

VMware Horizon JMP Server Installations- und Einrichtungshandbuch

DEZ 2019

VMware Horizon 7 7.11



vmware®

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2018–2019 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

1	VMware Horizon JMP Server Installations- und Einrichtungshandbuch	5
2	Übersicht der Aufgaben zum Installieren und Konfigurieren von JMP Server	6
3	Systemanforderungen für JMP Server	8
	Erforderliche JMP-Technologiekomponenten	8
	Hardwareanforderungen für JMP Server	9
	Unterstütztes Betriebssystem für JMP Server	9
	Netzwerkanforderungen für JMP Server	9
	Datenbankanforderungen für JMP Server	10
	Unterstützter Webbrowser für JMP Integrated Workflow	11
4	Vorbereiten der SQL Server-Datenbank und -Anmeldung für JMP Server	12
	Erstellen einer SQL Server Datenbank für JMP Server	12
	Erstellen der SQL Server-Anmeldung für den JMP Server-Host	13
	Erstellen einer SQL Server-Anmeldung zur Windows-Authentifizierung für den JMP Server-Host	14
	Erstellen der Anmeldedaten zur SQL Server-Authentifizierung für den JMP Server-Host	15
	Gewähren von Datenbankbesitzer- und Systemverwaltungs-Berechtigungen für Windows-Benutzer	16
5	Installation und Upgrade von JMP Server	18
	Installieren von JMP Server	19
	JMP Server upgraden	22
6	Konfigurieren der JMP Server-Instanz	23
	Synchronisieren der Uhrzeit zwischen dem Horizon-Verbindungsserver und den JMP Server-Hosts	23
	Konfigurieren von TLS-Zertifikaten und Verschlüsselungssammlungen für JMP Server	24
	Überblick über Aufgaben zur Einrichtung von TLS-Zertifikaten für JMP Server	24
	Ersetzen des standardmäßigen TLS-Zertifikats	27
	Konfigurieren von JMP Server zur Verwendung einer Zertifikatskettendatei	28
	Konfigurieren des JMP-Servers zur Verwendung des Zertifikats für Active Directory	29
	Konfigurieren von JMP Server zur Verwendung des Horizon-Verbindungsserver-Zertifikats	30
	Konfigurieren des JMP Servers zur Verwendung des App Volumes Manager-Zertifikats	32
	Konfigurieren von Verschlüsselungssammlungen für JMP Server	33
	Verwenden einer restriktiveren CORS-Richtlinie auf Ihrem JMP Server	34
7	Aktualisieren des Datenbankkennworts nach der JMP Server-Installation	36

[Aktualisieren des Datenbankkennworts für VMware JMP-Plattform-Dienste](#) 36

[Aktualisieren des Datenbankkennworts für den VMware JMP-Dateifreigabe-Dienst](#) 38

8 Fehlerbehebung für Ihren JMP Server 40

[JMP Server ist nicht verfügbar \(Fehler\)](#) 40

[Fehler tritt nach Aktualisierung des Kennworts für Dienstkonto auf](#) 41

[Deinstallieren von JMP Server](#) 42

VMware Horizon JMP Server Installations- und Einrichtungshandbuch

1

VMware Horizon JMP Server Installations- und Einrichtungshandbuch beschreibt die Installation und Konfiguration von VMware Horizon[®] Just-in-Time Management Platform (JMP) Server. Nach Installation von JMP Server und Konfiguration der Einstellungen von JMP können Sie mit der Definition der JMP-Zuweisungen beginnen und dazu die JMP Integrated Workflow-Funktionen in VMware Horizon Console verwenden.

Die Informationen in diesem Dokument sind für Benutzer gedacht, die JMP Server installieren möchten. Sie sind für erfahrene Windows-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und Vorgängen in Datencentern vertraut sind.

Übersicht der Aufgaben zum Installieren und Konfigurieren von JMP Server

2

Sie müssen vor und nach der Installation von HorizonJMP Server und vor der Arbeit mit den HorizonJMP Integrated Workflow-Funktionen bestimmte Aufgaben ausführen.

In der folgenden Liste finden Sie eine allgemeine Beschreibung der Aufgaben, die Sie ausführen müssen. Die Verfahren für die Durchführung dieser Aufgaben werden in den Themen nach dieser Übersicht beschrieben.

- 1 Vergewissern Sie sich, dass die JMP Server-Systemanforderungen erfüllt sind. Siehe [Kapitel 3 Systemanforderungen für JMP Server](#).
- 2 Erstellen Sie eine SQL-Serverdatenbank, die zum Speichern von Informationen zu den JMP Server-Diensten verwendet wird, die bei der Installation erstellt werden. Siehe [Erstellen einer SQL Server Datenbank für JMP Server](#).
- 3 Erstellen Sie die SQL Server-Anmeldung, die der JMP Server-Host zum Herstellen der Verbindung mit der im obigen Schritt erstellten SQL Server-Datenbank verwendet. Weitere Informationen finden Sie unter [Erstellen der SQL Server-Anmeldung für den JMP Server-Host](#).
- 4 Stellen Sie sicher, dass die Windows-Benutzeranmeldung, die zum Installieren von JMP Server verwendet wird, über genügend Rechte zum Ändern der SQL Server-Datenbank verfügt, die Sie zum Speichern der Informationen für die JMP Server-Dienste erstellt haben. Siehe [Gewähren von Datenbankbesitzer- und Systemverwaltungs-Berechtigungen für Windows-Benutzer](#).
- 5 (Optional) Wenn der im obigen Schritt verwendete SQL Server die TLS-Verschlüsselung verwendet, importieren Sie dessen TLS-Zertifikat im lokalen Windows-Zertifikatsspeicher auf dem JMP Server-Host. Weitere Details zum Exportieren und Importieren des TLS-Zertifikats des SQL Servers finden Sie im Abschnitt „Aktivieren der Verschlüsselung für einen spezifischen Client“ im Microsoft TechNet-Artikel [Aktivieren der SSL-Verschlüsselung für eine Instanz von SQL Server an der Microsoft-Verwaltungskonsole](#).
- 6 Installieren Sie JMP Server. Siehe [Installieren von JMP Server](#).
- 7 Synchronisieren Sie die Uhrzeit zwischen Ihrem Horizon Connection Server-Host und dem Windows-Host für Ihre JMP Server-Instanz. Siehe [Synchronisieren der Uhrzeit zwischen dem Horizon-Verbindungsserver und den JMP Server-Hosts](#).

- 8 Konfigurieren Sie die TLS-Zertifikate für Ihre JMP Server-Instanz zur sicheren Kommunikation mit den Instanzen des VMware Horizon 7-Verbindungsservers, VMware App Volumes™ Manager, VMware User Environment Manager™ und sonstigen Systemen im Netzwerk Ihrer Organisation. Siehe [Konfigurieren von TLS-Zertifikaten und Verschlüsselungssammlungen für JMP Server](#).
- 9 (Optional) Ändern Sie die standardmäßigen Verschlüsselungssammlungen, die Ihre JMP Server-Instanz unterstützt, zu den Verschlüsselungssammlungen, die Ihre Organisation unterstützt. Siehe [Konfigurieren von Verschlüsselungssammlungen für JMP Server](#).
- 10 (Optional) Verwenden Sie eine restriktivere Richtlinie zur Ressourcenfreigabe zwischen verschiedenen Ursprüngen (Cross-Origin Resource Sharing, CORS) für Ihre JMP Server-Instanz, um die Kommunikation mit Ihrer Horizon 7-Verbindungsserverinstanz sicherer zu machen. Siehe [Verwenden einer restriktiveren CORS-Richtlinie auf Ihrem JMP Server](#).
- 11 Starten Sie mit dem Windows Systems Manager die JMP Server-Dienste neu, bevor Sie die JMP-Einstellungen konfigurieren. Weitere Informationen hierzu finden Sie unter „Erstmaliges Konfigurieren der JMP-Einstellungen“ im Dokument *Verwaltung der VMware Horizon Console*.

Systemanforderungen für JMP Server

3

Vor Installation von VMware HorizonJMP Server und Verwendung der JMP Integrated Workflow-Funktionen müssen bestimmte Hardware- und Softwareanforderungen erfüllt sein.

Dieses Kapitel enthält die folgenden Themen:

- [Erforderliche JMP-Technologiekomponenten](#)
- [Hardwareanforderungen für JMP Server](#)
- [Unterstütztes Betriebssystem für JMP Server](#)
- [Netzwerkanforderungen für JMP Server](#)
- [Datenbankanforderungen für JMP Server](#)
- [Unterstützter Webbrowser für JMP Integrated Workflow](#)

Erforderliche JMP-Technologiekomponenten

Um JMP Server erfolgreich zu installieren, müssen Sie mindestens eine unterstützte Version des Horizon 7-Servers bereits installiert haben.

Um alle verfügbaren JMP Integrated Workflow-Funktionen wie die Verwaltung der Anwendungsbereitstellung und die kontextbezogene Richtlinienverwaltung zu verwenden, müssen Sie außerdem zusätzliche VMware-Produkte mit JMP-Technologie installieren. Sie können diese zusätzlichen Produkte vor oder nach der Installation von JMP Server installieren. Wenn Sie sie nach der Installation von JMP Server installieren, müssen Sie JMP Server mit Horizon Console neu konfigurieren.

Im Folgenden sind die unterstützten Versionen der VMware-Produkte mit JMP-Technologie aufgeführt.

- VMware Horizon 7 7.5 oder höher (Mindestanforderung für JMP Server-Installation)
- VMware App Volumes 2.xx, Version 2.14 oder höher (für Anwendungsbereitstellungsmanagement in Echtzeit). App Volumes 4.0 wird nicht unterstützt.
- VMware Dynamic Environment Manager 9.2.1 oder höher (für kontextbezogene Richtlinienverwaltung)
- VMware Identity Manager™ 2.9.2 oder höher (für die Integration in VMware Workspace™ ONE™)

Hardwareanforderungen für JMP Server

Sie müssen JMP Server auf einer eigens dafür eingerichteten physischen oder virtuellen Maschine installieren, die bestimmte Hardwareanforderungen erfüllt.

In der folgenden Tabelle sind die Hardware-Mindestanforderungen für eine JMP Server-Instanz in einer Produktionsumgebung aufgelistet.

Tabelle 3-1. Horizon JMP Server-Hardwareanforderungen für eine Produktionsumgebung

Hardwarekomponente	Mindestanforderung in einer Produktionsumgebung
Prozessor	4-Core-CPUs
Arbeitsspeicher	8 GB
Speicher	100 GB

In der folgenden Tabelle sind die Hardware-Mindestanforderungen für eine JMP Server-Instanz in einer Proof-of-Concept (PoC)- oder Laborumgebung aufgelistet.

Tabelle 3-2. Horizon JMP Server-Hardwareanforderungen für eine Laborumgebung

Hardwarekomponente	Mindestanforderung in einer Laborumgebung
Prozessor	4-Core-CPUs
Arbeitsspeicher	4 GB
Speicher	25 GB

Unterstütztes Betriebssystem für JMP Server

Sie müssen JMP Server auf einem unterstützten Windows Server Betriebssystem installieren.

Die beiden Arten von JMP Server-Installation, Proof-of-Concept (POC) und Production, werden auf den folgenden Windows Server-Betriebssystemen unterstützt.

Tabelle 3-3. Betriebssystemunterstützung für JMP Server

Betriebssystem	Version	Edition
Windows Server 2008 R2 SP1	64 Bit	Standard
		Enterprise
		Datencenter
Windows Server 2012 R2	64 Bit	Standard
		Datencenter
Windows Server 2016	64 Bit	Standard
		Datencenter

Netzwerkanforderungen für JMP Server

Die physische oder virtuelle Maschine, auf der Sie JMP Server installieren möchten, muss alle Produktendpunkte für alle PoDs (Points of Delivery) in Ihrem Netzwerk erreichen können.

Bevor Sie die JMP Integrated Workflow-Funktionen verwenden können, muss die Authentifizierung für die Sicherheit und die CA-signierten Zertifikate bereits vollständig für die JMP Server-Instanz und alle Technologieendpunkte, die mit Ihrer JMP Server-Instanz interagieren, konfiguriert sein. Weitere Informationen finden Sie unter [Konfigurieren von TLS-Zertifikaten und Verschlüsselungssammlungen für JMP Server](#).

Datenbankanforderungen für JMP Server

Für das JMP Server-Installationsprogramm sind bestimmte SQL Server-Datenbankversionen erforderlich, um die JMP Server-Installation durchführen zu können.

JMP Server unterstützt die folgenden SQL Server-Versionen und Editionen in den beiden unterstützten Arbeitslastumgebungen: Proof-of-Concept (PoC) oder Produktion.

Tabelle 3-4. Datenbankanforderungen für JMP Server

Arbeitslasttyp	Datenbankserver	Version	Edition
Proof-of-Concept (PoC)	SQL Server Express 2014	64 Bit	Frei
Produktion	SQL Server 2012 (SP1, SP2, SP3 und SP4)	64 Bit	Standard und Enterprise
Produktion	SQL Server 2014 (SP1 und SP2 mit CU7 oder höher)	64 Bit	Standard und Enterprise
Produktion	SQL Server 2016 (SP1 mit CU6 oder höher)	64 Bit	Standard und Enterprise

Vor dem Ausführen des JMP Server-Installationsprogramms müssen Sie die SQL Server-Datenbank erstellen, die das JMP Server-Installationsprogramm im Installationsvorgang verwendet. Ausführliche Informationen dazu finden Sie unter [Erstellen einer SQL Server Datenbank für JMP Server](#).

Sie müssen auch die Anmeldedaten angeben, die das JMP Server-Installationsprogramm zum Herstellen der Verbindung zur erstellten SQL Server-Datenbank benötigt. Sie können den Authentifizierungstyp auswählen, den das JMP Server-Installationsprogramm verwendet. Standardmäßig wird die Windows-Authentifizierung verwendet. Unabhängig davon, ob Sie die Windows-Authentifizierung oder die SQL Server-Authentifizierung verwenden, müssen die Anmeldedaten für das JMP Server-Installationsprogramm bereits in der SQL Server-Instanz vorhanden sein, bevor Sie mit der Installation von JMP Server beginnen. Ausführliche Informationen dazu finden Sie unter [Erstellen der SQL Server-Anmeldung für den JMP Server-Host](#).

Außerdem müssen Sie eine SQL Server-Anmeldung für das Windows-Server-Benutzerkonto erstellen, das Sie zur Installation von JMP Server verwenden möchten. Dieser Windows-Benutzer muss mit den entsprechenden Anmeldedaten zum Ändern der erstellten SQL Server-Datenbank konfiguriert sein.

Wenn Ihr SQL Server mit TLS-Verschlüsselung aktiviert ist, müssen Sie dessen TLS-Zertifikat exportieren und es anschließend in Ihrer JMP Server-Instanz importieren, um eine verschlüsselte Kommunikation mit dem SQL Server zu ermöglichen.

Unterstützter Webbrowser für JMP Integrated Workflow

Sie greifen auf die Benutzeroberfläche von JMP Integrated Workflow an der VMware Horizon-Konsole zu, einer webbasierten Anwendung, die mit dem VMware Horizon 7-Verbindungsserver Version 7.5 und höher installiert wird.

Die folgenden Webbrowser werden zur Verwendung der JMP Integrated Workflow-Funktionen unterstützt.

- Google Chrome (neueste Versionen unterstützt)
- Mozilla Firefox (neueste Versionen unterstützt)
- Internet Explorer 10 und 11
- Microsoft Edge

Vorbereiten der SQL Server-Datenbank und -Anmeldung für JMP Server

4

Vor dem Ausführen des JMP Server-Installationsprogramms müssen Sie eine SQL Server-Datenbank für Ihre JMP Server-Instanz erstellen. Sie müssen außerdem das SQL Server-Anmeldekonto erstellen, das das JMP Server-Installationsprogramm zum Herstellen einer Verbindung zu dieser SQL Server-Datenbank benötigt. Das Windows-Server-Anmeldekonto, das zur Ausführung des JMP Server-Installationsprogramms verwendet wird, muss auch ordnungsgemäßen Zugriff auf die SQL Server-Datenbank haben, die Sie für den JMP Server erstellt haben.

Dieses Kapitel enthält die folgenden Themen:

- Erstellen einer SQL Server Datenbank für JMP Server
- Erstellen der SQL Server-Anmeldung für den JMP Server-Host
- Gewähren von Datenbankbesitzer- und Systemverwaltungs-Berechtigungen für Windows-Benutzer

Erstellen einer SQL Server Datenbank für JMP Server

In einer SQL Server-Datenbank werden Informationen zu JMP Server-Diensten und die von Horizon-Desktopadministratoren erstellten JMP-Zuweisungen gespeichert. Sie müssen diese Datenbank vor Ausführen des JMP Server-Installationsprogramms erstellen.

Hinweis Das Verwenden eines Remote-SQL Servers ist bei Hostausfällen praktisch.

Voraussetzungen

- Stellen Sie sicher, dass eine unterstützte Version von SQL Server auf einem System installiert ist, dass für den Host, auf dem Sie JMP Server installieren möchten, remote ist, aber sich in Ihrer Netzwerkumgebung befindet. Weitere Informationen finden Sie unter [Datenbankanforderungen für JMP Server](#).
- Verwenden Sie unbedingt SQL Server Management Studio zum Erstellen und Verwalten der Datenbank. Wenn Sie JMP Server in einer PoC-Umgebung installieren, können Sie SQL Server Management Studio Express verwenden. Laden Sie das Programm von der folgenden Website herunter und installieren Sie es.

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

Verfahren

- 1 Wählen Sie im System, auf dem Microsoft SQL Server installiert ist, **Start > Alle Programme > Microsoft SQL Server 2016, Microsoft SQL Server 2014** oder **Microsoft SQL Server 2012** aus.
- 2 Wählen Sie **SQL Server Management Studio** aus.
- 3 Stellen Sie im Objekt-Explorer-Bereich eine Verbindung zu einer Instanz der SQL Server-Datenbank-Engine her und erweitern Sie dann den Knoten für diese Instanz.
- 4 Klicken Sie mit der rechten Maustaste auf **Datenbanken** und wählen Sie **Neue Datenbank** aus.
- 5 Geben Sie im Textfeld **Datenbankname** einen Namen für die Datenbank ein, die Sie für JMP Server erstellen. Verwenden Sie dazu nur ASCII-Zeichen.

Beispiel: **JMPDB**

Wichtig Es werden nur ASCII-Zeichen unterstützt.

- 6 Verwenden Sie die Standardwerte für die Parameter `Initial size` und `Autogrowth` für die Datenbank und die Protokolldateien.
- 7 Klicken Sie auf **OK**.
SQL Server Management Studio fügt Ihre Datenbank zum Ordner **Datenbanken** im Objekt-Explorer-Bereich hinzu.
- 8 Beenden Sie Microsoft SQL Server Management Studio.

Nächste Schritte

Erstellen Sie vor der Installation von JMP Server eine SQL Server-Anmeldung für den JMP Server-Host. Siehe [Erstellen der SQL Server-Anmeldung für den JMP Server-Host](#).

Erstellen der SQL Server-Anmeldung für den JMP Server-Host

Bei der Installation von JMP Server greift das Installationsprogramm auf die SQL Server-Datenbank zu, die Sie zum Speichern der Informationen zu den JMP Server-Diensten erstellt haben, die installiert werden. Sie müssen die SQL Server-Anmeldung auswählen, die das JMP Server-Installationsprogramm verwenden soll.

Wählen Sie für den Zugriff auf die erstellte SQL Server-Datenbank entweder die Anmeldung für die Windows-Authentifizierung aus oder die Anmeldung für die SQL Server-Authentifizierung. Standardmäßig wird die Anmeldung für die Windows-Authentifizierung verwendet. Vergewissern Sie sich vor dem Ausführen des JMP Server-Installationsprogramms, dass die Anmeldedaten für die ausgewählte SQL Server-Anmeldung vorhanden sind.

Anhand der folgenden Tabelle ermitteln Sie die Aufgaben zum Erstellen der SQL Server-Anmeldung, die das JMP Server-Installationsprogramm verwenden soll.

Tabelle 4-1. SQL Server-Anmeldungstypen

SQL Server-Anmeldungstyp	Verwenden der Aufgabedetails in Abschnitt
Windows-Authentifizierung (Standard)	Erstellen einer SQL Server-Anmeldung zur Windows-Authentifizierung für den JMP Server-Host
SQL Server-Authentifizierung	Erstellen der Anmeldedaten zur SQL Server-Authentifizierung für den JMP Server-Host

Erstellen einer SQL Server-Anmeldung zur Windows-Authentifizierung für den JMP Server-Host

Sie können angeben, dass das JMP Server-Installationsprogramm eine Anmeldung zur Windows-Authentifizierung verwenden soll, wenn es auf die von Ihnen erstellte SQL Server-Datenbank zugreift. Vor dem Ausführen des JMP Server-Installationsprogramms müssen die Anmeldedaten für diese SQL Server-Anmeldung am JMP Server-Host verfügbar sein, auf dem Sie JMP Server installieren.

Benutzer, die mit dem JMP Server-Host verbunden sind, können auf die JMP SQL Server-Datenbank zugreifen. Sie müssen jedoch auch sicherstellen, dass das Windows-Server-Benutzerkonto, das zur Installation von JMP Server verwendet wird, Schreibzugriff auf die SQL Server-Datenbank hat, die Sie für JMP Server erstellt haben. Siehe [Gewähren von Datenbankbesitzer- und Systemverwaltungs-Berechtigungen für Windows-Benutzer](#).

Voraussetzungen

Vergewissern Sie sich, dass Sie die SQL Server-Datenbank für Ihre JMP Server-Instanz erstellt haben. Informationen zum Erstellen der Datenbank finden Sie unter [Erstellen einer SQL Server Datenbank für JMP Server](#).

Verfahren

- 1 Melden Sie sich bei einer SQL Server Management Studio-Sitzung als Sysadmin (SA) an oder verwenden Sie ein Benutzerkonto mit SA-Rechten.
- 2 Erweitern Sie im Objekt-Explorer-Bereich den Ordner für die SQL Server-Instanz, in der Sie die Datenbank für Ihre JMP Server-Instanz erstellt haben.
- 3 Erweitern Sie den Ordner **Sicherheit**, klicken Sie mit der rechten Maustaste auf **Anmeldungen** und wählen Sie **Neue Anmeldung** aus.
- 4 Geben Sie im Dialogfeld **Anmelden – Neu** auf der Seite **Allgemein** einen Anmeldenamen im Format *domain_name\computer_name\$* ein, wobei *computer_name* der Name des JMP Server-Host ist und *domain_name* die Domäne, zu der der Host gehört.

Beispiel: **mycompany\jmpserver\$**

- 5 Wählen Sie **Windows-Authentifizierung** aus.
- 6 Wählen Sie in der Liste **Standarddatenbank** eine Standarddatenbank für die Anmeldung aus. Die Master-Datenbank ist der Standardwert für dieses Element.
- 7 Wählen Sie in der Liste **Standardsprache** eine Standardsprache für die Anmeldung aus.

- 8 Weisen Sie für das neue Anmeldekonto eine Sysadmin-Serverrolle zu.
 - a Klicken Sie im Bereich „Seite auswählen“ auf der linken Seite auf die Registerkarte **Serverrollen**.
 - b Aktivieren Sie auf der Seite „Serverrollen“ das Kontrollkästchen für **sysadmin**.
- 9 Klicken Sie auf **OK**.

Die neuen Anmeldedaten werden im Bereich „Objekt-Explorer“ im Ordner **Anmeldungen** hinzugefügt.

Nächste Schritte

Erstellen Sie die SQL Server-Anmeldedaten für das Windows Server-Benutzerkonto, das zur Installation von JMP Server verwendet wird. Siehe [Gewähren von Datenbankbesitzer- und Systemverwaltungs-Berechtigungen für Windows-Benutzer](#).

Erstellen der Anmeldedaten zur SQL Server-Authentifizierung für den JMP Server-Host

Sie können angeben, dass das JMP Server-Installationsprogramm die Anmeldedaten für die SQL Server-Authentifizierung für den Zugriff auf die erstellte SQL Server-Datenbank verwendet. Vor Ausführung des JMP Server-Installationsprogramms müssen die Anmeldedaten für diesen SQL Server-Anmeldetyp für den JMP Server-Host vorhanden sein.

Voraussetzungen

Vergewissern Sie sich, dass Sie die SQL Server-Datenbank für JMP Server erstellt haben. Informationen zum Erstellen der Datenbank finden Sie unter [Erstellen einer SQL Server Datenbank für JMP Server](#).

Verfahren

- 1 Melden Sie sich bei einer SQL Server Management Studio-Sitzung als Sysadmin (SA) oder über ein Benutzerkonto mit SA-Rechten an.
- 2 Erweitern Sie im Objekt-Explorer-Bereich den Ordner für die SQL Server-Instanz, in der Sie die JMP Server-Datenbank erstellt haben.
- 3 Erweitern Sie den Ordner **Sicherheit**, klicken Sie mit der rechten Maustaste auf **Anmeldungen** und wählen Sie **Neue Anmeldung** aus.
- 4 Geben Sie im Dialogfeld **Anmelden – Neu** auf der Seite **Allgemein** einen Wert im Textfeld **Anmeldename** ein und verwenden Sie dazu nur ASCII-Zeichen. Klicken Sie alternativ auf **Suche** und suchen Sie im Dialogfeld **Benutzer oder Gruppe auswählen** die gewünschten Anmeldedaten.

Wichtig Es werden nur ASCII-Zeichen unterstützt.

- 5 Wählen Sie **SQL Server-Authentifizierung** aus.
- 6 Geben Sie in den Textfeldern **Kennwort** und **Kennwort bestätigen** ein Kennwort für den neuen Anmeldenamen ein. Verwenden Sie nur ASCII-Zeichen.
- 7 Wenn Sie ein bestehendes Kennwort ändern, wählen Sie **Altes Kennwort angeben** aus und geben Sie dann das alte Kennwort im Textfeld **Altes Kennwort** ein.

- 8 Aktivieren oder deaktivieren Sie entsprechend der Richtlinie Ihrer Organisation die Kontrollkästchen für **Kennwortrichtlinie erzwingen**, **Kennwortablauf erzwingen** und **Benutzer muss das Kennwort bei der nächsten Anmeldung ändern**.
- 9 Wählen Sie in der Liste **Standarddatenbank** eine Standarddatenbank für die Anmeldung aus. Die Master-Datenbank ist der Standardwert für dieses Element.
- 10 Wählen Sie in der Liste **Standardsprache** eine Standardsprache für die Anmeldung aus.
- 11 Weisen Sie für das neue Anmeldekonto eine Sysadmin-Serverrolle zu.
 - a Klicken Sie im Bereich „Seite auswählen“ auf der linken Seite auf die Registerkarte **Serverrollen**.
 - b Aktivieren Sie auf der Seite „Serverrollen“ das Kontrollkästchen für **sysadmin**.
- 12 Klicken Sie auf **OK**.

Die neuen Anmeldedaten werden im Bereich „Objekt-Explorer“ im Ordner **Anmeldungen** hinzugefügt.

Nächste Schritte

Erstellen Sie die SQL Server-Anmeldedaten für das Windows Server-Benutzerkonto, das zur Installation von JMP Server verwendet wird. Siehe [Gewähren von Datenbankbesitzer- und Systemverwaltungs-Berechtigungen für Windows-Benutzer](#).

Gewähren von Datenbankbesitzer- und Systemverwaltungs-Berechtigungen für Windows-Benutzer

Neben der Erstellung einer SQL Server-Anmeldung für den JMP Server-Hostcomputer muss auch das Windows-Benutzerkonto erstellt werden, das Sie für die Installation der JMP Server-Instanz verwenden möchten. Dieses Windows-Benutzerkonto muss Sysadmin- und Datenbankbesitzerrechte in der erstellten SQL Server-Datenbank erhalten.

Voraussetzungen

- Vergewissern Sie sich, dass die SQL Server-Datenbank für den JMP Server erstellt wurde, den Sie installieren möchten. Siehe [Erstellen einer SQL Server Datenbank für JMP Server](#).
- Überprüfen Sie, ob die SQL Server-Anmeldung für den JMP Server-Host erstellt wurde. Siehe [Erstellen der SQL Server-Anmeldung für den JMP Server-Host](#).

Verfahren

- 1 Melden Sie sich bei einer SQL Server Management Studio-Sitzung als Sysadmin (SA) an oder verwenden Sie ein Benutzerkonto mit SA-Rechten.
- 2 Stellen Sie im Objekt-Explorer-Bereich eine Verbindung zur SQL Server-Instanz her, die Sie für den JMP Server erstellt haben.

- 3 Erstellen Sie die SQL Server-Anmeldung für das Windows-Benutzerkonto, das Sie für die Installation des JMP Servers verwenden möchten.
 - a Erweitern Sie den Ordner **Sicherheit**, klicken Sie mit der rechten Maustaste auf **Anmeldungen** und wählen Sie **Neue Anmeldung** aus.
 - b Klicken Sie im Dialogfeld **Anmelden – Neu** auf **Suche**.
 - c Wählen Sie im Dialogfeld **Benutzer oder Gruppe auswählen** den gültigen Active Directory-Benutzer aus, den Sie zur Installation von JMP Server verwenden möchten.
 - d Wählen Sie im Dialogfeld „Anmelden – Neu“ unter „Seite auswählen“ die Option **Serverrollen** und aktivieren Sie das Kontrollkästchen für **sysadmin**.
 - e Klicken Sie auf **OK**, um das Dialogfeld **Anmelden – Neu** zu schließen.
- 4 Gewähren Sie dem Windows-Benutzerkonto die erforderlichen Berechtigungen.
 - a Klicken Sie im linken Bereich auf **Datenbanken**.
 - b Wählen Sie die Datenbank aus, die Sie für Ihre JMP Server-Instanz erstellt haben, klicken Sie auf **Sicherheit** und anschließend auf **Benutzer**
 - c Klicken Sie im Bereich „Benutzer“ mit der rechten Maustaste auf Ihre Windows-Benutzeranmeldung und wählen Sie aus dem Kontextmenü die Option **Eigenschaften** aus.
 - d Wählen Sie unter „Datenbankrollen-Mitgliedschaft“ die Rolle **db_owner** aus.
 - e Klicken Sie auf **OK**.

Die neuen Anmeldedaten werden im Bereich „Objekt-Explorer“ im Ordner **Anmeldungen** hinzugefügt.

Nächste Schritte

Installieren Sie die JMP Server-Instanz anhand der Informationen in [Installieren von JMP Server](#) .

Installation und Upgrade von JMP Server

5

Um die JMP Integrated Workflow-Funktionen verwenden zu können, müssen Sie zunächst eine JMP Server-Instanz und die erforderlichen VMware JMP-Technologieprodukte installieren und konfigurieren. Sie können Ihre JMP Server-Installation mit einer neuen Version des JMP Server-Installationsprogramms upgraden.

Hinweis In Horizon 7 Version 7.5 können Sie nur eine Instanz von JMP Server installieren.

Hinweis Wenn Sie ein Upgrade Ihrer aktuellen JMP Server-Instanz durchführen möchten, verwenden Sie für die besten Ergebnisse das Upgrade-Installationsprogramm wie in [JMP Server upgraden](#) beschrieben. Das Upgrade-Installationsprogramm ist die bevorzugte Methode für die Durchführung eines JMP Server-Upgrades.

Wenn Sie nicht das bevorzugte Installationsprogramm für Upgrades verwenden und stattdessen die aktuelle JMP Server-Instanz deinstallieren und dann eine neue Instanz installieren, beachten Sie die folgende Einschränkung. Eine neue JMP Server-Instanz kann keine JMP-Konfigurationen oder Zuweisungsdaten verwenden, die von einer früheren JMP Server-Instanz in der vorhandenen Datenbank erstellt wurden. Um Ihre vorhandenen JMP-Konfigurationen und -Zuweisungen mit einer neuen JMP Server-Instanz zu verwenden, führen Sie die folgenden Schritte in der entsprechenden Reihenfolge aus.

- 1 Bevor Sie die JMP Server-Instanz deinstallieren, erstellen Sie eine Sicherungskopie der Datei `.encryption.key`. Diese finden Sie unter `C:\Windows\System32\config\systemprofile\AppData\Local\VMware\JMP`.
- 2 Deinstallieren Sie die JMP Server-Instanz.
- 3 Installieren Sie die neue JMP Server-Instanz.
- 4 Navigieren Sie zu `C:\Windows\System32\config\systemprofile\AppData\Local\VMware\JMP` und suchen Sie die Datei `.encryption.key`. Ersetzen Sie diese Datei durch die zuvor erstellte Sicherungsschlüsseldatei.
- 5 Starten Sie VMware JMP Platform Services neu.

Dieses Kapitel enthält die folgenden Themen:

- [Installieren von JMP Server](#)
- [JMP Server upgraden](#)

Installieren von JMP Server

Vor Verwendung der JMP Integrated Workflow-Funktionen müssen Sie JMP Server installieren und konfigurieren.

Die JMP Server-Installationsprogrammdatei ist im Download von VMware Horizon 7 Version 7.5 oder höher enthalten. Sie müssen das JMP Server-Installationsprogramm separat ausführen, nachdem Sie Horizon 7 Version 7.5 oder höher erfolgreich installiert haben.

Voraussetzungen

- Bestätigen Sie, dass Sie die Systemanforderungen für die Komponenten erfüllen, die zur Installation von JMP Server erforderlich sind. Siehe [Kapitel 3 Systemanforderungen für JMP Server](#).
- Zur Ausführung des JMP Server-Installationsprogramms auf einem Windows Server-Host müssen Sie ein Domänenbenutzerkonto mit Verwaltungsrechten auf diesem Hostsystem verwenden.
- Vergewissern Sie sich, dass die SQL Server-Datenbank, die Ihre JMP Server-Instanz verwenden muss, in einem Remotesystem erstellt wurde und Sie den entsprechenden Zugriff darauf haben. Siehe [Erstellen einer SQL Server Datenbank für JMP Server](#).
- Überprüfen Sie, ob die SQL Server-Anmeldungen und -Berechtigungen für den JMP Server-Host und das Windows-Domänenbenutzerkonto konfiguriert sind, die Sie zur Installation von JMP Server benötigen. Siehe [Erstellen der SQL Server-Anmeldung für den JMP Server-Host](#).
- Sammeln Sie die Informationen für den sicheren oder nicht sicheren HTTP-Port, den Benutzeroberflächenport und die signierten Zertifikate, die Sie für die JMP Integrated Workflow-Funktionen benötigen.
- Verschaffen Sie sich ein TLS-Zertifikat, das von einer Zertifizierungsstelle signiert wurde, und ersetzen Sie damit das standardmäßige TLS-Zertifikat, das vom JMP Server-Installationsprogramm installiert wurde.
- Ermitteln Sie vor Installation von JMP Server anhand der folgenden Tabelle den erforderlichen Installationstyp.

Installationstyp	Vom JMP Server-Installationsprogramm durchgeführte Aktion
Produktionsumgebung	Generiert eine JMP Server-Instanz, die die SQL Server Standard oder Enterprise Edition verwendet.
Entwicklungsumgebung oder Proof-of-Concept (PoC)-Umgebung	Generiert eine JMP Server-Instanz, die SQL Server Express verwendet.

- Fügen Sie die folgenden Dateien zur McAfee Antivirus-Ausschlussliste hinzu, bevor Sie JMP Server installieren.
 - C:\Programme (x86)\VMware\JMP\nssm-2.24\nssm-2.24\win32\nssm.exe
 - C:\Programme (x86)\VMware\JMP\com\xmp\node_modules\winser\bin\nssm.exe

Verfahren

- 1 Suchen Sie zum Starten des Assistenten **VMware JMP-Installationsprogramm** die JMP Server-Installationsprogrammdatei und doppelklicken Sie darauf.

Der Dateiname des JMP Server-Installationsprogramms lautet `VMware-Jmp-Installer-e.x.p-xxxxxxx.exe`, wobei `xxxxxxx` die Build-Nummer bezeichnet. Beispiel: `VMware-Jmp-Installer-e.x.p-7259616.exe`.

Hinweis Wenn Sie den Installationsvorgang protokollieren möchten, führen Sie das JMP Server-Installationsprogramm an einer Eingabeaufforderung aus und verwenden Sie den folgenden Befehl. Dabei bezeichnet *Log_Folder_Path* den Ordner, in dem die Protokolldatei erstellt wird.

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

- 2 Klicken Sie auf der Willkommen-Seite auf **Weiter** und akzeptieren Sie die VMware-Lizenzbedingungen.
- 3 Klicken Sie auf **Weiter**, um den HTTPS-Datenverkehr zuzulassen.

Hinweis JMP Server belegt Port 443 und optional die Ports 80, 3000–3004, 888 und 8889. Um den HTTP-Datenverkehr über Port 80 zuzulassen, aktivieren Sie das Kontrollkästchen für **HTTP zulassen?**.

- 4 Geben Sie die SQL Server-Instanz und die Informationen zum Datenbankkatalog an.
 - a Geben Sie die IP-Adresse oder den Namen der SQL Server-Instanz ein, um eine Verbindung zur Datenbank herzustellen, die Sie für JMP Server erstellt haben. Klicken Sie optional auf **Durchsuchen**, um die Auswahl vorzunehmen.
 - b Wählen Sie die Anmeldedaten zur Authentifizierung aus, die Sie zur Herstellung einer Verbindung mit der SQL Server-Datenbank verwenden möchten.

Option	Beschreibung
Windows-Authentifizierung über Anmeldeinformationen des aktuellen Benutzers	Mit den Administrator-Anmeldedaten, die Sie in diesem Installationsvorgang verwenden, wird eine Verbindung zur SQL Server-Datenbankinstanz hergestellt.
Serverauthentifizierung mit dem nachstehenden Benutzernamen und Kennwort	<p>Geben Sie die Anmelde-ID und das Kennwort zur Herstellung einer Verbindung mit der SQL Server-Datenbankinstanz an.</p> <p>Hinweis Das Kennwort fungiert als SQL-Authentifizierungskennwort und darf keines der folgenden Zeichen enthalten: <code>, ; = () .</code></p> <p>Wenn das Kennwort eines dieser Zeichen enthält, schlägt die Installation der Dynamic Environment Manager-Komponenten fehl, und ein Rollback wird durchgeführt.</p>

Hinweis Die verwendeten Anmeldedaten müssen bereits in der SQL Server-Instanz konfiguriert sein, die JMP Server für den Zugriff verwendet. Siehe [Erstellen der SQL Server-Anmeldung für den JMP Server-Host](#).

- c Geben Sie im Textfeld **Name des Datenbankkatalogs** den Namen der Datenbank ein, den Sie mithilfe von [Erstellen einer SQL Server Datenbank für JMP Server](#) erstellt haben. Klicken Sie optional auf **Durchsuchen** und wählen Sie den Datenbankkatalog aus der verfügbaren Liste aus.

Der ausgewählte Datenbankkatalog wird zum Speichern von Informationen zu den JMP Server-Diensten verwendet.

- d (Optional) Wenn Sie die bestehende Datenbank überschreiben möchten, aktivieren Sie das Kontrollkästchen für **Bestehende Datenbank überschreiben**.

Hinweis Bei der ersten Ausführung des JMP Server-Installationsprogramms werden die erforderlichen Datenbanktabellen erstellt. Wenn Sie das Installationsprogramm erneut ausführen, um weitere JMP Server-Instanzen für den Lastausgleichsdienst zu erstellen, stellt das Installationsprogramm fest, dass die Datenbank bereits vorhanden ist und erstellt die Tabellen nicht neu. Durch Auswahl dieser Option werden die bestehenden Informationen in der Datenbank überschrieben.

- e Um eine sichere Kommunikation zwischen JMP Server und der SQL Server-Instanz sicherzustellen, muss das Kontrollkästchen für **SSL aktivieren** aktiviert sein. Das Kontrollkästchen **SSL aktivieren** ist standardmäßig aktiviert.

Wichtig Wenn das Kontrollkästchen **SSL aktivieren** aktiviert ist, stellen Sie sicher, dass das in SQL Server verwendete TLS/SSL-Zertifikat in den lokalen Windows-Zertifikatspeicher auf dem JMP Server-Host importiert wird. Andernfalls schlägt der JMP Server-Installationsvorgang mit der Fehlermeldung „Fehler beim Ausführen der Datei uem_migrate.bat“ fehl, und wenn Sie im Fehlerdialogfeld auf **OK** klicken, wird ein Rollback der Installation durchgeführt.

Weitere Informationen zum Exportieren und Importieren des TLS/SSL-Zertifikats des SQL Servers finden Sie im Abschnitt „Aktivieren der Verschlüsselung für einen spezifischen Client“ im Microsoft TechNet-Artikel [Aktivieren der SSL-Verschlüsselung für eine Instanz von SQL Server an der Microsoft-Verwaltungskonsole](#).

- f Klicken Sie auf **Weiter**.

5 Klicken Sie auf der Seite **Bereit zum Installieren des Programms** auf **Installieren**.

6 Klicken Sie auf **Fertigstellen**, wenn die Installation erfolgreich abgeschlossen ist.

Nach erfolgreicher Installation sind die JMP Server-Dienste installiert und werden auf Ihrem Windows-Server-Host gestartet.

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

Nächste Schritte

Synchronisieren Sie die Uhrzeit zwischen der neu erstellten JMP Server-Instanz und ihrer verknüpften Horizon Connection Server. Siehe [Synchronisieren der Uhrzeit zwischen dem Horizon-Verbindungsserver und den JMP Server-Hosts](#).

JMP Server upgraden

Wenn Sie ein Upgrade Ihrer aktuellen JMP Server-Installation auf eine neuere JMP Server-Version durchführen, werden alle vorhandenen JMP-Einstellungskonfiguration und JMP-Zuweisungen beibehalten.

Die JMP Server-Installationsprogrammdatei ist beim Download der Horizon 7-Version 7.5 oder höher enthalten. Für das Upgrade Ihrer vorhandenen JMP Server-Installation müssen Sie das JMP Server-Installationsprogramm separat ausführen, nachdem Sie erfolgreich die Horizon 7-Version 7.6 oder höher installiert haben.

Voraussetzungen

Sie müssen ein Domänenbenutzerkonto mit Administratorrechten auf dem Hostsystem verwenden, um die neue JMP Server-Installationsdatei auszuführen.

Verfahren

- 1 Suchen Sie zum Starten des Assistenten **VMware JMP-Installationsprogramm** die neue JMP Server-Installationsprogrammdatei und doppelklicken Sie darauf.
Das Installationsprogramm überprüft, ob eine vorhandene JMP Server-Installation vorhanden ist.
- 2 Klicken Sie im JMP-Upgrade-Dialogfeld auf **OK**.
- 3 Klicken Sie im Begrüßungsbildschirm auf **Weiter**.
- 4 Lesen und akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf **Weiter**.
- 5 Behalten Sie beim Datenbankserver für die Seite der JMP Server-Plattformdienste die vorhandenen Datenbankeinstellungen bei und klicken Sie auf **Weiter**.
- 6 Klicken Sie auf der Seite **Bereit zum Installieren des Programms** auf **Installieren**.
Die Installation wird fortgesetzt und es dauert einige Minuten.
- 7 Klicken Sie auf **Fertigstellen**, wenn die Installation erfolgreich abgeschlossen ist.

Nach erfolgreichem Upgrade werden die drei JMP Server-Dienste auf Ihrem Windows Server-Host neu gestartet.

Konfigurieren der JMP Server-Instanz

6

Nach erfolgreicher Installation der JMP Server-Instanz müssen Sie Konfigurationsaufgaben durchführen, um sicherzustellen, dass sich die JMP Server-Instanz erfolgreich bei Horizon Connection Server authentifizieren und sicher mit anderen Servern im Netzwerk kommunizieren kann.

Dieses Kapitel enthält die folgenden Themen:

- [Synchronisieren der Uhrzeit zwischen dem Horizon-Verbindungsserver und den JMP Server-Hosts](#)
- [Konfigurieren von TLS-Zertifikaten und Verschlüsselungssammlungen für JMP Server](#)

Synchronisieren der Uhrzeit zwischen dem Horizon-Verbindungsserver und den JMP Server-Hosts

Die Uhrzeit am Horizon-Verbindungsserver und an den JMP Server-Hosts muss synchronisiert werden, damit der Authentifizierungsvorgang zwischen beiden Servern erfolgreich durchgeführt wird.

Wenn Sie an der Benutzeroberfläche der Horizon Console auf die JMP Integrated Workflow-Funktionen zugreifen, authentifiziert JMP Server das Token, das er vom Horizon-Verbindungsserver erhält, der seinerseits ein Token an JMP Server zurückgibt. Wenn die Uhrzeit zwischen beiden Hosts nicht synchronisiert ist, weist der Horizon-Verbindungsserver das vom JMP Server gesendete Token zurück. Die JMP Integrated Workflow-Funktionen sind daraufhin auf der Benutzeroberfläche der Horizon Console nicht verfügbar. Im Bereich „JMP-Einstellung“ wird folgende Fehlermeldung angezeigt.

Das Horizon-SSO-Token konnte nicht verifiziert werden.

Für einen erfolgreichen Authentifizierungsvorgang ist es erforderlich, die Uhrzeit am Horizon-Verbindungsserver und an den JMP Server-Hosts mit einem gemeinsamen NTP (Network Time Protocol)-Server zu synchronisieren.

Verfahren

- 1 Verwenden Sie die folgenden VMware-Tool-Befehle am Windows-Host.

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

- 2 Am ESXi-Host synchronisieren Sie ESXi Clocks mit einem NTP-Server.
 - a Starten Sie den VMware Host Client und stellen Sie eine Verbindung zum ESXi-Host her.
 - b Klicken Sie auf **Konfigurieren**.
 - c Klicken Sie unter **System** auf die Option **Uhrzeitkonfiguration** und anschließend auf **Bearbeiten**.
 - d Wählen Sie **NTP (Network Time Protocol) verwenden (NTP-Client aktivieren)** aus.
 - e Geben Sie im Textfeld „NTP-Server hinzufügen“ die IP-Adresse oder den vollqualifizierten Domännennamen mindestens eines NTP-Servers ein, mit dem die Synchronisierung durchgeführt werden soll.

Nächste Schritte

Konfigurieren Sie die TLS-Zertifikate für JMP Server. Siehe [Überblick über Aufgaben zur Einrichtung von TLS-Zertifikaten für JMP Server](#).

Konfigurieren von TLS-Zertifikaten und Verschlüsselungssammlungen für JMP Server

Um sicherzustellen, dass Ihre JMP Server-Instanz sicher mit anderen Servern im Netzwerk kommuniziert, müssen Sie die JMP Server-Instanz zur Verwendung von TLS-Zertifikaten konfigurieren, die von einer gültigen Zertifizierungsstelle signiert wurden. Zur Verbesserung der sicheren Verbindungen können Sie optional auch die standardmäßigen Verschlüsselungssammlungen ändern, die andere Server bei der Kommunikation mit Ihrer JMP Server-Instanz akzeptieren und vorschlagen.

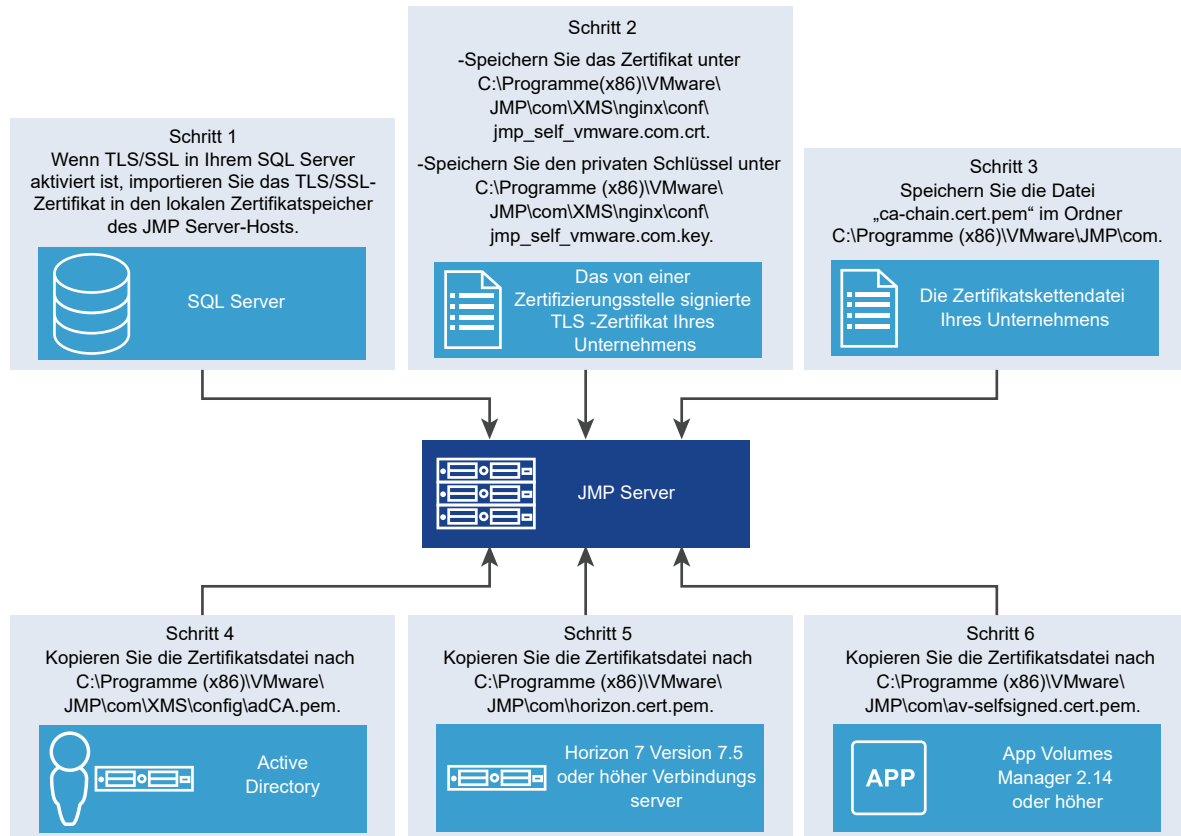
Standardmäßig installiert das JMP Server-Installationsprogramm ein selbstsigniertes TLS-Serverzertifikat für die installierte JMP Server-Instanz. Sie können das Standardzertifikat für Testzwecke verwenden. Wenn Sie die JMP Server-Instanz in einer Produktionsumgebung verwenden, müssen Sie das Standardzertifikat so bald wie möglich durch ein von einer Zertifizierungsstelle signiertes TLS-Serverzertifikat ersetzen. Die Verwendung von Zertifikaten, die nicht von einer Zertifizierungsstelle signiert wurden, kann von nicht vertrauenswürdigen Parteien dazu ausgenutzt werden, sich als Ihr Server auszugeben und Daten abzufangen. Siehe [Überblick über Aufgaben zur Einrichtung von TLS-Zertifikaten für JMP Server](#).

Überblick über Aufgaben zur Einrichtung von TLS-Zertifikaten für JMP Server

Nach der erfolgreichen Installation von JMP Server müssen Sie verschiedene Aufgaben zur Einrichtung der TLS-Serverzertifikate ausführen. Diese wurden von einer gültigen Zertifizierungsstelle (Certificate Authority, CA) für die Verwendung mit der JMP Server-Instanz signiert.

Zusätzlich zu den in diesem Thema beschriebenen Aufgaben bietet das folgende Diagramm eine visuelle Übersicht über die wesentlichen erforderlichen Schritte zur Konfiguration der Zertifikate für JMP Server. Stellen Sie sicher, dass Sie die in den nach dieser Übersicht folgenden Themen ausführlich beschriebenen Schritte zur erfolgreichen Konfiguration der jeweiligen Zertifikate befolgen. Entscheiden Sie, ob Sie die als optional gekennzeichneten Aufgaben ausführen müssen, um sicherzustellen, dass Ihre JMP Server-Konfiguration sicherer ist. Nachdem Sie das Zertifikat konfiguriert haben, müssen Sie die drei JMP Server-Dienste mit dem Windows-Dienst-Manager neu starten.

Abbildung 6-1. Wesentliche Schritte zur Konfiguration der Zertifikate für JMP Server



- 1 Wenn TLS/SSL in Ihrem SQL Server aktiviert ist, stellen Sie sicher, dass das TLS/SSL-Zertifikat in den lokalen Zertifikatspeicher des JMP Server-Hosts importiert wurde.
- 2 Ersetzen Sie das TLS-Serverzertifikat, das vom JMP Server-Installationsprogramm generiert wurde.

Das vom JMP Server-Installationsprogramm generierte standardmäßige Serverzertifikat ist selbstsigniert und wird vom Netzwerk Ihrer Organisation nicht erkannt. Ersetzen Sie das selbstsignierte Zertifikat durch ein gültiges TLS-Zertifikat einer Zertifizierungsstelle. Siehe [Ersetzen des standardmäßigen TLS-Zertifikats](#).

Wenn Ihre Organisation über kein gültiges TLS-Webserverzertifikat verfügt, beziehen Sie ein signiertes TLS-Serverzertifikat von einer Zertifizierungsstelle. Weitere Informationen finden Sie unter *Szenarien zum Einrichten von TLS-Zertifikaten für Horizon 7*.

- 3 Wenn die Serverzertifikate Ihrer Organisation von einer Zwischenzertifizierungsstelle signiert wurden, konfigurieren Sie JMP Server zur Verwendung der Zertifikatskette Ihrer Organisation (`ca-chain.cert.pem`). JMP Server kann damit die anderen Server in Ihrem Netzwerk authentifizieren. Siehe [Konfigurieren von JMP Server zur Verwendung einer Zertifikatskettendatei](#).

Hinweis Wenn die TLS-Serverzertifikate Ihrer Organisation direkt von einer von NodeJS als vertrauenswürdig angesehenen Stammzertifizierungsstelle signiert wurden, müssen Sie keine Zertifikatskettendatei oder Stammzertifikatsdatei (`ca.cert.pem`) bereitstellen.

- 4 Beziehen Sie das CA-Zertifikat, das zum Signieren des Zertifikats für den Active Directory-Server verwendet wird, speichern Sie es in der Datei `adCA.pem` und fügen Sie die Datei zum JMP Server-XMS-Konfigurationsordner hinzu. Ausführliche Informationen dazu finden Sie unter [Konfigurieren des JMP-Servers zur Verwendung des Zertifikats für Active Directory](#).
- 5 Exportieren Sie das CA-signierte Zertifikat für den Horizon-Verbindungsserver in eine Datei `horizon.cert.pem` und fügen Sie die Datei zum JMP Server-Startordner hinzu. Ausführliche Informationen dazu finden Sie unter [Konfigurieren von JMP Server zur Verwendung des Horizon-Verbindungsserver-Zertifikats](#).

Mit der Datei `horizon.cert.pem` kann der JMP Server den Verbindungsserver als vertrauenswürdigen Server authentifizieren und kann eine Verbindung zu ihm herstellen.

Hinweis Sie müssen diese Aufgabe für jeden Verbindungsserver-Pod ausführen, der als Schnittstelle für die JMP Server-Instanz fungiert. Der Inhalt der einzelnen von der Zertifizierungsstelle signierten und exportierten Zertifikate muss ebenfalls in der Datei `horizon.cert.pem` hinzugefügt werden.

- 6 Wenn Sie App Volumes-AppStacks beim Erstellen von JMP-Zuweisungen zuweisen, müssen Sie Ihre JMP Server-Instanz zur Verwendung des selbstsignierten Zertifikats der App Volumes-Manager-Instanz konfigurieren, damit sie mit der App Volumes-Manager-Instanz sicher kommunizieren kann. Siehe [Konfigurieren des JMP Servers zur Verwendung des App Volumes Manager-Zertifikats](#).
- 7 (Optional) Ändern Sie die standardmäßigen Verschlüsselungssammlungen, die Ihre JMP Server-Instanz unterstützt, zu den Verschlüsselungen, die Ihre Organisation unterstützt. Siehe [Konfigurieren von Verschlüsselungssammlungen für JMP Server](#).
- 8 (Optional) Aktivieren Sie eine restriktivere Richtlinie zur Ressourcenfreigabe zwischen verschiedenen Ursprüngen (Cross-Origin Resource Sharing, CORS) für Ihren JMP Server, um die Kommunikation mit Ihrer Horizon 7-Verbindungsserverinstanz sicherer zu machen. Siehe [Verwenden einer restriktiveren CORS-Richtlinie auf Ihrem JMP Server](#).
- 9 Starten Sie mit dem Windows-Dienst-Manager die drei JMP Server-Dienste neu.

Nach dem Konfigurieren der Serverzertifikate können Sie an der Horizon Console mit dem Konfigurieren der JMP-Einstellungen fortfahren und dann die JMP Integrated Workflow-Funktionen verwenden. Weitere Informationen finden Sie im Abschnitt „Erstmaliges Konfigurieren der JMP-Einstellungen“ in *Verwaltung der VMware Horizon Console*.

Ersetzen des standardmäßigen TLS-Zertifikats

Ersetzen Sie das standardmäßige TLS-Zertifikat, das vom JMP Server-Installationsprogramm mit dem von einer Zertifizierungsstelle signierten TLS-Zertifikat Ihrer Organisation installiert wurde.

Nach erfolgreicher Installation der JMP Server-Instanz können Sie über die Horizon-Konsole in einem Webbrowser darauf zugreifen. Wenn Ihr Netzwerk jedoch das installierte standardmäßige TLS-Zertifikat nicht erkennt, wird beim erstmaligen Konfigurieren der JMP-Einstellungen das Dialogfeld mit einer Sicherheitswarnung im Webbrowser angezeigt. Sie können das standardmäßige, selbstsignierte Zertifikat für Testzwecke verwenden. Um jedoch eine sichere Verbindung mit der JMP Server-Instanz sicherzustellen, müssen Sie das Standardzertifikat und den Schlüssel durch ein CA-signiertes TLS-Zertifikat und einen privaten Schlüssel ersetzen.

Wichtig Wenn Sie entscheiden, das Zertifikat und die Schlüsseldateien mit Dateinamen zu benennen, die sich von den vom JMP Server-Installationsprogramm erstellten Standardnamen unterscheiden, dann müssen Sie die JMP Server-NGINX-Konfigurationsdatei mit den neuen Dateinamen ändern.

Voraussetzungen

- Installieren Sie JMP Server. Siehe [Installieren von JMP Server](#).
- Beziehen Sie ein CA-signiertes TLS-Zertifikat und ersetzen Sie damit das standardmäßige TLS-Zertifikat, das vom JMP Server-Installationsprogramm installiert wurde. Zum Generieren eines Zertifikats können Sie Zertifikats-Tools wie Microsoft Certreq oder OpenSSL on Windows verwenden. Weitere Informationen finden Sie unter „Beziehen von TLS-Zertifikaten von einer Zertifizierungsstelle“ in *Szenarien zum Einrichten von TLS-Zertifikaten für Horizon 7*.

Verfahren

- 1 Halten Sie am JMP Server-Host die drei JMP Server-Dienste mit dem Windows-Dienst-Manager-Tool an.
 - a Klicken Sie mit der rechten Maustaste auf das Windows-Symbol **Start** und wählen Sie **Ausführen** aus.
 - b Geben Sie im Dialogfeld „Ausführen“ `services.msc` im Textfeld **Öffnen** ein und klicken Sie auf **OK**.
 - c Suchen Sie die folgenden drei JMP Server-Dienste im Bereich „Dienste (lokal)“ im Fenster „Dienste“ und klicken Sie bei jedem Dienst auf **Anhalten**.
 - VMware JMP API Service
 - VMware JMP File Share Service
 - VMware JMP Platform Services
- 2 Speichern Sie die Datei mit Ihrem von der Zertifizierungsstelle signierten TLS-Serverzertifikat als `jmp_self_vmware.com.crt` im NGINX-Konfigurationsordner auf dem JMP Server-Host.
 Beispiel: `C:\Programme (x86)\VMware\JMP\com\XMS\nginx\conf\jmp_self_vmware.com.crt`

- 3 Speichern Sie den privaten Schlüssel für das CA-signierte TLS-Serverzertifikat als `jmp_self_vmware.com.key`.

Beispiel: `C:\Programme (x86)\VMware\JMP\com\XMS\nginx\conf\jmp_self_vmware.com.key`

- 4 (Optional) Wenn Sie Dateinamen verwenden möchten, die sich von den erwarteten Zertifikatsdateinamen unterscheiden, wie etwa `jmp_self_vmware.com.crt` oder `jmp_self_vmware.com.key`, dann müssen Sie die NGINX-Konfigurationsdatei mit den neuen Dateinamen ändern.
 - a Öffnen Sie die Konfigurationsdatei `C:\Programme (x86)\VMware\JMP\com\XMS\nginx\conf\nginx.conf`.
 - b Suchen Sie nach den Eigenschaften `jmp_self_vmware.com.crt` und `jmp_self_vmware.com.key` und ersetzen Sie sie durch die neuen Dateinamen, die Sie gewählt haben.
 - c Speichern Sie die Datei `nginx.conf`.

Sie können nun sicher auf die JMP Integrated Workflow-Funktionen zugreifen und das Dialogfeld mit der Sicherheitswarnung des Webbrowsers wird nicht mehr angezeigt.

Nächste Schritte

Wenn die gesamte Zertifikatskette Ihrer Organisation von einer Zwischenzertifizierungsstelle signiert wurde, müssen Sie Ihre JMP Server-Instanz zur Verwendung einer Zertifikatskettendatei konfigurieren. Siehe [Konfigurieren von JMP Server zur Verwendung einer Zertifikatskettendatei](#). Fahren Sie andernfalls mit der Konfiguration Ihrer JMP Server-Instanz zur Verwendung des Zertifikats für Active Directory fort. Siehe [Konfigurieren des JMP-Servers zur Verwendung des Zertifikats für Active Directory](#).

Konfigurieren von JMP Server zur Verwendung einer Zertifikatskettendatei

Konfigurieren Sie die JMP Server-Instanz mit der gesamten Zertifikatskette Ihrer Organisation, die die Stamm- und Zwischenzertifikate umfasst, wenn eine Zwischenzertifizierungsstelle die Zertifikate der Server Ihres Unternehmens signiert hat.

Voraussetzungen

- Stoppen Sie die drei JMP Server-Dienste mit dem Windows-Dienst-Manager.

Verfahren

- 1 Erstellen Sie eine Datei mit dem Namen `ca-chain.cert.pem`. Öffnen Sie die Datei in einem Texteditor wie z. B. Notepad++.
- 2 Öffnen Sie im selben Texteditor das Stammzertifikat Ihrer Organisation. Kopieren Sie den Inhalt des Stammzertifikats in `ca-chain.cert.pem`.

Wiederholen Sie diesen Schritt für alle Zwischenzertifikats-Dateien, sofern vorhanden. Fügen Sie den Inhalt jedes Zwischenzertifikats an das Ende von `ca-chain.cert.pem` an.

3 Speichern und schließen Sie `ca--chain.cert.pem`.

Sie verfügen jetzt über eine Zertifikatskettendatei, die die Stamm- und Zwischenzertifikate Ihrer Organisation enthält.

4 Kopieren Sie die Zertifikatskettendatei `ca-chain.cert.pem` in den Ordner `C:\Programme (x86)\VMware\JMP\com`.

Wenn die Zertifikatskette vorhanden ist, kann Ihre JMP Server-Instanz die Horizon 7- und App Volumes-Instanzen authentifizieren und sicher mit ihnen kommunizieren.

Nächste Schritte

Konfigurieren Sie die JMP Server-Instanz mit dem Active Directory-Zertifikat, damit die JMP Server-Instanz den Active Directory-Server authentifizieren kann, wenn Desktopadministratoren die JMP Integrated Workflow-Funktionen verwenden. Siehe [Konfigurieren des JMP-Servers zur Verwendung des Zertifikats für Active Directory](#).

Konfigurieren des JMP-Servers zur Verwendung des Zertifikats für Active Directory

Damit JMP Server das Active Directory validiert, mit dem Horizon Console verbunden ist, müssen Sie JMP Server so konfigurieren, dass das Zertifikat für diesen Active Directory-Server verwendet wird.

Sie müssen das Zertifizierungsstellen-Stammzertifikat der Active Directory-Domäne in eine Zertifikatsdatei namens `adCA.pem` exportieren und diese Datei im JMP Server-XMS-Konfigurationsordner ablegen.

Voraussetzungen

- JMP Server muss installiert sein.
- Active Directory muss für LDAP über SSL (LDAPS) oder StartTLS (LDAP über TLS) konfiguriert sein.
- Zertifizierungsstellen-Stammzertifikate der Active Directory-Domänen. Wenn die Zertifikate nicht im PEM-Format (Base64-verschlüsselt) vorliegen, konvertieren Sie die Datei anhand der Informationen in der OpenSSL-Dokumentation (oder einem ähnlichen Dokument) in ein PEM-Format.

Hinweis Wenn mehrere Stammzertifikate aus verschiedenen Domänen vorhanden sind, können Sie alle PEM-formatierten Zertifikate in einer einzelnen Datei zusammenfassen, indem Sie die Inhalte der einzelnen Dateien nacheinander in eine einzelne `.pem`-Datei kopieren.

Verfahren

- 1 Vergewissern Sie sich, dass der Name der PEM-formatierten Zertifikatsdatei `adCA.pem` lautet.
- 2 Kopieren Sie die Datei `adCA.pem` in den JMP Server-XMS-Konfigurationsordner.

Beispiel: `C:\Programme (x86)\VMware\JMP\com\XMS\config\adCA.pem`.

Wenn das Active Directory-Zertifikat für Ihre JMP Server-Instanz konfiguriert ist, wird das Active Directory als vertrauenswürdiger Server erkannt und Horizon Console-Benutzer können erfolgreich die JMP Integrated Workflow-Funktionen verwenden.

Nächste Schritte

Konfigurieren Sie JMP Server mit dem Verbindungsserverzertifikat, damit die JMP Server-Instanz den Verbindungsserver authentifizieren kann, wenn Desktopadministratoren die JMP Integrated Workflow-Funktionen verwenden. Siehe [Konfigurieren von JMP Server zur Verwendung des Horizon-Verbindungsserver-Zertifikats](#).

Konfigurieren von JMP Server zur Verwendung des Horizon-Verbindungsserver-Zertifikats

Damit JMP Server den Horizon 7-Verbindungsserver validieren kann, mit dem Horizon Console verbunden ist, müssen Sie JMP Server zur Verwendung des Horizon 7-Verbindungsserver-Zertifikats konfigurieren.

Sie müssen das Horizon 7-Verbindungsserver-Zertifikat in eine Zertifikatsdatei namens `horizon.cert.pem` exportieren und diese Datei im JMP Server-Startordner ablegen.

Wichtig Der Inhalt der einzelnen von der Zertifizierungsstelle signierten und exportieren Zertifikate muss in derselben Datei `horizon.cert.pem` hinzugefügt werden.

Gehen Sie folgendermaßen vor, wenn Sie ein von der Zertifizierungsstelle signiertes oder selbstsigniertes Horizon 7-Verbindungsserver-Zertifikat hinzufügen.

Voraussetzungen

- JMP Server muss installiert sein.
- Sie müssen Verwaltungszugriff auf den Horizon 7-Verbindungsserver haben.

Verfahren

- 1 Melden Sie sich beim Windows Server-Host für den Horizon 7-Verbindungsserver an, der als Schnittstelle für Horizon Console und den installierten JMP Server dient.
- 2 Klicken Sie mit der rechten Maustaste auf das Windows-Symbol **Start**, wählen Sie **Ausführen** aus und geben Sie `mmc.exe` ein.

Das Fenster mit dem MMC-Dienstprogramm wird geöffnet.

- 3 Hinzufügen des Snap-ins mit den Zertifikaten.
 - a Wählen Sie im Fenster **Konsolenstamm** die Optionen **Datei > Snap-In hinzufügen/entfernen** aus.
 - b Wählen Sie im Fenster **Snap-Ins hinzufügen bzw. entfernen** im Bereich „Verfügbare Snap-Ins“ die Option **Zertifikate** aus und klicken Sie auf **Hinzufügen**.
 - c Klicken Sie nach dem Hinzufügen der Zertifikate auf **OK**.
 - d Wählen Sie im Snap-In-Fenster „Zertifikate“ die Option **Computerkonto** aus und klicken Sie auf **Weiter**.

- e Wählen Sie im Fenster „Computer auswählen“ die Option **Lokaler Computer** aus und klicken Sie auf **Fertigstellen**.

Das Snap-In „Zertifikate (Lokaler Computer)“ wird im Bereich „Ausgewählte Snap-Ins“ hinzugefügt.

- f Klicken Sie auf **OK**, um das Dialogfeld **Snap-Ins hinzufügen bzw. entfernen** zu schließen.

- 4 Wählen Sie im Fenster „Konsolenstamm“ die Optionen **Konsolenstamm > Zertifikate (Lokaler Computer)** aus und anschließend im linken Fensterbereich den Ordner **Persönliche > Zertifikate**, um dessen Inhalt anzuzeigen.

- 5 Exportieren des Horizon-Verbindungsserver-Zertifikats.

- a Suchen Sie im Bereich mit den Zertifikatsinhalten das Zertifikat mit einem Anzeigenamen **vdm**. Dieses Zertifikat gehört zum Horizon-Verbindungsserver.
- b Klicken Sie mit der rechten Maustaste auf das Zertifikat und wählen Sie **Alle Aufgaben > Exportieren** aus.
- c Klicken Sie im Dialogfeld „Zertifikatexport-Assistent“ auf **Weiter**.
- d Wählen Sie **Nein, privaten Schlüssel nicht exportieren** aus und klicken Sie auf **Weiter**.
- e Wählen Sie das Format **Base-64-verschlüsselt X.509 (.CER)** aus und klicken Sie auf **Weiter**.
- f Geben Sie den Dateinamen als **horizon.cert.pem** ein und klicken Sie auf **Durchsuchen**, um zum Ordner zu navigieren, in dem Sie das exportierte Zertifikat speichern möchten.

Wichtig Speichern Sie die exportierte Zertifikatdatei mit der Dateierweiterung **.pem** und **nicht** mit der Dateierweiterung **.cer** oder **.crt**. Öffnen Sie die exportierte Zertifikatdatei gegebenenfalls in einem Texteditor und speichern Sie sie als **horizon.cert.pem**.

- g Klicken Sie auf **Weiter** und anschließend auf **Fertigstellen**, um das Fenster **Zertifikatexport-Assistent** zu schließen.

Das Zertifikat wird erfolgreich exportiert.

- 6 Navigieren Sie zum Speicherort, an dem das exportierte Zertifikat **horizon.cert.pem** gespeichert ist und kopieren Sie es in den JMP Server-Startordner.

Beispiel: C:\Programme (x86)\VMware\JMP\com\horizon.cert.pem.

Wenn das Verbindungsserver-Zertifikat für JMP Server konfiguriert ist, wird der Verbindungsserver als vertrauenswürdiger Server erkannt, und Horizon Console-Benutzer können erfolgreich die JMP Integrated Workflow-Funktionen verwenden.

Nächste Schritte

Sehen Sie sich die optionalen Aufgaben an, die in [Überblick über Aufgaben zur Einrichtung von TLS-Zertifikaten für JMP Server](#) aufgelistet sind, und entscheiden Sie, ob Sie diese ebenfalls ausführen müssen. Starten Sie nach dem Fertigstellen der erforderlichen Konfigurationsaufgaben die JMP Server-Dienste neu und konfigurieren Sie die JMP-Einstellungen. Weitere Informationen finden Sie im Abschnitt „Erstmaliges Konfigurieren der JMP-Einstellungen“ in *Verwaltung der VMware Horizon Console*.

Konfigurieren des JMP Servers zur Verwendung des App Volumes Manager-Zertifikats

Wenn Sie App Volumes-AppStacks beim Erstellen von JMP-Zuweisungen zuweisen, müssen Sie Ihre JMP Server-Instanz zur Verwendung des Zertifikats der App Volumes Manager-Instanz konfigurieren, damit sie mit der App Volumes Manager-Instanz sicher kommunizieren kann.

In einer PoC-Installationsumgebung müssen Sie das selbstsignierte Zertifikat der App Volumes Manager-Instanz in eine Zertifikatsdatei mit dem Namen `av-selfsigned.cert.pem` exportieren, damit es von JMP Server verwendet werden kann. Wenn der App Volumes Manager ein von einer Zertifizierungsstelle signiertes Zertifikat verwendet, konfigurieren Sie JMP Server für die Verwendung der Zertifikatskettendatei Ihrer Organisation, `ca-chain.cert.pem` zur Authentifizierung der App Volumes Manager-Instanz. Siehe [Konfigurieren von JMP Server zur Verwendung einer Zertifikatskettendatei](#).

Voraussetzungen

- JMP Server muss installiert sein.
- Sie benötigen administrativen Zugriff auf die App Volumes-Manager-Instanz oder den Lastausgleichsdienst, der sie verwaltet.

Verfahren

- 1 Melden Sie sich an Ihrem JMP Server-Host über einen Webbrowser bei der App Volumes-Manager-Instanz oder dem Lastausgleichsdienst an, der die App Volumes-Manager-Instanzen in Ihrer Umgebung verwaltet.
- 2 Suchen Sie die Informationen des Zertifikats, die von der App Volumes Manager-Instanz oder dem Lastausgleich verwendet werden, mithilfe der Zertifikatsverwaltung Ihres Webbrowsers und exportieren Sie die Zertifikatsdatei im Base-64-kodierten x.509 (.CER)-Format in die Datei `C:\Programme (x86)\VMware\JMP\com\av-selfsigned.cert.pem`.

Wichtig Speichern Sie die exportierte Zertifikatsdatei mit der Dateierweiterung `.pem` und **nicht** mit der Dateierweiterung `.cer` oder `.crt`. Öffnen Sie die exportierte Zertifikatsdatei gegebenenfalls in einem Texteditor und speichern Sie sie als `av-selfsigned.cert.pem`.

Wenn Sie beispielsweise Google Chrome verwenden, klicken Sie auf **Einstellungen > Erweitert** und wählen Sie **Zertifikate verwalten**. Wählen Sie im Zertifikatsdialogfeld das App Volumes Manager-Zertifikat aus und klicken Sie auf **Exportieren**. Verwenden Sie den Zertifikatsexportassistenten zum Exportieren des Base-64-kodierten x.509 (.CER)-Formats der App Volumes Manager-Zertifikatsdatei in die Datei `C:\Programme (x86)\VMware\JMP\com\av-selfsigned.cert.pem`. Möglicherweise müssen Sie die Datei umbenennen, sodass sie nur die `.pem`-Dateierweiterung aufweist, statt `.pem.cer`.

- 3 Wenn Sie alle Aufgaben zur Konfiguration der TLS-Zertifikate, die benötigt werden, um JMP Server sicherer zu machen, abgeschlossen haben, müssen Sie die JMP Server-Dienste neu starten. Weitere Informationen zur Überprüfung der verbleibenden Aufgaben zur Konfiguration des TLS-Zertifikats finden Sie unter [Überblick über Aufgaben zur Einrichtung von TLS-Zertifikaten für JMP Server](#).

Konfigurieren von Verschlüsselungssammlungen für JMP Server

Die JMP Server-Installation umfasst standardmäßige Server- und Client-Verschlüsselungs-Suites, die zwischen Ihren JMP Server-, Horizon Connection Server-, App Volumes- und Dynamic Environment Manager-Instanzen akzeptiert und vorgeschlagen werden. Sie können optional diese standardmäßigen Verschlüsselungs-Suites, die JMP Server unterstützt, zu Verschlüsselungs-Suites ändern, die Ihre Organisation unterstützt.

Welche Verschlüsselungs-Suite verwendet wird, hängt davon ab, ob JMP Server als Server fungiert, der die Anforderung für eine sichere Verbindung empfängt, oder als Client, von dem die Anforderung für eine sichere Verbindung mit Horizon Connection Server, App Volumes oder Dynamic Environment Manager ausgeht.

Sie müssen die Liste der Verschlüsselungs-Suites in dem Format angeben, das in <https://www.openssl.org/docs/man1.0.2/apps/ciphers.html#CIPHER-LIST-FORMAT> definiert ist. Die folgende Liste von Verschlüsselungs-Suites ist die serverseitige Standardeinstellung.

```
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
```

Zusätzlich zur obigen Verschlüsselungs-Zeichenfolge werden die tatsächlich verwendeten Verschlüsselungs-Suites auch von den akzeptierten Protokollen TLSv1.1 und TLSv1.2 bestimmt, die in der Datei `nginx.conf` definiert sind.

Verfahren

- 1 Halten Sie am JMP Server-Host die drei JMP Server-Dienste mit dem Windows-Dienst-Manager-Tool an.
 - a Klicken Sie mit der rechten Maustaste auf das Windows-Symbol **Start** und wählen Sie **Ausführen** aus.
 - b Geben Sie im Dialogfeld „Ausführen“ `services.msc` im Textfeld **Öffnen** ein und klicken Sie auf **OK**.
 - c Suchen Sie im Fenster „Dienste“ im Bereich „Dienste (lokal)“ nach den folgenden drei JMP Server-Diensten und klicken Sie für jeden Dienst auf **Anhalten**.
 - VMware JMP API Service
 - VMware JMP File Share Service
 - VMware JMP Platform Services
- 2 Ändern Sie die Konfigurationsdatei, die die Verschlüsselungs-Suite enthält.

So ändern Sie die serverseitige Verschlüsselungs-Suite:

 - a Navigieren Sie zum Ordner `C:\Programme (x86)\VMware\JMP\com\XMS\nginx\conf`.
 - b Erstellen Sie eine Sicherungskopie der Datei `nginx.conf`, bevor Sie diese ändern.
 - c Öffnen Sie die Datei `csr.req` in Notepad.

- d Suchen Sie nach der Zeile, die mit `ssl_ciphers` beginnt, und ändern Sie die Verschlüsselungs-Suite nach Bedarf.
- e Speichern Sie Ihre Änderungen in Datei `nginx.conf`.

So ändern Sie die clientseitige Verschlüsselungs-Suite:

- a Navigieren Sie zum Ordner `C:\Programme (x86)\VMware\JMP\com\xmp\conf`.
- b Öffnen Sie die Datei `jmp.js` in Notepad.
- c Erstellen Sie eine Sicherungskopie der Datei `jmp.js`, bevor Sie diese ändern.
- d Suchen Sie die Zeile, die den folgenden Codeausschnitt enthält.

```
ciphers: '!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES'
```

- e Ändern Sie die Verschlüsselungs-Suite nach dem `ciphers:-`Abschnitt im Codeausschnitt.
Beispiel:

```
ciphers:'your_organization_cipher_suite'
```

- f Speichern Sie Ihre Änderungen in der Datei `jmp.js`.
- 3 Starten Sie die drei JMP Server-Dienste mit dem Windows-Dienst-Manager-Tool neu, damit die neue Liste der Verschlüsselungs-Suites wirksam wird.

Verwenden einer restriktiveren CORS-Richtlinie auf Ihrem JMP Server

Sie können eine restriktivere CORS-Richtlinie (Cross-Origin Resource Sharing) für Ihre JMP Server-Instanz verwenden, indem Sie eine Whitelist der Horizon 7-Verbindungsserverinstanzen erstellen, die auf Ihren JMP Server zugreifen dürfen.

Standardmäßig darf ein Horizon 7-Verbindungsserver auf Ihre JMP Server-Instanz zugreifen, wenn er das Zertifikat verwendet, das auch in der Zertifikatskettendatei vorhanden ist, die Sie mit [Konfigurieren von JMP Server zur Verwendung einer Zertifikatskettendatei](#) konfiguriert haben. Führen Sie die folgenden Schritte aus, um sicherzustellen, dass nur die genehmigte Liste der Horizon 7-Verbindungsserverinstanzen Zugriff auf Ihren JMP Server hat.

Verfahren

- 1 Öffnen Sie in einem Texteditor die NGINX-Konfigurationsdatei unter `C:\Programme (x86)\VMware\JMP\com\XMS\nginx\conf\nginx.conf`.
- 2 Suchen Sie die beiden Stellen mit der folgenden Zeichenfolge und kommentieren Sie beide aus, indem Sie das vorangehende `#`-Zeichen entfernen, sodass sie wie folgt angezeigt werden.

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

- 3 Suchen Sie die beiden Stellen mit der folgenden Zeichenfolge und kommentieren Sie beide aus, indem Sie ein vorangehendes #-Zeichen hinzufügen, sodass sie wie folgt angezeigt werden.

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

- 4 Fügen Sie die genehmigte Liste der Verbindungsserverinstanzen zur Whitelist hinzu.

- a Suchen Sie nach dem folgenden Inhalt in der Datei.

```
# CORS: Whitelist of origins allowed to contact JMP
# Syntax Documentation: https://nginx.org/en/docs/http/nginx_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 Fügen Sie nach der default '';-Zeile jeweils eine Zeile für jede Verbindungsserverinstanz hinzu, die in der Whitelist enthalten sein soll.

Wenn beispielsweise die Domännennamen der Verbindungsserverinstanzen, die eine Verbindung zu Ihrem JMP Server herstellen dürfen, `www.testhorizon.com` und `www.prodhorizon.com` lauten, dann werden die Zeilen, die hinzugefügt werden sollen, im folgenden Beispiel fett angezeigt.

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

- 5 Speichern Sie Ihre Änderungen in Datei `nginx.conf`.
- 6 Starten Sie die JMP-Plattform-Dienste mit dem Windows-Dienst-Manager neu.

Aktualisieren des Datenbankkennworts nach der JMP Server-Installation

7

Wenn Sie das Kennwort für die SQL Server-Datenbank, das bei der ersten Installation von JMP Server verwendet wurde, ändern, müssen Sie auch das Datenbankkennwort aktualisieren, das von den VMware JMP Server-Diensten verwendet wird.

Dieses Kapitel enthält die folgenden Themen:

- [Aktualisieren des Datenbankkennworts für VMware JMP-Plattform-Dienste](#)
- [Aktualisieren des Datenbankkennworts für den VMware JMP-Dateifreigabe-Dienst](#)

Aktualisieren des Datenbankkennworts für VMware JMP-Plattform-Dienste

Wenn Sie das Kennwort für die SQL Server-Datenbank, das bei der Installation von JMP Server verwendet wurde, ändern, müssen Sie auch das Datenbankkennwort aktualisieren, das von den VMware JMP-Plattform-Diensten verwendet wird, um eine Verbindung zu Ihrer SQL Server-Datenbank herzustellen.

Voraussetzungen

Prüfen Sie, ob Sie über die zum Ändern der Datenbankinformationen auf dem JMP Server-Host erforderlichen Administratorberechtigungen verfügen.

Verfahren

- 1 Halten Sie auf dem JMP Server-Host den VMware JMP Plattform Services-Dienst mit dem Windows-Dienst-Manager an.
 - a Klicken Sie mit der rechten Maustaste auf das Windows-Symbol **Start** und wählen Sie **Ausführen** aus.
 - b Geben Sie im Dialogfeld „Ausführen“ `services.msc` im Textfeld **Öffnen** ein und klicken Sie auf **OK**.
 - c Suchen Sie im Bereich „Dienste (Lokal)“ des Fensters „Dienste“ nach VMware JMP Plattform Services und klicken Sie auf **Beenden**.

- 2 Öffnen Sie das Fenster **ODBC-Datenquellenadministrator**, indem Sie auf eine der folgenden ausführbaren Dateien doppelklicken, die für Ihren JMP Server-Host geeignet ist.
 - C:\Windows\SysWow64\odbcad64.exe
 - C:\Windows\system32\odbcad32.exe
- 3 Klicken Sie im Fenster „ODBC-Datenquellenadministrator“ auf **System-DSN** und wählen Sie im Bereich „Benutzerdatenquellen“ **svmanager** aus.
- 4 Klicken Sie auf **Konfigurieren**.
Der Assistent für die DSN-Konfiguration von Microsoft SQL Server wird geöffnet.
- 5 Klicken Sie auf **Weiter**.

Vorsicht Nehmen Sie keine Änderungen der in den Textfeldern **Name** oder **Server** der Datenquelle vorhandenen Informationen vor.

- 6 Stellen Sie sicher, dass **Mit SQL Server-Authentifizierung anhand des vom Benutzer eingegebenen Benutzernamens und Kennworts** aktiviert ist.
- 7 Geben Sie im Textfeld **Kennwort** ein neues Kennwort ein und klicken Sie auf **Weiter**.
- 8 Klicken Sie erneut auf **Weiter**, ohne die auf der Seite mit den Standarddatenbankinformationen vorhandenen Angaben zu ändern.
- 9 Klicken Sie auf **Fertigstellen**.
Das Übersichtsfenster „ODBC Microsoft SQL Server Setup“ mit den Konfigurationsdetails wird angezeigt.
- 10 Prüfen Sie die zusammengefassten Informationen und klicken Sie auf **OK**, um die Änderung des Kennworts für den Dienst VMware JMP Plattform Services fortzusetzen.
- 11 Fügen Sie die neuen Kennwortinformationen zur Datenbankkonfigurationsdatei der VMware JMP-Plattform-Dienste hinzu, bevor Sie den Dienst VMware JMP Plattform Services neu starten.
 - a Starten Sie einen Text-Editor als Administrator und öffnen Sie die unter C:\Programme (x86)\VMware\JMP\com\XMS\config\database.yml vorhandene Datenbankkonfigurationsdatei.
 - b Suchen Sie nach der Zeile mit der Eigenschaft „username“ und fügen Sie nach dieser Zeile eine neue Zeile mit der Eigenschaft „password“ ein.
 - c Geben Sie die Informationen für das erstellte Kennwort wie im folgenden Beispiel gezeigt ein.

```
password: new_password
```

Wichtig Diese Kennwortinformationen werden nach dem Neustart des Dienstes VMware JMP Plattform Services automatisch aus der Datei database.yml entfernt.

12 Starten Sie den Dienst VMware JMP Platform Services neu.

- a Klicken Sie mit der rechten Maustaste auf das Windows-Symbol **Start** und wählen Sie **Ausführen** aus.
- b Geben Sie im Dialogfeld „Ausführen“ `services.msc` im Textfeld **Öffnen** ein und klicken Sie auf **OK**.
- c Suchen Sie im Bereich „Dienste (Lokal)“ des Fensters „Dienste“ nach VMware JMP Platform Services und klicken Sie auf **Starten**.

Nächste Schritte

Sofern noch nicht geschehen, müssen Sie auch die Anmeldeinformationen für die Datenbank aktualisieren, die der VMware JMP-Dateifreigabe-Dienst verwendet. Siehe [Aktualisieren des Datenbankkennworts für den VMware JMP-Dateifreigabe-Dienst](#).

Aktualisieren des Datenbankkennworts für den VMware JMP-Dateifreigabe-Dienst

Wenn Sie das Kennwort der SQL Server-Datenbank, das bei der Installation von JMP Server verwendet wurde, ändern, müssen Sie auch das Datenbankkennwort aktualisieren, das vom VMware JMP-Dateifreigabe-Dienst verwendet wird, um eine Verbindung zu Ihrer SQL Server-Datenbank herzustellen.

Voraussetzungen

Prüfen Sie, ob Sie über die zum Ändern der Datenbankinformationen auf dem JMP Server-Host erforderlichen Administratorberechtigungen verfügen.

Verfahren

- 1 Halten Sie auf dem JMP Server-Host den VMware JMP File Share Service-Dienst mit dem Windows-Dienst-Manager an.
 - a Klicken Sie mit der rechten Maustaste auf das Windows-Symbol **Start** und wählen Sie **Ausführen** aus.
 - b Geben Sie im Dialogfeld „Ausführen“ `services.msc` im Textfeld **Öffnen** ein und klicken Sie auf **OK**.
 - c Suchen Sie im Bereich „Dienste (Lokal)“ des Fensters „Dienste“ nach VMware JMP File Share Service und klicken Sie auf **Beenden**.
- 2 Aktualisieren Sie das vom VMware JMP-Dateifreigabe-Dienst verwendete Kennwort. Ermitteln Sie anhand der folgenden Informationen, welche Schritte Sie für den Typ der bei der JMP Server-Installation verwendeten SQL Server-Verbindung ausführen müssen.
 - Verbindung mithilfe der SQL Server-Authentifizierung:
 - 1 Navigieren Sie zum Ordner `C:/Programme (x86)/VMware/JMP/com/uem` und öffnen Sie die Datei `db.json` in einem Texteditor.

- 2 Fügen Sie einen neuen password-Parameter hinzu und stellen Sie ihn auf das neue Kennwort der SQL Server-Datenbank ein, das Sie erstellt haben, nachdem JMP Server installiert wurde. Es folgt ein Beispiel.

```
"jmp.production": {
  "server": "MyOrg-DB_server\\SQL2014",
  "database": "MyOrg-database",
  "userName": "sa",
  "password": "new_SQL_password",
  "stamp": "nnXXpIIGeImfPJWbu0YAQA==.EDlk3lCqSubg6Y2uIwSSgw=="
}
```

- 3 Speichern Sie die Datei und beenden Sie den Texteditor.

■ Verbindung mithilfe der Windows-Authentifizierung:

- 1 Navigieren Sie zum Ordner C:/Programme (x86)/VMware/JMP/com/uem und öffnen Sie die Datei db.json in einem Texteditor.
- 2 Ersetzen Sie den vorhandenen Inhalt der Datei durch den folgenden Inhalt, in dem Sie <IP address> durch die IP-Adresse für den SQL Server-Host und <Database name> durch den gültigen Datenbanknamen ersetzen müssen.

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

- 3 Speichern Sie die Datei und beenden Sie den Texteditor.

3 Starten Sie VMware JMP File Share Service neu.

- a Klicken Sie mit der rechten Maustaste auf das Windows-Symbol **Start** und wählen Sie **Ausführen** aus.
- b Geben Sie im Dialogfeld „Ausführen“ services.msc im Textfeld **Öffnen** ein und klicken Sie auf **OK**.
- c Suchen Sie im Bereich „Dienste (Lokal)“ des Fensters „Dienste“ nach VMware JMP File Share Service und klicken Sie auf **Starten**.

Nächste Schritte

Sofern noch nicht geschehen, müssen Sie auch die Anmeldeinformationen für die Datenbank aktualisieren, die von den VMware JMP-Plattform-Diensten verwendet werden. Siehe [Aktualisieren des Datenbankkennworts für VMware JMP-Plattform-Dienste](#).

Fehlerbehebung für Ihren JMP Server

8

Beim Installieren, Konfigurieren und Registrieren Ihrer JMP Server-Instanz können Fehlermeldungen auftreten. In diesem Kapitel finden Sie Informationen zur Fehlerbehebung.

Dieses Kapitel enthält die folgenden Themen:

- [JMP Server ist nicht verfügbar \(Fehler\)](#)
- [Fehler tritt nach Aktualisierung des Kennworts für Dienstkonto auf](#)
- [Deinstallieren von JMP Server](#)

JMP Server ist nicht verfügbar (Fehler)

Sie können keine Verbindung zu Ihrer JMP Server-Instanz herstellen.

Problem

Wenn Sie Horizon Console verwenden, um Ihre JMP Server-Instanz zu registrieren, wird eventuell die folgende Fehlermeldung angezeigt: Der angegebene JMP Server ist nicht verfügbar. dass Sie Ihre Angabe ändern und es später erneut versuchen sollen.

Ursache

Diese Fehlermeldung kann mehrere Ursachen haben. Verwenden Sie die im folgenden Abschnitt enthaltenen Informationen, um die Ursache und die passende Problemumgehung zu ermitteln.

Lösung

- 1 Stellen Sie sicher, dass die Zertifikate korrekt konfiguriert sind.
Verwenden Sie die in [Konfigurieren von TLS-Zertifikaten und Verschlüsselungssammlungen für JMP Server](#) enthaltenen Informationen.
- 2 Nachdem Sie versucht haben, die JMP Server-URL zu registrieren, prüfen Sie die HTTP-Antwort des Webbrowsers.

Wenn Sie eine HTTP-Antwort erhalten haben, die der folgenden Ausgabe ähnelt,

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

führen Sie die folgenden Schritte aus, um zu prüfen, ob das für die Anmeldung bei Horizon Console verwendete Benutzerkonto über ausreichende Administratorrechte verfügt.

- a Wählen Sie in Horizon Administrator **View-Konfiguration > Administratoren** aus.
- b Prüfen Sie im Bereich „Administrator“, ob Ihr Administrator-Benutzerkonto als `<Domänenname>\Administrator` (und nicht als `BUILTIN\Administrator`) angezeigt wird und ob ihm vollständige Administratorrechte zugewiesen sind.
- c Falls „BUILTIN\Administrator“ angezeigt wird, wenden Sie die in den [Versionshinweisen für VMware Horizon 7 Version 7.5](#) beschriebene Problemumgehung an.

Informationen zur Verwaltung von Administratorberechtigungen finden Sie im Dokument *Horizon 7-Verwaltung* im Abschnitt zum Verwalten und Prüfen der Berechtigungen.

- 3 Wenn die HTTP-Antwort des Webbrowsers JWT-Meldungen (JSON Web Token) enthält, die ähnlich wie die Fehlermeldung `{"code":403,"error":"Error: Unable to verify Horizon JWT","error_code":"1044","error_type":"horizonJwtVerificationError"}` lauten, stellen Sie sicher, dass die Uhrzeit zwischen dem JMP Server-Host und dem Horizon Connection Server-Host synchronisiert ist.

Verwenden Sie die in [Synchronisieren der Uhrzeit zwischen dem Horizon-Verbindungsserver und den JMP Server-Hosts](#) enthaltenen Informationen.

Fehler tritt nach Aktualisierung des Kennworts für Dienstkonto auf

Nach dem Ändern von Kennwörtern für Dienstkonten, die während der Erstkonfiguration von JMP Server verwendet wurden, erhalten Sie eine Fehlermeldung beim Versuch, Aufgaben mit Ihrer JMP Server-Instanz durchzuführen.

Sie müssen auch die JMP Server-Datenbank mit den neuen Kennwortdaten aktualisieren. Verwenden Sie die Ruby on Rails-Konsole, um die in der SQL Server-Datenbank von JMP Server gespeicherten Kennwörter zu aktualisieren.

Vorsicht Das Ändern von Werten mithilfe der Ruby on Rails-Konsole kann erhebliche Auswirkungen auf Ihre Umgebung haben. Wenn Sie mit der Ruby on Rails-Konsole nicht vertraut sind, üben Sie das Ausführen von Befehlen in einer Testumgebung, bevor Sie Änderungen in einer Produktionsumgebung anwenden.

Problem

Beim Versuch, integrierte JMP-Workflow-Aufgaben mit Ihrer JMP Server-Instanz durchzuführen, wird möglicherweise eine der folgenden Fehlermeldungen angezeigt.

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

Ursache

Wenn Sie eines der Kennwörter für Dienstkonten, die bei der Erstkonfiguration Ihrer JMP Server-Instanz verwendet wurden, aktualisieren, erhalten Sie möglicherweise eine der oben aufgeführten Fehlermeldungen, da JMP Server weiterhin die alten Kennwörter verwendet. Fehler 1 kann auftreten, wenn das Kennwort des Horizon 7-Dienstkontos geändert wurde. Fehler 2 kann auftreten, wenn das Kennwort eines App Volumes Manager-Dienstkontos geändert wurde oder wenn der Dienst nicht verfügbar ist. Fehler 3 kann auftreten, wenn das Kennwort des Active Directory (AD) geändert wurde.

Lösung

- 1 Navigieren Sie über eine Windows-Eingabeaufforderung auf Ihrem JMP Server-Hostcomputer zu dem XMS-Konfigurationsordner von JMP Server und starten Sie die Ruby on Rails-Konsole.

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

- 2 Um die Kennworteinträge in der SQL Server-Datenbank zu aktualisieren, verwenden Sie die folgenden Ruby on Rails-Konsolenbefehle.

Tabelle 8-1. Befehle zum Aktualisieren der Kennwörter in der SQL Server-Datenbank

Aktion	Ruby on Rails-Konsolenbefehle
Aktualisieren Sie das Kennwort für Horizon 7.	<pre>a=Xms::Service.find_by_service_type("horizon") a.password="<new_Horizon7_password>" a.save</pre>
Aktualisieren Sie das Kennwort für App Volumes Manager.	<pre>a=Xms::Service.find_by_service_type("avmgr") a.password="<new_AVM_password>" a.save</pre>
Aktualisieren Sie das Active Directory-Kennwort.	<pre>a=Xms::IdentityService.find_by(netbios_name:"<netbios-name>") a.password="<new_AD_password>" a.save</pre>

- 3 Um das Kennwort für die Dynamic Environment Manager-Instanz zu aktualisieren, verwenden Sie das Dialogfeld **UEM-Dateifreigabe bearbeiten** in der Registerkarte **UEM** von Horizon Console.

Weitere Informationen finden Sie unter „Bearbeiten der Informationen der User Environment Manager-Konfigurationsdateifreigabe“ im Dokument *Verwaltung der VMware Horizon Console*.

Hinweis Wenn auch das AD-Kennwort aktualisiert wurde, müssen Sie den AD-Kennworteintrag in der SQL Server-Datenbank von JMP Server vor dem Aktualisieren des Kennworts für Dynamic Environment Manager aktualisieren.

Deinstallieren von JMP Server

Zur Problembehebung müssen Sie möglicherweise JMP Server deinstallieren und neu installieren.

Diese Vorgehensweise beschreibt, wie JMP Server deinstalliert wird, wenn Probleme auftreten, die nicht anhand anderer Methoden behoben werden können.

Voraussetzungen

- Überprüfen Sie, ob Sie über die korrekten Verwaltungsrechte zum Deinstallieren von JMP Server verfügen.
- Bevor Sie einen JMP Server deinstallieren, müssen Sie alle Dynamic Environment Manager-Konfigurationsdateifreigaben löschen, die mit diesem JMP Server verknüpft sind. Weitere Informationen finden Sie unter „Löschen der Informationen in der User Environment Manager-Konfigurationsdateifreigabe“ in *Verwaltung der VMware Horizon Console*.

Verfahren

- 1 Öffnen Sie das Microsoft Windows-Programm und die Konsole mit den Funktionen.
Klicken Sie beispielsweise auf **Start >Einstellungen >System >Apps und Funktionen**.
- 2 Wählen Sie **VMware JMP** aus der Liste der installierten Anwendungen aus.
- 3 Klicken Sie zum Beenden der Deinstallationsschritte auf **Deinstallieren** und befolgen Sie die Anweisungen des Assistenten.

Nächste Schritte

Installieren Sie JMP Server erneut. Weitere Details finden Sie im Dokument [Installieren von JMP Server](#) .