部署及設定 Access Point

Unified Access Gateway 2.8

vmware®

您可以在 VMware 網站上找到最新的技術說明文件，網址為:

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

如果您對此文件有何想法，請將您的回應意見提交至：

docfeedback@vmware.com

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

內容

部署及設定 VMware Access Point

*《部署及設定 Access Point》*提供設計 VMware Horizon®、VMware Identity Manager™ 和 VMware AirWatch® 部署的相關資訊，這些部署使用 VMware Access Point™ 來提供對組織應用程式的安全外部存取。這些應用程式可以是 Windows 應用程式、軟體即服務 (SaaS) 應用程式和桌面平台。本指南也提供部署 Access Point 虛擬應用裝置以及在部署後變更組態設定的相關指示。

主要對象

此資訊適用於想要部署和使用 Access Point 應用裝置的任何人。本資訊是專為具有經驗且熟悉虛擬機器技術和資料中心作業的 Linux 和 Windows 系統管理員所撰寫。

準備部署 Access Point

1

針對想從公司防火牆外部存取遠端桌面平台和應用程式的使用者，Access Point 可做為安全閘道使用。

本章節討論下列主題:

Access Point 作為安全閘道

Access Point 為第 7 層安全性應用裝置，通常安裝在非軍事區 (DMZ) 中。Access Point 可用來確保只有進入公司資料中心的流量是代表經過嚴格驗證的遠端使用者流量。

Access Point 會將驗證要求導向至適當的伺服器，並捨棄所有未經驗證的要求。使用者只能存取其有權存取的資源。

Access Point 虛擬應用裝置還能確保經過驗證之使用者的流量只能導向該使用者真正有權使用的桌面平台和應用程式資源。這個層級的保護涉及具體檢測桌面平台通訊協定、協調可能迅速變動的原則和網路位址，以便精確地控制存取權限。

Access Point 應用裝置通常位於網路非軍事區 (DMZ) 內，做為公司信任網路中的連線 Proxy 主機。這種設計可為虛擬桌面平台、應用程式主機以及伺服器阻擋面向公眾的網際網路，因此提供了額外一層的安全保護。

Access Point 是專為 DMZ 設計的強化安全應用裝置。以下是實作的強化設定。

- 最新 Linux 核心和軟體修補程式
- 適用於網際網路和內部網路流量的多重 NIC 支援
- 已停用 SSH
- 已停用 FTP、Telnet、Rlogin 或 Rsh 服務
- 已停用不需要的服務

使用 Access Point 而非虛擬私人網路

Access Point 與通用 VPN 解決方案很類似，因為它們都可確保僅在代表經過嚴格驗證的使用者時，才會將流量轉送至內部網路。

Access Point 優於通用 VPN 的方面包括下列項目。

- Access Control Manager。Access Point 會自動套用存取規則。Access Point 會識別使用者的使用權利，以及內部連線所需的位址 (可能會快速變更)。VPN 也有相同的功效，因為大多數的 VPN 允許管理員分別針對每位使用者或使用者群組設定網路連線規則。剛開始，使用 VPN 可以順利運作，但需要投入大量的管理工作來維護必要規則。
- 使用者介面。Access Point 不會變更簡潔的 Horizon Client 使用者介面。利用 Access Point，當 Horizon Client 啟動時，經驗證的使用者會在其 View 環境中，並對其桌面平台和應用程式擁有受控制的存取權。根據 VPN 的要求，您必須先設定 VPN 軟體並分別進行驗證，然後才能啟動 Horizon Client。
- 效能。Access Point 是專為將安全性和效能最大化而設計。有了 Access Point，您不需要其他封裝就可以保護 PCoIP、HTML Access 及 WebSocket 通訊協定。VPN 會實作為 SSL VPN。此實作可滿足安全需求，而且在啟用傳輸層安全性 (Transport Layer Security, TLS) 的情況下，我們都會認為它們是安全的，不過使用 SSL/TLS 的基礎通訊協定只是以 TCP 為基礎。論及利用無連線 UDP 式傳輸的現代化視訊遠端通訊協定，當強制透過 TCP 型傳輸時，其效能優勢可能會大打折扣。這種說法不見得適用於所有 VPN 技術，因為能額外與 DTLS 或 IPsec (而非 SSL/TLS) 協同作業的技術也能與 View 桌面平台通訊協定搭配運作。

Access Point 系統和網路需求

若要部署 Access Point 應用裝置，請確定您的系統符合硬體和軟體需求。

支援的 VMware 產品版本

您必須對特定版本的 Access Point 使用特定版本的 VMware 產品。請參閱產品版本說明以取得關於相容性的最新資訊，並參閱 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php 上的 VMware 產品互通性對照表。版本說明和互通性對照表中的資訊會取代本指南中的資訊。

Access Point 2.8 可用作搭配下列 VMware 產品使用的安全閘道。

- Vmware AirWatch 8.4 及更新版本
- VMware Identity Manager 2.7 及更新版本
- VMware Horizon 6.2 及更新版本
- VMware Horizon Air Hybrid Mode 1.0 及更新版本
- VMware Horizon Air 15.3 及更新版本

ESXi 伺服器的硬體需求

部署 Access Point 應用裝置的 vSphere 版本必須與 Horizon 產品支援的版本以及您使用的版本相同。

如果您計劃使用 vSphere Web Client，請確認已安裝用戶端整合外掛程式。如需詳細資訊，請參閱 vSphere 說明文件。開始部署精靈之前，若未安裝此外掛程式，精靈會提示您安裝外掛程式。這需要您關閉瀏覽器並結束精靈。

備註 在 Access Point 應用裝置上設定時鐘 (UTC)，讓應用裝置擁有正確的時間。例如，開啟 Access Point 虛擬機器上的主控台視窗，然後使用箭頭按鈕選取正確的時區。另外，確認 ESXi 主機的時間是否與 NTP 伺服器同步，並確認在應用裝置虛擬機器上執行的 VMware Tools 會將虛擬機器的時間與 ESXi 主機的時間同步。

虛擬應用裝置需求

Access Point 應用裝置的 OVF 套件會自動選取 Access Point 需要的虛擬機器組態。雖然您可以變更這些設定，但 VMware 建議您不要將 CPU、記憶體或磁碟空間變更為比預設 OVF 設定還要小的值。

確定您要用於應用裝置的資料存放區具備足夠的可用磁碟空間，並符合其他系統需求。

- 虛擬應用裝置下載大小為 2.5 GB
- 精簡佈建磁碟最低需求為 2.5 GB
- 完整佈建磁碟最低需求為 20 GB

需要下列資訊才能部署虛擬應用裝置

- 靜態 IP 位址
- DNS 伺服器的 IP 位址
- 根使用者的密碼
- Access Point 應用裝置所指向的負載平衡器伺服器執行個體的 URL

網路功能組態需求

您可以使用一個、兩個或三個網路介面，Access Point 要求替每個網路介面設定不同的靜態 IP 位址。許多 DMZ 實作使用分開的網路來保護不同的流量類型。請根據 Access Point 部署所在之 DMZ 的網路設計來對其設定。

- 一個網路介面適合用於 POC (概念證明) 或測試用途。使用一個 NIC 時，外部、內部和管理流量都在同一個子網路上。
- 使用兩個網路介面時，外部流量位於一個子網路上，內部和管理流量位於另一個子網路上。
- 使用三個網路介面是最安全的選項。使用第三個 NIC 時，外部、內部和管理流量都能擁有自己的子網路。

重要事項 請確認您已指派 IP 集區給每個網路。Access Point 應用裝置接著便可以在部署時提取子網路遮罩和閘道設定。若要在 vCenter Server 中新增 IP 集區，如果您使用的是原生 vSphere Client，請前往資料中心的 **IP 集區**索引標籤。或者，如果您使用 vSphere Web Client，則可以建立網路通訊協定設定檔。前往資料中心的**管理**索引標籤，並選取**網路通訊協定設定檔**索引標籤。如需詳細資訊，請參閱設定虛擬機器網路的通訊協定設定檔。

記錄保留需求

記錄檔依預設會設定成使用特定數量的空間，且該數量會小於彙總中的磁碟大小總計。Access Point 的記錄檔依預設會輪替。您必須使用 syslog 保存這些記錄項目。請參閱 從 Access Point 應用裝置收集記錄。

DMZ 型 Access Point 應用裝置的防火牆規則

DMZ 型 Access Point 應用裝置需要在前端和後端防火牆設定某些防火牆規則。在安裝期間，Access Point 服務預設設為接聽特定網路連接埠。

DMZ 型 Access Point 應用裝置部署通常包含兩個防火牆。

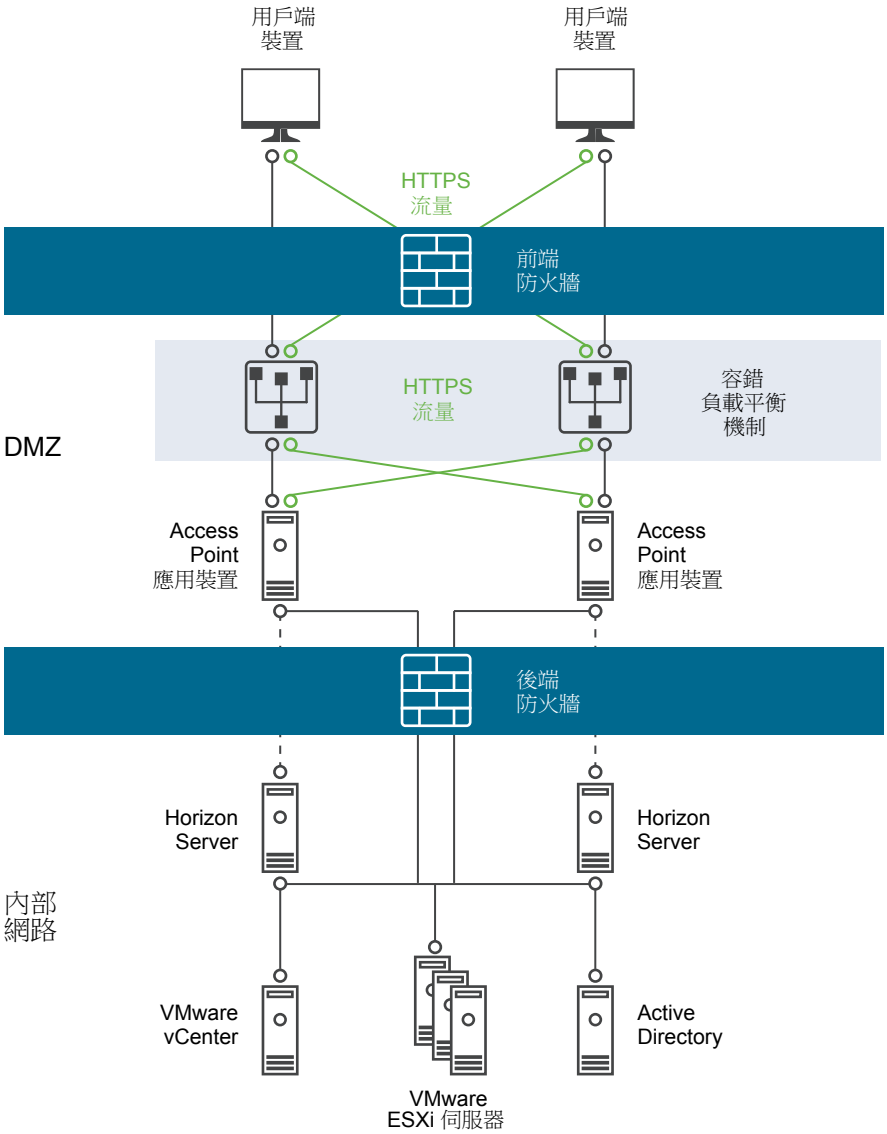
- 保護 DMZ 和內部網路需要面向外部網路的前端防火牆。您可以設定此防火牆允許外部網路流量到達 DMZ。
- 提供第二層安全性則需要位於 DMZ 與內部網路之間的後端防火牆。您可以設定此防火牆僅接受發自 DMZ 內服務的流量。

防火牆原則可嚴格控制來自 DMZ 服務的輸入通訊，進而大幅降低內部網路出現漏洞的風險。

若要允許外部用戶端裝置連線至 DMZ 內的 Access Point 應用裝置，前端防火牆必須允許特定連接埠上的流量。依預設，外部用戶端裝置和外部 Web 用戶端 (HTML Access) 會透過 TCP 連接埠 443 連接 DMZ 內的 Access Point 應用裝置。如果您使用 Blast 通訊協定，則必須在防火牆上開啟連接埠 443。如果您使用 PCOIP 通訊協定，則必須在防火牆上開啟連接埠 4172。

下圖顯示包含前端和後端防火牆的組態範例。

圖 1-1 雙防火牆拓撲



Access Point 負載平衡拓撲

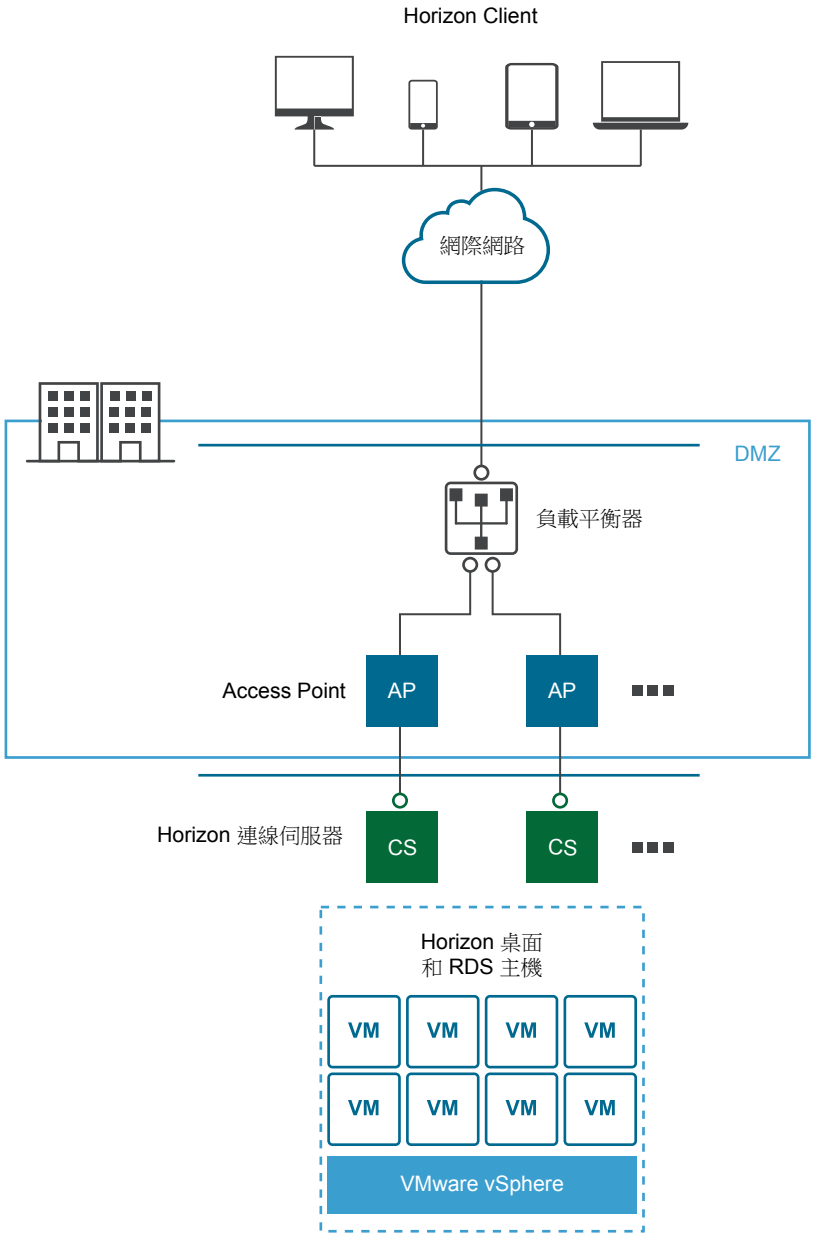
您可以實作數個不同的拓撲。

DMZ 中的 Access Point 應用裝置可以設定為指向某個伺服器或位於一組伺服器前方的負載平衡器。Access Point 應用裝置可與設定為使用 HTTPS 的標準第三方負載平衡解決方案搭配運作。

若 Access Point 應用裝置指向伺服器前方的負載平衡器，在選擇伺服器執行個體時就不會固定不變。例如，負載平衡器可能會根據可用性以及負載平衡器所知道的每個伺服器執行個體上目前的工作階段數目來做出選擇。公司防火牆內部的伺服器執行個體通常具備負載平衡器，以便支援內部存取。在使用 Access Point 時，您可以將 Access Point 應用裝置指向這個通常已在使用中的相同負載平衡器。

您也可以讓一或多個 Access Point 應用裝置指向某一個伺服器執行個體。在這兩種方法中，都請在 DMZ 中的兩部 (含) 以上 Access Point 應用裝置前方使用負載平衡器。

圖 1-2 負載平衡器後方的多個 Access Point 應用裝置



Horizon 通訊協定

當 Horizon Client 使用者連接至 Horizon 環境時，系統會使用數個不同的通訊協定。第一個連線一律會是透過 HTTPS 的主要 XML-API 通訊協定。在成功驗證之後，系統也會建立一或多個次要通訊協定。

- 主要 Horizon 通訊協定

使用者在 Horizon Client 輸入主機名稱，而這會啟動主要 Horizon 通訊協定。這是用於驗證授權和工作階段管理的控制通訊協定。它會透過 HTTPS (透過 SSL 的 HTTP) 使用 XML 結構化訊息。此通訊協定有時稱為 Horizon XML-API 控制通訊協定。在以上「負載平衡器後方的多個 Access Point 應用裝置」圖片所示的負載平衡環境中，負載平衡器會將此連線路由傳送至其中一個 Access Point 應用裝置。負載平衡器一般會先根據可用性選取應用裝置，然後根據目前工作階段的最小數量，從可用應用裝置路由傳送流量。此組態會在可用的一組 Access Point 應用裝置之間，從不同的用戶端平均散佈流量

- 次要 Horizon 通訊協定

  在 Horizon Client 對其中一個 Access Point 應用裝置建立安全通訊之後，使用者隨即進行驗證。如果此驗證嘗試成功，則會從 Horizon Client 建立一或多個次要連線。這些次要連線可以包括下列項目

  - 用於封裝 TCP 通訊協定的 HTTPS 通道，例如 RDP、MMR/CDR 和用戶端架構通道。(TCP 443)。
  - Blast Extreme 顯示通訊協定 (TCP 443 和 UDP 443)。
  - PCoIP 顯示通訊協定 (TCP 4172 和 UDP 4172)。

這些次要 Horizon 通訊協定必須路由傳送至路由傳送主要 Horizon 通訊協定的相同 Access Point 應用裝置。然後 Access Point 即可根據經過驗證的使用者工作階段來授權次要通訊協定。Access Point 的一項重要安全性功能是，僅在流量代表經過驗證的使用者時，Access Point 才會將流量轉送至公司資料中心。如果錯誤地將次要通訊協定路由傳送至不同的 Access Point 應用裝置，而非主要通訊協定應用裝置，則系統不會對其授權，且會放置在 DMZ 中。連線失敗。如果未正確設定負載平衡器，則錯誤地路由傳送次要通訊協定屬於常見問題。

適用於 Access Point 搭配多個網路介面卡的 DMZ 設計

Access Point 為第 7 層安全性應用裝置，通常安裝在非軍事區 (DMZ) 中。Access Point 可用來確保只有進入公司資料中心的流量是代表經過嚴格驗證的遠端使用者流量。

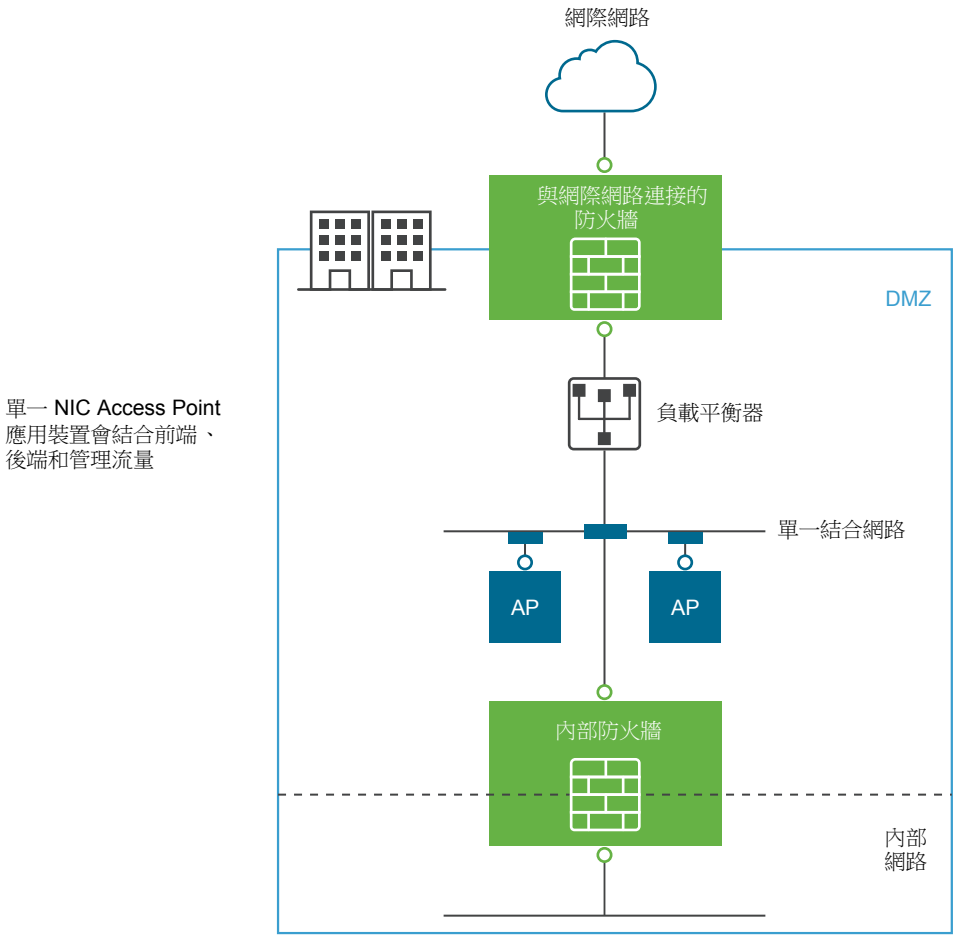
Access Point 的其中一個組態設定為要使用的虛擬網路介面卡 (NIC) 數量。部署 Access Point 時，您會為網路選取部署組態。您可以指定一、二或三個 NIC 設定，其指定方式為 onenic、twonic 或 threenic。

減少每個虛擬 LAN 上已開啟連接埠的數量，並區隔不同類型的網路流量以大幅改善安全性。主要優勢在於區隔與隔離不同類型的網路流量以作為深度防禦 DMZ 安全性設計策略的一部分。這可透過在 DMZ 內實作不同的實體交換器並在 DMZ 內具有多個虛擬 LAN，或隸屬於完整 VMware NSX 所管理 DMZ 的一部分來實現。

一般的單一 NIC DMZ 部署

最簡單的 Access Point 部署是使用單一 NIC，其中的所有網路流量會結合在單一網路上。來自網際網路對向防火牆的流量會導向至其中一個可用的 Access Point 應用裝置。然後 Access Point 會經由內部防火牆將授權流量轉送至內部網路上的資源。Access Point 會捨棄未經授權的流量。

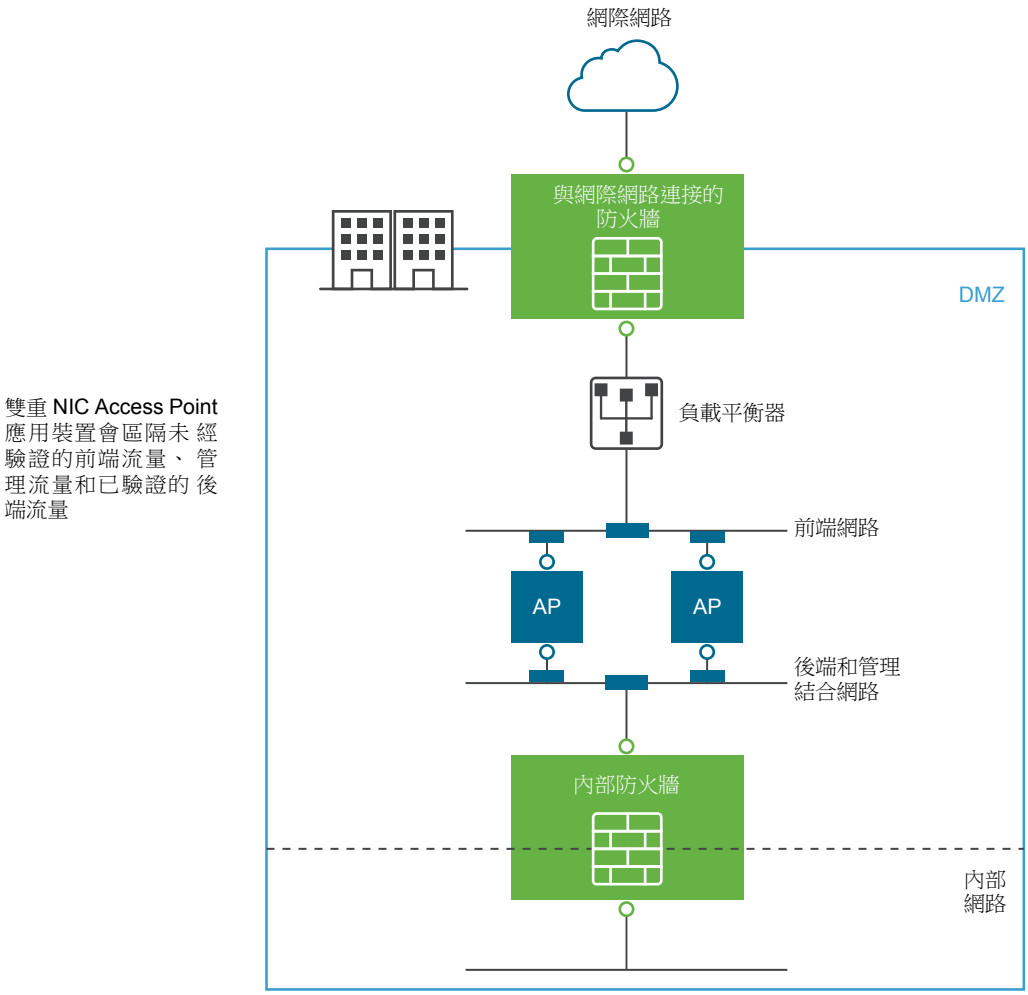
圖 1-3 Access Point 單一 NIC 選項



從後端和管理流量區隔未經驗證的使用者流量

對於單一 NIC 部署的改善即為指定兩個 NIC。第一個仍會用於網際網路對向未經驗證的存取，但後端驗證流量和管理流量則會區隔至不同的網路上。

圖 1-4 Access Point 兩個 NIC 選項



在兩個 NIC 部署中，透過內部防火牆通往內部網路的流量必須由 Access Point 授權。未經授權的流量不會在此後端網路上。管理流量 (例如 Access Point 的 REST API) 只會在此第二個網路上

如果裝置在未經驗證的前端網路上遭到破解，例如負載平衡器，則在這兩個 NIC 部署中便無法重新設定裝置略過 Access Point。它會結合第 4 層防火牆規則與第 7 層 Access Point 安全性。相同地，如果網際網路對向防火牆設定錯誤而允許通過 TCP 連接埠 9443，則這仍不會將 Access Point 管理 REST API 向網際網路使用者公開。深度防禦原則會使用多層級防護，例如知道單一組態錯誤或系統攻擊不一定會產生整體的弱點

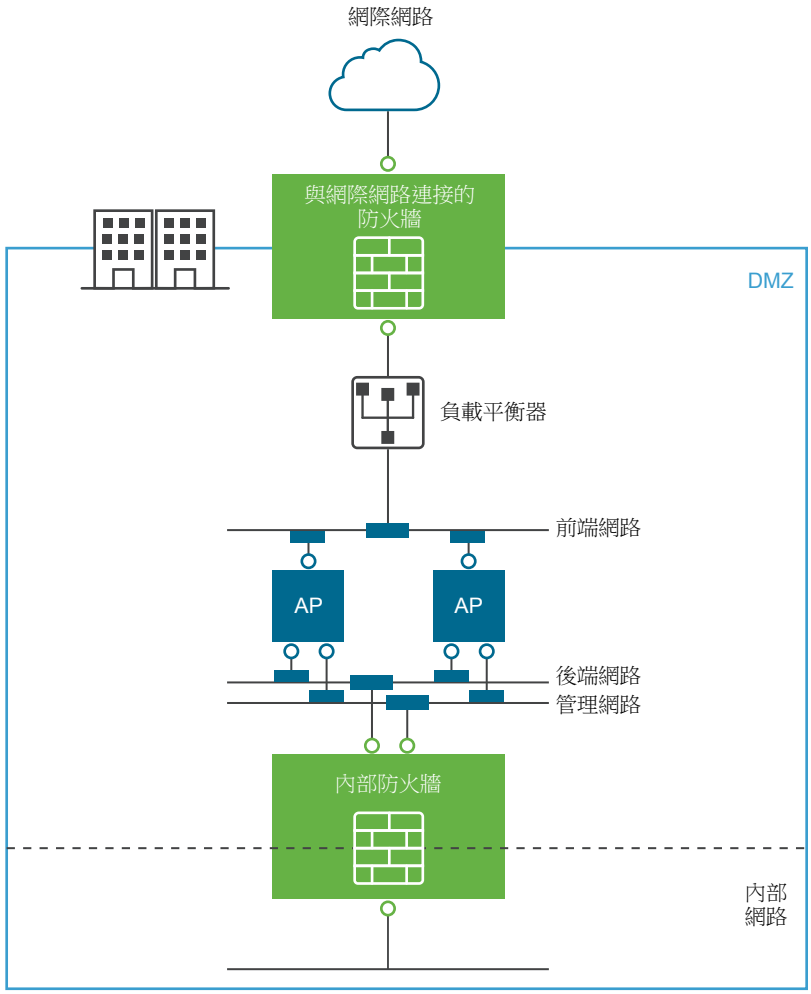
在兩個 NIC 部署中，在 DMZ 內的後端網路上放置額外的基礎結構系統 (如 DNS 伺服器、RSA SecurID 驗證管理員伺服器) 很常見，以便讓這些伺服器無法顯示在網際網路對向網路上。在 DMZ 內放置基礎結構系統可防禦來自遭破解前端系統之網際網路對向 LAN 的第 2 層攻擊，並可有效減少整體攻擊面。

多數 Access Point 網路流量為 Blast 和 PCoIP 的顯示通訊協定。利用單一 NIC，往返於網際網路的顯示通訊協定流量會與往返於後端系統的流量結合。使用兩個以上的 NIC 時，流量會遍及前端和後端 NIC 與網路。這可減少單一 NIC 的潛在瓶頸，並產生效能優勢。

Access Point 也支援進一步的區隔，即允許將管理流量區隔至特定的管理 LAN。如此一來，通往連接埠 9443 的 HTTPS 管理流量僅能夠從管理 LAN 進行傳輸。

圖 1-5 Access Point 三個 NIC 選項

三個 NIC Access Point 應用裝置會提供完整區隔 未經驗證的前端流量、已 驗證的後端流量和管理流量



部署 Access Point 應用裝置 2

Access Point 會封裝為 OVF，並且部署至 vSphere ESX 或 ESXi 主機作為預先設定的虛擬應用裝置。

您可以使用兩個主要方法來安裝 Access Point 應用裝置。

- vSphere Client 或 vSphere Web Client 可用來部署 Access Point OVF 範本。系統將提示您進行基本設定，包括 NIC 部署組態、IP 位址和管理介面密碼。部署 OVF 之後，登入 Access Point 管理員使用者介面以設定 Access Point 系統設定、設定多個使用案例中的安全 Edge Service，以及設定 DMZ 中的驗證。請參閱 使用 OVF 範本精靈來部署 Access Point。
- PowerShell 指令碼可以用來部署 Access Point 和設定多個使用案例中的安全 Edge Service。您會下載 zip 檔案、為環境設定 PowerShell 指令碼，以及執行指令碼以部署 Access Point。請參閱 使用 PowerShell 來部署 Access Point 應用裝置。

本章節討論下列主題:

- 使用 OVF 範本精靈部署 Access Point
- 從管理組態頁面設定 Access Point
- 更新 SSL 伺服器簽署的憑證

使用 OVF 範本精靈部署 Access Point

若要部署 Access Point，您必須使用 vSphere Client 或 vSphere Web Client 部署 OVF 範本，接著開啟應用裝置的電源，然後進行設定。

部署 Access Point 之後，您會前往管理使用者介面 (UI) 來設定 Access Point 環境並設定桌面平台和應用程式資源，以及要在 DMZ 中使用的驗證方法。

Access Point 部署內容

部署 OVF 時，您會設定需要的網路介面 (NIC) 數量、IP 位址及設定管理員密碼。其他部署內容可透過 Access Point 管理頁面進行設定。

表格 2-1. 部署選項 Access Point

部署內容	說明
部署組態	指定 Access Point 虛擬機器中的可用網路介面數目。 依預設不會設定此內容，這表示系統會使用一個網路介面控制器 (NIC)。
外部 (網際網路對向) IP 位址	(必要) 指定在網際網路上用來存取此虛擬機器的公用 IPv4 或 IPv6 位址。 **備註** 電腦名稱是透過此網際網路 IPv4 或 IPv6 位址的 DNS 查詢來設定。 預設值：無。
管理網路 IP 位址	指定連線至管理網路之介面的 IP 位址。 如果未設定，管理伺服器會在網際網路對向介面上進行接聽。 預設值：無。
後端網路 IP 位址	指定連線至後端網路之介面的 IP 位址。 如果未設定，傳送至後端系統的網路流量會透過其他網路介面路由傳送。 預設值：無。
DNS 伺服器位址	(必要) 為此虛擬機器指定一或多個網域名稱伺服器的 IPv4 位址，多個位址之間以空格分隔 (範例：192.0.2.1 192.0.2.2)。您最多可指定三部伺服器。 依預設不會設定此內容，這表示系統會使用與網際網路對向 NIC 相關聯的 DNS 伺服器。 **警告** 如果將此選項留空而且沒有與網際網路對向 NIC 相關聯的 DNS 伺服器，應用裝置將無法正確部署。
根使用者的密碼	(必要) 指定此虛擬機器根使用者的密碼。密碼必須是有效的 Linux 密碼。 預設值：無。
管理員使用者的密碼	(必要) 如果未設定此密碼，您將無法存取 Access Point 應用裝置上的管理主控台和 REST API。 密碼長度至少必須有 8 個字元，至少包含一個大寫字母和一個小寫字母、一個數字和一個特殊字元，其中包括 ! @ # $ % * ( )。 預設值：無。

表格 2-1. 部署選項 Access Point (繼續)

部署內容	說明
當地語系化訊息使用的語言設定	(必要) 指定在產生錯誤訊息時使用的語言設定。 ■ **en_US** 表示英文 ■ **ja_JP** 表示日文 ■ **fr_FR** 表示法文 ■ **de_DE** 表示德文 ■ **zh_CN** 表示簡體中文 ■ **zh_TW** 表示繁體中文 ■ **ko_KR** 表示韓文 預設值：en_US。
Syslog 伺服器 URL	指定用來記錄 Access Point 事件的 Syslog 伺服器。 這個值可以是 URL、主機名稱或 IP 位址。配置和連接埠號碼為選用 (範例：syslog://server.example.com:514)。 依預設不會設定此內容，這表示不會將事件記錄到 Syslog 伺服器。

使用 OVF 範本精靈來部署 Access Point

您可以透過登入 vCenter Server 並使用 [部署 OVF 範本] 精靈來部署 Access Point 應用裝置。

備註 如果使用 vSphere Web Client 來部署 OVF，您也可以指定 DNS 伺服器、閘道以及每個網路的網路遮罩位址。如果使用原生 vSphere Client，請確認您已指派 IP 集區給每個網路。若要使用原生 vSphere Client 在 vCenter Server 中新增 IP 集區，請前往資料中心的 IP 集區索引標籤。或者，如果您使用 vSphere Web Client，則可以建立網路通訊協定設定檔。前往資料中心的 [管理] 索引標籤，並選取 [網路通訊協定設定檔] 索引標籤。

先決條件

- 自行熟悉精靈中提供的部署選項。請參閱 Access Point 系統和網路需求。
- 決定要為 Access Point 應用裝置設定的網路介面和靜態 IP 位址數量。請參閱 網路功能組態需求。
- 從 VMware 網站 (https://my.vmware.com/web/vmware/downloads) 下載 Access Point 應用裝置的 `.ova` 安裝程式檔案，或決定要使用的 URL (範例：`http://example.com/vapps/euc-access-point-Y.Y.0.0-xxxxxxx_OVF10.ova`)，其中 *Y.Y* 是版本號碼，而 *xxxxxxx* 是組建編號。

程序

1 使用原生 vSphere Client 或 vSphere Web Client 登入 vCenter Server 執行個體。

對於 IPv4 網路，請使用原生 vSphere Client 或 vSphere Web Client。對於 IPv6 網路，請使用 vSphere Web Client。

2 選取功能表命令來啟動 [部署 OVF 範本] 精靈。

選項	功能表命令
vSphere Client	選取**檔案 > 部署 OVF 範本**。
vSphere Web Client	選取屬於虛擬機器的有效父系物件的任何詳細目錄物件，例如資料中心、資料夾、叢集、資源集區或主機，並從**動作**功能表中選取**部署 OVF 範本**。

3 在精靈的 [選取來源] 頁面上，瀏覽至您下載的 `.ova` 檔案位置或輸入 URL，然後按**下一步**。

詳細資料頁面隨即顯示。檢閱產品詳細資料、版本和大小需求。

4 按照精靈的提示進行，並參考下列準則以完成精靈。

選項	說明
選取部署組態	對於 IPv4 網路，您可以使用一、二或三個網路介面 (NIC)。對於 IPv6 網路，請使用三個 NIC。Access Point 會要求為每個 NIC 設定不同的靜態 IP 位址。許多 DMZ 實作使用分開的網路來保護不同的流量類型。請根據 Access Point 部署所在之 DMZ 的網路設計來對其設定。
磁碟格式	對於評估和測試環境，選取 [精簡佈建] 格式。對於生產環境，選取其中一個 [完整佈建] 格式。[完整佈建積極式歸零] 是一種完整虛擬磁碟格式，支援容錯之類的叢集功能，但需要的建立時間比其他虛擬磁碟類型還要久。
虛擬機器儲存區原則	(僅限 vSphere Web Client) 在目的地資源上啟用儲存區原則後，即可使用此選項。

選項	說明
設定網路/網路對應	如果您使用 vSphere Web Client，[設定網路] 頁面可讓您將每個 NIC 對應至網路，並指定通訊協定設定。 a 從 **IP 通訊協定**下拉式清單中，選取 IPv4 或 IPv6。 b 選取表格中的第一列**網際網路**，然後按一下向下箭頭來選取目的地網路。如果您選取 IPv6 作為 IP 通訊協定，則必須選取具有 IPv6 功能的網路。 在您選取該列之後，您也可以在視窗下半部輸入 DNS 伺服器、閘道和網路遮罩的 IP 位址。 c 如果您使用多個 NIC，請選取下一列 **ManagementNetwork**，接著選取目的地網路，然後您可以為該網路輸入 DNS 伺服器、閘道和網路遮罩的 IP 位址。 如果您僅使用一個 NIC，則所有列都會對應到相同網路。 d 如果您有第三個 NIC，則也請選取第三列並完成設定。 如果您僅使用兩個 NIC，對於這個第三列 **BackendNetwork**，請選取您用於 **ManagementNetwork** 的相同網路。 在 vSphere Web Client 中，當您完成精靈之後，系統會自動為您建立網路通訊協定設定檔 (如果不存在)。 如果您使用原生 vSphere Client (而不是 Web Client)，[網路對應] 頁面可讓您將每個 NIC 對應至一個網路，但沒有欄位可用來指定 DNS 伺服器、閘道和網路遮罩位址。如先決條件中所述，您必須已對每個網路指派 IP 集區，或已建立網路通訊協定設定檔。
自訂內容範本	在 [內容] 頁面上的文字方塊是 Access Point 專屬的，對於其他類型的虛擬應用裝置來說可能並非必要。精靈頁面中的文字會說明每個設定。如果文字在精靈右側被截斷，請從視窗右下角拖曳以調整其大小。您必須在下列文字方塊中輸入值： ■ **IPMode：STATICV4/STATICV6**。如果您輸入 STATICV4，則必須輸入 NIC 的 IPv4 位址。如果您輸入 STATICV6，則必須輸入 NIC 的 IPv6 位址。 ■ **使用 {tcp|udp}/listening-port-number/destination-ip-address:destination-port-nu 格式的轉送規則逗號分隔清單** ■ **NIC 1 (ETH0) IPv4 位址**。如果您已針對 NIC 模式輸入 STATICV4，請輸入 NIC 的 IPv4 位址。 ■ **使用 ipv4-network-address/bits.ipv4-gateway-address 格式之 NIC 1 (eth0) 的 IPv4 自訂路由逗號分隔清單** ■ **IPv6 位址**。如果您已針對 NIC 模式輸入 STATICV6，請輸入 NIC 的 IPv6 位址。 ■ **DNS 伺服器位址**。針對虛擬機器的網域名稱伺服器輸入以空格分隔的 IPv4 或 IPv6 位址。 ■ **管理網路 IP 位址** - 如果您指定了 2 個 NIC，以及**後端網路 IP 位址** - 如果您指定了 3 個 NIC ■ **密碼選項**。輸入此虛擬機器根使用者的密碼，以及存取管理主控台並啟用 REST API 存取之管理員使用者的密碼。 所有其他設定皆為選用或已輸入預設設定。請注意精靈頁面上所列的密碼需求。如需所有部署內容的說明，請參閱 Access Point 部署內容。

5 在 [即將完成] 頁面上，選取**部署後開啟電源**，然後按一下**完成**。

vCenter Server 狀態區域會出現 [部署 OVF 範本] 工作，以供您監控部署。您也可以在虛擬機器上開啟主控台，檢視在系統開機期間顯示的主控台訊息。檔案 `/var/log/boot.msg` 中也會記錄這些訊息。

6 部署完成後，確認使用者可以透過開啟瀏覽器並輸入下列 URL 來連線至應用裝置：

```
https://FQDN-of-AP-appliance
```

在此 URL 中，*FQDN-of-AP-appliance* 是 Access Point 應用裝置的 DNS 可解析完整網域名稱。

如果部署成功，您會看到 Access Point 所指向之伺服器所提供的網頁。如果部署不成功，您可以刪除應用裝置虛擬機器，然後重新部署應用裝置。最常見的錯誤是未正確輸入憑證指紋。

Access Point 應用裝置會自動部署並啟動。

下一個

登入 Access Point 管理員使用者介面 (UI) 並設定桌面平台和應用程式資源，允許透過 Access Point 以及要在 DMZ 中使用的驗證方法，進行網際網路的遠端存取。管理主控台 URL 的格式為 `https://<mycoAccessPointappliance.com:9443/admin/index.html`。

從管理組態頁面設定 Access Point

部署 OVF 且 Access Point 應用裝置開啟電源之後，請登入 Access Point 管理員使用者介面以進行下列設定。

- Access Point 系統組態和 SSL 伺服器憑證。
- Horizon、Reverse Proxy、每一應用程式通道的 Edge Service 設定，以及 AirWatch 的 Proxy 設定。
- RSA SecurID、RADIUS、X.509 憑證，以及 RSA 調適性驗證的驗證設定。
- SAML 身分識別提供者和服務提供者設定。

下列選項可從組態頁面存取。

- 下載 Access Point 記錄 zip 檔案。
- 匯出 Access Point 設定以擷取組態設定。
- 匯入 Access Point 設定以建立和更新整個 Access Point 組態。

設定 Access Point 系統設定

您可以設定用來從管理員組態頁面加密用戶端與 Access Point 應用裝置之間通訊的安全性通訊協定和密碼編譯演算法。

Access Point 管理員使用者介面 URL 格式為 `https://<mycoAccessPointappliance.com>:9443/admin/index.html`。若要登入，請輸入您在部署 OVF 時設定的管理員使用者名稱和密碼。

先決條件

- 檢閱 Access Point 部署內容。需要下列設定資訊
  - Access Point 應用裝置的靜態 IP 位址
  - DNS 伺服器的 IP 位址

- 管理主控台的密碼
- Access Point 應用裝置所指向的伺服器執行個體或負載平衡器的 URL
- 儲存事件記錄檔的 Syslog 伺服器 URL

程序

1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。

2 在 [進階設定] 區段中，按一下**系統組態**齒輪圖示。

3 編輯下列 Access Point 應用裝置組態值。

選項	預設值和說明
地區設定	指定在產生錯誤訊息時使用的語言設定。 ■ **en_US** 表示英文 ■ **ja_JP** 表示日文 ■ **fr_FR** 表示法文 ■ **de_DE** 表示德文 ■ **zh_CN** 表示簡體中文 ■ **zh_TW** 表示繁體中文 ■ **ko_KR** 表示韓文
管理員密碼	此密碼是在部署應用裝置時設定。您可以重設它。 密碼長度至少必須有 8 個字元，至少包含一個大寫字母和一個小寫字母、一個數字和一個特殊字元，其中包括 ! @ # $ % * ( )。
加密套件	在多數情況下，不需要變更預設的設定。這是可用來加密用戶端與 Access Point 應用裝置之間通訊的密碼編譯演算法。加密設定可用於啟用各種安全性通訊協定。
接受加密順序	預設值為 [否]。選取**是**可啟用 TLS 加密清單順序控制。
SSL 3.0 已啟用	預設值為 [否]。選取**是**可啟用 SSL 3.0 安全性通訊協定。
TLS 1.0 已啟用	預設值為 [否]。選取**是**可啟用 TLS 1.0 安全性通訊協定。
TLS 1.1 已啟用	預設值為 [是]。TLS 1.1 安全性通訊協定已啟用。
TLS 1.2 已啟用	預設值為 [是]。TLS 1.2 安全性通訊協定已啟用。
Syslog URL	輸入用來記錄 Access Point 事件的 Syslog 伺服器 URL。這個值可以是 URL、主機名稱或 IP 位址。如果您未設定 Syslog 伺服器 URL，則不會記錄任何事件。輸入為 `syslog://server.example.com:514`。
健全狀況檢查 URL	輸入負載平衡器連線到的 URL，並檢查 Access Point 的健全狀況。
要快取的 Cookie	Access Point 快取的 Cookie 集。預設值為 [無]。
IP 模式	選取靜態 IP 模式，可為 STATICV4 或 STATICV6。
工作階段逾時	預設值為 **36000000** 毫秒。
靜止模式	啟用**是**可暫停 Access Point 應用裝置，達成一致的狀態來執行維護工作
監控間隔	預設值為 **60**。

4 按一下**儲存**。

下一個

針對 Access Point 部署時所搭配的元件設定 Edge Service 設定。設定 Edge 設定之後，請設定驗證設定。

更新 SSL 伺服器簽署的憑證

在簽署的憑證到期時，您可加以取代。

若是生產環境，VMware 強烈建議您盡快更換預設憑證。在部署 Access Point 應用裝置時所產生的預設 TLS/SSL 伺服器憑證並未經信任的憑證授權機構簽署。

先決條件

- 新簽署的憑證和私密金鑰會儲存到您可以存取的電腦
- 將憑證轉換為 PEM 格式檔案，再將 .pem 檔案轉換為單行格式。請參閱＜將憑證檔案轉換為單行 PEM 格式＞。

程序

1. 在管理主控台中，按一下**選取**。
2. 在 [進階設定] 區段中，按一下 [SSL 伺服器憑證設定] 齒輪圖示。
3. 在 [私密金鑰] 列，按一下**選取**並瀏覽至私密金鑰檔案。
4. 按一下**開啟**以上傳檔案。
5. 在 [憑證鏈結] 列，按一下 [選取] 並瀏覽至憑證鏈結檔案。
6. 按一下**開啟**以上傳檔案。
7. 按一下**儲存**。

下一個

如果簽署憑證的 CA 並不知名，請設定用戶端信任根憑證和中繼憑證。

使用 PowerShell 來部署 Access Point

3

您可以使用 PowerShell 指令碼來部署 Access Point。提供的 PowerShell 指令碼可作為範例指令碼，您可加以改寫來符合您環境的特定需求。

使用 PowerShell 指令碼時，為了部署 Access Point，指令碼會呼叫 OVF Tool 命令，並確認設定以自動建構正確的命令列語法。這個方法也能讓您在部署期間套用 TLS/SSL 伺服器憑證組態等進階設定。

本章節討論下列主題:

使用 PowerShell 部署 Access Point 的系統需求

若要使用 PowerShell 指令碼部署 Access Point，您必須使用特定版本的 VMware 產品。

- vSphere ESX 主機搭配 vCenter Server。
- PowerShell 指令碼會在 Windows 8.1 或更新版本機器或 Windows Server 2008 R2 或更新版本上執行。

  此機器也可以是在 Windows 上執行的 vCenter Server 或單獨的 Windows 機器。
- 執行指令碼的 Windows 機器必須安裝 VMware OVF Tool 命令。

  您必須從 https://www.vmware.com/support/developer/ovf/ 安裝 OVF Tool 4.0.1 或更新版本。

您必須選取要使用的 vSphere 資料存放區和網路。

vSphere 網路通訊協定設定檔必須與每個參考的網路名稱相關聯。此網路通訊協定設定檔會指定如 IPv4 子網路遮罩、閘道等網路設定。Access Point 的部署使用這些值，所以請確認值正確無誤。

使用 PowerShell 來部署 Access Point 應用裝置

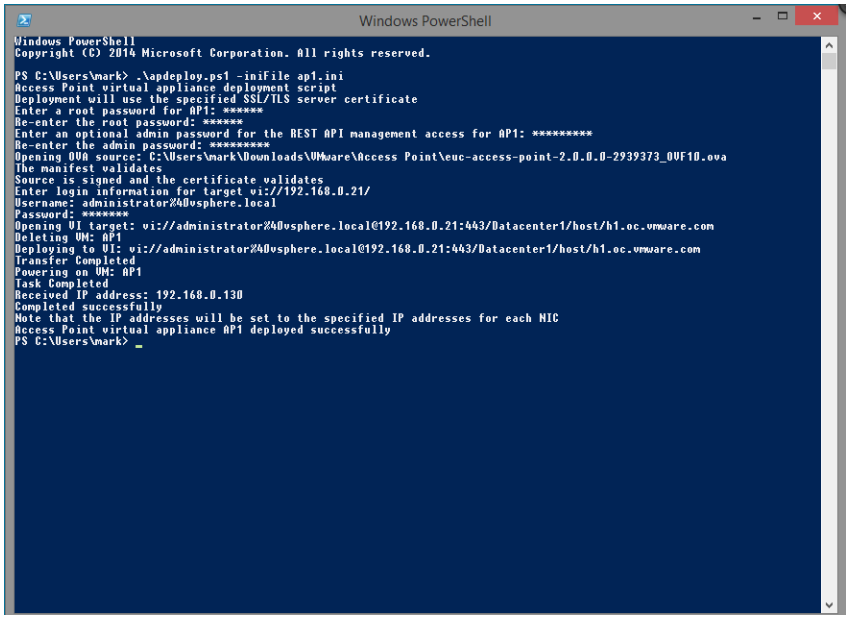
PowerShell 指令碼能為您的環境備妥所有組態設定。當您執行 PowerShell 指令碼來部署 Access Point 時，解決方案會在首次系統開機時做好生產準備。

先決條件

- 請確認系統需求適當且可供使用。

以下是在環境中部署 Access Point 的範例指令碼。

圖 3-1 範例 PowerShell 指令碼



程序

1 從 My VMware 將 Access Point OVA 下載至您的 Windows 機器。

2 將 ap-deploy-XXX.zip 檔案下載到 Windows 機器上的資料夾。

您可以前往 https://communities.vmware.com/docs/DOC-30835 取得 zip 檔案。

3 開啟 PowerShell 指令碼，並將目錄修改為指令碼的所在位置。

4 為 Access Point 虛擬應用裝置建立 .INI 組態檔案。

例如：部署新的 Access Point 應用裝置 AP1。組態檔案的名稱為 ap1.ini。該檔案含有 AP1 的所有組態設定。您可以使用 apdeploy.ZIP 檔案中的範例 .INI 檔案來建立 .INI 檔案，接著再適度修改設定。

備註 您可以將獨一無二的 .INI 檔案用於環境中的多個 Access Point 部署。您必須適度變更 .INI 檔案中的 IP 位址和名稱參數，才能部署多個應用裝置。

要修改的 .INI 檔案範例。

```
name=AP1
source=C:\APs\euc-access-point-2.8.0.0-000000000_OVF10.ova
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esx1.myco.int
ds=Local Disk 1
netInternet=VM Network
netManagementNetwork=VM Network
netBackendNetwork=VM Network

[Horizon/WebReverseProxy/AirwatchTunnel]
```

```
proxyDestinationUrl=https://192.168.0.209

# For IPv4, proxydestinationURL=https://192.168.0.209
# For IPv6, proxyDEstinationUrl=[fc00:10:112:54::220]
```

5 若要確定指令碼執行成功，請輸入 PowerShell set-executionpolicy 命令。

```
set-executionpolicy -scope currentuser unrestricted
```

如果指令碼執行目前受到限制，您才必須執行這個命令一次。

如果出現與指令碼相關的警告，請執行命令以解除封鎖警告：

```
unblock-file -path .\apdeploy.ps1
```

6 執行命令以開始部署。如果您未指定 .INI 檔案，指令碼的預設值為 ap.ini。

```
.\apdeploy.ps1 -iniFile ap1.ini
```

7 當出現提示時，請輸入認證並完成指令碼。

備註 如果系統提示您新增目標機器的指紋，請輸入 **yes**。

Access Point 應用裝置部署即告完成，並可供生產之用。

如需 PowerShell 指令碼的詳細資訊，請參閱 https://communities.vmware.com/docs/DOC-30835。

部署使用案例

4

本章中說明的部署案例可協助您找出並組織環境中的 Access Point 部署。

您可以利用 Horizon View、Horizon Air Hybrid-Mode、VMware Identity Manager 及 VMware AirWatch 部署 Access Point。

本章節討論下列主題:

利用 Horizon View 和 Horizon Air Hybrid-Mode 部署 Access Point

您可以利用 Horizon View 和 Horizon Air Hybrid-Mode 部署 Access Point。對於 VMware Horizon 的 View 元件，Access Point 應用裝置會履行以往由 View 安全伺服器扮演的角色。

部署案例

Access Point 能提供安全的遠端存取能力，供您存取客戶資料中心內的內部部署虛擬桌面平台和應用程式。它能與內部部署的 Horizon View 或 Horizon Air Hybrid-Mode 搭配運作，實現統合的管理功能。

Access Point 讓企業得以有效保證使用者的身分識別，而且能精準控制使用者對於有權使用之桌面平台和應用程式的存取權限。

Access Point 虛擬應用裝置通常部署在網路的非軍事區 (DMZ)。在 DMZ 中部署能確保所有進入資料中心並前往桌面平台和應用程式資源的流量是代表經過嚴格驗證之使用者的流量。Access Point 虛擬應用裝置還能確保經過驗證之使用者的流量只能導向該使用者有權使用的桌面平台和應用程式資源。這個層級的保護涉及具體檢測桌面平台通訊協定、協調可能迅速變動的原則和網路位址，以便精確地控制存取權限。

您必須確認已滿足需求才能以 Horizon 順暢地部署 Access Point。

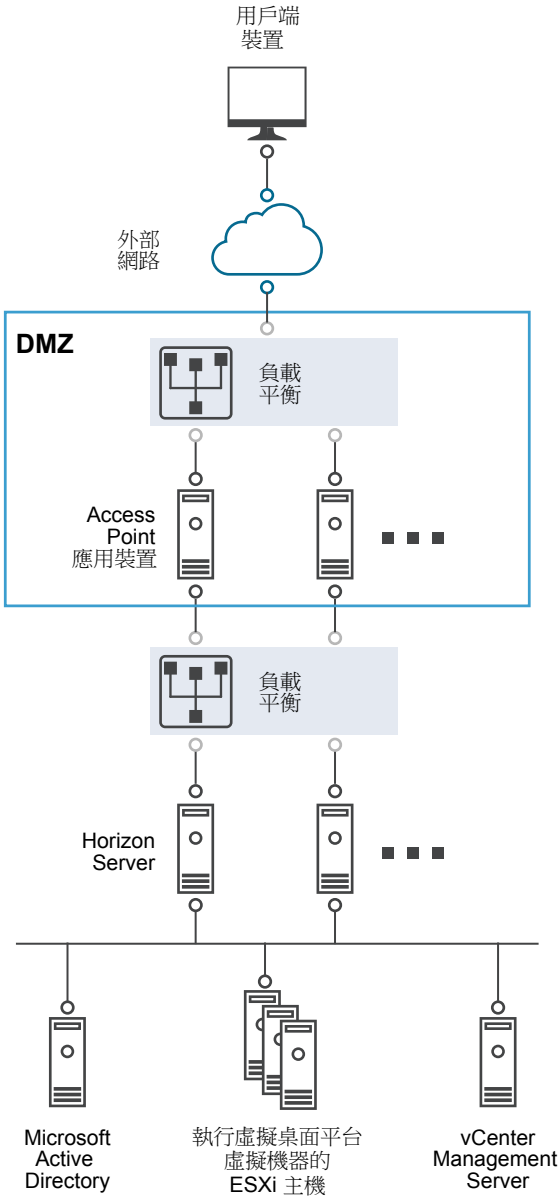
- Access Point 應用裝置指向 Horizon Server 前方的負載平衡器，伺服器執行個體的選擇不會固定不變。
- Access Point 取代 Horizon 安全伺服器。
- 連接埠 443 必須可供 Blast TCP/UDP 使用。

- 以 Horizon 部署 Access Point 時，必須啟用 Blast 安全閘道和 PCoIP 安全閘道。如此可確保顯示通訊協定能自動透過 Access Point 成為 Proxy。BlastExternalURL 和 pcoipExternalURL 設定會指定 Horizon Client 使用的連線位址，以便透過 Access Point 上的適當閘道路由傳送這些顯示通訊協定連線。由於這些閘道能代表經過驗證的使用者確保顯示通訊協定流量受到控制，因此能改善安全性。未經過驗證的顯示通訊協定流量會遭到 Access Point 忽略。
- 在 View 連線伺服器執行個體上停用安全閘道，並在 Access Point 應用裝置上啟用這些閘道。

Access Point 與 View 安全伺服器的主要差異如下所示。

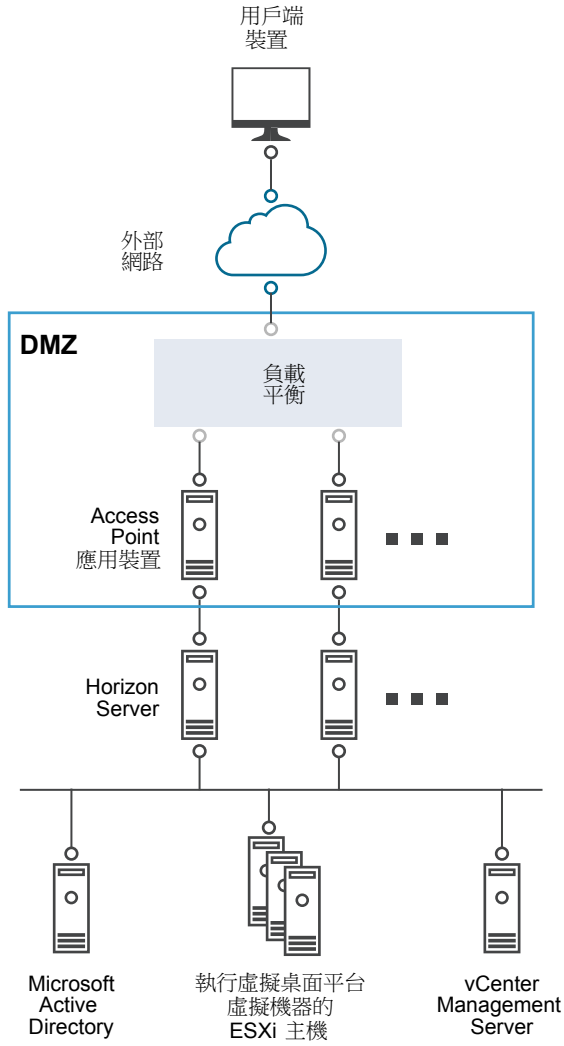
- 安全部署。Access Point 會實作為強化、鎖定且預先設定的 Linux 虛擬機器
- 可擴充。您可以將 Access Point 連接到個別的 View 連線伺服器，或透過多部 View 連線伺服器前方的負載平衡器予以連接，藉此改善高可用性。它可作為 Horizon Client 與後端 View 連線伺服器之間的層。由於部署快速，因此它能迅速垂直擴充或垂直縮減，以滿足快速變遷的企業需求。

圖 4-1 指向負載平衡器的 Access Point 應用裝置



或者，您也可以讓一或多部 Access Point 應用裝置指向個別伺服器執行個體。在這兩種方法中，都請在 DMZ 中的兩部 (含) 以上 Access Point 應用裝置前方使用負載平衡器。

圖 4-2 指向 Horizon Server 執行個體的 Access Point 應用裝置



驗證

使用者驗證與 View 安全伺服器非常類似。Access Point 支援的使用者驗證方法包括下列項目。

- Active Directory 使用者名稱和密碼
- Kiosk 模式。如需 Kiosk 模式的詳細資料，請參閱 Horizon 說明文件。
- RSA SecurID 雙因素驗證，由 RSA 針對 SecurID 正式認證
- 透過幾項第三方雙因素安全供應商解決方案的 RADIUS
- 智慧卡、CAC 或 PIV X.509 使用者憑證
- SAML

搭配使用 View 連線伺服器時，以上驗證方法都能獲得支援。Access Point 不需要直接與 Active Directory 通訊。這種模式的通訊能做為透過 View 連線伺服器的 Proxy，因此能直接存取 Active Directory。在根據驗證原則驗證使用者工作階段後，Access Point 就能將權利資訊的要求以及桌面平台和應用程式的啟動要求轉送給 View 連線伺服器。Access Point 還能管理其桌面平台和應用程式通訊協定處理常式，讓它們只轉送授權的通訊協定流量。

Access Point 能自行處理智慧卡驗證。內容包括讓 Access Point 與線上憑證狀態通訊協定 (Online Certificate Status Protocol, OCSP) 伺服器通訊，以便檢查 X.509 憑證撤銷等選項。

設定 Horizon 設定

您可以透過 Horizon View 和 Horizon Air Hybrid-Mode 部署 Access Point。對於 VMware Horizon 的 View 元件，Access Point 應用裝置會履行以往由 View 安全伺服器扮演的角色。

程序

1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。

2 在 [一般設定] > [Edge Service 設定] 行中，按一下**顯示**。

3 按一下 **Horizon 設定**齒輪圖示。

4 在 [Horizon 設定] 頁面中，將 [否] 變更為**是**以啟用 Horizon

5 為 Horizon 設定下列 Edge Service 設定資源

選項	說明
識別碼	依預設會設定為 View。Access Point 可與使用 View XML 通訊協定的伺服器進行通訊，例如 View 連線伺服器、Horizon Air 和 Horizon Air Hybrid-Mode。
連線伺服器 URL	輸入 Horizon server 或負載平衡器的位址。輸入格式為 https://00.00.00.00
Proxy 目的地 URL 指紋	輸入 Horizon server 指紋的清單。 如果未提供指紋的清單，則必須由信任的 CA 核發伺服器憑證。輸入十六進位的指紋數字。例如，sha=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3

6 若要設定驗證方法規則和其他進階設定，請按一下**較多**。

選項	說明
驗證方法	選取要使用的驗證方法。 預設會使用使用者名稱和密碼的傳遞驗證。您在 Access Point 中設定的驗證方法會在下拉式功能表中列出。 若要設定包括在第一個驗證嘗試失敗時套用第二個驗證方法的驗證。 a 從第一個下拉式功能表選取一個驗證方法。 b 按一下 **+** 並選取 AND 或 OR。 c 從第三個下拉式功能表選取第二個驗證方法。 若要要求使用者透過兩個驗證方法進行驗證，請在下拉式功能表中將 OR 變更為 AND。
健全狀況檢查 URL	如果已設定負載平衡器，請輸入負載平衡器用來連線的 URL，並檢查 Access Point 應用裝置的健全狀況。

選項	說明
SAML SP	輸入 View XMLAPI 代理之 SAML 服務提供者的名稱。此名稱必須符合所設定服務提供者中繼資料的名稱，或為特殊值 DEMO。
PCOIP 已啟用	將 [否] 變更為**是**可指定是否啟用 PCoIP 安全閘道。
Proxy 外部 URL	輸入 Access Point 應用裝置的外部 URL。用戶端會使用此 URL 透過 PCoIP 安全閘道進行安全連線。此連線用於 PCoIP 流量。預設值為 Access Point IP 位址和連接埠 4172。
智慧卡提示	將 [否] 變更為**是**可啟用 Access Point 應用裝置，可支援智慧卡使用者名稱提示功能。使用者的智慧卡憑證可透過智慧卡提示功能，對應至多個 Active Directory 網域使用者帳戶。
Blast 已啟用	若要使用 Blast 安全閘道，請將 [否] 變更為**是**。
Blast 外部 URL	輸入 Access Point 應用裝置的 FQDN URL，以便使用者用來從網頁瀏覽器透過 Blast 安全閘道進行安全連線。您可以輸入 https://exampleappliance:443
通道已啟用	如果使用了 View 安全通道，請將 [否] 變更為**是**。用戶端會使用此外部 URL 透過 View 安全閘道進行通道連線。此通道用於 RDP、USB 和多媒體重新導向 (MMR) 流量。
通道外部 URL	輸入 Access Point 應用裝置的外部 URL。若未設定，則系統會使用預設的 Access Point 預設值。
符合 Windows 使用者名稱	將 [否] 變更為**是**以符合 RSA SecurID 與 Windows 使用者名稱。如果設為 [是]，則 securID-auth 會設定為 true，並且會強制 securID 與 Windows 使用者名稱相符。
閘道位置	將 [否] 變更為**是**以啟用要求起始的位置。安全伺服器和 Access Point 會設定閘道位置。位置可以是外部或內部的。
Windows SSO 已啟用	將 [否] 變更為**是**以啟用 RADIUS 驗證。Windows 登入會使用第一次成功的 RADIUS 存取要求中所使用的認證。

7 按一下**儲存**。

部署為 Reverse Proxy 的 Access Point

Access Point 可用作 Web Reverse Proxy，並且可以在 DMZ 中作為單純的 Reverse Proxy 或驗證 Reverse Proxy。

部署案例

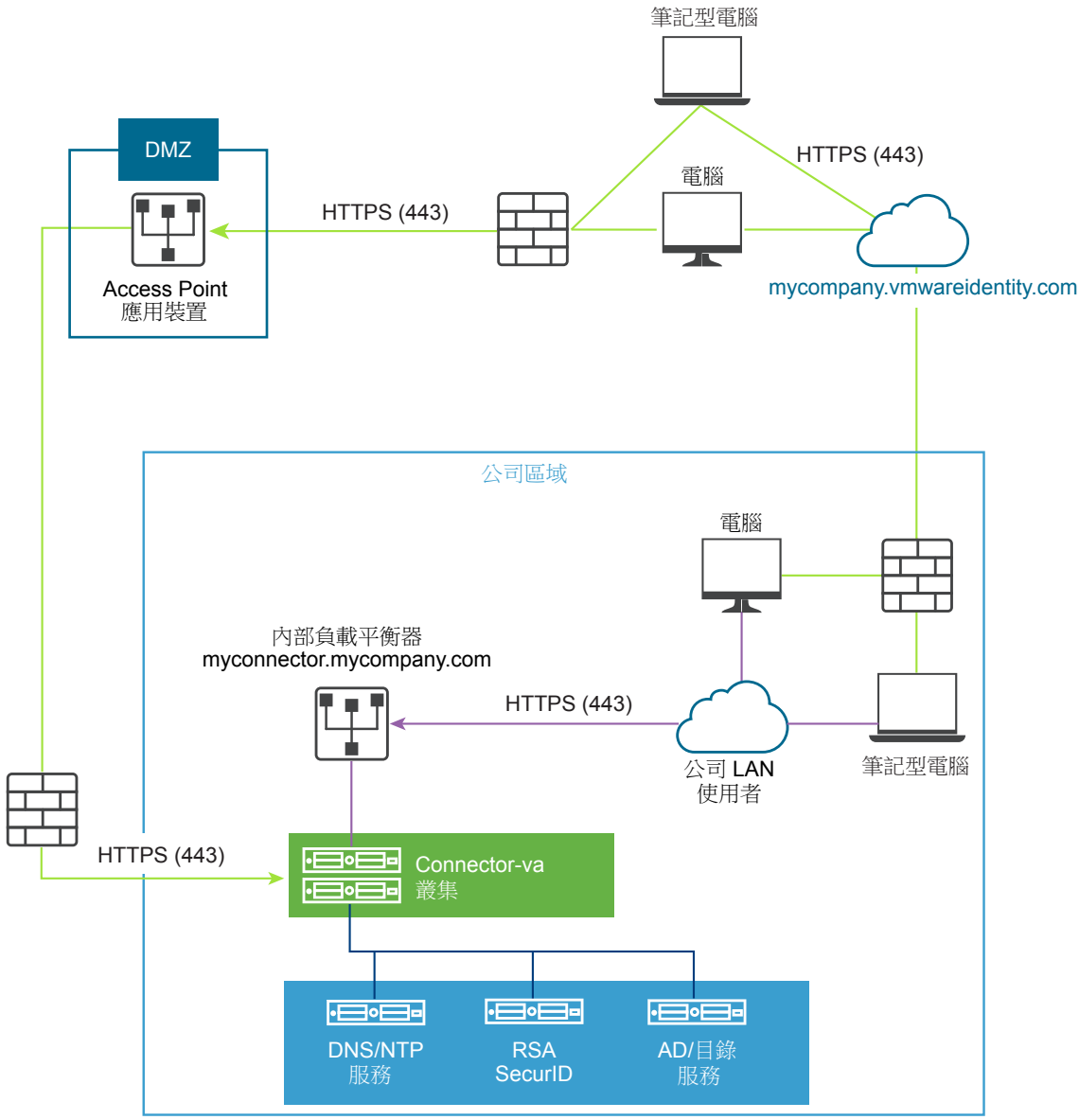
Access Point 能讓您從遠端安全地存取內部部署的 VMware Identity Manager。Access Point 應用裝置通常部署在網路的非軍事區 (DMZ)。利用 VMware Identity Manager，Access Point 應用裝置可作為使用者的瀏覽器與資料中心的 VMware Identity Manager 服務之間的 Web Reverse Proxy。Access Point 也允許從遠端存取 VMware Identity Manager 目錄來啟動 Horizon 應用程式。

搭配 VMware Identity Manager 的 Access Point 部署需求

- 分割 DNS
- VMware Identity Manager 應用裝置必須以完整網域名稱 (FQDN) 作為主機名稱。

- Access Point 必須使用內部 DNS。這表示 proxyDestinationURL 必須使用 FQDN。

圖 4-3 指向連接器的 Access Point 應用裝置



瞭解 Reverse Proxy

作為一種解決方案，Access Point 提供遠端使用者對應用程式入口網站的存取，進行單一登入並存取其資源。您會在 Edge Service Manager 上啟用驗證 Reverse Proxy。目前支援 RSA SecurID 和 RADIUS 驗證方法。

備註 在 Web Reverse Proxy 上啟用驗證之前，您必須先產生身分識別提供者中繼資料。

Access Point 能在搭配或未搭配瀏覽器型用戶端驗證的情況下提供 VMware Identity Manager 和 Web 應用程式的遠端存取權，進而啟動 Horizon 桌面平台。

- 支援對瀏覽器型用戶端使用 RADIUS 和 RSA SecurID 作為驗證方法。

對於 Access Point 2.8 版，Reverse Proxy 支援僅限 VMware Identity Manager 和內部 Web 資源 (如 Confluence 和 WIKI)。未來我們將會擴充資源清單。

備註 `authCookie` 和 `unSecurePattern` 內容不適用於驗證 Reverse Proxy。您必須使用 `authMethods` 內容來定義驗證方法。

為 VMware Identity Manager 設定 Reverse Proxy

您可以設定 Web Reverse Proxy 服務以搭配使用 Access Point 和 VMware Identity Manager。

先決條件

搭配 VMware Identity Manager 的 Access Point 部署需求。

- 分割 DNS
- VMware Identity Manager 服務必須以完整網域名稱 (FQDN) 作為主機名稱。
- Access Point 必須使用內部 DNS。這表示 proxyDestination URL 必須使用 FQDN。

程序

1. 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
2. 在 [一般設定] > [Edge Service 設定] 行中，按一下**顯示**。
3. 按一下 **Reverse Proxy 設定**齒輪圖示。
4. 在 [Reverse Proxy 設定] 頁面，將 [否] 變更為**是**以啟用 Reverse Proxy。
5. 為 Horizon 設定下列 Edge Service 設定資源。

選項	說明
識別碼	Edge Service 識別碼會設定為 WEB_REVERSE_PROXY。
Proxy 目的地 URL	輸入 VMware Identity Manager 伺服器的位址。例如，您可以輸入 **`https://vmwareidentitymgr.example.com`**。
Proxy 目的地 URL 指紋	針對 proxyDestination URL，輸入可接受 SSL 伺服器憑證指紋的清單。如果您納入萬用字元 *，則允許使用任何憑證。指紋的格式為 [alg=]xx:xx，其中 alg 可以是 sha1 (預設值) 或 md5。「xx」為十六進位數字。例如，sha=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3 如果未設定指紋，則必須由受信任的 CA 核發伺服器憑證。
Proxy 模式	輸入轉送至目的地 URL 的相符 URI 路徑。例如，您可以輸入 **`(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`**。

6 若要設定其他進階設定，請按一下**較多**。

選項	說明
驗證方法	預設會使用使用者名稱和密碼的傳遞驗證。您在 Access Point 中設定的驗證方法會在下拉式功能表中列出。您在 Access Point 中設定的驗證方法會在下拉式功能表中列出。
健全狀況檢查 URL	如果已設定負載平衡器，請輸入負載平衡器用來連線的 URL，並檢查 Access Point 應用裝置的健全狀況。
SAML SP	輸入 View XML API 代理之 SAML 服務提供者的名稱。此名稱必須符合所設定服務提供者中繼資料的名稱，或為特殊值 **DEMO**。
啟用代碼	輸入 VMware Identity Manager 服務所產生並匯入 Access Point 以設定 VMware Identity Manager 與 Access Point 之間信任的代碼。
外部 URL	預設值為 Access Point 主機 URL，連接埠 443。您可以輸入其他外部 URL。輸入為 `https://<host:port>`.

7 按一下**儲存**。

利用 AirWatch Tunnel 部署 Access Point

Access Point 應用裝置會部署在 DMZ 中。部署作業涉及安裝 Access Point 元件和 AirWatch 元件，如 Agent 及通道代理伺服器服務

為 AirWatch 環境部署 AirWatch Tunnel 涉及設定初始硬體、設定伺服器資訊、在 AirWatch 管理主控台內配置應用程式設定、下載安裝程式檔案，以及在 AirWatch Tunnel 伺服器上執行安裝程式等作業。

您可以在 OVF 安裝完成及變更值之後手動設定每個 Edge Service。

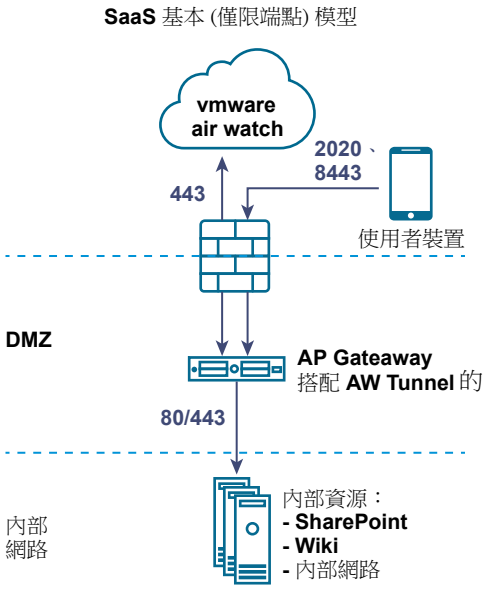
如需利用 AirWatch 部署 Access Point 的詳細資訊，請參閱 https://resources.air-watch.com/view/vb7zp7wwhpw756m2pfxy 。

AirWatch 的通道代理伺服器部署

通道代理伺服器部署能透過 AirWatch 提供的 VMware Browser 行動應用程式保護使用者裝置和網站之間的網路流量。

行動應用程式能利用通道代理伺服器來建立安全的 HTTPS 連線，進而保護機密資料。若要搭配使用內部應用程式與 AirWatch Tunnel 代理伺服器，請務必將 AirWatch SDK 內嵌在應用程式中，如此一來您就可以透過此元件獲得通道功能。

圖 4-4 通道代理伺服器部署

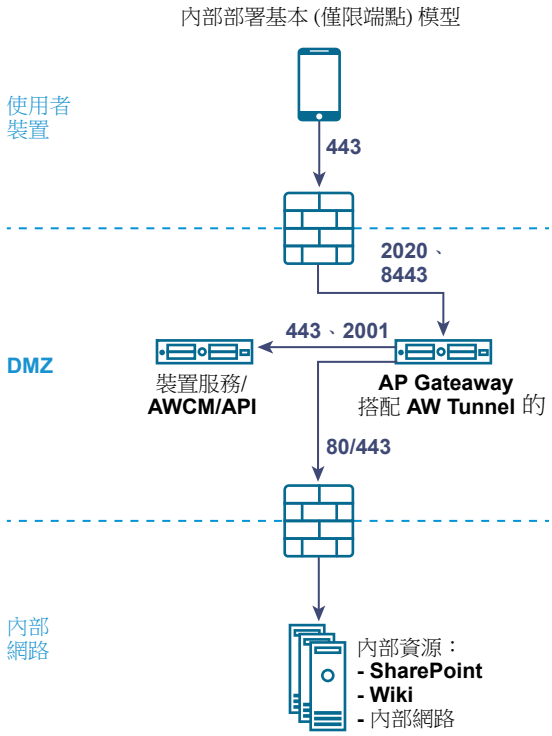


使用 AirWatch 的每一應用程式通道部署

每一應用程式通道部署能讓內部和公用應用程式安全地存取位在安全內部網路之內的公司資源。

它會使用 iOS 7+ 或 Android 5.0+ 等作業系統提供的每一應用程式功能。這些作業系統允許行動管理員核准的特定應用程式，以應用程式為依據存取內部資源。使用此解決方案的優點，在於不需變更行動應用程式的程式碼。相較於其他任何自訂解決方案，來自作業系統的支援能提供更順暢的使用者體驗及強化的安全性。

圖 4-5 每一應用程式通道部署



針對 AirWatch 設定每一應用程式通道和 Proxy 設定

通道代理伺服器部署能透過 VMware Browser 行動應用程式保護使用者裝置和網站之間的網路流量。

程序

1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。

2 在 [一般設定] > [Edge Service 設定] 行中，按一下**顯示**。

3 按一下**每一應用程式通道和 Proxy 設定**齒輪圖示。

4 將 [否] 變更為**是**以啟用通道代理伺服器。

5 設定下列 Edge Service 設定資源。

選項	說明
識別碼	依預設會設定為 View。Access Point 可與使用 View XML 通訊協定的伺服器進行通訊，例如 View 連線伺服器、Horizon Air 和 Horizon Air Hybrid-Mode。
API 伺服器 URL	輸入 AirWatch API 伺服器 URL。例如，您可以輸入 https://example.com:<連接埠>。
API 伺服器使用者名稱	輸入用來登入 API 伺服器的使用者名稱。
API 伺服器密碼	輸入用來登入 API 伺服器的密碼。
組織群組代碼	輸入使用者的組織。
AirWatch 伺服器主機名稱	輸入 AirWatch 伺服器主機名稱。

6 若要設定其他進階設定，請按一下**較多**。

選項	說明
AirWatch 連出代理伺服器	將 [否] 變更為**是**以初始化通道代理伺服器服務。
連出代理伺服器主機	輸入安裝連出代理伺服器所在的主機名稱。 **備註** 這不是通道代理伺服器。
連出代理伺服器連接埠	輸入連出代理伺服器的連接埠號碼。
連出代理伺服器使用者名稱	輸入用來登入連出代理伺服器的使用者名稱。
連出代理伺服器密碼	輸入用來登入連出代理伺服器的密碼。
NTLM 驗證	將 [否] 變更為**是**以指定連出代理伺服器要求需要 NTLM 驗證。
AirWatch Tunnel 代理伺服器適用	將 [否] 變更為**是**以使用此 Proxy 作為 AirWatch Tunnel 的連出代理伺服器。如果未啟用，則 Access Point 會對初始 API 呼叫使用此 Proxy，以便從 AirWatch 管理主控台取得組態。

7 按一下**儲存**。

使用 TLS/SSL 憑證設定 Access Point

5

您必須設定 Access Point 應用裝置的 TLS/SSL 憑證。

備註 設定 Access Point 應用裝置的 TLS/SSL 憑證僅適用於 Horizon View、Horizon Air Hybrid-Mode 及 Web Reverse Proxy。

設定 Access Point 應用裝置的 TLS/SSL 憑證

用戶端在連線至 Access Point 應用裝置時必須使用 TLS/SSL。面向用戶端的 Access Point 應用裝置和終止 TLS/SSL 連線的中繼伺服器需要 TLS/SSL 伺服器憑證。

TLS/SSL 伺服器憑證是由憑證授權機構 (CA) 簽署。CA 是一個受信任的實體，可保證憑證的身分及其建立者。當憑證是由信任的 CA 簽署時，使用者不會再收到要求他們確認憑證的訊息，而精簡型用戶端裝置可以連線，無需要求額外組態。

當您部署 Access Point 應用裝置時就會產生預設的 TLS/SSL 伺服器憑證。針對生產環境，VMware 建議您盡快取代預設憑證。預設憑證並非由信任的 CA 所簽署。預設憑證只能用於非生產環境

選取正確的憑證類型

您可將多種 TLS/SSL 憑證類型用於 Access Point。為您的部署選取正確的憑證類型十分重要。憑證類型不同，其成本也不同，端視其可使用在的伺服器數目而定。

無論您選取何種憑證類型，請務必遵循 VMware 的安全建議：針對憑證使用完整網域名稱 (FQDN)。請勿使用簡單伺服器名稱或 IP 位址，即使針對內部網域內的通訊。

單一伺服器名稱憑證

您可針對特定伺服器，產生具有主體名稱的憑證。例如：`dept.example.com`。

如果只有一個 Access Point 應用裝置需要憑證，這種憑證類型就很有用。

當您提交憑證簽署要求至 CA 時，需提供與憑證相關聯的伺服器名稱。請確定 Access Point 應用裝置可以解析您提供的伺服器名稱，使其符合憑證關聯的名稱。

主體別名

主體別名 (SAN) 是在核發憑證時可以新增至憑證的屬性。使用此屬性新增主體名稱 (URL) 至憑證，讓憑證可以驗證多個伺服器。

例如，假設針對位於負載平衡器後面的 Access Point 應用裝置核發了三個憑證：`ap1.example.com`、`ap2.example.com` 和 `ap3.example.com`。透過在此範例中新增代表負載平衡器主機名稱的主體別名，例如 `horizon.example.com`，憑證就能生效，因為它符合用戶端指定的主機名稱。

萬用字元憑證

產生萬用字元憑證以用於多個服務。例如：`*.example.com`。

如果有多個伺服器需要憑證，萬用字元就很有用。如果除了 Access Point 應用裝置以外，您環境中還有其他應用程式需要 TLS/SSL 憑證，您也能為這些伺服器使用萬用字元憑證。不過，如果使用與其他服務共用的萬用字元憑證，則 VMware Horizon 產品的安全性也會取決於上述其他服務的安全性。

備註 萬用字元憑證只能用於單一網域層級。例如，具有主體名稱 `*.example.com` 的萬用字元憑證可以用於子網域 `dept.example.com`，但不能用於 `dept.it.example.com`。

您匯入至 Access Point 應用裝置的憑證必須是用戶端機器信任的，也必須能夠適用於 Access Point 的所有執行個體以及所有負載平衡器，無論是使用萬用字元還是主體別名 (SAN) 憑證。

將憑證檔案轉換為單行 PEM 格式

若要使用 Access Point REST API 進行憑證設定或要使用 PowerShell 指令碼，您必須將憑證轉換為 PEM 格式檔案以取得憑證鏈結和私密金鑰，接著必須將 `.pem` 檔案轉換為包含內嵌換行字元的單行格式。

設定 Access Point 時，可能有三種憑證類型需要加以轉換。

- 請一律為 Access Point 應用裝置安裝並設定 TLS/SSL 伺服器憑證。
- 如果計劃使用智慧卡驗證，您必須針對將要放在智慧卡上的憑證，安裝並設定信任的 CA 簽發者憑證。
- 如果計劃使用智慧卡驗證，VMware 建議您為 Access Point 應用裝置上所安裝的 SAML 伺服器憑證，安裝並設定簽署 CA 的根憑證。

對於這三種憑證類型，執行相同程序以將憑證轉換為包含憑證鏈結的 PEM 格式檔案。對於 TLS/SSL 伺服器憑證和根憑證，另請將每個檔案轉換為包含私密金鑰的 PEM 檔案。接著必須將每個 `.pem` 檔案轉換為可將 JSON 字串傳遞至 Access Point REST API 的單行格式。

先決條件

- 確認您擁有憑證檔案。檔案可能是 PKCS#12 (`.p12` 或 `.pfx`) 格式，也可能是 Java JKS 或 JCEKS 格式。
- 自行熟悉您將用來轉換憑證的 `openssl` 命令列工具。請參閱 https://www.openssl.org/docs/apps/openssl.html。
- 如果憑證是 Java JKS 或 JCEKS 格式，請自行熟悉 Java `keytool` 命令列工具，以先將憑證轉換為 `.p12` 或 `.pks` 格式，之後才能再轉換為 `.pem` 檔案。

程序

1 如果憑證是 Java JKS 或 JCEKS 格式，請使用 `keytool` 將憑證轉換為 `.p12` 或 `.pks` 格式。

重要事項 在此轉換期間，請使用相同的來源和目的地密碼。

2 如果憑證是 PKCS#12 (`.p12` 或 `.pfx`) 格式，或已將憑證轉換為 PKCS#12 格式後，請使用 `openssl` 將憑證轉換為 `.pem` 檔案。

例如，如果憑證的名稱是 `mycaservercert.pfx`，請使用下列命令轉換憑證：

```
openssl pkcs12 -in mycaservercert.pfx -nokeys -out mycaservercert.pem
openssl pkcs12 -in mycaservercert.pfx -nodes -nocerts -out mycaservercert.pem
openssl rsa -in mycaservercertkey.pem -check -out mycaservercertkeyrsa.pem
```

3 編輯 `mycaservercert.pem`，然後移除任何不需要的憑證項目。檔案中應該會包含一個 SSL 伺服器憑證，後面則有任何必要的中繼 CA 憑證和根 CA 憑證。

4 使用下列 UNIX 命令，將每個 `.pem` 檔案轉換為可將 JSON 字串傳遞至 Access Point REST API 的值。

```
awk 'NF {sub(/\r/, ""); printf "%s\\n",$0;}' cert-name.pem
```

在此範例中，*cert-name*`.pem` 是憑證檔案的名稱。

新格式會將所有憑證資訊放在具有內嵌換行字元的單行中。如果您具有中繼憑證，該憑證也必須使用單行格式，並新增至第一個憑證，讓這兩個憑證位於同一行上。

現在，您可以使用這些 `.pem` 檔案並搭配 https://communities.vmware.com/docs/DOC-30835 上的部落格文章〈Using PowerShell to Deploy VMware Access Point〉(使用 PowerShell 部署 VMware Access Point) 內附的 PowerShell 指令碼，來設定 Access Point 的憑證。或者，您也可以建立並使用 JSON 要求來設定憑證。

下一個

如果您轉換的是 TLS/SSL 伺服器憑證，請參閱更換 Access Point 的預設 TLS/SSL 伺服器憑證。若是智慧卡憑證，請參閱在 Access Point 應用裝置上設定憑證或智慧卡驗證。

更換 Access Point 的預設 TLS/SSL 伺服器憑證

若要在 Access Point 應用裝置上儲存信任的 CA 簽署的 TLS/SSL 伺服器憑證，您必須將憑證轉換為正確格式，然後使用 PowerShell 指令碼或 Access Point REST API 來設定憑證。

若是生產環境，VMware 強烈建議您盡快更換預設憑證。在部署 Access Point 應用裝置時所產生的預設 TLS/SSL 伺服器憑證並未經信任的憑證授權單位簽署。

重要事項 此外，也請在信任的 CA 簽署的憑證過期之前，使用此程序定期更換憑證，大約是每兩年一次。

此程序說明如何使用 REST API 更換憑證。比較簡單的方法是運用 https://communities.vmware.com/docs/DOC-30835 中的部落格文章〈Using PowerShell to Deploy VMware Access Point〉(使用 PowerShell 部署 VMware Access Point) 內附的 PowerShell 指令碼。如果您已部署具名的 Access Point 應用裝置，則再次執行指令碼會關閉應用裝置電源、將其刪除，然後使用您指定的目前設定重新部署該應用裝置。

先決條件

- 除非您已擁有有效的 TLS/SSL 伺服器憑證及其私密金鑰，否則請向憑證授權單位取得新簽署的憑證。當您產生憑證簽署要求 (CSR) 以取得憑證時，請確定也有一併產生私密金鑰。請勿使用低於 1024 的 KeyLength 值來產生伺服器的憑證。

  若要產生 CSR，您必須知道用戶端裝置將用來連線至 Access Point 應用裝置的完整網域名稱 (FQDN) 以及組織單位、組織、城市、州及國家，以便完成主體名稱。

- 將憑證轉換為 PEM 格式檔案，再將 `.pem` 檔案轉換為單行格式。請參閱 將憑證檔案轉換為單行 PEM 格式。
- 自行熟悉 Access Point REST API。此 API 的規格位於安裝 Access Point 的虛擬機器上，可從下列 URL 取得：`https://access-point-appliance.example.com:9443/rest/swagger.yaml`。

程序

1 建立 JSON 要求，用以提交憑證給 Access Point 應用裝置。

```
{
  "privateKeyPem": "string",
  "certChainPem": "string"
}
```

在此範例中，*string* 值是依先決條件所述而建立的 JSON 單行 PEM 值。

2 使用 REST 用戶端 (例如 `curl` 或 `postman`)，以使用 JSON 要求來叫用 Access Point REST API，並將憑證和金鑰儲存在 Access Point 應用裝置上。

下列範例使用 `curl` 命令。在此範例中，*access-point-appliance.example.com* 是 Access Point 應用裝置的完整網域名稱，而 *cert*.json 是您在上一個步驟中建立的 JSON 要求。

```
curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X PUT https://access-point-appliance.example.com:9443/rest/v1/config/certs/ssl < ~/cert.json
```

下一個

如果簽署憑證的 CA 並不知名，請設定用戶端信任根憑證和中繼憑證。

變更 TLS 或 SSL 通訊所用的安全性通訊協定和加密套件

雖然在幾乎所有情況下都無須變更預設設定，您仍可設定用來加密用戶端和 Access Point 應用裝置之間通訊的安全性通訊協定和密碼編譯演算法。

預設設定包括使用 128 位元或 256 位元 AES 加密的加密套件 (除了匿名 DH 演算法)，然後按強度對其排序。依預設會啟用 TLS v1.1 和 TLS v1.2。TLS v1.0 和 SSL v3.0 會停用。

先決條件

- 自行熟悉 Access Point REST API。此 API 的規格位於安裝 Access Point 的虛擬機器上，可從下列 URL 取得：`https://access-point-appliance.example.com:9443/rest/swagger.yaml`。
- 自行熟悉用於設定加密套件和通訊協定的特定內容：`cipherSuites`、`ssl30Enabled`、`tls10Enabled`、`tls11Enabled` 和 `tls12Enabled`。

程序

1 建立 JSON 要求，用以指定要使用的通訊協定和加密套件。

下列範例具有預設設定。

```
{
"cipherSuites":
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA",
  "ssl30Enabled": "false",
  "tls10Enabled": "false",
  "tls11Enabled": "true",
  "tls12Enabled": "true"
}
```

2 使用 REST 用戶端 (例如 `curl` 或 `postman`)，以使用 JSON 要求來叫用 Access Point REST API 並設定通訊協定和加密套件。

在此範例中，*access-point-appliance.example.com* 是 Access Point 應用裝置的完整網域名稱。

```
curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X PUT https://access-point-
appliance.example.com:9443/rest/v1/config/system < ~/ciphers.json
```

ciphers.json 是您在上一個步驟中建立的 JSON 要求。

將會使用您指定的加密套件和通訊協定。

設定 DMZ 中的驗證

6

初始部署 VMware Access Point 時，Active Directory 密碼驗證會設定為預設值。使用者輸入其 Active Directory 使用者名稱和密碼之後，這些憑證會傳送到後端系統進行驗證。

您可以設定 Access Point 服務以執行憑證/智慧卡驗證、RSA SecurID 驗證、RADIUS 驗證和 RSA 調適性驗證。

備註 使用 Active Directory 的密碼驗證是可搭配 AirWatch 部署使用的唯一驗證方法。

本章節討論下列主題:

在 Access Point 應用裝置上設定憑證或智慧卡驗證

您可以在 Access Point 中設定 x509 憑證驗證，以允許用戶端在其桌面平台或行動裝置上使用憑證進行驗證，或是使用智慧卡配接器進行驗證。

憑證式驗證是根據使用者所擁有的驗證工具 (私密金鑰或智慧卡)，以及個人所知道的驗證內容 (私密金鑰的密碼或智慧卡 PIN)。智慧卡驗證提供雙因素驗證，一是驗證個人擁有的 (智慧卡)，一是驗證個人知道的 (PIN)。使用者可將智慧卡用於登入遠端 View 桌面平台作業系統，以及用於啟用智慧卡功能的應用程式，例如採用憑證簽署電子郵件以證明寄件者身分的電子郵件應用程式。

利用此功能，系統會對 Access Point 服務執行智慧卡憑證驗證。Access Point 使用 SAML 聲明來向 Horizon server 傳遞有關使用者的 X.509 憑證與智慧卡 PIN 的資訊。

您可以設定憑證撤銷檢查，以防止使用者憑證已撤銷的使用者進行驗證。通常當使用者離開組織、遺失智慧卡，或調動部門時，就會撤銷憑證。支援使用「憑證撤銷清單」(CRL) 和「線上憑證狀態通訊協定」(OCSP) 的憑證撤銷檢查。CRL 是核發憑證的 CA 所發佈的撤銷憑證清單。OCSP 是用來取得憑證撤銷狀態的憑證驗證通訊協定。

您可以在相同的憑證驗證介面卡組態中同時設定 CRL 和 OCSP。當您同時設定兩種類型的憑證撤銷檢查，且啟用了 [若 OCSP 失敗則使用 CRL] 核取方塊時，將會先檢查 OCSP，如果 OCSP 失敗，撤銷檢查會退而使用 CRL。如果 CRL 失敗，撤銷檢查不會回復使用 OCSP。

您也可以將驗證設定為讓 Access Point 要求智慧卡驗證，接著同時將驗證傳遞至伺服器，而後者會要求 Active Directory 驗證。

備註 針對 VMware Identity Manager，驗證一律會透過 Access Point 傳遞至 VMware Identity Manager 服務。只有當 Access Point 搭配 Horizon 7 使用時，才能設定在 Access Point 應用裝置上執行智慧卡驗證。

在 Access Point 上設定憑證驗證

您可從 Access Point 管理主控台啟用並設定憑證驗證。

先決條件

- 從簽署由您的使用者提供之憑證的 CA 取得根憑證和中繼憑證。請參閱 取得憑證授權機構憑證
- 確認已在服務提供者上新增 Access Point SAML 中繼資料，且服務提供者 SAML 中繼資料已複製到 Access Point 應用裝置。
- (選用) 適用於憑證驗證的有效憑證原則的物件識別碼 (OID) 清單。
- CRL 的檔案位置和 OCSP 伺服器的 URL，用於撤銷檢查。
- (選用) OCSP 回應簽署憑證檔案位置。
- 同意表單內容 (如果同意表單會在驗證前顯示)。

程序

1. 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
2. 在 [一般設定] 的 [驗證設定] 區段中，按一下**顯示**。
3. 按一下 [X.509 憑證] 行的齒輪。
4. 設定 X.509 憑證表單。

   星號表示必填文字方塊。所有其他文字方塊均為選填。

選項	說明
啟用 X.509 憑證	將 [否] 變更為**是**可啟用憑證驗證。
***名稱**	為此驗證方法命名。
***根憑證和中繼 CA 憑證**	按一下**選取**以選取要上傳的憑證檔案。您可選取多個已編碼為 DER 或 PEM 的根 CA 和中繼 CA 憑證。
CRL 快取大小	輸入憑證撤銷清單快取大小。預設值為 100
啟用憑證撤銷	將 [否] 變更為**是**可啟用憑證撤銷檢查。撤銷檢查會導致已撤銷使用者憑證的使用者無法驗證。
使用來自憑證的 CRL	選取此核取方塊，可使用由核發憑證的 CA 所發行的憑證撤銷清單 (CRL) 來驗證憑證的狀態 (已撤銷或未撤銷)。
CRL 位置	輸入要從中擷取 CRL 的伺服器檔案路徑或本機檔案路徑。

選項	說明
啟用 OCSP 撤銷	選取此核取方塊，以使用線上憑證狀態通訊協定 (OCSP) 憑證驗證通訊協定瞭解憑證的撤銷狀態。
若 OCSP 失敗則使用 CRL	如果您同時設定 CRL 和 OCSP，您可以選取此方塊，以在 OCSP 檢查無法使用時回復為使用 CRL。
傳送 OCSP Nonce	如果您希望在回應中傳送 OCSP 要求的唯一識別碼，請選取此核取方塊。
OCSP URL	如果您已啟用 OCSP 撤銷，請輸入用於撤銷檢查的 OCSP 伺服器位址。
OCSP 回應程式的簽署憑證	輸入回應程式 OCSP 憑證的路徑，*/path/to/file.cer*。
驗證之前啟用同意表單	選取此核取方塊以包含同意表單頁面，使其在使用者使用憑證驗證登入其 Workspace ONE 入口網站前顯示。
同意表單內容	在此輸入同意表單中顯示的文字。

5 按一下**儲存**。

下一個

已設定 X.509 憑證驗證，且 Access Point 應用裝置設定在負載平衡器後方時，請確定 Access Point 已設定在負載平衡器使用 SSL 傳遞，並且未設定在負載平衡器終止 SSL。此組態可確保 SSL 信號交換會在 Access Point 與用戶端之間進行，以便將憑證傳遞至 Access Point。

取得憑證授權機構憑證

針對您使用者和管理員提供的智慧卡上的所有受信任使用者憑證，您必須取得所有適用的 CA (憑證授權機構) 憑證。這些憑證包含根憑證，而且，如果使用者的智慧卡憑證是由中繼憑證授權機構發給的，則可以包含中繼憑證。

如果您沒有使用者和管理員所提供智慧卡上簽署憑證的 CA 根憑證或中繼憑證，您可以從 CA 簽署的使用者憑證或包含該憑證的智慧卡匯出憑證。請參閱 從 Windows 取得 CA 憑證。

程序

- 從以下其中一個來源取得 CA 憑證。
  - 執行 Microsoft 憑證服務的 Microsoft IIS 伺服器。請參閱 Microsoft TechNet 網站以取得在您組織中安裝 Microsoft IIS、發行憑證，及散佈憑證的相關資訊。
  - 信任 CA 的公用根憑證。這在已具備智慧卡基礎結構與標準化智慧卡散佈及驗證方法的環境中，是最常見的根憑證來源。

從 Windows 取得 CA 憑證

如果您具有 CA 簽署的使用者憑證或包含憑證的智慧卡，則當 Windows 信任根憑證時，可以從 Windows 匯出根憑證。若使用者憑證的發行者為中繼憑證授權單位，您可匯出該憑證。

程序

1 如果使用者憑證在智慧卡上，請將智慧卡插入讀卡機中，將使用者憑證新增至您的個人存放區。

如果使用者憑證未出現在您的個人存放區中，請使用讀卡機軟體將使用者憑證匯出至檔案。在此程序的步驟 4 中使用此檔案。

2 在 Internet Explorer 中，選取**工具 > 網際網路選項**。

3 在**內容**索引標籤上，按一下**憑證**。

4 在**個人**索引標籤上，選取您要使用的憑證，並按一下**檢視**。

如果使用者憑證未出現在清單中，請按一下**匯入**手動從檔案匯入憑證。匯入憑證後，您便可以從清單中選取憑證。

5 在**憑證路徑**索引標籤中，選取樹狀結構頂端的憑證，並按一下**檢視憑證**。

如果已將使用者憑證簽署成為信任階層的一部分，則正在簽署的憑證可由另一個更高層級的憑證簽署。選取父憑證 (實際簽署使用者憑證的憑證) 作為您的根憑證。在某些情況下，發行者可能是中繼 CA。

6 在**詳細資料**索引標籤上，按一下**複製到檔案**。

憑證匯出精靈隨即出現。

7 按**下一步 > 下一步**，並輸入您要匯出的檔案名稱與位置。

8 按**下一步**將檔案儲存在指定的位置作為根憑證。

在 Access Point 中設定 RSA SecurID 驗證

將 Access Point 應用裝置設為 RSA SecurID 伺服器中的驗證代理程式之後，您必須將 RSA SecurID 組態資訊新增至 Access Point 應用裝置。

先決條件

- 確認 RSA 驗證管理員 (RSA SecurID 伺服器) 已安裝且正確設定。
- 從 RSA SEcurID 伺服器下載壓縮的 sdconf.rec 檔案，並解壓縮伺服器組態檔。

程序

1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。

2 在 [一般設定] 的 [驗證設定] 區段中，按一下**顯示**。

3 按一下 [RSA SecurID] 行的齒輪。

4 設定 RSA SecurID 頁面。

設定 SecurID 頁面時需要在 RSA SecurID 伺服器上使用的資訊和產生的檔案。

選項	動作
啟用 RSA SecurID	將 [否] 變更為**是**可啟用 SecurID 驗證。
*名稱	名稱為 securid-auth。
*反覆運算的數目	輸入允許的驗證嘗試次數。這是使用 RSA SecurID Token 時，登入嘗試失敗次數的上限。預設為五次嘗試。 **備註** 當您設定多個目錄且利用額外的目錄實作 RSA SecurID 驗證時，請將**允許的驗證嘗試次數**設定為與每個 RSA SecurID 組態相同的值。如果值不同，SecurID 驗證將會失敗。
*外部主機名稱	輸入 Access Point 執行個體的 IP 位址。輸入的值必須與將 Access Point 應用裝置做為驗證代理程式新增至 RSA SecurID 伺服器時所用的值相符。

選項	動作
*內部主機名稱	在 RSA SecurID 伺服器中輸入指派給 **IP 位址**提示的值。
*伺服器組態	按一下 [變更] 以上傳 RSA SecurID 伺服器組態檔。首先，您必須從 RSA SecurID 伺服器下載壓縮檔，並解壓縮伺服器組態檔 (依預設名稱為 `sdconf.rec`)。
*名稱 ID 尾碼	輸入可讓 View 提供 TrueSSO 經驗的名稱識別碼。

針對 Access Point 設定 RADIUS

您可以設定 Access Point，以便要求使用者使用 RADIUS 驗證。您會在 Access Point 應用裝置上設定 RADIUS 伺服器資訊。

RADIUS 支援提供範圍廣泛的替代式雙因素 Token 型驗證選項。因為雙因素驗證解決方案 (例如 RADIUS) 可與安裝在不同伺服器上的驗證管理員搭配使用，您必須設定 RADIUS 伺服器，並可供 Identity Manager 服務存取

當使用者登入，且 RADIUS 驗證啟用時，瀏覽器中會顯示一個特殊的登入對話方塊。使用者在登入對話方塊中輸入其 RADIUS 驗證使用者名稱和密碼。如果 RADIUS 伺服器發出存取挑戰，則 Access Point 會顯示對話方塊並提示輸入第二個密碼。目前支援的 RADIUS 挑戰限制為提示文字輸入。

使用者在對話方塊中輸入認證後，RADIUS 伺服器便可將 SMS 簡訊或電子郵件，或使用其他頻外機制的文字，連同代碼傳送到使用者手機。使用者可將此文字與代碼輸入到登入對話方塊以完成驗證。

如果 RADIUS 伺服器提供從 Active Directory 匯入使用者的功能，則使用者可能會先看到要求提供 Active Directory 認證的提示，然後才會看到要求提供 RADIUS 驗證使用者名稱與密碼的提示。

設定 RADIUS 驗證

在 Access Point 應用裝置上，您必須啟用 RADIUS 驗證、輸入來自 RADIUS 伺服器的組態設定，並將驗證類型變更為 RADIUS 驗證。

先決條件

- 確認要做為驗證管理員伺服器的伺服器已安裝 RADIUS 軟體並加以設定。設定 RADIUS 伺服器，然後從 Access Point 設定 RADIUS 要求。請參閱 RADIUS 廠商的設定指南，以取得設定 RADIUS 伺服器的相關資訊。

需要下列 RADIUS 伺服器資訊。

- RADIUS 伺服器的 IP 位址或 DNS 名稱。
- 驗證連接埠號碼。驗證連接埠通常為 1812。
- 驗證類型。驗證類型包括 PAP (密碼驗證通訊協定)、CHAP (Challenge Handshake 驗證通訊協定)、MSCHAP1、MSCHAP2 (Microsoft Challenge Handshake 驗證通訊協定，版本 1 和 2)。
- 用於在 RADIUS 通訊協定訊息中加密和解密的 RADIUS 共用密碼。
- RADIUS 驗證所需的特定逾時和重試值

程序

1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。

2 在 [一般設定] 的 [驗證設定] 區段中，按一下**顯示**。

3 按一下 [RADIUS] 行的齒輪。

選項	動作
啟用 RADIUS	將 [否] 變更為**是**以啟用 RADIUS 驗證。
名稱*	名稱為 radius-auth
驗證類型*	輸入 RADIUS 伺服器支援的驗證通訊協定。PAP、CHAP、MSCHAP1 或 MSCHAP2 中的一個。
共用密碼*	輸入 RADIUS 共用密碼。
允許的驗證嘗試次數 *	使用 RADIUS 登入時，輸入登入嘗試失敗的次數上限。預設為三次嘗試。
對 RADIUS 伺服器的嘗試次數 *	輸入重試嘗試的總數。如果主要伺服器未回應，服務會等待設定的時間經過後再次進行重試。
伺服器逾時 (以秒為單位)*	輸入 RADIUS 伺服器逾時 (以秒為單位)，在此時間之後，如果 RADIUS 伺服器未回應，即會傳送重試。
RADIUS 伺服器主機名稱*	輸入 RADIUS 伺服器的主機名稱或 IP 位址。
驗證連接埠*	輸入 RADIUS 驗證連接埠號碼。連接埠通常為 1812。
領域首碼	(選用) 使用者帳戶位置稱為領域。 如果您指定領域首碼字串，則該名稱傳送至 RADIUS 伺服器時會放置在使用者名稱的開頭。例如，如果輸入的使用者名稱為 jdoe，並指定領域首碼 DOMAIN-A\，則會將使用者名稱 DOMAIN-A\jdoe 傳送至 RADIUS 伺服器。如果不設定這些欄位，則只會傳送所輸入的使用者名稱。
領域尾碼	(選用) 如果設定領域尾碼，則字串會放置在使用者名稱的結尾。例如，如果尾碼為 @myco.com，則會傳送使用者名稱 jdoe@myco.com 至 RADIUS 伺服器。
名稱 ID 尾碼	輸入可讓 View 提供 TrueSSO 經驗的名稱識別碼。
登入頁面複雜密碼提示	輸入要在使用者登入頁面的訊息中顯示的文字字串，可引導使用者輸入正確的 RADIUS 密碼。例如，如果將此欄位設定為 **先 AD 密碼然後 SMS 密碼**，登入頁面訊息會顯示**先輸入您的 AD 密碼然後輸入 SMS 密碼。**預設的文字字串為 **RADIUS 密碼**。
啟用次要伺服器	將 [否] 變更為**是**可針對高可用性設定次要 RADIUS 伺服器。如步驟 3 所述，設定次要伺服器資訊。

4 按一下**儲存**。

在 Access Point 中設定 RSA 調適性驗證

與針對 Active Directory 僅進行使用者名稱及密碼驗證相比，RSA 調適性驗證的實作能提供更強大的多重要素驗證。調適性驗證能根據風險程度和原則來監控及驗證使用者登入嘗試。

啟用調適性驗證時，系統會使用在 RSA Policy Management 應用程式中設定之風險原則內的風險指標，以及 Access Point 的調適性驗證服務組態來判斷是否使用者名稱和密碼來驗證使用者，抑或是需要其他資訊來驗證使用者。

驗證支援的 RSA 調適性驗證方法

Access Point 中支援的 RSA 調適性驗證強式驗證方法，即透過電話、電子郵件或 SMS 簡訊和挑戰問題進行頻外驗證。您可以在服務上啟用可提供的 RSA 調適性驗證方法。RSA 調適性驗證原則會判斷該使用哪個次要驗證方法。

頻外驗證是一種需要隨著使用者名稱和密碼傳送額外驗證的程序。當使用者在 RSA 調適性驗證伺服器中註冊時，他們需要根據伺服器組態提供電子郵件地址、電話號碼或兩者。若需要額外驗證，RSA 調適性驗證伺服器會透過提供的通道傳送一次性密碼。除了使用者名稱和密碼之外，使用者還需要輸入該密碼。

當使用者在 RSA 調適性驗證伺服器中註冊時，挑戰問題會要求使用者回答一系列的問題。您可以設定要回答的註冊問題數目，以及登入頁面上出現的挑戰問題數目。

向 RSA 調適性驗證伺服器註冊使用者

您必須先在 RSA 調適性驗證資料庫中佈建使用者，才能使用調適性驗證來進行驗證。當使用者首次以他們的使用者名稱和密碼登入時，系統會將他們新增至 RSA 調適性驗證資料庫。根據您在服務中設定 RSA 調適性驗證的方式，當使用者登入時，系統會要求他們提供電子郵件地址、電話號碼、文字訊息服務號碼 (SMS)，或是要求他們設定挑戰問題的回應。

備註 RSA 調適性驗證不允許在使用者名稱中使用國際字元。如果您想要允許在使用者名稱中使用多位元組字元，請聯絡 RSA 支援以設定 RSA 調適性驗證和 RSA 驗證管理員。

在 Access Point 中設定 RSA 調適性驗證

若要為服務設定 RSA 調適性驗證，您需要啟用 RSA 調適性驗證；選取要套用的調適性驗證方法，以及新增 Active Directory 連線資訊和憑證。

先決條件

- 以用於次要驗證的驗證方法正確設定了 RSA 調適性驗證。
- 有關 SOAP 端點位址和 SOAP 使用者名稱的詳細資料。
- 可供使用的 Active Directory 組態資訊和 Active Directory SSL 憑證。

程序

1. 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
2. 在 [一般設定] 的 [驗證設定] 區段中，按一下**顯示**。
3. 按一下 [RSA 調適性驗證] 行的齒輪。

4 選取適合環境的設定。

備註 星號表示必填欄位。其他欄位為選填。

選項	說明
啟用 RSA AA 介面卡	將 [否] 變更為**是**以啟用 RSA 調適性驗證。
名稱*	名稱為 rsaaa-auth。
SOAP 端點*	輸入 RSA 調適性驗證介面卡和服務整合所需的 SOAP 端點位址。
SOAP 使用者名稱*	輸入用來簽署 SOAP 訊息的使用者名稱和密碼。
SOAP 密碼*	輸入 RSA 調適性驗證 SOAP API 密碼。
RSA 網域	輸入調適性驗證伺服器的網域位址。
啟用 OOB 電子郵件	選取 [是] 以啟用利用電子郵件訊息傳送一次性密碼給使用者的頻外驗證。
啟用 OOB SMS	選取 [是] 以啟用利用 SMS 簡訊傳送一次性密碼給使用者的頻外驗證。
啟用 SecurID	選取 [是] 以啟用 SecurID。系統會要求使用者輸入其 RSA Token 和密碼。
啟用密碼問題	如果您要使用註冊和挑戰問題來進行驗證，請選取 [是]。
註冊問題數目*	輸入使用者註冊驗證介面卡伺服器時需要設定的問題數目。
挑戰問題數目*	輸入使用者必須正確回答才能登入的挑戰問題數目。
允許的驗證嘗試次數*	輸入在認定驗證失敗之前，要向嘗試登入之使用者顯示挑戰問題的次數。
目錄類型*	Active Directory 是唯一支援的目錄。
使用 SSL	如果您的目錄連線使用 SSL，請選取 [是]。您可以在 [目錄憑證] 欄位中新增 Active Directory SSL 憑證。
伺服器主機*	輸入 Active Directory 主機名稱。
伺服器連接埠	輸入 Active Directory 連接埠號碼。
使用 DNS 服務位置	如果目錄連線使用 DNS 服務位置，請選取 [是]。
基本 DN	輸入要開始搜尋帳戶的 DN。例如，OU=myUnit,DC=myCorp,DC=com。
繫結 DN*	輸入可搜尋使用者的帳戶。例如，CN=binduser,OU=myUnit,DC=myCorp,DC=com
繫結密碼	輸入繫結 DN 帳戶的密碼。
搜尋屬性	輸入包含使用者名稱的帳戶屬性。
目錄憑證	若要建立安全的 SSL 連線，請將目錄伺服器憑證新增至文字方塊。若為多重伺服器案例，請新增憑證授權機構的根憑證。
使用 STARTTLS	將 [否] 變更為**是**可使用 STARTTLS。

5 按一下**儲存**。

產生 Access Point SAML 中繼資料

您必須在 Access Point 應用裝置上產生 SAML 中繼資料並與伺服器交換中繼資料，才能建立智慧卡驗證需要的共同信任。

安全性聲明標記語言 (SAML) 是一種以 XML 為基礎的標準，用於說明以及交換不同安全網域之間的驗證與授權資訊。在被稱為 SAML 聲明的 XML 文件中，SAML 在身分識別提供者與服務提供者之間傳遞使用者相關資訊。在此案例下，Access Point 是身分識別提供者而伺服器是服務提供者。

先決條件

- 在 Access Point 應用裝置上設定時鐘 (UTC)，讓應用裝置擁有正確的時間。例如，開啟 Access Point 虛擬機器上的主控台視窗，然後使用箭頭按鈕選取正確的時區。另外，確認 ESXi 主機的時間是否與 NTP 伺服器同步。確認在應用裝置虛擬機器上執行的 VMware Tools 會將虛擬機器的時間與 ESXi 主機的時間同步。

  重要事項 如果 Access Point 應用裝置上的時鐘不符合伺服器主機上的時鐘，智慧卡驗證可能會無法運作。

- 取得可用來簽署 Access Point 中繼資料的 SAML 簽署憑證。

  備註 如果您的設定中有多部 Access Point 應用裝置，VMware 建議您建立並使用特定的 SAML 簽署憑證。在此情況下，所有應用裝置都必須設定為使用相同的簽署憑證，以便伺服器可以接受來自任何一部 Access Point 應用裝置的聲明。使用特定的 SAML 簽署憑證時，來自所有應用裝置的 SAML 中繼資料皆相同。

- 將 SAML 簽署憑證轉換為 PEM 格式檔案，再將 `.pem` 檔案轉換為單行格式 (如果您尚未這麼做)。請參閱 將憑證檔案轉換為單行 PEM 格式。

程序

1. 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
2. 在 [進階設定] 區段中，按一下 **SAML 身分識別提供者設定**齒輪圖示。
3. 選取**提供憑證**核取方塊。
4. 若要新增私密金鑰檔案，請按一下**選取**並瀏覽至憑證的私密金鑰檔案。
5. 若要新增憑證鏈結檔案，請按一下**選取**並瀏覽至憑證鏈結檔案。
6. 按一下**儲存**。
7. 在 [主機名稱] 文字方塊中，輸入主機名稱並下載身分識別提供者設定。

建立其他服務提供者使用的 SAML 驗證器

在 Access Point 應用裝置上產生 SAML 中繼資料後，您可以將該資料複製到後端服務提供者。複製此資料給服務提供者是建立 SAML 驗證器程序的一部分，如此可讓 Access Point 做為身分識別提供者。

對於 Horizon Air Hybrid-mode 伺服器，請參閱產品說明文件中的特定指示。

將服務提供者 SAML 中繼資料複製到 Access Point

在建立並啟用 SAML 驗證器以便讓 Access Point 可以做為身分識別提供者後，即可在該後端系統上產生 SAML 中繼資料，並使用中繼資料在 Access Point 應用裝置上建立服務提供者。此資料交換可在身分識別提供者 (Access Point) 和 View 連線伺服器之類的後端服務提供者之間建立信任。

先決條件

確認已在後端服務提供者伺服器上為 Access Point 建立 SAML 驗證器。

程序

1 擷取服務提供者 SAML 中繼資料 (通常是 XML 檔案的形式)。

如需相關指示，請參閱服務提供者的說明文件。

不同的服務提供者有不同的程序。例如，您必須開啟瀏覽器並輸入 https://*connection-server.example.com*/SAML/metadata/sp.xml 之類的 URL

接著，您可以使用**另存新檔**命令，將網頁儲存為 XML 檔案。此檔案的內容開頭為下列文字：

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

2 在 Access Point 管理員 UI 的 [手動設定] 區段中，按一下**選取**。

3 在 [進階設定] 區段中，按一下 **SAML 伺服器提供者設定**齒輪圖示。

4 在 [服務提供者名稱] 文字方塊中，輸入服務提供者名稱。

5 在 [中繼資料 XML] 文字方塊中，貼上您在步驟 1 中建立的中繼資料檔案。

6 按一下**儲存**。

Access Point 和服務提供者現在可以交換驗證與授權資訊了。

疑難排解 Access Point 部署 7

您可以使用多種程序來診斷及修正於環境中部署 Access Point 時遭遇的問題。

您可以使用疑難排解程序來調查此類問題的成因，並試圖自行修正問題，或者您也可以向 VMware 技術支援取得協助。

本章節討論下列主題:

- 疑難排解部署錯誤
- 從 Access Point 應用裝置收集記錄
- 啟用偵錯模式

疑難排解部署錯誤

當您在環境中部署 Access Point 時，可能會遭遇難題。您可以使用多種程序來診斷及修正部署時發生的問題。

執行從網際網路下載的指令碼時出現安全警告

請確認 PowerShell 指令碼是您要執行的指令碼，然後從 PowerShell 主控台執行以下命令：

```
unblock-file .\apdeploy.ps1
```

找不到 ovftool 命令

請確認您已在 Windows 機器上安裝 OVF Tool 軟體，且該軟體安裝在指令碼預期的位置。

內容 netmask1 中的網路無效

- 這則訊息可能會指出 netmask0、netmask1 或 netmask2。請確認已在這三個網路各自的 .INI 檔案中設定值，如 netInternet、netManagementNetwork 及 netBackendNetwork。
- 請確認 vSphere 網路通訊協定設定檔已與每個參考的網路名稱相關聯。它能指定如 IPv4 子網路遮罩、閘道等網路設定。請確認相關聯的網路通訊協定設定檔中每項設定的值均正確無誤。

有關作業系統識別碼不受支援的警告訊息

警告訊息顯示指定的作業系統識別碼 SUSE Linux Enterprise Server 12.0 64-bit (id:85) 在選定主機上不受支援。它與以下 OS 識別碼對應：Other Linux (64-bit)。

請忽略這則警告訊息。它會自動與支援的作業系統對應。

針對 RSA SecurID 驗證設定 Access Point

將以下文字行加入 .INI 檔案的 Horizon 區段。

```
authMethods=securid-auth && sp-auth
matchWindowsUserName=true
```

在 .INI 檔案的底部新增區段。

```
[SecurIDAuth]
serverConfigFile=C:\temp\sdconf.rec
externalHostName=192.168.0.90
internalHostName=192.168.0.90
```

兩個 IP 位址都應設定為 Access Point 的 IP 位址。sdconf.rec 檔案是從 RSA 驗證管理員取得的，該檔案的設定必須完整。請確認您使用的是 Access Point 2.5 或更新版本，而且可以從 Access Point 存取網路上的 RSA 驗證管理員伺服器。重新執行 apdeploy Powershell 命令，以重新部署針對 RSA SecurID 設定的 Access Point。

定位器無法參考物件錯誤

這則錯誤通知您 vSphere OVF Tool 使用的 target= 值不是 vCenter 環境所需的正確值。請使用 https://communities.vmware.com/docs/DOC-30835 列示的表格，以取得用來參考 vCenter 主機或叢集之目標格式的範例。最上層物件的指定方式如下：

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/
```

物件現可列出要在下一層使用的可能名稱。

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/Cluster1/
or
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esxhost1
```

在目標中使用的資料夾名稱、主機名稱及叢集名稱有區分大小寫。

從 Access Point 應用裝置收集記錄

您可在瀏覽器中輸入 URL，以取得包含 Access Point 應用裝置記錄的 ZIP 檔案。

使用下列 URL 可從 Access Point 應用裝置收集記錄。

```
https://access-point-appliance.example.com:9443/rest/v1/monitor/support-archive
```

在此範例中，*access-point-appliance.example.com* 是 Access Point 應用裝置的完整網域名稱。

這些記錄檔是從應用裝置的 `/opt/vmware/gateway/logs` 目錄收集而來。

下表包含 ZIP 檔案中所含各種檔案的說明。

表格 7-1. 包含有助於疑難排解之系統資訊的檔案

檔案名稱	說明
`df.log`	包含磁碟空間使用量的相關資訊。
`netstat.log`	包含網路連線的相關資訊。
`ap_config.json`	包含 Access Point 應用裝置的目前組態設定。
`ps.log`	包含處理程序清單。
`ifconfig.log`	包含網路介面的相關資訊。
`free.log`	包含記憶體使用量的相關資訊。

表格 7-2. Access Point 的記錄檔

檔案名稱	說明
`esmanager.log`	包含在連接埠 443 和 80 上進行接聽之 Edge Service Manager 處理程序的記錄訊息。
`authbroker.log`	包含負責處理驗證介面卡之 AuthBroker 處理程序的記錄訊息。
`admin.log`	包含在連接埠 9443 上提供 Access Point REST API 之處理程序的記錄訊息。
`admin-zookeeper.log`	包含用來儲存 Access Point 組態資訊之資料層的相關記錄訊息。
`tunnel.log`	包含做為 XML API 處理的一部分之通道處理程序的記錄訊息。
`bsg.log`	包含 Blast 安全閘道的記錄訊息。
`SecurityGateway_*.log`	包含 PCoIP 安全閘道的記錄訊息。

結尾是「`-std-out.log`」的記錄檔包含寫入至各種處理程序之 `stdout` 的資訊，而這些記錄檔通常是空白檔案。

AirWatch 的 Access Point 記錄檔

- `/var/log/airwatch/tunnel/vpnd`

  tunnel-init.log 和 tunnel.log 是擷取自此目錄。

- `/var/log.airwatch/proxy`

  proxy.log 是擷取自此目錄。

- `/var/log/airwatch/appliance-agent`

  appliance-agent.log 是擷取自此目錄。

啟用偵錯模式

您可以啟用 Access Point 應用裝置的偵錯模式，以便檢視或操縱應用裝置的內部狀態。偵錯模式可讓您在環境中測試部署案例。

先決條件

- 確認 Access Point 應用裝置並非使用中。

  備註 收集未運作之 Access Point 應用裝置的相關記錄資訊是實用的做法。記錄可依照典型的方法取得。

程序

1. 登入 Access Point 機器。
2. 在命令列介面中輸入以下命令。

   ```
   cd /opt/vmare/gateway/conf
   ```

3. 檢視記錄內容檔案。

   ```
   vi log4j-esmanager.properties
   ```

4. 在內容檔案中找出以下文字行並予以編輯。藉由偵錯來取代資訊。

   ```
   log4j.logger.com.vmware=info,default
   ```

5. 輸入命令以從任何路徑變更記錄組態。

   ```
   supervisorctl restart esmanager
   ```