View Agent Direct-Connection 外掛程式管理

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

View Agent Direct-Connection 外掛程式管理

《View Agent Direct-Connection 外掛程式管理》提供安裝和設定 View Agent Direct-Connection 外掛程式的相關資訊。此外掛程式是 Horizon Agent 的可安裝擴充程式，允許 Horizon Client 直接連線至虛擬機器型的桌面平台、已發佈的桌面平台或應用程式，而不需使用 Horizon 連線伺服器。所有桌面平台和應用程式功能的運作方式與使用者透過連線伺服器連線時相同。

主要對象

本資訊專供想要在虛擬機器型桌面平台或 RDS 主機上安裝、升級或設定 View Agent Direct-Connection 外掛程式的管理員使用。本指南是專為具有經驗且熟悉虛擬機器技術和資料中心操作的 Windows 系統管理員所撰寫。

安裝 View Agent Direct-Connection 外掛程式

1

View Agent Direct-Connection (VADC) 外掛程式啟用 Horizon Client 來直接連線至虛擬機器型桌面平台、已發佈的桌面平台或應用程式。VADC 外掛程式為 Horizon Agent 的延伸，並安裝在虛擬機器型桌面平台或 RDS 主機上。

本章節討論下列主題：

View Agent Direct-Connection 外掛程式系統需求

View Agent Direct-Connection (VADC) 外掛程式安裝於 Horizon Agent 安裝所在的機器。如需 Horizon Agent 支援的作業系統清單，請參閱《Horizon 安裝》文件中的〈Horizon Agent 支援的作業系統〉。

VADC 外掛程式具有以下其他需求：

- 已安裝 VADC 外掛程式的虛擬或實體機器必須擁有至少 128 MB 的視訊 RAM，才能正常運作。
- 對於虛擬機器，您必須先安裝 VMware Tools，然後再安裝 Horizon Agent。
- 實體機器支援 Windows 10 Enterprise 1803 版或 1809 版。

VADC 外掛程式支援通訊協定如下所示：

- 已安裝 VADC 外掛程式的虛擬機器支援 Blast 和 PCoIP 通訊協定。
- 已安裝 VADC 外掛程式的實體機器僅支援 Blast 通訊協定。

備註 支援 VADC 的虛擬機器型桌面平台可加入 Microsoft Active Directory 網域，也可以成為工作群組的成員。

安裝 View Agent Direct-Connection 外掛程式

View Agent Direct-Connection (VADC) 外掛程式封裝在可從 VMware 網站下載並安裝的 Windows Installer 檔案中。

必要條件

- 確認已安裝 Horizon Agent。如果您的環境未包含連線伺服器，請從命令列安裝 Horizon Agent，然後指定告知 Horizon Agent 不要登錄至連線伺服器的參數。請參閱為 HTML Access 安裝 Horizon Agent。
- 啟用 vSphere 6.0 及更新版本上虛擬機器的畫面 DMA 設定。若畫面 DMA 停用，則使用者會在連線至遠端桌面平台時看到黑色畫面。如需關於設定畫面 DMA 方法的詳細資訊，請參閱 VMware 知識庫 (KB) 文章 2144475 http://kb.vmware.com/kb/2144475。

程序

1 從 VMware 下載頁面下載 VADC 外掛程式安裝程式檔案，網址為 http://www.vmware.com/go/downloadview。

對於 64 位元 Windows，安裝程式檔案名稱為 VMware-viewagent-direct-connection-x86_64-y.y.y-xxxxxx.exe，而對於 32 位元 Windows，安裝程式檔案名稱則為 VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe，其中 y.y.y 為版本號碼，xxxxxx 為組建編號。

2 按兩下安裝程式檔案。

3 (選擇性) 變更 TCP 連接埠號碼。

預設連接埠編號是 443。

4 (選擇性) 選擇如何設定 Windows 防火牆服務。

依預設，會選取**自動設定 Windows 防火牆**，並且安裝程式會將 Windows 防火牆設定為允許所需網路連線。

5 (選擇性) 選擇是否停用 SSL 3.0。

依預設，**自動停用 SSLv3 支援 (建議)** 已選取，且安裝程式會在作業系統層級停用 SSL 3.0。如果 SSL 3.0 已在登錄中明確啟用或停用，則不會顯示此選項，安裝程式不會執行任何動作。如果此選項已取消選取，安裝程式也不會執行任何動作。

6 依照提示完成安裝。

以無訊息方式安裝 View Agent Direct-Connection 外掛程式

您可以使用 Microsoft Windows Installer (MSI) 的無訊息安裝功能來安裝 View Agent Direct-Connection (VADC) 外掛程式。在無訊息安裝中，您可以使用命令列且不必回應精靈提示。

透過無訊息安裝，您便能有效地將 VADC 外掛程式部署在大型企業中。如需 Windows Installer 的詳細資訊，請參閱《在 Horizon 中設定虛擬桌面平台》文件中的〈Microsoft Windows Installer 命令列選項〉。VADC 外掛程式支援以下 MSI 屬性。

表 1-1. 無訊息安裝 View Agent Direct-Connection 外掛程式的 MSI 屬性

MSI 屬性	說明	預設值
LISTENPORT	VADC 外掛程式用於接受遠端連線的 TCP 連接埠。依預設，安裝程式會將 Windows 防火牆設定為允許此連接埠上的流量。	443
MODIFYFIREWALL	若設定為 1，此安裝程式會將 Windows 防火牆設定為允許 LISTENPORT 上的流量。若設定為 0，此安裝程式會將 Windows 防火牆設定為不允許 LISTENPORT 上的流量。	1
DISABLE_SSLV3	如果 SSL 3.0 已在登錄中明確啟用或停用，則安裝程式會忽略此內容。否則，如果將此內容設定為 1，安裝程式會在作業系統層級停用 SSL 3.0；如果設定為 0，安裝程式不會執行任何動作。	1

必要條件

- 確認已安裝 Horizon Agent。如果您的環境未包含連線伺服器，請從命令列安裝 Horizon Agent，然後指定告知 Horizon Agent 不要登錄至連線伺服器的參數。請參閱為 HTML Access 安裝 Horizon Agent。

程序

1 開啟 Windows 命令提示。

2 藉由命令列選項執行 VADC 外掛程式安裝程式檔案可指定無訊息安裝。可以選擇性地指定其他 MSI 屬性。

下列範例使用預設選項安裝 VADC 外掛程式。

```
VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe /s
```

下列範例安裝 VADC 外掛程式並指定 VADC 將要接聽遠端連線的 TCP 連接埠。

```
VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe /s /v"/qn LISTENPORT=9999"
```

View Agent Direct-Connection 外掛程式進階組態 2

您可以使用預設 View Direct-Connection 外掛程式組態設定，或透過 Windows Active Directory 群組原則物件 (GPO) 或修改特定 Windows 登錄設定來自訂此組態設定。

本章節討論下列主題：

View Agent Direct-Connection 外掛程式組態設定

VMware View Agent 組態 ADMX 範本檔 (`view_agent_direct_connection.admx`) 包含與 View Agent Direct-Connection 外掛程式相關的原則設定。

View Agent Direct-Connection 組態設定位於群組原則管理編輯器的**電腦組態 > 系統管理範本 > VMware View Agent 組態 > View Agent Direct-Connection 組態**。

表 2-1. View Agent Direct-Connection 外掛程式組態設定

設定	說明
應用程式已啟用	此設定支援遠端桌面工作階段主機上的應用程式啟動。預設設定為已啟用。
用戶端設定名稱值組	傳遞給用戶端的值清單，使用「名稱=值」的格式。範例：clientCredentialCacheTimeout=1440。
用戶端工作階段逾時	若未連線用戶端，工作階段可維持使用中的最長時間 (以秒為單位)。預設值為 36000 秒 (10 小時)。
用戶端設定：AlwaysConnect	可將值設為 TRUE 或 FALSE。AlwaysConnect 設定會傳送至 Horizon Client。如果將此原則設為 TRUE，則該原則會覆寫所有儲存的用戶端喜好設定。預設沒有設定任何值。啟用此原則會將值設為 TRUE。停用此原則會將值設為 FALSE。
用戶端設定: AutoConnect	此設定會覆寫任何儲存的 Horizon Client 喜好設定。預設沒有設定任何值。啟用此原則會將值設為 true，停用此原則會將值設為 false。

表 2-1. View Agent Direct-Connection 外掛程式組態設定 (續)

設定	說明
用戶端設定: ScreenSize	傳送到 Horizon Client 的 ScreenSize 設定。如果已啟用，則它會覆寫任何儲存的用戶端喜好設定。如果未設定或已停用，則會使用用戶端喜好設定。
多媒體重新導向 (MMR) 已啟用	決定是否啟用用戶端系統的 MMR。MMR 是一種 Microsoft DirectShow 篩選器，會將 Horizon 桌面平台上特定轉碼器中的多媒體資料直接透過 TCP 通訊端轉送給用戶端系統。然後，當播放時，該資料會在用戶端系統上直接解碼。預設值為停用。 如果用戶端系統的視訊顯示硬體沒有重疊支援，則 MMR 無法正確運作。用戶端系統的資源可能不足以處理本機多媒體解碼。
重設已啟用	可將值設為 TRUE 或 FALSE。設定為 TRUE 時，已驗證的 Horizon Client 可以執行作業系統層級的重新開機作業。預設設定為已停用 (FALSE)。
工作階段逾時	使用 Horizon Client 登入後，使用者可保持工作階段為開啟狀態的時段。此值以分鐘為單位設定，預設值為 600 分鐘。達到此逾時後，會中斷連線所有的使用者桌面平台和應用程式工作階段。
USB 自動連線	可將值設為 TRUE 或 FALSE。插入 USB 裝置時將其連線至桌面平台。如果已設定此原則，則它會複寫所有儲存的用戶端喜好設定。預設沒有設定任何值。
USB 已啟用	可將值設為 TRUE 或 FALSE。決定桌面平台是否可以使用連線至用戶端系統的 USB 裝置。預設值已啟用。基於安全理由，為避免使用外接裝置，請將設定變更為「已停用」(FALSE)。
使用者閒置逾時	如果此時段的 Horizon Client 上不存在任何使用者活動，則會中斷連線使用者的桌面平台和應用程式工作階段。此值以秒為單位設定。預設值為 900 秒 (15 分鐘)。

驗證設定

驗證設定位於群組原則管理編輯器的**電腦設定 > 系統管理範本 > VMware View Agent 組態 > View Agent Direct-Connection 組態**。在此資料夾內的是「以目前使用者身分登入」設定。

表 2-2. View Agent Direct-Connection 外掛程式驗證設定

設定	說明
允許舊版用戶端	停用時，早於 5.5 版的 Horizon Client 版本將不會使用「以目前使用者身分登入」功能進行驗證。如果未進行此設定，則支援舊版用戶端。
允許 NTLM 後援	啟用時，如果無法存取網域控制站，則 Horizon Client 會使用 NTLM 驗證而非 Kerberos。如果未進行此設定，則不允許 NTLM 後援。
需要通道繫結	啟用時，通道繫結會額外提供一層安全防護層來保護 NTLM 驗證。早於 5.5 版的 Horizon Client 版本不支援通道繫結。
用戶端認證快取逾時	Horizon Client 允許使用者使用儲存的密碼的時段 (以分鐘為單位)。0 表示從不，而 -1 表示永久。Horizon Client 可讓使用者選擇在此設定設為有效值時，儲存其密碼。預設為 0 (從不)。
免責聲明已啟用	可將值設為 TRUE 或 FALSE。如果設為 TRUE，則會顯示登入時使用者接受的免責聲明文字。如果已寫入文字，則會顯示「免責聲明文字」或 GPO `Configuration\Windows Settings\Security Settings\Local Policies\Security Options: Interactive logon`。disclaimerEnabled 的預設設定為 FALSE。
免責聲明文字	登入時向 Horizon Client 使用者顯示的免責聲明文字。「免責聲明已啟用」原則必須設為 TRUE。如果未指定文字，則預設為使用 Windows 原則 `Configuration\Windows Settings\Security Settings\Local Policies\Security Options` 中的值。

表 2-2. View Agent Direct-Connection 外掛程式驗證設定 (續)

設定	說明
X509 憑證驗證	決定是否停用、允許或需要智慧卡 X.509 憑證驗證。
X509 SSL 憑證驗證已啟用	決定是否從 Horizon Client 透過直接 SSL 連線啟用智慧卡 X.509 憑證驗證。如果透過中繼 SSL 終止點處理 X.509 憑證驗證，則不需要此選項。變更此設定需要重新啟動 Horizon Agent。

通訊協定和網路設定

通訊協定和網路設定位於群組原則管理編輯器的**電腦設定 > 系統管理範本 > VMware View Agent 組態 > View Agent Direct-Connection 組態**。

表 2-3. View Agent Direct-Connection 外掛程式組態設定

設定	說明
預設通訊協定	Horizon Client 用來連線至桌面平台的預設顯示通訊協定。如果未設定值，則預設值為 BLAST。
外部 Blast 連接埠	傳送給 Horizon Client 的連接埠號碼，做為用於 HTML5/Blast 通訊協定的目的地 TCP 連接埠號碼。數字前的 + 字元表示用於 HTTPS 之連接埠號碼中的相對數字。如果在外部公開的連接埠號碼與服務正在接聽的連接埠不相符，則只會設定此值。通常，此連接埠號碼處於 NAT 環境。預設沒有設定任何值。
外部 Framework 通道連接埠	傳送給 Horizon Client 的連接埠號碼，做為用於 Framework 通道通訊協定的目的地 TCP 連接埠號碼。數字前的 + 字元表示用於 HTTPS 之連接埠號碼中的相對數字。如果在外部公開的連接埠號碼與服務正在接聽的連接埠不相符，則只會設定此值。通常，此連接埠號碼處於 NAT 環境。預設沒有設定任何值。
外部 IP 位址	傳送給 Horizon Client 的 IPV4 位址，做為用於次要通訊協定 (RDP、PCoIP、Framework 通道等) 的目的地 IP 位址。如果在外部公開的位址與桌面平台機器的位址不相符，則只會設定此值。通常，此位址處於 NAT 環境。預設沒有設定任何值。
外部 PCoIP 連接埠	傳送給 Horizon Client 的連接埠號碼，做為用於 PCoIP 通訊協定的目的地 TCP/UDP 連接埠號碼。數字前的 + 字元表示用於 HTTPS 之連接埠號碼中的相對數字。如果在外部公開的連接埠號碼與服務正在接聽的連接埠不相符，則只會設定此值。通常，此連接埠號碼處於 NAT 環境。預設沒有設定任何值。
外部 RDP 連接埠	傳送給 Horizon Client 的連接埠號碼，做為用於 RDP 通訊協定的目的地 TCP 連接埠號碼。數字前的 + 字元表示用於 HTTPS 之連接埠號碼中的相對數字。如果在外部公開的連接埠號碼與服務正在接聽的連接埠不相符，則只會設定此值。通常，此連接埠號碼處於 NAT 環境。預設沒有設定任何值。
HTTPS 連接埠號碼	外掛程式接聽來自 Horizon Client 的傳入 HTTPS 要求的 TCP 連接埠。如果此值已變更，則必須對 Windows 防火牆進行對應的變更，以允許傳入流量。預設值為 443。

外部連接埠號碼和外部 IP 位址值用於網路位址轉譯 (NAT) 和連接埠對應支援。如需詳細資訊，請參閱使用網路位址轉譯和連接埠對應。

對於智慧卡驗證，簽署智慧卡憑證的憑證授權機構 (CA) 必須位於 Windows 憑證存放區中。如需如何新增憑證授權機構的相關資訊，請參閱將憑證授權機構新增至 Windows 憑證存放區。

備註 如果使用者嘗試使用智慧卡登入 Windows 7 或 Windows Server 2008 R2 機器且智慧卡憑證已由中繼 CA 簽署，則嘗試可能會失敗，因為 Windows 會向用戶端傳送不含中繼 CA 名稱的受信任的簽發者清單。如果發生這種情況，用戶端將無法選取適當的智慧卡憑證。若要避免此問題，請在登錄機碼 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL` 中將登錄值 `SendTrustedIssuerList` (REG_DWORD) 設定為 0。將此登錄值設定為 0 後，Windows 不會向用戶端傳送受信任的簽發者清單，因此，便可透過智慧卡選取所有有效憑證。

在 SSL/TLS 中停用弱加密方式

若要有更高的安全性，您可以設定網域原則 GPO (群組原則物件)，以確保 Horizon Client 與虛擬機器型桌面平台或 RDS 主機之間使用 SSL/TLS 的通訊不會允許弱加密。

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 VADC 機器，使新的群組原則生效。

結果

備註 如果 Horizon Client 未設定為支援任何受虛擬桌面平台作業系統支援的密碼，TLS/SSL 交涉將會失敗，並且用戶端將無法連線。

如需設定 Horizon Client 中支援之加密套件的相關資訊，請參閱 Horizon Client 文件，網址為 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html。

取代預設自我簽署 TLS 伺服器憑證

自我簽署的 TLS 伺服器憑證無法為 Horizon Client 提供足夠的保護，來抵禦遭竄改和竊聽的威脅。若要保護桌面平台免受這些威脅，必須取代這些產生的自我簽署憑證。

安裝後，View Agent Direct-Connection 外掛程式首次啟動時，會自動產生自我簽署的 TLS 伺服器憑證，並將其置於 Windows 憑證存放區。TLS 通訊協定交涉期間，會向 Horizon Client 呈現 TLS 伺服器憑證，以便向用戶端提供此桌面平台的相關資訊。此預設自我簽署的 TLS 伺服器憑證無法提供有關此桌面平台的保證，除非該憑證由用戶端信任的憑證授權機構 (CA) 所簽署的憑證取代，並已通過 Horizon Client 憑證檢查的完全驗證。

將此憑證儲存於 Windows 憑證存放區的程序，以及將此憑證取代為適當 CA 簽署之憑證的程序，皆與連線伺服器所使用的程序相同。如需此憑證取代程序的詳細資料，請參閱《Horizon 安裝》文件中的〈設定 Horizon Server 的 TLS 憑證〉。

支援具有主體別名 (SAN) 的憑證和萬用字元憑證。

備註 若要使用 View Agent Direct-Connection 外掛程式，將 CA 簽署的 TLS 伺服器憑證散佈給大量桌面平台，請使用 Active Directory Enrollment 將憑證散佈給每個虛擬機器。

授與 Horizon Client 存取桌面平台和應用程式的權限

可讓使用者直接存取桌面平台和應用程式的授權機制會在稱為 **View Agent Direct-Connection 使用者**的本機作業系統群組中受到控制。

如果使用者為此群組的成員，則該使用者具有連線至虛擬機器型桌面平台、已發佈的桌面平台或已發佈應用程式的權限。首次安裝外掛程式時，會建立此本機群組，且該群組包含「已驗證的使用者」群組。由外掛程式成功驗證的所有使用者均具有存取桌面平台或應用程式的權限。

若要限制對此桌面平台或 RDS 主機的存取，您可以修改此群組的成員資格，以指定使用者和使用者群組清單。這些使用者可以是本機或網域使用者及使用者群組。如果使用者不在此群組中，則驗證後使用者會收到一則訊息，指出使用者無權存取此虛擬機器型桌面平台或此 RDS 主機上主控的已發佈桌面平台和應用程式。

使用網路位址轉譯和連接埠對應

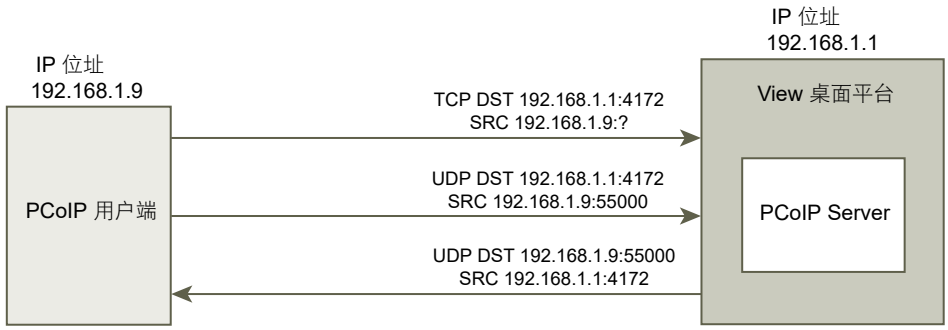
如果 Horizon Client 連線至不同網路上的虛擬機器型桌面平台，則需要網路位址轉譯 (NAT) 和連接埠對應組態。

在此處所示的範例中，您必須在桌面平台上設定外部定址資訊，以便 Horizon Client 可以透過 NAT 或者連接埠對應裝置來使用該資訊連線至桌面平台。該 URL 與連線伺服器上的外部 URL 和 PCoIP 外部 URL 設定相同。

當 Horizon Client 位於不同的網路上且 NAT 裝置在 Horizon Client 與執行外掛程式的桌面平台之間時，需要 NAT 或者連接埠對應組態。例如，如果在 Horizon Client 與桌面平台之間存在防火牆，則防火牆會用作 NAT 或者連接埠對應裝置。

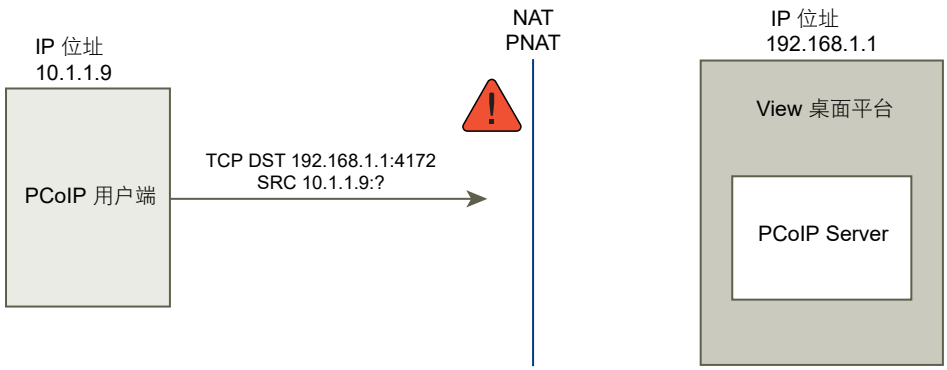
IP 位址為 192.168.1.1 的桌面平台部署範例說明 NAT 與連接埠對應的組態。在相同網路上 IP 位址為 192.168.1.9 的 Horizon Client 系統透過使用 TCP 與 UDP 建立 PCoIP 連線。該連線為直接連接，不具有任何 NAT 或連接埠對應組態。

圖 2-1. 相同網路上用戶端的直接 PCoIP



如果您在用戶端與桌面平台之間新增 NAT 裝置，以便它們在不同位址空間中作業，並且不對外掛程式做出任何組態變更，則 PCoIP 封包將無法正確地路由傳送，並且會失敗。在此範例中，用戶端使用不同的位址空間，且具有 10.1.1.9 的 IP 位址。此安裝程式會失敗，因為用戶端將會使用桌面平台的位址來傳送 TCP 和 UDP Pcoip 封包。目的地位址 192.168.1.1 將無法從用戶端網路運作，並且可能會導致用戶端顯示空白畫面。

圖 2-2. 透過 NAT 裝置的用戶端 PCoIP 顯示失敗

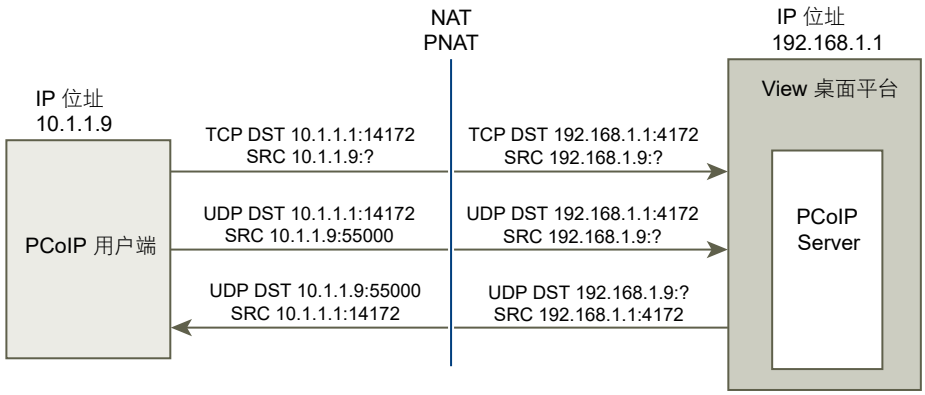


若要解決該問題，您必須將外掛程式設定為使用外部 IP 位址。如果針對該桌面平台將 `externalIPAddress` 設定為 10.1.1.1，則當桌面平台通訊協定連線至桌面平台時，外掛程式會為用戶端提供 IP 位址 10.1.1.1。對於 PCoIP，必須針對此設定在桌面平台上啟動 PCoIP 安全閘道服務。

對於連接埠對應，當桌面平台使用標準 PCoIP 連接埠 4172，而用戶端必須使用其他目的地連接埠 (在連接埠對應裝置上對應至連接埠 4172) 時，您必須針對此設定來設定外掛程式。如果連接埠對應裝置對應連接埠 14172 至 4172，則用戶端必須對 PCoIP 使用目的地連接埠 14172。您必須對 PCoIP 設定此設定。在外掛程式中，將 `externalPCoIPPort` 設定為 14172。

在使用 NAT 與連接埠對應的組態中，`externalIPAdress` 設定為 10.1.1.1 (此為轉譯為 192.168.1.1 的網路)，`externalPColPPort` 設定為 14172 (此為對應至 4172 的連接埠)。

圖 2-3. 透過 NAT 裝置和連接埠對應的用戶端 PCoIP



對於 PCoIP 的外部 PCoIP TCP/UDP 連接埠組態，如果 RDP 連接埠 (3389) 或架構通道連接埠 (32111) 為連接埠對應，您必須設定 `externalRDPPort` 和 `externalFrameworkChannelPort` 來指定 TCP 連接埠號碼，用戶端將使用此號碼透過連接埠對應裝置實現連線。

進階定址配置

將虛擬機器型桌面平台設定為可透過同一外部 IP 位址上的 NAT 和連接埠對應裝置存取時，您必須為每個桌面平台提供一組唯一的連接埠號碼。然後，用戶端可使用相同的目的地 IP 位址，但針對 HTTPS 連線使用唯一的 TCP 連接埠號碼，以直接連線到特定虛擬桌面平台。

例如，HTTPS 連接埠 1000 指向一個桌面平台，而 HTTPS 連接埠 1005 指向另一個桌面平台，兩者使用相同的目的地 IP 位址。在此情況下，為桌面平台通訊協定連線的每個桌面平台設定唯一的外部連接埠號碼過於複雜。因此，外掛程式設定 `externalPCoIPPort`、`externalRDPPort` 及 `externalFrameworkChannelPort` 可以選擇性地執行關聯運算式 (而非靜態值)，以定義相對於用戶端所使用的基礎 HTTPS 連接埠號碼的連接埠號碼。

如果連接埠對應裝置針對 HTTPS 使用連接埠號碼 1000，則對應至 TCP 443；針對 RDP 的連接埠號碼 1001 對應至 TCP 3389；針對 PCoIP 的連接埠號碼 1002 對應至 TCP 和 UDP 4172；以及針對架構通道的連接埠號碼 1003 對應至 TCP 32111，若要簡化組態，可將外部連接埠號碼設定為 `externalRDPPort=+1`、`externalPCoIPPort=+2` 與 `externalFrameworkChannelPort=+3`。在 HTTPS 連線來自使用 HTTPS 目的地連接埠號碼為 1000 的用戶端時，會相對於此連接埠號碼 1000 自動計算外部連接埠號碼，並且分別使用 1001、1002 和 1003。

若要部署其他虛擬桌面平台，如果連接埠對應裝置針對 HTTPS 使用連接埠號碼 1005，則對應至 TCP 443；針對 RDP 使用的連接埠號碼 1006 對應至 TCP 3389；針對 PCoIP 使用的連接埠號碼 1007 對應至 TCP 和 UDP 4172；以及針對架構通道的連接埠號碼 1008 對應至 TCP 32111，並且桌面平台 (+1、+2、+3 等) 上的外部連接埠組態完全相同，在 HTTPS 連線來自使用 HTTPS 目的地連接埠號碼為 1005 的用戶端時，會相對於此連接埠號碼 1005 自動計算外部連接埠號碼，並且分別使用 1006、1007 和 1008。

此配置可讓所有桌面平台進行相同的設定，並共用同一外部 IP 位址。針對基礎 HTTPS 連接埠號碼以 5 遞增來配置連接埠號碼 (1000、1005、1010 ...)，可在同一 IP 位址上存取超過 12,000 個虛擬桌面平台。基礎連接埠號碼用於根據連接埠對應裝置組態，決定要將連線路由到的虛擬桌面平台。針對所有虛擬桌面平台上設定的 `externalIPAddress`=10.20.30.40、`externalRDPPort`=+1、`externalPCoIPPort`=+2 及 `externalFrameworkChannelPort`=+3，虛擬桌面平台的對應與 NAT 和連接埠對應資料表中所述相同。

表 2-4. NAT 和連接埠對應值

虛擬機器數目	桌面平台 IP 位址	HTTPS	RDP	PCOIP (TCP 和 UDP)	架構通道
0	192.168.0.0	10.20.30.40:1000 -> 192.168.0.0:443	10.20.30.40:1001 -> 192.168.0.0:3389	10.20.30.40:1002 -> 192.168.0.0:4172	10.20.30.40:1003 -> 192.168.0.0:32111
1	192.168.0.1	10.20.30.40:1005 -> 192.168.0.1:443	10.20.30.40:1006 -> 192.168.0.1:3389	10.20.30.40:1007 -> 192.168.0.1:4172	10.20.30.40:1008 -> 192.168.0.1:32111
2	192.168.0.2	10.20.30.40:1010 -> 192.168.0.2:443	10.20.30.40:1011 -> 192.168.0.2:3389	10.20.30.40:1012 -> 192.168.0.2:4172	10.20.30.40:1013 -> 192.168.0.2:32111
3	192.168.0.3	10.20.30.40:1015 -> 192.168.0.3:443	10.20.30.40:1016 -> 192.168.0.3:3389	10.20.30.40:1017 -> 192.168.0.3:4172	10.20.30.40:1018 -> 192.168.0.3:32111

在此範例中，Horizon Client 連線到 IP 位址 10.20.30.40，HTTPS 目的地連接埠號碼為 (1000 + *n* * 5)，其中 *n* 是桌面平台號碼。若要連線到桌面平台 3，用戶端會連線到 10.20.30.40:1015。此定址配置可明顯簡化每個桌面平台的組態設定。所有桌面平台均設定為相同的外部位址和連接埠組態。NAT 和連接埠對應設定是透過此一致模式在 NAT 和連接埠對應裝置中執行的，並且所有桌面平台均可在單一的公用 IP 位址上進行存取。通常，用戶端會使用解析至此 IP 位址的單一公用 DNS 名稱。

將憑證授權機構新增至 Windows 憑證存放區

對於智慧卡驗證，簽署智慧卡憑證的憑證授權機構 (CA) 必須存在於 Windows 憑證存放區中。如果不存在，您可以將 CA 新增至 Windows 憑證存放區。

必要條件

確認 Microsoft Management Console (MMC) 具有憑證嵌入式管理單元。請參閱《Horizon 安裝》文件中的〈將憑證嵌入式管理單元新增到 MMC 中〉。

程序

1 啟動 MMC。

2 在 MMC 主控台中，展開**憑證 (本機電腦)** 節點，並移至**信任的根憑證授權機構 > 憑證**資料夾。

如果根憑證存在，而且憑證鏈結中沒有任何中繼憑證，請結束 MMC。

3 以滑鼠右鍵按一下**信任的根憑證授權機構 > 憑證**資料夾，然後按一下**所有工作 > 匯入**。

4 在**憑證匯入**精靈中，按**下一步**並瀏覽至儲存根 CA 憑證所在的位置。

5 選取根 CA 憑證檔案，然後按一下**開啟**。

6 依序按**下一步**、**下一步**，然後按一下**完成**。

7 如果智慧卡憑證是由中繼 CA 所簽署，則匯入憑證鏈結中的所有中繼憑證。

   a 移至**憑證 (本機電腦) > 中繼憑證授權機構 > 憑證**資料夾。

   b 針對每個中繼憑證重複步驟 3 到 6。

設定 HTML Access

3

View Agent Direct-Connection (VADC) 外掛程式支援對虛擬機器型桌面平台和已發佈的桌面平台與應用程式進行 HTML Access。

本章節討論下列主題：

為 HTML Access 安裝 Horizon Agent

若要支援 HTML Access，您必須透過特定參數在虛擬機器型桌面平台上安裝 Horizon Agent。

必要條件

- 從位於 http://www.vmware.com/go/downloadview 的 VMware 下載頁面下載 Horizon Agent 安裝程式檔案。

  安裝程式檔案名稱為 `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`，其中 *YYMM* 是行銷版本號碼，*y.y.y* 是內部版本號碼，而 *xxxxxx* 是組建編號。

程序

- 從命令列安裝 Horizon Agent，並指定告知 Horizon Agent 不要登錄至連線伺服器的參數。

  此範例會安裝 Horizon Agent。

  ```
  VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /v VDM_SKIP_BROKER_REGISTRATION=1
  ```

後續步驟

安裝 View Agent Direct-Connection 外掛程式。請參閱安裝 View Agent Direct-Connection 外掛程式。

設定靜態內容傳遞

如果桌面平台需要服務於 HTML Access 用戶端，則必須在桌面平台上執行一些設定工作。這可讓使用者直接指出桌面平台上的瀏覽器。

必要條件

- 從 VMware 下載頁面 http://www.vmware.com/go/downloadview 下載 Horizon HTML Access `portal.war` zip 檔案。

  檔案名稱為 `VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip`，其中 *y.y.y* 是版本編號，而 *xxxxxx* 是組建編號。

程序

1. 開啟**控制台**。
2. 導覽至**程式和功能 > 開啟或關閉 Windows 功能**。
3. 選取核取方塊 **Internet Information Services**，然後按一下**確定**。
4. 在**控制台**上，導覽至**系統管理工具 > Internet Information Services (IIS) Manager**。
5. 展開左窗格中的項目。
6. 在**預設的網站**上按一下滑鼠右鍵，然後選取**編輯繫結...**。
7. 按一下**新增**。
8. 指定 **https**、**全未指派**和連接埠 **443**。
9. 在 **SSL 憑證**欄位中，選取正確的憑證。

選項	動作
憑證 **vdm** 存在。	選取 **vdm**，然後按一下**確定**。
憑證 **vdm** 不存在。	選取 **vdmdefault**，然後按一下**確定**。

10. 在**網站繫結**對話方塊中，移除 **http 連接埠 80** 的項目，然後按一下**關閉**。
11. 按一下**預設的網站**。
12. 按兩下 **MIME 類型**。
13. 如果**副檔名** .json 不存在，請在**動作**窗格中，按一下**新增...**。否則，請略過下兩個步驟。
14. 針對**副檔名**，輸入 **.json**。
15. 針對 **MIME 類型**，輸入 **text/h323**，然後按一下**確定**。
16. 針對**副檔名**，輸入 **.mem**。
17. 針對 **MIME 類型**，輸入 **text/plain**，然後按一下**確定**。
18. 將 `VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip` 複製到暫存資料夾。

19 解壓縮 VMware-Horizon-View-HTML-Access-*y.y.y-xxxxxx*.zip。

結果是名稱為 portal.war 的檔案。

20 將 portal.war 重新命名為 portal.zip。

21 將 portal.zip 解壓縮到資料夾 C:\inetpub\wwwroot。

如有必要，請調整資料夾的權限，以允許新增檔案。

已建立資料夾 C:\inetpub\wwwroot\portal。

22 開啟**記事本**。

23 使用以下內容 (將 <*桌面平台的 IP 位址或 DNS 名稱*> 取代為桌面平台的實際 IP 位址或 DNS 名稱) 建立檔案 C:\inetpub\wwwroot\Default.htm：

```
<HEAD>
<noscript>
   <meta HTTP-EQUIV="REFRESH" content="0; url=https://<IP address or DNS name of desktop>/portal/
webclient/index.html">
</noscript>
</HEAD>
<script>
   var destination = 'https://<IP address or DNS name of desktop>/portal/webclient/index.html';
   var isSearch = !!window.location.search;
   window.location.href = destination + (isSearch ? window.location.search + '&' : '?') +
'vadc=1' + (window.location.hash || '');
</script>
```

設定信任的 CA 簽署的 TLS 伺服器憑證

您可以設定信任的 CA 簽署的 TLS 伺服器憑證，以確保用戶端與桌面平台間的流量是真實的。

必要條件

- 使用信任的 CA 簽署的 TLS 伺服器憑證取代預設自我簽署的 TLS 伺服器憑證。請參閱 取代預設自我簽署 TLS 伺服器憑證。這會建立一個易記名稱值為 **vdm** 的憑證。
- 如果桌面平台為用戶端的靜態內容服務，請設定靜態內容傳遞。請參閱設定靜態內容傳遞。
- 自行熟悉 Windows 憑證存放區。請參閱《Horizon 安裝》文件中的〈設定連線伺服器以使用新的 TLS 憑證〉。

程序

1 在 Windows 憑證存放區中，導覽至**個人 > 憑證**。

2 按兩下易記名稱為 **vdm** 的憑證。

3 按一下**詳細資料**索引標籤。

4 複製**指紋**值。

5 啟動 Windows 登錄編輯程式。

6 導覽至登錄機碼 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config。

7 新增字串 (REG_SZ) 值 SSLHash 到此登錄機碼。

8 將 SSLHash 值設定為**指紋**值。

停用 Windows 10 和 Windows 2016 桌面平台上的 HTTP/2 通訊協定

使用某些網頁瀏覽器時，可能會在存取 Windows 10 VADC 或 Windows 2016 VADC 桌面平台時遇到錯誤 ERR_SPDY_PROTOCOL_ERROR。您可以透過停用桌面平台上的 HTTP/2 通訊協定來防止這個錯誤。

程序

1 啟動 Windows 登錄編輯程式。

2 導覽至登錄機碼 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters。

3 新增 2 個新 REG_DWORD 值 EnableHttp2Tls 和 EnableHttp2Cleartext 到這個登錄機碼。

4 將兩個值都設為 **0**。

5 將桌面平台重新開機。

在遠端桌面服務主機上設定 View Agent Direct-Connection

4

Horizon 支援遠端桌面服務 (RDS) 主機，該主機提供使用者可從 Horizon Client 存取的已發佈的桌面平台和應用程式。已發佈的桌面平台會透過桌面平台工作階段連線到 RDS 主機。在一般 Horizon 部署中，用戶端會透過 Horizon 連線伺服器連線到桌面平台和應用程式。不過，如果在 RDS 主機上安裝 View Agent Direct-Connection 外掛程式，則用戶端可直接連線至已發佈的桌面平台或應用程式，而無需使用連線伺服器。

本章節討論下列主題：

遠端桌面平台服務主機

遠端桌面平台服務 (RDS) 主機是主控應用程式和桌面平台以進行遠端存取的伺服器電腦。

在 Horizon 部署中，RDS 主機是擁有 Microsoft 遠端桌面服務角色、Microsoft 遠端桌面工作階段主機服務，且已安裝 Horizon Agent 的 Windows 伺服器。如果 RDS 主機也已安裝 VADC 外掛程式，則 RDS 主機可支援 View Agent Direct-Connection (VADC)。如需關於設定 RDS 主機和安裝 Horizon Agent 的相關資訊，請參閱《在 Horizon 中設定已發佈的桌面平台和應用程式》文件中的〈設定遠端桌面服務主機〉。如需安裝 VADC 外掛程式的資訊，請參閱第 1 章 安裝 View Agent Direct-Connection 外掛程式。

備註 當您安裝 Horizon Agent 時，安裝程式會詢問 Horizon Agent 將連線到的連線伺服器的主機名稱或 IP 位址。透過執行含有參數的安裝程式，您可以讓該安裝程式略過此步驟。

```
VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"
```

在設定 RDS 主機和安裝 VADC 外掛程式後，您必須授權 RDS 桌面平台和應用程式。請參閱授權已發佈的桌面平台和應用程式。

授權已發佈的桌面平台和應用程式

您必須先賦予使用者對已發佈桌面平台和應用程式的權利，使用者才能存取這些桌面平台和應用程式。

如果 RDS 主機執行的是 Windows Server 2012 R2，請執行**伺服器管理員**，並導覽至**遠端桌面服務**以設定權利。

桌面平台權利

若要賦予使用者啟動已發佈桌面平台的權利，請執行下列步驟：

- 確定該使用者是本機群組 **View Agent Direct-Connection 使用者**的成員。依預設，所有已驗證的使用者皆為此群組的成員。
- 對於 Windows 2012 R2，請執行**伺服器管理員**，並導覽至**遠端桌面服務**以設定權利。使用快速入門精靈來部署 RDSH 服務。

應用程式權利

若要賦予使用者啟動應用程式的權利，請執行下列步驟：

- 確定該使用者是本機群組 **View Agent Direct-Connection 使用者**的成員。依預設，所有已驗證的使用者皆為此群組的成員。
- 對於 Windows 2012 R2，請執行**伺服器管理員**，並導覽至**遠端桌面服務**以設定權利。

對 View Agent Direct-Connection 外掛程式進行疑難排解

5

當使用 View Agent Direct-Connection 外掛程式時，您可能會遇到已知問題。

當您調查 View Agent Direct-Connection 外掛程式問題時，請確認已安裝並正在執行正確的版本。

如果需要透過 VMware 提出支援問題，請始終啟用完整記錄，重新產生問題，並且產生資料收集工具 (DCT) 記錄組。然後 VMware 技術支援可以分析這些記錄。如需有關產生 DCT 記錄組的詳細資料，請參閱「收集 VMware 的診斷資訊」知識庫文章 (KB)，網址為 http://kb.vmware.com/kb/1017939。

本章節討論下列主題：

安裝的圖形驅動程式不正確

若要讓 PCoIP 正常運作，則必須安裝正確版本的圖形驅動程式。

問題

使用者使用 PCoIP 連線至桌面平台或應用程式時，會顯示黑色螢幕。

原因

錯誤的圖形驅動程式正在執行中。如果在安裝 Horizon Agent 後安裝錯誤版本的 VMware Tools，便會發生此情況。

解決方案

- 重新安裝 Horizon Agent。

視訊 RAM 不足

若要支援 PCoIP，執行桌面平台或 RDS 主機的虛擬機器必須至少具有 128 MB 的視訊 RAM。

問題

使用者使用 PCoIP 連線至桌面平台或應用程式時，會顯示黑色螢幕。

原因

虛擬機器沒有足夠的視訊 RAM。

解決方案

- 為每個虛擬機器至少設定 128 MB 的視訊 RAM。

啟用完整記錄以包含追蹤和偵錯資訊

View Agent Direct-Connection 外掛程式會將記錄項目寫入標準 Horizon Agent 記錄中。依預設，記錄中不包含 TRACE 與 DEBUG 資訊。

問題

Horizon Agent 記錄不包含 TRACE 與 DEBUG 資訊。

原因

未啟用完整記錄。必須啟用完整記錄才會包含 Horizon Agent 中的 TRACE 與 DEBUG 資訊。

解決方案

1. 開啟命令提示並執行 `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat loglevels`
2. 針對完整記錄輸入 **3**。

   除錯記錄檔位於 `%ALLUSERSPROFILE%\VMware\VDM\logs`。檔案 `debug*.log` 具有從 Horizon Agent 和外掛程式的記錄的資訊。搜尋 `wsnm_xmlapi` 以尋找外掛程式的記錄行。

   Horizon Agent 啟動時將記錄外掛程式版本：

   ```
   2012-10-01T12:09:59.078+01:00 INFO (09E4-0C08) <logloaded> [MessageFrameWork] Plugin
   'wsnm_xmlapi - VMware View Agent XML API Handler Plugin' loaded, version=e.x.p build-
   855808, buildtype=release
   ```

   ```
   2012-10-01T12:09:59.078+01:00 TRACE (09E4-06E4) <PluginInitThread> [wsnm_xmlapi] Agent XML
   API Protocol Handler starting
   ```