

VMware Horizon JMP Server のインストールと セットアップ ガイド

更新日 : 2018 年 6 月 19 日
VMware Horizon 7 7.5



vmware®

最新の技術ドキュメントは VMware の Web サイト (<https://docs.vmware.com/jp/>) にあります
このドキュメントに関するご意見および感想がある場合は、docfeedback@vmware.com までお送りください。

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

ヴィエムウェア株式会社
105-0013 東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

Copyright © 2018 VMware, Inc. 無断転載を禁ず。著作権および商標情報。

目次

1	VMware Horizon JMP Server のインストールとセットアップ ガイド	5
2	JMP Server のインストールと構成の概要	6
3	JMP Server のシステム要件	8
	JMP テクノロジーの必須コンポーネント	8
	JMP Server のハードウェア要件	8
	JMP Server のサポート対象オペレーティング システム	9
	JMP Server のネットワーク要件	9
	JMP Server のデータベース要件	10
	JMP Integrated Workflow でサポートされる Web ブラウザ	10
4	JMP Server の SQL Server データベースとログインの準備	11
	JMP Server の SQL Server データベースの作成	11
	JMP Server ホストに SQL Server のログイン情報を作成する	12
	JMP Server ホストに SQL Server Windows 認証のログイン情報を作成する	12
	JMP Server ホストに SQL Server 認証のログイン情報を作成する	13
	Windows ユーザーへのデータベース所有者権限とシステム管理権限の付与	15
5	JMP Server のインストール	17
	JMP Server のインストール	17
	JMP Server のアンインストール	20
6	JMP Server インスタンスの構成	21
	Horizon 接続サーバと JMP Server ホスト間の時間の同期	21
	JMP Server の TLS 証明書と暗号化サイトの構成	22
	JMP Server に TLS 証明書を設定するタスクの概要	22
	デフォルトの TLS 証明書の置き換え	24
	証明書チェーン ファイルを使用するように JMP Server を設定する	26
	Active Directory の証明書を使用するように JMP Server を構成する	26
	Horizon 接続サーバ証明書を使用するように JMP Server を設定する	27
	App Volumes Manager の自己署名証明書を使用するように JMP Server を構成する	29
	JMP Server の暗号化サイトの構成	29
	JMP Server により制限の厳しい CORS ポリシーを使用する	30
7	JMP Server のインストール後のデータベース パスワードの更新	32
	VMware JMP プラットフォーム サービスのデータベース パスワードの更新	32
	VMware JMP ファイル共有サービスのデータベース パスワードの更新	34

8 JMP Server のトラブルシューティング 36

JMP Server 使用不可エラー 36

VMware Horizon JMP Server のインストールとセットアップ ガイド

1

『VMware Horizon JMP Server のインストールとセットアップ ガイド』では、VMware Horizon[®] Just-in-Time Management Platform (JMP) Server をインストールして構成する方法を説明します。JMP Server をインストールして JMP を構成すると、VMware Horizon Console で JMP Integrated Workflow 機能を使用して JMP の割り当てを定義できます。

このドキュメントの情報は、JMP Server をインストールするユーザーを対象としています。本書は、仮想マシン テクノロジーとデータセンターの運用に精通している経験豊富な Windows システム管理者を対象にしています。

JMP Server のインストールと構成の概要

2

Horizon JMP Server をインストールする前後と Horizon JMP Integrated Workflow 機能を使用する前に、特定のタスクを実行する必要があります。

次のリストに、必要なタスクの概要を示します。これらのタスクを実行する手順は、この概要の後のトピックで説明します。

- 1 JMP Server のシステム要件を満たしていることを確認します。第 3 章「[JMP Server のシステム要件](#)」を参照してください。
- 2 インストールで作成される JMP Server サービスの情報を保存する SQL Server データベースを作成します。[JMP Server の SQL Server データベースの作成](#)」を参照してください。
- 3 前の手順で作成した SQL Server データベースに接続する JMP Server ホストが使用する SQL Server のログイン情報を作成します。詳細については、「[JMP Server ホストに SQL Server のログイン情報を作成する](#)」を参照してください。
- 4 JMP Server のインストールで使用する Windows ユーザーのログイン情報に、JMP Server サービスの情報が保存される SQL Server データベースを変更できる権限が付与されていることを確認します。[Windows ユーザーへのデータベース所有者権限とシステム管理権限の付与](#)」を参照してください。
- 5 (オプション) 前の手順の SQL Server が TLS 暗号化を使用している場合は、JMP Server ホストの Windows ローカル証明書ストアに TLS 証明書をインポートします。SQL Server の TLS 証明書をエクスポートまたはインポートする方法については、Microsoft TechNet の記事、[How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console](#) で「Enable encryption for a specific client」を参照してください。
- 6 JMP Server をインストールします。[JMP Server のインストール](#)」を参照してください。
- 7 JMP Server インスタンスで、Horizon Connection Server ホストと Windows ホストの時刻を同期します。[Horizon 接続サーバと JMP Server ホスト間の時間の同期](#)」を参照してください。
- 8 VMware Horizon 7 接続サーバ、VMware App Volumes™ Manager、VMware User Environment Manager™、ネットワーク内の他のシステムのインスタンスとセキュアな通信ができるように、JMP Server インスタンスに TLS 証明書を設定します。[JMP Server の TLS 証明書と暗号化スイートの構成](#)」を参照してください。
- 9 (オプション) JMP Server インスタンスがサポートするデフォルトの暗号化スイートを組織でサポートする暗号化スイートに変更します。[JMP Server の暗号化スイートの構成](#)」を参照してください。

- 10 (オプション) JMP Server インスタンスで、より制限の厳しいクロスオリジン リソース共有 (CORS) ポリシーを使用し、Horizon 7 接続サーバとのセキュア通信の安全性を強化します。[「JMP Server により制限の厳しい CORS ポリシーを使用する」](#)を参照してください。
- 11 『VMware Horizon Console の管理』ドキュメントの「JMP 設定の初期構成」の説明に従って JMP を構成する前に、Windows システム マネージャを使用して、JMP Server サービスを再起動します。

JMP Server のシステム要件

VMware Horizon JMP Server をインストールして JMP Integrated Workflow 機能を使用する前に、特定のハードウェア要件とソフトウェア要件を満たす必要があります。

この章では次のトピックについて説明します。

- JMP テクノロジーの必須コンポーネント
- JMP Server のハードウェア要件
- JMP Server のサポート対象オペレーティングシステム
- JMP Server のネットワーク要件
- JMP Server のデータベース要件
- JMP Integrated Workflow でサポートされる Web ブラウザ

JMP テクノロジーの必須コンポーネント

JMP Server をインストールして JMP Integrated Workflow 機能を使用する前に、JMP テクノロジーを構成する VMware 製品のサポート対象バージョンがインストールされている必要があります。

JMP Server のインストールを開始する前に、次のバージョンの VMware 製品をインストールする必要があります。

- VMware Horizon 7 バージョン 7.5 以降
- VMware App Volumes 2.14 以降
- VMware User Environment Manager 9.2.1 以降
- VMware Identity Manager™ 2.9.2 以降 (VMware Workspace™ ONE™ との統合)

JMP Server のハードウェア要件

特定のハードウェア要件を満たす専用の物理マシンまたは仮想マシンに JMP Server をインストールする必要があります。

次の表に、本番環境の JMP Server インスタンスのハードウェア最小要件を示します。

表 3-1. 本番環境の Horizon JMP Server のハードウェア要件

ハードウェア コンポーネント	本番環境の最小要件
プロセッサ	4 コア CPU
メモリ	8 GB
ストレージ	100 GB

次の表に、事前検証 (PoC) 環境またはラボ環境の JMP Server インスタンスのハードウェア最小要件を示します。

表 3-2. ラボ環境の Horizon JMP Server のハードウェア要件

ハードウェア コンポーネント	ラボ環境の最小要件
プロセッサ	4 コア CPU
メモリ	4 GB
ストレージ	25 GB

JMP Server のサポート対象オペレーティング システム

サポートされている Windows Server オペレーティング システムに JMP Server をインストールする必要があります。

事前検証 (POC) 環境と本番環境の 2 つの JMP Server インストール環境では、次の Windows Server オペレーティング システムがサポートされています。

表 3-3. JMP Server のオペレーティング システム サポート

オペレーティング システム	バージョン	エディション
Windows Server 2008 R2 SP1	64 ビット	Standard Enterprise Datacenter
Windows Server 2012 R2	64 ビット	Standard Datacenter
Windows Server 2016	64 ビット	Standard Datacenter

JMP Server のネットワーク要件

JMP Server をインストールする物理マシンまたは仮想マシンは、ネットワーク上のすべての到達ポイント (PoDs) にあるすべての製品エンドポイントに接続できる必要があります。

JMP Integrated Workflow 機能を使用する前に、JMP Server インスタンスだけでなく、JMP Server インスタンスと対話するすべてのテクノロジー エンドポイントにセキュリティおよび CA 署名付き証明書認証を構成する必要があります。詳細については、[「JMP Server の TLS 証明書と暗号化スイートの構成」](#)を参照してください。

JMP Server のデータベース要件

JMP Server インストーラで JMP Server をインストールするには、特定のバージョンの SQL Server データベースが必要です。

JMP Server は、事前検証 (PoC) と本番の 2 つのワークロード環境をサポートしています。それぞれの環境でサポートしている SQL Server のバージョンとエディションは次のとおりです。

表 3-4. JMP Server のデータベース要件

ワークロード タイプ	データベース サーバ	バージョン	エディション
事前検証 (PoC)	SQL Server Express 2014	64 ビット	空き
本番	SQL Server 2012 (SP1、SP2、SP3、SP4)	64 ビット	Standard および Enterprise
本番	SQL Server 2014 (SP1、SP2、CU7 以降)	64 ビット	Standard および Enterprise
本番	SQL Server 2016 (SP1、CU6 以降)	64 ビット	Standard および Enterprise

JMP Server インストーラを実行する前に、JMP Server インストーラがインストール プロセスで使用する SQL Server データベースを作成する必要があります。詳細については、[「JMP Server の SQL Server データベースの作成」](#)を参照してください。

また、JMP Server インストーラが SQL Server データベースとの接続で使用するログイン認証情報を指定する必要があります。JMP Server インストーラが使用する認証タイプを選択できます。デフォルトは Windows 認証です。いずれの場合も、JMP Server のインストールを開始する前に、JMP Server インストーラが使用するログイン認証情報が SQL Server インスタンスに存在している必要があります。詳細については、[「JMP Server ホストに SQL Server のログイン情報を作成する」](#)を参照してください。

また、JMP Server のインストールで使用する Windows サーバのユーザー アカウントに、SQL Server のログイン情報を作成する必要があります。この Windows ユーザーには、作成した SQL Server データベースを変更できるように、適切な認証情報を設定する必要があります。

SQL Server で TLS 暗号化が有効になっている場合は、SQL Server で暗号化された通信が行われるように、TLS 証明書をエクスポートして JMP Server インスタンスにインポートする必要があります。

JMP Integrated Workflow でサポートされる Web ブラウザ

JMP Integrated Workflow ユーザー インターフェイス (UI) にアクセスするには、VMware Horizon コンソールを使用します。このコンソールは、VMware Horizon 7 接続サーババージョン 7.5 以降と一緒にインストールされる Web ベースのアプリケーションです。

JMP Integrated Workflow 機能は、次の Web ブラウザをサポートしています。

- Google Chrome (サポートされる最新バージョン)
- Mozilla Firefox (サポートされる最新バージョン)
- Internet Explorer 10 および 11
- Microsoft Edge

JMP Server の SQL Server データベースとログインの準備

4

JMP Server インストーラを実行する前に、使用する JMP Server インスタンスに SQL Server データベースを作成する必要があります。また、この SQL Server データベースに JMP Server インストーラが接続するときに使用される SQL Server のログイン アカウントを作成する必要があります。JMP Server インストーラを実行する Windows サーバのログイン アカウントには、JMP Server の SQL Server データベースに対して適切なアクセス権が必要です。

この章では次のトピックについて説明します。

- JMP Server の SQL Server データベースの作成
- JMP Server ホストに SQL Server のログイン情報を作成する
- Windows ユーザーへのデータベース所有者権限とシステム管理権限の付与

JMP Server の SQL Server データベースの作成

JMP Server サービスの情報と Horizon デスクトップの管理者が作成した JMP 割り当ての情報は、SQL Server データベースに保存されます。JMP Server インストーラを実行する前に、このデータベースを作成する必要があります。

開始する前に

- JMP Server をインストールするホストまたはネットワーク環境に、サポートされているバージョンの SQL Server がインストールされていることを確認します。詳細については、「[JMP Server のデータベース要件](#)」を参照してください。
- SQL Server Management Studio を使用してデータベースを作成し管理することを確認します。事前検証 (PoC) 環境に JMP Server をインストールする場合は、SQL Server Management Studio Express を使用できます。次の Web サイトからダウンロードしてインストールします。

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

手順

- 1 Microsoft SQL Server がインストールされているコンピュータで、[スタート]-[すべてのプログラム]-[Microsoft SQL Server 2016] の順に選択し、[Microsoft SQL Server 2014] または [Microsoft SQL Server 2012] を選択します。
- 2 [SQL Server Management Studio] を選択します。
- 3 [オブジェクトエクスプローラー] ペインで、SQL Server Database Engine のインスタンスに接続し、このインスタンスのノードを展開します。

- 4 [データベース] を右クリックして、[新しいデータベース] を選択します。
- 5 [データベース名] テキスト ボックスに、JMP Server に作成するデータベースの名前を入力します。ASCII 文字のみを使用してください。

例：JMPDB

重要 非 ASCII 文字はサポートされません。

- 6 データベースとログ ファイルに **Initial size** と **Autogrowth** のパラメータのデフォルト値を使用します。
- 7 [OK] をクリックします。

SQL Server Management Studio により、[オブジェクト エクスプローラ] ペインの [データベース] フォルダにデータベースが追加されます。

- 8 Microsoft SQL Server Management Studio を終了します。

次に進む前に

JMP Server をインストールする前に、JMP Server ホストに SQL Server のログイン情報を作成します。[「JMP Server ホストに SQL Server のログイン情報を作成する」](#)を参照してください。

JMP Server ホストに SQL Server のログイン情報を作成する

JMP Server のインストール中に、インストーラは SQL Server データベースにアクセスして、インストールする JMP Server サービスの情報を格納アクセスします。JMP Server インストーラが使用する SQL Server ログイン タイプを選択する必要があります。

この SQL Server データベースにアクセスするには、Windows 認証または SQL Server 認証のログイン情報を選択します。デフォルトでは、Windows 認証のログイン情報が使用されます。JMP Server インストーラを実行する前に、選択した SQL Server ログイン タイプに認証情報が存在することを確認します。

以下の表を参照して、JMP Server のインストーラが使用する SQL Server のログイン情報を作成してください。

表 4-1. SQL Server ログイン タイプ

SQL Server ログイン タイプ	タスクの詳細が記述されたセクション
Windows 認証 (デフォルト)	「JMP Server ホストに SQL Server Windows 認証のログイン情報を作成する」
SQL Server 認証	「JMP Server ホストに SQL Server 認証のログイン情報を作成する」

JMP Server ホストに SQL Server Windows 認証のログイン情報を作成する

JMP Server インストーラが Windows 認証のログイン情報を使用して SQL Server データベースにアクセスするように指定できます。JMP Server インストーラを実行する前に、JMP Server をインストールする JMP Server ホストに SQL Server ログインの認証情報が存在する必要があります。

JMP Server ホストに接続しているユーザーは、JMP SQL Server データベースにアクセスできます。ただし、JMP Server のインストールで使用される Windows Server ユーザー アカウントに、JMP Server に作成した SQL Server データベースへの書き込みアクセス権が必要です。[「Windows ユーザーへのデータベース所有者権限とシステム管理権限の付与」](#)を参照してください。

開始する前に

JMP Server インスタンスに SQL Server データベースが作成されていることを確認します。データベースの作成方法については、[「JMP Server の SQL Server データベースの作成」](#)を参照してください。

手順

- 1 sysadmin (SA) として SQL Server Management Studio セッションにログインするか、SA 権限を持つユーザー アカウントにログインします。
- 2 [オブジェクト エクスプローラ] ペインで、JMP Server インスタンスのデータベースを作成した SQL サーバ インスタンスのフォルダを展開します。
- 3 [セキュリティ] フォルダを展開し、[ログイン] を右クリックして [新しいログイン] を選択します。
- 4 [ログイン-新規作成] ダイアログ ボックスの [全般] ページで、ログイン名を <domain_name\computer_name>\$ の形式で入力します。<computer_name> は JMP Server のホスト名、<domain_name> はホストのドメインです。

例：**mycompany\jmpserver\$**

- 5 [Windows 認証] を選択します。
- 6 [デフォルトのデータベース] リストから、デフォルトでログインするデータベースを選択します。この項目のデフォルト値はマスター データベースです。
- 7 [デフォルト言語] リストから、デフォルトのログイン言語を選択します。
- 8 新しいログイン アカウントに sysadmin サーバ ロールを割り当てます。
 - a 左側にある [ページの選択] ペインで [サーバ ロール] タブをクリックします。
 - b [サーバ ロール] ページで、[sysadmin] チェック ボックスを選択します。
- 9 [OK] をクリックします。

新しいログイン情報が [オブジェクト エクスプローラ] ペインの [ログイン] フォルダの下に追加されます。

次に進む前に

JMP Server のインストールに使用する Windows Server ユーザー アカウントに SQL Server のログイン認証情報を作成します。[「Windows ユーザーへのデータベース所有者権限とシステム管理権限の付与」](#)を参照してください。

JMP Server ホストに SQL Server 認証のログイン情報を作成する

JMP Server インストーラが SQL Server 認証のログイン情報を使用して SQL Server データベースにアクセスするように指定できます。JMP Server インストーラを実行する前に、この SQL Server ログイン タイプの認証情報が JMP Server ホストに存在している必要があります。

開始する前に

JMP Server に SQL Server データベースが作成されていることを確認します。データベースの作成方法については、[\[JMP Server の SQL Server データベースの作成\]](#) を参照してください。

手順

- 1 sysadmin (SA) として SQL Server Management Studio セッションにログインするか、SA 権限を持つユーザー アカウントにログインします。
- 2 [オブジェクト エクスプローラ] ペインで、JMP Server データベースを作成した SQL サーバ インスタンスのフォルダを展開します。
- 3 [セキュリティ] フォルダを展開し、[ログイン] を右クリックして [新しいログイン] を選択します。
- 4 [ログイン - 新規作成] ダイアログ ボックスの [全般] ページで、[ログイン名] テキスト ボックスに値を入力します。値には ASCII 文字のみを使用してください。あるいは、[検索] をクリックして、[ユーザーまたはグループの選択] ダイアログ ボックスでログイン情報を検索します。

重要 非 ASCII 文字はサポートされません。

- 5 [SQL Server 認証] を選択します。
- 6 [パスワード] と [パスワードの確認] テキスト ボックスに、新しいログイン名のパスワードを入力します。ASCII 文字のみを使用してください。
- 7 既存のパスワードを変更する場合は、[古いパスワードを指定する] を選択して、[古いパスワード] テキスト ボックスに古いパスワードを入力します。
- 8 組織のポリシーに応じて、[パスワード ポリシーを適用する]、[パスワードの期限を適用する]、[次回ログイン時にユーザーにパスワードの変更を求める] チェック ボックスを選択または選択解除します。
- 9 [デフォルトのデータベース] リストから、デフォルトでログインするデータベースを選択します。この項目のデフォルト値はマスター データベースです。
- 10 [デフォルト言語] リストから、ログインのデフォルト言語を選択します。
- 11 新しいログイン アカウントに sysadmin サーバ ロールを割り当てます。
 - a 左側にある [ページの選択] ペインで [サーバ ロール] タブをクリックします。
 - b [サーバ ロール] ページで、[sysadmin] チェック ボックスを選択します。
- 12 [OK] をクリックします。

新しいログイン情報が [オブジェクト エクスプローラ] ペインの [ログイン] フォルダの下に追加されます。

次に進む前に

JMP Server のインストールに使用する Windows Server ユーザー アカウントに SQL Server のログイン認証情報を作成します。[\[Windows ユーザーへのデータベース所有者権限とシステム管理権限の付与\]](#) を参照してください。

Windows ユーザーへのデータベース所有者権限とシステム管理権限の付与

JMP Server ホスト マシンに SQL Server のログイン情報を作成するだけでなく、JMP Server インスタンスをインストールする Windows ユーザー アカウントを作成する必要があります。この Windows ユーザー アカウントには、作成した SQL Server データベースの sysadmin とデータベース所有者権限を与える必要があります。

開始する前に

- インストールする JMP Server に SQL Server データベースが作成されていることを確認します。[「JMP Server の SQL Server データベースの作成」](#)を参照してください。
- JMP Server ホストに SQL Server のログイン情報が作成されていることを確認します。[「JMP Server ホストに SQL Server のログイン情報を作成する」](#)を参照してください。

手順

- 1 sysadmin (SA) として SQL Server Management Studio セッションにログインするか、SA 権限を持つユーザー アカウントにログインします。
- 2 [オブジェクト エクスプローラ] ペインで、JMP Server に作成した SQL サーバ インスタンスに接続します。
- 3 JMP Server のインストールに使用する Windows ユーザー アカウントに SQL Server のログイン情報を作成します。
 - a [セキュリティ] フォルダを展開し、[ログイン] を右クリックして [新しいログイン] を選択します。
 - b [ログイン - 新規作成] ダイアログ ボックスで、[検索] をクリックします。
 - c [ユーザーまたはグループの選択] ダイアログ ボックスで、JMP Server のインストールに使用する有効な Active Directory ユーザーを選択します。
 - d [ログイン - 新規作成] ダイアログ ボックの [ページを選択] で、[サーパロール] を選択し、[sysadmin] チェック ボックスを選択します。
 - e [OK] をクリックし、[ログイン - 新規作成] ダイアログ ボックスを閉じます。
- 4 Windows ユーザー アカウントに権限を付与します。
 - a 左側のペインで、[データベース] をクリックします。
 - b JMP Server インスタンスに作成したデータベースを選択して、[セキュリティ]、[ユーザー] の順にクリックします。
 - c [ユーザー] ペインで、Windows ユーザー ログインを右クリックし、コンテキスト メニューから [プロパティ] を選択します。
 - d [データベース ロール メンバーシップ] で、[db_owner] ロールを選択します。
 - e [OK] をクリックします。

新しいログイン情報が [オブジェクト エクスプローラ] ペインの [ログイン] フォルダの下に追加されます。

次に進む前に

[「JMP Server のインストール」](#) の情報を参考にして、JMP Server インスタンスをインストールします。

JMP Server のインストール

JMP Integrated Workflow 機能を使用するには、JMP Server と VMware JMP テクノロジー製品をインストールして構成する必要があります。

注 Horizon 7 バージョン 7.5 リリースでは、JMP Server のインスタンスを 1 つだけインストールできます。

この章では次のトピックについて説明します。

- [JMP Server のインストール](#)
- [JMP Server のアンインストール](#)

JMP Server のインストール

JMP Integrated Workflow 機能を使用する前に、JMP Server をインストールして構成する必要があります。

VMware Horizon 7 バージョン 7.5 以降をダウンロードすると、JMP Server インストーラ ファイルが含まれています。Horizon 7 バージョン 7.5 以降が正常にインストールされたら、JMP Server インストーラを個別に実行する必要があります。

開始する前に

- JMP Server をインストールに必要なコンポーネントがシステム要件を満たしていることを確認します。[第 3 章「JMP Server のシステム要件」](#)を参照してください。
- Windows Server ホストで JMP Server インストーラを実行するには、そのホスト システムの管理者権限を持つドメイン ユーザー アカウントを使用する必要があります。
- JMP Server インスタンスが使用する SQL Server データベースが作成され、このデータベースに対して適切なアクセス権があることを確認します。
- JMP Server のインストールに使用する JMP Server ホストと Windows ドメイン ユーザー アカウントに、SQL Server のログイン情報とアクセス権が設定されていることを確認します。[「JMP Server ホストに SQL Server のログイン情報を作成する」](#)を参照してください。
- JMP Integrated Workflow 機能で使用するセキュア/非セキュア HTTP ポート、ユーザー インターフェイス ポート、署名付き証明書の情報を収集します。
- 証明書認証局によって署名された TLS 証明書を取得して、JMP Server インストーラによってインストールされたデフォルトの TLS 証明書と置き換えます。

- JMP Server をインストールする前に、次の表を参照して、使用するインストールのタイプを決めます。

インストール タイプ	JMP Server インストーラによって実行されるアクション
本番環境	SQL Server Standard または Enterprise エディションを使用する JMP Server インスタンスを生成します。
開発環境または事前検証 (PoC) の環境	SQL Server Express を使用する JMP Server インスタンスを生成します。

- JMP Server をインストールする前に、McAfee Antivirus の除外リストに次のファイルを追加します。
 - 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

手順

- 1 [VMware JMP インストーラ] ウィザードを開始するには、JMP Server インストーラ ファイルを見つけて、ダブルクリックします。

JMP Server インストーラのファイル名は、**VMware-Jmp-Installer-e.x.p-<xxxxxxx>.exe** で、<xxxxxxx> はビルド番号です。例：**VMware-Jmp-Installer-e.x.p-7259616.exe**

注 インストール プロセスをログに記録する場合は、ログ ファイルを作成するフォルダをここでは、コマンド プロンプトから JMP Server インストーラを実行します。<Log_Folder_Path> はログ ファイルの作成先です。

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

- 2 [よろこ] ページで [次へ] をクリックし、VMware のライセンス条件に同意します。
- 3 HTTPS トラフィックを許可するには、[次へ] をクリックします。

注 JMP Server はポート 443 を使用します。オプションで、ポート 80、3000 ~ 3004、888、8889 も使用します。ポート 80 で HTTP トラフィックを許可するには、[HTTP を許可しますか?] チェック ボックスをオンにします。

4 SQL Server インスタンスとデータベース カタログ情報を入力します。

- a JMP Server に作成したデータベースに接続する SQL Server インスタンスの IP アドレスまたは名前を入力します。必要であれば、[参照] をクリックして選択します。
- b SQL Server データベースとの接続で使用する認証情報を選択します。

オプション	説明
[現在のユーザーの Windows 認証情報]	このインストール プロセスで使用している管理者の認証情報が、SQL Server データベース インスタンスとの接続で使用されます。
[次のログイン ID およびパスワードを利用したサーバ認証]	[ログイン ID] と [パスワード] に、SQL Server データベース インスタンスとの接続で使用する ID とパスワードを入力します。

注 使用するログイン認証情報は、JMP Server がアクセスする SQL Server インスタンスですすでに設定されている必要があります。[「JMP Server ホストに SQL Server のログイン情報を作成する」](#) を参照してください。

- c [データベース カタログ名] テキストボックスに、[「JMP Server の SQL Server データベースの作成」](#) で作成したデータベースの名前を入力します。必要であれば、[参照] をクリックして、使用可能なリストからデータベース カタログを選択します。

選択したデータベース カタログに、JMP Server サービスに関する情報が保存されます。

- d (オプション) 既存のデータベースを上書きする場合は、[既存のデータベースを上書きする] チェック ボックスをオンにします。

注 初めて JMP Server インストーラを実行した場合は、必要なデータベース テーブルが作成されます。ロード バランシングの目的で複数の JMP Server インスタンスを作成するためにインストーラを再度実行した場合、インストーラはデータベースの存在を確認し、テーブルを再作成しません。このオプションを選択すると、データベース内の既存の情報が上書きされます。

- e JMP Server と SQL Server インスタンス間でセキュアな通信を行うには、[SSL を有効にする] チェック ボックスがオンになっていることを確認します。デフォルトでは、[SSL の有効化] チェック ボックスが選択されています。

重要 [SSL の有効化] チェック ボックスが選択されている場合は、SQL Server で使用する TLS/SSL 証明書が JMP Server ホストの Windows ローカル証明書ストアにインポートされていることを確認します。そうしないと、JMP Server インストール プロセスが失敗し、「uem_migrate.bat ファイルの実行に失敗しました」というエラーが発生します。エラー ダイアログ ボックスで [OK] をクリックすると、インストールがロールバックします。

SQL Server の TLS/SSL 証明書をエクスポートまたはインポートする方法については、Microsoft TechNet の記事、[How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console](#) で「Enable encryption for a specific client」を参照してください。

- f [次へ] をクリックします。

5 [プログラムのインストール準備] ページで、[インストール] をクリックします。

6 インストールが正常に終了したら、[終了] をクリックします。

インストールに成功すると、Windows Server ホストに次の JMP Server サービスがインストールされ、開始します。

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

次に進む前に

新しくインストールされた JMP Server インスタンスとそれに関連する Horizon Connection Server の時間を同期します。[「Horizon 接続サーバと JMP Server ホスト間の時間の同期」](#) を参照してください。

JMP Server のアンインストール

問題を解決するために、JMP Server のアンインストールと再インストールが必要になる場合があります。

ここでは、他の方法で解決できない問題が発生した場合に JMP Server をアンインストールする方法について説明します。

開始する前に

- JMP Server のアンインストールに必要な管理者権限があることを確認します。
- JMP Server をアンインストールする前に、その JMP Server に関連付けられている User Environment Manager 構成共有をすべて削除します。『VMware Horizon Console の管理』で「User Environment Manager 構成共有情報の削除」を参照してください。

手順

- 1 Microsoft Windows の [プログラムと機能] コンソールを開きます。
たとえば、[スタート] > [設定] > [システム] > [アプリと機能] の順にクリックします。
- 2 インストールされているアプリケーションのリストから [VMware JMP] を選択します。
- 3 [アンインストール] をクリックし、ウィザードに従ってアンインストール手順を完了します。

次に進む前に

JMP Server を再インストールします。詳細については、[「JMP Server のインストール」](#) を参照してください。

JMP Server インスタンスの構成

JMP Server インスタンスのインストールに成功したら、構成タスクを実行して、JMP Server インスタンスが Horizon Connection Server で認証され、ネットワーク内の他のサーバと安全に通信できることを確認する必要があります。

この章では次のトピックについて説明します。

- [Horizon 接続サーバと JMP Server ホスト間の時間の同期](#)
- [JMP Server の TLS 証明書と暗号化スイートの構成](#)

Horizon 接続サーバと JMP Server ホスト間の時間の同期

サーバ間で認証プロセスを成功させるには、Horizon 接続サーバと JMP Server ホストの両方の時間を同期する必要があります。

Horizon Console のユーザー インターフェイスから JMP Integrated Workflow の機能にアクセスすると、JMP Server が Horizon 接続サーバから受信したトークンを認証し、次に Horizon 接続サーバが JMP Server からトークンを受信します。2 台のホスト間で時間が同期されていないと、Horizon 接続サーバは JMP Server から提供されたトークンを拒否し、JMP Integrated Workflow の機能が Horizon Console ユーザー インターフェイスから使用できなくなります。[JMP 設定] ペインに次のエラー メッセージが表示されます。

Horizon SSO トークンを検証できませんでした。

認証に成功するには、Horizon 接続サーバと JMP Server ホストの時間を共通の NTP (Network Time Protocol) サーバの時間を同期する必要があります。

手順

- 1 Windows ホストで、次の VMware Tool コマンドを使用します。

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

- 2 ESXi ホストで、ネットワーク タイム サーバと ESXi の時間を同期します。
 - a VMware Host Client を起動し、ESXi ホストに接続します。
 - b [構成] をクリックします。
 - c [システム] の下で、[時間の構成] を選択して [編集] をクリックします。

- d [Network Time Protocol を使用 (NTP クライアントの有効化)] を選択します。
- e [NTP サーバの追加] テキスト ボックスに、同期する 1 つ以上の NTP サーバの IP アドレスまたは完全修飾ドメイン名を入力します。

次に進む前に

JMP Server の TLS 証明書を設定します。[「JMP Server に TLS 証明書を設定するタスクの概要」](#) を参照してください。

JMP Server の TLS 証明書と暗号化スイートの構成

JMP Server インスタンスがネットワーク内の他のサーバと安全に通信を行うには、有効な証明書認証局 (CA) が署名した TLS 証明書を使用するように JMP Server インスタンスを構成する必要があります。セキュア接続を強化するため、他のサーバが受け入れ、JMP Server インスタンスとの通信で提案するデフォルトの暗号化スイートを変更できます。

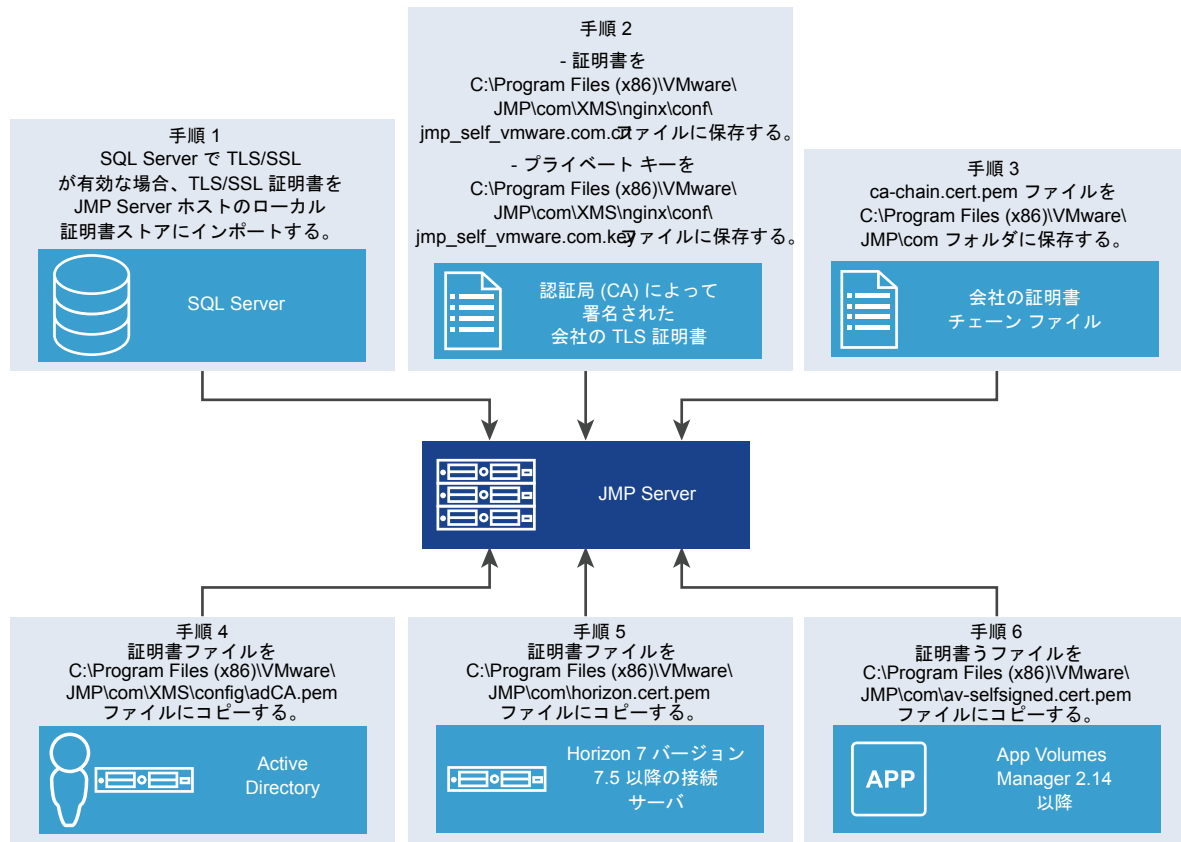
デフォルトでは、JMP Server インストーラは、インストールされている JMP Server インスタンスに自己署名 TLS サーバ証明書をインストールします。デフォルト証明書はテスト用に使用できます。本番環境で JMP Server インスタンスを使用する場合、できるだけ早くデフォルトの証明書を CA 署名付きの TLS サーバ証明書で置き換える必要があります。CA の署名がない証明書を使用すると、信頼されていないパーティがユーザーのサーバになりすましてトラフィックを傍受できる可能性があります。[「JMP Server に TLS 証明書を設定するタスクの概要」](#) を参照してください。

JMP Server に TLS 証明書を設定するタスクの概要

JMP Server のインストールに成功した後、有効な証明書認証局 (CA) によって署名された TLS サーバ証明書を JMP Server インスタンスで使用するため、いくつかのタスクを実行する必要があります。

このトピックで説明するタスク以外に、JMP Server の証明書を構成する場合、以下の図に示す手順が必要になります。特定の証明書を正常に構成するには、この概要で示すトピックの手順に従ってください。タスクの説明にオプションというマークが付いている場合は、そのタスクを実行して JMP Server 構成の安全性を強化するかどうかを決めます。証明書の構成を完了したら、Windows サービス マネージャを使用して、3 つの JMP Server サービスを再起動する必要があります。

図 6-1. JMP Server の証明書を構成する主な手順



- 1 SQL Server で TLS/SSL が有効な場合は、TLS/SSL 証明書が JMP Server のホストのローカル証明書ストアにインポートされていることを確認します。
- 2 JMP Server インストーラが生成した TLS サーバ証明書を置き換えます。

JMP Server インストーラが生成したデフォルトのサーバ証明書は自己署名で、組織のネットワークによって認識されていません。自己署名の証明書を CA から取得した有効な TLS 証明書に置き換えます。[「デフォルトの TLS 証明書の置き換え」](#)を参照してください。

有効な TLS Web サーバ証明書が組織にない場合は、CA から署名付き TLS サーバ証明書を取得します。Horizon 7 の TLS 証明書設定のシナリオの情報を参照してください。

- 3 組織のサーバ証明書が中間 CA によって署名されている場合は、組織の証明書チェーン ファイル **ca-chain.cert.pem** を使用するように JMP Server を構成します。これにより、JMP Server がネットワーク内の他のサーバを認証できるようになります。[「証明書チェーン ファイルを使用するように JMP Server を設定する」](#)を参照してください。

注 組織の TLS サーバ証明書が NodeJS で信頼されたルート CA に直接署名されている場合は、証明書チェーン ファイルまたはルート証明書ファイル (**ca.cert.pem**) を指定する必要はありません。

- 4 Active Directory サーバの証明書に署名する CA 証明書を取得して **adCA.pem** ファイルに保存し、このファイルを JMP Server XMS 構成フォルダに追加します。詳細については、[「Active Directory の証明書を使用するように JMP Server を構成する」](#)を参照してください。

- Horizon 接続サーバの CA 署名付き証明書を **horizon.cert.pem** ファイルにエクスポートし、このファイルを JMP Server ホーム フォルダに追加します。詳細については、[「Horizon 接続サーバ証明書を使用するように JMP Server を設定する」](#)を参照してください。

JMP Server は、**horizon.cert.pem** ファイルを使用して、信頼できるサーバとして接続サーバを認証し、接続が可能になります。

注 このタスクは、JMP Server インスタンスとやり取りする接続サーバ ポッドごとに完了する必要があります。エクスポートされた CA 署名付き証明書のコンテンツを 同じ **horizon.cert.pem** ファイルに追加します。

- JMP 割り当ての作成時に App Volumes AppStacks を割り当てる場合は、App Volumes Manager インスタンスの自己署名証明書を使用するように JMP Server インスタンスを構成します。これにより、App Volumes Manager インスタンスとの通信を保護できます。[「App Volumes Manager の自己署名証明書を使用するように JMP Server を構成する」](#)を参照してください。
- (オプション) JMP Server インスタンスがサポートするデフォルトの暗号化スイートを組織でサポートする暗号に変更します。[「JMP Server の暗号化スイートの構成」](#)を参照してください。
- (オプション) JMP Server で、より制限の厳しいクロスオリジン リソース共有 (CORS) ポリシーを有効にし、Horizon 7 接続サーバインスタンスとのセキュア通信の安全性を強化します。[「JMP Server により制限の厳しい CORS ポリシーを使用する」](#)を参照してください。
- Windows サービス マネージャを使用して、3 つの JMP Server サービスを再起動します。

サーバ証明書を構成したら、Horizon Console で JMP を構成し、JMP Integrated Workflow 機能を開始できます。『VMware Horizon Console の管理』の「JMP 設定の初期構成」を参照してください。

デフォルトの TLS 証明書の置き換え

JMP Server インストーラによってインストールされたデフォルトの TLS 証明書を証明書認証局 (CA) によって署名されている組織の TLS 証明書と置き換えます。

JMP Server インスタンスのインストールに成功すると、Web ブラウザで Horizon コンソールからアクセスできます。ただし、インストールされているデフォルトの TLS 証明書がネットワークで認識されていない場合は、JMP を最初に構成するときに、Web ブラウザのセキュリティ アラート ダイアログ ボックスが表示されます。テスト目的でデフォルトの自己署名証明書を使用することもできますが、JMP Server インスタンスとのセキュアな接続を行うため、デフォルトの証明書とキーを CA 署名付きの TLS 証明書とプライベート キーに置き換えます。

重要 JMP Server インストーラによって作成されたデフォルトの名前と異なるファイル名を証明書とキー ファイルに付ける場合は、新しいファイル名を使用するように JMP Server NGINX 構成ファイルを変更する必要があります。

開始する前に

- JMP Server をインストールします。[「JMP Server のインストール」](#)を参照してください。
- CA 署名付きの TLS 証明書を取得して、JMP Server インストーラによってインストールされたデフォルトの TLS 証明書と置き換えます。Microsoft Certreq や Windows 用 OpenSSL などの証明書ツールを使用すると、証明書を生成します。『Horizon 7 の TLS 証明書設定のシナリオ』の「認証局からの TLS 証明書の取得」を参照してください。

手順

- 1 JMP Server ホストで、Windows サービス マネージャ ツールを使用して 3 つの JMP Server サービスを停止します。
 - a Windows の [スタート] アイコンを右クリックし、[ファイル名を指定して実行] を選択します。
 - b [ファイル名を指定して実行] ダイアログ ボックスの [名前] テキスト ボックスに **services.msc** と入力し、[OK] をクリックします。
 - c [サービス] ウィンドウの [サービス (ローカル)] ペインで、次の 3 つ JMP Server サービスを見つけて、[停止] をクリックします。
 - VMware JMP API Service
 - VMware JMP File Share Service
 - VMware JMP Platform Services
- 2 JMP Server ホストの NGINX 構成フォルダに、認証局 (CA) 署名付き TLS サーバ証明書ファイルを **jmp_self_vmware.com.crt** という名前で保存します。

例 : C:\Program Files
(x86)\VMware\JMP\com\XMS\nginx\conf\jmp_self_vmware.com.crt
- 3 CA 署名付き TLS サーバ証明書に付属のプライベート キーを **jmp_self_vmware.com.key** という名前で保存します。

例 : C:\Program Files
(x86)\VMware\JMP\com\XMS\nginx\conf\jmp_self_vmware.com.key
- 4 (オプション) 予想される証明書ファイル名 (**jmp_self_vmware.com.crt** や **jmp_self_vmware.com.key**) と異なるファイル名を使用する場合は、新しいファイル名を使用するように NGINX 構成ファイルを変更する必要があります。
 - a C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\nginx.conf 構成ファイルを開きます。
 - b **jmp_self_vmware.com.crt** と **jmp_self_vmware.com.key** プロパティを見つけて、選択した新しいファイル名に置き換えます。
 - c **nginx.conf** ファイルを保存します。

Web ブラウザのセキュリティ アラート ダイアログ ボックスを表示せずに、JMP Integrated Workflow 機能に安全にアクセスできます。

次に進む前に

組織の証明書チェーン全体が中間 CA によって署名されている場合は、証明書チェーン ファイルを使用するように JMP Server インスタンスを構成します。[「証明書チェーン ファイルを使用するように JMP Server を設定する」](#)を参照してください。それ以外の場合は、Active Directory の証明書を使用するように JMP Server インスタンスを構成します。[「Active Directory の証明書を使用するように JMP Server を構成する」](#)を参照してください。

証明書チェーン ファイルを使用するように JMP Server を設定する

中間 CA が組織内のサーバの証明書に署名している場合、ルート証明書と中間証明書を含む組織の証明書チェーン全体を JMP Server インスタンスに設定できます。

開始する前に

- Windows サービス マネージャを使用して、次の 3 つの JMP Server サービスを停止します。

手順

- 1 組織全体の証明書チェーン ファイル (**ca chain.cert.pem**) を取得します。
- 2 **ca-chain.cert.pem** 証明書チェーン ファイルを **C:\Program Files (x86)\VMware\JMP\com** フォルダにコピーします。

証明書チェーンを配置すると、JMP Server インスタンスで Horizon 7 と App Volumes インスタンスを認証し、セキュアな通信を行うことができます。

次に進む前に

デスクトップ管理者が JMP Integrated Workflow 機能を使用するときに、JMP Server インスタンスで Active Directory サーバを認証できるように、Active Directory の証明書で JMP Server インスタンスを設定できます。[「Active Directory の証明書を使用するように JMP Server を構成する」](#) を参照してください。

Active Directory の証明書を使用するように JMP Server を構成する

Horizon Console が接続している Active Directory の検証を JMP Server で行うには、その Active Directory サーバの証明書を使用するように JMP Server を構成する必要があります。

Active Directory ドメインのルート CA 証明書を **adCA.pem** ファイルという証明書ファイルにエクスポートし、このファイルを JMP Server XMS 設定フォルダに配置する必要があります。

開始する前に

- JMP Server をインストールする必要があります。
- SSL 経由の LDAP (LDAPS) または StartTLS (TLS 経由の LDAP) には、Active Directory を構成する必要があります。
- Active Directory ドメインのルート CA 証明書。証明書が PEM (Base64 エンコード) 形式でない場合は、OpenSSL のドキュメント（または類似ドキュメント）を参照して、ファイルを PEM 形式に変換してください。

注 異なるドメインの複数のルート証明書がある場合、各ファイルのコンテンツを 1 つの **.pem** ファイルにコピーすると、すべての PEM 形式の証明書を 1 つのファイルにまとめることができます。

手順

- 1 PEM 形式の証明書ファイルの名前が **adCA.pem** であることを確認します。

2 **adCA.pem** ファイルを JMP Server XMS 設定フォルダにコピーします。

例: **C:\Program Files (x86)\VMware\JMP\com\XMS\config\adCA.pem**。

JMP Server インスタンスに構成された Active Directory 証明書により、Active Directory が信頼できるサーバとして認識され、Horizon Console ユーザーが JMP Integrated Workflow 機能を正常に使用できるようになります。

次に進む前に

デスクトップ管理者が JMP Integrated Workflow 機能を使用するときに、JMP Server インスタンスが接続サーバの認証を行うように、接続サーバ証明書を使用して JMP Server を構成します。[「Horizon 接続サーバ証明書を使用するように JMP Server を設定する」](#)を参照してください。

Horizon 接続サーバ証明書を使用するように JMP Server を設定する

Horizon Console が接続している Horizon 7 接続サーバの検証を JMP Server で実行するには、Horizon 7 接続サーバ証明書を使用するように JMP Server を構成する必要があります。

horizon.cert.pem ファイルという証明書ファイルに Horizon 7 接続サーバ証明書をエクスポートし、このファイルを JMP Server ホーム フォルダに配置します。

重要 エクスポートされた CA 署名付き証明書のコンテンツを 同じ **horizon.cert.pem** ファイルに追加します。

CA 署名付き証明書または自己署名付きの Horizon 7 接続サーバ証明書を追加するときにも、同じ手順を行います。

開始する前に

- JMP Server をインストールする必要があります。
- Horizon 7 接続サーバに対する管理アクセスが権限が必要です。

手順

- 1 インストールした Horizon Console や JMP Server と Horizon 7 接続サーバが接続できるように、Windows Server ホストにログインします。
- 2 Windows の [スタート] アイコンを右クリックし、[ファイル名を指定して実行] を選択して **mmc.exe** を入力します。
MMC ユーティリティのウィンドウが表示されます。
- 3 証明書スナップインを追加します。
 - a **[コンソール ルート]** ウィンドウで、[ファイル]-[スナップインの追加/削除] の順に選択します。
 - b **[スナップインの追加または削除]** ウィンドウで、[使用可能なスナップイン] ペインから [証明書] を選択して、[追加] をクリックします。
 - c 証明書を追加したら、[OK] をクリックします。
 - d 証明書スナップイン ウィンドウで、[コンピュータ アカウント] を選択し、[次へ] をクリックします。

- e コンピュータの選択ウィンドウで、[ローカル コンピュータ] を選択し、[完了] をクリックします。
証明書 (ローカル コンピュータ) スナップインが、[選択されたスナップイン] ペインに追加されます。
 - f **[スナップインの追加または削除]** ダイアログ ボックスを閉じるには、[OK] をクリックします。
- 4 コンソール ルート ウィンドウに戻り、[コンソール ルート] - [証明書 (ローカル コンピュータ)] の順に選択し、[個人用] - [証明書] の順に選択します。左側のペインの [] フォルダにコンテンツが表示されます。
- 5 Horizon 接続サーバ証明書をエクスポートします。
- a 証明書コンテンツのペインで、フレンドリ名が **vdm** の証明書を見つけます。
この証明書は、Horizon 接続サーバに属しています。
 - b 証明書を右クリックし、[すべてのタスク] - [エクスポート] の順に選択します。
 - c [証明書のエクスポート ウィザード] ダイアログ ボックスで、[次へ] をクリックします。
 - d [いいえ、プライベート キーをエクスポートしません] を選択して、[次へ] をクリックします。
 - e [Base-64 エンコード X.509 (.CER)] を選択して、[次へ] をクリックします。
 - f ファイル名として **horizon.cert.pem** を入力し、[参照] をクリックして、エクスポートする証明書の保存先フォルダに移動します。

重要 エクスポートした証明書ファイルは、**.pem** 拡張子を付けて保存する必要があります。拡張子に **.cer** または **.crt** は使用[できません]。必要に応じて、エクスポートした証明書ファイルをテキスト エディタで開き、**horizon.cert.pem** という名前で保存します。

- g [次へ] をクリックして [完了] をクリックし、**[証明書のエクスポート ウィザード]** ウィンドウを閉じます。
証明書が正常にエクスポートされます。
- 6 エクスポートした **horizon.cert.pem** 証明書を保存した場所に移動し、JMP Server ホーム フォルダにコピーします。

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

JMP Server インスタンスに構成された接続サーバの証明書により、接続サーバが信頼できるサーバとして認識され、Horizon Console ユーザーが JMP Integrated Workflow 機能を正常に使用できるようになります。

次に進む前に

表示されるオプションのタスクを確認して「[JMP Server に TLS 証明書を設定するタスクの概要](#)」に表示されたオプションのタスクを確認し、タスクの完了が必要かどうかを確認します。必要な構成タスクがすべて完了したら、JMP Server サービスを再起動し、JMP 設定を構成します。詳細については、『VMware Horizon Console の管理』で「JMP 設定の初期構成」を参照してください。

App Volumes Manager の自己署名証明書を使用するように JMP Server を構成する

JMP 割り当ての作成時に App Volumes AppStacks を割り当てる場合は、App Volumes Manager インスタンスの自己署名証明書を使用するように JMP Server インスタンスを構成します。これにより、App Volumes Manager インスタンスとの通信を保護できます。

JMP Server が使用できるように、App Volumes Manager インスタンスの自己署名証明書を **av-selfsigned.cert.pem** という名前のファイルにエクスポートする必要があります。

開始する前に

- JMP Server をインストールする必要があります。
- App Volumes Manager インスタンスに対する管理アクセス権限、またはこのインスタンスを管理するロードバランサに対する管理アクセス権限が必要です。

手順

- 1 JMP Server ホストで Web ブラウザーを使用して、環境内の App Volumes Manager インスタンスにログインするか、App Volumes Manager インスタンスを管理するロードバランサにログインします。
- 2 App Volumes Manager インスタンスまたはロードバランサで使用する自己署名証明書の情報を検索するには、Web ブラウザの [サイト情報] ダイアログボックスで自己署名証明書をエクスポートして、**C:\Program Files (x86)\VMware\JMP\com\av-selfsigned.cert.pem** ファイルに保存します。

重要 エクスポートした証明書ファイルは、**.pem** 拡張子を付けて保存する必要があります。拡張子に **.cer** または **.crt** は使用[できません]。必要に応じて、エクスポートした証明書ファイルをテキストエディタで開き、**av-selfsigned.cert.pem** という名前で保存します。

たとえば、Google Chrome Web ブラウザの場合は、証明書のエクスポートウィザードを使用して、**C:\Program Files (x86)\VMware\JMP\com** フォルダの **av-selfsigned.cert.pem** ファイルに App Volumes Manager 自己署名証明書ファイルをコピーします。

- 3 JMP Server のセキュリティ強化に必要な TLS 証明書を構成したら、JMP Server サービスを再起動します。残りの TLS 証明書の構成作業については、[JMP Server に TLS 証明書を設定するタスクの概要](#) を参照してください。

JMP Server の暗号化スイートの構成

JMP Server には、JMP Server、Horizon Connection Server、App Volumes、User Environment Manager のインスタンス間で承諾され、提案されるデフォルトの暗号化スイートが設定されています。JMP Server がサポートしているデフォルト暗号化スイートは、必要に応じて、組織でサポートする暗号に変更できます。

<https://www.openssl.org/docs/man1.0.2/apps/ciphers.html#CIPHER-LIST-FORMAT> で定義されている形式で暗号化リスト指定する必要があります。デフォルトの暗号化方式リストを次に示します。

```
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
```

手順

- 1 JMP Server ホストで、Windows サービス マネージャ ツールを使用して 3 つの JMP Server サービスを停止します。
 - a Windows の [スタート] アイコンを右クリックし、[ファイル名を指定して実行] を選択します。
 - b [ファイル名を指定して実行] ダイアログ ボックスの [名前] テキスト ボックスに **services.msc** と入力し、[OK] をクリックします。
 - c [サービス] ウィンドウの [サービス (ローカル)] ペインで、次の 3 つの JMP Server サービスを見つけ、各サービスで [停止] をクリックします。
 - VMware JMP API Service
 - VMware JMP File Share Service
 - VMware JMP Platform Services
- 2 C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf フォルダに移動します。
- 3 変更する前に、**nginx.conf** ファイルのバックアップ コピーを作成します。
- 4 **nginx.conf** ファイルをメモ帳で開きます。
- 5 **ssl_ciphers** で始まる行を見つけます。必要に応じて、暗号化リストを変更します。
- 6 **nginx.conf** ファイルに行った変更を保存します。
- 7 Windows サービス マネージャ ツールを使用して JMP Server サービスを再起動し、新しい暗号化リストを有効にします。

JMP Server により制限の厳しい CORS ポリシーを使用する

JMP Server インスタンスで、より制限の厳しいクロスオリジン リソース共有 (CORS) ポリシーを使用するには、JMP Server と信頼関係のある Horizon 7 接続サーバ インスタンスのホワイトリストを作成します。

デフォルトでは、「[証明書チェーン ファイルを使用するように JMP Server を設定する](#)」の手順で設定した証明書チェーン ファイルにある証明書を使用している場合、Horizon 7 接続サーバ インスタンスは JMP Server インスタンスにアクセスできます。承認リストにある Horizon 7 接続サーバ インスタンスだけに JMP Server へのアクセスが許可されるように、次の手順を実行します。

手順

- 1 テキスト エディタで **C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\nginx.conf** にある NGINX 構成ファイルを開きます。
- 2 次のテキストを含む行 (2 箇所) に移動し、先頭の **#** マークを削除してコメントを解除します。

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

- 3 次のテキストを含む行 (2 箇所) に移動し、先頭に **#** マークを付けてコメントにします。

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

- 4 接続サーバインスタンスの承認リストをホワイトリストに追加します。

- a ファイルで次のコンテンツを見つけます。

```
# 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 **default ''**; 行の後に、ホワイトリストに追加する接続サーバインスタンスごとに 1 行ずつ追加します。

たとえば、JMP Server への接続を許可する接続サーバインスタンスのドメイン名が **www.testhorizon.com** と **www.prodhorizon.com** の場合、追加する行は次のようになります (太字の部分)。

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

- 5 **nginx.conf** ファイルに行った変更を保存します。
- 6 Windows サービス マネージャを使用して、JMP Platform サービスを再起動します。

JMP Server のインストール後のデータベース パスワードの更新

7

JMP Server の初回インストールで使った SQL Server データベースのパスワードを変更するには、VMware JMP Server サービスが使用するデータベースのパスワード情報も更新する必要があります。

この章では次のトピックについて説明します。

- [VMware JMP プラットフォーム サービスのデータベース パスワードの更新](#)
- [VMware JMP ファイル共有サービスのデータベース パスワードの更新](#)

VMware JMP プラットフォーム サービスのデータベース パスワードの更新

JMP Server をインストールするときに使った SQL Server データベースのパスワードを変更する場合は、SQL Server データベースに接続している VMware JMP プラットフォーム サービスのデータベース パスワードも更新する必要があります。

開始する前に

JMP Server ホストのデータベース情報を変更する場合は、適切な管理者権限があることを確認します。

手順

- 1 JMP Server ホストで、Windows サービス マネージャ ツールを使用して **VMware JMP Platform Services** プロセスを停止します。
 - a Windows の [スタート] アイコンを右クリックし、[ファイル名を指定して実行] を選択します。
 - b [ファイル名を指定して実行] ダイアログ ボックスの [名前] テキスト ボックスに **services.msc** と入力し、[OK] をクリックします。
 - c [サービス] ウィンドウの [サービス (ローカル)] ペインで、**VMware JMP Platform Services** を探し、[停止] をクリックします。
- 2 次の実行可能ファイルの中で JMP Server ホストに適切な実行可能ファイルをダブルクリックし、[ODBC データソースの管理者] ウィンドウを開きます。
 - C:\Windows\SysWow64\odbcad64.exe
 - C:\Windows\system32\odbcad32.exe

- 3 [ODBC データ ソースの管理者] ウィンドウで [システム DSN] をクリックし、[ユーザー データ ソース] ペインで **svmanager** を選択します。

- 4 [構成] をクリックします。

Microsoft SQL Server 用の DSN の設定ウィザードが表示されます。

- 5 [次へ] をクリックします。

注意 データ ソースの [名] または [サーバ] テキスト ボックスの既存の情報は変更しないでください。

- 6 [ユーザーが入力する SQL Server 用のログイン ID とパスワードを使う] が選択されていることを確認します。

- 7 [パスワード] テキスト ボックスに新しいパスワードを入力して、[次へ] をクリックします。

- 8 デフォルトのデータベース情報に表示されている情報に変更せずに、[次へ] をもう一度クリックします。

- 9 [終了] をクリックします。

[ODBC Microsoft SQL Server セットアップ] のサマリ ウィンドウに、構成の詳細が表示されます。

- 10 サマリ情報を確認します。VMware JMP Platform Services サービスのパスワードの変更に進むには、[OK] をクリックします。

- 11 VMware JMP Platform Services サービスを再起動する前に、VMware JMP プラットフォーム サービス データベースの構成ファイルに新しいパスワードの情報を追加します。

- a 管理者としてテキスト エディタを使用し、**C:\Program Files (x86)\VMware\JMP\com\XMS\config\database.yml** にあるデータベース構成ファイルを開きます。
- b ユーザー名プロパティの行に移動し、パスワード プロパティの行の後に新しい行を挿入します。
- c 作成したパスワードの情報を入力します。次の例のようになります。

```
[password:] new_password
```

重要 VMware JMP Platform Services サービスが再起動すると、このパスワード情報は **database.yml** ファイルから自動的に削除されます。

- 12 VMware JMP Platform Services サービスを再起動します。

- a Windows の [スタート] アイコンを右クリックし、[ファイル名を指定して実行] を選択します。
- b [ファイル名を指定して実行] ダイアログ ボックスの [名前] テキスト ボックスに **services.msc** と入力し、[OK] をクリックします。
- c [サービス] ウィンドウの [サービス (ローカル)] ペインで、**VMware JMP Platform Services** を探し、[開始] をクリックします。

次に進む前に

この操作をまだ行っていない場合は、VMware JMP ファイル共有サービスで使用するデータベース ログイン アカウント情報も更新する必要があります。[「VMware JMP ファイル共有サービスのデータベース パスワードの更新」](#)を参照してください。

VMware JMP ファイル共有サービスのデータベース パスワードの更新

JMP Server をインストールするときに使用した SQL Server データベースのパスワードを変更する場合は、SQL Server データベースに接続している VMware JMP ファイル共有サービスのデータベース パスワードも更新する必要があります。

開始する前に

JMP Server ホストのデータベース情報を変更する場合は、適切な管理者権限があることを確認します。

手順

- 1 JMP Server ホストで、Windows サービス マネージャ ツールを使用して **VMware JMP File Share Service** プロセスを停止します。
 - a Windows の [スタート] アイコンを右クリックし、[ファイル名を指定して実行] を選択します。
 - b [ファイル名を指定して実行] ダイアログ ボックスの [名前] テキスト ボックスに **services.msc** と入力し、[OK] をクリックします。
 - c [サービス] ウィンドウの [サービス (ローカル)] ペインで、**VMware JMP File Share Service** を探し、[停止] をクリックします。
- 2 VMware JMP ファイル共有サービスが使用するパスワードを更新します。次の情報を使用して JMP Server のインストール中に使用した SQL Server 接続タイプに応じて実行する手順を確認します。

- SQL 認証接続モードの場合：

- 1 管理者としてコマンド プロンプト ウィンドウを開きます。
- 2 次のコマンドをコピーして <password> の情報を変更し、新しいパスワード値で置き換えます。

```
SET NODE_ENV=jump.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 コマンド プロンプト ウィンドウにコマンドを貼り付け、Enter キーを押します。

- Windows 認証接続モード：

- 1 **C:/Program Files (x86)/VMware/JMP/com/uem** フォルダに移動し、テキスト エディタで **db.json** ファイルを開きます。

- 2 既存のファイルの内容を次の内容で置き換えます。ここで、<IP address> は SQL サーバ ホストの IP アドレス、<Database name> は有効なデータベース名です。

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

- 3 ファイルを保存します。

3 VMware JMP File Share Service を再起動します。

- a Windows の [スタート] アイコンを右クリックし、[ファイル名を指定して実行] を選択します。
- b [ファイル名を指定して実行] ダイアログ ボックスの [名前] テキスト ボックスに **services.msc** と入力し、[OK] をクリックします。
- c [サービス] ウィンドウの [サービス (ローカル)] ペインで、**VMware JMP File Share Service** を探し、[開始] をクリックします。

次に進む前に

この操作をまだ行っていない場合は、VMware JMP プラットフォーム サービスで使用するデータベース ログインアカウント情報も更新する必要があります。[「VMware JMP プラットフォーム サービスのデータベース パスワードの更新」](#)を参照してください。

JMP Server のトラブルシューティング

JMP Server インスタンスのインストール、構成または登録時にエラー メッセージが表示される場合があります。この章のトラブルシューティング情報を使用できます。

JMP Server 使用不可エラー

JMP Server インスタンスに接続できません。

問題

Horizon Console を使用して、JMP Server インスタンスを登録しているときに、「**入力した JMP Server は利用できません。入力を修正してから、後でやり直してください。**」というエラー メッセージが表示される場合があります。

原因

このエラー メッセージが表示された原因はいくつか考えられます。原因と回避策を確認するには、次のセクションの情報を kullanarak ください。

解決方法

- 1 証明書が正しく構成されていることを確認します。
「[JMP Server の TLS 証明書と暗号化スイートの構成](#)」の情報を確認します。
- 2 JMP Server URL の登録を行った後に、Web ブラウザからの HTTP 応答を確認します。

次の出力のような HTTP 応答を受信したとします。

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

この場合、次の手順に従って、Horizon Console へのログイに使用したユーザー アカウントに適切な管理者権限を付与されていることを確認します。

- a Horizon Administrator で、[View 構成] > [管理者] の順に選択します。
- b [管理者] ペインで、管理者ユーザー アカウントが <domain-name>\Administrator と表示され (BUILTIN\Administrator ではありません)、このアカウントに完全な管理者権限が割り当てられていることを確認します。

- c BUILTIN\Administrators が表示されている場合は、[VMware Horizon 7 バージョン 7.5 リリース ノート](#)に記載されている回避策を行います。

管理者権限の管理方法については、『Horizon 7 の管理』ドキュメントで「権限の管理と確認」を参照してください。

- 3 Web ブラウザの HTTP 応答の JSON Web トークン (JWT) メッセージに、`{"code": 403,"error":"Error: Unable to verify Horizon JWT","error_code":"1044","error_type":"horizonJwtVerificationError"}` のようなエラー メッセージが含まれる場合は、JMP Server ホストと Horizon Connection Server ホスト間で時刻が同期されていることを確認します。

[「Horizon 接続サーバと JMP Server ホスト間の時間の同期」](#) の情報を使用します。