

VMware vRealize Orchestrator 설치 및 구성

vRealize Orchestrator 7.2

이 문서는 새 버전으로 교체되기 전까지 나열된 각 제품 버전 및 모든 이후 버전을 지원합니다. 이 문서에 대한 최신 버전을 확인하려면 <http://www.vmware.com/kr/support/pubs>를 참조하십시오.

KO-002396-01

vmware[®]

VMware 웹 사이트 (<http://www.vmware.com/kr/support/>) 에서 최신 기술 문서를 확인할 수 있습니다.
또한 VMware 웹 사이트에서 최신 제품 업데이트를 제공합니다.
이 문서에 대한 의견이 있으면 docfeedback@vmware.com으로 사용자 의견을 보내주십시오.

Copyright © 2008–2017 VMware, Inc. 판권 소유. [저작권 및 상표 정보](#).

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

목차

VMware vRealize Orchestrator 설치 및 구성	7
업데이트된 정보	9
1 VMware vRealize Orchestrator 소개	11
Orchestrator 플랫폼의 주요 기능	11
Orchestrator 사용자 유형과 관련 책임	13
Orchestrator 아키텍처	13
Orchestrator 플러그인	14
2 Orchestrator 시스템 요구 사항	15
Orchestrator Appliance에 대한 하드웨어 요구 사항	15
지원되는 디렉토리 서비스	15
Orchestrator에서 지원하는 브라우저	16
Orchestrator 데이터베이스 요구 사항	16
Orchestrator Appliance에 포함된 소프트웨어	16
암호 요구 사항	16
국제화 지원 레벨	17
3 Orchestrator 구성 요소 설정	19
vCenter Server 설정	19
인증 방법	19
Orchestrator 데이터베이스 설정	20
4 Orchestrator 설치 및 업그레이드	21
Orchestrator Appliance 다운로드 및 배포	21
Orchestrator Appliance 전원 켜기 및 홈 페이지 열기	22
루트 암호 변경	23
vRealize Orchestrator 장치에서 SSH 관리자 로그인 사용 또는 사용 안 함	23
Orchestrator Appliance의 네트워크 설정 구성	24
Orchestrator Appliance 5.5.x 이상을 7.x로 업그레이드	24
기본 VMware 저장소를 사용하여 Orchestrator Appliance 업그레이드	24
ISO 이미지를 사용하여 Orchestrator Appliance 업그레이드	25
지정된 저장소를 사용하여 Orchestrator Appliance 업그레이드	26
Orchestrator 클러스터 5.5.x 이상을 7.x로 업그레이드	27
Orchestrator 클러스터 7.0에서 7.x로 업그레이드	28
5 Orchestrator Appliance 에 vRealize Orchestrator 구성	29
제어 센터 로그인	30
Orchestrator 네트워크 포트	30

- 인증 유형 선택 31
 - LDAP 설정 구성 32
 - vRealize Automation 인증 구성 35
 - vCenter Single Sign-On 설정 구성 36
- Orchestrator 데이터베이스 연결 구성 38
 - 데이터베이스 SSL 인증서 가져오기 38
 - 데이터베이스 연결 구성 39
 - Orchestrator 데이터베이스 내보내기 41
 - Orchestrator 데이터베이스 가져오기 41
- 인증서 관리 41
 - Orchestrator 인증서 관리 41
- Orchestrator 플러그인 구성 43
 - Orchestrator 플러그인 관리 43
 - 플러그인 제거 44
- Orchestrator 시작 옵션 45
- Orchestrator 가용성 및 확장성 45
 - Orchestrator 클러스터 구성 46
 - Orchestrator 클러스터 모니터링 및 동기화 48
 - 로드 밸런서 구성 48
- 고객 경험 향상 프로그램 구성 49
 - VMware에 수신되는 정보의 범주 49
 - 고객 경험 향상 프로그램(CEIP) 참여 49

6 API 서비스 사용 51

- REST API를 사용하여 SSL 인증서 및 키 저장소 관리 51
 - REST API를 사용하여 SSL 인증서 삭제 51
 - REST API를 사용하여 SSL 인증서 가져오기 52
 - REST API를 사용하여 키 저장소 생성 53
 - REST API를 사용하여 키 저장소 삭제 53
 - REST API를 사용하여 키 추가 53
- 제어 센터 REST API를 사용하여 Orchestrator 구성 자동화 54

7 추가 구성 옵션 55

- 제어 센터에서 새 사용자 만들기 55
- Orchestrator 구성 내보내기 55
- Orchestrator 구성 가져오기 56
- Orchestrator 구성 마이그레이션 57
 - Orchestrator 구성을 Windows에서 가상 장치로 마이그레이션 57
 - Windows용 vRealize Orchestrator 6.x 인스턴스의 클러스터를 vRealize Orchestrator 7.1 또는 7.2 가상 장치의 클러스터로 마이그레이션 58
- 워크플로 실행 속성 구성 60
- Orchestrator 로그 파일 60
 - 로그 지속성 61
 - Orchestrator 로그 구성 62
 - 워크플로 로그 검사 62
 - Orchestrator 로그 필터링 63

- 8 외부 Orchestrator 서버에서 vRealize Automation 7.2로 마이그레이션 65**
 - 마이그레이션 시나리오 66
 - Windows용 외부 vRealize Orchestrator 6.x를 vRealize Automation 7.2로 마이그레이션 66
 - 외부 vRealize Orchestrator 6.x 가상 장치를 vRealize Automation 7.2로 마이그레이션 68
 - 외부 vRealize Orchestrator 7.x를 vRealize Automation 7.2로 마이그레이션 70

- 9 내장된 vRealize Orchestrator 서버 구성 73**

- 10 구성 사용 사례 및 문제 해결 75**
 - Orchestrator를 vCenter Server 확장으로 등록 75
 - Orchestrator 인증 등록 취소 76
 - SSL 인증서 변경 76
 - 로컬 저장소에 인증서 추가 76
 - Orchestrator Appliance 관리 사이트의 인증서 변경 77
 - 실행 중인 워크플로 취소 77
 - Orchestrator 서버 디버깅 사용 78
 - Orchestrator 구성 및 요소 백업 78
 - vRealize Orchestrator 백업 및 복원 80
 - vRealize Orchestrator 백업 80
 - vRealize Orchestrator 인스턴스 복원 81
 - Site Recovery Manager 를 사용한 Orchestrator의 재해 복구 82
 - vSphere Replication 에 대한 가상 시스템 구성 82
 - 보호 그룹 만들기 83
 - 복구 계획 만들기 83
 - 폴더의 복구 계획 구성 84
 - 복구 계획 편집 84

- 11 시스템 속성 설정 87**
 - Orchestrator 클라이언트에 대한 비관리자의 액세스 사용 안 함 87
 - 워크플로 및 작업에 대한 서버 파일 시스템 액세스 설정 88
 - Orchestrator 시스템에 쓰기 액세스 권한을 허용하는 js-io-rights.comf 파일의 규칙 88
 - 워크플로 및 작업에 대한 서버 파일 시스템 액세스 설정 88
 - 워크플로 및 작업에 대한 운영 체제 명령의 액세스 설정 89
 - Java 클래스에 JavaScript 액세스 설정 90
 - 사용자 지정 시간 초과 속성 설정 90

- 12 이후 작업 정보 93**
 - Orchestrator Appliance 웹 콘솔에서 Orchestrator 클라이언트에 로그인 93

- 색인 95

VMware vRealize Orchestrator 설치 및 구성

설치 및 구성 VMware vRealize Orchestrator은 VMware® vRealize Orchestrator의 설치, 업그레이드 및 구성에 대한 정보와 지침을 제공합니다.

대상 사용자

이 정보는 가상 시스템 기술과 데이터 센터 작업에 익숙한 고급 vSphere 관리자 및 숙련된 시스템 관리자를 대상으로 제공됩니다.

업데이트된 정보

이 VMware vRealize Orchestrator 설치 및 구성 설명서는 제품의 각 릴리스에 따라 또는 필요에 따라 업데이트됩니다.

다음 표에는 VMware vRealize Orchestrator 설치 및 구성 설명서의 업데이트 기록이 나와 있습니다.

개정	설명
EN-002396-01	<ul style="list-style-type: none">■ “Windows용 외부 vRealize Orchestrator 6.x를 vRealize Automation 7.2로 마이그레이션,” (66 페이지) 섹션을 업데이트했습니다.■ “외부 vRealize Orchestrator 6.x 가상 장치를 vRealize Automation 7.2로 마이그레이션,” (68 페이지) 섹션을 업데이트했습니다.■ “외부 vRealize Orchestrator 7.x를 vRealize Automation 7.2로 마이그레이션,” (70 페이지) 섹션을 업데이트했습니다.■ 9장, “내장된 vRealize Orchestrator 서버 구성,” (73 페이지) 섹션을 업데이트했습니다.■ vRealize Orchestrator 로드 밸런싱 설명서를 업데이트했습니다.
EN-002396-00	최초 릴리스

VMware vRealize Orchestrator 소개

1

VMware vRealize Orchestrator는 VMware 제품은 물론 타사 기술을 관리할 자동화, 구성 가능 프로세스를 만들고 실행할 수 있는 확장 가능한 워크플로 라이브러리를 제공하는 개발 및 프로세스 자동화 플랫폼입니다.

vRealize Orchestrator는 VMware 및 타사 애플리케이션(서비스 데스크, 변경 관리 시스템, IT 자산 관리 시스템 등) 모두의 관리 및 운영 작업을 자동화합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [“Orchestrator 플랫폼의 주요 기능,”](#) (11 페이지)
- [“Orchestrator 사용자 유형과 관련 책임,”](#) (13 페이지)
- [“Orchestrator 아키텍처,”](#) (13 페이지)
- [“Orchestrator 플러그인,”](#) (14 페이지)

Orchestrator 플랫폼의 주요 기능

Orchestrator는 오케스트레이션 도구에 필요한 공통 기능을 제공하는 오케스트레이션 플랫폼, 하위 시스템의 제어를 통합하는 플러그인 아키텍처 그리고 워크플로 라이브러리의 세 가지 다른 계층으로 구성됩니다. Orchestrator는 새 플러그인 및 라이브러리를 사용하여 확장할 수 있는 개방형 플랫폼이며 REST API를 통해 더 큰 아키텍처에 통합될 수 있습니다.

목록에는 Orchestrator의 주요 기능이 나열되어 있습니다.

- | | |
|------------------|---|
| 지속성 | 운영 등급 데이터베이스는 프로세스, 워크플로 상태 및 구성 정보 등 관련 정보 저장에 사용됩니다. |
| 중앙 집중식 관리 | Orchestrator는 중앙 집중식으로 프로세스를 관리할 방법을 제공합니다. 전체 버전 기록을 가진 애플리케이션 서버 기반 플랫폼은 같은 스토리지 위치에 스크립트와 프로세스 관련 기본 형식을 저장할 수 있습니다. 이러한 방식으로 버전 관리가 되지 않고 서버에 적절한 변경 제어가 없는 스크립트를 방지할 수 있습니다. |

검사점 설정	워크플로의 각 단계는 데이터베이스에 저장되므로 서버를 다시 시작해야 할 경우 데이터 손실이 예방됩니다. 이 기능은 특히 장기 실행 프로세스에 유용합니다.
제어 센터	제어 센터 인터페이스는 런타임 작업, 워크플로 모니터링, 통합 로그 액세스 및 구성 그리고 워크플로 실행 및 시스템 리소스 간 상관 관계에 중앙 집중식 관리 인터페이스를 제공해 vRealize Orchestrator 인스턴스의 관리 효율성을 향상시킵니다. VRealize Orchestrator 로깅 메커니즘은 vRealize Orchestrator 엔진 처리량에 대한 다양한 성능 메트릭을 수집하는 추가 로그 파일을 사용해 최적화됩니다.
버전 관리	모든 Orchestrator 플랫폼 개체에는 관련 버전 기록이 있습니다. 버전 기록은 프로젝트 단계 또는 위치에 프로세스를 배포할 때 기본 변경 관리에 유용합니다.
스크립팅 엔진	Mozilla Rhino JavaScript 엔진은 Orchestrator 플랫폼을 위한 빌딩 블록을 만드는 방법을 제공합니다. 스크립팅 엔진은 기본 버전 제어, 변수 유형 확인, 이름 공간 관리 및 예외 처리를 사용해 향상됩니다. 이 엔진은 다음 빌딩 블록에서 사용할 수 있습니다. <ul style="list-style-type: none"> ■ 작업 ■ 워크플로 ■ 정책
워크플로 엔진	워크플로 엔진을 사용해 비즈니스 프로세스를 자동화할 수 있습니다. 워크플로 엔진은 워크플로에서 단계별 프로세스 자동화를 만들기 위해 다음 개체를 사용합니다. <ul style="list-style-type: none"> ■ Orchestrator가 제공하는 워크플로 및 작업 ■ 고객이 만든 사용자 지정 빌딩 블록 ■ 플러그인이 Orchestrator에 추가한 개체 사용자, 기타 워크플로, 스케줄 또는 정책이 워크플로를 시작할 수 있습니다.
정책 엔진	정책 엔진을 사용해 Orchestrator 서버 또는 플러그인된 기술에서 변경되는 조건에 반응해 이벤트를 모니터링하고 생성할 수 있습니다. 정책은 플랫폼이나 플러그인에서 이벤트를 집계할 수 있으며 이는 통합된 기술에서 변경되는 조건을 처리하는 데 도움이 됩니다.
보안	Orchestrator는 다음과 같은 고급 보안 기능을 제공합니다. <ul style="list-style-type: none"> ■ 서버 간에 가져오고 내보낸 콘텐츠에 서명하고 암호화하는 공용 키 인 프라(PKI). ■ 내보낸 콘텐츠의 보기, 편집 및 재배포 방법을 제어하는 디지털 저작권 관리(DRM). ■ 데스크톱 클라이언트와 서버 간 암호화된 통신과 웹 프론트 엔드에 HTTPS 액세스를 제공하는 SSL(Secure Sockets Layer). ■ 고급 액세스 권한 관리를 통해 이러한 프로세스가 조작하는 프로세스 및 개체에 대한 액세스를 제어할 수 있습니다.
암호화	vRealize Orchestrator는 문자열 암호화를 위해 256비트 암호화 키를 사용하는 FIPS 준수 AES(Advanced Encryption Standard)를 사용합니다. 암호화 키는 임의로 생성되며 클러스터의 일부가 아닌 장치 전반에서 고유합니다. 클러스터의 모든 노드가 같은 암호 키를 공유합니다.

Orchestrator 사용자 유형과 관련 책임

Orchestrator는 전역 사용자 역할의 특정 책임을 기반으로 다양한 도구와 인터페이스를 제공합니다. Orchestrator에는 관리자 그룹에 포함된 모든 권한을 가진 사용자(관리자)와 관리자 그룹에 포함되지 않은 제한된 권한을 가진 사용자(최종 사용자)가 있습니다.

모든 권한을 가진 사용자

Orchestrator 관리자 및 개발자는 동등한 관리 권한을 가지지만 책임이라는 관점에서 구분됩니다.

관리자	<p>이 역할은 Orchestrator 플랫폼의 모든 기능에 액세스할 수 있습니다. 기본 관리 책임은 다음 항목을 포함합니다.</p> <ul style="list-style-type: none"> ■ Orchestrator 설치 및 구성 ■ Orchestrator 및 애플리케이션의 액세스 권한 관리 ■ 패키지 가져오기 및 내보내기 ■ 워크플로 및 스케줄 지정 작업 실행 ■ 가져온 요소의 버전 제어 관리 ■ 새 워크플로 및 플러그인 생성
개발자	<p>이 사용자 유형은 Orchestrator 플랫폼의 모든 기능에 액세스할 수 있습니다. 개발자에게는 Orchestrator 클라이언트 인터페이스의 액세스 권한이 부여되며 다음과 같은 책임이 있습니다.</p> <ul style="list-style-type: none"> ■ Orchestrator 플랫폼 기능을 확장하는 애플리케이션 작성 ■ 기존 워크플로를 사용자 지정하고 새 워크플로 및 플러그인을 생성해 프로세스 자동화

제한된 권한을 가진 사용자

최종 사용자	<p>최종 사용자는 관리자나 개발자가 Orchestrator 클라이언트에서 사용할 수 있도록 만든 워크플로 및 정책을 실행 및 스케줄링할 수 있습니다.</p>
---------------	--

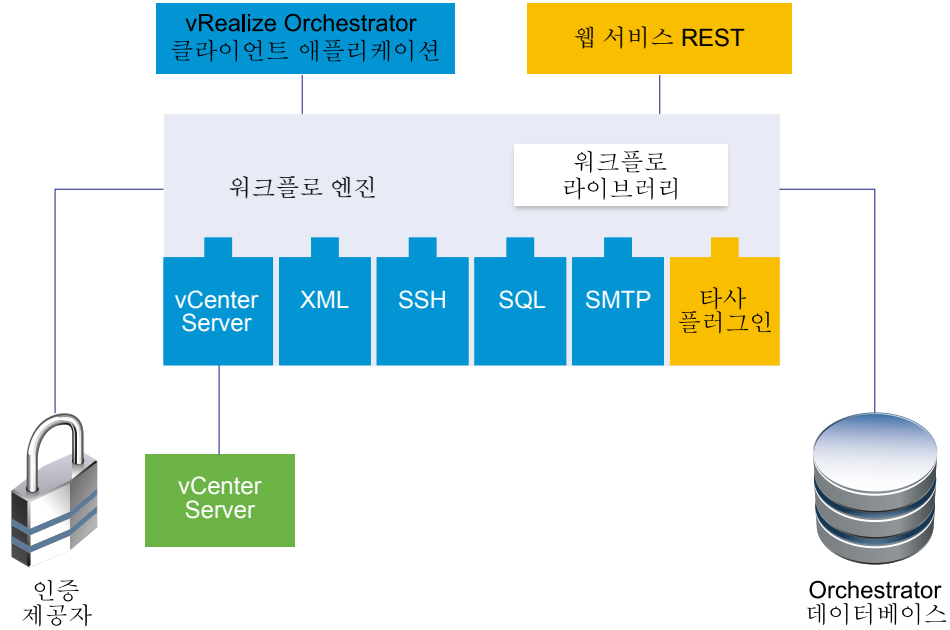
Orchestrator 아키텍처

Orchestrator는 사용자가 오케스트레이션 프로세스를 자동화하는 워크플로를 생성하고 실행할 수 있는 워크플로 라이브러리와 워크플로 엔진을 포함하고 있습니다. 사용자는 Orchestrator가 일련의 플러그인을 통해 액세스하는 다양한 기술의 개체에서 워크플로를 실행합니다.

Orchestrator는 vCenter Server 플러그인을 포함하는 표준 플러그인 집합을 제공해 사용자가 플러그인이 노출된 다양한 환경에서 작업을 오케스트레이션할 수 있습니다.

Orchestrator는 또한 개방형 아키텍처를 제공해 외부 타사 애플리케이션을 오케스트레이션 플랫폼에 플러그인할 수 있습니다. 사용자는 직접 정의한 플러그인된 기술의 개체를 워크플로에서 실행할 수 있습니다. Orchestrator는 사용자 계정을 관리하기 위해 인증 제공자에게 접속하며 실행하는 워크플로의 정보를 저장하기 위해 데이터베이스에 접속합니다. Orchestrator 클라이언트 인터페이스 또는 웹 서비스를 통해 Orchestrator, Orchestrator 워크플로 및 노출한 개체에 액세스할 수 있습니다.

그림 1-1. VMware vRealize Orchestrator 아키텍처



Orchestrator 플러그인

플러그인을 통해 Orchestrator에서 외부 기술과 애플리케이션에 액세스하고 이를 제어할 수 있습니다. Orchestrator 플러그인에서 외부 기술을 노출시킴으로써 외부 기술의 개체와 기능에 액세스하는 워크플로에서 개체와 기능을 통합할 수 있습니다.

플러그인을 사용하여 액세스할 수 있는 외부 기술에는 가상화 관리 도구, 이메일 시스템, 데이터베이스, 디렉토리 서비스, 원격 제어 인터페이스 등이 포함될 수 있습니다.

Orchestrator는 VMware vCenter Server API 및 이메일 기능과 같은 기술을 통해 워크플로 통합에 사용할 수 있는 일련의 표준 플러그인을 제공합니다. 플러그인을 사용하면 새로운 IT 서비스를 자동으로 수행하거나 기존 vRealize Automation 인프라 및 애플리케이션 서비스의 기능을 적용할 수 있습니다. 또한 Orchestrator 개방형 플러그인 아키텍처를 사용하여 다른 애플리케이션에 액세스하는 플러그인을 개발할 수 있습니다.

VMware가 개발하는 Orchestrator 플러그인은 .vmoapp 파일로 배포됩니다. VMware에서 개발하고 배포하는 Orchestrator 플러그인에 대한 자세한 내용은

http://www.vmware.com/support/pubs/vco_plugins_pubs.html를 참조하십시오. 타사

Orchestrator 플러그인에 대한 자세한 내용은

<https://solutionexchange.vmware.com/store/vco> 페이지를 참조하십시오.

Orchestrator 시스템 요구 사항

시스템은 Orchestrator가 제대로 작동하기 위해 필요한 기술적 요구 사항을 충족해야 합니다.

지원되는 vCenter Server, vSphere Web Client, vRealize Automation 및 기타 VMware 솔루션과 호환 가능한 데이터베이스 버전 목록은 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

이 장에서는 다음 주제에 대해 설명합니다.

- “Orchestrator Appliance에 대한 하드웨어 요구 사항,” (15 페이지)
- “지원되는 디렉토리 서비스,” (15 페이지)
- “Orchestrator에서 지원하는 브라우저,” (16 페이지)
- “Orchestrator 데이터베이스 요구 사항,” (16 페이지)
- “Orchestrator Appliance에 포함된 소프트웨어,” (16 페이지)
- “암호 요구 사항,” (16 페이지)
- “국제화 지원 레벨,” (17 페이지)

Orchestrator Appliance에 대한 하드웨어 요구 사항

Orchestrator Appliance는 사전 구성된 Linux 기반 가상 시스템입니다. 장치를 배포하기 전에 시스템이 하드웨어 최소 요구 사항을 충족하는지 확인하십시오.

Orchestrator Appliance의 하드웨어 구성을 다음과 같습니다.

- CPU 2개
- 메모리 6GB
- 하드 디스크 17GB

Orchestrator 서버에는 최소 2GB의 여유 메모리가 필요하므로 기본 메모리 크기를 줄이지 마십시오.

지원되는 디렉토리 서비스

LDAP 서버를 인증에 사용하려면 작동하는 LDAP 서버를 설정하고 구성했는지 확인하십시오.

참고 LDAP 인증은 사용되지 않으며 향후 버전에서 지원되지 않습니다.

Orchestrator는 다음 디렉토리 서비스 유형을 지원합니다.

- Windows Server Active Directory

- OpenLDAP

중요 양방향 신뢰를 갖지만 같은 트리에 있지 않은 멀티 도메인은 지원되지 않고 Orchestrator에서 작동하지 않습니다. 멀티 도메인 Active Directory를 지원하는 구성만 도메인 트리에 해당합니다. 포리스트와 외부 트러스트가 지원되지 않습니다.

Orchestrator에서 지원하는 브라우저

제어 센터에는 웹 브라우저가 필요합니다.

제어 센터에 연결하려면 다음 브라우저 중 하나를 사용해야 합니다.

- Microsoft Internet Explorer 10 이상
- Mozilla Firefox
- Google Chrome

Orchestrator 데이터베이스 요구 사항

Orchestrator 서버에는 데이터베이스가 필요합니다. Orchestrator PostgreSQL에 사전 구성된 데이터베이스는 즉시 사용 가능합니다. 환경에 따라 외부 데이터베이스를 사용할 수도 있습니다.

지원되는 데이터베이스 버전 전체 목록은 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

Orchestrator Appliance에 포함된 소프트웨어

Orchestrator Appliance는 최적화된 Orchestrator 실행 환경을 제공하는 사전 구성된 가상 시스템입니다. 이 장치는 사전 설치된 소프트웨어와 함께 제공됩니다.

Orchestrator Appliance 패키지에는 다음 소프트웨어가 포함됩니다.

- VMware용 SUSE Linux Enterprise 서버 11 업데이트 3, 64비트 에디션
- PostgreSQL
- Orchestrator

기본 Orchestrator Appliance 데이터베이스 구성은 즉시 사용할 수 있습니다.

포함된 LDAP의 기본 구성은 실험 및 테스트 용도에만 적합합니다. 운영 환경에서 Orchestrator Appliance를 사용하려면 새 디렉토리 서비스를 설정하고 이와 작동하도록 Orchestrator 서버를 구성해야 합니다. 또한 vRealize Automation, vSphere 또는 vCenter Single Sign-On을 통해 Orchestrator 서버를 인증하도록 구성할 수도 있습니다. 외부 LDAP 또는 Single Sign-On 구성에 대한 자세한 내용은 [“인증 유형 선택,”](#) (31 페이지)을(를) 참조하십시오.

운영 환경에 대한 데이터베이스 구성에 대한 자세한 내용은 [“Orchestrator 데이터베이스 설정,”](#) (20 페이지)을(를) 참조하십시오.

참고 LDAP 인증은 사용되지 않으며 향후 버전에서 지원되지 않습니다.

암호 요구 사항

Orchestrator Appliance의 루트 암호를 구성하는 경우 사전 정의된 암호 요구 사항을 충족해야 합니다.

OVF 템플릿에서 Orchestrator Appliance를 배포하는 경우 정의하는 루트 암호는 8자 이상이어야 합니다.

제어 센터에서 로컬 사용자 암호를 변경하는 경우 새 암호가 모든 요구 사항을 충족하지 않으면 허용되지 않습니다.

- 암호는 8자 이상이어야 합니다.
- 암호는 하나 이상의 숫자를 포함해야 합니다.
- 암호는 하나 이상의 대문자를 포함해야 합니다.
- 암호는 하나 이상의 소문자를 포함해야 합니다.
- 암호는 하나 이상의 특수 문자를 포함해야 합니다.

참고 ASCII가 아닌 문자 또는 확장 ASCII 문자는 지원되지 않습니다. 이러한 문자는 암호를 정의하는 과정에서 허용될 수 있으나 저장 작업 중 그리고 Orchestrator 노드를 클러스터에 조인할 때 해당 작업의 실패를 유발합니다.

국제화 지원 레벨

Orchestrator 제어 센터는 스페인어, 프랑스어, 독일어, 중국어(번체), 중국어(간체), 한국어, 일본어 로케일을 지원합니다. Orchestrator 클라이언트는 국제화 레벨 1을 지원합니다.

Orchestrator의 비 ASCII 문자 지원

Orchestrator 클라이언트는 현지화되지 않았지만 영어 이외의 운영 체제에서 실행 가능하고 비 ASCII 문자도 지원합니다.

표 2-1. Orchestrator GUI의 비 ASCII 문자 지원

비 ASCII 문자에 대한 지원				
Orchestrator 항목	설명 필드	이름 필드	입력 및 출력 매개 변수	특성
작업	예	아니요	아니요	아니요
폴더	예	예	-	-
구성 요소	예	예	-	아니요
패키지	예	예	-	-
정책	예	예	-	-
정책 템플릿	예	예	-	-
리소스 요소	예	예	-	-
워크플로	예	예	아니요	아니요
워크플로 프레젠테이션 표시 그룹 및 입력 단계	예	예	-	-

Oracle 데이터베이스에 대한 비 ASCII 문자 지원

Oracle 데이터베이스에 문자를 올바른 형식으로 저장하려면 데이터베이스 연결을 구성하고 Orchestrator의 테이블 구조를 빌드하기 전에 NLS_CHARACTER_SET 매개 변수를 AL32UTF8로 설정해야 합니다. 이 설정은 다국어 환경에서 매우 중요합니다.

Orchestrator 구성 요소 설정

Orchestrator Appliance를 다운로드하고 배포하면 Orchestrator 서버는 사전 구성됩니다. 배포 후 서비스가 자동으로 시작됩니다.

Orchestrator 설정의 가용성 및 확장성을 강화하려면 다음 지침을 따르십시오.

- 데이터베이스를 설치 및 구성하고 Orchestrator를 구성하여 데이터베이스에 연결합니다.
- 인증 제공자를 설치 및 구성하고 이와 작동하도록 Orchestrator를 구성합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [“vCenter Server 설정,”](#) (19 페이지)
- [“인증 방법,”](#) (19 페이지)
- [“Orchestrator 데이터베이스 설정,”](#) (20 페이지)

vCenter Server 설정

Orchestrator 설정에서 vCenter Server 인스턴스의 개수를 증가시키면 Orchestrator는 더 많은 세션을 관리해야 합니다. 각 활성 세션은 해당 vCenter Server에서 작업을 생성하며 지나치게 많은 활성 세션은 10개 이상의 vCenter Server가 연결되는 경우 Orchestrator에 시간 초과를 유발할 수 있습니다.

vCenter Server의 지원되는 버전 목록은 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

참고 네트워크의 대역폭 및 지연 시간이 충분하다면 Orchestrator 설정의 다른 가상 시스템에서 여러 vCenter Server 인스턴스를 실행할 수 있습니다. LAN을 사용하여 Orchestrator와 vCenter Server 간 통신을 향상시키려면 100MB 선이 필수입니다.

인증 방법

Orchestrator에서 사용자 권한을 인증 및 관리하려면 LDAP 서버, Single Sign-On 서버 또는 vRealize Automation에 대한 연결이 필요합니다.

참고 LDAP 인증은 사용되지 않으며 향후 버전에서 지원되지 않습니다.

Orchestrator Appliance를 다운로드하고 배포하면 Orchestrator 서버는 장치와 함께 배포되는 포함된 ApacheDS LDAP 서버와 작동하도록 사전 구성됩니다. 포함된 LDAP의 기본 구성은 테스트 용도에만 적합합니다. 운영 환경에서 Orchestrator를 사용하려면 LDAP 서버나 vCenter Single Sign-On 서버를 설정하거나 vRealize Automation과의 연결을 설정하고 이를 Orchestrator와 작동할 수 있도록 구성해야 합니다.

Orchestrator 서버와 물리적으로 가장 가까운 거리에 위치한 LDAP 서버에 연결하여 시스템 성능을 저하시키는 LDAP 쿼리에 대한 응답 시간을 줄일 수 있습니다. Orchestrator는 Active Directory 및 OpenLDAP 서비스 유형을 지원합니다.

LDAP 쿼리의 성능을 향상시키려면 사용자 및 그룹 조회 기본을 가능한 구체적으로 지정합니다. 액세스가 필요하지 않은 다수의 사용자로 이루어진 전체 조직을 포함하는 대신 액세스가 필요한 대상 그룹으로 사용자를 제한합니다. 필요한 리소스는 선택한 데이터베이스 및 디렉토리 서비스의 조합에 따라 다릅니다. 권장 사항은 LDAP 서버 설명서를 참조하십시오.

vCenter Single Sign-On 인증 방법을 사용하려면 먼저 vCenter Single Sign-On을 설치해야 합니다. 설치 및 구성된 vCenter Single Sign-On 서버를 사용하려면 Orchestrator 서버를 구성해야 합니다.

vRealize Automation 및 vSphere를 통해 제어 센터의 인증 설정에서 Single Sign-On 인증을 사용할 수 있습니다.

Orchestrator 데이터베이스 설정

Orchestrator에는 워크플로와 작업을 저장할 데이터베이스가 필요합니다.

Orchestrator Appliance를 다운로드하고 배포하면 Orchestrator 서버는 해당 장치에 배포된 PostgreSQL 데이터베이스와 작동하도록 미리 구성됩니다. 기본 Orchestrator Appliance 데이터베이스 구성은 즉시 사용할 수 있습니다. 그러나 고부하 운영 환경에서 Orchestrator를 사용하려면 별도의 데이터베이스를 설정하고 제어 센터에서 작동하도록 Orchestrator를 구성해야 합니다.

Orchestrator 서버는 Oracle, Microsoft SQL Server 그리고 PostgreSQL 데이터베이스를 지원합니다.

Orchestrator 데이터베이스를 설정하는 일반적인 워크플로는 다음과 같은 단계로 구성됩니다.

- 1 데이터베이스를 생성합니다. 데이터베이스 생성에 대한 자세한 내용은 데이터베이스 제공자의 설명서를 참조하십시오.
- 2 데이터베이스 원격 연결을 활성화합니다.
- 3 데이터베이스 연결 매개 변수를 구성합니다. 자세한 내용은 [“Orchestrator 데이터베이스 연결 구성,”](#) (38 페이지) 항목을 참조하십시오.

Orchestrator 클러스터를 설정하려면 데이터베이스가 다중 연결을 허용하도록 구성하여 클러스터에 있는 여러 Orchestrator 서버 인스턴스의 연결을 허용할 수 있도록 해야 합니다.

데이터베이스 설정은 Orchestrator 성능에 영향을 미칠 수 있습니다. Orchestrator 서버가 설치된 시스템을 제외한 다른 시스템에 데이터베이스를 설치하십시오. 이 방법을 사용하면 JVM과 데이터베이스 서버가 CPU, RAM 및 I/O를 공유하지 않습니다.

Orchestrator 서버의 거의 모든 활동이 데이터베이스에서 작업을 트리거하므로 데이터베이스의 위치가 중요합니다. 데이터베이스 연결 지연을 방지하기 위해 Orchestrator 서버와 지리적으로 가장 가까우며 사용 가능한 가장 높은 대역폭을 가진 네트워크에 있는 데이터베이스 서버에 연결하십시오.

Orchestrator 데이터베이스의 크기는 설정과 워크플로 토큰의 처리 방식에 따라 다릅니다. 각 vCenter Server 개체에 50KB를, 각 워크플로 실행에 4KB를 할당하십시오.



주의 Orchestrator 데이터베이스가 설치된 시스템에 사용 가능한 디스크 공간이 1GB 이상인지 확인하십시오.

하드 디스크 공간이 부족하면 Orchestrator 서버와 클라이언트가 제대로 작동하지 않을 수 있습니다.

Orchestrator 설치 및 업그레이드

Orchestrator는 서버 구성 요소 및 클라이언트 구성 요소로 구성됩니다.

클라이언트 설치 가능 Orchestrator는 64비트 Windows, Linux 및 Mac 시스템에서 작동할 수 있습니다.

Orchestrator를 사용하려면 Orchestrator 서버 서비스를 시작한 다음 Orchestrator 클라이언트를 시작해야 합니다.

Orchestrator 제어 센터를 사용하여 Orchestrator 기본 구성 설정을 변경할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [“Orchestrator Appliance 다운로드 및 배포,”](#) (21 페이지)
- [“Orchestrator Appliance 5.5.x 이상을 7.x로 업그레이드,”](#) (24 페이지)
- [“Orchestrator 클러스터 5.5.x 이상을 7.x로 업그레이드,”](#) (27 페이지)
- [“Orchestrator 클러스터 7.0에서 7.x로 업그레이드,”](#) (28 페이지)

Orchestrator Appliance 다운로드 및 배포

템플릿에서 Orchestrator Appliance를 배포하여 다운로드 및 설치합니다.

필수 조건

- vCenter Server가 설치되고 실행 중인지 확인합니다.
- 장치를 배포하는 호스트가 하드웨어 최소 요구 사항을 충족하는지 확인합니다. 자세한 내용은 [“Orchestrator Appliance에 대한 하드웨어 요구 사항,”](#) (15 페이지)을 참조하십시오.
- 시스템이 분리되거나 인터넷에 연결되지 않은 경우 VMware 웹 사이트에서 해당 장치에 대한 .ova 파일을 다운로드해야 합니다.

프로시저

- 1 vSphere Web Client에 관리자로 로그인합니다.
- 2 vSphere Web Client에서 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트와 같은 가상 시스템의 유효한 상위 개체인 인벤토리 개체를 선택합니다.
- 3 **작업 > OVF 템플릿 배포**를 선택합니다.
- 4 .ova 파일의 경로 또는 URL을 입력하고 **다음**을 클릭합니다.
- 5 OVF 템플릿 세부 정보를 검토하고 **다음**을 클릭합니다.
- 6 라이선스 계약 조건에 동의하고 **다음**을 클릭합니다.
- 7 배포된 장치의 이름 및 위치를 입력하고 **다음**을 클릭합니다.

- 8 호스트, 클러스터, 리소스 풀 또는 vApp을 장치가 실행되는 대상으로 선택하고 **다음**을 클릭합니다.
- 9 저장하려는 가상 디스크 및 장치의 스토리지에 대한 형식을 선택합니다.

형식	설명
느리게 비워지는 씩 프로비저닝	기본 씩 형식의 가상 디스크를 생성합니다. 가상 디스크에 필요한 공간은 가상 디스크 생성 중에 할당됩니다. 물리적 디바이스에 남아 있는 데이터는 생성 동안에 지워지지 않지만 나중에 가상 시스템에서 처음으로 쓰는 경우, 해당 데이터는 요구대로 비워집니다.
빠르게 비워지는 씩 프로비저닝	Fault Tolerance와 같은 클러스터링 기능을 지원합니다. 가상 디스크에 필요한 공간은 가상 디스크 생성 중에 할당됩니다. 물리적 디바이스에 남아 있는 모든 데이터는 가상 디스크를 생성하는 동안 비워집니다. 다른 형식의 디스크를 생성하는 것보다 이 형식의 디스크를 생성하는 것이 더 오래 걸릴 수도 있습니다.
씬 프로비저닝된 형식	하드 디스크 공간을 절약합니다. 씬 디스크의 경우 선택하는 디스크 크기 값에 기반하여 디스크가 필요로 하는 만큼의 데이터스토어 공간을 프로비저닝합니다. 씬 디스크는 먼저 작은 크기부터 시작합니다. 초기 작업을 위해 이 디스크에 필요한 데이터스토어 공간 만큼의 크기만 사용합니다.

- 10 사용하려는 옵션을 선택하고 루트 사용자 계정의 초기 암호를 설정합니다.
초기 암호는 8자 이상이어야 합니다.

중요 Orchestrator Appliance의 루트 계정에 대한 암호는 365일 후에 만료됩니다. Orchestrator Appliance에 루트로 로그인하고 `passwd -x number_of_days name_of_account`를 실행하여 계정에 대한 만료 시간을 늘릴 수 있습니다. Orchestrator Appliance 루트 암호의 만료 시간을 무한대로 늘리려면 `passwd -x 99999 root`를 실행합니다.

- 11 (선택 사항) 네트워크 설정을 구성하고 **다음**을 클릭합니다.
기본적으로 Orchestrator Appliance는 DHCP를 사용합니다. 장치 웹 콘솔에서 이 설정을 변경하고 고정 IP 주소를 할당할 수 있습니다.
- 12 완료 준비 페이지를 검토하고 **마침**을 클릭합니다.

Orchestrator Appliance가 배포되었습니다.

Orchestrator Appliance 전원 켜기 및 홈 페이지 열기

Orchestrator Appliance를 사용하려면 먼저 전원을 켜고 가상 장치에 대한 IP 주소를 가져와야 합니다.

프로시저

- 1 vSphere Web Client에 관리자로 로그인합니다.
- 2 Orchestrator Appliance를 마우스 오른쪽 버튼으로 클릭하고 **전원 > 전원 켜기**를 선택합니다.
- 3 **요약** 탭에서 Orchestrator Appliance IP 주소를 확인합니다.
- 4 웹 브라우저에서 Orchestrator Appliance 가상 시스템의 IP 주소로 이동합니다.

`http://orchestrator_appliance_ip`

루트 암호 변경

보안을 이유로 Orchestrator Appliance 루트 암호를 변경할 수 있습니다.

중요 Orchestrator Appliance의 루트 계정에 대한 암호는 365일 후에 만료됩니다. Orchestrator Appliance에 루트로 로그인하고 `passwd -x number_of_days name_of_account`를 실행하여 계정에 대한 만료 시간을 늘릴 수 있습니다. Orchestrator Appliance 루트 암호의 만료 시간을 무한대로 늘리려면 `passwd -x 99999 root` 명령을 실행합니다.

필수 조건

- Orchestrator Appliance를 다운로드 및 배포합니다.
- 애플리케이션이 가동되어 실행 중인지 확인합니다.

프로시저

- 1 웹 브라우저에서 `https://orchestrator_appliance_ip:5480`으로 이동합니다.
- 2 장치 사용자 이름 및 암호를 입력합니다.
- 3 **관리** 탭을 클릭합니다.
- 4 **현재 관리자 암호** 텍스트 상자에 현재 루트 암호를 입력합니다.
- 5 **새 관리자 암호 및 새 관리자 암호 다시 입력** 텍스트 상자에 새 암호를 입력합니다.
- 6 **암호 변경**을 클릭합니다.

Orchestrator Appliance 루트 리눅스 사용자의 암호가 변경되었습니다.

vRealize Orchestrator 장치에서 SSH 관리자 로그인 사용 또는 사용 안 함

SSH를 사용하여 Orchestrator Appliance에 루트로 로그인할 수 있도록 하거나 로그인할 수 없도록 설정할 수 있습니다.

필수 조건

- Orchestrator Appliance를 다운로드 및 배포합니다.
- 애플리케이션이 가동되어 실행 중인지 확인합니다.

프로시저

- 1 웹 브라우저에서 `https://orchestrator_appliance_ip:5480`으로 이동합니다.
- 2 루트로 로그인합니다.
- 3 **관리** 탭에서 **SSH 서비스 사용**을 선택하여 Orchestrator SSH 서비스를 사용하도록 설정합니다.
- 4 (선택 사항) **관리자 SSH 로그인 사용**을 클릭하면 SSH를 사용하여 Orchestrator Appliance에 루트로 로그인할 수 있습니다.
- 5 **설정 저장**을 클릭합니다.

SSH 상태가 실행 중으로 표시됩니다.

Orchestrator Appliance의 네트워크 설정 구성

Orchestrator Appliance의 네트워크 설정을 구성하여 정적 IP 주소를 할당하고 프록시 설정을 정의합니다.

필수 조건

- Orchestrator Appliance를 다운로드 및 배포합니다.
- 애플리케이션이 가동되어 실행 중인지 확인합니다.

프로시저

- 1 웹 브라우저에서 `https://orchestrator_appliance_ip:5480`으로 이동합니다.
- 2 루트로 로그인합니다.
- 3 **네트워크** 탭에서 **주소**를 클릭합니다.
- 4 장치가 IP 주소 설정을 가져오는 방법을 선택합니다.

옵션	설명
DHCP	DHCP 서버에서 IP 설정을 가져옵니다. 기본 설정입니다.
정적	정적 IP 설정을 사용합니다. IP 주소, 넷마스크 및 게이트웨이를 입력합니다.

네트워크 설정에 따라 IPv4 및 IPv6 주소 유형을 선택해야 할 수 있습니다.

- 5 (선택 사항) 필요한 네트워크 구성 정보를 입력합니다.
- 6 **설정 저장**을 클릭합니다.
- 7 (선택 사항) 프록시 설정을 지정하고 **설정 저장**을 클릭합니다.

Orchestrator Appliance 5.5.x 이상을 7.x로 업그레이드

vRealize Orchestrator 7.2는 버전 5.5.x, 6.0.x, 7.0 및 7.1에서 인플레이스 업그레이드를 지원합니다.

가상 장치 관리 인터페이스(VAMI)를 통해 기존 Orchestrator Appliance를 업그레이드할 수 있습니다.

기본 VMware 저장소를 사용하여 Orchestrator Appliance 업그레이드

Orchestrator를 구성하여 기본 VMWare 저장소에서 업그레이드 패키지를 다운로드할 수 있습니다.

필수 조건

- 모든 네트워크 파일 시스템을 마운트 해제합니다. 자세한 내용은 vSphere 가상 시스템 관리 설명서를 참조하십시오.
- Orchestrator Appliance의 메모리를 6GB 이상으로 늘립니다. 자세한 내용은 vSphere 가상 시스템 관리 설명서를 참조하십시오.
- Orchestrator 가상 시스템의 스냅샷을 생성합니다. 자세한 내용은 vSphere 가상 시스템 관리 설명서를 참조하십시오.
- 외부 데이터베이스를 사용하는 경우 해당 데이터베이스를 백업하십시오.
- 사전 구성된 Orchestrator PostgreSQL 데이터베이스를 사용하는 경우 제어 센터의 **데이터베이스 내보내기** 메뉴를 사용하여 데이터베이스를 백업하십시오.

프로시저

- 1 https://orchestrator_server:5480에 있는 VAMI(가상 장치 관리 인터페이스)로 이동하고 **루트**로 로그인합니다.
- 2 **업데이트** 탭에서 **설정**을 클릭합니다.
기본 저장소 사용 옵션 옆에 있는 라디오 버튼이 선택됩니다.
- 3 **상태** 페이지에서 **업데이트 확인**을 클릭합니다.
- 4 사용 가능한 업데이트가 있으면 **업데이트 설치**를 클릭합니다.
- 5 VMware 최종 사용자 사용권 계약에 동의하고 업데이트 설치를 확인합니다.
- 6 업데이트를 완료하려면 Orchestrator Appliance를 다시 시작합니다.
 - a VAMI(가상 장치 관리 인터페이스)에 **루트**로 다시 로그인합니다.
- 7 (선택 사항) **업데이트** 탭에서 최신 버전의 Orchestrator Appliance가 설치되었는지 확인합니다.

Orchestrator Appliance를 성공적으로 업그레이드했습니다.

후속 작업

제어 센터의 **구성 검증** 페이지에서 Orchestrator가 제대로 구성되었는지 확인합니다.

ISO 이미지를 사용하여 Orchestrator Appliance 업그레이드

Orchestrator를 구성하여 장치의 CD-ROM 드라이브에 마운트된 ISO 이미지 파일에서 업그레이드 패키지를 다운로드할 수 있습니다.

필수 조건

- 모든 네트워크 파일 시스템을 마운트 해제합니다. 자세한 내용은 vSphere 가상 시스템 관리 설명서를 참조하십시오.
- Orchestrator Appliance의 메모리를 6GB 이상으로 늘립니다. 자세한 내용은 vSphere 가상 시스템 관리 설명서를 참조하십시오.
- Orchestrator 가상 시스템의 스냅샷을 생성합니다. 자세한 내용은 vSphere 가상 시스템 관리 설명서를 참조하십시오.
- 외부 데이터베이스를 사용하는 경우 해당 데이터베이스를 백업하십시오.
- 사전 구성된 Orchestrator PostgreSQL 데이터베이스를 사용하는 경우 제어 센터의 **데이터베이스 내보내기** 메뉴를 사용하여 데이터베이스를 백업하십시오.

프로시저

- 1 공식 VMware 다운로드 사이트에서 VMware vRealize Orchestrator Appliance 버전 .iso 업데이트 저장소 아카이브를 다운로드합니다.
- 2 Orchestrator Appliance 가상 장치의 CD-ROM 드라이브를 연결합니다. 자세한 내용은 vSphere 가상 장치 관리 설명서를 참조하십시오.
- 3 ISO 이미지 파일을 장치의 CD-ROM 드라이브에 마운트합니다. 자세한 내용은 vSphere 가상 장치 관리 설명서를 참조하십시오.
- 4 https://orchestrator_server:5480에 있는 VAMI(가상 장치 관리 인터페이스)로 이동하고 **루트**로 로그인합니다.
- 5 **업데이트** 탭에서 **설정**을 클릭합니다.
- 6 **CD-ROM 업데이트 사용** 옵션 옆에 있는 라디오 버튼을 선택합니다.

- 7 **상태** 페이지로 돌아갑니다.
사용 가능한 업그레이드 버전이 표시됩니다.
- 8 **업데이트 설치**를 클릭합니다.
- 9 VMware 최종 사용자 사용권 계약에 동의하고 업데이트 설치를 확인합니다.
- 10 업데이트를 완료하려면 Orchestrator Appliance를 다시 시작합니다.
 - a VAMI(가상 장치 관리 인터페이스)에 **루트**로 다시 로그인합니다.
- 11 (선택 사항) **업데이트** 탭에서 최신 버전의 Orchestrator Appliance가 설치되었는지 확인합니다.
Orchestrator Appliance를 성공적으로 업그레이드했습니다.

후속 작업

제어 센터의 **구성 검증** 페이지에서 Orchestrator가 제대로 구성되었는지 확인합니다.

지정된 저장소를 사용하여 Orchestrator Appliance 업그레이드

Orchestrator를 구성하여 업그레이드 아카이브를 업로드하는 로컬 저장소를 사용할 수 있습니다.

필수 조건

- 모든 네트워크 파일 시스템을 마운트 해제합니다. 자세한 내용은 vSphere 가상 시스템 관리 설명서를 참조하십시오.
- Orchestrator Appliance의 메모리를 6GB 이상으로 늘립니다. 자세한 내용은 vSphere 가상 시스템 관리 설명서를 참조하십시오.
- Orchestrator 가상 시스템의 스냅샷을 생성합니다. 자세한 내용은 vSphere 가상 시스템 관리 설명서를 참조하십시오.
- 외부 데이터베이스를 사용하는 경우 해당 데이터베이스를 백업하십시오.
- 사전 구성된 Orchestrator PostgreSQL 데이터베이스를 사용하는 경우 제어 센터의 **데이터베이스 내보내기** 메뉴를 사용하여 데이터베이스를 백업하십시오.

프로시저

- 1 업그레이드를 위한 로컬 저장소를 준비합니다.
 - a 로컬 웹 서버를 설치하고 구성합니다.
 - b 공식 VMware 다운로드 사이트에서 `VMware-vRO-Appliance-version-build_number-updaterepo.zip`을 다운로드합니다.
 - c .ZIP 압축 파일을 로컬 저장소에 풉니다.
- 2 `https://orchestrator_server:5480`에 있는 VAMI(가상 장치 관리 인터페이스)로 이동하고 **루트**로 로그인합니다.
- 3 **업데이트** 탭에서 **설정**을 클릭합니다.
- 4 **지정된 저장소 사용** 옵션 옆에 있는 라디오 버튼을 선택합니다.
- 5 Update_Repo 디렉토리를 가리키도록 로컬 저장소의 URL 주소를 입력합니다.
`http://local_web_server:port/build/mts/release/bora-build_number/publish/exports/Update_Repo`
- 6 로컬 저장소에 인증이 필요한 경우 사용자 이름과 암호를 입력합니다.
- 7 **설정 저장**을 클릭합니다.
- 8 **상태** 페이지에서 **업데이트 확인**을 클릭합니다.

- 9 사용 가능한 업데이트가 있으면 **업데이트 설치**를 클릭합니다.
- 10 VMware 최종 사용자 사용권 계약에 동의하고 업데이트 설치를 확인합니다.
- 11 업데이트를 완료하려면 Orchestrator Appliance를 다시 시작합니다.
 - a VAMI(가상 장치 관리 인터페이스)에 **루트**로 다시 로그인합니다.
- 12 (선택 사항) **업데이트** 탭에서 최신 버전의 Orchestrator Appliance가 설치되었는지 확인합니다.

Orchestrator Appliance를 성공적으로 업그레이드했습니다.

후속 작업

제어 센터의 **구성 검증** 페이지에서 Orchestrator가 제대로 구성되었는지 확인합니다.

Orchestrator 클러스터 5.5.x 이상을 7.x로 업그레이드

단일 인스턴스를 업그레이드하고 버전 7.x에서 새로 설치된 노드를 가입하여 Orchestrator 클러스터를 버전 7.x로 업그레이드할 수 있습니다.

필수 조건

- 모든 vRealize Orchestrator 서버 노드의 스냅샷을 생성합니다.
- Orchestrator 공유 데이터베이스를 백업합니다.

프로시저

- 1 모든 클러스터 노드에서 Orchestrator 서비스인 vco-server, vco-configurator, vco-proxy를 중지합니다.
- 2 클러스터에서 Orchestrator 서버 인스턴스 중 하나만 업그레이드합니다.

“[기본 VMware 저장소를 사용하여 Orchestrator Appliance 업그레이드](#),” (24 페이지) 항목을 참조하십시오.
- 3 업그레이드한 Orchestrator 서버의 구성 서비스를 시작하고 **루트**로 제어 센터에 로그인합니다.
- 4 **구성 검증** 페이지로 이동하여 시스템 구성 요소의 상태를 확인합니다.
- 5 업그레이드된 버전에서 새 Orchestrator 장치를 배포합니다.
- 6 기존 인스턴스의 네트워크 설정으로 새 노드를 구성합니다.
- 7 제어 센터의 **Orchestrator 클러스터 관리** 페이지에서 새 노드를 클러스터의 업그레이드된 노드에 가입시킵니다.
- 8 제어 센터의 **시작 옵션** 페이지에서 Orchestrator 서버를 다시 시작하여 노드 간의 구성 지문을 일치하도록 합니다.
- 9 제어 센터의 **구성 검증** 페이지를 열어 vRealize Orchestrator 클러스터가 올바르게 구성되었는지 확인합니다.
- 10 (선택 사항) 클러스터의 각 노드에 대해 **단계 5**에서 **단계 9**까지를 반복합니다.

Orchestrator 클러스터를 성공적으로 업그레이드했습니다.

Orchestrator 클러스터 7.0에서 7.x로 업그레이드

클러스터에서 여러 Orchestrator 서버 인스턴스가 함께 작동합니다. Orchestrator 서버 인스턴스의 클러스터 집합이 이미 설정되어 있는 경우 해당 노드를 업그레이드하여 클러스터를 최신 Orchestrator 버전으로 업그레이드할 수 있습니다.

프로시저

- 1 모든 클러스터 노드에서 Orchestrator 서비스인 vco-server, vco-configurator, vco-proxy를 중지합니다.
- 2 클러스터에서 Orchestrator 서버 인스턴스 중 하나를 업그레이드합니다.
“기본 VMware 저장소를 사용하여 Orchestrator Appliance 업그레이드,” (24 페이지) 항목을 참조하십시오.
- 3 업그레이드한 Orchestrator 서버의 구성 서비스를 시작하고 **루트**로 제어 센터에 로그인합니다.
- 4 **구성 검증** 페이지로 이동하여 시스템 구성 요소의 상태를 확인합니다.
- 5 클러스터의 기타 모든 Orchestrator 서버 인스턴스를 업그레이드합니다.
- 6 제어 센터의 **시작 옵션** 페이지에서 Orchestrator 서버를 다시 시작하여 노드 간의 구성 지문을 일치하도록 합니다.
- 7 제어 센터의 **구성 검증** 페이지를 열어 vRealize Orchestrator 클러스터가 올바르게 구성되었는지 확인합니다.

Orchestrator 클러스터를 성공적으로 업그레이드했습니다.

Orchestrator Appliance 에 vRealize Orchestrator 구성

5

Orchestrator Appliance는 미리 구성된 Linux 기반 가상 시스템이지만 기본 vCenter Server 플러그인과 기타 기본 Orchestrator 플러그인을 구성해야 합니다. 또한 Orchestrator 설정을 변경하고 싶을 수도 있습니다.

Orchestrator Appliance를 중간 또는 대규모 환경에서 사용하려고 한다면 최적의 성능을 위해 인증 제공자를 변경하십시오.

참고 LDAP 인증은 사용되지 않으며 향후 버전에서 지원되지 않습니다.

Orchestrator Appliance에는 미리 구성된 PostgreSQL 데이터베이스와 포함된 ApacheDS LDAP 서버가 포함되어 있습니다. PostgreSQL 데이터베이스와 ApacheDS LDAP 서버는 가상 장치 Linux 콘솔에서 로컬로만 액세스할 수 있습니다.

미리 구성된 소프트웨어	기본 사용자 그룹 또는 사용자	암호
미리 구성된 PostgreSQL	사용자: vmware	vmware
포함된 ApacheDS LDAP	사용자 그룹: vcoadmins 사용자: vcoadmin 기본적으로 관리자가 Orchestrator 관리자로 설정되어 있습니다.	vcoadmin
포함된 ApacheDS LDAP	사용자 그룹: vcousers 사용자: vcouser	vcouser

미리 구성된 PostgreSQL 데이터베이스는 즉시 사용 가능합니다. 고부하 운영 환경에서 Orchestrator 장치를 사용하려면 미리 구성된 PostgreSQL을 외부 데이터베이스 인스턴스로 교체하십시오. 외부 데이터베이스 설정에 대한 자세한 내용은 [“Orchestrator 데이터베이스 연결 구성,”](#) (38 페이지) 항목을 참조하십시오.

포함된 ApacheDS LDAP는 테스트용으로만 적합합니다. 운영 환경에서 Orchestrator 장치를 사용하려면 디렉토리 서비스를 외부 지원으로 구성하거나 vRealize Automation, vSphere 및 vCenter Single Sign-On 인증을 사용하십시오. 외부 디렉토리 서비스 설정 또는 vRealize Automation, vSphere 및 vCenter Single Sign-On 인증 제공자에 대한 자세한 내용은 [“인증 유형 선택,”](#) (31 페이지) 항목을 참조하십시오.

이 장에서는 다음 주제에 대해 설명합니다.

- [“제어 센터 로그인,”](#) (30 페이지)
- [“Orchestrator 네트워크 포트,”](#) (30 페이지)
- [“인증 유형 선택,”](#) (31 페이지)
- [“Orchestrator 데이터베이스 연결 구성,”](#) (38 페이지)
- [“인증서 관리,”](#) (41 페이지)

- “Orchestrator 플러그인 구성,” (43 페이지)
- “Orchestrator 시작 옵션,” (45 페이지)
- “Orchestrator 가용성 및 확장성,” (45 페이지)
- “고객 경험 향상 프로그램 구성,” (49 페이지)

제어 센터 로그인

구성 프로세스를 시작하려면 제어 센터에 액세스해야 합니다.

프로시저

- 1 웹 브라우저에서 `https://사용자의_orchestrator_서버_IP_또는_DNS_이름:8281`로 이동해 **Orchestrator 제어 센터**를 클릭하거나 `https://사용자의_orchestrator_서버_IP_또는_DNS_이름:8283/vco-controlcenter`로 직접 이동해 제어 센터에 액세스합니다.
- 2 초기에 설정한 기본 사용자 이름과 암호로 로그인합니다.
 - 사용자 이름: `root`
기본 사용자 이름은 변경할 수 없습니다.
 - 암호: `your_password`

중요 Orchestrator Appliance의 루트 계정에 대한 암호는 365일 후에 만료됩니다. Orchestrator Appliance에 루트로 로그인하고 `passwd -x number_of_days name_of_account`를 실행하여 계정에 대한 만료 시간을 늘릴 수 있습니다. Orchestrator Appliance 루트 암호의 만료 시간을 무한대로 늘리려면 `passwd -x 99999 root`를 실행합니다.

제어 센터에 로그인했습니다.

Orchestrator 네트워크 포트

Orchestrator는 다른 시스템과 통신하기 위해 특정 포트를 사용합니다. 포트는 변경할 수 없는 기본값으로 설정되어 있습니다.

기본 구성 포트

Orchestrator 서비스를 제공하려면 기본 포트를 설정하고 방화벽이 수신되는 TCP 연결을 허용하도록 구성해야 합니다.

참고 기타 포트는 사용자 지정 플러그인을 사용하면 필요할 수 있습니다.

표 5-1. VMware vRealize Orchestrator 기본 구성 포트

포트	번호	프로토콜	소스	대상	설명
HTTP 서버 포트	8280	TCP	최종 사용자 웹 브라우저	Orchestrator 서버	Orchestrator 기본 HTTP 웹 포트 8280으로 전송된 요청은 기본 HTTPS 웹 포트 8281로 리디렉션됩니다.
HTTPS 서버 포트	8281	TCP	최종 사용자 웹 브라우저	Orchestrator 서버	Web Orchestrator 홈 페이지의 액세스 포트.
웹 구성 HTTPS 액세스 포트	8283	TCP	최종 사용자 웹 브라우저	Orchestrator 구성	Orchestrator 구성의 웹 UI에 대한 SSL 액세스 포트.

외부 통신 포트

Orchestrator가 외부 서비스와 통신할 수 있도록 방화벽이 송신 연결을 허용하도록 구성해야 합니다.

표 5-2. VMware vRealize Orchestrator 외부 통신 포트

포트	번호	프로토콜	소스	대상	설명
LDAP	389	TCP	Orchestrator 서버	LDAP 서버	LDAP 인증 서버의 조회 포트입니다. 참고 LDAP 인증은 사용되지 않으며 향후 버전에서 지원되지 않습니다.
SSL을 사용하는 LDAP	636	TCP	Orchestrator 서버	LDAP 서버	보안 LDAP 인증 서버의 조회 포트.
글로벌 카탈로그를 사용하는 LDAP	3268	TCP	Orchestrator 서버	글로벌 카탈로그 서버	Microsoft 글로벌 카탈로그 서버 쿼리가 전달되는 포트.
vCenter Single Sign-On 서버	7444	TCP	Orchestrator 서버	vCenter Single Sign-On 서버	vCenter Single Sign-On 5.5를 사용해 vCenter Single Sign-On 인증(레거시) 을 구성할 때 vCenter Single Sign-On 서버와 통신하기 위해 사용되는 포트.
SQL Server	1433	TCP	Orchestrator 서버	Microsoft SQL Server	Orchestrator 데이터베이스로 구성된 Microsoft SQL Server 인스턴스와 통신하기 위해 사용되는 포트.
PostgreSQL	5432	TCP	Orchestrator 서버	PostgreSQL 서버	Orchestrator 데이터베이스로 구성된 PostgreSQL Server와 통신하기 위해 사용되는 포트.
Oracle	1521	TCP	Orchestrator 서버	Oracle DB 서버	Orchestrator 데이터베이스로 구성된 Oracle 데이터베이스 서버와 통신하기 위해 사용되는 포트.
SMTP 서버 포트	25	TCP	Orchestrator 서버	SMTP 서버	이메일 알림을 위해 사용되는 포트.
vCenter Server API 포트	443	TCP	Orchestrator 서버	vCenter Server	오케스트레이션된 vCenter Server 인스턴스에서 가상 인프라 및 가상 시스템 정보를 얻기 위해 Orchestrator가 사용하는 vCenter Server API 통신 포트.

인증 유형 선택

사용자 권한이 올바르게 작동되고 이를 관리하려면 Orchestrator 사용 시 인증 방법이 필요합니다.

Orchestrator는 다음 유형의 인증을 지원합니다.

LDAP 인증

Orchestrator가 작업 중인 LDAP 서버에 연결합니다.

참고 LDAP 인증은 사용되지 않으며 향후 버전에서 지원되지 않습니다.

vRealize Automation 인증

Orchestrator가 vRealize Automation 구성 요소 레지스트리를 통해 인증됩니다.

vSphere 인증

Orchestrator가 Platform Services Controller를 통해 인증됩니다.

vCenter Single Sign-On 인증(레거시)

필수 인증 제공자가 vCenter Single Sign-On 5.5인 경우에만 이 인증 모드를 사용합니다.

Orchestrator Appliance를 다운로드하고 배포하면 Orchestrator 서버는 장치에 포함된 ApacheDS LDAP 디렉토리 서비스와 함께 작동하도록 사전 구성됩니다. 그러나 vRealize Automation, vSphere 또는 SSO(레거시)를 통해 인증하도록 Orchestrator를 미리 구성한 경우 LDAP 옵션은 더 이상 **인증 모드** 드롭다운 메뉴에서 표시되지 않습니다.

중요 vSphere 인벤토리 개체를 관리하기 위해 vSphere Web Client를 통해 Orchestrator를 사용하려면 Orchestrator를 구성하여 vCenter Server 및 vSphere Web Client 모두가 연결된 동일한 플랫폼 서비스 컨트롤러와 함께 작동하도록 해야 합니다.

LDAP 설정 구성

사용자를 인증하고 권한을 관리하기 위해 인프라의 작업 LDAP 서버에 연결하도록 Orchestrator를 구성할 수 있습니다.

참고 LDAP 인증은 사용되지 않으며 향후 버전에서 지원되지 않습니다.

보안 SSL을 통한 LDAP, Windows Server 2008 또는 2012 및 AD를 사용하는 경우 **LDAP 서버 서명 요구 사항** 그룹 정책이 LDAP 서버에서 비활성화되어 있는지 확인합니다.

중요 같은 트리에 있지 않지만 양방향 신뢰를 갖는 멀티 도메인은 지원되지 않고 Orchestrator에서 작동하지 않습니다. 멀티 도메인 Active Directory를 지원하는 구성만 도메인 트리에 해당합니다. 포리스트와 외부 트러스트가 지원되지 않습니다.

1 LDAP 서버 SSL 인증서 가져오기(32 페이지)

LDAP 서버가 SSL을 사용하는 경우 SSL 인증서 파일을 제어 센터로 가져와 Orchestrator와 LDAP 간 보안 연결을 설정할 수 있습니다.

2 LDAP 인증 구성(33 페이지)

Orchestrator를 디렉토리 서버 인스턴스에 연결하려면 LDAP 서버의 호스트, 포트 및 검색 기본을 제공하여 연결 URL을 생성해야 합니다. 또한 사용자 자격 증명, 사용자, 그룹 조회 경로를 제공하여 LDAP 사용자가 Orchestrator 클라이언트에 대해 인증할 수 있도록 해야 합니다.

3 일반 Active Directory LDAP 오류(35 페이지)

LDAP:오류 코드 49 에러 메시지가 표시되고 LDAP 인증 서버 연결에 문제가 발생하면 어떤 LDAP 기능에서 문제가 발생하는지 파악할 수 있습니다.

LDAP 서버 SSL 인증서 가져오기

LDAP 서버가 SSL을 사용하는 경우 SSL 인증서 파일을 제어 센터로 가져와 Orchestrator와 LDAP 간 보안 연결을 설정할 수 있습니다.

제어 센터의 **인증서** 페이지에서 LDAP SSL 인증서를 가져올 수 있습니다.

필수 조건

- LDAP 서버, Windows Server 2008, Windows Server 2012 및 Active Directory를 사용하는 경우 **LDAP 서버 서명 요구 사항** 그룹 정책이 LDAP 서버에서 비활성화되어 있는지 확인하십시오.
- 자체 서명된 서버 인증서 또는 인증 기관에서 서명한 인증서를 가져옵니다.
- SSL 액세스를 위해 LDAP 서버를 구성합니다. LDAP 서버 설명서의 지침을 참조하십시오.
- 신뢰할 수 있는 인증서를 명확하게 지정하여 SSL 권한 부여를 올바르게 수행하십시오.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **인증서**를 클릭합니다.

- 3 신뢰할 수 있는 인증서 탭에서 가져오기를 클릭합니다.
- 4 URL 또는 파일에서 LDAP SSL 인증서를 로드합니다.

옵션	작업
URL 또는 프록시 URL에서 가져오기	LDAP 서버의 URL 입력: <code>https://your_LDAP_server_IP_address</code> 또는 <code>your_LDAP_server_IP_address:port</code>
파일에서 가져오기	LDAP SSL 인증서 파일을 열고 이를 찾아 가져옵니다.

- 5 가져오기를 클릭합니다.

가져오기가 완료되었음을 확인하는 메시지가 나타납니다.

가져온 인증서는 신뢰할 수 있는 SSL 인증서 목록에 표시됩니다. Orchestrator와 LDAP 서버 간 보안 연결이 활성화됩니다.

후속 작업

LDAP 연결 URL을 생성하는 경우 제어 센터의 **인증 제공자 구성** 페이지에서 SSL을 활성화해야 합니다.

LDAP 인증 구성

Orchestrator를 디렉토리 서버 인스턴스에 연결하려면 LDAP 서버의 호스트, 포트 및 검색 기본을 제공하여 연결 URL을 생성해야 합니다. 또한 사용자 자격 증명, 사용자, 그룹 조회 경로를 제공하여 LDAP 사용자가 Orchestrator 클라이언트에 대해 인증할 수 있도록 해야 합니다.

지원되는 디렉토리 서비스 유형은 LDAP 및 OpenLDAP 기반 디렉토리 서비스를 통한 Active Directory입니다.

참고 워크플로 또는 작업에 대한 액세스 권한을 Orchestrator 개체에 할당한 후 LDAP 서버 또는 디렉토리 서비스 유형을 변경하면 이러한 권한을 다시 설정해야 합니다.

사용자 정보를 수집하고 저장하는 사용자 지정 애플리케이션을 구성한 후 LDAP 설정을 변경하면 새 LDAP 데이터베이스에서 사용될 때 인증 기록은 유효하지 않습니다.

필수 조건

상세한 설정 정보를 사용하여 LDAP 인증을 구성합니다. **“LDAP 인증 설정,”** (34 페이지) 항목을 참조하십시오.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **인증 제공자 구성**을 클릭합니다.
- 3 **인증 모드** 드롭다운 메뉴에서 **LDAP 인증**을 선택합니다.
- 4 **LDAP 클라이언트** 드롭다운 메뉴에서 사용하려는 디렉토리 서버의 유형을 선택합니다.
- 5 사용 중인 환경에서 LDAP 서버를 구성합니다.
- 6 **변경 내용 저장**을 클릭합니다.
- 7 **로그인 테스트**에 LDAP 사용자의 자격 증명을 입력하여 해당 사용자가 Orchestrator 클라이언트에 액세스할 수 있는지 테스트합니다.

성공적으로 로그인한 후 시스템은 사용자가 Orchestrator 관리자 그룹에 포함되는지 여부를 확인합니다.

후속 작업

데이터베이스를 구성합니다. 자세한 내용은 [“Orchestrator 데이터베이스 연결 구성,”](#) (38 페이지) 항목을 참조하십시오.

LDAP 인증 설정

Orchestrator와 디렉토리 서버를 성공적으로 연결하려면 특정 LDAP 서버 설정과 일치하도록 LDAP 인증 설정을 구성해야 합니다.

표 5-3. LDAP 인증 옵션

옵션	설명
기본 LDAP 호스트	제어 센터가 사용자 자격 증명을 확인하는 첫 번째 호스트의 IP 주소 또는 DNS 이름입니다.
보조 LDAP 호스트	기본 LDAP 호스트가 사용할 수 없는 상태인 경우 제어 센터가 사용자 자격 증명을 확인하는 호스트의 IP 주소 또는 DNS 이름입니다.
포트	LDAP 서버의 조회 포트 값입니다. 참고 Orchestrator는 Active Directory 계층 도메인 구조를 지원합니다. 도메인 컨트롤러가 글로벌 카탈로그를 사용하도록 구성되어 있는 경우 포트 3268을 사용해야 합니다. 기본 포트 389는 글로벌 카탈로그 서버에 연결하는 데 사용할 수 없습니다.
루트	루트 네임스페이스의 컨테이너입니다. 도메인 이름이 company.org이면 루트 컨테이너는 dc=company,dc=org 입니다. 참고 크기가 큰 서비스 디렉토리의 성능을 향상하기 위해 트리 구조에서 특정 컨테이너를 정의하여 검색 기준을 좁힐 수 있습니다. 예를 들어, 전체 디렉토리를 검색하지 않고 ou=employees,dc=company,dc=org 로 지정할 수 있습니다. 이 검색 필터는 직원 조직 구성 단위에서 모든 사용자를 반환합니다. 필수 텍스트 상자에 입력한 값은 다음 LDAP 연결 URL을 생성합니다. <code>ldap://DomainController:389/ou=employees,dc=company,dc=org</code>
SSL 사용	이 옵션을 사용하는 경우 Orchestrator와 LDAP 간의 연결은 암호화됩니다. 참고 LDAP가 SSL을 사용하는 경우 먼저 SSL 인증서를 가져오고 Orchestrator 서버 서비스를 다시 시작해야 합니다. “LDAP 서버 SSL 인증서 가져오기,” (32 페이지) 항목을 참조하십시오.
사용자 이름	디렉토리 트리를 찾을 수 있는 권한을 갖는 사용자 계정의 이름입니다. Active Directory에서 다음 형식 중 하나로 사용자 이름을 지정할 수 있습니다. <ul style="list-style-type: none"> ■ 기본 사용자 이름(예: user) ■ 고유 이름(예: cn=user,ou=employees,dc=company,dc=org) ■ 사용자 계정 이름(예: user@company.org)
암호	디렉토리 트리를 찾을 수 있는 권한을 갖는 사용자 계정의 암호입니다.
사용자 조회 기본	Orchestrator가 잠재적 사용자를 검색하는 LDAP 컨테이너 또는 조직 구성 단위입니다.
관리 그룹	관리 그룹은 Orchestrator에 대한 관리 권한을 부여하는 LDAP 그룹이어야 합니다. 예를 들어, Domain Admins 입니다.

표 5-3. LDAP 인증 옵션 (계속)

옵션	설명
요청 시간 초과	Orchestrator 서버가 서비스 디렉토리로 쿼리를 보내고 응답을 기다리는 시간을 결정하는 밀리초 단위 값입니다. 시간 초과 기간이 경과하면 이 값을 수정하여 시간 초과가 Orchestrator 서버에서 발생하는지 여부를 확인합니다.
호스트 연결 가능 시간 초과	대상 호스트에 대한 연결 확인을 위해 시간 초과 기간을 결정하는 밀리초 단위 값입니다.
링크 참조 해제	이 옵션을 선택하면 LDAP 서버는 사용자 별칭을 검색된 사용자 개체로 확인합니다.
필터 특성	LDAP 조회가 반환하는 LDAP 특성을 필터링합니다. 이 확인란을 선택하면 특정 특성을 반환하지 않아서 LDAP에서 검색 속도가 빨라집니다. 그러나 추후 자동화를 위해 추가로 몇 개의 LDAP 특성을 사용해야 할 수 있습니다.

일반 Active Directory LDAP 오류

LDAP:오류 코드 49 에러 메시지가 표시되고 LDAP 인증 서버 연결에 문제가 발생하면 어떤 LDAP 기능에서 문제가 발생하는지 파악할 수 있습니다.

표 5-4. 일반 Active Directory 인증 오류

오류	설명
525	사용자를 찾을 수 없습니다.
52e	사용자 자격 증명이 올바르지 않습니다.
530	사용자가 현재 로그인할 수 있도록 허용되지 않았습니다.
531	사용자가 해당 워크스테이션에 로그인할 수 있도록 허용되지 않았습니다.
532	암호가 만료되었습니다.
533	이 사용자 계정은 사용할 수 없습니다.
701	이 사용자 계정은 만료되었습니다.
773	사용자 암호를 다시 설정해야 합니다.
775	사용자 계정이 잠겼습니다.

vRealize Automation 인증 구성

vRealize Automation 구성 요소 레지스트리를 통해 인증하도록 Orchestrator를 구성할 수 있습니다.

필수 조건

vRealize Automation을 설치 및 구성하고 vRealize Automation 서버가 실행되고 있는지 확인합니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **인증 제공자 구성**을 클릭합니다.
- 3 **인증 모드** 드롭다운 메뉴에서 **vRealize Automation**을 선택합니다.
- 4 **호스트 주소** 텍스트 상자에서 vRealize Automation 호스트 주소를 입력하고 **연결**을 클릭합니다.

- 5 **인증서 수락**을 클릭합니다.
- 6 **사용자 이름** 및 **암호** 텍스트 상자에서 vRealize Automation 관리자 계정의 자격 증명을 입력합니다.
계정은 임시적인 솔루션으로 Orchestrator를 등록 또는 제거하는 데만 사용됩니다.
- 7 (선택 사항) **라이선스 구성** 확인란을 선택합니다.
- 8 **등록**을 클릭합니다.
- 9 **기본 테넌트** 텍스트 상자에 기본 도메인을 입력하여 도메인 이름 없이 로그인하는 사용자를 인증합니다. 기본값은 `vsphere.local`입니다.
- 10 **관리자 그룹** 텍스트 상자에서 관리자 그룹을 입력하고 **검색**을 클릭합니다.
- 11 관리자 그룹을 선택합니다.
- 12 **변경 내용 저장**을 클릭합니다.
성공적으로 저장했다는 메시지가 표시됩니다.

후속 작업

변경 내용이 적용되도록 제어 센터의 시작 옵션 페이지에서 Orchestrator 서버를 다시 시작합니다.

vCenter Single Sign-On 설정 구성

VMware vCenter Single Sign-On은 중재 인증 아키텍처 패턴을 구현하는 인증 서비스입니다. Orchestrator를 구성하여 Platform Services Controller 서버를 실행 중인 vCenter Single Sign-On 인스턴스에 연결할 수 있습니다.

vCenter Single Sign-On 서버는 보안 토큰 서비스(STS)라는 인증 인터페이스를 제공합니다. 클라이언트가 STS로 인증 메시지를 보내면 STS는 사용자 자격 증명을 ID 소스 중 하나와 비교하여 확인합니다. 성공적으로 인증되면 STS는 토큰을 생성합니다.

Platform Services Controller에는 vSphere Web Client의 일부인 vCenter Single Sign-On 관리 인터페이스가 포함되어 있습니다. vCenter Single Sign-On을 구성하고 vCenter Single Sign-On 사용자 및 그룹을 관리하려면 vSphere Web Client에 vCenter Single Sign-On 관리자 권한 사용자로 로그인합니다. 이 사용자는 vCenter Server 관리자와 다른 사용자일 수도 있습니다. vSphere Web Client 로그인 페이지에서 자격 증명을 제공해야 vCenter Single Sign-On 관리 도구에 액세스하여 사용자를 생성하고 다른 사용자에게 관리자 권한을 할당할 수 있습니다.

vSphere Web Client 사용 시 vSphere Web Client 로그인 페이지에서 자격 증명을 제공하여 vCenter Single Sign-On에 인증합니다. 그러면 사용 권한을 가지고 있는 모든 vCenter Server 인스턴스를 모두 볼 수 있습니다. vCenter Server에 연결된 후에는 추가 인증이 필요하지 않습니다. 개체에서 수행할 수 있는 작업은 해당 개체에 대한 사용자의 vCenter Server 사용 권한에 따라 다릅니다.

Platform Services Controller에 대한 자세한 내용은 vSphere 보안을 참조하십시오.

vCenter Single Sign-On을 통해 인증하도록 Orchestrator를 구성한 후 동일한 vCenter Single Sign-On 인스턴스를 사용하여 vSphere Web Client에 등록된 vCenter Server 인스턴스를 사용할 수 있도록 구성합니다.

vSphere Web Client에 로그인하면 Orchestrator 웹 플러그인은 로그인에 사용된 사용자 프로파일을 대신하여 Orchestrator 서버와 통신합니다.

vSphere Platform Services Controller를 통한 인증 구성

제어 센터에서 vSphere 인증 모드를 사용하여 vCenter Single Sign-On 서버로 Orchestrator 서버를 등록합니다. vCenter Single Sign-On 인증을 vCenter Server 6.0 이상과 함께 사용합니다.

필수 조건

VMware vCenter Single Sign-On을 설치 및 구성하고 vCenter Single Sign-On 서버가 실행되고 있는지 확인합니다.

중요 Orchestrator 서버의 시계와 vCenter Server 장치를 동기화해야 합니다. 그렇지 않으면 복잡한 vCenter Single Sign-On 오류가 발생할 수 있습니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **인증 제공자 구성**을 클릭합니다.
- 3 **인증 모드** 드롭다운 메뉴에서 **vSphere**를 선택합니다.
- 4 **호스트 주소** 텍스트 상자에서 Platform Services Controller 호스트 주소를 입력하고 **연결**을 클릭합니다.
- 5 **인증서 수락**을 클릭합니다.
- 6 **사용자 이름** 및 **암호** 텍스트 상자에서 vCenter Single Sign-On 관리자 계정의 자격 증명을 입력합니다.
계정은 임시적인 솔루션으로 Orchestrator를 등록 또는 제거하는 데만 사용됩니다.
- 7 (선택 사항) **라이선스 구성** 확인란을 선택합니다.
- 8 **등록**을 클릭합니다.
- 9 **기본 테넌트** 텍스트 상자에 기본 도메인을 입력하여 도메인 이름 없이 로그인하는 사용자를 인증합니다. 기본값은 **vsphere.local**입니다.
- 10 **관리자 그룹** 텍스트 상자에서 관리자 그룹을 입력하고 **검색**을 클릭합니다.
- 11 **변경 내용 저장**을 클릭합니다.
성공적으로 저장했다는 메시지가 표시됩니다.

Orchestrator를 vCenter Single Sign-On으로 성공적으로 등록했습니다.

Orchestrator를 vCenter Single Sign-On(레거시) 솔루션으로 등록

제어 센터에서 Single Sign-On 레거시 인증 모드를 사용하여 Orchestrator 서버를 vCenter Single Sign-On 서버로 등록할 수 있습니다. Single Sign-On 레거시 인증은 vCenter Server 버전 5.5 및 업데이트 2로 시작하는 해당 업데이트 릴리스만 함께 사용합니다.

필수 조건

VMware vCenter Single Sign-On을 설치 및 구성하고 vCenter Single Sign-On 서버가 실행되고 있는지 확인합니다.

중요 Orchestrator 서버의 시계와 vCenter Server 장치를 동기화해야 합니다. 그렇지 않으면 복잡한 vCenter Single Sign-On 오류가 발생할 수 있습니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.

- 2 인증 제공자 구성을 클릭합니다.
- 3 인증 모드 드롭다운 메뉴에서 **SSO(레거시)**를 선택합니다.
- 4 **STS URL** 텍스트 상자에서 vCenter Single Sign-On 토큰 서비스 인터페이스의 URL을 입력합니다.
`https://your_vcenter_single_sign_on_server:7444/sts/STSService/vsphere.local`
- 5 **관리 URL** 텍스트 상자에서 vCenter Single Sign-On 관리 서비스 인터페이스의 URL을 입력합니다.
`https://your_vcenter_single_sign_on_server:7444/sso-adminserver/sdk/vsphere.local`
- 6 연결을 클릭합니다.
- 7 인증서 수락을 클릭합니다.
- 8 **사용자 이름 및 암호** 텍스트 상자에서 vCenter Single Sign-On 관리자의 자격 증명을 입력합니다.
 계정은 임시적인 솔루션으로 Orchestrator를 등록 또는 제거하는 데만 사용됩니다.
- 9 등록을 클릭합니다.
- 10 **기본 테넌트** 텍스트 상자에 기본 도메인을 입력하여 도메인 이름 없이 로그인하는 사용자를 인증합니다. 기본값은 `vsphere.local`입니다.
- 11 **관리자 그룹** 텍스트 상자에서 관리자 그룹을 입력하고 **검색**을 클릭합니다.
- 12 **변경 내용 저장**을 클릭합니다.
 성공적으로 저장했다는 메시지가 표시됩니다.

Orchestrator를 vCenter Single Sign-On으로 성공적으로 등록했습니다.

Orchestrator 데이터베이스 연결 구성

Orchestrator 서버에는 데이터 저장을 위한 데이터베이스가 필요합니다.

Orchestrator Appliance를 다운로드하고 배포하면 Orchestrator 서버는 해당 장치에 사전 설치된 PostgreSQL 데이터베이스와 작동하도록 구성됩니다.

사전 구성된 Orchestrator PostgreSQL 데이터베이스는 즉시 사용 가능합니다. 고부하 운영 환경에서 보다 나은 성능을 구현하려면 개별 관계형 데이터베이스 관리 시스템(RDBMS)을 설치하고 Orchestrator용 데이터베이스를 생성합니다. Orchestrator용 데이터베이스 생성에 대한 자세한 내용은 **“Orchestrator 데이터베이스 설정,”** (20 페이지)을 참조하십시오. Orchestrator를 외부 데이터베이스와 함께 사용하려면 원격 연결용 데이터베이스를 구성하십시오.

데이터베이스 SSL 인증서 가져오기

데이터베이스가 SSL을 사용하는 경우 SSL 인증서를 제어 센터로 가져와 Orchestrator와 데이터베이스 간 보안 연결을 설정해야 합니다.

필수 조건

- SSL 액세스를 위한 데이터베이스를 구성합니다. 데이터베이스 설명서의 지침을 참조하십시오.
- 자체 서명된 서버 인증서 또는 인증 기관에서 서명한 인증서를 가져옵니다.
- 신뢰할 수 있는 인증서를 명확하게 지정하여 SSL 권한 부여를 올바르게 수행하십시오.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.

- 2 인증서를 클릭합니다.
- 3 신뢰할 수 있는 인증서 탭에서 가져오기를 클릭합니다.
- 4 URL 또는 파일에서 데이터베이스 SSL 인증서를 로드합니다.

옵션	작업
URL 또는 프록시 URL에서 가져오기	데이터베이스 서버의 URL 입력: <code>https://your_database_server_IP_address</code> 또는 <code>your_database_server_IP_address:port</code>
파일에서 가져오기	데이터베이스 SSL 인증서 파일을 얻고 이를 찾아 가져옵니다.

가져온 인증서는 신뢰할 수 있는 SSL 인증서 목록에 표시됩니다. Orchestrator와 데이터베이스 간 보안 연결이 활성화됩니다.

후속 작업

데이터베이스 연결을 구성하는 경우 제어 센터의 **데이터베이스 구성** 페이지에서 SSL을 활성화해야 합니다.

데이터베이스 연결 구성

Orchestrator 데이터베이스에 대한 연결을 설정하려면 데이터베이스 연결 매개 변수를 설정해야 합니다.

필수 조건

- Orchestrator 서버에서 사용할 새 데이터베이스를 설정합니다. [“Orchestrator 데이터베이스 설정,”](#) (20 페이지) 항목을 참조하십시오.
- 동적 포트를 사용하도록 구성된 SQL Server 데이터베이스를 사용하는 경우 SQL Server Browser 서비스가 실행 중인지 확인합니다.
- Microsoft SQL Server 데이터베이스 사용 시 트랜잭션 교착 상태를 방지하려면 ALLOW_SNAPSHOT_ISOLATION 및 READ_COMMITTED_SNAPSHOT 데이터베이스 옵션을 활성화해야 합니다.
- Microsoft SQL Server 데이터베이스가 동적 포트를 사용하는 경우 SQL Server 브라우저가 실행되고 있는지 확인하십시오.
- Oracle 데이터베이스를 사용할 때 ORA-01450 오류를 방지하려면 데이터베이스 블록 크기를 올바르게 구성했는지 확인합니다. 필요한 최소 크기는 Oracle 데이터베이스 인덱스에서 사용 중인 블록 크기에 따라 다릅니다.
- Oracle 데이터베이스에 문자를 올바른 형식으로 저장하려면 데이터베이스 연결을 구성하고 Orchestrator의 테이블 구조를 빌드하기 전에 NLS_CHARACTER_SET 매개 변수를 AL32UTF8로 설정해야 합니다. 이 설정은 다국어 환경에서 매우 중요합니다.
- 보안 연결을 통해 데이터베이스와 통신하도록 Orchestrator를 구성하려면 데이터베이스 SSL 인증서를 가져와야 합니다. 자세한 내용은 [“데이터베이스 SSL 인증서 가져오기,”](#) (38 페이지) 항목을 참조하십시오.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **데이터베이스 구성**을 클릭합니다.

- 3 **데이터베이스 유형** 드롭다운 메뉴에서 Orchestrator 서버에서 사용할 데이터베이스 유형을 선택합니다.

옵션	설명
Oracle	Oracle 데이터베이스 인스턴스와 함께 작동하도록 Orchestrator를 구성합니다.
SQL Server	Microsoft SQL Server 데이터베이스 인스턴스와 함께 작동하도록 Orchestrator를 구성합니다.
PostgreSQL	PostgreSQL 데이터베이스 인스턴스와 함께 작동하도록 Orchestrator를 구성합니다.
처리 중인 DerbyDB	처리 중인 DerbyDB 데이터베이스와 함께 작동하도록 Orchestrator를 구성합니다. 참고 DerbyDB를 사용해서는 안 됩니다.

- 4 데이터베이스 연결 매개 변수를 입력하고 **변경 내용 저장**을 클릭합니다.

옵션	설명
서버 주소	데이터베이스 서버 IP 주소 또는 DNS 이름입니다. 이 옵션은 모든 데이터베이스에 적용됩니다.
포트	데이터베이스 서버 포트는 데이터베이스와 통신하는 데 사용됩니다. 이 옵션은 모든 데이터베이스에 적용됩니다.
SSL 사용	데이터베이스에 대한 SSL 연결을 사용하려면 SSL 사용 을 선택합니다. 이 옵션을 사용하려면 데이터베이스 SSL 인증서를 Orchestrator로 가져와야 합니다. 이 옵션은 모든 데이터베이스에 적용됩니다.
데이터베이스 이름	데이터베이스의 고유한 전체 이름입니다. 데이터베이스 이름은 초기화 매개 변수 파일의 SERVICE_NAMES 매개 변수에 지정됩니다. 이 옵션은 SQL Server 및 PostgreSQL 데이터베이스에만 유효합니다.
사용자 이름	Orchestrator에서 선택한 데이터베이스에 연결하고 데이터베이스를 운영하는 데 사용하는 사용자 이름입니다. 선택한 이름은 대상 데이터베이스에서 db_owner 권한이 있는 유효한 사용자여야 합니다. 이 옵션은 모든 데이터베이스에 적용됩니다.
암호	사용자 이름의 암호입니다. 이 옵션은 모든 데이터베이스에 적용됩니다.
인스턴스 이름(있는 경우)	데이터베이스 초기화 매개 변수 파일의 INSTANCE_NAME 매개 변수로 식별할 수 있는 데이터베이스 인스턴스의 이름입니다. 이 옵션은 SQL Server 및 Oracle 데이터베이스에만 유효합니다.
도메인	Windows 인증을 사용하려면 SQL Server 시스템의 도메인 이름을 입력합니다(예: company.org). SQL 인증을 사용하려면 이 텍스트 상자를 그대로 비워 둡니다. 이 옵션은 SQL Server에만 유효하며, Windows 인증을 사용할지 또는 SQL Server 인증을 사용할지 지정합니다.
Windows 인증 모드(NTLMv2) 사용	Windows 인증을 사용할 때 NTLMv2 응답을 전송하려면 선택합니다. 이 옵션은 SQL Server에만 유효합니다.

지정한 매개 변수가 올바른 경우 데이터베이스 연결에 성공했다는 메시지가 표시됩니다.

- 5 필요한 경우, Orchestrator에 대한 테이블 구조를 업데이트합니다.
6 **변경 내용 저장**을 클릭합니다.

데이터베이스 연결을 성공적으로 구성했습니다.

Orchestrator 데이터베이스 내보내기

서버 데이터베이스의 전체 백업된 아카이브를 생성합니다. Linux에서 실행 중인 PostgreSQL 데이터베이스만 내보낼 수 있습니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **데이터베이스 내보내기**를 클릭합니다.
- 3 데이터베이스와 함께 워크플로 토큰 및 로그 이벤트를 내보낼지 여부를 선택합니다.
- 4 **데이터베이스 내보내기**를 클릭합니다.

제어 센터는 Orchestrator 서버를 설치한 시스템에 `vco-db-dump-databaseName@hostname.gz` 파일을 생성합니다. 이 파일을 사용하여 시스템을 복제 및 복구할 수 있습니다.

Orchestrator 데이터베이스 가져오기

시스템 오류가 발생하는 경우 Orchestrator를 다시 설치한 후 이전에 내보낸 데이터베이스를 가져올 수 있습니다.

필수 조건

새 Orchestrator 데이터베이스는 비어 있어야 합니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **데이터베이스 가져오기**를 클릭합니다.
- 3 이전 설치에서 내보낸 `.gz` 파일을 찾아 선택합니다.
- 4 **데이터베이스 가져오기**를 클릭합니다.

데이터베이스를 성공적으로 가져왔다는 메시지가 표시됩니다. 새 시스템은 이전 시스템의 데이터베이스를 획득합니다.

인증서 관리

특정 서버용으로 발급되어 서버 공개 키에 대한 정보를 포함하는 인증서를 사용하여 Orchestrator에서 생성된 모든 요소에 서명하고 신뢰성을 보장할 수 있습니다. 클라이언트가 서버에서 일반적으로 패키지인 요소를 수신하면 클라이언트는 사용자의 ID를 확인하고 서명의 신뢰 여부를 결정합니다.

중요 Orchestrator가 포함된 Apache Derby 데이터베이스를 사용하면 서버 인증서를 변경할 수 없습니다.

Orchestrator 인증서 관리

제어 센터의 **인증서** 페이지에서 또는 Orchestrator 클라이언트를 통해 구성 워크플로 범주에서 SSL 신뢰 관리자 워크플로를 사용하여 Orchestrator 인증서를 관리할 수 있습니다.

인증서를 Orchestrator 신뢰 저장소에 가져오기

제어 센터는 vCenter Server, 관계형 데이터베이스 관리 시스템(RDBMS), LDAP, Single Sign-On 및 기타 서버와 통신하는 데 보안 연결을 사용합니다. URL 또는 PEM- 인코딩 파일에서 필수 SSL 인증서를 가져올 수 있습니다. 서버 인스턴스에 대해 SSL 연결을 사용할 때마다 **인증서** 페이지의 **신뢰할 수 있는 인증서** 탭에서 해당 인증서를 가져오고 해당 SSL 인증서를 가져와야 합니다.

Orchestrator에서 URL 주소 또는 PEM- 인코드 파일로부터 SSL 인증서를 로드할 수 있습니다.

옵션	설명
URL 또는 프록시 URL에서 가져오기	원격 서버의 URL입니다. <code>https://your_server_IP_address</code> 또는 <code>your_server_IP_address:port</code>
파일에서 가져오기	PEM- 인코드 인증서 파일의 경로입니다. PEM- 인코드 인증서 파일 가져오기에 대한 자세한 정보는 “제어 센터를 통해 신뢰할 수 있는 인증서 가져오기,” (43 페이지)를 참조하십시오.

자체 서명된 서버 인증서 생성

Orchestrator Appliance는 장치의 네트워크 설정을 기준으로 자동 생성되고 자체 서명된 SSL 인증서를 포함합니다. 장치의 네트워크 설정이 변경된 경우 수동으로 자체 서명된 새 인증서를 생성해야 합니다. 자체 서명된 인증서를 생성하여 암호화된 통신을 보장하고 패키지에 서명을 제공할 수 있습니다. 그러나, 수신자는 사용자로 할당된 타사 제공자가 아니라 사용자의 서버에 의해 실제로 발급되고 자체 서명된 패키지인지 확인할 수 없습니다. 서버 ID를 증명하려면 CA(인증 기관)에 의해 서명된 인증서를 사용합니다.

제어 센터 인증서 페이지의 **Orchestrator 서버 SSL 인증서** 탭에서 자체 서명된 인증서를 생성할 수 있습니다.

옵션	설명
서명 알고리즘	디지털 서명을 생성하는 암호화 알고리즘입니다.
일반 이름	Orchestrator 서버의 호스트 이름입니다.
조직	조직의 이름입니다. (예: VMware)
조직 구성 단위	조직 구성 단위의 이름입니다. (예: R&D)
국가 코드	국가 코드 약어입니다. (예: US)

Orchestrator는 사용 중인 환경에 대한 고유한 서버 인증서를 생성합니다. 인증서의 공개 키에 대한 세부 정보가 **Orchestrator 서버 SSL 인증서** 탭에 표시됩니다. 개인 키는 Orchestrator 데이터베이스의 vmo_keystore 테이블에 저장됩니다.

Orchestrator 서버 SSL 인증서 가져오기

vRealize Orchestrator는 SSL 인증서를 사용하여 보안 통신 중 클라이언트와 원격 서버에 대해 자체 시스템을 식별합니다. 기본적으로 Orchestrator는 장치의 네트워크 설정을 기준으로 자동 생성되고 자체 서명된 SSL 인증서를 포함합니다. CA(인증 기관)에 의해 서명된 SSL 인증서를 가져와서 인증서 신뢰 오류를 방지할 수 있습니다.

CA(인증 기관)에 의해 서명된 인증서를 공개 키 및 개인 키를 포함하는 PEM- 인코드 파일로 가져와야 합니다.

패키지 서명 인증서

Orchestrator 서버에서 내보낸 패키지는 디지털로 서명되어 있습니다. 패키지 서명에 사용될 새 인증서를 가져오고, 내보내고 또는 생성합니다. 패키지 서명 인증서는 암호화된 통신 및 Orchestrator 패키지 서명을 보장하는 데 사용되는 디지털 ID 양식입니다.

Orchestrator Appliance는 장치의 네트워크 설정을 기준으로 자동 생성된 패키지 서명 인증서를 포함합니다. 장치의 네트워크 설정이 변경된 경우 수동으로 새 패키지 서명 인증서를 생성해야 합니다.

참고 Orchestrator Appliance는 초기 Orchestrator 구성 중 자동 생성되고 자체 서명된 패키지 서명 인증서를 포함합니다. 패키지 서명 인증서를 변경할 수 있으며 변경 후에 내보내는 모든 패키지는 새 인증서로 서명됩니다.

제어 센터를 통해 신뢰할 수 있는 인증서 가져오기

기타 서버와 안전하게 통신하려면 Orchestrator 서버가 기타 서버의 ID를 확인할 수 있어야 합니다. 이를 위해 원격 엔티티의 SSL 인증서를 Orchestrator 신뢰 저장소로 가져와야 할 수 있습니다. 인증서를 신뢰하기 위해 특정 URL에 대한 연결을 설정하는 방법으로 인증서를 신뢰 저장소로 가져오거나 PEM-인코드 파일 형태로 직접 가져올 수 있습니다.

필수 조건

SSL을 통해 Orchestrator를 연결할 서버의 정규화된 도메인 이름을 찾습니다.

프로시저

- 1 SSH를 통해 Orchestrator Appliance에 **루트로** 로그인합니다.
- 2 다음 명령을 실행하여 원격 서버의 인증서를 검색합니다.

```
openssl s_client -connect host_or_dns_name:secure_port
```

 - a 암호화되지 않은 포트를 사용하는 경우, starttls 및 필수 프로토콜을 openssl 명령과 함께 사용합니다.

```
openssl s_client -connect host_or_dns_name:25 -starttls smtp
```
- 3 -----BEGIN CERTIFICATE-----부터 -----END CERTIFICATE----- 태그까지의 텍스트를 텍스트 편집기에 복사하고 파일로 저장합니다.
- 4 제어 센터에 **루트로** 로그인합니다.
- 5 **인증서** 페이지로 이동합니다.
- 6 **신뢰할 수 있는 인증서** 탭에서 **가져오기**를 클릭하고 **PEM- 인코드 파일에서 가져오기** 옵션을 선택합니다.
- 7 인증서 파일을 찾아보고 **가져오기**를 클릭합니다.

원격 서버 인증서를 Orchestrator 신뢰 저장소로 성공적으로 가져왔습니다.

Orchestrator 플러그인 구성

기본 Orchestrator 플러그인은 워크플로를 통해서만 구성됩니다.

기본 Orchestrator 플러그인을 구성하려면 Orchestrator 클라이언트에서 특정 워크플로를 사용해야 합니다.

Orchestrator 플러그인 관리

제어 센터의 **플러그인 관리** 페이지에서 Orchestrator에 설치된 모든 플러그인 목록을 확인하고 기본 관리 작업을 수행할 수 있습니다.

플러그인 로깅 수준 변경

Orchestrator의 로깅 수준을 변경하는 대신 특정 플러그인에 대해서만 로깅 수준을 변경할 수 있습니다.

새 플러그인 설치

Orchestrator 플러그인을 사용하여 Orchestrator 서버를 다른 소프트웨어 제품과 통합할 수 있습니다. Orchestrator Appliance에는 사전 설치된 플러그인 집합이 포함되어 있으며, 사용자 지정 플러그인을 설치할 수도 있습니다.

모든 Orchestrator 플러그인은 제어 센터에서 설치됩니다. 사용할 수 있는 파일 확장명은 .vmoapp 및 .dar입니다. .vmoapp 파일은 여러 .dar 파일의 컬렉션을 포함할 수 있고 애플리케이션으로 설치될 수 있는 반면, .dar 파일은 하나의 플러그인과 연결된 모든 리소스를 포함합니다.

플러그인 사용 안 함

플러그인 이름 옆에 있는 **사용** 확인란을 선택 취소하여 플러그인을 사용하지 않도록 설정할 수 있습니다.

이 작업은 플러그인 파일을 제거하지 않습니다. Orchestrator에서 플러그인 설치 제거에 대한 자세한 내용은 [“플러그인 제거,”](#) (44 페이지)을 참조하십시오.

플러그인 제거

제어 센터를 사용하여 플러그인을 사용하지 않도록 설정할 수 있습니다. 이 작업을 수행해도 Orchestrator Appliance 파일 시스템에서 플러그인 파일이 제거되지는 않습니다. 플러그인 파일을 제거하려면 Orchestrator Appliance에 로그인하여 플러그인 파일을 수동으로 제거해야 합니다.

프로시저

- 1 Orchestrator Appliance에서 플러그인을 삭제합니다.
 - a SSH를 통해 Orchestrator Appliance에 **루트**로 로그인합니다.
 - b 텍스트 편집기를 사용하여 /etc/vco/app-server/plugins/_VSOPuginInstallationVersion.xml 파일을 엽니다.
 - c 제거할 플러그인에 해당하는 코드 행을 삭제합니다.
 - d /var/lib/vco/app-server/plugins 디렉토리로 이동합니다.
 - e 제거할 플러그인이 포함된 .dar 압축 파일을 삭제합니다.
- 2 vRealize Orchestrator 서비스를 다시 시작합니다.


```
service vco-configurator restart && service vco-server restart
```
- 3 제어 센터에 **루트**로 로그인합니다.
- 4 **플러그인 관리** 페이지에서 플러그인이 제거되었는지 확인합니다.
- 5 Orchestrator 클라이언트를 통해 플러그인과 관련된 패키지 및 폴더를 삭제합니다.
 - a Orchestrator 클라이언트에 로그인합니다.
 - b 왼쪽 상단의 드롭다운 메뉴에서 **디자인**을 선택합니다.
 - c **패키지 보기**를 클릭합니다.
 - d 삭제할 패키지를 마우스 오른쪽 버튼으로 클릭하고 **컨텐츠와 함께 요소 삭제**를 선택합니다.

참고 읽기 전용 상태로 잠겨 있는 Orchestrator 요소(예: 표준 라이브러리의 워크플로)는 삭제되지 않습니다.

- e 오른쪽 상단의 **도구** 메뉴에서 **사용자 기본 설정**을 선택합니다.

기본 설정 컨텍스트 메뉴가 열립니다.
- f **일반** 페이지에서 **비어 있지 않은 폴더 삭제 허용됨** 확인란을 선택합니다.

이제 한번의 클릭으로 하위 폴더 및 워크플로를 포함하여 전체 폴더를 삭제할 수 있습니다.

- g 워크플로 보기를 클릭합니다.
 - h 제거할 플러그인의 폴더를 삭제합니다.
 - i **작업** 보기를 클릭합니다.
 - j 제거할 플러그인의 작업 모듈을 삭제합니다.
- 6 vRealize Orchestrator 서비스를 다시 시작합니다.

플러그인과 관련된 모든 사용자 지정 워크플로, 작업, 정책, 구성, 설정 및 리소스를 제거했습니다.

Orchestrator 시작 옵션

제어 센터의 **시작 옵션** 페이지에서 Orchestrator 서버 서비스를 시작, 중지 및 다시 시작할 수 있습니다.

처음 Orchestrator를 시작하면 서버가 데이터베이스 테이블에 있는 Orchestrator 플러그인 콘텐츠를 설치하기 때문에 5~10분 정도 소요됩니다.

시작 옵션 페이지는 vco-server 서비스의 상태를 표시합니다.

상태	설명
실행 중	Orchestrator 서버 서비스가 시작되었으며 올바르게 실행되고 있습니다.
정의되지 않음	Orchestrator 서버 서비스가 시작 중입니다.
중지됨	Orchestrator 서버 서비스가 실행되지 않고 있습니다.

Orchestrator 가용성 및 확장성

Orchestrator 서비스의 가용성을 높이려면 클러스터의 여러 Orchestrator 서버 인스턴스를 공유 데이터베이스와 함께 시작합니다. vRealize Orchestrator는 클러스터의 일부로 작동하도록 구성되지 않는 한 단일 인스턴스로 작동합니다.

Orchestrator 클러스터

동일한 서버 및 플러그인 구성을 지닌 여러 Orchestrator 서버 인스턴스는 클러스터에서 함께 작동하며 단일 데이터베이스를 공유합니다.

모든 Orchestrator 서버 인스턴스는 하트비트를 교환하며 서로 간에 통신합니다. 각 하트비트는 노드가 특정 시간 간격으로 클러스터의 공유 데이터베이스에 기록하는 타임 스탬프입니다. 네트워크 문제, 무응답 데이터베이스 서버 또는 과부하로 Orchestrator 클러스터 노드의 응답이 중지될 수 있습니다. 활성 Orchestrator 서버 인스턴스가 페일오버 시간 초과 기간 내에 하트비트를 보내지 못하면 응답 없음으로 간주됩니다. 페일오버 시간 초과는 페일오버 하트비트 수와 하트비트 간격 값을 곱한 값과 동일합니다. 이는 신뢰할 수 없는 노드에 대한 정의로 사용되고 사용 가능한 리소스 및 운영 로드 에 따라 사용자 지정할 수 있습니다.

데이터베이스와의 연결이 끊어지면 Orchestrator 노드는 대기 모드로 전환되고 데이터베이스 연결이 복구되기 전까지 해당 모드를 유지합니다. 클러스터의 다른 노드는 스크립팅 가능한 작업 또는 워크플로 호출과 같은 완료되지 않은 지난 항목에서 모든 중단된 워크플로를 재개하여 활성 작업을 제어합니다.

Orchestrator는 클러스터 상태 모니터링 및 페일오버 알림을 전송하는 내장된 도구를 제공하지 않습니다. 로드 밸런서와 같은 외부 구성 요소를 사용하여 클러스터 상태를 모니터링할 수 있습니다. 노드가 실행 중인지 확인하려면 `https://your_orchestrator_server_IP_or_DNS_name:8281/vco/api/healthstatus` 페이지에서 상태 확인 REST API 서비스를 사용하여 노드의 상태를 확인할 수 있습니다.

중요 클러스터링된 환경에서는 여러 사용자의 워크플로 개발이 지원되지 않습니다. 다른 사용자가 클러스터 내의 다른 Orchestrator 노드를 사용하여 동일한 리소스를 수정하면 동시성 문제가 발생합니다. 클러스터에서 둘 이상의 활성 Orchestrator 서버 노드를 사용하려면 먼저 필요한 워크플로를 개발해야 합니다. 그런 다음 Orchestrator를 클러스터에서 작동하도록 설정할 수 있습니다.

Orchestrator 클러스터 구성

Orchestrator 서버 인스턴스의 클러스터를 생성하여 Orchestrator 서비스의 가용성을 높일 수 있습니다.

Orchestrator 클러스터는 하나의 데이터베이스를 공유하는 2개 이상의 Orchestrator 서버 인스턴스로 구성됩니다.

필수 조건

- 2개 이상의 Orchestrator 서버 인스턴스를 설치합니다.
- 공유 데이터베이스로 사용하려는 외부 데이터베이스가 다른 Orchestrator 인스턴스의 연결을 허용하도록 구성합니다.

Microsoft SQL Server 데이터베이스 사용 시 트랜잭션 교착 상태를 방지하려면 `ALLOW_SNAPSHOT_ISOLATION` 및 `READ_COMMITTED_SNAPSHOT` 데이터베이스 옵션을 활성화해야 합니다.

- Microsoft SQL Server 데이터베이스가 동적 포트를 사용하는 경우 SQL Server 브라우저가 실행되고 있는지 확인하십시오.
- Orchestrator 서버 인스턴스가 설치된 가상 시스템의 시계를 동기화합니다.

프로시저

- 1 첫 번째 Orchestrator 노드를 구성합니다.
 - a 첫 번째 Orchestrator 서버의 제어 센터에 **루트**로 로그인합니다.
 - b **시작 옵션** 페이지에서 Orchestrator 서버 서비스를 중지합니다.
 - c 외부 공유 데이터베이스의 연결을 구성합니다. 자세한 내용은 **“데이터베이스 연결 구성,”** (39 페이지) 항목을 참조하십시오.

인증서, 라이선싱, 인증 제공자 등 구성에 대한 변경 사항은 Orchestrator 인스턴스가 공유 데이터베이스를 사용할 수 있도록 구성된 후 수행되어야 합니다.
 - d 인증 제공자를 구성합니다. **“인증 유형 선택,”** (31 페이지) 항목을 참조하십시오.
 - e (선택 사항) 추가 시스템 속성을 설정합니다. 자세한 내용은 **11장, “시스템 속성 설정,”** (87 페이지) 항목을 참조하십시오.
 - f (선택 사항) **로그 통합** 페이지를 열고 원격 로그 서버를 사용하도록 Orchestrator를 구성합니다.

- g (선택 사항) **Orchestrator 클러스터 관리** 페이지의 **Orchestrator 노드 설정** 탭에서 Orchestrator 노드 설정에 대한 값을 제공하고 **저장**을 클릭합니다.

옵션	설명
활성 노드 개수	클러스터에 있는 활성 Orchestrator 서버 인스턴스의 최대 개수입니다. 활성 노드는 워크플로를 실행하고 클라이언트 요청에 응답하는 Orchestrator 서버 인스턴스입니다. 활성 Orchestrator 노드가 응답을 중지하면 비활성 Orchestrator 서버 인스턴스가 이를 대체합니다. 클러스터의 활성 Orchestrator 노드의 기본 개수는 1개입니다.
하트비트 간격(밀리초)	Orchestrator 노드가 실행 중임을 표시하기 위해 해당 노드에서 전송하는 두 개의 네트워크 하트비트 간의 밀리초 단위의 시간 간격입니다. 기본값은 12초입니다.
페일오버 하트비트 개수	Orchestrator 노드가 실패로 간주되기 전에 존재하지 않는 하트비트의 개수입니다. 기본값은 10개의 하트비트입니다.

기본 페일오버 시간 초과는 2분으로 기본 페일오버 하트비트 수와 하트비트 간격 기본값을 곱한 값과 동일합니다.

- h 제어 센터의 **구성 검증** 페이지에서 노드가 올바르게 구성되었는지 확인합니다.
- i (선택 사항) 외부 플러그인을 설치합니다.
- j 첫 번째 Orchestrator 노드에서 Orchestrator 서버 서비스를 시작합니다.
- k **시작 옵션** 페이지에서 **활성 구성 지문** 문자열 및 **보류 중인 구성 지문** 문자열이 일치하는지 확인합니다.

참고 두 문자열이 일치할 때까지 **시작 옵션** 페이지를 여러 번 새로 고침해야 할 수 있습니다.

- l (선택 사항) 외부 플러그인을 구성합니다.
- 2 Orchestrator 클러스터를 구성합니다.
- a 두 번째 Orchestrator 서버의 제어 센터에 **루트**로 로그인합니다.
- b **Orchestrator 클러스터 관리** 페이지에서 **노드를 클러스터에 조인** 탭을 클릭합니다.
- c **호스트 이름** 텍스트 상자에서 첫 번째 Orchestrator 서버 인스턴스의 호스트 이름 또는 IP 주소를 입력합니다.
- d **사용자 이름** 및 **암호** 텍스트 상자에서 제어 센터 자격 증명을 입력합니다.
- e **조인**을 클릭합니다.
- Orchestrator 인스턴스가 가입하는 노드의 구성을 복제합니다.

Orchestrator 인스턴스의 클러스터가 구성되었습니다.

후속 작업

Orchestrator 클러스터 관리 페이지의 **활성 노드 개수** 텍스트 상자에서 값을 변경하여 Orchestrator 서버 활성 노드를 클러스터에 추가할 수 있습니다.

Orchestrator 클러스터 모니터링 및 동기화

클러스터를 생성한 후 클러스터 노드의 상태를 모니터링하고 노드의 동기화를 유지하기 위한 추가 작업을 수행할 수 있습니다.

Orchestrator 클러스터 관리 페이지의 **Orchestrator 노드 설정** 탭에서 클러스터에 조인할 Orchestrator 인스턴스의 구성 동기화 상태를 확인할 수 있습니다.

중요 제어 센터는 클러스터의 다른 노드와 비교하여 로컬 노드의 상태를 보고합니다.

구성 동기화 상태	로컬 노드	원격 노드
동기화됨	로컬 노드의 구성은 마지막으로 다시 시작한 이래 변경되지 않았습니다.	원격 노드의 구성은 로컬 노드의 구성과 동일합니다.
노드를 다시 시작해야 합니다.	로컬 노드의 구성이 변경되었거나 원격 노드에서 복제되었습니다. 로컬 노드를 다시 시작하여 보류 중인 구성을 적용합니다.	원격 노드의 구성이 로컬 노드와 동기화되었으나 적용되지 않았습니다. 원격 노드를 다시 시작하여 구성을 적용합니다.
구성 동기화 필요	해당 없음	원격 노드의 활성 구성은 로컬 노드의 활성 구성과 다릅니다.
노드의 제어 센터를 사용할 수 없음	해당 없음	원격 노드의 제어 센터 서비스(vco-configurator)가 중지되었거나 연결되지 않습니다. 동기화 상태를 검색할 수 없습니다.
사용할 수 없음 로컬 노드 누락	로컬 노드가 클러스터 노드 목록에 없습니다. 로컬 노드의 동기화 상태를 검색할 수 없습니다.	해당 없음

구성 푸시 및 노드 다시 시작

로컬 노드의 구성을 변경하는 경우 **구성 푸시 및 노드 다시 시작** 드롭다운 메뉴 옵션을 사용하여 로컬 노드 구성을 클러스터의 모든 다른 노드에 복사합니다. 구성을 복사하고 노드를 나중에 다시 시작하려면 **구성 푸시** 옵션을 사용합니다.

Orchestrator 클러스터에서 노드 제거

클러스터에서 노드를 삭제하려면 노드가 Orchestrator 클러스터에서 사용되지 않는 데이터베이스와 작동하도록 구성해야 합니다.

참고 노드의 데이터베이스를 변경하면 인증서 및 라이선스를 가져오거나 다시 생성해야 합니다.

제어 센터에서 노드가 더 이상 클러스터의 일부가 아닌 것으로 표시되면 https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/#/control-app/ha?remove-nodes의 고급 **Orchestrator 클러스터 관리** 페이지에 액세스하여 남은 기록을 제거합니다.

로드 밸런서 구성

로드 밸런서는 고가용성 배포에서 서버 간에 작업을 분산시킵니다.

Orchestrator 클러스터를 구성한 후 로드 밸런서를 설정하여 vRealize Orchestrator의 여러 인스턴스 간에 트래픽을 분산할 수 있습니다. 자세한 내용은 [vRealize Orchestrator 로드 밸런싱](#)을 참조하십시오.

고객 경험 향상 프로그램 구성

고객 경험 향상 프로그램(CEIP) 참여를 선택하면 VMware에 VMware 제품 및 서비스의 품질, 안정성 및 기능을 개선할 수 있는 익명의 정보가 전달됩니다.

VMware에 수신되는 정보의 범주

CEIP(고객 환경 향상 프로그램)는 VMware가 VMware 제품 및 서비스를 향상시키고 문제를 수정할 수 있도록 하는 정보를 VMware에 제공합니다. CEIP에 참여하도록 선택하면 VMware는 정기적으로 CEIP 보고서에 사용자의 VMware 제품 및 서비스 사용에 대한 특정 유형의 기술 정보를 수집합니다.

VMware가 수집하는 정보의 유형 및 이 정보를 사용하는 방법에 대한 자세한 내용을 보려면 <http://www.vmware.com/trustvmware/ceip.html>에서 VMware CEIP 포털을 참조하십시오.

고객 경험 향상 프로그램(CEIP) 참여

제어 센터에서 고객 경험 향상 프로그램(CEIP) 참여

프로시저

- 1 제어 센터에 root로 로그인하고 **고객 경험 향상 프로그램** 페이지를 엽니다.
- 2 **고객 경험 향상 프로그램 참여** 확인란을 선택하여 해당 프로그램을 활성화하거나 확인란을 선택 해제하여 프로그램을 비활성화한 후 **저장**을 클릭합니다.
- 3 (선택 사항) 프록시 호스트를 수동으로 추가하려면 **자동 프록시 검색** 확인란을 선택 해제합니다.

API 서비스 사용

제어 센터를 통한 Orchestrator 구성 외에도 장치에 저장된 Orchestrator REST API, 제어 센터 REST API 또는 명령줄 유틸리티를 사용하여 Orchestrator 서버 구성 설정을 수정할 수 있습니다.

구성 플러그인은 Orchestrator 패키지에 기본적으로 포함되어 있습니다. 구성 플러그인 워크플로는 Orchestrator 워크플로 라이브러리 또는 Orchestrator REST API를 통해 액세스할 수 있습니다. 이 워크플로를 통해 신뢰할 수 있는 인증서 및 Orchestrator 서버의 키 저장소 설정을 변경할 수 있습니다. 제공되는 모든 Orchestrator REST API 서비스 호출에 대한 자세한 내용은 https://orchestrator_서버_IP_또는_DNS_이름:8281/vco/api/docs에서 Orchestrator REST API 참조 설명서를 참조하십시오.

- **REST API를 사용하여 SSL 인증서 및 키 저장소 관리**(51 페이지)
제어 센터를 통한 SSL 인증서 관리 외에도 구성 플러그인에서 워크플로를 실행하거나 REST API를 사용하여 신뢰할 수 있는 인증서 및 키 저장소를 관리할 수도 있습니다.
- **제어 센터 REST API를 사용하여 Orchestrator 구성 자동화**(54 페이지)
제어 센터 REST API는 Orchestrator 서버 구성을 위해 리소스에 대한 액세스를 제공합니다. 제어 센터 REST API를 타사 시스템과 사용하여 Orchestrator 구성을 자동화할 수 있습니다.

REST API를 사용하여 SSL 인증서 및 키 저장소 관리

제어 센터를 통한 SSL 인증서 관리 외에도 구성 플러그인에서 워크플로를 실행하거나 REST API를 사용하여 신뢰할 수 있는 인증서 및 키 저장소를 관리할 수도 있습니다.

구성 플러그인은 SSL 인증서 및 키 저장소 가져오기 및 삭제에 대한 워크플로를 포함합니다. 이러한 워크플로는 Orchestrator 클라이언트의 워크플로 보기에서 **라이브러리 > 구성 > SSL 신뢰 관리자 및 라이브러리 > 구성 > 키 저장소**로 이동하여 액세스할 수 있습니다. 또한 이러한 워크플로는 Orchestrator REST API를 사용하여 실행할 수도 있습니다.

REST API를 사용하여 SSL 인증서 삭제

구성 플러그인의 신뢰할 수 있는 인증서 삭제 워크플로를 실행하거나 REST API를 사용하여 SSL 인증서를 삭제할 수 있습니다.

프로시저

- 1 신뢰할 수 있는 인증서 삭제 워크플로의 워크플로 서비스 URL에서 GET 요청을 만듭니다.
GET `https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name>Delete trusted certificate`
- 2 정의의 URL에서 GET 요청을 만들어 신뢰할 수 있는 인증서 삭제 워크플로 정의를 검색합니다.
GET `https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd`

- 3 신뢰할 수 있는 인증서 삭제 워크플로의 실행 개체를 보유하는 URL에서 POST 요청을 만듭니다.

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd/executions/
```

- 4 요청 본문의 실행 컨텍스트 요소에 신뢰할 수 있는 인증서 삭제 워크플로의 입력 매개 변수로 삭제하려는 인증서 이름을 제공합니다.

REST API를 사용하여 SSL 인증서 가져오기

구성 플러그인에서 워크플로를 실행하거나 REST API를 사용하여 SSL 인증서를 가져올 수 있습니다.

파일 또는 URL에서 신뢰할 수 있는 인증서를 가져올 수 있습니다. 제어 센터를 사용하여 Orchestrator에서 인증서 가져오기에 대한 자세한 내용은 [“Orchestrator 인증서 관리,”](#) (41 페이지)를 참조하십시오.

프로시저

- 1 워크플로 서비스의 URL에서 GET 요청을 만듭니다.

옵션	설명
파일에서 신뢰할 수 있는 인증서 가져오기	파일에서 신뢰할 수 있는 인증서를 가져옵니다.
URL에서 신뢰할 수 있는 인증서 가져오기	URL 주소에서 신뢰할 수 있는 인증서를 가져옵니다.
프록시 서버를 사용하여 URL에서 신뢰할 수 있는 인증서 가져오기	프록시 서버를 사용하여 URL 주소에서 신뢰할 수 있는 인증서를 가져옵니다.
인증서 별칭이 포함된 URL에서 신뢰할 수 있는 인증서 가져오기	URL 주소에서 인증서 별칭이 있는 신뢰할 수 있는 인증서를 가져옵니다.

파일에서 신뢰할 수 있는 인증서를 가져오려면 다음 GET 요청을 만듭니다.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Import trusted certificate from a file
```

- 2 정의의 URL에서 GET 요청을 만들어 워크플로 정의를 검색합니다.

파일 워크플로에서 신뢰할 수 있는 인증서 가져오기에 대한 정의를 검색하려면 다음 GET 요청을 만듭니다.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5
```

- 3 워크플로의 실행 개체를 보유하는 URL에서 POST 요청을 만듭니다.

파일 워크플로에서 신뢰할 수 있는 인증서를 가져오려면 다음 POST 요청을 만듭니다.

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5/executions
```

- 4 요청 본문의 실행 컨텍스트 요소에 워크플로의 입력 매개 변수에 대한 값을 제공합니다.

매개 변수	설명
cer	SSL 인증서를 가져오려는 CER 파일입니다. 이 매개 변수는 파일 워크플로에서 신뢰할 수 있는 인증서 가져오기에 적용됩니다.
url	SSL 인증서를 가져오려는 URL입니다. HTTPS가 아닌 서비스의 경우 지원되는 형식은 IP_address_or_DNS_name:port입니다. 이 매개 변수는 URL 워크플로에서 신뢰할 수 있는 인증서 가져오기에 적용됩니다.

REST API를 사용하여 키 저장소 생성

구성 플러그인의 키 저장소 생성 워크플로를 실행하거나 REST API를 사용하여 키 저장소를 생성할 수 있습니다.

프로시저

- 1 키 저장소 생성 워크플로의 워크플로 서비스 URL에서 GET 요청을 만듭니다.
GET `https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Create a keystore`
- 2 정의의 URL에서 GET 요청을 만들어 키 저장소 생성 워크플로 정의를 검색합니다.
GET `https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/`
- 3 키 저장소 생성 워크플로의 실행 개체를 보유하는 URL에서 POST 요청을 만듭니다.
POST `https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/executions/`
- 4 요청 본문의 실행 컨텍스트 요소에 키 저장소 생성 워크플로의 입력 매개 변수로 생성하려는 키 저장소 이름을 제공합니다.

REST API를 사용하여 키 저장소 삭제

구성 플러그인의 키 저장소 삭제 워크플로를 실행하거나 REST API를 사용하여 키 저장소를 삭제할 수 있습니다.

프로시저

- 1 키 저장소 삭제 워크플로의 워크플로 서비스 URL에서 GET 요청을 만듭니다.
GET `https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name>Delete a keystore`
- 2 정의의 URL에서 GET 요청을 만들어 키 저장소 삭제 워크플로 정의를 검색합니다.
GET `https://{orchestrator_host}:{port}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/`
- 3 키 저장소 삭제 워크플로의 실행 개체를 보유하는 URL에서 POST 요청을 만듭니다.
POST `https://{orchestrator_host}:{port}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/executions/`
- 4 요청 본문의 실행 컨텍스트 요소에 키 저장소 삭제 워크플로의 입력 매개 변수로 삭제하려는 키 저장소 이름을 제공합니다.

REST API를 사용하여 키 추가

구성 플러그인의 키 추가 워크플로를 실행하거나 REST API를 사용하여 키를 추가할 수 있습니다.

프로시저

- 1 키 추가 워크플로의 워크플로 서비스 URL에서 GET 요청을 만듭니다.
GET `https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Add key`
- 2 정의의 URL에서 GET 요청을 만들어 키 추가 워크플로 정의를 검색합니다.
GET `https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/`
- 3 키 추가 워크플로의 실행 개체를 보유하는 URL에서 POST 요청을 만듭니다.
POST `https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/executions/`

- 요청 본문의 실행 컨텍스트 요소에서 키 저장소, 키 별칭, PEM-인코드 키, 인증서 체인 및 키 암호를 키 추가 워크플로의 입력 매개 변수로 제공합니다.

제어 센터 REST API를 사용하여 Orchestrator 구성 자동화

제어 센터 REST API는 Orchestrator 서버 구성을 위해 리소스에 대한 액세스를 제공합니다. 제어 센터 REST API를 타사 시스템과 사용하여 Orchestrator 구성을 자동화할 수 있습니다.

제어 센터 REST API의 루트 끝점은 https://orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/api입니다. 제어 센터 REST API를 통해 수행할 수 있는 모든 서비스 호출에 대한 자세한 내용은 https://orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/docs에서 제어 센터 REST API 참조 설명서를 참조하십시오.

명령줄 유틸리티

Orchestrator 명령줄 유틸리티를 사용하여 Orchestrator 구성을 자동화할 수 있습니다.

SSH를 통해 Orchestrator Appliance에 루트로 로그인하여 명령줄 유틸리티에 액세스합니다. 유틸리티는 `/var/lib/vco/tools/configuration-cli/bin`에 위치합니다. 사용 가능한 구성 옵션을 보려면 `./vro-configure.sh --help`를 실행합니다.

추가 구성 옵션

제어 센터를 사용하여 기본 Orchestrator 동작을 변경할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- “제어 센터에서 새 사용자 만들기,” (55 페이지)
- “Orchestrator 구성 내보내기,” (55 페이지)
- “Orchestrator 구성 가져오기,” (56 페이지)
- “Orchestrator 구성 마이그레이션,” (57 페이지)
- “워크플로 실행 속성 구성,” (60 페이지)
- “Orchestrator 로그 파일,” (60 페이지)

제어 센터에서 새 사용자 만들기

잠재적 보안 문제를 방지하기 위해, 루트 암호를 변경하는 대신 언제든지 새 사용자 계정을 만들고 해당 계정에 암호를 지정할 수 있습니다. 새 사용자 계정을 만들면 제어 센터에서 루트 계정에 액세스할 수 없습니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **설정** 페이지에서 **자격 증명 변경**을 클릭합니다.
- 3 **기존 암호** 텍스트 상자에 현재 암호를 입력합니다.
- 4 **새 사용자 이름** 텍스트 상자에 새 사용자 이름을 입력합니다.
- 5 **새 암호** 텍스트 상자에 새 암호를 입력합니다.
- 6 새 암호를 다시 입력하여 확인합니다.
- 7 **자격 증명 변경**을 클릭합니다.

Orchestrator 구성 내보내기

제어 센터에서는 Orchestrator 구성 설정을 로컬 파일로 내보낼 수 있는 메커니즘을 제공합니다. 이 메커니즘을 사용하여 시스템 구성에 대한 원하는 시점을 스냅샷을 생성하고 이 구성을 새 Orchestrator 인스턴스로 가져올 수 있습니다.

정기적으로 구성 설정을 내보내고 저장해야 하며, 특히 수정 사항이 있거나 유지 보수 작업을 수행하거나, 시스템을 업그레이드할 때는 더욱 그래야 합니다.

중요 내보낸 구성이 있는 파일은 중요한 관리 정보를 포함하고 있으므로 안전하게 유지해야 합니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **구성 내보내기/가져오기**를 클릭합니다.
- 3 내보낼 파일의 유형을 선택합니다.

참고 플러그인 구성에 암호화된 속성이 포함된 경우 **플러그인 구성 내보내기**를 선택할 때는 가져올 때 데이터의 암호를 성공적으로 해독할 수 있도록 **서버 구성 내보내기**도 선택해야 합니다.

- 4 (선택 사항) 구성 파일을 보호할 암호를 입력합니다.
나중에 구성을 가져올 때 이 암호를 사용합니다.
- 5 **내보내기(Export)**를 클릭합니다.

Orchestrator에서 `orchestrator-config-export-hostname-dateReference.zip` 파일이 생성되고 로컬 시스템에 다운로드됩니다. 이 파일을 사용하여 시스템을 복제하거나 복원할 수 있습니다.

참고 Orchestrator 인스턴스 복제를 선택한 경우 데이터베이스 설정을 복제된 Orchestrator로 가져와서는 안됩니다. 대신, 다른 외부 데이터베이스에 연결을 구성해야 합니다.

Orchestrator 구성 가져오기

시스템 오류가 발생하는 경우 Orchestrator를 다시 설치한 후 이전에 내보낸 시스템 구성을 복원할 수 있습니다.

Orchestrator 구성을 복제하기 위해 가져오기 절차를 사용하는 경우 새 vCenter Server 플러그인 ID가 생성되므로 vCenter Server 플러그인 구성이 유효하지 않게 되며 작동하지 않습니다.

필수 조건

제어 센터의 **시작 옵션** 페이지에서 Orchestrator 서버를 중지합니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **구성 내보내기/가져오기**를 클릭하고 **구성 가져오기** 탭으로 이동합니다.
- 3 이전 설치에서 내보낸 .zip 파일을 찾아 선택합니다.
- 4 구성을 내보낼 때 사용한 암호를 입력합니다.
암호를 사용해 구성을 내보내지 않았다면 이 단계는 필요하지 않습니다.
- 5 **가져오기**를 클릭합니다.
- 6 가져올 파일의 유형을 선택합니다.

중요 새 버전의 모든 플러그인을 내보낸 파일이 포함할 수 있는 이전 버전으로 대체할 것이 아니면 플러그인 강제 가져오기를 사용하지 마십시오. 버전 비호환성으로 인해 플러그인이 작동을 멈출 수 있습니다.

- 7 **가져오기 완료**를 클릭합니다.

구성을 성공적으로 가져왔다는 메시지가 표시됩니다. 새 시스템은 이전 구성을 완전히 복제합니다.

후속 작업

- 제어 센터의 **구성 검증** 페이지를 열어 vRealize Orchestrator가 올바르게 구성되었는지 확인합니다.

- 변경 내용이 적용되도록 제어 센터의 **시작 옵션** 페이지에서 Orchestrator 서버를 다시 시작합니다.

Orchestrator 구성 마이그레이션

Orchestrator 마이그레이션 도구는 구성 설정, 플러그인, 플러그인 구성, 인증서 및 라이선스 정보를 vRealize Orchestrator 7.x로 가져올 수 있는 아카이브로 묶어 줍니다.

다음 명령줄 옵션은 vro-migrate export 명령과 함께 사용할 수 있습니다.

옵션	설명
password	내보낸 아카이브를 보호하기 위한 암호를 설정합니다. 아카이브에 암호가 제공되지 않으면 보호되지 않습니다.
vroRootPath	vRealize Orchestrator 서버의 루트 경로를 지정합니다.

Orchestrator 구성을 Windows에서 가상 장치로 마이그레이션

5.5.x 및 6.x Orchestrator Windows 독립형 구성을 Orchestrator Appliance로 마이그레이션할 수 있습니다.

필수 조건

- 소스 및 대상 Orchestrator 서버를 중지합니다.
- 데이터베이스 스키마를 포함하여 소스 Orchestrator 서버의 데이터베이스를 백업합니다.

프로시저

- 대상 Orchestrator 서버에서 마이그레이션 도구를 다운로드합니다.
 - 제어 센터에 **루트**로 로그인합니다.
 - 구성 내보내기/가져오기** 페이지를 열고 **구성 마이그레이션** 탭을 클릭합니다.
 - 페이지의 설명에 지정된 마이그레이션 도구를 다운로드하거나 https://orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/api/server/migration-tool에서 직접 다운로드합니다.
- 소스 Orchestrator 서버에서 Orchestrator 구성을 내보냅니다.
 - 다운로드한 아카이브의 압축을 풀고 Orchestrator 설치 폴더에 해당 폴더를 배치합니다.
Windows 기반 설치에서 Orchestrator 설치 폴더의 기본 경로는 C:\Program Files\VMware\Orchestrator입니다.
 - PATH 환경 변수가 Orchestrator와 함께 설치된 Java JRE의 bin 폴더를 가리키도록 설정합니다.
 - Windows 명령 프롬프트를 사용하여 Orchestrator 설치 폴더 아래 bin 폴더로 이동합니다.
기본적으로 bin 폴더의 경로는 C:\Program Files\VMware\Orchestrator\migration-cli\bin입니다.
 - 명령줄에서 export 명령을 실행합니다.

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```


이 명령은 VMware vRealize Orchestrator 구성 파일과 플러그인을 내보내기 아카이브로 합쳐 줍니다.
아카이브는 migration-cli 폴더와 동일한 폴더에 생성됩니다.
- 대상 Orchestrator 서버로 구성을 가져옵니다.
 - 제어 센터에서 **구성 내보내기/가져오기**를 열고 **구성 마이그레이션** 탭을 클릭합니다.
 - 가져오기**를 클릭합니다.

- c 가져올 파일의 유형을 선택합니다.

참고

소스 및 대상 Orchestrator 서버가 구성되어 동일한 외부 데이터베이스를 사용하는 경우, **데이터베이스 설정 마이그레이션** 확인란을 선택 취소하여 데이터베이스 스키마가 최신 버전으로 업그레이드되지 않도록 합니다. 그렇지 않으면 소스 Orchestrator 환경의 작동이 중지됩니다.

- d **마이그레이션 완료**를 클릭합니다.
- 4 소스 vRealize Orchestrator가 vRealize Automation을 인증 제공자로 사용하는 경우, vRealize Automation 서버의 SSL 인증서를 Orchestrator 신뢰 저장소에 가져오고 대상 Orchestrator 서버의 라이선스 제공자를 변경합니다.
 - a 제어 센터의 **인증서** 페이지에서 **URL에서 가져오기**를 클릭합니다.
 - b vRealize Automation 서버의 URL을 제공합니다.
 - c 제어 센터의 **라이선싱** 페이지로 이동합니다.
 - d **라이선스 제공자 선택** 드롭다운 메뉴에서 **vRA 라이선스**를 선택합니다.
 - 5 소스 vRealize Orchestrator가 **vSphere** 또는 **SSO(레거시)** 인증 모드를 사용하는 경우, 라이선스 제공자를 **수동 라이선스**로 변경하고 수동 라이선스 키를 입력합니다.

마이그레이션이 성공적으로 완료되었다는 메시지가 표시됩니다.

후속 작업

- 제어 센터의 **구성 검증** 페이지를 열어 vRealize Orchestrator가 올바르게 구성되었는지 확인합니다.
- 변경 내용이 적용되도록 제어 센터의 **시작 옵션** 페이지에서 Orchestrator 서버를 다시 시작합니다.

Windows용 vRealize Orchestrator 6.x 인스턴스의 클러스터를 vRealize Orchestrator 7.1 또는 7.2 가상 장치의 클러스터로 마이그레이션

Windows에 설치되어 있는 vRealize Orchestrator 6.x 인스턴스의 클러스터를 vRealize Orchestrator 7.1 또는 7.2 버전 가상 장치의 클러스터로 마이그레이션할 수 있습니다.

필수 조건

- 클러스터에서 Orchestrator 6.x 인스턴스의 Orchestrator 서버 서비스를 중지합니다.
- 외부 Orchestrator 서버의 데이터베이스를 백업합니다(데이터베이스 스키마 포함).
- 대상 버전에 Orchestrator 노드를 배포합니다. 자세한 내용은 [“Orchestrator Appliance 다운로드 및 배포,”](#) (21 페이지) 항목을 참조하십시오.

프로시저

- 1 대상 Orchestrator 서버에서 마이그레이션 도구를 다운로드합니다.
 - a 제어 센터에 **루트**로 로그인합니다.
 - b **구성 내보내기/가져오기** 페이지를 열고 **구성 마이그레이션** 탭을 클릭합니다.
 - c 설명에 지정된 마이그레이션 도구를 다운로드하거나 https://orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/api/server/migration-tool에서 직접 다운로드합니다.

- 2 소스 Orchestrator 서버 노드 중 하나에서 Orchestrator 구성을 내보냅니다.
 - a PATH 환경 변수가 Orchestrator와 함께 설치된 Java JRE의 bin 폴더를 가리키도록 설정합니다.
 - b 마이그레이션 도구를 소스 Orchestrator가 설치되어 있는 Windows 서버에 업로드합니다.
 - c 다운로드한 아카이브의 압축을 풀고 Orchestrator 설치 폴더에 해당 폴더를 배치합니다.
Windows 기반 설치에서 Orchestrator 설치 폴더의 기본 경로는 C:\Program Files\VMware\Orchestrator입니다.
 - d 관리자 권한으로 Windows 명령 프롬프트를 실행하고 Orchestrator 설치 폴더 아래의 bin 폴더로 이동합니다.
기본적으로 bin 폴더의 경로는 C:\Program Files\VMware\Orchestrator\migration-cli\bin입니다.
 - e 명령줄에서 export 명령을 실행합니다.
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
이 명령은 VMware vRealize Orchestrator 구성 파일과 플러그인을 내보내기 아카이브로 합쳐 줍니다.
아카이브는 migration-cli 폴더와 동일한 폴더에 생성됩니다.
- 3 대상 Orchestrator 서버로 구성을 가져옵니다.
 - a 제어 센터에서 **구성 내보내기/가져오기**를 열고 **구성 마이그레이션** 탭을 클릭합니다.
 - b 내보낸 구성 파일을 찾아보고 **가져오기**를 클릭합니다.
 - c 가져올 파일의 유형을 선택합니다.

옵션	설명
데이터베이스 설정 마이그레이션	vRealize Orchestrator 6.x 클러스터의 데이터베이스를 사용합니다.
플러그인 마이그레이션	Orchestrator 플랫폼에 포함되어 있지 않은 모든 플러그인을 마이그레이션합니다.
레거시 플러그인 구성 마이그레이션	<i>Orchestrator_install_folder\app-server\conf\plugins</i> 폴더에 저장되어 있는 플러그인의 구성을 마이그레이션합니다.
신뢰할 수 있는 인증서 마이그레이션	vRealize Orchestrator 6.x 클러스터의 신뢰 저장소에서 모든 인증서를 마이그레이션합니다.

- d **마이그레이션 완료**를 클릭합니다.
마이그레이션이 성공적으로 완료되었다는 메시지가 표시됩니다.
- 4 Orchestrator 클러스터를 다시 구성합니다.
 - a 고급 **Orchestrator 클러스터 관리** 페이지를 https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter/#/control-app/ha?remove-nodes에서 엽니다.
 - b Orchestrator 6.x 노드 옆에 있는 확인란을 선택하고 **제거**를 클릭합니다.
 - c 제어 센터의 **구성 검증** 페이지에서 Orchestrator가 올바르게 구성되었는지 확인합니다.
Orchestrator 클러스터가 일관성 없는 상태임 경고를 무시할 수 있으며, 이 경고는 Orchestrator 서버 서비스를 시작하면 나타나지 않습니다.
 - d 라이선싱 오류가 나타나는 경우 제어 센터의 **라이선싱** 페이지에서 적절한 라이선스 제공자를 구성합니다.

- 5 제어 센터의 **시작 옵션** 페이지에서 대상 Orchestrator 서버의 Orchestrator 서버 서비스를 시작합니다.
 - a **시작 옵션** 페이지에서 **활성 구성 지문** 문자열 및 **보류 중인 구성 지문** 문자열이 일치하는지 확인합니다.

참고 두 문자열이 일치할 때까지 **시작 옵션** 페이지를 여러 번 새로 고침해야 할 수 있습니다.

vRealize Orchestrator 6.x 클러스터를 7.1 또는 7.2 버전 Orchestrator 가상 장치의 클러스터로 성공적으로 마이그레이션했습니다.

후속 작업

- Orchestrator 클라이언트에 로그인하고 모든 설치한 플러그인의 구성이 올바른지 확인합니다.
- 대상 Orchestrator 클러스터에 노드를 더 추가합니다. 자세한 내용은 **“Orchestrator 클러스터 구성.”** (46 페이지) 항목을 참조하십시오.

워크플로 실행 속성 구성

기본적으로 노드별로 최대 300개의 워크플로를 실행할 수 있으며 현재 실행 중인 워크플로의 개수가 이에 도달하면 최대 10,000개의 워크플로를 대기열에 추가할 수 있습니다.

Orchestrator 노드가 동시에 300개 이상의 워크플로를 실행해야 하는 경우 보류 중인 워크플로는 대기열에 추가됩니다. 활성 워크플로 실행이 완료되면 대기열의 다음 워크플로가 실행되기 시작합니다. 대기 중인 워크플로가 최대 개수에 도달하면 보류 중인 워크플로 중 하나가 실행되기 전까지는 다음 워크플로 실행이 실패합니다.

제어 센터의 **고급 옵션** 페이지에서 워크플로 실행 속성을 구성할 수 있습니다.

옵션	설명
안전 모드 사용	안전 모드를 사용하면 실행 중인 모든 워크플로가 취소되고 다음 Orchestrator 노드 시작 시 재개되지 않습니다.
동시 실행 워크플로 개수	동시에 실행되는 Orchestrator 노드 워크플로의 최대 개수입니다.
대기열에서 실행 중인 워크플로의 최대 개수	사용할 수 없는 상태가 되기 전까지 Orchestrator 노드가 수락하는 워크플로 실행 요청의 개수입니다.
워크플로별로 유지되는 실행의 최대 개수	완료된 워크플로 실행의 최대 개수는 클러스터의 워크플로마다 각각 기록으로 유지됩니다. 개수를 초과하면 가장 오래된 워크플로 실행이 삭제됩니다.
로그 이벤트 만료 일수	로그 이벤트가 제거되기 전에 데이터베이스에서 유지되는 클러스터에 대한 로그 이벤트의 기간(일)입니다.

Orchestrator 로그 파일

VMware 기술 지원은 사용자의 지원 요청이 제출되면 정기적으로 진단 정보를 요청합니다. 해당 제품이 실행되는 호스트에서 진단된 이 정보에는 제품 관련 로그 및 구성 파일이 포함됩니다.

제어 센터의 **로그 내보내기** 메뉴에서 Orchestrator 구성 파일 및 로그 파일을 포함하는 ZIP 번들을 다운로드할 수 있습니다.

표 7-1. Orchestrator 로그 파일 목록

파일 이름	위치	설명
scripting.log	/var/log/vco/app-server	워크플로 및 작업의 스크립팅 로그 메시지를 제공합니다. scripting.log 파일을 사용하여 워크플로 실행 및 작업 실행을 일반 Orchestrator 작업에서 분리합니다. 이 정보는 server.log 파일에도 포함됩니다.
server.log	/var/log/vco/app-server	Orchestrator 서버의 모든 작업에 대한 정보를 제공합니다. Orchestrator 또는 Orchestrator에서 실행하는 모든 애플리케이션을 디버깅할 때 server.log 파일을 분석합니다.
metrics.log	/var/log/vco/app-server	서버에 대한 런타임 정보를 포함합니다. 해당 정보는 5분마다 로그 파일에 추가됩니다.
localhost_access_log.txt	/var/log/vco/app-server	서버의 HTTP 요청 로그입니다.
localhost_access_log.date.txt	/var/log/vco/configuration	제어 센터 서비스의 HTTP 요청 로그입니다.
controlcenter.log	/var/log/vco/configuration	제어 센터 서비스의 로그 파일입니다.

로깅 지속성

모든 종류의 Orchestrator 스크립트(예: 워크플로, 정책 또는 작업)에서 정보를 기록할 수 있습니다. 정보에는 유형 및 수준이 있습니다. 유형은 영구 또는 비영구로 구분할 수 있습니다. 수준은 DEBUG, INFO, WARN, ERROR, TRACE 및 FATAL로 구분됩니다.

표 7-2. 영구 및 비영구 로그 생성

로그 수준	영구 유형	비영구 유형
DEBUG	Server.debug("short text", "long text");	System.debug("text")
INFO	Server.log("short text", "long text");	System.log("text");
WARN	Server.warn("short text", "long text");	System.warn("text");
ERROR	Server.error("short text", "long text");	System.error("text");

영구 로그

영구 로그(서버 로그)는 이전 워크플로 실행 로그를 추적하고 Orchestrator 데이터베이스에 저장됩니다. 서버 로그를 보려면 워크플로, 완료된 워크플로 실행 또는 정책을 선택하고 Orchestrator 클라이언트의 **이벤트** 탭을 클릭해야 합니다.

비영구 로그

비영구 로그(시스템 로그)를 사용하여 스크립트를 생성하는 경우 Orchestrator 서버는 실행 중인 모든 Orchestrator 애플리케이션에 해당 로그에 대해 알리지만 이 정보는 데이터베이스에 저장되지 않습니다. 애플리케이션이 다시 시작되면 로그 정보는 손실됩니다. 비영구 로그는 실시간 정보 및 디버깅 용도로 사용됩니다. 시스템 로그를 보려면 Orchestrator 클라이언트의 완료된 워크플로 실행을 선택하고 **스키마** 탭에서 **로그**를 클릭해야 합니다.

Orchestrator 로그 구성

제어 센터의 **로그 구성** 페이지에서 필요한 서버 로그 및 스크립팅 로그의 수준을 설정할 수 있습니다. 하루에 두 로그 중 하나가 여러 번 생성되는 경우 문제가 발생하는 원인을 찾기 어렵습니다.

서버 로그 및 스크립팅 로그의 기본 로그 수준은 정보입니다. 로그 수준을 변경하면 서버가 로그에 입력되는 모든 새 메시지와 데이터베이스의 활성 연결 수에 영향을 줍니다. 로깅의 자세한 정도는 내림차순으로 감소합니다.



주의 로그 수준을 디버그 또는 모두로 설정해야만 문제를 디버그할 수 있습니다. 성능에 심각한 영향을 줄 수 있기 때문에 운영 환경에서는 이러한 설정을 사용하지 마십시오.

로그 순환 설정

서버 로그가 너무 커지는 것을 방지하려면 **최대 파일 개수** 및 **최대 파일 크기(MB)** 텍스트 상자의 값을 변경하여 서버 로그의 최대 파일 크기 및 개수를 설정할 수 있습니다.

Orchestrator 로그 파일 내보내기

제어 센터를 사용하여 구성, 서버, 래퍼 및 설치 로그 파일을 포함하는 문제 해결 정보를 ZIP 아카이브로 생성할 수 있습니다.

로그 정보는 `vco-logs-date_hour.zip`으로 명명된 ZIP 아카이브에 저장됩니다.

워크플로 로그 검사

제어 센터의 검사 워크플로 페이지에 액세스하여 완료된 워크플로의 시스템 로그 및 서버 로그를 신속하게 검사하거나 내보낼 수 있습니다.

참고 Orchestrator를 클러스터의 일부로 사용하는 경우 시스템 로그는 워크플로가 시작되는 서버 노드에만 저장됩니다.

중요 로그 정보는 임시적으로 저장됩니다.

- 시스템 로그는 최대 10MB까지 저장됩니다. 로그 파일의 최대 수는 노트당 5개입니다.
- 서버 로그는 데이터베이스에 15일 간 저장됩니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **워크플로 검사**를 클릭합니다.
- 3 **완료된 워크플로** 탭을 클릭합니다.
- 4 (선택 사항) 검사하려는 워크플로 토큰 유형을 선택하고 날짜 범위를 선택한 후 **적용**을 클릭합니다.
- 5 (선택 사항) 이름, ID 또는 토큰 ID별로 워크플로를 검색합니다.
- 6 검사하려는 토큰 ID를 클릭합니다.
워크플로 실행 로그 보기가 전체 화면에 나타납니다.
- 7 시스템 로그 및 서버 로그를 검사합니다.
- 8 (선택 사항) **토큰 로그 내보내기**를 클릭하여 워크플로 토큰 로그를 .zip 파일로 내보냅니다.

Orchestrator 로그 필터링

특정 워크플로 실행에 대한 Orchestrator 서버 로그를 필터링하고 워크플로 실행에 대한 진단 데이터를 수집할 수 있습니다.

Orchestrator 로그는 실시간으로 모니터링할 수 있는 여러 유용한 정보를 포함합니다. 동일한 워크플로의 여러 인스턴스가 동시에 실행되면 Orchestrator 라이브 로그 스트림에서 각 실행에 대한 진단 데이터를 필터링하여 다른 워크플로 실행을 추적할 수 있습니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **라이브 로그 스트림**을 클릭합니다.
- 3 검색 창에 검색 매개 변수를 입력합니다.
예를 들면 사용자 이름, 워크플로 이름, 워크플로 ID 또는 토큰 ID로 필터링할 수 있습니다.
- 4 (선택 사항) **대소문자 구분 및 필터(grep)**을 선택하여 상세하게 검색 결과를 필터링합니다.
필터(grep)를 선택하면 라이브 스트림은 검색 매개 변수와 일치하는 줄만 표시합니다.

Orchestrator 라이브 로그 스트림은 검색 매개 변수에 따라 필터링됩니다.

후속 작업

제어 센터의 라이브 로그 스트림 페이지를 통해 액세스할 수 없는 이전 로그를 필터링하려는 경우 타사 로그 분석 도구를 사용할 수 있습니다.

외부 Orchestrator 서버에서 vRealize Automation 7.2로 마이그레이션

8

기존 외부 Orchestrator 서버에서 vRealize Automation에 포함된 vRealize Orchestrator 인스턴스로 마이그레이션할 수 있습니다.

vRealize Orchestrator를 외부 서버 인스턴스로 배포하고 vRealize Automation을 구성하여 해당 외부 인스턴스로 작업하거나 vRealize Automation Appliance에 포함된 vRealize Orchestrator 서버를 구성하고 사용할 수 있습니다.

vRealize Automation 7.2 릴리스를 사용하여 VMware는 외부 vRealize Orchestrator를 vRealize Automation에 내장된 Orchestrator 서버로 마이그레이션할 것을 권장합니다. 외부에서 포함된 Orchestrator로의 마이그레이션은 다음과 같은 이점을 제공합니다.

- 총 소유 비용을 절감합니다.
- 배포 모델을 간소화합니다.
- 운영 효율성을 개선합니다.

참고 다음 경우에 외부 vRealize Orchestrator의 사용을 고려하십시오.

- vRealize Automation 환경의 여러 테넌트
- 지리적으로 분산된 환경
- 워크로드 처리
- 특정 플러그인 사용(예: Site Recovery Manager 플러그인)

이 장에서는 다음 주제에 대해 설명합니다.

- [“마이그레이션 시나리오,”](#) (66 페이지)
- [“Windows용 외부 vRealize Orchestrator 6.x를 vRealize Automation 7.2로 마이그레이션,”](#) (66 페이지)
- [“외부 vRealize Orchestrator 6.x 가상 장치를 vRealize Automation 7.2로 마이그레이션,”](#) (68 페이지)
- [“외부 vRealize Orchestrator 7.x를 vRealize Automation 7.2로 마이그레이션,”](#) (70 페이지)

마이그레이션 시나리오

외부 vRealize Orchestrator 인스턴스를 vRealize Automation에 포함된 vRealize Orchestrator 인스턴스로 마이그레이션하는 절차는 사용자의 설정에 따라 다릅니다. 외부 Orchestrator 서버가 Windows 기반인지 또는 가상 장치인지 여부, 해당 서버가 포함된 데이터베이스 또는 외부 데이터베이스를 사용하는지 여부 및 기타 조건에 따라 여러 가지 마이그레이션 시나리오가 존재합니다. 마이그레이션 프로세스를 vRealize Orchestrator, vRealize Automation의 업그레이드 또는 두 가지 모두의 업그레이드와 결합할 수 있습니다. 이 경우 마이그레이션 절차는 제품의 소스 버전에 따라 결정됩니다.

마이그레이션 시나리오 매트릭스

소스 배포를 기준으로 마이그레이션 시나리오를 선택할 수 있습니다.

vRealize Orchestrator 배포	vRealize Automation 배포	마이그레이션 시나리오
vRealize Orchestrator 6.0.3 가상 장치	vRealize Automation 6.2.3	“외부 vRealize Orchestrator 6.x 가상 장치를 vRealize Automation 7.2로 마이그레이션,” (68 페이지)
Windows용 vRealize Orchestrator 6.0.4	vRealize Automation 6.2.4	“Windows용 외부 vRealize Orchestrator 6.x를 vRealize Automation 7.2로 마이그레이션,” (66 페이지)
vRealize Orchestrator 6.0.4 가상 장치	vRealize Automation 6.2.4	“외부 vRealize Orchestrator 6.x 가상 장치를 vRealize Automation 7.2로 마이그레이션,” (68 페이지)
vRealize Orchestrator 6.0.5 가상 장치	vRealize Automation 6.2.5	“외부 vRealize Orchestrator 6.x 가상 장치를 vRealize Automation 7.2로 마이그레이션,” (68 페이지)
vRealize Orchestrator 7.0 가상 장치(외부 Oracle 데이터베이스 12 c 사용)	vRealize Automation 7.0 또는 IaaS	“외부 vRealize Orchestrator 7.x를 vRealize Automation 7.2로 마이그레이션,” (70 페이지)
vRealize Orchestrator 7.0.1 가상 장치(외부 PostgreSQL 9.3.9 데이터베이스 사용)	vRealize Automation 7.0.1 또는 IaaS	“외부 vRealize Orchestrator 7.x를 vRealize Automation 7.2로 마이그레이션,” (70 페이지)
vRealize Orchestrator 7.1 가상 장치	vRealize Automation 7.1	“외부 vRealize Orchestrator 7.x를 vRealize Automation 7.2로 마이그레이션,” (70 페이지)
vRealize Orchestrator 7.2 가상 장치	vRealize Automation 7.2	“외부 vRealize Orchestrator 7.x를 vRealize Automation 7.2로 마이그레이션,” (70 페이지)
Windows용 vRealize Orchestrator 6.0.3	vRealize Automation 6.2.3	“Orchestrator 구성을 Windows에서 가상 장치로 마이그레이션,” (57 페이지)

Windows용 외부 vRealize Orchestrator 6.x를 vRealize Automation 7.2로 마이그레이션

vRealize Automation을 6.x 버전에서 7.2 버전으로 업그레이드한 후에 Windows에 설치되어 있는 기존의 외부 Orchestrator 6.x를 vRealize Automation 7.2에 내장된 Orchestrator 서버로 마이그레이션할 수 있습니다.

참고 여러 개의 vRealize Automation Appliance 노드가 있는 분산된 vRealize Automation 환경을 사용하는 경우, 기본 vRealize Automation 노드에서만 마이그레이션 절차를 수행하십시오.

필수 조건

- vRealize Automation을 6.x 버전에서 7.2 버전으로 업그레이드합니다.

- 외부 Orchestrator의 Orchestrator 서버 서비스를 중지합니다.
- 외부 Orchestrator 서버의 데이터베이스를 백업합니다(데이터베이스 스키마 포함).

참고 새로운 데이터베이스를 완전히 구성할 때까지 소스 Orchestrator 환경을 사용할 계획인 경우, 소스 데이터베이스의 사본을 생성합니다. 그렇지 않으면 동일한 데이터베이스를 사용하도록 대상 Orchestrator를 구성할 수 있습니다. 하지만 이 경우 데이터베이스 스키마가 대상 Orchestrator의 버전으로 업그레이드되기 때문에 소스 Orchestrator 환경이 더 이상 작동하지 않습니다.

프로시저

- 1 대상 Orchestrator 서버에서 마이그레이션 도구를 다운로드합니다.
 - a SSH를 통해 vRealize Automation Appliance에 **루트**로 로그인합니다.
 - b migration-tool.zip 아카이브(/var/lib/vco/downloads 디렉토리에 있음)를 다운로드합니다.
- 2 소스 Orchestrator 서버에서 Orchestrator 구성을 내보냅니다.
 - a PATH 환경 변수가 Orchestrator와 함께 설치된 Java JRE의 bin 폴더를 가리키도록 설정합니다.
 - b 마이그레이션 도구를 외부 Orchestrator가 설치되어 있는 Windows 서버에 업로드합니다.
 - c 다운로드한 아카이브의 압축을 풀고 Orchestrator 설치 폴더에 해당 폴더를 배치합니다.
Windows 기반 설치에서 Orchestrator 설치 폴더의 기본 경로는 C:\Program Files\VMware\Orchestrator입니다.
 - d Windows 명령 프롬프트를 관리자로 실행하고 Orchestrator 설치 폴더의 bin 폴더로 이동합니다.
기본적으로 bin 폴더의 경로는 C:\Program Files\VMware\Orchestrator\migration-cli\bin입니다.
 - e 명령줄에서 export 명령을 실행합니다.
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
이 명령은 VMware vRealize Orchestrator 구성 파일과 플러그인을 내보내기 아카이브로 합쳐 줍니다.
아카이브는 migration-cli 폴더와 동일한 폴더에 생성됩니다.
- 3 내보낸 구성을 vRealize Automation 7.2에 내장된 Orchestrator 서버로 마이그레이션합니다.
 - a 내보낸 구성 파일을 vRealize Automation Appliance의 /usr/lib/vco/tools/configuration-cli/bin 디렉토리에 업로드합니다.
 - b /usr/lib/vco/tools/configuration-cli/bin 디렉토리에서 내보낸 Orchestrator 구성 파일의 소유권을 변경합니다.
chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
 - c import 명령으로 vro-configure 스크립트를 실행하여 Orchestrator 구성 파일을 내장된 vRealize Orchestrator 서버로 가져옵니다.
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip

- 4 db-migrate 명령으로 vro-configure 스크립트를 실행하여 데이터베이스를 내부 PostgreSQL 데이터베이스로 마이그레이션합니다.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
```

참고 특수 문자를 포함하는 암호는 따옴표 안에 넣어야 합니다.

JDBC_connection_URL은 사용하는 데이터베이스 유형에 따라 결정됩니다.

PostgreSQL: jdbc:postgresql://*host:port/database_name*

MSSQL: jdbc:jtds:sqlserver://*host:port/database_name*;domain=*domain*

Oracle: jdbc:oracle:thin:@*host:port:database*

Windows에 설치되어 있는 외부 vRealize Orchestrator 6.x를 vRealize Automation 7.2에 포함된 vRealize Orchestrator 인스턴스로 성공적으로 마이그레이션했습니다.

후속 작업

내장된 vRealize Orchestrator 서버를 설정합니다. 9장, “[내장된 vRealize Orchestrator 서버 구성](#),” (73 페이지) 항목을 참조하십시오.

외부 vRealize Orchestrator 6.x 가상 장치를 vRealize Automation 7.2로 마이그레이션

vRealize Automation을 6.x 버전에서 7.2 버전으로 업그레이드한 후에 기존의 외부 Orchestrator 6.x 가상 장치를 vRealize Automation 7.2에 내장된 Orchestrator 서버로 마이그레이션할 수 있습니다.

참고 여러 개의 vRealize Automation Appliance 노드가 있는 분산된 vRealize Automation 환경을 사용하는 경우, 기본 vRealize Automation 노드에서만 마이그레이션 절차를 수행하십시오.

필수 조건

- vRealize Automation을 6.x 버전에서 7.2 버전으로 업그레이드합니다.
- Orchestrator 서버 서비스 및 외부 Orchestrator의 제어 센터 서비스를 중지합니다.
- 외부 Orchestrator 서버의 데이터베이스를 백업합니다(데이터베이스 스키마 포함).

프로시저

- 1 대상 Orchestrator 서버에서 소스 Orchestrator로 마이그레이션 도구를 다운로드합니다.
 - a SSH를 통해 vRealize Orchestrator 6.x 가상 장치에 **루트**로 로그인합니다.
 - b /var/lib/vco 디렉토리에서 scp 명령을 실행하여 migration-tool.zip 아카이브를 다운로드합니다.


```
scp root@vra-va-hostname.domain.name:/var/lib/vco/downloads/migration-tool.zip ./
```
 - c unzip 명령을 실행하여 마이그레이션 도구 아카이브의 압축을 풉니다.


```
unzip migration-tool.zip
```

- 2 소스 Orchestrator 서버에서 Orchestrator 구성을 내보냅니다.
 - a `/var/lib/vco/migration-cli/bin` 디렉토리에서 `export` 명령을 실행합니다.


```
./vro-migrate.sh export
```

이 명령은 VMware vRealize Orchestrator 구성 파일과 플러그인을 내보내기 아카이브로 합쳐 줍니다.

파일 이름이 `orchestrator-config-export-orchestrator_ip_address-date_hour.zip`인 아카이브가 `/var/lib/vco` 폴더에 생성됩니다.
- 3 내보낸 구성을 vRealize Automation 7.2에 내장된 Orchestrator 서버로 마이그레이션합니다.
 - a SSH를 통해 vRealize Automation Appliance에 루트로 로그인합니다.
 - b `/usr/lib/vco/tools/configuration-cli/bin` 디렉토리에서 `scp` 명령을 실행하여 내보낸 구성 아카이브를 다운로드합니다.


```
scp root@orchestrator_ip_or_DNS_name:/var/lib/vco/orchestrator-config-export-orchestrator_ip_address-date_hour.zip ./
```
 - c 내보낸 Orchestrator 구성 파일의 소유권을 변경합니다.


```
chown vco:vco orchestrator-config-export-orchestrator_ip_address-date_hour.zip
```
 - d Orchestrator 서버 서비스 및 내장된 vRealize Orchestrator 서버의 제어 센터 서비스를 중지합니다.


```
service vco-server stop && service vco-configurator stop
```
 - e `import` 명령으로 `vro-configure` 스크립트를 실행하여 Orchestrator 구성 파일을 내장된 vRealize Orchestrator 서버로 가져옵니다.


```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```
- 4 마이그레이션을 시작하려는 외부 Orchestrator 서버에서 내장된 PostgreSQL 데이터베이스를 사용하는 경우, 데이터베이스 구성 파일을 편집합니다.
 - a `/storage/db/pgsql/data/postgresql.conf` 파일에서 `listen_addresses` 행의 주석 처리를 제거합니다.
 - b `listen_addresses`의 값을 와일드카드(*)로 설정합니다.


```
listen_addresses = '*'
```
 - c 행을 `/storage/db/pgsql/data/pg_hba.conf` 파일에 추가합니다.


```
host all all vra-va-hostname.domain.name/32 md5
```

참고 `pg_hba.conf` 파일은 IP 주소 및 서브넷 마스크에서 CIDR 접두사 형식을 대신 사용해야 합니다.

 - d PostgreSQL 서버 서비스를 다시 시작합니다.


```
service postgresql restart
```

- 5 db-migrate 명령으로 vro-configure 스크립트를 실행하여 데이터베이스를 내부 PostgreSQL 데이터베이스로 마이그레이션합니다.

```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
```

참고 특수 문자를 포함하는 암호는 따옴표 안에 넣어야 합니다.

JDBC_connection_URL은 사용하는 데이터베이스 유형에 따라 결정됩니다.

PostgreSQL: jdbc:postgresql://*host:port/database_name*

MSSQL: jdbc:jtds:sqlserver://*host:port/database_name*;domain=*domain*

Oracle: jdbc:oracle:thin:@*host:port:database*

- 6 postgresql.conf 및 pg_hba.conf 파일의 기본 구성으로 되돌립니다.
 - a PostgreSQL 서버 서비스를 다시 시작합니다.

외부 vRealize Orchestrator 6.x 가상 장치를 vRealize Automation 7.2에 포함된 vRealize Orchestrator 인스턴스로 성공적으로 마이그레이션했습니다.

후속 작업

내장된 vRealize Orchestrator 서버를 설정합니다. 9장, “내장된 vRealize Orchestrator 서버 구성,” (73 페이지) 항목을 참조하십시오.

외부 vRealize Orchestrator 7.x를 vRealize Automation 7.2로 마이그레이션

기존의 외부 Orchestrator 인스턴스의 구성을 내보내고 vRealize Automation에 내장된 Orchestrator 서버로 가져올 수 있습니다.

참고 여러 개의 vRealize Automation Appliance 노드가 있는 경우 기본 vRealize Automation 노드에서만 마이그레이션 절차를 수행하십시오.

필수 조건

- vRealize Automation을 6.x 버전에서 7.2 버전으로 업그레이드합니다.
- 외부 Orchestrator의 Orchestrator 서버 서비스를 중지합니다.
- 외부 Orchestrator 서버의 데이터베이스를 백업합니다(데이터베이스 스키마 포함).

프로시저

- 1 외부 Orchestrator 서버의 구성을 내보냅니다.
 - a 외부 Orchestrator 서버의 제어 센터에 **루트**로 로그인합니다.
 - b **시작 옵션** 페이지에서 Orchestrator 서버 서비스를 중지하여 원치 않는 변경이 데이터베이스에 발생하지 않도록 합니다.
 - c **구성 내보내기/가져오기** 페이지로 이동합니다.
 - d **구성 내보내기** 페이지에서 **서버 구성 내보내기**, **변들 플러그인**, **플러그인 구성 내보내기**를 선택합니다.

2. 내보낸 구성을 내장된 Orchestrator 인스턴스로 마이그레이션합니다.
 - a. 내보낸 Orchestrator 구성 파일을 vRealize Automation Appliance 의 `/usr/lib/vco/tools/configuration-cli/bin` 디렉토리로 업로드합니다.
 - b. SSH를 통해 vRealize Automation Appliance에 루트로 로그인합니다.
 - c. Orchestrator 서버 서비스 및 내장된 vRealize Orchestrator 서버의 제어 센터 서비스를 중지합니다.


```
service vco-server stop && service vco-configurator stop
```
 - d. `/usr/lib/vco/tools/configuration-cli/bin` 디렉토리로 이동합니다.
 - e. 내보낸 Orchestrator 구성 파일의 소유권을 변경합니다.


```
chown vco:vco orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```
 - f. `import` 명령으로 `vro-configure` 스크립트를 실행하여 Orchestrator 구성 파일을 내장된 vRealize Orchestrator 서버로 가져옵니다.


```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-orchestrator_appliance_ip-date_hour.zip
```
3. `db-migrate` 명령으로 `vro-configure` 스크립트를 실행하여 데이터베이스를 내부 PostgreSQL 데이터베이스로 마이그레이션합니다.


```
./vro-configure.sh db-migrate --sourceJdbcUrl JDBC_connection_URL --sourceDbUsername database_user --sourceDbPassword database_user_password
```

참고 특수 문자를 포함하는 암호는 따옴표 안에 넣어야 합니다.

JDBC_connection_URL은 사용하는 데이터베이스 유형에 따라 결정됩니다.

PostgreSQL: `jdbc:postgresql://host:port/database_name`

MSSQL: `jdbc:jtds:sqlserver://host:port/database_name#;domain=domain`

Oracle: `jdbc:oracle:thin:@host:port:database`

외부 Orchestrator 서버 인스턴스를 vRealize Automation에 내장된 vRealize Orchestrator 인스턴스로 성공적으로 마이그레이션했습니다.

후속 작업

내장된 vRealize Orchestrator 서버를 설정합니다. 9장, “내장된 vRealize Orchestrator 서버 구성,” (73 페이지) 항목을 참조하십시오.

내장된 vRealize Orchestrator 서버 구성

9

외부 Orchestrator 서버의 구성을 내보내고 vRealize Automation 7.2로 가져온 후에는 vRealize Automation에 내장된 Orchestrator 서버를 구성해야 합니다.

필수 조건

외부에서 내부 vRealize Orchestrator로 구성을 마이그레이션합니다.

프로시저

- 1 SSH를 통해 vRealize Automation Appliance에 **루트**로 로그인합니다.
- 2 내장된 vRealize Orchestrator 서버의 제어 센터 서비스를 시작합니다.

```
service vco-configurator start
```
- 3 내장된 Orchestrator 서버의 제어 센터에 **루트**로 로그인합니다.

참고 외부 vRealize Orchestrator 7.2 인스턴스에서 마이그레이션하는 경우 **단계 8**로 건너뛰십시오.

- 4 고급 Orchestrator 관리 페이지(<https://vra-va-hostname.domain.name:8283/vco-controlcenter/#/?advanced>)로 이동합니다.
 - a 키보드에서 F5 버튼을 클릭하여 브라우저 페이지를 새로 고칩니다.
- 5 **데이터베이스 구성** 페이지에서 **저장**을 클릭합니다.

참고 **저장** 버튼이 활성화되어 있지 않으면 **데이터베이스 업데이트**를 클릭한 다음 **저장**을 클릭합니다.

- 6 제어 센터의 **구성 검증** 페이지에서 Orchestrator가 올바르게 구성되었는지 확인합니다.
- 7 **라이선싱** 페이지에서 **vRA 라이선스**를 **라이선스 제공자 선택** 드롭다운 메뉴에서 선택합니다.
- 8 외부 Orchestrator가 클러스터 모드에서 작동하도록 구성된 경우 vRealize Automation에서 Orchestrator 클러스터를 재구성합니다.
 - a 고급 **Orchestrator 클러스터 관리** 페이지에 <https://vra-va-hostname.domain.name:8283/vco-controlcenter/#/control-app/ha?advanced&remove-nodes>로 이동합니다.

참고 클러스터에서 기존 노드 옆에 **제거** 확인란이 나타나지 않는 경우, 키보드에서 F5 버튼을 클릭하여 브라우저 페이지를 새로 고침해야 합니다.

- b **Orchestrator 노드 설정** 페이지에서 **활성 노드 개수**를 10으로 변경합니다.

- c 클러스터에서 외부 Orchestrator 노드 중 일부를 제거하려는 경우 해당 노드 옆에 있는 확인란을 선택하고 **제거**를 클릭합니다.
 - d 고급 클러스터 관리 페이지에서 나가려면 URL에서 &remove-nodes 문자열을 제거하고 키보드에서 F5 버튼을 클릭하여 브라우저 페이지를 새로 고칩니다.
 - e 제어 센터의 **구성 검증** 페이지에서 Orchestrator가 제대로 구성되었는지 확인합니다.
- 9 (선택 사항) **패키지 서명 인증서** 탭(인증서 페이지에 있음) 아래에서 새 패키지 서명 인증서를 생성합니다.
 - 10 (선택 사항) **기본 데몬트 및 기본 그룹(인증 제공자 구성** 페이지에 있음)의 값을 변경합니다.
 - 11 **시작 옵션** 페이지에서 vRealize Automation에 내장된 Orchestrator 서버의 Orchestrator 서버 서비스를 시작합니다.
 - 12 vco-server 서비스가 등록됨으로 나타나는지 **서비스** 탭(vRealize Automation Appliance 관리 콘솔에 있음) 아래에서 확인합니다.
 - 13 외부 Orchestrator 서버의 vco 서비스를 선택하고 **등록 취소**를 클릭합니다.

후속 작업

- 외부 Orchestrator 서버에서 신뢰하는 모든 인증서를 내장된 Orchestrator의 신뢰 저장소로 가져옵니다. 자세한 내용은 **“Orchestrator 인증서 관리,”** (41 페이지) 항목을 참조하십시오.
- Orchestrator 구성을 동기화하려면 vRealize Automation 복제 노드를 vRealize Automation 클러스터에 결합합니다.
- 마이그레이션한 내장된 Orchestrator 서버로 이동하도록 vRealize Orchestrator 끝점을 업데이트합니다.
- vRA 호스트 추가 및 vRA 호스트 워크플로의 IaaS 호스트 추가를 실행하여 vRealize Automation 호스트 및 IaaS 호스트를 vRealize Automation 플러그인의 인벤토리에 추가합니다.

구성 사용 사례 및 문제 해결

Orchestrator 서버가 vCenter Server 장치와 함께 작동하도록 구성할 수 있습니다. 또한 Orchestrator에서 플러그인을 제거하거나 자체 서명된 인증서를 변경할 수도 있습니다.

구성 사용 사례는 해결 방법이 있는 경우 문제를 이해하고 해결할 수 있는 문제 해결 주제뿐 아니라 Orchestrator 서버에 대한 특정 구성 요구 사항을 충족하도록 수행할 수 있는 작업 흐름을 제공합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [“Orchestrator를 vCenter Server 확장으로 등록,”](#) (75 페이지)
- [“Orchestrator 인증 등록 취소,”](#) (76 페이지)
- [“SSL 인증서 변경,”](#) (76 페이지)
- [“실행 중인 워크플로 취소,”](#) (77 페이지)
- [“Orchestrator 서버 디버깅 사용,”](#) (78 페이지)
- [“Orchestrator 구성 및 요소 백업,”](#) (78 페이지)
- [“vRealize Orchestrator 백업 및 복원,”](#) (80 페이지)
- [“Site Recovery Manager를 사용한 Orchestrator의 재해 복구,”](#) (82 페이지)

Orchestrator를 vCenter Server 확장으로 등록

Orchestrator 서버에 vCenter Single Sign-On으로 등록하고 vCenter Server와 작업할 수 있도록 이를 구성한 후 Orchestrator를 vCenter Server 확장으로 등록해야 합니다.

프로시저

- 1 Orchestrator 클라이언트에 관리자로 로그인합니다.
- 2 **워크플로** 보기를 클릭합니다.
- 3 워크플로 계층 목록에서 **라이브러리 > vCenter > 구성**을 확장합니다.
- 4 **vCenter Orchestrator를 vCenter Server 확장으로 등록** 워크플로를 마우스 오른쪽 버튼으로 클릭하고 **시작 워크플로**를 선택합니다.
- 5 vCenter Server 인스턴스를 선택하여 Orchestrator를 등록합니다.
- 6 `https://your_orchestrator_server_IP_or_DNS_name:8281` 또는 요청을 Orchestrator 서버 노드로 리디렉션하는 로드 밸런서의 서비스 URL을 입력합니다.
- 7 **제출**을 클릭합니다.

Orchestrator 인증 등록 취소

제어 센터의 인증 제공자 구성 페이지에서 Single Sign-On 솔루션으로 Orchestrator를 등록 취소합니다.

Orchestrator vCenter Single Sign-On 또는 vRealize Automation 인증을 다시 구성하려면 먼저 Orchestrator 인증을 등록 취소해야 합니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **인증 제공자 구성**을 클릭합니다.
- 3 **등록 취소**를 클릭합니다.
- 4 (선택 사항) ID 서버에서 등록 데이터를 삭제하려면 자격 증명을 입력합니다.
- 5 **ID 서비스** 섹션에서 **등록 취소**를 클릭합니다.

Orchestrator 서버 인스턴스를 성공적으로 등록 취소했습니다.

SSL 인증서 변경

기본적으로 Orchestrator 서버는 자체 서명된 SSL 인증서를 사용하여 Orchestrator 클라이언트와 원격으로 통신합니다. 회사 보안 정책에 따라 회사의 SSL 인증서를 사용해야 하는 경우 SSL 인증서를 변경할 수 있습니다.

신뢰할 수 있는 SSL Internet 연결을 통해 Orchestrator를 사용하려고 시도하고 웹 브라우저에서 제어 센터를 열면 Mozilla Firefox를 사용하는 경우 연결을 신뢰할 수 없다는 경고가 표시되거나 Internet Explorer를 사용하는 경우 웹 사이트의 보안 인증서에 문제가 있다는 경고가 표시됩니다.

이 웹 사이트를 계속 탐색합니다(권장하지 않음)을 클릭하면 신뢰할 수 있는 저장소의 SSL 인증서를 가져왔다 해도 웹 브라우저의 주소 표시줄에 적색의 인증서 오류 알림이 지속적으로 표시됩니다. 웹 브라우저에서 Orchestrator를 사용할 수 있으나 타사 시스템이 HTTPS를 통해 API에 액세스하려는 경우 올바르게 작동하지 않을 수 있습니다.

또한 Orchestrator 클라이언트를 시작하고 SSL 연결을 통해 Orchestrator 서버에 연결하려고 시도하면 인증서 경고가 표시될 수 있습니다.

이 문제는 상용 인증 기관에서 서명한 인증서를 설치하여 해결할 수 있습니다. Orchestrator 클라이언트에서 인증서 경고가 표시되지 않도록 하려면 루트 CA 인증서를 Orchestrator 클라이언트가 설치되어 있는 시스템의 Orchestrator 키 저장소에 추가합니다.

로컬 저장소에 인증서 추가

CA에서 인증서를 받은 후 이를 로컬 저장소에 추가해야 인증서 경고 또는 오류 메시지 없이 제어 센터가 작동됩니다.

이 워크플로는 Internet Explorer를 사용하여 인증서를 로컬 저장소에 추가하는 절차를 설명합니다.

- 1 Internet Explorer를 열고 `https://orchestrator_server_IP_or_DNS_name:8283/`로 이동합니다.
- 2 메시지가 표시되면 **이 웹 사이트를 계속 탐색합니다(권장하지 않음)**를 클릭합니다.
인증서 오류가 Internet Explorer 주소 표시줄의 오른쪽에 표시됩니다.
- 3 인증서 오류를 클릭하고 **인증서 보기**를 선택합니다.
- 4 **인증서 설치**를 클릭합니다.

- 5 인증서 가져오기 마법사의 시작 페이지에서 **다음**을 클릭합니다.
- 6 인증서 저장소 창에서 **모든 인증서를 다음 저장소에 배치**를 선택합니다.
- 7 **신뢰할 수 있는 루트 인증 기관**을 찾아 선택합니다.
- 8 마법사를 완료하고 Internet Explorer를 다시 시작합니다.
- 9 SSL 연결을 통해 Orchestrator 서버로 이동합니다.

더 이상 주의가 나타나지 않으며 주소 표시줄에 인증서 오류 메시지가 표시되지 않습니다.

VMware Service Manager와 같은 기타 애플리케이션 및 시스템은 SSL 연결을 통해 Orchestrator REST API에 액세스할 수 있어야 합니다.

Orchestrator Appliance 관리 사이트의 인증서 변경

Orchestrator Appliance에서는 Light HTTPd를 사용하여 고유한 관리 사이트를 실행합니다. 회사 보안 정책에 따라 회사의 SSL 인증서를 사용해야 하는 경우 Orchestrator Appliance 관리 사이트의 SSL 인증서를 변경할 수 있습니다.

필수 조건

기본적으로 Orchestrator Appliance SSL 인증서와 개인 키는 `/opt/vmware/etc/lighttpd/server.pem`에 있는 PEM 파일에 저장됩니다. 새 인증서를 설치하려면 새 SSL 인증서 및 개인 키를 Java 키 저장소에 서 PEM 파일로 내보내십시오.

프로시저

- 1 Orchestrator Appliance Linux 콘솔에 루트로 로그인합니다.
- 2 `/opt/vmware/etc/lighttpd/lighttpd.conf` 파일을 찾아 편집기에서 엽니다.
- 3 다음 줄을 찾습니다.


```
#### SSL engine
ssl.engine = "enable"
ssl.pemfile = "/opt/vmware/etc/lighttpd/server.pem"
```
- 4 `ssl.pemfile` 특성이 새 SSL 인증서 및 개인 키를 포함하는 PEM 파일을 지정하도록 변경합니다.
- 5 `lighttpd.conf` 파일을 저장합니다.
- 6 다음 명령을 실행하여 `light-httpd` 서버를 다시 시작합니다.


```
service vami-lighttp restart
```

Orchestrator Appliance 관리 사이트의 인증서가 변경되었습니다.

실행 중인 워크플로 취소

Orchestrator 서버가 중단되면 작업이 올바르게 수행되지 않을 수 있으므로 해당 워크플로는 취소됩니다.

필수 조건

제어 센터의 **시작 옵션** 페이지에서 Orchestrator 서버를 중지합니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **문제 해결**을 클릭합니다.

3 실행 중인 워크플로를 취소합니다.

옵션	설명
모든 워크플로 실행 취소	워크플로 ID를 입력하여 해당 워크플로에 대한 모든 토큰을 취소합니다. 서버가 중지되지 않은 경우 워크플로 토큰이 취소되지 않을 수 있습니다.
ID별로 실행 중인 워크플로 취소	취소하려는 모든 토큰 ID를 입력합니다. 토큰 ID를 쉼표로 구분하십시오. 서버가 중지되지 않은 경우 워크플로 토큰이 취소되지 않을 수 있습니다.
모든 토큰 취소	서버에서 실행 중인 모든 워크플로를 취소합니다. 이 옵션을 사용하려면 서버를 중지해야 합니다.

다음 서버 시작 시 워크플로는 취소됨 상태로 설정됩니다.

후속 작업

제어 센터의 **워크플로 검사** 페이지에서 워크플로가 취소되었는지 확인하십시오.

Orchestrator 서버 디버깅 사용

Orchestrator 서버를 디버그 모드에서 시작하여 플러그인 개발 시 문제를 디버깅할 수 있습니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **Orchestrator 디버깅**을 클릭합니다.
- 3 **디버그 사용**을 클릭합니다.
- 4 (선택 사항) 기본 포트와 다른 포트를 입력합니다.
- 5 (선택 사항) **일시 중단**을 클릭합니다.
이 옵션을 선택하면 Orchestrator 서버를 시작하기 전에 디버거를 연결해야 합니다.
- 6 **저장**을 클릭합니다.
- 7 제어 센터에서 시작 옵션 페이지를 열고 **다시 시작**을 클릭합니다.

Orchestrator 서버는 시작 시 지정된 포트에 원격 Java 디버거를 연결하기 전까지 일시 중단됩니다.

Orchestrator 구성 및 요소 백업

Orchestrator 구성의 스냅샷을 생성하고 해당 구성을 새 Orchestrator 인스턴스로 가져와 백업할 수 있습니다. 또한 수정된 Orchestrator 요소를 백업할 수도 있습니다.

표준 워크플로, 작업, 정책 또는 구성 요소를 편집한 후 상위 버전의 Orchestrator와 동일한 요소를 포함하는 패키지를 가져오면 요소에 대한 변경 사항이 손실됩니다. 업그레이드 후 수정된 사용자 지정 요소가 사용 가능하도록 하려면 해당 절차를 시작하기 전에 이를 패키지로 내보내야 합니다.

각 Orchestrator 서버 인스턴스는 고유 인증서를 포함하고 있으며 각 vCenter Server 플러그인 인스턴스는 고유 ID를 보유합니다. 인증서 및 고유 ID는 Orchestrator 서버 및 vCenter Server 플러그인의 ID를 정의합니다. Orchestrator 요소를 백업하지 않거나 Orchestrator 구성을 백업 용도로 내보내지 않는 경우 이러한 식별자를 변경합니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **구성 내보내기/가져오기**를 클릭합니다.
- 3 내보낼 파일의 유형을 선택합니다.

- 4 (선택 사항) 구성 파일 보호를 위한 암호를 입력합니다.
구성을 가져올 때 동일한 암호를 사용합니다.
- 5 **내보내기(Export)**를 클릭합니다.
- 6 Orchestrator 클라이언트 애플리케이션에 로그인합니다.
- 7 생성 또는 편집한 모든 Orchestrator 요소를 포함하는 패키지를 생성합니다.
 - a **패키지** 보기를 클릭합니다.
 - b 패키지 목록의 제목 표시줄에서 메뉴 버튼을 클릭하고 **패키지 추가**를 선택합니다.
 - c 새 패키지 이름을 입력하고 **확인**을 클릭합니다.
패키지 이름에 대한 구문은 *domain.your_company.folder.package_name*입니다.
예: com.vmware.myfolder.mypackage.
 - d 패키지를 마우스 오른쪽 버튼으로 클릭하고 **편집**을 선택합니다.
 - e **일반** 탭에서 패키지에 대한 설명을 추가합니다.
 - f **워크플로** 탭에서 패키지에 워크플로를 추가합니다.
 - g (선택 사항) 패키지에 정책 템플릿, 작업, 구성 요소, 리소스 요소 및 플러그인을 추가합니다.
- 8 패키지를 내보냅니다.
 - a 내보내려는 패키지를 마우스 오른쪽 버튼으로 클릭하고 **패키지 내보내기**를 선택합니다.
 - b 패키지를 저장하려는 위치를 찾아 선택하고 **열기**를 클릭합니다.
 - c (선택 사항) 해당 인증서를 사용하여 패키지에 서명합니다.
 - d (선택 사항) 내보낸 패키지에 제한을 적용합니다.
 - e (선택 사항) 내보낸 패키지의 콘텐츠에 대한 제한을 적용하려면 필요에 따라 옵션을 선택 해제합니다.

옵션	설명
버전 기록 내보내기	패키지의 버전 기록은 내보낼 수 없습니다.
구성 설정 값 내보내기	패키지 구성 요소의 특성 값은 내보낼 수 없습니다.
글로벌 태그 내보내기	패키지의 글로벌 태그는 내보낼 수 없습니다.

 - f **저장**을 클릭합니다.
- 9 Orchestrator 구성을 새 Orchestrator 서버 인스턴스로 가져옵니다.
 - a 새 Orchestrator 인스턴스의 제어 센터에 **관리자**로 로그인합니다.
 - b **구성 내보내기/가져오기**를 클릭하고 **구성 가져오기** 탭으로 이동합니다.
 - c 이전 설치에서 내보낸 .zip 파일을 찾아 선택합니다.
 - d 구성을 내보낼 때 사용한 암호를 입력합니다.
암호를 지정하지 않았다면 이 단계는 필요하지 않습니다.
 - e **가져오기**를 클릭합니다.
- 10 새 Orchestrator 인스턴스로 내보낸 패키지를 가져옵니다.
 - a 새 Orchestrator 인스턴스의 Orchestrator 클라이언트 애플리케이션에 로그인합니다.
 - b Orchestrator 클라이언트의 드롭다운 메뉴에서 **관리**를 선택합니다.
 - c **패키지** 보기를 클릭합니다.

- d 왼쪽 창에서 마우스 오른쪽 버튼을 클릭하고 **패키지 가져오기**를 선택합니다.
- e 가져오려는 패키지를 찾은 다음 선택하고 **열기**를 클릭합니다.
내보내기에 대한 인증서 정보가 표시됩니다.
- f 패키지 가져오기 세부 정보를 검토하고 **가져오기** 또는 **가져오기 및 제공자 신뢰**를 선택합니다.
패키지 가져오기 보기가 표시됩니다. 가져온 패키지 요소의 버전이 서버에 있는 버전보다 상위 버전인 경우 시스템이 가져올 요소를 선택합니다.
- g 가져오지 않을 요소는 선택 해제합니다.
예를 들어 상위 버전이 존재하는 사용자 지정 요소를 선택 해제합니다.
- h (선택 사항) 패키지의 구성 요소 특성 값을 가져오지 않을 경우 **구성 설정 값 가져오기** 확인란을 선택 해제합니다.
- i 드롭다운 메뉴에서 패키지의 태그를 가져올지 여부를 선택합니다.

옵션	설명
태그 가져오기 및 기존 값 유지	기존 태그 값을 덮어쓰지 않고 패키지에서 태그를 가져옵니다.
태그 가져오기 및 기존 값 덮어쓰기	패키지에서 태그를 가져오고 기존 값을 덮어씁니다.
태그 가져오지 않음	패키지에서 태그를 가져오지 않습니다.

- j **선택한 요소 가져오기**를 클릭합니다.

vRealize Orchestrator 백업 및 복원

vSphere Data Protection을 사용하여 vRealize Orchestrator 인스턴스를 포함하는 가상 시스템 (VM)을 백업 및 복원할 수 있습니다.

vSphere Data Protection은 vSphere 환경에서 사용할 수 있는 VMware 디스크 기반 백업 및 복원 솔루션입니다. vSphere Data Protection은 vCenter Server와 완전히 통합됩니다.

vSphere Data Protection을 통해 백업 작업을 관리하고 중복 제거된 대상 저장 위치에 백업을 저장할 수 있습니다. vSphere Data Protection을 배포 및 구성한 후 vSphere Web Client 인터페이스를 통해 vSphere Data Protection에 액세스하여 백업 및 가상 시스템의 복구를 선택, 스케줄링, 구성 및 관리할 수 있습니다. vSphere Data Protection은 백업을 수행할 때 가상 시스템에 대한 중지 상태의 스냅샷을 생성합니다. 모든 백업 작업에 중복 제거도 자동으로 수행됩니다.

vSphere Data Protection 배포 및 구성 방법에 대한 자세한 내용은 vSphere Data Protection 관리 설명서를 참조하십시오.

vRealize Orchestrator 백업

vRealize Orchestrator 인스턴스를 가상 시스템으로 백업할 수 있습니다.

전체 VM 백업 이전에 데이터베이스를 내보낼 수 있습니다. 데이터베이스 내보내기 방법에 대한 자세한 내용은 **“Orchestrator 데이터베이스 내보내기,”** (41 페이지)을 참조하십시오.

vRealize Orchestrator 및 외부 데이터베이스가 서로 다른 시스템에 있는 경우 각 데이터베이스를 개별로 백업해야 합니다.

참고 단일 제품의 모든 VM 구성 요소가 함께 백업되도록 하려면 vRealize Orchestrator 환경의 VM을 단일 vCenter Server 폴더에 저장하고 해당 폴더에 대한 백업 정책 작업을 생성합니다.

필수 조건

- vSphere Data Protection 장치가 배포되고 구성되었는지 확인합니다.
vSphere Data Protection 배포 및 구성 방법에 대한 자세한 내용은 vSphere Data Protection 관리 설명서를 참조하십시오.

- vSphere Web Client를 사용하여 환경을 관리하는 vCenter Server 인스턴스에 로그인합니다. vSphere Data Protection 구성 중 사용된 관리자 권한이 있는 사용자로 로그인합니다.

프로시저

- 1 vSphere Web Client 홈 페이지에서 **vSphere Data Protection**을 클릭합니다.
- 2 **VDP 장치** 드롭다운 메뉴에서 vSphere Data Protection 장치를 선택하고 **연결**을 클릭합니다.
- 3 **시작** 탭에서 **백업 작성 작업**을 클릭합니다.
- 4 **게스트 이미지**를 클릭하여 vRealize Orchestrator 인스턴스를 백업하고 **다음**을 클릭합니다.
- 5 **전체 이미지**를 선택하여 전체 가상 시스템을 백업하고 **다음**을 클릭합니다.
- 6 **가상 시스템** 트리를 확장하고 vRealize Orchestrator VM의 확인란을 선택합니다.
- 7 프롬프트 메시지에 따라 백업 스케줄, 보존 정책 및 백업 작업의 이름을 설정합니다.

가상 시스템의 백업 및 복원 방법에 대한 자세한 내용은 vSphere Data Protection 관리 설명서를 참조하십시오.

백업 작업이 **백업** 탭의 백업 작업 목록에 표시됩니다.

- 8 (선택 사항) **백업** 탭을 열고 해당 백업 작업을 선택한 다음 **지금 백업**을 클릭하여 vRealize Orchestrator를 백업할 수 있습니다.

참고 또는, 설정한 스케줄에 따라 자동으로 백업이 시작되도록 대기할 수 있습니다.

백업 프로세스가 **최근 작업** 페이지에 표시됩니다.

VM 이미지가 **복원** 탭의 백업 목록에 표시됩니다.

후속 작업

복원 탭을 열고 VM 이미지가 백업 목록에 있는지 확인합니다.

vRealize Orchestrator 인스턴스 복원

원래 위치 또는 동일한 vCenter Server의 다른 위치에서 vRealize Orchestrator 인스턴스를 복원할 수 있습니다.

vRealize Orchestrator 및 외부 데이터베이스가 서로 다른 시스템에서 실행되는 경우 먼저 데이터베이스를 복원한 후 vRealize Orchestrator VM을 복원해야 합니다.

필수 조건

- vSphere Data Protection 장치가 배포되고 구성되었는지 확인합니다. vSphere Data Protection 배포 및 구성 방법에 대한 자세한 내용은 vSphere Data Protection 관리 설명서를 참조하십시오.
- vRealize Orchestrator 인스턴스를 백업합니다. [“vRealize Orchestrator 백업,”](#) (80 페이지) 항목을 참조하십시오.
- vSphere Web Client를 사용하여 환경을 관리하는 vCenter Server 인스턴스에 로그인합니다. vSphere Data Protection 구성 중 사용된 관리자 권한이 있는 사용자로 로그인합니다.

프로시저

- 1 vSphere Web Client 홈 페이지에서 **vSphere Data Protection**을 클릭합니다.
- 2 **VDP 장치** 드롭다운 메뉴에서 vSphere Data Protection 장치를 선택하고 **연결**을 클릭합니다.
- 3 **복원** 탭을 엽니다.

- 4 백업 작업 목록에서 복원하려는 vRealize Orchestrator 백업을 선택합니다.

참고 VM이 여러 개 있는 경우 동시에 복원하여 동기화해야 합니다.

- 5 동일한 vCenter Server에서 vRealize Orchestrator 인스턴스를 복원하려면 **복원** 아이콘을 클릭하고 vRealize Orchestrator를 복원하려는 vCenter Server의 위치를 설정하라는 메시지를 따릅니다.

전원 켜기를 선택 취소하여 해당 장치가 전원이 켜지는 마지막 구성 요소가 되도록 해야 합니다. 가상 장치의 백업 및 복원 방법에 대한 자세한 내용은 vSphere Data Protection 관리 설명서를 참조하십시오.

복원이 성공적으로 초기화되었다는 메시지가 표시됩니다.

- 6 (선택 사항) 데이터베이스 호스트가 외부에 있고 로드 밸런서 구성을 복원하려는 경우 데이터베이스 호스트를 켭니다.

- 7 vRealize Orchestrator Appliance를 켭니다.

복원된 vRealize Orchestrator VM이 vCenter Server 인벤토리에 표시됩니다.

후속 작업

제어 센터의 **구성 검증** 페이지를 열어 vRealize Orchestrator가 올바르게 구성되었는지 확인합니다.

Site Recovery Manager 를 사용한 Orchestrator의 재해 복구

vRealize Orchestrator를 보호하려면 Site Recovery Manager를 구성해야 합니다. Site Recovery Manager에 대한 일반 구성 작업을 완료하여 해당 보호를 구현합니다.

환경 준비

Site Recovery Manager 구성을 시작하기 전에 다음 사전 요구 사항을 충족하는지 확인하십시오.

- 보호된 복구 사이트에 vSphere 5.5가 설치되어 있는지 확인합니다.
- Site Recovery Manager 5.8을 사용하고 있는지 확인합니다.
- vRealize Orchestrator가 구성되어 있는지 확인합니다.

vSphere Replication 에 대한 가상 시스템 구성

Site Recovery Manager를 사용하려면 vSphere Replication에 대한 가상 시스템 또는 어레이 기반 복제를 구성해야 합니다.

다음 단계에 따라 필요한 가상 시스템에서 vSphere Replication을 활성화합니다.

프로시저

- 1 vSphere Web Client에서 vSphere Replication이 활성화되어야 하는 가상 시스템을 선택하고 **작업 > 모든 vSphere Replication 작업 > 복제 구성**을 클릭합니다.
- 2 복제 유형 창에서 **vCenter Server로 복제**를 선택하고 **다음**을 클릭합니다.
- 3 대상 사이트 창에서 복구 사이트용 vCenter를 선택하고 **다음**을 클릭합니다.
- 4 복제 서버 창에서 vSphere Replication서버를 선택하고 **다음**을 클릭합니다.
- 5 대상 위치 창에서 **편집**을 클릭하고 복제된 파일이 저장될 대상 데이터스토어를 선택한 후 **다음**을 클릭합니다.
- 6 복제 옵션 창의 기본 설정을 유지하고 **다음**을 클릭합니다.

- 7 복구 설정 창에서 **복구 지점 목표(RPO)** 및 **특정 시점 인스턴스**에 대한 시간을 입력하고 **다음**을 클릭합니다.
- 8 완료 준비 창에서 설정 내용을 확인하고 **완료**를 클릭합니다.
- 9 이 단계를 vSphere Replication이 활성화되어야 하는 모든 가상 시스템에서 반복합니다.

보호 그룹 만들기

보호 그룹을 만들어 Site Recovery Manager를 활성화하여 가상 시스템을 보호할 수 있습니다.

보호 그룹을 만드는 경우 작업이 예상대로 완료될 때까지 기다립니다. Site Recovery Manager가 보호 그룹을 만들고 그룹에서 가상 시스템의 보호가 성공적으로 수행되는지 확인합니다.

필수 조건

다음 작업 중 하나를 수행했는지 확인하십시오.

- 어레이 기반 복제가 구성된 가상 시스템을 데이터스토어에 포함
- 가상 시스템에 vSphere Replication 구성
- 위 사항 전부 또는 일부를 조합하여 수행

프로시저

- 1 vSphere Web Client에서 **사이트 복구 > 보호 그룹**을 선택합니다.
- 2 **개체** 탭에서 아이콘을 클릭하여 보호 그룹을 만듭니다.
- 3 보호 그룹 유형 페이지에서 보호된 사이트를 선택하고 복제 유형을 선택한 후 **다음**을 클릭합니다.

옵션	작업
어레이 기반 복제 그룹	어레이 기반 복제(ABR)를 선택하고 어레이 쌍을 선택합니다.
vSphere Replication 보호 그룹	vSphere Replication을 선택합니다.

- 4 데이터스토어 그룹 또는 가상 시스템을 선택하여 보호 그룹에 추가합니다.

옵션	작업
어레이 기반 복제 보호 그룹	데이터스토어 그룹을 선택하고 다음 을 클릭합니다.
vSphere Replication 보호 그룹	목록에서 가상 시스템을 선택하고 다음 을 클릭합니다.

vSphere Replication 보호 그룹을 생성하면 vSphere Replication에 대해 구성되거나 보호 그룹에 아직 없는 가상 시스템만이 목록에 표시됩니다.

- 5 설정을 검토하고 **마침**을 클릭합니다.

보호 그룹 아래 **개체** 탭에서 보호 그룹의 생성 진행 상태를 모니터링할 수 있습니다.

- Site Recovery Manager가 인벤토리 매핑을 보호된 가상 시스템에 올바르게 적용했다면 보호 그룹의 보호 상태는 정상입니다.
- Site Recovery Manager가 스토리지 정책과 연관된 모든 가상 시스템을 올바르게 보호했다면 보호 그룹의 보호 상태는 정상입니다.

복구 계획 만들기

복구 계획을 만들어 Site Recovery Manager의 가상 시스템 복구 방식을 설정합니다.

프로시저

- 1 vSphere Web Client에서 **사이트 복구 > 복구 계획**을 선택합니다.

- 2 **개체** 탭에서 아이콘을 클릭하여 복구 계획을 만듭니다.
- 3 계획의 이름 및 설명을 입력하고 폴더를 선택한 후 **다음**을 클릭합니다.
- 4 복구 사이트를 선택하고 **다음**을 클릭합니다.
- 5 메뉴에서 그룹 유형을 선택합니다.

옵션	설명
VM 보호 그룹	이 옵션을 선택하여 어레이 기반 복제 및 vSphere Replication 보호 그룹을 포함하는 복구 계획을 작성합니다.
스토리지 정책 보호 그룹	이 옵션을 선택하여 스토리지 정책 보호 그룹을 포함하는 복구 계획을 작성합니다.

기본값은 **VM 보호 그룹**입니다.

참고 확장된 스토리지를 사용하는 경우 그룹 유형에 대한 **스토리지 정책 보호 그룹**을 선택합니다.

- 6 복구할 계획에 대한 하나 이상의 보호 그룹을 선택하고 **다음**을 클릭합니다.
- 7 **네트워크 테스트** 값을 클릭하고 복구 테스트 동안 사용할 네트워크를 선택한 후 **다음**을 클릭합니다.
기본 옵션은 분리된 네트워크 자동 생성입니다.
- 8 요약 정보를 검토하고 **마침**을 클릭하여 복구 계획을 만듭니다.

폴더의 복구 계획 구성

복구 계획을 구성할 폴더를 생성할 수 있습니다.

복구 계획을 폴더에 구성하면 복구 계획이 여러 개인 경우 유용합니다. 복구 계획을 폴더에 배치하고 다른 사용자 또는 그룹에 대한 각 폴더에 다른 권한을 부여하여 복구 계획에 대한 액세스를 제한할 수 있습니다.

프로시저

- 1 vSphere Web Client의 홈 보기에서 **사이트 복구**를 클릭합니다.
- 2 **인벤토리 트리**를 확장하고 **복구 계획**을 클릭합니다.
- 3 **관련 개체** 탭을 선택하고 **폴더**를 클릭합니다.
- 4 **폴더 생성** 아이콘을 클릭하고 생성하려는 폴더의 이름을 입력한 후 **확인**을 클릭합니다.
- 5 새 복구 계획 또는 기존 복구 계획을 폴더에 추가합니다.

옵션	설명
새 복구 계획 생성	폴더를 마우스 오른쪽 버튼으로 클릭하고 복구 계획 생성 을 선택합니다.
기존 복구 계획 추가	인벤토리 트리에서 복구 계획을 폴더로 끌어 놓습니다.

- 6 (선택 사항) 폴더 이름을 바꾸거나 폴더를 삭제하려면 폴더를 마우스 오른쪽 버튼으로 클릭하고 **폴더 이름 변경** 또는 **폴더 삭제**를 선택합니다.
폴더는 비어 있는 경우에만 삭제할 수 있습니다.

복구 계획 편집

복구 계획을 편집하여 해당 복구 계획을 만들 때 지정한 속성을 변경할 수 있습니다. 보호된 사이트 또는 복구 사이트에서 복구 계획을 편집할 수 있습니다.

프로시저

- 1 vSphere Web Client에서 **사이트 복구 > 복구 계획**을 선택합니다.

- 2 복구 계획을 마우스 오른쪽 버튼으로 클릭하고 **계획 편집**을 선택합니다.
모니터 탭의 **복구 단계** 보기에서 **복구 계획 편집** 아이콘을 클릭하여 복구 계획을 편집할 수도 있습니다.
- 3 (선택 사항) **복구 계획 이름** 텍스트 상자에서 계획의 이름 또는 설명을 변경하고 **다음**을 클릭합니다.
- 4 복구 사이트 페이지에서 **다음**을 클릭합니다.
복구 사이트는 변경할 수 없습니다.
- 5 (선택 사항) 복구 계획에 추가할 하나 이상의 보호 그룹을 선택 또는 선택 해제하거나 계획에서 보호 그룹을 제거하고 **다음**을 클릭합니다.
- 6 (선택 사항) 테스트 네트워크를 클릭하여 복구 사이트의 다른 테스트 네트워크를 선택하고 **다음**을 클릭합니다.
- 7 요약 정보를 검토하고 **마침**을 클릭하여 복구 계획에 대해 지정된 변경 내용을 수행합니다.
최근 작업 보기에서 계획 업데이트를 모니터링할 수 있습니다.

시스템 속성 설정

시스템 속성을 설정하여 기본 Orchestrator 동작을 변경할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- “Orchestrator 클라이언트에 대한 비관리자의 액세스 사용 안 함,” (87 페이지)
- “워크플로 및 작업에 대한 서버 파일 시스템 액세스 설정,” (88 페이지)
- “워크플로 및 작업에 대한 운영 체제 명령의 액세스 설정,” (89 페이지)
- “Java 클래스에 JavaScript 액세스 설정,” (90 페이지)
- “사용자 지정 시간 초과 속성 설정,” (90 페이지)

Orchestrator 클라이언트에 대한 비관리자의 액세스 사용 안 함

Orchestrator 관리자 그룹의 구성원이 아닌 모든 사용자의 Orchestrator 클라이언트에 대한 액세스를 거부하도록 Orchestrator 서버를 구성할 수 있습니다.

기본적으로 실행 권한을 부여 받은 모든 사용자는 Orchestrator 클라이언트에 연결할 수 있습니다. 그러나 Orchestrator 구성 시스템 속성을 설정하여 Orchestrator 클라이언트에 대한 액세스를 Orchestrator 관리자로 제한할 수 있습니다.

중요 해당 설정이 구성되지 않았거나 잘못 설정된 경우 Orchestrator는 Orchestrator 클라이언트에 대한 모든 사용자의 액세스를 허용합니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **시스템 속성**을 클릭합니다.
- 3 **추가** 아이콘(+)을 클릭합니다.
- 4 키 텍스트 상자에 `com.vmware.o11n.smart-client-disabled`를 입력합니다.
- 5 값 텍스트 상자에 `true`를 입력합니다.
- 6 (선택 사항) **설명** 텍스트 상자에 **Orchestrator 클라이언트 연결 사용 안 함**을 입력합니다.
- 7 **추가**를 클릭합니다.
- 8 팝업 메뉴에서 **변경 내용 저장**을 클릭합니다.
성공적으로 저장했다는 메시지가 표시됩니다.
- 9 Orchestrator 서버를 다시 시작합니다.

Orchestrator 관리자 그룹의 구성원이 아닌 모든 사용자의 Orchestrator 클라이언트에 대한 액세스를 비활성화했습니다.

워크플로 및 작업에 대한 서버 파일 시스템 액세스 설정

Orchestrator에서 워크플로 및 작업은 특정 파일 시스템 디렉토리에 대해 액세스가 제한되어 있습니다. `js-io-rights.conf` Orchestrator 구성 파일을 수정하여 서버 파일 시스템의 다른 부분으로 액세스를 확장할 수 있습니다.

Orchestrator 시스템에 쓰기 액세스 권한을 허용하는 `js-io-rights.conf` 파일의 규칙

`js-io-rights.conf` 파일은 서버 파일 시스템의 정의된 디렉토리에 쓰기 액세스 권한을 허용하는 규칙을 포함하고 있습니다.

`js-io-rights.conf` 파일의 필수 콘텐츠

`js-io-rights.conf` 파일의 끝 줄에는 다음 정보가 포함되어야 합니다.

- 권한 허용 및 거부 여부를 나타내는 더하기(+) 또는 빼기(-) 표시
- 읽기(r), 쓰기(w) 및 실행(x) 권한 수준
- 권한이 적용되는 경로

`js-io-rights.conf` 파일의 기본 콘텐츠

Orchestrator Appliance의 `js-io-rights.conf` 구성 파일에 대한 기본 콘텐츠는 다음과 같습니다.

```
-rwx /
+rxw /var/run/vco
-rwx /etc/vco/app-server/security/
+rx /etc/vco
+rx /var/log/vco/
```

기본 `js-io-rights.conf` 구성 파일의 첫 두 줄에서 다음과 같은 액세스 권한을 허용합니다.

```
-rwx /                파일 시스템에 대한 모든 액세스가 거부됩니다.
+rxw /var/run/vco    /var/run/vco 디렉토리에서 쓰기, 읽기 및 실행 액세스가 허용됩니다.
```

`js-io-rights.conf` 파일 규칙

Orchestrator는 `js-io-rights.conf` 파일에 나타난 순서대로 액세스 권한을 확인합니다. 각 줄은 이전 줄을 재정의할 수 있습니다.

중요 `js-io-rights.conf` 파일에서 `+rxw /`를 설정하여 파일 시스템의 모든 부분에 대한 액세스를 허용할 수 있습니다. 그러나 이는 보안 위험을 높일 수 있습니다.

워크플로 및 작업에 대한 서버 파일 시스템 액세스 설정

워크플로 및 Orchestrator API가 액세스할 수 있는 서버 파일 시스템의 부분을 변경하려면 `js-io-rights.conf` 구성 파일을 수정합니다. `js-io-rights.conf` 파일은 워크플로가 Orchestrator 서버 파일 시스템에 액세스하려고 시도하면 생성됩니다.

프로시저

- 1 루트로 Orchestrator Appliance Linux 콘솔에 로그인합니다.
- 2 `/etc/vco/app-server`로 이동합니다.

- 3 텍스트 편집기에서 `js-io-rights.conf` 구성 파일을 엽니다.
- 4 필요한 줄을 `js-io-rights.conf` 파일에 추가하여 파일 시스템 영역에 대한 액세스를 허용하거나 거부합니다.

예를 들어 다음 줄은 `/path_to_folder/noexec` 디렉토리에서 실행 권한을 거부합니다.

```
-x /path_to_folder/noexec
```

`/path_to_folder/noexec`는 실행 권한을 유지하지만 `/path_to_folder/noexec/bar`는 실행 권한을 유지하지 않습니다. 두 디렉토리 모두 읽기 및 쓰기가 가능합니다.

워크플로 및 Orchestrator API에 대해 파일 시스템의 액세스 권한을 수정했습니다.

워크플로 및 작업에 대한 운영 체제 명령의 액세스 설정

Orchestrator API는 Orchestrator 서버 호스트 운영 체제에서 명령을 실행하는 스크립팅 클래스인 `Command`를 제공합니다. Orchestrator 서버 호스트에 대한 무단 액세스를 방지하기 위해 Orchestrator 애플리케이션에는 기본적으로 `Command` 클래스를 실행할 권한이 없습니다. Orchestrator 애플리케이션이 호스트 운영 체제에서 명령을 실행하는 데 권한이 필요한 경우 `Command` 스크립팅 클래스를 활성화할 수 있습니다.

Orchestrator 구성 시스템 속성을 설정하여 `Command` 클래스에 대한 사용 권한을 부여할 수 있습니다.

프로시저

- 1 제어 센터에 **관리자**로 로그인합니다.
- 2 **시스템 속성**을 클릭합니다.
- 3 **추가** 아이콘(+)을 클릭합니다.
- 4 키 텍스트 상자에 `com.vmware.js.allow-local-process`를 입력합니다.
- 5 값 텍스트 상자에 `true`를 입력합니다.
- 6 설명 텍스트 상자에 시스템 속성에 대한 설명을 입력합니다.
- 7 **추가**를 클릭합니다.
- 8 팝업 메뉴에서 **변경 내용 저장**을 클릭합니다.
성공적으로 저장했다는 메시지가 표시됩니다.
- 9 Orchestrator 서버를 다시 시작합니다.

Orchestrator 서버 호스트 운영 시스템에서 로컬 명령을 실행할 수 있는 권한이 Orchestrator 애플리케이션에 부여되었습니다.

참고 `com.vmware.js.allow-local-process` 시스템 속성을 `true`로 설정하면 `Command` 스크립팅 클래스가 파일 시스템의 모든 위치에서 쓰기가 허용됩니다. 이 속성은 `js-io-rights.conf` 파일에서 `Command` 스크립팅 클래스 전용으로 설정한 모든 파일 시스템 액세스 권한을 재정의합니다. `js-io-rights.conf` 파일에서 설정한 파일 시스템 액세스 권한은 여전히 `Command` 외 모든 스크립팅 클래스에 적용됩니다.

Java 클래스에 JavaScript 액세스 설정

기본적으로 Orchestrator에서는 제한된 Java 클래스 집합으로 JavaScript 액세스가 제한됩니다. 보다 광범위한 Java 클래스에 대한 JavaScript 액세스가 필요한 경우 이 액세스를 허용하도록 Orchestrator 시스템 속성을 설정해야 합니다.

JavaScript 엔진에 Java 가상 시스템(JVM)에 대한 전체 액세스 권한을 허용하면 잠재적 보안 문제가 나타납니다. 잘못된 형식 또는 악성 스크립트가 Orchestrator 서버를 실행하는 사용자가 액세스하는 모든 시스템 구성 요소에 액세스할 수 있습니다. 따라서 Orchestrator JavaScript 엔진은 기본적으로 `java.util.*` 패키지의 클래스에만 액세스할 수 있습니다.

JavaScript가 `java.util.*` 패키지 외부 클래스에 액세스하게 해야 한다면 JavaScript 액세스를 허용할 Java 패키지를 구성 파일에 나열하십시오. 그런 다음 이 파일을 가리키도록 `com.vmware.scripting.rhino-class-shutter-file` 시스템 속성을 설정하십시오.

프로시저

- JavaScript 액세스를 허용할 Java 패키지 목록을 저장하려면 텍스트 구성 파일을 작성합니다.
예를 들어 JavaScript가 `java.net` 패키지의 모든 클래스와 `java.lang.Object` 클래스에 액세스하게 하려면 다음 내용을 파일에 추가합니다.

```
java.net.*
java.lang.Object
```
- 구성 파일에 적절한 이름을 지정해 적절한 위치에 저장합니다.
- 제어 센터에 **관리자**로 로그인합니다.
- 시스템 속성**을 클릭합니다.
- 추가** 아이콘(+)을 클릭합니다.
- 키** 텍스트 상자에 `com.vmware.scripting.rhino-class-shutter-file`을 입력합니다.
- 값** 텍스트 상자에 구성 파일의 경로를 입력합니다.
- 설명** 텍스트 상자에 시스템 속성에 대한 설명을 입력합니다.
- 추가**를 클릭합니다.
- 팝업 메뉴에서 **변경 내용 저장**을 클릭합니다.
성공적으로 저장했다는 메시지가 표시됩니다.
- Orchestrator 서버를 다시 시작합니다.

JavaScript 엔진이 지정한 Java 클래스에 액세스할 수 있습니다.

사용자 지정 시간 초과 속성 설정

vCenter Server가 오버로드되면 Orchestrator 서버로 응답을 반환하는 시간이 기본으로 지정된 20000밀리초보다 오래 걸리게 됩니다. 이를 방지하려면 Orchestrator 구성 파일을 수정하여 기본 시간 초과 기간을 늘려야 합니다.

기본 시간 초과 기간이 특정 작업 완료 전에 만료되면 Orchestrator 서버 로그에 오류가 포함됩니다.

```
Operation 'getPropertyContent' total time : '5742228' for 1823 calls, mean time : '3149.0', min time : '0',
max time : '32313' Timeout, unable to get property 'info' com.vmware.vmo.plugin.vi4.model.TimeoutException
```

프로시저

- 제어 센터에 **관리자**로 로그인합니다.

- 2 시스템 속성을 클릭합니다.
- 3 추가 아이콘(+)을 클릭합니다.
- 4 키 텍스트 상자에 `com.vmware.vmo.plugin.vi4.waitUpdatesTimeout`을 입력합니다.
- 5 값 텍스트 상자에 새 시간 초과 기간을 밀리초 단위로 입력합니다.
- 6 (선택 사항) 설명 텍스트 상자에 시스템 속성에 대한 설명을 입력합니다.
- 7 추가를 클릭합니다.
- 8 팝업 메뉴에서 **변경 내용 저장**을 클릭합니다.
성공적으로 저장했다는 메시지가 표시됩니다.
- 9 Orchestrator 서버를 다시 시작합니다.

설정된 값이 기본 시간 초과로 설정된 값인 20000밀리초를 재정의합니다.

이후 작업 정보

vRealize Orchestrator를 설치 및 구성하면 Orchestrator를 사용하여 가상 환경의 관리와 연관되어 자주 반복되는 프로세스를 자동화할 수 있습니다.

- Orchestrator 클라이언트에 로그인하여 vCenter Server 인벤토리 개체 또는 Orchestrator가 플러그인을 통해 액세스하는 기타 개체에서 워크플로를 실행 및 스케줄링합니다. VMware vRealize Orchestrator 클라이언트사용을 참조하십시오.
- 표준 Orchestrator 워크플로를 복제 및 수정하고 자체적으로 작업 및 워크플로를 작성하여 vCenter Server에서 작업을 자동화합니다.
- 플러그인 및 웹 서비스를 개발하여 Orchestrator 플랫폼을 확장합니다.
- vSphere Web Client를 사용하여 vSphere 인벤토리 개체에서 워크플로를 실행합니다.

Orchestrator Appliance 웹 콘솔에서 Orchestrator 클라이언트에 로그인

일반적인 관리 작업을 수행하거나 워크플로를 편집하고 생성하려면 Orchestrator 클라이언트 인터페이스에 로그인해야 합니다.

Orchestrator 클라이언트 인터페이스는 관리 권한을 가지고 있으며 워크플로, 작업 및 기타 사용자 지정 요소를 개발하고자 하는 개발자를 위해 설계되었습니다.

중요 Orchestrator Appliance 서버의 시계와 Orchestrator 클라이언트 시스템의 시계를 동기화해야 합니다.

필수 조건

- Orchestrator Appliance를 다운로드 및 배포합니다.
- 애플리케이션이 가동되어 실행 중인지 확인합니다.
- Orchestrator 클라이언트를 실행할 워크스테이션에 64비트 Java를 설치합니다.

참고 32비트 Java는 지원되지 않습니다.

프로시저

- 1 웹 브라우저에서 Orchestrator Appliance 가상 시스템의 IP 주소로 이동합니다.
http://orchestrator_appliance_ip
- 2 **Orchestrator 클라이언트 시작**을 클릭합니다.
- 3 **호스트 이름** 텍스트 상자에 Orchestrator Appliance의 IP 또는 도메인 이름을 입력합니다.
Orchestrator Appliance의 IP 주소가 기본적으로 표시됩니다.

- 4 Orchestrator 클라이언트 사용자 이름과 암호를 사용하여 로그인합니다.

vRealize Automation 인증, vCenter Single Sign-On 또는 다른 디렉토리 서비스를 인증 방법으로 사용하는 경우 해당 자격 증명을 입력하여 Orchestrator 클라이언트에 로그인합니다.

- 5 보안 경고 창에서 인증서 경고를 처리할 옵션을 선택합니다.

Orchestrator 클라이언트는 SSL 인증서를 사용하여 Orchestrator 서버와 통신합니다. 신뢰할 수 있는 CA는 설치하는 동안에는 인증서에 서명하지 않습니다. Orchestrator 서버에 연결할 때마다 인증서 경고가 수신됩니다.

옵션	설명
무시	현재 SSL 인증서를 계속 사용합니다. 같은 Orchestrator 서버에 다시 연결하거나, 원격 Orchestrator 서버와 워크플로를 동기화하려고 시도하면 경고 메시지가 다시 나타납니다.
취소	창을 닫고 로그인 프로세스를 중지합니다.
이 인증서를 설치하고 이와 관련된 보안 경고를 더 이상 표시 안 함	인증서를 설치하고 보안 경고를 더 이상 표시하지 않으려면 이 확인란을 선택하고 무시 를 클릭합니다.

기본 SSL 인증서를 CA가 서명한 인증서로 변경할 수 있습니다. SSL 인증서를 변경하는 방법에 대한 자세한 내용은 VMware vRealize Orchestrator 설치 및 구성을 참조하십시오.

후속 작업

패키지를 가져오거나, 워크플로를 시작하거나, 시스템에 대한 루트 액세스 권한을 설정할 수 있습니다.

색인

A

ASCII가 아닌 문자 **17, 39**

C

Command 스크립팅 클래스 **89**

I

i18n 지원 **17**

ISO 이미지 **25**

J

JavaScript **90**

js-io-rights.conf 파일

규칙 **88**

컨텐츠 **88**

L

LDAP

LDAP 서버 서명 요구 사항 **32**

SSL 인증서 **32**

인증 **33, 34**

LDAP 오류

525 **35**

52e **35**

530 **35**

531 **35**

532 **35**

533 **35**

701 **35**

773 **35**

775 **35**

O

Orchestrator, 확장으로 등록 **75**

Orchestrator API

js-io-rights.conf 파일 **88**

파일 시스템 액세스 **88**

Orchestrator Appliance

다운로드 **21**

메모리 **15**

배포 **21**

시스템 요구 사항 **15**

암호 변경 **23**

업그레이드 **24, 26**

하드 디스크 **15**

Orchestrator Appliance 다운로드 **21**

Orchestrator Appliance 배포 **21**

Orchestrator Appliance 암호 변경 **23**

Orchestrator VM 복원 **81**

Orchestrator 개요 **11**

Orchestrator 구성 **73**

Orchestrator 구성 마이그레이션 **57**

Orchestrator 마이그레이션 **65, 66, 68, 70**

Orchestrator 백업 **80**

Orchestrator 버전 **16**

Orchestrator 복원 **80, 81**

Orchestrator 서버 디버깅 **78**

Orchestrator 서버 백업 **80**

Orchestrator 서버 복원 **80, 81**

Orchestrator 설치 **21**

Orchestrator 아키텍처 **13**

Orchestrator 업그레이드 **21**

Orchestrator 요소, 백업 **78**

Orchestrator 인증 등록 취소 **76**

Orchestrator 클라이언트, 액세스 사용 안 함 **87**

Orchestrator 클라이언트에 대한 액세스 사용 안 함 **87**

Orchestrator 클러스터, 업그레이드 **27, 28**

Orchestrator 플러그인 **14**

OS **16**

R

REST API

SSL 인증서 가져오기 **52**

SSL 인증서 관리 **51**

SSL 인증서 삭제 **51**

키 저장소 삭제 **53**

키 저장소 생성 **53**

키 추가 **53**

S

SSH 로그인 **23**

SSH 로그인 사용 **23**

SSH 로그인 사용 안 함 **23**

SSL 신뢰 관리자 **51**

SSL 인증서 **76**

V

- vCenter Server **75**
- vCenter Single Sign-On, 등록 **37**
- vCenter Single Sign-On 구성 **37**
- VMware vRealize Orchestrator 서버,
Windows 서비스로 설치 **45**
- vRealize Automation 인증 **35**
- vSphere Replication에 대한 가상 시스템 구
성 **82**
- vSphere 인증 **37**

ㄱ

- 가용성 **19**
- 검사점 설정 **11**
- 고객 경험 향상 프로그램 **49**
- 고객 환경 향상 프로그램, 수집된 정보 **49**
- 관리 사이트 SSL 인증서 변경 **77**
- 구성
 - Orchestrator 서버 **29**
 - 구성 설정 가져오기 **56**
 - 구성 설정 내보내기 **55**
 - 네트워크 설정 **24**
 - 데이터베이스 연결 **38, 39**
 - 프록시 설정 **24**
- 구성 마이그레이션 **57**
- 국제화 **17**
- 권한 거부, js-io-rights.conf 파일 **88**
- 권한 허용, js-io-rights.conf 파일 **88**
- 규칙, js-io-rights.conf 파일 **88**
- 기본 포트
 - HTTP 포트 **30**
 - HTTPS 포트 **30**
 - LDAP 포트 **30**
 - Oracle 포트 **30**
 - SMTP 포트 **30**
 - SQL Server 포트 **30**
 - SSL을 사용하는 LDAP **30**
 - vCenter API 포트 **30**
 - 글로벌 카탈로그를 사용하는 LDAP **30**
 - 데이터 포트 **30**
 - 메시징 포트 **30**
 - 명령 포트 **30**
 - 웹 구성 HTTP 액세스 포트 **30**
 - 웹 구성 HTTPS 액세스 포트 **30**
 - 조회 포트 **30**

ㄷ

- 대상 **7**
- 데이터베이스
 - Oracle **20**
 - SQL Server **20**
 - SQL Server Express **20**

- SSL 인증서 가져오기 **38**

서버 크기 **20**

설정 **20**

설치 **20**

연결 매개 변수 **39**

데이터베이스 가져오기 **41**

데이터베이스 내보내기 **41**

데이터베이스 요구 사항 **16**

디버그 로깅 **43**

디버그 모드 **78**

디버깅 **78**

ㄴ

라이브 스트림 **63**

로그

비영구 로그 **61**

영구 로그 **61**

로그 파일 **63**

로그인

Linux 콘솔 **22**

Orchestrator 클라이언트 **93**

로드 밸런서 **48**

로컬 저장소, 인증서 **76**

ㄹ

마이그레이션 **57, 58, 66**

마이그레이션 도구 **57**

마이그레이션 매트릭스 **58, 66**

명령줄 도구 **51**

ㄴ

백업, 구성 **78**

버전 관리 **11**

보안 **11**

보호 그룹

vSphere Replication **83**

생성 **83**

스토리지 정책 **83**

어레이 기반 복제 **83**

복구 계획

속성 변경 **84**

폴더 생성 **84**

폴더 이름 변경 **84**

폴더에 추가 **84**

ㄷ

사용 사례 **75**

사용 안 함 **49**

사용자 권한 **31**

사용자 역할 **13**

사용하도록 설정 **49**

- 서버 로그
 - 내보내기 **62**
 - 로그 수준 **62**
 - 서버 모드 **45**
 - 서버 인증서
 - CA 서명됨 **41**
 - 자체 서명됨 **41**
 - 서비스
 - VMware vRealize Orchestrator 서버 **45**
 - 시작 **45**
 - 설정 지침
 - LDAP 서버 **19**
 - vCenter Server **19**
 - vCenter Single Sign-On **19**
 - 디렉토리 서비스 **19**
 - 수준 또는 권한, js-io-rights.conf 파일 **88**
 - 스크립팅
 - Java 클래스 액세스 **90**
 - 서터 시스템 속성 **90**
 - 운영 체제 명령 액세스 **89**
 - 스크립팅 엔진 **11**
 - 시간 초과 **90**
 - 시나리오 **75**
 - 시스템 속성 **60, 87, 90**
 - 시스템 요구 사항
 - Orchestrator Appliance **15**
 - 디렉토리 서비스 **15**
 - 지원되는 데이터베이스 **16**
 - 지원되는 브라우저 **16**
 - 실행 중인 워크플로 취소, 워크플로 ID 취소 **77**
- ㅇ**
- 암호 **55**
 - 암호 요구 사항 **16**
 - 어레이 기반 복구 계획, 생성 **83**
 - 업데이트된 정보 **9**
 - 완료된 워크플로, 워크플로 로그 **62**
 - 운영 체제 명령, 액세스 **89**
 - 워크플로 검사 **62**
 - 워크플로 엔진 **11**
 - 워크플로 취소 **77**
 - 인증 유형 **31**
- ㅈ**
- 재해 복구 **82**
 - 전원 켜기 **22**
 - 정적 IP 할당 **24**
 - 정책 엔진 **11**
 - 제어 센터 **30**
 - 제어 센터 REST API **54**
 - 지속성 **11**
- ㅊ**
- 최대 동시 워크플로 **60**
 - 최대 보류 중인 워크플로 **60**
 - 추가, 인증서 **76**
 - 추가 구성 옵션 **55**
 - 컨텐츠, js-io-rights.conf 파일 **88**
 - 클러스터 모드 **45, 46**
- ㅌ**
- 파일 시스템
 - 워크플로 액세스 설정 **88**
 - 워크플로에서 액세스 **88**
 - 플러그인, 플러그인 제거 **44**
 - 필터링, Orchestrator 로그 **63**
- ㅎ**
- 하드웨어 요구 사항, Orchestrator Appliance **15**
 - 확장성 **19**
 - 후속 작업 **93**

