僅將受信任叢集的所需狀態組態與已套用組態進行比較。

修復受信任叢集

修復是 vSphere Trust Authority 用來解決受信任叢集不一致組態的程序。隨著時間的推移或由於其他運作錯誤，受信任叢集的組態會變得不一致。

透過下列方式使用修復：

- 檢查受信任叢集健全狀況。
- 如果受信任叢集狀況不良，請進行修復。

可以使用 vSphere Client 或 CLI 來檢查受信任叢集健全狀況。請參閱[檢查受信任叢集健全狀況](#)。還可以使用 vSphere Client 或 CLI 來修復受信任叢集。請參閱[修復受信任叢集](#)。

備註 此外，將主機新增至現有的受信任叢集時也適合使用修復程序。請參閱[使用 vSphere Client 將主機新增到受信任叢集](#)和[使用 CLI 將主機新增到受信任叢集](#)。

檢查受信任叢集健全狀況

您可以使用 vSphere Client 或命令列檢查受信任叢集的健全狀況狀態。

必要條件

- 適用於受信任叢集的 vCenter Server 必須執行 vSphere 7.0 Update 1 或更新版本。
- 如果使用 PowerCLI，則需要 12.1.0 或更新版本。

程序

1 檢查受信任叢集健全狀況。

工具	步驟
vSphere Client	<ol style="list-style-type: none"> 使用 vSphere Client 連線到受信任叢集的 vCenter Server。 以 Trust Authority 管理員身分登入。 導覽至受信任叢集，選取設定，然後選取 Trust Authority。 按一下檢查健全狀況。
CLI	<ol style="list-style-type: none"> 在 PowerCLI 工作階段中，執行 Connect-VIServer cmdlet，以 Trust Authority 管理員身分連線至受信任叢集的 vCenter Server。 <div data-bbox="678 604 1377 657" data-label="Text"> <pre>Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'</pre> </div> 執行 Get-TrustedClusterAppliedStatus cmdlet，例如： <div data-bbox="678 743 1297 793" data-label="Text"> <pre>Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'</pre> </div>

2 如果發生錯誤，請參閱[修復受信任叢集](#)。

修復受信任叢集

您可以使用 vSphere Client 或命令列修復受信任叢集的組態。

必要條件

適用於受信任叢集的 vCenter Server 必須執行 vSphere 7.0 Update 1 或更新版本。

程序

1 連線至受信任叢集的 vCenter Server。

工具	步驟
vSphere Client	<ol style="list-style-type: none"> 使用 vSphere Client 連線到受信任叢集的 vCenter Server。 以 Trust Authority 管理員身分登入。
CLI	<p>在 PowerCLI 工作階段中，執行 Connect-VIServer cmdlet，以 Trust Authority 管理員身分連線至受信任叢集的 vCenter Server。</p> <div data-bbox="639 1514 1339 1566" data-label="Text"> <pre>Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'</pre> </div>

2 修復受信任叢集，然後重新檢查受信任叢集健全狀況。

工具	步驟
vSphere Client	<ol style="list-style-type: none"> 導覽至受信任叢集。 選取設定，然後選取 Trust Authority。 按一下修復。 按一下檢查健全狀況。
CLI	<ol style="list-style-type: none"> 將 Set-TrustedCluster cmdlet 與 -Remediate 參數搭配執行，例如： <pre>Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate</pre> 執行 Get-TrustedClusterAppliedStatus cmdlet，例如： <pre>Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'</pre>

在 vSphere 環境中使用加密

10

無論您使用的是標準金鑰提供者、受信任金鑰提供者還是 vSphere Native Key Provider，在 vSphere 環境中使用加密都需要進行一些準備工作。

請參閱以下資訊將您的環境設定為使用金鑰提供者：

- [第 7 章 設定和管理標準金鑰提供者](#)
- [第 8 章 設定和管理 vSphere Native Key Provider](#)
- [設定 vSphere Trust Authority](#)

設定您的環境之後，您可以使用 vSphere Client 建立已加密的虛擬機器和虛擬磁碟，以及加密現有虛擬機器和磁碟。

您可以透過使用 API 和 `crypto-util` CLI 執行其他工作。請參閱 vSphere Web Services SDK 程式設計指南以取得 API 說明文件，以及參閱 `crypto-util` 命令列說明以取得有關此工具的詳細資料。

本章節討論下列主題：

- [建立加密儲存區原則](#)
- [明確啟用主機加密模式](#)
- [使用 API 停用主機加密模式](#)
- [建立加密的虛擬機器](#)
- [複製加密的虛擬機器](#)
- [加密現有虛擬機器或虛擬磁碟](#)
- [解密已加密的虛擬機器或虛擬磁碟](#)
- [變更虛擬磁碟的加密原則](#)
- [解決缺少加密金鑰問題](#)
- [將鎖定的虛擬機器解除鎖定](#)
- [解決 ESXi 主機加密模式問題](#)
- [重新啟用 ESXi 主機加密模式](#)
- [設定金鑰伺服器憑證到期臨界值](#)
- [vSphere 虛擬機器加密和核心傾印](#)

- 在 ESXi 主機上啟用和停用金鑰持續性
- 使用 vSphere Client 對加密虛擬機器進行重設金鑰
- 使用 vSphere Client 設定預設金鑰提供者
- 使用 CLI 設定預設金鑰提供者

建立加密儲存區原則

您必須先建立加密儲存區原則，然後才能建立加密的虛擬機器。建立一次儲存區原則後，每次加密虛擬機器或虛擬磁碟時都指派該原則。

如果您想要搭配使用虛擬機器加密與其他 I/O 篩選器，或使用 vSphere Client 中的 **建立虛擬機器儲存區原則精靈**，請參閱 vSphere 儲存區說明文件以瞭解詳細資料。

必要條件

- 設定與金鑰提供者的連線。

雖然可以在沒有金鑰提供者連線的情況下建立虛擬機器加密儲存區原則，但您在無法在建立與金鑰提供者的信任連線之前執行加密工作。

- 所需權限：**密碼編譯作業.管理加密原則**。

程序

- 1 使用 vSphere Client 登入 vCenter Server。
- 2 選取**首頁**，按一下**原則和設定檔**，然後按一下**虛擬機器儲存區原則**。
- 3 按一下**建立**。
- 4 選取 vCenter Server，輸入原則名稱，(選擇性) 輸入說明，然後按**下一步**。
- 5 在**原則結構**頁面上，勾選**啟用基於主機的角色**，然後按**下一步**。
- 6 在**基於主機的服務**頁面上，選取**使用儲存區原則元件**，從下拉式功能表中選擇**預設加密內容**，然後按**下一步**。
- 7 在**儲存區相容性**頁面上，保持**相容**為選取狀態，選取資料存放區，然後按**下一步**。
- 8 檢閱資訊，然後按一下**完成**。

結果

虛擬機器加密儲存區原則將新增到清單中，並可在加密虛擬機器時使用。

明確啟用主機加密模式

如果您想在 ESXi 主機上執行加密工作 (如建立加密的虛擬機器)，則必須設定主機加密模式。在大多數情況下，當您執行加密工作時，會自動啟用主機加密模式。

有時，明確開啟加密模式是必要的。請參閱**虛擬機器加密工作的必要條件和所需權限**。

必要條件

所需權限：**Cryptographic operations.Register host**

程序

- 1 使用 vSphere Client 登入 vCenter Server。
- 2 瀏覽到 ESXi 主機，然後按一下**設定**。
- 3 在 [系統] 下，按一下**安全性設定檔**。
- 4 在 [主機加密模式] 面板中，按一下**編輯**。
- 5 選取**已啟用**，然後按一下**確定**。

使用 API 停用主機加密模式

如果使用者擁有足夠權限，則在使用者執行加密工作時，會自動啟用主機加密模式。啟用主機加密模式後，會加密所有核心傾印以避免敏感資訊洩漏給支援人員。如果您不再將虛擬機器加密用於 ESXi 主機，您可以停用加密模式。

為 ESXi 主機啟用加密模式後，可能需要將其停用。例如，可能需要停用加密模式才能產生 ESXi 支援服務包 (使用 `vm-support` 命令)。如果主機上存在金鑰材料，則主機加密模式切換 (主機 > 設定 > 安全性設定檔 > 編輯主機加密模式) 將無法運作。

透過叫用 `CryptoManagerHostDisable` API 方法，可以使用 API 停用主機加密模式。

為 ESXi 主機定義的密碼編譯模式或狀態包括：

- `pendingIncapable`：停用主機密碼編譯，即主機無法執行 vSphere 虛擬機器加密作業。
- `Incapable`：主機無法安全地接收敏感材料。
- `prepared`：主機已準備好接收敏感材料，但尚未設定主機金鑰。
- `safe`：主機已經過安全密碼編譯 (已啟用)，並已設定主機金鑰，即可以執行 vSphere 虛擬機器加密作業。

在主機上叫用 `CryptoManagerHostDisable` 後，主機的密碼編譯狀態將如下變更：

- 如果原始主機密碼編譯狀態為 `incapable` 或 `prepared`，則主機密碼編譯狀態將變更為 `incapable`。
- 如果原始主機密碼編譯狀態為 `safe`，則主機密碼編譯狀態將變更為 `pendingIncapable`。
- 如果主機密碼編譯狀態為 `pendingIncapable`，則主機密碼編譯狀態仍為 `pendingIncapable`。

此工作顯示了如何使用 vCenter Server 受管理物件瀏覽器 (MOB) 停用主機加密模式。如需有關使用 API 的詳細資訊，請參閱 vSphere Web Services API 說明文件，網址為 <https://developer.vmware.com/apis/968/vsphere>。

程序

- 1 以管理員身分登入 vCenter Server。
- 2 從要停用其加密模式的 ESXi 主機解除登錄所有加密虛擬機器。

3 存取 vCenter Server 上的 MOB。

```
https://vcenter_server/mob
```

4 在主機上叫用 `CryptoManagerHostDisable` 方法。

- a 在內容名稱下，按一下內容。
- b 在 `rootFolder` 下，按一下 **group-D1 (資料中心)**。
- c 在 `childEntity` 下，按一下相應的資料中心。
- d 在 `hostFolder` 下，按一下相應的主機。
- e 在 `childEntity` 下，按一下相應的叢集。
- f 在主機下，按一下相應的主機。
- g 在 `configManager` 下，按一下 **configManager**。
- h 在 `cryptoManager` 下，按一下 **CryptoManagerHost-*number***。
- i 按一下 **CryptoManagerHostDisable**。

主機密碼編譯狀態會變更為 `pendingIncapable` 或 `incapable`，具體取決於其原始密碼編譯狀態。

5 對要停用加密模式的其他主機重複步驟 4。

6 將主機重新開機。

結果

停用主機加密模式後，除非重新啟用主機加密模式，否則無法執行加密作業，例如新增已加密虛擬機器。

備註 將已停用加密模式的 ESXi 主機重新開機後，如果主機密碼編譯狀態最初為 `pendingIncapable`，則主機密碼編譯狀態仍為 `pendingIncapable`。若要重新啟用主機加密模式，請重新存取 vCenter Server MOB 並叫用 `ConfigureCryptoKey` API 方法。重新啟用主機加密模式時，如果主機密碼編譯狀態為 `pendingIncapable`，請使用原始主機金鑰識別碼。

建立加密的虛擬機器

您可以使用 vSphere Client 建立加密虛擬機器。

vSphere Client 依虛擬機器加密儲存區原則進行篩選，從而簡化加密虛擬機器的建立程序。

備註 建立加密的虛擬機器比加密現有虛擬機器速度更快，且使用更少的儲存資源。如果可能，請在建立期間加密虛擬機器。

必要條件

- 設定金鑰提供者並將其設定為預設值。
- 建立加密儲存區原則，或使用綁定的範例「虛擬機器加密原則」。
- 確定虛擬機器已關閉電源。

- 確認您具有必要權限：
 - **密碼編譯作業.加密新增項目**
 - 如果主機加密模式未處於 [已啟用] 狀態，則還需要**密碼編譯作業.登錄主機**。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。
- 3 在物件上按一下滑鼠右鍵，然後選取**新增虛擬機器**。
- 4 依照提示建立已加密的虛擬機器。

選項	動作
選取建立類型	建立新的虛擬機器。
選取名稱和資料夾	指定虛擬機器的唯一名稱和目標位置。
選取運算資源	指定您有權限為其建立加密虛擬機器的物件。請參閱 虛擬機器加密工作的必要條件和所需權限 。
選取儲存區	選取 加密此虛擬機器 核取方塊。將顯示包括加密的虛擬機器儲存區原則。選取虛擬機器儲存區原則 (配套的範例為虛擬機器加密原則)，然後選取相容的資料存放區。
選取相容性	選取相容性。您只能將加密的虛擬機器移轉到含有相容性 ESXi 6.5 及更新版本的主機中。
選取客體作業系統	選取打算稍後安裝在虛擬機器上的客體作業系統。
自訂硬體	<p>自訂硬體，例如，透過變更磁碟大小或 CPU。</p> <p>(選用) 選取虛擬機器選項索引標籤，然後展開加密。選取不進行加密的磁碟。當您取消選取磁碟時，僅加密虛擬機器首頁和任何其他選取的磁碟。</p> <p>會加密您新增的所有新硬碟。您可稍後變更個別硬碟的儲存區原則。</p>
即將完成	檢閱資訊，然後按一下 完成 。

複製加密的虛擬機器

使用相同的金鑰加密複製的加密虛擬機器，除非您變更金鑰。若要變更金鑰，可以使用 vSphere Client、PowerCLI 或 API。如果使用 PowerCLI 或 API，則只需一步即可複製加密的虛擬機器並變更金鑰。

您可以在複製期間執行下列作業。

- 從未加密的虛擬機器或範本虛擬機器建立加密的虛擬機器。
- 從加密的虛擬機器或範本虛擬機器建立解密的虛擬機器。
- 使用與來源虛擬機器金鑰不同的金鑰來雙重加密目的地虛擬機器。
- 從 vSphere 8.0 開始，對具有 vTPM 的虛擬機器選取**取代**選項時，會以新的空白 vTPM 開始，該 vTPM 將取得自己的金鑰和身分識別。

備註 vSphere 8.0 包含 `vpzd.clone.tpmProvisionPolicy` 進階設定，可將 vTPM 的預設複製行為設定為「取代」。

您可以從加密的虛擬機器建立即時複製虛擬機器，並注意即時複製品將與來源虛擬機器共用相同的金鑰。無法雙重加密來源或即時複製虛擬機器上的金鑰。

若要使用 API 複製加密機器，請參閱 vSphere Web Services SDK 程式設計指南。

必要條件

- 必須設定並啟用金鑰提供者。
- 建立加密儲存區原則，或使用綁定的範例「虛擬機器加密原則」。
- 所需權限 (適用於所有金鑰提供者)：
 - 密碼編譯作業.複製
 - 密碼編譯作業.加密
 - 密碼編譯作業.解密
 - 密碼編譯作業.雙重加密
 - 如果主機加密模式未處於 [已啟用] 狀態，則還需要密碼編譯作業.登錄主機權限。

程序

- 1 在 vSphere Client 詳細目錄中，瀏覽至虛擬機器。
- 2 若要建立已加密機器的複製品，請在虛擬機器上按一下滑鼠右鍵，選取**複製 > 複製到虛擬機器**，並依照提示進行操作。
 - a 在**選取名稱和資料夾**頁面中，指定名稱和用於複製的目標位置。
 - b 在**選取計算資源**頁面上，指定您擁有權限的物件。

- c (選擇性) 變更已複製 vTPM 的金鑰。

圖 10-1. 選取 TPM 佈建原則

VM-01 - Clone Existing Virtual Machine

1 Select a name and folder

2 Select a compute resource

3 Select TPM provision policy

4 Select storage

5 Select clone options

6 Ready to complete

Select TPM provision policy

TPM Provision Policy

☒ Copy ☐ Replace

⚠ The virtual machine clone will be created with exact copy of the TPM device and will continue to have access to the source virtual machine's secrets. This may result in unintentional secret exposure if the cloned virtual machine is compromised.

CANCEL BACK NEXT

複製虛擬機器會複製整個虛擬機器，包括 vTPM 及其可用於確定系統之身分識別的密碼。若要變更 vTPM 上的密碼，請對 **TPM 佈建原則** 選取取代。

備註 取代 vTPM 的密碼時，將取代所有金鑰，包括工作負載相關金鑰。最佳做法是，在取代金鑰之前，確保工作負載不再使用 vTPM。否則，已複製虛擬機器中的工作負載可能無法正常運作。

- d 在**選取儲存區**頁面中選取資料存放區。可以在複製作業進行時變更儲存區原則。例如，從使用加密原則變更為非加密原則會解密磁碟。
- e 在**選取複製選項**頁面上選取複製選項，如 vSphere 虛擬機器管理說明文件中所述。
- f 在**即將完成**頁面上，檢閱資訊並按一下**完成**。

3 (選擇性) 變更已複製虛擬機器的金鑰。

依預設，會使用與父系相同的金鑰建立複製的虛擬機器。最佳做法是變更已複製的虛擬機器金鑰，以確保多部虛擬機器沒有相同的金鑰。

- a 確定淺層或深度雙重加密。

若要使用不同的 DEK 和 KEK，請對已複製的虛擬機器執行深度雙重加密。若要使用不同的 KEK，請對已複製的虛擬機器執行淺層雙重加密。對於深度雙重加密，必須關閉虛擬機器電源。您可以在虛擬機器開啟電源且虛擬機器已有快照存在時執行淺層雙重加密作業。僅允許在單一快照分支 (磁碟鏈結) 上對具有快照的加密虛擬機器進行淺層雙重加密。不支援多個快照分支。如果淺層雙重加密在使用新 KEK 更新鏈結中的所有連結之前失敗，您仍可以存取加密的虛擬機器 (如果有舊 KEK 和新 KEK)。

- b 使用 API 對複製品執行雙重加密。請參閱 vSphere Web Services SDK 程式設計指南。

加密現有虛擬機器或虛擬磁碟

您可以透過變更現有虛擬機器或虛擬磁碟的儲存區原則進行加密。您只能為已加密的虛擬機器加密虛擬磁碟。

必要條件

- 設定金鑰提供者並將其設定為預設值。
- 建立加密儲存區原則，或使用綁定的範例「**虛擬機器加密原則**」。
- 確定虛擬機器已關閉電源。
- 確認您具有必要權限：
 - **密碼編譯作業.加密新增項目**
 - 如果主機加密模式未處於 [已啟用] 狀態，則還需要**密碼編譯作業.登錄主機**。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在想要變更的虛擬機器上按一下滑鼠右鍵，然後選取**虛擬機器原則** > **編輯虛擬機器儲存區原則**。
您可以設定虛擬機器檔案 (由虛擬機器首頁表示) 的儲存區原則，以及虛擬磁碟的儲存區原則。
- 3 選取儲存區原則。
 - 若要加密虛擬機器及其硬碟，請選取加密儲存區原則，然後按一下**確定**。
 - 若要加密虛擬機器而不加密虛擬磁碟，請開啟**針對每個磁碟設定**，為虛擬機器首頁選取加密儲存區原則，並為虛擬磁碟選取其他儲存區原則，然後按一下**確定**。
您無法加密未加密虛擬機器的虛擬磁碟。
- 4 如果您願意，可以從 vSphere Client 中的**編輯設定**功能表中加密虛擬機器或加密虛擬機器和磁碟。
 - a 在虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
 - b 選取**虛擬機器選項**索引標籤，然後開啟**加密**。選擇加密原則。如果取消選取所有磁碟，則僅會加密虛擬機器首頁。
 - c 按一下**確定**。

解密已加密的虛擬機器或虛擬磁碟

您可以透過變更儲存區原則來解密虛擬機器和/或其磁碟。

此工作說明如何使用 vSphere Client 解密已加密的虛擬機器。

所有已加密的虛擬機器均需要已加密的 vMotion。在虛擬機器解密期間，會保留 [已加密的 vMotion] 設定。若要變更此設定以不再使用 [已加密的 vMotion]，請明確變更此設定。

此工作說明如何使用儲存區原則執行解密。對於虛擬磁碟，您也可以使用**編輯設定**功能表執行解密。

必要條件

- 虛擬機器必須加密。
- 虛擬機器必須關閉電源或處於維護模式。
- 所需權限：**密碼編譯作業.解密**

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在想要變更的虛擬機器上按一下滑鼠右鍵，然後選取**虛擬機器原則 > 編輯虛擬機器儲存區原則**。
您可以設定虛擬機器檔案 (由虛擬機器首頁表示) 的儲存區原則，以及虛擬磁碟的儲存區原則。
- 3 選取儲存區原則。
 - 若要解密虛擬機器及其硬碟，請關閉**針對每個磁碟設定**，從下拉式功能表中選取儲存區原則，然後按一下**確定**。
 - 若要解密虛擬磁碟而不解密虛擬機器，請開啟**針對每個磁碟設定**，為虛擬機器首頁選取加密儲存區原則，並為虛擬磁碟選取其他儲存區原則，然後按一下**確定**。
您無法解密虛擬機器並將磁碟保留為已加密。
- 4 如果您願意，可以使用 vSphere Client 從**編輯設定**功能表中解密虛擬機器和磁碟。
 - a 在虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
 - b 選取**虛擬機器選項**索引標籤，然後展開**加密**。
 - c 若要解密虛擬機器及其硬碟，請從**加密虛擬機器**下拉式功能表中選擇**無**。
 - d 若要解密虛擬磁碟而不解密虛擬機器，請取消選取該磁碟。
 - e 按一下**確定**。
- 5 (選擇性) 可以變更 [已加密的 vMotion] 設定。
 - a 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。
 - b 按一下**虛擬機器選項**，然後開啟**加密**。
 - c 設定已加密的 vMotion 值。

變更虛擬磁碟的加密原則

從 vSphere Client 建立加密的虛擬機器時，您可以選擇加密在虛擬機器建立期間新增的哪些虛擬磁碟。您可以使用**編輯虛擬機器儲存區原則**選項解密虛擬磁碟。

備註 加密的虛擬機器可擁有未加密的虛擬磁碟。但是，未加密的虛擬機器不可擁有加密的虛擬磁碟。

請參閱**虛擬磁碟加密**。

此工作說明如何使用儲存區原則變更加密原則。您也可以使用**編輯設定**功能表進行此變更。

必要條件

- 您必須擁有**密碼編譯作業.管理加密原則**權限。
- 確定虛擬機器已關閉電源。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在虛擬機器上按一下滑鼠右鍵，然後選取**虛擬機器原則** > **編輯虛擬機器儲存區原則**。
- 3 變更儲存區原則。
 - 若要變更虛擬機器及其硬碟的儲存區原則，請選取加密儲存區原則，然後按一下**確定**。
 - 若要加密虛擬機器而不加密虛擬磁碟，請開啟**針對每個磁碟設定**，為虛擬機器首頁選取加密儲存區原則，並為虛擬磁碟選取其他儲存區原則，然後按一下**確定**。

您無法加密未加密虛擬機器的虛擬磁碟。
- 4 如果您願意，可以從**編輯設定**功能表中變更儲存區原則。
 - a 在虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
 - b 選取**虛擬硬體**索引標籤，展開硬碟，然後從下拉式功能表中選取加密原則。
 - c 按一下**確定**。

解決缺少加密金鑰問題

如果 ESXi 主機無法從 vCenter Server 取得加密虛擬機器或加密虛擬磁碟的金鑰 (KEK)，則加密虛擬機器將變為鎖定。使金鑰在金鑰伺服器 (KMS) 上可供使用後，您可以解除鎖定已加密的虛擬機器。

在某些情況下，使用標準金鑰提供者時，ESXi 主機無法從 vCenter Server 取得加密虛擬機器或加密虛擬磁碟的金鑰加密金鑰 (KEK)。在這種情況下，您仍可以解除登錄或重新載入虛擬機器。然而，您無法執行其他虛擬機器作業，例如開啟虛擬機器的電源。採取必要步驟使所需金鑰在金鑰伺服器上可供使用後，可以使用 vSphere Client 將鎖定的加密虛擬機器解除鎖定。

如果虛擬機器金鑰無法使用，vCenter Server 警示會向您發出通知，並且虛擬機器狀態會顯示為無效。該虛擬機器無法開啟電源。如果虛擬機器金鑰可用，但是已加密磁碟的金鑰無法使用，則虛擬機器狀態不會顯示為無效。但是，虛擬機器無法開啟電源並產生下列錯誤：

```
The disk [/path/to/the/disk.vmdk] is encrypted and a required key was not found.
```

備註 下列程序說明會導致虛擬機器變為鎖定狀態的情況，顯示的對應警示和事件記錄，以及在每個案例中要執行的動作。

程序

- 1 如果 vCenter Server 系統和金鑰伺服器之間的連線有問題，vCenter Server 將產生虛擬機器警示。此外，還會在事件記錄中顯示一條錯誤訊息。

還原與金鑰伺服器的連線。當金鑰伺服器與金鑰可供使用時，解除鎖定已鎖定的虛擬機器。請參閱[將鎖定的虛擬機器解除鎖定](#)。也可以將主機重新開機並重新登錄虛擬機器，以便在還原連線後將其解除鎖定。

中斷與金鑰伺服器的連線不會自動將虛擬機器鎖定。僅當滿足以下條件時，虛擬機器才會進入鎖定狀態：

- 該金鑰在 ESXi 主機上無法使用。
- vCenter Server 無法從金鑰伺服器擷取金鑰。

每次重新開機後，ESXi 主機必須能夠連線 vCenter Server。vCenter Server 從金鑰伺服器請求具有相應識別碼的金鑰，並使其可供 ESXi 使用。

備註 在 vSphere 7.0 Update 2 及更新版本中，可以在 ESXi 重新開機後保留加密金鑰。請參閱[ESXi 主機上的 vSphere 金鑰持續性](#)。

如果在還原與金鑰提供者的連線後虛擬機器仍保持鎖定狀態，請參閱[將鎖定的虛擬機器解除鎖定](#)。

- 2 如果連線已還原，請登錄虛擬機器。如果出現錯誤，或者雖然作業成功但虛擬機器處於鎖定狀態，請驗證您是否有 vCenter Server 系統的[密碼編譯作業.登錄虛擬機器](#)權限。

如果金鑰可用，則無需此權限即可開啟已加密虛擬機器的電源。如果必須擷取金鑰，則需要此權限來登錄虛擬機器。

- 3 如果金鑰伺服器上的金鑰不再可用，則 vCenter Server 會產生虛擬機器警示。此外，還會在事件記錄中顯示一條錯誤訊息。

要求金鑰伺服器管理員還原金鑰。如果您要開啟電源的虛擬機器已從詳細目錄中移除並且很長時間未登錄，您可能會遇到非作用中金鑰。如果您將 ESXi 主機重新開機，而金鑰伺服器不可用，也會發生此情況。

- a 使用受管理物件瀏覽器 (MOB) 或 vSphere API 擷取金鑰識別碼。

從 `VirtualMachine.config.keyId.keyId` 擷取 `keyId`。

- b 要求金鑰伺服器管理員重新啟動與該金鑰識別碼相關聯的金鑰。

- c 還原金鑰後，請參閱[將鎖定的虛擬機器解除鎖定](#)。

如果可在金鑰伺服器上還原金鑰，則 vCenter Server 會擷取此金鑰，並在下次需要時將其推送至 ESXi 主機。

- 4 如果金鑰伺服器可供存取且 ESXi 主機已開啟電源，但是 vCenter Server 系統無法使用，請遵循這些步驟解除鎖定虛擬機器。

- a 還原 vCenter Server 系統，或設定不同的 vCenter Server 系統，然後與金鑰伺服器建立信任。

您必須使用相同的金鑰提供者名稱，但金鑰伺服器 IP 位址可以不同。

- b 登錄所有鎖定的虛擬機器。

新的 vCenter Server 執行個體會從金鑰伺服器擷取金鑰，並且虛擬機器會解除鎖定。

- 5 如果只有 ESXi 主機上的金鑰遺失，則 vCenter Server 會產生虛擬機器警示並在事件記錄中顯示下列訊息：

由於主機上的金鑰遺失，虛擬機器已鎖定。

vCenter Server 系統可以從金鑰提供者擷取遺失金鑰。不需要手動復原金鑰。請參閱[將鎖定的虛擬機器解除鎖定](#)。

將鎖定的虛擬機器解除鎖定

當已加密的虛擬機器處於鎖定狀態時，vCenter Server 警示會通知您。採取必要步驟使所需金鑰在金鑰伺服器上可供使用後，可以使用 vSphere Client 將鎖定的加密虛擬機器解除鎖定。

必要條件

- 確認您具有所需權限：[密碼編譯作業.登錄虛擬機器](#)
- 執行選擇性工作可能需要其他權限，例如啟用主機加密。
- 解除鎖定已鎖定的虛擬機器之前，請查明鎖定原因，並嘗試手動修正此問題。請參閱[解決缺少加密金鑰問題](#)。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 導覽至虛擬機器的[摘要索引標籤](#)。
當虛擬機器鎖定時，會顯示虛擬機器已鎖定警示。
- 3 決定是否要確認警示，還是將警示重設為綠色，但不立即解除鎖定虛擬機器。
當您按一下[確認](#)或[重設為綠色](#)時，警示會消失，但虛擬機器會在解除鎖定之前保持鎖定狀態。
- 4 導覽至虛擬機器的[監控索引標籤](#)，然後按一下[事件](#)以取得有關為何鎖定虛擬機器的詳細資訊。
- 5 在解除鎖定虛擬機器之前執行建議的疑難排解。
- 6 導覽至虛擬機器的[摘要索引標籤](#)，然後按一下位於虛擬機器主控台下方的[解除鎖定虛擬機器](#)。
此時會顯示一則訊息，警告加密金鑰資料已傳輸到主機。
- 7 按一下[是](#)。

解決 ESXi 主機加密模式問題

在某些情況下，ESXi 主機的加密模式會變為停用。

在包含任何已加密的虛擬機器的情況下，ESXi 主機需要啟用主機加密模式。如果主機偵測到其主機金鑰遺失，或如果金鑰提供者不可用，則主機可能無法啟用加密模式。當無法啟用主機加密模式時，vCenter Server 會產生警示。

程序

- 1 如果 vCenter Server 系統和金鑰提供者之間的連線有問題，則會產生警示並在事件記錄中顯示錯誤訊息。
必須還原與包含相關加密金鑰的金鑰提供者的連線。
- 2 如果金鑰遺失，則會產生警示並在事件記錄中顯示錯誤訊息。
必須確保金鑰存在於金鑰提供者中。有關從備份還原的資訊，請參閱說明文件以瞭解金鑰管理廠商。

後續步驟

還原與金鑰提供者的連線或手動將金鑰復原至金鑰提供者之後，如果主機加密模式仍保持停用狀態，請重新啟用主機加密模式。請參閱[重新啟用 ESXi 主機加密模式](#)。

重新啟用 ESXi 主機加密模式

從 vSphere 6.7 開始，vCenter Server 警示會在 ESXi 主機的加密模式變為停用時通知您。如果主機加密模式已停用，您可以重新啟用此模式。

必要條件

- 驗證您具有所需權限：[密碼編譯作業.登錄主機](#)。
- 重新啟用加密模式之前，請查明原因，並嘗試手動修正此問題。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 導覽到 ESXi 主機的**摘要**索引標籤。
停用加密模式時，會顯示 [主機需要啟用加密模式] 警示。
- 3 決定是否確認警示，還是將警示重設為綠色，但不立即重新啟用主機加密模式。
當您按一下**確認**或**重設為綠色**時，警示會消失，但主機的加密模式會在重新啟用之前保持停用狀態。
- 4 導覽到 ESXi 主機的**監控**索引標籤，然後按一下**事件**。
隨即顯示有關停用加密模式的原因的更多資訊。執行建議的疑難排解，然後重新啟用加密模式。
- 5 在**摘要**索引標籤中，按一下**啟用主機加密模式**以重新啟用主機加密。
此時會顯示一則訊息，警告加密金鑰資料已傳輸到主機。
- 6 按一下**是**。

設定金鑰伺服器憑證到期臨界值

依預設，vCenter Server 會在金鑰伺服器 (KMS) 憑證到期前 30 天通知您。您可以變更此預設值。

金鑰伺服器憑證具有到期日期。達到到期日期的臨界值時，會顯示一則警示通知您。

vCenter Server 和金鑰伺服器交換兩種類型的憑證：伺服器和用戶端。vCenter Server 系統上的 VMware Endpoint 憑證存放區 (VECS) 會儲存伺服器憑證以及每個金鑰提供者一個用戶端憑證。由於提供兩種憑證類型，因此每種憑證類型有兩個警示（一個用於用戶端，一個用於伺服器）。

程序

- 1 使用 vSphere Client 登入 vCenter Server 系統。
- 2 在物件階層中，選取 vCenter Server 系統。
- 3 按一下**設定**。
- 4 在**設定**下，按一下**進階設定**，然後按一下**編輯設定**。
- 5 按一下**篩選器**圖示並輸入 `vpxd.kmscert.threshold`，或捲動到組態參數本身。
- 6 輸入您的值 (以天為單位)，然後按一下**儲存**。

vSphere 虛擬機器加密和核心傾印

如果您的環境使用 vSphere 虛擬機器加密，且 ESXi 主機上發生錯誤，則產生的核心傾印會加密以保護客戶資料。此外，vm-support 套件中包含的核心傾印也會加密。

備註 核心傾印可能包含敏感資訊。處理核心傾印時，請遵循您組織的資料安全性和隱私權政策。

ESXi 主機上的核心傾印

當 ESXi 主機、使用者環境或虛擬機器出現故障時，會產生核心傾印，並且主機將重新開機。如果 ESXi 主機已啟用加密模式，會使用 ESXi 金鑰快取中的金鑰加密核心傾印。(根據使用的金鑰提供者，金鑰來自外部金鑰伺服器、金鑰提供者服務或 vCenter Server)。如需背景資訊，請參閱 [vSphere 虛擬機器加密如何保護您的環境](#)。

當 ESXi 主機「安全無憂」時，會產生核心傾印，並建立一個事件。此事件表示發生了核心傾印，並顯示下列資訊：環境名稱、發生時間、用於加密核心傾印的金鑰的 keyID，以及核心傾印檔案名稱。您可以在 vCenter Server 之**工作和事件**下的「事件」檢視器中檢視事件。

下表顯示依 vSphere 版本列出的用於每個核心傾印類型的加密金鑰。

表 10-1. 核心傾印加密金鑰

核心傾印類型	加密金鑰 (ESXi6.5)	加密金鑰 (ESXi6.7 及更新版本)
ESXi 核心	主機金鑰	主機金鑰
使用者環境 (hostd)	主機金鑰	主機金鑰
加密的虛擬機器 (VM)	主機金鑰	虛擬機器金鑰

在 ESXi 主機重新開機後可執行的動作，視多個因素而定。

- 在大多數情況下，金鑰提供者會在重新開機後嘗試將金鑰推送到 ESXi 主機。如果此作業成功，您可以產生 vm-support 套件，並且可以解密或重新加密此核心傾印。請參閱[解密或重新加密已加密的核心傾印](#)。
- 如果 vCenter Server 無法連線至 ESXi 主機，您可能能夠擷取金鑰。請參閱[解決缺少加密金鑰問題](#)。
- 如果主機使用自訂金鑰，且該金鑰不同於 vCenter Server 推送給主機的金鑰，則您無法操縱核心傾印。請避免使用自訂金鑰。

核心傾印和 vm-support 套件

當您因嚴重錯誤連絡 VMware 技術支援時，您的支援代表通常會要求您產生 vm-support 套件。此套件包含記錄檔和其他資訊，包括核心傾印。如果支援代表無法透過查看記錄檔和其他資訊解決此問題，他們可能會要求您解密核心傾印並提供相關資訊。若要保護金鑰等敏感資訊，請遵循組織的安全性和隱私權政策。請參閱[針對使用加密的 ESXi 主機收集 vm-support 套件](#)。

vCenter Server 系統上的核心傾印

vCenter Server 系統上的核心傾印未加密。vCenter Server 已包含潛在的敏感資訊。至少確保 vCenter Server 受到保護。請參閱[第 4 章 保護 vCenter Server 系統的安全](#)。您也可以考慮關閉 vCenter Server 系統的核心傾印。記錄檔中的其他資訊可協助判定此問題。

針對使用加密的 ESXi 主機收集 vm-support 套件

如果已為 ESXi 主機啟用主機加密模式，則 vm-support 套件中的所有核心傾印皆已加密。您可以從 vSphere Client 收集套件，如果打算稍後解密核心傾印，您可以指定密碼。

vm-support 套件包含記錄檔、核心傾印檔案等。

必要條件

通知您的支援代表已針對 ESXi 主機啟用主機加密模式。您的支援代表可能會要求您解密核心傾印並擷取相關資訊。

備註 核心傾印可能包含敏感資訊。請遵循組織的安全性和隱私權政策以保護敏感資訊 (如主機金鑰)。

程序

- 1 使用 vSphere Client 登入 vCenter Server 系統。
- 2 按一下**主機和叢集**，然後在 ESXi 主機上按一下滑鼠右鍵。
- 3 選取**匯出系統記錄**。
- 4 在對話方塊中，選取**已加密核心傾印的密碼**，然後指定並確認密碼。
- 5 其他選項保留預設值，或進行變更 (如果 VMware 技術支援要求)，然後按一下**匯出記錄**。
- 6 指定檔案的位置。

- 7 如果您的支援代表要求您解密 `vm-support` 套件中的核心傾印，請登入任一 ESXi 主機並遵循下列步驟。

- a 登入 ESXi 並連線至 `vm-support` 套件所在的目錄。

檔案名稱遵循 `esx.date_and_time.tgz` 模式。

- b 確保有足夠的空間來儲存套件、未壓縮的套件和重新壓縮的套件，或移動套件。
- c 將套件解壓縮到本機目錄。

```
vm-support -x *.tgz .
```

產生的檔案階層可能包含 ESXi 主機的核心傾印檔案 (通常位於 `/var/core` 中)，並且可能包含虛擬機器的多個核心傾印檔案。

- d 分別解密每個加密的核心傾印檔案。

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

`vm-support-incident-key-file` 為您在目錄頂層找到的事件金鑰檔案。

`encryptedZdump` 為加密的核心傾印檔案的名稱。

`decryptedZdump` 為命令產生的檔案的名稱。讓該名稱與 `encryptedZdump` 名稱類似。

- e 提供您在建立 `vm-support` 套件時所指定的密碼。
- f 移除加密的核心傾印，並再次壓縮套件。

```
vm-support --reconstruct
```

- 8 移除包含機密資訊的任何檔案。

解密或重新加密已加密的核心傾印

您可以透過使用 `crypto-util` CLI 解密或重新加密 ESXi 主機上的加密核心傾印。

您可以親自解密並檢查 `vm-support` 套件中的核心傾印。核心傾印可能包含敏感資訊。請遵循您組織的安全性和隱私權政策以保護金鑰等敏感資訊。

如需有關重新加密 `crypto-util` 的核心傾印和其他功能的詳細資料，請參閱命令列說明。

備註 `crypto-util` 適用於進階使用者。

必要條件

用於加密核心傾印的金鑰必須在產生核心傾印的 ESXi 主機上可用。

程序

- 1 直接登入發生核心傾印的 ESXi 主機。

如果 ESXi 主機處於鎖定模式，或者如果 SSH 存取已停用，您可能必須首先啟用存取。

2 判斷核心傾印是否已加密。

選項	說明
監控核心傾印	<code>crypto-util envelope describe vmmcores.ve</code>
zdump 檔案	<code>crypto-util envelope describe --offset 4096 zdumpFile</code>

3 解密核心傾印 (視其類型而定)。

選項	說明
監控核心傾印	<code>crypto-util envelope extract vmmcores.ve vmmcores</code>
zdump 檔案	<code>crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted</code>

在 ESXi 主機上啟用和停用金鑰持續性

必須在 ESXi 主機上啟用金鑰持續性。預設為不啟用。

如需有關金鑰持續性的概念資訊，請參閱 [ESXi 主機上的 vSphere 金鑰持續性](#)。

必要條件

啟用金鑰持續性的需求：

- ESXi 7.0 Update 2 或更新版本
- ESXi 主機安裝有 TPM 2.0
- 可以存取 ESXCLI 命令集。您可以遠端執行 ESXCLI 命令，或在 ESXi Shell 中執行。

備註 使用 vSphere Native Key Provider 時，不需要金鑰持續性。vSphere Native Key Provider 設計為立即可用，無需存取金鑰伺服器即可執行。

為了增強安全性，TPM 還可使用封裝原則，以防止在 ESXi 主機重新開機期間竄改。請參閱 [什麼是 TPM 封裝原則](#)。

程序

- 1 使用 SSH 或其他遠端主控台連線，以啟動 ESXi 主機上的工作階段。
- 2 以 root 身分登入。

3 啟用或停用金鑰持續性。

- a 若要啟用金鑰持續性，請執行以下作業：

```
esxcli system security keypersistence enable
```

- b 若要停用持續性，請執行以下作業：

```
esxcli system security keypersistence disable --remove-all-stored-keys
```

使用 vSphere Client 對加密虛擬機器進行重設金鑰

可以使用 vSphere Client 對加密的虛擬機器執行淺層重設金鑰。可能會出於業務或符合性原因對加密虛的擬機器執行重設金鑰。

淺層重設金鑰或重設金鑰 (也稱為淺層重設金鑰) 可讓您在加密的虛擬機器上使用新的 (及不同的) 金鑰加密金鑰 (KEK)。可以在虛擬機器開啟電源時執行重設金鑰作業。如果虛擬機器已有快照存在，也可以執行重設金鑰。僅允許在單一快照分支 (磁碟鏈結) 上對具有快照的加密虛擬機器進行重設金鑰。不支援多個快照分支。如果重設金鑰在使用新 KEK 更新鏈結中的所有連結之前失敗，您仍可以存取加密的虛擬機器 (如果有舊 KEK 和新 KEK)。

必要條件

所需權限：**密碼編譯作業.管理金鑰伺服器**

程序

- 1 使用 vSphere Client 登入 vCenter Server 系統。
- 2 瀏覽詳細目錄清單並選取加密的虛擬機器。
- 3 在加密的虛擬機器上按一下滑鼠右鍵，然後選取**虛擬機器原則**。
- 4 選取**重新加密**。
- 5 按一下**是**。

加密的虛擬機器將使用新 KEK 重設金鑰。

備註 如果重設金鑰失敗，事件子系統將張貼以下事件：

```
com.vmware.vc.vm.crypto.RekeyFail
```

使用 vSphere Client 設定預設金鑰提供者

在下列情況下必須設定預設金鑰提供者：沒有將第一個金鑰提供者設為預設金鑰提供者，或是您的環境使用多個金鑰提供者，而您移除了預設金鑰提供者。您可以使用 vSphere Client 在 vCenter Server 層級設定預設金鑰提供者。

必要條件

最佳做法是確認 [金鑰提供者] 索引標籤中的 [連線狀態] 是否顯示 [作用中] 和綠色核取記號。

程序

- 1 使用 vSphere Client 登入。
- 2 導覽到 vCenter Server。
- 3 按一下**設定**，然後選取**安全性**下的**金鑰提供者**。
- 4 選取金鑰提供者。
- 5 按一下**設定為預設值**。

此時將顯示確認對話方塊。

- 6 按一下**設定為預設值**。

金鑰提供者會顯示為目前的預設值。

使用 CLI 設定預設金鑰提供者

在下列情況下必須設定預設金鑰提供者：沒有將第一個金鑰提供者設為預設金鑰提供者，或是您的環境使用多個金鑰提供者，而您移除了預設金鑰提供者。您可以使用 PowerCLI 在 vCenter Server 層級、叢集層級或叢集資料夾層級設定預設金鑰提供者。

必要條件

最佳做法是確認 [金鑰提供者] 索引標籤中的 [連線狀態] 是否顯示 [作用中] 和綠色核取記號。

您必須擁有包含 **密碼編譯作業.管理 KMS** 權限的角色。在 vSphere Trust Authority 中，該角色必須套用至受信任叢集。

程序

- 1 確保您已經以管理員身分連線到您建立金鑰提供者的 vCenter Server。

備註 在 vSphere Trust Authority 中，連線到受信任叢集的 vCenter Server。

```
Connect-VIServer -server VC_ip_address -User admin_user -Password 'password'
```

- 2 取得金鑰提供者。

```
Get-KeyProvider
```

您可以使用 `-Name keyprovider` 選項來指定單一金鑰提供者。

- 3 將 `Get-KeyProvider` 金鑰提供者資訊指派給變數。

例如，此命令會將資訊指派給變數 `$kp`。

```
$kp = Get-KeyProvider
```

如果您有多個金鑰提供者，可以使用 `Select-Object` 選取其中一個。

```
$kp = Get-KeyProvider | Select-Object -Index 0
```

4 使用以下 PowerCLI 命令之一。

設定預設值的位置	命令
vCenter Server 層級	<code>Set-KeyProvider -KeyProvider \$kp -DefaultForSystem</code>
叢集層級	<p>此範例命令為叢集 <code>CL-01</code> 設定金鑰提供者。</p> <pre>Add-EntityDefaultKeyProvider -KeyProvider \$kp -Entity 'CL-01'</pre>
叢集資料夾層級	<p>此範例命令為叢集資料夾 <code>Cluster-Folder-01</code> 設定金鑰提供者。</p> <pre>Add-EntityDefaultKeyProvider -KeyProvider \$kp -Entity 'Cluster-Folder-01'</pre>

使用虛擬信賴平台模組保護虛擬機器

11

透過虛擬信賴平台模組 (vTPM) 功能，可以將 TPM 2.0 虛擬密碼處理器新增至虛擬機器。

vTPM 是實體信賴平台模組 2.0 晶片的基於軟體的表示。vTPM 可像任何其他虛擬裝置一樣運作。您可以使用與新增虛擬 CPU、記憶體、磁碟控制器或網路控制器的相同方式，將 vTPM 新增至虛擬機器。vTPM 不需要硬體信賴平台模組晶片。

本章節討論下列主題：

- [什麼是虛擬信賴平台模組](#)
- [使用虛擬信賴平台模組建立虛擬機器](#)
- [為現有虛擬機器新增虛擬信賴平台模組](#)
- [從虛擬機器移除虛擬信賴平台模組](#)
- [識別已啟用虛擬信賴平台模組的虛擬機器](#)
- [檢視虛擬信賴平台模組裝置憑證](#)
- [匯出並取代虛擬信賴平台模組裝置憑證](#)

什麼是虛擬信賴平台模組

虛擬信賴平台模組 (vTPM) 是實體信賴平台模組 2.0 晶片的基於軟體的表示。vTPM 可像任何其他虛擬裝置一樣運作。

vTPM 提供以硬體為基礎的安全相關功能，例如隨機數字產生、證明、金鑰產生等。新增至虛擬機器時，vTPM 可讓客體作業系統建立和儲存私有金鑰。這些金鑰不會向客體作業系統本身公開。因此，會減少虛擬機器攻擊面。通常，破壞客體作業系統會破壞其密碼，但啟用 vTPM 可大幅降低此風險。這些金鑰僅供客體作業系統用於加密或簽署。透過連結 vTPM，用戶端可以遠端證明虛擬機器的身分，並驗證其正在執行的軟體。

vTPM 不需要 ESXi 主機上存在實體信賴平台模組 (TPM) 2.0 晶片。但是，如果您想要執行主機證明，則需要 TPM 2.0 實體晶片等外部實體。請參閱[使用信賴平台模組保護 ESXi 主機](#)。

備註 依預設，沒有儲存區原則與已啟用 vTPM 的虛擬機器相關聯。僅加密虛擬機器檔案 (虛擬機器主檔案)。如果您願意，可以選擇為虛擬機器及其磁碟明確新增加密，但虛擬機器檔案已加密。

如何為虛擬機器設定 vTPM

從虛擬機器角度來看，vTPM 是一個虛擬裝置。您可以將 vTPM 新增至新虛擬機器或現有的虛擬機器。vTPM 依賴虛擬機器加密來保護重要的 TPM 資料，因此，要求您設定金鑰提供者。設定 vTPM 時，會加密虛擬機器檔案而非磁碟。您可以選擇為虛擬機器及其磁碟明確新增加密。

備份已啟用 vTPM 的虛擬機器時，備份必須包含所有虛擬機器資料，包括 *.nvram 檔案。如果您的備份未包含 *.nvram 檔案，則無法使用 vTPM 還原虛擬機器。此外，由於啟用 vTPM 之虛擬機器的虛擬機器主檔案已加密，請確保加密金鑰在還原時可供使用。

從 vSphere 8.0 開始，在複製具有 vTPM 的虛擬機器時，針對具有 vTPM 的虛擬機器選取**取代**選項時，會從一個新的空白 vTPM 開始，該 vTPM 將取得自己的密碼和身分識別。取代 vTPM 的密碼時，將取代所有金鑰，包括工作負載相關金鑰。最佳做法是，在取代金鑰之前，確保工作負載不再使用 vTPM。否則，已複製虛擬機器中的工作負載可能無法正常運作。

針對 vTPM 的 vSphere 要求

若要使用 vTPM，您的 vSphere 環境必須符合下列需求：

- 虛擬機器需求：
 - EFI 韌體
 - 硬體版本 14 及更新版本
- 元件需求：
 - 針對 Windows 虛擬機器要求 vCenter Server 6.7 及更新版本，針對 Linux 虛擬機器要求 vCenter Server 7.0 Update 2 及更新版本。
 - 虛擬機器加密 (加密虛擬機器主檔案)。
 - 為 vCenter Server 設定的金鑰提供者。請參閱 [vSphere 金鑰提供者的比較](#)。
- 客體作業系統支援：
 - Linux
 - Windows Server 2008 及更新版本
 - Windows 7 及更新版本

硬體 TPM 和虛擬 TPM 之間的差異

使用硬體信賴平台模組 (TPM) 為認證或金鑰提供安全儲存區。vTPM 與 TPM 執行相同的功能，但在軟體中執行密碼編譯副處理器功能。vTPM 使用 *.nvram 檔案做為其安全的儲存區，該檔案透過虛擬機器加密進行加密。

硬體 TPM 包含預先載入的金鑰，稱為簽署金鑰 (EK)。EK 具有私密和公開金鑰。EK 為 TPM 提供唯一的身分識別。對於 vTPM，將由 VMware Certificate Authority (VMCA) 或第三方憑證授權機構 (CA) 提供此金鑰。一旦 vTPM 使用某個金鑰，該金鑰通常不會變更，因為這樣做會導致 vTPM 中儲存的敏感資訊失效。vTPM 在任何時候都不會連絡第三方 CA。

使用虛擬信賴平台模組建立虛擬機器

您可以在建立虛擬機器時新增虛擬信賴平台模組 (vTPM)，以增強客體作業系統的安全性。必須先建立金鑰提供者，然後才能新增 vTPM。

VMware 虛擬 TPM 與 TPM 2.0 相容，並且會建立啟用 TPM 的虛擬晶片以供虛擬機器及其裝載的客體作業系統使用。

必要條件

- 確保您的 vSphere 環境已設定金鑰提供者。如需詳細資訊，請參閱以下內容：
 - [設定 vSphere Trust Authority](#)
 - [第 7 章 設定和管理標準金鑰提供者](#)
 - [第 8 章 設定和管理 vSphere Native Key Provider](#)
- 您使用的客體作業系統可以是 Windows Server 2008 及更新版本、Windows 7 及更新版本或 Linux。
- 在您環境中執行的 ESXi 主機必須是 ESXi 6.7 或更新版本 (Windows 客體作業系統) 或 7.0 Update 2 (Linux 客體作業系統)。
- 虛擬機器必須使用 EFI 韌體。
- 確認您具有必要權限：
 - [密碼編譯作業.複製](#)
 - [密碼編譯作業.加密](#)
 - [密碼編譯作業.加密新增項目](#)
 - [密碼編譯作業.移轉](#)
 - [密碼編譯作業.登錄虛擬機器](#)

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。
- 3 在物件上按一下滑鼠右鍵，選取**新虛擬機器**，然後遵循提示來建立虛擬機器。

選項	動作
選取建立類型	建立新的虛擬機器。
選取名稱和資料夾	指定名稱和目標位置。
選取運算資源	指定您有權限為其建立虛擬機器的物件。請參閱 虛擬機器加密工作的必要條件和所需權限 。
選取儲存區	選取相容的資料存放區。
選取相容性	必須為 Windows 客體作業系統選取 ESXi 6.7 及更新版本 ，或為 Linux 客體作業系統選取 ESXi 7.0 U2 及更新版本 。

選項	動作
選取客體作業系統	選取 Windows 或 Linux 以用作客體作業系統。
自訂硬體	按一下 新增裝置 ，然後選取 信賴平台模組 。 您可以進一步自訂硬體，例如，透過變更磁碟大小或 CPU。
即將完成	檢閱資訊，然後按一下 完成 。

結果

啟用 vTPM 的虛擬機器即顯示在您所指定的詳細目錄中。

為現有虛擬機器新增虛擬信賴平台模組

您可以將虛擬信賴平台模組 (vTPM) 新增至現有虛擬機器，以增強客體作業系統的安全性。必須先建立金鑰提供者，然後才能新增 vTPM。

VMware 虛擬 TPM 與 TPM 2.0 相容，並且會建立啟用 TPM 的虛擬晶片以供虛擬機器及其裝載的客體作業系統使用。

必要條件

- 確保您的 vSphere 環境已設定金鑰提供者。如需詳細資訊，請參閱以下內容：
 - [設定 vSphere Trust Authority](#)
 - [第 7 章 設定和管理標準金鑰提供者](#)
 - [第 8 章 設定和管理 vSphere Native Key Provider](#)
- 您使用的客體作業系統可以是 Windows Server 2008 及更新版本、Windows 7 及更新版本或 Linux。
- 確認已關閉虛擬機器。
- 在您環境中執行的 ESXi 主機必須是 ESXi 6.7 或更新版本 (Windows 客體作業系統) 或 7.0 Update 2 (Linux 客體作業系統)。
- 虛擬機器必須使用 EFI 韌體。
- 確認您具有必要權限：
 - [密碼編譯作業.複製](#)
 - [密碼編譯作業.加密](#)
 - [密碼編譯作業.加密新增項目](#)
 - [密碼編譯作業.移轉](#)
 - [密碼編譯作業.登錄虛擬機器](#)

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。

- 2 在您想要修改的詳細目錄中的虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
- 3 在 [編輯設定] 對話方塊中，按一下**新增裝置**，然後選取**信賴平台模組**。
- 4 按一下**確定**。

虛擬機器的**摘要索引標籤**的**虛擬機器硬體**窗格中現在會包括 [虛擬信賴平台模組]。

從虛擬機器移除虛擬信賴平台模組

您可以從虛擬機器移除虛擬信賴平台模組 (vTPM) 安全性。

移除 vTPM 裝置會導致虛擬機器上的所有加密資訊變得無法復原。從虛擬機器移除 vTPM 之前，停用客體作業系統中使用 BitLocker 等 vTPM 裝置的所有應用程式。如果執行此操作失敗，可能會導致虛擬機器無法開機。此外，無法從包含快照的虛擬機器中移除 vTPM。

必要條件

- 確定虛擬機器已關閉電源。
- 確認您具有必要權限：**密碼編譯作業.解密**

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在您想要修改的詳細目錄中的虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
- 3 在 [編輯設定] 對話方塊的**虛擬硬體**索引標籤中，找到信賴平台模組項目。
- 4 將指標移至裝置上方，然後按一下**移除圖示**。

只有可安全移除的虛擬硬體才會顯示此圖示。

- 5 按一下**刪除**以確認您要移除裝置。

vTPM 裝置已標記為移除。

- 6 按一下**確定**。

確認虛擬信賴平台模組項目不再顯示於虛擬機器的**摘要索引標籤**的**虛擬機器硬體**窗格中。

識別已啟用虛擬信賴平台模組的虛擬機器

您可以識別哪些虛擬機器能夠使用虛擬信賴平台模組 (vTPM)。

您可以產生詳細目錄中所有虛擬機器的清單，其中顯示虛擬機器名稱、作業系統和 vTPM 狀態。您也可以將此清單匯出至 CSV 檔案，以用於合規性稽核。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 選取 vCenter Server 執行個體、主機或叢集。
- 3 按一下**虛擬機器**索引標籤，然後按一下**虛擬機器**。

- 4 若要檢視已啟用 TPM 的所有虛擬機器，請按一下左下角的三列**資料行選取器**，然後選取 **TPM**。

TPM 資料行針對已啟用 TPM 的虛擬機器顯示為「存在」。未啟用 TPM 的虛擬機器會列為「不存在」。

- 5 您可以將詳細目錄清單視圖的內容匯出至 CSV 檔案。

- a 按一下清單視圖右下角的**匯出**。

[匯出清單內容] 對話方塊隨即開啟，並列出 CSV 檔案中包含項目的可用選項。

- b 選取是要將全部資料列還是目前所選的資料列列在 CSV 檔案中。
- c 透過可用選項，選取要列在 CSV 檔案中的資料行。
- d 按一下**匯出**。

CSV 檔案隨即產生且可供下載。

檢視虛擬信賴平台模組裝置憑證

虛擬信賴平台模組 (vTPM) 裝置預先設定了預設憑證，您可以檢閱這些憑證。

必要條件

您的環境中必須具有已啟用 vTPM 的虛擬機器。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。
- 3 按一下**虛擬機器**，然後按一下**虛擬機器**。
- 4 選取要檢視其憑證資訊的已啟用 vTPM 的虛擬機器。

如有必要，請按一下左下角的三列**資料行選取器**，然後選取 **TPM** 以顯示 TPM 為「存在」的虛擬機器。

- 5 按一下**設定索引標籤**。
- 6 在 **TPM** 下，選取**憑證**。
- 7 選取憑證並檢視其資訊。
- 8 (選擇性) 若要匯出憑證資訊，請按一下**匯出**。

憑證會儲存到磁碟。

後續步驟

您可以使用第三方憑證授權機構 (CA) 核發的憑證取代預設憑證。請參閱[匯出並取代虛擬信賴平台模組裝置憑證](#)。

匯出並取代虛擬信賴平台模組裝置憑證

您可以取代虛擬信賴平台模組 (vTPM) 裝置隨附的預設憑證。

必要條件

您的環境中必須具有已啟用 vTPM 的虛擬機器。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。
- 3 在想要取代其憑證資訊的詳細目錄中，選取已啟用 vTPM 的虛擬機器。
- 4 按一下 **設定** 索引標籤。
- 5 在 **TPM** 下，選取 **簽署要求**。
- 6 選取憑證。
- 7 若要匯出憑證資訊，請按一下 **匯出**。
憑證會儲存到磁碟。
- 8 根據匯出的憑證簽署要求 (CSR) 取得第三方憑證授權機構 (CA) 核發的憑證。
您可以使用 IT 環境中可能具有的任何 CA。
- 9 如果您有新的憑證，請取代現有憑證。
 - a 在您想要取代其憑證的詳細目錄中的虛擬機器上按一下滑鼠右鍵，然後選取 **編輯設定**。
 - b 在 **編輯設定** 對話方塊中，展開 **安全性裝置**，然後展開 **信賴平台模組**。
將顯示憑證。
 - c 針對您想要取代的憑證，按一下 **取代**。
將顯示 **檔案上傳** 對話方塊。
 - d 在您的本機機器上，找到新憑證並上傳。
新憑證會取代 vTPM 裝置隨附的預設憑證。
 - e 在虛擬機器的 [摘要] 索引標籤的 **虛擬信賴平台模組** 清單下，憑證名稱將會更新。

透過虛擬式安全性保護 Windows 客體作業系統

12

在 vSphere 6.7 及更新版本中，您可以在支援的 Windows 客體作業系統上啟用 Microsoft 虛擬化型安全性 (VBS)。

Microsoft VBS 是 Windows 10 和 Windows Server 2016 作業系統中引入的一項功能，可使用硬體和軟體虛擬化透過建立隔離、受 Hypervisor 限制的專用子系統來增強系統安全性。

VBS 可讓您使用下列 Windows 安全性功能來強化系統，並隔離關鍵系統和使用者密碼使其不受影響：

- Credential Guard：旨在隔離和強化關鍵系統和使用者密碼使其不受影響。
- Device Guard：提供一組功能，旨在共同運作來防止及避免惡意程式碼在 Windows 系統上執行。
- 可設定的程式碼完整性：可確保只有受信任的程式碼可從開機載入器開始執行。

如需詳細資訊，請參閱 Microsoft 說明文件中有關虛擬式安全性的主題。

透過 vCenter Server 為虛擬機器啟用 VBS 之後，您可以在 Windows 客體作業系統內啟用 VBS。

本章節討論下列主題：

- [vSphere 虛擬式安全性最佳做法](#)
- [在虛擬機器上啟用虛擬式安全性](#)
- [在現有虛擬機器上啟用以虛擬化為基礎的安全性](#)
- [在客體作業系統上啟用以虛擬化為基礎的安全性](#)
- [停用以虛擬化為基礎的安全性](#)
- [識別已啟用 VBS 的虛擬機器](#)

vSphere 虛擬式安全性最佳做法

請遵循虛擬式安全性 (VBS) 的最佳做法，盡可能地提高 Windows 客體作業系統環境的安全性和管理性。

遵循這些最佳做法來避免出現問題。

VBS 硬體需求

針對 VBS 使用下列硬體：

- Intel
 - Haswell CPU 或更新版本。為獲得最佳效能，請使用 Skylake-EP CPU 或更新版本。

- Ivy Bridge CPU 是可接受的。
- Sandy Bridge CPU 可能會導致部分效能降低。
- AMD
 - Zen 2 系列 CPU (Rome) 或更新版本。
 - 舊版本的 CPU 可能會導致效能降低。

針對「關於頁面大小變更的機器檢查例外狀況」Intel CPU 漏洞的緩解措施可能會在 VBS 使用時對客體作業系統效能產生負面影響。如需詳細資訊，請參閱 VMware 知識庫文章，網址為 <https://kb.vmware.com/kb/76050>。

VBS 和 Windows 客體作業系統相容性

在 Intel 上，雖然 Windows Server 2016 版本 1607 和 1703 需要修補程式，但 Windows 10、Windows Server 2016 和更新版本的虛擬機器支援 VBS。查看 Microsoft 說明文件以瞭解 ESXi 主機硬體相容性。若要使用 Intel CPU 實現 VBS，需要使用 vSphere 6.7 或更新版本以及硬體版本 14 或更新版本。

在 AMD 上，Windows 10 版本 1809 和 Windows 2019 及更新版本的虛擬機器支援 VBS。若要使用 AMD CPU 實現 VBS，需要使用 vSphere 7.0 Update 2 或更新版本及硬體版本 19 或更新版本。

Windows 10 最初要求啟用 Hyper-V 後才能實現 VBS。Windows 10 不要求啟用 Hyper-V。Windows Server 2016 及更新版本也同樣適用。如需詳細資訊，請參閱目前的 Microsoft 說明文件和《VMware vSphere 版本說明》。

VBS 上不支援的 VMware 功能

啟用 VBS 時，虛擬機器不支援下列功能：

- Fault Tolerance
- PCI 傳遞
- CPU 或記憶體熱新增

VBS 的安裝和升級注意須知

設定 VBS 之前，請瞭解下列安裝和升級注意須知：

- 在低於版本 14 的虛擬硬體版本上針對 Windows 10 和 Windows Server 2016 及更新版本設定的新虛擬機器，預設為使用舊版 BIOS 進行建立。將虛擬機器的韌體類型從舊版 BIOS 變更為 UEFI 後，您必須重新安裝客體作業系統。
- 如果您計劃將虛擬機器從舊版 vSphere 移轉至 vSphere 6.7 或更新版本，並且在虛擬機器上啟用 VBS，請使用 UEFI 來避免重新安裝作業系統。

在虛擬機器上啟用虛擬式安全性

建立虛擬機器的同時，可以為支援的 Windows 客體作業系統啟用 Microsoft 虛擬式安全性 (VBS)。

設定 VBS 的程序涉及首先在虛擬機器中啟用 VBS，然後在 Windows 客體作業系統中啟用 VBS。

必要條件

如需可接受的 CPU，請參閱 [vSphere 虛擬式安全性最佳做法](#)。

要使用 Intel CPU 實現 VBS，需要使用 vSphere 6.7 或更新版本。建立使用硬體版本 14 或更新版本以及下列其中一個支援的客體作業系統的虛擬機器：

- Windows 10 (64 位元) 或更新版本
- Windows Server 2016 (64 位元) 或更新版本

要使用 AMD CPU 實現 VBS，需要使用 vSphere 7.0 Update 2 或更新版本。建立使用硬體版本 19 或更新版本以及下列其中一個支援的客體作業系統的虛擬機器：

- Windows 10 (64 位元) 版本 1809 或更新版本
- Windows Server 2019 (64 位元) 或更新版本

在啟用 VBS 之前，請確保已安裝 Windows 10 版本 1809 和 Windows Server 2019 的最新修補程式。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在詳細目錄中選取一個物件，此物件必須為虛擬機器的有效父系物件，例如 ESXi 主機或叢集。
- 3 在物件上按一下滑鼠右鍵，選取**新虛擬機器**，然後遵循提示來建立虛擬機器。

選項	動作
選取建立類型	建立虛擬機器。
選取名稱和資料夾	指定名稱和目標位置。
選取運算資源	指定您有權限為其建立虛擬機器的物件。
選取儲存區	在虛擬機器儲存區原則中，選取儲存區原則。選取相容的資料存放區。
選取相容性	Intel CPU：確保選取 ESXi 6.7 及更新版本 。 AMD CPU：確保選取 ESXi 7.0 U2 及更新版本 。
選取客體作業系統	選取與作業系統版本最相符的 Windows 客體作業系統選項。 選取 啟用 Windows 虛擬式安全性 核取方塊。
自訂硬體	自訂硬體，例如，透過變更磁碟大小或 CPU。
即將完成	檢閱資訊，然後按一下 完成 。

結果

摘要索引標籤下的 [虛擬機器詳細資料] 動態磚顯示「**虛擬化型安全性 - 啟用**」。

後續步驟

請參閱[在客體作業系統上啟用以虛擬化為基礎的安全性](#)。

在現有虛擬機器上啟用以虛擬化為基礎的安全性

您可以為支援的 Windows 客體作業系統在現有虛擬機器上啟用 Microsoft 虛擬式安全性 (VBS)。

設定 VBS 的程序涉及首先在虛擬機器中啟用 VBS，然後在客體作業系統中啟用 VBS。

備註 在低於版本 14 的硬體版本上針對 Windows 10、Windows Server 2016 和 Windows Server 2019 設定的新虛擬機器，預設為使用舊版 BIOS 進行建立。如果將虛擬機器的韌體類型從舊版 BIOS 變更為 UEFI，您必須重新安裝客體作業系統。

必要條件

如需可接受的 CPU，請參閱 [vSphere 虛擬式安全性最佳做法](#)。

要使用 Intel CPU 實現 VBS，需要使用 vSphere 6.7 或更新版本。必須已使用硬體版本 14 或更新版本，以及下列其中一個支援的客體作業系統建立虛擬機器：

- Windows 10 (64 位元) 或更新版本
- Windows Server 2016 (64 位元) 或更新版本

要使用 AMD CPU 實現 VBS，需要使用 vSphere 7.0 Update 2 或更新版本。必須已使用硬體版本 19 或更新版本、以及下列其中一個支援的客體作業系統建立虛擬機器：

- Windows 10 (64 位元) 版本 1809 或更新版本
- Windows Server 2019 (64 位元) 或更新版本

在啟用 VBS 之前，請確保已安裝 Windows 10 版本 1809 和 Windows Server 2019 的最新修補程式。

程序

- 1 在 vSphere Client 中，瀏覽到虛擬機器。
- 2 在虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
- 3 按一下**虛擬機器選項索引標籤**。
- 4 針對虛擬式安全性選取**啟用核取方塊**。
- 5 按一下**確定**。

結果

摘要索引標籤下的 [虛擬機器詳細資料] 動態磚顯示「**虛擬化型安全性 - 啟用**」。

後續步驟

請參閱[在客體作業系統上啟用以虛擬化為基礎的安全性](#)。

在客體作業系統上啟用以虛擬化為基礎的安全性

您可以為支援的 Windows 客體作業系統啟用 Microsoft 虛擬式安全性 (VBS)。

從 Windows 客體作業系統內啟用 VBS。Windows 會透過群組原則物件 (GPO) 設定和強制執行 VBS。GPO 可讓您關閉和開啟各種服務，例如 VBS 提供的安全開機、Device Guard 和 Credential Guard。某些 Windows 版本還需要您執行啟用 Hyper-V 平台的其他步驟。

如需詳細資料，請參閱有關部署 Device Guard 以啟用虛擬式安全性的 Microsoft 說明文件。

必要條件

- 確定虛擬機器上已啟用虛擬式安全性。

程序

- 1 在 Microsoft Windows 中，編輯群組原則以開啟 VBS 並選擇其他與 VBS 相關的安全性選項。
- 2 (選擇性) 對於低於 Redstone 4 的 Microsoft Windows 版本，請在 Windows 功能控制台中啟用 Hyper-V 平台。
- 3 將客體作業系統重新開機。

停用以虛擬化為基礎的安全性

如果您無法再對虛擬機器使用虛擬式安全性 (VBS)，您可以停用 VBS。針對虛擬機器停用 VBS 時，Windows VBS 選項保持不變，但可能會引發效能問題。在虛擬機器上停用 VBS 之前，請停用 Windows 內的 VBS 選項。

必要條件

確定虛擬機器已關閉電源。

程序

- 1 在 vSphere Client 中，瀏覽到使用 VBS 的虛擬機器。
如需有關尋找使用 VBS 的虛擬機器的說明，請參閱[識別已啟用 VBS 的虛擬機器](#)。
- 2 在虛擬機器上按一下滑鼠右鍵，然後選取**編輯設定**。
- 3 按一下**虛擬機器選項**。
- 4 針對虛擬式安全性取消選取**啟用核取方塊**。
會出現訊息提醒您在客體作業系統停用 VBS。
- 5 按一下**確定**。
- 6 請確認虛擬機器的**摘要索引標籤**不會再在客體作業系統說明中顯示「VBS true」。

識別已啟用 VBS 的虛擬機器

您可以識別哪些虛擬機器已啟用 VBS，用於進行報告和符合性。

程序

- 1 透過使用 vSphere Client 連線至 vCenter Server。
- 2 在詳細目錄中選取 vCenter Server 執行個體、資料中心或主機。
- 3 按一下**虛擬機器索引標籤**，然後按一下**虛擬機器**。
- 4 若要顯示 VBS 資料行，請按一下左下角的三列**資料行選取器**，然後選取 VBS 核取方塊。
- 5 掃描 VBS 資料行中是否「存在」。

確保 vSphere 網路安全

13

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。

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。

使用防火牆

為虛擬網路新增防火牆保護，方法是在其中的部分或所有虛擬機器上安裝和設定以主機為基礎的防火牆。

為提高效率，您可以設定私人虛擬機器乙太網路或虛擬網路。有了虛擬網路，您可以在虛擬網路最前面的虛擬機器上安裝以主機為基礎的防火牆。此防火牆可以用作實體網路介面卡和虛擬網路中剩餘虛擬機器之間的保護緩衝區。

以主機為基礎的防火牆可能會降低效能。請先根據效能目標平衡安全性需求，然後在虛擬網路中的其他虛擬機器上安裝以主機為基礎的防火牆。

請參閱[使用防火牆確保網路安全](#)。

使用網路分割

將主機中的不同虛擬機器區域置於不同網路區段。如果將每個虛擬機器區域隔離在各自的網路區段中，可以大大降低區域之間洩漏資料的風險。分割可防止多種威脅，包括位址解析通訊協定 (ARP) 詐騙。使用 ARP 詐騙，攻擊者可操縱 ARP 資料表以重新對應 MAC 和 IP 位址，從而存取進出主機的網路流量。攻擊者使用 ARP 詐騙產生攔截式 (MITM) 攻擊、執行拒絕服務 (DoS) 攻擊、劫持目標系統，並以其他方式破壞虛擬網路。

仔細規劃分割可減少虛擬機器區域之間封包傳輸的機會。因此，分割可防止嗅探攻擊 (嗅探攻擊需向受害者傳送網路流量)。此外，攻擊者無法使用一個虛擬機器區域中的不安全服務存取主機中的其他虛擬機器區域。可以使用兩種方法之一實作分割。

- 為虛擬機器區域使用單獨的實體網路介面卡，確保已將區域隔離。為虛擬機器區域使用單獨的實體網路介面卡可能是最安全的方法。在建立初始區段之後，此方法更不容易出現錯誤組態。
- 設定虛擬區域網路 (VLAN)，協助保護網路。VLAN 幾乎能夠提供實際實作單獨網路所具有的所有安全性優點，且不增加硬體額外負荷。VLAN 可為您節省部署和維護其他裝置、纜線等成本。請參閱[透過 VLAN 保護虛擬機器的安全](#)。

防止對虛擬機器進行未經授權的存取

保護虛擬機器安全的需求通常與保護實體機器安全的需求相同。

- 如果將虛擬機器網路連線到實體網路，將會遭到破壞，就像由實體機器組成的網路一樣。
- 即使您不將某個虛擬機器連線到實體網路，該虛擬機器也會遭到其他虛擬機器的攻擊。

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的存取。保護虛擬機器免受此類未經授權的存取。

如需有關保護虛擬機器的其他資訊，請參閱標題為「虛擬機器 (VM) 保護的安全虛擬網路組態」的 NIST 文件，網址為：

<https://csrc.nist.gov/publications/detail/sp/800-125b/final>

本章節討論下列主題：

- [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](#)
- [標準交換器保護和 VLAN](#)
- [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 主機內建立多個網路](#)
- [在 ESXi 主機上使用網際網路通訊協定安全性](#)
- [確保 SNMP 組態正確](#)
- [vSphere 網路安全性最佳做法](#)

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 VMware 產品 (包括 vSphere 和 vSAN) 中所有支援的連接埠和通訊協定的清單，請參閱 VMware Ports and Protocols Tool™，網址為 <https://ports.vmware.com/>。可以依 VMware 產品搜尋連接埠、建立自訂連接埠清單，以及列印或儲存連接埠清單。

針對具有 vCenter Server 的組態設定防火牆

如果要透過 vCenter Server 存取 ESXi 主機，通常會使用防火牆來保護 vCenter Server。

必須在進入點佈設防火牆。防火牆可能位於用戶端和 vCenter Server 或 vCenter Server 之間，並且用戶端均可受防火牆保護。

如需 VMware 產品 (包括 vSphere 和 vSAN) 中所有支援的連接埠和通訊協定的清單，請參閱 VMware Ports and Protocols Tool™，網址為 <https://ports.vmware.com/>。可以依 VMware 產品搜尋連接埠、建立自訂連接埠清單，以及列印或儲存連接埠清單。

設定了 vCenter Server 的網路可透過 vSphere Client、其他 UI 用戶端或使用 vSphere API 的用戶端接收通訊。在一般作業期間，vCenter Server 會在指定的連接埠上接聽來自其受管理的主機和用戶端的資料。vCenter Server 還假定其受管理主機會在指定的連接埠上接聽來自 vCenter Server 的資料。如果在其中任一元素之間存在防火牆，必須確保防火牆中有開啟的連接埠可支援資料傳輸。

您可能還可以在網路中的其他存取點處佈設防火牆，具體取決於網路使用量及用戶端所需的安全性層級。根據網路組態的安全性風險，選取防火牆位置。通常使用以下防火牆位置。

- 在 vSphere 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 Client 與 ESXi 主機之間 (如果使用者透過 vSphere Client 存取虛擬機器)。此連線是 vSphere Client 與 vCenter Server 之間連線的補充，它需要一個不同的連接埠。
- 在 vCenter Server 與 ESXi 主機之間。
- 在網路中的 ESXi 主機之間。儘管主機之間的流量通常被認為是受信任的，但是，如果您擔心電腦間存在安全性缺口，可以在主機間新增防火牆。

如果要在 ESXi 主機間新增防火牆，並打算在這些主機間移轉虛擬機器，則在將來源主機和目標主機分隔開的任何防火牆中開啟連接埠。

- 在 ESXi 主機與網路儲存區 (如 NFS 或 iSCSI 儲存區) 之間。這些連接埠並非專屬於 VMware。可根據網路規格進行設定。

透過防火牆連線到 vCenter Server

在防火牆中開啟 TCP 連接埠 443，讓 vCenter Server 能夠接收資料。

依預設，vCenter Server 使用 TCP 連接埠 443 來接聽其用戶端的資料。如果您在 vCenter Server 及其用戶端之間設有防火牆，必須設定可讓 vCenter Server 從用戶端接收資料的連線。防火牆組態取決於您的站台所使用的內容，請連絡您的本機防火牆系統管理員以取得相關資訊。

透過防火牆連線 ESXi 主機

如果您在 ESXi 主機及 vCenter Server 之間設有防火牆，請確保受管理的主機能夠接收資料。

若要設定用於接收資料的連線，請開啟用於 vSphere High Availability、vMotion、vSphere Fault Tolerance 等服務的流量的連接埠。如需組態檔、vSphere Client 存取權限，以及防火牆命令的討論，請參閱**設定 ESXi 防火牆**。如需連接埠清單，請參閱 VMware Ports and Protocols Tool™，網址為 <https://ports.vmware.com>。

針對沒有 vCenter Server 的組態設定防火牆

如果您的環境不包含 vCenter Server，用戶端可以直接連線到 ESXi 網路。

您可以使用數種方式連線到獨立 ESXi 主機。

- VMware Host Client
- ESXCLI 介面
- vSphere Web Services SDK 或 vSphere Automation SDK
- 第三方用戶端

獨立主機的防火牆需求與存在 vCenter Server 時的需求相似。

- 使用防火牆保護 ESXi 層，或保護用戶端及 ESXi 層，具體取決於您的組態。該防火牆可為網路提供基本保護。
- 此類組態中的授權是您在每個主機上安裝的 ESXi 套件的一部分。由於授權功能駐留在 ESXi 上，因此無需帶防火牆的單獨授權伺服器。

您可以使用 ESXCLI 或使用 VMware Host Client 設定防火牆連接埠。請參閱 vSphere 單一主機管理 - VMware Host Client。

透過防火牆連線到虛擬機器主控台

特定連接埠必須開啟，使用者和管理員才能與虛擬機器主控台通訊。必須開啟哪些連接埠會視虛擬機器主控台的類型，以及是透過包含 vSphere Client 的 vCenter Server 連線還是直接從 VMware Host Client 連線到 ESXi 主機而定。

如需有關連接埠、用途和分類 (傳入、傳出或雙向) 的詳細資訊，請參閱 VMware Ports and Protocols Tool™，網址為 <https://ports.vmware.com>。

透過 vSphere Client 連線到以瀏覽器為基礎的虛擬機器主控台

使用 vSphere 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 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 Client 在連接埠 443 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 Client 連線到 VMware Remote Console

如果使用 vSphere Client 並連線到 VMware Remote Console (VMRC)，則必須可進行下列存取：

- 防火牆必須允許 vSphere Client 在連接埠 443 上存取 vCenter Server。
- 防火牆必須允許 VMRC 存取連接埠 443 上的 vCenter Server，並存取連接埠 902 (對於 11.0 之前的 VMRC 版本) 和連接埠 443 (對於 VMRC 11.0 版及更高版本) 上的 ESXi 主機。如需有關 VMRC 11.0 版和 ESXi 連接埠需求的詳細資訊，請參閱 VMware 知識庫文章，網址為 <https://kb.vmware.com/s/article/76672>。

使用 VMware Host Client 直接連線到 ESXi 主機

如果直接連線到 ESXi 主機，則可以使用 VMware Host Client 虛擬機器主控台。

備註 請勿使用 VMware Host Client 直接連線到由 vCenter Server 系統管理的主機。如果您透過 VMware Host Client 對此類主機進行變更，會導致環境不穩定。

防火牆必須允許在連接埠 443 和 902 上存取 ESXi 主機

VMware Host Client 使用連接埠 902 為虛擬機器上的客體作業系統 MKS 活動提供連線。使用者正是透過此連接埠，與虛擬機器的客體作業系統及應用程式進行互動。VMware 不支援為此功能設定不同的連接埠。

確保實體交換器安全

確保每個 ESXi 主機上實體交換器的安全，以防止攻擊者取得主機及其虛擬機器的存取權。

為了最好地保護主機，請確保實體交換器連接埠已設定為停用跨距樹狀目錄，並確保為外部實體交換器和虛擬交換器 (在虛擬交換器標記 (VST) 模式下) 之間的主幹連結設定了非干涉選項。

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。

為了防止實體交換器受到潛在的拒絕服務 (DoS) 攻擊，可以在 ESXi 主機上開啟客體 BPDU 篩選器。

- 3 登入實體交換器，並確保已連線 ESXi 主機的實體交換器連接埠上尚未啟用動態主幹連線通訊協定 (DTP)。
- 4 如果實體交換器連接埠已連線到虛擬交換器 VLAN 主幹連線連接埠，則定期檢查實體交換器連接埠來確保它們已正確設定為主幹連接埠。

使用安全性原則確保標準交換器連接埠安全

標準交換器上的 VMkernel 連接埠群組或虛擬機器連接埠群組具有可設定的安全性原則。安全性原則決定您對虛擬機器強制執行的防模擬和截斷攻擊保護的強度。

與實體網路介面卡一樣，虛擬機器網路介面卡可以模擬另一台虛擬機器。模擬會造成安全性風險。

- 虛擬機器可以傳送可能來自不同電腦的畫面，以便其可以接收針對該電腦的網路畫面。
- 可以對虛擬機器網路介面卡加以設定，從而接收針對其他電腦的畫面。

在為標準交換器新增 VMkernel 連接埠群組或虛擬機器連接埠群組時，ESXi 會為群組中的連接埠設定安全性原則。可以使用此安全性原則確保主機能防止其虛擬機器的客體作業系統模擬網路中的其他電腦。可能會嘗試模擬的客體作業系統偵測不到模擬行為已被阻止。

安全性原則決定您對虛擬機器強制執行的防模擬和截斷攻擊保護的強度。若要正確使用安全性設定檔中的設定，請參閱 vSphere 網路文件中的〈安全性原則〉一節。本節說明：

- 虛擬機器網路介面卡如何控制傳輸。
- 此層級的攻擊如何進行。

保護 vSphere Standard Switch 的安全

您可以透過限制一些虛擬機器網路介面卡的 MAC 位址模式，來保護標準交換器流量不受第 2 層的攻擊。

每個虛擬機器網路介面卡均具有一個初始 MAC 位址和一個有效的 MAC 位址。

初始 MAC 位址

建立介面卡時將指派初始 MAC 位址。儘管可以從客體作業系統外部重新設定初始 MAC 位址，但客體作業系統無法變更初始 MAC 位址。

有效 MAC 位址

每個介面卡都具有一個有效 MAC 位址，可篩選出目的地 MAC 位址與有效 MAC 位址不同的傳入網路流量。客體作業系統負責設定有效 MAC 位址，且通常使有效 MAC 位址與初始 MAC 位址相符。

建立虛擬機器網路介面卡時會發生什麼

虛擬機器網路介面卡建立後，其有效 MAC 位址與初始 MAC 位址相同。客體作業系統可隨時將有效 MAC 位址更改為其他值。如果作業系統變更了有效 MAC 位址，其網路介面卡將接收傳送到新 MAC 位址的網路流量。

透過網路介面卡傳送封包時，客體作業系統通常會將其介面卡的有效 MAC 位址輸入乙太網路畫面的來源 MAC 位址欄位中。它還會將接收網路介面卡的 MAC 位址輸入目的地 MAC 位址欄位中。僅當封包中的目的地 MAC 位址與其自身有效的 MAC 位址相符時，接收介面卡才接受封包。

作業系統可傳送具有模擬來源 MAC 位址的畫面。因此作業系統可以模擬接收網路授權的網路介面卡，並且對網路中的裝置發起惡意攻擊。

使用安全性原則保護連接埠和群組

透過在連接埠群組或連接埠上設定安全性原則，防止虛擬流量受到模擬和第 2 層攔截攻擊。

分散式連接埠群組和連接埠上的安全性原則包含下列選項：

- MAC 位址變更 (請參閱 [MAC 位址變更](#))
- 混合模式 (請參閱[混合模式作業](#))
- 偽造的傳輸 (請參閱[偽造的傳輸](#))

您可以透過選取與 vSphere 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。透過此選項，虛擬機器能夠接收 Mac 位址不同於 VMX 中所設定位址的框架。

當 **MAC 位址變更** 選項設定為**接受**時，ESXi 接受將虛擬機器的有效 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 不接受將虛擬機器的有效 MAC 位址變更為不同於初始 MAC 位址的其他位址的要求。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。

備註 從 vSphere 7.0 開始，**偽造的傳輸**和 **MAC 位址變更**的預設值變更為了「拒絕」，而不是「接受」。請連絡您的儲存裝置廠商進行驗證。

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。

備註 從 vSphere 7.0 開始，**偽造的傳輸**和 **MAC 位址變更**的預設值變更為「拒絕」，而不是「接受」。

混合模式作業

混合模式會消除虛擬機器介面卡執行的任何接收篩選，因此客體作業系統將接收在網路上觀察到的所有流量。依預設，虛擬機器介面卡不能在混合模式中運作。

儘管混合模式對於追蹤網路活動很有用，但它是一種不安全的運作模式，因為混合模式中的任何介面卡均可存取封包，即使某些封包僅由特定的網路介面卡接收也是如此。這表示，虛擬機器中的管理員或根使用者可以檢視傳送至其他客體或主機作業系統的流量。

如需為混合模式設定虛擬機器介面卡的相關資訊，請參閱 vSphere 網路說明文件中有關為 vSphere Standard Switch 或標準連接埠群組設定安全性原則的主題。

備註 有時，您可能確實需要將標準虛擬交換器或分散式虛擬交換器設定為在混合模式中運作 (例如，執行網路入侵偵測軟體或封包嗅探器時)。

標準交換器保護和 VLAN

VMware 標準交換器可提供保護，以抵禦對 VLAN 安全性的特定威脅。標準交換器的設計方式可保護 VLAN 免受多種攻擊，其中包含 VLAN 跳躍。

具備此保護功能並不保證您的虛擬機器組態不容易遭受其他類型的攻擊。例如，標準交換器不會保護實體網路免受這些攻擊；標準交換器僅可保護虛擬網路。

標準交換器和 VLAN 可抵禦以下類型的攻擊。

由於新的安全威脅會隨著時間不斷進化，因此請勿認為此表已詳盡列出所有攻擊。請定期檢查 Web 上的 VMware 安全性資源，以瞭解安全性、最新安全性警示，以及 VMware 安全性策略的相關資訊。

MAC 填滿

MAC 填滿透過含有標記為來自多個不同來源之 MAC 位址的封包以填滿交換器。許多交換器使用關聯記憶體資料表來瞭解和儲存每個封包的來源位址。當資料表已滿時，交換器就會進入完全開放狀態，其中的每個傳入封包便會在所有連接埠上廣播，讓攻擊者看見交換器上的所有流量。此狀態可能會導致 VLAN 間的封包洩漏。

雖然 VMware 標準交換器會儲存 MAC 位址資料表，但是標準交換器不會從可觀察到的流量中取得 MAC 位址，而且不容易遭受此類型的攻擊。

802.1q 和 ISL 標記攻擊

802.1q 和 ISL 標記攻擊透過讓交換器充當主幹並將流量廣播至其他 VLAN，以強制交換器將框架從某個 VLAN 重新導向至另一個 VLAN。

VMware 標準交換器不會執行此攻擊類型所需的動態主幹連線，因此不容易遭受此類攻擊。

雙重封裝攻擊

雙重封裝攻擊會在攻擊者建立雙重封裝封包時發生，此類封包中內部標籤的 VLAN 識別碼與外部標籤的 VLAN 識別碼不同。為了回溯相容，原生 VLAN 會從已傳輸的封包去除外部標籤，除非另以其他方式設定。當原生 VLAN 交換器去除外部標籤時僅會剩下內部標籤，這個內部標籤會將封包路由至與在目前遺失的外部標籤中所識別到的不同 VLAN。

VMware 標準交換器會在針對特定 VLAN 設定的連接埠上，置放虛擬機器嘗試傳送的任何雙重封裝框架。因此，VMware 標準交換器不容易遭受此類型的攻擊。

多點傳送暴力密碼破解攻擊

與幾乎同時傳送大量多點傳送框架至已知的 VLAN 有關，這會使交換器超載，如此一來交換器便會錯誤地允許部分框架廣播至其他 VLAN。

VMware 標準交換器不允許框架離開其正確的廣播網域 (VLAN)，因此不容易遭受此類型的攻擊。

跨距樹狀目錄攻擊

跨距樹狀目錄攻擊以跨距樹狀目錄通訊協定 (STP) 為攻擊目標，此通訊協定通常用來控制 LAN 各部分間的橋接。攻擊者會傳送嘗試變更網路拓撲的橋接通訊協定資料單位 (BPDU) 封包，以將其自行建立為根橋接。建立為根橋接後，攻擊者便可窺探已傳輸框架的內容。

VMware 標準交換器不支援 STP，因此不容易遭受此類型的攻擊。

隨機框架攻擊

隨機框架攻擊與傳送大量封包有關，封包中的來源和目的地地址保持不變，但欄位的長度、類型或內容卻隨機遭到變更。此攻擊的目標是強制交換器錯誤地將封包路由至不同的 VLAN。

VMware 標準交換器不容易遭受此類型的攻擊。

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。

標準交換器中的規則同樣適用於 vSphere Distributed Switch 中的 VLAN。如需詳細資訊，請參閱 [標準交換器保護和 VLAN](#)。

程序

- 1 對於具有靜態繫結的分散式連接埠群組，停用自動展開功能。

自動展開功能預設為啟用。

若要停用自動展開功能，請使用 vSphere Web Services SDK 或命令列介面，設定分散式連接埠群組下的 `autoExpand` 內容。請參閱《vSphere Web Services SDK》說明文件。

- 2 請確保已完整記錄所有 vSphere Distributed Switch 的全部私人 VLAN 識別碼。
- 3 如果您在 dvPortgroup 上使用 VLAN 標記，則 VLAN 識別碼必須對應於外部 VLAN 感知上游交換器上的識別碼。如果未正確地追蹤 VLAN 識別碼，錯誤地重複使用識別碼可能會允許非預期的流量。同樣地，錯誤或遺失的 VLAN 識別碼可能會讓流量不流經實體和虛擬機器。
- 4 請確保與 vSphere Distributed Switch 關聯的虛擬連接埠群組上不存在任何未使用的連接埠。
- 5 標記所有 vSphere Distributed Switch。

與 ESXi 主機相關聯的 vSphere Distributed Switch 需要交換器名稱所對應的文字方塊。此標籤用作交換器的功能性描述元，如同與實體交換器相關聯的主機名稱。vSphere Distributed Switch 上的標籤指示交換器的功能或 IP 子網路。例如，您可以將交換器標示為內部以指示其僅適用於虛擬機器之私人虛擬交換器上的內部網路。沒有任何流量通過實體網路介面卡。

- 6 如果未使用網路健全狀況檢查，請針對 vSphere Distributed Switch 將停用。

依預設已停用網路健全狀況檢查。啟用後，健全狀況檢查封包將包含攻擊者可能會使用之主機、交換器及連接埠的相關資訊。僅將網路健全狀況檢查用於疑難排解，並在疑難排解完成後將其關閉。

- 7 透過在連接埠群組或連接埠上設定安全性原則，防止虛擬流量受到模擬和第 2 層攔截攻擊。

分散式連接埠群組和連接埠上的安全性原則包含下列選項：

- MAC 位址變更 (請參閱 [MAC 位址變更](#))
- 混合模式 (請參閱 [混合模式作業](#))
- 偽造的傳輸 (請參閱 [偽造的傳輸](#))

透過從分散式交換器的右鍵功能表中選取**管理分散式連接埠群組**，然後在精靈中選取**安全性**，可以檢視和變更目前設定。請參閱 vSphere 網路說明文件。

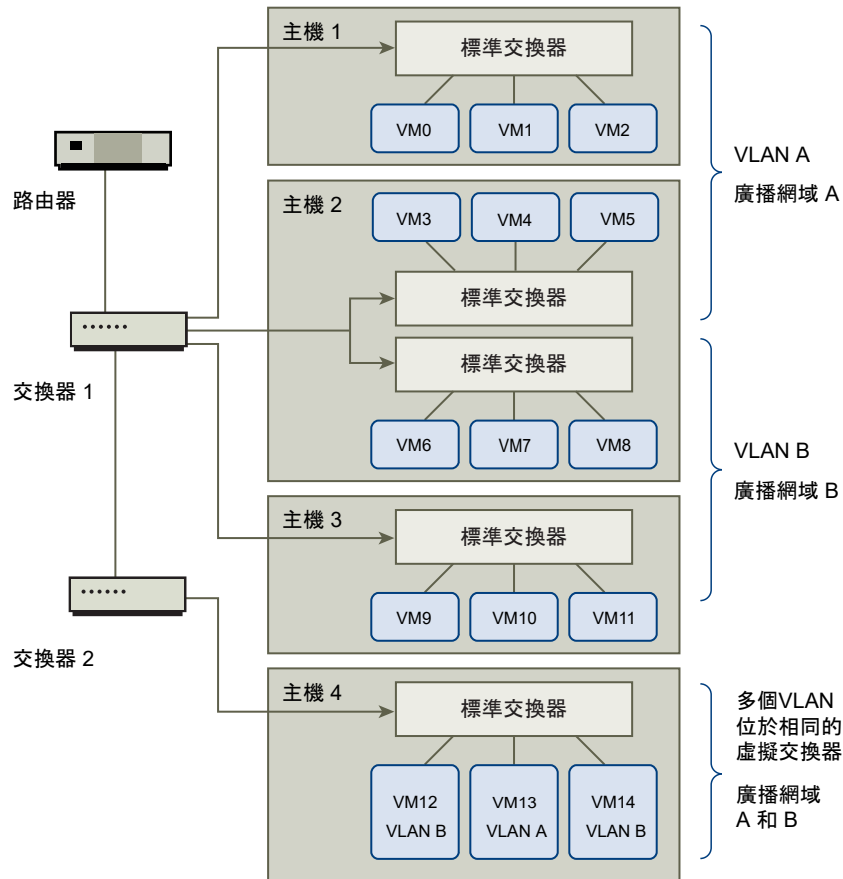
透過 VLAN 保護虛擬機器的安全

網路可能是任何系統中最薄弱的環節之一。虛擬機器網路需要的保護絲毫不少於實體網路。使用 VLAN 可以提高您環境的網路安全性。

VLAN 是一套 IEEE 標準網路配置組合，可透過特定的標記方式將封包的路由限制在 VLAN 中的連接埠內。正確設定後，VLAN 可提供保護一組虛擬機器免遭意外或惡意入侵的可靠方法。

VLAN 可讓您將實體網路分段，讓網路中的兩個虛擬機器無法相互傳輸封包，除非它們屬於相同 VLAN。例如，會計記錄和交易是一家公司最敏感的內部資訊。如果公司的銷售、貨運和會計員工均使用同一實體網路中的虛擬機器，則可透過設定 VLAN 來保護會計部門的虛擬機器。

圖 13-1. 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 4094 之間的 VLAN 識別碼。
- 虛擬客體標記 (VGT) - 虛擬機器處理 VLAN 流量。若要啟動 VGT 模式，請將 VLAN 識別碼設定為 4095。在分散式交換器上，您還可以透過使用 **VLAN 主幹連線**選項，允許以 VLAN 為基礎的虛擬機器流量。

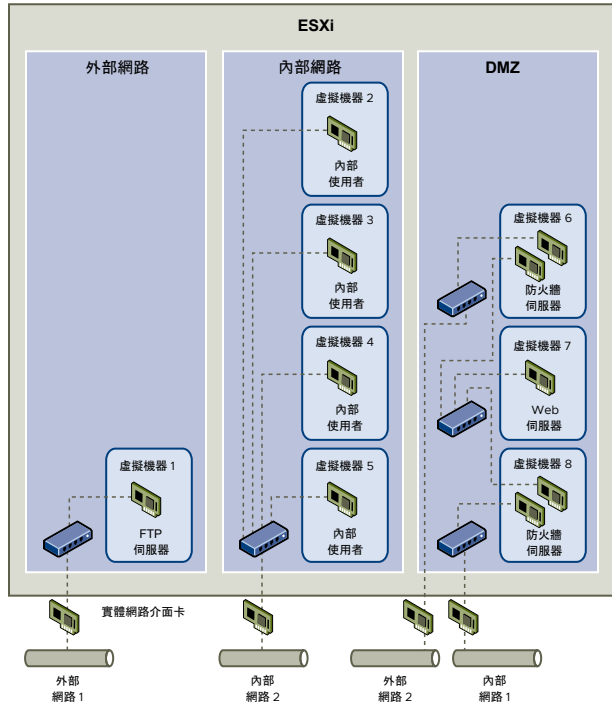
在標準交換器上，您可以在交換器或連接埠群組層級上設定 VLAN 網路模式，而在分散式交換器上，您可以在分散式連接埠群組或連接埠層級上設定。

- 3 請確保已完全記錄了每台虛擬交換器上的所有 VLAN，而且每台虛擬交換器有且僅有所需的 VLAN。

在單一 ESXi 主機內建立多個網路

ESXi 系統的設計可讓您將某些虛擬機器群組連線到內部網路，將其他虛擬機器群組連線到外部網路，並將其他虛擬機器群組同時連線到外部和內部網路，而這一切都在同一主機上進行。此功能是由對虛擬機器的基本隔離和對虛擬網路連線功能的有計劃使用組合而成的。

圖 13-2. 單一 ESXi 主機上設定的外部網路、內部網路和 DMZ



在圖中，系統管理員已將主機設定到三個不同的虛擬機器區域：FTP 伺服器、內部虛擬機器和 DMZ。每個區域均提供唯一功能。

FTP 伺服器區域

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。

內部網路區域

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 區域

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其內容、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。

使用虛擬機器區域的優勢

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，您可在同一 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，因此您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。如果您要確認不存在一般虛擬交換器路徑，可透過在 vSphere Client 中檢閱網路交換器配置，以檢查是否可能存在共用連絡點。

若要保護虛擬機器的資源，請為每個虛擬機器設定資源保留區和限制，以降低 DoS 和 DDoS 攻擊的風險。透過在 DMZ 的前後端安裝軟體防火牆，可以進一步保護 ESXi 主機和虛擬機器。最後，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。

在 ESXi 主機上使用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 ESXi 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` 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` 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> 。
<code>--sa-spi= 安全性參數索引</code>	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= 加密演算法</code>	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"> ■ <code>3des-cbc</code> ■ <code>aes128-cbc</code> ■ <code>null</code>(表示不提供任何加密)
<code>--encryption-key= 加密金鑰</code>	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= 驗證演算法</code>	必要。指定驗證演算法 <code>hmac-sha1</code> 或 <code>hmac-sha2-256</code> 。
<code>--integrity-key= 驗證金鑰</code>	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= 名稱</code>	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 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

- ◆ 在命令提示字元中，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 命令列出可用的安全性原則。

程序

- ◆ 在命令提示字元中，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 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 ■ any
<code>--flow-direction= 方向</code>	使用 <code>in</code> 或 <code>out</code> 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 <code>tunnel</code> 或 <code>transport</code> 。
<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=spl
```

移除 IPsec 安全性原則

您可以使用 ESXCLI 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

- ◆ 在命令提示字元中，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。

ESXi 包含一個可傳送通知 (設陷和通知) 並接收 GET、GETBULK 和 GETNEXT 要求的 SNMP 代理程式。依預設，不會啟用 SNMP。必須在每台 ESXi 主機上設定 SNMP。可以使用 ESXCLI、PowerCLI 或 vSphere Web Services SDK 進行設定。

如需有關設定 SNMP (包括 SNMP v3) 的詳細資訊，請參閱 vSphere 監控和效能說明文件。SNMP v3 提供比 SNMP v1 或 SNMP v2c 更高的安全性，包含金鑰驗證和加密。如需有關 `esxcli system snmp` 命令選項的詳細資訊，請參閱 ESXCLI 參考。

程序

- 1 若要確定是否使用了 SNMP，請執行下列命令。

```
esxcli system snmp get
```

- 2 若要啟用 SNMP，請執行以下命令。

```
esxcli system snmp set --enable true
```

- 3 若要停用 SNMP，請執行以下命令。

```
esxcli system snmp set --enable false
```

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 vSphere 網路安全性建議

遵循一般網路安全建議是保護 vSphere 網路環境的第一步。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。

保護 vSphere 網路環境的建議

- 跨距樹狀目錄通訊協定 (STP) 會偵測並阻止在網路拓撲中形成迴圈。VMware 虛擬交換器會以其他方式阻止迴圈，但不直接支援 STP。當網路拓撲發生變更時，網路重新獲知拓撲需要一些時間 (30–50 秒)。在這段時間內，不允許任何流量通過。為了避免這些問題，網路廠商建立了允許交換器連接埠繼續轉送流量的功能。如需詳細資訊，請參閱 VMware 知識庫文章，網址為：<https://kb.vmware.com/kb/1003804>。請參閱您的網路廠商說明文件，以瞭解適當的網路和網路硬體組態。
- 確保分散式虛擬交換器的 Netflow 流量僅傳送到授權的收集器 IP 位址。Netflow 匯出未加密且可能包含有關虛擬網路的資訊。此資訊增加了攻擊者在傳輸過程中檢視和擷取敏感資訊的可能性。如果需要 Netflow 匯出，請確認所有 Netflow 目標 IP 位址均正確無誤。
- 確保僅授權的管理員可以透過使用角色型存取控制來存取虛擬網路元件。例如，為虛擬機器管理員指定僅存取其虛擬機器所在連接埠群組的權限。為網路管理員指定存取所有虛擬網路元件的權限，但沒有虛擬機器的存取權。有限存取可降低錯誤組態 (無論是意外還是惡意) 的風險，並增強職責分離與最少權限的重要安全性概念。
- 請確保連接埠群組未設定為原生 VLAN 的值。實體交換器通常設有原生 VLAN，依預設，該原生 VLAN 通常為 VLAN 1。ESXi 沒有原生 VLAN。在連接埠群組中指定含 VLAN 的框架有標籤，但未在連接埠群組中指定含 VLAN 的框架不會加上標籤。這可能會產生問題，因為具有標籤 1 的虛擬機器最終會屬於實體交換器的原生 VLAN。

例如，Cisco 實體交換器之 VLAN 1 的框架會取消標籤，因為 VLAN1 是該實體交換器的原生 VLAN。但是，ESXi 主機中指定為 VLAN 1 的框架會加上標籤 1。因此，傳送到原生 VLAN 的 ESXi 主機流量無法正確路由，因為該原生 VLAN 帶有標籤 1，而沒有取消標籤。來自原生 VLAN 的實體交換器流量不可見，因為原生 VLAN 未加上標籤。如果 ESXi 虛擬交換器連接埠群組使用原生 VLAN 識別碼，則來自該連接埠上的虛擬機器的流量對交換器上的原生 VLAN 不可見，因為交換器預期的是取消標籤的流量。

- 請確保連接埠群組未設定為由上游實體交換器保留的 VLAN 值。實體交換器保留某些 VLAN 識別碼用於內部用途，且通常禁止設定為這些值的流量。例如，Cisco Catalyst 交換器通常保留 VLAN 1001–1024 和 4094。使用保留的 VLAN 可能會導致網路上的拒絕服務。
- 請確保連接埠群組未設定為 VLAN 4095，虛擬客體標記 (VGT) 除外。將連接埠群組設定為 VLAN 4095 可啟動 VGT 模式。在此模式下，虛擬交換器會將所有網路框架傳遞到虛擬機器，不需要修改 VLAN 標籤，直接留給虛擬機器處理。
- 在分散式虛擬交換器上限制連接埠層級組態覆寫。連接埠層級組態覆寫預設為停用。啟用覆寫時，您可以使用除連接埠群組層級設定以外的其他虛擬機器安全性設定。某些虛擬機器需要唯一組態，但監控不可或缺。如果不監控覆寫，則可存取含危險分散式虛擬交換器組態之虛擬機器的任何人都可以嘗試利用該存取權。
- 確保分散式虛擬交換器連接埠鏡像流量僅傳送到授權的收集器連接埠或 VLAN。vSphere Distributed Switch 可以將流量從一個連接埠鏡像到另一個連接埠，以允許封包擷取裝置收集特定流量。連接埠鏡像以未加密格式傳送所有指定流量的複本。此鏡像流量包含擷取封包中的完整資料，如果方向錯誤，可能會完全損壞這些資料。如果需要連接埠鏡像，請確認所有連接埠鏡像目的地 VLAN、連接埠和上行識別碼皆正確無誤。

標記 vSphere 網路元件

識別 vSphere 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延伸而引進任何錯誤。

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。

在 vSphere 中採用網路隔離做法

網路隔離做法可以提高 vSphere 環境的網路安全性。

隔離 vSphere 管理網路

vSphere 管理網路提供在每個元件上存取 vSphere 管理介面的權限。在管理介面上執行的服務為攻擊者提供了獲取系統存取權限的機會。遠端攻擊可能會首先獲取此網路的存取權限。如果攻擊者獲得了管理網路的存取權限，它會提供暫存區域以進一步入侵。

以在 ESXi 主機或叢集上執行的最安全的虛擬機器安全性層級來保護管理網路，從而嚴格控制管理網路的存取權。無論管理網路的受限程度為何，管理員都必須具有此網路的存取權才能設定 ESXi 主機和 vCenter Server 系統。

將 vSphere 管理連接埠群組置於常用標準交換器上的專用 VLAN 中。如果生產虛擬機器未使用 vSphere 管理連接埠群組的 VLAN，生產 (虛擬機器) 流量可以共用標準交換器。

檢查網路區段是否未進行路由，路由至包含其他管理相關項目的網路除外。路由網路區段可能對 vSphere Replication 有意義。尤其確保生產虛擬機器流量無法路由到此網路。

使用下列其中一種方法，嚴格控制管理功能的存取權。

- 若要在特別敏感的環境中存取管理網路，請設定受控閘道或其他受控方法。例如，需要管理員透過 VPN 連線至管理網路。僅允許受信任的管理員存取管理網路。
- 設定執行管理用戶端的堡壘主機。

隔離儲存區流量

確保以 IP 為基礎的儲存區流量已隔離。以 IP 為基礎的儲存區包括 iSCSI 和 NFS。虛擬機器可能會與以 IP 為基礎的儲存區組態共用虛擬交換器和 VLAN。此類型的組態可能會向未經授權的虛擬機器使用者公開以 IP 為基礎的儲存區流量。

以 IP 為基礎的儲存區通常不會加密。任何對此網路具有存取權的人員都可以檢視以 IP 為基礎的儲存區流量。若要限制未經授權的使用者檢視以 IP 為基礎的儲存區流量，請以邏輯方式將以 IP 為基礎的儲存區網路流量與生產流量相區隔。從 VMkernel 管理網路的獨立 VLAN 或網路區段上設定以 IP 為基礎的儲存裝置介面卡，以限制未經授權的使用者檢視流量。

隔離 vMotion 流量

vMotion 移轉資訊以純文字格式進行傳輸。任何對此資訊流經的網路具有存取權的人員都可以進行檢視。潛在攻擊者可能會攔截 vMotion 流量以取得虛擬機器的記憶體內容。他們還可能會暫存移轉期間修改內容的 MITM 攻擊。

在隔離網路上，將 vMotion 流量與生產流量相區隔。將網路設定為不可路由，即確保第 3 層路由器不會跨越此網路和其他網路，從而阻止從外部存取網路。

將常用標準交換器上的專用 VLAN 用於 vMotion 連接埠群組。如果生產虛擬機器不使用 vMotion 連接埠群組的 VLAN，則生產 (虛擬機器) 流量可以使用相同的標準交換器。

隔離 vSAN 流量

設定 vSAN 網路時，請在其自己的第 2 層網路區段上隔離 vSAN 流量。您可以使用專用交換器或連接埠，或使用 VLAN 來執行此隔離。

僅在需要時透過 vSphere Network Appliance API 使用虛擬交換器

不要將主機設定為傳送網路資訊到虛擬機器，除非您正在使用使用了 vSphere Network Appliance API (DvFilter) 的產品。如果 vSphere Network Appliance API 處於啟用狀態，則攻擊者可能會嘗試將虛擬機器連線到篩選器。此連線可能會導致存取主機上的其他虛擬機器網路。

如果您正在使用使用了此 API 的產品，請確認是否已正確設定主機。請參閱《開發和部署 vSphere 解決方案、vService 和 ESX 代理程式》中有關 DvFilter 的章節，網址為 <https://developer.vmware.com/docs/6518/developing-and-deploying-vsphere-solutions--vservices--and-esx-agents>。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 在 vSphere Client 詳細目錄中瀏覽到主機。
- 2 按一下**設定**。
- 3 在 [系統] 下，按一下**進階系統設定**。
- 4 向下捲動到 `Net.DVFilterBindIpAddress`，並確認該參數的值是否為空。

參數的順序不是嚴格按字母順序排列的。在 [篩選器] 文字方塊中輸入 **DVFilter**，以顯示所有相關的參數。

- 5 確認設定。
 - 如果未使用 DvFilter 設定，請確保值為空。
 - 如果您使用 DvFilter 設定，請確定參數的值正確無誤。該值必須符合使用 DvFilter 之產品所使用的值。

有關多個 vSphere 元件的最佳做法

14

某些安全性最佳做法 (例如在環境中設定 PTP 或 NTP) 會影響多個 vSphere 元件。設定環境時請考慮這些建議。

如需相關資訊，請參閱第 3 章 保護 ESXi 主機和第 5 章 確保虛擬機器安全。

本章節討論下列主題：

- 同步 vSphere 網路上的時鐘
- 儲存區安全性最佳做法
- 確認已停用向客體傳送主機效能資料
- 設定 ESXi Shell 和 vSphere Client 的逾時

同步 vSphere 網路上的時鐘

確認 vSphere 網路上所有元件的時鐘均已同步。如果 vSphere 網路中實體機器的時鐘未同步，則在網路機器之間進行通訊時，無法將對時間敏感的 SSL 憑證和 SAML Token 辨識為有效。

未同步的時鐘可能會導致驗證問題，從而使安裝失敗或使 vCenter Server`vmware-vpxd` 服務無法啟動。

vSphere 中的時間不一致情況可能會導致環境中的元件在不同服務中首次開機失敗，具體取決於環境中時間不準確的地方和時間同步的時機。當目的地 vCenter Server 的目標 ESXi 主機與 NTP 或 PTP 不同步時，通常會發生問題。同樣地，如果目的地 vCenter Server 移轉到因全自動 DRS 而設為不同時間的 ESXi 主機，也可能會產生問題。

若要避免時間同步問題，請在安裝、移轉或升級 vCenter Server 執行個體之前，確保下列內容正確無誤。

- 即將部署目的地 vCenter Server 的目標 ESXi 主機已同步至 NTP 或 PTP。
- 執行來源 vCenter Server 的 ESXi 主機已同步至 NTP 或 PTP。
- 從 vSphere 6.7 升級或移轉至 vSphere 8.0 時，如果 vCenter Server Appliance 連線至外部 Platform Services Controller，請確保執行外部 Platform Services Controller 的 ESXi 主機已同步至 NTP 或 PTP。
- 如果您要從 vSphere 6.7 升級或移轉至 vSphere 8.0，請確認來源 vCenter Server 或 vCenter Server Appliance 和外部 Platform Services Controller 具有正確的時間。

請確認 vCenter Server 執行所在的任何 Windows 主機電腦與網路時間伺服器 (NTP) 伺服器同步。請參閱 VMware 知識庫文章，網址為 <https://kb.vmware.com/s/article/1318>。

若要將 ESXi 時鐘與 NTP 或 PTP 伺服器同步，您可以使用 VMware Host Client。如需編輯 ESXi 主機時間組態的相關資訊，請參閱《vSphere 單一主機管理 - VMware Host Client》說明文件中的〈在 VMware Host Client 中編輯 ESXi 主機的時鐘組態〉主題。

若要瞭解如何變更 vCenter Server 的時間同步化設定，請參閱《vCenter Server 組態》說明文件中的〈設定系統時區及時間同步化設定〉主題。

若要瞭解如何使用 vSphere Client 編輯主機的時鐘組態，請參閱《vCenter Server 和主機管理》說明文件中的〈編輯主機的時鐘組態設定〉主題。

■ 使 ESXi 時鐘與網路時間伺服器同步

安裝 vCenter Server 之前，請確保 vSphere 網路上所有機器的時鐘均已同步。

■ 在 vCenter Server 中設定時間同步化設定

可在部署後變更 vCenter Server 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 之前，請確保 vSphere 網路上所有機器的時鐘均已同步。

此工作說明如何從 VMware Host Client 設定 NTP。

程序

- 1 啟動 VMware Host Client，然後連線至 ESXi 主機。
- 2 按一下**管理**。
- 3 在**系統**下，按一下**時間和日期**，然後按一下**編輯設定**。
- 4 選取**使用網路時間通訊協定 (啟用 NTP 用戶端)**。
- 5 在 [NTP 伺服器] 文字方塊中，輸入要與之同步的一或多部 NTP 伺服器的 IP 位址或完整網域名稱。
- 6 從 **NTP 服務啟動原則**下拉式功能表中，選取**隨主機一起啟動和停止**。
- 7 按一下**儲存**。

主機即會與 NTP 伺服器同步。

在 vCenter Server 中設定時間同步化設定

可在部署後變更 vCenter Server 中的時間同步化設定。

部署 vCenter Server 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 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 中只能使用一種定期時間同步化形式。如果您決定使用本機時間同步軟體，則會停用 vCenter Server VMware Tools 週期性時間同步。

使用 VMware Tools 時間同步化

您可以將 vCenter Server 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 組態中新增或取代 NTP 伺服器

若要設定 vCenter Server 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 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 執行下列 `ntp.set` 命令，將 NTP 伺服器新增至 vCenter Server 組態。

```
ntp.set --servers IP-addresses-or-host-names
```

在此命令中，*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)。

此命令將移除目前的 NTP 伺服器 (如有)，並將新的 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，此命令會將 NTP 組態中的目前 NTP 伺服器取代為您指定的新 NTP 伺服器。

- 3 (選擇性) 若要驗證是否已成功套用新的 NTP 組態設定，請執行以下命令。

```
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。

- 4 (選擇性) 若要驗證 NTP 伺服器是否可供連線，請執行以下命令。

```
ntp.test --servers IP-addresses-or-host-names
```

該命令將傳回 NTP 伺服器的狀態。

後續步驟

如果停用 NTP 同步，您可以將 vCenter Server 中的時間同步設定設定為以 NTP 伺服器為基礎。請參閱 [將 vCenter Server 與 NTP 伺服器的時間同步](#)。

將 vCenter Server 與 NTP 伺服器的時間同步

您可以將 vCenter Server 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 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 組態中新增或取代 NTP 伺服器](#)。

程序

- 1 存取應用裝置 shell 並以具有管理員或超級管理員角色的使用者身分登入。
具有超級管理員角色的預設使用者是根使用者。
- 2 執行下列命令以啟用以 NTP 為基礎的時間同步化。

```
timesync.set --mode NTP
```

- 3 (選擇性) 執行下列命令以確認已成功套用 NTP 同步化。

```
timesync.get
```

該命令傳回時間同步化處於 NTP 模式。

儲存區安全性最佳做法

遵循儲存區安全性提供者概略列出的儲存區安全性最佳做法。您還可以利用 CHAP 與相互 CHAP 來保護 iSCSI 儲存區、遮罩與區域 SAN 資源，並設定 NFS 4.1 的 Kerberos 認證。

另請參閱 [管理 VMware vSAN 說明文件](#)。

保護 iSCSI 儲存區安全

為主機設定的儲存區可能包括一或多個使用 iSCSI 的儲存區域網路 (SAN)。在主機上設定 iSCSI 時，可採取措施將安全性風險降到最低。

iSCSI 支援使用 TCP/IP 透過網路連接埠 (而非透過直接連線到 SCSI 裝置) 來存取 SCSI 裝置和交換資料。iSCSI 交易將原始 SCSI 資料區塊封裝在 iSCSI 記錄中，並將資料傳輸到要求資料的裝置或使用者。

iSCSI SAN 支援有效利用現有乙太網路基礎結構，為主機提供其可動態共用的儲存資源的存取權限。iSCSI SAN 是適用於依賴一般儲存區集區服務多個使用者之環境的經濟型儲存區解決方案。與任一網路系統一樣，iSCSI SAN 也可能會受到安全性破壞。

備註 用於保護 iSCSI SAN 安全的需求和程序，與和主機相關聯的硬體 iSCSI 介面卡和透過主機直接設定的 iSCSI 的需求和程序相似。

保護 iSCSI 裝置安全

若要保護 iSCSI 裝置，每當主機嘗試存取目標 LUN 上的資料時，都要求 ESXi 主機 (或啟動器) 向 iSCSI 裝置 (或目標) 進行驗證。

驗證可確保啟動器具有存取目標的權限。您可在 iSCSI 裝置上設定驗證時授與此權限。

對於 iSCSI，ESXi 不支援安全遠端通訊協定 (SRP) 或公開金鑰驗證方式。您只能搭配 NFS 4.1 使用 Kerberos。

ESXi 支援 CHAP 和相互 CHAP 驗證。vSphere 儲存區說明文件解釋如何選取適用於 iSCSI 裝置的最佳驗證方法，以及如何設定 CHAP。

確保 CHAP 密碼的唯一性。設定每台主機的不同相互驗證密碼。如果可能，請為連線至 ESXi 主機的每個用戶端設定不同的密碼。唯一的密碼可確保即使一個主機受到危害，攻擊者仍無法建立其他任意主機以及向儲存裝置進行驗證。使用共用密碼，一台主機受危害可能會使得攻擊者能夠向儲存裝置進行驗證。

保護 iSCSI SAN

計劃 iSCSI 組態時，應採取一些措施提高 iSCSI SAN 的整體安全性。iSCSI 組態是否安全性取決於 IP 網路，因此在設定網路時，強制執行良好的安全性標準可協助保護 iSCSI 儲存區。

下列是強制執行良好安全性標準的一些具體建議。

保護傳輸的資料

iSCSI SAN 中的一個主要安全性風險便是攻擊者會探查到傳輸的儲存資料。

採取其他措施，使攻擊者無法輕鬆看到 iSCSI 資料。無論是 iSCSI 硬體介面卡還是 ESXi iSCSI 啟動器，均不會對其傳輸到目標的資料和從目標接收的資料進行加密，這會造成資料更容易遭受探查攻擊。

若允許虛擬機器與 iSCSI 組態共用標準交換器和 VLAN，可能造成 iSCSI 流量遭到虛擬機器攻擊者的不當使用。若要協助確保侵入者無法接聽 iSCSI 傳輸，請確保任何虛擬機器都無法查看 iSCSI 儲存區網路。

如果您使用 iSCSI 硬體介面卡，若要達成此目標，您可以確保 iSCSI 介面卡和 ESXi 實體網路介面卡未透過共用交換器或其他某些方式，而不小心在主機外部連線。如果直接透過 ESXi 主機設定 iSCSI，若要達成此目標，您可以不與虛擬機器使用同一標準交換器，而改用不同的標準交換器來設定 iSCSI 儲存區。

除了透過提供專用標準交換器來保護 iSCSI SAN 之外，您還可以在 iSCSI SAN 自己的 VLAN 上進行設定來提高效能和安全性。將 iSCSI 組態置於獨立的 VLAN 上，可確保只有 iSCSI 介面卡能夠看到 iSCSI SAN 內的傳輸。同時，來自其他來源的網路壅塞不會影響 iSCSI 流量。

保護 iSCSI 連接埠安全

當執行 iSCSI 裝置時，ESXi 不會開啟任何接聽網路連線的連接埠。此措施可降低侵入者透過備用連接埠侵入 ESXi 並控制主機的機率。因此，執行 iSCSI 不會在連線的 ESXi 端產生任何額外的安全性風險。

您執行的任何 iSCSI 目標裝置都必須具有一或多個開啟的 TCP 連接埠可接聽 iSCSI 連線。如果 iSCSI 裝置軟體中存在任何安全性漏洞，則資料遭遇的風險並非 ESXi 所造成。若要降低此風險，請安裝儲存設備製造商提供的所有安全性修補程序，並限制連線到 iSCSI 網路的裝置。

遮罩 SAN 資源並進行分區

可以使用分區設定和 LUN 遮罩來分隔 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 儲存區說明文件。

針對 NFS 4.1 使用 Kerberos

藉由 NFS 4.1 版，ESXi 支援 Kerberos 驗證機制。

RPCSEC_GSS Kerberos 機制是一種驗證服務。它可讓安裝在 ESXi 上的 NFS 4.1 用戶端在掛接 NFS 共用之前向 NFS 伺服器證明其身分。Kerberos 安全性使用密碼編譯在不安全的網路連線中運作。

針對 NFS 4.1，Kerberos 的 ESXi 實作提供兩種安全性模型 krb5 和 krb5i，這兩種模型提供不同的安全層級。

- 僅用於驗證的 Kerberos (krb5) 支援身分識別驗證。
- 用於驗證和資料完整性的 Kerberos (krb5i)，除身分識別驗證之外，還提供資料完整性服務。這些服務透過檢查資料封包是否存在任何潛在修改，協助保護 NFS 流量免遭竄改。

Kerberos 支援密碼編譯演算法，該演算法可防止未經授權的使用者取得 NFS 流量的存取權。ESXi 上的 NFS 4.1 用戶端會嘗試使用 AES256-CTS-HMAC-SHA1-96 或 AES128-CTS-HMAC-SHA1-96 演算法來存取 NAS 伺服器上的共用。在使用 NFS 4.1 資料存放區之前，請先確保 NAS 伺服器上已啟用 AES256-CTS-HMAC-SHA1-96 或 AES128-CTS-HMAC-SHA1-96。

下表比較了 ESXi 支援的 Kerberos 安全性層級。

表 14-1. Kerberos 安全性類型

		ESXi 6.0	ESXi 6.5 及更新版本
僅用於驗證的 Kerberos (krb5)	RPC 標頭的完整性總和檢查碼	是 (採用 DES)	是 (採用 AES)
	RPC 資料的完整性總和檢查碼	否	否
用於驗證和資料完整性的 Kerberos (krb5i)	RPC 標頭的完整性總和檢查碼	否 (krb5i)	是 (採用 AES)
	RPC 資料的完整性總和檢查碼		是 (採用 AES)

當您使用 Kerberos 驗證時，需考量下列事項：

- ESXi 將 Kerberos 與 Active Directory 網域搭配使用。

- 做為 vSphere 管理員，您可指定 Active Directory 認證，為 NFS 使用者提供 NFS 4.1 Kerberos 資料存放區的存取權。單一認證集用於存取掛接在該主機上的所有 Kerberos 資料存放區。
 - 當多個 ESXi 主機共用 NFS 4.1 資料存放區時，必須針對存取共用資料存放區的所有主機使用相同的 Active Directory 認證。若要自動化指派程序，請在主機設定檔中設定使用者並將設定檔套用至所有 ESXi 主機。
 - 不能針對多台主機共用的同一個 NFS 4.1 資料存放區使用兩種安全機制 AUTH_SYS 和 Kerberos。
- 如需逐步指示，請參閱 vSphere 儲存區 說明文件。

確認已停用向客體傳送主機效能資料

在安裝了 VMware Tools 的 Windows 作業系統中，vSphere 會包括虛擬機器效能計數器。效能計數器允許虛擬機器擁有者在客體作業系統內進行準確的效能分析。依預設，vSphere 不會向客體虛擬機器公開主機資訊。

依預設，已停用向虛擬機器傳送主機效能資料的功能。此預設設定可防止虛擬機器取得有關實體主機的詳細資訊。如果虛擬機器受到安全性破壞，此設定可防止攻擊者取得主機資料。

備註 下列程序說明了基本程序。請考慮使用 ESXCLI 或 VMware PowerCLI 命令在所有主機上同時執行此工作。

程序

- 1 在主控虛擬機器的 ESXi 系統上，瀏覽到 VMX 檔案。

虛擬機器組態檔位於 `/vmfs/volumes/datastore` 目錄中，其中 *datastore* 是儲存虛擬機器檔案之儲存裝置的名稱。

- 2 在 VMX 檔案中，確認是否設定了下列參數。

```
tools.guestlib.enableHostInfo=FALSE
```

- 3 儲存並關閉該檔案。

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 Client 的逾時

為了防止侵入者使用閒置工作階段，請設定 ESXi Shell 和 vSphere Client 的逾時。

ESXi Shell 逾時

對於 ESXi Shell，您可以從 vSphere Client 和 Direct Console 使用者介面 (DCUI) 來設定下列逾時。

可用性逾時

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

閒置逾時

閒置逾時值是使用者從閒置互動式工作階段登出之前可以經過的時間量。對閒置逾時的變更會在下次使用者登入 ESXi Shell 時套用。變更不會影響現有工作階段。

變更 vSphere Client 逾時

依預設，vSphere Client 工作階段會在閒置 120 分鐘後終止。若要變更預設值：

- 1 在 vSphere Client 中，導覽到 vCenter Server 執行個體。
- 2 選取**設定**索引標籤，然後在**設定**下選取**一般**。
- 3 按一下**編輯**。
- 4 選取**逾時設定**。
- 5 輸入您的選擇，然後按一下**儲存**。

透過 TLS Configurator 公用程式管理 vSphere TLS 通訊協定組態

15

vSphere 依預設僅啟用 TLS。預設為停用 TLS 1.0 和 TLS 1.1。無論是否執行全新安裝、升級或移轉，vSphere 都會停用 TLS 1.0 和 TLS 1.1。您可以使用 TLS Configurator 公用程式，在 vCenter Server 系統上暫時啟用舊版通訊協定。當所有連線均使用 TLS 1.2 之後，則可以停用較不安全的舊版。

從 ESXi 8.0 開始，僅支援 TLS 1.2。ESXi 8.0 不再支援 TLS 1.0 和 1.1，您也無法啟用這些較舊的通訊協定版本。在 ESXi 8.0 上執行 TLS Configurator 公用程式失敗，但不報告錯誤。

在 vCenter Server 上重新設定舊通訊協定版本之前，請考慮您的環境。根據您的環境需求和軟體版本，除了 TLS 1.2 以外，您可能還需要重新啟用 TLS 1.0 和 TLS 1.1 以維持互通性。請參閱 VMware 知識庫文章 (網址為：<https://kb.vmware.com/s/article/2145796>) 以取得支援 TLS 1.2 的 VMware 產品。關於第三方整合，請參閱廠商說明文件。TLS Configurator 公用程式可與 vSphere 8.0 及舊版搭配使用，包括 7.0、6.7、6.5 和 6.0。

vCenter Server 使用的連接埠可啟用或停用 TLS 通訊協定。TLS 組態公用程式 `scan` 選項會顯示各項服務已啟用的 TLS 版本。請參閱[針對 TLS 通訊協定掃描 vCenter Server](#)。

如需 VMware 產品 (包括 vSphere 和 vSAN) 中所有支援的連接埠和通訊協定的清單，請參閱 VMware Ports and Protocols Tool™，網址為 <https://ports.vmware.com/>。可以依 VMware 產品搜尋連接埠、建立自訂連接埠清單，以及列印或儲存連接埠清單。

vCenter Server 和 Envoy

在 vSphere 7.0 及更新版本中，vCenter Server 執行兩個反向 Proxy 服務：

- VMware 反向代理服務，`rhttpproxy`
- Envoy

Envoy 是開放原始碼 Edge 和服務 Proxy。Envoy 擁有連接埠 443，且所有傳入 vCenter Server 要求均透過 Envoy 路由。在 vSphere 7.0 及更新版本中，`rhttpproxy` 充當 Envoy 的組態管理伺服器。如此一來，TLS 組態會套用至 `rhttpproxy`，而後者隨後將組態傳送至 Envoy。

有關 vSphere 和 TLS 的附註和警告

- vSphere 6.7 版本是 vCenter Server for Windows 的最後一個版本。如需在 vCenter Server for Windows 上重新設定 Update Manager 連接埠的 TLS 的相關資訊，請參閱 6.7 版產品的 vSphere 安全性說明文件。

- 您可以使用 TLS 1.2 來加密 vCenter Server 與外部 Microsoft SQL Server 之間的連線。您無法僅使用 TLS 1.2 與外部 Oracle 資料庫連線。請參閱 VMware 知識庫文章，網址為 <https://kb.vmware.com/kb/2149745>。
- 對於 vSphere 6.7 及更早版本，請勿在 Windows Server 2008 上執行的 vCenter Server 或 Platform Services Controller 執行個體停用 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〉。

本章節討論下列主題：

- 執行選擇性 vCenter Server TLS 手動備份
- 在 vCenter Server 系統上啟用或停用 TLS 版本
- 針對 TLS 通訊協定掃描 vCenter Server
- 還原 vCenter Server TLS 組態變更

執行選擇性 vCenter Server TLS 手動備份

TLS 組態公用程式會在每次指令碼修改 vCenter Server 時執行 TLS 組態的備份。如果必須儲存備份至特定目錄，您可以執行手動備份。

對於 vCenter Server，預設目錄為 `/tmp/yearmonthdayTtime`。

程序

- 1 使用 SSH 連線到 vCenter Server。
- 2 將目錄變更為 `/usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`。
- 3 若要備份至特定目錄，請執行下列命令。

```
directory_path/VcTlsReconfigurator> ./reconfigureVc backup -d backup_directory_path
```

- 4 確認您的備份已成功。

成功備份會與以下範例類似。由於命令的執行方式，每次執行 `reconfigureVc backup` 命令時，顯示的服務順序可能不同。

```
vCenter Transport Layer Security reconfigurator, version=8.0.0, build=10068142
For more information refer to the following article: https://kb.vmware.com/kb/2147469
Log file: "/var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log".
===== Backing up vCenter Server TLS configuration =====
Using backup directory: /tmp/20220714T225653
Backing up: vmcam
Backing up: vmdird
Backing up: vmware-rhttpproxy
Backing up: vmware-std
Backing up: vami-lighttp
Backing up: vmware-rbd-watchdog
```

```
Backing up: rsyslog
Backing up: vmware-updatemgr
Backing up: vmware-sps
Backing up: vmware-vpxd
```

- 5 (選擇性) 如果您之後必須執行還原，您可以執行以下命令。

```
reconfigureVc restore -d optional_custom_backup_directory_path
```

在 vCenter Server 系統上啟用或停用 TLS 版本

您可使用 TLS 組態公用程式來啟用或停用 vCenter Server 系統上的 TLS 版本。在執行該程序過程中，您可以停用 TLS 1.0 並啟用 TLS 1.1 和 TLS 1.2，也可以停用 TLS 1.0 和 TLS 1.1 並僅啟用 TLS 1.2。

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 使用 administrator@vsphere.local 的使用者名稱和密碼，或以可執行指令碼之 vCenter Single Sign-On 管理員群組的其他成員身分，來登入 vCenter Server 系統。
- 2 前往指令碼所在的目錄。

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

- 3 根據您要使用的 TLS 版本執行命令。

- 停用 TLS 1.0 並同時啟用 TLS 1.1 和 TLS 1.2，請執行以下命令。

```
directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2
```

- 停用 TLS 1.0 和 TLS 1.1 並僅啟用 TLS 1.2，請執行以下命令。

```
directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2
```

- 4 如果您的環境包含其他 vCenter Server 系統，請在每個 vCenter Server 系統上重複該程序。

針對 TLS 通訊協定掃描 vCenter Server

啟用或停用 vCenter Server 上的 TLS 版本後，您可以使用 TLS 組態公用程式來檢視變更。

TLS 組態公用程式 scan 選項會顯示各項服務已啟用的 TLS 版本。

程序

- 1 登入 vCenter Server 系統。
 - a 使用 SSH 連線應用裝置，並以具有執行指令碼權限的使用者身分登入。
 - b 如果 Bash shell 目前尚未啟用，請執行以下命令。

```
shell.set --enabled true
shell
```

- 2 前往 VcTlsReconfigurator 目錄。

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

- 3 若要顯示哪些服務已啟用 TLS 以及已使用哪些連接埠，請執行下列命令。

```
reconfigureVc scan
```

還原 vCenter Server 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。

必要條件

還原變更之前，請使用 vCenter Server 管理介面來執行 vCenter Server 的備份。

程序

- 1 以具有指令碼執行權限的使用者身分連線至要還原變更的 vCenter Server。
- 2 如果 Bash shell 目前尚未啟用，請執行以下命令。

```
shell.set --enabled true
shell
```

- 3 前往 VcTlsReconfigurator 目錄。

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

- 4 檢閱先前備份。

```
grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log
```

輸出與下列範例類似。

```
2022-07-14T22:56:53.706Z INFO Using backup directory: /tmp/20220714T225653
2022-07-14T22:58:08.594Z INFO Using backup directory: /tmp/20220714T225808
```

5 執行下列命令以執行還原。

```
reconfigureVc restore -d Directory_path_from_previous_step
```

TLS 組態已還原。在程序過程中，會重新啟動 vCenter Server。

6 請對任何其他 vCenter Server 執行個體重複該程序。

下列資料表列出了一些預設權限，為角色選取這些權限時，可以與使用者配對，也可以指派給物件。

在設定權限時，請確認對所有物件類型的每項特定動作均設定了適當的權限。除了要擁有對正操縱的物件的存取權限之外，部分作業需要有對根資料夾或父系資料夾的存取權限。部分作業還需要對父系資料夾及相關物件的存取權限或執行權限。

vCenter Server 延伸可能定義未在此處列出的其他權限。如需這些權限的詳細資訊，請參閱延伸說明文件。

本章節討論下列主題：

- 警示權限
- Auto Deploy 與映像設定檔權限
- 憑證權限
- 憑證授權機構權限
- 憑證管理權限
- Cns 權限
- 計算原則權限
- 內容程式庫權限
- 密碼編譯作業權限
- dvPort 群組權限
- Distributed Switch 權限
- 資料中心權限
- 資料存放區權限
- 資料存放區叢集權限
- ESX Agent Manager 權限
- 延伸權限
- 外部統計資料提供者權限
- 資料夾權限

- 全域權限
- 混合連結模式權限
- 健全狀況更新提供者權限
- 主機 CIM 權限
- 主機組態權限
- 主機熵集區權限
- 主機的 Intel Software Guard Extensions 權限
- 主機詳細目錄權限
- 主機本機作業權限
- 主機統計資料權限
- 主機信賴平台模組權限
- 主機 vSphere Replication 權限
- 主機設定檔權限
- vCenter Server 設定檔權限
- vSphere with Tanzu 權限
- 網路權限
- NSX 權限
- VMware 可觀察性權限
- OvfManager 權限
- 與合作夥伴 REST 精靈互動權限
- 效能權限
- 外掛程式權限
- 權限 (Permissions) 權限
- 資源權限
- 排定的工作權限
- 工作階段權限
- 虛擬機器儲存區原則權限
- 儲存區視圖權限
- 主管服務權限
- 工作權限
- 承租人管理權限

- Transfer Service 權限
- VcTrusts/VcIdentity 權限
- 受信任基礎結構管理員權限
- vApp 權限
- VcIdentityProviders 權限
- VMware vSphere Lifecycle Manager 組態權限
- VMware vSphere Lifecycle Manager ESXi 健全狀況透視圖權限
- VMware vSphere Lifecycle Manager 一般權限
- VMware vSphere Lifecycle Manager 硬體相容性權限
- VMware vSphere Lifecycle Manager 映像權限
- VMware vSphere Lifecycle Manager 映像修復權限
- VMware vSphere Lifecycle Manager 設定權限
- VMware vSphere Lifecycle Manager 管理基準權限
- VMware vSphere Lifecycle Manager 管理修補程式和升級權限
- VMware vSphere Lifecycle Manager 上傳檔案權限
- 虛擬機器變更組態權限
- 虛擬機器客體作業權限
- 虛擬機器互動權限
- 虛擬機器編輯詳細目錄權限
- 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
- 虛擬機器類別權限
- vSAN 權限
- vSphere 區域權限
- vService 權限
- vSphere 標記權限
- vSphere Client 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 16-1. 警示權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	Alarm.Acknowledge
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	Alarm.Create
停用警示動作	允許在觸發警示之後阻止警示動作。警示自身未停用。	對其定義了警示的物件	Alarm.DisableActions
在實體上停用或啟用警示	允許在特定目標類型上啟用或停用特定警示。	可觸發警示的物件	Alarm.ToggleEnableOnEntity
修改警示	允許變更警示的內容。	對其定義了警示的物件	Alarm.Edit
移除警示	允許刪除警示。	對其定義了警示的物件	Alarm.Delete
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	Alarm.SetStatus

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。如需有關 Auto Deploy 的詳細資訊，請參閱 VMware ESXi 安裝和設定說明文件。

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 16-2. Auto Deploy 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 主機 <ul style="list-style-type: none"> ■ 關聯機器 	允許使用者將主機與機器關聯。	vCenter Server	AutoDeploy.Host.AssociateMachine
<ul style="list-style-type: none"> ■ 映像設定檔 <ul style="list-style-type: none"> ■ 建立 ■ 編輯 	建立 允許建立映像設定檔。 編輯 允許編輯映像設定檔。	vCenter Server	AutoDeploy.Profile.Create AutoDeploy.Profile.Edit
<ul style="list-style-type: none"> ■ 規則 <ul style="list-style-type: none"> ■ 建立 ■ 編輯 ■ 刪除 	建立 允許建立 Auto Deploy 規則。 編輯 允許編輯 Auto Deploy 規則。 刪除 允許刪除 Auto Deploy 規則。	vCenter Server	AutoDeploy.Rule.Create AutoDeploy.Rule.Edit AutoDeploy.Rule.Delete
<ul style="list-style-type: none"> ■ 規則集 <ul style="list-style-type: none"> ■ 啟用 ■ 編輯 	啟用 允許啟用 Auto Deploy 規則集。 編輯 允許編輯 Auto Deploy 規則集。	vCenter Server	AutoDeploy.RuleSet.Activate AutoDeploy.RuleSet.Edit

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 vSphere 驗證說明文件中的「進行憑證管理作業所需的權限」。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表 16-3. 主機憑證權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
管理憑證	允許對 ESXi 主機進行憑證管理。	vCenter Server	Certificate.Manage

憑證授權機構權限

憑證授權機構權限控制 VMware Certificate Authority (VMCA) 憑證的各個方面。

表 16-4. 憑證授權機構權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
建立/刪除 (管理員權限)。	允許對 vCenter Server 憑證的管理進行完全管理層級存取。	vCenter Server	CertificateAuthority.Administer
建立/刪除 (低於管理員權限)。	允許在 vSphere Client 的 [憑證管理] 頁面中檢視 VMCA 根憑證。	vCenter Server	CertificateAuthority.Manage

憑證管理權限

憑證管理權限控制哪些使用者可以管理 vCenter Server 憑證。

表 16-5. 憑證管理權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
建立/刪除 (管理員權限)。	允許對 vCenter Server 憑證相關作業的各種內部 API 和功能進行完全管理層級存取。	vCenter Server	CertificateManagement.Administer
建立/刪除 (低於管理員權限)。	<p>允許減少對各種內部 API 和功能的管理存取。此權限限制憑證相關作業，這樣使用者便無法提升非管理員權限。允許的作業包括：</p> <ul style="list-style-type: none"> ■ 產生憑證簽署要求 ■ 建立和擷取受信任的根鏈結 ■ 刪除具有 憑證管理.建立/刪除 (低於管理員權限)。權限之使用者建立的受信任的根鏈結 ■ 擷取機器 SSL 憑證 ■ 擷取用於驗證 vCenter Server 核發的 Token 的簽署憑證鏈結 	vCenter Server	CertificateManagement.Manage

Cns 權限

雲端原生存放區 (Cns) 權限控制哪些使用者可以存取雲端原生儲存使用者介面。

表 16-6. Cns 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
可搜尋	允許儲存區管理員檢視雲端原生儲存使用者介面。	根 vCenter Server	Cns.Searchable

計算原則權限

計算原則權限控制管理計算原則的能力。

表 16-7. 計算原則權限

vSphere Client 中的 權限名稱	說明	要求	API 中的權限名稱
建立和刪除計算原則	允許建立和刪除計算原則。	根 vCenter Server	ComputePolicy.Manage

內容程式庫權限

內容程式庫會為虛擬機器範本和 vApp 提供簡單且有效的管理。內容程式庫權限會控制可檢視或管理內容程式庫不同方面的人選。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

備註 內容程式庫權限的繼承可在單一 vCenter Server 執行個體的環境中運作。不過，從詳細目錄的觀點來看，內容程式庫並非 vCenter Server 系統的直接子系。內容程式庫的直接父系為全域根物件。此關聯性表示，如果您在 vCenter Server 層級上設定權限並將其散佈到子物件，此權限將套用到資料中心、資料夾、叢集、主機、虛擬機器等，但不會套用到您在此 vCenter Server 執行個體中看到和操作的內容程式庫。若要指派內容程式庫的權限，管理員必須將該權限做為全域權限授與使用者。全域權限支援從全域根物件跨解決方案指派權限。

表 16-8. 內容程式庫權限

vSphere Client 中的 權限名稱	說明	要求	API 中的權限名稱
新增程式庫項目	允許在程式庫中新增項目。	程式庫	ContentLibrary.AddLibraryItem
將根憑證新增至信任存放區	允許將根憑證新增到受信任的根憑證存放區。	vCenter Server	ContentLibrary.AddCertToTrustStore
簽入範本	允許簽入範本。	程式庫	ContentLibrary.CheckInTemplate
簽出範本	允許簽出範本。	程式庫	ContentLibrary.CheckOutTemplate
建立已發佈程式庫的訂閱	允許建立程式庫訂閱。	程式庫	ContentLibrary.AddSubscription
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	ContentLibrary.CreateLocalLibrary
建立或刪除 Harbor 登錄	允許建立或刪除 VMware Tanzu Harbor 登錄服務。	要建立的 vCenter Server。要刪除的登錄。	ContentLibrary.ManageRegistry

表 16-8. 內容程式庫權限 (續)

vSphere Client 中的			
權限名稱	說明	要求	API 中的權限名稱
建立已訂閱程式庫	允許建立已訂閱程式庫。	vCenter Server	ContentLibrary.CreateSubscribedLibrary
建立、刪除或清除 Harbor 登錄專案	允許建立、刪除或清除 VMware Tanzu Harbor 登錄專案。	登錄	ContentLibrary.ManageRegistryProject
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。	ContentLibrary.DeleteLibraryItem
刪除本機程式庫	允許刪除本機程式庫。	程式庫	ContentLibrary.DeleteLocalLibrary
從信任存放區刪除根憑證	允許從受信任的根憑證存放區中刪除根憑證。	vCenter Server	ContentLibrary.DeleteCertFromTrustStore
刪除已訂閱程式庫	允許刪除已訂閱程式庫。	程式庫	ContentLibrary.DeleteSubscribedLibrary
刪除已發佈程式庫的訂閱	允許刪除程式庫的訂閱。	程式庫	ContentLibrary.DeleteSubscription
下載檔案	允許從內容程式庫下載檔案。	程式庫	ContentLibrary.DownloadSession
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。	ContentLibrary.EvictLibraryItem
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	ContentLibrary.EvictSubscribedLibrary

表 16-8. 內容程式庫權限 (續)

vSphere Client 中的 權限名稱	說明	要求	API 中的權限名稱
匯入儲存區	如果來源檔案 URL 以 ds:// 或 file:// 開頭，將允許使用者匯入程式庫項目。依預設，將停用內容程式庫管理員的此權限。由於從儲存區 URL 匯入即表示匯入內容，因此只有在必要時以及在執行匯入的使用者不存在安全性問題時，才會啟用此權限。	程式庫	ContentLibrary.ImportStorage
在指定的計算資源上管理 Harbor 登錄資源	允許管理 VMware Tanzu Harbor 登錄資源。	運算叢集	ContentLibrary.ManageClusterRegistryResource
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	ContentLibrary.ProbeSubscription
將程式庫項目發佈至其訂閱者	允許向訂閱者發佈程式庫項目。	程式庫。將此權限設定為散佈到所有程式庫項目。	ContentLibrary.PublishLibraryItem
將程式庫發佈至其訂閱者	允許向訂閱者發佈程式庫。	程式庫	ContentLibrary.PublishLibrary
讀取儲存區	允許讀取內容程式庫儲存區。	程式庫	ContentLibrary.ReadStorage
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。	ContentLibrary.SyncLibraryItem
同步已訂閱程式庫	允許同步已訂閱程式庫。	程式庫	ContentLibrary.SyncLibrary
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	ContentLibrary.TypeIntrospection
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 Client 使用者介面元素。	程式庫	ContentLibrary.UpdateConfiguration

表 16-8. 內容程式庫權限 (續)

vSphere Client 中的			
權限名稱	說明	要求	API 中的權限名稱
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	ContentLibrary.UpdateSession
更新程式庫	允許更新內容程式庫。	程式庫	ContentLibrary.UpdateLibrary
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。	ContentLibrary.UpdateLibraryItem
更新本機程式庫	允許更新本機程式庫。	程式庫	ContentLibrary.UpdateLocalLibrary
更新已訂閱程式庫	允許更新已訂閱程式庫的內容。	程式庫	ContentLibrary.UpdateSubscribedLibrary
更新已發佈程式庫的訂閱	允許更新訂閱參數。使用者可以更新已訂閱程式庫的 vCenter Server 執行個體規格及其虛擬機器範本項目放置等參數。	程式庫	ContentLibrary.UpdateSubscription
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 Client 使用者介面元素。	程式庫	ContentLibrary.GetConfiguration

密碼編譯作業權限

密碼編譯作業權限可控制對特定類型的物件執行特定類型密碼編譯作業的人員。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表 16-9. 密碼編譯作業權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
直接存取	允許使用者存取加密的資源。使用者可以匯出虛擬機器、對虛擬機器進行 NFC 存取，以及開啟已加密虛擬機器的主控台工作階段。	虛擬機器、主機或資料存放區	Cryptographer.Access
新增磁碟	允許使用者將磁碟新增到加密的虛擬機器。	虛擬機器	Cryptographer.AddDisk
複製	允許使用者複製加密的虛擬機器。	虛擬機器	Cryptographer.Clone
解密	允許使用者解密虛擬機器或磁碟。	虛擬機器	Cryptographer.Decrypt
加密	允許使用者加密虛擬機器或虛擬機器磁碟。	虛擬機器	Cryptographer.Encrypt
加密新增項目	允許使用者在建立虛擬機器期間加密虛擬機器，或在建立磁碟期間加密磁碟。	虛擬機器資料夾	Cryptographer.EncryptNew
管理加密原則	允許使用者使用加密 IO 篩選器管理虛擬機器儲存區原則。依預設，使用加密儲存區原則的虛擬機器不會使用其他儲存區原則。	vCenter Server 根資料夾	Cryptographer.ManageEncryptionPolicy
管理 KMS	允許使用者管理 vCenter Server 系統的金鑰管理伺服器。管理工作包括新增和移除 KMS 執行個體，以及建立與 KMS 的信任關係。	vCenter Server 系統	Cryptographer.ManageKeyServers

表 16-9. 密碼編譯作業權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
管理金鑰	允許使用者執行金鑰管理作業。vSphere Client 中不支援這些作業，但可以使用 crypto-util 或 API 來執行這些作業。	vCenter Server 根資料夾	Cryptographer.ManageKeys
移轉	允許使用者將加密的虛擬機器移轉至其他 ESXi 主機。支援使用或不使用 vMotion 和 Storage vMotion 的移轉。支援移轉到其他 vCenter Server 執行個體。	虛擬機器	Cryptographer.Migrate
Recrypt	允許使用者使用不同金鑰對虛擬機器或磁碟進行雙重加密。深度和淺層雙重加密作業都需要此權限。	虛擬機器	Cryptographer.Recrypt
登錄虛擬機器	允許使用者向 ESXi 主機登錄加密的虛擬機器。	虛擬機器資料夾	Cryptographer.RegisterVM
登錄主機	允許使用者在主機上啟用加密。您可以在主機上明確啟用加密，虛擬機器建立程序也可以啟用加密。	獨立主機的主機資料夾、叢集中主機的叢集	Cryptographer.RegisterHost
讀取 KMS 資訊	允許使用者列出 vCenter Server 和主機上的 vSphere Native Key Provider。此外，還允許使用者取得 vSphere Native Key Provider 資訊。	vCenter Server 或主機	Cryptographer.ReadKeyServersInfo

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 16-10. 分散式虛擬連接埠群組權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
建立	允許建立分散式虛擬連接埠群組。	虛擬連接埠群組	DVPortgroup.Create
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	DVPortgroup.Delete
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	DVPortgroup.Modify
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	DVPortgroup.PolicyOp
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	DVPortgroup.ScopeOp

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 16-11. vSphere Distributed Switch 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
建立	允許建立分散式交換器。	資料中心、網路資料夾	DVSwitch.Create
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	DVSwitch.Delete
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	DVSwitch.HostOp
修改	允許變更分散式交換器的組態。	分散式交換器	DVSwitch.Modify

表 16-11. vSphere Distributed Switch 權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
移動	允許將 vSphere Distributed Switch 移到其他資料夾。	分散式交換器	DVSwitch.Move
Network I/O Control 作業	允許變更 vSphere Distributed Switch 的資源設定。	分散式交換器	DVSwitch.ResourceManagement
原則作業	允許變更 vSphere Distributed Switch 的原則。	分散式交換器	DVSwitch.PolicyOp
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	DVSwitch.PortConfig
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	DVSwitch.PortSetting
VSPAN 作業	允許變更 vSphere Distributed Switch 的 VSPAN 組態。	分散式交換器	DVSwitch.Vspan

資料中心權限

資料中心權限控制在 vSphere 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 16-12. 資料中心權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	Datacenter.Create
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	Datacenter.Move
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	Datacenter.IpPoolConfig
查詢 IP 集區配置	允許設定 IP 位址集區。	資料中心	Datacenter.IpPoolQueryAllocations
重新設定資料中心	允許重新設定資料中心。	資料中心	Datacenter.Reconfigure
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	Datacenter.IpPoolReleaseIp

表 16-12. 資料中心權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	Datacenter.Delete
重新命名資料中心	允許變更資料中心的名稱。	資料中心	Datacenter.Rename
更新資料中心 Carbon 資訊	允許收集與能量和碳測量相 關的度量。	資料中心	Datacenter.UpdateCarbonInfo

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 16-13. 資料存放區權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	Datastore.AllocateSpace
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	Datastore.Browse
設定資料存放區 IO 管理	允許設定 Storage I/O Control。	資料存放區	Datastore.ConfigIOManagement
設定資料存放區	允許設定資料存放區。	資料存放區	Datastore.Config
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	Datastore.FileManagement
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	Datastore.Move

表 16-13. 資料存放區權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	Datastore.Delete
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	Datastore.DeleteFile
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	Datastore.Rename
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	Datastore.UpdateVirtualMachineFiles
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	Datastore.UpdateVirtualMachineMetadata

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 16-14. 資料存放區叢集權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	StoragePod.Config

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 16-15. ESX Agent Manager

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
設定	允許在主機或叢集上部署代理程式虛擬機器。	虛擬機器	EAM.Config
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	EAM.Modify
檢視	允許檢視代理程式虛擬機器。	虛擬機器	EAM.View

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 16-16. 延伸權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
登錄延伸	允許延伸登錄 (外掛程式)。	根 vCenter Server	Extension.Register
解除登錄延伸	允許取消登錄延伸 (外掛程式)。	根 vCenter Server	Extension.Unregister
更新延伸	允許更新延伸 (外掛程式)。	根 vCenter Server	Extension.Update

外部統計資料提供者權限

外部統計資料提供者權限可控制通知 vCenter Server 有關 Proactive Distributed Resource Scheduler (DRS) 統計資料的能力。

這些權限僅適用於 VMware 內部的 API。

資料夾權限

資料夾權限控制建立和管理資料夾的能力。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表 16-17. 資料夾權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
建立資料夾	允許建立新資料夾。	資料夾	Folder.Create
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	Folder.Delete
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	Folder.Move
重新命名資料夾	允許變更資料夾的名稱。	資料夾	Folder.Rename

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 16-18. 全域權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	Global.VCServer
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	Global.CancelTask
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	Global.CapacityPlanning
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	Global.Diagnostics

表 16-18. 全域權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	Global.DisableMethods
啟用方法	允許 vCenter Server 延伸的伺服器對 vCenter Server 管理的物件啟用某些作業。	根 vCenter Server	Global.EnableMethods
全域標籤	允許新增或移除全域標籤。	根主機或 vCenter Server	Global.GlobalTag
健全狀況	允許檢視 vCenter Server 元件的健全狀況。	根 vCenter Server	Global.Health
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	Global.Licenses
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	Global.LogEvent
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	Global.ManageCustomFields
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	Global.Proxy
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	Global.ScriptAction
服務管理員	允許在 ESXCLI 中使用 <code>resxstop</code> 命令。	根主機或 vCenter Server	Global.ServiceManagers
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	Global.SetCustomField
設定	允許讀取並修改執行階段 vCenter Server 組態設定。	根 vCenter Server	Global.Settings
系統標籤	允許新增或移除系統標籤。	根 vCenter Server	Global.SystemTag

混合連結模式權限

混合連結模式權限控制將雲端 vCenter Server 執行個體與內部部署 vCenter Single Sign-On 網域連結的各個方面。(適用於 VMware Cloud on AWS。)

表 16-19. 混合連結模式權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
建立	允許建立和刪除社群所需的完整管理層級存取權。	SDDC	HLM.Create
管理	允許為來源建立信任和存取社群 (讀取層級)。	SDDC	HLM.Manage

健全狀況更新提供者權限

健全狀況更新提供者權限可控制硬體廠商通知 vCenter Server 有關 Proactive HA 事件的能力。

這些權限僅適用於 VMware 內部的 API。

主機 CIM 權限

主機 CIM 權限控制主機健全狀況監控的 CIM 使用。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表 16-20. 主機 CIM 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> CIM CIM 互動 	允許用戶端取得用於 CIM 服務的票證。	主機	Host.Cim.CimInteraction

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 16-21. 主機組態權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> 組態 進階設定 	允許設定進階主機組態選項。	主機	Host.Config.AdvancedConfig
<ul style="list-style-type: none"> 組態 驗證存放區 	允許設定 Active Directory 驗證儲存。	主機	Host.Config.AuthenticationStore

表 16-21. 主機組態權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
■ 組態 ■ 變更 PciPassthru 設定	允許變更主機的 PciPassthru 設定。	主機	Host.Config.PciPassthru
■ 組態 ■ 變更 SNMP 設定	允許變更主機的 SNMP 設定。	主機	Host.Config.Snmp
■ 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	Host.Config.DateTime
■ 組態 ■ 變更設定	允許在 ESXi 主機上設定鎖定模式。	主機	Host.Config.Settings
■ 組態 ■ 連線	允許變更主機的連線狀態 (連線或中斷連線)。	主機	Host.Config.Connection
■ 組態 ■ 韌體	允許更新 ESXi 主機的韌體。	主機	Host.Config.Firmware
■ 組態 ■ GuestStore 設定	允許對 GuestStore 進行變更。	GuestStore 存放庫	Host.Config.GuestStore
■ 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	Host.Config.HyperThreading
■ 組態 ■ 映像組態	允許變更與主機相關聯的映像。		Host.Config.Image
■ 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	Host.Config.Maintenance
■ 組態 ■ 記憶體組態	允許修改主機組態。	主機	Host.Config.Memory
■ 組態 ■ NVDIMM	允許讀取和設定非揮發性 DIMM。	主機	Host.Config.Nvdim
■ 組態 ■ 網路組態	允許設定網路、防火牆和 vMotion 網路。	主機	Host.Config.Network
■ 組態 ■ 電源	允許設定主機電源管理設定。	主機	Host.Config.Power
■ 組態 ■ ProductLocker 設定	允許設定 ESXi productlocker 資料夾。	主機	Host.Config.ProductLocker
■ 組態 ■ 隔離	允許將主機置於隔離模式。	主機	Host.Config.Quarantine
■ 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	Host.Config.Patch

表 16-21. 主機組態權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 組態 <ul style="list-style-type: none"> ■ 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	Host.Config.NetService
<ul style="list-style-type: none"> ■ 組態 <ul style="list-style-type: none"> ■ 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	Host.Config.Storage
<ul style="list-style-type: none"> ■ 組態 <ul style="list-style-type: none"> ■ 系統管理 	允許延伸，以操縱主機上的檔案系統。	主機	Host.Config.SystemManagement
<ul style="list-style-type: none"> ■ 組態 <ul style="list-style-type: none"> ■ 系統資源 	允許更新系統資源階層的組態。	主機	Host.Config.Resources
<ul style="list-style-type: none"> ■ 組態 <ul style="list-style-type: none"> ■ 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	Host.Config.AutoStart

主機熵集區權限

主機熵集區權限控制檢視和新增 ESXi 主機熵的能力。

表 16-22. 主機熵集區權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 熵集區 <ul style="list-style-type: none"> ■ 讀取 	允許讀取主機熵集區資訊。	主機	Host.Entropy.Read
<ul style="list-style-type: none"> ■ 熵集區 <ul style="list-style-type: none"> ■ 寫入 	允許向主機熵集區新增熵。	主機	Host.Entropy.Write

主機的 Intel Software Guard Extensions 權限

主機的 Intel Software Guard Extensions 權限控制多通訊端 ESXi 主機上遠端證明的各個方面。

表 16-23. 主機的 Intel Software Guard Extensions (SGX) 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ Intel Software Guard Extensions (SGX) <ul style="list-style-type: none"> ■ Intel Software Guard Extensions (SGX) 登錄主機 	允許向 Intel SGX 登錄服務登錄主機 (使 SGX 工作負載能夠在支援多通訊端 SGX 的主機上執行時執行 SGX 遠端證明)。	主機	Host.Sgx.Register

主機詳細目錄權限

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 16-24. 主機詳細目錄權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
■ 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	Host.Inventory.AddHostToCluster
■ 詳細目錄 ■ 新增獨立主機	允許新增獨立主機。	主機資料夾	Host.Inventory.AddStandaloneHost
■ 詳細目錄 ■ 建立叢集	允許建立新的叢集。	主機資料夾	Host.Inventory.CreateCluster
■ 詳細目錄 ■ 管理叢集生命週期	允許管理叢集。	叢集	Host.Inventory.ManageClusterLifecycle
■ 詳細目錄 ■ 修改叢集	允許變更叢集的內容。	叢集	Host.Inventory.EditCluster
■ 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	Host.Inventory.MoveCluster
■ 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	Host.Inventory.MoveHost
■ 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	Host.Inventory.DeleteCluster
■ 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	Host.Inventory.RemoveHostFromCluster
■ 詳細目錄 ■ 重新命名叢集	允許重新命名叢集。	叢集	Host.Inventory.RenameCluster

主機本機作業權限

當 VMware Host Client 直接連線到主機時執行的主機本機作業權限控制動作。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表 16-25. 主機本機作業權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 本機作業 <ul style="list-style-type: none"> ■ 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	Host.Local.InstallAgent
<ul style="list-style-type: none"> ■ 本機作業 <ul style="list-style-type: none"> ■ 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	Host.Local.CreateVM
<ul style="list-style-type: none"> ■ 本機作業 <ul style="list-style-type: none"> ■ 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	Host.Local.DeleteVM
<ul style="list-style-type: none"> ■ 本機作業 <ul style="list-style-type: none"> ■ 管理使用者群組 	允許在主機上管理本機帳戶。	根主機	Host.Local.ManageUserGroups
<ul style="list-style-type: none"> ■ 本機作業 <ul style="list-style-type: none"> ■ 重新設定虛擬機器 	允許重新設定虛擬機器。	根主機	Host.Local.ReconfigVM

主機統計資料權限

主機統計資訊權限控制從資料處理裝置 (DPU) 存取統計資訊的能力。

這些權限僅適用於 VMware 內部的 API。

主機信賴平台模組權限

主機信賴平台模組權限控制與管理信賴平台模組 (TPM) 晶片相關的作業。

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 16-26. 主機信賴平台模組權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 信賴平台模組 <ul style="list-style-type: none"> ■ 讀取 ■ 解除封裝 	<p>讀取 允許讀取有關 ESXi 主機中安裝的 TPM 狀態的詳細資訊。</p> <p>解除封裝 允許請求 ESXi 主機解密查問以證明其狀態。</p>	主機	<p>Host.Tpm.Read</p> <p>Host.Tpm.Unseal</p>

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 16-27. 主機 vSphere Replication 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ vSphere Replication ■ 管理複寫 	允許管理此主機上的虛擬機器複寫。	主機	Host.Hbr.HbrManagement

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 16-28. 主機設定檔權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
清除	允許清除設定檔相關的資訊。	根 vCenter Server	Profile.Clear
建立	允許建立主機設定檔。	根 vCenter Server	Profile.Create
刪除	允許刪除主機設定檔。	根 vCenter Server	Profile.Delete
編輯	允許編輯主機設定檔。	根 vCenter Server	Profile.Edit
匯出	允許匯出主機設定檔。	根 vCenter Server	Profile.Export
檢視	允許檢視主機設定檔。	根 vCenter Server	Profile.View

vCenter Server 設定檔權限

vCenter Server 設定檔權限控制列出設定檔以及將組態從一個 vCenter Server 匯出和匯入到另一個的各個方面。

表 16-29. vCenter Server 設定檔權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
vCenter Server 設定檔讀取權限	允許列出和匯出 vCenter Server 設定檔	vCenter Server	Infraprofile.Read
vCenter Server 設定檔寫入權限	允許將設定檔匯入另一個 vCenter Server 中並對其進行驗證。	vCenter Server	Infraprofile.Write

vSphere with Tanzu 權限

命名空間權限可控制哪些人可以建立和管理 VMware vSphere® with VMware Tanzu™ 命名空間。

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 16-30. 命名空間權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
允許磁碟解除委任作業	允許對資料存放區執行解除委任作業。	資料存放區	Namespaces.ManageDisks
備份工作負載元件檔案	允許備份 etcd 叢集的內容 (僅在 VMware Cloud on AWS 中使用)。	叢集	Namespaces.Backup
列出可存取的命名空間	允許列出可存取的命名空間。	叢集	Namespaces.ListAccess
修改叢集範圍的組態	允許修改叢集範圍的組態，以及啟用和停用叢集命名空間。	叢集	Namespaces.ManageCapabilities
修改叢集範圍的命名空間自助服務組態	允許修改命名空間自助服務組態。	叢集 (用於啟動與停用) 範本 (用於修改組態) vCenter Server (用於建立範本)	Namespaces.SelfServiceManage
修改命名空間組態	允許修改命名空間組態選項，例如資源配置和使用者權限。	叢集	Namespaces.Manage
切換叢集功能	允許操縱叢集功能的狀態 (僅在 VMware Cloud on AWS 內部使用)。	叢集	NA
將叢集升級到較新版本	允許啟動叢集升級。	叢集	Namespaces.Upgrade

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 16-31. 網路權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
指派網路	允許將網路指派到虛擬機器。	網路、虛擬機器	Network.Assign
設定	允許設定網路。	網路、虛擬機器	Network.Config
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 and 目的地位置。	網路	Network.Move
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	Network.Delete

NSX 權限

NSX 權限控制與 NSX 管理相關的工作。

表 16-32. NSX 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
讀取 NSX 組態	允許讀取 NSX 物件。	NSX	Nsx.Read
管理 NSX 組態	允許從 vSphere 管理員的角度管理 NSX 物件。	NSX	Nsx.Manage
修改 NSX 組態	允許從企業管理員的角度管理 NSX 物件。	NSX	Nsx.ModifyAll

VMware 可觀察性權限

VMware 可觀察性權限控制代理程式存取 vCenter Server 上可觀察性 API 的能力。

這些權限僅適用於 VMware 內部的 API。

OvfManager 權限

OvfManager 權限控制存取 vService Manager 的能力。

這些權限僅適用於 VMware 內部的 API。

與合作夥伴 REST 精靈互動權限

與合作夥伴 REST 精靈互動權限控制對讀取和寫入作業的存取。

表 16-33. 與合作夥伴 REST 精靈互動權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
從合作夥伴的 REST 精靈執行 GET 作業	允許合作夥伴佈建的 REST 用戶端執行 GET 作業。	執行 GET 作業的合作夥伴使用者。	PartnerRestDaemon.Read
對合作夥伴的 REST 精靈執行修改作業	允許合作夥伴佈建的 REST 用戶端執行 POST、PUT 和 DELETE 作業。	執行 POST、PUT 或 DELETE 作業的合作夥伴使用者。	PartnerRestDaemon.Write

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 16-34. 效能權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	Performance.ModifyIntervals

外掛程式權限

外掛程式權限控制 vSphere Client 外掛程式的管理。

表 16-35. 外掛程式權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
管理外掛程式	允許管理 vSphere Client 外掛程式。	vCenter Server	Plugin.Management

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 16-36. 權限 (Permissions) 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	Authorization.ModifyPermissions
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 Client 使用者介面元素。	任何物件	Authorization.ModifyPrivileges
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	Authorization.ModifyRoles
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	Authorization.ReassignRolePermissions

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 16-37. 資源權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	Resource.ApplyRecommendation
將 vApp 指派給資源集區	允許將 vApp 指派到資源集區。	資源集區	Resource.AssignVAppToPool
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	Resource.AssignVMToPool

表 16-37. 資源權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
建立資源集區	允許建立資源集區。	資源集區, 叢集	Resource.CreatePool
移轉已關閉電源的虛擬機器	允許將已關閉電源的虛擬機器移轉到不同的資源集區或主機。	虛擬機器	Resource.ColdMigrate
移轉已開啟電源的虛擬機器	允許運用 vMotion 將已開啟電源的虛擬機器移轉到不同的資源集區或主機。		Resource.HotMigrate
修改資源集區	允許變更資源集區的配置。	資源集區	Resource.EditPool
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 and 目的地位置。	資源集區	Resource.MovePool
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	Resource.QueryVMotion
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	Resource.DeletePool
重新命名資源集區	允許重新命名資源集區。	資源集區	Resource.RenamePool

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 16-38. 排定的工作權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	ScheduledTask.Create
修改工作	允許重新設定排定的工作的內容。	任何物件	ScheduledTask.Edit
移除工作	允許移除佇列中排定的工作。	任何物件	ScheduledTask.Delete
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	ScheduledTask.Run

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 16-39. 工作階段權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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	Sessions.ImpersonateUser
訊息	允許設定全域登入訊息。	根 vCenter Server	Sessions.GlobalMessage
驗證工作階段	允許驗證工作階段有效性。	根 vCenter Server	Sessions.ValidateSession
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	Sessions.TerminateSession
privilege.StorageProfile.ViewPermissions.label	允許收集工作階段。	根 vCenter Server	Sessions.CollectPrivilegeChecks

虛擬機器儲存區原則權限

虛擬機器儲存區原則權限控制為虛擬機器建立和管理儲存區原則的能力。

表 16-40. 虛擬機器儲存區原則權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
套用虛擬機器儲存區原則	允許使用虛擬機器儲存區原則。	根 vCenter Server	StorageProfile.Apply
更新虛擬機器儲存區原則	允許建立和更新虛擬機器儲存區設定檔。	根 vCenter Server	StorageProfile.Update
虛擬機器儲存區原則編輯權限	允許編輯指派的虛擬機器儲存區原則。	根 vCenter Server	StorageProfile.EditPermissions
虛擬機器儲存區原則檢視權限	允許檢視虛擬機器儲存區原則的可用權限。	根 vCenter Server	StorageProfile.ViewPermissions
檢視虛擬機器儲存區原則	允許檢視定義的虛擬機器儲存區原則。	根 vCenter Server	StorageProfile.View

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 16-41. 儲存區視圖權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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 的唯一讀權限。	根 vCenter Server	StorageViews.ConfigureService
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	StorageViews.View

主管服務權限

主管服務權限控制哪些使用者可以在 vSphere with Tanzu 環境中建立和管理主管服務。

表 16-42. 主管服務權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
管理主管服務	允許建立、更新或刪除主管服務。還允許在叢集上安裝主管服務，以及建立或刪除主管服務版本。	叢集	SupervisorServices.Manage

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 16-43. 工作權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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 Client 使用者介面元素。	根 vCenter Server	Task.Create
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 Client 使用者介面元素。	根 vCenter Server	Task.Update

承租人管理權限

承租人管理權限控制定義和擷取承租人管理實體的各個方面。(適用於 VMware Cloud on AWS。)

表 16-44. 承租人管理權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
承租人佈建作業	允許定義一組用於承租人管理的資源。	根資料夾和目前標記為服務提供者的每個實體。	TenantManager.Update
承租人查詢作業	允許擷取承租人管理資源清單。	根資料夾和目前標記為服務提供者的每個實體。	TenantManager.Query

Transfer Service 權限

Transfer Service 權限為 VMware 內部權限。請勿使用這些權限。

VcTrusts/VcIdentity 權限

VcTrusts/VcIdentity 權限控制對與 vCenter Server 系統之間的信任相關的各種內部 API 及功能的存取權。

表 16-45. VcTrusts/VcIdentity 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
建立/更新/刪除 (管理員權限)	允許對與 vCenter Server 系統之間的信任相關的各種內部 API 及功能的完整管理層級存取權。	不適用	Trust.Administer
建立/更新/刪除 (低於管理員權限)	允許對與 vCenter Server 系統之間的信任相關的各種內部 API 及功能的精簡管理存取權。此權限會限制建立/更新/刪除 VcTrusts/VcIdentity，因此使用者無法升階非管理員權限。	不適用	Trust.Manage

受信任基礎結構管理員權限

受信任基礎結構管理員權限將會設定和管理 vSphere Trust Authority 部署。

這些權限決定了哪些人可以對 vSphere Trust Authority 部署執行設定和管理工作。如需有關 Trust Authority 角色和 TrustedAdmins 群組的詳細資訊，請參閱 [vSphere Trust Authority 的必要條件和必要權限](#)。

表 16-46. 受信任基礎結構管理員權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
設定金鑰伺服器信任	允許管理金鑰提供者服務的金鑰提供者。	根 vCenter Server	TrustedAdmin.ManageKMSTrust
設定 Trust Authority 主機 TPM 憑證	允許建立和修改證明服務設定。	根 vCenter Server	TrustedAdmin.ConfigureHostCertificates
設定 Trust Authority 主機中繼資料	允許編輯要由證明服務證明的基礎映像。	根 vCenter Server	TrustedAdmin.ConfigureHostMetadata
設定證明 SSO	允許編輯 Trust Authority 主機可信的主機。	根 vCenter Server	TrustedAdmin.ManageAttestingSSO
設定 Token 轉換原則	允許設定 Token 轉換原則。	根 vCenter Server	TrustedAdmin.ConfigureTokenConversionPolicy
列出受信任基礎結構主機	允許讀取有關受信任主機和 Trust Authority 主機的資訊。	根 vCenter Server	TrustedAdmin.ReadTrustedHosts
列出 STS 的相關資訊	允許匯出受信任主機的詳細資料，以便將其匯入至 Trust Authority 叢集。	根 vCenter Server	TrustedAdmin.ReadStsInfo

表 16-46. 受信任基礎結構管理員權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
管理受信任基礎結構主機	允許編輯有關受信任主機和 Trust Authority 主機的資訊。	根 vCenter Server	TrustedAdmin.ManageTrustedHosts
讀取金鑰伺服器信任	允許讀取金鑰提供者服務的金鑰提供者。	根 vCenter Server	TrustedAdmin.ReadKMSTrust
讀取證明 SSO	允許讀取 Trust Authority 主機可信任的主機。	根 vCenter Server	TrustedAdmin.ReadAttestingSSO
擷取 TPM Trust Authority 主機憑證	允許讀取證明服務的設定。	根 vCenter Server	TrustedAdmin.RetrieveTPMHostCertificates
擷取 Trust Authority 主機中繼資料	允許讀取證明服務可證明的基礎映像。	根 vCenter Server	TrustedAdmin.RetrieveHostMetadata

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 16-47. vApp 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
新增虛擬機器	允許將虛擬機器新增到 vApp。	vApp	VApp.AssignVM
指派資源集區	允許將資源集區指派到 vApp。	vApp	VApp.AssignResourcePool
指派 vApp	允許將一個 vApp 指派給另一個 vApp	vApp	VApp.AssignVApp
複製	允許複製 vApp。	vApp	VApp.Clone
建立	允許建立 vApp。	vApp	VApp.Create
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.Delete
匯出	允許從 vSphere 匯出 vApp。	vApp	VApp.Export

表 16-47. vApp 權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
匯入	允許將 vApp 匯入 vSphere。	vApp	VApp.Import
移動	允許將 vApp 移動到新詳細目錄位置。	vApp	VApp.Move
關閉電源	允許對 vApp 執行關閉電源作業。	vApp	VApp.PowerOff
開啟電源	允許對 vApp 執行開啟電源作業。	vApp	VApp.PowerOn
從 URL 提取	允許列出遠端來源檔案描述元。	vApp	VApp.PullFromUrls
重新命名	允許重新命名 vApp。	vApp	VApp.Rename
暫停	允許暫停 vApp。	vApp	VApp.Suspend
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.Unregister
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.ExtractOvfEnvironment
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.ApplicationConfig
vApp 執行個體組態	允許修改 vApp 的執行個體組態，如原則。	vApp	VApp.InstanceConfig
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 Client 使用者介面元素。	vApp	VApp.ManagedByConfig
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	VApp.ResourceConfig

VcIdentityProviders 權限

VcIdentityProviders 權限控制對 VcIdentityProviders API 的存取權。

表 16-48. VcIdentityProviders 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
建立	允許對 VcIdentityProviders API (vCenter Server 身分識別提供者) 的僅建立權限。	不適用	VcIdentityProviders.Create
管理	允許對 VcIdentityProviders API (vCenter Server 身分識別提供者) 的管理層級寫入權限 (建立、讀取、更新、刪除)。	不適用	VcIdentityProviders.Manage
讀取	允許對 VcIdentityProviders API (vCenter Server 身分識別提供者) 的讀取權限。	不適用	VcIdentityProviders.Read

VMware vSphere Lifecycle Manager 組態權限

VMware vSphere Lifecycle Manager 組態權限可控制設定 vSphere Lifecycle Manager 服務的能力。

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。

備註 僅向管理員或受信任的使用者指派授權使用者叫用 VMware vSphere Lifecycle Manager API (接受 URL) 的權限。

表 16-49. VMware vSphere Lifecycle Manager 組態權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 設定 <ul style="list-style-type: none"> ■ 設定服務 	允許設定 vSphere Lifecycle Manager 服務和排定的修補程式下載工作。	根 vCenter Server	VcIntegrity.General.com.vmware.vcIntegrity.Configure

VMware vSphere Lifecycle Manager ESXi 健全狀況透視圖權限

VMware vSphere Lifecycle Manager ESXi 健全狀況透視圖權限可控制檢查 ESXi 主機和叢集之健全狀況的能力。

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 16-50. VMware vSphere Lifecycle Manager ESXi 健全狀況透視圖權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ ESXi 健全狀況透視圖 <ul style="list-style-type: none"> ■ 讀取 ■ 寫入 	讀取 允許查詢 ESXi 主機和叢集的健全狀況。目前未使用寫入。	主機叢集	VcIntegrity.lifecycleHealth.Read VcIntegrity.lifecycleHealth.Write

VMware vSphere Lifecycle Manager 一般權限

VMware vSphere Lifecycle Manager 一般權限可控制讀取和寫入 Lifecycle Manager 資源的能力。

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 16-51. VMware vSphere Lifecycle Manager 一般權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ Lifecycle Manager：一般權限 <ul style="list-style-type: none"> ■ 讀取 ■ 寫入 	讀取 允許讀取 vSphere Lifecycle Manager 資源。需要此權限才能取得工作資訊。 寫入 允許寫入 vSphere Lifecycle Manager 資源。需要此權限才能取消 vSphere Lifecycle Manager 工作。	根 vCenter Server	VcIntegrity.lifecycleGeneral.Read VcIntegrity.lifecycleGeneral.Write

VMware vSphere Lifecycle Manager 硬體相容性權限

VMware vSphere Lifecycle Manager 硬體相容性權限可控制探索和解決潛在硬體相容性問題的能力。

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 16-52. VMware vSphere Lifecycle Manager 硬體相容性權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ Lifecycle Manager：硬體相容性權限 <ul style="list-style-type: none"> ■ 存取硬體相容性 ■ 寫入 	存取硬體相容性 和 寫入 允許存取硬體相容性資料並解決潛在的硬體相容性問題。	主機	VcIntegrity.HardwareCompatibility.Read VcIntegrity.HardwareCompatibility.Write

VMware vSphere Lifecycle Manager 映像權限

VMware vSphere Lifecycle Manager 映像權限可控制管理映像的能力。

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。

備註 僅向管理員或受信任的使用者指派授權使用者叫用 VMware vSphere Lifecycle Manager API (接受 URL) 的權限。

表 16-53. VMware vSphere Lifecycle Manager 映像權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ Lifecycle Manager: 映像權限 <ul style="list-style-type: none"> ■ 讀取 ■ 寫入 	<p>讀取 允許讀取 vSphere Lifecycle Manager 映像。需要此權限才能執行下列操作：</p> <ul style="list-style-type: none"> ■ 列出叢集的所有草稿 ■ 取得有關草稿的詳細資訊 ■ 對草稿執行掃描 ■ 驗證草稿 ■ 擷取草稿的內容 ■ 計算有效元件清單 ■ 取得目前所需狀態文件的內容 ■ 在叢集上啟動掃描 ■ 取得符合性結果 ■ 取得建議 ■ 將目前所需狀態匯出為存放庫、JSON 檔案或 ISO <p>寫入 允許管理 vSphere Lifecycle Manager 映像。需要此權限才能執行下列操作：</p> <ul style="list-style-type: none"> ■ 建立、刪除或認可草稿 ■ 匯入所需的狀態 ■ 產生建議 ■ 設定或刪除草稿的不同部分 	根 vCenter Server	VcIntegrity.lifecycleSettings.Read VcIntegrity.lifecycleSettings.Write

VMware vSphere Lifecycle Manager 映像修復權限

VMware vSphere Lifecycle Manager 映像權限可控制修復映像的能力。

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 16-54. VMware vSphere Lifecycle Manager 映像修復權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ Lifecycle Manager : 映像修復權限 <ul style="list-style-type: none"> ■ 讀取 ■ 寫入 	讀取 允許執行修復預先檢查。 寫入 允許執行修復。	叢集	VcIntegrity.lifecycleSoftwareRemediation. Read VcIntegrity.lifecycleSoftwareRemediation. Write

VMware vSphere Lifecycle Manager 設定權限

VMware vSphere Lifecycle Manager 設定權限可控制管理存放庫和修復原則的能力。

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。

備註 僅向管理員或受信任的使用者指派授權使用者叫用 VMware vSphere Lifecycle Manager API (接受 URL) 的權限。

表 16-55. VMware vSphere Lifecycle Manager 設定權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ Lifecycle Manager : 設定權限 <ul style="list-style-type: none"> ■ 讀取 ■ 寫入 	讀取 允許讀取 vSphere Lifecycle Manager 存放庫和修復原則。 寫入 允許寫入 vSphere Lifecycle Manager 存放庫和修復原則。	根 vCenter Server	VcIntegrity.lifecycleSoftwareSpecification. Read VcIntegrity.lifecycleSoftwareSpecification. Write

VMware vSphere Lifecycle Manager 管理基準權限

VMware vSphere Lifecycle Manager 管理基準權限可控制管理基準和基準群組的能力。

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 16-56. VMware vSphere Lifecycle Manager 管理基準權限

權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 管理基準 <ul style="list-style-type: none"> ■ 連結基準 ■ 管理基準 	連結基準 允許將基準和基準群組連結到 vSphere 詳細目錄中的物件。 管理基準 允許建立、編輯或刪除基準和基準群組。	根 vCenter Server	VcIntegrity.Baseline.com.vmware.vcIntegrity.AssignBaselines VcIntegrity.Baseline.com.vmware.vcIntegrity.ManageBaselines

VMware vSphere Lifecycle Manager 管理修補程式和升級權限

VMware vSphere Lifecycle Manager 管理修補程式和升級權限可控制檢視、掃描和修復適用的修補程式、延伸或升級的能力。

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 16-57. VMware vSphere Lifecycle Manager 管理修補程式和升級權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 管理修補程式和升級 <ul style="list-style-type: none"> ■ 修復以套用修補程式、延伸和升級 ■ 掃描適用的修補程式、延伸和升級 ■ 暫存修補程式和延伸 ■ 檢視符合性狀態 	<p>修復以套用修補程式、延伸和升級 允許在使用基準時修復虛擬機器和主機以套用修補程式、延伸或升級。此外，此權限還允許檢視符合性狀態。</p> <p>掃描適用的修補程式、延伸和升級 允許在使用基準時掃描虛擬機器和主機以搜尋適用的修補程式、延伸或升級。</p> <p>暫存修補程式和延伸 允許在使用基準時將修補程式或延伸暫存至 ESXi 主機。此外，此權限還允許檢視 ESXi 主機的符合性狀態。</p> <p>檢視符合性狀態 允許檢視 vSphere 詳細目錄中物件的基準符合性資訊。</p>	根 vCenter Server	<p>VcIntegrity.Updates.com.vmware.vcIntegrity.Remediate</p> <p>VcIntegrity.Updates.com.vmware.vcIntegrity.Scan</p> <p>VcIntegrity.Updates.com.vmware.vcIntegrity.Stage</p> <p>VcIntegrity.Updates.com.vmware.vcIntegrity.ViewStatus</p>

VMware vSphere Lifecycle Manager 上傳檔案權限

VMware vSphere Lifecycle Manager 上傳檔案權限可控制將更新匯入 vSphere Lifecycle Manager 存放庫的能力。

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。

備註 僅向管理員或受信任的使用者指派授權使用者叫用 VMware vSphere Lifecycle Manager API (接受 URL) 的權限。

表 16-58. VMware vSphere Lifecycle Manager 上傳檔案權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 上傳檔案 <ul style="list-style-type: none"> ■ 上傳檔案 	允許上傳升級 ISO 和離線修補程式服務包。	根 vCenter Server	VcLifecycle.Upgrade

虛擬機器變更組態權限

虛擬機器變更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 16-59. 虛擬機器變更組態權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
■ 變更組態 ■ 擷取磁碟租用	允許對虛擬機器執行磁碟租用作業。	虛擬機器	VirtualMachine.Config.DiskLease
■ 變更組態 ■ 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	VirtualMachine.Config.AddExistingDisk
■ 變更組態 ■ 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	VirtualMachine.Config.AddNewDisk
■ 變更組態 ■ 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	VirtualMachine.Config.AddRemoveDevice
■ 變更組態 ■ 進階組態	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	VirtualMachine.Config.AdvancedConfig
■ 變更組態 ■ 變更 CPU 計數	允許變更虛擬 CPU 的數目。	虛擬機器	VirtualMachine.Config.CPUCount
■ 變更組態 ■ 變更記憶體	允許變更配置給虛擬機器的記憶體數量。	虛擬機器	VirtualMachine.Config.Memory
■ 變更組態 ■ 變更設定	允許變更一般虛擬機器設定。	虛擬機器	VirtualMachine.Config.Settings
■ 變更組態 ■ 變更分頁檔放置	允許變更虛擬機器的分頁檔放置原則。	虛擬機器	VirtualMachine.Config.SwapPlacement
■ 變更組態 ■ 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	VirtualMachine.Config.Resource
■ 變更組態 ■ 設定主機 USB 裝置	允許將主機式 USB 裝置連結到虛擬機器。	虛擬機器	VirtualMachine.Config.HostUSBDevice
■ 變更組態 ■ 設定原始裝置	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	VirtualMachine.Config.RawDevice

表 16-59. 虛擬機器變更組態權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 變更組態 ■ 設定管理者 	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	VirtualMachine.Config.ManagedBy
<ul style="list-style-type: none"> ■ 變更組態 ■ 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	VirtualMachine.Config.MksControl
<ul style="list-style-type: none"> ■ 變更組態 ■ 擴充虛擬磁碟 	允許擴充虛擬磁碟的大小。	虛擬機器	VirtualMachine.Config.DiskExtend
<ul style="list-style-type: none"> ■ 變更組態 ■ 修改裝置設定 	允許變更現有裝置的內容。	虛擬機器	VirtualMachine.Config.EditDevice
<ul style="list-style-type: none"> ■ 變更組態 ■ 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	VirtualMachine.Config.QueryFTCompatibility
<ul style="list-style-type: none"> ■ 變更組態 ■ 查詢無人負責的檔案 	允許查詢無人負責的檔案。	虛擬機器	VirtualMachine.Config.QueryUnownedFiles
<ul style="list-style-type: none"> ■ 變更組態 ■ 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	VirtualMachine.Config.ReloadFromPath
<ul style="list-style-type: none"> ■ 變更組態 ■ 移除磁碟 	允許移除虛擬磁碟裝置。	虛擬機器	VirtualMachine.Config.RemoveDisk
<ul style="list-style-type: none"> ■ 變更組態 ■ 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	VirtualMachine.Config.Rename
<ul style="list-style-type: none"> ■ 變更組態 ■ 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	VirtualMachine.Config.ResetGuestInfo
<ul style="list-style-type: none"> ■ 變更組態 ■ 設定註解 	允許新增或編輯虛擬機器註釋。	虛擬機器	VirtualMachine.Config.Annotation
<ul style="list-style-type: none"> ■ 變更組態 ■ 切換磁碟變更追蹤 	允許啟用或停用虛擬機器的磁碟變更追蹤。	虛擬機器	VirtualMachine.Config.ChangeTracking

表 16-59. 虛擬機器變更組態權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 變更組態 ■ 切換分支父系 	允許啟用或停用虛擬機器分支父系。	虛擬機器	VirtualMachine.Config.ToggleForkParent
<ul style="list-style-type: none"> ■ 變更組態 ■ 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	VirtualMachine.Config.UpgradeVirtualHardware

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 與檔案和應用程式互動的能力。

如需有關這些作業的詳細資訊，請參閱《vSphere Web Services 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 16-60. 虛擬機器客體作業

vSphere Client 中的權限名稱	說明	生效物件	API 中的權限名稱
<ul style="list-style-type: none"> ■ 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	VirtualMachine.GuestOperations.ModifyAliases
<ul style="list-style-type: none"> ■ 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	VirtualMachine.GuestOperations.QueryAliases
<ul style="list-style-type: none"> ■ 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 Client 使用者介面元素。	虛擬機器	VirtualMachine.GuestOperations.Modify
<ul style="list-style-type: none"> ■ 客體作業 ■ 客體作業程式執行 	允許涉及在虛擬機器中執行應用程式的虛擬機器客體作業。沒有與此權限相關聯的 vSphere Client 使用者介面元素。	虛擬機器	VirtualMachine.GuestOperations.Execute
<ul style="list-style-type: none"> ■ 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 Client 使用者介面元素。	虛擬機器	VirtualMachine.GuestOperations.Query

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 16-61. 虛擬機器互動

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 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	VirtualMachine.Interact.AnswerQuestion
<ul style="list-style-type: none"> ■ 互動 ■ 虛擬機器上的備份作業 	允許對虛擬機器執行備份作業。	虛擬機器	VirtualMachine.Interact.Backup
<ul style="list-style-type: none"> ■ 互動 ■ 設定 CD 媒體 	允許設定虛擬 DVD 或 CD-ROM 裝置。	虛擬機器	VirtualMachine.Interact.SetCDMedia
<ul style="list-style-type: none"> ■ 互動 ■ 設定磁碟片媒體 	允許設定虛擬磁碟片裝置。	虛擬機器	VirtualMachine.Interact.SetFloppyMedia
<ul style="list-style-type: none"> ■ 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	VirtualMachine.Interact.ConsoleInteract
<ul style="list-style-type: none"> ■ 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	VirtualMachine.Interact.CreateScreenshot
<ul style="list-style-type: none"> ■ 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	VirtualMachine.Interact.DefragmentAllDisks
<ul style="list-style-type: none"> ■ 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	VirtualMachine.Interact.DeviceConnection
<ul style="list-style-type: none"> ■ 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	VirtualMachine.Interact.DnD
<ul style="list-style-type: none"> ■ 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	VirtualMachine.Interact.GuestControl
<ul style="list-style-type: none"> ■ 互動 ■ 插入 USB HID 掃描碼 	允許插入 USB HID 掃描碼。	虛擬機器	VirtualMachine.Interact.PutUsbScanCodes
<ul style="list-style-type: none"> ■ 互動 ■ 暫停或取消暫停 	允許暫停或取消暫停虛擬機器。	虛擬機器	VirtualMachine.Interact.Pause

表 16-61. 虛擬機器互動 (續)

vSphere Client 中的 權限名稱	說明	要求	API 中的權限名稱
■ 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	VirtualMachine.Interact.SESparseMaintenance
■ 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	VirtualMachine.Interact.PowerOff
■ 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	VirtualMachine.Interact.PowerOn
■ 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	VirtualMachine.Interact.Record
■ 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	VirtualMachine.Interact.Replay
■ 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	VirtualMachine.Interact.Reset
■ 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	VirtualMachine.Interact.EnableSecondary
■ 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	VirtualMachine.Interact.Suspend
■ 互動 ■ 暫停 Fault Tolerance	允許暫停虛擬機器的 Fault Tolerance 功能。	虛擬機器	VirtualMachine.Interact.DisableSecondary
■ 互動 ■ 暫停到記憶體	允許暫停虛擬機器的記憶體。	虛擬機器	VirtualMachine.Interact.SuspendToMemory
■ 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	VirtualMachine.Interact.MakePrimary
■ 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	VirtualMachine.Interact.DisableSecondary
■ 互動 ■ 關閉 Fault Tolerance	允許關閉虛擬機器的 Fault Tolerance 功能。	虛擬機器	VirtualMachine.Interact.TurnOffFaultTolerance

表 16-61. 虛擬機器互動 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 互動 <ul style="list-style-type: none"> ■ 開啟 Fault Tolerance 	允許開啟虛擬機器的 Fault Tolerance 功能。	虛擬機器	VirtualMachine.Interact.CreateSecondary
<ul style="list-style-type: none"> ■ 互動 <ul style="list-style-type: none"> ■ 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	VirtualMachine.Interact.ToolsInstall

虛擬機器編輯詳細目錄權限

虛擬機器編輯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 16-62. 虛擬機器編輯詳細目錄權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 編輯詳細目錄 <ul style="list-style-type: none"> ■ 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	VirtualMachine.Inventory.CreateFromExisting
<ul style="list-style-type: none"> ■ 編輯詳細目錄 <ul style="list-style-type: none"> ■ 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	VirtualMachine.Inventory.Create
<ul style="list-style-type: none"> ■ 編輯詳細目錄 <ul style="list-style-type: none"> ■ 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	VirtualMachine.Inventory.Move
<ul style="list-style-type: none"> ■ 編輯詳細目錄 <ul style="list-style-type: none"> ■ 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	VirtualMachine.Inventory.Register

表 16-62. 虛擬機器編輯詳細目錄權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 編輯詳細目錄 <ul style="list-style-type: none"> ■ 移除 	<p>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。</p> <p>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。</p>	虛擬機器	VirtualMachine.Inventory.Delete
<ul style="list-style-type: none"> ■ 編輯詳細目錄 <ul style="list-style-type: none"> ■ 解除登錄 	<p>允許從 vCenter Server 或主機詳細目錄中解除登錄虛擬機器。</p> <p>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。</p>	虛擬機器	VirtualMachine.Inventory.Unregister

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 16-63. 虛擬機器佈建權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 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	VirtualMachine.Provisioning.DiskRandomAccess
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 允許檔案存取 	允許在與虛擬機器關聯的檔案上執行作業，包括 vmx、磁碟、記錄和 nvram。	虛擬機器	VirtualMachine.Provisioning.FileRandomAccess
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 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	VirtualMachine.Provisioning.DiskRandomRead
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 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	VirtualMachine.Provisioning.GetVmFiles

表 16-63. 虛擬機器佈建權限 (續)

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 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	VirtualMachine.Provisioning.PutVmFiles
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 複製範本 	允許複製範本。	範本	VirtualMachine.Provisioning.CloneTemplate
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 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	VirtualMachine.Provisioning.Clone
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 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	VirtualMachine.Provisioning.CreateTemplateFromVM
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 自訂客體 	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	VirtualMachine.Provisioning.Customize
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 部署範本 	允許從範本部署虛擬機器。	範本	VirtualMachine.Provisioning.DeployTemplate
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 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	VirtualMachine.Provisioning.MarkAsTemplate
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 標記為虛擬機器 	允許將現有範本標記為虛擬機器。	範本	VirtualMachine.Provisioning.MarkAsVM
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 修改自訂規格 	允許建立、修改或刪除自訂規格。	根 vCenter Server	VirtualMachine.Provisioning.ModifyCustSpecs
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 升階磁碟 	允許對虛擬機器的磁碟進行升階作業。	虛擬機器	VirtualMachine.Provisioning.PromoteDisks
<ul style="list-style-type: none"> ■ 佈建 <ul style="list-style-type: none"> ■ 讀取自訂規格 	允許讀取自訂規格。	虛擬機器	VirtualMachine.Provisioning.ReadCustSpecs

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。

表 16-64. 虛擬機器服務組態權限

vSphere Client 中的權限名稱	說明	API 中的權限名稱
<ul style="list-style-type: none"> ■ 服務組態 ■ 允許通知 	允許產生和使用有關服務狀態的通知。	VirtualMachine.Namespace.Event
<ul style="list-style-type: none"> ■ 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。	VirtualMachine.Namespace.EventNotify
<ul style="list-style-type: none"> ■ 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。	VirtualMachine.Namespace.Management
<ul style="list-style-type: none"> ■ 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。	VirtualMachine.Namespace.ModifyContent
<ul style="list-style-type: none"> ■ 服務組態 ■ 查詢服務組態 	允許擷取虛擬機器服務清單。	VirtualMachine.Namespace.Query
<ul style="list-style-type: none"> ■ 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。	VirtualMachine.Namespace.ReadContent

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 16-65. 虛擬機器快照管理權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
<ul style="list-style-type: none"> ■ 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	VirtualMachine.State.CreateSnapshot
<ul style="list-style-type: none"> ■ 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	VirtualMachine.State.RemoveSnapshot
<ul style="list-style-type: none"> ■ 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	VirtualMachine.State.RenameSnapshot
<ul style="list-style-type: none"> ■ 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	VirtualMachine.State.RevertToSnapshot

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 16-66. 虛擬機器 vSphere Replication 權限

權限名稱	說明	要求	API 中的權限名稱
■ vSphere Replication ■ 設定複寫	允許對虛擬機器進行複寫設定。	虛擬機器	VirtualMachine.Hbr.ConfigureReplication
■ 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	VirtualMachine.Hbr.ReplicaManagement
■ vSphere Replication ■ 監控複寫	允許監控複寫。	虛擬機器	VirtualMachine.Hbr.MonitorReplication

虛擬機器類別權限

虛擬機器類別權限控制哪些使用者可以在 Kubernetes 命名空間上新增和移除虛擬機器類別。

表 16-67. 虛擬機器類別權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
管理虛擬機器類別	允許管理主管叢集中 Kubernetes 命名空間上的虛擬機器類別。	叢集	VirtualMachineClasses.Manage

vSAN 權限

vSAN 權限控制哪些使用者可以執行淺層重設金鑰作業。

表 16-68. vSAN 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
■ 叢集 ■ ShallowRekey	允許對叢集執行淺層重設金鑰。	叢集	Vsan.Cluster.ShallowRekey

vSphere 區域權限

vSphere 區域權限控制哪些使用者可以在 vSphere with Tanzu 上建立和管理 vSphere 區域。

表 16-69. vSphere 區域權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
連結和中斷連結 vSphere 區域的 vSphere 物件	允許將物件與 vSphere 區域相關聯。	叢集	Zone.ObjectAttachable
建立、更新和刪除 vSphere 區域及其關聯	允許建立和刪除 vSphere 區域。	叢集	Zone.Manage

vService 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 16-70. vService 權限

vSphere Client 中的權限名稱	說明	要求	API 中的權限名稱
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.CreateDependency
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.DestroyDependency
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.ReconfigureDependency
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	vService.UpdateDependency

vSphere 標記權限

vSphere 標記權限控制在 vCenter Server 詳細目錄物件上建立、刪除標籤與標籤類別，以及指派和移除標籤的能力。

您可以在階層中的不同層級設定此權限。例如，如果您在資料夾層級設定了某項權限，則可以將此權限散佈到該資料夾中的一或多個物件。[要求] 資料行中列出的物件必須具有權限集，可以直接具有，也可以透過繼承獲得。

表 16-71. vSphere 標記權限

vSphere Client 中的			
權限名稱	說明	要求	API 中的權限名稱
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	InventoryService.Tagging.AttachTag
在物件上指派或取消指派 vSphere 標籤	允許為物件指派或取消指派標籤。使用此權限可限制物件使用者可以指派或取消指派標籤的物件。	任何物件	InventoryService.Tagging.ObjectAttachable
建立 vSphere 標籤	允許建立標籤。	任何物件	InventoryService.Tagging.CreateTag
建立 vSphere 標籤類別	允許建立標籤類別。	任何物件	InventoryService.Tagging.CreateCategory
刪除 vSphere 標籤	允許刪除標籤。	任何物件	InventoryService.Tagging.DeleteTag
刪除 vSphere 標籤類別	允許刪除標籤類別。	任何物件	InventoryService.Tagging.DeleteCategory
編輯 vSphere 標籤	允許編輯標籤。	任何物件	InventoryService.Tagging.EditTag
編輯 vSphere 標籤類別	允許編輯標籤類別。	任何物件	InventoryService.Tagging.EditCategory
修改類別的 UsedBy 欄位	允許變更標籤類別的 UsedBy 欄位。	任何物件	InventoryService.Tagging.ModifyUsedByForCategory
修改標籤的 UsedBy 欄位	允許變更標籤的 UsedBy 欄位。	任何物件	InventoryService.Tagging.ModifyUsedByForTag

vSphere Client 權限

vSphere Client 權限可控制對 vCenter Server 的離線存取。

這些權限僅適用於 VMware Cloud。

瞭解 vSphere 強化與符合性

17

組織希望透過降低資料竊取、網路攻擊或未經授權存取的風險來保護其資料安全。組織通常還必須遵守從政府標準到私人標準的一或多項規定，例如國家標準與技術研究院 (NIST) 和防禦資訊系統代理機構安全性技術實作指南 (DISA STIG)。確保您的 vSphere 環境符合此類標準需要瞭解更廣泛的考量事項，包括人員、流程和技術。

對需要注意的安全性和合規性主題的高層級概觀可協助您規劃合規性策略。您也可以從 VMware 網站的其他合規性相關資源中受益。

本章節討論下列主題：

- [vSphere 環境中的安全性與符合性](#)
- [瞭解 vSphere 安全性組態指南](#)
- [關於國家標準與技術研究院](#)
- [關於 DISA STIG](#)
- [關於 VMware 安全性開發生命週期](#)
- [vSphere 中的稽核記錄](#)
- [瞭解安全性與合規性後續步驟](#)
- [vCenter Server 和 FIPS](#)

vSphere 環境中的安全性與符合性

「安全性」和「合規性」詞彙通常互換使用。但是，它們是唯一且不同的概念。

「安全性」(通常視為資訊安全性) 通常被定義為可供實作的一組技術、實體和管理控制，以提供機密性、完整性和可用性。例如，您可以透過鎖定哪些帳戶可以登入主機以及透過何種方式登入 (SSH、Direct Console 等) 來保護主機。相較之下，「合規性」是為了滿足不同法規架構所建立的最低控制所必需的一系列要求，這些監管架構對任何特定類型的技術、廠商或組態提供有限的指導。例如，支付卡產業 (PCI) 已建立安全性準則來協助組織主動保護客戶的帳戶資料。

「安全性」降低了資料竊取、網路攻擊或未經授權存取的風險，而「合規性」則證明了安全性控制已到位 (通常在定義的時間表內)。「安全性」主要在設計決策中概略列出，並在技術組態中反白顯示。「合規性」側重於對應安全性控制與特定需求之間的關聯性。合規性對應提供了一個集中式視圖，可列出許多必需的安全性控制。透過包括根據 NIST、PCI、FedRAMP、HIPAA 等網域所述的每個相應安全性控制的合規性引用來進一步詳細說明這些控制。

有效的網路安全和合規性計畫建立在三個核心上：人員、流程和技術。一般的誤解是，僅靠技術可以解決您的所有網路安全需求。技術確實在資訊安全性計畫的開發和執行中發揮著重要的作用。但是，沒有流程和程序、感知和訓練的技術會在您的組織內建立漏洞。

定義安全性與合規性策略時，請謹記下列事項：

- 人們需要一般的感知和訓練，而 IT 人員則需要特定的訓練。
- 程序定義了如何使用組織內的活動、角色和說明文件來降低風險。只有當人們正確地遵循流程時，流程才會有效。
- 技術可用於防止或減少網路安全風險對您組織的影響。使用哪種技術取決於組織內的風險接受程度。

VMware 提供的合規性套件中包含《稽核指南》和《產品適用性指南》，有助於縮小合規性和法規需求與實作指南之間的差距。如需詳細資訊，請參閱 <https://core.vmware.com/compliance>。

合規性詞彙表

「合規性」說明了對於理解非常重要的特定詞彙和定義。

表 17-1. 合規性詞彙

詞彙	定義
CJIS	刑事司法資訊服務。在合規性方面，CJIS 制定了一項安全性原則，其規定了地方、州和聯邦刑事司法和執法機構如何採取安全預防措施來保護敏感資訊，例如指紋和犯罪背景。
DISA STIG	防禦資訊系統代理機構安全性技術實作指南。防禦資訊系統代理機構 (DISA) 是負責維護國防部 (DoD) IT 基礎結構的安全性狀態的實體。DISA 透過開發和使用安全性技術實作指南 (「STIG」) 來完成此工作。
FedRAMP	聯邦風險和授權管理計畫。FedRAMP 是一項政府範圍的計畫，可以為雲端產品和服務的安全性評估、授權和持續監控提供標準化方法。
HIPAA	健康保險流通與責任法案。HIPAA 於 1996 年通過國會表決，其功能如下： <ul style="list-style-type: none"> ■ 可讓數百萬美國工作者及其家屬在更換工作或丟失工作時能夠轉移和繼續享有醫療保險。 ■ 減少醫療保健欺詐和濫用 ■ 規定業界範圍內有關電子帳單及其他流程的醫療保健資訊標準 ■ 需要保護和保密處理受保護的健康資訊 後一個項目對《vSphere 安全性》說明文件最為重要。
NCCoE	國家網路安全卓越中心。NCCoE 是一家美國政府組織，負責針對美國企業遇到的網路安全問題制定和公開分享解決方案。該中心由來自網路安全技術公司、其他聯邦機構和學術界的人組成，以解決每個問題。
NIST	國家標準與技術研究院。NIST 成立於 1901 年，是美國商務部內部的一個非監管聯邦機構。NIST 的使命是透過以提高經濟安全性和改善生活質量方式推進測量科學、標準和技術來倡導美國的創新和產業競爭力。

表 17-1. 合規性詞彙 (續)

詞彙	定義
PAG	產品適用性指南。為正在考慮公司解決方案以協助他們滿足合規性需求的組織提供常規指導的一份文件。
PCI DSS	支付卡產業資料安全標準。一組安全標準，旨在確保所有接受、處理、儲存或傳輸信用卡資訊的所有公司都能維持安全的環境。
VVD/VCF 合規性解決方案	VMware Validated Design/VMware Cloud Foundation。VMware Validated Design 提供全面且經過廣泛測試的藍圖，以建置和運作軟體定義資料中心。VVD/VCF 合規性解決方案使客戶能夠滿足多個政府和行業法規的合規性需求。

瞭解 vSphere 安全性組態指南

VMware 建立安全性強化指南，以提供有關以安全方式部署和操作 VMware 產品的規範性指導。對於 vSphere，本指南稱為《vSphere 安全性組態指南》(以前稱為強化指南)。

《vSphere 安全性組態指南》(網址為 <https://core.vmware.com/security-configuration-guide>) 包含適用於 vSphere 的安全性最佳做法。《vSphere 安全性組態指南》未直接與法規準則或架構相對應，因此不是合規性指南。此外，《vSphere 安全性組態指南》不能作為安全性檢查清單使用。安全性始終是一種權衡。當您執行安全性控制時，可能會對可用性、運作或其他營運工作造成負面影響。無論建議來自 VMware 還是其他產業來源，在進行安全性變更之前，都需要仔細考量您的工作負載、使用模式、組織結構等。如果您的組織需遵守法規合規性需求，請參閱 [vSphere 環境中的安全性與符合性](https://core.vmware.com/compliance) 或造訪 <https://core.vmware.com/compliance>。此網站提供合規性套件和產品稽核指南，可協助 vSphere 管理員和法規稽核員針對法規架構保護及證明虛擬基礎結構，例如 NIST 800-53v4、NIST 800-171、PCI DSS、HIPAA、CJIS、ISO 27001 等。

《vSphere 安全性組態指南》不會討論保護下列項目：

- 在虛擬機器內執行的軟體，例如客體作業系統和應用程式
- 透過虛擬機器網路執行的流量
- 附加元件產品的安全性

《vSphere 安全性組態指南》並非意味著要用作「合規性」工具。《vSphere 安全性組態指南》確實使您能夠對合規性採取初始步驟，但是單獨使用時，並不能確保您的部署符合標準。如需有關符合性的詳細資訊，請參閱 [vSphere 環境中的安全性與符合性](https://core.vmware.com/compliance)。

閱讀 vSphere 安全性組態指南

《vSphere 安全性組態指南》是包含安全性相關準則的試算表，可協助您修改 vSphere 安全性組態。這些準則根據受影響的元件分組到索引標籤中。

不要盲目地將《vSphere 安全組態指南》中的準則套用至您的環境，而是花時間評估每個設定，並就是否將其套用做出明智的決定。您至少可以使用 [評估] 資料行中的指示來驗證部署的安全性。

《vSphere 安全組態指南》有助於開始在部署中實作合規性。與防禦資訊系統代理機構 (DISA) 和其他合規性準則搭配使用時，《vSphere 安全組態指南》可讓您將 vSphere 安全性控制對應到每個準則的合規性類型模板。

關於國家標準與技術研究院

國家標準與技術研究院 (NIST) 是一個非監管政府機構，用於開發技術、度量、標準和準則。符合 NIST 標準和準則已成為當今許多產業的首要任務。

國家標準與技術研究院 (NIST) 成立於 1901 年，現在是美國商務部的一部分。NIST 是美國最古老的物理科學實驗室之一。現在，從最小的技術到最大和最複雜的人造產品、從納米級裝置到抗震摩天大樓和全域通訊網路，都支援 NIST 測量。

聯邦資訊安全管理法案 (FISMA) 是 2002 年通過的美國聯邦法律，要求聯邦機構開發、記錄和實作資訊安全性和保護計畫。NIST 透過產生重要的安全性標準和準則 (例如，FIPS 199、FIPS 200 和 SP 800 系列)，在 FISMA 實作中發揮著重要作用。

政府和私人組織使用 NIST 800-53 來保護資訊系統安全。網路安全和隱私權控制對於保護組織營運 (包括任務、職能、形象和信譽)、組織資產和個人免受各種威脅的影響至關重要。其中一些威脅包括惡意網路攻擊、自然災害、結構故障，以及人為錯誤。VMware 已邀請第三方稽核合作夥伴根據 NIST 800-53 控制目錄評估 VMware 產品和解決方案。如需詳細資訊，請造訪 NIST 網頁，網址為：<https://www.nist.gov/cyberframework>。

關於 DISA STIG

國防資訊系統局 (DISA) 開發並發佈了安全性技術實作指南 (STIG)。DISA STIG 提供了強化系統和降低威脅的技術指引。

防禦資訊系統代理機構 (DISA) 是負責維護 DOD 資訊網路 (DODIN) 的安全性狀態的美國國防部 (DoD) 戰鬥支援代理機構。DISA 完成此工作的方式之一是開發、散佈和強制執行安全性技術實作指南或 STIG。簡而言之，STIG 是以標準為基礎的可攜式系統強化指南。STIG 是美國國防部 IT 系統必須實作的指南，可為非國防部實體提供經過審核的安全基準以衡量其安全性態勢。

VMware 等廠商根據 DISA 通訊協定和意見反應向 DISA 提交建議的安全性強化指引以進行評估。此程序完成後，將在 DISA 組織網站上發佈官方 STIG，網址為 <https://public.cyber.mil/stigs/>。VMware 在《vSphere 安全性組態指南》中提供了針對 vSphere 的安全性基準和強化指引。請參閱 <https://core.vmware.com/security>。

關於 VMware 安全性開發生命週期

VMware 安全性開發生命週期 (SDL) 程式在 VMware 軟體產品的開發階段識別並降低了安全性風險。VMware 還會運作 VMware 安全性回應中心 (VMware Security Response Center, VSRC)，來分析和修復 VMware 產品中的軟體安全性問題。

SDL 是 VMware 安全性工程、通訊和回應 (vSECR) 群組以及 VMware 產品開發群組用來識別並緩解安全性問題的軟體開發方法。如需有關 VMware 安全性開發生命週期的詳細資訊，請參閱網頁，網址為：<https://www.vmware.com/security/sdl.html>。

VSRC 與客戶和安全性研究社群合作，以實現解決安全性問題並且及時為客戶提供可操作安全資訊的目標。如需有關 VMware 安全性回應中心 (VMware Security Response Center) 的詳細資訊，請參閱網頁，網址為：<https://www.vmware.com/security/vsrc.html>。

vSphere 中的稽核記錄

網路流量、符合性警示、防火牆活動、作業系統變更和佈建活動的稽核記錄，被視為維護任何 IT 環境安全性的最佳做法。此外，記錄是許多規範和標準的特定需求。

確保您瞭解基礎結構變更的第一個步驟是稽核您的環境。依預設，vSphere 包括可讓您檢視並追蹤變更的工具。例如，您可以對 vSphere 階層中的任何物件使用 vSphere Client 中的工作和事件索引標籤來查看發生的變更。也可以使用 PowerCLI 擷取事件和工作。此外，vRealize Log Insight 提供記錄稽核功能以支援收集和保留重要系統事件。最後，還有許多提供 vCenter Server 稽核的第三方工具可供使用。

記錄檔可以提供稽核線索來協助判斷哪些使用者或物件正在存取主機、虛擬機器等。如需詳細資訊，請參閱 [ESXi 記錄檔位置](#)。

Single Sign-On 稽核事件

Single Sign-On (SSO) 稽核事件是用於存取 SSO 服務的使用者或系統動作的記錄。

vCenter Server 6.7 Update 2 及更新版本透過為以下操作新增事件來改善 VMware vCenter Single Sign-On 稽核：

- 使用者管理
- 登入
- 群組建立
- 身分識別來源
- 原則更新

支援的身分識別來源包括 vsphere.local、整合式 Windows 驗證 (IWA) 和 Active Directory over LDAP。

當使用者透過 Single Sign-On 登入 vCenter Server，或做出影響 SSO 的變更時，下列稽核事件會寫入到 SSO 稽核記錄檔：

- **登入和登出嘗試**：所有成功和失敗的登入及登出作業的事件。
- **變更權限**：變更使用者角色或權限的事件。
- **帳戶變更**：變更使用者帳戶資訊的事件，例如，使用者名稱、密碼或任何其他帳戶資訊。
- **安全性變更**：變更安全性組態、參數或原則的事件。
- **帳戶已啟用或停用**：啟用或停用帳戶時的事件。
- **身分識別來源**：新增、刪除或編輯身分識別來源的事件。

在 vSphere Client 中，事件資料顯示在**監控**索引標籤中。請參閱 vSphere 監控和效能說明文件。

SSO 稽核事件資料包含下列詳細資料：

- 事件發生時的時間戳記。
- 執行動作的使用者。
- 事件的說明。
- 事件的嚴重性。
- 用於連線到 vCenter Server 的用戶端的 IP 位址 (如果可用)。

SSO 稽核事件記錄概觀

vSphere Single-Sign On 程序會將稽核事件寫入 `/var/log/audit/sso-events/` 目錄中的 `audit_events.log` 檔案。

注意 絕不手動編輯 `audit_events.log` 檔案，因為這麼做可能會導致稽核記錄失敗。

使用 `audit_events.log` 檔案時，請謹記下列事項：

- 一旦達到 50 MB，便會封存記錄檔。
- 最多保留 10 個封存檔。如果達到該限制，會在建立新封存檔時清除最舊的檔案。
- 封存檔命名為 `audit_events- <index>.log.gz`，其中 `index` 是從 1 到 10 的數字。建立的第一個封存檔是索引 1，且隨著每個後續封存檔而增加。
- 最舊的事件在封存檔索引 1 中。最高的索引檔案為最新的封存檔。

瞭解安全性與合規性後續步驟

執行安全性評估是瞭解基礎結構中是否有任何漏洞的第一步。安全性評估屬於安全性稽核，可審查系統和實務，包括安全合規性。

安全性評估通常是指掃描組織的實體基礎結構 (防火牆、網路、硬體等) 以識別漏洞和問題。安全性評估與安全性稽核不同。安全性稽核不僅包括對實體基礎結構的審查，還包括其他領域，例如原則和標準作業系統程序，包括安全合規性。稽核之後，您可以決定解決系統中的問題的步驟。

準備執行安全性稽核時，您可能會考慮下列常規問題：

- 1 我們的組織是否有義務遵守合規性規定？如果是，應遵守哪個規定？
- 2 我們的稽核間隔是多久？
- 3 我們的內部自我評估間隔是多久？
- 4 我們是否可以存取先前的稽核結果？曾經是否檢視過這些結果？
- 5 是否使用第三方稽核公司來協助我們準備稽核？如果是，他們對虛擬化的滿意程度如何？
- 6 我們是否針對系統和應用程式執行漏洞掃描？時機和頻率？
- 7 我們的內部網路安全原則是什麼？
- 8 您的稽核記錄是否根據您的需求進行設定？請參閱 [vSphere 中的稽核記錄](#)。

如果沒有針對何處開始的具體指導或方向，您可以透過以下方式快速啟動保護 vSphere 環境的安全：

- 使用最新的軟體和韌體修補程式讓您的環境保持最新
- 為所有帳戶維護良好的密碼管理和安全機制
- 檢閱廠商核准的安全性建議
- 參考《VMware 安全性組態指南》(請參閱[瞭解 vSphere 安全性組態指南](#))
- 使用來自 NIST、ISO 等原則架構的立即可用且經過驗證的指導
- 遵循 PCI、DISA 和 FedRAMP 等符合法規的架構的指導

vCenter Server 和 FIPS

在 vSphere 7.0 Update 2 及更新版本中，可以在 vCenter Server Appliance 上啟用 FIPS 驗證的密碼編譯。

FIPS 140-2 是美國和加拿大政府標準，用於指定密碼編譯模組的安全性需求。vSphere 使用 FIPS 驗證的密碼編譯模組，與 FIPS 140-2 標準指定的模組相符。vSphere FIPS 支援的目的是簡化各種規範環境下的合規性和安全性活動。

在 vSphere 6.7 及更新版本中，ESXi 和 vCenter Server 使用 FIPS 驗證的密碼編譯來保護管理介面和 VMware Certificate Authority (VMCA)。

vSphere 7.0 Update 2 及更新版本為 vCenter Server Appliance 提供了額外的 FIPS 驗證的密碼編譯。

備註 vSphere 的相容性優於 FIPS，因此某些元件需要注意一些考量事項。請參閱[使用 FIPS 時的考量事項](#)。

FIPS 模組

密碼編譯模組是一組執行安全性功能的硬體、軟體或韌體。ESXi 使用多個經過 FIPS 140-2 驗證的密碼編譯模組。

下表顯示了 ESXi 使用的經 FIPS 140-2 驗證的密碼編譯模組集。

表 17-2. FIPS 模組

密碼編譯模組	安全性原則版本	演算法 (CAVP)	密碼編譯模組驗證計劃
Vmkernel 密碼編譯模組	1.0	AES、SHS、DRBG、HMAC (C 1172)	憑證 #3073
Vmkernel 密碼編譯模組載入器	不適用	HMAC、SHS (C 1171)	憑證 #3073
Vmkernel DRBG 密碼編譯模組	不適用	AES、DRBG (C 499)	NA
VMware OpenSSL FIPS 物件模組	2.0.20-vmw	DRBG、AES、SHS、HMAC、DSA、RSA、ECDSA、KAS-FFC、KAS-ECC (C 470)	憑證 #3550 和 #3857

在 vCenter Server Appliance 上啟用和停用 FIPS

可以使用 HTTP 要求在 vCenter Server Appliance 上啟用或停用 FIPS 驗證的密碼編譯。依預設，FIPS 驗證的加密處於停用狀態。

您可以使用多種方式執行 HTTP 要求。此工作顯示如何使用 vSphere Client 中的開發人員中心在 vCenter Server Appliance 上啟用和停用 FIPS 驗證的加密。如需有關使用 API 以與 vCenter Server Appliance 搭配使用的詳細資訊，請參閱《VMware vCenter Server 管理程式設計指南》。

程序

- 1 使用 vSphere Client 登入 vCenter Server 系統。
- 2 從功能表中，選取**開發人員中心**。
- 3 按一下 **API Explorer**。
- 4 從**選取 API** 下拉式功能表中，選取**應用裝置**。
- 5 向下捲動查看類別，然後展開 **system/security/global_fips**。
- 6 展開 **GET**，然後按一下**試用下的執行**。

您可以在**回應**下檢視目前設定。

- 7 變更設定。

- a 若要啟用 FIPS，請展開 **PUT**，在 `request_body` 中輸入下列內容，然後按一下**執行**。

```
{
  "enabled":true
}
```

- b 若要停用 FIPS，請展開 **PUT**，在 `request_body` 中輸入下列內容，然後按一下**執行**。

```
{
  "enabled":false
}
```

結果

啟用或停用 FIPS 驗證的加密後，vCenter Server Appliance 會重新開機。

使用 FIPS 時的考量事項

在 vCenter Server Appliance 上啟用 FIPS 時，某些元件目前存在功能限制。

在 vCenter Server 上啟用 FIPS 後，應該看不到任何差異，但需要考慮一些注意事項。

表 17-3. FIPS 考量事項

產品或元件	考量事項	因應措施
vSphere Single Sign-On	啟用 FIPS 時，vCenter Server 僅支援密碼編譯模組進行同盟驗證。因此，RSA SecureID 和某些 CAC 卡不再起作用。	使用同盟驗證。如需詳細資料，請參閱《vSphere 驗證》說明文件。
非 VMware 和合作夥伴 vSphere Client UI 外掛程式	在啟用了 FIPS 的情況下，這些外掛程式可能無法運作。	升級外掛程式以使用一致的加密程式庫。請參閱「準備本機外掛程式以符合 FIPS」，網址為 https://code.vmware.com/docs/13385/preparing-local-plug-ins-for-fips-compliance 。