Horizon 安全性

VMware Horizon 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

VMware Horizon 安全性

《Horizon 安全性》對於 VMware Horizon 的安全功能提供一個簡要的參考。

- 所需的系統和資料庫登入帳戶。
- 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。
- 必須針對正確 VMware Horizon 作業開啟或啟用的外部介面、連接埠以及服務。

主要對象

此資訊適用於 IT 決策者、架構設計人員、管理員，以及必須熟悉 VMware Horizon 安全性元件的其他人。

VMware Horizon 帳戶、資源和記錄檔 1

對特定元件使用不同的帳戶可防止給予個人超出其所需的存取權和權限。瞭解組態檔和具有敏感性資料的其他檔案的位置，有助於設定各種主機系統的安全性。

本章節討論下列主題：

VMware Horizon 帳戶

您必須設定系統與資料庫帳戶來管理 VMware Horizon 元件。

表 1-1. VMware Horizon 系統帳戶

Horizon 元件	必要帳戶
Horizon Client	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。使用者帳戶必須是遠端桌面平台使用者群組的成員，但這些帳戶不需要 Horizon 管理員權限。
vCenter Server	在 Active Directory 中，使用執行 vCenter Server 中支援 VMware Horizon 所需作業的權限，來設定使用者帳戶。 如需所需權限的相關資訊，請參閱《Horizon 安裝》文件。
連線伺服器	在安裝 VMware Horizon 時，您可以將特定的網域使用者、本機管理員群組或特定的網域使用者群組指定為 Horizon 管理員。建議您建立 Horizon 管理員專用的網域使用者群組。預設值是目前登入的網域使用者。 在 Horizon Console 中，您可以使用**設定 > 管理員**來變更 Horizon 管理員清單。 請參閱《Horizon 管理》文件以取得所需權限的相關資訊。

表 1-2. Horizon 資料庫帳戶

Horizon 元件	必要帳戶
Horizon Connection Server 所使用的事件資料庫	Microsoft SQL Server、Oracle 或 PostgreSQL 資料庫會儲存 Horizon 事件資料。您需要針對 Horizon Console 可用來存取事件資料的資料庫建立管理帳戶。

若要降低安全性弱點的風險，請採取下列動作：

- 在不同於您組織所使用的其他資料庫伺服器的伺服器上，設定 VMware Horizon 資料庫。

- 請不要允許單一使用者帳戶存取多個資料庫。
- 針對事件資料庫的存取設定個別的帳戶。

VMware Horizon 資源

VMware Horizon 包含必須受到保護的數個組態檔和類似資源。

表 1-3. Horizon 連線伺服器資源

資源	位置	保護
LDAP 設定	不適用。	LDAP 資料會自動受到保護，做為角色型存取控制的一部分。
LDAP 備份檔案	`%ProgramData%\VMWare\VDM\backups`	受到存取控制保護。
`locked.properties` (安全閘道組態檔)	*`install_directory`*`\VMware\VMware View\Server\sslgateway\conf`	請確認此檔案受到保護而無法由非 Horizon 管理員的任何使用者進行存取。
`absg.properties` (Blast 安全閘道組態檔)	*`install_directory`*`\VMware\VMware View\Server\appblastgateway`	請確認此檔案受到保護而無法由非 Horizon 管理員的任何使用者進行存取。
記錄檔	請參閱 VMware Horizon 記錄檔	受到存取控制保護。
`web.xml` (Tomcat 組態檔)	*`install_directory`*`\VMware View\Server\broker\web apps\ROOT\Web INF`	受到存取控制保護。

VMware Horizon 記錄檔

VMware Horizon 所建立的記錄檔會記錄其元件的安裝與操作。

備註 VMware Horizon 記錄檔是由 VMware 支援所使用。VMware 建議您設定並使用事件資料庫來監視 VMware Horizon。如需詳細資訊，請參閱《Horizon 安裝》和《Horizon 管理》文件。

表 1-4. VMware Horizon 記錄檔

Horizon 元件	檔案路徑與其他資訊
所有元件 (安裝記錄)	*`%TEMP%`*`\vminst.log_`*`date_timestamp`* *`%TEMP%`*`\vmmsi.log_`*`date_timestamp`*
Horizon Agent	*`<Drive Letter>`*`:\ProgramData\VMware\VDM\logs` 若要存取儲存於 *`<Drive Letter>`*`:\ProgramData\VMware\VDM\logs` 中的 VMware Horizon 記錄檔，您必須使用較高的管理員權限才能從程式開啟記錄。在程式檔案上按一下滑鼠右鍵，然後選取**以系統管理員身分執行**。 如果已設定使用者資料磁碟 (UDD)，則 *<Drive Letter>* 可能會對應至 UDD。 PCoIP 記錄的名稱為 `pcoip_agent*.log` 和 `pcoip_server*.log`。

表 1-4. VMware Horizon 記錄檔 (續)

Horizon 元件	檔案路徑與其他資訊
遠端桌面平台功能	您可以在 Windows 代理程式和用戶端、Mac 用戶端和 Linux 用戶端上，在遠端桌面平台功能的資料收集工具 (DCT) 服務包中設定記錄層級和產生記錄檔。 Windows 代理程式：C:\Program Files\VMware\VMware View\Agent\DCT\support.bat Windows 用戶端：C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT\support.bat Mac 用戶端：/Applications/VMware Horizon Client.app/Contents/Library/dct/HorizonCollector.sh Linux 用戶端：/usr/bin/vmware-view-log-collector
已發佈的應用程式	Microsoft SQL Server、Oracle 資料庫伺服器或 PostgreSQL 資料庫伺服器上所設定的 Horizon 事件資料庫。 Windows 應用程式事件記錄。預設為停用狀態。
連線伺服器	<*磁碟機代號*>:\ProgramData\VMware\log\ConnectionServer。 **備註** 此檔案路徑為一個符號連結，會重新導向至記錄檔的實際位置，即<*磁碟機代號*>:\ProgramData\VMware\VDM\logs。 記錄目錄可在一般組態 ADMX 範本檔 (vdm_common.admx) 的記錄組態設定中設定。 PCoIP 安全閘道記錄會寫入到 PCoIP Secure Gateway 子目錄中名為 SecurityGateway_*.log 的檔案中。 Blast 安全閘道記錄會寫入到 Blast Secure Gateway 子目錄中名為 absg*.log 的檔案中。
Horizon 服務	Microsoft SQL Server、Oracle 資料庫伺服器或 PostgreSQL 資料庫伺服器上所設定的 Horizon 事件資料庫。 Windows 系統事件記錄。

VMware Horizon 安全性設定 2

VMware Horizon 包含您可以用來調整組態安全性的數個設定。您可以使用 Horizon Console，或使用 ADSI Edit 公用程式 (如果適用)，來存取這些設定。

備註 如需 Horizon Client 和 Horizon Agent 安全性設定的相關資訊，請參閱《Horizon Client 和 Agent 安全性》文件。

本章節討論下列主題：

Horizon Console 中的安全性相關全域設定

用戶端工作階段和連線的安全性相關全域設定可從 Horizon Console 中的**設定 > 全域設定 > 安全性設定**下方，或從**設定 > 全域設定 > 一般設定**下方存取。

表 2-1. 安全性相關的全域設定

設定	說明
變更資料復原密碼	從加密備份還原 Horizon LDAP 組態時，必須要有此密碼。 安裝連線伺服器時，您必須提供資料復原密碼。安裝完成後，您可以在 Horizon Console 中變更此密碼。 備份連線伺服器時，系統會將 Horizon LDAP 組態匯出為加密的 LDIF 資料。若要使用 `vdmimport` 公用程式還原加密的備份，您必須提供資料復原密碼。密碼必須包含 1 至 128 個字元。請遵循組織的最佳做法，產生安全密碼。
訊息安全模式	決定 JMS 訊息在 VMware Horizon 元件之間傳遞時所使用的安全性機制。 ■ 如果設為**已停用**，就會停用訊息安全性模式。 ■ 若設為**已啟用**，則會簽署和驗證舊版 JMS 訊息。VMware Horizon 元件會拒絕未簽署的訊息。此模式支援 TLS 和一般 JMS 連線的混合。 ■ 若設為**增強**，則 TLS 將用於所有 JMS 連線，以加密所有訊息。此外，還會啟用存取控制，以限制 VMware Horizon 元件可傳送和接收訊息的 JMS 主題。 ■ 如果設為**混合**，則會啟用訊息安全模式，但不會對 VMware Horizon 元件強制執行。 新安裝的預設設定為**增強**。如果從舊版升級，則會保留舊版中使用的設定。 **重要** VMware 強烈建議在升級所有連線伺服器執行個體和 VMware Horizon 桌面平台至此版本後，將訊息安全模式設定為**增強**。**增強**設定可提供許多重要的安全性改進和 MQ (訊息佇列) 更新。
增強安全性狀態 (唯讀)	當**訊息安全模式**由**已啟用**變更為**增強**時顯示的唯讀欄位。因為變更是分階段進行，此欄位會顯示在不同階段時的進度： ■ **等待訊息匯流排重新啟動**是第一階段。在您手動重新啟動網繭中的所有連線伺服器執行個體或網繭中所有連線伺服器主機上的 VMware Horizon 訊息匯流排元件服務之前，會一直顯示此狀態。 ■ **正在擱置增強**是下一個狀態。重新啟動所有 Horizon 訊息匯流排元件服務之後，系統會開始針對所有桌面平台將訊息安全模式變更為**增強**。 ■ **增強**是最後的狀態，表示所有元件目前正在使用**增強**訊息安全模式。
網路中斷後重新驗證安全通道連線	決定當 Horizon Client 使用安全通道連線至 VMware Horizon 桌面平台和應用程式時，在網路中斷後是否必須重新驗證使用者認證。 此設定可加強安全性。例如，如果筆記型電腦遭竊，並移至不同的網路上，使用者便無法自動取得 VMware Horizon 桌面平台和應用程式的存取權，因為網路連線暫時中斷。 此設定依預設為停用。
強制中斷使用者連線	自使用者登入 VMware Horizon 起經過指定的分鐘數後，將中斷與所有桌面平台及應用程式的連線。將會同時中斷所有桌面平台和應用程式的連線，無論使用者在何時開啟它們。 預設值為 600 分鐘。
支援應用程式的用戶端。如果使用者停止使用鍵盤與滑鼠，請中斷與應用程式的連線並捨棄 SSO 認證	在用戶端裝置上無鍵盤或滑鼠活動時保護應用程式工作階段。如果設定為 **...分鐘後**，則 VMware Horizon 將在無使用者活動進行後的指定分鐘數後中斷與所有應用程式的連線，並捨棄 SSO 認證。會中斷與桌面平台工作階段的連線。使用者必須再次登入才能與中斷連線的應用程式重新連線，或者啟動新的桌面平台或應用程式。 如果設定為**永不**，VMware Horizon 將永不會因為使用者無活動而中斷應用程式連線或捨棄 SSO 認證。 預設值為**永不**。

表 2-1. 安全性相關的全域設定 (續)

設定	說明
其他用戶端。 捨棄 SSO 認證	在特定時段後捨棄 SSO 認證。此設定適用於不支援應用程式遠端處理的用戶端。如果設定為 **...分鐘後**，使用者必須在其登入 VMware Horizon 起的指定分鐘數後再次登入才能連線到桌面平台，無論用戶端裝置上發生任何使用者活動。 預設值為 **15 分鐘後**。
View Administrator 工作階段逾時	決定 Horizon Console 工作階段要持續閒置多久的時間，工作階段才會逾時。 **重要** 若將 Horizon Console 工作階段逾時設為很大的分鐘數，會增加未經授權使用者 Horizon Console 的風險。若您允許讓工作階段持續閒置很長的時間，請小心。 依預設，Horizon Console 工作階段逾時為 30 分鐘。您可以將工作階段逾時設為 1 到 4320 分鐘。

備註 所有對 VMware Horizon 的 Horizon Client 連線和 Horizon Console 連線都需要 TLS。如果您的 VMware Horizon 部署使用負載平衡器或其他面向用戶端的中繼伺服器，您可以將 TLS 卸載到這些負載平衡器或中繼伺服器，然後在個別連線伺服器執行個體上設定非 TLS 連線。請參閱《Horizon 管理》文件中的〈將 TLS 連線卸載至中繼伺服器〉。

變更資料復原密碼

您在安裝連線伺服器時，必須提供資料復原密碼。安裝完成後，您可以在 Horizon Console 中變更此密碼。從備份復原 Horizon LDAP 組態時，必須要有此密碼。

備份連線伺服器時，系統會將 Horizon LDAP 組態匯出為加密的 LDIF 資料。若要還原加密的備份 VMware Horizon 組態，您必須提供資料復原密碼。

密碼必須包含 1 至 128 個字元。請遵循組織的最佳做法，產生安全密碼。

程序

1 在 Horizon Console 中，選取**設定 > 全域設定**。

2 在**安全性設定**索引標籤上，按一下**變更資料復原密碼**。

3 輸入兩次新密碼。

4 (選擇性) 輸入密碼提醒。

結果

備註 排程將備份的 VMware Horizon 組態資料時，也可變更資料復原密碼。請參閱《Horizon 管理》文件中的〈排程 Horizon 組態備份〉。

後續步驟

當您使用 `vdmimport` 公用程式還原備份 VMware Horizon 組態時，請提供新密碼。

Horizon 元件的訊息安全模式

您可以設定訊息安全模式，以指定 JMS 訊息在通過 VMware Horizon 元件時所使用的安全機制。

下表顯示可設定訊息安全模式的選項。若要設定選項，請在**全域設定**頁面上的**安全性設定**索引標籤上，從**訊息安全模式**清單中選取該選項。

表 2-2. 訊息安全模式選項

選項	說明
已停用	停用訊息安全模式。
混合	啟用訊息安全模式，但未強制實施。 您可以使用此模式來偵測 VMware Horizon 環境中較舊的元件。連線伺服器產生的記錄檔包含這些元件的參考。這不是建議使用的設定。請僅在探索需要升級的元件時才使用此設定。
已啟用	訊息安全模式會啟用，使用訊息簽署和加密的組合。如果簽章遺失或無效，或如果簽署簽章後修改了訊息，便會拒絕 JMS 訊息。 某些 JMS 訊息由於帶有如使用者認證的機密資訊，因此已加密。如果您使用**已啟用**設定，您也可以使用 IPSec 來加密連線伺服器執行個體之間，以及連線伺服器執行個體與 Unified Access Gateway 應用裝置之間的所有 JMS 訊息。
增強	所有 JMS 連線均會使用 SSL。此外也會啟用 JMS 存取控制，讓桌面平台和連線伺服器執行個體只能傳送和接收某些主題的 JMS 訊息。

當您第一次將 VMware Horizon 安裝在系統上時，訊息安全模式會設為**增強**。如果您從舊版升級 VMware Horizon，訊息安全模式會保持不變更其現有設定。

重要 如果您打算將已升級的 VMware Horizon 環境從**已啟用**變更為**增強**，您必須先升級所有連線伺服器執行個體和 VMware Horizon 桌面平台。在將設定變更為**增強**之後，新設定會分階段生效。

1. 您必須在網繭中的所有連線伺服器主機上手動重新啟動 VMware Horizon 訊息匯流排元件服務，或重新啟動連線伺服器執行個體。
2. 在服務重新啟動之後，連線伺服器執行個體會在所有桌面平台上重新設定訊息安全模式，將模式變更為**增強**。
3. 若要在 Horizon Console 中監控進度，請移至**設定 > 全域設定**。

   在**安全性設定**索引標籤上，當所有元件均已轉換為 [增強] 模式時，**增強安全性狀態**項目將會顯示**增強**。

   此外，您可以使用 `vdmutil` 命令列公用程式來監控進度。請參閱使用 vdmutil 公用程式設定 JMS 訊息安全模式。

如果您計劃將使用中 VMware Horizon 環境從**已停用**變更為**已啟用**，或從**已啟用**變更為**已停用**，則進行最後變更前，請先短暫變更為**混合**模式。例如，如果目前模式為**已停用**，請先變更為**混合**模式一天，再變更為**已啟用**。在**混合**模式中，系統會將簽署附加至訊息但不驗證，這可讓訊息的變更在整個環境傳播。

使用 vdmutil 公用程式設定 JMS 訊息安全模式

您可以使用 `vdmutil` 命令列介面設定和管理在 VMware Horizon 元件之間傳遞 JMS 訊息時所使用的安全機制。

公用程式的語法和位置

vdmutil 命令可以執行與舊版 VMware Horizon 隨附的 lmvutil 命令相同的作業。此外，vdmutil 命令具有選項，可決定使用的訊息安全模式以及監控將所有 VMware Horizon 元件變更為增強模式的進度。在 Windows 命令提示字元中使用 vdmutil 命令的下列格式。

```
vdmutil command_option [additional_option argument] ...
```

可使用的其他選項視命令選項而定。此主題著重於訊息安全模式的選項。如需與 Cloud Pod 架構相關的其他選項，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

依預設，vdmutil 命令執行檔的路徑是 C:\Program Files\VMware\VMware View\Server\tools\bin。若要避免在命令列上輸入路徑，請將路徑新增至您的 PATH 環境變數中。

驗證

您必須以具有管理員角色的使用者身分執行命令。您可以使用 Horizon Console，將管理員角色指派給使用者。請參閱《Horizon 管理》文件中的〈設定角色型委派管理〉。

vdmutil 命令包括指定要用於驗證的使用者名稱、網域和密碼的選項。

表 2-3. vdmutil 命令驗證選項

選項	說明
--authAs	Horizon 管理員使用者的名稱。請勿使用 *domain**username* 或使用者主體名稱 (UPN) 格式。
--authDomain	在 --authAs 選項中指定的 Horizon 管理員使用者的完整網域名稱。
--authPassword	在 --authAs 選項中所指定之 Horizon 管理員使用者的密碼。輸入 "*" 而非密碼會使 vdmutil 命令提示輸入密碼，並且不會在命令列上的命令歷程記錄中保留敏感的密碼。

您必須使用驗證選項搭配除 --help 和 --verbose 之外的所有 vdmutil 命令選項。

特定於 JMS 訊息安全模式的選項

下表僅列出與檢視、設定或監控 JMS 訊息安全模式相關的 vdmutil 命令列選項。如需可搭配特定選項使用的引數清單，請使用 --help 命令列選項。

如果作業成功，vdmutil 命令將傳回 0；如果作業失敗，該命令將傳回失敗特定的非零代碼。vdmutil 命令會將錯誤訊息寫為標準錯誤。如果作業產生輸出，或使用 --verbose 選項啟用詳細記錄，vdmutil 命令會用美式英文將輸出寫為標準輸出。

表 2-4. vdmutil 命令選項

選項	說明
--activatePendingConnectionServerCertificates	針對本機網繭中的連線伺服器執行個體啟用擱置安全憑證。
--countPendingMsgSecStatus	計算導致無法轉換為增強模式或從增強模式轉換的機器數目。
--createPendingConnectionServerCertificates	針對本機網繭中的連線伺服器執行個體建立新的擱置安全憑證。
--getMsgSecLevel	取得本機網繭的增強訊息安全狀態。此狀態與針對 VMware Horizon 環境中的所有元件將 JMS 訊息安全模式從**已啟用**變更為**增強**的程序有關。

表 2-4. vdmutil 命令選項 (續)

選項	說明
`--getMsgSecMode`	取得本機網繭的訊息安全模式。
`--help`	列出 `vdmutil` 命令選項。您也可以針對特定命令使用 `--help`，例如 `--setMsgSecMode --help`。
`--listMsgBusSecStatus`	列出本機網繭中所有連線伺服器的訊息匯流排安全狀態。
`--listPendingMsgSecStatus`	列出導致無法轉換為增強模式或從增強模式轉換的機器。預設限制為 25 個項目。
`--setMsgSecMode`	設定本機網繭的訊息安全模式。
`--verbose`	啟用詳細記錄。您可以將此選項新增至任何其他選項，以取得詳細的命令輸出。`vdmutil` 命令會寫入到標準輸出。

Horizon Console 中的安全性相關伺服器設定

與安全性相關的伺服器設定可從 Horizon Console 中的**設定 > 伺服器**下方存取。

表 2-5. 安全性相關的伺服器設定

設定	說明
使用 PCoIP 安全閘道與機器進行 PCoIP 連線	決定當使用者使用 PCoIP 顯示通訊協定連線至 VMware Horizon 桌面平台和應用程式時，Horizon Client 是否要與連線伺服器主機建立進一步的安全連線。 如果停用此設定，就會直接在用戶端系統與 VMware Horizon 桌面平台或遠端桌面服務 (RDS) 主機之間建立桌面平台或應用程式工作階段，略過連線伺服器主機。 此設定依預設為停用。
使用安全通道連線到機器	決定當使用者連線至 VMware Horizon 桌面平台或應用程式時，Horizon Client 是否要與連線伺服器主機建立進一步的 HTTPS 連線。 如果停用此設定，就會直接在用戶端系統與 VMware Horizon 桌面平台或遠端桌面服務 (RDS) 主機之間建立桌面平台或應用程式工作階段，略過連線伺服器主機。 此設定依預設為啟用。
使用 Blast 安全閘道，以透過 Blast 連線至機器	決定使用網頁瀏覽器或 Blast Extreme 顯示通訊協定存取桌面平台的用戶端，是否使用 Blast 安全閘道建立與連線伺服器的安全通道。 如果未啟用，則使用 Blast Extreme 工作階段和網頁瀏覽器的用戶端會略過連線伺服器，直接與 VMware Horizon 桌面平台建立連線。 此設定依預設為停用。

如需關於這些設定及其安全性含意的詳細資訊，請參閱《Horizon 管理》文件。

Horizon LDAP 中的安全性相關設定

安全性相關設定提供於 Horizon LDAP 的 `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` 物件路徑下方。您可以使用 ADSI Edit 公用程式，在連線伺服器執行個體上變更這些設定的值。變更會自動散佈到群組中其他所有的連線伺服器執行個體。

表 2-6. Horizon LDAP 中的安全性相關設定

名稱/值對	說明
cs-allowunencryptedstartsession	屬性為 pae-NameValuePair。 此屬性會控制啟動遠端使用者工作階段時，在連線伺服器執行個體與桌面平台之間是否需要安全通道。 在桌面平台電腦上安裝 Horizon Agent 時，此屬性沒有作用，且一律需要安全通道。 在所有情況下，使用者認證與授權票證都是透過一個靜態金鑰保護。安全通道使用動態金鑰提供進一步的保密能力。 如果設為 **0**，當無法建立安全通道時，遠端使用者工作階段將無法啟動。如果所有桌面平台都位於受信任的網域，或所有桌面平台都已安裝 Horizon Agent，則此設定相當合適。 如果設為 **1**，即使無法建立安全通道，還是可啟動遠端使用者工作階段。如果某些桌面平台已經安裝舊版 Horizon Agent，且未處於受信任的網域，則此設定相當合適。 預設設定為 **1**。
keysize	屬性為 pae-MSGSecOptions。 將訊息安全性模式設定為**增強**時，將使用 TLS 而非使用每則訊息加密來確保 JMS 連線的安全。在增強訊息安全模式中，驗證僅適用於一個訊息類型。針對增強訊息模式，VMware 建議將金鑰大小增加為 2048 個位元。如果您未使用增強訊息安全模式，VMware 建議不要變更 512 個位元的預設值，因為增加金鑰大小會影響效能和擴充性。如果您希望所有金鑰都是 2048 位元，則必須在安裝第一個連線伺服器執行個體之後，以及在建立其他伺服器和桌面平台之前，立即變更 DSA 金鑰大小。

使用者驗證的安全性相關伺服器設定

使用者驗證的安全性相關伺服器設定可從 Horizon Console 中的**設定 > 全域設定 > 全域設定**或**設定 > 伺服器**下方存取。這些安全性設定將決定 Horizon Client 可透過何種方式登入連線伺服器。

- 針對使用者在 Horizon Client 的**選項**功能表中選取**以目前使用者身分登入**時所傳遞的使用者身分識別和認證資訊，若要允許連線伺服器執行個體接受這些資訊，請為連線伺服器執行個體啟用**接受以目前使用者身分登入**設定。此設定適用於 Windows 版 Horizon Client。如需詳細資訊，請參閱《Horizon 管理》文件。
- 若要在 Horizon Client 中隱藏伺服器 URL，請啟用**在用戶端使用者介面中隱藏伺服器資訊**全域設定。如需詳細資訊，請參閱《Horizon 管理》文件中的〈用戶端工作階段的全域設定〉。
- 若要在 Horizon Client 中隱藏**網域**下拉式功能表，請啟用**在用戶端使用者介面中隱藏網域清單**全域設定。如需詳細資訊，請參閱《Horizon 管理》文件中的〈用戶端工作階段的全域設定〉。
- 若要將網域清單傳送至 Horizon Client，請啟用 Horizon Console 中的**傳送網域清單**全域設定。如需詳細資訊，請參閱《Horizon 管理》文件中的〈用戶端工作階段的全域設定〉。

備註 並非所有設定都適用於各種 Horizon Client。若要查看特定 Horizon Client 的使用者驗證設定，請參閱 Horizon Client 說明文件，網址為 https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。

提供伺服器詳細資料

若要讓「以目前使用者身分登入」功能順利運作，VMware Horizon 必須在進行使用者驗證之前，將連線伺服器的伺服器主體名稱 (Windows 身分識別) 提供給連線端用戶端。

依預設會隱藏這項資訊，但可藉由在 Horizon Console 中啟用**接受以目前使用者身分登入**設定加以提供。您可以就個別的伺服器選擇此設定。如果指定的伺服器未啟用此設定，則從 Windows 版 Horizon Client 登入伺服器的使用者將必須輸入認證，即使他們已啟用**以目前使用者身分登入**設定，仍是如此。決定是否為伺服器啟用**接受以目前使用者身分登入**設定時，請考量連線端用戶端是使用內部網路 (因而受到您某種程度的控制) 還是外部網路 (因此未受控制)。

在用戶端使用者介面中隱藏伺服器資訊設定只會影響用戶端的使用者介面，而不會變更伺服器提供給用戶端的資訊內容。此設定依預設為停用。

提供網域資訊

可用的使用者網域清單可在進行使用者驗證之前提供給連線端用戶端，且若提供，使用者將可在下拉式功能表中檢視此清單。

依預設會隱藏這項資訊，但可藉由在 Horizon Console 中啟用**傳送網域清單**全域設定加以提供。

如果用戶端透過設定為執行雙因素預先驗證的 Unified Access Gateway 應用裝置連線至環境，則可以將網域清單提供給用戶端，沒有安全顧慮。在預先驗證成功之前，網域清單不會傳送至用戶端。如需關於為 Unified Access Gateway 應用裝置設定雙因素驗證的詳細資訊，請參閱 Unified Access Gateway 說明文件，網址為 https://docs.vmware.com/tw/Unified-Access-Gateway/index.html。

在用戶端使用者介面中隱藏網域清單設定只會影響用戶端的使用者介面，而不會變更伺服器提供給用戶端的資訊內容。此設定依預設為停用。

當使用者登入伺服器時，若**傳送網域清單**已停用且**在用戶端使用者介面中隱藏網域清單**已啟用，則 Horizon Client 中的**網域**下拉式功能表會顯示 `*DefaultDomain*`，且使用者可能需要在**使用者名稱**文字方塊中輸入網域，例如 username@domain。使用者若未手動輸入網域，且系統中已設定了多個網域，其可能就無法登入伺服器。

下表顯示**傳送網域清單**和**在用戶端使用者介面中隱藏網域清單**全域設定如何決定使用者可用來登入伺服器的方式。

傳送網域清單設定	在用戶端使用者介面中隱藏網域清單設定	使用者登入方式
已停用 (預設值)	已啟用	**網域**下拉式功能表已隱藏。使用者必須在**使用者名稱**文字方塊中輸入下列其中一個值。 ■ 使用者名稱 (不允許使用多個網域) ■ ***domain**username*** ■ ***username*@*domain.com***
已停用 (預設值)	已停用	如果在用戶端上設定了預設網域，則**網域**下拉式功能表中會出現該預設網域。如果用戶端無法識別預設網域，則**網域**下拉式功能表中會出現 `*DefaultDomain*`。使用者必須在**使用者名稱**文字方塊中輸入下列其中一個值。 ■ 使用者名稱 (不允許使用多個網域) ■ ***domain**username*** ■ ***username*@*domain.com***
已啟用	已啟用	**網域**下拉式功能表已隱藏。使用者必須在**使用者名稱**文字方塊中輸入下列其中一個值。 ■ 使用者名稱 (不允許使用多個網域) ■ ***domain**username*** ■ ***username*@*domain.com***
已啟用	已停用	使用者可以在**使用者名稱**文字方塊中輸入使用者名稱，然後從**網域**下拉式功能表中選取網域。或者，使用者也可以在**使用者名稱**文字方塊中輸入下列其中一個值。 ■ ***domain**username*** ■ ***username*@*domain.com***

連接埠和服務

3

必須開啟某些 UDP 和 TCP 連接埠，VMware Horizon 元件才能夠彼此通訊。瞭解每個類型的 VMware Horizon 伺服器上執行的 Windows 服務，有助於找出不屬於伺服器的服務。

本章節討論下列主題：

- VMware Horizon TCP 和 UDP 連接埠
- VMware Horizon TrueSSO 連接埠
- 連線伺服器主機上的服務

VMware Horizon TCP 和 UDP 連接埠

VMware Horizon 會使用 TCP 和 UDP 連接埠，在其元件之間進行網路存取。

在安裝期間，VMware Horizon 可以選擇性地設定 Windows 防火牆規則，以開放依預設使用的連接埠。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 安裝》文件中的〈取代 VMware Horizon 服務的預設連接埠〉。

如需 VMware Horizon 用於與 TrueSSO 解決方案相關聯憑證登入的連接埠清單，請參閱 VMware Horizon TrueSSO 連接埠。

表 3-1. VMware Horizon 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
連線伺服器或 Unified Access Gateway 應用裝置	55000	Horizon Agent	4172	UDP	PCoIP (非 SALSA20) (如果使用 PCoIP 安全閘道)。
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。
連線伺服器或 Unified Access Gateway 應用裝置	*	Horizon Agent	3389	TCP	Microsoft RDP 到 VMware Horizon 遠端桌面平台的流量 (如果使用通道連線)。

表 3-1. VMware Horizon 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
連線伺服器或 Unified Access Gateway 應用裝置	*	Horizon Agent	9427	TCP	Windows 多媒體重新導向、用戶端磁碟機重新導向、Microsoft Teams 最佳化、HTML5 多媒體重新導向、VMware 印表機重新導向和 USB 重新導向 (使用通道連線時)。
連線伺服器或 Unified Access Gateway 應用裝置	*	Horizon Agent	32111	TCP	USB 重新導向和時區同步化 (如果使用通道連線)。
連線伺服器或 Unified Access Gateway 應用裝置	*	Horizon Agent	4172	TCP	PCoIP (如果使用 PCoIP 安全閘道)。
連線伺服器或 Unified Access Gateway 應用裝置	*	Horizon Agent	22443	TCP	VMware Blast Extreme (如果使用 Blast 安全閘道)。
連線伺服器或 Unified Access Gateway 應用裝置	*	Horizon Agent	22443	TCP	HTML Access (如果使用 Blast 安全閘道)。
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。
Horizon Agent	4172	連線伺服器或 Unified Access Gateway 應用裝置	55000	UDP	PCoIP (非 SALSA20) (如果使用 PCoIP 安全閘道)。
Horizon Agent	4172	Unified Access Gateway 應用裝置	*	UDP	PCoIP。VMware Horizon 桌面平台和應用程式會從 UDP 連接埠 4172 將 PCoIP 資料回傳至 Unified Access Gateway 應用裝置。 目的地 UDP 連接埠將會是所接收 UDP 封包中的來源連接埠，由於這是回覆資料，所以通常不需要為此新增明確防火牆規則。
Horizon Agent (未受管理的)	*	連線伺服器執行個體	389	TCP	在未受管理的代理程式安裝期間存取 AD LDS。 **備註** 對於此連接埠的其他使用方式，請參閱此表格下方的備註。
Horizon Client	*	連線伺服器或 Unified Access Gateway 應用裝置	80	TCP	用戶端連線依預設啟用 TLS (HTTPS 存取)，但在某些情況下可以使用連接埠 80 (HTTP 存取)。請參閱 VMware Horizon 中的 HTTP 重新導向。
Horizon Client	*	連線伺服器或 Unified Access Gateway 應用裝置	443	TCP	記錄至 VMware Horizon 時為 HTTPS。(使用通道連線時，此連接埠也用於通道處理)。

表 3-1. VMware Horizon 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	*	連線伺服器或 Unified Access Gateway 應用裝置	4172	TCP 與 UDP	PCoIP (如果使用 PCoIP 安全閘道)。
Horizon Client	*	Horizon Agent	3389	TCP	Microsoft RDP 到 VMware Horizon 桌面平台的流量 (如果使用直接連線而非通道連線)。
Horizon Client	*	Horizon Agent	9427	TCP	Windows 多媒體重新導向、用戶端磁碟機重新導向、Microsoft Teams 最佳化、HTML5 多媒體重新導向、VMware 印表機重新導向和 USB 重新導向 (如果使用直接連線而非通道連線)。
Horizon Client	*	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	*	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
Horizon Client	*	連線伺服器或 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。
網頁瀏覽器	*	Unified Access Gateway 應用裝置	8443	TCP	HTML Access。
連線伺服器	*	連線伺服器	48080	TCP	供在連線伺服器元件之間進行內部通訊使用。
連線伺服器	*	vCenter Server	80	TCP	SOAP 訊息 (如果對 vCenter Server 的存取停用 TLS)。
連線伺服器	*	vCenter Server	443	TCP	SOAP 訊息 (如果對 vCenter Server 的存取啟用 TLS)。
連線伺服器	*	連線伺服器	4100	TCP	JMS 路由器間的流量。
連線伺服器	*	連線伺服器	4101	TCP	JMS TLS 路由器間的流量。
連線伺服器	*	連線伺服器	8472	TCP	供在 Cloud Pod 架構中進行網繭間通訊使用。
連線伺服器	*	連線伺服器	22389	TCP	供在 Cloud Pod 架構中進行全域 LDAP 複寫使用。
連線伺服器	*	連線伺服器	22636	TCP	供在 Cloud Pod 架構中進行安全的全域 LDAP 複寫使用。
連線伺服器	*	連線伺服器	32111	TCP	金鑰共用流量。
連線伺服器	*	憑證授權機構	*	HTTP，HTTPS	CRL 或 OCSP 查詢

表 3-1. VMware Horizon 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
Unified Access Gateway 應用裝置	*	連線伺服器或負載平衡器	443	TCP	HTTPS 存取。Unified Access Gateway 應用裝置會在 TCP 連接埠 443 進行連線，以與連線伺服器執行個體或位在多個連線伺服器執行個體前方的負載平衡器進行通訊。
Horizon Help Desk Tool	*	Horizon Agent	3389	TCP	Microsoft RDP 到 Horizon 桌面平台進行遠端協助的流量。

備註 用戶端用於 PCoIP 的 UDP 連接埠號碼可能會變更。如果連接埠 50002 正在使用中，用戶端會選擇 50003。如果連接埠 50003 正在使用中，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。

備註 Microsoft Windows Server 需要在 VMware Horizon 環境中的所有連線伺服器之間開放某個動態範圍的連接埠。Microsoft Windows 需要這些連接埠來進行遠端程序呼叫 (RPC) 和 Active Directory 複寫的一般作業。如需動態範圍連接埠的詳細資訊，請參閱 Microsoft Windows Server 說明文件。

備註 在連線伺服器執行個體上，連接埠 389 可供不常見且特定的連線存取。如表中所示，安裝未受管理的代理程式時、使用 LDAP 編輯器直接編輯資料庫時，以及使用 repadmin 之類工具發出命令時會存取它。當 AD LDS 已安裝時，即會為這些用途建立防火牆規則，但若不需要存取該連接埠，則可停用它。

備註 依預設，VMware Blast Extreme Adaptive Transport 會從暫時連接埠範圍 49152-65535 開始保留一些連接埠。請參閱知識庫文章 52558。

VMware Horizon 中的 HTTP 重新導向

透過 HTTP 的連線嘗試會以無訊息的方式重新導向至 HTTPS，但連線至 Horizon Console 的嘗試除外。新版 Horizon Client 不需要 HTTP 重新導向，因為它們預設使用 HTTPS，但當使用者使用網頁瀏覽器來進行諸如下載 Horizon Client 的動作時，這就很有用。

HTTP 重新導向的問題在於，它是非安全的通訊協定。如果使用者沒有養成在位址列中輸入 **`https://`** 的習慣，即使是在正常顯示所需的網頁時，攻擊者仍可侵入網頁瀏覽器、安裝惡意程式碼或竊取認證。

備註 只有在您設定外部防火牆允許輸入流量到 TCP 連接埠 80 的情況下，外部連線才會進行 HTTP 重新導向。

透過 HTTP 連線至 Horizon Console 的嘗試不會重新導向。相反地，系統會傳回錯誤訊息，表示您必須使用 HTTPS。

若要防止所有 HTTP 連線嘗試重新導向，請參閱《Horizon 安裝》文件中的〈阻止用戶端連線的 HTTP 重新導向至連線伺服器〉。

如果您將 TLS 用戶端連線卸載至中繼裝置，則也可連線至連線伺服器執行個體的連接埠 80。請參閱《Horizon 管理》文件中的〈將 TLS 連線卸載至中繼伺服器〉。

若要在變更 TLS 連接埠號碼時允許 HTTP 重新導向，請參閱《Horizon 安裝》文件中的〈變更連接埠號碼以讓 HTTP 重新導向至連線伺服器〉。

VMware Horizon TrueSSO 連接埠

VMware Horizon 會使用 TrueSSO 連接埠作為通訊路徑 (連接埠和通訊協定)，而安全性控制項會用於讓憑證在 Horizon Connection Server 與虛擬桌面平台或已發佈的應用程式之間傳遞，以取得與 TrueSSO 解決方案相關聯的憑證登入。

表 3-2. VMware Horizon 所使用的 TrueSSO 連接埠

來源	目標	連接埠	通訊協定	說明
Horizon Client	VMware Identity Manager 應用裝置	TCP 443	HTTPS	從產生 SAML 判斷提示和構件的 VMware Identity Manager 應用裝置啟動 VMware Horizon。
Horizon Client	Horizon Connection Server	TCP 443	HTTPS	啟動 Horizon Client。
Horizon Connection Server	VMware Identity Manager 應用裝置	TCP 443	HTTPS	連線伺服器會對 VMware Identity Manager 執行 SAML 解析。VMware Identity Manager 會驗證構件並傳回判斷提示。
Horizon Connection Server	Horizon 註冊伺服器	TCP 32111		使用註冊伺服器。
註冊伺服器	ADCS			註冊伺服器會從 Microsoft 憑證授權單位 (CA) 要求憑證，以產生一個暫時性且存留期短的憑證。 在與 CA 的初始通訊中，註冊服務會使用 TCP 135 RPC，以及從 1024 - 5000 和 49152 - 65535 的隨機連接埠。請參閱 https://support.microsoft.com/en-us/help/832017#method4 中的憑證服務。 註冊伺服器也會與網域控制站通訊，使用所有相關的連接埠來探索 DC 並繫結至及查詢 Active Directory。 請參閱 https://support.microsoft.com/en-us/help/832017#method1 與 https://support.microsoft.com/en-us/help/832017#method12。
Horizon Agent	Horizon Connection Server	TCP 4002	透過 TLS 的 JMS	Horizon Agent 會要求及接收用於登入的憑證。
虛擬桌面平台或已發佈的應用程式	AD DC			Windows 會驗證 Active Directory 憑證的真確性。請參閱 Microsoft 說明文件以取得連接埠和通訊協定的清單，因為可能需要多個連接埠。
Horizon Client	Horizon Agent (通訊協定工作階段)	TCP/UDP 22443	Blast	登入 Windows 桌面平台或應用程式，而遠端工作階段會在 Horizon Client 上啟動。
Horizon Client	Horizon Agent (通訊協定工作階段)	UDP 4172	PCoIP	登入 Windows 桌面平台或應用程式，而遠端工作階段會在 Horizon Client 上啟動。

連線伺服器主機上的服務

VMware Horizon 的作業取決於在連線伺服器主機上執行的數個服務。

表 3-3. Horizon 連線伺服器主機服務

服務名稱	啟動類型	說明
VMware Horizon Blast 安全閘道	自動	提供安全的 HTML Access 和 Blast Extreme 服務。如果用戶端是透過 Blast 安全閘道連線至連線伺服器，則此服務必須在執行狀態下。
VMware Horizon 連線伺服器	自動	提供連線 Broker 服務。此服務必須永遠處於執行狀態。當您啟動或停止這項服務時，該服務也會啟動或停止 Framework、訊息匯流排、安全閘道和 Web 服務。此服務不會啟動或停止 VMwareVDMDS 服務或 VMware Horizon 指令碼主機服務。
VMware Horizon 架構元件	手動	提供事件記錄、安全和 COM+ 架構服務。此服務必須永遠處於執行狀態。
VMware Horizon 訊息匯流排元件	手動	在 VMware Horizon 元件之間提供通訊服務。此服務必須永遠處於執行狀態。
VMware Horizon PCoIP 安全閘道	手動	提供 PCoIP 安全閘道服務。如果用戶端是透過 PCoIP 安全閘道連線至連線伺服器，則此服務必須在執行狀態下。
VMware Horizon 指令碼主機	已停用	針對在您刪除虛擬機器時執行的第三方指令碼提供支援。此服務依預設為停用。若您要執行指令碼，則須啟用此服務。
VMware Horizon 安全閘道元件	手動	提供一般閘道服務。此服務必須永遠處於執行狀態。
VMware Horizon Web 元件	手動	提供 Web 服務。此服務必須永遠處於執行狀態。
VMwareVDMDS	自動	提供 Horizon LDAP 服務。此服務必須永遠處於執行狀態。在 VMware Horizon 升級期間，此服務可確保現有資料能正確移轉。

憑證指紋驗證和自動憑證產生

4

VMware Horizon 會使用許多公開金鑰憑證。這些憑證中的一部分是使用涉及受信任第三方的機制進行驗證，但這種機制不一定能提供必要的精確度、速度或彈性。VMware Horizon 會使用一個替代機制，這在多種情況稱為指紋驗證。

指紋驗證不會驗證個別憑證欄位或建立信任的鏈結，而是會將憑證視為 Token，將整個位元組序列 (或其密碼編譯雜湊) 與預先共用的位元組序列或雜湊進行比對。一般來說，這是透過個別受信任通道的即時共用，且表示服務呈現的憑證可經過驗證而成為預期的確切憑證。

Horizon 訊息匯流排會在連線伺服器之間進行通訊，也會在 Horizon Agent 與連線伺服器執行個體之間進行通訊。設定通道會使用每一訊息簽章與裝載加密，而主要通道則是使用 TLS 與相互驗證加以保護。使用 TLS 來保護通道時，用戶端與伺服器的驗證會涉及 TLS 憑證和憑證指紋驗證。針對 Horizon 訊息匯流排通道，伺服器一律為訊息路由器。用戶端也可能成為訊息路由器，因為這是訊息路由器共用訊息的方式。不過，用戶端是連線伺服器執行個體或 Horizon Agent。

系統會以不同的方式提供初始憑證指紋及設定訊息簽署金鑰。在連線伺服器上，憑證指紋會儲存在 LDAP 中，以便 Horizon Agent 可以與任何連線伺服器通訊，且所有連線伺服器之間彼此可以通訊。Horizon 訊息匯流排伺服器和用戶端憑證會自動產生並定期交換，且會自動刪除過時的憑證，所以不需要手動介入或確實可行。主要通道每一端的憑證會根據排程自動產生，並透過設定通道進行交換。您無法自行取代這些憑證。系統會自動移除已到期的憑證。

類似機制適用於網繭間的通訊。

其他通訊通道可以使用客戶提供的憑證，但預設為自動產生憑證。其中包括安全通道、註冊伺服器和 vCenter 連線，以及顯示通訊協定和輔助通道。如需關於如何取代這些憑證的詳細資訊，請參閱《Horizon 管理》文件。預設憑證會在安裝時產生，且除了 PCoIP 之外不會自動更新。如果 PKI 產生的憑證無法供 PCoIP 使用，則會在每次啟動時自動產生新憑證。即便已使用 PKI 產生的憑證，這些通道多數仍會使用指紋驗證。

vCenter 憑證的驗證會使用技術的組合。連線伺服器執行個體一律會嘗試驗證所收到使用 PKI 的憑證。如果此驗證失敗，則在檢閱憑證後，VMware Horizon 管理員可允許連線繼續，且連線伺服器會記住憑證的密碼編譯雜湊，以便用於後續使用指紋驗證的自動接受。

在連線伺服器執行個體上設定安全性通訊協定和加密套件

5

您可以設定連線伺服器接受的安全性通訊協定及加密套件。您可以定義適用於複寫的群組中的所有連線伺服器執行個體的全域接受原則，或者您可以定義個別連線伺服器執行個體的接受原則。

您也可以設定連線至 vCenter Server 時，連線伺服器執行個體建議的安全性通訊協定及加密套件。您可以定義適用於複寫的群組中的所有連線伺服器執行個體的全域建議原則。您無法定義要退出全域建議原則的個別執行個體。

備註 連線伺服器的安全性設定不適用於 Blast 安全閘道 (BSG)。您必須個別為 BSG 設定安全性。請參閱 第 6 章 針對 Blast 安全閘道設定安全性通訊協定和加密套件。

Oracle 的 Unlimited Strength Jurisdiction Policy 檔案已納為標準，依預設可允許 256 位元的金鑰。

本章節討論下列主題：

安全性通訊協定及加密套件的預設全域原則

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。

表 5-1. 預設全域接受原則

預設安全性通訊協定	預設加密套件
■ TLS 1.2	■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

表 5-2. 預設全域建議原則

預設安全性通訊協定	預設加密套件
■ TLS 1.2	■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

在 FIPS 模式中，僅會啟用 GCM 加密套件。

設定全域接受與建議原則

全域接受與建議原則定義於 Horizon LDAP 屬性中。這些原則適用於所有的連線伺服器執行個體。若要變更全域原則，您可以在任何連線伺服器執行個體上編輯 Horizon LDAP。

每個原則在下列的 Horizon LDAP 位置中，都是單一值屬性：
`cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int`

Horizon LDAP 中定義的全域接受與建議原則

您可以編輯定義全域接受與建議原則的 Horizon LDAP 屬性。

全域接受原則

下列屬性會列出安全性通訊協定。您必須將最新的通訊協定放在最前面，藉以排序清單：

```
pae-ServerSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

下列屬性會列出加密套件。此範例會顯示縮寫的清單：

```
pae-ServerSSLCipherSuites =
\LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

下列屬性會控制加密套件的優先順序。通常，伺服器的加密套件順序不重要，且系統會使用用戶端的順序。若要改為使用伺服器的加密套件順序，請設定下列屬性：

```
pae-ServerSSLHonorClientOrder = 0
```

全域建議原則

下列屬性會列出安全性通訊協定。您必須將最新的通訊協定放在最前面，藉以排序清單：

```
pae-ClientSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

下列屬性會列出加密套件。此清單應該依喜好排序。將最喜歡的加密套件放在最前面，第二喜歡的套件放在下一個，以此類推。此範例會顯示縮寫的清單：

```
pae-ClientSSLCipherSuites =
\LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

變更全域接受與建議原則

若要變更安全性通訊協定及加密套件的全域接受與建議原則，請使用 ADSI Edit 公用程式編輯 Horizon LDAP 屬性。

必要條件

- 請熟悉定義接受與建議原則的 Horizon LDAP 屬性。請參閱 Horizon LDAP 中定義的全域接受與建議原則。
- 如需如何在 Windows Server 作業系統版本使用 ADSI Edit 公用程式的資訊，請參閱 Microsoft TechNet 網站。

程序

1. 在連線伺服器電腦上啟動 ADSI Edit 公用程式。
2. 在主控台樹狀結構中，選取**連線至**。
3. 在**選取或輸入辨別名稱或命名內容**文字方塊中，輸入辨別名稱 **DC=vdi, DC=vmware, DC=int**。
4. 在**選取或輸入網域或伺服器**文字方塊中，選取或輸入 **localhost:389**，或連線伺服器電腦的完整網域名稱 (FQDN) 後面再加上連接埠 389。

   例如：**localhost:389** 或 **mycomputer.mydomain.com:389**
5. 依序展開 ADSI Edit 樹狀結構和 **OU=Properties**，選取 **OU=Global**，然後選取右窗格中的 **CN=Common**。
6. 在 **CN=Common, OU=Global, OU=Properties** 物件上，選取您要變更的每個屬性，然後輸入安全性通訊協定或加密套件的新清單。
7. 如果您已修改 `pae-ServerSSLSecureProtocols`，請在每個連線伺服器執行個體上，重新啟動 Windows 服務 VMware Horizon 安全閘道元件。

   修改 `pae-ClientSSLSecureProtocols` 之後，您不需要重新啟動任何服務。

設定個別伺服器上的接受原則

若要在個別的連線伺服器執行個體上指定本機接受原則，您必須將內容新增至 `locked.properties` 檔案。如果 `locked.properties` 檔案不存在於伺服器上，您必須建立該檔案。

您要為想要設定的每個安全性通訊協定，新增 `secureProtocols.`*`n`* 項目。請使用下列語法：`secureProtocols.`*`n`*`=`*安全性通訊協定*。

您要為想要設定的每個加密套件，新增 `enabledCipherSuite.`*`n`* 項目。請使用下列語法：`enabledCipherSuite.`*`n`*`=`*加密套件*。

變數 *n* 是您循序 (1、2、3) 新增到每個項目類型的整數。

您需要新增 honorClientOrder 項目以控制加密套件的優先順序。通常，伺服器的加密套件順序不重要，且系統會使用用戶端的順序。若要改為使用伺服器的加密套件順序，請使用下列語法：

```
honorClientOrder=false
```

請確認 locked.properties 檔案中的項目擁有正確的語法，且加密套件和安全性通訊協定的名稱拼寫正確。檔案中的任何錯誤都可能會造成用戶端與伺服器之間的交涉失敗。

程序

1 在連線伺服器電腦上的 TLS/SSL 閘道組態資料夾中，建立或編輯 locked.properties 檔案。

例如：*install_directory*\VMware\VMware View\Server\sslgateway\conf\

2 新增 secureProtocols.*n* 和 enabledCipherSuite.*n* 項目，包括相關聯的安全性通訊協定和加密套件。

3 儲存 locked.properties 檔案。

4 重新啟動 VMware Horizon Connection Server 服務，讓變更生效。

範例： 個別伺服器上的預設接受原則

下列範例說明 locked.properties 檔案中，指定預設原則所需的項目：

```
# The following list should be ordered with the latest protocol first:

secureProtocols.1=TLSv1.2

# This setting must be the latest protocol given in the list above:

preferredSecureProtocol=TLSv1.2

# The order of the following list is unimportant unless honorClientOrder is false:

enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
enabledCipherSuite.2=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.3=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
enabledCipherSuite.4=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

# Use the client's ordering of cipher suites (ignores the ordering given above):

honorClientOrder=true
```

備註 在 FIPS 模式中，僅會啟用 GCM 加密套件。

在遠端桌面平台上設定建議原則

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

必要條件

若要避免連線失敗，請將連線伺服器設定為接受相同的原則。

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
   ```

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。

   此清單必須依照喜好順序列出，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
   ```

VMware Horizon 中已停用的舊版通訊協定和加密

依預設，在 VMware Horizon 中會停用某些被認為不再安全的舊版通訊協定和加密。如有必要，您可以手動加以啟用。

DHE 加密套件

如需詳細資訊，請參閱 http://kb.vmware.com/kb/2121183。與 DSA 憑證相容的加密套件會使用 Diffie-Hellman 暫時金鑰，且自 Horizon 6 (6.2 版) 起，這些套件已不再預設為啟用。

對於連線伺服器執行個體和 VMware Horizon 桌面平台，您可以藉由編輯 Horizon LDAP 資料庫、`locked.properties` 檔案或登錄來啟用這些加密套件，如本指南中所述。請參閱變更全域接受與建議原則、設定個別伺服器上的接受原則與在遠端桌面平台上設定建議原則。您可以依照下列順序，定義包含一或多個下列套件的加密套件清單：

- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (僅限 TLS 1.2，不是 FIPS)
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (僅限 TLS 1.2，不是 FIPS)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (僅限 TLS 1.2)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (僅限 TLS 1.2)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA

對於 View Agent Direct-Connection (VADC) 機器，您可以在執行《Horizon 安裝》文件中的〈針對 Horizon Agent 機器停用 SSL/TLS 中的弱加密〉程序時，將下列項目新增至加密清單，以啟用 DHE 加密套件。

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

備註 您無法啟用 ECDSA 憑證的支援。這些憑證從未受到支援。

SSLv3

在 VMware Horizon 中，已移除 SSL 3.0 版。

RC4

對於連線伺服器執行個體和 VMware Horizon 桌面平台，您可以藉由編輯組態檔 `C:\Program Files\VMware\VMware View\Server\jre\conf\security\java.security`，在連線伺服器或 Horizon Agent 機器上啟用 RC4。檔案的結尾處是名為 `jdk.tls.legacyAlgorithms` 的多行項目。請從這個項目中移除 `RC4_128` 和其後的逗號，並視情況重新啟動連線伺服器或 Horizon Agent 機器。

對於 View Agent Direct-Connection (VADC) 機器，您可以在執行《Horizon 安裝》文件中的〈針對 Horizon Agent 機器停用 SSL/TLS 中的弱加密〉程序時，將下列項目新增至加密清單以啟用 RC4。

```
TLS_RSA_WITH_RC4_128_SHA
```

TLS 1.0

在 VMware Horizon 中，TLS 1.0 依預設為停用。

如需詳細資訊，請參閱 https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf 和 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf。如需如何啟用 TLS 1.0 的指示，請參閱《Horizon 升級》文件中的〈在從連線伺服器連往 vCenter 的連線上啟用 TLSv1〉。

針對 Blast 安全閘道設定安全性通訊協定和加密套件

6

連線伺服器的安全性設定不適用於 Blast 安全閘道 (BSG)。您必須個別為 BSG 設定安全性。

本章節討論下列主題：

針對 Blast 安全閘道 (BSG) 設定安全性通訊協定和加密套件

您可以透過編輯 `absg.properties` 檔案，以設定 BSG 的用戶端接聽程式可接受的安全性通訊協定及加密套件。

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。`localHttpsProtocolLow` 和 `localHttpsProtocolHigh` 這兩個內容會決定 BSG 接聽程式將接受的通訊協定範圍。例如，設定 `localHttpsProtocolLow=tls1.0` 和 `localHttpsProtocolHigh=tls1.2` 會導致接聽程式接受 TLS 1.0、TLS 1.1 和 TLS 1.2。預設設定為 `localHttpsProtocolLow=tls1.2` 和 `localHttpsProtocolHigh=tls1.2`，表示依預設僅允許使用 TLS 1.2。您可以檢查 BSG 的 `absg.log` 檔案來找出針對特定 BSG 執行個體所實施的值。

您必須使用 OpenSSL 中定義的格式來指定加密清單。您可以在網頁瀏覽器中搜尋 `openssl cipher string`，然後查看加密清單格式。下列是預設的加密清單：

```
ECDHE+AESGCM
```

備註 在 FIPS 模式中，僅會啟用 GCM 加密套件 (`ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256`)。

程序

1. 在連線伺服器執行個體上，編輯檔案 *`install_directory`*`\VMware\VMware View\Server\appblastgateway\absg.properties`。

   依預設，安裝目錄為 *%ProgramFiles%*。

2. 編輯 `localHttpsProtocolLow` 和 `localHttpsProtocolHigh` 內容來指定通訊協定範圍。

   例如，

   ```
   localHttpsProtocolLow=tls1.0
   localHttpsProtocolHigh=tls1.2
   ```

若僅要啟用一個通訊協定，請為 `localHttpsProtocolLow` 和 `localHttpsProtocolHigh` 指定相同的通訊協定。

3 編輯 `localHttpsCipherSpec` 內容來指定加密套件清單。

例如，

```
localHttpsCipherSpec=!aNULL:kECDH+AESGCM:ECDH+AESGCM:kECDH+AES:ECDH+AES
```

4 重新啟動 Windows 服務 VMware Horizon Blast 安全閘道。

針對 PCoIP 安全閘道設定安全性通訊協定和加密套件

7

連線伺服器的安全性設定不適用於 PCoIP 安全閘道 (PSG)。您必須個別為 PSG 設定安全性。

本章節討論下列主題：

針對 PCoIP 安全閘道 (PSG) 設定安全性通訊協定和加密套件

您可以透過編輯登錄，以設定 PSG 的用戶端接聽程式可接受的安全性通訊協定及加密套件。如有需要，也可在 RDS 主機上執行此工作。

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。預設設定為 `tls1.2:tls1.1`。

備註 在 FIPS 模式中，僅會啟用 TLS 1.2 (tls1.2)。

下列是預設的加密清單：

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:@STRENGTH"
```

備註 在 FIPS 模式中，僅會啟用 GCM 加密套件 (`ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256`)。

程序

1 在連線伺服器執行個體或 RDS 主機上，開啟登錄編輯程式，並導覽至 `HKLM\Software\Teradici\SecurityGateway`。

2 新增或編輯 REG_SZ 登錄值 `SSLProtocol` 以指定通訊協定清單。

例如，

```
tls1.2:tls1.1
```

3 新增或編輯 REG_SZ 登錄值 `SSLCipherList` 以指定加密套件清單。

例如，

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256
```

4 新增或編輯 REG_SZ 登錄值 `SSLDisableAES128`，以篩選交涉 128 位元 AES 加密金鑰的加密套件。如果未定義，該值會預設為 **0**，表示將不會套用篩選器。若要排除這些加密套件，請將登錄值設定為 **1** 來開啟篩選器。

5 新增或編輯 REG_SZ 登錄值 `SSLDisableRSACipher`，以篩選使用 RSA 進行金鑰交換的加密套件。如果未定義，該值會預設為 **1**，表示將從清單篩選這些加密套件。如果需要包含它們，請將登錄值設定為 **0** 來關閉篩選器。

在安全的 VMware Horizon 環境中部署 USB 裝置

8

USB 裝置容易受到稱為 BadUSB 的安全性威脅，其中，某些 USB 裝置上的韌體可能會遭到劫持並取代為惡意程式碼。例如，使裝置重新導向網路流量或模擬鍵盤並擷取按鍵輸入。您可以設定 USB 重新導向功能，以保護 VMware Horizon 部署免遭此安全性弱點的影響。

透過停用 USB 重新導向，可以防止任何 USB 裝置重新導向至使用者的遠端桌面平台和應用程式。或者，可以停用特定 USB 裝置的重新導向功能，讓使用者僅能存取其遠端桌面平台和應用程式上的特定裝置。

根據組織中的安全性需求決定是否採取這些步驟。這些步驟不具有強制性。可以安裝 USB 重新導向功能，並針對 VMware Horizon 部署中的所有 USB 裝置啟用該功能。請謹慎考慮，至少您的組織應嘗試限制暴露於此安全性弱點之下。

本章節討論下列主題：

- 針對所有類型的裝置停用 USB 重新導向
- 針對特定裝置停用 USB 重新導向

針對所有類型的裝置停用 USB 重新導向

部分高度安全的環境會要求防止使用者可能連接到用戶端裝置的所有 USB 裝置重新導向至遠端桌面平台和應用程式。您可以針對所有桌面平台集區、特定桌面平台集區或桌面平台集區中的特定使用者停用 USB 重新導向。

請根據情況使用以下任一策略：

- 在桌面平台映像或 RDS 主機上安裝 Horizon Agent 時，取消選取 **USB 重新導向**安裝選項。(依預設，會取消選取此選項)。此方法會防止存取所有從桌面平台映像或 RDS 主機部署的遠端桌面平台和應用程式上的 USB 裝置。
- 在 Horizon Console 中，編輯特定集區的 **USB 存取**原則，以拒絕或允許存取。透過此方法，您無需變更桌面平台映像，便可控制在特定桌面平台和應用程式集區中對 USB 裝置的存取。

  已發佈桌面平台和應用程式集區只能使用全域 **USB 存取**原則。無法針對個別已發佈桌面平台或應用程式集區設定此原則。
- 在 Horizon Console 中，於桌面平台或應用程式集區層級設定原則後，可以透過依序選取**使用者覆寫**設定和某個使用者來覆寫集區中特定使用者的原則。
- 請根據情況，在 Horizon Agent 端或用戶端上將 `Exclude All Devices` 原則設定為 **`true`**。

- 使用智慧原則建立原則，以停用 **USB 重新導向** Horizon 原則設定。透過此方法，您可以在符合特定條件時，停用特定遠端桌面平台上的 USB 重新導向。例如，您可以設定原則，在使用者從公司網路外部連線至遠端桌面平台時，停用 USB 重新導向。

如果將 `Exclude All Devices` 原則設定為 **`true`**，則 Horizon Client 會防止重新導向所有 USB 裝置。您可以使用其他原則設定，以允許重新導向特定裝置或裝置系列。如果將原則設定為 **`false`**，則除了由其他原則設定封鎖的裝置以外，Horizon Client 會允許重新導向所有 USB 裝置。您可以為 Horizon Agent 和 Horizon Client 設定此原則。下表顯示了您可以為 Horizon Agent 設定的 `Exclude All Devices` 原則如何與 Horizon Client 合併，以為用戶端電腦產生有效原則。依預設，允許重新導向所有 USB 裝置，封鎖的裝置除外。

表 8-1. 結合排除所有裝置原則的效果

排除 Horizon Agent 上的所有裝置原則	Horizon Client 上的排除所有裝置原則	結合的有效排除所有裝置原則
`false` 或未定義 (包含所有 USB 裝置)	**`false`** 或未定義 (包含所有 USB 裝置)	包含所有 USB 裝置
`false` (包含所有 USB 裝置)	**`true`** (排除所有 USB 裝置)	排除所有 USB 裝置
`true` (排除所有 USB 裝置)	任何或未定義	排除所有 USB 裝置

如果已將 `Disable Remote Configuration Download` 原則設為 **`true`**，則 Horizon Agent 上 `Exclude All Devices` 的值就不會傳送到 Horizon Client，但是 Horizon Agent 和 Horizon Client 會強制執行 `Exclude All Devices` 的本機值。

這些原則包含在 Horizon Agent 組態 ADMX 範本檔 (`vdm_agent.admx`) 中。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》中的〈Horizon Agent 組態 ADMX 範本中的 USB 設定〉。

針對特定裝置停用 USB 重新導向

一些使用者可能需要重新導向特定的本機連線 USB 裝置，才能在遠端桌面平台或應用程式上執行工作。例如，醫師可能需要使用錄音機 USB 裝置來記錄患者的醫療資訊。在這些情況下，則無法停用對所有 USB 裝置的存取權限。您可以使用群組原則設定，針對特定裝置啟用或停用 USB 重新導向。

針對特定裝置啟用 USB 重新導向之前，請確保您信任已連線到企業中的用戶端機器的實體裝置。確保您可以信任供應鏈。如果可能，請追蹤 USB 裝置的保管鏈結。

此外，教導員工，以確保他們不會從未知來源連線裝置。如果可能，將環境中的裝置限制為僅接受已簽署的韌體更新、經過 FIPS 140-2 層級 3 認證以及不支援任何欄位可更新類型的韌體。這些類型的 USB 裝置來源難以找到，甚至可能找不到 (視裝置需求而定)。這些選項可能不切實際，但值得考慮。

每個 USB 裝置都有自己的廠商和產品識別碼，可供電腦進行識別。透過設定 Horizon Agent 組態群組原則設定，您可以針對未知裝置類型設定包含原則。透過此方法，可避免將未知裝置插入您環境所帶來的風險。

例如，您可以防止所有裝置 (除了已知裝置廠商和產品識別碼 vid/pid=0123/abcd) 重新導向至遠端桌面平台或應用程式：

```
ExcludeAllDevices   Enabled

IncludeVidPid       o:vid-0123_pid-abcd
```

備註 此範例組態會提供保護，但受到影響的裝置可能會報告任何 vid/pid，因此，仍可能會發生攻擊。

依預設，Horizon 會封鎖某些裝置系列，使其無法重新導向至遠端桌面平台或應用程式。例如，HID (人機介面裝置) 和鍵盤將被封鎖，無法顯示在客體中。一些已發佈的 BadUSB 程式碼將 USB 鍵盤裝置做為目標。

您可以防止特定的裝置系列重新導向至遠端桌面平台或應用程式。例如，可以封鎖所有視訊、音訊和大量儲存裝置：

```
ExcludeDeviceFamily   o:video;audio;storage
```

反之，可以建立一個白名單，阻止所有裝置重新導向，但允許使用特定的裝置系列。例如，可以封鎖儲存裝置以外的所有裝置：

```
ExcludeAllDevices     Enabled

IncludeDeviceFamily   o:storage
```

如果遠端使用者登入桌面平台或應用程式並對其產生影響，則可能會出現其他風險。您可以阻止 USB 存取來自公司防火牆外部的任何 Horizon 連線。USB 裝置可供內部使用，但無法對外使用。

請注意，如果您封鎖 TCP 連接埠 32111 以停用對 USB 裝置的外部存取，時區同步化將無法運作，因為連接埠 32111 也用於時區同步化。對於零用戶端，USB 流量將內嵌於 UDP 連接埠 4172 上的虛擬通道中。由於連接埠 4172 用於顯示通訊協定以及 USB 重新導向，因此，您無法封鎖連接埠 4172。如果需要，您可以在零用戶端上停用 USB 重新導向。如需詳細資料，請參閱零用戶端產品文宣或連絡零用戶端廠商。

設定原則以封鎖某些裝置系列或特定裝置，有助於降低受到 BadUSB 惡意程式碼之影響的風險。這些原則並不能降低所有風險，但有利於整體安全性策略。

這些原則包含在 Horizon Agent 組態 ADMX 範本檔 (vdm_agent.admx) 中。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》。

連線伺服器上的 HTTP 保護措施

9

運用某些措施來保護使用 HTTP 通訊協定的通訊。

本章節討論下列主題：

- 網際網路工程工作推動小組標準
- 全球資訊網協會標準
- 其他保護措施
- 設定 HTTP 保護措施

網際網路工程工作推動小組標準

連線伺服器符合特定的網際網路工程工作推動小組 (IETF) 標準。

- RFC 5746 傳輸層安全性 (TLS) – 重新交涉指示延伸 (也稱為安全重新交涉) 依預設為啟用。

  備註 連線伺服器依預設會停用用戶端起始的重新交涉。若要啟用，請編輯登錄值 `[HKLM\SOFTWARE\VMware, Inc.\VMware VDM\plugins\wsnm\TunnelService\Params]JvmOptions`，並從字串中移除 **`-Djdk.tls.rejectClientInitiatedRenegotiation=true`**。

- RFC 6797 HTTP 嚴格傳輸安全性 (HSTS) (也稱為傳輸安全性) 依預設為啟用。無法停用此設定。
- RFC 7034 HTTP 標頭欄位 X-Frame-Options (也稱為反點閱綁架) 依預設為啟用。您可以透過將項目 `x-frame-options=OFF` 新增到 `locked.properties` 檔案來加以停用。如需如何將屬性新增到 `locked.properties` 檔案的資訊，請參閱設定 HTTP 保護措施。

  備註 在早於 7.2 版的版本中，變更此選項不會影響對 HTML Access 的連線。

- 可防護跨網站要求偽造攻擊的 RFC 6454 來源檢查預設會啟用。您可以透過將項目 `checkOrigin=false` 新增到 `locked.properties` 來加以停用。如需詳細資訊，請參閱跨來源資源共用。

  備註 在舊版中，預設會停用此保護。

HTTP 嚴格傳輸安全性

HTTP 嚴格傳輸安全性 (HSTS) 功能是一種安全性原則機制，可讓您指示網頁瀏覽器應一律使用 HTTPS 進行連線，以利防止攔截式攻擊。

標頭會新增至連接埠 443 上的所有 HTTP 回應，指定一年的存留期。您可以將多值內容 hstsFlags 新增至 locked.properties 檔案，以設定選用內容。可設定的值如下。

內容	值
includeSubDomains	適用於此站台的所有子網域。
preload	提示要在 HSTS 預先載入清單中包含此站台。

備註 這些內容也可能會影響到非 Horizon URL，因此依預設不會設定。除非您瞭解其含意，否則請勿設定。

全球資訊網協會標準

連線伺服器符合特定全球資訊網協會 (W3C) 標準。

- 跨原始來源資源共用 (CORS) 會限制用戶端跨原始來源要求。您可以對 `locked.properties` 新增項目 `enableCORS = true` 來啟用它，或新增項目 `enableCORS=false` 來加以停用。
- 可減少廣泛類別內容插入漏洞的內容安全性原則 (CSP)，依預設為啟用。您可以透過將項目 `enableCSP=false` 新增到 `locked.properties` 來加以停用。

跨來源資源共用

視用戶端需求提供原則陳述式，並透過檢查要求是否符合原則，跨來源資源共用 (CORS) 功能可規範用戶端跨來源要求。您可以設定此功能並在必要時加以啟用。

原則包括可接受的一組 HTTP 方法、要求的來源，以及有效的內容類型。這些原則可能因要求 URL 而異，並且可視需要透過將項目新增至 `locked.properties` 檔案來重新設定。

內容名稱後面的省略符號表示內容可以接受清單。

表 9-1. CORS 內容

內容	值類型	主要預設值	其他預設值
`enableCORS`	`true` `false`	`false`	`n/a`
`acceptContentType ...`	`http-content-type`	`application/x-www-form-urlencoded,application/xml,text/xml`	`admin`=application/json,application/text,application/x-www-form-urlencoded `portal`=application/json `rest`=application/json `sse`=application/json `view-vlsi-rest`=application/json

表 9-1. CORS 內容 (續)

內容	值類型	主要預設值	其他預設值
acceptHeader...	http-header-name	*	admin=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Cache-Control,Connection,Content-Language,Content-Length,Content-Type,Cookie,csrftoken,DNT,Host,Origin,Referer,User-Agent broker=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,Gateway-Location,Gateway-Name,Gateway-Type,Host,Origin,Referer,User-Agent,X-CSRF-Token,X-EUC-Gateway,X-EUC-Health,X-Forwarded-For,X-Forwarded-Host,X-Forwarded-Proto portal=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,Host,Origin,Referer,User-Agent,X-CSRF-Token rest=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,csrfToken,Host,Origin,Referer,User-Agent,X-Require-Cloud-Admin-Privilege view-vlsi=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,csrfToken,Host,Origin,Referer,User-Agent,X-Require-Cloud-Admin-Privilege view-vlsi-rest=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,csrfToken,Host,Origin,Referer,User-Agent,X-Require-Cloud-Admin-Privilege

表 9-1. CORS 內容 (續)

內容	值類型	主要預設值	其他預設值
exposeHeader...	http-header-name	*	n/a
filterHeaders	true false	true	n/a
checkOrigin	true false	true	n/a
checkReferer	true false	false	n/a
allowCredentials	true false	false	admin=true broker=true health=true misc=true portal=true rest=true saml=true sse=true tunnel=true view-vlsi=true view-vlsi-rest=true
allowMethod...	http-method-name	GET,HEAD,POST	health=GET,HEAD misc=GET,HEAD rest=GET,POST,PUT, PATCH,DELETE saml=GET,HEAD sse=GET,POST tunnel=GET,POST
allowPreflight	true false	true	n/a
maxAge	cache-time	0	n/a
balancedHost	load-balancer-name	OFF	n/a
portalHost...	gateway-name	OFF	n/a
chromeExtension...	chrome-extension-hash	ppkfnjlimknmjoaemnpidmdlfchhehel **備註** 此值為 Chrome 版 Horizon Client 的 Chrome 擴充功能識別碼。	n/a

以下為 locked.properties 檔案中的 CORS 內容範例。

```
enableCORS = true
allowPreflight = true
checkOrigin = true
```

```
checkOrigin-misc = false
allowMethod.1 = GET
allowMethod.2 = HEAD
allowMethod.3 = POST
allowMethod-saml.1 = GET
allowMethod-saml.2 = HEAD
acceptContentType.1 = application/x-www-form-urlencoded
acceptContentType.2 = application/xml
acceptContentType.3 = text/xml
```

來源檢查

來源檢查依預設為啟用。啟用時，將僅在要求不具有來源，或具有的來源等於外部 URL 指定的位址、等於 balancedHost 位址、任何 portalHost 位址、任何 chromeExtension 雜湊、null 或 localhost 時才接受要求。如果來源不屬於上述任何一種情況，則系統會記錄「未預期的來源」錯誤並傳回狀態 404。

備註 某些瀏覽器不會提供「來源」標頭，或不一定只提供一個。當「來源」標頭不存在時，可以選擇性地檢查要求中的「推薦者」標頭。「推薦者」標頭的標頭名稱中具有一個「r」。若要檢查「推薦者」標頭，請將下列內容新增至 locked.properties 檔案：

```
checkReferer=true
```

如果對多個連線伺服器主機執行負載平衡，您必須將 balancedHost 項目新增至 locked.properties 檔案，以指定負載平衡器位址。此位址會採用連接埠 443。

如果用戶端透過 Unified Access Gateway 應用裝置或另一個閘道連線，您必須將 portalHost 項目新增至 locked.properties 檔案來指定所有閘道位址。這些位址會採用連接埠 443。您也必須指定 portalHost 項目，利用與外部 URL 所指定名稱不同的名稱來提供對連線伺服器主機的存取。

Chrome 擴充功能用戶端會將其初始來源設定為其本身的身分識別。若要讓連線成功，請透過將 chromeExtension 項目新增至 locked.properties 檔案來登錄擴充功能。例如：

```
chromeExtension.1=bpifadopbphhpkkcfohecfadckmpjmjd
```

內容安全性原則

內容安全性原則 (CSP) 功能透過向符合規範的瀏覽器提供原則指令，可減少廣泛類別的內容插入漏洞，例如跨網站指令碼 (XSS)。此功能依預設為啟用狀態。您可以透過將項目新增至 locked.properties 以重新設定原則指令。

表 9-2. CSP 內容

內容	值類型	主要預設值	其他預設值
enableCSP	true false	true	n/a
content-security-policy	directives-list	default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval' data:;style-src 'self' 'unsafe-inline';font-src 'self' data: ;frame-ancestors 'none'	admin=default-src 'self' https://feedback.esp.vmware.com; script-src https://feedback.esp.vmware.com 'unsafe-inline' 'unsafe-eval';style-src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https:;frame-ancestors 'none' portal=default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval' data:;style-src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data: blob:;media-src 'self' blob:;connect-src 'self' wss:;frame-src 'self' blob:;child-src 'self' blob:;object-src 'self' blob:;frame-ancestors 'self' rest= default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval' data:;style-src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https:;frame-ancestors 'none'
x-content-type-options	OFF specification	nosniff	n/a
x-frame-options	OFF specification	deny	portal = sameorigin
x-xss-protection	OFF specification	1; mode=block	n/a

您可以將 CSP 內容新增至 locked.properties 檔案。CSP 內容範例：

```
enableCSP = true
content-security-policy = default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;style-src 'self'
 'unsafe-inline';font-src 'self' data:
```

```
content-security-policy-newadmin = default-src 'self';script-src 'self' 'unsafe-inline'
'unsafe-eval' data:;style-src 'self'
 'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https:
content-security-policy-portal = default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-
eval' data:;style-src 'self'
'unsafe-inline';font-src 'self' data:;img-src 'self' data: blob:;media-src 'self'
blob:;connect-src 'self' wss:;frame-src
'self' blob:;child-src 'self' blob:;object-src 'self' blob:
x-content-type-options = nosniff
x-frame-options = deny
x-frame-options-portal = sameorigin
x-xss-protection = 1; mode=block
```

其他保護措施

除了網際網路工程工作推動小組標準和 W3 標準，VMware Horizon 還運用其他措施來保護使用 HTTP 通訊協定的通訊。

降低 MIME 類型的安全性風險

依預設，VMware Horizon 會在其 HTTP 回應中傳送標頭 `x-content-type-options: nosniff`，以防止利用 MIME 類型混淆所發動的攻擊。

您可以透過將下列項目新增到 `locked.properties` 檔案來停用此功能：

```
x-content-type-options=OFF
```

減少跨網站指令碼攻擊

依預設，VMware Horizon 會使用 XSS (跨網站指令碼) 篩選功能，以減少藉由在其 HTTP 回應中傳送標頭 `x-xss-protection=1; mode=block` 而發動的跨網站指令碼攻擊。

您可以透過將下列項目新增到 `locked.properties` 檔案來停用此功能：

```
x-xss-protection=OFF
```

內容類型檢查

依預設，VMware Horizon 只會接受具有下列宣告內容類型的要求：

- application/x-www-form-urlencoded
- application/xml
- text/xml

備註 在舊版中，預設會停用此保護。

若要限制 VMware Horizon 可接受的內容類型，請將下列項目新增至檔案 `locked.properties`：

```
acceptContentType.1=content-type
```

例如：

```
acceptContentType.1=x-www-form-urlencoded
```

若要接受其他內容類型，請新增項目 `acceptContentType.2=content-type`，依此類推。

若要接受具有任何宣告內容類型的要求，請指定 `acceptContentType=*`。

用戶端行為監控

連線伺服器可用於處理來自用戶端要求的資源有限，而行為異常用戶端可能會佔用那些資源，導致他人無法使用服務。用戶端行為監控是一種用來防止不當行為的偵測和防護類別。

信號交換監控

在連接埠 443 上的 TLS 信號交換必須在可設定的期間內完成，否則系統會將其強制終止。依預設，此期間為 10 秒。如果已啟用智慧卡驗證，則在連接埠 443 上的 TLS 信號交換可以在 100 秒內完成。

您可以視需要將下列內容新增至 `locked.properties` 檔案，以便調整連接埠 443 上的 TLS 信號交換時間：

```
handshakeLifetime = lifetime_in_seconds
```

例如：

```
handshakeLifetime = 20
```

您也可以選擇將負責處理過度執行 TLS 信號交換的用戶端自動新增到黑名單。如需詳細資訊，請參閱用戶端加入黑名單。

要求接收監控

HTTP 要求必須在 30 秒內完整接收，否則連線將會強制終止。

傳送要求所花費時間超過此值的用戶端可以選擇性地自動新增至黑名單。如需詳細資訊，請參閱用戶端加入黑名單。

要求計數

單一用戶端每分鐘不應傳送 100 個以上的 HTTP 要求，不過，如果超過此臨界值，依預設不會採取任何動作。

超過此臨界值的用戶端可以選擇性地自動新增至黑名單。如需詳細資訊，請參閱用戶端加入黑名單。

如果已啟用用戶端加入黑名單，您可能需要設定要求計數臨界值。

您可以將下列內容新增至 `locked.properties` 檔案，調整每個用戶端提供的 HTTP 要求數目上限：

```
requestTallyThreshold = max_served_requests_in_30_seconds
```

範例:

```
requestTallyThreshold = 100
```

您可以將下列內容新增至 `locked.properties` 檔案，調整每個用戶端失敗的 HTTP 要求數目上限：

```
tarPitGraceThreshold = max_failed_requests_in_30_seconds
```

範例:

```
tarPitGraceThreshold = 5
```

用戶端加入黑名單

由於它會降低效能，並且若未正確設定會讓使用者不耐煩，因此依預設會停用此類型的保護。如果使用閘道 (例如 Unified Access Gateway 應用裝置) 請勿啟用用戶端加入黑名單，因為它會將所有用戶端連線都顯示為相同的 IP 位址。

如果啟用，來自黑名單上用戶端的連線會延遲一段可設定的時間，之後才會進行處理。如果來自相同用戶端的許多連線同時延遲，則會拒絕來自該用戶端的進一步連線，而非予以延遲。此臨界值可供設定。

您可以將下列內容新增到 `locked.properties` 檔案，以便啟用此功能：

```
secureHandshakeDelay = delay_in_milliseconds
```

例如：

```
secureHandshakeDelay = 2000
```

若要停用 HTTPS 連線的黑名單，請移除 `secureHandshakeDelay` 項目或將其設為 0。

發生 TLS 信號交換滿溢時，用戶端的 IP 位址會新增至黑名單並持續一段最短的期間，即等於 `handshakeLifetime` 和 `secureHandshakeDelay` 的總和。

使用上述範例中的值，行為異常用戶端的 IP 位址會列入黑名單 22 秒：

```
(20 * 1000) + 2000 = 22 seconds
```

每當來自同一 IP 位址的連線行為異常時，最短期間即會延長。最短期間已到期之後，以及系統已處理來自該 IP 位址的上次延遲連線之後，該 IP 位址即會從黑名單中移除。

TLS 信號交換滿溢不是將用戶端加入黑名單的唯一原因。其他原因包括一系列的已放棄連線或因錯誤而結束的一系列要求，例如多次嘗試存取不存在的 URL。這些觸發各自有不同的最短黑名單期間。若要將這些額外觸發的監控延伸至連接埠 80，請將下列項目新增至 `locked.properties` 檔案：

```
insecureHandshakeDelay = delay_in_milliseconds
```

例如：

```
insecureHandshakeDelay = 1000
```

若要停用 HTTP 連線的黑名單，請移除 `insecureHandshakeDelay` 項目或將其設為 0。

行為監控內容

使用這些內容來監控用戶端的行為。這些內容包含防止不當行為之偵測和防護的內容。

表 9-3. 行為監控內容

內容	說明	預設值	動態
handshakeLifetime	TLS 信號交換的時間上限 (以秒為單位)。	10 或 100 (請參閱信號交換監控。)	否
secureHandshakeDelay	加入黑名單時，進行 TLS 信號交換之前的延遲時間 (以毫秒為單位)。	0 (加入黑名單關閉)	否
insecureHandshakeDelay	加入黑名單時，進行非 TLS 信號交換之前的延遲時間 (以毫秒為單位)。	0 (加入黑名單關閉)	否
requestTallyThreshold	針對用戶端加入黑名單，每 30 秒期間提供的 HTTP 要求。	50	否
tarPitGraceThreshold	針對用戶端加入黑名單，每 30 秒期間未提供的 HTTP 要求。	3	否
secureBlacklist...	連接埠 443 上要在加入黑名單時立即拒絕的 IP 位址清單。	不適用	是
insecureBlacklist...	連接埠 80 上要在加入黑名單時立即拒絕的 IP 位址清單。	不適用	是
secureWhitelist...	連接埠 443 上要排除加入黑名單的 IP 位址清單。	不適用	是
insecureWhitelist...	連接埠 80 上要排除加入黑名單的 IP 位址清單。	不適用	是

動態項目的變更會立即生效，而不需重新啟動服務。

使用者代理程式白名單

設定白名單以限制可以與 VMware Horizon 進行互動的使用者代理程式。依預設會接受所有的使用者代理程式。

備註 這不是一種嚴密的安全性功能。使用者代理程式偵測會根據連線用戶端或瀏覽器提供的使用者代理程式要求標頭，而這可能會遭到假冒。某些瀏覽器允許使用者修改要求標頭。

使用者代理程式是根據其名稱和最低版本所指定。例如：

```
clientWhitelist-portal.1 = Chrome-14
clientWhitelist-portal.2 = Safari-5.1
```

這表示僅允許 Google Chrome 14 版及更新版本，以及 Safari 5.1 版及更新版本使用 HTML Access 進行連線。所有瀏覽器皆可連線至其他服務。

您可以輸入下列識別的使用者代理程式名稱：

- Android

- Chrome
- Edge
- IE
- Firefox
- Opera
- Safari

備註 VMware Horizon 並不支援這些所有的使用者代理程式。這些是範例。

設定 HTTP 保護措施

若要設定 HTTP 保護措施，您必須在連線伺服器執行個體上的閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

例如：*`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

- 在 `locked.properties` 中使用下列語法設定內容：

  ```
  myProperty = newValue
  ```

- 內容名稱一律須區分大小寫，且值可能會區分大小寫。=符號周圍的空格是選擇性的。
- 您可以針對 CORS 和 CSP 內容設定服務特定值以及主要值。例如，管理員服務負責處理 Horizon Console 要求，且可以透過在內容名稱後附加 `-admin` 來為此服務設定內容，而不會影響其他服務。

  ```
  myProperty-admin = newValueForAdmin
  ```

- 如果同時指定了主要值和服務特定值，則會將服務特定值套用至指定名稱的服務，並將主要值套用至所有其他服務。此情況的唯一例外狀況為特殊值「OFF」。如果內容的主要值設定為「OFF」，則系統會忽略此內容的所有服務特定值。

  例如：

  ```
  myProperty = OFF
  myProperty-admin = newValueForAdmin    ; ignored
  ```

- 部分內容可接受值的清單。

  若要設定單一值，請輸入下列內容：

  ```
  myProperty = newValue
  myProperty-admin = newValueForAdmin
  ```

若要針對接受清單值的內容設定多個值，您可以在各行指定每個值：

```
myProperty.1 = newValue1
myProperty.2 = newValue2
myProperty-admin.1 = newValueForAdmin1
myProperty-admin.2 = newValueForAdmin2
```

- 若要判斷進行服務特定組態時要使用的正確服務名稱，請查詢偵錯記錄以取得包含下列順序的行：

```
(ajp:admin:Request21) Request from abc.def.com/10.20.30.40: GET /admin/
```

在此範例中，服務名稱為 `admin`。您可以使用下列一般服務名稱：

- `newadmin` 表示 Horizon Console
- `broker` 表示連線伺服器
- `docroot` 表示本機檔案服務
- `portal` 表示 HTML Access
- `saml` 表示 SAML 通訊 (vIDM)
- `tunnel` 表示安全通道
- `view-vlsi` 表示 View API
- `misc` 表示其他項目
- `rest` 表示 REST API