VMware Horizon View Agent Direct-Connection 外掛程式管理

Horizon View 5.3

View Agent 5.3

本文件支援所列的每個產品版本，並支援後續版本直到新版本的文件取代本文件為止。若要查看本文件的最新版本，請參閱 http://www.vmware.com/support/pubs。

ZH_TW-001290-00

vmware®

您可以在 VMware 網站上找到最新的技術說明文件，網址為:

http://www.vmware.com/support/

VMware 網站還提供了最新的產品更新。

如果您對此文件有何想法，請將您的回應意見提交至：

docfeedback@vmware.com

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

內容

VMware Horizon View Agent Direct-Connection 外掛程式管理

VMware Horizon View Agent Direct-Connection 外掛程式管理 提供關於安裝和設定 VMware Horizon View Agent Direct-Connection 外掛程式 的資訊。此外掛程式是 View Agent 的可安裝 擴充檔，允許 View Client 直接連接到 View 桌面平台，而不需要使用 View 連接伺服器。

在虛擬機器上執行 VMware Horizon View Agent Direct-Connection 外掛程式時，用戶端可直接連接到 虛擬桌面平台。所有 View 桌面平台的功能 PCoIP、HTML5 Access、RDP、USB 重新導向和工作階段管理的作業方式，與使用者透過 View 連接伺服器的作業方式 相同。

使用的 讀者

此資訊的是提供給 想要在 VMware 虛擬桌面平台上安裝、升級或使用 VMware Horizon View Agent Direct-Connection 外掛程式 的任何人。此指南是為熟悉 虛擬機器技術和資料中心作業且具豐富經驗的 Windows 系統管理員而 編寫。

設定和安裝 VMware Horizon View Agent Direct-Connection 外掛程式

1

安裝 Horizon View Agent Direct-Connection 外掛程式包含檢查 View 桌面平台是否符合特定系統需求的程序，然後在虛擬機器上執行外掛程式安裝程式。

本章節討論下列主題:

VMware Horizon View Agent Direct-Connection 外掛程式系統需求

Horizon View Agent Direct-Connection j 外掛程式必須在符合特定軟體需求的 View 虛擬機器上 安裝。

表格 1-1. Horizon View Agent Direct-Connection 外掛程式的 系統需求

vSphere 版本	作業系統版本	軟體
指定 View Agent 版本支援的 任何 vSphere 版本。 **重要事項** 必須在 vSphere 5.x ESXi 主機上管理所有虛擬桌面平台。	指定 View Agent 版本支援的 任何作業系統版本。	■ View Agent 5.3 或 更新版 ■ 您必須在安裝 VMware Tool 後，安裝 Horizon View Agent。

重要事項 為了 PCoIP 的正常運作，必須 為每台 View 虛擬機器設定至少 128MB 的視訊 RAM。

可將虛擬機器加入 Microsoft Active Directory 網域，或成為工作群組的 一員。

安裝 VMware Horizon View Agent Direct-Connection 外掛程式

您必須在執行 View Agent 的 Windows 虛擬機器上安裝 Horizon View Agent Direct-Connection 外掛程式。

先決條件

確認執行支援 View Agent 版本的虛擬機器已設定足夠的視訊 RAM，且在支援的 ESXi 上執行。請參閱 "VMware Horizon View Agent Direct-Connection 外掛程式系統需求," 第 7 頁。

程序

1 以管理員身份登入並啟動作業系統適用的安裝程式。

作業系統	安裝程式
Windows 64 位元	`VMware-viewagent-direct-connection-x86_64-x.y.z-nnnnnn.exe`
Windows 32 位元	`VMware-viewagent-direct-connection-x.y.z-nnnnnn.exe`

安裝程式確認已安裝正確的 Windows 作業系統和 View Agent 版本。

2 您也可選擇在「組態資訊」對話方塊，輸入外掛程式用來接聽 View Client HTTPS 請求的 TCP 通訊埠號碼。

預設的 TCP 連接埠號碼是 443 且在多數情況下不應變更，但是如果需要可在安裝後變更連接埠號碼。

預設會選取**自動設定 Windows 防火牆**核取方塊。此選項會為此 TCP 連接埠新增防火牆規則，允許 View 用戶端的連線。如果 Windows 防火牆正在執行且此規則尚未建立，View Client 將無法連接。

下一個

使用 View Client 存取此虛擬機器，測試是否完整安裝。在 View Client 中不需指定 View 連接伺服器執行個體或安全伺服器的名稱或 IP 位址，您可在執行此外掛程式時，指定 View 桌面平台的名稱或 IP 位址。您可如常進行驗證，而選取和連接桌面平台的使用者體驗與透過 View 連接伺服器連接時相同。

解除安裝 VMware Horizon View Agent Direct-Connection 外掛程式

您可如其他 Windows 應用程式一樣，解除安裝 Horizon View Agent Direct-Connection 外掛程式。

程序

1 前往**控制台 > 程式和功能。**

2 選取 **VMware View Agent Direct-Connection 外掛程式**

3 選取**解除安裝。**

然後會移除 Horizon View Agent Direct-Connection 外掛程式，並重新啟動 View Agent。

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

您可使用 預設 Horizon View Direct-Connection 外掛程式組態設定或 透過 Windows Active Directory 群組原則 (GPO) 自訂，或 使用特定的 Windows 登錄設定。

本章節討論下列主題:

VMware Horizon View Agent Direct-Connection 外掛程式組態設定

全部組態 Horizon View Agent Direct-Connection 外掛程式儲存在 每台 View 桌面平台的本機登錄中。您可透過 本機原則編輯程式或直接修改登錄以使用 Windows Active Directory 群組原則 (GPO)， 管理這些設定。

外掛程式將使用 預設值。但您可變更這些預設值。您可在登錄機碼設定 這些登錄值：

`HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration\XMLAPI`

表格 2-1. Direct-Connection 外掛程式 組態設定

設定	登錄值	類型	描述
HTTPS 連接埠號碼	httpsPortNumber	REG_SZ	外掛程式接聽 View Client HTTPS 請求的 TCP 連接埠。如果變更此值，您必須 在 Windows 防火牆進行相對的變更，允許進行此新的作業。
工作階段逾時	sessionTimeout	REG_SZ	登入 View Client 後，使用者可保持工作階段 開啟的時間。此值以分鐘為單位設定，如果未設定或停用此原則， 則預設值為 600 分鐘。桌面平台 工作階段逾時時，會中止工作階段且會從桌面平台中斷 View Client 的連線。
啟用免責聲明	disclaimerEnabled	REG_SZ	設定值為 `TRUE` 或 `FALSE`。如果設定為 `TRUE`，則登入時會在使用者接受時，顯示 免責聲明文字。如果有編寫，則顯示「免責聲明文字」的文字，或顯示 GPO `Configuration\Windows Settings\Security Settings\Local Policies\Security Options:Interactive logon` 的文字。disclaimerEnabled 的預設設定為 `FALSE`。

表格 2-1. Direct-Connection 外掛程式 組態設定 (繼續)

設定	登錄值	類型	描述
免責聲明文字	disclaimerText	REG_SZ	登入時顯示給 View Client 使用者的 免責聲明文字。「啟用免責聲明」原則必須設定為 TRUE。如果沒有指定文字，則預設會 使用 Windows 原則 Configuration\Windows Settings\Security Settings\Local Policies\Security Options 的文字。
用戶端設定：AlwaysConnect	alwaysConnect	REG_SZ	設定值為 TRUE 或 FALSE。AlwaysConnect 設定會傳送到 View Client。如果此原則設定為 TRUE，會覆寫任何儲存的用戶端偏好設定。 預設不會設定值。啟用此原則會設定值為 TRUE。停用此原則會設定值為 FALSE。
外部 PCoIP 連接埠	externalPCoIPPort	REG_SZ	傳送到 View Client，供 PCoIP 通訊協定使用的目的地 TCP/UDP 連接埠號碼所使用的 連接埠號碼。號碼前的 A + 字元代表 HTTPS 使用連接埠號碼的相對 號碼。僅在對外公開連接埠 號碼與接聽服務的連接埠不相符時，才會設定此值。一般情況下， 此連接埠號碼會在 NAT 環境使用。預設不會設定值。
外部 Blast 連接埠	externalBlastPort	REG_SZ	傳送到 View Client，供 HTML5/Blast 通訊協定使用的目的地 TCP 連接埠號碼所使用的 連接埠號碼。號碼前的 A + 字元代表 HTTPS 使用連接埠號碼的相對 號碼。僅在對外公開連接埠 號碼與接聽服務的連接埠不相符時，才會設定此值。一般情況下， 此連接埠號碼會在 NAT 環境使用。預設不會設定值。
外部 RDP 連接埠	externalRDPPort	REG_SZ	傳送到 View Client，供 RDP 通訊協定使用的目的地 TCP 連接埠號碼所使用的 連接埠號碼。號碼前的 A + 字元 代表 HTTPS 使用連接埠號碼的相對 號碼。僅在對外公開連接埠號碼與接聽服務的連接埠不相符時，才會設定此值。一般情況下，此連接埠號碼會在 NAT 環境使用。預設不會設定值。
外部 IP 位址	externalIPAddress	REG_SZ	傳送到 View Client，供次要通訊協定（RDP、PCoIP、架構通道等）使用的目的地 IP 位址所使用的 IP v4 位址。僅在對外公開 位址與桌面平台機器位址不相符時，才會設定此值。一般情況下，此位址會在 NAT 環境使用。預設不會設定值。
外部架構通道連接埠	externalFrameworkChannelPort	REG_SZ	傳送到 View Client，供架構通道通訊協定使用的目的地 TCP 連接埠號碼所使用的 連接埠號碼。號碼前的 A + 字元代表 HTTPS 使用連接埠號碼的相對 號碼。僅在對外公開連接埠 號碼與接聽服務的連接埠不相符時，才會設定此值。一般情況下，此 連接埠號碼會在 NAT 環境使用。預設不會設定值。
啟用 USB	usbEnabled	REG_SZ	設定值為 TRUE 或 FALSE。決定桌面平台是否可使用連接到用戶端系統的 USB 裝置。預設值為啟用。為了安全起見要避免 使用外部裝置，變更設定為 停用 (FALSE)。
用戶端設定：USB AutoConnect	usbAutoConnect	REG_SZ	設定值為 TRUE 或 FALSE。插入時，連接 USB 裝置到桌面平台。如果設定此原則，則會覆寫任何儲存的用戶端 偏好設定。預設不會設定值。

表格 2-1. Direct-Connection 外掛程式 組態設定 (繼續)

設定	登錄值	類型	描述
啟用重設	resetEnabled	REG_SZ	設定值為 TRUE 或 FALSE。設定為 TRUE 時，驗證的 View 用戶端可執行 作業系統層級的重新開機。預設設定會停用 (FALSE)。
用戶端認證快取逾時	clientCredentialCacheTimeout	REG_SZ	View 用戶端允許使用者 使用儲存密碼的時間（以分鐘計算）。0 代表永不使用，而 -1 代表始終使用。View Client 提供使用者在設定此設定為有效值時，擁有儲存密碼的 選項。預設為 0（永不）。

View Client 設定不會變更 外掛程式的行為。這些設定會傳送到 View Client 進行解譯。

外部通訊埠號碼和 外部 IP 位址值會供「網路位址轉譯 (NAT)」和 通訊埠對應支援使用。如需更多資訊，請參閱 “使用網路位址 轉譯和連接埠對應,” 第 12 頁.

您可使用「本機原則編輯程式」或使用 Active Directory 的「群組原則物件 (GPO)」，設定 覆寫這些登錄設定的原則。原則設定優先於 一般登錄設定。GPO 範本檔案可供設定 原則使用。在預設位置安裝 View Agent 和外掛程式時， 範本檔案的位置如下：

```
C:\Program Files\VMware\VMware View\Agent\extras\view_agent_direct_connection.adm
```

您可匯入此範本 檔案到 Active Directory 或「本機群組原則編輯程式」，以簡化 這些組態設定的管理。請參閱〈Microsoft 原則編輯程式〉和 GPO 處理文件，了解使用此方式管理原則設定的詳細資料。 外掛程式的原則設定儲存在以下登錄機碼：

```
HKEY_LOCAL_MACHINE Software\Policies\VMware, Inc.\VMware VDM\Agent\Configuration\XMLAPI
```

停用 SSL/TLS 的弱密碼

您可使用此 View 桌面平台強化程序，確保使用 SSL/TLS 通訊協定的 View Client 與 View 桌面平台通訊，不允許使用較弱的密碼。

停用弱密碼的組態儲存在 Windows 登錄中。必須在執行 View Agent Direct-Connection 外掛程式的所有桌面平台作業系統上，完成這些設定的變更。

備註 這些設定會影響作業系統上 SSL/TLS 的所有使用。

SSL 3.0 和 TLS 1.0 (RFC2246) 搭配 INTERNET-DRAFT `56-bit Export Cipher Suites For TLS draft-ietf-tls-56-bit-ciphersuites-00.txt` 使用時，可提供使用不同密碼套組的選項。每個密碼套組會決定 SSL/TLS 工作階段中所使用的機碼交換、驗證、加密和 MAC 演算法。

先決條件

您必須擁有使用 `Regedt32.exe` 登錄編輯程式，編輯 Windows 登錄機碼的經驗。

程序

- 啟動「登錄編輯程式」`Regedt32.exe`，並找到此登錄機碼：
  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL`

下一個

表格 2-2. 密碼套組更新

Windows XP SP3	Windows Vista 和更新版
1 在子機碼 `\Ciphers\DES 56/56` 新增 DWORD 值 `Enabled` ，並使用 `0x0` 值。 2 在子機碼 `\Hashes\MD5` 新增 DWORD 值 `Enabled` 並使用 `0x0` 值。 這些更新將可確保在 Windows XP SP3 上僅可使用以下密碼： ■ SSLv3 168 位元 DES-CBC3-SHA ■ SSLv3 128 位元 RC4-SHA ■ TLSv1 168 位元 DES-CBC3-SHA ■ TLSv1 128 位元 RC4-SHA	1 在子機碼 `\Hashes` 建立子機碼 `MD5`。 2 在子機碼 `\Hashes \MD5` 新增 DWORD 值 `Enabled` 並使用 `0x0` 值。 這些更新將可確保在 Windows Vista 和更新版上僅可使用以下密碼： ■ SSLv3 168 位元 DES-CBC3-SHA ■ SSLv3 128 位元 RC4-SHA ■ TLSv1 256 位元 AES256-SHA ■ TLSv1 128 位元 AES128-SHA ■ TLSv1 168 位元 DES-CBC3-SHA ■ TLSv1 128 位元 RC4-SHA

取代預設 自我簽署 SSL 伺服器憑證

自我簽署 SSL 伺服器憑證無法提供 View Client 足夠的防護，以抵禦 竄改和竊用的威脅。要防護您的桌面平台不受到這些 威脅，您必須取代產生的自我簽署憑證。

View Agent Direct-Connection 外掛程式在安裝後第一次啟動時，會 自動產生自我簽署 SSL 伺服器憑證並放置於 Windows 憑證存放區。會在 SSL 通訊協定協商期間提供 View Client SSL 伺服器憑證，以提供用戶端有關此 Vieew 桌面平台的資訊。此預設自我簽署 SSL 伺服器憑證無法 保證此桌面平台的安全，除非使用用戶端信賴的 憑證授權機構 (CA) 簽署且經 View Client 憑證檢查完整驗證的 憑證取而代之。

在 Windows 憑證存放區存放此憑證 的程序以及使用適當 CA 簽署憑證取代的 程序，與 View 連接伺服器（5.1 版或更新）所使用的程序 相同。請參閱 VMware Horizon View 安裝文件中的〈設定 View 伺服器 SSL 憑證〉，了解此憑證取代程序 的詳細資料。

支援使用「主體別名 (SAN)」和「萬用字元名稱 (SAN)」的憑證。

備註 要使用 View Agent Direct-Connection 外掛程式 將 CA 簽署的 SSL 伺服器憑證大量散發至 View 桌面平台，使用「Active Directory 註冊」，散發 憑證到每台虛擬機器。如需詳細資訊，請參閱：http://technet.microsoft.com/en-us/library/cc732625.aspx

授權 View Client 存取 View 桌面平台

允許 View Client 使用者直接存取 View 桌面平台的授權機制會受到本機作業系統內名為 **View Agent 直接連線使用者**的群組所控制。

如果使用者是此群組的成員，則授權該使用者直接連線到桌面平台。先安裝外掛程式時，則會建立此本機群組並內含「已驗證使用者」群組。將授權外掛程式成功驗證的使用者，存取桌面平台。

要限制存取此桌面平台，您可修改此群組的成員，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和使用者群組。如果 View Client 使用者不在此群組中，使用者會在驗證後接收到訊息，說明未授權使用者存取此桌面平台。

使用網路位址 轉譯和連接埠對應

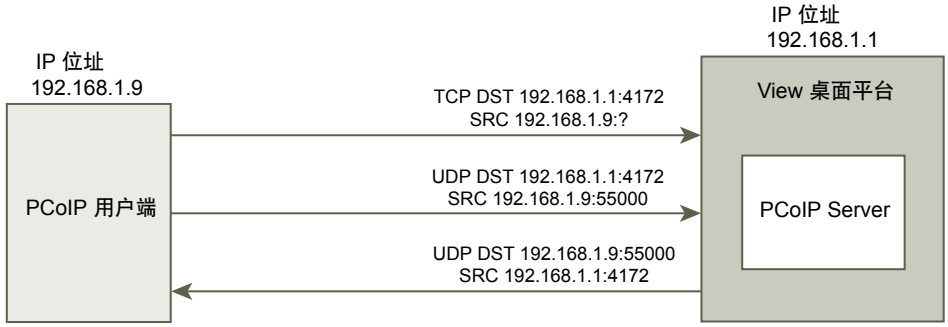
如果 View Client 連接到不同網路的 View 桌面，則需要設定 網路位址轉譯 (NAT) 和連接埠對應。

在這些範例中， 您必須在 View 桌面上設定外部定址資訊，讓 View Client 可使用此資訊，透過 NAT 或連接埠對應裝置連接到 View 桌面。此 URL 與外部 URL 以及 View 連線伺服器和安全伺服器上的 PCoIP 外部 URL 設定相同。

View Client 位於 不同網路且 NAT 裝置介於 View Client 和 View 虛擬 桌面間執行外掛程式時，則必須設定 NAT 或連接埠對應。 舉例來說，如果防火牆介於 View Client 和 View 虛擬桌面間，那麼防火牆就是扮演 NAT 或連接埠對應裝置的角色。

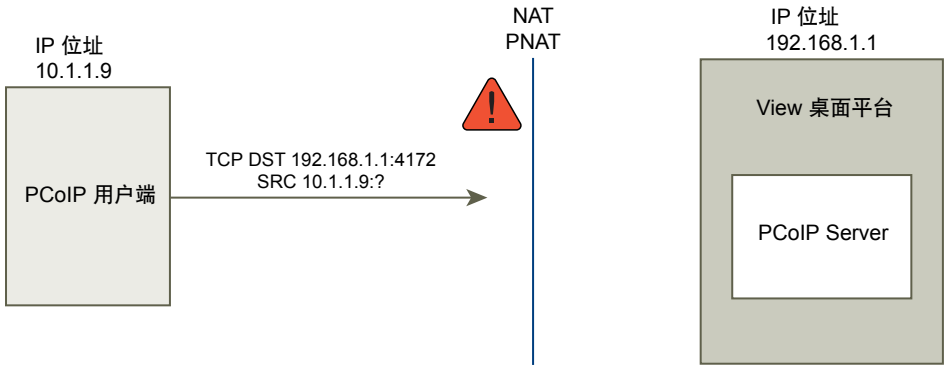
部署 IP 位址為 192.168.1.1 的 View 桌面範例，說明 NAT 和連接埠對應的組態設定。在相同網路上，IP 位址為 192.168.1.9 的 View Client 系統， 使用 TCP 和 UDP 建立 PCoIP 連線。此 為直接連線，不需設定任何 NAT 或連接埠對應組態。

圖 2-1 從相同網路上的用戶端 直接連接 PCoIP



如果您在用戶端和桌面間新增 NAT 裝置，讓 用戶端和桌面在不同的位址空間運作，且沒有 變更任何外掛程式設定，如此一來，將無法正確轉送 PCoIP 封包並導致 失敗。在此範例中，用戶端使用不同的位址空間，且 IP 位址為 10.1.1.9。此設定會失敗是因為用戶端會使用 桌面的位址，來傳送 TCP 和 UDP PCoIP 封包。從用戶端網路，目的地位址 192.168.1.1 將無法正常運作，且可能導致 用戶端顯示空白畫面。

圖 2-2 透過 NAT 裝置，從用戶端連接 PCoIP 顯示失敗訊息

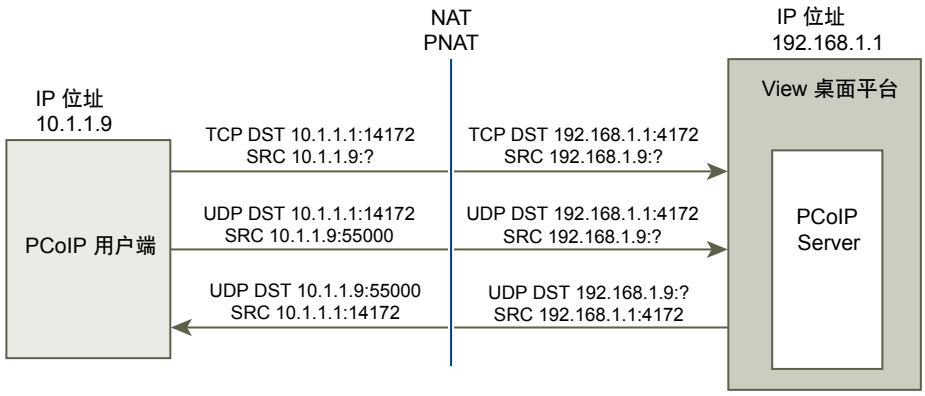


要解決這個問題，您 必須設定外掛程式使用外部 IP 位址。如果將此桌面的 `externalIPAddress` 設定為 10.1.1.1， 從桌面通訊協定連接到桌面時， 外掛程式將提供用戶端 10.1.1.1 的 IP 位址。針對 PCoIP 進行此設定時， 必須在桌面上啟用 PCoIP 安全閘道服務。

針對連接埠對應， 桌面使用標準 PCoIP 連接埠 4172，但用戶端使用不同的 目的地連接埠（該連接埠對應到連接埠對應裝置上的連接埠 4172）時，您必須 針對此設定，設定外掛程式。 如果連接埠對應裝置對應連接埠 14172 到 4172， 用戶端進行 PCoIP 連線時就必須使用目的地連接埠 14172。您必須設定 PCoIP 。將 外掛程式的 `externalPCoIPPort` 設為 14172。

在使用 NAT 和連接埠對應的組態設定中， `externalIPAdress` 設定為 10.1.1.1，網路會將此位址 轉譯為 192.168.1.1，而 `externalPColPPort` 設定為 14172，連接埠對應到 4172。

圖 2-3 透過 NAT 裝置和連接埠對應， 從用戶端連接 PCoIP



針對 PCoIP 的外部 PCoIP TCP/UDP 連接埠組態設定，如果 RDP 連接埠 (3389) 或架構 通道連接埠 (32111) 已進行連接埠對應，您必須設定 `externalRDPPort` 和 `externalFrameworkChannelPort` ，以指定 TCP 連接埠號碼，讓用戶端可 使用這些連接埠號碼，透過連接埠對應裝置進行連線。

進階位址分配計劃

您設定多台 View 桌面平台，以透過相同外部 IP 位址上的 NAT 和連接埠對應裝置存取時，您必須提供每台 View 桌面平台唯一一組連接埠號碼。然後用戶端可在使用相同的目的地 IP 位址時，但 HTTPS 連線使用唯一的 TCP 連接埠號碼將連線導向至特定的虛擬桌面平台。

位址分配計劃範例

在此範例中，HTTPS 連接埠 1000 會導向至一個桌面平台，而 HTTPS 連接埠 1005 會導向到其他桌面平台，但均使用相同目的地 IP 位址。在此案例中，在桌面平台通訊協定連線時為每個 View 桌面平台設定唯一的外部連接埠號碼將會非常複雜。因此，外掛程式設定 `externalPCoIPPort`、`externalRDPPort` 以及 `externalFrameworkChannelPort` 可取用選用的相關運算式而非靜態值，以定應用戶端使用的基本 HTTPS 連接埠號碼相關的連接埠號碼。

如果連接埠對應裝置為 HTTPS 使用連接埠號碼 1000，並對應至 TCP 443；為 RDP 使用連接埠號碼 1001，並對應至 TCP 3389；為 PCoIP 使用連接埠號碼 1002，並對應至 TCP 和 UDP 4172；為架構通道使用連接埠號碼 1003，並對應至 TCP 32111，以簡化組態，則可設定外部連接埠號碼為 `externalRDPPort=+1`, `externalPCoIPPort=+2` 且 `externalFrameworkChannelPort=+3`。使用 HTTPS 目的地連接埠號碼 1000 從用戶端進行 HTTPS 連線時，會相對於此連接埠號碼 1000，自動計算外部連接埠號碼分別為 1001、1002 和 1003。

要部署其他虛擬桌面平台時，如果連接埠對應裝置為 HTTPS 使用連接埠號碼 1005，並對應至 TCP 443；為 RDP 使用連接埠號碼 1006，並對應至 3389；為 PCoIP 使用連接埠號碼 1007，並對應至 TCP 和 UDP 4172；為架構通道使用連接埠號碼 1008，並對應至 TCP 32111 時，在桌面平台（+1、+2、+3 等等）使用完全相同外部連接埠組態的情況下，從使用 HTTPS 目的地連接埠號碼 1005 的用戶端進行 HTTPS 連線時，會相對於此連接埠號碼，自動計算外部連接埠號碼分別為 1006、1007 和 1008。

此計劃允許所有 View 桌面平台使用相同方式設定，且共用相同的外部 IP 位址。以五為增量配置基本 HTTPS 連接埠號碼的連接埠號碼（1000、1005、1010 …）時，將允許存取相同 IP 位址上超過 12,000 個虛擬桌面平台， 並根據連接埠對應裝置組態，使用基本連接埠號碼決定要路由連線的虛擬桌面平台。在所有虛擬桌面平台上設定為 `externalIPAddress=10.20.30.40`、`externalRDPPort=+1`、`externalPCoIPPort=+2` 且 `externalFrameworkChannelPort=+3` 時，會在 NAT 和連接埠對應表描述對應至虛擬桌面平台。

表格 2-3. NAT 和連接埠對應值

VM#	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

View Client 會連線至 IP 位址 10.20.30.40 以及 HTTPS 目的地連接埠號碼（1000 + *n* * 5），而 *n* 是 View 桌面平台號碼。要連接至 View 桌面平台 3，用戶端會連接至 10.20.30.40:1015。此位址分配計劃大幅簡化每台 View 桌面平台的組態設定。會使用相同的外部位址和連接埠組態，設定所有桌面平台。在 NAT 和連接埠對應裝置內，會使用一致的模式完成 NAT 和連接埠對應組態，且可存取單一公開 IP 位址上的所有 View 桌面平台。用戶端通常會使用解析此 IP 位址的單一公開 DNS 名稱。

疑難排解 VMware Horizon View Agent Direct-Connection 外掛程式

3

使用 Horizon View Agent Direct-Connection 外掛程式時，您可能遇到一些已知問題，必須進行疑難排解。

研究 Horizon View Agent Direct-Connection 外掛程式的問題時，請確認安裝且執行的版本正確。在以上範例中，外掛程式版本詳細資料為 `version=e.x.p build-855808, buildtype=release`。記錄的外掛程式名稱是 VMware View Agent XML API Handler Plugin。

如果問題需要請求 VMware 的支援，請始終啟用完整記錄、重新產生問題並產生「資料收集工具 (DCT)」記錄集。VMware 技術支援接著會分析這些記錄。如需產生 DCT 記錄集的詳細資料，請參閱 VMware View KB 文章〈收集診斷資訊〉http://kb.vmware.com/kb/1017939。

啟用完整記錄以包含 TRACE 和 DEBUG 資訊

Horizon View Agent Direct-Connection 外掛程式寫入記錄項目到標準 View Agent 記錄。預設記錄不含 TRACE 和 DEBUG 資訊。

問題

Horizon View Agent Direct-Connection 外掛程式寫入記錄項目到標準 View Agent 記錄。預設標準 View Agent 記錄不含 TRACE 和 DEBUG 資訊。

原因

並未啟用完整記錄。您必須啟用完整記錄，View Agent 記錄才會內含 TRACE 和 DEBUG 資訊。

解決方案

1 開啟指令行並執行 `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat loglevels`

2 輸入 **3** 以啟用完整記錄。

除錯記錄檔案位於 `%ALLUSERSPROFILE%\VMware\VDM\logs`。檔案 `debug*.log` 包含 View Agent 和外掛程式記錄的資訊。搜尋 `wsnm_xmlapi` ，找到外掛程式記錄行。

啟動 View Agent 時，會記錄外掛程式版本：

```
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
```

為虛擬機器設定的視訊 RAM 不足

必須為虛擬機器設定正確的視訊 RAM。

問題

使用 PCoIP 時，顯示黑色畫面。

原因

為虛擬機器設定不足的視訊 RAM 為 16MB 或 32MB。

解決方案

- 請為每台虛擬機器設定至少 128MB 的視訊 RAM。

安裝不正確的 圖形驅動程式

必須安裝正確版的 Horizon View Agent 圖形驅動程式。安裝 Horizon View Agent 後，可能使圖形驅動程式降級。Horizaon View Agent 後安裝 不正確的 VMware Tool 版本，則可能會 發生此問題。

問題

使用 PCoIP 時因為降級的圖形驅動程式，所以 顯示黑色畫面。

原因

安裝不正確的 圖形驅動程式版本。

解決方案

- 重新安裝 Horizon View Agent。

索引