

View 安全性

VMware Horizon 7 7.2



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

Copyright © 2009-2017 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

目錄

View 安全性	5
1 Horizon 7 帳戶、資源和記錄檔	6
Horizon 7 帳戶	6
Horizon 7 資源	7
Horizon 7 記錄檔	7
2 View 安全性設定	9
View Administrator 中的安全性相關全域設定	9
View Administrator 中的安全性相關伺服器設定	11
View LDAP 中的安全性相關設定	12
3 連接埠和服務	13
View TCP 和 UDP 連接埠	13
View 中的 HTTP 重新導向	16
View 連線伺服器主機上的服務	17
安全伺服器上的服務	17
4 在 View 連線伺服器執行個體或安全伺服器上設定安全性通訊協定及加密套件	19
安全性通訊協定及加密套件的預設全域原則	19
設定全域接受與建議原則	20
View LDAP 中定義的全域接受與建議原則	20
變更全域接受與建議原則	21
設定個別 View Server 上的接受原則	21
在 View 桌面平台上設定建議原則	22
View 中已停用的舊版通訊協定和加密	23
5 針對 Blast 安全閘道設定安全性通訊協定和加密套件	25
針對 Blast 安全閘道 (BSG) 設定安全性通訊協定和加密套件	25
6 在安全的 Horizon 7 環境中部署 USB 裝置	27
針對所有類型的裝置停用 USB 重新導向	27
針對特定裝置停用 USB 重新導向	28
7 連線伺服器和安全伺服器上的 HTTP 保護措施	30
網際網路工程工作推動小組標準	30
全球資訊網協會標準	31

跨來源資源共用	31
內容安全性原則	32
其他保護措施	33
降低 MIME 類型的安全性風險	33
減少跨網站指令碼攻擊	34
內容類型檢查	34
使用者代理程式白名單	34
設定 HTTP 保護措施	35

View 安全性

《View 安全性》對於 VMware Horizon 7 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 View 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 View 安全性元件的其他人。

Horizon 7 帳戶、資源和記錄檔

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。

備註 從 Horizon 7.0 開始，View Agent 已重新命名為 Horizon Agent。

本章節討論下列主題：

- [Horizon 7 帳戶](#)
- [Horizon 7 資源](#)
- [Horizon 7 記錄檔](#)

Horizon 7 帳戶

您必須設定系統與資料庫帳戶來管理 Horizon 7 元件。

表 1-1. Horizon 7 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 Horizon 7 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《View 安裝》文件。
View Composer	在 Active Directory 中，建立搭配 View Composer 使用的使用者帳戶。View Composer 需要此帳戶才能將連結複製桌面平台加入您的 Active Directory 網域中。 使用者帳戶不應該是 Horizon 管理帳戶。請為帳戶提供在指定的 Active Directory 容器中建立與移除電腦物件所需的最小權限。例如，此帳戶不需要網域管理員權限。 如需所需權限的相關資訊，請參閱《View 安裝》文件。
連線伺服器	在安裝 Horizon 7 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 Administrator 中，您可以使用 View 組態 > 管理員 來變更 Horizon 管理員清單。 請參閱《View 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
View Composer 資料庫	SQL Server 或 Oracle 資料庫可儲存 View Composer 資料。您要針對可以與 View Composer 使用者帳戶建立關聯的資料庫，建立管理帳戶。 如需設定 View Composer 資料庫的相關資訊，請參閱《View 安裝》文件。
Horizon 連線伺服器所使用的事件資料庫	SQL Server 或 Oracle 資料庫會儲存 Horizon 事件資料。您需要針對 Horizon Administrator 可以用來存取事件資料的資料庫建立管理帳戶。 如需設定 View Composer 資料庫的相關資訊，請參閱《View 安裝》文件。

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 Horizon 7 資料庫。
- 請不要允許單一使用者帳戶存取多個資料庫。
- 針對 View Composer 資料庫和事件資料庫的存取，設定不同的帳戶。

Horizon 7 資源

Horizon 7 包含必須受到保護的數個組態檔和類似資源。

表 1-3. Horizon 連線伺服器和安全伺服器資源

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 Horizon 7 記錄檔	受到存取控制保護。
web.xml (Tomcat 組態檔)	install_directory\VMware View\Server\broker\webapps\ROOT\Web INF	受到存取控制保護。

Horizon 7 記錄檔

Horizon 7 所建立的記錄檔會記錄其元件的安裝與操作。

備註 Horizon 7 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 Horizon 7。如需詳細資訊，請參閱《View 安裝》和《View 整合》文件。

表 1-4. Horizon 7 記錄檔

Horizon 元件	檔案路徑與其他資訊
所有元件 (安裝記錄)	<p>%TEMP%\vminst.log_date_timestamp</p> <p>%TEMP%\vmmsi.log_date_timestamp</p>
Horizon Agent	<p><Drive Letter>:\ProgramData\VMware\VDM\logs</p> <p>若要存取儲存於 <Drive Letter>:\ProgramData\VMware\VDM\logs 中的 Horizon 7 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。</p> <p>如果已設定使用者資料磁碟 (UDD)，則 <Drive Letter> 可能會對應至 UDD。</p> <p>PCoIP 記錄的名稱為 pcoip_agent*.log 和 pcoip_server*.log。</p>
已發佈的應用程式	<p>在 SQL Server 或 Oracle 資料庫伺服器上設定的 View 事件資料庫。</p> <p>Windows 應用程式事件記錄。預設為停用狀態。</p>
View Composer	<p>連結複製桌面平台上的 %system_drive%\Windows\Temp\vmware-viewcomposer-ga-new.log。</p> <p>View Composer 記錄包含執行 QuickPrep 與 Sysprep 指令碼的相關資訊。此記錄會記錄指令碼執行的開始時間和結束時間，以及任何輸出或錯誤訊息。</p>
連線伺服器或安全伺服器	<p><Drive Letter>:\ProgramData\VMware\VDM\logs。</p> <p>記錄目錄可在 View 一般組態 ADMX 範本檔 (vdm_common.admx) 的記錄組態設定中設定。</p> <p>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。</p> <p>Blast 安全閘道記錄會寫入到 Blast Secure Gateway 子目錄中名為 absrg*.log 的檔案中。</p>
Horizon 服務	<p>在 SQL Server 或 Oracle 資料庫伺服器上設定的 Horizon 事件資料庫。</p> <p>Windows 系統事件記錄。</p>

View 安全性設定

View 包含您可以用來調整組態安全性的數個設定。您可以使用 **View Administrator**，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：

- [View Administrator 中的安全性相關全域設定](#)
- [View Administrator 中的安全性相關伺服器設定](#)
- [View LDAP 中的安全性相關設定](#)

View Administrator 中的安全性相關全域設定

可在 **View Administrator** 中的 **View 組態 > 全域設定** 下，存取適用於用戶端工作階段和連線的安全性相關全域設定。

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	<p>當您從加密的備份還原 View LDAP 組態時，需要密碼。</p> <p>安裝 View 連線伺服器 5.1 版或更新版本時，您要提供資料復原密碼。安裝完成後，您可以在 View Administrator 中變更此密碼。</p> <p>備份 View 連線伺服器時，會將 View 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。</p>
訊息安全模式	<p>決定 JMS 訊息在 View 元件之間傳遞時所使用的安全性機制。</p> <ul style="list-style-type: none"> ■ 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。View 元件會拒絕未簽署的訊息。此模式支援 SSL 和一般 JMS 連線的混合。 ■ 若設為增強，則 SSL 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 View 元件可傳送和接收訊息的 JMS 主題。 ■ 如果設為混合，則會啟用訊息安全性模式，但不會針對早於 View Manager 3.0 的 View 元件強制執行。 <p>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。</p> <p>重要 VMware 強烈建議在升級所有 View 連線伺服器執行個體、安全性伺服器以及 View 桌面平台至此版本後，將訊息安全性模式設定為增強。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。</p>
增強安全性狀態 (唯讀)	<p>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：</p> <ul style="list-style-type: none"> ■ 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 View 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 View 訊息匯流排元件服務之後，系統會開始針對所有桌面平台和安全伺服器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	<p>決定當 Horizon Client 使用安全通道連線至 View 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。</p> <p>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 View 桌面平台和應用程式的存取權，因為網路連線暫時中斷。</p> <p>此設定依預設為停用。</p>
強制中斷使用者連線	<p>自使用者登入 View 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。</p> <p>預設值為 600 分鐘。</p>
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	<p>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 View 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。</p> <p>如果設定為永不，View 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。</p> <p>預設值為永不。</p>
其他用戶端。 捨棄 SSO 認證	<p>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 View 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。</p> <p>預設值為 15 分鐘後。</p>

設定	說明
啟用 IPsec 以進行安全伺服器配對	決定安全伺服器與 View 連線伺服器執行個體之間是否使用網際網路通訊協定安全性 (IPsec) 連線。在 FIPS 模式中安裝安全伺服器之前必須先停用此設定，否則配對將會失敗。 預設會啟用安全伺服器連線的 IPsec。
View Administrator 工作階段逾時	決定 View Administrator 工作階段會持續閒置多久的時間，工作階段才會逾時。 重要 若將 View Administrator 工作階段逾時分鐘設為很大的數字，會增加未經授權使用 View Administrator 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，View Administrator 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。

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。

備註 所有與 View 之間的 Horizon Client 連線與 View Administrator 連線都需要 SSL。如果您的 View 部署使用負載平衡器或其他面向用戶端的中繼伺服器，您便可以將 SSL 卸載到這些負載平衡器或中繼伺服器，然後在個別的 View 連線伺服器執行個體與安全伺服器上設定非 SSL 連線。請參閱《View 管理》文件中的「將 SSL 連線卸載到中繼伺服器」。

View Administrator 中的安全性相關伺服器設定

可在 View Administrator 中的 **View 組態 > 伺服器** 下存取安全性相關的伺服器設定。

表 2-2. 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 View 桌面平台和應用程式時，Horizon Client 要與 View 連線伺服器還是安全伺服器主機建立其他安全的連線。 如果停用此設定，就會直接在用戶端系統與 View 桌面平台或遠端桌面平台服務 (RDS) 主機之間建立桌面平台或應用程式工作階段，略過 View 連線伺服器或安全伺服器主機。 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 View 桌面平台或應用程式時，Horizon Client 要與 View 連線伺服器還是安全伺服器主機建立其他 HTTPS 連線。 如果停用此設定，就會直接在用戶端系統與 View 桌面平台或遠端桌面平台服務 (RDS) 主機之間建立桌面平台或應用程式工作階段，略過 View 連線伺服器或安全伺服器主機。 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 View 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 View 連線伺服器，直接與 View 桌面平台建立連線。 此設定依預設為停用。

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。

View LDAP 中的安全性相關設定

安全性相關的設定是在 View LDAP 的

`cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` 物件路徑底下提供。您可以使用 ADSI Edit 公用程式，在 View 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 View 連線伺服器執行個體。

表 2-3. View LDAP 中的安全性相關設定

名稱/值對	說明
cs-allowunencryptedstartsession	<p>屬性為 <code>pae-NameValuePair</code>。</p> <p>此屬性會控制啟動遠端使用者工作階段時，在 View 連線伺服器執行個體與桌面平台之間是否需要安全通道。</p> <p>在桌面平台電腦上安裝 View Agent 5.1 或更新版本，或 Horizon Agent 7.0 或更新版本時，此屬性沒有作用，且一律需要安全通道。安裝 View 5.1 之前的 View Agent 時，如果桌面平台電腦不是網域成員，且對於 View 連線伺服器執行個體的網域不是雙向信任，則無法建立安全通道。在此情況下，此屬性對於決定是否可以在沒有安全通道的情況下啟動遠端使用者工作階段相當重要。</p> <p>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。</p> <p>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經安裝 View Agent 5.1 或更新版本，則此設定相當合適。</p> <p>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 View Agent，且未處於受信任的網域，則此設定相當合適。</p> <p>預設設定為 1。</p>

連接埠和服務

必須開啟某些 UDP 和 TCP 連接埠，View 元件才能夠彼此通訊。瞭解每個類型的 View Server 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：

- View TCP 和 UDP 連接埠
- View 連線伺服器主機上的服務
- 安全伺服器上的服務

View TCP 和 UDP 連接埠

View 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，View 可以選擇性地設定 Windows 防火牆規則，以開放預設使用的連接埠。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《View 安裝》文件中的〈取代 View 服務的預設連接埠〉。

表 3-1. View 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
安全伺服器、View 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)。
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。
安全伺服器	500	View 連線伺服器	500	UDP	IPsec 交涉流量。
安全伺服器	*	View 連線伺服器	4001	TCP	JMS 流量。
安全伺服器	*	View 連線伺服器	4002	TCP	JMS SSL 流量。
安全伺服器	*	View 連線伺服器	8009	TCP	AJP13 正向網路流量 (如果未使用 IPsec)。
安全伺服器	*	View 連線伺服器	*	ESP	AJP13 正向網路流量 (沒有透過 NAT 使用 IPsec 時)。
安全伺服器	4500	View 連線伺服器	4500	UDP	AJP13 正向網路流量 (透過 NAT 裝置使用 IPsec 時)。

來源	連接埠	目標	連接埠	通訊協定	說明
安全伺服器、View 連線伺服器或 Unified Access Gateway 應用裝置	*	Horizon Agent	3389	TCP	Microsoft RDP 到 View 桌面平台的流量 (如果使用通道連線)。
安全伺服器、View 連線伺服器或 Unified Access Gateway 應用裝置	*	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)。
安全伺服器、View 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)。
安全伺服器、View 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)。
安全伺服器、View 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)。
安全伺服器、View 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	View 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)。
Horizon Agent	4172	Unified Access Gateway 應用裝置	*	UDP	PCoIP。View 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。

來源	連接埠	目標	連接埠	通訊協定	說明
Horizon Client	*	View 連線伺服器或安全伺服器或 Unified Access Gateway 應用裝置	80	TCP	用戶端連線預設啟用 SSL (HTTPS 存取)，但在某些情況下可以使用連接埠 80 (HTTP 存取)。請參閱 View 中的 HTTP 重新導向 。
Horizon Client	*	View 連線伺服器、安全伺服器或 Unified Access Gateway 應用裝置	443	TCP	記錄至 View 時為 HTTPS(使用通道連線時，此連接埠也用於通道處理)。
Horizon Client	*	View 連線伺服器或安全伺服器或 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 View 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 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)。
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	*	View 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。
網頁瀏覽器	*	安全伺服器或 Unified Access Gateway 應用裝置	8443	TCP	HTML Access。
View 連線伺服器	*	View 連線伺服器	48080	TCP	供在 View 連線伺服器元件之間進行內部通訊使用。
View 連線伺服器	*	vCenter Server 或 View Composer	80	TCP	SOAP 訊息 (如果對 vCenter Server 或 View Composer 的存取停用 SSL)。
View 連線伺服器	*	vCenter Server	443	TCP	SOAP 訊息 (如果對 vCenter Server 的存取啟用 SSL)。
View 連線伺服器	*	View Composer	18443	TCP	SOAP 訊息 (如果對 View Composer 的存取啟用 SSL)。
View 連線伺服器	*	View 連線伺服器	4100	TCP	JMS 路由器間的流量。
View 連線伺服器	*	View 連線伺服器	4101	TCP	JMS SSL 路由器間的流量。

來源	連接埠	目標	連接埠	通訊協定	說明
View 連線伺服器	*	View 連線伺服器	8472	TCP	供在 Cloud Pod 架構中進行網間通訊使用。
View 連線伺服器	*	View 連線伺服器	22389	TCP	供在 Cloud Pod 架構中進行全域 LDAP 複寫使用。
View 連線伺服器	*	View 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。
Unified Access Gateway 應用裝置	*	View 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 View 連線伺服器執行個體或位在多個 View 連線伺服器執行個體前方的負載平衡器進行通訊。
View Composer 服務	*	ESXi 主機	902	TCP	當 View Composer 自訂連結複製磁碟 (包括 View Composer 內部磁碟) 且這些磁碟被指定持續性磁碟與系統可處置的磁碟時使用。

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 Horizon 7 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。

View 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，但連線到 View Administrator 的嘗試則除外。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 連線到 View Administrator 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《View 安裝》文件中的「防止用戶端連線透過 HTTP 重新導向至連線伺服器」。

如果您將 SSL 用戶端連線卸載至中繼裝置，則也可連線到 View 連線伺服器執行個體或安全伺服器的連接埠 80。請參閱《View 管理》文件中的「將 SSL 連線卸載到中繼伺服器」。

若要在變更 SSL 連接埠號碼時允許 HTTP 重新導向，請參閱《View 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」。

View 連線伺服器主機上的服務

View 的作業取決於在 View 連線伺服器主機上執行的數個服務。

表 3-2. View 連線伺服器主機服務

服務名稱	啟動類型	描述
VMware Horizon View 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 View 連線伺服器，則此服務必須在執行狀態下。
VMware Horizon View 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 View 指令碼主機服務。
VMware Horizon View Framework 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 View 訊息匯流排元件	手動	在 View 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 View 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 View 連線伺服器，則此服務必須在執行狀態下。
VMware Horizon View 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 View 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 View 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 LDAP 目錄服務。此服務必須永遠處於執行狀態。在 View 升級期間，此服務可確保現有資料能正確移轉。

安全伺服器上的服務

View 的作業取決於在安全伺服器上執行的數個服務。

表 3-3. 安全伺服器服務

服務名稱	啟動類型	說明
VMware Horizon View 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 安全閘道連線至此安全伺服器，則此服務必須處於執行狀態。
VMware Horizon View 安全伺服器	自動	提供安全伺服器服務。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 和安全閘道服務。
VMware Horizon View Framework 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。

服務名稱	啟動類型	說明
VMware Horizon View 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 安全閘道連線至此安全伺服器，則此服務必須處於執行狀態。
VMware Horizon View 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。

在 View 連線伺服器執行個體或安全伺服器上設定安全性通訊協定及加密套件

4

您可以設定 View 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 View 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 View 連線伺服器執行個體與安全伺服器的接受原則。

您也可以設定連線至 vCenter Server 和 View Composer 時，View 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 View 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 View 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 5 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](#)
- [設定全域接受與建議原則](#)
- [設定個別 View Server 上的接受原則](#)
- [在 View 桌面平台上設定建議原則](#)
- [View 中已停用的舊版通訊協定和加密](#)

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 4-1. 預設全域原則

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 1.1	■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
■ TLS 1.0	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	■ TLS_RSA_WITH_AES_128_CBC_SHA
	■ TLS_RSA_WITH_AES_256_CBC_SHA

如果所有連線的用戶端都支援 TLS 1.1 和 (或) TLS 1.2，您可以從接受原則中移除 TLS 1.0。

設定全域接受與建議原則

全域接受與建議原則是在 View LDAP 屬性中定義。這些原則適用於複寫的群組中的所有 View 連線伺服器執行個體和安全伺服器。若要變更全域原則，您可以在任何 View 連線伺服器執行個體上編輯 View LDAP。

每個原則在下列的 View LDAP 位置中，都是單一值屬性：

`cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int`

View 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 View 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 View LDAP 屬性。

必要條件

- 請熟悉定義接受與建議原則的 View LDAP 屬性。請參閱 [View 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 View 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 View 連線伺服器電腦的完整網域名稱 (FQDN)，後面接著連接埠 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 **OU=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和安全伺服器上，重新啟動 Windows 服務 VMware Horizon View 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 View Server 上的接受原則

若要在個別的 View 連線伺服器執行個體或安全伺服器上指定本機接受原則，您必須將屬性新增至 **locked.properties** 檔。如果 **locked.properties** 檔不存在於 View Server 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 View 連線伺服器或安全伺服器電腦上的 SSL 開道組態資料夾中，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 View 連線伺服器服務或 VMware Horizon View 安全伺服器服務，讓您的變更生效。

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
secureProtocols.2=TLSv1.1
secureProtocols.3=TLSv1

# 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_CBC_SHA256
enabledCipherSuite.2=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.3=TLS_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.4=TLS_RSA_WITH_AES_128_CBC_SHA

# Use the ordering of cipher suites given above:

honorClientOrder=false
```

在 View 桌面平台上設定建議原則

您可以在執行 Windows 的 View 桌面平台上設定建議原則，對 View 連線伺服器的訊息匯流排連線進行安全性的控制。

請確實將 View 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 View 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
```

View 中已停用的舊版通訊協定和加密

根據預設，在 View 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、安全伺服器和 View 桌面平台，您可以藉由編輯 View LDAP 資料庫、locked.properties 檔案或登錄來啟用這些加密套件，如本指南所說明。請參閱[變更全域接受與建議原則](#)、[設定個別 View Server 上的接受原則](#)和在 [View 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 Composer 和 View Agent Direct-Connection (VADC) 機器，您可以在執行《View 安裝》文件中的〈針對 View Composer 和 Horizon Agent 機器停用 SSL/TLS 中的弱加密〉程序時，將下列項目新增到加密清單，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

Horizon 7 已移除 SSL 3.0 版。

如需詳細資訊，請參閱 <http://tools.ietf.org/html/rfc7568>。

RC4

如需更多資訊，請參閱 <http://tools.ietf.org/html/rfc7465>。

對於連線伺服器執行個體、安全伺服器和 View 桌面平台，您可以藉由編輯組態檔 C:\Program Files\VMware\VMware View\Server\jre\lib\security\java.security，在連線伺服器、安全伺服器或 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、安全伺服器或 Horizon Agent 機器。

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

```
TLS_RSA_WITH_RC4_128_SHA
```

TLS 1.0

在 Horizon 7 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《View 升級》文件中的〈在從連線伺服器連往 vCenter 的連線上啟用 TLSv1〉和〈在從 View Composer 連往 vCenter 和 ESXi 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

View 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

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，`localHttpsProtocolLow=tls1.0` 和 `localHttpsProtocolHigh=tls1.2` 設定將造成接聽程式接受 TLS 1.0、TLS 1.1 和 TLS 1.2。預設設定為 `localHttpsProtocolLow=tls1.1` 和 `localHttpsProtocolHigh=tls1.2`。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 <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 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=ECDHE-RSA-AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

- 4 重新啟動 VMware HorizonView Blast 安全閘道這個 Windows 服務。

在安全的 Horizon 7 環境中部署 USB 裝置

6

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 Horizon 7 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 Horizon 7 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 Horizon 7 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 Administrator 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。

RDS 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 RDS 桌面平台或應用程式集區設定此原則。

- 在 View Administrator 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 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 6-1. 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 Exclude All Devices** 上的值就不會傳送到 **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 7** 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 7** 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 7** 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。如需更多資訊，請參閱在 **Horizon 7** 中設定遠端桌面平台功能。

連線伺服器和安全伺服器上的 HTTP 保護措施

7

Horizon 7 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

連線伺服器和安全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 連線伺服器和安全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 Horizon 7 (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。

全球資訊網協會標準

連線伺服器和安全伺服器符合特定全球資訊網協會 (W3C) 標準。

- 會限制用戶端跨來源要求的跨來源資源共用 (CORS)，依預設為啟用。您可以透過將項目 `enableCORS=false` 新增到 `locked.properties` 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。此功能依預設為啟用狀態。

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。這些可能因要求 URL 而異，並且可視需要透過將項目新增至 `locked.properties` 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 7-1. CORS 內容

內容	值類型	主要預設值	其他預設值
<code>enableCORS</code>	<code>true</code> <code>false</code>	<code>true</code>	n/a
<code>acceptContentType...</code>	<code>http-content-type</code>	<code>application/x-www-form-urlencoded,application/xml,text/xml</code>	<ul style="list-style-type: none"> ■ <code>admin=application/x-amf</code> ■ <code>helpdesk=application/json,application/text,application/x-www-form-urlencoded</code> ■ <code>view-vlsi-rest=application/json</code>
<code>acceptHeader...</code>	<code>http-header-name</code>	*	n/a
<code>exposeHeader...</code>	<code>http-header-name</code>	*	n/a
<code>filterHeaders</code>	<code>true</code> <code>false</code>	<code>true</code>	n/a
<code>checkOrigin</code>	<code>true</code> <code>false</code>	<code>true</code>	n/a
<code>allowCredentials</code>	<code>true</code> <code>false</code>	<code>false</code>	<code>admin=true</code> <code>broker=true</code> <code>helpdesk=true</code> <code>misc=true</code> <code>portal=true</code> <code>saml=true</code> <code>tunnel=true</code> <code>view-vlsi=true</code> <code>view-vlsi-rest=true</code>

內容	值類型	主要預設值	其他預設值
allowMethod...	http-method-name	GET, HEAD, POST	misc=GET, HEAD saml=GET, HEAD
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	OFF	n/a

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，或具有的來源等於在外部 URL 中指定的位址、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。

如果對多個連線伺服器或安全伺服器執行負載平衡，您必須將 balancedHost 項目新增到 locked.properties，以指定負載平衡器位址。此位址會採用連接埠 443。

如果用戶端需要透過 Unified Access Gateway 或另一個閘道連線，您必須透過將 portalHost 項目新增至 locked.properties 來指定所有閘道位址。這些位址也會採用連接埠 443。如果您想提供對連線伺服器或安全伺服器的存取，但使用的名稱與外部 URL 中所指定的不同，請執行相同動作。

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 來登錄擴充功能。

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 7-2. 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:	portal=child-src 'self' blob;;default-src 'self';connect-src 'self' wss;;font-src 'self' data::img-src 'self' data: blob;;media-src 'self' blob;;object-src 'self' blob;;script-src 'self' 'unsafe-inline' 'unsafe-eval' data::style-src 'self' 'unsafe-inline';frame- ancestors 'self'
x-frame-options	OFF specification	deny	portal=sameorigin
x-content-type-options	OFF specification	nosniff	n/a
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' data:
content-security-policy-portal = default-src 'self';frame-ancestors 'self'
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，Horizon 7 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，Horizon 7 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，Horizon 7 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，Horizon 7 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 View 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=*`。

備註 在早於 Horizon 7 (7.2 版) 的版本中，變更此清單不會影響 Horizon Administrator 的連線。

使用者代理程式白名單

設定白名單以限制可以與 Horizon 7 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 Horizon 7 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或安全伺服器執行個體上的 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\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 Administrator 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：

- **admin** 表示 Horizon Administrator
- **broker** 表示連線伺服器
- **docroot** 表示本機檔案服務
- **helpdesk** 表示服務台
- **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