Verwalten von vRealize Automation

30. August 2017
vRealize Automation 7.3

vmware®

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

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

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

1 Verwalten von vRealize Automation

Verwalten von vRealize Automation stellt Informationen zur Wartung von VMware vRealize ™ Automation bereit, einschließlich Informationen zum Starten und Beenden einer Bereitstellung sowie zum Verwalten von Zertifikaten und der Appliance-Datenbank. Es sind außerdem Informationen zum Sichern und Wiederherstellen von vRealize Automation enthalten.

Zielgruppe

Diese Informationen sind für alle Benutzer vorgesehen, die eine vRealize Automation-Bereitstellung verwalten möchten. Die Informationen sind für erfahrene Systemadministratoren bestimmt, die mit der Windows- oder Linux-VM-Technologie und Datencenteroperationen vertraut sind.

VMware Technical Publications – Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter http://www.vmware.com/support/pubs.

Aktualisierte Informationen 2

Verwalten von vRealize Automation wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für *Verwalten von vRealize Automation*.

Revision	Beschreibung
30. August 2017	■ Die Themen „Verwenden der vRealize Automation-Überwachungsprotokollierung“, auf Seite 59 und „Konfigurieren von vRealize Automation für die Überwachungsprotokollierung mit Log Insight“, auf Seite 59 zur Überwachungsprotokollierung wurden hinzugefügt. ■ Die Themen „Aktualisieren von eingebettetem vRealize Orchestrator, sodass vRealize Automation-Zertifikate als vertrauenswürdig eingestuft werden“, auf Seite 21 und „Aktualisieren von externem vRealize Orchestrator, sodass vRealize Automation-Zertifikate als vertrauenswürdig eingestuft werden“, auf Seite 22 zur erneuten Registrierung von vRealize Orchestrator für vRealize Automation-Zertifikate wurden hinzugefügt.
DE-002419-02	■ „Manuelle Wiederherstellung der Appliance-Datenbank nach einem schwerwiegenden Fehler“, auf Seite 34 wurde aktualisiert. ■ „Ersetzen von Zertifikaten in der vRealize Automation-Appliance“, auf Seite 15 wurde aktualisiert. ■ „Starten von vRealize Automation“, auf Seite 11 wurde aktualisiert.
DE-002419-01	„Manuelle Wiederherstellung der Appliance-Datenbank nach einem schwerwiegenden Fehler“, auf Seite 34 wurde hinzugefügt.
DE-002419-00	Erstversion.

Verwalten und Anpassen von vRealize Automation -Komponenten und -Optionen

3

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

Dieses Kapitel behandelt die folgenden Themen:

Übermitteln einer Nachricht per Broadcast im Meldungs-Board-Portlet

Als Mandantenadministrator nutzen Sie das Meldungs-Board-Portlet, um per Broadcast eine Nachricht an alle Benutzer zu übermitteln, denen das Portlet auf der Registerkarte „Start“ angezeigt wird.

Bei allen neuen Benutzern, die Sie zu vRealize Automation hinzufügen, ist das Portlet standardmäßig auf der Registerkarte „Start“ enthalten. Bestehende Benutzer müssen das Portlet hinzufügen, um Ihre Nachrichten zu empfangen.

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

Für das Meldungs-Board gelten folgende Einschränkungen.

Tabelle 3-1. Meldungs-Board-Portlet – Einschränkungen

Option	Einschränkungen
Einschränkungen im Zusammenhang mit URL-Nachrichten	■ 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	■ Zur Gewährleistung der Sicherheit unterstützen benutzerdefinierte Nachrichten 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 an der vRealize Automation-Konsole als **Mandantenadministrator** an.

Vorgehensweise

1 Wählen Sie die Registerkarte **Start** aus.

2 Klicken Sie in der rechten oberen Ecke auf das Symbol **Bearbeiten** ().

3 Wählen Sie **Portlets hinzufügen**.

4 Suchen Sie das Meldungs-Board und klicken Sie auf **Hinzufügen**.

5 Klicken Sie auf **Schließen**.

Das Portlet wird oben auf der Registerkarte „Start“ hinzugefügt. Wenn Sie ein Benutzer sind und eine Nachricht per Broadcast übermittelt wird, wird die Nachricht so lange angezeigt, bis sie vom Mandantenadministrator geändert oder entfernt wird. Wenn Sie der Mandantenadministrator sind, konfigurieren Sie die Nachricht.

6 Klicken Sie auf **Neue Nachricht hinzufügen**, um die Nachricht als Mandantenadministrator zu konfigurieren.

7 Konfigurieren Sie eine der folgenden Optionen:

Option	Beschreibung
URL	Geben Sie die URL der Seite ein.
Benutzerdefinierte Nachricht	Geben Sie die Nachricht als einfachen Text ein.

8 Klicken Sie auf **Veröffentlichen**.

Die Nachricht wird per Broadcast an alle Mandantenbenutzer übermittelt, die das Meldungs-Board-Portlet auf ihrer Registerkarte „Start“ hinzugefügt haben.

Zum Ändern oder Entfernen der Nachricht müssen Sie als Mandantenadministrator angemeldet sein. Zum Ändern der Nachricht wiederholen Sie die gleichen Schritte. Zum Entfernen der Nachricht entfernen Sie die URL oder den Text und veröffentlichen die leere Nachricht.

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 völlig neu starten, z. B. nach einem Stromausfall, einem kontrollierten Herunterfahren oder einer Wiederherstellung, müssen Sie die Komponenten in einer bestimmten Reihenfolge starten.

Voraussetzungen

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

Vorgehensweise

1 Starten Sie die MS SQL-Datenbankmaschine. Wenn Sie eine eigenständige Legacy-PostgreSQL-Datenbank verwenden, starten Sie auch diese Maschine.

2 (Optional) Wenn Sie eine Bereitstellung ausführen, die Lastausgleichsdienste mit Integritätsprüfungen verwendet, deaktiveren Sie die Integritätsprüfung, bevor Sie die vRealize Automation-Appliance starten. Nur die Ping-Integritätsprüfung darf aktiviert sein.

3 Starten Sie alle Instanzen der vRealize Automation-Appliance gleichzeitig und warten Sie etwa 15 Minuten auf den Start der Appliances. Stellen Sie sicher, dass die vRealize Automation-Appliance-Dienste aktiviert sind und ausgeführt werden.

   Wenn mehrere Knoten vorhanden sind und Sie nur einen Knoten starten, müssen Sie möglicherweise zusätzlich 35 Minuten warten. Die zusätzliche Wartezeit entfällt jedoch, sobald Sie den zweiten Knoten starten.

4 Starten Sie den primären Webknoten und warten Sie, bis der Startvorgang abgeschlossen ist.

5 (Optional) Wenn Sie eine verteilte Bereitstellung ausführen, starten Sie alle sekundären Webknoten und warten Sie 5 Minuten.

6 Starten Sie die primäre Manager Service-Maschine und warten Sie je nach Site-Konfiguration 2 bis 5 Minuten.

7 (Optional) Wenn Sie eine verteilte Bereitstellung ausführen, starten Sie sekundäre Manager Service-Maschinen 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.

8 Starten Sie die Distributed Execution Manager-Orchestrator und -Workers sowie alle vRealize Automation-Proxy-Agents.

   Sie können diese Komponenten in beliebiger Reihenfolge starten und brauchen nicht zu warten, bis ein Startvorgang abgeschlossen ist, bevor Sie eine weitere Komponente starten.

9 Wenn Sie die Integritätsprüfungen für die Lastausgleichsdienste deaktiviert haben, aktivieren Sie diese wieder.

10 Vergewissern Sie sich, dass der Start erfolgreich war.

   a Öffnen Sie in einem Webbrowser die URL für die Verwaltungsschnittstelle der vRealize Automation-Appliance.

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

   c Klicken Sie auf die Registerkarte **Aktualisieren**, um den Fortschritt des Dienststarts zu überwachen.

Wenn alle Dienste als registriert aufgelistet sind, ist das System betriebsbereit.

Neustarten von vRealize Automation

Wenn Sie mehr als eine vRealize Automation-Komponente neu starten, müssen Sie die Komponenten in einer angegebenen Reihenfolge neu starten.

Sie müssen einige Komponenten in der Bereitstellung möglicherweise neu starten, um anormales Produktverhalten zu beheben. Wenn Sie vCenter Server zum Verwalten Ihrer virtuellen Maschinen verwenden, verwenden Sie den `restart`-Gastbefehl zum Neustart von vRealize Automation.

Wenn Sie eine Komponente oder einen Dienst nicht neu starten können, folgen Sie den Anweisungen in „Herunterfahren von vRealize Automation“, auf Seite 13 und „Starten von vRealize Automation“, auf Seite 11.

Voraussetzungen

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

Vorgehensweise

1 Starten Sie alle Instanzen der vRealize Automation-Appliance gleichzeitig neu.

2 Starten Sie den primären Webknoten neu und warten Sie, bis der Startvorgang abgeschlossen ist.

3 Wenn Sie eine verteilte Bereitstellung ausführen, starten Sie alle sekundären Webknoten neu und warten Sie, bis der Startvorgang abgeschlossen ist.

4 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 belassen möchten, befolgen 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.

5 Starten Sie die Distributed Execution Manager-Orchestrator und -Workers und alle vRealize Automation-Agents neu und warten Sie, bis der Startvorgang für alle Komponenten abgeschlossen ist.

   Sie können diese Komponenten in beliebiger Reihenfolge neu starten.

6 Vergewissern Sie sich, dass der neu gestartete Dienst registriert ist.

   a Öffnen Sie in einem Webbrowser die URL für die Verwaltungsschnittstelle der vRealize Automation-Appliance.

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

   c Klicken Sie auf die Registerkarte **Aktualisieren**, um den Fortschritt des Dienststarts zu überwachen.

Wenn alle Dienste als registriert aufgelistet sind, ist das System betriebsbereit.

Herunterfahren von vRealize Automation

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

Wenn Sie vCenter Server zum Verwalten Ihrer virtuellen Maschinen verwenden, verwenden Sie den `shutdown`-Gastbefehl zum Herunterfahren von vRealize Automation.

Vorgehensweise

1 Fahren Sie die Distributed Execution Manager-Orchestrator und -Workers und alle vRealize Automation-Agents in beliebiger Reihenfolge herunter und warten Sie, bis das Herunterfahren aller Komponenten abgeschlossen ist.

2 Fahren Sie die virtuellen Maschinen herunter, die den Manager Service ausführen, und warten Sie, bis das Herunterfahren abgeschlossen ist.

3 (Optional) Bei verteilten Bereitstellungen fahren Sie alle sekundären Webknoten herunter und warten Sie, bis das Herunterfahren abgeschlossen ist.

4 Fahren Sie den primären Webknoten herunter und warten Sie, bis das Herunterfahren abgeschlossen ist.

5 (Optional) Bei verteilten Bereitstellungen fahren Sie alle sekundären Instanzen der vRealize Automation-Appliance herunter und warten, bis das Herunterfahren abgeschlossen ist.

6 Fahren Sie die primäre vRealize Automation-Appliance herunter und warten Sie, bis das Herunterfahren abgeschlossen ist.

   Sofern zutreffend, ist die primäre vRealize Automation-Appliance diejenige, die die (schreibfähige) Master-Appliance-Datenbank enthält. Notieren Sie sich den Namen der primären vRealize Automation-Appliance. Sie benötigen diese Informationen beim Neustart von vRealize Automation.

7 Fahren Sie die virtuellen MSSQL-Maschinen in beliebiger Reihenfolge herunter und warten Sie, bis das Herunterfahren abgeschlossen ist.

8 Wenn Sie eine eigenständige Legacy-PostgreSQL-Datenbank verwenden, fahren Sie auch diese Maschine herunter.

Sie haben Ihre vRealize Automation-Bereitstellung heruntergefahren.

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 die sichere Kommunikation untereinander zu erleichtern. Bei diesen Komponenten handelt es sich um:

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

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

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 Verwaltungskonsole der virtuellen vRealize Automation-Appliance bietet drei Optionen zum Aktualisieren oder Ersetzen von Zertifikaten für vorhandene Bereitstellungen:

- **Zertifikat generieren** – Verwenden Sie diese Option, damit das System ein selbstsigniertes Zertifikat generiert.
- **Zertifikat importieren** – Verwenden Sie diese Option, wenn Sie über ein Zertifikat verfügen, das Sie benutzen möchten.
- **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 vRealize Automation-Verwaltungskonsole hochladen zu müssen.

Sie können auch die Option zur Beibehaltung des vorhandenen Zertifikats verwenden, um Ihr vorhandenes Zertifikat beizubehalten.

Hinweis Bei einer geclusterten Bereitstellung müssen Sie Änderungen des Zertifikats über die Virtual Appliance Management Interface (VAMI) auf dem Masterknoten initiieren.

Zertifikate für die Management-Site 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 virtuellen Appliance nicht eingeben, schlägt die Zertifikatsersetzung fehl und die Meldung `Unable to load private key` wird angezeigt.

Die vRealize Orchestrator-Komponente, die Ihrer vRealize Automation-Bereitstellung zugeordnet ist, verfügt über ihre eigenen Zertifikate und muss die vRealize Automation-Zertifikate ebenfalls als vertrauenswürdig einstufen. Standardmäßig ist die vRealize Orchestrator-Komponente in vRealize Automation eingebettet, aber sie haben die Möglichkeit, 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 vRealize Automation-Zertifikate aktualisieren oder ersetzen, müssen Sie vRealize Orchestrator aktualisieren, sodass es die neuen Zertifikate als vertrauenswürdig einstuft.

Hinweis Wenn Sie eine vRealize Orchestrator-Bereitstellung mit mehreren Knoten verwenden, die hinter einem Laustausgleichsdienst platziert ist, müssen alle vRealize Orchestrator-Knoten dasselbe Zertifikat verwenden.

Wichtige Informationen zu Fehlerbehebung, Unterstützung und Anforderungen an die Vertrauenswürdigkeit finden Sie im VMware Knowledgebase-Artikel unter http://kb.vmware.com/kb/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 3-2. Beispielzertifikatwerte und -befehle (openssl)

Von Zertifizierungsstelle bereitgestellt	Befehl	Einträge der virtuellen Appliance
RSA-Privatschlüssel	openssl pkcs12 -in *path _to_.pfx certificate_file* -nocerts -out key.pem	**RSA-Privatschlüssel**
PEM-Datei	openssl pkcs12 -in *path _to_.pfx certificate_file* -clcerts -nokeys -out cert.pem	**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 vRealize Automation-Appliance-Zertifikat aktualisieren oder ersetzen, wird das Vertrauen zu anderen zugehörigen Komponenten automatisch erneut initiiert. Weitere Informationen zum Aktualisieren von Zertifikaten finden Sie unter „Aktualisieren von vRealize Automation-Zertifikaten“, auf Seite 14.

Vorgehensweise

1 Öffnen Sie in einem Webbrowser die URL für die Verwaltungsschnittstelle der vRealize Automation-Appliance.

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-Einstellungen > Hosteinstellungen** aus.

4 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.

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	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	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	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. **Hinweis** Im Fall von verketteten Zertifikaten sind möglicherweise zusätzliche Attribute verfügbar. 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**.

Nach einigen Minuten 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.

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.

Es gibt drei Optionen für das Ersetzen eines Zertifikats:

- Zertifikat generieren – Verwenden Sie diese Option, damit das System ein selbstsigniertes Zertifikat generiert.
- Zertifikat importieren – Verwenden Sie diese Option, wenn Sie über ein Zertifikat verfügen, das Sie benutzen möchten.
- Fingerabdruck des Zertifikats bereitstellen – Wenn Sie ein Zertifikat akzeptieren, das von einer Zertifizierungsstelle signiert wurde, Ihr System diesem Zertifikat aber nicht vertraut, müssen Sie angeben, ob Sie den Fingerabdruck des Zertifikats akzeptieren. Der Fingerabdruck wird verwendet, um umgehend festzustellen, ob ein angegebenes Zertifikat mit einem anderen Zertifikat übereinstimmt, zum Beispiel mit einem zuvor akzeptieren Zertifikat.

Sie können auch die Option zur Beibehaltung des vorhandenen Zertifikats verwenden, um Ihr vorhandenes Zertifikat beizubehalten.

Vorgehensweise

1 Öffnen Sie in einem Webbrowser die URL für die Verwaltungsschnittstelle der vRealize Automation-Appliance.

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-Einstellungen > Zertifikate** aus.

4 Klicken Sie im Menü **Komponententyp** auf **IaaS-Web**.

5 Navigieren Sie zum Fensterbereich **IaaS-Webzertifikat**.

6 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	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.
Importieren	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. **Hinweis** Im Fall von verketteten Zertifikaten sind möglicherweise zusätzliche Attribute verfügbar. 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.
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.

7 Klicken Sie auf „Einstellungen speichern“.

Nach einigen Minuten werden die Zertifikatdetails 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.

Vorgehensweise

1 Öffnen Sie in einem Webbrowser die URL für die Verwaltungsschnittstelle der vRealize Automation-Appliance.

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-Einstellungen > Zertifikate** aus.

4 Klicken Sie im Menü **Zertifikatstyp** 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	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	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. **Hinweis** Im Fall von verketteten Zertifikaten sind möglicherweise zusätzliche Attribute verfügbar. 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.
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 Lastausgleichsdienst, wenn dies vom Netzwerk oder dem Lastausgleichsdienst gefordert wird.

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

Wenn Sie einen Lastausgleichsdienst verwenden, muss der Hostname der vollqualifizierte Domänenname des Lastausgleichsdiensts sein.

9 Ignorieren Sie ggf. etwaige Zertifikatswarnungen.

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

11 Wenn Sie einen Lastausgleichsdienst 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“, auf Seite 22.

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. Siehe https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2147612.

Vorgehensweise

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

```
service vco-server stop
service vco-configuration stop
```

2 Setzen Sie den Authentifizierungsanbieter vRealize Orchestrator zurück.

   a Führen Sie den Befehl `/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication` aus.

   b Löschen Sie `/etc/vco/app-server/vco-registration-id`.

   c Führen Sie `vcac-vami vco-service-reconfigure` aus.

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

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

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. Siehe https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2147612.

Vorgehensweise

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

```
service vco-configuration 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“, auf Seite 25.

Vorgehensweise

1 Suchen des Management-Agent-Bezeichners auf Seite 23

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 auf Seite 24

Die vRealize Automation-Appliance verwendet lighttpd zum Ausführen der eigenen Management-Site. Sie können das SSL-Zertifikat des Management-Site-Diensts ersetzen, wenn das Zertifikat abläuft oder wenn Sie ein selbstsigniertes Zertifikat verwenden und die Sicherheitsrichtlinien Ihres Unternehmens die Verwendung ihrer SSL-Zertifikate vorschreiben. Sie sichern den Management-Site-Dienst auf Port 5480.

3 Aktualisieren der Zertifikatserkennung für Management-Agents auf Seite 25

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.

Vorgehensweise

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

Die vRealize Automation-Appliance verwendet lighttpd zum Ausführen der eigenen Management-Site. Sie können das SSL-Zertifikat des Management-Site-Diensts ersetzen, wenn das Zertifikat abläuft oder wenn Sie ein selbstsigniertes Zertifikat verwenden und die Sicherheitsrichtlinien Ihres Unternehmens die Verwendung ihrer SSL-Zertifikate vorschreiben. Sie sichern den Management-Site-Dienst auf Port 5480.

Sie können ein neues Zertifikat installieren oder das vom vRealize Automation-Dienst auf Port 443 verwendete Zertifikat wiederverwenden.

Wenn Sie ein neues Zertifikat anfordern, um ein von einer anderen Zertifizierungsstelle ausgestelltes Zertifikat zu aktualisieren, empfiehlt es sich, den allgemeinen Namen (Common Name) des vorhandenen Zertifikats wiederzuverwenden.

Voraussetzungen

- Neue Zertifikate erfordern das PEM-Format, und der Privatschlüssel darf nicht verschlüsselt sein. Standardmäßig werden das SSL-Zertifikat und der private Schlüssel für die Management-Site der vRealize Automation-Appliance in einer PEM-Datei unter `/opt/vmware/etc/lighttpd/server.pem` gespeichert.

  Weitere Informationen zum Exportieren eines Zertifikats und eines Privatschlüssels aus einem Java-Keystore in eine PEM-Datei finden Sie unter „Extrahieren von Zertifikaten und privaten Schlüsseln“, auf Seite 15.

Vorgehensweise

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-lighttp 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.

Das neue Zertifikat für die Management-Site der vRealize Automation-Appliance wird installiert.

Weiter

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“, auf Seite 26.
- Weitere Informationen zur manuellen Aktualisierung finden Sie unter „Manuelles Aktualisieren der Zertifikatserkennung für Management-Agents“, auf Seite 25.

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 auf Seite 25

  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 auf Seite 26

  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“, auf Seite 26.

Voraussetzungen

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

Vorgehensweise

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" thumb-
print="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" thumb-
print="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 navigieren Sie zu **vRA-Einstellungen > Cluster**.

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“, auf Seite 25.

Verwenden Sie dieses Verfahren für die automatische Aktualisierung von Zertifikatsinformationen.

Vorgehensweise

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.

Vorgehensweise

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

Option	Argument	Hinweise
`-vamih`	*vra-va-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 00000000-0000-0000-0000-000000000000 kann nicht hinzugefügt werden“.
`-nd`	*00000000-0000-0000-0000-000000000000*	Management-Agent-Bezeichner.
`-tp`	*0000000000000000000000000000000000000000*	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-va-hostname.domain.name:5480"
-cu "root" -cp "Kennwort" -hn "machine-hostname.domain.name"
-nd "00000000-0000-0000-0000-000000000000"
-tp "0000000000000000000000000000000000000000"
```

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

Wenn Sie Kommas im OU-Abschnitt des IaaS-Zertifikats verwenden, treten möglicherweise STOMP-WebSocket-Fehler in den Manager Service-Protokolldateien auf und die Bereitstellung von virtuellen Maschinen schlägt ggf. fehl. Sie können die Kommas entfernen oder die Abrufmethode von WebSocket in HTTP ändern, um diese Probleme zu beheben.

Weitere Informationen zum Manager Service finden Sie unter *Installieren von vRealize Automation 7.3*.

Vorgehensweise

1 Öffnen Sie die Manager Service-Konfigurationsdatei in einem Texteditor.

Die Manager Service-Konfigurationsdatei befindet sich in folgendem Verzeichnis: `C:\\:Programme (x86)\VMware\vCAC\Server\Manager Service.exe.config`.

2 Fügen Sie dem Abschnitt `<appSettings>` der Manager Service-Konfigurationsdatei die folgenden Zeilen hinzu.

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

3 Starten Sie den Manager Service neu.

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 Master 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.

Eine Clusterkonfiguration enthält einen Master-Knoten und einen oder mehrere Replikatknoten. Der Master-Knoten ist der vRealize Automation-Appliance-Knoten mit der Master-Datenbank, der die Systemfunktionalität unterstützt. Replikatknoten enthalten Kopien der Datenbank, die eingesetzt werden können, wenn der Master-Knoten ausfällt.

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 aufrecht erhält und legt in Hochverfügbarkeitskofigurationen fest, wie das Failover erfolgt, wenn der Master- bzw. 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 mindestens zwei Knoten erforderlich, während für den synchronen Modus mindestens drei Knoten erforderlich sind. Der synchrone Modus aktiviert das automatische Failover.

Replikationsmodus	Vorteile	Nachteile
Synchron	■ Minimiert die Möglichkeit des Datenverlusts. ■ Ruft das automatische Failover auf.	■ Kann die Systemleistung beeinträchtigen. ■ Erfordert mindestens drei Knoten.
Asynchron	■ 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 **Datenbank** 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.

Konfigurieren der Appliance-Datenbank

Auf der Seite der VAMI-Datenbank (Virtual Appliance Management Interface) können Sie die Konfiguration der Appliance-Datenbank überwachen oder aktualisieren. Zudem können Sie hier die Master-Knotenbezeichnung und den von der Datenbank verwendeten Synchronisierungsmodus 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 Master 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 3-4. Synchronisierungsstatus für die Replikationsmodi der Appliance-Datenbank

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

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

Die Spalte „Priorität“ zeigt die Position der Replikatknoten in Beziehung zum Master-Knoten. Der Master-Knoten hat keinen Prioritätswert. Wählen Sie zum Heraufstufen eines Replikats zum Master den Knoten mit dem niedrigsten Prioritätswert.

Im synchronen Modus ruft vRealize Automation das automatische Failover auf. Sollte der Masterknoten ausfallen, wird der nächste verfügbare Replikatknoten automatisch zum neuen Master. 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 7.3*.
- Melden Sie sich an der vRealize Automation-Verwaltungskonsole als **root** an.
- Konfigurieren Sie einen geeigneten eingebetteten Postgres-Appliance-Datenbankcluster als Teil der vRealize Automation-Bereitstellung.

Vorgehensweise

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.
   - Vergewissern Sie sich, dass der richtige Knoten als Master-Knoten bezeichnet 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 Master 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.

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 Masterknoten der vRealize Automation-Appliance ausfällt oder deren Ausführung beendet wird.

Voraussetzungen

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

Vorgehensweise

1 Entfernen Sie die IP-Adresse des Master-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 Klicken Sie auf **vRA-Einstellungen > Datenbank**.

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 Master-Knoten aufgelistet.

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

a Isolieren Sie den ehemaligen Master-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 Master-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 Masterknoten 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 Masterknotens der vRealize Automation-Appliance als Root-Benutzer an.

g Klicken Sie auf **vRA-Einstellungen > Datenbank**.

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

i Wenn der ehemalige Master-Knoten ordnungsgemäß zurückgesetzt wurde, starten Sie ihn neu.

j Stellen Sie bei eingeschaltetem vorherigem Master sicher, dass die folgenden Dienste ausgeführt werden.

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

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

Hinweis Wenn ein Master-Knoten, der zur Replik herabgestuft wurde, nach wie vor als Master aufgelistet wird, müssen Sie, um das Problem zu beheben, möglicherweise manuell dafür sorgen, dass er dem Cluster wieder beitritt.

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 Master-Knoten läuft und normal ausgeführt wird. Die Datenbank-Failover-Wartung besteht aus zwei Schritten: Wartung des Masters und Wartung eines Replikatknotens. Wenn ein Master-Knoten ersetzt und zum Replikat wurde, müssen Sie eine Wartung ausführen, damit er bei Bedarf erneut als Master 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 7.3* installiert und konfiguriert.
- Melden Sie sich an der vRealize Automation-Verwaltungskonsole als **root** an.
- Installieren und konfigurieren Sie einen entsprechenden eingebetteten Postgres-Appliance-Datenbankcluster.
- Wenn Ihre Datenbank den synchronen Replikationsmodus verwendet, vergewissern Sie sich, dass der Cluster mindestens drei aktive Knoten enthält.
-

Vorgehensweise

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

2 Isolieren Sie den Master-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 im Virtual Appliance Management Interface **vRA-Einstellungen > Datenbank**.

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

Replikatknoten werden aufsteigend nach Priorität aufgelistet.

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

6 Führen Sie die entsprechende Replikatwartung durch.

7 Vergewissern Sie sich nach Abschluss der Wartung, dass die virtuelle Appliance mit Netzwerkkonnektivität ausgeführt wird und dass ihr HAProxy-Dienst läuft.

a Melden Sie sich an der vRealize Automation-Verwaltungskonsole als **root** an.

b Stellen Sie sicher, dass der Replikatknoten angepingt und nach Name aufgelöst werden kann sowie einen aktuellen Status auf der Registerkarte „Virtual Appliance Management Console-Datenbank“ aufweist.

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

Mit diesem Vorgang wird die Datenbank zurückgesetzt, sodass sie zum Replizieren des aktuellen Masters konfiguriert wird und den Replikatknoten mit der neuesten haproxy-Konfiguration vom Master-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 Postgres-vRA-Datenbanktabelle zum Konfigurieren als fehlerfrei angezeigt wird, dass er angepingt und nach Name aufgelöst werden kann.

Weiter

Beheben Sie Probleme mit dem vorherigen Master-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 Masters 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.
```

Vorgehensweise

1 Versuchen Sie, die Datenbank mithilfe der Virtual Appliance Management Interface (VAMI) über einen der Datenbankknoten wiederherzustellen.

   a Öffnen Sie, falls möglich, die VAMI-Datenbankseite des Knotens mit dem aktuellsten Stand. Im Normalfall war dieser Knoten der Masterknoten, bevor die Datenbank ausgefallen ist.

   b Wenn die VAMI für den Masterknoten 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“, auf Seite 31.

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_locati-
on() as replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_time-
stamp;
 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 shut-
down-backup-sessions
```

   Unter Verwendung des FQDN des aktuellen Knotens wie folgt:

```
server masterserver fqdn-des-aktuellen-Knoten:5432 check on-marked-up shutdown-backup-sessi-
ons
```

7 Speichern Sie die Datei.

8 Führen Sie den Befehl `service haproxy restart` aus.

9 Öffnen Sie die VAMI-Datenbankseite für den Knoten mit dem neusten Stand.

   Dieser Knoten sollte als Masterknoten und die 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** und **Aktualisieren**, 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.

Sichern von vRealize Automation

Der Systemadministrator sichert regelmäßig die gesamte vRealize Automation-Installation.

Sie können mehrere Strategien verwenden, einzeln oder in Kombination, um vRealize Automation-Systemkomponenten zu sichern. Bei virtuellen Maschinen können Sie die Snapshot-Funktion verwenden, um Snapshot-Images von wichtigen Komponenten zu erstellen. Wenn ein Systemfehler auftritt, können Sie diese Images verwenden, um Komponenten in ihren Zustand zum Zeitpunkt der Erstellung der Images wiederherzustellen. Sie können vollständige, differenzielle und inkrementelle Sicherungen und Wiederherstellungen von virtuellen Maschinen durchführen. Alternativ und bei nicht virtuellen Maschinenkomponenten können Sie Kopien entscheidender Konfigurationsdateien für Systemkomponenten erstellen, die verwendet werden können, um diese Komponenten in einen benutzerdefinierten konfigurierten Zustand nach der Neuinstallation wiederherzustellen.

Eine vollständige Sicherung enthält die folgenden Komponenten:

- Infrastruktur-MS-SQL-Datenbank.
- PostgreSQL-Datenbank (Betrifft ausschließlich ältere Installationen, bei denen keine Appliance-Datenbank verwendet wird.)
- Ggf. Identitätsverwaltungskomponenten.
- vRealize Automation-Appliance.
- IaaS-Komponenten.
- (Optional) Software-Lastausgleichsdienste.
- (Optional) Lastausgleichsdienste, die Ihre verteilte Bereitstellung unterstützen. Informationen zu Überlegungen zur Sicherung erhalten Sie in der Dokumentation des Anbieters für Ihren Lastausgleichsdienst.

Richtlinien für die Planung von Backups

Halten Sie sich bei der Planung von Backups an die folgenden Richtlinien:

- Wenn Sie ein vollständiges System sichern, sichern Sie alle Instanzen der vRealize Automation-Appliance und Datenbanken so zeitgleich wie möglich, vorzugsweise innerhalb von Sekunden.
- Minimieren Sie die Anzahl aktiver Transaktionen, bevor Sie mit einem Backup beginnen. Planen Sie die regelmäßige Sicherung für Phasen ein, in denen Ihr System die geringste Aktivität aufweist.
- Sichern Sie alle Datenbanken gleichzeitig.
- Sichern Sie den Lastausgleichsdienst einer virtuellen Appliance gleichzeitig mit der vRealize Automation-Appliance.
- Erstellen Sie ein Backup von allen Instanzen der vRealize Automation-Appliance, wenn Sie Zertifikate aktualisieren.
- Erstellen Sie ein Backup von allen IaaS-Komponenten, wenn Sie Zertifikate aktualisieren.

Sichern der vRealize Automation -Zertifikate

Der Systemadministrator sichert Zertifikate und Zertifikatsketten zum Installationszeitpunkt oder beim Ersetzen eines Zertifikats.

Sichern Sie die folgenden Zertifikate:

- Zertifikate der vRealize Automation-Appliance und die gesamte entsprechende Zertifikatskette.
- Zertifikate der IaaS und die gesamte entsprechende Zertifikatskette.

Sichern der Lastausgleichsdienste

Lastausgleichsdienste verteilen in High Availability-Bereitstellungen die Arbeitslast auf die Server. Der Systemadministrator sichert die Lastausgleichsdienste regelmäßig zusammen mit anderen Komponenten.

Halten Sie sich beim Sichern der Lastausgleichsdienste an Ihre Standortrichtlinien und achten Sie darauf, dass die Netzwerktopologie und der vRealize Automation-Sicherungsplan eingehalten werden.

Sichern der vRealize Automation -Datenbanken

Der Datenbankadministrator sichert die Infrastruktur-MSSQL-Server- und vRealize Automation-Appliance-Datenbank.

Als Best Practice empfiehlt es sich, die Infrastruktur-MSSQL- und vRealize Automation-Appliance-Datenbank bzw. Legacy-PostgreSQL-Datenbanken so zeitgleich wie möglich zu sichern, um Datenverlust zu vermeiden bzw. zu minimieren. Sichern Sie Datenbanken zudem mit aktiviertem Point-in-Time, wenn zutreffend. Mit der Point-in-Time-Wiederherstellung stellen Sie sicher, dass die beiden Datenbanken miteinander übereinstimmen. Wenn nur eine Datenbank fehlschlägt, müssen Sie die ausgeführte Datenbank auf das aktuellste Backup wiederherstellen, sodass die Datenbanken übereinstimmen.

Infrastruktur-MSSQL-Datenbank

Befolgen Sie Ihre internen Verfahren, um die Infrastruktur-MSSQL-Datenbank außerhalb des vRealize Automation-Frameworks zu sichern.

Verwenden Sie folgende Richtlinien, wenn Sie ein Backup erstellen:

- Überprüfen Sie nach Möglichkeit, ob alle IaaS-Workflows vollständig sind und ob alle IaaS-Dienste angehalten wurden oder die Aktivität minimiert wurde.
- Führen Sie die Sicherung mit aktiviertem Point-in-Time durch.
- Sichern Sie die MSSQL-Datenbank zur gleichen Zeit wie die anderen Komponenten.
- Sichern Sie die Passphrase für Ihre Datenbank.

Hinweis Ihre Datenbank wird durch eine Passphrase geschützt. Bei der Wiederherstellung der Datenbank sollten Sie die Passphrase zur Hand haben. In der Regel notieren Sie die Passphrase bei der Installation an einem sicheren und für Sie leicht zugänglichen Ort.

Appliance-Datenbank oder Legacy-PostgreSQL-Datenbank

Wenn Sie eine in einer vRealize Automation-Appliance eingebettete Appliance-Datenbank bzw. Legacy-PostgreSQL-Datenbank verwenden, können Sie die Datenbank durch ein Backup der gesamten Appliance mithilfe einer der unter „vRealize Automation-Appliance“ beschriebenen Methoden sichern. Wenn Sie eine Legacy-PostgreSQL-Datenbank verwenden, können Sie auch die Datenbank separat sichern. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel *Migration von einer externen vPostgres-Appliance zu einer vPostgres-Instanz, die sich in der vCAC-Appliance befindet (2083562)* unter http://kb.vmware.com/kb/2083562.

Eine eigenständige Legacy-PostgreSQL-Appliance muss separat gesichert werden. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel *Migration von einer externen vPostgres-Appliance zu einer vPostgres-Instanz, die sich in der vCAC-Appliance befindet (2083562)* unter http://kb.vmware.com/kb/2083562.

Sichern der vRealize Automation -Appliance

Der Systemadministrator sichert die vRealize Automation-Appliance durch das Exportieren oder Klonen der Appliance. Sie können auch die zu verwendenden Konfigurationsdateien kopieren, um die Konfiguration zum Zeitpunkt der Sicherung wiederherzustellen.

Sichern Sie Appliances, indem Sie sie exportieren oder klonen.

Als Best Practice empfiehlt es sich, Ihre vRealize Automation-Appliance und Ihre Datenbanken gleichzeitig zu sichern.

Zum Erstellen von Backups können Sie die folgenden Methoden verwenden.

- Die Exportfunktion von vSphere.
- Klonen.
- VMware vSphere Data Protection zum Erstellen von Sicherungen für die gesamte Appliance.
- vSphere Replication, um die virtuelle Appliance in einer anderen Site zu replizieren.
- VMware Recovery Manager zur Bereitstellung von Hochverfügbarkeit, indem die Appliance in einem anderen Datencenter gesichert wird.

Snapshots können Sie nur dann zum Sichern von virtuellen Appliances verwenden, wenn Sie sie in einem anderen als dem Speicherort der Appliance speichern oder replizieren. Wenn nach einem Fehler der Zugriff auf das Snapshot-Image möglich ist, so stellt dies die direkteste Methode zum Wiederherstellen der Appliance dar.

Um nur die Konfigurationsinformationen für die Appliance beizubehalten, sichern Sie die folgenden Dateien und behalten Sie den Besitzer, die Gruppe und die Berechtigungen für jede Datei bei. Die folgenden Dateien werden ebenfalls beim Exportieren oder Klonen einer Appliance gesichert.

- `/etc/vcac/encryption.key`
- `/etc/vcac/vcac.keystore`
- `/etc/vcac/vcac.properties`
- `/etc/vcac/security.properties`
- `/etc/vcac/server.xml`
- `/etc/vcac/solution-users.properties`
- `/etc/apache2/server.pem`
- `/etc/vco/app-server/sso.properties`
- `/etc/vco/app-server/plugins/*`
- `/etc/vco/app-server/vmo.properties`
- `/etc/vco/app-server/js-io-rights.conf`
- `/etc/vco/app-server/security/*`
- `/etc/vco/app-server/vco-registration-id`
- `/etc/vco/app-server/vcac-registration.status`
- `/etc/vco/configuration/passwd.properties`
- `/var/lib/rabbitmq/.erlang.cookie`

- `/var/lib/rabbitmq/mnesia/**`

Sichern der IaaS-Komponenten

Der Systemadministrator sichert die IaaS-Komponenten. Halten Sie sich bei der Planung von Backups an die folgenden Richtlinien.

Sie können IaaS-Komponenten sichern, indem Sie einen Snapshot der VMs in der folgenden Reihenfolge erstellen:

- Proxy-Agents und DEMs
- Manager Service
- Websites

Sichern Sie für Agents die folgenden Informationen:

1 Den Namen des Agents.

2 Den Namen des Endpoints. Beachten Sie, dass dieser Name nicht mit der Endpoint-Adresse identisch ist.

3 Die folgenden Dateien im Installationsordner des Agents (*vRA_Ordner*\Agents*Agent_Name*\):

– Die Datei „VRMAgent.exe.config“

– Die Datei „RepoUtil.exe.config“

Sichern Sie für DEMs die folgenden Informationen:

1 Den Namen des Agents.

2 Die folgenden Dateien im Installationsordner des DEM (*vRA_Ordner*\Distributed Execution Manager*DEM_Name*>\):

– Die Datei „ManagerService.exe.config“

– Die Datei „policy.config“

Sichern Sie für Webkomponenten die folgenden Dateien:

1 Nur für den primären Webknoten, im Ordner „Model Manager-Daten“ (*vRA_Ordner*\Server)

– Den Ordner „ConfigTool“ (betrifft nur den primären Webknoten)

– Die Datei „policy.config“

2 Die folgenden Dateien im Installationsordner (*vRA_Ordner*\Server\Website\):

– Die Datei „Web.config“

3 Die folgenden Dateien im Installationsordner (*vRA_Ordner*\Web API\):

– Die Datei „Web.config“

– Die Datei „policy.config“

4 Den Namen der IIS-Instanz.

Aktivieren des Manager Service-Failover-Hosts

Wenn auf dem aktiven Manager Service-Host ein Systemfehler auftritt, können Sie als Ersatz einen passiven Manager Service-Host heraufstufen. Sie können vRealize Automation so konfigurieren, dass ein sekundärer Failover-Server aktiviert wird, wenn auf dem Manager Service-Host ein Systemfehler auftritt.

Voraussetzungen

Wenn Sie den F5-Lastausgleich verwenden, stellen Sie sicher, dass aktive und passive Manager Service-Knoten korrekt mit dem Lastausgleich konfiguriert sind. Diese Konfiguration ist erforderlich, um Ping-Ausfälle des Proxy-Agent zu vermeiden.

1 Melden Sie sich beim F5-Lastausgleich an und wählen Sie **Lokaler Datenverkehr > Pools** aus.

2 Wählen Sie den Manager Service-Pool aus.

3 Klicken Sie im Abschnitt „Konfiguration“ auf **Erweitert**.

4 Wählen Sie die Option **Ablegen für Aktion bei ausgefallenem Dienst** aus.

5 Klicken Sie auf **OK** und anschließend auf **Fertig**.

Weitere Informationen hierzu finden Sie im Handbuch *Installieren von vRealize Automation 7.3*.

Vorgehensweise

1 Ändern Sie den Starttyp für den vCloud Automation Center-Manager Service auf dem aktiven Manager Service-Host in den manuellen Starttyp um, wenn das System verfügbar ist.

   a Wählen Sie auf dem aktiven Server **Start > Verwaltung > Dienste** aus.

   b Wählen Sie **Manuell** als Starttyp für den vCloud Automation Center-Dienst aus.

   c Halten Sie den VMware vCloud Automation Center-Dienst an.

2 Legen Sie den passiven Manager Service-Host als aktiven Host fest, indem Sie als Starttyp des vRealize Automation-Manager Service den automatischen Start festlegen und den Dienst dann starten.

   a Wählen Sie auf dem aktiven Server **Start > Verwaltung > Dienste** aus.

   b Wählen Sie **Automatisch** als Starttyp für den vRealize Automation aus.

   c Starten Sie den VMware vCloud Automation Center-Dienst.

3 (Optional) Öffnen Sie ein neues Browserfenster und stellen Sie sicher, dass Sie die Manager Service-URL für die Integritätsprüfung unter `https://MS_LB_FQDN/VMPSProvision` aufrufen können. *MS_LB_FQDN* steht dabei für Ihren Manager Service-Lastausgleichs-FQDN.

Systemwiederherstellung von vRealize Automation

Ein Systemadministrator verwendet Sicherungen, um vRealize Automation nach einem Systemausfall in einen funktionellen Zustand wiederherzustellen. Wenn IaaS-Komponenten wie z. B. Manager Service-Maschinen ausfallen, müssen Sie diese erneut installieren.

Wenn Sie von einer Sicherung wiederherstellen, sind nach der Sicherung bereitgestellte Maschinen noch vorhanden, aber werden nicht von vRealize Automation verwaltet. Sie werden z. B. nicht in der Elementenliste für den Besitzer angezeigt. Verwenden Sie den Infrastruktur-Organisator, um virtuelle Maschinen zu importieren und sie wieder verwalten zu können.

Führen Sie diese Schritte der Reihe nach durch, beginnend mit der ersten Komponente, die wiederhergestellt werden muss. Wenn eine Komponente ordnungsgemäß funktioniert, muss sie nicht wiederhergestellt werden.

1 Wiederherstellen von vRealize Automation-Datenbanken auf Seite 41

Ein Systemadministrator stellt die IaaS-MSSQL-Datenbank und die PostgreSQL-Datenbank wiederher.

2 Wiederherstellen der vRealize Automation-Appliance und des Lastausgleichsdiensts auf Seite 43

Wenn ein Fehler auftritt, stellt ein Systemadministrator die vRealize Automation-Appliance wieder her. Wenn ein Lastausgleichsdienst verwendet wird, stellt der Administrator den Lastausgleichsdienst sowie die virtuellen Appliances wiederher, die der Dienst verwaltet. Wenn während der Wiederherstellung ein Hostname geändert wird, müssen Sie Konfigurationsdateien entsprechend aktualisieren.

3 Wiederherstellen der IaaS-Website, Manager Services sowie deren Lastausgleichsdienste auf Seite 44

Ein Systemadministrator stellt die IaaS-Website und Manager Service sowie deren zugehörige Lastausgleichsdienste wiederher.

4 Neuinstallieren des DEM-Orchestrators und der DEM Workers auf Seite 47

Bei einem Fehler installiert ein Systemadministrator alle DEMs neu.

5 Neuinstallieren der IaaS-Agents auf Seite 47

Der Systemadministrator installiert alle IaaS-Agents neu, die wiederhergestellt werden müssen.

Wiederherstellen von vRealize Automation -Datenbanken

Ein Systemadministrator stellt die IaaS-MSSQL-Datenbank und die PostgreSQL-Datenbank wiederher.

Stellen Sie eine Datenbank in den folgenden Situationen wiederher:

- Wenn beide Datenbanken ausfallen, stellen Sie sie vom letzten bekannten Zeitpunkt wiederher, zu dem beide Datenbanken gesichert wurden.
- Wenn eine Datenbank ausfällt, stellen Sie diese wiederher. Setzen Sie die funktionale Datenbank auf die Version zurück, welche während der Erstellung der Sicherung zur Wiederherstellung der ausgefallenen Datenbank verwendet wurde.

Die Sicherungsdauer kann von Datenbank zu Datenbank unterschiedlich sein. Je größer die Differenz zwischen den letzten Betriebszeiten der Datenbanken ist, desto höher ist die Wahrscheinlichkeit eines Datenverlusts.

Sie sollten vollständige Datenbanken von VMs sichern, anstatt eine PostgreSQL-Datenbank direkt zu sichern. Informationen zur Wiederherstellung einer PostgreSQL-Datenbank finden Sie im VMware-Knowledgebase-Artikel Migration von einer externen vPostgres-Appliance zu einer vPostgres-Instanz, die sich in der vCAC-Appliance befindet (2083562).

Datenbank-Kennwortsätze

Zur Sicherheit der IaaS-MSSQL-Datenbank ist ein Sicherheitskennwortsatz erforderlich, um einen Verschlüsselungsschlüssel zum Schutz der Daten zu generieren. Sie legen diesen Kennwortsatz bei der Installation von vRealize Automation fest.

Wenden Sie sich für Informationen bezüglich Verlust oder Änderung eines Kennwortsatzes an den technischen Support von VMware.

Konfigurieren der SQL-Datenbank für einen neuen Hostnamen

Sie können für denselben Hostnamen eine SQL-Datenbank in vRealize Automation aus einer Sicherung wiederherstellen, ohne dass weitere Schritte erforderlich sind. Bei der Wiederherstellung auf einem Host mit einem anderen Namen wären hingegen zusätzliche Schritte zur Überprüfung der Konfigurationsinformationen erforderlich.

Vorgehensweise

1 Aktualisieren Sie die Datenbankeinträge.

   a Suchen Sie in SQL Server Management Studio die folgende Tabelle.

   `DynamicOps.RepositoryModel.Models`

   b Suchen Sie in der Tabelle die Zeichenfolge `Data Source` und aktualisieren Sie den SQL Server-Hostnamen im FQDN-Format. Aktualisieren Sie jede Instanz der Verbindungszeichenfolge.

   `Data Source=`*`neuer-Datenbank-Server-FQDN`*`;...`

2 Aktualisieren Sie auf jedem IaaS-Website-Host, der nicht neu installiert wird, den Namen des Datenbankserver-Hosts.

   a Öffnen Sie die folgende Datei in einem Texteditor.

   `C:\Programme (x86)\VMware\vCAC\Server\Model Manager Web\Web.config`

   b Nehmen Sie die folgenden Änderungen vor.

   - Suchen Sie die Zeichenfolge `Data Source` und aktualisieren Sie den SQL Server-Hostnamen im FQDN-Format. Aktualisieren Sie jede Instanz der Verbindungszeichenfolge.

     `Data Source=`*`neuer-Datenbank-Server-FQDN`*

   - Wenn Sie auch den Datenbanknamen geändert haben, aktualisieren Sie `Initial Catalog`.

     `Initial Catalog=`*`neuer-Datenbank-Name`*`;`

   c Speichern und schließen Sie `Web.config`.

3 Öffnen Sie als Administrator eine Eingabeaufforderung und führen Sie `iisreset` aus.

4 Aktualisieren Sie auf jedem Host mit dem IaaS-Manager-Dienst, der nicht neu installiert wird, den Namen des Datenbankservers-Hosts.

   a Öffnen Sie die folgende Datei in einem Texteditor.

   `C:\Programme (x86)\VMware\vCAC\Server\ManagerService.exe.config`

   b Nehmen Sie die folgenden Änderungen vor.

   - Suchen Sie die Zeichenfolge `Data Source` und aktualisieren Sie den SQL Server-Hostnamen im FQDN-Format. Aktualisieren Sie jede Instanz der Verbindungszeichenfolge.

     `Data Source=`*`neuer-Datenbank-Server-FQDN`*

   - Wenn Sie auch den Datenbanknamen geändert haben, aktualisieren Sie `Initial Catalog`.

     `Initial Catalog=`*`neuer-Datenbank-Name`*`;`

   c Speichern und schließen Sie `ManagerService.exe.config`.

5 Starten Sie den Manager Service neu.

Weiter

Wiederherstellen der vRealize Automation -Appliance und des Lastausgleichsdiensts

Wenn ein Fehler auftritt, stellt ein Systemadministrator die vRealize Automation-Appliance wieder her. Wenn ein Lastausgleichsdienst verwendet wird, stellt der Administrator den Lastausgleichsdienst sowie die virtuellen Appliances wiederher, die der Dienst verwaltet. Wenn während der Wiederherstellung ein Hostname geändert wird, müssen Sie Konfigurationsdateien entsprechend aktualisieren.

Unter folgenden Bedingungen kann das Wiederherstellen einer ausgefallenen virtuellen Appliance erforderlich sein:

- Sie führen eine Minimalbereitstellung aus und Ihre einzige vRealize Automation-Appliance schlägt fehl oder wird beschädigt.
- Sie führen eine verteilte Bereitstellung aus, und nicht alle, aber einige virtuelle Appliances fallen aus.
- Sie führen eine verteilte Bereitstellung aus, und sämtliche virtuelle Appliances fallen aus.

Wie Sie einen Lastausgleichsdienst für eine vRealize Automation-Appliance oder virtuelle Appliance bereitstellen, richtet sich nach Ihrem Bereitstellungstyp und danach, welche Appliances fehlgeschlagen sind.

- Wenn Sie eine einzelne virtuelle Appliance mit unverändertem Namen verwenden, stellen Sie die virtuelle Appliance wiederher, oder stellen Sie sie erneut bereit und stellen Sie eine Gruppe von gesicherten Dateien wiederher. Es sind keine weiteren Schritte erforderlich.
- Wenn Sie eine verteilte Bereitstellung ausführen, welche einen Lastausgleichsdienst verwendet, und Sie den Namen der virtuellen Appliance oder die IP-Adresse des Lastausgleichsdiensts ändern, müssen Sie die Appliance erneut bereitstellen und ihre Sicherungsdateien wiederherstellen. Sie müssen zudem Zertifikate für Ihre Bereitstellung neu generieren und kopieren.

Weitere Informationen zum erneuten Bereitstellen, erneuten Konfigurieren oder Hinzufügen von virtuellen Appliances zu einem Cluster finden Sie in der *Installieren von vRealize Automation 7.3*-Dokumentation für die vRealize Automation-Appliance.

Vorgehensweise

1 Stellen Sie die vRealize Automation-Appliance erneut bereit.

   Nach der erneuten Bereitstellung der vRealize Automation-Appliance müssen Sie auch die Appliance-Datenbank konfigurieren, wenn dies auf Ihre Systemkonfiguration anwendbar ist.

2 Stellen Sie sämtliche gesicherten Dateien wiederher.

3 Überprüfen Sie die Dateiberechtigungen und Besitzer für die wiederhergestellten Dateien.

   a Stellen Sie sicher, dass der vCAC-Benutzer die Dateien im `vcac`-Verzeichnis besitzt und nur der vCAC-Benutzer über Lese- und Schreibberechtigungen verfügt. Aktualisieren Sie die geänderten Einstellungen.

   b Stellen Sie sicher, dass der Root-Benutzer die Dateien im `apache2`-Verzeichnis besitzt und nur der Besitzer über Lese- und Schreibberechtigungen verfügt. Aktualisieren Sie die geänderten Einstellungen.

   c Stellen Sie sicher, dass der vCO-Benutzer die Dateien im `vco`-Verzeichnis besitzt und nur der Besitzer über Lese- und Schreibberechtigungen verfügt. Aktualisieren Sie die geänderten Einstellungen.

   Wenn der Hostname bzw. die virtuelle IP-Adresse unverändert ist, ist der Wiederherstellungsvorgang abgeschlossen.

4 Wenn Sie einen Lastausgleichsdienst verwenden und sich die dazugehörige IP-Adresse geändert hat, erstellen Sie die Zertifikate für jede der virtuellen Appliances neu und kopieren Sie die Zertifikate.

   a Unter Verwendung eines Befehls in folgendem Format erhalten Sie ein Zertifikat:

   ```
   C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe
   \Vcac-Config.exe GetServerCertificates -url https://VA FQDN
   --FileName .\Vcac-Config-time-stamp.data -v
   ```

   b Unter Verwendung eines Befehls in folgendem Format registrieren Sie Ihr Lösungsbenutzerzertifikat:

   ```
   C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe
   \Vcac-Config.exe RegisterSolutionUser -url https://VA FQDN --Tenant vsphere.local
   -cu administrator@vsphere.local -cp vmware --FileName .\Vcac-Config-time-stamp.data -v
   ```

   c Unter Verwendung eines Befehls in folgendem Format registrieren Sie die Ereignisüberschriften mit dem neuen Benutzer der Lösung:

   ```
   C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe Regis-
   terCatalogTypes -v
   ```

   d Unter Verwendung eines Befehls in folgendem Format verschieben Sie die Informationen zu Ihrem Lösungsbenutzerzertifikat in die Datenbank:

   ```
   C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\Cafe
   \Vcac-Config.exe MoveRegistrationDataToDB -d vcac -s localhost
   -f .\Vcac-Config-time-stamp.data -v
   ```

5 Navigieren Sie zur Verwaltungskonsole der vRealize Automation-Appliance und vergewissern Sie sich, dass die SSL-, Datenbank- und SSO-Einstellungen ordnungsgemäß konfiguriert sind.

6 Aktualisieren Sie geänderte Einstellungen.

7 Starten Sie den vRealize Automation-Server-Dienst oder speichern Sie die Seite mit den SSO-Einstellungen.

8 Konfigurieren Sie den Lastausgleichsdienst, um den Datenverkehr an die virtuellen Appliances zu verteilen.

Weiter

„Wiederherstellen des IaaS-Website-Diensts oder des Web-Lastausgleichsdiensts“, auf Seite 45

Wiederherstellen der IaaS-Website, Manager Services sowie deren Lastausgleichsdienste

Ein Systemadministrator stellt die IaaS-Website und Manager Service sowie deren zugehörige Lastausgleichsdienste wiederher.

1 Wiederherstellen des IaaS-Website-Diensts oder des Web-Lastausgleichsdiensts auf Seite 45

   Wenn der Server für Ihren IaaS-Website-Dienst oder Web-Lastausgleichsdienst fehlschlägt, stellt ein Systemadministrator die IaaS-Website-Komponenten wieder her und konfiguriert den Lastausgleichsdienst im Falle geänderter Hostnamen neu.

2 Wiederherstellen des Manager Service oder Manager Service-Lastausgleichsdiensts auf Seite 46

   Wenn der Server für Ihren Manager Service oder Lastausgleichsdienst fehlschlägt, stellt ein Systemadministrator den Manager Service wiederher und konfiguriert den Lastausgleichsdienst im Falle geänderter Hostnamen neu.

Wiederherstellen des IaaS-Website-Diensts oder des Web-Lastausgleichsdiensts

Wenn der Server für Ihren IaaS-Website-Dienst oder Web-Lastausgleichsdienst fehlschlägt, stellt ein Systemadministrator die IaaS-Website-Komponenten wieder her und konfiguriert den Lastausgleichsdienst im Falle geänderter Hostnamen neu.

Sie können den Server oder Lastausgleichsdienst durch erneutes Installieren wiederherstellen. Sie können den Server oder Lastausgleichsdienst auch umbenennen. Wenn Sie den Server umbenennen, müssen Sie die Konfigurationsdateien bearbeiten, um den neuen Hostnamen für nicht wiederhergestellte Komponenten verwenden zu können.

Weitere Informationen finden Sie in der Dokumentation zu *Installieren von vRealize Automation 7.3*.

Vorgehensweise

1 Installieren Sie die Website-Komponente mithilfe des benutzerdefinierten IaaS-Installationsprogramms.

  Installieren Sie nicht zum jetzigen Zeitpunkt die ModelManagerData-Komponente.

  Um den Verlust von verschlüsselten Daten zu verhindern, verwenden Sie denselben Kennwortsatz wie bei der ursprünglichen Installation.

2 Wenn Sie über Sicherungen von Konfigurationsdateien verfügen, kopieren Sie die Dateien auf den Server, auf dem Sie die Installation vornehmen möchten, und stellen Sie sicher, dass diese Einstellungen für Ihre aktuelle Bereitstellung korrekt sind.

3 Wenn Sie bei der erneuten Installation der Website-Maschine oder des Lastausgleichsdiensts den Hostnamen geändert haben, aktualisieren Sie den Hostnamen in den zugehörigen Konfigurationsdateien.

  Wenn in Ihrer Bereitstellung kein Lastausgleichsdienst verwendet wird, entspricht die Adresse dem Hostnamen der Maschine, auf der die Model Manager-Datenkomponente installiert ist. Verwenden Sie für eine Umgebung mit Web-Lastausgleichsdienst die Adresse des Website-Lastausgleichsdiensts.

Dateipfad	Maschinentyp
<*vCAC Folder*>\Server\Website\Web.config	Maschinen, auf denen die Website-Komponente installiert ist.
<*vCAC Folder*>\Server\ManagerService.exe.config	Maschinen, auf denen eine Manager Service-Komponente installiert ist.
<*vCAC Folder*>\Distributed Execution Manager\<*DEM Name*>\DynamicOps.DEM.exe.config	Maschinen, auf denen DEM-Worker oder DEM-Orchestrator installiert sind.
<*vCAC Folder*>\Agents\<*Agent Name*>\<*Agent Config File*>	Sämtliche installierte Maschinen und Agenten.
<*vCAC-Ordner*>\Server\Model Manager Data\Cafe\Vcac-Config.exe.config	Maschinen, auf denen eine Model Manager-Dienstkomponente installiert ist.

4 Suchen Sie für jede Datei die Zeile `key="repositoryAddress"` und ändern Sie den Wert des `value`-Attributs, um auf die Adresse Ihrer Website zu zeigen.

  Beispiel:

  `value="https://myWebsite.myhostname.name:Port/repository/`

5 Wenn Sie die primäre IaaS-Website-Komponente erneut installieren und über eine Sicherung der Metamodell-Daten verfügen, kopieren Sie die Daten auf die neue Website.

  Führen Sie diesen Schritt nicht durch, wenn Sie eine sekundäre Website-Komponente erneut installieren.

  Kopieren Sie die folgenden Ordner aus dem Installationsordner unter (`<vCAC Folder>\Server\`):

  - Model Manager-Datenordner

- ConfigTool-Ordner

Wiederherstellen des Manager Service oder Manager Service-Lastausgleichsdiensts

Wenn der Server für Ihren Manager Service oder Lastausgleichsdienst fehlschlägt, stellt ein Systemadministrator den Manager Service wiederher und konfiguriert den Lastausgleichsdienst im Falle geänderter Hostnamen neu.

Wenn der Server für Ihren Manager Service oder Lastausgleichsdienst fehlschlägt, können Sie ihn durch erneutes Installieren wiederherstellen. Wenn Sie den Server oder Lastausgleichsdienst umbenennen, müssen Sie die Konfigurationsdateien für nicht wiederhergestellte Komponenten bearbeiten, sodass bei ihnen der neue Hostname verwendet wird.

Voraussetzungen

„Wiederherstellen des IaaS-Website-Diensts oder des Web-Lastausgleichsdiensts“, auf Seite 45.

Vorgehensweise

1 Installieren Sie alle zutreffenden Manager Service-Maschinen erneut.

   a Stellen Sie sicher, dass die vollqualifizierten Domänennamen (FQDNs) für den Speicherort für die Wiederherstellung korrekt sind.

   b Stellen Sie sicher, dass der FQDN für den Manager Service (und nicht für den Lastausgleichsdienst) mit dem FQDN für den lokalen Host übereinstimmt.

   c Stellen Sie sicher, dass es sich bei dem Kennwortsatz um denselben wie bei der ursprünglichen Installation handelt.

2 Wenn der Hostname des Manager Service bzw. des Lastausgleichsdiensts geändert wurde, aktualisieren Sie sämtliche DEM-Konfigurationsdateien.

   a Öffnen Sie auf dem Server, auf dem sich der Agent bzw. DEM befindet, die Datei `DynamicOps.DEM.exe.config` in einem Editor.

   Der Dateispeicherort lautet wie folgt, wobei *DEO* den Namen von Distributed Execution Manager Orchestrator für den Distributed Execution Manager Worker darstellt.

   `C:\Programme (x86)\VMware\vCAC\Distributed Execution Manager\`*`DEO Name`*`\DynamicOps.`*`DEO`*`.exe.config`

   b Suchen Sie das Element `endpoint` und ändern Sie den Wert des `address`-Attributs in den neuen Hostnamen des Manager Service bzw. Manager Service-Lastausgleichsdiensts.

   Beispielsweise `address="https://MSHostName.domain.name/VMPS`.

   c Wiederholen Sie diesen Schritt für jeden Agent oder DEM in Ihrer Bereitstellung.

3 Wenn der Hostname des Service Manager bzw. des Lastausgleichsdiensts geändert wurde, aktualisieren Sie sämtliche Agent-Konfigurationsdateien.

   a Öffnen Sie auf dem Server, auf dem sich der Agent befindet, die Datei `DynamicOps.DEM.exe.config` in einem Editor.

   Der Dateispeicherort lautet wie folgt, wobei *DEO* den Namen von Distributed Execution Manager Orchestrator für den Distributed Execution Manager Worker darstellt.

   `C:\Programme (x86)\VMware\vCAC\Agents\`*`Agent Name`*`\DynamicOps.`*`Agent Name`*`.exe.config`

   b Suchen Sie das Element `endpoint` und ändern Sie den Wert des `address`-Attributs in den neuen Hostnamen des Manager Service bzw. Manager Service-Lastausgleichsdiensts.

   Beispiel: `address="https://MSHostName.domain.name/VMPS`

   c Wiederholen Sie diesen Schritt für jeden Agent in Ihrer Bereitstellung.

4 Starten Sie den Dienst für jede Datei `ManagerService.exe.config` neu.

Weiter

„Neuinstallieren des DEM-Orchestrators und der DEM Workers“, auf Seite 47

Neuinstallieren des DEM-Orchestrators und der DEM Workers

Bei einem Fehler installiert ein Systemadministrator alle DEMs neu.

Befolgen Sie die Anleitungen in *Installieren von vRealize Automation 7.3* für die Installation eines DEM-Orchestrators und DEM-Workers.

Beim Neuinstallieren eines DEM-Workers oder -Orchestrators ist es ratsam, die zuvor verwendeten Namen zu verwenden. Wenn Sie Namen angeben, die zuvor verwendet wurden, erhalten Sie eine Nachricht ähnlich der folgenden.

```
DEM-Name ist bereits vorhanden. Klicken Sie auf „Ja“ zum Eingeben eines anderen Namens für diesen DEM. Klicken Sie auf „Nein“, wenn Sie einen DEM mit demselben Namen wiederherstellen oder neu installieren.
```

Klicken Sie auf **Nein**, um den Namen wiederzuverwenden und mit der Installation fortzufahren.

Weiter

„Neuinstallieren der IaaS-Agents“, auf Seite 47.

Neuinstallieren der IaaS-Agents

Der Systemadministrator installiert alle IaaS-Agents neu, die wiederhergestellt werden müssen.

Installieren Sie den DEM-Orchestrator und die DEM-Workers neu. Installieren Sie anschließend die IaaS-Agents neu. Anleitungen zum Installieren von IaaS-Agents finden Sie unter *Installieren von vRealize Automation 7.3*.

Wenn Sie vSphere-Agents neu installieren, verwenden Sie denselben Endpointnamen wie den zum Zeitpunkt der Installation.

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.

Vorgehensweise

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.

Vorgehensweise

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
`frequency.dow=<day-of-week>`	Tag, an dem die Datenerfassung stattfindet.
`frequency.hod=<hour-of-day>`	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. Sie können ein Konvertierungstool wie etwa www.dailycoding.com/UTILS/CONVERTER/IMAGETOBASE64.ASPX verwenden.
- cURL muss auf der Maschine installiert sein, auf der Sie die Befehle ausführen.
- Sie benötigen Anmeldedaten als vRealize Automation-Benutzer mit der Systemadministrator-Rolle.

Vorgehensweise

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

Betriebssystem	Befehl
Linux/Mac	`export VCAC=<VA URL>`
Windows	`set VCAC=<VA URL>`

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

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

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	`export AUTH="Bearer <Auth Token>"`
Windows	`set AUTH=Bearer <Auth Token>`

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

Betriebssystem	Befehl
Linux/Mac	`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":"<filename>","contentType":"image/png","image":"<IMAGE DATA as base64 string>"}'`
Windows	`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\":\"<filename>\",\"contentType\":\"image/png\",\"image\":\"<IMAGE DATA as base64 string>\"}"`

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	`curl https://$VCAC/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: $AUTH" --request DELETE`
Windows	`curl https://%VCAC%/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: %AUTH%" --request DELETE`

Anpassen von Daten-Rollover-Einstellungen

Sie können vRealize Automation-Daten-Rollover-Einstellungen aktivieren und 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 konfigurieren, die vRealize Automation Daten in der von IaaSverwendeten SQL Server-Datenbank beibehält, bevor diese archiviert oder gelöscht werden. Diese Funktion ist standardmäßig 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-Appliance-Zeitzonenkonfiguration ausgeführt. Mit der Einstellung `DataRollover MaximumAgeInDays` können Sie die maximale Aufbewahrungsdauer der Daten in Tagen festlegen.

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.

Hinweis Berücksichtigen Sie vorhandene Systemdaten und die potenziellen Auswirkungen auf die Systemleistung, bevor Sie Daten-Rollover aktivieren. Beispiel: Wenn Sie diese Funktion ein Jahr, nachdem mit der Ausführung von vRealize Automation in Ihrer Umgebung begonnen wurde, aktivieren, müssen Sie überprüfen, ob der Wert von `DataRollover MaximumAgeInDays` auf 300 oder höher gesetzt wurde, um sicherzustellen, dass die Aktivierung der Daten-Rollover-Funktion die Systemleistung nicht beeinträchtigt.

Vorgehensweise

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 IsArchiveEnabled	Gibt an, ob Rollover-Daten nach Erreichen der maximalen Tageszahl in Archivtabellen verschoben werden sollen. Standardmäßig ist dieser Wert auf „True“ festgelegt. Wenn Sie den Wert auf „False“ festlegen, werden alle Daten, die älter sind als in der Einstellung `DataRollover MaximumAgeInDays` 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. Standardmäßig ist dieser Wert auf 90 Tage festgelegt.
DataRollover Status	Gibt an, ob Daten-Rollover aktiviert werden kann. Zum Aktivieren von Daten-Rollover legen Sie den Wert auf „Aktiviert“ fest. Standardmäßig ist dieser Wert auf „Deaktiviert“ festgelegt. Wenn Sie diesen Workflow deaktivieren, während er ausgeführt wird, hat dies keine Auswirkungen auf den aktuellen Workflow. Der nächste Workflow wird jedoch deaktiviert.

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

Das Feld „Wert“ für die entsprechende Einstellung kann nun bearbeitet werden, und Sie können den Cursor in das Feld setzen, um den Wert zu ändern.

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="600000"/>`
- `<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-Arbeitselementen (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-Dienstkontos 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.

Vorgehensweise

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
MaxOutstandingResourceIntensive-WorkItems	Grenzwert für die gleichzeitige Bereitstellung (der Standardwert ist 8)
CloneExecutionTimeout	Zeitüberschreitungsintervall für die Ausführung der virtuellen Bereitstellung
SetupOSExecutionTimeout	Zeitüberschreitungsintervall für die Ausführung der virtuellen Bereitstellung
CloneTimeout	Zeitüberschreitungsintervall für die Klonbereitstellung bei der virtuellen Bereitstellung
SetupOSTimeout	Zeitüberschreitungsintervall für das Setup des Betriebssystems bei der virtuellen Bereitstellung
CloudInitializeProvisioning	Zeitüberschreitungsintervall für die Initialisierung der Cloud-Bereitstellung
MaxOutstandingDataCollectionWorkItems	Grenzwert für die gleichzeitige Datenerfassung
InventoryTimeout	Zeitüberschreitungsintervall für die Ausführung der Bestandslistendatenerfassung
PerformanceTimeout	Zeitüberschreitungsintervall für die Ausführung der Leistungsdatenerfassung
StateTimeout	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 *ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds* – 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.

Vorgehensweise

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
RepositoryWorkflowTimerCallbackMiliSeconds	Überprüft den Repository-Dienst oder den Model Manager-Webdienst auf Aktivitäten. Der Standardwert ist 10000.
ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds	Sucht nach abgelaufenen Maschinen-Leases. Der Standardwert ist 3600000.
BulkRequestWorkflowTimerCallbackMiliSeconds	Sucht nach Massenanforderungen. Der Standardwert ist 10000.
MachineRequestTimerCallbackMiliSeconds	Sucht nach Maschinenanforderungen. Der Standardwert ist 10000.
MachineWorkflowCreationTimerCallbackMiliSeconds	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.

Vorgehensweise

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
RepositoryLogSeverity	Hier wird festgelegt, unterhalb welchen Schweregrads Ereignisse ignoriert werden sollen. ■ *Error* protokolliert nur behebbare Fehler und Fehler von darüber hinausgehendem Schweregrad. ■ *Warning* protokolliert nicht kritische Warnungen und Warnungen von darüber hinausgehendem Schweregrad. ■ *Information* protokolliert alle Informationsmeldungen und Meldungen von darüber hinausgehendem Schweregrad. ■ *Verbose* protokolliert einen Debugging-Eintrag und kann die Leistung beeinträchtigen. Beispielsweise `<add key="RepositoryLogSeverity" value="Warning" />`.
RepositoryLogCategory	Hier wird eine Kategorie festgelegt, für die alle Ereignisse jeden Schweregrads protokolliert werden. Beispiel: `<add key="RepositoryLogCategory" value="MissingMachines,UnregisteredMachines,AcceptMachineRequest,RejectMachineRequest" />` protokolliert alle Ereignisse von fehlenden Maschinen oder Maschinen, deren Registrierung aufgehoben wurde, sowie jede angenommene oder abgelehnte Maschinenanforderung.

4 Speichern und schließen Sie die Datei.

5 Wählen Sie **Start > Verwaltung > Dienste** aus und starten Sie den vCloud Automation Center-Dienst neu.

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 3-5. Optionen zum Überwachen und Anzeigen von Protokollen

Ziel	Rolle	Menüabfolge und Beschreibung
Zeigen Sie Informationen über stattgefundene Aktionen an, wie beispielsweise den Aktionstypen, Datum und Uhrzeit der Aktion usw.	IaaS-Administrator	Zeigen Sie Standardprotokollinformationen an oder steuern Sie Anzeigeinhalt mit den Spalten- und Filteroptionen. Wählen Sie **Infrastruktur > Überwachung > Überwachungsprotokoll** aus. 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.
Zeigen Sie den Status des geplanten und verfügbaren Distributed Execution Managers und andere Workflows an.	IaaS-Administrator	Zeigen Sie den Workflowstatus an und öffnen Sie optional einen bestimmten Workflow, um seine Details anzuzeigen. Wählen Sie **Infrastruktur > Überwachung > DEM-Status** aus.
Zeigen Sie Protokolldaten an und exportieren Sie sie optional.	IaaS-Administrator	Zeigen Sie Standardprotokollinformationen an oder steuern Sie Anzeigeinhalt mit den Spalten- und Filteroptionen. Wählen Sie **Infrastruktur > Überwachung > Protokoll** aus.
Zeigen Sie den Status und den Verlauf des ausgeführten Distributed Execution Managers und andere Workflows an.	IaaS-Administrator	Zeigen Sie den Workflowverlauf an und öffnen Sie optional einen bestimmten Workflow, um seine Details zur Ausführung anzuzeigen. Wählen Sie **Infrastruktur > Überwachung > Workflowverlauf** aus.
Zeigen Sie eine Liste von Ereignissen an, einschließlich Ereignistyp, Uhrzeit, Benutzer-ID usw. Zeigen Sie optional eine Seite mit den Ereignisdetails an.	Systemadministrator	Zeigen Sie eine Liste von Ereignissen und deren zugeordnete Attribute an, wie beispielsweise Laufzeit, Ereignisbeschreibung, Mandantenname, Zieltyp und -ID sowie andere Charakteristiken. Wählen Sie **Administration > Ereignisse > Ereignisprotokolle** aus.
Überwachen Sie den Anforderungsstatus und zeigen Sie Details zu den Anforderungen an.	Mandantenadministrator oder Business-Gruppenmanager	Zeigen Sie den Status der Anforderungen an, für die Sie verantwortlich sind, bzw. die Ihre eigenen sind. Klicken Sie auf **Anforderungen**.
Zeigen Sie Informationen über die neuesten Ereignisse an.	IaaS-Administrator oder Mandantenadministrator	Zeigen Sie die neuesten Ereignisse für den zurzeit angemeldeten Benutzer an. Wählen Sie **Infrastruktur > Neueste Ereignisse** aus.

Überwachen von Ereignisprotokollen und Diensten

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

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 3-6. Identitätsdienstgruppe

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

Tabelle 3-7. 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 3-8. Servicekataloggruppe (Kontrolldienste)

Dienst	Beschreibung
notification-service	Benachrichtigungsdienst
workitem-service	Arbeitselementdienst
approval-service	Genehmigungsdienst
catalog-service	Servicekatalog

Tabelle 3-9. IaaS-Dienstgruppe

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

Tabelle 3-10. 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-Einstellungen > 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 Dienstnamen 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-Überwachungsereignisse in VMware Log Insight exportieren, um das Anzeigen von Überwachungsereignissen zu ermöglichen.

Voraussetzungen

Vorgehensweise

1 Melden Sie sich bei der Verwaltungsschnittstelle der virtuellen Appliance als Systemadministrator an.

2 Wählen Sie **vRA-Einstellungen > 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.

5 Klicken Sie auf **Einstellungen speichern**.

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

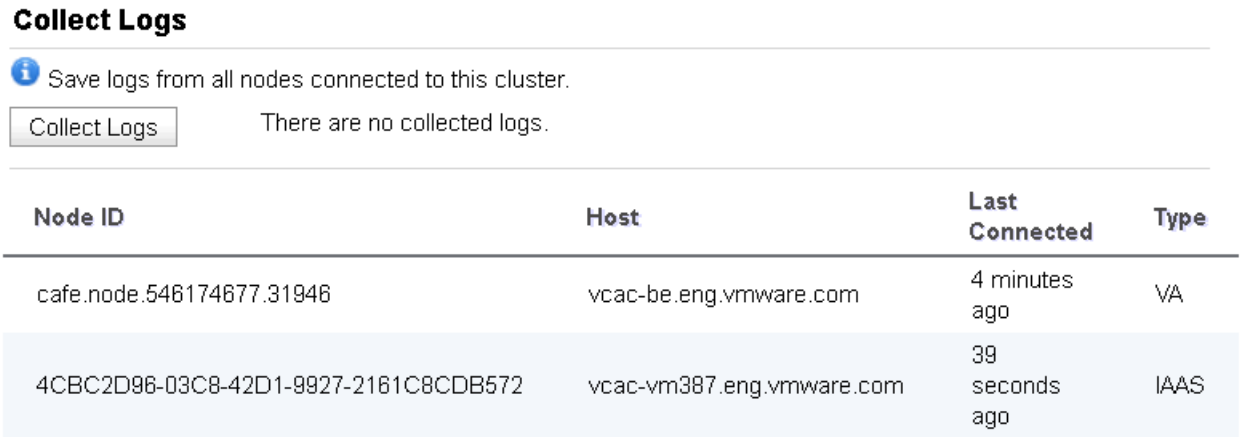
Anzeigen von Hostinformationen für Cluster in verteilten Bereitstellungen

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 3-1. Tabelle „Info zur verteilten Bereitstellung“



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. Weitere Informationen finden Sie unter „Erfassen von Protokollen für Cluster und verteilte Bereitstellungen“, auf Seite 61.

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.

Erfassen von Protokollen für Cluster und verteilte Bereitstellungen

Sie können eine ZIP-Datei erstellen, die alle Protokolldateien für Server in Ihrer Bereitstellung enthält.

In der Tabelle „Info zur verteilten Bereitstellung“ sind die Knoten aufgelistet, für die Protokolldateien erfasst werden.

Informationen zur Konfiguration der Bereitstellung der vRealize Automation-Appliance finden Sie unter *Installieren von vRealize Automation 7.3*.

Vorgehensweise

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

2 Klicken Sie auf **vRA-Einstellungen**.

3 Klicken Sie auf die Registerkarte **Cluster**.

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

4 Klicken Sie auf **Protokolle erfassen**.

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

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

Sie entfernen den Eintrag für einen Knoten aus der Tabelle „Info zur verteilten Bereitstellung“, wenn der Knoten aus Ihrem Bereitstellungscluster entfernt wird oder wenn Sie ein Management-Agent-Zertifikat ersetzen.

Vorgehensweise

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 **vRA-Einstellungen**.

3 Klicken Sie auf die Registerkarte **Cluster**.

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

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

```
./vcac-config cluster-config-node --action list
```

5 Suchen Sie die Knoten-ID, z. B. `cafe.node.46686239.17144`, in der JSON-Ausgabe.

6 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:

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

7 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 funktionelle Integrität einer ausgewählten virtuellen vRealize Automation-Maschine.

IaaS-Administratoren können den Integritätsdienst für das Ausführen von Tests konfigurieren, die die Integrität einer ausgewählten virtuellen vRealize Automation-Maschine untersuchen. Die Tests stellen fest, ob die Komponenten registriert und alle erforderlichen Ressourcen verfügbar sind. Die folgende Tabelle zeigt die Test-Suites des Integritätsdienstes und einige Beispieltests in jeder Suite.

Option	Beschreibung
Systemtests für vRealize Automation	■ SSO-/Identity VA-Verbindungstest ■ Lizenzprüfung in vRealize Automation – Ist die Lizenz abgelaufen? ■ Root-Kennwort-Überprüfung in der virtuellen vRealize Automation-Appliance – Läuft das Kennwort bald ab?
Mandantentests für vRealize Automation	■ Überprüfung der Speicherpfade der vSphere-Reservierung ■ Überprüfung der Reservierungsrichtlinie für Reservierungszuweisungen ■ Überprüfung des Portaldienststatus
Tests für vRealize Orchestrator	■ Überprüfung der Anzahl aktiver vRO-Knoten ■ Überprüfung der Nutzung des Java-Speicher-Heaps auf den vRO-Knoten ■ Überprüfung des Status des vro-Serverdienstes auf den vRO-Knoten

Nachdem Sie eine Test-Suite auf einer virtuellen Maschine ausgeführt haben, gibt der Integritätsdienst Rückmeldung zur Anzahl der bestandenen oder fehlgeschlagenen Tests. Über fehlgeschlagene Tests gibt der Integritätsdienst die folgenden Informationen:

- Die Ursache für das Fehlschlagen
- Einen Link zu weiteren Informationen, die Ihnen dabei helfen können, das Problem zu beheben.

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

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

Durchführen von Systemprüfungen für vRealize Automation

Sie können den Integritätsprüfungsdienst für die Ausführung von Systemprüfungen auf einer ausgewählten virtuellen vRealize Automation-Appliance konfigurieren. Durch diese Prüfungen können Sie feststellen, ob Komponenten wie die vRealize Automation-Lizenz registriert sind und erforderlichen Ressourcen wie Arbeitsspeicher auf der virtuellen vRealize Automation-Appliance verfügbar sind.

Voraussetzungen

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

Vorgehensweise

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.
Beschreibung	(Optional) Beschreibung.
Produkt	Wählen Sie vRealize Automation aus.
Planen	Häufigkeit, mit der die Prüfungen durchgeführt werden.

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.

Abschnitt	Option	Beschreibung
Virtuelle vRealize Automation-Appliance		
	Adresse des öffentlichen Webservers	Basis-URL für den vRealize Automation-Lastausgleich Beispiel: https://*load-balancer-host.domain*/.
	Adresse der SSH-Konsole	Vollqualifizierter Domänenname der vRealize Automation-Appliance. Beispiel: *va-host.domain*.
	Benutzer der SSH-Konsole	root
	Kennwort der SSH-Konsole	Das Root-Kennwort.
vRealize Automation-Systemmandant		
	Administrator des Systemmandanten	Administrator
	Kennwort des Systemmandanten	Das Administratorkennwort.
vRealize Automation-Festplattenspeicherüberwachung		
	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.

Weiter

„Anzeigen der Ergebnisse des vRealize Automation-Integritätsprüfungstests“, auf Seite 66

Ausführen von Mandantentests für vRealize Automation

Sie können den Integritätsprüfungsdienst für die Ausführung von Mandantentests auf einer ausgewählten virtuellen vRealize Automation-Appliance konfigurieren. Diese Tests ermitteln, ob Mandantenkomponenten wie z. B. Software-Dienste registriert sind und ob erforderliche Ressourcen, wie beispielsweise virtuelle vSphere-Maschinen, zur Verfügung stehen.

Voraussetzungen

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

Vorgehensweise

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.
Beschreibung	(Optional) Beschreibung.
Produkt	Wählen Sie vRealize Automation aus.
Planen	Häufigkeit, mit der die Prüfungen durchgeführt werden.

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.

Abschnitt	Option	Beschreibung
Virtuelle vRealize Automation-Appliance		
	vRealize Automation-Web-Adresse	Basis-URL für vRealize Automation. Beispielsweise https://*va-host.domain*/.
	Adresse der SSH-Konsole	Vollqualifizierter Domänenname des SSH-Hosts. Beispielsweise *ssh-host.domain*.
	Benutzer der SSH-Konsole	root
	Kennwort der SSH-Konsole	Kennwort für Root.
vRealize Automation-Mandant		
	Zu testender Mandant	Zu Testzwecken ausgewählter Mandant.
	Benutzername des Fabric-Administrators	Benutzername des Fabric-Administrators.
	Kennwort des Fabric-Administrators	Kennwort des Fabric-Administrators.
vRealize Automation-Systemmandant		

Abschnitt	Option	Beschreibung
	Administrator des Systemmandanten	Administrator
	Kennwort des Systemmandanten	Kennwort des Administrators.

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.

Weiter

„Anzeigen der Ergebnisse des vRealize Automation-Integritätsprüfungstests“, auf Seite 66

Durchführen von Tests für vRealize Orchestrator

Sie können den Integritätsprüfungsdienst für das Ausführen von Tests für vRealize Orchestrator auf dem vRealize Orchestrator-Host konfigurieren. Diese Tests stellen sicher, dass Komponenten wie der vro-Serverdienst registriert sind und erforderliche Ressourcen, wie z. B. ausreichende Java-Arbeitsspeicher-Heaps, verfügbar sind.

Voraussetzungen

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

Vorgehensweise

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.
Beschreibung	(Optional) Beschreibung.
Produkt	Wählen Sie vRealize Orchestrator aus.
Planen	Häufigkeit, mit der die Prüfungen durchgeführt werden.

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.

Abschnitt	Option	Beschreibung
vRealize Orchestrator-Host/Lastausgleich		
	Clientadresse	Vollqualifizierter Domänenname des vRealize Orchestrator-Hosts. Beispielsweise *vro-host.domain* oder die Basis-URL für den vRealize Orchestrator-Lastausgleich, https://*load-balancer-host.domain*/.

Abschnitt	Option	Beschreibung
	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.
vRealize Orchestrator-Instanzen hinter dem Lastausgleich		
	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.

Weiter

„Anzeigen der Ergebnisse des vRealize Automation-Integritätsprüfungstests“, auf Seite 66

Anzeigen der Ergebnisse des vRealize Automation -Integritätsprüfungstests

Nach Abschluss eines Integritätsprüfungstests für eine virtuelle Maschine können Sie die Ergebnisse 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 Test-Suite wurde nach Zeitplan oder bei Bedarf ausgeführt.
- Melden Sie sich bei der vRealize Automation-Konsole als **IaaS-Administrator** oder **Mandantenadministrator** an.

Vorgehensweise

1 Wählen Sie **Verwaltung > Integrität**.

2 Klicken Sie auf die Mitte einer Testkarte.

Es wird eine Liste mit dem Status jedes Tests angezeigt. Klicken Sie für alle fehlgeschlagenen Tests auf **Ursache**, um festzustellen, warum der Test fehlgeschlagen ist. Wenn ein **Wartung**-Link verfügbar ist, klicken Sie darauf, um in einem Artikel zu erfahren, wie Sie das Problem beheben können.

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 eine Eingabeaufforderung und führen Sie diese Befehle auf jeder virtuellen vRealize Automation-Appliance 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
  ```

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 3-11. Auswählen eines Ressourcenüberwachungsszenarios

Ressourcenüberwachungsszenario	Erforderliche Berechtigungen	Speicherort
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.	**Fabric-Administrator** (Ressourcenauslastung auf Computing-Ressourcen in Ihrer Fabric-Gruppe überwachen)	**Infrastruktur > Computing-Ressourcen > Computing-Ressourcen**
Überwachung der Maschinen, die aktuell bereitgestellt sind und von vRealize Automation verwaltet werden.	**Fabric-Administrator**	**Infrastruktur > Maschinen > Verwaltete Maschinen**
Überwachung des aktuell zugeteilten Umfangs an Speicher, Arbeitsspeicher und Maschinenkontingenten Ihrer Reservierung sowie Bestimmen der für die Reservierung verfügbaren Kapazität.	**Fabric-Administrator** (Ressourcenauslastung für Reservierungen auf Ihren Computing-Ressourcen und physischen Maschinen überwachen)	**Infrastruktur > Reservierungen > Reservierungen**
Überwachung des aktuell verbrauchten Umfangs an Speicher, Arbeitsspeicher und Maschinenkontingenten Ihrer Business-Gruppen sowie Bestimmen der für die Reservierung verfügbaren Kapazität.	■ **Mandantenadministrator** (Ressourcenauslastung für alle Gruppen in Ihrem Mandanten überwachen) ■ **Business-Gruppenmanager** (Ressourcenauslastung für von Ihnen verwaltete Gruppen überwachen)	**Administration > Benutzer und Gruppen > Business-Gruppen**

Sie können Ihrer vRealize Automation-Homepage auch Ressourcenüberwachungs-Portlets hinzufügen, um andere Ressourcenauslastungsstatistiken zu überwachen.

Verwalten von Ressourcenberichten

Sie können Echtzeitressourcenberichte zur Startseite hinzufügen, um die virtuelle, physische und Cloud-Ressourcenverwendung zu überwachen, das Layout zu ändern und ihre Daten an andere Anwendungen zu exportieren.

Hinzufügen von Berichten zur Startseite

Sie können der Startseite einen oder mehrere IaaS-Berichte hinzufügen. Diese Echtzeitberichte listen Ihre zuletzt geöffneten Aufgaben, Kataloganforderungen, bereitgestellten Elemente und bereitgestellten Maschinen aufgeschlüsselt nach Benutzer, Blueprint, Computing-Ressource und Business-Gruppe auf. Zwei Berichte zeigen zudem aktualisierte Übersichten über Rückforderungseinsparungen an.

Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole an.

Vorgehensweise

1 Navigieren Sie zur Seite **Start**.

2 Klicken Sie auf das Symbol „Bearbeiten“  oben rechts auf der Seite, und klicken Sie im Dropdown-Menü auf **Portlets hinzufügen**.

3 Klicken Sie für jeden Bericht, den Sie der Startseite hinzufügen möchten, auf **Hinzufügen**.

Wenn die Schaltfläche **Hinzufügen** deaktiviert ist, weist dies darauf hin, dass der Bericht bereits hinzugefügt wurde.

4 Klicken Sie auf **Schließen**.

Weiter

„Konfigurieren des Berichtslayouts“, auf Seite 69.

Konfigurieren des Berichtslayouts

Sie können die Startseite so konfigurieren, dass Berichte in einer, zwei, drei oder vier Spalten angezeigt werden. Sie können einen Bericht von einer Spalte in eine andere verschieben.

Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole an.

Vorgehensweise

1 Navigieren Sie zur Seite **Start**.

2 Klicken Sie auf das Symbol „Bearbeiten“ () oben rechts auf der Seite, und klicken Sie im Dropdown-Menü auf **Layout ändern**.

3 Wählen Sie ein Berichtslayout aus.

Option	Beschreibung
1 Spalte	Legen Sie das Berichtslayout mit einer Spalte an.
2 Spalten	Legen Sie das Berichtslayout mit zwei Spalten mit gleicher oder unterschiedlicher Breite an.
3 Spalten	Legen Sie das Berichtslayout mit drei Spalten mit gleicher oder unterschiedlicher Breite an.
4 Spalten	Legen Sie das Berichtslayout mit vier gleich breiten Spalten an.

4 Klicken Sie auf **Übernehmen**.

5 Zeigen Sie auf die Titelleiste eines Berichts.

Der Cursor wird zu einem Vierfachpfeil.

6 Ziehen Sie den Bericht an seine neue Position.

Die Berichtsbreite ändert sich und wird an die neue Position angepasst.

Exportieren von Berichtsdaten

Sie können IaaS-Berichte auf Ihrer Startseite in CSV-Dateien speichern und darin die Daten entsprechend Ihrer Bedürfnisse anpassen.

Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole an.
- „Hinzufügen von Berichten zur Startseite“, auf Seite 69.

Vorgehensweise

1 Navigieren Sie zur Seite **Start**.

2 Klicken Sie zum Speichern im Bericht auf **Als CSV-Datei exportieren**.

In manchen Browsern wird die Datei sofort gespeichert. In Firefox wird ein Dialogfeld mit Auswahlen für das Öffnen oder Speichern des Berichts mit Microsoft Excel oder einer anderen Anwendung geöffnet.

3 (Optional) Wählen Sie, ob Sie die Berichtsdaten öffnen oder speichern möchten, und welche Anwendung verwendet werden soll.

Ressourcenberichte

Ressourcenberichte zeigen Daten über verwendete und zurückgeforderte Maschinen und Ressourcen nach Besitzer, Computing-Ressource und Gruppe an.

Name	Beschreibung
Mein Posteingang	Zeigt eine Liste der zuletzt geöffneten Aufgaben in Ihrem Posteingang an. Klicken Sie auf eine Zeile, um die Detailseite einer Aufgabe anzuzeigen. Klicken Sie auf **Mehr**, um die vollständige Liste der Posteingangaufgaben anzuzeigen.
Meine offenen Anforderungen	Zeigt eine Liste der neuesten Kataloganforderungen an. Klicken Sie auf eine Zeile, um die Detailseite einer Anforderung anzuzeigen. Klicken Sie auf **Mehr**, um die vollständige Liste der Anforderungen anzuzeigen.
Meine neuesten Anforderungen	Zeigt eine Liste der neuesten Kataloganforderungen unabhängig vom Status an. Klicken Sie auf eine Zeile, um die Detailseite einer Anforderung anzuzeigen. Klicken Sie auf **Mehr**, um die vollständige Liste der Anforderungen anzuzeigen.
Meine Elemente	Zeigt eine Liste der neuesten bereitgestellten Elemente an. Klicken Sie auf eine Zeile, um die Detailseite eines Elements anzuzeigen. Klicken Sie auf **Mehr**, um die vollständige Liste der Elemente anzuzeigen.
Meine Gruppenanforderungen	Zeigt eine Liste der neuesten Kataloganforderungen für Benutzer in von Ihnen verwalteten Gruppen an. Klicken Sie auf eine Zeile, um die Detailseite einer Anforderung anzuzeigen. Klicken Sie auf **Mehr**, um die vollständige Liste der Anforderungen anzuzeigen.
Meine Gruppenelemente	Zeigt eine Liste der neuesten bereitgestellten Elemente für Benutzer in von Ihnen verwalteten Gruppen an. Klicken Sie auf eine Zeile, um die Detailseite eines Elements anzuzeigen. Klicken Sie auf **Mehr**, um die vollständige Liste der Elemente anzuzeigen.
Neu und interessant	Hebt Katalogelemente hervor, die zuletzt im Katalog zur Verfügung gestellt wurden.
Ereigniskalender	Zeigt einen Kalender mit wichtigen Ereignissen für Katalogelemente an, die Sie besitzen, wie z. B. Lease-Ablaufdatum und Maschinenvernichtung.
Business-Gruppen-Ressourcenzuteilungen	Zeigt die Ressourcenzuteilungen für Business-Gruppen in einem Mandanten an. Wenn Sie ein Mandantenadministrator sind, zeigt das Portlet die Ressourcenzuteilungen für alle Mandanten-Business-Gruppen an. Wenn Sie ein Business-Gruppenmanager sind, zeigt das Portlet die Ressourcenzuteilung für Ihre Business-Gruppen an.

Name	Beschreibung
IaaS-Kapazitätsauslastung nach Blueprint	Zeigt die Anzahl der Maschinen, die über die einzelnen Blueprints bereitgestellt werden, sowie die insgesamt von diesen Maschinen verwendeten Ressourcen an.
IaaS-Kapazitätsauslastung nach Gruppe	Zeigt die Anzahl der Maschinen, die den Benutzern in jeder Business-Gruppe gehören, sowie die insgesamt von diesen Maschinen verwendeten Ressourcen an.
IaaS-Kapazitätsauslastung nach Besitzer	Zeigt die Anzahl der Maschinen, die den einzelnen Benutzern gehören, sowie die insgesamt von diesen Maschinen verwendeten Ressourcen an.
IaaS-Kapazitätsauslastung nach Computing-Ressource	Zeigt die Anzahl der Maschinen, die in den einzelnen Computing-Ressourcen bereitgestellt werden, sowie die insgesamt von diesen Maschinen verwendeten Ressourcen an.
Meine Reisen	Zeigt einen Beispiel-Verbraucherbericht an.

Hinzufügen des Portlets für Business-Gruppen-Ressourcenzuteilungen zur Registerkarte „Start“

Das Portlet für Business-Gruppen-Ressourcenzuteilungen ist ein Dashboard-Portlet, das Sie der Registerkarte **Start** hinzufügen, um die Ressourcen für Business-Gruppen zu überwachen.

Wenn Sie ein Mandantenadministrator sind, zeigt das Portlet die Ressourcenzuteilungen für alle Mandanten-Business-Gruppen an. Wenn Sie ein Business-Gruppenmanager sind, zeigt das Portlet die Ressourcenzuteilung für Ihre Business-Gruppen an.

Wenn Sie kein Mandantenadministrator oder Business-Gruppenmanager sind, ist das Portlet nicht für die Installation auf Ihrer Registerkarte **Start** verfügbar.

Voraussetzungen

Melden Sie sich an der vRealize Automation-Konsole als **Mandantenadministrator** oder **Business-Gruppenmanager** an.

Vorgehensweise

1 Wählen Sie **Start** aus.

2 Klicken Sie in der rechten oberen Ecke auf das Symbol **Bearbeiten** ().

3 Wählen Sie **Portlets hinzufügen**.

4 Suchen Sie die Option „Business-Gruppen-Ressourcenzuteilungen“ und klicken Sie auf **Hinzufügen**.

5 Klicken Sie auf **Schließen**.

Das Portlet wird oben auf der Registerkarte „Start“ hinzugefügt.

6 Klicken Sie auf die Titelleiste des Portlets und ziehen Sie, um es an eine andere Stelle zu verschieben.

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 3-12. Terminologie der Ressourcenverwendung

Begriff	Beschreibung
Physisch	Zeigt die tatsächliche Arbeitsspeicher- oder Speicherkapazität einer Computing-Ressource an.
Reserviert	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 %.
Verwaltet	Zeigt an, dass die Maschine bereitgestellt ist und sich derzeit unter der vRealize Automation-Verwaltung befindet.
Zugewiesen	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 %.
Verwendet	Für die virtuelle Bereitstellung zeigt dies die Speichermenge an, die von bereitgestellten Maschinen verwendet wird. Wenn ein Standardspeicher verwendet wird, sind der verwendete Speicher und der zugewiesene Speicher identisch. Wird jedoch eine speichereffiziente Speichertechnologie verwendet (beispielsweise FlexClone oder Thin Provisioning), ist der verwendete Speicher normalerweise kleiner als der zugewiesene Speicher, da Maschinen genau die erforderliche Speichermenge verbrauchen.
Frei	Für die virtuelle Bereitstellung ist dies die ungenutzte physische Kapazität auf einem Speicherpfad.

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 an der vRealize Automation-Konsole 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.

Vorgehensweise

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.

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 an der vRealize Automation-Konsole 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.

Vorgehensweise

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 **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.

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“, auf Seite 75.

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“, auf Seite 77.

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 an der vRealize Automation-Konsole als **Fabric-Administrator** an.

Vorgehensweise

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 3-13. Datenerfassungstypen

Datenerfassungstyp	Beschreibung
Datenerfassung für Infrastrukturquellen-Endpoints	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. Die Endpoint-Datenerfassung wird alle vier Stunden ausgeführt.
Erfassung von Bestandslistendaten	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. Die Erfassung von Bestandslistendaten wird alle 24 Stunden ausgeführt. Das standardmäßige Zeitüberschreitungsintervall für die Erfassung von Bestandslistendaten beträgt zwei Stunden.
Erfassung von Zustandsdaten	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. Die Zustandsdatenerfassung wird alle 15 Minuten ausgeführt. Das standardmäßige Zeitüberschreitungsintervall für die Zustandsdatenerfassung beträgt eine Stunde.

Tabelle 3-13. Datenerfassungstypen (Fortsetzung)

Datenerfassungstyp	Beschreibung
Leistungsdatenerfassung (nur Computing-Ressourcen von vSphere)	Aktualisiert den Datensatz der durchschnittlichen CPU-, Speicherplatz-, Arbeitsspeicher- und Netzwerkauslastung für jede durch die Bestandslistendatenerfassung ermittelte virtuelle Maschine. Die Leistungsdatenerfassung wird alle 24 Stunden ausgeführt. Das standardmäßige Zeitüberschreitungsintervall für die Leistungsdatenerfassung beträgt zwei Stunden.
Erfassung von Netzwerk- und Sicherheitsbestandslistendaten (nur vSphere-Computing-Ressourcen)	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.
Erfassung von WMI-Daten (nur Windows-Computing-Ressourcen)	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.

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 an der vRealize Automation-Konsole als **IaaS-Administrator** an.

Vorgehensweise

1 Wählen Sie **Infrastruktur > Endpoints > Endpoints** aus.

2 Zeigen Sie auf den Endpoint, für den Sie eine Datenerfassung ausführen möchten, und klicken Sie auf **Datenerfassung**.

3 Klicken Sie auf **Starten**.

4 (Optional) Klicken Sie auf **Aktualisieren**, um eine aktualisierte Meldung über den Status der von Ihnen initiierten Datenerfassung zu erhalten.

5 Klicken Sie auf **Abbrechen**, um zur Seite Endpoints zurückzukehren.

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 an der vRealize Automation-Konsole als **Fabric-Administrator** an.

Vorgehensweise

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 an der vRealize Automation-Konsole als **Fabric-Administrator** an.

Vorgehensweise

1 Wählen Sie **Infrastruktur > Computing-Ressourcen > Computing-Ressourcen** aus.

2 Klicken Sie auf **Kosten aktualisieren**.

3 Klicken Sie auf **Jetzt anfordern**.

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 Zielmaschine 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 Datencenter-Standorts erforderlich sind:

1 Ein Systemadministrator entfernt die Informationen zum Datencenterstandort 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.

Die Massenimporte-Funktion importiert virtuelle Maschinen, die mit den definierten Daten, wie beispielsweise Reservierung, Speicherpfad, Blueprint, Besitzer und benutzerdefinierte Eigenschaften, interagiert. 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 Umgebung in eine andere.

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*.

Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole 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. In Abhängigkeit von Ihren Rechten wird die virtuelle Maschine auf der Registerkarte **Verwaltete Maschinen** oder der Registerkarte **Elemente** angezeigt.

Die Massenimportoption unterstützt nicht die Bereitstellungen, die über einen Blueprint vorgenommen werden, der ein NSX-Netzwerk und eine Sicherheitskomponente bzw. eine Softwarekomponente enthält.

Voraussetzungen

- Melden Sie sich an der vRealize Automation-Konsole 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*.

Vorgehensweise

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 **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
Endpoint	Erforderliche Informationen für den Zugriff auf einen Virtualisierungshost.
Computing-Ressource	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**.

2 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-Nr. – Ja oder Nein	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	Geben Sie für die Bereitstellung, die Sie in der vRealize Automation-Zielumgebung erstellen, einen neuen Namen ein (zum Beispiel den Namen der virtuellen Maschine). **Hinweis** 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.
Blueprint-ID	Geben Sie die ID des Blueprints in die vRealize Automation-Zielumgebung ein, die Sie zum Importieren der virtuellen Maschine verwenden. **Hinweis** 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 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.

b Wenn Sie eine virtuelle Maschine mit einer statischen IP-Adresse importieren, 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 ein Import 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 der Import 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 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
Startzeit	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.
Jetzt	Importvorgang direkt starten.
Verzögerung (Sekunden)	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.
Batchgröße	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.
Verwaltete Maschinen ignorieren	Behalten Sie die Deaktivierung bei.
Benutzervalidierung überspringen	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.
Import testen	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 an der vRealize Automation-Konsole als **Fabric-Administrator** und als **Business-Gruppenmanager** an.

Vorgehensweise

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
Endpoint	Erforderliche Informationen für den Zugriff auf einen Virtualisierungshost.
Computing-Ressource	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
Startzeit	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.
Jetzt	Importvorgang direkt starten.
Verzögerung (Sekunden)	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.
Batchgröße	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.
Verwaltete Maschinen ignorieren	Behalten Sie die Deaktivierung bei.
Benutzervalidierung überspringen	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.
Import testen	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 ™ 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 an der vRealize Automation-Konsole 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*.

Vorgehensweise

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
Endpoint	Erforderliche Informationen für den Zugriff auf einen Virtualisierungshost.
Computing-Ressource	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. 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. 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.	ImportBlueprint
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
Startzeit	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.
Jetzt	Migrationsvorgang direkt starten.
Verzögerung (Sekunden)	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.
Batchgröße	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.
Verwaltete Maschinen ignorieren	Behalten Sie die Deaktivierung bei.
Benutzervalidierung überspringen	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.
Import testen	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.

Index

S

T

U

V

W

Z