

Guide d'installation et de configuration de VMware Horizon JMP Server

Modifié le 19 juin 2018
VMware Horizon 7 7.5



vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

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

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

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

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Copyright © 2018 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

Table des matières

1	Guide d'installation et de configuration de VMware Horizon JMP Server	5
2	Présentation des tâches d'installation et de configuration de JMP Server	6
3	Configuration système requise pour JMP Server	8
	Composants de la technologie JMP requis	8
	Configuration matérielle requise pour JMP Server	8
	Système d'exploitation pris en charge pour JMP Server	9
	Exigences de réseau pour JMP Server	9
	Configuration requise de la base de données pour JMP Server	10
	Navigateur Web pris en charge pour JMP Integrated Workflow	11
4	Préparation de la base de données SQL Server et de la connexion pour JMP Server	12
	Créer une base de données SQL Server pour JMP Server	12
	Créer une connexion SQL Server pour l'hôte JMP Server	13
	Créer une connexion d'authentification Windows SQL Server pour l'hôte JMP Server	14
	Créer une connexion d'authentification SQL Server pour l'hôte JMP Server	15
	Octroi d'autorisations au propriétaire de la base de données et à l'administration système pour l'utilisateur Windows	16
5	Installation de JMP Server	18
	Installer JMP Server	18
	Désinstaller JMP Server	21
6	Configuration de l'instance de JMP Server	23
	Synchroniser l'heure entre des hôtes de Serveur de connexion Horizon et de JMP Server	23
	Configuration de certificats TLS et de suites de chiffrement pour JMP Server	24
	Présentation des tâches de configuration des certificats TLS pour JMP Server	24
	Remplacer le certificat TLS par défaut	26
	Configurer JMP Server pour utiliser un fichier de chaîne de certificats	28
	Configurer JMP Server pour qu'il utilise le certificat pour Active Directory	29
	Configurer JMP Server pour qu'il utilise le certificat du Serveur de connexion Horizon	30
	Configurer JMP Server pour qu'il utilise le certificat auto-signé d' App Volumes Manager	31
	Configuration de suites de chiffrement pour JMP Server	32
	Utiliser une stratégie CORS plus restrictive sur votre JMP Server	33

- 7 Mise à jour du mot de passe de base de données après l'installation de JMP Server 35**
 - [Mettre à jour le mot de passe de base de données pour VMware JMP Platform Services 35](#)
 - [Mettre à jour le mot de passe de base de données pour VMware JMP File Share Service 37](#)
- 8 Dépannage de votre JMP Server 39**
 - [Erreur JMP Server n'est pas disponible 39](#)

Guide d'installation et de configuration de VMware Horizon JMP Server

1

Guide d'installation et de configuration de VMware Horizon JMP Server explique comment installer et configurer VMware Horizon[®] Just-in-Time Management Platform (JMP) Server. Une fois JMP Server installé et les paramètres JMP configurés, vous pouvez commencer à définir des attributions JMP à l'aide des fonctionnalités de JMP Integrated Workflow dans VMware Horizon Console.

Les informations contenues dans ce document sont conçues pour les personnes qui souhaitent installer JMP Server. Elles sont destinées aux administrateurs système Windows expérimentés qui connaissent bien le fonctionnement des centres de données et la technologie des machines virtuelles.

Présentation des tâches d'installation et de configuration de JMP Server

2

Vous devez effectuer certaines tâches avant et après l'installation d'Horizon JMP Server et avant de pouvoir commencer à utiliser les fonctionnalités d'Horizon JMP Integrated Workflow.

La liste suivante fournit une description générale des tâches que vous devez effectuer. Les procédures pour réaliser ces tâches sont décrites dans les rubriques qui suivent cette présentation.

- 1 Vérifiez que la configuration système requise de JMP Server est respectée. Reportez-vous à la section [Chapitre 3 Configuration système requise pour JMP Server](#).
- 2 Créez une base de données SQL Server qui est utilisée pour stocker des informations sur les services JMP Server qui sont créés lors de l'installation. Reportez-vous à la section [Créer une base de données SQL Server pour JMP Server](#).
- 3 Créez la connexion SQL Server qui est utilisée par l'hôte JMP Server pour vous connecter à la base de données SQL Server que vous avez créée à l'étape précédente. Pour plus d'informations, reportez-vous à la section [Créer une connexion SQL Server pour l'hôte JMP Server](#).
- 4 Vérifiez que la connexion d'utilisateur Windows qui est utilisée pour installer JMP Server dispose des privilèges suffisants pour modifier la base de données SQL Server que vous avez créée pour stocker des informations pour les services JMP Server. Reportez-vous à la section [Octroi d'autorisations au propriétaire de la base de données et à l'administration système pour l'utilisateur Windows](#).
- 5 (Facultatif) Si le serveur SQL Server utilisé dans les étapes précédentes utilise le chiffrement TLS, importez son certificat TLS dans le magasin de certificats local Windows sur l'hôte JMP Server. Reportez-vous à la section « Activer le chiffrement pour un client spécifique » de l'article [Comment activer le chiffrement SSL pour une instance de SQL Server à l'aide de la console MMC](#) de Microsoft TechNet pour en savoir plus sur l'exportation et l'importation du certificat TLS de SQL Server.
- 6 Installez JMP Server. Reportez-vous à la section [Installer JMP Server](#).
- 7 Synchronisez l'heure entre votre hôte Horizon Connection Server et l'hôte Windows pour votre instance de JMP Server. Reportez-vous à la section [Synchroniser l'heure entre des hôtes de Serveur de connexion Horizon et de JMP Server](#).
- 8 Configurez les certificats TLS pour que votre instance de JMP Server communique en toute sécurité avec les instances du Serveur de connexion VMware Horizon 7, VMware App Volumes™ Manager, VMware User Environment Manager™ et d'autres systèmes dans le réseau de votre organisation. Reportez-vous à la section [Configuration de certificats TLS et de suites de chiffrement pour JMP Server](#).

- 9 (Facultatif) Modifiez les suites de chiffrement par défaut que votre instance de JMP Server prend en charge par les suites de chiffrement que votre organisation prend en charge. Reportez-vous à la section [Configuration de suites de chiffrement pour JMP Server](#).
- 10 (Facultatif) Utilisez une stratégie plus restrictive de partage des ressources cross-origin (CORS) sur votre instance de JMP Server pour une communication sécurisée ajoutée avec votre instance du Serveur de connexion Horizon 7. Reportez-vous à la section [Utiliser une stratégie CORS plus restrictive sur votre JMP Server](#).
- 11 À l'aide du Gestionnaire système Windows, redémarrez les services JMP Server avant de configurer les paramètres JMP à l'aide de la section « Configurer les paramètres JMP pour la première fois » dans le document *Administration de VMware Horizon Console*.

Configuration système requise pour JMP Server

3

Des exigences matérielles et logicielles spécifiques doivent être satisfaites avant que VMware Horizon JMP Server puisse être installé et que les fonctionnalités de JMP Integrated Workflow puissent être utilisées.

Ce chapitre aborde les rubriques suivantes :

- [Composants de la technologie JMP requis](#)
- [Configuration matérielle requise pour JMP Server](#)
- [Système d'exploitation pris en charge pour JMP Server](#)
- [Exigences de réseau pour JMP Server](#)
- [Configuration requise de la base de données pour JMP Server](#)
- [Navigateur Web pris en charge pour JMP Integrated Workflow](#)

Composants de la technologie JMP requis

Les versions prises en charge des produits VMware qui constituent la technologie JMP doivent être installées pour que vous puissiez installer JMP Server et utiliser les fonctionnalités de JMP Integrated Workflow.

Les versions suivantes des produits VMware doivent être installées pour que vous puissiez commencer l'installation de JMP Server.

- VMware Horizon 7 version 7.5 ou version ultérieure
- VMware App Volumes 2.14 ou version ultérieure
- VMware User Environment Manager 9.2.1 ou version ultérieure
- VMware Identity Manager™ 2.9.2 ou version ultérieure (pour l'intégration à VMware Workspace™ ONE™)

Configuration matérielle requise pour JMP Server

Vous devez installer JMP Server sur une machine physique ou virtuelle dédiée qui répond à des exigences matérielles spécifiques.

Le tableau suivant répertorie la configuration matérielle minimale requise pour une instance de JMP Server dans un environnement de production.

Tableau 3-1. Configuration matérielle requise d'Horizon JMP Server pour un environnement de production

Composant matériel	Configuration minimale requise dans un environnement de production
Processeur	CPU à 4 cœurs
Mémoire	8 Go
Stockage	100 Go

Le tableau suivant répertorie la configuration matérielle minimale requise pour une instance de JMP Server dans une validation technique ou un environnement de laboratoire.

Tableau 3-2. Configuration matérielle requise d'Horizon JMP Server pour un environnement de laboratoire

Composant matériel	Configuration minimale requise dans un environnement de laboratoire
Processeur	CPU à 4 cœurs
Mémoire	4 Go
Stockage	25 Go

Système d'exploitation pris en charge pour JMP Server

Vous devez installer JMP Server sur un système d'exploitation Windows Server pris en charge.

Les deux types d'installation de JMP Server, validation technique et de production, sont pris en charge sur les systèmes d'exploitation Windows Server suivants.

Tableau 3-3. Système d'exploitation pris en charge pour JMP Server

Système d'exploitation	Version	Édition
Windows Server 2008 R2 SP1	64 bits	Standard
		Enterprise
		Datacenter
Windows Server 2012 R2	64 bits	Standard
		Datacenter
Windows Server 2016	64 bits	Standard
		Datacenter

Exigences de réseau pour JMP Server

La machine physique ou virtuelle sur laquelle vous prévoyez d'installer JMP Server doit pouvoir atteindre tous les points de terminaison de produit pour tous les points de distribution sur votre réseau.

Avant de commencer à utiliser les fonctionnalités de JMP Integrated Workflow, la sécurité et l'authentification par certificat signé par une autorité de certification doivent déjà être configurées pour l'instance de JMP Server, de même pour tous les points de terminaison de technologie qui interagissent avec votre instance de JMP Server. Pour plus d'informations, reportez-vous à [Configuration de certificats TLS et de suites de chiffrement pour JMP Server](#).

Configuration requise de la base de données pour JMP Server

Le programme d'installation de JMP Server requiert des versions de base de données SQL Server spécifiques pour effectuer l'installation de JMP Server.

JMP Server prend en charge les versions et éditions suivantes de SQL Server dans les deux environnements de charge de travail pris en charge : validation technique ou production.

Tableau 3-4. Configuration requise de la base de données pour JMP Server

Type de charge de travail	Serveur de base de données	Version	Édition
Validation technique	SQL Server Express 2014	64 bits	Libre
Production	SQL Server 2012 (SP1, SP2, SP3 et SP4)	64 bits	Standard et Entreprise
Production	SQL Server 2014 (SP1 et SP2 avec CU7 ou version ultérieure)	64 bits	Standard et Entreprise
Production	SQL Server 2016 (SP1 avec CU6 ou version ultérieure)	64 bits	Standard et Entreprise

Avant d'exécuter le programme d'installation de JMP Server, vous devez créer la base de données SQL Server qui utilise le programme d'installation de JMP Server pendant le processus d'installation. Reportez-vous à la section [Créer une base de données SQL Server pour JMP Server](#) pour plus d'informations.

Vous devez également fournir les informations d'identification de connexion que le programme d'installation de JMP Server doit utiliser pour se connecter à la base de données SQL Server que vous avez créée. Vous pouvez sélectionner le type d'authentification que le programme d'installation de JMP Server utilise. La valeur par défaut utilisée est l'authentification Windows. Si vous sélectionnez l'authentification Windows ou l'authentification SQL Server, les informations d'identification de connexion que le programme d'installation de JMP Server utilise doivent déjà exister dans l'instance de SQL Server avant de commencer l'installation de JMP Server. Reportez-vous à la section [Créer une connexion SQL Server pour l'hôte JMP Server](#) pour plus d'informations.

De plus, vous devez créer une connexion SQL Server pour le compte d'utilisateur Windows Server que vous prévoyez d'utiliser pour installer le JMP Server. Cet utilisateur de Windows doit être configuré pour que les informations d'identification appropriées modifient la base de données SQL Server que vous avez créée.

Si votre serveur SQL Server est activé avec le chiffrement TLS, vous devez exporter son certificat TLS et importer le certificat dans votre instance de JMP Server pour permettre une communication chiffrée avec le serveur SQL Server.

Navigateur Web pris en charge pour JMP Integrated Workflow

Vous accédez à l'interface utilisateur de JMP Integrated Workflow à l'aide de la Console VMware Horizon, qui est une application Web installée avec le Serveur de connexion VMware Horizon 7 version 7.5 et ultérieure.

Les navigateurs Web suivants sont pris en charge pour une utilisation avec les fonctionnalités de JMP Integrated Workflow.

- Google Chrome (dernières versions prises en charge)
- Mozilla Firefox (dernières versions prises en charge)
- Internet Explorer 10 et 11
- Microsoft Edge

Préparation de la base de données SQL Server et de la connexion pour JMP Server

4

Avant d'exécuter le programme d'installation de JMP Server, vous devez créer une base de données SQL Server que votre instance de JMP Server va utiliser. Vous devez également créer le compte de connexion SQL Server requis par le programme d'installation de JMP Server pour vous connecter à cette base de données SQL Server. Le compte de connexion Windows Server utilisé pour exécuter le programme d'installation de JMP Server doit également disposer d'un accès approprié à la base de données SQL Server que vous avez créée pour le JMP Server.

Ce chapitre aborde les rubriques suivantes :

- [Créer une base de données SQL Server pour JMP Server](#)
- [Créer une connexion SQL Server pour l'hôte JMP Server](#)
- [Octroi d'autorisations au propriétaire de la base de données et à l'administration système pour l'utilisateur Windows](#)

Créer une base de données SQL Server pour JMP Server

Des informations sur les services JMP Server et les attributions JMP que les administrateurs de postes de travail Horizon créent sont stockées dans une base de données SQL Server. Vous devez créer cette base de données avant d'exécuter le programme d'installation de JMP Server.

Prérequis

- Vérifiez qu'une version prise en charge de SQL Server est installée sur l'hôte sur lequel vous prévoyez d'installer JMP Server ou dans votre environnement de réseau. Pour plus d'informations, reportez-vous à [Configuration requise de la base de données pour JMP Server](#).
- Vérifiez que vous utilisez SQL Server Management Studio pour créer et administrer la base de données. Si vous installez JMP Server dans un environnement de validation technique, vous pouvez utiliser SQL Server Management Studio Express. Téléchargez-le et installez-le à partir du site Web suivant.

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

Procédure

- 1 Sur l'ordinateur sur lequel Microsoft SQL Server est installé, sélectionnez **Démarrer > Tous les programmes > Microsoft SQL Server 2016, Microsoft SQL Server 2014 ou Microsoft SQL Server 2012**.

- 2 Sélectionnez **SQL Server Management Studio**.
- 3 Dans le volet Explorateur d'objets, connectez-vous à une instance du Moteur de base de données Microsoft SQL Server et développez le nœud pour cette instance.
- 4 Cliquez avec le bouton droit sur **Bases de données** et sélectionnez **Nouvelle base de données**.
- 5 Dans la zone de texte **Nom de la base de données**, entrez un nom en utilisant uniquement des caractères ASCII pour la base de données que vous créez pour JMP Server.

Par exemple : **JMPDB**

Important Les caractères non-ASCII ne sont pas pris en charge.

- 6 Utilisez les valeurs par défaut pour les paramètres `Initial size` et `Autogrowth` de la base de données et des fichiers journaux.
- 7 Cliquez sur **OK**.
SQL Server Management Studio ajoute votre base de données au dossier **Bases de données** du volet Explorateur d'objets.
- 8 Quittez Microsoft SQL Server Management Studio.

Suivant

Avant d'installer JMP Server, créez une connexion SQL Server pour l'hôte JMP Server. Reportez-vous à la section [Créer une connexion SQL Server pour l'hôte JMP Server](#).

Créer une connexion SQL Server pour l'hôte JMP Server

Lors de l'installation de JMP Server, le programme d'installation accède à la base de données SQL Server que vous avez créée pour stocker les informations sur les services JMP Server en cours d'installation. Vous devez sélectionner le type de connexion SQL Server que le programme d'installation de JMP Server doit utiliser.

Pour accéder à la base de données SQL Server que vous avez créée, sélectionnez une connexion d'authentification Windows ou une connexion d'authentification SQL Server. Par défaut, la connexion d'authentification Windows est utilisée. Avant d'exécuter le programme d'installation de JMP Server, assurez-vous que les informations d'identification existent pour le type de connexion SQL Server que vous avez sélectionnée.

Utilisez le tableau suivant pour déterminer les tâches que vous devez terminer pour créer la connexion SQL Server que le programme d'installation de JMP Server doit utiliser.

Tableau 4-1. Types de connexion SQL Server

Type de connexion SQL Server	Utilisez les détails de la tâche dans la section
Authentification Windows (par défaut)	Créer une connexion d'authentification Windows SQL Server pour l'hôte JMP Server
SQL Server authentication (Authentification SQL Server)	Créer une connexion d'authentification SQL Server pour l'hôte JMP Server

Créer une connexion d'authentification Windows SQL Server pour l'hôte JMP Server

Vous pouvez spécifier le programme d'installation de JMP Server pour utiliser une connexion d'authentification Windows lorsque vous accédez à la base de données SQL Server que vous avez créée. Avant d'exécuter le programme d'installation de JMP Server, les informations d'identification de cette connexion SQL Server doivent exister pour l'hôte JMP Server sur lequel vous installez JMP Server.

Les utilisateurs connectés à l'hôte JMP Server peuvent accéder à la base de données SQL Server JMP. Toutefois, vous devez également vérifier que le compte d'utilisateur Windows Server utilisé pour installer JMP Server a accès en écriture à la base de données SQL Server que vous avez créée pour JMP Server. Reportez-vous à la section [Octroi d'autorisations au propriétaire de la base de données et à l'administration système pour l'utilisateur Windows](#).

Prérequis

Assurez-vous que vous avez créé la base de données SQL Server pour votre instance de JMP Server. Pour créer la base de données, reportez-vous à la section [Créer une base de données SQL Server pour JMP Server](#).

Procédure

- 1 Connectez-vous à une session SQL Server Management Studio en tant que sysadmin (SA) ou utilisez un compte d'utilisateur avec des privilèges SA.
- 2 Dans le volet Explorateur d'objets, développez le dossier de l'instance de SQL Server dans lequel vous avez créé la base de données pour votre instance de JMP Server.
- 3 Développez le dossier **Sécurité**, cliquez avec le bouton droit sur **Connexions** et sélectionnez **Nouvelle connexion**.
- 4 Dans la boîte de dialogue **Connexion - Nouveau**, sur la page **Général**, entrez un nom de connexion au format *nom_domaine\nom_ordinateur\$*, où *nom_ordinateur* est le nom de l'hôte JMP Server et *nom_domaine* est le domaine auquel l'hôte appartient.

Par exemple : **mycompany\jmpserver\$**
- 5 Sélectionnez **Authentification Windows**.
- 6 Dans la liste **Base de données par défaut**, sélectionnez une base de données par défaut pour la connexion. La base de données Master est la valeur par défaut pour cet élément.
- 7 Dans la liste **Langue par défaut**, sélectionnez une langue par défaut à utiliser pour la connexion.
- 8 Attribuez le rôle Serveur sysadmin pour le compte de la nouvelle connexion.
 - a Cliquez sur l'onglet **Rôles du serveur** dans le volet Sélectionner une page sur le côté gauche.
 - b Sur la page Rôles du serveur, cochez la case **sysadmin**.
- 9 Cliquez sur **OK**.

La nouvelle connexion est ajoutée sous le dossier **Connexions** dans le volet Explorateur d'objets.

Suivant

Créez les informations d'identification de connexion SQL Server pour le compte d'utilisateur Windows Server qui est utilisé pour installer JMP Server. Reportez-vous à la section [Octroi d'autorisations au propriétaire de la base de données et à l'administration système pour l'utilisateur Windows](#).

Créer une connexion d'authentification SQL Server pour l'hôte JMP Server

Vous pouvez spécifier le programme d'installation de JMP Server pour utiliser une connexion SQL Server qui utilise la connexion d'authentification SQL Server afin d'accéder à la base de données SQL Server que vous avez créée. Avant d'exécuter le programme d'installation de JMP Server, les informations d'identification de connexion pour ce type de connexion SQL Server doivent exister pour l'hôte JMP Server.

Prérequis

Assurez-vous que vous avez créé la base de données SQL Server pour JMP Server. Pour créer la base de données, reportez-vous à la section [Créer une base de données SQL Server pour JMP Server](#).

Procédure

- 1 Connectez-vous à une session SQL Server Management Studio en tant que sysadmin (SA) ou en utilisant un compte d'utilisateur avec des privilèges SA.
- 2 Dans le volet Explorateur d'objets, développez le dossier de l'instance SQL Server dans lequel vous avez créé la base de données JMP Server.
- 3 Développez le dossier **Sécurité**, cliquez avec le bouton droit sur **Connexions** et sélectionnez **Nouvelle connexion**.
- 4 Dans la boîte de dialogue **Connexion - Nouveau**, sur la page **Général**, entrez une valeur dans la zone de texte **Nom de connexion** en utilisant uniquement des caractères ASCII. Vous pouvez également cliquer sur **Rechercher** et utiliser la boîte de dialogue **Sélectionner un utilisateur ou un groupe** pour localiser la connexion que vous souhaitez utiliser.

Important Les caractères non-ASCII ne sont pas pris en charge.

- 5 Sélectionnez **Authentification SQL Server**.
- 6 Dans les zones de texte **Mot de passe** et **Confirmer le mot de passe**, entrez un mot de passe pour le nom de la nouvelle connexion. Utilisez uniquement des caractères ASCII.
- 7 Si vous modifiez un mot de passe existant, sélectionnez **Spécifier l'ancien mot de passe**, puis entrez l'ancien mot de passe dans la zone de texte **Ancien mot de passe**.
- 8 En fonction de la stratégie de votre organisation, cochez ou décochez les cases **Appliquer la stratégie de mot de passe**, **Appliquer l'expiration de mot de passe** et **L'utilisateur doit changer de mot de passe à la prochaine connexion**.

- 9 Dans la liste **Base de données par défaut**, sélectionnez une base de données par défaut pour la connexion. La base de données Master est la valeur par défaut pour cet élément.
- 10 Dans la liste **Langue par défaut**, sélectionnez une langue par défaut pour la connexion.
- 11 Attribuez le rôle Serveur sysadmin pour le compte de la nouvelle connexion.
 - a Cliquez sur l'onglet **Rôles du serveur** dans le volet Sélectionner une page sur le côté gauche.
 - b Sur la page Rôles du serveur, cochez la case **sysadmin**.
- 12 Cliquez sur **OK**.

La nouvelle connexion est ajoutée sous le dossier **Connexions** dans le volet Explorateur d'objets.

Suivant

Créez les informations d'identification de connexion SQL Server pour le compte d'utilisateur Windows Server qui est utilisé pour installer JMP Server. Reportez-vous à la section [Octroi d'autorisations au propriétaire de la base de données et à l'administration système pour l'utilisateur Windows](#).

Octroi d'autorisations au propriétaire de la base de données et à l'administration système pour l'utilisateur Windows

Outre la création d'une connexion SQL Server pour la machine hôte JMP Server, le compte d'utilisateur Windows que vous prévoyez d'utiliser pour installer l'instance de JMP Server doit être créé. Ce compte d'utilisateur Windows doit recevoir des privilèges de propriétaire de base de données et sysadmin dans la base de données SQL Server que vous avez créée.

Prérequis

- Assurez-vous que la base de données SQL Server a été créée pour le JMP Server que vous prévoyez d'installer. Reportez-vous à la section [Créer une base de données SQL Server pour JMP Server](#).
- Vérifiez que la connexion à SQL Server a été créée pour l'hôte JMP Server. Reportez-vous à la section [Créer une connexion SQL Server pour l'hôte JMP Server](#).

Procédure

- 1 Connectez-vous à une session SQL Server Management Studio en tant que sysadmin (SA) ou utilisez un compte d'utilisateur avec des privilèges SA.
- 2 Dans le volet Explorateur d'objets, connectez-vous à l'instance SQL Server que vous avez créée pour le JMP Server.

- 3 Créez la connexion SQL Server du compte d'utilisateur Windows que vous prévoyez d'utiliser pour l'installation du JMP Server.
 - a Développez le dossier **Sécurité**, cliquez avec le bouton droit sur **Connexions** et sélectionnez **Nouvelle connexion**.
 - b Dans la boîte de dialogue **Connexion - Nouveau**, cliquez sur **Rechercher**.
 - c Dans la boîte de dialogue **Sélectionner un utilisateur ou un groupe**, sélectionnez l'utilisateur Active Directory valide que vous prévoyez d'utiliser pour installer le JMP Server.
 - d Dans la boîte de dialogue Connexion - Nouveau, sous Sélectionner une page, choisissez **Rôles du serveur** et cochez la case **sysadmin**.
 - e Cliquez sur **OK** pour fermer la boîte de dialogue **Connexion - Nouveau**.
- 4 Accordez des autorisations au compte d'utilisateur Windows.
 - a Dans le volet de gauche, cliquez sur **Bases de données**.
 - b Sélectionnez la base de données que vous avez créée pour votre instance de JMP Server, puis cliquez sur **Sécurité** et sur **Utilisateurs**.
 - c Dans le volet Utilisateurs, cliquez avec le bouton droit sur votre connexion d'utilisateur Windows et sélectionnez **Propriétés** dans le menu contextuel.
 - d Sous Appartenance au rôle de base de données, sélectionnez le rôle **db_owner**.
 - e Cliquez sur **OK**.

La nouvelle connexion est ajoutée sous le dossier **Connexions** dans le volet Explorateur d'objets.

Suivant

Installez l'instance de JMP Server en utilisant les informations contenues dans la section [Installer JMP Server](#).

Installation de JMP Server

Pour utiliser les fonctionnalités de JMP Integrated Workflow, vous devez tout d'abord installer et configurer JMP Server et les produits de technologie VMware JMP requis.

Remarque Dans Horizon 7 version 7.5, vous ne pouvez installer qu'une seule instance de JMP Server.

Ce chapitre aborde les rubriques suivantes :

- [Installer JMP Server](#)
- [Désinstaller JMP Server](#)

Installer JMP Server

Avant de pouvoir utiliser les fonctionnalités de JMP Integrated Workflow, vous devez installer et configurer JMP Server.

Le fichier de programme d'installation de JMP Server est inclus lorsque vous téléchargez VMware Horizon 7 version 7.5 ou ultérieure. Vous devez exécuter le programme d'installation de JMP Server séparément après avoir installé correctement Horizon 7 version 7.5 ou ultérieure.

Prérequis

- Vérifiez que vous avez respecté la configuration système requise pour les composants qui doivent installer JMP Server. Reportez-vous à la section [Chapitre 3 Configuration système requise pour JMP Server](#).
- Pour exécuter le programme d'installation de JMP Server sur un hôte Windows Server, vous devez utiliser un compte d'utilisateur de domaine disposant de privilèges administratifs sur le système hôte.
- Assurez-vous que la base de données SQL Server que doit utiliser votre instance de JMP Server a été créée et que vous disposez de l'accès lui correspondant.
- Vérifiez que les connexions et les autorisations SQL Server ont été configurées pour l'hôte JMP Server et le compte d'utilisateur de domaine Windows que vous prévoyez d'utiliser pour installer JMP Server. Reportez-vous à la section [Créer une connexion SQL Server pour l'hôte JMP Server](#).
- Rassemblez les informations pour le port HTTP sécurisé ou non sécurisé, le port de l'interface utilisateur et les certificats auto-signés à utiliser avec les fonctionnalités de JMP Integrated Workflow.

- Obtenez un certificat TLS signé par une autorité de certification et utilisez-le pour remplacer le certificat TLS par défaut installé par le programme d'installation de JMP Server.
- Avant d'installer JMP Server, utilisez le tableau suivant pour déterminer le type d'installation à utiliser.

Type d'installation	Action effectuée par le programme d'installation de JMP Server
Environnement de production	Génère une instance de JMP Server qui utilise SQL Server édition Standard ou Entreprise.
Environnement de développement ou validation technique	Génère une instance de JMP Server qui utilise SQL Server Express.

- Ajoutez les fichiers suivants à la liste d'exclusion de McAfee Antivirus avant d'installer JMP Server.
 - C:\Program Files (x86)\VMware\JMP\nssm-2.24\nssm-2.24\win32\nssm.exe
 - C:\Program Files (x86)\VMware\JMP\com\xmp\node_modules\winser\bin\nssm.exe

Procédure

- 1 Pour démarrer l'assistant **Installation de VMware JMP**, recherchez le fichier de programme d'installation de JMP Server et double-cliquez dessus.

Le nom du fichier de programme d'installation de JMP Server est `VMware-Jmp-Installer-e.x.p-xxxxxxx.exe`, où `xxxxxxx` est le numéro de build. Par exemple, `VMware-Jmp-Installer-e.x.p-7259616.exe`.

Remarque Si vous voulez journaliser le processus d'installation, exécutez le programme d'installation de JMP Server à partir d'une invite de commande à l'aide de la commande suivante, où *Log_Folder_Path* est le dossier dans lequel le fichier journal doit être créé.

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

- 2 Cliquez sur **Suivant** sur la page d'accueil et acceptez les termes de licence VMware.
- 3 Pour autoriser le trafic HTTPS, cliquez sur **Suivant**.

Remarque JMP Server utilise le port 443 et, éventuellement, les ports 80, 3000 à 3004, 888 et 8889. Pour autoriser le trafic HTTP sur le port 80, cochez la case **Autoriser HTTP ?**.

4 Fournissez les informations sur l'instance de SQL Server et le catalogue de base de données.

- a Entrez l'adresse IP ou le nom de l'instance de SQL Server pour vous connecter à la base de données que vous avez créée pour JMP Server. Facultativement, cliquez sur **Parcourir** pour faire la sélection.
- b Sélectionnez les informations d'identification d'authentification à utiliser pour vous connecter à la base de données SQL Server.

Option	Description
Informations d'identification pour l'authentification Windows de l'utilisateur actuel	Les informations d'identification d'administrateur que vous utilisez pendant ce processus d'installation sont utilisées pour vous connecter à l'instance de base de données SQL Server.
Authentification de serveur à l'aide de l'ID d'ouverture de session et du mot de passe ci-dessous	Fournissez les informations ID d'ouverture de session et Mot de passe à utiliser pour vous connecter à l'instance de base de données SQL Server.

Remarque Les informations d'identification de connexion que vous utilisez doivent déjà être configurées dans l'instance de SQL Server à laquelle JMP Server va accéder. Reportez-vous à la section [Créer une connexion SQL Server pour l'hôte JMP Server](#).

- c Dans la zone de texte **Nom du catalogue de base de données**, entrez le nom de la base de données que vous avez créée à l'aide de la section [Créer une base de données SQL Server pour JMP Server](#). En option, cliquez sur **Parcourir** et sélectionnez le catalogue de base de données dans la liste disponible.

Le catalogue de base de données sélectionné est utilisé pour stocker des informations sur les services JMP Server.

- d (Facultatif) Si vous voulez écraser la base de données existante, cochez la case **Écraser la base de données existante**.

Remarque La première fois que le programme d'installation de JMP Server est exécuté, les tableaux de base de données nécessaires sont créés. Si vous exécutez à nouveau le programme d'installation pour créer plusieurs instances de JMP Server pour l'équilibrage de charge, le programme d'installation détecte que la base de données existe déjà et ne recrée pas les tableaux. Sélectionner cette option écrase les informations existantes dans la base de données.

- e Pour garantir une communication sécurisée entre JMP Server et l'instance de SQL Server, vérifiez que la case **Activer SSL** est cochée. La case **Activer SSL** est cochée par défaut.

Important Lorsque la case **Activer SSL** est cochée, vérifiez que le certificat TLS/SSL utilisé dans SQL Server est importé dans le magasin de certificats local Windows sur l'hôte JMP Server. Si ce n'est pas le cas, le processus d'installation de JMP Server échoue avec l'erreur « Échec de l'exécution du uem_migrate.bat » et, lorsque vous cliquez sur **OK** dans la boîte de dialogue d'erreur, l'installation est restaurée.

Reportez-vous à la section « Activer le chiffrement pour un client spécifique » de l'article [Comment activer le chiffrement SSL pour une instance de SQL Server à l'aide de la console MMC](#) de Microsoft TechNet pour en savoir plus sur l'exportation et l'importation du certificat TLS/SSL de SQL Server.

- f Cliquez sur **Suivant**.

5 Sur la page **Prêt à installer le programme**, cliquez sur **Installer**.

6 Lorsque l'installation s'est terminée correctement, cliquez sur **Terminer**.

Lorsque l'installation est réussie, les services JMP Server suivants sont installés et démarrés sur votre hôte Windows Server.

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

Suivant

Synchronisez l'heure entre l'instance de JMP Server récemment installée et son serveur Horizon Connection Server associé. Reportez-vous à la section [Synchroniser l'heure entre des hôtes de Serveur de connexion Horizon et de JMP Server](#).

Désinstaller JMP Server

Vous devrez peut-être désinstaller et réinstaller JMP Server pour résoudre un problème.

Cette procédure décrit comment désinstaller JMP Server si vous rencontrez des problèmes qui ne peuvent pas être résolus avec d'autres méthodes.

Prérequis

- Vérifiez que vous disposez des privilèges d'administration corrects pour désinstaller JMP Server.
- Avant de désinstaller un JMP Server, supprimez tous les partages de configuration User Environment Manager qui sont associés à ce JMP Server. Reportez-vous à la section « Supprimer des informations de partage de configuration User Environment Manager » dans *Administration de VMware Horizon Console*.

Procédure

- 1 Ouvrez la console Programmes et fonctionnalités de Microsoft Windows.
Par exemple, cliquez sur **Démarrer > Paramètres > Système > Applications et fonctionnalités**.
- 2 Sélectionnez **VMware JMP** dans la liste des applications installées.
- 3 Pour terminer les étapes de désinstallation, cliquez sur **Désinstaller** et suivez l'assistant.

Suivant

Réinstallez JMP Server. Pour plus d'informations, reportez-vous au document [Installer JMP Server](#).

Configuration de l'instance de JMP Server

6

Après l'installation réussie de l'instance de JMP Server, vous devez effectuer les tâches de configuration afin de garantir que l'instance de JMP Server peut s'authentifier avec Horizon Connection Server et communiquer en toute sécurité avec d'autres serveurs dans votre réseau.

Ce chapitre aborde les rubriques suivantes :

- [Synchroniser l'heure entre des hôtes de Serveur de connexion Horizon et de JMP Server](#)
- [Configuration de certificats TLS et de suites de chiffrement pour JMP Server](#)

Synchroniser l'heure entre des hôtes de Serveur de connexion Horizon et de JMP Server

L'heure sur les hôtes de Serveur de connexion Horizon et de JMP Server doit être synchronisée pour que le processus d'authentification entre les deux serveurs réussisse.

Lorsque vous accédez aux fonctionnalités de JMP Integrated Workflow à l'aide de l'interface utilisateur d'Horizon Console, JMP Server authentifie le jeton reçu de la part du Serveur de connexion Horizon, qui à son tour renvoie un jeton à JMP Server. Si l'heure n'est pas synchronisée entre les deux hôtes, le Serveur de connexion Horizon refuse le jeton fourni par JMP Server et les fonctionnalités de JMP Integrated Workflow ne sont plus disponibles dans l'interface utilisateur d'Horizon Console. Le volet Paramètre JMP affiche le message d'erreur suivant.

Le jeton SSO d'Horizon n'a pas pu être vérifié.

Pour qu'un processus d'authentification réussisse, synchronisez l'heure des hôtes de Serveur de connexion Horizon et de JMP Server avec l'heure d'un serveur NTP (Network Time Protocol) commun.

Procédure

- 1 Utilisez les commandes de VMware Tool suivantes sur l'hôte Windows.

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

- 2 Sur l'hôte ESXi, synchronisez les horloges ESXi avec un serveur de temps du réseau.
 - a Démarrez VMware Host Client, puis connectez-vous à l'hôte ESXi.
 - b Cliquez sur **Configurer**.
 - c Sous **Système**, sélectionnez **Configuration de l'heure** et cliquez sur **Modifier**.
 - d Sélectionnez **Utiliser le protocole de temps du réseau (activer le client NTP)**.
 - e Dans la zone de texte Ajouter un serveur NTP, entrez l'adresse IP ou le nom de domaine qualifié d'un ou plusieurs serveurs NTP avec lesquels vous voulez effectuer la synchronisation.

Suivant

Configurez les certificats TLS pour JMP Server. Reportez-vous à la section [Présentation des tâches de configuration des certificats TLS pour JMP Server](#).

Configuration de certificats TLS et de suites de chiffrement pour JMP Server

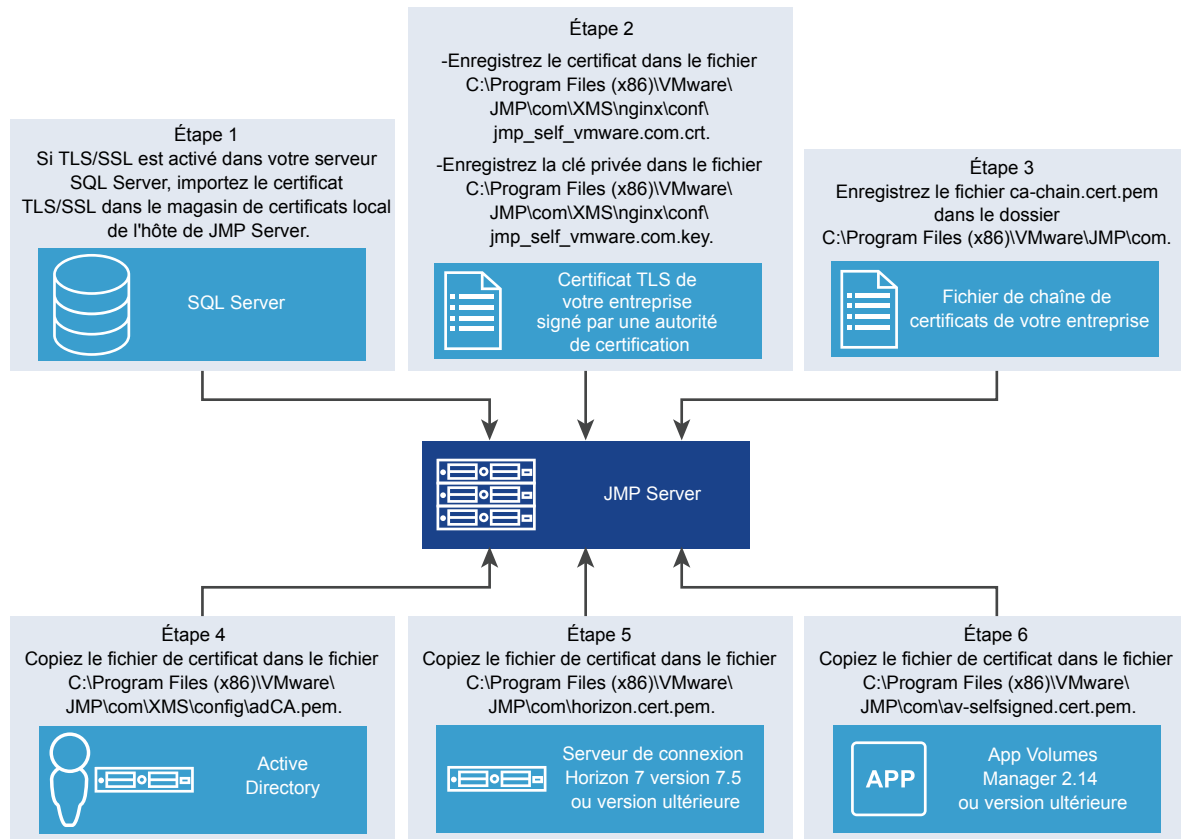
Pour vous assurer que votre instance de JMP Server communique en toute sécurité avec les autres serveurs de votre réseau, vous devez configurer votre instance de JMP Server pour qu'elle utilise des certificats TLS signés par une autorité de certification valide. Afin d'améliorer les connexions sécurisées, vous pouvez également modifier les suites de chiffrement par défaut que d'autres serveurs acceptent et proposent lors de la communication avec votre instance de JMP Server.

Par défaut, le programme d'installation de JMP Server installe un certificat de serveur TLS auto-signé pour l'instance de JMP Server que vous avez installée. Vous pouvez utiliser le certificat par défaut à des fins de test. Si vous utilisez l'instance de JMP Server dans un environnement de production, vous devez remplacer le certificat par défaut par un certificat de serveur TLS signé par une autorité de certification dès que possible. L'utilisation de certificats non signés par une autorité de certification peut permettre à des parties non approuvées d'intercepter le trafic en se faisant passer pour votre serveur. Reportez-vous à la section [Présentation des tâches de configuration des certificats TLS pour JMP Server](#).

Présentation des tâches de configuration des certificats TLS pour JMP Server

Après l'installation réussie de JMP Server, vous devez effectuer plusieurs tâches pour configurer les certificats de serveur TLS qui sont signés par une autorité de certification valide afin de les utiliser avec l'instance de JMP Server.

Outre les tâches présentées dans cette rubrique, le schéma suivant fournit un résumé visuel des principales étapes requises pour configurer les certificats pour JMP Server. Veillez à suivre les étapes détaillées décrites dans les rubriques qui suivent cette présentation pour configurer correctement les certificats spécifiques. Pour les tâches marquées comme facultatives, déterminez si vous devez les effectuer pour vérifier que votre configuration de JMP Server est plus sécurisée. Lorsque vous avez terminé les configurations de certificat, vous devez redémarrer les trois services JMP Server à l'aide du Gestionnaire des services Windows.

Figure 6-1. Principales étapes de configuration des certificats pour JMP Server

- 1 Si TLS/SSL est activé dans votre serveur SQL Server, vérifiez que le certificat TLS/SSL a été importé dans le magasin de certificats local de l'hôte de JMP Server.
- 2 Remplacez le certificat de serveur TLS que le programme d'installation de JMP Server a généré.

Le certificat de serveur par défaut que le programme d'installation de JMP Server a généré est auto-signé et n'est pas reconnu par le réseau de votre organisation. Remplacez le certificat auto-signé par un certificat TLS valide que vous avez obtenu de la part d'une autorité de certification. Reportez-vous à la section [Remplacer le certificat TLS par défaut](#).

Si votre organisation ne dispose pas d'un certificat de serveur Web TLS valide, obtenez un certificat de serveur TLS signé de la part d'une autorité de certification. Consultez les informations contenues dans le document *Scénarios de configuration des certificats TLS pour Horizon 7*.

- 3 Si une autorité de certification intermédiaire a signé les certificats de serveur de votre organisation, configurez JMP Server pour qu'il utilise le fichier de chaîne de certificats de votre organisation, `ca-chain.cert.pem`, pour permettre à JMP Server d'authentifier les autres serveurs dans votre réseau. Reportez-vous à la section [Configurer JMP Server pour utiliser un fichier de chaîne de certificats](#).

Remarque Si une autorité de certification racine approuvée par NodeJS a signé les certificats de serveur TLS de votre organisation directement, il est inutile de fournir un fichier de chaîne de certificats ou le fichier de certificat racine, `ca.cert.pem`.

- 4 Obtenez le certificat d'autorité de certification qui est utilisé pour signer le certificat pour le serveur Active Directory, stockez-le dans le fichier `adCA.pem` et ajoutez le fichier dans le dossier de configuration XMS de JMP Server. Reportez-vous à la section [Configurer JMP Server pour qu'il utilise le certificat pour Active Directory](#) pour plus d'informations.
- 5 Exportez le certificat signé par une autorité de certification pour le Serveur de connexion Horizon dans un fichier `horizon.cert.pem` et ajoutez le fichier dans le dossier de base de JMP Server. Reportez-vous à la section [Configurer JMP Server pour qu'il utilise le certificat du Serveur de connexion Horizon](#) pour plus d'informations.

Avec le fichier `horizon.cert.pem`, JMP Server peut authentifier le Serveur de connexion comme un serveur digne de confiance auquel il peut se connecter.

Remarque Vous devez terminer cette tâche pour chaque espace du Serveur de connexion qui communique avec l'instance de JMP Server. Le contenu de chacun des certificats signés par une autorité de certification exportés doit être ajouté dans le même fichier `horizon.cert.pem`.

- 6 Si vous attribuez des AppStacks App Volumes lors de la création d'attributions JMP, configurez votre instance de JMP Server afin qu'elle utilise le certificat auto-signé de l'instance d'App Volumes Manager pour communiquer en toute sécurité avec l'instance d'App Volumes Manager. Reportez-vous à la section [Configurer JMP Server pour qu'il utilise le certificat auto-signé d'App Volumes Manager](#).
- 7 (Facultatif) Modifiez les suites de chiffrement par défaut que votre instance de JMP Server prend en charge par les chiffrements que votre organisation prend en charge. Reportez-vous à la section [Configuration de suites de chiffrement pour JMP Server](#).
- 8 (Facultatif) Utilisez une stratégie plus restrictive de partage des ressources cross-origin (CORS) sur votre JMP Server pour une communication plus sécurisée avec votre instance du Serveur de connexion Horizon 7. Reportez-vous à la section [Utiliser une stratégie CORS plus restrictive sur votre JMP Server](#).
- 9 Redémarrez les trois services JMP Server à l'aide du Gestionnaire des services Windows.

Après avoir configuré les certificats de serveur, vous pouvez passer à Horizon Console pour configurer les paramètres JMP et commencer à utiliser les fonctionnalités de JMP Integrated Workflow. Reportez-vous à la section « Configurer les paramètres JMP pour la première fois » dans le document *Administration de VMware Horizon Console*.

Remplacer le certificat TLS par défaut

Remplacez le certificat TLS par défaut installé par le programme d'installation de JMP Server par un certificat TLS de votre organisation qui est signé par une autorité de certification.

Après l'installation réussie de l'instance de JMP Server, vous pouvez y accéder à l'aide de la Console Horizon sur un navigateur Web. Toutefois, si votre réseau ne reconnaît pas le certificat TLS par défaut qui a été installé, la boîte de dialogue d'alerte de sécurité du navigateur Web s'affiche lorsque vous configurez les paramètres JMP pour la première fois. Même si vous pouvez utiliser un certificat auto-signé par défaut, pour le test et pour garantir une connexion sécurisée avec l'instance de JMP Server, remplacez le certificat par défaut et la clé par un certificat TLS signé par une autorité de certification et par une clé privée.

Important Si vous décidez de donner aux fichiers de certificat et de clé des noms différents de ceux par défaut créés par le programme d'installation de JMP Server, vous devez modifier le fichier de configuration NGINX de JMP Server pour utiliser les nouveaux noms de fichier.

Prérequis

- Installez JMP Server. Reportez-vous à la section [Installer JMP Server](#).
- Obtenez un certificat TLS signé par une autorité de certification et remplacez le certificat TLS par défaut installé par le programme d'installation de JMP Server. Vous pouvez utiliser des outils de certificat, tels que Microsoft Certreq ou OpenSSL sous Windows, pour générer un certificat. Reportez-vous à la section « Obtention de certificats TLS à partir d'une autorité de certification » dans le document *Scénarios de configuration des certificats TLS pour Horizon 7*.

Procédure

- 1 Dans l'hôte JMP Server, arrêtez les trois services JMP Server à l'aide de l'outil Gestionnaire des services Windows.
 - a Cliquez avec le bouton droit sur l'icône **Démarrer** de Windows et sélectionnez **Exécuter**.
 - b Dans la boîte de dialogue Exécuter, tapez `services.msc` dans la zone de texte **Ouvrir**, puis cliquez sur **OK**.
 - c Recherchez les trois services JMP Server suivants dans le volet Services (local) de la fenêtre Services et, pour chaque service, cliquez sur **Arrêter**.
 - VMware JMP API Service
 - VMware JMP File Share Service
 - VMware JMP Platform Services
- 2 Enregistrez votre fichier de certificat de serveur TLS signé par une autorité de certification avec le nom `jmp_self_vmware.com.crt` dans le dossier de configuration NGINX sur l'hôte JMP Server.
- 3 Enregistrez la clé privée qui accompagne le certificat de serveur TLS signé par une autorité de certification avec le nom `jmp_self_vmware.com.key`.

Par exemple : `C:\Program Files
(x86)\VMware\JMP\com\XMS\nginx\conf\jmp_self_vmware.com.crt`

Par exemple : `C:\Program Files
(x86)\VMware\JMP\com\XMS\nginx\conf\jmp_self_vmware.com.key`

- 4 (Facultatif) Si vous voulez utiliser des noms de fichier différents des noms de fichier de certificat attendus, `jmp_self_vmware.com.crt` ou `jmp_self_vmware.com.key`, vous devez modifier le fichier de configuration NGINX avec les nouveaux noms de fichier.
 - a Ouvrez le fichier de configuration `C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\nginx.conf`.
 - b Recherchez les occurrences des propriétés `jmp_self_vmware.com.crt` et `jmp_self_vmware.com.key` et remplacez-les par les nouveaux noms de fichier que vous avez sélectionnés.
 - c Enregistrez le fichier `nginx.conf`.

Vous pouvez maintenant accéder en toute sécurité aux fonctionnalités de JMP Integrated Workflow sans que la boîte de dialogue d'alerte de sécurité du navigateur Web ne s'affiche.

Suivant

Si une autorité de certification intermédiaire a signé la chaîne de certificats complète de votre organisation, configurez votre instance de JMP Server pour qu'elle utilise un fichier de chaîne de certificats. Reportez-vous à la section [Configurer JMP Server pour utiliser un fichier de chaîne de certificats](#). Si vous ne l'avez pas déjà fait, effectuez la configuration de votre instance de JMP Server pour utiliser le certificat pour Active Directory. Reportez-vous à la section [Configurer JMP Server pour qu'il utilise le certificat pour Active Directory](#).

Configurer JMP Server pour utiliser un fichier de chaîne de certificats

Si une autorité de certification intermédiaire a signé les certificats des serveurs de votre organisation, configurez l'instance de JMP Server avec la chaîne de certificats complète de votre organisation, qui inclut les certificats racines et intermédiaires.

Prérequis

- Utilisez le Gestionnaire des services Windows pour arrêter les trois services JMP Server.

Procédure

- 1 Obtenez le fichier de chaîne de certificats complète de votre organisation, `ca-chain.cert.pem`.
- 2 Copiez le fichier de chaîne de certificats `ca-chain.cert.pem` dans le dossier `C:\Program Files (x86)\VMware\JMP\com`.

Une fois la chaîne de certificats en place, votre instance de JMP Server peut authentifier les instances d'Horizon 7 et d'App Volumes et communiquer avec elles en toute sécurité.

Suivant

Configurez l'instance de JMP Server avec le certificat Active Directory afin que l'instance de JMP Server puisse authentifier le serveur Active Directory lorsque des administrateurs de poste de travail utilisent les fonctionnalités de JMP Integrated Workflow. Reportez-vous à la section [Configurer JMP Server pour qu'il utilise le certificat pour Active Directory](#).

Configurer JMP Server pour qu'il utilise le certificat pour Active Directory

Pour que JMP Server valide le serveur Active Directory avec lequel la Horizon Console est connectée, vous devez configurer JMP Server afin qu'il utilise le certificat pour ce serveur Active Directory.

Vous devez exporter le certificat d'autorité de certification racine du domaine Active Directory dans un fichier de certificat nommé `adCA.pem` et placer ce fichier dans le dossier de configuration XMS de JMP Server.

Prérequis

- JMP Server doit être installé.
- Active Directory doit être configuré pour LDAP sur SSL (LDAPS) ou StartTLS (LDAP sur TLS).
- Certificats d'autorité de certification racine des domaines Active Directory. Si les certificats ne sont pas au format PEM (codés en Base64), consultez la documentation d'OpenSSL (ou un document similaire) pour convertir le fichier au format PEM.

Remarque Lorsque vous disposez de plusieurs certificats racines depuis des domaines différents, vous pouvez combiner tous les certificats au format PEM en un seul fichier en copiant le contenu de chaque fichier un par un dans un fichier unique `.pem`.

Procédure

- 1 Assurez-vous que le nom du fichier de certificat au format PEM est `adCA.pem`.
- 2 Copiez le fichier `adCA.pem` dans le dossier configuration XMS de JMP Server.

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

Avec le certificat Active Directory configuré pour votre instance de JMP Server, le serveur Active Directory est reconnu comme un serveur approuvé et les utilisateurs de la Horizon Console peuvent utiliser correctement les fonctionnalités de JMP Integrated Workflow.

Suivant

Configurez JMP Server avec le certificat du Serveur de connexion afin qu'une instance de JMP Server puisse authentifier le Serveur de connexion lorsque les administrateurs de poste de travail utilisent les fonctionnalités de JMP Integrated Workflow. Reportez-vous à la section [Configurer JMP Server pour qu'il utilise le certificat du Serveur de connexion Horizon](#).

Configurer JMP Server pour qu'il utilise le certificat du Serveur de connexion Horizon

Pour que JMP Server valide le Serveur de connexion Horizon 7 auquel la Horizon Console est connectée, vous devez configurer JMP Server afin qu'il utilise le certificat du Serveur de connexion Horizon 7.

Vous devez exporter le certificat du Serveur de connexion Horizon 7 dans un fichier de certificat nommé `horizon.cert.pem` et placer ce fichier dans le dossier de base de JMP Server.

Important Le contenu de chacun des certificats signés par une autorité de certification exportés doit être ajouté dans le même fichier `horizon.cert.pem`.

Utilisez ces mêmes procédures lors de l'ajout d'un certificat du Serveur de connexion Horizon 7 signé par une autorité de certification ou auto-signé.

Prérequis

- JMP Server doit être installé.
- Vous devez disposer d'un accès administratif au Serveur de connexion Horizon 7.

Procédure

- 1 Connectez-vous à l'hôte Windows Server pour le Serveur de connexion Horizon 7 qui communique avec la Horizon Console et le serveur JMP Server que vous avez installé.
- 2 Cliquez avec le bouton droit sur l'icône **Démarrer** de Windows, sélectionnez **Exécuter** et tapez `mmc.exe`.

La fenêtre d'utilitaire de la console de gestion Microsoft s'affiche.
- 3 Ajoutez le composant logiciel enfichable Certificats.
 - a Dans la fenêtre **Racine de la console**, sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.
 - b Dans la fenêtre **Ajouter ou supprimer des composants logiciels enfichables**, sélectionnez **Certificats** dans le volet Composants logiciels enfichables disponibles et cliquez sur **Ajouter**.
 - c Une fois les certificats ajoutés, cliquez sur **OK**.
 - d Dans la fenêtre de composant logiciel enfichable Certificats, sélectionnez **Compte d'ordinateur** et cliquez sur **Suivant**.
 - e Dans la fenêtre Sélectionner un ordinateur, sélectionnez **Ordinateur local** et cliquez sur **Terminer**.

Le composant logiciel enfichable Certificats (ordinateur local) est ajouté dans le volet Composants logiciels enfichables sélectionnés.
 - f Cliquez sur **OK** pour fermer la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**.

- 4 Dans la fenêtre Racine de la console, sélectionnez **Racine de la Console > Certificats (ordinateur local)** et sélectionnez le dossier **Personnel > Certificats** dans le volet de gauche pour afficher son contenu.
- 5 Exportez le certificat du Serveur de connexion Horizon.
 - a Dans le volet de contenu des certificats, recherchez le certificat avec le nom convivial **vdm**.
Ce certificat appartient au Serveur de connexion Horizon.
 - b Cliquez avec le bouton droit sur le certificat et sélectionnez **Toutes les tâches > Exporter**.
 - c Dans la boîte de dialogue de l'assistant d'exportation de certificat, cliquez sur **Suivant**.
 - d Sélectionnez **Non, ne pas exporter la clé privée** et cliquez sur **Suivant**.
 - e Sélectionnez le format **Base-64 encode X.509 (.CER)** et cliquez sur **Suivant**.
 - f Entrez le nom de fichier **horizon.cert.pem** et cliquez sur **Parcourir** pour accéder au dossier dans lequel vous voulez enregistrer le certificat exporté.

Important Vous devez enregistrer le fichier de certificat exporté avec l'extension de fichier **.pem**, **pas** avec l'extension **.cer** ou **.crt**. Si nécessaire, ouvrez le fichier de certificat exporté dans un éditeur de texte et enregistrez-le avec le nom **horizon.cert.pem**.

- g Cliquez sur **Suivant** et cliquez sur **Terminer** pour fermer la fenêtre de **l'assistant d'exportation de certificat**.

Le certificat est exporté correctement.

- 6 Accédez à l'emplacement dans lequel vous avez enregistré le certificat **horizon.cert.pem** exporté et copiez-le dans le dossier de base de JMP Server.

Par exemple : C:\Program Files (x86)\VMware\JMP\com\horizon.cert.pem.

Avec le certificat du Serveur de connexion configuré pour JMP Server, le Serveur de connexion est reconnu comme un serveur approuvé et les utilisateurs de la Horizon Console peuvent utiliser correctement les fonctionnalités de JMP Integrated Workflow.

Suivant

Examinez les tâches facultatives répertoriées dans la section [Présentation des tâches de configuration des certificats TLS pour JMP Server](#) et déterminez si vous devez également les terminer. Si vous avez terminé toutes les tâches de configuration nécessaires, redémarrez les services de JMP Server et configurez les paramètres JMP. Pour plus d'informations, reportez-vous à la section « Configurer les paramètres JMP pour la première fois » dans le document *Administration de VMware Horizon Console*.

Configurer JMP Server pour qu'il utilise le certificat auto-signé d'App Volumes Manager

Si vous attribuez des AppStacks App Volumes lors de la création d'attributions JMP, configurez votre instance de JMP Server afin qu'elle utilise le certificat auto-signé de l'instance d'App Volumes Manager pour communiquer en toute sécurité avec l'instance d'App Volumes Manager.

Vous devez exporter le certificat autosigné de l'instance d'App Volumes Manager dans un fichier de certificat nommé `av-selfsigned.cert.pem` pour que JMP Server puisse l'utiliser.

Prérequis

- JMP Server doit être installé.
- Vous devez disposer d'un accès administratif à l'instance d'App Volumes Manager ou à l'équilibrage de charge qui le gère.

Procédure

- 1 À partir de votre hôte JMP Server, utilisez un navigateur Web pour vous connecter à l'instance d'App Volumes Manager ou à l'équilibrage de charge qui gère les instances d'App Volumes Manager dans votre environnement.
- 2 Pour rechercher les informations de certificat auto-signé qui sont utilisées par l'instance d'App Volumes Manager ou l'équilibrage de charge, utilisez la boîte de dialogue d'informations de site de votre navigateur Web, exportez le fichier de certificat auto-signé et enregistrez-le dans `C:\Program Files (x86)\VMware\JMP\com\av-selfsigned.cert.pem`.

Important Vous devez enregistrer le fichier de certificat exporté avec l'extension de fichier `.pem`, **pas** avec l'extension `.cer` ou `.crt`. Si nécessaire, ouvrez le fichier de certificat exporté dans un éditeur de texte et enregistrez-le avec le nom `av-selfsigned.cert.pem`.

Par exemple, lorsque vous utilisez un navigateur Web Google Chrome, utilisez l'assistant d'exportation de certificat pour copier le fichier de certificat auto-signé d'App Volumes Manager dans le fichier `av-selfsigned.cert.pem` dans le répertoire `C:\Program Files (x86)\VMware\JMP\com`.

- 3 Si vous avez terminé toutes les tâches nécessaires pour configurer les certificats TLS nécessaires pour rendre JMP Server plus sûr, redémarrez les services de JMP Server. Reportez-vous à la section [Présentation des tâches de configuration des certificats TLS pour JMP Server](#) pour voir les tâches de configuration restantes du certificat TLS.

Configuration de suites de chiffrement pour JMP Server

L'installation de JMP Server inclut des suites de chiffrement par défaut qui sont acceptées et proposées entre des instances de JMP Server, d'Horizon Connection Server, d'App Volumes et d'User Environment Manager. Vous pouvez éventuellement modifier ces suites de chiffrement par défaut que JMP Server prend en charge par les chiffrements que votre organisation prend en charge.

Vous devez spécifier la liste de chiffrements en utilisant le format défini dans la section <https://www.openssl.org/docs/man1.0.2/apps/ciphers.html#CIPHER-LIST-FORMAT>. La liste de chiffrements suivante est celle par défaut.

```
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
```


Procédure

- 1 Dans l'hôte JMP Server, arrêtez les trois services JMP Server à l'aide de l'outil Gestionnaire des services Windows.
 - a Cliquez avec le bouton droit sur l'icône **Démarrer** de Windows et sélectionnez **Exécuter**.
 - b Dans la boîte de dialogue Exécuter, tapez `services.msc` dans la zone de texte **Ouvrir**, puis cliquez sur **OK**.
 - c Dans le volet Services (local) de la fenêtre Services, recherchez les trois services JMP Server suivants et, pour chaque service, cliquez sur **Arrêter**.
 - VMware JMP API Service
 - VMware JMP File Share Service
 - VMware JMP Platform Services
- 2 Accédez au dossier `C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf`.
- 3 Créez une copie de sauvegarde du fichier `nginx.conf` avant de le modifier.
- 4 Ouvrez le fichier `nginx.conf` avec le Bloc-notes.
- 5 Recherchez la ligne qui commence par `ssl_ciphers` et modifiez la liste de chiffrements, le cas échéant.
- 6 Enregistrez les modifications apportées au fichier `nginx.conf`.
- 7 Utilisez l'outil Gestionnaire des services Windows pour redémarrer les trois services JMP Server pour que la nouvelle liste de suites de chiffrement prenne effet.

Utiliser une stratégie CORS plus restrictive sur votre JMP Server

Vous pouvez utiliser une stratégie plus restrictive de partage des ressources cross-origin (CORS) sur votre instance de JMP Server en créant une liste blanche des instances du Serveur de connexion Horizon 7 qui sont approuvées pour accéder à votre JMP Server.

Par défaut, un Serveur de connexion Horizon 7 peut accéder à votre instance de JMP Server s'il utilise le même certificat qui se trouve dans le fichier de chaîne de certificats que vous avez configuré à l'aide de la section [Configurer JMP Server pour utiliser un fichier de chaîne de certificats](#). Pour vous assurer que seule la liste approuvée des instances du Serveur de connexion Horizon 7 a accès à votre JMP Server, procédez comme suit.

Procédure

- 1 À l'aide d'un éditeur de texte, ouvrez le fichier de configuration NGINX qui se trouve dans l'emplacement `C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\nginx.conf`.
- 2 Recherchez les deux occurrences du texte suivant et supprimez le commentaire de chacun d'eux en supprimant le caractère `#` au début afin qu'ils apparaissent comme suit.

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

- 3 Recherchez les deux occurrences du texte suivant et supprimez-les en ajoutant un caractère # au début afin qu'ils apparaissent comme suit.

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

- 4 Ajoutez la liste approuvée des instances du Serveur de connexion à la liste blanche.

- a Recherchez le contenu suivant dans le fichier.

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

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

- b Après la ligne `default ''`, ajoutez une ligne pour chaque instance du Serveur de connexion que vous voulez inclure dans la liste blanche.

Par exemple, si les noms de domaine des instances du Serveur de connexion qui sont autorisées à se connecter à votre JMP Server sont `www.testhorizon.com` et `www.prodhorizon.com`, les lignes à ajouter sont affichées en gras dans l'exemple suivant.

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

- 5 Enregistrez les modifications apportées au fichier `nginx.conf`.
- 6 Redémarrez les services JMP Platform Services à l'aide du Gestionnaire des services Windows.

Mise à jour du mot de passe de base de données après l'installation de JMP Server

7

Si vous modifiez le mot de passe de base de données SQL Server qui a été utilisé lors de la première installation de JMP Server, vous devez également mettre à jour les informations de mot de passe de base de données utilisées par les services VMware JMP Server.

Ce chapitre aborde les rubriques suivantes :

- [Mettre à jour le mot de passe de base de données pour VMware JMP Platform Services](#)
- [Mettre à jour le mot de passe de base de données pour VMware JMP File Share Service](#)

Mettre à jour le mot de passe de base de données pour VMware JMP Platform Services

Si vous modifiez le mot de passe de base de données SQL Server qui a été utilisé lorsque JMP Server a été installé, vous devez également mettre à jour le mot de passe de base de données qui est utilisé par VMware JMP Platform Services pour vous connecter à votre base de données SQL Server.

Prérequis

Vérifiez que vous disposez des privilèges d'administration corrects pour modifier les informations de base de données dans l'hôte JMP Server.

Procédure

- 1 Dans l'hôte JMP Server, arrêtez le processus VMware JMP Platform Services à l'aide de l'outil Gestionnaire des services Windows.
 - a Cliquez avec le bouton droit sur l'icône **Démarrer** de Windows et sélectionnez **Exécuter**.
 - b Dans la boîte de dialogue Exécuter, tapez `services.msc` dans la zone de texte **Ouvrir**, puis cliquez sur **OK**.
 - c Recherchez VMware JMP Platform Services dans le volet Services (local) de la fenêtre Services et cliquez sur **Arrêter**.
- 2 Ouvrez la fenêtre **Administrateur de sources de données ODBC** en double-cliquant sur l'un des fichiers exécutables suivants qui est approprié pour votre hôte JMP Server.
 - `C:\Windows\SysWow64\odbcad64.exe`

- C:\Windows\system32\odbcad32.exe

3 Dans la fenêtre Administrateur de sources de données ODBC, cliquez sur **Nom DSN système** et sélectionnez **svmanager** dans le volet Sources de données utilisateur.

4 Cliquez sur **Configurer**.

L'assistant Configuration de source de données de Microsoft SQL Server s'affiche.

5 Cliquez sur **Suivant**.

Attention Ne modifiez pas les informations existantes dans les zones de texte **Nom** ou **Serveur** de la source de données.

6 Assurez-vous que l'option **Avec l'authentification SQL Server utilisant un ID de connexion entré par l'utilisateur** est sélectionnée.

7 Entrez un nouveau mot de passe dans la zone de texte **Mot de passe** et cliquez sur **Suivant**.

8 Cliquez à nouveau sur **Suivant**, sans les remplacer par les informations existantes sur la page d'informations de base de données par défaut.

9 Cliquez sur **Terminer**.

La fenêtre Programme d'installation de ODBC pour Microsoft SQL Server s'affiche avec les détails de configuration.

10 Passez en revue les informations récapitulatives et cliquez sur **OK** pour poursuivre la modification du mot de passe pour le service VMware JMP Platform Services.

11 Ajoutez les nouvelles informations de mot de passe dans le fichier de configuration de base de données VMware JMP Platform Services avant de redémarrer le service VMware JMP Platform Services.

- a À l'aide d'un éditeur de texte, en tant qu'administrateur, ouvrez le fichier de configuration de base de données qui se trouve dans C:\Program Files (x86)\VMware\JMP\com\XMS\config\database.yml.
- b Recherchez la ligne correspondant à la propriété de nom d'utilisateur et insérez une nouvelle ligne après celle-ci.
- c Entrez les informations du mot de passe que vous avez créé afin qu'il s'affiche comme indiqué dans l'exemple suivant.

```
password: new_password
```

Important Ces informations de mot de passe sont automatiquement supprimées du fichier database.yml lorsque le service VMware JMP Platform Services est redémarré.

12 Redémarrez le service VMware JMP Platform Services.

- a Cliquez avec le bouton droit sur l'icône **Démarrer** de Windows et sélectionnez **Exécuter**.
- b Dans la boîte de dialogue Exécuter, tapez `services.msc` dans la zone de texte **Ouvrir**, puis cliquez sur **OK**.
- c Recherchez VMware JMP Platform Services dans le volet Services (local) de la fenêtre Services et cliquez sur **Démarrer**.

Suivant

Si vous ne l'avez pas déjà fait, vous devez également mettre à jour les informations de compte de connexion de base de données utilisées par VMware JMP File Share Service. Reportez-vous à la section [Mettre à jour le mot de passe de base de données pour VMware JMP File Share Service](#).

Mettre à jour le mot de passe de base de données pour VMware JMP File Share Service

Si vous modifiez le mot de passe de base de données SQL Server qui a été utilisé lorsque JMP Server a été installé, vous devez également mettre à jour le mot de passe de base de données qui est utilisé par VMware JMP File Share Service pour vous connecter à la base de données SQL Server.

Prérequis

Vérifiez que vous disposez des privilèges d'administration corrects pour modifier les informations de base de données dans l'hôte JMP Server.

Procédure

- 1 Dans l'hôte JMP Server, arrêtez le processus VMware JMP File Share Service à l'aide de l'outil Gestionnaire des services Windows.
 - a Cliquez avec le bouton droit sur l'icône **Démarrer** de Windows et sélectionnez **Exécuter**.
 - b Dans la boîte de dialogue Exécuter, tapez `services.msc` dans la zone de texte **Ouvrir**, puis cliquez sur **OK**.
 - c Recherchez VMware JMP File Share Service dans le volet Services (local) de la fenêtre Services et cliquez sur **Arrêter**.
- 2 Mettez à jour le mot de passe utilisé par VMware JMP File Share Service. Utilisez les informations suivantes pour déterminer les étapes à utiliser en fonction du type de connexion de SQL Server utilisé lors de l'installation de JMP Server.
 - Pour le mode de connexion de l'authentification SQL :
 - 1 Ouvrez une fenêtre d'invite de commande en tant qu'administrateur.

- 2 Copiez les commandes suivantes et modifiez les informations <password> avec la nouvelle valeur de mot de passe.

```
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 Collez les commandes dans la fenêtre d'invite de commande et appuyez sur Entrée.

■ Pour le mode de connexion de l'authentification Windows :

- 1 Accédez au dossier C:/Program Files (x86)/VMware/JMP/com/uem et ouvrez le fichier db.json dans un éditeur de texte.
- 2 Remplacez le contenu de fichier existant par le contenu suivant, où <IP address> est l'adresse IP de l'hôte SQL Server et <Database name> est le nom de la base de données valide.

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

- 3 Enregistrez le fichier.

3 Redémarrez VMware JMP File Share Service.

- a Cliquez avec le bouton droit sur l'icône **Démarrer** de Windows et sélectionnez **Exécuter**.
- b Dans la boîte de dialogue Exécuter, tapez `services.msc` dans la zone de texte **Ouvrir**, puis cliquez sur **OK**.
- c Recherchez VMware JMP File Share Service dans le volet Services (local) de la fenêtre Services et cliquez sur **Démarrer**.

Suivant

Si vous ne l'avez pas déjà fait, vous devez également mettre à jour les informations de compte de connexion de base de données utilisées par VMware JMP Platform Services. Reportez-vous à la section [Mettre à jour le mot de passe de base de données pour VMware JMP Platform Services](#).

Dépannage de votre JMP Server

Vous pouvez rencontrer des messages d'erreur lors de l'installation, de la configuration et de l'enregistrement de votre instance de JMP Server. Vous pouvez utiliser les informations de dépannage contenues dans ce chapitre.

Erreur JMP Server n'est pas disponible

Vous ne parvenez pas à vous connecter à votre instance de JMP Server.

Problème

Lorsque vous utilisez la Horizon Console pour enregistrer votre instance de JMP Server, vous pouvez voir le message d'erreur Le JMP Server que vous avez entré n'est pas disponible. Modifiez votre entrée ou réessayez ultérieurement.

Cause

Le message d'erreur peut s'afficher pour plusieurs raisons. Pour déterminer la cause et la solution, utilisez les informations dans la section suivante.

Solution

- 1 Assurez-vous que les certificats sont correctement configurés.

Utilisez les informations contenues dans la section [Configuration de certificats TLS et de suites de chiffrement pour JMP Server](#).

- 2 Après avoir essayé d'enregistrer l'URL de JMP Server, examinez la réponse HTTP dans un navigateur Web.

Si vous avez reçu une réponse HTTP semblable à la sortie suivante,

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

suivez les étapes ci-dessous pour vérifier que le compte d'utilisateur que vous avez utilisé pour vous connecter à Horizon Console dispose des privilèges d'administrateur suffisants.

- a Dans Horizon Administrator, sélectionnez **Configuration de View > Administrateurs**.

- b Dans le volet Administrateur, vérifiez que votre compte d'utilisateur administrateur s'affiche sous la forme *<nom-domaine>\Administrator* (et non BUILTIN\Administrator) et qu'il dispose de privilèges administrateur complets.
- c Si vous voyez BUILTIN\Administrator, appliquez la solution décrite dans les [Notes de mise à jour de VMware Horizon 7 version 7.5](#).

Pour plus d'informations sur la gestion des autorisations d'administrateur, reportez-vous à la section « Gérer et consulter des autorisations » dans le document *Administration d'Horizon 7*.

- 3 Si des messages JSON Web Token (JWT) dans la réponse HTTP du navigateur Web sont similaires au message d'erreur suivant `{"code":403,"error":"Error: Unable to verify Horizon JWT","error_code":"1044","error_type":"horizonJwtVerificationError"}`, assurez-vous que les heures de votre hôte JMP Server et de l'hôte Horizon Connection Server sont synchronisées.

Utilisez les informations fournies dans la section [Synchroniser l'heure entre des hôtes de Serveur de connexion Horizon et de JMP Server](#).