

VMware Horizon JMP Server 설치 및 설정 가이드

2019년 12월

VMware Horizon 7 7.11



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

docfeedback@vmware.com

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

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

Copyright © 2018–2019 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

1	VMware Horizon JMP Server 설치 및 설정 가이드	5
2	JMP Server 설치 및 구성 작업 개요	6
3	JMP Server에 대한 시스템 요구 사항	8
	필수 JMP 기술 구성 요소	8
	JMP Server에 대한 하드웨어 요구 사항	8
	JMP Server에 대해 지원되는 운영 체제	9
	JMP Server에 대한 네트워크 요구 사항	9
	JMP Server에 대한 데이터베이스 요구 사항	10
	JMP Integrated Workflow에 대해 지원되는 웹 브라우저	10
4	JMP Server에 대한 SQL Server 데이터베이스 및 로그인 준비	12
	JMP Server용 SQL Server 데이터베이스 생성	12
	JMP Server 호스트에 대한 SQL Server 로그인 생성	13
	JMP Server 호스트에 대한 SQL Server Windows 인증 로그인 생성	14
	JMP Server 호스트에 대한 SQL Server 인증 로그인 생성	15
	Windows 사용자에게 데이터베이스 소유자 및 시스템 관리 권한 부여	16
5	JMP Server 설치 및 업그레이드	18
	JMP Server 설치	18
	JMP Server 업그레이드	21
6	JMP Server 인스턴스 구성	23
	Horizon 연결 서버와 JMP Server 호스트 사이의 시간 동기화	23
	JMP Server에 대한 TLS 인증서 및 암호 그룹 구성	24
	JMP Server용 TLS 인증서 설정 작업 개요	24
	기본 TLS 인증서 교체	26
	인증서 체인 파일을 사용하도록 JMP Server 구성	28
	Active Directory에 대한 인증서를 사용하도록 JMP Server 구성	28
	Horizon 연결 서버 인증서를 사용하도록 JMP Server 구성	29
	App Volumes Manager의 인증서를 사용하도록 JMP Server 구성	31
	JMP Server에 대한 암호 그룹 구성	32
	JMP Server에 대해 더 제한적인 CORS 정책 사용	33
7	JMP Server 설치 후 데이터베이스 암호 업데이트	35
	VMware JMP 플랫폼 서비스에 대한 데이터베이스 암호 업데이트	35
	VMware JMP 파일 공유 서비스에 대한 데이터베이스 암호 업데이트	37

8 JMP Server 문제 해결 39

JMP Server를 사용할 수 없음 오류 39

서비스 계정 암호가 업데이트된 후 오류가 발생함 40

JMP Server 제거 41

VMware Horizon JMP Server 설치 및 설정 가이드

1

“VMware Horizon JMP Server 설치 및 설정 가이드”에서는 VMware Horizon® JMP(Just-in-Time Management Platform) Server를 설치하고 구성하는 방법에 대해 설명합니다. JMP Server를 설치하고 JMP 설정을 구성한 후 VMware Horizon Console의 JMP Integrated Workflow 기능을 사용하여 JMP 할당 정의를 시작할 수 있습니다.

이 문서의 정보는 JMP Server를 설치하려는 모든 사용자를 대상으로 합니다. 이 정보는 가상 시스템 기술과 데이터 센터 운영을 잘 아는 숙련된 Windows 시스템 관리자를 대상으로 작성되었습니다.

JMP Server 설치 및 구성 작업 개요

2

Horizon JMP Server를 설치하기 전과 설치한 후, HorizonJMP Integrated Workflow 기능을 사용하기 전에 특정 작업을 수행해야 합니다.

다음 목록에서는 완료해야 하는 작업에 대한 개괄적인 설명을 제공합니다. 이러한 작업을 수행하는 절차는 이 개요 다음에 이어지는 항목에서 설명합니다.

- 1 JMP Server 시스템 요구 사항이 충족되었는지 확인합니다. [장 3 JMP Server에 대한 시스템 요구 사항](#)의 내용을 참조하십시오.
- 2 설치 중에 생성된 JMP Server 서비스에 대한 정보를 저장하는 데 사용되는 SQL Server 데이터베이스를 생성합니다. [JMP Server용 SQL Server 데이터베이스 생성](#)의 내용을 참조하십시오.
- 3 이전 단계에서 생성한 SQL Server 데이터베이스에 연결할 JMP Server 호스트에서 사용되는 SQL Server 로그인을 생성합니다. 자세한 내용은 [JMP Server 호스트에 대한 SQL Server 로그인 생성](#)에 나와 있습니다.
- 4 JMP Server를 설치하는 데 사용되는 Windows 사용자 로그인에 JMP Server 서비스 관련 정보를 저장하기 위해 생성한 SQL Server 데이터베이스를 수정할 수 있는 충분한 권한이 있는지 확인합니다. [Windows 사용자에게 데이터베이스 소유자 및 시스템 관리 권한 부여](#)의 내용을 참조하십시오.
- 5 (선택 사항) 이전 단계에서 사용된 SQL Server가 TLS 암호화를 사용하는 경우 해당 TLS 인증서를 JMP Server 호스트의 Windows 로컬 인증서 저장소로 가져옵니다. SQL Server의 TLS 인증서 내보내기 및 가져오기에 대한 자세한 내용은 Microsoft TechNet 문서 [Microsoft Management Console을 사용하여 SQL Server 인스턴스에 대해 SSL 암호화를 활성화하는 방법](#)의 "특정 클라이언트에 대해 암호화 사용" 섹션을 참조하십시오.
- 6 JMP Server를 설치합니다. [JMP Server 설치](#)의 내용을 참조하십시오.
- 7 Horizon Connection Server 호스트와 JMP Server 인스턴스용 Windows 호스트 간의 시간을 동기화합니다. [Horizon 연결 서버와 JMP Server 호스트 사이의 시간 동기화](#)의 내용을 참조하십시오.
- 8 VMware Horizon 7 연결 서버, VMware App Volumes™ Manager, VMware User Environment Manager™ 및 조직의 네트워크에 있는 기타 시스템의 인스턴스와 안전하게 통신하도록 JMP Server 인스턴스에 대한 TLS 인증서를 구성합니다. [JMP Server에 대한 TLS 인증서 및 암호 그룹 구성](#)의 내용을 참조하십시오.
- 9 (선택 사항) JMP Server 인스턴스가 지원하는 기본 암호 그룹을 조직에서 지원하는 암호 그룹으로 변경합니다. [JMP Server에 대한 암호 그룹 구성](#)의 내용을 참조하십시오.

- 10 (선택 사항) Horizon 7 연결 서버 인스턴스와 더 안전하게 통신할 수 있도록 JMP Server 인스턴스에서 더 제한적인 원본 간 리소스 공유(CORS) 정책을 사용하십시오. [JMP Server에 대해 더 제한적인 CORS 정책 사용](#)의 내용을 참조하십시오.
- 11 "VMware Horizon Console 관리" 문서의 "처음으로 JMP 설정 구성"을 사용하여 JMP 설정을 구성하기 전에 Windows 시스템 관리자를 사용하여 JMP Server를 다시 시작합니다.

JMP Server에 대한 시스템 요구 사항

3

VMware Horizon JMP Server를 설치하고 JMP Integrated Workflow 기능을 사용하려면 특정 하드웨어 및 소프트웨어 요구 사항이 충족되어야 합니다.

본 장은 다음 항목을 포함합니다.

- 필수 JMP 기술 구성 요소
- JMP Server에 대한 하드웨어 요구 사항
- JMP Server에 대해 지원되는 운영 체제
- JMP Server에 대한 네트워크 요구 사항
- JMP Server에 대한 데이터베이스 요구 사항
- JMP Integrated Workflow에 대해 지원되는 웹 브라우저

필수 JMP 기술 구성 요소

JMP Server를 성공적으로 설치하려면 지원되는 Horizon 7 서버 버전이 이미 설치되어 있어야 합니다.

사용 가능한 모든 JMP Integrated Workflow 기능(예: 애플리케이션 제공 관리 및 상황별 정책 관리)을 사용하려면 JMP 기술을 구성하는 추가 VMware 제품도 설치해야 합니다. JMP Server를 설치하기 전 또는 설치한 후에 이러한 추가 제품을 설치할 수 있습니다. JMP Server를 설치한 후에 추가 제품을 설치하려면 Horizon Console을 사용하여 JMP Server를 재구성해야 합니다.

다음은 JMP 기술을 구성하는 지원되는 VMware 제품 버전입니다.

- VMware Horizon 7 7.5 이상(JMP Server 설치를 위한 최소 요구 사항)
- VMware App Volumes 2.xx, 버전 2.14 이상(실시간 애플리케이션 제공 관리용). App Volumes 4.0은 지원되지 않습니다.
- VMware Dynamic Environment Manager 9.2.1 이상(상황별 정책 관리용)
- VMware Identity Manager™ 2.9.2 이상(VMware Workspace™ ONE™과의 통합용)

JMP Server에 대한 하드웨어 요구 사항

특정 하드웨어 요구 사항을 충족하는 전용 물리적 또는 가상 시스템에 JMP Server를 설치해야 합니다.

다음 표에는 운영 환경의 JMP Server 인스턴스에 대한 최소 하드웨어 요구 사항이 나와 있습니다.

표 3-1. 운영 환경의 Horizon JMP Server 하드웨어 요구 사항

하드웨어 구성 요소	운영 환경에 필요한 최소값
프로세서	4코어 CPU
메모리	8GB
스토리지	100GB

다음 표에는 개념 증명(PoC) 및 테스트 환경의 JMP Server 인스턴스에 대한 최소 하드웨어 요구 사항이 나열되어 있습니다.

표 3-2. 테스트 환경의 Horizon JMP Server 하드웨어 요구 사항

하드웨어 구성 요소	테스트 환경에 필요한 최소값
프로세서	4코어 CPU
메모리	4GB
스토리지	25GB

JMP Server에 대해 지원되는 운영 체제

지원되는 Windows Server 운영 체제에 JMP Server를 설치해야 합니다.

두 가지 유형의 JMP Server 설치, 개념 증명(PoC) 및 운영이 다음 Windows Server 운영 체제에서 지원됩니다.

표 3-3. JMP Server에 대한 운영 체제 지원

운영 체제	버전	버전
Windows Server 2008 R2 SP1	64비트	Standard Enterprise 데이터 센터
Windows Server 2012 R2	64비트	Standard 데이터 센터
Windows Server 2016	64비트	Standard 데이터 센터

JMP Server에 대한 네트워크 요구 사항

JMP Server를 설치하려는 물리적 또는 가상 시스템이 네트워크 전반의 모든 PoD(Points of Delivery)에 대한 모든 제품 끝점에 연결할 수 있어야 합니다.

JMP Integrated Workflow 기능을 사용하기 전에 JMP Server 인스턴스 및 JMP Server 인스턴스와 상호 작용하는 모든 기술 끝점에 대한 모든 보안 및 CA에서 서명된 인증서 인증이 이미 구성되어 있어야 합니다. 자세한 내용은 [JMP Server에 대한 TLS 인증서 및 암호 그룹 구성](#)에 나와 있습니다.

JMP Server에 대한 데이터베이스 요구 사항

JMP Server 설치 관리자에서 JMP Server 설치를 수행하려면 특정 SQL Server 데이터베이스 버전이 필요합니다.

JMP Server에서는 두 가지 지원되는 워크로드 환경(개념 증명(PoC) 또는 운영)에서 다음과 같은 SQL Server 버전 및 에디션을 지원합니다.

표 3-4. JMP Server에 대한 데이터베이스 요구 사항

워크로드 유형	데이터베이스 서버	버전	버전
개념 증명(PoC)	SQL Server Express 2014	64비트	사용 가능
운영	SQL Server 2012(SP1, SP2, SP3 및 SP4)	64비트	Standard 및 Enterprise
운영	SQL Server 2014(CU7 이상이 적용된 SP1 및 SP2)	64비트	Standard 및 Enterprise
운영	SQL Server 2016(CU6 이상이 적용된 SP1)	64비트	Standard 및 Enterprise

JMP Server 설치 관리자를 실행하기 전에 JMP Server 설치 관리자에서 설치 프로세스 중에 사용하는 SQL Server 데이터베이스를 생성해야 합니다. 자세한 내용은 [JMP Server용 SQL Server 데이터베이스 생성](#)의 내용을 참조하십시오.

또한 JMP Server 설치 관리자에서 사용자가 생성한 SQL Server 데이터베이스에 연결하는 데 사용해야 하는 로그인 자격 증명을 제공해야 합니다. JMP Server 설치 관리자에서 사용하는 인증의 유형을 선택할 수 있습니다. 사용되는 기본값은 Windows 인증입니다. Windows 인증 또는 SQL Server 인증을 선택하든지 JMP Server 설치를 시작하기 전에 JMP Server 설치 관리자에서 사용하는 로그인 자격 증명에 SQL Server 인스턴스에 이미 있어야 합니다. 자세한 내용은 [JMP Server 호스트에 대한 SQL Server 로그인 생성](#)의 내용을 참조하십시오.

또한 JMP Server를 설치하는 데 사용할 Windows Server 사용자 계정에 대한 SQL Server 로그인을 생성해야 합니다. 생성한 SQL Server 데이터베이스를 수정할 수 있는 적절한 자격 증명을 가지도록 이 Windows 사용자를 구성해야 합니다.

SQL Server가 TLS 암호화를 사용하도록 설정된 경우 SQL Server와의 암호화된 통신을 가능하게 하려면 해당 TLS 인증서를 내보내고 이 인증서를 JMP Server 인스턴스로 가져와야 합니다.

JMP Integrated Workflow에 대해 지원되는 웹 브라우저

VMware Horizon 7 연결 서버 버전 7.5 이상과 함께 설치되는 웹 기반 애플리케이션인 VMware Horizon 콘솔을 사용하여 JMP Integrated Workflow 사용자 인터페이스(UI)에 액세스합니다.

JMP Integrated Workflow 기능과 함께 사용하도록 지원되는 웹 브라우저는 다음과 같습니다.

- Google Chrome(최신 버전이 지원됨)
- Mozilla Firefox(최신 버전이 지원됨)
- Internet Explorer 10 및 11

- Microsoft Edge

JMP Server에 대한 SQL Server 데이터베이스 및 로그인 준비

4

JMP Server 설치 관리자를 실행하기 전에 사용할 JMP Server 인스턴스에 대한 SQL Server 데이터베이스를 생성해야 합니다. JMP Server 설치 관리자에서 SQL Server 데이터베이스에 연결하는 데 필요한 SQL Server 로그인 계정도 생성해야 합니다. 또한 JMP Server 설치 관리자를 실행하는 데 사용되는 Windows Server 로그인 계정에 JMP Server용으로 생성한 SQL Server 데이터베이스에 대한 적절한 액세스 권한이 있어야 합니다.

본 장은 다음 항목을 포함합니다.

- JMP Server용 SQL Server 데이터베이스 생성
- JMP Server 호스트에 대한 SQL Server 로그인 생성
- Windows 사용자에게 데이터베이스 소유자 및 시스템 관리 권한 부여

JMP Server용 SQL Server 데이터베이스 생성

Horizon 데스크톱 관리자가 생성하는 JMP Server 서비스 및 JMP 할당에 대한 정보는 SQL Server 데이터베이스에 저장됩니다. JMP Server 설치 관리자를 실행하기 전에 이 데이터베이스를 생성해야 합니다.

참고 원격 SQL Server는 호스트 장애가 발생할 경우에 유용합니다.

사전 요구 사항

- 지원되는 SQL Server 버전이 JMP Server를 설치하려는 호스트에서 원격이지만 사용 중인 네트워크 환경에 포함되는 시스템에 설치되어 있는지 확인합니다. 자세한 내용은 [JMP Server에 대한 데이터베이스 요구 사항](#)에 나와 있습니다.
- SQL Server Management Studio를 사용하여 데이터베이스를 생성하고 관리하는지 확인하십시오. PoC 환경에서 JMP Server를 설치하는 경우 SQL Server Management Studio Express를 사용할 수 있습니다. 다음 웹 사이트에서 다운로드하여 설치합니다.

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

절차

- 1 Microsoft SQL Server가 설치된 시스템에서 **시작 > 모든 프로그램 > Microsoft SQL Server 2016, Microsoft SQL Server 2014** 또는 **Microsoft SQL Server 2012**를 선택합니다.
- 2 **SQL Server Management Studio**를 선택합니다.

3 [개체 탐색기] 창에서 SQL Server 데이터베이스 엔진의 인스턴스에 연결한 다음 해당 인스턴스에 대한 노드를 확장합니다.

4 **데이터베이스**를 마우스 오른쪽 버튼으로 클릭하고 **새 데이터베이스**를 선택합니다.

5 **데이터베이스 이름** 텍스트 상자에서 ASCII 문자만 사용하여 JMP Server에 대해 생성할 이름을 입력합니다.

예: JMPDB

중요 ASCII가 아닌 문자는 지원되지 않습니다.

6 데이터베이스 및 로그 파일에 대한 Initial size 및 Autogrowth 매개변수에는 기본값을 사용합니다.

7 **확인**을 클릭합니다.

SQL Server Management Studio에서 [개체 탐색기] 창의 **데이터베이스** 폴더에 데이터베이스를 추가합니다.

8 Microsoft SQL Server Management Studio를 종료하십시오.

다음에 수행할 작업

JMP Server를 설치하기 전에 JMP Server 호스트에 대한 SQL Server 로그인을 생성합니다. [JMP Server 호스트에 대한 SQL Server 로그인 생성](#)의 내용을 참조하십시오.

JMP Server 호스트에 대한 SQL Server 로그인 생성

JMP Server 설치 동안 설치 관리자에서 사용자가 생성한 SQL Server 데이터베이스에 액세스하여 설치 중인 JMP Server 서비스에 대한 정보를 저장합니다. JMP Server 설치 관리자에서 사용할 SQL Server 로그인 유형을 선택해야 합니다.

생성한 SQL Server 데이터베이스에 액세스하려면 Windows 인증 로그인 또는 SQL Server 인증 로그인을 선택합니다. 기본적으로 Windows 인증 로그인이 사용됩니다. JMP Server 설치 관리자를 실행하기 전에 선택한 SQL Server 로그인 유형에 대한 자격 증명이 있는지 확인합니다.

다음 표를 사용하여 JMP Server 설치 관리자에서 사용할 SQL Server 로그인을 생성하기 위해 완료해야 하는 작업을 확인합니다.

표 4-1. SQL Server 로그인 유형

SQL Server 로그인 유형	섹션에서 작업 세부 정보 사용
Windows 인증(기본값)	JMP Server 호스트에 대한 SQL Server Windows 인증 로그인 생성
SQL Server 인증	JMP Server 호스트에 대한 SQL Server 인증 로그인 생성

JMP Server 호스트에 대한 SQL Server Windows 인증 로그인 생성

사용자가 생성한 SQL Server 데이터베이스에 액세스할 때 Windows 인증 로그인을 사용하도록 JMP Server 설치 관리자를 지정할 수 있습니다. JMP Server 설치 관리자를 실행하기 전에 JMP Server를 설치하는 JMP Server 호스트에 대한 해당 SQL Server 로그인의 자격 증명이 있어야 합니다.

JMP Server 호스트에 연결된 사용자는 JMP SQL Server 데이터베이스에 액세스할 수 있습니다. 그러나 JMP Server를 설치하는 데 사용된 Windows Server 사용자 계정에 JMP Server용으로 생성한 SQL Server 데이터베이스에 대한 쓰기 액세스 권한이 있는지도 확인해야 합니다. [Windows 사용자에게 데이터베이스 소유자 및 시스템 관리 권한 부여](#)의 내용을 참조하십시오.

사전 요구 사항

JMP Server 인스턴스용 SQL Server 데이터베이스를 생성했는지 확인합니다. 데이터베이스를 생성하려면 [JMP Server용 SQL Server 데이터베이스 생성](#)의 내용을 참조하십시오.

절차

- 1 sysadmin(SA)으로 SQL Server Management Studio 세션에 로그인하거나 SA 권한이 있는 사용자 계정을 사용합니다.
- 2 개체 탐색기 창에서 JMP Server 인스턴스용 데이터베이스를 생성한 SQL Server 인스턴스에 대한 폴더를 확장합니다.
- 3 **보안** 폴더를 확장하고 **로그인**을 마우스 오른쪽 버튼으로 클릭한 후 **새 로그인**을 선택합니다.
- 4 **로그인 - 신규** 대화 상자의 **일반** 페이지에서 `domain_name\computer_name$` 형식의 로그인을 이름을 입력합니다. 여기서 `computer_name`은 JMP Server 호스트의 이름이고 `domain_name`은 호스트가 속한 도메인입니다.

예: mycompanyWjmpserver\$

- 5 **Windows 인증**을 선택합니다.
- 6 **기본 데이터베이스** 목록에서 로그인을 위한 기본 데이터베이스를 선택합니다. 마스터 데이터베이스가 이 항목의 기본값입니다.
- 7 **기본 언어** 목록에서 로그인에 사용할 기본 언어를 선택합니다.
- 8 새 로그인 계정에 대해 sysadmin 서버 역할을 할당합니다.
 - a 왼쪽에 있는 [페이지 선택] 창에서 **서버 역할** 탭을 클릭합니다.
 - b [서버 역할] 페이지에서 **sysadmin** 확인란을 선택합니다.
- 9 **확인**을 클릭합니다.

개체 탐색기 창의 **로그인** 폴더 아래에 새 로그인이 추가됩니다.

다음에 수행할 작업

JMP Server를 설치하는 데 사용되는 Windows Server 사용자 계정에 대한 SQL Server 로그인 자격 증명을 생성합니다. [Windows 사용자에게 데이터베이스 소유자 및 시스템 관리 권한 부여](#)의 내용을 참조하십시오.

JMP Server 호스트에 대한 SQL Server 인증 로그인 생성

SQL Server 인증 로그인을 사용하여 사용자가 생성한 SQL Server 데이터베이스에 액세스하는 SQL Server 로그인을 사용하도록 JMP Server 설치 관리자를 지정할 수 있습니다. JMP Server 설치 관리자를 실행하기 전에 JMP Server 호스트에 대한 SQL Server 로그인 유형의 로그인 자격 증명이 있어야 합니다.

사전 요구 사항

JMP Server용 SQL Server 데이터베이스를 생성했는지 확인합니다. 데이터베이스를 생성하려면 [JMP Server용 SQL Server 데이터베이스 생성](#)의 내용을 참조하십시오.

절차

- 1 sysadmin(SA)으로 또는 SA 권한이 있는 사용자 계정을 사용하여 SQL Server Management Studio 세션에 로그인합니다.
- 2 개체 탐색기 창에서 JMP Server 데이터베이스를 생성한 SQL Server 인스턴스에 대한 폴더를 확장합니다.
- 3 **보안** 폴더를 확장하고 **로그인**을 마우스 오른쪽 버튼으로 클릭한 후 **새 로그인**을 선택합니다.
- 4 **로그인 - 신규** 대화 상자의 **일반** 페이지에서 ASCII 문자만을 사용하여 **로그인 이름** 텍스트 상자에 값을 입력합니다. 또는 **검색**을 클릭하고 **사용자 또는 그룹 선택** 대화 상자를 사용하여 사용할 로그인을 찾습니다.

중요 ASCII가 아닌 문자는 지원되지 않습니다.

- 5 **SQL Server 인증**을 선택합니다.
- 6 **암호 및 암호 확인** 텍스트 상자에 새 로그인 이름의 암호를 입력합니다. ASCII 문자만 사용합니다.
- 7 기존 암호를 변경하는 경우 **이전 암호 지정**을 선택한 다음 **이전 암호** 텍스트 상자에 이전 암호를 입력합니다.
- 8 조직의 정책에 따라 **암호 정책 강제 적용**, **암호 만료 강제 적용** 및 **다음 로그인할 때 반드시 암호 변경** 확인란을 선택하거나 선택 취소합니다.
- 9 **기본 데이터베이스** 목록에서 로그인을 위한 기본 데이터베이스를 선택합니다. 마스터 데이터베이스가 이 항목의 기본값입니다.
- 10 **기본 언어** 목록에서 로그인을 위한 기본 언어를 선택합니다.
- 11 새 로그인 계정에 대해 sysadmin 서버 역할을 할당합니다.
 - a 왼쪽에 있는 [페이지 선택] 창에서 **서버 역할** 탭을 클릭합니다.
 - b [서버 역할] 페이지에서 **sysadmin** 확인란을 선택합니다.
- 12 **확인**을 클릭합니다.

개체 탐색기 창의 **로그인** 폴더 아래에 새 로그인이 추가됩니다.

다음에 수행할 작업

JMP Server를 설치하는 데 사용되는 Windows Server 사용자 계정에 대한 SQL Server 로그인 자격 증명을 생성합니다. [Windows 사용자에게 데이터베이스 소유자 및 시스템 관리 권한 부여](#)의 내용을 참조하십시오.

Windows 사용자에게 데이터베이스 소유자 및 시스템 관리 권한 부여

JMP Server 호스트 시스템에 대한 SQL Server 로그인을 생성하는 것 외에도 JMP Server 인스턴스를 설치하는 데 사용할 Windows 사용자 계정을 생성해야 합니다. 이 Windows 사용자 계정에는 사용자가 생성한 SQL Server 데이터베이스의 sysadmin 및 데이터베이스 소유자 권한을 부여해야 합니다.

사전 요구 사항

- 설치하려는 JMP Server에 대한 SQL Server 데이터베이스가 생성되었는지 확인합니다. [JMP Server용 SQL Server 데이터베이스 생성](#)의 내용을 참조하십시오.
- JMP Server 호스트에 대한 SQL Server 로그인이 생성되었는지 확인합니다. [JMP Server 호스트에 대한 SQL Server 로그인 생성](#)의 내용을 참조하십시오.

절차

- 1 sysadmin(SA)으로 SQL Server Management Studio 세션에 로그인하거나 SA 권한이 있는 사용자 계정을 사용합니다.
- 2 개체 탐색기 창에서 JMP Server에 대해 생성한 SQL Server 인스턴스에 연결합니다.
- 3 JMP Server를 설치하는 데 사용하려는 Windows 사용자 계정에 대한 SQL Server 로그인을 생성합니다.
 - a **보안** 폴더를 확장하고 **로그인**을 마우스 오른쪽 버튼으로 클릭한 후 **새 로그인**을 선택합니다.
 - b **로그인 - 신규** 대화 상자에서 **검색**을 클릭합니다.
 - c **사용자 또는 그룹 선택** 대화 상자에서 JMP Server를 설치하는 데 사용하려는 유효한 Active Directory 사용자를 선택합니다.
 - d [로그인 - 신규] 대화 상자의 [페이지 선택] 아래에서 **서버 역할**을 선택하고 **sysadmin** 확인란을 선택합니다.
 - e **확인**을 클릭하여 **로그인 - 신규** 대화 상자를 닫습니다.
- 4 Windows 사용자 계정에 사용 권한을 부여합니다.
 - a 왼쪽 창에서 **데이터베이스**를 클릭합니다.
 - b JMP Server 인스턴스용으로 생성한 데이터베이스를 선택하고 **보안**을 클릭한 후 **사용자**를 클릭합니다.
 - c [사용자] 창에서 Windows 사용자 로그인을 마우스 오른쪽 버튼으로 클릭한 후 상황에 맞는 메뉴에서 **속성**을 선택합니다.

d [데이터베이스 역할 멤버 자격] 아래에서 **db_owner** 역할을 선택합니다.

e **확인**을 클릭합니다.

개체 탐색기 창의 **로그인** 폴더 아래에 새 로그인 이 추가됩니다.

다음에 수행할 작업

[JMP Server 설치](#) 의 정보를 사용하여 JMP Server 인스턴스를 설치합니다.

JMP Server 설치 및 업그레이드

5

JMP Integrated Workflow 기능을 사용하려면 먼저 JMP Server 인스턴스와 필수 VMware JMP 기술 제품을 설치하여 구성해야 합니다. 새 버전의 JMP Server 설치 관리자를 사용하여 JMP Server 설치를 업그레이드할 수 있습니다.

참고 Horizon 7 버전 7.5 릴리스에서는 하나의 JMP Server 인스턴스만 설치할 수 있습니다.

참고 현재 JMP Server 인스턴스를 업그레이드하려면 [JMP Server 업그레이드](#)에 설명된 대로 설치 관리자를 사용하는 것이 가장 좋습니다. 업그레이드 설치 관리자는 JMP Server 업그레이드를 수행하는 기본 방법입니다.

기본 설정 설치 관리자를 업그레이드에 사용하지 않고, 대신 현재 JMP Server 인스턴스를 제거하고 새 인스턴스를 설치하도록 선택하는 경우 다음 제한 사항을 확인하십시오. 새 JMP Server 인스턴스는 이전 JMP Server 인스턴스에서 기존 데이터베이스에 생성된 JMP 구성 또는 할당 데이터를 사용할 수 없습니다. 새 JMP Server 인스턴스에서 기존 JMP 구성 및 할당을 사용하려면 다음 단계를 순서대로 수행합니다.

- 1 JMP Server 인스턴스를 제거하기 전에 C:\Windows\System32\config\systemprofile\AppData\Local\VMware\JMP에 있는 .encryption.key 파일의 백업 복사본을 만듭니다.
- 2 JMP Server 인스턴스를 제거합니다.
- 3 JMP Server의 새 인스턴스를 설치합니다.
- 4 C:\Windows\System32\config\systemprofile\AppData\Local\VMware\JMP로 이동한 후 .encryption.key 파일을 찾습니다. 이 파일을 이전에 생성한 백업 키 파일로 바꿉니다.
- 5 VMware JMP Platform Services를 다시 시작합니다.

본 장은 다음 항목을 포함합니다.

- [JMP Server 설치](#)
- [JMP Server 업그레이드](#)

JMP Server 설치

JMP Integrated Workflow 기능을 사용하려면 먼저 JMP Server를 설치 및 구성해야 합니다.

VMware Horizon 7 버전 7.5 이상을 다운로드하면 JMP Server 설치 관리자 파일이 포함됩니다. Horizon 7 버전 7.5 이상을 설치한 후 JMP Server 설치 관리자를 별도로 실행해야 합니다.

사전 요구 사항

- JMP Server를 설치하는 데 필요한 구성 요소에 대한 시스템 요구 사항을 충족하는지 확인합니다. [장 3 JMP Server에 대한 시스템 요구 사항](#)의 내용을 참조하십시오.
- Windows Server 호스트에서 JMP Server 설치 관리자를 실행하려면 해당 호스트 시스템에 대한 관리 권한이 있는 도메인 사용자 계정을 사용 해야 합니다.
- JMP Server 인스턴스에서 사용해야 하는 SQL Server 데이터베이스가 원격 시스템에서 생성되었고 이에 대한 적절한 액세스 권한이 있는지 확인합니다. [JMP Server용 SQL Server 데이터베이스 생성](#)의 내용을 참조하십시오.
- JMP Server를 설치하는 데 사용할 JMP Server 호스트 및 Windows 도메인 사용자 계정에 대한 SQL Server 로그인 및 사용 권한이 구성되었는지 확인합니다. [JMP Server 호스트에 대한 SQL Server 로그인 생성](#)의 내용을 참조하십시오.
- JMP Integrated Workflow 기능과 함께 사용될 보안 또는 비보안 HTTP 포트, UI 포트 및 서명된 인증서에 대한 정보를 수집합니다.
- 인증 기관에서 서명된 TLS 인증서를 가져온 후 이를 사용하여 JMP Server 설치 관리자에서 설치된 기본 TLS 인증서를 교체합니다.
- JMP Server를 설치하기 전에 다음 표를 사용하여 사용할 설치 유형을 확인합니다.

설치 유형	JMP Server 설치 관리자에서 수행되는 작업
운영 환경	SQL Server Standard 또는 Enterprise Edition을 사용하는 JMP Server 인스턴스를 생성합니다.
개발 또는 개념 증명(PoC) 환경	SQL Server Express를 사용하는 JMP Server 인스턴스를 생성합니다.

- JMP Server를 설치하기 전에 다음 파일을 McAfee Antivirus 제외 목록에 추가합니다.
 - C:\Program Files (x86)\VMware\JMP\Wnssm-2.24\Wnssm-2.24\Win32\Wnssm.exe
 - C:\Program Files (x86)\VMware\JMP\Wcom\Wxmp\Wnode_modules\Wwinser\Wbin\Wnssm.exe

절차

- 1 **VMware JMP Installer** 마법사를 시작하려면 JMP Server 설치 관리자 파일을 찾아 두 번 클릭합니다.

JMP Server 설치 관리자 파일 이름은 VMware-Jmp-Installer-e.x.p-xxxxxxx.exe입니다. 여기서 xxxxxxx는 빌드 번호입니다. 예를 들어, VMware-Jmp-Installer-e.x.p-7259616.exe입니다.

참고 설치 프로세스를 기록하려면 명령 프롬프트에서 다음 명령을 사용하여 JMP Server 설치 관리자를 실행합니다. 여기서 Log_Folder_Path는 로그 파일이 생성될 폴더입니다.

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

- 2 시작 페이지에서 **다음**을 클릭하고 VMware 사용 약관에 동의합니다.

3 HTTPS 트래픽을 허용하려면 **다음**을 클릭합니다.

참고 JMP Server는 포트 443과 선택적으로 포트 80, 3000-3004, 888 및 8889를 사용합니다. 포트 80을 통한 HTTP 트래픽을 허용하려면 **HTTP 허용** 확인란을 선택합니다.

4 SQL Server 인스턴스 및 데이터베이스 카탈로그 정보를 제공합니다.

- a JMP Server에 대해 생성한 데이터베이스에 연결하기 위한 SQL Server 인스턴스의 이름 또는 IP 주소를 입력합니다. 선택적으로 **찾아보기**를 클릭하여 선택합니다.
- b SQL Server 데이터베이스에 연결하는 데 사용할 인증 자격 증명을 선택합니다.

옵션	설명
현재 사용자의 Windows 인증 자격 증명	이 설치 프로세스 중에 사용하는 관리자 자격 증명은 SQL Server 데이터베이스 인스턴스에 연결하는 데 사용됩니다.
다음 로그인 ID 및 암호를 사용하여 서버 인증	SQL Server 데이터베이스 인스턴스에 연결하는 데 사용할 로그인 ID 및 암호 정보를 제공합니다. 참고 암호는 SQL 인증 암호로 작동하며 , ; = () . 문자를 포함하지 않아야 합니다. 암호에 이러한 문자가 포함되어 있으면 Dynamic Environment Manager 구성 요소의 설치가 실패하고 롤백됩니다.

참고 사용하는 로그인 자격 증명은 JMP Server에서 액세스할 SQL Server 인스턴스에 이미 구성되어 있어야 합니다. [JMP Server 호스트에 대한 SQL Server 로그인 생성](#)의 내용을 참조하십시오.

- c **데이터베이스 카탈로그 이름** 텍스트 상자에 [JMP Server용 SQL Server 데이터베이스 생성](#)을 사용하여 생성한 데이터베이스의 이름을 입력합니다. 선택적으로 **찾아보기**를 클릭하고 사용 가능한 목록에서 데이터베이스 카탈로그를 선택합니다.

선택한 데이터베이스 카탈로그는 JMP Server 서비스에 대한 정보를 저장하는 데 사용됩니다.

- d (선택 사항) 기존 데이터베이스를 덮어쓰려는 경우 **기존 데이터베이스 덮어쓰기** 확인란을 선택합니다.

참고 JMP Server 설치 관리자가 처음 실행될 때 필요한 데이터베이스 테이블이 생성됩니다. 로드 밸런싱을 위해 추가 JMP Server 인스턴스를 생성하도록 설치 관리자를 다시 실행하면 설치 관리자에서 데이터베이스가 이미 있음을 확인하고 테이블을 다시 생성하지 않습니다. 이 옵션을 선택하면 데이터베이스의 기존 정보가 덮어써집니다.

- e JMP Server와 SQL Server 인스턴스 간에 안전하게 통신하려면 **SSL 사용** 확인란이 선택되었는지 확인합니다. **SSL 사용** 확인란은 기본적으로 선택되어 있습니다.

중요 SSL 사용 확인란이 선택되어 있으면 SQL Server에서 사용되는 TLS/SSL 인증서를 JMP Server 호스트의 Windows 로컬 인증서 저장소로 가져왔는지 확인합니다. 그렇지 않으면 JMP Server 설치 프로세스는 "uem_migrate.bat 파일을 실행하지 못했습니다." 오류를 표시하며 실패하고, 오류 대화 상자에서 **확인**을 클릭하면 설치가 롤백됩니다.

SQL Server의 TLS/SSL 인증서 내보내기 및 가져오기에 대한 자세한 내용은 Microsoft TechNet 문서 [Microsoft Management Console을 사용하여 SQL Server 인스턴스에 대해 SSL 암호화를 활성화하는 방법](#)의 "특정 클라이언트에 대해 암호화 사용" 섹션을 참조하십시오.

- f 다음을 클릭합니다.

5 프로그램 설치 준비 완료 페이지에서 **설치**를 클릭합니다.

6 설치가 성공적으로 완료되면 **마침**을 클릭합니다.

성공적으로 설치되면 다음 JMP Server 서비스가 Windows Server 호스트에 설치되어 시작됩니다.

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

다음에 수행할 작업

새로 설치된 JMP Server 인스턴스 및 연결된 Horizon Connection Server 사이의 시간을 동기화합니다. [Horizon 연결 서버와 JMP Server 호스트 사이의 시간 동기화](#)의 내용을 참조하십시오.

JMP Server 업그레이드

현재 JMP Server 설치를 JMP Server의 최신 버전으로 업그레이드할 경우 모든 기존 JMP 설정 구성 및 JMP 할당이 보존됩니다.

Horizon 7 버전 7.5 이상을 다운로드하면 JMP Server 설치 관리자 파일이 포함됩니다. 기존 JMP Server 설치를 업그레이드하려면 Horizon 7 버전 7.6 이상을 설치한 후 JMP Server 설치 관리자를 별도로 실행해야 합니다.

사전 요구 사항

해당 호스트 시스템에서 관리자 권한을 가진 도메인 사용자 계정을 사용하여 새 JMP Server 설치 관리자 파일을 실행해야 합니다.

절차

- 1 VMware JMP Installer** 마법사를 시작하려면 새 JMP Server 설치 관리자 파일을 찾아 두 번 클릭합니다.

설치 관리자는 기존 JMP Server 설치가 있는지 확인합니다.

- 2 JMP 업그레이드 대화 상자에서 **확인**을 클릭합니다.
- 3 [시작] 화면에서 **다음**을 클릭합니다.
- 4 라이선스 계약을 읽고 수락한 후 **다음**을 클릭합니다.
- 5 JMP Server 플랫폼 서비스 페이지에 대한 데이터베이스 서버에서 기존 데이터베이스 설정을 유지하고 **다음**을 클릭합니다.
- 6 **프로그램 설치 준비 완료** 페이지에서 **설치**를 클릭합니다.
설치가 진행되고 완료하는 데 몇 분 정도 걸립니다.
- 7 설치가 성공적으로 완료되면 **마침**을 클릭합니다.

성공적으로 업그레이드되면 3가지 JMP Server 서비스가 Windows Server 호스트에서 다시 시작됩니다.

JMP Server 인스턴스 구성

6

JMP Server 인스턴스를 설치한 후 JMP Server 인스턴스가 Horizon Connection Server로 인증하고 네트워크에 있는 다른 서버와 안전하게 통신할 수 있도록 구성 작업을 수행해야 합니다.

본 장은 다음 항목을 포함합니다.

- Horizon 연결 서버와 JMP Server 호스트 사이의 시간 동기화
- JMP Server에 대한 TLS 인증서 및 암호 그룹 구성

Horizon 연결 서버와 JMP Server 호스트 사이의 시간 동기화

두 서버 사이의 인증 프로세스를 성공적으로 완료하려면 Horizon 연결 서버와 JMP Server 호스트 모두의 시간이 동기화되어야 합니다.

Horizon Console UI를 사용하여 JMP Integrated Workflow 기능에 액세스하는 경우 JMP Server가 Horizon 연결 서버에서 받은 토큰을 인증한 후 JMP Server에 토큰을 반환합니다. 두 호스트 간의 시간이 동기화되지 않으면 Horizon 연결 서버가 JMP Server에서 제공된 토큰을 거부하고 Horizon Console UI에서 JMP Integrated Workflow 기능을 사용할 수 없게 됩니다. [JMP 설정] 창에 다음과 같은 오류 메시지가 표시됩니다.

Horizon SSO 토큰을 확인할 수 없습니다.

인증 프로세스를 성공적으로 완료하려면 Horizon 연결 서버와 JMP Server 호스트의 시간을 공통 NTP(네트워크 시간 프로토콜) 서버와 동기화하십시오.

절차

- 1 Windows 호스트에서 다음 VMware Tool 명령을 사용합니다.

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

- 2 ESXi 호스트에서 ESXi 클럭을 네트워크 시간 서버와 동기화합니다.
 - a VMware Host Client를 시작하고 ESXi 호스트에 연결합니다.
 - b **구성**을 클릭합니다.
 - c **시스템**에서 **시간 구성**을 클릭하고 **편집**을 클릭합니다.

- d **네트워크 시간 프로토콜 사용(NTP 클라이언트 사용)**을 선택합니다.
- e [NTP 서버 추가] 텍스트 상자에 동기화할 하나 이상의 NTP 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)을 입력합니다.

다음에 수행할 작업

JMP Server에 대한 TLS 인증서를 구성합니다. [JMP Server용 TLS 인증서 설정 작업 개요](#)의 내용을 참조하십시오.

JMP Server에 대한 TLS 인증서 및 암호 그룹 구성

JMP Server 인스턴스가 네트워크에 있는 다른 서버와 안전하게 통신하도록 하려면 유효한 인증 기관(CA)에서 서명한 TLS 인증서를 사용하도록 JMP Server 인스턴스를 구성해야 합니다. 필요에 따라 보안 연결을 개선하기 위해 JMP Server 인스턴스와 통신할 때 다른 서버에서 승인하고 제안하는 기본 암호 그룹을 변경할 수도 있습니다.

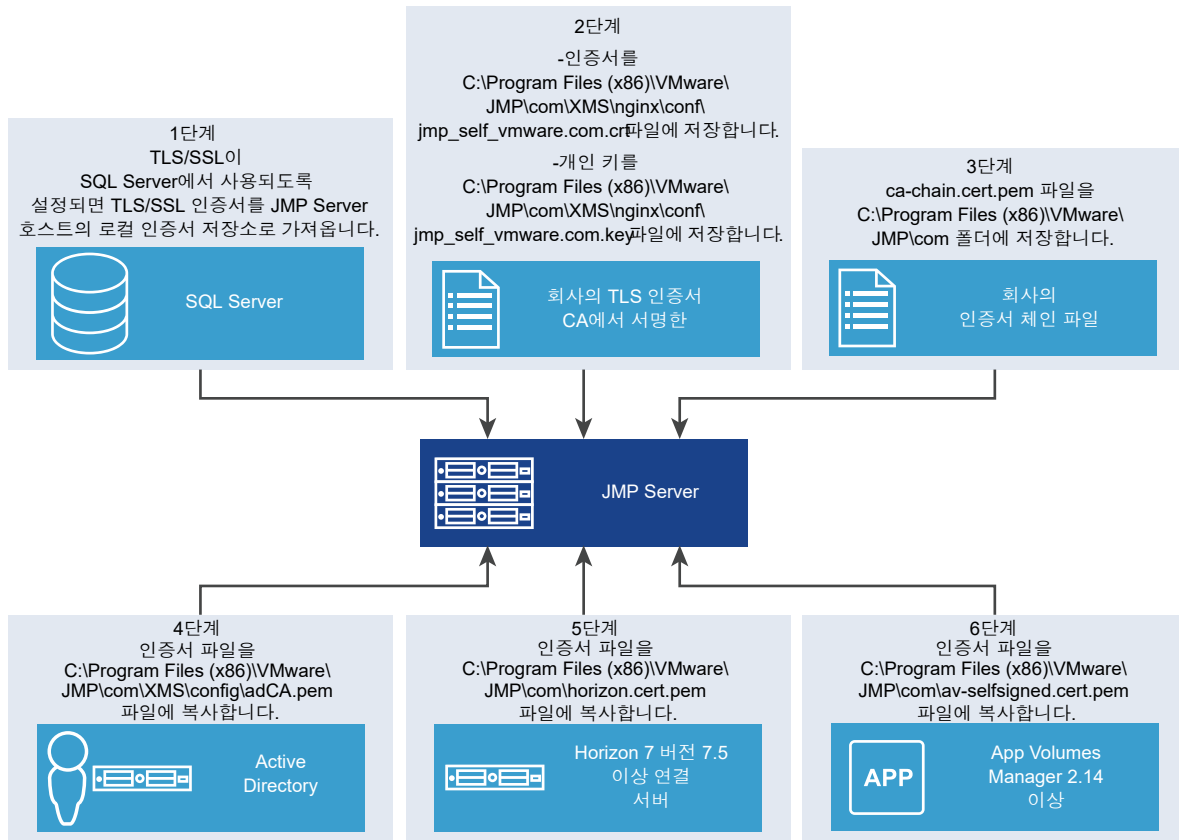
기본적으로 JMP Server 설치 관리자는 사용자가 설치한 JMP Server 인스턴스에 대해 자체 서명된 TLS 서버 인증서를 설치합니다. 테스트 용도로 기본 인증서를 사용할 수 있습니다. 운영 환경에서 JMP Server 인스턴스를 사용하는 경우 가능한 한 빨리 기본 인증서를 CA 서명 TLS 서버 인증서로 교체해야 합니다. 신뢰할 수 없는 사용자가 CA에서 서명하지 않은 인증서를 사용하여 서버로 가장하여 트래픽을 인터셉트할 수 있습니다. [JMP Server용 TLS 인증서 설정 작업 개요](#)의 내용을 참조하십시오.

JMP Server용 TLS 인증서 설정 작업 개요

JMP Server를 성공적으로 설치한 후 JMP Server 인스턴스에 사용하도록 유효한 인증 기관(CA)에서 서명한 TLS 서버 인증서를 설정하려면 몇 가지 작업을 수행해야 합니다.

이 항목에 설명된 작업 외에도 다음 다이어그램에서 JMP Server에 대한 인증서를 구성하는 데 필요한 기본 단계를 시각적으로 요약해서 보여 줍니다. 특정 인증서를 성공적으로 구성하려면 이 개요 다음에 나오는 항목에 설명되어 있는 자세한 단계를 수행해야 합니다. 선택 사항으로 표시된 작업의 경우 더 안전한 JMP Server 구성을 위해 해당 작업을 수행해야 하는지 여부를 결정하십시오. 인증서 구성을 완료한 후에 Windows 서비스 관리자를 사용하여 3가지 JMP Server 서비스를 다시 시작해야 합니다.

그림 6-1. JMP Server에 대한 인증서를 구성하는 기본 단계



- 1 SQL Server에서 TLS/SSL이 사용되도록 설정되어 있으면 TLS/SSL 인증서를 JMP Server 호스트의 로컬 인증서 저장소로 가져왔는지 확인합니다.
- 2 JMP Server 설치 관리자가 생성한 TLS 서버 인증서를 교체합니다.
JMP Server 설치 관리자가 생성한 기본 서버 인증서는 조직의 네트워크에서 인식되지 않는 자체 서명된 인증서입니다. 자체 서명된 인증서를 CA에서 가져온 유효한 TLS 인증서로 교체합니다. [기본 TLS 인증서 교체](#)의 내용을 참조하십시오.
조직에 유효한 TLS 웹 서버 인증서가 없으면 CA에서 서명된 TLS 서버 인증서를 가져옵니다. "Horizon 7용 TLS 인증서 설정 시나리오"의 정보를 참조하십시오.
- 3 중간 CA에서 조직의 서버 인증서에 서명한 경우 JMP Server에서 네트워크에 있는 다른 서버를 인증하는 데 도움을 주기 위해 조직의 인증서 체인 파일 ca-chain.cert.pem을 사용하도록 JMP Server를 구성합니다. [인증서 체인 파일을 사용하도록 JMP Server 구성](#)의 내용을 참조하십시오.

참고 NodeJS에서 신뢰하는 루트 CA가 조직의 TLS 서버 인증서에 직접 서명한 경우 인증서 체인 파일 또는 루트 인증서 파일 ca.cert.pem을 제공할 필요가 없습니다.

- 4 Active Directory 서버용 인증서에 서명하여 adCA.pem 파일에 저장하고 이 파일을 JMP Server XMS 구성 폴더에 추가하는 데 사용되는 CA 인증서를 가져옵니다. 자세한 내용은 [Active Directory에 대한 인증서를 사용하도록 JMP Server 구성](#)의 내용을 참조하십시오.

- Horizon 연결 서버를 위한 CA에서 서명된 인증서를 `horizon.cert.pem` 파일로 내보내고 이 파일을 JMP Server 홈 폴더에 추가합니다. 자세한 내용은 [Horizon 연결 서버 인증서를 사용하도록 JMP Server 구성](#)의 내용을 참조하십시오.

JMP Server는 `horizon.cert.pem` 파일을 사용하여 연결 서버를 연결 가능한 신뢰할 수 있는 서버로 인증할 수 있습니다.

참고 JMP Server 인스턴스와 상호 작용하는 각 연결 서버 포트에 대해 이 작업을 완료해야 합니다. 내보낸 각 CA에서 서명된 인증서의 콘텐츠가 동일한 `horizon.cert.pem` 파일에 추가되어야 합니다.

- JMP 할당을 생성할 때 App Volumes AppStack을 할당할 경우 App Volumes Manager 인스턴스와 안전하게 통신할 수 있게 App Volumes Manager 인스턴스의 자체 서명된 인증서를 사용하도록 JMP Server 인스턴스를 구성하십시오. [App Volumes Manager의 인증서를 사용하도록 JMP Server 구성](#)의 내용을 참조하십시오.
- (선택 사항) JMP Server 인스턴스가 지원하는 기본 암호 그룹을 조직에서 지원하는 암호로 변경합니다. [JMP Server에 대한 암호 그룹 구성](#)의 내용을 참조하십시오.
- (선택 사항) Horizon 7 연결 서버 인스턴스와 더 안전하게 통신할 수 있도록 JMP Server에서 더 제한적인 원본 간 리소스 공유(CORS) 정책을 사용하십시오. [JMP Server에 대해 더 제한적인 CORS 정책 사용](#)의 내용을 참조하십시오.
- Windows 서비스 관리자를 사용하여 세 개의 JMP Server 서비스를 다시 시작합니다.

서버 인증서를 구성한 후 Horizon Console로 이동하여 JMP 설정을 구성하고 JMP Integrated Workflow 기능을 사용할 수 있습니다. "VMware Horizon Console 관리"에서 "처음으로 JMP 설정 구성"을 참조하십시오.

기본 TLS 인증서 교체

JMP Server 설치 관리자에서 설치된 기본 TLS 인증서를 인증 기관(CA)에서 서명된 조직의 TLS 인증서로 교체합니다.

JMP Server 인스턴스를 성공적으로 설치한 후 웹 브라우저에서 Horizon 콘솔을 사용하여 액세스할 수 있습니다. 그러나 네트워크에서 설치된 기본 TLS 인증서를 인식하지 못하는 경우 처음으로 JMP 설정을 구성할 때 웹 브라우저의 보안 경고 대화 상자가 나타납니다. 자체 서명된 기본 인증서를 테스트용으로 사용할 수 있지만 JMP Server 인스턴스와 안전하게 연결하려면 기본 인증서 및 키를 CA에서 서명된 TLS 인증서 및 개인 키로 교체하십시오.

중요 JMP Server 설치 관리자에서 생성된 기본 이름과 다른 인증서 및 키 파일 이름을 지정하려면 새 파일 이름을 사용하도록 JMP Server NGINX 구성 파일을 수정해야 합니다.

사전 요구 사항

- JMP Server를 설치합니다. [JMP Server 설치](#)의 내용을 참조하십시오.

- CA에서 서명된 TLS 인증서를 가져오고 JMP Server 설치 관리자에서 설치된 기본 TLS 인증서를 교체합니다. Microsoft Certreq 또는 Windows용 OpenSSL과 같은 인증서 도구를 사용하여 인증서를 생성할 수 있습니다. "Horizon 7용 TLS 인증서 설정 시나리오"에 있는 "인증 기관에서 TLS 인증서 가져오기"의 정보를 참조하십시오.

절차

- 1 JMP Server 호스트에서 Windows 서비스 관리자 도구를 사용하여 세 개의 JMP Server 서비스를 중지합니다.
 - a Windows **시작** 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **실행**을 선택합니다.
 - b [실행] 대화 상자에서 **열기** 텍스트 상자에 services.msc를 입력하고 **확인**을 클릭합니다.
 - c [서비스] 창의 [서비스(로컬)] 창에서 다음 세 개의 JMP Server 서비스를 찾은 다음 각 서비스에 대해 **중지**를 클릭합니다.
 - VMware JMP API Service
 - VMware JMP File Share Service
 - VMware JMP Platform Services
- 2 CA에서 서명된 TLS 서버 인증서 파일을 JMP Server 호스트의 NGINX 구성 폴더에 jmp_self_vmware.com.crt로 저장합니다.

예: C:\Program Files (x86)\VMware\JMP\com\XMSWnginx\conf\jmp_self_vmware.com.crt
- 3 CA에서 서명된 TLS 서버 인증서의 동봉된 개인 키를 jmp_self_vmware.com.key로 저장합니다.

예: C:\Program Files (x86)\VMware\JMP\com\XMSWnginx\conf\jmp_self_vmware.com.key
- 4 (선택 사항) 예상 인증서 파일 이름 jmp_self_vmware.com.crt 또는 jmp_self_vmware.com.key와 다른 파일 이름을 사용하려면 새 파일 이름으로 NGINX 구성 파일을 수정해야 합니다.
 - a C:\Program Files (x86)\VMware\JMP\com\XMSWnginx\conf\nginx.conf 구성 파일을 엽니다.
 - b jmp_self_vmware.com.crt 및 jmp_self_vmware.com.key 속성을 모두 찾아서 선택한 새 파일 이름으로 바꿉니다.
 - c nginx.conf 파일을 저장합니다.

이제 웹 브라우저 보안 경고 대화 상자가 표시되지 않고 JMP Integrated Workflow 기능에 안전하게 액세스할 수 있습니다.

다음에 수행할 작업

중간 CA에서 조직의 전체 인증서 체인에 서명한 경우 인증서 체인 파일을 사용하도록 JMP Server 인스턴스를 구성합니다. [인증서 체인 파일을 사용하도록 JMP Server 구성](#)의 내용을 참조하십시오. 그렇지 않으면 Active Directory에 대한 인증서를 사용하도록 JMP Server 인스턴스 구성을 진행합니다. [Active Directory에 대한 인증서를 사용하도록 JMP Server 구성](#)의 내용을 참조하십시오.

인증서 체인 파일을 사용하도록 JMP Server 구성

중간 CA(인증 기관)에서 조직 서버의 인증서에 서명한 경우 루트 및 중간 인증서를 포함하는 조직의 전체 인증서 체인으로 JMP Server 인스턴스를 구성하십시오.

사전 요구 사항

- Windows 서비스 관리자를 사용하여 세 개의 JMP Server 서비스를 중지합니다.

절차

- 1 이름이 `ca-chain.cert.pem`인 파일을 생성합니다. 메모장++와 같은 텍스트 편집기에서 파일을 엽니다.
- 2 동일한 텍스트 편집기에서 조직의 루트 인증서를 엽니다. 루트 인증서의 콘텐츠를 `ca-chain.cert.pem`으로 복사합니다.

중간 인증서 파일(있는 경우)에 대해 이 단계를 반복합니다. 각 중간 인증서의 콘텐츠를 `ca-chain.cert.pem`의 끝에 추가합니다.
- 3 `ca-chain.cert.pem`을 저장한 후 닫습니다.

이제 조직의 루트 및 중간 인증서가 포함된 인증서 체인 파일이 준비되었습니다.
- 4 `ca-chain.cert.pem` 인증서 체인 파일을 `C:\Program Files (x86)\VMware\JMPWcom` 폴더로 복사합니다.

인증서 체인이 배치되면 JMP Server 인스턴스가 Horizon 7 및 App Volumes 인스턴스를 인증하고 이러한 인스턴스와 안전하게 통신할 수 있습니다.

다음에 수행할 작업

데스크톱 관리자가 JMP Integrated Workflow 기능을 사용할 때 JMP Server 인스턴스가 Active Directory 서버를 인증할 수 있도록 Active Directory 인증서로 JMP Server 인스턴스를 구성합니다. [Active Directory에 대한 인증서를 사용하도록 JMP Server 구성](#)의 내용을 참조하십시오.

Active Directory에 대한 인증서를 사용하도록 JMP Server 구성

JMP Server에서 Horizon Console이 연결된 Active Directory의 유효성을 검사하려면 해당 Active Directory 서버에 대한 인증서를 사용하도록 JMP Server를 구성해야 합니다.

Active Directory 도메인의 루트 CA 인증서를 `adCA.pem` 파일이라는 인증서 파일로 내보내고 이 파일을 JMP Server XMS 구성 폴더에 배치해야 합니다.

사전 요구 사항

- JMP Server가 설치되어야 합니다.
- Active Directory가 LDAPS(SSL을 통한 LDAP) 또는 StartTLS(TLS를 통한 LDAP)를 대상으로 구성되어야 합니다.

- Active Directory 도메인의 루트 CA 인증서. 인증서가 PEM(Base64 인코딩) 형식이 아닌 경우 OpenSSL 문서(또는 유사한 문서)를 참조하여 파일을 PEM 형식으로 변환하십시오.

참고 다른 도메인의 여러 루트 인증서가 있는 경우 각 파일의 내용을 하나씩 단일 .pem 파일로 복사하여 모든 PEM 형식 인증서를 단일 파일에 결합할 수 있습니다.

절차

- 1 PEM 형식의 인증서 파일 이름은 adCA.pem입니다.
- 2 adCA.pem 파일을 JMP Server XMS 구성 폴더에 복사합니다.

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

JMP Server 인스턴스에 대한 Active Directory 인증서가 구성되면 Active Directory가 신뢰할 수 있는 서버로 인식되므로 Horizon Console 사용자가 JMP Integrated Workflow 기능을 사용할 수 있습니다.

다음에 수행할 작업

데스크톱 관리자가 JMP Integrated Workflow 기능을 사용할 때 JMP Server 인스턴스가 연결 서버를 인증할 수 있도록 연결 서버 인증서로 JMP Server를 구성합니다. [Horizon 연결 서버 인증서를 사용하도록 JMP Server 구성](#)의 내용을 참조하십시오.

Horizon 연결 서버 인증서를 사용하도록 JMP Server 구성

JMP Server에서 Horizon Console이 연결된 Horizon 7 연결 서버의 유효성을 검사하려면 Horizon 7 연결 서버 인증서를 사용하도록 JMP Server를 구성해야 합니다.

Horizon 7 연결 서버 인증서를 horizon.cert.pem 파일이라는 인증서 파일로 내보내고 이 파일을 JMP Server 홈 폴더에 배치해야 합니다.

중요 내보낸 각 CA에서 서명된 인증서의 내용이 동일한 horizon.cert.pem 파일에 추가되어야 합니다.

CA에서 서명되거나 자체 서명된 Horizon 7 연결 서버 인증서를 추가할 때 이러한 동일한 절차를 사용하십시오.

사전 요구 사항

- JMP Server가 설치되어야 합니다.
- Horizon 7 연결 서버에 대한 관리 액세스 권한이 있어야 합니다.

절차

- 1 설치한 Horizon Console 및 JMP Server와 상호 작용하는 Horizon 7 연결 서버용 Windows Server 호스트에 로그인합니다.
- 2 Windows **시작** 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **실행**을 선택한 후 mmc.exe를 입력합니다.

MMC 유틸리티 창이 나타납니다.

3 인증서 스냅인을 추가합니다.

- a **콘솔 루트** 창에서 **파일 > 스냅인 추가/제거**를 선택합니다.
- b **스냅인 추가 또는 제거** 창의 [사용 가능한 스냅인] 창에서 **인증서**를 선택하고 **추가**를 클릭합니다.
- c 인증서가 추가된 후 **확인**을 클릭합니다.
- d [인증서 스냅인] 창에서 **컴퓨터 계정**을 선택하고 **다음**을 클릭합니다.
- e [컴퓨터 선택] 창에서 **로컬 컴퓨터**를 선택하고 **마침**을 클릭합니다.
인증서(로컬 컴퓨터) 스냅인이 [선택한 스냅인] 창에 추가됩니다.
- f **확인**을 클릭하여 **스냅인 추가 또는 제거** 대화 상자를 닫습니다.

4 [콘솔 루트] 창으로 돌아가서 **콘솔 루트 > 인증서(로컬 컴퓨터)**를 선택하고 왼쪽 창의 **개인 > 인증서** 폴더를 선택하여 콘텐츠를 표시합니다.

5 Horizon 연결 서버 인증서를 내보냅니다.

- a [인증서 콘텐츠] 창에서 대화명이 **vdm**인 인증서를 찾습니다.
이 인증서는 Horizon 연결 서버에 속해 있습니다.
- b 인증서를 마우스 오른쪽 버튼으로 클릭하고 **모든 작업 > 내보내기**를 선택합니다.
- c [인증서 내보내기 마법사] 대화 상자에서 **다음**을 클릭합니다.
- d **아니요, 개인 키를 내보내지 않습니다.**를 선택하고 **다음**을 클릭합니다.
- e **Base-64 인코딩 X.509(.CER)** 형식을 선택하고 **다음**을 클릭합니다.
- f 파일 이름을 **horizon.cert.pem**으로 입력하고 **찾아보기**를 클릭하여 내보낸 인증서를 저장할 폴더로 이동합니다.

중요 내보낸 인증서 파일을 .cer 또는 .crt 파일 확장명이 **아닌**.pem 파일 확장명으로 저장해야 합니다. 필요한 경우 내보낸 인증서 파일을 텍스트 편집기에서 열고 horizon.cert.pem으로 저장합니다.

- g **다음**을 클릭하고 **마침**을 클릭하여 **인증서 내보내기 마법사** 창을 닫습니다.
성공적으로 인증서를 내보냈습니다.

6 내보낸 horizon.cert.pem 인증서를 저장한 위치로 이동하여 해당 인증서를 JMP Server 홈 폴더에 복사합니다.

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

JMP Server에 대한 연결 서버 인증서가 구성되면 연결 서버가 신뢰할 수 있는 서버로 인식되고 Horizon Console 사용자가 JMP Integrated Workflow 기능을 사용할 수 있습니다.

다음에 수행할 작업

[JMP Server용 TLS 인증서 설정 작업 개요](#)에 나열된 선택적 작업을 검토하고 이러한 작업도 완료해야 하는지 확인하십시오. 필요한 모든 구성 작업을 완료한 후 JMP Server 서비스를 다시 시작하고 JMP 설정을 구성하십시오. 자세한 내용은 “VMware Horizon Console 관리”에서 “처음으로 JMP 설정 구성”을 참조하십시오.

App Volumes Manager의 인증서를 사용하도록 JMP Server 구성

JMP 할당을 생성할 때 App Volumes AppStack을 할당할 경우 App Volumes Manager 인스턴스와 안전하게 통신할 수 있게 App Volumes Manager 인스턴스의 인증서를 사용하도록 JMP Server 인스턴스를 구성하십시오.

PoC 설치 환경에서 JMP Server가 App Volumes Manager 인스턴스의 자체 서명된 인증서를 사용할 수 있도록 하려면 해당 인증서를 `av-selfsigned.cert.pem` 파일이라는 인증서 파일로 내보내야 합니다. App Volumes Manager가 CA 서명 인증서를 사용하는 경우 조직의 인증서 체인 파일 `ca chain.cert.pem`을 사용하여 App Volumes Manager 인스턴스를 인증하도록 JMP Server를 구성합니다. [인증서 체인 파일을 사용하도록 JMP Server 구성](#)의 내용을 참조하십시오.

사전 요구 사항

- JMP Server가 설치되어야 합니다.
- App Volumes Manager 인스턴스 또는 이를 관리하는 로드 밸런서에 대한 관리 액세스 권한이 있어야 합니다.

절차

- 1 JMP Server 호스트에서 웹 브라우저를 사용하여 App Volumes Manager 인스턴스 또는 환경에서 App Volumes Manager 인스턴스를 관리하는 로드 밸런서에 로그인합니다.
- 2 App Volumes Manager 인스턴스 또는 로드 밸런서에서 사용되는 인증서 정보를 찾으려면 웹 브라우저의 인증서 관리자 사용하고 인증서 파일을 Base-64 인코딩된 X.509(.CER) 형식으로 `C:\Program Files (x86)\VMware\JMP\com\Wav-selfsigned.cert.pem` 파일로 내보냅니다.

중요 내보낸 인증서 파일을 `.cer` 또는 `.crt` 파일 확장명이 아닌 `.pem` 파일 확장명으로 저장해야 합니다. 필요한 경우 내보낸 인증서 파일을 텍스트 편집기에서 열고 `av-selfsigned.cert.pem`으로 저장합니다.

예를 들어, Google Chrome 웹 브라우저를 사용하는 경우 **설정 > 고급**을 클릭하고 **인증서 관리**를 선택합니다. 인증서 대화 상자에서 App Volumes Manager 인증서를 선택하고 **내보내기**를 클릭합니다. 인증서 내보내기 마법사를 사용하여 Base 64 인코딩된 X.509(.CER) 형식으로 App Volumes Manager 인증서 파일을 `C:\Program Files (x86)\VMware\JMP\com\Wav-selfsigned.cert.pem` 파일로 내보냅니다. `.pem.cer` 파일 확장명 대신 `.pem` 파일 확장명만 포함하도록 파일 이름을 변경해야 할 수 있습니다.

- 3 JMP Server의 보안을 강화하는 데 필요한 TLS 인증서를 구성하기 위해 수행해야 하는 모든 작업을 완료한 경우 JMP Server 서비스를 다시 시작합니다. 나머지 TLS 인증서 구성 작업을 검토하려면 [JMP Server용 TLS 인증서 설정 작업 개요](#)를 참조하십시오.

JMP Server에 대한 암호 그룹 구성

JMP Server 설치에는 JMP Server, Horizon Connection Server, App Volumes 및 Dynamic Environment Manager 인스턴스 사이에서 승인 및 제안되는 기본 서버 측 및 클라이언트 측 암호 그룹이 포함되어 있습니다. 필요에 따라 JMP Server에서 지원하는 이러한 기본 암호 그룹을 조직에서 지원하는 암호 그룹으로 변경할 수 있습니다.

어떤 암호 그룹을 사용할지는 JMP Server가 보안 연결 요청을 수신하는 서버로 작동하는지 또는 Horizon Connection Server, App Volumes 또는 Dynamic Environment Manager에 대한 보안 연결 요청을 시작하는 클라이언트로 작동하는지에 따라 다릅니다.

<https://www.openssl.org/docs/man1.0.2/apps/ciphers.html#CIPHER-LIST-FORMAT>에 정의된 형식을 사용하여 암호 그룹 목록을 지정해야 합니다. 다음 암호 그룹 목록은 서버 측에 사용되는 기본 암호 그룹입니다.

```
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
```

이전 암호 문자열 외에도, 사용되는 실제 암호 그룹은 nginx.conf 파일에 정의되어 있는 허용된 프로토콜 TLSv1.1 및 TLSv1.2에 의해서도 결정됩니다.

절차

- 1 JMP Server 호스트에서 Windows 서비스 관리자 도구를 사용하여 세 개의 JMP Server 서비스를 중지합니다.
 - a Windows **시작** 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **실행**을 선택합니다.
 - b [실행] 대화 상자에서 **열기** 텍스트 상자에 services.msc를 입력하고 **확인**을 클릭합니다.
 - c [서비스] 창의 [서비스(로컬)] 창에서 다음과 같은 세 개의 JMP Server 서비스를 찾은 후 각 서비스에 대해 **중지**를 클릭합니다.
 - VMware JMP API Service
 - VMware JMP File Share Service
 - VMware JMP Platform Services
- 2 암호 그룹을 포함하는 구성 파일을 수정합니다.

서버 측 암호 그룹을 수정하려면:

- a C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf 폴더로 이동합니다.
- b 수정하기 전에 nginx.conf 파일의 백업 복사본을 생성합니다.
- c 메모장에서 nginx.conf 파일을 엽니다.
- d ssl_ciphers로 시작하는 줄을 찾아서 필요에 따라 암호 그룹을 수정합니다.
- e nginx.conf 파일의 변경 내용을 저장합니다.

클라이언트 측 암호 그룹을 수정하려면:

- a C:\Program Files (x86)\VMware\JMP\com\Xmp\conf 폴더로 이동합니다.

- b 메모장에서 jmp.js 파일을 엽니다.
- c 수정하기 전에 jmp.js 파일의 백업 복사본을 생성합니다.
- d 다음 코드 조각이 포함된 줄을 찾습니다.

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

- e 코드 조각에서 ciphers: 섹션 다음에 나오는 암호 그룹을 수정합니다. 예:

```
ciphers:' "your_organization_cipher_suite" '
```

- f jmp.js 파일의 변경 내용을 저장합니다.

- 3 새 암호 그룹 목록을 적용하려면 Windows 서비스 관리자 도구를 사용하여 세 개의 JMP Server 서비스를 다시 시작합니다.

JMP Server에 대해 더 제한적인 CORS 정책 사용

JMP Server에 액세스하도록 신뢰할 수 있는 Horizon 7 연결 서버 인스턴스의 화이트리스트를 생성하여 JMP Server 인스턴스에 대해 더 제한적인 원본 간 리소스 공유(CORS) 정책을 사용할 수 있습니다.

기본적으로 Horizon 7 연결 서버가 [인증서 체인 파일을 사용하도록 JMP Server 구성](#)을 사용하여 구성된 인증서 체인 파일에 있는 동일한 인증서를 사용 중인 경우 JMP Server 인스턴스에 액세스할 수 있습니다. 승인된 Horizon 7 연결 서버 인스턴스 목록만 JMP Server에 액세스할 수 있도록 하려면 다음 단계를 수행합니다.

절차

- 1 텍스트 편집기를 사용하여 NGINX 구성 파일(C:\Program Files (x86)\VMware\JMP\com\XMS\nginx\conf\nginx.conf)을 엽니다.
- 2 다음 텍스트를 두 개 찾아서 다음과 같이 표시될 수 있도록 앞의 # 표시를 제거하여 각각의 주석을 제거합니다.

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

- 3 다음 텍스트를 두 개 찾아서 다음과 같이 표시될 수 있도록 앞에 # 표시를 추가하여 각각을 주석 처리합니다.

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

4 승인된 연결 서버 인스턴스 목록을 화이트리스트에 추가합니다.

a 파일에서 다음 콘텐츠를 찾습니다.

```
# 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://W/YOUR_CONNECTION_SERVER_DOMAINW.com)$" "$http_origin";
}
```

b default ''; 줄 뒤에 화이트리스트에 포함할 각 연결 서버 인스턴스에 대한 줄을 추가합니다.

예를 들어, JMP Server에 연결하도록 허용된 연결 서버 인스턴스의 도메인 이름이 `www.testhorizon.com` 및 `www.prodhorizon.com`인 경우 추가할 줄이 다음 예에 굵게 표시되어 있습니다.

```
default '';
    "~*^(https://W/testhorizonW.com)$" "$http_origin";~*^(https://W/prodhorizonW.com)$" "$http_origin";
```

5 nginx.conf 파일의 변경 내용을 저장합니다.

6 Windows 서비스 관리자를 사용하여 JMP Platform Services를 다시 시작합니다.

JMP Server 설치 후 데이터베이스 암호 업데이트

7

초기 JMP Server 설치 중에 사용한 SQL Server 데이터베이스 암호를 수정하는 경우 VMware JMP Server 서비스에서 사용하는 데이터베이스 암호 정보도 업데이트해야 합니다.

본 장은 다음 항목을 포함합니다.

- [VMware JMP 플랫폼 서비스에 대한 데이터베이스 암호 업데이트](#)
- [VMware JMP 파일 공유 서비스에 대한 데이터베이스 암호 업데이트](#)

VMware JMP 플랫폼 서비스에 대한 데이터베이스 암호 업데이트

JMP Server를 설치할 때 사용한 SQL Server 데이터베이스 암호를 수정하는 경우 VMware JMP 플랫폼 서비스에서 SQL Server 데이터베이스에 연결하기 위해 사용하는 데이터베이스 암호도 업데이트해야 합니다.

사전 요구 사항

JMP Server 호스트에서 데이터베이스 정보를 변경하기 위한 올바른 관리자 권한이 있는지 확인합니다.

절차

- 1 JMP Server 호스트에서 Windows 서비스 관리자 도구를 사용하여 VMware JMP Platform Services 프로세스를 중지합니다.
 - a Windows **시작** 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **실행**을 선택합니다.
 - b [실행] 대화 상자에서 **열기** 텍스트 상자에 services.msc를 입력하고 **확인**을 클릭합니다.
 - c [서비스] 창의 [서비스(로컬)] 창에서 VMware JMP Platform Services를 찾은 후 **중지**를 클릭합니다.
- 2 다음 실행 파일 중에서 JMP Server 호스트에 적합한 파일을 두 번 클릭하여 **ODBC 데이터 소스 관리자** 창을 엽니다.
 - C:\Windows\SysWow64\odbcad64.exe
 - C:\Windows\system32\odbcad32.exe

3 [ODBC 데이터 소스 관리자] 창에서 **시스템 DSN**을 클릭하고 [사용자 데이터 소스] 창에서 **svmanager**를 선택합니다.

4 **구성**을 클릭합니다.

Microsoft SQL Server DSN 구성 마법사가 나타납니다.

5 **다음**을 클릭합니다.

경고 데이터 소스 이름 또는 서버 텍스트 상자에 있는 기존 정보는 변경하지 마십시오.

6 사용자가 입력한 로그인 ID 및 암호를 사용하여 **SQL Server 인증**을 선택했는지 확인합니다.

7 **암호** 텍스트 상자에 새 암호를 입력하고 **다음**을 클릭합니다.

8 기본 데이터베이스 정보 페이지의 기존 정보는 변경하지 않고 **다음**을 다시 클릭합니다.

9 **마침**을 클릭합니다.

[ODBC Microsoft SQL Server 설정 요약] 창에 구성 세부 정보와 함께 표시됩니다.

10 요약 정보를 검토하고 **확인**을 클릭하여 VMware JMP Platform Services 서비스에 대한 암호 수정을 계속 진행합니다.

11 VMware JMP Platform Services 서비스를 다시 시작하기 전에 VMware JMP 플랫폼 서비스 데이터베이스 구성 파일에 새 암호 정보를 추가합니다.

a 관리자 권한으로 텍스트 편집기를 사용하여 C:\Program Files (x86)\VMware\JMP\com\XMS\Wconfig\database.yml에 있는 데이터베이스 구성 파일을 엽니다.

b username 속성에 대한 줄을 찾은 후 이 줄 다음에 password 속성에 대한 새 줄을 삽입합니다.

c 다음 예와 같이 나타나도록 생성한 암호에 대한 정보를 입력합니다.

```
password: new_password
```

중요 이 암호 정보는 VMware JMP Platform Services 서비스를 다시 시작한 후에 database.yml 파일에서 자동으로 제거됩니다.

12 VMware JMP Platform Services 서비스를 다시 시작합니다.

a Windows **시작** 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **실행**을 선택합니다.

b [실행] 대화 상자에서 **열기** 텍스트 상자에 services.msc를 입력하고 **확인**을 클릭합니다.

c [서비스] 창의 [서비스(로컬)] 창에서 VMware JMP Platform Services를 찾은 후 **시작**을 클릭합니다.

다음에 수행할 작업

VMware JMP 파일 공유 서비스에서 사용되는 데이터베이스 로그인 계정 정보를 아직 업데이트하지 않은 경우 업데이트해야 합니다. [VMware JMP 파일 공유 서비스에 대한 데이터베이스 암호 업데이트](#)의 내용을 참조하십시오.

VMware JMP 파일 공유 서비스에 대한 데이터베이스 암호 업데이트

JMP Server를 설치할 때 사용한 SQL Server 데이터베이스 암호를 수정하는 경우 VMware JMP 파일 공유 서비스에서 SQL Server 데이터베이스에 연결하기 위해 사용하는 데이터베이스 암호도 업데이트해야 합니다.

사전 요구 사항

JMP Server 호스트에서 데이터베이스 정보를 변경하기 위한 올바른 관리자 권한이 있는지 확인합니다.

절차

- 1 JMP Server 호스트에서 Windows 서비스 관리자 도구를 사용하여 VMware JMP File Share Service 프로세스를 중지합니다.
 - a Windows **시작** 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **실행**을 선택합니다.
 - b [실행] 대화 상자에서 **열기** 텍스트 상자에 services.msc를 입력하고 **확인**을 클릭합니다.
 - c [서비스] 창의 [서비스(로컬)] 창에서 VMware JMP File Share Service를 찾은 후 **중지**를 클릭합니다.
- 2 VMware JMP 파일 공유 서비스에서 사용되는 암호를 업데이트합니다. 다음 정보를 사용하여 JMP Server 설치 중에 사용되는 SQL Server 연결 유형에 따라 사용할 단계를 결정합니다.
 - SQL 인증 연결 모드:
 - 1 C:/Program Files (x86)/VMware/JMP/com/uem 폴더로 이동한 다음, 텍스트 편집기에서 db.json 파일을 엽니다.
 - 2 새 password 매개 변수를 추가하고 JMP Server 설치 후에 생성한 새 SQL Server 데이터베이스 암호로 설정합니다. 다음은 예입니다.

```
"jmp.production": {
  "server": "MyOrg-DB_server\\SQL2014",
  "database": "MyOrg-database",
  "userName": "sa",
  "password": "new_SQL_password",
  "stamp": "nnXXpIIgeImfPJWbu0YAQA==.EDIk3lCqSubg6Y2uIwSSgw=="
}
```

- 3 파일을 저장하고 텍스트 편집기를 종료합니다.

- Windows 인증 연결 모드:
 - 1 C:/Program Files (x86)/VMware/JMP/com/uem 폴더로 이동한 다음, 텍스트 편집기에서 db.json 파일을 엽니다.

- 2 기존 파일 콘텐츠를 다음 콘텐츠로 바꿉니다. 여기서 <IP address>는 SQL Server 호스트의 IP 주소이고 <Database name>은 유효한 데이터베이스 이름입니다.

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

- 3 파일을 저장하고 텍스트 편집기를 종료합니다.

3 VMware JMP File Share Service를 다시 시작합니다.

- a Windows **시작** 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **실행**을 선택합니다.
- b [실행] 대화 상자에서 **열기** 텍스트 상자에 services.msc를 입력하고 **확인**을 클릭합니다.
- c [서비스] 창의 [서비스(로컬)] 창에서 VMware JMP File Share Service를 찾은 후 **시작**을 클릭합니다.

다음에 수행할 작업

VMware JMP 플랫폼 서비스에서 사용되는 데이터베이스 로그인 계정 정보를 아직 업데이트하지 않은 경우 업데이트해야 합니다. [VMware JMP 플랫폼 서비스에 대한 데이터베이스 암호 업데이트](#)의 내용을 참조하십시오.

JMP Server 문제 해결

8

JMP Server 인스턴스를 설치, 구성 및 등록할 때 오류 메시지가 발생할 수 있습니다. 이 장의 문제 해결 정보를 사용할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- [JMP Server를 사용할 수 없음 오류](#)
- [서비스 계정 암호가 업데이트된 후 오류가 발생함](#)
- [JMP Server 제거](#)

JMP Server를 사용할 수 없음 오류

JMP Server 인스턴스에 연결할 수 없습니다.

문제

Horizon Console을 사용하여 JMP Server 인스턴스를 등록하는 경우 입력한 JMP Server를 사용할 수 없습니다. 입력 항목을 수정하거나 나중에 다시 시도하십시오. 오류 메시지가 표시될 수 있습니다.

원인

여러 가능한 이유 중 하나로 인해 이 오류 메시지가 나타납니다. 원인 및 해결 방법을 확인하려면 다음 섹션의 정보를 사용하십시오.

해결책

- 1 인증서가 올바르게 구성되어 있는지 확인합니다.

[JMP Server에 대한 TLS 인증서 및 암호 그룹 구성](#)의 정보를 사용합니다.

- 2 JMP Server URL 등록을 시도한 후에 웹 브라우저에서 HTTP 응답을 검토합니다.

다음 출력과 비슷한 HTTP 응답을 수신하는 경우

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

다음 단계에 따라 Horizon Console에 로그인하는 데 사용한 사용자 계정에 충분한 관리자 권한이 있는지 확인합니다.

- a Horizon Administrator에서 **View 구성 > 관리자**를 선택합니다.
 - b 관리자 창에서 관리자 사용자 계정이 "<domain-name>\Administrator(BUILTIN\Administrator 아님)"로 표시되는지, 모든 관리자 권한이 할당되었는지 확인합니다.
 - c BUILTIN\Administrator가 표시되면 [VMware Horizon 7 버전 7.5 릴리스 정보](#)에 설명된 해결 방법을 적용하십시오.
- 관리자 사용 권한을 관리하는 방법에 대한 내용은 "Horizon 7 관리" 문서에서 "사용 권한 관리 및 검토"를 참조하십시오.

- 3 웹 브라우저의 HTTP 응답에 오류 메시지 {"code":403,"error":"Error: Unable to verify Horizon JWT","error_code":"1044","error_type":"horizonJwtVerificationError"}와 유사한 JWT(JSON 웹 토큰) 메시지가 표시되면 JMP Server 호스트와 Horizon Connection Server 호스트 간의 시간이 동기화되어 있는지 확인합니다.

[Horizon 연결 서버와 JMP Server 호스트 사이의 시간 동기화](#)에 제공된 정보를 사용합니다.

서비스 계정 암호가 업데이트된 후 오류가 발생함

JMP Server 초기 구성 동안 사용되는 서비스 계정 사용자 암호를 변경한 후 JMP Server 인스턴스를 사용하여 작업을 수행하려고 하면 오류 메시지가 표시됩니다.

새 암호 정보를 JMP Server 데이터베이스에도 업데이트해야 합니다. Ruby on Rails 콘솔을 사용하여 JMP Server의 SQL Server 데이터베이스에 저장된 암호를 업데이트합니다.

경고 Ruby on Rails 콘솔을 사용하여 값을 수정하면 작업 환경에 심각한 영향을 미칠 수 있습니다. Ruby on Rails 콘솔에 익숙하지 않은 경우 운영 환경에서 변경 내용을 적용하기 전에 테스트 환경에서 명령을 실행해봅니다.

문제

JMP Server 인스턴스에서 JMP 통합 워크플로 작업을 수행하려고 하면 다음 오류 중 하나가 나타날 수 있습니다.

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

원인

JMP Server 인스턴스의 초기 구성 동안 사용된 서비스 계정 암호를 업데이트하는 경우, JMP Server에서 여전히 이전 암호를 사용하기 때문에 위에 나열된 오류 중 하나가 표시될 수 있습니다. 오류 1은 Horizon 7 서비스 계정 암호가 변경된 경우에 발생할 수 있습니다. 오류 2는 App Volumes Manager 서비스 계정 암호가 변경되었거나 서비스가 다운된 경우에 발생할 수 있습니다. 오류 3은 AD(Active Directory) 암호가 변경된 경우에 발생할 수 있습니다.

해결책

- 1 JMP Server 호스트 시스템의 Windows 명령 프롬프트에서 JMP Server XMS 구성 폴더로 이동한 후 Ruby on Rails 콘솔을 시작합니다.

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

- 2 SQL Server 데이터베이스에서 암호 항목을 업데이트하려면 다음 Ruby on Rails 콘솔 명령을 사용합니다.

표 8-1. SQL Server 데이터베이스에서 암호를 업데이트하기 위한 명령

조치	Ruby on Rails 콘솔 명령
Horizon 7 암호를 업데이트합니다.	<pre>a=Xms::Service.find_by_service_type("horizon") a.password=<new_Horizon7_password> a.save</pre>
App Volumes Manager 암호를 업데이트합니다.	<pre>a=Xms::Service.find_by_service_type("avmgr") a.password=<new_AVM_password> a.save</pre>
Active Directory 암호를 업데이트합니다.	<pre>a=Xms::IdentityService.find_by(netbios_name:<netbios-name>) a.password=<new_AD_password> a.save</pre>

- 3 Dynamic Environment Manager 인스턴스에 대한 암호를 업데이트하려면 Horizon Console의 **UEM** 탭에서 있는 **UEM 파일 공유 편집** 대화상자를 사용합니다.

“VMware Horizon Console 관리” 문서의 “User Environment Manager 구성 파일 공유 정보 편집”을 참조하십시오.

참고 AD 암호도 업데이트된 경우 Dynamic Environment Manager에 대한 암호를 업데이트하기 전에 JMP Server SQL Server 데이터베이스에서 AD 암호 항목을 업데이트해야 합니다.

JMP Server 제거

문제를 해결하려면 JMP Server를 제거한 후 다시 설치해야 할 수 있습니다.

이 절차는 다른 방법으로 해결할 수 없는 문제가 발생하는 경우 JMP Server를 제거하는 방법에 대해 설명합니다.

사전 요구 사항

- JMP Server를 제거할 수 있는 올바른 관리 권한이 있는지 확인합니다.
- JMP Server를 제거하기 전에 해당 JMP Server와 연결된 모든 Dynamic Environment Manager 구성 공유를 삭제합니다. “VMware Horizon Console 관리”에서 “User Environment Manager 구성 공유 정보 삭제”를 참조하십시오.

절차

- 1 Microsoft Windows 프로그램 및 기능 콘솔을 엽니다.
예를 들어, **시작 >설정 >시스템 >앱 및 기능**을 클릭합니다.
- 2 설치된 애플리케이션 목록에서 **VMware JMP**를 선택합니다.
- 3 제거 단계를 완료하려면 **제거**를 클릭하고 마법사에 따릅니다.

다음에 수행할 작업

JMP Server를 다시 설치합니다. 자세한 내용은 [JMP Server 설치](#) 문서를 참조하십시오.