

設定 Horizon 7 for Linux 桌面平台

2019 年 12 月

VMware Horizon 7 7.11



vmware®

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

如果您對於本文件有任何意見，歡迎寄至：

docfeedback@vmware.com

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

Copyright © 2016-2019 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

目錄

設定 Horizon 7 for Linux 桌面平台 6

1 功能和系統需求 7

- HorizonLinux 桌面平台的功能 7
- Horizon7 for Linux 桌面平台的組態步驟概觀 12
- Horizon 7for Linux 的系統需求 13
 - 2D 圖形卡的虛擬機器設定 22
 - 在 Linux 桌面平台上設定工作階段協作 22

2 為桌面平台部署準備 Linux 虛擬機器 25

- 建立虛擬機器和安裝 Linux 25
- 準備用於遠端桌面平台部署的 Linux 機器 26
- 安裝 Horizon Agent 相依性套件 28

3 設定 Linux 桌面平台的 Active Directory 整合 30

- 整合 Linux 與 Active Directory 30
 - 使用 OpenLDAP 伺服器傳遞驗證 31
 - 對 Microsoft Active Directory 設定 SSSD LDAP 驗證 31
 - 使用 Winbind 網域加入解決方案 31
 - 設定 PowerBroker Identity Services Open (PBISO) 驗證 32
 - 設定 Samba 離線網域加入 33
 - 針對 RHEL/CentOS 8.0 使用 Realmd 加入解決方案 34
- 設定 Single Sign-On 36
- 設定智慧卡重新導向 37
 - 設定 RHEL 8.0 桌面平台的智慧卡重新導向 38
 - 設定 RHEL 7.x/6.x 桌面平台的智慧卡重新導向 43
 - 設定 Ubuntu 桌面平台的智慧卡重新導向 48
 - 設定 SLED/SLES 桌面平台的智慧卡重新導向 58
- 設定 True SSO for Linux 桌面平台 64
 - 在 RHEL/CentOS 8.0 桌面平台上設定 True SSO 65
 - 設定 RHEL/CentOS 7.x 桌面平台的 True SSO 67
 - 設定 Ubuntu 桌面平台的 True SSO 70
 - 設定 SLED/SLES 桌面平台的 True SSO 75

4 設定 Linux 桌面平台的圖形卡 79

- 針對 vGPU 設定支援的 Linux 發行版 79
 - 在 ESXi 主機上安裝適用於 NVIDIA GRID vGPU 圖形卡的 VIB 79

- 在 Linux 虛擬機器上針對 vGPU 設定共用 PCI 裝置 81
- 安裝 NVIDIA GRID vGPU 顯示驅動程式 82
- 確認已安裝 NVIDIA 顯示驅動程式 82
- 針對 vDGA 設定 RHEL 6.x 83
 - 在主機上針對 NVIDIA GRID 啟用 DirectPath I/O 83
 - 新增 vDGA 傳遞裝置到 RHEL 6.x 虛擬機器 84
 - 安裝 vDGA 的 NVIDIA 顯示驅動程式 85
 - 確認已安裝 NVIDIA 顯示驅動程式 86

5 安裝 Horizon Agent 88

- 在 Linux 虛擬機器上安裝 Horizon Agent 88
 - install_viewagent.sh 命令列選項 89
- 設定 Linux 代理程式的憑證 91
- 升級 Linux 虛擬機器上的 Horizon Agent 91
 - 升級 Linux 虛擬機器上的 Horizon Agent 92
- 解除安裝 Horizon 7 for Linux 機器 93

6 Linux 桌面平台的組態選項 94

- 在 Linux 桌面平台上設定組態檔中的選項 94
- 使用 智慧原則 102
 - 智慧原則的需求 102
 - 安裝 Dynamic Environment Manager 102
 - 設定 Dynamic Environment Manager 103
 - Horizon 智慧型原則設定 103
 - 將條件新增至 Horizon 智慧型原則定義 103
 - 在 Dynamic Environment Manager 中建立 Horizon 智慧型原則 104
- Linux 桌面平台的 Blast 設定範例 105
- Linux 桌面平台用戶端磁碟機重新導向選項的範例 106

7 建立和管理 Linux 桌面平台集區 107

- 建立 Linux 的手動桌面平台集區 107
- 管理 Linux 桌面平台集區 108
- 為 Linux 建立自動完整複製桌面平台集區 110
- 為 Linux 建立即時複製浮動桌面平台集區 111
- 代理 PowerCLI 命令 114

8 針對手動桌面平台集區大量部署 Horizon 7 117

- Linux 桌面平台大量部署的概觀 117
- Linux 桌面平台大量升級的概觀 119
- 建立用於複製 Linux 桌面平台機器的虛擬機器範本 119
- 用於部署 Linux 桌面平台的範例 PowerCLI 指令碼輸入檔 121

- 用於複製 Linux 虛擬機器的範例指令碼 122
- 將複製的虛擬機器加入 AD 網域的範例指令碼 126
- 使用 SSH 將複製的虛擬機器加入 AD 網域的範例指令碼 128
- 上傳組態檔至 Linux 虛擬機器的範例指令碼 132
- 使用 SSH 上傳組態檔至 Linux 虛擬機器的範例指令碼 135
- 在 Horizon Agent 上升級 Linux 桌面平台機器的範例 PowerCLI 指令碼 140
- 使用 SSH 在 Linux 虛擬機器上升級 Horizon Agent 的範例指令碼 144
- 在 Linux 虛擬機器上執行作業的範例指令碼 150

9 疑難排解 Linux 桌面平台 154

- 在 Horizon Console 中使用 Horizon Help Desk Tool 154
 - 在 Horizon Console 中 啟動 Horizon Help Desk Tool 155
 - 在 Horizon Help Desk Tool 中對使用者進行疑難排解 155
 - Horizon Help Desk Tool 的工作階段詳細資料 157
 - Horizon Help Desk Tool 的工作階段處理程序 160
 - 在 Horizon Help Desk Tool 中疑難排解 Linux 桌面平台工作階段 161
- 收集 Horizon 7 for Linux 機器的診斷資訊 162
- Horizon Agent 無法在 iPad Pro Horizon Client 上中斷連線 162
- SLES 12 SP1 桌面平台不會自動重新整理 162
- SSO 無法連線到關閉電源代理程式 163
- 在建立 Linux 的手動桌面平台集區後無法連線虛擬機器 163

設定 Horizon 7 for Linux 桌面平台

《設定 Horizon 7 for Linux 桌面平台》文件提供設定 Linux 虛擬機器以作為 VMware Horizon[®] 7 for Linux 桌面平台的相關資訊。這些資訊包括準備 Linux 客體作業系統、在虛擬機器上安裝 Horizon Agent，以及在 Horizon Console 中設定機器以便用於 Horizon 7 部署中。

主要對象

本資訊適用對象是想要設定和使用執行於 Linux 客體作業系統的遠端桌面平台的任何使用者。這項資訊是針對具有經驗且熟悉虛擬機器技術和資料中心作業的 Linux 系統管理員所撰寫。

功能和系統需求

1

在 Horizon 6.2.x 或更新版本中，使用者可以連線至執行 Linux 作業系統的遠端桌面平台。

本章節討論下列主題：

- [HorizonLinux 桌面平台的功能](#)
- [Horizon7 for Linux 桌面平台的組態步驟概觀](#)
- [Horizon 7for Linux 的系統需求](#)

HorizonLinux 桌面平台的功能

下列清單顯示 HorizonLinux 桌面平台支援的主要功能。

Linux 桌面平台上支援的功能

Active Directory 整合

執行下列 Linux 發行版的即時複製桌面平台，可以使用 PowerBroker Identity Services Open (PBISO) 執行 Active Directory 的離線網域加入。

- Ubuntu 16.04 和 18.04
- SLED/SLES 12.x

如需詳細資訊，請參閱[整合 Linux 與 Active Directory](#) 中的〈PowerBroker Identity Services Open (PBISO) 驗證〉一節。

執行下列 Linux 發行版的即時複製桌面平台，可以使用 Samba 執行 Active Directory 的離線網域加入。

- Ubuntu 16.04 和 18.04
- RHEL 7.3 和 8.0

Audio-in

支援從用戶端主機到遠端 Linux 桌面平台的音訊輸入重新導向。此功能並非以 USB 重新導向功能為基礎。如果您要啟用此功能，則必須在安裝期間加以選取。您必須在您的應用程式中，選取系統預設音訊輸入裝置

「PulseAudio 伺服器 (本機)」作為音訊輸入。下列 Linux 發行版支援此功能。

- 具有 MATE 或 Gnome Fallback (Metacity) 桌面平台環境的 Ubuntu 16.04 x64
- 具有 MATE 或 Gnome Ubuntu 桌面平台環境的 Ubuntu 18.04 x64
- 具有 KDE 或 Gnome 桌面平台環境的 RHEL 7.x Workstation x64
- 具有 Gnome 桌面平台環境的 RHEL 8.0 Workstation x64
- SLED/SLES 12.x SP3 x64

音訊輸出

支援音訊輸出重新導向。此功能依預設為啟用狀態。若要停用此功能，您必須將 `RemoteDisplay.allowAudio` 選項設為 **false**。使用 Chrome 和 Firefox 瀏覽器存取時，VMware Horizon HTML Access 會為 Linux 桌面平台提供音訊輸出支援。

自動完整複製桌面平台集區

您可以為 Linux 桌面平台建立自動的完整複製桌面平台集區。

用戶端磁碟機重新導向

當您啟用用戶端磁碟機重新導向 (CDR) 功能時，本機系統的共用資料夾和磁碟機將變成可供您存取。您可以使用遠端 Linux 桌面平台上位於主目錄中的 `tsclient` 資料夾。若要使用此功能，您必須安裝 CDR 元件。

剪貼簿重新導向

透過剪貼簿重新導向功能，您可以在用戶端主機與遠端 Linux 桌面平台之間複製並貼上 RTF 文字或純文字。您可以使用 Horizon Agent 選項來設定複製/貼上方向和最大文字大小。此功能依預設為啟用狀態。您可以在安裝期間停用它。

FIPS 140-2 模式

聯邦資訊處理標準 (FIPS) 140-2 模式的支援雖然尚未經過 NIST 密碼編譯模組驗證方案 (CMVP) 驗證，但已適用於 Linux 桌面平台。

Horizon 7 Agent for Linux 會實作專為 FIPS 140-2 符合性所設計的密碼編譯模組。這些模組會在 CMVP 憑證 #2839 和 #2866 所列出的作業環境中加以驗證，並移植到此平台。不過，在 VMware NIST CAVP 和 CMVP 憑證中納入新作業環境的 CAVP 和 CMVP 測試需求仍維持在產品藍圖上完成。

備註 要支援 FIPS 140-2 模式，必須使用傳輸層安全性 (TLS) 通訊協定 1.2 版。

服務台工具

Horizon Help Desk Tool 是可用來對 Linux 桌面平台工作階段進行疑難排解的 Web 應用程式。您可以使用 Horizon Help Desk Tool 來取得 Horizon 7 使用者工作階段的狀態，以及執行疑難排解和維護作業。請參閱在 [Horizon Console](#) 中使用 [Horizon Help Desk Tool](#)。

Horizon 智慧型原則

您可以使用 VMware Dynamic Environment Manager™ 9.4 或更新版本來建立 Horizon 智慧原則，以控制 USB 重新導向、剪貼簿重新導向和用戶端磁

碟機重新導向功能在特定遠端 Linux 桌面平台上的行為。請參閱[使用智慧原則](#)。

H.264 編碼器

H.264 可改善 Horizon 桌面平台的 Blast Extreme 效能，在低頻寬網路下尤其如此。如果用戶端系統停用了 H.264，Blast Extreme 將會自動回復為 JPEG/PNG 編碼。

H.264 編碼器同時包含硬體 H.264 支援和軟體編碼器支援。硬體 H.264 支援有下列需求。

- 使用 NVIDIA 圖形卡設定 vGPU。
- 在 NVIDIA 圖形卡中安裝 NVIDIA 驅動程式 384 系列或更新版本。

系統符合前述需求時，Horizon 7 for Linux 即會使用硬體 H.264 編碼器。否則，會使用軟體 H.264 編碼器。

即時複製浮動桌面平台集區

您可以為 Linux 桌面平台建立即時複製浮動桌面平台集區。僅在已安裝下列 Linux 發行版的系統上才支援使用此功能。

- Ubuntu 16.04 和 18.04
- RHEL 7.1 或更新版本
- RHEL 8.0
- SLED/SLES 12.x

如需詳細資訊，請參閱[為 Linux 建立即時複製浮動桌面平台集區](#)。

K Desktop Environment

下列 Linux 發行版支援 K Desktop Environment (KDE)。

- CentOS 6.x 和 7.x
- RHEL 6.x 和 7.x
- Ubuntu 16.04 和 18.04

鍵盤配置和地區設定同步化

此功能可指定是否將用戶端的系統地區設定和目前的鍵盤配置與 Horizon Linux Agent 桌面平台進行同步化。當此設定已啟用或未設定時，則允許進行同步化。當此設定已停用時，則不允許進行同步化。

僅 Windows 版 VMware Horizon 支援此功能，並且僅適用於英文、法文、德文、日文、韓文、西班牙文、簡體中文和繁體中文地區設定。

無失真 PNG

桌面平台上產生的影像和視訊會在用戶端裝置上以像素精準方式呈現。

手動桌面平台集區

機器來源。

- 受管理的虛擬機器 - vCenter 虛擬機器的機器來源。新部署和升級部署可支援受管理的虛擬機器。

- 未受管理的虛擬機器 - 其他來源的機器來源。只有從未受管理的虛擬機器部署進行升級時，才可支援未受管理的虛擬機器。

備註 為確保能達到最佳效能，請勿使用未受管理的虛擬機器。

MATE 桌面平台環境

下列 Linux 發行版支援 MATE 桌面平台環境。

- Ubuntu 16.04
- Ubuntu 18.04

多台監視器

- vDGA/vGPU 桌面平台可在四台監視器上支援最大解析度 2560x1600。
- VMware vSphere® 6.0 或更新版本上的 2D 桌面平台在四台監視器上最高可支援 2048x1536 的解析度，在三台監視器上最高可支援 2560x1600 的解析度。

對於 Ubuntu 16.04 和 18.04，您必須使用 Gnome、KDE 或 MATE 桌面平台環境才能使用多台監視器功能。如需詳細資訊，請參閱 <http://kb.vmware.com/kb/2151294>。

針對 SLES 12 SP1，您必須使用核心層級為 kernel-default-3.12.49-11.1 的預設套件。如果您已升級套件，則多台監視器功能會失敗，而桌面平台會顯示在一台監視器中。

從 VMware HorizonHTML Access™ 5.0 版開始，Horizon 7 for Linux 桌面平台已可支援多台監視器功能。

VMware Blast 的網路智慧支援

VMware Blast 支援網路智慧傳輸。此功能依預設為啟用狀態。

啟用使用者資料包通訊協定 (UDP) 時，Blast 會建立傳輸控制通訊協定 (TCP) 和 UDP 連線。Blast 會根據目前的網路狀況，動態地選取其中一個用於傳輸資料的傳輸，以提供最佳的使用者體驗。例如，在區域網路中，TCP 的效能優於 UDP，因此 Blast 會選取 TCP 來傳輸資料。同樣地，在廣域網路 (WAN) 中，UDP 的效能優於 TCP，因此 Blast 會該環境中選取 UDP 傳輸。

如果使用的其中一個內嵌元件不支援 UDP，則 Blast 僅會建立 TCP 連線。例如，如果您的連線使用 Horizon 連線伺服器或安全伺服器的 Blast 安全閘道元件，則僅會建立 TCP 連線。即使用戶端和代理程式皆啟用 UDP，連線仍會使用 TCP，因為 Blast 安全閘道不支援 UDP。如果使用者從公司網路外部連線，UDP 元件將需要支援 UDP 的 VMware Unified Access Gateway (舊稱為 Access Point)。

請使用下列資訊建立以 UDP 為基礎的 Blast 連線。

- 如果用戶端直接連線至 Linux 桌面平台，請同時在用戶端和代理程式中啟用 UDP。依預設會同時在用戶端和代理程式中啟用 UDP。

- 如果用戶端使用 **Unified Access Gateway** 連線至 **Linux** 桌面平台，請在用戶端、代理程式和 **Unified Access Gateway** 中啟用 UDP。

工作階段協作

透過工作階段協作功能，使用者可以邀請其他使用者加入現有的遠端 **Linux** 桌面平台工作階段，也可以在收到其他使用者的邀請時加入協作工作階段。僅在已安裝下列 **Linux** 發行版的遠端 **Linux** 桌面平台上才支援使用此功能。

- 具有 **Gnome** 桌面平台環境的 **Ubuntu 18.04**
- 具有 **Gnome Classic** 桌面平台環境的 **RHEL 7.5** 或更新版本
- 具有 **Gnome Classic** 桌面平台環境的 **RHEL 8.0**

Single Sign-on

下列 **Linux** 發行版支援 **Single Sign-On (SSO)**。

- **RHEL 8.0/7.x/6.x Workstation x64**
- **CentOS 8.0/7.x/6.x x64**
- **SLED/SLES 12.x SP3/SP2/SP1**
- **Ubuntu 18.04/16.04 x64**

智慧卡重新導向

下列 **Linux** 發行版支援智慧卡重新導向。

- **RHEL 8.0**
- **RHEL 7.1 及更新版本**
- **RHEL 6.6 及更新版本**
- **Ubuntu 18.04/16.04**
- **SLED/SLES 12.x SP3**

此功能支援個人身分驗證 (PIV) 卡和通用存取卡 (CAC)。如需詳細資訊，請參閱[設定智慧卡重新導向](#)。

True SSO 支援

下列 **Linux** 發行版支援 **True SSO**。

- **RHEL 7.x/8.0**
- **CentOS 7.x/8.0**
- **SLED/SLES 12.x SP3**
- **Ubuntu 18.04/16.04**

如需詳細資訊，請參閱[設定 True SSO for Linux 桌面平台](#)。

USB 重新導向

USB 重新導向功能可讓您從遠端 **Linux** 桌面平台存取本機連結的 **USB** 裝置。若要使用 **USB** 功能，您必須安裝 **USB** 重新導向元件和 **USB VHCI** 驅動程式核心模組。確保您有足夠權限可使用所要重新導向的 **USB** 裝置。

3Dconnexion 滑鼠

若要開始使用 3Dconnexion 滑鼠，您必須在 Linux 桌面平台上安裝適當的裝置驅動程式，並使用 [連線 USB 裝置] 功能表為滑鼠配對。

3D 圖形

3D 圖形功能支援下列 Linux 版本和圖形卡的組合：

- 搭載 NVIDIA GRID K1 或 K2 圖形卡的 RHEL 6.x Workstation x64 支援 vDGA。
- <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html> 上列出的 Linux 發行版和 NVIDIA 圖形卡支援 vGPU。

Linux 桌面平台和桌面平台集區的限制

Linux 桌面平台和桌面平台集區具有下列限制：

- 不支援虛擬列印、依據位置列印和即時視訊。
- 不支援 VMware HTML Access 檔案傳輸功能。

備註 使用安全伺服器時，必須在內部防火牆中開放連接埠 22443，才能在安全伺服器和 Linux 桌面平台之間允許流量。

Horizon7 for Linux 桌面平台的組態步驟概觀

依據虛擬機器上安裝的是 2D 圖形或 3D 圖形，當您安裝和設定 Horizon7 for Linux 桌面平台時，您必須執行不同順序的步驟。

2D 圖形 - 組態步驟概觀

對於 2D 圖形，執行下列步驟：

- 1 檢閱設定 Horizon7 for Linux 部署的系統需求。請參閱 [Horizon 7for Linux 的系統需求](#)。
- 2 在 vSphere 中建立虛擬機器並安裝 Linux 作業系統。請參閱[建立虛擬機器和安裝 Linux](#)。
- 3 為部署為 Horizon7 環境的桌面平台準備客體作業系統。請參閱[準備用於遠端桌面平台部署的 Linux 機器](#)。
- 4 設定 Linux 客體作業系統以 Active Directory 驗證。此步驟會根據您的環境需求以第三方軟體實作。如需詳細資訊，請參閱[整合 Linux 與 Active Directory](#)。
- 5 在 Linux 虛擬機器上安裝 Horizon Agent。請參閱在 [Linux 虛擬機器上安裝 Horizon Agent](#)。
- 6 建立包含已設定 Linux 虛擬機器的桌面平台集區。請參閱[建立 Linux 的手動桌面平台集區](#)。

3D 圖形 - 組態步驟概觀

您必須先在 Linux 虛擬機器上完成 NVIDIA GRID vGPU 或 vDGA 組態，才可在機器上安裝 Horizon Agent 並且在 Horizon Console 中部署桌面平台集區。

- 1 檢閱設定 Horizon7 for Linux 部署的系統需求。請參閱 [Horizon 7for Linux 的系統需求](#)。

- 2 在 vSphere 中建立虛擬機器並安裝 Linux 作業系統。請參閱[建立虛擬機器和安裝 Linux](#)。
- 3 為部署為 Horizon7 環境的桌面平台準備客體作業系統。請參閱[準備用於遠端桌面平台部署的 Linux 機器](#)。
- 4 設定 Linux 客體作業系統以 Active Directory 驗證。此步驟會根據您的環境需求以第三方軟體實作。如需詳細資訊，請參閱[整合 Linux 與 Active Directory](#)。
- 5 在 ESXi 主機和 Linux 虛擬機器上設定 3D 功能。依照您欲安裝的 3D 功能之程序進行。
 - 請參閱[針對 vGPU 設定支援的 Linux 發行版](#)。
 - 請參閱[針對 vDGA 設定 RHEL 6.x](#)。
- 6 在 Linux 虛擬機器上安裝 Horizon Agent。請參閱在 [Linux 虛擬機器上安裝 Horizon Agent](#)。
- 7 建立包含已設定 Linux 虛擬機器的桌面平台集區。請參閱[建立 Linux 的手動桌面平台集區](#)。

大量部署

利用 Horizon Console，您只能在手動桌面平台集區部署 Linux 虛擬機器。利用 vSphere PowerCLI，您可以開發能夠自動化部署 Linux 桌面平台機器集區的指令碼。請參閱[第 8 章 針對手動桌面平台集區大量部署 Horizon 7](#)。

Horizon 7for Linux 的系統需求

若要安裝 Horizon 7for Linux，您的 Linux 系統必須符合作業系統、Horizon 7 和 vSphere 平台的特定需求。

Horizon Agent 支援的 Linux 版本

下表列出 Horizon Agent 支援的 Linux 作業系統。

表 1-1. Horizon Agent 支援的 Linux 作業系統

Linux 發行版	架構
Ubuntu 16.04 和 18.04	x64
備註 您必須套用 VMware 知識庫文章 http://kb.vmware.com/kb/2151294 中說明的其中一個解決方案。	
RHEL 6.6、6.7、6.8、6.9、6.10、7.2、7.3、7.4、7.5、7.6、7.7 和 8.0	x64
CentOS 6.6、6.7、6.8、6.9、6.10、7.2、7.3、7.4、7.5、7.6、7.7 和 8.0	x64
NeoKylin 6 Update 1	x64

表 1-1. Horizon Agent 支援的 Linux 作業系統 (續)

Linux 發行版	架構
SLED 12.x SP1/SP2/SP3	x64
SLES 12.x SP1/SP2/SP3	x64

備註 Linux 代理程式具有某些 Linux 發行版的相依性套件。如需詳細資訊，請參閱[安裝 Horizon Agent 相依性套件](#)。

備註 在 RHEL/CentOS 8.0 系統上，Horizon Agent 僅支援 X11 顯示伺服器通訊協定。不支援 Wayland 通訊協定。

需要的平台和 Horizon 7 軟體版本

若要安裝及使用 Horizon 7 for Linux，您的部署必須符合 vSphere 平台、Horizon 7 和 Horizon Client 軟體的特定需求。

表 1-2. 需要的平台和 Horizon 7 軟體版本

平台和軟體	支援的版本
vSphere 平台版本	<ul style="list-style-type: none"> ■ vSphere 6.0 U2 或更新版本 ■ vSphere 6.5 U1 或更新版本 ■ vSphere 6.7 或更新版本
Horizon 環境	<ul style="list-style-type: none"> ■ Horizon 連線伺服器 7.11
Horizon Client 軟體	<ul style="list-style-type: none"> ■ Android 版 Horizon Client 5.3.0 ■ Windows 版 Horizon Client 5.3.0 ■ Linux 版 Horizon Client 5.3.0 ■ Mac OS X 版 Horizon Client 5.3.0 ■ iOS 版 Horizon Client 5.3.0 (iPad Pro) ■ Chrome、Firefox 和 Internet Explorer 上需要 HTML Access 5.3.0 ■ 不支援零用戶端。

Linux 虛擬機器使用的 TCP/UDP 連接埠

Horizon Agent 和 Horizon Client 在彼此之間與各種 Horizon Server 元件之間的網路存取會使用 TCP 或 UDP 連接埠。

表 1-3. Linux 虛擬機器使用的 TCP/UDP 連接埠

來源	連接埠	目標	連接埠	通訊協定	說明
Horizon Client	*	Linux 代理程式	22443	TCP/UDP	若未使用 Blast 安全閘道，則為 Blast
安全伺服器、 Horizon 連線伺服器 或 Access Point 應 用裝置	*	Linux 代理程式	22443	TCP/UDP	若使用 Blast 安全閘道，則為 Blast
HorizonAgent	*	Horizon 連線伺服器	4001、4002	TCP	JMS SSL 流量。

備註 如需關於用戶端所使用 TCP 與 UDP 連接埠的詳細資訊，請參閱《Horizon Client 和 Agent 安全性》文件與 [VMware Horizon 7 指南中的網路連接埠](#)。

若要允許使用者連接至其 Linux 桌面平台，桌面平台必須可以接受來自 Horizon Client 裝置、安全伺服器和 Horizon Connection Server 的連入 TCP 連線。

在 Ubuntu 和 Kylin 發行版上，iptables 防火牆預設會設定為使用「接受」的輸入原則。

在 RHEL 和 CentOS 發行版上，如有可能，Horizon Agent 安裝程式指令碼會將 iptables 防火牆設定為使用「接受」的輸入原則。

確定 RHEL 或 CentOS 客體作業系統上的 iptables 對來自 Blast 連接埠 22443 的新連線具有「接受」的輸入原則。

啟用 BSG 時，用戶端連線會從 Horizon Client 裝置透過安全伺服器或 Horizon Connection Server 上的 BSG 導向 Linux 桌面平台。未啟用 BSG 時，則是直接從 Horizon Client 裝置對 Linux 桌面平台連線。

確認 Linux 虛擬機器使用的 Linux 帳戶

表 1-4. 帳戶名稱和帳戶類型列出 Linux 虛擬機器使用的帳戶名稱和帳戶類型。

表 1-4. 帳戶名稱和帳戶類型

帳戶名稱	帳戶類型	使用者
根	Linux 作業系統內建	Java Standalone Agent、 mksvchanserver、Shell 指令碼
vmwblast	由 Linux 代理程式安裝程式建立	VMwareBlastServer
<目前登入的使用者>	Linux 作業系統內建、AD 使用者或 LDAP 使用者	Python 指令碼

桌面平台環境

Horizon7 for Linux 支援不同 Linux 發行版的多種桌面平台環境。[表 1-5. 支援的桌面平台環境](#)列出各個 Linux 發行版的預設桌面平台環境，以及 Linux 版 Horizon 7 支援的其他桌面平台環境。

表 1-5. 支援的桌面平台環境

Linux 發行版	預設桌面平台環境	Horizon7 for Linux 桌面平台所支援的桌面平台環境
Ubuntu 18.04	Gnome	Gnome Ubuntu、K Desktop Environment (KDE)、MATE
Ubuntu 16.04	Unity	Gnome Flashback (Metacity)、KDE、MATE
RHEL/CentOS 6.x	Gnome	Gnome、KDE
RHEL/CentOS 7.x	Gnome	Gnome、KDE
RHEL/CentOS 8.0	Gnome	Gnome
SLED 12 SP1/SP2/SP3	Gnome	Gnome
SLES 12 SP1/SP2/SP3	Gnome	Gnome
NeoKylin 6 Update 1	Mate	Mate

若要變更其中一個支援的 Linux 發行版上使用的預設桌面平台環境，您必須使用下列適用於您的 Linux 桌面平台的步驟和命令。

備註 只有在 Linux 桌面平台使用預設歡迎畫面 (登入畫面) 時，才可執行 KDE 和 MATE 桌面平台環境的 Single Sign-On (SSO)。您必須使用表 1-6. 用來安裝桌面平台環境的命令中列出的命令來安裝 KDE 和 MATE。

使用 RHEL/CentOS 7.x 和 Ubuntu 18.04/16.04 發行版時，SSO 將無法解除鎖定已鎖定的 KDE 工作階段。您必須手動輸入密碼，才能將鎖定的工作階段解除鎖定。

- 1 使用預設桌面平台環境設定，安裝支援的 Linux 發行版作業系統。
- 2 針對您的特定 Linux 發行版，請執行表 1-6. 用來安裝桌面平台環境的命令中的適當命令。

表 1-6. 用來安裝桌面平台環境的命令

Linux 發行版	新的預設桌面平台環境	用來變更預設桌面平台環境的命令
RHEL/CentOS 6.x	KDE	# yum groupinstall "X Window System" "KDE Desktop"
RHEL/CentOS 7.x	KDE	# yum groupinstall "KDE Plasma Workspaces"
Ubuntu 18.04/16.04	KDE	# apt install plasma-desktop
Ubuntu 18.04	MATE 1.225	# apt install ubuntu-mate-desktop
Ubuntu 16.04	MATE 1.16	# apt-add-repository ppa:ubuntu-mate-dev/xenial-mate # apt update # apt upgrade # apt install mate # apt install ubuntu-mate-themes
Ubuntu 16.04	Gnome Flashback (Metacity)	# apt install gnome-session-flashback

- 3 若要開始使用新的預設桌面平台環境，請重新啟動桌面平台。

如果您在安裝了多個桌面平台環境的 Linux 桌面平台上啟用 SSO，請使用下列資訊，選取要在 SSO 工作階段中使用的桌面平台環境。

- 針對 Ubuntu 18.04/16.04 和 RHEL/CentOS 7.x，請使用 [表 1-7. SSODesktopType 選項](#) 中的資訊來設定 `/etc/vmware/viewagent-custom.conf` 檔案中的 `SSODesktopType` 選項，以指定要用於 SSO 的桌面平台環境。

表 1-7. SSODesktopType 選項

桌面平台類型	SSODesktopType 選項設定
MATE	SSODesktopType=UseMATE
GnomeUbuntu	SSODesktopType=UseGnomeUbuntu
GnomeFlashback	SSODesktopType=UseGnomeFlashback
KDE	SSODesktopType=UseKdePlasma
GnomeClassic	SSODesktopType=UseGnomeClassic

- 針對 RHEL/CentOS 6.x，若要讓 SSO 登入工作階段使用 KDE，請從 `/usr/share/xsession` 目錄中移除 KDE 啟動檔案以外的所有桌面平台啟動檔案。以下列這一組命令為例。

```
# cd /usr/share/xsessions
# mkdir backup
# mv *.desktop backup
# mv backup/kde*.desktop ./
```

使用者在初始設定之後必須將其 Linux 桌面平台登出或重新開機，才能使用 KDE 作為其下一個 SSO 工作階段中的預設桌面平台。

- 針對 RHEL/CentOS 8.0，若要讓 SSO 登入工作階段使用 Gnome Classic，請從 `/usr/share/xsession` 目錄中移除 Gnome Classic 啟動檔案以外的所有桌面平台啟動檔案。以下列這一組命令為例。

```
# cd /usr/share/xsessions
# mkdir backup
# mv *.desktop backup
# mv backup/gnome-classic.desktop ./
```

使用者在初始設定之後必須將其 Linux 桌面平台登出或重新開機，才能使用 Gnome Classic 作為其下一個 SSO 工作階段中的預設桌面平台。

如果您在安裝了多個桌面平台環境的 Linux 桌面平台上停用 SSO，則不需要執行任何前述步驟。使用者在登入該 Linux 桌面平台時，必須選取其所需的桌面平台環境。

網路需求

VMware Blast Extreme 支援使用者資料包通訊協定 (UDP) 和傳輸控制通訊協定 (TCP)。網路狀況會影響 UDP 和 TCP 的效能。若要獲得最優質的使用者體驗，請根據網路狀況選取 UDP 或 TCP。

- 如果網路狀況良好 (例如，在區域網路 (LAN) 環境中)，請選取 TCP。
- 如果網路狀況不佳 (例如，在封包遺失且時間延遲的廣域網路 (WAN) 環境中)，請選取 UDP。

使用網路分析器工具 (例如 Wireshark) 來判斷 VMware Blast Extreme 是否使用 TCP 或 UDP。使用下列參考範例中使用 Wireshark 的一組步驟。

- 1 在您的 Linux 虛擬機器上下載並安裝 Wireshark。

針對 RHEL/CentOS 6:

```
sudo yum install wireshark
```

針對 Ubuntu 18.04/16.04:

```
sudo apt install tshark
```

針對 SLES/SLED 12:

```
sudo zypper install wireshark
```

- 2 使用 VMware Horizon Client 連線至 Linux 桌面平台。
- 3 開啟終端機視窗並執行下列命令以顯示 VMware Blast Extreme 使用的 TCP 套件或 UDP 套件。

```
sudo tshark -i any | grep 22443
```

網路狀況牽動著 USB 重新導向和用戶端磁碟機重新導向 (CDR) 功能的效用。如果網路狀況不佳 (例如, 因頻寬受限而導致時間延遲和封包遺失), 使用者體驗就會變差。在這種情況下, 使用者可能會遇到下列其中一種狀況。

- 遠端檔案的複製可能會很慢。在此情況下, 請改為傳輸較小的檔案。
- USB 裝置未出現在遠端 Linux 桌面平台中。
- USB 資料未完整傳輸。例如, 在複製大型檔案時, 您取得的檔案大小可能會小於原始檔案。

USB 重新導向的 VHCI 驅動程式

USB 重新導向功能對 USB 虛擬主機控制器介面 (VHCI) 核心驅動程式具有相依性。若要支援 USB 3.0 和 USB 重新導向功能, 您必須執行下列步驟:

- 1 從 <https://sourceforge.net/projects/usb-vhci/files/linux%20kernel%20module/> 下載 USB VHCI 原始程式碼。
- 2 若要編譯 VHCI 驅動程式原始程式碼, 並在您的 Linux 系統上安裝產生的二進位檔, 請使用 [表 1-8. 編譯及安裝 USB VHCI 驅動程式](#) 中的命令。

例如，如果您將安裝檔案 VMware-horizonagent-linux-x86_64-*<version>*-*<build-number>*.tar.gz 解壓縮到 /install_tmp/ 目錄下，則 *full-path_to_patch-file* 為 /install_tmp/VMware-horizonagent-linux-x86_64-*<version>*-*<buildnumber>*/resources/vhci/patch/vhci.patch，且要使用的 patch 命令為

```
# patch -p1 < /install_tmp/VMware-horizonagent-linux-x86_64-<version>-<build-number>/resources/vhci/patch/vhci.patch
```

備註 安裝 Horizon for Linux 之前必須完成 VHCI 驅動程式安裝。

表 1-8. 編譯及安裝 USB VHCI 驅動程式

Linux 發行版	編譯及安裝 USB VHCI 驅動程式的步驟
Ubuntu 18.04	<ol style="list-style-type: none"> 安裝相依性套件。 <pre># apt-get install make # apt-get install gcc # apt-get install libelf-dev</pre> 編譯及安裝 VHCI 驅動程式。 <pre># tar -xzvf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < full-path_to_patch-file # make clean && make && make install</pre>
Ubuntu 16.04	<p>編譯及安裝 VHCI 驅動程式。</p> <pre># tar -xzvf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < full-path_to_patch-file # make clean && make && make install</pre>

表 1-8. 編譯及安裝 USB VHCI 驅動程式 (續)

Linux 發行版	編譯及安裝 USB VHCI 驅動程式的步驟
RHEL/CentOS 6.9/6.10	1 安裝相依性套件。
RHEL/CentOS 7.x	<pre># yum install gcc-c++ # yum install kernel-devel-\$(uname -r) # yum install kernel-headers-\$(uname -r) # yum install patch # yum install elfutils-libelf-devel</pre>
RHEL/CentOS 8.0	<pre># yum install gcc-c++ # yum install kernel-devel-\$(uname -r) # yum install kernel-headers-\$(uname -r) # yum install patch # yum install elfutils-libelf-devel</pre>
	2 編譯及安裝 VHCI 驅動程式。
	<pre># tar -xzf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < full-path-to-patch-file # make clean && make && make install</pre>
	3 (RHEL/CentOS 8.0) 若要確保 VHCI 驅動程式可與 USB 重新導向正常搭配運作，請設定 USB 驅動程式的簽署設定。
	a 建立 USB 驅動程式的 SSL 金鑰配對。
	<pre>openssl req -new -x509 -newkey rsa:2048 -keyout MOK.priv -outform DER -out MOK.der -nodes -days 36500 -subj "/CN=Descriptive name/"</pre>
	b 簽署 USB 驅動程式。
	<pre>sudo /usr/src/kernels/\$(uname -r)/scripts/sign-file sha256 ./MOK.priv ./MOK.der /lib/modules/\$(uname -r)/kernel/drivers/usb/host/usb-vhci-iocifc.ko sudo /usr/src/kernels/\$(uname -r)/scripts/sign-file sha256 ./MOK.priv ./MOK.der /lib/modules/\$(uname -r)/kernel/drivers/usb/host/usb-vhci-hcd.ko</pre>
	c 登錄用於 UEFI 安全開機的金鑰。
	<pre>sudo mokutil --import MOK.der</pre>
	備註 此命令會發出要求，以設定用於 UEFI 安全開機的機器擁有者金鑰 (MOK) 密碼。
	d 若要在 vSphere 主控台中設定 UEFI 安全開機，請將系統重新開機。如需詳細資訊，請參閱 https://sourceware.org/systemtap/wiki/SecureBoot 。
SLED/SLES 12 SP2	1 找出目前核心套件的版本。
	<pre># rpm -qa grep kernel-default-\$(echo \$(uname -r) cut -d '-' -f 1,2)</pre>
	輸出結果為目前所安裝核心套件的名稱。例如，如果套件名稱為 kernel-default-3.0.101-63.1，則目前的核心套件版本將是 3.0.101-63.1。
	2 安裝 kernel-devel、kernel-default-devel、kernel-macros 和 patch 套件。
	<pre># zypper install --oldpackage kernel-devel-<kernel-package-version> \ kernel-default-devel-<kernel-package-version> kernel-macros-<kernel-package-version> patch</pre>
	例如：
	<pre># zypper install --oldpackage kernel-devel-4.4.21-90.1 kernel-default-devel-4.4.21-90.1 kernel-macros-4.4.21-90.1 patch</pre>

表 1-8. 編譯及安裝 USB VHCI 驅動程式 (續)

Linux 發行版 編譯及安裝 USB VHCI 驅動程式的步驟

3 編譯及安裝 VHCI 驅動程式。

```
# tar -xzvf vhci-hcd-1.15.tar.gz
# cd vhci-hcd-1.15
# patch -p1 < full-path_to_patch-file
# mkdir -p linux/$(echo $(uname -r) | cut -d '-' -f 1)/drivers/usb/core
# cp /lib/modules/$(uname -r)/source/include/linux/usb/hcd.h linux/$(echo $(uname -r) | cut -d '-' -f 1)/drivers/usb/core
# make clean && make && make install
```

此外，請遵循下列指導方針：

- 如果您的 Linux 核心變更為新版本，則必須重新編譯並重新安裝 VHCI 驅動程式，但不需重新安裝 Horizon for Linux。
- 您也可以使用與 Ubuntu 18.04/16.04 系統的下列範例相類似的步驟，將動態核心模組支援 (DKMS) 新增至 VHCI 驅動程式。

a 安裝核心標頭。

```
# apt install linux-headers-$(uname -r)
```

b 使用下列命令安裝 dkms。

```
# apt install dkms
```

c 解壓縮並修補 VHCI TAR 檔案。

```
# tar xzvf vhci-hcd-1.15.tar.gz
# cd vhci-hcd-1.15
# patch -p1 <full-path_to_patch-file>
# cd ..
```

d 將解壓縮的 VHCI 來源檔案複製到 /usr/src 目錄。

```
# cp -r vhci-hcd-1.15 /usr/src/usb-vhci-hcd-1.15
```

e 建立名為 dkms.conf 的檔案，並將其置於 /usr/src/usb-vhci-hcd-1.15 目錄中。

```
# touch /usr/src/usb-vhci-hcd-1.15/dkms.conf
```

f 將下列內容新增至 dkms.conf 檔案。

```
PACKAGE_NAME="usb-vhci-hcd"
PACKAGE_VERSION=1.15
MAKE_CMD_TMPL="make KVERSION=$(kernelver)"

CLEAN="$MAKE_CMD_TMPL clean"

BUILT_MODULE_NAME[0]="usb-vhci-iocifc"
DEST_MODULE_LOCATION[0]="/kernel/drivers/usb/host"
```

```
MAKE[0]="$MAKE_CMD_TMPL"

BUILT_MODULE_NAME[1]="usb-vhci-hcd"
DEST_MODULE_LOCATION[1]="/kernel/drivers/usb/host"
MAKE[1]="$MAKE_CMD_TMPL"

AUTOINSTALL="YES"
```

- g 在 dkms 中新增此 VHCI 驅動程式。

```
# dkms add usb-vhci-hcd/1.15
```

- h 建置 VHCI 驅動程式。

```
# dkms build usb-vhci-hcd/1.15
```

- i 安裝 VHCI 驅動程式。

```
# dkms install usb-vhci-hcd/1.15
```

2D 圖形卡的虛擬機器設定

建立特定 Horizon 7 for Linux 虛擬機器時，必須變更 vCPU 和虛擬記憶體設定以滿足效能需求。

設定為使用 NVIDIA vDGA 的虛擬機器會使用 NVIDIA 實體圖形卡。設定為使用 NVIDIA GRID vGPU 的虛擬機器會使用以 NVIDIA 實體圖形加速器為基礎的 NVIDIA 虛擬圖形卡。您不需變更這些虛擬機器的 vCPU 和虛擬記憶體設定。

設定為使用 2D 圖形卡的虛擬機器將使用 VMware 虛擬顯示卡，且您必須變更 vCPU 和虛擬記憶體設定，才能改善桌面平台效能。使用下列指導方針：

- 對於 2D 桌面平台中改善的效能，請為 Linux 虛擬機器設定更多 vCPU 和虛擬記憶體。例如，設定 2 個 vCPU 和 2 GB 的虛擬記憶體。
- 對於多台監視器 (例如四台監視器) 的大型螢幕顯示，請為虛擬機器設定 4 個 vCPU 和 4 GB 的虛擬記憶體。
- 對於 2D 桌面平台中改善的視訊播放，請為虛擬機器設定 4 個 vCPU 和 4 GB 的虛擬記憶體。

在 Linux 桌面平台上設定工作階段協作

透過工作階段協作功能，使用者可以邀請其他使用者加入現有的 Linux 遠端桌面工作階段。

工作階段協作的系統需求

若要支援工作階段協作功能，您的 Horizon 部署必須符合特定需求。

表 1-9. 工作階段協作的系統需求

元件	需求
用戶端系統	工作階段擁有者和協作者必須已在用戶端系統上安裝 Windows、Mac 或 Linux 版 Horizon Client 4.10 或更新版本，或必須使用 HTML Access 4.10 或更新版本。
Linux 遠端桌面平台	必須在 Linux 虛擬桌面平台中安裝 Horizon Agent 7.7 或更新版本。必須在桌面平台集區和 VDI 層級上啟用工作階段協作功能。
連線伺服器	連線伺服器執行個體會使用 Enterprise 授權。
顯示通訊協定	VMware Blast

備註 RHEL 8.0 桌面平台需要額外的系統組態，才能支援工作階段協作。請參閱[設定 RHEL 8.0 桌面平台以進行工作階段協作](#)。

如需如何使用工作階段協作功能的相關資訊，請參閱 Horizon Client 說明文件。

在組態檔中設定工作階段協作選項

在 `/etc/vmware/viewagent-custom.conf` 檔案中設定下列選項，以啟用或停用工作階段協作功能。

■ CollaborationEnable

在 `/etc/vmware/config` 檔案中設定下列選項，以設定要在協作工作階段期間使用的設定。

- `collaboration.logLevel`
- `collaboration.maxCollabors`
- `collaboration.enableEmail`
- `collaboration.serverUrl`
- `collaboration.enableControlPassing`

如需詳細資訊，請參閱在[Linux 桌面平台上設定組態檔中的選項](#)。

工作階段協作功能限制

使用者無法在協作工作階段中使用下列遠端桌面平台功能。

- USB 重新導向
- 音訊輸入重新導向
- 用戶端磁碟機重新導向
- 智慧卡重新導向
- 剪貼簿重新導向

使用者無法在協作工作階段中變更遠端桌面平台的解析度。

使用者在相同的用戶端機器上不能有多個協作工作階段。

備註 如果在使用者第一次登入遠端桌面平台後，系統匣中的工作階段協作圖示沒有回應，請指示使用者調整遠端桌面平台視窗的大小。調整桌面平台視窗的大小後，工作階段協作圖示將變得可回應。

設定 RHEL 8.0 桌面平台以進行工作階段協作

若要在 RHEL 8.0 桌面平台上使用工作階段協作功能，您必須先下載並安裝 GNOME 3.28.26 Shell 延伸。

程序

- 1 從 <https://extensions.gnome.org/extension/615/appindicator-support/> 將所需的 GNOME Shell 延伸下載至 RHEL 8.0 系統。針對 Shell 版本，請選取 **3.28**。針對延伸版本，請選取 **26**。
- 2 將下載的套件解壓縮，並將目錄重新命名為 `appindicatorsupport@rgcjonas.gmail.com` (此套件中 `metadata.json` 檔案內的「uuid」值)。
- 3 使用 `mv` 命令，將 `appindicatorsupport@rgcjonas.gmail.com` 目錄移至下列位置：`/usr/share/gnome-shell/extensions`。

依預設，只有根使用者可以讀取 `appindicatorsupport@rgcjonas.gmail.com` 目錄中的 `metadata.json` 檔案。若要支援工作階段協作，您還必須讓其他使用者能夠讀取此檔案。

- 4 請執行命令，將 `metadata.json` 設為可供其他使用者讀取，如下列範例所示。

```
chmod a+r metadata.json
```

- 5 安裝 `gnome-tweaks`。
- 6 在桌面平台環境中，使用鍵盤按以下一系列的按鍵，以重新啟動 GNOME Shell。

```
Alt+F2  
r  
Enter
```

- 7 在桌面平台環境中執行 `gnome-tweaks`，然後啟用 **KStatusNotifierItem/AppIndicator Support**。

為桌面平台部署準備 Linux 虛擬機器

2

設定 Linux 桌面平台牽涉到建立 Linux 虛擬機器和為遠端桌面平台部署準備作業系統。

本章節討論下列主題：

- 建立虛擬機器和安裝 Linux
- 準備用於遠端桌面平台部署的 Linux 機器
- 安裝 Horizon Agent 相依性套件

建立虛擬機器和安裝 Linux

您會在 vCenter Server 中為 Horizon7 中部署的每個遠端桌面平台建立新虛擬機器。您必須在虛擬機器上安裝 Linux 發行版。

必要條件

- 驗證您的部署符合支援 Linux 桌面平台的需求。請參閱 [Horizon 7for Linux 的系統需求](#)。
- 熟悉在 vCenter Server 中建立虛擬機器和安裝客體作業系統的步驟。請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的「建立和準備虛擬機器」。
- 熟悉您計劃與虛擬機器搭配使用之監視器的視訊記憶體 (vRAM) 設定需求。請參閱 [Horizon 7for Linux 的系統需求](#)。

程序

- 1 在 vSphere Web Client 或 vSphere Client 中，建立新虛擬機器。

2 設定自訂組態選項。

a 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。

b 指定 vCPU 和 vMemory 大小的數量。

針對必要的設定，請遵循 Linux 發行版適用的安裝指南中的指示。

例如，Ubuntu 18.04 指定對 vMemory 設定 2048 MB 和 2 個 vCPU。

c 選取**視訊卡**，並指定顯示器數量和總視訊記憶體 (vRAM)。

針對使用 2D 圖形的虛擬機器 (使用 VMware 驅動程式)，設定 vSphere Web Client 中的 vRAM 大小。vRAM 大小在 vDGA 或 NVIDIA GRID vGPU 機器 (使用 NVIDIA 驅動程式) 上沒有影響。

針對必要的設定，請遵循 [2D 圖形卡的虛擬機器設定](#) 中的指導方針。請勿使用視訊記憶體計算機。

3 將虛擬機器開機並安裝 Linux 發行版。**4 設定要用於特定 Linux 發行版的桌面平台環境。**

如需其他資訊，請參閱 [Horizon 7 for Linux 的系統需求](#) 中的〈桌面平台環境〉一節。

5 確保可將系統主機名稱解析為 127.0.0.1。

準備用於遠端桌面平台部署的 Linux 機器

您必須執行某些工作以準備要在 Horizon 7 部署中作為桌面平台使用的 Linux 機器。

若要準備 Linux 機器以供 Horizon 7 進行管理，您必須啟用機器與連線伺服器之間的通訊。您必須在 Linux 機器上設定網路，以便 Linux 機器可以使用其 FQDN (完整網域名稱) ping 連線伺服器執行個體。

Open VMware Tools (OVT) 已預先安裝在 RHEL 8.0/7x、CentOS 8.0/7x 和 SLED/SLES 12.x 機器上。如果您是要準備這些機器以用作遠端桌面平台，則可略過下列程序中的步驟 1 到 5，這些步驟說明如何以手動執行安裝程式來安裝 VMware Tools。

如果您正在使用 Ubuntu 16.04/18.04 機器，請在該機器上安裝 OVT。如果您準備將此機器作為遠端桌面平台，則可略過下列程序中的步驟 1 到 5，並使用下列命令，在您的 Ubuntu 16.04/18.04 機器上手動安裝 OVT：

```
apt-get install open-vm-tools-desktop
```

必要條件

- 驗證已在 vCenter Server 中建立新虛擬機器 (VM)，以及已在機器上安裝您的 Linux 發行版
- 自行熟悉在 Linux 虛擬機器上裝載和安裝 VMware Tools 的步驟。請參閱 vSphere 虛擬機器管理文件中的「在 Linux 虛擬機器中手動安裝或升級 VMware Tools」。
- 自行熟悉設定 Linux 機器以使機器可透過 DNS 解析的步驟。這些步驟可能因不同 Linux 發行版和版本而有所不同。如需指示，請查閱您的 Linux 發行版和版本的說明文件。

程序

1 在 vSphere Web Client 或 vSphere Client 中，在虛擬機器上裝載 VMware Tools 虛擬磁碟。

- 2 以滑鼠右鍵按一下 VMware Tools 安裝程式檔案 `VMwareTools.x.x.x-xxxx.tar.gz`，按一下解壓縮至，然後為您的 Linux 發行版選取桌面平台。

`vmware-tools-distrib` 資料夾隨即解壓縮到桌面平台。

- 3 在虛擬機器上，以 `root` 身分登入，並開啟終端機視窗。
- 4 解壓縮 VMware Tools tar 安裝程式檔案。

例如：

```
tar xzpf /mnt/cdrom/VMwareTools-x.x.x-yyyy.tar.gz
```

- 5 執行安裝程式並設定 VMware Tools。

不同 Linux 發行版中的命令可能有些微不同。例如：

```
cd vmware-tools-distrib
sudo ./vmware-install.pl -d
```

通常情況下，執行完安裝程式檔案之後會執行 `vmware-config-tools.pl` 組態檔案。

- 6 將 Linux 機器的主機名稱對應至 `/etc/hosts` 檔案中的 127.0.0.1。

針對 RHEL、CentOS、SLES 和 SLED，您必須手動將主機名稱對應至 127.0.0.1，因為它並不會自動對應。此步驟對 Ubuntu 來說並非必要，因為系統會依預設進行對應。此步驟在您大量部署桌面平台時也非必要，因為複製處理程序會新增此對應。

備註 如果您在安裝 Horizon Agent 之後變更了 Linux 機器的主機名稱，您必須將新的主機名稱對應至 `/etc/hosts` 檔案中的 127.0.0.1。否則，系統會繼續使用舊的主機名稱。

- 7 對於 RHEL 和 CentOS，請確認已停用 `virbr0`。

```
virsh net-destroy default
virsh net-undefine default
service libvirtd restart
```

- 8 確保網繭中的 Horizon Connection Server 執行個體可透過 DNS 解析。

- 9 設定 Linux 機器，讓預設執行層級為 5。

執行層級必須是 5，Linux 桌面平台才能運作。

- 10 在設定以 OpenLDAP 伺服器驗證的 Ubuntu 機器上，設定機器的完整網域名稱。

此步驟可確保該資訊能在 Horizon Console [工作階段] 頁面的 [使用者] 欄位中正確顯示。依照下列方法編輯 `/etc/hosts` 檔案：

- a `# nano /etc/hosts`
- b 新增完整網域名稱。例如：127.0.0.1 hostname.domainname hostname。
- c 結束並儲存檔案。

11 對於 SUSE，請停用 [透過 DHCP 變更主機名稱]。設定主機名稱或網域名稱。

- a 在 Yast 中，按一下網路設定。
- b 按一下主機名稱/DNS 索引標籤。
- c 取消選取透過 DHCP 變更主機名稱。
- d 輸入主機名稱和網域名稱。
- e 按一下確定。

安裝 VMware Tools 之後，如果您升級 Linux 核心，VMware Tools 可能停止執行。若要解決問題，請參閱 <http://kb.vmware.com/kb/2050592>。

安裝 Horizon Agent 相依性套件

Horizon Agent for Linux 具有某些 Linux 發行版特有的相依性套件。在安裝 Horizon Agent for Linux 之前，您必須先安裝這些套件。

必要條件

確認已在 vCenter Server 中建立新虛擬機器 (VM)，以及已在機器上安裝您的 Linux 發行版。

程序

1 安裝依預設不會進行安裝或升級的強制套件。如果任何套件不符合需求，則安裝程式會中斷安裝。

表 2-1. 強制相依性套件

Linux 發行版	套件
RHEL 7.5	<code>yum install libappindicator-gtk3</code>
SLES 12.x SP1/SLED 12.x SP1 從 SUSE 存放庫將 xf86-video-vmware 升級為比 13.0.2-3.2 更新的版本。	<ol style="list-style-type: none"> 登錄 SUSE 12.x 以啟用 SUSE 存放庫。 <code>SUSEConnect -r 登錄代碼 -e 電子郵件</code> 更新 xf86-video-vmware 版本。 <code>zypper update xf86-video-vmware</code>
SLES 12.x	<p>當您正在安裝 Horizon Agent 時，需要為 SLES 12.x Linux 桌面平台安裝 python-gobject2。</p> <ol style="list-style-type: none"> 登錄 SUSE 12.x 以啟用 SUSE 存放庫。 <code>SUSEConnect -r 登錄代碼 -e 電子郵件</code> 安裝 python-gobject2。 <code>zypper install python-gobject2</code>
Ubuntu 16.04	<code>apt-get install python-dbus python-gobject</code>
Ubuntu 18.04	<code>apt-get install python python-dbus python-gobject</code>

2 安裝 Horizon Agent 選用套件。

- 依預設，RHEL 或 CentOS 6.7 會安裝 `glibc-2.12-1.166.el6.x86_64`，而這可能導致鎖死問題。因此，桌面平台連線會中斷。若要解決此問題，您必須從線上存放庫將 `glibc` 升級為最新版本。

```
sudo yum install glibc
```

設定 Linux 桌面平台的 Active Directory 整合

3

Horizon 7 使用現有的 Microsoft Active Directory (AD) 基礎結構進行使用者驗證及管理。您可以整合 Linux 桌面平台與 Active Directory，讓使用者可以使用自己的 Active Directory 使用者帳戶登入 Linux 桌面平台。

備註 Horizon Agent 預期 Linux 桌面平台和用戶端使用者應位於相同的 Active Directory 網域中。如果桌面平台和使用者的網域不同，Horizon Agent 可能會將桌面平台網域誤認為使用者網域。

本章節討論下列主題：

- [整合 Linux 與 Active Directory](#)
- [設定 Single Sign-On](#)
- [設定智慧卡重新導向](#)
- [設定 True SSO for Linux 桌面平台](#)

整合 Linux 與 Active Directory

有多個解決方案可用來整合 Linux 與 Microsoft Active Directory (AD)，且 Horizon 7 for Linux 桌面平台對於所使用的解決方案不具相依性。

以下是已知可在 Horizon 7 for Linux 桌面平台環境中運作的解決方案。

- OpenLDAP 伺服器傳遞驗證
- 對 Microsoft Active Directory 執行的系統安全服務精靈 (SSSD) LDAP 驗證
- Winbind 網域加入
- PowerBroker Identity Services Open (PBISO) 驗證
- Samba 離線網域加入

如果您使用 LDAP 型解決方案，您必須在範本虛擬機器中執行組態，而不需在複製的虛擬機器中執行其他步驟。

備註 若要簡化部署程序，請對 Microsoft Active Directory 使用 SSSD LDAP 驗證的解決方案。

使用 OpenLDAP 伺服器傳遞驗證

您可以設定 OpenLDAP 伺服器並使用傳遞驗證 (PTA) 機制，來針對 Active Directory 驗證使用者認證。OpenLDAP 傳遞驗證解決方案大致牽涉到下列步驟。

程序

- 1 若要啟用 LDAPS (透過 SSL 的輕量型目錄存取通訊協定)，請在 Active Directory 上安裝憑證服務。
- 2 設定 OpenLDAP 伺服器。
- 3 將使用者資訊 (密碼除外) 從 Active Directory 同步至 OpenLDAP 伺服器。
- 4 設定 OpenLDAP 伺服器以委派密碼驗證給個別處理程序 (例如 saslauthd)，以對 Active Directory 執行密碼驗證。
- 5 設定 Linux 桌面平台，以使用 LDAP 用戶端對 OpenLDAP 伺服器驗證使用者。

對 Microsoft Active Directory 設定 SSSD LDAP 驗證

透過在 Linux 桌面平台中設定系統安全服務精靈 (SSSD)，您可以對 Windows Active Directory 使用 LDAP 驗證。

使用下列高階步驟來設定 SSSD LDAP 驗證解決方案。

程序

- 1 若要啟用 LDAPS (透過安全通訊端層的輕量型目錄存取通訊協定)，請在 Active Directory 伺服器上安裝憑證服務。
- 2 若要使用直接對 Microsoft Active Directory 執行的 LDAP 驗證，請在 Linux 桌面平台中設定 SSSD。

使用 Winbind 網域加入解決方案

基於 Kerberos 的驗證解決方案的 Winbind 網域加入解決方案，是向 Active Directory 進行驗證的另一種方法。

使用下列高階步驟來設定 Winbind 網域加入解決方案。

程序

- 1 在 Linux 桌面平台上安裝 winbind、samba 和 Kerberos 套件。
- 2 將 Linux 桌面平台加入至 Microsoft Active Directory。

後續步驟

如果您使用 Winbind 網域加入解決方案或其他 Kerberos 驗證型解決方案，請將範本虛擬機器加入至 Active Directory，並將複製的虛擬機器重新加入至 Active Directory。例如，請使用下列命令：

```
sudo /usr/bin/net ads join -U <domain_user>%<domain_password>
```

請使用下列選項，對 Winbind 解決方案的已複製虛擬機器執行網域重新加入命令：

- 使用 SSH 或 vSphere PowerCLI 等工具遠端連線到每個虛擬機器，然後執行命令。如需指令碼的詳細資訊，請參閱 [第 8 章 針對手動桌面平台集區大量部署 Horizon 7](#)。
- 將命令包含在 Shell 指令碼中，然後在 `/etc/vmware/viewagent-custom.conf` 檔案中設定 Horizon Agent RunOnceScript 選項的指令碼路徑。如需詳細資訊，請參閱在 [Linux 桌面平台上設定組態檔中的選項](#)。

設定 PowerBroker Identity Services Open (PBISO) 驗證

PowerBroker Identity Services Open (PBISO) 驗證方法是一種適用於執行離線網域加入的支援解決方案。

執行下列步驟，以使用 PBISO 將 Linux 桌面平台加入至 Active Directory。

程序

- 1 從 <https://www.beyondtrust.com/products/powerbroker-identity-services-open/> 下載 PBISO 8.5.6 或更新版本。
- 2 在 Linux 虛擬機器上安裝 PBISO。

```
sudo ./pbis-open-8.5.6.2029.linux.x86_64.deb.sh
```

- 3 安裝 Horizon 7 Agent for Linux。
- 4 使用 PBISO 將 Linux 桌面平台加入至 AD 網域。

在下列範例中，**lxdc.vdi** 是網域名稱，**administrator** 是網域使用者名稱。

```
sudo domainjoin-cli join lxdc.vdi administrator
```

- 5 為網域使用者設定預設組態。

```
sudo /opt/pbis/bin/config UserDomainPrefix lxdc
sudo /opt/pbis/bin/config AssumeDefaultDomain true
sudo /opt/pbis/bin/config LoginShellTemplate /bin/bash
sudo /opt/pbis/bin/config HomeDirTemplate %H/%U
```

- 6 編輯 `/etc/pamd.d/common-session` 檔案。
 - a 找出內容為 **session sufficient pam_lsass.so** 的一行。
 - b 將該行取代為 **session [success=ok default=ignore] pam_lsass.so**。

備註 在重新安裝或更新 Horizon Agent for Linux 之後，必須重複此步驟。

- 針對 Ubuntu 16.04，將以下幾行附加至 `/usr/share/lightdm/lightdm.conf.d/50-unity-greeter.conf` 組態檔。

```
allow-guest=false
greeter-show-manual-login=true
```

備註 如果您使用 Ubuntu 18.04，則不需要變更 lightdm 組態檔。

- 將系統重新開機，然後登入。

後續步驟

備註

- 如果 `/opt/pbis/bin/config AssumeDefaultDomain` 選項設為 **false**，您必須在 `/etc/vmware/viewagent-custom.conf` 檔案中更新 `SSOUserFormat=<username>@<domain>` 設定。
- 使用 Horizon 即時複製浮動桌面平台集區功能時，為避免在新的網路介面卡新增至複製的虛擬機器時遺失 DNS 伺服器設定，請為您的 Linux 系統修改 `resolv.conf` 檔案。請使用下列關於 Ubuntu 16.04 系統的範例，作為在 `/etc/resolvconf/resolv.conf.d/head` 檔案中新增所需行的指引。

```
nameserver 10.10.10.10
search mydomain.org
```

設定 Samba 離線網域加入

若要在 Horizon 7 for Linux 桌面平台環境中的即時複製虛擬機器上支援 SSO，請在主要 Linux 虛擬機器上設定 Samba。

以下面的程序為例，使用 Samba 將即時複製 Linux 桌面平台離線網域加入至 Active Directory。此程序提供 Ubuntu 系統適用的步驟。

程序

- 在主要 Linux 虛擬機器上，安裝 `winbind` 和 `samba` 套件，包括任何其他相依程式庫，例如 `smbfs` 和 `smbclient`。
- 使用下列命令來安裝 Samba `tdb-tools` 套件。

```
sudo apt-get install tdb-tools
```

- 安裝 Horizon 7 Agent for Linux。
- 編輯 `/etc/samba/smb.conf` 組態檔，使其具有類似於下列範例的內容。

```
[global]
security = ads
realm = LAB.EXAMPLE.COM
workgroup = LAB
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
```

```
winbind enum group = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
```

- 5 編輯 `/etc/krb5.conf` 組態檔，使其具有類似於下列範例的內容。

```
[libdefaults]
default_realm = EXAMPLE.COM

krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms

kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true

[realms]
YOUR-DOMAIN = {
kdc = 10.111.222.33
}

[domain_realm]
your-domain = EXAMPLE.COM
.your-domain = EXAMPLE.COM
```

- 6 編輯 `/etc/nsswitch.conf` 組態檔，如下列範例所示。

```
passwd: files winbind
group: files winbind
shadow: files winbind
gshadow: files
```

- 7 確認主機名稱正確無誤，且系統日期和時間已與 DNS 系統同步化。
- 8 若要通知 Horizon Agent Linux 虛擬機器已使用 Samba 方法進行加入網域，請在 `/etc/vmware/viewagent-custom.conf` 檔案中設定以下選項。

```
OfflineJoinDomain=samba
```

- 9 將系統重新開機，然後重新登入。

針對 RHEL/CentOS 8.0 使用 Realmd 加入解決方案

若要確保功能的作業 (例如單一登入) 對 RHEL/CentOS 8.0 桌面平台正常執行，請使用 `realmd` 解決方案來將桌面平台加入 Active Directory (AD) 網域。

程序

- 1 為 RHEL/CentOS 8.0 系統設定完整主機名稱。

例如，如果 **rhel8** 是系統的非完整主機名稱，且 **LXD.VDI** 是 AD 網域，請執行以下命令。

```
# hostnamectl set-hostname rhel8.lxd.vdi
```

- 2 確認與 AD 網域的網路連線，如以下範例所示。

```
# realm discover -vvv LXD.VDI
```

- 3 安裝所需的相依性套件，如以下範例所示。

```
# dnf install -y sssd adcli samba-common-tools oddjob oddjob-mkhomedir
```

- 4 加入 AD 網域，如下列範例所示。

```
# realm join -U Administrator LXD.VDI
```

- 5 編輯 `/etc/sss/sss.conf`，使其具有類似於下列範例的內容。在 `ad_gpo_map_interactive = +gdm-vmwcred[domain/domain name]` 區段下新增。

```
[sss]
domains = LXD.VDI
config_file_version = 2
services = nss, pam

[domain/LXD.VDI]
ad_domain = LXD.VDI
krb5_realm = LXD.VDI
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False
fallback_homedir = /home/%u
access_provider = ad
ad_gpo_map_interactive = +gdm-vmwcred
```

- 6 若要確保網域加入生效，請將系統重新開機，然後重新登入。
- 7 確認已正確設定網域使用者。以下範例顯示如何使用 `id` 命令從網域使用者 **zyc1** 傳回組態輸出。

```
# id zyc1

uid=1084401403(zyc1) gid=1084400513(domain users) groups=1084400513(domain users)
```

8 使用網域使用者的認證，確認您可以成功登入桌面平台。

備註 對於 RHEL/CentOS 8.0 桌面平台，Horizon Agent 僅支援 X11 顯示伺服器通訊協定。若要將 X11 設定為系統的預設顯示伺服器通訊協定，請按一下登入畫面上的 [設定] 圖示，然後從下拉式功能表中選取 **Classic (X11 顯示伺服器)**。

設定 Single Sign-On

若要設定 Single Sign-On (SSO)，您必須執行一些組態步驟。

Horizon Single Sign-On 模組會與 Linux 中的 PAM (插入式驗證模組) 通訊，並且不依賴於您用來整合 Linux 與 Active Directory (AD) 的方法。Horizon SSO 已知可與整合 Linux 與 AD 的 OpenLDAP 和 Winbind 解決方案搭配使用。

依預設，SSO 會假設 AD 的 sAMAccountName 屬性為登入識別碼。為確保對 SSO 使用正確的登入識別碼，如果您使用 OpenLDAP 或 Winbind 解決方案，則必須執行下列設定步驟：

- 針對 OpenLDAP，將 sAMAccountName 設定為 uid。
- 針對 Winbind，新增下列陳述式至組態檔 /etc/samba/smb.conf。

```
winbind use default domain = true
```

如果使用者必須指定要登入的網域名稱，您必須在 Linux 桌面平台上設定 SSUserFormat 選項。如需詳細資訊，請參閱在 [Linux 桌面平台上設定組態檔中的選項](#)。SSO 一律使用大寫的簡短網域名稱。例如，如果網域為 mydomain.com，SSO 會使用 MYDOMAIN 作為網域名稱。因此，設定 SSUserFormat 選項時，您必須指定 MYDOMAIN。關於簡短和完整網域名稱，所適用的規則如下：

- 針對 OpenLDAP，您必須使用大寫的簡短網域名稱。
- Winbind 支援完整和簡短網域名稱。

AD 支援在登入名稱中使用特殊字元，但 Linux 不支援。因此，設定 SSO 時請勿在登入名稱中使用特殊字元。

在 AD 中，如果使用者的 UserPrincipalName (UPN) 屬性和 sAMAccount 屬性不符，而且使用者使用 UPN 登入，SSO 將會失敗。例如，如果您在 AD mycompany.com 中有使用者 juser，但使用者的 UPN 設定為 juser123@mycompany.com 而非 juser@mycompany.com，SSO 將會失敗。因應措施是讓使用者使用 sAMAccount 中儲存的名稱來登入。例如，juser。

Horizon 7 不要求使用者名稱區分大小寫。您必須確保 Linux 作業系統可以處理不區分大小寫的使用者名稱。

- 針對 Winbind，使用者名稱預設不區分大小寫。
- 針對 OpenLDAP，Ubuntu 使用 NSCD 來驗證使用者，並且預設不區分大小寫。RHEL 和 CentOS 使用 SSSD 來驗證使用者，並且預設區分大小寫。若要變更設定，請編輯檔案 /etc/sss/sss.conf，並在 [domain/default] 區段新增下列程式行：

```
case_sensitive = false
```

如果您的 Linux 桌面平台安裝了多個桌面平台環境，請參閱[桌面平台環境](#)，以選取要與 SSO 搭配使用的桌面平台環境。

設定智慧卡重新導向

若要設定智慧卡重新導向，您必須執行一些組態步驟。

智慧卡重新導向概觀

桌面平台若執行下列已安裝指定 Horizon Agent 版本的 Linux 發行版，即支援智慧卡重新導向。

表 3-1. 智慧卡重新導向的系統需求

Linux 發行版	Horizon Agent
RHEL 8.0	Horizon Agent 7.10 或更新版本
RHEL 7.1 或更新版本	Horizon Agent 7.8 或更新版本
RHEL 6.6 或更新版本	Horizon Agent 6.2.1 或更新版本
Ubuntu 18.04/16.04	Horizon Agent 7.9 或更新版本
SLED/SLES 12.x SP3	Horizon Agent 7.9 或更新版本

安裝 Horizon Agent 時，您必須先停用 SELinux。您也必須特別選取智慧卡重新導向元件，因為該元件並非預設選取。如需詳細資訊，請參閱 [install_viewagent.sh 命令列選項](#)。

如果在虛擬機器上啟用了智慧卡重新導向功能，則 vSphereClient 的 USB 重新導向無法與智慧卡搭配使用。

智慧卡重新導向一次僅支援一個智慧卡讀取器。如果連接了兩部以上的讀卡機到用戶端系統，此功能將無法運作。

智慧卡重新導向僅支援一張卡片上一個憑證。如果卡片上有多個憑證，則會使用第一個插槽中的憑證，並忽略其他憑證。此行為為 Linux 的限制。

備註 Linux 桌面平台上的智慧卡重新導向支援 PIV 卡。當您使用 Linux 版 HorizonClient 透過 PIV 卡來驗證代理時，您必須將 PIV 智慧卡設定為支援 TLSv1.2，以避免發生 SSL 錯誤。使用 VMware 知識庫文章 <http://kb.vmware.com/kb/2150470> 中所說明的解決方案。

備註 在 Horizon7 (7.0.1 版) 或更新版本中已啟用智慧卡 SSO。RHEL 6.x 桌面平台支援智慧卡 SSO，但 RHEL 7.x 和 RHEL 8.0 桌面平台不支援此功能。

設定智慧卡重新導向

若要設定智慧卡重新導向，請執行下列工作。

- 1 依照 Linux 經銷商與智慧卡廠商提供的指示，為您的桌面平台設定智慧卡。
- 2 依照您的 Linux 發行版所適用的程序，整合您的桌面平台與 Active Directory 網域。
- 3 依照您的 Linux 發行版所適用的程序，在您的桌面平台上設定智慧卡重新導向。

設定 RHEL 8.0 桌面平台的智慧卡重新導向

若要設定 RHEL 8.0 桌面平台的智慧卡方向，請先整合桌面平台與 Active Directory 網域。然後安裝必要的程式庫與根 CA 憑證，然後再安裝 Horizon Agent。

整合 RHEL 8.0 桌面平台與 Active Directory 以支援智慧卡重新導向

請使用下列程序整合 RHEL 8.0 桌面平台與 Active Directory (AD) 網域，以支援智慧卡重新導向。

此程序中的某些範例使用預留位置值來代表您網路組態中的實體，例如 AD 網域的 DNS 名稱。請將預留位置值取代為您的組態特有的資訊，如下表所說明。

預留位置值	說明
<code>dns_IP_ADDRESS</code>	DNS 名稱伺服器的 IP 位址
<code>rhel8sc.rzview2.com</code>	RHEL 8.0 系統的完整主機名稱
<code>rhel8sc</code>	RHEL 8.0 系統的非完整主機名稱
<code>rzview2.com</code>	AD 網域的 DNS 名稱
<code>RZVIEW2.COM</code>	AD 網域的 DNS 名稱 (全部使用大寫字母)
<code>RZVIEW2</code>	包含 Samba 伺服器的工作群組或 NT 網域的 DNS 名稱 (全部使用大寫字母)
<code>rzviewdns.rzview2.com</code>	AD 伺服器的主機名稱

程序

- 在 RHEL 8.0 系統上，執行以下操作。
 - 根據組織要求設定網路和 DNS 設定。
 - 停用 IPv6。
 - 停用自動 DNS。
- 設定 `/etc/hosts` 組態檔，使其具有類似於下列範例的內容。

```
127.0.0.1      rhel8sc.rzview2.com rhel8sc localhost localhost.localdomain localhost4
localhost4.localdomain4
::1           localhost localhost.localdomain localhost6 localhost6.localdomain6

dns_IP_ADDRESS  rzviewdns.rzview2.com
```

- 設定 `/etc/resolv.conf` 組態檔，使其具有類似於下列範例的內容。

```
# Generated by NetworkManager
search rzview2.com
nameserver dns_IP_ADDRESS
```

- 安裝 AD 整合所需的套件。

```
# yum install -y samba-common-tools oddjob-mkhomedir
```

5 啟用 oddjobd 服務。

```
# systemctl enable oddjobd.service
# systemctl start oddjobd.service
```

6 指定系統身分和驗證來源。

```
# authselect select sssd with-smartcard with-mkhomedir
```

7 啟動 oddjobd 服務。

```
# systemctl enable oddjobd.service
# systemctl start oddjobd.service
```

8 若要支援智慧卡驗證，請建立 /etc/sss/sss.conf 檔案。

```
# touch /etc/sss/sss.conf
# chmod 600 touch /etc/sss/sss.conf
# chown root:root /etc/sss/sss.conf
```

9 將所需內容新增到 /etc/sss/sss.conf 中，如下列範例所示。在 [pam] 區段下方指定 pam_cert_auth = True。

```
[sss]
config_file_version = 2
domains = rzview2.com
services = nss, pam, pac

[domain/RZVIEW2.COM]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
cache_credentials = true

[pam]
pam_cert_auth = True
```

10 啟用 sssd 服務。

```
# systemctl enable sssd.service
# systemctl start sssd.service
```

11 編輯 /etc/krb5.conf 組態檔，使其具有類似於下列範例的內容。

```
# To opt out of the system crypto-policies configuration of krb5, remove the
# symlink at /etc/krb5.conf.d/crypto-policies which will not be recreated.
includedir /etc/krb5.conf.d/

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
```

```

admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = /etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
    default_realm = RZVIEW2.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    RZVIEW2.COM = {
        kdc = rzviewdns.rzview2.com
        admin_server = rzviewdns.rzview2.com
        default_domain = rzviewdns.rzview2.com
        pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
        pkinit_cert_match = <KU>digitalSignature
        pkinit_kdc_hostname = rzviewdns.rzview2.com
    }

[domain_realm]
    .rzview2.com = RZVIEW2.COM
    rzview2.com = RZVIEW2.COM

```

12 編輯 /etc/samba/smb.conf 組態檔，使其具有類似於下列範例的內容。

```

[global]
    workgroup = RZVIEW2
    security = ads
    passdb backend = tdbsam
    printing = cups
    printcap name = cups
    load printers = yes
    cups options = raw
    password server = rzviewdns.rzview2.com
    realm = RZVIEW2.COM
    idmap config * : range = 16777216-33554431
    template homedir = /home/RZVIEW2/%U
    template shell = /bin/bash
    kerberos method = secrets and keytab

[homes]
    comment = Home Directories
    valid users = %S, %D%w%S
    browseable = No
    read only = No
    inherit acls = Yes

[printers]
    comment = All Printers
    path = /var/tmp
    printable = Yes

```



```

create mask = 0600
browseable = No

[print$]
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = @printadmin root
force group = @printadmin
create mask = 0664
directory mask = 0775

```

- 13 加入 AD 網域，如下列範例所示。

```
# net ads join -U AdminUser
```

執行 `join` 命令將傳回類似下列範例的輸出。

```

Enter AdminUser's password:
Using short domain name -- RZVIEW2
Joined 'RHEL8SC' to dns domain 'rzview2.com'

```

- 14 確認 RHEL 8.0 桌面平台已成功加入 AD 網域。

```
# net ads testjoin

Join is OK
```

後續步驟

設定 [RHEL 8.0 桌面平台的智慧卡重新導向](#)

設定 RHEL 8.0 桌面平台的智慧卡重新導向

若要在 RHEL 8.0 桌面平台上設定智慧卡重新導向，請安裝此功能所依賴的程式庫、支援受信任的智慧卡驗證所需的根 CA 憑證，以及所需的 PC/SC Lite 程式庫。

必要條件

整合 [RHEL 8.0 桌面平台與 Active Directory](#) 以支援智慧卡重新導向

程序

- 1 安裝所需的程式庫。

```
# yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-tools
```

- 2 啟用 `pcscd` 服務。

```
# systemctl enable pcscd
# systemctl start pcscd
```

- 3 確保 `/etc/sss/sss.conf` 組態檔包含以下行，這會啟用智慧卡驗證。

```
[pam]
pam_cert_auth = True
```

- 4 將所需的 CA 憑證複製到 `/etc/sss/pki/sss_auth_ca_db.pem`。

```
# openssl x509 -inform der -in certificate.cer -out certificate.pem
# cp certificate.pem /etc/sss/pki/sss_auth_ca_db.pem
```

- 5 若要確認智慧卡的狀態，請執行以下 `pkcs11-tool` 命令，並確認命令傳回正確的輸出。

```
# pkcs11-tool -L

# pkcs11-tool --login -0

# pkcs11-tool --test --login
```

- 6 設定 PKCS11 模組。

```
cp libcmP11.so /usr/lib64/
```

- 7 建立 `/usr/share/p11-kit/modules/libcmP11.module` 檔案。在檔案中新增下列內容。

```
# This file describes how to load the opensc module
# See: http://p11-glue.freedesktop.org/doc/p11-kit/config.html

# This is a relative path, which means it will be loaded from
# the p11-kit default path which is usually $(libdir)/pkcs11.
# Doing it this way allows for packagers to package opensc for
# 32-bit and 64-bit and make them parallel installable
module: /usr/lib64/libcmP11.so
priority: 99
```

- 8 將 PC/SC Lite 更新至 1.8.8 版。

```
# yum install -y git flex autoconf automake libtool libudev-devel flex
# git clone https://salsa.debian.org/rousseau/PCSC.git
# cd PCSC
# git checkout -b 1.8.8 pcsc-1.8.8
# ./bootstrap
# ./configure --build=x86_64-redhat-linux-gnu --host=x86_64-redhat-linux-gnu
#   --program-prefix= --disable-dependency-tracking --prefix=/usr --exec-prefix=/usr
#   --bindir=/usr/bin --sbindir=/usr/sbin --sysconfdir=/etc --datadir=/usr/share
#   --includedir=/usr/include --libdir=/usr/lib64 --libexecdir=/usr/libexec
#   --localstatedir=/var --sharedstatedir=/var/lib --mandir=/usr/share/man
#   --infodir=/usr/share/info --disable-static --enable-usbdropdir=/usr/lib64/pcsc/drivers
# make
# make install
```

- 9 安裝 Horizon Agent 7.10 或更新版本，並啟用智慧卡重新導向。

10 將系統重新開機，然後重新登入。

設定 RHEL 7.x/6.x 桌面平台的智慧卡重新導向

若要設定 RHEL 7.x/6.x 桌面平台的智慧卡方向，請先整合桌面平台與 Active Directory 網域。然後安裝必要的程式庫與根 CA 憑證，然後再安裝 Horizon Agent。

整合 RHEL 7.x/6.x 桌面平台與 Active Directory 以支援智慧卡重新導向

若要在 RHEL 7.x/6.x 桌面平台上支援智慧卡重新導向，請使用 Samba 和 Winbind 解決方案整合桌面平台與 Active Directory (AD) 網域。

請使用下列程序整合 RHEL 7.x/6.x 桌面平台與 AD 網域，以支援智慧卡重新導向。

此程序中的某些範例使用預留位置值來代表您網路組態中的實體，例如 AD 網域的 DNS 名稱。請將預留位置值取代為您的組態特有的資訊，如下表所說明。

預留位置值	說明
dns_IP_ADDRESS	DNS 名稱伺服器的 IP 位址
mydomain.com	AD 網域的 DNS 名稱
MYDOMAIN.COM	AD 網域的 DNS 名稱 (全部使用大寫字母)
MYDOMAIN	包含 Samba 伺服器的工作群組或 NT 網域的 DNS 名稱 (全部使用大寫字母)
ads-hostname	AD 伺服器的主機名稱

備註 執行 RHEL 6.0 (或更新版本) 或 RHEL 7.1 (或更新版本) 的桌面平台可支援智慧卡重新導向。

程序

1 在 RHEL 7.x/6.x 桌面平台上，安裝所需的套件。

```
# yum install nscd samba-winbind krb5-workstation pam_krb5 samba-winbind-clients authconfig-gtk
```

2 編輯系統連線的網路設定。開啟 NetworkManager 控制台，並導覽至系統連線的 **IPv4 設定**。針對 [IPv4 方法]，選取 **自動 (DHCP)**。在 **DNS** 文字方塊中，輸入您 DNS 名稱伺服器的 IP 位址。然後，按一下 **套用**。

3 執行下列命令，並確認該命令傳回 RHEL 桌面平台的完整網域名稱 (FQDN)。

```
# hostname -f
```

4 編輯 /etc/resolv.conf 組態檔，如下列範例所示。

```
search mydomain.com
nameserver dns_IP_ADDRESS
```

- 5 在 RHEL 桌面平台上，停用安全增強式 Linux (SELinux)。編輯 `etc/selinux/config` 組態檔，如下列範例所示。

```
SELINUX=disabled
```

- 6 編輯 `/etc/krb5.conf` 組態檔，如下列範例所示。

```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_realm = MYDOMAIN.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname
        admin_server = ads-hostname
        default_domain = ads-hostname
    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM
```

- 7 編輯 `/etc/samba/smb.conf` 組態檔，如下列範例所示。

```
[global]
    workgroup = MYDOMAIN
    password server = ads-hostname
    realm = MYDOMAIN.COM
    security = ads
    idmap config * : range = 16777216-33554431
    template homedir = /home/MYDOMAIN/%U
    template shell = /bin/bash
    kerberos method = secrets and keytab
    winbind use default domain = true
    winbind offline logon = false
    winbind refresh tickets = true

    passdb backend = tdbsam
```

- 8 開啟 `authconfig-gtk` 工具，並如下所示進行設定。
- 選取 **身分識別和驗證** 索引標籤。針對 [使用者帳戶資料庫]，選取 **Winbind**。
 - 選取 **進階選項** 索引標籤，然後選取在第一次登入時建立主目錄核取方塊。

- c 選取**身分識別和驗證**索引標籤，然後按一下**加入網域**。在出現要求您儲存變更的警示時，按一下**儲存**。
- d 在出現提示時，輸入網域管理員的使用者名稱和密碼，然後按一下**確定**。

您的 RHEL 桌面平台便會加入 AD 網域。

- 9 設定 PAM Winbind 的票證快取。編輯 `/etc/security/pam_winbind.conf` 組態檔，使其包含下列範例中顯示的文字行。

```
[global]

# authenticate using kerberos
;krb5_auth = yes

# create homedirectory on the fly
;mkhomedir = yes
```

- 10 重新啟動 Winbind 服務。

```
# sudo service winbind restart
```

- 11 若要確認 AD 加入，請執行下列命令，並確認命令傳回正確的輸出。

- `net ads testjoin`
- `net ads info`

- 12 將系統重新開機，然後重新登入。

後續步驟

設定 [RHEL 7.x/6.x 桌面平台的智慧卡重新導向](#)

設定 RHEL 7.x/6.x 桌面平台的智慧卡重新導向

若要在 RHEL 7.x/6.x 桌面平台上設定智慧卡重新導向，請安裝此功能所依賴的程式庫、驗證所需的根 CA 憑證，以及所需的 PC/SC Lite 程式庫。此外，您還必須編輯某些組態檔以完成驗證設定。

請使用下列程序來設定 RHEL 7.x/6.x 桌面平台的智慧卡重新導向。

此程序中的某些範例使用預留位置值來代表您網路組態中的實體，例如 AD 網域的 DNS 名稱。請將預留位置值取代為您的組態特有的資訊，如下表所說明。

預留位置值	說明
<code>dns_IP_ADDRESS</code>	DNS 名稱伺服器的 IP 位址
<code>mydomain.com</code>	AD 網域的 DNS 名稱
<code>MYDOMAIN.COM</code>	AD 網域的 DNS 名稱 (全部使用大寫字母)
<code>MYDOMAIN</code>	包含 Samba 伺服器的工作群組或 NT 網域的 DNS 名稱 (全部使用大寫字母)
<code>ads-hostname</code>	AD 伺服器的主機名稱

執行 RHEL 6.0 (或更新版本) 或 RHEL 7.1 (或更新版本) 的桌面平台可支援智慧卡重新導向。

備註 如果您使用 vSphere 主控台登入已安裝 Horizon Agent 且已啟用智慧卡重新導向的 RHEL 7.x，則可能會遇到兩分鐘或更長時間的延遲登出時間。此延遲的登出僅會從 vSphere 主控台發生。自 Horizon Client 的 RHEL 7.x 登出體驗不會受到影響。

必要條件

整合 RHEL 7.x/6.x 桌面平台與 Active Directory 以支援智慧卡重新導向

程序

- 1 安裝所需的程式庫。

```
yum install nss-tools nss-pam-ldapd esc pam_pkcs11 pam_krb5 opensc pcsc-lite-ccid authconfig
authconfig-gtk krb5-libs krb5-workstation krb5-pkinit pcsc-lite pcsc-lite-libs
```

- 2 安裝根憑證授權機構 (CA) 憑證。

- a 下載根 CA 憑證，並將其儲存至桌面平台上的 /tmp/certificate.cer。請參閱《[如何匯出根憑證授權機構憑證](#)》。
- b 找出您所下載的根 CA 憑證，並將其傳輸至 .pem 檔案。

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- c 使用 certutil 命令將根 CA 憑證安裝至系統資料庫 /etc/pki/nssdb。

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- d 將根 CA 憑證複製到 /etc/pam_pkcs11/cacerts 目錄。

```
mkdir -p /etc/pam_pkcs11/cacerts

cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

- 3 導覽至 **應用程式 > Sundry > 驗證**，選取 **啟用智慧卡支援** 核取方塊，然後按一下 **套用**。
- 4 複製智慧卡驅動程式，並將驅動程式的程式庫新增至系統資料庫 /etc/pki/nssdb。

```
cp libcmP11.so /usr/lib64/
modutil --add "piv card 2.0" --libfile /usr/lib64/libcmP11.so --dbdir /etc/pki/nssdb/
```

- 5 編輯 /etc/pam_pkcs11/pam_pkcs11.conf 組態檔中的模組設定，如下列範例所示。

```
pkcs11_module coolkey {
    module = libcmP11.so;
    description = "Cool Key";
    slot_num = 0;
```

```
ca_dir = /etc/pam_pkcs11/cacerts;
nss_dir = /etc/pki/nssdb;
cert_policy = ca, signature;
}
```

- 6 編輯 `/etc/pam_pkcs11/cn_map` 檔案，使其包含類似下列範例的內容。若要包含特定內容，請參閱智慧卡憑證中所列的使用者資訊。

```
user sc -> user-sc
```

- 7 編輯 `/etc/krb5.conf/` 組態檔，如下列範例所示。

```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_realm = MYDOMAIN.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname
        admin_server = ads-hostname
        default_domain = ads-hostname
        pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
        pkinit_cert_match = <KU>digitalSignature
        pkinit_kdc_hostname = ads-hostname
    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM
```

- 8 編輯 `/etc/pam.d/system-auth` 組態檔，使其包含下列範例中顯示的文字行。

```
auth optional pam_krb5.so use_first_pass no_subsequent_prompt
preauth_options=X509_user_identity=PKCS11:/usr/lib64/libcsp11.so
```

- 9 重新啟動 PC/SC 精靈。

```
chkconfig pcscd on
service pcscd start
```

- 10 安裝您的 RHEL 發行版所需的 PC/SC Lite 版本。

- 針對 RHEL 7.x，請安裝 PC/SC Lite 1.8.8 版。

```
yum install git flex autoconf automake libtool libudev-devel flex
git clone https://salsa.debian.org/rousseau/PCSC.git
cd PCSC
git checkout -b 1.8.8 pcsc-1.8.8
./bootstrap
```

```
./configure --build=x86_64-redhat-linux-gnu --host=x86_64-redhat-linux-gnu --program-prefix=
--disable-dependency-tracking --prefix=/usr --exec-prefix=/usr --bindir=/usr/bin --
sbindir=/usr/sbin
--sysconfdir=/etc --datadir=/usr/share --includedir=/usr/include --libdir=/usr/lib64
--libexecdir=/usr/libexec --localstatedir=/var --sharedstatedir=/var/lib --mandir=/usr/
share/man
--infodir=/usr/share/info --disable-static --enable-usbdropdir=/usr/lib64/pcsc/drivers
make
make install
```

- 針對 RHEL 6.x，請安裝 PC/SC Lite 1.7.4 版。

```
yum groupinstall "Development tools"
yum install libudev-devel
service pcscd stop
wget https://alioth.debian.org/frs/download.php/file/3598/pcsc-lite-1.7.4.tar.bz2
tar -xjvf pcsc-lite-1.7.4.tar.bz2
cd ./pcsc-lite-1.7.4
./configure --prefix=/usr/ --libdir=/usr/lib64/ --enable-usbdropdir=/usr/lib64/pcsc/drivers
--enable-conffdir=/etc --enable-ipcdirdir=/var/run --disable-libusb --disable-serial --disable-
usb
--disable-libudev
make
make install
service pcscd start
```

11 安裝 Horizon Agent 套件，並啟用智慧卡重新導向。

```
sudo ./install_viewagent.sh -m yes
```

安裝您的 RHEL 發行版所需的套件：

- 針對 RHEL 7.x，請安裝 Horizon Agent 7.8 或更新版本。
- 針對 RHEL 6.x，請安裝 View Agent 6.2.1 或更新版本。

12 將系統重新開機，然後重新登入。

設定 Ubuntu 桌面平台的智慧卡重新導向

若要設定 Ubuntu 桌面平台的智慧卡方向，請先整合桌面平台與 Active Directory 網域。然後安裝必要的程式庫與根 CA 憑證，然後再安裝 Horizon Agent。

整合 Ubuntu 桌面平台與 Active Directory 以支援智慧卡重新導向

若要在 Ubuntu 桌面平台上支援智慧卡重新導向，請使用 Samba 和 Winbind 解決方案整合桌面平台與 Active Directory (AD) 網域。

請使用下列程序整合 Ubuntu 桌面平台與 AD 網域，以支援智慧卡重新導向。

此程序中的某些範例使用預留位置值來代表您網路組態中的實體，例如 AD 網域的 DNS 名稱。請將預留位置值取代為您的組態特有的資訊，如下表所說明。

預留位置值	說明
dns_IP_ADDRESS	DNS 名稱伺服器的 IP 位址
mydomain.com	AD 網域的 DNS 名稱
MYDOMAIN.COM	AD 網域的 DNS 名稱 (全部使用大寫字母)
MYDOMAIN	包含 Samba 伺服器的工作群組或 NT 網域的 DNS 名稱 (全部使用大寫字母)
ads-hostname	AD 伺服器的主機名稱
ads-hostname.mydomain.com	AD 伺服器的完整網域名稱 (FQDN)
mytimeserver.mycompany.com	NTP 時間伺服器的 DNS 名稱
AdminUser	Linux 桌面平台管理員的使用者名稱

程序

- 1 在您的 Ubuntu 桌面平台上編輯 `/etc/hostname` 組態檔，以定義桌面平台的主機名稱。
- 2 設定 DNS。
 - a 將 DNS 伺服器名稱和 IP 位址新增至 `/etc/hosts` 組態檔。
 - b 將您 DNS 名稱伺服器的 IP 位址和 AD 網域的 DNS 名稱新增至 `/etc/network/interfaces` 組態檔，如下列範例所示。

```
dns-nameservers dns_IP_ADDRESS
dns-search mydomain.com
```

- 3 安裝 `resolvconf` 套件。

- a 執行安裝命令。

```
# apt-get install -y resolvconf
```

允許系統安裝套件並重新開機。

- b 確認您位於 `/etc/resolv.conf` 檔案中的 DNS 組態，如下列範例所示。

```
# cat /etc/resolv.conf
...
nameserver dns_IP_ADDRESS
search mydomain.com
```

4 設定網路時間同步化。

a 安裝 ntpdate 套件。

```
# apt-get install -y ntpdate
```

b 將 NTP 伺服器資訊新增至 /etc/systemd/timesyncd.conf 組態檔，如下列範例所示。

```
[Time]
NTP=mytimeserver.mycompany.com
```

5 重新啟動 NTP 服務。

```
sudo service ntpdate restart
```

6 安裝所需的 AD 加入套件。

a 執行安裝命令。

```
# apt-get install -y samba krb5-config krb5-user winbind libpam-winbind
libnss-winbind
```

b 在安裝提示字元要求您提供預設 Kerberos 領域時，以大寫字母輸入 AD 網域的 DNS 名稱 (例如 MYDOMAIN.COM)。然後，選取**確定**。

7 編輯 /etc/krb5.conf 組態檔，如下列範例所示。

```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_realm = MYDOMAIN.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname.mydomain.com
        admin_server = ads-hostname.mydomain.com
        default_domain = ads-hostname.mydomain.com
        pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
        pkinit_cert_match = <KU>digitalSignature
        pkinit_kdc_hostname = ads-hostname.mydomain.com
    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM
```

- 8 若要確認 Kerberos 憑證，請執行下列命令。

```
# kinit Administrator@MYDOMAIN.COM

# klist
```

確認命令傳回的輸出與下列範例類似。

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@MYDOMAIN.COM
principal
2019-05-27T17:12:03    2019-05-28T03:12:03    krbtgt/MYDOMAIN.COM@MYDOMAIN.COM
renew until 2019-05-28T17:12:03
```

- 9 編輯 /etc/samba/smb.conf 組態檔，如下列範例所示。

```
[global]
    workgroup = MYDOMAIN
    realm = MYDOMAIN.COM
    password server = ads-hostname.mydomain.com
    security = ads
    kerberos method = secrets only
    winbind use default domain = true
    winbind offline logon = false
    template homedir = /home/%D/%U
    template shell = /bin/bash
    client use spnego = yes
    client ntlmv2 auth = yes
    encrypt passwords = yes
    passdb backend = tdbsam
    winbind enum users = yes
    winbind enum groups = yes
    idmap uid = 10000-20000
    idmap gid = 10000-20000
```

- 10 加入 AD 網域，並檢查整合。

- a 執行 AD 加入命令。

```
# net ads join -U AdminUser@mydomain.com
# systemctl stop samba-ad-dc
# systemctl enable smbd nmbd winbind
# systemctl restart smbd nmbd winbind
```

- b 修改 /etc/nsswitch.conf 組態檔，如下列範例所示。

```
passwd:    compat systemd winbind
group:     compat systemd winbind
shadow:    compat
gshadow:   files
```

- c 若要查看 AD 加入的結果，請執行下列命令，並確認命令傳回正確的輸出。

```
# wbinfo -u

# wbinfo -g
```

- d 若要查看 Winbind 名稱服務切換，請執行下列命令，並確認命令傳回正確的輸出。

```
# getent group|grep 'domain admins'

# getent passwd|grep 'ads-hostname'
```

11 啟用所有 PAM 設定檔。

```
# pam-auth-update
```

在 [PAM 組態] 畫面中，選取所有 PAM 設定檔，包括在登入時建立主目錄，然後選取**確定**。

12 在 Ubuntu 16.04 上，在登入畫面中啟用使用者切換。修改 /usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf 檔案，如下列範例所示。

```
user-session=ubuntu
greeter-show-manual-login=true
```

後續步驟

設定 [Ubuntu 桌面平台的智慧卡重新導向](#)

設定 Ubuntu 桌面平台的智慧卡重新導向

若要在 Ubuntu 桌面平台上設定智慧卡重新導向，請安裝該功能所依賴的程式庫，和支援受信任的智慧卡驗證所需的根 CA 憑證。此外，您還必須編輯某些組態檔以完成驗證設定。

此程序中的某些範例使用預留位置值來代表您網路組態中的實體，例如 AD 網域的 DNS 名稱。請將預留位置值取代為您的組態特有的資訊，如下表所說明。

預留位置值	說明
dns_IP_ADDRESS	DNS 名稱伺服器的 IP 位址
mydomain.com	AD 網域的 DNS 名稱
MYDOMAIN.COM	AD 網域的 DNS 名稱 (全部使用大寫字母)
MYDOMAIN	包含 Samba 伺服器的工作群組或 NT 網域的 DNS 名稱 (全部使用大寫字母)
ads-hostname	AD 伺服器的主機名稱
ads-hostname.mydomain.com	AD 伺服器的完整網域名稱 (FQDN)
mytimeserver.mycompany.com	NTP 時間伺服器的 DNS 名稱
AdminUser	Linux 桌面平台管理員的使用者名稱

必要條件

整合 [Ubuntu](#) 桌面平台與 [Active Directory](#) 以支援智慧卡重新導向

程序

- 1 安裝所需的程式庫。

```
# apt-get install -y pcscd pcsc-tools pkg-config libpam-pkcs11 opensc  
libengine-pkcs11-openssl libnss3-tools
```

- 2 安裝根憑證授權機構 (CA) 憑證。

- a 下載根 CA 憑證，並將其儲存至桌面平台上的 `/tmp/certificate.cer`。請參閱《[如何匯出根憑證授權機構憑證](#)》。
- b 找出您所下載的根 CA 憑證，並將其傳輸至 `.pem` 檔案。

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- c 使用 `certutil` 命令將根 CA 憑證安裝至系統資料庫 `/etc/pki/nssdb`。

```
# certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- d 將根 CA 憑證複製到 `/etc/pam_pkcs11/cacerts` 目錄。

```
# mkdir -p /etc/pam_pkcs11/cacerts  
  
# cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

- 3 建立 `pkcs11` 雜湊檔案。

```
# chmod a+r certificate.pem  
# pkcs11_make_hash_link
```

4 複製所需的驅動程式，並將所需的程式庫檔案新增至 `nssdb` 目錄。

a 執行下列命令。

```
# cp libcmP11.so /usr/lib/
# mkdir -p /etc/pki/nssdb
# certutil -N -d /etc/pki/nssdb
# certutil -A -n rootca -i certificate.pem -t "CT,CT,CT" -d /etc/pki/nssdb
# modutil -dbdir /etc/pki/nssdb/ -add "piv card 2.0" -libfile /usr/lib/libcmP11.so
```

b 確認預期的憑證已成功載入。

```
# certutil -L -d /etc/pki/nssdb

Certificate Nickname

rootca
```

c 確認預期的程式庫已成功新增。

```
modutil -dbdir /etc/pki/nssdb -list

Listing of PKCS #11 Modules
-----
1. NSS Internal PKCS #11 Module
   slots: 2 slots attached
   status: loaded

   slot: NSS Internal Cryptographic Services
   token: NSS Generic Crypto Services

   slot: NSS User Private Key and Certificate Services
   token: NSS Certificate DB

2. piv card 2.0
   library name: /usr/lib/libcmP11.so
   slots: There are no slots attached to this module
   status: loaded
-----
```

5 設定 pam_pkcs11 程式庫。

- a 使用預設範例內容建立 `pam_pkcs11.conf` 檔案。

```
# mkdir /etc/pam_pkcs11
# zcat /usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz |
tee /etc/pam_pkcs11/pam_pkcs11.conf
```

- b 編輯 `/etc/pam_pkcs11/pam_pkcs11.conf` 檔案，如下列範例所示。

```
use_pkcs11_module = mysc;

pkcs11_module mysc {
    module = /usr/lib/libcmP11.so;
    description = "LIBCMP11";
    slot_num = 0;
    ca_dir = /etc/pki/cacerts;
    nss_dir = /etc/pki/nssdb;
    cert_policy = ca;
}
...
use_mappers = cn, null;
...
mapper cn {
    debug = false;
    module = internal;
    # module = /lib/pam_pkcs11/cn_mapper.so;
    ignorecase = true;
    mapfile = file:///etc/pam_pkcs11/cn_map;
    # mapfile = "none";
}
```

- c 編輯 `/etc/pam_pkcs11/cn_map` 檔案，使其包含以下這一行。

```
ads-hostname -> ads-hostname
```

6 設定 PAM 驗證。

- a 編輯 `/etc/pam.d/gdm-password` 組態檔。將 `pam_pkcs11.so` 授權行放在 `common-auth` 這一行前面，如下列範例所示。

```
#%PAM-1.0
auth    requisite      pam_nologin.so
auth    required        pam_succeed_if.so user != root quiet_success
auth    sufficient
pam_pkcs11.so
@include common-auth
auth    optional        pam_gnome_keyring.so
@include common-account
```

- b 針對 Ubuntu 16.04，請編輯 `/etc/pam.d/lightdm` 組態檔。將 `pam_pkcs11.so` 授權行放在 `common-auth` 這一行前面，如下列範例所示。

```
#%PAM-1.0
auth    requisite      pam_nologin.so debug
auth    sufficient      pam_succeed_if.so user ingroup nopasswdlogin debug
auth    [success=3 default=ignore]      pam_pkcs11.so
@include common-auth
auth    optional        pam_gnome_keyring.so
auth    optional        pam_kwallet.so
```

- c 針對 Ubuntu 16.04，請編輯 `/etc/pam.d/unity` 組態檔。將 `pam_pkcs11.so` 授權行放在 `common-auth` 這一行前面，如下列範例所示。

```
auth    [success=3 default=ignore]      pam_pkcs11.so
@include common-auth
auth    optional        pam_gnome_keyring.so
```

- 7 若要確認智慧卡硬體和安裝在智慧卡上的憑證，請執行下列命令。

```
# pcsc_scan

# pkcs11_listcerts

# pkcs11_inspect
```


8 設定 Gnome 螢幕保護程式，使其會在智慧卡移除時鎖定。

a 安裝螢幕保護程式套件。

```
# apt-get install gnome-screensaver
```

b 若要設定螢幕保護程式，請編輯 `/etc/pam_pkcs11/pkcs11_eventmgr.conf` 檔案，如下列範例所示。

```
pkcs11_eventmgr {
    # Run in background? Implies debug=false if true
    daemon = true;

    # show debug messages?
    debug = false;

    # polling time in seconds
    polling_time = 1;

    # expire time in seconds
    # default = 0 ( no expire )
    expire_time = 0;

    # pkcs11 module to use
    pkcs11_module = /usr/lib/libcmP11.so;

    #
    # list of events and actions
    # Card inserted
    event card_insert {
        # what to do if an action fail?
        # ignore : continue to next action
        # return : end action sequence
        # quit : end program
        on_error = ignore ;

        # You can enter several, comma-separated action entries
        # they will be executed in turn
        action = "gnome-screensaver-command --poke";
    }

    # Card has been removed
    event card_remove {
        on_error = ignore;
        action = "gnome-screensaver-command --lock";
    }

    # Too much time card removed
    event expire_time {
```

```

    on_error = ignore;
    action = "/bin/false";
}
}

```

- c 執行 `pkcs11_eventmgr`。

```
# /usr/bin/pkcs11_eventmgr &
```

- 9 安裝 Horizon Agent 套件，並啟用智慧卡重新導向。

```
# sudo ./install_viewagent.sh -m yes
```

備註 您必須安裝 Horizon Agent 7.9 或更新版本。

- 10 將系統重新開機，然後重新登入。

設定 SLED/SLES 桌面平台的智慧卡重新導向

若要設定 SLED/SLES 桌面平台的智慧卡方向，請先整合桌面平台與 Active Directory 網域。然後安裝必要的程式庫與根 CA 憑證，然後再安裝 Horizon Agent。

整合 SLED/SLES 桌面平台與 Active Directory 以支援智慧卡重新導向

若要在 SLED/SLES 桌面平台上支援智慧卡重新導向，請使用 Samba 和 Winbind 解決方案整合桌面平台與 Active Directory (AD) 網域。

請使用下列程序整合 SLED/SLES 桌面平台與 AD 網域，以支援智慧卡重新導向。

此程序中的某些範例使用預留位置值來代表您網路組態中的實體，例如 AD 網域的 DNS 名稱。請將預留位置值取代為您的組態特有的資訊，如下表所說明。

預留位置值	說明
<code>dns_IP_ADDRESS</code>	DNS 名稱伺服器的 IP 位址
<code>mydomain.com</code>	AD 網域的 DNS 名稱
<code>MYDOMAIN.COM</code>	AD 網域的 DNS 名稱 (全部使用大寫字母)
<code>MYDOMAIN</code>	包含 Samba 伺服器的工作群組或 NT 網域的 DNS 名稱 (全部使用大寫字母)
<code>ads-hostname</code>	AD 伺服器的主機名稱
<code>ads-hostname.mydomain.com</code>	AD 伺服器的完整網域名稱 (FQDN)
<code>mytimeserver.mycompany.com</code>	NTP 時間伺服器的 DNS 名稱
<code>AdminUser</code>	Linux 桌面平台管理員的使用者名稱

程序

- 1 設定您 SLED/SLES 桌面平台的網路設定。
 - a 藉由編輯 `/etc/hostname` 和 `/etc/hosts` 組態檔來定義桌面平台的主機名稱。
 - b 設定 DNS 伺服器 IP 位址，並停用**自動 DNS**。對於 SLES 12 SP3，也請停用**透過 DHCP 變更主機名稱**。
 - c 若要設定網路時間同步化，請將您的 NTP 伺服器資訊新增至 `/etc/ntp.conf` 檔案，如下列範例所示。

```
server mytimeserver.mycompany.com
```

- 2 安裝所需的 AD 加入套件。

```
# zypper in krb5-client samba-winbind
```

3 編輯所需的組態檔。

- a 編輯 `/etc/samba/smb.conf` 檔案，如下列範例所示。

```
[global]
    workgroup = MYDOMAIN
    usershare allow guests = NO
    idmap gid = 10000-20000
    idmap uid = 10000-20000
    kerberos method = secrets and keytab
    realm = MYDOMAIN.COM
    security = ADS
    template homedir = /home/%D/%U
    template shell = /bin/bash
    winbind use default domain=true
    winbind offline logon = yes
    winbind refresh tickets = yes

[homes]
    ...
```

- b 編輯 `/etc/krb5.conf/` 檔案，如下列範例所示。

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    clocks skew = 300

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname.mydomain.com
        default_domain = mydomain.com
        admin_server = ads-hostname.mydomain.com
    }

[logging]
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log
    default = SYSLOG:NOTICE:DAEMON

[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM

[appdefaults]
    pam = {
        ticket_lifetime = 1d
        renew_lifetime = 1d
        forwardable = true
        proxiable = false
        minimum_uid = 1
    }
```

- c 編輯 `/etc/security/pam_winbind.conf` 檔案，如下列範例所示。

```
cached_login = yes
krb5_auth = yes
krb5_ccache_type = FILE
```

- d 編輯 `/etc/nsswitch.conf` 檔案，如下列範例所示。

```
passwd: compat winbind
group: compat winbind
```

- 4 加入 AD 網域，如下列範例所示。

```
# net ads join -U AdminUser
```

- 5 啟用 Winbind 服務。

- a 若要啟用並啟動 Winbind，請執行以下一系列的命令。

```
# pam-config --add --winbind
# pam-config -a --mkhomedir
# systemctl enable winbind
# systemctl start winbind
```

- b 若要確定 AD 使用者可直接登入桌面平台而無須重新啟動 Linux 伺服器，請執行以下一系列的命令。

```
# systemctl stop nscd
# nscd -i passwd
# nscd -i group
# systemctl start nscd
```

- 6 若要確認 AD 加入成功，請執行下列命令，並確認命令傳回正確的輸出。

```
# wbinfo -u

# wbinfo -g
```

後續步驟

設定 [SLED/SLES 桌面平台的智慧卡重新導向](#)

設定 SLED/SLES 桌面平台的智慧卡重新導向

若要在 SLED/SLES 桌面平台上設定智慧卡重新導向，請安裝該功能所依賴的程式庫，和支援受信任的智慧卡驗證所需的根 CA 憑證。此外，您還必須編輯某些組態檔以完成驗證設定。

此程序中的某些範例使用預留位置值來代表您網路組態中的實體，例如 AD 網域的 DNS 名稱。請將預留位置值取代為您的組態特有的資訊，如下表所說明。

預留位置值	說明
dns_IP_ADDRESS	DNS 名稱伺服器的 IP 位址
mydomain.com	AD 網域的 DNS 名稱
MYDOMAIN.COM	AD 網域的 DNS 名稱 (全部使用大寫字母)
MYDOMAIN	包含 Samba 伺服器的工作群組或 NT 網域的 DNS 名稱 (全部使用大寫字母)
ads-hostname	AD 伺服器的主機名稱
ads-hostname.mydomain.com	AD 伺服器的完整網域名稱 (FQDN)
mytimeserver.mycompany.com	NTP 時間伺服器的 DNS 名稱
AdminUser	Linux 桌面平台管理員的使用者名稱

必要條件

整合 [SLED/SLES 桌面平台與 Active Directory](#) 以支援智慧卡重新導向

程序

1 安裝所需的程式庫套件。

a 安裝 PAM 程式庫和其他套件。

```
# zypper install pam_pkcs11 mozilla-nss mozilla-nss-tools
pcsc-lite pcsc-ccid opensc coolkey pcsc-tools
```

b 若要安裝 PC/SC 工具，請執行以下一系列的命令。

```
# SUSEConnect --list-extensions
# SUSEConnect -p PackageHub/12.3/x86_64
# zypper in pcsc-tools
```

2 安裝根憑證授權機構 (CA) 憑證。

a 下載根 CA 憑證，並將其儲存至桌面平台上的 /tmp/certificate.cer。請參閱《[如何匯出根憑證授權機構憑證](#)》。

b 找出您下載的根 CA 憑證，並將其傳輸至 .pem 檔案，然後建立雜湊檔案。

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
# cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
# chmod a+r /etc/pam_pkcs11/cacerts/certificate.pem
# cd /etc/pam_pkcs11/cacerts
# pkcs11_make_hash_link
```

- c 將信賴起點安裝至 NSS 資料庫。

```
# mkdir /etc/pam_pkcs11/nssdb
# certutil -N -d /etc/pam_pkcs11/nssdb
# certutil -L -d /etc/pam_pkcs11/nssdb
# certutil -A -n rootca -i certificate.pem -t "CT,CT,CT" -d /etc/pam_pkcs11/nssdb
```

- d 安裝所需的驅動程式。

```
# cp libcmP11.so /usr/lib64/
# modutil -add "piv card 2.0" -libfile /usr/lib64/libcmP11.so -dbdir /etc/pam_pkcs11/nssdb/
```

3 編輯 /etc/pam_pkcs11/pam_pkcs11.conf 檔案。

- a 刪除 `use_pkcs11_module = nss` 這一行。在其位置新增 `use_pkcs11_module = mysc` 這一行。
- b 新增 `mysc` 模組，如下列範例所示。

```
pkcs11_module mysc {
    module = /usr/lib64/libcmP11.so;
    description = "MY Smartcard";
    slot_num = 0;
    nss_dir = /etc/pam_pkcs11/nssdb;
    cert_policy = ca, ocsf_on, signature, crl_auto;
}
```

- c 更新一般名稱對應程式組態，如下列範例所示。

```
# Assume common name (CN) to be the login
mapper cn {
    debug = false;
    module = internal;
    # module = /usr/lib64/pam_pkcs11/cn_mapper.so;
    ignorecase = true;
    mapfile = file:///etc/pam_pkcs11/cn_map;}
```

- d 刪除 `use_mappers = ms` 這一行。在其位置新增 `se_mappers = cn, null` 這一行。

4 編輯 /etc/pam_pkcs11/cn_map 組態檔，使其包含以下這一行。

```
ads-hostname -> ads-hostname
```

5 修改 PAM 組態。

- a 若要能夠設定智慧卡驗證，請先停用 `pam_config` 工具。

```
# find /etc/pam.d/ -type l -iname "common-*" -delete
# for X in /etc/pam.d/common-*-pc; do cp -ivp $X ${X:0:-3}; done
```

- b 在 `/etc/pam.d/` 目錄下建立名為 `common-auth-smartcard` 的檔案。在檔案中新增下列內容。

```
auth    required      pam_env.so
auth    sufficient     pam_pkcs11.so
auth    optional       pam_gnome_keyring.so
auth    [success=1 default=ignore] pam_unix.so nullok_secure try_first_pass
auth    required       pam_winbind.so use_first_pass
```

- c 針對 SLED/SLES 12 SP3，請在以下兩個檔案中，將 `auth include common-auth` 一行取代為 `auth include common-auth-smartcard` 這一行：`/etc/pam.d/gdm` 和 `/etc/pam.d/xscreensaver`。

6 停用防火牆。

```
# rcSuSEfirewall2 stop
# chkconfig SuSEfirewall2_setup off
# chkconfig SuSEfirewall2_init off
```

備註 防火牆啟用時，智慧卡重新導向有時會失敗。

7 安裝智慧卡重新導向所需的程式庫套件。

- a 針對 SLED/SLES 12 SP3，請執行下列安裝命令。

```
# SUSEConnect -p sle-sdk/12.3/x86_64
# zypper in git autoconf automake libtool flex libudev-devel gcc
```

- b 針對 SLES 12 SP3，請安裝 `systemd-devel`。

```
# zypper in systemd-devel
```

8 安裝 Horizon Agent 套件，並啟用智慧卡重新導向。

```
# sudo ./install_viewagent.sh -m yes
```

備註 您必須安裝 Horizon Agent 7.9 或更新版本。

9 將系統重新開機，然後重新登入。

設定 True SSO for Linux 桌面平台

True Single Sign-On (True SSO) 功能可在使用者首次登入 VMware Identity Manager 後，授與使用者對 Linux 虛擬桌面平台或已發佈桌面平台或應用程式的存取權。使用者可以使用智慧卡或 RSA SecurID 或

RADIUS 驗證登入 VMware Identity Manager，然後在不輸入其 Active Directory 認證的情況下存取遠端 Linux 資源。

如果使用者使用 Active Directory (AD) 認證進行驗證，則不需要 True SSO 功能。不過，您可以設定即使在這種情況下仍使用 True SSO，以便桌面平台可以同時支援 AD 認證和 True SSO。

連線至 Linux 虛擬桌面平台或已發佈的桌面平台或應用程式時，使用者可以選取使用原生 Horizon Client 或 HTML Access。

True SSO 具有下列限制：

- 只有使用下列發行版的桌面平台可支援此功能：RHEL/CentOS 8.0、RHEL/CentOS 7.x、Ubuntu 16.04 和 18.04，以及 SLED/SLES 12.x SP3。
- 在 RHEL/CentOS 7.x 桌面平台上，此功能僅支援下列加入方法：預設加入網域工具、Samba、系統安全服務精靈 (SSSD)，以及 Kerberos 網路驗證通訊協定。

若要在 Linux 環境中設定 True SSO，請執行下列工作。

- 1 在 Horizon 7 環境中安裝和設定 True SSO。請參閱《Horizon 7 管理》文件中的〈設定 True SSO〉。
- 2 依照您的 Linux 發行版所適用的程序，整合您的桌面平台與 AD 網域。
- 3 依照您的 Linux 發行版所適用的程序，在您的桌面平台上設定 True SSO。

在 RHEL/CentOS 8.0 桌面平台上設定 True SSO

若要在 RHEL/CentOS 8.0 桌面平台上支援 True SSO，您必須先將系統與 Active Directory (AD) 網域整合。接著，您必須修改系統上的特定組態以支援 True SSO 功能。

備註 即時複製 RHEL 8.0 桌面平台不支援 True SSO。

此程序中的某些範例使用預留位置值來代表您網路組態中的實體，例如 AD 網域的 DNS 名稱。請將預留位置值取代為您的組態特有的資訊，如下表所說明。

預留位置值	說明
mydomain.com	AD 網域的 DNS 名稱
MYDOMAIN.COM	AD 網域的 DNS 名稱 (全部使用大寫字母)
MYDOMAIN	NetBIOS 網域的名稱

必要條件

- 確認 Active Directory (AD) 伺服器可在 RHEL/CentOS 8.0 系統上由 DNS 解析。
- 設定系統的主機名稱。
- 設定系統上的網路時間通訊協定 (NTP)。

程序

- 1 在 RHEL/CentOS 8.0 系統上，確認與 Active Directory 的網路連線。

```
# realm discover mydomain.com
```

- 2 安裝所需的相依性套件。

```
# yum install oddjob oddjob-mkhomedir sssd adcli samba-common-tools
```

- 3 加入 AD 網域。

```
# realm join --verbose mydomain.com -U administrator
```

- 4 下載根 CA 憑證，並將其複製到所需的目錄作為 .pem 檔案。

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem

# cp /tmp/certificate.pem /etc/sss/pki/sss_auth_ca_db.pem
```

- 5 修改 /etc/sss/sss.conf 組態檔，如下列範例所示。

```
[sss]
domains = mydomain.com
config_file_version = 2
services = nss, pam

[domain/mydomain.com]
ad_domain = mydomain.com
krb5_realm = IMYDOMAIN.COM
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False          <----- Use short name for user
fallback_homedir = /home/%u@%d
access_provider = ad
ad_gpo_map_interactive = +gdm-vmwcred      <----- Add this line for SSO

[pam]                                     <----- Add pam section for certificate login
pam_cert_auth = True                     <----- Add this line to enable certificate
login for system
pam_p11_allowed_services = +gdm-vmwcred  <----- Add this line to enable certificate
login for VMware Horizon Agent

[certmap/mydomain.com/truesso]           <----- Add this section and following lines to
set match and map rule for certificate user
matchrule = <EKU>msScLogin
maprule = (&(|(userPrincipal={subject_principal})(samAccountName={subject_principal.short_name}))
domains = mydomain.com
priority = 10
```

6 安裝 Horizon Agent 套件，並啟用 True SSO。

備註 您必須安裝 Horizon Agent 7.11 或更新版本。

```
# sudo ./install_viewagent.sh -T yes
```

7 修改 /etc/vmware/viewagent-custom.conf 組態檔，使其包含下列行。

```
NetbiosDomain = MYDOMAIN
```

8 將系統重新開機，然後重新登入。

設定 RHEL/CentOS 7.x 桌面平台的 True SSO

若要設定 RHEL/CentOS 7.x 桌面平台的 True SSO，請先整合桌面平台與 Active Directory 網域。然後安裝所需的程式庫與根 CA 憑證，然後再安裝 Horizon Agent。

整合 RHEL/CentOS 7.x 桌面平台與 Active Directory 以支援 True SSO

若要在 RHEL/CentOS 7.x 系統上 Horizon 7 Linux 桌面平台環境中的即時複製虛擬機器上支援 True SSO，您必須在主要 Linux 虛擬機器上設定 Samba。

透過 RHEL/CentOS 7.x `realmd` 功能提供簡單的方式來探索並加入身分識別網域。`realmd` 會設定基礎 Linux 系統服務 (例如 SSSD 或 Winbind)，以連線至網域，而不是將系統連線至網域本身。下列步驟描述如何使用 `realmd` 與 Samba 執行 RHEL/CentOS 7.x 桌面平台對 Active Directory 的離線網域加入。

必要條件

- RedHat Enterprise Linux (RHEL) 系統已訂閱 Red Hat Network (RHN) 或已在本機安裝 `yum` 工具。
- 在 Linux 系統上，Active Directory (AD) 伺服器可由 DNS 解析。
- 網路時間通訊協定 (NTP) 會設定於 Linux 系統上。

程序

- 1 確認 RHEL/CentOS 系統可以探索到 AD 伺服器。使用下列範例，其中必須將 `ADdomain.example.com` 以您的 AD 伺服器資訊取代。

```
sudo realm discover ADdomain.example.com
```

- 2 安裝 Samba `tdb-tools` 套件。

Samba `tdb-tools` 套件無法從官方 Red Hat 存放庫下載。您必須手動下載套件。例如，請使用下列命令從 CentOS 7.5 系統下載此套件，然後將下載的套件安裝到您的 RHEL 系統。

```
yumdownloader tdb-tools
```

如果您沒有 CentOS 系統，請移至 <https://rpmfind.net/linux/rpm2html/search.php?query=tdb-tools&submit=Search+...&system=&arch=>，下載 `tdb-tools-1.3.15-1.el7.x86_64.rpm` 套件，然後將它安裝到您的 RHEL 系統。

3 安裝 Samba 和相依性套件。

```
sudo yum install sssd-tools sssd adcli samba-common pam_ldap pam_krb5 samba samba-client krb5-workstation
```

4 使用下列範例來執行 join 命令，其中必須將 *DNSdomain.example.com* 取代為您環境專用的 DNS 網域路徑。

```
sudo realm join DNSdomain.example.com -U administrator
```

加入命令成功之後，您會收到下列訊息。

```
已成功在領域中註冊機器
```

5 將系統重新開機，然後重新登入。

後續步驟

在 [RHEL/CentOS 7.x 桌面平台上設定 True SSO](#)

在 RHEL/CentOS 7.x 桌面平台上設定 True SSO

若要在 RHEL/CentOS 7.x 桌面平台上啟用 True SSO 功能，請安裝 True SSO 功能所依賴的程式庫、支援受信任驗證所需的根 CA 憑證，以及 Horizon Agent。此外，您還必須編輯某些組態檔以完成驗證設定。

請使用下列程序在 RHEL 7.x 和 CentOS 7.x 桌面平台上啟用 True SSO。若要在這些桌面平台上支援 True SSO，您必須安裝 Horizon Agent 7.6 或更新版本。

此程序中的某些範例使用預留位置值來代表您網路組態中的實體，例如 AD 網域的 DNS 名稱。請將預留位置值取代為您的組態特有的資訊，如下表所說明。

預留位置值	說明
dns_server	DNS 名稱伺服器路徑
mydomain.com	AD 網域的 DNS 名稱
MYDOMAIN.COM	AD 網域的 DNS 名稱 (全部使用大寫字母)

必要條件

- 針對 VMware Identity Manager 和 Horizon Connection Server 設定 True SSO。
- [整合 RHEL/CentOS 7.x 桌面平台與 Active Directory 以支援 True SSO](#)
- 取得根憑證授權機構憑證，並將其儲存至 RHEL/CentOS 7.x 桌面平台上的 /tmp/certificate.cer。請參閱《[如何匯出根憑證授權機構憑證](#)》。

程序

1 安裝 PKCS11 支援套件群組。

```
yum install -y nss-tools nss-pam-ldapd pam_krb5 krb5-libs krb5-workstation krb5-pkinit
```

2 安裝根憑證授權機構 (CA) 憑證。

- a 找出您所下載的根 CA 憑證，並將其傳輸至 .pem 檔案。

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- b 使用 `certutil` 命令將根 CA 憑證安裝至系統資料庫 `/etc/pki/nssdb`。

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- c 將根 CA 憑證新增至 RHEL/CentOS 7.x 系統上受信任的 CA 憑證清單，並使用 `update-ca-trust` 命令更新全系統的信任存放區組態。

```
cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
update-ca-trust
```

3 在系統的 SSSD 組態檔中為您的網域修改適當的區段，如下列範例所示。

```
[domain/mydomain.com]
ad_domain = mydomain.com
krb5_realm = MYDOMAIN.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
#set the next line to false, so you can use the short name instead of the full domain name.
use_fully_qualified_names = False
fallback_homedir = /home/%u@%d
access_provider = ad
```

4 修改 Kerberos 組態檔 `/etc/krb5.conf`，如下列範例所示。

```
[libdefaults]
dns_lookup_realm = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
default_ccache_name = KEYRING:persistent:%{uid}
# Add following line, if the system doesn't add it automatically
default_realm = MYDOMAIN.COM

[realms]
MYDOMAIN.COM = {
    kdc = dns_server
    admin_server = dns_server
    # Add the following three lines for pkinit_*
    pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
    pkinit_kdc_hostname = your_org_DNS_server
    pkinit_eku_checking = kpServerAuth
```

```
}
[domain_realm]
mydomain.com = MYDOMAIN.COM
.mydomain.com = MYDOMAIN.COM
```

- 5 安裝 Horizon Agent 套件，並啟用 True SSO。

```
sudo ./install_viewagent.sh -T yes
```

備註 您必須安裝 Horizon Agent 7.6 或更新版本。

- 6 將下列參數新增至 Horizon Agent 自訂組態檔 `/etc/vmware/viewagent-custom.conf`。請使用下列範例，其中 `NETBIOS_NAME_OF_DOMAIN` 是您組織網域的 NetBIOS 名稱。

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

- 7 將系統重新開機，然後重新登入。

設定 Ubuntu 桌面平台的 True SSO

若要設定 Ubuntu 桌面平台的 True SSO，請先整合桌面平台與 Active Directory 網域。然後安裝所需的程式庫與根 CA 憑證，然後再安裝 Horizon Agent。

整合 Ubuntu 桌面平台與 Active Directory 以支援 True SSO

若要在 Ubuntu 16.04 或 18.04 桌面平台上支援 True SSO，請使用 Samba 和 Winbind 解決方案整合桌面平台與 Active Directory 網域。

請使用下列程序整合 Ubuntu 16.04 或 18.04 桌面平台與 AD 網域。

此程序中的某些範例使用預留位置值來代表您網路組態中的實體，例如 Ubuntu 桌面平台的主機名稱。請將預留位置值取代為您的組態特有的資訊，如下表所說明。

預留位置值	說明
dns_IP_ADDRESS	DNS 名稱伺服器的 IP 位址
mydomain.com	AD 網域的 DNS 名稱
MYDOMAIN.COM	AD 網域的 DNS 名稱 (全部使用大寫字母)
myhost	Ubuntu 桌面平台的主機名稱
MYDOMAIN	包含 Samba 伺服器的工作群組或 NT 網域的 DNS 名稱 (全部使用大寫字母)
ads-hostname	AD 伺服器的主機名稱
admin-user	AD 網域管理員的使用者名稱

必要條件

- 在 Linux 系統上，Active Directory (AD) 伺服器可由 DNS 解析。
- 網路時間通訊協定 (NTP) 會設定於 Linux 系統上。

程序

- 1 在 Ubuntu 16.04 或 18.04 桌面平台上，安裝 samba 和 winbind 套件。

```
sudo apt install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind
```

- 2 出現提示時，請依照下列方式設定 Kerberos 驗證設定。

- a 針對預設的 **Kerberos 第 5 版領域**，請輸入您 AD 網域的 DNS 名稱 (全部使用大寫字母)。例如，如果您的 AD 網域名稱為 **mydomain.com**，請輸入 **MYDOMAIN.COM**。
- b 針對您領域的 **Kerberos 伺服器**，請輸入您 AD 伺服器的主機名稱 (在這整個程序的各個範例中均顯示為 **ads_hostname**)。
- c 針對您 **Kerberos 領域的管理伺服器**，再次輸入您 AD 伺服器的主機名稱。

- 3 更新 PAM 組態。

- a 開啟 PAM 組態頁面。

```
pam-auth-update
```

- b 選取在登入時建立主目錄，然後選取確定。

- 4 編輯 /etc/nsswitch.conf 組態檔，如下列範例所示。

```
passwd: compat winbind
group: compat winbind
shadow: compat
gshadow: files
```

- 5 若要確保自動產生的 resolv.conf 檔案會以您的 AD 網域作為搜尋網域，請編輯系統連線的 NetworkManager 設定。

- a 開啟 NetworkManager 控制台，並導覽至系統連線的 **IPv4 設定**。針對 [方法]，選取**僅限自動 (DHCP) 位址**。在 **DNS 伺服器**文字方塊中，輸入您 DNS 名稱伺服器 IP 位址 (在這整個程序的各個範例中均顯示為 **dns_IP_ADDRESS**)。然後，按一下**儲存**。
- b 編輯系統連線的組態檔 (位於 /etc/NetworkManager/system-connections)。請使用下列範例。

```
[ipv4]
dns=dns_IP_ADDRESS
dns-search=mydomain.com
ignore-auto-dns=true
method=auto
```

備註 在建立新的即時複製虛擬桌面平台時，會新增新的虛擬網路介面卡。當新的網路介面卡新增至即時複製虛擬桌面平台時，虛擬桌面平台範本中的任何網路介面卡設定 (例如 **DNS 伺服器**) 都會遺失。為避免在新的網路介面卡新增至複製的虛擬桌面平台時遺失 **DNS 伺服器**設定，您必須為 Linux 系統指定 **DNS 伺服器**。

- c 編輯 `/etc/resolv.conf` 組態檔以指定 DNS 伺服器，如下列範例所示。

```
nameserver dns_IP_ADDRESS

search mydomain.com
```

- d 將系統重新開機，然後重新登入。

- 6 編輯 `/etc/hosts` 組態檔，如下列範例所示。

```
127.0.0.1    localhost
127.0.1.1    myhost.mydomain.com myhost
```

- 7 編輯 `/etc/samba/smb.conf` 組態檔，如下列範例所示。

```
[global]
security = ads
realm = MYDOMAIN.COM
workgroup = MYDOMAIN
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum group = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
kerberos method = secrets and keytab
winbind refresh tickets = true
```

- 8 重新啟動 `smbd` 服務。

```
sudo systemctl restart smbd.service
```

- 9 編輯 `/etc/krb5.conf` 組態檔，使其具有類似下列範例的內容。

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    dns_lookup_realm = true
    dns_lookup_kdc = true

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname
        admin_server = ads-hostname
    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COMmydomain.com = MYDOMAIN.COM
```


10 將您的 Ubuntu 桌面平台加入 AD 網域。

- a 起始 Kerberos 票證。

```
sudo kinit admin-user
```

出現提示時，輸入您的管理員密碼。

- b 確認票證已成功建立。

```
sudo klist
```

此命令會傳回票證的相關資訊，包括其有效起始時間和到期時間。

- c 建立 Kerberos Keytab 檔案。

```
sudo net ads keytab create -U admin-user
```

- d 加入 AD 網域。

```
sudo net ads join -U admin-user
```

11 重新啟動並確認 Winbind 服務。

- a 重新啟動 Winbind 服務。

```
sudo systemctl restart winbind.service
```

- b 若要確認 Winbind 服務，請執行下列命令，並確認命令傳回正確的輸出。

- `wbinfo -u`
- `wbinfo -g`
- `getend passwd`
- `getend group`

12 將系統重新開機，然後重新登入。

後續步驟

在 [Ubuntu 桌面平台上設定 True SSO](#)

在 Ubuntu 桌面平台上設定 True SSO

若要在 Ubuntu 16.04 或 18.04 桌面平台上啟用 True SSO 功能，請安裝 True SSO 功能所依賴的程式庫、支援受信任驗證所需的根 CA 憑證，以及 Horizon Agent。此外，您還必須編輯某些組態檔以完成驗證設定。

請使用下列程序在 Ubuntu 16.04 和 18.04 桌面平台上啟用 True SSO。若要在這些桌面平台上支援 True SSO，您必須安裝 Horizon Agent 7.8 或更新版本。

必要條件

- 針對 VMware Identity Manager 和 Horizon Connection Server 設定 True SSO。
- 整合 [Ubuntu](#) 桌面平台與 [Active Directory](#) 以支援 True SSO
- 取得根憑證授權機構憑證，並將其儲存至桌面平台上的 `/tmp/certificate.cer`。請參閱《[如何匯出根憑證授權機構憑證](#)》。

程序

- 1 在 Ubuntu 16.04 或 18.04 桌面平台上，安裝 pkcs11 支援套件。

```
sudo apt install libpam-pkcs11
```

- 2 安裝 libnss3-tools 套件。

```
sudo apt install libnss3-tools
```

- 3 安裝根憑證授權機構 (CA) 憑證。

- a 找出您所下載的根 CA 憑證，並將其傳輸至 `.pem` 檔案。

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- b 使用 `certutil` 命令將根 CA 憑證安裝至系統資料庫 `/etc/pki/nssdb`。

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- c 將根 CA 憑證複製到 `/etc/pam_pkcs11/cacerts` 目錄。

```
mkdir -p /etc/pam_pkcs11/cacerts

cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

- d 建立根 CA 憑證的雜湊連結。在 `/etc/pam_pkcs11/cacerts` 目錄中，執行下列命令。

```
pkcs11_make_hash_link
```

- 4 安裝 Horizon Agent 套件，並啟用 True SSO。

```
sudo ./install_viewagent.sh -T yes
```

備註 若要使用 True SSO 功能，您必須安裝 Horizon Agent 7.8 或更新版本。

- 5 將下列參數新增至 Horizon Agent 自訂組態檔 `/etc/vmware/viewagent-custom.conf`。請使用下列範例，其中 `NETBIOS_NAME_OF_DOMAIN` 是您組織網域的 NetBIOS 名稱。

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

6 編輯 /etc/pam_pkcs11/pam_pkcs11.conf 組態檔。

- a 如有需要，請建立 /etc/pam_pkcs11/pam_pkcs11.conf 組態檔。在 /usr/share/doc/libpam-pkcs11/examples 中找出範例檔案，並將其複製到 /etc/pam_pkcs11 目錄，然後將該檔案重新命名為 pam_pkcs11.conf。視需要將您的系統資訊新增至檔案內容。
- b 修改 /etc/pam_pkcs11/pam_pkcs11.conf 組態檔，使其包含類似下列範例的內容。

```
use_pkcs11_module = coolkey;
pkcs11_module coolkey {
    module = /usr/lib/vmware/viewagent/sso/libvmwpkcs11.so;
    slot_num = 0;
    ca_dir = /etc/pam_pkcs11/cacerts;
    nss_dir = /etc/pki/nssdb;
}
```

7 修改 PAM 組態檔中的 auth 參數。

- a 開啟 PAM 組態檔。
 - 針對 Ubuntu 16.04，請開啟 /etc/pam.d/lightdm。
 - 針對 Ubuntu 18.04，請開啟 /etc/pam.d/gdm-vmwcred。
- b 編輯 PAM 組態檔，如下列範例所示。

```
auth requisite pam_vmw_cred.so
auth sufficient pam_pkcs11.so try_first_pass
```

8 將系統重新開機，然後重新登入。

設定 SLED/SLES 桌面平台的 True SSO

若要設定 SLED/SLES 桌面平台的 True SSO，請先整合桌面平台與 Active Directory 網域。然後安裝所需的程式庫與根 CA 憑證，然後再安裝 Horizon Agent。

整合 SLED/SLES 桌面平台與 Active Directory 以支援 True SSO

若要在 SLED 12.x SP3 或 SLES 12.x SP3 桌面平台上支援 True SSO，請使用 Samba 和 Winbind 解決方案整合桌面平台與 Active Directory 網域。

請使用下列程序整合 SLED/SLES 桌面平台與 AD 網域。

必要條件

- 在 Linux 系統上，Active Directory (AD) 伺服器可由 DNS 解析。
- 網路時間通訊協定 (NTP) 會設定於 Linux 系統上。

程序**1 在 SLED/SLES 桌面平台上，安裝 samba 和 winbind 套件。**

```
zypper install samba-winbind krb5-client samba-winbind-32bit
```

- 2 開啟 YaST 安裝工具，並導覽至 **網路服務 > Windows 網域成員資格**。
- 3 在 [Windows 網域成員資格] 畫面上，如下所示進行設定。
 - a 針對 **網域或工作群組**，輸入包含 Samba 伺服器的工作群組或 NT 網域的 DNS 名稱 (全部使用大寫字母)。例如，如果您的工作群組名為 **mydomain**，請輸入 **MYDOMAIN**。
 - b 選取 **也使用 SMB 資訊進行 Linux 驗證**。
 - c 選取 **在登入時建立主目錄**。
 - d 選取 **離線驗證**。
 - e 選取 **SSH 的 Single Sign-On**。
- 4 在提示詢問您是否要加入網域時，選取 **是**。
- 5 輸入指定工作群組的管理員名稱和密碼，然後選取 **確定**。
此時會出現一則訊息，確認您的 SLED/SLES 桌面平台已成功加入網域。選取 **確定**。
- 6 編輯 `/etc/samba/smb.conf` 組態檔，使其包含下列參數。

```
[global]
...
winbind use default domain = yes
```

- 7 將系統重新開機，然後重新登入。
- 8 測試並確認您的 SLED/SLES 桌面平台整合。
執行下列測試命令，並確認命令傳回正確的輸出。請將 **mydomain** 取代為您的 Samba 伺服器工作群組或 NT 網域的名稱。
 - `net ads testjoin`
 - `net ads info`
 - `wbinform --krb5auth=mydomain\\open%open`
 - `ssh localhost -l mydomain\\open`

後續步驟

在 [SLED/SLES 桌面平台上設定 True SSO](#)

在 SLED/SLES 桌面平台上設定 True SSO

若要在 SLED/SLES 12.x SP3 桌面平台上啟用 True SSO 功能，請安裝 True SSO 功能所依賴的程式庫、支援受信任驗證所需的根 CA 憑證，以及 Horizon Agent。此外，您還必須編輯某些組態檔以完成驗證設定。

請使用下列程序，在 SLED 12.x SP3 和 SLES 12.x SP3 桌面平台上啟用 True SSO。若要在這些桌面平台上支援 True SSO，您必須安裝 Horizon Agent 7.8 或更新版本。

必要條件

- 針對 VMware Identity Manager 和 Horizon Connection Server 設定 True SSO。

- 整合 SLED/SLES 桌面平台與 Active Directory 以支援 True SSO
- 取得根憑證授權機構憑證，並將其儲存至 SLED/SLES 12.x SP3 桌面平台上的 /tmp/certificate.cer。請參閱《如何匯出根憑證授權機構憑證》。

程序

- 1 針對 SLES 12.x SP3 桌面平台，請執行下列命令以安裝必要的套件。

```
zypper install mozilla-nss-tools pam_krb5 krb5-client krb5-plugin-preauth-pkinit
```

- 2 針對 SLED 12.x SP3 桌面平台，請執行下列步驟以安裝必要的套件。

- a 將 SLES .iso 檔案下載至 SLED 桌面平台的本機磁碟 (例如 /tmp/SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso)。

您必須新增 SLES .iso 檔案作為 SLED 桌面平台的套件來源，因為目前只有適用於 SLES 系統的必要 krb5-plugin-preauth-pkinit 套件。

- b 在 SLED 桌面平台上掛接 SLES .iso 檔案，並安裝必要套件。

```
sudo mkdir -p /mnt/sles
sudo mount -t iso9660 /tmp/SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso /mnt/sles
sudo zypper ar -f /mnt/sles sles
zypper install mozilla-nss-tools pam_krb5 krb5-client krb5-plugin-preauth-pkinit
```

- c 安裝完成後，請將 SLES .iso 檔案取消掛接。

```
sudo umount /mnt/sles
```

- 3 安裝根憑證授權機構 (CA) 憑證。

- a 找出您所下載的根 CA 憑證，並將其傳輸至 .pem 檔案。

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- b 使用 certutil 命令將根 CA 憑證安裝至系統資料庫 /etc/pki/nssdb。

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- c 將根 CA 憑證新增至 pam_pkcs11。

```
cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
```

- 4 編輯 /etc/krb5.conf 組態檔，使其具有類似下列範例的內容。

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
```

```

default_ccache_name = KEYRING:persistent:%{uid}

[realms]
  MYDOMAIN.COM = {
    kdc = ads-hostname
    admin_server = ads-hostname
    pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
    pkinit_kdc_hostname = ads-hostname
    pkinit_eku_checking = kpServerAuth
  }

[domain_realm]
  .mydomain.com = MYDOMAIN.COMmydomain.com = MYDOMAIN.COM

```

請將範例中的預留位置值取代為您的網路組態特有的資訊，如下表所說明。

預留位置值	說明
mydomain.com	AD 網域的 DNS 名稱
MYDOMAIN.COM	AD 網域的 DNS 名稱 (全部使用大寫字母)
ads-hostname	AD 伺服器的主機名稱 (區分大小寫)

5 安裝 Horizon Agent 套件，並啟用 True SSO。

```
sudo ./install_viewagent.sh -T yes
```

備註 若要使用 True SSO 功能，您必須安裝 Horizon Agent 7.8 或更新版本。

6 將下列參數新增至 Horizon Agent 自訂組態檔 /etc/vmware/viewagent-custom.conf。請使用下列範例，其中 **NETBIOS_NAME_OF_DOMAIN** 是您組織網域的 NetBIOS 名稱。

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

7 將系統重新開機，然後重新登入。

設定 Linux 桌面平台的圖形卡

您可以設定目前支援的 Linux 發行版，以在 ESXi 主機或客體作業系統上利用 NVIDIA 功能。

設定 3D 圖形的虛擬機器複製需求

在設定 3D 圖形之前，您必須考慮下列虛擬機器複製需求。

- 對於 vGPU，請在基礎虛擬機器中完成圖形設定。複製虛擬機器。圖形設定適用於複製的虛擬機器，且不需要進一步的設定。
- 對於 vDGA，請在基礎虛擬機器中完成圖形設定。複製虛擬機器。不過，在將複製的虛擬機器開啟電源之前，您必須先從複製的虛擬機器中移除現有的 NVIDIA 傳遞 PCI 裝置，並將新的 NVIDIA 傳遞 PCI 裝置新增至複製的虛擬機器。您無法在虛擬機器之間共用 NVIDIA 傳遞 PCI 裝置。每台虛擬機器都會使用專用的 NVIDIA 傳遞 PCI 裝置。

本章節討論下列主題：

- 針對 vGPU 設定支援的 Linux 發行版
- 針對 vDGA 設定 RHEL 6.x

針對 vGPU 設定支援的 Linux 發行版

您可以設定支援的 Linux 發行版，以利用 ESXi 主機上的 NVIDIA vGPU (共用 GPU 硬體加速) 功能。

您必須使用符合 ESXi 主機 GPU 驅動程式 (.vib) 的 NVIDIA Linux 虛擬機器顯示驅動程式。請參閱 NVIDIA 網站以取得驅動程式套件的相關資訊。

備註 如需支援 vGPU 之 NVIDIA 圖形卡與 Linux 發行版的相關資訊，請參閱 <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>。

注意 開始之前，請確認未在 Linux 虛擬機器上安裝 Horizon Agent。如果您在將機器設為使用 NVIDIA vGPU 之前先安裝 Horizon Agent，則會覆寫 xorg.conf 檔案中所需的組態參數，而且 NVIDIA vGPU 將無法運作。您必須在完成 NVIDIA vGPU 組態後才可安裝 Horizon Agent。

在 ESXi 主機上安裝適用於 NVIDIA GRID vGPU 圖形卡的 VIB

您必須為 ESXi 6.0 U1 或更新版本主機上的 NVIDIA GRID 圖形卡下載並安裝 VIB。

NVIDIA 提供包含 vGPU Manager 的 vGPU 軟體套件，也就是您在此程序中安裝於 ESXi 主機上的套件，以及 Linux 顯示驅動程式，這會在之後的程序中安裝於 Linux 虛擬機器。

必要條件

- 驗證您的環境中已安裝 vSphere 6.0 U1 或更新版本。
- 確認 ESXi 主機上已安裝所需的 vGPU 圖形卡。

備註 如需支援 vGPU 之 NVIDIA 圖形卡與 Linux 發行版的相關資訊，請參閱 <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>。

程序

- 1 從 [NVIDIA 驅動程式下載](#) 網站下載適用於 NVIDIA GRID vGPU 圖形卡的 VIB。
從下拉式功能表選取適當的 VIB 版本。

選項	說明
產品類型	GRID
產品系列	選取 NVIDIA GRID vGPU 。
產品	選取 ESXi 主機上安裝的版本 (例如 GRID K2)。
作業系統	選取 VMware vSphere ESXi 版本。

- 2 解壓縮 vGPU 軟體套件的 .zip 檔案。
- 3 將 vGPU Manager 資料夾上傳到 ESXi 主機。

備註 您將會在之後的程序於 Linux 虛擬機器上安裝 Linux 顯示驅動程式。

- 4 關閉或暫停 ESXi 主機上的所有虛擬機器。
- 5 使用 SSH 連線到 ESXi 主機。
- 6 停止 xorg 服務。

```
# /etc/init.d/xorg stop
```

- 7 安裝 NVIDIA VIB。

例如：

```
# esxcli system maintenanceMode set --enable true
# esxcli software vib install -v /path-to-vib/NVIDIA-VIB-name.vib
# esxcli system maintenanceMode set --enable false
```


8 將 ESXi 主機重新開機或更新。

- ◆ 對於已安裝的 ESXi 主機，將主機重新開機。
- ◆ 對於無狀態 ESXi 主機，請執行下列步驟以更新主機。(這些步驟也可用於已安裝的主機。)

```
Update vmkdevmgr:
# kill -HUP $(cat /var/run/vmware/vmkdevmgr.pid)

Wait for the update to complete:
# localcli --plugin-dir /usr/lib/vmware/esxcli/int deviceInternal bind

This is a new requirement with the NVIDIA 352.* host driver:
# /etc/init.d/nvidia-vgpu start

Restart xorg, which is used for GPU assignment:
# /etc/init.d/xorg start
```

9 驗證 xorg 服務在重新啟動主機後開始執行。

在 Linux 虛擬機器上針對 vGPU 設定共用 PCI 裝置

若要使用 NVIDIA vGPU，您必須為 Linux 虛擬機器設定共用的 PCI 裝置。

必要條件

- 確認 Linux 虛擬機器已備妥可作為桌面平台。請參閱[建立虛擬機器和安裝 Linux](#)與準備用於遠端桌面平台部署的 [Linux 機器](#)。
- 確認未在 Linux 虛擬機器上安裝 Horizon Agent。
- 確認已在 ESXi 主機上安裝 NVIDIA VIB。請參閱在 [ESXi 主機上安裝適用於 NVIDIA GRID vGPU 圖形卡的 VIB](#)。
- 自行熟悉可與 NVIDIA vGPU 使用的虛擬 GPU 類型，這些類型是您以 **GPU 設定檔**設定所做的選擇。虛擬 GPU 類型在安裝於 ESXi 主機的實體 GPU 上提供不同的功能。

備註 如需支援 vGPU 之 NVIDIA 圖形卡與 Linux 發行版的相關資訊，請參閱 <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>。

程序

- 1 關閉虛擬機器電源。
- 2 在 vSphere Web Client 中，選取虛擬機器，然後在 **虛擬機器硬體**索引標籤下，按一下**編輯設定**。
- 3 在**新增裝置**功能表中，選取**共用 PCI 裝置**。
- 4 按一下**新增**，並從下拉式功能表選取 **NVIDIA GRID vGPU**。
- 5 針對 **GPU 設定檔**設定，從下拉式功能表選取虛擬 GPU 類型。
- 6 按一下**保留所有記憶體**，然後按**確定**。

您必須保留所有虛擬機器的記憶體，GPU 才能支援 NVIDIA GRID vGPU。

7 開啟虛擬機器電源。

安裝 NVIDIA GRID vGPU 顯示驅動程式

若要安裝 NVIDIA GRID vGPU 顯示驅動程式，您必須停用預設的 NVIDIA 驅動程式、下載 NVIDIA 顯示驅動程式，並在虛擬機器上設定 PCI 裝置。

必要條件

- 確認您已從 NVIDIA 下載網站下載 vGPU 軟體套件、解壓縮套件，並備妥 Linux 顯示驅動程式 (套件元件)。請參閱在 [ESXi 主機上安裝適用於 NVIDIA GRID vGPU 圖形卡的 VIB](#)。

另外確認共用 PCI 裝置已新增至虛擬機器。請參閱在 [Linux 虛擬機器上針對 vGPU 設定共用 PCI 裝置](#)。

程序

- 1 將 NVIDIA Linux 顯示驅動程式複製到虛擬機器。
- 2 開啟虛擬機器的遠端終端機，或輸入 Ctrl-Alt-F2、登入為 root 身分並執行 `init 3` 命令來停用 X Windows，以切換到文字主控台。
- 3 安裝 NVIDIA 驅動程式所需的額外元件。

```
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
```

- 4 將可執行檔旗標新增至 NVIDIA GRID vGPU 驅動程式套件。

```
chmod +x NVIDIA-Linux-x86_64-version-grid.run
```

- 5 啟動 NVIDIA GRID vGPU 安裝程式。

```
sudo ./NVIDIA-Linux-x86_64-version-grid.run
```

- 6 接受 NVIDIA 軟體授權合約，並選取是來自動更新 X 組態設定。

後續步驟

在 Linux 虛擬機器上安裝 Horizon Agent。請參閱在 [Linux 虛擬機器上安裝 Horizon Agent](#)。

建立包含已設定 Linux 虛擬機器的桌面平台集區。請參閱[建立 Linux 的手動桌面平台集區](#)。

確認已安裝 NVIDIA 顯示驅動程式

您可以在 Horizon 桌面平台工作階段中顯示 NVIDIA 驅動程式輸出，以確認 Linux 虛擬機器上已安裝 NVIDIA 顯示驅動程式。

必要條件

- 確認是否已安裝 NVIDIA 顯示驅動程式。
- 確認已在 Linux 虛擬機器上安裝 Horizon Agent。請參閱在 [Linux 虛擬機器上安裝 Horizon Agent](#)。

- 確認 Linux 虛擬機器已部署於桌面平台集區。請參閱[建立 Linux 的手動桌面平台集區](#)。

程序

- 1 重新啟動 Linux 虛擬機器。

Horizon Agent 啟動指令碼會初始化 X 伺服器並顯示拓撲。

您無法繼續在 vSphere 主控台中檢視虛擬機器顯示畫面。

- 2 從 Horizon Client，連接至 Linux 桌面平台。
- 3 在 Linux 桌面平台工作階段中，驗證已安裝 NVIDIA 顯示驅動程式。

開啟終端機視窗，並執行 `glxinfo | grep NVIDIA` 命令。

NVIDIA 驅動程式輸出隨即顯示。例如：

```
[root]# glxinfo | grep NVIDIA
server glx vendor string: NVIDIA Corporation
client glx vendor string: NVIDIA Corporation
OpenGL vendor string: NVIDIA Corporation
OpenGL version string: 4.5.0 NVIDIA 346.47
OpenGL shading language version string: 4.50 NVIDIA
```

使用者可以在遠端桌面平台上存取 NVIDIA 圖形功能。

在確認已安裝 NVIDIA 顯示驅動程式之後，請執行下列工作以讓安裝正確運作。

- 如果您升級 Linux 核心，Horizon Agent 可能無法與 Horizon 連線伺服器通訊。若要解決問題，請重新安裝 NVIDIA 驅動程式。
- 在 Linux 虛擬機器中設定 NVIDIA GRID 授權。如需詳細資訊，請參閱 NVIDIA 說明文件。如果未設定授權，則 Linux 桌面平台無法正確運作。例如，自動調整會無法運作。

針對 vDGA 設定 RHEL 6.x

您可以設定 RHEL 6.x 客體作業系統，讓 Horizon 7 for Linux 桌面平台得以在 ESXi 主機上利用 vDGA 功能。

注意 開始之前，請確認未在 Linux 虛擬機器上安裝 Horizon Agent。如果您在將機器設為使用 vDGA 之前先安裝 Horizon Agent，則會覆寫 `xorg.conf` 檔案中所需的組態參數，而且 vDGA 將無法運作。您必須在完成 vDGA 組態後才可安裝 Horizon Agent。

在主機上針對 NVIDIA GRID 啟用 DirectPath I/O

設定 Linux 虛擬機器以使用 vDGA 之前，您必須使 NVIDIA GRID GPU PCI 裝置可在 ESXi 主機上的 DirectPath I/O 傳遞使用。

必要條件

- 驗證您的環境中已安裝 vSphere 6.0 或更新版本。
- 驗證 ESXi 主機上已安裝 NVIDIA GRID K1 或 K2 圖形卡。

程序

- 1 在 vSphere Web Client 中，瀏覽至 ESXi 主機。
- 2 按一下**管理**索引標籤，然後按一下**設定**。
- 3 在 [硬體] 區段中，按一下 **PCI 裝置**。
- 4 若要啟用 NVIDIA GRID GPU 的 DirectPath I/O 傳遞，請按一下**編輯**。

圖示	描述
綠色圖示	PCI 裝置處於作用中狀態且可啟用。
橙色圖示	裝置的狀態已變更。您必須先將主機重新開機，然後才能使用該裝置。

- 5 選取 NVIDIA GRID GPU 並按一下**確定**。
PCI 裝置即新增至「可供 VM 使用的 DirectPath I/O PCI 裝置」表格。
- 6 將主機重新開機，以讓 PCI 裝置可供 Linux 虛擬機器使用。

新增 vDGA 傳遞裝置到 RHEL 6.x 虛擬機器

若要將 RHEL 6.x 虛擬機器設定為使用 vDGA，您必須新增 PCI 裝置到虛擬機器。藉由此步驟，即可傳遞 ESXi 主機上的實體裝置，以在虛擬機器上使用。

必要條件

- 確認 Linux 虛擬機器已備妥可作為桌面平台。請參閱[建立虛擬機器和安裝 Linux](#)與準備用於遠端桌面平台部署的 [Linux 機器](#)。
- 確認未在 Linux 虛擬機器上安裝 Horizon Agent。
- 驗證 NVIDIA GRID GPU PCI 裝置可供主機上的 DirectPath I/O 傳遞使用。請參閱[在主機上針對 NVIDIA GRID 啟用 DirectPath I/O](#)。

程序

- 1 以 sudo 權限設定的本機使用者身分登入 RHEL 6.x 客體作業系統。
- 2 在 vSphere Web Client 中，選取虛擬機器，然後在 **虛擬機器硬體** 索引標籤下，按一下**編輯設定**。
- 3 在**新增裝置**功能表中，選取 **PCI 裝置**。
- 4 按一下**新增**，並從下拉式功能表選取 PCI 裝置。
- 5 按一下**保留所有記憶體**，然後按**確定**。
您必須保留所有虛擬機器的記憶體，GPU 才能支援 vDGA。
- 6 打開虛擬機器的電源，並開啟 vSphere 主控台來連線至機器。

7 驗證 NVIDIA GRID 裝置已傳遞到虛擬機器。

開啟終端機視窗，並執行下列命令：

```
lspci | grep NVIDIA
```

XX:00.0 VGA 相容控制器隨即顯示。例如：

```
NVIDIA Corporation GK104GL [GRID K2]
```

安裝 vDGA 的 NVIDIA 顯示驅動程式

若要安裝 vDGA 的 NVIDIA 顯示驅動程式，您必須停用預設的 NVIDIA 驅動程式、下載 NVIDIA 顯示驅動程式，並在虛擬機器上設定 PCI 裝置。

必要條件

- 確認 PCI 裝置已新增至 RHEL 6.x 虛擬機器。請參閱[新增 vDGA 傳遞裝置到 RHEL 6.x 虛擬機器](#)。

程序

1 停用並將預設的 NVIDIA Nouveau 驅動程式加入黑名單。

- a 編輯 `grub.conf` 檔案。

針對 RHEL 6.x，該檔案為 `/boot/grub/grub.conf`。

RHEL 版本	命令
6.x	<code>sudo vi /boot/grub/grub.conf</code>

- b 在核心選項尾端新增 `rdblacklist=nouveau` 行。

- c 編輯 `blacklist.conf` 檔案。

```
sudo vi /etc/modprobe.d/blacklist.conf
```

- d 在 `blacklist.conf` 檔案的任意處新增下列行。

```
blacklist nouveau
```

2 重新啟動虛擬機器。

顯示的外觀與風格有變更。

3 (選擇性) 驗證已停用 Nouveau 驅動程式。

```
/sbin/lsmmod | grep nouveau
```

如果 `grep` 搜尋未傳回任何結果，則 Nouveau 驅動程式為停用。

- 4 從 [NVIDIA 驅動程式下載](#) 網站下載 NVIDIA 驅動程式。

從 NVIDIA 下拉式功能表選取適當的驅動程式版本：

選項	說明
產品類型	GRID
產品系列	GRID 系列
產品	選取 ESXi 主機上安裝的版本 (例如 GRID K2)。
作業系統	Linux 64 位元或 Linux 32 位元

- 5 若要連線至虛擬機器，請開啟遠端終端機，或輸入 **Ctrl-Alt-F2** 使用文字主控台，以 **root** 身分登入，然後執行 **init 3** 命令以停用 X Windows。
- 6 安裝 NVIDIA 驅動程式所需的額外元件。

```
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
```

- 7 將可執行檔旗標新增至 vDGA 的 NVIDIA 驅動程式套件。

```
chmod +x NVIDIA-Linux-x86_64-version.run
```

- 8 執行 NVIDIA 安裝程式。

```
sudo ./NVIDIA-Linux-x86_64-version.run
```

- 9 接受 NVIDIA 軟體授權合約，並選取是來更新 X 組態設定。

後續步驟

在 Linux 虛擬機器上安裝 Horizon Agent。請參閱[在 Linux 虛擬機器上安裝 Horizon Agent](#)。

建立包含已設定 Linux 虛擬機器的桌面平台集區。請參閱[建立 Linux 的手動桌面平台集區](#)。

確認已安裝 NVIDIA 顯示驅動程式

您可以在 Horizon 桌面平台工作階段中顯示 NVIDIA 驅動程式輸出，以確認 Linux 虛擬機器上已安裝 NVIDIA 顯示驅動程式。

必要條件

- 確認是否已安裝 NVIDIA 顯示驅動程式。
- 確認已在 Linux 虛擬機器上安裝 Horizon Agent。請參閱[在 Linux 虛擬機器上安裝 Horizon Agent](#)。
- 確認 Linux 虛擬機器已部署於桌面平台集區。請參閱[建立 Linux 的手動桌面平台集區](#)。

程序

1 重新啟動 Linux 虛擬機器。

Horizon Agent 啟動指令碼會初始化 X 伺服器並顯示拓撲。

您無法繼續在 vSphere 主控台中檢視虛擬機器顯示畫面。

2 從 Horizon Client，連接至 Linux 桌面平台。

3 在 Linux 桌面平台工作階段中，驗證已安裝 NVIDIA 顯示驅動程式。

開啟終端機視窗，並執行 `glxinfo | grep NVIDIA` 命令。

NVIDIA 驅動程式輸出隨即顯示。例如：

```
[root]# glxinfo | grep NVIDIA
server glx vendor string: NVIDIA Corporation
client glx vendor string: NVIDIA Corporation
OpenGL vendor string: NVIDIA Corporation
OpenGL version string: 4.5.0 NVIDIA 346.47
OpenGL shading language version string: 4.50 NVIDIA
```

使用者可以在遠端桌面平台上存取 NVIDIA 圖形功能。

在確認已安裝 NVIDIA 顯示驅動程式之後，請執行下列工作以讓安裝正確運作。

- 如果您升級 Linux 核心，Horizon Agent 可能無法與 Horizon 連線伺服器通訊。若要解決問題，請重新安裝 NVIDIA 驅動程式。
- 在 Linux 虛擬機器中設定 NVIDIA GRID 授權。如需詳細資訊，請參閱 NVIDIA 說明文件。如果未設定授權，則 Linux 桌面平台無法正確運作。例如，自動調整會無法運作。

安裝 Horizon Agent

5

您必須在 Linux 桌面平台上安裝 Horizon Agent，如此 Horizon Connection Server 才能與其通訊並管理桌面平台。

本章節討論下列主題：

- 在 Linux 虛擬機器上安裝 Horizon Agent
- 設定 Linux 代理程式的憑證
- 升級 Linux 虛擬機器上的 Horizon Agent
- 解除安裝 Horizon 7 for Linux 機器

在 Linux 虛擬機器上安裝 Horizon Agent

您必須先在 Linux 虛擬機器上安裝 Horizon Agent，之後才能夠將機器部署為遠端桌面平台。

從 Horizon 7.0.1 版開始，Horizon Agent for Linux 會使用 vCenter 管理的虛擬機器。受管理的虛擬機器可提供下列增強功能。

- vCenter 是 Linux 桌面平台部署的必要需求。
- 在 Linux 上安裝 Horizon Agent 時不需要登錄。
- 對於涉及許多 Linux 桌面平台的部署，您可以將 Horizon Agent 安裝在基礎虛擬機器上。

注意 如果您打算使用 NVIDIA GRID vGPU 或 vDGA，請務必在安裝 Horizon Agent 之前，先在 Linux 虛擬機器上設定這些 3D 功能。若先安裝 Horizon Agent，則會覆寫 `xorg.conf` 檔案中的所需參數，而且 3D 圖形功能將無法運作。

請參閱針對 vGPU 設定支援的 Linux 發行版或針對 vDGA 設定 RHEL 6.x。請在完成 3D 圖形組態之後再安裝 Horizon Agent。

對於 2D 圖形組態，您可以在完成準備用於遠端桌面平台部署的 Linux 機器中的步驟後再安裝 Horizon Agent。

必要條件

- 驗證 Linux 客體作業系統已準備就緒而可供桌面平台使用。請參閱準備用於遠端桌面平台部署的 Linux 機器。

- 自行熟悉 Linux 適用的 Horizon Agent 安裝程式指令碼。請參閱 [install_viewagent.sh 命令列選項](#)。

程序

- 1 從 VMware 下載網站下載 Linux 版 Horizon Agent 安裝程式檔案，網址為 <https://my.vmware.com/web/vmware/downloads>。

在 [桌面平台及使用者運算] 區段下，選取 [檢視 VMware Horizon 的下載元件]。在 Horizon 7 for Linux 下，選取適用於 64 位元 Linux 系統之 VMware Horizon 7 的 [下載] 頁面。

64 位元 Linux 的安裝程式檔案名稱為 `VMware-horizonagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz`，其中，`y.y.y` 是版本號碼，而 `xxxxxxx` 是組建編號。

- 2 在客體作業系統上解壓縮您的 Linux 發行版的 tarball。

例如：

```
tar -xzf VMware-horizonagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz
```

- 3 導覽至 tar ball 資料夾。
- 4 以 superuser 的身分執行 `install_viewagent.sh` 指令碼。
請參閱 [install_viewagent.sh 命令列選項](#) 以取得命令列選項的清單。
例如：

```
sudo ./install_viewagent.sh
```

- 5 如果您執行 `install_viewagent.sh` 而未指定 `-A` 選項，請輸入 **Yes** 來接受 EULA。

除非您接受 EULA，否則安裝程式不會執行。

- 6 將 Linux 重新開機以使變更生效。

安裝之後，會啟動 `viewagent` 服務。請使用 `sudo service viewagent status` 確認服務已啟動。

後續步驟

在桌面平台集區部署虛擬機器。請參閱 [建立 Linux 的手動桌面平台集區](#)。

install_viewagent.sh 命令列選項

`install_viewagent.sh` 指令碼會在 Linux 客體作業系統上安裝 Horizon Agent。

在 gnome 桌面平台環境的命令提示視窗中，使用下列格式的 `install_viewagent.sh` 指令碼。

```
install_viewagent.sh command_option 引數 [command_option 引數] . . .
```

`install_viewagent.sh` 指令碼包括強制和選用參數。

表 5-1. install_viewagent.sh 選用但必要的參數

選用參數 (必要資訊)	說明
-A yes no	接受或拒絕使用者授權合約 (EULA) 和聯邦資訊處理標準 (FIPS) 聲明。您必須指定 yes ，安裝才能繼續。

表 5-2. install_viewagent.sh 選用參數

選用參數	說明
-a yes no	安裝或略過音訊輸入重新導向支援。預設值為 yes 。
-f yes no	安裝或略過專為聯邦資訊處理標準 (FIPS) 140-2 所設計的密碼編譯模組支援。預設值為 no 。如需詳細資訊，請參閱 HorizonLinux 桌面平台的功能 中的 FIPS 140-2 模式說明。
-j	JMS SSL 金鑰儲存區密碼。依預設，安裝程式會產生隨機字串。
-m yes no	安裝或略過智慧卡重新導向支援。預設值為 no 。
-r yes no	在安裝之後自動重新啟動系統。預設值為 no 。
-s	自我簽署憑證主體 DN。依預設，安裝程式會使用 Blast。
-C yes no	安裝或略過剪貼簿重新導向支援。預設值為 yes 。
-F yes no	安裝或略過 CDR 支援。預設值為 yes 。
-M yes no	將 Linux 代理程式升級為受管理或未受管理的代理程式。預設值為 yes 。
-S yes no	安裝或略過 Single Sign-On (SSO) 支援。預設值為 yes 。
-T yes no	安裝或略過 True Single Sign-On (True SSO) 支援。預設值為 no 。
-U yes no	安裝或略過 USB 支援。預設值為 no 。

表 5-3. install_viewagent.sh 參數範例

條件	範例
全新安裝	<pre>sudo ./install_viewagent.sh -A yes</pre> <p>全新安裝一律需要建立新的桌面平台集區。</p>
從未受管理的虛擬機器升級，並保留未受管理的虛擬機器樣式	<pre>sudo ./install_viewagent.sh -A yes-M no</pre> <p>此類型的升級不需要建立新的桌面平台集區。您可以重複使用現有的桌面平台集區。</p> <p>備註 為確保能達到最佳效能，請勿使用未受管理的虛擬機器。</p>
從未受管理的虛擬機器部署升級，並轉換為受管理的虛擬機器樣式。此升級需要在代理上建立新的桌面平台集區	<pre>sudo ./install_viewagent.sh -A yes</pre> <p>此類型的升級需要建立新的桌面平台集區。您必須刪除現有的桌面平台集區。</p>

設定 Linux 代理程式的憑證

當您安裝 Linux 代理程式時，安裝程式會產生 VMwareBlastServer 的自我簽署憑證。

- 當代理停用 Blast 安全閘道時，VMwareBlastServer 會向使用 HTML Access 來連線至 Linux 桌面平台的瀏覽器顯示此憑證。
- 當代理啟用 Blast 安全閘道時，Blast 安全閘道的憑證會向瀏覽器顯示憑證。

若要符合產業或安全法規，您可以將自我簽署憑證取代為憑證授權單位 (CA) 簽署的憑證。

程序

- 1 將私密金鑰和憑證安裝至 VMwareBlastServer。
 - a 將私密金鑰重新命名為 `rui.key`，並將憑證重新命名為 `rui.crt`。
 - b 執行 `sudo chmod 550 /etc/vmware/ssl`。
 - c 將 `rui.crt` 和 `rui.key` 複製到 `/etc/vmware/ssl`。
 - d 執行 `chmod 440 /etc/vmware/ssl`。
- 2 將根和中繼憑證授權單位安裝至 Linux 作業系統憑證授權單位存放區。

備註 如需變更 Linux 系統設定，請參閱 Linux 發行版說明文件。

升級 Linux 虛擬機器上的 Horizon Agent

您可以藉由安裝最新版本的 Horizon Agent，來升級 Linux 虛擬機器上的 Horizon Agent。

未受管理的虛擬機器：代理程式安裝程式會將虛擬機器登錄至需要代理管理資訊的代理。桌面平台集區建立精靈會使用 [機器來源] 頁面中的**其他來源**，選取已登錄的虛擬機器。

受管理的虛擬機器：安裝程式不會與代理通訊。桌面平台集區建立精靈會使用 [機器來源] 頁面中的**vCenter 虛擬機器**，透過 vCenter 選取虛擬機器。受管理的虛擬機器部署支援下列功能。

- 遠端機器電源原則
- 允許使用者重設其機器

備註 Horizon Agent for Linux 7.0.0 和更早版本的運作方式與未受管理的虛擬機器相同。Horizon Agent for Linux 7.0.1 的運作方式與受管理的虛擬機器支援相同。

您可以使用下列方法，從未受管理升級為受管理的虛擬機器部署。

- 保留未受管理的虛擬機器部署，並升級為必要版本。此類型的升級不需要在 Horizon Connection Server 中進行任何組態修改。

- 從未受管理的虛擬機器部署，升級為任何版本的受管理虛擬機器部署。此類型的升級需要在 Horizon Connection Server 上建立新的桌面平台集區。

備註 從受管理的虛擬機器部署升級時，您可以保留受管理的虛擬機器部署，並升級為必要版本。不過，在升級期間從受管理的虛擬機器部署轉換為未受管理的虛擬機器部署，則是不受支援的。

以下是可用於升級的參數。

表 5-4. 用於升級 Horizon Agent 的選用參數

參數	說明
-A yes	EULA 和 FIPS 陳述式接受。您必須指定 yes ，安裝才能繼續。如果未指定此參數，安裝指令碼會出現提示，要求您輸入值。
-a yes no	安裝或略過音訊輸入重新導向支援。
-f yes no	安裝或略過專為聯邦資訊處理標準 (FIPS) 140-2 所設計的密碼編譯模組支援。預設值為 no 。如需詳細資訊，請參閱 HorizonLinux 桌面平台的功能 中的 FIPS 140-2 模式說明。
-m yes no	安裝或略過智慧卡重新導向支援。預設值為 no 。
-r yes no	安裝之後將作業系統重新開機。預設值為 no 。
-C yes no	安裝或略過剪貼簿重新導向支援。預設值為 yes 。
-F yes no	安裝或略過 CDR 支援。預設值為 yes 。
-M yes no	將 Linux 代理程式升級為受管理 未受管理的代理程式。預設值為 yes 。
-S yes no	安裝或略過 Single Sign-On (SSO) 支援。預設值為 yes 。
-U yes no	安裝或略過 USB 支援。預設值為 no 。

升級 Linux 虛擬機器上的 Horizon Agent

您可以藉由安裝最新版本的 Horizon Agent，來升級 Linux 機器上的 Horizon Agent。

必要條件

- 確認 VMwareBlastServer 處理程序未執行。

若要停止此處理程序，請確定使用者已登出機器，且沒有作用中的桌面平台工作階段，或是將機器重新開機。

程序

- 1 從 VMware 下載網站下載最新的 Horizon Agent for Linux 安裝程式檔案，網址為 <https://my.vmware.com/web/vmware/downloads>。

在 [桌面平台及使用者運算] 下，選取下載 VMware Horizon 7，其中包含 Horizon Agent for Linux 的安裝程式。

64 位元 Linux 的安裝程式檔案名稱為 `VMware-viewagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz`，其中，`y.y.y` 是版本號碼，而 `xxxxxxx` 是組建編號。

- 2 在客體作業系統上解壓縮您的 Linux 發行版的 tarball。

例如：

```
tar -xzf <Horizon Agent tar ball>
```

- 3 導覽至 tar ball 資料夾。
- 4 若要升級未受管理的虛擬機器，請使用下列其中一個部署案例來執行 `install_viewagent.sh` 指令碼。

選項	說明
升級未受管理的虛擬機器部署，並保留未受管理的虛擬機器部署	<pre>sudo ./install_viewagent.sh -A yes -M no</pre> <p>備註 為確保能達到最佳效能，請勿使用未受管理的虛擬機器。</p>
升級未受管理的虛擬機器部署，並將其變更為受管理的虛擬機器部署	<pre>sudo ./install_viewagent.sh -A yes -M yes</pre> <p>備註 在 Horizon Console 中，針對未受管理的虛擬機器部署刪除現有的桌面平台集區，並為受管理的虛擬機器部署建立桌面平台集區。如需詳細資訊，請參閱建立 Linux 的手動桌面平台集區。</p>
升級受管理的虛擬機器部署	<pre>sudo ./install_viewagent.sh -A yes -M yes</pre> <p>備註 升級之後，您現有的桌面平台集區將可重複使用。</p>

解除安裝 Horizon 7 for Linux 機器

若要解除安裝虛擬機器上的 Horizon 7 for Linux，您必須解除安裝 Horizon Agent，並移除組態檔。

必要條件

確認 VMwareBlastServer 處理程序未執行。若要停止此處理程序，請確定您已登出機器，且沒有作用中的桌面平台工作階段，或是將機器重新開機。

程序

- 1 在虛擬機器上開啟終端機視窗，並執行 Horizon Agent 解除安裝指令碼。

```
sudo /usr/lib/vmware/viewagent/bin/uninstall_viewagent.sh
```

此指令碼會停止 Horizon Agent 處理程序，並從安裝目錄 `/usr/lib/vmware/viewagent` 中刪除 Horizon Agent 服務和軟體。

- 2 手動刪除 `/etc/vmware` 目錄中的 Horizon 7 for Linux 組態檔。

Linux 桌面平台的組態選項

6

您可以使用組態檔設定各種選項來自訂使用者體驗。

本章節討論下列主題：

- 在 Linux 桌面平台上設定組態檔中的選項
- 使用 智慧原則
- Linux 桌面平台的 Blast 設定範例
- Linux 桌面平台用戶端磁碟機重新導向選項的範例

在 Linux 桌面平台上設定組態檔中的選項

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

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

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

```
RemoteDisplay.buildToPNG=TRUE
```

進行組態變更之後，請將 Linux 重新開機以讓變更生效。

`/etc/vmware/config` 中的組態選項

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

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

表 6-1. /etc/vmware/config 中的組態選項

選項	值/格式	預設值	說明
Clipboard.Direction	0, 1, 2, 或 3	2	使用此選項來指定剪貼簿重新導向原則。有效值如下： <ul style="list-style-type: none"> ■ 0 - 停用剪貼簿重新導向。 ■ 1 - 啟用雙向剪貼簿重新導向。 ■ 2 - 僅啟用從用戶端到遠端桌面平台的剪貼簿重新導向。 ■ 3 - 僅啟用從遠端桌面平台到用戶端的剪貼簿重新導向。
RemoteDisplay.allowAudio	true 或 false	true	設定此選項可啟用/停用音訊輸出。
RemoteDisplay.allowH264	true 或 false	true	設定此選項，可啟用或停用 H.264 編碼。
RemoteDisplay.buildToPNG	true 或 false	false	圖形應用程式，特別是圖形設計應用程式，會需要在 Linux 桌面平台的用戶端有像素精準的影像呈現。您可以針對 Linux 桌面平台上產生和在用戶端裝置上呈現的影像和視訊播放，設定無失真建立 PNG 模式。此功能會在用戶端和 ESXi 主機之間使用額外的頻寬。啟用此選項會停用 H.264 編碼。
RemoteDisplay.enableNetworkContinuity	true 或 false	true	設定此選項，可啟用或停用 Horizon Agent for Linux 中的網路持續性功能。
RemoteDisplay.enableNetworkIntelligence	true 或 false	true	設定此選項，可啟用或停用 Horizon Agent for Linux 中的網路智慧功能。
RemoteDisplay.enableStats	true 或 false	false	在 mks 記錄中啟用或停用 VMware Blast 顯示通訊協定統計資料，例如頻寬、FPS、RTT 等。
RemoteDisplay.enableUDP	true 或 false	true	設定此選項，可啟用或停用 Horizon Agent for Linux 中的 UDP 通訊協定支援。
RemoteDisplay.maxBandwidthKbps	整數	1000000	指定 VMware Blast 工作階段的最大頻寬 (單位為千位元/秒，即 kbps)。頻寬包括所有影像處理、音訊、虛擬通道和 VMware Blast 控制流量。有效值必須小於 4 Gbps (4096000)。
RemoteDisplay.minBandwidthKbps	整數	256	指定 VMware Blast 工作階段的最小頻寬 (單位為千位元/秒，即 kbps)。頻寬包括所有影像處理、音訊、虛擬通道和 VMware Blast 控制流量。
RemoteDisplay.maxFPS	整數	30	指定畫面更新的最大速率。使用此設定，可管理使用者所使用的平均頻寬。有效值必須介於 3 與 60 之間。預設值為每秒 30 次更新。
RemoteDisplay.maxQualityJPEG	可用值範圍：1-100	90	指定用於 JPEG/PNG 編碼的桌面平台顯示的影像畫質。高畫質設定用於較為靜態的畫面區域，可產生較佳影像畫質。
RemoteDisplay.midQualityJPEG	可用值範圍：1-100	35	指定用於 JPEG/PNG 編碼的桌面平台顯示的影像畫質。用來設定桌面平台顯示的中等畫質設定。
RemoteDisplay.minQualityJPEG	可用值範圍：1-100	25	指定用於 JPEG/PNG 編碼的桌面平台顯示的影像畫質。低畫質設定用於經常變動的畫面區域，例如，在執行捲動時。

表 6-1. /etc/vmware/config 中的組態選項 (續)

選項	值/格式	預設值	說明
RemoteDisplay.qpmaxH264	可用值範圍: 0-51	36	使用此選項來設定 H264minQP 量化參數, 其指定設定為使用 H.264 編碼的遠端顯示的最佳影像畫質。將該值設定為大於針對 RemoteDisplay.qpminH264 設定的值。
RemoteDisplay.qpminH264	可用值範圍: 0-51	10	使用此選項來設定 H264maxQP 量化參數, 其指定設定為使用 H.264 編碼的遠端顯示的最低影像畫質。將該值設定為小於針對 RemoteDisplay.qpmaxH264 設定的值。
UsbRedirPlugin.log.logLevel	error、warn、info、debug、trace 或 verbose	info	使用此選項, 可設定 USB 重新導向外掛程式的記錄層級。
UsbRedirServer.log.logLevel	error、warn、info、debug、trace 或 verbose	info	使用此選項, 可設定 USB 重新導向伺服器的記錄層級。
VMWPKcs11Plugin.log.enable	true 或 false	false	設定此選項可啟用或停用 True SSO 功能的記錄模式。
VMWPKcs11Plugin.log.logLevel	error、warn、info、debug、trace 或 verbose	info	使用此選項, 可設定 True SSO 功能的記錄層級。
VVC.RTAV.Enable	true 或 false	true	設定此選項可啟用/停用音訊輸入。
VVC.ScRedir.Enable	true 或 false	true	設定此選項可啟用/停用智慧卡重新導向。
VVC.logLevel	fatalerror、warn、info、debug 或 trace	info	使用此選項以設定 VVC Proxy 節點的記錄層級。
cdserver.cacheEnable	true 或 false	true	設定此選項, 可啟用或停用從代理程式到用戶端的寫入快取功能。
cdserver.customizedSharedFolderPath	folder_path	/home/	<p>使用此選項可將用戶端磁碟機重新導向 (CDR) 共用資料夾位置從預設的 /home/user/tsclient 目錄變更為自訂目錄。</p> <p>例如, 如果使用者 test 要將 CDR 共用資料夾放在 /mnt/test/tsclient (而不是 /home/test/tsclient) 中, 則該使用者可以指定 cdserver.customizedSharedFolderPath=/mnt/。</p> <p>備註 為了使此選項生效, 指定的資料夾必須存在且已使用正確的使用者權限進行設定。</p>
cdserver.forcedByAdmin	true 或 false	false	設定此選項, 可控制用戶端是否可以共用未使用 cdserver.shareFolders 選項指定的其他資料夾。
cdserver.logLevel	error、warn、info、debug、trace 或 verbose	info	使用此選項, 可設定 vmware-CDRserver.log 檔案的記錄層級。

表 6-1. /etc/vmware/config 中的組態選項 (續)

選項	值/格式	預設值	說明
cdrserver.permissions	R	RW	<p>使用此選項，可在 Horizon Agent 所具備 Horizon Client 共用的資料夾上套用其他的讀取/寫入權限。例如：</p> <ul style="list-style-type: none"> ■ 如果 Horizon Client 共用的資料夾具有 read 和 write 權限，而您設定 cdrserver.permissions=R，則 Horizon Agent 僅具有 read 存取權限。 ■ 如果 Horizon Client 共用的資料夾僅具有 read 權限，而您設定 cdrserver.permissions=RW，則 Horizon Agent 仍僅有 read 存取權限。Horizon Agent 無法變更 Horizon Client 所設定的 read only (唯讀) 屬性。Horizon Agent 僅能移除寫入權限。 <p>一般使用方式如下：</p> <ul style="list-style-type: none"> ■ cdrserver.permissions=R ■ #cdrserver.permissions=R (例如，註解排除或刪除該項目)
cdrserver.sharedFolders	<i>file_path1,R; file_path2,; file_path3,R; . .</i>	未定義	<p>指定用戶端可以與 Linux 桌面平台共用的一或多個資料夾的檔案路徑。例如：</p> <ul style="list-style-type: none"> ■ 針對 Windows 用戶端：C:\spreadsheets,;D:\ebooks,R ■ 針對非 Windows 用戶端：/tmp/spreadsheets;/tmp/ebooks,;/home/finance,R
collaboration.logLevel	error、info 或 debug	info	<p>使用此選項，可設定協作工作階段所使用的記錄層級。如果記錄層級為 debug，則會記錄對 collabui 函數進行的所有呼叫和 collabor 清單的內容。</p>
collaboration.maxCollabors	小於 10 的整數	5	<p>指定您可以邀請加入工作階段的協作者數目上限。</p>
collaboration.enableEmail	true 或 false	true	<p>設定此選項，可啟用或停用使用已安裝的電子郵件應用程式傳送協作邀請。此選項停用時，即便已安裝電子郵件應用程式，您仍無法使用電子郵件邀請協作者。</p>
collaboration.serverUrl	[URL]	未定義	<p>指定要納入協作邀請的伺服器 URL。</p>
collaboration.enableControlPassing	true 或 false	true	<p>設定此選項，可允許或限制協作者對 Linux 桌面平台進行控制。若要指定唯讀協作工作階段，請將此選項設為 false。</p>
mksVNCServer.useUInputButtonMapping	true 或 false	false	<p>設定此選項可啟用 Ubuntu 或 RHEL 7.x CentOS 上的慣用左手滑鼠支援，而 RHEL 6.x 支援左手使用者的滑鼠，您不需要設定此選項。</p>
mksvhan.clipboardSize	整數	1024	<p>使用此選項，可指定所要複製及貼上的剪貼簿大小上限。</p>
vdpservice.log.logLevel	fatalerror、warn、info、debug 或 trace	info	<p>使用此選項，可設定 vdpservice 的記錄層級。</p>
viewusb.AllowAudioIn	{m o}: {true false}	未定義，其相當於 true	<p>使用此選項，可允許或不允許將音訊輸入裝置重新導向。範例：o:false</p>

表 6-1. /etc/vmware/config 中的組態選項 (續)

選項	值/格式	預設值	說明
viewusb.AllowAudioOut	{m o}: {true false}	未定義，其相當於 false	設定此選項，可允許或不允許音訊輸出裝置的重新導向。
viewusb.AllowAutoDeviceSplitting	{m o}: {true false}	未定義，其相當於 false	設定此選項，可允許或不允許複合 USB 裝置的自動分割。 範例: m:true
viewusb.AllowDevDescFailsafe	{m o}: {true false}	未定義，其相當於 false	設定此選項後，即便 Horizon Client 無法取得組態或裝置描述元時，仍可允許或不允許將裝置重新導向。若要在即使無法取得組態或裝置描述元的情形下也允許裝置，請將它納入在 Include 篩選器當中，例如 IncludeVidPid 或 IncludePath 。
viewusb.AllowHIDBootable	{m o}: {true false}	未定義，其相當於 true	使用此選項以允許或不允許將鍵盤或滑鼠以外可在開機時使用的輸入裝置 (又稱為 HID 可開機裝置) 重新導向。
viewusb.AllowKeyboardMouse	{m o}: {true false}	未定義，其相當於 false	使用此選項，可以允許或不允許將具備整合式指向裝置 (例如滑鼠、軌跡球或觸控板) 的鍵盤重新導向。
viewusb.AllowSmartcard	{m o}: {true false}	未定義，其相當於 false	設定此選項，可允許或不允許將智慧卡裝置重新導向。
viewusb.AllowVideo	{m o}: {true false}	未定義，其相當於 true	使用此選項，可允許或不允許將視訊裝置重新導向。
viewusb.DisableRemoteConfig	{m o}: {true false}	未定義，其相當於 false	設定此選項，可停用或啟用在執行 USB 裝置篩選時使用 Horizon Agent 設定。
viewusb.ExcludeAllDevices	{true false}	未定義，其相當於 false	使用此選項，可排除或包含所有 USB 裝置，以決定是否進行重新導向。如果設定為 true ，您可以使用其他原則設定，以允許將特定裝置或裝置系列重新導向。如果設定為 false ，您可以使用其他原則設定，以避免將特定裝置或裝置系列重新導向。如果在 Horizon Agent 上將 ExcludeAllDevices 的值設為 true ，且此設定已傳遞至 Horizon Client，則 Horizon Agent 設定會覆寫 Horizon Client 設定。
viewusb.ExcludeFamily	{m o}: <i>family_name_1</i> ; family_name_2 ;...	未定義	使用此選項，可排除裝置系列以避免進行重新導向。例如: m:bluetooth;smart-card 如果您已經啟用自動裝置分割功能，Horizon 便會檢驗複合 USB 裝置每個介面的裝置系列，以確認必須排除的介面。如果您已經停用自動裝置分割功能，Horizon 便會檢驗整個複合 USB 裝置的裝置系列。 備註 依預設系統會排除滑鼠和鍵盤不進行重新導向，因此不需使用此設定來排除。
viewusb.ExcludePath	{m o}: <i>bus-x1</i> [/ <i>y1</i>].../ <i>port-z1</i> ; <i>bus-x2</i> [/ <i>y2</i>].../ <i>port-z2</i> ;...	未定義	使用此選項，可排除位於指定集線器或連接埠路徑上的裝置，以避免進行重新導向。您必須以十六進位指定匯流排和連接埠號碼。您不能在路徑中使用萬用字元。 例如: m:bus-1/2/3_port- 02;bus-1/1/1/4_port-ff

表 6-1. /etc/vmware/config 中的組態選項 (續)

選項	值/格式	預設值	說明
viewusb.ExcludeVidPid	<code>{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</code>	未定義	設定此選項，可排除具有特定廠商和產品識別碼的裝置，以避免進行重新導向。您必須以十六進位指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。 例如: <code>o:vid-0781_pid-****;vid-0561_pid-554c</code>
viewusb.IncludeFamily	<code>{m o}:family_name_1[;family_name_2]...</code>	未定義	設定此選項，可包含能夠重新導向的裝置系列。 例如: <code>o:storage; smart-card</code>
viewusb.IncludePath	<code>{m o}:bus-x1[/y1].../port-z1[;bus-x2[/y2].../portz2;...]</code>	未定義	使用此選項，可包含指定集線器或連接埠路徑上能夠重新導向的裝置。您必須以十六進位指定匯流排和連接埠號碼。您不能在路徑中使用萬用字元。 例如: <code>m:bus-1/2_port-02;bus-1/7/1/4_port-0f</code>
viewusb.IncludeVidPid	<code>{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</code>	未定義	設定此選項，可包含具有指定廠商和產品識別碼且能夠重新導向的裝置。您必須以十六進位指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。 例如: <code>o:vid-***_pid-0001;vid-0561_pid-554c</code>
viewusb.SplitExcludeVidPid	<code>{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</code>	未定義	使用此選項，可排除或包含指定的複合 USB 裝置，以決定是否根據廠商和產品識別碼進行分割。設定的格式為 <code>vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</code> 。 您必須以十六進位格式指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。 範例: <code>m:vid-0f0f_pid-55**</code>
viewusb.SplitVidPid	<code>{m o}:vid-xxxx_pid-yyy([exintf:zz[;exintf:ww]])[;...]</code>	未定義	設定此選項，可將根據廠商和產品識別碼指定的複合 USB 裝置元件視為個別裝置。設定的格式為 <code>vid-xxxx_pid-yyy(exintf:zz[;exintf:ww])</code> 。 您可以使用 exintf 關鍵字，藉由指定它們的介面號碼來將元件自重新導向清單中排除。您必須以十六進位指定識別碼，及以十進位指定介面號碼，包括任何前置的 0。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。 範例: <code>o:vid-0f0f_pid-*** (exintf-01);vid-0781_pid-554c(exintf:01;exintf:02)</code> 備註 Horizon 不會自動包含您未明確排除的元件。您必須指定篩選原則，例如 納入 VidPid 裝置 ，以納入那些元件。

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

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

表 6-2. /etc/vmware/viewagent-custom.conf 中的組態選項

選項	值	預設值	說明
CDREnable	true 或 false	true	使用此選項，可啟用或停用用戶端磁碟機重新導向 (CDR) 功能。
CollaborationEnable	true 或 false	true	使用此選項，可啟用或停用 Linux 桌面平台上的工作階段協作功能。
EndpointVPNEnable	true 或 false	false	設定此選項，可在對 Dynamic Environment Manager 主控台中所使用端點 IP 位址的範圍評估端點 IP 位址時，指定要使用用戶端的實體網路卡 IP 位址或 VPN IP 位址。如果選項設為 false，則會使用用戶端的實體網路卡 IP 位址。否則，即會使用 VPN IP 位址。
HelpDeskEnable	true 或 false	true	設定此選項，可啟用或停用 Help Desk Tool 功能。
KeyboardLayoutSync	true 或 false	true	<p>使用此選項，可指定是否將用戶端的系統地區設定清單和目前的鍵盤配置與 Linux 版 Horizon Agent 桌面平台同步。</p> <p>當此設定已啟用或未設定時，則允許進行同步化。當此設定已停用時，則不允許進行同步化。</p> <p>僅 Windows 版 Horizon Client 支援此功能，並且僅適用於英文、法文、德文、日文、韓文、西班牙文、簡體中文和繁體中文地區設定。</p>
LogCnt	整數	-1	<p>使用此選項以設定 /tmp/vmware-root 中保留的記錄檔計數。</p> <ul style="list-style-type: none"> ■ -1 - 全部保留 ■ 0 - 全部刪除 ■ > 0 - 保留的記錄檔計數。
NetbiosDomain	全大寫字母的文字字串		設定 True SSO 時，使用此選項來設定您組織的網域的 NetBIOS 名稱。
OfflineJoinDomain	pbis 或 samba	pbis	使用此選項可設定即時複製離線網域加入。執行離線網域加入的可用方法包括 PowerBroker Identity Services Open (PBISO) 驗證和 Samba 離線網域加入。如果此屬性的值不是 pbis 或 samba，則會忽略離線網域加入。
RunOnceScript			<p>使用此選項可將複製的虛擬機器重新加入至 Active Directory。主機名稱變更後，請設定 RunOnceScript 選項。指定的指令碼只會在第一次主機名稱變更後執行一次。當代理程式服務啟動，且主機名稱在代理程式安裝後有所變更時，即會以根權限執行指令碼。</p> <p>以 Winbind 解決方案為例，您必須將基礎虛擬機器加入含有 Winbind 的 Active Directory，並將此選項設定為指令碼路徑。指令碼必須包含網域重新加入命令 /usr/bin/net ads join -U <ADUserName>%<ADUserPassword>。在虛擬機器複製之後，作業系統自訂會變更主機名稱。當代理程式服務啟動時，指令碼即會執行，而將複製的虛擬機器加入 Active Directory。</p>
RunOnceScriptTimeout		120	<p>使用此選項來為 RunOnceScript 選項設定逾時時間 (秒)。</p> <p>例如，設定 RunOnceScriptTimeout=120</p>

表 6-2. /etc/vmware/viewagent-custom.conf 中的組態選項 (續)

選項	值	預設值	說明
SSLCiphers	文字字串	!aNULL:kECDH +AESGCM:ECDH +AESGCM:RSA +AESGCM:kECDH +AES:ECDH+AES:RSA +AES	使用此選項來指定加密清單。您必須使用 https://www.openssl.org/docs/manmaster/man1/ciphers.html 中定義的格式。
SSLProtocols	文字字串	TLSv1_1:TLSv1_2	使用此選項來指定安全性通訊協定。支援的通訊協定為 TLSv1.0、TLSv1.1 和 TLSv1.2。
SSODesktopType	UseGnomeClassic 、 UseGnomeFlashback 、 UseGnomeUbuntu 、 UseMATE 或 UseKdePlasma	UseGnomeClassic	<p>此選項會指定 SSO 啟用時所要使用的桌面平台環境，而不是預設桌面平台環境。</p> <p>在指定要使用選取的桌面平台環境之前，您必須先確定您的桌面平台已安裝該環境。在 Ubuntu 16.04/18.04 桌面平台中設定此選項後，無論 SSO 功能是否啟用，此選項都會生效。如果在 RHEL.x/CentOS 7.x 桌面平台中指定此選項，則必須在啟用 SSO 後，才會使用選取的桌面平台環境。</p> <p>備註 RHEL/CentOS 8.0 和 RHEL/CentOS 6.x 桌面平台不支援此選項。Horizon 7 僅支援 RHEL/CentOS 8.0 桌面平台上的 Gnome 桌面平台環境。如需在 RHEL/CentOS 6.x 桌面平台上啟用 SSO 時如何將 KDE 設定為預設桌面平台環境的詳細資訊，請參閱桌面平台環境。</p>
SSOEnable	true 或 false	true	設定此選項可啟用/停用單一登入 (SSO)。
SSOUserFormat	文字字串	[username]	<p>使用此選項來指定 Single Sign-On 登入名稱的格式。預設值為僅使用者名稱。如果也需要網域名稱，請設定此選項。一般來說，登入名稱為網域名稱加上特殊字元並接著使用者名稱。如果特殊字元為反斜線，您必須使用另一個反斜線來逸出。登入名稱格式的範例如下所示：</p> <ul style="list-style-type: none"> ■ SSOUserFormat=[domain]\\[username] ■ SSOUserFormat=[domain]+[username] ■ SSOUserFormat=[username]@[domain]
子網路	採用 CIDR IP 位址格式 的值	[subnet]	將此選項設定為子網路，其他機器可用它來連線至 Horizon Agent for Linux。如果有多個具有不同子網路的本機 IP 位址，則會使用已設定子網路中的本機 IP 位址來連線至 Horizon Agent for Linux。您必須以 CIDR IP 位址格式指定該值。例如，Subnet=123.456.7.8/24。
UEMEnable	true 或 false	false	設定此選項，可啟用或停用 Dynamic Environment Manager 智慧型原則。如果選項設為啟用，且在滿足 Dynamic Environment Manager 智慧型原則中的條件時，即會強制執行原則。
UEMNetworkPath	文字字串		此選項必須設定為在 Dynamic Environment Manager 主控台中設定的相同網路路徑。路徑的格式必須類似於 //10.111.22.333/view/LinuxAgent/UEMConfig。

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

使用 智慧原則

您可使用智慧原則建立原則，以控制特定遠端 Linux 桌面平台上 USB 重新導向、剪貼簿重新導向以及用戶端磁碟機重新導向功能的行為。

您可以為使用者環境設定建立原則，以控制 USB 重新導向、虛擬列印、剪貼簿重新導向、用戶端磁碟機重新導向、Web 和 Chrome 檔案傳輸功能，以及頻寬設定檔在已發佈的桌面平台或應用程式中的行為。使用者環境設定的 Horizon 智慧型原則會在登入期間套用，且可在工作階段重新連線期間重新整理。若要在使用者重新連線至工作階段時重新套用 Horizon 智慧型原則，您可以設定觸發的工作。

您可以為 Dynamic Environment Manager 在使用者電腦開機時套用的電腦環境設定建立原則。這些 Horizon 智慧型原則會控制 Flash 多媒體重新導向、Integrated Printing 和 USB 重新導向的行為。電腦環境設定的 Horizon 智慧型原則會在電腦開機期間套用，且可在工作階段重新連線期間重新整理。

使用智慧原則，您可以建立只在符合特定條件時才生效的原則。例如，您可以設定一個原則，在使用者從公司網路外部連線至遠端桌面平台時，停用用戶端磁碟機重新導向功能。

智慧原則的需求

若要使用智慧原則，您的 Horizon 7 環境必須符合特定需求。

- 您必須在想以智慧原則管理的遠端桌面平台上安裝 Horizon Agent 7.5 或更新版本以及 VMware Dynamic Environment Manager 9.4 或更新版本。
- 使用者必須使用 Horizon Client 4.8 或更新版本連線至您想以智慧原則管理的遠端 Linux 桌面平台。
- 必須啟用 DEMEnable 選項，且必須在 /etc/vmware/viewagent-custom.conf 檔案中設定 DEMNetworkPath 選項。請參閱在 [Linux 桌面平台上設定組態檔中的選項](#)。
- 您必須安裝用戶端套件才能存取網路共用儲存區。例如，在 Ubuntu 18.04 系統上，為已啟用 NFS 的共用儲存區安裝 nfs-common 套件，以及為已啟用 Samba 的儲存區安裝 cifs-utils 套件。

安裝 Dynamic Environment Manager

若要使用 Horizon 智慧原則來控制遠端 Linux 桌面平台上的遠端桌面平台功能行為，您必須在遠端 Windows 桌面平台上安裝 Dynamic Environment Manager 9.4 或更新版本。

您可以從 VMware 下載頁面下載 Dynamic Environment Manager 安裝程式。您可在要用來管理 Dynamic Environment Manager 環境的 Windows 桌面平台上安裝 Dynamic Environment Manager 管理主控台元件。在 Windows 桌面平台的 Dynamic Environment Manager 管理主控台中，您可以控制遠端 Linux 桌面平台上的遠端桌面平台功能行為。

對於已發佈桌面平台集區，則必須在提供已發佈桌面平台工作階段的 RDS 主機上安裝 Dynamic Environment Manager。

如需 Dynamic Environment Manager 系統需求與完整安裝指示，請參閱《安裝和設定 VMware Dynamic Environment Manager》文件。

設定 Dynamic Environment Manager

您必須先設定 Dynamic Environment Manager，才能將其用來建立遠端桌面平台功能的智慧型原則。

若要設定 Dynamic Environment Manager，請遵照《VMware Dynamic Environment Manager 管理指南》中的組態指示來進行。

Horizon 智慧型原則設定

您可建立 Horizon 智慧型原則，藉以控制 Dynamic Environment Manager 中遠端功能的行為。

您可以為使用者環境設定建立原則，以控制 USB 重新導向、虛擬列印、剪貼簿重新導向、用戶端磁碟機重新導向、Web 和 Chrome 檔案傳輸功能，以及頻寬設定檔在已發佈的桌面平台或應用程式中的行為。使用者環境設定的 Horizon 智慧型原則會在登入期間套用，且可在工作階段重新連線期間重新整理。若要在使用者重新連線至工作階段時重新套用 Horizon 智慧型原則，您可以設定觸發的工作。請參閱《VMware Dynamic Environment Manager 管理指南》中的「設定使用者環境設定的 Horizon 智慧型原則」主題中的完整原則清單。

您可以為 Dynamic Environment Manager 在使用者電腦開機時套用的電腦環境設定建立原則。這些 Horizon 智慧型原則會控制 Flash 多媒體重新導向、Integrated Printing 和 USB 重新導向的行為。電腦環境設定的 Horizon 智慧型原則會在電腦開機期間套用，且可在工作階段重新連線期間重新整理。請參閱《VMware Dynamic Environment Manager 管理指南》中的「設定電腦環境設定的 Horizon 智慧型原則」主題中的完整原則清單。

一般來說，為 Dynamic Environment Manager 中的遠端功能設定的 Horizon 智慧型原則設定，會覆寫對等的登錄機碼以及群組原則設定。

將條件新增至 Horizon 智慧型原則定義

在 Dynamic Environment Manager 中定義 Horizon 智慧型原則時，可新增必須符合才能讓原則生效的條件。例如，您可以新增只會在使用者從公司網路外部連線至遠端桌面平台時，停用用戶端磁碟機重新導向功能的條件。

重要 您必須將下列條件新增至 Horizon 智慧型原則定義，讓支援的原則設定在遠端 Linux 桌面平台中生效。這些是目前支援的唯一條件。如果已設定其他條件，條件評估的最終結果為 **false**。

表 6-3. 遠端 Linux 桌面平台的必要條件

條件	說明
Operating System Architecture	檢查作業系統的架構。值必須設為 Linux。
Endpoint IP address	檢查端點 IP 位址是否位於指定範圍。範圍開頭的空白欄位會解釋為 0，而結尾為 255。

不過，您可以設定多個 Endpoint IP address 條件，如下列範例所示。

```
Operating system is Linux
AND Endpoint IP address is in range 11.22.33.44 – 11.22.33.54
OR Endpoint IP address is in range 11.22.33.66 – 11.22.33.77
```

如需在 Dynamic Environment Manager 管理主控台中新增和編輯條件的詳細資訊，請參閱《VMware Dynamic Environment Manager 管理指南》。

在 Dynamic Environment Manager 中建立 Horizon 智慧型原則

您可以使用 Dynamic Environment Manager 管理主控台在 Dynamic Environment Manager 中建立 Horizon 智慧型原則。在定義 Horizon 智慧型原則時，可新增必須符合才能讓智慧型原則生效的條件。

必要條件

- 安裝和設定 Dynamic Environment Manager。請參閱[安裝 Dynamic Environment Manager](#) 與 [設定 Dynamic Environment Manager](#)。
- 熟悉可新增至 Horizon 智慧型原則定義的條件。請參閱[將條件新增至 Horizon 智慧型原則定義](#)。
- 啟用 DEMEnable 選項，然後在 /etc/vmware/viewagent-custom.conf 檔案中設定 DEMNetworkPath 選項。請參閱在 [Linux 桌面平台上設定組態檔中的選項](#)。

備註 在高延遲網路中，儲存您新的或更新智慧型原則之後，請讓 Dynamic Environment Manager 至少有一分鐘的時間來完成變更的處理，之後再通知使用者連線至受影響的桌面平台。

您可以為使用者環境設定建立原則，以控制 USB 重新導向、虛擬列印、剪貼簿重新導向、用戶端磁碟機重新導向、Web 和 Chrome 檔案傳輸功能，以及頻寬設定檔在已發佈的桌面平台或應用程式中的行為。使用者環境設定的 Horizon 智慧型原則會在登入期間套用，且可在工作階段重新連線期間重新整理。若要在使用者重新連線至工作階段時重新套用 Horizon 智慧型原則，請設定觸發的工作。

您可以為 Dynamic Environment Manager 在使用者電腦開機時套用的電腦環境設定建立原則。這些 Horizon 智慧型原則會控制 Flash 多媒體重新導向、Integrated Printing 和 USB 重新導向的行為。電腦環境設定的 Horizon 智慧型原則會在電腦開機期間套用，且可在工作階段重新連線期間重新整理。

如需使用 Dynamic Environment Manager 管理主控台的完整資訊，請參閱《VMware Dynamic Environment Manager 管理指南》文件。

程序

- 1 在 Dynamic Environment Manager 管理主控台中，選取**使用者環境**以建立使用者環境設定的原則，或選取**電腦環境**索引標籤以建立電腦環境設定的原則。
現有 Horizon 智慧型原則定義 (若有) 會出現在 [Horizon 智慧型原則] 窗格中。
- 2 選取 **Horizon 智慧型原則**，然後按一下**建立**，以建立新的智慧型原則。

3 選取設定索引標籤，然後定義智慧型原則設定。

- a 在 [一般設定] 區段中，於**名稱**文字方塊中輸入智慧型原則的名稱。

例如，若智慧型原則會影響用戶端磁碟機重新導向功能，可將智慧型原則命名為 **CDR**。

- b 在 [Horizon 智慧型原則設定] 區段中，選取要包括在智慧型原則中的遠端桌面平台功能和設定。

您可以選取多個遠端桌面平台功能。

4 新增使用新智慧型原則搭配遠端 Linux 桌面平台所需的條件。

- a 選取**條件**索引標籤，按一下**新增**，然後選取**作業系統架構**條件。

- b 將值設為 **Linux**。

```
Operating System is Linux
```

- c 按一下**新增**，然後選取**端點 IP 位址**條件。

依預設會新增 **AND** 運算子。

- d 在 [端點 IP 位址] 對話方塊中，設定端點的 IP 位址範圍，然後按一下**確定**。

以下是條件陳述式的範例：

```
Operating System is Linux  
AND Endpoint IP address is in range 11.22.33.44 – 11.22.33.54
```

5 按一下儲存以儲存智慧型原則。

Dynamic Environment Manager 會在每次使用者連線或重新連線到遠端桌面平台時處理 Horizon 智慧型原則。

Dynamic Environment Manager 會按照智慧型原則名稱的字母順序處理多個智慧型原則。Horizon 智慧型原則會按照字母順序出現在 [Horizon 智慧型原則] 窗格中。若智慧型原則互有衝突，則最後處理的智慧型原則會優先獲得採用。例如，若有一個名為 **Sue** 的智慧型原則會對名為 **Sue** 的使用者啟用 USB 重新導向，以及另一個名為 **Pool** 的智慧型原則會對名為 **Ubuntu1604** 的桌面平台集區停用 USB 重新導向，則當 **Sue** 連線至 **Ubuntu1604** 桌面平台集區的遠端桌面平台時，將會啟用 USB 重新導向功能。

Linux 桌面平台的 Blast 設定範例

您可以調整遠端桌面平台顯示的影像畫質，以改善使用者體驗。當網路連線不佳時，改善影像畫質有助於保持一致的使用者體驗。

VMware Blast Extreme 通訊協定設定範例

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

表 6-4. /etc/vmware/config 中的 Blast 組態選項範例

選項名稱	參數	高速 LAN	LAN	專用 WAN	寬頻 WAN	低速 WAN	極低速
頻寬設定	RemoteDisplay.maxBandwidthKbps	1000000 (1 Gbps)	1000000 (1 Gbps)	1000000 (1 Gbps)	5000 (5 Mbps)	2000 (2 Mbps)	1000 (1 Mbps)
最大 FPS	RemoteDisplay.maxFPS	60	30	30	20	15	5
音訊播放	RemoteDisplay.allowAudio	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE
顯示品質 (JPEG/PNG)	RemoteDisplay.maxQualityJPEG	90	90	90	70	60	50
顯示品質 (JPEG/PNG)	RemoteDisplay.midQualityJPEG	35	35	35	35	35	35
顯示品質 (JPEG/PNG)	RemoteDisplay.minQualityJPEG	25	25	25	20	20	20
顯示品質 (H.264)	RemoteDisplay.qpmaxH264	28	36	36	36	36	42
顯示品質 (H.264)	RemoteDisplay.qpminH264	10	10	10	10	10	10

Linux 桌面平台用戶端磁碟機重新導向選項的範例

設定用戶端磁碟機重新導向 (CDR) 選項，以判斷是否可從遠端 Linux 桌面平台存取本機系統的共用資料夾和磁碟機。

將項目新增至 /etc/vmware/config 檔案來進行 CDR 設定。

下列組態範例會共用 C:\ebooks 和 C:\spreadsheets 資料夾、將這兩個資料夾設為唯讀，並防止用戶端共用更多資料夾。

```
cdserver.forcedByAdmin=true
cdserver.sharedFolders=d:\ebooks,;c:\spreadsheets,
cdserver.permissions=R
```

在先前的範例中，逗號 "," 放置在 **ebooks** 之後，而 **spreadsheets** 對於正確選項剖析則是強制使用。

包含在 cdserver.sharedFolders 選項中的任何 "R" 會影響該設定中所列出的所有資料夾。在下列範例中，即便 R 值僅放在 /home/jsmith 資料夾路徑之後，**ebooks** 和 **spreadsheets** 資料夾仍皆為唯讀。

```
cdserver.sharedFolders=d:\ebooks,;c:\spreadsheets,;/home/jsmith,R
```

建立和管理 Linux 桌面平台集區

7

若要設定 Linux 虛擬機器以用作遠端桌面平台，您必須使用 Linux 虛擬機器來建立桌面平台集區。

Horizon for Linux 支援下列桌面平台集區類型：

- 具有 vCenter 虛擬機器的手動桌面平台集區
- 自動完整複製桌面平台集區
- 即時複製浮動桌面平台集區

若要使用 vCenter 虛擬機器來建立手動桌面平台集區，您必須在所有虛擬機器上安裝 Horizon Agent。然後使用連線伺服器桌面平台集區建立精靈，將虛擬機器新增至桌面平台集區。若要複製大量虛擬機器，請參閱 [Linux 桌面平台大量部署的概觀](#)。

若要建立自動完整複製桌面平台集區，您必須在 Linux 虛擬機器範本上安裝 Horizon 7 Agent。然後使用連線伺服器桌面平台集區建立精靈來複製完整的虛擬機器。

若要建立即時複製浮動桌面平台集區，您必須透過 PBIS Open 環境設定在 Linux 虛擬機器上安裝 Horizon 7 Agent，並從中建立範本。然後，使用連線伺服器桌面平台集區建立精靈，建立即時複製浮動桌面平台集區。

本章節討論下列主題：

- [建立 Linux 的手動桌面平台集區](#)
- [管理 Linux 桌面平台集區](#)
- [為 Linux 建立自動完整複製桌面平台集區](#)
- [為 Linux 建立即時複製浮動桌面平台集區](#)
- [代理 PowerCLI 命令](#)

建立 Linux 的手動桌面平台集區

您可以為 Linux 虛擬機器建立手動桌面平台集區。

下列程序針對 Linux 型手動桌面平台集區提供設定強制設定的指導方針。如需關於建立手動桌面平台集區的詳細資訊，請參閱《在 Horizon Console 中設定虛擬桌面平台》。

必要條件

- 驗證 Linux 客體作業系統上已安裝 Horizon Agent。請參閱在 [Linux 虛擬機器上安裝 Horizon Agent](#)。
- 確認 VMware vCenter Server 已新增至 Horizon Connection Server。

程序

- 1 在 Horizon Console 中，新增手動桌面平台集區。

選取 [詳細目錄 > 桌面平台 > 新增](#)。

備註 請不要將 Windows 和 Linux 虛擬機器建立在相同的桌面平台集區中。

- 2 選取手動桌面平台集區。
- 3 選取由 vCenter Server 管理或未受管理的虛擬機器，然後按下一步。
- 4 為桌面平台集區中的機器選取專用或浮動使用者指派，然後按下一步。
- 5 遵循精靈中的提示建立集區。

在 [桌面平台集區設定] 頁面上，設定下列選項。

選項	說明
預設顯示通訊協定	VMware Blast
允許使用者選擇通訊協定	否
3D 轉譯器	使用 vSphere Client 管理 (適用於 2D 或 vDGA 桌面平台)，針對 vGPU 桌面平台則使用 NVIDIA GRID vGPU

備註 集區設定是必要的。若未設定，您可能無法連線到桌面平台，而會遇到通訊協定錯誤或黑色畫面。

- 6 建立桌面平台集區後，請授權使用者使用桌面平台集區中的機器。在 Horizon Console 中，選取桌面平台集區、選取 **權利 > 新增權利**，並新增使用者或群組。

Linux 虛擬機器已準備就緒，可在 Horizon7 部署中作為遠端桌面平台。

管理 Linux 桌面平台集區

當您建立手動桌面平台集區並將 Linux 機器新增至集區時，您可以藉由設定來管理手動桌面平台集區。您必須只將 Linux 客體作業系統新增至手動桌面平台集區。如果集區同時包含 Windows 和 Linux 客體作業系統，則系統會將該集區視為 Windows 集區，而您無法連線至 Linux 桌面平台。

管理作業的支援

- 停用或啟用桌面平台集區
- 複製自動桌面平台集區
- 刪除桌面平台集區

您可以從 Horizon 7 中移除虛擬機器，或是從磁碟中刪除虛擬機器。

遠端設定的支援

表 7-1. 遠端設定

遠端設定	選項
遠端機器電源原則	<ul style="list-style-type: none"> ■ 不執行電源動作 ■ 確認機器電源永遠開啟 ■ 暫止 ■ 關閉電源
中斷連線後自動登出	<ul style="list-style-type: none"> ■ 立即 ■ 永不 ■ 在 n 分鐘後
允許使用者重設/重新啟動其機器	<ul style="list-style-type: none"> ■ 是 ■ 否
允許使用者從不同的用戶端裝置起始單獨的工作階段	<ul style="list-style-type: none"> ■ 是 ■ 否
「登出後刪除機器」，用於具有完整複製和浮動的自動桌面平台集區	<ul style="list-style-type: none"> ■ 是 ■ 否

支援 Horizon Console 作業

- 中斷工作階段連線
- 登出工作階段
- 重設/重新啟動桌面平台
- 傳送訊息

對於專用桌面平台集區，您可以新增或移除每個虛擬機器的使用者指派。對於大量作業，則必須使用 HorizonPowerCLI Cmdlet。

- Update-UserOwnership
- Remove-UserOwnership

備註 請勿變更遠端顯示通訊協定設定。這些設定必須維持與桌面平台集區建立期間所指定的相同。

設定	選項
預設顯示通訊協定	VMware Blast
允許使用者選擇通訊協定	否
3D 轉譯器	<ul style="list-style-type: none"> ■ 針對 2D 或 vDGA，請使用 vSphere Client 進行管理 ■ NVIDIA GRID vGPU

如需詳細資訊，請參閱《VMware Horizon Console 管理》說明文件。

為 Linux 建立自動完整複製桌面平台集區

您可以為 Linux 虛擬機器建立自動完整複製桌面平台集區。建立自動完整複製桌面平台集區之後，您可以使用 Linux 虛擬機器作為 Horizon 7 部署中的遠端桌面平台。

下列程序針對 Linux 型自動完整複製桌面平台集區提供設定強制設定的指導方針。如需關於建立自動完整複製桌面平台集區的詳細資訊，請參閱《在 Horizon Console 中設定虛擬桌面平台》。

必要條件

- 驗證 Linux 客體作業系統上已安裝 Horizon Agent。請參閱在 [Linux 虛擬機器上安裝 Horizon Agent](#)。
- 執行虛擬機器複製之前，請建立複製所依據的虛擬機器範本。請參閱[建立用於複製 Linux 桌面平台機器的虛擬機器範本](#)。
- 如果您使用 Winbind 解決方案來將 Linux 虛擬機器加入 Active Directory，您必須在虛擬機器範本中完成 Winbind 解決方案的設定。
- 如果您使用 Winbind 解決方案，則必須在虛擬機器上執行網域加入命令。在 Shell 指令碼中併入命令，並指定 /etc/vmware/viewagent-custom.conf 中 Horizon Agent 選項 RunOnceScript 的指令碼路徑。如需詳細資訊，請參閱在 [Linux 桌面平台上設定組態檔中的選項](#)。
- 驗證 vCenter Server 已新增至 Horizon 連線伺服器。

程序

1 建立客體自訂規格。

請參閱 vSphere 虛擬機器管理文件中的「在 vSphere Web Client 中建立 Linux 的自訂規格」。建立規格時，請確定您正確指定下列設定。

設定	值
目標虛擬機器作業系統	Linux
電腦名稱	使用虛擬機器名稱。
網域	指定 Horizon 7 環境的網域。
網路設定	使用標準網路設定。
主要 DNS	指定有效位址。

備註 如需客體作業系統自訂支援對照表的詳細資訊，請參閱 <http://partnerweb.vmware.com/programs/guestOS/guest-os-customization-matrix.pdf>。

2 在 Horizon Console 中，新增自動桌面平台集區。

選取**詳細目錄 > 桌面平台 > 新增**。

3 選取自動桌面平台集區，然後按下一步。

4 選取完整虛擬機，接著選取 vCenter Server 執行個體，然後按下一步。

5 遵循精靈中的提示建立集區。

- a 在 [桌面平台集區設定] 頁面上，設定下列選項。

選項	說明
預設顯示通訊協定	VMware Blast
允許使用者選擇通訊協定	否
3D 轉譯器	使用 vSphere Client 管理 (適用於 2D 或 vDGA 桌面平台)，針對 vGPU 桌面平台則使用 NVIDIA GRID vGPU

- b 出現提示時，請設定**虛擬機器命名**選項。

選項	說明
手動指定名稱	手動輸入名稱。
命名模式	例如，指定 LinuxVM-{n}。 您也必須指定下列桌面平台集區大小調整選項： <ul style="list-style-type: none"> ■ 機器數目上限 ■ 備用、電源開啟機器數目

- c 出現提示時，請依序選取 vCenter Server 設定。

您無法略過 vCenter Server 設定：

- 1 範本
 - 2 虛擬機器資料夾位置
 - 3 主機或叢集
 - 4 資源集區
 - 5 資料存放區
- 6 建立桌面平台集區後，請授權使用者使用桌面平台集區中的機器。在 Horizon Console 中，選取桌面平台集區、選取**權利 > 新增權利**，並新增使用者或群組。
- 7 等候直到桌面平台集區中的所有 Linux 虛擬機器皆變為可用。

為 Linux 建立即時複製浮動桌面平台集區

您可以使用**新增桌面平台集區**精靈，為 Linux 虛擬機器建立即時複製浮動桌面平台集區。建立即時複製浮動桌面平台集區後，您可以將 Linux 虛擬機器作為 Horizon 7 部署中的遠端桌面平台。

Horizon 7 Agent for Linux 僅在具有 Ubuntu 18.04/16.04、RHEL 7.1 或更新版本、RHEL 8.0 或 SLED/SLES 12.x 的系統上支援即時複製桌面平台集區。

備註 從 Linux 桌面平台建立的即時複製桌面平台集區上不支援 vGPU 圖形功能。

下列程序針對 Linux 型即時複製桌面平台集區提供設定強制設定的指導方針。如需關於建立即時複製桌面平台集區的詳細資訊，請參閱《在 Horizon Console 中設定虛擬桌面平台》。

必要條件

- 熟悉在 vCenter Server 中建立虛擬機器和安裝 Linux 作業系統的步驟。如需詳細資訊，請參閱[建立虛擬機器和安裝 Linux](#)。
- 瞭解使用 PBISO 驗證解決方案或 Samba Winbind 離線加入進行 AD 整合的步驟。如需詳細資訊，請參閱[設定 PowerBroker Identity Services Open \(PBISO\) 驗證](#)或[設定 Samba 離線網域加入](#)。

備註 若要從執行 RHEL 8.0 的 Linux 虛擬機器建立即時複製桌面平台集區，請使用 Samba Winbind 離線加入來執行 AD 整合。使用 PBISO 驗證的 RHEL 8.0 虛擬機器不支援即時複製桌面平台集區。

- 熟悉 Horizon 7 Agent for Linux 的安裝步驟。如需詳細資訊，請參閱在[Linux 虛擬機器上安裝 Horizon Agent](#)。
- 瞭解使用 VMware vSphere Web Client 為已關閉電源的 Linux 虛擬機器擷取快照的步驟。請參閱《vSphere 單一主機管理 - VMware Host Client》中的〈在 VMware Host Client 中擷取快照〉。
- 確認 vCenter Server 已新增至 Horizon 連線伺服器。

程序

- 1 建立已安裝 Ubuntu 18.04/16.04、RHEL 7.1 或更新版本、RHEL 8.0 或 SLED/SLES 12.x 的 Linux 虛擬機器 (VM)。

如需詳細資訊，請參閱[建立虛擬機器和安裝 Linux](#)。

- 2 使用下列命令，在 Ubuntu 18.04/16.04 機器上手動安裝 Open VMware Tools (OVT):

```
# apt-get install open-vm-tools
```

如需其他資訊，請參閱[準備用於遠端桌面平台部署的 Linux 機器](#)。

- 3 安裝 Linux 發行版所需的任何相依性套件。

如需詳細資訊，請參閱[安裝 Horizon Agent 相依性套件](#)。

- 4 在 Linux 虛擬機器中安裝 Horizon Agent for Linux。

```
# sudo ./install_viewagent.sh -A yes
```

如需詳細資料，請參閱在[Linux 虛擬機器上安裝 Horizon Agent](#)。

- 5 整合您的 Linux 虛擬機器與 Active Directory。

- 若要使用 PBISO 驗證解決方案，請執行下列步驟：
 - a 從 <https://www.beyondtrust.com/products/powerbroker-identity-services-open/> 下載 PBIS Open 8.5.6 或更新版本，並將其安裝在您的 Linux 虛擬機器上。

```
# sudo ./pbis-open-8.5.6.2029.linux.x86_64.deb.sh
```

- b 使用[整合 Linux 與 Active Directory](#)的〈PowerBroker Identity Services Open (PBISO) 驗證〉一節中的資訊，整合您的 Linux 虛擬機器與 Active Directory。

- 若要使用 Samba Winbind 離線加入，請在 `/etc/vmware/viewagent-custom.conf` 檔案中將 `OfflineJoinDomain` 設定為 `samba`。

備註 您必須使用 Samba Winbind 將 RHEL 8.0 虛擬機器與 Active Directory 整合。否則，即時複製浮動桌面平台集區的建立將會失敗。

- 如果要停用離線網域加入功能，您必須在 `OfflineJoinDomain/etc/vmware/viewagent-custom.conf` 檔案中將 選項設定為無。否則，即時複製浮動桌面平台集區的建立將會失敗。

- 6 如果您的 DHCP 伺服器不會廣播至 DNS 伺服器，請為您的 Linux 系統指定 DNS 伺服器。

在建立新的即時複製虛擬機器時，會新增新的虛擬網路介面卡。當新的網路介面卡新增至即時複製虛擬機器時，虛擬機器範本中的任何網路介面卡設定 (如 DNS 伺服器) 都會遺失。PBIS 需要有效的 DNS 伺服器，`/etc/hosts` 中的 FQDN 對應並不合用。為避免在新的網路介面卡新增至複製的虛擬機器時遺失 DNS 伺服器設定，您必須在 Linux 系統中指定 DNS 伺服器。例如，在 Ubuntu 16.04 系統中，您可以將以下幾行新增至 `/etc/resolvconf/resolv.conf.d/head` 檔案中，以指定 DNS 伺服器。

```
nameserver 10.10.10.10
search mydomain.org
```

- 7 (選用) 如果您想要在主要 Linux VDI 即時複製代理程式的 `/etc/fstab` 檔案中新增 NFS 掛接，請使用下列其中一個方法。

- 在 `/etc/fstab` 中新增「soft」旗標，例如：

```
10.111.222.333:/share /home/nfsmount nfs
size=8192,wsz=8192,timeo=14,soft,intr,tcp
```

- 如果您不想在 `/etc/fstab` 中使用「soft」旗標，則無法在主要 Linux 虛擬機器映像中設定 `/etc/fstab`。您可以撰寫關閉電源指令碼以設定 `/etc/fstab` 檔案，然後為 ClonePrep 工具指定此關閉電源指令碼。如需詳細資訊，請參閱《VMware Horizon Console 管理》文件。

- 8 關閉 Linux 虛擬機器，然後使用 VMware vSphere® Web Client 為您關閉電源的 Linux 虛擬機器建立快照，以建立主要映像。

如需相關資訊，請參閱《vSphere 單一主機管理 - VMware Host Client》中的〈在 VMware Host Client 中擷取快照〉。

- 9 在 Horizon Console 中，新增自動桌面平台集區。

選取 **詳細目錄 > 桌面平台 > 新增**。

- 10 選取 **自動桌面平台集區**，然後按下一步。

- 11 選取 **即時複製**，接著選取 **vCenter Server 執行個體**，然後按下一步。

12 遵循精靈中的提示建立集區。

- a 出現提示時，請設定**虛擬機器命名**選項。

選項	說明
啟用佈建	選取此選項。
發生錯誤時停止佈建	選取此選項。
命名模式	指定 Horizon 7 在所有桌面平台虛擬機器名稱中用作前置詞 (後面再加上唯一數字) 的模式。例如，指定 LinuxVM-{n} 。
機器的最大數目	指定集區中的機器總數。
備用 (開啟電源) 機器數目	指定要保留給使用者使用的桌面平台虛擬機器數目。
預先佈建所有機器	選取此選項可讓 Horizon 7 佈建 機器的最大數目 中指定的虛擬機器數目。

- b 出現提示時，請選取**使用 VMware Virtual SAN** 作為儲存空間管理原則。
- c 出現提示時，請指定網域設定、AD 容器，以及任何必須在複製虛擬機器後執行的其他自訂指令碼。

重要 當您使用 ClonePrep 關閉電源或同步後指令碼時，請確認指令碼位於 `/var/userScript` 資料夾中、擁有者為根使用者，並將檔案權限設定為 700。

在 Horizon Console 中，您可以藉由選取**詳細目錄 > 桌面平台**，來檢視新增至集區的桌面平台虛擬機器。

在您建立集區後，如果集區還存在，則請勿刪除主要映像或從 vCenter Server 詳細目錄中加以移除。如果您誤將主要映像虛擬機器從 vCenter Server 詳細目錄中移除，則必須將其新增回詳細目錄，然後使用目前的映像執行推送映像。

後續步驟

賦予使用者存取集區的權利。請參閱《在 Horizon Console 中設定虛擬桌面平台》中的〈將權利新增至桌面平台集區〉。

代理 PowerCLI 命令

用來在連線伺服器和 Windows 桌面平台上執行各種管理工作的 Horizon PowerCLI Cmdlet，也可用於 Linux 桌面平台。

建立手動桌面平台集區

```
Add-ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadRender usevc|vgpu -
Pool_id <pool id> [more parameters]
```

下列選項和值為 Linux 桌面平台的必要項目。

- DefaultProtocol Blast
- AllowProtocolOverride \$false

- `threedRender usevc|vgpu`。若為 vGPU 桌面平台，請使用 `-threedRender vgpu`，若為 2D/DGA 桌面平台，請使用 `-threedRender usevc`。

範例

- 建立名為 `LinuxDesktop`、具有虛擬機器 (VM) `LinuxVM-01` 的浮動 Linux 桌面平台集區。

```
Add-ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -threedRender usevc -Pool_id
LinuxDesktop -Id (Get-DesktopVM -Name LinuxVM-01).id -Persistence NonPersistent -Vc_name
myvc.myorg.org
```

- 建立名為 `LinuxDesktop` 的專用 Linux vGPU 桌面平台集區，所有虛擬機器皆以 `LinuxVM-` 作為虛擬機器名稱的開頭。

```
Get-DesktopVM | Where-Object {$_.Name.StartsWith("LinuxVM-")} | Add-ManualPool -DefaultProtocol
Blast -AllowProtocolOverride $false -Persistence Persistent -threedRender vgpu -Pool_id
LinuxDesktop
```

- 建立具有第一個 RHEL 6 x64 虛擬機器的浮動 Linux 桌面平台集區 `LinuxDesktop`。

```
Get-DesktopVM | Where-Object {$_.GuestID -eq "rhel6_64Guest"} | Select-Object -Index 0 | Add-
ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -Persistence NonPersistent -
threedRender usevc -Pool_id LinuxDesktop
```

建立完整複製自動桌面平台集區

```
Add-AutomaticPool -DefaultProtocol Blast -AllowProtocolOverride $false -threedRender usevc|vgpu `
-Pool_id <pool id> -Vc_id <vCenter id> `
-NamePrefix <VM Name Prefix>" `
-templatePath <Virtual Machine Template Path> `
-VmFolderPath <Virtual Machine Folder Path> `
-ResourcePoolPath <Resource Pool Path> `
-dataStorePaths <Datastore Path> `
-customizationSpecName <Customization Specification Name> `
[more parameters]
```

下列選項和值為 Linux 桌面平台的必要項目。

- `DefaultProtocol Blast`
- `AllowProtocolOverride $false`
- `threedRender usevc|vgpu` 若為 vGPU 桌面平台，請使用 `-threedRender vgpu`，若為 2D 桌面平台，請使用 `-threedRender usevc`。

範例

```
Add-AutomaticPool -DefaultProtocol Blast -AllowProtocolOverride $false -threedrender usevc `
-pool_id FullClone-Linux `
-Vc_id (Get-ViewVC -serverName myvc.myorg.org).vc_id `
-NamePrefix "FullClone-{n:fixed=3}" `
-Persistence NonPersistent -deletePolicy DeleteOnUse `
-VmFolderPath "/LinuxVDI/vm/FullClone" `
-ResourcePoolPath "/LinuxVDI/host/LinuxVDICluster/Resources" `
```

```
-templatePath "/LinuxVDI/vm/LinuxTemplate" `
-dataStorePaths "/LinuxVDI/host/LinuxVDICluster/datastore" `
-customizationSpecName "linux-spec" `
-maximumCount 100
```

新增或移除桌面平台集區權利

- 為網域 mydomain.org 的網域使用者群組賦予 LinuxDesktop 的權利。

```
Add-PoolEntitlement -Pool_id LinuxDesktop -Sid (Get-User -Name "domain user" -Domain
"mydomain.org").sid
```

- 移除 mydomain.org 網域的網域使用者群組對 LinuxDesktop 的權利。

```
Remove-PoolEntitlement -Pool_id LinuxDesktop -Sid (Get-User -Name "domain user" -Domain
"mydomain.org").sid
```

對專用桌面平台集區中的虛擬機器指派或移除使用者

- 將 myuser 使用者指派給位於專用桌面平台集區中的 LinuxVM-01 虛擬機器。

```
Update-UserOwnership -Machine_id (Get-DesktopVM -Name "LinuxVM-01").machine_id -Sid (Get-User -
Name "myuser" | Where-Object {$_.cn -eq "myuser"}).sid
```

- 從位於專用桌面平台集區中的 LinuxVM-01 虛擬機器移除 myuser 使用者。

```
Remove-UserOwnership -Machine_id (Get-DesktopVM -Name "LinuxVM-01").machine_id
```

登出桌面平台連線

- 從 myuser 的桌面平台工作階段中登出。

```
Get-RemoteSession -Username "mydomain.org\myuser" | Send-SessionLogoff
```

如需代理 PowerCLI Cmdlet 的詳細資訊，請參閱《Horizon 7 整合》中的〈使用 Horizon PowerCLI 模組〉。

針對手動桌面平台集區大量部署 Horizon 7

8

利用 Horizon Console，您可以自動建立 Windows (而非 Linux) 桌面平台機器集區。不過，您可以開發能夠自動化部署 Linux 桌面平台機器集區的指令碼。

提供的範例指令碼僅供說明之用。對於使用範例指令碼時可能產生的問題，VMware 概不負責。

本章節討論下列主題：

- [Linux 桌面平台大量部署的概觀](#)
- [Linux 桌面平台大量升級的概觀](#)
- [建立用於複製 Linux 桌面平台機器的虛擬機器範本](#)
- [用於部署 Linux 桌面平台的範例 PowerCLI 指令碼輸入檔](#)
- [用於複製 Linux 虛擬機器的範例指令碼](#)
- [將複製的虛擬機器加入 AD 網域的範例指令碼](#)
- [使用 SSH 將複製的虛擬機器加入 AD 網域的範例指令碼](#)
- [上傳組態檔至 Linux 虛擬機器的範例指令碼](#)
- [使用 SSH 上傳組態檔至 Linux 虛擬機器的範例指令碼](#)
- [在 Horizon Agent 上升級 Linux 桌面平台機器的範例 PowerCLI 指令碼](#)
- [使用 SSH 在 Linux 虛擬機器上升級 Horizon Agent 的範例指令碼](#)
- [在 Linux 虛擬機器上執行作業的範例指令碼](#)

Linux 桌面平台大量部署的概觀

要部署 Linux 的手動桌面平台，必須執行數個步驟。如果計劃部署多個桌面平台，您可以使用 PowerCLI 指令碼將一些步驟自動化。

對於部分作業，您可以選擇讓 PowerCLI 或 SSH 在 Linux 機器上執行命令。下表說明這兩個方法之間的差異。

PowerCLI	SSH
不需安裝額外工具。	<ul style="list-style-type: none"> ■ 針對 Ubuntu，您必須使用 <code>sudo apt-get install openssh-server</code> 命令安裝 SSH 伺服器。針對 RHEL 和 CentOS，預設會安裝 <code>openssh-server</code>，但您必須確保防火牆設定可允許 <code>ssh</code>。 ■ 必須下載 SSH 用戶端應用程式 <code>pscp.exe</code> 和 <code>plink.exe</code>，並將它們放在與 PowerCLI 指令碼相同的資料夾中。
上傳檔案和命令執行較緩慢。	上傳檔案和命令執行較快速。
必須提供 ESXi 主機的管理員認證。	不須提供 ESXi 主機的管理員認證。
無法處理執行指令碼來安裝 Horizon Agent 時管理員密碼中的特殊字元，或執行指令碼來加入網域時 AD 使用者密碼中的特殊字元。	可以處理執行指令碼來安裝 Horizon Agent 時管理員密碼中的特殊字元，或執行指令碼來加入網域時 AD 使用者密碼中的特殊字元。

備註 PowerCLI 式和 SSH 式指令碼均可處理 vCenter Server 管理員和 Linux 管理員密碼中的特殊字元。PowerCLI 式指令碼也可以處理 ESXi 主機管理員密碼中的特殊字元。在上述所有情況下，不需使用逸出字元。

如需 vSphere PowerCLI 的詳細資訊，請參閱 <https://www.vmware.com/support/developer/PowerCLI>。

大量部署一組 Linux 桌面平台的程序涉及下列步驟：

- 1 建立虛擬機器範本，然後在虛擬機器上安裝 Horizon Agent。

請參閱[建立用於複製 Linux 桌面平台機器的虛擬機器範本](#)。

- 2 建立客體自訂規格。

請參閱 vSphere 虛擬機器管理文件中的「在 vSphere Web Client 中建立 Linux 的自訂規格」。建立規格時，請確定您正確指定下列設定。

設定	值
目標虛擬機器作業系統	Linux
電腦名稱	使用虛擬機器名稱。
網域	指定 Horizon 7 環境的網域。
網路設定	使用標準網路設定。
主要 DNS	指定有效位址。

備註 如需客體作業系統自訂支援對照表的詳細資訊，請參閱 <http://partnerweb.vmware.com/programs/guestOS/guest-os-customization-matrix.pdf>。

- 3 複製虛擬機器。

請參閱[用於複製 Linux 虛擬機器的範例指令碼](#)。

- 4 如果您使用 Winbind 解決方案，請將複製的虛擬機器加入 Active Directory (AD) 網域中。您可以使用下面的範例指令碼來執行網域加入命令，或使用 `/etc/vmware/viewagent-custom.conf` 中的選項 `RunOnceScript` (設定於範本虛擬機器中) 來執行。

請參閱[將複製的虛擬機器加入 AD 網域的範例指令碼](#)或使用 [SSH](#) 將複製的虛擬機器加入 AD 網域的範例指令碼。

5 更新虛擬機器中的組態選項。

請參閱[上傳組態檔至 Linux 虛擬機器的範例指令碼](#)或使用 [SSH](#) 上傳組態檔至 Linux 虛擬機器的範例指令碼。

6 建立桌面集區。

請參閱[建立 Linux 的手動桌面平台集區](#)。

如需執行開機、關機、重新啟動或刪除虛擬機器的範例指令碼，請參閱在 [Linux 虛擬機器上執行作業的範例指令碼](#)。此指令碼可從 vCenter Server 刪除虛擬機器。

Linux 桌面平台大量升級的概觀

要大量升級 Linux 的手動桌面平台，必須執行數個步驟。您可以使用 PowerCLI 指令碼將部分步驟自動化。

大量升級未受管理的桌面平台

若要將未受管理的虛擬機器大量升級為受管理或未受管理的虛擬機器，您必須使用範例升級指令碼將新的 Horizon Agent 上傳至現有的虛擬機器，然後執行升級命令。

- 如果您保留未受管理的虛擬機器，則可重複使用您現有的桌面平台集區。
- 如果您從未受管理的虛擬機器升級為受管理的虛擬機器，您必須刪除現有的桌面平台集區，然後建立新的桌面平台集區。如需詳細資訊，請參閱[升級 Linux 虛擬機器上的 Horizon Agent](#)。

大量升級受管理的桌面平台

若要大量升級受管理的虛擬機器，請選取下列其中一個方法。

方法	說明
在範本虛擬機器中，安裝或升級新的 Horizon Agent，並建立快照。	<ul style="list-style-type: none"> ■ 現有的虛擬機器已刪除，因此使用者資料和設定檔將會遺失，除非使用者資料和設定檔位於共用伺服器上，例如 NFS 伺服器。 ■ 完成虛擬機器取代後，View Administrator 上的虛擬機器狀態可能會是「遺失」。您必須重新啟動代理服務加以修正。
使用升級的範例指令碼將新的 Horizon Agent 上傳至現有的虛擬機器，然後執行升級命令。	使用者資料和設定檔會保留下來。

建立用於複製 Linux 桌面平台機器的虛擬機器範本

執行虛擬機器複製之前，您必須建立複製所依據的虛擬機器範本。

必要條件

- 驗證您的部署符合支援 Linux 桌面平台的需求。請參閱 [Horizon 7for Linux 的系統需求](#)。

- 熟悉在 vCenter Server 中建立虛擬機器和安裝客體作業系統的步驟。請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的「建立和準備虛擬機器」。
- 熟悉您必須與虛擬機器搭配使用之顯示器所需的視訊記憶體 (vRAM) 值。請參閱 [2D 圖形卡的虛擬機器設定](#)。
- 請熟悉 AD 整合的步驟。請參閱第 3 章 設定 Linux 桌面平台的 Active Directory 整合。
- 熟悉在 Linux 上安裝 Horizon Agent 的步驟。請參閱第 5 章 安裝 Horizon Agent。
- 如有必要，請熟悉使用 Horizon 7 組態檔設定選項的步驟。請參閱第 6 章 Linux 桌面平台的組態選項。
- 若您計劃安裝圖形卡，請熟悉相關步驟。請參閱第 4 章 設定 Linux 桌面平台的圖形卡。

程序

- 1 在 vSphere Web Client 或 vSphere Client 中，建立新虛擬機器。
- 2 設定自訂組態選項。
 - a 在虛擬機器上按一下滑鼠右鍵，然後按一下**編輯設定**。
 - b 指定 vCPU 和 vMemory 大小的數量。
請遵循 Linux 發行版安裝指南中的 vCPU 及 vMemory 大小準則。
例如，Ubuntu 18.04 指定對 vMemory 設定 2048 MB 和 2 個 vCPU。
 - c 選取**視訊卡**，並指定顯示器數量和總視訊記憶體 (vRAM)。
針對使用 2D 圖形的虛擬機器 (使用 VMware 驅動程式)，設定 vSphere Web Client 中的 vRAM 大小。vRAM 大小在 vDGA 或 NVIDIA GRID vGPU 機器 (使用 NVIDIA 驅動程式) 上沒有影響。
請遵循 [2D 圖形卡的虛擬機器設定](#)中的指導方針。請勿使用視訊記憶體計算機。
- 3 將虛擬機器開機並安裝 Linux 發行版。
- 4 建立具備 root 權限的使用者，例如：ViewUser。這個使用者僅用來安裝和解除安裝 Horizon Agent。
- 5 編輯 /etc/sudoers 和新增行 ViewUser ALL=(ALL) NOPASSWD:ALL。
透過 /etc/sudoers 中的這行，不需要密碼即可以 ViewUser 的身分執行 sudo。執行本章節中提供的範例指令碼來安裝 Horizon Agent 時，您會指定 ViewUser 作為輸入。
- 6 如果 Linux 發行版為 RHEL、CentOS 或 NeoKylin，請編輯 /etc/sudoers 並註解排除下列行：


```
Defaults requiretty
Defaults !visiblepw
```
- 7 如果 Linux 發行版不是 RHEL/CentOS 8.x、RHEL/CentOS 7.x 或 SLED/SLES 12.x，請安裝 VMware Tools。
RHEL/CentOS 8.0、RHEL/CentOS 7.x 與 SLED/SLES 12.x 依預設會安裝 Open VM Tools。

8 安裝和設定相依性套件。

- a 如果 Linux 發行版執行的是低於 9.10 的 Open VM Tools 版本，請安裝 deployPkg 外掛程式。

指示位於 <http://kb.vmware.com/kb/2075048>。

- b 如果 Linux 發行版為 Ubuntu，請參閱下列知識庫文章來判斷要在虛擬機器中安裝和設定的相依性套件。

- 針對 Ubuntu 18.04 和 16.04，請參閱知識庫文章 <https://kb.vmware.com/s/article/2051469> 和 <https://kb.vmware.com/s/article/59687>。

- 針對 Ubuntu 18.04，也請參閱知識庫文章 <https://kb.vmware.com/s/article/56409>。

9 針對 RHEL 和 CentOS，請啟用 [網路連線] 設定自動連線。

10 執行 AD 整合工作。

11 執行安裝圖形卡的步驟。

12 安裝 Horizon Agent。

```
sudo ./install_viewagent.sh -A yes
```

請參閱第 5 章 安裝 Horizon Agent。

13 使用 Horizon 7 組態檔執行其他組態。

14 關閉虛擬機器並建立快照。

用於部署 Linux 桌面平台的範例 PowerCLI 指令碼輸入檔

部署 Linux 桌面平台的範例 PowerCLI 指令碼會讀取包含桌面平台機器相關資訊的輸入檔。

輸入檔的類型為 csv，並且包含下列資訊：

- 桌面平台虛擬機器名稱
- 父虛擬機器名稱
- 客體自訂規格
- 複製的桌面平台機器所在的資料存放區
- 管理桌面平台機器的 ESXi 伺服器
- 用於複製的父虛擬機器快照
- 指出在桌面平台虛擬機器存在時是否加以刪除的旗標

下列範例顯示輸入檔可能包含的內容。

```
VMName,Parentvm,CustomSpec,Datastore,Host,FromSnapshot,DeleteIfPresent
linux-001,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-002,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-003,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-004,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-005,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
```

範例指令碼假設此輸入檔的名稱是 CloneVMs.csv，而檔案位在與指令碼相同的資料夾中。

用於複製 Linux 虛擬機器的範例指令碼

您可以自訂和使用下列範例指令碼，以複製任意數量的虛擬機器 (VM)。

若要複製和貼上不含分頁符號的指令碼內容，請使用本主題的 HTML 版本，您可以從 Horizon7 說明文件頁面取得，網址為 <https://docs.vmware.com/tw/VMware-Horizon-7/index.html>。

指令碼輸入

此指令碼會讀取一個輸入檔，描述於用於部署 Linux 桌面平台的範例 PowerCLI 指令碼輸入檔。此指令碼也會互動地要求下列資訊：

- vCenter Server 的 IP 位址
- vCenter Server 的管理員登入名稱
- vCenter Server 的管理員密碼
- 複製類型，必須是「完整」
- 是否停用 vSphere 虛擬機器主控台

指令碼內容

```
<#
Create Clones from a Master VM

The Tool supports creation of Full clone from Master VM.
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
```

```

    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

function IsVMExists ()
{
    Param($VMExists)
    Write-Host "Checking if the VM $VMExists already Exists"
    [bool]$Exists = $false

    #Get all VMS and check if the VMs is already present in VC
    $listvm = Get-vm
    foreach ($lvm in $listvm)
    {
        if($VMExists -eq $lvm.Name )
        {
            $Exists = $true
        }
    }
    return $Exists
}

function Disable_VM_Console()
{
    Param($VMToDisableConsole)
    $vmConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
    $extra = New-Object VMware.Vim.optionvalue
    $extra.Key="RemoteDisplay.maxConnections"
    $extra.Value="0"
    $vmConfigSpec.extraconfig += $extra
    $vm = Get-VM $VMToDisableConsole | Get-View
    $vm.ReconfigVM($vmConfigSpec)
}

function Delete_VM()
{
    Param($VMToDelete)
    Write-Host "Deleting VM $VMToDelete"
    Get-VM $VMToDelete | where { $_.PowerState -eq "PoweredOn" } | Stop-VM -confirm:$false
    Get-VM $VMToDelete | Remove-VM -DeleteFromDisk -confirm:$false
}

#----- Main Script -----

$svcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$svcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$svcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
$cloneType = GetInput -prompt 'Clone Type ("full")' -IsPassword $false
$disableVMConsole = GetInput -prompt 'Disable vSphere VM Console ("yes" or "no", recommend "yes")' -

```

```

IsPassword $false
"-----"
$csvFile = '.\CloneVMs.csv'

# Check that user passed only full clone
if (($CloneType.length > 0) -and ($CloneType -ne "full"))
{
    write-host -ForegroundColor Red "Clone type supports only 'full' (case sensitive)"
    exit
}
if (($disableVMConsole.length > 0) -and ($disableVMConsole -ne "yes" -or $disableVMConsole -ne "no"))
{
    write-host -ForegroundColor Red "Disable vSphere VM Console supports only 'yes' or 'no' (case sensitive)"
    exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File $CSVFile not found"
    exit
}

# Connect to the VC (Parameterize VC)
#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile
#$csvData = Import-CSV $csvFile -
header("VMName","Parentvm","CustomSpec","Datastore","Host","FromSnapshot","DeleteIfPresent")
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $destVMName=$line.VMName
    $srcVM = $line.Parentvm
    $cSpec = $line.CustomSpec
    $targetDSName = $line.Datastore
    $destHost = $line.Host
    $srcSnapshot = $line.FromSnapshot
    $deleteExisting = $line.DeleteIfPresent
    if (IsVMExists ($destVMName))

```

```

{
    Write-Host "VM $destVMName Already Exists in VC $vcAddress"
    if($deleteExisting -eq "TRUE")
    {
        Delete_VM ($destVMName)
    }
    else
    {
        Write-Host "Skip clone for $destVMName"
        continue
    }
}
$vm = get-vm $srcvm -ErrorAction Stop | get-view -ErrorAction Stop
$cloneSpec = new-object VMware.VIM.VirtualMachineCloneSpec
$cloneSpec.Location = new-object VMware.VIM.VirtualMachineRelocateSpec
Write-Host "Using Datastore $targetDSName"
$newDS = Get-Datastore $targetDSName | Get-View
$cloneSpec.Location.Datastore = $newDS.summary.Datastore
Set-VM -vm $srcVM -snapshot (Get-Snapshot -vm $srcVM -Name $srcSnapshot) -confirm:$false
$cloneSpec.Snapshot = $vm.Snapshot.CurrentSnapshot
$cloneSpec.Location.Host = (get-vmhost -Name $destHost).Extensiondata.MoRef
$cloneSpec.Location.Pool = (Get-ResourcePool -Name Resources -Location (Get-VMHost -Name
$destHost)).Extensiondata.MoRef
# Start the Clone task using the above parameters
$task = $vm.CloneVM_Task($vm.parent, $destVMName, $cloneSpec)
# Get the task object
$task = Get-Task | where { $_.id -eq $task }
#Wait for the taks to Complete
Wait-Task -Task $task

$newvm = Get-vm $destVMName
$customSpec = Get-OSCustomizationSpec $cSpec
Set-vm -OSCustomizationSpec $cSpec -vm $newvm -confirm:$false
if ($disableVMConsole -eq "yes")
{
    Disable_VM_Console($destVMName)
}
# Start the VM
Start-VM $newvm
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

指令碼執行

下列訊息是來自指令碼的執行：

```

PowerCLI C:\scripts> .\CloneVMs.ps1
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
Clone Type<"Full"> : Full
Disable vSphere VM Console ("yes" or "no", recommend "yes") : yes

```

複製程序耗費的時間視桌面平台機器的數量而定，範圍從數分鐘到數小時不等。若要確認程序已完成，請從 vSphere Client，確定已將最新的桌面平台虛擬機器開機、具有自己的唯一主機名稱，而且 VMware Tools 正在執行。

將複製的虛擬機器加入 AD 網域的範例指令碼

您可以自訂和使用下列範例指令碼，以將複製的虛擬機器 (VM) 加入 Active Directory (AD) 網域。

如果您對 AD 整合使用 Winbind 解決方案，則必須執行此指令碼，因為加入網域的步驟對複製的虛擬機器將會失敗。此指令碼會在每個虛擬機器上執行命令來加入網域。如果您使用 OpenLDAP 解決方案，則不需要執行此指令碼。

若要複製和貼上不含分頁符號的指令碼內容，請使用本主題的 HTML 版本，您可以從 Horizon7 文件頁面取得，網址是：https://www.vmware.com/support/pubs/view_pubs.html。

指令碼輸入

此指令碼會讀取一個輸入檔，在用於部署 Linux 桌面平台的範例 PowerCLI 指令碼輸入檔中有加以描述。此指令碼也會互動地要求下列資訊：

- vCenter Server 的 IP 位址
- vCenter Server 的管理員登入名稱
- vCenter Server 的管理員密碼
- ESXi 主機的管理員登入名稱
- ESXi 主機的管理員密碼
- Linux 虛擬機器的使用者登入名稱
- Linux 虛擬機器的使用者密碼
- 獲得授權可將機器加入網域的 AD 使用者的登入名稱
- 獲得授權之 AD 使用者的密碼

指令碼內容

```
<#
.SYNOPSIS
run command "sudo /usr/bin/net ads join"

.DESRIPTION
The tool is to run the command "sudo /usr/bin/net ads join" to join Linux to AD

.NOTES
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
```

```

Write-Host $prompt -NoNewLine
[Console]::ForegroundColor = "Blue"
if ($IsPassword)
{
    $input = Read-Host -AsSecureString
    $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
}
else
{
    $input = Read-Host
}

[Console]::ResetColor()
return $input
}
#----- Handle input -----
"-----"
SvcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
SvcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
SvcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$adUser = GetInput -prompt 'Type the AD user name to join the AD' -IsPassword $false
""
"Please type the AD user password."
"Please note that special character in password may not work with the script"
$adUserPassword = GetInput -prompt 'Your AD user password' -IsPassword $true
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#----- Main Script -----

#Connect to vCenter
#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file

```

```

$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "sudo /usr/bin/net ads join -U $adUser%$adUserPassword"
    Write-Host "Run cmd 'sudo /usr/bin/net ads join' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

指令碼執行

下列訊息是來自指令碼的執行：

```

PowerCLI C:\scripts> .\ClonedVMs_JoinDomain.ps1
-----
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****
-----
Type the AD user name to join the AD: viewadmin
Please type the AD user password.
Please note that special character in password may not work with the script.
Your AD user password: *****

```

使用 SSH 將複製的虛擬機器加入 AD 網域的範例指令碼

您可以自訂和使用下列範例指令碼，以將複製的虛擬機器 (VM) 加入 Active Directory (AD) 網域。此指令碼使用 SSH 在 Linux 虛擬機器上執行命令。

如果您對 AD 整合使用 Winbind 解決方案，則必須執行此指令碼，因為加入網域的步驟對複製的虛擬機器將會失敗。此指令碼會在每個虛擬機器上執行命令來加入網域。如果您使用 OpenLDAP 解決方案，則不需要執行此指令碼。

若要複製和貼上不含分頁符號的指令碼內容，請使用本主題的 HTML 版本，您可以從 Horizon7 文件頁面取得，網址是：https://www.vmware.com/support/pubs/view_pubs.html。

指令碼輸入

此指令碼會讀取一個輸入檔，在[用於部署 Linux 桌面平台的範例 PowerCLI 指令碼輸入檔](#)中有加以描述。此指令碼也會互動地要求下列資訊：

- vCenter Server 的 IP 位址
- vCenter Server 的管理員登入名稱
- vCenter Server 的管理員密碼
- Linux 虛擬機器的使用者登入名稱
- Linux 虛擬機器的使用者密碼
- 獲得授權可將機器加入網域的 AD 使用者的登入名稱
- 獲得授權之 AD 使用者的密碼

指令碼內容

```
<#
.SYNOPSIS
run command "sudo /usr/bin/net ads join" via SSH

.DESCRIPTION
The tool is to run the command "sudo /usr/bin/net ads join" to join Linux machine to AD via SSH

.NOTES
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
```

```

if ($IsPlink)
{
    if (Test-Path ".\plink.exe")
    {
        write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
    }
    else
    {
        write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
        exit
    }
}
if ($IsPSCP)
{
    if (Test-Path ".\pscp.exe")
    {
        write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
    }
    else
    {
        write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
        exit
    }
}
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + "'" + $cmd + "'"
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        {
            echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
        }
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"

```

```

    write-host "Upload file: $command"
    Invoke-Expression $command
}

#----- Handle input -----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $false
"-----"
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$adUser = GetInput -prompt 'Type the AD user name to join the AD' -IsPassword $false
""
`nPlease type the AD user password."
[Console]::ForegroundColor = "Yellow"
"Plase note that special character should be escaped. For example, $ should be \$\"
[Console]::ResetColor()
$adUserPassword = GetInput -prompt 'Your AD user password' -IsPassword $true
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#----- Main Script -----

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "sudo /usr/bin/net ads join -U $adUser%$adUserPassword"
    Write-Host "Run cmd 'sudo /usr/bin/net ads join' in VM '$VMName' with user '$guestUser'"
}

```

```

    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

指令碼執行

下列訊息是來自指令碼的執行：

```

PowerCLI C:\scripts> .\ClonedVMs_JoinDomain_SSH.ps1
-----
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****
-----
Type the AD user name to join the AD: viewadmin
Please type the AD user password.
Please note that special character should be escaped. For example, $ should be \$
Your AD user password: *****

```

上傳組態檔至 Linux 虛擬機器的範例指令碼

您可以自訂和使用下列範例指令碼，將組態檔 `config` 和 `viewagent-custom.conf` 上傳到多個 Linux 虛擬機器 (VM)。

若要複製和貼上不含分頁符號的指令碼內容，請使用本主題的 HTML 版本，您可以從 Horizon7 文件頁面取得，網址是：https://www.vmware.com/support/pubs/view_pubs.html。

指令碼輸入

此指令碼會讀取一個輸入檔，在[用於部署 Linux 桌面平台的範例 PowerCLI 指令碼輸入檔](#)中有加以描述。此指令碼也會互動地要求下列資訊：

- vCenter Server 的 IP 位址
- vCenter Server 的管理員登入名稱
- vCenter Server 的管理員密碼
- ESXi 主機的管理員登入名稱
- ESXi 主機的管理員密碼
- Linux 虛擬機器的使用者登入名稱
- Linux 虛擬機器的使用者密碼

指令碼內容

```
<#
Upload the configuration files config and viewagent-custom.conf to Linux VMs
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

#----- Handle Input -----
"-----"
write-host -ForegroundColor Blue 'Please ensure your config file and viewagent-custom.conf file are
in current working directory'
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"

$csvFile = '.\CloneVMs.csv'
$setConfig = $false
$setCustomConf = $false
$config_File = "config"
$customConf_File = "viewagent-custom.conf"

#check if config file exists
if(Test-Path $config_File)
{
    $setConfig = $true
    write-host -ForegroundColor Yellow '"config" file found'
```

```

}
else
{
    write-host -ForegroundColor Yellow '"config" file not found, skip it'
}

if(Test-Path $customConf_File)
{
    $setCustomConf = $true
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file found'
}
else
{
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file not found, skip it'
}

if (($setConfig -eq $false)-AND ($setCustomConf -eq $false))
{
    write-host -ForegroundColor Red 'Both file not found, exit'
    exit
}

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    #Try to delete the configuration file from home folder on destination VM
    $cmd = "rm -rf config viewagent-custom.conf"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
    $guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    if ($setConfig)
    {

```

```

Write-Host "Upload File '$config_File' to '$destFolder' of VM '$VMName' with user '$guestUser'"
Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $config_File

$cmd = "sudo mv ./ $config_File /etc/vmware/";
Write-Host "Move configuraton file: $cmd"
Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
}

if ($setCustomConf)
{
Write-Host "Upload File '$customConf_File' to '$destFolder' of VM '$VMName' with user
'$guestUser'"
Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $customConf_File

$cmd = "sudo mv ./ $customConf_File /etc/vmware/";
Write-Host "Move configuraton file: $cmd"
Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
}
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

指令碼執行

下列訊息是來自指令碼的執行：

```

PowerCLI C:\scripts> .\UpdateOptionFile.ps1
-----
Please ensure your config file and view-agent.conf file are in current working directory.
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

```

使用 SSH 上傳組態檔至 Linux 虛擬機器的範例指令碼

您可以自訂和使用下列範例指令碼，將組態檔 `config` 和 `viewagent-custom.conf` 上傳到多個 Linux 虛擬機器 (VM)。此指令碼使用 SSH 在 Linux 虛擬機器上執行命令。

若要複製和貼上不含分頁符號的指令碼內容，請使用本主題的 HTML 版本，您可以從 Horizon7 文件頁面取得，網址是：https://www.vmware.com/support/pubs/view_pubs.html。

指令碼輸入

此指令碼會讀取一個輸入檔，在[用於部署 Linux 桌面平台的範例 PowerCLI 指令碼輸入檔](#)中有加以描述。此指令碼也會互動地要求下列資訊：

- vCenter Server 的 IP 位址
- vCenter Server 的管理員登入名稱
- vCenter Server 的管理員密碼
- Linux 虛擬機器的使用者登入名稱
- Linux 虛擬機器的使用者密碼

指令碼內容

```
<#
Upload the configuration files config and viewagent-custom.conf to Linux VMs using SSH
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
```



```

        exit
    }
}
if ($IsPSCP)
{
    if (Test-Path ".\pscp.exe")
    {
        write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
    }
    else
    {
        write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
        exit
    }
}
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + "'" + $cmd + "'"
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file: $command"
    Invoke-Expression $command
}

#----- Handle Input -----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $true
"-----"
write-host -ForegroundColor Blue 'Please ensure your config file and viewagent-custom.conf file are
in current working directory'

```

```

$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"

$csvFile = '.\CloneVMs.csv'
$setConfig = $false
$setCustomConf = $false
$config_File = "config"
$customConf_File = "viewagent-custom.conf"

#check if config file exists
if(Test-Path $config_File)
{
    $setConfig = $true
    write-host -ForegroundColor Yellow '"config" file found'
}
else
{
    write-host -ForegroundColor Yellow '"config" file not found, skip it'
}

if(Test-Path $customConf_File)
{
    $setCustomConf = $true
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file found'
}
else
{
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file not found, skip it'
}

if (($setConfig -eq $false)-AND ($setCustomConf -eq $false))
{
    write-host -ForegroundColor Red 'Both file not found, exit'
    exit
}

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

```

```

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    #Try to delete the configuration file from home folder on destination VM
    $cmd = "rm -rf config viewagent-custom.conf"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

    if ($setConfig)
    {
        Write-Host "Upload File '$config_File' to '$destFolder' of VM '$VMName' with user '$guestUser'"
        UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
        $config_File -DestPath $destFolder

        $cmd = "sudo mv ./ $config_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
        RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
    }

    if ($setCustomConf)
    {
        Write-Host "Upload File '$customConf_File' to '$destFolder' of VM '$VMName' with user
        '$guestUser'"
        UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
        $customConf_File -DestPath $destFolder

        $cmd = "sudo mv ./ $customConf_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
        RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
    }
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

指令碼執行

下列訊息是來自指令碼的執行：

```

PowerCLI C:\scripts> .\UpdateOptionFile.ps1
-----
Please ensure your config file and view-agent.conf file are in current working directory.
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

```

在 Horizon Agent 上升級 Linux 桌面平台機器的範例 PowerCLI 指令碼

您可以自訂和使用下列範例指令碼，在多個 Linux 虛擬機器 (VM) 上升級 Horizon Agent。

此指令碼會在安裝 Horizon Agent 之前上傳安裝程式 tar ball 到每個虛擬機器。上傳工作可能很費時，特別是牽涉到大量虛擬機器且網路速度緩慢時。為了節省時間，您可以執行使用 SSH 的指令碼，或將安裝程式 tar ball 放置在每個虛擬機器可使用的共用位置上，以便不需要上傳檔案。

若要複製和貼上不含分頁符號的指令碼內容，請使用本主題的 HTML 版本，您可以從 Horizon7 文件頁面取得，網址是：<https://docs.vmware.com/tw/VMware-Horizon-7/index.html>。

指令碼輸入

此指令碼會讀取一個輸入檔，在[用於部署 Linux 桌面平台的範例 PowerCLI 指令碼輸入檔](#)中有加以描述。此指令碼也會互動地要求下列資訊：

- 接受 Horizon Agent EULA (使用者授權合約)
- vCenter Server 的 IP 位址
- vCenter Server 的管理員登入名稱
- vCenter Server 的管理員密碼
- ESXi 主機的管理員登入名稱
- ESXi 主機的管理員密碼
- Linux 客體作業系統的使用者登入名稱
- Linux 客體作業系統的使用者密碼
- Horizon Agent tar ball 路徑
- 升級為受管理的虛擬機器
- 安裝智慧卡重新導向功能

指令碼內容

```
<#
Upload the Linux Agent installer tar ball and re-install
#>

#-----
Functions-----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
```

```

    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
#-----Handle
input-----
"-----"
$acceptEULA = GetInput -prompt 'Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no")' -
IsPassword $false
if ($acceptEULA -ne "yes")
{
    write-host -ForegroundColor Red "You need accept the EULA with 'yes'(case sensitive)"
    exit
}
$svcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$svcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$svcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$agentInstaller = GetInput -prompt 'Type the Horizon Agent tar ball path' -IsPassword $false
"-----"
$UpgradeToManagedVM = GetInput -prompt 'Upgrade to managed VM ("yes" or "no")' -IsPassword $false
if (($UpgradeToManagedVM -ne "yes") -AND $UpgradeToManagedVM -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
$installSmartcard = GetInput -prompt 'Install the Smartcard redirection feature ("yes" or "no")' -
IsPassword $false
if (($installSmartcard -ne "yes") -AND $installSmartcard -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
"-----"

#csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#check if file exists

```

```

if (!(Test-Path $agentInstaller))
{
write-host -ForegroundColor Red "installer File not found"
exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
write-host -ForegroundColor Red "CSV File not found"
exit
}
#-----
Functions-----
function GetSourceInstallerMD5()
{
    $agentInstallerPath = Convert-Path $agentInstaller;
    $md5 = New-Object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider;
    $md5HashWithFormat =
[System.BitConverter]::ToString($md5.ComputeHash([System.IO.File]::ReadAllBytes($agentInstallerPath)))
;
    $md5Hash = ($md5HashWithFormat.replace("-", "")).ToLower();
    return $md5Hash;
}

#-----
Main-----
#Get installer MD5Sum
$installerMD5Hash = GetSourceInstallerMD5;

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "rm -rf VMware-*linux-*"

```

```

Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

#Upload installer tar ball to Linux VM
Write-Host "Upload File '$agentInstaller' to '$destFolder' of VM '$VMName' with user '$guestUser'"
Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $agentInstaller

#Check the uploaded installer md5sum
$cmd = "md5sum VMware-*linux-*"
Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
$output = Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -
GuestUser $guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

if($output.Contains($installerMD5Hash))
{
    Write-Host $VMName": Uploaded installer's MD5Sum matches the local installer's MD5Sum";
    Write-Host $VMName": Extract the installer and do installation";
    $cmd = "tar -xzf VMware-*linux-*.tar.gz"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    $cmd = "sudo setenforce 0";
    Write-Host "Set the selinux to permissive mode: $cmd"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    $cmd = "sudo killall /usr/lib/vmware/viewagent/VMwareBlastServer/VMwareBlastServer"
    Write-Host "Stop VMwareBlastServer before upgrading: $cmd"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    #Run the upgrade command.
    $cmd = "cd VMware-*linux-* && sudo ./install_viewagent.sh -A yes -m $installSmartcard -M
$UpgradeToManagedVM"
    Write-Host "Run upgrade cmd in VM '$VMName' with user '$guestUser': $cmd"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    $cmd = "sudo shutdown -r +1&"
    Write-Host "Reboot to apply the Horizon Agent installation"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
}
else
{
    Write-Host $VMName": Uploaded installer's MD5Sum does NOT match the local installer's MD5Sum";
    Write-Host $VMName": Skip the installation. Please check your network and VMware Tools
status";
    exit;
}

```

```

    }
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

指令碼執行

下列訊息是來自指令碼的執行：

```

PowerCLI C:\scripts> .\InstallAgent.ps1
-----
Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no"): yes
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: HorizonUser
Your VM guest OS user password: *****
-----
Type the Horizon Agent tar ball path. Please take care of the installer arch: .\VMware-viewagent-
linux-x86_64-x.y.z-1234567.tar.gz
-----
Upgrade to managed VM ("yes" or "no"): yes
Install the Smartcard redirection feature ("yes" or "no"): no

```

使用 SSH 在 Linux 虛擬機器上升級 Horizon Agent 的範例指令碼

您可以自訂和使用下列範例指令碼，在多個 Linux 虛擬機器 (VM) 上升級 Horizon Agent。此指令碼使用 SSH 在 Linux 虛擬機器上執行命令。

若要複製和貼上不含分頁符號的指令碼內容，請使用本主題的 HTML 版本，您可以從 Horizon7 文件頁面取得，網址是：https://www.vmware.com/support/pubs/view_pubs.html。

指令碼輸入

此指令碼會讀取一個輸入檔，在用於部署 Linux 桌面平台的範例 PowerCLI 指令碼輸入檔中有加以描述。此指令碼也會互動地要求下列資訊：

- 接受 Horizon Agent EULA (使用者授權合約)
- vCenter Server 的 IP 位址
- vCenter Server 的管理員登入名稱
- vCenter Server 的管理員密碼
- ESXi 主機的管理員登入名稱
- ESXi 主機的管理員密碼

- Linux 客體作業系統的使用者登入名稱
- Linux 客體作業系統的使用者密碼
- Horizon Agent tar ball 路徑
- 升級為受管理的虛擬機器
- 安裝智慧卡重新導向功能

指令碼內容

```
<#
Upload the Linux Agent installer tar ball and re-install
#>

#-----
Functions-----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
}
```

```

}
if ($IsPSCP)
{
    if (Test-Path ".\pscp.exe")
    {
        write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
    }
    else
    {
        write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
        exit
    }
}
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + "'" + $cmd + "'"
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file $LocalPath to VM $VM_Name with user $User"
    Invoke-Expression $command
}

#-----Handle
input-----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $true
"-----"
$acceptEULA = GetInput -prompt 'Accept Linux View Agent EULA in tar bundle ("yes" or "no")' -
IsPassword $false
if ($acceptEULA -ne "yes")

```

```

{
    write-host -ForegroundColor Red "You need accept the EULA with 'yes'(case sensitive)"
    exit
}
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$agentInstaller = GetInput -prompt 'Type the View Agent tar ball path' -IsPassword $false
"-----"
$UpgradeToManagedVM = GetInput -prompt 'Upgrade to managed VM ("yes" or "no")' -IsPassword $false
if (($UpgradeToManagedVM -ne "yes") -AND $UpgradeToManagedVM -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
$installSmartcard = GetInput -prompt 'Install the Smartcard redirection feature ("yes" or "no")' -
IsPassword $false
if (($installSmartcard -ne "yes") -AND $installSmartcard -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#check if file exists
if (!(Test-Path $agentInstaller))
{
    write-host -ForegroundColor Red "installer File not found"
    exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File not found"
    exit
}
#-----
Functions-----
function GetSourceInstallerMD5()
{
    $agentInstallerPath = Convert-Path $agentInstaller;
    $md5 = New-Object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider;
    $md5HashWithFormat =
[System.BitConverter]::ToString($md5.ComputeHash([System.IO.File]::ReadAllBytes($agentInstallerPath)))
;
    $md5Hash = ($md5HashWithFormat.replace("-", "")).ToLower();
    return $md5Hash;
}

```

```

}

#-----
Main-----
#Get installer MD5Sum
$installerMD5Hash = GetSourceInstallerMD5;

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "rm -rf VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

    #Upload installer tar ball to Linux VM
    Write-Host "Upload File '$agentInstaller' to '$destFolder' of VM '$VMName' with user '$guestUser'"
    UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
$agentInstaller -DestPath $destFolder

    #Check the uploaded installer md5sum
    $cmd = "md5sum VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    $output = RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd -
$returnOutput $true

    if($output.Contains($installerMD5Hash))
    {
        Write-Host $VMName": Uploaded installer's MD5Sum matches the local installer's MD5Sum";
        Write-Host $VMName": Extract the installer and do installation";

        $cmd = "tar -xzf VMware-*linux-*.tar.gz"
        Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
        RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
    }
}

```

```

    $cmd = "sudo setenforce 0";
    Write-Host "Set the selinux to permissive mode: $cmd"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

    $cmd = "sudo killall /usr/lib/vmware/viewagent/VMwareBlastServer/VMwareBlastServer"
    Write-Host "Stop VMwareBlastServer before upgrading: $cmd"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

    #Run the upgrade command.
    $cmd = "cd VMware-*--linux-* && sudo ./install_viewagent.sh -r yes -A yes -m $installSmartcard
-M $UpgradeToManagedVM"
    Write-Host "Run upgrade cmd in VM '$VMName' with user '$guestUser': $cmd"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
    Write-Host -ForegroundColor Yellow "Linux Agent installer will reboot the Linux VM after
upgrade, and you may hit the ssh connection closed error message, which is expectation"
    }
    else
    {
        Write-Host $VMName": Uploaded installer's MD5Sum does NOT match the local installer's MD5Sum";
        Write-Host $VMName": Skip the installation. Please check your network and VMware Tools
status";
        exit;
    }
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

指令碼執行

下列訊息是來自指令碼的執行：

```

PowerCLI C:\scripts> .\InstallAgent.ps1
-----
Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no"): yes
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****
-----
Type the Horizon Agent tar ball path. Please take care of the installer arch: .\VMware-viewagent-
linux-x86_64-x.y.z-1234567.tar.gz
-----
-----
Upgrade to managed VM ("yes" or "no"): yes
Install the Smartcard redirection feature ("yes" or "no"): no

```

在 Linux 虛擬機器上執行作業的範例指令碼

您可以自訂和使用下列範例指令碼，在多個 Linux 虛擬機器 (VM) 上執行作業。該作業包含開啟電源、關閉電源、關機、重新啟動和刪除虛擬機器。

此指令碼可從 vCenter Server 刪除虛擬機器，但無法從 View 刪除。

若要複製和貼上不含分頁符號的指令碼內容，請使用本主題的 HTML 版本，您可以從 Horizon7 文件頁面取得，網址是：https://www.vmware.com/support/pubs/view_pubs.html。

指令碼輸入

此指令碼會讀取一個輸入檔，在用於部署 Linux 桌面平台的範例 PowerCLI 指令碼輸入檔中有加以描述。此指令碼也會互動地要求下列資訊：

- vCenter Server 的 IP 位址
- vCenter Server 的管理員登入名稱
- vCenter Server 的管理員密碼
- 要執行的動作，可以是開機、關機、關閉客體、重新啟動虛擬機器、重新啟動虛擬機器客體或刪除虛擬機器。
- 虛擬機器上各作業的等候間隔時間 (以秒為單位)。

指令碼內容

```
<#
.DESCRIPTION
The Tool supports:
1. Power off VMs
2. Power on VMs
3. Shutdown VMs
4. Restart VMs
5. Restart VM guest
6. Delete VMs from Disk
.NOTES
#>

#----- Functions -----

function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
}
```

```

    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

function IsVMExists ($VMExists)
{
    Write-Host "Checking if the VM $VMExists Exists"
    [bool]$Exists = $false

    #Get all VMS and check if the VMs is already present in VC
    $listvm = Get-vm
    foreach ($lvm in $listvm)
    {
        if($VMExists -eq $lvm.Name )
        {
            $Exists = $true
            Write-Host "$VMExists is Exist"
        }
    }
    return $Exists
}

function Delete_VM($VMToDelete)
{
    Write-Host "Deleting VM $VMToDelete"
    Get-VM $VMToDelete | where { $_.PowerState -eq "PoweredOn" } | Stop-VM -confirm:$false
    Get-VM $VMToDelete | Remove-VM -DeleteFromDisk -confirm:$false
}

#----- Handle input -----
"-----"
$svcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$svcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$svcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"

$action = GetInput -prompt 'Select action: 1). Power On 2). Power Off 3) Shutdown VM Guest 4).
Restart VM 5). Restart VM Guest 6). Delete VM' -IsPassword $false
$sleepTime = GetInput -prompt 'Wait time (seconds) between each VM' -IsPassword $false
"-----"

[Console]::ForegroundColor = "Yellow"
switch ($action)
{
    1
    {
        "Your selection is 1). Power On"
    }
    2
    {
        "Your selection is 2). Power Off"
    }
}

```

```

}
3
{
    "Your selection is 3) Shutdown"
}
4
{
    "Your selection is 4). Restart VM"
}
5
{
    "Your selection is 5). Restart VM Guest"
}
6
{
    "Your selection is 6). Delete VM"
}
default
{
    "Invalid selection for action: $action"
    exit
}
}
[Console]::ResetColor()
$csvFile = '.\CloneVMs.csv'

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File not found"
    exit
}
"-----"

#----- Main -----
#Read input CSV file
Disconnect-VIServer $vcAddress -Confirm:$false
#Connect-VIServer $vcAddress -ErrorAction Stop -user $vcAdmin -password $vcPassword
Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
$csvData = Import-CSV $csvFile

foreach ($line in $csvData)
{
    $VMName = $line.VMName
    switch ($action)
    {
        1
        {
            Get-VM $VMName | Start-VM -Confirm:$false
        }
        2
        {
            Get-VM $VMName | Stop-VM -Confirm:$false
        }
        3
    }
}

```



```

    {
        Get-VM $VMName | Shutdown-VMGuest -Confirm:$false
    }
    4
    {
        Get-VM $VMName | Restart-VM -Confirm:$false
    }
    5
    {
        Get-VM $VMName | Restart-VMGuest -Confirm:$false
    }
    6
    {
        if (IsVMExists ($VMName))
        {
            Delete_VM ($VMName)
        }
    }
    default{}
}
Start-Sleep -s $sleepTime
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

指令碼執行

下列訊息是來自指令碼的執行：

```

PowerCLI C:\scripts> .\VMOperations.ps1
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****

-----
Select action: 1). Power On 2). Power Off 3) Shutdown VM Guest 4). Restart VM 5). Restart VM Guest
6). Delete VM: 1
Wait time (seconds) between each VM: 20
-----

Your selection is 6). Delete VM

```

針對開機、重新啟動虛擬機器和重新啟動虛擬機器客體作業，請指定虛擬機器之間的等候時間，至少 20 秒來避免開機風暴情況，該情況可能造成某些作業失敗。

疑難排解 Linux 桌面平台

9

當您管理 Linux 桌面平台時可能會發生某些問題。您可以遵循各種程序來診斷和修正問題。

本章節討論下列主題：

- 在 [Horizon Console](#) 中使用 [Horizon Help Desk Tool](#)
- 收集 [Horizon 7 for Linux](#) 機器的診斷資訊
- [Horizon Agent](#) 無法在 [iPad Pro Horizon Client](#) 上中斷連線
- [SLES 12 SP1](#) 桌面平台不會自動重新整理
- [SSO](#) 無法連線到關閉電源代理程式
- 在建立 [Linux](#) 的手動桌面平台集區後無法連線虛擬機器

在 Horizon Console 中使用 Horizon Help Desk Tool

Horizon Help Desk Tool 是一個可用來取得 Horizon 7 使用者工作階段狀態及執行疑難排解和維護作業的 Web 應用程式。

在 Horizon Help Desk Tool 中，您可以查閱使用者工作階段，以排解問題及執行桌面平台維護作業，例如重新啟動或重設桌面平台。

若要設定 Horizon Help Desk Tool，您必須符合下列需求：

- Horizon 7 的 Horizon Enterprise 版授權或 Horizon Apps Advanced 版授權。若要確認您擁有正確的授權，請參閱《Horizon 7 管理》文件。
- 用來儲存 Horizon 7 元件相關資訊的事件資料庫。如需關於設定事件資料庫的詳細資訊，請參閱《Horizon 7 管理》文件。
- 用來登入 Horizon Help Desk Tool 的服務台管理員角色或服務台管理員 (唯讀) 角色。如需這些角色的詳細資訊，請參閱《Horizon 7 管理》文件。
- 在每個連線伺服器執行個體上啟用計時分析工具以檢視登入區段。

請使用下列 `vdmadmin` 命令，在每個連線伺服器執行個體上啟用計時分析工具：

```
vdmadmin -I -timingProfiler -enable
```

請使用下列 `vdmadmin` 命令，在使用管理連接埠的連線伺服器執行個體上啟用計時分析工具：

```
vdmadmin -I -timingProfiler -enable -server {ip/server}
```

- 在 `/etc/vmware/viewagent-custom.conf` 組態檔案中啟用 `HelpDeskEnable` 選項。

在 Horizon Console 中 啟動 Horizon Help Desk Tool

Horizon Help Desk Tool 已整合至 Horizon Console。您可以搜尋要在 Horizon Help Desk Tool 中疑難排解問題的使用者。

程序

- 1 您可以在 [使用者搜尋] 文字方塊中搜尋使用者名稱，或直接導覽至 Horizon Help Desk Tool 工具。

- 在 Horizon Console 中，於 [使用者搜尋] 文字方塊中輸入使用者名稱。
- 選取**監視器 > 服務台**，然後在 [使用者搜尋] 文字方塊中輸入使用者名稱。

Horizon Console 會在搜尋結果中顯示使用者的清單。搜尋可以傳回最多 100 個相符的結果。

- 2 選取使用者名稱。

使用者資訊會顯示在使用者卡片中。

後續步驟

若要針對問題進行疑難排解，請在使用者卡片中按一下相關索引標籤。

在 Horizon Help Desk Tool 中對使用者進行疑難排解

在 Horizon Help Desk Tool 中，您可以檢視使用者卡片中的基本使用者資訊。您可以按一下使用者卡片中的索引標籤，以取得關於特定元件的詳細資料。

使用者詳細資料有時會顯示在資料表中。您可以依資料表資料行排序這些使用者詳細資料。

- 若要依遞增順序排序資料行，請按一下資料行。
- 若要依遞減順序排序資料行，請按兩下資料行。
- 若不要排序資料行，請按三下資料行。

基本使用者資訊

顯示基本使用者資訊，例如使用者的使用者名稱、電話號碼和電子郵件地址，以及使用者的連線或中斷連線狀態。如果使用者具有桌面平台工作階段，則使用者會處於連線狀態。如果使用者沒有桌面平台工作階段，則使用者會處於中斷連線狀態。

您也可以按一下電子郵件位址，以傳送訊息給使用者。

工作階段

工作階段索引標籤會顯示使用者連線的桌面平台工作階段的相關資訊。

您可以使用**篩選器**文字方塊篩選桌面平台工作階段。

備註 工作階段索引標籤不會顯示從 vSphere Client 或 ESXi 存取虛擬機器之工作階段的工作階段資訊。

工作階段索引標籤會包含下列資訊：

表 9-1. 工作階段索引標籤

選項	說明
狀態	顯示桌面平台工作階段之狀態的相關資訊。 <ul style="list-style-type: none"> 如果工作階段已連線，則呈現為綠色。 如果工作階段是本機工作階段，或工作階段執行於本機網繭中，則顯示 L。
電腦名稱	桌面平台工作階段的名稱。按一下名稱可開啟卡片中的工作階段資訊。 您可以按一下工作階段卡片中的索引標籤來檢視其他資訊： <ul style="list-style-type: none"> 詳細資料索引標籤會顯示使用者資訊，例如虛擬機器資訊、CPU 或記憶體使用量。 處理程序索引標籤會顯示關於 CPU 和記憶體相關處理程序的資訊。
通訊協定	適用於桌面平台工作階段的顯示通訊協定。
類型	顯示桌面平台是已發佈桌面平台還是虛擬機器桌面平台。
連線時間	工作階段與連線伺服器連線的時間。
工作階段持續時間	工作階段持續與連線伺服器連線的時間長度。

桌面平台

桌面平台索引標籤會顯示使用者有權使用的已發佈桌面平台或虛擬桌面平台的相關資訊。

表 9-2. 桌面平台

選項	說明
狀態	顯示桌面平台工作階段之狀態的相關資訊。 <ul style="list-style-type: none"> 如果工作階段已連線，則呈現為綠色。
桌面平台集區名稱	工作階段的桌面平台集區名稱。
桌面平台類型	顯示桌面平台是已發佈的桌面平台還是虛擬機器桌面平台。 備註 如果工作階段執行於網繭聯盟中的不同網繭，則不會顯示任何資訊。
類型	顯示桌面平台權利類型的相關資訊。 <ul style="list-style-type: none"> 若為本機權利，則顯示「本機」。
vCenter	顯示 vCenter Server 中的虛擬機器名稱。 備註 如果工作階段執行於網繭聯盟中的不同網繭，則不會顯示任何資訊。
預設通訊協定	桌面平台工作階段的預設顯示通訊協定。

活動

活動索引標籤會顯示關於使用者活動的事件記錄資訊。您可以根據時間範圍篩選活動，例如過去 12 個小時或過去 30 天，或是依管理員名稱來篩選。按一下**僅限服務台事件**，即可僅根據 Horizon Help Desk Tool 活動進行篩選。按一下重新整理圖示以重新整理事件記錄。按一下匯出圖示以將事件記錄匯出為檔案。

備註 對於 Cloud Pod 架構環境中的使用者並不會顯示事件記錄資訊。

表 9-3. 活動

選項	說明
時間	選取時間範圍。預設值為過去 12 個小時。 <ul style="list-style-type: none"> ■ 過去 12 個小時 ■ 過去 24 個小時 ■ 過去 7 天 ■ 過去 30 天 ■ 全部
管理員	管理員使用者的名稱。
訊息	針對使用者或管理員顯示其所執行活動的專屬訊息。
資源名稱	顯示活動執行所在桌面平台集區或虛擬機器名稱的相關資訊。

Horizon Help Desk Tool 的工作階段詳細資料

當您在工作階段索引標籤上的**電腦名稱**選項中按一下使用者名稱時，**詳細資料**索引標籤上會出現工作階段詳細資料。您可以檢視 Horizon Client、虛擬或已發佈桌面平台，以及 CPU 和記憶體의詳細資料。

用戶端

根據 Horizon Client 的類型顯示資訊，並且包含諸如使用者名稱、Horizon Client 的版本、用戶端機器的 IP 位址，以及用戶端機器的作業系統等詳細資料。

備註 如果您已升級 Horizon Agent，則必須也將 Horizon Client 升級至最新版本。否則將不會顯示 Horizon Client 的版本。如需關於升級 Horizon Client 的詳細資訊，請參閱《Horizon 7 升級》文件。

虛擬機器

顯示虛擬桌面平台或已發佈桌面平台的相關資訊。

表 9-4. 虛擬機器詳細資料

選項	說明
電腦名稱	桌面平台工作階段的名稱。
代理程式版本	Horizon Agent 版本。
作業系統版本	作業系統版本。
連線伺服器	工作階段連線的連線伺服器。
集區	桌面平台集區的名稱。
vCenter	vCenter Server 的 IP 位址。

表 9-4. 虛擬機器詳細資料 (續)

選項	說明
工作階段狀態	桌面平台工作階段的狀態。工作階段狀態可以是已連線或已中斷連線。
工作階段持續時間	工作階段持續與連線伺服器連線的時間。
狀態持續時間	工作階段保持於相同狀態的時間。
登入時間	登入工作階段之使用者的登入時間。
登入持續時間	使用者持續登入 Linux 桌面平台的時間長度。

使用者經驗度量

顯示使用 VMware Blast 顯示通訊協定之虛擬或已發佈桌面平台工作階段的效能詳細資料。若要檢視這些效能詳細資料，請按一下[更多](#)。若要重新整理這些詳細資料，請按一下重新整理圖示。

表 9-5. Blast 顯示通訊協定詳細資料

選項	說明
畫面播放速率	Blast 工作階段中的畫面播放速率 (每秒畫面數)。
Skype 狀態	針對 Linux 桌面平台工作階段，此選項會顯示為不適用。
Blast 工作階段計數器	<ul style="list-style-type: none"> ■ 預估頻寬 (上行)。上行訊號的預估頻寬。 ■ 封包遺失 (上行)。上行訊號的封包遺失百分比。
Blast 影像處理計數器	<ul style="list-style-type: none"> ■ 已傳輸的位元組。已為 Blast 工作階段傳輸之影像處理資料的位元組總數。 ■ 已接收的位元組。已為 Blast 工作階段接收之影像處理資料的位元組總數。
Blast 音訊計數器	<ul style="list-style-type: none"> ■ 已傳輸的位元組。已為 Blast 工作階段傳輸之音訊資料的位元組總數。 ■ 已接收的位元組。已為 Blast 工作階段接收之音訊資料的位元組總數。
Blast CDR 計數器	<ul style="list-style-type: none"> ■ 已傳輸的位元組。已為 Blast 工作階段傳輸之用戶端磁碟機重新導向資料的位元組總數。 ■ 已接收的位元組。已為 Blast 工作階段接收之用戶端磁碟機重新導向資料的位元組總數。

CPU 和記憶體使用量以及網路和磁碟效能

顯示虛擬或已發佈桌面平台的 CPU 和記憶體使用量圖，以及 Blast 顯示通訊協定的網路或磁碟效能。

備註 在桌面平台上 Horizon Agent 啟動或重新啟動之後，效能圖可能不會立即顯示時間表。時間表會在幾分鐘後顯示。

表 9-6. CPU 使用率

選項	說明
工作階段 CPU	目前工作階段的 CPU 使用率。
主機 CPU	指派工作階段之虛擬機器的 CPU 使用率。

表 9-7. 記憶體使用量

選項	說明
工作階段記憶體	目前工作階段的記憶體使用量。
主機記憶體	指派工作階段之虛擬機器的記憶體使用量。

表 9-8. 網路效能

選項	說明
延遲	顯示 PCoIP 或 Blast 工作階段的延遲圖。 延遲時間即為來回行程時間 (以毫秒為單位)。追蹤此延遲時間的效能計數器為 VMware Blast 工作階段計數器 > RTT 。

表 9-9. 磁碟效能

選項	說明
讀取	每秒讀取輸入/輸出 (I/O) 作業的數目。
寫入	每秒寫入 I/O 作業的數目。
磁碟延遲	顯示磁碟延遲的圖表。磁碟延遲即為從 Windows 效能計數器所擷取每秒輸入/輸出作業 (IOPS) 資料的時間 (以毫秒為單位)。
平均讀取	每秒隨機讀取 I/O 作業的平均數目。
平均寫入	每秒隨機寫入 I/O 作業的平均數目。
平均延遲	從 Windows 效能計數器擷取之 IOPS 資料的平均延遲時間 (以毫秒為單位)。

工作階段登入區段

顯示登入持續時間以及在登入期間建立的使用量區段。

表 9-10. 工作階段登入區段

選項	說明
登入持續時間	時間長度的計算從使用者按一下桌面平台集區時起算，計算到使用者登入 Linux 桌面平台時為止。
工作階段登入時間	使用者登入工作階段的時間長度。
登入區段	<p>顯示在登入期間建立的區段。</p> <ul style="list-style-type: none"> ■ 代理。連線伺服器處理工作階段連線或重新連線的總時間。此時間從使用者按一下桌面平台集區時起算，計算到通道連線設定完成時為止。其中包括使用者驗證、機器選取，以及為了設定通道連線而執行的機器準備等連線伺服器工作所耗費的時間。 ■ 互動式。Horizon Agent 處理工作階段連線或重新連線作業的總時間。此時間從 Blast Extreme 使用通道連線時起算，計算到使用者登入至 Linux 桌面平台時為止。 ■ 通訊協定連線。PCoIP 或 Blast 通訊協定連線在完成登入程序期間所花費的時間總計。 ■ 登入指令碼。登入指令碼從開始執行到完成所花費的時間總計。 ■ 驗證。連線伺服器驗證工作階段的總時間。 ■ 虛擬機器啟動。啟動虛擬機器所花費的總時間。這段時間包括作業系統開機、繼續執行暫停的機器，以及 Horizon Agent 指出本身已準備好進行連線所花費的時間。

Horizon Help Desk Tool 的工作階段處理程序

當您在工作階段索引標籤上的**電腦名稱**選項中按一下使用者名稱時，**處理程序**索引標籤上會顯示工作階段處理程序。

處理程序

針對每個工作階段，您可以檢視 CPU 和記憶體相關處理程序的其他詳細資料。例如，如果您發現某个工作階段的 CPU 和記憶體使用量異常偏高，則可以在**處理程序**索引標籤上檢視處理程序的詳細資料。

對於 RDS 主機工作階段，**處理程序**索引標籤會顯示目前使用者或目前系統處理程序啟動的目前 RDS 主機工作階段處理程序。

表 9-11. 工作階段處理程序詳細資料

選項	說明
處理程序名稱	工作階段處理程序的名稱。例如 chrome.exe。
CPU	處理程序的 CPU 使用率 (以百分比為單位)。
記憶體	處理程序的記憶體使用量 (以 KB 為單位)。
磁碟	<p>記憶體磁碟 IOPS。系統會使用下列公式進行計算： $(\text{目前時間的 I/O 位元組總數}) - (\text{目前時間前一秒的 I/O 位元組總數})$。</p> <p>如果「工作管理員」顯示正值，則此計算顯示的值可能是每秒 0 KB。</p>
使用者名稱	擁有處理程序之使用者的使用者名稱。

表 9-11. 工作階段處理程序詳細資料 (續)

選項	說明
主機 CPU	指派工作階段之虛擬機器的 CPU 使用率。
主機記憶體	指派工作階段之虛擬機器的記憶體使用量。
處理程序	虛擬機器中的處理程序計數
重新整理	重新整理圖示會重新整理處理程序的清單。
結束處理程序	結束正在執行的處理程序。 備註 您必須具有服務台管理員角色才能結束處理程序。 若要結束處理程序，請選取處理程序，然後按一下 結束處理程序 按鈕。 您無法結束可能會在 處理程序 索引標籤中列出的重要處理程序，例如 Windows 核心處理程序。如果您要結束某個重要處理程序，則 Horizon Help Desk Tool 會顯示一則訊息，表示其無法結束此系統處理程序。

在 Horizon Help Desk Tool 中疑難排解 Linux 桌面平台工作階段

在 Horizon Help Desk Tool 中，您可以根據使用者的連線狀態對 Linux 桌面平台工作階段進行疑難排解。

必要條件

- 啟動 Horizon Help Desk Tool。

程序

- 1 在使用者卡片上，按一下**工作階段**索引標籤。

效能卡隨即出現，顯示 CPU 和記憶體使用量，並且包含 Horizon Client 和虛擬或已發佈桌面平台的相關資訊。

- 2 選擇疑難排解選項。

選項	動作
傳送訊息	將訊息傳送給已發佈的桌面平台或虛擬桌面平台上的使用者。您可以選擇訊息的嚴重性，以包含「警告」、「資訊」或「錯誤」。 按一下 傳送訊息 ，並輸入嚴重性類型和訊息詳細資料，然後按一下 提交 。
重新啟動	在虛擬桌面平台上啟動「重新啟動」程序。此功能不適用於已發佈的桌面平台工作階段。 按一下 重新啟動 VDI 。
中斷連線	中斷桌面平台或應用程式工作階段的連線。 按一下 更多 > 中斷連線 。

選項	動作
登出	起始已發佈的桌面平台或虛擬桌面平台的登出程序。 按一下 更多 > 登出 。
重設	啟動虛擬機器的重設作業。此功能不適用於已發佈的桌面平台。 按一下 更多 > 重設虛擬機器 。
	備註 使用者可能會遺失未儲存的工作。

收集 Horizon 7 for Linux 機器的診斷資訊

您可以收集診斷資訊，協助 VMware 技術支援診斷並解決 Horizon 7 for Linux 機器的問題。您將建立 Data Collection Tool (DCT) 組合，該組合會取得機器的組態資訊並記錄至壓縮的 tarball。

程序

- 1 以具備所需權限的使用者身分登入 Linux 虛擬機器。
- 2 開啟命令提示字元，並執行 `dct-debug.sh` 指令碼。

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

指令碼會產生包含 DCT 組合的 tarball。例如：

```
ubuntu-12-vdm-sdct-20150201-0606-agent.tgz
```

tarball 是在執行指令碼所在的目錄 (目前的工作目錄) 中產生。

Horizon Agent 無法在 iPad Pro Horizon Client 上中斷連線

在 iPad Pro Horizon Client 上重新啟動或關閉後，SUSE Horizon Agent 連線無法中斷。

問題

當您在 iPad Pro Horizon Client 上重新啟動或關閉 SUSE 虛擬機器時，桌面平台沒有回應。Horizon Agent 無法中斷連線。

原因

在重新啟動或關閉作業後，SUSE 機器可能無法正確地將訊息傳送至 Horizon Client。

解決方案

- ◆ 從 iPad Pro Horizon Client 手動中斷桌面平台連線。

SLES 12 SP1 桌面平台不會自動重新整理

在多台監視器模式中，當您拖曳 GNOME 終端機時，SLES 12 SP1 不會自動重新整理。

問題

當您以多台監視器模式啟動 SLES 12 SP1，然後回到視窗模式時，在您拖曳 GNOME 終端機後，桌面平台不會自動重新整理。

原因

GNOME 終端機不會回應拖曳作業。

解決方案

- 1 結束 GNOME Shell 工作階段。

```
kill -9 <process id of gnome-shell>
```

- 2 再次重新啟動 GNOME Shell 工作階段。

SSO 無法連線到關閉電源代理程式

Single Sign-On (SSO) 不會連線到關閉電源代理程式。

問題

當您以代理的身分登入並連線到代理程式時，SSO 無法連線到關閉電源代理程式。

解決方案

- ◆ 手動登入桌面平台，或在中斷連線後重新連線到代理程式。

在建立 Linux 的手動桌面平台集區後無法連線虛擬機器

虛擬機器狀態為沒有回應。

問題

在您建立手動桌面平台集區後，虛擬機器的狀態可能是 [正在等待代理程式] 或 [無法連線]。

原因

有若干使用者錯誤組態或設定可能會導致虛擬機器處於 [無法連線] 或 [正在等待代理程式] 狀態。

- 確認選項 `machine.id` 存在於虛擬機器 `vmx` 組態檔中。

如果不存在，請確認虛擬機器已正確新增至桌面平台集區。若非如此，請重新建立桌面平台集區，讓代理將該選項重新寫入至 `vmx` 組態檔。

- 確認 VMware Tool 或 Open VM Tool 已正確安裝。

如果安裝 VMware Tool 或 Open VM Tool 的步驟未正確執行，則 `vmware-rpctool` 命令可能不會存在於 Linux 虛擬機器中的 `PATH` 下。您必須遵循指南來安裝 VMware Tool 或 Open VM Tool。

完成安裝後，請執行命令。

```
#vmware-rpctool "machine.id.get"
```

machine.id 值會從虛擬機器 vmx 組態檔中列出。

- 確認代理的 FQDN 是否可在代理程式 Linux 虛擬機器中解析為 IP 位址。