vSphere 驗證

Update 1

VMware vSphere 7.0
VMware ESXi 7.0
vCenter Server 7.0

vmware®

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

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

目錄

關於 vSphere 驗證

vSphere 驗證說明文件提供的資訊，可協助您執行憑證管理和 vCenter Single Sign-On 組態等一般工作。

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，我們更新了本指南，以移除非包含性語言的執行個體。

vSphere 驗證說明如何管理 vCenter Server 和相關服務的憑證，以及如何使用 vCenter Single Sign-On 來設定驗證。

表 1-1. vSphere 驗證要點

主題	內容要點
使用驗證	■ 管理驗證服務。 ■ 使用 vCenter Server 管理介面管理 vCenter Server。
vSphere 安全性憑證	■ 憑證模型以及取代憑證的選項。 ■ 從 UI 取代憑證 (簡單情況)。 ■ 使用 Certificate Manager 公用程式取代憑證。 ■ 使用 CLI 取代憑證 (複雜情況)。 ■ 憑證管理 CLI 參考。
使用 vCenter Single Sign-On 進行 vSphere 驗證	■ 驗證程序的架構。 ■ 如何新增身分識別來源，以便網域中的使用者可進行驗證。 ■ 雙重要素驗證。 ■ 管理使用者、群組和原則。

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。

相關說明文件

隨附文件 vSphere 安全性說明可用的安全性功能，以及可採取的措施以保護該環境免受攻擊。該文件還說明了如何設定權限，並包含了權限參考。

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：http://www.vmware.com/security/hardening-guides.html。《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。

預定對象

此資訊適用於想要設定 vCenter Server 驗證並管理憑證的管理員。該資訊是針對熟悉虛擬機器技術和資料中心作業且富有經驗的 Linux 系統管理員而撰寫。

憑證管理和驗證入門

1

vCenter Server 為 vSphere 環境提供一般基礎結構服務，包括憑證管理和使用 vCenter Single Sign-On 進行驗證。

本章節討論下列主題：

vSphere 憑證管理和驗證概觀

vSphere 提供可讓您對 vCenter Server 和 ESXi 元件執行憑證管理工作，以及透過 vCenter Single Sign-On 設定驗證的服務。

vSphere 憑證管理概觀

依預設，vSphere 可讓您使用 VMware Certificate Authority (VMCA) 憑證佈建 vCenter Server 元件和 ESXi 主機。也可以使用儲存在 VMware Endpoint 憑證存放區 (VECS) 中的自訂憑證。

vCenter Single Sign-On 概觀

vCenter Single Sign-On 可讓 vSphere 元件透過安全的 Token 機制相互通訊。vCenter Single Sign-On 使用對於理解非常重要的特定詞彙和定義。

表 1-1. vCenter Single Sign-On 詞彙

詞彙	定義
主體	可驗證的實體，例如使用者。
身分識別提供者	管理身分識別來源和驗證主體的服務。範例：Microsoft Active Directory Federation Services (AD FS) 和 vCenter Single Sign-On。
身分識別來源 (目錄服務)	儲存和管理主體。主體由有關使用者或服務帳戶 (例如名稱、位址、電子郵件和群組成員資格) 的屬性集合組成。範例：Microsoft Active Directory 和 VMware Directory Service (vmdir)。

表 1-1. vCenter Single Sign-On 詞彙 (續)

詞彙	定義
驗證	判斷某人或某事物實際上是否符合其自身聲明的方式。例如，使用者在提供其認證 (例如智慧卡、使用者名稱和正確密碼等) 時進行驗證。
授權	驗證主體有權存取哪些物件的程序。
Token	已簽署的資料集合，組成了指定主體的身分識別資訊。Token 可能不僅包括有關主體的基本資訊 (例如，電子郵件地址和全名)，也可能包括主體的群組和角色，這取決於 Token 類型。
vmdir	VMware Directory Service。vCenter Server 中的內部 (本機) LDAP 存放庫，包含使用者身分識別、群組和組態資料。
OpenID Connect (OIDC)	以 OAuth2 為基礎的驗證通訊協定。vCenter Server 與 Active Directory Federation Services (AD FS) 互動時會使用 OIDC 功能。

vCenter Single Sign-On 驗證類型

vCenter Single Sign-On 使用不同類型的驗證，具體取決於是包含內建 vCenter Server 身分識別提供者還是外部身分識別提供者。

表 1-2. vCenter Single Sign-On 驗證類型

驗證類型	什麼充當身分識別提供者?	vCenter Server 會處理密碼嗎?	說明
基於 Token 的驗證	外部身分識別提供者。例如，AD FS。	否	vCenter Server 透過特定通訊協定連絡外部身分識別提供者，並取得表示特定使用者身分身分識別的 Token。
簡單驗證	vCenter Server	是	使用者名稱和密碼會直接傳遞至 vCenter Server，以透過其身分識別來源驗證認證。

管理憑證

您可以透過 vSphere Client 或使用 API、指令碼或 CLI 來管理憑證。

您可以使用不同的介面來管理憑證。

表 1-3. 用於管理憑證的介面

介面	說明
vSphere Client	Web 介面 (以 HTML5 為基礎的用戶端)。請參閱使用 vSphere Client 管理憑證。
vSphere Automation API	請參閱《VMware vSphere Automation SDK 程式設計指南》。

表 1-3. 用於管理憑證的介面 (續)

介面	說明
憑證管理公用程式	支援產生憑證簽署要求 (CSR) 和取代憑證的命令列工具。請參閱透過 vSphere Certificate Manager 公用程式管理憑證。
用於管理憑證和目錄服務的 CLI	用於管理憑證、VMware Endpoint 憑證存放區 (VECS) 和 VMware Directory Service (vmdir) 的命令集。請參閱第 3 章 使用 CLI 命令管理服務和憑證。

從 vSphere Client 管理憑證

您可以從 vSphere Client 管理憑證。

程序

1 以具有本機 vCenter Single Sign-On 網域中管理員權限的使用者身分登入 vCenter Server。

預設網域為 vsphere.local。

2 選取**管理**。

3 在**憑證**下，按一下**憑證管理**。

機器 SSL 憑證和信任的根憑證面板隨即顯示。

4 執行憑證工作，例如檢視憑證詳細資料、更新機器 SSL 憑證、新增受信任的根憑證等。

使用指令碼管理憑證

vCenter Server 包括用於產生憑證簽署要求 (CSR)、管理憑證及管理服務的指令碼。

例如，您可以使用 `certool` 公用程式來產生 CSR 並取代憑證。請參閱透過 vSphere Certificate Manager 公用程式管理憑證。

使用 CLI 管理 vSphere Client 不支援的工作，或建立適用於您環境的自訂指令碼。

表 1-4. 用於管理憑證和相關聯服務的 CLI

CLI	說明	連結
`certool`	產生與管理憑證及金鑰。VMware Certificate Authority (VMCA) 的一部分。	certool 初始化命令參考
`vecs-cli`	管理 VMware 憑證存放區執行個體的內容。屬於 VMware Authentication Framework 精靈 (VMAFD) 的一部分。	vecs-cli 命令參考
`dir-cli`	建立與更新 VMware Directory Service 中的憑證。屬於 VMAFD 的一部分。	dir-cli 命令參考
`sso-config`	更新 Security Token Service (STS) 憑證。	取代 STS 憑證
`service-control`	用於啟動、停止及列出服務的命令。	在執行其他 CLI 命令之前，請執行此命令來停止服務。

必要條件

啟用以透過 SSH 登入 vCenter Server。請參閱使用管理介面管理 vCenter Server。

程序

1 登入 vCenter Server shell。

在通常情況下，您必須是根使用者或管理員使用者。如需詳細資料，請參閱執行 CLI 所需的權限。

2 在以下其中一個預設位置存取 CLI。

所需的權限將視要執行的工作而定。有時，系統會提示您輸入兩次密碼，以保護敏感資訊。

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin
/opt/vmware/bin/sso-config.sh
```

`service-control` 命令不要求您輸入路徑。

管理驗證服務

您可以從 vSphere Client 或使用 CLI 來管理驗證服務。您也可以使用 API 來管理 vCenter Server 身分識別提供者聯盟組態程序。

可以使用不同的介面管理驗證。

表 1-5. 用於管理驗證服務的介面

介面	說明
vSphere Client	Web 介面 (以 HTML5 為基礎的用戶端)。
API	管理 vCenter Server 身分識別提供者聯盟設定程序。
`sso-config`	用於設定 vCenter Server 內建身分識別提供者的命令列公用程式。

從 vSphere Client 管理驗證服務

您可以從 vSphere Client 管理 vCenter Server 驗證服務。

程序

1 以具有本機 vCenter Single Sign-On 網域中管理員權限的使用者身分登入 vCenter Server。

預設網域為 vsphere.local。

2 選取**管理**。

3 在 **Single Sign On** 下，按一下**組態**以管理身分識別提供者，並設定密碼和鎖定原則。

使用指令碼管理驗證服務

vCenter Server 包含用於管理驗證服務的公用程式 `sso-config`。

使用 `sso-config` 公用程式執行 vSphere Client 不支援的管理工作，或建立適用於您環境的自訂指令碼。

表 1-6. 用於管理驗證和相關聯服務的 CLI

CLI	說明	連結
`sso-config`	用於設定 vCenter Server 內建身分識別提供者的命令列公用程式。	若要參閱 `sso-config` 說明，請執行 `sso-config.sh -help`，或參閱 VMware 知識庫文章 (網址為 https://kb.vmware.com/s/article/67304) 以瞭解使用範例。
`service-control`	用於啟動、停止及列出服務的命令。	在執行其他 CLI 命令之前，請執行此命令來停止服務。

必要條件

啟用以透過 SSH 登入 vCenter Server。請參閱使用管理介面管理 vCenter Server。

程序

1 登入 vCenter Servershell。

在通常情況下，您必須是根使用者或管理員使用者。如需詳細資料，請參閱執行 CLI 所需的權限。

2 在以下預設位置存取 `sso-config` 公用程式。

所需的權限將視要執行的工作而定。有時，系統會提示您輸入兩次密碼，以保護敏感資訊。

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

`service-control` 命令不需要您指定路徑。

管理 vCenter Server

您可以從 vCenter Server 管理介面或從 vCenter Server shell 管理 vCenter Server。

如需有關管理 vCenter Server 的詳細資訊，請參閱 vCenter Server 組態。

表 1-7. 用於管理 vCenter Server 的介面

介面	說明
vCenter Server 管理介面	使用此介面來重新設定系統設定。請參閱使用管理介面管理 vCenter Server。
vCenter Server shell	使用此命令列介面可在 VMCA、VECS 和 VMDIR 上執行服務管理作業。請參閱透過 vSphere Certificate Manager 公用程式管理憑證和第 3 章 使用 CLI 命令管理服務和憑證。

使用管理介面管理 vCenter Server

您可以使用 vCenter Server 管理介面來設定系統設定。設定包括時間同步化、網路設定及 SSH 登入設定。您還可以變更根密碼、將應用裝置加入 Active Directory 網域，以及離開 Active Directory 網域。

程序

1 在瀏覽器中，前往 Web 介面，網址為 `https://vcenter_server_ip:5480`。

2 如果顯示有關不受信任之 SSL 憑證的警告訊息，請根據公司安全性原則和您所使用的瀏覽器解決問題。

3 以 root 身分登入。

預設 root 密碼是部署 vCenter Server 時設定的 root 密碼。

結果

您會看到 vCenter Server 管理介面的 [摘要] 頁面。

從 vCenter ServerShell 管理 vCenter Server

您可以透過 vCenter Servershell 使用服務管理公用程式和 CLI。您可以使用 TTY1 登入主控台，或使用 SSH 連線至 shell。

程序

1 如有必要，請啟用 SSH 登入。

a 登入 vCenter Server 管理介面，網址為 https://*vcenter_server_ip*:5480。

b 在 [導覽器] 中選取**存取**，然後按一下**編輯**。

c 開啟**啟用 SSH 登入**，然後按一下**確定**。

您可以遵循相同的步驟為 vCenter Server 啟用 Bash shell。

2 存取 shell。

- 如果您可直接存取 vCenter Server 主控台，請選取**登入**，然後按 Enter。
- 若要遠端連線，請使用 SSH 或其他遠端主控台連線來啟動 vCenter Server 的工作階段。

3 以 root 身分登入，密碼是您最初部署 vCenter Server 時所設定的密碼。

如果您已變更根密碼，請使用新密碼。

將 vCenter Server 新增到 Active Directory 網域

如果想要將 Active Directory 身分識別來源新增到 vCenter Server，您必須將 vCenter Server 加入 Active Directory 網域。

如果您無法使用 vCenter Server 身分識別提供者聯盟或 Active Directory over LDAPS，則 vCenter Server 可支援整合式 Windows 驗證 (IWA)。若要使用 IWA，必須將 vCenter Server 加入您的 Active Directory 網域。

程序

1. 透過使用 vSphere Client，以具有本機 vCenter Single Sign-On 網域 (預設為 vsphere.local) 中管理員權限的使用者身分登入 vCenter Server。
2. 選取**管理**。
3. 展開 **Single Sign On**，然後按一下**組態**。
4. 在**身分識別提供者**索引標籤下，按一下 **Active Directory 網域**。
5. 按一下**加入 AD**，輸入網域、選擇性組織單位，以及使用者名稱和密碼，然後按一下**加入**。
6. 重新啟動 vCenter Server。

後續步驟

若要從加入的 Active Directory 網域連結使用者和群組，請新增加入的網域做為 vCenter Single Sign-On 身分識別來源。請參閱新增或編輯 vCenter Single Sign-On 身分識別來源。

vSphere 安全性憑證

2

vSphere 透過使用憑證來加密通訊、驗證服務，以及簽署 Token，以提供安全性。

vSphere 使用憑證：

- 加密兩個節點 (例如 vCenter Server 和 ESXi 主機) 之間的通訊。
- 驗證 vSphere 服務。
- 執行內部動作，例如簽署 Token。

vSphere 的內部憑證授權機構 (VMware Certificate Authority (VMCA)) 會提供 vCenter Server 和 ESXi 所需的所有憑證。VMCA 已安裝在每台 vCenter Server 主機上，可立即保護解決方案，不需要任何其他修改。保留此預設組態將為憑證管理提供最低運作額外負荷。vSphere 提供了可在這些憑證到期時進行更新的機制。

vSphere 還提供了可使用您自己的憑證取代特定憑證的機制。但是，僅取代提供節點間加密的 SSL 憑證，可保持低憑證管理額外負荷。

對於管理憑證，建議使用下列選項：

表 2-1. 用於管理憑證的建議選項

模式	說明	優點
VMCA 預設憑證	VMCA 會為 vCenter Server 和 ESXi 主機提供所有憑證。	最簡單且最低的額外負荷。VMCA 可以管理 vCenter Server 和 ESXi 主機的憑證生命週期。
VMCA 預設憑證與外部 SSL 憑證 (混合模式)	您可以取代 vCenter ServerSSL 憑證，並讓 VMCA 管理解決方案使用者和 ESXi 主機的憑證。或者，對於高安全性意識部署，您也可以取代 ESXi 主機 SSL 憑證。	簡單且安全。VMCA 管理內部憑證，但會使用您公司核准的 SSL 憑證，並且讓這些憑證受您的瀏覽器信任，您可從中受益。

VMware 不建議取代解決方案使用者憑證或 STS 憑證，也不建議使用下層 CA 來取代 VMCA。如果您選擇其中一個選項，可能會遇到非常複雜的問題，且可能對安全性產生負面影響，並且增加不必要的運作風險。如需有關在 vSphere 環境中管理憑證的詳細資訊，請參閱標題為〈新產品逐步解說 - 混合 vSphere SSL 憑證取代〉的部落格文章，網址為：http://vmware.com/go/hybridvmca。

您可以使用下列選項來取代現有憑證。

表 2-2. 不同的憑證取代方法

選項	請參閱
使用 vSphere Client。	使用 vSphere Client 管理憑證
使用 vSphere Automation API 管理憑證生命週期。	VMware vSphere Automation SDK 程式設計指南
從命令列使用 vSphere Certificate Manager 公用程式。	透過 vSphere Certificate Manager 公用程式管理憑證
使用 CLI 命令來手動取代憑證。	第 3 章 使用 CLI 命令管理服務和憑證

本章節討論下列主題：

- 不同解決方案路徑的憑證需求
- 憑證管理概觀
- 使用 vSphere Client 管理憑證
- 透過 vSphere Certificate Manager 公用程式管理憑證
- 手動憑證取代

不同解決方案路徑的憑證需求

視您是否將 VMCA 做為中繼 CA 使用或您使用的為自訂憑證而定，憑證需求會有所不同。機器憑證的需求也有所不同。

登入前，請確保您環境中所有節點的時間均已同步。

所有匯入憑證的需求

- 金鑰大小：2048 位元 (下限) 至 16384 位元 (上限) (PEM 編碼)
- PEM 格式。VMware 支援 PKCS8 和 PKCS1 (RSA 金鑰)。將金鑰新增到 VECS 之後，系統會將其轉換為 PKCS8。
- x509 第 3 版
- SubjectAltName 必須包含 DNS Name=*machine_FQDN*
- CRT 格式
- 包含下列金鑰使用方法：數位簽章、金鑰編密。
- 增強金鑰使用方法可以為空白或包含伺服器驗證。

VMCA 不支援以下憑證。

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

符合 RFC 2253 的憑證

憑證必須符合 RFC 2253。

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

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

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

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

將 VMCA 作為中繼 CA 使用時的需求

當您將 VMCA 作為中繼 CA 使用時，憑證必須符合以下需求。

憑證類型	憑證需求

根憑證	■ 您可以使用 vSphere Certificate Manager 建立 CSR。請參閱使用 vSphere Certificate Manager 產生 CSR 並準備根憑證 (中繼 CA)。
	■ 如果您偏好手動建立 CSR，則傳送要求簽署的憑證必須符合下列需求：
	■ 金鑰大小：2048 位元 (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
	■ 對於根憑證，CA 延伸必須設為 true，憑證簽署必須位於需求清單中。例如：
	`basicConstraints = critical,CA:true`
	`keyUsage = critical,digitalSignature,keyCertSign`
	■ 必須啟用 CRL 簽署。
	■ 增強金鑰使用方法可以為空白或包含伺服器驗證。
	■ 對憑證鏈結的長度無明確限制。VMCA 預設使用 OpenSSL (為 10 個憑證)。
	■ 不支援含萬用字元或多個 DNS 名稱的憑證。
	■ 您無法建立 VMCA 的附屬 CA。
	如需使用 Microsoft 憑證授權機構的範例，請參閱 VMware 知識庫文章：Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x (在 vSphere 6.x 中建立 Microsoft 憑證授權機構範本以建立 SSL 憑證)，網址為 http://kb.vmware.com/kb/2112009。

機器 SSL 憑證	您可以使用 vSphere Certificate Manager 建立 CSR 或手動建立 CSR。 如果您手動建立 CSR，則其必須符合上述所有匯入憑證的需求中所列的需求。您也必須指定主機的 FQDN。
解決方案使用者憑證	您可以使用 vSphere Certificate Manager 建立 CSR 或手動建立 CSR。 **備註** 每位解決方案使用者必須使用不同的名稱。如果您手動產生憑證，則**主體**下可能顯示為 **CN**，視您使用的工具而定。 如果您使用 vSphere Certificate Manager，則工具會提示您輸入每位解決方案使用者的憑證資訊。vSphere Certificate Manager 會將資訊儲存在 `certool.cfg` 中。請參閱 Certificate Manager 提示輸入的資訊。

自訂憑證的需求

當您要使用自訂憑證時，憑證必須符合以下需求。

憑證類型	憑證需求
機器 SSL 憑證	每個節點上的機器 SSL 憑證必須具有與第三方或企業 CA 不同的獨立憑證。 ■ 您可以使用 vSphere Client 或 vSphere Certificate Manager 產生 CSR，也可以手動建立 CSR。CSR 必須符合上述所有匯入憑證的需求中所列的需求。 ■ 對於大部分的欄位，您可以接受預設值，或提供站台專屬值。機器的 FQDN 為必填。
解決方案使用者憑證	各節點上的每個解決方案使用者必須具有與第三方或企業 CA 不同的獨立憑證。 ■ 您可以使用 vSphere Certificate Manager 產生 CSR，也可以自行準備 CSR。CSR 必須符合上述所有匯入憑證的需求中所列的需求。 ■ 如果您使用 vSphere Certificate Manager，則工具會提示您輸入每位解決方案使用者的憑證資訊。vSphere Certificate Manager 會將資訊儲存在 `certool.cfg` 中。請參閱 Certificate Manager 提示輸入的資訊。 **備註** 每位解決方案使用者必須使用不同的名稱。手動產生的憑證在**主體**下可能顯示為 **CN**，視您使用的工具而定。 之後當您使用自訂憑證取代解決方案使用者憑證時，請提供第三方 CA 的完整簽署憑證鏈結。

備註 請勿在任何自訂憑證中使用 CRL 發佈點、授權資訊存取或憑證範本資訊。

憑證管理概觀

設定或更新憑證基礎結構所需的工作取決於您的環境中的需求。您必須考量是要執行全新安裝還是升級，以及是否正考慮使用 ESXi 或 vCenter Server。

未取代 VMware 憑證的管理員

VMCA 可處理所有憑證管理。VMCA 使用以 VMCA 做為根憑證授權機構的憑證佈建 vCenter Server 元件和 ESXi 主機。如果您要從舊版 vSphere 升級為 vSphere 6，所有自我簽署的憑證都會取代為 VMCA 簽署的憑證。

如果您目前沒有取代 VMware 憑證，則您的環境將開始使用 VMCA 簽署憑證而非自我簽署的憑證。

將 VMware 憑證取代為自訂憑證的管理員

如果公司原則需要由第三方或企業 CA 簽署的憑證，或需要自訂憑證資訊，則您有數個全新安裝選擇。

- 使 VMCA 根憑證經第三方 CA 或企業 CA 簽署。將 VMCA 根憑證取代為該簽署的憑證。在此情況下，VMCA 憑證為中繼憑證。VMCA 使用包含完整憑證鏈結的憑證佈建 vCenter Server 元件和 ESXi 主機。
- 如果公司原則不允許鏈結中存在中繼憑證，則可以明確取代這些憑證。您可以使用 vSphere Client、vSphere Certificate Manager 公用程式，或使用憑證管理 CLI 執行手動憑證取代。

升級使用自訂憑證的環境時，您可以保留部分憑證。

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

  升級至 vSphere 6.0 或更新版本後，可以將憑證模式設定為**自訂**。如果憑證模式為 VMCA (預設值)，且使用者從 vSphere Client 執行憑證重新整理，則 VMCA 簽署憑證會取代自訂憑證。

- 若要將簡單 vCenter Server 安裝升級為內嵌式部署，則 vCenter Server 會保留自訂憑證。升級後，您的環境會如往常一般正常運作。將會保留現有的 vCenter Server 和 vCenter Single Sign-On 憑證。這些憑證將用做機器 SSL 憑證。此外，VMCA 會將 VMCA 簽署憑證指派給每個解決方案使用者 (vCenter 服務集合)。解決方案使用者僅使用此憑證來向 vCenter Single Sign-On 進行驗證。公司原則通常不要求取代解決方案使用者憑證。

  您可以針對大多數的憑證管理工作使用命令列公用程式 vSphere Certificate Manager。

vSphere 憑證介面

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

表 2-3. 用於管理 vCenter Server 憑證的介面

介面	使用
vSphere Client	透過圖形化使用者介面執行一般憑證工作。
vSphere Automation API	請參閱《VMware vSphere Automation SDK 程式設計指南》。
Certificate Manager 公用程式	從 vCenter Server 安裝的命令列執行一般憑證取代工作。
憑證管理 CLI	使用 `dir-cli`、`certool` 和 `vecs-cli` 執行所有憑證管理工作。
`sso-config` 公用程式	從 vCenter Server 安裝的命令列執行 STS 憑證管理。

對於 ESXi，您可以從 vSphere Client 執行憑證管理。VMCA 會佈建憑證並將其本機儲存於 ESXi 主機。VMCA 不會在 VMDIR 或 VECS 中儲存 ESXi 主機憑證。請參閱 vSphere 安全性說明文件。

支援的 vCenter 憑證

對於 vCenter Server 以及相關的機器與服務，支援下列憑證：

- 由 VMware Certificate Authority (VMCA) 產生及簽署的憑證。
- 自訂憑證。
  - 從您自己的內部 PKI 產生的企業憑證。
  - 由外部 PKI (例如 Verisign、GoDaddy 等) 產生的第三方 CA 簽署憑證。

使用 OpenSSL 建立的自我簽署憑證，若無根 CA 存在則不支援

憑證取代概觀

根據公司原則以及要設定之系統的需求，您可以執行不同類型的憑證取代。您可以使用 vSphere Certificate Manager 公用程式或以手動方式使用安裝隨附的 CLI，從 vCenter Server 執行憑證取代。

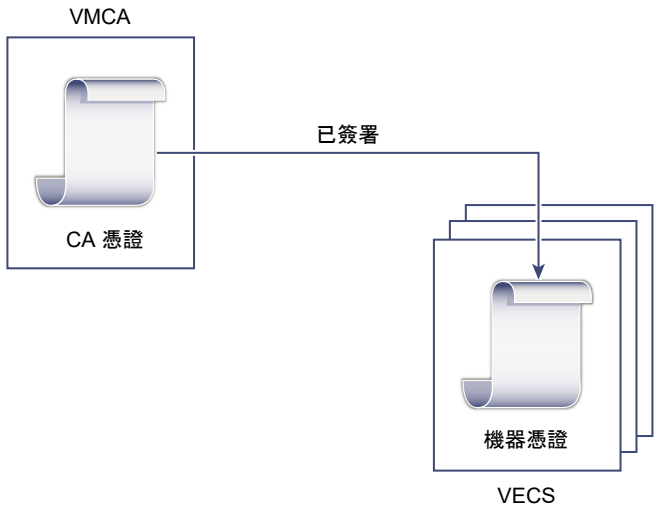
VMCA 包含在每個 vCenter Server 部署中。VMCA 會使用由 VMCA 做為憑證授權機構進行簽署的憑證來佈建每個節點、每個 vCenter Server 解決方案使用者和每個 ESXi 主機。

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

用 VMCA 簽署的憑證取代

如果您的 VMCA 憑證到期或出於其他原因想將其取代，則可使用憑證管理 CLI 執行該程序。依預設，VMCA 根憑證會在 10 年後到期，而 VMCA 簽署的所有憑證都會在根憑證到期時到期 (即最多 10 年期限)。

圖 2-1. VMCA 簽署的憑證儲存在 VECS 中



您可以使用下列 vSphere Certificate Manager 選項：

- 將機器 SSL 憑證取代為 VMCA 憑證
- 將解決方案使用者憑證取代為 VMCA 憑證

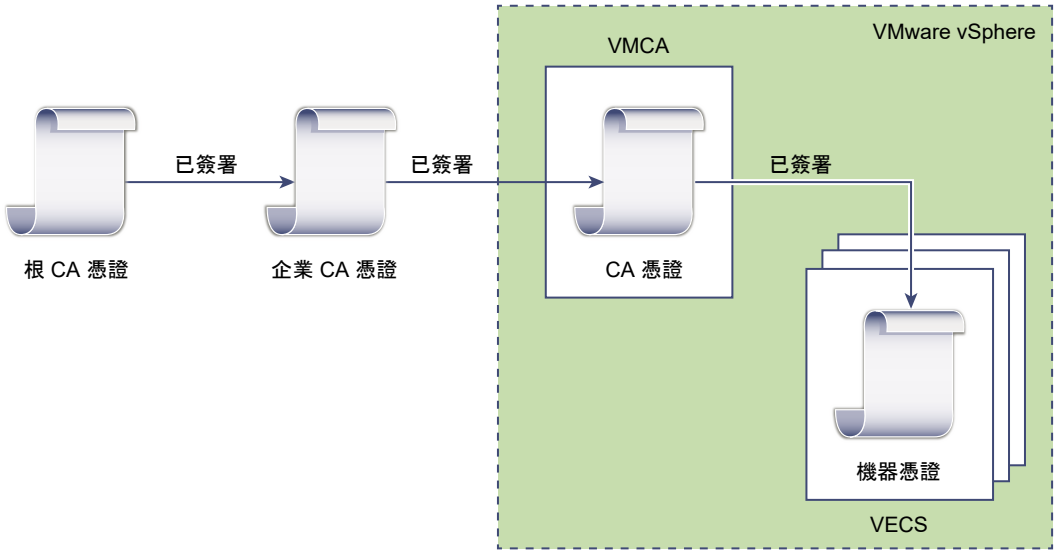
如需手動憑證取代的相關資訊，請參閱用新的 VMCA 簽署憑證取代現有的 VMCA 簽署憑證。

使 VMCA 成為中繼 CA

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

備註 如果執行的全新安裝中包含 vCenter Server，則在新增 ESXi 主機之前取代 VMCA 根憑證。這樣一來，VMCA 將簽署整個鏈結，且不需要產生新憑證。

圖 2-2. 第三方或企業 CA 簽署的憑證使用 VMCA 做為中繼 CA



您可以使用下列 vSphere Certificate Manager 選項：

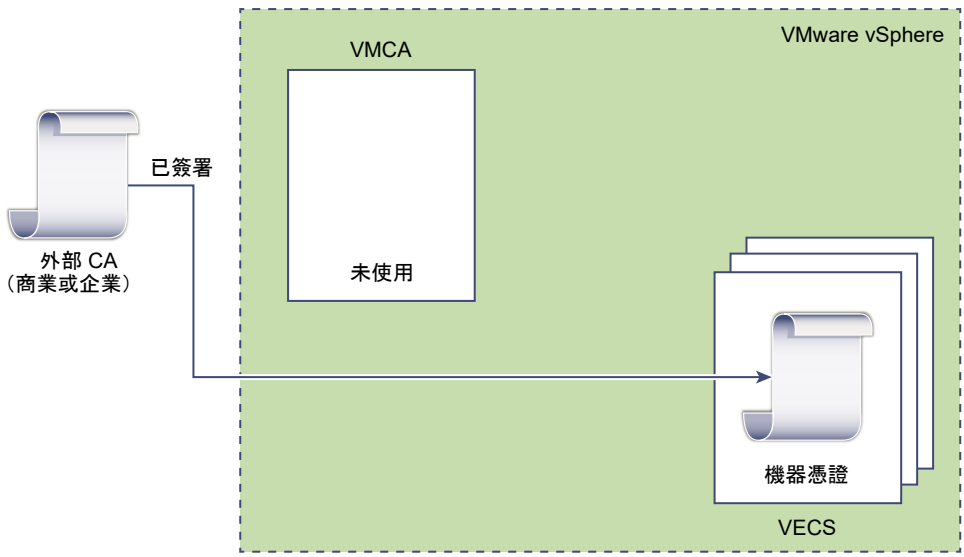
- 將 VMCA 根憑證取代為自訂簽署憑證並取代所有憑證
- 將機器 SSL 憑證取代為 VMCA 憑證 (多節點增強型連結模式部署)
- 將解決方案使用者憑證取代為 VMCA 憑證 (多節點增強型連結模式部署)

如需手動憑證取代的相關資訊，請參閱使用 VMCA 做為中繼憑證授權機構。

用自訂憑證而非 VMCA 進行佈建

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

圖 2-3. 外部憑證直接儲存在 VECS 中



您可以使用下列 vSphere Certificate Manager 選項：

- 將機器 SSL 憑證取代為自訂憑證
- 將解決方案使用者憑證取代為自訂憑證

如需手動憑證取代的相關資訊，請參閱將自訂憑證與 vSphere 搭配使用。

也可以使用 vSphere Client 產生機器 SSL 憑證 (自訂) 的 CSR，然後在 CA 傳回憑證後將其取代。請參閱使用 vSphere Client 產生機器 SSL 憑證的憑證簽署要求 (自訂憑證)。

混合部署

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

公司原則通常不允許存在中繼 CA。在這些情況下，混合部署是很好的解決方案。這樣可最大限度地減少要取代的憑證數目，並確保所有流量的安全。混合部署僅保留內部流量 (即解決方案使用者流量) 以使用預設 VMCA 簽署憑證。

ESXi 憑證取代

對於 ESXi 主機，您可以透過 vSphere Client 變更憑證佈建行為。如需詳細資料，請參閱 vSphere 安全性說明文件。

表 2-4. ESXi 憑證取代選項

選項	說明
VMware Certificate Authority 模式 (預設)	從 vSphere Client 更新憑證時，VMCA 會核發用於主機的憑證。如果您將 VMCA 根憑證變更為包含憑證鏈結，則主機憑證會包含完整鏈結。
自訂憑證授權機構模式	允許您手動更新和使用並非由 VMCA 簽署或核發的憑證。
指紋模式	可用於在重新整理期間保留 5.5 憑證。將此模式僅暫時用於偵錯情況。

vSphere 使用憑證所在位置

VMware Certificate Authority (VMCA) 會使用憑證佈建您的環境。憑證包括用於安全連線的機器 SSL 憑證、用於向 vCenter Single Sign-On 驗證服務的解決方案使用者憑證，以及用於 ESXi 主機的憑證。

使用中的憑證如下。

表 2-5. vSphere 中的憑證

憑證	已佈建	註解
ESXi 憑證	VMCA (預設)	儲存在 ESXi 本機主機上。
機器 SSL 憑證	VMCA (預設)	儲存在 VECS 中。
解決方案使用者憑證	VMCA (預設)	儲存在 VECS 中。

表 2-5. vSphere 中的憑證 (續)

憑證	已佈建	註解
vCenter Single Sign-On SSL 簽署憑證	於安裝期間佈建。	從命令列管理此憑證。 **備註** 請勿在檔案系統中變更此憑證，否則可能導致無法預期的行為。
VMware Directory Service (VMDIR) SSL 憑證	於安裝期間佈建。	從 vSphere 6.5 開始，機器 SSL 憑證會用作 vmdir 憑證。

ESXi

ESXi 憑證儲存在每台主機本機上的 `/etc/vmware/ssl` 目錄中。VMCA 預設佈建 ESXi 憑證，但是您可以改為使用自訂憑證。ESXi 憑證會在主機首次新增到 vCenter Server 以及主機重新連線時佈建。

機器 SSL 憑證

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

每個 vCenter Server 節點都擁有自己的機器 SSL 憑證。在 vCenter Server 節點上執行的所有服務都會使用此機器 SSL 憑證公開其 SSL 端點。

以下服務使用機器 SSL 憑證。

- 反向 Proxy 服務。與個別 vCenter 服務的 SSL 連線一律經過反向 Proxy。流量並不會進入服務本身。
- vCenter Server 服務 (vpxd)。
- VMware Directory Service (vmdir)。

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

解決方案使用者憑證

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

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

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

VECS 中包括下列解決方案使用者憑證存放區：

- `machine`：由 License Server 及記錄服務所使用。

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

- `vpxd`：vCenter 服務精靈 (vpxd) 存放區。vpxd 會使用儲存在此存放區中的解決方案使用者憑證來驗證 vCenter Single Sign-On。
- `vpxd-extension`：vCenter 延伸存放區。包含 Auto Deploy 服務、Inventory Service 及不屬於其他解決方案使用者的其他服務。
- `vsphere-webclient`：vSphere Client 存放區。還包括一些其他服務，例如效能圖服務。
- `wcp`：VMware vSphere® with VMware Tanzu™ 存放區。

內部憑證

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

vCenter Single Sign-On 簽署憑證

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

您可以從 CLI 取代此憑證。請參閱取代 STS 憑證。

VMware Directory Service SSL 憑證

從 vSphere 6.5 開始，機器 SSL 憑證會用作 VMware 目錄憑證。如需 vSphere 早期版本的相關資訊，請參閱對應的說明文件。

vSphere 虛擬機器加密憑證

vSphere 虛擬機器加密解決方案透過外部金鑰管理伺服器 (KMS) 連線。取決於解決方案向 KMS 的驗證方式，可能會產生憑證並將其儲存在 VECS 中。請參閱 vSphere 安全性說明文件。

VMCA 和 VMware Core Identity Services

核心身分識別服務是每個 vCenter Server 系統的一部分。VMCA 是每個 VMware Core Identity Services 群組的一部分。請使用管理 CLI 和 vSphere Client 與這些服務進行互動。

VMware Core Identity Services 包含數個元件。

表 2-6. Core Identity Services

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

VMware Endpoint 憑證存放區概觀

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

VECS 會隨 VMware Authentication Framework 精靈 (VMAFD) 一併執行。VECS 會在每個 vCenter Server 節點上執行，且具有包含憑證與金鑰的金鑰儲存區。

VECS 會定期輪詢 VMware Directory Service (vmdir) 以查看受信任的根存放區是否有任何更新。您也可以使用 `vecs-cli` 命令明確管理 VECS 中的憑證和金鑰。請參閱 vecs-cli 命令參考。

VECS 包含下列存放區。

表 2-7. VECS 中的存放區

存放區	說明
機器的 SSL 存放區 (MACHINE_SSL_CERT)	■ 由每個 vSphere 節點上反向 Proxy 服務所使用。 ■ 由每個 vCenter Server 節點上 VMware Directory Service (vmdir) 所使用。 vSphere 6.0 及更新版本中的所有服務都會透過使用機器 SSL 憑證的反向 Proxy 進行通訊。為確保回溯相容性，5.x 服務仍會使用特定的連接埠。因此，部分服務 (例如 vpxd) 仍會將自己的連接埠維持開啟。
解決方案使用者存放區 ■ machine ■ vpxd ■ vpxd-extension ■ vsphere-webclient ■ wcp	對於每個解決方案使用者，VECS 包含一個存放區。每個解決方案使用者憑證的主旨必須是唯一的，例如，機器憑證不能與 vpxd 憑證的主旨相同。 解決方案使用者憑證用於透過 vCenter Single Sign-On 進行驗證。vCenter Single Sign-On 會檢查憑證是否有效，但不會檢查其他憑證屬性。 VECS 中包括下列解決方案使用者憑證存放區： ■ machine：由 License Server 及記錄服務所使用。 **備註** 機器解決方案使用者憑證與機器的 SSL 憑證毫無關聯。機器解決方案使用者憑證用於進行 SAML Token 交換。機器的 SSL 憑證用於對機器進行安全 SSL 連線。 ■ vpxd：vCenter 服務精靈 (vpxd) 存放區。vpxd 會使用儲存在此存放區中的解決方案使用者憑證來驗證 vCenter Single Sign-On。 ■ vpxd-extension：vCenter 延伸存放區。包含 Auto Deploy 服務、Inventory Service 及不屬於其他解決方案使用者的其他服務。 ■ vsphere-webclient：vSphere Client 存放區。還包括一些其他服務，例如效能圖服務。 ■ wcp：VMware vSphere® with VMware Tanzu™ 存放區。 每個 vCenter Server 節點均包含一個 machine 憑證。
受信任的根存放區 (TRUSTED_ROOTS)	包含所有受信任的根憑證。
vSphere Certificate Manager 公用程式備份存放區 (BACKUP_STORE)	由 VMCA (VMware Certificate Manager) 用於支援憑證還原。只有最新狀態會儲存為備份，您無法還原一個以上的步驟。
其他存放區	其他存放區可能由解決方案新增。例如，Virtual Volumes 解決方案將新增一個 SMS 存放區。除非 VMware 說明文件或 VMware 知識庫文章指示您修改這些存放區中的憑證，否則請勿這麼做。 **備註** 刪除 TRUSTED_ROOTS_CRLS 存放區會損壞您的憑證基礎結構。請勿刪除或修改 TRUSTED_ROOTS_CRLS 存放區。

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

部分憑證會在啟動期間暫時或永久儲存在檔案系統中。請勿變更檔案系統中的憑證。

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

管理憑證撤銷

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

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

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

大型部署中的憑證取代

取代具有大量 vCenter Server 主機之部署中的憑證時，可以使用 vSphere Certificate Management 公用程式或手動取代憑證。一些最佳做法可引導您完成所選程序。

取代具有多個 vCenter Server 節點之環境中的機器 SSL 憑證

如果您的環境包含多個 vCenter Server 節點，可以使用 vSphere Client 或 vSphere Certificate Manager 公用程式取代憑證，或使用 ESXCLI 命令手動取代。

vSphere Certificate Manager

在每台機器上執行 vSphere Certificate Manager。視您所執行的工作而定，系統也會提示您輸入憑證資訊。

手動憑證取代

對於手動憑證取代，您需要在每台機器上執行憑證取代命令。如需詳細資訊，請參閱下列主題：

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

在具有多個處於增強型連結模式下的 vCenter Server 系統的環境中取代解決方案使用者憑證

如果您的環境包含多個處於增強型連結模式下的 vCenter Server 系統，請依照下列步驟進行憑證取代。

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

vSphere Certificate Manager

在每台機器上執行 vSphere Certificate Manager。視您所執行的工作而定，系統也會提示您輸入憑證資訊。

手動憑證取代

1. 產生或要求憑證。您需要下列憑證：
   - 每個 vCenter Server 上機器解決方案使用者的憑證。

- 每個節點上的下列每個解決方案使用者的憑證：
  - vpxd 解決方案使用者
  - vpxd-extension 解決方案使用者
  - vsphere-webclient 解決方案使用者
  - wcp 解決方案使用者

2 取代每個節點上的憑證。確切程序會視您所執行的憑證取代類型而定。請參閱透過 vSphere Certificate Manager 公用程式管理憑證。

如需詳細資訊，請參閱下列主題：

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

包含外部解決方案之環境中的憑證取代

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

您可以執行 `ls_update_certs` 指令碼來解決此問題。如需詳細資料，請參閱 VMware 知識庫文章，網址為 http://kb.vmware.com/kb/2109074。

使用 vSphere Client 管理憑證

您可以使用 vSphere Client 檢視和管理憑證。也可以使用 vSphere Certificate Manager 公用程式執行許多憑證管理工作。

vSphere Client 可讓您執行以下管理工作。

- 檢視受信任的根憑證和機器 SSL 憑證。
- 更新現有憑證或取代憑證。
- 產生機器 SSL 憑證的自訂憑證簽署要求 (CSR)，並且在憑證授權機構傳回憑證將其取代。

大部分的憑證取代工作流程完全可從 vSphere Client 進行。若要產生機器 SSL 憑證的 CSR，您可以使用 vSphere Client 或 Certificate Manager 公用程式。

支援的工作流程

依預設，vCenter Server 安裝完成後，該節點上的 VMware Certificate Authority 會使用憑證佈建環境中的所有其他節點。請參閱第 2 章 vSphere 安全性憑證，取得管理憑證的目前建議。

您可以使用下列其中一個工作流程來更新或取代憑證。

更新憑證

您可以讓 VMCA 透過 vSphere Client 更新您環境中的 SSL 憑證和解決方案使用者憑證。

使 VMCA 成為中繼 CA

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

將憑證取代為自訂憑證

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

備註 如果您使用 VMCA 做為中繼 CA 或使用自訂憑證，可能會遇到非常複雜的問題，且可能對安全性產生負面影響，並且增加不必要的運作風險。如需有關在 vSphere 環境中管理憑證的詳細資訊，請參閱標題為〈新產品逐步解說 - 混合 vSphere SSL 憑證取代〉的部落格文章，網址為：http://vmware.com/go/hybridvmca。

從 vSphere Client 深入瞭解憑證存放區

每個 vCenter Server 節點上均包含 VMware Endpoint 憑證存放區 (VECS) 執行個體。您可以從 vSphere Client 深入瞭解 VMware Endpoint 憑證存放區內的不同存放區，包括機器 SSL 和受信任的根憑證。

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

必要條件

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

程序

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

   如果在安裝期間指定了其他網域，請以 administrator@*mydomain* 身分登入。
3. 導覽至憑證管理 UI。
   a. 從**首頁**功能表中，選取**管理**。
   b. 在**憑證**下，按一下**憑證管理**。
4. 如果系統提示您，請輸入 vCenter Server 的認證。
5. 深入瞭解儲存在 VMware Endpoint 憑證存放區 (VECS) 中的憑證。

   VMware Endpoint 憑證存放區概觀會說明個別存放區內的項目。
6. 若要檢視憑證的詳細資料，請選取該憑證，然後按一下**檢視詳細資料**。

7 使用**動作**功能表來更新或取代憑證。

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

設定 vCenter 憑證到期警告臨界值

vCenter Server 會監控 VMware Endpoint 憑證存放區 (VECS) 中的所有憑證，並在距離憑證到期 30 天或更短時間時發出警示。您可以使用 `vpxd.cert.threshold` 進階選項來變更收到警告的時間。

程序

1 登入 vSphere Client。

2 選取 vCenter Server 物件，然後按一下**設定**。

3 按一下**進階設定**。

4 按一下**編輯設定**，然後篩選**臨界值**。

5 將 `vpxd.cert.threshold` 的設定變更為所需的值，然後按一下**儲存**。

從 vSphere Client 將 VMCA 憑證更新為新的 VMCA 簽署憑證

您可以使用新的 VMCA 簽署憑證取代所有 VMCA 簽署憑證。此程序稱為更新憑證。可以從 vSphere Client 更新您環境中的所選憑證或所有憑證。

必要條件

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

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至憑證管理 UI。

a 從**首頁**功能表中，選取**管理**。

b 在**憑證**下，按一下**憑證管理**。

4 如果系統提示您，請輸入 vCenter Server 的認證。

5 更新本機系統的 VMCA 簽署機器 SSL 憑證。

a 選取**機器 SSL 憑證**。

b 按一下**動作 > 更新**。

c 按一下**更新**。

vCenter Server 服務會自動重新啟動。您必須重新登入，因為將服務會自動重新啟動會結束 UI 工作階段。

將您的系統設定為使用自訂憑證

您可以將環境設定為使用自訂憑證。

您可以使用 Certificate Manager 公用程式針對每個機器和每個解決方案使用者產生憑證簽署要求 (CSR)。您也可以為每個機器產生 CSR，並且當您從第三方 CA 收到憑證時使用 vSphere Client 將其取代。將 CSR 提交給您的內部或第三方 CA 後，CA 會傳回已簽署憑證和根憑證。您可以從 vCenter ServerUI 上傳根憑證和已簽署憑證。

使用 vSphere Client 產生機器 SSL 憑證的憑證簽署要求 (自訂憑證)

機器 SSL 憑證是由每個 vCenter Server 節點上的反向 Proxy 服務所使用。每台機器必須具有機器 SSL 憑證，以便與其他服務進行安全通訊。您可以使用 vSphere Client，產生機器 SSL 憑證的憑證簽署要求 (CSR) 並且在準備就緒後取代憑證。

必要條件

憑證必須符合以下需求：

- 金鑰大小：2048 位元 (下限) 至 16384 位元 (上限) (PEM 編碼)
- CRT 格式
- x509 第 3 版
- SubjectAltName 必須包含 DNS Name=<machine_FQDN>。
- 包含下列金鑰使用方法：數位簽章、不可否認性、金鑰編密

備註 請勿在任何自訂憑證中使用 CRL 發佈點、授權資訊存取或憑證範本資訊。

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至憑證管理 UI。

a 從**首頁**功能表中，選取**管理**。

b 在**憑證**下，按一下**憑證管理**。

4 輸入您 vCenter Server 的認證。

5 產生 CSR。

a 在**機器 SSL 憑證**下，對於您想要取代的憑證按一下**動作 > 產生憑證簽署要求 (CSR)**。

b 輸入您的憑證資訊，然後按**下一步**。

> **備註** 當您使用 vCenter Server 產生金鑰大小為 16384 位元的 CSR 時，由於該作業佔用大量 CPU，因此產生需要幾分鐘的時間才能完成。

c 複製或下載 CSR。

d 按一下**完成**。

e 向憑證授權機構提供 CSR。

後續步驟

當憑證授權機構傳回憑證時，取代憑證存放區中的現有憑證。請參閱新增自訂憑證。

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

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

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

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

必要條件

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

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

程序

1 在您環境中的每台機器上，啟動 vSphere Certificate Manager，然後選取選項 1。

2 提供密碼以及 vCenter ServerIP 位址或主機名稱 (如果出現此提示)。

3 選取選項 1 以產生 CSR，回應提示並結束 Certificate Manager。

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

4 如果還希望取代所有解決方案使用者憑證，請重新啟動 Certificate Manager。

5 選取選項 5。

6 提供密碼以及 vCenter ServerIP 位址或主機名稱 (如果出現此提示)。

7 選取選項 1 以產生 CSR，回應提示並結束 Certificate Manager。

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

後續步驟

執行憑證取代。

將受信任的根憑證新增至憑證存放區

如果要在環境中使用第三方憑證，必須將受信任的根憑證新增至憑證存放區。

必要條件

從第三方或內部 CA 取得自訂根憑證。

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至憑證管理 UI。

a 從**首頁**功能表中，選取**管理**。

b 在**憑證**下，按一下**憑證管理**。

4 如果系統提示您，請輸入 vCenter Server 的認證。

5 在**受信任的根憑證**下，按一下**新增**。

6 按一下**瀏覽**，然後選取憑證鏈結的位置。

您可以使用以下檔案類型：CER、PEM 或 CRT。

7 按一下**新增**。

憑證將新增至存放區。

新增自訂憑證

您可以將自訂機器 SSL 憑證新增至憑證存放區。

通常，取代每個元件的機器 SSL 憑證就已足夠。

必要條件

針對您要取代的每個憑證產生憑證簽署要求 (CSR)。您可以透過 Certificate Manager 公用程式來產生 CSR。您也可以使用 vSphere Client 產生機器 SSL 憑證的 CSR。將憑證和私密金鑰放置到 vCenter Server 可存取的位置。

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至憑證管理 UI。

a 從**首頁**功能表中，選取**管理**。

b 在**憑證**下，按一下**憑證管理**。

4 如果系統提示您，請輸入 vCenter Server 的認證。

5 在**機器 SSL 憑證**下，針對您要取代的憑證按一下**動作 > 匯入並取代憑證**。

6 按一下相應的憑證取代選項，然後按**下一步**。

選項	說明
取代為 VMCA	建立 VMCA 產生的 CSR 來取代目前憑證。
取代為從 vCenter Server 產生的憑證。	使用由 vCenter Server 產生的 CSR 所簽署的憑證來取代目前憑證。
取代為外部 CA 憑證 (需要私密金鑰)	使用由外部 CA 簽署的憑證來取代目前憑證。

7 輸入 CSR 資訊，或上傳適當的憑證。

8 按一下**取代**。

vCenter Server 服務會自動重新啟動。

透過 vSphere Certificate Manager 公用程式管理憑證

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

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

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

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

Certificate Manager 公用程式位置

您可以在命令列上執行工具，如下所示：

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

本文件中的 Certificate Manager 選項和工作流程

依序執行 Certificate Manager 選項以完成工作流程。部分選項 (如產生 CSR) 會用於不同的工作流程。

將 VMCA 根憑證取代為自訂簽署憑證並取代所有憑證。

此單選項工作流程 (選項 2) 可單獨使用，也可在中繼憑證工作流程中使用。請參閱重新產生新的 VMCA 根憑證並取代所有憑證。

使 VMCA 成為中繼憑證授權機構

若要使 VMCA 成為中繼 CA，您必須多次執行 Certificate Manager。此工作流程提供用於取代機器 SSL 憑證和解決方案使用者憑證的完整步驟。

1 若要產生 CSR，請選取選項 2，將 VMCA 根憑證取代為自訂簽署憑證並取代所有憑證。您稍後可能需要提供憑證的部分相關資訊。當系統提示您需要再次選取選項時，請選取選項 1。

   將 CSR 提交至外部或企業 CA。您會從 CA 收到一個已簽署的憑證和一個根憑證。

2 合併 VMCA 根憑證和 CA 根憑證，然後儲存檔案。

3 選取選項 2，將 VMCA 根憑證取代為自訂簽署憑證並取代所有憑證。此程序會取代本機上的所有憑證。

4 在增強型連結模式組態中連線多個 vCenter Server 執行個體時，必須取代每個節點上的憑證。

   a 首先，將機器 SSL 憑證取代為 (新的) VMCA 憑證 (選項 3)。

   b 然後，將解決方案使用者憑證取代為 (新的) VMCA 憑證 (選項 6)。

請參閱使 VMCA 成為中繼憑證授權機構 (Certificate Manager)。

將所有憑證取代為自訂憑證

若要將所有憑證取代為自訂憑證，您必須多次執行 Certificate Manager。此工作流程提供用於取代機器 SSL 憑證和解決方案使用者憑證的完整步驟。

1 在每台機器上分別產生機器 SSL 憑證和解決方案使用者憑證的憑證簽署要求。

   a 若要產生機器 SSL 憑證的 CSR，請選取選項 1。

   b 如果公司原則要求您取代所有憑證，您還需要選取選項 5。

2 從 CA 收到已簽署的憑證和根憑證後，即可使用選項 1 來取代每台機器上的機器 SSL 憑證。

3 如果您還希望取代解決方案使用者憑證，請選取選項 5。

4 最後，在增強型連結模式組態中連線多個 vCenter Server 執行個體時，必須在每個節點上重複此程序。

請參閱用自訂憑證取代所有憑證 (Certificate Manager)。

備註 執行 Certificate Manager 公用程式時會出現下列提示：

```
Enter proper value for VMCA 'Name':
```

輸入執行憑證組態之機器的完整網域名稱，回應提示。

重新產生新的 VMCA 根憑證並取代所有憑證

您可以重新產生 VMCA 根憑證，並將本機機器 SSL 憑證和本機解決方案使用者憑證取代為 VMCA 簽署憑證。在增強型連結模式組態中連線多個 vCenter Server 執行個體時，您必須取代每個 vCenter Server 上的憑證。

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

- administrator@vsphere.local 的密碼
- 兩個字母形式的國碼
- 公司名稱
- 組織名稱
- 組織單位
- 狀態
- 位置
- IP 位址 (選用)
- 電子郵件
- 主機名稱，即要進行憑證取代之機器的完整網域名稱。如果主機名稱與 FQDN 不相符，憑證取代就無法正確完成，而您的環境可能會最終處於不穩定狀態。
- vCenter Server 的 IP 位址。
- VMCA 名稱，即執行憑證組態之機器的完整網域名稱。

必要條件

當您使用此選項執行 vSphere Certificate Manager 時，必須瞭解以下資訊。

- administrator@vsphere.local 的密碼。
- 您希望產生新 VMCA 簽署憑證之機器的 FQDN。所有其他內容都會預設為預先定義的值，但您可以變更這些值。

程序

1. 在 vCenter Server 上啟動 vSphere Certificate Manager。
2. 選取選項 4。
3. 對提示做出回應。

   Certificate Manager 會根據您的輸入，產生新的 VMCA 根憑證，並取代您執行 Certificate Manager 所在系統上的所有憑證。在 Certificate Manager 將服務重新啟動後，取代程序即已完成。
4. 若要取代機器 SSL 憑證，請使用選項 3 `Replace Machine SSL certificate with VMCA Certificate` 執行 vSphere Certificate Manager。

5 若要取代解決方案使用者憑證，請使用選項 6
`Replace Solution user certificates with VMCA certificates` 執行 Certificate Manager。

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

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

VMware 不建議取代 STS 憑證，也不建議使用次級 CA 來取代 VMCA。如果您選擇其中一個選項，可能會遇到非常複雜的問題，且可能對安全性產生負面影響，並且增加不必要的運作風險。如需有關在 vSphere 環境中管理憑證的詳細資訊，請參閱標題為〈新產品逐步解說 - 混合 vSphere SSL 憑證取代〉的部落格文章，網址為：http://vmware.com/go/hybridvmca。

若要使 VMCA 成為中繼 CA，您必須多次執行 Certificate Manager。此工作流程提供一組用於取代機器 SSL 憑證的完整步驟。

1 若要產生 CSR，請選取選項 1，將機器 SSL 憑證取代為自訂憑證，然後執行選項 1。

您會從 CA 收到一個已簽署的憑證和一個根憑證。

2 合併 VMCA 根憑證和 CA 根憑證，然後儲存檔案。

3 選取選項 2，將 VMCA 根憑證取代為自訂簽署憑證並取代所有憑證。此程序會取代本機上的所有憑證。

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

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

- 您可以使用 vSphere Certificate Manager 建立 CSR。
- 如果您偏好手動建立 CSR，則傳送要求簽署的憑證必須符合下列需求：
  - 金鑰大小：2048 位元 (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
  - 對於根憑證，CA 延伸必須設為 true，憑證簽署必須位於需求清單中。例如：

```
basicConstraints        = critical,CA:true
keyUsage                = critical,digitalSignature,keyCertSign
```

  - 必須啟用 CRL 簽署。
  - 增強金鑰使用方法可以為空白或包含伺服器驗證。
  - 對憑證鏈結的長度無明確限制。VMCA 預設使用 OpenSSL (為 10 個憑證)。
  - 不支援含萬用字元或多個 DNS 名稱的憑證。

- 您無法建立 VMCA 的附屬 CA。

  如需使用 Microsoft 憑證授權機構的範例，請參閱 VMware 知識庫文章：Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x (在 vSphere 6.x 中建立 Microsoft 憑證授權機構範本以建立 SSL 憑證)，網址為 http://kb.vmware.com/kb/2112009。

必要條件

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

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

程序

1. 執行 vSphere Certificate Manager。

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

2. 選取選項 2。

   剛開始時您可以使用此選項產生 CSR，而不是取代憑證。

3. 提供密碼以及 vCenter ServerIP 位址或主機名稱 (如果出現此提示)。

4. 選取選項 1 來產生 CSR 並回應提示。

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

5. 命名憑證簽署要求 (CSR) `root_signing_cert.csr`。

6. 將 CSR 傳送到企業或外部 CA 進行簽署，然後命名產生的已簽署憑證 `root_signing_cert.cer`。

7. 在文字編輯器中，按以下方式合併憑證。

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

8. 將檔案儲存為 `root_signing_chain.cer`。

後續步驟

將現有根憑證取代為鏈結的根憑證。請參閱將 VMCA 根憑證取代為自訂簽署憑證並取代所有憑證。

將 VMCA 根憑證取代為自訂簽署憑證並取代所有憑證

您可以使用 vSphere Certificate Manager 產生 CSR 並將其傳送至企業或第三方 CA 進行簽署。然後，您可以將 VMCA 根憑證取代為自訂簽署憑證，並將所有現有的憑證取代為自訂 CA 所簽署的憑證。

您可以在 vCenter Server 上執行 vSphere Certificate Manager，將 VMCA 根憑證取代為自訂簽署憑證。

必要條件

- 產生憑證鏈結。
  - 您可以使用 vSphere Certificate Manager 建立 CSR 或手動建立 CSR。
  - 當您從第三方或企業 CA 收到已簽署的憑證後，將它與初始 VMCA 根憑證合併，以建立完整鏈結。

    如需憑證需求和憑證合併程序的相關資訊，請參閱使用 vSphere Certificate Manager 產生 CSR 並準備根憑證 (中繼 CA)。
- 收集所需的資訊。
  - administrator@vsphere.local 的密碼
  - 有效的自訂根憑證 (`.crt` 檔案)
  - 有效的自訂根使用者金鑰 (`.key` 檔案)

程序

1. 在 vCenter Server 主機上啟動 vSphere Certificate Manager 並選取選項 2。
2. 再次選取選項 2 以啟動憑證取代並回應提示。
   a. 出現提示時，指定根憑證的完整路徑。
   b. 如果是第一次取代憑證，系統會提示您輸入用於機器 SSL 憑證的資訊。

      此資訊包含所需的機器 FQDN 並儲存於 `certool.cfg` 檔案中。

將機器 SSL 憑證取代為 VMCA 憑證 (中繼 CA)

使用 VMCA 當做中繼 CA 時，您可以明確地取代機器 SSL 憑證。首先，取代 vCenter Server 上的 VMCA 根憑證，接著可以取代將由 VMCA 的新 root 帳戶簽署的機器 SSL 憑證。您亦可使用該選項來取代已損壞或即將到期的機器 SSL 憑證。

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

- administrator@vsphere.local 的密碼
- 兩個字母形式的國碼
- 公司名稱
- 組織名稱
- 組織單位

- 狀態
- 位置
- IP 位址 (選用)
- 電子郵件
- 主機名稱，即要進行憑證取代之機器的完整網域名稱。如果主機名稱與 FQDN 不相符，憑證取代就無法正確完成，而您的環境可能會最終處於不穩定狀態。
- vCenter Server 的 IP 位址。
- VMCA 名稱，即執行憑證組態之機器的完整網域名稱。

必要條件

- 您必須瞭解以下資訊以使用此選項執行 Certificate Manager。
  - administrator@vsphere.local 的密碼。
  - 您希望產生新 VMCA 簽署憑證之機器的 FQDN。所有其他內容都會預設為預先定義的值，但您可以變更這些值。
  - vCenter Server 系統的主機名稱或 IP 位址。

程序

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

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

結果

vSphere Certificate Manager 取代機器 SSL 憑證。

將解決方案使用者憑證取代為 VMCA 憑證 (中繼 CA)

使用 VMCA 當做中繼 CA 時，您可以明確地取代解決方案使用者憑證。首先，取代 vCenter Server 上的 VMCA 根憑證，接著可以取代將由 VMCA 的新 root 帳戶簽署的解決方案使用者憑證。您亦可使用該選項來取代已損壞或即將到期的解決方案憑證。

必要條件

- 如果您在增強型連結模式組態中由 vCenter Server 的多個執行個體組成的部署中取代 VMCA 根憑證，請明確將所有 vCenter Server 節點重新啟動。
- 您必須瞭解以下資訊以使用此選項執行 Certificate Manager。
  - administrator@vsphere.local 的密碼
  - vCenter Server 系統的主機名稱或 IP 位址

程序

1 啟動 vSphere Certificate Manager 並選取選項 6。

2 對提示做出回應。

如需詳細資訊，請參閱 VMware 知識庫文章，網址為 http://kb.vmware.com/kb/2112281。

結果

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

用自訂憑證取代所有憑證 (Certificate Manager)

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

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

使用自訂憑證時，請將 VMCA 簽署的憑證取代為自訂憑證。您可以使用 vSphere Client、vSphere Certificate Manager 公用程式或 CLI 進行手動憑證取代。憑證存儲在 VECS 中。

若要將所有憑證取代為自訂憑證，您必須多次執行 Certificate Manager。此工作流程提供用於取代機器 SSL 憑證和解決方案使用者憑證的完整步驟。

1 在每台機器上分別產生機器 SSL 憑證和解決方案使用者憑證的憑證簽署要求。

a 若要產生機器 SSL 憑證的 CSR，請選取選項 1。

b 如果公司原則不允許混合部署，請選取選項 5。

2 從 CA 收到已簽署的憑證和根憑證後，即可使用選項 1 來取代每台機器上的機器 SSL 憑證。

3 如果您還希望取代解決方案使用者憑證，請選取選項 5。

4 最後，當增強型連結模式組態中連線多個 vCenter Server 執行個體時，必須在每個節點上重複此程序。

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

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

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

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

必要條件

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

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

- 若要產生機器 SSL 憑證的 CSR，系統會提示您輸入憑證內容，這些內容儲存在 `certool.cfg` 檔案中。對於大部分的欄位，您可以接受預設值，或提供站台專屬值。機器的 FQDN 為必填。

程序

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

   在程序過程中，您必須提供目錄。Certificate Manager 會將憑證和金鑰檔案放置於目錄中。
4. 如果還希望取代所有解決方案使用者憑證，請重新啟動 Certificate Manager。
5. 選取選項 5。
6. 提供密碼以及 vCenter ServerIP 位址或主機名稱 (如果出現此提示)。
7. 選取選項 1 以產生 CSR，回應提示並結束 Certificate Manager。

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

後續步驟

執行憑證取代。

將機器 SSL 憑證取代為自訂憑證

機器 SSL 憑證是由每個 vCenter Server 節點上的反向 Proxy 服務所使用。每台機器必須具有機器 SSL 憑證，以便與其他服務進行安全通訊。您可以將每個節點上的憑證取代為自訂憑證。

必要條件

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

1. 若要使用 vSphere Certificate Manager 產生 CSR，請參閱使用 vSphere Certificate Manager 產生憑證簽署要求 (自訂憑證)。
2. 若要明確產生 CSR，請向第三方或企業 CA 要求每台機器的憑證。憑證必須符合以下需求：
   - 金鑰大小：2048 位元 (下限) 至 16384 位元 (上限) (PEM 編碼)
   - CRT 格式
   - x509 第 3 版
   - SubjectAltName 必須包含 DNS Name=<machine_FQDN>。
   - 包含下列金鑰使用方法：數位簽章、不可否認性、金鑰編密

備註 請勿在任何自訂憑證中使用 CRL 發佈點、授權資訊存取或憑證範本資訊。

另請參閱 VMware 知識庫文章〈從 Microsoft 憑證授權機構取得 vSphere 憑證〉，網址為 http://kb.vmware.com/kb/2112014。

程序

1 啟動 vSphere Certificate Manager 並選取選項 1。

2 選取選項 2 以啟動憑證取代並回應提示。

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

- administrator@vsphere.local 的密碼
- 有效的機器 SSL 自訂憑證 (`.crt` 檔案)
- 有效的機器 SSL 自訂金鑰 (`.key` 檔案)
- 用於自訂機器 SSL 憑證 (`.crt` 檔案) 的有效簽署憑證
- vCenter Server 的 IP 位址

將解決方案使用者憑證取代為自訂憑證

許多公司僅要求您取代可從外部存取之服務的憑證。但 Certificate Manager 也支援取代解決方案使用者憑證。解決方案使用者是服務的集合，例如，與 vSphere Client 相關聯的所有服務。

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

格式應類似以下內容。

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

必要條件

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

1 若要使用 vSphere Certificate Manager 產生 CSR，請參閱使用 vSphere Certificate Manager 產生憑證簽署要求 (自訂憑證)。

2 向第三方或企業 CA 為每個節點上的每個解決方案使用者要求憑證。您可以使用 vSphere Certificate Manager 產生 CSR，也可以手動準備。CSR 必須符合以下需求：

- 金鑰大小：2048 位元 (下限) 至 16384 位元 (上限) (PEM 編碼)
- CRT 格式
- x509 第 3 版
- SubjectAltName 必須包含 DNS Name=<machine_FQDN>。
- 每個解決方案使用者憑證必須具有不同的 `Subject`。例如，您可以考慮加入解決方案使用者名稱 (例如 vpxd) 或其他唯一識別碼。

- 包含下列金鑰使用方法：數位簽章、不可否認性、金鑰編密

另請參閱 VMware 知識庫文章〈從 Microsoft 憑證授權機構取得 vSphere 憑證〉，網址為 http://kb.vmware.com/kb/2112014。

程序

1 啟動 vSphere Certificate Manager 並選取選項 5。

2 選取選項 2 以啟動憑證取代並回應提示。

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

- administrator@vsphere.local 的密碼
- 機器解決方案使用者的憑證與金鑰
- 機器解決方案使用者的憑證和金鑰 (`vpxd.crt` 和 `vpxd.key`)
- 所有解決方案使用者的一組完整憑證與金鑰 (`vpxd.crt` 和 `vpxd.key`)

重新發佈舊憑證以還原最後執行的作業

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

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

重設所有憑證

若要將全部現有 vCenter 憑證取代為由 VMCA 簽署的憑證，請使用 `Reset All Certificates` 選項。

使用此選項時，會覆寫目前 VECS 中的所有自訂憑證。

vSphere Certificate Manager 可以取代所有憑證。取代的憑證取決於您選擇的選項。

手動憑證取代

對於某些特殊的憑證取代案例，您無法使用 vSphere Certificate Manager 公用程式。可改為使用隨附於安裝的 CLI 進行憑證取代。

瞭解停止和啟動服務

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

您必須在憑證取代程序期間停止和啟動服務。

請遵循下列準則。

- 請勿停止服務以產生新的公開/私密金鑰配對或新憑證。

- 如果您是唯一的管理員，當您新增根憑證時，不需要停止服務。舊的根憑證仍然可用，所有服務仍可以使用該憑證進行驗證。新增根憑證後，請將所有服務停止並立即重新啟動，以避免主機發生問題。
- 如果您的環境包含多個管理員，請在新增根憑證前停止服務，並於新增憑證後重新啟動服務。
- 在 VECS 中刪除機器 SSL 憑證之前立即停止服務。

用新的 VMCA 簽署憑證取代現有的 VMCA 簽署憑證

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

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

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

必要條件

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

產生新的 VMCA 簽署根憑證

您使用 `certool`CLI 或 vSphere Certificate Manager 公用程式產生新的 VMCA 簽署憑證並將此憑證發佈到 vmdir。

程序

1 在 vCenter Server 上，產生新的自我簽署憑證和私密金鑰。

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

2 將現有根憑證取代為新的憑證。

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

命令會產生憑證、將憑證新增至 vmdir 及 VECS。

3 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

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

4 (選擇性) 將新的根憑證發佈到 vmdir。

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

此命令立即更新 vmdir 的所有執行個體。如果您不執行此命令，則將新憑證傳播至所有節點可能需要花些時間。

5 重新啟動所有服務。

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

範例： 產生新的 VMCA 簽署根憑證

下列範例會顯示確認目前根 CA 資訊以及重新產生根憑證的所有步驟。

1 (選用) 在 vCenter Server 上，列出 VMCA 根憑證以確定其位於憑證存放區。

```
/usr/lib/vmware-vmca/bin/certool --getrootca
```

輸出會類似下列內容：

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

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

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry list --store TRUSTED_ROOTS --text
```

在只有一個根憑證的最單純情況下，輸出會類似下列內容：

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

3 產生新的 VMCA 根憑證。此命令會將憑證新增到 VECS 中的 TRUSTED_ROOTS 存放區以及 vmdir (VMware Directory Service)。

```
/usr/lib/vmware-vmca/bin/certool --selfca --config=/usr/lib/vmware-vmca/share/config/certool.cfg
```

用 VMCA 簽署憑證取代機器 SSL 憑證

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

每台機器必須具有機器 SSL 憑證，以便與其他服務進行安全通訊。在增強型連結模式組態中連線多個 vCenter Server 執行個體時，必須在每個節點上執行機器 SSL 憑證產生命令。

必要條件

準備好停止所有服務，並啟動處理憑證傳播和儲存的服務。

程序

1 為每部需要新憑證的機器製作一份 `certool.cfg` 的複本。

您可以在 `/usr/lib/vmware-vmca/share/config/` 目錄中找到 `certool.cfg` 檔案。

2 編輯每台機器的自訂組態檔以包含該機器的 FQDN。

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

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

例如：

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

4 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

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

5 新增憑證到 VECS。

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

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

6 重新啟動所有服務。

```

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

範例： 將機器憑證取代為 VMCA 簽署憑證

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

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

2 為機器 SSL 憑證產生金鑰配對。在增強型連結模式組態中連線的多個 vCenter Server 執行個體的部署中，請在每個 vCenter Server 節點上執行此命令。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=ssl-key.priv --pubkey=ssl-key.pub
```

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

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

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --
config=ssl-config.cfg
```

`new-vmca-ssl.crt` 檔案會在當前目錄中建立。

4 (選用) 列出 VECS 的內容。

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

- vCenter Server 的輸出範例：

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

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

- 在每個 vCenter Server 上，執行下列命令以更新 MACHINE_SSL_CERT 存放區中的機器 SSL 憑證。您必須為每台機器個別更新憑證，因為每台機器的 FQDN 都不相同。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/vecs-cli --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-
vmca-ssl.crt --key ssl-key.priv
```

後續步驟

您也可以取代 ESXi 主機的憑證。請參閱 vSphere 安全性出版物。

用新的 VMCA 簽署憑證取代解決方案使用者憑證

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

許多 VMware 客戶未取代解決方案使用者憑證。僅將機器 SSL 憑證取代為自訂憑證。此一混合式方法可滿足客戶安全性團隊的需求。

- 這些憑證位於 Proxy 後方，或屬於自訂憑證。
- 不使用任何中繼 CA。

可以取代機器解決方案使用者憑證以及每個 vCenter Server 系統上的解決方案使用者憑證。

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

必要條件

準備好停止所有服務，並啟動處理憑證傳播和儲存的服務。

程序

1. 製作一份 `certool.cfg` 的複本，移除名稱、IP 位址、DNS 名稱和電子郵件欄位，然後重新命名該檔案 (例如重新命名為 `sol_usr.cfg`)。

   做為產生過程的一部分，您可以從命令列重新命名憑證。解決方案使用者無需其他資訊。如果保留預設資訊，所產生的憑證可能會造成混淆。

2. 為每個解決方案使用者產生公開/私密金鑰檔案配對和憑證，並於您先前自訂的組態檔中傳遞。

   例如：

   ```
   certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
   certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
   ```

3. 找到每個解決方案使用者的名稱。

   ```
   dir-cli service list
   ```

   您可以使用取代憑證時返回的唯一識別碼。輸入和輸出內容可能如下。

   ```
   dir-cli service list
   Enter password for administrator@vsphere.local:
   1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
   2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
   3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
   4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
   5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
   6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
   ```

在增強型連結模式組態中連線的多個 vCenter Server 執行個體的部署中，`dir-cli service list` 的輸出包括所有節點中的所有解決方案使用者。請執行 `vmafd-cli get-machine-id --server-name localhost` 以找出每台主機的本機機器識別碼。每個解決方案使用者名稱都包含機器識別碼。

4 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

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

5 針對每個解決方案使用者，先後取代 vmdir 和 VECS 中的現有憑證。

下列範例說明如何取代 vpxd 服務的憑證。

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

備註 如果您不取代 vmdir 中的憑證，解決方案使用者就無法向 vCenter Single Sign-On 進行驗證。

6 重新啟動所有服務。

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

範例： 使用 VMCA 簽署解決方案使用者憑證

1 在增強型連結模式組態中，針對每個 vCenter Server 節點上的每個解決方案使用者產生公開/私密金鑰配對。其中包括機器解決方案的配對，以及每個其他解決方案使用者 (vpxd、vpxd-extension、vsphere-webclient、wcp) 的配對。

a 為機器解決方案使用者產生金鑰配對。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b 為每個節點上的 vpxd 解決方案使用者產生金鑰配對。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

c 為每個節點上的 vpxd-extension 解決方案使用者產生金鑰配對。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

d 為每個節點上的 vsphere-webclient 解決方案使用者產生金鑰配對。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

e 為每個節點上的 wcp 解決方案使用者產生金鑰配對。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2 為機器解決方案使用者以及每個 vCenter Server 節點上的每個其他解決方案使用者 (vpxd、vpxd-extension、vsphere-webclient、wcp)，產生由新 VMCA 根憑證簽署的解決方案使用者憑證。

備註 `--Name` 參數必須是唯一的。包含解決方案使用者存放區的名稱，可讓您輕鬆辨識憑證與解決方案使用者之間的對應關係。在每種情況下，範例皆包含名稱，例如 `vpxd` 或 `vpxd-extension`。

a 執行下列命令，為該節點上的機器解決方案使用者產生解決方案使用者憑證。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-key.priv
--Name=machine
```

b 為每個節點上的機器解決方案使用者產生憑證。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-key.priv
--Name=machine
```

c 為每個節點上的 vpxd 解決方案使用者產生憑證。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --
Name=vpxd
```

d 為每個節點上的 vpxd-extensions 解決方案使用者產生憑證。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-
extension-key.priv --Name=vpxd-extension
```

e 執行下列命令，為每個節點上的 vsphere-webclient 解決方案使用者產生憑證。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-
webclient-key.priv --Name=vsphere-webclient
```

f 執行下列命令，為每個節點上的 wcp 解決方案使用者產生憑證。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp
```

3 將 VECS 中的解決方案使用者憑證取代為新的解決方案使用者憑證。

備註 `--store` 和 `--alias` 參數必須與預設服務名稱完全相符。

a 取代每個節點上的機器解決方案使用者憑證：

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert new-
machine-vc.crt --key machine-vc-key.priv
```

b 取代每個節點上的 vpxd 解決方案使用者憑證。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt
--key vpxd-key.priv
```

c 取代每個節點上的 vpxd-extension 解決方案使用者憑證。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-extension
--cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d 取代每個節點上的 vsphere-webclient 解決方案使用者憑證。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias vsphere-
webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias vsphere-
webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e 取代每個節點上的 wcp 解決方案使用者憑證。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-wcp.crt --
key wcp-key.priv
```

4 使用新的解決方案使用者憑證更新 VMware Directory Service (vmdir)。系統會提示您輸入 vCenter Single Sign-On 管理員密碼。

a 執行 `dir-cli service list`，為每個解決方案使用者取得唯一的服務識別碼尾碼。在 vCenter Server 系統上執行此命令。

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

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

b 取代每個 vCenter Server 節點上 vmdir 中的機器憑證。例如，如果 machine-6fd7f140-60a9-11e4-9e28-005056895a69 是 vCenter Server 上的機器解決方案使用者，請執行此命令：

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

c 取代每個節點上 vmdir 中的 vpxd 解決方案使用者憑證。例如，如果 vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 是 vpxd 解決方案使用者識別碼，請執行此命令：

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

d 取代每個節點上 vmdir 中的 vpxd-extension 解決方案使用者憑證。例如，如果 vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 是 vpxd-extension 解決方案使用者識別碼，請執行此命令：

```
/usr/lib/vmware-vmafd/bin/dir-cli update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

e 取代每個節點上的 vsphere-webclient 解決方案使用者憑證。例如，如果 vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 是 vsphere-webclient 解決方案使用者識別碼，請執行此命令：

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

f 取代每個節點上的 wcp 解決方案使用者憑證。例如，如果 wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e 是 wcp 解決方案使用者識別碼，請執行此命令：

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt
```

後續步驟

重新啟動每個 vCenter Server 節點上的所有服務。

使用 VMCA 做為中繼憑證授權機構

您可以將 VMCA 根憑證取代為憑證鏈結中包含 VMCA 的第三方 CA 簽署憑證。然後，VMCA 產生的所有憑證都會包含完整鏈結。您可以將現有憑證取代為新產生的憑證。

如果您使用 VMCA 做為中繼 CA 或使用自訂憑證，可能會遇到非常複雜的問題，且可能對安全性產生負面影響，並且增加不必要的運作風險。如需有關在 vSphere 環境中管理憑證的詳細資訊，請參閱標題為〈新產品逐步解說 - 混合 vSphere SSL 憑證取代〉的部落格文章，網址為：http://vmware.com/go/hybridvmca。

取代根憑證 (中繼 CA)

將 VMCA 憑證取代為自訂憑證的第一個步驟，是產生 CSR 並傳送此 CSR 進行簽署。然後將已簽署的憑證做為根憑證新增至 VMCA。

您可以使用 Certificate Manager 公用程式或其他工具來產生 CSR。CSR 必須符合以下需求：

- 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
- 對於根憑證，CA 延伸必須設為 true，憑證簽署必須位於需求清單中。例如：

```
basicConstraints        = critical,CA:true
keyUsage                = critical,digitalSignature,keyCertSign
```

- 必須啟用 CRL 簽署。
- 增強金鑰使用方法可以為空白或包含伺服器驗證。
- 對憑證鏈結的長度無明確限制。VMCA 預設使用 OpenSSL (為 10 個憑證)。
- 不支援含萬用字元或多個 DNS 名稱的憑證。
- 您無法建立 VMCA 的附屬 CA。

  如需使用 Microsoft 憑證授權機構的範例，請參閱 VMware 知識庫文章：Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x (在 vSphere 6.x 中建立 Microsoft 憑證授權機構範本以建立 SSL 憑證)，網址為 http://kb.vmware.com/kb/2112009。

當您取代根憑證時，VMCA 會驗證下列憑證屬性：

- 金鑰大小：2048 位元 (下限) 至 16384 位元 (上限)
- 金鑰使用方式：憑證簽署
- 基本限制：主體類型 CA

程序

1 產生 CSR 並將其傳送至您的 CA。

  依照 CA 指示進行。

2 準備包含已簽署之 VMCA 憑證以及第三方 CA 或企業 CA 之完整 CA 鏈結的憑證檔案。儲存檔案，例如儲存為 `rootca1.crt`。

  您可以將所有 PEM 格式的 CA 憑證複製到單一檔案，以完成此步驟。您可以從 VMCA 根憑證開始複製，並於根 CA PEM 憑證結束複製。例如：

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

3 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

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

4 取代現有的 VMCA 根 CA。

```
certool --rootca --cert=rootca1.crt --privkey=root1.key
```

當您執行此命令時，會執行下列動作：

- 將新的自訂根憑證新增到檔案系統中的憑證位置。
- 將自訂根憑證附加到 VECS 中的 TRUSTED_ROOTS 存放區 (過一段時間)。
- 將自訂根憑證新增到 vmdir (過一段時間)。

5 (選擇性) 如果要將變更傳播到所有 vmdir (VMware Directory Service) 執行個體，請將新的根憑證發佈到 vmdir，並提供每個檔案的完整檔案路徑。

例如：

```
dir-cli trustedcert publish --cert rootca1.crt
```

vmdir 節點間的複寫每隔 30 秒會進行一次。您不需要明確將根憑證新增到 VECS，因為 VECS 會每隔 5 分鐘輪詢 vmdir 是否有新的根憑證檔案。

6 (選擇性) 如有必要，您可以強制重新整理 VECS。

```
vecs-cli force-refresh
```

7 重新啟動所有服務。

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

範例： 取代根憑證

使用具有 `--rootca` 選項的 `certool` 命令，將 VMCA 根憑證取代為自訂 CA 根憑證。

```
/usr/lib/vmware-vmca/bin/certool --rootca --cert=<path>/root.pem --privkey=<path>/root.key
```

當您執行此命令時，會執行下列動作：

- 將新的自訂根憑證新增到檔案系統中的憑證位置。
- 將自訂根憑證附加到 VECS 中的 TRUSTED_ROOTS 存放區。
- 將自訂根憑證新增到 vmdir。

後續步驟

如果公司原則需要，您可以從憑證存放區移除原始的 VMCA 根憑證。如果您這麼做，必須取代 vCenter Single Sign-On 簽署憑證。請參閱取代 STS 憑證。

取代機器 SSL 憑證 (中繼 CA)

從 CA 收到簽署憑證並將其用做 VMCA 根憑證之後，您可以取代所有機器 SSL 憑證。

這些步驟與取代使用 VMCA 做為憑證授權機構之憑證的步驟基本相同。不過，在此情況下，VMCA 會簽署所有具有完整鏈結的憑證。

每台機器必須具有機器 SSL 憑證，以便與其他服務進行安全通訊。在增強型連結模式組態中連線多個 vCenter Server 執行個體時，必須在每個節點上執行機器 SSL 憑證產生命令。

必要條件

對於每個機器 SSL 憑證，`SubjectAltName` 必須包含 `DNS Name=<Machine FQDN>`。

程序

1 為每部需要新憑證的機器製作一份 `certool.cfg` 的複本。

   您可以在 `/usr/lib/vmware-vmca/share/config/` 目錄中找到 `certool.cfg` 檔案。

2 編輯每台機器的自訂組態檔以包含該機器的 FQDN。

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

3 為每台機器產生公開/私密金鑰檔案配對和憑證，並於您先前自訂的組態檔中傳遞。

   例如：

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --config
machine1.cfg
```

4 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

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

5 新增憑證到 VECS。

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

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

6 重新啟動所有服務。

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

範例：取代機器 SSL 憑證 (VMCA 為中繼 CA)

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

```
Country = US
Name = vmca-<FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

2 為機器 SSL 憑證產生金鑰配對。在增強型連結模式組態中連線的多個 vCenter Server 執行個體的部署中，請在每個 vCenter Server 節點上執行此命令。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=ssl-key.priv --pubkey=ssl-key.pub
```

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

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

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --
config=ssl-config.cfg
```

`new-vmca-ssl.crt` 檔案會在當前目錄中建立。

4 (選用) 列出 VECS 的內容。

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

- vCenter Server 的輸出範例：

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

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

- 在每個 vCenter Server 上，執行下列命令以更新 MACHINE_SSL_CERT 存放區中的機器 SSL 憑證。您必須為每台機器個別更新憑證，因為每台機器的 FQDN 都不相同。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/vecs-cli --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-
vmca-ssl.crt --key ssl-key.priv
```

取代解決方案使用者憑證 (中繼 CA)

取代機器 SSL 憑證後，您可以取代解決方案使用者憑證。

許多 VMware 客戶未取代解決方案使用者憑證。僅將機器 SSL 憑證取代為自訂憑證。此一混合式方法可滿足客戶安全性團隊的需求。

- 這些憑證位於 Proxy 後方，或屬於自訂憑證。
- 不使用任何中繼 CA。

可以取代機器解決方案使用者憑證以及每個 vCenter Server 系統上的解決方案使用者憑證。

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

必要條件

每個解決方案使用者憑證必須具有不同的 `Subject`。例如，您可以考慮加入解決方案使用者名稱 (例如 vpxd) 或其他唯一識別碼。

程序

1 製作一份 `certool.cfg` 的複本，移除名稱、IP 位址、DNS 名稱和電子郵件欄位，然後重新命名該檔案 (例如重新命名為 `sol_usr.cfg`)。

做為產生過程的一部分，您可以從命令列重新命名憑證。解決方案使用者無需其他資訊。如果保留預設資訊，所產生的憑證可能會造成混淆。

2 為每個解決方案使用者產生公開/私密金鑰檔案配對和憑證，並於您先前自訂的組態檔中傳遞。

例如：

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3 找到每個解決方案使用者的名稱。

```
dir-cli service list
```

您可以使用取代憑證時返回的唯一識別碼。輸入和輸出內容可能如下。

```
dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

在增強型連結模式組態中連線的多個 vCenter Server 執行個體的部署中，`dir-cli service list` 的輸出包括所有節點中的所有解決方案使用者。請執行 `vmafd-cli get-machine-id --server-name localhost` 以找出每台主機的本機機器識別碼。每個解決方案使用者名稱都包含機器識別碼。

4 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

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

5 先後取代 vmdir 和 VECS 中的現有憑證。

對於解決方案使用者，您必須以此順序新增憑證。例如：

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

備註 如果您不取代 vmdir 中的憑證，解決方案使用者就無法登入 vCenter Single Sign-On。

6 重新啟動所有服務。

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

範例： 取代解決方案使用者憑證 (中繼 CA)

1 在增強型連結模式組態中，針對每個 vCenter Server 節點上的每個解決方案使用者產生公開/私密金鑰配對。其中包括機器解決方案的配對，以及每個其他解決方案使用者 (vpxd、vpxd-extension、vsphere-webclient、wcp) 的配對。

a 為機器解決方案使用者產生金鑰配對。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b 為每個節點上的 vpxd 解決方案使用者產生金鑰配對。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

c 為每個節點上的 vpxd-extension 解決方案使用者產生金鑰配對。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

d 為每個節點上的 vsphere-webclient 解決方案使用者產生金鑰配對。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

e 為每個節點上的 wcp 解決方案使用者產生金鑰配對。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2 為機器解決方案使用者以及每個 vCenter Server 節點上的每個其他解決方案使用者 (vpxd、vpxd-extension、vsphere-webclient、wcp)，產生由新 VMCA 根憑證簽署的解決方案使用者憑證。

備註 `--Name` 參數必須是唯一的。包含解決方案使用者存放區的名稱，可讓您輕鬆辨識憑證與解決方案使用者之間的對應關係。在每種情況下，範例皆包含名稱，例如 `vpxd` 或 `vpxd-extension`。

a 執行下列命令，為該節點上的機器解決方案使用者產生解決方案使用者憑證。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

b 為每個節點上的機器解決方案使用者產生憑證。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

c 為每個節點上的 vpxd 解決方案使用者產生憑證。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd
```

d 為每個節點上的 vpxd-extensions 解決方案使用者產生憑證。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension
```

e 執行下列命令，為每個節點上的 vsphere-webclient 解決方案使用者產生憑證。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient
```

f 執行下列命令，為每個節點上的 wcp 解決方案使用者產生憑證。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --Name=wcp
```

3 將 VECS 中的解決方案使用者憑證取代為新的解決方案使用者憑證。

備註 `--store` 和 `--alias` 參數必須與預設服務名稱完全相符。

a 取代每個節點上的機器解決方案使用者憑證：

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert new-
machine-vc.crt --key machine-vc-key.priv
```

b 取代每個節點上的 vpxd 解決方案使用者憑證。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt
--key vpxd-key.priv
```

c 取代每個節點上的 vpxd-extension 解決方案使用者憑證。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-extension
--cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d 取代每個節點上的 vsphere-webclient 解決方案使用者憑證。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias vsphere-
webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias vsphere-
webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e 取代每個節點上的 wcp 解決方案使用者憑證。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-wcp.crt --
key wcp-key.priv
```

4 使用新的解決方案使用者憑證更新 VMware Directory Service (vmdir)。系統會提示您輸入 vCenter Single Sign-On 管理員密碼。

a 執行 `dir-cli service list`，為每個解決方案使用者取得唯一的服務識別碼尾碼。在 vCenter Server 系統上執行此命令。

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
```

```
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

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

b 取代每個 vCenter Server 節點上 vmdir 中的機器憑證。例如，如果 machine-6fd7f140-60a9-11e4-9e28-005056895a69 是 vCenter Server 上的機器解決方案使用者，請執行此命令：

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

c 取代每個節點上 vmdir 中的 vpxd 解決方案使用者憑證。例如，如果 vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 是 vpxd 解決方案使用者識別碼，請執行此命令：

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

d 取代每個節點上 vmdir 中的 vpxd-extension 解決方案使用者憑證。例如，如果 vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 是 vpxd-extension 解決方案使用者識別碼，請執行此命令：

```
/usr/lib/vmware-vmafd/bin/dir-cli update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

e 取代每個節點上的 vsphere-webclient 解決方案使用者憑證。例如，如果 vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 是 vsphere-webclient 解決方案使用者識別碼，請執行此命令：

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

f 取代每個節點上的 wcp 解決方案使用者憑證。例如，如果 wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e 是 wcp 解決方案使用者識別碼，請執行此命令：

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt
```

將自訂憑證與 vSphere 搭配使用

如果公司原則需要，您可以將部分或全部 vSphere 中所使用的憑證取代為由第三方或企業 CA 簽署的憑證。如果執行該作業，則 VMCA 將不會在您的憑證鏈結中。您負責將所有 vCenter 憑證儲存到 VECS 中。

您可以取代所有憑證，或使用混合解決方案。例如，考量取代所有用於網路流量的憑證，但保留 VMCA 簽署解決方案使用者憑證。解決方案使用者憑證僅用於向 vCenter Single Sign-On 進行驗證。vCenter Server 僅將解決方案使用者憑證用於內部通訊。不會將解決方案使用者憑證用於外部通訊。

備註 如果您不希望使用 VMCA，就需要自行負責取代所有憑證、使用憑證佈建新的元件，以及追蹤憑證到期。

即使您決定使用自訂憑證，仍可以使用 VMware Certificate Manager 公用程式進行憑證取代。請參閱用自訂憑證取代所有憑證 (Certificate Manager)。

如果您在取代憑證後使用 vSphere 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。

要求憑證及匯入自訂根憑證

您可以使用來自企業或第三方 CA 的自訂憑證。第一步，從憑證授權機構要求憑證並將根憑證匯入到 VMware Endpoint 憑證存放區 (VECS) 中。

必要條件

憑證必須符合以下需求：

- 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、不可否認性、金鑰編密
- 某天的開始時間早於目前時間。
- CN (和 SubjectAltName) 設為 ESXi 主機在 vCenter Server 詳細目錄中所擁有的主機名稱 (或 IP 位址)。

程序

1. 將下列憑證的憑證簽署要求 (CSR) 傳送給您的企業或第三方憑證提供者。
   - 每台機器有一個機器 SSL 憑證。對於機器 SSL 憑證，SubjectAltName 欄位必須包含完整網域名稱 (DNS NAME=*machine_FQDN*)。
   - 或者，每個節點有五個解決方案使用者憑證。解決方案使用者憑證不需包含 IP 位址、主機名稱或電子郵件地址。每個憑證必須具有不同的憑證主體。

   一般來說，會為信任鏈結產生 PEM 檔案，並為每個 vCenter Server 節點產生已簽署的 SSL 憑證。

2 列出 TRUSTED_ROOTS 和機器 SSL 存放區。

```
vecs-cli store list
```

a 確認目前的根憑證和所有機器 SSL 憑證都經 VMCA 簽署。

b 記下序號、簽發者以及主體 CN 欄位。

c (選擇性) 使用網頁瀏覽器開啟將取代憑證之節點的 HTTPS 連線，檢查憑證資訊並確認其與機器 SSL 憑證相符。

3 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

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

4 發佈自訂根憑證。

```
dir-cli trustedcert publish --cert <my_custom_root>
```

如果您未在命令列上指定使用者名稱和密碼，系統會提示您指定。

5 重新啟動所有服務。

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

後續步驟

如果公司原則需要，您可以從憑證存放區移除原始的 VMCA 根憑證。如果您這麼做，必須重新整理 vCenter Single Sign-On 憑證。請參閱取代 STS 憑證。

將機器 SSL 憑證取代為自訂憑證

收到自訂憑證後，您可以取代每個機器憑證。

在開始取代憑證之前，您必須準備好下列資訊：

- administrator@vsphere.local 的密碼
- 有效的機器 SSL 自訂憑證 (`.crt` 檔案)
- 有效的機器 SSL 自訂金鑰 (`.key` 檔案)
- 有效的自訂根憑證 (`.crt` 檔案)

必要條件

您一定已收到第三方或企業 CA 核發給每台機器的憑證。

- 金鑰大小：2048 位元 (下限) 至 16384 位元 (上限) (PEM 編碼)
- CRT 格式

- x509 第 3 版
- SubjectAltName 必須包含 DNS Name=<machine_FQDN>。
- 包含下列金鑰使用方法：數位簽章、不可否認性、金鑰編密

程序

1 停止所有服務，並啟動處理憑證建立、傳播和儲存的服務。

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

2 登入每個節點，並將從 CA 收到的新機器憑證新增到 VECS 中。

所有機器都需要使用本機憑證存放區中的新憑證，以透過 SSL 進行通訊。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-path>
--key <key-file-path>
```

3 重新啟動所有服務。

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

範例： 將機器 SSL 憑證取代為自訂憑證

此範例顯示如何使用自訂憑證取代機器 SSL 憑證。您可以在每個節點上以相同方式取代機器 SSL 憑證。

1 首先，刪除 VECS 中的現有憑證。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
```

2 接著，新增替代憑證。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --
cert /tmp/custom-certs/ms-ca/signed-ssl/custom-w1-vim-cat-dhcp-094.eng.vmware.com.crt --key /tmp/
custom-certs/ms-ca/signed-ssl/custom-x3-vim-cat-dhcp-1128.vmware.com.priv
```

使用 CLI 命令管理服務和憑證

3

您可以使用一組 CLI 來管理 VMCA (VMware Certificate Authority)、VECS (VMware Endpoint 憑證存放區)、VMware Directory Service (vmdir) 和安全性 Token 服務憑證 (STS)。vSphere Certificate Manager 公用程式也支援多項相關工作，但手動憑證管理和管理其他服務需要使用 CLI。

通常使用 SSH 連線至應用裝置 Shell，來存取 CLI 工具以管理憑證和相關聯的服務。如需詳細資訊，請參閱 VMware 知識庫文章，網址為 http://kb.vmware.com/kb/2100508。

手動憑證取代提供使用 CLI 命令取代憑證的範例。

表 3-1. 用於管理憑證和相關聯服務的 CLI 工具

CLI	說明	請參閱
`certool`	產生與管理憑證及金鑰。VMware Certificate Management 服務是 VMCAD 的一部分。	certool 初始化命令參考
`vecs-cli`	管理 VMware 憑證存放區執行個體的內容。屬於 VMware Authentication Framework 精靈 (VMAFD) 的一部分。	vecs-cli 命令參考
`dir-cli`	建立與更新 VMware Directory Service 中的憑證。屬於 VMAFD 的一部分。	dir-cli 命令參考
`sso-config`	管理 STS 憑證。	命令列說明。
`service-control`	啟動或停止服務，例如做為憑證取代工作流程的一部分。	在執行其他 CLI 命令之前，請執行此命令來停止服務。

CLI 位置

依預設，您可以在下列位置找到 CLI。

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin/sso-config.sh
```

備註 `service-control` 命令不需要您指定路徑。

本章節討論下列主題：

執行 CLI 所需的權限

所需的權限將視您所使用的 CLI 及您所想要執行之命令上的 CLI 而定。例如，對於大多數憑證管理作業，您必須為本機 vCenter Single Sign-on 網域 (依預設為 vsphere.local) 指派管理員。某些命令可用於所有使用者。

dir-cli

您必須是本機網域 (依預設為 vsphere.local) 中管理員群組的成員，方可執行 `dir-cli` 命令。如果沒有指定使用者名稱和密碼，則會提示您輸入本機 vCenter Single Sign-on 網域的管理員密碼，預設密碼為 administrator@vsphere.local。

vecs-cli

最初，僅擁有總括存取權限的儲存區擁有者和使用者可存取儲存區。管理員群組中的使用者擁有總括存取權。

MACHINE_SSL_CERT 和 TRUSTED_ROOTS 存放區是特殊存放區。只有根使用者或管理員使用者 (視安裝類型而定) 具有完整的存取權。

certool

大多數的 `certool` 命令都是只有管理員群組中的使用者才能使用。所有使用者都可以執行下列命令。

- `genselfcacert`
- `initscr`
- `getdc`
- `waitVMDIR`
- `waitVMCA`
- `genkey`
- `viewcert`

變更 certool 組態選項

執行 `certool --gencert` 或某些其他憑證初始化或管理命令時，命令會從組態檔讀取所有值。您可以編輯現有檔案、使用 `--config=<file name>`選項覆寫預設組態檔，或覆寫命令列上的值。

依預設，組態檔 `certool.cfg` 位於 `/usr/lib/vmware-vmca/share/config/` 目錄中。

該檔案中有數個欄位，預設值如下：

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

您可以變更這些值，方法是按如下方式在命令列上指定修改的檔案，或在命令列上覆寫個別值。

- 建立組態檔的複本並編輯檔案。使用 `--config` 命令列選項指定檔案。請指定完整路徑，以避免路徑名稱問題。
- ```
  /usr/lib/vmware-vmca/bin/certool --gencert --config /tmp/myconfig.cfg
  ```
- 在命令列上覆寫個別值。例如，如果要覆寫位置，請執行此命令：

  ```
  /usr/lib/vmware-vmca/bin/certool --gencert --privkey=private.key --Locality="Mountain View"
  ```

指定 `--Name` 以取代憑證主體名稱的 CN 欄位。

- 對於解決方案使用者憑證，慣例上名稱會是 <sol_user name>@<domain>，但如果您環境中採用的慣例有所不同，可以變更名稱。
- 對於機器 SSL 憑證，會使用機器的 FQDN。

  VMCA 僅允許使用一個 DNSName (在 `Hostname` 欄位中) 且不得使用其他別名。如果 IP 位址是由使用者指定，也會儲存在 SubAltName 中。

使用 `--Hostname` 參數指定憑證的 SubAltName 的 DNSName。

certool 初始化命令參考

`certool` 初始化命令可讓您產生憑證簽署要求、檢視和產生由 VMCA 簽署的憑證和金鑰、匯入根憑證以及執行其他憑證管理作業。

在許多情況下，您將組態檔傳遞到 `certool` 命令。請參閱變更 certool 組態選項。如需使用量範例，請參閱用新的 VMCA 簽署憑證取代現有的 VMCA 簽署憑證。命令列說明提供選項的詳細資料。

certool --initcsr

產生憑證簽署要求 (CSR)。該命令產生 PKCS10 檔案和私密金鑰。
  ```

選項	說明
--gencsr	產生 CSR 時需要。
--privkey <key_file>	私密金鑰檔案的名稱。
--pubkey <key_file>	公開金鑰檔案的名稱。
--csrfile <csr_file>	要傳送到 CA 提供者的 CSR 檔案的檔案名稱。
--config <config_file>	組態檔的選用名稱。預設值為 certool.cfg。

範例：

```
certool --gencsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

certool --selfca

建立自我簽署的憑證並使用自我簽署的根 CA 佈建 VMCA 伺服器。使用此選項為佈建 VMCA 伺服器最簡單的方式之一。您可以改為使用第三方根憑證佈建 VMCA 伺服器，以讓 VMCA 成為中繼 CA。請參閱使用 VMCA 做為中繼憑證授權機構。

此命令會提早 3 天產生憑證，以避免時區衝突。

選項	說明
--selfca	產生自我簽署的憑證時需要。
--predate <number_of_minutes>	可讓您將根憑證的 [有效起始時間] 欄位設定為目前時間之前的指定分鐘數。此選項可協助對潛在時區問題進行說明。上限為 3 天。
--config <config_file>	組態檔的選用名稱。預設值為 certool.cfg。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

範例：

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280  --selfca --server= 192.0.2.24 --
srp-upn=administrator@vsphere.local
```

certool --rootca

匯入根憑證。將指定憑證和私密金鑰新增到 VMCA。VMCA 一律使用最新根憑證進行簽署，但是其他根憑證在您將其手動刪除之前仍受信任。這意味著，您可以一次執行一個步驟來更新基礎結構，最後才刪除不再使用的憑證。

選項	說明
--rootca	匯入根 CA 時需要。
--cert <certfile>	憑證檔案的名稱。
--privkey <key_file>	私密金鑰檔案的名稱。此檔案必須為 PEM 編碼格式。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

範例：

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

certool --getdc

傳回由 vmdir 使用的預設網域名稱。

選項	說明
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。
--port <port_num>	選用的連接埠號碼。預設值為連接埠 389。

範例：

```
certool --getdc
```

certool --waitVMDIR

請等待，直到 VMware Directory Service 正在執行或--wait 指定的逾時結束為止。搭配使用此選項和其他選項可排程某些工作，例如傳回預設網域名稱。

選項	說明
--wait	要等待的選用分鐘數。預設值為 3。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。
--port <port_num>	選用的連接埠號碼。預設值為連接埠 389。

範例：

```
certool --waitVMDIR --wait 5
```

certool --waitVMCA

請等待，直到 VMCA 服務正在執行或指定的逾時結束為止。搭配使用此選項和其他選項可排程某些工作，例如產生憑證。

選項	說明
--wait	要等待的選用分鐘數。預設值為 3。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。
--port <port_num>	選用的連接埠號碼。預設值為連接埠 389。

範例：

```
certool --waitVMCA --selfca
```

certool --publish-roots

強制更新根憑證。此命令需要管理權限。

選項	說明
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

範例：

```
certool --publish-roots
```

certool 管理命令參考

certool 管理命令可讓您檢視、產生與撤銷憑證，以及檢視有關憑證的資訊。

certool --genkey

產生私密和公開金鑰配對。然後，可使用這些檔案產生 VMCA 簽署的憑證。

選項	說明
--genkey	產生私密和公開金鑰時所需的選項。
--privkey <keyfile>	私密金鑰檔案的名稱。
--pubkey <keyfile>	公開金鑰檔案的名稱。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

範例：

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

certool --gencert

從 VMCA 伺服器產生憑證。此命令會使用 certool.cfg 或指定組態檔中的資訊。您可以使用憑證來佈建機器憑證或解決方案使用者憑證。

選項	說明
--gencert	產生憑證時所需的選項。
--cert <certfile>	憑證檔案的名稱。此檔案必須為 PEM 編碼格式。
--privkey <keyfile>	私密金鑰檔案的名稱。此檔案必須為 PEM 編碼格式。
--config <config_file>	組態檔的選用名稱。預設值為 certool.cfg。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

範例：

```
certool --gencert --privkey=<filename> --cert=<filename>
```

certool --getrootca

以人類可讀的形式列印目前的根 CA 憑證。此輸出不可做為憑證使用，而會變更為人類可讀的內容。

選項	說明
`--getrootca`	列印根憑證時所需的選項。
`--server <server>`	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

範例：

```
certool --getrootca --server=remoteserver
```

certool --viewcert

以人類可讀的形式列印憑證中的所有欄位。

選項	說明
`--viewcert`	檢視憑證時所需的選項。
`--cert <certfile>`	組態檔的選用名稱。預設值為 `certool.cfg`。

範例：

```
 certool --viewcert --cert=<filename>
```

certool --enumcert

列出 VMCA 伺服器知曉的所有憑證。必要的 `filter` 選項可讓您列出所有憑證或僅列出撤銷的、作用中或到期的憑證。

選項	說明
`--enumcert`	列出所有憑證時所需的選項。
`--filter [all | active]`	必要篩選器。指定所有或作用中的選項。目前不支援已撤銷和到期的選項。

範例：

```
certool --enumcert --filter=active
```

certool --status

將指定憑證傳送給 VMCA 伺服器，以檢查哪些憑證已撤銷。如果憑證已撤銷，則列印「憑證：已撤銷」，否則，列印「憑證：使用中」。

選項	說明
--status	檢查憑證狀態時所需的選項。
--cert <certfile>	組態檔的選用名稱。預設值為 certool.cfg。
--server <server>	VMCA 伺服器的選用名稱。依預設，命令使用 localhost。

範例：

```
certool --status --cert=<filename>
```

certool --genselfcacert

根據組態檔中的值，產生自我簽署的憑證。此命令會提早 3 天產生憑證，以避免時區衝突。

選項	說明
--genselfcacert	產生自我簽署的憑證時需要。
--outcert <cert_file>	憑證檔案的名稱。此檔案必須為 PEM 編碼格式。
--outprivkey <key_file>	私密金鑰檔案的名稱。此檔案必須為 PEM 編碼格式。
--config <config_file>	組態檔的選用名稱。預設值為 certool.cfg。

範例：

```
certool --genselfcert --privkey=<filename> --cert=<filename>
```

vecs-cli 命令參考

vecs-cli 命令集可讓您管理 VMware 憑證存放區 (VECS) 的執行個體。將這些命令與 dir-cli 和 certool 搭配使用，以管理您的憑證基礎結構和驗證服務。

vecs-cli store create

建立憑證存放區。

選項	說明
--name <name>	憑證存放區的名稱。
--server <server-name>	用於指定伺服器名稱 (如果您連線至遠端 VECS 執行個體)。
--upn <user-name>	用於登入--server <server-name> 指定之伺服器執行個體的使用者主體名稱。建立存放區時，會在目前使用者內容中建立。因此，存放區的擁有者是目前使用者內容，而不總是根使用者。

範例：

```
vecs-cli store create --name <store>
```

vecs-cli store delete

刪除憑證存放區。您無法刪除 MACHINE_SSL_CERT、TRUSTED_ROOTS 和 TRUSTED_ROOT_CRLS 系統存放區。具有所需權限的使用者可以刪除解決方案使用者存放區。

選項	說明
`--name <name>`	要刪除的憑證存放區的名稱。
`--server <server-name>`	用於指定伺服器名稱 (如果您連線至遠端 VECS 執行個體)。
`--upn <user-name>`	用於登入`--server <server-name>` 指定之伺服器執行個體的使用者主體名稱。建立存放區時，會在目前使用者內容中建立。因此，存放區的擁有者是目前使用者內容，而不總是根使用者。

範例：

```
vecs-cli store delete --name <store>
```

vecs-cli store list

列出憑證存放區。

選項	說明
`--server <server-name>`	用於指定伺服器名稱 (如果您連線至遠端 VECS 執行個體)。
`--upn <user-name>`	用於登入`--server <server-name>` 指定之伺服器執行個體的使用者主體名稱。建立存放區時，會在目前使用者內容中建立。因此，存放區的擁有者是目前使用者內容，而不總是根使用者。

VECS 包含下列存放區。

表 3-2. VECS 中的存放區

存放區	說明
機器的 SSL 存放區 (MACHINE_SSL_CERT)	■ 由每個 vSphere 節點上反向 Proxy 服務所使用。 ■ 由每個 vCenter Server 節點上 VMware Directory Service (vmdir) 所使用。 vSphere 6.0 及更新版本中的所有服務都會透過使用機器 SSL 憑證的反向 Proxy 進行通訊。為確保回溯相容性，5.x 服務仍會使用特定的連接埠。因此，部分服務 (例如 vpxd) 仍會將自己的連接埠維持開啟。
解決方案使用者存放區 ■ machine ■ vpxd ■ vpxd-extension ■ vsphere-webclient ■ wcp	對於每個解決方案使用者，VECS 包含一個存放區。每個解決方案使用者憑證的主旨必須是唯一的，例如，機器憑證不能與 vpxd 憑證的主旨相同。 解決方案使用者憑證用於透過 vCenter Single Sign-On 進行驗證。vCenter Single Sign-On 會檢查憑證是否有效，但不會檢查其他憑證屬性。 VECS 中包括下列解決方案使用者憑證存放區： ■ machine：由 License Server 及記錄服務所使用。 **備註** 機器解決方案使用者憑證與機器的 SSL 憑證毫無關聯。機器解決方案使用者憑證用於進行 SAML Token 交換。機器的 SSL 憑證用於對機器進行安全 SSL 連線。 ■ vpxd：vCenter 服務精靈 (vpxd) 存放區。vpxd 會使用儲存在此存放區中的解決方案使用者憑證來驗證 vCenter Single Sign-On。 ■ vpxd-extension：vCenter 延伸存放區。包含 Auto Deploy 服務、Inventory Service 及不屬於其他解決方案使用者的其他服務。 ■ vsphere-webclient：vSphere Client 存放區。還包括一些其他服務，例如效能圖服務。 ■ wcp：VMware vSphere® with VMware Tanzu™ 存放區。 每個 vCenter Server 節點均包含一個 machine 憑證。
受信任的根存放區 (TRUSTED_ROOTS)	包含所有受信任的根憑證。
vSphere Certificate Manager 公用程式備份存放區 (BACKUP_STORE)	由 VMCA (VMware Certificate Manager) 用於支援憑證還原。只有最新狀態會儲存為備份，您無法還原一個以上的步驟。
其他存放區	其他存放區可能由解決方案新增。例如，Virtual Volumes 解決方案將新增一個 SMS 存放區。除非 VMware 說明文件或 VMware 知識庫文章指示您修改這些存放區中的憑證，否則請勿這麼做。 **備註** 刪除 TRUSTED_ROOTS_CRLS 存放區會損壞您的憑證基礎結構。請勿刪除或修改 TRUSTED_ROOTS_CRLS 存放區。

範例：

```
vecs-cli store list
```

vecs-cli store permissions

授與或撤銷存放區權限。使用 --grant 或 --revoke 選項。

存放區的擁有者可以執行所有作業，包括授與和撤銷權限。本機 vCenter Single Sign-On 網域的管理員，預設為 administrator@vsphere.local，具備所有存放區上的所有權限，包括授與和撤銷權限。

您可以使用 `vecs-cli get-permissions --name <store-name>`擷取存放區的目前設定。

選項	說明
`--name <name>`	憑證存放區的名稱。
`--user <username>`	為其授與權限的使用者的唯一名稱。
`--grant [read|write]`	授與讀取或寫入權限。
`--revoke [read|write]`	撤銷讀取或寫入權限。目前不支援。

vecs-cli store get-permissions

擷取存放區目前的權限設定。

選項	說明
`--name <name>`	憑證存放區的名稱。
`--server <server-name>`	用於指定伺服器名稱 (如果您連線至遠端 VECS 執行個體)。
`--upn <user-name>`	用於登入`--server <server-name>` 指定之伺服器執行個體的使用者主體名稱。建立存放區時，會在目前使用者內容中建立。因此，存放區的擁有者是目前使用者內容，而不總是根使用者。

vecs-cli entry create

在 VECS 中建立一個項目。使用此命令新增私密金鑰或憑證到存放區。

備註 請勿使用此命令將根憑證新增至 TRUSTED_ROOTS 存放區。請改為使用 `dir-cli` 命令發佈根憑證。

選項	說明
`--store <NameOfStore>`	憑證存放區的名稱。
`--alias <Alias>`	憑證的選用別名。受信任的根存放區將忽略此選項。
`--cert <certificate_file_path>`	憑證檔案的完整路徑。
`--key <key-file-path>`	對應於憑證之金鑰的完整路徑。 選擇性。
`--password <password>`	用於加密私密金鑰的選擇性密碼。
`--server <server-name>`	用於指定伺服器名稱 (如果您連線至遠端 VECS 執行個體)。
`--upn <user-name>`	用於登入`--server <server-name>` 指定之伺服器執行個體的使用者主體名稱。建立存放區時，會在目前使用者內容中建立。因此，存放區的擁有者是目前使用者內容，而不總是根使用者。

vecs-cli entry list

列出指定存放區中的所有項目。

選項	說明
--store <NameOfStore>	憑證存放區的名稱。

vecs-cli entry getcert

從 VECS 擷取憑證。您可以將憑證傳送到輸出檔案，或將其顯示為人類可讀的文字。

選項	說明
--store <NameOfStore>	憑證存放區的名稱。
--alias <Alias>	憑證的別名。
--output <output_file_path>	要將憑證寫入的檔案。
--text	顯示人類可讀的憑證版本。
--server <server-name>	用於指定伺服器名稱 (如果您連線至遠端 VECS 執行個體)。
--upn <user-name>	用於登入--server <server-name> 指定之伺服器執行個體的使用者主體名稱。建立存放區時，會在目前使用者內容中建立。因此，存放區的擁有者是目前使用者內容，而不總是根使用者。

vecs-cli entry getkey

擷取儲存在 VECS 中的金鑰。您可以將金鑰傳送到輸出檔案，或將其顯示為人類可讀的文字。

選項	說明
--store <NameOfStore>	憑證存放區的名稱。
--alias <Alias>	金鑰的別名。
--output <output_file_path>	要將金鑰寫入的輸出檔案。
--text	顯示人類可讀的金鑰版本。
--server <server-name>	用於指定伺服器名稱 (如果您連線至遠端 VECS 執行個體)。
--upn <user-name>	用於登入--server <server-name> 指定之伺服器執行個體的使用者主體名稱。建立存放區時，會在目前使用者內容中建立。因此，存放區的擁有者是目前使用者內容，而不總是根使用者。

vecs-cli entry delete

刪除憑證存放區中的項目。如果您刪除 VECS 中的項目，則會將其從 VECS 永久移除。唯一的例外是目前的根憑證。VECS 會輪詢 vmdir 是否有根憑證。

選項	說明
--store <NameOfStore>	憑證存放區的名稱。
--alias <Alias>	您想要刪除之項目的別名。
--server <server-name>	用於指定伺服器名稱 (如果您連線至遠端 VECS 執行個體)。

選項	說明
--upn <user-name>	用於登入--server <server-name> 指定之伺服器執行個體的使用者主體名稱。建立存放區時，會在目前使用者內容中建立。因此，存放區的擁有者是目前使用者內容，而不總是根使用者。
-y	隱藏確認提示。僅適用進階使用者。

vecs-cli force-refresh

強制重新整理 VECS。依預設，VECS 會每隔 5 分隔輪詢 vmdir 是否有新根憑證檔案。使用此命令可從 vmdir 立即更新 VECS。

選項	說明
--server <server-name>	用於指定伺服器名稱 (如果您連線至遠端 VECS 執行個體)。
--upn <user-name>	用於登入--server <server-name> 指定之伺服器執行個體的使用者主體名稱。建立存放區時，會在目前使用者內容中建立。因此，存放區的擁有者是目前使用者內容，而不總是根使用者。

dir-cli 命令參考

dir-cli 公用程式支援建立和更新解決方案使用者，帳戶管理，以及管理 VMware Directory Service (vmdir) 中的憑證和密碼。您可以使用 dir-cli 管理和查詢 vCenter Server 執行個體的網域功能層級。

dir-cli nodes list

列出所有在增強型連結模式下連線的 vCenter Server 系統。

選項	說明
--login <admin_user_id>	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
--password <admin_password>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。
--server <psc_ip_or_fqdn>	使用此選項可連線至其他 vCenter Server，以查看其複寫合作夥伴。

dir-cli computer password-reset

可讓您重設網域中機器帳戶的密碼。

選項	說明
--login <admin_user_id>	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
--password <admin_password>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。
--live-dc-hostname <server name>	vCenter Server 執行個體的目前名稱。

dir-cli service create

建立解決方案使用者。主要供第三方解決方案使用。

選項	說明
`--name <name>`	要建立的解決方案使用者的名稱。
`--cert <cert file>`	憑證檔案的路徑。可以是 VMCA 簽署的憑證或第三方憑證。
`--ssogroups <comma-separated-groupnames>`	將解決方案使用者設為指定群組的成員。
`--wstrustrole <ActAsUser>`	將解決方案使用者設為內建系統管理員或使用者群組的成員。換句話說，決定解決方案使用者是否具有管理權限。
`--ssoadminrole <Administrator/User>`	將解決方案使用者設為 ActAsUser 群組的成員。ActAsUser 角色可讓某些使用者代表其他使用者執行作業。
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli service list

列出 `dir-cli` 知道的解決方案使用者。

選項	說明
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli service delete

刪除 vmdir 中的解決方案使用者。刪除解決方案使用者時，使用這個 vmdir 執行個體的所有管理節點都無法使用所有相關聯的服務。

選項	說明
`--name`	要刪除的解決方案使用者的名稱。
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli service update

更新指定解決方案使用者 (即服務集合) 的憑證。執行此命令後，VECS 會在 5 分鐘後提取變更，您也可以使用 `vecs-cli force-refresh` 強制執行重新整理。

選項	說明
`--name <name>`	要更新的解決方案使用者的名稱。
`--cert <cert_file>`	要指派給服務的憑證的名稱。

選項	說明
--login <admin_user_id>	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
--password <admin_password>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli user create

在 vmdir 內建立一般使用者。此命令可用於透過使用者名稱和密碼向 vCenter Single Sign-On 進行驗證的個人使用者。僅在原型設計期間使用此命令。

選項	說明
--account <name>	要建立的 vCenter Single Sign-On 使用者的名稱。
--user-password <password>	使用者的初始密碼。
--first-name <name>	使用者的名字。
--last-name <name>	使用者的姓氏。
--login <admin_user_id>	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
--password <admin_password>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli user modify

刪除 vmdir 內的指定使用者。

選項	說明
--account <name>	要刪除的 vCenter Single Sign-On 使用者的名稱。
--password-never-expires	如果您要針對必須向 vCenter Server 進行驗證的自動工作建立使用者帳戶，並且想要確保工作在密碼到期時不停止執行，請將此選項設定為 true。 請謹慎使用此選項。
--password-expires	如果想要還原 --password-never-expires 選項，請將此選項設定為 true。
--login <admin_user_id>	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
--password <admin_password>	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli user delete

刪除 vmdir 內的指定使用者。

選項	說明
`--account <name>`	要刪除的 vCenter Single Sign-On 使用者的名稱。
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli user find-by-name

在 vmdir 內依名稱尋找使用者。此命令傳回的資訊取決於您在 `--level` 選項中指定的內容。

選項	說明
`--account <name>`	要刪除的 vCenter Single Sign-On 使用者的名稱。
`--level <info level 0|1|2>`	傳回以下資訊： ■ 層級 0 - 帳戶和 UPN ■ 層級 1 - 層級 0 資訊 + 名字和姓氏 ■ 層級 2：層級 0 + 帳戶已停用旗標、帳戶已鎖定旗標、密碼永遠不會到期旗標、密碼已到期旗標和密碼到期旗標。 預設層級為 0。
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli group modify

將使用者或群組新增至現有的群組。

選項	說明
`--name <name>`	vmdir 中群組的名稱。
`--add <user_or_group_name>`	要新增的使用者或群組的名稱。
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli group list

列出指定的 vmdir 群組。

選項	說明
`--name <name>`	vmdir 中群組的選擇性名稱。此選項可讓您檢查特定群組是否存在。
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli ssogroup create

在本機網域 (依預設為 vsphere.local) 內建立群組。

如果想要建立群組以管理 vCenter Single Sign-On 網域的使用者權限，請使用此命令。例如，如果您建立某群組並隨後將該群組新增到 vCenter Single Sign-On 網域的管理員群組，則新增到該群組的所有使用者都具有該網域的管理員權限。

也可以將 vCenter 詳細目錄物件的權限授與 vCenter Single Sign-On 網域中的群組。請參閱 vSphere 安全性說明文件。

選項	說明
`--name <name>`	vmdir 中群組的名稱。長度上限為 487 個字元。
`--description <description>`	群組的選擇性說明。
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli trustedcert publish

將信任的根憑證發佈到 vmdir。

選項	說明
`--cert <file>`	憑證檔案的路徑。
`--crl <file>`	VMCA 不支援此選項。
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。
`--chain`	如果要發佈鏈結的憑證，請指定此選項。不需要選項值。

dir-cli trustedcert publish

將信任的根憑證發佈到 vmdir。

選項	說明
`--cert <file>`	憑證檔案的路徑。
`--crl <file>`	VMCA 不支援此選項。
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。
`--chain`	如果要發佈鏈結的憑證，請指定此選項。不需要選項值。

dir-cli trustedcert unpublish

解除發佈目前 vmdir 中信任的根憑證。例如，如果您已將其他根憑證新增到 vmdir (目前為環境中所有其他憑證的根憑證)，請使用此命令。強化環境的過程中，會解除發佈目前不再使用的憑證。

選項	說明
`--cert-file <file>`	要解除發佈的憑證檔案的路徑
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli trustedcert list

列出所有信任的根憑證及其對應的識別碼。您需要憑證識別碼才能使用 `dir-cli trustedcert get` 擷取憑證。

選項	說明
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli trustedcert get

從 vmdir 擷取信任的根憑證，然後將其寫入指定的檔案。

選項	說明
`--id <cert_ID>`	要擷取的憑證的識別碼。 `dir-cli trustedcert list` 命令顯示識別碼。
`--outcert <path>`	憑證檔案的寫入路徑。
`--outcrl <path>`	CRL 檔案的寫入路徑。目前未使用。
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli password create

建立符合密碼需求的隨機密碼。此命令可供第三方解決方案使用者使用。

選項	說明
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli password reset

可讓管理員重設使用者的密碼。如果您是非管理員使用者，但想重設密碼，請改用 `dir-cli password change`。

選項	說明
`--account`	為其指派新密碼的帳戶的名稱。
`--new`	指定使用者的新密碼。
`--login <admin_user_id>`	本機 vCenter Single Sign-On 網域的管理員，依預設為 administrator@vsphere.local。
`--password <admin_password>`	管理員使用者的密碼。如果未指定密碼，系統會提示您指定。

dir-cli password change

可讓使用者變更其密碼。您必須是擁有帳戶的使用者，才能做出此變更。管理員可使用 `dir-cli password reset` 重設任何密碼。

選項	說明
`--account`	帳戶名稱。
`--current`	擁有帳戶之使用者的目前密碼。
`--new`	擁有帳戶之使用者的新密碼。

使用 vCenter Single Sign-On 進行 vSphere 驗證

4

vCenter Single Sign-On 是一種驗證代理和安全性 Token 交換基礎結構。vCenter Single Sign-On 會在使用者驗證時發出 Token。使用者可使用 Token 向 vCenter Server 服務進行驗證。然後，使用者即可執行其有權執行的動作。

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

使用者和服務帳戶可使用 Token 或使用者名稱和密碼進行驗證。解決方案使用者會使用憑證進行驗證。如需取代解決方案使用者憑證的相關資訊，請參閱第 2 章 vSphere 安全性憑證。

下一個步驟是授權可以通過驗證來執行某些工作的使用者。在通常情況下，指派 vCenter Server 權限的方法通常是將使用者指派到具有角色的群組。vSphere 包含其他權限模型，例如全域權限。請參閱 vSphere 安全性說明文件。

本章節討論下列主題：

- vCenter Single Sign-On 如何保護您的環境
- 瞭解 vCenter Server 身分識別提供者聯盟
- 設定 vCenter Server 身分識別提供者同盟
- 瞭解 vCenter Single Sign-On
- 設定 vCenter Single Sign-On 身分識別來源
- 管理 Security Token Service
- 管理 vCenter Single Sign-On 原則
- 管理 vCenter Single Sign-On 使用者和群組
- 瞭解其他驗證選項
- 管理登入訊息
- vCenter Single Sign-On 安全性最佳做法

vCenter Single Sign-On 如何保護您的環境

vCenter Single Sign-On 可讓 vSphere 元件透過安全的 Token 機制相互通訊。

vCenter Single Sign-On 將使用下列服務。

- 透過外部身分識別提供者聯盟或 vCenter Server 內建身分識別提供者來驗證使用者。內建身分識別提供者支援本機帳戶、Active Directory 或 OpenLDAP、整合式 Windows 驗證 (IWA)，以及其他驗證機制 (智慧卡、RSA SecurID 和 Windows 工作階段驗證)。
- 透過憑證進行的解決方案使用者驗證。
- 安全性 Token 服務 (STS)。
- 用於安全流量的 SSL。

身分識別提供者概觀

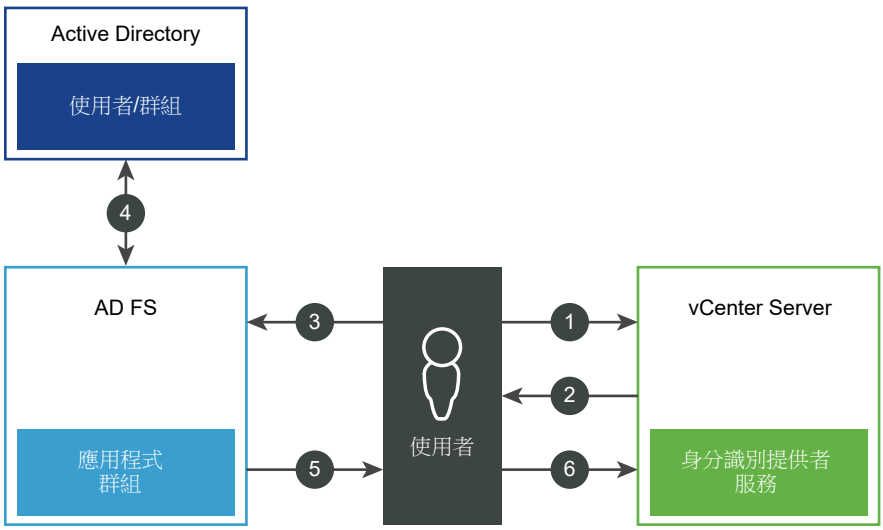
在 vSphere 7.0 之前，vCenter Server 包括內建身分識別提供者。依預設，vCenter Server 使用 vsphere.local 網域做為身分識別來源，但您可以在部署期間加以變更。您可以使用 LDAP/S、OpenLDAP/S 和整合式 Windows 驗證 (IWA) 設定 vCenter Server 內建身分識別提供者，以使用 Active Directory (AD) 做為其身分識別來源。此類組態可讓客戶使用其 AD 帳戶登入 vCenter Server。

從 vSphere 7.0 開始，您可以使用同盟驗證為外部身分識別提供者設定 vCenter Server。在此類組態中，將取代 vCenter Server 做為身分識別提供者。目前，vSphere 支援 Active Directory Federation Services (AD FS) 做為外部身分識別提供者。在此組態中，AD FS 會代表 vCenter Server 與身分識別來源互動。

使用者透過 vCenter Server 身分識別提供者同盟驗證登入

下圖顯示 vCenter Server 身分識別提供者聯盟的使用者登入流程。

圖 4-1. vCenter Server 身分識別提供者聯盟使用者登入



vCenter Server、AD FS 和 Active Directory 以如下方式進行互動：

1 使用者可以透過輸入使用者名稱，在 vCenter Server 登陸頁面上啟動。

2 如果使用者名稱用於聯盟網域，vCenter Server 會將驗證要求重新導向至 AD FS。

3 如有需要，AD FS 會提示使用者使用 Active Directory 認證登入。

4 AD FS 會使用 Active Directory 驗證使用者。

5 AD FS 透過來自 Active Directory 的群組資訊核發安全性 Token。

6 vCenter Server 使用 Token 將使用者登入。

現在使用者已通過驗證，因此可檢視並修改使用者角色對其擁有權限的任何物件。

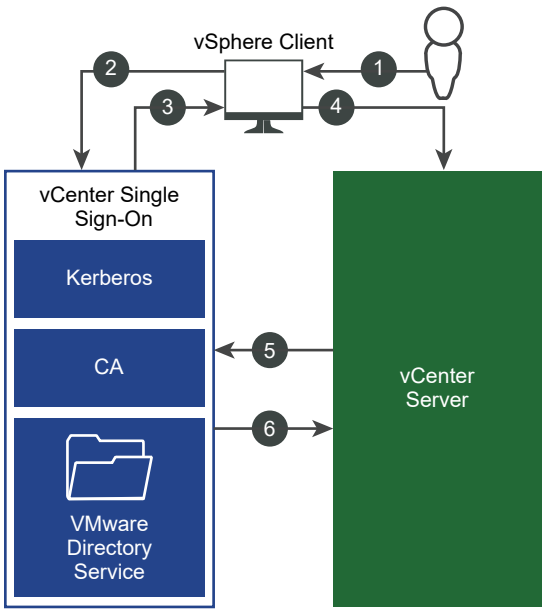
備註 系統初始會向每個使用者指派「無存取權」的角色。vCenter Server 管理員必須至少為使用者指派「唯讀」角色，使用者才能登入。請參閱 vSphere 安全性說明文件。

如果無法連線到外部身分識別提供者，則登入程序會退回到 vCenter Server 登陸頁面，並顯示相應的資訊訊息。使用者仍然可以使用 vsphere.local 身分識別來源中的本機帳戶登入。

使用者透過 vCenter Server 內建身分識別提供者登入

下圖顯示在 vCenter Server 充當身分識別提供者時的使用者登入流程。

圖 4-2. 使用者透過 vCenter Server 內建身分識別提供者登入



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

如果已設定整合式 Windows 驗證 (IWA)，使用者也可以透過勾選**使用 Windows 工作階段驗證**核取方塊來登入，而無需重新輸入其 Windows 密碼。

2 vSphere Client 會將登入資訊傳遞到 vCenter Single Sign-On 服務，該服務將檢查 vSphere Client 的 SAML Token。如果 vSphere Client 的 Token 有效，vCenter Single Sign-On 隨後會檢查使用者是否位於已設定的身分識別來源中 (例如，Active Directory)。

- 如果僅使用了使用者名稱，則 vCenter Single Sign-On 將在預設網域中檢查。

- 如果使用者名稱中包含網域名稱 (*DOMAIN*\user1 或 user1@*DOMAIN*)，則 vCenter Single Sign-On 將檢查該網域。

3 如果使用者可驗證身分識別來源，則 vCenter Single Sign-On 會將表示該使用者的 Token 傳回到 vSphere Client。

4 vSphere Client 會將 Token 傳遞到 vCenter Server 系統。

5 vCenter Server 與 vCenter Single Sign-On 伺服器確認 Token 是否有效且未到期。

6 vCenter Single Sign-On 伺服器會將 Token 傳回到 vCenter Server 系統，以利用 vCenter Server 授權架構允許使用者存取。

現在使用者已通過驗證，因此可檢視並修改使用者角色對其擁有權限的任何物件。

備註 系統初始會向每個使用者指派「無存取權」的角色。vCenter Server 管理員必須至少為使用者指派「唯讀」角色，使用者才能登入。請參閱 vSphere 安全性說明文件。

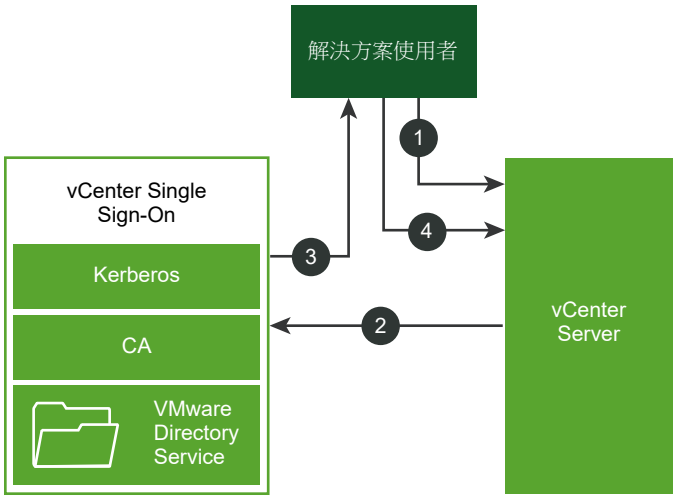
解決方案使用者的登入

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

備註 vCenter Server 僅使用解決方案使用者憑證進行內部通訊。不會將解決方案使用者憑證用於外部通訊。

下圖顯示了解決方案使用者的登入流程。

圖 4-3. 解決方案使用者的登入



1 解決方案使用者會嘗試連線至 vCenter Server 服務。

2 解決方案使用者會重新導向到 vCenter Single Sign-On。如果該解決方案使用者對 vCenter Single Sign-On 來說是新的使用者，則必須提供有效憑證。

3 如果憑證有效，則 vCenter Single Sign-On 會為解決方案使用者指派 SAML Token (Bearer Token)。此 Token 由 vCenter Single Sign-On 簽署。

4 然後，解決方案使用者會重新導向到 vCenter Single Sign-On，並且可以根據其權限執行相關工作。

下次解決方案使用者必須進行驗證，可使用 SAML Token 登入 vCenter Server。

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

支援的加密

支援 AES 加密，此加密是最高層級加密。當 vCenter Single Sign-On 使用 Active Directory 做為身分識別來源時，支援的加密會影響安全性。

每當 ESXi 主機或 vCenter Server 加入 Active Directory 時，它也會影響安全性。

瞭解 vCenter Server 身分識別提供者聯盟

從 vSphere 7.0 開始，vCenter Server 支援使用同盟驗證登入 vCenter Server。

若要啟用對 vCenter Server 進行同盟驗證，您可以設定與外部身分識別提供者的連線。您設定的身分識別提供者執行個體會取代 vCenter Server 做為身分識別提供者。目前，vCenter Server 僅支援 Active Directory Federation Services (AD FS) 做為外部身分識別提供者。

備註 隨著 vSphere 轉向基於 Token 的驗證，VMware 鼓勵您使用同盟驗證。vCenter Server 繼續擁有本機帳戶，用於管理存取和錯誤復原。

vCenter Server 身分識別提供者聯盟的運作方式

vCenter Server 身分識別提供者聯盟可讓您設定外部身分識別提供者進行同盟驗證。在此組態中，外部身分識別提供者會代表 vCenter Server 與身分識別來源互動。

vCenter Server 身分識別提供者聯盟基礎

從 vSphere 7.0 開始，vCenter Server 支援同盟驗證。在此案例中，當使用者登入 vCenter Server 時，vCenter Server 會將使用者登入重新導向至外部身分識別提供者。使用者認證不再直接提供給 vCenter Server。而是由使用者將認證提供給外部身分識別提供者。vCenter Server 信任由外部身分識別提供者執行驗證。在聯盟模型中，使用者永遠不會將認證直接提供給任何服務或應用程式，而只會提供給身分識別提供者。因此，您可以使用身分識別提供者來「聯盟」應用程式和服務，例如 vCenter Server。

vCenter Server 身分識別提供者聯盟優勢

vCenter Server 身分識別提供者聯盟提供以下優勢。

- 您可以將 Single Sign-On 與現有的同盟基礎結構和應用程式搭配使用。
- 可以提高資料中心的安全性，因為 vCenter Server 永遠不會處理使用者的認證。

- 您可以使用外部身分識別提供者支援的驗證機制，例如多重要素驗證。

vCenter Server 身分識別提供者聯盟元件

下列元件包括使用 Microsoft Active Directory Federation Services (AD FS) 的 vCenter Server 身分識別提供者聯盟組態：

- vCenter Server
- vCenter Server 上設定的身分識別提供者服務
- AD FS 伺服器和相關聯的 Microsoft Active Directory 網域
- AD FS 應用程式群組
- 對應至 vCenter Server 群組和使用者的 Active Directory 群組和使用者

備註 目前，vCenter Server 僅支援 AD FS 做為外部身分識別提供者。

vCenter Server 身分識別提供者聯盟架構

在 vCenter Server 身分識別提供者聯盟中，vCenter Server 會使用 OpenID Connect (OIDC) 通訊協定來接收可向 vCenter Server 驗證使用者的身分識別 Token。

若要在 vCenter Server 和身分識別提供者之間建立信賴方信任，則必須在兩者之間建立識別資訊和共用密碼。在 AD FS 中，您可以透過建立稱為應用程式群組 (由伺服器應用程式和 Web API 組成) 的 OIDC 組態來執行此操作。這兩個元件會指定 vCenter Server 用於信任和與 AD FS 伺服器進行通訊的資訊。您也可以在 vCenter Server 中建立對應的身分識別提供者。最後，您可以在 vCenter Server 中設定群組成員資格，以授權來自 AD FS 網域中的使用者登入。

AD FS 管理員必須提供下列資訊，才能建立 vCenter Server 身分識別提供者組態：

- 用戶端識別碼：由 AD FS [應用程式群組] 精靈所產生並用於識別應用程式群組本身的 UUID 字串。
- 共用密碼：由 AD FS [應用程式群組] 精靈所產生並用於向 AD FS 驗證 vCenter Server 的密碼。
- OpenID 位址：AD FS 伺服器的 OpenID 提供者探索端點 URL，指定眾所周知的位址，通常是與路徑「`/.well-known/openid-configuration`」相連接的簽發者端點。例如：`https://webserver.example.com/adfs/.well-known/openid-configuration`。

vCenter Server 身分識別提供者聯盟和增強型連結模式

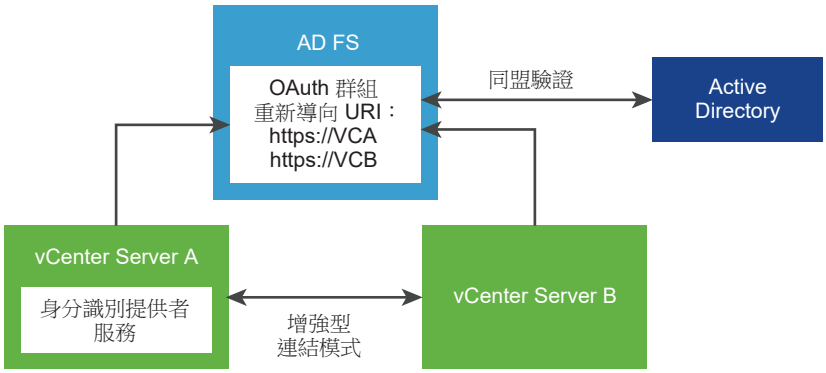
在使用增強型連結模式的 vCenter Server 環境中啟用身分識別提供者聯盟時，驗證和工作流程將繼續如往常一般運作。

如果您使用增強型連結模式組態，請在使用同盟驗證登入 vCenter Server 時注意下列事項。

- 根據 vCenter Server 權限和角色模型，使用者會繼續查看相同的詳細目錄，並且可以執行相同的動作。
- 增強型連結模式下的 vCenter Server 主機不需要存取彼此的身分識別提供者。例如，假設有兩個 vCenter Server 系統 A 和 B，且使用增強型連結模式。當 vCenter ServerA 授權使用者後，也會在 vCenter Server B 上授權該使用者。

下圖顯示使用增強型連結模式和 vCenter Server 身分識別提供者聯盟的驗證工作流程。

圖 4-4. 增強型連結模式和 vCenter Server 身分識別提供者聯盟



1 在增強型連結模式組態中部署了兩個 vCenter Server 節點。

2 已使用 vSphere Client 中的 [變更身分識別提供者] 精靈在 vCenter Server A 設定 AD FS 設定。此外，已為 AD FS 使用者或群組建立群組成員資格和權限。

3 vCenter ServerA 將 AD FS 組態複寫至 vCenter Server B。

4 兩個 vCenter Server 節點的所有重新導向 URI 都會新增至 AD FS 中的 OAuth 應用程式群組。僅建立一個 OAuth 應用程式群組。

5 當使用者登入 vCenter ServerA 並獲得該伺服器授權時，該使用者也會在 vCenter Server B 上獲得授權。如果使用者先登入 vCenter Server B，則同樣適用。

vCenter Server 增強型連結模式支援身分識別提供者聯盟的下列組態案例。在此區段中，「AD FS 設定」和「AD FS 組態」一詞是指您使用 [變更身分識別提供者] 精靈在 vSphere Client 中進行的設定，以及針對 AD FS 使用者或群組建立的任何群組成員資格或權限。

在現有的增強型連結模式組態上啟用 AD FS

高層級步驟：

1 在增強型連結模式組態中，部署 N 個 vCenter Server 節點。

2 在其中一個連結的 vCenter Server 節點上設定 AD FS。

3 AD FS 組態會複寫至所有其他 (N-1 個) vCenter Server 節點。

4 將全部 N 個 vCenter Server 節點的所有重新導向 URI 新增至 AD FS 中已設定的 OAuth 應用程式群組。

將新的 vCenter Server 連結至現有的增強型連結模式 AD FS 組態

高層級步驟：

1 (必要條件) 在 vCenter ServerN 節點增強型連結模式組態上設定 AD FS。

2 部署新的獨立 vCenter Server 節點。

3 使用 *N* 個節點中的一個節點做為其複寫合作夥伴，將新 vCenter Server 重新指向 N 節點 AD FS 增強型連結模式網域。

4 現有增強型連結模式組態中的所有 AD FS 設定都會複寫到新的 vCenter Server。

N 節點 AD FS 增強型連結模式網域中的 AD FS 設定會覆寫新連結 vCenter Server 上的任何現有 AD FS 設定。

5 將新 vCenter Server 的所有重新導向 URI 新增至 AD FS 中現有的已設定 OAuth 應用程式群組。

從增強型連結模式 AD FS 組態取消連結 vCenter Server

高層級步驟：

1 (必要條件) 在 N 節點 vCenter Server 增強型連結模式組態上設定 AD FS。

2 解除登錄 N 節點組態中的其中一部 vCenter Server 主機並將其重新指向至新網域，以將該主機從 N 節點組態取消連結。

3 網域重新指向程序不會保留 SSO 設定，因此未連結的 vCenter Server 節點上的所有 AD FS 設定都會還原並遺失。若要繼續在此 vCenter Server 未連結的節點上使用 AD FS，您必須從頭開始重新設定 AD FS，或者必須將 vCenter Server 重新連結至已設定 AD FS 的增強型連結模式組態。

vCenter Server 身分識別提供者同盟注意須知和互通性

vCenter Server 身分識別提供者同盟可以與許多其他 VMware 功能進行交互操作。

規劃 vCenter Server 身分識別提供者同盟策略時，請考慮可能的互通性限制。

驗證機制

在 vCenter Server 身分識別提供者聯盟組態中，外部身分識別提供者會處理驗證機制 (密碼、MFA、生物識別等)。

vCenter Server 原則

vCenter Server 充當身分識別提供者時，您可以控制 vsphere.local 網域的 vCenter Server 密碼、鎖定和 Token 原則。將同盟驗證與 vCenter Server 搭配使用時，外部身分識別提供者會控制儲存在身分識別來源 (例如 Active Directory) 中帳戶的密碼、鎖定和 Token 原則。

稽核與符合性

使用 vCenter Server 身分識別提供者同盟時，vCenter Server 會繼續為成功的使用者登入建立記錄項目。但是，外部身分識別提供者會負責追蹤和記錄動作，例如失敗的密碼輸入嘗試和使用者帳戶鎖定。vCenter Server 不會記錄此類事件，因為它們無法向 vCenter Server 顯示。例如，當 AD FS 為身分識別提供者時，AD FS 會追蹤並記錄同盟登入的錯誤。當 vCenter Server 是用於本機登入的身分識別提供者時，vCenter Server 會追蹤並記錄本機登入的錯誤。在同盟組態中，vCenter Server 會繼續記錄使用者在登入後的動作。

現有的 VMware 產品整合

VMware 產品與 vCenter Server(例如 vROps、vSAN、NSX 等) 的整合會繼續像之前一樣運作。

整合登入後的產品

整合登入後的產品 (即不需要單獨登入) 會繼續像之前一樣運作。

API、SDK 和 CLI 存取的簡單驗證

依賴 API、SDK 或使用簡單驗證 (即使用者名稱和密碼) 的 CLI 命令的現有指令碼、產品和其他功能，可如以往般繼續運作。在內部，驗證是透過傳遞使用者名稱和密碼進行。此使用者名稱和密碼的傳遞會削弱使用身分識別聯盟的某些優點，因為它會公開密碼給 vCenter Server(和您的指令碼)。如果可能，請考慮移轉至以 Token 為基礎的驗證。

vCenter Server 管理介面

如果使用者是 Administrators 群組的成員，則支援存取 vCenter Server 管理介面 (先前稱為 vCenter Server 應用裝置管理介面或 VAMI)。

在 AD FS 登入頁面上輸入使用者名稱文字

AD FS 登入頁面不支援傳遞文字以預先填入使用者名稱文字方塊。因此，在使用 AD FS 進行同盟登入期間，於 vCenter Server 登陸頁面上輸入您的使用者名稱並重新導向至 AD FS 登入頁面後，您必須在 AD FS 登入頁面上重新輸入您的使用者名稱。需要您在 vCenter Server 登陸頁面上輸入的使用者名稱，以將登入重新導向至適當的身分識別提供者，並且需要 AD FS 登入頁面上的使用者名稱，以使用 AD FS 進行驗證。無法將使用者名稱傳遞至 AD FS 登入頁面，這是 AD FS 的限制。您無法直接從 vCenter Server 設定或變更此行為。

vCenter Server 身分識別提供者同盟生命週期

管理 vCenter Server 身分識別提供者同盟的生命週期時，有一些特定考量事項。

您可以使用下列方式管理 vCenter Server 身分識別提供者同盟生命週期。

從使用 Active Directory 移轉至 AD FS

如果您使用 Active Directory 做為 vCenter Server 的身分識別來源，則移轉為使用 AD FS 最直接。如果您的 Active Directory 群組和角色符合您的 AD FS 群組和角色，則無需執行任何其他動作。當群組和角色不相符時，您必須執行一些額外的工作。如果 vCenter Server 是網域成員，請考慮將其從網域中移除，因為不需要它或用於身分識別聯盟。

跨網域重新指向和移轉

vCenter Server 身分識別提供者同盟支援跨網域重新指向，也就是將 vCenter Server 從一個 vSphere SSO 網域移到另一個。重新指向的 vCenter Server 會從所指向的 vCenter Server 系統或系統接收已複寫的 AD FS 組態。

一般而言，除非下列其中一項成立，否則您不需要針對跨網域重新指向執行任何其他 AD FS 重新設定。

1 重新指向 vCenter Server 的 AD FS 組態與所指向之 vCenter Server 的 AD FS 組態不同。

2 這是重新指向的 vCenter Server 第一次接收 AD FS 組態。

在這些情況下，您必須將 vCenter Server 系統的重新導向 URI 新增至 AD FS 伺服器上對應的應用程式群組。例如，如果將具有 AD FS 應用程式群組 A (或沒有 AD FS 組態) 的 vCenter Server1 重新指向至具有 AD FS 應用程式群組 B 的 vCenter Server 2，則必須將 vCenter Server 1 的重新導向 URI 新增至應用程式群組 B。

設定 vCenter Server 身分識別提供者同盟

在您最初部署 vCenter Server 之後，您可以為同盟驗證設定外部身分識別提供者。

您可以從 vSphere Client 或 API 設定 vCenter Server 身分識別提供者同盟。還必須在外部身分識別提供者上執行某些組態。若要設定 vCenter Server 身分識別提供者同盟，您必須擁有 vCenter Single Sign-On 管理員權限。vCenter Single Sign-On 管理員權限不同於 vCenter Server 或 ESXi 上的管理員角色。在全新安裝中，僅 vCenter Single Sign-On 管理員 (依預設為 administrator@vsphere.local) 可向 vCenter Single Sign-On 進行驗證。

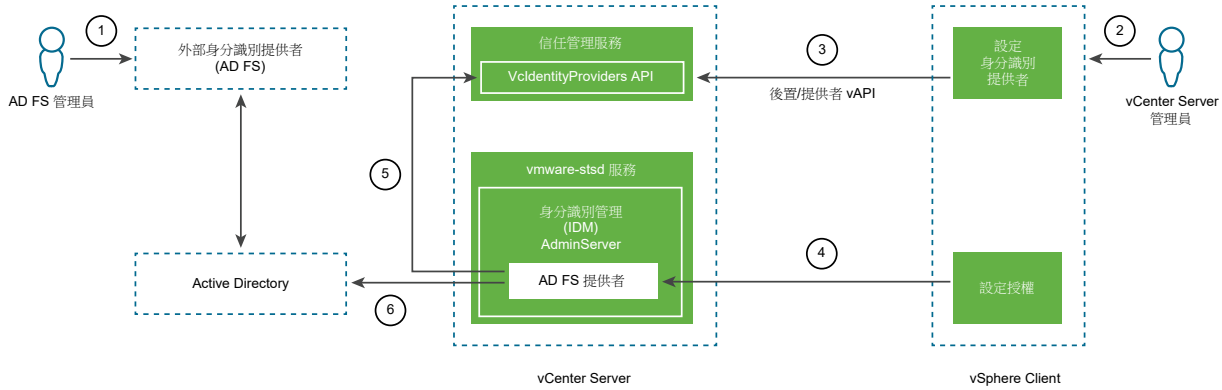
vCenter Server 身分識別提供者聯盟設定程序流程

為了有效地設定 vCenter Server 身分識別提供者聯盟，您必須瞭解發生的通訊流程。

vCenter Server 身分識別提供者聯盟設定程序流程

下圖顯示了設定 vCenter Server 身分識別提供者聯盟時發生的程序流程。

圖 4-5. vCenter Server 身分識別提供者聯盟設定程序流程



vCenter Server、AD FS 和 Active Directory 以如下方式進行互動。

1 AD FS 管理員為 vCenter Server 設定 AD FS OAuth 應用程式。

2 vCenter Server 管理員使用 vSphere Client 登入 vCenter Server。

3 vCenter Server 管理員將 AD FS 身分識別提供者新增至 vCenter Server，並同時輸入 Active Directory 網域的相關資訊。

   vCenter Server 需要此資訊才能與 AD FS 伺服器的 Active Directory 網域建立 LDAP 連線。使用此連線時，vCenter Server 搜尋使用者和群組，並在下一個步驟中將其新增至 vCenter Server 的本機群組。如需詳細資訊，請參閱下文中標題為「搜尋 Active Directory 網域」的章節。

4 vCenter Server 管理員在 vCenter Server 中為 AD FS 使用者設定授權權限。

5 AD FS 提供者查詢 VcIdentityProviders API，以取得 Active Directory 來源的 LDAP 連線資訊。

6 AD FS 提供者在 Active Directory 中搜尋查詢的使用者或群組，以完成授權設定。

搜尋 Active Directory 網域

可以使用 vSphere Client 中的 [設定主要身分識別提供者] 精靈，將 AD FS 設定為 vCenter Server 中的外部身分識別提供者。在設定過程中，必須輸入 Active Directory 網域的相關資訊，包括使用者和群組辨別名稱資訊。設定 AD FS 進行驗證需要此 Active Directory 連線資訊。必須具備此連線，才能搜尋 Active Directory 使用者名稱和群組並將其對應至 vCenter Server 中的角色和權限，而 AD FS 則用於驗證使用者。[設定主要身分識別提供者] 精靈的這一步驟不會建立 Active Directory Over LDAP 身分識別來源。而 vCenter Server 會使用此資訊與 Active Directory 網域建立可進行有效搜尋的連線，以便在此尋找使用者和群組。

假設使用下列辨別名稱項目的範例：

- 使用者的基本辨別名稱：cn=Users,dc=corp,dc=local
- 群組的基本辨別名稱：dc=corp,dc=local
- 使用者名稱：cn=Administrator,cn=Users,dc=corp,dc=local

如果 AdfsUser@corp.local 使用者是 ADGroup@corp.local 群組的成員，則在精靈中輸入此資訊可允許 vCenter Server 管理員搜尋和尋找 ADGroup@corp.local 群組，並將其新增至 vCenter Server Administrators@vsphere.local 群組。如此一來，AdfsUser@corp.local 使用者在登入後會被授與 vCenter Server 的管理權限。

當您為 Active Directory 使用者和群組設定全域權限時，vCenter Server 也會使用此搜尋程序。無論是設定全域權限，還是新增使用者或群組，在這兩種情況下，您都可以從**網域**下拉式功能表中選取「Microsoft ADFS」進行搜尋，並從 Active Directory 網域中選取使用者和群組。

使用受信任的根憑證存放區而非 JRE 信任存放區

如果在 vSphere 7.0 中將自我簽署的根 CA 憑證匯入到了 JRE 信任存放區，則從 vSphere 7.0 Update 1 開始，您可以將憑證登錄至受信任的根憑證存放區。

若要使用自我簽署的根 CA 憑證在 vSphere 7.0 中設定 vCenter Server 身分識別提供者聯盟，則必須將其匯入至 JRE 信任存放區。從 vSphere 7.0 Update 1 開始，您可以將憑證登錄至受信任的根憑證存放區。此變更表示應將自我簽署的根 CA 憑證新增至受信任的根憑證存放區 (也稱為 VMware Endpoint 憑證存放區或 VECS)。JRE 信任存放區中的憑證會繼續運作，但是 vCenter Server 將對受信任根憑證存放區的使用執行標準化。

程序

1 使用 vSphere Client 登入 vCenter Server。

2 導覽至**管理 > 憑證 > 憑證管理**。

3 在**受信任的根憑證**旁邊，按一下**新增**。

4 瀏覽 AD FS 根憑證，然後按一下**新增**。

憑證隨即新增至**受信任的根憑證**下的面板中。

設定 vCenter Server 身分識別提供者聯盟

安裝或升級至 vSphere 7.0 或更新版本之後，您可以設定 vCenter Server 身分識別提供者聯盟。目前，vCenter Server 僅支援 Active Directory Federation Services (AD FS) 做為外部身分識別提供者。

vCenter Server 僅支援一個外部身分識別提供者 (一個 AD FS 來源) 和 vsphere.local 身分識別來源。無法使用多個外部身分識別提供者。vCenter Server 身分識別提供者聯盟使用 OpenID Connect (OIDC)，以供使用者登入 vCenter Server。

注意 如果您使用先前新增至 vCenter Server 的 Active Directory 身分識別來源做為 AD FS 身分識別來源，請不要從 vCenter Server 中刪除現有的身分識別來源。這樣做會導致先前指派的角色和群組成員資格出現回歸問題。具有全域權限的 AD FS 使用者和新增至管理員群組的使用者都將無法登入。

因應措施：如果您不需要先前指派的角色和群組成員資格，且想要移除先前的 Active Directory 身分識別來源，請先移除身分識別來源，然後再建立 AD FS 提供者並在 vCenter Server 中設定群組成員資格。

必要條件

Active Directory Federation Services 需求：

- 必須已部署適用於 Windows Server 2016 或更新版本的 AD FS。
- AD FS 必須連線至 Active Directory。
- 在設定過程中，必須在 AD FS 中建立 vCenter Server 的應用程式群組。請參閱 VMware 知識庫文章，網址為 https://kb.vmware.com/s/article/78029。
- 通常，您會使用由公開信任的憑證授權機構簽署的 AD FS 伺服器憑證 (請參閱 https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/overview/ad-fs-requirements)。也可以使用自我簽署的憑證。這樣一來，則必須將 AD FS 根 CA 憑證新增至受信任的根憑證存放區 (也稱為 VMware 憑證存放區)。

如需有關設定 AD FS 的詳細資訊，請參閱 Microsoft 說明文件。

vCenter Server 和其他需求：

- vSphere 7.0 或更新版本
- vCenter Server 必須能夠連線至 AD FS 探索端點，以及在探索端點中繼資料中通告的授權、Token、登出、JWKS 和任何其他端點。
- 您需要 **VcIdentityProviders.管理**權限，才能建立、更新或刪除同盟驗證所需的 vCenter Server 身分識別提供者。若要限制使用者僅檢視身分識別提供者組態資訊，請指派 **VcIdentityProviders.讀取**權限。

程序

1 使用 vSphere Client 登入 vCenter Server。

2 (選擇性) 如果使用自我簽署的憑證，請將您的根 AD FS 憑證新增至受信任的根憑證存放區。

a 導覽至**管理 > 憑證 > 憑證管理**。

b 在受信任的根存放區旁邊，按一下**新增**。

c 瀏覽 AD FS 根憑證，然後按一下**新增**。

憑證隨即新增至 [受信任的根憑證] 下的面板中。

3 導覽至組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**組態**。

4 選取**身分識別提供者**索引標籤，並取得重新導向 URI。

a 按一下「變更身分識別提供者」連結旁邊的資訊「i」**圖示**。

此時會在彈出橫幅中顯示兩個重新導向 URI。

b 將這兩個 URI 複製到檔案，或將其記下，以供稍後在設定 AD FS 伺服器的後續步驟中使用。

c 關閉彈出橫幅。

5 在 AD FS 中建立 OpenID Connect 組態，並將其設定用於 vCenter Server。

若要在 vCenter Server 和身分識別提供者之間建立信賴方信任，則必須在兩者之間建立識別資訊和共用密碼。在 AD FS 中，您可以透過建立稱為應用程式群組 (由伺服器應用程式和 Web API 組成) 的 OpenID Connect 組態來執行此操作。這兩個元件會指定 vCenter Server 用於信任和與 AD FS 伺服器進行通訊的資訊。若要在 AD FS 中啟用 OpenID Connect，請參閱 VMware 知識庫文章，網址為 https://kb.vmware.com/s/article/78029。

建立 AD FS 應用程式群組時，請注意下列事項。

- 需要用到在先前步驟中取得並儲存的兩個重新導向 URI。
- 將下列資訊複製到檔案，或將其記下來，以供在下一個步驟中設定 vCenter Server 身分識別提供者時使用。
  - 用戶端識別碼
  - 共用密碼
  - AD FS 伺服器的 OpenID 位址

6 在 vCenter Server 上建立身分識別提供者。

a 返回 vSphere Client 中的**身分識別提供者**索引標籤。

b 按一下「變更身分識別提供者」連結。

[設定主要身分識別提供者] 精靈隨即開啟。

c 選取 **Microsoft ADFS**，然後按**下一步**。

在下列文字方塊中輸入先前收集的資訊：

- 用戶端識別碼
- 共用密碼
- AD FS 伺服器的 OpenID 位址

d 按**下一步**。

e 輸入 Active Directory over LDAP 連線的使用者和群組資訊，以搜尋使用者和群組。

選項	說明
使用者的基本辨別名稱	使用者的基本辨別名稱。
群組的基本辨別名稱	群組的基本辨別名稱。
Username	網域中使用者的識別碼，該使用者對使用者和群組的基本 DN 僅具有最小唯讀存取權。
密碼	網域中使用者的識別碼，該使用者對使用者和群組的基本 DN 僅具有最小唯讀存取權。
主要伺服器 URL	網域的網域主控站 LDAP 伺服器。 使用 **`ldap://hostname:port`** 或 **`ldaps://hostname:port`** 格式。通常為連接埠 389 用於 LDAP 連線，而連接埠 636 用於 LDAPS 連線。對於 Active Directory 多網域控制站部署，通常為連接埠 3268 用於 LDAP，而連接埠 3269 用於 LDAPS。 在主要或次要 LDAP URL 中使用 **`ldaps://`** 時，需要為 Active Directory 伺服器的 LDAPS 端點建立信任的憑證。
次要伺服器 URL	用於容錯移轉之次要網域控制站 LDAP 伺服器的位址。
SSL 憑證	如果您想要將 LDAPS 用於 Active Directory LDAP 伺服器或 OpenLDAP 伺服器身分識別來源，請按一下**瀏覽**以選取憑證。

f 按**下一步**，檢閱資訊，然後按一下**完成**即可完成此精靈。

7 導覽至 vCenter Single Sign-On 使用者組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**使用者和群組**。

8 透過 vCenter Server 中的全域或物件權限，針對 AD FS 授權設定群組成員資格或權限。

a 按一下**群組**索引標籤。

b 按一下**管理員**群組，然後按一下**新增成員**。

c 從下拉式功能表中選取 **Microsoft ADFS**。

d 在下拉式功能表下方的文字方塊中，輸入 **vcenter** 並等待下拉式選取範圍出現。

可能需要幾秒鐘的時間才能顯示選取範圍，因為 vCenter Server 要建立與 Active Directory 的連線並進行搜尋。

e 選取 **VCenterAdmins**，並將其新增至群組。

f 按一下**儲存**。

9 確認以 Active Directory 使用者身分登入 vCenter Server。

瞭解 vCenter Single Sign-On

如果您未使用外部身分識別提供者，則必須瞭解內建身分識別提供者的基礎架構、vCenter Single Sign-On，以及其對安裝和升級的影響。

vCenter Single Sign-On 元件

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

在安裝期間，下列元件會做為 vCenter Server 部署的一部分進行部署。

STS (Security Token Service)

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

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

管理伺服器

管理伺服器允許具有 vCenter Single Sign-On 管理員權限的使用者，從 vSphere Client 設定 vCenter Single Sign-On 伺服器並管理使用者和群組。一開始，只有使用者 administrator@*your_domain_name* 具有這些權限。您可以在安裝 vCenter Server 時變更 vSphere 網域。請勿使用您的 Microsoft Active Directory 或 OpenLDAP 網域名稱命名此網域名稱。

VMware Directory Service (vmdir)

VMware Directory Service (vmdir) 與您安裝期間指定的網域相關聯，並包含在每個 vCenter Server 部署中。此服務是一種多承租人、對等複寫的目錄服務，可在連接埠 389 上提供 LDAP 目錄。它也會儲存並管理 vCenter Single Sign-On 使用者帳戶和密碼，這些帳戶和密碼受 SHA-512 雜湊演算法保護。

如果您的環境包含多個在連結模式下設定的 vCenter Server 執行個體，則一個 vmdir 執行個體中的 vmdir 內容更新將傳播到所有其他 vmdir 執行個體。

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

Identity Management 服務

處理身分識別來源和 STS 驗證要求。

將 vCenter Single Sign-On 與 vSphere 搭配使用

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

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

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

  使用者可以檢視的物件，以及使用者可以執行的動作，通常是由 vCenter Server 權限設定決定。vCenter Server 管理員會從 vSphere Client 中的**權限**介面指派這些權限，而不是透過 vCenter Single Sign-On。請參閱 vSphere 安全性說明文件。

vCenter Single Sign-On 和 vCenter Server 使用者

使用者可透過在登入頁面上輸入其認證，向 vCenter Single Sign-On 進行驗證。連線到 vCenter Server 後，已驗證的使用者可以檢視所有 vCenter Server 執行個體，或其角色有權檢視的其他 vSphere 物件。無需進一步驗證。

安裝之後，vCenter Single Sign-On 網域的管理員，預設是 administrator@vsphere.local，會具有 vCenter Single Sign-On 和 vCenter Server 的管理員存取權。然後，該使用者可以新增身分識別來源、設定預設身分識別來源，以及管理 vCenter Single Sign-On 網域中的使用者和群組。

可對 vCenter Single Sign-On 進行驗證的所有使用者都可以重設其密碼。請參閱變更 vCenter Single Sign-On 密碼 。只有 vCenter Single Sign-On 管理員能為遺失密碼的使用者重設密碼。

vCenter Single Sign-On 管理員使用者

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

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

備註 您無法重新命名 vCenter Single Sign-On 管理員使用者，其預設為 administrator@vsphere.local，或如果您在安裝期間指定了不同的網域，則為 administrator@*mydomain*。為提高安全性，請考量在 vCenter Single Sign-On 網域中建立其他具名使用者，並為這些使用者指派管理權限。然後您可以停止使用管理員帳戶。

其他使用者帳戶

在 vsphere.local 網域 (或安裝時建立的預設網域) 中，下列使用者帳戶會在 vCenter Server 內自動建立。這些使用者帳戶是 shell 帳戶。vCenter Single Sign-On 密碼原則不適用於這些帳戶。

表 4-1. 其他 vSphere 使用者帳戶

帳戶	說明
K/M	適用於 Kerberos 金鑰管理。
krbtgt/VSPHERE.LOCAL	適用於整合式 Windows 驗證相容性。
waiter-*random_string*	適用於 Auto Deploy。

ESXi 使用者

獨立的 ESXi 主機未與 vCenter Single Sign-On 整合。如需新增 ESXi 主機至 Active Directory 的相關資訊，請參閱 vSphere 安全性。

如果您使用 VMware Host Client、ESXCLI 或 PowerCLI 為受管理 ESXi 主機建立本機 ESXi 使用者，vCenter Server 不會感知這些使用者。因此，建立本機使用者可能會造成混亂，尤其是如果您使用相同的使用者名稱。能夠向 vCenter Single Sign-On 驗證的使用者若具有 ESXi 主機物件上的對應權限，則可以檢視和管理 ESXi 主機。

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

如何登入 vCenter Server 元件

您可以透過連線至 vSphere Client 來登入。

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

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

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

vCenter Single Sign-On 網域中的群組

vCenter Single Sign-On 網域 (依預設為 vsphere.local) 包括數個預先定義的群組。將使用者新增到其中一個群組，讓其可執行對應的動作。

請參閱管理 vCenter Single Sign-On 使用者和群組。

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

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

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

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

表 4-2. vsphere.local 網域中的群組

權限	說明
使用者	vCenter Single Sign-On 網域 (依預設為 vsphere.local) 中的使用者。
SolutionUsers	vCenter 服務的解決方案使用者群組。每個解決方案使用者會使用憑證向 vCenter Single Sign-On 進行個別驗證。依預設，VMCA 會使用憑證佈建解決方案使用者。請勿明確向此群組新增成員。
CAAdmins	CAAdmins 群組的成員擁有 VMCA 的管理員權限。除非您有足夠的理由，否則請勿向此群組新增成員。
DCAdmins	DCAdmins 群組的成員可以對 VMware Directory Service 執行網域控制站管理員動作。 **備註** 請勿直接管理網域控制站。而是使用 `vmdir` CLI 或 vSphere Client 執行對應工作。
SystemConfiguration.BashShellAdministrators	此群組中的使用者可以啟用和停用對 BASH shell 的存取。依預設，使用 SSH 連線到 vCenter Server 的使用者只能存取受限制的 shell 中的命令。此群組中的使用者可以存取 BASH shell。
ActAsUsers	允許 Act-As Users 的成員從 vCenter Single Sign-On 取得 Act-As Token。
ExternalIDPUsers	vSphere 不使用此內部群組。VMware vCloud Air 需要此群組。
SystemConfiguration.Administrators	SystemConfiguration.Administrators 群組的成員可以在 vSphere Client 中檢視和管理系統組態。這些使用者可檢視服務、啟動與重新啟動服務、對服務進行疑難排解，以及查看並管理可用節點。
DCClients	此群組供內部使用，允許管理節點對 VMware Directory Service 中的資料進行存取。 **備註** 請勿修改此群組。任何變更都可能會影響憑證基礎結構。
ComponentManager.Administrators	ComponentManager.Administrators 群組的成員可以叫用登錄或解除登錄服務 (即，修改服務) 的 Component Manager API。取得此服務的讀取權限並不需要此群組的成員資格。
LicenseService.Administrators	LicenseService.Administrators 的成員擁有對所有授權相關資料的完整寫入權限，且可以針對在授權服務中登錄的所有產品資產新增、移除、指派以及取消指派序列金鑰。
管理員	VMware Directory Service (vmdir) 的管理員。此群組的成員可以執行 vCenter Single Sign-On 管理工作。除非您有足夠的理由並瞭解後果，否則請勿向此群組新增成員。

表 4-2. vsphere.local 網域中的群組 (續)

權限	說明
TrustedAdmins	此群組的成員可以執行 VMware® vSphere Trust Authority™ 設定和管理工作。依預設，此群組不包含任何成員。您必須將成員新增到此群組，才能執行 vSphere Trust Authority 工作。
AutoUpdate	此群組在 vCenter Cloud Gateway 內部使用。
SyncUsers	此群組在 vCenter Cloud Gateway 內部使用。
vSphereClientSolutionUsers	此群組在 vSphere Client 內部使用。
ServiceProviderUsers	此群組的成員可以管理 vSphere with Tanzu 和 VMware Cloud on AWS 基礎結構。
NsxAdministrators	此群組用於 NSX。
WorkloadStorage	工作負載儲存區群組。
RegistryAdministrators	此群組的成員可以管理登錄。
NsxAuditors	此群組用於 NSX。
NsxViAdministrators	此群組用於 NSX。
SystemConfiguration.SupportUsers	SystemConfiguration.SupportUsers 群組的成員可以存取支援服務包 API。
SystemConfiguration.ReadOnly	此群組的成員可以存取 vCenter Server Appliance 唯讀作業。

設定 vCenter Single Sign-On 身分識別來源

當使用者僅使用使用者名稱登入時，vCenter Single Sign-On 會於預設身分識別來源中檢查使用者能否進行驗證。當使用者在登入畫面中登入並包含網域名稱時，vCenter Single Sign-On 會檢查指定的網域，確認該網域是否已新增為身分識別來源。您可以新增身分識別來源、移除身分識別來源，以及變更預設值。

您可以從 vSphere Client 設定 vCenter Single Sign-On。若要設定 vCenter Single Sign-On，您必須擁有 vCenter Single Sign-On 管理員權限。vCenter Single Sign-On 管理員權限不同於 vCenter Server 或 ESXi 上的管理員角色。在全新安裝中，僅 vCenter Single Sign-On 管理員 (依預設為 administrator@vsphere.local) 可向 vCenter Single Sign-On 進行驗證。

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

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

從 vSphere 7.0 開始，vCenter Server 支援同盟驗證以登入 vCenter Server。隨著 vSphere 轉向基於 Token 的驗證，VMware 鼓勵您使用同盟驗證。請參閱瞭解 vCenter Server 身分識別提供者聯盟。

管理員可以新增身分識別來源、設定預設身分識別來源，以及在 vsphere.local 身分識別來源中建立使用者和群組。

使用者和群組資料儲存在 Active Directory、OpenLDAP 中，或安裝 vCenter Single Sign-On 所在機器的作業系統本機上。安裝完成之後，vCenter Single Sign-On 的每個執行個體都會擁有身分識別來源 *your_domain_name*，例如 vsphere.local。此身分識別來源位於 vCenter Single Sign-On 內部。

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

以下是可用的身分識別來源。

- Active Directory over LDAP。vCenter Single Sign-On 支援多個 Active Directory over LDAP 身分識別來源。
- Active Directory (整合式 Windows 驗證) 2003 版及更新版本。vCenter Single Sign-On 允許將單一 Active Directory 網域指定為身分識別來源。該網域可包含子網域或做為樹系的根網域。VMware 知識庫文章 2064250 說明 vCenter Single Sign-On 支援的 Microsoft Active Directory 信任關係。
- OpenLDAP 2.4 及更新版本。vCenter Single Sign-On 支援多個 OpenLDAP 身分識別來源。

備註 對 Microsoft Windows 的未來更新將變更 Active Directory 的預設行為，以要求使用強式驗證和加密。此變更會影響 vCenter Server 向 Active Directory 進行驗證的方式。如果您使用 Active Directory 做為 vCenter Server 的身分識別來源，則必須計劃啟用 LDAPS。如需有關此 Microsoft 安全性更新的詳細資訊，請參閱 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 和 https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html。

設定 vCenter Single Sign-On 的預設網域

每個 vCenter Single Sign-On 身分識別來源都與某個網域相關聯。vCenter Single Sign-On 會使用預設網域驗證未使用網域名稱登入的使用者身分。屬於某網域 (非預設網域) 的使用者在登入時必須包含該網域名稱。

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

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

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**組態**。

4 在**身分識別提供者**索引標籤下，按一下**身分識別來源**，選取身分識別來源，然後按一下**設定為預設值**。

5 按一下**確定**。

在網域顯示中，預設網域顯示在 [類型] 欄中 (預設)。

新增或編輯 vCenter Single Sign-On 身分識別來源

僅在使用者位於已新增為 vCenter Single Sign-On 身分識別來源的網域中時，才可登入 vCenter Server。vCenter Single Sign-On 管理員使用者可以新增身分識別來源，或變更使用者新增的身分識別來源設定。

身分識別來源可以是 Active Directory over LDAP、原生 Active Directory (整合式 Windows 驗證) 網域，也可以是 OpenLDAP 目錄服務。請參閱具有 vCenter Single Sign-On 的 vCenter Server 的身分識別來源。

安裝之後，具有 vCenter Single Sign-On 內部使用者的 vsphere.local 網域 (或您在安裝期間指定的網域) 立即可供使用。

必要條件

如果要新增 Active Directory (整合式 Windows 驗證) 身分識別來源，則 vCenter Server 必須位於 Active Directory 網域中。請參閱將 vCenter Server 新增到 Active Directory 網域。

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**組態**。

4 在**身分識別提供者**索引標籤上，按一下**身分識別來源**，然後按一下**新增**。

5 選取身分識別來源，然後輸入身分識別來源設定。

選項	說明
Active Directory (整合式 Windows 驗證)	對於原生 Active Directory 實作，請使用此選項。如果您想要使用此選項，則執行 vCenter Single Sign-On 服務所在的機器必須位於 Active Directory 網域。 請參閱 Active Directory 身分識別來源設定。
Active Directory over LDAP	此選項需要您指定網域控制站和其他資訊。請參閱 Active Directory over LDAP 和 OpenLDAP 伺服器身分識別來源設定。
OpenLDAP	對於 OpenLDAP 身分識別來源，請使用此選項。請參閱 Active Directory over LDAP 和 OpenLDAP 伺服器身分識別來源設定。

備註 如果使用者帳戶已鎖定或停用，則 Active Directory 網域中的驗證以及群組和使用者搜尋會失敗。使用者帳戶必須具有使用者和群組 OU 的唯讀存取權，並且必須能夠讀取使用者和群組屬性。依預設，Active Directory 會提供此存取權。使用特殊服務使用者以提升安全性。

6 按一下**新增**。

後續步驟

系統初始會向每個使用者指派「無存取權」的角色。vCenter Server 管理員必須至少為使用者指派「唯讀」角色，使用者才能登入。請參閱 vSphere 安全性說明文件。

Active Directory over LDAP 和 OpenLDAP 伺服器身分識別來源設定

Active Directory over LDAP 身分識別來源優先於 Active Directory (整合式 Windows 驗證) 選項。OpenLDAP 伺服器身分識別來源適用於使用 OpenLDAP 的環境。

如果要設定 OpenLDAP 身分識別來源，請參閱 VMware 知識庫文章 (網址為 http://kb.vmware.com/kb/2064977) 瞭解其他需求。

備註 對 Microsoft Windows 的未來更新將變更 Active Directory 的預設行為，以要求使用強式驗證和加密。此變更會影響 vCenter Server 向 Active Directory 進行驗證的方式。如果您使用 Active Directory 做為 vCenter Server 的身分識別來源，則必須計劃啟用 LDAPS。如需有關此 Microsoft 安全性更新的詳細資訊，請參閱 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 和 https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html。

表 4-3. Active Directory over LDAP 和 OpenLDAP 伺服器設定

選項	說明
名稱	身分識別來源的名稱。
使用者的基本 DN	使用者的基本辨別名稱。輸入要從中開始使用者搜尋的 DN。例如，cn=Users,dc=myCorp,dc=com。
群組的基本 DN	群組的基本辨別名稱。輸入要從中開始群組搜尋的 DN。例如，cn=Groups,dc=myCorp,dc=com。
網域名稱	網域的 FQDN。

表 4-3. Active Directory over LDAP 和 OpenLDAP 伺服器設定 (續)

選項	說明
網域別名	對於 Active Directory 身分識別來源，網域的 NetBIOS 名稱。如果使用 SSPI 驗證，請將 Active Directory 網域的 NetBIOS 名稱新增為身分識別來源的別名。 對於 OpenLDAP 身分識別來源，如果沒有指定別名，則會新增大寫字母的網域名稱。
使用者名稱	網域中使用者的識別碼，該使用者對使用者和群組的基本 DN 僅具有最小唯讀存取權。
密碼	**使用者名稱**所指定使用者的密碼。
連線到	連線到的網域控制站。可以是網域中的任何網域控制站或特定的控制器。
主要伺服器 URL	網域的網域主控站 LDAP 伺服器。 使用 **ldap://hostname:port** 或 **ldaps://hostname:port** 格式。通常為連接埠 389 用於 LDAP 連線，而連接埠 636 用於 LDAPS 連線。對於 Active Directory 多網域控制站部署，通常為連接埠 3268 用於 LDAP，而連接埠 3269 用於 LDAPS。 在主要或次要 LDAP URL 中使用 **ldaps://** 時，需要為 Active Directory 伺服器的 LDAPS 端點建立信任的憑證。
次要伺服器 URL	用於容錯移轉之次要網域控制站 LDAP 伺服器的位址。
SSL 憑證	如果您想要將 LDAPS 用於 Active Directory LDAP 伺服器或 OpenLDAP 伺服器身分識別來源，請按一下**瀏覽**以選取憑證。若要從 Active Directory 匯出根 CA 憑證，請參閱 Microsoft 說明文件。

Active Directory 身分識別來源設定

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

使用 Active Directory (整合式 Windows 驗證)身分識別來源的必要條件

僅在身分識別來源可用的情況下，才能設定 vCenter Single Sign-On 使用該 Active Directory (整合式 Windows 驗證) 身分識別來源。請依照 vCenter Server 組態說明文件中的指示進行操作。

備註 Active Directory (整合式 Windows 驗證) 一律使用 Active Directory 網域樹系的根。若要將您的整合式 Windows 驗證身分識別來源設定為 Active Directory 樹系內的子網域，請參閱 VMware 知識庫文章，網址為 http://kb.vmware.com/kb/2070433。

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

如果您已在 Active Directory 中啟用診斷事件記錄來確定可能需要強化的位置，您可能會在該目錄伺服器上看到事件識別碼為 2889 的記錄事件。使用整合式 Windows 驗證時，事件識別碼 2889 會作為異常產生，而非安全性風險。如需有關事件識別碼 2889 的詳細資訊，請參閱 VMware 知識庫文章，網址為：https://kb.vmware.com/s/article/78644。

表 4-4. 新增身分識別來源設定

文字方塊	說明
網域名稱	網域名稱的 FQDN，例如 mydomain.com。不提供 IP 位址。此網域名稱必須可由 vCenter Server 系統進行 DNS 解析。
使用機器帳戶	選取此選項可將本機機器帳戶用作 SPN。選取此選項時，應僅指定網域名稱。如果您打算重新命名此機器，請勿選取此選項。
使用服務主體名稱 (SPN)	如果您打算重新命名本機機器，請選取此選項。您必須指定 SPN、能夠透過身分識別來源進行驗證的使用者，以及該使用者的密碼。
服務主體名稱 (SPN)	可協助 Kerberos 識別 Active Directory 服務的 SPN。請在名稱中包含網域，例如 STS/`example.com`。 SPN 在網域中必須是唯一的。執行 `setspn -S` 命令可檢查是否未建立任何重複項目。如需 `setspn` 的相關資訊，請參閱 Microsoft 說明文件。
使用者主體名稱 (UPN) **密碼**	能夠透過此身分識別來源進行驗證之使用者的名稱和密碼。請使用電子郵件地址格式，例如 `jchin@mydomain.com`。您可以透過 Active Directory 服務介面編輯器 (ADSI 編輯) 來驗證使用者主體名稱。

使用 CLI 新增或移除身分識別來源

您可以使用 `sso-config` 公用程式來新增或移除身分識別來源。

身分識別來源可以是原生 Active Directory (整合式 Windows 驗證) 網域、AD over LDAP、使用 LDAPS (LDAP over SSL) 的 AD over LDAP，或 OpenLDAP。請參閱具有 vCenter Single Sign-On 的 vCenter Server 的身分識別來源。您也可以使用 `sso-config` 公用程式來設定智慧卡和 RSA SecurID 驗證。

必要條件

如果要新增 Active Directory 身分識別來源，則 vCenter Server 必須位於 Active Directory 網域中。請參閱將 vCenter Server 新增到 Active Directory 網域。

啟用 SSH 登入。請參閱從 vCenter ServerShell 管理 vCenter Server。

程序

1. 使用 SSH 或其他遠端主控台連線，以啟動 vCenter Server 系統上的工作階段。
2. 以 root 身分登入。
3. 變更至 `sso-config` 公用程式所在的目錄。

   ```
   cd /opt/vmware/bin
   ```

4. 若要參閱 `sso-config` 說明，請執行 `sso-config.sh -help`，或參閱 VMware 知識庫文章 (網址為 https://kb.vmware.com/s/article/67304) 以瞭解使用範例。

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

您可以使用 vCenter Single Sign-On 進行 Windows 工作階段驗證 (SSPI)。您必須將 vCenter Server 加入 Active Directory 網域，之後才可以使用 SSPI。

必要條件

- 將 vCenter Server 加入 Active Directory 網域。請參閱將 vCenter Server 新增到 Active Directory 網域。
- 確認已正確設定網域。請參閱 VMware 知識庫文章，網址為 http://kb.vmware.com/kb/2064250。
- 確認已安裝增強型驗證外掛程式。請參閱 vCenter Server 安裝和設定。

備註 當您將 vCenter Server 設定為搭配 Active Directory Federation Services 使用同盟驗證時，增強型驗證外掛程式僅適用於 vCenter Server 為身分識別提供者的組態 (基於 LDAP 的 Active Directory、整合式 Windows 驗證和 OpenLDAP 組態)。

程序

1. 導覽至 vSphere Client 登入頁面。
2. 選取**使用 Windows 工作階段驗證**核取方塊。
3. 使用 Active Directory 使用者名稱和密碼登入。
   - 如果 Active Directory 網域是預設的身分識別來源，請使用您的使用者名稱登入，例如，jlee。
   - 否則請包含網域名稱，例如，jlee@example.com。

管理 Security Token Service

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

做為 Token 簽發者，STS 會使用私密金鑰來簽署 Token，並發佈服務的公用憑證以驗證 Token 簽章。vCenter Single Sign-On 管理 STS 簽署憑證。STS 簽署憑證不會儲存在 VMware Endpoint 憑證存放區 (VECS) 中，而是儲存在 VMware Directory Service (vmdir) 中。Token 的存留期可能很長，在過去可能已由多個金鑰中的任何一個進行簽署。

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

解決方案使用者

有效憑證。

其他使用者

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

STS 會根據主要認證對使用者進行驗證，並建構包含使用者屬性的 SAML Token。依預設，VMWare Certificate Authority (VMCA) 會產生 STS 簽署憑證。您可以使用 CLI 取代預設 STS 簽署憑證，也可以使用 vSphere Client 來更新 STS 簽署憑證。除非您公司的安全性原則要求取代所有憑證，否則請勿取代 STS 簽署憑證。

STS 憑證持續時間和到期時間

vSphere 7.0 Update 1 的全新安裝會建立一個 STS 憑證，其持續時間為 10 年。當 STS 憑證即將到期時，vCenter Server 警示會從 90 天開始每週警告您一次，然後在距離七天時每日警告您一次。

取代 STS 憑證

vCenter Single Sign-On 伺服器包括 Security Token Service (STS)。安全性 Token 服務是一項核發、驗證和續訂安全性 Token 的 Web 服務。您可以取代 STS 使用的憑證。

若要使用公司要求的憑證或更新即將到期的憑證，您可以取代現有的 STS 簽署憑證。如果想要取代預設的 STS 簽署憑證，您必須先產生新的憑證。

STS 憑證有效期為 10 年，且不是對外憑證。如果不是公司的安全政策要求，請勿取代此憑證。

注意 您必須使用此處所述的程序。請勿直接取代檔案系統中的憑證。

必要條件

啟用以透過 SSH 登入 vCenter Server。請參閱從 vCenter ServerShell 管理 vCenter Server。

程序

1. 以根使用者身分登入 vCenter Server Shell。
2. 建立憑證。
   a. 建立頂層目錄以存放新憑證，並確認目錄的位置。

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

   b. 將 `certool.cfg` 檔案複製到新目錄。

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

c 開啟 certool.cfg 檔案的複本，然後對其進行編輯以使用本機 vCenter Server IP 位址和主機名稱。國家/地區是必要的，並且必須是兩個字元，如以下範例所示。

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

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

d 產生金鑰。

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

e 產生憑證。

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

f 建立具有憑證鏈結和私密金鑰的 PEM 檔案。

```
cat newsts.cer /var/lib/vmware/vmca/root.cer sts.key > newsts.pem
```

3 更新 STS 簽署憑證，例如：

```
/opt/vmware/bin/sso-config.sh -set_signing_cert -t vsphere.local /root/newsts/newsts.pem
```

4 重新啟動屬於 ELM 群組的任何 vCenter Server 節點以及任何閘道。

STS 服務和 vSphere Client 都將重新啟動。必須執行重新啟動，驗證才能正常運作。

判定 LDAPS SSL 憑證的到期日期

使用 Active Directory over LDAPS 時，您可以為 LDAP 流量上傳 SSL 憑證。SSL 憑證在預先定義的週期之後到期。您可以檢視憑證的到期日期，以便您知道在憑證到期之前加以取代或更新。

您僅在使用 Active Directory over LDAP 或 OpenLDAP 身分識別來源，並為伺服器指定 ldaps:// URL 時才會看到憑證到期資訊。

程序

1 以根使用者身分登入 vCenter Server。

2 執行下列命令。

```
/opt/vmware/bin/sso-config.sh -get_identity_sources
```

忽略 SLF4J 訊息。

3 若要確定到期日期，請檢視 SSL 憑證的詳細資料並驗證 `NotAfter` 欄位。

管理 vCenter Single Sign-On 原則

vCenter Single Sign-On 原則一般會對本機帳戶和 Token 強制執行安全性規則。您可以檢視和編輯預設 vCenter Single Sign-On 密碼原則、鎖定原則和 Token 原則。

編輯 vCenter Single Sign-On 密碼原則

vCenter Single Sign-On 密碼原則會決定密碼格式和密碼到期。此密碼原則僅適用於 vCenter Single Sign-On 網域 (vsphere.local) 中的使用者。

依預設，vCenter Single Sign-On 內建使用者帳戶密碼會在 90 天後到期。vSphere Client 會在密碼即將到期時提醒您。

請參閱變更 vCenter Single Sign-On 密碼 。

備註 管理員帳戶 (administrator@vsphere.local) 不會遭到鎖定，其密碼也不會到期。適當的安全性做法是透過此帳戶稽核登入，並定期輪替密碼。

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**組態**。

4 按一下**本機帳戶**索引標籤。

5 針對**密碼原則**列按一下**編輯**。

6 編輯密碼原則。

選項	說明
說明	密碼原則說明。
存留時間上限	使用者必須變更密碼前，密碼有效的天數上限。您可以輸入的天數上限為 999999999。若值為零 (0)，表示密碼永遠不會到期。

選項	說明
限制重複使用	無法重複使用的先前密碼的數目。例如，如果您輸入 6，則使用者無法重複使用最近六個密碼中的任何一個。
長度上限	允許密碼包含的字元數上限。
最小長度	密碼必須包含的最小字元數目。最小長度不得少於字母、數字和特殊字元需求的最小總和。
字元需求	密碼必須包含的不同字元類型的最小數目。您可以按照以下方式指定每種類型字元的數目： ■ 特殊字元：& # % ■ 字母：A b c D ■ 大寫：A B C ■ 小寫：a b c ■ 數字：1 2 3 ■ 相同的相鄰：該數值必須大於 0。例如，如果輸入 1，則不允許使用以下密碼：p@$$word。 最小字母字元數不得少於大寫和小寫字元的總和。 在密碼中支援非 ASCII 字元。在舊版 vCenter Single Sign-On 中，受支援的字元則存在限制。

7 按一下**儲存**。

編輯 vCenter Single Sign-On 鎖定原則

如果使用者嘗試使用不正確的認證登入，vCenter Single Sign-On 鎖定原則會指定何時鎖定使用者的 vCenter Single Sign-On 帳戶。管理員可以編輯鎖定原則。

如果使用者多次嘗試使用錯誤的密碼登入 vsphere.local，則使用者將被鎖定。透過鎖定原則，管理員可以指定登入嘗試失敗的次數上限，以及設定兩次失敗之間的時間間隔。該原則還指定在自動解除鎖定帳戶之前必須經過的時間長。

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

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**組態**。

4 按一下**本機帳戶**索引標籤。

5 針對**鎖定原則**列按一下**編輯**。

您可能需要向下捲動才能看到**鎖定原則**列。

6 編輯參數。

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

7 按一下**儲存**。

編輯 vCenter Single Sign-On Token 原則

vCenter Single Sign-On Token 原則會指定 Token 內容，例如時鐘容限和續訂計數。您可以編輯 Token 原則，確保 Token 規格符合貴公司的安全性標準。

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**組態**。

4 按一下**本機帳戶**索引標籤。

5 針對 **Token 可信度**列按一下**編輯**。

您可能需要向下捲動才能看到 **Token 可信度**列。

6 編輯 Token 原則組態參數。

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

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

7 按一下**儲存**。

編輯 Active Directory (整合式 Windows 驗證) 使用者的密碼到期通知

Active Directory 密碼到期通知與 vCenter ServerSSO 密碼到期是分開的。Active Directory 使用者的預設密碼到期通知為 30 天，但實際密碼到期取決於您的 Active Directory 系統。vSphere Client 將控制到期通知。您可以變更預設到期通知，以符合您公司的安全性標準。

必要條件

- 啟用以透過 SSH 登入 vCenter Server。請參閱從 vCenter ServerShell 管理 vCenter Server。

程序

1 以具有管理員權限的使用者身分登入 vCenter ServerShell。

具有超級管理員角色的預設使用者是 root 使用者。

2 將目錄變更為 vSphere Client`webclient.properties` 檔案的位置。

```
cd /etc/vmware/vsphere-ui
```

3 使用文字編輯器開啟 `webclient.properties` 檔案。

4 編輯下列變數。

```
sso.pending.password.expiration.notification.days = 30
```

5 重新啟動 vSphere Client。

```
service-control --stop vsphere-ui
service-control --start vsphere-ui
```

管理 vCenter Single Sign-On 使用者和群組

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

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

新增 vCenter Single Sign-On 使用者

vSphere Client 中**使用者**索引標籤上列出的使用者在 vCenter Single Sign-On 內部，屬於 vsphere.local 網域。您可以從其中一個 vCenter Single Sign-On 管理介面將使用者新增到該網域。

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

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至 vCenter Single Sign-On 使用者組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**使用者和群組**。

4 如果 vsphere.local 不是目前選取的網域，請從下拉式功能表中選取此網域。

您不能將使用者新增到其他網域。

5 在**使用者**索引標籤上，按一下**新增使用者**。

6 輸入新使用者的使用者名稱和密碼。

建立使用者後，將不能變更使用者名稱。密碼必須符合系統的密碼原則需求。

7 (選擇性) 輸入新使用者的名字和姓氏。

8 (選擇性) 輸入此使用者的電子郵件地址和說明。

9 按一下**新增**。

結果

新增使用者時，該使用者最初沒有執行管理作業的權限。

後續步驟

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

停用和啟用 vCenter Single Sign-On 使用者

如果 vCenter Single Sign-On 使用者帳戶停用，則使用者無法登入 vCenter Single Sign-On 伺服器，直到管理員啟用該帳戶。您可以從其中一個 vCenter Single Sign-On 管理介面停用和啟用帳戶。

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

必要條件

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

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至 vCenter Single Sign-On 使用者組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**使用者和群組**。

4 選取使用者名稱，按一下垂直省略符號圖示，然後按一下**停用**。

5 按一下**確定**。

6 若要再次啟用使用者，請依序按一下垂直省略符號圖示、**啟用**以及**確定**。

刪除 vCenter Single Sign-On 使用者

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

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

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至 vCenter Single Sign-On 使用者組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**使用者和群組**。

4 選取**使用者**，然後從下拉式功能表中選取 vsphere.local 網域。

5 在使用者清單中，選取要刪除的使用者，然後按一下垂直省略符號圖示。

6 按一下**刪除**。

請謹慎執行作業。您無法復原此動作。

編輯 vCenter Single Sign-On 使用者

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

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

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

您可以從 vSphere Client 中檢閱 vCenter Single Sign-On 密碼原則。以 administrator@vsphere.local 身分登入，然後從**管理**功能表中，選取**組態 > 本機帳戶 > 密碼原則**。

另請參閱編輯 vCenter Single Sign-On 密碼原則。

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至 vCenter Single Sign-On 使用者組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**使用者和群組**。

4 按一下**使用者**。

5 按一下垂直省略符號圖示，然後選取**編輯**。

6 編輯使用者屬性。

您無法變更使用者名稱。

密碼必須符合系統的密碼原則需求。

7 按一下**確定**。

新增 vCenter Single Sign-On 群組

vCenter Single Sign-On **群組**索引標籤顯示本機網域 (依預設為 vsphere.local) 中的群組。如果需要針對群組成員 (主體) 使用容器，可新增群組。

無法從 vCenter Single Sign-On **群組**索引標籤將群組新增到其他網域 (例如 Active Directory 網域)。

如果未向 vCenter Single Sign-On 新增身分識別來源，建立群組並新增使用者可協助您組織整理本機網域。

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至 vCenter Single Sign-On 使用者組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**使用者和群組**。

4 選取**群組**，然後按一下**新增群組**。

5 輸入群組的名稱與說明。

建立群組後，將不能變更群組名稱。

6 從**新增成員**下拉式功能表中，選取包含要新增至群組之成員的身分識別來源。

如果您已設定外部身分識別提供者 (例如 AD FS) 進行同盟驗證，則可在**新增成員**下拉式功能表中選取此身分識別提供者。

7 輸入搜尋詞彙。

8 選取成員。

您可以新增多個成員。

9 按一下**新增**。

後續步驟

請參閱向 vCenter Single Sign-On 群組新增成員。

向 vCenter Single Sign-On 群組新增成員

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

如需背景資訊，請參閱 VMware 知識庫文章，網址為 http://kb.vmware.com/kb/2095342。

Web 介面中的**群組**索引標籤上所列出的群組屬於 vsphere.local 網域。請參閱 vCenter Single Sign-On 網域中的群組。

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至 vCenter Single Sign-On 使用者組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**使用者和群組**。

4 按一下**群組**索引標籤，然後按一下群組 (例如「管理員」)。

5 從**新增成員**下拉式功能表中，選取包含要新增至群組之成員的身分識別來源。

如果您已設定外部身分識別提供者 (例如 AD FS) 進行同盟驗證，則可在**新增成員**下拉式功能表中選取此身分識別提供者。

6 輸入搜尋詞彙。

7 選取成員。

您可以新增多個成員。

8 按一下**儲存**。

從 vCenter Single Sign-On 群組中移除成員

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

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至 vCenter Single Sign-On 使用者組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**使用者和群組**。

4 選取**群組**，然後按一下群組。

5 在群組成員清單中，選取要移除的使用者或群組，然後按一下垂直省略符號圖示。

6 按一下**移除成員**。

7 按一下**移除**。

結果

使用者從群組中移除，但在系統中仍然可用。

變更 vCenter Single Sign-On 密碼

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

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

備註 您僅可在密碼未到期時變更密碼。

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

程序

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

   如果在安裝期間指定了其他網域，請以 administrator@*mydomain* 身分登入。
3. 在上方的導覽窗格中 [說明] 功能表的右側，按一下您的使用者名稱以彈出下拉式功能表。

   此外，還可以選取 **Single Sign On > 使用者和群組**，然後從垂直省略符號功能表中選取**編輯**。
4. 輸入您目前的密碼。
5. 輸入新密碼並進行確認。

   該密碼必須符合密碼原則。
6. 按一下**儲存**。

瞭解其他驗證選項

從 vSphere 7.0 開始，外部身分識別提供者聯盟是 vCenter Server 的慣用驗證方法。您仍可以使用 Windows 工作階段驗證 (SSPI)、使用智慧卡 (UPN 式通用存取卡，簡稱 CAC)，或使用 RSA SecurID Token 進行驗證。

雙因素驗證方法

政府機關或大型企業經常需要使用雙因素驗證方法。

外部身分識別提供者同盟

外部身分識別提供者同盟可讓您使用外部身分識別提供者支援的驗證機制，包括多重要素驗證。

智慧卡驗證

智慧卡驗證僅為將實體卡片讀卡機連結至所登入電腦的使用者提供存取權。例如，通用存取卡 (CAC) 驗證。

管理員可以部署 PKI，以便讓智慧卡憑證成為 CA 核發的唯一用戶端憑證。對於這種部署，僅提供智慧卡憑證給使用者。使用者選取憑證後，系統會提示輸入 PIN。只有實體卡片和 PIN 都與憑證相符的使用者才能登入。

RSA SecurID 驗證

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

如需詳細資料，請參閱有關 RSA SecurID 設定的兩篇 vSphere 部落格文章。

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

指定非預設驗證方法

管理員可以從 vSphere Client 設定非預設驗證方法，或使用 `sso-config` 指令碼進行設定。

- 對於智慧卡驗證，您可以從 vSphere Client 執行 vCenter Single Sign-On 設定，或使用 `sso-config` 執行。設定包含啟用智慧卡驗證和設定憑證撤銷原則。
- 對於 RSA SecurID，您可使用 `sso-config` 指令碼設定網域的 RSA Authentication Manager，並啟用 RSA Token 驗證。無法從 vSphere Client 設定 RSA SecurID 驗證。然而，如果啟用 RSA SecurID，則該驗證方法會顯示在 vSphere Client 中。

組合使用驗證方法

您可以透過使用 `sso-config` 單獨啟用或停用每種驗證方法。首先，在測試雙因素驗證方法時，將使用者名稱和密碼驗證保留為啟用狀態，然後在測試後，僅設定一種啟用的驗證方法。

智慧卡驗證登入

智慧卡是一張內嵌整合式電路晶片的小塑膠卡。許多政府機關及大型企業均採用通用存取卡 (CAC) 等智慧卡，以增強其系統的安全性並符合安全法規。智慧卡將在每台機器均包含一個智慧卡讀卡機的環境中進行使用。一般會預先安裝用於管理智慧卡的智慧卡硬體磁碟機。

系統會提示登入 vCenter Server 系統的使用者使用智慧卡和 PIN 組合進行驗證，如下所示。

1. 使用者將智慧卡插入智慧卡讀卡機時，瀏覽器會讀取卡片上的憑證。
2. 瀏覽器會提示使用者選取一個憑證，然後提示使用者使用該憑證對應的 PIN。
3. vCenter Single Sign-On 會檢查智慧卡上的憑證是否為已知。如果撤銷檢查已開啟，vCenter Single Sign-On 亦會檢查憑證是否已撤銷。
4. 如果憑證對 vCenter Single Sign-On 來說已知，且不是已撤銷的憑證，則表示使用者已經過驗證，因此可以執行該使用者有權執行的工作。

備註 一般情況下，在測試期間將使用者名稱和密碼驗證保留為啟用狀態有其必要性。測試完成後，停用使用者名稱和密碼驗證並啟用智慧卡驗證。隨後，vSphere Client 將僅允許智慧卡登入。只有在機器上擁有根或管理員權限的使用者，才能透過直接登入至 vCenter Server 來重新啟用使用者名稱和密碼驗證。

設定並使用智慧卡驗證

您可以將環境設定為在使用者透過 vSphere Client 連線到 vCenter Server 時必須進行智慧卡驗證。

設定智慧卡驗證需要先設定反向 Proxy，然後啟用並設定智慧卡驗證本身。您可以使用 `sso-config` 公用程式來管理智慧卡驗證。

設定反向 Proxy 以申請用戶端憑證

在啟用智慧卡驗證之前，您必須先在 vCenter Server 系統上設定反向 Proxy。

vSphere 6.5 及更新版本中需要反向 Proxy 組態。

必要條件

將 CA 憑證複製到 vCenter Server 系統上。

備註 vCenter Server 7.0 支援 HTTP/2 通訊協定。所有新型瀏覽器和應用程式 (包括 vSphere Client) 都使用 HTTP/2 連線至 vCenter Server。但是，智慧卡驗證需要使用 HTTP/1.1 通訊協定。啟用智慧卡驗證會停用 HTTP/2 的應用程式層通訊協定協商 (ALPN，https://tools.ietf.org/html/rfc7301)，從而有效防止瀏覽器使用 HTTP/2。僅使用 HTTP/2 (不依賴 ALPN) 的應用程式會繼續運作。

程序

1. 以 root 使用者身分登入 vCenter Server。
2. 建立信任用戶端 CA 存放區。

   此存放區包含用戶端憑證的信任核發 CA 憑證。此處的用戶端是瀏覽器，智慧卡程序會藉由該瀏覽器提示使用者相關資訊。

   下列範例會顯示如何在 vCenter Server 上建立憑證存放區。

   針對單一憑證：

   ```
   cd /usr/lib/vmware-sso/
   openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer > /usr/lib/vmware-sso/vmware-sts/
   conf/clienttrustCA.pem
   ```

   針對多個憑證：

   ```
   cd /usr/lib/vmware-sso/
   openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer >> /usr/lib/vmware-sso/vmware-sts/
   conf/clienttrustCA.pem
   ```

3. 對包括反向 Proxy 定義的 `/etc/vmware-rhttpproxy/config.xml` 檔案進行備份，然後在編輯器中開啟 `config.xml`。
4. 進行下列變更，然後儲存檔案。

   ```
   <http>
   <maxConnections> 2048 </maxConnections>
   ```

```
<requestClientCertificate>true</requestClientCertificate>
<clientCertificateMaxSize>4096</clientCertificateMaxSize>
<clientCAListFile>/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem</clientCAListFile>
</http>
```

`config.xml` 檔案包含其中某些元素。根據需要取消註解、更新或新增元素。

5 重新啟動服務。

```
/usr/lib/vmware-vmon/vmon-cli --restart rhttpproxy
```

使用命令列管理智慧卡驗證

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

您可以在以下位置找到 `sso-config` 指令碼：

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

支援的驗證類型和撤銷設定的組態儲存在 VMware Directory Service 中，並於 vCenter Single Sign-On 網域中的所有 vCenter Server 執行個體之間複寫。

如果使用者名稱和密碼驗證已停用，並且智慧卡驗證出現問題，則使用者無法登入。在這種情況下，根使用者或管理員使用者可以從 vCenter Server 命令列開啟使用者名稱和密碼驗證。下列命令可啟用使用者名稱和密碼驗證。

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

如果您使用預設承租人，請使用 vsphere.local 做為承租人名稱。

如果使用 OCSP 進行撤銷檢查，您可以仰賴在智慧卡憑證 AIA 延伸中指定的預設 OCSP。您還可以覆寫預設值並設定一或多個備用 OCSP 回應程式。例如，您可以設定 vCenter Single Sign-On 站台的本機 OCSP 回應程式，使其處理撤銷檢查要求。

備註 如果您的憑證未定義 OCSP，請改為啟用 CRL (憑證撤銷清單)。

必要條件

- 確認環境中已設定企業公開金鑰基礎結構 (PKI)，並且憑證符合下列需求：
  - 使用者主體名稱 (UPN) 必須與主體別名 (SAN) 延伸中的 Active Directory 帳戶相對應。
  - 憑證必須在 [應用程式原則] 或 [增強金鑰使用方法] 欄位中指定 [用戶端驗證]，否則瀏覽器不會顯示該憑證。
- 將 Active Directory 身分識別來源新增到 vCenter Single Sign-On。
- 將 vCenter Server 管理員角色指派給 Active Directory 身分識別來源中的一或多個使用者。然後，這些使用者便可以執行管理工作，因為他們可以驗證並具有 vCenter Server 管理員權限。
- 確保您已設定反向 Proxy，並重新啟動實體或虛擬機器。

程序

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

a 直接登入或使用 SSH 登入應用裝置主控台。

b 按如下方式啟用應用裝置 shell。

```
shell
chsh -s "/bin/bash" root
```

c 使用 WinSCP 或類似公用程式將憑證複製到 vCenter Server 上的 `/usr/lib/vmware-sso/vmware-sts/conf`。

d 按如下方式選擇性地停用 shell。

```
chsh -s "/bin/appliancesh" root
```

2 若要啟用智慧卡驗證，請執行以下命令。

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

例如：

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

使用逗點分隔多個憑證，但是不要在逗點後加空格。

3 若要停用所有其他驗證方法，請執行以下命令。

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

4 (選擇性) 若要設定憑證原則允許清單，請執行以下命令。

```
sso-config.sh -set_authn_policy -certPolicies policies
```

若要指定多個原則，請用逗號加以分隔，例如：

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

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

5 (選擇性) 使用 OCSP 開啟和設定撤銷檢查。

a 使用 OCSP 開啟撤銷檢查。

```
sso-config.sh  -set_authn_policy -t tenantName  -useOcsp true
```

b 如果 OCSP 回應程式連結不是透過憑證的 AIA 延伸提供的，請提供覆寫 OCSP 回應程式 URL 及 OCSP 授權機構核發的憑證。

為每個 vCenter Single Sign-On 站台設定備用 OCSP。您可以為 vCenter Single Sign-On 站台指定多個備用 OCSP 回應程式以允許容錯移轉。

```
sso-config.sh -t tenant -add_alt_ocsp  [-siteID yourPSCClusterID] -ocspUrl http://
ocsp.xyz.com/ -ocspSigningCert yourOcspSigningCA.cer
```

備註 依預設，組態會套用至目前的 vCenter Single Sign-On 站台。僅當您為其他 vCenter Single Sign-On 站台設定備用 OCSP 時，指定 `siteID` 參數。

請考慮下列範例。

```
 .sso-config.sh -t vsphere.local -add_alt_ocsp -ocspUrl http://
failover.ocsp.nsn0.rcvs.nit.disa.mil/ -ocspSigningCert ./
DOD_JITC_EMAIL_CA-29__0x01A5__DOD_JITC_ROOT_CA_2.cer
 Adding alternative OCSP responder for tenant :vsphere.local
 OCSP responder is added successfully!
 [
 site::   78564172-2508-4b3a-b903-23de29a2c342
     [
     OCSP url::   http://ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
     [
     OCSP url::   http://failover.ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
 ]
```

c 若要顯示目前的備用 OCSP 回應程式設定，請執行以下命令。

```
sso-config.sh -t tenantName -get_alt_ocsp]
```

d 若要移除目前的備用 OCSP 回應程式設定，請執行以下命令。

```
sso-config.sh -t tenantName -delete_alt_ocsp [-allSite] [-siteID
pscSiteID_for_the_configuration]
```

6 (選擇性) 若要列出組態資訊，請執行以下命令。

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

管理智慧卡驗證

您可以在 vSphere Client 中啟用和停用智慧卡驗證、自訂登入橫幅和設定撤銷原則。

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

如果使用者名稱和密碼驗證已停用，並且智慧卡驗證出現問題，則使用者無法登入。在這種情況下，根使用者或管理員使用者可以從 vCenter Server 命令列開啟使用者名稱和密碼驗證。下列命令可啟用使用者名稱和密碼驗證。

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

必要條件

- 確認環境中已設定企業公開金鑰基礎結構 (PKI)，並且憑證符合下列需求：
  - 使用者主體名稱 (UPN) 必須與主體別名 (SAN) 延伸中的 Active Directory 帳戶相對應。
  - 憑證必須在 [應用程式原則] 或 [增強金鑰使用方法] 欄位中指定 [用戶端驗證]，否則瀏覽器不會顯示該憑證。
- 將 Active Directory 身分識別來源新增到 vCenter Single Sign-On。
- 將 vCenter Server 管理員角色指派給 Active Directory 身分識別來源中的一或多個使用者。然後，這些使用者便可以執行管理工作，因為他們可以驗證並具有 vCenter Server 管理員權限。
- 確保您已設定反向 Proxy，並重新啟動實體或虛擬機器。

程序

1. 取得憑證，並將其複製到 `sso-config` 公用程式可存取的資料夾中。
   a. 直接登入或使用 SSH 登入 vCenter Server 主控台。
   b. 按如下方式啟用 shell。

      ```
      shell
      chsh -s "/bin/bash" root
      csh -s "bin/appliance/sh" root
      ```

   c. 使用 WinSCP 或類似公用程式將憑證複製到 vCenter Server 上的 `/usr/lib/vmware-sso/vmware-sts/conf` 目錄。
   d. 按如下方式選擇性地停用應用裝置 shell。

      ```
      chsh -s "/bin/appliancesh" root
      ```

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

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

4 導覽至組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**組態**。

5 在**身分識別提供者**索引標籤下，按一下**智慧卡驗證**，然後按一下**編輯**。

6 選取或取消選取驗證方法，然後按一下**儲存**。

您可以單獨選擇智慧卡驗證，也可以同時選擇智慧卡驗證以及密碼與 Windows 工作階段驗證。

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

受信任的 CA 憑證隨即顯示。

7 在**受信任的 CA 憑證**索引標籤中，按一下**新增**，然後按一下**瀏覽**。

8 從受信任的 CA 選取所有憑證，然後按一下**新增**。

後續步驟

您的環境可能需要增強型 OCSP 組態。

- 如果您的 OCSP 回應是由智慧卡簽署 CA 以外的其他 CA 核發，請提供 OCSP 簽署 CA 憑證。
- 您可以為多站台部署中的每個 vCenter Server 站台設定一或多個本機 OCSP 回應程式。您可以使用 CLI 設定這些備用 OCSP 回應程式。請參閱使用命令列管理智慧卡驗證。

設定智慧卡驗證的撤銷原則

您可以自訂憑證撤銷檢查，並可指定 vCenter Single Sign-On 尋找已撤銷憑證之相關資訊的位置。

您可以使用 vSphere Client 或 `sso-config` 指令碼自訂行為。您選取的設定部分取決於 CA 的支援情況。

- 如果停用撤銷檢查，vCenter Single Sign-On 將略過任何 CRL 或 OCSP 設定。vCenter Single Sign-On 不會對任何憑證執行檢查。
- 如果啟用撤銷檢查，則設定取決於 PKI 設定。

  僅使用 OCSP

  如果核發 CA 支援 OCSP 回應程式，請啟用 **OCSP** 並停用 **CRL 做為 OCSP 的容錯移轉**。

  僅使用 CRL

  如果核發 CA 不支援 OSCP，請啟用 **CRL 檢查**並停用 **OSCP 檢查**。

  同時使用 OSCP 和 CRL

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

- 如果啟用撤銷檢查，進階使用者可以指定下列其他設定。

  OSCP URL

依預設，vCenter Single Sign-On 將檢查正在接受驗證之憑證中所定義的 OCSP 回應程式的位置。如果憑證中不存在授權資訊存取延伸，或者您想要將其覆寫，您可以明確指定位置。

使用來自憑證的 CRL

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

CRL 位置

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

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

必要條件

- 確認環境中已設定企業公開金鑰基礎結構 (PKI)，並且憑證符合下列需求：
  - 使用者主體名稱 (UPN) 必須與主體別名 (SAN) 延伸中的 Active Directory 帳戶相對應。
  - 憑證必須在 [應用程式原則] 或 [增強金鑰使用方法] 欄位中指定 [用戶端驗證]，否則瀏覽器不會顯示該憑證。
- 確認 vCenter Server 憑證受使用者的工作站信任。否則，瀏覽器不會嘗試驗證。
- 將 Active Directory 身分識別來源新增到 vCenter Single Sign-On。
- 將 vCenter Server 管理員角色指派給 Active Directory 身分識別來源中的一或多個使用者。然後，這些使用者便可以執行管理工作，因為他們可以驗證並具有 vCenter Server 管理員權限。

程序

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

   如果在安裝期間指定了其他網域，請以 administrator@*mydomain* 身分登入。
3. 導覽至組態 UI。
   a 從**首頁**功能表中，選取**管理**。
   b 在 **Single Sign On** 下，按一下**組態**。
4. 在**身分識別提供者**索引標籤下，按一下**智慧卡驗證**。
5. 按一下**憑證撤銷**，然後按一下**編輯**以啟用或停用撤銷檢查。
6. 如果憑證原則已在您的環境中生效，您可以在**憑證原則**窗格中新增原則。

設定 RSA SecurID 驗證

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

如需詳細資料，請參閱有關 RSA SecurID 設定的兩篇 vSphere 部落格文章。

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

必要條件

- 確認已正確設定您環境中的 RSA Authentication Manager，且使用者擁有 RSA Token。需要 RSA Authentication Manager 8.0 版或更新版本。
- 確認已將 RSA Manager 使用的身分識別來源新增至 vCenter Single Sign-On。請參閱新增或編輯 vCenter Single Sign-On 身分識別來源。
- 確認 RSA Authentication Manager 系統能夠解析 vCenter Server 主機名稱，並且 vCenter Server 系統能夠解析 RSA Authentication Manager 主機名稱。
- 透過選取**存取 > 驗證代理程式 > 產生組態檔**，從 RSA Manager 匯出 `sdconf.rec` 檔案。若要尋找 `sdconf.rec` 檔案，請解壓縮產生的 `AM_Config.zip` 檔案。
- 將 `sdconf.rec` 檔案複製到 vCenter Server 節點。

程序

1. 變更至 `sso-config` 指令碼所在的目錄。

   ```
   /opt/vmware/bin
   ```

2. 若要啟用 RSA SecurID 驗證，請執行以下命令。

   ```
   sso-config.sh  -t tenantName  -set_authn_policy -securIDAuthn true
   ```

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

3. (選擇性) 若要停用其他驗證方法，請執行以下命令。

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

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

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

   例如：

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

您可以指定下列選項。

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

5 (選擇性) 若要將承租人組態變更為非預設值，請執行下列命令。

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

預設值通常是適用的，例如：

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

6 (選擇性) 如果您的身分識別來源未使用使用者主體名稱做為使用者識別碼，請設定身分識別來源 userID 屬性。(僅限 Active Directory over LDAP 身分識別來源支援的情況。)

userID 屬性可判定哪個 LDAP 屬性會用做 RSA userID。

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

例如：

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

7 若要顯示目前設定，請執行下列命令。

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

結果

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

備註 使用 ***userID@domainName*** 或 ***userID@domain_upn_suffix*** 使用者名稱格式。

管理登入訊息

您可以建立使用者登入時顯示的登入訊息。

您可以設定訊息、免責聲明或條款與條件。此外，您也可以將訊息設定為在登入前需要確認訊息。

管理登入訊息

您可以在環境中加入登入訊息。您可以啟用和停用登入訊息，也可以要求使用者按一下 [明確同意] 核取方塊。

程序

1 使用 vSphere Client 登入 vCenter Server。

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

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

3 導覽至組態 UI。

a 從**首頁**功能表中，選取**管理**。

b 在 **Single Sign On** 下，按一下**組態**。

4 按一下**登入訊息**索引標籤。

5 按一下**編輯**並設定登入訊息。

選項	說明
顯示登入訊息	切換開啟**顯示登入訊息**以啟用登入訊息。除非您開啟此交換器，否則無法對登入訊息進行變更。
登入訊息	訊息的標題。依預設，當**同意**核取方塊切換開啟時，登入訊息文字為 `I agree to Terms and Conditions`。您必須將 `Terms and Conditions` 取代為您自己的文字。如果**同意**核取方塊已關閉，則會顯示 `Login message`，您可以透過此項輸入您的訊息。
[同意] 核取方塊	切換開啟**同意**核取方塊來要求使用者在登入前按一下核取方塊。也可以顯示不含核取方塊的訊息。
登入訊息的詳細資料	按一下登入訊息時使用者所看到的訊息，例如，條款與條件的文字。您必須在此文字方塊中輸入部分詳細資料。

6 按一下**儲存**。

vCenter Single Sign-On 安全性最佳做法

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

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

檢查密碼到期

預設 vCenter Single Sign-On 密碼原則的密碼存留時間為 90 天。密碼將在 90 天後到期，然後您無法再登入。檢查到期並及時重新整理密碼。

設定 NTP

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

NTP 還可讓您更輕鬆地追蹤記錄檔中的侵入者。不正確的時間設定讓您難以檢查和關聯要偵測攻擊的記錄檔，且會導致稽核不準確。

疑難排解驗證

5

以下主題提供 vCenter Server 驗證問題疑難排解的起點。如需其他指示，請搜尋此說明文件中心和 VMware 知識庫系統。

本章節討論下列主題：

判定 Lookup Service 錯誤的原因

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

問題

vCenter Server 和 Web Client 安裝程式顯示錯誤 `Could not contact Lookup Service. Please check VM_ssoreg.log...`。

原因

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

解決方案

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

   在該訊息中，系統暫存資料夾指的是 `%TEMP%`。

3 在記錄檔中，搜尋以下訊息。

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

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

無法使用 Active Directory 網域驗證登入

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

問題

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

原因

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

解決方案

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

若要將您的整合式 Windows 驗證身分識別來源設定為 Active Directory 樹系內的子網域，請參閱 VMware 知識庫文章，網址為 http://kb.vmware.com/kb/2070433。依預設，整合式 Windows 驗證會使用 Active Directory 樹系的根網域。

如果變更預設身分識別來源未能解決此問題，則執行以下額外的疑難排解步驟。

1 同步 vCenter Server 和 Active Directory 網域控制器之間的時鐘。

2 確認每個網域控制站在 Active Directory 網域 DNS 服務中是否均有指標記錄 (PTR)。

確認網域控制站的 PTR 記錄資訊與控制器的 DNS 名稱是否相符。使用 vCenter Server 時，請執行以下命令來執行此工作：

a 若要列出網域控制站，請執行以下命令：

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

相關位址位於回答區段，如以下範例中所示：

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

b 對於每個網域控制站，請執行以下命令來驗證正向和反向解析：

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

相關位址位於回答區段，如以下範例中所示：

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

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

相關位址位於回答區段，如以下範例中所示：

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

3 如果執行上述步驟未能解決問題，請從 Active Directory 網域中移除 vCenter Server，然後重新加入網域。請參閱 vCenter Server 組態說明文件。

4 關閉所有連線到 vCenter Server 的瀏覽器工作階段，然後重新啟動所有服務。

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

由於使用者帳戶被鎖定，vCenter Server 登入失敗

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

問題

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

原因

您已超過嘗試登入失敗的次數上限。

解決方案

- 如果您嘗試以系統網域 (預設為 vsphere.local) 中的使用者登入，請要求您的 vCenter Single Sign-On 管理員解除鎖定您的帳戶。如果鎖定在鎖定原則中設為到期，您可以等候直到帳戶解除鎖定。vCenter Single Sign-On 管理員可以使用 CLI 命令來解除鎖定您的帳戶。
- 如果您做為 Active Directory 或 LDAP 網域中的使用者身分登入，請要求您的 Active Directory 或 LDAP 管理員解除鎖定您的帳戶。

VMware 目錄服務複寫可能需要很長時間

如果您的環境包含多個透過增強型連結模式連線的 vCenter Server 執行個體，而當其中一個 vCenter Server 執行個體無法使用時，您的環境會繼續正常運作。當 vCenter Server 重新恢復可用時，通常會使用透過增強型連結模式連線的合作夥伴在 30 秒內複寫使用者資料及其他資訊。但是，在某些情況下，複寫可能需要很長時間。

問題

例如，在某些情況下，當您的環境包含多個位於不同位置的 vCenter Server 執行個體，並且您在某個 vCenter Server 無法使用時進行了重大變更，則跨 VMware 目錄服務執行個體的複寫不會立即開始。例如，在複寫完成之前，新增到可用 vCenter Server 執行個體的新使用者不會出現在另一個執行個體中。複寫可能需要很長時間，視您的增強型連結模式拓撲而定。

原因

在一般作業期間，於某個 vCenter Server 執行個體 (節點) 中對 VMware 目錄服務 (vmdir) 執行個體所做的變更，會於約 30 秒內顯示在其直接複寫合作夥伴中。視複寫拓撲而定，某個節點中的變更可能必須透過中繼節點傳播，才能到達每個節點中的各個 vmdir 執行個體。複寫的資訊包括使用 VMware vMotion 建立、複製或移轉之虛擬機器的使用者資訊、憑證資訊、授權資訊及更多資訊。

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

解決方案

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

匯出 vCenter Server 支援服務包

您可以透過 vSphere Client 或使用 API，匯出包含 vCenter Server 服務之記錄檔的支援服務包。匯出後，您可以本機深入瞭解記錄或將服務包傳送到 VMware 支援。

如需有關 API 的詳細資訊，請參閱《vCenter Server 管理程式設計指南》。

必要條件

確認 vCenter Server 已成功部署且正在執行。

程序

1. 從網頁瀏覽器連線至 vCenter Server 組態管理介面，網址為 https://*vcenter_server_ip*:5480。
2. 對於 vCenter Server，以 root 使用者身分登入。
3. 從**動作**功能表中，選取**建立支援服務包**。
4. 除非瀏覽器設定阻止立即下載，否則支援服務包會儲存到本機電腦。

驗證服務記錄參考

vCenter Server 驗證服務使用 Syslog 進行記錄。您可以檢查記錄檔以判斷失敗的原因。

表 5-1. 服務記錄

服務	說明
VMware 目錄服務	依預設，vmdir 記錄會儲存至 `/var/log/messages` 或 `/var/log/vmware/vmdird/`。 針對部署時發生的問題，`/var/log/vmware/vmdir/vmafdvmdirclient.log` 可能也包含有用的疑難排解資料。
VMware Single Sign-On	vCenter Single Sign-On 記錄會儲存至 `/var/log/vmware/sso/`。
VMWare Certificate Authority (VMCA)	VMCA 服務記錄位於 `/var/log/vmware/vmcad/vmcad-syslog.log`。
VMware Endpoint 憑證存放區 (VECS)	VECS 服務記錄位於 `/var/log/vmware/vmafdd/vmafdd-syslog.log`。
VMware Lookup Service	Lookup Service 記錄位於 `/var/log/vmware/sso/lookupServer.log`。