

vRealize Automation 관리

2020년 12월 21일

vRealize Automation 8.1

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

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

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

Copyright © 2021 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

1	vRealize Automation 관리	4
2	사용자 관리	5
	vRealize Automation에서 프로젝트에 대해 Active Directory 그룹을 사용하도록 설정하는 방법	6
	vRealize Automation에서 사용자를 제거하는 방법	7
	vRealize Automation에서 사용자 역할을 편집하는 방법	7
	vRealize Automation에서 그룹 역할 할당을 편집하는 방법	8
	vRealize Automation 사용자 역할이란?	8
3	장치 유지 보수	17
	vRealize Automation 시작 및 중지	17
	vRealize Automation에 대한 DNS 할당 업데이트	19
	시간 동기화를 사용하도록 설정하는 방법	20
	시간 동기화를 비활성화하는 방법	21
	루트 암호를 재설정하는 방법	21
4	vRealize Automation에서 다중 조직 테넌트 구성 사용	23
	vRealize Automation에 대한 다중 조직 테넌트 설정	25
	단일 노드 다중 조직 배포에서 인증서 및 DNS 구성 관리	27
	클러스터링된 vRealize Automation 배포에서 인증서 및 DNS 구성 관리	29
	테넌트에 로그인하고 vRealize Automation에 사용자 추가	31
	vRealize Automation 다중 조직 배포에 vRealize Orchestrator 사용	32
5	로그 사용	33
	로그 및 로그 번들을 사용하는 방법	33
	vRealize Log Insight로 로그 전달을 구성하는 방법	35
	Syslog 통합을 생성하거나 업데이트하는 방법	38
	로그를 위해 Syslog 통합을 삭제하는 방법	39
6	고객 환경 향상 프로그램 참여	40
	프로그램 참여 또는 탈퇴 방법	40
	프로그램에 대한 데이터 수집을 구성하는 방법	41

vRealize Automation 관리

1

이 가이드에서는 vRealize Automation 배포의 중요한 인프라 및 사용자 관리 측면을 모니터링하고 관리하는 방법을 설명합니다.

여기에 설명된 작업은 vRealize Automation 배포가 제대로 작동하도록 유지하는 데 필수적입니다. 이러한 작업에는 사용자 및 그룹 관리 그리고 시스템 로그 모니터링이 포함됩니다.

또한 다중 조직 배포를 구성하고 관리하는 방법도 설명합니다.

일부 vRealize Automation 관리 작업은 vRealize Automation 내에서 완료되지만 다른 작업은 vRealize Suite Lifecycle Manager 및 Workspace ONE Access와 같은 관련 제품을 사용해야 합니다. 사용자는 해당 작업을 완료하기 전에 이러한 제품과 기능을 숙지해야 합니다.

예를 들어, 백업, 복원 및 재해 복구에 대한 자세한 내용은 [vRealize Suite 제품 설명서](#)에서 **백업 및 복원 및 재해 복구 > 2019** 섹션을 참조하십시오.

참고 재해 복구는 vRealize Automation 8.0.1 이상에서 지원됩니다.

vRealize Suite Lifecycle Manager 설치, 업그레이드 및 관리 작업에 대한 자세한 내용은 [Lifecycle Manager 제품 설명서](#)를 참조하십시오.

vRealize Automation의 사용자 및 그룹 관리

2

vRealize Automation은 VMware 제공 ID 관리 애플리케이션인 VMware Workspace ONE Access를 사용하여 사용자와 그룹을 가져오고 관리합니다. 사용자와 그룹을 가져오거나 생성한 후에는 [ID 및 액세스 관리] 페이지를 사용하여 단일 테넌트 배포에 대한 역할 할당을 관리할 수 있습니다.

vRealize Automation은 VMware Lifecycle Manager(vRSLCM 또는 LCM)를 사용하여 설치됩니다. vRealize Automation을 설치할 때 ID 관리를 지원하기 위해 기존 Workspace ONE Access 인스턴스를 가져오거나 새로 배포해야 합니다. 이러한 두 시나리오에 따라 관리 옵션이 정의됩니다.

- 새 Workspace ONE Access 인스턴스를 배포하면 LCM을 통해 사용자와 그룹을 관리할 수 있습니다. 설치 중에 Workspace ONE Access를 사용하여 Active Directory 연결을 설정할 수 있습니다. 또는 여기에 설명된 대로 [ID 및 액세스 관리] 페이지를 사용하여 vRealize Automation 내에서 사용자와 그룹의 일부 측면을 살펴보고 편집할 수 있습니다.
- 기존 Workspace ONE Access 인스턴스를 사용하는 경우에는 설치 중에 LCM을 통해 vRealize Automation에서 사용할 인스턴스를 가져옵니다. 이 경우 Workspace ONE Access를 계속 사용하여 사용자와 그룹을 관리하거나 LCM의 관리 기능을 사용할 수 있습니다.

다중 조직 배포에서의 사용자 관리에 대한 자세한 내용은 [테넌트에 로그인하고 vRealize Automation에 사용자 추가](#) 항목을 참조하십시오.

vRealize Automation 사용자에게 역할을 할당해야 합니다. 역할은 애플리케이션 내의 기능에 대한 액세스를 정의합니다. Workspace ONE Access 인스턴스를 사용하여 vRealize Automation을 설치하면 기본 조직이 생성되고 설치 관리자에게 조직 소유자 역할이 할당됩니다. 다른 모든 vRealize Automation 역할은 조직 소유자가 할당합니다.

vRealize Automation에는 조직 역할, 서비스 역할 및 프로젝트 역할이라는 세 가지 유형의 역할이 있습니다. vRealize Automation Cloud Assembly, Service Broker 및 Code Stream의 경우, 일반적으로 사용자 수준 역할은 리소스를 사용할 수 있지만 관리자 수준 역할은 리소스를 생성하고 구성하는 데 필요합니다. 조직 역할은 테넌트 내에서 사용 권한을 정의합니다. 조직 소유자에게는 관리자 수준 사용 권한이 있고, 조직의 멤버에게는 사용자 수준 사용 권한이 있습니다. 조직 소유자는 다른 사용자를 추가하고 관리할 수 있습니다.

조직 역할	서비스 역할
■ 조직 소유자	■ Cloud Assembly 관리자
■ 조직 멤버	■ Cloud Assembly 사용자
	■ Cloud Assembly 뷰어
	■ Service Broker 관리자
	■ Service Broker 사용자
	■ Service Broker 뷰어
	■ Code Stream 관리자
	■ Code Stream 사용자
	■ Code Stream 뷰어

또한 테이블에 표시되지 않은 두 가지 주요 프로젝트 수준 역할(프로젝트 관리자 및 프로젝트 사용자)이 있습니다. 이러한 역할은 Cloud Assembly를 통해 프로젝트를 기반으로 임시로 할당됩니다. 이러한 역할은 다소 유동적입니다. 동일한 사용자가 한 프로젝트의 관리자이면서 다른 프로젝트의 사용자가 될 수도 있습니다. 자세한 내용은 [vRealize Automation 사용자 역할이란?](#) 항목을 참조하십시오.

LCM 및 Workspace ONE Access 작업에 대한 자세한 내용은 [VMware Identity Manager를 사용한 사용자 관리](#)를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [vRealize Automation에서 프로젝트에 대해 Active Directory 그룹을 사용하도록 설정하는 방법](#)
- [vRealize Automation에서 사용자를 제거하는 방법](#)
- [vRealize Automation에서 사용자 역할을 편집하는 방법](#)
- [vRealize Automation에서 그룹 역할 할당을 편집하는 방법](#)
- [vRealize Automation 사용자 역할이란?](#)

vRealize Automation에서 프로젝트에 대해 Active Directory 그룹을 사용하도록 설정하는 방법

사용자를 프로젝트에 추가할 때 [그룹 추가] 페이지에 그룹이 없으면 [ID 및 액세스 관리] 페이지를 확인하고 그룹이 있으면 추가합니다. vRealize Automation의 [ID 및 액세스 관리] 페이지에 그룹이 나열되어 있지 않으면, 그룹이 Workspace One Access 인스턴스에서 동기화되지 않았을 수 있습니다. 동기화되었는지 확인한 후 이 절차를 사용하여 여기에 표시된 대로 그룹을 추가할 수 있습니다.

Active Directory 그룹 멤버를 프로젝트에 추가하려면 그룹이 Workspace One Access 인스턴스와 동기화되고 그룹이 조직에 추가되었는지 확인해야 합니다.

사전 요구 사항

그룹이 동기화되지 않은 경우 프로젝트에 추가하려고 할 때 사용할 수 없습니다. Active Directory 그룹을 Lifecycle Manager 인스턴스와 동기화했는지 확인합니다.

절차

- 1 추가 중인 동일한 Active Directory 도메인의 사용자로 vRealize Automation에 로그인합니다. 예: @mycompany.com
- 2 Cloud Assembly의 헤더 오른쪽 탐색에서 [ID 및 액세스 관리]를 클릭합니다.
- 3 **엔터프라이즈 그룹**을 클릭한 다음 **역할 할당**을 클릭합니다.
- 4 검색 기능을 사용하여 추가할 그룹을 찾아서 선택합니다.
- 5 조직 역할을 할당합니다.
그룹에는 최소한 조직 멤버 역할이 있어야 합니다. 자세한 내용은 [vRealize Automation Cloud Assembly 사용자 역할이란?](#)을 참조하십시오.
- 6 **서비스 액세스 추가**를 클릭하여 서비스를 하나 이상 추가하고 각각에 대한 역할을 선택합니다.
- 7 **할당**을 클릭합니다.

결과

이제 Active Directory 그룹을 프로젝트에 추가할 수 있습니다.

vRealize Automation에서 사용자를 제거하는 방법

vRealize Automation에서 필요에 따라 사용자를 제거할 수 있습니다.

기본적으로 모든 사용자가 나열되며 [ID 및 액세스 관리] 페이지를 통해 사용자를 추가할 수 없습니다. 사용자를 삭제할 수 있습니다.

절차

- 1 [ID 및 액세스 관리] 페이지에서 [활성 사용자] 탭을 선택합니다.
- 2 삭제할 사용자를 찾아서 선택합니다.
- 3 **사용자 제거**를 클릭합니다.

결과

선택한 사용자가 제거됩니다.

vRealize Automation에서 사용자 역할을 편집하는 방법

vRealize Automation으로 가져온 Workspace ONE Access 사용자에게 할당된 역할을 편집할 수 있습니다.

사전 요구 사항

절차

- 1 Cloud Assembly의 헤더 오른쪽 탐색에서 [ID 및 액세스 관리]를 클릭합니다.

- 2 [활성 사용자] 탭에서 원하는 사용자를 선택하고 **역할 편집**을 클릭합니다.
- 3 사용자의 서비스 역할 및 조직을 편집할 수 있습니다.
 - [조직 역할 할당] 머리글 옆의 드롭다운을 선택하여 조직과 사용자의 관계를 변경합니다.
 - 사용자에게 대한 새 서비스 역할을 추가하려면 [서비스 액세스 추가]를 클릭합니다.
 - 사용자 역할을 제거하려면 해당 서비스 옆의 X를 클릭합니다.
- 4 **저장**을 클릭합니다.

결과

사용자 역할 할당이 지정된 대로 업데이트됩니다.

vRealize Automation에서 그룹 역할 할당을 편집하는 방법

vRealize Automation에서 그룹에 대한 역할 할당을 편집할 수 있습니다.

사전 요구 사항

vRealize Automation 배포와 연결된 유효한 vIDM 인스턴스에서 사용자와 그룹을 가져왔습니다.

절차

- 1 Cloud Assembly의 헤더 오른쪽 탐색에서 [ID 및 액세스 관리]를 클릭합니다.
- 2 [엔터프라이즈 그룹] 탭을 선택합니다.
- 3 검색 필드에서 역할 할당을 편집하려는 그룹의 이름을 입력합니다.
- 4 선택한 그룹에 대한 역할 할당을 편집합니다. 다음 두 가지 옵션 중에서 선택할 수 있습니다.
 - 조직 역할 할당
 - 서비스 역할 할당
- 5 **할당**을 클릭합니다.

결과

지정된 대로 역할 할당이 업데이트됩니다.

vRealize Automation 사용자 역할이란?

조직 소유자는 사용자에게 조직 역할 및 서비스 역할을 할당할 수 있습니다. 역할은 사용자가 수행하거나 볼 수 있는 작업을 결정합니다. 그런 다음 서비스 관리자는 서비스에서 프로젝트 역할을 할당할 수 있습니다. 할당할 역할을 결정하려면 다음 표의 작업을 평가 합니다.

Cloud Assembly 서비스 역할

vRealize Automation Cloud Assembly 서비스 역할은 사용자가 vRealize Automation Cloud Assembly에서 보고 수행할 수 있는 작업을 결정합니다. 이러한 서비스 역할은 조직 소유자가 콘솔에서 정의합니다.

표 2-1. vRealize Automation Cloud Assembly 서비스 역할 설명

역할	설명
Cloud Assembly 관리자	전체 사용자 인터페이스 및 API 리소스에 대해 읽기/쓰기 액세스 권한을 갖고 있어야 합니다. 클라우드 계정 추가, 새 프로젝트 생성 및 프로젝트 관리자 할당 등을 볼 수 있고 수행할 수 있는 유일한 사용자 역할입니다.
Cloud Assembly 사용자	Cloud Assembly 관리자 역할이 없는 사용자입니다. vRealize Automation Cloud Assembly 프로젝트에서는 관리자가 프로젝트에 사용자를 프로젝트 멤버로 추가합니다. 관리자는 프로젝트 관리자를 추가할 수도 있습니다. 두 가지 역할에 대한 사용 권한은 아래에 정의되어 있습니다.
Cloud Assembly 뷰어	정보를 볼 수 있지만 정보를 생성, 업데이트 또는 삭제할 수 없는 사용자입니다. 이것은 읽기 전용 역할입니다.

서비스 역할 외에도 vRealize Automation Cloud Assembly에는 프로젝트 역할이 있습니다.

프로젝트 역할은 vRealize Automation Cloud Assembly에 정의되며 프로젝트마다 다를 수 있습니다.

다음 표에는 다양한 서비스 및 프로젝트 역할이 볼 수 있고 수행할 수 있는 내용이 있습니다. 서비스 관리자에게는 사용자 인터페이스의 모든 영역에 대한 모든 권한이 있습니다.

프로젝트 역할에 대한 설명은 사용자에게 부여할 사용 권한을 결정하는 데 도움이 됩니다.

- 프로젝트 관리자는 서비스 관리자가 생성한 인프라를 활용하여, 프로젝트의 멤버가 개발 작업에 필요한 리소스를 사용할 수 있도록 보장합니다.
- 프로젝트 멤버는 프로젝트 내에서 작업하며 Blueprint를 설계 및 배포합니다.
- 프로젝트 뷰어는 Blueprint 다운로드와 같은 비파괴적인 작업을 수행할 수 있는 몇 가지 경우를 제외하고 읽기 전용 액세스로 제한됩니다.

표 2-2. vRealize Automation Cloud Assembly 서비스 역할 및 프로젝트 역할

UI 컨텍스트	작업	Cloud Assembly 관리자	Cloud Assembly 뷰어	Cloud Assembly 사용자 프로젝트 관련 작업을 보고 수행하려면 사용자가 프로젝트 관리자 또는 멤버여야 합니다.		
				프로젝트 관리자	프로젝트 구성원	프로젝트 뷰어
Cloud Assembly 액세스						
콘솔	vRA 콘솔에서 Cloud Assembly를 보고 열 수 있음	예	예	예	예	예
인프라						
	[인프라] 탭을 보고 열기	예	예	예	예	예
구성 - 프로젝트	프로젝트 생성	예				
	프로젝트 요약, 사용자, 프로비저닝, Kubernetes, 통합 및 테스트 프로젝트 구성에서 값 업데이트 또는 삭제.	예		예. 프로젝트		
	사용자를 추가하고 프로젝트에서 역할을 할당합니다.	예		예. 프로젝트.		
	프로젝트 보기	예	예	예. 프로젝트	예. 프로젝트	예. 프로젝트
구성 - 클라우드 영역	클라우드 영역 생성, 업데이트 또는 삭제	예				
	클라우드 영역 보기	예	예			
구성 - Kubernetes 영역	Kubernetes 영역 생성, 업데이트 또는 삭제	예				
	Kubernetes 영역 보기	예	예			
구성 - 버전	버전 생성, 업데이트 또는 삭제	예				
	버전 보기	예	예			
구성 - 이미지 매핑	이미지 매핑 생성, 업데이트 또는 삭제	예				
	이미지 매핑 보기	예	예			
구성 - 네트워크 프로파일	네트워크 프로파일 생성, 업데이트 또는 삭제	예				
	이미지 네트워크 프로파일 보기	예	예			
구성 - 스토리지 프로파일	스토리지 프로파일 생성, 업데이트 또는 삭제	예				
	이미지 스토리지 프로파일 보기	예	예			
구성 - 가격 책정 카드	가격 책정 카드 생성, 업데이트 또는 삭제	예				

표 2-2. vRealize Automation Cloud Assembly 서비스 역할 및 프로젝트 역할 (계속)

UI 컨텍스트	작업	Cloud Assembly 관리자	Cloud Assembly 뷰어	Cloud Assembly 사용자 프로젝트 관련 작업을 보고 수행하려면 사용자가 프로젝트 관리자 또는 멤버여야 합니다.		
				프로젝트 관리자	프로젝트 구성원	프로젝트 뷰어
	가격 책정 카드 보기	예	예			
구성 - 태그	태그 생성, 업데이트 또는 삭제	예				
	태그 보기	예	예			
리소스 - 계산	검색된 계산 리소스에 태그 추가	예				
	검색된 계산 리소스 보기	예	예			
리소스 - 네트워크	네트워크 태그, IP 범위 및 IP 주소 수정	예				
	검색된 네트워크 리소스 보기	예	예			
리소스 - 보안	검색된 보안 그룹에 태그 추가	예				
	검색된 보안 그룹 보기	예	예			
리소스 - 스토리지	검색된 스토리지에 태그 추가	예				
	스토리지 보기	예	예			
리소스 - 시스템	시스템 추가 및 삭제	예				
	시스템 보기	예	예	예, 프로젝트	예, 프로젝트	예, 프로젝트
리소스 - 볼륨	검색된 스토리지 볼륨 삭제	예				
	검색된 스토리지 볼륨 보기	예	예	예, 프로젝트	예, 프로젝트	예, 프로젝트
리소스 - Kubernetes	Kubernetes 클러스터 배포 또는 추가, 네임스페이스 생성 또는 추가	예				
	Kubernetes 클러스터 및 네임스페이스 보기	예	예	예, 프로젝트	예, 프로젝트	예, 프로젝트
작업 - 요청	배포 요청 기록 삭제	예				
	배포 요청 기록 보기	예	예	예, 프로젝트	예, 프로젝트	예, 프로젝트
작업 - 이벤트 로그	이벤트 로그 보기	예	예	예, 프로젝트	예, 프로젝트	예, 프로젝트
연결 - 클라우드 계정	클라우드 계정 생성, 업데이트 또는 삭제	예				
	클라우드 계정 보기	예	예			
연결 - 통합	통합 생성, 업데이트 또는 삭제	예				
	통합 보기	예	예			

표 2-2. vRealize Automation Cloud Assembly 서비스 역할 및 프로젝트 역할 (계속)

UI 컨텍스트	작업	Cloud Assembly 관리자	Cloud Assembly 뷰어	Cloud Assembly 사용자 프로젝트 관련 작업을 보고 수행하려면 사용자가 프로젝트 관리자 또는 멤버여야 합니다.		
				프로젝트 관리자	프로젝트 구성원	프로젝트 뷰어
온보딩	온보딩 계획 생성, 업데이트 또는 삭제	예				
	온보딩 계획 보기	예	예			예. 프로젝트
마켓플레이스						
	[마켓플레이스] 탭을 보고 열기	예	예			
	[설계] 탭에서 다운로드된 Blueprint 사용	예		예. 프로젝트와 연결된 경우.	예. 프로젝트와 연결된 경우.	
마켓플레이스 - Blueprint	Blueprint 다운로드	예				
	Blueprint 보기	예	예			
마켓플레이스 - 이미지	이미지 다운로드	예				
	이미지 보기	예	예			
마켓플레이스 - 다운로드	다운로드한 모든 항목의 로그 보기	예	예			
확장성						
	[확장성] 탭을 보고 열기	예	예			예
이벤트	확장성 이벤트 보기	예	예			
구독	확장성 구독 생성, 업데이트 또는 삭제	예				
	구독 사용 안 함	예				
	구독 보기	예	예			
라이브러리 - 이벤트 항목	이벤트 항목 보기	예	예			
라이브러리 - 작업	확장성 작업 생성, 업데이트 또는 삭제	예				
	확장성 작업 보기	예	예			
라이브러리 - 워크플로	확장성 워크플로 보기	예	예			
작업 - 작업 실행	확장성 작업 실행 취소 또는 삭제	예				

표 2-2. vRealize Automation Cloud Assembly 서비스 역할 및 프로젝트 역할 (계속)

UI 컨텍스트	작업	Cloud Assembly 관리자	Cloud Assembly 뷰어	Cloud Assembly 사용자 프로젝트 관련 작업을 보고 수행하려면 사용자가 프로젝트 관리자 또는 멤버여야 합니다.		
				프로젝트 관리자	프로젝트 구성원	프로젝트 뷰어
	확장성 작업 실행 보기	예	예			예, 프로젝트
활동 - 워크플로 실행	확장성 워크플로 실행 보기	예	예			
설계						
설계	[설계] 탭을 열고 Blueprint 목록 보기	예	예	예, 프로젝트	예, 프로젝트	예, 프로젝트
Blueprint	Blueprint 생성, 업데이트 및 삭제	예		예, 프로젝트	예, 프로젝트	
	Blueprint 보기	예	예	예, 프로젝트	예, 프로젝트	예, 프로젝트
	Blueprint 다운로드	예	예	예, 프로젝트	예, 프로젝트	예, 프로젝트
	Blueprint 업로드	예		예, 프로젝트	예, 프로젝트	
	Blueprint 배포	예		예, 프로젝트	예, 프로젝트	
	버전 및 Blueprint 복원	예		예, 프로젝트	예, 프로젝트	
	카탈로그에 Blueprint 릴리스	예		예, 프로젝트		
사용자 지정 리소스	사용자 지정 리소스 생성, 업데이트 또는 삭제	예				
	사용자 지정 리소스 보기	예	예	예, 프로젝트	예, 프로젝트	예, 프로젝트
사용자 지정 작업	사용자 지정 작업 생성, 업데이트 또는 삭제	예				
	사용자 지정 작업 보기	예	예	예, 프로젝트	예, 프로젝트	예, 프로젝트
배포						
	[배포] 탭 보기 및 열기	예	예	예	예	예

표 2-2. vRealize Automation Cloud Assembly 서비스 역할 및 프로젝트 역할 (계속)

UI 컨텍스트	작업	Cloud Assembly 관리자	Cloud Assembly 뷰어	Cloud Assembly 사용자 프로젝트 관련 작업을 보고 수행하려면 사용자가 프로젝트 관리자 또는 멤버여야 합 니다.		
				프로젝 트 관리 자	프로젝 트 구성 원	프로젝 트 뷰어
	배포 세부 정보, 배포 기록 및 문제 해결 정보를 포함한 배포 보기.	예	예	예. 프로 젝트	예. 프로 젝트	예. 프 로젝트
	정책에 따라 배포에서 2일차 작업 실행	예		예. 프로 젝트	예. 프로 젝트	

Service Broker 서비스 역할

vRealize Automation Service Broker 서비스 역할은 사용자가 vRealize Automation Service Broker에
서 보고 수행할 수 있는 작업을 결정합니다. 이러한 서비스 역할은 조직 소유자가 콘솔에서 정의합니다.

표 2-3. Service Broker 서비스 역할 설명

역할	설명
Service Broker 관리자	전체 사용자 인터페이스 및 API 리소스에 대해 읽기/쓰기 액세스 권한을 갖고 있어야 합니다. 새 프로젝트 생성 및 프로젝트 관리 자 할당을 비롯한 모든 작업을 수행할 수 있는 유일한 사용자 역 할입니다.
Service Broker 사용자	vRealize Automation Service Broker 관리자 역할이 없는 모든 사용자입니다. vRealize Automation Service Broker 프로젝트에서는 관리자 가 프로젝트에 사용자를 프로젝트 멤버로 추가합니다. 관리자는 프로젝트 관리자를 추가할 수도 있습니다. 두 가지 역할에 대한 사용 권한은 아래에 정의되어 있습니다.
Service Broker 뷰어	읽기 전용 권한이 있는 사용자는 정보를 볼 수 있지만 값을 생성, 업데이트 또는 삭제할 수는 없습니다.

서비스 역할 외에도 vRealize Automation Service Broker에는 프로젝트 역할이 있습니다.

프로젝트 역할은 vRealize Automation Service Broker에 정의되며 프로젝트마다 다를 수 있습니다.

다음 표에는 다양한 서비스 및 프로젝트 역할이 볼 수 있고 수행할 수 있는 내용이 있습니다. 서비스 관리
자에게는 사용자 인터페이스의 모든 영역에 대한 모든 권한이 있습니다.

프로젝트 역할에 대한 다음 설명을 사용하면 사용자에게 부여할 사용 권한을 결정하는 데 도움이 됩니다.

- 프로젝트 관리자는 서비스 관리자가 생성한 인프라를 활용하여, 프로젝트의 멤버가 개발 작업에 필요
한 리소스를 사용할 수 있도록 보장합니다.
- 프로젝트 멤버는 프로젝트 내에서 작업하며 Blueprint를 설계 및 배포합니다.

- 프로젝트 뷰어는 읽기 전용 액세스로 제한됩니다.

표 2-4. Service Broker 서비스 역할 및 프로젝트 역할

UI 컨텍스트	작업	Service Broker 관리자	Service Broker 뷰어	Service Broker 사용자		
				프로젝트 관련 작업을 보고 수행하려면 사용자가 프로젝트 관리자여야 합니다.		
				프로젝트 관리자	프로젝트 구성원	프로젝트 뷰어
Service Broker 액세스						
콘솔	콘솔에서 Service Broker를 보고 열 수 있음	예	예	예	예	예
인프라						
	[인프라] 탭을 보고 열기	예	예			
구성 - 프로젝트	프로젝트 생성	예				
	프로젝트 요약, 사용자, 프로비저닝, Kubernetes 및 통합에서 값 업데이트 또는 삭제	예				
	프로젝트 보기	예	예			
구성 - 클라우드 영역	클라우드 영역 생성, 업데이트 또는 삭제	예				
	클라우드 영역 보기	예	예			
구성 - Kubernetes 영역	Kubernetes 영역 생성, 업데이트 또는 삭제	예				
	Kubernetes 영역 보기	예	예			
연결 - 클라우드 계정	클라우드 계정 생성, 업데이트 또는 삭제	예				
	클라우드 계정 보기	예	예			
연결 - 통합	통합 생성, 업데이트 또는 삭제	예				
	통합 보기	예	예			
작업 - 요청	배포 요청 기록 삭제	예				
	배포 요청 기록 보기	예				
작업 - 이벤트 로그	이벤트 로그 보기	예				
컨텐츠 및 정책						
	[컨텐츠 및 정책] 탭을 보고 열기	예	예			
컨텐츠 소스	컨텐츠 소스 생성, 업데이트 또는 삭제	예				
	컨텐츠 소스 보기	예	예			
컨텐츠 공유	공유 컨텐츠 추가 또는 제거	예				

표 2-4. Service Broker 서비스 역할 및 프로젝트 역할 (계속)

UI 컨텍스트	작업	Service Broker 관리자	Service Broker 뷰어	Service Broker 사용자 프로젝트 관련 작업을 보고 수행하려면 사용자가 프로젝트 관리자여야 합니다.		
				프로젝트 관리자	프로젝트 구성원	프로젝트 뷰어
컨텐츠	공유 컨텐츠 보기	예	예			
	양식 사용자 지정 및 항목 구성	예				
	컨텐츠 보기	예	예			
정책 - 정의	정책 정의 생성, 업데이트 또는 삭제	예				
	정책 정의 보기	예	예			
정책 - 적용	적용 로그 보기	예	예			
알림 - 이메일 서버	이메일 서버 구성	예				
카탈로그						
	[카탈로그] 탭 보기 및 열기	예	예	예	예	예
	사용 가능한 카탈로그 항목 보기	예	예	예, 프로젝트	예, 프로젝트	예, 프로젝트
	카탈로그 항목 요청	예		예, 프로젝트	예, 프로젝트	
배포						
	[배포] 탭 보기 및 열기	예	예	예,	예	예
	배포 세부 정보, 배포 기록 및 문제 해결 정보를 포함한 배포 보기.	예	예	예, 프로젝트	예, 프로젝트	예, 프로젝트
	정책에 따라 배포에서 2일차 작업 실행	예		예, 프로젝트	예, 프로젝트	
승인						
	[승인] 탭 보기 및 열기	예	예	예	예	예
	승인 요청에 응답	예		Service Broker 사용자 역할만	Service Broker 사용자 역할만	Service Broker 사용자 역할만

vRealize Automation 장치 유지 보 수

3

시스템 관리자는 설치된 vRealize Automation 애플리케이션이 제대로 작동하도록 다양한 작업을 수행해야 할 수 있습니다.

vRealize Automation을 지금 막 시작한 경우에는 이러한 작업이 필요하지 않습니다. 이러한 작업의 수행 방법을 아는 것은 성능 또는 제품 동작 문제를 해결해야 하는 경우에 유용합니다.

본 장은 다음 항목을 포함합니다.

- vRealize Automation 시작 및 중지
- vRealize Automation에 대한 DNS 할당 업데이트
- vRealize Automation의 시간 동기화를 사용하도록 설정하는 방법
- 시간 동기화를 비활성화하는 방법
- vRealize Automation에 대한 루트 암호를 재설정하는 방법

vRealize Automation 시작 및 중지

vRealize Automation을 시작하거나 종료할 때 적절한 절차를 검토합니다.

vRealize Automation 종료

데이터 무결성을 보존하려면 가상 장치의 전원을 끄기 전에 vRealize Automation 서비스를 종료합니다.

참고 가능하면 `vraccli reset vidm` 명령을 사용하지 마십시오. 이 명령은 Workspace One Access의 모든 구성을 재설정하고 사용자와 프로비저닝된 리소스 간의 연결을 끊습니다.

- 1 SSH 또는 VMRC를 사용하여 vRealize Automation 장치의 콘솔에 로그인합니다.

- 모든 클러스터 노드에서 vRealize Automation 서비스를 종료하려면 다음 명령 집합을 실행합니다.

참고 실행을 위해 이러한 명령을 복사했지만 실행에 실패한 경우 해당 명령을 메모장에 붙여 넣은 다음 실행하기 전에 다시 복사합니다. 이 절차에서는 설명서 소스에 있을 수 있는 숨겨진 문자와 기타 아티팩트를 제거합니다.

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

- vRealize Automation 장치를 종료합니다.

vRealize Automation 배포가 이제 종료됩니다.

vRealize Automation 시작

계획되지 않은 종료, 제어된 종료 또는 복구 절차 후에는 특정 순서로 vRealize Automation 구성 요소를 다시 시작해야 합니다. vRLCM은 중요하지 않은 구성 요소이므로 언제든지 시작할 수 있습니다. vRealize Automation을 시작하기 전에 VMware Workspace ONE Access(이전의 VMware Identity Management) 구성 요소를 시작해야 합니다.

참고 vRealize Automation 구성 요소를 시작하기 전에 해당하는 로드 밸런서가 실행 중인지 확인합니다.

- 모든 vRealize Automation 장치의 전원을 켜고 시작될 때까지 기다립니다.
- SSH 또는 VMRC를 사용하여 임의 장치의 콘솔에 로그인하고 다음 명령을 실행하여 모든 노드의 서비스를 복원합니다.

```
/opt/scripts/deploy.sh
```

- 다음 명령을 사용하여 모든 서비스가 작동 및 실행 중인지 확인합니다.

```
kubectl get pods --all-namespaces
```

참고 서비스마다 3개 인스턴스가 표시되어야 하며 해당 상태는 실행 중 또는 완료됨이어야 합니다.

모든 서비스가 실행 중 또는 완료됨으로 나열되면 vRealize Automation을 사용할 준비가 된 것입니다.

vRealize Automation 다시 시작

클러스터의 장치 중앙에서 모든 vRealize Automation 서비스를 다시 시작할 수 있습니다. 앞의 지침에 따라 vRealize Automation을 종료한 다음 지침을 사용하여 vRealize Automation을 시작합니다. vRealize Automation을 다시 시작하기 전에 모든 해당하는 로드 밸런서 및 VMware Workspace ONE Access 구성 요소가 실행 중인지 확인합니다.

모든 서비스가 실행 중 또는 완료됨으로 나열되면 vRealize Automation을 사용할 준비가 된 것입니다.
다음 명령을 실행하여 모든 서비스가 실행되고 있는지 확인합니다.

```
kubect1 -n prelude get pods
```

vRealize Automation에 대한 DNS 할당 업데이트

관리자는 vRealize Automation에 대한 DNS 할당을 업데이트할 수 있습니다.

절차

- 1 SSH 또는 VMRC를 사용하여 vRealize Automation 장치의 콘솔에 로그인합니다.
- 2 모든 클러스터 노드에서 vRealize Automation 서비스를 종료하려면 다음 명령 집합을 실행합니다.

```
/opt/scripts/svc-stop.sh  
sleep 120  
/opt/scripts/deploy.sh --onlyClean
```

- 3 vCenter에 로그인하고 Shut Down Guest OS 명령을 사용하여 모든 vRealize Automation 노드를 종료합니다.
- 4 각 vRealize Automation 노드에 대한 OVF DNS 속성을 업데이트합니다.
 - a vCenter 인벤토리에서 vRealize Automation 노드로 이동합니다.
 - b [구성] 탭을 선택하고 [설정]을 확장합니다.
 - c vApp 옵션을 선택합니다.
 - d OVF 속성 목록에서 vami.DNS.vRealize_Automation을 찾아 선택합니다.
 - e **값 설정**을 클릭하고 [속성 값] 텍스트 상자에 새 DNS 항목을 입력합니다.
 - f **확인**을 클릭합니다.
- 5 모든 vRealize Automation 노드를 시작하고 노드가 완전히 시작되어 콘솔에 파란색 화면으로 표시될 때까지 기다립니다.
- 6 vRealize Automation 노드를 다시 시작하고 완전히 시작될 때까지 기다립니다.
- 7 SSH를 사용하여 각 vRealize Automation 노드에 로그인하고 새 DNS 서버가 /etc/resolve.conf에 나열되는지 확인합니다.
- 8 vRealize Automation 노드 중 하나에서 다음 명령을 실행하여 vRealize Automation 서비스를 시작합니다. /opt/scripts/deploy.sh

결과

vRealize Automation DNS 설정이 지정된 대로 변경됩니다.

vRealize Automation의 시간 동기화를 사용하도록 설정하는 방법

vRealize Automation 장치 명령줄을 사용하여 vRealize Automation 배포에서 시간 동기화를 사용하도록 설정할 수 있습니다.

NTP(Network Time Protocol) 네트워킹 프로토콜을 사용하여 독립형 또는 클러스터링된 vRealize Automation 배포에 대한 시간 동기화를 구성할 수 있습니다. vRealize Automation은 상호 배타적인 두 가지 NTP 구성을 지원합니다.

NTP 구성	설명
ESXi	<p>vRealize Automation 장치를 호스팅하는 ESXi 서버가 NTP 서버와 동기화되는 경우가 구성을 사용할 수 있습니다. 클러스터링된 배포를 사용하는 경우 모든 ESXi 호스트가 NTP 서버와 동기화되어야 합니다.</p> <p>참고 vRealize Automation 배포가 NTP 서버와 동기화되지 않은 ESXi 호스트로 마이그레이션될 경우 클럭 드리프트(clock drift)가 발생할 수 있습니다.</p> <p>ESXi용 NTP 구성에 대한 자세한 내용은 KB 문서 57147 vSphere Web Client를 사용하여 ESXi 호스트에서 NTP(Network Time Protocol) 구성을 참조하십시오.</p>
systemd	<p>이 구성은 systemd-timesyncd 데몬을 사용하여 vRealize Automation 배포의 클럭을 동기화합니다.</p> <p>참고 기본적으로 systemd-timesyncd 데몬을 사용하도록 설정되어 있지만 NTP 서버 없이 구성되어 있습니다. vRealize Automation 장치에서 동적 IP 구성을 사용하는 경우, 장치는 DHCP 프로토콜이 수신한 NTP 서버를 사용할 수 있습니다.</p>

절차

1 vRealize Automation 장치 명령줄에 **root**로 로그인합니다.

2 ESXi에서 NTP를 사용하도록 설정합니다.

a `vracli ntp esxi` 명령을 실행합니다.

b `vracli ntp apply` 명령을 실행합니다.

ESXi NTP 구성이 vRealize Automation 배포에 적용됩니다.

3 systemd에서 NTP를 사용하도록 설정합니다.

a `vracli ntp systemd --set FQDN_or_IP_of_systemd_server` 명령을 실행합니다.

참고 systemd NTP 서버의 네트워크 주소를 쉽표로 구분하여 여러 서버를 추가할 수 있습니다.

b `vracli ntp apply` 명령을 실행합니다.

systemd NTP 구성이 vRealize Automation 배포에 적용됩니다.

4 (선택 사항) NTP 구성의 상태를 확인하려면 `vracli ntp status` 명령을 실행합니다.

NTP 서버와 vRealize Automation 배포 사이에 시간 차이가 10분 이상이면 NTP 구성이 실패할 수 있습니다. 이 문제를 해결하려면 NTP 서버와 동기화된 vRealize Automation 장치를 재부팅합니다.

시간 동기화를 비활성화하는 방법

vRealize Automation 장치 명령줄을 사용하여 vRealize Automation 배포에서 NTP(Network Time Protocol) 시간 동기화를 비활성화할 수 있습니다.

`vracli ntp reset` 명령을 실행하고 `vracli ntp apply` 명령을 실행하여 새 구성을 적용하여 vRealize Automation 장치의 NTP 구성을 재설정할 수도 있습니다.

사전 요구 사항

ESXi 또는 systemd와 시간 동기화를 구성했는지 확인합니다. [vRealize Automation의 시간 동기화를 사용하도록 설정하는 방법](#)의 내용을 참조하십시오.

절차

- 1 vRealize Automation 장치 명령줄에 **root**로 로그인합니다.
- 2 ESXi 또는 systemd와 시간 동기화를 비활성화하려면 `vracli ntp disable` 명령을 실행합니다.
- 3 `vracli ntp apply` 명령을 실행합니다.
- 4 (선택 사항) NTP 구성의 상태를 확인하려면 `vracli ntp status` 명령을 실행합니다.

vRealize Automation에 대한 루트 암호를 재설정하는 방법

분실하거나 잊어버린 vRealize Automation 루트 암호를 재설정할 수 있습니다.

이 절차에서는 호스트 vCenter Appliance에서 명령줄 창을 사용하여 조직의 vRealize Automation 루트 암호를 재설정합니다.

사전 요구 사항

이 프로세스는 vRealize Automation 관리자를 위한 것으로 호스트 vCenter 장치에 액세스하는 데 필요한 자격 증명이 필요합니다.

절차

- 1 [vRealize Automation 시작 및 중지](#)에 설명된 절차를 사용하여 vRealize Automation를 종료하고 시작합니다.
- 2 Photon 운영 체제 명령줄 창이 나타나면 **e**를 입력하고 **Enter** 키를 눌러 GNU GRUB 부팅 메뉴 편집기를 엽니다.

- 3 GNU GRUB 편집기에서 아래와 같이 `linux "/" $photon_linux root=rootpartition`으로 시작하는 줄 끝에 `rw init=/bin/bash`를 입력합니다.

```

GNU GRUB  version 2.02~beta2

setparams 'Photon'

linux "/"$photon_linux root=$rootpartition root_ifnames=0 $photon_cmd\
line coredump_filter=0x37 consoleblank=0 rw init=/bin/bash_
if [ "$photon_initrd" ]; then
    initrd "/"$photon_initrd
fi

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.

```

- 4 **F10** 키를 클릭하여 변경 내용을 푸시하고 vRealize Automation를 다시 시작합니다.
- 5 vRealize Automation가 다시 시작될 때까지 기다립니다.
- 6 `root [/]#` 프롬프트에서 `passwd`를 입력하고 **Enter** 키를 누릅니다.
- 7 New password: 프롬프트에서 새 암호를 입력하고 **Enter** 키를 누릅니다.
- 8 Retype new password: 프롬프트에서 새 암호를 다시 입력하고 **Enter** 키를 누릅니다.
- 9 `root [/]#` 프롬프트에서 `reboot -f`를 입력하고 **Enter** 키를 눌러 루트 암호 재설정 프로세스를 완료합니다.

```

root [ / ]# passwd
New password:
Retype new password:
passwd: password updated successfully
root [ / ]# reboot -f_

```

다음에 수행할 작업

vRealize Automation 관리자는 이제 새 루트 암호를 사용하여 vRealize Automation에 로그인할 수 있습니다.

vRealize Automation에서 다중 조직 테넌트 구성 사용

4

vRealize Automation을 사용하는 경우 고객 IT 제공자는 각 배포 내에서 여러 테넌트 또는 조직을 설정할 수 있습니다. 제공자는 여러 테넌트 조직을 설정하고 각 배포 내에 인프라를 할당할 수 있습니다. 제공자는 테넌트의 사용자를 관리할 수도 있습니다. 각 테넌트는 자체 프로젝트, 리소스 및 배포를 관리합니다.

vRealize Automation 다중 조직 구성에서 제공자는 여러 조직을 생성할 수 있으며 각 테넌트 조직은 자체 프로젝트, 리소스 및 배포를 사용합니다. 제공자는 테넌트 인프라를 원격으로 관리할 수 없지만 테넌트에 로그인하고 테넌트 내에서 인프라를 관리할 수 있습니다.

다중 테넌시는 아래에 설명된 것과 같이 3개의 다른 VMware 제품의 조정 및 구성에 의존합니다.

- **Workspace ONE Access** - 이 제품은 다중 테넌시에 대한 인프라 지원 및 테넌트 조직 내에서 사용자 및 그룹 관리를 제공하는 **Active Directory** 도메인 연결을 제공합니다.
- **vRealize Suite Lifecycle Manager** - 이 제품은 vRealize Automation과 같은 지원되는 제품에 대한 테넌트의 생성 및 구성을 지원합니다. 또한 몇 가지 인증서 관리 기능을 제공합니다.
- **vRealize Automation** - 제공자 및 사용자는 vRealize Automation에 로그인하여 배포를 생성하고 관리하는 테넌트에 액세스합니다.

다중 테넌시를 구성하는 경우 사용자는 3개의 모든 제품과 관련 설명서를 숙지해야 합니다.

LCM 및 Workspace ONE Access 작업에 대한 자세한 내용은 [VMware Identity Manager를 사용한 사용자 관리](#) 및 [VMware Workspace ONE Access 관리](#)의 내용을 참조하십시오.

vRealize Suite Lifecycle Manager 권한이 있는 관리자는 ID 및 테넌트 관리 서비스 아래 [Lifecycle Manager 테넌트] 페이지를 사용하여 테넌트를 생성하고 관리합니다. 테넌트는 **Active Directory IWA** 또는 **LDAP** 연결을 사용하여 구성되며 vRealize Automation 배포에 필요한 연결된 **VMware Workspace ONE Access** 인스턴스에서 지원됩니다. Lifecycle Manager 사용에 대한 자세한 내용은 관련 설명서를 참조하십시오.

다중 테넌시를 구성할 때는 기본 또는 마스터 테넌트로 시작합니다. 이 테넌트는 기본 **Workspace ONE Access** 애플리케이션을 배포할 때 생성되는 기본 테넌트입니다. 하위 테넌트라고도하는 기타 테넌트는 마스터 테넌트에 기반할 수 있습니다. vRealize Automation은 현재 표준 3개 노드 배포를 통해 최대 20개의 테넌트 조직을 지원합니다.

다중 테넌시를 위해 vRealize Automation을 구성할 때는 먼저 단일 조직 구성으로 애플리케이션을 설치한 후 Lifecycle Manager를 사용하여 다중 조직 구성을 설정해야 합니다. Workspace ONE Access 배포는 테넌트 및 연결된 **Active Directory** 도메인 연결 관리를 지원합니다.

다중 테넌시를 처음 구성하면 Lifecycle Manager에서 제공자 관리자가 지정됩니다. 필요한 경우 나중에 이 지정을 변경하거나 관리자를 추가할 수 있습니다. 다중 조직 구성에서 vRealize Automation 사용자 및 그룹은 주로 Workspace ONE Access를 통해 관리됩니다.

조직이 생성되면 인증된 사용자는 자신의 애플리케이션에 로그인하여 프로젝트와 리소스를 생성하거나 사용하고 배포를 생성할 수 있습니다. 관리자는 vRealize Automation에서 사용자 역할을 관리할 수 있습니다.

다중 조직 구성에 대한 설정

vRealize Automation 설치를 완료한 후 다중 조직 배포를 사용하도록 설정할 수 있습니다. 다중 조직 구성을 설정하는 경우 다중 테넌시 사용을 위해 외부 Workspace ONE Access를 구성한 다음 Lifecycle Manager를 사용하여 테넌트를 생성하고 구성해야 합니다. 이것은 새 배포와 기존 배포 모두에 적용됩니다. 테넌트를 설정하는 초기 단계는 Lifecycle Manager를 사용하여 Workspace ONE Access에서 기본적으로 생성된 마스터 테넌트에 대한 별칭을 설정해야 합니다. 이 마스터 테넌트를 기반으로 생성하는 하위 테넌트는 이 마스터 테넌트에서 Active Directory 도메인 구성을 상속합니다.

Lifecycle Manager에서는 테넌트를 제품(예: vRealize Automation) 및 특정 환경에 할당합니다. 테넌트를 설정할 때 테넌트 관리자도 지정해야 합니다. 기본적으로 다중 테넌시는 테넌트 호스트 이름에 기반하여 사용되도록 설정됩니다. 사용자는 DNS 이름으로 테넌트 이름을 수동 구성하도록 선택할 수 있습니다. 이 절차를 진행하는 동안 다중 테넌시 지원을 위해 여러 플래그를 설정해야 하며 로드 밸런서도 구성해야 합니다.

클러스터링된 인스턴스를 사용하는 경우 Workspace ONE Access 및 vRealize Automation 테넌트 기반 호스트 이름이 로드 밸런서를 가리킵니다.

클러스터링된 vRealize Automation 및 Workspace ONE Access 로드 밸런서에 와일드카드 인증서를 사용하지 않으면, 사용자가 테넌트 호스트 이름을 인증서의 SAN 항목으로 추가해야 합니다. SAN 항목으로 추가해야 합니다.

vRealize Automation 또는 Lifecycle Manager에서 테넌트를 삭제할 수 없습니다. 기존 다중 테넌시 배포에 테넌트를 추가하는 작업은 Lifecycle Manager를 사용하여 수행할 수 있지만 이 경우 3-4시간의 다운타임이 불가피합니다.

호스트 이름 및 다중 테넌시

이전 버전의 vRealize Automation에서는 사용자가 디렉토리 경로를 기반으로 하는 URL을 사용하여 테넌트에 액세스했습니다. 현재 다중 테넌시 구현에서는 사용자가 호스트 이름을 기반으로 테넌트에 액세스합니다.

또한 vRealize Automation 사용자가 테넌트에 액세스하는 데 사용하는 호스트 이름 형식은 Workspace ONE Access 내에서 테넌트에 액세스하는 데 사용되는 형식과 다릅니다. 예를 들어 올바른 호스트 이름은 다음과 같습니다. *tenant1.example.eng.vmware.com*(*vidm-node1.eng.vmware.com*과 대조됨)

멀티 테넌시 및 인증서

다중 조직 구성과 관련된 모든 구성 요소에 대한 인증서를 생성해야 합니다. 단일 노드 구성을 사용하는지 또는 클러스터링된 구성을 사용하는지에 따라 **Workspace ONE Access**, **Lifecycle Manager** 및 **vRealize Automation**에 대해 하나 이상의 인증서가 필요합니다.

인증서를 구성할 때 **SAN** 이름이나 전용 이름에 와일드카드를 사용할 수 있습니다. 새 테넌트를 추가할 때 마다 인증서를 업데이트해야 하기 때문에, 와일드카드를 사용하면 인증서 관리가 다소 간단해집니다.

vRealize Automation 및 **Workspace ONE Access** 로드 밸런서에 와일드카드 인증서를 사용하지 않으면, 새로 생성된 모든 테넌트의 인증서에 테넌트 호스트 이름을 **SAN** 항목으로 추가해야 합니다. 또한 **SAN**을 사용하는 경우에는 호스트를 추가 또는 삭제하거나 호스트 이름을 변경할 때 인증서를 수동으로 업데이트해야 합니다. 테넌트의 **DNS** 항목도 업데이트해야 합니다.

Lifecycle Manager는 테넌트별로 별도의 인증서를 생성하지 않습니다. 대신 각 테넌트 호스트 이름이 나열된 단일 인증서를 생성합니다. 기본 구성의 경우 테넌트의 **CNAME**은 다음 형식을 사용합니다.

tenantname vrahostname.domain. 고가용성 구성의 경우 이름은

tenantname.vraLBhostname.domain 형식을 사용합니다.

클러스터링된 **Workspace ONE Access** 구성을 사용하는 경우 **Lifecycle Manager**가 로드 밸런서 인증서를 업데이트할 수 없으므로 수동으로 업데이트해야 합니다. 또한 **Lifecycle Manager** 외부에 있는 제품 또는 서비스를 다시 등록해야 하는 경우 이 프로세스는 수동 프로세스입니다.

본 장은 다음 항목을 포함합니다.

- [vRealize Automation에 대한 다중 조직 테넌시 설정](#)
- [테넌트에 로그인하고 vRealize Automation에 사용자 추가](#)
- [vRealize Automation 다중 조직 배포에 vRealize Orchestrator 사용](#)

vRealize Automation에 대한 다중 조직 테넌시 설정

vRealize Suite Lifecycle Manager를 사용하여 **vRealize Automation**에 대한 다중 조직 테넌시를 설정할 수 있습니다.

다음은 **DNS** 및 인증서 구성을 포함하여 **vRealize Automation**에 대한 다중 테넌시를 설정하는 절차에 대한 개략적인 설명입니다. 단일 노드 배포에 중점을 두고 있지만 클러스터링된 구성에 대한 참고 사항을 포함합니다.

vRealize Automation 다중 조직 구성을 설정하는 방법에 대한 자세한 내용 및 비디오 데모는 <https://vmwarelab.org/2020/04/14/vrealize-automation-8-1-multi-tenancy-setup-with-vrealize-suite-lifecycle-manager-8-1/>에서 참조 하십시오.

사전 요구 사항

- **Workspace ONE Access** 버전 3.3.2를 설치하고 구성합니다.
- **vRealize Suite Lifecycle Manager** 버전 8.1을 설치하고 구성합니다.

절차

1 필요한 A 및 CNAME 유형 DNS 레코드를 생성합니다.

- 마스터 테넌트 및 각 하위 테넌트에 대해 SAN 인증서를 생성하고 적용해야 합니다.
- 단일 노드 배포의 경우 vRealize Automation FQDN은 vRealize Automation 장치를 가리키고 Workspace ONE Access FQDN은 Workspace ONE Access 장치를 가리킵니다.
- 클러스터링된 배포의 경우 Workspace ONE Access와 vRealize Automation 테넌트 기반 FQDN 모두 해당하는 로드 밸런서를 가리켜야 합니다. Workspace ONE Access는 SSL 종료를 사용하여 구성되므로 인증서가 Workspace ONE Access 클러스터와 로드 밸런서 모두에 적용됩니다. vRealize Automation 로드 밸런서는 SSL 패스스루를 사용하기 때문에 인증서가 vRealize Automation 클러스터에만 적용됩니다.

자세한 내용은 [단일 노드 다중 조직 배포에서 인증서 및 DNS 구성 관리](#) 및 [클러스터링된 vRealize Automation 배포에서 인증서 및 DNS 구성 관리](#)의 내용을 참조하십시오.

2 Workspace ONE 3.3.2 및 vRA 8.1 모두에 대해 필요한 다중 도메인(SAN) 인증서를 생성하거나 가져옵니다.

인증서 라이선스 및 암호를 생성할 수 있는 잠금 서비스를 사용하여 Lifecycle Manager에서 인증서를 생성할 수 있습니다. 또는 CA 서버 또는 다른 메커니즘을 사용하여 인증서를 생성할 수 있습니다.

추가 테넌트를 추가하거나 생성해야 하는 경우 vRealize Automation 및 Workspace ONE Access 테넌트를 다시 생성하고 적용해야 합니다.

인증서를 생성한 후에는 수명 주기 작업 기능을 사용하여 Lifecycle Manager 내에서 적용할 수 있습니다. 환경 및 제품을 선택한 다음 오른쪽 메뉴에서 [인증서 바꾸기] 옵션을 선택해야 합니다. 그런 다음 제품을 선택할 수 있습니다. 인증서를 바꾸는 경우 환경에서 연결된 모든 제품을 다시 신뢰해야 합니다.

다음 단계를 진행하기 전에 인증서가 적용되고 모든 서비스가 다시 시작될 때까지 기다려야 합니다.

자세한 내용은 [단일 노드 다중 조직 배포에서 인증서 및 DNS 구성 관리](#) 및 [클러스터링된 vRealize Automation 배포에서 인증서 및 DNS 구성 관리](#)의 내용을 참조하십시오.

3 Workspace ONE Access 인스턴스 또는 클러스터에 Workspace ONE SAN 인증서를 적용합니다.**4** vRealize Suite Lifecycle Manager 8.1에서 [테넌시 사용] 마법사를 실행하여 다중 테넌시를 사용하도록 설정하고 기본 마스터 테넌트에 대한 별칭을 생성합니다.

테넌시를 사용하도록 설정하려면 제공자 조직 마스터 테넌트 또는 기본 테넌트에 대한 별칭을 생성해야 합니다. 테넌시를 사용하도록 설정한 후에는 마스터 테넌트 FQDN을 통해 Workspace ONE Access에 액세스할 수 있습니다.

예를 들어 기존 Workspace ONE Access FQDN이 `idm.example.local`이고 기본 테넌트의 별칭을 생성한 경우, 테넌시를 사용하도록 설정하면 Workspace ONE Access FQDN이 `default-tenant.example.local`로 변경되고 Workspace ONE Access와 통신하는 모든 클라이언트가 이제 `default-tenant.example.local`를 통해 통신합니다.

5 vRealize Automation 인스턴스 또는 클러스터에 vRealize Automation SAN 인증서를 적용합니다.

Lifecycle Manager 수명 주기 작업 서비스를 통해 SAN 인증서를 적용할 수 있습니다. 환경의 세부 정보를 확인한 후 오른쪽 메뉴에서 [인증서 바꾸기]를 선택해야 합니다. 테넌트를 추가하기 전에 인증서 바꾸기 작업이 완료될 때까지 기다려야 합니다. 인증서 바꾸기의 일환으로 vRealize Automation 서비스가 다시 시작됩니다.

6 Lifecycle Manager에서 [테넌트 추가] 마법사를 실행하여 원하는 테넌트를 구성합니다.

[ID 및 테넌트 관리]에 있는 [Lifecycle Manager 테넌트 관리] 페이지를 사용하여 테넌트를 추가합니다. 이전에 인증서와 DNS 설정을 구성한 테넌트만 추가할 수 있습니다.

테넌트를 생성할 때 테넌트 관리자를 지정해야 하며 이 테넌트에 대한 Active Directory 연결을 선택할 수 있습니다. 사용 가능한 연결은 기본 또는 마스터 테넌트에서 구성된 연결을 기반으로 합니다. 또한 테넌트가 연결되는 제품 또는 제품 인스턴스를 선택해야 합니다.

다음에 수행할 작업

테넌트를 생성한 후에는 [ID 및 테넌트 관리]에 있는 [Lifecycle Manager 테넌트 관리] 페이지를 사용하여 테넌트 관리자를 변경하거나 추가하고, Active Directory 디렉토리를 테넌트에 추가하고, 테넌트에 대한 제품 연결을 변경할 수 있습니다.

또한 Workspace ONE Access 인스턴스에 로그인하여 테넌트 구성을 보고 검증할 수 있습니다.

단일 노드 다중 조직 배포에서 인증서 및 DNS 구성 관리

다중 조직 테넌시 vRealize Automation 구성은 여러 제품 간에 조정된 구성에 의존하며, 다중 조직 테넌시 구성이 작동하려면 DNS 설정과 인증서가 올바르게 구성되어 있어야 합니다.

다중 조직 구성은 다음 구성 요소에 대한 단일 노드 배포를 가정합니다.

- Lifecycle Manager
- Workspace ONE Access Identity Manager
- vRealize Automation

또한 제공자 조직에 해당하는 기본 테넌트로 시작하여 테넌트-1과 테넌트-2라는 두 개의 하위 테넌트를 생성한다고 가정합니다.

vRealize Suite Lifecycle Manager에서 잠금 관리자 서비스를 사용하여 인증서를 생성하고 적용하거나 다른 메커니즘을 사용할 수 있습니다. Lifecycle Manager를 사용하면 vRealize Automation 또는 Workspace ONE Access에서 인증서를 교체하거나 다시 신뢰할 수 있습니다.

DNS 요구 사항

아래에 설명된 대로 시스템 구성 요소에 대한 기본 A 유형 레코드와 CNAME 유형 레코드를 모두 생성해야 합니다.

- 다중 테넌시를 사용하도록 설정하는 경우 각 시스템 구성 요소와 생성할 각 테넌트 모두에 대해 기본 A 유형 레코드를 생성해야 합니다.

- 생성할 각각의 테넌트는 물론 마스터 테넌트에 대해 다중 테넌시 **A** 유형 레코드를 생성합니다.
- 마스터 테넌트를 제외하고 생성할 각각의 테넌트에 대해 다중 테넌시 **CNAME** 유형 레코드를 생성합니다.

단일 노드 다중 테넌시 배포를 위한 인증서 요구 사항

SAN(주체 대체 이름) 인증서 2개를(Workspace ONE Access용 1개와 vRealize Automation용 1개)를 생성해야 합니다.

- vRealize Automation 인증서에는 vRealize Automation 서버의 호스트 이름과 생성할 테넌트의 이름이 나열됩니다.
- Workspace ONE Access 인증서에는 Workspace ONE Access 서버의 호스트 이름과 생성 중인 테넌트 이름이 나열됩니다.
- 전용 SAN 이름을 사용하는 경우에는 호스트를 추가 또는 삭제하거나 호스트 이름을 변경할 때 인증서를 수동으로 업데이트해야 합니다. 테넌트의 DNS 항목도 업데이트해야 합니다. 구성을 간소화하는 옵션으로 Workspace ONE Access 및 vRealize Automation 인증서에 대해 와일드카드를 사용할 수 있습니다. 예: *.example.com 및 *.vra.example.com.

참고 vRealize Automation 8.x는 <https://publicsuffix.org>의 공용 접미사 목록에 있는 규격과 일치하는 DNS 이름에 대해서만 와일드카드 인증서를 지원합니다. 예를 들어 *.myorg.com은 올바른 이름이고 *.myorg.local은 잘못되었습니다.

Lifecycle Manager는 테넌트별로 별도의 인증서를 생성하지 않습니다. 대신 각 테넌트 호스트 이름이 나열된 단일 인증서를 생성합니다. 기본 구성의 경우 테넌트의 CNAME은 다음 형식을 사용합니다.

tenantname vrahostname.domain. 고가용성 구성의 경우 이름은 다음 형식을 사용합니다.

tenantname.vraLBhostname.domain.

요약

다음 표에는 단일 노드 Workspace ONE Access 및 단일 노드 vRealize Automation 배포를 위한 DNS 및 인증서 요구 사항이 요약되어 있습니다.

DNS 요구 사항	SAN 인증서 요구 사항
Main A Type Records lcm.example.local WorkspaceOne.example.local vra.example.local	Workspace One Certificate 호스트 이름: WorkspaceOne.example.local, default-tenant.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local
Multi-tenancy A Type Records default-tenant.example.local tenant-1.example.local tenant-2.example.local	
Multi-Tenancy CNAME Type Records tenant-1.vra.example.local tenant-2.vra.example.local	vRealize Automation Certificate 호스트 이름: vra.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local

클러스터링된 vRealize Automation 배포에서 인증서 및 DNS 구성 관리

클러스터링된 다중 조직 vRealize Automation 배포를 설정하려면 해당되는 모든 구성 요소 간에 인증서와 DNS 구성을 조정해야 합니다.

일반적인 클러스터링된 구성에는 3개의 Workspace ONE Access 장치와 3개의 vRealize Automation 장치뿐 아니라 단일 Lifecycle Manager 장치가 있습니다.

이 구성은 다음과 같은 구성 요소에 대해 클러스터링된 배포를 가정합니다.

- Workspace ONE Access Identity Manager 장치:

- idm1.example.local
- idm2.example.local
- idm3.example.local
- idm-lb.example.local

- vRealize Automation 장치:

- vra1.example.local
- vra2.example.local
- vra3.example.local
- vra-lb.example.local

- Lifecycle Manager 장치

DNS 요구 사항

다중 테넌시를 사용하도록 설정하는 경우 각 구성 요소와 생성하는 각 테넌트 모두에 대해 기본 A 유형 레코드를 생성해야 합니다. 또한 마스터 테넌트를 포함하지 않고 생성할 각 테넌트에 대해 다중 테넌시 CNAME 유형 레코드를 생성해야 합니다. 마지막으로 Workspace ONE Access 및 vRealize Automation 로드 밸런서에 대한 기본 A 유형 레코드도 생성해야 합니다.

- 3개의 Workspace ONE Access 장치와 해당하는 FQDN을 가리키는 vRealize Automation 장치에 대한 A 유형 레코드를 생성합니다.
- 또한 Workspace ONE Access 로드 밸런서와 해당하는 FQDN을 가리키는 vRealize Automation 로드 밸런서에 대한 A 유형 레코드를 생성합니다.
- Workspace ONE Access 로드 밸런서의 IP 주소를 가리키는 기본 테넌트 및 테넌트-1 및 테넌트-2에 대한 다중 테넌시 A 유형 레코드를 생성합니다.
- vRealize Automation 로드 밸런서의 IP 주소를 가리키는 테넌트-1 및 테넌트-2에 대한 CNAME 레코드를 생성합니다.

SAN(주체 대체 이름) 인증서 요구 사항

2개의 Workspace ONE Access 인증서를 생성해야 합니다. 클러스터 장치에 적용되는 인증서 하나와 로드 밸런서에 적용되는 인증서 하나입니다. 또한 vRealize Automation 장치, 생성하는 테넌트(기본 테넌트 제외) 및 로드 밸런서에 적용되는 인증서를 생성합니다.

- Workspace ONE Access 장치의 FQDN과 기본 테넌트 및 생성하는 다른 테넌트가 나열된 Workspace ONE Access 장치에 대한 인증서를 생성합니다. 이 인증서에는 Workspace ONE Access 장치의 IP 주소가 포함되어야 합니다.
- 가장 좋은 방법은 로드 밸런서에서 SSL 종료를 생성하는 것입니다. 이 종료를 지원하려면 Workspace ONE Access 로드 밸런서의 FQDN과 기본 테넌트 및 생성하는 다른 테넌트가 나열된 Workspace ONE Access 로드 밸런서에 대한 인증서를 생성합니다. 이 인증서에는 로드 밸런서의 IP 주소가 포함되어야 합니다.
- 관련 로드 밸런서 및 생성하려는 테넌트를 비롯한 3개의 vRealize Automation 장치의 호스트 이름을 나열하는, vRealize Automation에 대한 인증서를 생성해야 합니다. 또한 3개의 vRealize Automation 장치에 대한 IP 주소를 나열해야 합니다.
- 선택 사항으로, 구성을 간소화하기 위해 Workspace ONE Access 및 vRealize Automation 인증서에 와일드카드를 사용할 수 있습니다. 예: *.example.com, *.vra.example.com 및 *.vra-lb.example.com.

참고 vRealize Automation 8.x는 <https://publicsuffix.org>의 공용 접미사 목록에 있는 규격과 일치하는 DNS 이름에 대해서만 와일드카드 인증서를 지원합니다. 예를 들어 *.myorg.com은 올바른 이름이고 *.myorg.local은 잘못되었습니다.

클러스터링된 Workspace ONE Access 구성을 사용하는 경우 Lifecycle Manager가 로드 밸런서 인증서를 업데이트할 수 없으므로 해당 인증서를 수동으로 업데이트해야 합니다. 또한 Lifecycle Manager 외부에 있는 제품 또는 서비스를 다시 등록해야 하는 경우 이 프로세스는 수동 프로세스입니다.

클러스터링된 다중 조직 구성에 대한 DNS 항목 및 인증서 요약

다음 표에는 클러스터링된 Workspace ONE Access 및 클러스터링된 vRealize Automation 다중 조직 배포에 대한 DNS 및 인증서 요구 사항이 요약되어 있습니다.

DNS 요구 사항	SAN 인증서 요구 사항
Main A Type Records lcm.example.local WorkspaceOne-1.example.local WorkspaceOne-2.example.local WorkspaceOne-3.example.local vra.example-1.local vra.example-2.local vra.example-3.local	Workspace One Certificate 호스트 이름: WorkspaceOne.example.local, default-tenant.example.local, tenant-1.example.local, tenant-2.example.local
Multi-Tenancy A Type Records default-tenant.example.local tenant-1.vra.example.local tenant-2.vra.example.local	Workspace One LB Certificate (LB Terminated) 호스트 이름: WorkSpaceOne-lb.example.local, default-tenant.example.local, vra.example.local, tenant-1.example.local, tenant-2.example.local
Multi-Tenancy CNAME Type Records tenant-1.vra-lb.example.local - vra-lb.example.local tenant-2.vra-lb.example.local - vra.lb.example.local	vRealize Automation Certificate 호스트 이름: vra-1.example.local, vra-2.example.local, vra-3.example.local, vra-lb.example.local, tenant-1.example.local, tenant-2.example.local SSL 패스스루를 사용하기 때문에 vRealize Automation 로드 밸런서에 인증서가 필요하지 않습니다.

테넌트에 로그인하고 vRealize Automation에 사용자 추가

Lifecycle Manager에서 vRealize Automation에 대한 테넌트를 생성한 후 Workspace ONE Access에 로그인하여 테넌트를 보고 사용자를 추가할 수 있습니다.

연결된 Workspace ONE Access 인스턴스에 로그인하여 vRealize Automation 배포에 대해 생성된 테넌트를 볼 수 있습니다. 사용할 URL은 `https://default-tenant.name.domainname.local`이거나 클러스터링되지 않은 배포의 경우 `https://idm.domainname.local`로, 이는 기본 테넌트 Workspace ONE Access URL로 다시 연결합니다.

다음 URL을 사용하여 Workspace ONE Access에서 특정 테넌트를 검증할 수 있습니다. `https://tenant-1.domainname.local`. 이 URL은 지정된 테넌트에 대한 사용자를 표시하는 페이지를 엽니다. **사용자 추가**를 클릭하여 임시로 추가 사용자를 생성할 수 있습니다.

인증된 사용자는 `https://vra.domainname.local`을 사용하여 vRealize Automation의 기본 제공자 조직에 로그인할 수 있습니다. 이 보기는 모든 vRealize Automation 관련 서비스에 대한 액세스를 제공합니다.

인증된 사용자는 `https://tenantname.vra.domainname.local`을 사용하여 vRealize Automation의 해당 테넌트에 로그인할 수 있습니다.

Workspace ONE Access의 사용자 관리에 대한 자세한 내용은 <https://docs.vmware.com/kr/VMware-Workspace-ONE-Access/3.3/idm-administrator.pdf>의 내용을 참조하십시오.

로컬 사용자 추가

연결된 Workspace ONE Access 인스턴스를 사용하여 배포에 로컬 사용자를 추가할 수 있습니다. 로컬 사용자는 외부 ID 제공자에 저장되지 않는 사용자입니다.

vRealize Automation 다중 조직 배포에 vRealize Orchestrator 사용

vRealize Automation 다중 조직 테넌트 배포에 vRealize Orchestrator를 사용할 수 있습니다.

기본 테넌트는 기본적으로 내장된 vRealize Orchestrator 통합과의 통합을 지원합니다. vRealize Orchestrator는 통합 페이지에서 미리 구성된 대로 사용할 수 있습니다. 하위 테넌트에 미리 등록된 vRealize Orchestrator 통합이 없습니다. vRealize Orchestrator 통합을 추가하는 몇 가지 옵션이 있습니다.

- vRealize Orchestrator의 [인증 제공자 구성]으로 이동하고 해당 vRealize Automation 테넌트의 호스트 주소를 사용하여 연결하여 내장된 vRealize Orchestrator와의 통합을 추가할 수 있습니다. 그런 다음 **인프라 > 연결 > 통합**을 선택하고 내장된 vRO를 통합으로 추가할 수 있습니다.
- 다중 조직 vRealize Automation을 인증 제공자로 사용하는 외부 vRealize Orchestrator 인스턴스를 추가할 수 있습니다.

vRealize Automation 다중 조직 배포를 인증 제공자로 사용하는 모든 vRealize Orchestrator 인스턴스는 새 통합을 생성하고 자격 증명을 제공하지 않고 vRealize Orchestrator FQDN을 제공하여 모든 테넌트에 등록할 수 있습니다.

vRealize Automation에서 로그 사용

5

제공된 `vracli` 명령줄 유틸리티를 사용하여 vRealize Automation에서 로그를 생성 및 사용할 수 있습니다.

vRealize Automation에서 직접 로그를 사용하거나 대신 vRealize Log Insight로 모든 로그를 전달할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- vRealize Automation에서 로그 및 로그 번들을 사용하는 방법
- vRealize Log Insight로 로그 전달을 구성하는 방법
- vRealize Automation에서 Syslog 통합을 생성하거나 업데이트하는 방법

vRealize Automation에서 로그 및 로그 번들을 사용하는 방법

vRealize Automation에서 vRealize Automation 로그 및 로그 번들을 생성 및 사용할 수 있습니다.

또는 자동으로 로그를 vRealize Log Insight로 전달할 수 있습니다. 로그를 vRealize Log Insight로 전달하는 방법에 대한 자세한 내용은 [vRealize Log Insight로 로그 전달을 구성하는 방법](#)을 참조하십시오.

`vracli` 명령줄 유틸리티를 사용하는 방법에 대한 정보는 `vracli` 명령줄에서 `--help` 인수를 사용하여 확인할 수 있습니다. 예를 들면 `vracli log-bundle --help`입니다.

로그 번들 명령

단순 로그 번들 또는 모든 서비스의 집계된(콜드 스토리지) 로그를 생성할 수 있습니다. 두 로그 번들 모두 서비스에 대한 모든 로그를 포함하지만 콜드 스토리지 번들에는 추가 문제 해결 값을 제공할 수 있는 백버전의 서비스 로그의 집계된 스트림의 복사본이 포함됩니다. 콜드 스토리지 에이전트는 지속적으로 서비스에서 로그를 집계하고 로컬 파일 시스템에 저장합니다. 단순 로그 번들은 일반적으로 문제 해결에 필요한 모든 것입니다.

각 노드에서 로그를 수집하기 위한 기본 시간 초과 값을 변경할 수도 있습니다.

클러스터된 환경에서는 한 노드에서만 `vracli log-bundle` 명령을 실행하면 됩니다.

- 로그 번들 명령 도움말을 표시합니다.

```
vracli log-bundle --help
```

- 단순 로그 번들을 생성합니다.

```
vracli log-bundle
```

- 콜드 스토리지 로그 번들을 생성합니다.

```
vracli log-bundle --include-cold-storage
```

- 각 노드에서 로그를 수집하기 위한 시간 초과 값을 변경합니다. 예를 들어 환경에 대규모 로그 파일, 느린 네트워킹, 높은 CPU 사용량 등이 포함된 경우 시간 초과를 1000초 기본값보다 크게 설정해야 할 수 있습니다.

```
vracli log-bundle --collector-timeout $CUSTOM_TIMEOUT_IN_SECONDS
```

로그 번들 구조

vRealize Automation 서비스는 Kubernetes 포드에서 컨테이너화되었습니다. 생성된 로그 번들은 `log-bundle-{{TIMESTAMP}}.tar.xz` 이름 형식을 사용하는 `tar.xz` 아카이브입니다. 여기서 `TIMESTAMP`는 초 단위의 epoch 타임 스탬프입니다. 일반 로그 번들에는 환경의 모든 노드의 로그가 포함됩니다. 어떤 이유로 로그 번들을 생성할 수 없는 경우 폴백 번들이 대신 생성됩니다. 폴백 번들에는 현재 노드에 대한 로그만 포함됩니다. 이 두 가지 로그 번들 유형의 구조에는 다소 차이가 있습니다.

- 일반 로그 번들

일반 로그 번들은 다음과 같은 범주로 구성됩니다.

- 호스트 로그 및 구성

각 호스트 및 호스트별 로그에 대한 구성이 클러스터 노드(호스트)당 하나의 디렉토리에 수집됩니다. 디렉토리 이름은 노드 호스트 이름과 일치합니다. 디렉토리 콘텐츠는 호스트 파일 시스템과 일치합니다. 디렉토리 수는 클러스터 노드 수와 일치합니다.

콜드 스토리지 로그는 `/hostname/services-logs/all/aggregated.log`로 구조화된 JSON 로그에 있습니다.

- 포드 로그

서비스는 Kubernetes 포드에서 컨테이너화되었습니다. 서비스 로그는 네임스페이스당 단일 디렉토리가 포함된 `pods` 디렉토리에 있으며 파일 이름은 해당 네임스페이스 이름과 일치합니다. 일반적으로 클러스터 노드당 각 포드의 하나의 인스턴스가 있습니다. 포드 디렉토리에는 각 컨테이너 애플리케이션에 대한 로그 파일이 포함됩니다.

예를 들어 vRealize Orchestrator Control Center 로그는 각 `/pods/prelude/vco-app-hash/` 디렉토리의 `vco-controlcenter-app.log` 파일에 상주합니다.

- 환경 파일

환경 파일에는 노드 및 포드당 현재 리소스 사용량에 대한 정보가 포함됩니다. 모든 사용 가능한 Kubernetes 엔티티에 대한 클러스터 정보 및 설명도 포함됩니다.

- 폴백 로그 번들

vracli 명령이 완료될 때까지 기다리는 동안 오류 메시지를 수신하는 경우 폴백 번들이 생성됩니다. 이 오류를 수신하는 경우 클러스터의 각 호스트 또는 노드에서 **vracli log-bundle** 명령을 실행하여 최대한 많은 정보를 수집해야 합니다.

■ 폴백 컨테이너 로그

폴백 로그는 `/fallback-containers` 디렉토리에 있습니다. 로그 파일 이름을 검토하여 포드가 로그를 생성한 컨테이너를 식별할 수 있습니다.

pod-name-some-hash-container-name-other-hash.log

■ 폴백 콜드 스토리지

번들과 함께 콜드 스토리지 로그를 수집하는 경우 현재 호스트의 폴백 로그는 `/fallback-cold-storage` 디렉토리에 있습니다.

vRealize Log Insight로 로그 전달을 구성하는 방법

더욱 강력한 로그 분석 및 보고서 생성을 활용하기 위해 vRealize Automation에서 vRealize Log Insight로 로그를 전달할 수 있습니다.

vRealize Automation은 **fluentd-based** 로깅 에이전트와 함께 번들로 구성됩니다. 에이전트는 로그 번들에 포함되고 나중에 검토될 수 있도록 로그를 수집 및 저장합니다. vRealize Log Insight API를 사용하여 로그의 복사본을 vRealize Log Insight 서버로 전달하도록 에이전트를 구성할 수 있습니다. 제공된 API는 기타 프로그램이 vRealize Log Insight와 통신하도록 허용합니다.

vRealize Log Insight에 대한 자세한 내용은 vRealize Log Insight API 설명서를 포함하여 **vRealize Log Insight 설명서** 및 `/api/v1/events/ingest/{agentId}` 페이지를 참조하십시오.

제공된 **vracli** 명령줄 유틸리티를 사용하여 자동으로 계속해서 vRealize Automation 로그를 vRealize Log Insight로 전달하도록 로깅 에이전트를 구성합니다.

모든 로그 줄에는 호스트 이름 및 환경 태그가 지정되어 있기 때문에 vRealize Log Insight에서 검사할 수 있습니다. HA(고가용성) 환경에서 로그에는 로그가 시작된 노드에 따라 서로 다른 호스트 이름으로 태그가 지정됩니다. 환경 태그는 아래의 "vRealize Log Insight 통합 구성 또는 업데이트" 섹션에 설명된 대로 `--environment ENV` 옵션을 사용하여 구성할 수 있습니다. HA 환경에서 환경 태그는 로그가 시작된 노드에 관계없이 모든 로그 줄에 대해 동일한 값을 가집니다.

vracli 명령줄 유틸리티를 사용하는 방법에 대한 정보는 **vracli** 명령줄에서 `--help` 인수를 사용하여 확인할 수 있습니다. 예를 들면 **vracli vrli --help**입니다.

vRealize Log Insight의 기존 구성 확인

Command

vracli vrli

Arguments

명령줄 인수가 없습니다.

Output

vRealize Log Insight 통합에 대한 현재 구성이 JSON 형식으로 출력됩니다.

Exit codes

다음과 같은 종료 코드가 가능합니다.

- 0 - vRealize Log Insight와의 통합이 구성되었습니다.
- 1 - 명령 실행의 일부로 예외가 발생했습니다. 자세한 내용은 오류 메시지를 검토하십시오.
- 61(ENODATA) - vRealize Log Insight와의 통합이 구성되지 않았습니다. 자세한 내용은 오류 메시지를 검토하십시오.

Example – check integration configuration

```
$ vracli vrli
No vRLI integration configured

$ vracli vrli
{
  "agentId": "0",
  "environment": "prod",
  "host": "my-vrli.local",
  "port": 443,
  "scheme": "https",
  "sslVerify": false
}
```

참고 다음 샘플에 표시된 것과 같이 로그를 전송하는 데 사용할 서로 다른 호스트 체계(기본값: https) 및 포트(기본값: 443)를 설정할 수 있습니다.

```
vracli vrli set some-host
vracli vrli set some-host:9543
vracli vrli set http://some-host:9543
```

포트 9543은 [vRealize Log Insight 설명서](#)의 "vRealize Log Insight 관리" 항목 "포트 및 외부 인터페이스"에 설명된 것과 같이 vRealize Log Insight 수집 API에서 사용됩니다.

vRealize Log Insight의 통합 구성 또는 업데이트

Command

```
vracli vrli set [options] FQDN_OR_URL
```

Arguments

다음 명령줄 인수를 사용할 수 있습니다.

- FQDN_OR_URL - vRealize Log Insight API 구성을 사용하여 로그를 게시하는 데 사용될 vRealize Log Insight 서버의 FQDN 또는 IP 주소입니다. 기본적으로 포트 443 및 HTTPS 스키마가 사용됩니다. 이러한 설정 중 하나를 변경해야 하는 경우 URL을 대신 사용할 수 있습니다.

■ 옵션

- **--agent-id SOME_ID** - 이 장치에 대한 로깅 에이전트의 ID를 설정합니다. 기본값은 0입니다. vRealize Log Insight API 구성을 사용하여 vRealize Log Insight에 게시되는 로그에 대한 로깅 에이전트를 식별하는 데 사용됩니다.
- **--environment ENV** - 현재 환경에 대한 식별자를 설정합니다. vRealize Log Insight 로그에서 각 로그 줄 이벤트에 대한 태그로 사용할 수 있습니다. 기본값은 **prod**입니다.
- **--ca-file /path/to/server-ca.crt** - vRealize Log Insight 서버 인증서를 서명하는 데 사용되었던 CA(인증 기관) 인증서가 포함된 파일을 지정합니다. 로깅 에이전트가 지정된 CA를 신뢰하도록 강제하고 vRealize Log Insight 서버의 인증서를 확인하도록 설정합니다. 인증서를 확인하기 위해 필요한 경우 파일에 전체 인증서 체인이 포함될 수 있습니다. 자체 서명된 인증서의 경우 인증서 자체를 전달합니다.
- **--ca-cert CA_CERT** - **--ca-file**과 동일한 방식으로 파일을 지정하지만 인증서(체인) 인라인을 문자열로 전달합니다.
- **--insecure** - 서버 인증서의 SSL 확인을 비활성화합니다. 로그를 게시할 때 로깅 에이전트가 모든 SSL 인증서를 수락하도록 강제합니다.

Output

출력이 예상되지 않습니다.

Exit codes

다음과 같은 종료 코드가 가능합니다.

- 0 - 구성이 업데이트되었습니다.
- 1 - 실행의 일부로 예외가 발생했습니다. 자세한 내용은 오류 메시지를 검토하십시오.

Examples – Configure or update integration configuration

```
$ vracli vrli set my-vrli.local
$ vracli vrli set 10.20.30.40

$ vracli vrli set --ca-file /etc/ssl/certs/ca.crt 10.20.30.40

$ vracli vrli set --ca-cert "$(cat /etc/ssl/certs/ca.crt)" 10.20.30.40

$ vracli vrli set --insecure http://my-vrli.local:8080

$ vracli vrli set --agent-id my-vrli-agent my-vrli.local

$ vracli vrli set --environment staging my-vrli.local
```

vRealize Log Insight의 통합 지우기

Command

```
vracli vrli unset
```

Arguments

명령줄 인수가 없습니다.

Output

확인이 일반 텍스트 형식으로 출력됩니다.

Exit codes

다음과 같은 종료 코드가 가능합니다.

- 0 - 구성이 지워졌거나 구성이 없습니다.
- 1 - 실행의 일부로 예외가 발생했습니다. 자세한 내용은 오류 메시지를 검토하십시오.

Examples – Clear integration

```
$ vracli vrli unset
Clearing vRLI integration configuration

$ vracli vrli unset
No vRLI integration configured
```

vRealize Automation에서 Syslog 통합을 생성하거나 업데이트하는 방법

Syslog 서버에 로깅 정보를 보내도록 vRealize Automation을 구성할 수 있습니다.

`vracli remote-syslog set` 명령은 Syslog 통합을 생성하거나 기존 통합을 덮어쓰는 데 사용됩니다.

vRealize Automation 원격 Syslog 통합은 다음 연결 유형을 지원합니다.

- UDP 연결.
- TLS를 사용하지 않는 TCP 연결.

참고 TLS를 사용하지 않고 Syslog 통합을 생성하려면 `vracli remote-syslog set` 명령에 `--disable-ssl` 플래그를 추가합니다.

- TLS를 사용한 TCP 연결.

vRealize Log Insight와의 로깅 통합 구성에 대한 자세한 내용은 [vRealize Log Insight로 로그 전달을 구성하는 방법](#) 항목을 참조하십시오.

사전 요구 사항

하나 이상의 원격 Syslog 서버를 구성합니다.

절차

- 1 vRealize Automation 장치 명령줄에 **root**로 로그인합니다.

- 2 Syslog 서버에 대해 통합을 생성하려면 `vraccli remote-syslog set` 명령을 실행합니다.

```
vraccli remote-syslog set -id name_of_integration protocol_type://syslog_URL_or_FQDN:syslog_port
```

참고 `vraccli remote-syslog set` 명령에 포트를 입력하지 않으면 포트 값은 기본적으로 514이 됩니다.

참고 Syslog 구성에 인증서를 추가할 수 있습니다. 인증서 파일을 추가하려면 `--ca-file` 플래그를 사용합니다. 인증서를 일반 텍스트로 추가하려면 `--ca-cert` 플래그를 사용합니다.

- 3 (선택 사항) 기존 Syslog 통합을 덮어쓰려면 `vraccli remote-syslog set`를 실행하고 `-id` 플래그 값을 덮어쓸 통합의 이름으로 설정합니다.

참고 기본적으로 vRealize Automation 장치는 Syslog 통합을 덮어쓸 것인지 확인을 요청합니다. 확인 요청을 건너뛰려면 `-f` 또는 `--force` 플래그를 `vraccli remote-syslog set` 명령에 추가합니다.

다음에 수행할 작업

장치에서 현재 Syslog 통합을 검토하려면 `vraccli remote-syslog` 명령을 실행합니다.

vRealize Automation 에서 로깅을 위해 Syslog 통합을 삭제하는 방법

`vraccli remote-syslog unset` 명령을 실행하여 vRealize Automation 장치에서 Syslog 통합을 삭제할 수 있습니다.

사전 요구 사항

vRealize Automation 장치에서 Syslog 통합을 하나 이상 생성합니다. [vRealize Automation에서 Syslog 통합을 생성하거나 업데이트하는 방법](#)의 내용을 참조하십시오.

절차

- 1 vRealize Automation 장치 명령줄에 **root**로 로그인합니다.
- 2 다음 방법 중 하나를 사용하여 vRealize Automation 장치에서 Syslog 통합을 삭제합니다.
 - 특정 Syslog 통합을 삭제하려면 `vraccli remote-syslog unset -id Integration_name` 명령을 실행합니다.
 - vRealize Automation 장치에서 모든 Syslog 통합을 삭제하려면 `-id` 플래그 없이 `vraccli remote-syslog unset` 명령을 실행합니다.

참고 기본적으로 vRealize Automation 장치는 모든 Syslog 통합을 삭제할 것인지 확인을 요청합니다. 확인 요청을 건너뛰려면 `-f` 또는 `--force` 플래그를 `vraccli remote-syslog unset` 명령에 추가합니다.

vRealize Automation의 고객 환경 향상 프로그램 참여

6

이 제품은 VMware의 CEIP(고객 환경 향상 프로그램)에 참여하는 제품입니다. CEIP는 VMware가 제품 및 서비스를 개선하고, 문제를 수정하고, VMware 제품을 배포하고 사용하는 최적의 방법을 사용자에게 알려주도록 하는 정보를 VMware에 제공합니다.

CEIP를 통해 수집되는 데이터에 대한 세부 정보와 VMware에서 해당 정보를 사용하는 목적은 신뢰 및 보장 센터(<http://www.vmware.com/trustvmware/ceip.html>)에 명시되어 있습니다.

본 장은 다음 항목을 포함합니다.

- vRealize Automation의 고객 환경 향상 프로그램 참여 또는 탈퇴 방법
- vRealize Automation의 고객 환경 향상 프로그램에 대한 데이터 수집 시간을 구성하는 방법

vRealize Automation의 고객 환경 향상 프로그램 참여 또는 탈퇴 방법

CEIP(고객 환경 향상 프로그램)는 vRealize Automation 장치 명령줄에서 참여하거나 탈퇴할 수 있습니다.

vRealize Automation를 설치하고 vRealize LCM(Lifecycle Manager)을 사용하여 CEIP 프로그램에 참여할 수 있습니다. 설치 후 명령줄 옵션을 사용하여 프로그램에 참여하거나 탈퇴할 수도 있습니다.

명령줄 옵션을 사용하여 고객 환경 향상 프로그램에 참여하려면:

- 1 vRealize Automation 장치 명령줄에 **root**로 로그인합니다.
- 2 `vracli ceip on` 명령을 실행합니다.
- 3 고객 환경 향상 프로그램 정보를 검토하고 `vracli ceip on --acknowledge-ceip` 명령을 실행합니다.
- 4 vRealize Automation 서비스를 다시 시작하려면 `/opt/scripts/deploy.sh` 명령을 실행합니다.

명령줄 옵션을 사용하여 고객 환경 향상 프로그램에서 탈퇴하려면:

- 1 vRealize Automation 장치 명령줄에 **root**로 로그인합니다.
- 2 `vracli ceip off` 명령을 실행합니다.
- 3 vRealize Automation 서비스를 다시 시작하려면 `/opt/scripts/deploy.sh` 명령을 실행합니다.

vRealize Automation의 고객 환경 항상 프로그램에 대한 데이터 수집 시간을 구성하는 방법

CEIP(고객 환경 항상 프로그램)에서 VMware로 데이터를 보내는 요일과 시간을 설정할 수 있습니다.

절차

1 vRealize Automation 장치 명령줄에 **root**로 로그인합니다.

2 텍스트 편집기에서 다음 파일을 엽니다.

`/etc/telemetry/telemetry-collector-vami.properties`

3 요일(`dow`)과 시간(`hod`) 속성을 편집합니다.

속성	설명
<code>frequency.dow=<day-of-week></code>	데이터 수집을 수행하는 요일.
<code>frequency.hod=<hour-of-day></code>	데이터 수집을 수행하는 현지 시간. 가능한 값은 0-23입니다.

4 `telemetry-collector-vami.properties`를 저장하고 닫습니다.

5 다음 명령을 입력하여 설정을 적용합니다.

`vcac-config telemetry-config-update --update-info`

변경 내용이 배포에 포함된 모든 노드에 적용됩니다.