VMware Horizon JMP Server Installation and Setup Guide

Modified on 19 JUN 2018
VMware Horizon 7 7.5

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Contents

VMware Horizon JMP Server Installation and Setup Guide

1

VMware Horizon JMP Server Installation and Setup Guide describes how to install and configure VMware Horizon® Just-in-Time Management Platform (JMP) Server. After the JMP Server is installed, and the JMP settings configured, you can begin defining JMP assignments using the JMP Integrated Workflow features in VMware Horizon Console.

The information in this document is intended for anyone who wants to install JMP Server. It is written for experienced Windows system administrators who are familiar with virtual machine technology and data center operations.

Overview of Tasks for Installing and Configuring JMP Server

2

You must perform certain tasks before and after you install Horizon JMP Server, and before you can begin using the Horizon JMP Integrated Workflow features.

The following list provides a high-level description of the tasks that you must complete. The procedures for carrying out these tasks are described in the topics that follow this overview.

1. Ensure that the JMP Server system requirements are met. See Chapter 3 System Requirements For JMP Server.
2. Create a SQL Server database that is used to store information about the JMP Server services that are created during installation. See Create a SQL Server Database for JMP Server.
3. Create the SQL Server login that is used by the JMP Server host to connect to the SQL Server database that you created in the previous step. See Create a SQL Server Login for the JMP Server Host for more information.
4. Ensure that the Windows user login that is used to install JMP Server has sufficient privileges to modify the SQL Server database that you created to store the information for the JMP Server services. See Granting Database Owner and System Administration Permissions for Windows User.
5. (Optional) If the SQL Server used in the previous steps uses TLS encryption, import its TLS certificate into the Windows local certificate store on the JMP Server host. See the "Enable encryption for a specific client" section in the Microsoft TechNet article How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console for details on exporting and importing the SQL Server's TLS certificate.
6. Install JMP Server. See Install JMP Server.
7. Synchronize time between your Horizon Connection Server host and the Windows host for your JMP Server instance. See Synchronize Time Between Horizon Connection Server and JMP Server Hosts.
8. Configure TLS certificates for your JMP Server instance to communicate securely with the instances of VMware Horizon 7 Connection Server, VMware App Volumes™ Manager, VMware User Environment Manager™, and other systems in your organization's network. See Configuring TLS Certificates and Cipher Suites for JMP Server.
9. (Optional) Change the default cipher suites that your JMP Server instance supports with cipher suites that your organization supports. See Configuring Cipher Suites for JMP Server.

10 (Optional) Use a more restrictive Cross-Origin Resource Sharing (CORS) policy on your JMP Server instance for an added secure communication with your Horizon 7 Connection Server instance. See Use a More Restrictive CORS Policy on Your JMP Server.

11 Using Windows Systems Manager, restart the JMP Server services before configuring the JMP settings using "Configure JMP Settings for the First Time" in the *VMware Horizon Console Administration* document.

System Requirements For JMP Server

3

Specific hardware and software requirements must be met before VMware Horizon JMP Server can be installed and the JMP Integrated Workflow features can be used.

This chapter includes the following topics:

Required JMP Technology Components

Supported versions of the VMware products that comprise the JMP technology must be installed before you can install JMP Server and use the JMP Integrated Workflow features.

The following versions of the VMware products must be installed before you begin installing JMP Server.

- VMware Horizon 7 version 7.5 or later
- VMware App Volumes 2.14 or later
- VMware User Environment Manager 9.2.1 or later
- VMware Identity Manager™ 2.9.2 or later (for integration with VMware Workspace™ ONE™)

Hardware Requirements for JMP Server

You must install JMP Server on a dedicated physical or virtual machine that meets specific hardware requirements.

The following table lists the minimum hardware requirements for a JMP Server instance in a production environment.

Table 3-1. Horizon JMP Server Hardware Requirements for a Production Environment

Hardware Component	Minimum Required in a Production Environment
Processor	4 core CPUs
Memory	8 GB
Storage	100 GB

The following table lists the minimum hardware requirements for a JMP Server instance in a proof-of-concept (PoC) or a laboratory environment.

Table 3-2. Horizon JMP Server Hardware Requirements for a Laboratory Environment

Hardware Component	Minimum Required in a Laboratory Environment
Processor	4 core CPUs
Memory	4 GB
Storage	25 GB

Supported Operating System for JMP Server

You must install JMP Server on a supported Windows Server operating system.

The two types of JMP Server installation, proof-of-concept (POC) and production, are supported on the following Windows Server operating systems.

Table 3-3. Operating System Support for JMP Server

Operating System	Version	Edition
Windows Server 2008 R2 SP1	64-bit	Standard Enterprise Datacenter
Windows Server 2012 R2	64-bit	Standard Datacenter
Windows Server 2016	64-bit	Standard Datacenter

Network Requirements for JMP Server

The physical or virtual machine on which you plan to install JMP Server must be able to reach all product endpoints for all the points of delivery (PoDs) across your network.

Before you begin using the JMP Integrated Workflow features, all the security and CA-signed certificate authentication must already be configured for the JMP Server instance and all the technology endpoints that interact with your JMP Server instance. See Configuring TLS Certificates and Cipher Suites for JMP Server for more information.

Database Requirements for JMP Server

The JMP Server installer requires specific SQL Server database versions to perform the JMP Server installation.

JMP Server supports the following SQL Server versions and editions in the two supported workload environments: proof-of-concept (PoC) or production.

Table 3-4. Database Requirements for JMP Server

Workload Type	Database Server	Version	Edition
Proof-of-Concept (PoC)	SQL Server Express 2014	64-bit	Free
Production	SQL Server 2012 (SP1, SP2, SP3, and SP4)	64-bit	Standard and Enterprise
Production	SQL Server 2014 (SP1 and SP2 with CU7 or later)	64-bit	Standard and Enterprise
Production	SQL Server 2016 (SP1 with CU6 or later)	64-bit	Standard and Enterprise

Before running the JMP Server installer, you must create the SQL Server database that the JMP Server installer uses during the installation process. See Create a SQL Server Database for JMP Server for details.

You must also provide the login credentials that the JMP Server installer must use to connect to the SQL Server database that you created. You can select the type of authentication that the JMP Server installer uses. The default used is the Windows authentication. Whether you select the Windows authentication or SQL Server authentication, the login credentials that the JMP Server installer uses must already exist in the SQL Server instance before you can begin installing JMP Server. See Create a SQL Server Login for the JMP Server Host for details.

In addition, you must create a SQL Server login for the Windows Server user account that you plan to use to install the JMP Server. This Windows user must be configured to have the proper credentials to modify the SQL Server database you created.

If your SQL Server is enabled with TLS encryption, you must export its TLS certificate and import the certificate into your JMP Server instance to enable an encrypted communication with the SQL Server.

Supported Web Browser for JMP Integrated Workflow

You access the JMP Integrated Workflow user interface (UI) using the VMware Horizon Console, which is a Web-based application that is installed with VMware Horizon 7 Connection Server version 7.5 and later.

The following Web browsers are supported for use with the JMP Integrated Workflow features.

- Google Chrome (latest versions supported)
- Mozilla Firefox (latest versions supported)

- Internet Explorer 10 and 11
- Microsoft Edge

Preparing the SQL Server Database and Login for JMP Server

4

Before running the JMP Server installer, you must create a SQL Server database for your JMP Server instance to use. You also need to create the SQL Server login account that the JMP Server installer requires to connect to that SQL Server database. The Windows Server login account used to run the JMP Server installer must also have proper access to the SQL Server database that you created for the JMP Server.

This chapter includes the following topics:

Create a SQL Server Database for JMP Server

Information about the JMP Server services and the JMP assignments that Horizon desktop administrators create are stored in a SQL Server database. You must create this database before running the JMP Server installer.

Prerequisites

- Verify that a supported version of SQL Server is installed on the host on which you plan to install JMP Server or in your network environment. For details, see Database Requirements for JMP Server.
- Ensure that you use SQL Server Management Studio to create and administer the database. If you are installing JMP Server in a PoC environment, you can use SQL Server Management Studio Express. Download and install it from the following website.

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

Procedure

1. On the computer where your Microsoft SQL Server is installed, select **Start > All Programs > Microsoft SQL Server 2016**, **Microsoft SQL Server 2014**, or **Microsoft SQL Server 2012**.
2. Select **SQL Server Management Studio**.
3. In the Object Explorer pane, connect to an instance of the SQL Server Database Engine, and then expand the node for that instance.

4 Right-click **Databases** and select **New Database**.

5 In the **Database name** text box, enter a name, using ASCII characters only, for the database you are creating for JMP Server.

For example: **`JMPDB`**

Important Non-ASCII characters are not supported.

6 Use the default values for the `Initial size` and `Autogrowth` parameters for the database and log files.

7 Click **OK**.

SQL Server Management Studio adds your database to the **Databases** folder in the Object Explorer pane.

8 Exit Microsoft SQL Server Management Studio.

What to do next

Before you install JMP Server, create a SQL Server login for the JMP Server host. See Create a SQL Server Login for the JMP Server Host.

Create a SQL Server Login for the JMP Server Host

During the JMP Server installation, the installer accesses the SQL Server database that you created to store the information about the JMP Server services being installed. You must select the SQL Server login type that the JMP Server installer is to use.

To access the SQL Server database you created, select either a Windows authentication login or a SQL Server Authentication login. By default, the Windows authentication login is used. Before you run the JMP Server installer, ensure that the credentials exist for the SQL Server login type that you selected.

Use the following table to determine which tasks you must finish to create the SQL Server login that the JMP Server installer is to use.

Table 4-1. SQL Server Login Types

SQL Server Login Type	Use Task Details in Section
Windows authentication (default)	Create a SQL Server Windows Authentication Login for the JMP Server Host
SQL Server authentication	Create a SQL Server Authentication Login for the JMP Server Host

Create a SQL Server Windows Authentication Login for the JMP Server Host

You can specify the JMP Server installer to use a Windows authentication login when accessing the SQL Server database you created. Before you run the JMP Server installer, the credentials for that SQL Server login must exist for the JMP Server host on which you are installing JMP Server.

Users connected to the JMP Server host can access the JMP SQL Server database. However, you must also ensure that the Windows Server user account that is used to install JMP Server has write access to the SQL Server database that you created for JMP Server. See Granting Database Owner and System Administration Permissions for Windows User

Prerequisites

Ensure that you have created the SQL Server database for your JMP Server instance. To create the database, see Create a SQL Server Database for JMP Server.

Procedure

1. Log in to a SQL Server Management Studio session as the sysadmin (SA) or use a user account with SA privileges.
2. In the Object Explorer pane, expand the folder for the SQL server instance in which you created the database for your JMP Server instance.
3. Expand the **Security** folder, right-click **Logins**, and select **New Login.**
4. In the **Login - New** dialog box, on the **General** page, enter a login name in the format *domain_name**computer_name*$, where *computer_name* is the name of the JMP Server host and *domain_name* is the domain in which the host belongs.

   For example: **`mycompany\jmpserver$`**
5. Select **Windows authentication**.
6. From the **Default database** list, select a default database for the login. The master database is the default value for this item.
7. From the **Default language** list, select a default language to use for the login.
8. Assign a sysadmin Server role for the new login account.
   a. Click the **Server Roles** tab in the Select a Page pane on the left side.
   b. In the Server roles page, select the **sysadmin** check box.
9. Click **OK**.

The new login is added under the **Logins** folder in the Object Explorer pane.

What to do next

Create the SQL Server login credentials for the Windows Server user account that is used to install JMP Server. See Granting Database Owner and System Administration Permissions for Windows User.

Create a SQL Server Authentication Login for the JMP Server Host

You can specify the JMP Server installer to use a SQL Server login that uses SQL Server Authentication login to access the SQL Server database that you created. Before you run the JMP Server installer, the login credentials for that SQL Server login type must exist for the JMP Server host.

Prerequisites

Ensure that you have created the SQL Server database for JMP Server. To create the database, see Create a SQL Server Database for JMP Server.

Procedure

1. Log in to a SQL Server Management Studio session as the sysadmin (SA) or using a user account with SA privileges.
2. In the Object Explorer pane, expand the folder for the SQL server instance in which you created the JMP Server database.
3. Expand the **Security** folder, right-click **Logins**, and select **New Login.**
4. In the **Login - New** dialog box, on the **General** page, enter a value in the **Login name** text box using ASCII characters only. Alternatively, click **Search** and use the **Select User or Group** dialog box to locate the login you want to use.

   Important Non-ASCII characters are not supported.
5. Select **SQL Server authentication**.
6. In the **Password** and **Confirm Password** text boxes, enter a password for the new login name. Use ASCII characters only.
7. If you are changing an existing password, select **Specify old password**, and then enter the old password in the **Old password** text box.
8. Depending on your organization's policy, select or deselect the **Enforce password policy**, **Enforce password expiration**, and **User must change password at next login** check boxes.
9. From the **Default database** list, select a default database for the login. The master database is the default value for this item.
10. From the **Default language** list, select a default language for the login.
11. Assign a sysadmin Server role for the new login account.
    a. Click the **Server Roles** tab in the Select a Page pane on the left side.
    b. In the Server roles page, select the **sysadmin** check box.
12. Click **OK**.

The new login is added under the **Logins** folder in the Object Explorer pane.

What to do next

Create the SQL Server login credentials for the Windows Server user account that is used to install JMP Server. See Granting Database Owner and System Administration Permissions for Windows User.

Granting Database Owner and System Administration Permissions for Windows User

Besides creating a SQL Server login for the JMP Server host machine, the Windows user account that you plan to use to install the JMP Server instance must be created. This Windows user account must be given sysadmin and database owner privileges in the SQL Server database that you created.

Prerequisites

- Ensure that the SQL Server database has been created for the JMP Server you plan to install. See Create a SQL Server Database for JMP Server.
- Verify that SQL Server login has been created for the JMP Server host. See Create a SQL Server Login for the JMP Server Host.

Procedure

1. Log in to a SQL Server Management Studio session as the sysadmin (SA) or use a user account with SA privileges.
2. In the Object Explorer pane, connect to the SQL server instance that you created for the JMP Server.
3. Create the SQL Server Login for the Windows user account you plan to use for installing the JMP Server.
   a. Expand the **Security** folder, right-click **Logins**, and select **New Login.**
   b. In the **Login - New** dialog box, click **Search**.
   c. In the **Select User or Group** dialog box, select the valid Active Directory user that you plan to use to install JMP Server.
   d. In the Login - New dialog box, under Select a Page, choose **Server Roles** and select the **sysadmin** check box.
   e. Click **OK** to close the **Login-New** dialog box.
4. Grant permissions to the Windows user account.
   a. In the left pane, click **Databases**.
   b. Select the database you created for your JMP Server instance, click **Security**, and then click **Users**
   c. In the Users pane, right-click your Windows user login, and select **Properties** from the contextual menu.
   d. Under Database role membership, select **db_owner** role.
   e. Click **OK**.

The new login is added under the **Logins** folder in the Object Explorer pane.

What to do next

Install the JMP Server instance using the information in Install JMP Server.

Installing JMP Server

5

To use the JMP Integrated Workflow features, you must first install and configure JMP Server and the required VMware JMP technology products.

Note In Horizon 7 version 7.5 release, you can install only one instance of JMP Server.

This chapter includes the following topics:

Install JMP Server

Before you can use the JMP Integrated Workflow features, you must install and configure JMP Server.

The JMP Server installer file is included when you download VMware Horizon 7 version 7.5 or later. You must run the JMP Server installer separately after you successfully install Horizon 7 version 7.5 or later.

Prerequisites

- Confirm that you have met the system requirements for the components that are required to install JMP Server. See Chapter 3 System Requirements For JMP Server.
- To run the JMP Server installer on a Windows Server host, you must use a domain user account with administrative privileges on that host system.
- Ensure that the SQL Server database that your JMP Server instance must use has been created and that you have the appropriate access to it.
- Verify that the SQL Server logins and permissions have been configured for the JMP Server host and Windows domain user account that you plan to use to install JMP Server. See Create a SQL Server Login for the JMP Server Host.
- Gather the information for the secure or insecure HTTP port, UI port, and signed certificates to be used with the JMP Integrated Workflow features.
- Obtain a TLS certificate signed by a Certificate Authority and use it to replace the default TLS certificate installed by the JMP Server installer.

- Before you install JMP Server, use the following table to determine the type of installation to use.

Installation Type	Action Taken by JMP Server Installer
Production Environment	Generates a JMP Server instance that uses SQL Server Standard or Enterprise edition.
Development or Proof of Concept (PoC) Environment	Generates a JMP Server instance that uses SQL Server Express.

- Add the following files to the McAfee Antivirus exclusion list before you install JMP Server.
  - `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`

Procedure

1. To start the **VMWare JMP Installer** wizard, locate and double-click the JMP Server installer file.

   The JMP Server installer filename is `VMware-Jmp-Installer-e.x.p-xxxxxxx.exe`, where *xxxxxxx* is the build number. For example, `VMware-Jmp-Installer-e.x.p-7259616.exe`.

   Note If you want to log the installation process, run the JMP Server installer from a command prompt using the following command, where *Log_Folder_Path* is the folder where the log file is to be created.

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

2. Click **Next** in the Welcome page and accept the VMware license terms.
3. To allow HTTPS traffic, click **Next**.

   Note JMP Server takes up port 443 and, optionally, ports 80, 3000–3004, 888, and 8889. To allow HTTP traffic over port 80, select the **Allow HTTP?** check box.

4. Provide the SQL Server instance and database catalog information.
   a. Enter the IP Address or the name of the SQL Server instance for connecting to the database you created for JMP Server. Optionally, click **Browse** to make the selection.
   b. Select which authentication credentials you want to use to connect to the SQL Server database.

Option	Description
Windows authentication credentials of current user	The administrator credentials you are using during this installation process is used to connect to the SQL Server database instance.
Server authentication using the Login ID and password below	Provide the **Login ID** and **Password** information to use to connect to the SQL Server database instance.

   Note The login credentials you use must already be configured in the SQL Server instance that JMP Server is going to access. See Create a SQL Server Login for the JMP Server Host.

c In the **Name of database catalog** text box, enter the name of the database you created using Create a SQL Server Database for JMP Server. Optionally, click **Browse** and select the database catalog from the available list.

The selected database catalog is used to store information about the JMP Server services.

d (Optional) If you want to overwrite the existing database, select the **Overwrite existing database** check box.

Note The first time the JMP Server installer is run, the necessary database tables are created. If you run the installer again to create more JMP Server instances for load balancing, the installer finds that the database already exists and does not recreate the tables. Selecting this option overwrites the existing information in the database.

e To ensure a secure communication between JMP Server and the SQL Server instance, verify that the **Enable SSL** check box is selected. The **Enable SSL** check box is selected by default.

Important When the **Enable SSL** check box is selected, ensure that the TLS/SSL certificate used in SQL Server is imported into the Windows local certificate store on the JMP Server host. Otherwise, the JMP Server installation process fails with the error "Failed to execute `uem_migrate.bat` file" and when you click **OK** in the error dialog box, installation is rolled back.

See the "Enable encryption for a specific client" section in the Microsoft TechNet article How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console for details on exporting and importing the SQL Server's TLS/SSL certificate.

f Click **Next**.

5 In the **Ready to Install Program** page, click **Install**.

6 Click **Finish** when the installation finishes successfully.

With a successful installation, the following JMP Server services are installed and started on your Windows Server host.

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

What to do next

Synchronize the time between the newly installed JMP Server instance and its associated Horizon Connection Server. See Synchronize Time Between Horizon Connection Server and JMP Server Hosts.

Uninstall JMP Server

You might need to uninstall and reinstall JMP Server to resolve a problem.

This procedure describes how to uninstall JMP Server if you encounter problems that cannot be resolved with other methods.

Prerequisites

- Verify that you have the correct administrative privileges to uninstall JMP Server.
- Before uninstalling a JMP Server, delete all User Environment Manager configuration shares that are associated with that JMP Server. See "Delete User Environment Manager Configuration Share Information" in *VMware Horizon Console Administration*.

Procedure

1. Open the Microsoft Windows Program and Features console.

   For example, click **Start > Settings > System > Apps and Features**.
2. Select **VMware JMP** from the list of installed applications.
3. To finish the uninstallation steps, click **Uninstall** and follow the wizard.

What to do next

Reinstall JMP Server. See the Install JMP Server document for details.

Configuring the JMP Server Instance

6

After successfully installing the JMP Server instance, you must perform configuration tasks to ensure the JMP Server instance can successfully authenticate with Horizon Connection Server and can communicate securely with other servers in your network.

This chapter includes the following topics:

Synchronize Time Between Horizon Connection Server and JMP Server Hosts

The time in both the Horizon Connection Server and JMP Server hosts must be synchronized in order for the authentication process between the two servers to be successful.

When you access the JMP Integrated Workflow features using the Horizon Console UI, JMP Server authenticates the token it receives from Horizon Connection Server, which in turn returns a token to JMP Server. If time is unsynchronized between the two hosts, the Horizon Connection Server rejects the token provided by JMP Server, and the JMP Integrated Workflow features become unavailable from the Horizon Console UI. The JMP Setting pane displays the following error message.

```
Horizon SSO token could not be verified.
```

For a successful authentication process, synchronize time on the Horizon Connection Server and JMP Server hosts to a common Network Time Protocol (NTP) Server.

Procedure

1 Use the following VMware Tool commands on the Windows host.

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

2 On the ESXi host, synchronize ESXi Clocks with a Network Time Server.

   a Start the VMware Host Client, and connect to the ESXi host.

   b Click **Configure**.

c Under **System**, click **Time Configuration**, and click **Edit**.

d Select **Use Network Time Protocol (Enable NTP client)**.

e In the Add NTP Server text box, enter the IP address or fully qualified domain name of one or more NTP servers to synchronize with.

What to do next

Configure the TLS certificates for JMP Server. See Overview of Tasks for Setting Up TLS Certificates for JMP Server.

Configuring TLS Certificates and Cipher Suites for JMP Server

To ensure that your JMP Server instance communicates securely with other servers in your network, you must configure your JMP Server instance to use TLS certificates that a valid Certificate Authority (CA) signed. To enhance the secure connections, you can also optionally change the default cipher suites that other servers accept and propose when communicating with your JMP Server instance.

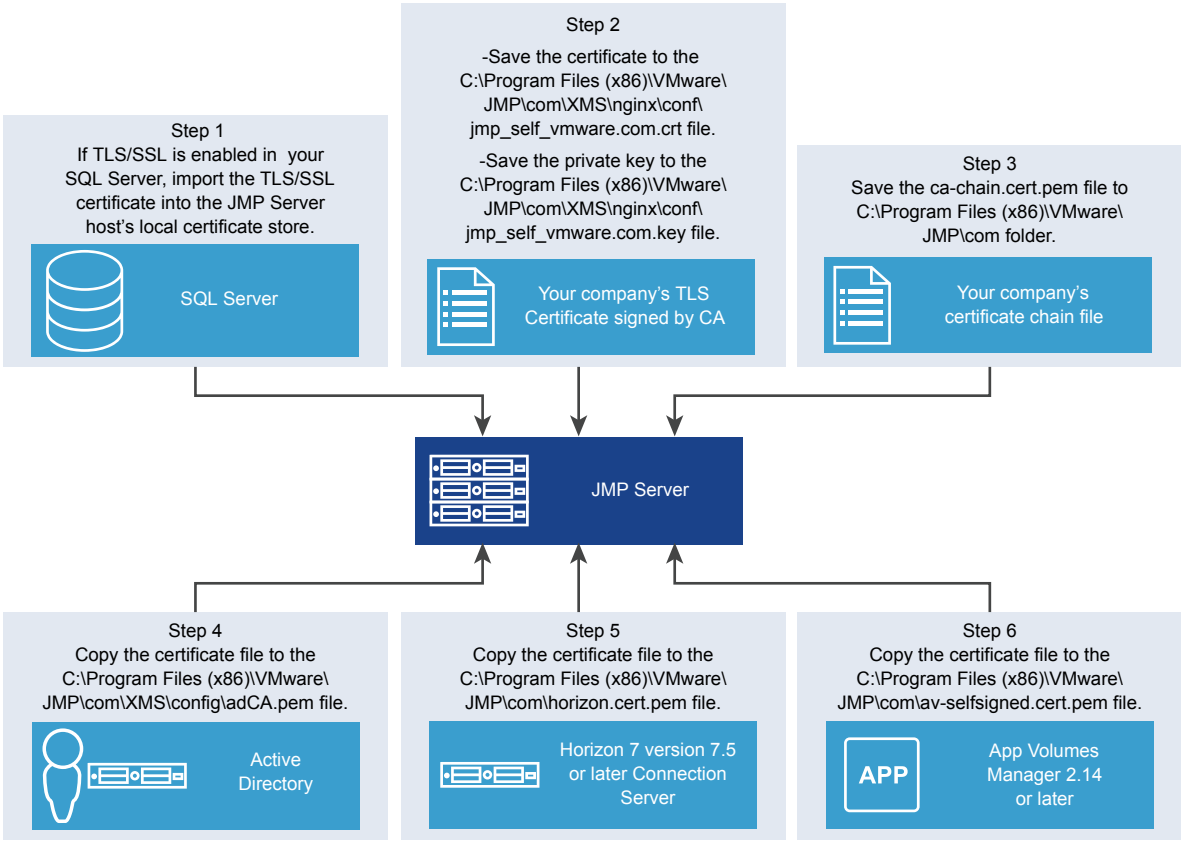
By default, the JMP Server installer installs a self-signed TLS server certificate for the JMP Server instance you installed. You can use the default certificate for testing purposes. If you are using the JMP Server instance in a production environment, you must replace the default certificate with a CA-signed TLS server certificate as soon as possible. Use of certificates that a CA did not sign can allow untrusted parties to intercept traffic by masquerading as your server. See Overview of Tasks for Setting Up TLS Certificates for JMP Server.

Overview of Tasks for Setting Up TLS Certificates for JMP Server

After successfully installing JMP Server, you must perform several tasks to set up the TLS server certificates that are signed by a valid Certificate Authority (CA) for use with the JMP Server instance.

In addition to the tasks outlined in this topic, the following diagram provides a visual summary of the main steps required to configure the certificates for JMP Server. Ensure that you follow the detailed steps that are described in the topics that follow this overview to configure the specific certificates successfully. For the tasks that are marked as optional, determine whether you have to perform those tasks to ensure your JMP Server configuration is more secure. After you complete the certificate configurations, you must restart the three JMP Server services using the Windows Services Manager.

Figure 6-1. Main Steps to Configure the Certificates for JMP Server



1 If TLS/SSL is enabled in your SQL Server, ensure that the TLS/SSL certificate has been imported into the JMP Server's host's local certificate store.

2 Replace the TLS server certificate that the JMP Server installer generated.

   The default server certificate that the JMP Server installer generated is self-signed and unrecognized by your organization's network. Replace the self-signed certificate with a valid TLS certificate that you obtained from a CA. See Replace the Default TLS Certificate.

   If your organization does not have a valid TLS Web server certificate, obtain a signed TLS server certificate from a CA. Refer to the information in *Scenarios for Setting Up TLS Certificates for Horizon 7*.

3 If an intermediate CA signed your organization's server certificates, configure JMP Server to use your organization's certificate chain file, `ca-chain.cert.pem`, to help JMP Server authenticate other servers in your network. See Configure JMP Server to Use a Certificate Chain File.

   Note If a root CA trusted by NodeJS signed your organization's TLS server certificates directly, you do not need to provide a certificate chain file or the root certificate file, `ca.cert.pem`.

4 Obtain the CA certificate which is used to sign the certificate for the Active Directory server, store it into `adCA.pem` file, and add the file into the JMP Server XMS configuration folder. See Configure JMP Server to Use the Certificate for Active Directory for details.

5 Export the CA-signed certificate for Horizon Connection Server into a `horizon.cert.pem` file and add the file into the JMP Server home folder. See Configure JMP Server to Use the Horizon Connection Server Certificate for details.

   With the `horizon.cert.pem` file, JMP Server can authenticate Connection Server as a trustworthy server to which it can connect.

   Note You must finish this task for each Connection Server pod that interfaces with the JMP Server instance. The contents of each of the exported CA-signed certificate must be appended into the same `horizon.cert.pem` file.

6 If you are assigning App Volumes AppStacks when creating JMP assignments, configure your JMP Server instance to use the App Volumes Manager instance's self-signed certificate so that it can securely communicate with the App Volumes Manager instance. See Configure JMP Server to Use the App Volumes Manager Self-Signed Certificate.

7 (Optional) Change the default cipher suites that your JMP Server instance supports with ciphers that your organization supports. See Configuring Cipher Suites for JMP Server.

8 (Optional) Enable a more restrictive Cross-Origin Resource Sharing (CORS) policy on your JMP Server for an added secure communication with your Horizon 7 Connection Server instance. See Use a More Restrictive CORS Policy on Your JMP Server.

9 Restart the three JMP Server services using the Windows Services Manager.

After you configure the server certificates, you can proceed to Horizon Console to configure the JMP settings and begin using the JMP Integrated Workflow features. See "Configure JMP Settings for the First Time" in *VMware Horizon Console Administration*.

Replace the Default TLS Certificate

Replace the default TLS certificate installed by the JMP Server installer with your organization's TLS certificate that is signed by a Certificate Authority (CA).

After you successfully install the JMP Server instance, you can access it using the Horizon Console on a Web browser. However, if your network does not recognize the default TLS certificate that was installed, the Web browser's security alert dialog box appears when you configure the JMP settings for the first time. Although you can use the default, self-signed certificate for testing purposes, to ensure a secure connection with the JMP Server instance, replace the default certificate and key with a CA-signed TLS certificate and private key.

Important If you decide to name the certificate and key files with filenames that are different from the default names created by the JMP Server installer, you must modify the JMP Server NGINX configuration file to use the new filenames.

Prerequisites

- Install JMP Server. See Install JMP Server.

- Obtain a CA-signed TLS certificate and replace the default TLS certificate installed by the JMP Server installer. You can use certificate tools, such as Microsoft Certreq or OpenSSL on Windows, to generate a certificate. Refer to information in "Obtaining TLS Certificates from a Certificate Authority" in *Scenarios for Setting Up TLS Certificates for Horizon 7*.

Procedure

1. In the JMP Server host, stop the three JMP Server services using the Windows Services Manager tool.
   a. Right-click the Windows **Start** icon and select **Run**.
   b. In the Run dialog box, type `services.msc` in the **Open** text box, and click **OK**.
   c. Locate the following three JMP Server services in the Services (Local) pane of the Services window and for each service, click **Stop**.
      - `VMware JMP API Service`
      - `VMware JMP File Share Service`
      - `VMware JMP Platform Services`
2. Save your CA-signed TLS server certificate file as `jmp_self_vmware.com.crt` in the NGINX configuration folder on the JMP Server host.

   For example: `C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\jmp_self_vmware.com.crt`
3. Save the CA-signed TLS server certificate's accompanying private key as `jmp_self_vmware.com.key`.

   For example: `C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\jmp_self_vmware.com.key`
4. (Optional) If you want to use filenames that are different from the expected certificate filenames, `jmp_self_vmware.com.crt` or `jmp_self_vmware.com.key`, you must modify the NGINX configuration file with the new filenames.
   a. Open the `C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\nginx.conf` configuration file.
   b. Locate the occurrences of the `jmp_self_vmware.com.crt` and `jmp_self_vmware.com.key` properties and replace them with the new filenames you had selected.
   c. Save the `nginx.conf` file.

You can now securely access the JMP Integrated Workflow features without the Web browser security alert dialog box appearing.

What to do next

If an intermediate CA signed your organization's entire certificate chain, configure your JMP Server instance to use a certificate chain file. See Configure JMP Server to Use a Certificate Chain File. If not, proceed to configure your JMP Server instance to use the certificate for Active Directory. See Configure JMP Server to Use the Certificate for Active Directory.

Configure JMP Server to Use a Certificate Chain File

If an intermediate CA signed your organization servers' certificates, configure the JMP Server instance with your organization's entire certificate chain, which includes the root and intermediate certificates.

Prerequisites

- Use Windows Services Manager to stop the three JMP Server services.

Procedure

1. Obtain your organization's entire certificate chain file, `ca-chain.cert.pem`.
2. Copy the `ca-chain.cert.pem` certificate chain file into the `C:\Program Files (x86)\VMware\JMP\com` folder.

With the certificate chain in place, your JMP Server instance can authenticate the Horizon 7 and App Volumes instances and securely communicate with them.

What to do next

Configure the JMP Server instance with the Active Directory certificate so that the JMP Server instance can authenticate the Active Directory server when desktop administrators use the JMP Integrated Workflow features. See Configure JMP Server to Use the Certificate for Active Directory.

Configure JMP Server to Use the Certificate for Active Directory

For JMP Server to validate the Active Directory with which Horizon Console is connected, you must configure JMP Server to use the certificate for that Active Directory server.

You must export the root CA certificate of the Active Directory domain into a certificate file named `adCA.pem` file and place this file in the JMP Server XMS configuration folder.

Prerequisites

- JMP Server must be installed.
- Active Directory must be configured for LDAP over SSL (LDAPS) or StartTLS (LDAP over TLS).

- Root CA certificates of the Active Directory domains. If the certificates are not in PEM (Base64 encoded) format, see the OpenSSL documentation (or a similar document) to convert the file to a PEM format.

  Note When you have multiple root certificates from different domains, you can combine all the PEM formatted certificates into a single file by copying the contents of each file one by one to a single `.pem` file.

Procedure

1. Ensure that name of the PEM formatted certificate file is `adCA.pem`.
2. Copy the `adCA.pem` file to the JMP Server XMS configuration folder.

   For example: `C:\Program Files (x86)\VMware\JMP\com\XMS\config\adCA.pem`.

With the Active Directory certificate configured for your JMP Server instance, the Active Directory is recognized as a trusted server and Horizon Console users can successfully use the JMP Integrated Workflow features.

What to do next

Configure JMP Server with the Connection Server certificate so that JMP Server instance can authenticate Connection Server when desktop administrators use the JMP Integrated Workflow features. See Configure JMP Server to Use the Horizon Connection Server Certificate.

Configure JMP Server to Use the Horizon Connection Server Certificate

For JMP Server to validate the Horizon 7 Connection Server to which Horizon Console is connected, you must configure JMP Server to use the Horizon 7 Connection Server certificate.

You must export the Horizon 7 Connection Server certificate into a certificate file named `horizon.cert.pem` file and place this file in the JMP Server home folder.

Important The contents of each of the exported CA-signed certificates must be appended into the same `horizon.cert.pem` file.

Use these same procedures when adding a CA-signed or self-signed Horizon 7 Connection Server certificate.

Prerequisites

- JMP Server must be installed.
- You must have administrative access to Horizon 7 Connection Server.

Procedure

1. Log in to the Windows Server host for the Horizon 7 Connection Server that interfaces with the Horizon Console and the JMP Server you installed.

2 Right-click the Windows **Start** icon, select **Run**, and type `mmc.exe`.

   The MMC utility window appears.

3 Add the Certificates snap-in.

   a In the **Console Root** window, select **File > Add/Remove Snap-in**.

   b In the **Add or Remove Snap-ins** window, select **Certificates** from the Available snap-ins pane, and click **Add**.

   c After the certificates have been added, click **OK**.

   d In the Certificates snap-in window, select **Computer account** and click **Next**.

   e In the Select Computer window, select **Local computer** and click **Finish**.

      The Certificates (Local Computer) snap-in is added in the Selected snap-ins pane.

   f Click **OK** to close the **Add or Remove Snap-ins** dialog box.

4 Back in the Console Root window, select **Console Root > Certificates (Local Computer)** and select the **Personal > Certificates** folder on the left pane to display its contents.

5 Export the Horizon Connection Server certificate.

   a In the certificates content pane, locate the certificate with a Friendly Name of **`vdm`**.

      This certificate belongs to the Horizon Connection Server.

   b Right-click the certificate and select **All Tasks > Export**.

   c In the Certificate Export Wizard dialog box, click **Next**.

   d Select **No, do not export the private key**, and click **Next**.

   e Select the **Base-64 encode X.509 (.CER)** format and click **Next**.

   f Enter the filename as **`horizon.cert.pem`** and click **Browse** to navigate to the folder where you want to save the exported certificate.

      Important You must save the exported certificate file with the `.pem` file extension, and **not** with the `.cer` or `.crt` file extensions. If necessary, open the exported certificate file in a text editor and save it as `horizon.cert.pem`.

   g Click **Next** and click **Finish** to close the **Certificate Export Wizard** window.

   The certificate is exported successfully.

6 Navigate to where you saved the exported `horizon.cert.pem` certificate and copy it to the JMP Server home folder.

   For example: `C:\Program Files (x86)\VMware\JMP\com\horizon.cert.pem`.

With the Connection Server certificate configured for JMP Server, the Connection Server is recognized as a trusted server and Horizon Console users can successfully use the JMP Integrated Workflow features.

What to do next

Review the optional tasks listed in Overview of Tasks for Setting Up TLS Certificates for JMP Server and determine if you must also complete them. If you have finished all the necessary configuration tasks, restart the JMP Server services and configure the JMP settings. See "Configure JMP Settings for the First Time" in *VMware Horizon Console Administration* for more information.

Configure JMP Server to Use the App Volumes Manager Self-Signed Certificate

If you are assigning App Volumes AppStacks when creating JMP assignments, configure your JMP Server instance to use the App Volumes Manager instance's self-signed certificate so that it can securely communicate with the App Volumes Manager instance.

You must export the self-signed certificate of the App Volumes Manager instance into a certificate file named `av-selfsigned.cert.pem` file in order for JMP Server to use it.

Prerequisites

- JMP Server must be installed.
- You must have administrative access to the App Volumes Manager instance or the load balancer that manages it.

Procedure

1. From your JMP Server host, use a Web browser to log in to the App Volumes Manager instance or the load balancer that manages the App Volumes Manager instances in your environment.
2. To locate the self-signed certificate information that is used by the App Volumes Manager instance or load balancer, use your Web browser's site information dialog box and export the self-signed certificate file and save it to the `C:\Program Files (x86)\VMware\JMP\com\av-selfsigned.cert.pem` file.

   Important You must save the exported certificate file with the `.pem` file extension, and **not** with the `.cer` or `.crt` file extensions. If necessary, open the exported certificate file in a text editor and save it as `av-selfsigned.cert.pem`.

   For example, when using a Google Chrome Web browser, use the Certificate Export Wizard to copy the App Volumes Manager self-signed certificate file into the `av-selfsigned.cert.pem` file in the `C:\Program Files (x86)\VMware\JMP\com` folder.
3. If you have finished all the tasks necessary to configure the TLS certificates necessary to make JMP Server more secure, restart the JMP Server services. See Overview of Tasks for Setting Up TLS Certificates for JMP Server to review any remaining TLS certificate configuration tasks.

Configuring Cipher Suites for JMP Server

TheJMP Server installation includes default cipher suites that are accepted and proposed between JMP Server, Horizon Connection Server, App Volumes, and User Environment Manager instances. You can optionally change these default cipher suites that JMP Server supports with ciphers that your organization supports.

You must specify the list of ciphers using the format that is defined in https://www.openssl.org/docs/man1.0.2/apps/ciphers.html#CIPHER-LIST-FORMAT. The following cipher list is the default.

```
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
```

Procedure

1. In the JMP Server host, stop the three JMP Server services using the Windows Services Manager tool.
   a. Right-click the Windows **Start** icon and select **Run**.
   b. In the Run dialog box, type `services.msc` in the **Open** text box, and click **OK**.
   c. In the Services (Local) pane of the Services window, locate the following three JMP Server services and for each service, click **Stop**.
      - `VMware JMP API Service`
      - `VMware JMP File Share Service`
      - `VMware JMP Platform Services`
2. Navigate to the `C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf` folder.
3. Create a backup copy of the `nginx.conf` file before modifying it.
4. Open the `nginx.conf` file with Notepad.
5. Locate the line that begins with `ssl_ciphers` and modify the cipher list as necessary.
6. Save the changes you made to the `nginx.conf` file.
7. Use the Windows Services Manager tool to restart the three JMP Server services for the new cipher suites list to take effect.

Use a More Restrictive CORS Policy on Your JMP Server

You can use a more restrictive Cross-Origin Resource Sharing (CORS) policy on your JMP Server instance by creating a whitelist of the Horizon 7 Connection Server instances that are trusted to access your JMP Server.

By default, a Horizon 7 Connection Server can access your JMP Server instance if it is using the same certificate that is in the certificate chain file that you configured using Configure JMP Server to Use a Certificate Chain File. To ensure that only the approved list of Horizon 7 Connection Server instances have access to your JMP Server, perform the following steps.

Procedure

1. Using a text editor, open the NGINX configuration file at `C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\nginx.conf`.
2. Locate the two occurrences of the following text and uncomment each one by removing the leading # mark so that they appear as follows.

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

3. Locate the two occurrences of the following text and comment them out by adding a leading # mark so that they appear as follows.

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

4. Add the approved list of Connection Server instances to the whitelist.
   a. Locate the following content in the file.

   ```
   # 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. After the `default '';` line, add a line for each Connection Server instance you want to include in the whitelist.

   For example, if the domain names of the Connection Server instances that are allowed to connect to your JMP Server are `www.testhorizon.com` and `www.prodhorizon.com`, then the lines to add are shown in bold in the following example.

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

5. Save the changes you made to the `nginx.conf` file.
6. Restart the JMP Platform Services using the Windows Services Manager.

Updating the Database Password After JMP Server Installation

7

If you modify the SQL Server database password that was used during the initial JMP Server installation, you must also update the database password information used by the VMware JMP Server services.

This chapter includes the following topics:

Update the Database Password for VMware JMP Platform Services

If you modify the SQL Server database password that was used when JMP Server was installed, you must also update the database password that is used by the VMware JMP Platform Services to connect to your SQL Server database.

Prerequisites

Verify that you have the correct administrative privileges to change the database information in the JMP Server host.

Procedure

1. In the JMP Server host, stop the `VMware JMP Platform Services` process using the Windows Services Manager tool.
   a. Right-click the Windows **Start** icon and select **Run**.
   b. In the Run dialog box, type `services.msc` in the **Open** text box, and click **OK**.
   c. Locate `VMware JMP Platform Services` in the Services (Local) pane of the Services window and click **Stop**.
2. Open the **ODBC Data Source Administrator** window by double-clicking one of the following executable files that is appropriate for your JMP Server host.
   - `C:\Windows\SysWow64\odbcad64.exe`
   - `C:\Windows\system32\odbcad32.exe`

3 In the ODBC Data Source Administrator window, click **System DSN** and select the **svmanager** in the User Data Sources pane.

4 Click **Configure**.

The Microsoft SQL Server DSN Configuration wizard appears.

5 Click **Next**.

Caution Do not change the existing information in the data source **Name** or **Server** text boxes.

6 Ensure that the **With SQL Server authentication using a login ID and password entered by the user** is selected.

7 Enter a new password in the **Password** text box and click **Next**.

8 Click **Next** again, without changing to the existing information in the default database info page.

9 Click **Finish**.

The ODBC Microsoft SQL Server Setup summary window appears with the configuration details.

10 Review the information summary and click **OK** to proceed with the password modification for the `VMware JMP Platform Services` service.

11 Add the new password information to the VMware JMP Platform Services database configuration file before restarting the `VMware JMP Platform Services` service.

a Using a text editor as an administrator, open the database configuration file at `C:\Program Files (x86)\VMware\JMP\com\XMS\config\database.yml`.

b Locate the line for the username property and insert a new line after that line for the password property.

c Enter the information for the password you created so that it appears as shown in the following example.

```
password: new_password
```

Important This password information is automatically removed from the `database.yml` file after the `VMware JMP Platform Services` service is restarted.

12 Restart the `VMware JMP Platform Services` service.

a Right-click the Windows **Start** icon and select **Run**.

b In the Run dialog box, type `services.msc` in the **Open** text box, and click **OK**.

c Locate `VMware JMP Platform Services` in the Services (Local) pane of the Services window and click **Start**.

What to do next

If you have not already done so, you must also update the database login account information used by the VMware JMP File Share Service. See Update Database Password for VMware JMP File Share Service.

Update Database Password for VMware JMP File Share Service

If you modify the SQL Server database password that was used when JMP Server was installed, you must also update the database password that is used by the VMware JMP File Share Service to connect to the SQL Server database.

Prerequisites

Verify that you have the correct administrative privileges to change the database information in the JMP Server host.

Procedure

1. In the JMP Server host, stop the `VMware JMP File Share Service` process using the Windows Services Manager tool.
   a. Right-click the Windows **Start** icon and select **Run**.
   b. In the Run dialog box, type `services.msc` in the **Open** text box, and click **OK**.
   c. Locate `VMware JMP File Share Service` in the Services (Local) pane of the Services window and click **Stop**.
2. Update the password used by the VMware JMP File Share Service. Use the following information to determine the steps to use depending on the type of SQL Server connection that used during the JMP Server installation.
   - For the SQL Authentication connection mode:
     1. Open a command prompt window as an administrator.
     2. Copy the following commands and modify the <password> information with the new password value.

```
SET NODE_ENV=jmp.production
cd C:/Program Files (x86)/VMware/JMP/com/uem
call "../../nodev8/npm" run-script migrate --silent --scripts-prepend-node-path=auto -- --
db="{\"password\":\"<password>\"}"
```

     3. Paste the commands to the command prompt window and press Enter.
   - For the Windows Authentication connection mode:
     1. Navigate to the `C:/Program Files (x86)/VMware/JMP/com/uem` folder and open the `db.json` file in a text editor.

2. Replace the existing file contents with the following content, where <IP address> is the IP address for the SQL Server host and the <Database name> is the valid database name.

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

3. Save the file.

3. Restart the `VMware JMP File Share Service`.
   a. Right-click the Windows **Start** icon and select **Run**.
   b. In the Run dialog box, type `services.msc` in the **Open** text box, and click **OK**.
   c. Locate `VMware JMP File Share Service` in the Services (Local) pane of the Services window and click **Start**.

What to do next

If you have not already done so, you must also update the database login account information used by the VMware JMP Platform Services. See Update the Database Password for VMware JMP Platform Services.

Troubleshooting Your JMP Server

8

You might encounter error messages when installing, configuring, and registering your JMP Server instance. You can use the troubleshooting information in this chapter.

JMP Server Is Unavailable Error

You are unavailable to connect to your JMP Server instance.

Problem

While using Horizon Console to register your JMP Server instance, you might see the error message `The JMP Server you entered is unavailable. Modify your entry or try again later.`

Cause

The error message appears for one of multiple possible reasons. To determine the cause and the workaround, use the information in the following section.

Solution

1 Ensure that the certificates are configured correctly.

Use the information in Configuring TLS Certificates and Cipher Suites for JMP Server.

2 After you tried to register the JMP Server URL, review the HTTP response from the Web browser.

If you received an HTTP response similar to the following output,

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

use the following steps to verify that the user account that you used to log into Horizon Console has the sufficient administrator privileges.

a In Horizon Administrator, select **View Configuration > Administrators**.

b In the Administrator pane, verify that your Administrator user account appears as <*domain-name*>\Administrator (not as BUILTIN\Administrator) and that it is assigned full administrator privileges.

c If you see BUILTIN\Administrator, apply the workaround described in the Release Notes for VMware Horizon 7 version 7.5.

For information about managing administrator permissions, see "Manage and Review Permissions" in the *Horizon 7 Administration* document.

3 If there are JSON Web Token (JWT) messages in the Web browser's HTTP response that are similar to the following error message `{"code":403,"error":"Error: Unable to verify Horizon JWT","error_code":"1044","error_type":"horizonJwtVerificationError"}`, ensure that the times between your JMP Server host and Horizon Connection Server host are synchronized.

Use the information provided in Synchronize Time Between Horizon Connection Server and JMP Server Hosts.