

Verwalten von vRealize Automation

21. Dezember 2020
vRealize Automation 8.0

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

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

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2021 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

- 1** Verwalten von vRealize Automation 4
- 2** Verwalten von Benutzern 5
 - Aktivieren von Active Directory-Gruppen in vRealize Automation für Projekte 6
 - Entfernen von Benutzern in vRealize Automation 7
 - Wie bearbeite ich Benutzerrollen in vRealize Automation? 7
 - Vorgehensweise zum Bearbeiten der Rollenzuweisung für Gruppen in vRealize Automation 8
- 3** Verwalten der Appliance 10
 - Starten und Stoppen von vRealize Automation 10
 - Vorgehensweise zum Aktivieren der Uhrzeitsynchronisierung 12
 - Vorgehensweise zum Deaktivieren der Uhrzeitsynchronisierung 13
 - Wie setze ich das Root-Kennwort zurück? 14
- 4** Arbeiten mit Protokollen 16
 - Wie arbeite ich mit Protokollen und Protokollpaketen? 16
 - Wie konfiguriere ich die Protokollweiterleitung zu vRealize Log Insight? 18
- 5** Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit 23
 - Wie nehme ich am Programm teil bzw. wie beende ich die Teilnahme? 23
 - Wie konfiguriere ich die Datenerfassungszeit für das Programm? 24

Verwalten von vRealize Automation

1

Während die meisten Verwaltungsaufgaben in vRealize Automation von VMware vRealize Suite Lifecycle Manager durchgeführt werden, beschreibt dieses Handbuch einige wichtige Benutzer- und Systemverwaltungsaufgaben, die Sie innerhalb von vRealize Automation durchführen können.

Weitere Informationen zum Arbeiten mit vRealize Suite Lifecycle Manager finden Sie unter [Installation, Upgrade und Verwaltung von vRealize Suite Lifecycle Manager](#).

Einige vRealize Automation-Verwaltungsaufgaben werden innerhalb von vRealize Automation abgeschlossen, für andere müssen verwandte Produkte wie vRealize Suite Lifecycle Manager und Workspace ONE Access genutzt werden. Die Benutzer sollten sich mit diesen Produkten und ihren Funktionalitäten vertraut machen, bevor sie die entsprechenden Aufgaben ausführen.

Informationen zur Sicherung, Wiederherstellung und zur Notfallwiederherstellung finden Sie z. B. im Abschnitt über **Sicherung und Wiederherstellung und Notfallwiederherstellung > 2019** in der [vRealize Suite-Produktdokumentation](#).

Hinweis Die Notfallwiederherstellung wird von vRealize Automation 8.0.0 nicht unterstützt. Um vRealize Automation in Szenarien mit Notfallwiederherstellung verwenden zu können, führen Sie ein Upgrade auf vRealize Automation 8.0.1 oder höher durch.

Verwalten von Benutzern und Gruppen in vRealize Automation

2

vRealize Automation verwendet VMware Workspace ONE Access, die von VMware zur Verfügung gestellte Identitätsverwaltungsanwendung, zum Importieren und Verwalten von Benutzern und Gruppen. Nach dem Importieren oder Erstellen von Benutzern und Gruppen können Sie Rollenzuweisungen über die Seite „Identitäts- und Zugriffsverwaltung“ verwalten.

vRealize Automation wird mithilfe von VMware Lifecycle Manager (vRSLCM oder LCM) installiert. Bei der Installation von vRealize Automation müssen Sie eine vorhandene Workspace ONE Access-Instanz importieren oder eine neue bereitstellen, damit die Identitätsverwaltung unterstützt wird. Diese beiden Szenarien definieren Ihre Verwaltungsoptionen.

- Wenn Sie eine neue Workspace ONE Access-Instanz bereitstellen, können Sie Benutzer und Gruppen über LCM verwalten. Während der Installation können Sie eine Active Directory-Verbindung mithilfe von Workspace ONE Access einrichten. Alternativ können Sie einige Aspekte von Benutzern und Gruppen innerhalb von vRealize Automation über die Seite „Identitäts- und Zugriffsverwaltung“ anzeigen und bearbeiten. Das wird hier beschrieben.
- Wenn Sie eine vorhandene Workspace ONE Access-Instanz verwenden, importieren Sie sie während der Installation für die Verwendung mit vRealize Automation über LCM. In diesem Fall können Sie zum Verwalten von Benutzern und Gruppen weiterhin Workspace ONE Access verwenden, oder Sie können die Verwaltungsfunktionen in LCM verwenden.

vRealize Automation-Benutzern müssen Rollen zugewiesen werden. Rollen definieren die Zugriffsrechte auf Funktionen innerhalb der Anwendung. Wenn vRealize Automation mit einer Workspace ONE Access-Instanz installiert wird, wird eine Standardorganisation erstellt und dem Installationsprogramm wird die Rolle des Organisationsbesitzers zugewiesen. Alle anderen vRealize Automation-Rollen werden vom Organisationsbesitzer zugewiesen.

In vRealize Automation gibt es drei Arten von Rollen: Organisationsrollen, Dienstrollen und Projektrollen. Für vRealize Automation Cloud Assembly, Service Broker und Code Stream können Rollen auf Benutzerebene typischerweise Ressourcen verwenden, während Rollen auf Administratorebene erforderlich sind, um Ressourcen zu erstellen und zu konfigurieren. Organisationsrollen definieren Berechtigungen innerhalb des Mandanten. Organisationsbesitzer verfügen über Berechtigungen auf Administratorebene, während Organisationsmitglieder über Berechtigungen auf Benutzerebene verfügen. Organisationsbesitzer können andere Benutzer hinzufügen und verwalten.

Organisationsrollen	Dienstrollen
■ Organisationsbesitzer	■ Cloud Assembly-Administrator
■ Organisationsmitglied	■ Cloud Assembly-Benutzer
	■ Service Broker-Administrator
	■ Service Broker-Benutzer
	■ Code Stream-Administrator
	■ Code Stream-Benutzer
	■ Code Stream-Betrachter

Darüber hinaus gibt es zwei Hauptrollen auf Projektebene, die nicht in der Tabelle angezeigt werden: Projektadministrator und Projektbenutzer. Diese Rollen werden projektbezogen ad hoc mit Cloud Assembly zugewiesen. Diese Rollen sind fließend. Derselbe Benutzer kann ein Administrator für ein Projekt und ein Benutzer in einem anderen Projekt sein.

Weitere Informationen zum Arbeiten mit LCM und Workspace ONE Access finden Sie unter [Benutzerverwaltung mit VMware Identity Manager](#).

Dieses Kapitel enthält die folgenden Themen:

- [Aktivieren von Active Directory-Gruppen in vRealize Automation für Projekte](#)
- [Entfernen von Benutzern in vRealize Automation](#)
- [Wie bearbeite ich Benutzerrollen in vRealize Automation?](#)
- [Vorgehensweise zum Bearbeiten der Rollenzuweisung für Gruppen in vRealize Automation](#)

Aktivieren von Active Directory-Gruppen in vRealize Automation für Projekte

Ist eine Gruppe auf der Seite „Gruppen hinzufügen“ nicht verfügbar, wenn Sie Benutzer zu Projekten hinzufügen, überprüfen Sie die Seite „Identitäts- und Zugriffsverwaltung“ und fügen Sie die Gruppe hinzu, sofern sie verfügbar ist. Wenn die Gruppe auf der Seite „Identitäts- und Zugriffsverwaltung“ in vRealize Automation nicht aufgeführt ist, wurde die Gruppe möglicherweise nicht in Ihrer Workspace One Access-Instanz synchronisiert. Sie können überprüfen, ob die Synchronisierung durchgeführt wurde, und dann mit diesem Verfahren die Gruppe wie hier dargestellt hinzufügen.

Um Mitglieder einer Active Directory-Gruppe zu einem Projekt hinzuzufügen, müssen Sie sicherstellen, dass die Gruppe mit Ihrer Workspace One Access-Instanz synchronisiert wurde und dass die Gruppe zur Organisation hinzugefügt wird.

Voraussetzungen

Wenn Sie versuchen, nicht synchronisierte Gruppen zu einem Projekt hinzuzufügen, sind sie nicht verfügbar. Sie müssen Ihre Active Directory-Gruppen mit Ihrer Lifecycle Manager-Instanz synchronisiert haben.

Verfahren

- 1 Melden Sie sich bei vRealize Automation als Benutzer aus derselben Active Directory-Domäne an, die Sie hinzufügen. Beispiel: @mycompany.com
- 2 Klicken Sie in Cloud Assembly rechts oben in der Navigationsleiste auf „Identitäts- und Zugriffsverwaltung“.
- 3 Klicken Sie auf **Unternehmensgruppen** und anschließend auf **Rollen zuweisen**.
- 4 Suchen Sie mithilfe der Suchfunktion die Gruppe, die Sie hinzufügen, und wählen Sie sie aus.
- 5 Weisen Sie eine Organisationsrolle zu.

Die Gruppe muss mindestens über die Organisationsmitglied-Rolle verfügen. Weitere Informationen finden Sie unter [Was sind die vRealize Automation Cloud Assembly-Benutzerrollen](#).

- 6 Klicken Sie auf **Dienstzugriff hinzufügen**, fügen Sie einen oder mehrere Dienste hinzu und wählen Sie für jeden eine Rolle aus.
- 7 Klicken Sie auf **Zuweisen**.

Ergebnisse

Sie können nun die Active Directory-Gruppe zu einem Projekt hinzufügen.

Entfernen von Benutzern in vRealize Automation

Sie können Benutzer nach Bedarf in vRealize Automation entfernen.

Alle Benutzer sind standardmäßig aufgeführt und Sie können keine Benutzer über die Seite „Identitäts- und Zugriffsverwaltung“ hinzufügen. Sie können Benutzer löschen.

Verfahren

- 1 Wählen Sie auf der Seite „Identitäts- und Zugriffsverwaltung“ die Registerkarte „Aktive Benutzer“ aus.
- 2 Suchen und wählen Sie die Benutzer aus, die Sie löschen möchten.
- 3 Klicken Sie auf **Benutzer entfernen**.

Ergebnisse

Die ausgewählten Benutzer werden entfernt.

Wie bearbeite ich Benutzerrollen in vRealize Automation?

Sie können Rollen bearbeiten, die in vRealize Automation importierten Workspace One Access-Benutzern zugewiesen wurden.

Voraussetzungen

Verfahren

- 1 Klicken Sie in Cloud Assembly rechts oben in der Navigationsleiste auf „Identitäts- und Zugriffsverwaltung“.
- 2 Wählen Sie den gewünschten Benutzer auf der Registerkarte „Aktive Benutzer“ aus und klicken Sie auf **Rollen bearbeiten**.
- 3 Sie können die Organisations- und Dienstrollen für den Benutzer bearbeiten.
 - Über die Auswahl im Dropdown-Menü neben der Überschrift „Organisationsrollen zuweisen“ können Sie die Beziehung des Benutzers zur Organisation ändern.
 - Klicken Sie auf „Dienstzugriff hinzufügen“, um neue Dienstrollen für den Benutzer hinzuzufügen.
 - Um Benutzerrollen zu entfernen, klicken Sie auf das X neben dem entsprechenden Dienst.
- 4 Klicken Sie auf **Speichern**.

Ergebnisse

Die Zuweisung der Benutzerrolle wird wie angegeben aktualisiert.

Vorgehensweise zum Bearbeiten der Rollenzuweisung für Gruppen in vRealize Automation

Sie können Rollenzuweisungen für Gruppen in vRealize Automation bearbeiten.

Voraussetzungen

Benutzer und Gruppen wurden aus einer gültigen vIDM-Instanz importiert, die Ihrer vRealize Automation-Bereitstellung zugeordnet ist.

Verfahren

- 1 Klicken Sie in Cloud Assembly rechts oben in der Navigationsleiste auf „Identitäts- und Zugriffsverwaltung“.
- 2 Wählen Sie die Registerkarte „Unternehmensgruppen“ aus.
- 3 Geben Sie den Namen der Gruppe, für die Sie die Rollenzuweisungen bearbeiten möchten, in das Suchfeld ein.
- 4 Bearbeiten Sie die Rollenzuweisungen für die ausgewählte Gruppe. Sie haben zwei Möglichkeiten:
 - Organisationsrollen zuweisen
 - Dienstrollen zuweisen
- 5 Klicken Sie auf **Zuweisen**.

Ergebnisse

Rollenzuweisungen werden wie angegeben aktualisiert.

Verwalten der vRealize Automation-Appliance

3

Als Systemadministrator müssen Sie möglicherweise verschiedene Aufgaben ausführen, um sicherzustellen, dass die installierte vRealize Automation-Anwendung ordnungsgemäß funktioniert.

Wenn Sie zum ersten Mal mit vRealize Automation arbeiten, sind diese Aufgaben nicht erforderlich. Kenntnisse bezüglich der Durchführung dieser Aufgaben sind nützlich, wenn Sie Probleme bei der Leistung oder dem Produktverhalten beheben müssen.

Dieses Kapitel enthält die folgenden Themen:

- [Starten und Stoppen von vRealize Automation](#)
- [Vorgehensweise zum Aktivieren der Uhrzeitsynchronisierung in vRealize Automation](#)
- [Vorgehensweise zum Deaktivieren der Uhrzeitsynchronisierung](#)
- [Vorgehensweise zum Zurücksetzen des Root-Kennworts für vRealize Automation](#)

Starten und Stoppen von vRealize Automation

Gehen Sie beim Starten oder Herunterfahren von vRealize Automation ordnungsgemäß vor.

vRealize Automation herunterfahren

Um die Datenintegrität zu erhalten, fahren Sie die vRealize Automation-Dienste herunter, bevor Sie die virtuellen Appliances ausschalten.

Hinweis Vermeiden Sie die Verwendung der `vracli reset vdm`-Befehle, falls dies überhaupt möglich ist. Dieser Befehl setzt die gesamte Konfiguration von Workspace ONE Access zurück und unterbricht die Zuordnung zwischen Benutzern und bereitgestellten Ressourcen.

- 1 Melden Sie sich bei der Konsole einer vRealize Automation-Appliance entweder per SSH oder per VMRC an.

- Um die vRealize Automation-Dienste auf allen Clusterknoten herunterzufahren, führen Sie die folgenden Befehle aus.

Hinweis Wenn Sie einen dieser Befehle zum Ausführen kopieren und er fehlschlägt, fügen Sie ihn zuerst in Notepad ein und kopieren Sie ihn dann erneut, bevor Sie ihn ausführen. Bei diesem Vorgang werden alle ausgeblendeten Zeichen und anderen Artefakte, die in der Dokumentationsquelle vorhanden sein könnten, ausgeblendet.

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

- Fahren Sie die vRealize Automation-Appliances herunter.

Ihre Bereitstellung von vRealize Automation wird jetzt heruntergefahren.

vRealize Automation starten

Nach einem ungeplanten Ausfall, einem kontrollierten Herunterfahren oder einem Wiederherstellungsvorgang müssen Sie die vRealize Automation-Komponenten in einer bestimmten Reihenfolge neu starten. vRLCM ist eine nicht kritische Komponente. Sie können sie also jederzeit starten. Komponenten von VMware Workspace ONE Access, vormals VMware Identity Management, müssen vor dem Starten von vRealize Automation gestartet werden.

Hinweis Überprüfen Sie, ob die entsprechenden Lastausgleichsdienste ausgeführt werden, bevor Sie die vRealize Automation-Komponenten starten.

- Schalten Sie alle vRealize Automation-Appliances ein und warten Sie, bis sie gestartet wurden.
- Melden Sie sich für jede Appliance mit SSH oder VMRC bei der Konsole an und führen Sie den folgenden Befehl aus, um die Dienste auf allen Knoten wiederherzustellen.

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

- Stellen Sie mit folgendem Befehl sicher, dass alle Dienste in Betrieb sind.

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

Hinweis Sie sollten drei Instanzen jedes Dienstes im Status „Wird ausgeführt“ oder „Abgeschlossen“ sehen.

Wenn alle Dienste als „Wird ausgeführt“ oder „Abgeschlossen“ aufgelistet sind, ist vRealize Automation betriebsbereit.

vRealize Automation neu starten

Sie können alle vRealize Automation-Dienste zentral von jeder der Appliances in Ihrem Cluster neu starten. Folgen Sie den vorausgehenden Anweisungen, um vRealize Automation herunterzufahren, und starten Sie dann vRealize Automation anhand der Anweisungen. Bevor Sie vRealize Automation neu starten, stellen Sie sicher, dass alle anwendbaren Lastausgleichsdienste und VMware Workspace ONE Access-Komponenten ausgeführt werden.

Wenn alle Dienste als „Wird ausgeführt“ oder „Abgeschlossen“ aufgelistet sind, ist vRealize Automation betriebsbereit.

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob alle Dienste ausgeführt werden:

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

Vorgehensweise zum Aktivieren der Uhrzeitsynchronisierung in vRealize Automation

Sie können die Uhrzeitsynchronisierung in Ihrer vRealize Automation-Bereitstellung mithilfe der Befehlszeile der vRealize Automation-Appliance aktivieren.

Sie können die Uhrzeitsynchronisierung für Ihre eigenständige oder geclusterte vRealize Automation-Bereitstellung mithilfe des NTP-Netzwerkprotokolls (Network Time Protocol) konfigurieren. vRealize Automation unterstützt zwei sich gegenseitig ausschließende NTP-Konfigurationen:

NTP-Konfiguration	Beschreibung
ESXi	<p>Sie können diese Konfiguration verwenden, wenn der ESXi-Server, auf dem die vRealize Automation-Appliance gehostet wird, mit einem NFS-Server synchronisiert ist. Wenn Sie eine geclusterte Bereitstellung verwenden, müssen alle ESXi-Hosts mit einem NFS-Server synchronisiert werden.</p> <p>Hinweis Es kann zu einem Uhrenfehler kommen, wenn die vRealize Automation-Bereitstellung auf einen ESXi-Host migriert wird, der nicht mit einem NTP-Server synchronisiert ist.</p> <p>Weitere Informationen zum Konfigurieren von NTP für ESXi finden Sie im KB-Artikel 57147 Konfigurieren von NTP (Network Time Protocol) auf einem ESXi-Host mithilfe des vSphere Web Client.</p>
systemd	<p>Diese Konfiguration verwendet den systemd-timesyncd-Daemon, um die Uhren in Ihrer vRealize Automation-Bereitstellung zu synchronisieren.</p> <p>Hinweis Der systemd-timesyncd-Daemon ist standardmäßig aktiviert, aber ohne NFS-Server konfiguriert. Wenn die vRealize Automation-Appliance eine dynamische IP-Konfiguration verwendet, kann die Appliance alle vom DHCP-Protokoll empfangenen NTP-Server verwenden.</p>

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als **root** an.

2 Aktivieren Sie NTP mit ESXi.

- a Führen Sie den Befehl `vracli ntp esxi --enable` aus.
- b Führen Sie den Befehl `vracli ntp apply` aus.

Die ESXi-NTP-Konfiguration wird auf die vRealize Automation-Bereitstellung angewendet.

3 Aktivieren Sie NTP mit systemd.

- a Führen Sie den Befehl `vracli ntp systemd --set FQDN_or_IP_of_systemd_server` aus.

Hinweis Sie können mehrere NTP-Server vom Typ `systemd` hinzufügen, indem Sie deren Netzwerkadressen durch ein Komma trennen.

- b Führen Sie den Befehl `vracli ntp apply` aus.

Die `systemd`-NTP-Konfiguration wird auf die vRealize Automation-Bereitstellung angewendet.

4 (Optional) Führen Sie den Befehl `vracli ntp status` aus, um den Status der NTP-Konfiguration zu bestätigen.

Die NTP-Konfiguration kann fehlschlagen, wenn zwischen dem NTP-Server und der vRealize Automation-Bereitstellung eine Zeitdifferenz von mehr als 10 Minuten besteht. Zur Behebung dieses Problems starten Sie die vRealize Automation-Appliance neu, die mit dem NTP-Server synchronisiert ist.

Vorgehensweise zum Deaktivieren der Uhrzeitsynchronisierung

Sie können die NTP-Uhrzeitsynchronisierung (Network Time Protocol) in Ihrer vRealize Automation-Bereitstellung mithilfe der Befehlszeile der vRealize Automation-Appliance deaktivieren.

Voraussetzungen

Stellen Sie sicher, dass die Uhrzeitsynchronisierung mit ESXi oder `systemd` konfiguriert ist. Weitere Informationen hierzu finden Sie unter [Vorgehensweise zum Aktivieren der Uhrzeitsynchronisierung in vRealize Automation](#).

Verfahren

- 1** Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als **root** an.
- 2** Deaktivieren Sie eine ESXi-NTP-Konfiguration.
 - a Führen Sie den Befehl `vracli ntp esxi --disable` aus.
 - b Führen Sie den Befehl `vracli ntp apply` aus.

Die ESXi-NTP-Konfiguration ist deaktiviert.

3 Deaktivieren Sie eine systemd-NTP-Konfiguration.

a Führen Sie den Befehl `vracli ntp systemd --disable FQDN_or_IP_of_systemd_server` aus.

b Führen Sie den Befehl `vracli ntp apply` aus.

Die systemd-NTP-Konfiguration ist deaktiviert.

4 (Optional) Führen Sie den Befehl `vracli ntp status` aus, um den Status der NTP-Konfiguration zu bestätigen.

Vorgehensweise zum Zurücksetzen des Root-Kennworts für vRealize Automation

Sie können ein verloren gegangenes oder vergessenes vRealize Automation-Root-Kennwort zurücksetzen.

In diesem Verfahren verwenden Sie ein Befehlszeilenfenster auf der vCenter-Host-Appliance, um das vRealize Automation-Root-Kennwort Ihrer Organisation zurückzusetzen.

Voraussetzungen

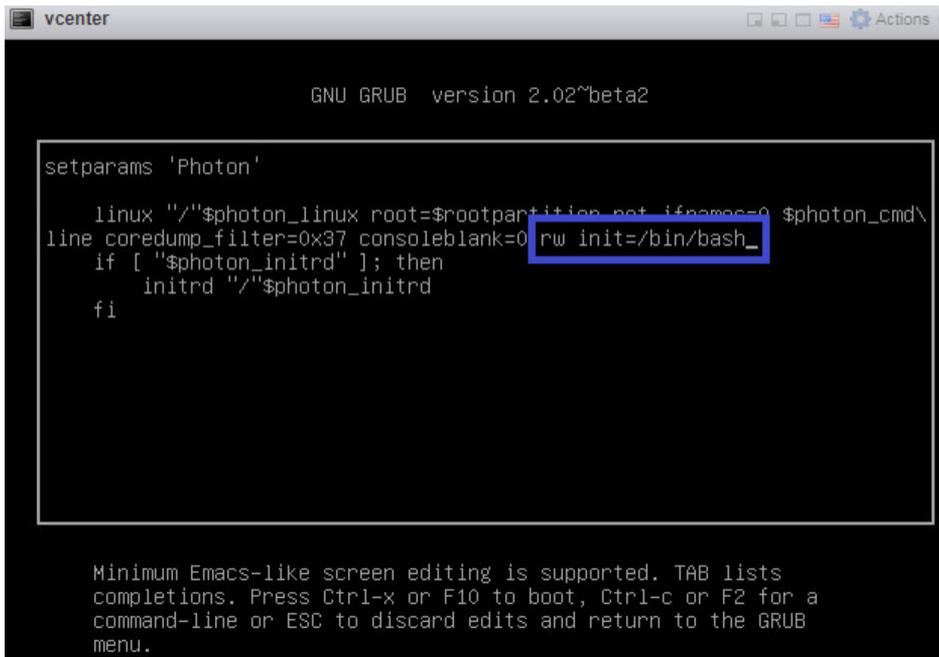
Dieser Vorgang kann von vRealize Automation-Administratoren durchgeführt werden und erfordert die Anmeldedaten, die für den Zugriff auf die vCenter-Host-Appliance benötigt werden.

Verfahren

1 Fahren Sie vRealize Automation herunter und starten Sie das Programm mithilfe des in [Starten und Stoppen von vRealize Automation](#) beschriebenen Verfahrens.

2 Wenn das Befehlszeilenfenster des Photon-Betriebssystems angezeigt wird, geben Sie `e` ein und drücken die **Eingabetaste**, um den Editor des GNU GRUB-Startmenüs zu öffnen.

- 3 Geben Sie wie unten angezeigt im GNU GRUB-Editor den Wert `rw init=/bin/bash` am Ende der Zeile ein, die mit `linux "/" $photon_linux root=rootpartition` beginnt:



```

vcenter
GNU GRUB version 2.02~beta2

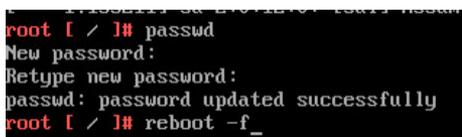
setparams 'Photon'

linux "/"$photon_linux root=$rootpartition rw init=/bin/bash $photon_cmd\
line coredump_filter=0x37 consoleblank=0
if [ "$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 Drücken Sie **F10**, um die Änderung weiterzugeben und vRealize Automation neu zu starten.
- 5 Warten Sie, bis vRealize Automation neu gestartet wurde.
- 6 Geben Sie an der `root [/]#`-Eingabeaufforderung den Wert `passwd` ein und drücken Sie die **Eingabetaste**.
- 7 Geben Sie an der `New password:-`Eingabeaufforderung Ihr neues Kennwort ein und drücken Sie die **Eingabetaste**.
- 8 Geben Sie an der `Retype new password:-`Eingabeaufforderung erneut Ihr neues Kennwort ein und drücken Sie die **Eingabetaste**.
- 9 Geben Sie an der `root [/]#`-Eingabeaufforderung den Wert `reboot -f` ein und drücken Sie die **Eingabetaste**, um den Vorgang zum Zurücksetzen des Root-Kennworts abzuschließen.



```

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

```

Nächste Schritte

Als vRealize Automation-Administrator können Sie sich jetzt mit dem neuen Root-Kennwort bei vRealize Automation anmelden.

Arbeiten mit Protokollen in vRealize Automation

4

Mit den bereitgestellten Befehlszeilendienstprogramm `vracli` können Sie Protokolle in vRealize Automation erstellen und verwenden.

Sie können die Protokolle direkt in vRealize Automation verwenden oder stattdessen alle Protokolle an vRealize Log Insight weiterleiten.

Dieses Kapitel enthält die folgenden Themen:

- [Wie arbeite ich mit Protokollen und Protokollpaketen in vRealize Automation?](#)
- [Wie konfiguriere ich die Protokollweiterleitung zu vRealize Log Insight?](#)

Wie arbeite ich mit Protokollen und Protokollpaketen in vRealize Automation?

Sie können vRealize Automation-Protokolle und -Protokollpakete in vRealize Automation erstellen und verwenden.

Alternativ können Sie Protokolle automatisch an vRealize Log Insight weiterleiten. Weitere Informationen zum Weiterleiten von Protokollen an vRealize Log Insight finden Sie unter [Wie konfiguriere ich die Protokollweiterleitung zu vRealize Log Insight?](#).

Sie erhalten Informationen zur Nutzung des Befehlszeilendienstprogramms `vracli`, wenn Sie das Argument `--help` in der Befehlszeile von `vracli` verwenden. Beispiel: `vracli log-bundle --help`.

Protokollpaketbefehle

Sie können ein einfaches Protokollpaket oder ein aggregiertes (Cold-Storage-)Protokoll aller Dienste erstellen. Während beide Protokollpakete alle Protokolle für Ihre Dienste enthalten, enthält das Cold-Storage-Paket eine Kopie eines aggregierten Streams von zurückliegenden Versionen der Dienstprotokolle, die bei der Fehlersuche zusätzliche Informationen liefern können. Der Cold-Storage-Agent aggregiert ständig Protokolle der Dienste und speichert sie auf dem lokalen Dateisystem. Ein einfaches Protokollpaket ist in der Regel alles, was zur Fehlerbehebung benötigt wird.

Außerdem können Sie den standardmäßigen Zeitüberschreitungswert zum Erfassen von Protokollen von jedem Knoten ändern.

In einer geclusterten Umgebung müssen Sie lediglich den Befehl `vracli log-bundle` auf einem Knoten ausführen.

- Zeigen Sie die Hilfe zum Protokollpaket-Befehl an:

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

- Erstellen Sie ein einfaches Protokollpaket.

```
vracli log-bundle
```

- Erstellen Sie ein Cold-Storage-Protokollpaket:

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

- Ändern Sie den Zeitüberschreitungswert zum Erfassen von Protokollen von jedem Knoten. Wenn Ihre Umgebung beispielsweise große Protokolldateien enthält, das Netzwerk langsam, die CPU-Auslastung hoch ist usw., müssen Sie den Zeitüberschreitungswert möglicherweise auf einen höheren Wert als den Standardwert von 1000 Sekunden festlegen.

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

Protokollpaketstrukturen

vRealize Automation-Dienste sind in Containern in Kubernetes-Pods verpackt. Das generierte Protokollpaket ist ein `tar.xz`-Archiv, das ein `log-bundle-{{TIMESTAMP}}.tar.xz`-Namensformat verwendet, wobei `TIMESTAMP` ein Epoch-Zeitstempel in Sekunden ist. Ein normales Protokollpaket enthält Protokolle aller Knoten in der Umgebung. Wenn das Protokollpaket aus irgendeinem Grund nicht generiert werden kann, wird stattdessen ein Fallback-Paket erstellt. Das Fallback-Paket enthält Protokolle nur für den aktuellen Knoten. Es gibt leichte Unterschiede in der Struktur der beiden Protokollpakettypen.

- Normale Protokollpakete

Normale Protokollpakete sind in folgende Kategorien unterteilt:

- Hostprotokolle und -konfiguration

Die Konfiguration für jeden Host und seine hostspezifischen Protokolle werden in einem Verzeichnis pro Clusterknoten (Host) erfasst. Der Verzeichnisname entspricht dem Hostnamen des Knotens. Der Inhalt des Verzeichnisses entspricht dem Dateisystem des Hosts. Die Anzahl der Verzeichnisse entspricht der Anzahl der Clusterknoten.

Cold-Storage-Protokolle befinden sich in einem strukturierten JSON-Protokoll als `/Hostname/services-logs/all/aggregated.log`.

- Pod-Protokolle

Dienste sind in Containern in Kubernetes-Pods verpackt. Dienstprotokolle befinden sich im `Pods`-Verzeichnis, das ein einzelnes Verzeichnis pro Namespace mit einem Dateinamen enthält, der dem Namespace-Namen entspricht. In der Regel gibt es pro Clusterknoten eine Instanz jedes Pods. Das Pod-Verzeichnis enthält für jede seiner Container-Anwendungen eine Protokolldatei.

Zum Beispiel befinden sich Protokolle von vRealize Orchestrator Control Center in einer `vco-controlcenter-app.log`-Datei in jedem der `/pods/prelude/vco-app-hash/-`Verzeichnisse.

- Umgebungsdatei

Die Umgebungsdatei enthält Informationen über die aktuelle Ressourcennutzung pro Knoten und pro Pods. Sie enthält außerdem Clusterinformationen und Beschreibungen für alle verfügbaren Kubernetes-Elemente.

- Fallback-Protokollpakete

Wenn Sie beim Warten auf die Beendigung des `vraccli`-Befehls eine Fehlermeldung erhalten, wird ein Fallback-Paket generiert. Wenn Sie diesen Fehler erhalten, sollten Sie den Befehl `vraccli log-bundle` auf jedem Host oder Knoten im Cluster ausführen, um so viele Informationen wie möglich zu erfassen.

- Fallback-Containerprotokolle

Fallback-Protokolle befinden sich im Verzeichnis `/fallback-containers`. Anhand des Namens der Protokolldatei können Sie erkennen, welcher Container in welchem Pod die Protokolle erzeugt hat:

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

- Fallback bei Cold-Storage

Wenn Sie mit dem Paket Cold-Storage-Protokolle erfassen, befinden sich die Fallback-Protokolle des aktuellen Hosts im Verzeichnis `/fallback-cold-storage`.

Wie konfiguriere ich die Protokollweiterleitung zu vRealize Log Insight?

Sie können Protokolle von vRealize Automation an vRealize Log Insight weiterleiten, um die Vorteile einer robusteren Protokollanalyse und Berichtsgenerierung zu nutzen.

vRealize Automation ist mit einem [fluentd-basierten](#) Protokollierungsagenten gebündelt. Der Agent sammelt und speichert Protokolle, damit sie in ein Protokollpaket aufgenommen und später untersucht werden können. Sie können den Agenten so konfigurieren, dass er eine Kopie der Protokolle an einen vRealize Log Insight-Server weiterleitet. Verwenden Sie dazu die vRealize Log Insight-API. Die bereitgestellte API ermöglicht anderen Programmen die Kommunikation mit vRealize Log Insight.

Weitere Informationen zu vRealize Log Insight, einschließlich der Dokumentation für die vRealize Log Insight-API, finden Sie in der [Dokumentation zu vRealize Log Insight](#) und auf der Seite `/api/v1/events/ingest/{agentId}`.

Konfigurieren Sie den Protokollierungsagenten so, dass er vRealize Automation-Protokolle automatisch und kontinuierlich an vRealize Log Insight weiterleitet. Verwenden Sie dazu das bereitgestellte Befehlszeilendienstprogramm `vraccli`.

Sie erhalten Informationen zur Nutzung des Befehlszeilendienstprogramms `vracli`, wenn Sie das Argument `--help` in der Befehlszeile von `vracli` verwenden. Beispiel: `vracli vrli --help`.

Überprüfen der vorhandenen Konfiguration von vRealize Log Insight

Command

```
vracli vrli
```

Arguments

Es gibt keine Befehlszeilenargumente.

Output

Die aktuelle Konfiguration für die vRealize Log Insight-Integration wird im JSON-Format ausgegeben.

Exit codes

Folgende Exit-Codes sind möglich:

- 0 – Integration mit vRealize Log Insight ist konfiguriert.
- 1 – Im Rahmen der Befehlsausführung ist eine Ausnahme aufgetreten. Sehen Sie sich die Details der Fehlermeldung an.
- 61 (ENODATA) – Integration mit vRealize Log Insight ist nicht konfiguriert. Sehen Sie sich die Details der Fehlermeldung an.

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
}
```

Hinweis Sie können ein anderes Hostschema (Standardwert ist HTTPS) und einen anderen Port (Standardwert ist 443) zum Senden der Protokolle verwenden. Siehe hierzu folgende Beispiele:

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

Port 9543 wird von der vRealize Log Insight-Aufnahme-API verwendet, die im Thema *Verwalten von vRealize Log Insight* unter *Ports und externe Schnittstellen* in der [Dokumentation zu vRealize Log Insight](#) beschrieben wird.

Konfigurieren oder Aktualisieren der Integration von vRealize Log Insight

Command

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

Arguments

Die folgenden Befehlszeilenargumente sind verfügbar:

- FQDN_OR_URL – der FQDN oder die IP-Adresse des vRealize Log Insight-Servers, der bzw. die zum Senden von Protokollen unter Verwendung der vRealize Log Insight-API-Konfiguration verwendet wird. Standardmäßig werden Port 443 und ein HTTPS-Schema verwendet. Wenn eine dieser Einstellungen geändert werden muss, können Sie stattdessen eine URL verwenden.
- Optionen
 - `--agent-id SOME_ID` – Festlegen der ID des Protokollierungsagenten für diese Appliance. Der Standardwert lautet 0. Wird verwendet, um den Protokollierungsagenten für Protokolle zu identifizieren, die an vRealize Log Insight gesendet werden. Verwenden Sie dazu die vRealize Log Insight-API-Konfiguration.
 - `--environment ENV` – Festlegen eines Bezeichners für die aktuelle Umgebung. Steht in den vRealize Log Insight-Protokollen als Tag für jedes Protokollzeilenereignis zur Verfügung. Der Standardwert lautet prod.
 - `--ca-file /path/to/server-ca.crt` – Geben Sie eine Datei an, die das Zertifizierungsstellenzertifikat enthält, das zum Signieren des vRealize Log Insight-Serverzertifikats verwendet wurde. Zwingt den Protokollierungsagenten, der angegebenen Zertifizierungsstelle zu vertrauen, und ermöglicht ihr, das Zertifikat des vRealize Log Insight-Servers zu verifizieren. Die Datei kann eine ganze Zertifikatskette enthalten, wenn dies zur Verifizierung des Zertifikats erforderlich ist. Übergeben Sie im Falle eines selbstsignierten Zertifikats das Zertifikat selbst.

- `--ca-cert CA_CERT` – Geben Sie eine Datei auf die gleiche Weise wie `--ca-file` an, aber übergeben Sie das Zertifikat (Kette) inline als Zeichenfolge.
- `--insecure` – Deaktiviert die SSL-Verifizierung des Serverzertifikats. Zwingt den Protokollierungsagenten, beim Senden von Protokollen ein beliebiges SSL-Zertifikat zu akzeptieren.

Output

Es wird keine Ausgabe erwartet.

Exit codes

Folgende Exit-Codes sind möglich:

- 0 – Die Konfiguration wurde aktualisiert.
- 1 – Im Rahmen der Ausführung ist eine Ausnahme aufgetreten. Sehen Sie sich die Details der Fehlermeldung an.

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
```

Löschen der Integration von vRealize Log Insight

Command

```
vracli vrli unset
```

Arguments

Es gibt keine Befehlszeilenargumente.

Output

Die Bestätigung wird im reinen Textformat ausgegeben.

Exit codes

Folgende Exit-Codes sind möglich:

- 0 – Die Konfiguration wurde gelöscht oder es war keine Konfiguration vorhanden.
- 1 – Im Rahmen der Ausführung ist eine Ausnahme aufgetreten. Sehen Sie sich die Details der Fehlermeldung an.

Examples – Clear integration

```
$ vracli vrli unset  
Clearing vRLI integration configuration
```

```
$ vracli vrli unset  
No vRLI integration configured
```

Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) für vRealize Automation

Dieses Produkt nimmt am Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) von VMware teil. Mit dem CEIP werden Informationen für VMware bereitgestellt, mit denen es VMware ermöglicht wird seine Produkte und Dienste zu verbessern, Probleme zu beheben und Benutzern Hinweise zur optimalen Bereitstellung und Verwendung unserer Produkte zu geben.

Einzelheiten zu den im Rahmen des CEIP erfassten Daten sowie zum Zweck der Verwendung durch VMware können im Trust & Assurance Center unter <http://www.vmware.com/trustvmware/ceip.html> eingesehen werden.

Dieses Kapitel enthält die folgenden Themen:

- [Wie nehme ich am Programm zur Verbesserung der Kundenzufriedenheit \(Customer Experience Improvement Program\) für vRealize Automation teil bzw. wie beende ich die Teilnahme?](#)
- [Wie konfiguriere ich die Datenerfassungszeit für das Programm zur Verbesserung der Benutzerfreundlichkeit für vRealize Automation?](#)

Wie nehme ich am Programm zur Verbesserung der Kundenzufriedenheit (Customer Experience Improvement Program) für vRealize Automation teil bzw. wie beende ich die Teilnahme?

Über die Befehlszeile der vRealize Automation-Appliance können Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) beitreten oder es verlassen.

Sie können dem CEIP-Programm bei der Installation von vRealize Automation und mit dem vRealize Lifecycle Manager (LCM) beitreten. Sie können dem Programm auch nach der Installation mithilfe von Befehlszeilenoptionen beitreten oder es verlassen.

So treten Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit mithilfe von Befehlszeilenoptionen bei:

- 1 Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als **Root**-Benutzer an.

- 2 Führen Sie den Befehl `vracli ceip on` aus.
- 3 Überprüfen Sie die Informationen des Programms zur Verbesserung der Benutzerfreundlichkeit und führen Sie den Befehl `vracli ceip on --acknowledge-ceip` aus.
- 4 Um die vRealize Automation-Dienste neu zu starten, führen Sie den Befehl `/opt/scripts/deploy.sh` aus.

So verlassen Sie das Programm zur Verbesserung der Benutzerfreundlichkeit mithilfe von Befehlszeilenoptionen:

- 1 Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als **Root**-Benutzer an.
- 2 Führen Sie den Befehl `vracli ceip off` aus.
- 3 Um die vRealize Automation-Dienste neu zu starten, führen Sie den Befehl `/opt/scripts/deploy.sh` aus.

Wie konfiguriere ich die Datenerfassungszeit für das Programm zur Verbesserung der Benutzerfreundlichkeit für vRealize Automation?

Sie können den Tag und die Uhrzeit festlegen, an dem bzw. zu der das Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) Daten an VMware sendet.

Verfahren

- 1 Melden Sie sich bei der Befehlszeile der vRealize Automation-Appliance als **Root**-Benutzer an.
- 2 Öffnen Sie die folgende Datei in einem Texteditor.
`/etc/telemetry/telemetry-collector-vami.properties`
- 3 Bearbeiten Sie die Eigenschaften für den Wochentag (`dow`, `day-of-week`) und die Wochenstunde (`hod`, `hour-of-day`).

Eigenschaft	Beschreibung
<code>frequency.dow=<day-of-week></code>	Tag, an dem die Datenerfassung stattfindet.
<code>frequency.hod=<hour-of-day></code>	Lokale Uhrzeit des Tages, an dem die Datenerfassung stattfindet. Mögliche Werte sind 0 bis 23.

- 4 Speichern und schließen Sie `telemetry-collector-vami.properties`.
- 5 Wenden Sie die Einstellung an, indem Sie den folgenden Befehl eingeben.
`vcac-config telemetry-config-update --update-info`
Die Änderungen werden auf alle Knoten in Ihrer Bereitstellung angewendet.