

# vRealize Automation 관리

2020년 12월 21일

vRealize Automation 8.0

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](http://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](http://www.vmware.com/kr)

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

# 목차

<b>1</b>	<b>vRealize Automation 관리</b>	<b>4</b>
<b>2</b>	<b>사용자 관리</b>	<b>5</b>
	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
<b>3</b>	<b>장치 유지 보수</b>	<b>9</b>
	vRealize Automation 시작 및 중지	9
	시간 동기화를 사용하도록 설정하는 방법	10
	시간 동기화를 비활성화하는 방법	11
	루트 암호를 재설정하는 방법	12
<b>4</b>	<b>로그 사용</b>	<b>14</b>
	로그 및 로그 번들을 사용하는 방법	14
	vRealize Log Insight로 로그 전달을 구성하는 방법	16
<b>5</b>	<b>고객 환경 향상 프로그램 참여</b>	<b>20</b>
	프로그램 참여 또는 탈퇴 방법	20
	프로그램에 대한 데이터 수집을 구성하는 방법	21

# vRealize Automation 관리

# 1

대부분의 vRealize Automation 관리 작업이 VMware vRealize Suite Lifecycle Manager에서 완료되지만 이 가이드에서는 vRealize Automation 내에서 완료할 수 있는 일부 중요한 사용자 및 시스템 관리 작업을 설명합니다.

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

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** vRealize Automation 8.0.0에서는 재해 복구가 지원되지 않습니다. 재해 복구 시나리오에서 vRealize Automation을 사용하려면 vRealize Automation 8.0.1 이상으로 업그레이드하십시오.

---

# 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 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.

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
	■ Service Broker 관리자
	■ Service Broker 사용자
	■ 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.

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 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 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 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 `vracli 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.
- 2 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
```

### 3 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.

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

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

- 3 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 완료되어야 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.

```
kubectl -n prelude get pods
```

## 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 경우 이 구성을 사용할 수 있습니다. 클러스터링된 배포를 사용하는 경우 모든 ESXi 호스트가 NTP 서버와 동기화되어야 합니다.</p> <p><b>참고</b> 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 <a href="#">57147 vSphere Web Client를 사용하여 ESXi 호스트에서 NTP(Network Time Protocol) 구성</a>을 참조하십시오.</p>
systemd	<p>이 구성은 systemd-timesyncd 데몬을 사용하여 vRealize Automation 배포의 클럭을 동기화합니다.</p> <p><b>참고</b> 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 --enable` 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.

## 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 NTP 구성을 비활성화합니다.
  - a `vracli ntp esxi --disable` 명령을 실행합니다.
  - b `vracli ntp apply` 명령을 실행합니다.

ESXi NTP 구성이 비활성화되었습니다.
- 3 systemd NTP 구성을 비활성화합니다.
  - a `vracli ntp systemd --disable FQDN_or_IP_of_systemd_server` 명령을 실행합니다.
  - b `vracli ntp apply` 명령을 실행합니다.

systemd NTP 구성이 비활성화되었습니다.
- 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 rw init=/bin/bash
line coredump_filter=0x37 consoleblank=0
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 로그 사용

# 4

제공된 `vraccli` 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 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.

`vraccli` 명령줄 유틸리티를 사용하는 방법에 대한 정보는 `vraccli` 명령줄에서 `--help` 인수를 사용하여 확인할 수 있습니다. 예를 들면 `vraccli 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 `vraccli log-bundle` 명령을 실행하면 됩니다.

- 로그 번들 명령 도움말을 표시합니다.

```
vraccli log-bundle --help
```

- 단순 로그 번들을 생성합니다.

```
vraccli 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.

**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 Automation의 고객 환경 향상 프로그램 참여

## 5

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 향상 프로그램에 대한 데이터 수집 시간을 구성하는 방법

CEIP(고객 환경 향상 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=&lt;day-of-week&gt;</code>	데이터 수집을 수행하는 요일.
<code>frequency.hod=&lt;hour-of-day&gt;</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.