Horizon Client 和 Agent 安全性

Horizon Client 3.x/4.x/5.x 和 View Agent 6.2.x/Horizon Agent 7.x

2019 年 12 月

VMware Horizon 7 7.11

vmware®

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

如果您對於本文件有任何意見，歡迎寄至：

docfeedback@vmware.com

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

目錄

Horizon Client 和 Agent 安全性

《Horizon Client 和 Agent 安全性》對於 VMware Horizon®Client™ 和 Horizon Agent (適用於 Horizon 7) 或 VMware View Agent® (適用於 Horizon 6) 的安全性功能提供簡要的參考。本指南是《Horizon 7 安全性》指南的附屬項目，針對 VMware Horizon™ 6 和 Horizon 7 的每個主要和次要版本都會發行本指南。《Horizon Client 和 Agent 安全性》指南會在每一季隨著用戶端和代理程式軟體的每季發行進行更新。

Horizon Client 是使用者從其用戶端裝置啟動的應用程式，目的是要連接至遠端應用程式或桌面平台。View Agent (適用於 Horizon 6) 或 Horizon Agent (適用於 Horizon 7) 是代理程式軟體，可在遠端桌面平台的作業系統中或提供遠端應用程式的 Microsoft RDS 主機中執行。本指南包括下列資訊：

- 所需的系統登入帳戶。系統安裝/啟動期間所建立帳戶的登入識別碼，以及有關如何變更預設值的指示。
- 擁有安全性含意的組態選項與設定。
- 必須受到保護的資源 (例如與安全性相關的組態檔和密碼) 以及對於安全作業建議的存取控制。
- 記錄檔的位置及其用途。
- 指派給服務使用者的權限。
- 必須針對正確的用戶端和代理程式作業開啟或啟用的外部介面、連接埠以及服務。
- 有關客戶如何獲取並套用最新安全性更新或修補程式的資訊。

主要對象

這項資訊適用於 IT 決策者、架構設計人員、管理員，以及必須熟悉 Horizon 6 或 Horizon 7 安全性元件 (包括用戶端和代理程式) 的其他人員。

VMware Technical Publications Glossary

VMware 技術出版品將為您提供可能不熟悉的術語詞彙。如需 VMware 技術說明文件中所用術語的定義，請前往 http://www.vmware.com/support/pubs。

外部連接埠

1

為了讓產品正確運作，並依據您要使用的功能，必須開啟各種連接埠，遠端桌面平台上的用戶端和代理程式才能夠彼此通訊。

本章節討論下列主題：

- 瞭解通訊協定
- View Agent 或 Horizon Agent 的防火牆規則
- 用戶端和代理程式使用的 TCP 和 UDP 連接埠

瞭解通訊協定

Horizon 6 和 Horizon 7 元件會使用幾種不同的通訊協定來交換訊息。

表 1-1. 預設連接埠 列出各通訊協定所用的預設連接埠。必要時，您可以變更使用的連接埠號碼，以遵守組織政策或避免發生爭用情況。

表 1-1. 預設連接埠

通訊協定	連接埠
JMS	TCP 連接埠 4001 TCP 連接埠 4002
HTTP	TCP 連接埠 80
HTTPS	TCP 連接埠 443
MMR/CDR	針對多媒體重新導向和用戶端磁碟機重新導向，TCP 連接埠 9427
RDP	TCP 連接埠 3389
PCoIP	TCP 連接埠 4172 UDP 連接埠 4172、50002、55000
USB 重新導向	TCP 連接埠 32111。此連接埠也用於時區同步化。
VMware Blast Extreme	TCP 連接埠 8443、22443 UDP 連接埠 443、8443、22443
HTML Access	TCP 連接埠 8443、22443

View Agent 或 Horizon Agent 的防火牆規則

View Agent 和 Horizon Agent 安裝程式會選擇性地在遠端桌面平台和 RDS 主機上設定 Windows 防火牆規則，以開啟預設的網路連接埠。這些是傳入連接埠，除非另有說明。

View Agent 和 Horizon Agent 安裝程式會設定輸入 RDP 連線的本機防火牆規則，以符合主機作業系統目前的 RDP 連接埠，通常是 3389。

如果您指示 View Agent 或 Horizon Agent 安裝程式不要啟用遠端桌面支援，則程式不會開啟連接埠 3389 和 32111，此時您必須手動開啟這些連接埠。

如果您在安裝之後變更 RDP 連接埠號碼，您必須變更相關聯的防火牆規則。如果您在安裝後變更預設連接埠，則必須手動重新設定 Windows 防火牆規則，以便允許在更新的連接埠上進行存取。請參閱《Horizon 7 安裝》文件中的〈取代 View 服務的預設連接埠〉。

在 RDS 主機的 View Agent 或 Horizon Agent 上，Windows 防火牆規則會將由 256 個連續 UDP 連接埠組成的區塊顯示為開啟，以供輸入流量使用。此連接埠的區塊可供 VMware Blast 內部用於 View Agent 或 Horizon Agent 中。RDS 主機上有一個特殊的 Microsoft 簽署驅動程式，可封鎖從外部來源輸入至這些連接埠的流量。此驅動程式會造成 Windows 防火牆將連接埠視為已關閉。

如果您使用虛擬機器範本作為桌面來源，則只有在範本屬於桌面網域成員時，防火牆例外才能執行於已部署的桌面。您可以使用 Microsoft 群組原則設定，來管理本機防火牆例外。如需詳細資訊，請參閱 Microsoft 知識庫 (KB) 文章 875357。

表 1-2. View Agent 或 Horizon Agent 安裝期間開啟的 TCP 與 UDP 連接埠

通訊協定	連接埠
RDP	TCP 連接埠 3389
USB 重新導向和時區同步化	TCP 連接埠 32111
MMR (多媒體重新導向) 和 CDR (用戶端磁碟機重新導向)	TCP 連接埠 9427
PCoIP	針對 RDS 主機，PCoIP 會使用下列連接埠號碼：TCP 連接埠 4172 和 UDP 連接埠 4172 (雙向)。 針對桌面平台，PCoIP 會使用從可設定範圍中選擇的連接埠號碼。依預設，TCP 連接埠為 4172 至 4173，而 UDP 連接埠為 4172 至 4182。針對這些連接埠的防火牆規則不會指定連接埠號碼，但會動態地遵循每個 PCoIP Server 所開啟的連接埠。所選的連接埠號碼會透過連線伺服器傳達給用戶端。
VMware Blast	TCP 連接埠 22443 UDP 連接埠 22443 (雙向) **備註** Linux 桌面平台上未使用 UDP。
HTML Access	TCP 連接埠 22443

表 1-2. View Agent 或 Horizon Agent 安裝期間開啟的 TCP 與 UDP 連接埠 (續)

通訊協定	連接埠
XDMCP	UDP 177 **備註** 此連接埠只會對執行 Ubuntu 18.04 的 Linux 桌面平台中開啟，以進行 XDMCP 存取。防火牆規則會封鎖對此連接埠的所有外部主機存取。
X11	TCP 6100 **備註** 此連接埠只會對執行 Ubuntu 18.04 的 Linux 桌面平台中開啟，以進行 XServer 存取。防火牆規則會封鎖對此連接埠的所有外部主機存取。

用戶端和代理程式使用的 TCP 和 UDP 連接埠

View Agent (適用於 Horizon 6)、Horizon Agent (適用於 Horizon 7) 和 Horizon Client 在彼此之間與各種伺服器元件之間的網路存取使用 TCP 和 UDP 連接埠。

表 1-3. View Agent 或 Horizon Agent 使用的 TCP 和 UDP 連接埠

來源	連接埠	目標	連接埠	通訊協定	說明
Horizon Client	*	View Agent/ Horizon Agent	3389	TCP	Microsoft RDP 到遠端桌面平台的流量 (如果使用直接連線而非通道連線)。
Horizon Client	*	View Agent/ Horizon Agent	9427	TCP	Windows Media MMR 重新導向和用戶端磁碟機重新導向 (如果使用直接連線而非通道連線)。 **備註** 使用 VMware Blast 時不需要用戶端磁碟機重新導向。
Horizon Client	*	View Agent/ Horizon Agent	32111	TCP	USB 重新導向和時區同步化 (如果使用直接連線而非通道連線)。
Horizon Client	*	View Agent/ Horizon Agent	4172	TCP 與 UDP	PCoIP (如果未使用 PCoIP 安全閘道)。 **備註** 因為來源連接埠可能不同，請參閱此表格下方的附註。
Horizon Client	*	Horizon Agent	22443	TCP 與 UDP	VMware Blast (如果使用直接連線而非通道連線)。 **備註** Linux 桌面平台上未使用 UDP。
瀏覽器	*	View Agent/ Horizon Agent	22443	TCP	HTML Access (如果使用直接連線而非通道連線)。
安全伺服器、連線伺服器或 Unified Access Gateway 應用裝置	*	View Agent/ Horizon Agent	3389	TCP	Microsoft RDP 到遠端桌面平台的流量 (如果使用通道連線)。
安全伺服器、連線伺服器或 Unified Access Gateway 應用裝置	*	View Agent/ Horizon Agent	9427	TCP	Windows Media MMR 重新導向和用戶端磁碟機重新導向 (如果使用通道連線)。

表 1-3. View Agent 或 Horizon Agent 使用的 TCP 和 UDP 連接埠 (續)

來源	連接埠	目標	連接埠	通訊協定	說明
安全伺服器、連線伺服器或 Unified Access Gateway 應用裝置	*	View Agent/ Horizon Agent	32111	TCP	USB 重新導向和時區同步化 (如果使用通道連線)。
安全伺服器、連線伺服器或 Unified Access Gateway 應用裝置	55000	View Agent/ Horizon Agent	4172	UDP	PCoIP (非 SALSA20) (如果使用 PCoIP 安全閘道)。
安全伺服器、連線伺服器或 Unified Access Gateway 應用裝置	*	View Agent/ Horizon Agent	4172	TCP	PCoIP (如果使用 PCoIP 安全閘道)。
安全伺服器、連線伺服器或 Unified Access Gateway 應用裝置	*	Horizon Agent	22443	TCP 與 UDP	VMware Blast (如果使用 Blast 安全閘道)。 **備註** Linux 桌面平台上未使用 UDP。
安全伺服器、連線伺服器或 Unified Access Gateway 應用裝置	*	View Agent/ Horizon Agent	22443	TCP	HTML Access (如果使用 Blast 安全閘道)。
View Agent/Horizon Agent	*	連線伺服器	4001、4002	TCP	JMS SSL 流量。
View Agent/Horizon Agent	4172	Horizon Client	*	UDP	PCoIP (如果未使用 PCoIP 安全閘道)。 **備註** 因為目標連接埠可能不同，請參閱此表格下方的附註。
View Agent/Horizon Agent	4172	連線伺服器、安全伺服器或 Unified Access Gateway 應用裝置	55000	UDP	PCoIP (非 SALSA20) (如果使用 PCoIP 安全閘道)。

備註 代理程式用於 PCoIP 的 UDP 連接埠號碼可能會變更。如果連接埠 50002 正在使用中，代理程式會選擇 50003。如果連接埠 50003 正在使用中，代理程式會選擇連接埠 50004，依此類推。您必須將表格中列出星號 (*) 之處的防火牆設定為任何。

表 1-4. Horizon Client 使用的 TCP 和 UDP 連接埠

來源	連接埠	目標	連接埠	通訊協定	說明
Horizon Client	*	連線伺服器、安全伺服器或 Unified Access Gateway 應用裝置	443	TCP	用來登入 Horizon 6 或 Horizon 7 的 HTTPS。(使用通道連線時，此連接埠也用於通道處理)。 **備註** Horizon Client 4.4 及更新版本支援 UDP 連接埠 443 (請參閱以下資訊)。
Horizon Client 4.4 或更新版本	*	Unified Access Gateway 應用裝置 2.9 或更新版本	443	UDP	如果已使用 Blast 安全閘道，且已啟用 UDP 通道伺服器，則 HTTPS 可用於登入至 Horizon 6 或 Horizon 7。(使用通道連線時，此連接埠也用於通道處理)。
Unified Access Gateway 應用裝置 2.9 或更新版本	443	Horizon Client 4.4 或更新版本	*	UDP	如果已使用 Blast 安全閘道，且已啟用 UDP 通道伺服器，則 HTTPS 可用於登入至 Horizon 6 或 Horizon 7。(使用通道連線時，此連接埠也用於通道處理)。
Horizon Client	*	View Agent/ Horizon Agent	22443	TCP	HTML Access 和 VMware Blast (如果未使用 Blast 安全閘道)。
Horizon Client	*	Horizon Agent	22443	UDP	VMware Blast (如果未使用 Blast 安全閘道)。 **備註** 連線至 Linux 桌面平台時不會使用。
Horizon Agent	22443	Horizon Client	*	UDP	VMware Blast (如果未使用 Blast 安全閘道)。 **備註** 連線至 Linux 桌面平台時不會使用。
Horizon Client	*	View Agent/ Horizon Agent	3389	TCP	Microsoft RDP 到遠端桌面平台的流量 (如果使用直接連線而非通道連線)。
Horizon Client	*	View Agent/ Horizon Agent	9427	TCP	Windows Media MMR 重新導向和用戶端磁碟機重新導向 (如果使用直接連線而非通道連線)。 **備註** 使用 VMware Blast 時不需進行 CDR。
Horizon Client	*	View Agent/ Horizon Agent	32111	TCP	USB 重新導向和時區同步化 (如果使用直接連線而非通道連線)。
Horizon Client	*	View Agent/ Horizon Agent	4172	TCP 與 UDP	PCoIP (如果未使用 PCoIP 安全閘道)。 **備註** 因為來源連接埠可能不同，請參閱此表格下方的附註。
Horizon Client	*	連線伺服器、安全伺服器或 Unified Access Gateway 應用裝置	4172	TCP 與 UDP	PCoIP (非 SALSA20) (如果使用 PCoIP 安全閘道)。 **備註** 因為來源連接埠可能不同，請參閱此表格下方的附註。
View Agent/Horizon Agent	4172	Horizon Client	*	UDP	PCoIP (如果未使用 PCoIP 安全閘道)。 **備註** 因為目標連接埠可能不同，請參閱此表格下方的附註。
安全伺服器、View 連線伺服器或 Unified Access Gateway 應用裝置	4172	Horizon Client	*	UDP	PCoIP (非 SALSA20) (如果使用 PCoIP 安全閘道)。 **備註** 因為目標連接埠可能不同，請參閱此表格下方的附註。

表 1-4. Horizon Client 使用的 TCP 和 UDP 連接埠 (續)

來源	連接埠	目標	連接埠	通訊協定	說明
Horizon Client	*	連線伺服器、安全伺服器或 Unified Access Gateway 應用裝置	8443	TCP	HTML Access 和 VMware Blast (如果使用 Blast 安全閘道)。
Horizon Client	*	連線伺服器、安全伺服器或 Unified Access Gateway 應用裝置	8443	UDP	VMware Blast (如果使用 Blast 安全閘道)。 **備註** 連線至 Linux 桌面平台時不會使用。
View 連線伺服器、安全伺服器或 Unified Access Gateway 應用裝置	8443	Horizon Client	*	UDP	VMware Blast (如果使用 Blast 安全閘道)。 **備註** 連線至 Linux 桌面平台時不會使用。

備註 用戶端用於 PCoIP 和 VMware Blast 的 UDP 連接埠號碼可能會變更。如果連接埠 50002 正在使用中，則用戶端會選擇 50003。如果連接埠 50003 正在使用中，則用戶端會選擇連接埠 50004，依此類推。您必須將表格中列出星號 (*) 之處的防火牆設定為任何。

安裝的服務、精靈和處理程序

2

執行用戶端或代理程式安裝程式時，會安裝數個元件。

本章節討論下列主題：

Windows 機器上 View Agent 或 Horizon Agent 安裝程式所安裝的服務

遠端桌面平台和應用程式的作業依賴數個 Windows 服務。

表 2-1. View Agent (適用於 Horizon 6) 或 Horizon Agent (適用於 Horizon 7) 服務

服務名稱	啟動類型	說明
VMware Blast	自動	針對 HTML Access 以及使用 VMware Blast Extreme 通訊協定與原生用戶端連線來提供服務。
VMware Horizon View Agent	自動	為 View Agent/Horizon Agent 提供服務。
VMware Horizon View Composer Guest Agent Server	自動	如果此虛擬機器屬於 View Composer 連結複製桌面平台集區，則提供服務。
VMware Horizon View Persona Management	如果功能已啟用，則為自動；否則為已停用	為 VMware Persona Management 功能提供服務。
VMware Horizon View 指令碼主機	已停用	為執行啟動工作階段指令碼 (若有的話) 提供支援，以在桌面平台工作階段開始之前設定桌面平台安全性原則。原則會以用戶端裝置和使用者的位置為基礎。
VMware Netlink Supervisor Service	自動	為了支援掃描器重新導向功能和序列連接埠重新導向功能，為核心與使用者空間處理程序之間的傳輸資訊提供監視服務。
VMware Scanner Redirection Client Service	自動	(View Agent 6.0.2 及更新版本) 為掃描器重新導向功能提供服務。
VMware Serial Com Client Service	自動	(View Agent 6.1.1 及更新版本) 為序列連接埠重新導向功能提供服務。
VMware Snapshot Provider	手動	為用於複製的虛擬機器快照提供服務。

表 2-1. View Agent (適用於 Horizon 6) 或 Horizon Agent (適用於 Horizon 7) 服務 (續)

服務名稱	啟動類型	說明
VMware Tools	自動	提供在主機和客體作業系統之間同步化物件的支援，它可增強虛擬機器客體作業系統的效能並改善虛擬機器的管理。
VMware USB Arbitration Service	自動	列舉連線到用戶端的各種 USB 裝置，並判斷要連線到用戶端的裝置以及要連線到遠端桌面平台的裝置。
VMware View USB	自動	為 USB 重新導向功能提供服務。

Windows 用戶端上安裝的服務

Horizon Client 的作業依賴數個 Windows 服務。

表 2-2. Horizon Client Services

服務名稱	啟動類型	說明
VMware Horizon Client	自動	提供 Horizon Client 服務。
VMware Netlink Supervisor Service	自動	為了支援掃描器重新導向功能和序列埠重新導向功能，為核心與使用者空間處理程序之間的傳輸資訊提供監視服務。
VMware Scanner Redirection Client Service	自動	(Horizon Client 3.2 及更新版本) 為掃描器重新導向功能提供服務。
VMware Serial Com Client Service	自動	(Horizon Client 3.4 及更新版本) 為序列埠重新導向功能提供服務。
VMware USB Arbitration Service	自動	列舉連線到用戶端的各種 USB 裝置，並判斷要連線到用戶端的裝置以及要連線到遠端桌面平台的裝置。
VMware View USB	自動	(Horizon Client 4.3 及更早版本) 為 USB 重新導向功能提供服務。 **備註** 在 Horizon Client 4.4 及更新版本中，此服務已移除，且 USBD 服務已移至 `vmware-remotemks.exe` 處理程序。

安裝在其他用戶端和 Linux 桌面平台中的精靈

為了確保安全，請務必瞭解 Horizon Client 是否安裝了任何精靈或處理程序。

表 2-3. Horizon Client 所安裝的服務、處理程序或精靈 (依用戶端類型)

類型	服務、處理程序或精靈
Linux 用戶端	■ `vmware-usbarbitrator`，它會列舉連線到用戶端的各種 USB 裝置，並判斷要連線到用戶端的裝置以及要連線到遠端桌面平台的裝置。 ■ `vmware-view-used`，它會為 USB 重新導向功能提供服務。 **備註** 這些精靈會在您於安裝期間按一下**在安裝後登錄並啟動服務**核取方塊時自動啟動。這些處理程序會以 root 的身分執行。
Mac 用戶端	Horizon Client 不會建立任何精靈。
Chrome OS 用戶端	Horizon Client 會在一個 Android 處理程序中執行。Horizon Client 不會建立任何精靈。

表 2-3. Horizon Client 所安裝的服務、處理程序或精靈 (依用戶端類型) (續)

類型	服務、處理程序或精靈
iOS 用戶端	Horizon Client 不會建立任何精靈。
Android 用戶端	Horizon Client 會在一個 Android 處理程序中執行。Horizon Client 不會建立任何精靈。
Windows 10 UWP 用戶端	Horizon Client 不會建立或觸發任何系統服務。
Windows 市集用戶端	Horizon Client 不會建立或觸發任何系統服務。
Linux 桌面平台	■ `StandaloneAgent`，它會使用 root 特殊權限來執行，並且會在 Linux 系統啟動並執行時啟動。`StandaloneAgent` 會與連線伺服器通訊，以執行遠端桌面工作階段管理 (設定/移除工作階段、在連線伺服器中將遠端桌面狀態更新為代理)。 ■ `VMwareBlastServer`，會由 `StandaloneAgent` 於收到連線伺服器的 `StartSession` 要求時啟動。`VMwareBlastServer` 精靈使用 `vmwblast` (安裝 Linux Agent 時所建立的系統帳戶) 特殊權限來執行。它會透過內部 `MKSControl` 通道與 `StandaloneAgent` 通訊，並使用 VMware Blast 顯示通訊協定與 Horizon Client 通訊。

要保護的資源

3

這些資源包括相關的組態檔、密碼和存取控制。

本章節討論下列主題：

實施最佳做法來保護用戶端系統

實施這些最佳做法來保護用戶端系統。

- 請確定已設定用戶端系統在閒置一段時間後會進入睡眠狀態，使用者必須輸入密碼才能喚醒電腦。
- 要求使用者在啟動用戶端系統時，輸入使用者名稱和密碼。請勿設定用戶端系統允許自動登入。
- 若是 Mac 用戶端系統，請考慮對金鑰鏈和使用者帳戶設定不同的密碼。密碼不同時，在系統代替使用者輸入任何密碼之前，會顯示提示。此外，也請考量開啟 FileVault 防護。

組態檔位置

必須保護的資源包括安全性相關的組態檔。

表 3-1. 組態檔的位置（依用戶端類型）

類型	目錄路徑
Linux 用戶端	當 Horizon Client 啟動時，即會依下列順序從各個位置處理組態設定： 1 `/etc/vmware/view-default-config` 2 `~/.vmware/view-preferences` 3 `/etc/vmware/view-mandatory-config` 如果在多個位置定義同一個設定，則將採用最後讀取的檔案或命令列選項的值。
Windows 用戶端	可能包括部分私人資訊的使用者設定位於下列檔案中： `C:\Users\`*`user-name`*`\AppData\Roaming\VMware\VMware Horizon View Client\prefs.txt`

表 3-1. 組態檔的位置 (依用戶端類型) (續)

類型	目錄路徑
Mac 用戶端	Mac 用戶端啟動後會產生部分組態檔。 ■ `$HOME/Library/Preferences/com.vmware.horizon.plist` ■ `$HOME/Library/Preferences/com.vmware.vmrc.plist` ■ `$HOME/Library/Preferences/com.vmware.horizon.keyboard.plist` ■ `/Library/Preferences/com.vmware.horizon.plist`
Chrome OS 用戶端	安全性相關設定會出現在使用者介面而不是組態檔中。任何使用者都看不到任何組態檔。
iOS 用戶端	安全性相關設定會出現在使用者介面而不是組態檔中。任何使用者都看不到任何組態檔。
Android 用戶端	安全性相關設定會出現在使用者介面而不是組態檔中。任何使用者都看不到任何組態檔。
Windows 10 UWP 用戶端	安全性相關設定會出現在使用者介面而不是組態檔中。任何使用者都看不到任何組態檔。
Windows 市集用戶端	安全性相關設定會出現在使用者介面而不是組態檔中。任何使用者都看不到任何組態檔。
View Agent 或 Horizon Agent (使用 Windows 作業系統的遠端桌面平台)	安全性相關設定只會出現在 Windows 登錄中。
Linux 桌面平台	您可以使用文字編輯器來開啟下列組態檔並指定 SSL 相關設定。 `/etc/vmware/viewagent-custom.conf`

帳戶

用戶端使用者必須在 Active Directory 中具備帳戶。

Horizon Client 使用者帳戶

在 Active Directory 中，為能夠存取遠端桌面平台和應用程式的使用者設定使用者帳戶。如果您計劃使用 RDP 通訊協定，此使用者帳戶必須是遠端桌面平台使用者群組的成員。

一般來說，使用者不應該是 Horizon 管理員。如果 Horizon 管理員需要驗證使用者體驗，請建立並授權個別的測試帳戶。在桌面平台上，Horizon 使用者不應該是特殊權限群組 (例如管理員) 的成員，因為這麼一來他們將能夠修改鎖定的組態檔和 Windows 登錄。

安裝期間建立的系統帳戶

Horizon Client 應用程式不會在任何類型的用戶端上建立任何服務使用者帳戶。針對 Windows 版 Horizon Client 所建立的服務，登入識別碼為 Local System。

在 Mac 用戶端上，於第一次啟動時，使用者必須授與 Local Admin 存取權，才能啟動 USB 和虛擬列印 (ThinPrint) 服務。在這些服務第一次啟動之後，標準使用者便具備這些服務的執行存取權。同樣地，在 Linux 用戶端上，`vmware-usbarbitrator` 和 `vmware-view-used` 精靈會在您於安裝期間按一下**在安裝後登錄並啟動服務**核取方塊時自動啟動。這些處理程序會以 root 的身分執行。

View Agent 或 Horizon Agent 不會在 Windows 桌面平台上建立任何服務使用者帳戶。但會在 Linux 桌面平台上建立系統帳戶 `vmwblast`。在 Linux 桌面平台上，`StandaloneAgent` 精靈會使用 root 特殊權限執行，而 `VmwareBlastServer` 精靈則會使用 `vmwblast` 特殊權限執行。

用戶端和代理程式的安全性設定

4

有數個用戶端和代理程式設定可用來調整組態的安全性。您可以透過使用群組原則物件或編輯 Windows 登錄設定，來存取遠端桌面平台和 Windows 用戶端的設定。

如需與記錄收集相關的組態設定，請參閱第 6 章 用戶端和代理程式記錄檔位置。如需與安全性通訊協定和加密套件相關的組態設定，請參閱第 5 章 設定安全性通訊協定及加密套件。

本章節討論下列主題：

- 設定憑證檢查
- View Agent 和 Horizon Agent 組態範本中安全性相關的設定
- 在 Linux 桌面平台上設定組態檔中的選項
- HTML Access 的群組原則設定
- Horizon Client 組態範本中的安全性設定
- 設定 Horizon Client 憑證驗證模式
- 設定本機安全性授權保護

設定憑證檢查

管理員可設定憑證驗證模式，比如設定為能夠永遠執行完整的驗證。管理員也可以設定是否在有任何或部分伺服器憑證檢查失敗時，允許使用者選擇是否拒絕用戶端連線。

當連線伺服器執行個體與 Horizon Client 之間產生 SSL/TLS 連線時，就要檢查憑證。管理員可以設定驗證模式，以使用下列任一策略：

- 允許使用者選擇驗證模式。本清單其餘部分說明三種驗證模式。
- (無驗證) 不執行憑證檢查。
- (警告) 如果伺服器提出自我簽署憑證的話，則使用者會被警告。使用者可選擇是否允許此類型的連線。
- (完整安全性) 執行完整驗證，凡是無法通過完整驗證的連線均會遭到拒絕。

憑證驗證包括下列檢查：

- 憑證已被撤銷了嗎？

- 憑證是否用於驗證寄件者身分並將伺服器通訊加密以外的目的？也就是說，它是正確的憑證類型嗎？
- 憑證是否已到期，或是尚未生效？也就是說，根據電腦的時鐘，憑證有效嗎？
- 憑證上的一般名稱是否符合傳送該憑證的伺服器主機名稱？如果負載平衡器將 Horizon Client 重新導向至一台其憑證與在 Horizon Client 中輸入的主機名稱不符的伺服器，則會發生不符的情形。另一個會發生不符的原因是您在用戶端輸入 IP 位址，而非主機名稱。
- 憑證是由未知或未受信任的憑證授權機構 (CA) 簽署的嗎？自我簽署憑證是一種未受信任的憑證授權機構。

  若要通過此檢查，必須將憑證之信任鏈放在裝置之本機憑證存放區的根目錄。

如果您使用 SSL Proxy 伺服器檢查從用戶端環境傳送至網際網路的流量，您可以透過 SSL Proxy 伺服器啟用對次要連線的憑證檢查。您也可以將 VMware Blast 連線設定為使用 Proxy 伺服器。Windows、Mac 和 Linux 版 Horizon Client5.2 及更新版本可支援這些功能。

如需關於如何為特定類型的用戶端設定適用的憑證檢查和 SSL Proxy 伺服器的資訊，請參閱該用戶端的 Horizon Client 安裝和設定文件。這些文件也包含使用自我簽署憑證的相關資訊。

View Agent 和 Horizon Agent 組態範本中安全性相關的設定

安全性相關的設定是在 View Agent 和 Horizon Agent 的 ADM 和 ADMX 範本檔中提供。ADM 和 ADMX 範本檔名為 `vdm_agent.adm` 和 `vdm_agent.admx`。除非另有說明，否則這些設定僅包含「電腦設定」設定。

安全性設定儲存在客體機器的 `HKLM\Software\VMware, Inc.\VMware VDM\Agent\Configuration` 底下的登錄中。

表 4-1. View Agent (適用於 Horizon 6) 或 Horizon Agent (適用於 Horizon 7) 組態範本中的安全性相關設定

設定	說明
`AllowDirectRDP`	決定 Horizon Client 裝置之外的用戶端是否可以使用 RDP 直接連線至遠端桌面平台。停用此設定時，代理程式僅允許受 Horizon 管理的連線通過 Horizon Client。 從 Mac 版 Horizon Client 連線至遠端桌面平台時，請勿停用 `AllowDirectRDP` 設定。如果停用此設定，則連線會失敗，並出現拒絕存取錯誤。 依預設，使用者登入遠端桌面工作階段時，您可以使用 RDP 連線至虛擬機器。RDP 連線會終止遠端桌面工作階段，且使用者未儲存的資料和設定可能會遺失。在關閉外部 RDP 連線前，使用者無法登入桌面平台。要避免發生此情況，停用 `AllowDirectRDP` 設定。 **重要** Windows 遠端桌面服務必須在每個桌面平台的客體作業系統上執行。您可以使用此設定，防止使用者建立 RDP 與其桌面平台的直接連線。 此設定依預設為啟用。 對等的 Windows 登錄值為 `AllowDirectRDP`。
`AllowSingleSignon`	決定是否使用單一登入 (SSO) 將使用者連線至桌面平台和應用程式。若啟用此設定，當使用者登入伺服器時，只需要輸入一次認證。若停用此設定，當使用者進行遠端連線時，則必須重新驗證。 此設定依預設為啟用。 對等的 Windows 登錄值為 `AllowSingleSignon`。

表 4-1. View Agent (適用於 Horizon 6) 或 Horizon Agent (適用於 Horizon 7) 組態範本中的安全性相關設定 (續)

設定	說明
CommandsToRunOnConnect	指定首次連線某個工作階段時，要執行的命令或命令指令碼的清單。 預設沒有指定任何清單。 對等的 Windows 登錄值為 CommandsToRunOnConnect。
CommandsToRunOnDisconnect	指定某個工作階段中斷連線時，要執行的命令或命令指令碼的清單。 預設沒有指定任何清單。 對等的 Windows 登錄值為 CommandsToRunOnReconnect。
CommandsToRunOnReconnect	指定某個工作階段中斷連線後重新連線時，要執行的命令或命令指令碼的清單。 預設沒有指定任何清單。 對等的 Windows 登錄值為 CommandsToRunOnDisconnect。
ConnectionTicketTimeout	指定 Horizon 連線票證的有效時間長度 (以秒為單位)。 Horizon Client 裝置在連線至代理程式時，會使用連線票證以進行驗證和單一登入。基於安全理由，連線票證的有效時間長度是有限的。當使用者連線至遠端桌面平台時，在連線票證逾時期間內必須進行驗證，否則工作階段會逾時。如果未設定此設定，則預設的逾時期間為 900 秒。 對等的 Windows 登錄值為 VdmConnectionTicketTimeout。
CredentialFilterExceptions	指定不允許載入代理程式 CredentialFilter 的執行檔。檔案名稱不得包含路徑或尾碼。使用分號分隔多個檔案名稱。 預設沒有指定任何清單。 對等的 Windows 登錄值為 CredentialFilterExceptions。

如需有關這些設定及其安全性含意的詳細資訊，請參閱《View 管理》文件。

在 Linux 桌面平台上設定組態檔中的選項

您可以透過新增項目到檔案 /etc/vmware/config 或 /etc/vmware/viewagent-custom.conf 來設定某些選項。

在 Horizon Agent 的安裝期間，安裝程式會將兩個組態範本檔 config.template 和 viewagent-custom.conf.template 複製到 /etc/vmware。此外，如果 /etc/vmware/config 和 /etc/vmware/viewagent-custom.conf 不存在，則安裝程式會將 config.template 複製到 config，並將 viewagent-custom.conf.template 複製到 viewagent-custom.conf。範本檔中會列出並記載所有組態選項。若要設定選項，只需移除註解並適當變更值。

例如，/etc/vmware/config 中的下列程式行可啟用無失真建立 PNG 模式。

```
RemoteDisplay.buildToPNG=TRUE
```

進行組態變更之後，請將 Linux 重新開機以讓變更生效。

/etc/vmware/config 中的組態選項

VMwareBlastServer 和其相關外掛程式使用組態檔 `/etc/vmware/config`。

備註　下表的說明包含 Horizon Agent 組態檔中由每個代理程式強制執行的 USB 原則設定。Horizon Agent 會使用這些設定來決定是否可以將某個 USB 轉送至主機。Horizon Agent 也會將這些設定傳遞至 Horizon Client 進行解譯並強制執行。強制執行是根據您是指定合併 **(m)** 修飾詞來套用 Horizon Agent 篩選原則設定以及 Horizon Client 篩選原則設定，或是指定覆寫 **(o)** 修飾詞以使用 Horizon Agent 篩選原則設定而非 Horizon Client 篩選原則設定來進行解譯和強制執行。

表 4-2. `/etc/vmware/config` 中的組態選項

選項	值/格式	預設值	說明
Clipboard.Direction	`0, 1, 2,`或 `3`	`2`	使用此選項來指定剪貼簿重新導向原則。有效值如下： ■ 0 - 停用剪貼簿重新導向。 ■ 1 - 啟用雙向剪貼簿重新導向。 ■ 2 - 僅啟用從用戶端到遠端桌面平台的剪貼簿重新導向。 ■ 3 - 僅啟用從遠端桌面平台到用戶端的剪貼簿重新導向。
RemoteDisplay.allowAudio	`true` 或 `false`	`true`	設定此選項可啟用/停用音訊輸出。
RemoteDisplay.allowH264	`true` 或 `false`	`true`	設定此選項，可啟用或停用 H.264 編碼。
RemoteDisplay.buildToPNG	`true` 或 `false`	`false`	圖形應用程式，特別是圖形設計應用程式，會需要在 Linux 桌面平台的用戶端有像素精準的影像呈現。您可以針對 Linux 桌面平台上產生和在用戶端裝置上呈現的影像和視訊播放，設定無失真建立 PNG 模式。此功能會在用戶端和 ESXi 主機之間使用額外的頻寬。啟用此選項會停用 H.264 編碼。
RemoteDisplay.enableNetworkContinuity	`true` 或 `false`	`true`	設定此選項，可啟用或停用 Horizon Agent for Linux 中的網路持續性功能。
RemoteDisplay.enableNetworkIntelligence	`true` 或 `false`	`true`	設定此選項，可啟用或停用 Horizon Agent for Linux 中的網路智慧功能。
RemoteDisplay.enableStats	`true` 或 `false`	`false`	在 mks 記錄中啟用或停用 VMware Blast 顯示通訊協定統計資料，例如頻寬、FPS、RTT 等。
RemoteDisplay.enableUDP	`true` 或 `false`	`true`	設定此選項，可啟用或停用 Horizon Agent for Linux 中的 UDP 通訊協定支援。
RemoteDisplay.maxBandwidthKbps	整數	1000000	指定 VMware Blast 工作階段的最大頻寬 (單位為千位元/秒，即 kbps)。頻寬包括所有影像處理、音訊、虛擬通道和 VMware Blast 控制流量。有效值必須小於 4 Gbps (4096000)。
RemoteDisplay.minBandwidthKbps	整數	256	指定 VMware Blast 工作階段的最小頻寬 (單位為千位元/秒，即 kbps)。頻寬包括所有影像處理、音訊、虛擬通道和 VMware Blast 控制流量。
RemoteDisplay.maxFPS	整數	30	指定畫面更新的最大速率。使用此設定，可管理使用者所使用的平均頻寬。有效值必須介於 3 與 60 之間。預設值為每秒 30 次更新。

表 4-2. `/etc/vmware/config` 中的組態選項 (續)

選項	值/格式	預設值	說明
RemoteDisplay.maxQualityJPEG	可用值範圍：1-100	90	指定用於 JPEG/PNG 編碼的桌面平台顯示的影像畫質。高畫質設定用於較為靜態的畫面區域，可產生較佳影像畫質。
RemoteDisplay.midQualityJPEG	可用值範圍：1-100	35	指定用於 JPEG/PNG 編碼的桌面平台顯示的影像畫質。用來設定桌面平台顯示的中等畫質設定。
RemoteDisplay.minQualityJPEG	可用值範圍：1-100	25	指定用於 JPEG/PNG 編碼的桌面平台顯示的影像畫質。低畫質設定用於經常變動的畫面區域，例如，在執行捲動時。
RemoteDisplay.qpmaxH264	可用值範圍：0-51	36	使用此選項來設定 H264minQP 量化參數，其指定設定為使用 H.264 編碼的遠端顯示的最佳影像畫質。將該值設定為大於針對 RemoteDisplay.qpminH264 設定的值。
RemoteDisplay.qpminH264	可用值範圍：0-51	10	使用此選項來設定 H264maxQP 量化參數，其指定設定為使用 H.264 編碼的遠端顯示的最低影像畫質。將該值設定為小於針對 RemoteDisplay.qpmaxH264 設定的值。
UsbRedirPlugin.log.logLevel	`error`、`warn`、`info`、`debug`、`trace` 或 `verbose`	`info`	使用此選項，可設定 USB 重新導向外掛程式的記錄層級。
UsbRedirServer.log.logLevel	`error`、`warn`、`info`、`debug`、`trace` 或 `verbose`	`info`	使用此選項，可設定 USB 重新導向伺服器的記錄層級。
VMWPkcs11Plugin.log.enable	`true` 或 `false`	`false`	設定此選項可啟用或停用 True SSO 功能的記錄模式。
VMWPkcs11Plugin.log.logLevel	`error`、`warn`、`info`、`debug`、`trace` 或 `verbose`	`info`	使用此選項，可設定 True SSO 功能的記錄層級。
VVC.RTAV.Enable	`true` 或 `false`	`true`	設定此選項可啟用/停用音訊輸入。
VVC.ScRedir.Enable	`true` 或 `false`	`true`	設定此選項可啟用/停用智慧卡重新導向。
VVC.logLevel	`fatalerror`、`warn`、`info`、`debug` 或 `trace`	`info`	使用此選項以設定 VVC Proxy 節點的記錄層級。
cdrserver.cacheEnable	`true` 或 `false`	`true`	設定此選項，可啟用或停用從代理程式到用戶端的寫入快取功能。
cdrserver.customizedSharedFolderPath	`folder_path`	`/home/`	使用此選項可將用戶端磁碟機重新導向 (CDR) 共用資料夾位置從預設的 `/home/`*`user`*`/tsclient` 目錄變更為自訂目錄。 例如，如果使用者 `test` 要將 CDR 共用資料夾放在 `/mnt/test/tsclient` (而不是 `/home/test/tsclient`) 中，則該使用者可以指定 **`cdrserver.customizedSharedFolderPath=/mnt/`**。 **備註** 為了使此選項生效，指定的資料夾必須存在且已使用正確的使用者權限進行設定。

表 4-2. `/etc/vmware/config` **中的組態選項 (續)**

選項	值/格式	預設值	說明
cdrserver.forcedByAdmin	`true` 或 `false`	`false`	設定此選項，可控制用戶端是否可以共用未使用 `cdrserver.shareFolders` 選項指定的其他資料夾。
cdrserver.logLevel	`error`、`warn`、`info`、`debug`、`trace` 或 `verbose`	`info`	使用此選項，可設定 `vmware-CDRserver.log` 檔案的記錄層級。
cdrserver.permissions	`R`	`RW`	使用此選項，可在 Horizon Agent 所具備 Horizon Client 共用的資料夾上套用其他的讀取/寫入權限。例如： ■ 如果 Horizon Client 共用的資料夾具有 `read` 和 `write` 權限，而您設定 **`cdrserver.permissions=R`**，則 Horizon Agent 僅具有 `read` 存取權限。 ■ 如果 Horizon Client 共用的資料夾僅具有 `read` 權限，而您設定 **`cdrserver.permissions=RW`**，則 Horizon Agent 仍僅有 `read` 存取權限。Horizon Agent 無法變更 Horizon Client 所設定的 `read only` (唯讀) 屬性。Horizon Agent 僅能移除寫入權限。 一般使用方式如下： ■ **`cdrserver.permissions=R`** ■ **`#cdrserver.permissions=R`** (例如，註解排除或刪除該項目)
cdrserver.sharedFolders	***`file_path1`*`,R;`*`file-path2`*`,;`*`file_path3`*`,R; ...`**	未定義	指定用戶端可以與 Linux 桌面平台共用的一或多個資料夾的檔案路徑。例如： ■ 針對 Windows 用戶端：**`C:\spreadsheets,;D:\ebooks,R`** ■ 針對非 Windows 用戶端：**`/tmp/spreadsheets;/tmp/ebooks,;/home/finance,R`**
collaboration.logLevel	`error`、`info` 或 `debug`	`info`	使用此選項，可設定協作工作階段所使用的記錄層級。如果記錄層級為 `debug`，則會記錄對 `collabui` 函數進行的所有呼叫和 `collabor` 清單的內容。
collaboration.maxCollabors	小於 10 的整數	5	指定您可以邀請加入工作階段的協作者數目上限。
collaboration.enableEmail	`true` 或 `false`	`true`	設定此選項，可啟用或停用使用已安裝的電子郵件應用程式傳送協作邀請。此選項停用時，即便已安裝電子郵件應用程式，您仍無法使用電子郵件邀請協作者。
collaboration.serverUrl	[URL]	未定義	指定要納入協作邀請的伺服器 URL。
collaboration.enableControlPassing	`true` 或 `false`	`true`	設定此選項，可允許或限制協作者對 Linux 桌面平台進行控制。若要指定唯讀協作工作階段，請將此選項設為 **`false`**。
mksVNCServer.useUInputButtonMapping	`true` 或 `false`	`false`	設定此選項可啟用 Ubuntu 或 RHEL 7.x. CentOS 上的慣用左手滑鼠支援，而 RHEL 6.x 支援左手使用者的滑鼠，您不需要設定此選項。
mksvhan.clipboardSize	整數	1024	使用此選項，可指定所要複製及貼上的剪貼簿大小上限。

表 4-2. `/etc/vmware/config` **中的組態選項 (續)**

選項	值/格式	預設值	說明
vdpservice.log.logLevel	`fatalerror`、`warn`、`info`、`debug` 或 `trace`	`info`	使用此選項，可設定 `vdpservice` 的記錄層級。
viewusb.AllowAudioIn	**`{m|o}:{true|false}`**	未定義，其相當於 `true`	使用此選項，可允許或不允許將音訊輸入裝置重新導向。範例：**`o:false`**
viewusb.AllowAudioOut	**`{m|o}:{true|false}`**	未定義，其相當於 `false`	設定此選項，可允許或不允許音訊輸出裝置的重新導向。
viewusb.AllowAutoDeviceSplitting	**`{m|o}:{true|false}`**	未定義，其相當於 `false`	設定此選項，可允許或不允許複合 USB 裝置的自動分割。 範例：**`m:true`**
viewusb.AllowDevDescFailsafe	**`{m|o}:{true|false}`**	未定義，其相當於 `false`	設定此選項後，即便 Horizon Client 無法取得組態或裝置描述元時，仍可允許或不允許將裝置重新導向。若要在即使無法取得組態或裝置描述元的情形下也允許裝置，請將它納入在 Include 篩選器當中，例如 **`IncludeVidPid`** 或 **`IncludePath`**。
viewusb.AllowHIDBootable	**`{m|o}:{true|false}`**	未定義，其相當於 `true`	使用此選項以允許或不允許將鍵盤或滑鼠以外可在開機時使用的輸入裝置 (又稱為 HID 可開機裝置) 重新導向。
viewusb.AllowKeyboardMouse	**`{m|o}:{true|false}`**	未定義，其相當於 `false`	使用此選項，可以允許或不允許將具備整合式指向裝置 (例如滑鼠、軌跡球或觸控板) 的鍵盤重新導向。
viewusb.AllowSmartcard	**`{m|o}:{true|false}`**	未定義，其相當於 `false`	設定此選項，可允許或不允許將智慧卡裝置重新導向。
viewusb.AllowVideo	**`{m|o}:{true|false}`**	未定義，其相當於 `true`	使用此選項，可允許或不允許將視訊裝置重新導向。
viewusb.DisableRemoteConfig	**`{m|o}:{true|false}`**	未定義，其相當於 `false`	設定此選項，可停用或啟用在執行 USB 裝置篩選時使用 Horizon Agent 設定。
viewusb.ExcludeAllDevices	**`{true|false}`**	未定義，其相當於 `false`	使用此選項，可排除或包含所有 USB 裝置，以決定是否進行重新導向。如果設定為 **`true`**，您可以使用其他原則設定，以允許將特定裝置或裝置系列重新導向。如果設定為 **`false`**，您可以使用其他原則設定，以避免將特定裝置或裝置系列重新導向。如果在 Horizon Agent 上將 **`ExcludeAllDevices`** 的值設為 **`true`**，且此設定已傳遞至 Horizon Client，則 Horizon Agent 設定會覆寫 Horizon Client 設定。
viewusb.ExcludeFamily	**`{m|o}:`*`family_name_1`*`[;family_name_2;...]`**	未定義	使用此選項，可排除裝置系列以避免進行重新導向。例如：**`m:bluetooth;smart-card`** 如果您已經啟用自動裝置分割功能，Horizon 便會檢驗複合 USB 裝置每個介面的裝置系列，以確認必須排除的介面。如果您已經停用自動裝置分割功能，Horizon 便會檢驗整個複合 USB 裝置的裝置系列。 **備註** 依預設系統會排除滑鼠和鍵盤不進行重新導向，因此不需使用此設定來排除。

表 4-2. `/etc/vmware/config` **中的組態選項 (續)**

選項	值/格式	預設值	說明
viewusb.ExcludePath	**{m|o}:bus-*x1*[/*y1*].../ port-*z1*[;bus-*x2*[/*y2*].../port-*z2*;...]**	未定義	使用此選項，可排除位於指定集線器或連接埠路徑上的裝置，以避免進行重新導向。您必須以十六進位指定匯流排和連接埠號碼。您不能在路徑中使用萬用字元。 例如： **m:bus-1/2/3_port- 02;bus-1/1/1/4_port-ff**
viewusb.ExcludeVidPid	**{m|o}:vid-*xxx1*_pid-*yyy1*[;vid-*xxx2*_pid-*yyy2*;..]**	未定義	設定此選項，可排除具有特定廠商和產品識別碼的裝置，以避免進行重新導向。您必須以十六進位指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。 例如：**o:vid-0781_pid- ****;vid-0561_pid-554c**
viewusb.IncludeFamily	**{m|o}:*family_name_1*[;*family_name_2*]...**	未定義	設定此選項，可包含能夠重新導向的裝置系列。 例如：**o:storage; smart-card**
viewusb.IncludePath	**{m|o}:bus-*x1*[/*y1*].../ port-*z1*[;bus-*x2*[/*y2*].../portz2;...]**	未定義	使用此選項，可包含指定集線器或連接埠路徑上能夠重新導向的裝置。您必須以十六進位指定匯流排和連接埠號碼。您不能在路徑中使用萬用字元。 例如：**m:bus-1/2_port- 02;bus-1/7/1/4_port-0f**
viewusb.IncludeVidPid	**{m|o}:vid-*xxx1*_pid-*yyy1*[;vid-*xxx2*_pid-*yyy2;...*]**	未定義	設定此選項，可包含具有指定廠商和產品識別碼且能夠重新導向的裝置。您必須以十六進位指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。 例如：**o:vid-***_pid-0001;vid-0561_pid-554c**
viewusb.SplitExcludeVidPid	**{m|o}:vid-*xxx1*_pid-*yyy1*[;vid-*xxx2*_pid-*yyy2*;...]**	未定義	使用此選項，可排除或包含指定的複合 USB 裝置，以決定是否根據廠商和產品識別碼進行分割。設定的格式為 **vid-*xxx1*_pid-*yyy1*[;vid-*xxx2*_pid-*yyy2*;...]**。您必須以十六進位格式指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。 範例：**m:vid-0f0f_pid-55****
viewusb.SplitVidPid	**{m|o}:vid-*xxxx*_pid-*yyyy*([exintf:*zz*[;exintf:*ww*]])[;...]**	未定義	設定此選項，可將根據廠商和產品識別碼指定的複合 USB 裝置元件視為個別裝置。設定的格式為 **vid-*xxxx*_pid-*yyyy*(exintf:*zz*[;exintf:*ww*])**。 您可以使用 **exintf** 關鍵字，藉由指定它們的介面號碼來將元件自重新導向清單中排除。您必須以十六進位指定識別碼，及以十進位指定介面號碼，包括任何前置的 0。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。 範例： **o:vid-0f0f_pid-***(exintf-01);vid-0781_pid-554c(exintf:01;exintf:02)** **備註** Horizon 不會自動包含您未明確排除的元件。您必須指定篩選原則，例如**納入 VidPid 裝置**，以納入那些元件。

/etc/vmware/viewagent-custom.conf 中的組態選項

Java Standalone Agent 使用組態檔 `/etc/vmware/viewagent-custom.conf`。

表 4-3. `/etc/vmware/viewagent-custom.conf` 中的組態選項

選項	值	預設值	說明
CDREnable	`true` 或 `false`	`true`	使用此選項，可啟用或停用用戶端磁碟機重新導向 (CDR) 功能。
CollaborationEnable	`true` 或 `false`	`true`	使用此選項，可啟用或停用 Linux 桌面平台上的工作階段協作功能。
EndpointVPNEnable	`true` 或 `false`	`false`	設定此選項，可在對 Dynamic Environment Manager 主控台中所使用端點 IP 位址的範圍評估端點 IP 位址時，指定要使用用戶端的實體網路卡 IP 位址或 VPN IP 位址。如果選項設為 `false`，則會使用用戶端的實體網路卡 IP 位址。否則，即會使用 VPN IP 位址。
HelpDeskEnable	`true` 或 `false`	`true`	設定此選項，可啟用或停用 Help Desk Tool 功能。
KeyboardLayoutSync	`true` 或 `false`	`true`	使用此選項，可指定是否將用戶端的系統地區設定清單和目前的鍵盤配置與 Linux 版 Horizon Agent 桌面平台同步。 當此設定已啟用或未設定時，則允許進行同步化。當此設定已停用時，則不允許進行同步化。 僅 Windows 版 Horizon Client 支援此功能，並且僅適用於英文、法文、德文、日文、韓文、西班牙文、簡體中文和繁體中文地區設定。
LogCnt	整數	-1	使用此選項以設定 `/tmp/vmware-root` 中保留的記錄檔計數。 ■ -1 - 全部保留 ■ 0 - 全部刪除 ■ > 0 - 保留的記錄檔計數。
NetbiosDomain	全大寫字母的文字字串		設定 True SSO 時，使用此選項來設定您組織的網域的 NetBIOS 名稱。
OfflineJoinDomain	`pbis` 或 `samba`	`pbis`	使用此選項可設定即時複製離線網域加入。執行離線網域加入的可用方法包括 PowerBroker Identity Services Open (PBISO) 驗證和 Samba 離線網域加入。如果此屬性的值不是 `pbis` 或 `samba`，則會忽略離線網域加入。
RunOnceScript			使用此選項可將複製的虛擬機器重新加入至 Active Directory。 主機名稱變更後，請設定 `RunOnceScript` 選項。指定的指令碼只會在第一次主機名稱變更後執行一次。當代理程式服務啟動，且主機名稱在代理程式安裝後有所變更時，即會以根權限執行指令碼。 以 Winbind 解決方案為例，您必須將基礎虛擬機器加入含有 Winbind 的 Active Directory，並將此選項設定為指令碼路徑。指令碼必須包含網域重新加入命令`/usr/bin/net ads join -U <ADUserName>%<ADUserPassword>`。在虛擬機器複製之後，作業系統自訂會變更主機名稱。當代理程式服務啟動時，指令碼即會執行，而將複製的虛擬機器加入 Active Directory。

表 4-3. `/etc/vmware/viewagent-custom.conf` 中的組態選項 (續)

選項	值	預設值	說明
RunOnceScriptTimeout		120	使用此選項來為 RunOnceScript 選項設定逾時時間 (秒)。 例如，設定 `RunOnceScriptTimeout=120`
SSLCiphers	文字字串	!aNULL:kECDH +AESGCM:ECDH +AESGCM:RSA +AESGCM:kECDH +AES:ECDH+AES:RSA +AES	使用此選項來指定加密清單。您必須使用 https://www.openssl.org/docs/manmaster/man1/ciphers.html 中定義的格式。
SSLProtocols	文字字串	TLSv1_1:TLSv1_2	使用此選項來指定安全性通訊協定。支援的通訊協定為 TLSv1.0、TLSv1.1 和 TLSv1.2。
SSODesktopType	`UseGnomeClassic`、`UseGnomeFlashback`、`UseGnomeUbuntu`、`UseMATE` 或 `UseKdePlasma`	N/A	此選項會指定 SSO 啟用時所要使用的桌面平台環境，而不是預設桌面平台環境。 在指定要使用選取的桌面平台環境之前，您必須先確定您的桌面平台已安裝該環境。在 Ubuntu 16.04/18.04 桌面平台中設定此選項後，無論 SSO 功能是否啟用，此選項都會生效。如果在 RHEL.x/CentOS 7.x 桌面平台中指定此選項，則必須在啟用 SSO 後，才會使用選取的桌面平台環境。 **備註** RHEL/CentOS 8.0 和 RHEL/CentOS 6.x 桌面平台不支援此選項。Horizon 7 僅支援 RHEL/CentOS 8.0 桌面平台上的 Gnome 桌面平台環境。如需在 RHEL/CentOS 6.x 桌面平台上啟用 SSO 時如何將 KDE 設定為預設桌面平台環境的詳細資訊，請參閱#unique_20/unique_20_Connect_42_section_F8FCD42564F3457A9491B067F9F65276。
SSOEnable	`true` 或 `false`	`true`	設定此選項可啟用/停用單一登入 (SSO)。
SSOUserFormat	文字字串	[username]	使用此選項來指定 Single Sign-On 登入名稱的格式。預設值為僅使用者名稱。如果也需要網域名稱，請設定此選項。一般來說，登入名稱為網域名稱加上特殊字元並接著使用者名稱。如果特殊字元為反斜線，您必須使用另一個反斜線來逸出。登入名稱格式的範例如下所示： ■ SSOUserFormat=[domain]\\[username] ■ SSOUserFormat=[domain]+[username] ■ SSOUserFormat=[username]@[domain]
子網路	採用 CIDR IP 位址格式的值	[subnet]	將此選項設定為子網路，其他機器可用它來連線至 Horizon Agent for Linux。如果有多個具有不同子網路的本機 IP 位址，則會使用已設定子網路中的本機 IP 位址來連線至 Horizon Agent for Linux。您必須以 CIDR IP 位址格式指定該值。例如，Subnet=123.456.7.8/24。

表 4-3. /etc/vmware/viewagent-custom.conf 中的組態選項 (續)

選項	值	預設值	說明
UEMEnable	true 或 false	false	設定此選項，可啟用或停用 Dynamic Environment Manager 智慧型原則。如果選項設為啟用，且在滿足 Dynamic Environment Manager 智慧型原則中的條件時，即會強制執行原則。
UEMNetworkPath	文字字串		必須將這個選項設定為在 User Environment Manager 主控台中設定的相同網路路徑。路徑的格式必須類似於 //10.111.22.333/view/LinuxAgent/UEMConfig。

備註 SSLCiphers、SSLProtocols 和 SSLCipherServerPreference 這三個安全性選項是用於 VMwareBlastServer 處理程序。啟動 VMwareBlastServer 處理程序時，Java Standalone Agent 會將這些選項傳入為參數。啟用 Blast 安全閘道 (BSG) 時，這些選項會影響 BSG 與 Linux 桌面平台之間的連線。停用 BSG 時，這些選項會影響用戶端與 Linux 桌面平台之間的連線。

HTML Access 的群組原則設定

HTML Access 的群組原則設定會在名為 vdm_blast.adm 和 vdm_blast.admx 的 ADM 和 ADMX 範本檔中進行指定。範本適用於 VMware Blast 顯示通訊協定，即 HTML Access 使用的唯一顯示通訊協定。

對於 HTML Access 4.0 及更新版本與 Horizon 7 (7.x 版)，《在 Horizon 7 中設定遠端桌面平台功能》文件中的〈VMware Blast 原則設定〉說明了 VMware Blast 群組原則設定。

如果您有 HTML Access 3.5 或更早版本和 Horizon 6 (6.2.x 版) 或更早版本，下表說明了適用於 HTML Access 的群組原則設定。在 Horizon 7 (7.x 版) 及更新版本中，有更多 VMware Blast 群組原則設定可供使用。

表 4-4. HTML Access 3.5 或更早版本和 Horizon 6 (6.2.x 版) 或更早版本的群組原則設定

設定	說明
畫面空白	控制是否可在 HTML Access 工作階段時，從 Horizon 6 外檢視遠端虛擬機器。例如，管理員可能在使用者透過 HTML Access 連線至桌面平台時，使用 vSphere Web Client 來開啟虛擬機器上的主控台。 啟用或未設定此設定時，若有人嘗試從 Horizon 6 外存取遠端虛擬機器，而 HTML Access 工作階段正在使用中，則遠端虛擬機器可能顯示空白畫面。
工作階段回收	控制已放棄遠端工作階段的廢棄項目收集。啟用此設定時，您可設定回收的間隔和閾值。 間隔會控制回收器執行的頻率。您可設定間隔的單位為毫秒。 閾值會決定工作階段持續的時間，就會廢棄並成為可刪除的項目。您可設定閾值的單位為秒。

表 4-4. HTML Access 3.5 或更早版本和 Horizon 6 (6.2.x 版) 或更早版本的群組原則設定 (續)

設定	說明
設定剪貼簿重新導向	決定允許剪貼簿重新導向的方向。僅可複製和貼上文字。您可選取以下其中一個值： ■ **僅啟用用戶端到伺服器** (代表僅允許從用戶端系統複製和貼上到遠端桌面平台。) ■ **兩個方向都停用** ■ **兩個方向都啟用** ■ **僅啟用伺服器到用戶端** (代表僅允許從遠端桌面平台複製和貼上到用戶端系統。) 此設定僅適用於 View Agent 或 Horizon Agent。 停用或未設定此設定時，預設值為**僅啟用用戶端到伺服器**。
HTTP 服務	允許您變更 Blast Agent 服務的安全 (HTTPS) TCP 連接埠。預設連接埠是 22443。 啟用此設定，可變更連接埠編號。若要變更此設定，您必須也更新受影響遠端桌面平台 (已安裝 View Agent 或 Horizon Agent) 之防火牆上的設定。

Horizon Client 組態範本中的安全性設定

安全性相關的設定是在 Horizon Client ADM 和 ADMX 範本檔的「安全性」區段和「指令碼定義」區段中提供。ADM 範本檔名為 `vdm_client.adm`，而 ADMX 範本檔名為 `vdm_client.admx`。除非另有說明，否則這些設定僅包含「電腦設定」設定。如果有提供「使用者設定」設定，且您為此設定定義一個值，則該值會複寫相等的「電腦設定」設定。

下表說明 ADM 和 ADMX 範本檔中「安全性」區段的設定。

表 4-5. Horizon Client 組態範本：安全性設定

設定	說明
`Allow command line credentials` (電腦組態設定)	決定是否可以透過 Horizon Client 命令列選項提供使用者認證。如果已停用此設定，則使用者從命令列執行 Horizon Client 時就無法使用 `smartCardPIN` 和 `password` 選項。 此設定依預設為啟用。 對等的 Windows 登錄值為 `AllowCmdLineCredentials`。
`Servers Trusted For Delegation` (電腦組態設定)	指定使用者選取**以目前使用者身分登入**核取方塊時，接受使用者識別碼和認證資訊的連線伺服器執行個體。如果您未指定任何連線伺服器執行個體，則所有連線伺服器執行個體都可以接受這項資訊。 若要新增連線伺服器執行個體，請使用下列其中一種格式： ■ **`domain\system$`** ■ **`system$@domain.com`** ■ 連線伺服器服務的服務主體名稱 (SPN)。 對等的 Windows 登錄值為 `BrokersTrustedForDelegation`。

表 4-5. Horizon Client 組態範本：安全性設定 (續)

設定	說明
Certificate verification mode (電腦組態設定)	設定 Horizon Client 執行的憑證檢查層級。您可以選取下列其中一種模式： ■ No Security。沒有憑證檢查。 ■ Warn But Allow。如果連線伺服器主機出示自我簽署憑證，則會出現警告，但使用者仍可繼續連線到連線伺服器。憑證名稱不需要符合使用者在 Horizon Client 中提供的連線伺服器名稱。如果發生其他任何憑證錯誤情況，將會顯示錯誤對話方塊，並且阻止使用者連線到連線伺服器。Warn But Allow 是預設值。 ■ Full Security。如果發生任何類型的憑證錯誤，使用者就無法連線到連線伺服器。使用者會看見憑證錯誤。 設定此群組原則設定時，使用者可以檢視 Horizon Client 中選取的憑證驗證模式，但是無法進行設定。SSL 組態對話方塊會通知使用者，管理員已鎖定這項設定。 若未設定或已停用此設定，Horizon Client 使用者就可以選取憑證驗證模式。 如果您不想將憑證驗證設定設為群組原則，您也可以藉由修改 Windows 登錄設定來啟用憑證驗證。
Default value of the 'Log in as current user' checkbox (電腦和使用者組態設定)	指定 Horizon Client 連線對話方塊上**以目前使用者身分登入**核取方塊的預設值。 此設定會覆寫 Horizon Client 安裝期間指定的預設值。 如果使用者從命令列執行 Horizon Client 並指定 logInAsCurrentUser 選項，則該值會覆寫此設定。 選取**以目前使用者身分登入**核取方塊時，使用者登入用戶端系統時提供的身分和認證資訊都會傳遞至連線伺服器執行個體，且最終傳遞至遠端桌面平台。取消選取此核取方塊時，使用者必須多次提供身分和認證資訊，才能存取遠端桌面平台。 此設定依預設為停用。 對等的 Windows 登錄值為 LogInAsCurrentUser。
Display option to Log in as current user (電腦和使用者組態設定)	決定是否可以在 Horizon Client 連線對話方塊上看到**以目前使用者身分登入**核取方塊。 如果可以看到，使用者就可以選取或取消選取該核取方塊，並且覆寫其預設值。如果隱藏，使用者就無法在 Horizon Client 連線對話方塊中覆寫該核取方塊的預設值。 您可以使用原則設定 Default value of the 'Log in as current user' checkbox 指定**以目前使用者身分登入**核取方塊的預設值。 此設定依預設為啟用。 對等的 Windows 登錄值為 LogInAsCurrentUser_Display。
Enable jump list integration (電腦組態設定)	決定跳躍清單是否會出現在 Windows 7 及更新版本系統工作列上的 Horizon Client 圖示中。跳躍清單可讓使用者連線至最近的連線伺服器執行個體和遠端桌面平台。 如果 Horizon Client 為共用狀態，您可能不希望使用者看到最近的桌面平台名稱。您可以停用此設定以停用跳躍清單。 此設定依預設為啟用。 對等的 Windows 登錄值為 EnableJumplist。
Enable SSL encrypted framework channel (電腦和使用者組態設定)	決定是否要啟用以 SSL 加密的架構通道。 ■ **啟用**：啟用 SSL，但如果遠端桌面平台沒有 SSL 支援，則允許退回之前的未加密連線。 ■ **停用**：停用 SSL。不建議使用此設定，但如果不存在通道，且之後可能由 WAN 加速器產品進行最佳化，則此設定可能有用。 ■ **強制執行**：啟用 SSL，並拒絕連線到沒有 SSL 支援的桌面平台。 對等的 Windows 登錄值為 EnableTicketSSLAuth。

表 4-5. Horizon Client 組態範本：安全性設定 (續)

設定	說明
`Configures SSL protocols and cryptographic algorithms` (電腦和使用者組態設定)	設定加密清單，以限制在建立加密 SSL 連線之前某些密碼編譯演算法和通訊協定的使用。加密清單由一個或多個以冒號分隔的加密字串組成。 **備註** 所有加密字串均區分大小寫。 ■ Horizon Client 4.10 及更新版本的預設值為 **TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES** ■ Horizon Client 4.2 及更新版本的預設值為 **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES** ■ Horizon Client 4.0.1 和 4.1 的預設值為 **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH**。 ■ Horizon Client 4.0 的預設值為 **TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH**。 ■ Horizon Client 3.5 的預設值為 **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH**。 ■ Horizon Client 3.3 和 3.4 的預設值為 **TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH**。 ■ Horizon Client 3.2 及更早版本的值為 **SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH**。 從 Horizon Client 4.10 開始已永久停用 TLS v1.0，因此不再支援 TLS v1.0。 在 Horizon Client 4.0.1 到 4.9 中，會啟用 TLS v1.0、TLS v1.1 和 TLS v1.2。(SSL v2.0 和 v3.0 已移除。)如果 TLS v1.0 不一定要與伺服器相容，您可以停用 TLS v1.0。 在 Horizon Client 4.0 中，會啟用 TLS v1.1 和 TLS v1.2。(TLS v1.0 已停用。SSL v2.0 和 v3.0 已移除。) 在 Horizon Client 3.5 中，會啟用 TLS v1.0、TLS v1.1 和 TLS v1.2。(停用 SSL v2.0 和 v3.0。)在 Horizon Client 3.3 及 3.4 中，會啟用 TLS v1.0 和 TLS v1.1。(停用 SSL v2.0、v3.0 和 TLS v1.2。) 在 Horizon Client 3.2 及更早版本中，也會啟用 SSL v3.0。(停用 SSL v2.0 和 TLS v1.2。) 加密套件使用 128 或 256 位元 AES，移除匿名 DH 演算法，然後依加密演算法金鑰長度為目前加密清單排序。 組態的參考連結：http://www.openssl.org/docs/apps/ciphers.html 對等的 Windows 登錄值為 `SSLCipherList`。 如果您不想將此設定設為群組原則，您也可以將 `SSLCipherList` 值名稱新增至用戶端電腦上的下列其中一個登錄機碼，以啟用此設定： ■ 針對 32 位元 Windows：`HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security` ■ 針對 64 位元 Windows：`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware,Inc.\VMware VDM\Client\Security`
`Enable Single Sign-On for smart card authentication` (電腦組態設定)	決定是否啟用智慧卡驗證的單一登入。啟用單一登入時，Horizon Client 會先將加密的智慧卡 PIN 儲存在暫存記憶體中，再提交至連線伺服器。停用單一登入時，Horizon Client 不會顯示自訂的 PIN 對話方塊。 對等的 Windows 登錄值為 `EnableSmartCardSSO`。

下表說明 ADM 和 ADMX 範本檔中「指令碼定義」區段的設定。

表 4-6. 指令碼定義區段中的安全性相關設定

設定	說明
`Connect all USB devices to the desktop on launch`	決定用戶端系統上的所有可用 USB 裝置是否在啟動桌面平台時連線至桌面平台。 此設定依預設為停用。 對等的 Windows 登錄值為 `connectUSBOnStartup`。
`Connect all USB devices to the desktop when they are plugged in`	決定是否將外掛到用戶端系統的 USB 裝置連線至桌面平台。 此設定依預設為停用。 對等的 Windows 登錄值為 `connectUSBOnInsert`。
`Logon Password`	指定 Horizon Client 登入時使用的密碼。Active Directory 會以純文字格式儲存密碼。 預設未定義此設定。 對等的 Windows 登錄值為 `Password`。

如需有關這些設定及其安全性含意的詳細資訊，請參閱 Windows 版 Horizon Client 說明文件。

設定 Horizon Client 憑證驗證模式

您可以將 `CertCheckMode` 值名稱新增至 Windows 用戶端電腦上的登錄機碼，藉以設定 Horizon Client 憑證驗證模式。

在 32 位元 Windows 系統上，登錄機碼為 `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`。在 64 位元 Windows 系統上，登錄機碼為 `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`。

在登錄機碼中使用下列其中一個值：

- `0` - 實作**不要驗證伺服器身分識別憑證**選項。
- `1` - 實作**在連線至未受信任的伺服器前提出警告**選項。
- `2` - 實作**永不連線至未受信任的伺服器**選項。

您也可以藉由設定憑證驗證模式群組原則設定，來設定 Horizon Client 憑證驗證模式。如果您在登錄機碼中同時設定了群組原則設定及 `CertCheckMode` 設定，則群組原則設定的優先順序會高於登錄機碼值。

設定群組原則設定或登錄設定時，使用者可以檢視 Horizon Client 中選取的憑證驗證模式，但是無法進行設定。

如需設定憑證驗證模式群組原則設定的相關資訊，請參閱 Horizon Client 組態範本中的安全性設定。

設定本機安全性授權保護

Horizon Client 和 Horizon Agent 支援本機安全性授權 (LSA) 保護。LSA 保護可防止具有未受保護認證的使用者讀取記憶體及插入程式碼。

如需關於設定 LSA 保護的詳細資訊，請閱讀 Microsoft Windows Server 說明文件。

為 Horizon Client 4.4 及更早版本設定 LSA 保護時，下列功能會失敗：

- 以目前使用者身分登入

為 Horizon 7 (7.2 版) 以前的 Horizon Agent 版本設定 LSA 保護時，下列功能會失敗：

- 智慧卡驗證
- True SSO

設定安全性通訊協定及加密套件

5

您可以設定 Horizon Client、View Agent/Horizon Agent 和伺服器元件之間所接受和建議的安全性通訊協定及加密套件。

本章節討論下列主題：

安全性通訊協定及加密套件的預設原則

全域接受和建議原則依預設會啟用特定的安全性通訊協定和加密套件。

下表列出依預設為 Horizon Client 啟用的通訊協定和加密套件。在 Windows 版、Linux 版和 Mac 版 Horizon Client 3.1 及更新版本中，這些加密套件和通訊協定也用來加密 USB 通道 (USB 服務精靈和 View Agent 或 Horizon Agent 之間的通訊)。若為 4.0 以前的 Horizon Client 版本，USB 服務精靈會在連線到遠端桌面平台時將 `RC4 ( :RC4-SHA: +RC4 )` 新增至加密控制字串的尾端。從 Horizon Client 4.0 起不再新增 RC4。

Horizon Client 4.2 及更新版本

表 5-1. Horizon Client 4.2 及更新版本上依預設會啟用安全性通訊協定和加密套件

預設安全性通訊協定	預設加密套件
TLS 1.2	■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1 ■ TLS 1.0 **備註** 從 Horizon Client 4.10 開始已永久停用 TLS v1.0，因此不再支援 TLS v1.0。	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

從 Horizon Client 4.10 開始已永久停用 TLS v1.0，因此不再支援 TLS v1.0。

在 Horizon Client 4.2 到 4.9 中，依預設會啟用 TLS v1.0，以確保 Horizon Client 依預設可連線到 Horizon Cloud 隨附裝載的基礎結構伺服器。預設的加密字串為 !aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES。如果 TLS v1.0 不一定要與伺服器相容，您可以停用 TLS v1.0。

Horizon Client 4.0.1 和 4.1

表 5-2. Horizon Client 4.0.1 和 4.1 上依預設會啟用安全性通訊協定和加密套件

預設安全性通訊協定	預設加密套件
TLS 1.2	■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1 ■ TLS 1.0	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

依預設會啟用 TLS 1.0，以確保 Horizon Client 依預設可連線到 Horizon Cloud 隨附裝載的基礎結構伺服器。預設加密字串為 TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA +AES:@STRENGTH。如果 TLS 1.0 不一定要與伺服器相容，您可以停用 TLS 1.0。

Horizon Client 4.0

表 5-3. Horizon Client 4.0 上依預設會啟用安全性通訊協定和加密套件

預設安全性通訊協定	預設加密套件
TLS 1.2	■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

重要 TLS 1.0 依預設為停用。SSL 3.0 已移除。

Horizon Client 3.5

表 5-4. Horizon Client 3.5 上依預設會啟用安全性通訊協定和加密套件

預設安全性通訊協定	預設加密套件
TLS 1.2	■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1 ■ TLS 1.0	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Horizon Client 3.3 和 3.4

表 5-5. Horizon Client 3.3 和 3.4 上依預設會啟用安全性通訊協定和加密套件

預設安全性通訊協定	預設加密套件
■ TLS 1.1 ■ TLS 1.0	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

備註 也支援 TLS 1.2，但未預設啟用。若要啟用 TLS 1.2，請遵循 VMware 知識庫 2121183 中的指示，完成指示後即可支援表 5-4. Horizon Client 3.5 上依預設會啟用安全性通訊協定和加密套件 中所列的加密套件。

Horizon Client 3.0、3.1 和 3.2

表 5-6. Horizon Client 3.0、3.1 和 3.2 上依預設會啟用安全性通訊協定和加密套件

預設安全性通訊協定	預設加密套件
■ TLS 1.1 ■ TLS 1.0 ■ SSL 3.0 (僅在 Windows 用戶端上啟用)	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA (0xc022) ■ TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA (0xc021) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA (0xc01f) ■ TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA (0xc01e) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

備註 也支援 TLS 1.2，但未預設啟用。若要啟用 TLS 1.2，請遵循 VMware 知識庫 2121183 中的指示，完成指示後即可支援表 5-4. Horizon Client 3.5 上依預設會啟用安全性通訊協定和加密套件 中所列的加密套件。

針對特定用戶端類型設定安全性通訊協定和加密套件

對於設定所使用的通訊協定和加密套件，每個用戶端類型都有自己的方法。

只有 View Server 不支援目前設定時，您才應在 Horizon Client 中變更安全性通訊協定。如果為 Horizon Client 設定安全性通訊協定，但未在用戶端連線的 View Server 上啟用該通訊協定，則會發生 TLS/SSL 錯誤，並且連線會失敗。

若要將通訊協定和加密變更為預設值以外的值，請使用用戶端特定機制：

- 在 Windows 用戶端系統上，您可以使用群組原則設定或 Windows 登錄設定。
- 在 Windows 10 UWP 用戶端系統上，您可以使用 Horizon Client 選項中的 SSL 選項設定。
- 在 Linux 用戶端系統上，您可以使用組態檔內容或命令列選項。
- 在 Mac 用戶端系統上，您可以使用 Horizon Client 中的 [喜好設定] 設定。
- 在 iOS、Android 和 Chrome OS 用戶端系統上，您可以使用 Horizon Client 設定中的 [進階 SSL 選項] 設定。

如需詳細資訊，請參閱 Horizon Client 說明文件。

在 SSL/TLS 中停用弱加密

為獲得更佳的安全性，您可設定網域原則 GPO (群組原則物件)，以確保執行 View Agent 或 Horizon Agent 的 Windows 機器不會在使用 SSL/TLS 通訊協定通訊時使用弱加密。

程序

1. 在 Active Directory 伺服器上，選取**開始 > 系統管理工具 > 群組原則管理**，並在 GPO 上按一下滑鼠右鍵，然後選取**編輯**，來編輯 GPO。
2. 在群組原則管理編輯器中，瀏覽至**電腦設定 > 原則 > 系統管理範本 > 網路 > SSL 組態設定**。
3. 按兩下 **SSL 加密套件順序**。
4. 在 [SSL 加密套件順序] 視窗中，按一下**啟用**。
5. 在 [選項] 窗格中，以下列加密清單取代 [SSL 加密套件] 文字方塊的所有內容。

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

加密套件在上方以單獨行列出以便閱讀。當您將清單貼在文字方塊內時，加密套件必須位於一行中且逗點後不含空格。

6 結束群組原則管理編輯器。

7 重新啟動 View Agent 或 Horizon Agent 機器，使新的群組原則生效。

針對 HTML Access Agent 設定安全性通訊協定和加密套件

從 View Agent 6.2 開始，您可以透過編輯 Windows 登錄來設定 HTML Access Agent 使用的加密套件。從 View Agent 6.2.1 開始，您也可以設定所使用的安全性通訊協定。您也可以在群組原則物件 (GPO) 中指定組態。

對於 View Agent 6.2.1 和更新版本，HTML Access Agent 預設僅使用 TLS 1.1 和 TLS 1.2。允許的通訊協定如下 (從低到高)：TLS 1.0、TLS 1.1 和 TLS 1.2。絕不允許較舊的通訊協定，例如 SSLv3 和更早的通訊協定。`SslProtocolLow` 和 `SslProtocolHigh` 這兩個登錄值會決定 HTML Access Agent 將接受的通訊協定範圍。例如，`SslProtocolLow=tls_1.0` 和 `SslProtocolHigh=tls_1.2` 設定將造成 HTML Access Agent 接受 TLS 1.0、TLS 1.1 和 TLS 1.2。預設設定為 `SslProtocolLow=tls_1.1` 和 `SslProtocolHigh=tls_1.2`。

您必須使用 https://www.openssl.org/docs/manmaster/man1/ciphers.html 的〈CIPHER LIST FORMAT〉一節中所定義的格式來指定加密清單。下列是預設的加密清單：

```
ECDHE-RSA-AES256-SHA:AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

程序

1 啟動 Windows 登錄編輯程式。

2 導覽至 `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` 登錄機碼。

3 新增兩個新字串 (REG_SZ) 值 `SslProtocolLow` 和 `SslProtocolHigh`，以指定通訊協定的範圍。

   登錄值的資料必須是 `tls_1.0`、`tls_1.1` 或 `tls_1.2`。若僅要啟用一個通訊協定，請為這兩個登錄值指定相同的通訊協定。如果這兩個登錄值有任何一個不存在，或其資料未設為三個通訊協定的其中一個，則會使用預設的通訊協定。

4 新增新字串 (REG_SZ) 值 `SslCiphers`，以指定加密套件清單。

   在登錄值的資料欄位中輸入或貼上加密套件清單。例如，

   ```
   ECDHE-RSA-AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
   ```

5 重新啟動 VMware Blast 這個 Windows 服務。

若要還原為使用預設加密清單，請刪除 `SslCiphers` 登錄值，並重新啟動 VMware Blast 這個 Windows 服務。請勿僅刪除值的資料部分，因為 HTML Access Agent 會依據 OpenSSL 加密清單格式定義，將所有加密視為無法接受。

HTML Access Agent 啟動時，會將通訊協定和加密資訊寫入其記錄檔。您可以檢查記錄檔，以判斷所實施的值。

在未來，預設的通訊協定和加密套件可能會變更，以因應 VMware 不斷演進的網路安全性最佳做法。

在遠端桌面平台上設定建議原則

您可以在執行 Windows 的遠端桌面平台上設定建議原則，以控制連線到連線伺服器的訊息匯流排安全性。

請確實將連線伺服器設定成接受相同原則，以避免連線失敗。

程序

1. 在遠端桌面平台上啟動 Windows 登錄編輯程式。
2. 導覽至 `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration` 登錄機碼。
3. 新增字串 (REG_SZ) 值 `ClientSSLSecureProtocols`。
4. 以 **\LIST:*protocol_1*,*protocol_2*,...** 的格式將值設定為加密套件清單。

   列出通訊協定，愈新的通訊協定愈先列出。例如：

   ```
   \LIST:TLSv1.2,TLSv1.1,TLSv1
   ```

5. 新增字串 (REG_SZ) 值 `ClientSSLCipherSuites`。
6. 以 **\LIST:*cipher_suite_1*,*cipher_suite_2*,...** 的格式將值設定為加密套件清單。

   此清單應依照喜好順序列出，且愈常用的加密套件愈先列出。例如：

   ```
   \LIST:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
   ```

用戶端和代理程式記錄檔位置

6

用戶端和代理程式所建立的記錄檔會記錄其元件的安裝與作業。

本章節討論下列主題：

Windows 版 Horizon Client 記錄

記錄檔有助於疑難排解安裝、顯示通訊協定和各種功能元件的問題。您可以使用群組原則設定來設定部分記錄檔的位置、詳細資訊和保留期間。

記錄位置

針對下表中的檔案名稱，*YYYY* 代表年，*MM* 為月，*DD* 為日，而 *XXXXXX* 為數字。

表 6-1. Windows 版 Horizon Client 記錄檔

記錄類型	目錄路徑	檔案名稱
安裝	`C:\Users\%username%\AppData\Local\Temp`	`vminst.log_XXXXXX_XXXXXX.txt` `vmmsi.log_XXXXXX_XXXXXX.txt`
PCoIP 用戶端 來自 `vmware-remotemks.exe` 處理程序	`C:\Users\%username%\AppData\Local\Temp`	`pcoip_client_YYYY_MM_DD_XXXXXX.txt` **備註** 您可以使用 GPO 來設定記錄層級，從 0 到 3 (最詳細)。請使用 View PCoIP 用戶端工作階段變數 ADMX 範本檔 `pcoip.admx`。此設定稱為**設定 PCoIP 事件記錄詳細資訊**。

表 6-1. Windows 版 Horizon Client 記錄檔 (續)

記錄類型	目錄路徑	檔案名稱
Horizon Client UI 來自 vmware-view.exe 處理程序	C:\Users\%*username*%\AppData\Local\VMware\VDM\Logs	vmware-horizon-viewclient-*YYYY-MM-DD-XXXXXX*.txt **備註** 您可以使用 GPO 來設定記錄位置。請使用 View 一般組態 ADMX 範本檔 vdm_common.admx。
Horizon Client 記錄 來自 vmware-view.exe 處理程序	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username-XXXXXX*	vmware-crtbora-*XXXXXX*.log
訊息架構	C:\Users\%*username*%\AppData\Local\VMware\VDM\Logs	log-*YYYY-MM-DD-XXXXXX*.txt debug-*YYYY-MM-DD-XXXXXX*.txt
遠端 MKS (mouse-keyboard-screen) 記錄 來自 vmware-remotemks.exe 處理程序	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username*	ViewMP-Client-*XXXXXX*.log vmware-mks-*XXXXXX*.log vmware-rdeSvc-*XXXXXX*.log vmware-vvaClient-*XXXXXX*.log
Tsdr 用戶端 來自 vmware-remotemks.exe 處理程序	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username*	vmware-ViewTsdr-Client-*XXXXXX*.log
Tsmmr 用戶端 來自 vmware-remotemks.exe 處理程序	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username*	vmware-ViewTsmmr-Client-*XXXXXX*.log
VdpService 用戶端 來自 vmware-remotemks.exe 處理程序	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username*	vmware-vdpServiceClient-*XXXXXX*.log
WSNM 服務 來自 wsnm.exe 處理程序	C:\ProgramData\VMware\VDM\logs	debug-yyyy-mm-dd-*XXXXXX*.txt **備註** 您可以使用 GPO 來設定記錄位置。請使用 View 一般組態 ADMX 範本檔 vdm_common.admx。
USB 重新導向 來自 vmware-view-usbd.exe 或 vmware-remotemks.exe 處理程序	C:\ProgramData\VMware\VDM\logs	debug-yyyy-mm-dd-*XXXXXX*.txt 在 Horizon Client 4.4 及更新版本中，vmware-view-usbd.exe 處理程序已移除，並且 USBD 處理程序已移至 vmware-remotemks.exe 處理程序。 **備註** 您可以使用 GPO 來設定記錄位置。請使用 View 一般組態 ADMX 範本檔 vdm_common.admx。
序列埠重新導向 來自 vmwsprrdpwks.exe 處理程序	C:\ProgramData\VMware\VDM\Logs	Serial*.txt Netlink*.txt
掃描器重新導向 來自 ftscanmgr.exe 處理程序	C:\ProgramData\VMware\VDM\Logs	Scanner*.txt Netlink*.txt

記錄組態

您可以使用群組原則設定來進行一些組態變更：

- 針對 PCoIP 用戶端記錄，您可以設定記錄層級，從 0 到 3 (最詳細)。請使用 View PCoIP 用戶端工作階段變數 ADMX 範本檔 `pcoip.admx`。此設定稱為**設定 PCoIP 事件記錄詳細資訊**。
- 針對用戶端 UI 記錄，設定記錄位置、詳細資訊和保留原則。請使用 View 一般組態 ADMX 範本檔 `vdm_common.admx`。
- 針對 USB 重新導向記錄，設定記錄位置、詳細資訊和保留原則。請使用 View 一般組態 ADMX 範本檔 `vdm_common.admx`。
- 針對 WSNM 服務記錄，設定記錄位置、詳細資訊和保留原則。請使用 View 一般組態 ADMX 範本檔 `vdm_common.admx`。

您也可以使用命令列命令來設定詳細資訊等級。導覽至 `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT` 目錄，並輸入下列命令：

```
support.bat loglevels
```

將會顯示新的命令提示字元視窗，並提示您選取詳細資訊等級。

收集記錄服務包

您可以使用用戶端 UI 或命令列命令將記錄收集到 .zip 檔案，以便傳送該檔案給 VMware 技術支援。

- 在 **Horizon Client** 視窗中，從 [選項] 功能表選取**支援資訊**，並在顯示的對話方塊中，按一下**收集支援資料**。
- 從命令列，導覽至 `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT` 目錄，並輸入下列命令：`support.bat`。

Mac 版 Horizon Client 記錄

記錄檔有助於疑難排解安裝、顯示通訊協定和各種功能元件的問題。您可以建立組態檔來設定詳細資訊等級。

記錄位置

表 6-2. Mac 版 Horizon Client 記錄檔

記錄類型	目錄路徑	檔案名稱
Horizon Client UI	`~/Library/Logs/VMware Horizon Client`	
PCoIP 用戶端	`~/Library/Logs/VMware Horizon Client`	
即時音訊視訊	`~/Library/Logs/VMware`	`vmware-RTAV-pid.log`
USB 重新導向	`~/Library/Logs/VMware`	
VChan	`~/Library/Logs/VMware Horizon Client`	

表 6-2. Mac 版 Horizon Client 記錄檔 (續)

記錄類型	目錄路徑	檔案名稱
遠端 MKS (mouse-keyboard-screen) 記錄	~/Library/Logs/VMware	
Crtbora	~/Library/Logs/VMware	

記錄組態

在 Horizon Client 3.1 及更新版本中，Horizon Client 會在 Mac 用戶端上的 ~/Library/Logs/VMware Horizon Client 目錄中產生記錄檔。管理員可透過在 Mac 用戶端上的 /Library/Preferences/com.vmware.horizon.plist 檔案中設定機碼，來設定記錄檔的數目上限以及可保留記錄檔的天數上限。

表 6-3. 用於記錄檔收集的 plist 機碼

機碼	說明
MaxDebugLogs	記錄檔的數目上限。上限值為 100。
MaxDaysToKeepLogs	可保留記錄檔的天數上限。此值沒有限制。

當您啟動 Horizon Client 時，將刪除與這些準則不符的檔案。

如果未在 com.vmware.horizon.plist 檔案中設定 MaxDebugLogs 或 MaxDaysToKeepLogs 機碼，則記錄檔的預設數目為 5 個，可保留記錄檔的預設天數為 7 天。

Linux 版 Horizon Client 記錄

記錄檔有助於疑難排解安裝、顯示通訊協定和各種功能元件的問題。您可以建立組態檔來設定詳細資訊等級。

記錄位置

表 6-4. Linux 版 Horizon Client 記錄檔

記錄類型	目錄路徑	檔案名稱
安裝	/tmp/vmware-root/	.vmware-installer-pid.log vmware-vmis-pid.log
Horizon Client UI	/tmp/vmware-*username*/	vmware-horizon-client-pid.log
PCoIP 用戶端	/tmp/teradici-*username*/	pcoip_client_*YYYY_MM_DD_XXXXXX*.log
即時音訊視訊	/tmp/vmware-*username*/	vmware-RTAV-pid.log
USB 重新導向	/tmp/vmware-root/	vmware-usbarb-pid.log vmware-view-usbd-pid.log
VChan	/tmp/vmware-*username*/	VChan-Client.log **備註** 當您透過設定「export VMW_RDPVC_BRIDGE_LOG_ENABLED=1」啟用 RDPVCBridge 記錄時便會建立此記錄。

表 6-4. Linux 版 Horizon Client 記錄檔 (續)

記錄類型	目錄路徑	檔案名稱
遠端 MKS (mouse-keyboard-screen) 記錄	/tmp/vmware-*username*/	vmware-mks-pid.log vmware-MKSVchanClient-pid.log vmware-rdeSvc-pid.log
VdpService 用戶端	/tmp/vmware-*username*/	vmware-vdpServiceClient-pid.log
Tsdr 用戶端	/tmp/vmware-*username*/	vmware-ViewTsdr-Client-pid.log

記錄組態

您可以使用組態內容 (view.defaultLogLevel) 來設定用戶端記錄的詳細資訊等級，從 0 (收集所有事件) 到 6 (僅收集嚴重事件)。

針對 USB 的特定記錄，您可以使用下列命令列命令：

```
vmware-usbarbitrator --verbose
vmware-view-usbd -o log:trace
```

收集記錄服務包

記錄收集器位於 /usr/bin/vmware-view-log-collector。若要使用記錄收集器，您必須具備執行權限。您可以從 Linux 命令列輸入下列命令來設定權限：

```
chmod +x /usr/bin/vmware-view-log-collector
```

您可以從 Linux 命令列輸入下列命令來執行記錄收集器：

```
/usr/bin/vmware-view-log-collector
```

行動裝置上的 Horizon Client 記錄

在行動裝置上，您可能必須安裝協力廠商程式，以導覽至儲存記錄檔所在的目錄。行動用戶端具有用於傳送記錄服務包到 VMware 的組態設定。因為記錄可能影響效能，您應該只在必須疑難排解問題時啟用記錄。

iOS 用戶端記錄

針對 iOS 用戶端，記錄檔位於 *User Programs*/Horizon/ 下的 tmp 和 Documents 目錄中。若要導覽至這些目錄，您必須先安裝協力廠商應用程式，例如 iFunbox。

您可以透過開啟 Horizon Client 設定中的**記錄**設定來啟用記錄。在此設定啟用時，如果用戶端未預期地結束，或如果您結束用戶端然後重新啟動用戶端，記錄檔會合併並壓縮成單一 GZ 檔案。之後您可以透過電子郵件將服務包傳送給 VMware。如果您的裝置連接到 PC 或 Mac，您也可使用 iTunes 擷取記錄檔。

Android 用戶端記錄

針對 Android 用戶端，記錄檔位於 `Android/data/com.vmware.view.client.android/files/` 目錄中。若要導覽至此目錄，您必須先安裝協力廠商應用程式，例如 File Explorer 或 My Files。

依預設，只會在應用程式未預期地結束時建立記錄。您可以透過開啟 Horizon Client 設定中的**啟用記錄**設定來變更此預設值。若要透過電子郵件傳送記錄服務包給 VMware，您可以使用用戶端的 [一般設定] 中的**傳送記錄**設定。

Chrome OS 用戶端記錄

Chrome OS 用戶端的記錄僅能透過 JavaScript 主控台取得。

Windows 10 UWP 用戶端記錄

針對 Windows 10 UWP 用戶端，記錄位於 `C:\Windows\Users\%username%\AppData\Local\VMware\VDM\logs` 目錄中。

您可以透過開啟 Horizon Client 選項中 [記錄] 區段的**啟用進階記錄**選項，然後按一下**收集支援資訊**按鈕來啟用記錄。系統將會提示您選取用於記錄的資料夾，而且您可以如同對任何其他資料夾般壓縮該資料夾。

Windows 市集用戶端記錄

針對已安裝 Windows 市集版 Horizon Client (而不是 Windows 版 Horizon Client) 的 Windows 市集用戶端，記錄檔位於 `C:\Users\%username%\AppData\Local\Packages\VMwareInc.VMwareViewClient_23chmsjxv380w\LocalState\logs` 目錄中。

您可以透過開啟 Horizon Client [一般設定] 中的**啟用進階記錄**設定，然後按一下**收集支援資訊**按鈕來啟用記錄。系統將會提示您選取用於記錄的資料夾，而且您可以如同對任何其他資料夾般壓縮該資料夾。

來自 Windows 機器的 Horizon Agent 記錄

記錄檔有助於疑難排解安裝、顯示通訊協定和各種功能元件的問題。您可以使用群組原則設定來設定部分記錄檔的位置、詳細資訊和保留期間。

記錄位置

針對下表中的檔案名稱，*YYYY* 代表年，*MM* 為月，*DD* 為日，而 *XXXXXX* 為數字。

表 6-5. Windows 版 Horizon Client 記錄檔

記錄類型	目錄路徑	檔案名稱
安裝	C:\Users\%*username*%\AppData\Local\Temp	vminst.log_*XXXXXX_XXXXXX*.txt vmmsi.log_*XXXXXX_XXXXXX*.txt
View Agent (適用於 Horizon 6) 或 Horizon Agent (適用於 Horizon 7)	*<Drive Letter>*:\ProgramData\VMware\VDM\logs	pcoip_agent_*YYYY_MM_DD_XXXXXX*.txt pcoip_agent_*YYYY_MM_DD_XXXXXX*.txt vmware-vdpServiceServer-*XXXXXX*.log Serial*.txt Scanner*.txt Netlink*.txt debug-yyyy-mm-dd-*XXXXXX*.txt **備註** 您可以使用 GPO 來設定記錄位置。請使用 View 一般組態 ADMX 範本檔 vdm_common.admx。

記錄組態

有數個方法可供設定記錄選項。

- 您可以使用群組原則設定來設定記錄位置、詳細資訊和保留原則。請使用 View 一般組態 ADMX 範本檔 vdm_common.admx。
- 您可以使用命令列命令來設定詳細資訊等級。導覽至 C:\Program Files\VMware\VMware View\Agent\DCT 目錄，並輸入下列命令：support.bat loglevels。將會顯示新的命令提示字元視窗，並提示您選取詳細資訊等級。
- 您可以將 vdmadmin 命令與 -A 選項搭配使用，以設定依 View Agent 或 Horizon Agent 的記錄。如需指示，請參閱《Horizon 7 管理》文件。

收集記錄服務包

您可以使用命令列命令將記錄收集到 .zip 檔案，以便傳送該檔案給 VMware 技術支援。從命令列，導覽至 C:\Program Files\VMware\VMware View\Agent\DCT 目錄，並輸入下列命令：support.bat。

Linux 桌面平台記錄

記錄檔有助於疑難排解安裝、顯示通訊協定和各種功能元件的問題。您可以建立組態檔來設定詳細資訊等級。

記錄位置

表 6-6. Linux 桌面平台記錄檔

記錄類型	目錄路徑
安裝	/tmp/vmware-root
View Agent (適用於 Horizon 6) 或 Horizon Agent (適用於 Horizon 7)	/var/log/vmware
View Agent (適用於 Horizon 6) 或 Horizon Agent (適用於 Horizon 7)	/usr/lib/vmware/viewagent/viewagent-debug.log

記錄組態

編輯 /etc/vmware/config 檔案以設定記錄。

收集記錄服務包

您可以建立 Data Collection Tool (DCT) 服務包，該服務包會收集機器的組態資訊並記錄至壓縮的 tarball。在 Linux 桌面平台中開啟命令提示字元，並執行 dct-debug.sh 指令碼。

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

tarball 是在執行指令碼所在的目錄 (目前的工作目錄) 中產生。檔案名稱包含作業系統、時間戳記和其他資訊；例如：ubuntu-12-vdm-sdct-20150201-0606-agent.tgz

此命令會從 /tmp/vmware-root 目錄和 /var/log/vmware 目錄收集記錄檔，並且也會收集下列系統記錄和組態檔：

- /var/log/messages*
- /var/log/syslog*
- /var/log/boot*.log
- /proc/cpuinfo, /proc/meminfo, /proc/vmstat, /proc/loadavg
- /var/log/audit/auth.log*
- /etc/hosts
- /etc/resolv.conf
- /etc/nsswitch.conf
- /var/log/Xorg*
- /etc/X11/xorg.conf
- /usr/lib/vmware/viewagent 中的核心檔案
- /var/crash/_usr_lib_vmware_viewagent* 中的任何損毀檔案

套用安全性修補程式

7

修補程式發行版本可能包含下列 Horizon 6 或 Horizon 7 元件的安裝程式檔案：View Composer、連線伺服器、View Agent 或 Horizon Agent，以及各種用戶端。您必須套用的修補程式元件取決於部署所需的錯誤修正。

視所需的錯誤修正而定，按照下列順序安裝適用的 Horizon 6 或 Horizon 7 元件：

1 View Composer

2 連線伺服器

3 View Agent (適用於 Horizon 6) 或 Horizon Agent (適用於 Horizon 7)

4 Horizon Client

如需為伺服器元件套用修補程式的相關指示，請參閱 《Horizon 7 升級》文件。

本章節討論下列主題：

套用 View Agent 或 Horizon Agent 的修補程式

套用修補程式需下載及執行修補程式的安裝程式。

需要在以下位置執行下列步驟：連結複製桌面平台集區的父虛擬機器、完整複製集區中的每個虛擬機器桌面平台，或只包含一個虛擬機器桌面平台之集區的個別桌面平台虛擬機器。

必要條件

確認您要用來執行修補程式安裝程式的主機上，擁有具備管理權限的網域使用者帳戶。

程序

1 在所有父虛擬機器、用於完整複製範本的虛擬機器、集區中的完整複製以及手動新增的個別虛擬機器上，下載 View Agent (適用於 Horizon 6) 或 Horizon Agent (適用於 Horizon 7) 修補程式版本的安裝程式檔案。

   您的 VMware 連絡人會提供此下載的相關指示。

2 執行您針對 View Agent 或 Horizon Agent 修補程式版本所下載的安裝程式。

備註 在 Horizon 6 (6.2 版) 和更新版本中，您無須解除安裝舊版，即可安裝修補程式。

3 如果您已停用佈建新虛擬機器以準備套用修補程式到 View Composer，請再次啟用佈建。

4 針對將用來建立連結複製桌面平台集區的父虛擬機器，擷取虛擬機器的快照。

如需擷取快照的相關資訊，請參閱 vSphere Client 線上說明。

5 針對連結複製桌面平台集區，使用您所建立的快照重新撰寫桌面平台集區。

6 確認您可以使用 Horizon Client 登入已修補的桌面平台集區。

7 如果您取消了任何連結複製桌面平台集區的任何重新整理或重新撰寫作業，請再次排程工作。

套用 Horizon Client 修補程式

在桌面用戶端裝置上，套用修補程式需下載及執行修補程式的安裝程式。在行動用戶端上，套用修補程式只需安裝從銷售應用程式的網站 (例如 Google Play、Windows 市集或 Apple App Store) 取得的更新。

程序

1 在每個用戶端系統上，下載 Horizon Client 修補版本的安裝程式檔案。

您的 VMware 連絡人會提供此下載的相關指示。或者，您可以前往用戶端下載頁面：http://www.vmware.com/go/viewclients。正如之前所述，針對某些用戶端，您可能要從應用程式商店獲得修補程式發行版本。

2 如果用戶端裝置是 Mac 或 Linux 桌上型電腦或筆記型電腦，請從您的裝置上移除目前的用戶端軟體版本。

使用自訂的裝置專屬方法來移除應用程式。

備註 使用 Windows 版 Horizon Client 3.5 和更新版本時，您無須解除安裝舊版，即可在 Windows 用戶端上安裝修補程式。使用 Windows 版 Horizon Client 4.1 和更新版本時，您可以啟用 [線上升級 Horizon Client] 功能，以線上方式在 Windows 用戶端上升級 Horizon Client。使用 Mac 版 Horizon Client 4.4 及更新版本時，您可以啟用 [線上升級 Horizon Client] 功能，以線上方式在 Mac 用戶端上升級 Horizon Client。

3 如果適用的話，執行您針對 Horizon Client 修補程式發行版本所下載的安裝程式。

如果您是從 Apple App Store 或 Google Play 下載修補程式，當您下載應用程式時通常即已安裝，並不需要執行安裝程式。

4 確認您可以使用新修補的 Horizon Client 登入已修補的桌面平台集區。