部署及設定 VMware Unified Access Gateway

Unified Access Gateway 2103

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

部署及設定 VMware Unified Access Gateway

《部署及設定 Unified Access Gateway》會提供如何設計 VMware Horizon®、VMware Workspace ONE Access 和 Workspace ONE UEM 部署的相關資訊，這些部署會使用 VMware Unified Access Gateway™ 以便能夠從外部安全地存取組織的應用程式。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 Unified Access Gateway 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 Unified Access Gateway 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 VMware Unified Access Gateway

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，Unified Access Gateway 可做為安全閘道使用。

備註 VMware Unified Access Gateway® 先前稱為 VMware Access Point。

本章節討論下列主題：

Unified Access Gateway 作為安全閘道

Unified Access Gateway 為應用裝置，通常安裝在非軍事區 (DMZ) 中。Unified Access Gateway 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。

Unified Access Gateway 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。

Unified Access Gateway 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。

Unified Access Gateway 可作為您的公司信任網路內連線的 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。

Unified Access Gateway 專為 DMZ 所設計。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 Unified Access Gateway 而非虛擬私人網路

Unified Access Gateway 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。

Unified Access Gateway 優於通用 VPN 的方面包括下列項目。

- Access Control Manager。Unified Access Gateway 會自動套用存取規則。Unified Access Gateway 會辨識使用者的權利和在內部連線所需的定址。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。Unified Access Gateway 不會變更簡潔的 Horizon Client 使用者介面。利用 Unified Access Gateway，當 Horizon Client 啟動時，經驗證的使用者會在其 Horizon Connection Server 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。Unified Access Gateway 是專為將安全性和效能最大化而設計。有了 Unified Access Gateway，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 Horizon Connection Server 桌面平台通訊協定搭配運作。

Unified Access Gateway 系統和網路需求

若要部署 Unified Access Gateway 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 Unified Access Gateway 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。

如需 Unified Access Gateway 生命週期支援原則的相關資訊，請參閱 https://kb.vmware.com/s/article/2147313。

ESXi 伺服器的硬體需求

部署 Unified Access Gateway 應用裝置的 VMware vSphere 版本必須與 VMware 產品支援的版本相同。

如果您計劃要使用 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 Unified Access Gateway 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 Unified Access Gateway 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

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

- CPU 最低需求為 2000 MHz
- 至少 4 GB 記憶體

重要 Unified Access Gateway 是 VMware 虛擬應用裝置。VMware 利用已更新的虛擬應用裝置映像檔案來散佈安全性和一般修補程式。除了增加記憶體和透過 vCenter Server **編輯**設定執行的 vCPU 數量以外，不支援自訂 Unified Access Gateway 應用裝置或升級個別元件。

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 (取決於 Unified Access Gateway 版本)
- 精簡佈建磁碟最低需求為 3.5 GB
- 完整佈建磁碟最低需求為 20 GB

備註 除了最低磁碟需求之外，vSphere 也可以在 ESXi 資料存放區上為每部虛擬機器建立其他檔案，例如交換檔。磁碟空間也用於使用 vCenter Server 建立的任何虛擬機器快照。ESXi 資料存放區也包含每部虛擬機器的一些其他小型檔案。

如果未設定記憶體保留，vSphere 會建立每部虛擬機器的交換檔（`.vswp`），最高為虛擬機器記憶體的大小。此交換空間可用於任何未保留的虛擬機器記憶體。例如，具有 vSphere 完整佈建磁碟的 4 GB RAM Unified Access Gateway 應用裝置會使用 20 GB ESXi `.vmdk` 檔案，而應用裝置可使用 4 GB ESXi 交換檔。這會導致總磁碟空間需求為 24 GB。同樣地，針對具有 16 GB RAM 的 Unified Access Gateway 應用裝置，則總磁碟空間需求可能為 36 GB。

如需有關交換空間和記憶體過度認可的詳細資訊，請參閱《vSphere 資源管理》說明文件。

需要下列資訊才能部署虛擬應用裝置。

- 靜態 IP 位址 (建議)

- DNS 伺服器的 IP 位址
- 根使用者的密碼
- 管理員使用者的密碼
- Unified Access Gateway 應用裝置所指向負載平衡器之伺服器執行個體的 URL

Unified Access Gateway 大小調整選項

- **標準**：如果 Horizon 部署支援最多 2000 個 Horizon 連線，則建議使用此組態，以配合連線伺服器容量。針對並行連線最多 10,000 個的 Workspace ONE UEM 部署 (行動使用案例)，也建議使用此組態。
- **大型**：針對 Unified Access Gateway 需要支援超過 50,000 個並行連線的 Workspace ONE UEM 部署，建議使用此組態。此大小可讓 Content Gateway、每一應用程式通道和 Proxy 以及反向 Proxy 使用相同的 Unified Access Gateway 應用裝置。
- **超大型**：針對 Workspace ONE UEM 部署，建議使用此組態。此大小可讓 Content Gateway、每一應用程式通道和 Proxy 以及反向 Proxy 使用相同的 Unified Access Gateway 應用裝置。
- **備註** 標準、大型和超大型部署的虛擬機器選項：
  - 標準 - 2 核心和 4 GB RAM
  - 大型 - 4 核心和 16 GB RAM
  - 超大型 - 8 核心和 32 GB RAM

  您可以使用 PowerShell 設定這些設定。如需 PowerShell 參數的相關資訊，請參閱使用 PowerShell 來部署 Unified Access Gateway 應用裝置。

  如需 Unified Access Gateway 大小調整建議的詳細資訊，您可以查看 VMware 組態上限。

支援的瀏覽器版本

支援啟動管理員 UI 的瀏覽器為 Chrome、Firefox 和 Internet Explorer。請使用最新版本的瀏覽器。

使用 Windows Hyper-V Server 時的硬體需求

使用 Unified Access Gateway 進行 Workspace ONE UEM 每一應用程式通道部署時，您可以在 Microsoft Hyper-V 伺服器上安裝 Unified Access Gateway 應用裝置。

支援的 Microsoft 伺服器為 Windows Server 2012 R2 和 Windows Server 2016。

網路功能組態需求

您可以使用一個、兩個或三個網路介面，Unified Access Gateway 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 Unified Access Gateway 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。

多點傳送 DNS 和 .local 主機名稱

UAG (Unified Access Gateway) 3.7 及更新版本除了支援單點傳播 DNS 外，也支援多點傳送 DNS。網域尾碼為 .local 的多標籤名稱，會路由傳送至所有可使用多點傳送 DNS 通訊協定來執行 IP 多點傳送的本機介面。

請避免在單點傳播 DNS 伺服器中定義 .local，因為 RFC6762 會保留此網域供多點傳送 DNS 使用。例如，如果您在組態設定中使用某個主機名稱 hostname.example.local (如 UAG 上的 Proxy 目的地 URL)，則無法使用單點傳播 DNS 來解析此主機名稱，因為 .local 已保留供多點傳送 DNS 使用。

或者，您也可以使用下列其中一個不需要 .local 網域尾碼的方法：

- 指定 IP 位址，而非指定 .local 主機名稱。
- 您可以在 DNS 伺服器中新增其他的替代 DNS A 記錄。

  在前面的主機名稱範例中，您可以將 hostname.example.int 新增至與 hostname.example.local 相同的 IP 位址中，並將其用在 UAG 組態內。
- 您可以定義本機 hosts 檔案項目。

  在前面的範例中，您可以為 hostname.example.local 定義本機 hosts 項目。

  hosts 檔案項目會指定名稱和 IP 位址，並可藉由使用 UAG 管理員 UI 或透過 PowerShell .ini 檔案設定來加以設定。

  重要 UAG 上的 /etc/hosts 檔案不得進行編輯。

  在 UAG 上，系統會先搜尋本機 hosts 檔案項目，然後才會執行 DNS 搜尋。此類搜尋可確保當主機名稱存在於 hosts 檔案上時，系統便可使用 .local 名稱，而且完全不需要進行 DNS 搜尋。

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。Unified Access Gateway 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 Unified Access Gateway 應用裝置收集記錄。

DMZ 型 Unified Access Gateway 應用裝置的防火牆規則

DMZ 型 Unified Access Gateway 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，Unified Access Gateway 服務預設設為接聽特定網路連接埠。

DMZ 型 Unified Access Gateway 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。

下表列出 Unified Access Gateway 內不同服務的連接埠需求。

備註 所有 UDP 連接埠都需要允許轉送資料包和回覆資料包。

表 1-1. Secure Email Gateway 的連接埠需求

連接埠	通訊協定	來源	目標/目的地	說明
443* 或任何大於 1024 的連接埠	HTTPS	裝置 (從網際網路和 Wi-Fi)	Unified Access Gateway Secure Email Gateway 端點	Secure Email Gateway 會接聽連接埠 11443
443* 或任何大於 1024 的連接埠	HTTPS	Workspace ONE UEM Console	Unified Access Gateway Secure Email Gateway 端點	Secure Email Gateway 會接聽連接埠 11443
443* 或任何大於 1024 的連接埠	HTTPS	Email Notification Service (啟用時)	Unified Access Gateway Secure Email Gateway 端點	Secure Email Gateway 會接聽連接埠 11443
5701	HTTP	Secure Email Gateway	Secure Email Gateway	用於 Hazelcast 分散式快取
41232	HTTPS	Secure Email Gateway	Secure Email Gateway	用於 Vertx 叢集管理
44444	HTTPS	Secure Email Gateway	Secure Email Gateway	用於診斷和管理功能

備註 由於 Secure Email Gateway (SEG) 服務會以非根使用者的身分在 Unified Access Gateway 上執行，因此 SEG 無法在系統連接埠上執行。因此，自訂連接埠必須大於連接埠 1024。

表 1-2. Horizon 的連接埠需求

連接埠	通訊協定	來源	目標	說明
443	TCP	網際網路	Unified Access Gateway	針對 Web 流量，Horizon Client XML - API、Horizon Tunnel 和 Blast Extreme
443	UDP	網際網路	Unified Access Gateway	UDP 443 會在內部轉送至 Unified Access Gateway 上 UDP 通道伺服器服務的 UDP 9443。
8443	UDP	網際網路	Unified Access Gateway	Blast Extreme (選用)
8443	TCP	網際網路	Unified Access Gateway	Blast Extreme (選用)
4172	TCP 與 UDP	網際網路	Unified Access Gateway	PCoIP (選用)

表 1-2. Horizon 的連接埠需求 (續)

連接埠	通訊協定	來源	目標	說明
443	TCP	Unified Access Gateway	Horizon 連線伺服器	Horizon Client XML-API、Blast extreme HTML Access、Horizon Air 主控台存取 (HACA)
22443	TCP 與 UDP	Unified Access Gateway	桌面平台和 RDS 主機	Blast Extreme
4172	TCP 與 UDP	Unified Access Gateway	桌面平台和 RDS 主機	PCoIP (選用)
32111	TCP	Unified Access Gateway	桌面平台和 RDS 主機	USB 重新導向的架構通道
3389	TCP	Unified Access Gateway	桌面平台和 RDS 主機	僅在 Horizon Client 使用 RDP 通訊協定時需要。
9427	TCP	Unified Access Gateway	桌面平台和 RDS 主機	MMR 和 CDR

備註 若要允許外部用戶端裝置連線至 DMZ 內的 Unified Access Gateway 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 連線至 DMZ 內的 Unified Access Gateway 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 8443，但您也可以設定 Blast 使用連接埠 443。

表 1-3. Web 反向 Proxy 的連接埠需求

連接埠	通訊協定	來源	目標	說明
443	TCP	網際網路	Unified Access Gateway	針對 Web 流量
任意	TCP	Unified Access Gateway	內部網路網站	任何已設定且由內部網路接聽中的自訂連接埠。例如 80、443 和 8080 等。
88	TCP	Unified Access Gateway	KDC 伺服器/AD 伺服器	如果設定了對 Kerberos 的 SAML/對 Kerberos 的憑證，則需要身分識別橋接以存取 AD。
88	UDP	Unified Access Gateway	KDC 伺服器/AD 伺服器	如果設定了對 Kerberos 的 SAML/對 Kerberos 的憑證，則需要身分識別橋接以存取 AD。

表 1-4. 管理員 UI 的連接埠需求

連接埠	通訊協定	來源	目標	說明
9443	TCP	管理員 UI	Unified Access Gateway	管理介面

表 1-5. Content Gateway 基本端點組態的連接埠需求

連接埠	通訊協定	來源	目標	說明
443* 或任何連接埠 > 1024	HTTPS	裝置 (從網際網路和 Wi-Fi)	Unified Access Gateway Content Gateway 端點	如果使用 443，則 Content Gateway 會在連接埠 10443 上接聽。
443* 或任何連接埠 > 1024	HTTPS	Workspace ONE UEM 裝置服務	Unified Access Gateway Content Gateway 端點	
443* 或任何連接埠 > 1024	HTTPS	Workspace ONE UEM 主控台	Unified Access Gateway Content Gateway 端點	如果使用 443，則 Content Gateway 會在連接埠 10443 上接聽。
443* 或任何連接埠 > 1024	HTTPS	Unified Access Gateway Content Gateway 端點	Workspace ONE UEM API Server	
存放庫正在接聽的任何連接埠。	HTTP 或 HTTPS	Unified Access Gateway Content Gateway 端點	Web 型內容存放庫，例如 SharePoint/WebDAV/ CMIS 等	任何已設定且由內部網路網站接聽中的自訂連接埠。
137–139 和 445	CIFS 或 SMB	Unified Access Gateway Content Gateway 端點	網路共用型存放庫 (Windows 檔案共用)	內部網路共用

表 1-6. Content Gateway 轉送端點組態的連接埠需求

連接埠	通訊協定	來源	目標/目的地	說明
443* 或任何連接埠 > 1024	HTTP/ HTTPS	Unified Access Gateway 轉送伺服器 (Content Gateway 轉送)	Unified Access Gateway Content Gateway 端點	如果使用 443，則 Content Gateway 會在連接埠 10443 上接聽。
443* 或任何連接埠 > 1024	HTTPS	裝置 (從網際網路和 Wi-Fi)	Unified Access Gateway 轉送伺服器 (Content Gateway 轉送)	如果使用 443，則 Content Gateway 會在連接埠 10443 上接聽。
443* 或任何連接埠 > 1024	TCP	Workspace ONE UEM 裝置服務	Unified Access Gateway 轉送伺服器 (Content Gateway 轉送)	如果使用 443，則 Content Gateway 會在連接埠 10443 上接聽。
443* 或任何連接埠 > 1024	HTTPS	Workspace ONE UEM Console		

表 1-6. Content Gateway 轉送端點組態的連接埠需求 (續)

連接埠	通訊協定	來源	目標/目的地	說明
443* 或任何連接埠 > 1024	HTTPS	Unified Access Gateway Content Gateway 轉送	Workspace ONE UEM API 伺服器	
443* 或任何連接埠 > 1024	HTTPS	Unified Access Gateway Content Gateway 端點	Workspace ONE UEM API 伺服器	
存放庫正在接聽的任何連接埠。	HTTP 或 HTTPS	Unified Access Gateway Content Gateway 端點	Web 型內容存放庫，例如 SharePoint/WebDAV/ CMIS 等	任何已設定且由內部網路網站接聽中的自訂連接埠。
443* 或任何連接埠 > 1024	HTTPS	Unified Access Gateway (Content Gateway 轉送)	Unified Access Gateway Content Gateway 端點	如果使用 443，則 Content Gateway 會在連接埠 10443 上接聽。
137–139 和 445	CIFS 或 SMB	Unified Access Gateway Content Gateway 端點	網路共用型存放庫 (Windows 檔案共用)	內部網路共用

備註 由於 Content Gateway 服務在 Unified Access Gateway 中會以非根使用者的身分執行，Content Gateway 無法在系統連接埠上執行，因此自訂連接埠應 > 1024。

表 1-7. VMware Tunnel 的連接埠需求

連接埠	通訊協定	來源	目標/目的地	驗證	附註 (請參閱頁面底部的「附註」一節)
2020 *	HTTPS	裝置 (從網際網路和 Wi-Fi)	VMware Tunnel 代理伺服器	安裝完成後請執行下列命令：`netstat -tlpn | grep [Port]`	
8443 *	TCP、UDP	裝置 (從網際網路和 Wi-Fi)	VMware Tunnel 每一應用程式通道	安裝完成後請執行下列命令：`netstat -tlpn | grep [Port]`	1

表 1-8. VMware Tunnel 基本端點組態

連接埠	通訊協定	來源	目標/目的地	驗證	附註 (請參閱頁面底部的「附註」一節)
SaaS：443：2001 *	HTTPS	VMware Tunnel	Workspace ONE UEM Cloud Messaging 伺服器	`curl -Ivv https://<AWCM URL>:<port>/awcm/status/ping` 預期的回應為 HTTP 200 確定。	2
SaaS：443 內部部署：80 或 443	HTTP 或 HTTPS	VMware Tunnel	Workspace ONE UEM REST API 端點 ■ SaaS：`https://asXXX.awmdm.com` 或 `https://asXXX.airwatchportals.com` ■ 內部部署：通常是您的 DS 或主控台伺服器	`curl -Ivv https://<API URL>/api/mdm/ping` 預期的回應是 HTTP 401 未經授權。	5
80、443、任何 TCP	HTTP、HTTPS 或 TCP	VMware Tunnel	內部資源	確認 VMware Tunnel 可透過必要的連接埠存取內部資源。	4
514 *	UDP	VMware Tunnel	Syslog 伺服器		
內部部署：2020	HTTPS	Workspace ONE UEM 主控台	VMware Tunnel 代理伺服器	內部部署使用者可以使用 `telnet` 命令測試連線：`telnet <Tunnel Proxy URL> <port>`	6

表 1-9. VMware Tunnel 階層式組態

連接埠	通訊協定	來源	目標/目的地	驗證	附註 (請參閱頁面底部的「附註」一節)
SaaS：443 內部部署：2001 *	TLS v1.2	VMware Tunnel 前端	Workspace ONE UEM Cloud Messaging 伺服器	對 `https://<AWCM URL>:<port>/awcm/status` 使用 `wget`，並確定您收到 HTTP 200 回應以進行驗證。	2
8443	TLS v1.2	VMware Tunnel 前端	VMware Tunnel 後端	使用 Telnet 從 VMware Tunnel 前端連線至連接埠上的 VMware Tunnel 後端伺服器	3

表 1-9. VMware Tunnel 階層式組態 (續)

連接埠	通訊協定	來源	目標/目的地	驗證	附註 (請參閱頁面底部的「附註」一節)
SaaS：443 內部部署：2001	TLS v1.2	VMware Tunnel 後端	Workspace ONE UEM Cloud Messaging 伺服器	對 `https://<AWCM URL>:<port>/awcm/status` 使用 `wget`，並確定您收到 HTTP 200 回應以進行驗證。	2
80 或 443	TCP	VMware Tunnel 後端	內部網站/Web 應用程式		4
80、443、任何 TCP	TCP	VMware Tunnel 後端	內部資源		4
80 或 443	HTTPS	VMware Tunnel 前端和後端	Workspace ONE UEM REST API 端點 ■ SaaS：`https://asXXX.awmdm.com` 或 `https://asXXX.airwatchportals.com` ■ 內部部署：通常是您的 DS 或主控台伺服器	`curl -Ivv https://<API URL>/api/mdm/ping` 預期的回應是 HTTP 401 未經授權。	5

表 1-10. VMware Tunnel 前端和後端組態

連接埠	通訊協定	來源	目標/目的地	驗證	附註 (請參閱頁面底部的「附註」一節)
SaaS：443 內部部署：2001	HTTP 或 HTTPS	VMware Tunnel 前端	Workspace ONE UEM Cloud Messaging 伺服器	`curl -Ivv https://<AWCM URL>:<port>/awcm/status/ping` 預期的回應為 HTTP 200 確定。	2
80 或 443	HTTP 或 HTTPS	VMware Tunnel 後端和前端	Workspace ONE UEM REST API 端點 ■ SaaS：`https://asXXX.awmdm.com` 或 `https://asXXX.airwatchportals.com` ■ 內部部署：通常是您的 DS 或主控台伺服器	`curl -Ivv https://<API URL>/api/mdm/ping` 預期的回應是 HTTP 401 未經授權。 僅在初始部署期間，VMware Tunnel 端點才需要存取 REST API 端點。	5

表 1-10. VMware Tunnel 前端和後端組態 (續)

連接埠	通訊協定	來源	目標/目的地	驗證	附註 (請參閱頁面底部的「附註」一節)
2010 *	HTTPS	VMware Tunnel 前端	VMware Tunnel 後端	使用 Telnet 從 VMware Tunnel 前端連線至連接埠上的 VMware Tunnel 後端伺服器	3
80、443、任何 TCP	HTTP、HTTPS 或 TCP	VMware Tunnel 後端	內部資源	確認 VMware Tunnel 可透過必要的連接埠存取內部資源。	4
514 *	UDP	VMware Tunnel	Syslog 伺服器		
內部部署：2020	HTTPS	Workspace ONE UEM	VMware Tunnel 代理伺服器	內部部署使用者可以使用 `telnet` 命令測試連線：`telnet <Tunnel Proxy URL> <port>`	6

下列幾點對於 VMware Tunnel 需求有效。

備註 * - 此連接埠可在必要時根據您的環境限制進行變更

1 如果使用連接埠 443，則每一應用程式通道會在連接埠 8443 上接聽。

   備註 在相同的應用裝置上啟用 VMware Tunnel 和 Content Gateway 服務，並啟用 TLS 連接埠共用時，每項服務的 DNS 名稱都必須是唯一的。未啟用 TLS 時，這兩項服務只能使用一個 DNS 名稱，因為連接埠將會區分傳入流量。(針對 Content Gateway，如果使用 443，則 Content Gateway 會在連接埠 10443 上接聽。)

2 供 VMware Tunnel 查詢 Workspace ONE UEM 主控台以進行符合性和追蹤用途。

3 僅供 VMware Tunnel 前端拓撲將裝置要求轉送至內部 VMware Tunnel 後端。

4 供使用 VMware Tunnel 的應用程式存取內部資源。

5 VMware Tunnel 必須與 API 通訊以進行初始化。確定 REST API 與 VMware Tunnel 伺服器之間有連線存在。導覽至**群組和設定 > 所有設定 > 系統 > 進階 > 站台 URL**，以設定 REST API 伺服器 URL。此頁面不適用於 SaaS 客戶。SaaS 客戶的 REST API URL 通常是您的主控台或裝置服務伺服器 URL。

6 若要從 Workspace ONE UEM 主控台對 VMware Tunnel Proxy 成功執行「測試連線」，則必須符合此需求。此需求為選用，可以省略而不會遺失裝置的功能。針對 SaaS 客戶，Workspace ONE UEM 主控台可能已因為連接埠 2020 上的輸入網際網路需求，會在連接埠 2020 上具有 VMware Tunnel Proxy 的輸入連線。

部署 VMware Tunnel 與 Unified Access Gateway 的系統需求

若要部署具有 Unified Access Gateway 的 VMware Tunnel，請確定您的系統符合下列需求：

Hypervisor 需求

部署 VMware Tunnel 的 Unified Access Gateway 需要以 Hypervisor 部署虛擬應用裝置。您必須有具備完整權限可部署 OVF 的專用管理員帳戶。

支援的 Hypervisor

- VMware vSphere Web Client

  備註 對於特定版本的 Unified Access Gateway，您必須使用特定版本的 VMware 產品。部署 Unified Access Gateway 應用裝置的 VMware vSphere 版本必須與 VMware 產品支援的版本相同。

- Windows Server 2012 R2 或 Windows Server 2016 上的 Microsoft Hyper-V

軟體需求

確定您有最新版的 Unified Access Gateway。VMware Tunnel 支援 Unified Access Gateway 與 Workspace ONE UEM Console 之間的回溯相容性。回溯相容性可讓您在升級您 Workspace ONE UEM Console 之後立即升級 VMware Tunnel 伺服器。若要確保 Workspace ONE UEM Console 與 VMware Tunnel 之間的對等性，請考慮盡早升級。

硬體需求

Unified Access Gateway 的 OVF 套件會自動選取 VMware Tunnel 需要的虛擬機器組態。雖然您可以變更這些設定，但請勿將 CPU、記憶體或磁碟空間變更為比預設 OVF 設定還要小的值。

若要變更預設設定，請在 vCenter 中關閉虛擬機器的電源。以滑鼠右鍵按一下虛擬機器，然後選取**編輯設定**。

預設組態會使用 4 GB 的 RAM 和 2 個 CPU。您必須依據自己的硬體需求變更預設組態。為了處理所有的裝置負載和維護需求，建議您至少應執行兩個 VMware Tunnel 伺服器。

表 1-11. 硬體需求

裝置數目	最多 40000	40000-80000	80000-120000	120000-160000
伺服器數目	2	3	4	5
CPU 核心	4 個 CPU 核心*	各有 4 個 CPU 核心	各有 4 個 CPU 核心	各有 4 個 CPU 核心
RAM (GB)	8	8	8	8
硬碟空間 (GB)	10 GB 用於發行版 (僅限 Linux) 400 MB 用於安裝程式 約 10 GB 作為記錄檔空間**			

*您可以僅部署單一 VMware Tunnel 應用裝置，作為較小部署的一部分。但基於運作時間和效能考量，建議您至少應部署兩部各具有四個 CPU 核心的負載平衡伺服器，無論裝置數目為何。

**10 GB 用於一般部署。請根據您的記錄使用方式和儲存記錄的需求擴充記錄檔大小。

VMware Tunnel Proxy 伺服器的連接埠需求

您可以使用下列兩種組態模式之一來設定 VMware Tunnel Proxy 伺服器：

- 使用 VMware Tunnel Proxy 伺服器端點的基本端點 (單層)
- 使用 VMware Tunnel Proxy 伺服器轉送和 VMware Tunnel Proxy 伺服器端點的轉送端點 (多層)

表 1-12. VMware Tunnel Proxy 伺服器基本端點組態的連接埠需求

來源	目標或目的地	通訊協定	連接埠	驗證	備註
裝置 (從網際網路和 Wi-Fi)	VMware Tunnel Proxy 伺服器端點	HTTPS	2020*	安裝完成後請執行下列命令：`netstat -tlpn | grep [Port]`	裝置會透過指定的連接埠連線至為 VMware Tunnel 設定的公用 DNS。
VMware Tunnel Proxy 伺服器端點	Workspace ONE UEM Cloud Messaging 伺服器	HTTPS	SaaS：443 內部部署：2001*	`curl -Ivv https://<AWCM URL>:<port>/awcm/status/ping` 預期的回應是 `HTTP 200 OK`。	供 VMware Tunnel Proxy 伺服器查詢 Workspace ONE UEM 主控台以進行符合性和追蹤用途。為此至少須支援 TLS 1.2。
VMware Tunnel Proxy 伺服器端點	UEM REST API ■ SaaS‡：https://asXXX.awmdm.com 或 https://asXXX.airwatchportals.com ■ 內部部署†：通常是裝置服務或主控台伺服器	HTTP 或 HTTPS	SaaS：443 內部部署：2001*	`curl -Ivv https://<API URL>/api/mdm/ping` 預期的回應是 `HTTP 401 unauthorized`	VMware Tunnel Proxy 伺服器必須與 UEM REST API 通訊以進行初始化。在 Workspace ONE UEM 主控台中，移至**群組和設定 > 所有設定 > 系統 > 進階 > 站台 URL**，以設定 **REST API URL**。此頁面不適用於 Workspace ONE UEM SaaS 客戶。Workspace ONE UEM SaaS 客戶的 **REST API URL** 通常是**主控台 URL** 或**裝置服務 URL**。
VMware Tunnel Proxy 伺服器端點	內部資源	HTTP、HTTPS 或 TCP	80、443、任何 TCP	確認 VMware Tunnel Proxy 伺服器端點可透過必要的連接埠存取內部資源。	供使用 VMware Tunnel Proxy 伺服器的應用程式存取內部資源。確切的端點或連接埠取決於這些資源的所在位置。

表 1-12. VMware Tunnel Proxy 伺服器基本端點組態的連接埠需求 (續)

來源	目標或目的地	通訊協定	連接埠	驗證	備註
VMware Tunnel Proxy 伺服器端點	Syslog 伺服器	UDP	514*		
Workspace ONE UEM Console	VMware Tunnel Proxy 伺服器端點	HTTPS	2020*	內部部署† 客戶可以使用 Telnet 命令來測試連線：`telnet <TunnelProxyURL><port>`	這是從 Workspace ONE UEM Console 到 VMware Tunnel Proxy 伺服器端點的「測試連線」成功的必要條件。

表 1-13. VMware Tunnel Proxy 伺服器轉送端點組態的連接埠需求

來源	目標或目的地	通訊協定	連接埠	驗證	備註
裝置 (從網際網路和 Wi-Fi)	VMware Tunnel Proxy 伺服器轉送	HTTPS	2020*	安裝完成後請執行下列命令：`netstat -tlpn | grep [Port]`	裝置會透過指定的連接埠連線至為 VMware Tunnel 設定的公用 DNS。
VMware Tunnel Proxy 伺服器轉送	Workspace ONE UEM Cloud Messaging 伺服器	HTTP 或 HTTPS	SaaS：443 內部部署：2001*	`curl -Ivv https://<AWCM URL>:<port>/awcm/status/ping` 預期的回應是 `HTTP 200 OK`。	供 VMware Tunnel Proxy 伺服器查詢 Workspace ONE UEM 主控台以進行符合性和追蹤用途。為此至少須支援 TLS 1.2。
VMware Tunnel Proxy 伺服器轉送	UEM REST API ■ SaaS‡：https://asXXX.awmdm.com 或 https://asXXX.airwatchportals.com ■ 內部部署†：通常是裝置服務或主控台伺服器	HTTP 或 HTTPS	SaaS：443 內部部署：2001*	`curl -Ivv https://<API URL>/api/mdm/ping` 預期的回應是 `HTTP 401 unauthorized` 只有在初始部署期間，VMware Tunnel Proxy 伺服器轉送才需要存取 UEM REST API。	VMware Tunnel Proxy 伺服器必須與 UEM REST API 通訊以進行初始化。在 Workspace ONE UEM 主控台中，移至**群組和設定 > 所有設定 > 系統 > 進階 > 站台 URL**，以設定 **REST API URL**。此頁面不適用於 Workspace ONE UEM SaaS 客戶。Workspace ONE UEM SaaS 客戶的 **REST API URL** 通常是**主控台 URL** 或**裝置服務 URL**。

表 1-13. VMware Tunnel Proxy 伺服器轉送端點組態的連接埠需求 (續)

來源	目標或目的地	通訊協定	連接埠	驗證	備註
VMware Tunnel Proxy 伺服器端點	UEM REST API ■ SaaS‡：https://asXXX.awmdm.com 或 https://asXXX.airwatchportals.com ■ 內部部署†：通常是裝置服務或主控台伺服器	HTTP 或 HTTPS	SaaS：443 內部部署：2001*	`curl -Ivv https://<API URL>/api/mdm/ping` 預期的回應是 `HTTP 401 unauthorized` 只有在初始部署期間，VMware Tunnel Proxy 伺服器轉送才需要存取 UEM REST API。	VMware Tunnel Proxy 伺服器必須與 UEM REST API 通訊以進行初始化。在 Workspace ONE UEM 主控台中，移至**群組和設定 > 所有設定 > 系統 > 進階 > 站台 URL**，以設定 **REST API URL**。此頁面不適用於 Workspace ONE UEM SaaS 客戶。Workspace ONE UEM SaaS 客戶的 **REST API URL** 通常是**主控台 URL** 或**裝置服務 URL**。
VMware Tunnel Proxy 伺服器轉送	VMware Tunnel Proxy 伺服器端點	HTTPS	2010*	在連接埠 2010 上執行從 VMware Tunnel Proxy 伺服器轉送到 VMware Tunnel Proxy 伺服器端點的 Telnet。	將裝置要求從轉送伺服器轉送至端點伺服器。為此至少須支援 TLS 1.2。
VMware Tunnel Proxy 伺服器端點	內部資源	HTTP、HTTPS 或 TCP	80、443、任何 TCP	確認 VMware Tunnel Proxy 伺服器端點可透過必要的連接埠存取內部資源。	供使用 VMware Tunnel Proxy 伺服器的應用程式存取內部資源。確切的端點或連接埠取決於這些資源的所在位置。
VMware Tunnel Proxy 伺服器端點	Syslog 伺服器	UDP	514*		
Workspace ONE UEM 主控台	VMware Tunnel Proxy 伺服器轉送	HTTPS	2020*	內部部署† 客戶可以使用 Telnet 命令來測試連線：`telnet <Tunnel ProxyURL><port>`	這是從 Workspace ONE UEM Console 到 VMware Tunnel Proxy 伺服器轉送的「測試連線」成功的必要條件。

備註

- * 此連接埠可能根據您的環境限制而變更。
- † 內部部署表示 Workspace ONE UEM 主控台的位置。

- ‡ 若是需要允許輸出通訊的 SaaS 客戶，請參閱列出最新 IP 範圍的 VMware 知識庫文章：https://support.workspaceone.com/articles/115001662168-。

VMware 每一應用程式通道的連接埠需求

您可以使用下列兩種組態模式之一來設定 VMware 每一應用程式通道：

- 使用 VMware 每一應用程式通道基本端點的基本端點 (單層)
- 使用 VMware 每一應用程式通道前端和 VMware 每一應用程式通道後端的階層式 (多層)

表 1-14. VMware 每一應用程式通道基本端點組態的連接埠需求

來源	目的地	通訊協定	連接埠	驗證	備註
裝置 (從網際網路和 Wi-Fi)	VMware 每一應用程式通道基本端點	TCP、UDP	8443*	安裝完成後請執行下列命令：`netstat -tlpn | grep [Port]`	裝置會透過指定的連接埠連線至為 VMware Tunnel 設定的公用 DNS。如果使用 443，則每一應用程式通道元件會在連接埠 8443 上接聽。
VMware 每一應用程式通道基本端點	Workspace ONE UEM Cloud Messaging 伺服器	HTTPS	SaaS：443 內部部署：2001*	對 `https://<AWCM URL>:<port>/awcm/status` 使用 `wget`，並確定您收到 `HTTP 200` 回應以進行驗證。	供 VMware 每一應用程式通道查詢 Workspace ONE UEM 主控台以進行符合性和追蹤用途。為此至少須支援 TLS 1.2。

表 1-14. VMware 每一應用程式通道基本端點組態的連接埠需求 (續)

來源	目的地	通訊協定	連接埠	驗證	備註
VMware 每一應用程式通道基本端點	內部網站/Web 應用程式/資源	HTTP、HTTPS 或 TCP	80、443、任何必要的 TCP		供使用 VMware 每一應用程式通道的應用程式存取內部資源。確切的端點或連接埠取決於這些資源的所在位置。
VMware 每一應用程式通道基本端點	UEM REST API ■ SaaS‡：https://asXXX.awmdm.com 或 https://asXXX.airwatchportals.com ■ 內部部署†：通常是裝置服務或主控台伺服器	HTTP 或 HTTPS	80 或 443	`curl -Ivv https://<API URL>/api/mdm/ping` 預期的回應是 `HTTP 401 unauthorized`	VMware 每一應用程式通道必須與 UEM REST API 通訊以進行初始化。在 Workspace ONE UEM 主控台中，移至**群組和設定 > 所有設定 > 系統 > 進階 > 站台 URL**，以設定 **REST API URL**。此頁面不適用於 Workspace ONE UEM SaaS 客戶。Workspace ONE UEM SaaS 客戶的 **REST API URL** 通常是**主控台 URL** 或**裝置服務 URL**。

表 1-15. VMware 每一應用程式通道階層式組態的連接埠需求

來源	目的地	通訊協定	連接埠	驗證	備註
裝置 (從網際網路和 Wi-Fi)	VMware 每一應用程式通道前端	TCP、UDP	8443*	安裝完成後請執行下列命令：`netstat -tlpn | grep [Port]`	裝置會透過指定的連接埠連線至為 VMware Tunnel 設定的公用 DNS。如果使用 443，則每一應用程式通道元件會在連接埠 8443 上接聽。
VMware 每一應用程式通道前端	Workspace ONE UEM Cloud Messaging 伺服器	HTTPS	SaaS：443 內部部署：2001*	對 `https://<AWCM URL>:<port>/awcm/status` 使用 `wget`，並確定您收到 `HTTP 200` 回應以進行驗證。	供 VMware 每一應用程式通道查詢 Workspace ONE UEM 主控台以進行符合性和追蹤用途。為此至少須支援 TLS 1.2。

表 1-15. VMware 每一應用程式通道階層式組態的連接埠需求 (續)

來源	目的地	通訊協定	連接埠	驗證	備註
VMware 每一應用程式通道前端	VMware 每一應用程式通道後端	TCP	8443	在連接埠 8443 上執行從 VMware 每一應用程式通道前端到 VMware 每一應用程式通道後端的 Telnet。	將裝置要求從前端伺服器轉送至後端伺服器。為此至少須支援 TLS 1.2。
VMware 每一應用程式通道後端	Workspace ONE UEM Cloud Messaging 伺服器	HTTPS	SaaS：443 內部部署：2001*	對 `https://<AWCM URL>:<port>/awcm/status` 使用 `wget`，並確定您收到 `HTTP 200` 回應以進行驗證。	供 VMware 每一應用程式通道查詢 Workspace ONE UEM 主控台以進行符合性和追蹤用途。為此至少須支援 TLS 1.2。
VMware Tunnel 後端	內部網站/Web 應用程式/資源	HTTP、HTTPS 或 TCP	80、443、任何必要的 TCP		供使用 VMware 每一應用程式通道的應用程式存取內部資源。確切的端點或連接埠取決於這些資源的所在位置。

表 1-15. VMware 每一應用程式通道階層式組態的連接埠需求 (續)

來源	目的地	通訊協定	連接埠	驗證	備註
VMware 每一應用程式通道前端	UEM REST API ■ SaaS‡ : https://asXXX.awmdm.com 或 https://asXXX.airwatchportals.com ■ 內部部署† : 通常是裝置服務或主控台伺服器	HTTP 或 HTTPS	80 或 443	`curl -Ivv https://<API URL>/api/mdm/ping` 預期的回應是 `HTTP 401 unauthorized`	VMware 每一應用程式通道必須與 UEM REST API 通訊以進行初始化。在 Workspace ONE UEM 主控台中，移至**群組和設定 > 所有設定 > 系統 > 進階 > 站台 URL**，以設定 **REST API URL**。此頁面不適用於 Workspace ONE UEM SaaS 客戶。Workspace ONE UEM SaaS 客戶的 **REST API URL** 通常是**主控台 URL** 或**裝置服務 URL**。
VMware 每一應用程式通道後端	UEM REST API ■ SaaS‡ : https://asXXX.awmdm.com 或 https://asXXX.airwatchportals.com ■ 內部部署† : 通常是裝置服務或主控台伺服器	HTTP 或 HTTPS	80 或 443	`curl -Ivv https://<API URL>/api/mdm/ping` 預期的回應是 `HTTP 401 unauthorized`	VMware 每一應用程式通道必須與 UEM REST API 通訊以進行初始化。在 Workspace ONE UEM 主控台中，移至**群組和設定 > 所有設定 > 系統 > 進階 > 站台 URL**，以設定 **REST API URL**。此頁面不適用於 Workspace ONE UEM SaaS 客戶。Workspace ONE UEM SaaS 客戶的 **REST API URL** 通常是**主控台 URL** 或**裝置服務 URL**。

備註

- * 此連接埠可能根據您的環境限制而變更。
- † 內部部署表示 Workspace ONE UEM 主控台的位置。
- ‡ 若是需要允許輸出通訊的 SaaS 客戶，請參閱以下 VMware 知識庫文章，其中列出目前的最新 IP 範圍：SaaS 資料中心的 VMware Workspace ONE IP 範圍。

網路介面連線需求

您可以使用一、二或三個網路介面。每個介面應有不同的 IP 位址。許多安全 DMZ 實作都會使用區隔的網路來隔離不同的流量類型。

請根據虛擬應用裝置部署所在之 DMZ 的網路設計來設定該裝置。如需網路 DMZ 的相關資訊，請洽詢網路管理員。

- 使用一個網路介面時，外部、內部和管理流量都會在同一個子網路上。
- 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。
- 使用第三個網路介面時，外部、內部和管理流量都會有其各自的子網路。

備註 使用多個網路介面部署時，每個網路介面必須位於不同的子網路上。

Unified Access Gateway 負載平衡拓撲

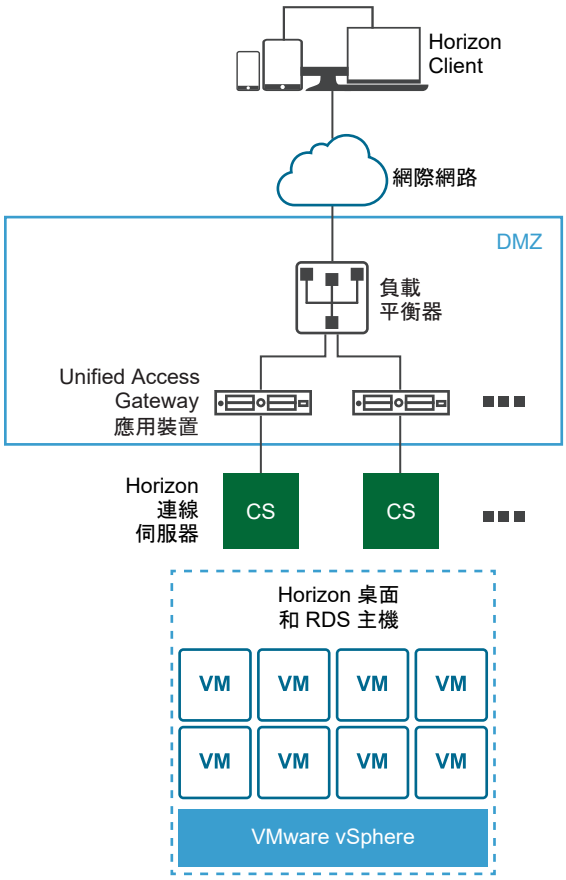
DMZ 中的 Unified Access Gateway 應用裝置可以設定為指向某個伺服器或位於一組伺服器前方的負載平衡器。Unified Access Gateway 應用裝置可與設定為使用 HTTPS 的標準第三方負載平衡解決方案搭配運作。

備註 Unified Access Gateway 已通過認證，可在將 Unified Access Gateway 部署為 Web 反向 Proxy 時與 Avi Vantage 負載平衡器搭配使用。

若 Unified Access Gateway 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 Unified Access Gateway 時，您可以將 Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway 應用裝置前方使用負載平衡器。

圖 1-1. 負載平衡器後方多個 Unified Access Gateway 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。此通訊協定透過 HTTPS 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。在上圖「負載平衡器後方多個 Unified Access Gateway 應用裝置」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 Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway 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、TCP 8443、UDP 443 和 UDP 8443)
- 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主要 Horizon 通訊協定路由傳送到的相同 Unified Access Gateway 應用裝置。然後 Unified Access Gateway 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。Unified Access Gateway 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，Unified Access Gateway 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 Unified Access Gateway 應用裝置，而非主要通訊協定應用裝置，則使用者不會獲得授權，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。

Content Gateway 和通道代理伺服器的負載平衡考量事項

當您使用負載平衡器搭配 Content Gateway 和通道代理伺服器時，請留意下列考量事項：

- 設定負載平衡器來「傳送原始 HTTP 標頭」以避免裝置發生連線問題。Content Gateway 和通道代理伺服器會使用要求 HTTP 標頭中的資訊來驗證裝置。
- 每一應用程式通道元件會要求每個用戶端在連線建立後進行驗證。連線之後，系統將會為用戶端建立一個工作階段並儲存在記憶體中。如此一來，每一項用戶端資料都會使用相同的工作階段，讓資料可以使用相同的金鑰進行加密和解密。設計負載平衡解決方案時，必須在啟用 IP/工作階段型持續性的情況下設定負載平衡器。替代的解決方案可能是在用戶端上使用 DNS 循環配置資源，這表示用戶端針對每個連線可以選取不同的伺服器。

健全狀況監控

負載平衡器會藉由透過定期傳送 `HTTPS GET /favicon.ico` 要求來監控每個 Unified Access Gateway 應用裝置的健全狀況。例如，`https://uag1.myco-dmz.com/favicon.ico`。此監控設定於負載平衡器上。它將會執行此 `HTTPS GET`，並預期 Unified Access Gateway 的回應為 `"HTTP/1.1 200 OK"`，以得知其「狀況良好」。如果其回應是 `"HTTP/1.1 200 OK"` 以外的回應，或無法取得任何回應，則會將特定 Unified Access Gateway 應用裝置標示為關閉，且不會嘗試將用戶端要求路由傳送至該處。它將會繼續輪詢，以便偵測該應用裝置何時恢復可用狀態。

Unified Access Gateway 可置於「靜止」模式，且其後就不會再以 `"HTTP/1.1 200 OK"` 回應來回應負載平衡器健全狀況監控要求。此時它會以 `"HTTP/1.1 503"` 回應，指出 Unified Access Gateway 服務暫時無法使用。此設定通常在 Unified Access Gateway 應用裝置排定的維護、計劃的重新設定或計劃的升級之前使用。在此模式下，負載平衡器不會將新的工作階段導向至此應用裝置，因為此應用裝置會標示為無法使用，但可允許現有的工作階段繼續執行，直到使用者中斷連線或達到工作階段時間上限為止。因此，此作業並不會中斷現有的使用者工作階段。在經過整體工作階段計時器上限後 (通常為 10 小時)，應用裝置將可供維護。此功能可在策略中用來執行一組 Unified Access Gateway 應用裝置的輪流升級，讓使用者擁有不停機的服務。

設定用於負載平衡 UAG 的 Avi Vantage (用作 Web 反向 Proxy 時)

此處記載的資訊可協助您在將 Unified Access Gateway 部署為 Web 反向 Proxy 時，設定 Avi Vantage 以用作負載平衡解決方案。此組態涉及必須透過使用 Avi 控制器來執行的一組工作。

透過使用 Avi UI，您必須建立 IP 群組、建立自訂健全狀況監視器設定檔、建立集區、安裝 VIP 所需的 SSL 憑證，以及建立虛擬服務。

透過使用虛擬服務中使用的 VIP，您可以存取 Web 反向 Proxy。

必要條件

- 確保您已將 Unified Access Gateway 部署為 Web 反向 Proxy。

  部署為 Reverse Proxy

- 確保已部署 Avi 控制器，且您具有控制器和 Avi UI 的存取權。

  如需關於 Avi Vantage 的詳細資訊，請參閱 Avi 說明文件。

程序

1 建立 IP 群組

  建立具有需要用於負載平衡之 Unified Access Gateway 伺服器清單的 IP 群組。

2 建立自訂健全狀況監控設定檔

  在 Avi Vantage 上建立 Unified Access Gateway 的健全狀況監控設定檔。健全狀況監控設定檔用於監控 Unified Access Gateway 的健全狀況。

3 建立集區

  集區包含 Unified Access Gateway 伺服器的清單和 Unified Access Gateway 的健全狀況監控設定檔。系統會接著將集區新增至 VS (虛擬服務)。

4 安裝 VIP 所需的 SSL 憑證 (虛擬 IP)

  SSL 連線會在 Avi 虛擬服務終止。因此，必須將 SSL 憑證指派給虛擬服務。若要使此指派發生，則必須在 Avi Vantage 安裝 SSL 憑證。

5 建立虛擬服務

  使用 Unified Access Gateway 伺服器的 VIP 建立虛擬服務。這是用戶端裝置連線的 VIP。

建立 IP 群組

建立具有需要用於負載平衡之 Unified Access Gateway 伺服器清單的 IP 群組。

由於相同的 Unified Access Gateway 伺服器在兩個不同的集區中用作集區成員，因此 IP 群組可連結至集區，而非直接將伺服器連結至集區。對集區成員所做的任何組態變更，例如新增或移除伺服器，都必須在 IP 群組層級完成。

程序

1 從 Avi Vantage UI 導覽至**範本 > 群組**。

2 按一下**建立 IP 群組**。

3 輸入 **IP 群組名稱**。

4 在 **IP 資訊**區段中，輸入 Unified Access Gateway 伺服器的 IP 位址。

5 按一下**新增**。

6 按一下**儲存**。

後續步驟

建立自訂健全狀況監控設定檔

建立自訂健全狀況監控設定檔

在 Avi Vantage 上建立 Unified Access Gateway 的健全狀況監控設定檔。健全狀況監控設定檔用於監控 Unified Access Gateway 的健全狀況。

如需有關健全狀況監控設定檔的詳細資訊，請參閱 Avi 說明文件。

程序

1 從 Avi Vantage UI 導覽至**範本 > 設定檔 > 健全狀況監視器**。

2 按一下**建立**。

3 在**新增健全狀況監視器**視窗中，輸入 Unified Access Gateway 的設定檔資訊。

   a 將**健全狀況監視器連接埠**的值輸入為 `443`。

   b 將**用戶端要求資料**的值輸入為 `GET /favicon.ico HTTP/1.1`。

   c 將**回應碼**選取為 `2XX`。

   d 啟用 **SSL 屬性**。

   e 將 **SSL 設定檔**選取為 `System-Standard`。

   f 將**維護回應碼**的值輸入為 `503`。

4 按一下**儲存**。

後續步驟

建立集區

建立集區

集區包含 Unified Access Gateway 伺服器的清單和 Unified Access Gateway 的健全狀況監控設定檔。系統會接著將集區新增至 VS (虛擬服務)。

一般虛擬服務則指向一個集區。

程序

1 從 Avi Vantage UI 導覽至**應用程式 > 集區**。

2 按一下**建立集區**。

3 在**選取雲端**視窗中，選取屬於 VMware vCenter/vSphere ESX 雲端基礎結構類型的雲端。

   雲端基礎結構類型已設定為 Avi 控制器部署的一部分。

4 按**下一步**。

5 在**新增集區**視窗中，輸入下列項目以外的必要資訊：

a 在**負載平衡**欄位中，選擇使用 `Source IP Address` 作為雜湊金鑰的 `Consistent Hash`。

b 在**健全狀況監視器**區段中，按一下**新增作用中監視器**。

c 選取先前針對 Unified Access Gateway 所建立的健全狀況監視器。

6 選取**啟用 SSL**。

7 將 **SSL 設定檔**選擇為 `System-Standard`。

8 按**下一步**。

9 在**伺服器**索引標籤中，新增先前已建立之 Unified Access Gateway 伺服器的 IP 群組。

10 按**下一步**。

11 導覽至**進階 > 檢閱**。

12 按一下**儲存**。

後續步驟

安裝 VIP 所需的 SSL 憑證 (虛擬 IP)

安裝 VIP 所需的 SSL 憑證 (虛擬 IP)

SSL 連線會在 Avi 虛擬服務終止。因此，必須將 SSL 憑證指派給虛擬服務。若要使此指派發生，則必須在 Avi Vantage 安裝 SSL 憑證。

備註 建議安裝由有效憑證授權機構簽署的憑證，而非使用自我簽署的憑證。

如需有關安裝 SSL 憑證的詳細資訊，請參閱 Avi 說明文件。

後續步驟

建立虛擬服務

建立虛擬服務

使用 Unified Access Gateway 伺服器的 VIP 建立虛擬服務。這是用戶端裝置連線的 VIP。

程序

1 從 Avi Vantage UI 導覽至**應用程式 > 虛擬服務**。

2 按一下**建立虛擬服務 > 進階設定**。

3 在**選取雲端**視窗中，選取屬於 VMware vCenter/vSphere ESX 雲端基礎結構類型的雲端。

雲端基礎結構類型已設定為 Avi 控制器部署的一部分。

4 在**新增虛擬服務**視窗中，設定虛擬服務。

a 輸入虛擬服務名稱。

b 輸入 VIP 位址。

c 在**服務**中，將連接埠號碼輸入為 `443`。

d 針對連接埠號碼 `443`，選取 **SSL** 核取方塊。

連接埠 `443` 已啟用 SSL。

e 將**應用程式設定檔**選取為 `System-Secure-HTTP`。

f 選取先前針對 Unified Access Gateway 所建立的**集區**。

g 將 **SSL 設定檔**選取為 `System-Standard`。

h 選取先前已安裝的 SSL 憑證。

5 按**下一步**。

6 導覽至**進階**索引標籤。

7 按一下**儲存**。

後續步驟

使用 VIP 存取 Web 反向 Proxy。

Unified Access Gateway 高可用性

用於使用者運算產品和服務的 Unified Access Gateway 需要 Workspace ONE 和 VMware Horizon 內部部署的高可用性。不過，使用第三方負載平衡器會增加部署和疑難排解程序的複雜性。此解決方案可減少在 DMZ 前端 Unified Access Gateway 中使用第三方負載平衡器的需求。

備註 此解決方案不是一般用途負載平衡器。

對於偏好此模式部署的使用者，Unified Access Gateway 將繼續在前端支援第三方負載平衡器。如需更多資訊，請參閱 Unified Access Gateway 負載平衡拓撲。針對 Amazon AWS 和 Microsoft Azure 部署不支援 Unified Access Gateway 高可用性。

實作

Unified Access Gateway 需要管理員提供 IPv4 虛擬 IP 位址和群組 ID。Unified Access Gateway 只會將虛擬 IP 位址指派給叢集中已設定使用相同虛擬 IP 位址和群組 ID 的一個節點。如果擁有該虛擬 IP 位址的 Unified Access Gateway 失敗，則該虛擬 IP 位址會自動重新指派給叢集中的其中一個可用節點。在設定使用相同群組 ID 的叢集中的節點之間會發生 HA 和負載散佈。

源自於相同來源 IP 位址的多個連線會傳送到為 Horizon 和 Web 反向 Proxy 處理來自該用戶端的第一個連線相同的 Unified Access Gateway。此解決方案在叢集中支援 10,000 個並行連線。

備註 針對這些案例需要工作階段相似性。

針對 VMware Tunnel (個別應用程式 VPN)、Secure Email Gateway 和 Content Gateway 服務，HA 和負載散佈是使用最少連線演算法來完成。

備註 這些連線無狀態並且不需要工作階段相似性。

模式和相似性

不同 Unified Access Gateway 服務需要不同的演算法。

- 對於 VMware Horizon 及 Web 反向 Proxy - 來源 IP 相似性會用來搭配循環配置資源演算法進行散佈。
- 針對 VMware Tunnel (個別應用程式 VPN) 和 Content Gateway - 沒有任何工作階段相似性，且將最少連線演算法用於散佈。

用於散佈傳入流量的方法：

1 來源 IP 相似性：維護用戶端連線與 Unified Access Gateway 節點之間的相似性。具有相同來源 IP 位址的所有連線會傳送到相同的 Unified Access Gateway 節點。

2 具有高可用性的循環配置資源模式：傳入連線要求會依序在 Unified Access Gateway 節點的群組之間散佈。

3 最少連線模式搭配高可用性：新連線要求會傳送至具有的來自用戶端目前連線最少的 Unified Access Gateway 節點。

備註 來源 IP 相似性只有在傳入連線的 IP 對每個用戶端連線是唯一時才能運作。範例：如果在用戶端和 Unified Access Gateway 之間有網路元件 (例如 SNAT 閘道)，那麼來源 IP 相似性無法運作，因為從多個不同的用戶端到 Unified Access Gateway 的傳入流量具有相同的來源 IP 位址。

備註 虛擬 IP 位址必須屬於與 `eth0` 介面相同的子網路。

先決條件

- 用於 HA 的虛擬 IP 位址必須是唯一且可供使用。Unified Access Gateway 不會在組態期間驗證它是否是唯一的。IP 位址可能會顯示為已指派，但如果虛擬機器或實體機器已與該 IP 位址相關聯，則可能無法連線到該位址。
- 群組 ID 在指定的子網路中必須是唯一的。如果群組 ID 不是唯一的，可能會在群組中指派不一致的虛擬 IP 位址。例如，兩個或多個 Unified Access Gateway 節點可能最終會嘗試取得相同的虛擬 IP 位址。它可能會導致在多個 Unified Access Gateway 節點之間切換虛擬 IP 位址。
- 若要針對 Horizon 或 Web 反向 Proxy 設定 HA，請確保 Unified Access Gateway 的所有節點上的 TLS 伺服器憑證是相同的。

限制

- IPv4 支援使用浮動虛擬 IP 位址。IPv6 不支援。
- 僅支援 TCP 高可用性。
- 不支援 UDP 高可用性。
- 針對 VMware Horizon 使用案例，只有對 Horizon 連線伺服器的 XML API 流量會使用高可用性。高可用性不會用來散佈通訊協定 (顯示) 負載的流量，例如 Blast、PCoIP、RDP。因此，除了虛擬 IP 位址，Unified Access Gateway 節點的個別 IP 位址也必須可供 VMware Horizon 用戶端存取。

每個 Unified Access Gateway 上 HA 所需的組態

如需在 Unified Access Gateway 上設定 HA，請參閱設定高可用性設定。

設定高可用性設定

若要使用 Unified Access Gateway 高可用性，您可以在管理員使用者介面中啟用並設定**高可用性設定**。

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**高可用性設定**齒輪圖示。

3 在**高可用性設定**頁面中，將**已停用**變更為**已啟用**以啟用高可用性。

4 設定參數。

選項	說明
虛擬 IP 位址	HA 所使用的有效虛擬 IP 位址。 **備註** 用於 HA 的虛擬 IP 位址必須是唯一且可供使用。如果未設定唯一的位址，則 IP 位址可能會顯示為已指派，但如果虛擬機器或實體機器已與該 IP 位址相關聯，則可能無法連線到該位址。
群組 ID	HA 的群組 ID。輸入介於 1 到 255 之間的數值。 **備註** 群組 ID 在指定的子網路中必須是唯一的。如果未設定唯一的群組 ID，則影響可能會導致在群組中指派不一致的虛擬 IP 位址。例如，如果在 Unified Access Gateway 上有兩或多個閘道的 IP 位址，最終可能會嘗試取得同一個虛擬 IP 位址。

5 按一下**儲存**。

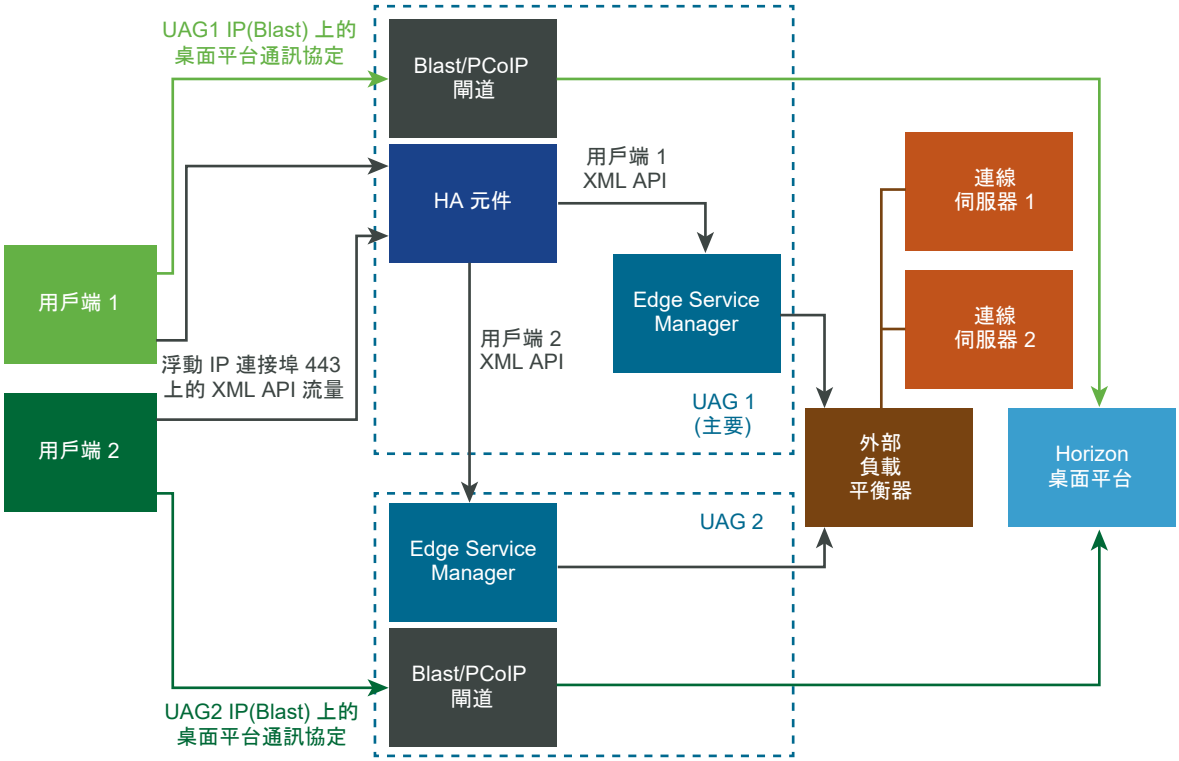
- **高可用性設定**的不同狀態指出下列：
- **未設定**：指出**高可用性設定**未設定。
- **處理中**：指出正在處理**高可用性設定**以便生效。
- **主要**：指出將節點選取為叢集中的主要節點且會散佈流量。
- **備份**：指出節點在叢集中處於備份狀態。
- **錯誤**：指出節點的 HA Proxy 組態可能有錯誤。

Unified Access Gateway 已設定使用 Horizon

多個 Unified Access Gateway 已設定使用相同的 Horizon 設定，並在每個 Unified Access Gateway 上啟用高可用性。

有一個用於 XML API 通訊協定的通用外部主機名稱。這個通用的外部主機名稱會與 Unified Access Gateway 節點上的 HA 設定中設定的浮動 IP 對應。桌面平台流量不會使用高可用性，並且不會散佈負載，因此，此解決方案需要 N + 1 個 VIP 用於 Horizon，其中的 N 是部署的 Unified Access Gateway 節點數。在每個 Unified Access Gateway 上，Blast、PCoIP 和通道外部 URL 必須是與對應的 Unified Access Gateway eth0 IP 位址相對應的外部 IP 位址或主機名稱。透過極差的網路連線並對 XML API 使用 UDP 連線的用戶端，會到達處理第一個 UDP XML API 連線的相同 Unified Access Gateway。

圖 1-2. 設定使用 Horizon 的 Unified Access Gateway



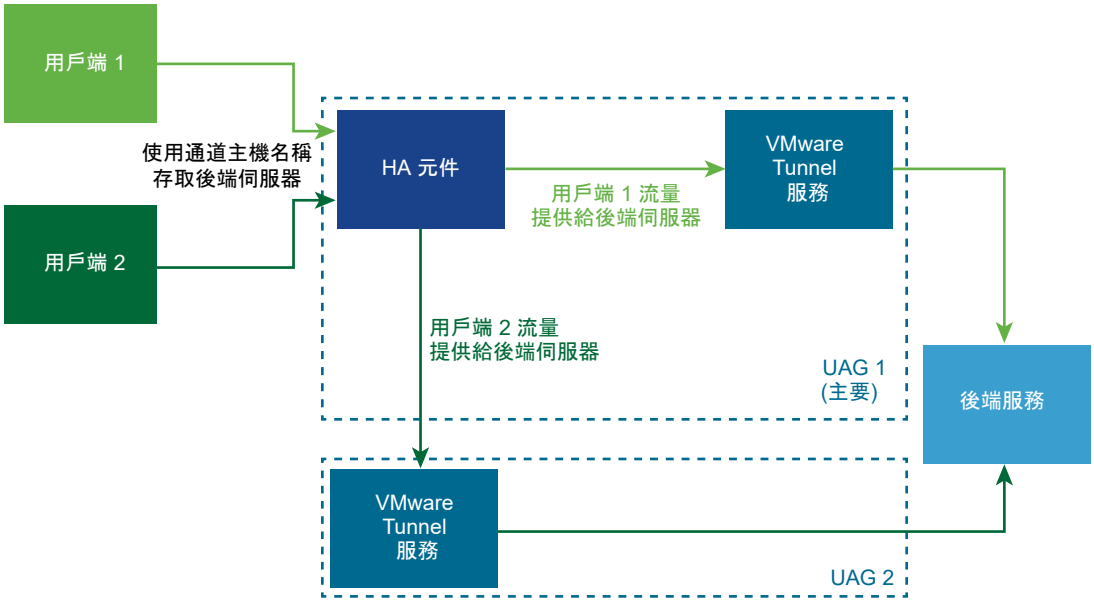
模式和相似性：相似性是基於來源 IP 位址。來自用戶端的第一個連線會使用循環配置資源機制散佈。然而來自相同用戶端的後續連線，則會傳送到處理第一個連線的相同 Unified Access Gateway。

具有基本組態的 VMware Tunnel (個別應用程式 VPN) 連線

VMware Tunnel (個別應用程式 VPN) 已在 Workspace ONE UEM 主控台中設定使用基本設定。

在 Workspace ONE UEM 主控台中針對 VMware Tunnel (個別應用程式 VPN) 設定所設定的通道伺服器主機名稱，會解析為 Unified Access Gateway 中針對 HA 設定的浮動 IP 位址。此浮動 IP 位址上的連線會在 Unified Access Gateway 上的已設定節點之間散佈。

圖 1-3. 具有基本組態的 VMware Tunnel (個別應用程式 VPN) 連線



模式和相似性：針對 HA 和負載的散佈使用最少連線演算法。新要求會傳送至具有的與用戶端目前連線最少的伺服器。不需要工作階段相似性，因為它們為無狀態的連線。

階層式模式的 VMware Tunnel (個別應用程式 VPN) 連線

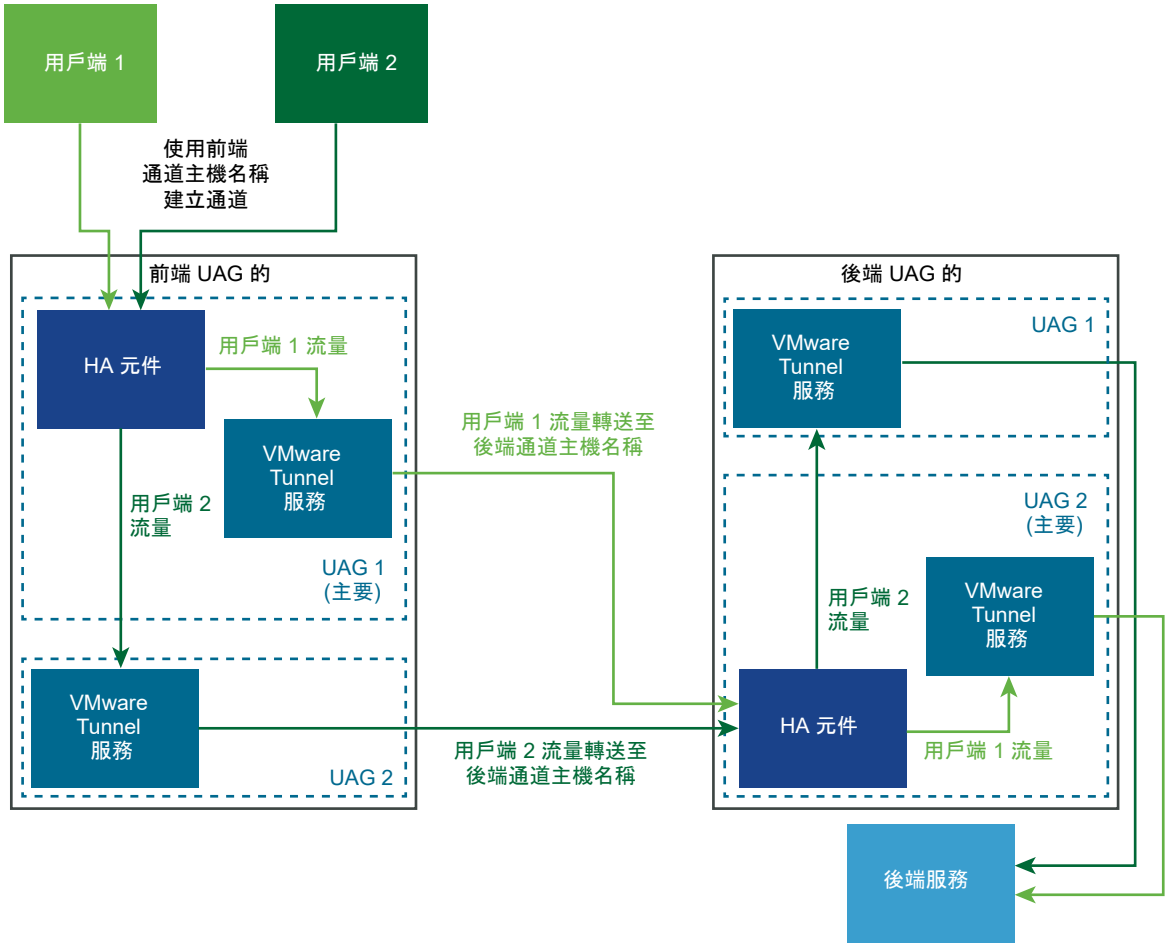
VMware Tunnel (個別應用程式 VPN) 已在 Workspace ONE UEM 主控台中設定使用階層式設定。

已在 Workspace ONE UEM 主控台中針對前端和後端設定兩個通道伺服器主機名稱。我們可以分別在前端和後端上部署兩組 Unified Access Gateway 節點。

Unified Access Gateway 上的前端節點已設定使用前端通道伺服器主機名稱。Unified Access Gateway 上前端節點的 HA 設定已設定使用外部浮動 IP 位址。前端通道伺服器主機名稱會解析為外部浮動 IP 位址。此外部浮動 IP 位址上的連線會在 Unified Access Gateway 上的前端節點之間散佈。

Unified Access Gateway 上的後端節點已設定使用後端通道伺服器主機名稱。Unified Access Gateway 上後端節點的 HA 設定已設定使用內部浮動 IP 位址。Unified Access Gateway 前端節點上的 VMware Tunnel (個別應用程式 VPN) 服務，會使用後端通道伺服器主機名稱將流量轉送至後端。後端通道伺服器主機名稱會解析為內部浮動 IP 位址。此內部浮動 IP 位址上的連線會在 Unified Access Gateway 上的後端節點之間散佈。

圖 1-4. 階層式模式的 VMware Tunnel (個別應用程式 VPN) 連線



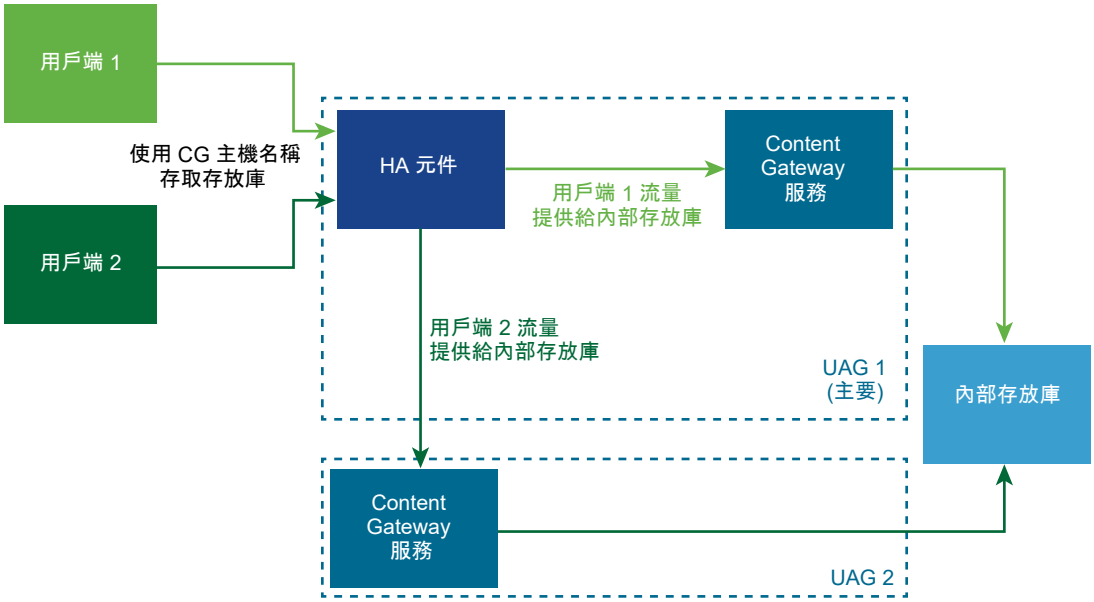
模式和相似性：針對 HA 和負載的散佈使用最少連線演算法。新要求會傳送至具有的與用戶端目前連線最少的伺服器。不需要工作階段相似性，因為它們為無狀態的連線。

Content Gateway 基本組態

Content Gateway 在 Workspace ONE UEM 主控台中設定為使用基本設定。

在 Workspace ONE UEM 主控台中針對 Content Gateway 設定所設定的 Content Gateway 伺服器主機名稱，會解析為 Unified Access Gateway 中針對 HA 設定的浮動 IP 位址。此浮動 IP 上的連線會在 Unified Access Gateway 上設定的節點之間進行負載平衡。

圖 1-5. Content Gateway 基本組態



模式和相似性：針對 HA 和負載的散佈使用最少連線演算法。新要求會傳送至具有的與用戶端目前連線最少的伺服器。不需要工作階段相似性，因為它們無狀態。

具有轉送和端點組態的 Content Gateway

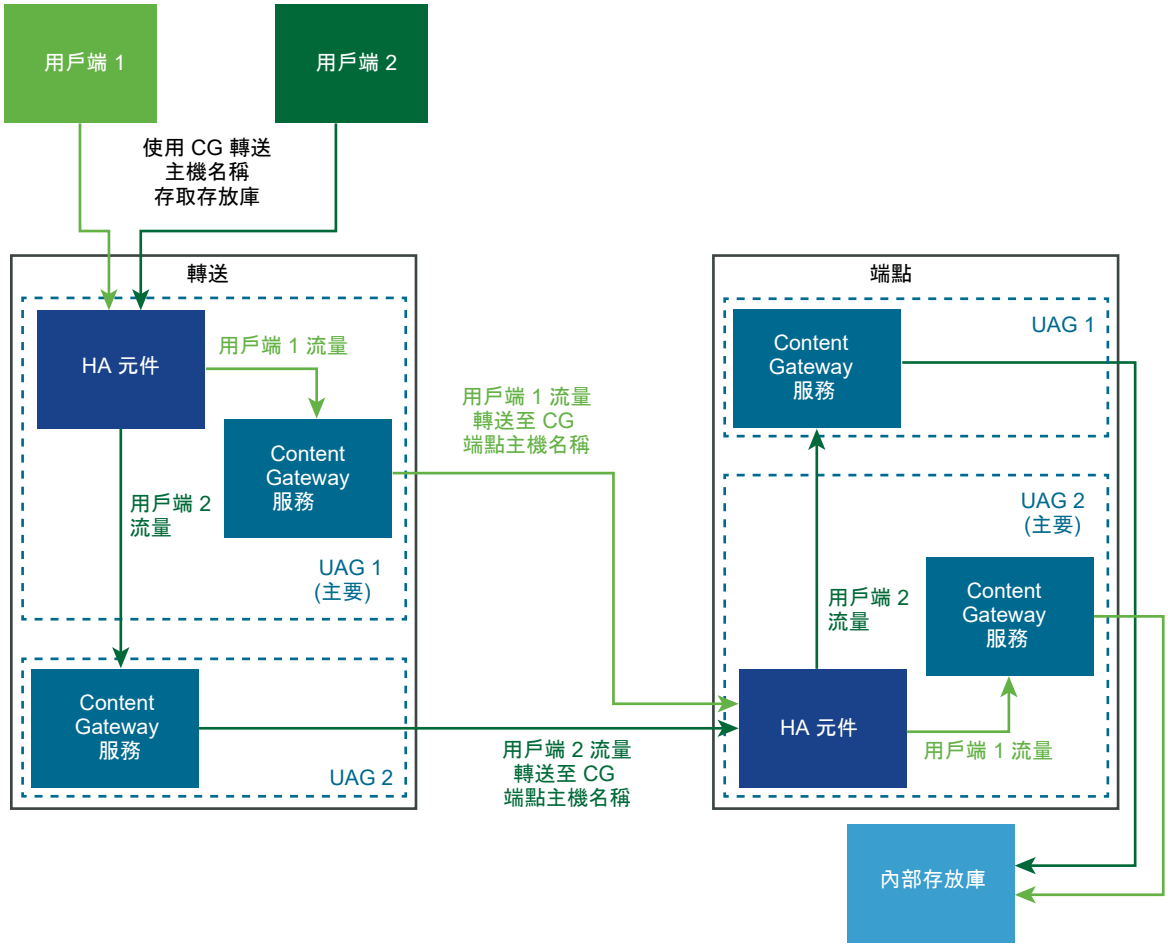
Content Gateway 在 Workspace ONE UEM 主控台中設定為使用轉送和端點組態。

在 Workspace ONE UEM 主控台中針對轉送和端點設定兩個 Content Gateway 伺服器主機名稱。Unified Access Gateway 上的兩組節點已針對轉送和端點部署。

Unified Access Gateway 上的轉送節點已設定使用轉送 Content Gateway 伺服器主機名稱。Unified Access Gateway 上轉送節點的 HA 設定已設定使用外部浮動 IP 位址。轉送 Content Gateway 伺服器主機名稱會解析為外部浮動 IP 位址。此外部浮動 IP 上的連線會在 Unified Access Gateway 上的轉送節點之間進行負載平衡。

Unified Access Gateway 上的端點節點設定為使用端點通道伺服器主機名稱。端點節點的 HA 設定在 Unified Access Gateway 上設定為使用內部浮動 IP 位址。前端 Unified Access Gateway 上的 Content Gateway 服務會將流量轉送至使用端點 Content Gateway 伺服器主機名稱的端點。端點 Content Gateway 伺服器主機名稱會解析為內部浮動 IP 位址。此內部浮動 IP 位址上的連線會在 Unified Access Gateway 上的端點節點之間進行負載平衡。

圖 1-6. 具有轉送和端點組態的 Content Gateway



模式和相似性：針對 HA 和負載的散佈使用最少連線演算法。新要求會傳送至具有的與用戶端目前連線最少的伺服器。不需要工作階段相似性，因為它們為無狀態的連線。

Unified Access Gateway 搭配多個網路介面卡的 DMZ 設計

Unified Access Gateway 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 Unified Access Gateway 時，您會為網路選取部署組態。

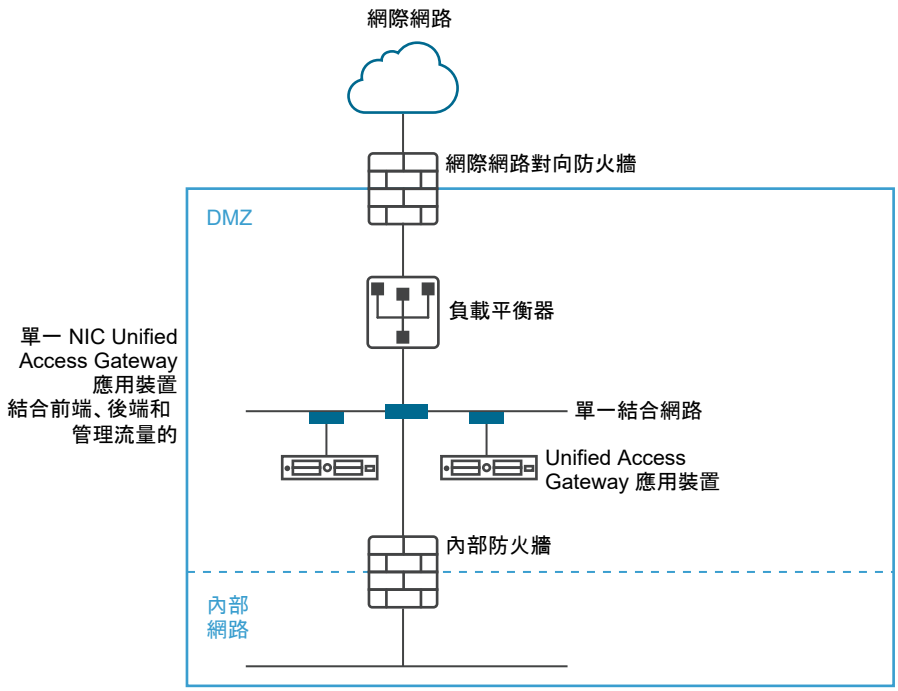
您可以指定一、二或三個 NIC 設定，其指定方式為 onenic、twonic 或 threenic。

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 Unified Access Gateway 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 Unified Access Gateway 應用裝置。然後 Unified Access Gateway 會經由內部防火牆將授權流量轉送至內部網路上的資源。Unified Access Gateway 會捨棄未經授權的流量。

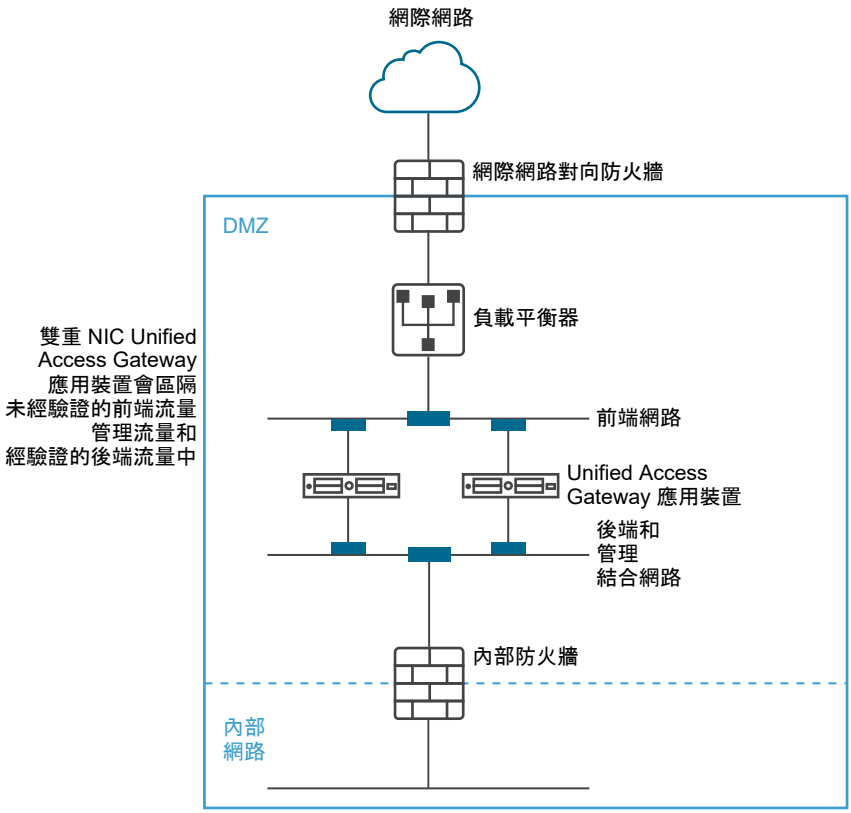
圖 1-7. Unified Access Gateway 單一 NIC 選項



從後端和管理流量區隔未經驗證的使用者流量

單一 NIC 部署的替代選項為指定兩個 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 1-8. Unified Access Gateway 兩個 NIC 選項



在兩個 NIC 部署中，Unified Access Gateway 必須授權流量透過內部防火牆進入內部網路。未經授權的流量不會在此後端網路上。管理流量 (例如 Unified Access Gateway 的 REST API) 只會在此第二個網路上

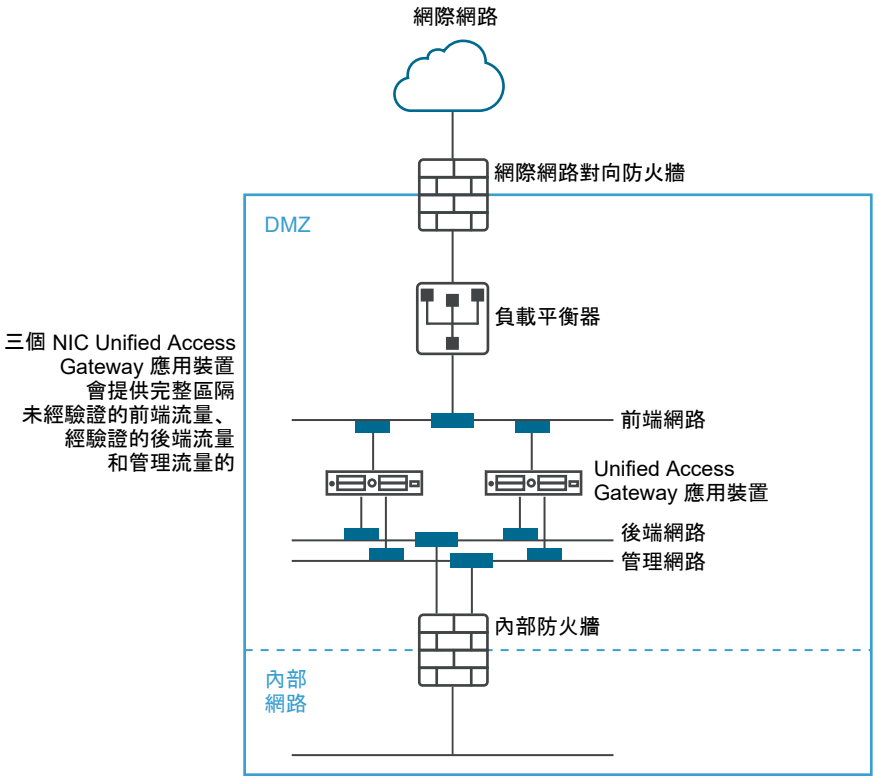
如果在未經驗證的前端網路上的裝置 (例如負載平衡器) 遭到破解，則在這兩個 NIC 部署中便無法重新設定裝置略過 Unified Access Gateway。它會結合第 4 層防火牆規則與第 7 層 Unified Access Gateway 安全性。相同地，如果網際網路對向防火牆設定錯誤而允許通過 TCP 連接埠 9443，則這仍不會將 Unified Access Gateway 管理 REST API 向網際網路使用者公開。深度防禦原則會使用多層級防護，例如知道單一組態錯誤或系統攻擊不一定會產生整體的弱點

在兩個 NIC 部署中，您可以在 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)，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 Unified Access Gateway 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。

Unified Access Gateway 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 1-9. Unified Access Gateway 三個 NIC 選項



不停機升級

不停機升級可讓您在使用者不停機的情況下升級 Unified Access Gateway。

如果**靜止模式**值設定為 [是]，當負載平衡器檢查應用裝置的健全狀況時，Unified Access Gateway 應用裝置會顯示為無法使用。進入負載平衡器的要求會傳送至負載平衡器後方的下一個 Unified Access Gateway 應用裝置。

必要條件

- 在負載平衡器後方設定兩個或多個 Unified Access Gateway 應用裝置。
- [健全狀況檢查 URL] 設定已設定了 URL，其負載平衡器會進行連線以便檢查 Unified Access Gateway 應用裝置的健全狀況。
- 在負載平衡器中檢查應用裝置的健全狀況。輸入 REST API 命令 `GET https://UAG-IP-Address:443/favicon.ico`。

如果 [靜止模式] 設定為 [否]，則回應為 `HTTP/1.1 200 OK`，如果 [靜止模式] 設定為 [是]，則為 `HTTP/1.1 503`。

備註

- 請勿使用 `GET https://UAG-IP-Address:443/favicon.ico` 以外的任何其他 URL。這樣會導致不正確的狀態回應與資源流失。
- 如果啟用了**高可用性**設定，則**靜止模式 (不停機)** 只會套用至 Web Reverse Proxy 和 Horizon。
- 在使用第三方負載平衡器時，如果平衡器設定為使用 `GET /favicon.ico` 執行健全狀況檢查，則適用**靜止模式 (不停機)**。

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 在**靜止模式**列中，啟用**是**以暫停 Unified Access Gateway 應用裝置。

當應用裝置停止時，在工作階段關閉之後，應用裝置維護的現有工作階段會持續 10 小時。

4 按一下**儲存**。

進入負載平衡器的新要求會傳送至下一個 Unified Access Gateway 應用裝置。

後續步驟

- 對於 vSphere 部署：
  a 透過匯出檔案來備份 JSON 檔案。
  b 刪除舊的 Unified Access Gateway 應用裝置。
  c 部署新版的 Unified Access Gateway 應用裝置。
  d 匯入您稍早匯出的 JSON 檔案。
- 對於 PowerShell 部署：
  a 刪除 Unified Access Gateway 應用裝置。
  b 使用第一次部署期間所使用的相同 INI 檔案重新部署 Unified Access Gateway。請參閱使用 PowerShell 來部署 Unified Access Gateway 應用裝置。

備註 如果您在重新啟用負載平衡器後看到通道伺服器憑證錯誤訊息，則套用先前在 Unified Access Gateway 應用裝置上使用的相同 SSL 伺服器憑證和私密金鑰 PEM 檔案。這是必要作業，因為私密金鑰基於安全因素無法匯出，因此 JSON 或 INI 檔案不可包含與 SSL 伺服器憑證相關聯的私密金鑰。使用 PowerShell 部署時會自動完成此作業，且您不需重新套用憑證。

在不含網路通訊協定設定檔 (NPP) 的情況下部署 Unified Access Gateway

Unified Access Gateway 的最新版本不接受來自網路通訊協定設定檔的網路遮罩或首碼和預設閘道設定。

部署您的 Unified Access Gateway 執行個體時，您必須提供此網路資訊。

如果是靜態部署，設定您的 Unified Access Gateway 執行個體時，請指定 IPv4 或 IPv6 位址、個別 NIC 的網路遮罩或首碼，以及 IPv4/IPv6 預設閘道。如果您未提供此資訊，則預設會對 IP 位址配置使用 DHCPV4+DHCPV6。

設定網路內容時，請注意下列事項：

- 如果您針對 NIC 的 `IPMode` 選取 STATICV4，則必須為該 NIC 指定 IPv4 位址和網路遮罩。
- 如果您為 NIC 的 `IPMode` 選取 STATICV6，則須為該 NIC 指定 IPv6 位址網路遮罩。
- 如果您針對 NIC 的 `IPMode` 同時選取 STATICV4 和 STATICV6，則必須為該 NIC 指定 IPv4 和 IPv6 位址和網路遮罩。
- 如果您未提供位址和網路遮罩資訊，則會由 DHCP 伺服器配置這些值。
- IPv4 和 IPv6 預設閘道內容為選用，但如果 Unified Access Gateway 需要與不在 Unified Access Gateway 中任何 NIC 之本機區段上的 IP 位址進行通訊，則必須進行指定。

如需關於設定網路內容的詳細資訊，請參閱使用 OVF 範本精靈來部署 Unified Access Gateway。

加入或退出客戶經驗改進計劃

VMware 客戶經驗改進計劃 (CEIP) 會提供資訊給 VMware，以便改善其產品和服務、修正問題，以及給予您如何部署和使用 VMware 產品的最佳建議。

本產品參與 VMware 的客戶經驗改進計劃 (「CEIP」)。關於透過 CEIP 所收集的資料以及 VMware 將其用於何種用途的詳細資料，請見 https://www.vmware.com/tw/solutions/trustvmware/ceip.html 上信任與保證中心的說明。

您可以隨時透過管理員 UI 加入或退出本產品的 CEIP。

程序

1 在**進階設定** > **系統組態**中，選取 [是] 或 [否]。

  如果您選取 [是]，則 [客戶經驗改進計劃] 對話方塊會顯示已勾選的核取方塊，表示您即將加入此計劃。

2 檢閱對話方塊上的資訊，然後按一下**關閉**。

3 在 [系統組態] 頁面上按一下**儲存**以儲存您的變更。

部署 Unified Access Gateway 應用裝置

2

Unified Access Gateway 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。

有兩個版本的 Unified Access Gateway OVA 可供使用：標準版本和 FIPS 版本。

OVA 的 FIPS 版本支援下列 Edge Service：

- Horizon (傳遞驗證、憑證驗證和 SAML 驗證)

  備註 憑證驗證包括智慧卡驗證和裝置憑證驗證。

- VMware 每一應用程式通道
- Secure Email Gateway

重要 FIPS 140-2 版本會使用 FIPS 認證的密碼集和雜湊執行，並啟用支援 FIPS 認證資料庫的限制服務。部署 Unified Access Gateway 後，就無法變更 FIPS 模式。

您可以使用兩種主要方法在 vSphere ESX 或 ESXi 主機上安裝 Unified Access Gateway 應用裝置。支援 Microsoft Server 2012 和 2016 Hyper-V 角色。

- vSphere Client 或 vSphere Web Client 可用來部署 Unified Access Gateway 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 Unified Access Gateway 管理員使用者介面以設定 Unified Access Gateway 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 Unified Access Gateway。
- PowerShell 指令碼可以用來部署 Unified Access Gateway 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 Unified Access Gateway。請參閱使用 PowerShell 來部署 Unified Access Gateway 應用裝置。

備註 針對每一應用程式通道和 Proxy 使用案例，您可以將 Unified Access Gateway 部署在 ESXi 或 Microsoft Hyper-V 環境中。

備註 在以上這兩個部署方法中，如果並未提供管理員 UI 密碼，則您稍後將無法新增管理員 UI 使用者來啟用對管理員 UI 或 API 的存取。如果您想要這麼做，則必須使用有效的密碼重新部署 Unified Access Gateway 執行個體。

本章節討論下列主題：

使用 OVF 範本精靈部署 Unified Access Gateway

若要部署 Unified Access Gateway，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 OVF 時，您會設定需要的網路介面 (NIC) 數量、IP 位址及設定管理員根密碼。

部署 Unified Access Gateway 之後，移至管理使用者介面 (UI) 以設定 Unified Access Gateway 環境。在管理員 UI 中，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。若要登入至管理員 UI 頁面，請移至 `https://<mycoUnifiedGatewayAppliance>.com:9443/admin/index.html`。

使用 OVF 範本精靈來部署 Unified Access Gateway

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

Unified Access Gateway 大小調整選項

若要簡化將 Unified Access Gateway 應用裝置部署為 Workspace ONE 安全閘道的程序，可以將大小調整選項新增至應用裝置中的部署組態。部署組態提供「標準」、「大型」和「超大型」虛擬機器的選擇。

- **標準：**如果 Horizon 部署支援最多 2000 個 Horizon 連線，則建議使用此組態，以配合連線伺服器容量。針對並行連線最多 10,000 個的 Workspace ONE UEM 部署 (行動使用案例)，也建議使用此組態。
- **大型：**針對 Unified Access Gateway 需要支援超過 50,000 個並行連線的 Workspace ONE UEM 部署，建議使用此組態。此大小可讓 Content Gateway、每一應用程式通道和 Proxy 以及反向 Proxy 使用相同的 Unified Access Gateway 應用裝置。
- **超大型**：針對 Workspace ONE UEM 部署，建議使用此組態。此大小可讓 Content Gateway、每一應用程式通道和 Proxy 以及反向 Proxy 使用相同的 Unified Access Gateway 應用裝置。
- **備註** 標準、大型和超大型部署的虛擬機器選項：
  - 標準 - 2 核心和 4 GB RAM
  - 大型 - 4 核心和 16 GB RAM
  - 超大型 - 8 核心和 32 GB RAM

  您可以使用 PowerShell 設定這些設定。如需 PowerShell 參數的相關資訊，請參閱使用 PowerShell 來部署 Unified Access Gateway 應用裝置。

  如需 Unified Access Gateway 大小調整建議的詳細資訊，您可以查看 VMware 組態上限。

必要條件

- 檢閱精靈中可用的部署選項。請參閱 Unified Access Gateway 系統和網路需求。

- 決定要為 Unified Access Gateway 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 Unified Access Gateway 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。
- 若有 Hyper-V 部署，且您要升級使用靜態 IP 的 Unified Access Gateway，請先刪除較舊的應用裝置，然後再部署較新的 Unified Access Gateway 執行個體。
- 若要在使用者不停機的情況下將較舊的應用裝置升級為 Unified Access Gateway 的新執行個體，請參閱不停機升級一節。

程序

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

針對 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 [選取來源] 頁面上，瀏覽至您下載的 `.ova` 檔案或輸入 URL，然後按**下一步**。

檢閱產品詳細資料、版本和大小需求。

4 按照提示進行，並參考下列準則以完成精靈。ESXi 和 Hyper-V 部署皆有兩個選項可指派 Unified Access Gateway 的 IP 指派。如果您打算升級，請先針對 Hyper-V 刪除具有相同 IP 位址的舊機器，然後再部署具有新位址的新機器。針對 ESXi，您可以關閉舊機器，並使用靜態指派以相同的 IP 位址部署新的機器。

選項	說明
名稱和位置	輸入 Unified Access Gateway 虛擬應用裝置的名稱。該名稱在詳細目錄資料夾內必須是唯一的。名稱區分大小寫。 選取虛擬應用裝置的位置。
部署組態	對於 IPv4 或 IPV6 網路，您可以使用一、二或三個網路介面 (NIC)。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 Unified Access Gateway 部署所在之 DMZ 的網路設計來對其設定。連同 NIC 數目，您也可以為 Unified Access Gateway 選擇**標準**或**大型**部署選項。 **備註** **標準**和**大型**部署的虛擬機器選項： ■ **標準** - 2 核心和 4 GB RAM ■ **大型** - 4 核心和 16 GB RAM
主機/叢集	選取要在其中執行虛擬應用裝置的主機或叢集。

選項	說明
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。
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。 將 OVF 範本中使用的網路對應到詳細目錄中的網路。 a 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。 b 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。 c 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。 **備註** 忽略 **IP 通訊協定**下拉式功能表 (如果有顯示)，且不要在此處進行任何選取。IP 通訊協定 (IPv4/IPv6/兩者) 的實際的選取取決於在自訂網路內容時，對 NIC 1 (eth0)、NIC 2 (eth1) 和 NIC 3 (eth2) 之 IPMode 所指定的 IP 模式。

選項	說明
自訂網路內容	在 [內容] 頁面上的文字方塊是 Unified Access Gateway 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。針對 STATICV4 的每個 NIC，您必須輸入 NIC 的 IPv4 位址。針對 STATICV6，您必須輸入 NIC 的 IPv6 位址。如果將文字方塊保留空白，則 IP 位址預設會配置為 DHCPV4+DHCPV6。 **重要** Unified Access Gateway 的最新版本不接受來自網路通訊協定設定檔 (NPP) 的網路遮罩或首碼值和預設閘道設定。若要使用靜態 IP 配置來設定 Unified Access Gateway，您必須在網路內容下設定網路遮罩/首碼。這些值無法從 NPP 填入。 **備註** ■ 這些值均區分大小寫。 ■ 在 vSphere 6.7 或更早版本中，使用 vSphere Client HTML5 部署 Unified Access Gateway 時，僅 NIC1 (eth0) 可用於組態。在 vSphere 7.0 中使用 vSphere Client HTML5 時，多個 NIC 可用於組態。 ■ **NIC1 的 IPMode (eth0)：STATICV4/STATICV6/DHCPV4/DHCPV6/AUTOV6/STATICV4+STATICV6/STATICV4+DHCPV6/STATICV4+AUTOV6/DHCPV4+AUTOV6/DHCPV4+STATICV6/DHCPV4+DHCPV6/DHCPV4+AUTOV6**。 ■ **NIC2 的 IPMode (eth1)：STATICV4/STATICV6/DHCPV4/DHCPV6/AUTOV6/STATICV4+STATICV6/STATICV4+DHCPV6/STATICV4+AUTOV6/DHCPV4+AUTOV6/DHCPV4+STATICV6/DHCPV4+DHCPV6/DHCPV4+AUTOV6**。 ■ **NIC3 的 IPMode (eth2)：STATICV4/STATICV6/DHCPV4/DHCPV6/AUTOV6/STATICV4+STATICV6/STATICV4+DHCPV6/STATICV4+AUTOV6/DHCPV4+AUTOV6/DHCPV4+STATICV6/DHCPV4+DHCPV6/DHCPV4+AUTOV6**。 ■ **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**。例如針對 IPv4 時為 `tcp/5262/10.110.92.129:9443, tcp/5263/10.20.30.50:7443`。 ■ **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**。例如，`20.2.0.0/16 10.2.0.1, 20.9.0.0/16 10.2.0.2, 10.2.0.1/32` 　　**備註** 如果未指定 **ipv4-gateway-address**，則新增的個別路由會具有閘道 0.0.0.0。 ■ **NIC 1 (eth0) IPv6 位址**。如果您已針對 NIC 模式輸入 STATICV6，請輸入 NIC 的 IPv6 位址。 ■ **NIC 1 (eth0) IPv4 網路遮罩**。輸入 NIC 的 IPv4 網路遮罩。 ■ **NIC 1 (eth0) IPv6 首碼**。輸入 NIC 的 IPv6 首碼。 ■ **NIC1 (eth0) 自訂組態**。以 `SectionName^Parameter=Value` 格式輸入 NIC 的自訂組態值。自訂組態項目的範例為 `DHCP^UseDNS=false`。此值在使用時，系統會停用 DHCP 伺服器所提供 DNS IP 位址的使用量。您可以使用相同的格式來新增多個此類 systemd.network 組態項目 (以分號分隔)。 ■ **DNS 伺服器位址**。針對 Unified Access Gateway 應用裝置的網域名稱伺服器輸入以空格分隔的 IPv4 或 IPv6 位址。IPv4 項目的範例為 `192.0.2.1 192.0.2.2`。IPv6 項目的範例為 `fc00:10:112:54::1`

選項	說明
	■ **IPv4 預設閘道**。如果 Unified Access Gateway 需要與不在 Unified Access Gateway 中任何 NIC 之本機區段上的 IP 位址進行通訊，請輸入 IPv4 預設閘道。 ■ **IPv6 預設閘道**。如果 Unified Access Gateway 需要與不在 Unified Access Gateway 中任何 NIC 之本機區段上的 IP 位址進行通訊，請輸入 IPv6 預設閘道。 ■ **NIC 2 (eth1) 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 2 (eth1) 的 IPv4 自訂路由逗號分隔清單**。例如，`20.2.0.0/16 10.2.0.1, 20.9.0.0/16 10.2.0.2, 10.2.0.1/32` **備註** 如果未指定 **ipv4-gateway-address**，所新增個別路由的閘道為 0.0.0.0 ■ **NIC 2 (eth1) IPv6 位址**。如果您已針對 NIC 模式輸入 STATICV6，請輸入 NIC 的 IPv6 位址。 ■ **NIC 2 (eth1) IPv4 網路遮罩**。輸入此 NIC 的 IPv4 網路遮罩。 ■ **NIC 2 (eth1) IPv6 首碼**。輸入此 NIC 的 IPv6 首碼。 ■ **NIC2 (eth1) 自訂組態**。使用與 NIC 1 相同的 `SectionName^Parameter=Value` 格式輸入 NIC 的自訂組態值。 ■ **NIC 3 (eth2) 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 3 (eth2) 的 IPv4 自訂路由逗號分隔清單**。例如，`20.2.0.0/16 10.2.0.1, 20.9.0.0/16 10.2.0.2, 10.2.0.1/32` **備註** 如果未指定 **ipv4-gateway-address**，所新增個別路由的閘道為 0.0.0.0 ■ **NIC 3 (eth2) IPv6 位址**。如果您已針對 NIC 模式輸入 STATICV6，請輸入 NIC 的 IPv6 位址。 ■ **NIC 3 (eth2) IPv4 網路遮罩**。輸入此 NIC 的 IPv4 網路遮罩。 ■ **NIC 3 (eth2) IPv6 首碼**。輸入此 NIC 的 IPv6 首碼。 ■ **NIC3 (eth2) 自訂組態**。使用與 NIC 1 相同的 `SectionName^Parameter=Value` 格式輸入 NIC 的自訂組態值。
虛擬機器根使用者密碼。	用於登入 Unified Access Gateway 虛擬機器的根使用者密碼。 若要建立根使用者密碼的密碼原則，您可以設定特定選項，例如密碼到期、最小長度、字元類型類別的最小數目、嘗試失敗次數上限，以及到達嘗試失敗次數上限後解除鎖定的時間。您也可以使用 PowerShell 並設定這些參數。 如需 PowerShell 參數的相關資訊，請參閱使用 PowerShell 來部署 Unified Access Gateway 應用裝置和#unique_36。
管理員 UI 密碼	管理員使用者用於登入 Unified Access Gateway 管理員 UI 的密碼。 若要為管理員使用者密碼建立密碼原則，您可以設定特定選項，例如最小長度、嘗試失敗次數上限、到達嘗試失敗次數上限後解除鎖定時間，以及管理員使用者已驗證工作階段的閒置逾時。
啟用 SSH	啟用 SSH 以存取 Unified Access Gateway 虛擬機器的選項。
允許使用密碼的 SSH 根使用者登入	使用 SSH 根使用者登入和密碼存取 Unified Access Gateway 虛擬機器的選項。 依預設，此選項的值為 `true`。

選項	說明
允許使用金鑰配對的 SSH 根使用者登入	使用 SSH 根使用者登入和公開-私密金鑰配對存取 Unified Access Gateway 虛擬機器的選項。 依預設，此值為 `false`。 Unified Access Gateway 管理員 UI 具有 **SSH 公開金鑰**欄位，管理員在使用金鑰-私密金鑰配對選項時，可透過此欄位上傳公開金鑰，以允許根使用者存取 Unified Access Gateway。若要讓此欄位成為管理員 UI 上的可用欄位，在部署時此選項和 **啟用 SSH** 的值必須是 `true`。若有任選項的值不是 `true`，管理員 UI 上的 **SSH 公開金鑰**欄位即無法使用。 **SSH 公開金鑰**欄位是管理員 UI 中的進階系統設定。請參閱設定 Unified Access Gateway 系統設定。
登入橫幅文字	用於自訂在使用 SSH 或 Unified Access Gateway Client 的 Web 主控台登入 vSphere 時顯示的橫幅文字的選項。 此選項只能在部署時進行設定。如果未設定此選項，則顯示的預設文字將為：VMware EUC Unified Access Gateway。 自訂文字中僅支援 ASCII 字元。對於多行橫幅文字，必須使用 `\n` 作為換行符號。 **備註** 使用 OVF 範本部署 Unified Access Gateway 並且設定了登入橫幅文字後，在第一次啟動 Unified Access Gateway 時，vSphere Client 的 Web 主控台將顯示預設橫幅文字，並忽略自訂橫幅文字。在後續啟動時，將會顯示自訂橫幅文字。
SecureRandom 來源	允許您設定 Java 程序用於加密函數的安全隨機位元產生器來源。 此選項只能在部署時進行設定。 支援的值包括：`/dev/random` 和 `/dev/urandom`。依預設，`/dev/random` 用於非 FIPS 模式下，`/dev/urandom` 用於 FIPS 模式下。
加入 CEIP	選取**加入 VMware 客戶經驗改進計劃**以加入 CEIP，或取消選取此選項以離開 CEIP。

重要 SSH 選項只能在部署期間進行設定。基於安全性相關原因，在部署後，無法透過 Unified Access Gateway 管理員 UI 或 API 來修改這些選項。

5 在**即將完成**頁面上，檢閱相關的資訊並按一下**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，檢視在系統啟動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 開啟虛擬機器電源。

7 開啟應用裝置電源後，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-UAG-appliance
```

在此 URL 中，*FQDN-of-UAG-appliance* 是 Unified Access Gateway 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 Unified Access Gateway 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。

結果

Unified Access Gateway 應用裝置會自動部署並啟動。

後續步驟

- 登入 Unified Access Gateway 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 Unified Access Gateway 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://<mycoUnified Access Gatewayappliance.com:9443/admin/index.html`。

  重要 您必須使用管理員 UI 來完成部署後 Unified Access Gateway 組態。如果並未提供管理員 UI 密碼，則您稍後將無法新增管理員 UI 使用者來啟用對管理員 UI 或 API 的存取。如果想要新增管理員 UI 使用者，則必須使用有效的管理員 UI 密碼來重新部署您的 Unified Access Gateway 執行個體。

  備註 如果您無法存取管理員 UI 登入畫面，請檢查以確認虛擬機器是否在 OVA 的安裝期間顯示 IP 位址。如果未設定 IP 位址，請使用 UI 中提及的 VAMI 命令來重新設定 NIC。以 "`cd /opt/vmware/share/vami`" 形式執行命令，然後執行命令 "`./vami_config_net`"。

從管理組態頁面設定 Unified Access Gateway

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

備註 當您第一次啟動 Unified Access Gateway 管理主控台時，系統會提示您變更在部署應用裝置時所設定的密碼。

[一般設定] 頁面和 [進階設定] 頁面包含下列項目。

- Unified Access Gateway 系統組態和 TLS 伺服器憑證
- Horizon、反向 Proxy、VMware Tunnel 及 Content Gateway (也稱為 CG) 的 Edge Service 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
- 網路設定
- 端點符合性檢查提供者設定
- 身分識別橋接設定組態
- 帳戶設定

下列選項可從 [支援設定] 頁面存取。

- 在 Unified Access Gateway 上監控每個 Edge 服務的工作階段。
- 下載 Unified Access Gateway 記錄檔。
- 匯出 Unified Access Gateway 設定以擷取組態設定。

- 設定記錄層級設定。

設定 Unified Access Gateway 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 Unified Access Gateway 應用裝置之間通訊的安全性通訊協定和密碼編譯演算法。

必要條件

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

    備註 最多可以指定兩個 DNS 伺服器 IP 位址。

    僅在未隨著組態設定或透過 DHCP 向 UAG 提供任何 DNS 伺服器位址時，Unified Access Gateway 才會使用平台預設後援公用 DNS 位址。
  - 管理主控台的密碼
  - Unified Access Gateway 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 Unified Access Gateway 應用裝置組態值。

選項	預設值和說明
UAG 名稱	唯一的 Unified Access Gateway 應用裝置名稱。 **備註** 應用裝置名稱可包含最多 24 個字元的文字字串，其中包括字母 (A-Z)、數字 (0-9)、減號 (-) 和句號 (.)。但是，應用裝置名稱不可包含空格。
地區設定	指定在產生錯誤訊息時使用的語言設定。 - **en_US** 表示美式英文。這是預設值。 - **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 - **es** 表示西班牙文 - **pt_BR** 表示葡萄牙文 (巴西) - **en_GB** 表示英式英文

選項	預設值和說明
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 Unified Access Gateway 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。
TLS 1.0 已啟用	預設為 NO。 選取**是**可啟用 TLS 1.0 安全性通訊協定。
TLS 1.1 已啟用	預設為 NO。 選取**是**可啟用 TLS 1.1 安全性通訊協定。
TLS 1.2 已啟用	預設為 YES。 TLS 1.2 安全性通訊協定已啟用。
TLS 1.3 已啟用	預設為 YES TLS 1.3 安全性通訊協定已啟用。
允許的主機標頭	輸入 IP 位址或主機名稱作為主機標頭值。此設定適用於具有 Horizon 和 Web 反向 Proxy 伺服器使用案例的 UAG 部署。 對於使用 Horizon 的 UAG 部署，您可能需要提供多個主機標頭。這取決於是否使用了 N+1 虛擬 IP (VIP)，以及是否啟用 Blast 安全閘道 (BSG) 和 VMware Tunnel，並將其設定為對外部使用連接埠 443。 Horizon 用戶端會在主機標頭中傳送用於 Blast 連線要求的 IP 位址。如果將 BSG 設定為使用連接埠 443，則允許的主機標頭必須包含在特定 UAG 之 Blast 外部 URL 中所設定 BSG 主機名稱的外部 IP 位址。 如果未指定主機標頭值，則依預設會接受用戶端傳送的任何主機標頭值。
CA 憑證	新增了 Syslog 伺服器時，便會啟用此選項。請選取有效的 Syslog 憑證授權機構的憑證。
健全狀況檢查 URL	輸入負載平衡器連線到的 URL，並檢查 Unified Access Gateway 的健全狀況。
要快取的 Cookie	Unified Access Gateway 快取的 Cookie 集。預設值為 [無]。
工作階段逾時	預設值為 **36000000** 毫秒。
靜止模式	啟用**是**可暫停 Unified Access Gateway 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**。
密碼使用期限	目前管理員密碼的有效天數。預設值為 90 天。若要密碼永不到期，請指定為零 (0)。
要求逾時	指出 Unified Access Gateway 等候要接收要求的時間上限。 預設值為 3000。 必須以毫秒為單位指定此逾時。
本文接收逾時	指出 Unified Access Gateway 等候要接收要求本文的時間上限。 預設值為 5000。 必須以毫秒為單位指定此逾時。
每個工作階段的連線數目上限	每個 TLS 工作階段允許的 TCP 連線數目上限。 預設值為 16。 若要讓允許的 TCP 連線數目沒有限制，請將此欄位的值設為 0。 **備註** 8 或更低的欄位值會導致 Horizon Client 中發生錯誤。

選項	預設值和說明
用戶端連線閒置逾時	指定關閉連線之前，用戶端連線可以維持閒置的時間 (以秒為單位)。預設值為 360 秒 (6 分鐘)。零值表示無閒置逾時。
驗證逾時	等待時間上限 (以毫秒為單位)，在此之前必須進行驗證。預設值為 300000。如果指定 0，則表示驗證沒有時間限制。
時鐘誤差容錯	輸入 Unified Access Gateway 時鐘與相同網路上其他時鐘之間允許的時間差異 (以秒為單位)。預設為 600 秒。
允許的系統 CPU 上限	指出一分鐘內允許的平均系統 CPU 使用率上限。 超過設定的 CPU 限制時，將不允許新的工作階段，且用戶端會收到 HTTP 503 錯誤，以指出 Unified Access Gateway 應用裝置暫時超載。此外，超出限制還會允許負載平衡器將 Unified Access Gateway 應用裝置標記為關閉，使得系統可將新要求導向至其他 Unified Access Gateway 應用裝置。 值以百分比表示。 預設值為 `100%`。
加入 CEIP	啟用時，會將客戶經驗改進計劃 (「CEIP」) 資訊傳送給 VMware。如需詳細資料，請參閱加入或退出客戶經驗改進計劃。
啟用 SNMP	切換為**是**可啟用 SNMP 服務。簡易網路管理通訊協定會透過 Unified Access Gateway 收集系統統計資料、記憶體和通道 Edge 服務 MIB 資訊。可用的管理資訊庫 (MIB) 清單如下： ■ UCD-SNMP-MIB::systemStats ■ UCD-SNMP-MIB::memory ■ VMWARE-TUNNEL-SERVER-MIB::vmwTunnelServerMIB
SNMP 版本	選取所需的 SNMP 版本。 **備註** 如果您已透過 PowerShell 部署 Unified Access Gateway，已啟用 SNMP 但未透過 PowerShell 或 Unified Access Gateway 管理員 UI 設定 SNMPv3 設定，則依預設會使用 SNMPv1 和 SNMPV2c 版本。 若要在管理員 UI 中設定 SNMPv3 設定，請參閱使用 Unified Access Gateway 管理員 UI 設定 SNMPv3。 若要透過 PowerShell 部署設定 SNMPv3 設定，則必須將特定的 SNMPv3 設定新增至 `INI` 檔案。請參閱使用 PowerShell 來部署 Unified Access Gateway 應用裝置。
管理員免責聲明文字	根據貴組織的使用者合約原則輸入免責聲明文字。 若要讓管理員成功登入 Unified Access Gateway 管理員 UI，管理員必須接受合約原則。 您可以透過 PowerShell 部署或使用 Unified Access Gateway 管理員 UI 來設定免責聲明文字。如需有關 `INI` 檔案中 PowerShell 設定的詳細資訊，請參閱使用 PowerShell 來部署 Unified Access Gateway 應用裝置。 使用 Unified Access Gateway 管理員 UI 來設定此文字方塊時，管理員必須先登入管理員 UI，然後再設定免責聲明文字。在後續的管理員登入時，系統會顯示該文字供管理員在存取登入頁面之前接受。
DNS	輸入新增至 `/run/systemd/resolve/resolv.conf` 組態檔的網域名稱系統位址。其中必須包含有效的 DNS 搜尋位址。按一下「+」可新增新的 DNS 位址。
DNS 搜尋	輸入新增至 `/etc/resolv.conf` 組態檔的網域名稱系統搜尋。其中必須包含有效的 DNS 搜尋位址。按一下「+」可新增新的 DNS 搜尋項目。

選項	預設值和說明
NTP 伺服器	網路時間通訊協定同步的 NTP 伺服器。您可以輸入有效的 IP 位址和主機名稱。任何從 `systemd-networkd.service` 組態或透過 DHCP 取得的每一介面 NTP 伺服器，其優先順序都會高於這些組態。按一下「+」可新增新的 NTP 伺服器。
後援 NTP 伺服器	用於網路時間通訊協定同步化的後援 NTP 伺服器。如果找不到 NTP 伺服器資訊，將會使用這些後援 NTP 伺服器的主機名稱或 IP 位址。按一下「+」可新增新的後援 NTP 伺服器。
SSH 公開金鑰	在使用公開-私密金鑰配對選項時，上傳公用金鑰以啟用對 Unified Access Gateway 的根使用者存取權。 管理員可將多個唯一的公用金鑰上傳至 Unified Access Gateway。 僅在部署期間將下列 SSH 選項設定為 `true` 時，此欄位才會在管理員 UI 中顯示：**啟用 SSH** 和**允許使用金鑰配對的 SSH 根使用者登入**。如需這些選項的相關資訊，請參閱使用 OVF 範本精靈來部署 Unified Access Gateway。

4 按一下**儲存**。

後續步驟

針對 Unified Access Gateway 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。

使用 Unified Access Gateway 管理員 UI 設定 SNMPv3

您可以在 Unified Access Gateway 管理員 UI 中設定 SNMPv3。SNMPv3 具有增強的安全性功能 (例如，驗證和隱私權)。Unified Access Gateway 持續支援預設版本的 SNMPv1 和 SNMPv2c。您也可以透過在 `INI` 檔案中新增特定的 SNMPv3 相關設定，來透過 PowerShell 部署設定 SNMPv3。

如果您已透過 PowerShell 部署 Unified Access Gateway，已啟用 SNMP 但未設定 SNMPv3 設定，則依預設會使用 SNMPv1 和 SNMPV2c 版本。

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 若要啟用 SNMP 服務，請將按鈕切換為 `Yes`。

備註 您必須先啟用 SNMP，才能設定 Tunnel。如果您在設定 Tunnel 之後才啟用 SNMP，則必須重新儲存 Tunnel 設定，SNMP 設定才能生效。

4 針對 **SNMP 版本**選取 `SNMPv3`。

5 輸入 **SNMPv3 USM 使用者**名稱。

6 選取 **SNMPv3 安全性層級**。

7 根據在上一個步驟中選取的安全性層級，執行下列動作：

安全性層級	動作
No Auth, No Priv **(無驗證、無隱私權)**	按一下**儲存**。 無需執行進一步動作。
Auth, No Priv **(驗證、無隱私權)**	a 選取 **SNMPv3 驗證演算法**。 b 輸入 **SNMPv3 驗證密碼**。 密碼的長度至少必須有 8 個字元。 c 確認在上一個步驟中輸入的**驗證密碼**。 d 按一下**儲存**。
Auth, Priv **(驗證、隱私權)**	a 選取 **SNMPv3 驗證演算法**。 b 輸入 **SNMPv3 驗證密碼**。 密碼的長度至少必須有 8 個字元。 c 確認在上一個步驟中輸入的**驗證密碼**。 d 選取 **SNMPv3 隱私權演算法**。 e 選取 **SNMPv3 隱私權密碼**。 密碼的長度至少必須有 8 個字元。 f 確認在上一個步驟中輸入的**隱私權密碼**。 g 按一下**儲存**。

設定 Syslog 伺服器設定

Syslog 伺服器會記錄 Unified Access Gateway (UAG) 應用裝置上發生的事件。

提供例如 Syslog 伺服器 URL、Syslog 類型、Syslog 用戶端憑證等詳細資料，以設定 Syslog 伺服器設定。您可以使用不同的通訊協定來設定多個 Syslog 伺服器。

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**下，按一下 **Syslog 伺服器設定**旁邊的齒輪圖示。

3 在 Syslog 伺服器設定視窗中，輸入下列詳細資料。

選項	說明
Syslog 類型	從下拉式功能表選取 Syslog 類型。 選項包括： ■ 注意：這是預設值。 ■ UDP：會透過 UDP 與網路以純文字傳送 Syslog 訊息。這是預設的選項。 ■ TLS：會在兩個 Syslog 伺服器之間新增 TLS 加密，以讓訊息保持安全。 ■ TCP：Syslog 訊息會透過 TCP 進行串流。 **備註** 此設定適用於 Unified Access Gateway 3.7 及更新版本。TCP 選項適用於 Unified Access Gateway 2009 及更新版本。
Syslog URL	當 Syslog 類型設定為 UDP 或 TCP 時，必須新增 Syslog URL。如果 Syslog 類型設定為 TLS，則必須新增 Syslog 伺服器主機名稱。 輸入用來記錄 Unified Access Gateway 事件的 Syslog 伺服器 URL。這個值可以是 URL、主機名稱或 IP 位址。 依預設，會記錄 Content Gateway 和 Secure Email Gateway Edge 服務事件。若要針對 Unified Access Gateway 上所設定的通道閘道 Edge 服務在 Syslog 伺服器上記錄事件，管理員必須使用資訊在 Workspaceone UEM Console 上設定 Syslog。`Syslog Hostname=localhost and Port=514` **備註** 這適用於 Unified Access Gateway 3.7 及更新版本。 按一下**新增**以新增伺服器詳細資料。新增的詳細資料會顯示在 Syslog 伺服器設定視窗的表格中，但在您按一下**儲存**之前不會儲存到後端。
Syslog 稽核 URL	輸入用來記錄 Unified Access Gateway 稽核事件的 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，則不會記錄任何稽核事件。 最多可提供兩個 URL。以逗號分隔的 URL。範例：`syslog://server1.example.com:514, syslog://server2.example.com:514`
Syslog 用戶端憑證	選取採用 PEM 格式的有效 Syslog 用戶端憑證。 **備註** 用戶端憑證和金鑰設定後會套用至以 TLS 模式設定的所有伺服器。
Syslog 用戶端憑證金鑰	選取採用 PEM 格式的有效 Syslog 用戶端憑證金鑰。 **備註** 使用 PowerShell 部署 Unified Access Gateway 時，如果提供了無效或到期的憑證或金鑰，就無法使用管理員 UI 執行個體。
Syslog 包括系統訊息	切換**是**，以啟用系統服務 (例如 haproxy、cron、ssh、核心、系統)，以將系統訊息傳送至 Syslog 伺服器。 依預設，此切換會設定為**否**。 或者，也可以透過 PowerShell 部署來設定此功能。如需有關 `INI` 檔案中設定的詳細資訊，請參閱使用 PowerShell 來部署 Unified Access Gateway 應用裝置。

4 按一下**儲存**。

如果您想要變更新增的 Sylsog 伺服器設定，按一下對應於表格中所列出伺服器的齒輪圖示。具有伺服器詳細資料的視窗隨即顯示。進行變更之後，按一下**確定**以更新詳細資料，然後按一下**儲存**將詳細資料儲存至後端。

變更網路設定

您可以從管理員 UI 為已設定的網路修改網路設定，例如 IP 位址、子網路遮罩、預設閘道和 IP 配置模式。

修改網路設定時，請留意下列限制：

- IPv4 是唯一受支援的 IP 模式，IPv6 不受支援。
- 當管理網路 IP 的 IP 位址動態變更時，對新的 IP 位址將不支援瀏覽器重新導向。
- 變更網際網路對向網路介面的 IP 位址、子網路遮罩或預設閘道時，所有目前的工作階段皆會遺失。

必要條件

- 確定您是以具有 ROLE_ADMIN 角色的管理員身分來登入。
- 如果您要將 IP 變更為靜態 IP 位址、子網路遮罩或預設閘道，則必須事先得知位址、子網路遮罩和預設閘道。

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**下，按一下**網路設定**旁邊的齒輪圖示。

此時會顯示已設定的網路及其設定的清單。

3 在 [網路設定] 視窗中，按一下要變更設定之網路旁邊的齒輪圖示，然後輸入下列資訊：

IPv4 組態

標籤	說明
IPv4 配置模式	選取要以靜態還是動態方式配置 IP。您必須為靜態 IP 配置指定此參數。
IPv4 位址	網路的 IP 位址。如果您選取 [動態 IP] 配置，則不需要指定 IP 位址。您必須為靜態 IP 配置指定此參數。
IPv4 網路遮罩	網路的 IPv4 網路遮罩。如果您選取 [動態 IP] 配置，則不需要指定 IPv4 網路遮罩。
IPv4 預設閘道	Unified Access Gateway 的 IPv4 預設閘道位址。如果您選取 [動態 IP] 配置，則不需要指定預設閘道 IP 位址。
IPv4 靜態路由	網路的 IPv4 自訂路由。按一下「+」可新增新的靜態路由。 NIC 的 IPv4 自訂路由逗號分隔清單，採用 ipv4-network-address/bits ipv4-gateway-address 格式。例如 20.2.0.0/16 10.2.0.1,20.9.0.0/16 10.2.0.2,10.2.0.1/32。 **備註** 如果未指定 ipv4-gateway-address，所新增個別路由的閘道為 0.0.0.0

IPv6 組態無法修改。

標籤	說明
IPv6 配置模式	指定 IP 的配置方式為靜態、動態或自動。
IPv6 位址	網路的 IP 位址。
IPv6 首碼	網路的 IPv6 首碼。
IPv6 預設閘道	Unified Access Gateway 的 IPv6 預設閘道位址。

4 按一下**儲存**。

如果成功變更設定，將會顯示一則成功訊息。如果無法更新網路設定，則會顯示錯誤訊息。

設定使用者帳戶設定

作為擁有 Unified Access Gateway 系統完整存取權的超級使用者管理員，您可以從管理員組態頁面新增和刪除使用者、變更密碼，以及修改使用者的角色。

包括低權限管理員的詳細資料等帳戶設定無法從應用裝置設定加以匯出或匯入。若要在 Unified Access Gateway 的新執行個體上設定新的低權限帳戶，請透過管理員 UI 來手動設定。

密碼到期

超級使用者和低權限管理員可檢視距離密碼到期所剩餘的時間。在**帳戶設定**頁面上，**密碼到期時間 (天)** 欄位會提供倒數天數，直到密碼到期的那一天。此欄位可協助使用者留意密碼到期日，並採取適當動作 (例如重設密碼)。

備註 密碼到期期間會往下四捨五入到下一個整數。

例如，如果密碼到期的剩餘天數為 1 天 23 小時，則該值會顯示為 1 天。

新增低權限管理員

您現在可以設定和新增可執行數目有限的工作 (例如唯讀作業、系統監控、下載記錄以及匯出組態) 的低權限管理員。

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] 下，選取 [帳戶設定] 齒輪圖示。

3 在 [帳戶設定] 視窗中，按一下**新增**。

角色會自動設定為 ROLE_MONITORING。

4 在 [帳戶設定] 視窗中，輸入下列資訊：

a 使用者的唯一使用者名稱。

b (選擇性) 新增使用者後，如果您想要立即啟用使用者，請選取**已啟用**方塊。

c 輸入使用者的密碼。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 ! @ # $ % * ( )。

d 確認密碼。

5 按一下**儲存**。

結果

您新增的管理員會在帳戶設定下列出。

後續步驟

低權限管理員可登入系統以變更密碼或執行監控工作。

修改使用者帳戶設定

作為超級使用者管理員，您可以變更使用者的密碼，以及啟用或停用使用者。

您也可以變更自己的密碼，但無法停用自己的帳戶。

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 [帳戶設定]。

使用者清單隨即顯示。

3 按一下您想要修改其帳戶之使用者旁的齒輪圖示。

4 編輯下列值。

a 根據您想要啟用或停用使用者來選取或取消選取**啟用**方塊。

b 若要重設使用者密碼，請輸入新密碼並確認密碼。如果您以管理員身分登入，則也必須輸入舊密碼。

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 ! @ # $ % * ( )。

5 按一下**儲存**。

使用 Unified Access Gateway 主控台重設管理員密碼

如果忘記管理員使用者的密碼，使用者可以使用根使用者認證登入 Unified Access Gateway 主控台，並重設管理員 UI 密碼。

必要條件

您必須擁有以根使用者或具有根權限之使用者身分登入虛擬機器的密碼。使用者必須是根群組的一部分。

如需根密碼的詳細資訊，請參閱疑難排解根使用者登入問題。

程序

1 以根使用者身分登入 Unified Access Gateway 主控台的作業系統。

2 輸入下列命令以重設管理員的密碼。

```
adminpwd

New password for user "admin": ********

Retype new password: ********
```

在此範例中，密碼的長度至少為 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 ! @ # $ % * ( )。

此時將顯示下列訊息。

```
adminpwd: password for "admin" updated successfully
```

3 輸入下列命令，以重設具有較低權限之管理員的密碼。

```
adminpwd [-u <username>]
```

```
New password for user "jdoe": ********
```

```
Retype new password: ********
```

管理員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 !@ # $ % * ( )。

此時將顯示下列訊息。

```
adminpwd: password for "jdoe" updated successfully
```

結果

已成功重設管理員使用者密碼。

後續步驟

使用者現在可以使用剛才設定的管理員密碼登入 Unified Access Gateway 介面。使用 `adminpwd` CLI 命令重設密碼後首次登入時，系統會要求使用者變更密碼。

備註 變更密碼後，使用者必須在第一次嘗試時登入。

刪除使用者

身為超級使用者管理員，您可以刪除非根使用者。

您無法刪除根管理員。

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] 下，選取 [帳戶設定] 齒輪圖示。

使用者清單隨即顯示。

3 按一下要刪除之使用者旁邊的「x」按鈕。

注意 會立即刪除使用者。此動作無法復原。

結果

系統會刪除使用者帳戶，並顯示一則訊息。

設定 JSON Web 權杖設定

Unified Access Gateway 支援 JSON Web 權杖 (JWT) 驗證。您可以設定 JSON Web 權杖設定，以在單一登入 Horizon 期間驗證 Workspace ONE Access 所發出的 SAML 構件，以及在 Unified Access Gateway 與 Horizon 通用代理搭配使用時支援 Horizon 通訊協定重新導向功能。

當 Workspace ONE Access Horizon 組態中啟用了**在 JWT 中包裝構件**核取方塊時，Workspace ONE Access 會發出 JWT 包裝的 Horizon SAML 構件。這可讓 Unified Access Gateway 應用裝置封鎖驗證嘗試，除非 SAML 構件驗證嘗試提供了受信任的 JWT。

在這兩個使用案例中，您都必須指定 JWT 設定，以允許 Unified Access Gateway 信任所收到 JWT 權杖的簽發者。

請對 JWT 設定使用動態公開金鑰 URL，以便讓 Unified Access Gateway 自動保有此信任的最新公開金鑰。如果 Unified Access Gateway 無法存取動態公開金鑰 URL，則您只能使用靜態公開金鑰。

下列程序會說明 JSON Web 權杖設定的組態：

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] 下，選取 [JWT 設定] 齒輪圖示。

3 在 [JWT 設定] 視窗中，按一下**新增**。

4 在 [帳戶設定] 視窗中，輸入下列資訊：

選項	預設值和說明
名稱	用來識別此驗證設定的名稱。
簽發者	JWT 簽發者值，在要驗證的傳入權杖中的簽發者宣告中指定。 依預設，此欄位的值會設定為**名稱**欄位。 **備註** 只會針對通用代理通訊協定重新導向使用案例來設定**簽發者**。
動態公開金鑰 URL	輸入用來動態擷取公開金鑰的 URL。
公用金鑰 URL 指紋	輸入公開金鑰 URL 指紋的清單。如果未提供指紋的清單，請確保伺服器憑證是由信任的 CA 核發。輸入十六進位的指紋數字。例如，sha1= C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3。
受信任的憑證	■ 若要選取 PEM 格式的憑證並新增至信任存放區，請按一下 +。 ■ 若要從信任存放區移除憑證，請按一下 -。 ■ 若要提供不同名稱，請編輯別名文字方塊。 依預設，別名名稱是 PEM 憑證的檔案名稱。
公開金鑰重新整理間隔	定期從 URL 擷取公開金鑰的時間間隔 (以秒為單位)。
靜態公開金鑰	**備註** 如果動態公開金鑰 URL 無法使用，請設定靜態公開金鑰。 按一下 + 以選取並新增要用於 JWT 驗證的公開金鑰。 檔案必須採用 PEM 格式。

5 按一下**儲存**。

結果

參數的詳細資料列於 [JWT 設定] 下方。

設定輸出 Proxy 設定

若要讓輸出連線經由 Web Proxy 伺服器從 Unified Access Gateway 前往網際網路上所需的主機，您必須在 Unified Access Gateway 管理員 UI 中設定**輸出 Proxy 設定**。

Unified Access Gateway 不支援 Proxy 伺服器驗證。

在此版本的 Unified Access Gateway 中，**輸出 Proxy 設定**僅支援 OPSWAT 和檔案伺服器 (透過使用 **URL 參考**上傳類型將 on-demand agent 可執行檔上傳至 Unified Access Gateway 時所使用) 的輸出連線。當來自 Unified Access Gateway 的傳出流量用於 OPSWAT 主機時，此類連線必須先經由 Web Proxy 伺服器。

下列程序會說明**輸出 Proxy 設定**的組態：

程序

1 登入管理員 UI，然後在**手動設定**區段中按一下**選取**。

2 移至**進階設定 > 輸出 Proxy 設定**，然後按一下齒輪方塊圖示。

3 在**輸出 Proxy 設定**視窗中，按一下**新增**。

4 輸入下列資訊：

選項	預設值和說明
名稱	您可以在管理員 UI 中新增多個 Proxy 伺服器設定。此文字方塊可用作每個 Proxy 伺服器設定的唯一識別碼。 **備註** 此文字方塊為必填，且無法更新。
Proxy 伺服器 URL	來自 Unified Access Gateway 的輸出連線會經由 Proxy 伺服器 (在此文字方塊中提及)，然後前往網際網路上所需的主機。 此文字方塊的值必須是主機名稱或首碼為 HTTP 或 HTTPS 的 IP 位址。
包含 Proxy 的主機	在此文字方塊中所提及主機的輸出連線，必須經由 Proxy 伺服器從 Unified Access Gateway 前往網際網路上的主機。 此文字方塊的值必須是主機名稱或 IP 位址。 **備註** 如果 OPSWAT 或檔案伺服器為主機，則必須在此文字方塊中設定對應的主機名稱。
受信任的憑證	■ 若要選取 PEM 格式的憑證並新增至信任存放區，請按一下 +。 ■ 若要從信任存放區移除憑證，請按一下 -。 ■ 若要提供不同名稱，請編輯別名文字方塊。 依預設，別名名稱是 PEM 憑證的檔案名稱。

5 按一下**儲存**。

設定 Unified Access Gateway 以自動套用授權的作業系統更新

有時，VMware 可能會授權一或多個作業系統套件的更新，以修正影響特定 Unified Access Gateway 版本的嚴重弱點，以及用於無可行因應措施的情況。

您可以設定 Unified Access Gateway 以自動擷取並將任何可用的授權 Photon OS 套件套用至您環境中已部署的 Unified Access Gateway 版本。然後，這些更新會在應用裝置下次開機時自動擷取並套用。

在舊版中，此類重要更新會根據 VMware 全球支援服務所提供的準則，使用 `tdnf` 命令來手動執行。

在**應用裝置更新設定**區段中，您可以選取套用更新的頻率，例如在 Unified Access Gateway 應用裝置下一次重新開機時或每次重新開機時。

備註 在此頁面上設定所需的更新配置後，更新僅會在開機週期期間套用至 Unified Access Gateway 應用裝置。

程序

1 登入管理員 UI，然後在**手動設定**區段中按一下**選取**。

2 移至**進階設定 > 應用裝置更新設定**，然後按一下齒輪方塊圖示。

3 在**應用裝置更新設定**視窗中，輸入下列資訊：

組態設定	動作
套用更新配置	選取可擷取 Photon OS 和 Unified Access Gateway 更新並套用至 Unified Access Gateway 的頻率。 依預設，更新配置為 `Don't apply updates`。 **重要** 如果您選取 `Apply updates on next boot` 配置，則在 Unified Access Gateway 下一次重新開機立即套用更新後，配置會自動重設為預設值。
作業系統更新 URL	輸入要從中擷取 Photon OS 套件並將其套用至 Unified Access Gateway 應用裝置的存放庫位置。 依預設，此文字方塊的值為 `https://packages.vmware.com/photon`。您可以使用預設值，也可以透過鏡像預設的 VMware 存放庫來提供自訂存放庫的 URL。鏡像存放庫中的檔案不得變更。 此文字方塊的值必須是絕對 URL，可以是首碼為 `https` 的 IP 位址或主機名稱。 **備註** 如果您為作業系統更新提供自訂 URL，則這些設定會在最多一分鐘後套用。

組態設定	動作
應用裝置更新 URL	輸入要從中擷取 Unified Access Gateway 授權 OS 套件清單並將其套用至 Unified Access Gateway 應用裝置的存放庫位置。 依預設，此文字方塊的值為 `https://packages.vmware.com/uag`。您可以使用預設值，也可以透過鏡像預設的 VMware 存放庫來提供自訂存放庫的 URL。鏡像存放庫中的這些檔案不得變更。 此文字方塊的值必須是絕對 URL，可以是首碼為 `https` 的 IP 位址或主機名稱。 **備註** 如果您為應用裝置更新提供自訂 URL，則這些設定會在最多一分鐘後套用。
受信任的憑證	■ 若要選取 PEM 格式的憑證並新增至信任存放區，請按一下 +。 ■ 若要提供不同名稱，請編輯別名文字方塊。 依預設，別名名稱是 PEM 憑證的檔案名稱。 ■ 若要從信任存放區移除憑證，請按一下 -。

4 按一下**儲存**。

結果

套用更新後，Unified Access Gateway 應用裝置會重新開機，並產生 `package-updates.log` 檔案。此記錄檔可在 `UAG-log-archive.zip` 中取得。您可以將 `package-updates.log` 檔案用於檢查更新的狀態和疑難排解目的。

如需從管理員 UI 存取 `UAG-log-archive.zip` 的相關資訊，請參閱從 Unified Access Gateway 應用裝置收集記錄。

更新 SSL 伺服器簽署的憑證

您可以在簽署的憑證到期時加以取代，或將預設憑證替代為 CA 簽署的憑證。

依預設，Unified Access Gateway 會使用自我簽署的 TLS/SSL 伺服器憑證。對於生產環境，VMware 強烈建議您將預設的自我簽署憑證取代為適用於您環境的受信任 CA 簽署憑證。

在上傳憑證時，請留意下列考量事項：

- 您可以將管理員和使用者的預設憑證取代為 PEM 憑證。
- 當您使用管理員介面上傳 CA 簽署的憑證時，管理員介面上的 SSL 連接器會更新並重新啟動，以確保上傳的憑證能夠生效。如果連接器無法使用上傳的 CA 簽署憑證來重新啟動，則會產生自我簽署憑證並將其套用於管理員介面，並通知使用者先前嘗試上傳憑證並未成功。

備註 使用 PowerShell 來部署 Unified Access Gateway 時，可以指定 SSL 伺服器憑證。您不需要手動進行取代。

必要條件

- 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 Unified Access Gateway 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 **TLS 伺服器憑證設定**齒輪圖示。

3 選取**管理員介面**或**網際網路介面**，將憑證套用至其中一個介面。您也可以選取兩個介面，而同時對兩者套用憑證。

4 選取 PEM 或 PFX 的**憑證類型**。

5 如果憑證類型為 **PEM**：

   a 在 [私密金鑰] 列，按一下**選取**並瀏覽至私密金鑰檔案。

   b 按一下**開啟**以上傳檔案。

   c 在 [憑證鏈結] 列，按一下**選取**並瀏覽至憑證鏈結檔案。

   d 按一下**開啟**以上傳檔案。

6 如果憑證類型為 **PFX**：

   a 在 [上傳 PFX] 列，按一下**選取**並瀏覽至 pfx 檔案。

   b 按一下**開啟**以上傳檔案。

   c 輸入 PFX 憑證的密碼。

   d 輸入 PFX 憑證的別名。

   有多個憑證存在時，您可以使用別名加以區分。

7 按一下**儲存**。

結果

憑證更新成功時，會顯示確認訊息。

使用 PowerShell 部署 Unified Access Gateway

3

您可以使用 PowerShell 指令碼來部署 Unified Access Gateway。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 Unified Access Gateway，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 Unified Access Gateway 的系統需求
- 使用 PowerShell 來部署 Unified Access Gateway 應用裝置

使用 PowerShell 部署 Unified Access Gateway 的系統需求

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

- 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。
- 具有 vCenter Server 的 VMware vSphere ESXi 主機。
- 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。
- Microsoft Hyper-V

  備註 如需詳細資訊，請參閱 VMware Workspace ONE UEM 說明文件。
- Microsoft Azure

  備註 如需詳細資訊，請參閱使用 Powershell 將 Unified Access Gateway 部署到 Microsoft Azure。
- Amazon AWS EC2

  備註 如需詳細資訊，請參閱使用 Powershell 將 Unified Access Gateway 部署到 Amazon Web Services。

您必須選取要使用的 vSphere 資料存放區和網路。

使用 PowerShell 來部署 Unified Access Gateway 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 Unified Access Gateway 時，解決方案會在首次系統開機時做好生產準備。

重要 您可以利用 PowerShell 部署在 INI 檔案中提供所有設定，而 Unified Access Gateway 執行個體在開機後便會處於生產就緒狀態。如果您在部署後不想變更任何設定，則不需提供管理員 UI 密碼。

不過，如果並未在部署期間提供管理員 UI 密碼，則管理員 UI 和 API 皆無法使用。如果並未在部署時提供管理員 UI 密碼，則您稍後將無法新增使用者來啟用對管理員 UI 或 API 的存取。您必須重新部署您的 Unified Access Gateway

備註

- Unified Access Gateway 3.5 及更新版本包含選用的 `sshEnabled` INI 內容。在 PowerShell INI 檔案的 `[General]` 區段中設定 `sshEnabled=true`，會在已部署的應用裝置上自動啟用 `ssh` 存取。除非在某些特定且可限制存取的情況下，否則 VMware 通常不建議在 Unified Access Gateway 上啟用 `ssh`。此功能主要用於無法使用替代主控台存取的 Amazon AWS EC2 部署。如需 Amazon AWS EC2 的詳細資訊，請參閱使用 PowerShell 將 Unified Access Gateway 部署到 Amazon Web Services。

  如果 `sshEnabled=true` 未指定或設定為 `false`，則不會啟用 `ssh` 。

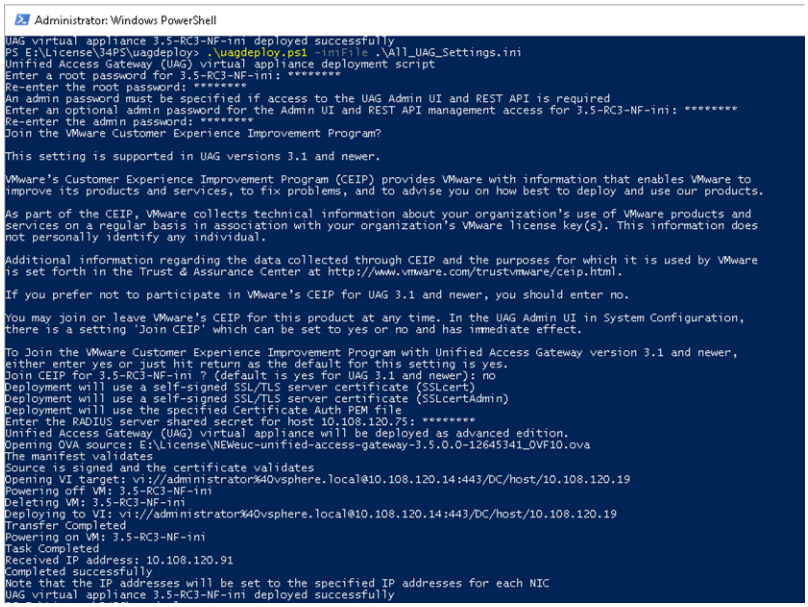
  針對 vSphere、Hyper-V 或 Microsoft Azure 部署通常不需要在 Unified Access Gateway 上啟用 `ssh` 存取，因為在這些平台上可以使用主控台存取。如果 Amazon AWS EC2 部署需要根主控台存取，請設定 `sshEnabled=true`。在啟用 `ssh` 的情況下，必須在防火牆或安全群組中將 TCP 連接埠 22 存取限定於個別管理員的來源 IP 位址。EC2 在與 Unified Access Gateway 網路介面相關聯的 EC2 安全群組中支援這項限制。
- Unified Access Gateway 2009 在 INI 檔案中包括用來啟用 Syslog 組態的 `sysLogType` 內容。
- 您可以使用 Unified Access Gateway 2009 在 INI 檔案中包含參數，以用於建立具有監控角色的低權限管理員使用者。不支援建立超級使用者管理員使用者。
- 您可以使用 Unified Access Gateway 2012 在 INI 檔案中提供下列內容：
  - rootPasswordExpirationDays - 此內容用於設定根使用者的密碼到期原則。預設的密碼到期時間為 365 天。到期時間可設定為 0，以防止密碼到期。
  - 自訂組態設定 - 必須新增至 systemd.network 檔案的自訂組態值可使用 `SectionName^Parameter=Value` 格式來提供。自訂組態項目的範例為 DHCP^UseDNS=false。此值在使用時，系統會停用 DHCP 伺服器所提供 DNS IP 位址的使用量。您可以使用相同的格式來新增多個此類 systemd.network 組態項目 (以分號分隔)。eth (0、1 和 2) 的自訂組態值範例包含在範例 INI 檔案的 `General` 區段中。

必要條件

- 若為 Hyper-V 部署，且如果您要升級使用靜態 IP 的 Unified Access Gateway，請先刪除較舊的應用裝置，然後再部署 Unified Access Gateway 的較新執行個體。
- 請確認系統需求適當且可供使用。

以下是在環境中部署 Unified Access Gateway 的範例指令碼。

圖 3-1. 範例 PowerShell 指令碼



程序

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

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

您可以從 Unified Access Gateway 的 VMware 下載頁面取得 `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 Unified Access Gateway 虛擬應用裝置建立 INI 組態檔案。

例如：部署新的 Unified Access Gateway 應用裝置 *UAG1*。組態檔案的名稱為 *uag1.ini*。該檔案含有 UAG1 的所有組態設定。您可以使用 uagdeploy.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 Unified Access Gateway 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。
- 若要將私密金鑰從 PKCS8 轉換為 PKCS1，也就是說，從 BEGIN PRIVATE KEY 格式到 BEGIN RSA PRIVATE KEY 格式，請執行下列 openssl 命令：

  ```
  openssl rsa -in key.pem -out keyrsa.pem
  ```

  若要轉換具有 .p12 或 .pfx 副檔名的 PKCS#12 格式檔案，以及確保該金鑰為 RSA 金鑰，請執行下列命令：

  ```
  openssl pkcs12 -in cert.pfx -nokeys -out cert.pem

  openssl pkcs12 -in cert.pfx -nodes -nocerts -out key.pem

  openssl rsa -in key.pem -check -out keyrsa.pem
  ```

要修改的 INI 檔案範例。

```
[General]
netManagementNetwork=
netInternet=
netBackendNetwork=
name=
dns = 192.0.2.1 192.0.2.2
dnsSearch = example1.com example2.com
ip0=10.108.120.119
diskMode=
source=
defaultGateway=10.108.120.125
target=
ds=
deploymentOption=threenic
eth0CustomConfig=DHCP^UseDNS=false
eth1CustomConfig=DHCP^UseDNS=false
eth2CustomConfig=DHCP^UseDNS=false
authenticationTimeout=300000
fipsEnabled=false
sysLogType=TCP
uagName=UAG1
locale=en_US
ipModeforNIC3=DHCPV4_DHCPV6
tls12Enabled=true
ipMode=DHCPV4_DHCPV6
requestTimeoutMsec=10000
ipModeforNIC2=DHCPV4_DHCPV6
```

```
tls11Enabled=false
clientConnectionIdleTimeout=180
tls10Enabled=false
adminCertRolledBack=false
cookiesToBeCached=none
healthCheckUrl=/favicon.ico
quiesceMode=false
syslogUrl=10.108.120.108:514
syslogSystemMessagesEnabled=false
isCiphersSetByUser=false
tlsPortSharingEnabled=true
ceipEnabled=true
bodyReceiveTimeoutMsec=15000
monitorInterval=60
cipherSuites=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TL
S_ECDHE_RSA_WITH_AES_128_CBC_SHA256
, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
adminPasswordExpirationDays=90
rootPasswordExpirationDays=365
passwordPolicyMinLen=6
passwordPolicyMinClass=4
passwordPolicyUnlockTime=900
passwordPolicyFailedLockout=3
httpConnectionTimeout=120
isTLS11SetByUser=false
sessionTimeout=36000000
ssl30Enabled=false
snmpEnabled= TRUE | FALSE
ntpServers=ipOrHostname1 ipOrHostname2
fallBackNtpServers=ipOrHostname1 ipOrHostname2
sshEnabled=
sshPasswordAccessEnabled=
sshKeyAccessEnabled=
sshPublicKey1=
adminDisclaimerText=

[SnmpSettings]
version=
usmUser=
securityLevel=
authAlgorithm=
authPassword=
privacyAlgorithm=
privacyPassword=

[WebReverseProxy1]
proxyDestinationUrl=https://10.108.120.21
trustedCert1=
instanceId=view
healthCheckUrl=/favicon.ico
userNameHeader=AccessPoint-User-ID
proxyPattern=/(.*)
landingPagePath=/
hostEntry1=10.108.120.21 HZNView.uagqe.auto.com
```

```
[Horizon]
proxyDestinationUrl=https://enterViewConnectionServerUrl
trustedCert1=
gatewayLocation=external
disableHtmlAccess=false
healthCheckUrl=/favicon.ico
proxyDestinationIPSupport=IPV4
smartCardHintPrompt=false
queryBrokerInterval=300
proxyPattern=(/|/view-client(.*)|/portal(.*)|/appblast(.*))
matchWindowsUserName=false
windowsSSOEnabled=false

[Airwatch]
tunnelGatewayEnabled=true
tunnelProxyEnabled=true
pacFilePath=
pacFileURL=
credentialFilePath=
apiServerUsername=domain\apiusername
apiServerPassword=*****
proxyDestinationUrl=https://null
ntlmAuthentication=false
healthCheckUrl=/favicon.ico
organizationGroupCode=
apiServerUrl=https://null
airwatchOutboundProxy=false
outboundProxyHost=1.2.3.4
outboundProxyPort=3128
outboundProxyUsername=proxyuser
outboundProxyPassword=****
reinitializeGatewayProcess=false
airwatchServerHostname=tunnel.acme.com
trustedCert1=c:\temp\CA-Cert-A.pem
hostEntry1=1.3.5.7 backend.acme.com

[AirwatchSecureEmailGateway]
airwatchOutboundProxy=false
memConfigurationId=abc123
apiServerUsername=domain\apiusername
healthCheckUrl=/favicon.ico
apiServerUrl=https://null
outboundProxyHost=1.2.3.4
outboundProxyPort=3128
outboundProxyUsername=proxyuser
outboundProxyPassword=****
reinitializeGatewayProcess=false
airwatchServerHostname=serverNameForSNI
apiServerPassword=****
trustedCert1=c:\temp\CA-Cert-A.pem
pfxCerts=C:\Users\admin\My Certs\mycacerts.pfx
hostEntry1=1.3.5.7 exchange.acme.com

[AirWatchContentGateway]
cgConfigId=abc123
```

```
apiServerUrl=https://null
apiServerUsername=domain\apiusername
apiServerPassword=*****
outboundProxyHost=
outboundProxyPort=
outboundProxyUsername=proxyuser
outboundProxyPassword=*****
airwatchOutboundProxy=false
hostEntry1=192.168.1.1 cgbackend.acme.com
trustedCert1=c:\temp\CA-Cert-A.pem
ntlmAuthentication=false
reinitializeGatewayProcess=false
airwatchServerHostname=cg.acme.com

[SSLCert]
pemPrivKey=
pemCerts=
pfxCerts=
pfxCertAlias=

[SSLCertAdmin]
pemPrivKey=
pemCerts=
pfxCerts=
pfxCertAlias=

[JWTSettings1]
publicKey1=
publicKey2=
publicKey3=
name=JWT_1

[JWTSettings2]
publicKey1=
publicKey2=
name=JWT_2

[AdminUser1]
name=monitoringUser1
enabled=true

[AdminUser2]
name=monitoringUser2
enabled=true

[OutboundProxySettings1]
proxyUrl=
name=
proxyType=HTTP
includedHosts1=
includedHosts2=
trustedCert1=

[OutboundProxySettings2]
proxyUrl=
```

```
name=
proxyType=HTTP
includedHosts1=
includedHosts2=
trustedCert1=
```

備註 具有監控角色的低權限管理員使用者的密碼，會以參數的形式提供給 PowerShell 指令碼。如果未提供密碼，則系統會提示使用者輸入密碼。提供參數作為 `newAdminUserPwd`，而其參數值類似於 `monitoringUser1:P@ssw0rd1;monitoringUser2:P@ssw0rd2`。INI 檔案中的 `enabled` 參數為選用，如果參數無法使用，則預設為 true。

5 若要確保指令碼的執行不會受限，請輸入 PowerShell `set-executionpolicy` 命令。

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

您只需執行此動作一次，即可移除此限制。

a (選擇性) 如果出現與指令碼相關的警告，請執行下列命令以解除封鎖警告：`unblock-file -path .\uagdeploy.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`。

```
.\uagdeploy.ps1 -iniFile uag1.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**。

Unified Access Gateway 應用裝置部署即告完成，並可供生產之用。

結果

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

後續步驟

如果您想要升級 Unified Access Gateway 同時保留現有的設定，請編輯 `.ini` 檔案將來源參考變更為新版本，然後重新執行 `.ini` 檔案： `uagdeploy.ps1 uag1.ini`。此程序可能需要長達 3 分鐘。

```
[General]
name=UAG1
source=C:\temp\euc-unified-access-gateway-3.2.1-7766089_OVF10.ova
```

如果您想要在服務不中斷的情況下升級，請參閱不停機升級。

Unified Access Gateway 的部署使用案例

4

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

您可以使用 Horizon、Horizon Cloud with On-Premises Infrastructure、Workspace ONE Access 和 Workspace ONE UEM 來部署 Unified Access Gateway。

本章節討論下列主題：

使用 Horizon 與 Horizon Cloud with On-Premises Infrastructure 進行部署

您可以使用 Unified Access Gateway 和 Horizon Cloud with On-Premises Infrastructure 雲端基礎結構來部署 Horizon Air。

部署案例

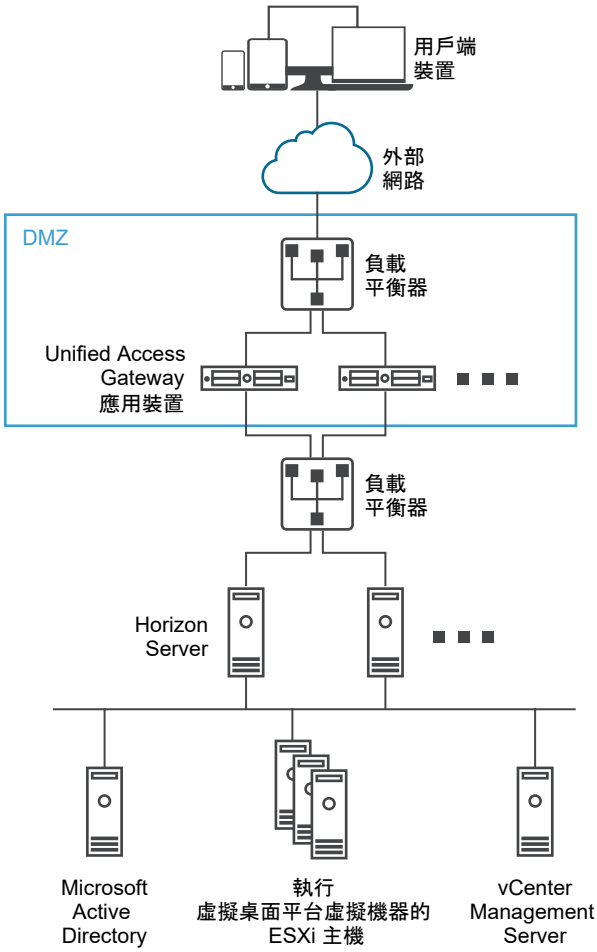
Unified Access Gateway 能提供安全的遠端存取能力，供您存取客戶資料中心內的內部部署虛擬桌面平台和應用程式。它能與 Horizon 或 Horizon Air 的內部部署搭配運作，以進行統合管理。

Unified Access Gateway 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。

Unified Access Gateway 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。Unified Access Gateway 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。

下圖顯示包含前端和後端防火牆的組態範例。

圖 4-1. DMZ 拓撲中的 Unified Access Gateway



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

- Unified Access Gateway 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。
- 依預設，連接埠 8443 必須可供 Blast TCP/UDP 使用。不過，也可以將連接埠 443 設定為可供 Blast TCP/UDP 使用。

  備註 如果您將 Unified Access Gateway 設定為使用 IPv4 和 IPv6 兩種模式，則必須將 Blast TCP/UDP 設定為連接埠 443。請參閱 Unified Access Gateway 對 Horizon 基礎結構支援 IPv4 和 IPv6 雙重模式。

- 使用 Unified Access Gateway 部署 Horizon 時，必須啟用 Blast 安全閘道和 PCoIP 安全閘道。這可確保顯示通訊協定可以自動透過 Unified Access Gateway 成為 Proxy。*BlastExternalURL* 和

pcoipExternalURL 設定會指定 Horizon Client 使用的連線位址，以便透過 Unified Access Gateway 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 Unified Access Gateway 忽略。

- 在 Horizon 連線伺服器執行個體上停用安全閘道 (Blast 安全閘道和 PCoIP 安全閘道)，並在 Unified Access Gateway 應用裝置上啟用這些閘道。

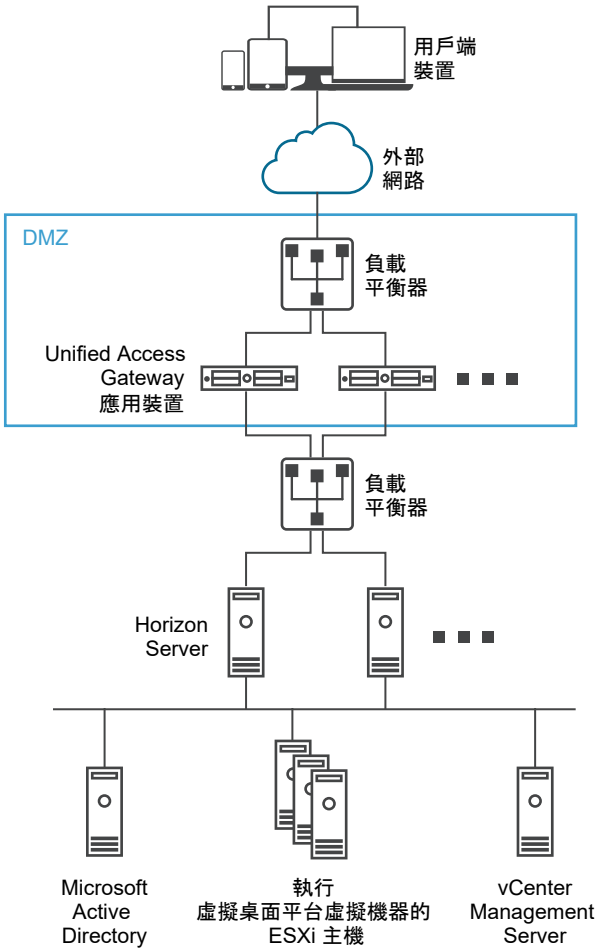
建議使用者使用 Unified Access Gateway 應用裝置 (而非 Horizon 安全伺服器) 來部署 Horizon 7。

備註 當 Proxy 模式中有重疊時，Horizon Connection Server 無法搭配已啟用的 Web 反向 Proxy 正常運作。因此，如果在相同的 Unified Access Gateway 執行個體上使用 Proxy 模式同時設定並啟用了 Horizon 和 Web 反向 Proxy 執行個體，請從 Horizon 設定中移除 Proxy 模式「/」，並保留 Web 反向 Proxy 中的模式以防止重疊。保留 Web 反向 Proxy 執行個體中的「/」Proxy 模式可確保使用者在按一下 Unified Access Gateway 的 URL 時會顯示正確的 Web 反向 Proxy 頁面。如果僅設定了 Horizon 設定，則不需要進行前述變更。

Horizon 安全伺服器和 Unified Access Gateway 應用裝置之間的差異如下所示。

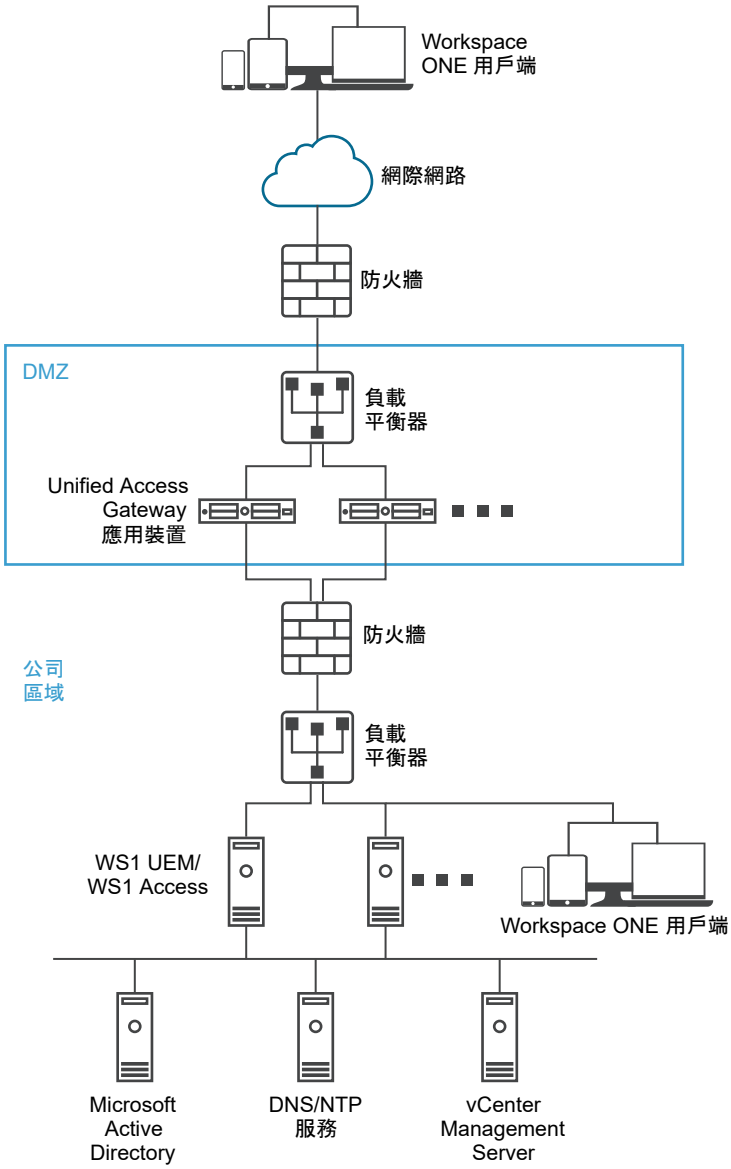
- 安全部署。Unified Access Gateway 可實作為強化、鎖定且預先設定的 Linux 虛擬機器。
- 可擴充。您可以將 Unified Access Gateway 連接到個別的 Horizon 連線伺服器，或透過多部 Horizon 連線伺服器前方的負載平衡器予以連接，藉此改善高可用性。它可作為 Horizon Client 與後端 Horizon 連線伺服器之間的層。由於部署快速，因此它能迅速垂直擴充或垂直縮減，以滿足快速變遷的企業需求。

圖 4-2. 指向負載平衡器的 Unified Access Gateway 應用裝置



或者，您也可以讓一或多部 Unified Access Gateway 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 Unified Access Gateway 應用裝置前方使用負載平衡器。

圖 4-3. 指向 Horizon Server 執行個體的 Unified Access Gateway 應用裝置



驗證

使用者驗證與 Horizon 安全伺服器類似。Unified Access Gateway 支援的使用者驗證方法包括：

- 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。
- 透過各種第三方雙因素安全性廠商解決方案的 RADIUS。
- 智慧卡、CAC 或 PIV X.509 使用者憑證。
- SAML。

搭配 Horizon Connection Server 時，以上驗證方法都能獲得支援。Unified Access Gateway 不需要直接與 Active Directory 通訊。這種模式的通訊能作為透過 Horizon Connection Server 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，Unified Access Gateway 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 Horizon Connection Server。Unified Access Gateway 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。

Unified Access Gateway 本身會處理智慧卡驗證。內容包括讓 Unified Access Gateway 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。

Unified Access Gateway 對 Horizon 基礎結構支援 IPv4 和 IPv6 雙重模式

您可以使用 Unified Access Gateway 來充當 Horizon 用戶端連線至後端 Horizon Connection Server 或代理程式環境的橋接器。在此案例中，Horizon Client 和 Horizon Connection Server 可設定具有不同的 IP 模式：IPv4 或 IPv6，反之亦然。

Horizon 後端環境可能包含連線伺服器、代理程式桌面平台或其他伺服器端基礎結構。

Horizon 基礎結構的 IP 模式組合

在 Horizon 基礎結構中，Horizon Client 和 Horizon Connection Server 可以有下列 IP 模式：

Horizon Client	Horizon Connection Server	支援
IPv4	IPv4	是
IPv6	IPv4	是
IPv6	IPv6	是
IPv4	IPv6	是

備註 當 Horizon Client 和 Horizon Connection Server 設定為使用不同的 IP 模式 (IPv4 或 IPv6，反之亦然)，**連線伺服器 IP 模式** (Unified Access Gateway 管理員 UI 中的設定) 可以具有下列其中一個值：與 Horizon Connection Server 相同的 IP 模式或混合模式 (`IPv4+IPv6`)。

例如：Horizon Client 設定為使用 IPv4，而 Horizon Connection Server 設定為使用 IPv6，則**連線伺服器 IP 模式**可以有 `IPv6` 或 `IPv4+IPv6` (混合模式) 值。

如需有關**連線伺服器 IP 模式**設定的詳細資訊，請參閱設定 Horizon 設定。

當 IP 模式為橋接 (IPv4 至 IPv6 或 IPv6 至 IPv4) 時，Unified Access Gateway 不支援下列：Horizon Tunnel、PCoIP 或 Blast UDP。

備註 必須將 Blast 外部 URL 設定為使用 TCP 連接埠 443 或 8443。

進階 Edge Service 設定

Unified Access Gateway 會使用不同的變數區分 Edge Service、設定的 Web Proxy 以及 Proxy 目的地 URL。

Proxy 模式和未受保護的模式

Unified Access Gateway 會使用 Proxy 模式將傳入 HTTP 要求轉送至正確的 Edge Service，例如 Horizon 或所設定的其中一個 Web 反向 Proxy 執行個體，例如 Workspace ONE Access。因此，它可以用作一個篩選器，以決定處理傳入流量時是否需要反向 Proxy。

如果選取了反向 Proxy，則 Proxy 會使用指定的未受保護模式，以決定是否允許傳入流量在不經驗證的情況下進入後端。

使用者必須指定 Proxy 模式，而指定未受保護的模式為選用。具有本身的登入機制，且想要讓登入頁面路徑、Javascript 或映像資源等特定 URL 在不經驗證的情況下傳遞後端的 Web 反向 Proxy (例如 Workspace ONE Access) 會使用未受保護的模式。

備註 未受保護的模式是 Proxy 模式的子集，因此兩者之間針對反向 Proxy 可能會有部分重複路徑。

備註 此模式也可用來排除某些 URL。例如，若要允許所有 URL 通過但封鎖 /admin，則可以使用下列運算式。`^/(?!admin(.*))(.*)`

每個 Edge Service 可以有不同的模式。例如，可以將 Horizon 的 `Proxy Pattern` 設定為 `(/|/view-client(.*)|/portal(.*)|/appblast(.*))`，以及將 Workspace ONE Access 的模式設定為 `(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`。

備註 當 Proxy 模式中有重疊時，Horizon Connection Server 無法搭配已啟用的 Web 反向 Proxy 正常運作。因此，如果在相同的 Unified Access Gateway 執行個體上使用 Proxy 模式同時設定並啟用了 Horizon 和 Web 反向 Proxy 執行個體 (例如 Workspace ONE Access)，請從 Horizon 設定中移除 Proxy 模式「/」，並保留 Workspace ONE Access 中的模式以防止重疊。

保留 Web 反向 Proxy 執行個體 (Workspace ONE Access) 中的「/」Proxy 模式可確保使用者在按一下 Unified Access Gateway 的 URL 時會顯示 Workspace ONE Access 頁面。

如果僅設定了 Horizon 設定，則不需要進行前述變更。

Proxy 主機模式

如果設定了多個 Web 反向 Proxy 執行個體，且 Proxy 模式中有重疊，則 Unified Access Gateway 會使用 `Proxy Host Pattern` 來加以區分。將 `Proxy Host Pattern` 設定為反向 Proxy 的 FQDN。

例如，可以將 SharePoint 的主機模式設定為 *sharepoint.myco.com*，以及將 JIRA 的模式設定為 *jira.myco.com*。

主機項目

僅在 Unified Access Gateway 無法連線後端伺服器或應用程式時才設定此文字方塊。當您將後端應用程式的 IP 位址和主機名稱新增至「主機項目」時，系統會將該資訊新增至 Unified Access Gateway 的 `/etc/hosts` 檔案。此欄位為所有 Edge Service 設定的通用欄位。

Proxy 目的地 URL

這是 Unified Access Gateway 為 Proxy 之 Edge Service 設定的後端伺服器應用程式 URL。例如：

- 針對 Horizon Connection Server，連線伺服器 URL 為 Proxy 目的地 URL。

- 針對 Web 反向 Proxy，所設定 Web 反向 Proxy 的應用程式 URL 為 Proxy 目的地 URL。

單一反向 Proxy 組態

當 Unified Access Gateway 接收到具有 URI 的單一傳入要求時，系統會使用 Proxy 模式來決定是要轉送要求或將其捨棄。

多個反向 Proxy 組態

1. 將 Unified Access Gateway 設定為反向 Proxy，並且具有 URI 路徑的傳入要求到達時，Unified Access Gateway 會使用 Proxy 模式來比對正確的 Web 反向 Proxy 執行個體。如果有相符項目，則會使用相符的模式。如果有多個相符項目，則會在步驟 2 中重複進行篩選和比對程序。如果沒有相符項目，則會捨棄要求，並將 HTTP 404 傳送回用戶端。
2. Proxy 主機模式用來篩選已在步驟 1 中篩選的清單。HOST 標頭則用來篩選要求，以及尋找反向 Proxy 執行個體。如果有相符項目，則會使用相符的模式。如果有多個相符項目，則會在步驟 3 中重複進行篩選和比對程序。
3. 請注意下列事項：
   - 系統會使用步驟 2 中已篩選清單的第一個相符項目。此相符項目可能不會永遠是正確的 Web 反向 Proxy 執行個體。因此，如果 Unified Access Gateway 中有多個反向 Proxy 設定，請確保 Web 反向 Proxy 執行個體的 Proxy 模式和 Proxy 主機模式的組合是唯一的。
   - 所有已設定反向 Proxy 的主機名稱應解析為與 Unified Access Gateway 執行個體之外部位址相同的 IP 位址。

如需設定反向 Proxy 的詳細資訊和相關指示，請參閱使用 Workspace ONE Access 設定反向 Proxy。

範例：兩個已設定的反向 Proxy，具有衝突 Proxy 模式、不同主機模式

假設第一個反向 Proxy 的 Proxy 模式為 `/(.*)` 且主機模式為 `host1.domain.com`，而第二個反向 Proxy 的模式為 `(/app2(.*)|/app3(.*)|/)` 且主機模式為 `host2.domain.com`。

- 如果提出將路徑設定為 `https://host1.domain.com/app1/index.html` 的要求，則要求會轉送至第一個反向 Proxy。
- 如果提出將路徑設定為 `https://host2.domain.com/app2/index.html` 的要求，則要求會轉送至第二個反向 Proxy。

範例：兩個反向 Proxy，具有互斥 Proxy 模式

假設第一個反向 Proxy 的 Proxy 模式為 `/app1(.*)`，而第二個反向 Proxy 的 Proxy 模式為 `(/app2(.*)|/app3(.*)|/)`。

- 如果提出將路徑設定為 `https://<uag domain name>/app1/index.html` 的要求，則要求會轉送至第一個反向 Proxy。
- 如果提出將路徑設定為 `https://<uag domain name>/app3/index.html` 或 `https://<uag domain name>/` 的要求，則要求會轉送至第二個反向 Proxy。

設定 Horizon 設定

您可以使用 Unified Access Gateway 和 Horizon Cloud with On-Premises Infrastructure 雲端基礎結構來部署 Horizon Air。對於 Horizon 部署，Unified Access Gateway 應用裝置會取代 Horizon 安全伺服器。

必要條件

如果您想要同時擁有 Horizon 和 Web Reverse Proxy 執行個體 (例如，在相同的 Unified Access Gateway 執行個體上設定並啟用的 Workspace ONE Access)，請參閱進階 Edge Service 設定。

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**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 Horizon。Unified Access Gateway 可與使用 Horizon XML 通訊協定的伺服器進行通訊，例如 Horizon 連線伺服器、Horizon Air 和 Horizon Cloud with On-Premises Infrastructure。
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`。
連線伺服器 URL 指紋	輸入 Horizon server 指紋的清單。 如果未提供指紋的清單，請確保伺服器憑證是由信任的 CA 核發。輸入十六進位的指紋數字。例如，sha1= C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3。
啟用 PCOIP	將 [否] 變更為**是**可指定是否啟用 PCoIP 安全閘道。
停用 PCOIP 舊版憑證	將**否**變更為**是**，以指定要使用上傳的 SSL 伺服器憑證，而不是舊版憑證。如果此參數設為**是**，舊版 PCoIP 用戶端將無法運作。
PCOIP 外部 URL	Horizon 用戶端用來對此 Unified Access Gateway 應用裝置建立 Horizon PCoIP 工作階段的 URL。它必須包含 IPv4 位址，且不是主機名稱。例如，`10.1.2.3:4172`。預設值為 Unified Access Gateway IP 位址和連接埠 4172。
啟用 Blast	若要使用 Blast 安全閘道，請將 [否] 變更為**是**。

選項	說明
連線伺服器 IP 模式	指出 Horizon Connection Server 的 IP 模式 此欄位可以具有以下值：`IPv4`、`IPv6` 和 `IPv4+IPv6`。 預設為 `IPv4`。 ■ 如果 Unified Access Gateway 應用裝置中的所有 NIC 均處於 IPv4 模式 (無 IPv6 模式)，則此欄位可以具有下列其中一個值：`IPv4` 或 `IPv4+IPv6` (混合模式)。 ■ 如果 Unified Access Gateway 應用裝置中的所有 NIC 均處於 IPv6 模式 (無 IPv4 模式)，則此欄位可以具有下列其中一個值：`IPv6` 或 `IPv4+IPv6` (混合模式)。
重新寫入來源標頭	如果對 Unified Access Gateway 的傳入要求具有 `Origin` 標頭，且已啟用**重新寫入來源標頭**欄位，Unified Access Gateway 會使用**連線伺服器 URL** 重寫 `Origin` 標頭。 **重新寫入來源標頭**欄位會隨著 Horizon Connection Server 的 `checkOrigin` CORS 內容一起運作。啟用此欄位時，Horizon 管理員可以不需要在 `locked.properties` 檔案中指定 Unified Access Gateway IP 位址。 如需來源檢查的相關資訊，請參閱《Horizon 7 安全性》說明文件。

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	預設會使用使用者名稱和密碼的傳遞驗證。 以下是支援的驗證方法：`SAML`、`SAML and Unauthenticated`、`RSA SecurID`、`SecurID and Unauthenticated`、`RADIUS`、`RADIUS and Unauthenticated` 和 `Device Certificate`。 **重要** 如果您已選擇任何 `Unauthenticated` 方法作為驗證方法，請確實將 Horizon Connection Server 中的**登入減速層級**設定為 `Low`。在存取遠端桌面平台或應用程式時，必須進行此組態，以避免端點的登入長時間延遲。 如需關於如何設定**登入減速層級**的詳細資訊，請參閱 VMware Docs 中的《Horizon 管理》說明文件。
啟用 Windows SSO	當驗證方法設定為 RADIUS，並且 RADIUS 密碼與 Windows 網域密碼相同時，便可啟用此功能。將**否**變更為**是**可對 Windows 網域登入認證使用 RADIUS 使用者名稱和密碼，從而不必再次提示使用者。 如果在多網域環境上設定 Horizon，且提供的使用者名稱未包含網域名稱，系統就不會將網域傳送至 CS。 如果已設定名稱識別碼尾碼，且提供的使用者名稱未包含網域名稱，則系統會將所設定的名稱識別碼尾碼值附加至使用者名稱。例如，如果使用者提供 jdoe 作為使用者名稱，且 NameIDSuffix 設定為 `@north.int`，則傳送的使用者名稱會是 `jdoe@north.int`。 如果已設定名稱識別碼尾碼，且提供的使用者名稱採用 UPN 格式，則系統會忽略名稱識別碼尾碼。例如，如果使用者提供 `jdoe@north.int`、NameIDSuffix - `@south.int`，則使用者名稱會是 `jdoe@north.int` 如果提供的使用者名稱採用 `<DomainName\username>` 格式 (例如，`NORTH\jdoe`)，則 Unified Access Gateway 會將使用者名稱和網域名稱分開傳送至 CS。

選項	說明
RADIUS 類別屬性	驗證方法設為 RADIUS 時，系統會啟用此選項。按一下「+」可新增類別屬性的值。輸入要用於使用者驗證的類別屬性名稱。按一下「-」可移除類別屬性。 **備註** 如果此欄位保留為空白，則不會執行其他授權。
免責聲明文字	在設定了**驗證方法**的情況下，要對使用者顯示並由使用者接受的 Horizon 免責聲明訊息。
智慧卡提示	將 [否] 變更為**是**，可啟用憑證驗證的密碼提示。
健全狀況檢查 URI 路徑	Unified Access Gateway 為了進行健全狀況狀態監控而連線之連線伺服器的 URI 路徑。
Blast 外部 URL	Horizon 用戶端用來對此 Unified Access Gateway 應用裝置建立 Horizon Blast 或 BEAT 工作階段的 URL。例如，`https://uag1.myco.com` 或 `https://uag1.myco.com:443`。 如果未指定 TCP 連接埠號碼，則預設 TCP 連接埠為 8443。如果未指定 UDP 連接埠號碼，則預設 UDP 連接埠也是 8443。
啟用 UDP 伺服器	頻寬低時，會透過 UDP 通道伺服器建立連線。
Blast Proxy 憑證	用於 Blast 的 Proxy 憑證。按一下**選取**來上傳 PEM 格式的憑證，然後新增至 BLAST 信任存放區。按一下**變更**來取代現有的憑證。 如果使用者將 Unified Access Gateway 的相同憑證手動上傳至負載平衡器，並且需要對 Unified Access Gateway 和 Blast 閘道使用不同的憑證，則建立 Blast 桌面平台工作階段將會失敗，因為用戶端與 Unified Access Gateway 之間的指紋不相符。對 Unified Access Gateway 或 Blast 閘道的自訂指紋輸入，會透過轉送指紋以建立用戶端工作階段來解決此問題。
啟用通道	如果使用了 Horizon 安全通道，請將 [否] 變更為**是**。用戶端會使用此外部 URL 透過 Horizon 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	Horizon 用戶端用來對此 Unified Access Gateway 應用裝置建立 Horizon Tunnel 工作階段的 URL。例如，`https://uag1.myco.com` 或 `https://uag1.myco.com:443`。 如果未指定 TCP 連接埠號碼，則預設 TCP 連接埠為 443。
通道代理伺服器憑證	用於 Horizon Tunnel 的 Proxy 憑證。按一下**選取**來上傳 PEM 格式的憑證，然後新增至通道信任存放區。按一下**變更**來取代現有的憑證。 如果使用者將 Unified Access Gateway 的相同憑證手動上傳至負載平衡器，並且需要對 Unified Access Gateway 和 Horizon Tunnel 使用不同的憑證，則建立通道工作階段將會失敗，因為用戶端與 Unified Access Gateway 之間的指紋不相符。對 Unified Access Gateway 或 Horizon Tunnel 的自訂指紋輸入，會透過轉送指紋以建立用戶端工作階段來解決此問題。
端點符合性檢查提供者	選取端點符合性檢查提供者。 預設為 OPSWAT。
Proxy 模式	輸入將相關 URI 與 Horizon Server URL (proxyDestinationUrl) 比對的規則運算式。其預設值為 `(/|/view-client(.*)|/portal(.*)|/appblast(.*))`。 **備註** 此模式也可用來排除某些 URL。例如，若要允許所有 URL 通過但封鎖 /admin，則可以使用下列運算式。`^/(?!admin(.*))(.*)`
SAML SP	輸入 Horizon 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。

選項	說明
移除憑證時登出	**備註** 將任何智慧卡驗證方法選取為**驗證方法**時，即可使用此選項。 如果此選項設為 `YES`，且已移除智慧卡，則會強制使用者從 Unified Access Gateway 工作階段登出。
RADIUS 的使用者名稱標籤	輸入文字即可自訂 Horizon Client 中的使用者名稱標籤。例如，`Domain Username` 必須啟用 RADIUS 驗證方法。若要啟用 RADIUS，請參閱設定 RADIUS 驗證。 預設標籤名稱為 `Username`。 標籤名稱的長度上限為 20 個字元。
RADIUS 的密碼標籤	輸入名稱即可在 Horizon Client 中自訂密碼標籤。例如，`Password` 必須啟用 RADIUS 驗證方法。若要啟用 RADIUS，請參閱設定 RADIUS 驗證。 預設標籤名稱為 `Passcode`。 標籤名稱的長度上限為 20 個字元。
比對 Windows 使用者名稱	將**否**變更為**是**以比對 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 使用者名稱進行比對。 如果在多網域環境上設定 Horizon，且提供的使用者名稱未包含網域名稱，系統就不會將網域傳送至 CS。 如果已設定名稱識別碼尾碼，且提供的使用者名稱未包含網域名稱，則系統會將所設定的名稱識別碼尾碼值附加至使用者名稱。例如，如果使用者提供 jdoe 作為使用者名稱，且 NameIDSuffix 設定為 `@north.int`，則傳送的使用者名稱會是 `jdoe@north.int`。 如果已設定名稱識別碼尾碼，且提供的使用者名稱採用 UPN 格式，則系統會忽略名稱識別碼尾碼。例如，如果使用者提供 `jdoe@north.int`、NameIDSuffix - `@south.int`，則使用者名稱會是 `jdoe@north.int` 如果提供的使用者名稱採用 `<DomainName\username>` 格式 (例如，`NORTH\jdoe`)，則 Unified Access Gateway 會將使用者名稱和網域名稱分開傳送至 CS。 **備註** 在 Horizon 7 中，如果您啟用**在用戶端使用者介面中隱藏伺服器資訊**和**在用戶端使用者介面中隱藏網域清單**設定，並且為連線伺服器執行個體選取了雙因素驗證 (RSA SecureID 或 RADIUS)，請不要強制執行 Windows 使用者名稱比對。強制執行 Windows 使用者名稱比對會防止使用者在使用者名稱文字方塊中輸入網域資訊，導致登入一律會失敗。如需詳細資訊，請參閱《Horizon 7 管理》文件中有關於雙因素驗證的主題。
閘道位置	從中起始連線要求的位置。安全伺服器和 Unified Access Gateway 會設定閘道位置。位置可以是 `External` 或 `Internal`。 **重要** 選取下列任何一種驗證方法時，必須將位置設定為 `Internal`：`SAML and Unauthenticated`、`SecurID and Unauthenticated` 或 `RADIUS and Unauthenticated`。
JWT 設定	**備註** 若要進行 Workspace ONE Access JWT SAML 構件驗證，請確定您已在**進階設定**的 **JWT 設定**區段中完成**名稱**欄位的設定。 選取其中一個已設定之 **JWT 設定**的名稱。

選項	說明
JWT 對象	用於 Workspace ONE Access Horizon SAML 構件驗證之 JWT 的預定收件者清單，此為選擇性清單。 若要讓 JWT 驗證成功，此清單中至少要有一位收件者符合 Workspace ONE Access Horizon 組態中所指定的其中一位對象。若未指定任何 JWT 對象，則 JWT 驗證不會考慮對象。
受信任的憑證	■ 若要選取 PEM 格式的憑證並新增至信任存放區，請按一下 **+**。 ■ 若要提供不同名稱，請編輯別名文字方塊。 依預設，別名名稱是 PEM 憑證的檔案名稱。 ■ 若要從信任存放區移除憑證，請按一下 **-**。 **備註** 受信任的憑證檔案名稱不得包含空格。
回應安全性標頭	若要新增標頭，請按一下 **+**。輸入安全性標頭的名稱。輸入值。 若要移除標頭，請按一下 **-**。編輯現有的安全性標頭，以更新標頭的名稱和值。 **重要** 在您按一下**儲存**後，才會儲存標頭名稱和值。 依預設會顯示部分標準安全性標頭。僅在已設定後端伺服器的回應中沒有對應的標頭存在時，才會將已設定標頭新增至用戶端的 Unified Access Gateway 回應。 **備註** 請謹慎修改安全性回應標頭。修改這些參數可能會影響到 Unified Access Gateway 的安全運作。
主機重新導向對應	如需 UAG 如何支援 HTTP 主機重新導向功能的相關資訊，以及要使用此功能所需的特定考慮事項，請參閱 Unified Access Gateway 對 HTTP 主機重新導向的支援。 ■ **來源主機** 輸入來源 (負載平衡器) 的主機名稱。 ■ **重新導向主機** 輸入必須與 Horizon Client 保持相似性之 Unified Access Gateway 應用裝置的主機名稱。
主機項目	輸入要在 `/etc/hosts` 檔案中新增的詳細資料。每個項目依序應包括一個 IP、一個主機名稱和一個選用的主機名稱別名 (以空格區隔)。例如，**`10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`**。按一下「+」符號可新增多個主機項目。 **重要** 只有在按一下**儲存**後，才會儲存主機項目。
SAML 對象	請務必選擇 SAML 或「SAML 和傳遞」驗證方法之一。 輸入對象 URL。 **備註** 如果文字方塊保持空白，則對象不受限。 若要了解 UAG 支援 SAML 對象的方式，請參閱 SAML 對象。
SAML 未驗證使用者名稱屬性	輸入自訂屬性名稱 **備註** 只有在**驗證方法**的值為 `SAML and Unauthenticated` 時，才能使用此欄位。 當 UAG 驗證 SAML 判斷提示時，如果在此欄位中指定的屬性名稱存在於判斷提示中，UAG 就會為針對身分識別提供者中的屬性而設定的使用者名稱提供未驗證存取。 如需關於 `SAML and Unauthenticated` 方法的詳細資訊，請參閱適用於 Unified Access Gateway 與第三方身分識別提供者整合的驗證方法。

選項	說明
預設未驗證使用者名稱	輸入必須用於未驗證存取的預設使用者名稱 選取下列其中一種**驗證方法**時，可以在管理員 UI 中使用此欄位：`SAML and Unauthenticated`、`SecurID and Unauthenticated` 和 `RADIUS and Unauthenticated`。 **備註** 針對 `SAML and Unauthenticated` 驗證方法，只有在 **SAML 未驗證使用者名稱屬性**欄位空白，或 SAML 判斷提示中缺少此欄位所指定的屬性名稱時，才會使用未驗證存取的預設使用者名稱。
停用 HTML Access	如果設定為 [是]，則會停用 Horizon 的 Web 存取。如需詳細資料，請參閱將 OPSWAT 設定為 Horizon 的端點符合性檢查提供者。

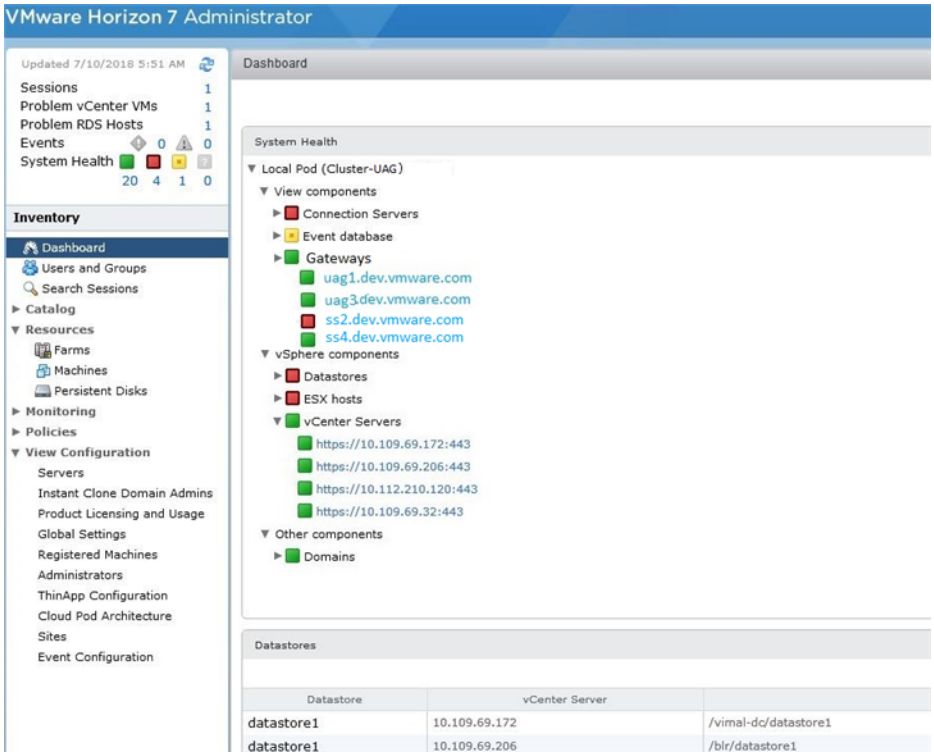
7 按一下**儲存**。

在 Horizon Console 中監控 Unified Access Gateway

Unified Access Gateway 與 Horizon 管理主控台的整合提供狀態、統計資料及 Horizon 管理員 UI 中工作階段資訊的能見度。您可以監控 Unified Access Gateway 的系統健全狀況。

Horizon 管理主控台中的新**閘道**索引標籤，提供登錄和解除登錄 Unified Access Gateway 的功能。

圖 4-4. 儀表板



儀表板畫面會顯示已登錄的 Unified Access Gateway 3.4 版或更新版本 、vSphere 元件、網域、桌面平台和資料存放區使用量的詳細資料。

Unified Access Gateway 對 HTTP 主機重新導向的支援

HTTP 主機重新導向功能可用來簡化某些多 VIP 環境中的 Horizon 負載平衡相似性需求。若要使用 HTTP 主機重新導向功能，UAG 管理員必須在 Horizon 設定中設定**主機重新導向對應**文字方塊。

當 HTTP 要求使用負載平衡器的主機名稱到達 UAG 時，UAG 會以 HTTP 307 重新導向來加以回應，並使用 UAG 本身所設定的主機名稱來取代負載平衡器的主機名稱。後續要求到達時，Horizon Client 則會直接與 UAG 重新連線。這可確保後續要求不會透過負載平衡器來路由傳送。重新導向功能避免了負載平衡器上的相似性控制問題，不會讓要求路由傳送至不正確的 UAG。

例如，請設想具有一個負載平衡器和兩個 UAG 應用裝置 (UAG1 和 UAG2) 的環境。如果要求使用負載平衡器的主機名稱 (`load-balancer.example.com`) 到達 UAG1，UAG1 會以 `HTTP 307` 重新導向來加以回應，並使用 UAG 本身所設定的主機名稱 (`uag1.example.com`) 來取代負載平衡器的主機名稱。後續要求到達時，Horizon Client 則會直接與 UAG1 重新連線。

使用 HTTP 主機重新導向時的考量事項

在使用 HTTP 主機重新導向功能時，您必須注意下列考量事項：

- 必須有 `N + 1` 個虛擬 IP 位址，其中

  `N` - 環境中所部署的 UAG 應用裝置數目

  `1` - 負載平衡器的 VIP
- 您無法使用在第 7 層運作的負載平衡器。

若要在 Horizon 中進行設定，請參閱設定 Horizon 設定

SAML 對象

SAML 對象是 UAG (Unified Access Gateway) 針對 Edge 服務 (例如 Horizon 和 Web 反向 Proxy) 所支援的功能。透過使用 SAML 對象功能，UAG 管理員可限制存取 Horizon Client 和後端應用程式的對象。

在 Horizon Edge 服務中，SAML 和 SAML 與傳遞驗證方法皆支援 SAML 對象。在 Web 反向 Proxy Edge 服務中，只有在已啟用身分識別橋接時，SAML 驗證方法才會支援 SAML 對象。

如果 **SAML 對象**已設定了值，則 UAG 會對照在 SAML 判斷提示中收到的對象來驗證這份值清單。如果有至少一個相符項，則會接受 SAML 判斷提示。如果沒有相符項，則 UAG 會拒絕 SAML 判斷提示。如果 SAML 對象未進行設定，則 UAG 不會驗證 SAML 判斷提示中的對象。

若要限制 Horizon Edge 服務的對象，請參閱設定 Horizon 設定。若要限制 Web 反向 Proxy Edge 服務的對象，則請參閱針對身分識別橋接設定 Web 反向 Proxy (對 Kerberos 的 SAML)。

Blast TCP 和 UDP 外部 URL 組態選項

Blast 安全閘道包含 Blast Extreme Adaptive Transport (BEAT) 網路功能，它會根據網路情況 (例如不同的速度和封包遺失) 進行動態調整。在 Unified Access Gateway 中，您可以設定 BEAT 通訊協定所使用的連接埠。

Blast 會使用標準連接埠 TCP 8443 和 UDP 8443。UDP 443 也可以用來透過 UDP 通道伺服器存取桌面平台。連接埠組態是透過 Blast 外部 URL 內容而設定。

表 4-1. BEAT 連接埠選項

Blast 外部 URL	用戶端使用的 TCP 連接埠	用戶端使用的 UDP 連接埠	說明
https://ap1.myco.com	8443	8443	此為預設表單，且需要在防火牆開啟 TCP 8443 以及選用的 UDP 8443，才能允許從網際網路到 Unified Access Gateway 的連線
https://ap1.myco.com:443	443	8443	需要開啟 TCP 443 或 UDP 8443 時，請使用此表單。
https://ap1.myco.com:xxxx	xxxx	8443	
https://ap1.myco.com:xxxx/?UDPPort=yyyy	xxxx	yyyy	

若要設定預設值以外的連接埠，部署時必須為相關的通訊協定新增內部 IP 轉送規則。轉送規則可以在部署時的 OVF 範本中指定，或透過利用 PowerShell 命令輸入的 INI 檔案指定。

Horizon 的端點符合性檢查

除了 Unified Access Gateway 應用裝置上可用的其他使用者驗證服務之外，端點符合性檢查功能為存取 Horizon 桌面平台提供額外一層的安全性。您可以使用此功能來確保符合各種原則，例如端點上的防毒原則或加密原則。

端點符合性檢查是進階設定，可在**端點符合性檢查提供者設定**頁面上進行設定。管理員可以使用此頁面來設定必須拒絕或允許存取的端點裝置狀態碼。設定頁面也具有時間間隔文字方塊，管理員可使用此方塊來設定在經驗證的使用者工作階段期間，端點的定期符合性檢查。

使用者驗證成功之後，當使用者嘗試從列出的權利啟動遠端桌面平台或應用程式時，以及在經驗證的工作階段期間，系統會檢查端點符合性。

成功驗證之後，如果端點裝置的狀態為設定要拒絕存取的狀態，則即使使用者已成功驗證，裝置仍會遭到拒絕存取。因此，使用者無法啟動遠端桌面平台或應用程式。

端點符合性原則是在雲端或內部部署中執行的服務上定義。OPSWAT MetaAccess persistent agent 或 OPSWAT MetaAccess on-demand agent 是 Horizon Client 上執行端點符合性檢查的 OPSWAT 代理程式。這些代理程式會針對符合性狀態向雲端或內部部署中執行的 OPSWAT 執行個體進行通訊。

將 OPSWAT 設定為 Horizon 的端點符合性檢查提供者

當您選取 OPSWAT 作為端點符合性檢查提供者時，必須進行特定設定才能讓 Unified Access Gateway 與 OPSWAT 進行整合。例如，您可以設定會發生定期符合性檢查的時間間隔，將 on-demand agent 可執行檔上傳至 Unified Access Gateway 等等。

在 **Horizon 設定**頁面上選取 OPSWAT 作為端點符合性檢查提供者時，Unified Access Gateway 會使用 OPSWAT 執行 Horizon Client 的端點裝置檢查。執行此檢查是為了讓具有不合規端點的使用者遭到 Horizon 桌面平台和應用程式拒絕存取。

必要條件

1 註冊 OPSWAT 帳戶並在 OPSWAT 站台上登錄您的應用程式。請參閱 https://go.opswat.com/communityRegistration。

2 請記下用戶端金鑰和用戶端秘密金鑰。您需要這些金鑰才能在 Unified Access Gateway 中設定 OPSWAT。

3 登入 OPSWAT 站台並設定您端點的符合性原則。

請參閱相關的 OPSWAT 說明文件。

程序

1 登入管理員 UI 並移至**進階設定 > 端點符合性檢查提供者設定**。

2 按一下**新增**。

3 選取 OPSWAT 作為**端點符合性檢查提供者**。

4 輸入**用戶端金鑰**和**用戶端密碼**。

5 在**符合性檢查間隔 (分鐘)** 中輸入所需的值。

- 有效值 (以分鐘為單位) - 5 至 1440
- 預設值 - 0

  0 表示**符合性檢查間隔 (分鐘)** 已停用。

如需定期符合性檢查和**符合性檢查間隔 (分鐘)** 的詳細資訊，請參閱定期端點符合性檢查的時間間隔。

6 在**符合性檢查快速間隔 (分鐘)** 中輸入所需的值。

重要 若要設定**符合性檢查快速間隔 (分鐘)**，請確定**符合性檢查間隔 (分鐘)** 已設定，而非 0。

- 有效值 (以分鐘為單位) - 1 至 1440
- 預設值 - 0

  0 表示**符合性檢查快速間隔 (分鐘)** 已停用。

如需定期符合性檢查和**符合性檢查快速間隔 (分鐘)** 的詳細資訊，請參閱定期端點符合性檢查的時間間隔。

7 若要變更狀態的預設值並允許端點啟動，請按一下**顯示允許的狀態碼**。

支援下列狀態碼：In compliance、Not in compliance、Out of license usage、Assessment pending、Endpoint unknown 和 Others。

8 針對所需的**狀態碼**，按一下可從**拒絕**變更為**允許**。

符合規定狀態碼的預設值為 ALLOW。只有符合規定的端點會允許啟動。

所有其他狀態碼的預設值則為 DENY。

9 若要將適用於 Windows 和 macOS 平台的 OPSWAT MetaAccess on-demand agent 可執行檔上傳至 Unified Access Gateway，請按一下**顯示 OPSWAT 隨選代理程式設定**，並設定所需的設定。

請參閱在 Unified Access Gateway 上傳 OPSWAT MetaAccess on-demand agent 軟體。

10 按一下**儲存**。

後續步驟

1 導覽至 Horizon 設定，找到**端點符合性檢查提供者**文字方塊，並從下拉式功能表中選取 `OPSWAT`。

2 按一下**儲存**。

在 Unified Access Gateway 上傳 OPSWAT MetaAccess on-demand agent 軟體

管理員可以在 Unified Access Gateway 上傳 on-demand agent 可執行檔。這可提供選項，讓 Horizon Client 在使用者成功驗證後，自動下載並執行 on-demand agent。

如需瞭解 on-demand agent 的相關資訊，請參閱關於 OPSWAT MetaAccess on-demand agent。

必要條件

在相關的 OPSWAT 網站上找出 on-demand agent 可執行檔，並將檔案下載至您的系統。

或者，您也可以將該可執行檔置於檔案伺服器中，並在設定管理員 UI 上的設定時指定對應的檔案伺服器位置 URL。透過此 URL 參考，Unified Access Gateway 可以從設定的 URL 下載檔案。

重要 為了讓 Unified Access Gateway 成功下載檔案，檔案伺服器的 `Content-Disposition` 標頭必須使用隨選代理程式的檔案名稱作為 HTTP 回應中的值。

程序

- 對於 Windows 平台，請依照所述內容執行下列步驟。

  a 選取**檔案上傳類型**。

  - 如果您不想上傳任何檔案，請選取 None。
  - None 是預設值。

  b 視選取的檔案上傳類型而定，輸入在 Unified Access Gateway 上傳 on-demand agent 所需的資訊。

選項	程序
本機	1 找到並選取您已從 OPSWAT 下載的 on-demand agent 可執行檔。 2 輸入 on-demand agent 的下列其他資訊：**名稱**和**參數**。
URL 參考	1 在**代理程式檔案 URL** 中，輸入 Unified Access Gateway 可從中下載 on-demand agent 可執行檔之檔案伺服器位置的 URL。 2 輸入代理程式的下列其他資訊：**名稱**、**參數**、**代理程式 URL 指紋**、**受信任的憑證**以及**代理程式檔案重新整理間隔 (秒)**

下列資訊可協助您瞭解將 on-demand agent 上傳至 Unified Access Gateway 時所提供的設定：

名稱

on-demand agent 可執行檔的名稱。

參數

Horizon Client 用來在端點上執行 on-demand agent 的命令列參數。

對於可在**參數**文字方塊中使用的命令列參數，請參閱相關的 OPSWAT 說明文件。

代理程式 URL 指紋

輸入代理程式 URL 指紋的清單。如果未提供指紋的清單，請確保伺服器憑證是由信任的 CA 核發。輸入十六進位的指紋數字。例如，sha1= C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3。

受信任的憑證

如果代理程式 URL 伺服器憑證不是由受信任的公用 CA 所核發，您可以在向代理程式 URL 通訊以下載 OPSWAT 代理程式時，指定使用由 Unified Access Gateway 信任的憑證 (PEM 格式)。這是代理程式 URL 指紋的替代方法。

若要選取 PEM 格式的憑證並新增至信任存放區，請按一下 **+**。若要從信任存放區移除憑證，請按一下 **-**。依預設，別名名稱是 PEM 憑證的檔案名稱。若要提供不同名稱，請編輯別名文字方塊。

代理程式檔案重新整理間隔 (秒)

從 URL 擷取 on-demand agent 可執行檔的定期時間間隔 (以秒為單位)，這是在**代理程式檔案 URL** 文字方塊中指定。

c 按一下**儲存**。

- 對於 macOS 平台，請依照所述內容執行下列步驟。

  a 選取**檔案上傳類型**。

  如果您不想上傳任何檔案，請選取 None。

  b 視選取的檔案上傳類型而定，輸入在 Unified Access Gateway 上傳 on-demand agent 所需的資訊。

選項	程序
本機	1 選取您已從 OPSWAT 下載的 on-demand agent 可執行檔。 2 輸入 on-demand agent 的下列其他資訊：**名稱**和**參數**。 3 在**可執行檔的路徑**文字方塊中，輸入 on-demand agent 可執行檔的位置。
URL 參考	1 在**代理程式檔案 URL** 中，輸入 Unified Access Gateway 可從中下載 on-demand agent 之檔案伺服器位置的 URL。 2 輸入代理程式的下列其他資訊：**名稱**、**參數**、**代理程式 URL 指紋**、**受信任的憑證**以及**代理程式檔案重新整理間隔 (秒)** 3 在**可執行檔的路徑**文字方塊中，輸入 on-demand agent 可執行檔的位置。

下列資訊可協助您瞭解將 on-demand agent 上傳至 Unified Access Gateway 時所提供的設定：

名稱

on-demand agent 可執行檔的名稱。

參數

Horizon Client 用來在端點上執行 on-demand agent 的命令列參數。

對於可在**參數**文字方塊中使用的命令列參數，請參閱相關的 OPSWAT 說明文件。

代理程式 URL 指紋

輸入代理程式 URL 指紋的清單。如果未提供指紋的清單，請確保伺服器憑證是由信任的 CA 核發。輸入十六進位的指紋數字。例如，sha1= C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3。

受信任的憑證

如果代理程式 URL 伺服器憑證不是由受信任的公用 CA 所核發，您可以在向代理程式 URL 通訊以下載 OPSWAT 代理程式時，指定使用由 Unified Access Gateway 信任的憑證 (PEM 格式)。這是代理程式 URL 指紋的替代方法。

若要選取 PEM 格式的憑證並新增至信任存放區，請按一下 **+**。若要從信任存放區移除憑證，請按一下 **-**。依預設，別名名稱是 PEM 憑證的檔案名稱。若要提供不同名稱，請編輯別名文字方塊。

代理程式檔案重新整理間隔

從 URL 擷取 on-demand agent 可執行檔的定期時間間隔 (以秒為單位)，這是在**代理程式檔案 URL** 文字方塊中指定。

可執行檔的路徑

on-demand agent 可執行檔的位置。

對於 macOS 端點，on-demand agent 檔案會以 zip 檔案的形式封裝。可執行檔會出現在 zip 檔案中。Horizon Client 會將該檔案解壓縮，並從此文字方塊中提到的位置在端點上執行該可執行檔。

c 按一下**儲存**。

後續步驟

若要完成下一組工作，請參閱將 OPSWAT 設定為 Horizon 的端點符合性檢查提供者。

關於 OPSWAT MetaAccess on-demand agent

OPSWAT MetaAccess on-demand agent 是 OPSWAT 用戶端。此代理程式可作為執行 OPSWAT MetaAccess persistent agent 的替代方法，安裝在端點上時，該代理程式會持續在端點上執行。因此，on-demand agent 僅會在需要時提供執行代理程式的選項。

OPSWAT MetaAccess 有兩種類型的用戶端：on-demand agent 和 persistent agent。

persistent agent 會由使用者在每個端點上安裝，並在安裝後持續在端點上執行。

如果是 on-demand agent，在使用者驗證成功後，即會從 Unified Access Gateway 自動下載代理程式並由 Horizon Client 執行。

備註 僅在 Horizon Client 沒有與 Unified Access Gateway 上所存在相同版本的 on-demand agent 時，才會進行下載。

管理員可以在 Unified Access Gateway 上傳適用於 Windows 和 macOS 的 on-demand agent 可執行檔。

若要將代理程式上傳至 Unified Access Gateway，請參閱在 Unified Access Gateway 上傳 OPSWAT MetaAccess on-demand agent 軟體。

如需關於 persistent agent 和 on-demand agent 命令的詳細資訊，請參閱相關的 OPSWAT 說明文件。

定期端點符合性檢查的時間間隔

管理員可以設定在經驗證的使用者工作階段期間，針對端點進行定期符合性檢查的時間間隔。定期符合性檢查可確保裝置在整個工作階段期維持合規性。**端點符合性檢查提供者**設定有兩個時間間隔：符合性檢查間隔和符合性檢查快速間隔。

設定**符合性檢查間隔 (分鐘)** 時，當使用者嘗試使用該端點上的 Horizon Client 執行遠端桌面平台或應用程式工作階段時，Unified Access Gateway 會在端點上執行符合性檢查。根據設定的時間間隔，系統會定期檢查端點的符合性。

在初始符合性檢查之後，有時候，端點可能會因多種原因 (例如管理員所做的原則變更) 而變得不合規。儘管符合性評估擱置中，端點可能需要存取權才能執行工作階段。如果裝置狀態為 `Assessment pending` 或 `Endpoint unknown`，則可以使用**符合性檢查快速間隔 (分鐘)**。

同時設定這兩個時間間隔，且如果裝置狀態為 `Assessment pending` 或 `Endpoint unknown`，則 Unified Access Gateway 會先執行符合性檢查快速間隔。端點變得合規後，Unified Access Gateway 會接著執行符合性檢查間隔。

在定期符合性檢查期間，如果發現端點不合規，則會中斷與使用者工作階段的連線。

符合性檢查間隔 (分鐘)

此文字方塊可讓您設定定期時間間隔，讓 Horizon Client 在某個工作階段期間，以該間隔將符合性檢查要求傳送至 Unified Access Gateway。

符合性檢查快速間隔 (分鐘)

此文字方塊可讓您設定定期且頻繁的時間間隔，讓 Horizon Client 在某個工作階段期間，針對處於 `In compliance` 以外狀態的特定端點，以該間隔將符合性檢查要求傳送至 Unified Access Gateway。狀態為 `Assessment pending` 和 `Endpoint unknown`，並且必須設定為 `ALLOW`。

例如，當 on-demand agent 正在評估端點且裝置狀態為 `Assessment pending` 或 `Endpoint unknown` 時，您可以將時間間隔設定為 `1 minute`，以便在工作階段開始時更頻繁地執行符合性檢查。

重要 僅在**符合性檢查間隔 (分鐘)** 的時間間隔已設定，且值並非 `0` 時，才能設定**符合性檢查快速間隔 (分鐘)**。

若要設定端點符合性檢查提供者的時間間隔，請參閱將 OPSWAT 設定為 Horizon 的端點符合性檢查提供者。

部署為 Reverse Proxy

Unified Access Gateway 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。

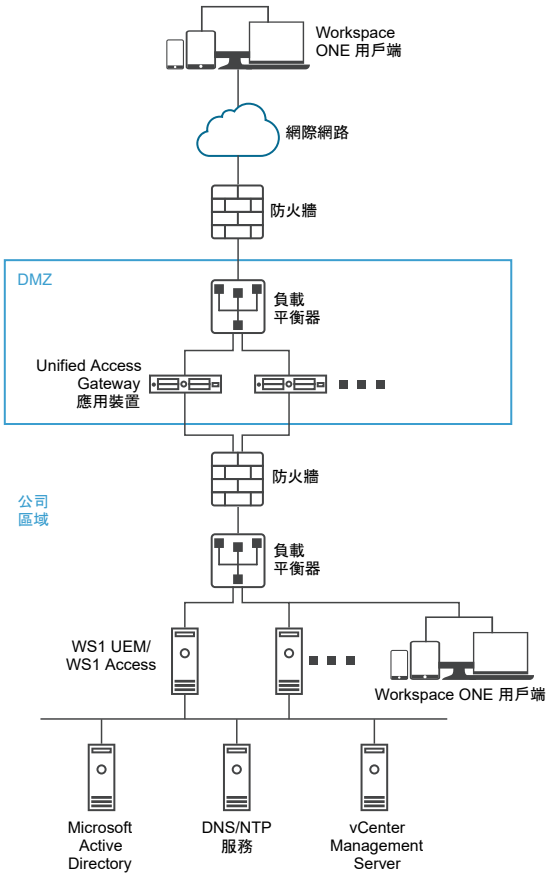
部署案例

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

備註 Unified Access Gateway 的單一執行個體可以同時處理最多 15000 個 TCP 連線。如果預期的負載超過 15000 個，則必須在負載平衡器後方設定 Unified Access Gateway 的多個執行個體。

如需設定 Reverse Proxy 時所用設定的相關資訊，請參閱進階 Edge Service 設定。

圖 4-5. 指向 VMware Identity Manager 的 Unified Access Gateway 應用裝置



瞭解 Reverse Proxy

Unified Access Gateway 提供遠端使用者對應用程式入口網站的存取，以進行單一登入並存取其資源。應用程式入口網站是一種 Unified Access Gateway 作為 Reverse Proxy 的 SharePoint、JIRA 或 VIDM 之類的後端應用程式。

備註 當 Proxy 模式中有重疊時，Horizon Connection Server 無法搭配已啟用的 Web 反向 Proxy 正常運作。因此，如果在相同的 Unified Access Gateway 執行個體上使用 Proxy 模式同時設定並啟用了 Horizon 和 Web 反向 Proxy 執行個體，請從 Horizon 設定中移除 Proxy 模式「/」，並保留 Web 反向 Proxy 中的模式以防止重疊。保留 Web 反向 Proxy 執行個體中的「/」Proxy 模式可確保使用者在按一下 Unified Access Gateway 的 URL 時會顯示正確的 Web 反向 Proxy 頁面。如果僅設定了 Horizon 設定，則不需要進行前述變更。

啟用和設定 Reverse Proxy 時，請注意下列幾點：

- 您必須在 Edge Service 管理員上啟用 Reverse Proxy 的驗證。目前支援 RSA SecurID 和 RADIUS 驗證方法。
- 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 (IDP 中繼資料)。
- Unified Access Gateway 能在搭配或未搭配瀏覽器型用戶端驗證的情況下提供 Workspace ONE Access 和 Web 應用程式的遠端存取權，進而啟動 Horizon 桌面平台。

- 您可以設定多個 Reverse Proxy 執行個體，且可刪除每個已設定的執行個體。
- 簡單 Proxy 模式會區分大小寫。頁面連結和 Proxy 模式必須相符。

圖 4-6. 已設定多個 Reverse Proxy

使用 Workspace ONE Access 設定反向 Proxy

您可以設定 Web 反向 Proxy 服務以搭配使用 Unified Access Gateway 和 Workspace ONE Access。

必要條件

請注意，使用 Workspace ONE Access 部署具有下列需求：

- 分割 DNS。主機名稱在外部必須解析為 Unified Access Gateway 的 IP 位址。在內部的 Unified Access Gateway 上，相同的主機名稱必須透過內部 DNS 對應或 Unified Access Gateway 上的主機名稱項目以解析為實際的 Web 伺服器。

  備註 如果您僅使用 Web 反向 Proxy 部署，則不需要設定身分識別橋接。

- Workspace ONE Access 服務必須以完整網域名稱 (FQDN) 作為主機名稱。
- Unified Access Gateway 必須使用內部 DNS。這表示 Proxy 目的地 URL 必須使用 FQDN。
- 如果 Unified Access Gateway 執行個體中有多個反向 Proxy 設定，則 Web 反向 Proxy 執行個體的 Proxy 模式和 Proxy 主機模式的組合必須是唯一的。
- 所有已設定反向 Proxy 的主機名稱必須解析為 Unified Access Gateway 執行個體之 IP 位址相同的 IP 位址。
- 如需進階 Edge Service 設定的相關資訊，請參閱進階 Edge Service 設定。

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 服務設定**中，按一下**顯示**。
3. 按一下 **Reverse Proxy 設定**齒輪圖示。
4. 在**反向 Proxy 設定**頁面中，按一下**新增**。
5. 在**啟用反向 Proxy 設定**區段，將**否**變更為**是**以啟用反向 Proxy。

6 設定下列 Edge Service 設定。

選項	說明
識別碼	Edge Service 識別碼會設定為 Web 反向 Proxy。
執行個體 ID	用來從所有其他 Web Reverse Proxy 執行個體中識別和區分某個 Web Reverse Proxy 執行個體的唯一名稱。
Proxy 目的地 URL	輸入 Web 應用程式的位址，這通常是後端 URL。例如，對於 Workspace ONE Access，在用戶端電腦上新增 IP 位址、Workspace ONE Access 主機名稱和外部 DNS。在管理員 UI 中，新增 IP 位址、Workspace ONE Access 主機名稱和內部 DNS。
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。如果您指定 *****，則系統會接受任何憑證。指紋的格式為 *[alg=]xx:xx*，其中 *alg* 可以是預設值 `sha1` 或 **md5**。*xx* 為十六進位數字。「:」分隔符號可以是空格，或不使用。系統會忽略指紋中的大小寫。例如： **sha1=B6 77 DC 9C 19 94 2E F1 78 F0 AD 4B EC 85 D1 7A F8 8B DC 34** **sha256=ad:5c:f1:48:47:94:7e:80:82:73:13:6c:83:52:be:78:ed:ff:50:23:56:a8:42:8a:d9:30:fc:3a:33:d6:c6:db** 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(.*))**。 **備註** 當您設定多個反向 Proxy 時，請在 Proxy 主機模式中提供主機名稱。

7 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 Unified Access Gateway 中設定的驗證方法會在下拉式功能表中列出。支援 RSA SecurID、RADIUS，以及裝置憑證驗證方法。
健全狀況檢查 URI 路徑	Unified Access Gateway 會連線至此 URI 路徑，以檢查您 Web 應用程式的健全狀況。
SAML SP	當您將 Unified Access Gateway 設定為 Workspace ONE Access 的已驗證反向 Proxy 時需要使用此選項。輸入 View XML API 代理之 SAML 服務提供者的名稱。此名稱必須符合使用 Unified Access Gateway 設定之服務提供者的名稱，或為特殊值 **DEMO**。如果使用 Unified Access Gateway 設定多個服務提供者，則其名稱必須是唯一的。
外部 URL	預設值為 Unified Access Gateway 主機 URL，連接埠 443。您可以輸入其他外部 URL。輸入為 `https://<host:port>`.

選項	說明
未受保護的模式	輸入已知的 Workspace ONE Access 重新導向模式。例如： `(/|/catalog-portal(.*)|/|/SAAS/|/SAAS|/SAAS/API/1.0/GET/image(.*)|/SAAS/horizon/css(.*)|/SAAS/horizon/angular(.*)|/SAAS/horizon/js(.*)|/SAAS/horizon/js-lib(.*)|/SAAS/auth/login(.*)|/SAAS/jersey/manager/api/branding|/SAAS/horizon/images/(.*)|/SAAS/jersey/manager/api/images/(.*)|/hc/(.*)/authenticate/(.*)|/hc/static/(.*)|/SAAS/auth/saml/response|/SAAS/auth/authenticatedUserDispatcher|/web(.*)|/SAAS/apps/|/SAAS/horizon/portal/(.*)|/SAAS/horizon/fonts(.*)|/SAAS/API/1.0/POST/sso(.*)|/SAAS/API/1.0/REST/system/info(.*)|/SAAS/API/1.0/REST/auth/cert(.*)|/SAAS/API/1.0/REST/oauth2/activate(.*)|/SAAS/API/1.0/GET/user/devices/register(.*)|/SAAS/API/1.0/oauth2/token(.*)|/SAAS/API/1.0/REST/oauth2/session(.*)|/SAAS/API/1.0/REST/user/resources(.*)|/hc/t/(.*)/(.*)/authenticate(.*)|/SAAS/API/1.0/REST/auth/logout(.*)|/SAAS/auth/saml/response(.*)|/SAAS/(.*)/(.*)auth/login(.*)|/SAAS/API/1.0/GET/apps/launch(.*)|/SAAS/API/1.0/REST/user/applications(.*)|/SAAS/auth/federation/sso(.*)|/SAAS/auth/oauth2/authorize(.*)|/hc/prepareSaml/failure(.*)|/SAAS/auth/oauthtoken(.*)|/SAAS/API/1.0/GET/metadata/idp.xml|/SAAS/auth/saml/artifact/resolve(.*)|/hc/(.*)/authAdapter(.*)|/hc/authenticate/(.*)|/SAAS/auth/logout|/SAAS/common.js|/SAAS/auth/launchInput(.*)|/SAAS/launchUsersApplication.do(.*)|/hc/API/1.0/REST/thinapp/download(.*)|/hc/t/(.*)/(.*)/logout(.*)|/SAAS/auth/wsfed/services(.*)|/SAAS/auth/wsfed/active/logon(.*))`
驗證 Cookie	輸入驗證 Cookie 名稱。例如：**`HZN`**
登入重新導向 URL	如果使用者從入口網站登出，請輸入重新導向 URL 以重新登入。例如：**`/SAAS/auth/login?dest=%s`**
Proxy 主機模式	外部主機名稱，用來檢查傳入主機以查看它是否符合該執行個體的模式。設定 Web 反向 Proxy 執行個體時，主機模式為選用。
受信任的憑證	■ 若要選取 PEM 格式的憑證並新增至信任存放區，請按一下 **+**。 ■ 若要提供不同名稱，請編輯別名文字方塊。 依預設，別名名稱是 PEM 憑證的檔案名稱。 ■ 若要從信任存放區移除憑證，請按一下 **-**。
回應安全性標頭	按一下「+」可新增標頭。輸入安全性標頭的名稱。輸入值。按一下「-」可移除標頭。編輯現有的安全性標頭，以更新標頭的名稱和值。 **重要** 在您按一下**儲存**後，才會儲存標頭名稱和值。依預設會顯示部分標準安全性標頭。僅在已設定後端伺服器的回應中沒有對應的標頭存在時，才會將已設定標頭新增至用戶端的 Unified Access Gateway 回應。 **備註** 請謹慎修改安全性回應標頭。修改這些參數可能會影響到 Unified Access Gateway 的安全運作。
主機項目	輸入要在 `/etc/hosts` 檔案中新增的詳細資料。每個項目依序應包括一個 IP、一個主機名稱和一個選用的主機名稱別名 (以空格區隔)。例如，**`10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`**。按一下「+」符號可新增多個主機項目。 **重要** 只有在按一下**儲存**後，才會儲存主機項目。

備註 僅在使用 Workspace ONE Access 時才適用 `UnSecure Pattern`、`Auth Cookie` 和 `Login Redirect URL` 選項。此處提供的值也適用於 Access Point 2.8 和 Unified Access Gateway 2.9。

備註 「驗證 Cookie」和「未受保護的模式」內容對驗證反向 Proxy 而言無效。您必須使用 `Auth Methods` 內容來定義驗證方法。

8 按一下**儲存**。

後續步驟

若要啟用身分識別橋接，請參閱設定身分識別橋接設定。

使用 VMware Workspace ONE UEM API 設定反向 Proxy

在使用 Workspace ONE UEM 的內部部署安裝時，通常會將 API 伺服器安裝在沒有傳入網際網路存取的防火牆後方。若要安全地使用 Workspace ONE Intelligence 自動化功能，您可以將 Unified Access Gateway 內部的 Web 反向 Proxy Edge 服務設定為只允許存取 API 服務，以便可以對裝置、使用者和其他資源採取動作。

必要條件

- UEM API 服務必須以完整網域名稱 (FQDN) 作為主機名稱。
- Unified Access Gateway 必須使用內部 DNS。這表示 Proxy 目的地 URL 必須使用 FQDN。
- 如果 Unified Access Gateway 執行個體中有多個反向 Proxy 設定，則 Web 反向 Proxy 執行個體的 Proxy 模式和 Proxy 主機模式的組合必須是唯一的。
- 所有已設定反向 Proxy 的主機名稱應解析為與 Unified Access Gateway 執行個體的 IP 位址相同的 IP 位址。
- 如需進階 Edge 服務設定的詳細資訊，請參閱進階 Edge Service 設定。

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 服務設定**中，按一下**顯示**。

3 按一下 **Reverse Proxy 設定**齒輪圖示。

4 在 [反向 Proxy 設定] 頁面中，按一下**新增**。

5 在 [啟用反向 Proxy 設定] 區段，將**否**變更為**是**以啟用反向 Proxy。

6 設定下列 Edge Service 設定。

選項	說明
識別碼	Edge Service 識別碼會設定為 Web 反向 Proxy。
執行個體 ID	用來從所有其他 Web Reverse Proxy 執行個體中識別和區分某個 Web Reverse Proxy 執行個體的唯一名稱。

選項	說明
Proxy 目的地 URL	輸入 Web 應用程式的位址，這通常是後端 URL。例如，對於 Workspace ONE UEM API 伺服器，這可能是與主控台登入不同的 URL/IP 位址。您可以在 UEM 設定頁面的**設定 > 系統 > 進階 > API > REST API > REST API URL** 下進行檢查，來確認此值。
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。如果您指定 *****，則系統會接受任何憑證。指紋的格式為 *[alg=]xx:xx*，其中 *alg* 可以是預設值 `sha1` 或 **md5**。*xx* 為十六進位數字。「:」分隔符號可以是空格，或不使用。系統會忽略指紋中的大小寫。例如： **`sha1=B6 77 DC 9C 19 94 2E F1 78 F0 AD 4B EC 85 D1 7A F8 8B DC 34`** **`sha256=ad:5c:f1:48:47:94:7e:80:82:73:13:6c:83:52:be:78:ed:ff:50:23:56:a8:42:8a:d9:30:fc:3a:33:d6:c6:db`** 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。對於 Workspace ONE UEM API，請使用：`(/API(.*)|/api(.*)|/Api(.*)|)`。 **備註** 當您設定多個反向 Proxy 時，請在 Proxy 主機模式中提供主機名稱。

7 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 Unified Access Gateway 中設定的驗證方法會在下拉式功能表中列出。支援 RSA SecurID、RADIUS，以及裝置憑證驗證方法。
外部 URL	預設值為 Unified Access Gateway 主機 URL，連接埠 443。您可以輸入其他外部 URL。輸入為 `https://<host:port>`. **備註** 使用位於負載平衡器後方的 Unified Access Gateway 時，請在此欄位中輸入負載平衡器 URL。
Proxy 主機模式	外部主機名稱，用來檢查傳入主機以查看它是否符合該特定執行個體的模式。設定 Web 反向 Proxy 執行個體時，主機模式為選用。
受信任的憑證	■ 若要選取 PEM 格式的憑證並新增至信任存放區，請按一下 **+**。 ■ 若要提供不同名稱，請編輯別名文字方塊。 依預設，別名名稱是 PEM 憑證的檔案名稱。 ■ 若要從信任存放區移除憑證，請按一下 **-**。
主機項目	輸入要在 `/etc/hosts` 檔案中新增的詳細資料。每個項目依序應包括一個 IP、一個主機名稱和一個選用的主機名稱別名 (以空格區隔)。例如，**`10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`**。按一下「+」符號可新增多個主機項目。 **重要** 只有在按一下**儲存**後，才會儲存主機項目。

8 按一下**儲存**。

後續步驟

若要將 Workspace UEM API Connector 設定為與 Workspace ONE Intelligence 搭配使用，請參閱《Workspace ONE Intelligence》說明文件中的〈開始使用自動化〉主題。使用為您 Unified Access Gateway 而非 UEM REST API 內部伺服器 URL 設定的外部 URL。

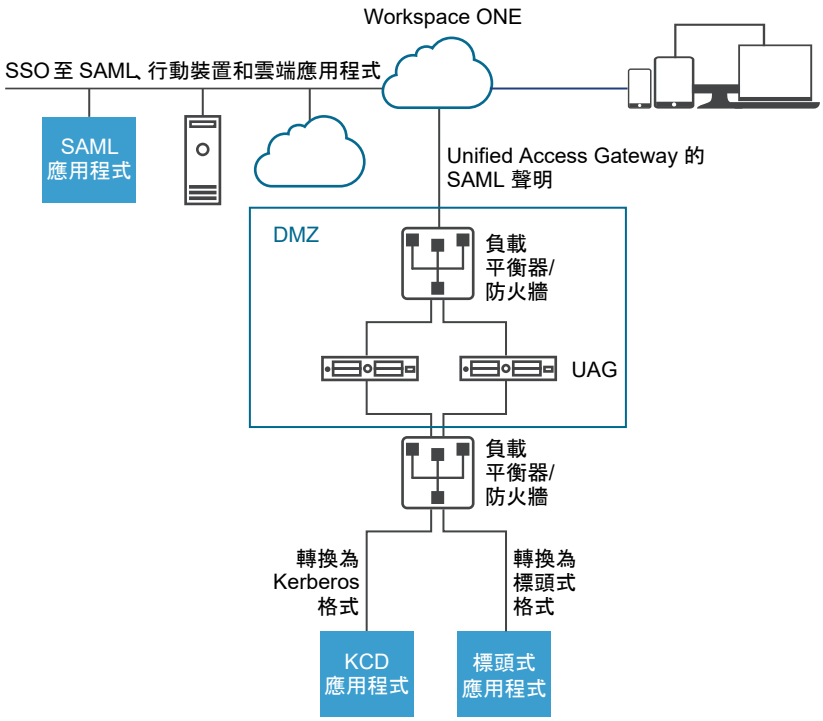
單一登入存取內部部署舊版 Web 應用程式的部署

可以設定 Unified Access Gateway 身分識別橋接功能，以便為使用 Kerberos 限制委派 (KCD) 或標頭式驗證的舊版 Web 應用程式提供單一登入 (SSO)。

身分識別橋接模式中的 Unified Access Gateway 會作為將使用者驗證傳遞至所設定舊版應用程式的服務提供者。Workspace ONE Access 則作為身分識別提供者，並提供進入 SAML 應用程式的 SSO。當使用者存取需要 KCD 或標頭式驗證的舊版應用程式時，Workspace ONE Access 會驗證使用者。具有使用者資訊的 SAML 聲明會傳送至 Unified Access Gateway。Unified Access Gateway 會使用此驗證以允許使用者存取應用程式。

備註 當 Proxy 模式中有重疊時，Horizon Connection Server 無法搭配已啟用的 Web 反向 Proxy 正常運作。因此，如果在相同的 Unified Access Gateway 執行個體上使用 Proxy 模式同時設定並啟用了 Horizon 和 Web 反向 Proxy 執行個體，請從 Horizon 設定中移除 Proxy 模式「/」，並保留 Web 反向 Proxy 中的模式以防止重疊。保留 Web 反向 Proxy 執行個體中的「/」Proxy 模式可確保使用者在按一下 Unified Access Gateway 的 URL 時會顯示正確的 Web 反向 Proxy 頁面。如果僅設定了 Horizon 設定，則不需要進行前述變更。

圖 4-7. Unified Access Gateway 身分識別橋接模式



身分識別橋接部署案例

可以設定 Unified Access Gateway 身分識別橋接模式以在雲端或內部部署環境中與 VMware Workspace® ONE® 搭配使用。

在雲端中使用 Unified Access Gateway 身分識別橋接搭配 Workspace ONE 用戶端

可以設定身分識別橋接模式，以在雲端中與 Workspace ONE 搭配使用來驗證使用者。當使用者要求存取舊版 Web 應用程式時，身分識別提供者會套用適當的驗證和授權原則。

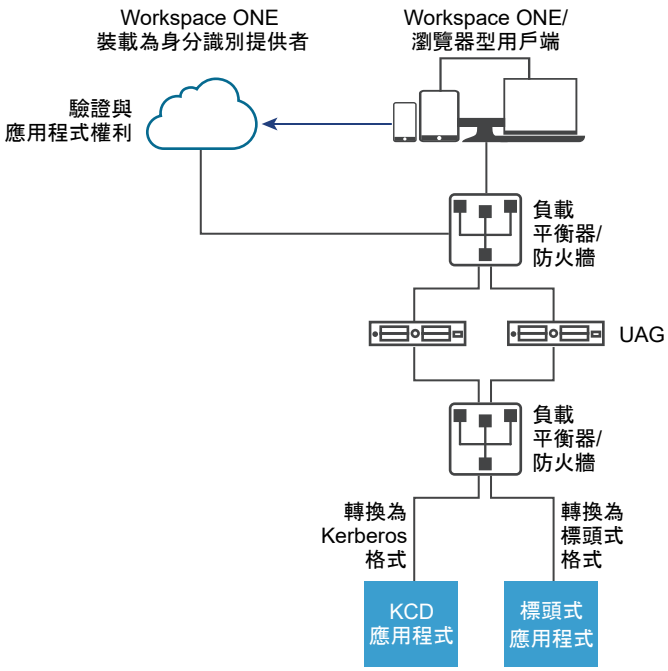
如果使用者通過驗證，則身分識別提供者會建立 SAML Token，並將它傳送給使用者。使用者會將 SAML Token 傳遞至 DMZ 中的 Unified Access Gateway。Unified Access Gateway 會驗證 SAML Token，並從 Token 擷取使用者主體名稱。

如果要求是針對 Kerberos 驗證，則會使用 Kerberos 限制委派來與 Active Directory 伺服器交涉。Unified Access Gateway 會模擬使用者來擷取 Kerberos Token 以使用應用程式進行驗證。

如果要求是針對標頭式驗證，則會將使用者標頭名稱傳送至網頁伺服器以要求使用應用程式進行驗證。

應用程式會將回應傳送回 Unified Access Gateway。回應會傳回給使用者。

圖 4-8. 雲端中的 Unified Access Gateway 身分識別橋接搭配 Workspace ONE



在內部部署使用身分識別橋接搭配 Workspace ONE 用戶端

將身分識別橋接模式設定為在內部部署環境中使用 Workspace ONE 驗證使用者時，使用者會輸入用來透過 Unified Access Gateway Proxy 存取內部部署舊版 Web 應用程式的 URL。Unified Access Gateway 會將要求重新導向至身分識別提供者以進行驗證。身分識別提供者會對要求套用驗證和授權原則。如果使用者通過驗證，則身分識別提供者會建立 SAML Token，並將 Token 傳送給使用者。

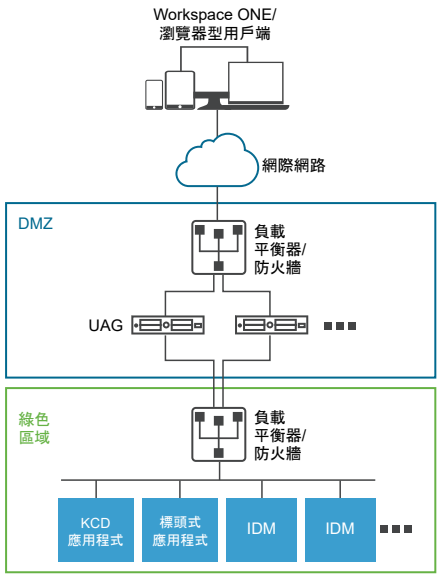
使用者會將 SAML Token 傳遞至 Unified Access Gateway。Unified Access Gateway 會驗證 SAML Token，並從 Token 擷取使用者主體名稱。

如果要求是針對 Kerberos 驗證，則會使用 Kerberos 限制委派來與 Active Directory 伺服器交涉。Unified Access Gateway 會模擬使用者來擷取 Kerberos Token 以使用應用程式進行驗證。

如果要求是針對標頭式驗證，則會將使用者標頭名稱傳送至網頁伺服器以要求使用應用程式進行驗證。

應用程式會將回應傳送回 Unified Access Gateway。回應會傳回給使用者。

圖 4-9. Unified Access Gateway 身分識別橋接內部部署



搭配使用身分識別橋接與對 Kerberos 的憑證

您可以設定身分識別橋接，以便為使用憑證驗證的內部部署舊版非 SAML 應用程式提供單一登入 (SSO)。請參閱針對身分識別橋接設定 Web Reverse Proxy (對 Kerberos 的憑證)。

設定身分識別橋接設定

在後端應用程式中設定了 Kerberos 時，若要在 Unified Access Gateway 中設定身分識別橋接，您需要上傳身分識別提供者中繼資料和 Keytab 檔案，並設定 KCD 領域設定。

備註 此版本的身分識別橋接可用單一網域設定支援跨網域。這表示使用者和 SPN 帳戶可以位於不同的網域。

當身分識別橋接啟用了標頭式驗證時，則不需要 Keytab 設定和 KCD 領域設定。

設定身分識別橋接設定使用 Kerberos 驗證之前，請確定下列項目可供使用。

- 已設定身分識別提供者，且已儲存身分識別提供者的 SAML 中繼資料。SAML 中繼資料檔案會上傳至 Unified Access Gateway (僅適用於 SAML 案例)。
- 針對 Kerberos 驗證，一部已啟用 Kerberos 的伺服器，且包含用於識別所要使用金鑰發佈中心的領域名稱。
- 針對 Kerberos 驗證，將 Kerberos Keytab 檔案上傳至 Unified Access Gateway。Keytab 檔案包括 Active Directory 服務帳戶的認證，該帳戶已設定來代表網域中的任何使用者針對指定的後端服務來取得 Kerberos 票證。
- 確保已開啟下列連接埠：
  - 用於傳入 HTTP 要求的連接埠 443
  - 用於與 Active Directory 進行 Kerberos 通訊的 TCP/UDP 連接埠 88

- Unified Access Gateway 使用 TCP 來與後端應用程式通訊。後端接聽所在的適當連接埠，例如 TCP 連接埠 8080。

備註

- 不支援為相同 Unified Access Gateway 執行個體上兩個不同 Reverse Proxy 執行個體同時進行身分識別橋接的 SAML 和對 Kerberos 的憑證設定。
- 不支援在相同應用裝置上未啟用身分識別橋接，且具有憑證授權機構但無憑證式驗證的 Web Reverse Proxy 執行個體。

使用 SAML 的標頭式驗證

從 IDP 到 SP (如果使用身分識別橋接，則為 Unified Access Gateway) 的 SAML 回應包含具有 SAML 屬性的 SAML 判斷提示。SAML 屬性可在 IDP 中設定為指向不同的參數，例如使用者名稱和電子郵件等。

在使用 SAML 的標頭式驗證中，SAML 屬性的值可作為 HTTP 標頭傳送至後端代理目的地。定義於 Unified Access Gateway 中的 SAML 屬性名稱與 IDP 中的名稱相同。例如，如果身分識別提供者將此屬性定義為 `Name: userNameValue: idmadmin`，則 Unified Access Gateway 中的 SAML 屬性名稱必須定義為 `"userName"`。

系統會忽略與 IDP 中所定義屬性不相符的 SAML 屬性。Unified Access Gateway 支援多個 SAML 屬性和多重值的 SAML 屬性。以下將針對各個案例，提供身分識別提供者預期會傳回的 SAML 判斷提示範例節錄。例如，

1. 預期 IDP 針對多個 SAML 屬性傳回的 SAML 回應

```
<saml:AttributeStatement>
      <saml:Attribute Name="userName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                  <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">idmadmin</
saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="userEmail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">63ecfabf-
a577-46c3-b4fa-caf7ae49a6a3</saml:AttributeValue>
      </saml:Attribute>
</saml:AttributeStatement>
```

在上述範例中，判斷提示包含兩個屬性，即 `"userName"` 和 `"userEmail"`。如果僅為 `"userName"` 設定了標頭式驗證，且標頭名稱為 `"HTTP_USER_NAME"`，則傳送的標頭為 `"HTTP_USER_NAME: idmadmin"`。由於未在 Unified Access Gateway 上設定用於標頭式驗證的 `"userEmail"`，因此不會將其作為標頭傳送。

2. 預期 IDP 針對多重值 SAML 屬性傳回的 SAML 回應

```
<saml:AttributeStatement>
      <saml:Attribute Name="group" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
            <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All Employees</
```

```
saml:AttributeValue>
             <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All Contractors</
saml:AttributeValue>
             <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All Executives</
saml:AttributeValue>
             <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All</
saml:AttributeValue>
     </saml:Attribute>
</saml:AttributeStatement>
```

在上述範例中，屬性 `"group"` 包含四個值，即 `"All Employees"`、`"All Contractors"`、`"All Executives"` 和 `"All"`。如果僅為 `"group"` 設定了標頭式驗證，且標頭名稱為 `"HTTP_GROUP"`，則傳送的標頭為 `"HTTP_GROUP: All Employees, All Contractors, All Executives, All"`，並以所有屬性值的逗號分隔清單作為標頭值。

設定領域設定

設定網域領域名稱、領域的金鑰發佈中心和 KDC 逾時。

領域是負責維護驗證資料的管理實體的名稱。為 Kerberos 驗證領域選取描述性的名稱非常重要。設定領域，也稱為網域名稱，以及 Unified Access Gateway 中對應的 KDC 服務。當 UPN 要求進入特定領域時，Unified Access Gateway 會在內部解析 KDC 以使用 Kerberos 提供的票證。

慣例是以大寫字母輸入相同的領域名稱與網域名稱。例如，領域名稱為 EXAMPLE.NET。Kerberos 用戶端會使用領域名稱來產生 DNS 名稱。

從 Unified Access Gateway 3.0 版開始，您可以刪除先前定義的領域。

重要 如果是跨網域設定，請新增所有領域的詳細資料，包括主要網域及次要網域或子網域和相關聯的 KDC 資訊。請確定領域之間有信任關係。

必要條件

一部已啟用 Kerberos 的伺服器，且包含用於識別所要使用金鑰發佈中心的領域名稱。

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 > 身分識別橋接設定**區段中，選取**領域設定**齒輪圖示。
3. 按一下**新增**。
4. 填妥表單。

標籤	說明
領域的名稱	使用網域名稱輸入領域。以大寫字母輸入領域。領域必須符合 Active Directory 中設定的網域名稱。
金鑰發佈中心	輸入領域的 KDC 伺服器。如果要新增一部以上伺服器，請以逗號區隔清單。
KDC 逾時 (以秒為單位)	輸入要等候 KDC 回應的時間。預設為 3 秒。

5 按一下**儲存**。

後續步驟

設定 Keytab 設定。

上傳 Keytab 設定

Keytab 是一個檔案，其中包含 Kerberos 主體和加密金鑰的配對。系統會針對需要單一登入的應用程式建立一個 Keytab 檔案。Unified Access Gateway 身分識別橋接會使用 Keytab 檔案來使用 Kerberos 向遠端系統進行驗證，而無需輸入密碼。

當使用者從身分識別提供者經過驗證進入 Unified Access Gateway 時，Unified Access Gateway 會從 Kerberos 網域控制站要求 Kerberos 票證以驗證使用者。

Unified Access Gateway 會使用 Keytab 檔案來模擬使用者，以向內部 Active Directory 網域進行驗證。Unified Access Gateway 必須在 Active Directory 網域上具有網域使用者服務帳戶。Unified Access Gateway 不會直接加入網域。

備註 如果管理員為某個服務帳戶重新產生 Keytab 檔案，則必須再次將 Keytab 檔案上傳至 Unified Access Gateway。

您也可以使用命令列來產生 Keytab 檔案。例如：

```
ktpass /princ HOST/username@domain.com /ptype KRB5_NT_PRINCIPAL /pass * /out
C:\Temp\kerberos.keytab /mapuser uagkerberos /crypto All
```

如需 `ktpass` 命令的詳細資訊，請參閱 Microsoft 說明文件。

必要條件

您必須可存取 Kerberos Keytab 檔案，才能上傳至 Unified Access Gateway。Keytab 檔案為二進位檔案。若可能，請使用 SCP 或其他安全方法在電腦之間傳輸 Keytab。

程序

1 在 [管理應用裝置組態範本] 區段中，按一下**新增**。

2 在 [身分識別橋接設定] 區段中，按一下**設定**。

3 在 [Kerberos Keytab 設定] 頁面中，按一下**新增 Keytab**。

4 輸入唯一名稱作為識別碼。

5 (選用) 在**主體名稱**文字方塊中輸入 Kerberos 主體名稱。

每個主體一律使用完整領域名稱。領域應該使用大寫字母。

確保此處輸入的主體名稱為在 Keytab 檔案中找到的第一個主體。如果相同的主體名稱未在上傳的 Keytab 檔案中，則 Keytab 上傳會失敗。

6 在**選取 Keytab 檔案**文字方塊中，按一下**選取**，並瀏覽至您儲存的 Keytab 檔案。按一下**開啟**。

如果您未輸入主體名稱，則會使用在 Keytab 中找到的第一個主體。您可以將多個 Keytab 合併成一個檔案。

7 按一下**儲存**。

針對身分識別橋接設定 Web Reverse Proxy (對 Kerberos 的 SAML)

若要針對身分識別橋接設定 Web Reverse Proxy (對 Kerberos 的 SAML)，您必須已將身分識別提供者中繼資料檔案儲存至 Unified Access Gateway。

然後，您可以在管理主控台上啟用身分識別橋接，並設定服務的外部主機名稱。

上傳身分識別提供者中繼資料

若要設定身分識別橋接功能，您必須將身分識別提供者的 SAML 憑證中繼資料 XML 檔案上傳至 Unified Access Gateway。

必要條件

SAML 中繼資料 XML 檔案必須儲存至您可以存取的電腦。

如果您使用 VMware Workspace ONE Access 作為身分識別提供者，請從 Workspace ONE Access 管理主控台的**目錄 > 設定 SAML 中繼資料 > 身分識別提供者 (IdP)** 中繼資料連結下載並儲存 SAML 中繼資料檔案。

程序

1 在管理主控台的**手動設定**下方，按一下**選取**。

2 在**進階設定 > 身分識別橋接設定**區段中，選取**上傳身分識別提供者中繼資料**齒輪圖示。

3 在**實體 ID** 文字方塊中輸入身分識別提供者的實體 ID。

如果未在 [實體 ID] 文字方塊中輸入值，則系統會剖析中繼資料檔案中的身分識別提供者名稱，並用作身分識別提供者的實體 ID。

4 在 **IDP 中繼資料**區段中，按一下**選取**，並瀏覽至您儲存的中繼資料檔案。按一下**開啟**。

5 按一下**儲存**。

後續步驟

針對 KDC 驗證，設定領域設定和 Keytab 設定。

針對標頭式驗證，當您設定身分識別橋接功能時，請以包含使用者 ID 之 HTTP 標頭的名稱來填入 [使用者標頭名稱] 選項。

針對身分識別橋接設定 Web 反向 Proxy (對 Kerberos 的 SAML)

啟用身分識別橋接，設定服務的外部主機名稱，並下載 Unified Access Gateway 服務提供者中繼資料檔案。

此中繼資料檔案會上傳至 VMware Workspace ONE Access 服務中的 Web 應用程式組態頁面。

必要條件

您必須已在 Unified Access Gateway 管理主控台上設定下列身分識別橋接設定。您可以在**進階設定**區段下找到這些設定。

- 身分識別提供者中繼資料已上傳至 Unified Access Gateway。
- 已設定 Kerberos 主體名稱，並已將 Keytab 檔案上傳至 Unified Access Gateway。
- 領域名稱和金鑰發佈中心資訊。

請確保 TCP/UDP 連接埠 88 已開啟，因為 Unified Access Gateway 使用此連接埠來與 Active Directory 進行 Kerberos 通訊。

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 **反向 Proxy 設定**頁面中按一下**新增**，以建立 Proxy 設定。

5 將**啟用反向 Proxy 設定**設為 [是]，並設定下列 Edge Service 設定。

選項	說明
識別碼	Edge Service 識別碼會設定為 Web 反向 Proxy。
執行個體 ID	Web 反向 Proxy 執行個體的唯一名稱。
Proxy 目的地 URL	指定 Web 應用程式的內部 URI。Unified Access Gateway 必須可以解析和存取此 URL。
Proxy 目的地 URL 指紋	輸入 URI 以符合此 Proxy 設定。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(.*))`**。 注意：當您設定多個反向 Proxy 時，請在 Proxy 主機模式中提供主機名稱

6 若要設定其他進階設定，請按一下**較多**。

選項	說明
驗證方法	預設會使用使用者名稱和密碼的傳遞驗證。您在 Unified Access Gateway 中設定的驗證方法會在下拉式功能表中列出。支援 RSA SecurID、RADIUS，以及裝置憑證驗證方法。
健全狀況檢查 URI 路徑	Unified Access Gateway 會連線至此 URI 路徑，以檢查您 Web 應用程式的健全狀況。

選項	說明
SAML SP	當您將 Unified Access Gateway 設定為 Workspace ONE Access 的已驗證反向 Proxy 時需要使用此選項。輸入 View XML API 代理之 SAML 服務提供者的名稱。此名稱必須符合使用 Unified Access Gateway 設定之服務提供者的名稱，或為特殊值 **DEMO**。如果使用 Unified Access Gateway 設定多個服務提供者，則其名稱必須是唯一的。
外部 URL	預設值為 Unified Access Gateway 主機 URL，連接埠 443。您可以輸入其他外部 URL。輸入為 `https://<host:port>`.
未受保護的模式	輸入已知的 Workspace ONE Access 重新導向模式。例如： `(/|/catalog-portal(.*)|/|/SAAS/|/SAAS|/SAAS/API/1.0/GET/image(.*)|/SAAS/horizon/css(.*)|/SAAS/horizon/angular(.*)|/SAAS/horizon/js(.*)|/SAAS/horizon/js-lib(.*)|/SAAS/auth/login(.*)|/SAAS/jersey/manager/api/branding|/SAAS/horizon/images/(.*)|/SAAS/jersey/manager/api/images/(.*)|/hc/(.*)/authenticate/(.*)|/hc/static/(.*)|/SAAS/auth/saml/response|/SAAS/auth/authenticatedUserDispatcher|/web(.*)|/SAAS/apps/|/SAAS/horizon/portal/(.*)|/SAAS/horizon/fonts(.*)|/SAAS/API/1.0/POST/sso(.*)|/SAAS/API/1.0/REST/system/info(.*)|/SAAS/API/1.0/REST/auth/cert(.*)|/SAAS/API/1.0/REST/oauth2/activate(.*)|/SAAS/API/1.0/GET/user/devices/register(.*)|/SAAS/API/1.0/oauth2/token(.*)|/SAAS/API/1.0/REST/oauth2/session(.*)|/SAAS/API/1.0/REST/user/resources(.*)|/hc/t/(.*)/(.*)/authenticate(.*)|/SAAS/API/1.0/REST/auth/logout(.*)|/SAAS/auth/saml/response(.*)|/SAAS/(.*)/(.*)auth/login(.*)|/SAAS/API/1.0/GET/apps/launch(.*)|/SAAS/API/1.0/REST/user/applications(.*)|/SAAS/auth/federation/sso(.*)|/SAAS/auth/oauth2/authorize(.*)|/hc/prepareSaml/failure(.*)|/SAAS/auth/oauthtoken(.*)|/SAAS/API/1.0/GET/metadata/idp.xml|/SAAS/auth/saml/artifact/resolve(.*)|/hc/(.*)/authAdapter(.*)|/hc/authenticate/(.*)|/SAAS/auth/logout|/SAAS/common.js|/SAAS/auth/launchInput(.*)|/SAAS/launchUsersApplication.do(.*)|/hc/API/1.0/REST/thinapp/download(.*)|/hc/t/(.*)/(.*)/logout(.*)|/SAAS/auth/wsfed/services(.*)|/SAAS/auth/wsfed/active/logon(.*))`
驗證 Cookie	輸入驗證 Cookie 名稱。例如：**HZN**
登入重新導向 URL	如果使用者從入口網站登出，請輸入重新導向 URL 以重新登入。例如：**/SAAS/auth/login?dest=%s**
Proxy 主機模式	外部主機名稱，用來檢查傳入主機以查看它是否符合該執行個體的模式。設定 Web 反向 Proxy 執行個體時，主機模式為選用。
受信任的憑證	■ 若要選取 PEM 格式的憑證並新增至信任存放區，請按一下 **+**。 ■ 若要提供不同名稱，請編輯別名文字方塊。 依預設，別名名稱是 PEM 憑證的檔案名稱。 ■ 若要從信任存放區移除憑證，請按一下 **-**。

選項	說明
回應安全性標頭	按一下「+」可新增標頭。輸入安全性標頭的名稱。輸入值。按一下「-」可移除標頭。編輯現有的安全性標頭，以更新標頭的名稱和值。 **重要** 在您按一下**儲存**後，才會儲存標頭名稱和值。依預設會顯示部分標準安全性標頭。僅在已設定後端伺服器的回應中沒有對應的標頭存在時，才會將已設定標頭新增至用戶端的 Unified Access Gateway 回應。 **備註** 請謹慎修改安全性回應標頭。修改這些參數可能會影響到 Unified Access Gateway 的安全運作。
主機項目	輸入要在 `/etc/hosts` 檔案中新增的詳細資料。每個項目依序應包括一個 IP、一個主機名稱和一個選用的主機名稱別名 (以空格區隔)。例如，**`10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`**。按一下「+」符號可新增多個主機項目。 **重要** 只有在按一下**儲存**後，才會儲存主機項目。

7 在 [啟用身分識別橋接] 區段中，將**否**變更為**是**。

8 設定下列身分識別橋接設定。

選項	說明
驗證類型	選取 SAML。
SAML 屬性	傳遞作為要求標頭的 SAML 屬性清單。僅在**啟用身分識別橋接**設定為**是**，且**驗證類型**設定為 **SAML** 時，才會顯示此選項。按一下「+」可將 SAML 屬性新增為標頭的一部分。
SAML 對象	請確定已選擇 SAML 驗證類型。 輸入對象 URL。 **備註** 如果文字方塊保持空白，則對象不受限。 若要了解 UAG 支援 SAML 對象的方式，請參閱 SAML 對象。
身分識別提供者	從下拉式功能表選取身分識別提供者。
Keytab	在下拉式功能表中，選取針對此反向 Proxy 設定的 Keytab。
目標服務主體名稱	輸入 Kerberos 服務主體名稱。每個主體一律使用完整領域名稱。例如，**`myco_hostname@MYCOMPANY`**。以大寫字母輸入領域名稱。如果您不新增名稱至文字方塊，則服務主體名稱會衍生自 Proxy 目的地 URL 的主機名稱。
服務登陸頁面	輸入在驗證聲明後將使用者重新導向至身分識別提供者的頁面。預設設定為 `/`。
使用者標頭名稱	針對標頭式驗證，輸入包含衍生自聲明之使用者 ID 的 HTTP 標頭名稱。

9 在 [下載 SP 中繼資料] 區段中，按一下**下載**。

儲存服務提供者中繼資料檔案。

10 按一下**儲存**。

後續步驟

將 Unified Access Gateway 服務提供者中繼資料檔案新增至 Workspace ONE Access 服務中的 Web 應用程式組態頁面。

將中繼資料檔案新增至 VMware Workspace ONE Access 服務

您必須將所下載的 Unified Access Gateway 服務提供者中繼資料檔案上傳至 Workspace ONE Access 服務中的 Web 應用程式組態頁面。

使用的 SSL 憑證必須與多個負載平衡 Unified Access Gateway 伺服器中所使用的憑證相同。

必要條件

您必須已將 Unified Access Gateway 服務提供者中繼資料檔案儲存至電腦。

程序

1 登入 Workspace ONE Access 管理主控台。

2 在 [目錄] 索引標籤中，按一下**新增應用程式**，並選取**建立新的應用程式**。

3 在 [應用程式詳細資料] 頁面的 [名稱] 文字方塊中輸入使用者易記名稱。

4 選取 **SAML 2.0 POST** 驗證設定檔。

您也可以新增此應用程式的說明及圖示，向 Workspace ONE 入口網站中的使用者顯示。

5 按**下一步**，並在 [應用程式組態] 頁面中，向下捲動至**透過下列項目設定**區段。

6 選取 [中繼資料 XML] 選項按鈕並將 Unified Access Gateway 服務提供者中繼資料文字貼入 [中繼資料 XML] 文字方塊內。

7 (選用) 在 [屬性對應] 區段中，將下列屬性名稱對應至使用者設定檔值。FORMAT 欄位值為「基本」。必須以小寫輸入屬性名稱。

名稱	設定的值
upn	userPrincipalName
userid	Active Directory 使用者 ID

8 按一下**儲存**。

後續步驟

授權使用者和群組使用此應用程式。

備註 Unified Access Gateway 僅支援單一網域使用者。如果身分識別提供者設定了多個網域，則僅能將應用程式授權給單一網域中的使用者。

針對身分識別橋接設定 Web Reverse Proxy (對 Kerberos 的憑證)

在您設定 Unified Access Gateway 橋接功能，以便為使用憑證驗證的內部部署舊版非 SAML 應用程式提供單一登入 (SSO) 之前，請先設定 Workspace ONE UEM 主控台以擷取和使用 CA 憑證。

啟用 Workspace ONE UEM 主控台以擷取和使用 CA 憑證

您可以在 CA 伺服器中新增使用者範本，並在 Workspace ONE UEM Console 中進行設定，讓 Workspace ONE UEM 能夠擷取並使用 CA 憑證。

程序

1 新增使用者範本

首先，在 CA 伺服器中新增使用者範本，讓 Workspace ONE UEM 能夠擷取憑證。

2 在主控台中新增憑證授權機構

在 Workspace ONE UEM 主控台中新增憑證授權機構 (CA)。

3 新增憑證授權機構要求範本

請在 Workspace ONE UEM 主控台中新增憑證授權機構之後新增 CA 要求範本。

4 更新安全性原則以使用擷取的 CA 憑證

在 Workspace ONE UEM 主控台中更新安全性原則以使用擷取的 CA 憑證。

新增使用者範本

首先，在 CA 伺服器中新增使用者範本，讓 Workspace ONE UEM 能夠擷取憑證。

程序

1 登入設定 CA 的伺服器。

2 按一下**開始**，然後輸入 **mmc.exe**。

3 在 MMC 視窗中，移至**檔案 > 新增/移除嵌入式管理單元**。

4 在**新增或移除嵌入式管理單元**視窗中，選取**憑證範本**，然後按一下**新增**。

5 按一下**確定**。

6 在**憑證範本**視窗中向下捲動，並選取**使用者 > 複製範本**，

7 在**新範本的內容**視窗中，選取**一般**索引標籤，然後提供**範本顯示名稱**的名稱。

範本名稱會自動填入此名稱，不含空格。

8 選取**主體名稱**索引標籤，然後選取**在要求中提供**。

9 按一下**套用**，然後再按一下**確定**。

10 在 MMC 視窗中，移至**檔案 > 新增/移除嵌入式管理單元**。

11 在**新增或移除嵌入式管理單元**視窗中，選取**憑證授權機構**，然後按一下**新增**。

12 在 MMC 視窗中，選取**憑證授權機構 > 憑證範本**。

13 以滑鼠右鍵按一下**憑證授權機構**，然後選取**新增 > 要發出的憑證範本**。

14 選取您在步驟 6 中建立的範本。

後續步驟

確認您新增的範本顯示於清單中。

登入 Workspace ONE UEM 主控台並新增 CA。

在主控台中新增憑證授權機構

在 Workspace ONE UEM 主控台中新增憑證授權機構 (CA)。

必要條件

- 您必須已在 CA 伺服器中新增使用者範本。
- 您必須具有 CA 簽發者的名稱。登入 Active Directory (AD) 伺服器，並從命令提示字元執行 `certutil` 命令以取得 CA 簽發者名稱。
- 指定 CA 的*使用者名稱*以作為*服務帳戶*類型。

程序

1. 登入 Workspace ONE UEM 主控台，並選取適當的組織群組。
2. 移至**所有設定**，然後從下拉式功能表中按一下**企業整合 > 憑證授權機構**。
3. 按一下**憑證授權單位**索引標籤，然後按一下**新增**。
4. 輸入憑證授權機構的下列資訊：

選項	說明
名稱	CA 的有效名稱
授權單位類型	Microsoft ADCS
通訊協定	ADCS
伺服器主機名稱	AD 伺服器的主機名稱
授權單位名稱	CA 簽發者名稱
驗證	服務帳戶
使用者名稱	具有格式為 *domain**username* 之服務帳戶的使用者名稱。
密碼	使用者名稱的密碼
其他選項	無

5. 按一下**儲存**。

新增憑證授權機構要求範本

請在 Workspace ONE UEM 主控台中新增憑證授權機構之後新增 CA 要求範本。

必要條件

1. 您必須已在 CA 伺服器中新增使用者範本。
2. 您必須已在 Workspace ONE UEM 主控台中新增 CA。

程序

1. 登入 Workspace ONE UEM 主控台，移至**所有設定**，然後從下拉式清單中按一下**企業整合 > 憑證授權機構**。

2 按一下**要求範本**索引標籤，然後按一下**新增**。

3 輸入範本的下列資訊：

選項	說明
名稱	憑證範本的有效名稱
說明 (選擇性)	範本的說明
憑證授權機構	先前新增的憑證授權機構
發行範本	在 CA 伺服器中建立之使用者範本的名稱
主旨名稱	若要新增主體名稱，請將游標停留在值欄位上 (預設值「CN=」後面)，接著按一下「+」按鈕，然後選取適當的電子郵件地址
私密金鑰長度	2048
私密金鑰類型	選取*簽署*
SAN 類型	按一下**新增**，然後選擇*使用者主體名稱*
自動憑證更新 (選用)	
啟用憑證撤銷 (選用)	
發佈私密金鑰 (選用)	

4 按一下**儲存**。

更新安全性原則以使用擷取的 CA 憑證

在 Workspace ONE UEM 主控台中更新安全性原則以使用擷取的 CA 憑證。

必要條件

程序

1 登入 Workspace ONE UEM 主控台，移至**所有設定**，然後從下拉式功能表中按一下**應用程式 > 安全性和原則 > 安全性原則**。

2 針對目前的設定選取**覆寫**。

3 啟用**整合式驗證**。

   a 選取**使用憑證**。

   b 將**認證來源**設為**已定義的憑證授權機構**。

   c 指定先前設定的**憑證授權機構**和**憑證範本**。

4 將**允許的站台**設為 *。

5 按一下**儲存**。

針對身分識別橋接設定 Web Reverse Proxy (對 Kerberos 的憑證)

設定 Unified Access Gateway 橋接功能，以便為使用憑證驗證的內部部署舊版非 SAML 應用程式提供單一登入 (SSO)。

必要條件

開始進行組態程序之前，請確定您可以使用下列檔案和憑證：

- 後端應用程式 (例如 Sharepoint 或 JIRA) 的 Keytab 檔案
- 根 CA 憑證或含有使用者中繼憑證的整個憑證鏈結。
- 您必須已在 Workspace ONE UEM 主控台中新增並上傳憑證。請參閱啟用 Workspace ONE UEM 主控台以擷取和使用 CA 憑證。

請參閱相關產品說明文件，以產生非 SAML 應用程式的根憑證和使用者憑證以及 Keytab 檔案。

請確保 TCP/UDP 連接埠 88 已開啟，因為 Unified Access Gateway 使用此連接埠來與 Active Directory 進行 Kerberos 通訊。

程序

1 從**驗證設定 > X509 憑證**移至：

a 在**根憑證和中繼 CA 憑證**中，按一下**選取**並上傳整個憑證鏈結。

b 在**啟用憑證撤銷**中，將設定切換為**是**。

c 選取**啟用 OCSP 撤銷**的核取方塊。

d 在 **OCSP URL** 文字方塊中，輸入 OCSP 回應者 URL。

Unified Access Gateway 會將 OCSP 要求傳送至指定的 URL，並接收包含指出憑證是否已撤銷之相關資訊的回應。

e 僅在需要將 OCSP 要求傳送至用戶端憑證中的 OCSP URL 時，才應選取**使用來自憑證的 OCSP URL** 核取方塊。如果未啟用此設定，則預設為 OCSP URL 文字方塊中的值。

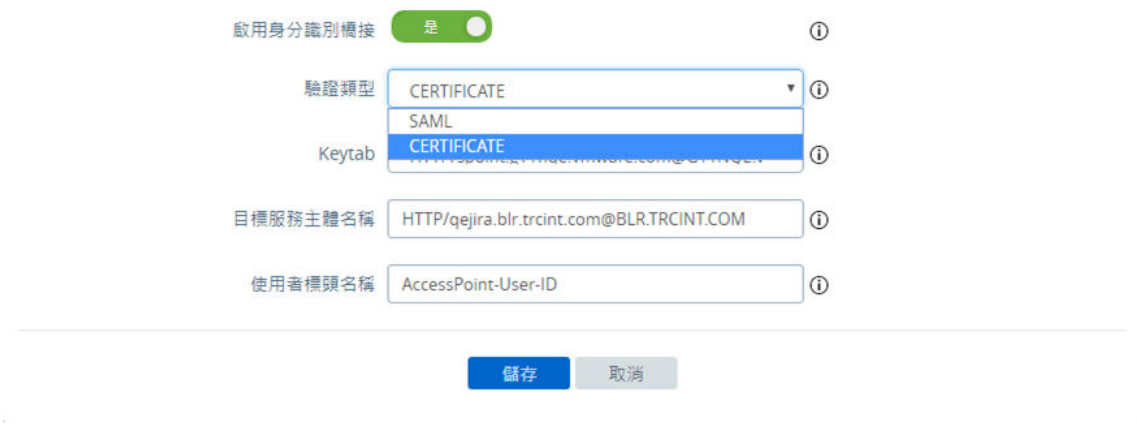
2 在**進階設定 > 身分識別橋接設定 > OSCP 設定**中，按一下**新增**。

a 按一下**選取**並上傳 OCSP 簽署憑證。

3 選取**領域設定**齒輪圖示並依照設定領域設定中所述設定領域設定。

4 從**一般設定 > Edge Service 設定**，選取 **Reverse Proxy 設定**齒輪圖示。

5 將**啟用身分識別橋接設定**設為**是**，接著設定下列身分識別橋接設定，然後按一下**儲存**。



選項	說明
驗證類型	從下拉式功能表中選取 CERTIFICATE。
Keytab	在下拉式功能表中，選取針對此 Reverse Proxy 設定的 Keytab。
目標服務主體名稱	輸入 Kerberos 服務主體名稱。每個主體一律使用完整領域名稱。例如，**myco_hostname@MYCOMPANY**。以大寫字母輸入領域名稱。如果您不新增名稱至文字方塊，則服務主體名稱會衍生自 Proxy 目的地 URL 的主機名稱。
使用者標頭名稱	針對標頭式驗證，輸入包含衍生自判斷提示之使用者 ID 的 HTTP 標頭名稱，或使用預設值 AccessPoint-User-ID。

後續步驟

當您使用 Workspace ONE Web 存取目標網站時，目標網站將會作為 Reverse Proxy。Unified Access Gateway 會驗證提供的憑證。如果憑證有效，則瀏覽器會顯示後端應用程式的使用者介面頁面。

如需特定的錯誤訊息和疑難排解資訊，請參閱疑難排解錯誤：身分識別橋接。

針對 Unified Access Gateway 與第三方身分識別提供者的整合來設定 Horizon

如果您使用的是 SAML 2.0 身分識別提供者，則可以直接整合身分識別提供者與 UAG (Unified Access Gateway)，以支援 Horizon Client 使用者驗證。若要對 UAG 使用 SAML 第三方整合，則必須使用 Horizon 連線伺服器 7.11 或更新版本。

對於 SAML 驗證和 AD 密碼驗證，驗證順序可以是「SAML 和傳遞」，而在與 Horizon True SSO 搭配使用時，驗證順序則可以是只有 SAML。

Unified Access Gateway 已與 SAML 身分識別提供者整合時，支援登入 Unified Access Gateway 的 Horizon Client 使用者進行未驗證存取。向 Unified Access Gateway 進行初始驗證後，使用者即可獲得已發佈應用程式的權利，而無需進行其他驗證。「SAML 和未驗證」方法支援此功能。

由於支援 UAG 與第三方 SAML 身分識別提供者整合，因此不會用到 Workspace ONE Access 安裝。

若要整合 UAG 與身分識別提供者，您必須使用服務提供者 (UAG) 資訊來設定身分識別提供者、將身分識別提供者的中繼資料檔案上傳到 UAG，並在 UAG 管理員 UI 主控台上設定 Horizon 設定。

如需在沒有 Active Directory 認證提示的情況下向 Horizon Client 驗證使用者的相關資訊，請經由 VMware Docs 參閱《Horizon 管理》指南中的〈驗證使用者而不要求認證〉和相關資訊。

使用 Unified Access Gateway 資訊來設定身分識別提供者

若要整合 UAG (服務提供者) 與身分識別提供者，您必須使用服務提供者資訊 (例如，實體 ID 和判斷提示取用者端點 URL) 來設定身分識別提供者。在本案例中，服務提供者是 UAG。

程序

1 登入身分識別提供者的管理主控台。

2 若要建立 SAML 應用程式，請在身分識別提供者的管理主控台上遵循適當的步驟。

如果身分識別提供者具有加密判斷提示功能，請確定您在身分識別提供者上建立之應用程式的 SAML 設定中已停用此功能。

3 以下列其中一種方式，使用 UAG 資訊來設定身分識別提供者：

選項	說明
從 UAG 下載 SAML 服務提供者中繼資料。	若要將 SAML 中繼資料匯入到身分識別提供者內，請確定身分識別提供者有支援匯入功能。 a 在 UAG 管理員 UI 的**手動設定**區段中，按一下**選取**。 b 在**一般設定**區段中，針對 **Edge Service 設定**按一下**顯示**。 c 按一下 **Horizon 設定**齒輪圖示。 d 在 **Horizon 設定**頁面上，按一下**更多**。 e 選取**驗證方法**。 **驗證方法**可以是 `SAML`、`SAML and Passthrough` 或 `SAML and Unauthenticated`。 **備註** 如果您選擇 `SAML and Unauthenticated`，請確實依照 在 Unified Access Gateway 上針對 SAML 整合來進行 Horizon 設定 中對此**驗證方法**的說明來設定 Horizon Connection Server 設定。 f 按一下**下載 SAML 服務提供者中繼資料**。 g 在**下載 SAML 服務提供者中繼資料**視窗中，選取身分識別提供者並輸入外部主機名稱。 h 按一下**下載**。 i 將 `.xml` 中繼資料檔案儲存到您擁有存取權之電腦上的位置。 j 登入身分識別提供者的管理主控台。 k 將所下載的中繼資料檔案匯入到身分識別提供者內。
在身分識別提供者的管理主控台上設定下列 SAML 設定。	a 將實體 ID 設定為 `https://<uagIP/domain>/portal` b 將判斷提示取用者端點 URL 設定為 `https://<uagIP/domain>/portal/samlsso`。

若要進一步瞭解 Unified Access Gateway 與第三方身分識別提供者的整合適用的驗證方法，請參閱適用於 Unified Access Gateway 與第三方身分識別提供者整合的驗證方法。

4 (選擇性) 設定使用者名稱的自訂屬性。

在 Unified Access Gateway 管理員 UI 中，當您選取 `SAML and Unauthenticated` 作為驗證方法時，如果 **SAML 未驗證使用者名稱屬性**設定為此處指定的相同屬性名稱，且 SAML 判斷提示已驗證，Unified Access Gateway 就會為針對此自訂屬性而設定的使用者名稱提供未驗證存取。

若要瞭解 Unified Access Gateway 如何為此使用者名稱提供未驗證存取，請參閱適用於 Unified Access Gateway 與第三方身分識別提供者整合的驗證方法。

後續步驟

將身分識別提供者的 SAML 中繼資料 XML 檔案上傳至 UAG。

將身分識別提供者的 SAML 中繼資料上傳至 Unified Access Gateway

若要在 Horizon 中設定 SAML 和「SAML 和傳遞」驗證方法，您必須將身分識別提供者的 SAML 憑證中繼資料 XML 檔案上傳至 UAG (Unified Access Gateway)。此上傳會讓 UAG 藉由使用身分識別提供者的公開金鑰來驗證判斷提示的簽章，而能夠信任身分識別提供者。

必要條件

您必須已從身分識別提供者下載 SAML 中繼資料 XML 檔案，並將此檔案儲存到您可以存取的電腦中。

程序

1 在 UAG 管理主控台的**手動設定**區段中，按一下**選取**。

2 在**進階設定 > 身分識別橋接設定**區段中，選取**上傳身分識別提供者中繼資料**齒輪圖示。

3 在**實體 ID** 文字方塊中輸入身分識別提供者的實體 ID。

如果未在 [實體 ID] 文字方塊中輸入值，則系統會剖析中繼資料檔案中的身分識別提供者名稱，並用作身分識別提供者的實體 ID。

4 在 **IDP 中繼資料**區段中，按一下**選取**，然後瀏覽至中繼資料檔案儲存所在的位置。

5 從**加密憑證類型**下拉式功能表中選取 **PEM** 作為憑證格式類型。

備註 如果您想要使用加密的判斷提示來驗證 SAML 驗證，則必須選取 PEM。判斷提示的加密和解密需要公開和私密金鑰的組合。身分識別提供者會使用公開金鑰來加密判斷提示，而該公開金鑰僅能使用公開和私密金鑰組合來由 UAG 解密，從而確保增強的安全性。

6 若是**私密金鑰**，按一下**選取**，並瀏覽至採用 PEM 格式的憑證私密金鑰的儲存位置。

7 若是**憑證鏈結**，請按一下**選取**，並瀏覽至採用 PEM 格式的憑證鏈結的儲存位置。

8 若是**允許未加密的 SAML 判斷提示**選項，請將按鈕切換為「是」。如果停用，在 SAML 驗證期間不允許未加密的判斷提示。

9 若要啟用**永遠強制 SAML 驗證**選項，請將按鈕切換為「是」。如果啟用此選項，使用此身分識別提供者時，永遠強制向使用者顯示 SAML 驗證頁面，前提是 IDP 也設定為強制 SAML 驗證。

10 按一下**儲存**。

隨即會顯示下列訊息：已成功儲存組態。

後續步驟

在 UAG 上設定用於選取驗證方法和選擇所需身分識別提供者的 Horizon 設定。

在 Unified Access Gateway 上針對 SAML 整合來進行 Horizon 設定

您必須在 UAG (Unified Access Gateway) 的 Horizon 設定頁面中選取相關的 SAML 驗證方法，並選擇組織所支援的 IDP (身分識別提供者)。驗證方法會決定使用者在搭配使用 Horizon Client 與 UAG 時的登入流程。

如需驗證方法的相關資訊，請參閱適用於 Unified Access Gateway 與第三方身分識別提供者整合的驗證方法。

必要條件

- 請確定您使用的是 Horizon 連線伺服器 7.11 或更新版本。
- 您必須已將身分識別提供者的中繼資料上傳至 UAG。

  請參閱將身分識別提供者的 SAML 中繼資料上傳至 Unified Access Gateway。

程序

1 在 UAG 管理員 UI 的**手動設定**區段中，按一下**選取**。

2 在**一般設定**區段中，針對 **Edge Service 設定**按一下**顯示**。

3 按一下 **Horizon 設定**齒輪圖示。

4 在 **Horizon 設定**頁面上，按一下**更多**以進行下列設定：

選項	說明
驗證方法	選取 `SAML`、`SAML and Passthrough` 或 `SAML and Unauthenticated` **備註** 如果 Horizon 連線伺服器上已啟用 TrueSSO，則只須使用 SAML 驗證方法。 **重要** 如果您選擇 `SAML and Unauthenticated`，請確實將 Horizon Connection Server 中的**登入減速層級**設定為 `Low`。在存取遠端桌面平台或應用程式時，必須進行此組態，以避免端點的登入長時間延遲。 如需關於如何設定**登入減速層級**的詳細資訊，請參閱 VMware Docs 中的《Horizon 管理》說明文件。
身分識別提供者	選取必須與 UAG 整合的身分識別提供者。 **備註** 只有在身分識別提供者的中繼資料已上傳至 UAG 時，該身分識別提供者才可供選取。

若要設定其他 Horizon 設定，請參閱設定 Horizon 設定。

適用於 Unified Access Gateway 與第三方身分識別提供者整合的驗證方法

SAML、SAML 和傳遞以及 SAML 和未驗證是支援的驗證方法，可用來將 UAG (Unified Access Gateway) 與第三方身分識別提供者整合，以控制對 Horizon 桌面平台和應用程式的存取。驗證方法會決定驗證 Horizon 使用者的方式。

當在 UAG 中設定 Horizon 設定時，您必須選取上述其中一個驗證方法。

SAML

在 SAML 驗證方法中，UAG 會先驗證 SAML 判斷提示。如果 SAML 判斷提示有效，UAG 便會將 SAML 判斷提示傳遞至 Horizon Connection Server。若要讓 Horizon Connection Server 接受判斷提示，您必須使用身分識別提供者的中繼資料來設定該連線伺服器。當使用者存取 Horizon Client 時，使用者會看到權利，但不會收到提供 Active Directory 認證的提示。

備註 如果 Horizon Connection Server 上已啟用 TrueSSO 設定，就必須使用 SAML 驗證方法。

SAML 和傳遞

在「SAML 和傳遞」驗證方法中，UAG 會驗證 SAML 判斷提示。如果 SAML 判斷提示有效，則使用者會在存取 Horizon Client 時收到要求其提供 Active Directory 驗證認證的提示。在此驗證方法中，UAG 不會將 SAML 判斷提示傳遞至 Horizon Connection Server。

SAML 和未驗證

在 SAML 和未驗證方法中，Unified Access Gateway 會結合 SAML 使用者驗證與 Horizon 的未驗證存取功能。如果 SAML 判斷提示有效，則使用者可以存取 RDS 主控的應用程式，而不需要進一步驗證。在 Horizon 未驗證存取功能中，系統會將角色型使用者別名與 Horizon 搭配使用，以判斷應用程式權利。使用者別名可用作 Horizon 的預設別名。此別名也可以在 Unified Access Gateway 組態 (**預設未驗證使用者名稱**) 中指定為預設值，或者這可以是在身分識別提供者所傳送 SAML 判斷提示中顯示為宣告的指定 SAML 屬性值。

Unified Access Gateway 管理員 UI 具有兩個文字方塊，即 **SAML 未驗證使用者名稱屬性**和**預設未驗證使用者名稱**，可用於指定使用者別名。當驗證方法為 SAML 和未驗證時，這些文字方塊在管理員 UI 上將可供使用。

如果在管理員 UI 中設定 **SAML 未驗證使用者名稱屬性**文字方塊，當 Unified Access Gateway 驗證 SAML 判斷提示且如果名稱存在於 SAML 判斷提示中，則 Unified Access Gateway 會將該值用作 Horizon 的未驗證存取使用者別名。

當 **SAML 未驗證使用者名稱屬性**文字方塊為空白，或在此文字方塊中所指定的屬性名稱在 SAML 判斷提示中遺失時，Unified Access Gateway 會使用在**預設未驗證使用者名稱**文字方塊中設定的預設使用者名稱作為 Horizon 未驗證存取使用者別名。

如果未使用 **SAML 未驗證使用者名稱屬性**，且**預設未驗證使用者名稱**文字方塊為空白，則 Unified Access Gateway 會使用 Horizon 中設定的預設使用者別名。

如需有關設定未驗證存取使用者之組態的詳細資訊，請參閱 VMware Docs 之《Horizon 管理》指南中的〈提供已發佈應用程式的未驗證存取〉和相關資訊。

如需有關為未驗證存取使用者提供授權 (發佈的應用程式) 之組態的詳細資訊，請參閱 VMware Docs 之《Horizon 管理》指南中的〈授權已發佈應用程式的未驗證存取〉和相關資訊。

Unified Access Gateway 的 Workspace ONE UEM 元件

您可以使用 Unified Access Gateway 應用裝置來部署 VMware Tunnel。Unified Access Gateway 支援 ESXi 或 Microsoft Hyper-V 環境上的部署。VMware Tunnel 可讓個別應用程式透過安全而有效的方法存取公司資源。Content Gateway (CG) 是 Workspace ONE UEM 內容管理解決方案的元件，可讓您安全地在行動裝置上存取內部部署存放庫內容。

VMware Tunnel 和 Content Gateway 的 DNS 需求

在相同的應用裝置上啟用 VMware Tunnel 和 Content Gateway 服務，並啟用 TLS 連接埠共用時，每項服務的 DNS 名稱都必須是唯一的。未啟用 TLS 時，這兩項服務只能使用一個 DNS 名稱，因為連接埠將會區分傳入流量。

在 Unified Access Gateway 上部署 VMware Tunnel

使用 Unified Access Gateway 應用裝置部署 VMware Tunnel，可讓個別應用程式透過安全而有效的方法存取公司資源。Unified Access Gateway 支援 ESXi 或 Microsoft Hyper-V 環境上的部署。

VMware Tunnel 由兩個獨立元件所組成：通道代理伺服器和每一應用程式通道。您可以使用單層或多層網路架構模型來部署 VMware Tunnel。

通道代理伺服器和每一應用程式通道部署模型皆可用於 Unified Access Gateway 應用裝置上的多層網路。此部署包含一個部署於 DMZ 中的前端 Unified Access Gateway 伺服器，以及一個部署於內部網路中的後端伺服器。

通道代理伺服器元件可透過從 Workspace ONE UEM 部署的 Workspace ONE Web 或任何具有 Workspace ONE SDK 功能的應用程式，保護使用者裝置與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。裝置會使用透過 SDK 核發的憑證對通道代理伺服器進行驗證，如 Workspace ONE UEM 主控台中所設定。一般而言，當未受管理的裝置需要安全地存取內部資源時，即應使用此元件。

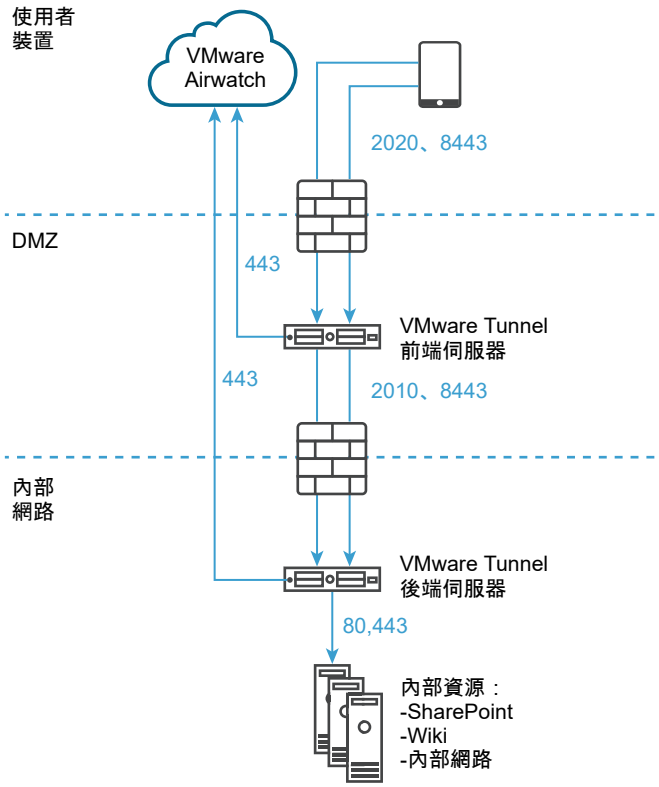
對於完整註冊的裝置，每一應用程式通道元件可讓裝置不需要 Workspace ONE SDK 即可連線至內部資源。此元件會使用 iOS、Android、Windows 10 和 macOS 作業系統的原生每一應用程式 VPN 功能。

如需關於這些平台和 VMware Tunnel 元件功能的詳細資訊，請參閱 Workspace ONE UEM 說明文件頁面中的最新《VMware Tunnel》說明文件。

為您的 Workspace ONE UEM 環境部署 VMware Tunnel 涉及下列作業：

1. 在 Workspace ONE UEM 主控台中設定 VMware Tunnel 主機名稱和連接埠資訊。請參閱 DMZ 型 Unified Access Gateway 應用裝置的防火牆規則。
2. 下載並部署 Unified Access Gateway OVF 範本。
3. 手動設定 VMware Tunnel。

圖 4-10. VMware Tunnel 多層部署：代理伺服器和每一應用程式通道



AirWatch v9.1 及更高版本支援階層式模式作為 VMware Tunnel 的多層部署模型。使用「階層式模式」時，每個從網際網路連至前端通道伺服器的通道元件皆必須有專用的輸入連接埠。前端和後端伺服器皆必須能夠與 Workspace ONE UEM API 和 AWCM 伺服器進行通訊。VMware Tunnel **階層式**模式支援每一應用程式通道元件的多層架構。

如需 Content Gateway 和通道代理伺服器的負載平衡考量事項，請參閱 Unified Access Gateway 負載平衡拓撲。

前往 VMware Workspace ONE UEM 說明文件頁面，以取得 Workspace ONE UEM 指南和版本說明的完整清單。

設定 VMware Tunnel 代理伺服器

使用組態精靈設定 VMware Tunnel 代理伺服器。在精靈中設定的選項會封裝在安裝程式中，您可以從 Workspace ONE UEM 主控台下載取得，並移至通道伺服器。

在 UEM Console 的**群組和設定 > 所有設定 > 系統 > 企業整合 > VMware Tunnel > 代理伺服器**下方設定 VMware Tunnel 代理伺服器。精靈會引導您逐步完成安裝程式組態。在精靈中設定的選項會封裝在安裝程式中，您可以從 Workspace ONE UEM 主控台下載取得，並移至通道伺服器。變更此精靈中的詳細資料時，通常必須使用新組態重新安裝 VMware Tunnel。

若要設定 VMware Tunnel 代理伺服器，您需要預計要安裝之伺服器的詳細資料。在組態之前，請先確定部署模型、主機名稱和連接埠，以及要實作的 VMware Tunnel 功能。您可以考慮變更存取記錄整合、SSL 卸載和企業憑證授權機構整合等項目。

備註 精靈會根據您的選取項目動態顯示適當的選項，組態畫面可能會顯示不同的文字方塊和選項。

程序

1 導覽至**群組和設定 > 所有設定 > 系統 > 企業整合 > VMware Tunnel > 代理伺服器**。

- 如果您是第一次設定 VMware Tunnel，請選取**設定**，然後遵循組態精靈畫面來進行。
- 如果您是第一次設定 VMware Tunnel，請依序選取**覆寫**、**啟用 VMware Tunnel** 切換開關和 **設定**。

  備註 覆寫 VMware Tunnel Proxy 設定並不會覆寫 VMware Tunnel 組態設定。

2 在**部署類型**畫面上，選取**啟用 Proxy (Windows 和 Linux)** 切換開關，然後使用 **Proxy 組態類型**下拉式功能表選取您要設定的元件。

3 在顯示的下拉式功能表中，選取您要設定**轉送端點**還是 **Proxy 組態類型**部署。若要查看所選類型的範例，請選取資訊圖示。

4 選取**下一步**。

5 在**詳細資料**畫面中，進行下列設定。**詳細資料**畫面上顯示的選項，取決於您在 **Proxy 組態類型**下拉式功能表中選取的組態類型。

- 在 **基本 Proxy 組態類型**中，請輸入下列資訊：

設定	說明
主機名稱	輸入通道伺服器之公用主機名稱的 FQDN，例如 tunnel.acmemdm.com。此主機名稱必須是公用的，因為這是裝置從網際網路連線到的 DNS。
轉送連接埠	Proxy 服務會安裝在此連接埠上。裝置會連線至 <轉送主機名稱>:<連接埠> 以使用 VMware Tunnel 代理伺服器功能。預設值為 2020。
轉送主機名稱	(僅限轉送端點)。輸入通道轉送伺服器之公用主機名稱的 FQDN，例如 tunnel.acmemdm.com。此主機名稱必須是公用的，因為這是裝置從網際網路連線到的 DNS。

設定	說明
啟用 SSL 卸載	如果您想要使用「SSL 卸載」來減輕對來自 VMware Tunnel 伺服器流量進行加密和解密時的負荷，請選取此核取方塊。
使用 Kerberos Proxy	若要針對目標後端 Web 服務允許 Kerberos 驗證的存取權，請選取 Kerberos Proxy 支援。此功能目前不支援 Kerberos 限制委派 (KCD)。如需詳細資訊，請參閱設定 Kerberos Proxy 設定。 端點伺服器必須位於與 KDC 相同的網域，Kerberos Proxy 才能成功與 KDC 進行通訊。

- 如果您選擇**轉送端點 Proxy 組態類型**，請輸入下列資訊：

設定	說明
轉送主機名稱	(僅限轉送端點)。輸入通道轉送伺服器之公用主機名稱的 FQDN，例如 tunnel.acmemdm.com。此主機名稱必須是公用的，因為這是裝置從網際網路連線到的 DNS。
端點主機名稱	通道端點伺服器的內部 DNS。此值是轉送伺服器在轉送端點連接埠上連線到的主機名稱。如果您打算在 SSL 卸載伺服器上安裝 VMware Tunnel，請輸入該伺服器的名稱來取代**主機名稱**。 輸入**主機名稱**時請勿包含通訊協定，例如 http://、https:// 等。
轉送連接埠	Proxy 服務會安裝在此連接埠上。裝置會連線至 <轉送主機名稱>:<連接埠> 以使用 VMware Tunnel 代理伺服器功能。預設值為 2020。
端點連接埠	(僅限轉送端點)。此值是 VMware Tunnel 轉送與 VMware Tunnel 端點之間通訊所使用的連接埠。預設值為 2010。 如果您使用 Proxy 和每一應用程式通道的組合，則轉送端點會安裝為階層式模式之前端伺服器的一部分。連接埠必須使用不同的值。
啟用 SSL 卸載	如果您想要使用「SSL 卸載」來減輕對來自 VMware Tunnel 伺服器流量進行加密和解密時的負荷，請選取此核取方塊。
使用 Kerberos Proxy	若要針對目標後端 Web 服務允許 Kerberos 驗證的存取權，請選取 Kerberos Proxy 支援。此功能目前不支援 Kerberos 限制委派 (KCD)。如需詳細資訊，請參閱設定 Kerberos Proxy 設定。 端點伺服器必須位於與 KDC 相同的網域，Kerberos Proxy 才能成功與 KDC 進行通訊。 在**領域**文字方塊中，輸入 KDC 伺服器的領域。

6 選取**下一步**。

7 在 **SSL** 畫面上，您可以設定公用 SSL 憑證，以保護裝置上已啟用應用程式對 VMware Tunnel 的用戶端-伺服器通訊。依預設，此設定會使用 AirWatch 憑證來保護伺服器-用戶端的通訊。

a 如果您想要將第三方 SSL 憑證用於 Workspace ONE Web 或具有 SDK 功能之應用程式與 VMware Tunnel 伺服器之間的加密，請選取**使用公用 SSL 憑證**選項。

b 選取**上傳**以上傳 .PFX 或 .P12 憑證檔案，並輸入密碼。此檔案必須同時包含您的公開和私密金鑰配對。CER 和 CRT 檔案不受支援。

8 選取**下一步**。

9 在**驗證**畫面上設定下列設定，以選取裝置用來向 VMware Tunnel 進行驗證的憑證。

依預設，所有元件會都使用 AirWatch 核發的憑證。若要將企業 CA 憑證用於用戶端-伺服器驗證，請選取**企業 CA** 選項。

a 選取**預設**可使用 AirWatch 核發的憑證。AirWatch 核發的預設用戶端憑證不會自動更新。若要更新這些憑證，請將 VPN 設定檔重新發佈至用戶端憑證即將到期或已到期的裝置。請導覽至**裝置 > 裝置詳細資料 > 更多 > 憑證**，以檢視裝置的憑證狀態。

b 若要選取**企業 CA** 來取代 AirWatch 核發的憑證，而將其用於 Workspace ONE Web、具有每一應用程式通道功能之應用程式或具有 SDK 功能之應用程式與 VMware Tunnel 之間的驗證，您必須在設定 VMware Tunnel 之前，先在您的 Workspace ONE UEM 環境中設定憑證授權機構和憑證範本。

c 選取用來向 CA 要求憑證的**憑證授權機構**和**憑證範本**。

d 選取**上傳**，將憑證授權機構之公開金鑰的完整鏈結上傳至組態精靈。

CA 範本的主體名稱中必須包含 CN=UDID。支援的 CA 包括 ADCS、RSA 和 SCEP。

憑證會根據您的 CA 範本設定自動更新。

10 按一下**新增**以新增中繼憑證。

11 選取**下一步**。

12 在**其他**畫面上，您可以使用 Proxy 或每一應用程式通道元件的存取記錄。請啟用**存取記錄**切換開關來設定此功能。

如果您想要使用此功能，您必須立即將其設定為組態的一部分，因為稍後若要啟用此功能，就必須重新設定通道並重新執行安裝程式。如需有關這些設定的詳細資訊，請參閱存取記錄和 Syslog 整合，以及為 VMware Tunnel 設定進階設定。

a 在 **Syslog 主機名稱**欄位中，輸入您 Syslog 主機的 URL。此設定會在您啟用存取記錄後顯示。

b 在 **UDP 連接埠**欄位中，輸入要用來與 syslog 主機進行通訊的連接埠。

13 選取**下一步**並檢閱組態的摘要，接著確認所有主機名稱、連接埠和設定皆正確無誤，然後選取**儲存**。

在 VMware Tunnel 的**組態**畫面上，安裝程式現已可供下載。

14 在**組態**畫面上，選取**一般**索引標籤。**一般**索引標籤可讓您執行下列動作：

a 您可以選取**測試連線**以確認連線狀況。

b 您可以選取**下載組態 XML**，以 XML 檔案形式擷取現有的 VMware Tunnel 執行個體。

c 您可以選取**下載 Unified Access Gateway** 超連結。此按鈕會下載非 FIPS OVA 檔案。下載檔案也包含 PowerShell 部署方法所需的 PowerShell 指令碼和 .ini 範本檔案。您必須從「My Workspace ONE」下載 VHDX 或 FIPS OVA。

d 如需舊版的安裝程式方法，您可以選取**下載 Windows 安裝程式**。

此按鈕會下載用來部署 VMware Tunnel 伺服器的單一 BIN 檔案。安裝所需的組態 XML 檔案可在確認憑證密碼之後從 Workspace ONE UEM 主控台下載取得。

15 選取**儲存**。

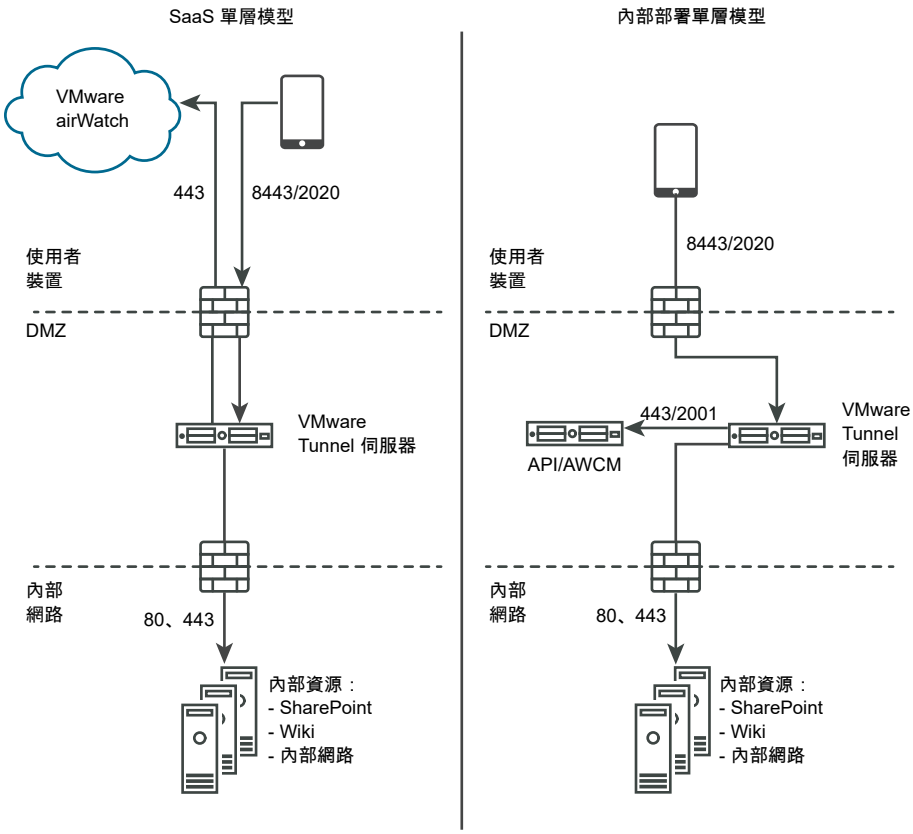
單層部署模型

如果您使用單層部署模型，請使用基本端點模式。VMware Tunnel 的基本端點部署模型，是使用公用 DNS 安裝在伺服器上的單一產品執行個體。

基本 VMware Tunnel 通常會安裝在 DMZ 中位於負載平衡器後方的內部網路中，而流量會透過已設定的連接埠轉送至 VMware Tunnel，繼而直接連線至您的內部 Web 應用程式。所有部署組態皆支援負載平衡和反向 Proxy。

基本端點通道伺服器會與 API 和 AWCM 進行通訊，以接收允許存取 VMware Tunnel 的核准用戶端清單。在此部署模型中，Proxy 和每一應用程式通道元件皆支援使用輸出 Proxy 與 API/AWCM 通訊。當裝置連線至 VMware Tunnel 時，系統會根據由 Workspace ONE UEM 核發的唯一 X.509 憑證對裝置進行驗證。在裝置通過驗證後，VMware Tunnel (基本端點) 會將要求轉送至內部網路。

如果基本端點安裝在 DMZ 中，則必須進行適當的網路變更，VMware Tunnel 才能透過必要的連接埠存取各項內部資源。將此元件安裝在 DMZ 中的負載平衡器後方，可盡可能減少實作 VMware Tunnel 所需的網路變更，並提供多一層的安全性，因為公用 DNS 並未直接指向主控 VMware Tunnel 的伺服器。



階層式模式部署

階層式部署模型架構包含具有個別角色的兩個 VMware Tunnel 執行個體。在階層式模式中，前端伺服器位於 DMZ 中，且會與您內部網路中的後端伺服器進行通訊。

僅「每一應用程式通道」元件支援階層式部署模型。如果您僅使用 Proxy 元件，則必須使用「轉送端點」模型。如需詳細資訊，請參閱轉送端點部署。

在階層式模式下，裝置會使用已設定的主機名稱並透過已設定的連接埠存取前端伺服器。存取前端伺服器的預設連接埠為連接埠 8443。階層式模式下的後端伺服器會安裝在主控內部網路網站和 Web 應用程式的內部網路中。此部署模型會區隔公用的前端伺服器與直接連線至內部資源的後端伺服器，如此可額外提供多一層的安全性。

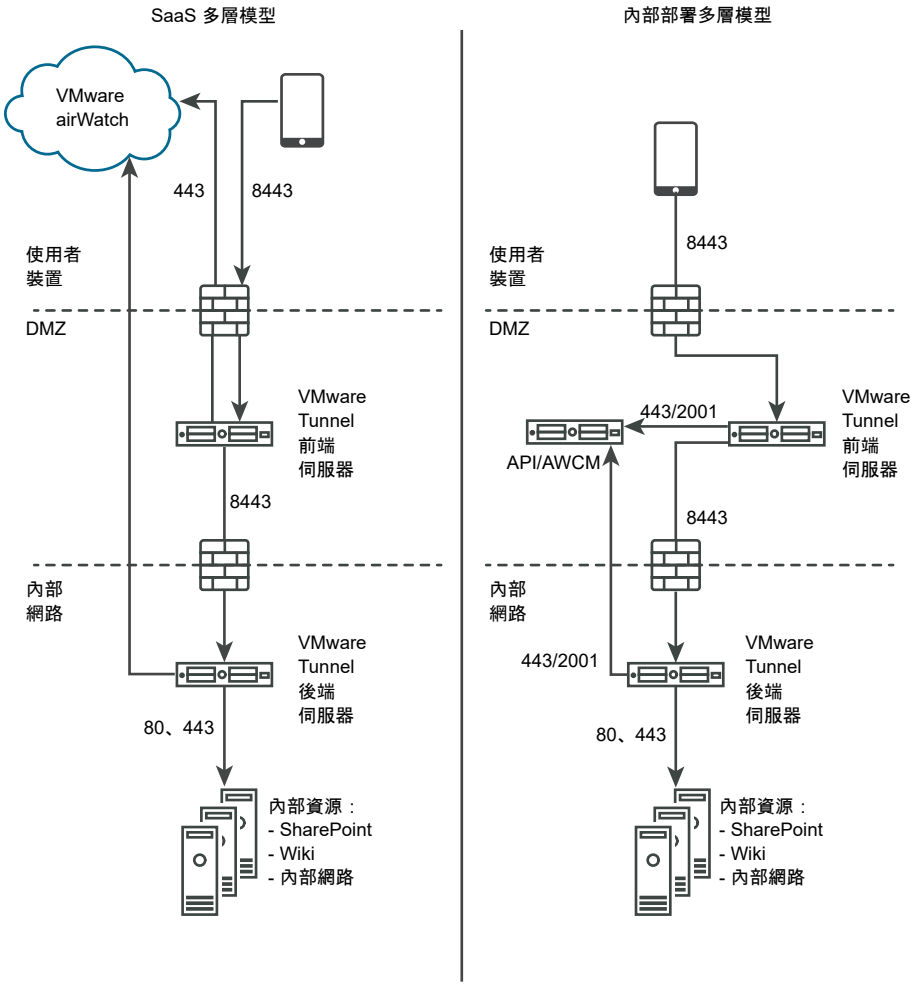
對 VMware Tunnel 提出要求時，前端伺服器可連線至 AWCM 以加速執行裝置的驗證。當裝置對 VMware Tunnel 提出要求時，前端伺服器會判斷裝置是否已獲得存取服務的授權。通過驗證後，系統會使用 TLS 透過單一連接埠將要求安全地轉送至後端伺服器。

後端伺服器會連線至裝置要求的內部 DNS 或 IP。

階層式模式會使用 TLS 連線 (或選用的 DTLS 連線) 進行通訊。您可以視需要主控任意數量的前端和後端伺服器。在搜尋作用中的後端伺服器以將裝置連線至內部網路時，每個前端伺服器都會獨立運作。您可以在 DNS 查閱表格中設定多個 DNS 項目，以允許負載平衡。

前端和後端伺服器都會與 Workspace ONE UEM API 伺服器和 AWCM 進行通訊。API 伺服器會提供 VMware Tunnel 組態，而 AWCM 則提供裝置驗證、裝置存取控制清單和流量規則。前端和後端伺服器會透過直接 TLS 連線與 API/AWCM 通訊，除非您啟用了輸出 Proxy 呼叫。如果前端伺服器無法與 API/AWCM 伺服器連線，請使用此連線。啟用時，前端伺服器會透過後端伺服器連線至 API/AWCM 伺服器。此流量和後端流量都會使用伺服器端流量規則進行路由傳送。如需詳細資訊，請參閱每一應用程式通道的網路流量規則

下圖說明階層式模式下「每一應用程式通道」元件的多層部署：



轉送端點部署

如果您使用多層部署模型和 VMware Tunnel 的代理伺服器元件，請使用轉送端點部署模式。轉送端點部署模式架構包含具有個別角色的兩個 VMware Tunnel 執行個體。VMware Tunnel 轉送伺服器位於 DMZ 中，且能透過已設定的連接埠從公用 DNS 存取。

如果您僅使用「每一應用程式通道」元件，請考慮使用階層式模式部署。如需詳細資訊，請參閱階層式模式部署。

依預設，用來存取公用 DNS 的連接埠為連接埠 8443 (用於每一應用程式通道) 和連接埠 2020 (用於 Proxy)。VMware Tunnel 端點伺服器會安裝在主控內部網路網站和 Web 應用程式的內部網路中。此伺服器必須具有可由轉送伺服器解析的內部 DNS 記錄。此部署模型會區隔公用的伺服器與直接連線至內部資源的伺服器，如此可提供多一層的安全性。

轉送伺服器角色會在裝置對 VMware Tunnel 提出要求時與 API 和 AWCM 元件通訊，並驗證裝置。在此部署模型中，轉送伺服器對 API 和 AWCM 的通訊可透過端點伺服器路由傳送至連出代理伺服器。每一應用程式通道服務必須直接與 API 和 AWCM 通訊。當裝置對 VMware Tunnel 提出要求時，轉送伺服器會判斷裝置是否已獲得存取服務的授權。通過驗證後，系統會使用 HTTPS 透過單一連接埠 (預設連接埠為 2010) 將要求安全地轉送至 VMware Tunnel 端點伺服器。

端點伺服器的角色會連線至裝置要求的內部 DNS 或 IP。端點伺服器不會與 API 或 AWCM 通訊，除非在 Workspace ONE UEM Console 的 VMware Tunnel 設定中將**透過 Proxy 啟用 API 和 AWCM 輸出呼叫**設為**已啟用**。轉送伺服器會定期執行健全狀況檢查，以確保端點作用中且可供使用。

這些元件可以安裝在共用或專用的伺服器上。請在專用 Linux 伺服器上安裝 VMware Tunnel，以確保效能不會受到相同伺服器上執行的其他應用程式影響。在轉送端點部署中，Proxy 和每一應用程式通道元件會安裝在相同的轉送伺服器上。

圖 4-11. 轉送端點部署的內部部署組態

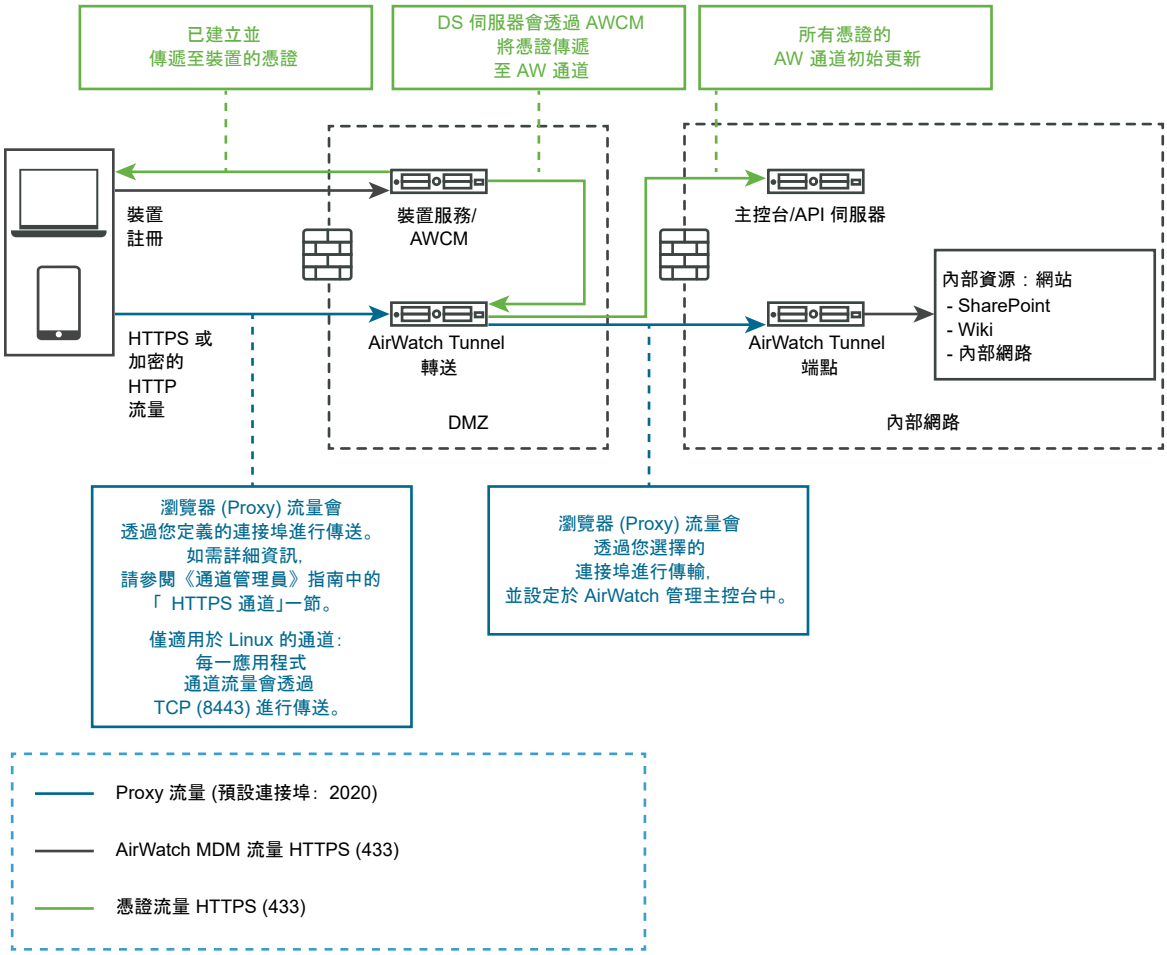
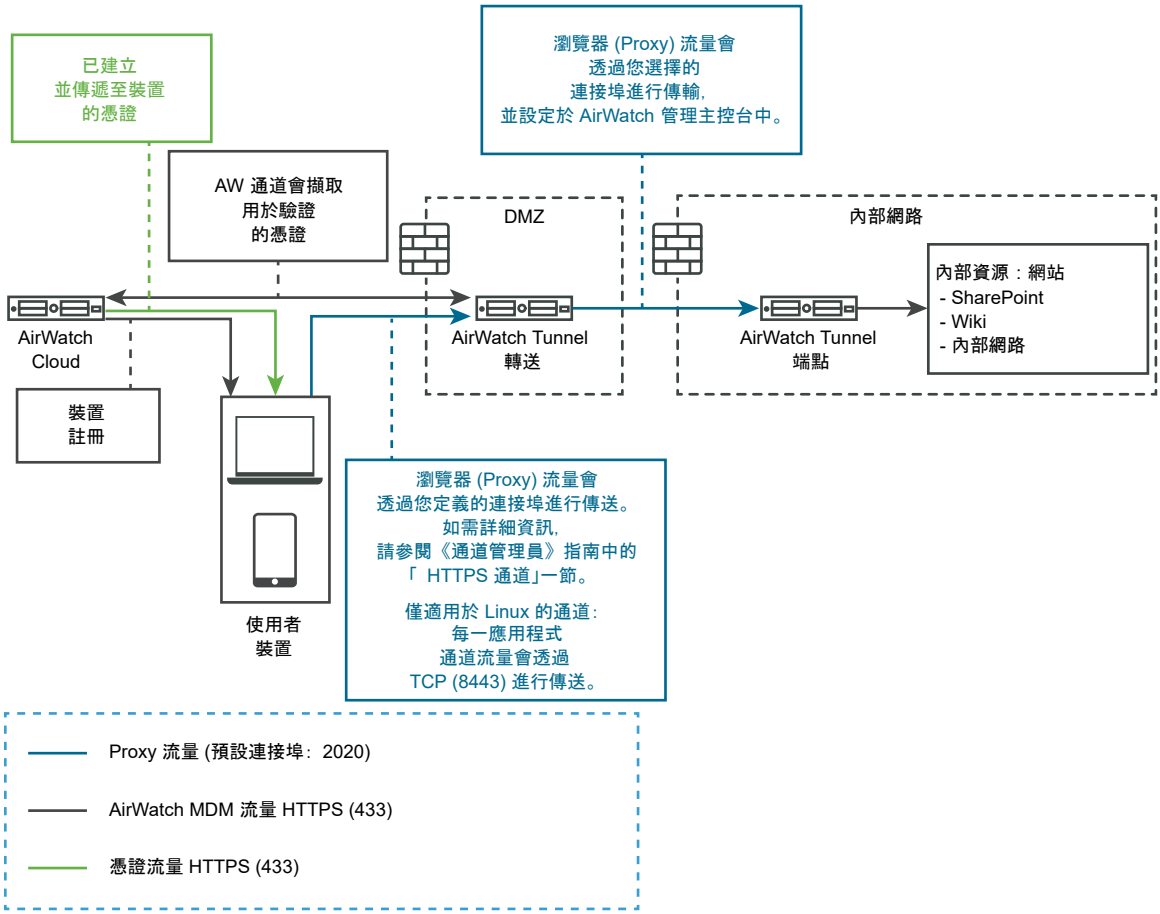


圖 4-12. 轉送端點部署的 SaaS 組態



設定的 Workspace ONE UEM 的 VMware Tunnel 設定

通道代理伺服器部署能透過 Workspace ONE Web 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 導覽至**一般設定 > Edge Service 設定**，然後按一下**顯示**。

3 按一下 **VMware Tunnel 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
API 伺服器 URL	輸入 Workspace ONE UEM 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。

選項	說明
組織群組 ID	輸入使用者的組織。
通道伺服器主機名稱	輸入在 Workspace ONE UEM 主控台中設定的 VMware Tunnel 外部主機名稱。

6 若要設定其他進階設定，請按一下**較多**。

選項	說明
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。
用於 VMware Tunnel 代理伺服器	將 [否] 變更為**是**以使用此 Proxy 作為 VMware Tunnel 的連出代理伺服器。如果未啟用，則 Unified Access Gateway 會對初始 API 呼叫使用此 Proxy，以便從 Workspace ONE UEM 主控台取得組態。
主機項目	輸入要在 `/etc/hosts` 檔案中新增的詳細資料。每個項目依序應包括一個 IP、一個主機名稱和一個選用的主機名稱別名 (以空格區隔)。例如，**`10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`**。按一下「+」符號可新增多個主機項目。 **重要** 只有在按一下**儲存**後，才會儲存主機項目。
受信任的憑證	■ 若要選取 PEM 格式的憑證並新增至信任存放區，請按一下 **+**。 ■ 若要提供不同名稱，請編輯別名文字方塊。 依預設，別名名稱是 PEM 憑證的檔案名稱。 ■ 若要從信任存放區移除憑證，請按一下 **-**。

7 按一下**儲存**。

使用 PowerShell 為 Workspace ONE UEM 部署 VMware Tunnel

您可以使用 PowerShell 為 Workspace ONE UEM 部署 VMware Tunnel。

如需使用 PowerShell 部署 VMware Tunnel 的相關資訊，請觀看此視訊：

VMware Tunnel PowerShell 部署 (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_h7y4lu0e/uiConfId/50138843/)

關於 TLS 連接埠共用

每當多個 Edge Service 設定為使用 TCP 連接埠 443 時，依預設會在 Unified Access Gateway 上啟用 TLS 連接埠共用。支援的 Edge 服務為 VMware Tunnel (每一應用程式 VPN)、Content Gateway、Secure Email Gateway 和 Web 反向 Proxy。

備註 如果您要共用 TCP 連接埠 443，請確保每個設定的 Edge Service 具有指向 Unified Access Gateway 的唯一外部主機名稱。

Unified Access Gateway 上的 Content Gateway

Content Gateway (CG) 是 Workspace ONE UEM 內容管理解決方案的元件，可讓您安全地在行動裝置上存取內部部署存放庫內容。

必要條件

您必須使用 Workspace ONE UEM 主控台設定 Content Gateway 節點，才能設定 Unified Access Gateway 上的 Content Gateway。設定節點之後，請記下自動產生的 *Content Gateway 組態 GUID*。

備註 縮寫 CG 也可用來表示 Content Gateway。

程序

1 導覽至**一般設定 > Edge Service 設定 > Content Gateway 設定**，然後按一下齒輪圖示。

2 若要啟用 Content Gateway 設定，請選取**是**。

3 進行下列設定：

選項	說明
識別碼	表示此服務已啟用。
API 伺服器 URL	Workspace ONE UEM API 伺服器 URL `[http[s]://]hostname[:port]` 目的地 URL 必須包含通訊協定、主機名稱或 IP 位址，以及連接埠號碼。例如：`https://load-balancer.example.com:8443` Unified Access Gateway 會從 API 伺服器提取 Content Gateway 的組態。
API 伺服器使用者名稱	用來登入 API 伺服器的使用者名稱。 **備註** 管理員帳戶至少需要具有與 Content Gateway 角色相關聯的權限。
API 伺服器密碼	用來登入 API 伺服器的密碼。
CG 主機名稱	用來設定 Edge 設定的主機名稱。
CG 組態 GUID	Workspace ONE UEM Content Gateway 組態識別碼。此識別碼會在使用 Workspace ONE UEM 主控台設定 Content Gateway 時自動產生。組態 GUID 會在 UEM Console 的 Content Gateway 頁面上，顯示於**設定 > 內容 > Content Gateway** 下方。
連出代理伺服器主機	安裝連出代理伺服器所在的主機。Unified Access Gateway 會透過連出代理伺服器 (若已設定) 建立 API 伺服器的連線。
連出代理伺服器連接埠	連出代理伺服器的連接埠。

選項	說明
連出代理伺服器使用者名稱	登入連出代理伺服器的使用者名稱。
連出代理伺服器密碼	登入連出代理伺服器的密碼。
NTLM 驗證	指定連出代理伺服器是否需要 NTLM 驗證。
受信任的憑證	■ 若要選取 PEM 格式的憑證並新增至信任存放區，請按一下 **+**。 ■ 若要提供不同名稱，請編輯別名文字方塊。 依預設，別名名稱是 PEM 憑證的檔案名稱。 ■ 若要從信任存放區移除憑證，請按一下 **-**。
主機項目	輸入要在 `/etc/hosts` 檔案中新增的詳細資料。每個項目依序必須包括一個 IP、一個主機名稱和一個選用的主機名稱別名 (以空格區隔)。例如，**`10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`**。按一下「+」可新增多個主機項目。 **重要** 只有在按一下**儲存**後，才會儲存主機項目。

備註 在 Unified Access Gateway 上，連接埠 80 上的 Content Gateway 不允許 HTTP 流量，因為 TCP 連接埠 80 由 Edge Service Manager 所使用。

4 按一下**儲存**。

Content Gateway 組態

在 Workspace ONE UEM Console 中設定 Content Gateway 設定，可建立節點並預先設定會封裝到組態檔中的設定，從而免除在安裝後於伺服器上手動進行設定的需求。

進行設定時必須選取平台、組態模型、相關聯的連接埠，且如有必要，還需上傳 SSL 憑證。

從 Workspace ONE UEM Console 9.6 版開始，Unified Access Gateway (UAG) 是設定 Content Gateway 節點時的建議安裝類型。您可以使用此選項在 Unified Access Gateway 上設定新的 Content Gateway，或將現有的 Content Gateway 移轉至 Unified Access Gateway。

如需關於在 Unified Access Gateway 上設定 Content Gateway 的詳細資訊，請參閱 UAG 說明文件中的〈Unified Access Gateway 上的 Workspace ONE UEM 元件〉。如需移轉的相關資訊，請參閱《將 Content Gateway 移轉至 Unified Access Gateway》說明文件。

如需 Content Gateway 自訂值的相關資訊，請參閱 VMware Docs 上作為《Workspace ONE UEM 說明文件》一部分的《Content Gateway》說明文件。

程序

1 在您選擇的組織群組中導覽至**群組和設定 > 所有設定 > 系統 > 企業整合 > Content Gateway**。

2 將**啟用 Content Gateway** 設為**已啟用**。

您可能必須選取**覆寫**以解除鎖定 Content Gateway 設定。

3 按一下**新增**。

4 完成顯示的欄位以設定 Content Gateway 執行個體。

a 設定**安裝類型**。

設定	說明
安裝類型	選取 Content Gateway 伺服器的作業系統。

b 設定**內容組態**設定。

設定	說明
組態類型	■ **基本** – 不具轉送元件的端點組態。 ■ **轉送** – 具有轉送元件的端點組態。
名稱	提供將 Content Gateway 執行個體連結至內容存放庫、存放庫範本或 RFS 節點時，用來選取此執行個體的唯一名稱。
Content Gateway 轉送位址	如果實作轉送組態，請輸入用來從網際網路存取 Content Gateway 轉送的 URL。
Content Gateway 轉送連接埠	如果實作轉送組態，請輸入轉送伺服器連接埠。
Content Gateway 端點位址	請輸入 Content Gateway 端點的主機名稱。在已設定連接埠上繫結的公用 SSL 憑證對此輸入項目必須是有效的。
Content Gateway 端點連接埠	輸入端點伺服器連接埠。

c 設定**內容 SSL 憑證**設定。

設定	說明
公用 SSL 憑證 (Linux 的需求之一)	如有必要，請上傳具有完整鏈結的 PKCS12 (.pfx) 憑證檔案，讓 Content Gateway 安裝程式繫結至連接埠。完整鏈結包含密碼、伺服器憑證、中繼憑證、根憑證和私密金鑰。 **備註** 若要確保您的 PFX 檔案包含整個憑證鏈結，您可以使用命令列工具 (例如 Certutil 或 OpenSSL) 執行 `certutil -dump myCertificate.pfx` 或 `openssl pkcs12 -in myCertificate.pfx -nokeys` 之類的命令。這些命令會顯示完整的憑證資訊。 需求會隨著平台和 SSL 組態而不同。
忽略 SSL 錯誤 (不建議使用)	如果使用自我簽署憑證，請考慮啟用此功能。如果已啟用，則 Content Gateway 會忽略憑證信任錯誤和憑證名稱不相符的情況。

從 Workspace ONE UEM Console 9.7 版開始不再支援 ICAP Proxy 組態。但現有的組態可供編輯。如需設定 ICAP Proxy 的相關資訊，請參閱 https://support.workspaceone.com/articles/115001675368。

5 選取**新增**。

6 選取**儲存**。

後續步驟

在設定期間，您需要為 Content Gateway 指定平台和組態模型。在 UEM Console 中完成設定之後，請下載安裝程式、設定其他節點，或管理已設定的節點。

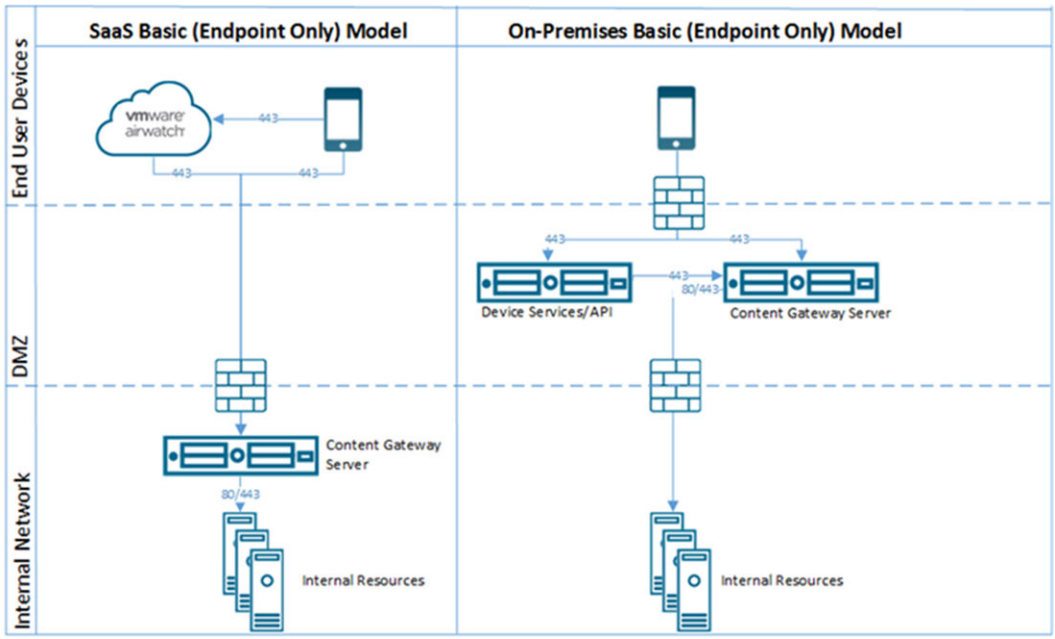
Content Gateway 的基本 (僅限端點) 部署模型

VMware Content Gateway 的基本端點部署模型，是使用公用 DNS 安裝在伺服器上的單一產品執行個體。

在基本部署模型中，VMware Content Gateway 通常會安裝在 DMZ 中位於負載平衡器後方的內部網路中，而流量會透過已設定的連接埠轉送至 VMware Content Gateway。接著 VMware Content Gateway 會直接連線至您的內部內容存放庫。所有部署組態皆支援負載平衡和 Reverse Proxy。

基本端點 Content Gateway 伺服器會與裝置服務通訊。裝置服務會將使用者裝置連線至正確的 Content Gateway。

如果基本端點安裝在 DMZ 中，則必須進行適當的網路變更，VMware Content Gateway 才能透過必要的連接埠存取各項內部資源。將此元件安裝在 DMZ 中的負載平衡器後方，可盡可能減少實作 VMware Content Gateway 所需的網路變更。如此可提供多一層的安全性，因為公用 DNS 並未直接指向主控 VMware Content Gateway 的伺服器。



Content Gateway 的轉送端點部署模型

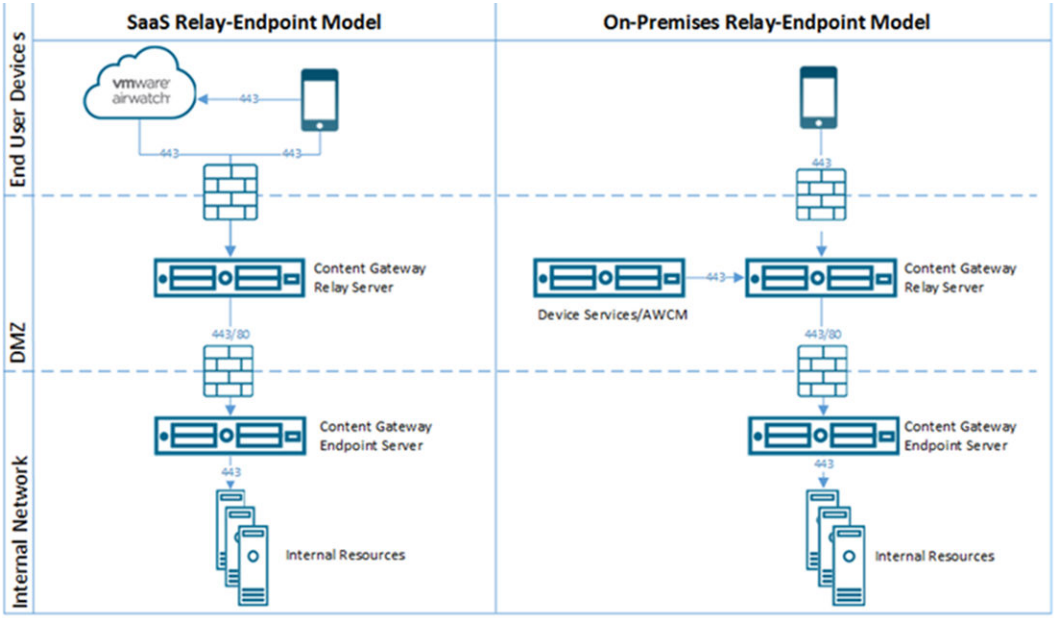
轉送端點部署模型架構包含具有個別角色的兩個 VMware Content Gateway 執行個體。

VMware Content Gateway 轉送伺服器位於 DMZ 中，且只能透過已設定的連接埠從公用 DNS 存取。

依預設，系統會使用 443 連接埠來存取 Content Gateway。VMware Content Gateway 端點伺服器會安裝在主控內部資源的內部網路中。此伺服器必須具有可由轉送伺服器解析的內部 DNS 記錄。此部署模型會區隔公用的伺服器與直接連線至內部資源的伺服器，如此可提供多一層的安全性。

端點伺服器的角色會連線至裝置要求的內部存放庫或內容。轉送伺服器會定期執行健全狀況檢查，以確保端點作用中且可供使用。

這些元件可以安裝在共用或專用的伺服器上。若要確保在相同伺服器上執行的其他應用程式不會影響效能，請在專用伺服器上安裝 VMware Content Gateway。



Unified Access Gateway 上的 Secure Email Gateway

Secure Email Gateway 是 Workspace ONE UEM 的元件之一，可協助您保護郵件基礎結構及啟用 Mobile Email Management (MEM) 功能。

必要條件

您必須使用 Workspace ONE UEM Console 設定 Secure Email Gateway，才能設定 Unified Access Gateway 上的 Secure Email Gateway。設定節點之後，請記下自動產生的 Secure Email Gateway 組態 GUID。如需詳細資訊，請參閱 Secure Email Gateway 說明文件。

備註 縮寫的 SEG 也可用來表示「Secure Email Gateway」。

備註

- 所有統一端點管理 (UEM) 版本都支援 Secure Email Gateway。
- Secure Email Gateway 會設定為遵循 Syslog 組態，此組態則會在 Unified Access Gateway 系統設定中進行設定。依預設，只有 Secure Email Gateway 中的 app.log 內容會以 Syslog 事件的形式來觸發。如需詳細資訊，請參閱 Unified Access Gateway 系統設定。

程序

1 導覽至**一般設定 > Edge Service 設定 > Secure Email Gateway 設定**，然後按一下齒輪圖示。

2 選取**是**以啟用 Secure Email Gateway 設定。

3 進行下列設定。

選項	預設值和說明
API 伺服器 URL	Workspace ONE UEM API 伺服器 URL `[http[s]://]hostname[:port]` 目的地 URL 必須包含通訊協定、主機名稱或 IP 位址，以及連接埠號碼。例如：`https://load-balancer.example.com:8443` Unified Access Gateway 會從 API 伺服器提取 Secure Email Gateway 組態。
API 伺服器使用者名稱	用來登入 API 伺服器的使用者名稱。 **備註** 管理員帳戶至少需要具有與 Secure Email Gateway 角色相關聯的權限。
API 伺服器密碼	用來登入 API 伺服器的密碼。
Secure Email Gateway 伺服器主機名稱	用來設定 Edge 設定的主機名稱。
MEM 組態 GUID	Workspace ONE UEM Mobile Email Management 組態識別碼。此識別碼會在 Workspace ONE UEM Console Console 上設定 Mobile Email Management 時自動產生。UEM Console 的 [Mobile Email Management 組態] 頁面上會顯示組態 GUID。
新增 SSL 憑證	如果已在 UEM Console 的 [電子郵件設定] 下啟用本機上傳 SSL 憑證的選項，請切換以新增 SSL 憑證。
SSL 憑證	按一下 [選取] 來上傳 .PFX 或 .P12 憑證檔案。 **備註** 您也可以在 Workspace ONE UEM Console 中上傳 SSL 憑證。 當憑證上傳到本機時，管理員 GUI 上會顯示憑證的指紋。
密碼	輸入 SSL 憑證的密碼。
連出代理伺服器主機	安裝連出代理伺服器所在的主機。Unified Access Gateway 會透過連出代理伺服器 (若已設定) 建立 API 伺服器的連線。
連出代理伺服器連接埠	連出代理伺服器的連接埠。
連出代理伺服器使用者名稱	登入連出代理伺服器的使用者名稱。
連出代理伺服器密碼	登入連出代理伺服器的密碼。
受信任的憑證	■ 若要選取 PEM 格式的憑證並新增至信任存放區，請按一下 **+**。 ■ 若要提供不同名稱，請編輯別名文字方塊。 依預設，別名名稱是 PEM 憑證的檔案名稱。 ■ 若要從信任存放區移除憑證，請按一下 **-**。
主機項目	輸入要在 /etc/hosts 檔案中新增的詳細資料。每個項目依序應包括一個 IP、一個主機名稱和一個選用的主機名稱別名 (以空格區隔)。例如，10.192.168.1 example1.com、10.192.168.2 example2.com example-alias。按一下「+」可新增多個主機項目。 **備註** 只有在按一下**儲存**後，才會儲存主機項目。

4 按一下**儲存**。

針對 Unified Access Gateway 上的 Secure Email Gateway 變更其記錄層級

您可以針對 Unified Access Gateway 中的 Secure Email Gateway 變更其記錄層級。

您也可以透過在 Workspace ONE UEM Console 上設定 Secure Email Gateway 索引鍵-值配對來變更記錄層級。若要使用索引鍵-值配對，您必須擁有所需的 Secure Email Gateway 自訂設定功能 (特定的 Windows 和 Unified Access Gateway 版本)。如需詳細資訊，請參閱 Secure Email Gateway V2 說明文件中的〈SEG 自訂閘道設定〉一節。

透過從 Workspace ONE UEM Console 使用索引鍵-值配對，您可以同時為所有 Unified Access Gateway 應用裝置變更記錄層級。

必要條件

您必須在 Linux 虛擬機器上啟用 SSH (如果尚未完成)。

程序

1 使用 Secure Shell 連線至 Unified Access Gateway Secure Email Gateway 機器。

2 使用命令編輯 SEG 的記錄組態檔。

```
vi /opt/vmware/docker/seg/container/config/logback.xml
```

3 尋找要變更記錄層級的適當記錄器。例如，`logger name="com.airwatch" groupKey="app.logger" level="error"`

4 將屬性 `level` 的值從 `error` 變更為任何層級，例如 `warn,Info、Debug`。

5 儲存檔案。

結果

記錄層級的變更隨即反映在記錄中。

在 Secure Email Gateway 上啟用 EWS Proxy

SEG (Secure Email Gateway) 會為 ENS (VMware Email Notification Service) 所使用的 EWS (Exchange Web 服務) 流量提供授權和符合性。

您也可以透過在 Workspace ONE UEM Console 上設定 Secure Email Gateway 索引鍵-值配對來啟用 EWS Proxy。若要使用索引鍵-值配對，您必須擁有所需的 Secure Email Gateway 自訂設定功能 (特定的 Windows 和 Unified Access Gateway 版本)。如需詳細資訊，請參閱 Secure Email Gateway 說明文件中的〈SEG 自訂閘道設定〉。

透過從 Workspace ONE UEM Console 使用索引鍵-值配對，您可以同時為所有 Unified Access Gateway 應用裝置啟用 EWS Proxy。

程序

1 使用 Secure Shell 連線至 Unified Access Gateway Secure Email Gateway 機器。

2 使用下列命令編輯內容檔案

```
vi /opt/vmware/docker/seg/container/config/override/application-override.properties
```

3 在 `application-override.properties` 檔案中新增項目。

```
enable.boxer.ens.ews.proxy=true
```

4 儲存檔案。

5 再次將 SEG 組態儲存在 Unified Access Gateway 管理員 UI 上。

其他部署使用案例

您可以使用相同應用裝置上的多個 Edge Service (例如使用 Horizon 和 Web 反向 Proxy) 來部署 Unified Access Gateway，也可以使用 VMware Tunnel、Content Gateway 和 Web 反向 Proxy 來部署 Unified Access Gateway。

部署 Unified Access Gateway 與多個服務的考量

一併部署 Edge Service 之前，請注意下列重要考量。

- 了解並符合網路需求 - 請參閱 DMZ 型 Unified Access Gateway 應用裝置的防火牆規則。
- 遵循調整大小的準則 - 請參閱使用 OVF 範本精靈來部署 Unified Access Gateway 主題中調整大小選項的小節。
- 當 Proxy 模式中有重疊時，Horizon Connection Server 無法搭配已啟用的 Web 反向 Proxy 正常運作。因此，如果在相同的 Unified Access Gateway 執行個體上使用 Proxy 模式同時設定並啟用了 Horizon 和 Web 反向 Proxy 執行個體，請從 Horizon 設定中移除 Proxy 模式「/」，並保留 Web 反向 Proxy 中的模式以防止重疊。保留 Web 反向 Proxy 執行個體中的「/」Proxy 模式可確保使用者在按一下 Unified Access Gateway 的 URL 時會顯示正確的 Web 反向 Proxy 頁面。如果僅設定了 Horizon 設定，則不需要進行前述變更。
- 在使用結合了 VMware Tunnel、Content Gateway、Secure Email Gateway 和 Web 反向 Proxy 的服務來部署 Unified Access Gateway 時，如果對所有服務使用相同的連接埠 443，則每個服務應具有唯一的外部主機名稱。請參閱關於 TLS 連接埠共用。
- 您可以使用管理員 UI 來獨立設定不同的 Edge Service，且可以根據需要匯入任何先前的設定。使用 PowerShell 部署時，INI 檔案會使部署生產就緒。
- 如果在相同的 Unified Access Gateway 應用裝置上啟用了 Horizon Blast 和 VMware Tunnel，則必須將 VMware Tunnel 設定為使用 443 和 8443 以外的其他連接埠號碼。如果您想要對 VMware Tunnel 使用連接埠 443 或 8443，則必須在不同的 Unified Access Gateway 應用裝置上部署 Horizon Blast 服務。

使用 TLS/SSL 憑證設定 Unified Access Gateway

5

您必須設定 Unified Access Gateway 應用裝置的 TLS/SSL 憑證。

備註 設定 Unified Access Gateway 應用裝置的 TLS/SSL 憑證僅適用於 Horizon、Horizon Air 及 Web Reverse Proxy。

本章節討論下列主題：

設定 Unified Access Gateway 應用裝置的 TLS/SSL 憑證

用戶端在連線至 Unified Access Gateway 應用裝置時必須使用 TLS/SSL。面向用戶端的 Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway。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 Unified Access Gateway 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，需提供要與憑證相關聯的伺服器名稱。請確定 Unified Access Gateway 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 Unified Access Gateway 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。

提交憑證簽署要求至 CA 時，請提供外部介面負載平衡器虛擬 IP 位址 (VIP) 作為一般名稱和 SAN 名稱。請確定 Unified Access Gateway 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。

憑證會用於連接埠 443。

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 Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway 時，可能有三種憑證類型需要加以轉換。

- 請一律為 Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway REST API 的單行格式。

必要條件

- 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 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 mycaservercertkey.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` (憑證和金鑰) 檔案轉換為可將 JSON 字串傳遞至 Unified Access Gateway 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。憑證看起來類似此範例。

圖 5-1. 位於單行的憑證檔案

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。

結果

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 Unified Access Gateway〉(使用 PowerShell 部署 VMware Unified Access Gateway) 內附的 PowerShell 指令碼，來設定 Unified Access Gateway 的憑證。或者，您也可以建立並使用 JSON 要求來設定憑證。

後續步驟

您可以使用 CA 簽署的憑證更新預設的自我簽署憑證。請參閱更新 SSL 伺服器簽署的憑證。若是智慧卡憑證，請參閱在 Unified Access Gateway 應用裝置上設定憑證或智慧卡驗證。

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 Unified Access Gateway 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 v1.2。TLS v1.0、TLS v1.1 和 SSL v3.0 會停用。

必要條件

- 自行熟悉 Unified Access Gateway REST API。此 API 的規格位於安裝 Unified Access Gateway 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`、`ssl30Disabled`、`tls10Enabled`、`tls11Disabled` 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_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_
WITH_AES_128_CBC_SHA256
, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
  "ssl30Enabled": "false",
  "tls10Enabled": "false",
  "tls11Enabled": "false",
  "tls12Enabled": "true"
}
```

2 使用 REST 用戶端 (例如 `curl` 或 `postman`)，以使用 JSON 要求來叫用 Unified Access Gateway 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 Unified Access Gateway 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。

結果

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 Unified Access Gateway 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 Unified Access Gateway 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 只能為 Edge Service 指定雙因素使用者驗證方法中的一個。這可以是憑證/智慧卡驗證、RADIUS 驗證或 RSA 調適性驗證。

備註 使用 Active Directory 的密碼驗證是唯一可用於部署的驗證方法。

本章節討論下列主題：

在 Unified Access Gateway 應用裝置上設定憑證或智慧卡驗證

您可以在 Unified Access Gateway 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 Horizon 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 Unified Access Gateway 服務執行智慧卡憑證驗證。Unified Access Gateway 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。

您可以在憑證驗證配接器組態中同時設定 CRL 和 OCSP。當您同時設定兩種類型的憑證撤銷檢查，且若啟用了 **OCSP 失敗**核取方塊時，則**使用 CRL**，將會先檢查 OCSP，如果 OCSP 失敗，撤銷檢查會退而使用 CRL。

備註 如果 CRL 失敗，撤銷檢查不會回復使用 OCSP。

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

在 Unified Access Gateway 上設定憑證驗證

您可從 Unified Access Gateway 管理主控台啟用並設定憑證驗證。

必要條件

- 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 Unified Access Gateway SAML 中繼資料，且服務提供者 SAML 中繼資料已複製到 Unified Access Gateway 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 Unified Access Gateway 管理員 UI 中，導覽至**手動設定**區段，然後按一下**選取**。
2. 在**一般設定 > 驗證設定**中，按一下**顯示**。
3. 按一下 x.509 憑證齒輪。

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。
***根憑證和中繼 CA 憑證**	若要上傳憑證檔案，請按一下**選取**。 您可選取多個已編碼為 DER 或 PEM 的根 CA 和中繼 CA 憑證。 **備註** 在 2012 及更新版本中，UAG 支援設定具有相同主體 DN 的多個 CA 憑證。當更新的 CA 簽發者憑證與相同的主體 DN (但不同的金鑰配對) 搭配使用時，此多憑證支援相當實用。此功能可讓您將新舊 CA 憑證一起使用，以支援由任一個 CA 憑證所簽發的用戶端憑證。UAG 會使用授權金鑰識別碼來識別對應於用來簽署憑證之私密金鑰的公開金鑰。當簽發者具有多個簽署金鑰 (由於多個並行金鑰配對或進行變更) 時，系統將會使用此延伸。
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
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。
使用來自憑證的 OCSP URL	選取此方塊以使用 OCSP URL。
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。

5 按一下**儲存**。

後續步驟

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

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。

後續步驟

將根憑證、中繼憑證或兩者新增至伺服器信任存放區檔案。

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。

後續步驟

將 CA 憑證新增至伺服器信任存放區檔案。

在 Unified Access Gateway 中設定 RSA SecurID 驗證

將 Unified Access Gateway 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 Unified Access Gateway 應用裝置。

必要條件

- 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*。
反覆運算的次數	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 Unified Access Gateway 應用裝置的 IP 位址。
內部主機名稱	輸入 Unified Access Gateway 應用裝置的 IP 位址。
伺服器組態	按一下**變更**以上傳 RSA SecurID 伺服器組態檔案。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	以 *@somedomain.com* 的形式輸入名稱識別碼。它可用來將其他內容 (例如網域名稱) 傳送至 RADIUS 伺服器或 RSA SecurID 伺服器。例如，如果使用者以 *user1* 的身分登入，則會將 *user1@somedomain.com* 傳送至伺服器。

設定 Unified Access Gateway 的 RADIUS

您可以設定 Unified Access Gateway，以便要求使用者使用強式 RADIUS 雙因素驗證。您會在 Unified Access Gateway 應用裝置上設定 RADIUS 伺服器資訊。

RADIUS 支援提供範圍廣泛的第三方雙因素驗證選項。若要在 Unified Access Gateway 上使用 RADIUS 驗證，您必須已設定可透過 Unified Access Gateway 在網路上存取的 RADIUS 伺服器。

當使用者登入並且已啟用 RADIUS 驗證時，使用者要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 RADIUS 挑戰存取，Unified Access Gateway 會向使用者顯示第二個對話方塊，提示其輸入挑戰回應文字，例如透過 SMS 文字或其他頻外機制傳達給使用者的代碼。對輸入 RADIUS 密碼和輸入挑戰回應的支援僅限於文字型輸入。輸入正確的挑戰回應文字即可完成驗證。

如果 RADIUS 伺服器需要使用者輸入其 Active Directory 密碼做為 RADIUS 密碼，那麼，針對 Horizon 使用管理員可以在 Unified Access Gateway 上啟用 Horizon Windows 單一登入功能，使得當 RADIUS 驗證完成時，使用者不會收到要求重新輸入相同的 Active Directory 網域密碼的後續提示。

設定 RADIUS 驗證

在 Unified Access Gateway 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。

必要條件

- 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 Unified Access Gateway 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。

選項	動作
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	以 *@somedomain.com* 的形式輸入名稱識別碼。它可用來將其他內容 (例如網域名稱) 傳送至 RADIUS 伺服器或 RSA SecurID 伺服器。例如，如果使用者以 *user1* 的身分登入，則會將 *user1@somedomain.com* 傳送至伺服器。
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**。
啟用基本 MS-CHAPv2 驗證	將 [否] 變更為**是**以啟用基本 MS-CHAPv2 驗證。如果此選項設為**是**，則會略過來自 RADIUS 伺服器回應的其他驗證。依預設會執行完整驗證。
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 Unified Access Gateway 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，以及調適性驗證的 Unified Access Gateway 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

Unified Access Gateway 中支援的 RSA 調適性驗證強式驗證方法，即為透過電話、電子郵件或 SMS 簡訊和挑戰問題進行的頻外驗證。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 Unified Access Gateway 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。

必要條件

- 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。

選項	說明
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 Unified Access Gateway SAML 中繼資料

您必須在 Unified Access Gateway 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，Unified Access Gateway 是身分識別提供者而伺服器是服務提供者。

必要條件

- 在 Unified Access Gateway 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 Unified Access Gateway 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 如果 Unified Access Gateway 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 Unified Access Gateway 中繼資料的 SAML 簽署憑證。

  備註 如果您的設定中有多部 Unified Access Gateway 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 Unified Access Gateway 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 設定**齒輪圖示。

3 按一下 **SAML 身分識別提供者設定**區段。

4 選取**提供憑證**。

5 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。

6 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。

7 按一下**儲存**。

8 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 Unified Access Gateway 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 Unified Access Gateway 做為身分識別提供者。

對於 Horizon Air 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 Unified Access Gateway

在建立並啟用 SAML 驗證器以便讓 Unified Access Gateway 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 Unified Access Gateway 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 (Unified Access Gateway) 和後端服務提供者 (例如 Horizon Connection Server) 之間建立信任。

必要條件

確認已在後端服務提供者伺服器上為 Unified Access Gateway 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 Unified Access Gateway 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**。

結果

Unified Access Gateway 和服務提供者現在可以交換驗證與授權資訊了。

疑難排解 Unified Access Gateway 部署

7

您可以使用多種程序來診斷及修正於環境中部署 Unified Access Gateway 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：

- 監控 Edge Service 工作階段統計資料
- 監控 SEG 健全狀況和診斷
- 監視所部署服務的健全狀況
- 疑難排解部署錯誤
- 疑難排解錯誤：身分識別橋接
- 疑難排解錯誤：Cert-to-Kerberos
- 疑難排解端點符合性
- 疑難排解管理員 UI 中的憑證驗證
- 疑難排解防火牆和連線問題
- 疑難排解根使用者登入問題
- 從 Unified Access Gateway 應用裝置收集記錄
- Syslog 格式和事件
- 匯出 Unified Access Gateway 設定
- 匯入 Unified Access Gateway 設定
- 疑難排解錯誤：Content Gateway
- 疑難排解高可用性
- 安全性的疑難排解：最佳做法
- 受 Unified Access Gateway 管理員 UI 設定變更影響的使用者工作階段

監控 Edge Service 工作階段統計資料

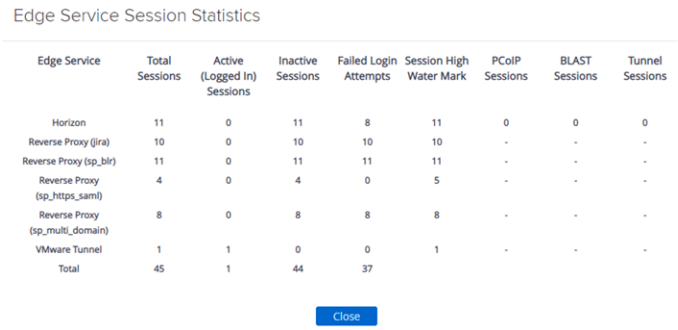
Unified Access Gateway 提供每個 Edge Service 的作用中工作階段的相關資訊。您可以從每個 Edge Service 的管理員 UI 中快速查看您部署的服務已設定、啟動並成功執行。

程序

1 導覽至**支援設定** > **Edge Service 工作階段統計資料**。

2 在**支援設定**區段中，按一下 **Edge Service 工作階段統計資料**齒輪圖示。

圖 7-1. Edge Service 工作階段統計資料



- **Edge Service** 會列出顯示工作階段統計資料的特定 Edge Service。
- **工作階段總計**指出作用中和非作用中工作階段的總數。
- **作用中工作階段 (登入的工作階段)** 指出持續中的驗證工作階段數目。
- **非作用中工作階段**指出未驗證工作階段數目。
- **登入嘗試失敗**指出失敗的登入嘗試數目。
- **工作階段高水位標記**指出在指定時間點並行工作階段數目的上限。
- **PCoIP 工作階段**指出與 PCoIP 建立的工作階段數目。
- **BLAST 工作階段**指出建立與 Blast 建立的工作階段數目。
- **通道工作階段**指出與 Horizon Tunnel 建立的工作階段數目。

表 7-1. Edge Service 工作階段統計資料的範例

Edge Service	工作階段總計	作用中 (已登入) 工作階段	非作用中工作階段	登入嘗試失敗	工作階段高水位標記	PCoIP 工作階段	BLAST 工作階段	通道工作階段
Horizon	11	0	11	8	11	0	0	0
Reverse Proxy (jira)	10	0	10	10	10	-	-	-
Reverse Proxy (sp_blr)	11	0	11	11	11	-	-	-

表 7-1. Edge Service 工作階段統計資料的範例 (續)

Edge Service	工作階段總計	作用中 (已登入) 工作階段	非作用中工作階段	登入嘗試失敗	工作階段高水位標記	PCoIP 工作階段	BLAST 工作階段	通道工作階段
Reverse Proxy (sp_https_saml)	4	0	4	0	5	-	-	-
Reverse Proxy (sp_multi_domain)	8	0	8	8	8	-	-	-
VMware Tunnel	1	1	0	0	1	-	-	-
總計	45	1	44	37		-	-	-

監控工作階段統計資料 API

此處列出的參數說明在最後一個的監控間隔擷取的工作階段統計資料。

URL 呼叫：`https://<UAGIP>:9443/rest/v1/monitor/stats`

表 7-2. Horizon View

屬性	說明
`totalSessions`	指出作用中和非作用中工作階段的總數。 管理員 UI：**工作階段總計**。
`highWaterMarkOfSessions`	指出在指定時間點並行工作階段數目的上限。 管理員 UI：**工作階段高水位標記**。
`authenticatedSessions`	指出正在進行的已驗證工作階段 (已登入工作階段) 的數目。 管理員 UI：**作用中 (已登入) 工作階段**。
`unauthenticatedSessions`	指出未經驗證的工作階段數目。 管理員 UI：**非作用中工作階段**。
`failedLoginAttempts`	指出登入嘗試失敗的次數。 管理員 UI：**登入嘗試失敗**
`userCount`	指出目前已驗證的唯一使用者數目。
BLAST	
`sessions`	指出作用中的 BLAST 工作階段數目。
`maxSessions`	指出已驗證的 BLAST 工作階段數目。
PCoIP	
`sessions`	指出在桌面平台或應用程式啟動期間建立的作用中 PCoIP 工作階段數目。
`maxSessions`	指出指定時間點的並行 PCoIP 工作階段數目的上限。

表 7-2. Horizon View (續)

屬性	說明
VMware Tunnel	
sessions	指出透過 View Client 對驗證建立的作用中 VMware Tunnel 工作階段數目。
maxSessions	指出指定時間點的並行 VMware Tunnel 工作階段數目的上限。

表 7-3. Web 反向 Proxy

屬性	說明
totalSessions	指出作用中和非作用中工作階段的總數。 管理員 UI：**工作階段總計**。
highWaterMarkOfSessions	指出在指定時間點並行工作階段數目的上限。 管理員 UI：**工作階段高水位標記**。
authenticatedSessions	指出正在進行的已驗證工作階段 (已登入工作階段) 的數目。 管理員 UI：**作用中 (已登入) 工作階段**。
unauthenticatedSessions	指出未經驗證的工作階段數目。 管理員 UI：**非作用中工作階段**。
failedLoginAttempts	指出登入嘗試失敗的次數。 管理員 UI：**登入嘗試失敗**。
userCount	指出目前已驗證的唯一使用者數目。
backendStatus	
status	指出是否可連線到後端應用程式。(執行中、無法連線)
reason	指出狀態並說明原因。(無法連線、錯誤詳細資料)
kcdStatus	
status	指出是否可連線到 KCD 伺服器。(執行中、無法連線)
reason	指出狀態並說明原因。(無法連線、錯誤詳細資料)

表 7-4. VMware Tunnel

屬性	說明
identifier	指出 VMware Tunnel 服務已啟用。
status	VMware Tunnel 服務 (vpnd 服務) 的狀態。
reason	指出 VMware Tunnel 服務的狀態並說明原因。啟動或關閉標籤表示服務狀態。例如，若服務已啟動並在執行，則可以連線，若服務已關閉，則無法連線到 VMware Tunnel 伺服器。
totalSessions	指出透過 VMware Tunnel 用戶端對驗證建立的作用中 VMware Tunnel 工作階段數目。
connections	指出來自 VMware Tunnel VMware Tunnel 伺服器的作用中輸出連線數目。
upTime	指出 VMware Tunnel 服務的作用中 (執行中) 時間。

表 7-4. VMware Tunnel (續)

屬性	說明
apiConnectivity	VMware Tunnel 伺服器的 API 連線。例如，True 或 False。
awcmConnectivity	VMware Tunnel 伺服器的 AWCM 連線。例如，True 或 False。
cascadeMode	提供階層式資訊。例如，「關閉」表示基本模式，前端或後端表示階層式設定。

表 7-5. Unified Access Gateway 應用裝置

屬性	說明
cpuCores	指出指派給應用裝置的處理器核心數目。
totalCpuLoadPercent	指示 CPU 負載 (以百分比為單位)。
totalMemoryMb	指示記憶體總計 (MB)。
freeMemoryMb	指示可用的未使用記憶體 (MB)。
cpuDetailedStats	提供所使用 CPU 的詳細統計資料。 ■ idle - CPU 不會執行任何工作。 ■ ioWait - CPU 會等待磁碟輸入/輸出作業完成。 ■ irq - 配置給硬體中斷的 CPU。 ■ nice - 用於配置多個處理程序 (需要超過 CPU 可提供的週期) 的 CPU。 ■ softIrq - CPU 會為軟中斷提供服務。 ■ steal - Xen Hypervisor 會將週期配置給其他工作。 ■ system - 作業系統所使用的 CPU。 ■ user - 使用者應用程式所使用的 CPU。

Horizon 的 Unified Access Gateway 工作階段流程

為了協助您瞭解 Horizon Edge 服務之 Unified Access Gateway 工作階段中工作階段統計資料如何變更，此主題中說明事件的流程。

此處說明的工作階段流程不包含在 Unified Access Gateway 管理員 UI 中為 Horizon 設定的任何驗證方法。

Edge 服務健全狀況檢查會根據**監控間隔** (Unified Access Gateway 管理員 UI 中的進階系統組態設定) 中設定的值發生。

若要查看此處所提及工作階段統計資料的定義，請參閱監控 Edge Service 工作階段統計資料。

1 當 Horizon Client 透過 Unified Access Gateway 將 XMLAPI 要求傳送到 Horizon Connection Server 時，會在 Unified Access Gateway 中建立新的工作階段。

在後續的 Edge 服務健全狀況檢查中，工作階段統計資料會具有下列值：

工作階段統計資料	值
Total Sessions	1
Active Sessions	0
Inactive Sessions	1
Failed Login Attempts	0
Session High Water Mark	1

收到來自 Horizon Connection Server 的回應後，Unified Access Gateway 會將回應傳送至 Horizon Client，並在使用者的裝置上顯示驗證提示。

2 出現驗證提示時，使用者的動作可能有所不同。根據動作，工作階段統計資料會有不同的值。

a 如果使用者的驗證成功，在後續的 Edge 服務健全狀況檢查中，工作階段統計資料會具有下列值：

工作階段統計資料	值
Total Sessions	1
Active Sessions	1
Inactive Sessions	0
Failed Login Attempts	0
Session High Water Mark	1

b 如果使用者提交不正確的驗證認證，則工作階段統計資料的變更取決於 Horizon Connection Server 所允許的登入嘗試次數。

- 如果允許的登入嘗試次數大於 1，則工作階段會維持非作用中狀態，直到登入嘗試次數達到 Horizon Connection Server 所允許的上限為止。

  每次登入嘗試失敗時 `Failed Login Attempts` 參數便會增加 1。

  在後續的 Edge 服務健全狀況檢查中，工作階段統計資料會具有下列值：

工作階段統計資料	值
Total Sessions	1
Active Sessions	0
Inactive Sessions	1
Failed Login Attempts	1
Session High Water Mark	1

- 如果允許的嘗試次數僅為 1，則系統會移除該工作階段。

  備註 移除工作階段時，`Total Sessions` 和 `Inactive Sessions` 會減少 1。

在後續的 Edge 服務健全狀況檢查中，工作階段統計資料會具有下列值：

工作階段統計資料	值
Total Sessions	0
Active Sessions	0
Inactive Sessions	0
Failed Login Attempts	1
Session High Water Mark	1

c 如果使用者在**驗證逾時** (Unified Access Gateway 管理員 UI 中設定的系統組態設定) 後嘗試進行驗證，則驗證會失敗且系統會移除該工作階段。

在後續的 Edge 服務健全狀況檢查中，工作階段統計資料會具有下列值：

工作階段統計資料	值
Total Sessions	0
Active Sessions	0
Inactive Sessions	0
Failed Login Attempts	1
Session High Water Mark	1

d 如果使用者取消驗證提示，則工作階段將不會通過驗證並維持在此狀態，直到從建立工作階段開始的時間超過**驗證逾時**為止。超過**驗證逾時**時，工作階段將會到期。

備註 已到期的工作階段會納入 Total Sessions 的一部分，直到達到工作階段總數的限制為止。此限制取決於 Unified Access Gateway 應用裝置的大小。

在後續的 Edge 服務健全狀況檢查中，工作階段統計資料會具有下列值：

工作階段統計資料	值
Total Sessions	1
Active Sessions	0
Inactive Sessions	1
Failed Login Attempts	0
Session High Water Mark	1

3 驗證成功完成後，如果在 Unified Access Gateway 中啟用 VMware Tunnel，且使用 Horizon Client，則會在 Unified Access Gateway 中建立通道工作階段。

在後續的 Edge 服務健全狀況檢查中，工作階段統計資料會具有下列值：

工作階段統計資料	值
Total Sessions	1
Active Sessions	1

工作階段統計資料	值
Inactive Sessions	0
Failed Login Attempts	0
Session High Water Mark	1
Tunnel Sessions	1 **備註** 如果在 Unified Access Gateway 中停用通道，則值會是 0。

4 根據使用者所選取用於啟動桌面平台或應用程式的顯示通訊協定 (PCOIP 或 Blast)，對應通訊協定的工作階段統計資料會受到影響。

例如，如果設為使用 Blast 通訊協定，則在後續的 Edge 服務健全狀況檢查中，工作階段統計資料會具有下列值：

工作階段統計資料	值
Total Sessions	1
Active Sessions	1
Inactive Sessions	0
Failed Login Attempts	0
Session High Water Mark	1
Tunnel Sessions	1
Blast Sessions	1
PCoIP Sessions	0

5 如果使用者將啟動的桌面平台或應用程式中斷連線，則在後續的 Edge 服務健全狀況檢查中，工作階段統計資料會具有下列值：

工作階段統計資料	值
Total Sessions	1
Active Sessions	1
Inactive Sessions	0
Failed Login Attempts	0
Session High Water Mark	1
Tunnel Sessions	1
Blast Sessions	0
PCoIP Sessions	0

6 使用者登出可能會由於各種原因發生，例如使用者起始的登出、使用者驗證後無活動或工作階段到期。當使用者登出時，在後續的 Edge 服務健全狀況檢查中，工作階段統計資料會具有下列值：

工作階段統計資料	值
Total Sessions	0
Active Sessions	0
Inactive Sessions	0
Failed Login Attempts	0
Session High Water Mark	1
Tunnel Sessions	0
Blast Sessions	0
PCoIP Sessions	0

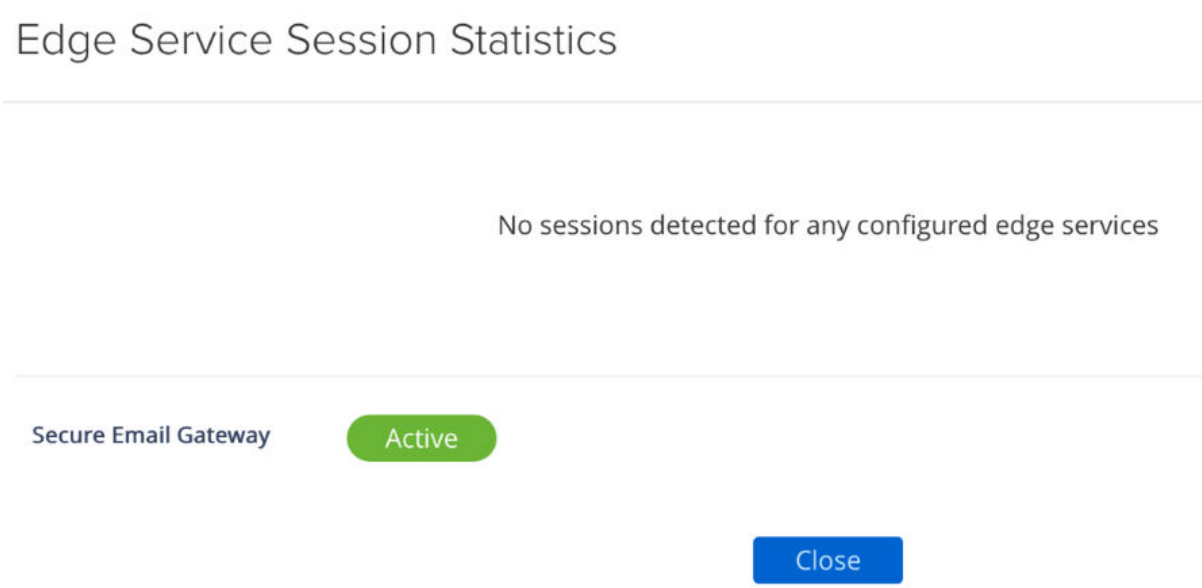
監控 SEG 健全狀況和診斷

您可以使用 SEG V2 的管理頁面來監控 SEG 的健全狀況和診斷。

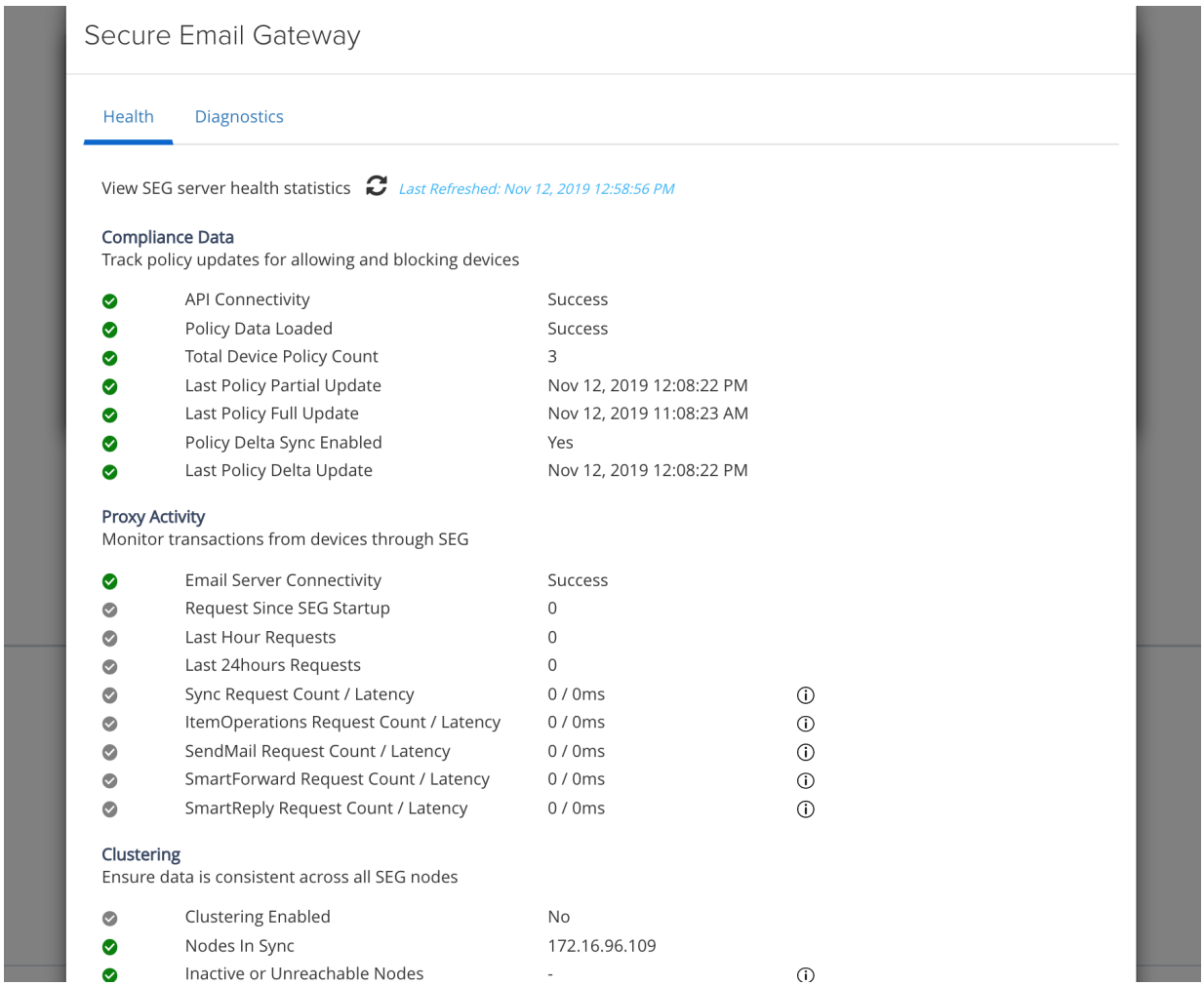
下列程序會說明用來檢視 SEG 健全狀況和診斷資訊的步驟。

1 導覽至**支援設定 > Edge Service 工作階段統計資料**。

2 在**支援設定**區段中，按一下 **Edge Service 工作階段統計資料**齒輪圖示。如果 SEG 已啟用，則會顯示下列畫面。



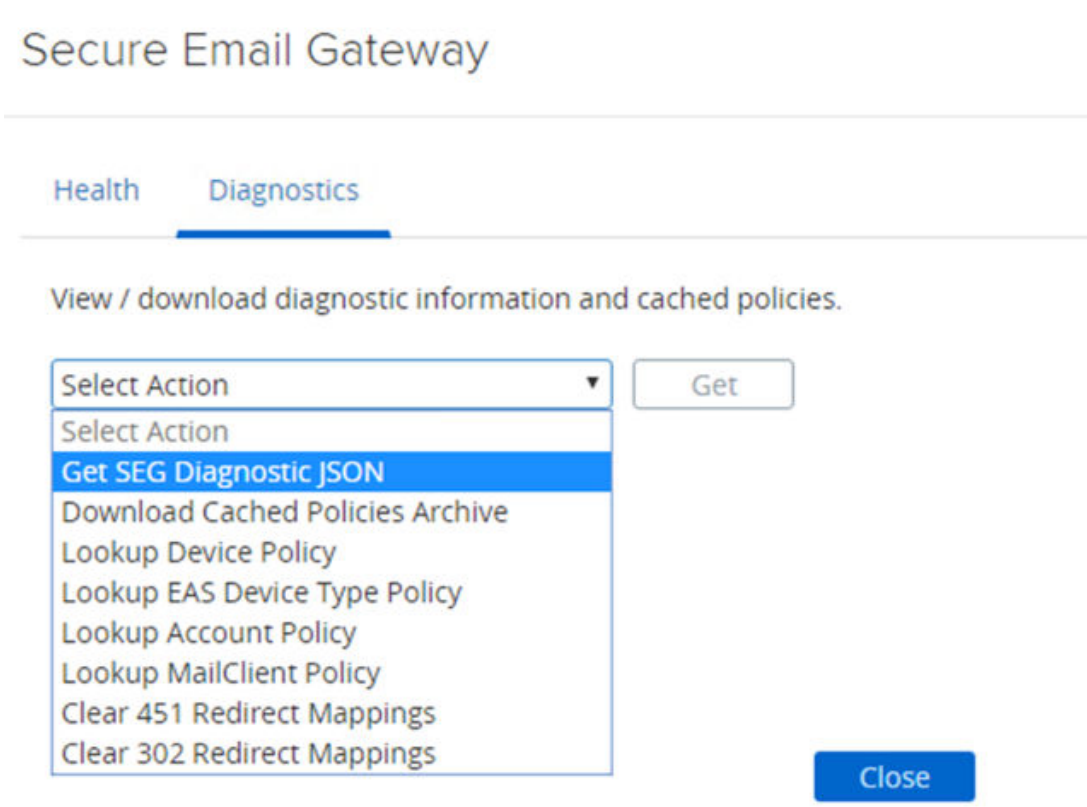
3 按一下**作用中**以開啟 SEG 的健全狀況和診斷監控畫面。隨即會出現下列畫面。



SEG 診斷畫面會為使用者提供下列選項：

- 檢視或下載 SEG 診斷 JSON。
- 從 SEG 快取查閱特定原則。
- 封存並下載 SEG 快取原則、重新導向對應和診斷資訊。
- 從 SEG 快取中清除重新導向對應。

下列影像顯示 SEG 的診斷畫面。



SEG 診斷 API

下表說明用於存取 SEG 診斷資訊的 API 路徑和參數。

SEG 診斷 URL：GET https://<UAGIP>:9443/rest/v1/monitor/seg/diagnostics/<apiPath>。

API 路徑	說明
診斷	檢視 SEG 診斷 JSON。
`policy/device/<easDeviceId>`	查閱指定 EAS 裝置識別碼的裝置原則。
`policy/account/<accountId>`	使用帳戶識別碼來查閱指定使用者或群組的原則。
`policy/easdevicetype/<easdevicetype>`	查閱指定 EAS 裝置類型的原則。
`policy/mailclient/<mailclientname>`	查閱指定郵件用戶端的原則。
`cache/archive`	封存並下載 SEG 快取原則、重新導向對應和診斷資訊。
`policy/account/<accountId>`	查閱指定 EAS 裝置識別碼的裝置原則。

下表列出了用於從 SEG 快取清除重新導向對應的 API。

清除重新導向快取對應 URL：DELETE https://<UAGIP>:9443/rest/v1/monitor/seg/cache/<parameter>

參數	說明
451	從 SEG 快取中清除 451 重新導向對應。
302	從 SEG 快取中清除 302 重新導向對應。

SEG 健全狀況 API

下表說明 SEG 健全狀況統計資料回應屬性。

SEG 健全狀況 URL：GET https://<UAGIP>:9443/rest/v1/monitor/seg/healthStats

回應屬性	說明
diagnosticExportTime	指定用來產生統計資料的時間 (以毫秒為單位)，從 UNIX epoch 時間起算。
apiConnectivity	從 SEG 到 API 伺服器的連線狀態。狀態值可以是**成功**或**失敗**。
policyDataLoaded	載入到 SEG 快取之原則資料的狀態。狀態值可以是**成功**、**進行中**或**失敗**。
totalDevicePolicyCount	指定已載入到 SEG 快取之裝置原則的計數。
lastPolicyPartialUpdate	指定最後成功的部分原則更新所用的執行時間 (以毫秒為單位)，從 UNIX epoch 時間起算。
lastPolicyFullUpdate	指定最後成功的原則更新所用的執行時間 (以毫秒為單位)，從 UNIX epoch 時間起算。
lastPolicyDeltaUpdate	指定最後的差異原則更新所用的執行時間 (以毫秒為單位)，從 UNIX epoch 時間起算。
policyDeltaSyncEnabled	可指出原則差異同步是否已啟用的旗標。
emailServerConnectivity	從 SEG 到 API 伺服器的連線狀態。 屬性值可以是**成功**或**失敗**。
requestsSinceSEGstartup	自 SEG 伺服器啟動後的 ActiveSync 要求數。
lastHourRequests	過去一小時內的 ActiveSync 要求數。
last24hourRequests	過去 24 小時內的 ActiveSync 要求數。
syncStat ■ 計數 ■ 延遲	指定**同步**要求的對應統計資料。 ■ 過去一小時期間的要求計數。 ■ 過去 24 小時期間的平均延遲。
itemOperationsStat ■ 計數 ■ 延遲	指定**項目作業**要求的對應統計資料。 ■ 過去一小時期間的要求計數。 ■ 過去 24 小時期間的平均延遲。
sendMailStat ■ 計數 ■ 延遲	指定**傳送郵件**要求的對應統計資料。 ■ 過去一小時期間的要求計數。 ■ 過去 24 小時期間的平均延遲。

回應屬性	說明
smartForwardStat ■ 計數 ■ 延遲	指定**智慧轉寄**要求的對應統計資料。 ■ 過去一小時期間的要求計數。 ■ 過去 24 小時期間的平均延遲。
smartReplyStat ■ 計數 ■ 延遲	指定**智慧回覆**要求的對應統計資料。 ■ 過去一小時期間的要求計數。 ■ 過去 24 小時期間的平均延遲。
clusteringEnabled	可指出叢集功能是否已啟用的旗標。
nodesOnline	叢集內處於作用中狀態的節點清單。
nodesOffline	已列在 MEM 組態中，但在叢集內未處於作用中狀態的節點清單。
nodesSynchronized	可指出叢集中的所有節點是否處於同步中的旗標。

監視所部署服務的健全狀況

您可以從管理員 UI 的 [Edge 設定] 中快速查看您部署的服務已設定、啟動並成功執行。

圖 7-2. 健全狀況檢查

服務前方會顯示一個圓形。色彩編碼如下所示。

- 黑色圓形 - 設定尚未設定。
- 紅色圓形 - 服務已關閉。
- 琥珀色圓形 - 服務部分執行中。
- 綠色圓形 - 服務正在執行中，且並未發生任何問題。

疑難排解部署錯誤

當您在環境中部署 Unified Access Gateway 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 .\uagdeploy.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 netInternet、netManagementNetwork 及 netBackendNetwork 這三個網路各自的 INI 檔案中設定值。

關於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。

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 Server 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。

錯誤訊息：無法從工作階段擷取用戶端憑證：`sessionId`

- 檢查是否已在瀏覽器中正確安裝使用者憑證。
- 檢查是否已在瀏覽器和 Unified Access Gateway 上啟用預設 TLS 通訊協定 1.2 版。

無法使用在 Chrome 瀏覽器上啟動的 VMware vSphere Web Client 部署 Unified Access Gateway ova

您必須在 vSphere Web Client 上用來部署 ova 檔案的瀏覽器上安裝用戶端整合外掛程式。在 Chrome 瀏覽器上安裝外掛程式後，系統會顯示一則錯誤訊息，指出瀏覽器並未安裝，且將不允許您在來源位置中輸入 ova 檔案 URL。這是 Chrome 瀏覽器方面的問題，與 Unified Access Gateway ova 無關。建議您使用不同的瀏覽器來部署 Unified Access Gateway ova。

無法使用 VMware vSphere HTML4/5 Web Client 部署 Unified Access Gateway ova

您可能會遇到錯誤，例如為內容指定的值無效。此問題與 Unified Access Gateway ova 無關。建議您改用 vSphere FLEX 用戶端來部署 ova。

無法使用 VMware vSphere 6.7 HTML5 Web Client 部署 Unified Access Gateway ova

您可能會在 VMware vSphere 6.7 HTML5 Web Client 的**部署內容**頁面上發現遺漏的欄位。此問題與 Unified Access Gateway ova 無關。建議您改用 vSphere FLEX 用戶端來部署 ova。

無法從 Workspace ONE Access 透過 Chrome 啟動 XenApp

部署 Unified Access Gateway 作為來自 Workspace ONE Access 的 Web 反向 Proxy 之後，您可能無法從 Chrome 瀏覽器啟動 XenApp。

請遵循下列步驟來解決此問題。

1 若要從 Workspace ONE Access 服務停用功能旗標 `orgUseNonNPAPIForCitrixLaunch`，請使用下列 REST API。

```
PUT https://fqdn/SAAS/jersey/manager/api/tenants/settings?tenantId=tenantname
{ "items":[ {"name":"orgUseNonNPAPIForCitrixLaunch","value": "false"} ] }
with the following two headers:
Content-Type application/vnd.vmware.horizon.manager.tenants.tenant.config.list+json
Authorization HZN value_of_HZN_cookie_for_admin_user
```

2 等待 24 小時使變更生效，或重新啟動 Workspace ONE Access 服務。

- 若要在 Linux 上重新啟動服務，請登入虛擬應用裝置並執行下列命令：`service horizon-workspace restart`。
- 若要在 Windows 上重新啟動服務，請執行下列指令碼：`install_dir\usr\local\horizon\scripts\horizonService.bat restart` 。

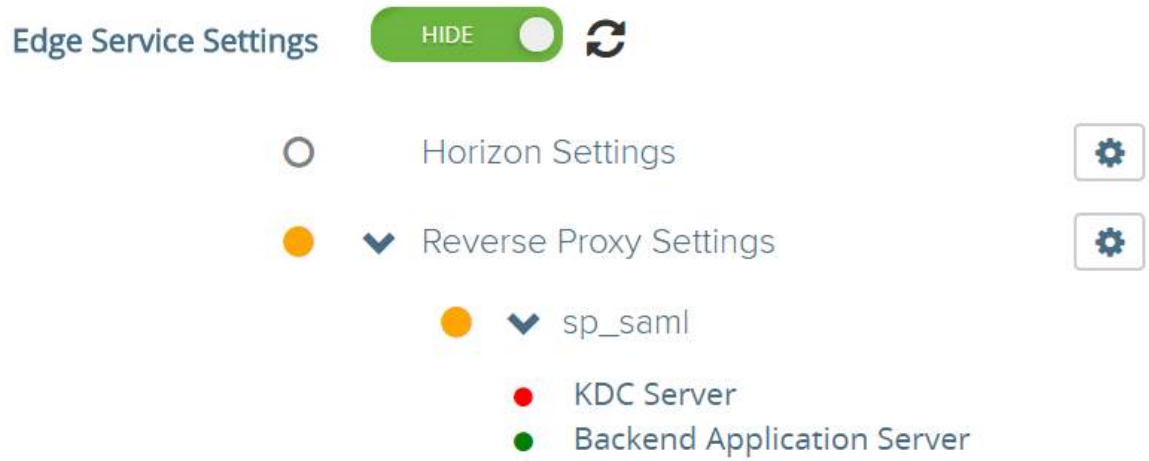
疑難排解錯誤：身分識別橋接

當您在環境中設定對 Kerberos 的憑證或對 Kerberos 的 SAML 時，可能會遭遇難題。您可以使用多種程序來診斷和修正這些問題。

監控 KDC 伺服器和後端應用程式伺服器的健全狀況。

您可以從管理員 UI 的 [Edge 設定] 中快速查看您部署的服務已設定、啟動並成功執行。

圖 7-3. 健全狀況檢查 - Reverse Proxy 設定



服務前方會顯示一個圓形。色彩編碼如下所示。

- 紅色圓形：如果狀態為紅色，則可能表示下列其中一種情況。
  - Unified Access Gateway 與 Active Directory 之間的連線問題
  - Unified Access Gateway 與 Active Directory 之間的連接埠封鎖問題。

    備註 確認 Active Directory 機器中已開放 TCP 和 UDP 連接埠 88。
  - 已上傳的 Keytab 檔案中主體名稱和密碼認證可能不正確。
- 綠色圓形：如果狀態為綠色，則表示 Unified Access Gateway 可以使用 Keytab 檔案中提供的認證來登入 Active Directory。

建立 Kerberos 內容時發生錯誤：時鐘誤差太大

此錯誤訊息：

```
ERROR:"wsportal.WsPortalEdgeService[createKerberosLoginContext: 119][39071f3d-9363-4e22-
a8d9-5e288ac800fe]: Error creating kerberos context.
Identity bridging may not work
javax.security.auth.login.LoginException: Clock skew too great"
```

顯示於 Unified Access Gateway 時間與 AD 伺服器時間顯著不同步時。請重設 AD 伺服器上的時間以符合 Unified Access Gateway 上的確切 UTC 時間。

建立 Kerberos 內容時發生錯誤：名稱或服務不明

此錯誤訊息：

```
wsportal.WsPortalEdgeService[createKerberosLoginContext: 133][]: Error creating kerberos
context.
Identity bridging may not work
javax.security.auth.login.LoginException: Name or service not known
```

顯示於 Unified Access Gateway 無法連線至設定的領域，或使用 Keytab 檔案中所提供的使用者詳細資料無法連線至 KDC 時。請確認下列項目：

- Keytab 檔案使用正確的 SPN 使用者帳戶密碼產生並上傳至 Unified Access Gateway
- 已將後端應用程式 IP 位址和主機名稱正確新增至主機項目。

接收使用者：user@domain.com 的 Kerberos Token 時發生錯誤，錯誤：Kerberos 委派錯誤：方法名稱：gss_acquire_cred_impersonate_name：未指定的 GSS 失敗。次要代碼可能會提供更多資訊

```
"Kerberos Delegation Error: Method name: gss_acquire_cred_impersonate_name: Server not
found in Kerberos database"
```

如果顯示此訊息，請檢查是否：

- 網域之間有信任關係。
- 目標 SPN 名稱已正確設定。

疑難排解錯誤：Cert-to-Kerberos

當您在環境中設定 Cert-to-Kerberos 時，可能會遭遇難題。您可以使用多種程序來診斷和修正這些問題。

錯誤訊息：內部錯誤。請連絡管理員

檢查 `/opt/vmware/gateway/logs/authbroker.log` 中的訊息

```
"OSCP validation of CN=clientCert, OU=EUC, O=<org name>, ST=<state name>, C=IN failed
with "Could not send OCSP request to responder: Connection refused (Connection
refused) , will attempt CRL validation"
```

這表示「X.509 憑證」中設定的 OCSP URL 無法連線或不正確。

OCSP 憑證無效時發生錯誤

```
"revocation.RevocationCheck: OSCP validation of CN=clientCert failed with "Could not
verify signing certificate for OCSP responder:http://asdkad01/ocsp". will attempt CRL
validation."
```

顯示於上傳了無效的 OCSP 憑證或是 OCSP 憑證已撤銷時。

OCSP 回應驗證失敗時發生錯誤

```
"WARN ocsp.BouncyCastleOCSPHandler: Failed to verify OCSP response:
CN=asdkAD01.Asdk.ADrevocation.RevocationCheck: 08/23 14:25:49,975" [tomcat-http--26]
WARN revocation.RevocationCheck: OSCP validation of CN=clientCert failed with "Could
not verify signing certificate for OCSP responder: http://asdkad01/ocsp". will attempt
CRL validation."
```

有時會在 OCSP 回應驗證失敗時顯示。

錯誤訊息：無法從工作階段擷取用戶端憑證：<sessionId>

如果顯示此訊息：

- 請檢查 X.509 憑證設定並判斷是否已設定
- 如果已設定 X.509 憑證設定：請檢查用戶端瀏覽器上安裝的用戶端憑證，以查看是否由 [X.509 憑證] 設定中 [根憑證和中繼 CA 憑證] 欄位上傳的相同 CA 所核發。

疑難排解端點符合性

當您在環境中部署端點符合性檢查提供者時，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。

備註 `Esmanager.log` 會記錄用於符合性檢查之裝置的 MAC 位址相關資訊。如果裝置具有多個 NIC 或切換至不同網路，則在識別用於端點符合性檢查的 MAC 位址時相當實用。

Unified Access Gateway 會顯示「不正確的用戶端認證」

Unified Access Gateway 會呼叫 OPSWAT API 以驗證所提供的用戶端金鑰和用戶端密碼。如果認證不正確，則不會儲存設定，從而導致

```
不正確的用戶端認證
```

錯誤。

確認 [使用者名稱] 和 [密碼] 欄位中輸入正確的用戶端金鑰與用戶端密碼。

若要產生用戶端認證，請在此處登錄您的應用程式：https://gears.opswat.com/o/app/register。

Unified Access Gateway 會顯示「DNS 無法解析主機 `https://gears.opswat.com`」

使用 Ping 命令來探索您區域 `gears.opswat.com` 的 IP 位址。

然後，使用來自 Ping 命令的 IP 位址以建立 `https://gears.opswat.com` 的 `/etc/hosts` 項目。從管理員 UI 導覽至 Horizon 設定並為 View Edge Service 提供**主機項目**中的值。

Unified Access Gateway 會顯示「連線至主機 `https://gears.opswat.com` 時要求逾時」

如果 UAG 中的 `gears.opswat.com` 主機項目設定錯誤或 `https://gears.opswat.com` 不接受連線要求，則可能會發生此情況。

疑難排解管理員 UI 中的憑證驗證

如果您在驗證 PEM 格式的憑證時發生錯誤，請查閱此處的錯誤訊息以取得更多資訊。

以下是產生錯誤的可能案例清單。

錯誤	問題
PEM 格式無效。可能是由於 BEGIN 格式錯誤。請參閱記錄以取得詳細資料。	PrivateKey BEGIN 憑證無效。
PEM 格式無效。例外狀況訊息：找不到 ---END RSA PRIVATE KEY。請參閱記錄以取得詳細資料。	PrivateKey END 憑證無效。
PEM 格式無效。例外狀況訊息：建立 RSA 私密金鑰時發生問題: java.lang.IllegalArgumentException: 無法從 byte[]: corrupted stream 建構序列 - 找到超出界限的長度。請參閱記錄以取得詳細資料。	憑證中的 PrivateKey 已損毀。
無法從 PEM 字串剖析憑證。請參閱記錄以取得詳細資料。	PublicKey BEGIN 憑證無效。
遇到格式錯誤的 PEM 資料。請參閱記錄以取得詳細資料。	PublicKey END 憑證無效。
遇到格式錯誤的 PEM 資料。請參閱記錄以取得詳細資料。	憑證中的 PublicKey 已損毀。
沒有目標/結尾憑證可供建置鏈結。	沒有目標/結尾憑證。
無法建置憑證鏈結路徑，所有目標憑證皆無效。可能缺少中繼憑證/根憑證。	沒有可供建置的憑證鏈結。
不明確的錯誤：找到多個憑證鏈結，但不確定要傳回哪一個	有多個憑證鏈結。
無法建置憑證鏈結路徑 CertificateExpiredException：憑證已於 *20171206054737GMT+00:00* 到期。請參閱記錄以取得詳細資料。	憑證已到期。

上傳採用 PEM 格式的憑證時遇到錯誤訊息「在資料流中偵測到未預期的資料」。	憑證鏈結的分葉和中繼之間遺失空白行或其他屬性。在分葉和中繼憑證之間新增空白行會解決此問題。
	圖 7-4. 範例
	`xICaEnL6VpPX/78whQYwvwt/Tv9XBZ0k7YXDK/umdaisLRbvfXknsuvCnQsH6qqF`
	`0wGjIChBWUMo0oHjqvbsezt3tkBigAVBRQHvFwY+3sAzm2fTYS5yh+Rp/BIAV0Ae`
	`cPUeybQ=`
	`-----END CERTIFICATE-----`
	
	`-----BEGIN CERTIFICATE-----`
	`MIIDxTCCAq2gAwIBAgIQAqxcJmoLQJuPC3nyrkYldzANBgkqhkiG9w0BAQUFADBs`
	`MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3`

疑難排解防火牆和連線問題

您可以從 Unified Access Gateway 執行個體透過各種工具和命令 (例如 tcpdump 和 curl) 來監控、測試和疑難排解網路問題，例如防火牆和連線問題。

安裝並執行 tcpdump

tcpdump 是一項命令列工具，可用來分析 TCP 封包以進行疑難排解和測試。

如果您尚未在 Unified Access Gateway 執行個體上安裝 tcpdump，請從命令列執行下列命令以安裝 tcpdump：

```
/etc/vmware/gss-support/install.sh
```

下列範例顯示 tcpdump 的使用方式：

- 執行下列命令以監控通過特定連接埠的流量。

  備註 如果您指定連接埠 8443，請確定外部防火牆並未封鎖 UDP 8443。

  a `tcpdump -i eth0 -n -v udp port 8443`

  b `tcpdump -i eth0 -n -v tcp port 8443`

  c `tcpdump -i any -n -v port 22443`

- 執行下列命令以追蹤 RADIUS 伺服器往來於 Unified Access Gateway 的封包：

```
nslookup <radius-server-hostname>
tracepath <radius-server-hostname>
tcpdump -i any -n -v port 1812
```

- 執行下列命令以追蹤 RSA SecurID 伺服器往來於 Unified Access Gateway 的封包：

```
nslookup <rsa-auth-server-hostname>
tracepath <rsa-auth-server-hostname>
```

使用 curl 命令

您也可以使用 curl 命令擷取網路連線的相關資訊。

- 執行下列命令以測試後端連線伺服器或 Web 伺服器的連線：

  `curl -v -k https://<hostname-or-ip-address>:443/`

  您可以在 esmanager.log 檔案中檢視後端伺服器的連線問題：

```
07/14 07:29:03,882[nioEventLoopGroup-7-1]ERROR
view.ViewEdgeService[onFailure: 165][]: Failed to resolve hostname
address in proxyDestinationUrl:xref:mbxxx-cs.xyz.in
```

- 您無法使用 `tcpdump` 測試後端虛擬桌面平台 (例如 PCoIP 4172 和 Blast 22443) 的連線，因為在工作階段準備就緒之前，桌面平台不會接聽這些連接埠號碼。請檢視記錄以確認這些連接埠是否發生連線失敗。
  - 針對 Horizon 架構通道 TCP 連線，請執行下列命令：

    ```
    curl -v telnet://<virtualdesktop-ip-address>:32111
    ```

  - 針對 Horizon MMR/CDR TCP 連線，請執行下列命令：

    ```
    curl -v telnet://<virtualdesktop-ip-address>:9427
    ```

  - 執行下列命令以測試從 Unified Access Gateway 到虛擬桌面平台的連接埠連線。執行此命令之前，請確保對虛擬桌面平台的工作階段處於作用中狀態。

    ```
    curl -v telnet://<virtualdesktop-ip-address>:22443
    ```

PowerShell 命令

從 PowerShell 命令列執行下列命令以監控特定連接埠的連線：

```
1  Test-NetConnection <uag-hostname-or-ip-address> -port 443
2  Test-NetConnection <uag-hostname-or-ip-address> -port 8443
3  Test-NetConnection <uag-hostname-or-ip-address> -port 4172
```

疑難排解根使用者登入問題

如果您使用正確的使用者名稱和密碼，以根使用者身分登入 Unified Access Gateway 主控台，但卻收到「登入不正確」錯誤時，請檢查鍵盤對應問題，並重設根密碼。

發生登入錯誤的原因有以下幾種：

- 所使用的鍵盤並未根據 Unified Access Gateway 的鍵盤定義正確對應特定的密碼字元
- 密碼已過期。部署 OVA 檔案之後根密碼已過期 365 天。
- 在部署應用裝置時未正確設定密碼。這是舊版 Unified Access Gateway 的已知問題。
- 忘記密碼。

若要測試鍵盤的對應字元是否正確，請嘗試在「登入:」使用者名稱提示出現時輸入密碼。這可讓您檢視每個密碼字元，並找出解譯錯誤的字元。

若是其他原因，請重設應用裝置的根密碼。

備註 若要重設根密碼，您必須：

- 擁有 vCenter 的登入存取權
- 知道 vCenter 的登入密碼
- 擁有存取應用裝置主控台的權限

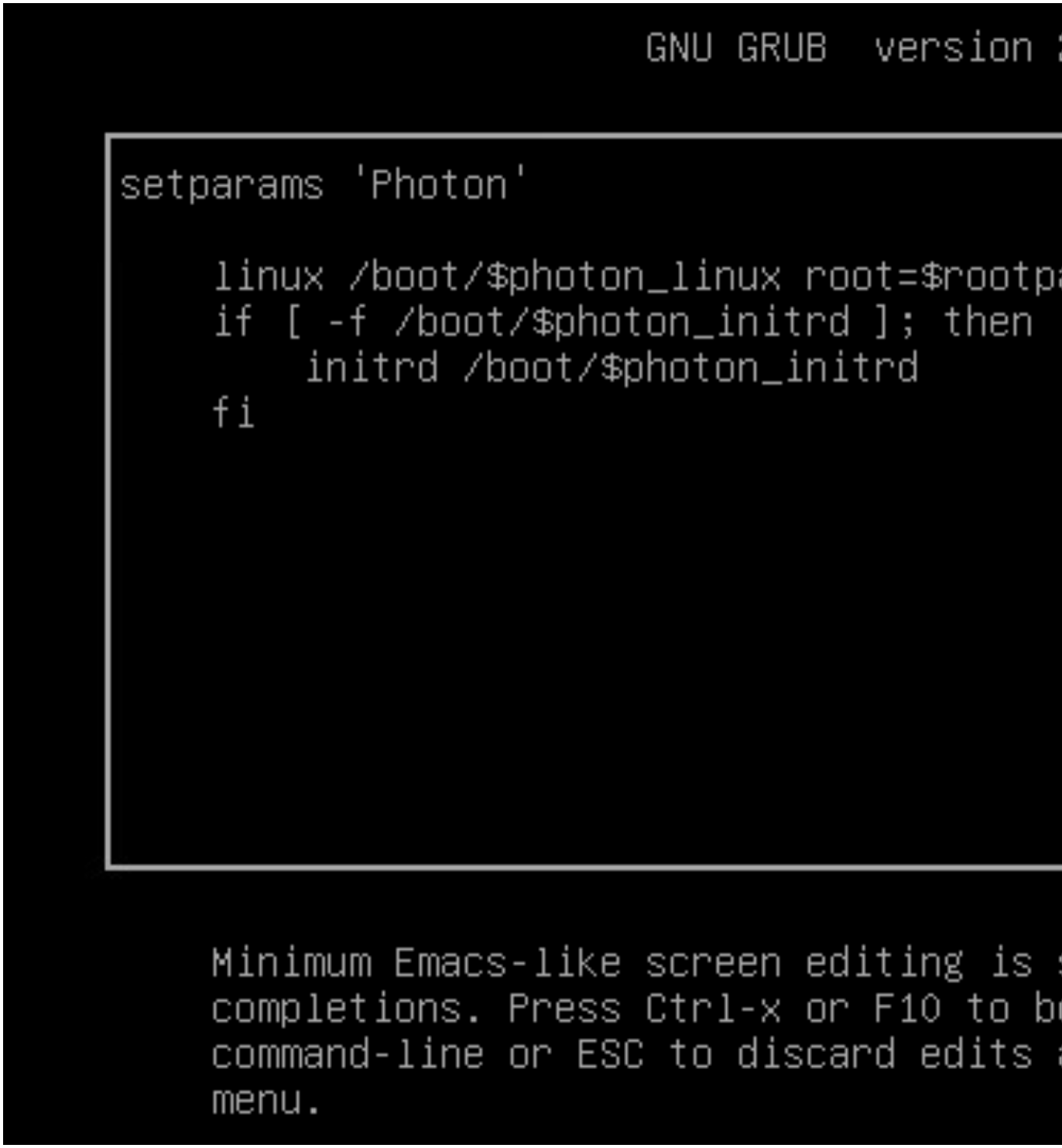
如果您為應用裝置設定了 Grub 2 開機載入器功能表密碼，則需要在此程序中輸入該密碼。

程序

1 從 vCenter 重新啟動應用裝置，並立即連線至主控台。

2 當 Photon OS 啟動顯示畫面顯示時，按下 e 來輸入 GNU GRUB 編輯功能表

3 在 GNU GRUB 中編輯功能表中，移至開頭為 `linux` 行的結尾，接著新增空格，然後輸入 `/boot/$photon_linux root=$rootpartition rw init=/bin/bash`。新增這些值後，GNU GRUB 編輯功能表看起來應完全類似下列：



備註 對於 FIPS 應用裝置，這行應該是 `linux /boot/$photon_linux root=$rootpartition rw init=/bin/bash fips=1`

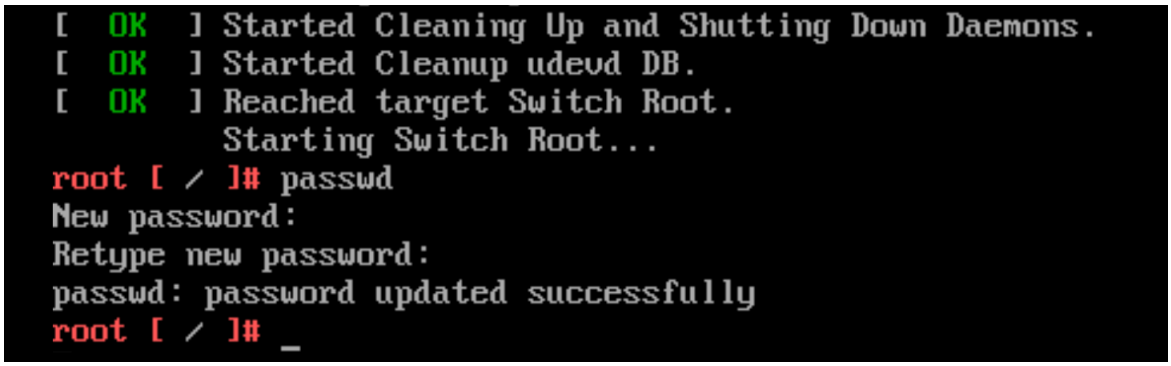
4 按 F10 鍵，然後在 bash 命令提示字元中輸入 **passwd** 來變更密碼。

```
passwd

New password:

Retype new password:

passwd: password updated successfully
```



5 將應用裝置重新開機 `reboot -f`

- 在應用裝置重新開機後，使用新設定的密碼以根使用者身分登入。

關於 Grub2 密碼

您可以在根使用者登入中使用 Grub2 密碼。

從 Unified Access Gateway 3.1 開始，依預設系統會設定 Grub2 編輯密碼。

使用者名稱為 root，而密碼則與您在部署 Unified Access Gateway 時所設定的根密碼相同。此密碼一律不會重設，除非您登入機器並明確進行重設。

備註 透過任何命令登入機器並手動變更根密碼時將不會重設 Grub2 密碼。這兩個密碼為互斥。系統僅在部署期間才會為兩者設定相同的密碼 (使用 UAG 3.1 版及更新版本時)。

從 Unified Access Gateway 應用裝置收集記錄

從管理員 UI 的 [支援設定] 區段下載 `UAG-log-archive.zip` 檔案。該 ZIP 檔案包含來自 Unified Access Gateway 應用裝置的所有記錄。

設定記錄層級

您可以透過管理員 UI 來管理記錄層級設定。移至**支援設定**頁面，並選取**記錄層級設定**。可以產生的記錄層級為「資訊」、「警告」、「錯誤」和「偵錯」。記錄層級依預設會設定為「資訊」。

記錄層級所收集資訊類型的說明如下所示。

表 7-6. 記錄層級

層級	收集的資訊類型
資訊	「資訊」層級指出可突顯服務進度的資訊訊息。
錯誤	「錯誤」層級指出可能仍允許服務繼續執行的錯誤事件。
警告	「警告」層級指出可能有害但通常可復原或可忽略的情況。
偵錯	指定一般有助於偵錯問題的事件、檢視或操縱應用裝置的內部狀態，以及在您的環境中測試部署案例。
追蹤	指出 Unified Access Gateway 統計資料收集的相關資訊、從 Unified Access Gateway 傳送至後端伺服器的要求詳細資料等。

收集記錄

從管理員 UI 的 [支援設定] 區段下載記錄 ZIP 檔案。

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 7-7. 包含有助於疑難排解之系統資訊的檔案

檔案名稱	說明	Linux 命令 (如果適用)
`version.info`	包含作業系統、核心、GCC 和 Unified Access Gateway 應用裝置的版本。	
`ipv4-forwardrules`	在應用裝置上設定的 IPv4 轉送規則。	
`df.log`	包含應用裝置上的磁碟空間使用量相關資訊。	`df -a -h --total`
`netstat.log`	包含開啟的連接埠和現有 TCP 連線的相關資訊。	`netstat -anop`
`netstat-s.log`	從應用裝置建立時開始的網路統計資料 (已傳送/已接收的位元組等)。	`netstat -s`
`netstat-r.log`	在應用裝置上建立的靜態路由。	`netstat -r`
`uag_config.json`、`uag_config.ini`、`uagstats.json`	Unified Access Gateway 應用裝置的完整組態，以 json 和 INI 檔案的形式顯示所有設定。	
`ps.log`	包含下載記錄時正在執行的處理程序。	`ps -elf --width 300`
`ifconfig.log`	應用裝置的網路介面組態。	`ifconfig -a`
`free.log`	下載記錄時的 RAM 可用性。	`free`
`top.log`	下載記錄時依記憶體使用量排序的處理程序清單。	`top -b -o %MEM -n 1`
`iptables.log`	IPv4 的 IP 表格。	`iptables-save`
`ip6tables.log`	IPv6 的 IP 表格。	`ip6tables-save`
`w.log`	運作時間、機器目前的使用者及其處理程序的相關資訊。	`w`

表 7-7. 包含有助於疑難排解之系統資訊的檔案 (續)

檔案名稱	說明	Linux 命令 (如果適用)
systemctl.log	目前在應用裝置上執行的服務清單	systemctl
resolv.conf	用來將本機用戶端直接連線至所有已知的 DNS 伺服器	
hastats.csv	包含每個節點的統計資料和每個後端類型 (Edge Service Manager、VMware Tunnel、Content Gateway) 的總統計資料資訊	
system_logs_archive	目錄包含下列記錄檔：cpu.info、mem.info、sysctl.log 和 journalctl_archive。	
cpu.info	包含從 /proc/cpuinfo 收集的虛擬機器的 CPU 資訊。	
mem.info	包含虛擬機器記憶體的相關資訊，例如從 /proc/meminfo 收集的可用記憶體總計、可用的記憶體等。	
sysctl.log	包含虛擬機器所有核心參數的相關資訊。	sysctl -a
journalctl_archive	包含 journalctl 記錄資訊的檔案，其資訊會跨越下載封存的時間為止 7 天的時間。 例如，如果管理員在今天上午 9:00 從 Unified Access Gateway 管理員 UI 下載記錄封存，則封存會包含到上午 9:00 為止過去 7 天的資訊。 如果收集的記錄大小小於或等於 25 MB，則只會產生單一檔案 journalctl.log。如果收集的記錄大小超過 25 MB，則會使用多個 journalctl.log 檔案來建立 journalctl_archive 資料夾 。	journalctl -x --since '1 week ago'
journald.conf	包含 journalctl 記錄的組態資訊。	
system-logs-collection-status.log	包含資訊指出是否成功收集下列記錄檔：cpu.info、mem.info、sysctl.log 和 journalctl_archive。	
hosts	包含 /etc/hosts 項目。	
firstboot	包含 Unified Access Gateway 第一次開機時產生的資訊。	
subsequentboot	包含 Unified Access Gateway 後續重新開機期間產生的資訊。	
trustedCertificatesStore.log	包含在 Unified Access Gateway 上傳受信任憑證時的憑證處理狀態相關資訊。	
vami-ovf.log	包含部署期間 Unified Access Gateway 應用裝置的組態相關資訊，例如 OVF 內容、網路等。	

表 7-8. Unified Access Gateway 的記錄檔

檔案名稱	說明	Linux 命令 (如果適用)
supervisord.log	主管 (Edge Service Manager 的管理員、管理員和 AuthBroker) 記錄。	
esmanager-x.log、esmanager-std-out.log	一或多個 Edge Service Manager 記錄，顯示在應用裝置上執行的後端處理程序。	
audit.log	所有管理員使用者作業的稽核記錄。	
authbroker.log	包含處理 Radius 和 RSA SecurID 驗證之 AuthBroker 處理程序所產生記錄訊息。	
admin.log、admin-std-out.log	管理員 GUI 記錄。包含在連接埠 9443 上提供 Unified Access Gateway REST API 之處理程序的記錄訊息。	
bsg.log	包含 Blast 安全閘道的記錄訊息。	
SecurityGateway_xxx.log	包含 PCoIP 安全閘道的記錄訊息。	
utserver.log	包含 UDP 通道伺服器所產生的記錄訊息。	
activeSessions.csv	作用中 Horizon 或 WRP 工作階段的清單。	
haproxy.conf	包含用於 TLS 連接埠共用的 HA Proxy 組態參數。	
vami.log	包含在部署期間執行 vami 命令以設定網路介面所產生的記錄訊息。	
content-gateway.log、content-gateway-wrapper.log、0.content-gateway-YYYY-mm.dd.log.zip	包含來自 Content Gateway 的記錄訊息。	
admin-zookeeper.log	包含用來儲存 Unified Access Gateway 組態之資料層的相關記錄訊息。	
package-updates.log	包含有關套用至 Unified Access Gateway 版本 (已在您的環境中發行並部署) 之套件更新 (OS 和 Unified Access Gateway) 狀態的記錄訊息。	
tunnel.log	包含作為 XML API 處理的一部分之通道處理程序的記錄訊息。您必須在 Horizon 設定中啟用通道才能查看此記錄。	
tunnel_snap.log	包含的資訊會指出是否成功收集 VMware Tunnel 伺服器和 Proxy 記錄。	
tunnel-snap.tar.gz	包含 VMware Tunnel 伺服器和 Proxy 記錄檔的 Tarball。	
appliance-agent.log	應用裝置代理程式 (用以啟動 Workspace ONE UEM 服務) 記錄。	
config.yml	包含 Content Gateway 組態和記錄層級詳細資料。	

表 7-8. Unified Access Gateway 的記錄檔 (續)

檔案名稱	說明	Linux 命令 (如果適用)
smb.conf	包含 SMB 用戶端組態。	
smb-connector.conf	包含 SMB 通訊協定和記錄層級詳細資料。	

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。

表 7-9. Unified Access Gateway 記錄檔的記錄輪替資訊

記錄檔案名稱	位置	內容
admin-zookeeper.log	/opt/vmware/gateway/conf/log4j-admin.properties	log4j.appender.zookeeper.MaxFileSize=10MB log4j.appender.zookeeper.MaxBackupIndex=5
admin.log	/opt/vmware/gateway/conf/log4j-admin.properties	log4j.appender.default.MaxFileSize=10MB log4j.appender.default.MaxBackupIndex=5
audit.log	/opt/vmware/gateway/conf/log4j-admin.properties	log4j.appender.adminAudit.MaxFileSize=10MB log4j.appender.adminAudit.MaxBackupIndex=5
authbroker.log	/opt/vmware/gateway/conf/log4j-authbroker.properties	appender.rollingFile.policies.size.size=10MB appender.rollingFile.strategy.max=5
bsg.log	/opt/vmware/gateway/lib/bsg/absg.properties	logFilesize=8*1024*1024 logBackupCount=5
esmanager.log	/opt/vmware/gateway/conf/log4j-esmanager.properties	log4j.appender.default.MaxFileSize=25MB log4j.appender.default.MaxBackupIndex=10
tunnel.log	/opt/vmware/gateway/conf/log4j-tunnel.properties	log4j.appender.default.MaxFileSize=25MB log4j.appender.default.MaxBackupIndex=5
檔案存在於 /var/log/journal	/etc/systemd/journald.conf	SystemMaxUse=1G
keepalived.log	/etc/logrotate.d/keepalived	rotate 5 size 5M
haproxy.log	/etc/logrotate.d/haproxy	rotate 5 size 25M

表 7-9. Unified Access Gateway 記錄檔的記錄輪替資訊 (續)

記錄檔案名稱	位置	內容
auth.log	/etc/logrotate.d/auth	rotate 10 大小 10M
/var/log/messages /var/log/cron	/etc/logrotate.d/messages_and_cron	rotate 20 size 50M maxage 30

Syslog 格式和事件

Syslog 伺服器會記錄 Unified Access Gateway 應用裝置上發生的事件。這些事件會擷取在具有特定格式的記錄檔中。為了協助您瞭解產生事件時所擷取的部分資訊，此主題會列出事件、事件範例和 Syslog 格式。

Syslog 格式

Syslog 稽核事件會記錄在 audit.log 中，而 Syslog 事件會記錄在 admin.log 和 esmanager.log 檔案中。所有記錄檔會遵循特定格式。

下表列出記錄檔、其各自的格式和欄位說明：

備註 產生的事件會遵循記錄格式；但這些事件可能僅包含格式中呈現的部分欄位。

記錄檔	記錄格式
■ audit.log ■ admin.log	<timestamp> <UAG hostname> <app name> <thread id> <log level> <file name> <function name> <line no.> <log message>
esmanager.log	<timestamp> <UAG hostname> <app name> <thread id> <log level> <file name> <function name> <line no.> <client IP> <username> <session type> <session id> <log message>

欄位	說明
<timestamp>	指出在 Syslog 伺服器中產生和記錄事件的時間。
<UAG hostname>	Unified Access Gateway 應用裝置的主機名稱。
<appname>	產生事件的應用程式。 **備註** 根據記錄檔，此欄位的值如下所示：UAG-AUDIT、UAG-ADMIN 和 UAG-ESMANAGER。
<thread id>	產生事件的執行緒識別碼。

欄位	說明
<log level>	記錄訊息中收集的資訊類型。 如需關於記錄層級的詳細資訊，請參閱從 Unified Access Gateway 應用裝置收集記錄。
<file name>	從中產生記錄的檔案名稱。
<function name>	從中產生記錄的檔案內函數名稱。
<line no.>	檔案中記錄的行號。
<client IP>	傳送要求至 Unified Access Gateway 應用裝置之元件 (例如 Horizon Client、負載平衡器等) 的 IP 位址。
<session type>	為其建立工作階段的 Edge 服務 (例如 Horizon 和 Web 反向 Proxy)。 如果工作階段適用於 Web 反向 Proxy，則系統會將工作階段類型稱為 WRP-*<instanceId>*。 **備註** *<instanceId>* 是 Web 反向 Proxy Edge 服務的執行個體識別碼。
<session id>	工作階段的唯一識別碼。
<log message>	提供事件中所發生項目的摘要。

Syslog 稽核事件

下表說明稽核事件與範例：

事件說明	事件範例
當管理員登入 Unified Access Gateway 管理員 UI、在管理員 UI 內執行組態變更，或登出管理員 UI 時會記錄事件。	■ Sep 8 08:50:04 *UAG Name* UAG-AUDIT: [qtp1062181581-73]INFO utils.SyslogAuditManager[logAuditLog: 418] - LOGIN_SUCCESS: SOURCE_IP_ADDR=*Client_Machine_IP_Address* USERNAME=admin ■ Sep 8 08:50:13 *UAG Name* UAG-AUDIT: [qtp1062181581-79]INFO utils.SyslogAuditManager[logAuditLog: 418] - LOGOUT_SUCCESS: SOURCE_IP_ADDR=*Client_Machine_IP_Address* USERNAME=admin ■ Sep 8 08:52:24 *UAG Name* UAG-AUDIT: [qtp1062181581-80]INFO utils.SyslogAuditManager[logAuditLog: 418] - CONFIG_CHANGE: SOURCE_IP_ADDR=*Client_Machine_IP_Address* USERNAME=admin: CHANGE=allowedHostHeaderValues:(null->) - tlsSyslogServerSettings:(null->[]) - dns:(null->) - sshPublicKeys:(null->[]) - ntpServers:(- null->) - adminPasswordExpirationDays:(90->50) - dnsSearch:(null->) - fallBackNtpServers:(null->) - ■ Sep 8 07:32:01 *UAG Name* UAG-ADMIN: [qtp1062181581-27]INFO utils.SyslogManager[save: 57] - SETTINGS:CONFIG_CHANGED:allowedHostHeaderValues:(null->) - tlsSyslogServerSettings:(null->[]) - dns:(null->) - sessionTimeout:(9223372036854775807->36000000) - sshPublicKeys:(null->[]) - ntpServers:(null->) - dnsSearch:(null->) - fallBackNtpServers:(null->) -

Syslog 事件

下表說明系統事件與範例：

事件說明	事件範例
當 Unified Access Gateway 內設定的任何 Edge 服務相應地啟動和停止時會記錄事件。	在下列事件範例中，*UAG 名稱*為在管理員 UI 的**系統組態**中設定為 Unified Access Gateway 一部分的選項： ■ `Sep 9 05:36:55 UAG Name UAG-ESMANAGER: [Curator-QueueBuilder-0]INFO utils.SyslogManager[start: 355][][][][] - Edge Service Manager : started` ■ `Sep 9 05:36:54 UAG Name UAG-ESMANAGER: [Curator-QueueBuilder-0]INFO utils.SyslogManager[stop: 1071][][][][] - Edge Service Manager : stopped`
在 Unified Access Gateway 管理員 UI 上啟用或停用 Web 反向 Proxy 設定時會記錄事件。	■ `Sep 8 09:34:52 UAG Name UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[stopService: 287][][][][] - Reverse Proxy Edge Service with instance id 'wiki' : stopped` ■ `Sep 8 12:08:18 UAG Name UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[startService: 211][][][][] - Reverse Proxy Edge Service with instance id 'wiki' : started`

事件說明	事件範例
在 Unified Access Gateway 管理員 UI 上啟用或停用 Horizon Edge 服務設定時會記錄事件。	■ Sep 8 09:15:21 *UAG Name* UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[startService: 335][][][][] - Horizon Edge Service : started ■ Sep 8 09:15:07 *UAG Name* UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[stopService: 702][][][][] - Horizon Edge Service : stopped
建立 Horizon 工作階段時，系統會記錄包含工作階段建立、使用者登入、使用者驗證、桌面平台啟動與工作階段終止等事件。	雖然該流程會記錄多個事件，但範例事件會包括登入案例、使用者驗證成功和失敗案例，以及驗證逾時。在其中一個範例中，Horizon 已設定為使用 RADIUS 驗證方法： ■ Sep 8 07:28:46 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[write: 163] [*Client_Machine_IP_Address*][][][5a0b-***-7cfa] - Created session : 5a0b-***-7cfa ■ Sep 8 07:28:51 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[putUserNameInMDC: 494] [*Client_Machine_IP_Address*][testradius] [Horizon][5a0b-***-7cfa] - UAG sessionId:5a0b-***-7cfa username:testradius ■ Sep 8 07:28:51 *UAG Name* UAG-ESMANAGER: [jersey-client-async-executor-1]INFO utils.SyslogManager[logMessage: 190] [*Client_Machine_IP_Address*][testradius] [Horizon][5a0b-***-7cfa] - Authentication successful for user testradius.**驗證類型**：RADIUS-AUTH，**子類型**：**密碼** ■ Sep 8 07:28:52 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[processDocument: 110] [*Client_Machine_IP_Address*][testradius] [Horizon][5a0b-***-7cfa] - Authentication attempt response - partial ■ Sep 8 07:29:02 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[putUserNameInMDC: 494] [*Client_Machine_IP_Address*][*user name*] [Horizon][5a0b-***-7cfa] - UAG sessionId:5a0b-***-7cfa username:*user name* ■ Sep 8 07:29:02 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[processXmlString: 190] [*Client_Machine_IP_Address*][*user name*] [Horizon][5a0b-***-7cfa] - Authentication attempt - LOGIN initiated ■ Sep 8 07:29:03 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO

事件說明	事件範例
	utils.SyslogManager[processDocument: 110] [*Client_Machine_IP_Address*][*user name*] [Horizon][5a0b-***-7cfa] - Authentication attempt response - ok ■ Sep 8 07:29:03 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[setAuthenticated: 384] [*Client_Machine_IP_Address*][*user name*] [Horizon][5a0b-***-7cfa] - HORIZON_SESSION:AUTHENTICATED:Horizon session authenticated - Session count:9, Authenticated sessions: 2 ■ Sep 8 07:29:04 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-41-1]INFO utils.SyslogManager[onSuccess: 109] [*Client_Machine_IP_Address*][*user name*] [Horizon][5a0b-***-7cfa] - Horizon Tunnel connection established ■ Sep 8 07:29:16 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[resolveHostName: 234] [*Client_Machine_IP_Address*][*user name*] [Horizon][5a0b-***-7cfa] - Accessing virtual/rdsh desktop using protocol BLAST with IP Address *IP_Address* ■ Sep 8 07:29:16 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-42-1]INFO utils.SyslogManager[onSuccess: 293] [*Client_Machine_IP_Address*][*user name*] [Horizon][5a0b-***-7cfa] - BSG route 5504-***-2905 with auth token Ob6NP-***-aEEqK added ■ Sep 8 07:29:55 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-46-1]INFO utils.SyslogManager[terminateSession: 450] [*Client_Machine_IP_Address*][*uesr name*] [Horizon][5a0b-***-7cfa] - HORIZON_SESSION:TERMINATED:Horizon Session terminated due to logout - Session count:9, Authenticated sessions: 2

Secure Email Gateway

Secure Email Gateway 會設定為遵循 Syslog 組態，此組態則會在 Unified Access Gateway 系統設定中進行設定。依預設，只有 Secure Email Gateway 中的 `app.log` 內容會以 Syslog 事件的形式來觸發。

如需關於 Syslog 組態的詳細資訊，請參閱設定 Unified Access Gateway 系統設定。

VMware Tunnel

如需詳細資訊，請參閱 VMware Docs 的《VMware Workspace ONE UEM 產品說明文件》中的〈存取記錄和 Syslog 整合〉和〈設定 VMware Tunnel〉。

匯出 Unified Access Gateway 設定

從管理員 UI 匯出 JSON 和 INI 格式的 Unified Access Gateway 組態設定。

您可以匯出所有 Unified Access Gateway 組態設定，並將其儲存為 JSON 或 INI 格式。您可以透過 Powershell 指令碼，使用匯出的 INI 檔案來部署 Unified Access Gateway。

程序

1 導覽至**支援設定 > 匯出** Unified Access Gateway 設定。

2 按一下 **JSON** 或 **INI**，以想要的格式匯出 Unified Access Gateway 設定。若要同時以這兩種格式儲存設定，請按一下**記錄封存**按鈕。

依預設檔案會儲存在您的 [下載] 資料夾中。

匯入 Unified Access Gateway 設定

Unified Access Gateway 管理員 UI 提供選項來以 JSON 格式匯出組態設定。以 JSON 格式匯出組態設定之後，您可以使用匯出的 JSON 檔案來設定新部署的 Unified Access Gateway 應用裝置版本。

程序

1 導覽至**支援設定 > 匯出 Unified Access Gateway 設定**。

2 按一下 JSON 以使用 JSON 格式匯出 Unified Access Gateway 設定。

依預設檔案會儲存在您的 [下載] 資料夾中

3 刪除舊的 Unified Access Gateway 應用裝置或將它置於靜止模式以稍後將其刪除。

4 部署新版的 Unified Access Gateway 應用裝置

5 在**匯入設定**區段按一下**選取**，匯入您稍早匯出的 JSON 檔案。

6 按一下**瀏覽**並導覽至先前匯出的 JSON 檔案，然後按一下**匯入**。

疑難排解錯誤：Content Gateway

當您在環境中設定 Content Gateway 時，可能會遭遇難題。您可以使用此程序來診斷和修正問題。

使用在 NetApp 伺服器上主控之共用的使用者同步、下載和上傳問題。

1 登入 Workspace ONE UEM Console。

2 導覽至 **Content Gateway 組態**頁面。

3 在**自訂閘道設定**區段中，按一下**新增列**。

4 在顯示的表格中，輸入下列值：

- **機碼** = `aw.fileshare.jcifs.active`
- **類型** = `Boolean`
- **值** = `true`

  預設值為 `false`。

5 按一下**儲存**。

6 在 Unified Access Gateway 管理員 UI 上，導覽至 **Content Gateway 設定**頁面。

7 按一下**儲存**。

備註 在儲存 Unified Access Gateway 管理員 UI 上的設定後，會從 Workspace ONE UEM Console 中擷取 Content Gateway 組態，並重新啟動 Content Gateway 服務。

若要讓 Content Gateway 組態變更生效，您必須更新 Workspace ONE UEM Console 中的**值**，然後儲存 Unified Access Gateway 管理員 UI 中的 Content Gateway 設定。

疑難排解高可用性

當您在環境中設定高可用性時，可能會遭遇難題。您可以使用多種程序來診斷和修正這些問題。

1 登入 Unified Access Gateway 主控台。

2 執行 `ip addr` 命令來檢查是否將設定的虛擬 IP 位址指派至 eth0 介面。

3 確保指派的該虛擬 IP 位址在與 eth0 介面相同的子網路內。確保可從用戶端電腦與它連接。如果有連線問題，則可能是因為虛擬 IP 位址不是唯一的，並且已指派給實體或虛擬機器。

4 在記錄服務包的 `haproxy.conf` 檔案中，與目前叢集相關的組態中可供使用。例如，

```
server uag1 127.0.0.1:XXXX .....
server uag2 <IP of machine 2>:XXXX ....
server uag3 <IP of machine 3>:XXXX ....
```

後端組態會基於 Unified Access Gateway 上進行的設定

- `lb_esmanageris` 用於 Horizon 和 Web 反向 Proxy 使用案例。
- `lb_cg_server` 用於 Content Gateway 使用案例。
- `lb_tunnel_server` 用於通道使用案例。

5 在記錄服務包的 `haproxy.conf` 檔案中，您可以找到有關用戶端連線來源、傳送的對應連線和處理連線的 Unified Access Gateway 伺服器的詳細資料。例如，

```
2018-11-27T07:21:09+00:00 ipv6-localhost haproxy[15909]:
                incoming:::ffff:<IP of Client:xxxx> backend:lb_esmanager
```

```
connecting-server:uag2/<IP of uag2> connecting-through:<IP of primary
node:xxxx> wait-time:1 connect-time:0 total-incoming:1 total-outgoing:1
total-to-server:1
```

6 若要檢視統計資料，請參閱從 Unified Access Gateway 應用裝置收集記錄。

表 7-10. CSV 檔案的範例

資料行名稱	說明
scur	指出此伺服器目前處理的並行連線數目。
smax	此伺服器在目前運作時間處理的並行連線數目上限。
stot	指出此伺服器在目前運作時間處理的連線數目總計。
bin	指出傳送至此伺服器的位元組總數。
bout	指出從此伺服器接收的位元組總數。
狀態	指出伺服器的狀態。例如，運作中或關閉。這會基於在此伺服器上執行的上次健全狀況檢查。

7 在下列情況下，會出現多個主要節點選取問題。

- 在節點上設定、要形成叢集的不同群組 ID 或虛擬 IP 位址。
- 虛擬 IP 位址和 eth0 位於不同子網路中。
- Unified Access Gateway 上的多個 NIC 設定在相同的子網路內。

安全性的疑難排解：最佳做法

服務在您的 Web 伺服器中偵測到負載平衡裝置時，這項關於網路的額外資訊將是弱點。您可以使用多種程序來診斷和修正這些問題。

系統會使用不同的技術來偵測是否有負載平衡裝置存在，包括 HTTP 標頭分析，以及對 IP 存留時間 (TTL) 值、IP 識別 (ID) 值和 TCP 初始序號 (ISN) 的分析。要判定負載平衡器後方的確切 Web 伺服器數目很難，因此報告的數字可能不精確。

此外，已知 Netscape Enterprise Server 3.6 版在伺服器接收到多個要求時，會在 HTTP 標頭中顯示錯誤的 `"Date:"` 欄位。這使得服務難以藉由分析 HTTP 標頭來判斷是否有負載平衡裝置存在。

此外，在執行掃描時，對 IP ID 和 TCP ISN 值分析所產生的結果可能因網路狀況不同而改變。入侵者可利用此弱點，使用此資訊與其他幾項資訊對您的網路發動精心設計的攻擊。

備註 如果負載平衡器後方的 Web 伺服器不相同，則 HTTP 弱點的掃描結果可能每次都不盡相同。

- Unified Access Gateway 為應用裝置，通常安裝在非軍事區 (DMZ) 中。下列步驟可協助您防止弱點掃描器對 Unified Access Gateway 偵測此問題。
  - 若要防止根據 HTTP 標頭分析來偵測是否有負載平衡裝置存在，您應使用網路時間通訊協定 (NTP) 將所有主機上 (至少在 DMZ 中) 的時鐘同步。

- 若要防止藉由分析 IP TTL 值、IP ID 值和 TCP ISN 值進行偵測，您可以使用會進行 TCP/IP 實作而為這些值產生隨機數字的主機。但是，現今大多數的作業系統都未隨附此類 TCP/IP 實作。

受 Unified Access Gateway 管理員 UI 設定變更影響的使用者工作階段

當某些 Unified Access Gateway 管理員 UI 設定變更時，現有的 XMLAPI 工作階段 (Unified Access Gateway 工作階段) 可能會終止，因此使用者無法存取已啟動的桌面平台和應用程式。變更的設定可能僅會影響已啟動的桌面平台和應用程式，或者同時影響 XMLAPI 和桌面平台或應用程式工作階段。

您必須計畫在維護時段內變更 Unified Access Gateway 管理員 UI 設定。

管理員 UI 設定	影響現有 Unified Access Gateway 工作階段	影響已啟動的桌面平台和應用程式
匯入設定 您可以使用此管理員 UI 區段，將先前匯出的 JSON 檔案 (來自先前的部署) 匯入，以設定新部署的 Unified Access Gateway 應用裝置版本。	Yes	Yes
Horizon 設定		
啟用 PCOIP	No	Yes
啟用 Blast	No	Yes
啟用 UDP 通道伺服器	No	Yes
啟用通道	Yes	Yes
停用 Horizon Edge 服務	Yes	Yes
驗證設定		
X.509 憑證	Yes	Yes
系統組態		
地區設定	Yes	Yes
加密套件	Yes	Yes
啟用 TLS 1.0	Yes	Yes
啟用 TLS 1.1	Yes	Yes
啟用 TLS 1.2	Yes	Yes
啟用 TLS 1.3	Yes	Yes
Syslog URL	Yes	Yes
Syslog 稽核 URL	Yes	Yes
要快取的 Cookie	Yes	Yes

管理員 UI 設定		影響現有 Unified Access Gateway 工作階段	影響已啟動的桌面平台和應用程式
監控間隔		Yes	Yes
網路設定	Yes		Yes
高可用性設定	Yes		Yes
TLS 伺服器憑證設定 (僅限網際網路對向介面)	Yes		Yes