

VMware Horizon JMP Server 安裝和設定指南

2020 年 3 月

VMware Horizon 7 7.12



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 © 2018-2020 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

目錄

1	VMware Horizon JMP Server 安裝和設定指南	5
2	安裝和設定 JMP Server 的工作概觀	6
3	JMP Server 的系統需求	7
	必要的 JMP 技術元件	7
	JMP Server 的硬體需求	7
	JMP Server 支援的作業系統	8
	JMP Server 的網路需求	8
	JMP Server 的資料庫需求	8
	JMP Server 的连接埠和通訊協定需求	9
	JMP Integrated Workflow 的支援網頁瀏覽器	10
4	為 JMP Server 準備 SQL Server 資料庫和登入	11
	為 JMP Server 建立 SQL Server 資料庫	11
	針對 JMP Server 主機建立 SQL Server 登入	12
	針對 JMP Server 主機建立 SQL Server Windows 驗證登入	12
	針對 JMP Server 主機建立 SQL Server 驗證登入	13
	授與 Windows 使用者資料庫擁有者和系統管理權限	14
5	安裝與升級 JMP Server	16
	安裝 JMP Server	16
	升級 JMP Server	19
6	設定 JMP Server 執行個體	20
	將 Horizon 連線伺服器和 JMP Server 主機之間的時間同步	20
	針對 JMP Server 設定 TLS 憑證和加密套件	21
	針對 JMP Server 設定 TLS 憑證的工作概觀	21
	取代預設的 TLS 憑證	23
	設定 JMP Server 以使用憑證鏈結檔案	24
	設定 JMP Server 以使用 Active Directory 的憑證	25
	設定 JMP Server 以使用 Horizon 連線伺服器憑證	26
	設定 JMP Server 以使用 App Volumes Manager 憑證	27
	設定 JMP Server 的加密套件	28
	在 JMP Server 上使用較多限制的 CORS 原則	29
7	在 JMP Server 安裝後更新資料庫密碼	31

[更新 VMware JMP 平台服務的資料庫密碼](#) 31

[更新 VMware JMP 檔案共用服務的資料庫密碼](#) 32

8 疑難排解您的 JMP Server 35

[JMP Server 無法使用錯誤](#) 35

[更新服務帳戶密碼之後發生錯誤](#) 36

[解除安裝 JMP Server](#) 37

VMware Horizon JMP Server 安裝和設定指南

1

《VMware Horizon JMP Server 安裝和設定指南》說明如何安裝和設定 VMware Horizon[®] Just-in-Time Management Platform (JMP) Server。安裝 JMP Server 並且 JMP 設定已設定之後，您可以開始使用 VMware Horizon Console 中的 JMP Integrated Workflow 功能來定義 JMP 指派。

此文件中的資訊適用於想要安裝 JMP Server 的任何人。這些資訊是針對熟悉虛擬機器技術及資料中心作業的資深 Windows 系統管理員所撰寫。

安裝和設定 JMP Server 的工作概觀

2

您必須在安裝 HorizonJMP Server 前後執行特定工作，才能開始使用 HorizonJMP Integrated Workflow 功能。

下列清單提供您必須完成工作的高階說明。執行這些工作的程序會在此概觀後續的各主題中描述。

- 1 確保已滿足 JMP Server 系統需求。請參閱[第 3 章 JMP Server 的系統需求](#)。
- 2 建立用於儲存安裝期間所建立 JMP Server 服務相關資訊的 SQL Server 資料庫。請參閱[為 JMP Server 建立 SQL Server 資料庫](#)。
- 3 建立 JMP Server 主機用來連線至您在上一個步驟中所建立 SQL Server 資料庫的 SQL Server 登入。如需詳細資訊，請參閱[針對 JMP Server 主機建立 SQL Server 登入](#)。
- 4 確保用於安裝 JMP Server 的 Windows 使用者登入擁有足夠的權限，可修改您建立用於儲存 JMP Server 服務資訊的 SQL Server 資料庫。請參閱[授與 Windows 使用者資料庫擁有者和系統管理權限](#)。
- 5 (選用) 如果在上一個步驟中使用的 SQL Server 使用 TLS 加密，請將其 TLS 憑證匯入 JMP Server 主機上的 Windows 本機憑證存放區。請參閱 Microsoft TechNet 文章[如何使用 Microsoft Management Console 為 SQL Server 執行個體啟用 SSL 加密的〈為特定用戶端啟用加密〉一節](#)，以取得匯出和匯入 SQL Server TLS 憑證的詳細資料。
- 6 安裝 JMP Server。請參閱[安裝 JMP Server](#)。
- 7 同步 Horizon Connection Server 主機與 JMP Server 執行個體 Windows 主機之間的時間。請參閱[將 Horizon 連線伺服器和 JMP Server 主機之間的時間同步](#)。
- 8 設定您 JMP Server 執行個體的 TLS 憑證，以便與 VMware Horizon 7 連線伺服器、VMware App Volumes Manager™、VMware User Environment Manager™，以及組織網路中其他系統的執行個體安全地通訊。請參閱[針對 JMP Server 設定 TLS 憑證和加密套件](#)。
- 9 (選用) 使用您的組織支援的加密套件來變更 JMP Server 執行個體支援的預設加密套件。請參閱[設定 JMP Server 的加密套件](#)。
- 10 (選用) 在您的 JMP Server 執行個體上使用較多限制的跨原始來源資源共用 (CORS) 原則，以增加與 Horizon 7 連線伺服器執行個體進行通訊的安全性。請參閱在[JMP Server 上使用較多限制的 CORS 原則](#)。
- 11 於使用《VMware Horizon Console 管理》文件中的〈第一次進行 JMP 設定〉進行 JMP 設定之前，請使用 Windows 系統管理員重新啟動 JMP Server 服務。

JMP Server 的系統需求

3

在您可以安裝 VMware HorizonJMP Server 和使用 JMP Integrated Workflow 功能之前，必須滿足特定硬體和軟體需求。

本章節討論下列主題：

- 必要的 JMP 技術元件
- JMP Server 的硬體需求
- JMP Server 支援的作業系統
- JMP Server 的網路需求
- JMP Server 的資料庫需求
- JMP Server 的连接埠和通訊協定需求
- JMP Integrated Workflow 的支援網頁瀏覽器

必要的 JMP 技術元件

若要成功安裝 JMP Server，您必須至少已安裝 Horizon 7 伺服器的受支援版本。

若要使用所有可用的 JMP Integrated Workflow 功能，例如應用程式交付管理和內容原則管理，您也必須安裝包含 JMP 技術的 VMware 產品。您可以在安裝 JMP Server 的之前或之後安裝這些額外產品。如果您在安裝 JMP Server 之後安裝這些產品，則將需要使用 Horizon Console 來重新設定 JMP Server。

以下是包含 JMP 技術且為受支援版本的 VMware 產品。

- VMware Horizon 7 (7.5) 或更新版本 (安裝 JMP Server 的最低需求)
- VMware App Volumes 2.xx、2.14 版或更新版本 (適用於即時應用程式交付管理)。不支援 App Volumes 4.0。
- VMware Dynamic Environment Manager 9.2.1 或更新版本 (用於內容原則管理)
- VMware Identity Manager™ 2.9.2 版或更新版本 (用來與 VMware Workspace™ ONE™ 整合)

JMP Server 的硬體需求

您必須在符合特定硬體需求的專用實體或虛擬機器上安裝 JMP Server。

下表列出了在生產環境中 JMP Server 執行個體的最低硬體需求。

表 3-1. 生產環境的 Horizon JMP Server 硬體需求

硬體元件	生產環境中的最低需求
處理器	4 核心 CPU
記憶體	8 GB
儲存空間	100 GB

下表列出了概念驗證 (PoC) 或在實驗室環境中 JMP Server 執行個體的最低硬體需求。

表 3-2. 實驗室環境的 Horizon JMP Server 硬體需求

硬體元件	實驗室環境中的最低需求
處理器	4 核心 CPU
記憶體	4GB
儲存空間	25 GB

JMP Server 支援的作業系統

您必須在支援的 Windows Server 作業系統上安裝 JMP Server。

在下列 Windows Server 作業系統上支援兩種 JMP Server 安裝類型，即概念驗證 (POC) 和生產。

表 3-3. JMP Server 的作業系統支援

作業系統	版本	版本
Windows Server 2008 R2 SP1	64 位元	Standard Enterprise 資料中心
Windows Server 2012 R2	64 位元	Standard 資料中心
Windows Server 2016	64 位元	Standard 資料中心

JMP Server 的網路需求

您計劃安裝 JMP Server 的實體或虛擬機器必須能夠連線您網路上所有交付點 (PoD) 的所有產品端點。

開始使用 JMP Integrated Workflow 功能之前，必須已為 JMP Server 執行個體以及與您 JMP Server 執行個體進行互動之所有技術端點設定所有安全性和 CA 簽署的憑證驗證。如需詳細資訊，請參閱[針對 JMP Server 設定 TLS 憑證和加密套件](#)。

JMP Server 的資料庫需求

JMP Server 安裝程式需要特定的 SQL Server 資料庫版本才能執行 JMP Server 安裝。

JMP Server 在概念驗證 (PoC) 或生產這兩個受支援的工作負載環境中支援下列 SQL Server 版本和版別。

表 3-4. JMP Server 的資料庫需求

工作負載類型	資料庫伺服器	版本	版本
概念驗證 (PoC)	SQL Server Express 2014	64 位元	可用
生產	SQL Server 2012 (SP1、SP2、SP3 和 SP4)	64 位元	Standard 和 Enterprise
生產	SQL Server 2014 (SP1 和 SP2 含 CU7 或更新版本)	64 位元	Standard 和 Enterprise
生產	SQL Server 2016 (SP1 含 CU6 或更新版本)	64 位元	Standard 和 Enterprise

執行 JMP Server 安裝程式之前，您必須建立 JMP Server 安裝程式會在安裝程序期間使用的 SQL Server 資料庫。如需詳細資料，請參閱[為 JMP Server 建立 SQL Server 資料庫](#)。

您也必須提供 JMP Server 安裝程式必須用來連線至您所建立 SQL Server 資料庫的登入認證。您可以選取 JMP Server 安裝程式會使用的驗證類型。使用的預設值為 Windows 驗證。無論您選取 Windows 驗證或 SQL Server 驗證，SQL Server 執行個體中必須已存在 JMP Server 安裝程式使用的登入認證，之後才能開始安裝 JMP Server。如需詳細資料，請參閱[針對 JMP Server 主機建立 SQL Server 登入](#)。

此外，您必須為您計劃用來安裝 JMP Server 的 Windows Server 使用者帳戶建立 SQL Server 登入。此 Windows 使用者必須經過設定以擁有適當的認證，才能修改您建立的 SQL Server 資料庫。

如果 SQL Server 已啟用使用 TLS 加密，您必須匯出其 TLS 憑證，然後將憑證匯入至 JMP Server 執行個體以啟用與 SQL Server 的加密通訊。

JMP Server 的連接埠和通訊協定需求

JMP Server 具有特定的連接埠和通訊協定需求，讓其能夠接聽資料流量並路由傳送至適當的服務。

下表說明 JMP Server 所使用的連接埠和通訊協定。如需外部元件 (例如 SQL Server 和 Horizon Connection Server) 用於接收來自 JMP Server 之資料流量的目的地連接埠相關資訊，請參閱 [VMware Horizon 7 中的網路連接埠指南的「JMP Server」一節](#)。

連接埠	通訊協定	用途
80	HTTP	通常會在 JMP Server 設定為接聽 HTTP 流量時使用。
443	HTTPS	JMP Server 所使用的預設 SSL 連接埠。
8888	HTTP	保留供 JMP API 服務內部使用。
8989	HTTP	保留供 JMP Server 內部使用。
3001	HTTP	保留供 JMP 平台服務內部使用。
3002	HTTP	保留供 JMP 平台服務內部使用。
8889	HTTP	保留供 JMP 檔案共用服務內部使用。

JMP Integrated Workflow 的支援網頁瀏覽器

您可以使用 VMware Horizon 主控台存取 JMP Integrated Workflow 使用者介面 (UI)，該主控台是隨 VMware Horizon 7 連線伺服器 (7.5 版) 及更新版本一併安裝而以 Web 為基礎的應用程式。

支援下列網頁瀏覽器以與 JMP Integrated Workflow 功能搭配使用。

- Google Chrome (支援最新版本)
- Mozilla Firefox (支援最新版本)
- Internet Explorer 10 和 11
- Microsoft Edge

為 JMP Server 準備 SQL Server 資料庫和登入

4

執行 JMP Server 安裝程式之前，您必須建立供 JMP Server 執行個體使用的 SQL Server 資料庫。您也需要建立 JMP Server 安裝程式連線至該 SQL Server 資料庫所需的 SQL Server 登入帳戶。用來執行 JMP Server 安裝程式的 Windows Server 登入帳戶也必須擁有您為 JMP Server 建立之 SQL Server 資料庫的適當存取權。

本章節討論下列主題：

- 為 JMP Server 建立 SQL Server 資料庫
- 針對 JMP Server 主機建立 SQL Server 登入
- 授與 Windows 使用者資料庫擁有者和系統管理權限

為 JMP Server 建立 SQL Server 資料庫

Horizon 桌面平台管理員所建立 JMP Server 服務和 JMP 指派的相關資訊會儲存在 SQL Server 資料庫中。執行 JMP Server 安裝程式之前，您必須建立此資料庫。

備註 在主機發生故障的情況下，使用遠端 SQL 伺服器會相當實用。

必要條件

- 確認在遠端計畫安裝 JMP Server 的主機但位於網路環境的系統上，是否已安裝支援的 SQL Server 版本。如需詳細資料，請參閱 [JMP Server 的資料庫需求](#)。
- 確保使用 SQL Server Management Studio 建立和管理資料庫。如果您要在 PoC 環境中安裝 JMP Server，則可以使用 SQL Server Management Studio Express。請從下列網站下載並進行安裝。

<https://www.microsoft.com/en-us/download/details.aspx?id=42299>

程序

- 1 在已安裝 Microsoft SQL Server 的系統上，選取**開始 > 所有程式 > Microsoft SQL Server 2016、Microsoft SQL Server 2014 或 Microsoft SQL Server 2012**。
- 2 選取 **SQL Server Management Studio**。
- 3 在 [物件總管] 窗格中，連線至 SQL Server 資料庫引擎的執行個體，然後展開該執行個體的節點。
- 4 在**資料庫**上按一下滑鼠右鍵，然後選取**新增資料庫**。

- 5 在**資料庫名稱**文字方塊中，針對您要為 JMP Server 建立的資料庫僅使用 ASCII 字元輸入名稱。

例如：JMPDB

重要 不支援非 ASCII 字元。

- 6 針對資料庫和記錄檔使用 Initial size 和 Autogrowth 參數的預設值。

- 7 按一下**確定**。

SQL Server Management Studio 會將您的資料庫新增至 [物件總管] 窗格中的**資料庫**資料夾。

- 8 結束 Microsoft SQL Server Management Studio。

後續步驟

安裝 JMP Server 之前，請為 JMP Server 主機建立 SQL Server 登入。請參閱[針對 JMP Server 主機建立 SQL Server 登入](#)。

針對 JMP Server 主機建立 SQL Server 登入

在 JMP Server 安裝期間，安裝程式會存取您建立用來儲存要安裝之 JMP Server 服務相關資訊的 SQL Server 資料庫。您必須選取 JMP Server 安裝程式要使用的 SQL Server 登入類型。

若要存取您建立的 SQL Server 資料庫，請選取 Windows 驗證登入或 SQL Server 驗證登入。依預設會使用 Windows 驗證登入。執行 JMP Server 安裝程式之前，請確保您為 SQL Server 登入類型選取的認證已存在。

使用下表來決定建立 JMP Server 安裝程式要使用之 SQL Server 登入所必須完成的工作。

表 4-1. SQL Server 登入類型

SQL Server 登入類型	使用區段中的工作詳細資料
Windows 驗證 (預設)	針對 JMP Server 主機建立 SQL Server Windows 驗證登入
SQL Server 驗證	針對 JMP Server 主機建立 SQL Server 驗證登入

針對 JMP Server 主機建立 SQL Server Windows 驗證登入

您可以指定 JMP Server 安裝程式在存取您建立的 SQL Server 資料庫時使用 Windows 驗證登入。執行 JMP Server 安裝程式之前，您要安裝 JMP Server 所在 JMP Server 主機上必須存在該 SQL Server 登入的認證。

連線至 JMP Server 主機的使用者可存取 JMP SQL Server 資料庫。不過，您也必須確保用於安裝 JMP Server 的 Windows Server 使用者帳戶擁有您為 JMP Server 所建立 SQL Server 資料庫的寫入權限。請參閱[授與 Windows 使用者資料庫擁有者和系統管理權限](#)

必要條件

確保您已針對 JMP Server 執行個體建立 SQL Server 資料庫。若要建立資料庫，請參閱[為 JMP Server 建立 SQL Server 資料庫](#)。

程序

- 1 以 sysadmin (SA) 身分或使用具有 SA 權限的使用者帳戶登入 SQL Server Management Studio 工作階段。
- 2 在 [物件總管] 窗格中，展開您在其中為 JMP Server 執行個體建立資料庫之 SQL 伺服器執行個體的資料夾。
- 3 展開安全性資料夾，在登入上按一下滑鼠右鍵，然後選取**新增登入**。
- 4 在**登入 - 新增**對話方塊中，於一般頁面上以格式 `domain_name\computer_name$` 輸入登入名稱，其中 `computer_name` 為 JMP Server 主機的名稱，而 `domain_name` 為主機所屬的網域。

例如：`mycompany\jmpserver$`

- 5 選取 **Windows 驗證**。
- 6 從**預設資料庫**清單中，選取該登入的預設資料庫。此項目的預設值為主要資料庫。
- 7 從**預設語言**清單中，選取要用於該登入的預設語言。
- 8 為新的登入帳戶指派 sysadmin 伺服器角色。
 - a 在左側的 [選取頁面] 窗格中按一下**伺服器角色**索引標籤。
 - b 在伺服器角色頁面中，選取 **sysadmin** 核取方塊。
- 9 按一下**確定**。

結果

隨即會在 [物件總管] 窗格中的**登入**資料夾下新增登入。

後續步驟

為用來安裝 JMP Server 的 Windows Server 使用者帳戶建立 SQL Server 登入認證。請參閱[授與 Windows 使用者資料庫擁有者和系統管理權限](#)。

針對 JMP Server 主機建立 SQL Server 驗證登入

您可以指定 JMP Server 安裝程式以使用會使用 SQL Server 驗證登入來存取您所建立 SQL Server 資料庫的 SQL Server 登入。執行 JMP Server 安裝程式之前，針對 JMP Server 主機之該 SQL Server 登入類型的登入認證必須存在。

必要條件

確保您已針對 JMP Server 建立 SQL Server 資料庫。若要建立資料庫，請參閱[為 JMP Server 建立 SQL Server 資料庫](#)。

程序

- 1 以 sysadmin (SA) 身分或使用具有 SA 權限的使用者帳戶登入 SQL Server Management Studio 工作階段。
- 2 在 [物件總管] 窗格中，展開您在其中建立 JMP Server 資料庫之 SQL 伺服器執行個體的資料夾。

- 3 展開**安全性**資料夾，在**登入**上按一下滑鼠右鍵，然後選取**新增登入**。
- 4 在**登入 - 新增**的對話方塊中，於一般頁面上的**登入名稱**文字方塊中僅使用 ASCII 字元來輸入值。或者，按一下**搜尋**，然後使用**選取使用者或群組**對話方塊，以找到您要使用的登入。

重要 不支援非 ASCII 字元。

- 5 選取 **SQL Server 驗證**。
- 6 在**密碼**和**確認密碼**文字方塊中，輸入新登入名稱的密碼。僅限使用 ASCII 字元。
- 7 如果您要變更現有的密碼，請選取**指定舊密碼**，然後在**舊密碼**文字方塊中輸入舊密碼。
- 8 根據您組織的原則，選取或取消選取**強制執行密碼原則**、**強制執行密碼逾期**和**使用者必須在下次登入時變更密碼**核取方塊。
- 9 從**預設資料庫**清單中，選取該登入的預設資料庫。此項目的預設值為主要資料庫。
- 10 從**預設語言**清單中，選取該登入的預設語言。
- 11 為新的登入帳戶指派 **sysadmin** 伺服器角色。
 - a 在左側的 [選取頁面] 窗格中按一下**伺服器角色**索引標籤。
 - b 在伺服器角色頁面中，選取 **sysadmin** 核取方塊。
- 12 按一下**確定**。

結果

隨即會在 [物件總管] 窗格中的**登入**資料夾下新增登入。

後續步驟

為用來安裝 JMP Server 的 Windows Server 使用者帳戶建立 SQL Server 登入認證。請參閱[授與 Windows 使用者資料庫擁有者和系統管理權限](#)。

授與 Windows 使用者資料庫擁有者和系統管理權限

除了為 JMP Server 主機機器建立的 SQL Server 登入，您計劃用來安裝 JMP Server 執行個體的 Windows 使用者帳戶必須已建立。此 Windows 使用者帳戶必須獲得您所建立 SQL Server 資料庫中的 sysadmin 和資料庫擁有者權限。

必要條件

- 確保已為您計劃安裝的 JMP Server 建立 SQL Server 資料庫。請參閱[為 JMP Server 建立 SQL Server 資料庫](#)。
- 確認已為 JMP Server 主機建立 SQL Server 登入。請參閱[針對 JMP Server 主機建立 SQL Server 登入](#)。

程序

- 1 以 sysadmin (SA) 身分或使用具有 SA 權限的使用者帳戶登入 SQL Server Management Studio 工作階段。

- 2 在 [物件總管] 窗格中，連線至您為 JMP Server 建立的 SQL 伺服器執行個體。
- 3 為您計劃用來安裝 JMP Server 的 Windows 使用者帳戶建立 SQL Server 登入。
 - a 展開**安全性**資料夾，在**登入**上按一下滑鼠右鍵，然後選取**新增登入**。
 - b 在**登入- 新增**對話方塊中，按一下**搜尋**。
 - c 在**選取使用者或群組**對話方塊中，選取您計劃用來安裝 JMP Server 的有效 Active Directory 使用者。
 - d 在 [登入 - 新增] 對話方塊中，選取頁面，選擇**伺服器角色**，然後選取 **sysadmin** 核取方塊。
 - e 按一下**確定**，關閉**登入 - 新增**對話方塊。
- 4 授與權限給 Windows 使用者帳戶。
 - a 在左窗格中，按一下**資料庫**。
 - b 選取您為 JMP Server 執行個體建立的資料庫，接著按一下**安全性**，然後按一下**使用者**。
 - c 在 [使用者] 窗格中，於 Windows 使用者登入上按一下滑鼠右鍵，然後從關聯式功能表中選取**內容**。
 - d 在 [資料庫角色成員資格] 下，選取 **db_owner** 角色。
 - e 按一下**確定**。

結果

隨即會在 [物件總管] 窗格中的**登入**資料夾下新增登入。

後續步驟

使用**安裝 JMP Server** 中的資訊安裝 JMP Server 執行個體。

安裝與升級 JMP Server

5

若要使用 JMP Integrated Workflow 功能，您必須先安裝並設定 JMP Server 執行個體和必要的 VMwareJMP 技術產品。您可以使用新版的 JMP Server 安裝程式來升級 JMP Server 安裝。

備註 在 Horizon 7(7.5 版) 版本中，您僅能安裝一個 JMP Server 的執行個體。

備註 如果您想要升級目前的 JMP Server 執行個體，請依照[升級 JMP Server](#) 中的說明使用安裝程式，以取得最佳結果。升級安裝程式是執行 JMP Server 升級的偏好方法。

如果您不使用偏好的安裝程式進行升級，而是決定改為先解除安裝目前的 JMP Server 執行個體，再安裝新的執行個體，請注意下列限制。新的 JMP Server 執行個體無法使用由先前的 JMP Server 執行個體在現有資料庫中建立的任何 JMP 組態或指派資料。若要將現有的 JMP 組態和指派用於新的 JMP Server 執行個體，請依序執行下列步驟。

- 1 在解除安裝 JMP Server 執行個體之前，請先備份 .encryption.key 檔案的複本，此檔案位於 C:\Windows\System32\config\systemprofile\AppData\Local\VMware\JMP 中。
 - 2 解除安裝 JMP Server 執行個體。
 - 3 安裝 JMP Server 的新執行個體。
 - 4 導覽至 C:\Windows\System32\config\systemprofile\AppData\Local\VMware\JMP，然後找出 .encryption.key 檔案。將此檔案取代為您先前建立的備份金鑰檔案。
 - 5 重新啟動 VMware JMP Platform Services。
-

本章節討論下列主題：

- [安裝 JMP Server](#)
- [升級 JMP Server](#)

安裝 JMP Server

在可以使用 JMP Integrated Workflow 功能之前，您必須安裝並設定 JMP Server。

當您下載 VMware Horizon 7 (7.5 版) 或更新版本時包含了 JMP Server 安裝程式檔案。成功安裝 Horizon 7 (7.5 版) 或更新版本之後，您必須分別執行 JMP Server 安裝程式。

必要條件

- 確認您已符合安裝 JMP Server 所需元件的系統需求。請參閱[第 3 章 JMP Server 的系統需求](#)。

- 若要在 Windows Server 主機上執行 JMP Server 安裝程式，您必須使用具有該主機系統上管理權限的網域使用者帳戶。
- 確保 JMP Server 執行個體必須使用的 SQL Server 資料庫已建立在遠端系統上，且您擁有對其適當的存取權。請參閱[為 JMP Server 建立 SQL Server 資料庫](#)。
- 確認已為您計劃用來安裝 JMP Server 的 JMP Server 主機和 Windows 網域使用者帳戶設定 SQL Server 登入和權限。請參閱[針對 JMP Server 主機建立 SQL Server 登入](#)。
- 針對要與 JMP Integrated Workflow 功能搭配使用之安全或不安全的 HTTP 連接埠和已簽署憑證，收集其相關資訊。
- 取得憑證授權機構簽署的 TLS 憑證，並使用它來取代 JMP Server 安裝程式所安裝的預設 TLS 憑證。
- 安裝 JMP Server 之前，請使用下表來決定要使用的安裝類型。

安裝類型	JMP Server 安裝程式所採取的動作
生產環境	產生使用 SQL Server Standard 或 Enterprise 版的 JMP Server 執行個體。
開發或概念驗證 (PoC) 環境	產生使用 SQL Server Express 的 JMP Server 執行個體。

- 安裝 JMP Server 之前，將下列檔案新增至 McAfee Antivirus 排除清單中。
 - C:\Program Files (x86)\VMware\JMP\nssm-2.24\nssm-2.24\win32\nssm.exe
 - C:\Program Files (x86)\VMware\JMP\com\xmp\node_modules\winser\bin\nssm.exe

程序

- 1 若要啟動 **VMware JMP 安裝程式** 精靈，請找到 JMP Server 安裝程式檔案並按兩下。

JMP Server 安裝程式檔案名稱為 VMware-Jmp-Installer-e.x.p-xxxxxxx.exe，其中 xxxxxxx 為組建編號。例如，VMware-Jmp-Installer-e.x.p-7259616.exe。

備註 如果您想要記錄安裝程序，請使用下列命令從命令提示字元執行 JMP Server 安裝程式，其中 *Log_Folder_Path* 為要建立記錄檔的資料夾。

```
VMware-Jmp-Installer-e.x.p-xxxxxxx.exe /log:"Log_Folder_Path"
```

- 2 在 [歡迎] 頁面中按**下一步**，並接受 VMware 授權條款。
- 3 若要允許 HTTPS 流量，請按**下一步**。

備註 若要允許透過連接埠 80 的 HTTP 流量，請選取**允許 HTTP?** 核取方塊。

4 提供 SQL Server 執行個體和資料庫目錄資訊。

- a 輸入用來連線至您為 JMP Server 所建立資料庫之 SQL Server 執行個體的 IP 位址或名稱。選擇性地按一下**瀏覽**以進行選取。
- b 選取您想要用來連線至 SQL Server 資料庫的驗證認證。

選項	說明
目前使用者的 Windows 驗證認證	您在此安裝程序期間使用的管理員認證會用來連線至 SQL Server 資料庫執行個體。
使用下列登入識別碼和密碼驗證伺服器	提供用來連線至 SQL Server 資料庫執行個體的登入識別碼和密碼資訊。 備註 密碼可用作 SQL 驗證密碼，且不可包含以下任何字元：, ; = () . 如果密碼包含其中任何字元，則 Dynamic Environment Manager 元件的安裝將失敗並復原。

備註 必須已在 JMP Server 所要存取之 SQL Server 執行個體中設定您使用的登入認證。請參閱[針對 JMP Server 主機建立 SQL Server 登入](#)。

- c 在**資料庫目錄的名稱**文字方塊中，輸入您使用為 JMP Server 建立 SQL Server 資料庫所建立資料庫的名稱。選擇性地按一下**瀏覽**，然後從可用清單中選取資料庫目錄。
選取的資料庫目錄會用來儲存 JMP Server 服務的相關資訊。
- d (選用) 如果您想要覆寫現有資料庫，請選取**覆寫現有資料庫**核取方塊。

備註 第一次執行 JMP Server 安裝程式時，系統會建立必要的資料庫資料表。如果您再次執行安裝程式以建立供負載平衡的更多 JMP Server 執行個體，則安裝程式會發現資料庫已存在，而不會重新建立資料表。選取此選項會覆寫資料庫中的現有資訊。

- e 若要確保 JMP Server 與 SQL Server 執行個體之間的安全通訊，請確認已選取**啟用 SSL**核取方塊。依預設會選取**啟用 SSL**核取方塊。

重要 選取**啟用 SSL**核取方塊時，請確保 SQL Server 中使用的 TLS/SSL 憑證已匯入至 JMP Server 主機上的 Windows 本機憑證存放區。否則，JMP Server 安裝程序會失敗並顯示錯誤「無法執行 uem_migrate.bat 檔案」，且當您在錯誤對話方塊中按一下**確定**時，安裝會回復。

請參閱 Microsoft TechNet 文章[如何使用 Microsoft Management Console 為 SQL Server 執行個體啟用 SSL 加密](#)的〈為特定用戶端啟用加密〉一節，以取得匯出和匯入 SQL Server TLS/SSL 憑證的詳細資料。

- f 按下一步。

5 在準備安裝程式頁面中，按一下**安裝**。

6 安裝成功完成後，按一下**完成**。

結果

成功安裝之後，系統會在您的 Windows Server 主機上安裝並啟動下列 JMP Server 服務。

- VMware JMP API Service
- VMware JMP File Share Service
- VMware JMP Platform Services

後續步驟

同步新安裝之 JMP Server 執行個體及其相關聯 Horizon Connection Server 之間的時間。請參閱[將 Horizon 連線伺服器 and JMP Server 主機之間的時間同步](#)。

升級 JMP Server

當您將目前的 JMP Server 安裝升級為 JMP Server 的更新版本時，系統會保留所有現有的 JMP 設定組態和 JMP 指派。

當您下載 Horizon 7 (7.5 版) 或更新版本時包含了 JMP Server 安裝程式檔案。若要升級現有的 JMP Server 安裝，成功安裝 Horizon 7 (7.6 版) 或更新版本之後，您必須分別執行 JMP Server 安裝程式。

必要條件

您必須使用具有該主機系統管理權限的網域使用者帳戶，才能執行新的 JMP Server 安裝程式檔案。

程序

- 1 若要啟動 **VMware JMP 安裝程式** 精靈，請找到新的 JMP Server 安裝程式檔案並按兩下。
安裝程式將檢查是否有現有的 JMP Server 安裝存在。
- 2 在 [JMP 升級] 對話方塊中按一下**確定**。
- 3 在 [歡迎] 畫面中，按**下一步**。
- 4 閱讀並接受授權合約條款，然後按**下一步**。
- 5 在 [JMP Server 平台服務] 頁面的 [資料庫伺服器] 中，保留現有的資料庫設定，然後按**下一步**。
- 6 在**準備安裝程式**頁面中，按一下**安裝**。
安裝將繼續執行，且需要數分鐘才能完成。
- 7 安裝成功完成後，按一下**完成**。

結果

成功升級之後，系統會在您的 Windows Server 主機上重新啟動三個 JMP Server 服務。

設定 JMP Server 執行個體

6

成功安裝 JMP Server 執行個體後，您必須執行組態工作，以確保可以成功向 Horizon Connection Server 驗證 JMP Server 執行個體，且能安全地與網路中其他伺服器進行通訊。

本章節討論下列主題：

- 將 Horizon 連線伺服器和 JMP Server 主機之間的時間同步
- 針對 JMP Server 設定 TLS 憑證和加密套件

將 Horizon 連線伺服器和 JMP Server 主機之間的時間同步

Horizon 連線伺服器和 JMP Server 主機中的時間必須同步，兩部伺服器之間的驗證程序才能成功。

當您使用 Horizon Console UI 存取 JMP Integrated Workflow 功能時，JMP Server 會驗證它從 Horizon 連線伺服器收到的權杖，然後依次傳回權杖至 JMP Server。如果兩台主機之間的時間未同步，Horizon 連線伺服器會拒絕 JMP Server 所提供的權杖，而 JMP Integrated Workflow 功能會變得無法從 Horizon Console UI 使用。[JMP 設定] 窗格會顯示下列錯誤訊息。

無法確認 Horizon SSO 權杖。

為了讓驗證程序成功，請將 Horizon 連線伺服器與 JMP Server 主機上的時間同步為通用網路時間通訊協定 (NTP) 伺服器。

程序

- 1 使用 Windows 主機上的下列 VMware Tools 命令。

```
C:\Program Files\VMware\VMware Tools>VMwareToolboxCmd.exe timesync status  
C:\Program Files\VMware\VMware Tools>VMwareToolboxCmd.exe timesync enable
```

- 2 在 ESXi 主機上，使 ESXi 時鐘與網路時間伺服器同步。
 - a 啟動 VMware Host Client，並連線至 ESXi 主機。
 - b 按一下設定。
 - c 在系統下，按一下時間組態，然後按一下編輯。

- d 選取**使用網路時間通訊協定 (啟用 NTP 用戶端)**。
- e 在 [新增 NTP 伺服器] 文字方塊中，輸入要與其同步之一或多個 NTP 伺服器的 IP 位址或完整網域名稱。

後續步驟

設定 JMP Server 的 TLS 憑證。請參閱[針對 JMP Server 設定 TLS 憑證的工作概觀](#)。

針對 JMP Server 設定 TLS 憑證和加密套件

若要確保您的 JMP Server 執行個體可以與您網路中的其他伺服器安全地進行通訊，則必須將 JMP Server 執行個體設定為使用有效憑證授權機構 (CA) 簽署的 TLS 憑證。若要增強安全連線，您也可以選擇性地可以變更與您 JMP Server 執行個體進行通訊時其他伺服器會接受和提議的預設加密套件。

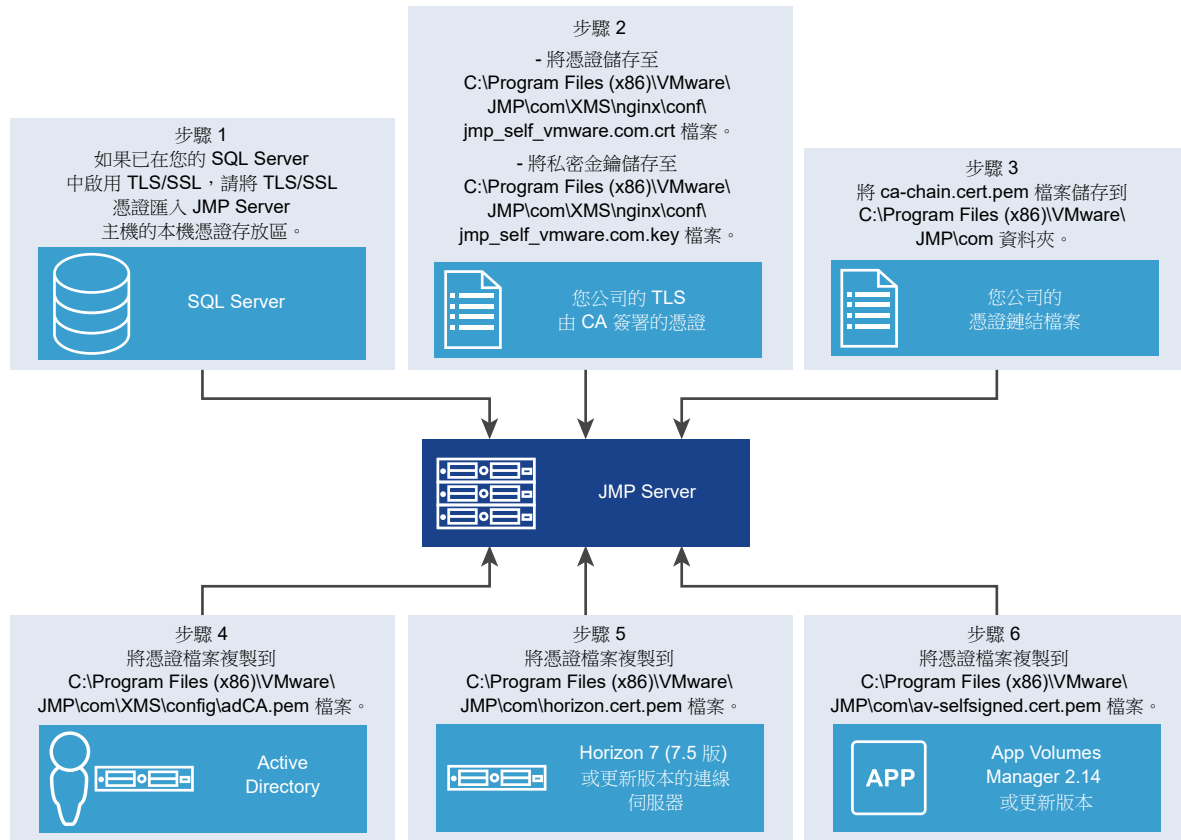
依預設，JMP Server 安裝程式會為您安裝的 JMP Server 執行個體安裝自我簽署的 TLS 伺服器憑證。您可以使用預設憑證進行測試。如果您在生產環境中使用 JMP Server 執行個體，則必須盡快以 CA 簽署的 TLS 伺服器憑證來取代預設憑證。使用未經 CA 簽署的憑證可能會讓不受信任者偽裝成您的伺服器來攔截流量。請參閱[針對 JMP Server 設定 TLS 憑證的工作概觀](#)。

針對 JMP Server 設定 TLS 憑證的工作概觀

成功安裝 JMP Server 之後，您必須執行數個工作來設定由有效憑證授權機構 (CA) 簽署以便與 JMP Server 執行個體搭配使用的 TLS 伺服器憑證。

除了本主題中概述的工作，下圖提供設定 JMP Server 憑證所需之主要步驟的視覺化摘要。確保您遵循此概觀之後主題中所述的詳細步驟，以成功設定特定的憑證。對於標記為選用的工作，請判斷是否必須執行那些工作，以確保您的 JMP Server 組態更安全。完成憑證組態之後，您必須使用 Windows 服務管理員重新啟動三個 JMP Server 服務。

圖 6-1. 設定 JMP Server 憑證的主要步驟



- 1 如果已在您的 SQL Server 中啟用 TLS/SSL，請確保已將 TLS/SSL 憑證匯入 JMP Server 主機的本機憑證存放區。
- 2 取代 JMP Server 安裝程式產生的 TLS 伺服器憑證。

JMP Server 安裝程式產生的預設伺服器憑證為自我簽署，且您的組織網路無法加以識別。請將自我簽署的憑證取代為您從 CA 取得的有效 TLS 憑證。請參閱[取代預設的 TLS 憑證](#)。

如果您的組織無有效的 TLS Web 伺服器憑證，請從 CA 取得簽署的 TLS 伺服器憑證。請參閱《用於設定 Horizon 7 之 TLS 憑證的案例》中的資訊。

- 3 如果組織的伺服器憑證是由中繼 CA 簽署，請設定 JMP Server 以使用組織的憑證鏈結檔案 ca-chain.cert.pem，進而協助 JMP Server 驗證您的網路中的其他伺服器。請參閱[設定 JMP Server 以使用憑證鏈結檔案](#)。

備註 如果您的組織的 TLS 伺服器憑證是由 NodeJS 信任的根 CA 直接簽署，則不需要提供憑證鏈結檔案或根憑證檔案 ca.cert.pem。

- 4 取得用來簽署 Active Directory 伺服器憑證的 CA 憑證、將其儲存到 adCA.pem 檔案，然後將該檔案新增至 JMP Server XMS 組態資料夾。如需詳細資料，請參閱[設定 JMP Server 以使用 Active Directory 的憑證](#)。
- 5 將 Horizon 連線伺服器的 CA 簽署的憑證匯出至 horizon.cert.pem 檔案，然後將該檔案新增至 JMP Server 主資料夾。如需詳細資料，請參閱[設定 JMP Server 以使用 Horizon 連線伺服器憑證](#)。

透過 `horizon.cert.pem` 檔案，JMP Server 可以將連線伺服器驗證為其可連線的可信任伺服器。

備註 您必須針對與 JMP Server 執行個體進行互動的每個連線伺服器網端完成此工作。必須將每個匯出 CA 簽署憑證的內容附加至同一個 `horizon.cert.pem` 檔案。

- 6 如果您在建立 JMP 指派時指派 App Volumes AppStack，請設定您的 JMP Server 執行個體以使用 App Volumes Manager 執行個體的自我簽署憑證，以便可以與 App Volumes Manager 執行個體安全地進行通訊。請參閱[設定 JMP Server 以使用 App Volumes Manager 憑證](#)。
- 7 (選用) 使用您組織支援的加密來變更 JMP Server 執行個體支援的預設加密套件。請參閱[設定 JMP Server 的加密套件](#)。
- 8 (選用) 在您的 JMP Server 上啟用較多限制的跨原始來源資源共用 (CORS) 原則，以增加與 Horizon 7 連線伺服器執行個體進行通訊的安全性。請參閱[在 JMP Server 上使用較多限制的 CORS 原則](#)。
- 9 使用 Windows 服務管理員重新啟動三個 JMP Server 服務。

設定伺服器憑證之後，您可以繼續前往 Horizon Console 來設定 JMP 設定並開始使用 JMP Integrated Workflow 功能。請參閱《VMware Horizon Console 管理》中的〈第一次進行 JMP 設定〉。

取代預設的 TLS 憑證

使用憑證授權機構 (CA) 所簽署的組織 TLS 憑證取代 JMP Server 安裝程式所安裝的預設 TLS 憑證。

成功安裝 JMP Server 執行個體之後，您可以在網頁瀏覽器上使用 Horizon 主控台來存取它。不過，如果您的網路無法辨識已安裝的預設 TLS 憑證，當您第一次進行 JMP 設定時，即會顯示網頁瀏覽器的安全性警示對話方塊。雖然您可以將預設的自我簽署憑證用於測試用途，若要確保與 JMP Server 執行個體的安全連線，請使用 CA 簽署的 TLS 憑證和私密金鑰取代預設的憑證和金鑰。

重要 如果您決定使用與 JMP Server 安裝程式所建立預設名稱不同的檔案名稱來為憑證和金鑰檔案命名，則必須修改 JMP Server NGINX 組態檔才能使用新檔案名稱。

必要條件

- 安裝 JMP Server。請參閱[安裝 JMP Server](#)。
- 取得 CA 簽署的 TLS 憑證，並取代 JMP Server 安裝程式安裝的預設 TLS 憑證。您可以使用如 Microsoft Certreq 或 Windows 上 OpenSSL 的憑證工具來產生憑證。請參閱《用於設定 Horizon 7 之 TLS 憑證的案例》中的〈從憑證授權機構取得 TLS 憑證〉資訊。

程序

- 1 在 JMP Server 主機中，使用 Windows 服務管理員工具停止三個 JMP Server 服務。
 - a 在 Windows **開始**圖示上按一下滑鼠右鍵，然後選取**執行**。
 - b 在 [執行] 對話方塊中，於**開啟**文字方塊中輸入 `services.msc`，然後按一下**確定**。
 - c 在 [服務] 視窗的 [服務 (本機)] 窗格找到下列三個 JMP Server 服務，然後針對每個服務按一下**停止**。
 - VMware JMP API Service
 - VMware JMP File Share Service
 - VMware JMP Platform Services
- 2 將您 CA 簽署的 TLS 伺服器憑證檔案儲存在 JMP Server 主機上 NGINX 組態資料夾中的 `jmp_self_vmware.com.crt`。

例如: `C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\jmp_self_vmware.com.crt`
- 3 將 CA 簽署的 TLS 伺服器憑證隨附私密金鑰儲存為 `jmp_self_vmware.com.key`。

例如: `C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\jmp_self_vmware.com.key`
- 4 (選用) 如果您想要使用與預期憑證檔案名稱 `jmp_self_vmware.com.crt` 或 `jmp_self_vmware.com.key` 不同的檔案名稱，則必須將 NGINX 組態檔修改為新檔案名稱。
 - a 開啟 `C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\nginx.conf` 組態檔。
 - b 找到 `jmp_self_vmware.com.crt` 和 `jmp_self_vmware.com.key` 內容項目，並將其取代為您選取新檔案名稱。
 - c 儲存 `nginx.conf` 檔案。

結果

您現在可以安全地存取 JMP Integrated Workflow 功能而不會出現網頁瀏覽器安全性警示對話方塊。

後續步驟

如果您組織的整個憑證鏈結由中繼 CA 所簽署，請將 JMP Server 執行個體設定為使用憑證鏈結檔案。請參閱[設定 JMP Server 以使用憑證鏈結檔案](#)。若否，請繼續設定您的 JMP Server 執行個體以使用 Active Directory 的憑證。請參閱[設定 JMP Server 以使用 Active Directory 的憑證](#)。

設定 JMP Server 以使用憑證鏈結檔案

如果您的組織伺服器憑證是由中繼憑證授權機構 (CA) 所簽署，請使用組織的整個憑證鏈結 (包括根憑證和中繼憑證) 來設定 JMP Server 執行個體。

必要條件

- 使用 Windows 服務管理員來停止三個 JMP Server 服務。

程序

- 1 建立名為 `ca-chain.cert.pem` 的檔案。在文字編輯器 (例如 Notepad++) 中開啟檔案。
- 2 在相同的文字編輯器中，開啟組織的根憑證。將根憑證的內容複製到 `ca-chain.cert.pem`。
針對任何中繼憑證檔案 (如果存在) 重複此步驟。將每個中繼憑證的內容附加到 `ca-chain.cert.pem` 的結尾。
- 3 儲存並關閉 `ca-chain.cert.pem`。
您現在已有一個憑證鏈結檔案，其中包含組織的根憑證和中繼憑證。
- 4 將 `ca-chain.cert.pem` 憑證鏈結檔案複製到 `C:\Program Files (x86)\VMware\JMP\com` 資料夾中。

結果

備妥憑證鏈結之後，JMP Server 執行個體即可驗證的 Horizon 7 和 App Volumes 執行個體，並與其安全地進行通訊。

後續步驟

設定具有 Active Directory 憑證的 JMP Server 執行個體，以便 JMP Server 執行個體可以在桌面平台管理員使用 JMP Integrated Workflow 功能時驗證 Active Directory 伺服器。請參閱[設定 JMP Server 以使用 Active Directory 的憑證](#)。

設定 JMP Server 以使用 Active Directory 的憑證

為了讓 JMP Server 驗證 Horizon Console 連線的 Active Directory，您必須設定 JMP Server 以使用該 Active Directory 伺服器的憑證。

您必須將 Active Directory 網域的根 CA 憑證匯出至名為 `adCA.pem` 的憑證檔案，並將此檔案放在 JMP Server XMS 組態資料夾中。

必要條件

- 必須安裝 JMP Server。
- 必須為 Active Directory 設定透過 SSL 的 LDAP (LDAPS) 或 StartTLS (透過 TLS 的 LDAP)。
- Active Directory 網域的根 CA 憑證。如果憑證未採用 PEM (Base64 編碼) 格式，請參閱 OpenSSL 說明文件 (或類似的文件) 以將檔案轉換為 PEM 格式。

備註 如果您擁有來自不同網域的多個根憑證，可以透過逐一將每個檔案的內容複製到單一 `.pem` 檔案，將所有 PEM 格式憑證合併至單一檔案。

程序

- 1 確保該 PEM 格式憑證檔案的名稱為 `adCA.pem`。
- 2 將 `adCA.pem` 檔案複製到 JMP Server XMS 組態資料夾。
例如：`C:\Program Files (x86)\VMware\JMP\com\XMS\config\adCA.pem`。

結果

透過為 JMP Server 執行個體設定的 Active Directory 憑證，系統會將 Active Directory 辨識為受信任的伺服器，而 Horizon Console 使用者可以成功使用 JMP Integrated Workflow 功能。

後續步驟

使用連線伺服器憑證設定 JMP Server，以便該 JMP Server 執行個體可在桌面平台管理員使用 JMP Integrated Workflow 功能時驗證連線伺服器。請參閱[設定 JMP Server 以使用 Horizon 連線伺服器憑證](#)。

設定 JMP Server 以使用 Horizon 連線伺服器憑證

為了讓 JMP Server 驗證 Horizon Console 連線的 Horizon 7 連線伺服器，您必須設定 JMP Server 以使用 Horizon 7 連線伺服器的憑證。

您必須將 Horizon 7 連線伺服器憑證匯出至名為 `horizon.cert.pem` 的憑證檔案，並將此檔案放在 JMP Server 主資料夾中。

重要 必須將每個匯出 CA 簽署憑證的內容附加至相同的 `horizon.cert.pem` 檔案。

新增 CA 簽署或自我簽署 Horizon 7 連線伺服器憑證時，請使用這些相同的程序。

必要條件

- 必須安裝 JMP Server。
- 您必須具有 Horizon 7 連線伺服器的管理存取權。

程序

- 1 登入與 Horizon Console 和您所安裝 JMP Server 互動之 Horizon 7 連線伺服器的 Windows Server 主機。
- 2 在 Windows **開始**圖示上按一下滑鼠右鍵、選取**執行**，然後輸入 `mmc.exe`。
MMC 公用程式視窗隨即顯示。
- 3 新增憑證嵌入式管理單元。
 - a 在**主控台根目錄**視窗中，選取**檔案 > 新增/移除嵌入式管理單元**。
 - b 在**新增或移除嵌入式管理單元**視窗，從 [可用的嵌入式管理單元] 窗格中，選取**憑證**，然後按一下**新增**。
 - c 新增憑證後，按一下**確定**。
 - d 在憑證嵌入式管理單元視窗中，選取**電腦帳戶**，然後按**下一步**。
 - e 在 [選取電腦] 視窗中，選取**本機電腦**，然後按**完成**。
憑證 (本機電腦) 嵌入式管理單元隨即在 [選取的嵌入式管理單元] 窗格中新增。
 - f 按一下**確定**以關閉**新增或移除嵌入式管理單元**對話方塊。
- 4 回到 [主控台根目錄] 視窗中，選取**主控台根目錄 > 憑證 (本機電腦)**，並在左窗格中選取**個人 > 憑證資料夾**以顯示其內容。

5 匯出 Horizon 連線伺服器憑證。

- a 在憑證內容窗格中，找到具有易記名稱 **vdm** 的憑證。
此憑證屬於 Horizon 連線伺服器。
- b 在憑證上按一下滑鼠右鍵，然後選取**所有工作 > 匯出**。
- c 在 [憑證匯出精靈] 對話方塊中，按**下一步**。
- d 選取**否，不要匯出私密金鑰**，然後按**下一步**。
- e 選取 **Base-64 編碼 X.509 (.CER)** 格式，然後按**下一步**。
- f 以 **horizon.cert.pem** 形式輸入檔案名稱，然後按一下**瀏覽**，導覽至要儲存已匯出憑證的資料夾。

重要 您必須使用 **.pem** 副檔名來儲存匯出的憑證檔案，而非使用 **.cer** 或 **.crt** 副檔名。如有必要，在文字編輯器中開啟匯出的憑證檔案，並將其儲存為 **horizon.cert.pem**。

- g 按**下一步**，然後按一下**完成**以關閉憑證匯出精靈視窗。

已成功匯出憑證。

6 導覽至儲存已匯出的 horizon.cert.pem 憑證的位置，然後將其複製到 JMP Server 主資料夾。

例如：C:\Program Files (x86)\VMware\JMP\com\horizon.cert.pem。

結果

透過為 JMP Server 設定的連線伺服器憑證，系統會將連線伺服器辨識為受信任的伺服器，而 Horizon Console 使用者可以成功使用 JMP Integrated Workflow 功能。

後續步驟

檢閱[針對 JMP Server 設定 TLS 憑證的工作概觀](#)中所列出的選用工作，並判斷您是否也必須完成這些工作。如果您已完成所有必要的組態工作，請重新啟動 JMP Server 服務，然後進行 JMP 設定。如需詳細資訊，請參閱《VMware Horizon Console 管理》中的〈第一次進行 JMP 設定〉。

設定 JMP Server 以使用 App Volumes Manager 憑證

如果您在建立 JMP 指派時指派 App Volumes AppStack，請設定您的 JMP Server 執行個體以使用 App Volumes Manager 執行個體的憑證，以便可以與 App Volumes Manager 執行個體安全地進行通訊。

在 PoC 安裝環境中，您必須將 App Volumes Manager 執行個體的自我簽署憑證匯出至名為 **av-selfsigned.cert.pem** 的憑證檔案，才能讓 JMP Server 使用該檔案。如果 App Volumes Manager 使用 CA 簽署的憑證，請將 JMP Server 設定為使用您組織的憑證鏈結檔案 **ca-chain.cert.pem** 以驗證 App Volumes Manager 執行個體。請參閱[設定 JMP Server 以使用憑證鏈結檔案](#)。

必要條件

- 必須安裝 JMP Server。
- 您必須具有 App Volumes Manager 執行個體或管理它之負載平衡器的管理存取權。

程序

- 1 從 JMP Server 主機，使用網頁瀏覽器登入 App Volumes Manager 執行個體或管理您環境中 App Volumes Manager 執行個體的負載平衡器。
- 2 若要尋找 App Volumes Manager 執行個體或負載平衡器使用的憑證資訊，請使用網頁瀏覽器的憑證管理員，然後將 Base-64 編碼 X.509 (.CER) 格式的憑證檔案匯出至 C:\Program Files (x86)\VMware\JMP\com\av-selfsigned.cert.pem 檔案。

重要 您必須使用 .pem 副檔名來儲存匯出的憑證檔案，而非使用 .cer 或 .crt 副檔名。如有必要，在文字編輯器中開啟匯出的憑證檔案，並將其儲存為 av-selfsigned.cert.pem。

例如，使用 Google Chrome 網頁瀏覽器時，按一下**設定 > 進階**，然後選取**管理憑證**。在 [憑證] 對話方塊中，選取 App Volumes Manager 憑證，然後按一下**匯出**。使用憑證匯出精靈將 Base-64 編碼 X.509 (.CER) 格式的 App Volumes Manager 憑證匯出至 C:\Program Files (x86)\VMware\JMP\com\av-selfsigned.cert.pem 檔案。您可能需要重新命名檔案，使其僅具有 .pem 副檔名，而非 .pem.cer 副檔名。

- 3 如果您已完成設定 TLS 憑證以提升 JMP Server 安全性的所有必要工作，請重新啟動 JMP Server 服務。請參閱[針對 JMP Server 設定 TLS 憑證的工作概觀](#)以檢閱任何剩餘的 TLS 憑證組態工作。

設定 JMP Server 的加密套件

JMP Server 安裝包括在 JMP Server、Horizon Connection Server、App Volumes 與 Dynamic Environment Manager 執行個體之間所接受和提議的預設伺服器端和用戶端加密套件。您可以選擇性地使用您組織支援的加密方式來變更 JMP Server 支援的這些預設加密套件。

系統所使用的加密套件取決於 JMP Server 是否作為接收安全連線要求的伺服器，或作為用戶端以起始 Horizon Connection Server、App Volumes 或 Dynamic Environment Manager 的安全連線要求。

您必須使用 <https://www.openssl.org/docs/man1.0.2/apps/ciphers.html#CIPHER-LIST-FORMAT> 中定義的格式來指定加密套件清單。下列是伺服器端使用的預設加密套件清單。

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES128-SHA:AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256:AES256-SHA:AES128-SHA:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4
```

除了上述加密字串以外，可接受的通訊協定 TLSv1.1 和 TLSv1.2 也會決定系統使用的實際加密套件，如 nginx.conf 檔案中所定義。

程序

- 1 在 JMP Server 主機中，使用 Windows 服務管理員工具停止三個 JMP Server 服務。
 - a 在 Windows **開始**圖示上按一下滑鼠右鍵，然後選取**執行**。
 - b 在 [執行] 對話方塊中，於**開啟**文字方塊中輸入 `services.msc`，然後按一下**確定**。
 - c 在 [服務] 視窗的 [服務 (本機)] 窗格中，找到下列三個 JMP Server 服務，然後針對每個服務，按一下**停止**。
 - VMware JMP API Service
 - VMware JMP File Share Service
 - VMware JMP Platform Services
- 2 修改包含加密套件的組態檔案。

若要修改伺服器端加密套件：

 - a 導覽至 `C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf` 資料夾。
 - b 在進行修改之前，請建立 `nginx.conf` 檔案的備份複本。
 - c 使用記事本開啟 `nginx.conf` 檔案。
 - d 找到以 `ssl_ciphers` 開頭的行，並視需要修改加密套件。
 - e 儲存您對 `nginx.conf` 檔案所做的變更。

若要修改用戶端加密套件：

 - a 導覽至 `C:\Program Files (x86)\VMware\JMP\com\xmp\conf` 資料夾。
 - b 使用記事本開啟 `jmp.js` 檔案。
 - c 在進行修改之前，請建立 `jmp.js` 檔案的備份複本。
 - d 找到包含下列程式碼片段的行。


```
ciphers:'!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES'
```
 - e 在程式碼片段中的 `ciphers:` 區段後修改加密套件。例如：


```
ciphers:'your_organization_cipher_suite'
```
 - f 儲存您對 `jmp.js` 檔案所做的變更。
- 3 使用 Windows 服務管理員工具來重新啟動這三個 JMP Server 服務，如此新的加密套件清單才會生效。

在 JMP Server 上使用較多限制的 CORS 原則

藉由建立受信任而可存取您 JMP Server 之 Horizon 7 連線伺服器執行個體的白名單，您可以在 JMP Server 執行個體上使用較多限制的跨原始來源資源共用 (CORS) 原則。

依預設，如果 Horizon 7 連線伺服器是使用與您使用[設定 JMP Server 以使用憑證鏈結檔案](#)所設定憑證鏈結檔案中的相同憑證，則該連線伺服器可以存取您的 JMP Server 執行個體。若要確保僅 Horizon 7 連線伺服器執行個體的已核准清單可以存取您的 JMP Server，請執行下列步驟。

程序

- 1 使用文字編輯器，開啟位於 C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\nginx.conf 的 NGINX 組態檔。

- 2 找到出現下列文字的兩處，並移除前置的 # 標記，將其取消註解，使其顯示如下。

```
add_header "Access-Control-Allow-Origin" "$cors_header" always;
```

- 3 找到出現下列文字的兩處，並新增前置的 # 標記，將其標記為註解，使其顯示如下。

```
# add_header "Access-Control-Allow-Origin" "$http_origin" always;
```

- 4 將連線伺服器執行個體核准的清單新增至白名單。

- a 在檔案中找到下列內容。

```
# CORS: Whitelist of origins allowed to contact JMP
# Syntax Documentation: https://nginx.org/en/docs/http/ngx_http_map_module.html
map $http_origin $cors_header {
    # default value
    # by default no one is allowed
    default '';

    # List of hosts allowed to access JMP
    # "~*(https://\YOUR_CONNECTION_SERVER_DOMAIN\.com)$" "$http_origin";
}
```

- b 在 default ''; 行後，針對您想要包含在白名單中的每個連線伺服器執行個體新增一行。

例如，如果允許連線至您 JMP Server 連線伺服器執行個體的網域名稱為 **www.testhorizon.com** 和 **www.prodhorizon.com**，則要新增的行在下列範例中會以粗體顯示。

```
default '';
"~*(https://\testhorizon\.com)$" "$http_origin";
"~*(https://\prodhorizon\.com)$" "$http_origin";
```

- 5 儲存您對 nginx.conf 檔案所做的變更。
- 6 使用 Windows 服務管理員重新啟動 JMP 平台服務。

在 JMP Server 安裝後更新資料庫密碼



如果您修改初始 JMP Server 安裝期間使用的 SQL Server 資料庫密碼，則也必須更新 VMware JMP Server 服務使用的資料庫密碼資訊。

本章節討論下列主題：

- [更新 VMware JMP 平台服務的資料庫密碼](#)
- [更新 VMware JMP 檔案共用服務的資料庫密碼](#)

更新 VMware JMP 平台服務的資料庫密碼

如果您修改 JMP Server 安裝時所使用的 SQL Server 資料庫密碼，則也必須更新由 VMware JMP 平台服務用來連線至您 SQL Server 資料庫的資料庫密碼。

必要條件

請確認您有正確的管理權限，才能變更 JMP Server 主機中的資料庫資訊。

程序

- 1 在 JMP Server 主機中，使用 Windows 服務管理員工具停止 VMware JMP Platform Services 程序。
 - a 在 Windows **開始**圖示上按一下滑鼠右鍵，然後選取**執行**。
 - b 在 [執行] 對話方塊中，於**開啟**文字方塊中輸入 `services.msc`，然後按一下**確定**。
 - c 找到 [服務] 視窗中 [服務 (本機)] 窗格的 VMware JMP Platform Services，然後按一下**停止**。
- 2 按兩下適用於您 JMP Server 主機的下列其中一個可執行檔，以開啟 **ODBC 資料來源管理員**視窗。
 - `C:\Windows\SysWow64\odbcad64.exe`
 - `C:\Windows\system32\odbcad32.exe`
- 3 在 [ODBC 資料來源管理員] 視窗中，按一下**系統 DSN**，然後選取 [使用者資料來源] 窗格中的 **svmanager**。
- 4 按一下**設定**。

Microsoft SQL Server DSN 組態精靈隨即顯示。

5 按下一步。

注意 請勿變更資料來源名稱或伺服器文字方塊中的現有資訊。

6 確保已選取使用由使用者所輸入的登入識別碼及密碼進行 SQL Server 帳戶驗證。

7 在密碼文字方塊中輸入新密碼，然後按下一步。

8 再次按下一步，不變更預設資料庫資訊頁面中的現有資訊。

9 按一下完成。

ODBC Microsoft SQL Server 設定摘要視窗會顯示組態詳細資料。

10 檢閱摘要資訊，然後按一下確定以繼續進行 VMware JMP Platform Services 服務的密碼修改。

11 將新的密碼資訊新增至 VMware JMP 平台服務資料庫組態檔，然後再重新啟動 VMware JMP Platform Services 服務。

- 以管理員身分，使用文字編輯器開啟位於 C:\Program Files (x86)\VMware\JMP\com\XMS\config\database.yml 的資料庫組態檔。
- 找到使用者名稱內容的行，然後在該行後插入密碼內容的新一行。
- 輸入您已建立的密碼資訊，以便其顯示如下列範例所示。

```
密碼: new_password
```

重要 VMware JMP Platform Services 服務重新啟動後，此密碼資訊將會自動從 database.yml 檔案中移除。

12 重新啟動 VMware JMP Platform Services 服務。

- 在 Windows 開始圖示上按一下滑鼠右鍵，然後選取執行。
- 在 [執行] 對話方塊中，於開啟文字方塊中輸入 services.msc，然後按一下確定。
- 找到 [服務] 視窗中 [服務 (本機)] 窗格的 VMware JMP Platform Services，然後按一下啟動。

後續步驟

如果尚未執行此操作，您也必須更新 VMware JMP 檔案共用服務所使用的資料庫登入帳戶資訊。請參閱[更新 VMware JMP 檔案共用服務的資料庫密碼](#)。

更新 VMware JMP 檔案共用服務的資料庫密碼

如果您修改 JMP Server 安裝時所使用的 SQL Server 資料庫密碼，則也必須更新由 VMware JMP 檔案共用服務用來連線至您 SQL Server 資料庫的資料庫密碼。

必要條件

請確認您有正確的管理權限，才能變更 JMP Server 主機中的資料庫資訊。

程序

- 1 在 JMP Server 主機中，使用 Windows 服務管理員工具停止 VMware JMP File Share Service 程序。
 - a 在 Windows 開始圖示上按一下滑鼠右鍵，然後選取**執行**。
 - b 在 [執行] 對話方塊中，於**開啟**文字方塊中輸入 `services.msc`，然後按一下**確定**。
 - c 找到 [服務] 視窗中 [服務 (本機)] 窗格的 VMware JMP File Share Service，然後按一下**停止**。
- 2 更新 VMware JMP 檔案共用服務所使用的密碼。使用下列資訊，以根據 JMP Server 安裝期間使用的 SQL Server 連線類型來判斷所用步驟。

- 針對 SQL 驗證連線模式：

- 1 導覽到 `C:/Program Files (x86)/VMware/JMP/com/uem` 資料夾，然後在文字編輯器中開啟 `db.json` 檔案。
- 2 新增新的 `password` 參數，並將其設定為安裝 JMP Server 後建立的新 SQL Server 資料庫密碼。範例如下。

```
"jmp.production": {
  "server": "MyOrg-DB_server\\SQL2014",
  "database": "MyOrg-database",
  "userName": "sa",
  "password": "new_SQL_password",
  "stamp": "nnXXpIIgeImfPJWbuOYAQA==.EDlk3lCqSubg6Y2uIwSSgw=="
}
```

- 3 儲存檔案並結束文字編輯器。

- 針對 Windows 驗證連線模式：

- 1 導覽到 `C:/Program Files (x86)/VMware/JMP/com/uem` 資料夾，然後在文字編輯器中開啟 `db.json` 檔案。
- 2 將現有檔案內容取代為下列內容，其中 `<IP address>` 為 SQL Server 主機的 IP 位址，而 `<Database name>` 為有效的資料庫名稱。

```
{
  "jmp.production": {
    "connectionString": "Server=<IP address>;Database=<Database name>;Trusted_Connection=Yes;"
  }
}
```

- 3 儲存檔案並結束文字編輯器。

- 3 重新啟動 VMware JMP File Share Service。

- a 在 Windows 開始圖示上按一下滑鼠右鍵，然後選取**執行**。
- b 在 [執行] 對話方塊中，於**開啟**文字方塊中輸入 `services.msc`，然後按一下**確定**。
- c 找到 [服務] 視窗中 [服務 (本機)] 窗格的 VMware JMP File Share Service，然後按一下**啟動**。

後續步驟

如果尚未執行此操作，您也必須更新 VMware JMP 平台服務所使用的資料庫登入帳戶資訊。請參閱[更新 VMware JMP 平台服務的資料庫密碼](#)。

疑難排解您的 JMP Server

8

安裝、設定及登錄 JMP Server 執行個體時您可能會遇到錯誤訊息。您可以使用本章中的疑難排解資訊。

本章節討論下列主題：

- [JMP Server 無法使用錯誤](#)
- [更新服務帳戶密碼之後發生錯誤](#)
- [解除安裝 JMP Server](#)

JMP Server 無法使用錯誤

您無法連線至您的 JMP Server 執行個體。

問題

使用 Horizon Console 來登錄 JMP Server 執行個體時，您可能會看到錯誤訊息：您輸入的 JMP Server 無法使用。請修改輸入的內容，或稍後再試一次。

原因

顯示錯誤訊息的原因有多種可能。若要確定原因及因應措施，請使用下列小節中的資訊。

解決方案

- 1 確保已正確設定憑證。
使用針對 [JMP Server 設定 TLS 憑證和加密套件](#) 中的資訊。
- 2 嘗試登錄 JMP Server URL 之後，請檢閱來自 Web 瀏覽器的 HTTP 回應。

如果您收到類似於下列輸出的 HTTP 回應，

```
{errors: {}, error: "Insufficient Horizon Privileges", code: 400}  
code:400  
error:"Insufficient Horizon Privileges"  
errors:{}
```

請使用下列步驟來確認您用來登入 Horizon Console 的使用者帳戶擁有足夠的管理員權限。

- a 在 Horizon Administrator 中，選取 **View 組態 > 管理員**。

- b 在 [管理員] 窗格中，確認您的管理員使用者帳戶顯示為 <domain-name>\Administrator (不是顯示為 BUILTIN\Administrator)，且其已獲指派完整管理員權限。
- c 如果您看到 BUILTIN\Administrator，請套用 [VMware Horizon 7 \(7.5 版\) 版本說明](#) 中所述的因應措施。

如需管理管理員權限的相關資訊，請參閱《Horizon 7 管理》文件中的〈管理和檢閱權限〉。

- 3 如果網頁瀏覽器 HTTP 回應的 JSON Web Token (JWT) 訊息中有類似以下的錯誤訊息：
`{"code":403,"error":"Error: Unable to verify Horizon JWT","error_code":"1044","error_type":"horizonJwtVerificationError"}`，請確保 JMP Server 主機與 Horizon Connection Server 主機之間的時間已同步。

使用將 [Horizon 連線伺服器](#) 和 [JMP Server 主機之間的時間同步](#) 中提供的資訊。

更新服務帳戶密碼之後發生錯誤

變更初始 JMP Server 組態期間使用的任何服務帳戶使用者密碼後，當您嘗試使用 JMP Server 執行個體來執行工作時收到錯誤訊息。

您也必須使用新密碼資訊來更新 JMP Server 資料庫。使用 Ruby on Rails 主控台來更新儲存在 JMP Server SQL Server 資料庫中的密碼。

注意 使用 Ruby on Rails 主控台修改值可能會對您的環境產生嚴重影響。如果您不熟悉 Ruby on Rails 主控台，請先在測試環境中的練習執行命令，然後再於生產環境中套用變更。

問題

當您嘗試使用 JMP Server 執行個體執行 JMP 整合式工作流程工作時，可能會看到下列錯誤之一。

```
Error 1: "errors":{}, "error": "Login failed", "code": 500}
Error 2: "Unable to contact AV Manager"
Error 3: "Users search fails in JMP Assignments"
```

原因

如果更新 JMP Server 執行個體初始組態期間使用過的任何服務帳戶密碼，因為 JMP Server 仍在使用舊密碼，您可能會看到上述所列的其中一個錯誤。如果變更了 Horizon 7 服務帳戶密碼，則可能會發生錯誤 1。如果變更了 App Volumes Manager 服務帳戶密碼，或如果服務已關閉，則可能會發生錯誤 2。如果變更了 Active Directory (AD) 密碼，則可能會發生錯誤 3。

解決方案

- 1 從 JMP Server 主機上的 Windows 命令提示字元中，導覽至 JMP Server XMS 組態資料夾，然後啟動 Ruby on Rails 主控台。

```
cd C:\Program Files (x86)\VMware\JMP\com\XMS
svmanager_run script/rails c production
```

2 若要更新 SQL Server 資料庫中的密碼項目，請使用下列 Ruby on Rails 主控台命令。

表 8-1. 用於更新 SQL Server 資料庫中密碼的命令

動作	Ruby on Rails 主控台命令
更新 Horizon 7 密碼。	<pre>a=Xms::Service.find_by_service_type("horizon") a.password=<new_Horizon7_password> a.save</pre>
更新 App Volumes Manager 密碼。	<pre>a=Xms::Service.find_by_service_type("avmgr") a.password=<new_AVM_password> a.save</pre>
更新 Active Directory 密碼。	<pre>a=Xms::IdentityService.find_by(netbios_name:<netbios-name>) a.password=<new_AD_password> a.save</pre>

3 若要更新 Dynamic Environment Manager 執行個體的密碼，請使用 Horizon Console 之 **UEM** 索引標籤中的**編輯 UEM 檔案共用對話方塊**。

請參閱《VMware Horizon Console 管理》文件中的〈編輯 User Environment Manager 組態檔案共用資訊〉。

備註 如果您也更新了 AD 密碼，則必須先更新 JMP Server SQL Server 資料庫中的 AD 密碼項目，然後再更新 Dynamic Environment Manager 的密碼。

解除安裝 JMP Server

您可能需要解除安裝並重新安裝 JMP Server 才能解決問題。

此程序說明如果您遇到無法使用其他方法解決的問題時，如何解除安裝 JMP Server。

必要條件

- 確認您有解除安裝 JMP Server 的正確管理權限。
- 解除安裝 JMP Server 之前，請刪除與該 JMP Server 相關聯的所有 Dynamic Environment Manager 組態共用。請參閱《VMware Horizon Console 管理》中的〈刪除 User Environment Manager 組態共用資訊〉。

程序

- 1 開啟 Microsoft Windows 程式和功能主控台。
例如，按一下**開始 > 設定 > 系統 > 應用程式與功能**。
- 2 從已安裝應用程式的清單中選取 **VMware JMP**。
- 3 若要完成解除安裝步驟，請按一下**解除安裝**，然後遵循精靈的步驟進行。

後續步驟

重新安裝 JMP Server。如需詳細資料，請參閱[安裝 JMP Server](#) 文件。