

Verwalten von vRealize Automation

21. Juli 2021

vRealize Automation 7.6

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 © 2015-2021 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

1	Verwalten und Anpassen von vRealize Automation-Komponenten und -Optionen	5
	Senden einer Meldung an alle Benutzer	5
	Erstellen einer Liste zulässiger URLs für das Meldungs-Board	8
	Starten und Herunterfahren von vRealize Automation	9
	Starten von vRealize Automation	9
	Neustarten von vRealize Automation	10
	Herunterfahren von vRealize Automation	12
	Aktualisieren von vRealize Automation-Zertifikaten	13
	Extrahieren von Zertifikaten und privaten Schlüsseln	15
	Ersetzen von Zertifikaten in der vRealize Automation-Appliance	15
	Ersetzen des Infrastructure as a Service-Zertifikats	19
	Ersetzen des IaaS Manager Service-Zertifikats	21
	Aktualisieren von eingebettetem vRealize Orchestrator, sodass vRealize Automation-Zertifikate als vertrauenswürdig eingestuft werden	23
	Aktualisieren von externem vRealize Orchestrator, sodass vRealize Automation-Zertifikate als vertrauenswürdig eingestuft werden	26
	Aktualisieren des Management-Site-Zertifikats der vRealize Automation-Appliance	27
	Ersetzen eines Management-Agent-Zertifikats	32
	Ändern der Abrufmethode für Zertifikate	35
	Verwalten der vRealize Automation Postgres-Appliance-Datenbank	36
	Konfigurieren der Appliance-Datenbank	37
	Szenarien für das automatische Failover für die aus drei Knoten bestehende Appliance-Datenbank	39
	Szenario: Durchführen eines manuellen Failovers der Appliance-Datenbank	42
	Szenario: Durchführen eines Wartungsdatenbank-Failover	44
	Manuelle Wiederherstellung der Appliance-Datenbank nach einem schwerwiegenden Fehler	45
	Backup und Wiederherstellung für vRealize Automation-Installationen	47
	Programm zur Verbesserung der Kundenzufriedenheit	48
	Beitreten bzw. Verlassen des Programm zur Verbesserung der Kundenzufriedenheit für vRealize Automation	48
	Konfigurieren der Datenerfassungszeit	48
	Anpassen von Systemeinstellungen	49
	Ändern des Symbols „Alle Services“ im Servicekatalog	49
	Anpassen von Daten-Rollover-Einstellungen	51
	Anpassen der Einstellungen in der Manager Service-Konfigurationsdatei	53
	Überwachen von vRealize Automation	59
	Überwachen von Workflows und Anzeigen von Protokollen	59
	Überwachen von Ereignisprotokollen und Diensten	60

Verwenden der vRealize Automation-Überwachungsprotokollierung	62
Anzeigen von Hostinformationen für Cluster in verteilten Bereitstellungen	64
Überwachen der Integrität von vRealize Automation	66
Konfigurieren von Systemtests für vRealize Automation	67
Konfigurieren von Mandantentests für vRealize Automation	69
Konfigurieren von Tests für vRealize Orchestrator	71
Benutzerdefinierte Testsuite	73
Anzeigen der Ergebnisse des vRealize Automation-Integritätsprüfungstests	75
Fehlerbehebung des Integritätsdienstes	76
Überwachung von vRealize Automation-Umgebungsressourcen mithilfe von SNMP	77
Überwachen und Verwalten von Ressourcen	77
Auswählen eines Ressourcenüberwachungsszenarios	77
Terminologie der Ressourcenverwendung	78
Herstellen einer Verbindung zu einer Cloud-Maschine	79
Reduzieren der Reservierungsauslastung durch Abgang	82
Außerbetriebnahme eines Speicherpfads	83
Datenerfassung	84
Grundlegende Informationen zur vSwap-Zuteilungsprüfung für vCenter Server-Endpoints	87
Entfernen der Datacenter-Standorte	88
Überwachen von Containern	89
Massenimport, -update oder -migration von virtuellen Maschinen	89
Importieren einer virtuellen Maschine in eine vRealize Automation-Umgebung	90
Aktualisieren einer virtuellen Maschine in einer vRealize Automation-Umgebung	96
Migrieren einer virtuellen Maschine zu einer anderen vRealize Automation-Umgebung	98

Verwalten und Anpassen von vRealize Automation-Komponenten und -Optionen

Sie können bereitgestellte Maschinen und andere Aspekte Ihrer vRealize Automation-Bereitstellung verwalten.

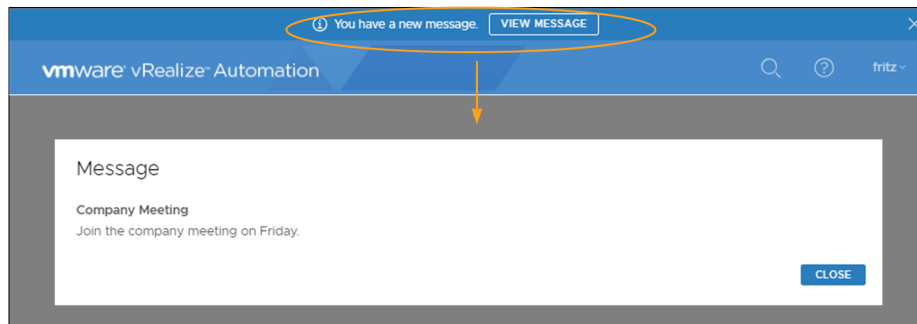
Dieses Kapitel enthält die folgenden Themen:

- [Senden einer Meldung an alle Benutzer](#)
- [Starten und Herunterfahren von vRealize Automation](#)
- [Aktualisieren von vRealize Automation-Zertifikaten](#)
- [Verwalten der vRealize Automation Postgres-Appliance-Datenbank](#)
- [Backup und Wiederherstellung für vRealize Automation-Installationen](#)
- [Programm zur Verbesserung der Kundenzufriedenheit](#)
- [Anpassen von Systemeinstellungen](#)
- [Überwachen von vRealize Automation](#)
- [Überwachen der Integrität von vRealize Automation](#)
- [Überwachung von vRealize Automation-Umgebungsressourcen mithilfe von SNMP](#)
- [Überwachen und Verwalten von Ressourcen](#)
- [Überwachen von Containern](#)
- [Massenimport, -update oder -migration von virtuellen Maschinen](#)

Senden einer Meldung an alle Benutzer

Als Mandantenadministrator können Sie eine Meldung an alle Benutzer senden. Die Benachrichtigung über die Meldung wird oben auf der Browserseite angezeigt. Die Benutzer können die Meldung dann mit einem Klick auf die Benachrichtigung öffnen.

Als Benutzer können Sie vom Banner oder von Ihrem persönlichen Dropdown-Menü in der Kopfzeile aus auf die Meldung zugreifen.



Über das Meldungs-Board können Sie eine Textnachricht oder eine Webseite per Broadcast übermitteln. Je nach Webseite können die Benutzer im Meldungs-Board durch die Website navigieren.

Für das Meldungs-Board gelten folgende Einschränkungen.

Tabelle 1-1. Meldungs-Board – Einschränkungen

Option	Einschränkungen
Einschränkungen im Zusammenhang mit URL-Nachrichten	<ul style="list-style-type: none"> ■ Die Ziel-URL muss in der Zulassungsliste des Meldungs-Boards enthalten sein. Siehe Erstellen einer Liste zulässiger URLs für das Meldungs-Board. ■ Sie können nur auf einer HTTPS-Site gehostete Inhalte veröffentlichen. ■ Selbstsignierte Zertifikate können nicht verwendet werden. Die Option zum Akzeptieren des Zertifikats wird im Meldungs-Board nicht angezeigt. ■ Die Meldungs-Board-URL ist in einem iframe eingebettet. Einige Websites funktionieren nicht in iframes, und es wird ein Fehler angezeigt. Der Fehler tritt auf, wenn X-Frame-Options in der Kopfzeile der Zielwebsite auf DENY oder SAMEORIGIN festgelegt ist. Falls die Zielwebsite von Ihnen gesteuert wird, können Sie die X-Frame-Options-Kopfzeile auf x-Frame-Options: ALLOW-FROM https://<vRealizeAutomationApplianceURL> festlegen. ■ Einige Websites verfügen über eine Weiterleitung zu einer Top-Level-Seite, durch die möglicherweise die gesamte vRealize Automation-Seite aktualisiert wird. Diese Art von Websites kann im Meldungs-Board nicht verwendet werden. Die Aktualisierung wird unterdrückt und die Meldung „Wird geladen...“ wird im Meldungs-Board angezeigt. ■ Wenn Sie eine interne HTML-Seite anzeigen, kann für die Seite nicht der vRealize Automation-Host als URL angegeben sein.
Einschränkungen im Zusammenhang mit benutzerdefinierten Nachrichten	<ul style="list-style-type: none"> ■ Zur Gewährleistung der Sicherheit lässt „Benutzerdefinierte Nachricht“ immer einfaches Markup zu, unterstützt aber keinen HTML-Code. Beispielsweise können Sie einen Link zu einer Website nicht mithilfe von <href> bereitstellen. Sie müssen die URL-Nachrichtenoption verwenden.

Voraussetzungen

Melden Sie sich bei vRealize Automation als **Mandantenadministrator** an.

Verfahren

- 1 Klicken Sie auf die Registerkarte **Administration**.
- 2 Wählen Sie **Benachrichtigungen > Meldungs-Board**.

- 3 Wählen Sie im Dropdown-Menü **Typ** den Nachrichtentyp aus.

Option	Beschreibung
Keine	Entfernt die Benachrichtigung über die Meldung.
Benutzerdefinierte Nachricht	Geben Sie die Nachricht als einfachen Text ein.
URL	<p>Geben Sie die URL der Seite ein.</p> <p>Die URL muss in der Zulassungsliste des Meldungs-Boards enthalten sein. Siehe Erstellen einer Liste zulässiger URLs für das Meldungs-Board.</p> <p>Wählen Sie Benutzer-ID einschließen, damit sich der Benutzer mithilfe seiner Benutzer-ID für vRealize Automation bei einer Website anmelden kann (in der Regel handelt es sich um Ihre interne Website). Die URL, die an die Website übergeben wird, ähnlich wie <code>http://company.com/internal/message?userID=richard_dawson@company.com</code>. Mit dieser Methode kann Ihre Website die <code>window.location.search</code> JavaScript-Eigenschaft verwenden, um die ID des aktuellen Benutzers für Ihre Website zur Verfügung zu stellen.</p>

- 4 Klicken Sie auf **OK**.

Ergebnisse

Die Meldung wird per Broadcast als Banner an alle Ihre Mandantenbenutzer verbreitet.

Zum Ändern oder Entfernen der Nachricht müssen Sie als Mandantenadministrator angemeldet sein. Zum Ändern der Nachricht wiederholen Sie die gleichen Schritte. Wenn Sie die Meldung entfernen möchten, wählen Sie als Typ „Keine“ und klicken Sie auf **OK**.

Erstellen einer Liste zulässiger URLs für das Meldungs-Board

Als Sicherheitsadministrator konfigurieren Sie eine Liste zulässiger URLs, die im Meldungs-Board verwendet werden können. Diese Zulassungsliste erhöht die Sicherheit.

Voraussetzungen

Melden Sie sich bei vRealize Automation als **Sicherheitsadministrator** an.

Verfahren

- 1 Wählen Sie **Administration > Meldungs-Board-Whitelist** aus.
- 2 Klicken Sie auf **Neu**.
- 3 Fügen Sie eine URL hinzu und klicken Sie auf **OK**.

Die URL-Einträge können Folgendes enthalten:

- IP-Adresse oder FQDN einer Site. Zum Beispiel `https://docs.vmware.com`.
- Enthält HTTPS.
- Kann zulässige Ports enthalten. Wenn kein Port angegeben ist, sind die Ports 80 und 443 zulässig.

- 4 Wiederholen Sie den Vorgang für jeden weiteren Eintrag.

Ergebnisse

Ein Mandantenadministrator kann keine URL zum Meldungs-Board hinzufügen, es sei denn, sie ist in dieser Liste enthalten.

Nächste Schritte

Stellen Sie sicher, dass Sie eine in der Zulassungsliste enthaltene URL zum Meldungs-Board hinzufügen und per Broadcast verbreiten können. Siehe [Senden einer Meldung an alle Benutzer](#).

Starten und Herunterfahren von vRealize Automation

Ein Systemadministrator führt ein kontrolliertes Herunterfahren oder Starten von vRealize Automation durch, um die System- und Datenintegrität zu bewahren.

Sie können kontrollierte Herunterfahren- und Startvorgänge auch nutzen, um Probleme mit der Leistung oder dem Produktverhalten zu beheben, die von einem nicht korrekten ersten Startvorgang herrühren. Verwenden Sie das Neustartverfahren, wenn nur einige Komponenten der Bereitstellung fehlschlagen.

Starten von vRealize Automation

Wenn Sie vRealize Automation starten, nachdem das Programm aus einem erwarteten oder unerwarteten Grund ausgeschaltet wurde, müssen Sie die Komponenten in einer bestimmten Reihenfolge starten.

Wenn Sie Bereitstellungskomponenten in vCenter Server verwalten, können Sie deren Gastbetriebssysteme von dort aus starten.

Voraussetzungen

Vergewissern Sie sich, dass die in Ihrer Bereitstellung verwendeten Lastausgleichsdienste ausgeführt werden.

Verfahren

- 1 Wenn Sie eine eigenständige Legacy-PostgreSQL-Datenbank verwenden, starten Sie diesen Server.
- 2 Starten Sie die eigenständigen vRealize Automation MS SQL-Server in beliebiger Reihenfolge.
- 3 Deaktivieren Sie in einer Bereitstellung, die Lastausgleichsdienste mit Integritätsprüfungen verwendet, alle Integritätsprüfungen mit Ausnahme von Pings.
- 4 Starten Sie die primäre vRealize Automation-Appliance.
- 5 Überprüfen Sie in der Verwaltungsschnittstelle der primären vRealize Automation-Appliance auf der Registerkarte **Cluster**, ob das System im synchronen oder asynchronen Modus ausgeführt wird. Eine Bereitstellung mit einer einzelnen Appliance ist immer asynchron.
 - Starten Sie bei einer synchronen Bereitstellung die verbleibenden vRealize Automation-Appliances.

- Navigieren Sie im Fall einer asynchronen Bereitstellung zur Verwaltungsschnittstelle der primären vRealize Automation-Appliance und warten Sie, bis der Lizenzierungsdienst ausgeführt wird und REGISTRIERT ist.

Starten Sie anschließend alle verbleibenden vRealize Automation-Appliances.

- 6 Verwenden Sie nach dem Start aller Appliances die zugehörigen Verwaltungsschnittstellen, um sicherzustellen, dass die Dienste ausgeführt werden und REGISTRIERT sind.

Es kann 15 Minuten oder noch länger dauern, bis Appliances starten.

- 7 Starten Sie alle IaaS-Webknoten und warten Sie 5 Minuten.
- 8 Starten Sie den primären Manager Service-Knoten und warten Sie 2 bis 5 Minuten.
- 9 Starten Sie sekundäre Manager Service-Knoten in einer verteilten Bereitstellung mit mehreren Manager Service-Knoten und warten Sie 2 bis 5 Minuten.

Starten Sie den Windows-Dienst nicht auf sekundären Maschinen und führen Sie ihn nicht aus, es sei denn, die Konfiguration ist für ein automatisches Manager Service-Failover vorgesehen.

- 10 Starten Sie in beliebiger Reihenfolge den DEM-Orchestrator, die DEM-Worker und alle vRealize Automation-Proxy-Agents.

Sie müssen nicht warten, bis ein Startvorgang abgeschlossen ist, bevor Sie einen anderen Startvorgang durchführen.

- 11 Wenn Sie die Integritätsprüfungen des Lastausgleichsdiensts deaktivieren mussten, aktivieren Sie sie erneut.

- 12 Stellen Sie sicher, dass die gestarteten Dienste ausgeführt werden und REGISTRIERT sind.

- a Melden Sie sich in einem Browser bei der Verwaltungsschnittstelle der primären vRealize Automation-Appliance an.

`https://vrealize-automation-appliance-FQDN:5480`

- b Klicken Sie auf die Registerkarte **Services**.

- c Überwachen Sie den Fortschritt des Startvorgangs, indem Sie auf **Aktualisieren** klicken.

Ergebnisse

Wenn alle Dienste REGISTRIERT sind, ist die Bereitstellung bereit.

Neustarten von vRealize Automation

Das Neustarten von vRealize Automation-Komponenten kann bei der Problembehebung hilfreich sein. Sie müssen die Komponenten in einer bestimmten Reihenfolge neu starten.

Wenn Sie Bereitstellungskomponenten in vCenter Server verwalten, können Sie deren Gastbetriebssysteme von dort aus neu starten.

Ist ein Neustart nicht möglich, verwenden Sie stattdessen die Anweisungen in [Herunterfahren von vRealize Automation](#) und [Starten von vRealize Automation](#).

Voraussetzungen

- Vergewissern Sie sich, dass alle in Ihrer Bereitstellung verwendeten Lastausgleichsdienste ausgeführt werden.

Verfahren

- 1 Stellen Sie sicher, dass die Datenbank der vRealize Automation-Appliance auf den asynchronen Modus festgelegt ist. Verwenden Sie bei Bedarf die Verwaltungsschnittstelle, um die Datenbank im asynchronen Modus auszuführen.

Nach Abschluss des gesamten Verfahrens können Sie zum synchronen Modus zurückkehren. Weitere Informationen hierzu finden Sie unter [Verwalten der vRealize Automation Postgres-Appliance-Datenbank](#).

- 2 Starten Sie die primäre vRealize Automation-Appliance neu und warten Sie, bis der Startvorgang abgeschlossen ist.
- 3 Verwenden Sie die Verwaltungsschnittstelle der primären vRealize Automation-Appliance, um sicherzustellen, dass der Lizenzierungsdienst ausgeführt wird und REGISTRIERT ist.
- 4 Starten Sie zur gleichen Zeit die verbleibenden vRealize Automation-Appliances neu.
- 5 Warten Sie, bis die Appliances neu gestartet wurden, und überprüfen Sie mithilfe der zugehörigen Verwaltungsschnittstellen, ob die Dienste ausgeführt werden und REGISTRIERT sind.

Es kann 15 Minuten oder länger dauern, bis die Appliances neu gestartet werden.

- 6 Starten Sie den primären Webknoten neu und warten Sie, bis der Startvorgang abgeschlossen ist.
- 7 Wenn Sie eine verteilte Bereitstellung mit mehreren Webknoten ausführen, starten Sie alle sekundären Webknoten neu und warten Sie, bis der Startvorgang abgeschlossen ist.
- 8 Starten Sie die Manager Service-Knoten neu und warten Sie, bis der Startvorgang abgeschlossen ist.

Wenn Sie ein automatisches Manager Service-Failover ausführen und die aktiven und passiven Knoten unverändert beibehalten möchten, verwenden Sie für den Neustart die folgende Reihenfolge:

- a Beenden Sie die passiven Manager Service-Knoten, ohne sie neu zu starten.
 - b Starten Sie den aktiven Manager Service-Knoten vollständig neu.
 - c Starten Sie die passiven Manager Service-Knoten neu.
- 9 Starten Sie in beliebiger Reihenfolge den DEM-Orchestrator, die DEM-Worker und alle vRealize Automation-Proxy-Agents neu. Warten Sie, bis alle Startvorgänge abgeschlossen sind.

Sie müssen nicht warten, bis ein Neustart abgeschlossen ist, bevor Sie einen anderen Neustart durchführen.

- 10 Stellen Sie sicher, dass die neu gestarteten Dienste ausgeführt werden und REGISTRIERT sind.
 - a Melden Sie sich in einem Browser bei der Verwaltungsschnittstelle der primären vRealize Automation-Appliance an.

https://vrealize-automation-appliance-FQDN:5480
 - b Klicken Sie auf die Registerkarte **Services**.
 - c Überwachen Sie den Fortschritt des Startvorgangs, indem Sie auf **Aktualisieren** klicken.

Ergebnisse

Wenn alle Dienste REGISTRIERT sind, ist die Bereitstellung bereit.

Herunterfahren von vRealize Automation

Zum Erhalten der Datenintegrität müssen Sie vRealize Automation in einer bestimmten Reihenfolge herunterfahren.

Wenn Sie Bereitstellungskomponenten in vCenter Server verwalten, können Sie die Gastbetriebssysteme von dort aus herunterfahren.

Verfahren

- 1 Fahren Sie in beliebiger Reihenfolge den DEM-Orchestrator, die DEM-Worker und alle vRealize Automation-Proxy-Agents herunter. Warten Sie, bis dieser Vorgang abgeschlossen ist.
- 2 Fahren Sie die Manager Service-Knoten herunter und warten Sie, bis dieser Vorgang abgeschlossen ist.
- 3 Fahren Sie sekundäre Webknoten in verteilten Bereitstellungen mit mehreren Webknoten herunter und warten Sie, bis der Vorgang abgeschlossen ist.
- 4 Fahren Sie den primären Webknoten herunter und warten Sie, bis der Vorgang abgeschlossen ist.
- 5 Verwenden Sie in verteilten Bereitstellungen mit mehreren vRealize Automation-Appliances im synchronen Modus die Verwaltungsschnittstelle der vRealize Automation-Appliance, um in den asynchronen Modus zu wechseln.
- 6 Fahren Sie sekundäre Appliances in verteilten Bereitstellungen mit mehreren vRealize Automation-Appliances herunter und warten Sie, bis der Vorgang abgeschlossen ist.
- 7 Fahren Sie die primäre vRealize Automation-Appliance herunter und warten Sie, bis der Vorgang abgeschlossen ist.

Bei der primären vRealize Automation-Appliance handelt es sich um die Appliance, die die primäre bzw. beschreibbare Appliance-Datenbank enthält. Notieren Sie sich die primäre Appliance, damit die Sicherung in der richtigen Reihenfolge gestartet werden kann.

- 8 Fahren Sie in beliebiger Reihenfolge alle eigenständigen vRealize Automation MS SQL-Server herunter und warten Sie, bis der Vorgang abgeschlossen ist.
- 9 Wenn Sie eine eigenständige Legacy-PostgreSQL-Datenbank verwenden, fahren Sie diesen Server herunter.

Aktualisieren von vRealize Automation-Zertifikaten

Ein Systemadministrator kann Zertifikate für vRealize Automation-Komponenten aktualisieren oder ersetzen.

vRealize Automation enthält drei Hauptkomponenten, die SSL-Zertifikate verwenden, um sichere Kommunikation untereinander zu erleichtern.

- vRealize Automation-Appliance
- IaaS-Website-Komponente
- IaaS Manager Service-Komponente

Zudem kann Ihre Bereitstellung Zertifikate für die Website der vRealize Automation-Appliance-Verwaltungsschnittstelle enthalten. Auch wird auf jeder IaaS-Maschine, die ein Zertifikat verwendet, ein Management-Agent ausgeführt.

Hinweis vRealize Automation verwendet mehrere Produkte von Drittanbietern, wie z. B. Rabbit MQ, um eine Vielzahl von Funktionen zu unterstützen. Einige dieser Produkte verwenden selbstsignierte Zertifikate, die auch dann beibehalten werden, wenn Sie primäre vRealize Automation-Zertifikate durch die von einer Zertifizierungsstelle bereitgestellten Zertifikate ersetzen. Aufgrund dieser Situation können Benutzer die Verwendung von Zertifikaten für bestimmte Ports nicht effektiv steuern. Ein Beispiel hierfür ist Port 5671, der von RabbitMQ für die interne Kommunikation verwendet wird.

Mit einer Ausnahme wirken sich Änderungen an späteren Komponenten in dieser Liste nicht auf frühere aus. Die Ausnahme besteht darin, dass ein aktualisiertes Zertifikat für IaaS-Komponenten bei der vRealize Automation-Appliance registriert werden muss.

Normalerweise werden selbstsignierte Zertifikate während der Produktinstallation generiert und auf diese Komponenten angewendet. In der Regel ersetzen Sie ein Zertifikat, um von selbstsignierten Zertifikaten zu den durch Zertifizierungsstellen zur Verfügung gestellten Zertifikaten zu wechseln, oder wenn ein Zertifikat abläuft. Wenn Sie ein Zertifikat für eine vRealize Automation-Komponente ersetzen, werden Vertrauensstellungen für andere vRealize Automation-Komponenten automatisch aktualisiert.

Beispiel: Wenn Sie in einem verteilten System mit mehreren Instanzen einer vRealize Automation-Appliance ein Zertifikat für eine vRealize Automation-Appliance aktualisieren, werden alle anderen zugehörigen Zertifikate automatisch aktualisiert.

Hinweis vRealize Automation unterstützt SHA2-Zertifikate. Die vom System generierten selbstsignierten Zertifikate verwenden SHA-256 mit RSA-Verschlüsselung. Aufgrund von Betriebssystem- oder Browseranforderungen müssen Sie möglicherweise eine Aktualisierung auf SHA2-Zertifikate durchführen.

Die Verwaltungsschnittstelle der vRealize Automation-Appliance bietet Optionen zum Aktualisieren oder Ersetzen von Zertifikaten.

In einer geclusterten Bereitstellung müssen Sie Änderungen über die Schnittstelle des primären Knotens initiieren.

- **Zertifikat erzeugen** – vRealize Automation muss ein selbstsigniertes Zertifikat erzeugen.
- **Zertifikat importieren** – Verwenden des eigenen Zertifikats.
- **Zertifikatsfingerabdruck bereitstellen** – Bereitstellen des Zertifikatsfingerabdrucks, um ein bereits im Zertifikatsspeicher enthaltenes Zertifikat auf IaaS-Windows-Servern zu verwenden.

Mit dieser Option wird das Zertifikat nicht von der vRealize Automation-Appliance an die IaaS-Server übertragen. Mit dieser Option können Benutzer bereits auf IaaS-Windows-Servern vorhandene Zertifikate bereitstellen, ohne die Zertifikate in die Verwaltungsschnittstelle der vRealize Automation-Appliance hochzuladen.

- **Vorhandenes beibehalten** – Fortsetzen der Verwendung des aktuellen Zertifikats.

Zertifikate für die Website der Verwaltungsschnittstelle der vRealize Automation-Appliance müssen keine Registrierungsanforderungen erfüllen.

Hinweis Wenn bei dem Zertifikat ein Kennwortsatz für die Verschlüsselung verwendet wird und Sie diesen beim Ersetzen Ihres Zertifikats auf der Appliance nicht eingeben, schlägt die Zertifikatsersetzung fehl und die Meldung `Unable to load private key` wird angezeigt.

VM-Vorlagen

Nach dem Ändern von Zertifikaten in der vRealize Automation-Appliance oder auf dem IaaS-Windows-Server müssen Sie Gast- und Software-Agents in VM-Vorlagen in vRealize Automation aktualisieren, damit die Vorlagen in vRealize Automation weiterhin funktionieren. Wenn Sie die Agents nicht aktualisieren, schlagen Bereitstellungsanforderungen mit Softwarekomponenten mit einem Fehler ähnlich dem folgenden Beispiel fehl.

```
The following component requests failed: Linux. Request failed: Machine VM-001:
InstallSoftwareWorkflow. Install software work item timeout.
```

vRealize Orchestrator

Nach dem Ändern von vRealize Automation-Zertifikaten müssen Sie vRealize Orchestrator aktualisieren, damit die neuen Zertifikate als vertrauenswürdig eingestuft werden.

Die vRealize Orchestrator-Komponente, die Ihrer vRealize Automation-Bereitstellung zugeordnet ist, verfügt über eigene Zertifikate und muss die vRealize Automation-Zertifikate ebenfalls als vertrauenswürdig einstufen. Die vRealize Orchestrator-Komponente ist standardmäßig in vRealize Automation eingebettet. Dennoch entscheiden sich einige Benutzer dazu, einen externen vRealize Orchestrator zu verwenden. In beiden Fällen finden Sie in der Dokumentation zu vRealize Orchestrator weitere Informationen zum Aktualisieren von vRealize Orchestrator-Zertifikaten.

Wenn Sie eine vRealize Orchestrator-Bereitstellung mit mehreren Knoten hinter einem Lastausgleichsdienst ausführen, müssen alle vRealize Orchestrator-Knoten dasselbe Zertifikat verwenden.

Weitere Informationen

Weitere Informationen zu Fehlerbehebung bei Zertifikaten, Unterstützbarkeit und Anforderungen hinsichtlich Vertrauenswürdigkeit finden Sie im [VMware Knowledgebase-Artikel 2106583](#).

Extrahieren von Zertifikaten und privaten Schlüsseln

Zertifikate, die Sie zusammen mit den virtuellen Appliances verwenden, müssen das PEM-Dateiformat aufweisen.

Für die Beispiele in der folgenden Tabelle werden openssl-GNU-Befehle verwendet, um die erforderlichen Zertifikatinformationen zum Konfigurieren der virtuellen Appliances zu extrahieren.

Tabelle 1-2. Beispielzertifikatwerte und -befehle (openssl)

Von Zertifizierungsstelle bereitgestellt	Befehl	Einträge der virtuellen Appliance
RSA-Privatschlüssel	<code>openssl pkcs12 -in <i>path_to_.pfx</i> <i>certificate_file</i> -nocerts -out key.pem</code>	RSA-Privatschlüssel
PEM-Datei	<code>openssl pkcs12 -in <i>path_to_.pfx</i> <i>certificate_file</i> -clcerts -nokeys -out cert.pem</code>	Zertifikatskette
(Optional) Kennwortsatz	Nicht verfügbar	Kennwortsatz

Ersetzen von Zertifikaten in der vRealize Automation-Appliance

Der Systemadministrator kann ein selbstsigniertes Zertifikat mit einem vertrauenswürdigen Zertifikat von einer Zertifizierungsstelle aktualisieren oder ersetzen. Sie können Zertifikate mit alternativen Antragstellernamen (Subject Alternative Name, SAN), Platzhalterzertifikate oder eine sonstige für Ihre Umgebung geeignete Methode für die Mehrfachverwendungszertifizierung

verwenden, vorausgesetzt, die Anforderungen im Hinblick auf die Vertrauenswürdigkeit sind erfüllt.

Wenn Sie das Zertifikat der vRealize Automation-Appliance aktualisieren oder ersetzen, wird das Vertrauen zu anderen zugehörigen Komponenten automatisch neu initiiert. Weitere Informationen zum Aktualisieren von Zertifikaten finden Sie unter [Aktualisieren von vRealize Automation-Zertifikaten](#).

Verfahren

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

`https://vrealize-automation-appliance-FQDN:5480`

- 2 Wählen Sie **vRA > Zertifikate** aus.
- 3 Wählen Sie die vRealize Automation-Komponente, für die Sie das Zertifikat aktualisieren.
- 4 Wählen Sie über das Menü **Zertifikatsaktion** die gewünschte Aktion aus.

Wenn Sie ein PEM-verschlüsseltes Zertifikat verwenden, beispielsweise für eine verteilte Umgebung, wählen Sie **Importieren** aus.

Zu importierende Zertifikate müssen vertrauenswürdig sein und außerdem auf alle Instanzen der vRealize Automation-Appliance und auf jeden Lastausgleichsdienst durch die Verwendung von Zertifikaten mit einem alternativen Antragstellernamen anwendbar sein.

Wenn Sie eine CSR-Anforderung für ein neues Zertifikat generieren möchten, um sie an eine Zertifizierungsstelle zu senden, wählen Sie **Anforderung zur Zertifikatssignierung (CSR) erstellen** aus. Eine CSR hilft der Zertifizierungsstelle dabei, ein Zertifikat mit den richtigen Werten zu erstellen, das Sie importieren können.

Hinweis Wenn Sie Zertifikatsketten verwenden, geben Sie die Zertifikate in der folgenden Reihenfolge an:

- a Von der Zwischenzertifizierungsstelle signiertes Client-/Serverzertifikat
- b Ein oder mehrere Zwischenzertifikate
- c Zertifizierungsstellen-Stammzertifikat

Option	Aktion
Vorhandene beibehalten	Behalten Sie die aktuelle SSL-Konfiguration bei. Wählen Sie diese Option zum Verwerfen der Änderungen.
Zertifikat generieren	<ul style="list-style-type: none"> a Der im Textfeld Allgemeiner Name angezeigte Wert ist der Hostname, wie er im oberen Teil der Seite angezeigt wird. Wenn zusätzliche Instanzen der vRealize Automation-Appliance verfügbar sind, werden ihre FQDNs dem SAN-Attribut des Zertifikats hinzugefügt. b Geben Sie den Namen Ihrer Organisation, wie z. B. den Unternehmensnamen, in das Textfeld Organisation ein. c Geben Sie Ihre Organisationseinheit, wie z. B. den Namen oder den Standort Ihrer Abteilung, in das Textfeld Organisationseinheit ein. d Geben Sie eine zweistellige Landeskennzahl nach ISO 3166 wie z. B. DE in das Textfeld Land ein.

Option	Aktion
Anforderung zur Zertifikatssignierung (CSR) erstellen	<ul style="list-style-type: none"> a Wählen Sie Anforderung zur Zertifikatssignierung (CSR) erstellen aus. b Überprüfen Sie die Einträge in den Textfeldern Organisation, Organisationseinheit, Landeskennzahl und Allgemeiner Name. Diese Einträge werden durch das vorhandene Zertifikat ausgefüllt. Sie können diese Einträge bei Bedarf bearbeiten. c Klicken Sie auf CSR erstellen, um eine Anforderung zur Zertifikatssignierung zu erstellen. Klicken Sie anschließend auf den Link Erstellte CSR hier herunterladen. Es wird ein Dialogfeld geöffnet, über das Sie die CSR an einem bestimmten Ort speichern und anschließend an die Zertifizierungsstelle senden können. d Wenn Sie das vorbereitete Zertifikat erhalten, klicken Sie auf Import und befolgen Sie die Anweisungen zum Importieren eines Zertifikats in vRealize Automation.
Importieren	<ul style="list-style-type: none"> a Kopieren Sie die Zertifikatwerte von BEGIN PRIVATE KEY zu END PRIVATE KEY, einschließlich der Kopfzeile und der Fußzeile, und fügen Sie sie in das Textfeld RSA-Privatschlüssel ein. b Kopieren Sie die Zertifikatwerte von BEGIN CERTIFICATE zu END CERTIFICATE, einschließlich der Kopfzeile und der Fußzeile, und fügen Sie sie in das Textfeld Zertifikatskette ein. Fügen Sie für mehrere Zertifikatwerte eine BEGIN CERTIFICATE-Kopfzeile und eine END CERTIFICATE-Fußzeile für jedes Zertifikat hinzu. <hr/> <p>Hinweis Im Fall von verketteten Zertifikaten sind möglicherweise zusätzliche Attribute verfügbar.</p> <hr/> <ul style="list-style-type: none"> c (Optional) Wenn das Zertifikat eine Passphrase zum Verschlüsseln des Zertifikatschlüssels verwendet, kopieren Sie die Passphrase und fügen Sie sie in das Textfeld Passphrase ein.

5 Klicken Sie auf **Einstellungen speichern**.

Um das Zertifikat der vRealize Automation-Appliance zu aktualisieren, müssen vRealize Automation-Dienste ordnungsgemäß gestartet werden. Der Neustart kann je nach Anzahl der vRealize Automation-Appliances in Ihrer Umgebung zwischen 15 Minuten und einer Stunde dauern.

Nach dem Neustart werden die Zertifikatsdetails für alle anwendbaren Instanzen der vRealize Automation-Appliance auf der Seite angezeigt.

6 Falls Ihr Netzwerk oder Lastausgleichsdienst dies erfordert, kopieren Sie das importierte oder neu erstellte Zertifikat in den Lastausgleichsdienst der virtuellen Appliance.

Möglicherweise müssen Sie den Root-SSH-Zugriff aktivieren, um das Zertifikat zu exportieren.

- a Falls Sie nicht bereits angemeldet sind, melden Sie sich bei der Managementkonsole der vRealize Automation-Appliance als Root-Benutzer an.
- b Klicken Sie auf die Registerkarte **Administrator**.
- c Klicken Sie auf das Untermenü **Administrator**.

- d Aktivieren Sie das Kontrollkästchen **SSH-Dienst aktiviert**.
Deaktivieren Sie das Kontrollkästchen, um SSH nach Abschluss des Vorgangs zu deaktivieren.
 - e Aktivieren Sie das Kontrollkästchen **SSH-Anmeldung des Administrators**.
Deaktivieren Sie das Kontrollkästchen, um SSH nach Abschluss des Vorgangs zu deaktivieren.
 - f Klicken Sie auf **Einstellungen speichern**.
- 7** Überprüfen Sie, ob Sie sich bei der vRealize Automation-Konsole anmelden können.
- a Öffnen Sie einen Browser und navigieren Sie zu `https://vcac-hostname.domain.name/vcac/`.

Wenn Sie einen Lastausgleichsdienst verwenden, muss der Hostname der vollqualifizierte Domänenname des Lastausgleichsdiensts sein.
 - b Ignorieren Sie ggf. etwaige Zertifikatswarnungen.
 - c Melden Sie sich mit **administrator@vsphere.local** und dem Kennwort an, das Sie beim Konfigurieren der Verzeichnisverwaltung angegeben haben.

Die Konsole wird auf der Seite **Mandanten** auf der Registerkarte **Administration** geöffnet.
Ein einzelner Mandant mit dem Namen `vsphere.local` wird in der Liste angezeigt.
- 8** Wenn Sie einen Lastausgleichsdienst verwenden, konfigurieren Sie alle anwendbaren Integritätsprüfungen und aktivieren Sie sie.

Ergebnisse

Das Zertifikat wird aktualisiert.

Ersetzen des Infrastructure as a Service-Zertifikats

Der Systemadministrator kann ein abgelaufenes oder selbstsigniertes Zertifikat durch ein von einer Zertifizierungsstelle ausgestelltes Zertifikat zur Gewährleistung der Sicherheit in einer Umgebung mit verteilter Bereitstellung ersetzen.

Sie können ein Zertifikat mit einem alternativen Antragstellernamen auf mehreren Maschinen verwenden. Die für die IaaS-Komponenten (Website und Manager Service) verwendeten Zertifikate müssen mit SAN-Werten (einschließlich FQDNs) aller Windows-Hosts ausgestellt werden, auf denen die entsprechende Komponente mit der Lastausgleichs-FQDN für dieselbe Komponente installiert ist.

Verfahren

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

`https://vrealize-automation-appliance-FQDN:5480`
- 2** Wählen Sie **vRA > Zertifikate** aus.

- 3 Klicken Sie im Menü **Komponententyp** auf **laaS-Web**.
- 4 Navigieren Sie zum Fensterbereich **laaS-Webzertifikat**.
- 5 Wählen Sie im Menü **Zertifikatsaktion** die Option zum Ersetzen des Zertifikats aus.

Wenn Sie ein PEM-verschlüsseltes Zertifikat verwenden, beispielsweise für eine verteilte Umgebung, wählen Sie **Importieren** aus.

Zu importierende Zertifikate müssen vertrauenswürdig sein und außerdem auf alle Instanzen der vRealize Automation-Appliance und auf jeden Lastausgleichsdienst durch die Verwendung von Zertifikaten mit einem alternativen Antragstellernamen anwendbar sein.

Hinweis Wenn Sie Zertifikatsketten verwenden, geben Sie die Zertifikate in der folgenden Reihenfolge an:

- a Von der Zwischenzertifizierungsstelle signiertes Client-/Serverzertifikat
- b Ein oder mehrere Zwischenzertifikate
- c Zertifizierungsstellen-Stammzertifikat

Option	Beschreibung
Vorhandene beibehalten	Behalten Sie die aktuelle SSL-Konfiguration bei. Wählen Sie diese Option aus, um Ihre Änderungen zu verwerfen.
Zertifikat generieren	<ol style="list-style-type: none"> a Der im Textfeld Allgemeiner Name angezeigte Wert ist der Hostname, wie er im oberen Teil der Seite angezeigt wird. Wenn zusätzliche Instanzen der vRealize Automation-Appliance verfügbar sind, werden ihre FQDNs dem SAN-Attribut des Zertifikats hinzugefügt. b Geben Sie den Namen Ihrer Organisation, wie z. B. den Unternehmensnamen, in das Textfeld Organisation ein. c Geben Sie Ihre Organisationseinheit, wie z. B. den Namen oder den Standort Ihrer Abteilung, in das Textfeld Organisationseinheit ein. d Geben Sie eine zweistellige Landeskennzahl nach ISO 3166 wie z. B. DE in das Textfeld Land ein.

Option	Beschreibung
Importieren	<p>a Kopieren Sie die Zertifikatwerte von BEGIN PRIVATE KEY zu END PRIVATE KEY, einschließlich der Kopfzeile und der Fußzeile, und fügen Sie sie in das Textfeld RSA-Privatschlüssel ein.</p> <p>b Kopieren Sie die Zertifikatwerte von BEGIN CERTIFICATE zu END CERTIFICATE, einschließlich der Kopfzeile und der Fußzeile, und fügen Sie sie in das Textfeld Zertifikatskette ein. Fügen Sie für mehrere Zertifikatwerte eine BEGIN CERTIFICATE-Kopfzeile und eine END CERTIFICATE-Fußzeile für jedes Zertifikat hinzu.</p> <hr/> <p>Hinweis Im Fall von verketteten Zertifikaten sind möglicherweise zusätzliche Attribute verfügbar.</p> <hr/> <p>c (Optional) Wenn das Zertifikat eine Passphrase zum Verschlüsseln des Zertifikatschlüssels verwendet, kopieren Sie die Passphrase und fügen Sie sie in das Textfeld Passphrase ein.</p>
Fingerabdruck des Zertifikats bereitstellen	Verwenden Sie diese Option, wenn Sie einen Fingerabdruck eines Zertifikats bereitstellen möchten, das im Zertifikatspeicher auf den IaaS-Servern bereits verwendet wird. Bei Verwendung dieser Option wird das Zertifikat nicht von der virtuellen Appliance an die IaaS-Server übertragen. Mit dieser Option können Benutzer vorhandene Zertifikate auf IaaS-Servern bereitstellen, ohne sie auf die Verwaltungsschnittstelle hochladen zu müssen.

6 Klicken Sie auf **Einstellungen speichern**.

Um das Zertifikat eines IaaS-Windows-Servers zu aktualisieren, müssen vRealize Automation-Dienste ordnungsgemäß gestartet werden. Der Neustart kann je nach Anzahl der vRealize Automation-Appliances in Ihrer Umgebung zwischen 15 Minuten und einer Stunde dauern.

Nach dem Neustart werden die Zertifikatsdetails auf der Seite angezeigt.

Ersetzen des IaaS Manager Service-Zertifikats

Ein Systemadministrator kann ein abgelaufenes Zertifikat oder ein selbstsigniertes Zertifikat mit einem Zertifikat von einer Zertifizierungsstelle ersetzen, um die Sicherheit in einer Umgebung mit einer verteilten Bereitstellung sicherzustellen.

Sie können ein Zertifikat mit einem alternativen Antragstellernamen auf mehreren Maschinen verwenden. Die für die IaaS-Komponenten (Website und Manager Service) verwendeten Zertifikate müssen mit SAN-Werten (einschließlich FQDNs) aller Windows-Hosts ausgestellt werden, auf denen die entsprechende Komponente mit der Lastausgleichs-FQDN für dieselbe Komponente installiert ist.

Der IaaS-Manager Service und der IaaS-Webdienst verwenden ein einzelnes Zertifikat gemeinsam.

Verfahren

- 1 Öffnen Sie die URL für die Verwaltungsschnittstelle der vRealize Automation-Appliance in einem Webbrowser.
- 2 Melden Sie sich mit dem Benutzernamen **root** und dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance angegeben haben.

- 3 Wählen Sie **vRA > Zertifikate** aus.
- 4 Klicken Sie im Menü **Komponententyp** auf **Manager Service**.
- 5 Wählen Sie aus dem Menü **Zertifikatsaktion** den Zertifikatstyp aus.

Wenn Sie ein PEM-verschlüsseltes Zertifikat verwenden, beispielsweise für eine verteilte Umgebung, wählen Sie **Importieren** aus.

Zu importierende Zertifikate müssen vertrauenswürdig sein und außerdem auf alle Instanzen der vRealize Automation-Appliance und auf jeden Lastausgleichsdienst durch die Verwendung von Zertifikaten mit einem alternativen Antragstellernamen anwendbar sein.

Hinweis Wenn Sie Zertifikatsketten verwenden, geben Sie die Zertifikate in der folgenden Reihenfolge an:

- a Von der Zwischenzertifizierungsstelle signiertes Client-/Serverzertifikat
- b Ein oder mehrere Zwischenzertifikate
- c Zertifizierungsstellen-Stammzertifikat

Option	Beschreibung
Vorhandene beibehalten	Behalten Sie die aktuelle SSL-Konfiguration bei. Wählen Sie diese Option aus, um Ihre Änderungen zu verwerfen.
Zertifikat generieren	<ol style="list-style-type: none"> a Der im Textfeld Allgemeiner Name angezeigte Wert ist der Hostname, wie er im oberen Teil der Seite angezeigt wird. Wenn zusätzliche Instanzen der vRealize Automation-Appliance verfügbar sind, werden ihre FQDNs dem SAN-Attribut des Zertifikats hinzugefügt. b Geben Sie den Namen Ihrer Organisation, wie z. B. den Unternehmensnamen, in das Textfeld Organisation ein. c Geben Sie Ihre Organisationseinheit, wie z. B. den Namen oder den Standort Ihrer Abteilung, in das Textfeld Organisationseinheit ein. d Geben Sie eine zweistellige Landeskennzahl nach ISO 3166 wie z. B. DE in das Textfeld Land ein.

Option	Beschreibung
Importieren	<p>a Kopieren Sie die Zertifikatwerte von BEGIN PRIVATE KEY zu END PRIVATE KEY, einschließlich der Kopfzeile und der Fußzeile, und fügen Sie sie in das Textfeld RSA-Privatschlüssel ein.</p> <p>b Kopieren Sie die Zertifikatwerte von BEGIN CERTIFICATE zu END CERTIFICATE, einschließlich der Kopfzeile und der Fußzeile, und fügen Sie sie in das Textfeld Zertifikatskette ein. Fügen Sie für mehrere Zertifikatwerte eine BEGIN CERTIFICATE-Kopfzeile und eine END CERTIFICATE-Fußzeile für jedes Zertifikat hinzu.</p> <hr/> <p>Hinweis Im Fall von verketteten Zertifikaten sind möglicherweise zusätzliche Attribute verfügbar.</p> <hr/> <p>c (Optional) Wenn das Zertifikat eine Passphrase zum Verschlüsseln des Zertifikatschlüssels verwendet, kopieren Sie die Passphrase und fügen Sie sie in das Textfeld Passphrase ein.</p>
Fingerabdruck des Zertifikats bereitstellen	Verwenden Sie diese Option, wenn Sie einen Fingerabdruck eines Zertifikats bereitstellen möchten, das im Zertifikatspeicher auf den IaaS-Servern bereits verwendet wird. Bei Verwendung dieser Option wird das Zertifikat nicht von der virtuellen Appliance an die IaaS-Server übertragen. Mit dieser Option können Benutzer vorhandene Zertifikate auf IaaS-Servern bereitstellen, ohne sie auf die Verwaltungsschnittstelle hochladen zu müssen.

6 Klicken Sie auf **Einstellungen speichern**.

Nach einigen Minuten werden die Zertifikatdetails auf der Seite angezeigt.

7 Kopieren Sie das importierte oder neu erstellte Zertifikat in den Lastenausgleichsdienst, wenn dies vom Netzwerk oder dem Lastenausgleichsdienst gefordert wird.

8 Öffnen Sie einen Browser und navigieren Sie zu `https://managerServiceAddress/vmpsProvision/` über einen Server, der einen DEM-Worker oder -Agent ausführt.

Wenn Sie einen Lastenausgleichsdienst verwenden, muss der Hostname der vollqualifizierte Domänenname des Lastenausgleichsdiensts sein.

9 Ignorieren Sie ggf. etwaige Zertifikatswarnungen.

10 Stellen Sie sicher, dass das neue Zertifikat bereitgestellt und vertrauenswürdig ist.

11 Wenn Sie einen Lastenausgleichsdienst verwenden, konfigurieren Sie alle anwendbaren Integritätsprüfungen und aktivieren Sie sie.

Aktualisieren von eingebettetem vRealize Orchestrator, sodass vRealize Automation-Zertifikate als vertrauenswürdig eingestuft werden

Wenn Sie vRealize Automation-Appliance- oder IaaS-Zertifikate aktualisieren oder ändern, müssen Sie vRealize Orchestrator aktualisieren, sodass es die neuen oder aktualisierten Zertifikate als vertrauenswürdig einstuft.

Dieses Verfahren gilt für alle vRealize Automation-Bereitstellungen, die eine eingebettete Instanz von vRealize Orchestrator verwenden. Wenn Sie eine externe Instanz von vRealize Orchestrator verwenden, finden Sie weitere Informationen unter [Aktualisieren von externem vRealize Orchestrator, sodass vRealize Automation-Zertifikate als vertrauenswürdig eingestuft werden](#).

Hinweis Bei diesem Verfahren werden die Mandanten- und die Gruppenauthentifizierung auf die Standardeinstellungen zurückgesetzt. Wenn Sie Ihre Authentifizierungskonfiguration angepasst haben, notieren Sie sich Ihre Änderungen, damit Sie die Authentifizierung nach Abschluss des Verfahrens erneut konfigurieren können.

Weitere Informationen zum Aktualisieren und Ersetzen von vRealize Orchestrator-Zertifikaten finden Sie in der Dokumentation zu vRealize Orchestrator.

In einer geclusterten Konfiguration müssen Sie diesen Vorgang auf dem primären vRealize Automation-Appliance-Knoten ausführen und dann einen `join-cluster`-Vorgang anhand des primären Knotens von jedem Replikat-vRealize Automation-Appliance-Knoten ausführen.

Hinweis Beenden Sie in einem Cluster den `vco-configurator`-Dienst auf allen Replikatknoten, bis der Vorgang abgeschlossen ist, um eine unerwünschte automatische Control Center-Synchronisierung zu vermeiden.

Wenn Sie vRealize Automation-Zertifikate ersetzen oder aktualisieren, ohne dieses Verfahren abzuschließen, kann auf das vRealize Orchestrator Control Center möglicherweise nicht zugegriffen werden, und in den Protokolldateien `vco-server` und `vco-configurator` werden Fehler aufgezeichnet.

Probleme beim Aktualisieren von Zertifikaten können auch auftreten, wenn vRealize Orchestrator so konfiguriert wird, dass es die Authentifizierung anhand eines anderen Mandaten oder einer anderen Gruppe vornimmt als vRealize Automation. Informationen finden Sie im VMware-Knowledgebase-Artikel [Ausnahme „Nicht vertrauenswürdige Zertifikatskette“ nach dem Ersetzen des vRA-Zertifikats \(2147612\)](#).

Die hier aufgeführten Beispiele für Trust-Befehlssyntax sind repräsentativ und nicht definitiv. Während Sie für die meisten typischen Bereitstellungen geeignet sind, kann es Situationen geben, in denen Sie mit Variationen der Befehle experimentieren müssen.

- Wenn Sie `--certificate` angeben, müssen Sie den Pfad zu einer gültigen Zertifikatsdatei im PEM-Format angeben.
- Wenn Sie `--uri` angeben, müssen Sie den URI angeben, von dem aus der Befehl ein vertrauenswürdiges Zertifikat abrufen kann.
- Wenn Sie die Option `--registry-certificate` angeben, geben Sie an, dass das angeforderte Zertifikat als Zertifikat für die Komponentenregistrierung behandelt und das vertrauenswürdige Zertifikat dem Truststore unter einem bestimmten vom Komponentenregistrierungszertifikat verwendeten Alias hinzugefügt werden soll.

Sie können Zertifikate auch verwalten, indem Sie SSL Trust Manager-Workflows in vRealize Orchestrator verwenden. Informationen hierzu finden Sie unter dem Thema *Verwalten von Orchestrator-Zertifikaten* in der [vRealize Orchestrator-Dokumentation](#).

Verfahren

- 1 Beenden Sie den vRealize Orchestrator-Server und die Control Center-Dienste.

```
service vco-server stop
service vco-configurator stop
```

- 2 Setzen Sie den vRealize Orchestrator-Authentifizierungsanbieter durch Ausführen des folgenden Befehls zurück.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
ls -l /etc/vco/app-server/
mv /etc/vco/app-server/vco-registration-id /etc/vco/app-server/vco-registration-id.old
vcac-vami vco-service-reconfigure
```

- 3 Überprüfen Sie das vertrauenswürdige Zertifikat für den vRealize Orchestrator-Truststore mithilfe der Befehlszeilenschnittstelle unter `/var/lib/vco/tools/configuration-cli/bin` mit dem folgenden Befehl.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

- Suchen Sie nach dem Zertifikat mit dem folgenden Alias: `vco.cafe.component-registry.ssl.certificate`. Dies sollte das vRealize Automation-Zertifikat sein, das die vRealize Orchestrator-Instanz als Authentifizierungsanbieter verwendet.
- Dieses Zertifikat muss mit dem neu konfigurierten vRealize Automation-Zertifikat übereinstimmen. Wenn es nicht übereinstimmt, können Sie es wie folgt ändern:
 - 1 Kopieren Sie die PEM-Datei des signierten vRealize Automation-Appliance-Zertifikats in den Ordner `/tmp` auf der-Appliance.
 - 2 Führen Sie den folgenden Befehl aus und fügen Sie dabei den entsprechenden Zertifikatspfad hinzu.

```
./vro-configure.sh trust --certificate path-to-the-certificate-file-in-PEM-format--registry-certificate
```

Nachstehend finden Sie einen Beispielbefehl.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --certificate /var/tmp/test.pem --registry-certificate
```

- 4 Möglicherweise müssen Sie die folgenden Befehle ausführen, um dem Zertifikat zu vertrauen.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --uri https://vra.domain.com

/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --registry-certificate --uri
https://vra.domain.com
```

- 5 Stellen Sie mit dem folgenden Befehl sicher, dass das vRealize Automation-Zertifikat jetzt in den vRealize Orchestrator-Truststore eingefügt ist.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

- 6 Starten Sie den vRealize Orchestrator-Server und die Control Center-Dienste.

```
service vco-server start
service vco-configurator start
```

Nächste Schritte

Sie können überprüfen, ob die Vertrauensstellung auf einem geclusterten System aktualisiert wurde.

- 1 Melden Sie sich bei der Virtual Appliance Management Interface (VAMI) als Root-Benutzer an.
- 2 Wählen Sie die Seite „Services“ aus.
- 3 Stellen Sie sicher, dass keine doppelten vco-Dienste aufgeführt sind.

Wenn eine Duplizierung der vco-Dienste angezeigt wird, klicken Sie auf **Registrierung aufheben**, um die Dienste zu entfernen, die nicht den Status Registered aufweisen.

- 4 Stellen Sie sicher, dass der vco-configurator auf allen Knoten der virtuellen Appliance gestartet wird.
- 5 Melden Sie sich beim vRealize Orchestrator Control Center an und navigieren Sie zur Seite „Konfiguration validieren“, um die Konfiguration zu validieren.
- 6 Navigieren Sie zur Seite „Authentifizierungsanbieter“ und überprüfen Sie, ob die Authentifizierungseinstellungen korrekt sind.

Sie können die Anmeldedaten auch auf dieser Seite testen.

Aktualisieren von externem vRealize Orchestrator, sodass vRealize Automation-Zertifikate als vertrauenswürdig eingestuft werden

Wenn Sie vRealize Automation-Appliance- oder IaaS-Zertifikate aktualisieren oder ändern, müssen Sie vRealize Orchestrator aktualisieren, sodass es die neuen oder aktualisierten Zertifikate als vertrauenswürdig einstuft.

Dieses Verfahren gilt für vRealize Automation-Bereitstellungen, die eine externe Instanz von vRealize Orchestrator verwenden.

Hinweis Bei diesem Verfahren werden die Mandanten- und die Gruppenauthentifizierung auf die Standardeinstellungen zurückgesetzt. Wenn Sie Ihre Authentifizierungskonfiguration angepasst haben, notieren Sie sich Ihre Änderungen, damit Sie die Authentifizierung nach Abschluss des Verfahrens erneut konfigurieren können.

Weitere Informationen zum Aktualisieren und Ersetzen von vRealize Orchestrator-Zertifikaten finden Sie in der Dokumentation zu vRealize Orchestrator.

Wenn Sie vRealize Automation-Zertifikate ersetzen oder aktualisieren, ohne dieses Verfahren abzuschließen, kann auf das vRealize Orchestrator-Control Center möglicherweise nicht zugegriffen werden und in den Protokolldateien vco-server und vco-configurator werden Fehler aufgezeichnet.

Probleme beim Aktualisieren von Zertifikaten können auch auftreten, wenn vRealize Orchestrator so konfiguriert wird, dass es die Authentifizierung anhand eines anderen Mandaten oder einer anderen Gruppe vornimmt als vRealize Automation. Weitere Informationen hierzu finden Sie im [Knowledgebase-Artikel 2147612](#).

Verfahren

- 1 Beenden Sie den vRealize Orchestrator-Server und die Control Center-Dienste.
`service vco-configurator stop`
- 2 Setzen Sie den Authentifizierungsanbieter vRealize Orchestrator zurück.
`/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication`
- 3 Starten Sie den vRealize Orchestrator-Control Center-Dienst.
`service vco-configurator start`
- 4 Melden Sie sich beim Control Center mithilfe der Root-Anmeldedaten der Virtual Appliance Management Interface (VAMI) an.
- 5 Heben Sie die Registrierung des Authentifizierungsanbieters auf und registrieren Sie ihn erneut.

Aktualisieren des Management-Site-Zertifikats der vRealize Automation-Appliance

Der Systemadministrator kann das SSL-Zertifikat des Management-Site-Diensts ersetzen, wenn es abläuft, oder um ein selbstsigniertes Zertifikat durch ein von einer Zertifizierungsstelle ausgegebenes Zertifikat zu ersetzen. Sie sichern den Management-Site-Dienst auf Port 5480.

Die vRealize Automation-Appliance verwendet lighttpd zum Ausführen der eigenen Management-Site. Wenn Sie ein Management-Site-Zertifikat ersetzen, müssen Sie auch alle Management-Agents so konfigurieren, dass sie das neue Zertifikat erkennen.

Wenn Sie eine verteilte Bereitstellung ausführen, können Sie Management-Agents automatisch oder manuell aktualisieren. Wenn Sie eine minimale Bereitstellung ausführen, müssen Sie den Management-Agent manuell aktualisieren.

Weitere Informationen hierzu finden Sie unter [Manuelles Aktualisieren der Zertifikatserkennung für Management-Agents](#).

Verfahren

1 Suchen des Management-Agent-Bezeichners

Den Management-Agent-Bezeichner können Sie bei der Erstellung und Registrierung eines neuen Serverzertifikats für die Management-Site verwenden.

2 Ersetzen des Management-Site-Zertifikats der vRealize Automation Appliance

Wenn das SSL-Zertifikat des Management-Site-Diensts abläuft oder Sie mit einem selbstsignierten Zertifikat begonnen haben und Site-Richtlinien ein anderes erfordern, können Sie das Zertifikat ersetzen.

3 Aktualisieren der Zertifikatserkennung für Management-Agents

Nach dem Ersetzen eines Management-Site-Zertifikats einer vRealize Automation-Appliance müssen Sie zur Erkennung des neuen Zertifikats alle Management-Agents aktualisieren, um eine vertrauenswürdige Kommunikation zwischen der Management-Site der virtuellen Appliance und den Management-Agents auf den IaaS-Hosts wiederherzustellen.

Suchen des Management-Agent-Bezeichners

Den Management-Agent-Bezeichner können Sie bei der Erstellung und Registrierung eines neuen Serverzertifikats für die Management-Site verwenden.

Verfahren

- 1 Öffnen Sie die Management-Agent-Konfigurationsdatei im Verzeichnis `<vra-installation-dir>\Management Agent\VMware.IaaS.Management.Agent.exe.config`.

- 2 Notieren Sie sich den Wert des Attributs „id“ für das Element „agentConfiguration“.

```
<agentConfiguration id="0E22046B-9D71-4A2B-BB5D-70817F901B27">
```

Ersetzen des Management-Site-Zertifikats der vRealize Automation Appliance

Wenn das SSL-Zertifikat des Management-Site-Diensts abläuft oder Sie mit einem selbstsignierten Zertifikat begonnen haben und Site-Richtlinien ein anderes erfordern, können Sie das Zertifikat ersetzen.

Sie dürfen das vom vRealize Automation-Dienst auf Port 443 verwendete Zertifikat wiederverwenden oder ein anderes verwenden. Wenn Sie anfordern, dass ein neues von der Zertifizierungsstelle ausgestelltes Zertifikat ein vorhandenes Zertifikat aktualisiert, wird als Best Practice empfohlen, den allgemeinen Namen des vorhandenen Zertifikats wiederzuverwenden.

Hinweis Die vRealize Automation-Appliance verwendet lighttpd zum Ausführen der eigenen Management-Site. Sie sichern den Management-Site-Dienst auf Port 5480.

Voraussetzungen

- Das Zertifikat muss im PEM-Format vorliegen.
- Das Zertifikat muss die beiden folgenden Elemente nacheinander zusammen in einer Datei enthalten:
 - a RSA-Privatschlüssel
 - b Zertifikatskette
- Der private Schlüssel kann nicht verschlüsselt werden.
- Der standardmäßige Speicherort und Dateiname lautet `/opt/vmware/etc/lighttpd/server.pem`.

Weitere Informationen zum Exportieren eines Zertifikats und eines privaten Schlüssels aus einem Java-Keystore in eine PEM-Datei finden Sie unter [Extrahieren von Zertifikaten und privaten Schlüsseln](#).

Verfahren

- 1 Melden Sie sich unter Verwendung der Appliance-Konsole oder SSH an.
- 2 Sichern Sie Ihre aktuelle Zertifikatsdatei.

```
cp /opt/vmware/etc/lighttpd/server.pem /opt/vmware/etc/lighttpd/server.pem-bak
```

- 3 Kopieren Sie das neue Zertifikat in Ihre Appliance, indem Sie den Inhalt der Datei `/opt/vmware/etc/lighttpd/server.pem` mit den neuen Zertifikatinformationen ersetzen.
- 4 Führen Sie folgenden Befehl aus, um den lighttpd-Server neu zu starten.


```
service vami-lighttpd restart
```
- 5 Führen Sie den folgenden Befehl aus, um den haproxy-Dienst neu zu starten.


```
service haproxy restart
```
- 6 Melden Sie sich bei der Verwaltungskonsole an und überprüfen Sie, ob das Zertifikat ersetzt wurde. Möglicherweise müssen Sie Ihren Browser neu starten.

Nächste Schritte

Aktualisieren Sie alle Management-Agents, damit das neue Zertifikat erkannt wird.

Bei verteilten Bereitstellungen können Sie Management-Agents manuell oder automatisch aktualisieren. Für Minimalinstallationen müssen Sie die Agents manuell aktualisieren.

- Weitere Informationen zur automatischen Aktualisierung finden Sie unter [Automatisches Aktualisieren von Management-Agents in einer verteilten Umgebung zur Erkennung eines Management-Site-Zertifikats der vRealize Automation Appliance](#).
- Weitere Informationen zur manuellen Aktualisierung finden Sie unter [Manuelles Aktualisieren der Zertifikatserkennung für Management-Agents](#).

Aktualisieren der Zertifikatserkennung für Management-Agents

Nach dem Ersetzen eines Management-Site-Zertifikats einer vRealize Automation-Appliance müssen Sie zur Erkennung des neuen Zertifikats alle Management-Agents aktualisieren, um eine vertrauenswürdige Kommunikation zwischen der Management-Site der virtuellen Appliance und den Management-Agents auf den IaaS-Hosts wiederherzustellen.

Jeder IaaS-Host führt einen Management-Agent aus und jeder Management-Agent muss aktualisiert werden. Minimalbereitstellungen müssen manuell aktualisiert werden, während verteilte Bereitstellungen manuell oder unter Verwendung eines automatisierten Prozesses aktualisiert werden können.

■ [Manuelles Aktualisieren der Zertifikatserkennung für Management-Agents](#)

Nach dem Ersetzen eines Management-Site-Zertifikats einer vRealize Automation-Appliance müssen Sie zur Erkennung des neuen Zertifikats die Management-Agents manuell aktualisieren, um eine vertrauenswürdige Kommunikation zwischen der Management-Site der virtuellen Appliance und den Management-Agents auf den IaaS-Hosts wiederherzustellen.

■ [Automatisches Aktualisieren von Management-Agents in einer verteilten Umgebung zur Erkennung eines Management-Site-Zertifikats der vRealize Automation Appliance](#)

Nachdem das Management-Site-Zertifikat in einer Hochverfügbarkeitsbereitstellung aktualisiert wurde, muss die Management-Agent-Konfiguration ebenfalls aktualisiert werden, um das neue Zertifikat zu erkennen und die vertrauenswürdige Kommunikation wiederherzustellen.

Manuelles Aktualisieren der Zertifikatserkennung für Management-Agents

Nach dem Ersetzen eines Management-Site-Zertifikats einer vRealize Automation-Appliance müssen Sie zur Erkennung des neuen Zertifikats die Management-Agents manuell aktualisieren, um eine vertrauenswürdige Kommunikation zwischen der Management-Site der virtuellen Appliance und den Management-Agents auf den IaaS-Hosts wiederherzustellen.

Führen Sie diese Schritte für jeden Management-Agent in Ihrer Bereitstellung aus, nachdem Sie ein Zertifikat für die Management-Site der vRealize Automation-Appliance ersetzt haben.

Bei verteilten Bereitstellungen können Sie Management-Agents manuell oder automatisch aktualisieren. Weitere Informationen zur automatischen Aktualisierung finden Sie unter [Automatisches Aktualisieren von Management-Agents in einer verteilten Umgebung zur Erkennung eines Management-Site-Zertifikats der vRealize Automation Appliance](#).

Voraussetzungen

Rufen Sie die SHA1-Fingerabdrücke des neuen Management-Site-Zertifikats der vRealize Automation-Appliance ab.

Verfahren

- 1 Stoppen Sie den Management-Agent-Dienst von VMware vCloud Automation Center.
- 2 Navigieren Sie zur Management-Agent-Konfigurationsdatei, die sich unter `[vcac_installation_folder]\Management Agent\VMware.IaaS.Management.Agent.exe.Config` befindet, in der Regel `C:\Programme (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`.
- 3 Öffnen Sie die Datei zur Bearbeitung und suchen Sie die Endpoint-Konfigurationseinstellungen für das alte Management-Site-Zertifikat. Dieses können Sie an der Endpoint-Adresse erkennen.

Beispiel:

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="D1542471C30A9CE694A512C5F0F19E45E6FA32E6" />
  </managementEndpoints>
</agentConfiguration>
```

- 4 Ändern Sie den Fingerabdruck in den SHA1-Fingerabdruck des neuen Zertifikats um.

Beispiel:

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="8598B073359BAE7597F04D988AD2F083259F1201" />
  </managementEndpoints>
</agentConfiguration>
```

- 5 Starten Sie den Management-Agent-Dienst von VMware vCloud Automation Center.
- 6 Melden Sie sich bei der Management-Site der virtuellen Appliance an und wählen Sie die Registerkarte **Cluster** aus.
- 7 Überprüfen Sie die Informationstabelle „Verteilte Bereitstellung“, um sicherzustellen, dass der IaaS-Server die virtuelle Appliance kürzlich kontaktiert hat. Dies bestätigt, dass das Update erfolgreich war.

Automatisches Aktualisieren von Management-Agents in einer verteilten Umgebung zur Erkennung eines Management-Site-Zertifikats der vRealize Automation Appliance

Nachdem das Management-Site-Zertifikat in einer Hochverfügbarkeitsbereitstellung aktualisiert wurde, muss die Management-Agent-Konfiguration ebenfalls aktualisiert werden, um das neue Zertifikat zu erkennen und die vertrauenswürdige Kommunikation wiederherzustellen.

Sie können die Informationen zum Management-Site-Zertifikat der vRealize Automation-Appliance für verteilte Systeme manuell oder automatisch aktualisieren. Informationen zum manuellen Update von Management-Agents finden Sie unter [Manuelles Aktualisieren der Zertifikatserkennung für Management-Agents](#).

Verwenden Sie dieses Verfahren für die automatische Aktualisierung von Zertifikatsinformationen.

Verfahren

- 1 Wenn Management-Agents ausgeführt werden, ersetzen Sie das Zertifikat auf einer einzelnen Management-Site der vRealize Automation-Appliance in Ihrer Umgebung.
- 2 Warten Sie 15 Minuten, bis der Management-Agent mit dem neuen Management-Site-Zertifikat der vRealize Automation-Appliance synchronisiert wurde.
- 3 Ersetzen Sie die Zertifikate auf anderen Management-Sites der vRealize Automation-Appliance in Ihrer Bereitstellung.

Management-Agents werden automatisch mit den Informationen des neuen Zertifikats aktualisiert.

Ersetzen eines Management-Agent-Zertifikats

Der Systemadministrator kann das Management-Agent-Zertifikat ersetzen, wenn es abläuft, oder ein selbstsigniertes Zertifikat durch ein von einer Zertifizierungsstelle ausgestelltes Zertifikat ersetzen.

Jeder IaaS-Host führt seinen eigenen Management-Agent aus. Wiederholen Sie diese Vorgehensweise auf jedem IaaS-Knoten, dessen Management-Agent Sie aktualisieren möchten.

Voraussetzungen

- Kopieren Sie vor dem Entfernen des Datensatzes den Management-Agent-Bezeichner in der Spalte mit der Knoten-ID. Sie verwenden diesen Bezeichner bei der Erstellung und Registrierung des neuen Management-Agent-Zertifikats.
- Wenn Sie ein neues Zertifikat anfordern, stellen Sie sicher, dass das CN-Attribut (Common Name, allgemeiner Name) im Zertifikat-Betrefffeld für das neue Zertifikat im folgenden Format eingegeben wird:

```
VMware Management Agent 00000000-0000-0000-0000-000000000000
```

Verwenden Sie die Zeichenfolge VMware Management Agent, gefolgt von einem einzelnen Leerzeichen und der GUID für den Management-Agent im angezeigten numerischen Format.

Verfahren

- 1 Beenden Sie den Management-Agent-Dienst im Windows-Dienste-Snap-In.
 - a Klicken Sie auf der Windows-Maschine auf **Starten**.
 - b Geben Sie in das Suchfeld von Windows **services.msc** ein und drücken Sie die Eingabetaste.
 - c Klicken Sie mit der rechten Maustaste auf **VMware vCloud Automation Center Management Agent** und anschließend zum Beenden des Dienstes auf **Beenden**.
- 2 Entfernen Sie das aktuelle Zertifikat von der Maschine. Informationen zum Verwalten von Zertifikaten auf Windows Server 2008 R2 finden Sie im Knowledge Base-Artikel von Microsoft unter <http://technet.microsoft.com/en-us/library/cc772354.aspx> oder im Wiki-Artikel von Microsoft unter <http://social.technet.microsoft.com/wiki/contents/articles/2167.how-to-use-the-certificates-console.aspx>.
 - a Öffnen Sie die Microsoft-Verwaltungskonsole, indem Sie den Befehl **mmc.exe** eingeben.
 - b Drücken Sie die Tastenkombination STRG+M, um ein neues Snap-In in der Konsole hinzuzufügen, oder wählen Sie die entsprechende Option im Dropdown-Menü „Datei“ aus.
 - c Wählen Sie **Zertifikate** aus und klicken Sie auf **Hinzufügen**.
 - d Wählen Sie **Computerkonto** aus und klicken Sie auf **Weiter**.
 - e Wählen Sie **Lokaler Computer: (Der Computer, auf dem diese Konsole ausgeführt wird)** aus.
 - f Klicken Sie auf **OK**.
 - g Erweitern Sie **Zertifikate (Lokaler Computer)** auf der linken Seite der Konsole.
 - h Erweitern Sie **Privat** und wählen Sie den Ordner für Zertifikate aus.
 - i Wählen Sie das aktuelle Management-Agent-Zertifikat aus und klicken Sie auf **Löschen**.
 - j Klicken Sie auf **Ja**, um die Löschung zu bestätigen.
- 3 Importieren Sie das neu erstellte Zertifikat in den lokalen Speicher `computer.personal` oder importieren Sie nichts, wenn Sie möchten, dass das System automatisch ein neues selbstsigniertes Zertifikat erstellt.

- 4 Registrieren Sie das Management-Agent-Zertifikat auf der Verwaltungswebseite der vRealize Automation-Appliance.

- a Öffnen Sie eine Eingabeaufforderung als Administrator und navigieren Sie zu dem Cafe-Verzeichnis auf der Maschine, auf der der Management-Agent installiert ist, unter `<vra-installation-dir>\Management Agent\Tools\Cafe`, normalerweise `C:\Programme (x86)\VMware\vCAC\Management Agent\Tools\Cafe`.
- b Geben Sie den `Vcac-Config.exe RegisterNode`-Befehl mit Optionen zum Registrieren des Management-Agent-Bezeichners und -Zertifikats in einem Schritt ein. Fügen Sie den zuvor aufgezeichneten Management-Agent-Bezeichner als Wert für die Option `-nd` hinzu.

Tabelle 1-3. Erforderliche Optionen und Argumente für Vcac-Config.exe-RegisterNode

Option	Argument	Hinweise
-vamih	vra-vd-hostname.domain.name:5480	Die URL des Hosts der Verwaltungswebseite, einschließlich einer Portangabe.
-cu	root	Der Benutzername, der der Root-Benutzer sein muss.
-cp	Kennwort	Kennwort für den Root-Benutzer als eine Zeichenfolge in Anführungszeichen.
-hn	machine-hostname.domain.name	Der Maschinenname des Management-Agent-Hosts, einschließlich Domäneninformationen. Dieser Wert muss mit dem Hostnamen übereinstimmen, mit dem der aktuelle Knoten in der vRealize Automation-Appliance registriert ist. Kann zusammen mit der oben angegebenen Option 1 für die Knoten-ID oder in der VAMI-Tabelle „Info zur verteilten Bereitstellung“ angezeigt werden. Wenn es nicht derselbe Wert ist, wird beim Ausführen des Befehls ein Fehler gemeldet, der so oder ähnlich lautet: „Fehler: Doppelte Knoten-ID 00000000-0000-0000-0000-00000000 kann nicht hinzugefügt werden“.
-nd	00000000-0000-0000-0000-000000000000 0	Management-Agent-Bezeichner.
-tp	000000000000000000000000000000000000 00000000	Fingerabdruck des SSL-Zertifikats des Hosts der Verwaltungswebseite, wie im Parameter -vamih definiert.

Das folgende Beispiel zeigt das Befehlsformat:

```
Vcac-Config.exe RegisterNode -v -vamih "vra-vam-hostname.domain.name:5480"  
-cu "root" -cp "password" -hn "machine-hostname.domain.name"  
-nd "000000000-0000-0000-0000-000000000000"  
-tp "000000000000000000000000000000000000000000000000"
```

5 Starten Sie den Management Agent neu.

Beispiel: Befehl zum Registrieren eines Management-Agent-Zertifikats

```
Vcac-Config.exe RegisterNode -v -vamih "vra-va.eng.mycompany:5480" -cu "root" -cp
"secret" -hn "iaas.eng.mycompany" -nd "C816CFBX-4830-4FD2-8951-C17429CEA291" -tp
"70928851D5B72B206E4B1CF9F6ED953EE1103DED"
```

Ändern der Abrufmethode für Zertifikate

Befinden sich im OU-Abschnitt des IaaS-Zertifikats Kommas, treten in den Manager Service-Protokolldateien unter Umständen STOMP WebSocket-Fehler auf. Darüber hinaus könnte das Bereitstellen virtueller Maschinen fehlschlagen. Sie können die Kommas entfernen oder die Abrufmethode von WebSocket in HTTP ändern.

Führen Sie zum Ändern der Abrufmethode die folgenden Schritte aus.

Verfahren

- 1 Öffnen Sie die folgende Datei in einem Texteditor.

C:\Programme (x86)\VMware\VMware vCAC\Server\Manager Service.exe.config

- 2** Fügen Sie die folgenden Zeilen zum Abschnitt `<appSettings>` hinzu.

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```

- ### 3 Speichern und schließen Sie Manager Service.exe.config.

- 4** Starten Sie den Manager Service neu.

Ergebnisse

Weitere Informationen zum Manager Service finden Sie unter *Installieren von vRealize Automation*.

Verwalten der vRealize Automation Postgres-Appliance-Datenbank

vRealize Automation benötigt die Appliance-Datenbank für den Systembetrieb. Sie können die Appliance-Datenbank über die Virtual Appliance Management Interface (VAMI) der vRealize Automation-Appliance verwalten.

Hinweis Diese Informationen gelten nur für Bereitstellungen, in denen eine eingebettete Appliance-Datenbank verwendet wird. Sie gelten nicht für Bereitstellungen mit einer externen Postgres-Datenbank.

Sie können die Datenbank als Einzelknoten oder mit mehreren Knoten für Hochverfügbarkeit per Failover konfigurieren. Das Installationsprogramm von vRealize Automation enthält einen Datenbankknoten auf jeder Installation von vRealize Automation-Appliance. Wenn Sie drei Instanzen einer vRealize Automation-Appliance installieren, erhalten Sie also drei Datenbankknoten. Automatisches Failover ist in anwendbaren Bereitstellungen implementiert. Die Appliance-Datenbank benötigt keine Wartung, es sei denn, eine Maschinenkonfiguration wird geändert oder Sie setzen in einer geclusterten Konfiguration einen anderen Knoten als primären Knoten ein.

Hinweis Die geclusterte Datenbankkonfiguration wird automatisch eingerichtet, wenn Sie eine virtuelle Appliance während des Cluster-Verknüpfungsvorgangs mit dem Cluster verknüpfen. Der Datenbankcluster ist nicht direkt abhängig vom virtuellen Appliance-Cluster. So kann z. B. eine virtuelle Maschine, die einem Cluster hinzugefügt wurde, selbst dann normal betrieben werden, wenn die eingebettete Appliance-Datenbank nicht gestartet wurde oder ausgefallen ist.

Für Hochverfügbarkeit verwendet vRealize Automation das PostgreSQLprimary-replica-Modell, um die Datenreplikation zu unterstützen. Dies bedeutet, dass alle Datenbankknoten in einem Cluster mit einem führenden Knoten, der als der primäre Knoten bezeichnet wird, und mit mehreren replizierenden Knoten, die als Replikate bezeichnet werden, arbeiten. Der primäre Knoten verarbeitet alle Datenbankanforderungen, und die Replikatknoten streamen Transaktionen vom primären Knoten lokal und geben diese lokal wieder.

Eine Clusterkonfiguration enthält einen primären Knoten und mindestens einen Replikatknoten. Der primäre Knoten ist der vRealize Automation-Appliance-Knoten mit der primären Datenbank, der die Systemfunktionalität unterstützt. Replikatknoten enthalten Kopien der Datenbank, die in den Dienst gezogen werden können, wenn der primäre Knoten fehlschlägt.

Es stehen mehrere Optionen für hochverfügbare Appliance-Datenbanken zur Verfügung. Die Auswahl des Replikationsmodus ist die wichtigste Option für die Datenbankkonfiguration. Der Replikationsmodus bestimmt, wie Ihre vRealize Automation-Bereitstellung die Datenintegrität aufrechterhält, und legt in Hochverfügbarkeitskonfigurationen fest, wie das Failover erfolgt, wenn der primäre Knoten fehlschlägt. Zwei Replikationsmodi sind verfügbar: synchron und asynchron.

Beide Replikationsmodi unterstützen Datenbank-Failover und haben Vor- und Nachteile. Zur Unterstützung eines hochverfügbaren Datenbank-Failovers sind für den asynchronen Modus zwei Knoten erforderlich, während für den synchronen Modus drei Knoten erforderlich sind. Der synchrone Modus aktiviert das automatische Failover.

Replikationsmodus	Vorteile	Nachteile
Synchron	<ul style="list-style-type: none"> ■ Minimiert die Möglichkeit des Datenverlusts. ■ Ruft das automatische Failover auf. 	<ul style="list-style-type: none"> ■ Kann die Systemleistung beeinträchtigen. ■ Erfordert drei Knoten.
Asynchron	<ul style="list-style-type: none"> ■ Erfordert nur zwei Knoten. ■ Beeinträchtigt die Systemleistung weniger als der synchrone Modus. 	Im Hinblick auf Datenverlust nicht so robust wie der asynchrone Modus.

vRealize Automation unterstützt beide Modi, wird aber standardmäßig im asynchronen Modus betrieben und bietet nur dann Hochverfügbarkeit, wenn mindestens zwei Appliance-Datenbankknoten vorhanden sind. Über die Registerkarte **Cluster** auf der Virtual Appliance Management Interface können Sie zwischen den Synchronisierungsmodi wechseln und Datenbankknoten nach Bedarf hinzufügen.

Im synchronen Modus ruft vRealize Automation das automatische Failover auf.

Wenn Sie mit einem Knoten in einer Konfiguration ohne Hochverfügbarkeit beginnen, können Sie später nach Bedarf weitere Knoten hinzufügen, um die Hochverfügbarkeit zu verbessern. Wenn Sie über die erforderliche Hardware verfügen und maximalen Schutz gegen Datenverlust benötigen, können Sie die Bereitstellung für den Betrieb im synchronen Modus konfigurieren.

Appliance-Datenbank-Failover

In einer Hochverfügbarkeitskonfiguration streamt der primäre Knoten konstant Transaktionen an die Replikatserver. Wenn der primäre Knoten ausfällt, ist das aktive und einsatzfähige Replikat bereit, mit schreibgeschützten Anforderungen fortzufahren. Wenn der neue primäre Knoten entweder manuell oder automatisch heraufgestuft wird, werden alle anstehenden Anforderungen zu ihm verschoben.

Konfigurieren der Appliance-Datenbank

Auf der Seite der VAMI-Datenbank (Virtual Appliance Management Interface) können Sie die Konfiguration der Appliance-Datenbank überwachen oder aktualisieren. Sie können diese Option auch verwenden, um die Bezeichnung des primären Knotens und den von der Datenbank verwendeten Synchronisierungsmodus zu ändern.

Die Appliance-Datenbank wird während der vRealize Automation-Systeminstallation installiert und konfiguriert. Sie können die Konfiguration aber über die Registerkarte **Datenbank** der Virtual Appliance Management Interface (VAMI) überwachen und ändern.

Das Textfeld **Verbindungsstatus** gibt an, ob die Datenbank mit dem vRealize Automation-System verbunden ist und korrekt funktioniert.

Wenn Ihre Appliance-Datenbank mehrere Knoten zur Failover-Unterstützung verwendet, werden in der Tabelle unten auf der Seite die Knoten und ihr Status angezeigt und angegeben, welcher Knoten der primäre Knoten ist. Das Textfeld **Replikationsmodus** zeigt den aktuell konfigurierten Betriebsmodus des Systems (synchron oder asynchron) an. Über diese Seite können Sie die Konfiguration der Appliance-Datenbank aktualisieren.

Die Spalte „Synchronisierungsstatus*“ in der Datenbankknotentabelle enthält die Synchronisierungsmethode für den Cluster. Diese Spalte zeigt zusammen mit der Spalte „Status“ den Status der Clusterknoten an. Der mögliche Status hängt davon ab, ob der Cluster asynchrone oder synchrone Replikation verwendet.

Tabelle 1-4. Synchronisierungsstatus für die Replikationsmodi der Appliance-Datenbank

Modus	Synchronisierungsstatusmeldung
Synchrone Replikation	Primärer Knoten – kein Status Replikatknoten – wird synchronisiert Andere Knoten – potenziell
Asynchrone Replikation	Primärer Knoten – kein Status Andere Knoten – potenziell

Die Spalte „Gültig“ gibt an, ob Replikate mit dem primären Knoten synchronisiert sind. Der primäre Knoten ist immer gültig.

Die Spalte „Priorität“ zeigt die Position der Replikatknoten in Beziehung zum primären Knoten. Der primäre Knoten hat keinen Prioritätswert. Wählen Sie zum Heraufstufen eines Replikatknotens zum primären Knoten den Knoten mit dem niedrigsten Prioritätswert aus.

Im synchronen Modus ruft vRealize Automation das automatische Failover auf. Sollte der primäre Knoten ausfallen, wird der nächste verfügbare Replikatknoten automatisch zum neuen primären Knoten. Der Failover-Vorgang dauert auf einer typischen vRealize Automation-Bereitstellung etwa 10 bis 30 Sekunden.

Voraussetzungen

- Installieren und konfigurieren Sie vRealize Automation gemäß der entsprechenden Anleitung in *Installieren von vRealize Automation*.
- Melden Sie sich bei der Verwaltung der vRealize Automation-Appliance als **Root**-Benutzer mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance verwendet haben.
- Konfigurieren Sie einen geeigneten eingebetteten Postgres-Appliance-Datenbankcluster als Teil der vRealize Automation-Bereitstellung.

Verfahren

- 1 Wählen Sie in der Virtual Appliance Management Interface **vRA-Einstellungen > Datenbank** aus.

- 2 Wenn Ihre Datenbank mehrere Konten verwendet, überprüfen Sie die Tabelle unten auf der Seite und vergewissern Sie sich, dass das System korrekt läuft.
 - Vergewissern Sie sich, dass alle Knoten aufgelistet sind.
 - Stellen Sie sicher, dass der entsprechende Knoten der ausgewiesene primäre Knoten ist.

Hinweis Klicken Sie nur dann auf **Synchronisierungsmodus**, um den Synchronisierungsmodus der Datenbank zu ändern, wenn Sie wissen, dass Ihre Daten sicher sind. Wird der Synchronisierungsmodus ohne entsprechende Vorbereitung geändert, kann das zu Datenverlust führen.

- 3 Um einen der Knoten zum primären Knoten heraufzustufen, klicken Sie in der betreffenden Spalte auf **Heraufstufen**.
- 4 Klicken Sie auf **Einstellungen speichern**, um die Konfiguration zu speichern, wenn Sie Änderungen vorgenommen haben.

Szenarien für das automatische Failover für die aus drei Knoten bestehende Appliance-Datenbank

Es gibt mehrere Hochverfügbarkeits-Failover-Szenarien für Appliance-Datenbanken, und das Verhalten von vRealize Automation hängt von der Konfiguration der Appliance-Datenbank und der Anzahl der Knoten ab, die ausfallen.

Fehlerszenarien einzelner Knoten

Wenn einer der drei Knoten ausfällt, wird ein automatisches Failover für vRealize Automation ausgelöst. Es können keine zusätzlichen automatischen Failover-Vorgänge durchgeführt werden, bis alle drei Knoten wiederhergestellt sind.

Die folgende Tabelle beschreibt das Verhalten und die Aktionen im Zusammenhang mit einem Ausfall eines primären Knotens in einer Hochverfügbarkeitsbereitstellung.

Tabelle 1-5. Der primäre Knoten schlägt fehl

Erwartetes Verhalten	<ul style="list-style-type: none"> ■ Der konfigurierte Synchronisierungsreplikatknoten wird zum primären Knoten und übernimmt automatisch die Funktionalität der Appliance-Datenbank. ■ Das potenzielle Synchronisierungsreplikat wird der Synchronisierungs-Standby-Knoten. ■ Die vRealize Automation-Bereitstellung funktioniert im Nur-Lese-Modus, bis das automatische Failover abgeschlossen ist.
Weitere Schritte	<ul style="list-style-type: none"> ■ Wenn der vorherige primäre Knoten wiederhergestellt wird, wird er von der Failover-Agent-Reparaturlogik automatisch als Replikat zurückgesetzt. Es sind keine manuellen Schritte erforderlich. ■ Wenn der vorherige primäre Knoten nicht wiederhergestellt werden kann, versetzen Sie die Appliance-Datenbank manuell in den asynchronen Modus.

Die folgende Tabelle beschreibt das Verhalten und die Aktionen im Zusammenhang mit einem Ausfall eines Synchronisierungsreplikatknotens in einer Hochverfügbarkeitsbereitstellung.

Tabelle 1-6. Das Synchronisierungsreplikat schlägt fehl

Erwartetes Verhalten	<ul style="list-style-type: none"> ■ Die vRealize Automation-Bereitstellung erfolgt ohne Ausfall. Es wird eine Verzögerung von ein paar Sekunden für Datenbankabfragen geben, bis das potentielle Replikat das neue Synchronisierungsreplikat wird. Die Appliance-Datenbank führt diese Aktion automatisch durch.
Weitere Schritte	<ul style="list-style-type: none"> ■ Wenn das frühere Synchronisierungsreplikat online geschaltet wird, wird es automatisch zu einem potenziellen Replikat. Es sind keine manuellen Schritte erforderlich. ■ Wenn das frühere Synchronisierungsreplikat nicht repariert werden kann, setzen Sie die Appliance-Datenbank manuell in den asynchronen Modus.

Die folgende Tabelle beschreibt das Verhalten und die Aktionen im Zusammenhang mit einem Ausfall eines primären Knotens in einer Hochverfügbarkeitsbereitstellung.

Tabelle 1-7. Das potenzielle Replikat schlägt fehl

Erwartetes Verhalten	Kein Ausfall während der Bereitstellung.
Weitere Schritte	<ul style="list-style-type: none"> ■ Wenn das frühere potenzielle Replikat online geschaltet wird, wird es automatisch zu einem potenziellen Replikat. Es sind keine manuellen Schritte erforderlich. ■ Wenn das frühere potenzielle Replikat nicht repariert werden kann, setzen Sie die Appliance-Datenbank manuell in den asynchronen Modus.

Fehlerszenarien mit zwei Knoten

Wenn zwei der drei Knoten gleichzeitig ausfallen, wechselt vRealize Automation in den Nur-Lese-Modus, bis eine manuelle Reparatur durchgeführt wird.

Die folgende Tabelle beschreibt das Verhalten und die Aktionen im Zusammenhang mit einem Ausfall eines primären Knotens und eines potenziellen Replikatknotens in einer Hochverfügbarkeitsbereitstellung.

Tabelle 1-8. Der primäre Knoten und das potenzielle Replikat schlagen fehl

Erwartetes Verhalten	<ul style="list-style-type: none"> ■ Das Synchronisierungsreplikat wird nicht automatisch zum primären Knoten heraufgestuft. vRealize Automation funktioniert im schreibgeschützten Modus, da es in der Lage ist, schreibgeschützte Transaktionen bis zur Durchführung einer manuellen Heraufstufung zu verarbeiten.
Weitere Schritte	<ul style="list-style-type: none"> ■ Manuelle Heraufstufung ist erforderlich. Setzen Sie die Appliance-Datenbank in den asynchronen Modus. ■ Wenn der primäre Knoten und das potenzielle Replikat wiederhergestellt sind, stellen Sie sie manuell so ein, dass sie mit dem neuen primären Knoten synchronisiert werden. An diesem Punkt können Sie vRealize Automation wieder in den synchronen Modus versetzen. ■ Wenn zwei von drei Knoten gleichzeitig ausgefallen sind, wird vRealize Automation in den Nur-Lese-Modus versetzt, bis Sie eine manuelle Reparatur durchführen. Wenn nur ein Datenbankknoten verfügbar ist, versetzen Sie Ihre Bereitstellung in den asynchronen Modus.

Die folgende Tabelle beschreibt das Verhalten und die Aktionen im Zusammenhang mit einem Ausfall eines Synchronisierungsreplikatknotens und eines potenziellen Knotens in einer Hochverfügbarkeitsbereitstellung.

Tabelle 1-9. Das Synchronisierungsreplikat und das potenzielle Replikat schlagen fehl

Erwartetes Verhalten	<ul style="list-style-type: none"> ■ vRealize Automation funktioniert im schreibgeschützten Modus, da es in der Lage ist, schreibgeschützte Transaktionen bis zur Durchführung einer manuellen Reparatur zu verarbeiten.
Weitere Schritte	<ul style="list-style-type: none"> ■ Manuelle Heraufstufung ist erforderlich. Setzen Sie die Appliance-Datenbank in den asynchronen Modus. ■ Wenn das Synchronisierungsreplikat und das potenzielle Replikat wiederhergestellt werden, sollten sie manuell zurückgesetzt werden, um mit dem primären Knoten synchronisiert zu werden. An diesem Punkt können Sie vRealize Automation wieder in den synchronen Modus versetzen. ■ Wenn zwei von drei Knoten gleichzeitig ausgefallen sind, wird vRealize Automation in den Nur-Lese-Modus versetzt, bis Sie eine manuelle Reparatur durchführen. Wenn nur ein Datenbankknoten verfügbar ist, versetzen Sie Ihre Bereitstellung in den asynchronen Modus.

Verknüpfungsfehler zwischen Knoten

Wenn bei einer verteilten Bereitstellung ein Verknüpfungsfehler zwischen Knoten auftritt, versucht der automatische Failover-Agent, die Konfiguration zu reparieren.

Die folgende Tabelle beschreibt das Verhalten und die Aktionen im Zusammenhang mit einem Verbindungsausfall zwischen zwei Sites in einer Hochverfügbarkeitsinstallation mit der angegebenen Konfiguration, wenn alle Knoten online bleiben

Site A: Primärer Knoten und potenzielles Replikat

Site B: Synchronisierungsreplikat

Tabelle 1-10. Verknüpfungsfehler zwischen zwei Sites, wenn alle Knoten aktiv und online bleiben

Erwartetes Verhalten	Keine Ausfallzeit für die vRealize Automation-Bereitstellung. Das potenzielle Replikat wird automatisch zum Synchronisierungsreplikat.
Weitere Schritte	Es sind keine manuellen Schritte erforderlich.

Die folgende Tabelle beschreibt das Verhalten und die Aktionen im Zusammenhang mit einem Verbindungsausfall zwischen zwei Sites in einer Hochverfügbarkeitsinstallation mit der angegebenen Konfiguration, wenn alle Knoten online bleiben

Site A: Primärer Knoten

Site B: Synchronisierungsreplikat und potenzielle Replikat

Tabelle 1-11. Verknüpfungsfehler zwischen zwei Sites, wenn alle Knoten aktiv und online bleiben – alternative Konfiguration

Erwartetes Verhalten	Synchronisierungsreplikat wird zum primären Knoten und übernimmt automatisch die Funktionalität der Appliance-Datenbank. Der Agent für automatisches Failover stuft das potenzielle Replikat hoch, um das neue Synchronisierungsreplikat zu werden. Die vRealize Automation-Bereitstellung erfolgt im Nur-Lese-Modus, bis diese Aktion abgeschlossen ist.
Weitere Schritte	Es sind keine manuellen Schritte erforderlich. Wenn die Verbindung wiederhergestellt wird, setzt der Agent für automatisches Failover den vorherigen primären Knoten als Replikat zurück.

Szenario: Durchführen eines manuellen Failovers der vRealize Automation Appliance-Datenbank

Falls es ein Problem mit der Postgres-Datenbank der vRealize Automation-Appliance gibt, führen Sie ein manuelles Failover auf einen Replikatknoten der vRealize Automation-Appliance im Cluster durch.

Führen Sie folgende Schritte aus, wenn die Postgres-Datenbank auf dem primären Knoten der vRealize Automation-Appliance ausfällt oder deren Ausführung beendet wird.

Hinweis Wenn ein Knoten in einen nicht ordnungsgemäßen Zustand wechselt, versuchen Sie nicht, dessen Verwaltungsschnittstelle der virtuellen Appliance für Vorgänge, einschließlich Failover, zu verwenden.

Voraussetzungen

- Konfigurieren Sie einen Cluster aus Knoten der vRealize Automation-Appliance. Jeder Knoten enthält eine Kopie des eingebetteten Postgres-Appliance-Datenbank.

Verfahren

- 1 Entfernen Sie die IP-Adresse des primären Knotens aus dem externen Lastausgleichsdienst.

- 2 Melden Sie sich bei der Verwaltungsschnittstelle der vRealize Automation-Appliance als Root-Benutzer an.

`https://vrealize-automation-appliance-FQDN:5480`

- 3 Wählen Sie **Cluster** aus.

- 4 Suchen Sie in der Liste der Datenbankknoten nach dem Replikatknoten mit der niedrigsten Priorität.

Replikatknoten werden aufsteigend nach Priorität aufgelistet.

- 5 Klicken Sie auf **Heraufstufen** und warten Sie, bis der Vorgang abgeschlossen ist.

Nach Abschluss wird der Replikatknoten als neuer primärer Knoten aufgelistet.

- 6 Beheben Sie Probleme mit dem vorherigen primären Knoten und fügen Sie ihn wieder zum Cluster hinzu:

- a Isolieren Sie den ehemaligen primären Knoten.

Trennen Sie den Knoten vom aktuellen Netzwerk. Dies ist das Netzwerk, das zu den verbleibenden Knoten der vRealize Automation-Appliance weiterleitet. Wählen Sie eine andere Netzwerkkarte für die Verwaltung oder nehmen Sie die Verwaltung direkt von der VM-Verwaltungskonsole aus vor.

- b Stellen Sie den vorherigen primären Knoten wieder her.

Starten Sie den Knoten, anderenfalls beheben Sie das Problem. Sie können zum Beispiel die virtuelle Maschine zurücksetzen, wenn sie nicht mehr reagiert.

- c Halten Sie als Root von einer Konsolensitzung aus den vpostgres-Dienst an.

```
service vpostgres stop
```

- d Fügen Sie den vorherigen primären Knoten wieder zum ursprünglichen Netzwerk hinzu. Dies ist das Netzwerk, das zu den anderen Knoten der vRealize Automation-Appliance weiterleitet.

- e Starten Sie als Root von einer Konsolensitzung aus den haproxy-Dienst neu.

```
service haproxy restart
```

- f Melden Sie sich bei der neuen Verwaltungsschnittstelle des primären Knotens der vRealize Automation-Appliance als Root-Benutzer an.

- g Wählen Sie **Cluster** aus.

- h Suchen Sie nach dem vorherigen primären Knoten und klicken Sie auf **Zurücksetzen**.

- i Wenn der vorherige primäre Knoten ordnungsgemäß zurückgesetzt wurde, starten Sie ihn neu.

- j Stellen Sie bei eingeschaltetem vorherigem primärem Knoten sicher, dass die folgenden Dienste ausgeführt werden.

```
haproxy horizon-workspace rabbitmq-server vami-lighttpd vcac-server vco-server
```

- k Fügen Sie den vorherigen primären Knoten erneut zum externen Lastausgleichsdienst hinzu.

Hinweis Wenn ein primärer Knoten, der zum Replikat herabgestuft wurde, nach wie vor als primärer Knoten aufgelistet wird, müssen Sie ihn zur Behebung des Problems möglicherweise manuell erneut dem Cluster hinzufügen.

Szenario: Durchführen eines Wartungsdatenbank-Failover

Als vRealize Automation-Systemadministrator müssen Sie einen Failover-Vorgang zur Appliance-Datenbankwartung durchführen.

In diesem Szenario wird davon ausgegangen, dass der aktuelle primäre Knoten aktiv ist und normal ausgeführt wird. Die Datenbank-Failover-Wartung besteht aus zwei Schritten: Wartung des primären Knotens und Wartung eines Replikatknotens. Wenn ein primärer Knoten ersetzt und zum Replikat wurde, müssen Sie eine Wartung ausführen, damit er bei Bedarf erneut als primärer Knoten eingesetzt werden kann.

Hinweis Stoppen Sie den HAProxy-Dienst auf der zutreffenden Hostmaschine nicht bzw. starten Sie ihn nicht neu, während Sie ein Wartungs-Failover durchführen.

Voraussetzungen

- vRealize Automation wird gemäß den Anweisungen im *Installieren von vRealize Automation* installiert und konfiguriert.
- Melden Sie sich bei der Verwaltung der vRealize Automation-Appliance als **Root**-Benutzer mit dem Kennwort an, das Sie bei der Bereitstellung der vRealize Automation-Appliance verwendet haben.
- Installieren und konfigurieren Sie einen entsprechenden eingebetteten Postgres-Appliance-Datenbankcluster.
- Wenn Ihre Datenbank den synchronen Replikationsmodus verwendet, vergewissern Sie sich, dass der Cluster drei aktive Knoten enthält.

Verfahren

- 1 Entfernen Sie die IP-Adresse des primären Knotens aus dem externen Lastausgleichsdienst.
- 2 Isolieren Sie den primären Knoten.

Trennen Sie den Knoten vom aktuellen Netzwerk. Dies sollte das Netzwerk sein, das an die verbleibenden vRealize Automation-Appliance-Knoten weiterleitet.
- 3 Wählen Sie eine andere Netzwerkkarte für die Verwaltung aus oder nehmen Sie die Verwaltung direkt über die Verwaltungsschnittstelle der virtuellen Appliance vor.
- 4 Wählen Sie auf der VAMI (Virtual Appliance Management Interface) **Cluster** aus.

- 5 Wählen Sie den Replikatknoten mit der niedrigsten Priorität für die Heraufstufung zum primären Knoten aus und klicken Sie auf **Heraufstufen**.

Replikatknoten werden aufsteigend nach Priorität aufgelistet.

Der bisherige primäre Knoten wird zum Replikatstatus herabgestuft, und der neue primäre Knoten wird heraufgestuft.

- 6 Führen Sie die entsprechende Replikatwartung durch.
- 7 Vergewissern Sie sich nach Abschluss der Wartung, dass die virtuelle Appliance mit Netzwerkonnektivität ausgeführt wird und dass ihr HAProxy-Dienst läuft.
 - a Melden Sie sich an der vRealize Automation-Verwaltungskonsolle als **root** an.
 - b Stellen Sie sicher, dass der Replikatknoten angepingt und nach Name aufgelöst werden kann sowie auf der Registerkarte „Virtual Appliance Management Interface-**Cluster**“ einen aktuellen Status aufweist.

- 8 Klicken Sie auf **Zurücksetzen** für den Replikatknoten.

Mit diesem Vorgang wird die Datenbank zurückgesetzt, sodass sie zum Replizieren des aktuellen primären Knotens konfiguriert wird und den Replikatknoten mit der neuesten haproxy-Konfiguration vom primären Knoten neu synchronisiert.

- 9 Nach dem erfolgreichen Zurücksetzen fügen Sie die Knoten-IP-Adresse der virtuellen Replikat-Appliance wieder zum IP-Adresspool des Lastausgleichsdiensts der externen virtuellen Appliance hinzu.
- 10 Stellen Sie sicher, dass der Replikatknoten in der Datenbanktabelle als fehlerfrei angezeigt wird, dass er angepingt und nach Name aufgelöst werden kann.

Nächste Schritte

Beheben Sie Probleme mit dem vorherigen primären Knoten und fügen Sie ihn wieder zum Cluster hinzu.

Manuelle Wiederherstellung der Appliance-Datenbank nach einem schwerwiegenden Fehler

Wenn die Appliance-Datenbank ausfällt und keine Datenbankknoten ausgeführt werden oder bei Ausfall des primären Knotens alle Replikatknoten nicht synchronisiert sind, gehen Sie wie folgt vor, um die Wiederherstellung der Datenbank zu versuchen.

Dieses Verfahren gilt für Situationen, in denen in einem Cluster im asynchronen Modus keine Datenbankknoten betriebsbereit sind. In diesem Szenario werden normalerweise auf der Seite der Virtual Appliance Management Interface (VAMI) Fehler ähnlich der folgenden angezeigt, wenn Sie versuchen, die Seite zu laden oder zu aktualisieren:

Fehler beim Initialisieren des Datenbankdiensts: JDBC-Verbindung für Transaktion konnte nicht geöffnet werden; verschachtelte Ausnahme ist org.postgresql.util.PSQLException: Der Verbindungsversuch ist fehlgeschlagen.

Verfahren

- 1 Versuchen Sie, die Datenbank mithilfe der Virtual Appliance Management Interface (VAMI) über einen der Datenbankknoten wiederherzustellen.
 - a Öffnen Sie, falls möglich, die Seite VAMI-**Cluster** (Virtual Appliance Management Interface) des Knotens mit dem aktuellsten Stand. Im Normalfall war dieser Knoten der primäre Knoten, bevor die Datenbank ausgefallen ist.
 - b Wenn die VAMI für den primären Knoten nicht geöffnet werden kann, versuchen Sie, sie für andere Replikatknoten zu öffnen.
 - c Wenn Sie einen Datenbankknoten mit einer funktionierenden Virtual Appliance Management Interface (VAMI) finden, versuchen Sie, ihn mithilfe eines manuellen Failovers wiederherzustellen.

Siehe [Szenario: Durchführen eines manuellen Failovers der vRealize Automation Appliance-Datenbank](#).
- 2 Wenn das Verfahren bei Schritt 1 fehlschlägt, starten Sie eine Shell-Sitzung und versuchen Sie, den Knoten mit dem neuesten Stand zu ermitteln. Starten Sie eine Shell-Sitzung mit Verbindung zu allen verfügbaren Clusterknoten und versuchen Sie, deren Datenbanken zu starten, indem Sie den folgenden Shell-Befehl ausführen: `service vpostgres start`
- 3 Gehen Sie für jeden Knoten, auf dem eine lokale Datenbank ausgeführt wird, wie folgt vor, um den Knoten mit dem neuesten Stand zu ermitteln.
 - a Führen Sie den folgenden Befehl aus, um den Knoten mit dem neuesten Stand zu ermitteln. Wenn der Befehl `f` zurückgibt, handelt es sich um den Knoten mit dem neuesten Stand und Sie können mit Schritt 4 fortfahren.

```
su - postgres
psql vcac
vcac=# select pg_is_in_recovery();
pg_is_in_recovery
```

- Wenn dieser Befehl ein `f` zurückgibt, weist dieser Knoten den neuesten Stand auf.
- Wenn der Knoten ein `t` zurückgibt, führen Sie den folgenden Befehl auf dem Knoten aus:

```
SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location() as
replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
```

Dieser Befehl sollte ein Ergebnis ähnlich dem nachfolgend dargestellten zurückgeben.

```
vcac=# SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location()
as replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
 receive_loc | replay_loc | replay_timestamp
-----+-----+-----
 0/20000000 | 0/203228A0 | 1491577215.68858
(1 row)
```

- 4 Vergleichen Sie die Ergebnisse aller Knoten, um zu ermitteln, welcher von ihnen den neusten Stand aufweist.

Wählen Sie den Knoten mit dem größten Wert in der Spalte `receive_loc` aus. Bei gleichen Werten wählen Sie den Knoten mit dem größten Wert in der Spalte `replay_loc` aus, und wenn auch hier sich mehrere Knoten denselben größten Wert teilen, wählen Sie unter diesen den Knoten mit dem größten Wert in der Spalte `replay_timestamp` aus.

- 5 Führen Sie den folgenden Befehl auf dem Knoten mit dem neusten Stand aus: `vcac-vami psql-promote-master -force`
- 6 Öffnen Sie die Datei `/etc/haproxy/conf.d/10-psql.cfg` in einem Texteditor und aktualisieren Sie die folgende Zeile

```
server masterserver sc-rdops-vm06-dhcp-170-156.eng.vmware.com:5432 check on-marked-up shutdown-backup-sessions
```

Unter Verwendung des FQDN des aktuellen Knotens wie folgt:

```
server masterserver current-node-fqdn:5432 check on-marked-up shutdown-backup-sessions
```

- 7 Speichern Sie die Datei.
- 8 Führen Sie den Befehl `service haproxy restart` aus.
- 9 Öffnen Sie die Seite VAMI-**Cluster** für den neuesten Knoten.
Dieser Knoten sollte als primärer Knoten mit den anderen Knoten als ungültige Replikate angezeigt werden. Darüber hinaus ist die Schaltfläche **Zurücksetzen** für die Replikate aktiviert.
- 10 Klicken Sie der Reihe nach für jedes Replikat auf **Zurücksetzen**, bis der Cluster-Zustand wiederhergestellt ist.

Backup und Wiederherstellung für vRealize Automation-Installationen

Um Systemausfallzeiten und Datenverlust bei Fehlern zu minimieren, sichern Administratoren regelmäßig die gesamte vRealize Automation-Installation. Wenn Ihr System ausfällt, können Sie es wiederherstellen, indem Sie das letzte fehlerfreie Backup wiederherstellen und einige Komponenten neu installieren.

Informationen zum Sichern und Wiederherstellen von vRealize Automation finden Sie in den folgenden Themen in der [Dokumentation zu vRealize Suite](#):

- vRealize Automation-Vorbereitungen für die Datensicherung
- Systemwiederherstellung von vRealize Automation

Programm zur Verbesserung der Kundenzufriedenheit

Dieses Produkt wird im Rahmen des Programms zur Verbesserung der Kundenzufriedenheit (Customer Experience Improvement Program, CEIP) von VMware berücksichtigt. Das Programm zur Verbesserung der Kundenzufriedenheit liefert VMware Informationen, die es VMware ermöglichen, Produkte und Dienste zu verbessern, Probleme zu beheben und Empfehlungen dazu zu geben, wie sich unsere Produkte am besten bereitstellen und nutzen lassen. Sie können jederzeit für vRealize Automation am Programm zur Verbesserung der Kundenzufriedenheit teilnehmen oder die Teilnahme beenden.

Details zu den über CEIP gesammelten Daten und dem Zweck zur Verwendung dieses Programms durch VMware finden Sie im Trust & Assurance Center unter <http://www.vmware.com/trustvmware/ceip.html>.

Beitreten bzw. Verlassen des Programm zur Verbesserung der Kundenzufriedenheit für vRealize Automation

Sie können jederzeit dem Programm zur Verbesserung der Kundenzufriedenheit (CEIP) für vRealize Automation beitreten oder dieses verlassen.

vRealize Automation bietet Ihnen die Möglichkeit, dem Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) beizutreten, wenn Sie das Produkt zunächst installieren und konfigurieren. Nach der Installation können Sie dem CEIP beitreten oder dieses verlassen, indem Sie diese Schritte ausführen.

Verfahren

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

`https://vrealize-automation-appliance-FQDN:5480`

- 2 Klicken Sie auf die Registerkarte **Telemetrie**.
- 3 Aktivieren bzw. deaktivieren Sie die Option **Am Programm zur Verbesserung der Benutzerfreundlichkeit von VMware teilnehmen**.

Wenn markiert, aktiviert die Option das Programm und sendet Daten an `https://vmware.com`.

- 4 Klicken Sie auf **Einstellungen speichern**.

Konfigurieren der Datenerfassungszeit

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

Verfahren

- 1 Melden Sie sich bei einer Konsolensitzung auf 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.

## Anpassen von Systemeinstellungen

Als Systemadministrator können Sie die Protokollierung sowie IaaS-E-Mail-Vorlagen anpassen. Sie können auch Einstellungen verwalten, die als Standardeinstellungen für jeden Mandanten (wie zum Beispiel E-Mail-Server) angezeigt werden, um Benachrichtigungen zu verarbeiten. Mandantenadministratoren können diese Standardeinstellungen überschreiben, falls für den jeweils zugehörigen Mandanten andere Einstellungen erforderlich sind.

## Ändern des Symbols „Alle Services“ im Servicekatalog

Sie können das Standardsymbol im Servicekatalog ändern und ein benutzerdefiniertes Bild anzeigen. Wenn Sie das Symbol ändern, dann wird es für alle Mandanten geändert. Für den Katalog können keine mandantenspezifischen Symbole konfiguriert werden.

Befehle werden für Linux, Mac oder Windows bereitgestellt, sodass Sie die cURL-Befehle unter jedem dieser Betriebssysteme ausführen können.

### Voraussetzungen

- Konvertieren Sie das Bild in eine Base64-codierte Zeichenfolge.
- cURL muss auf der Maschine installiert sein, auf der Sie die Befehle ausführen.
- Sie benötigen Anmeldedaten als vRealize Automation-Benutzer mit der Systemadministrator-Rolle.

## Verfahren

- 1 Legen Sie die VCAC-Variable in der Terminalsitzung für die cURL-Befehle fest.

| Betriebssystem | Befehl                                  |
|----------------|-----------------------------------------|
| Linux/Mac      | <code>export VCAC=&lt;VA URL&gt;</code> |
| Windows        | <code>set VCAC=&lt;VA URL&gt;</code>    |

- 2 Rufen Sie das Authentifizierungstoken für den Systemadministrator-Benutzer ab.

| Betriebssystem | Befehl                                                                                                                                                                                                                                                              |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Linux/Mac      | <code>curl https://\$VCAC/identity/api/tokens --insecure -H "Accept: application/json" -H 'Content-Type: application/json' --data '{"username": "&lt;Catalog Administrator User&gt;", "password": "&lt;password&gt;", "tenant": "vsphere.local"}'</code>            |
| Windows        | <code>curl https://%VCAC%/identity/api/tokens --insecure -H "Accept:application/json" -H "Content-Type:application/json" --data "{ \"username\": \"&lt;Catalog Administrator User&gt;\", \"password\": \"&lt;password&gt;\", \"tenant\": \"vsphere.local\"}"</code> |

Ein Authentifizierungstoken wird generiert.

- 3 Legen Sie die Authentifizierungstokenvariable fest, indem Sie <Auth Token> durch die im vorherigen Schritt generierte Tokenzeichenfolge ersetzen.

| Betriebssystem | Befehl                                               |
|----------------|------------------------------------------------------|
| Linux/Mac      | <code>export AUTH="Bearer &lt;Auth Token&gt;"</code> |
| Windows        | <code>set AUTH=Bearer &lt;Auth Token&gt;</code>      |

- 4 Fügen Sie die Base64-codierte Zeichenfolge für das Bild hinzu.

| Betriebssystem | Befehl                                                                                                                                                                                                                                                                                                                                                  |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Linux/Mac      | <code>curl https://\$VCAC/catalog-service/api/icons --insecure -H "Accept: application/json" -H 'Content-Type: application/json' -H "Authorization: \$AUTH" --data '{"id": "cafe_default_icon_genericAllServices", "fileName": "&lt;filename&gt;", "contentType": "image/png", "image": "&lt;IMAGE DATA as base64 string&gt;"}</code>                   |
| Windows        | <code>curl https://%VCAC%/catalog-service/api/icons --insecure -H "Accept: application/json" -H "Content-Type: application/json" -H "Authorization: %AUTH%" --data "{ \"id\": \"cafe_default_icon_genericAllServices\", \"fileName\": \"&lt;filename&gt;\", \"contentType\": \"image/png\", \"image\": \"&lt;IMAGE DATA as base64 string&gt;\"}"</code> |

## Ergebnisse

Das neue Services-Symbol wird nach etwa fünf Minuten im Servicekatalog angezeigt.

Wenn Sie auf das Standardsymbol zurücksetzen möchten, führen Sie nach dem Ausführen der Schritte 1-3 den folgenden Befehl aus.

| Betriebssystem | Befehl                                                                                                                                                 |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Linux/Mac      | <code>curl https://\$VCAC/catalog-service/api/icons/cafe_default_icon-genericAllServices --insecure -H "Authorization: \$AUTH" --request DELETE</code> |
| Windows        | <code>curl https://%VCAC%/catalog-service/api/icons/cafe_default_icon-genericAllServices --insecure -H "Authorization: %AUTH%" --request DELETE</code> |

## Anpassen von Daten-Rollover-Einstellungen

Sie können vRealize Automation-Daten-Rollover-Einstellungen konfigurieren, um zu steuern, wie Legacy-Daten im System aufbewahrt, archiviert oder gelöscht werden.

Mit der Funktion für Daten-Rollover können Sie die maximale Anzahl der Tage festlegen, die vRealize Automation Daten in der von IaaS verwendeten SQL Server-Datenbank beibehält, bevor diese und andere Rollover-Steuerelemente archiviert oder gelöscht werden.

Standardmäßig ist die Daten-Rollover-Funktion deaktiviert.

Daten-Rollover-Einstellungen werden auf der vRealize Automation-Seite **Globale Einstellungen** konfiguriert. Bei aktivierter Funktion werden Daten aus den folgenden SQL Server-Datenbanktabellen abgefragt und entfernt:

- UserLog
- Audit
- CategoryLog
- VirtualMachineHistory
- VirtualMachineHistoryProp
- AuditLogItems
- AuditLogItemsProperties
- TrackingLogItems
- WorkflowHistoryInstances
- WorkflowHistoryResults

Wenn Sie `DataRolloverIsArchiveEnabled` auf „True“ festlegen, werden Archivversionen der Tabellen im dbo-Schema erstellt. Die Archivversion von UserLog ist beispielsweise `UserLogArchive` und die Archivversion von VirtualMachineHistory ist `VirtualMachineHistoryArchive`.

Ist die Daten-Rollover-Funktion aktiviert, wird sie einmal täglich zu der vordefinierten Uhrzeit 3:00 Uhr gemäß der vRealize Automation-Zeitzonekonfiguration ausgeführt. Mit der Einstellung `DataRollover MaximumAgeInDays` können Sie die maximale Aufbewahrungsdauer der Daten in Tagen festlegen. Beachten Sie, dass dieser Vorgang in der Regel innerhalb weniger Minuten bis zu einer Stunde ausgeführt wird. Wenn diese Funktion jedoch zum ersten Mal aktiviert wird, kann es sein, dass der Vorgang viele Daten zu archivieren/löschen hat und daher viel länger dauern

kann, bis er abgeschlossen ist. Dieser Vorgang ist so konzipiert, dass er so lange läuft, bis er abgeschlossen ist. Er führt seine Arbeit in kleinen und schnellen Transaktionsblöcken durch, um keine Probleme mit der Parallelität zu verursachen. Beachten Sie, dass dieser Vorgang wie unten beschrieben gestoppt werden kann.

**Hinweis** Sie können den Daten-Rollover-Vorgang stoppen, indem Sie die **DataRollover Status**-Einstellung von „Wird ausgeführt“ in „Deaktiviert“ oder „Aktiviert“ ändern. Dies führt dazu, dass der aktuell laufende Vorgang problemlos beendet wird. Es geht keine Arbeit verloren. Alle Daten, die bis zum Beenden des Vorgangs archiviert oder gelöscht wurden, werden gespeichert.


Ist die Einstellung **DataRollover IsArchiveEnabled** auf „True“ festgelegt, werden Daten, die älter sind als in **DataRollover MaximumAgeInDays** angegeben, in die Archivtabellen verschoben. Ist die Einstellung **DataRollover IsArchiveEnabled** auf „False“ festgelegt, werden die Daten dauerhaft gelöscht und es erfolgt keine Archivierung. Gelöschte Daten können nicht wiederhergestellt werden.

#### Verfahren

- 1 Melden Sie sich an der vRealize Automation-Konsole als **Systemadministrator** an.
- 2 Wählen Sie **Infrastruktur > Administration > Globale Einstellungen** aus.
- 3 Suchen Sie auf der Seite **Globale Einstellungen** nach dem **Daten-Rollover**-Abschnitt der Tabelle und überprüfen und konfigurieren Sie die Einstellungen.

| Einstellung                   | Beschreibung                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DataRollover BatchSize        | Diese Einstellung ist auf 2.000 voreingestellt und muss wahrscheinlich nicht geändert werden. Wenn es jedoch einige Leistungseinbußen zu geben scheint, kann eine kleinere Batchgröße helfen. Eine größere Batchgröße kann die Arbeit schneller erledigen, übt aber mehr Druck auf die gleichzeitige Verarbeitung aus. Der gültige Wert liegt zwischen 100 und 20000. |
| DataRollover IsArchiveEnabled | Gibt an, ob Rollover-Daten nach Erreichen der maximalen Tageszahl in Archivtabellen verschoben werden sollen.<br><br>Standardmäßig ist dieser Wert auf „True“ festgelegt. Wenn Sie den Wert auf „False“ festlegen, werden alle Daten, die älter sind als in der Einstellung <b>DataRollover MaximumAgeInDays</b> angegeben, dauerhaft gelöscht.                       |
| DataRollover MaximumAgeInDays | Gibt an, für wie viele Tage das System Daten höchstens in der Datenbank beibehält, bevor sie in das Archiv verschoben oder dauerhaft gelöscht werden.<br><br>Standardmäßig ist dieser Wert auf 90 Tage festgelegt.                                                                                                                                                    |
| DataRollover Status           | Gibt an, ob Daten-Rollover aktiviert werden kann.<br><br>Standardmäßig ist dieser Wert auf „Deaktiviert“ festgelegt. Zum Aktivieren von Daten-Rollover legen Sie den Wert auf „Aktiviert“ fest.                                                                                                                                                                       |

| Einstellung                                  | Beschreibung                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DataRollover VirtualMachineHistory BatchSize | Gibt die Batchgröße in der Tabelle VirtualMachineHistory im Bereich von 1 bis 5 Datensätzen an. Die Standardeinstellung ist 1.                                                                                                                                                                                                                                            |
| DataRollover UpdateStatistics                | Die Updatestatistik ist standardmäßig ausgeschaltet, aber es wird dringend empfohlen, sie einzuschalten (auf 1 zu setzen), da aktualisierte Statistiken gut für die Abfrageleistung sind. Dies führt dazu, dass die gespeicherte Prozedur [dbo].[usp_DataRollover] nach dem Archivierungsvorgang den Befehl zur Aktualisierung der Statistiken für die Tabellen ausführt. |

- 4 Klicken Sie auf das Symbol **Bearbeiten** () in der ersten Tabellenspalte, um eine Einstellung zu bearbeiten.

Der Bereich **Wert** für die entsprechende Einstellung kann nun bearbeitet werden.

- 5 Klicken Sie auf das Symbol **Speichern** () in der ersten Tabellenspalte, um Ihre Änderungen zu speichern.

## Anpassen der Einstellungen in der Manager Service-Konfigurationsdatei

Sie können die Manager Service-Konfigurationsdatei (`managerService.exe.config`) verwenden, um gemeinsame Einstellungen für Maschinenbereitstellungen anzupassen.

Die Datei `managerService.exe.config` befindet sich in der Regel im Verzeichnis `%System-Drive%\Program Files x86\VMware\vCAC\Server`. Erstellen Sie immer eine Kopie der Datei, bevor Sie sie bearbeiten.

Verwenden Sie die folgenden Einstellungen der Datei `managerService.exe.config`, um verschiedene Aspekte der Maschinenbereitstellungen zu steuern. Es werden Standardwerte angezeigt.

- `<add key="ProcessLeaseWorkflowTimerCallbackIntervalMilliseconds" value="3600000"/>`
- `<add key="BulkRequestWorkflowTimerCallbackMilliseconds" value="10000"/>`
- `<add key="MachineRequestTimerCallbackMilliseconds" value="10000"/>`
- `<add key="MachineWorkflowCreationTimerCallbackMilliseconds" value="10000"/>`
- `<add key="RepositoryConnectionMaxRetryCount" value="100"/>`
- `<add key="MachineCatalogRegistrationRetryTimerCallbackMilliseconds" value="120000"/>`
- `<add key="MachineCatalogUnregistrationRetryTimerCallbackMilliseconds" value="120000"/>`
- `<add key="MachineCatalogUpdateMaxRetryCount" value="15"/>`

## Festlegen von ressourcenintensiven Gleichzeitigkeitsgrenzen

Zum Sparen von Ressourcen begrenzt vRealize Automation die Anzahl der gleichzeitig ausgeführten Instanzen von Maschinenbereitstellung und Datenerfassung. Sie können die Grenzwerte ändern.

### Konfigurieren der gleichzeitigen Maschinenbereitstellung

Mehrere gleichzeitige Anforderungen für die Maschinenbereitstellung können die Leistung von vRealize Automation beeinträchtigen. Sie können Änderungen an Grenzwerten für Proxy-Agents und Workflow-Aktivitäten vornehmen, um die Leistung zu beeinflussen.

Basierend auf den Anforderungen von Maschinenbesitzern an Ihrem Standort empfängt der vRealize Automation-Server möglicherweise mehrere gleichzeitige Anforderungen für die Maschinenbereitstellung. Dies kann in den folgenden Situationen passieren:

- Ein einzelner Benutzer reicht eine Anforderung für mehrere Maschinen ein
- Viele Benutzer fordern Maschinen gleichzeitig an
- Einer oder mehrere Gruppenmanager genehmigen mehrere ausstehende Maschinenanforderungen in kurzen Abständen

Der Zeitaufwand für die Bereitstellung einer Maschine durch vRealize Automation nimmt bei einer größeren Anzahl gleichzeitiger Anforderungen im Allgemeinen zu. Für die Zunahme der Bereitstellungszeit sind die folgenden drei wichtigen Faktoren ausschlaggebend:

- Die Auswirkung gleichzeitiger ressourcenintensiver vRealize Automation-Workflow-Aktivitäten auf die Leistung, einschließlich der SetupOS-Aktivitäten (für innerhalb der Virtualisierungsplattform erstellte Maschinen, etwa bei der WIM-basierten Bereitstellung) und der Klonaktivitäten (für innerhalb der Virtualisierungsplattform geklonte Maschinen).
- Der konfigurierte vRealize Automation-Grenzwert bezüglich der Anzahl ressourcenintensiver (und in der Regel zeitaufwändiger) Bereitstellungsaktivitäten, die gleichzeitig ausgeführt werden können. Der Standardwert sind acht Bereitstellungsaktivitäten. Gleichzeitige Aktivitäten über den konfigurierten Grenzwert hinaus werden zur Warteschlange hinzugefügt.
- Grenzwerte für die Virtualisierungsplattform oder das Cloud-Dienstkonto bezüglich der Anzahl von vRealize Automation-Arbeits Elementen (ressourcenintensiv oder auch nicht), die gleichzeitig ausgeführt werden können. Beispielsweise lautet der Grenzwert in vCenter Server standardmäßig vier Arbeitselemente. Arbeitselemente über diesen Grenzwert hinaus werden zur Warteschlange hinzugefügt.

Standardmäßig begrenzt vRealize Automation gleichzeitige Aktivitäten für die virtuelle Bereitstellung für Hypervisoren, die Proxy-Agents verwenden, auf acht Aktivitäten pro Endpoint. Dadurch wird sichergestellt, dass die von einem bestimmten Agent verwaltete Virtualisierungsplattform nie so viele ressourcenintensive Arbeitselemente erhält, dass die Ausführung anderer Elemente verhindert wird. Testen Sie die Auswirkungen eines geänderten

Grenzwerts sorgfältig, bevor Sie tatsächlich Änderungen vornehmen. Zur Festlegung des optimalen Grenzwerts für Ihren Standort müssen Sie möglicherweise die Ausführung von Arbeitselementen innerhalb der Virtualisierungsplattform sowie die Ausführung von Workflow-Aktivitäten innerhalb von vRealize Automation analysieren.

Wenn Sie den konfigurierten vRealize Automation-Grenzwert pro Agent anheben, müssen Sie möglicherweise wie folgt zusätzliche Konfigurationsanpassungen in vRealize Automation vornehmen:

- Die standardmäßigen Zeitüberschreitungsintervalle für die Ausführung der SetupOS- und Klon-Workflow-Aktivitäten betragen jeweils zwei Stunden. Überschreitet die für die Ausführung einer dieser Aktivitäten erforderliche Zeit diesen Grenzwert, wird die Aktivität abgebrochen und die Bereitstellung schlägt fehl. Um das Fehlschlagen zu verhindern, erhöhen Sie eines oder beide dieser Zeitüberschreitungsintervalle für die Ausführung.
- Die standardmäßigen Zeitüberschreitungsintervalle für die Übermittlung der SetupOS- und Klon-Workflow-Aktivitäten betragen jeweils 20 Stunden. Sobald eine dieser Aktivitäten gestartet wurde und die Maschine im Zusammenhang mit der Aktivität nicht innerhalb von 20 Stunden bereitgestellt wurde, wird die Aktivität abgebrochen und die Bereitstellung schlägt fehl. Wenn Sie deshalb den Grenzwert angehoben haben, sodass dieses Problem gelegentlich auftritt, sollten Sie einen oder beide dieser Zeitüberschreitungsintervalle für die Übermittlung anheben.

### Konfigurieren gleichzeitiger Datenerfassungen

Gleichzeitige Datenerfassungsaktivitäten werden von vRealize Automation standardmäßig beschränkt. Wenn Sie diesen Grenzwert ändern, können Sie unnötige Zeitüberschreitungen vermeiden, indem Sie die standardmäßigen Zeitüberschreitungsintervalle für die Ausführung der verschiedenen Datenerfassungstypen ändern.

vRealize Automation erfasst regelmäßig Daten von bekannten Virtualisierungs-Computing-Ressourcen über die Proxy-Agents und von Cloud-Dienstkonto und physischen Maschinen über die Endpoints, die diese repräsentieren. In Abhängigkeit von der Anzahl der Virtualisierungs-Computing-Ressourcen, Agents und Endpoints an Ihrem Standort werden gleichzeitige Datenerfassungen möglicherweise häufig durchgeführt.

Die Ausführungszeit für die Datenerfassung hängt von der Anzahl von Objekten auf Endpoints ab, einschließlich virtueller Maschinen, Datenspeichern, Vorlagen und Computing-Ressourcen. Eine einzelne Datenerfassung kann in Abhängigkeit von vielen Bedingungen ziemlich zeitaufwändig sein. Wie bei der Maschinenbereitstellung erhöht auch die gleichzeitige Ausführung den erforderlichen Zeitaufwand für die Datenerfassung.

Gleichzeitige Datenerfassungsaktivitäten werden auf zwei Aktivitäten pro Agent beschränkt. Aktivitäten über diesen Grenzwert hinaus werden zur Warteschlange hinzugefügt. Dadurch wird sichergestellt, dass jede Datenerfassung relativ schnell abgeschlossen wird und dass gleichzeitige Datenerfassungsaktivitäten möglichst nicht die IaaS-Leistung beeinträchtigen.

In Abhängigkeit von den Ressourcen und Begleitumständen an Ihrem Standort kann jedoch der konfigurierte Grenzwert angehoben werden, sodass die Leistung ausreicht, um gleichzeitige Aktivitäten der Proxy-Datenerfassung zu nutzen. Die Anhebung des Grenzwerts kann zwar den erforderlichen Zeitaufwand für eine einzelne Datenerfassung erhöhen, aber dies wird dadurch aufgewogen, dass mehr Daten von mehr Computing-Ressourcen und Maschinen gleichzeitig erfasst werden können.

Wenn Sie den konfigurierten Grenzwert pro Agent anheben, müssen Sie möglicherweise die standardmäßigen Zeitüberschreitungsintervalle für die Ausführung der verschiedenen Datenerfassungstypen anpassen, die einen Proxy-Agent verwenden (Bestandsliste, Leistung, Zustand, WMI). Überschreitet die für die Ausführung einer dieser Aktivitäten erforderliche Zeit die konfigurierten Zeitüberschreitungsintervalle, wird die Aktivität abgebrochen und neu gestartet. Um den Abbruch der Aktivität zu verhindern, erhöhen Sie eines oder mehrere dieser Zeitüberschreitungsintervalle für die Ausführung.

### Anpassen der Parallelitätsgrenzwerte und Zeitüberschreitungsintervalle

Sie können die Grenzwerte pro Agent für die gleichzeitige Bereitstellung, Datenerfassungsaktivitäten und die standardmäßigen Zeitüberschreitungsintervalle ändern.

Verwenden Sie bei der Eingabe eines Zeitwerts für diese Variablen das Format hh:mm:ss (hh=Stunden, mm=Minuten und ss=Sekunden).

#### Voraussetzungen

Melden Sie sich als Administrator an dem Server an, der den IaaS Manager Service hostet. Für verteilte Installationen ist dies der Server, auf dem der Manager Service installiert wurde.

#### Verfahren

- 1 Öffnen Sie die Datei `ManagerService.exe.config` in einem Editor. Diese Datei ist im Installationsverzeichnis von vRealize Automation Server gespeichert, in der Regel `%SystemDrive%\Programme x86\VMware\vCAC\Server`.
- 2 Suchen Sie nach dem Abschnitt `workflowTimeoutConfigurationSection`.
- 3 Aktualisieren Sie ggf. die folgenden Variablen.

| Parameter                                               | Beschreibung                                                                                     |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| <b><i>MaxOutstandingResourceIntensive WorkItems</i></b> | Grenzwert für die gleichzeitige Bereitstellung (der Standardwert ist 8)                          |
| <b><i>CloneExecutionTimeout</i></b>                     | Zeitüberschreitungsintervall für die Ausführung der virtuellen Bereitstellung                    |
| <b><i>SetupOSExecutionTimeout</i></b>                   | Zeitüberschreitungsintervall für die Ausführung der virtuellen Bereitstellung                    |
| <b><i>CloneTimeout</i></b>                              | Zeitüberschreitungsintervall für die Klonbereitstellung bei der virtuellen Bereitstellung        |
| <b><i>SetupOSTimeout</i></b>                            | Zeitüberschreitungsintervall für das Setup des Betriebssystems bei der virtuellen Bereitstellung |
| <b><i>CloudInitializeProvisioning</i></b>               | Zeitüberschreitungsintervall für die Initialisierung der Cloud-Bereitstellung                    |



| Parameter                                    | Beschreibung                                                                     |
|----------------------------------------------|----------------------------------------------------------------------------------|
| <b>MaxOutstandingDataCollectionWorkItems</b> | Grenzwert für die gleichzeitige Datenerfassung                                   |
| <b>InventoryTimeout</b>                      | Zeitüberschreitungsintervall für die Ausführung der Bestandslistendatenerfassung |
| <b>PerformanceTimeout</b>                    | Zeitüberschreitungsintervall für die Ausführung der Leistungsdatenerfassung      |
| <b>StateTimeout</b>                          | Zeitüberschreitungsintervall für die Ausführung der Statusdatenerfassung         |

- 4 Speichern und schließen Sie die Datei.
- 5 Wählen Sie **Start > Verwaltung > Dienste** aus.
- 6 Beenden Sie den vRealize Automation-Dienst und starten Sie ihn dann erneut.
- 7 (Optional) Wenn vRealize Automation im High Availability-Modus ausgeführt wird, müssen alle nach der Installation an der Datei `ManagerService.exe.config` vorgenommenen Änderungen auf dem primären Server und dem Failover-Server vorgenommen werden.

### Anpassen der Ausführungshäufigkeit von Maschinenrückrufen

Sie können die Häufigkeit mehrerer Rückrufprozeduren ändern, einschließlich der Häufigkeit, mit der die vRealize Automation-Rückrufprozedur für geänderte Maschinen-Leases ausgeführt wird.

vRealize Automation verwendet ein konfiguriertes Zeitintervall zum Ausführen verschiedener Rückrufprozeduren im Model Manager-Dienst, wie beispielsweise `ProcessLeaseWorkflowTimerCallbackIntervalMilliseconds` – hiermit wird nach Maschinen gesucht, deren Leases geändert wurden. Sie können diese Zeitintervalle ändern, um die Überprüfung häufiger oder seltener durchzuführen.

Bei der Eingabe eines Zeitwerts für diese Variablen geben Sie einen Wert in Millisekunden ein. Beispiel: 10000 Millisekunden = 10 Sekunden und 3600000 Millisekunden = 60 Minuten = 1 Stunde.

### Voraussetzungen

Melden Sie sich als Administrator an dem Server an, der den IaaS Manager Service hostet. Für verteilte Installationen ist dies der Server, auf dem der Manager Service installiert wurde.

### Verfahren

- 1 Öffnen Sie die Datei `ManagerService.exe.config` in einem Editor. Diese Datei ist im Installationsverzeichnis von vRealize Automation Server gespeichert, in der Regel `%SystemDrive%\Programme x86\VMware\VCAC\Server`.

## 2 Aktualisieren Sie ggf. die folgenden Variablen.

| Parameter                                                          | Beschreibung                                                                                                  |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b><i>RepositoryWorkflowTimerCallbackMiliSeconds</i></b>           | Überprüft den Repository-Dienst oder den Model Manager-Webdienst auf Aktivitäten. Der Standardwert ist 10000. |
| <b><i>ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds</i></b> | Sucht nach abgelaufenen Maschinen-Leases. Der Standardwert ist 3600000.                                       |
| <b><i>BulkRequestWorkflowTimerCallbackMiliSeconds</i></b>          | Sucht nach Massenanforderungen. Der Standardwert ist 10000.                                                   |
| <b><i>MachineRequestTimerCallbackMiliSeconds</i></b>               | Sucht nach Maschinenanforderungen. Der Standardwert ist 10000.                                                |
| <b><i>MachineWorkflowCreationTimerCallbackMiliSeconds</i></b>      | Sucht nach neuen Maschinen. Der Standardwert ist 10000.                                                       |

- 3 Speichern und schließen Sie die Datei.
- 4 Wählen Sie **Start > Verwaltung > Dienste** aus.
- 5 Halten Sie den vCloud Automation Center-Dienst an und starten Sie ihn anschließend erneut.
- 6 (Optional) Wenn vRealize Automation im High Availability-Modus ausgeführt wird, müssen alle nach der Installation an der Datei `ManagerService.exe.config` vorgenommenen Änderungen auf dem primären Server und dem Failover-Server vorgenommen werden.

## Anpassen von IaaS-Protokolleinstellungen

Sie können vRealize Automation so anpassen, dass nur die Informationen protokolliert werden, die im Manager Service-Protokoll angezeigt werden sollen.

Wenn vRealize Automation im High Availability-Modus ausgeführt wird und Sie nach der Installation Änderungen an der Datei `ManagerService.exe.config` vornehmen, müssen Sie die Änderungen auf den primären und Failover-vRealize Automation-Servern vornehmen.

### Verfahren

- 1 Melden Sie sich am vRealize Automation-Server mithilfe von Anmeldedaten mit Administratorzugriff an.
- 2 Bearbeiten Sie die Datei `ManagerService.exe.config` im Verzeichnis `%SystemDrive%\Programme (x86)\VMware\VCAC\Server` bzw. im Installationsverzeichnis des vRealize Automation-Servers, falls sie sich in einem anderen Speicherort befindet.

- 3 Bearbeiten Sie die Keys `RepositoryLogSeverity` und `RepositoryLogCategory`, um festzulegen, welche Ereignistypen in Ihre Protokolldateien geschrieben werden sollen.

| Option                       | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RepositoryLogSeverity</b> | <p>Hier wird festgelegt, unterhalb welchen Schweregrads Ereignisse ignoriert werden sollen.</p> <ul style="list-style-type: none"> <li>■ <i>Error</i> protokolliert nur behebbare Fehler und Fehler von darüber hinausgehendem Schweregrad.</li> <li>■ <i>Warning</i> protokolliert nicht kritische Warnungen und Warnungen von darüber hinausgehendem Schweregrad.</li> <li>■ <i>Information</i> protokolliert alle Informationsmeldungen und Meldungen von darüber hinausgehendem Schweregrad.</li> <li>■ <i>Verbose</i> protokolliert einen Debugging-Eintrag und kann die Leistung beeinträchtigen.</li> </ul> <p>Beispielsweise <code>&lt;add key="RepositoryLogSeverity" value="Warning" /&gt;</code>.</p> |
| <b>RepositoryLogCategory</b> | <p>Hier wird eine Kategorie festgelegt, für die alle Ereignisse jeden Schweregrads protokolliert werden. Beispiel: <code>&lt;add key="RepositoryLogCategory" value="MissingMachines,UnregisteredMachines,AcceptMachineRequest,RejectMachineRequest" /&gt;</code> protokolliert alle Ereignisse von fehlenden Maschinen oder Maschinen, deren Registrierung aufgehoben wurde, sowie jede angenommene oder abgelehnte Maschinenanforderung.</p>                                                                                                                                                                                                                                                                    |

- 4 Speichern und schließen Sie die Datei.
- 5 Wählen Sie **Start > Verwaltung > Dienste** aus und starten Sie den vCloud Automation Center-Dienst neu.

#### Ergebnisse

Um zu sehen, wie sich Ihre Änderungen auf die Protokollierung auswirken, können Sie die Manager Service-Protokolldatei anzeigen, die sich im Verzeichnis `%SystemDrive%\Program Files (x86)\VMware\vCAC\Server\Logs` der Maschine, auf der der Manager Service installiert ist, befindet, bzw. im Installationsverzeichnis des vRealize Automation-Servers, falls Sie die Datei an einem anderen Speicherort installiert haben.

## Überwachen von vRealize Automation

Abhängig von Ihrer Rolle können Sie Workflows oder Dienste überwachen, Ereignis- oder Überwachungsprotokolle anzeigen oder Protokolle für alle Hosts in einer verteilten Bereitstellung erfassen.

### Überwachen von Workflows und Anzeigen von Protokollen

Abhängig von Ihrer Rolle können Sie Workflows überwachen und Aktivitätsprotokolle anzeigen.

Tabelle 1-12. Optionen zum Überwachen und Anzeigen von Protokollen

| Ziel                                                                                                                                                       | Rolle                                               | Menüabfolge und Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zeigen Sie Informationen über stattgefundenene Aktionen an, wie beispielsweise den Aktionstypen, Datum und Uhrzeit der Aktion usw.                         | IaaS-Administrator                                  | <p>Zeigen Sie Standardprotokollinformationen an oder steuern Sie Anzeigehalt mit den Spalten- und Filteroptionen.</p> <p>Wählen Sie <b>Infrastruktur &gt; Überwachung &gt; Überwachungsprotokoll</b> aus.</p> <p>Das Überwachungsprotokoll stellt Details zum Status der verwalteten virtuellen Maschinen und der Aktivitäten bereit, die auf diesen Maschinen bei der Neukonfiguration ausgeführt wurden. Das Protokoll enthält Informationen zur Maschinenbereitstellung, NSX, Rückforderung und Neukonfigurationsaktionen.</p> |
| Zeigen Sie den Status des geplanten und verfügbaren Distributed Execution Managers und andere Workflows an.                                                | IaaS-Administrator                                  | <p>Zeigen Sie den Workflowstatus an und öffnen Sie optional einen bestimmten Workflow, um seine Details anzuzeigen.</p> <p>Wählen Sie <b>Infrastruktur &gt; Überwachung &gt; DEM-Status</b> aus.</p>                                                                                                                                                                                                                                                                                                                              |
| Zeigen Sie Protokolldaten an und exportieren Sie sie optional.                                                                                             | IaaS-Administrator                                  | <p>Zeigen Sie Standardprotokollinformationen an oder steuern Sie Anzeigehalt mit den Spalten- und Filteroptionen.</p> <p>Wählen Sie <b>Infrastruktur &gt; Überwachung &gt; Protokoll</b> aus.</p>                                                                                                                                                                                                                                                                                                                                 |
| Zeigen Sie den Status und den Verlauf des ausgeführten Distributed Execution Managers und andere Workflows an.                                             | IaaS-Administrator                                  | <p>Zeigen Sie den Workflowverlauf an und öffnen Sie optional einen bestimmten Workflow, um seine Details zur Ausführung anzuzeigen.</p> <p>Wählen Sie <b>Infrastruktur &gt; Überwachung &gt; Workflowverlauf</b> aus.</p>                                                                                                                                                                                                                                                                                                         |
| Zeigen Sie eine Liste von Ereignissen an, einschließlich Ereignistyp, Uhrzeit, Benutzer-ID usw. Zeigen Sie optional eine Seite mit den Ereignisdetails an. | Systemadministrator                                 | <p>Zeigen Sie eine Liste von Ereignissen und deren zugeordnete Attribute an, wie beispielsweise Laufzeit, Ereignisbeschreibung, Mandantenname, Zieltyp und -ID sowie andere Charakteristiken.</p> <p>Wählen Sie <b>Administration &gt; Ereignisse &gt; Ereignisprotokolle</b> aus.</p>                                                                                                                                                                                                                                            |
| Überwachen Sie den Anforderungsstatus und zeigen Sie Details zu den Anforderungen an.                                                                      | Mandantenadministrator oder Business-Gruppenmanager | <p>Zeigen Sie den Status der Anforderungen an, für die Sie verantwortlich sind, bzw. die Ihre eigenen sind.</p> <p>Klicken Sie auf <b>Anforderungen</b>.</p>                                                                                                                                                                                                                                                                                                                                                                      |
| Zeigen Sie Informationen über die neuesten Ereignisse an.                                                                                                  | IaaS-Administrator oder Mandantenadministrator      | <p>Zeigen Sie die neuesten Ereignisse für den zurzeit angemeldeten Benutzer an.</p> <p>Wählen Sie <b>Infrastruktur &gt; Neueste Ereignisse</b> aus.</p>                                                                                                                                                                                                                                                                                                                                                                           |

## Überwachen von Ereignisprotokollen und Diensten

Sie können vRealize Automation-Ereignisprotokolle und -Dienste überwachen, um ihren aktuellen und historischen Zustand zu bestimmen.

Der Standardaufbewahrungszeitraum für die Ereignisprotokolle beträgt 90 Tage. Sie können den Zeitraum in der Datei `/etc/vcac/vcac.properties` ändern.

Weitere Informationen zum Löschen von Protokollen durch Anpassen der Daten-Rollover-Einstellungen finden Sie unter *Konfigurieren von vRealize Automation*.

## vRealize Automation-Dienste

Ein Systemadministrator kann den Status von vRealize Automation-Diensten über das Ereignisprotokoll auf der Systemadministratorkonsole anzeigen.

Teilmenge der Dienste, die erforderlich sind, um einzelne Produktkomponenten auszuführen. So müssen z. B. Identitätsdienste und UI-Kerndienste ausgeführt werden, bevor Sie einen Mandanten konfigurieren können.

Die folgenden Tabellen zeigen, welche Dienste mit Bereichen der vRealize Automation-Funktionalität in Verbindung stehen.

**Tabelle 1-13. Identitätsdienstgruppe**

| Dienst             | Beschreibung             |
|--------------------|--------------------------|
| management-service | Identitätsdienstgruppe   |
| sts-service        | Single Sign On-Appliance |
| authorization      | Autorisierungsdienst     |
| Authentifizierung  | Authentifizierung        |
| eventlog-service   | Ereignisprotokolldienst  |
| licensing-service  | Lizenzierungsdienst      |

**Tabelle 1-14. UI-Kerndienste**

| Dienst           | Beschreibung                      |
|------------------|-----------------------------------|
| shel-ui-app      | Shell-Dienst                      |
| branding-service | Branding-Dienst                   |
| plugin-service   | Erweiterbarkeits(-Plug-In-)Dienst |
| portal-service   | Portaldienst                      |

Alle der folgenden Dienste sind erforderlich, um die IaaS-Komponente auszuführen.

**Tabelle 1-15. Servicekataloggruppe (Kontrolldienste)**

| Dienst               | Beschreibung            |
|----------------------|-------------------------|
| notification-service | Benachrichtigungsdienst |
| workitem-service     | Arbeitselementdienst    |

Tabelle 1-15. Servicekataloggruppe (Kontrolldienste) (Fortsetzung)

| Dienst           | Beschreibung       |
|------------------|--------------------|
| approval-service | Genehmigungsdienst |
| catalog-service  | Servicekatalog     |

Tabelle 1-16. IaaS-Dienstgruppe

| Dienst              | Beschreibung          |
|---------------------|-----------------------|
| iaas-proxy-provider | IaaS-Proxy            |
| iaas-server         | IaaS Windows-Maschine |

Tabelle 1-17. XaaS

| Dienst                    | Beschreibung                           |
|---------------------------|----------------------------------------|
| vco                       | vRealize Orchestrator                  |
| advanced-designer-service | XaaS-Blueprints und Ressourcenaktionen |

## Verwenden der vRealize Automation-Überwachungsprotokollierung

vRealize Automation bietet Überwachungsprotokollierung zur Unterstützung der Erfassung und Aufbewahrung wichtiger Systemereignisse.

Derzeit unterstützt vRealize Automation Überwachungsprotokollierung als Erweiterung der Ereignisprotokollierung. Diese Funktionalität bietet grundlegende Überwachungsinformationen, und die Aufbewahrungseinstellungen sind nur mithilfe geeigneter des Ereignis-Brokerdiensts der vRealize Automation-REST API möglich. Überwachungsprotokollierung ist derzeit für Mandantenadministratoren und für Systemadministratoren, die sich bei Mandanten anmelden können, verfügbar. Sie bietet Such- und Filterfunktionen für Ereignisse.

Standardmäßig unterstützt vRealize Automation Überwachungsprotokollierung für Workflowabonnements, Endpoint-Ereignisse sowie für Ereignisse zur Erstellung, Aktualisierung und Löschung von Fabric-Gruppen. vRealize Automation unterstützt auch die Anpassung der Überwachungsprotokollierung für verschiedene IaaS-Ereignisse.

vRealize Automation-Überwachungsprotokollierung ist standardmäßig deaktiviert. Sie können Sie aktivieren und deaktivieren, indem Sie das Kontrollkästchen **Aktiviert** im Abschnitt „Überwachungsprotokollintegration“ auf der Seite **vRA > Protokolle** der Virtual Appliance Management Interface (VAMI) aktivieren bzw. deaktivieren.

Überwachungsprotokollinformationen werden auf der standardmäßigen Seite „Ereignisprotokolle“ angezeigt. Wählen Sie als Mandantenadministrator **Administration > Ereignisprotokolle** aus, um diese Seite anzuzeigen. Überwachungsereignisse werden in der Ereignisprotokolltabelle mit der Bezeichnung „Überwachung“ im Feld „Ereignistyp“ identifiziert. Jeder Eintrag weist eine Ereignisbeschreibung für jedes Ereignis sowie Informationen zu Mandant, Uhrzeit, Benutzer und zum zugehörigen Dienstenamen auf.

Das Aktivieren der Überwachungsprotokollierung für alle anderen IaaS-Ereignisse erfordert eine benutzerdefinierte Konfigurationsdatei und das Ausführen der geeigneten Befehle auf Ihrer IaaS-Hostmaschine. Wenden Sie sich an VMware Professional Services, um Unterstützung zu erhalten.

Sie können vRealize Automation so konfigurieren, dass Ereignisse auf einen externen Syslog-Server exportiert werden, genauer gesagt VMware Log Insight.

## Konfigurieren von vRealize Automation für die Überwachungsprotokollierung mit Log Insight

Sie können vRealize Automation zum Exportieren von Überwachungsereignissen in VMware Log Insight konfigurieren, um das Anzeigen von Überwachungsereignissen zu vereinfachen.

Die Überwachungsprotokollierung ist standardmäßig deaktiviert, und Sie müssen sie aktivieren, um Überwachungsprotokollierungs-Ereignisse zu generieren und anzuzeigen.

Wenn verwendet, wird SSL in der vRealize Automation-Appliance konfiguriert, in der sich der Log Insight-Agent befindet, und betrifft die Verbindung mit dem Log Insight Syslog-Server. Wenn Sie SSL verwenden möchten, müssen Sie die entsprechenden Zertifikate und die Konnektivität zwischen vRealize Automation und dem in Ihrer Bereitstellung installierten Log Insight-Server konfigurieren.

### Voraussetzungen

vRealize Automation verwendet den Log Insight-Agent, der standardmäßig in einer vRealize Automation-Bereitstellung installiert ist, um Protokolleinträge zum Anzeigen in Log Insight zu lesen.

### Verfahren

- 1 Melden Sie sich bei der Verwaltungsschnittstelle der virtuellen Appliance als Systemadministrator an.
- 2 Wählen Sie **vRA > Protokolle** aus.
- 3 Vergewissern Sie sich, dass das Kontrollkästchen **Aktiviert** für die Überwachungsprotokollierung unter der Überschrift „Überwachungsprotokollintegration“ aktiviert ist.
- 4 Geben Sie unter der Überschrift „Log Insight-Agent-Konfiguration“ den **Host**-Maschinennamen für den Log Insight-Server ein.
  - a Geben Sie den Namen der **Host**-Maschine für den Log Insight-Agent ein.
  - b Geben Sie den für die Kommunikation mit dem Log Insight-Agent verwendeten **Port** ein.

- c Wählen Sie das entsprechende Kommunikationsprotokoll aus.
- d Verwenden Sie das Kontrollkästchen **SSL aktiviert**, um anzugeben, ob SSL für die Kommunikation zwischen Log Insight-Agent und Server verwendet werden soll.

Wenn Sie SSL nicht verwenden möchten, können Sie die restlichen Einstellungen auf der Seite ignorieren. Falls SSL verwendet wird, müssen Sie diese Einstellungen konfigurieren.

- 5 Wenn Sie SSL verwenden, nehmen Sie im Abschnitt für die vertrauenswürdigen SSL-Stammzertifikate die entsprechende Auswahl vor.

Standardmäßig verwendet die vRealize Automation-Appliance ein selbst signiertes Zertifikat. Wenn Sie ein vertrauenswürdiges Stammzertifikat verwenden möchten, müssen Sie dieses importieren.

- a Aktivieren Sie das entsprechende Kontrollkästchen, um anzugeben, ob Sie ein neues oder ein vorhandenes Zertifikat verwenden möchten.

Weitere Informationen finden Sie auf der Seite „vRealize Automation-Protokollierung konfigurieren“ der Verwaltungsschnittstelle der virtuellen Appliance.

- 6 Klicken Sie auf **Einstellungen speichern**.
- 7 Nehmen Sie die entsprechende Auswahl im Abschnitt „SSL-Serverzertifikate“ vor.
- 8 Verwenden Sie den Abschnitt „Konfiguration des Agent-Verhaltens“, um die Funktionsweise des Agent mit Protokolldateien zu konfigurieren.

## Ergebnisse

Überwachungsprotokollereignisse von vRealize Automation können in der Log Insight-Schnittstelle angezeigt werden.

## Anzeigen von Hostinformationen für Cluster in verteilten Bereitstellungen

Sie können Protokolle für alle Knoten, die in einer verteilten Bereitstellung gruppiert sind, über die Verwaltungskonsole der vRealize Automation-Appliance erfassen.

Sie können auch Informationen für jeden Host in Ihrer Bereitstellung anzeigen. Die Registerkarte **Cluster** auf der vRealize Automation Management Console enthält eine Tabelle mit Informationen zur verteilten Bereitstellung, die die folgenden Informationen anzeigt:

- Eine Liste mit allen Knoten in Ihrer Bereitstellung.
- Den Hostnamen für den Knoten. Der Hostname wird als vollqualifizierter Domänenname angegeben.
- Die Uhrzeit, als der Host das letzte Mal der Management Console geantwortet hat. Knoten für IaaS-Komponenten melden die Verfügbarkeit alle drei Minuten und Knoten für virtuelle Appliances alle neun Minuten.
- Den vRealize Automation-Komponententyp. Identifiziert, ob der Knoten eine virtuelle Appliance oder ein IaaS-Server ist.



Abbildung 1-1. Tabelle „Info zur verteilten Bereitstellung“

|   | Host / Node Name             | Version     | Last Connected | Type   | State* | Valid*                                |
|---|------------------------------|-------------|----------------|--------|--------|---------------------------------------|
| ▶ | cava-n-80-175.eng.vmware.com | 7.5.0.378   | 7 minutes ago  | MASTER | Up     | <input type="button" value="Delete"/> |
| ▶ | cava-n-85-043.eng.vmware.com | 7.5.0.14528 | 14 seconds ago | IAAS   |        | <input type="button" value="Delete"/> |

Mit dieser Tabelle können Sie Aktivitäten in Ihrer Bereitstellung überwachen. Beispiel: Wenn die Spalte „Zuletzt verbunden“ anzeigt, dass ein Host in letzter Zeit keine Verbindung hergestellt hat, kann dies ein Hinweis auf ein Problem mit dem Hostserver sein.

## Protokollsammlung

Sie können eine ZIP-Datei erstellen, die Protokolldateien für alle Hosts in Ihrer Bereitstellung enthält. Wählen Sie dazu die Schaltfläche „Support-Paket erstellen“ auf der Seite **vRA > Protokolle** aus. Weitere Informationen finden Sie unter [Erfassen von Protokollen für Cluster und verteilte Bereitstellungen](#).

## Entfernen von Knoten aus der Tabelle

Wenn Sie einen Host aus Ihrer Bereitstellung entfernen, entfernen Sie den entsprechenden Knoten aus der Tabelle mit den Informationen zur verteilten Bereitstellung zum Optimieren der Protokollerfassungszeiten. Klicken Sie auf die Schaltfläche **Löschen**, um einen Knoten aus der Tabelle zu entfernen.

## Erfassen von Protokollen für Cluster und verteilte Bereitstellungen

Zur Unterstützung von Aktivitäten zur Fehlerbehebung und Beibehaltung von Datensätzen können Sie eine ZIP-Datei erstellen, die alle Protokolldateien für Server in Ihrer Bereitstellung enthält.

In der Tabelle mit Informationen zur verteilten Bereitstellung auf der Registerkarte „Cluster“ der Verwaltungsschnittstelle der virtuellen Appliance werden die Knoten aufgelistet, für die Protokolldateien erfasst werden. Sie können auch Knoten aus dieser Tabelle löschen.

Informationen zur Konfiguration der Bereitstellung der vRealize Automation-Appliance finden Sie unter *Installieren von vRealize Automation*.

### Verfahren

- 1 Melden Sie sich bei der Verwaltungsschnittstelle der virtuellen Appliance als Systemadministrator an.
- 2 Klicken Sie auf **vRA > Protokolle**.
- 3 Klicken Sie auf **Support-Paket erstellen**.

Protokolldateien werden für jeden Knoten erfasst und in eine ZIP-Datei kopiert.

## Entfernen eines Knotens aus der Tabelle „Info zur verteilten Bereitstellung“

Löschen Sie einen Knoten, wenn Sie ihn aus dem Bereitstellungscluster entfernen oder ein Management Agent-Zertifikat ersetzen möchten.

In der Tabelle „Info zur verteilten Bereitstellung“ auf der Registerkarte „Cluster“ der Verwaltungsschnittstelle der virtuellen Appliance werden die Knoten für den anwendbaren Cluster aufgelistet. Sie können für jeden Knoten in der Tabelle auf die Schaltfläche **Löschen** klicken, um diesen Knoten aus dem Cluster zu entfernen. Alternativ können Sie folgendes Verfahren verwenden.

### Verfahren

- 1 Melden Sie sich bei der vRealize Automation-Appliance mit dem Benutzernamen **root** und dem Kennwort an, das Sie bei der Bereitstellung der Appliance angegeben haben.
- 2 Klicken Sie auf die Registerkarte **Cluster**.

In der Tabelle „Info zur verteilten Bereitstellung“ werden die Knoten für die verteilte Bereitstellung aufgelistet.

- 3 Suchen Sie die Knoten-ID für den zu entfernenden Knoten, indem Sie eine Eingabeaufforderung öffnen und den folgenden Befehl ausführen:

```
/usr/sbin/vcac-config cluster-config-node --action list
```

- 4 Suchen Sie die Knoten-ID, z. B. `cafe.node.46686239.17144`, in der JSON-Ausgabe.
- 5 Öffnen Sie eine Eingabeaufforderung und geben Sie einen Befehl im folgenden Format ein. Verwenden Sie dabei die Knoten-ID, die Sie im vorherigen Schritt ermittelt haben.

```
/usr/sbin/vcac-config cluster-config-node
--action delete --id Knoten-UID
```

Geben Sie beispielsweise den folgenden Befehl für die beispielhafte Knoten-ID `cafe.node.46686239.17144` ein:

```
/usr/sbin/vcac-config cluster-config-node --action delete --id cafe.node.46686239.17144
```

- 6 Klicken Sie auf **Aktualisieren**.

Der Knoten wird nicht mehr in der Anzeige angezeigt.

## Überwachen der Integrität von vRealize Automation

Der vRealize Automation-Integritätsdienst bewertet die funktionale Integrität einer vRealize Automation-Umgebung.

IaaS-Administratoren konfigurieren den Integritätsdienst zum Ausführen von Testsuites, die bestimmen, ob die Komponenten registriert und die erforderlichen Ressourcen verfügbar sind. In dieser Tabelle werden die vom Integritätsdienst bereitgestellten Testsuites und einige Beispieltests in jeder Suite angezeigt.

| Testsuites des Integritätsdiensts      | Beispieltests                                                                                                                                                                                                                                                                |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Systemtests für vRealize Automation    | <ul style="list-style-type: none"> <li>■ SSO-/Identity VA-Verbindungstest</li> <li>■ vRealize Automation-Lizenzprüfung – Ist die Lizenz abgelaufen?</li> <li>■ Root-Kennwortprüfung in der virtuellen vRealize Automation-Appliance – Läuft das Kennwort bald ab?</li> </ul> |
| Mandantentests für vRealize Automation | <ul style="list-style-type: none"> <li>■ Überprüfung der Speicherpfade der vSphere-Reservierung</li> <li>■ Überprüfung der Reservierungsrichtlinie für Reservierungszuweisungen</li> <li>■ Überprüfung des Portaldienststatus</li> </ul>                                     |
| Tests für vRealize Orchestrator        | <ul style="list-style-type: none"> <li>■ Überprüfung der Anzahl aktiver vRO-Knoten</li> <li>■ Überprüfung der Nutzung des Java-Speicher-Heaps auf den vRO-Knoten</li> <li>■ Überprüfung des Status des vro-Serverdienstes auf den vRO-Knoten</li> </ul>                      |

Nachdem Sie eine Testsuite auf einer virtuellen Maschine ausgeführt haben, gibt der Integritätsdienst die Anzahl der bestandenen oder fehlgeschlagenen Tests zurück. Für alle fehlgeschlagenen Tests stellt der Integritätsdienst folgende Links bereit:

| Link    | Inhalt                                                            |
|---------|-------------------------------------------------------------------|
| Ursache | Erläuterung zum Fehlschlagen des Tests.                           |
| Lösung  | Informationen, die Sie zum Beheben des Problems verwenden können. |

Sie können den Integritätsdienst zum Ausführen von Tests nach einem Zeitplan oder bei Bedarf konfigurieren.

Sie können auch Python verwenden, um benutzerdefinierte Tests zu erstellen. Weitere Informationen finden Sie im *vRealize Automation Health Service Extensibility Guide*.

Mandantenadministratoren mit der Rolle „Integritätsverbraucher“ können die Testergebnisse für ihre Mandanten einsehen, aber keine Tests konfigurieren oder ausführen.

## Konfigurieren von Systemtests für vRealize Automation

Ein **IaaS-Administrator** konfiguriert den Integritätsdienst zum Ausführen von Systemtests auf einer ausgewählten virtuellen vRealize Automation-Appliance. Mithilfe dieser Tests können Sie feststellen, ob Komponenten wie die vRealize Automation-Lizenz registriert und erforderliche Ressourcen, wie z. B. Arbeitsspeicher, auf der virtuellen Appliance verfügbar sind. Wenn Sie die Systemtests konfigurieren, werden die Tests auf der Seite „Integrität“ als Testkarten angezeigt.

Führen Sie dieses Verfahren durch, um den Integritätsdienst zum Ausführen von Systemtests für vRealize Automation zu konfigurieren.

### Voraussetzungen

Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.

### Verfahren

- 1 Wählen Sie **Verwaltung > Integrität**.
- 2 Klicken Sie auf **Neue Konfiguration**.
- 3 Geben Sie auf der Seite „Konfigurationsdetails“ die angeforderten Informationen ein.

| Option       | Beschreibung                                                                      |
|--------------|-----------------------------------------------------------------------------------|
| Name         | Ihr Titel für diese Konfiguration. Dieser Titel wird auf der Testkarte angezeigt. |
| Beschreibung | Eine Beschreibung der Testsuite.                                                  |
| Produkt      | Wählen Sie vRealize Automation aus.                                               |
| Planen       | Legen Sie fest, wie oft die Testsuite ausgeführt wird.                            |

- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie auf der Seite „Test-Suites auswählen“ **Systemprüfungen für vRealize Automation** aus.
- 6 Klicken Sie auf **Weiter**.
- 7 Geben Sie auf der Seite „Parameter konfigurieren“ die angeforderten Informationen ein.

**Tabelle 1-18. Virtuelle vRealize Automation-Appliance**

| Option                              | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adresse des öffentlichen Webservers | <ul style="list-style-type: none"> <li>■ Bei einer minimalen Bereitstellung ist dies die Basis-URL für den vRealize Automation-Appliance-Host. Beispielsweise <code>https://va-host.domain/</code>.</li> <li>■ Bei einer High Availability-Bereitstellung ist dies die Basis-URL für den vRealize Automation-Lastausgleichsdienst. Beispiel: <code>https://load-balancer-host.domain/</code>.</li> </ul> |
| Adresse der SSH-Konsole             | Vollqualifizierter Domänenname der vRealize Automation-Appliance. Beispiel: <code>va-host.domain</code> .                                                                                                                                                                                                                                                                                                |
| Benutzer der SSH-Konsole            | root                                                                                                                                                                                                                                                                                                                                                                                                     |
| Kennwort der SSH-Konsole            | Das Root-Kennwort.                                                                                                                                                                                                                                                                                                                                                                                       |

Tabelle 1-19. vRealize Automation-Systemmandant

| Option                            | Beschreibung               |
|-----------------------------------|----------------------------|
| Administrator des Systemmandanten | Administrator              |
| Kennwort des Systemmandanten      | Das Administratorkennwort. |

Tabelle 1-20. vRealize Automation-Festplattenspeicherüberwachung

| Option                                | Beschreibung                                                                                                                        |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Warnschwellenwert (in Prozent)        | Zulässiger Prozentsatz des Festplattenspeichers der virtuellen Appliance, der verwendet wird, bevor der Warntest fehlschlägt.       |
| Kritischer Schwellenwert (in Prozent) | Zulässiger Prozentsatz des Festplattenspeichers der virtuellen Appliance, der verwendet wird, bevor der kritische Test fehlschlägt. |

8 Klicken Sie auf **Weiter**.

9 Überprüfen Sie die Informationen auf der Seite „Übersicht“.

10 Klicken Sie auf **Beenden**.

Prüfungen werden nach dem ausgewählten Zeitplan durchgeführt.

#### Nächste Schritte

[Anzeigen der Ergebnisse des vRealize Automation-Integritätsprüfungstests](#)

## Konfigurieren von Mandantentests für vRealize Automation

Ein **laaS-Administrator** konfiguriert den Integritätsdienst zum Ausführen von Mandantentests auf einer ausgewählten virtuellen vRealize Automation-Appliance. Mithilfe dieser Tests können Sie feststellen, ob mandantenbezogene Komponenten wie Softwaredienste registriert und erforderliche Ressourcen wie virtuelle vSphere-Maschinen auf der virtuellen Appliance verfügbar sind. Wenn Sie die Mandantentests konfigurieren, werden die Tests auf der Seite „Integrität“ als Testkarten angezeigt.

Führen Sie dieses Verfahren durch, um den Integritätsdienst zum Ausführen von Mandantentests für vRealize Automation zu konfigurieren.

#### Voraussetzungen

Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.

#### Verfahren

1 Wählen Sie **Verwaltung > Integrität**.

2 Klicken Sie auf **Neue Konfiguration**.

- 3 Geben Sie auf der Seite „Konfigurationsdetails“ die angeforderten Informationen ein.

| Option       | Beschreibung                                                                      |
|--------------|-----------------------------------------------------------------------------------|
| Name         | Ihr Titel für diese Konfiguration. Dieser Titel wird auf der Testkarte angezeigt. |
| Beschreibung | Eine Beschreibung der Tests.                                                      |
| Produkt      | Wählen Sie vRealize Automation aus.                                               |
| Planen       | Wählen Sie aus, wie oft diese Tests ausgeführt werden sollen.                     |

- 4 Klicken Sie auf **Weiter**.

- 5 Wählen Sie auf der Seite „Test-Suites auswählen“ **Mandantentests für vRealize Automation**.

- 6 Klicken Sie auf **Weiter**.

- 7 Geben Sie auf der Seite „Parameter konfigurieren“ die angeforderten Informationen ein.

Tabelle 1-21. Virtuelle vRealize Automation-Appliance

| Option                           | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vRealize Automation-Web-Adresse  | <ul style="list-style-type: none"> <li>■ Bei einer minimalen Bereitstellung ist dies die Basis-URL für den vRealize Automation-Appliance-Host. Beispielsweise <code>https://va-host.domain/</code>.</li> <li>■ Bei einer High Availability-Bereitstellung ist dies die Basis-URL für den vRealize Automation-Lastausgleichsdienst. Beispiel: <code>https://load-balancer-host.domain/</code>.</li> </ul> |
| Adresse der SSH-Konsole          | Vollqualifizierter Domänenname des SSH-Hosts. Beispielsweise <code>ssh-host.domain</code> .                                                                                                                                                                                                                                                                                                              |
| Benutzer der SSH-Konsole         | root                                                                                                                                                                                                                                                                                                                                                                                                     |
| Kennwort der SSH-Konsole         | Kennwort für Root.                                                                                                                                                                                                                                                                                                                                                                                       |
| Max. Antwortzeit für Dienst (ms) | Maximaler Zeitraum in Millisekunden, während dem das System auf eine Antwort wartet.                                                                                                                                                                                                                                                                                                                     |

Tabelle 1-22. vRealize Automation-Mandant

| Option                                 | Beschreibung                                                                                                                                                                                                               |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zu testender Mandant                   | qe                                                                                                                                                                                                                         |
| Benutzername des Fabric-Administrators | <p>Benutzername des Fabric-Administrators.</p> <p><b>Hinweis</b> Dieser Fabric-Administrator muss auch über eine Mandantenadministrator- und eine IaaS-Administratorrolle verfügen, um alle Tests ausführen zu können.</p> |
| Kennwort des Fabric-Administrators     | Kennwort des Fabric-Administrators.                                                                                                                                                                                        |

Tabelle 1-23. vRealize Automation-Systemmandant

| Option                            | Beschreibung                 |
|-----------------------------------|------------------------------|
| Administrator des Systemmandanten | Administrator                |
| Kennwort des Systemmandanten      | Kennwort des Administrators. |

Tabelle 1-24. vRealize Automation-Festplattenspeicherüberwachung

| Option                                | Beschreibung                                                                                                                        |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Kritischer Schwellenwert (in Prozent) | Zulässiger Prozentsatz des Festplattenspeichers der virtuellen Appliance, der verwendet wird, bevor der kritische Test fehlschlägt. |

- 8 Klicken Sie auf **Weiter**.
  - 9 Überprüfen Sie die Informationen auf der Seite „Übersicht“.
  - 10 Klicken Sie auf **Beenden**.
- Prüfungen werden nach dem ausgewählten Zeitplan durchgeführt.

#### Nächste Schritte

[Anzeigen der Ergebnisse des vRealize Automation-Integritätsprüfungstests](#)

## Konfigurieren von Tests für vRealize Orchestrator

Ein **laaS-Administrator** konfiguriert den Integritätsdienst zum Ausführen von Tests für vRealize Orchestrator auf dem vRealize Orchestrator-Host. Diese Tests stellen sicher, dass Komponenten wie der vro-Serverdienst registriert und erforderliche Ressourcen wie ausreichende Java-Arbeitsspeicher-Heaps verfügbar sind. Wenn Sie die vRealize Orchestrator-Tests konfigurieren, werden die Tests auf der Seite „Integrität“ als Testkarten angezeigt.

#### Voraussetzungen

Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.

#### Verfahren

- 1 Wählen Sie **Verwaltung > Integrität**.
- 2 Klicken Sie auf **Neue Konfiguration**.
- 3 Geben Sie auf der Seite „Konfigurationsdetails“ die angeforderten Informationen ein.

| Option       | Beschreibung                                                                      |
|--------------|-----------------------------------------------------------------------------------|
| Name         | Ihr Titel für diese Konfiguration. Dieser Titel wird auf der Testkarte angezeigt. |
| Beschreibung | Eine Beschreibung der Tests.                                                      |

| Option  | Beschreibung                                                |
|---------|-------------------------------------------------------------|
| Produkt | Wählen Sie vRealize Orchestrator aus.                       |
| Planen  | Wählen Sie aus, wie oft die Tests ausgeführt werden sollen. |

- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie auf der Seite „Test-Suites auswählen“ **Tests für vRealize Orchestrator** aus.
- 6 Klicken Sie auf **Weiter**.
- 7 Geben Sie auf der Seite „Parameter konfigurieren“ die angeforderten Informationen ein.

Tabelle 1-25. vRealize Orchestrator-Host/Lastausgleich

| Option                         | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clientadresse                  | <ul style="list-style-type: none"> <li>■ Bei einer minimalen Bereitstellung ist dies der vollqualifizierte Domänenname des vRealize Orchestrator-Hosts. Beispiel: <i>vro-host.domain</i>.</li> <li>■ Bei einer Bereitstellung in einer Hochverfügbarkeitsumgebung ist dies die Basis-URL für den vRealize Orchestrator-Lastausgleichsdienst, <i>https://load-balancer-host.domain/</i>.</li> </ul> |
| Clientbenutzername             | Administrator                                                                                                                                                                                                                                                                                                                                                                                      |
| Clientkennwort                 | Das Administratorkennwort.                                                                                                                                                                                                                                                                                                                                                                         |
| SSH-Konsolen-Benutzername      | root                                                                                                                                                                                                                                                                                                                                                                                               |
| Kennwort der SSH-Konsole       | Das Root-Kennwort.                                                                                                                                                                                                                                                                                                                                                                                 |
| Schwellenwert der Heap-Nutzung | Zulässiger Prozentsatz des Heap-Speichers, der verwendet wird, bevor der Warntest fehlschlägt.                                                                                                                                                                                                                                                                                                     |

Tabelle 1-26. vRealize Orchestrator-Instanzen hinter dem Lastausgleichsdienst

| Option                    | Beschreibung                                                                    |
|---------------------------|---------------------------------------------------------------------------------|
| Adresse der SSH-Konsole   | IP-Adresse oder URL der vRealize Orchestrator-Instanz hinter dem Lastausgleich. |
| SSH-Konsolen-Benutzername | Benutzername mit Zugriff auf diese Instanz.                                     |
| Kennwort der SSH-Konsole  | Das Kennwort für den Benutzernamen.                                             |

- Klicken Sie auf **Hinzufügen**, um eine andere vRealize Orchestrator-Instanz zur Liste hinzuzufügen.
- Klicken Sie auf **Entfernen**, um eine ausgewählte vRealize Orchestrator-Instanz aus der Liste der Instanzen hinter dem Lastausgleich zu entfernen.

- 8 Klicken Sie auf **Weiter**.
- 9 Überprüfen Sie die Informationen auf der Seite „Übersicht“.



**10** Klicken Sie auf **Beenden**.

Prüfungen werden nach dem ausgewählten Zeitplan durchgeführt.

**Nächste Schritte**

[Anzeigen der Ergebnisse des vRealize Automation-Integritätsprüfungstests](#)

**Benutzerdefinierte Testsuite**

Sie können Python verwenden, um eine benutzerdefinierte Testsuite für den vRealize Automation-Integritätsprüfungsdienst zu erstellen.

Durch die Erstellung einer benutzerdefinierten Testsuite können Sie die für den Integritätsprüfungsdienst bereitgestellten Tests erweitern, indem Sie eine Testsuite zur Ermittlung der Integrität zusätzlicher vRealize Automation-Komponenten hinzufügen. Informationen zum Erstellen einer benutzerdefinierten Testsuite finden Sie im *vRealize Automation Health Service Extensibility Guide*.

**Hinzufügen einer benutzerdefinierten Testsuite**

Ein **laaS-Administrator** muss eine benutzerdefinierte Testsuite zum vRealize Automation-Integritätsdienst hinzufügen, bevor Sie die Testsuite ausführen.

Führen Sie dieses Verfahren durch, um eine benutzerdefinierte Testsuite für ein vRealize Automation-Asset hinzuzufügen.

**Voraussetzungen**

- Erstellen Sie ein Python-Wheel für die benutzerdefinierten Testsuitedateien. Informationen dazu finden Sie im *Erweiterbarkeitshandbuch für den vRealize Automation-Integritätsprüfungsdienst*.
- Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.

**Verfahren**

- 1** Klicken Sie auf **Administration > Integrität**.
- 2** Klicken Sie in der oberen rechten Ecke auf das Zahnradsymbol und wählen Sie **Erweiterbarkeit** aus.
- 3** Klicken Sie auf **Neues Asset**.
- 4** Geben Sie im Dialogfeld „Asset hinzufügen“ die erforderlichen Informationen ein.

| Option             | Beschreibung                                                                    |
|--------------------|---------------------------------------------------------------------------------|
| Asset-Titel        | Der Name und die Versionsnummer der ausgeführten Testsuite, z. B. Infoblox 1.0. |
| Asset-Beschreibung | Eine Beschreibung der im Python-Wheel enthaltenen Tests.                        |

| Option        | Beschreibung                                                                                      |
|---------------|---------------------------------------------------------------------------------------------------|
| Asset-Version | Versionsnummer der Testsuite.                                                                     |
| Asset-Datei   | Klicken Sie auf <b>Datei auswählen</b> und wählen Sie die benutzerdefinierten Testsuitedatei aus. |

## 5 Klicken Sie auf **Hinzufügen**.

Eine neue Zeile wird der Asset-Tabelle mit dem Status HOCHGELADEN hinzugefügt. Wenn der Status in INSTALLIERT geändert wird, ist Ihre Testsuite zur Verwendung bereit. Wenn der Installationsprozess fehlschlägt, wird ein Popup-Fenster mit einem Grund angezeigt.

**Hinweis** Wenn die Seite nicht aktualisiert wird, klicken Sie auf das Aktualisierungssymbol.

### Nächste Schritte

[Ausführen einer benutzerdefinierten Testsuite.](#)

## Ausführen einer benutzerdefinierten Testsuite

Ein **laaS-Administrator** konfiguriert den Integritätsdienst zum Ausführen einer benutzerdefinierten Testsuite in der vRealize Automation-Umgebung. Wenn Sie die benutzerdefinierte Testsuite konfigurieren, wird die Testsuite auf der Seite „Integrität“ als Testkarte angezeigt.

Führen Sie dieses Verfahren durch, um den Integritätsdienst zum Ausführen einer benutzerdefinierten Testsuite für vRealize Automation zu konfigurieren.

### Voraussetzungen

- [Hinzufügen einer benutzerdefinierten Testsuite.](#)
- Melden Sie sich bei vRealize Automation als **laaS-Administrator** an.

### Verfahren

- 1 Wählen Sie **Verwaltung > Integrität**.
- 2 Klicken Sie auf **Neue Konfiguration**.
- 3 Geben Sie auf der Seite „Konfigurationsdetails“ die angeforderten Informationen ein.

| Option       | Beschreibung                                                                      |
|--------------|-----------------------------------------------------------------------------------|
| Name         | Ihr Titel für diese Konfiguration. Dieser Titel wird auf der Testkarte angezeigt. |
| Beschreibung | Eine Beschreibung der Testsuite.                                                  |
| Produkt      | Wählen Sie das zu testende Produkt im Dropdown-Menü <b>Produkt</b> aus.           |
| Planen       | Wählen Sie aus, wie oft diese Testsuite ausgeführt werden soll.                   |

- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie auf der Seite „Testsuites auswählen“ die benutzerdefinierte Testsuite aus und klicken Sie auf **Weiter**.
- 6 Geben Sie auf der Seite „Parameter konfigurieren“ die angeforderten Informationen ein und klicken Sie auf **Weiter**.
- 7 Überprüfen Sie die Informationen auf der Seite „Übersicht“ und klicken Sie auf **Beenden**.  
Die benutzerdefinierte Testsuite wird gemäß dem ausgewählten Zeitplan ausgeführt.

#### Nächste Schritte

#### Anzeigen der Ergebnisse des vRealize Automation-Integritätsprüfungstests

### Anzeigen der Ergebnisse des vRealize Automation-Integritätsprüfungstests

Nach Ausführung der Tests können Sie die Ergebnisse des Integritätsdiensttests anzeigen.

Die Seite „Integrität“ zeigt alle konfigurierten Test-Suites als Testkarten an. Wenn eine Test-Suite ausgeführt wird, erscheint das Ergebnis in der Mitte der Testkarte.

Die Testkarten, die auf der Seite „Integrität“ angezeigt werden, werden nach Ihren Berechtigungen gefiltert.

- IaaS-Administratoren werden alle Textkarten angezeigt.
- Mandantenadministratoren mit der Rolle „Integritätsverbraucher“ werden nur die Testkarten Ihrer Mandanten angezeigt.

#### Voraussetzungen

- Die konfigurierte Testsuite wurde planmäßig ausgeführt.
- Melden Sie sich bei der vRealize Automation-Konsole als **IaaS-Administrator** oder **Mandantenadministrator** an.

#### Verfahren

- 1 Wählen Sie **Verwaltung > Integrität**.
- 2 Wenn ein Test nicht für die Ausführung geplant ist, klicken Sie auf der Testkarte auf **Ausführen**.
- 3 Klicken Sie nach Abschluss der Tests auf die Mitte einer Testkarte.

Eine Seite mit dem Status jedes Tests wird angezeigt. Wenn Sie wissen möchten, warum ein Test fehlgeschlagen ist, klicken Sie auf **Ursache**. Zum Öffnen eines Themas, das eine Erklärung zur Lösung des Problems enthält, klicken Sie gegebenenfalls auf den Link **Lösung**.

## Fehlerbehebung des Integritätsdienstes

Die Themen zur Fehlerbehebung des Integritätsdienstes bieten Lösungen für Probleme, die bei der Verwendung des Integritätsdienstes auftreten können.

### Dienststatus-Test schlägt fehl

Sie können die Probleme eines fehlgeschlagenen Dienststatus-Tests beheben, indem Sie die Einstellungen des Testzeitplans ändern.

#### Problem

Wenn ein Dienststatus-Test fehlschlägt und Sie auf **Ursache** klicken, wird diese Meldung angezeigt: SSH-Verbindung kann nicht hergestellt werden; Ausnahmemeldung:[Auth. fehlgeschlagen].

#### Ursache

Wenn die Test-Suite planmäßig alle 15 Minuten ausgeführt wird, blockiert die Systemanmeldung das Root-Benutzerkonto.

#### Lösung

- ◆ Ändern Sie den Testzeitplan in **Keine**, warten Sie 15 Minuten und führen Sie die Test-Suite erneut aus.

### Nach dem Upgrade ist die Seite „Integrität“ in der Appliance-Konsole leer

Nach dem Upgrade von vRealize Automation ist die Seite „Integrität“ in der Appliance-Konsole leer.

#### Problem

Der Integritätsdienst wird nach dem Upgrade nicht gestartet.

#### Lösung

- ◆ Öffnen Sie auf jeder virtuellen vRealize Automation-Appliance eine Eingabeaufforderung als **root** und führen Sie diese Befehle aus.
  - a Um den Integritätsdienst für den automatischen Start zu konfigurieren, führen Sie diesen Befehl aus.  
`chkconfig vrhb-service on`
  - b Um den Integritätsdienst auf dieser virtuellen Appliance zu starten, führen Sie diesen Befehl aus.  
`service vrhb-service start`

## Überwachung von vRealize Automation-Umgebungsressourcen mithilfe von SNMP

Als Systemadministrator, der mit SNMP vertraut ist, möchten Sie die vRealize Automation-REST API für vSNMP verwenden, um die Überwachung Ihrer vRealize Automation-Knoten zu vereinfachen. Mithilfe von vSNMP können Sie SNMP als verschlüsseltes Frühwarnsystem verwenden, wenn kurz bevorsteht, dass nicht mehr genügend CPU, RAM oder Festplattenspeicher für vRealize Automation vorhanden ist, um Verzögerungen zu vermeiden.

Sie können die SNMP-OIDs manuell überwachen oder Ressourcen aktiv überwachen, indem Sie SNMP-Traps festlegen.

Wenn beispielsweise vSNMP Ihnen ein Ereignis sendet, z. B. „Hohe CPU-Auslastung erkannt“, können Sie mit der Erfassung von Informationen zu Prozessen beginnen, die CPU verbrauchen, und ermitteln, welcher davon übermäßig viele Ressourcen in Anspruch nimmt. Sie können dann die CPU, den Arbeitsspeicher und andere Nutzungsdaten korrelieren, um zusätzliche Probleme zu beheben.

Mithilfe von vSNMP für vRealize Automation können Sie die gesamte Linux-Struktur zur Überwachung und zum Abrufen von Daten mithilfe der REST API oder unter Verwendung des auf Ihren vRealize Automation-Instanzen ausgeführten vSNMPD-Daemons offenlegen.

SNMP für vRealize Automation verfügt über keine Schnittstelle für die allgemeine Verwendung. Sie müssen die REST API- oder die Daemon-Befehle verwenden.

Informationen hierzu finden Sie unter „Verwenden von SNMP zum Überwachen von vRealize Automation“ im vRealize Automation-Programmierhandbuch. Das Programmierhandbuch finden Sie in der [Dokumentation zur vRealize Automation-API](#), und indem Sie den Link für die entsprechende Version auswählen.

## Überwachen und Verwalten von Ressourcen

Verschiedene vRealize Automation-Rollen überwachen die Ressourcenverwendung und verwalten Infrastruktur auf unterschiedliche Weise.

### Auswählen eines Ressourcenüberwachungsszenarios

Fabric-Administratoren, Mandantenadministratoren und Business-Gruppenmanager haben bezüglich der Ressourcenüberwachung unterschiedliche Bedenken. Aus diesem Grund ermöglicht vRealize Automation die Überwachung unterschiedlicher Aspekte der Ressourcenauslastung.

Beispielsweise hat ein Fabric-Administrator Bedenken wegen der Überwachung des Ressourcenverbrauchs von Reservierungen und Computing-Ressourcen, während ein Mandantenadministrator sich Gedanken um die Ressourcenauslastung der Bereitstellungsgruppen innerhalb eines Mandanten macht. In Abhängigkeit von Ihrer Rolle und der spezifischen Ressourcenauslastung, die Sie überwachen möchten, ermöglicht vRealize Automation verschiedene Methoden zur Nachverfolgung des Ressourcenverbrauchs.

**Tabelle 1-27. Auswählen eines Ressourcenüberwachungsszenarios**

| <b>Ressourcenüberwachungsszenario</b>                                                                                                                                                                                                                                                                                           | <b>Erforderliche Berechtigungen</b>                                                                                                                                                                                                                                          | <b>Speicherort</b>                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Überwachung des aktuell belegten Umfangs an physischem Speicher und Arbeitsspeicher auf Ihren Computing-Ressourcen sowie Bestimmen des verfügbaren Speichers bzw. Arbeitsspeichers. Sie können auch die Anzahl der reservierten und zugeteilten Maschinen, die auf jeder Computing-Ressource bereitgestellt werden, überwachen. | <b>Fabric-Administrator</b><br>(Ressourcenauslastung auf Computing-Ressourcen in Ihrer Fabric-Gruppe überwachen)                                                                                                                                                             | <b>Infrastruktur &gt; Computing-Ressourcen &gt; Computing-Ressourcen</b> |
| Überwachung der Maschinen, die aktuell bereitgestellt sind und von vRealize Automation verwaltet werden.                                                                                                                                                                                                                        | <b>Fabric-Administrator</b>                                                                                                                                                                                                                                                  | <b>Infrastruktur &gt; Maschinen &gt; Verwaltete Maschinen</b>            |
| Überwachung des aktuell zugeteilten Umfangs an Speicher, Arbeitsspeicher und Maschinenkontingenten Ihrer Reservierung sowie Bestimmen der für die Reservierung verfügbaren Kapazität.                                                                                                                                           | <b>Fabric-Administrator</b><br>(Ressourcenauslastung für Reservierungen auf Ihren Computing-Ressourcen und physischen Maschinen überwachen)                                                                                                                                  | <b>Infrastruktur &gt; Reservierungen &gt; Reservierungen</b>             |
| Überwachung des aktuell verbrauchten Umfangs an Speicher, Arbeitsspeicher und Maschinenkontingenten Ihrer Business-Gruppen sowie Bestimmen der für die Reservierung verfügbaren Kapazität.                                                                                                                                      | <ul style="list-style-type: none"> <li>■ <b>Mandantenadministrator</b><br/>(Ressourcenauslastung für alle Gruppen in Ihrem Mandanten überwachen)</li> <li>■ <b>Business-Gruppenmanager</b><br/>(Ressourcenauslastung für von Ihnen verwaltete Gruppen überwachen)</li> </ul> | <b>Administration &gt; Benutzer und Gruppen &gt; Business-Gruppen</b>    |

## Terminologie der Ressourcenverwendung

vRealize Automation verwendet explizite Terminologie für die Unterscheidung zwischen verfügbaren Ressourcen, Ressourcen, die für spezifische Verwendungen reserviert wurden, und Ressourcen, die aktiv von bereitgestellten Maschinen verarbeitet werden.

Die Tabelle mit der Terminologie der Ressourcenverwendung erklärt die Terminologie, die vRealize Automation zum Anzeigen der Ressourcenverwendung nutzt.

Tabelle 1-28. Terminologie der Ressourcenverwendung

| Begriff           | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Physisch</b>   | Zeigt die tatsächliche Arbeitsspeicher- oder Speicherkapazität einer Computing-Ressource an.                                                                                                                                                                                                                                                                                                         |
| <b>Reserviert</b> | Zeigt das Maschinenkontingent, die Arbeitsspeicher- und Speicherkapazität an, das bzw. die für eine Reservierung reserviert wurde. Wenn beispielsweise eine Computing-Ressource über eine physische Kapazität von 600 GB verfügt und es auf ihr drei Reservierungen für jeweils 100 GB gibt, dann beträgt der reservierte Speicher der Computing-Ressource 300 GB und der reservierte Speicher 50 %. |
| <b>Verwaltet</b>  | Zeigt an, dass die Maschine bereitgestellt ist und sich derzeit unter der vRealize Automation-Verwaltung befindet.                                                                                                                                                                                                                                                                                   |
| <b>Zugeteilt</b>  | Zeigt das Maschinenkontingent, die Arbeitsspeicher- oder Speicherressourcen an, die aktiv von den bereitgestellten Maschinen verarbeitet werden. Erwägen Sie beispielsweise eine Reservierung mit einem Maschinenkontingent von 10. Wenn sich 15 bereitgestellte Maschinen auf ihr befinden, aber nur 6 davon derzeit eingeschaltet sind, beträgt das Maschinenkontingent 60 %.                      |
| <b>Verwendet</b>  | Der Wert der Spalte <b>Verwendet</b> ist immer gleich dem Wert der Spalte <b>Zugeteilt</b> .                                                                                                                                                                                                                                                                                                         |
| <b>Frei</b>       | Gibt die nicht verwendete physische Kapazität in einem Speicherpfad an.                                                                                                                                                                                                                                                                                                                              |

## Herstellen einer Verbindung zu einer Cloud-Maschine

Bei der ersten Verbindung mit einer Cloud-Maschine müssen Sie sich als Administrator anmelden. Dann können Sie die Anmeldedaten hinzufügen, mit denen Sie sich bei der vRealize Automation-Konsole als Benutzer der Maschine anmelden möchten. Von diesem Zeitpunkt an können Sie sich mit Ihren vRealize Automation-Anmeldedaten anmelden.

**Wichtig** Wenn Sie Amazon Web Services verwenden, muss in der Amazon-Maschineninstanz RDP oder SSH aktiviert sein, und die Maschinen müssen in einer Sicherheitsgruppe vorhanden sein, für die die entsprechenden Ports geöffnet sind.

## Erfassen von Benutzeranmeldedaten für eine Amazon-Maschine

Um sich bei einer Amazon-Maschine als Administrator anzumelden, müssen Sie das Administratorkennwort der Maschine in Erfahrung bringen.

Das Administratorkennwort steht auf der Seite mit den Maschineninformationsdetails zur Verfügung. Wenn das Amazon-System-Image, von dem aus die Maschine bereitgestellt wird, nicht zum Generieren des Administratorkennworts bei jedem Start konfiguriert ist, müssen Sie das Kennwort mithilfe einer alternativen Vorgehensweise suchen. Informationen zu anderen Methoden für den Erhalt des Administratorkennworts finden Sie in den Themen *Connect to Your Amazon EC2 Instance* in der Amazon-Dokumentation.

Bei Bedarf können Sie die erforderlichen vRealize Automation-Benutzeranmeldedaten erstellen. Die Benutzeranmeldedaten sind dann für weitere Anmeldungen bei dieser Maschine gültig.

## Voraussetzungen

- Die Amazon-Maschine wurde bereits bereitgestellt.
- Melden Sie sich bei vRealize Automation als Maschinenbesitzer, **Business-Gruppenmanager** oder **Supportbenutzer** an.
- RDP oder SSH ist auf dem Amazon-System-Image aktiv, das für die Bereitstellung verwendet wird.
- Die Maschinen befinden sich in einer Sicherheitsgruppe, in der die richtigen Ports offen sind.

## Verfahren

- 1 Navigieren Sie zur Seite **Elemente** und filtern Sie nach den von Ihnen verwalteten Gruppen oder nach einer bestimmten Gruppe.
- 2 Wählen Sie in der Liste der Maschinen die Amazon-Maschine aus.  
  
Sie können im Dropdown-Menü **Aktionen** auf **Details anzeigen** klicken, um Details wie den Maschinentyp anzuzeigen.
- 3 Wählen Sie im Dropdown-Menü **Aktionen** die Option **Bearbeiten** aus.
- 4 Klicken Sie auf **Administratorkennwort anzeigen**, um das Administratorkennwort der Maschine abzurufen.  
  
Alternativ können Sie das Kennwort mit einem externen Amazon-Verfahren abrufen.
- 5 Wählen Sie im Dropdown-Menü **Aktionen** **Verbindungsherstellung mithilfe von RDP**.
- 6 Wenn Sie zur Eingabe der Anmeldedaten aufgefordert werden, klicken Sie auf **Anderes Konto verwenden**.
- 7 Geben Sie als Benutzernamen **LOCAL\Administrator** ein.
- 8 Geben Sie bei Aufforderung das Administratorkennwort ein.
- 9 Klicken Sie auf **OK**.  
  
Sie sind jetzt als Administrator bei der Maschine angemeldet.
- 10 Fügen Sie nach Bedarf Ihre vRealize Automation-Anmeldedaten hinzu. Beispiel: Öffnen Sie auf einer Windows-Servermaschine den Servermanager und wählen Sie **Konfiguration > Lokale Benutzer und Gruppen** aus. Fügen Sie Ihre Anmeldedaten im Format **DOMAENE\benutzername** zur Gruppe der **Remotedesktopbenutzer** hinzu.  
  
Ihr vRealize Automation-Benutzername und Ihr Kennwort sind jetzt gültige Anmeldedaten für spätere Anmeldungen bei dieser Maschine.
- 11 Melden Sie sich von der Amazon-Maschine ab.
- 12 Wählen Sie im Dropdown-Menü **Aktionen** **Verbindungsherstellung mithilfe von RDP**.
- 13 Wenn Sie zur Anmeldung aufgefordert werden, geben Sie Ihren vRealize Automation-Benutzernamen und Ihr Kennwort ein, um sich bei der Maschine anzumelden.



## Ergebnisse

Maschinenbesitzer können sich jetzt mit ihren vRealize Automation-Anmeldedaten bei der Maschine anmelden.

## Erfassen von Benutzeranmeldedaten für eine vCloud-Maschine

Um sich bei einer vCloud Air- oder vCloud Director-Maschine als Administrator anzumelden, müssen Sie das Administratorkennwort der Maschine in Erfahrung bringen.

Das Administratorkennwort steht auf der Seite mit den Maschineninformationsdetails zur Verfügung. Wenn das Maschinen-Image, von dem aus die Maschine bereitgestellt wird, nicht zum Generieren des Administratorkennworts bei jedem Start konfiguriert ist, können Sie das Kennwort mithilfe einer alternativen Vorgehensweise suchen. Informationen über andere Methoden zum Erhalten des Administratorkennworts finden Sie in der Dokumentation zu vCloud Air oder vCloud Director.

Bei Bedarf können Sie die erforderlichen vRealize Automation-Benutzeranmeldedaten erstellen. Die Benutzeranmeldedaten sind dann für weitere Anmeldungen bei dieser Maschine gültig.

### Voraussetzungen

- Die vCloud Air- oder vCloud Director-Maschine wurde bereits bereitgestellt.
- Melden Sie sich bei vRealize Automation als Maschinenbesitzer, **Business-Gruppenmanager** oder **Supportbenutzer** an.
- RDP oder SSH ist auf dem vCloud Air- oder vCloud Director-Maschinen-Image aktiv, das für die Bereitstellung verwendet wird.
- Die Maschinen befinden sich in einer Sicherheitsgruppe, in der die richtigen Ports offen sind.

### Verfahren

- 1 Navigieren Sie zur Seite **Elemente** und filtern Sie nach den von Ihnen verwalteten Gruppen oder nach einer bestimmten Gruppe.
- 2 Wählen Sie in der Liste der Maschinen die vCloud Air- oder vCloud Director-Maschine aus.  
Sie können im Dropdown-Menü **Aktionen** auf **Details anzeigen** klicken, um Details wie den Maschinentyp anzuzeigen.
- 3 Wählen Sie im Dropdown-Menü **Aktionen** die Option **Bearbeiten** aus.
- 4 Klicken Sie auf **Administratorkennwort anzeigen**, um das Administratorkennwort der Maschine abzurufen.  
Alternativ können Sie das Kennwort mit einem externen vCloud Air- oder vCloud Director-Verfahren abrufen.
- 5 Wählen Sie im Dropdown-Menü **Aktionen** **Verbindungsherstellung mithilfe von RDP**.
- 6 Wenn Sie zur Eingabe der Anmeldedaten aufgefordert werden, klicken Sie auf **Anderes Konto verwenden**.

**7** Geben Sie als Benutzernamen **LOCAL\Administrator** ein.

**8** Geben Sie bei Aufforderung das Administratorkennwort ein.

**9** Klicken Sie auf **OK**.

Sie sind jetzt als Administrator bei der Maschine angemeldet.

**10** Fügen Sie nach Bedarf Ihre vRealize Automation-Anmeldedaten hinzu. Beispiel: Öffnen Sie auf einer Windows-Servermaschine den Servermanager und wählen Sie **Konfiguration > Lokale Benutzer und Gruppen** aus. Fügen Sie Ihre Anmeldedaten im Format **DOMAENE\benutzername** zur Gruppe der **Remotedesktopbenutzer** hinzu.

Ihr vRealize Automation-Benutzername und Ihr Kennwort sind jetzt gültige Anmeldedaten für spätere Anmeldungen bei dieser Maschine.

**11** Melden Sie sich von der vCloud Air- oder vCloud Director-Maschine ab.

**12** Wählen Sie im Dropdown-Menü **AktionenVerbindungsherstellung mithilfe von RDP**.

**13** Wenn Sie zur Anmeldung aufgefordert werden, geben Sie Ihren vRealize Automation-Benutzernamen und Ihr Kennwort ein, um sich bei der Maschine anzumelden.

## Ergebnisse

Maschinenbesitzer können sich jetzt mit ihren vRealize Automation-Anmeldedaten bei der Maschine anmelden.

## Reduzieren der Reservierungsauslastung durch Abgang

Fabric-Administratoren können die Anzahl der Maschinen für eine bestimmte Reservierung langfristig reduzieren, während die Reservierung und die vorhandenen Maschinen, die auf ihr bereitgestellt sind, aktiv bleiben.

Sie können das reservierte Maschinenkontingent, den Arbeitsspeicher und den Speicher einer virtuellen Reservierung auf unter den aktuell zugewiesenen Betrag reduzieren. Dies ermöglicht die weitere Verwaltung von vorhandenen Maschinen, ohne Änderungen vorzunehmen, während die Bereitstellung von neuen Maschinen verhindert wird, bis die Zuteilung unter die neue reservierte Menge fällt.

---

**Hinweis** Da ausgeschaltete virtuelle Maschinen in den Summen des zugewiesenen Arbeitsspeichers und des Maschinenkontingents nicht enthalten sind, verhindert möglicherweise das Reduzieren des Arbeitsspeichers oder die Maschinenzuweisung einer Reservierung, dass gegenwärtig ausgeschaltete Maschinen wieder eingeschaltet werden.

---

Nehmen wir als Beispiel eine Business-Gruppe mit einer Reservierung, die 20 bereitgestellte Maschinen enthält, die in den nächsten 90 Tagen ablaufen werden. Wenn Sie diese Reservierung durch Abgang auf nicht mehr als 15 Maschinen reduzieren möchten, können Sie die Reservierung ändern, um die Quote von 20 Maschinen auf 15 zu reduzieren. Es können keine weiteren Maschinen auf der Reservierung bereitgestellt werden, bis die Anzahl der Maschinen auf der Reservierung durch die anstehenden Ablaufdaten reduziert wird.

## Außerbetriebnahme eines Speicherpfads

Wenn Sie einen Speicherpfad außer Betrieb nehmen und Maschinen in einen neuen Speicherpfad verschieben, muss ein Fabric-Administrator den Speicherpfad in vRealize Automation deaktivieren.

Nachfolgend finden Sie eine allgemeine Übersicht über die erforderlichen Schritte, um einen Speicherpfad außer Betrieb zu nehmen:

- 1 Ein Fabric-Administrator deaktiviert den Speicherpfad für alle Reservierungen, die diesen Speicherpfad verwenden. Siehe [Deaktivieren eines Speicherpfads](#).
- 2 Verschieben Sie die Maschinen in einen neuen Speicherpfad außerhalb von vRealize Automation.
- 3 Warten Sie, bis vRealize Automation die Erfassung von Bestandslistendaten automatisch ausführt, oder starten Sie die Erfassung von Bestandslistendaten manuell. Siehe [Konfigurieren der Datenerfassung für Computing-Ressourcen](#).

### Deaktivieren eines Speicherpfads

Fabric-Administratoren können Speicherpfade in Reservierungen deaktivieren, wenn Speicherpfade außer Betrieb genommen werden.

---



**Hinweis** Überprüfen Sie für jede Reservierung, bei der Sie einen Speicherpfad deaktivieren, ob ausreichend Speicherplatz in anderen aktivierten Speicherpfaden verbleibt.

---

#### Voraussetzungen

Melden Sie sich bei vRealize Automation als **Fabric-Administrator** an.

#### Verfahren

- 1 Wählen Sie **Infrastruktur > Reservierungen > Reservierungen** aus.
- 2 Zeigen Sie auf die Reservierung, in der der Speicherpfad, den Sie außer Betrieb nehmen, verwendet wird, und klicken Sie auf **Bearbeiten**.
- 3 Klicken Sie auf die Registerkarte **Ressourcen**.
- 4 Suchen Sie den Speicherpfad, den Sie außer Betrieb nehmen.
- 5 Klicken Sie auf das Symbol **Bearbeiten** (.
- 6 Aktivieren Sie das Kontrollkästchen in der Spalte „Deaktiviert“, um diesen Speicherpfad zu deaktivieren.
- 7 Klicken Sie auf das Symbol **Speichern** (.
- 8 Klicken Sie auf **OK**.
- 9 Wiederholen Sie diesen Vorgang für alle Reservierungen, die den Speicherpfad verwenden, den Sie außer Betrieb nehmen.

## Datenerfassung

vRealize Automation erfasst Daten von Infrastrukturquellen-Endpoints und deren Computing-Ressourcen.

Die Datenerfassung erfolgt in regelmäßigen Intervallen. Für jeden Datenerfassungstyp gilt ein Standardintervall, das Sie überschreiben oder ändern können. Für jeden Datenerfassungstyp gilt außerdem ein standardmäßiges Zeitüberschreitungsintervall, das Sie überschreiben oder ändern können.

IaaS-Administratoren können die Datenerfassung für Infrastrukturquellen-Endpoints und Fabric-Administratoren die Datenerfassung für Computing-Ressourcen manuell initiieren.

**Tabelle 1-29. Datenerfassungstypen**

| Datenerfassungstyp                                | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Datenerfassung für Infrastrukturquellen-Endpoints | <p>Aktualisiert Informationen über Virtualisierungshosts, Vorlagen und ISO-Images für Virtualisierungsumgebungen. Aktualisiert virtuelle Datencenter und Vorlagen für vCloud Director. Aktualisiert Amazon-Regionen und in Amazon-Regionen bereitgestellte Maschinen.</p> <p>Die Endpoint-Datenerfassung wird alle vier Stunden ausgeführt.</p>                                                                                                                                                                                                                                                                 |
| Erfassung von Bestandslistendaten                 | <p>Aktualisiert den Datensatz der virtuellen Maschinen, deren Ressourcennutzung an eine spezielle Computing-Ressource gebunden ist, einschließlich detaillierter Informationen über Netzwerke, Speicher und virtuelle Maschinen. Dieser Datensatz enthält zudem Informationen über nicht verwaltete virtuelle Maschinen, d. h. Maschinen, die außerhalb von vRealize Automation bereitgestellt werden.</p> <p>Die Erfassung von Bestandslistendaten wird alle 24 Stunden ausgeführt.</p> <p>Das standardmäßige Zeitüberschreitungsintervall für die Erfassung von Bestandslistendaten beträgt zwei Stunden.</p> |
| Erfassung von Zustandsdaten                       | <p>Aktualisiert den Datensatz des Betriebszustands für jede durch die Bestandslistendatenerfassung ermittelte Maschine. Bei der Zustandsdatenerfassung werden auch fehlende Maschinen erfasst, die von vRealize Automation verwaltet werden, aber in der Virtualisierungs-Computing-Ressource oder im Cloud-Endpoint nicht ermittelt werden können.</p> <p>Die Zustandsdatenerfassung wird alle 15 Minuten ausgeführt.</p> <p>Das standardmäßige Zeitüberschreitungsintervall für die Zustandsdatenerfassung beträgt eine Stunde.</p>                                                                           |

Tabelle 1-29. Datenerfassungstypen (Fortsetzung)

| Datenerfassungstyp                                                                            | Beschreibung                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Leistungsdatenerfassung (nur Computing-Ressourcen von vSphere)                                | <p>Aktualisiert den Datensatz der durchschnittlichen CPU-, Speicherplatz-, Arbeitsspeicher- und Netzwerkauslastung für jede durch die Bestandslistendatenerfassung ermittelte virtuelle Maschine.</p> <p>Die Leistungsdatenerfassung wird alle 24 Stunden ausgeführt.</p> <p>Das standardmäßige Zeitüberschreitungsintervall für die Leistungsdatenerfassung beträgt zwei Stunden.</p> |
| Erfassung von Netzwerk- und Sicherheitsbestandslistendaten (nur vSphere-Computing-Ressourcen) | <p>Aktualisiert den Datensatz der Netzwerk- und Sicherheitsdaten im Zusammenhang mit vCloud Networking and Security und NSX, insbesondere Informationen über Sicherheitsgruppen und Lastausgleich, für jede durch die Bestandslistendatenerfassung ermittelte Maschine.</p>                                                                                                            |
| Erfassung von WMI-Daten (nur Windows-Computing-Ressourcen)                                    | <p>Aktualisiert den Datensatz der Verwaltungsdaten für jede Windows-Maschine. Um Daten von Windows-Maschinen erfassen zu können, muss ein WMI-Agent installiert (normalerweise auf dem Manager Service-Host) und aktiviert sein.</p>                                                                                                                                                   |

## Manuelles Starten der Endpoint-Datenerfassung

Die Endpoint-Datenerfassung wird automatisch alle vier Stunden ausgeführt. IaaS-Administratoren können eine Endpoint-Datenerfassung jedoch jederzeit für jene Endpoints manuell starten, die keine Proxy-Agents benötigen.

Die Seite **Data Collection** liefert Informationen über den Status und das Alter von Datenerfassungen und ermöglicht Ihnen das manuelle Starten einer neuen Endpoint-Datenerfassung.

### Voraussetzungen

Melden Sie sich bei vRealize Automation als **IaaS-Administrator** an.

### Verfahren

- 1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.
- 2 Klicken Sie in die Zeile des Endpoints, von dem Sie Daten erfassen möchten.
- 3 Wählen Sie eine verfügbare Datenerfassungsaktion aus.

## Konfigurieren der Datenerfassung für Computing-Ressourcen

Sie können die Datenerfassung aktivieren bzw. deaktivieren, die Häufigkeit der Datenerfassung konfigurieren oder die Datenerfassung manuell anfordern.

Die Seite **Datenerfassung** enthält Informationen zum Status und Alter von Datenerfassungen. Darüber hinaus können Sie hier die Datenerfassung für Ihre Computing-Ressourcen konfigurieren.

## Voraussetzungen

Melden Sie sich bei vRealize Automation als **Fabric-Administrator** an.

## Verfahren

- 1 Wählen Sie **Infrastruktur > Computing-Ressourcen > Computing-Ressourcen** aus.
- 2 Zeigen Sie auf die Computing-Ressource, für die die Datenerfassung konfiguriert werden soll, und klicken Sie auf **Datenerfassung**.
- 3 Konfigurieren Sie Datenerfassungsspezifikationen für die Option **Computing-Ressource**.
  - Wählen Sie **Ein**, um die Datenerfassung zu aktivieren.
  - Wählen Sie **Aus**, um die Datenerfassung zu deaktivieren.
- 4 Konfigurieren Sie die Datenerfassung für die Option **Bestandsliste**.
  - Wählen Sie **Ein**, um die Datenerfassung zu aktivieren.
  - Wählen Sie **Aus**, um die Datenerfassung zu deaktivieren.
  - Geben Sie in das Textfeld **Häufigkeit** eine Zahl ein, um das Zeitintervall (in Stunden) für die Erfassung von Bestandslistendaten zu konfigurieren.
  - Klicken Sie auf **Jetzt anfordern**, um die Datenerfassung manuell zu starten.
- 5 Konfigurieren Sie die Datenerfassung für die Option **Zustand**.
  - Wählen Sie **Ein**, um die Datenerfassung zu aktivieren.
  - Wählen Sie **Aus**, um die Datenerfassung zu deaktivieren.
  - Geben Sie in das Textfeld **Häufigkeit** eine Zahl ein, um das Zeitintervall (in Minuten) für die Erfassung von Statusdaten zu konfigurieren.
  - Klicken Sie auf **Jetzt anfordern**, um die Datenerfassung manuell zu starten.
- 6 Konfigurieren Sie die Datenerfassung für die Option **Leistung**.

Diese Option ist nur für vSphere-Integrationen verfügbar.

  - Wählen Sie **Ein**, um die Datenerfassung zu aktivieren.
  - Wählen Sie **Aus**, um die Datenerfassung zu deaktivieren.
  - Geben Sie in das Textfeld **Häufigkeit** eine Zahl ein, um das Zeitintervall (in Stunden) für die Erfassung von Leistungsdaten zu konfigurieren.
  - Klicken Sie auf **Jetzt anfordern**, um die Datenerfassung manuell zu starten.
- 7 Konfigurieren Sie die Datenerfassung für die Option **Snapshot-Bestandsliste**.

Diese Option ist für Computing-Ressourcen verfügbar, die von vRealize Business for Cloud verwaltet werden.

  - Wählen Sie **Ein**, um die Datenerfassung zu aktivieren.
  - Wählen Sie **Aus**, um die Datenerfassung zu deaktivieren.

- Geben Sie in das Textfeld **Häufigkeit** eine Zahl ein, um das Zeitintervall (in Stunden) für die Erfassung von Snapshot-Daten zu konfigurieren.
- Klicken Sie auf **Jetzt anfordern**, um die Datenerfassung manuell zu starten.

8 Klicken Sie auf **OK**.

## Aktualisieren von Kostendaten für alle Computing-Ressourcen

Fabric-Administratoren können Kostenangaben für alle durch vRealize Business for Cloud verwalteten Computing-Ressourcen manuell aktualisieren.

### Voraussetzungen

Melden Sie sich bei vRealize Automation als **Fabric-Administrator** an.

### Verfahren

- 1 Wählen Sie **Infrastruktur > Computing-Ressourcen > Computing-Ressourcen** aus.
- 2 Klicken Sie auf **Kosten aktualisieren**.
- 3 Klicken Sie auf **Jetzt anfordern**.

### Ergebnisse

Wenn das Aktualisieren der Kostendaten abgeschlossen ist, wird der Status in „Erfolgreich“ geändert.

## Grundlegende Informationen zur vSwap-Zuteilungsprüfung für vCenter Server-Endpoints

Mithilfe von vSwap können Sie den verfügbaren Auslagerungsbereich für die maximale Größe der Auslagerungsdatei auf einer Zielformaschine bestimmen. Die vSwap-Prüfung erfolgt, wenn Sie eine virtuelle Maschine in vRealize Automation erstellen oder neu konfigurieren. Die vSwap-Zuteilungsprüfung ist nur für vCenter Server-Endpoints verfügbar.

Die vRealize Automation-Speicherzuteilung prüft, ob bei einer Erstellungs- oder Neukonfigurationsanforderung im Datenspeicher ausreichend Speicherplatz für die VM-Festplatten verfügbar ist. Wenn die Maschine jedoch eingeschaltet wird und nicht genügend Speicherplatz zum Erstellen der Auslagerungsdateien auf dem vCenter Server-Endpoint verfügbar ist, kann die Maschine nicht eingeschaltet werden. Wenn das Einschalten fehlschlägt, schlagen auch alle von der Maschine abhängigen Anpassungen fehl. Die Maschine ist möglicherweise auch nicht verfügbar. In Abhängigkeit von der Größe der Anforderung wird Feedback, dass die Maschine nicht eingeschaltet oder nicht bereitgestellt wird, nicht sofort angezeigt.

Mithilfe der vSwap-Zuteilungsprüfung können Sie diese Beschränkungen überwinden, indem Sie den verfügbaren Auslagerungsbereich für die maximale Größe der Auslagerungsdatei im Rahmen des Erstellungs- und Neukonfigurationsprozesses von vRealize Automation für vCenter Server-Endpoints prüfen. Zum Aktivieren der vSwap-Zuteilungsprüfung legen Sie die benutzerdefinierte Eigenschaft `VirtualMachine.Storage.ReserveMemory` in der Maschinenkomponenten oder im gesamten Maschinen-Blueprint auf „True“ fest.

Berücksichtigen Sie das folgende Verhalten für vSwap-Zuteilungsprüfungen:

- Die Auslagerungsdatei befindet sich im Datenspeicher, der die virtuelle Maschine enthält. Alternative vCenter Server-Konfigurationen für die Suche nach Auslagerungsdateien in einem dedizierten oder anderen Datenspeicher werden nicht unterstützt.
- Die Größe der Auslagerungsdatei wird beim Erstellen oder Neukonfigurieren einer virtuellen Maschine berücksichtigt. Die maximale Auslagerungsgröße ist die Größe des Arbeitsspeichers der virtuellen Maschine.
- Reservierte Werte für vRealize Automation-Speicherreservierungen in einem Host dürfen die physische Kapazität der Computing-Ressource nicht überschreiten.
- Beim Erstellen einer Reservierung darf die Summe der reservierten Werte den verfügbaren Speicherplatz nicht überschreiten.
- Arbeitsspeicherreservierungen auf Ressourcenpool-, Host- oder VM-Ebene in vSphere werden nicht für den vSphere-Endpoint erfasst und werden nicht für die Berechtigungen in vRealize Automation berücksichtigt.
- Der verfügbare Auslagerungsbereich wird von vSwap beim Einschalten für vorhandene Maschinen nicht validiert.
- Sie müssen die Datenerfassung erneut ausführen, um am vSphere-Endpoint vorgenommene Änderungen im Hinblick auf vSwap zu erfassen.

## Entfernen der Datencenter-Standorte

Um einen Datencenter-Standort aus einem Benutzermenü zu entfernen, muss ein Systemadministrator die Standortinformationen aus der Standortdatei entfernen, und ein Fabric-Administrator muss die Standortinformationen aus der Computing-Ressource entfernen.

Wenn Sie beispielsweise London zur Standortdatei hinzufügen, zehn Computing-Ressourcen mit diesem Standort verknüpfen und anschließend London aus der Datei entfernen, sind die Computing-Ressourcen immer noch mit dem Standort London verknüpft, und London ist immer noch in der Standort-Dropdownliste auf der Seite „Maschinenanforderung bestätigen“ enthalten. Um den Standort aus der Dropdownliste zu entfernen, muss ein Fabric-Administrator die Computing-Ressource bearbeiten und den Standort für alle Computing-Ressourcen auf „leer“ zurücksetzen, die mit dem Standort verknüpft sind.



Im Folgenden finden Sie eine grobe Übersicht über die Abfolge der Schritte, die für das Entfernen eines Datacenter-Standorts erforderlich sind:

- 1 Ein Systemadministrator entfernt die Informationen zum Datacenterstandort aus der Standortdatei.
- 2 Ein Fabric-Administrator entfernt alle Verknüpfungen der Computing-Ressourcen mit dem Standort, indem er die Standorte von jeder verknüpften Computing-Ressource bearbeitet.

## Überwachen von Containern

Sie können den Status eines Containers überwachen, den Sie in Container für vRealize Automation erstellen.

Sobald Sie Ihre Container auf Grundlage einer Vorlage erstellt haben, können Sie ihren Zustand überwachen. Wenn Sie auf einem Container auf **Details** klicken, können Sie die Netzwerkbandbreite, CPU- und Arbeitsspeichernutzung, Protokolle und Eigenschaften dieses Containers überwachen.

## Massenimport, -update oder -migration von virtuellen Maschinen

Sie können mit der Funktion Massenimporte virtuelle Maschinen in vRealize Automation importieren, migrieren oder aktualisieren. Massenimporte vereinfacht die Verwaltung mehrerer Maschinen in mehreren Umgebungen.

Massenimporte erstellt eine CSV-Datei, die definierende Daten zur virtuellen Maschine wie z. B. Reservierung, Speicherpfad, Blueprint, Besitzer und benutzerdefinierte Eigenschaften enthält. Sie verwenden die CSV-Datei, um virtuelle Maschinen in Ihre vRealize Automation-Umgebung zu importieren. Massenimporte unterstützt die folgenden Verwaltungsaufgaben:

- Importieren von einer oder mehreren nicht verwalteten virtuellen Maschinen, sodass sie in einer vRealize Automation-Umgebung verwaltet werden können.
- Globale Änderung einer Eigenschaft (z. B. Speicherpfad) der virtuellen Maschine.
- Migrieren einer virtuellen Maschine von einer vRealize Automation-Umgebung in eine andere.

---

**Hinweis** Nur vCloud Director und vSphere werden für den Massenimport unterstützt. Die Festlegung des Filters auf einen anderen Endpoint-Typ erzeugt keine Daten in der CSV-Datei.

---

Sie können die Befehle der Massenimporte-Funktion entweder über die vRealize Automation-Konsole oder die Befehlszeilenschnittstelle CloudUtil ausführen. Weitere Informationen zur Verwendung der Befehlszeilenschnittstelle CloudUtil finden Sie in der Dokumentation zu *Lebenszyklus-Erweiterbarkeit*.

**Hinweis** Beim Massenimport von Maschinen werden normale Bereitstellungsschritte nicht umgangen. Alle vorhandenen externen Workflows, die vom Ereignis-Broker während der Bereitstellung ausgelöst werden, werden für importierte Maschinen ausgeführt. Sie können Workflows für importierte Maschinen vorübergehend deaktivieren, indem Sie eine der folgenden Optionen durchführen:

- Deaktivieren Sie alle Ereignis-Broker-Abonnements. Wenn Sie Abonnements deaktivieren, müssen Sie einen Dienstausfall für Ihren vRealize Automation-Cluster planen, da die Erweiterbarkeit auf keine der während dieser Zeit bereitgestellten normalen Maschinen angewendet wird.
- Fügen Sie eine Bedingung zu Ereignisabonnements hinzu, damit das jeweilige Ereignis beim Importieren einer Maschine nicht ausgelöst wird. Um diese Bedingung hinzuzufügen, navigieren Sie zu „Ereignisabonnements“, wählen Sie das zu deaktivierende Abonnement aus und fügen Sie die benutzerdefinierte Eigenschaft `VirtualMachine.Imported.ConvergedBlueprint` ungleich `<ID des Import-Blueprints>` hinzu. Diese Bedingung wirkt sich nicht auf normal bereitgestellte Maschinen aus und wird nur auf importierte Maschinen angewendet.

#### Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Fabric-Administrator** und als **Business-Gruppenmanager** an.
- Wenn Sie virtuelle Maschinen importieren, die statische IP-Adressen verwenden, bereiten Sie einen ordnungsgemäß konfigurierten Adressenpool vor.

## Importieren einer virtuellen Maschine in eine vRealize Automation-Umgebung

Sie können eine nicht verwaltete virtuelle Maschine in eine vRealize Automation-Umgebung importieren.

Eine nicht verwaltete virtuelle Maschine ist in einem Hypervisor vorhanden, wird aber in einer vRealize Automation-Umgebung nicht verwaltet und kann nicht in der Konsole angezeigt werden. Nach dem Import einer nicht verwalteten virtuellen Maschine wird diese unter Verwendung der vRealize Automation-Verwaltungsschnittstelle verwaltet. Je nach Ihren Rechten wird die virtuelle Maschine auf der Registerkarte **Verwaltete Maschinen** oder der Registerkarte **Bereitstellungen** angezeigt.

Die Massenimportoption bietet keine Unterstützung für Bereitstellungen, die über einen Blueprint erfolgen, der eine NSX-Netzwerk- und Sicherheitskomponente oder eine Softwarekomponente enthält.

## Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Fabric-Administrator** und als **Business-Gruppenmanager** an.
- Wenn Sie virtuelle Maschinen importieren, die statische IP-Adressen verwenden, bereiten Sie einen ordnungsgemäß konfigurierten Adressenpool vor. Weitere Informationen über die Verwendung eines Netzwerkprofils zur Steuerung von IP-Adressbereichen finden Sie unter *Konfigurieren von vRealize Automation*.
- Wenn Sie zum Importieren einer virtuellen Maschine mit einer statischen IP-Adresse, die einer anderen virtuellen Maschine zugeteilt ist, den Massenimport verwenden, schlägt der Import fehl.

## Verfahren

- 1 Deaktivieren Sie vorübergehend alle Event Broker-Abonnements.

---

**Hinweis** Beim Deaktivieren von Abonnements müssen Sie einen Dienstausschlag für Ihren vRealize Automation-Cluster einplanen. Während dieses Vorgangs wird die Erweiterbarkeit auf keine normal bereitgestellte Maschine angewendet. Werden die Abonnements nicht deaktiviert, kann dies zu Datenverlust oder zur dauerhaften Löschung von Maschinen aus der Backing-Infrastruktur führen.

---

- 2 Generieren der CSV-Datendatei einer virtuellen Maschine.
  - a Wählen Sie **Infrastruktur > Administration > Massenimporte** aus.
  - b Klicken Sie auf **CSV-Datei generieren**.
  - c Wählen Sie im Dropdown-Menü **Maschinen** den Eintrag **Nicht verwaltet** aus.
  - d Wählen Sie im Dropdown-Menü den Standardwert **Business-Gruppe** aus.
  - e Geben Sie den Standardwert **Besitzer** ein.
  - f Wählen Sie im Dropdown-Menü den Standardwert **Blueprint** aus.

Der Blueprint muss veröffentlicht und einer Berechtigung hinzugefügt werden, damit der Import erfolgreich ausgeführt wird.

- g Wählen Sie im Dropdown-Menü den Standardwert **Komponentenmaschine** aus.

Wenn Sie einen Wert für **Business-Gruppe** und **Blueprint** auswählen, werden in der CSV-Datendatei möglicherweise die folgenden Ergebnisse angezeigt:

- Host Reservation (Name or ID) = INVALID\_RESERVATION
- Host To Storage (Name or ID) = INVALID\_HOST\_RESERVATION\_TO\_STORAGE

Diese Meldungen werden angezeigt, wenn Sie in der ausgewählten Business-Gruppe für die virtuelle Hostmaschine, auf der auch die nicht verwaltete virtuelle Maschine gehostet ist, nicht über eine Reservierung verfügen. Wenn Sie in dieser Business-Gruppe für den Host der nicht verwalteten Maschine über eine Reservierung verfügen, werden die Werte „Hostreservierung“ und „Host zu Speicher“ ordnungsgemäß eingegeben.

- h Wählen Sie im Dropdown-Menü **Ressource** einen der verfügbaren Ressourcentypen aus.

| Menüoption                 | Beschreibung                                                                                                               |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Endpoint</b>            | Erforderliche Informationen für den Zugriff auf einen Virtualisierungshost.                                                |
| <b>Computing-Ressource</b> | Erforderliche Informationen für den Zugriff auf eine Gruppe von virtuellen Maschinen, die ähnliche Funktionen durchführen. |

- i Wählen Sie aus dem Dropdown-Menü **Name** den Namen der VM-Ressource aus.
- j Klicken Sie auf **OK**.

### 3 Bearbeiten der CSV-Datendatei einer virtuellen Maschine.

- a Öffnen Sie die CSV-Datei und bearbeiten Sie die Datenkategorien, sodass sie mit den vorhandenen Kategorien in der vRealize Automation-Zielumgebung übereinstimmen.

Um die in einer CSV-Datendatei enthaltenen virtuellen Maschinen zu importieren, muss jede virtuelle Maschine den folgenden Elementen zugeordnet werden:

- Reservierung
- Speicherort
- Blueprint
- Komponente der virtuellen Maschine
- Besitzer, der in der Zielbereitstellung vorhanden ist

Für jede virtuelle Maschine müssen alle Werte in der vRealize Automation-Zielumgebung vorhanden sein, damit der Importvorgang ordnungsgemäß durchgeführt werden kann. Sie können die Werte für die Reservierung, den Speicherort, den Blueprint und den Besitzer ändern oder den Wert für eine statische IP-Adresse zu einzelnen virtuellen Maschinen hinzufügen, indem Sie die CSV-Datei bearbeiten.

| Überschrift                     | Kommentar                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| # Import—Yes or No              | Ändern Sie die Option in „Nein“, um zu verhindern, dass eine bestimmte virtuelle Maschine importiert wird.                                                                                                                                                                                                                                                                                                                                                            |
| Name der virtuellen Maschine    | Nicht ändern                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ID der virtuellen Maschine      | Nicht ändern                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Hostreservierung (Name oder ID) | Geben Sie den Namen oder die ID einer Reservierung in der vRealize Automation-Zielumgebung ein.                                                                                                                                                                                                                                                                                                                                                                       |
| Host zu Speicher (Name oder ID) | Geben Sie den Namen oder die ID eines Speicherorts in der vRealize Automation-Zielumgebung ein.                                                                                                                                                                                                                                                                                                                                                                       |
| Bereitstellungsname             | <p>Geben Sie für die Bereitstellung, die Sie in der vRealize Automation-Zielumgebung erstellen, einen neuen Namen ein (zum Beispiel den Namen der virtuellen Maschine).</p> <p><b>Hinweis</b> Jede virtuelle Maschine muss in ihre eigene Bereitstellung importiert werden. Sie können keine einzelne virtuelle Maschine in eine vorhandene Bereitstellung importieren. Sie können nicht mehrere virtuelle Maschinen in eine einzelne Bereitstellung importieren.</p> |
| Blueprint-ID                    | <p>Geben Sie die ID des Blueprints in die vRealize Automation-Zielumgebung ein, die Sie zum Importieren der virtuellen Maschine verwenden.</p> <p><b>Hinweis</b> Geben Sie nur die ID und nicht den Namen des Blueprints ein. Sie müssen einen Blueprint auswählen, der nur eine einzige Komponente einer virtuellen Maschine enthält. Der Blueprint muss veröffentlicht und einer Berechtigung hinzugefügt werden.</p>                                               |

| Überschrift                | Kommentar                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | Ordnen Sie für importierte virtuelle Maschinen keine Blueprints zu, die Komponentenprofile enthalten. Vorhandene Einstellungen auf importierten virtuellen Maschinen, wie z. B. Arbeitsspeicher oder Speichergröße, liegen möglicherweise außerhalb der Grenzwerte für Profile. In diesem Fall schlägt die Validierung für jede künftige auf Blueprints basierende Neukonfiguration der virtuellen Maschinen fehl. |
| ID der Komponentenmaschine | Geben Sie den Namen der Komponente einer virtuellen Maschine ein, die im ausgewählten Blueprint enthalten ist. Sie können keine virtuelle Maschine in einen Blueprint importieren, der mehr als eine Komponente beinhaltet.                                                                                                                                                                                        |
| Name des Besitzers         | Geben Sie einen Benutzer in die vRealize Automation-Zielumgebung ein, die für den Blueprint berechtigt ist.                                                                                                                                                                                                                                                                                                        |

Wenn Sie eine virtuelle Maschine mit einer oder mehreren benutzerdefinierten Eigenschaften importieren, geben Sie jede benutzerdefinierte Eigenschaft mit drei durch Komma getrennte Werten an, die an die Zeile mit den Werten für diese Maschine angehängt werden. Verwenden Sie dieses Format für jede benutzerdefinierte Eigenschaft.

*,Custom.Property.Name, Wert, FLAGS*

FLAGS sind drei Zeichen, die beschreiben, wie die Eigenschaft von vRealize Automation behandelt wird. Die Flags sind der Reihenfolge ihrer Nutzung nach:

- 1 H oder N = Ausgeblendet oder Nicht ausgeblendet
- 2 E oder O = Verschlüsselt oder Nicht verschlüsselt
- 3 R oder P = Laufzeit oder Nicht Laufzeit

Beispielsweise können Sie eine benutzerdefinierte Eigenschaft zum Konfigurieren einer statischen IP-Adresse für eine Maschine anhängen. Mit dem folgenden Format teilt diese benutzerdefinierte Eigenschaft eine verfügbare statische IP-Adresse aus einem Netzwerkprofil zu.

*,VirtualMachine.Network#.Address, w.x.y.z, HOP*

Sie ändern die Variablen mit den entsprechenden Informationen für Ihre virtuelle Maschine.

- Ändern Sie das Zeichen # in die Nummer der Netzwerkschnittstelle, die mit dieser statischen IP-Adresse konfiguriert wird. Beispielsweise `VirtualMachine.Network0.Address`.
- Ändern Sie *w.x.y.z* in die statische IP-Adresse für die virtuelle Maschine. Beispielsweise `11.27.42.57`.

Die Zeichenfolge des HOP-Flags – „Ausgeblendet“, „Nicht verschlüsselt“, „Nicht Laufzeit“ – legt die Sichtbarkeit der Eigenschaft fest. Da diese bestimmte Eigenschaft nur vom Massenimport verwendet wird, wird sie nach einem erfolgreichen Import aus der virtuellen Maschine entfernt.

Damit diese benutzerdefinierte Eigenschaft funktioniert, muss die IP-Adresse in einem ordnungsgemäß konfigurierten Adressenpool verfügbar sein. Wenn die IP-Adresse nicht gefunden werden kann oder bereits verwendet wird, ist der Import ohne die Definition der statischen IP-Adresse erfolgreich und ein Fehler wird protokolliert.

- b Speichern Sie die CSV-Datei.
- 4 Verwenden Sie die vRealize Automation-Verwaltungsschnittstelle, um Ihre virtuelle Maschine in eine vRealize Automation-Umgebung zu importieren.
  - a Wählen Sie **Infrastruktur > Administration > Massenimporte** aus.
  - b Klicken Sie auf **Neu**.
  - c Geben Sie im Textfeld **Name** einen eindeutigen Namen für diese Aufgabe ein. Beispiel: nicht verwalteter Import 10.
  - d Geben Sie im Textfeld **CSV-Datei** den Namen der CSV-Datei ein, indem Sie zum Namen der CSV-Datei navigieren.
  - e Wählen Sie Importoptionen aus.

| Option                                  | Beschreibung                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Startzeit</b>                        | Legen Sie ein zukünftiges Startdatum fest. Die ausgewählte Startzeit richtet sich nach der Ortszeit des Servers und nicht nach der Ortszeit der Workstation des Benutzers.                                                                                                                                                  |
| <b>Jetzt</b>                            | Importvorgang direkt starten.                                                                                                                                                                                                                                                                                               |
| <b>Verzögerung (Sekunden)</b>           | Wenn Sie zahlreiche virtuelle Maschinen importieren, wählen Sie die Anzahl der Sekunden aus, um die die Registrierung jeder virtuellen Maschine verzögert werden soll. Bei Auswahl dieser Menüoption wird der Importvorgang verlangsamt. Lassen Sie das Feld leer, wenn Sie keine Verzögerung auswählen möchten.            |
| <b>Batchgröße</b>                       | Wenn Sie zahlreiche virtuelle Maschinen importieren, wählen Sie die Gesamtanzahl der virtuellen Maschinen aus, die innerhalb eines bestimmten Zeitraums registriert werden sollen. Bei Auswahl dieser Menüoption wird der Importvorgang verlangsamt. Lassen Sie das Feld leer, wenn Sie keinen Grenzwert auswählen möchten. |
| <b>Verwaltete Maschinen ignorieren</b>  | Behalten Sie die Deaktivierung bei.                                                                                                                                                                                                                                                                                         |
| <b>Benutzervalidierung überspringen</b> | Bei Auswahl dieser Menüoption wird der Besitzer der virtuellen Maschine auf den Wert festgelegt, der in der Spalte „Besitzer“ der CSV-Datendatei aufgeführt ist, ohne dass überprüft wird, ob der Benutzer vorhanden ist. Bei Auswahl dieser Menüoption nimmt die Zeit für den Import möglicherweise ab.                    |
| <b>Import testen</b>                    | Testen Sie den Importvorgang, ohne die virtuellen Maschinen zu importieren, sodass Sie Ihre CSV-Datei auf Fehler überprüfen können.                                                                                                                                                                                         |

- f Klicken Sie auf **OK**.

Der Fortschritt des Vorgangs wird auf der Seite Massenimporte angezeigt.

## Aktualisieren einer virtuellen Maschine in einer vRealize Automation-Umgebung

Sie können eine Änderung an einer Eigenschaft für eine virtuelle Maschine vornehmen, zum Beispiel an einem Speicherpfad, um mindestens eine verwaltete virtuelle Maschine in einer vRealize Automation-Umgebung zu aktualisieren.

Eine verwaltete virtuelle Maschine ist eine Maschine, die in einer vRealize Automation-Umgebung verwaltet wird und in der Konsole angezeigt werden kann.

### Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Fabric-Administrator** und als **Business-Gruppenmanager** an.

### Verfahren

- 1 Generieren der CSV-Datendatei einer virtuellen Maschine.
  - a Wählen Sie **Infrastruktur > Administration > Massenimporte** aus.
  - b Klicken Sie auf **CSV-Datei generieren**.
  - c Wählen Sie im Dropdown-Menü **Maschinen** den Eintrag **Verwaltet** aus.
  - d Wählen Sie im Dropdown-Menü **Ressource** einen der verfügbaren Ressourcentypen aus.

| Option                     | Beschreibung                                                                                                               |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Endpoint</b>            | Erforderliche Informationen für den Zugriff auf einen Virtualisierungshost.                                                |
| <b>Computing-Ressource</b> | Erforderliche Informationen für den Zugriff auf eine Gruppe von virtuellen Maschinen, die ähnliche Funktionen durchführen. |

- e Wählen Sie im Dropdown-Menü **Name** den Namen der VM-Ressource aus.
- f (Optional) Wählen Sie **Benutzerdefinierte Eigenschaften einschließen** aus, wenn Sie die benutzerdefinierten Eigenschaften der virtuellen Maschine migrieren möchten.
- g Klicken Sie auf **OK**.



## 2 Bearbeiten der CSV-Datendatei einer virtuellen Maschine.

- a Öffnen Sie die CSV-Datei mit einem Texteditor und bearbeiten Sie die Datenkategorien, die Sie global ändern möchten.

Damit die in einer CSV-Datendatei enthaltenen virtuellen Maschinen aktualisiert werden, muss jede Maschine den folgenden Elementen zugeordnet werden:

- Reservierung
- Speicherort
- Blueprint
- Maschinenkomponente
- Besitzer, der in der Zielbereitstellung vorhanden ist

Für jede Maschine müssen alle Werte in der vRealize Automation-Zielumgebung vorhanden sein, damit die Aktualisierung erfolgreich ausgeführt werden kann. Sie können die Werte für die Reservierung, den Speicherort, den Blueprint und den Besitzer ändern oder den Wert für eine statische IP-Adresse zu einzelnen Maschinen hinzufügen, indem Sie die CSV-Datei bearbeiten.

- b Wenn Sie die statische IP-Adresse einer virtuellen Maschine ändern, fügen Sie der CSV-Datei einen Befehl im folgenden Format bei.

```
,VirtualMachine.Network#.Address, w.x.y.z, HOP
```

Konfigurieren Sie den Befehl mit den entsprechenden Informationen für Ihre virtuelle Maschine.

- Ändern Sie das Zeichen # in die Nummer der Netzwerkschnittstelle, die mit dieser statischen IP-Adresse konfiguriert wird. Beispielsweise `VirtualMachineNetwork0.Address`.
- Ändern Sie `w.x.y.z` in die statische IP-Adresse für die virtuelle Maschine. Beispielsweise `11.27.42.57`.
- Die `HOP`-Zeichenfolge „Hidden, Not encrypted, Not runtime“ legt die Sichtbarkeit der Eigenschaft fest. Diese Standardeigenschaft wird nach einem erfolgreichen Import von der virtuellen Maschine entfernt.

Damit die Aktualisierung erfolgreich ausgeführt werden kann, muss die IP-Adresse in einem ordnungsgemäß konfigurierten Adressenpool verfügbar sein. Wenn die IP-Adresse nicht gefunden werden kann oder bereits verwendet wird, ist die Aktualisierung ohne die Definition der statischen IP-Adresse erfolgreich und ein Fehler wird protokolliert.

- c Speichern Sie die CSV-Datei und schließen Sie den Texteditor.

- 3 Verwenden Sie die vRealize Automation-Verwaltungsschnittstelle, um mindestens eine virtuelle Maschine in einer vRealize Automation-Umgebung zu aktualisieren.
  - a Wählen Sie **Infrastruktur > Administration > Massenimporte** aus.
  - b Klicken Sie auf **Neu**.
  - c Geben Sie im Textfeld **Name** einen eindeutigen Namen für diese Aufgabe ein. Beispiel: global verwaltetes Update 10.
  - d Geben Sie im Textfeld **CSV-Datei** den Namen der CSV-Datei ein, indem Sie zum Namen der CSV-Datei navigieren.
  - e Wählen Sie Importoptionen aus.

| Option                                  | Beschreibung                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Startzeit</b>                        | Legen Sie ein zukünftiges Startdatum fest. Die angegebene Startzeit richtet sich nach der Ortszeit des Servers und nicht nach der Ortszeit der Workstation des Benutzers.                                                                                                                                                      |
| <b>Jetzt</b>                            | Importvorgang direkt starten.                                                                                                                                                                                                                                                                                                  |
| <b>Verzögerung (Sekunden)</b>           | Wenn Sie eine große Anzahl virtueller Maschinen aktualisieren, wählen Sie die Anzahl der Sekunden aus, um die die Aktualisierung jeder virtuellen Maschine verzögert werden soll. Bei Auswahl dieser Option wird der Aktualisierungsvorgang verlangsamt. Lassen Sie das Feld leer, wenn Sie keine Verzögerung angeben möchten. |
| <b>Batchgröße</b>                       | Wenn Sie eine große Anzahl virtueller Maschinen aktualisieren, wählen Sie die Gesamtanzahl der Maschinen aus, die innerhalb eines bestimmten Zeitraums aktualisiert werden sollen. Bei Auswahl dieser Option wird der Aktualisierungsvorgang verlangsamt. Lassen Sie das Feld leer, wenn Sie keinen Grenzwert angeben möchten. |
| <b>Verwaltete Maschinen ignorieren</b>  | Behalten Sie die Deaktivierung bei.                                                                                                                                                                                                                                                                                            |
| <b>Benutzervalidierung überspringen</b> | Bei Auswahl dieser Option wird der Besitzer der Maschine auf den Wert festgelegt, der in der Spalte „Besitzer“ der CSV-Datendatei aufgeführt ist, ohne dass überprüft wird, ob der Benutzer vorhanden ist. Bei Auswahl dieser Option nimmt die Zeit für die Aktualisierung möglicherweise ab.                                  |
| <b>Import testen</b>                    | Behalten Sie die Deaktivierung bei.                                                                                                                                                                                                                                                                                            |

- f Klicken Sie auf **OK**.

Der Fortschritt des Vorgangs wird auf der Seite „Massenimporte“ angezeigt.

## Migrieren einer virtuellen Maschine zu einer anderen vRealize Automation-Umgebung

Sie können mindestens eine verwaltete virtuelle Maschine in einer VMware vRealize <sup>TM</sup> Automation-Umgebung auf eine andere vRealize Automation-Umgebung migrieren.

Eine verwaltete virtuelle Maschine ist eine virtuelle Maschine, die in einer vRealize Automation-Umgebung verwaltet wird und in der Konsole angezeigt werden kann.

## Voraussetzungen

- Melden Sie sich bei vRealize Automation als **Fabric-Administrator** und als **Business-Gruppenmanager** an.
- Wenn Sie virtuelle Maschinen importieren, die statische IP-Adressen verwenden, bereiten Sie einen ordnungsgemäß konfigurierten Adressenpool vor. Weitere Informationen über die Verwendung eines Netzwerkprofils zur Steuerung von IP-Adressbereichen finden Sie unter *Konfigurieren von vRealize Automation*.

## Verfahren

- 1 Generieren der CSV-Datendatei einer virtuellen Maschine.
  - a Wählen Sie **Infrastruktur > Administration > Massenimporte** aus.
  - b Klicken Sie auf **CSV-Datei generieren**.
  - c Wählen Sie im Dropdown-Menü **Maschinen** den Eintrag **Verwaltet** aus.
  - d Wählen Sie im Dropdown-Menü **Ressource** einen der verfügbaren Ressourcentypen aus.

| Option                     | Beschreibung                                                                                                               |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Endpoint</b>            | Erforderliche Informationen für den Zugriff auf einen Virtualisierungshost.                                                |
| <b>Computing-Ressource</b> | Erforderliche Informationen für den Zugriff auf eine Gruppe von virtuellen Maschinen, die ähnliche Funktionen durchführen. |

- e Wählen Sie aus dem Dropdown-Menü **Name** den Namen der VM-Ressource aus.
- f (Optional) Wählen Sie **Benutzerdefinierte Eigenschaften einschließen** aus.  
 Sie schließen benutzerdefinierte Eigenschaften ein, wenn Sie eine virtuelle Maschine in eine neue Bereitstellung mit denselben Eigenschaften importieren.
- g Klicken Sie auf **OK**.

## 2 Bearbeiten der CSV-Datendatei einer virtuellen Maschine.

Ob Sie die CSV-Datendatei bearbeiten müssen, hängt von der Ähnlichkeit der Quell- und Zielumgebungen ab. Wenn die Konfigurationswerte in der Quellumgebung nicht mit den Werten in der Zielumgebung übereinstimmen, müssen Sie die CSV-Datendatei bearbeiten, sodass die Werte übereinstimmen, bevor Sie mit der Migration beginnen.

- a Öffnen Sie die CSV-Datei und bearbeiten Sie die Datenkategorien, sodass sie mit den vorhandenen Kategorien in der vRealize Automation-Zielumgebung übereinstimmen.

Um die in einer CSV-Datendatei enthaltenen virtuellen Maschinen zu migrieren, muss jede virtuelle Maschine einer Reservierung, einem Speicherort, einem Blueprint, einer Maschinenkomponente und einem Besitzer zugeordnet sein, der bzw. die in der vRealize Automation-Zielumgebung vorhanden ist. Für jede virtuelle Maschine müssen alle Werte in der vRealize Automation-Zielumgebung vorhanden sein, damit die Migration ordnungsgemäß durchgeführt werden kann. Sie können die Werte für die Reservierung, den Speicherort, den Blueprint und den Besitzer ändern oder den Wert für eine statische IP-Adresse zu einzelnen virtuellen Maschinen hinzufügen, indem Sie die CSV-Datei bearbeiten.

| Überschrift                     | Kommentar                                                                                                                                                                                                                                                                                                                                                                          | Beispiel                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| Import-Nr. – Ja oder Nein       | Ändern Sie die Option in „Nein“, um zu verhindern, dass eine bestimmte virtuelle Maschine importiert wird.                                                                                                                                                                                                                                                                         | Ja                                    |
| Name der virtuellen Maschine    | Nicht ändern                                                                                                                                                                                                                                                                                                                                                                       | MyMachine                             |
| ID der virtuellen Maschine      | Nicht ändern                                                                                                                                                                                                                                                                                                                                                                       | a6e05812-0b06-4d4e-a84a-fed242340426a |
| Hostreservierung (Name oder ID) | Geben Sie den Namen oder die ID einer Reservierung in der vRealize Automation-Zielumgebung ein.                                                                                                                                                                                                                                                                                    | DevReservation                        |
| Host zu Speicher (Name oder ID) | Geben Sie den Namen oder die ID eines Speicherorts in der vRealize Automation-Zielumgebung ein.                                                                                                                                                                                                                                                                                    | ce-san-1:custom-nfs-2                 |
| Bereitstellungsname             | Geben Sie für die Umgebung, die Sie in der vRealize Automation-Zielumgebung erstellen, einen neuen Namen ein.<br><br>Jede virtuelle Maschine muss zu ihrer eigenen Bereitstellung migriert werden. Sie können keine einzelne virtuelle Maschine in eine vorhandene Bereitstellung importieren. Sie können nicht mehrere virtuelle Maschinen in eine einzelne Umgebung importieren. | ImportedDeployment0001                |
| ID des konvergierten Blueprints | Geben Sie die ID des Blueprints in die vRealize Automation-Zielumgebung ein, die Sie zum Importieren der virtuellen Maschine verwenden.                                                                                                                                                                                                                                            | ImportBlueprint                       |

| Überschrift                   | Kommentar                                                                                                                                                                                                                                                                                  | Beispiel        |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
|                               | Stellen Sie sicher, dass Sie nur die Blueprint-ID eingeben. Geben Sie nicht den Blueprint-Namen ein. Sie müssen einen Blueprint auswählen, der nur eine einzige Komponente einer virtuellen Maschine enthält. Der Blueprint muss veröffentlicht und einer Berechtigung hinzugefügt werden. |                 |
| ID des Komponenten-Blueprints | Geben Sie den Namen der Komponente einer virtuellen Maschine ein, die im ausgewählten Blueprint enthalten ist. Sie können keine virtuelle Maschine in einen Blueprint importieren, der mehr als eine Komponente beinhaltet.                                                                | ImportedMachine |
| Name des Besitzers            | Geben Sie einen Benutzer in der vRealize Automation-Zielumgebung ein.                                                                                                                                                                                                                      | user@tenant     |

Beispiel für eine vollständige, ordnungsgemäß formatierte CSV-Zeile: Yes, MyMachine, a6e05812-0b06-4d4e-a84a-fed242340426, DevReservation, ce-san-1:custom-nfs-2, Imported Deployment 0001, ImportBlueprint, ImportedMachine, user@tenant

- b Wenn Sie eine virtuelle Maschine mit einer statischen IP-Adresse migrieren, fügen Sie der CSV-Datei einen Befehl im folgenden Format bei.

,VirtualMachine.Network#.Address, w.x.y.z, HOP

Konfigurieren Sie den Befehl mit den entsprechenden Informationen für Ihre virtuelle Maschine.

- Ändern Sie das Zeichen # in die Nummer der Netzwerkschnittstelle, die mit dieser statischen IP-Adresse konfiguriert wird. Beispielsweise VirtualMachineNetwork0.Address.
- Ändern Sie w.x.y.z in die statische IP-Adresse für die virtuelle Maschine. Beispielsweise 11.27.42.57.
- Die HOP-Zeichenfolge „Hidden, Not encrypted, Not runtime“ legt die Sichtbarkeit der Eigenschaft fest. Diese Standardeigenschaft wird nach einem erfolgreichen Import von der virtuellen Maschine entfernt.

Damit die Migration erfolgreich ausgeführt werden kann, muss die IP-Adresse in einem ordnungsgemäß konfigurierten Adressenpool verfügbar sein. Wenn die IP-Adresse nicht gefunden werden kann oder bereits verwendet wird, ist die Migration ohne die Definition der statischen IP-Adresse erfolgreich und ein Fehler wird protokolliert.

- c Speichern Sie die CSV-Datei.

- 3 Verwenden Sie die vRealize Automation-Verwaltungsschnittstelle, um Ihre virtuelle Maschine zu einer vRealize Automation-Umgebung zu migrieren.

- a Wählen Sie **Infrastruktur > Administration > Massenimporte** aus.
- b Klicken Sie auf **Neu**.

- c Geben Sie im Textfeld **Name** einen eindeutigen Namen für diese Aufgabe ein. Beispiel: verwaltete Migration 10.
- d Geben Sie im Textfeld **CSV-Datei** den Namen der CSV-Datei ein, indem Sie zum Namen der CSV-Datei navigieren.
- e Wählen Sie Importoptionen aus.

| Option                                  | Beschreibung                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Startzeit</b>                        | Legen Sie ein zukünftiges Startdatum fest. Die ausgewählte Startzeit richtet sich nach der Ortszeit des Servers und nicht nach der Ortszeit der Workstation des Benutzers.                                                                                                                                                |
| <b>Jetzt</b>                            | Migrationsvorgang direkt starten.                                                                                                                                                                                                                                                                                         |
| <b>Verzögerung (Sekunden)</b>           | Wenn Sie zahlreiche virtuelle Maschinen migrieren, wählen Sie die Anzahl der Sekunden aus, um die die Registrierung jeder virtuellen Maschine verzögert werden soll. Bei Auswahl dieser Option wird der Migrationsvorgang verlangsamt. Lassen Sie das Feld leer, wenn Sie keine Verzögerung auswählen möchten.            |
| <b>Batchgröße</b>                       | Wenn Sie zahlreiche virtuelle Maschinen migrieren, wählen Sie die Gesamtanzahl der virtuellen Maschinen aus, die innerhalb eines bestimmten Zeitraums registriert werden sollen. Bei Auswahl dieser Option wird der Migrationsvorgang verlangsamt. Lassen Sie das Feld leer, wenn Sie keinen Grenzwert auswählen möchten. |
| <b>Verwaltete Maschinen ignorieren</b>  | Behalten Sie die Deaktivierung bei.                                                                                                                                                                                                                                                                                       |
| <b>Benutzervalidierung überspringen</b> | Bei Auswahl dieser Option wird der Besitzer der virtuellen Maschine auf den Wert festgelegt, der in der Spalte „Besitzer“ der CSV-Datendatei aufgeführt ist, ohne dass überprüft wird, ob der Benutzer vorhanden ist. Bei Auswahl dieser Option nimmt die Zeit für die Migration möglicherweise ab.                       |
| <b>Import testen</b>                    | Testen Sie den Migrationsvorgang, ohne die virtuellen Maschinen zu migrieren, sodass Sie Ihre CSV-Datei auf Fehler überprüfen können.                                                                                                                                                                                     |

- f Klicken Sie auf **OK**.

Der Fortschritt des Vorgangs wird auf der Seite „Massenimporte“ angezeigt.